Classification des données d'utilisation

NetApp Data Classification

NetApp
February 02, 2026

Sommaire

Classification des données d’utilisation

Affichez les détails de gouvernance sur les données stockées dans votre organisation avec NetApp Data Classification

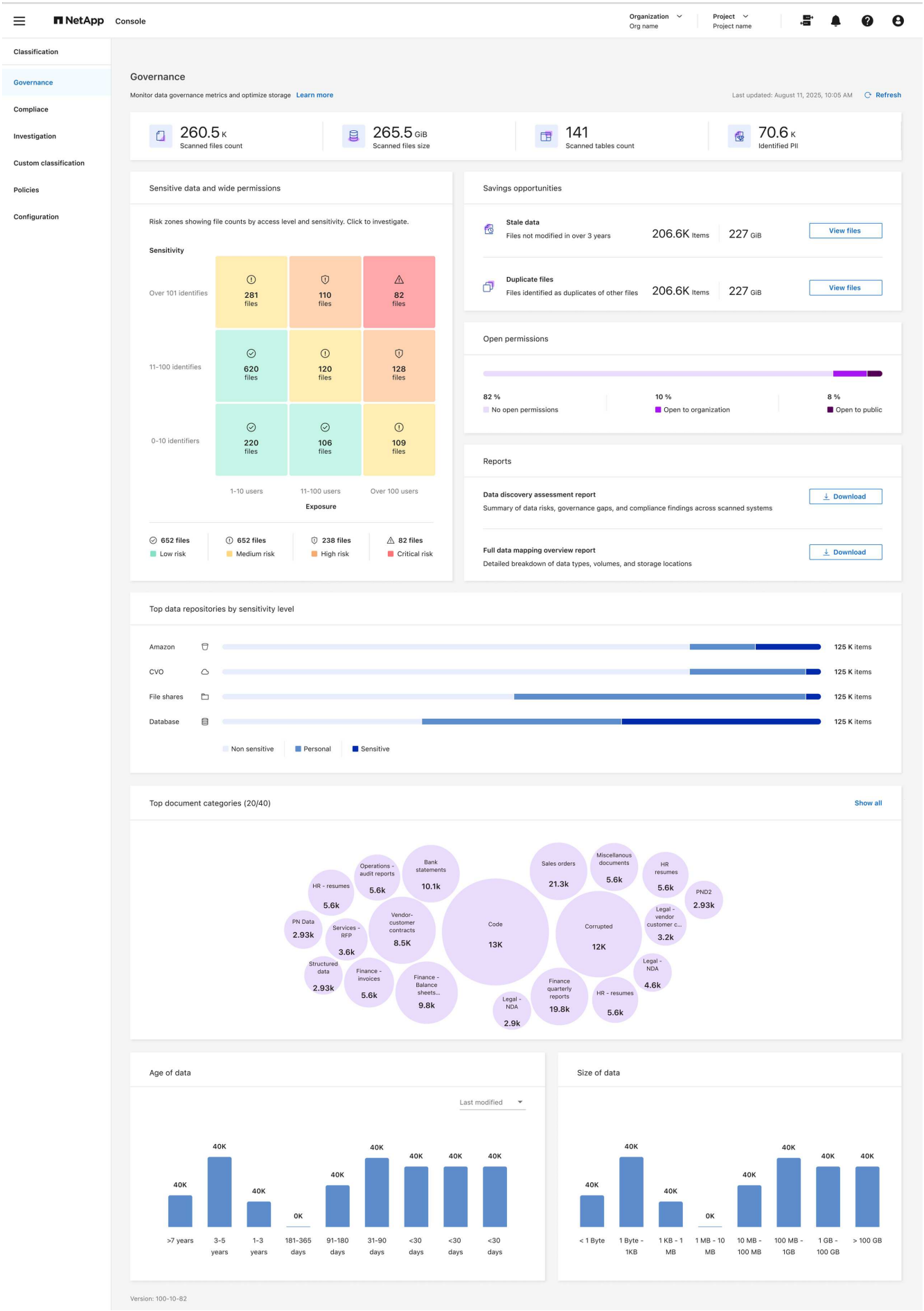
Maîtrisez les coûts liés aux données sur les ressources de stockage de votre organisation. La NetApp Data Classification identifie la quantité de données obsolètes, de fichiers en double et de fichiers très volumineux dans vos systèmes afin que vous puissiez décider si vous souhaitez supprimer ou hiérarchiser certains fichiers vers un stockage d’objets moins coûteux.

C’est ici que vous devriez commencer vos recherches. Depuis le tableau de bord de gouvernance, vous pouvez sélectionner un domaine pour une enquête plus approfondie.

De plus, si vous envisagez de migrer des données depuis des emplacements locaux vers le cloud, vous pouvez afficher la taille des données et si certaines d’entre elles contiennent des informations sensibles avant de les déplacer.

Consultez le tableau de bord de gouvernance

Le tableau de bord de gouvernance fournit des informations pour vous permettre d’augmenter l’efficacité et de contrôler les coûts liés aux données stockées sur vos ressources de stockage.


NetApp Console
Organization
Org name
Project
Project name
Classification
Governance
Compliace
Investigation
Custom classification
Policies
Configuration
Governance
Monitor data governance metrics and optimize storage Learn more
Last updated: August 11, 2025, 10:05 AM
Refresh
260.5 K
Scanned files count
265.5 GiB
Scanned files size
141
Scanned tables count
70.6 K
Identified PII
Sensitive data and wide permissions
Risk zones showing file counts by access level and sensitivity. Click to investigate.
Sensitivity
Over 101 identifies
11-100 identifies
0-10 identifiers
281 files
110 files
82 files
620 files
120 files
128 files
220 files
106 files
109 files
1-10 users
11-100 users
Over 100 users
Exposure
652 files
Low risk
652 files
Medium risk
238 files
High risk
82 files
Critical risk
Savings opportunities
Stale data
Files not modified in over 3 years
206.6K Items
227 GiB
View files
Duplicate files
Files identified as duplicates of other files
206.6K Items
227 GiB
View files
Open permissions
82 %
No open permissions
10 %
Open to organization
8 %
Open to public
Reports
Data discovery assessment report
Summary of data risks, governance gaps, and compliance findings across scanned systems
Download
Full data mapping overview report
Detailed breakdown of data types, volumes, and storage locations
Download
Top data repositories by sensitivity level
Amazon
CVO
File shares
Database
125 K items
Non sensitive
Personal
Sensitive
Top document categories (20/40)
Show all
Operations - audit reports 5.6k
Bank statements 10.1k
Sales orders 21.3k
Miscellanous documents 5.6k
HR resumes 5.6k
PND2 2.93k
HR - resumes 5.6k
PN Data 2.93k
Services - RFP 3.6k
Vendor-customer contracts 8.5K
Code 13K
Corrupted 12K
Legal - vendor customer c... 3.2k
Structured data 2.93k
Finance - invoices 5.6k
Finance - Balance sheets... 9.8k
Legal - NDA 2.9k
Finance quarterly reports 19.8k
HR - resumes 5.6k
Legal - NDA 4.6k
Age of data
Last modified
40K
>7 years
40K
3-5 years
40K
1-3 years
0K
181-365 days
40K
91-180 days
40K
31-90 days
40K
<30 days
40K
<30 days
40K
<30 days
Size of data
40K
< 1 Byte
40K
1 Byte - 1KB
40K
1 KB - 1 MB
0K
1 MB - 10 MB
40K
10 MB - 100 MB
40K
100 MB - 1GB
40K
1 GB - 100 GB
40K
> 100 GB
Version: 100-10-82

Étapes

1. Dans le menu de la NetApp Console , sélectionnez **Gouvernance > Classification**.
2. Sélectionnez **Gouvernance**.

   Le tableau de bord de gouvernance apparaît.

Examiner les possibilités d'économies

Le composant *Opportunités d'économie* affiche les données que vous pouvez supprimer ou hiérarchiser vers un stockage d'objets moins coûteux. Les données de *Saving Opportunities* sont mises à jour toutes les 2 heures. Vous pouvez également mettre à jour les données manuellement.

Étapes

1. Dans le menu Classification des données, sélectionnez **Gouvernance**.
2. Dans chaque mosaïque Opportunités d'économies du tableau de bord Gouvernance, sélectionnez **Optimiser le stockage** pour afficher les résultats filtrés dans la page Enquête. Pour découvrir les données que vous devriez supprimer ou transférer vers un stockage moins coûteux, étudiez les *Opportunités d'économie*.
   - **Données obsolètes** - Par défaut, les données sont considérées comme obsolètes si leur dernière modification remonte à plus de 3 ans. Vous pouvez [personnaliser la définition des données obsolètes](task-stale-data.html).
   - **Fichiers en double** - Fichiers dupliqués à d'autres emplacements dans les sources de données que vous analysez. "Voir quels types de fichiers en double sont affichés" .

Si l'une de vos sources de données implémente la hiérarchisation des données, les anciennes données qui résident déjà dans le stockage d'objets peuvent être identifiées dans la catégorie *Données obsolètes*.

Créer le rapport d'évaluation de la découverte de données

Le rapport d'évaluation de la découverte de données fournit une analyse de haut niveau de l'environnement analysé pour montrer les zones de préoccupation et les étapes de correction potentielles. Les résultats sont basés à la fois sur la cartographie et la classification de vos données. L'objectif de ce rapport est de sensibiliser à trois aspects importants de votre ensemble de données :

Fonctionnalité	Description
Préoccupations liées à la gouvernance des données	Une image détaillée de toutes les données que vous possédez et des domaines dans lesquels vous pouvez réduire la quantité de données pour économiser des coûts.
Expositions à la sécurité des données	Zones dans lesquelles vos données sont accessibles aux attaques internes ou externes en raison d'autorisations d'accès étendues.
Lacunes en matière de conformité des données	Où se trouvent vos informations personnelles ou sensibles, à des fins de sécurité et pour les DSAR (demandes d'accès aux données des personnes concernées).

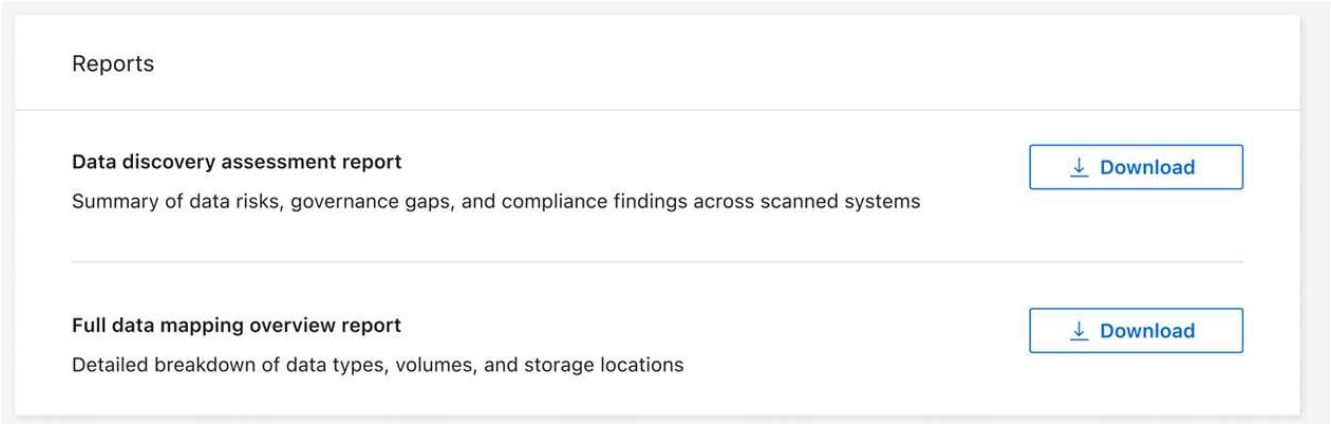
Avec le rapport, vous pouvez effectuer les actions suivantes :

- Réduisez les coûts de stockage en modifiant votre politique de conservation, ou en déplaçant ou en supprimant certaines données (données obsolètes ou en double).

- Protégez vos données disposant d'autorisations étendues en révisant les politiques de gestion des groupes globaux.
- Protégez vos données contenant des informations personnelles ou sensibles en déplaçant les PII vers des magasins de données plus sécurisés.

Étapes

1. Dans Classification des données, sélectionnez **Gouvernance**.
2. Dans la mosaïque des rapports, sélectionnez **Rapport d'évaluation de la découverte de données**.



Résultat

La classification des données génère un rapport PDF que vous pouvez consulter et partager.

Créer le rapport de synthèse du mappage des données

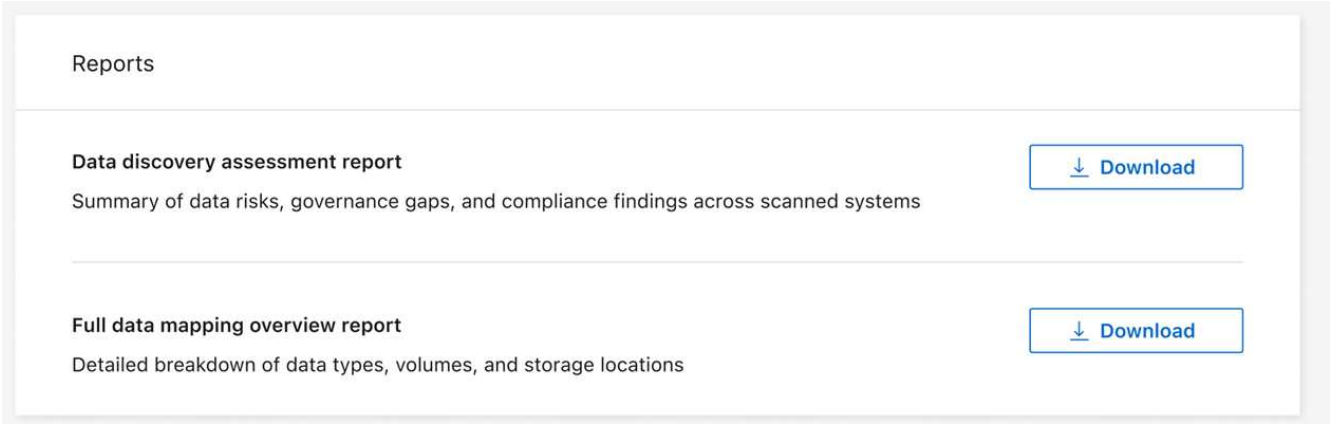
Le rapport d'aperçu du mappage des données fournit un aperçu des données stockées dans vos sources de données d'entreprise pour vous aider à prendre des décisions concernant les processus de migration, de sauvegarde, de sécurité et de conformité. Le rapport résume tous les systèmes et sources de données. Il fournit également une analyse pour chaque système.

Le rapport comprend les informations suivantes :

Catégorie	Description
Capacité d'utilisation	Pour tous les systèmes : répertorie le nombre de fichiers et la capacité utilisée pour chaque système. Pour les systèmes uniques : répertorie les fichiers qui utilisent le plus de capacité.
L'ère des données	Fournit trois tableaux et graphiques indiquant quand les fichiers ont été créés, modifiés pour la dernière fois ou consultés pour la dernière fois. 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 taille dans vos systèmes.

Étapes

1. Dans Classification des données, sélectionnez **Gouvernance**.
2. Dans la mosaïque des rapports, sélectionnez **Rapport d'aperçu complet du mappage des données**.



Résultat

La classification des données génère un rapport PDF que vous pouvez consulter et envoyer à d'autres groupes selon vos besoins.

Si le rapport est supérieur à 1 Mo, le fichier PDF est conservé sur l'instance de classification des données et vous verrez un message contextuel indiquant l'emplacement exact. Lorsque Data Classification est installé sur une machine Linux dans vos locaux ou sur une machine Linux que vous avez déployée dans le cloud, vous pouvez accéder directement au fichier PDF. Lorsque la classification des données est déployée dans le cloud, vous devez autoriser avec SSH l'instance de classification des données pour télécharger le fichier PDF.

Consultez les principaux référentiels de données classés par sensibilité des données

La zone *Principaux référentiels de données par niveau de sensibilité* du rapport Présentation du mappage des données répertorie les quatre principaux référentiels de données (systèmes et sources de données) qui contiennent les éléments les plus sensibles. Le graphique à barres de chaque système est divisé en :

- Données non sensibles
- Données personnelles
- Données personnelles sensibles

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

Étapes

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

Examiner les données sensibles et les autorisations étendues

La zone *Données sensibles et autorisations étendues* du tableau de bord de gouvernance affiche le nombre de fichiers contenant des données sensibles et disposant d'autorisations étendues. Le tableau présente les types d'autorisations suivants :

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

Étapes

1. Pour voir le nombre total de fichiers dans chaque catégorie, positionnez votre curseur sur chaque case.
2. Pour filtrer les résultats qui apparaîtront sur la page Enquête, sélectionnez une case et poursuivez vos recherches.

Examiner les données répertoriées par types d'autorisations ouvertes

La zone *Autorisations d'ouverture* du rapport Présentation du mappage des données affiche le pourcentage pour chaque type d'autorisations qui existent pour tous les fichiers en cours d'analyse. Le graphique montre les types d'autorisations suivants :

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

Étapes

1. Pour voir le nombre total de fichiers dans chaque catégorie, positionnez votre curseur sur chaque case.
2. Pour filtrer les résultats qui apparaîtront sur la page Enquête, sélectionnez une case et poursuivez vos recherches.

Vérifiez l'âge et la taille des données

Vous pouvez examiner les éléments des graphiques *Âge* et *Taille* du rapport Présentation du mappage des données pour voir s'il existe des données que vous devez supprimer ou transférer vers un stockage d'objets moins coûteux.

Étapes

1. Dans le graphique Âge des données, pour voir les détails sur l'âge des données, placez votre curseur sur un point du graphique.
2. Pour filtrer par tranche d'âge ou de taille, sélectionnez cet âge ou cette taille.
    - **Graphique de l'âge des données** - Catégorise les données en fonction de l'heure à laquelle elles ont été créées, de la dernière fois où elles ont été consultées ou de la dernière fois où elles ont été modifiées.
    - **Taille du graphique de données** - Catégorise les données en fonction de leur taille.

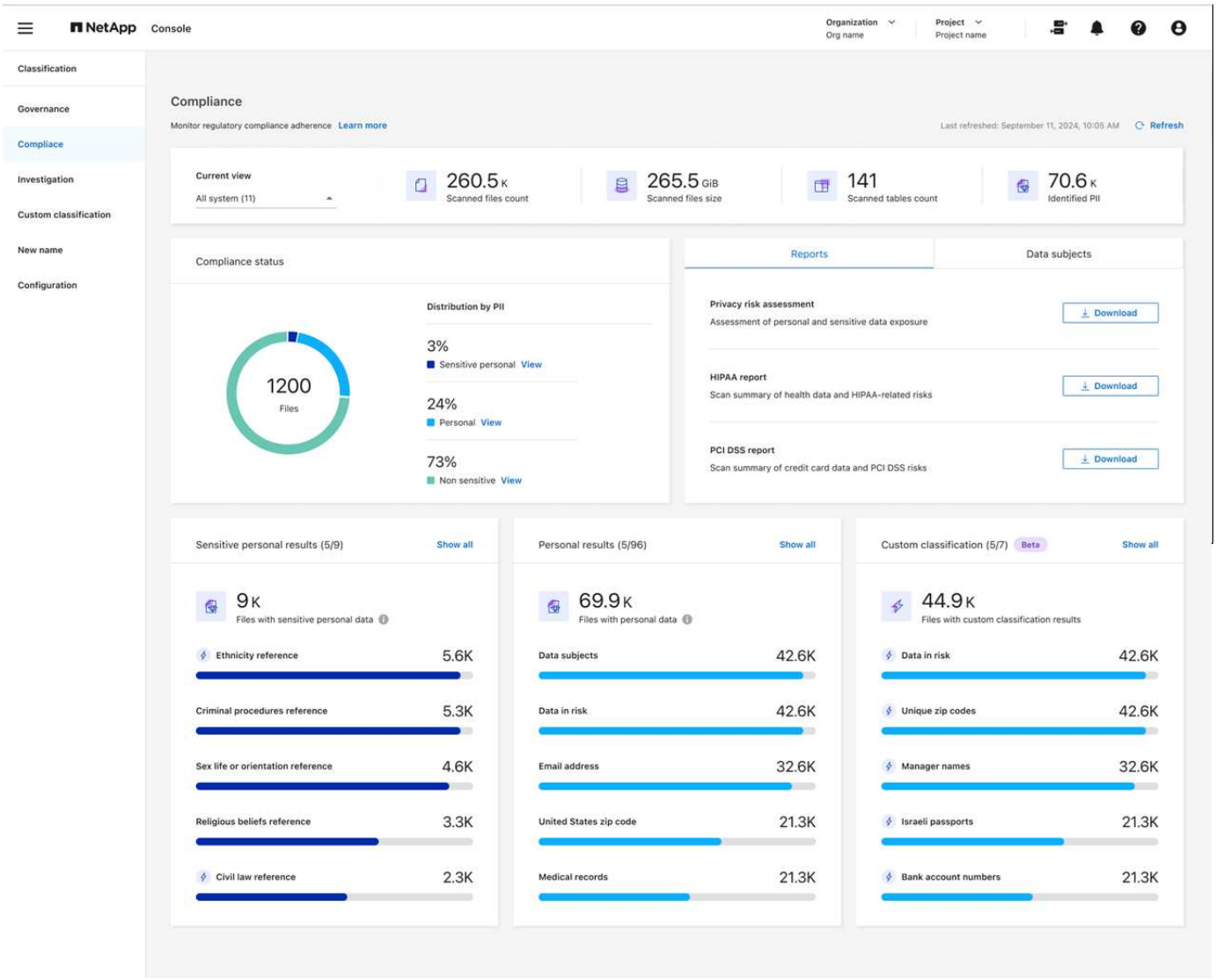
Si l'une de vos sources de données implémente la hiérarchisation des données, les anciennes données qui résident déjà dans le stockage d'objets peuvent être identifiées dans le graphique *Age of Data*.

Consultez les détails de conformité concernant les données privées stockées dans votre organisation avec NetApp Data Classification

Prenez le contrôle de vos données privées en consultant les détails sur les données personnelles (PII) et les données personnelles sensibles (SPII) de votre organisation. Vous pouvez également gagner en visibilité en examinant les catégories et les types de fichiers que NetApp Data Classification a trouvés dans vos données.

Les détails de conformité au niveau du fichier ne sont disponibles que si vous effectuez une analyse de classification complète. Les analyses de cartographie uniquement ne fournissent pas de détails au niveau du fichier.

Par défaut, le tableau de bord de classification des données affiche les données de conformité pour tous les systèmes et bases de données. Pour voir les données de certains systèmes uniquement, sélectionnez-les.



Vous pouvez filtrer les résultats de la page Enquête sur les données et télécharger un rapport des résultats sous forme de fichier CSV. Voir"Filtrage des données dans la page Enquête sur les données" pour plus de détails.

Afficher les fichiers contenant des données personnelles

La classification des données identifie automatiquement des mots, des chaînes et des modèles (Regex) spécifiques à l'intérieur des données. "Par exemple, les numéros de carte de crédit, les numéros de sécurité sociale, les numéros de compte bancaire, les mots de passe, etc."La classification des données identifie ce type d'informations dans des fichiers individuels, dans des fichiers au sein de répertoires (partages et dossiers) et dans des tables de base de données.

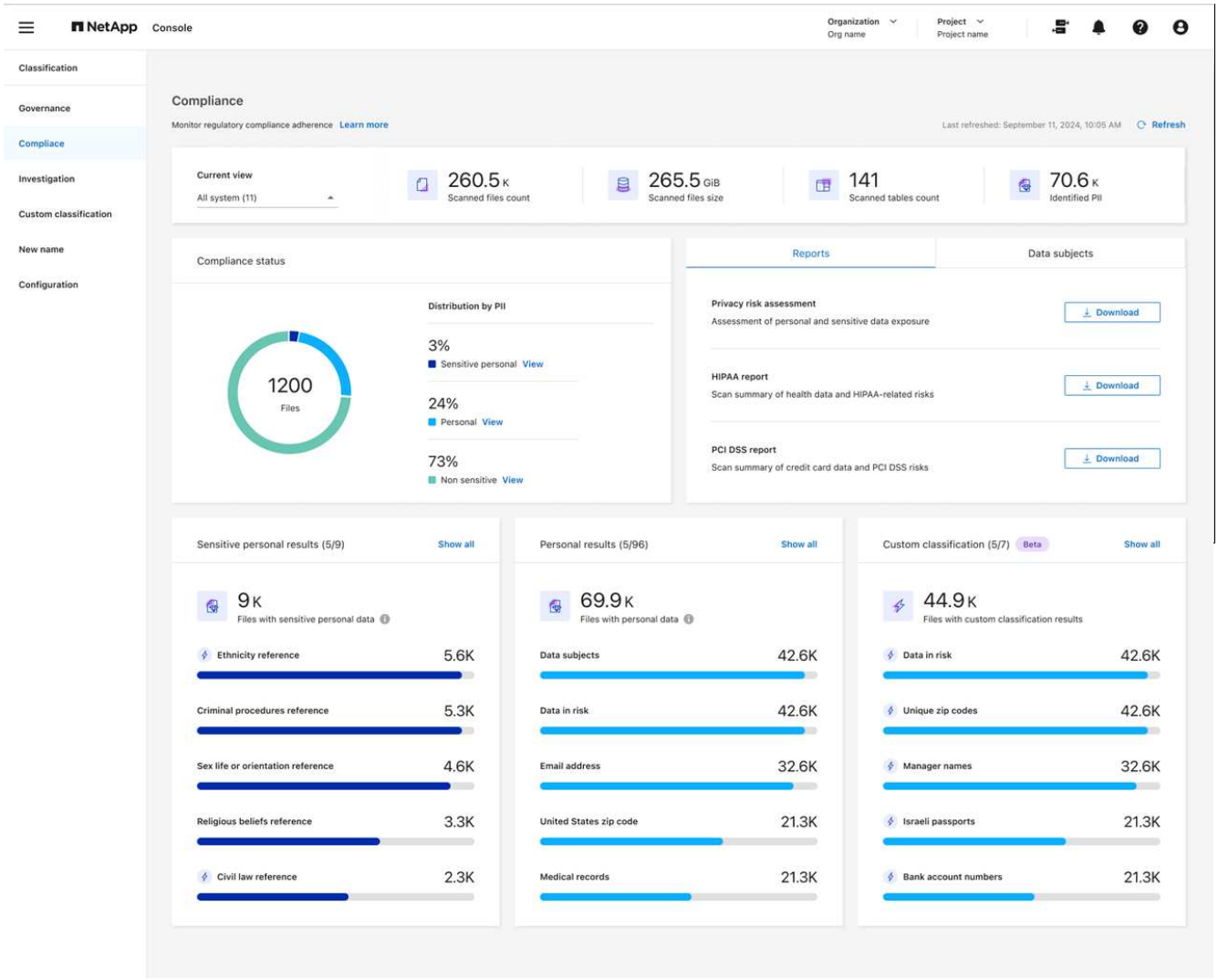
Vous pouvez également créer des termes de recherche personnalisés pour identifier les données personnelles

spécifiques à votre organisation. Pour plus d'informations, consultez la section "Créer une classification personnalisée" .

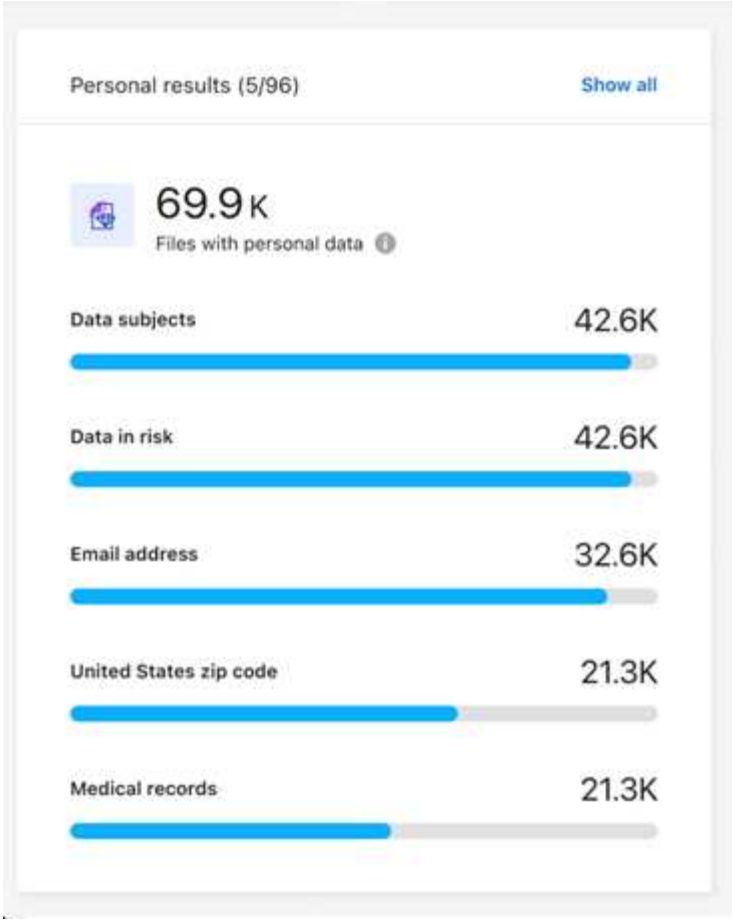
Pour certains types de données personnelles, la classification des données utilise la *validation de proximité* pour valider ses résultats. La validation s'effectue en recherchant un ou plusieurs mots-clés prédéfinis à proximité des données personnelles trouvées. Par exemple, la classification des données identifie un numéro de sécurité sociale américain (SSN) comme un SSN s'il voit un mot de proximité à côté de lui, par exemple, *SSN* ou *sécurité sociale*. "Le tableau des données personnelles" indique quand la classification des données utilise la validation de proximité.

Étapes

1. Dans le menu Classification des données, sélectionnez l'onglet **Conformité**.
2. Pour examiner les détails de toutes les données personnelles, sélectionnez l'icône à côté du pourcentage de données personnelles.

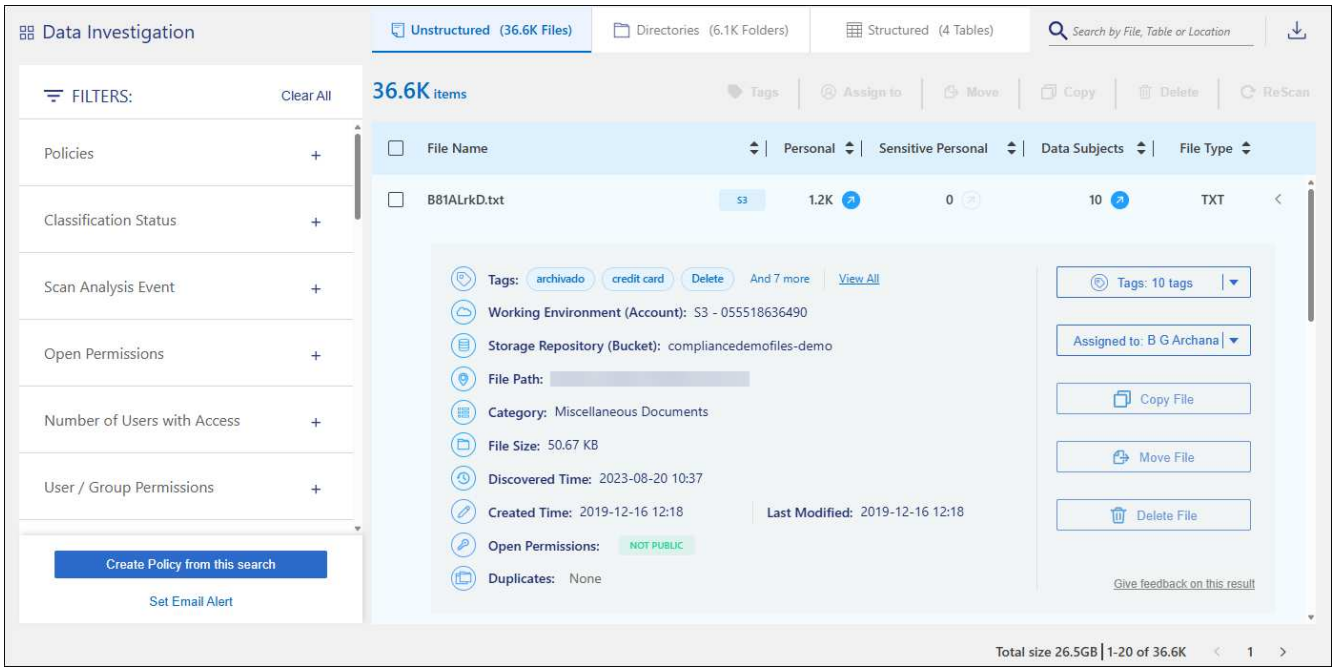


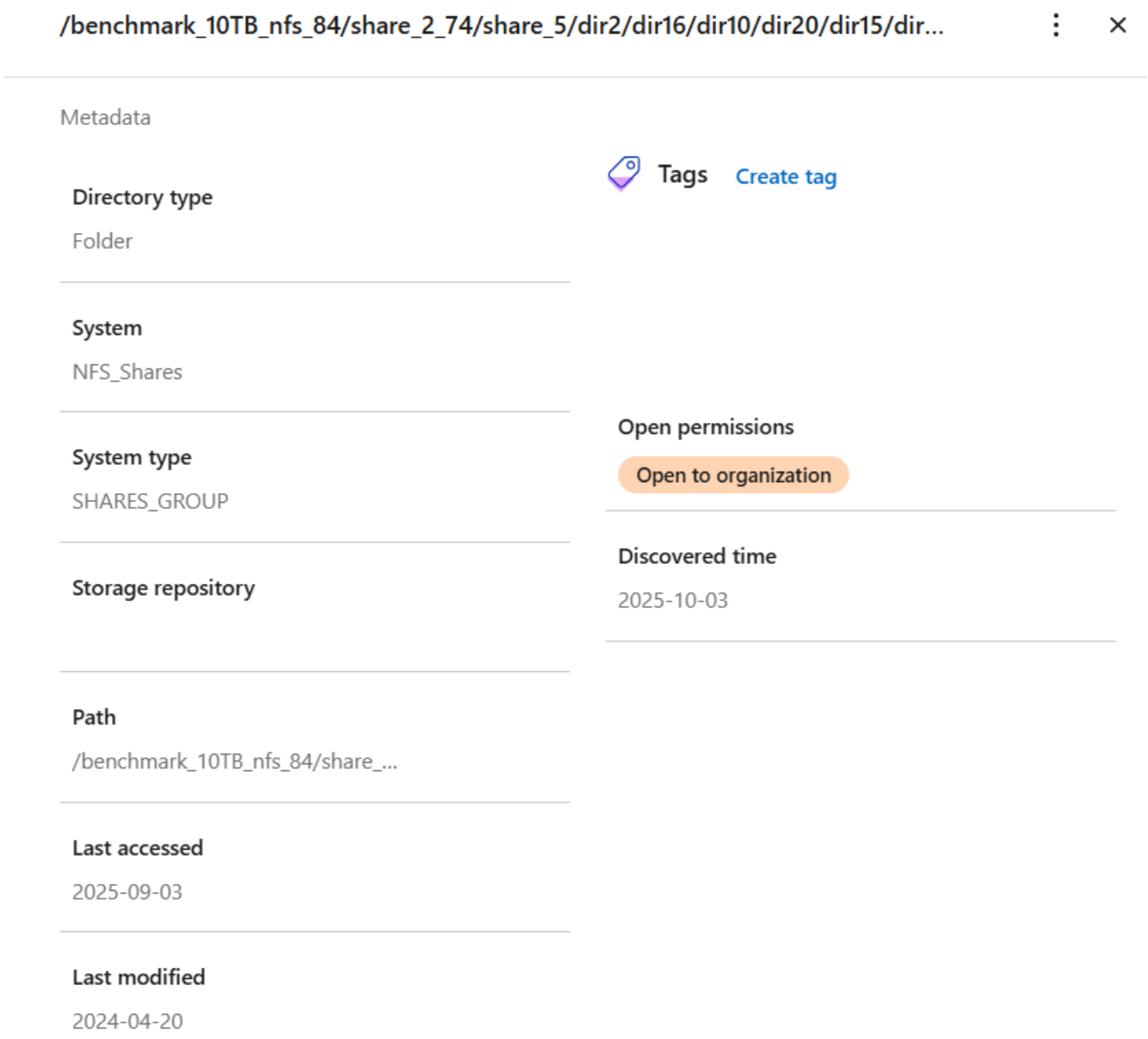
3. Pour examiner les détails d'un type spécifique de données personnelles, sélectionnez **Afficher tout**, puis sélectionnez l'icône en forme de flèche **Examiner les résultats** pour un type spécifique de données personnelles, par exemple, les adresses e-mail.



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

   Les images suivantes montrent les données personnelles trouvées dans un répertoire (partages et dossiers). Dans l'onglet **Structuré**, vous visualisez les données personnelles trouvées dans les bases de données. Dans l'onglet **Non structuré**, vous pouvez afficher les données au niveau du fichier.


Data Investigation
Unstructured (36.6K Files)
Directories (6.1K Folders)
Structured (4 Tables)
Search by File, Table or Location
FILTERS:
Clear All
Policies
Classification Status
Scan Analysis Event
Open Permissions
Number of Users with Access
User / Group Permissions
Create Policy from this search
Set Email Alert
36.6K items
Tags
Assign to
Move
Copy
Delete
ReScan
File Name
Personal
Sensitive Personal
Data Subjects
File Type
B81ALrkD.txt
S3
1.2K
0
10
TXT
Tags: archivado credit card Delete And 7 more View All
Working Environment (Account): S3 - 055518636490
Storage Repository (Bucket): compliancedemofiles-demo
File Path:
Category: Miscellaneous Documents
File Size: 50.67 KB
Discovered Time: 2023-08-20 10:37
Created Time: 2019-12-16 12:18
Last Modified: 2019-12-16 12:18
Open Permissions: NOT PUBLIC
Duplicates: None
Tags: 10 tags
Assigned to: B G Archana
Copy File
Move File
Delete File
Give feedback on this result
Total size 26.5GB | 1-20 of 36.6K
1



Afficher les fichiers contenant des données personnelles sensibles

La classification des données identifie automatiquement les types particuliers d'informations personnelles sensibles, telles que définies par les réglementations en matière de confidentialité telles que "articles 9 et 10 du RGPD" . Par exemple, des informations concernant la santé, l'origine ethnique ou l'orientation sexuelle d'une personne. "Voir la liste complète" . La classification des données identifie ce type d'informations dans des fichiers individuels, dans des fichiers au sein de répertoires (partages et dossiers) et dans des tables de base de données.

La classification des données utilise l'IA, le traitement du langage naturel (NLP), l'apprentissage automatique (ML) et l'informatique cognitive (CC) pour comprendre le sens du contenu qu'elle analyse afin d'extraire des entités et de les catégoriser en conséquence.

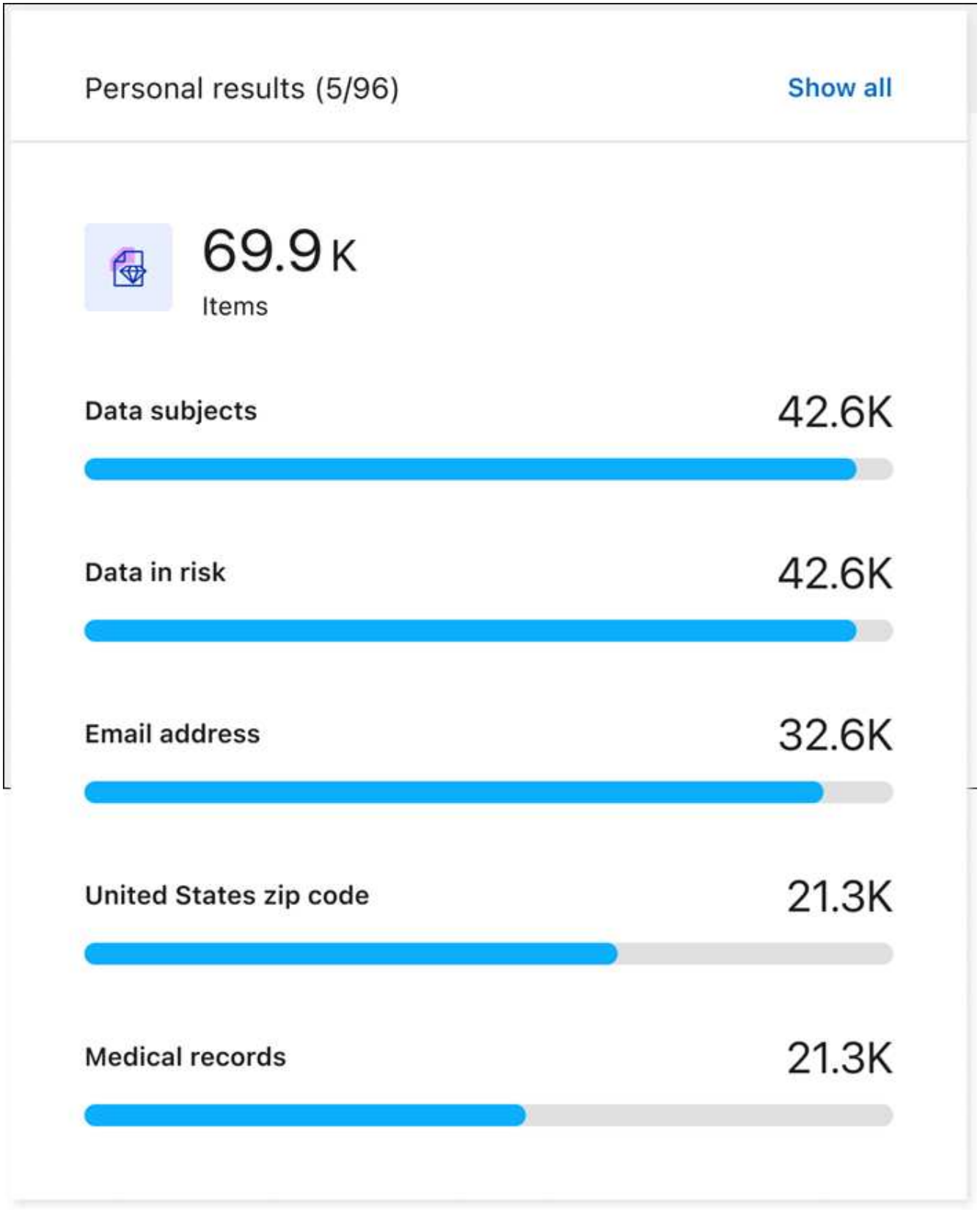
Par exemple, l'origine ethnique est une catégorie de données sensibles du RGPD. Grâce à ses capacités de PNL, la classification des données peut faire la différence entre une phrase qui dit « George est mexicain » (indiquant des données sensibles comme spécifié dans l'article 9 du RGPD), et « George mange de la

nourriture mexicaine ».

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

Étapes

1. Dans le menu Classification des données, sélectionnez **Conformité**.
2. Pour examiner les détails de toutes les données personnelles sensibles, recherchez la carte **Résultats personnels sensibles**, puis sélectionnez **Afficher tout**.



.

3. Pour examiner les détails d'un type spécifique de données personnelles sensibles, sélectionnez **Afficher tout**, puis sélectionnez l'icône en forme de flèche **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 **Enquêter sur les résultats** pour voir les informations masquées ou en téléchargeant la liste des fichiers.

Catégories de données privées dans la NetApp Data Classification

Il existe de nombreux types de données privées que NetApp Data Classification peut identifier dans vos volumes et bases de données.

La classification des données identifie deux types de données personnelles :

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

Si vous avez besoin d'une classification des données pour identifier d'autres types de données privées, tels que des numéros d'identification nationaux supplémentaires ou des identifiants de soins de santé, contactez votre gestionnaire de compte.

Types de données personnelles

Les données personnelles, ou *informations personnellement identifiables* (PII), trouvées dans les fichiers peuvent être des données personnelles générales ou des identifiants nationaux. La troisième colonne du tableau ci-dessous indique si la classification des données utilise"validation de proximité" pour valider ses conclusions pour l'identifiant.

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

Type	Identifiant	Validation de proximité ?	English	Allemand	Espagnol	Français	japonais
Général	Numéro de Carte de Crédit	Oui	✓	✓	✓		✓
	Personnes concernées	Non	✓	✓	✓		
	Adresse email	Non	✓	✓	✓		✓
	Numéro IBAN (numéro de compte bancaire international)	Non	✓	✓	✓		✓
	Adresse IP	Non	✓	✓	✓		✓
	Mot de passe	Oui	✓	✓	✓		✓

Type	Identifiant	Validation de proximité ?	English	Allemand	Espagnol	Français	japonais
Identifiants nationaux							

Type	Identifiant	Validation de proximité ?	English	Allemand	Espagnol	Français	japonais

Type	Identifiant	Validation de proximité ?	English	Allemand	Espagnol	Français	japonais

Type	Identifiant	Validation de proximité	English	Allemand	Espagnol	Français	japonais
	japonais (personnel et d'entreprise)						
	carte d'identité lettone	Oui	✓	✓	✓		
	carte d'identité lituanienne	Oui	✓	✓	✓		
	Carte d'identité luxembourgeoise	Oui	✓	✓	✓		
	Carte d'identité maltaise	Oui	✓	✓	✓		
	Numéro du Service national de santé (NHS)	Oui	✓	✓	✓		
	Compte bancaire néo-zélandais	Oui	✓	✓	✓		
	Permis de conduire néo-zélandais	Oui	✓	✓	✓		
	Numéro IRD de Nouvelle-Zélande (IDF)	Oui	✓	✓	✓		
	Numéro NHI (Indice national de santé) de Nouvelle-Zélande	Oui	✓	✓	✓		
	Numéro de passeport néo-zélandais	Oui	✓	✓	✓		
	Carte d'identité polonaise (PESEL)	Oui	✓	✓	✓		
	Numéro d'identification fiscale portugais (NIF)	Oui	✓	✓	✓		
	Carte d'identité roumaine (CNP)	Oui	✓	✓	✓		
	Carte d'identité nationale de Singapour (NRIC)	Oui	✓	✓	✓		
	Carte d'identité slovène (EMSO)	Oui	✓	✓	✓		
	Carte d'identité sud-africaine	Oui	✓	✓	✓		
	Numéro d'identification fiscale espagnol	Oui	✓	✓	✓		
	carte d'identité suédoise	Oui	✓	✓	✓		
	Carte d'identité britannique (NINO)	Oui	✓	✓	✓		
	Permis de conduire des États-Unis en Californie	Oui	✓	✓	✓		
	Permis de conduire de l'Indiana aux États-Unis	Oui	✓	✓	✓		
	Permis de conduire de l'État de New York aux États-Unis	Oui	✓	✓	✓		
	Permis de conduire des États-Unis au Texas	Oui	✓	✓	✓		
	Numéro de sécurité sociale aux États-Unis (SSN)	Oui	✓	✓	✓		

Types de données personnelles sensibles

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

Les SPII suivants ne peuvent actuellement être reconnus qu'en anglais :

- **Référence aux procédures pénales** : Données concernant les condamnations pénales et les infractions

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 le secteur médical et de la santé.
- **Codes médicaux ICD-10-CM** : Codes utilisés dans le secteur médical et de la santé.
- **Référence aux croyances philosophiques** : Données concernant les croyances philosophiques d’une personne physique.
- **Référence aux opinions politiques** : Données concernant les opinions politiques d’une personne physique.
- **Référence aux croyances religieuses** : Données concernant les croyances religieuses d’une personne physique.
- **Référence relative à la vie sexuelle ou à l’orientation sexuelle** : Données concernant la vie sexuelle ou l’orientation sexuelle d’une personne physique.

Types de catégories

La classification des données catégorise vos données comme suit.

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

Catégorie	Type	English	Allemand	Espagnol
Finance	Bilans	✓	✓	✓
	Bons de commande	✓	✓	✓
	Factures	✓	✓	✓
	Rapports trimestriels	✓	✓	✓
HEURE	Vérifications des antécédents	✓		✓
	Plans de rémunération	✓	✓	✓
	Contrats de travail	✓		✓
	Avis des employés	✓		✓
	Santé	✓		✓
	CV	✓	✓	✓
Légal	Accords de confidentialité	✓	✓	✓
	Contrats fournisseur-client	✓	✓	✓
Commercialisation	Campagnes	✓	✓	✓
	Conférences	✓	✓	✓
Opérations	Rapports d’audit	✓	✓	✓
Ventes	Commandes de vente	✓	✓	

Catégorie	Type	English	Allemand	Espagnol
Services	RFI	✓		✓
	Demande de propositions	✓		✓
	TRUIE	✓	✓	✓
	Formation	✓	✓	✓
Support	Plaintes et contraventions	✓	✓	✓

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

- Données d'application
- Fichiers d'archives
- Audio
- Fil d'Ariane des données d'application métier de classification des données
- Fichiers CAO
- Code
- Corrompu
- Base de données et fichiers d'index
- Fichiers de conception
- Données de candidature par courrier électronique
- Crypté (fichiers avec un score d'entropie élevé)
- Exécutables
- Données d'application financière
- Données d'application de santé
- Images
- Journaux
- Documents divers
- Présentations diverses
- Feuilles de calcul diverses
- Divers « Inconnu »
- Fichiers protégés par mot de passe
- Données structurées
- Vidéos
- Fichiers de zéro octet

Types de fichiers

La classification des données analyse tous les fichiers pour obtenir des informations sur les catégories et les métadonnées et affiche tous les types de fichiers dans la section types de fichiers du tableau de bord. Lorsque la classification des données détecte des informations personnelles identifiables (PII) ou lorsqu'elle effectue

une recherche DSAR, seuls les formats de fichiers suivants sont pris en charge :

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

Exactitude des informations trouvées

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

Sur la base de nos tests, le tableau ci-dessous montre l'exactitude des informations trouvées par Data Classification. Nous le décomposons par *précision* et *rappel* :

Précision
: La probabilité que ce que la classification des données trouve 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 informations personnelles contiennent réellement des informations personnelles. 1 fichier sur 10 serait un faux positif.

Rappel
: La probabilité que la classification des données trouve ce qu'elle devrait. Par exemple, un taux de rappel de 70 % pour les données personnelles signifie que la classification des données peut identifier 7 fichiers sur 10 qui contiennent réellement des informations personnelles dans votre organisation. La classification des données manquerait de 30 % des données et elles n'apparaîtraient pas dans le tableau de bord.

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

Type	Précision	Rappel
Données personnelles - Généralités	90%-95%	60%-80%
Données personnelles - Identifiants de pays	30%-60%	40%-60%
Données personnelles sensibles	80%-95%	20%-30%
Catégories	90%-97%	60%-80%

Créer une classification personnalisée dans NetApp Data Classification

La NetApp Data Classification vous permet de créer des catégories personnalisées ou des identifiants personnels pour identifier les données spécifiques aux exigences réglementaires et de conformité de votre organisation.

La classification des données prend en charge deux types de classificateurs personnalisés : les catégories et les identifiants personnels. Les catégories personnalisées sont créées à partir d'un ensemble de fichiers que vous téléchargez, à partir desquels la classification des données crée un modèle d'IA pour identifier les données similaires au sein de votre organisation (par exemple, une entreprise de recherche en santé pourrait créer une catégorie d'analyse clinique). Les identifiants personnels personnalisés sont créés à l'aide de listes de mots clés ou d'une expression régulière (regex) pour identifier les informations spécifiques à votre

organisation qui peuvent présenter un risque de non-conformité.

Toutes les classifications personnalisées sont disponibles dans le tableau de bord des classifications personnalisées.

Créer un identifiant personnel personnalisé

La classification des données vous permet de créer un identifiant personnel personnalisé à l'aide de mots clés contextuels ou d'une expression régulière afin d'identifier les données propres à votre organisation.

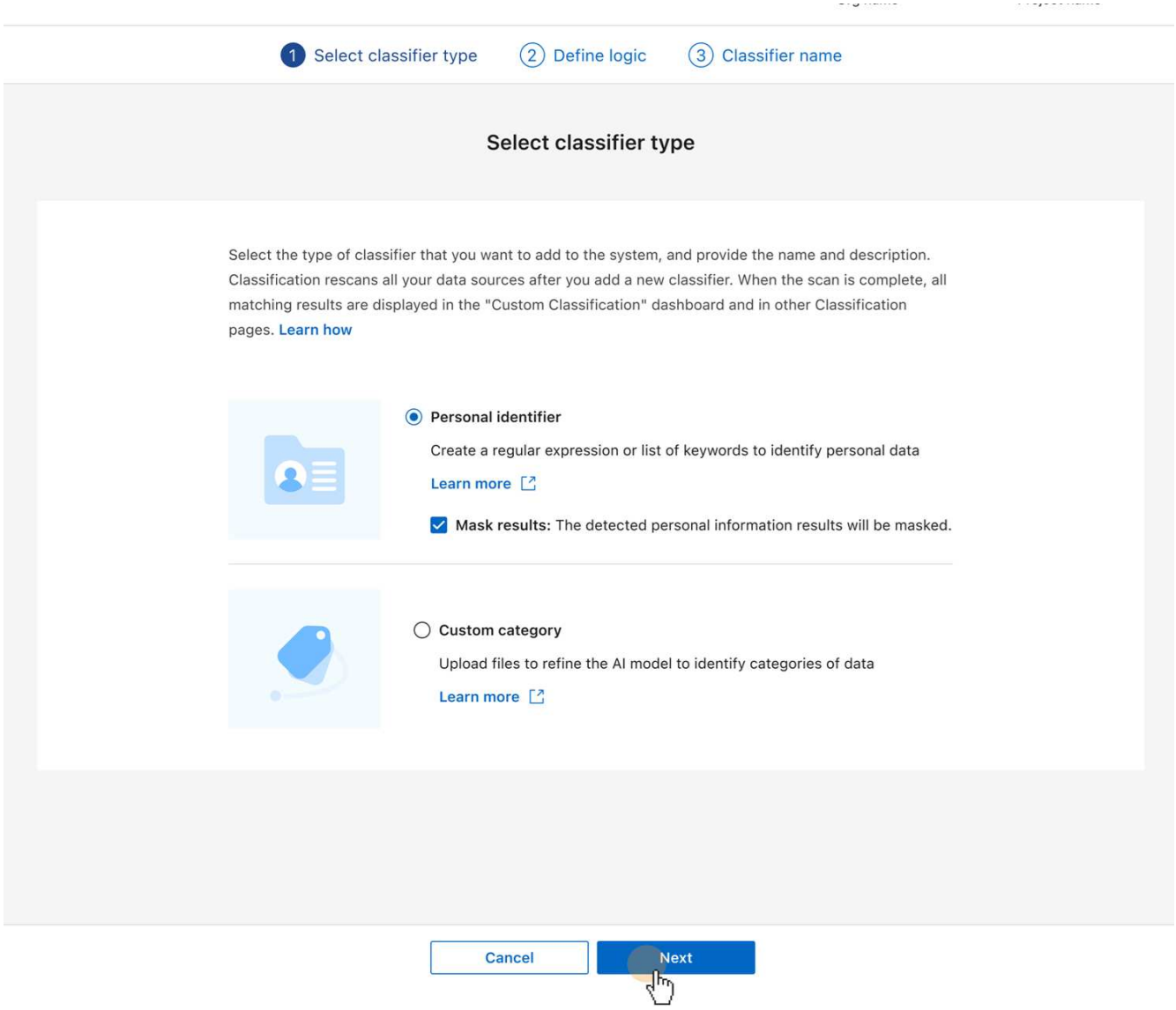
Exigences relatives aux mots-clés

Si vous créez votre identifiant personnel à l'aide d'une liste de mots clés, cette liste doit répondre aux exigences suivantes :

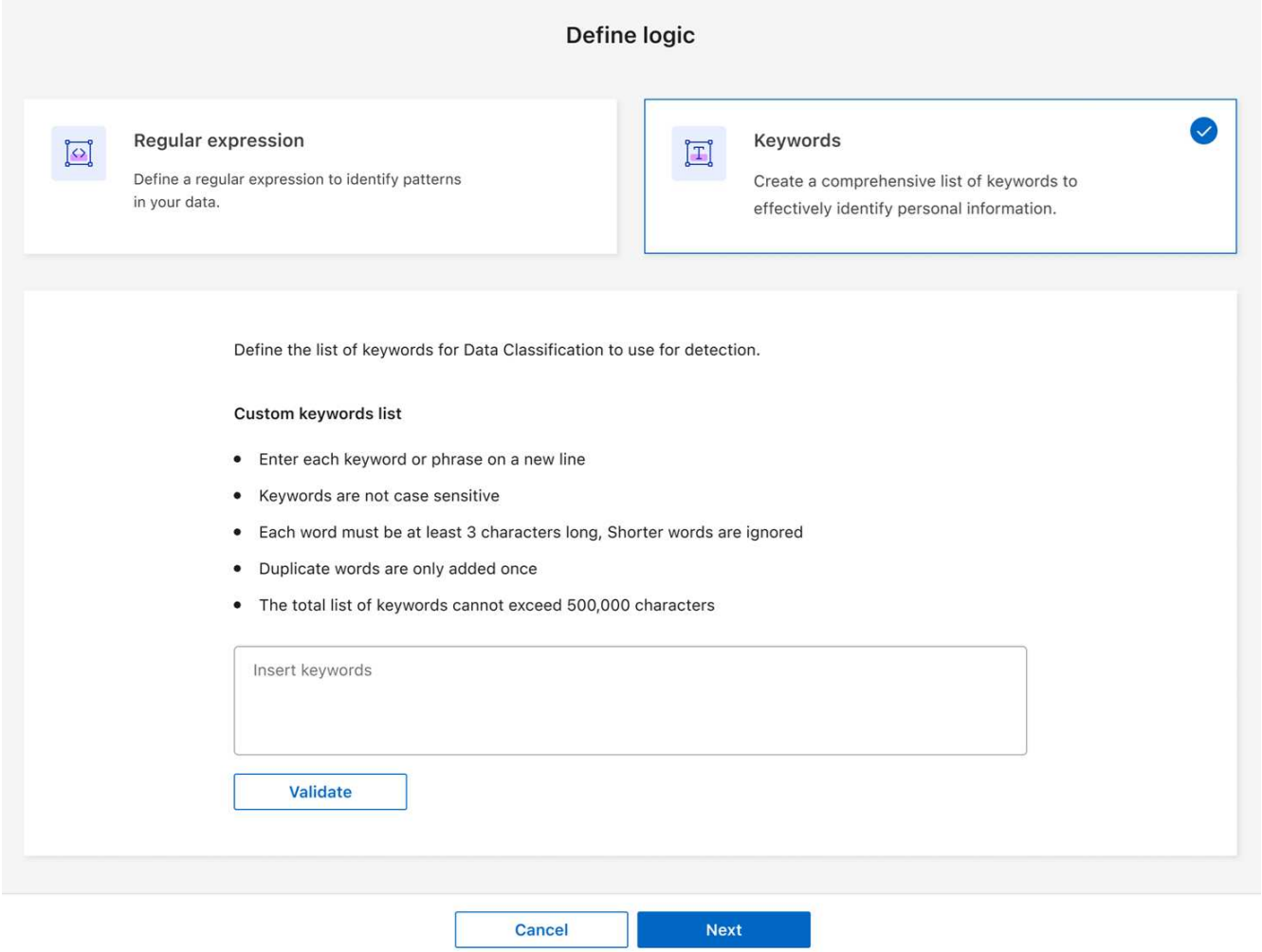
- La saisie des mots-clés n'est pas sensible à la casse.
- Les mots-clés doivent comporter au moins trois caractères. Les mots de moins de trois caractères sont ignorés.
- Les mots en double ne sont ajoutés qu'une seule fois.
- La liste totale des mots-clés ne peut pas dépasser 500 000 caractères. La liste doit inclure au moins un mot-clé.

Étapes

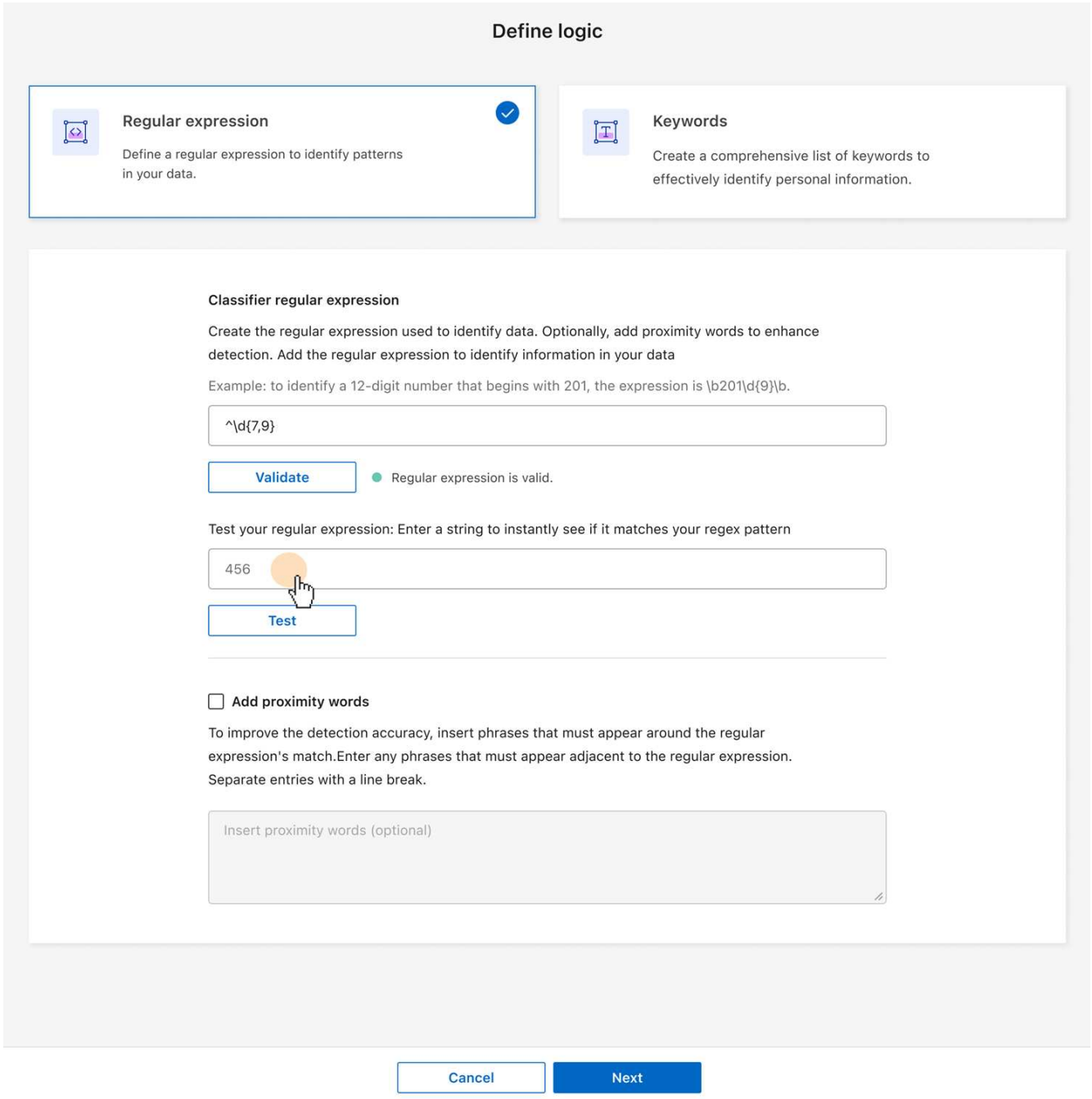
1. Sélectionnez l'onglet **Classification personnalisée**.
2. Sélectionnez **+ Nouveau classificateur** pour créer le classificateur personnalisé.
3. Sélectionnez **Identifiant personnel**. Vous pouvez également sélectionner **Masquer les résultats** pour masquer les données personnelles détectées.
4. Sélectionnez **Suivant**.



5. Pour ajouter le classificateur avec des mots clés, sélectionnez **Mots clés**. Saisissez une liste de mots-clés, chaque entrée sur une ligne distincte. Assurez-vous que les mots-clés respectent les exigences.



Pour ajouter le classificateur en tant qu'expression régulière, sélectionnez **Expression régulière** puis ajoutez un modèle pour détecter les informations spécifiques de vos données. Sélectionnez **Valider** pour confirmer la syntaxe de votre saisie.



a. Vous pouvez également saisir une chaîne de caractères d'exemple qui doit correspondre à votre modèle d'expression régulière, puis sélectionner **Tester** pour la vérifier.

b. Ajoutez éventuellement des mots de proximité. Si vous ajoutez des mots de proximité, la classification des données ne signale le modèle d'expression régulière que si les mots de proximité sont adjacents à la chaîne correspondante.

6. Sélectionnez **Suivant**.
7. Saisissez un **nom de classificateur** et une **description** pour identifier la catégorie personnalisée dans votre tableau de bord.
8. Sélectionnez **Enregistrer** pour créer l'identifiant personnel personnalisé.

Une fois que vous avez créé un identifiant personnel personnalisé, ses résultats sont capturés lors de la prochaine analyse planifiée. Pour obtenir des résultats plus rapidement, effectuez une analyse à la demande.

Pour consulter les résultats, voir Générer des rapports de conformité.

Créer une catégorie personnalisée

Grâce aux catégories personnalisées, vous pouvez catégoriser les données spécifiques à votre organisation. Des catégories personnalisées sont créées à partir de fichiers texte que vous téléchargez, à partir desquels la classification des données crée un modèle d'IA pour identifier des informations similaires dans d'autres fichiers.

exigences en matière de données de formation

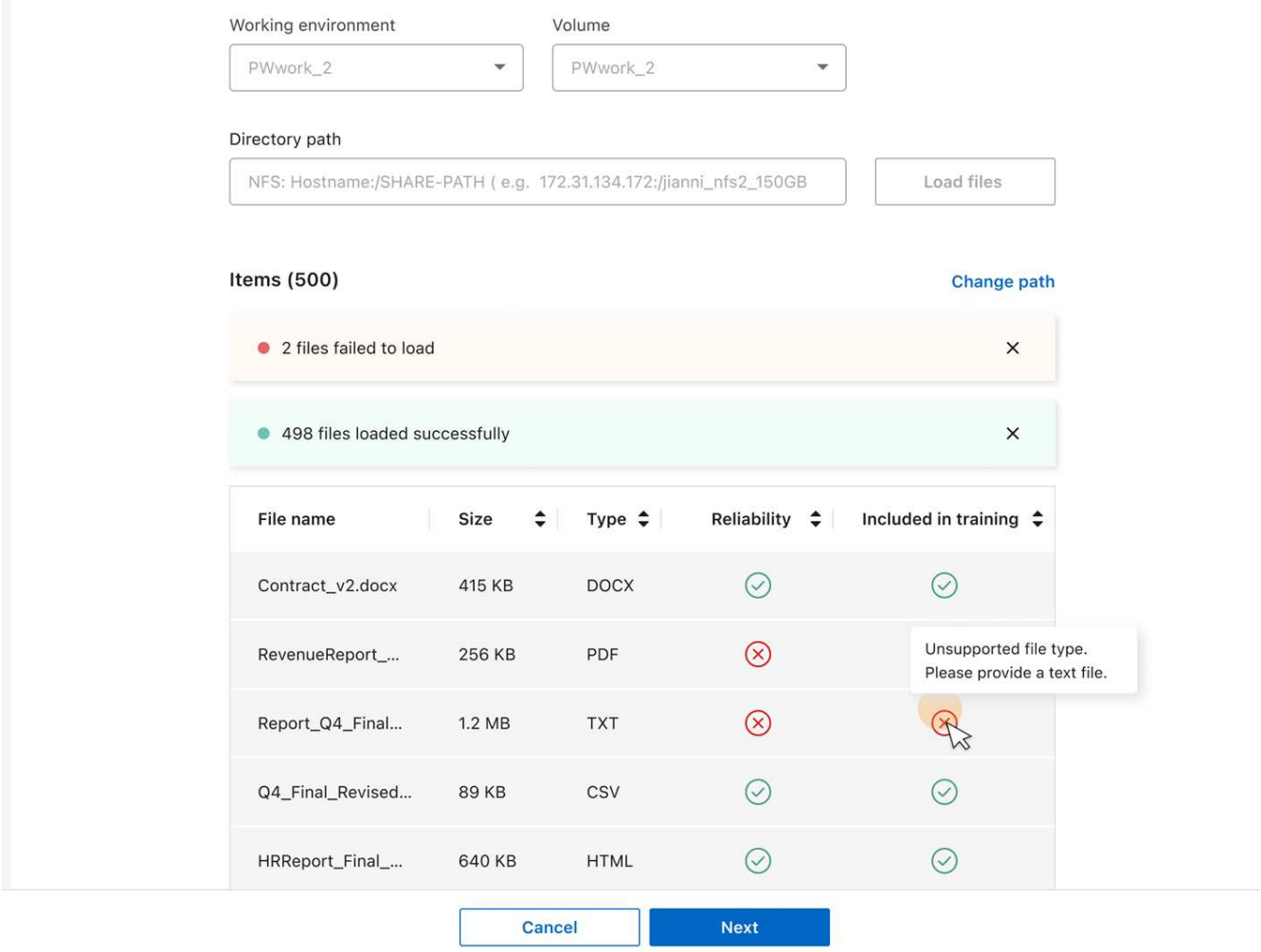
- L'ensemble de données d'entraînement doit contenir au minimum 25 fichiers. Le nombre maximal de fichiers est de 1 000.
- Tous les fichiers doivent se trouver directement dans le chemin d'accès que vous indiquez.
- Tous les fichiers doivent avoir une taille supérieure à 100 octets.
- Les données d'entraînement pour la classification des données doivent être de l'un des types de fichiers suivants : CSV, DOCX, DOC, GZ, JSON, PDF, PPTX, TXT, RTT, XLS ou XLSX. Vous pouvez télécharger une combinaison de tous les types de fichiers pris en charge.

Étapes

1. Dans la NetApp Data Classification, sélectionnez **Classification personnalisée**.
2. Sélectionnez **+ Nouveau classificateur**.
3. Choisissez **Catégorie personnalisée** comme type de classificateur, puis **Suivant**.
4. Définissez la logique de votre catégorie personnalisée à l'aide d'une collection de fichiers texte. Indiquez l'adresse IP de l'**adresse de travail**, puis sélectionnez le **volume** dans le menu déroulant.

   Saisissez le **chemin d'accès au répertoire** contenant les données d'entraînement.

5. Sélectionnez **Charger les fichiers** pour la classification des données afin d'effectuer une vérification des fichiers. Vous pouvez consulter le résumé des fichiers, qui indique le nom du fichier, sa taille, son type et des notes précisant si le fichier a été jugé acceptable pour la formation.



a. Pour modifier le chemin d'accès aux fichiers ou les recharger, sélectionnez **Modifier le chemin d'accès**, puis saisissez les données et rechargez les fichiers.

6. Lorsque vous êtes satisfait des fichiers téléchargés, sélectionnez **Suivant**.
7. Saisissez un **nom de classificateur** et une **description** pour identifier la catégorie personnalisée dans votre tableau de bord.
8. Sélectionnez **Enregistrer** pour créer la catégorie personnalisée.

Résultat

Une fois que vous avez créé une catégorie personnalisée, ses résultats sont pris en compte lors de la prochaine analyse planifiée. Pour obtenir des résultats plus rapidement, lancez l'analyse manuellement.

Modifier un classificateur personnalisé

Vous pouvez modifier la logique d'un identifiant personnel après sa création. Vous ne pouvez pas modifier le type d'identifiant personnel ni le type logique ; par exemple, vous ne pouvez pas transformer une catégorie personnalisée en identifiant personnel personnalisé. Vous ne pouvez pas non plus remplacer un identifiant personnalisé basé sur un mot-clé par un identifiant personnalisé basé sur une expression régulière.

Étapes

1. Dans la NetApp Data Classification, sélectionnez **Classification personnalisée**.
2. Identifiez le classificateur que vous souhaitez supprimer, puis sélectionnez le menu d'actions. … au bout de

sa rangée.

3. Sélectionnez **Modifier la logique**.
4. Si vous modifiez des mots clés, ajoutez, supprimez ou modifiez les mots clés appropriés. Si vous modifiez une expression régulière, saisissez la nouvelle expression régulière et validez-la. Ajoutez éventuellement des mots-clés de proximité.
5. Sélectionnez **Enregistrer** pour appliquer les modifications.

Supprimer un classificateur personnalisé

1. Dans la NetApp Data Classification, sélectionnez **Classification personnalisée**.
2. Identifiez le classificateur que vous souhaitez supprimer, puis sélectionnez le menu d'actions. … au bout de sa rangée.
3. Sélectionnez **Supprimer le classificateur**.

Prochaines étapes

- Générer des rapports de conformité

Examinez les données stockées dans votre organisation avec la NetApp Data Classification

Le tableau de bord d'investigation des données affiche des informations au niveau des fichiers et des répertoires sur vos données, vous permettant de trier et de filtrer les résultats. La page Enquête sur les données présente des informations sur les métadonnées et les autorisations des fichiers et des répertoires, ainsi que sur l'identification des fichiers en double. Grâce aux informations au niveau des fichiers, des répertoires et des bases de données, vous pouvez prendre des mesures pour améliorer la conformité de votre organisation et économiser de l'espace de stockage. La page Enquête sur les données prend également en charge le déplacement, la copie et la suppression de fichiers.

Pour obtenir des informations à partir de la page Enquête, vous devez effectuer une analyse de classification complète sur vos sources de données. Les sources de données ayant fait l'objet d'une analyse de mappage uniquement n'affichent pas les détails au niveau du fichier.

Structure d'enquête sur les données

La page Enquête sur les données trie les données en trois onglets :

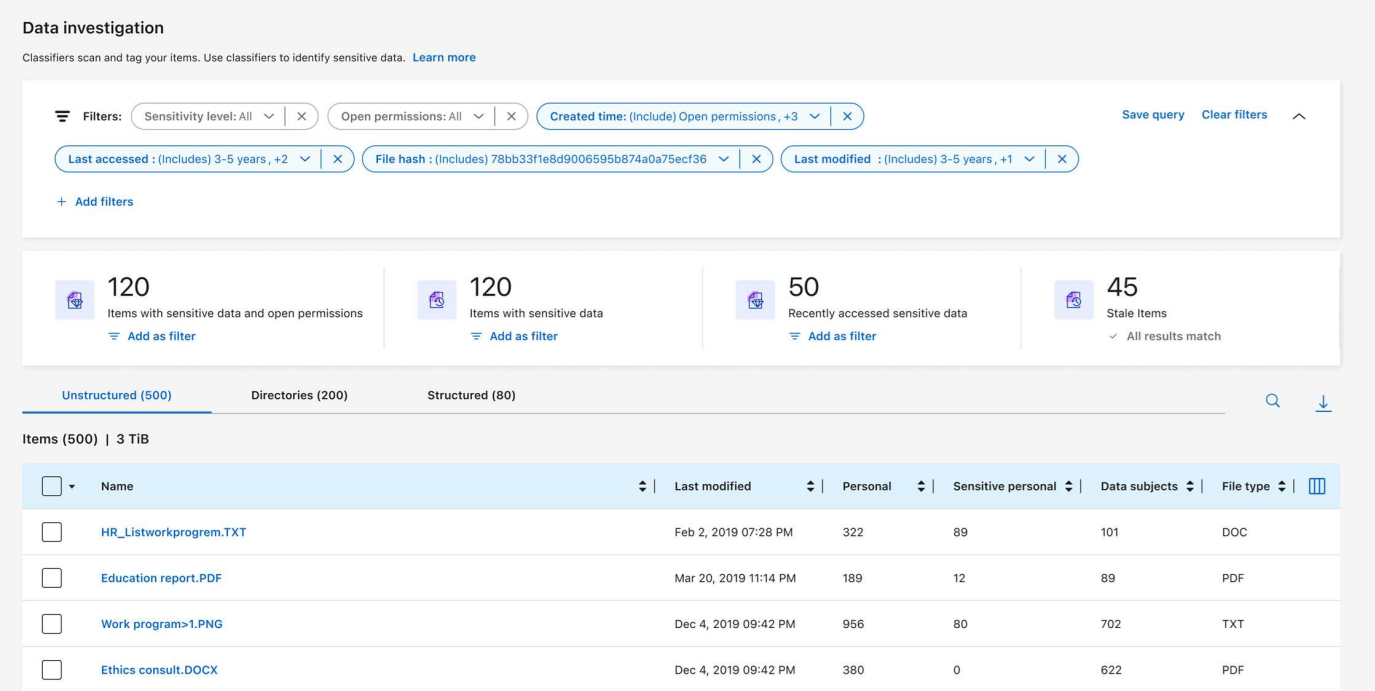
- **Données non structurées** : données de fichier
- **Répertoires** : dossiers et partages de fichiers
- **Structuré** : base de données

Filtres de données

La page Enquête sur les données fournit de nombreux filtres pour trier vos données afin que vous puissiez

obtenir ce dont vous avez besoin. Vous pouvez utiliser plusieurs filtres de concert.

Pour ajouter un filtre, sélectionnez le bouton **Ajouter un filtre**.



Sensibilité et contenu du filtre

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

Filtre	Détails
Catégorie	Sélectionnez le"types de catégories" .
Niveau de sensibilité	Sélectionnez le niveau de sensibilité : Personnel, Personnel sensible ou Non sensible.
Nombre d'identifiants	Sélectionnez la plage d'identifiants sensibles détectés par fichier. Comprend les données personnelles et les données personnelles sensibles. Lors du filtrage dans les répertoires, la classification des données totalise les correspondances de tous les fichiers de chaque dossier (et sous-dossiers). REMARQUE : la version de décembre 2023 (version 1.26.6) a supprimé l'option permettant de calculer le nombre de données d'informations personnelles identifiables (PII) par répertoires.
Données personnelles	Sélectionnez le"types de données personnelles" .
Données personnelles sensibles	Sélectionnez le"types de données personnelles sensibles" .
Personne concernée	Saisissez le nom complet ou l'identifiant connu de la personne concernée. "En savoir plus sur les personnes concernées ici" .

Filtrer le propriétaire de l'utilisateur et les autorisations de l'utilisateur

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

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

Filtrer chronologiquement

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

Filtre	Détails
Temps créé	Sélectionnez une plage horaire pendant laquelle le fichier a été créé. Vous pouvez également spécifier une plage horaire personnalisée pour affiner davantage les résultats de la recherche.
Temps découvert	Sélectionnez une plage horaire pendant laquelle la classification des données a découvert le fichier. Vous pouvez également spécifier une plage horaire personnalisée pour affiner davantage les résultats de la recherche.
Dernière modification	Sélectionnez une plage horaire pendant laquelle le fichier a été modifié pour la dernière fois. Vous pouvez également spécifier une plage horaire personnalisée pour affiner davantage les résultats de la recherche.
Dernier accès	Sélectionnez une plage horaire pendant laquelle le fichier ou le répertoire* a été consulté pour la dernière fois. Vous pouvez également spécifier une plage horaire personnalisée pour affiner davantage les résultats de la recherche. Pour les types de fichiers analysés par Data Classification, il s’agit de la dernière fois que Data Classification a analysé le fichier.

* L’heure du dernier accès à un répertoire n’est disponible que pour les partages NFS ou CIFS.

Filtrer les métadonnées

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

Filtre	Détails
Chemin du fichier	Saisissez jusqu’à 20 chemins partiels ou complets que vous souhaitez inclure ou exclure de la requête. Si vous entrez à la fois des chemins d’inclusion et des chemins d’exclusion, Data Classification recherche d’abord tous les fichiers dans les chemins inclus, puis supprime les fichiers des chemins exclus, puis affiche les résultats. Notez que l’utilisation de « * » dans ce filtre n’a aucun effet et que vous ne pouvez pas exclure des dossiers spécifiques de l’analyse : tous les répertoires et fichiers sous un partage configuré seront analysés.

Filtre	Détails
Type de répertoire	Sélectionnez le type de répertoire ; « Partager » ou « Dossier ».
Type de fichier	Sélectionnez le"types de fichiers" .
Taille du fichier	Sélectionnez la plage de taille du fichier.
Hachage de fichier	Saisissez le hachage du fichier pour rechercher un fichier spécifique, même si le nom est différent.

Type de stockage du filtre

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

Filtre	Détails
Type de système	Sélectionnez le type de système.
Nom de l'environnement système	Sélectionnez des systèmes spécifiques.
Référentiel de stockage	Sélectionnez le référentiel de stockage, par exemple un volume ou un schéma.

Requête de filtrage

Utilisez le filtre suivant pour afficher les données par requêtes enregistrées.

Filtre	Détails
Requête enregistrée	Sélectionnez une requête enregistrée ou plusieurs. Aller à la"onglet requêtes enregistrées" pour afficher la liste des requêtes enregistrées existantes et en créer de nouvelles.
Mots-clés	Sélectionner"le tag ou les tags" qui sont attribués à vos fichiers.

Statut de l'analyse du filtre

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

Filtre	Détails
État de l'analyse	Sélectionnez une option pour afficher la liste des fichiers en attente de première analyse, en cours d'analyse, en attente de nouvelle analyse ou dont l'analyse a échoué.
Événement d'analyse d'analyse	Sélectionnez si vous souhaitez afficher les fichiers qui n'ont pas été classés parce que la classification des données n'a pas pu revenir à l'heure du dernier accès, ou les fichiers qui ont été classés même si la classification des données n'a pas pu revenir à l'heure du dernier accès.

"Voir les détails sur l'horodatage « dernier accès »"pour plus d'informations sur les éléments qui apparaissent dans la page Investigation lors du filtrage à l'aide de l'événement d'analyse d'analyse.

Filtrer les données par doublons

Utilisez le filtre suivant pour afficher les fichiers dupliqués dans votre stockage.

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

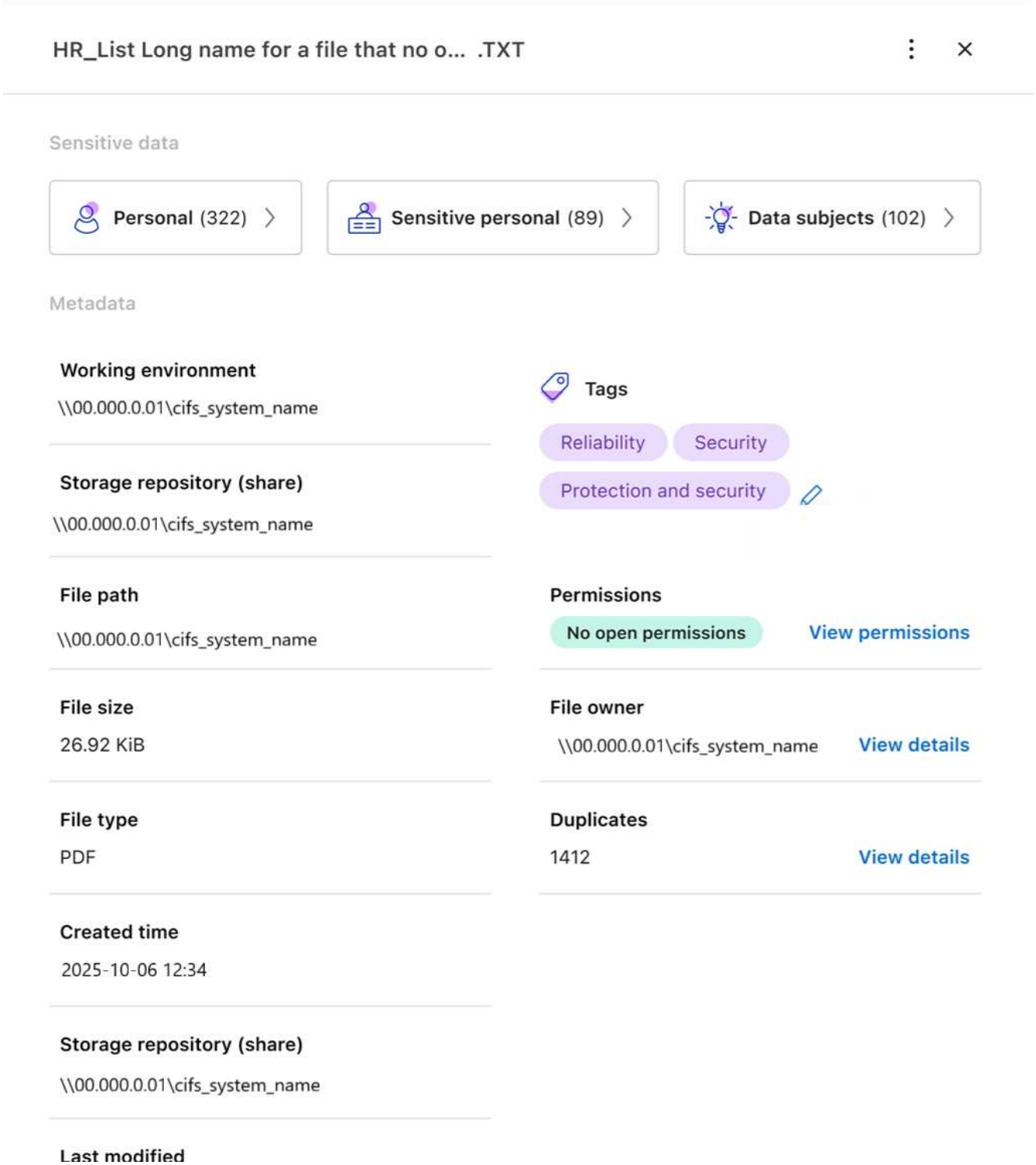
Afficher les métadonnées du fichier

En plus de vous montrer le système et le volume où réside le fichier, les métadonnées affichent beaucoup plus d'informations, notamment les autorisations du fichier, le propriétaire du fichier et s'il existe des doublons de ce fichier. Ces informations sont utiles si vous envisagez de"créer des requêtes enregistrées" car vous pouvez voir toutes les informations que vous pouvez utiliser pour filtrer vos données.

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

Étapes

1. Dans le menu Classification des données, sélectionnez **Enquête**.
2. Dans la liste Enquête sur les données à droite, sélectionnez le curseur vers le bas à droite pour n'importe quel fichier unique pour afficher les métadonnées du fichier.



3. En option, vous pouvez créer ou ajouter une balise au fichier avec le bouton **Créer une balise**. Sélectionnez une balise existante dans le menu déroulant ou ajoutez une nouvelle balise avec le bouton **+ Ajouter**. Les balises peuvent être utilisées pour filtrer les données.

Afficher les autorisations utilisateur pour les fichiers et les répertoires

Pour afficher une liste de tous les utilisateurs ou groupes ayant accès à un fichier ou à un répertoire et les types d'autorisations dont ils disposent, sélectionnez **Afficher toutes les autorisations**. Cette option est disponible uniquement pour les données dans les partages CIFS.

Si vous utilisez des identifiants de sécurité (SID) au lieu de noms d'utilisateur et de groupe, vous devez intégrer votre Active Directory dans la classification des données. Pour plus d'informations, consultez la section "ajouter Active Directory à la classification des données" .

Étapes

1. Dans le menu Classification des données, sélectionnez **Enquête**.
2. Dans la liste Enquête sur les données à droite, sélectionnez le curseur vers le bas à droite pour n'importe quel fichier unique pour afficher les métadonnées du fichier.
3. Pour afficher une liste de tous les utilisateurs ou groupes ayant accès à un fichier ou à un répertoire et les types d'autorisations dont ils disposent, dans le champ Autorisations d'ouverture, sélectionnez **Afficher toutes les autorisations**.

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

4. Sélectionnez le curseur vers le bas bouton pour n'importe quel groupe pour voir la liste des utilisateurs qui font partie du groupe.

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

5. Sélectionnez le nom d'un utilisateur ou d'un groupe pour actualiser la page Enquête afin de voir tous les fichiers et répertoires auxquels l'utilisateur ou le groupe a accès.

Vérifiez les fichiers en double dans vos systèmes de stockage

Vous pouvez vérifier si des fichiers en double sont stockés dans vos systèmes de stockage. Ceci est utile si vous souhaitez identifier les zones dans lesquelles vous pouvez économiser de l'espace de stockage. Il est également bon de s'assurer que certains fichiers disposant d'autorisations spécifiques ou d'informations sensibles ne sont pas inutilement dupliqués dans vos systèmes de stockage.

La classification des données compare tous les fichiers (à l'exclusion des bases de données) pour détecter les doublons s'ils sont :

- 1 Mo ou plus
- Ou contenir des informations personnelles ou des informations personnelles sensibles

La classification des données utilise la technologie de hachage pour déterminer les fichiers en double. Si deux fichiers ont le même code de hachage, ils sont considérés comme des copies exactes, même si leurs noms sont différents.

Étapes

1. Dans le menu Classification des données, sélectionnez **Enquête**.
2. Dans le volet Filtre, sélectionnez « Taille du fichier » ainsi que « Doublons » (« Contient des doublons ») pour voir quels fichiers d'une certaine plage de taille sont dupliqués dans votre environnement.
3. Vous pouvez également télécharger la liste des fichiers en double et l'envoyer à votre administrateur de stockage afin qu'il puisse décider quels fichiers, le cas échéant, peuvent être supprimés.
4. En option, vous pouvez supprimer, étiqueter ou déplacer les fichiers en double. Sélectionnez les fichiers sur lesquels vous souhaitez effectuer une action, puis sélectionnez l'action appropriée.

Voir si un fichier spécifique est dupliqué

Vous pouvez voir si un seul fichier contient des doublons.

Étapes

1. Dans le menu Classification des données, sélectionnez **Enquête**.
2. Dans la liste Enquête sur les données, sélectionnez à droite pour n'importe quel fichier unique pour afficher les métadonnées du fichier.

   Si des doublons existent pour un fichier, cette information apparaît à côté du champ *Doublons*.
3. Pour afficher la liste des fichiers en double et leur emplacement, sélectionnez **Afficher les détails**.
4. Sur la page suivante, sélectionnez **Afficher les doublons** pour afficher les fichiers dans la page Enquête.
5. En option, vous pouvez supprimer, étiqueter ou déplacer les fichiers en double. Sélectionnez les fichiers sur lesquels vous souhaitez effectuer une action, puis sélectionnez l'action appropriée.

> Vous pouvez utiliser la valeur « hachage de fichier » fournie dans cette page et la saisir directement dans la page Enquête pour rechercher un fichier en double spécifique à tout moment - ou vous pouvez l'utiliser dans une requête enregistrée.

Téléchargez votre rapport

Vous pouvez télécharger vos résultats filtrés au format CSV ou JSON.

Il peut y avoir jusqu'à trois fichiers de rapport téléchargés si la classification des données analyse des fichiers (données non structurées), des répertoires (dossiers et partages de fichiers) et des bases de données (données structurées).

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

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

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

Ce qui est inclus dans le rapport téléchargeable

Le **Rapport de données sur les fichiers non structurés** inclut les informations suivantes sur vos fichiers :

- Nom des fichiers
- Type d'emplacement
- Nom du système
- Référentiel de stockage (par exemple, un volume, un bucket, des partages)
- Type de référentiel
- Chemin du fichier
- Type de fichier
- Taille du fichier (en Mo)
- Temps de création

- Dernière modification
- Dernier accès
- Propriétaire du fichier
  - Les données du propriétaire du fichier englobent le nom du compte, le nom du compte SAM et l'adresse e-mail lorsque Active Directory est configuré.
- Catégorie
- Informations personnelles
- Informations personnelles sensibles
- Autorisations ouvertes
- Erreur d'analyse de numérisation
- Date de détection de suppression

  La date de détection de suppression identifie la date à laquelle le fichier a été supprimé ou déplacé. Cela vous permet d'identifier quand des fichiers sensibles ont été déplacés. Les fichiers supprimés ne contribuent pas au nombre de fichiers qui apparaît dans le tableau de bord ou sur la page Enquête. Les fichiers n'apparaissent que dans les rapports CSV.

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

- Type de système
- Nom du système
- Nom du répertoire
- Référentiel de stockage (par exemple, un dossier ou des partages de fichiers)
- Propriétaire du répertoire
- Temps de création
- Temps découvert
- Dernière modification
- Dernier accès
- Autorisations ouvertes
- Type de répertoire

Le **rapport de données structurées** inclut les informations suivantes sur vos tables de base de données :

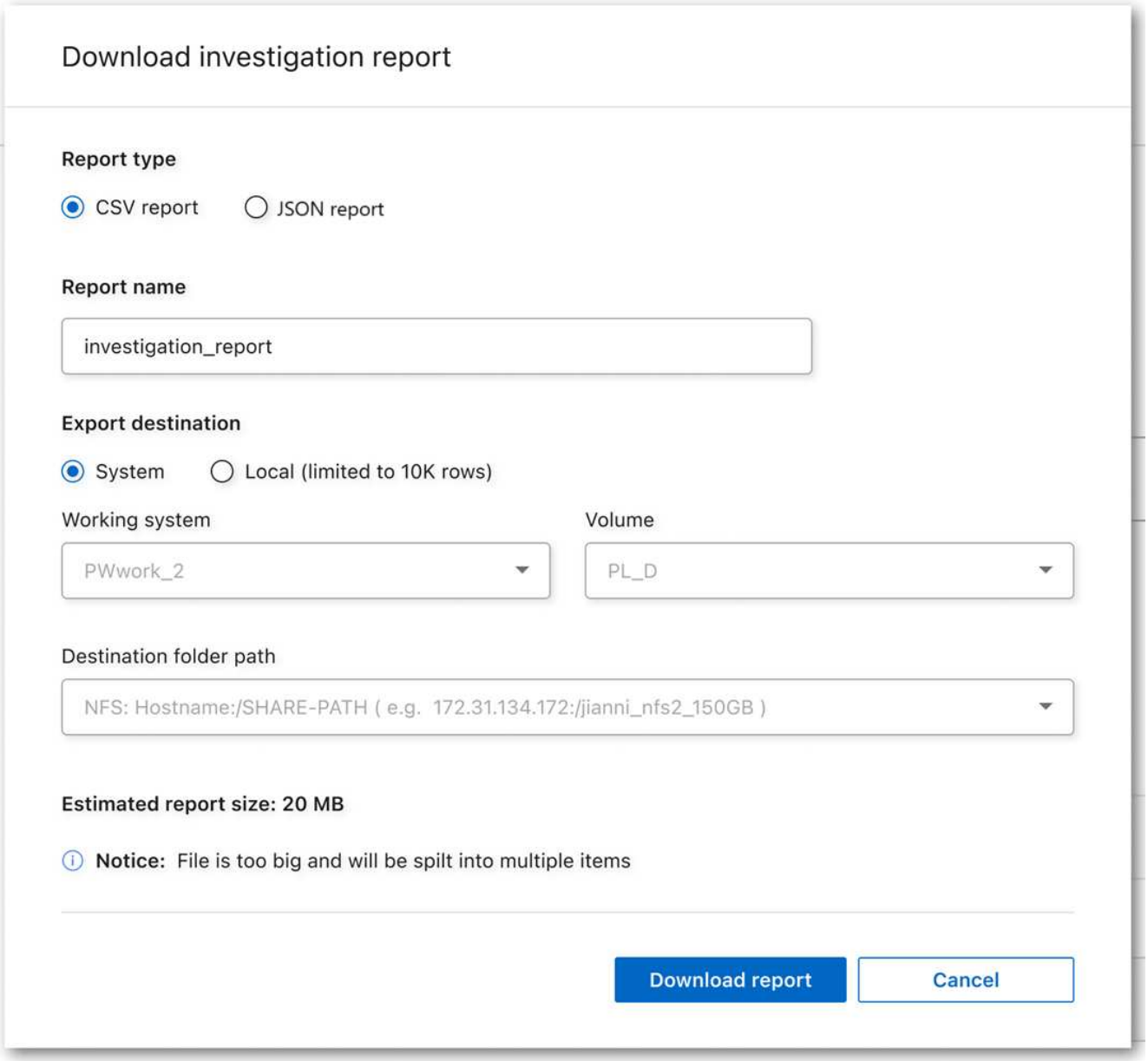
- Nom de la table de base de données
- Type d'emplacement
- Nom du système
- Référentiel de stockage (par exemple, un schéma)
- Nombre de colonnes
- Nombre de lignes
- Informations personnelles
- Informations personnelles sensibles

Étapes pour générer le rapport

1. À partir de la page Enquête sur les données, sélectionnez l'option bouton en haut à droite de la page.
2. Choisissez le type de rapport : CSV ou JSON.
3. Saisissez un **Nom de rapport**.
4. Pour télécharger le rapport complet, sélectionnez **Système** puis choisissez **Système** et **Volume** dans les menus déroulants respectifs. Fournissez un **chemin d'accès au dossier de destination**.

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

5. Sélectionnez **Télécharger le rapport**.



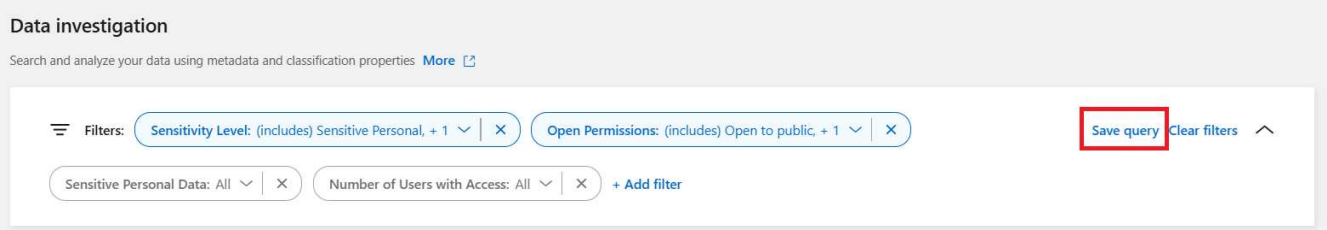
Résultat

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

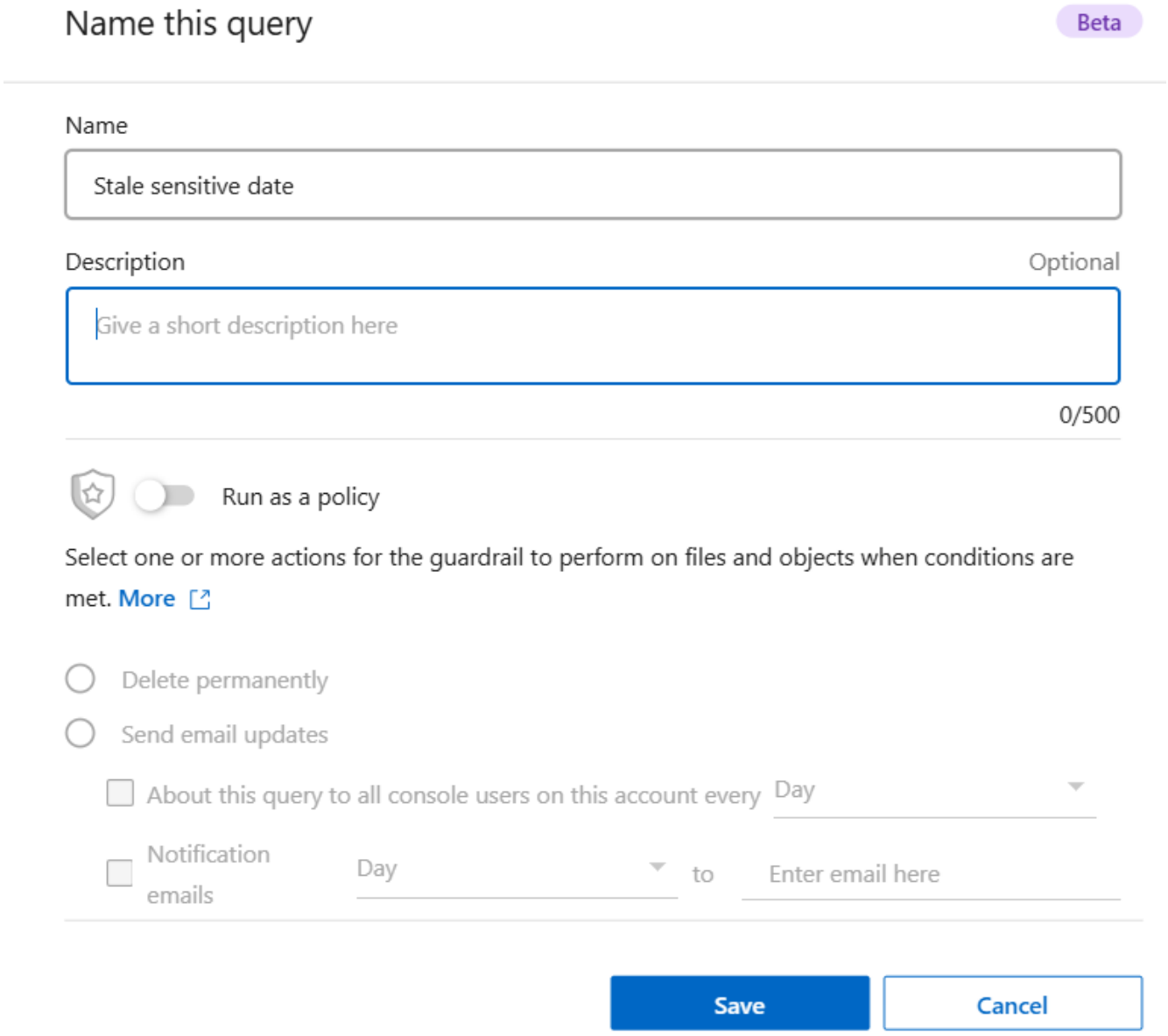
Créer une requête enregistrée en fonction des filtres sélectionnés

Étapes

1. Dans l'onglet Enquête, définissez une recherche en sélectionnant les filtres que vous souhaitez utiliser. Voir"Filtrage des données dans la page Investigation" pour plus de détails.
2. Une fois que vous avez défini toutes les caractéristiques du filtre à votre guise, sélectionnez **Enregistrer la requête**.



3. Nommez la requête enregistrée et ajoutez une description. Le nom doit être unique.
4. Vous pouvez éventuellement enregistrer la requête en tant que politique :
   a. Pour enregistrer la requête en tant que politique, activez le bouton **Exécuter en tant que politique**.
   b. Choisissez de **Supprimer définitivement** ou **Envoyer des mises à jour par e-mail**. Si vous choisissez les mises à jour par e-mail, vous pouvez envoyer les résultats de la requête par e-mail à *tous* les utilisateurs de la console quotidiennement, hebdomadairement ou mensuellement. Alternativement, vous pouvez envoyer la notification à une adresse e-mail spécifique aux mêmes fréquences.
5. Sélectionnez **Enregistrer**.



Une fois la recherche ou la politique créée, vous pouvez la visualiser dans l'onglet **Requêtes enregistrées**.

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

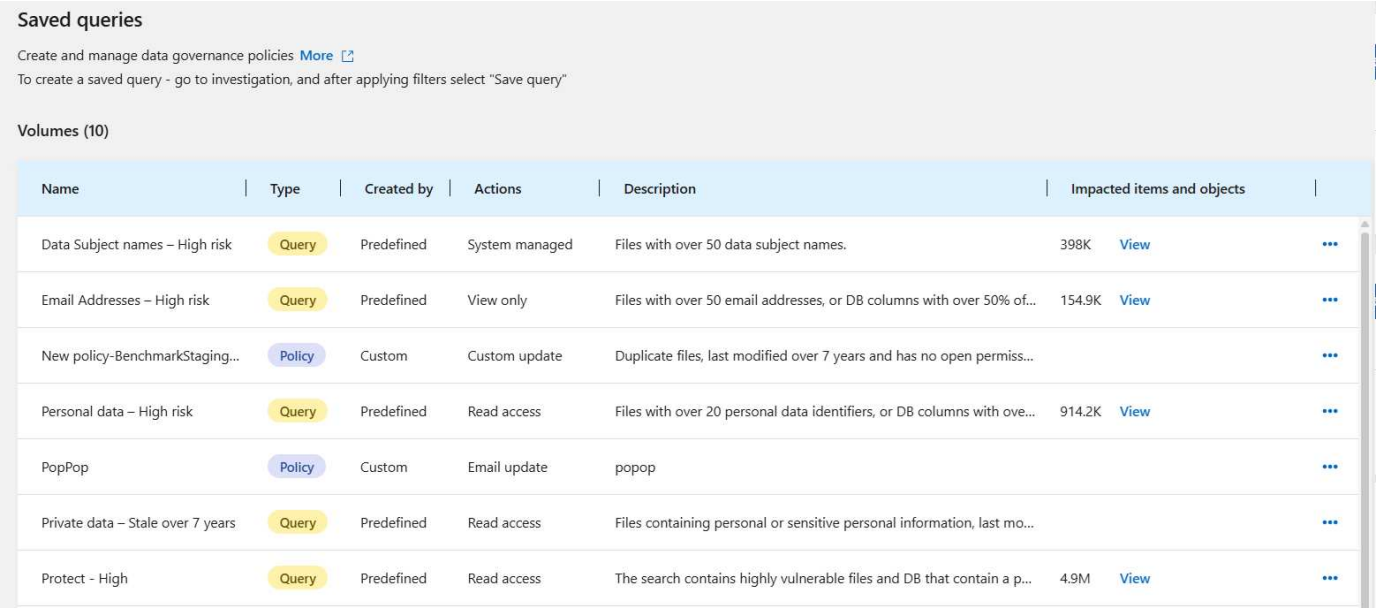
Gérer les requêtes enregistrées avec la NetApp Data Classification

NetaApp Data Classification prend en charge l'enregistrement de vos requêtes de recherche. Avec une requête enregistrée, vous pouvez créer des filtres personnalisés pour trier les requêtes fréquentes de votre page d'enquête sur les données. La classification des données comprend également des requêtes enregistrées prédéfinies basées sur des demandes courantes.

L'onglet **Requêtes enregistrées** du tableau de bord Conformité répertorie toutes les requêtes enregistrées prédéfinies et personnalisées disponibles sur cette instance de classification des données.

Les requêtes enregistrées peuvent également être enregistrées en tant que **politiques**. Alors que les requêtes filtrent les données, les politiques vous permettent d'agir sur les données. Avec une politique : vous pouvez supprimer les données découvertes ou envoyer des mises à jour par e-mail sur les données découvertes.

Les requêtes enregistrées apparaissent également dans la liste des filtres de la page Enquête.



Afficher les résultats des requêtes enregistrées dans la page Enquête

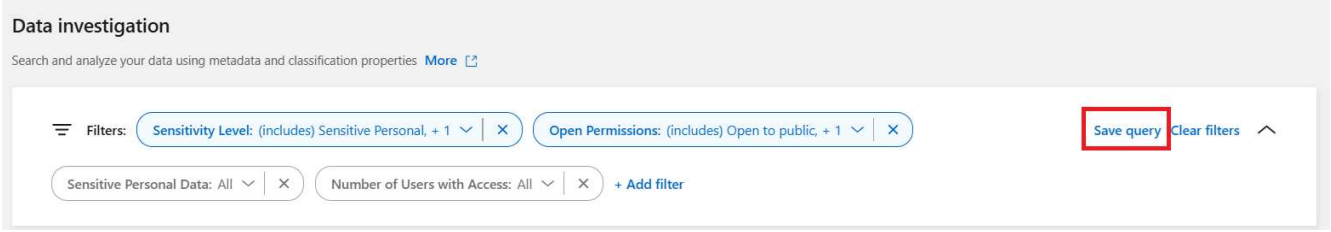
Pour afficher les résultats d'une requête enregistrée dans la page Investigation, sélectionnez l'icône bouton pour une recherche spécifique puis sélectionnez **Enquêter sur les résultats**.

Créer des requêtes et des politiques enregistrées

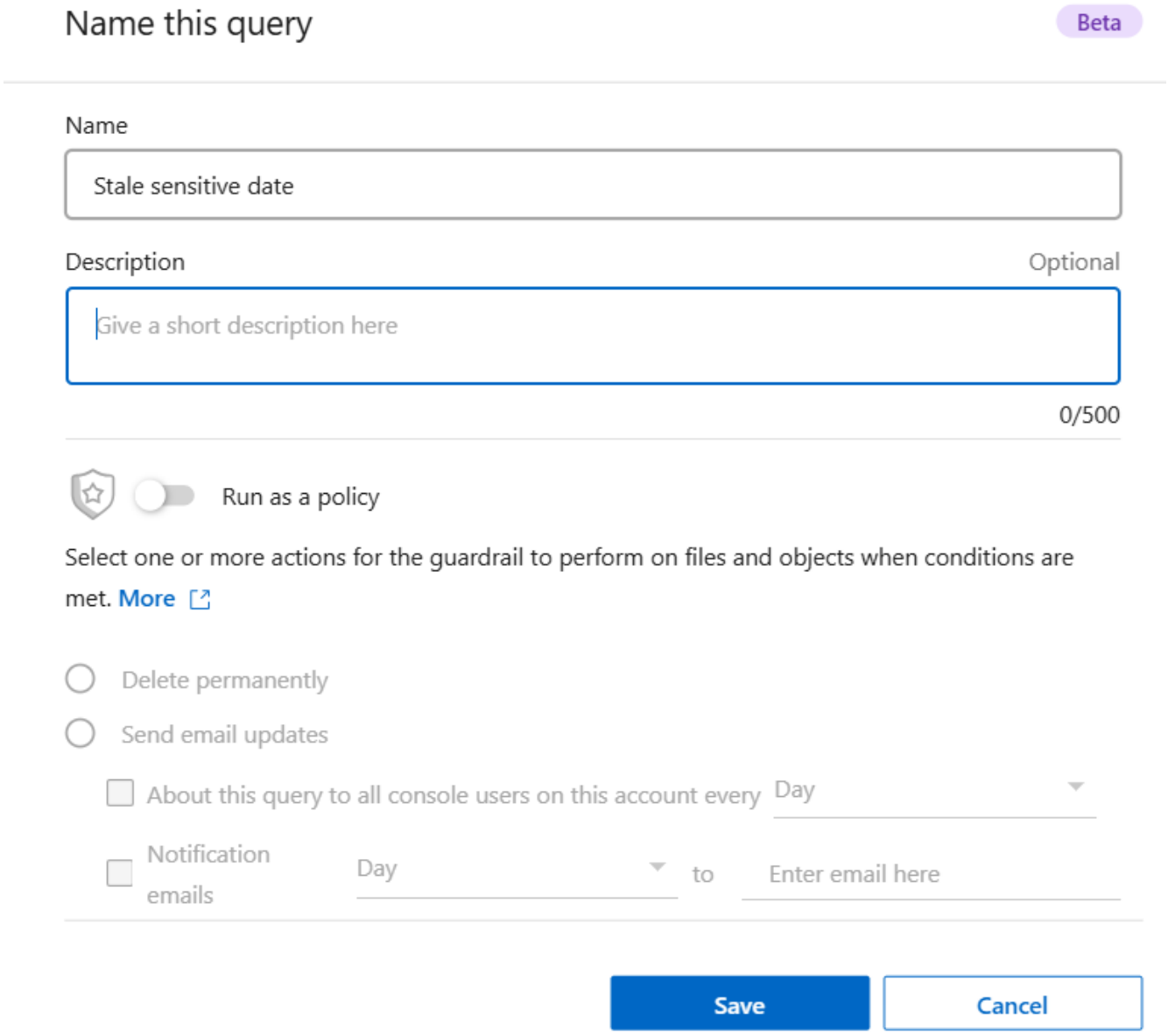
Vous pouvez créer vos propres requêtes enregistrées personnalisées qui fournissent des résultats pour des requêtes spécifiques à votre organisation. Les résultats sont renvoyés pour tous les fichiers et répertoires (partages et dossiers) qui correspondent aux critères de recherche.

Étapes

1. Dans l'onglet Enquête, définissez une recherche en sélectionnant les filtres que vous souhaitez utiliser. Voir"Filtrage des données dans la page Investigation" pour plus de détails.
2. Une fois que vous avez défini toutes les caractéristiques du filtre à votre guise, sélectionnez **Enregistrer la requête**.



3. Nommez la requête enregistrée et ajoutez une description. Le nom doit être unique.
4. Vous pouvez éventuellement enregistrer la requête en tant que politique :
   a. Pour enregistrer la requête en tant que politique, activez le bouton **Exécuter en tant que politique**.
   b. Choisissez de **Supprimer définitivement** ou **Envoyer des mises à jour par e-mail**. Si vous choisissez les mises à jour par e-mail, vous pouvez envoyer les résultats de la requête par e-mail à *tous* les utilisateurs de la console quotidiennement, hebdomadairement ou mensuellement. Alternativement, vous pouvez envoyer la notification à une adresse e-mail spécifique aux mêmes fréquences.
5. Sélectionnez **Enregistrer**.



Une fois la recherche ou la politique créée, vous pouvez la visualiser dans l'onglet **Requêtes enregistrées**.

Modifier les requêtes ou les politiques enregistrées

Vous pouvez modifier le nom et la description d'une requête enregistrée. Vous pouvez également convertir une requête en politique et vice versa.

Vous ne pouvez pas modifier les requêtes enregistrées par défaut. Vous ne pouvez pas modifier les filtres d'une requête enregistrée. Vous pouvez alternativement afficher les résultats de l'enquête d'une requête enregistrée, modifier les filtres, puis l'enregistrer en tant que nouvelle requête ou politique.

Étapes

1. Depuis la page Requêtes enregistrées, sélectionnez **Modifier la recherche** pour la recherche que vous souhaitez modifier.

2. Apportez les modifications aux champs nom et description. Pour modifier uniquement les champs nom et description.

   Vous pouvez éventuellement convertir la requête en politique ou convertir la politique en requête enregistrée. Activez le bouton **Exécuter en tant que politique** selon vos besoins. .. Si vous convertissez la requête en politique, choisissez **Supprimer définitivement** ou **Envoyer des mises à jour par e-mail**. Si vous choisissez les mises à jour par e-mail, vous pouvez envoyer les résultats de la requête par e-mail à *tous* les utilisateurs de la console quotidiennement, hebdomadairement ou mensuellement. Alternativement, vous pouvez envoyer la notification à une adresse e-mail spécifique aux mêmes fréquences.

3. Sélectionnez **Enregistrer** pour terminer les modifications.

Supprimer les requêtes enregistrées

Vous pouvez supprimer toute requête ou politique personnalisée enregistrée si vous n'en avez plus besoin. Vous ne pouvez pas supprimer les requêtes enregistrées par défaut.

Pour supprimer une requête enregistrée, sélectionnez l'icône bouton pour une recherche spécifique, sélectionnez **Supprimer la requête**, puis sélectionnez à nouveau **Supprimer la requête** dans la boîte de dialogue de confirmation.

Requêtes par défaut

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

- **Noms des personnes concernées - Risque élevé**

  Fichiers contenant plus de 50 noms de personnes concernées

- **Adresses e-mail - Risque élevé**

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

- **Données personnelles - Risque élevé**

  Fichiers contenant plus de 20 identifiants de données personnelles ou colonnes de base de données dont plus de 50 % de leurs lignes contiennent des identifiants de données personnelles

- **Données privées - Obsolètes depuis plus de 7 ans**

  Fichiers contenant des informations personnelles ou sensibles, modifiés pour la dernière fois il y a plus de 7 ans

- **Protéger - Élevé**

  Fichiers ou colonnes de base de données contenant un mot de passe, des informations de carte de crédit,

un numéro IBAN ou un numéro de sécurité sociale

- **Protéger - Faible**

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

- **Protéger - Moyen**

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

- **Données personnelles sensibles - Risque élevé**

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

Modifier les paramètres d'analyse de NetApp Data Classification pour vos référentiels

Vous pouvez gérer la manière dont vos données sont analysées dans chacun de vos systèmes et sources de données. Vous pouvez effectuer les modifications sur une base de « référentiel » ; ce qui signifie que vous pouvez effectuer des modifications pour chaque volume, schéma, utilisateur, etc. en fonction du type de source de données que vous analysez.

Certaines des choses que vous pouvez modifier sont si un référentiel est analysé ou non et si NetApp Data Classification effectue une"scan de cartographie ou scan de cartographie et de classification" . Vous pouvez également suspendre et reprendre l'analyse, par exemple, si vous devez arrêter l'analyse d'un volume pendant un certain temps.

Afficher l'état de l'analyse de vos référentiels

Vous pouvez afficher les référentiels individuels que NetApp Data Classification analyse (volumes, buckets, etc.) pour chaque système et source de données. Vous pouvez également voir combien ont été « cartographiés » et combien ont été « classés ». La classification prend plus de temps car l'identification complète de l'IA est effectuée sur toutes les données.

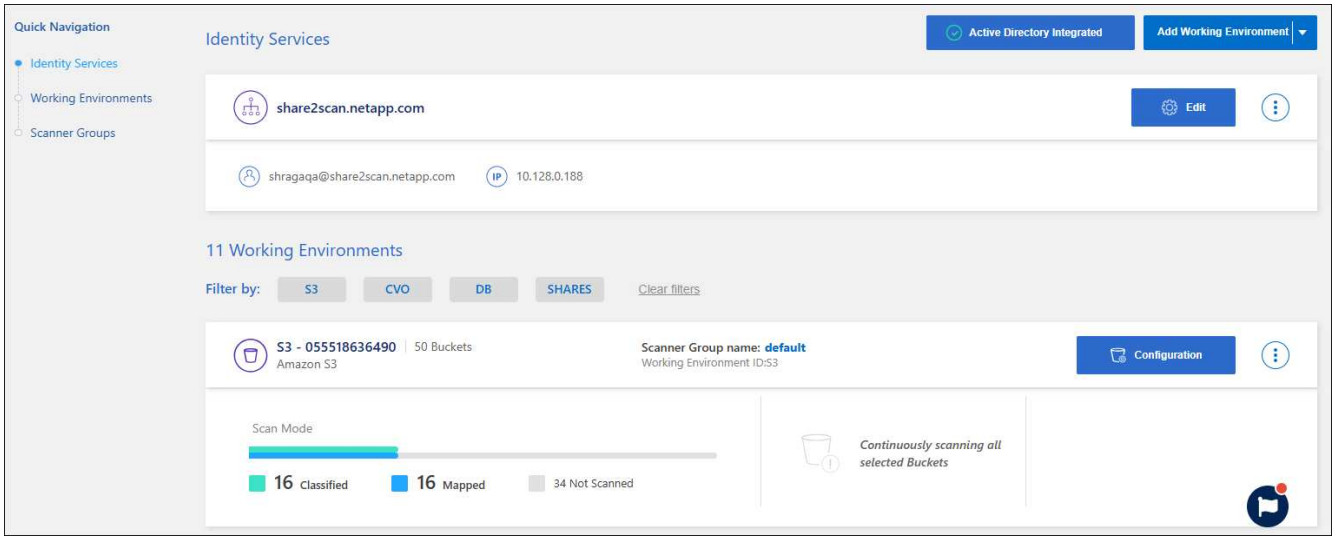
Vous pouvez afficher l'état de numérisation de chaque environnement de travail sur la page de configuration :

- **Initialisation** (point bleu clair) : La configuration de la carte ou de la classification est activée. Ce message apparaît brièvement avant de passer au statut « en attente dans la file d'attente ».
- **File d'attente en attente** (point orange) : la tâche d'analyse attend d'être répertoriée dans la file d'attente d'analyse.
- **En file d'attente** (point orange) : la tâche a été ajoutée avec succès à la file d'attente d'analyse. Le système commencera à cartographier ou à classer le volume lorsque son tour dans la file d'attente arrivera.
- **En cours d'exécution** (point vert) : la tâche d'analyse, qui était dans la file d'attente, est en cours d'exécution sur le référentiel de stockage sélectionné.
- **Terminé** (point vert) : L'analyse du référentiel de stockage est terminée.

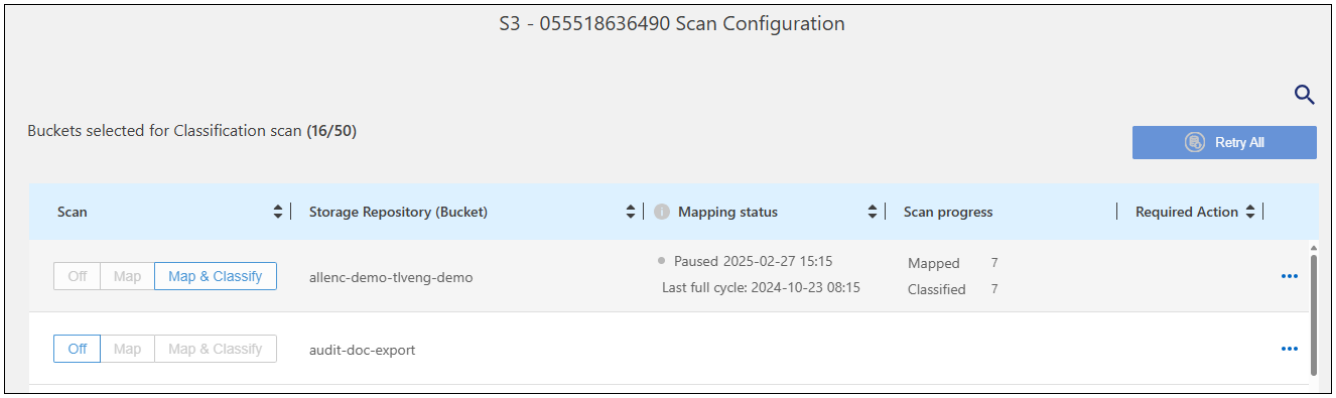
- **En pause** (point gris) : Vous avez interrompu la numérisation. Bien que les variations de volume ne soient pas affichées dans le système, les données analysées restent disponibles.
- **Erreur** (point rouge) : L'analyse ne peut pas se terminer car elle a rencontré des problèmes. Si vous devez effectuer une action, l'erreur apparaît dans l'info-bulle sous la colonne « Action requise ». Dans le cas contraire, le système affiche un statut « erreur » et tente de récupérer. Une fois terminé, le statut change.
- **Pas de numérisation** : la configuration du volume « Désactivé » a été sélectionnée et le système ne scanne pas le volume.

Étapes

1. Dans le menu Classification des données, sélectionnez **Configuration**.



2. Dans l'onglet Configuration, sélectionnez le bouton **Configuration** pour le système.
3. Dans la page Configuration de l'analyse, affichez les paramètres d'analyse pour tous les référentiels.



4. Pendant une analyse, placez votre curseur sur la barre de progression dans la colonne *État du mappage* pour afficher le nombre de fichiers en attente de mappage ou de classification pour ce référentiel.

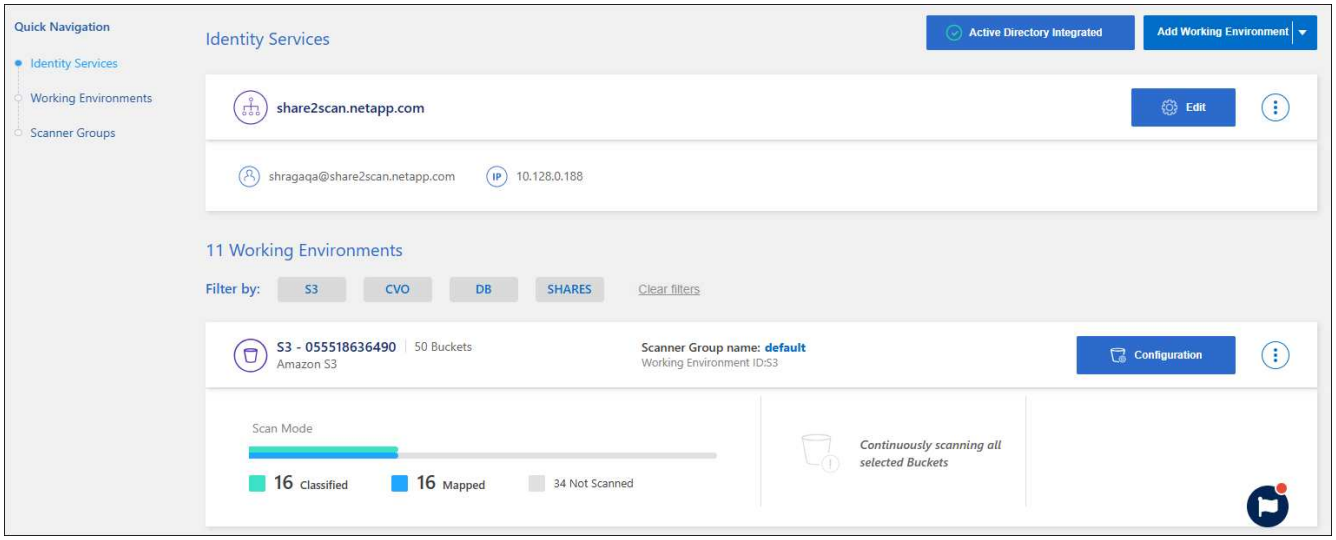
Modifier le type d'analyse d'un référentiel

Vous pouvez démarrer ou arrêter les analyses de mappage uniquement, ou les analyses de mappage et de classification, dans un système à tout moment à partir de la page Configuration. Vous pouvez également passer d'analyses de mappage uniquement à des analyses de mappage et de classification, et vice-versa.

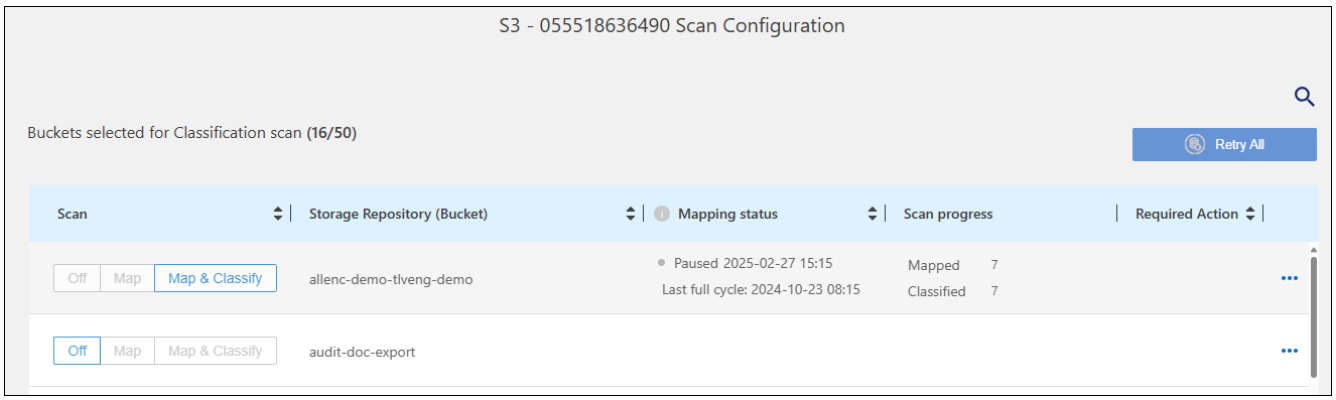
Les bases de données ne peuvent pas être configurées pour des analyses de mappage uniquement. L'analyse de la base de données peut être désactivée ou activée ; où activé est équivalent à Map & Classify.

Étapes

1. Dans le menu Classification des données, sélectionnez **Configuration**.
2. Dans l'onglet Configuration, sélectionnez le bouton **Configuration** pour le système.

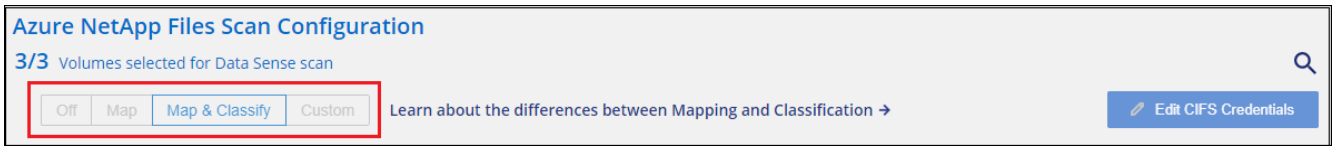


3. Dans la page Configuration de l'analyse, modifiez l'un des référentiels (compartiments dans cet exemple) pour effectuer des analyses **Map** ou **Map & Classify**.



Certains types de systèmes vous permettent de modifier le type d'analyse globalement pour tous les référentiels à l'aide d'une barre de boutons en haut de la page. Ceci est valable pour les systèmes Cloud Volumes ONTAP, ONTAP sur site, Azure NetApp Files et Amazon FSx pour ONTAP .

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



Prioriser les analyses

Vous pouvez prioriser les analyses de cartographie uniquement les plus importantes ou cartographier et classer les analyses pour garantir que les analyses hautement prioritaires sont effectuées en premier.

Par défaut, les analyses sont mises en file d'attente en fonction de l'ordre dans lequel elles sont lancées. Grâce à la possibilité de hiérarchiser les analyses, vous pouvez déplacer les analyses vers l'avant de la file d'attente. Plusieurs analyses peuvent être priorisées. La priorité est désignée selon un ordre premier entré, premier sorti, ce qui signifie que la première analyse que vous priorisez passe en tête de la file d'attente ; la deuxième analyse que vous priorisez devient la deuxième dans la file d'attente, et ainsi de suite.

La priorité est accordée une seule fois. Les réanalyses automatiques des données de cartographie se produisent dans l'ordre par défaut.

Étapes

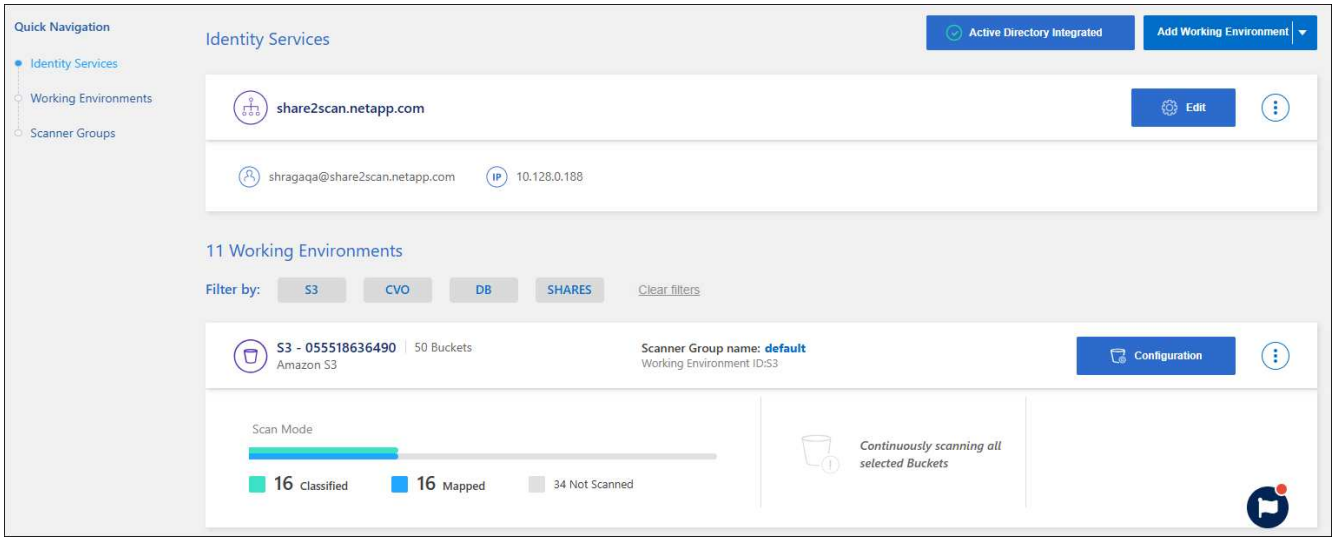
1. Dans le menu Classification des données, sélectionnez **Configuration**.
2. Sélectionnez les ressources que vous souhaitez prioriser.
3. Des actions … option, sélectionnez **Prioriser l'analyse**.

Arrêter la recherche d'un référentiel

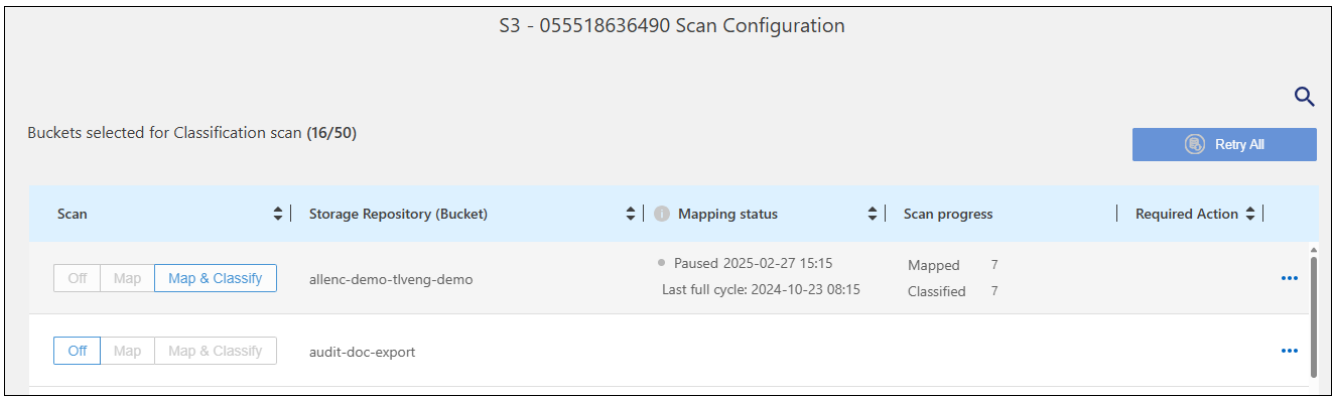
Vous pouvez arrêter l'analyse d'un référentiel (par exemple, un volume) si vous n'avez plus besoin de surveiller sa conformité. Vous pouvez le faire en désactivant la numérisation. Lorsque l'analyse est désactivée, toute l'indexation et les informations sur ce volume sont supprimées du système et la facturation de l'analyse des données est arrêtée.

Étapes

1. Dans le menu Classification des données, sélectionnez **Configuration**.
2. Dans l'onglet Configuration, sélectionnez le bouton **Configuration** pour le système.



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



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

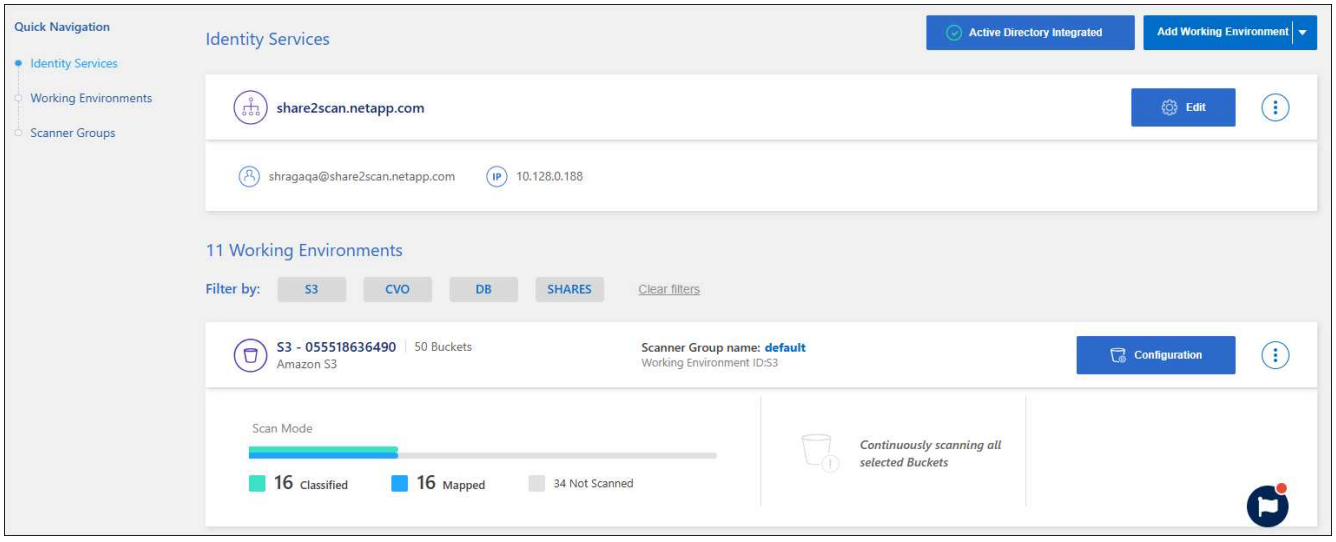
Vous pouvez « suspendre » l'analyse d'un référentiel si vous souhaitez arrêter temporairement l'analyse de certains contenus. La suspension de l'analyse signifie que la classification des données n'effectuera plus aucune analyse pour détecter les modifications ou les ajouts au référentiel. Tous les résultats d'analyse actuels restent accessibles dans la section Classification des données.

La suspension des analyses n'entraîne pas la suppression des frais de facturation, car les données restent présentes dans le système.

Vous pouvez reprendre la numérisation à tout moment.

Étapes

1. Dans le menu Classification des données, sélectionnez **Configuration**.
2. Dans l'onglet Configuration, sélectionnez le bouton **Configuration** pour le système.



3. Dans la page Configuration de l'analyse, sélectionnez les actions ••• icône.
4. Sélectionnez **Pause** pour suspendre l'analyse d'un volume ou sélectionnez **Reprendre** pour reprendre l'analyse d'un volume qui avait été précédemment suspendu.

Afficher les rapports de conformité de la NetApp Data Classification

NetApp Data Classification fournit des rapports que vous pouvez utiliser pour mieux comprendre l'état du programme de confidentialité des données de votre organisation.

Par défaut, les tableaux de bord de classification des données affichent les données de conformité et de gouvernance pour tous les systèmes, bases de données et sources de données. Si vous souhaitez afficher des rapports contenant des données pour certains systèmes uniquement, vous pouvez filtrer pour les voir uniquement.

- Les rapports de conformité ne sont disponibles que si vous effectuez une analyse de classification complète sur vos sources de données. Les sources de données ayant fait l'objet d'une analyse de mappage uniquement peuvent uniquement générer le rapport de mappage de données.
- NetApp ne peut pas garantir l'exactitude à 100 % des données personnelles et des données personnelles sensibles identifiées par Data Classification. Vous devez toujours valider les informations en examinant les données.

Les rapports suivants sont disponibles pour la classification des données :

- **Rapport d'évaluation de la découverte de données** : fournit une analyse de haut niveau de l'environnement analysé pour mettre en évidence les résultats du système et montrer les zones de préoccupation et les étapes de correction potentielles. Ce rapport est disponible dans le tableau de bord de gouvernance.
- **Rapport d'aperçu complet du mappage des données** : fournit des informations sur la taille et le nombre de fichiers dans vos systèmes. Cela inclut la capacité d'utilisation, l'âge des données, la taille des données et les types de fichiers. Ce rapport est disponible dans le tableau de bord de gouvernance.
- **Rapport de demande d'accès aux données personnelles** : vous permet d'extraire un rapport de tous les fichiers contenant des informations concernant le nom spécifique ou l'identifiant personnel d'une personne concernée. Ce rapport est disponible dans le tableau de bord Conformité.
- **Rapport HIPAA** : vous aide à identifier la répartition des informations de santé dans vos fichiers. Ce rapport est disponible dans le tableau de bord Conformité.
- **Rapport PCI DSS** : vous aide à identifier la répartition des informations de carte de crédit dans vos fichiers. Ce rapport est disponible dans le tableau de bord Conformité.
- **Rapport d'évaluation des risques liés à la confidentialité** : fournit des informations sur la confidentialité de vos données et un score de risque lié à la confidentialité. Ce rapport est disponible dans le tableau de bord Conformité.
- **Rapports sur un type d'informations spécifique** : Des rapports sont disponibles qui incluent des détails sur les fichiers identifiés contenant des données personnelles et des données personnelles sensibles. Vous pouvez également voir les fichiers classés par catégorie et par type de fichier.

Sélectionnez les systèmes pour les rapports

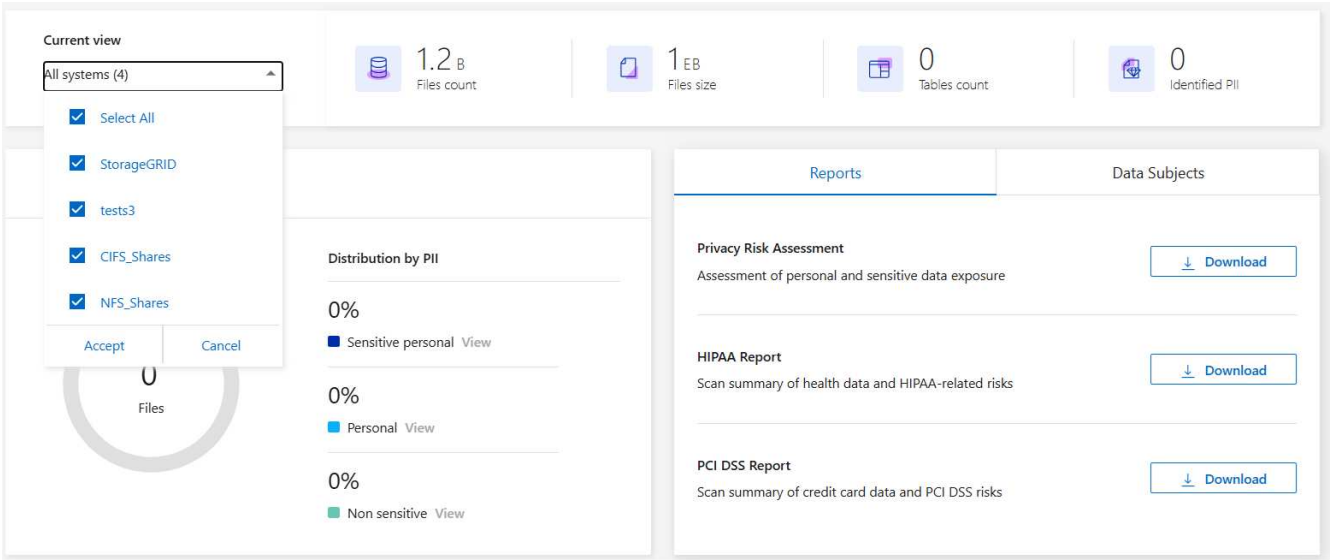
Vous pouvez filtrer le contenu du tableau de bord de conformité de la classification des données pour afficher les données de conformité pour tous les systèmes et bases de données, ou uniquement pour des systèmes spécifiques.

Lorsque vous filtrez le tableau de bord, la classification des données limite les données de conformité et les

rapports uniquement aux systèmes que vous avez sélectionnés.

Étapes

1. Dans le menu Classification des données, sélectionnez **Conformité**.
2. Sélectionnez la liste déroulante du filtre des systèmes, puis sélectionnez les systèmes.
3. Sélectionnez **Accepter** pour confirmer votre sélection.



Rapport de demande d’accès aux données personnelles

Les réglementations en matière de confidentialité telles que le RGPD européen accordent aux personnes concernées (telles que les clients ou les employés) le droit d’accéder à leurs données personnelles. Lorsqu’une personne concernée demande ces informations, on parle alors de demande d’accès aux données (DSAR). Les organisations sont tenues de répondre à ces demandes « sans retard injustifié », et au plus tard dans un délai d’un mois à compter de leur réception.

Vous pouvez répondre à un DSAR en recherchant le nom complet d’un sujet ou un identifiant connu (comme une adresse e-mail), puis en téléchargeant un rapport. Le rapport est conçu pour aider votre organisation à se conformer au RGPD ou à des lois similaires sur la confidentialité des données.

Comment la classification des données peut-elle vous aider à répondre à une DSAR ?

Lorsque vous effectuez une recherche sur une personne concernée, la classification des données recherche tous les fichiers contenant le nom ou l’identifiant de cette personne. La classification des données vérifie les dernières données pré-indexées pour le nom ou l’identifiant. Il ne lance pas de nouvelle analyse.

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

La recherche de personnes concernées n’est actuellement pas prise en charge dans les bases de données.

Rechercher des personnes concernées et télécharger des rapports

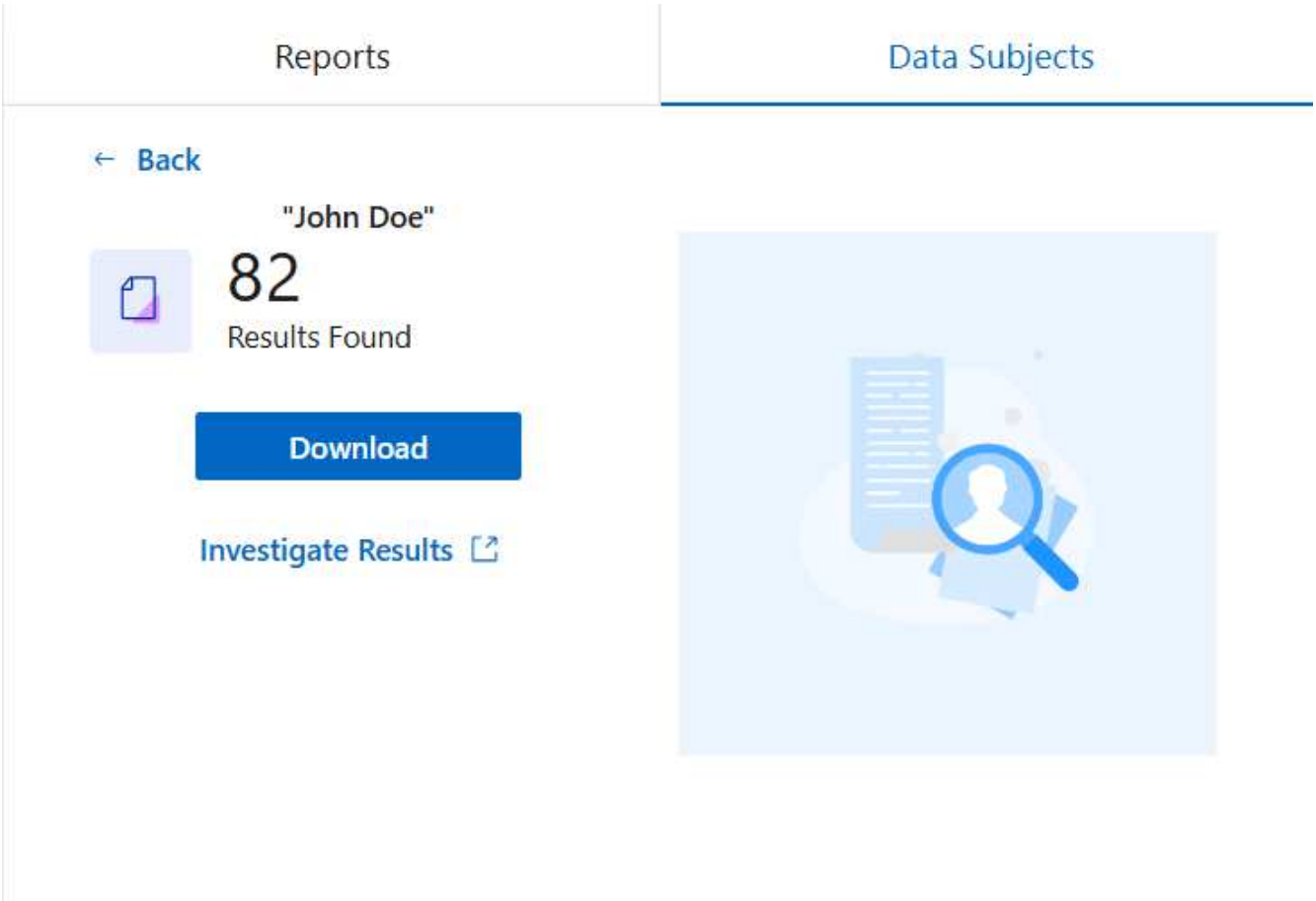
Recherchez le nom complet ou l’identifiant connu de la personne concernée, puis téléchargez un rapport de

liste de fichiers ou un rapport DSAR. Vous pouvez rechercher par"tout type d'informations personnelles" .

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

Étapes

1. Dans le menu Classification des données, sélectionnez **Conformité**.
2. Depuis la page Conformité, recherchez l'onglet **Personnes concernées**.
3. Dans la section **Personnes concernées**, saisissez un nom ou un identifiant connu, puis sélectionnez **Rechercher**.
4. Une fois la recherche terminée, sélectionnez **Télécharger** pour accéder à la réponse à la demande d'accès de la personne concernée. Sélectionnez **Enquêter sur les résultats** pour afficher plus d'informations sur la page Enquête sur les données.



5. Consultez les résultats dans la classification des données ou téléchargez-les sous forme de rapport en sélectionnant l'icône de téléchargement.

   a. Lorsque vous sélectionnez l'icône de téléchargement, configurez vos paramètres de téléchargement :

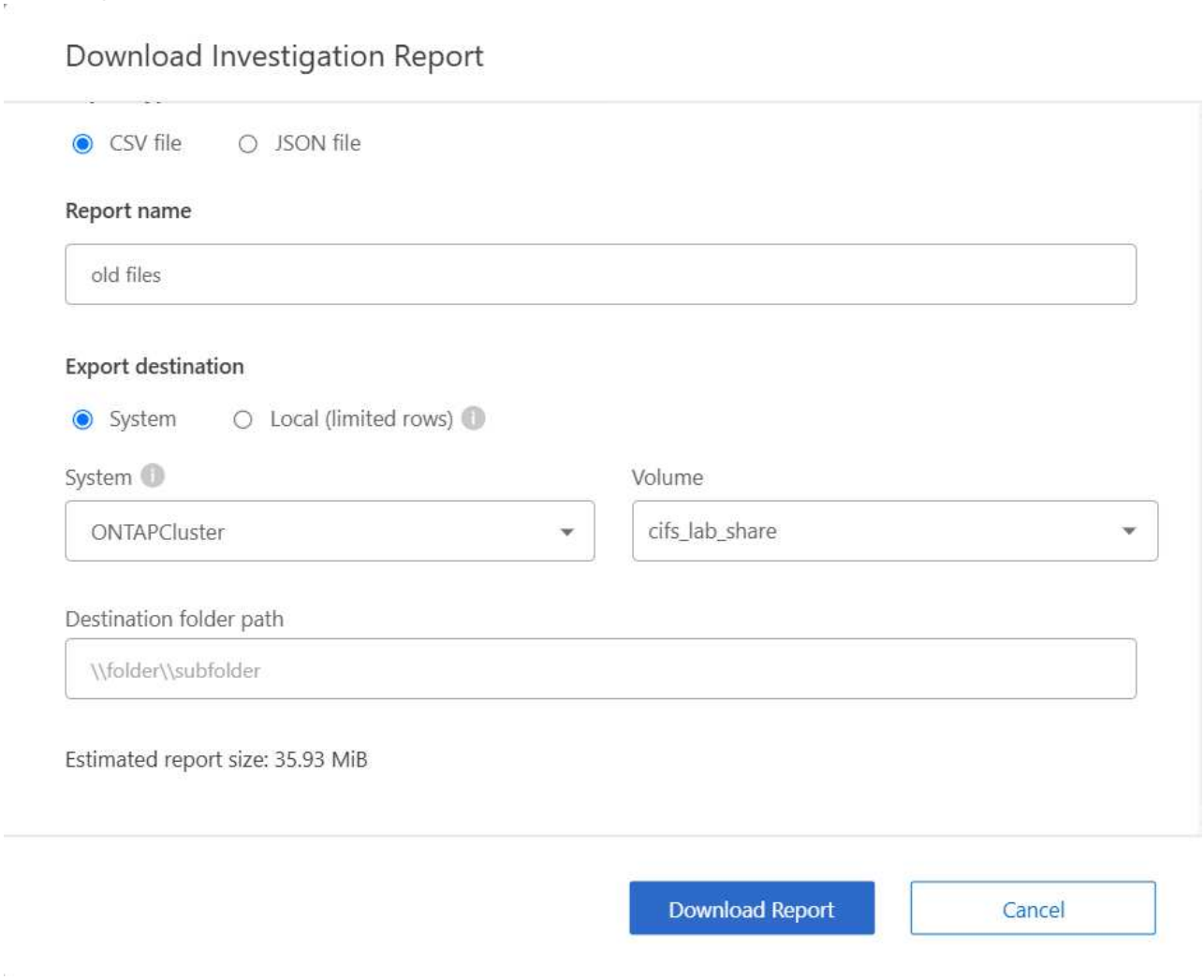
      - Choisissez le format du film : CSV ou JSON
      - Saisissez un **Nom du rapport**
      - Choisissez la destination d'exportation : **Système** ou votre machine **locale**.

      Si vous choisissez le système, toutes les données sont téléchargées. Vous devez également

sélectionner le **Système**, le **Volume** et le **Chemin du dossier de destination**.

Si vous choisissez **Local**, le rapport est limité aux 10 000 premières lignes de données non structurées, 5 000 lignes de données non structurées et 1 000 lignes de données structurées.

a. Sélectionnez **Télécharger le rapport** pour lancer le téléchargement.



Rapport sur la loi sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA)

Le rapport sur la loi sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA) peut vous aider à identifier les fichiers contenant des informations sur la santé. Il est conçu pour aider votre organisation à se conformer aux lois sur la confidentialité des données HIPAA. Les informations recherchées par la classification des données comprennent :

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

Le rapport comprend les informations suivantes :

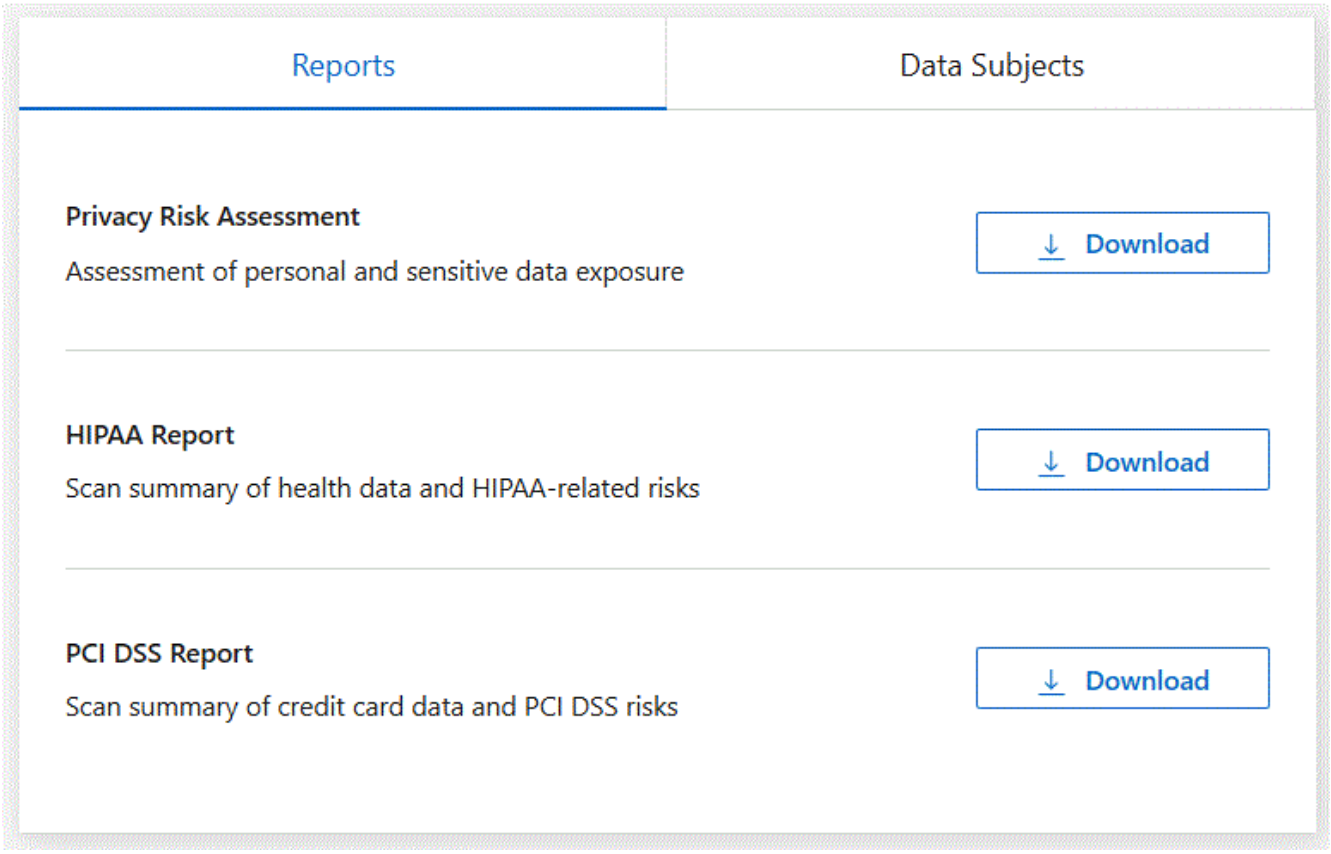
- Aperçu : Combien de fichiers contiennent des informations sur la santé et dans quels systèmes.
- Cryptage : pourcentage de fichiers contenant des informations sur la santé qui se trouvent sur des systèmes cryptés ou non cryptés. Ces informations sont spécifiques à Cloud Volumes ONTAP.
- Protection contre les ransomwares : pourcentage de fichiers contenant des informations sur la santé qui se trouvent sur des systèmes sur lesquels la protection contre les ransomwares est activée ou non. Ces informations sont spécifiques à Cloud Volumes ONTAP.
- Conservation : la période pendant laquelle les fichiers ont été modifiés pour la dernière fois. Cela est utile car vous ne devez pas conserver les informations de santé plus longtemps que nécessaire pour les traiter.
- Distribution des informations sur la santé : les systèmes dans lesquels les informations sur la santé ont été trouvées et si le cryptage et la protection contre les ransomwares sont activés.

Générer le rapport HIPAA

Accédez à l'onglet Conformité pour générer le rapport.

Étapes

1. Dans le menu Classification des données, sélectionnez **Conformité**.
2. Localisez le **volet Rapports**. Sélectionnez l'icône de téléchargement à côté de **Rapport HIPAA**.



Résultat

La classification des données génère un rapport PDF.

Rapport sur la norme de sécurité des données de l’industrie des cartes de paiement (PCI DSS)

Le rapport sur la norme de sécurité des données de l’industrie des cartes de paiement (PCI DSS) peut vous aider à identifier la répartition des informations de carte de crédit dans vos fichiers.

Le rapport comprend les informations suivantes :

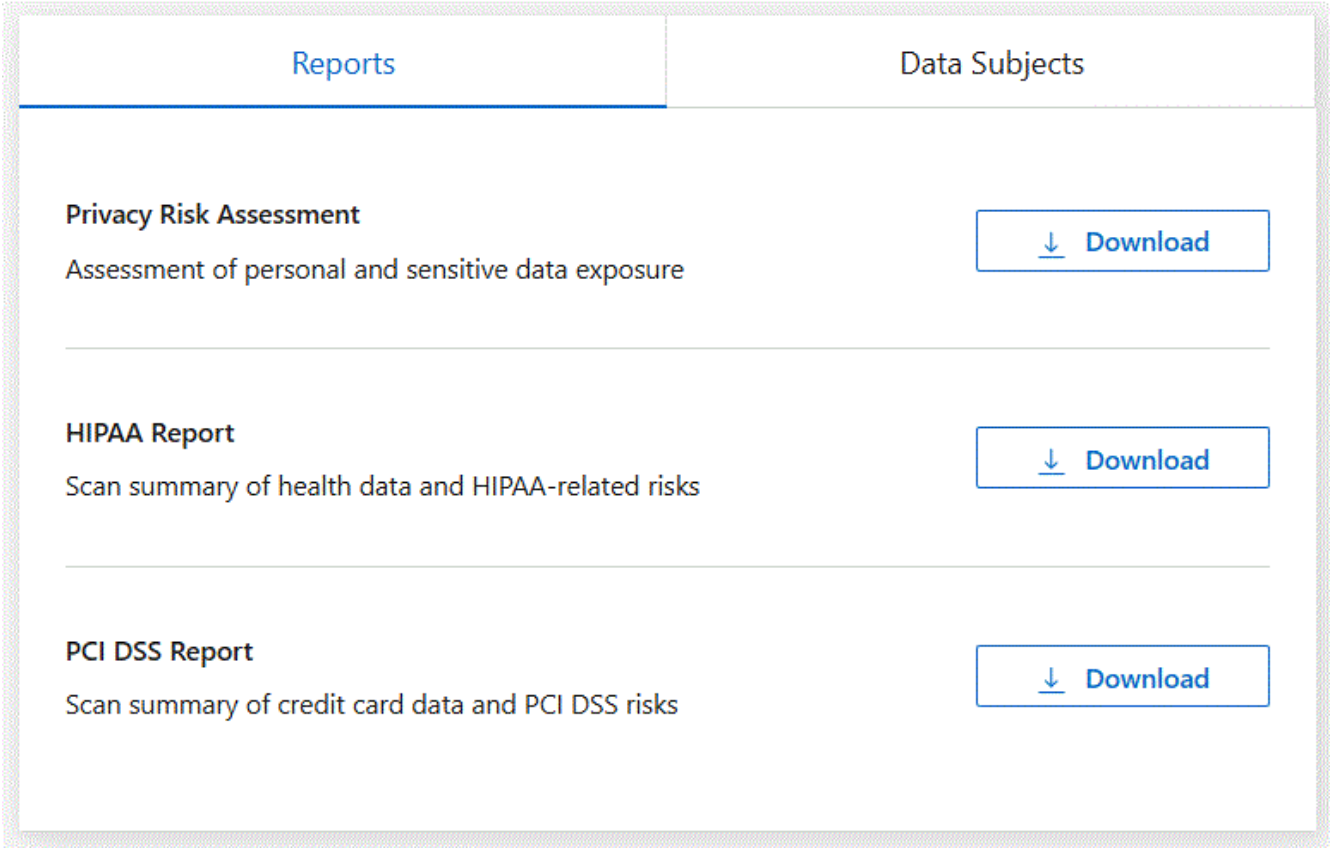
- Aperçu : Combien de fichiers contiennent des informations de carte de crédit et dans quels systèmes.
- Cryptage : pourcentage de fichiers contenant des informations de carte de crédit qui se trouvent sur des systèmes cryptés ou non cryptés. Ces informations sont spécifiques à Cloud Volumes ONTAP.
- Protection contre les ransomwares : pourcentage de fichiers contenant des informations de carte de crédit qui se trouvent sur des systèmes sur lesquels la protection contre les ransomwares est activée ou non. Ces informations sont spécifiques à Cloud Volumes ONTAP.
- Conservation : la période pendant laquelle les fichiers ont été modifiés pour la dernière fois. Cela est utile car vous ne devez pas conserver les informations de carte de crédit plus longtemps que nécessaire pour les traiter.
- Distribution des informations de carte de crédit : les systèmes sur lesquels les informations de carte de crédit ont été trouvées et si le cryptage et la protection contre les ransomwares sont activés.

Générer le rapport PCI DSS

Accédez à l’onglet Conformité pour générer le rapport.

Étapes

1. Dans le menu Classification des données, sélectionnez **Conformité**.
2. Localisez le **volet Rapports**. Sélectionnez l’icône de téléchargement à côté de **Rapport PCI DSS**.



Résultat

La classification des données génère un rapport PDF que vous pouvez consulter et envoyer à d'autres groupes selon vos besoins.

Rapport d'évaluation des risques liés à la vie privée

Le rapport d'évaluation des risques liés à la confidentialité fournit un aperçu de l'état des risques liés à la confidentialité de votre organisation, comme l'exigent les réglementations sur la confidentialité telles que le RGPD et le CCPA.

Le rapport comprend les informations suivantes :

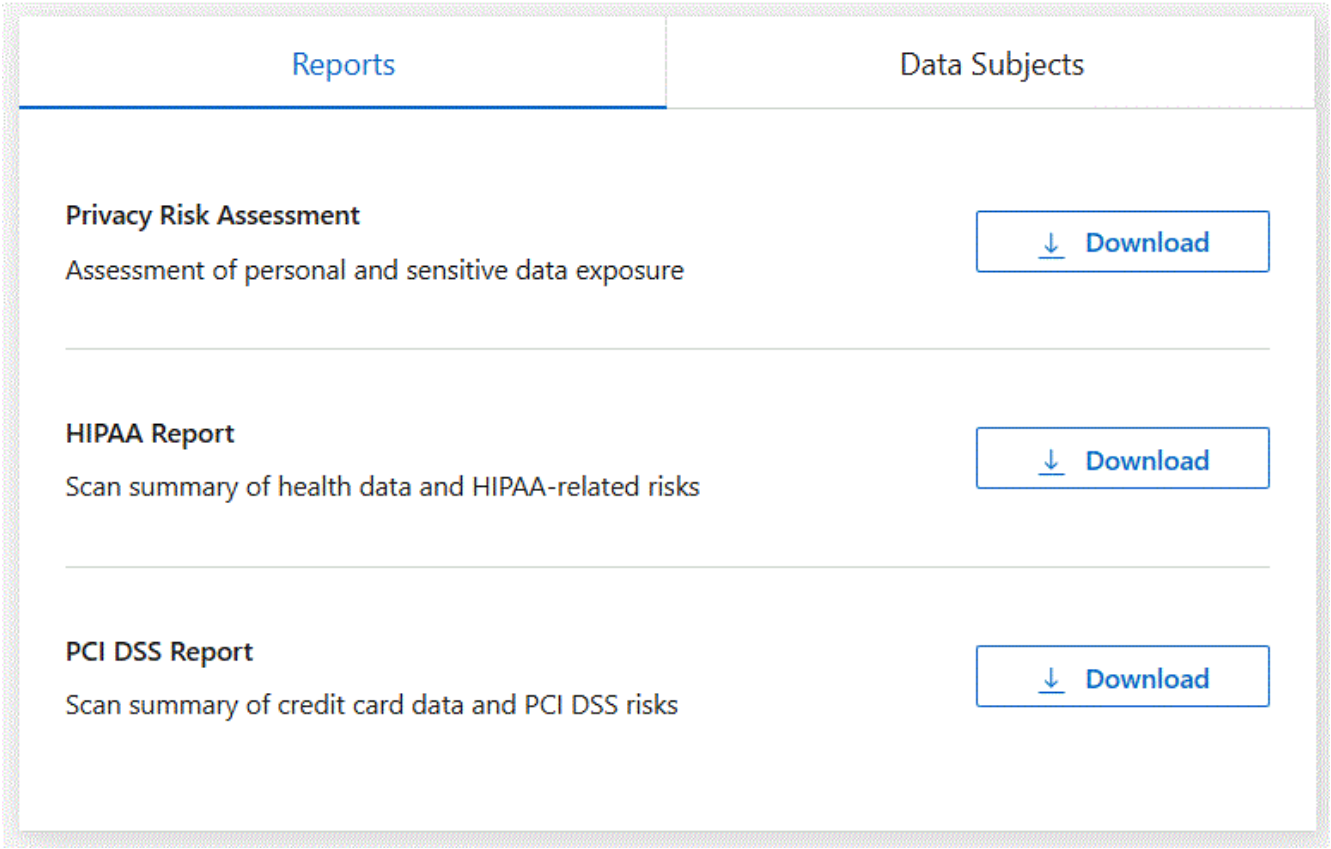
- État de conformité : un score de gravité et la distribution des données, qu'elles soient non sensibles, personnelles ou personnelles sensibles.
- Aperçu de l'évaluation : une répartition des types de données personnelles trouvées, ainsi que des catégories de données.
- Personnes concernées par cette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

Générer le rapport d'évaluation des risques liés à la confidentialité

Accédez à l'onglet Conformité pour générer le rapport.

Étapes

1. Dans le menu Classification des données, sélectionnez **Conformité**.
2. Localisez le **volet Rapports**. Sélectionnez l'icône de téléchargement à côté de **Rapport d'évaluation des risques liés à la confidentialité**.



Résultat

La classification des données génère un rapport PDF que vous pouvez consulter et envoyer à d'autres groupes selon vos besoins.

Score de gravité

La classification des données calcule le score de gravité du rapport d'évaluation des risques liés à la confidentialité sur la base de trois variables :

- Le pourcentage de données personnelles sur l'ensemble des données.
- Le pourcentage de données personnelles sensibles sur l'ensemble des données.
- Le pourcentage de fichiers qui incluent des personnes concernées, déterminé par des identifiants nationaux tels que les cartes d'identité nationales, les numéros de sécurité sociale et les numéros d'identification fiscale.

La logique utilisée pour déterminer le score est la suivante :

Score 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 %

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

Surveiller l'état de la NetApp Data Classification

Le tableau de bord NetApp Data Classification Health Monitor assure une surveillance en temps réel et fournit des informations sur les performances. Le Health Monitor recueille des informations sur votre infrastructure de classification des données, l'état de votre système, les indicateurs d'utilisation et les données d'utilisation, vous permettant ainsi d'identifier et de résoudre les problèmes.

Informations du moniteur de santé

Le tableau de bord Health Monitor présente les informations dans quatre catégories.

- **État de l'infrastructure**

  Consultez les informations relatives à la version, à la stabilité du système, au type de déploiement et à la taille de la machine.

- **Conteneurs problématiques**

  Consultez le champ des conteneurs problématiques pour obtenir des informations sur les conteneurs qui sont arrêtés ou redémarrés fréquemment. Utilisez ces informations pour examiner les conteneurs spécifiques.

- **Informations système**

  Le panneau d'informations système capture des informations essentielles sur la NetApp Console et la classification des données, telles que les adresses IP publiques et privées, le nom d'hôte, le système d'exploitation, la version de la console et l'ID de la console.

- **Utilisation et mise en œuvre**

  Examinez l'utilisation du processeur, l'utilisation du disque et l'utilisation de la mémoire. Ces valeurs sont affichées en unités de stockage (Go) ou en pourcentage de l'utilisation totale. Si un avertissement s'affiche dans un champ, sélectionnez-le pour obtenir des informations et des recommandations de correction.

Accédez au tableau de bord du Moniteur de santé

1. Dans Classification des données, sélectionnez **Configuration**.
2. Sous l'en-tête **Configuration**, sélectionnez **Moniteur d'intégrité de la classification des données**.

3. Dans le tableau de bord Health Monitor, vous pouvez :
   - Examiner l'utilisation et l'emploi. Si des avertissements apparaissent dans les indicateurs d'utilisation, sélectionnez-les pour obtenir des recommandations permettant de résoudre le problème.
   - Basculez l'affichage du graphique pour visualiser l'utilisation du processeur, l'utilisation du disque et l'utilisation de la mémoire. Vous pouvez modifier l'axe des x pour afficher le contenu sur des heures (6, 12 ou 24) ou des jours (2, 7 ou 14).
   - Actualisez le tableau de bord pour afficher les indicateurs de données les plus récents.