



Gérez les données cloud comme vous le pouvez

Cloud Data Sense

NetApp
December 15, 2022

Table des matières

- Gérez les données cloud comme vous le pouvez 1
 - Ajout d'identifiants de données personnels à vos acquisitions de détection de données 1
 - Affichage de l'état de vos actions de conformité 9
 - Audit de l'historique des actions de détection de données 10
 - Réduction de la vitesse d'acquisition de détection de données 12
 - Suppression des sources de données du cloud au bon sens 13
 - Désinstallation de Cloud Data SENSE 15

Gérez les données cloud comme vous le pouvez

Ajout d'identifiants de données personnels à vos acquisitions de détection de données

Data Sense offre de nombreuses façons d'ajouter une liste personnalisée de « données personnelles » que Data Sense identifiera dans les futures analyses, vous donnant une idée complète de l'emplacement des données potentiellement sensibles dans les fichiers *All* de votre entreprise.

- Vous pouvez ajouter des identificateurs uniques basés sur des colonnes spécifiques dans les bases de données que vous numérisez.
- Vous pouvez ajouter des mots-clés personnalisés à partir d'un fichier texte — ces mots sont identifiés dans vos données.
- Vous pouvez ajouter un motif personnel à l'aide d'une expression régulière (regex) — le regex est ajouté aux motifs prédéfinis existants.



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

Ajoutez des identifiants de données personnelles personnalisés à partir de vos bases de données

Une fonctionnalité que nous appelons *Data Fusion* vous permet d'analyser les données de votre organisation pour identifier si des identificateurs uniques de vos bases de données sont trouvés dans l'une de vos autres sources de données. Vous pouvez choisir les identificateurs supplémentaires que Data Sense recherche dans ses acquisitions en sélectionnant une colonne ou des colonnes spécifiques dans une table de base de données. Par exemple, le diagramme ci-dessous montre comment Data Fusion est utilisé pour analyser vos volumes, compartiments et bases de données pour rechercher les occurrences de tous vos identifiants client à partir de votre base de données Oracle.

Databases -- Structured Data

Database: Oracle
Schema: Accounts
Table: Customers
Column: Customer ID

Account	Name	Customer ID	Address
1234	ABC Co	135876	125 Main St
1235	XYZ Co	213536	35A Brick R
1236	Cat Co	359264	55 Wind Av
1237	Dog Co	472637	11025 Cor
1238	Zebra Co	582455	36 Sahara
...

Scan your volumes and buckets for occurrences of the Customer IDs in your Oracle database

Files -- Unstructured Data

File in Volume 1

```
XXXXXXXXXXXXX
xx213536xxx
XXXXXXXXXXXXX
xx472637xxx
XXXXXXXXXXXXX
XXXXXXXXXXXXX
```

File in Volume 2

```
XXXXXXXXXXXXX
XXXXXXXXXXXXX
XXXXXXXXXXXXX
XXXXXXXXXXXXX
XXXXXXXXXXXXX
xxx472637xx
```

File in Bucket 1

```
XXXXXXXXXXXXX
XXXXXXXXXXXXX
xx213536xxx
XXXXXXXXXXXXX
XXXXXXXXXXXXX
XXXXXXXXXXXXX
```

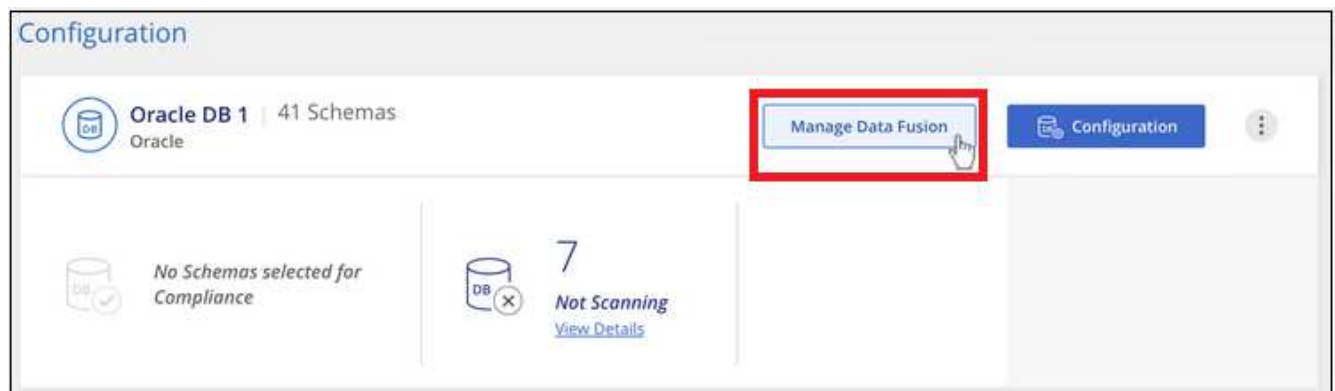
Comme vous pouvez le voir, deux ID de client uniques ont été trouvés sur deux volumes et dans un compartiment S3. Toutes les correspondances dans les tables de base de données seront également identifiées.

Notez que puisque vous scannez vos propres bases de données, quelle que soit la langue dans laquelle vos données sont stockées, vous pourrez identifier les données dans les futures analyses de détection de données.

Étapes

Vous devez avoir "ajout d'au moins un serveur de base de données" À Data Sense avant d'ajouter des sources de données Fusion.

1. Dans la page Configuration, cliquez sur **gérer Fusion de données** dans la base de données où résident les données source.



2. Cliquez sur **Ajouter une source de données Fusion** sur la page suivante.

3. Dans la page *Add Data Fusion Source* :

- Sélectionnez le schéma de la base de données dans le menu déroulant.
- Entrez le nom de la table dans ce schéma.
- Entrez la colonne ou les colonnes contenant les identifiants uniques que vous souhaitez utiliser.

Lors de l'ajout de plusieurs colonnes, entrez chaque nom de colonne ou de vue de table sur une ligne distincte.

Add Data Fusion Source

To add a Data Fusion source reference, specify one or more columns which contain your organization's unique identifiers, such as a column used to store customer IDs. Note that adding a Data Fusion Source will initiate an additional scan of your data stores.

Database Schema: Oracle1,Accounts

Table: Customers

Columns Containing Identifiers: Customer ID

Buttons: Add Data Fusion Source, Cancel

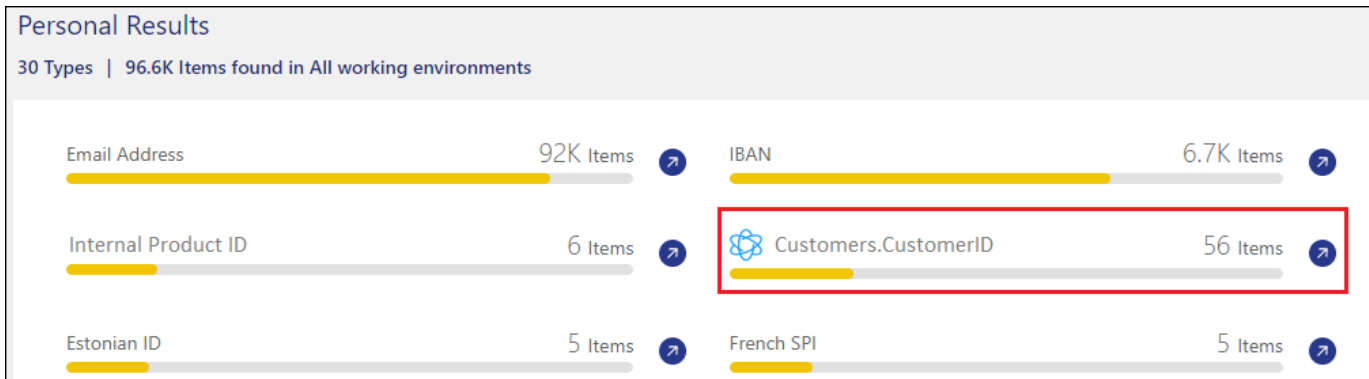
4. Cliquez sur **Ajouter une source de données Fusion**.

La page d'inventaire de Data Fusion affiche les colonnes source de la base de données que vous avez configurées détection des données à analyser.

Database Schema	Table	Data Fusion Source Columns	
Schema1	Table 1	Column 12, Column 4, Column 18	...
Schema2	Table 2	Column 2, Column 14, Column 8	...

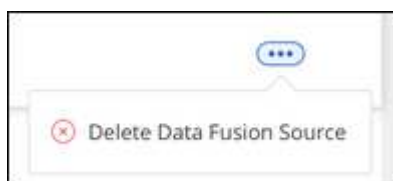
Résultats

Après l'analyse suivante, les résultats incluent ces nouvelles informations dans le tableau de bord de conformité sous la section « Résultats personnels » et dans la page Investigation du filtre « données personnelles ». Chaque colonne source que vous avez ajoutée apparaît dans la liste des filtres au format Table.Column, par exemple Customers.CustomerID.



Supprimer une source de Data Fusion

Si vous décidez à un moment donné de ne pas numériser vos fichiers à l'aide d'une source Data Fusion donnée, vous pouvez sélectionner la ligne source dans la page d'inventaire Data Fusion et cliquer sur **Supprimer la source Data Fusion**.



Ajoutez des mots-clés personnalisés à partir d'un fichier texte

Vous pouvez ajouter des mots-clés personnalisés à Data Sense afin qu'ils identifient des informations spécifiques dans vos données. Vous ajoutez les mots clés d'un fichier texte que vous définissez. Les mots-clés sont ajoutés aux mots-clés prédéfinis existants que Data Sense utilise déjà et les résultats seront visibles sous la section motifs personnels.

Par exemple, vous pouvez voir où les noms de produits internes sont mentionnés dans tous vos fichiers pour vous assurer que ces noms ne sont pas accessibles dans des emplacements qui ne sont pas sécurisés.

Après la mise à jour des mots-clés personnalisés, Data Sense redémarre l'analyse de toutes les sources de données. Les nouveaux résultats apparaissent dans Data Sense une fois l'analyse terminée.

Vous devez ajouter, ou créer, les fichiers texte qui incluent les mots clés personnalisés à l'emplacement suivant sur le système Data Sense :

```
/opt/netapp/Datasense/tools/datascience/custom_keywords/keywords_sets
```

Vous pouvez créer un seul fichier avec plusieurs mots-clés, ou vous pouvez ajouter de nombreux fichiers qui contiennent chacun certains mots-clés. Le format du fichier est un mot sur chaque ligne, par exemple, les noms de produits internes qui sont des types de hiboux sont répertoriés ci-dessous :

internal_product_names.txt

```
barred
barn
horned
snowy
screech
```

La recherche de données SENSE pour ces éléments n'est pas sensible à la casse.

Prenez en compte les conditions suivantes :

- Le nom de fichier ne doit pas contenir de chiffres.
- Chaque fichier peut contenir un maximum de 100,000 mots. S'il y a plus de mots, seuls les 100,000 premiers sont ajoutés.
- Chaque mot doit comporter au moins 3 caractères. Les mots plus courts sont ignorés.
- Les mots en double ne sont ajoutés qu'une seule fois.

Accès à la ligne de commande

Vous devrez accéder au système Data Sense pour lancer la commande afin d'ajouter des mots-clés personnalisés.

Lorsque Data Sense est installé sur votre site, vous pouvez accéder directement à la ligne de commande.

Lorsque Data Sense est déployé dans le cloud, vous devez utiliser SSH vers l'instance Data Sense. Vous vous connectez au système en saisissant l'utilisateur et le mot de passe, ou en utilisant la clé SSH fournie lors de l'installation du connecteur BlueXP. La commande SSH est :

```
ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
* <path_to_the_ssh_key> = emplacement des clés d'authentification ssh
* <machine_utilisateur> :
```

+

Pour AWS : utilisez <utilisateur ec2>

Pour Azure : utilisez l'utilisateur créé pour l'instance BlueXP

** Pour GCP : utilisez l'utilisateur créé pour l'instance BlueXP

- <datasense_ip> = adresse IP de l'instance de la machine virtuelle

Notez que vous devrez modifier les règles entrantes du groupe de sécurité pour accéder au système sur le cloud. Pour plus de détails, voir :

- ["Règles de groupe de sécurité dans AWS"](#)
- ["Règles de groupe de sécurité dans Azure"](#)
- ["Règles de pare-feu dans Google Cloud"](#)

Syntaxe de commande pour ajouter des mots-clés personnalisés

La syntaxe de commande permettant d'ajouter des mots-clés personnalisés à partir d'un fichier est la suivante :

```
sudo bash tools/datascience/custom_keywords/upload_custom_keywords.sh -s  
activate -f <file_name>.txt  
* <nom_fichier> = nom du fichier contenant les mots-clés.
```

Vous exécutez la commande à partir du chemin **/opt/netapp/Datase/**.

Si vous avez créé de nombreux fichiers contenant des mots-clés personnalisés, vous pouvez ajouter les mots-clés de tous les fichiers en même temps à l'aide de la commande suivante :

```
sudo bash tools/datascience/custom_keywords/upload_custom_keywords.sh -s  
activate
```

Exemple

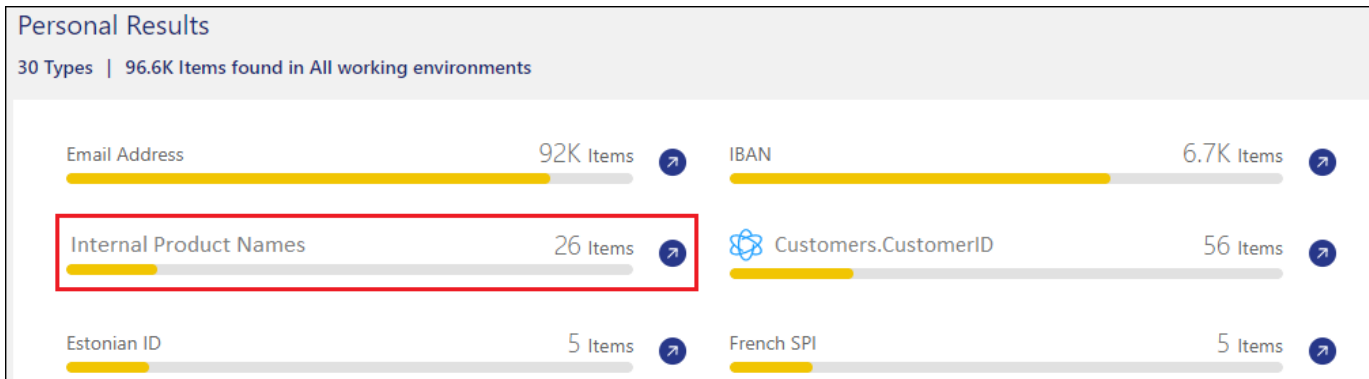
Pour voir où vos noms de produits internes sont mentionnés dans tous vos fichiers, entrez la commande suivante.

```
[user ~]$ cd /opt/netapp/Datasense/  
[user Datasense]$ sudo bash  
tools/datascience/custom_keywords/upload_custom_keywords.sh -s activate -f  
internal_product_names.txt
```

```
log v1.0 | 2022-08-24 08:16:25,332 | INFO | ds_logger |  
upload_custom_keywords | 126 | 1 | None | upload_custom_keywords_126 | All  
legal keywords were successfully inserted
```

.Résultats

Après l'analyse suivante, les résultats incluent ces nouvelles informations dans le tableau de bord de conformité sous la section « Résultats personnels » et dans la page Investigation du filtre « données personnelles ».



Comme vous pouvez le voir, le nom du fichier texte est utilisé comme nom dans le panneau des résultats personnels. De cette manière, vous pouvez activer des mots-clés à partir de différents fichiers texte et voir les résultats pour chaque type de mot-clé.

Désactiver les mots clés personnalisés

Si vous décidez ultérieurement que vous n'avez pas besoin de détection de données pour identifier certains mots-clés personnalisés que vous avez ajoutés précédemment, utilisez l'option **deactivate** de la commande pour supprimer les mots-clés qui sont définis dans le fichier texte.

```
sudo bash tools/datascience/custom_keywords/upload_custom_keywords.sh -s deactivate -f <file_name>.txt
```

Par exemple, pour supprimer les mots clés définis dans le fichier

```
*Internal_PRODUCT_Names.txt* :
```

```
[user ~]$ cd /opt/netapp/Datasense/  
[user Datasense]$ sudo bash  
tools/datascience/custom_keywords/upload_custom_keywords.sh -s deactivate  
-f internal_product_names.txt
```

```
log v1.0 | 2022-08-24 08:16:25,332 | INFO | ds_logger |  
upload_custom_keywords | 87 | 1 | None | upload_custom_keywords_87 |  
Deactivated keyword pattern from internal_product_names.txt successfully
```

Ajoutez des identificateurs de données personnelles personnalisés à l'aide d'un regex

Vous pouvez ajouter un modèle personnel pour identifier des informations spécifiques dans vos données à l'aide d'une expression régulière personnalisée (regex). Le regex est ajouté aux modèles prédéfinis que Data Sense utilise déjà et les résultats seront visibles sous la section motifs personnels.

Par exemple, vous pouvez voir où vos ID de produit internes sont mentionnés dans tous vos fichiers. Si l'ID de produit a une structure claire, par exemple, il s'agit d'un numéro à 12 chiffres commençant par 201, vous pouvez utiliser la fonction regex personnalisée pour la rechercher dans vos fichiers.

Après avoir ajouté la fenêtre regex, Data Sense redémarre l'acquisition de toutes les sources de données ; les nouveaux résultats apparaissent dans le message logique de données une fois l'analyse terminée.

Syntaxe de commande pour ajouter le regex

Vous devrez accéder au système Data Sense pour ajouter le fichier contenant les modèles de mots-clés personnalisés et lancer la commande pour ajouter les mots-clés personnalisés. [Voir comment accéder à la ligne de commande](#) Que vous ayez installé Data Sense dans votre site ou dans le cloud.

La syntaxe de commande permettant d'ajouter un regex personnalisé est la suivante :

```
sudo bash tools/datascience/custom_regex/custom_regex.sh -s activate -n
"<pattern_name>" -r "<regular_expression>"
* <nom_modèle> = nom qui apparaîtra dans l'interface utilisateur de
détection de données. Assurez-vous que le nom identifie ce que le regex
est conçu pour trouver. Le nom doit contenir au moins une lettre et peut
comporter jusqu'à 70 caractères.
* <Regular_expression> = ce peut être n'importe quelle expression
régulière légale.
```

Vous exécutez la commande à partir du chemin **/opt/netapp/Datase/**.

Notez que nous testons chaque nouveau regex pour vérifier s'il est trop large et qu'il renverrait trop de correspondances. Si c'est le cas, le message suivant apparaît :

```
log v1.0 | 2022-08-17 07:24:19,585 | ERROR | ds_logger | custom_regex |
119 | 1 | None | custom_regex_119 | The regex has high risk to identify
false positives. Please narrow the regular expression and try again. To
add it anyway, use the force flag (-f) at the end
Vous pouvez utiliser l'option *-f* à la fin de la ligne de commande si
vous voulez ajouter avec force le regex à Data Sense - même si nous
pensons qu'il est trop large.
```

Exemple

L'ID du produit est un numéro à 12 chiffres commençant par 201 ; l'expression régulière est donc **\b201\d{9}\b**. Et vous voulez que le texte de l'interface utilisateur de détection de données identifie ce modèle comme **ID produit interne**.

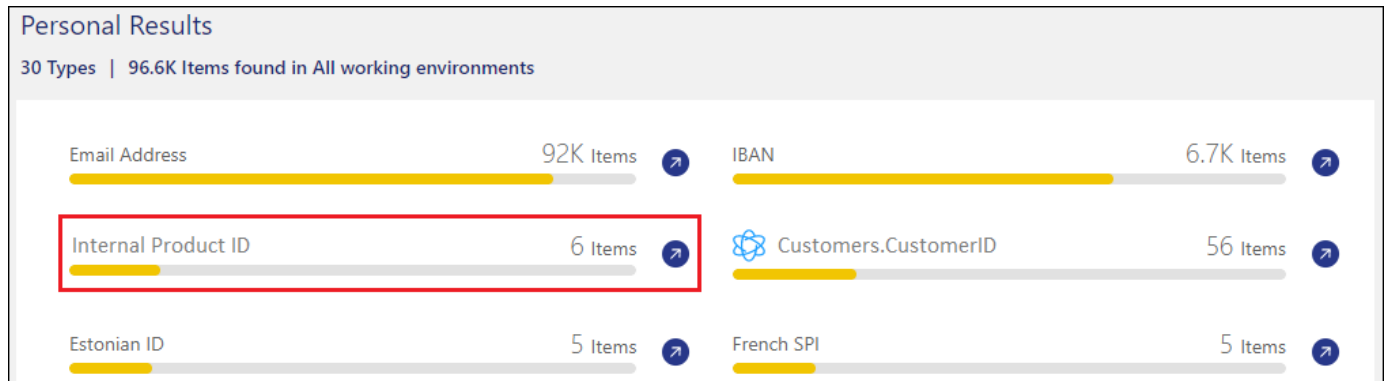
Pour voir où vos ID de produit internes sont mentionnés dans tous vos fichiers, entrez les commandes suivantes.

```
[user ~]$ cd /opt/netapp/Datasense/
[user Datasense]$ sudo bash tools/datascience/custom_regex/custom_regex.sh
-s activate -n "Internal Product ID" -r "\b201\d{9}\b"
```

```
[+] Adding Custom Regex to Data Sense
log v1.0 | 2022-08-23 13:19:01,476 | INFO | ds_logger | custom_regex | 154
| 1 | None | custom_regex_154 | A pattern named 'Internal Product ID' was
added successfully to Data Sense
```

Résultats

Après l'analyse suivante, les résultats incluent ces nouvelles informations dans le tableau de bord de conformité sous la section « Résultats personnels » et dans la page Investigation du filtre « données personnelles ».



Désactivez un regex personnalisé

Si vous décidez ultérieurement que vous n'avez pas besoin de détection de données pour identifier les modèles personnalisés que vous avez entrés en tant que regex, utilisez l'option **deactivate** de la commande pour supprimer chaque regex.

```
sudo bash tools/datascience/custom_regex/custom_regex.sh -s deactivate -n
"<pattern name>"
Par exemple, pour supprimer le * ID produit interne* regex :
```

```
[user ~]$ cd /opt/netapp/Datasense/
[user Datasense]$ sudo bash tools/datascience/custom_regex/custom_regex.sh
-s deactivate -n "Internal Product ID"
```

```
log v1.0 | 2022-08-17 09:13:15,431 | INFO | ds_logger | custom_regex | 31
| 1 | None | custom_regex_31 | A pattern named 'Internal Product ID' was
deactivated successfully
```

Affichage de l'état de vos actions de conformité

Lorsque vous exécutez une action à partir du volet Résultats de l'enquête sur de nombreux fichiers, par exemple la suppression de 100 fichiers, le processus peut prendre

un certain temps. Vous pouvez surveiller l'état de ces actions asynchrones dans le volet *action Status* pour savoir quand elles ont été appliquées à tous les fichiers.

Cela vous permet de voir les actions effectuées avec succès, celles en cours et celles qui ont échoué pour diagnostiquer et résoudre tout problème.

Le statut peut être :

- Terminé
- En cours
- En file d'attente
- Annulée
- Échec

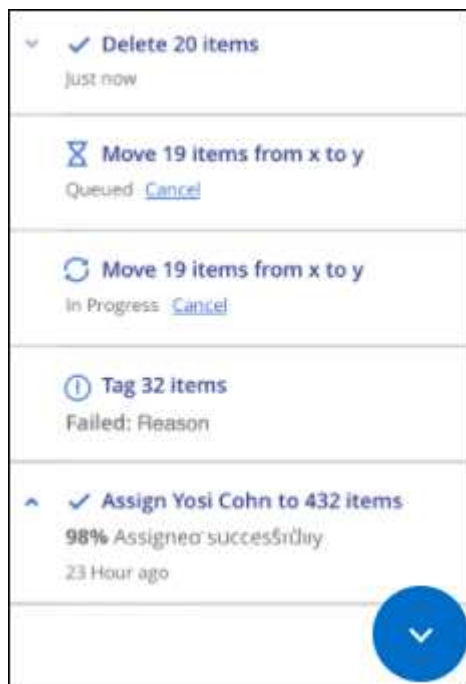
Notez que vous pouvez annuler toutes les actions ayant le statut « en attente » ou « en cours ».

Étapes

1. Dans le coin inférieur droit de l'interface utilisateur de détection de données, vous pouvez voir le bouton



2. Cliquez sur ce bouton et les 20 actions les plus récentes sont répertoriées.



Vous pouvez cliquer sur le nom d'une action pour afficher les détails correspondant à cette opération.

Audit de l'historique des actions de détection de données

Data Sense consigne les activités de gestion qui ont été effectuées sur des fichiers de tous les environnements de travail et des sources de données que Data Sense est en

train d'analyser. Vous pouvez afficher le contenu des fichiers journaux d'audit de détection de données ou les télécharger pour voir quels changements de fichier ont eu lieu, et quand.

Par exemple, vous pouvez voir quelle demande a été émise, l'heure de la demande et des détails tels que l'emplacement source en cas de suppression d'un fichier ou l'emplacement source et de destination en cas de déplacement d'un fichier.

Contenu du fichier journal

Chaque ligne du journal d'audit contient des informations dans ce format :

```
<full date> | <status> | ds_audit_logger | <module> | 0 | 0 | File <full file path> deleted from device <device path> - <result>
```

- Date et heure : horodatage complet de l'événement
- État - INFO, AVERTISSEMENT
- Type d'action (supprimer, copier, déplacer, créer la stratégie, mettre à jour la stratégie, Analyse des fichiers, téléchargement du rapport JSON, etc.)
- Nom du fichier (si l'action est pertinente pour un fichier)
- Détails de l'action - ce qui a été fait : dépend de l'action
 - Nom de la règle
 - Pour déplacer - Source et destination
 - Pour la copie - Source et destination
 - Pour balise - nom de balise
 - Pour attribuer à - nom d'utilisateur
 - Pour une alerte par e-mail : adresse e-mail/compte

Par exemple, les lignes suivantes du fichier journal indiquent une opération de copie réussie et une opération de copie ayant échoué.

```
2022-06-06 15:23:08,910 | INFO | ds_audit_logger | es_scanned_file | 237 | 49 | Copy file /CIFS_share/data/dop1/random_positives.tsv from device 10.31.133.183 (type: SMB_SHARE) to device 10.31.130.133:/export_reports (NFS_SHARE) - SUCCESS
2022-06-06 15:23:08,968 | WARNING | ds_audit_logger | es_scanned_file | 239 | 153 | Copy file /CIFS_share/data/compliance-netapp.tar.gz from device 10.31.133.183 (type: SMB_SHARE) to device 10.31.130.133:/export_reports (NFS_SHARE) - FAILURE
```

Accès au fichier journal

Les fichiers journaux d'audit se trouvent sur la machine Data Sense dans : `/opt/netapp/audit_logs/`

Chaque fichier journal peut avoir une taille maximale de 10 Mo. Lorsque cette limite est atteinte, un nouveau fichier journal démarre. Les fichiers journaux sont nommés « DataSense_audit.log », « DataSense_audit.log.1 »

», « DataSense_audit.log.2 », etc. Un maximum de 100 fichiers journaux sont conservés sur le système. Les anciens fichiers journaux sont supprimés automatiquement une fois le maximum atteint.

Lorsque Data Sense est installé sur votre site, vous pouvez naviguer directement vers le fichier journal.

Lorsque Data Sense est déployé dans le cloud, vous devez utiliser SSH vers l'instance Data Sense. Vous vous connectez au système en saisissant l'utilisateur et le mot de passe, ou en utilisant la clé SSH fournie lors de l'installation du connecteur BlueXP. La commande SSH est :

```
ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
* <path_to_the_ssh_key> = emplacement des clés d'authentification ssh
* <machine_utilisateur> :
```

+

Pour AWS : utilisez <utilisateur ec2>

Pour Azure : utilisez l'utilisateur créé pour l'instance BlueXP

** Pour GCP : utilisez l'utilisateur créé pour l'instance BlueXP

- <datasense_ip> = adresse IP de l'instance de la machine virtuelle

Notez que vous devrez modifier les règles entrantes du groupe de sécurité pour accéder au système dans le cloud. Pour plus de détails, voir :

- ["Règles de groupe de sécurité dans AWS"](#)
- ["Règles de groupe de sécurité dans Azure"](#)
- ["Règles de pare-feu dans Google Cloud"](#)

Réduction de la vitesse d'acquisition de détection de données

L'analyse des données a un impact négligeable sur vos systèmes de stockage et sur vos données. Cependant, si vous êtes préoccupé par un impact même très faible, vous pouvez configurer Data Sense pour effectuer des acquisitions « lentes ».

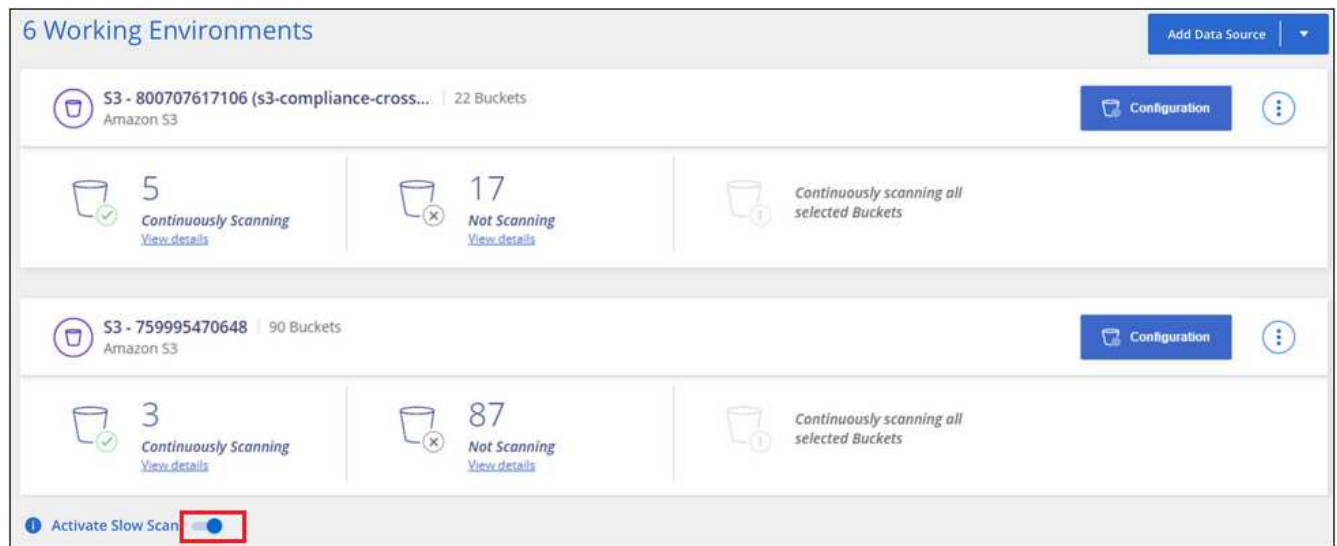
Lorsqu'elle est activée, l'analyse lente est utilisée sur toutes les sources de données ; vous ne pouvez pas configurer la numérisation lente pour un environnement de travail unique ou une source de données.



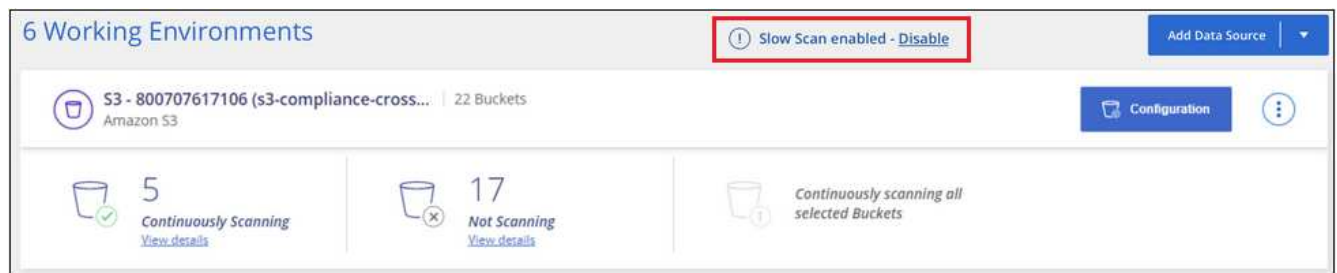
La vitesse de numérisation ne peut pas être réduite lors de la numérisation de bases de données.

Étapes

1. Depuis le bas de la *Configuration* page, déplacez le curseur vers la droite pour activer la numérisation lente.



Le haut de la page Configuration indique que la numérisation lente est activée.




2. Vous pouvez désactiver la numérisation lente en cliquant sur **Désactiver** dans ce message.

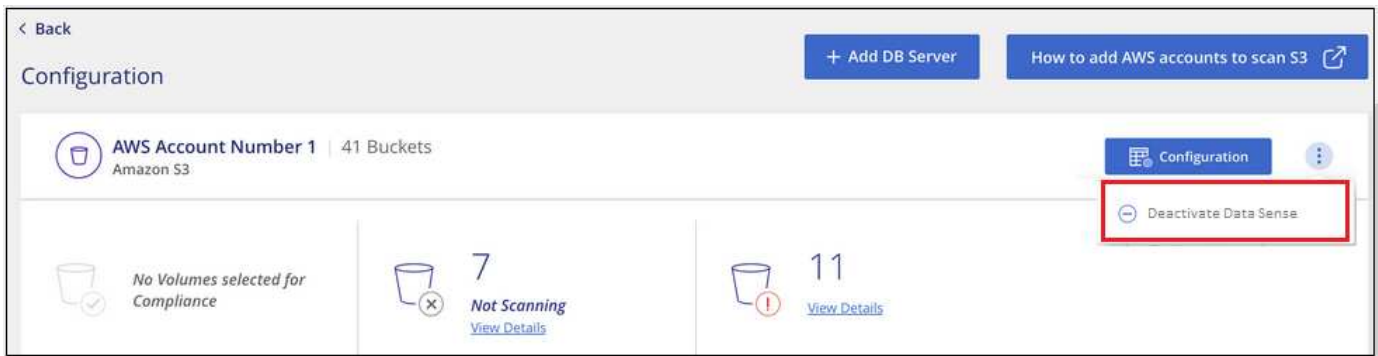
Suppression des sources de données du cloud au bon sens

Si nécessaire, vous pouvez arrêter l'analyse de Cloud Data SENSE pour un ou plusieurs environnements de travail, bases de données, groupes de partage de fichiers, comptes OneDrive, comptes Google Drive, Ou des comptes SharePoint.

Désactivation des analyses de conformité pour un environnement de travail

Lorsque vous désactivez les analyses, Cloud Data SENSE ne analyse plus les données de l'environnement de travail et supprime les informations de conformité indexées de l'instance Data Sense (les données de l'environnement de travail lui-même ne sont plus supprimées).

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



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

Suppression d'une base de données du Cloud Data SENSE

Si vous ne souhaitez plus scanner une certaine base de données, vous pouvez la supprimer de l'interface Cloud Data SENSE et arrêter toutes les analyses.


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



Suppression d'un compte OneDrive, SharePoint ou Google Drive de Cloud Data Sense

Si vous ne souhaitez plus analyser les fichiers utilisateur d'un compte OneDrive spécifique, d'un compte SharePoint spécifique ou d'un compte Google Drive, vous pouvez supprimer ce compte de l'interface Cloud Data Sense et arrêter toutes les analyses.

Étapes

1. Dans la page *Configuration*, cliquez sur  Dans la ligne du compte OneDrive, SharePoint ou Google Drive, puis cliquez sur **Supprimer le compte OneDrive**, **Supprimer le compte SharePoint** ou **Supprimer le compte Google Drive**.




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

Suppression d'un groupe de partages de fichiers du Cloud Data Sense

Si vous ne souhaitez plus analyser les fichiers utilisateur d'un groupe de partages de fichiers, vous pouvez supprimer le groupe de partages de fichiers de l'interface Cloud Data Sense et arrêter toutes les analyses.

Étapes

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



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

Désinstallation de Cloud Data SENSE

Vous pouvez désinstaller le logiciel Data Sense pour résoudre des problèmes ou supprimer définitivement le logiciel de l'hôte. La suppression de l'instance supprime également les disques associés où résident les données indexées - toutes les informations que Data Sense a numérisées seront définitivement supprimées.

Les étapes à suivre dépendent du déploiement de Data Sense dans le cloud ou sur un hôte sur site.

Désinstaller Data Sense à partir d'un déploiement dans le cloud

Vous pouvez désinstaller et supprimer l'instance Cloud Data Sense du fournisseur cloud si vous ne souhaitez plus utiliser Data Sense.

1. En haut de la page détection de données, cliquez sur  Puis cliquez sur **Désinstaller Data SENSE**.




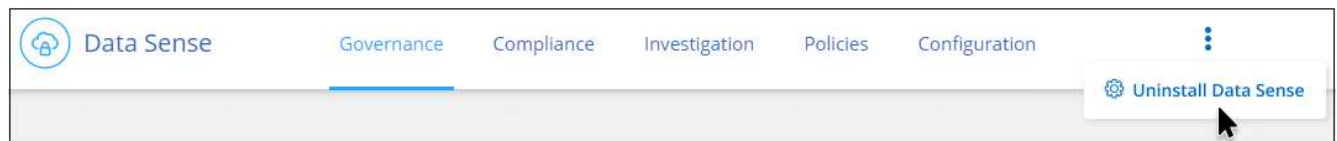
2. Dans la boîte de dialogue *Uninstall Data Sense*, tapez **uninstall** pour confirmer que vous souhaitez supprimer l'instance et toutes les données associées, puis cliquez sur **Uninstall**.

Vous pouvez aussi accéder à la console de votre fournisseur cloud et supprimer l'instance Cloud Data SENSE. L'instance s'appelle *CloudCompliance* avec un hachage (UUID) généré concaténé. Par exemple : *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

Désinstaller Data Sense d'un déploiement sur site

Vous pouvez désinstaller Data Sense à partir d'un hôte si vous ne souhaitez plus utiliser Data Sense ou si vous avez rencontré un problème nécessitant une réinstallation.

1. En haut de la page détection de données, cliquez sur  Puis cliquez sur **Désinstaller Data SENSE**.



2. Dans la boîte de dialogue *Uninstall Data SENSE*, tapez **uninstall** pour confirmer que vous souhaitez effacer toutes les informations de configuration, puis cliquez sur **Uninstall**.
3. Pour terminer la désinstallation depuis l'hôte, exécutez le script de désinstallation sur la machine hôte, par exemple :

```
uninstall.sh
```

Informations sur le copyright

Copyright © 2022 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 DÉLICTELLE (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.