



# Gérer la classification BlueXP

## BlueXP classification

NetApp  
April 03, 2024

# Sommaire

- Gérer la classification BlueXP ..... 1
  - Ajoutez des identifiants de données personnels à vos analyses de classification BlueXP ..... 1
  - Excluez des répertoires spécifiques des analyses de classification BlueXP ..... 16
  - Affichage de l'état de vos actions de conformité ..... 19
  - Définissez des ID de groupe supplémentaires comme ouverts à l'organisation ..... 20
  - Vérifiez l'historique des actions de classification BlueXP ..... 21
  - Réduction de la vitesse d'analyse de la classification BlueXP ..... 23
  - Suppression des sources de données de la classification BlueXP ..... 24
  - Désinstallation de la classification BlueXP ..... 26

# Gérer la classification BlueXP

## Ajoutez des identifiants de données personnels à vos analyses de classification BlueXP

La classification BlueXP offre de nombreuses façons d'ajouter une liste personnalisée des « données personnelles » que la classification BlueXP identifiera dans les analyses futures. Vous disposez ainsi d'une vue d'ensemble sur l'emplacement des données potentiellement sensibles dans *tous* les fichiers de votre entreprise.

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

Tous ces mécanismes pour ajouter des critères de numérisation personnalisés sont pris en charge dans toutes les langues.



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

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

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

## 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
```

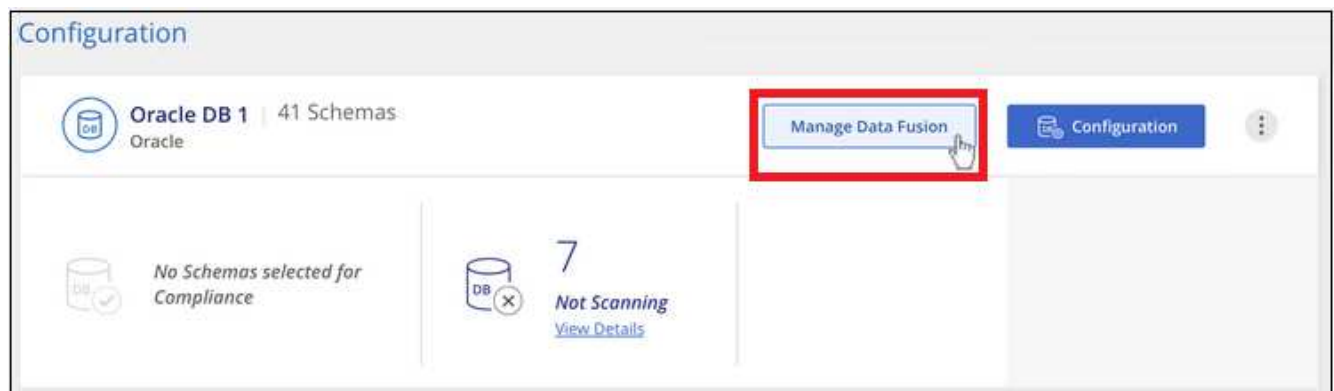
Comme vous pouvez le voir, deux ID de client uniques ont été trouvés sur deux volumes et dans un compartiment S3. Toutes les correspondances dans les tables de base de données seront également identifiées.

Notez que, puisque vous scannez vos propres bases de données, quelle que soit la langue dans laquelle vos données sont stockées, elles seront utilisées pour identifier les données lors des futures analyses de classification BlueXP.

### Étapes

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

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



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

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

- 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

Table

Oracle1,Accounts

Customers

Columns Containing Identifiers ⓘ

Customer ID

Add Data Fusion Source

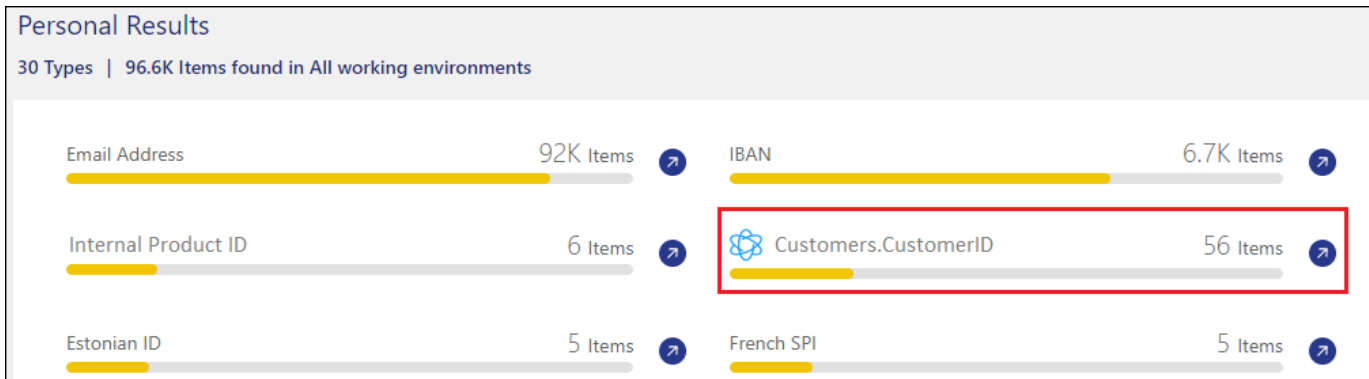
Cancel

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

Oracle DB 1 Data Fusion			<a href="#">+ Add Data Fusion source</a>
With Data Fusion, Data Sense can identify occurrences of your organization's unique identifiers found in your unstructured data stores, using structured data indexes containing those unique identifiers as a source reference. <a href="#">Learn More</a>			
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	...

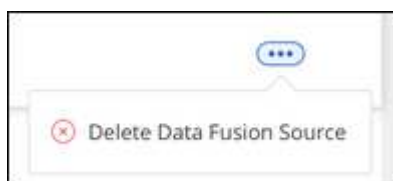
## Résultats

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 ». Le nom que vous avez utilisé pour le classificateur apparaît dans la liste de filtres, par exemple `Customers.CustomerID`.



## Supprimer une source de Data Fusion

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



## Ajoutez des mots clés personnalisés à partir d'une liste de mots

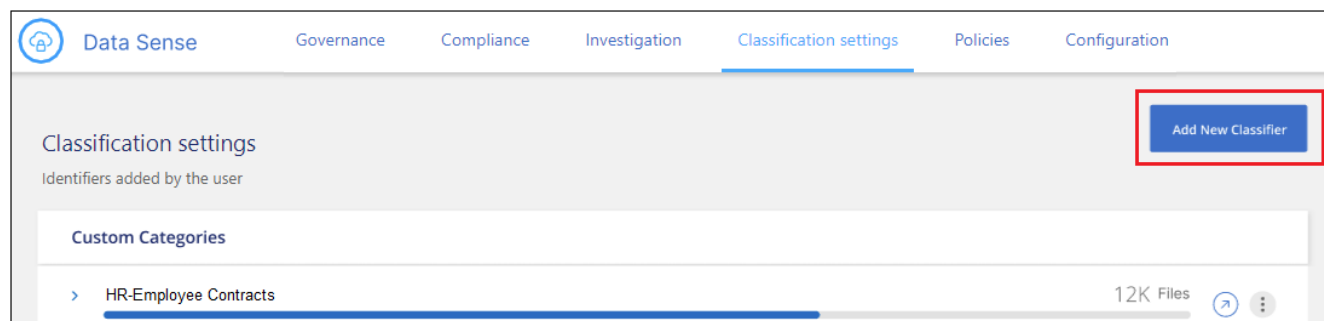
Vous pouvez ajouter des mots-clés personnalisés à la classification BlueXP pour identifier l'emplacement où se trouvent les informations. Pour ajouter ces mots-clés, entrez simplement les mots que vous souhaitez que la classification BlueXP reconnaisse. Les mots-clés sont ajoutés aux mots-clés prédéfinis que la classification BlueXP utilise déjà et les résultats sont visibles dans la section modèles personnels.

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

Après la mise à jour des mots-clés personnalisés, la classification BlueXP redémarre l'analyse de toutes les sources de données. Une fois l'analyse terminée, les nouveaux résultats apparaissent dans le tableau de bord de conformité de classification BlueXP, dans la section « Résultats personnels », et dans la page Investigation du filtre « données personnelles ».

### Étapes

1. Dans l'onglet *Paramètres de classification*, cliquez sur **Ajouter un nouveau classificateur** pour lancer l'assistant *Ajouter un classificateur personnalisé*.



2. Dans la page *Select type*, entrez le nom du classificateur, fournissez une brève description, sélectionnez **Personal identifier**, puis cliquez sur **Next**.

Le nom que vous entrez s'affiche dans l'interface de classification BlueXP en tant qu'en-tête pour les fichiers numérisés qui correspondent aux exigences du classificateur et en tant que nom du filtre dans la page Investigation.

Vous pouvez également cocher la case « Masquer les résultats détectés dans le système » pour que le résultat complet n'apparaisse pas dans l'interface utilisateur. Par exemple, vous pouvez vouloir le faire pour masquer les numéros de carte de crédit complets ou des données personnelles similaires (le masque apparaîtra dans l'interface utilisateur comme ceci: "Pass:[\*\*] \*\*\*\* \* 3434").

1 Select type    2 Select tool    3 Create Logic

## Select type

Select the type of classifier that you want to add to the system, and provide the name and description. Data Sense re-scans all your data sources after you add a new classifier. When the scan is complete, all matching results are displayed in the "Classification Settings" dashboard and in other Data Sense pages.

Classifier name

Internal Product Names

Description

Identify internal product names found in all files

☒ **Personal identifier**

The classifier will be added to the system as a new personal identifier. Any matches are considered "personal data", and they are added to the results that are displayed in the Personal Results page and in the Investigation page. [See the list of personal data that Data Sense identifies by default.](#)

☐ Mask detected results in the system

☐ **Category**

The classifier will be added to the system as a new Category. Any matches are added to the results that are displayed in the Categories page and in the Investigation page. [See the list of categories that Data Sense identifies by default.](#)

Previous    Next

3. Dans la page *Select Data Analysis Tool*, sélectionnez **Custom Keywords** comme méthode à utiliser pour définir le classificateur, puis cliquez sur **Next**.

## Select Data Analysis Tool

Select the tool that will be used to build the list of words, or patterns, that Data Sense will attempt to match in your data sources.

☒

**Custom keywords** ⓘ  
Create a custom personal pattern based on a list of keywords that you provide.

☐

**Custom regular expression** ⓘ  
Create a custom personal pattern based on a regular expression that you define.

☐

**DB fusion** ⓘ  
Create a custom personal pattern based on the values found in specific columns in your scanned database tables. This allows you to identify whether unique identifiers from your databases are found in any of your other data sources.

Previous

Next

4. Dans la page *Create Logic*, entrez les mots-clés que vous voulez reconnaître - chaque mot sur une ligne séparée - et cliquez sur **Validate**.

La capture d'écran ci-dessous montre les noms de produits internes (différents types de wls). La recherche de classification BlueXP pour ces éléments n'est pas sensible à la casse.



## Create Logic

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

---

### Custom keywords list <sup>1</sup>

- Maximum of 100,000 words.
- Separate between keywords with a new line
- The keywords are not case sensitive
- Each word must be at least 3 characters long. Shorter words are ignored.
- Duplicate words are only added once.

barred  
barn  
horned  
snowy  
screech

Validate

✔ Keywords list is **valid**.

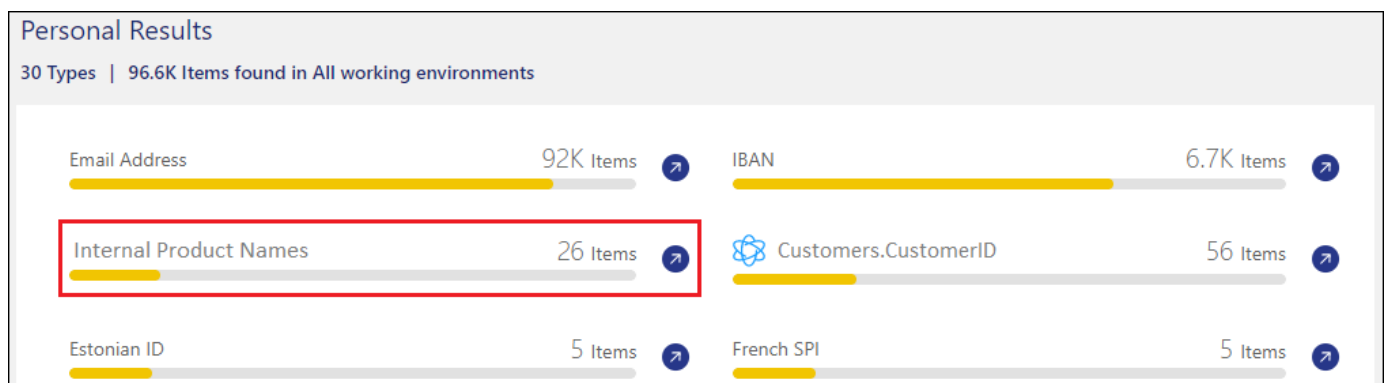
Previous

Done

5. Cliquez sur **terminé** et la classification BlueXP commence à analyser à nouveau vos données.

### Résultats

Une fois l'analyse terminée, les résultats incluront ces nouvelles informations dans le tableau de bord de conformité sous la section « Résultats personnels » et dans la page enquête du filtre « données personnelles ».



Comme vous pouvez le voir, le nom du classificateur est utilisé comme nom dans le panneau Résultats personnels. De cette manière, vous pouvez activer de nombreux groupes de mots-clés et voir les résultats pour chaque groupe.

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

Vous pouvez ajouter un modèle personnel pour identifier des informations spécifiques dans vos données à l'aide d'une expression régulière personnalisée (regex). Cela vous permet de créer un nouveau regex personnalisé pour identifier de nouveaux éléments d'informations personnelles qui n'existent pas encore dans le système. Le regex est ajouté aux modèles prédéfinis existants que la classification BlueXP utilise déjà, et les résultats seront visibles dans la section modèles personnels.

Par exemple, vous pouvez voir où vos ID de produit internes sont mentionnés dans tous vos fichiers. Si l'ID de produit a une structure claire, par exemple, il s'agit d'un numéro à 12 chiffres commençant par 201, vous pouvez utiliser la fonction regex personnalisée pour la rechercher dans vos fichiers. L'expression régulière de cet exemple est `\b201\d{9}\b`.

Une fois le regex ajouté, la classification BlueXP redémarre l'analyse de toutes les sources de données. Une fois l'analyse terminée, les nouveaux résultats apparaissent dans le tableau de bord de conformité de classification BlueXP, dans la section « Résultats personnels », et dans la page Investigation du filtre « données personnelles ».

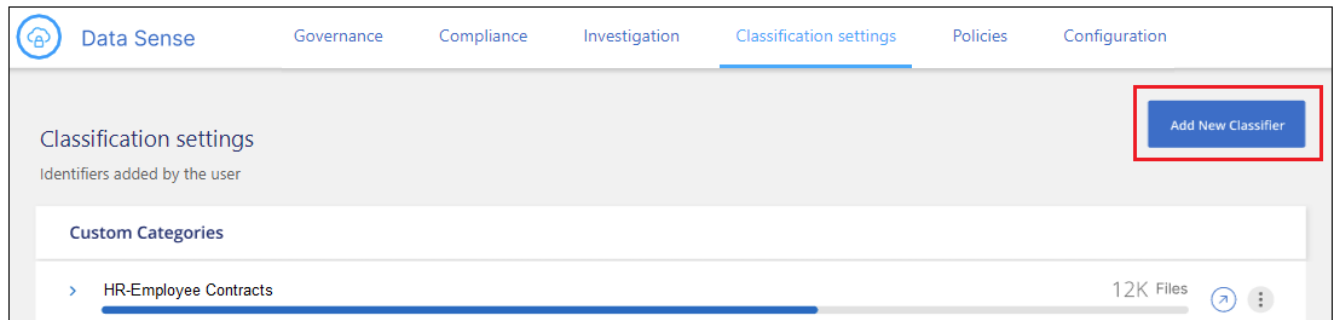
Si vous avez besoin d'aide pour construire l'expression régulière, reportez-vous à la section "[Expressions régulières 101](#)". Choisissez **Python** pour que la saveur puisse voir les types de résultats que la classification BlueXP correspond à l'expression régulière. Le "[Page Python Regex Tester](#)" est également utile en affichant une représentation graphique de vos répétitions.



Actuellement, nous n'autorisons pas l'utilisation d'indicateurs de motif lors de la création d'un regex - cela signifie que vous ne devez pas utiliser "/".

### Étapes

1. Dans l'onglet *Paramètres de classification*, cliquez sur **Ajouter un nouveau classificateur** pour lancer l'assistant *Ajouter un classificateur personnalisé*.



2. Dans la page *Select type*, entrez le nom du classificateur, fournissez une brève description, sélectionnez **Personal identifier**, puis cliquez sur **Next**.

Le nom que vous entrez s'affiche dans l'interface de classification BlueXP en tant qu'en-tête pour les fichiers numérisés qui correspondent aux exigences du classificateur et en tant que nom du filtre dans la page Investigation. Vous pouvez également cocher la case « Masquer les résultats détectés dans le système » pour que le résultat complet n'apparaisse pas dans l'interface utilisateur. Par exemple, vous pouvez vouloir le faire pour masquer les numéros complets de carte de crédit ou des données personnelles similaires.

1 Select type

2 Select tool

3 Create Logic

## Select type

Select the type of classifier that you want to add to the system, and provide the name and description. Data Sense re-scans all your data sources after you add a new classifier. When the scan is complete, all matching results are displayed in the "Classification Settings" dashboard and in other Data Sense pages.

---

Classifier name

Internal Product ID

Description

Identify internal product IDs found in all files

☒ **Personal identifier**  
The classifier will be added to the system as a new personal identifier. Any matches are considered "personal data", and they are added to the results that are displayed in the Personal Results page and in the Investigation page. [See the list of personal data that Data Sense identifies by default.](#)  
☐ Mask detected results in the system

☐ **Category**  
The classifier will be added to the system as a new Category. Any matches are added to the results that are displayed in the Categories page and in the Investigation page. [See the list of categories that Data Sense identifies by default.](#)

Previous

Next

3. Dans la page *Select Data Analysis Tool*, sélectionnez **Custom Regular expression** comme méthode à utiliser pour définir le classificateur, puis cliquez sur **Next**.

## Select Data Analysis Tool

Select the tool that will be used to build the list of words, or patterns, that Data Sense will attempt to match in your data sources.

☐

**Custom keywords** ⓘ  
Create a custom personal pattern based on a list of keywords that you provide.

☒

**Custom regular expression** ⓘ  
Create a custom personal pattern based on a regular expression that you define.

☐

**DB fusion** ⓘ  
Create a custom personal pattern based on the values found in specific columns in your scanned database tables. This allows you to identify whether unique identifiers from your databases are found in any of your other data sources.

Previous

Next

4. Dans la page *Create Logic*, entrez l'expression régulière et les mots de proximité, puis cliquez sur **Done**.
- Vous pouvez entrer n'importe quelle expression régulière légale. Cliquez sur le bouton **Valider** pour que la classification BlueXP vérifie que l'expression régulière est valide et qu'elle n'est pas trop large, ce qui signifie qu'elle renvoie trop de résultats.
  - Vous pouvez également saisir des mots de proximité pour vous aider à affiner la précision des résultats. Il s'agit de mots qui se trouvent généralement dans les 300 caractères du motif que vous recherchez (avant ou après le motif trouvé). Entrez chaque mot ou expression sur une ligne distincte.

## Create Logic

Create logic for the new identifier, based on regular expression and keywords that should be detected.

---

**Regular expression** ⓘ

Add the pattern that should be detected to identify specific information in your data, using a custom regular expression.

Validate

✓ **Success:** Regular expression is valid.

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

Previous Done

### Résultats

Le classificateur est ajouté et la classification BlueXP commence à analyser à nouveau toutes vos sources de données. Vous revenez à la page Classificateurs personnalisés où vous pouvez afficher le nombre de fichiers correspondant à votre nouveau classificateur. Les résultats de l'analyse de toutes vos sources de données prennent du temps en fonction du nombre de fichiers à numériser.

Data Sense Governance Compliance Investigation Classification settings Policies Configuration

Classification settings

Identifiers added by the user

Custom Categories

> HR - Employee Contracts 7.5K Files

Personal information

> Internal Product ID 12K Files

### Ajouter des catégories personnalisées

La classification BlueXP récupère les données qu'il analyse et les divise en différents types de catégories. Ces catégories sont des thèmes basés sur l'analyse par intelligence artificielle du contenu et des métadonnées de

chaque fichier. ["Voir la liste des catégories prédéfinies"](#).

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

Vous pouvez ajouter des catégories personnalisées à la classification BlueXP pour identifier où se trouvent les catégories d'informations spécifiques à votre patrimoine de données. Vous ajoutez chaque catégorie en créant des fichiers d'entraînement qui contiennent les catégories de données que vous souhaitez identifier, puis analysez ces fichiers pour les analyser par le biais de l'IA afin qu'il puisse identifier les données dans vos sources de données. Les catégories sont ajoutées aux catégories prédéfinies existantes identifiées par la classification BlueXP et les résultats sont visibles dans la section catégories.

Par exemple, vous pouvez voir où se trouvent les fichiers d'installation compressés au format .gz dans vos fichiers afin que vous puissiez les supprimer, si nécessaire.

Après la mise à jour des catégories personnalisées, la classification BlueXP redémarre l'analyse de toutes les sources de données. Une fois l'analyse terminée, les nouveaux résultats apparaissent dans le tableau de bord de conformité de classification BlueXP sous la section « catégories » et dans la page Investigation du filtre « Catégorie ». ["Voir comment afficher les fichiers par catégories"](#).

### Ce dont vous avez besoin

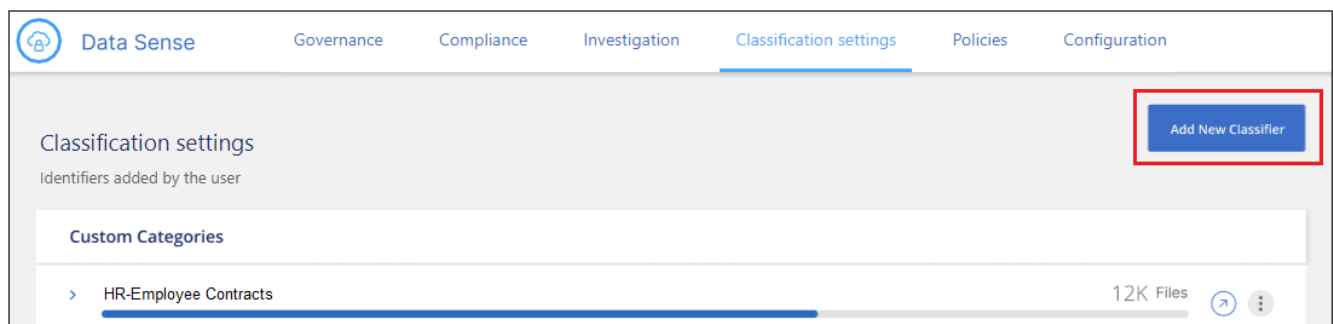
Vous devez créer au moins 25 fichiers d'entraînement contenant des échantillons des catégories de données que vous voulez que la classification BlueXP reconnaisse. Les types de fichiers suivants sont pris en charge :

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

Les fichiers doivent être d'au moins 100 octets et doivent se trouver dans un dossier accessible par la classification BlueXP.

### Étapes

1. Dans l'onglet *Paramètres de classification*, cliquez sur **Ajouter un nouveau classificateur** pour lancer l'assistant *Ajouter un classificateur personnalisé*.



2. Dans la page *Select type*, entrez le nom du classificateur, fournissez une brève description, sélectionnez **Catégorie**, puis cliquez sur **Suivant**.

Le nom que vous entrez s'affiche dans l'interface de classification BlueXP en tant qu'en-tête des fichiers numérisés correspondant à la catégorie de données que vous définissez, et en tant que nom du filtre dans la page Investigation.

1 Select type
2 Select tool
3 Create Logic

## Select type

Select the type of classifier that you want to add to the system, and provide the name and description. Data Sense re-scans all your data sources after you add a new classifier. When the scan is complete, all matching results are displayed in the "Classification Settings" dashboard and in other Data Sense pages.

Classifier name

Description

☐ **Personal identifier**  
The classifier will be added to the system as a new personal identifier. Any matches are considered "personal data", and they are added to the results that are displayed in the Personal Results page and in the Investigation page. [See the list of personal data that Data Sense identifies by default.](#)  
☐ Mask detected results in the system

☒ **Category**  
The classifier will be added to the system as a new Category. Any matches are added to the results that are displayed in the Categories page and in the Investigation page. [See the list of categories that Data Sense identifies by default.](#)

Previous
Next

- Dans la page *Créer logique*, assurez-vous que les fichiers d'apprentissage sont préparés, puis cliquez sur **Sélectionner les fichiers**.

## Create Logic

**AI-based similarity training** ⓘ

- Insert NFS folder path
- The folder should contain minimum 25 files and maximum 1000 files that will be used for the AI training.
- Supported file types: pdf, docx, doc, pptx, xls,xlsx, csv, txt, gz, rtf, docs, sheets, slides, json
- The keywords are not case sensitive
- Minimum file size: 100B

Compressed Installer files

- Entrez l'adresse IP du volume et le chemin où se trouvent les fichiers de formation, puis cliquez sur **Ajouter**.

**Insert folder path that contains at least 25 files for the training**

Enter the IP address and volume name, along with the path to the location of the training files.

IP:

Training Data - Folder path:

**Add** **Cancel**

5. Vérifiez que les fichiers d'entraînement ont été reconnus par la classification BlueXP. Cliquez sur **x** pour supprimer tous les fichiers de formation qui ne répondent pas aux exigences. Cliquez ensuite sur **terminé**.

**Create Logic**

**AI-based similarity training**

- Insert NFS folder path
- The folder should contain minimum 25 files and maximum 1000 files that will be used for the AI training.
- Supported file types: pdf, docx, doc, pptx, xls, xlsx, csv, txt, gz, rtf, docs, sheets, slides, json
- The keywords are not case sensitive
- Minimum file size: 100B

[Select Files](#)

**Compressed Installer files**

Total uploaded files: 54

File name	File Size	File Type	Reliability	included in training
File1	56	File type	Sufficient	x
File2	22	File type	Sufficient	x
File3	43	File type	Sufficient	x
File4	11	File type	Sufficient	x

**Previous** **Done**

## Résultats

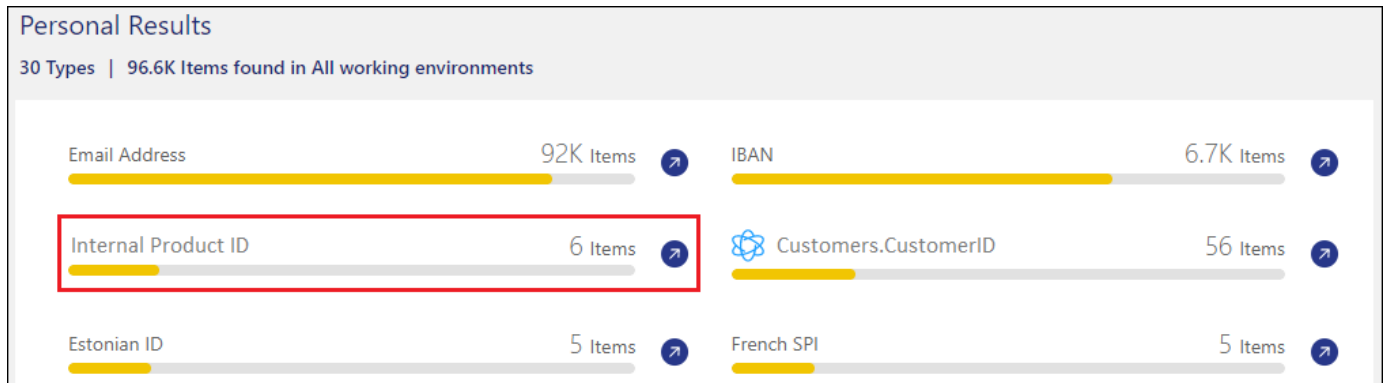
La nouvelle catégorie est créée telle que définie par les fichiers d'entraînement et ajoutée à la classification BlueXP. La classification BlueXP commence ensuite à analyser à nouveau toutes vos sources de données pour identifier les fichiers qui s'intègrent à cette nouvelle catégorie. Vous êtes renvoyé à la page Classifications personnalisées où vous pouvez afficher le nombre de fichiers correspondant à votre nouvelle catégorie. Les résultats de l'analyse de toutes vos sources de données prennent du temps en fonction du nombre de fichiers à numériser.

## Afficher les résultats de vos classificateurs personnalisés

Vous pouvez afficher les résultats de n'importe lequel de vos classificateurs personnalisés dans le tableau de

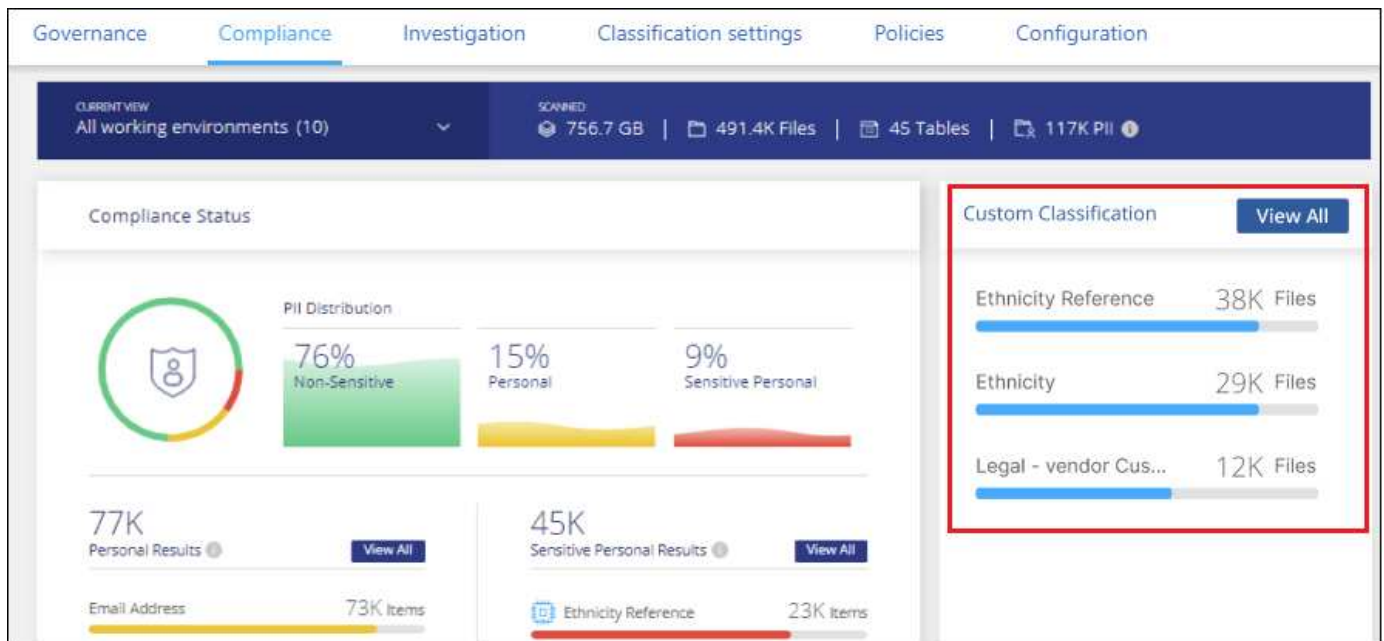


bord de conformité et dans la page Investigation. Par exemple, cette capture d'écran affiche les informations correspondantes dans le tableau de bord de conformité, sous la section « Résultats personnels ».



Cliquez sur le bouton  Pour afficher les résultats détaillés dans la page Investigation.

En outre, tous les résultats de votre classificateur personnalisé apparaissent dans l'onglet Classificateurs personnalisés, et les 6 meilleurs résultats de classificateur personnalisé sont affichés dans le tableau de bord de conformité, comme illustré ci-dessous.



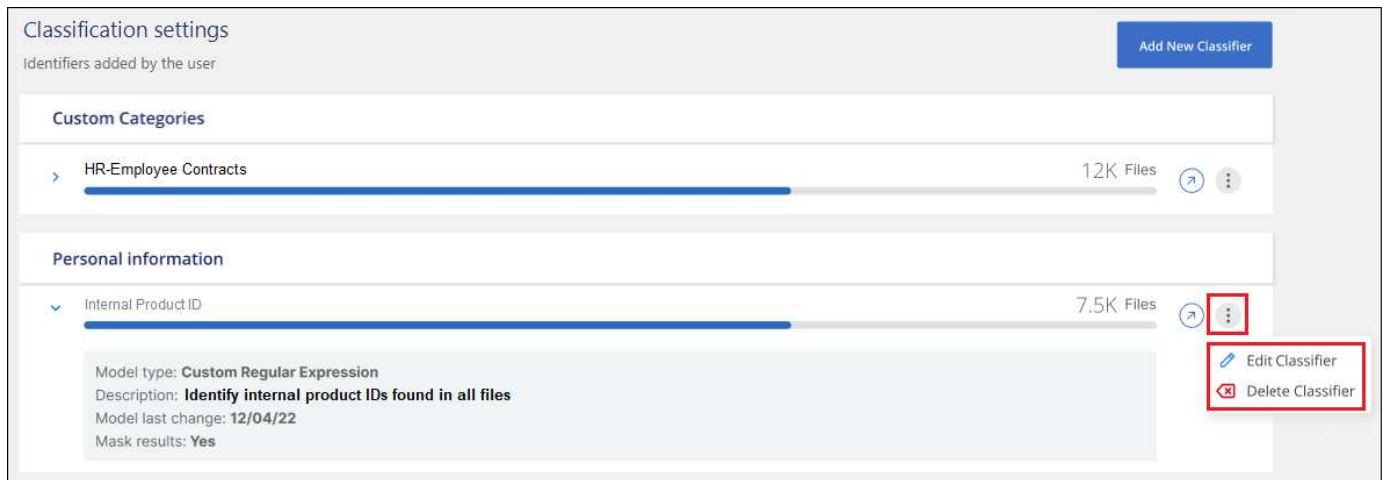
## Gérer les classificateurs personnalisés

Vous pouvez modifier n'importe lequel des classificateurs personnalisés que vous avez créés à l'aide du bouton **Edit Classificateur**.



Vous ne pouvez pas modifier les classificateurs Data Fusion pour le moment.

Et si vous décidez ultérieurement que vous n'avez pas besoin de la classification BlueXP pour identifier les modèles personnalisés que vous avez ajoutés, vous pouvez utiliser le bouton **Supprimer le classificateur** pour supprimer chaque élément.



## Excluez des répertoires spécifiques des analyses de classification BlueXP

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

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

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

### Sources de données prises en charge

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

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

### Définissez les répertoires à exclure de l'analyse

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



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

## Étapes

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

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

Ne modifiez rien d'autre dans ce fichier.

3. Enregistrez les modifications apportées au fichier.
4. Accédez à « /opt/netapp/Datasense/Tools/customer\_configuration/Data\_providers » et exécutez le script suivant :

```
update_data_providers_from_config_file.sh
```

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

## Résultat

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

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

## Exemples

### Configuration 1 :

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

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

### Résultats attendus pour les chemins qui seront exclus :

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

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

**Exemples de chemins qui ne seront pas exclus :**

- /CVO1/\*dossier
- /CVO1/foldername
- /CVO22/\*folder20

**Configuration 2 :**

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

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

**Résultats attendus pour les chemins qui seront exclus :**

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

**Exemples de chemins qui ne seront pas exclus :**

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

**Configuration 3 :**

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

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

**Résultats attendus pour les chemins qui seront exclus :**

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

**Exemples de chemins qui ne seront pas exclus :**

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

## Des caractères spéciaux s'échappant dans les noms de dossier

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

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

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

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

## Afficher la liste d'exclusion actuelle

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

```
get_data_providers_configuration.sh
```

## Affichage de l'état de vos actions de conformité

Lorsque vous exécutez une action asynchrone à partir du volet Résultats de l'enquête sur de nombreux fichiers, par exemple le déplacement ou la suppression de 100 fichiers, le processus peut prendre un certain temps. Vous pouvez contrôler l'état de ces actions dans le volet *action Status* pour savoir quand elles ont été appliquées à tous les fichiers.

Cela vous permet de voir les actions effectuées avec succès, celles en cours et celles qui ont échoué pour diagnostiquer et résoudre tout problème. Notez que les courtes opérations qui se sont terminées rapidement, telles que le déplacement d'un seul fichier, n'apparaissent pas dans le volet Statut des actions.

Le statut peut être :

- Réussite : Une action de classification BlueXP est terminée et tous les éléments ont réussi.
- Réussite partielle : Une action de classification BlueXP est terminée, certains éléments ont échoué et d'autres ont réussi.
- En cours - l'action est toujours en cours.
- En file d'attente - l'action n'a pas démarré.
- Annulé : l'action a été annulée.

- Echec - l'action a échoué.

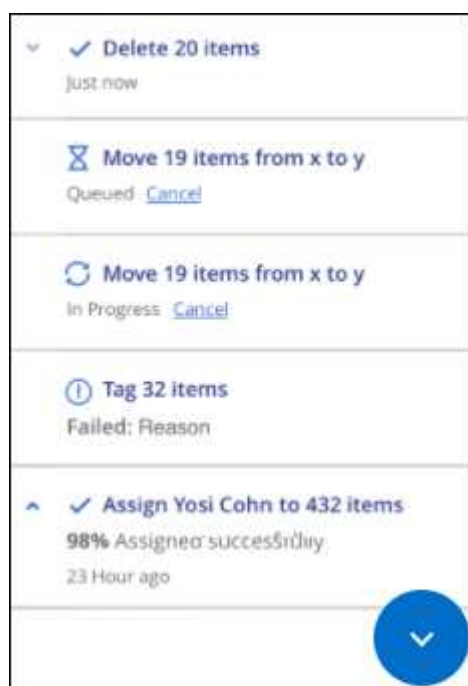
Notez que vous pouvez annuler toutes les actions ayant le statut « en attente » ou « en cours ».

## Étapes

1. En bas à droite de l'interface utilisateur de classification BlueXP, vous pouvez voir le bouton **actions**



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.

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

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

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

Pour activer cette fonctionnalité, vous devez vous connecter au système de classification BlueXP afin de modifier un fichier de configuration et d'exécuter un script. Découvrez comment ["Connectez-vous au système"](#)

de classification BlueXP" Selon que vous avez installé le logiciel manuellement sur une machine Linux ou si vous avez déployé l'instance dans le cloud.

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

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

### Étapes

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

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

Ne modifiez rien d'autre dans ce fichier.

3. Enregistrez les modifications apportées au fichier.
4. Accédez à « /opt/netapp/Datasense/Tools/customer\_configuration/Data\_providers » et exécutez le script suivant :

```
update_data_providers_from_config_file.sh
```

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

### Résultat

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

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

## Afficher la liste actuelle des ID de groupe

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

```
get_data_providers_configuration.sh
```

## Vérifiez l'historique des actions de classification BlueXP

Les activités de gestion des journaux de classification BlueXP qui ont été effectuées sur des fichiers depuis tous les environnements de travail et toutes les sources de données que la classification BlueXP analyse. La classification BlueXP consigne également les

## activités liées au déploiement de l'instance de classification BlueXP.

Vous pouvez afficher le contenu des fichiers journaux d'audit de classification BlueXP ou les télécharger pour voir quelles modifications de fichier ont été apportées et à quelle date. Par exemple, vous pouvez voir quelle demande a été émise, l'heure de la demande et des détails tels que l'emplacement source en cas de suppression d'un fichier ou l'emplacement source et de destination en cas de déplacement d'un fichier.

### Contenu du fichier journal

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

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

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

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

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

### Emplacements des fichiers journaux

Les fichiers journaux d'audit de gestion se trouvent sur la machine de classification BlueXP dans :  
`/opt/netapp/audit_logs/`

Les fichiers journaux d'audit d'installation sont écrits dans `/opt/netapp/install_logs/`



Chaque fichier journal peut avoir une taille maximale de 10 Mo. Lorsque cette limite est atteinte, un nouveau fichier journal démarre. Les fichiers journaux sont nommés « DataSense\_audit.log », « DataSense\_audit.log.1 », « DataSense\_audit.log.2 », etc. Un maximum de 100 fichiers journaux sont conservés sur le système - les anciens fichiers journaux sont automatiquement supprimés une fois le maximum atteint.

## Accédez aux fichiers journaux

Vous devez vous connecter au système de classification BlueXP pour accéder aux fichiers journaux. Découvrez comment "[Connectez-vous au système de classification BlueXP](#)" Selon que vous avez installé le logiciel manuellement sur une machine Linux ou si vous avez déployé l'instance dans le cloud.

## Réduction de la vitesse d'analyse de la classification BlueXP

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

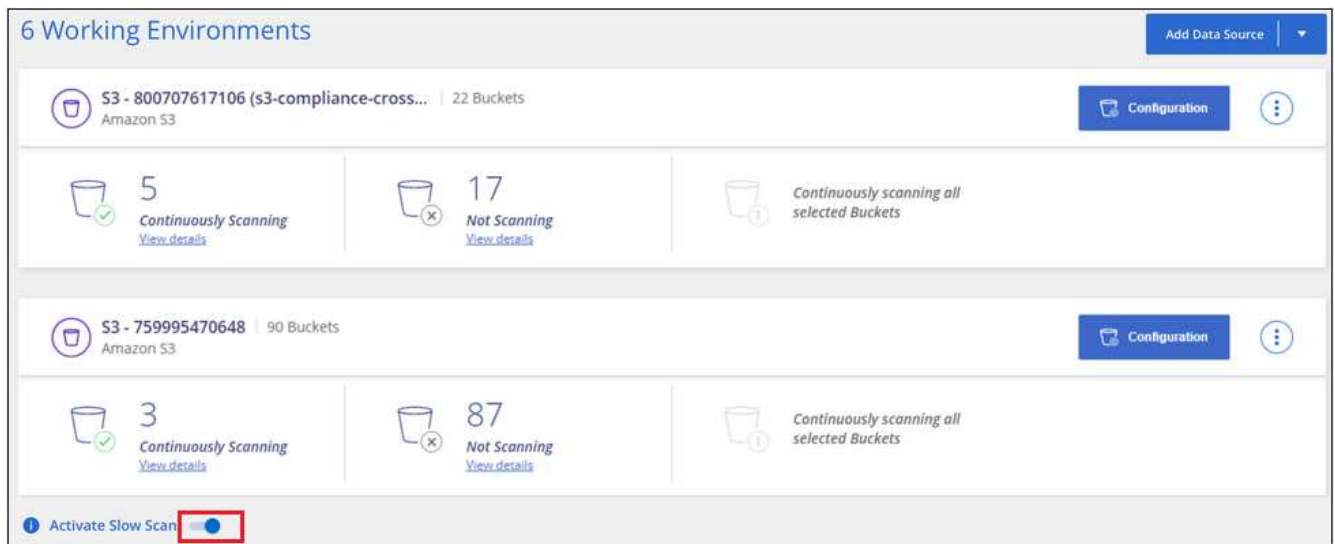
Lorsqu'elle est activée, l'analyse lente est utilisée sur toutes les sources de données ; vous ne pouvez pas configurer la numérisation lente pour un environnement de travail unique ou une source de données.



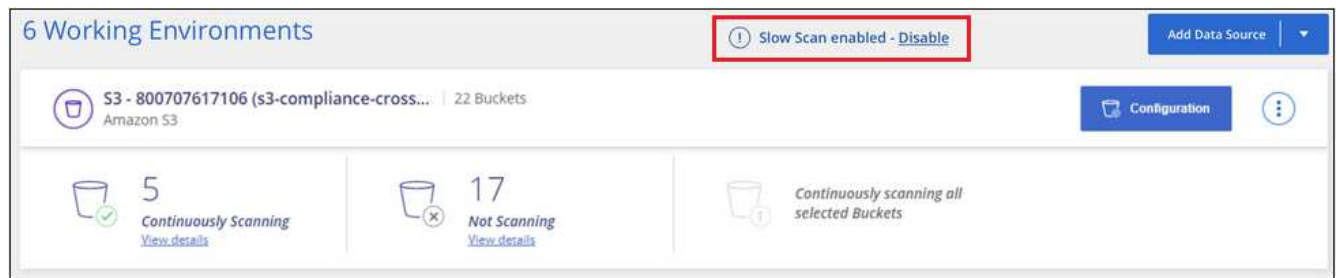
La vitesse de numérisation ne peut pas être réduite lors de la numérisation de bases de données.

### 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 de la classification BlueXP

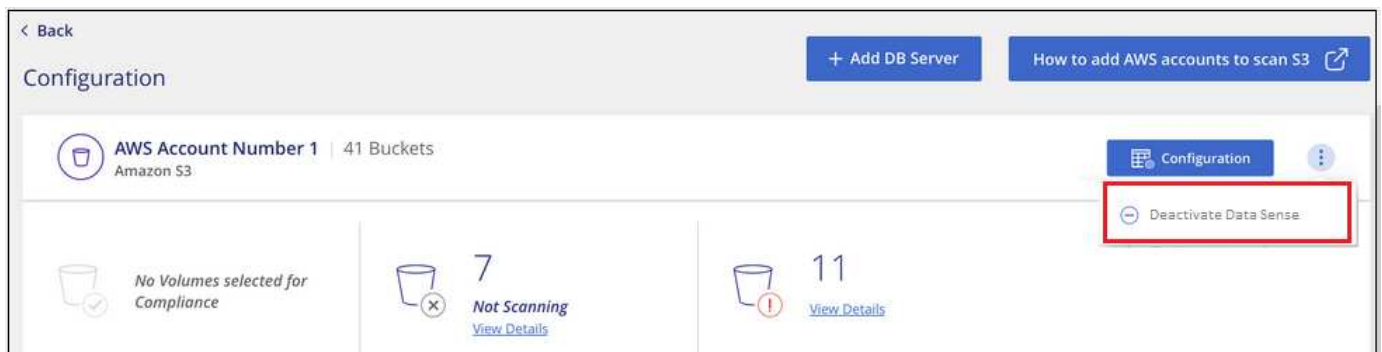
Si nécessaire, vous pouvez empêcher la classification BlueXP de scanner un ou plusieurs environnements de travail, bases de données, groupes de partage de fichiers, comptes OneDrive, comptes Google Drive, Ou SharePoint.

Le chargement pour l'analyse des données est interrompu lorsque la source de données est supprimée.

### Désactivation des analyses de conformité pour un environnement de travail

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


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

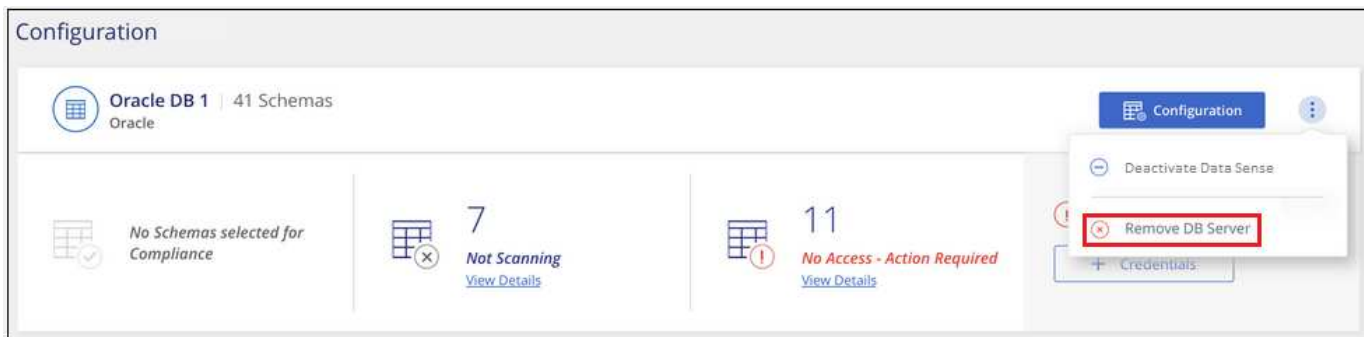


Vous pouvez également désactiver les analyses de conformité pour un environnement de travail à partir du panneau Services lorsque vous sélectionnez l'environnement de travail.

### Suppression d'une base de données de la classification BlueXP

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

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



## Suppression d'un compte OneDrive, SharePoint ou Google Drive de la classification BlueXP

Si vous ne souhaitez plus analyser les fichiers utilisateur à partir d'un compte OneDrive spécifique, d'un compte SharePoint spécifique ou d'un compte Google Drive, vous pouvez supprimer le compte de l'interface de classification BlueXP et arrêter toutes les analyses.

### Étapes

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




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

## Suppression d'un groupe de partages de fichiers de la classification BlueXP

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

### Étapes

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



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


## Désinstallation de la classification BlueXP

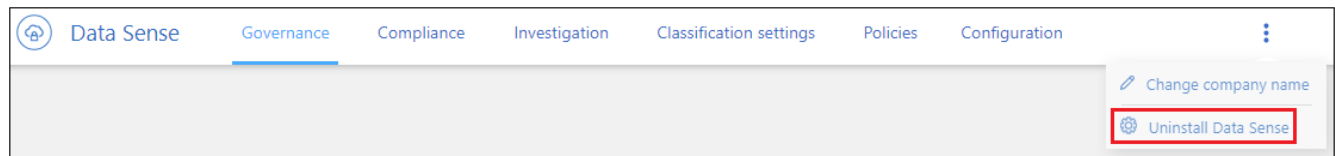
Vous pouvez désinstaller le logiciel de classification BlueXP pour résoudre des problèmes ou supprimer définitivement le logiciel de l'hôte. La suppression de l'instance supprime également les disques associés sur lesquels résident les données indexées. Toutes les informations analysées par BlueXP seront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

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

### Désinstallez la classification BlueXP d'un déploiement cloud

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

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



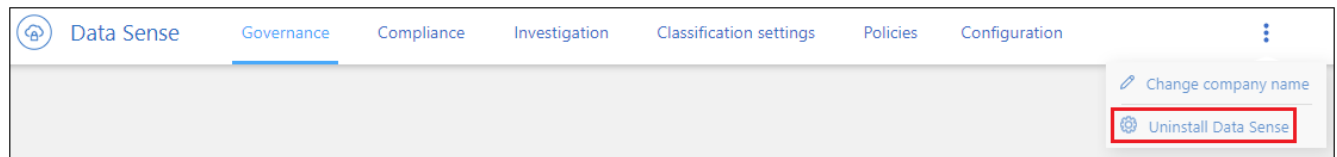
2. Dans la boîte de dialogue *Uninstall Data Sense*, tapez **uninstall** pour confirmer que vous souhaitez déconnecter l'instance de classification BlueXP du connecteur BlueXP, puis cliquez sur **Uninstall**.
3. Accédez à la console de votre fournisseur cloud et supprimez l'instance de classification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

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

### Désinstallez la classification BlueXP d'un déploiement sur site

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

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



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

```
cleanup.sh
```

Découvrez comment "[Connectez-vous à la machine hôte de classification BlueXP](#)".

## Informations sur le copyright

Copyright © 2024 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.