Gérer la classification des données

NetApp Data Classification

NetApp
February 11, 2026

Sommaire

Gérer la classification des données

Exclure des répertoires spécifiques des analyses de NetApp Data Classification

Si vous souhaitez que NetApp Data Classification exclue des répertoires spécifiques des analyses, vous pouvez ajouter ces noms de répertoire à un fichier de configuration. Après avoir appliqué cette modification, le moteur de classification des données exclut ces répertoires des analyses.

Par défaut, les analyses de classification des données excluent les données d'instantané de volume, qui sont identiques à leur source dans le volume.

Sources de données prises en charge

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

- ONTAP sur site
- Cloud Volumes ONTAP
- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Partages de fichiers généraux

Définir 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 des données afin de pouvoir modifier un fichier de configuration et exécuter un script. Découvrez comment"connectez-vous au système de classification des données" selon que vous avez installé manuellement le logiciel sur une machine Linux ou si vous avez déployé l'instance dans le cloud.

Considérations

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

Étapes

1. Sur le système de classification des données, accédez à « /opt/netapp/config/custom_configuration » puis ouvrez le fichier `data_provider.yaml` .
2. Dans la section « data_providers » sous la ligne « exclude : », entrez les chemins de répertoire à exclure. Par exemple:

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

Ne modifiez rien d'autre dans ce fichier.

3. Enregistrez les modifications dans le 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 dans 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/dossier1
- /CVO1/nomdossier1
- /CVO1/dossier10
- /CVO1/*dossier1
- /CVO1/+nomdossier1
- /CVO1/notfolder10
- /CVO22/dossier1
- /CVO22/nomdossier1
- /CVO22/dossier10

Exemples de chemins qui ne seront pas exclus :

- /CVO1/*dossier
- /CVO1/nom du dossier
- /CVO22/*dossier20

Configuration 2 :

Tout dossier contenant uniquement « *folder1 » au début du nom sera exclu.

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

Résultats attendus pour les chemins qui seront exclus :

- /CVO/*dossier1
- /CVO/*nomdossier1
- /CVO/*dossier10

Exemples de chemins qui ne seront pas exclus :

- /CVO/dossier1
- /CVO/nomdossier1
- /CVO/pas*dossier10

Configuration 3 :

Chaque dossier dans la source de données « CVO22 » qui contient « folder1 » n'importe où dans le nom sera exclu.

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

Résultats attendus pour les chemins qui seront exclus :

- /CVO22/dossier1
- /CVO22/nomdossier1
- /CVO22/dossier10

Exemples de chemins qui ne seront pas exclus :

- /CVO1/dossier1
- /CVO1/nomdossier1
- /CVO1/dossier10

Échapper les caractères spéciaux dans les noms de dossiers

Si vous avez un nom de dossier qui contient l'un des caractères spéciaux suivants et que vous souhaitez exclure les données de ce dossier de l'analyse, vous devrez 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 que le contenu du `data_provider.yaml` fichier de configuration soit différent de ce qui a été réellement validé après l'exécution du `update_data_providers_from_config_file.sh` scénario. Pour afficher la liste actuelle des répertoires que vous avez exclus de l'analyse de classification des données, exécutez la commande suivante depuis « /opt/netapp/Datasense/tools/customer_configuration/data_providers » :

```
get_data_providers_configuration.sh
```

Définir des ID de groupe supplémentaires comme ouverts à l'organisation dans la NetApp Data Classification

Lorsque des ID de groupe (GID) sont attachés à des fichiers ou des 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 GID ne sont pas initialement configurés avec le niveau d'autorisation « Ouvrir à l'organisation », vous pouvez ajouter cette autorisation au GID afin que tous les fichiers et dossiers auxquels ce GID est attaché soient considérés comme « ouverts à l'organisation ».

Une fois cette modification effectuée et NetApp Data Classification réanalyse vos fichiers et dossiers, tous les fichiers et dossiers auxquels ces ID de groupe sont associés afficheront cette autorisation dans la page Détails de l'enquête et apparaîtront également dans les rapports où vous affichez les autorisations de fichiers.

Pour activer cette fonctionnalité, vous devez vous connecter au système de classification des données afin de pouvoir modifier un fichier de configuration et exécuter un script. Découvrez comment"connectez-vous au système de classification des données" selon que vous avez installé manuellement le logiciel sur une machine Linux ou si vous avez déployé l'instance dans le cloud.

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

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

Étapes

1. Sur le système de classification des données, accédez à « /opt/netapp/config/custom_configuration » et ouvrez le fichier `data_provider.yaml` .
2. Dans la ligne « organization_group_ids: [] », ajoutez les ID de groupe. Par exemple:

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

   Ne changez rien d'autre dans ce fichier.
3. Enregistrez les modifications dans le 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 dans le moteur de classification.

Résultat

Toutes les analyses ultérieures de vos données identifieront les fichiers ou dossiers auxquels ces identifiants de groupe sont associés comme étant « ouverts à l'organisation ».

Vous pouvez modifier la liste des identifiants de groupe et supprimer tous les identifiants de groupe que vous avez ajoutés dans le passé en suivant ces mêmes étapes. La liste révisée des ID de groupe sera mise à jour après avoir exécuté le script pour valider vos modifications.

Afficher la liste actuelle des identifiants de groupe

Il est possible que le contenu du `data_provider.yaml` fichier de configuration différent de ce qui a été réellement validé après l'exécution du `update_data_providers_from_config_file.sh` scénario. Pour afficher la liste actuelle des ID de groupe que vous avez ajoutés à la classification des données, exécutez la commande suivante depuis « /opt/netapp/Datasense/tools/customer_configuration/data_providers » :

```
get_data_providers_configuration.sh
```

Personnalisez la définition des données obsolètes dans NetApp Data Classification

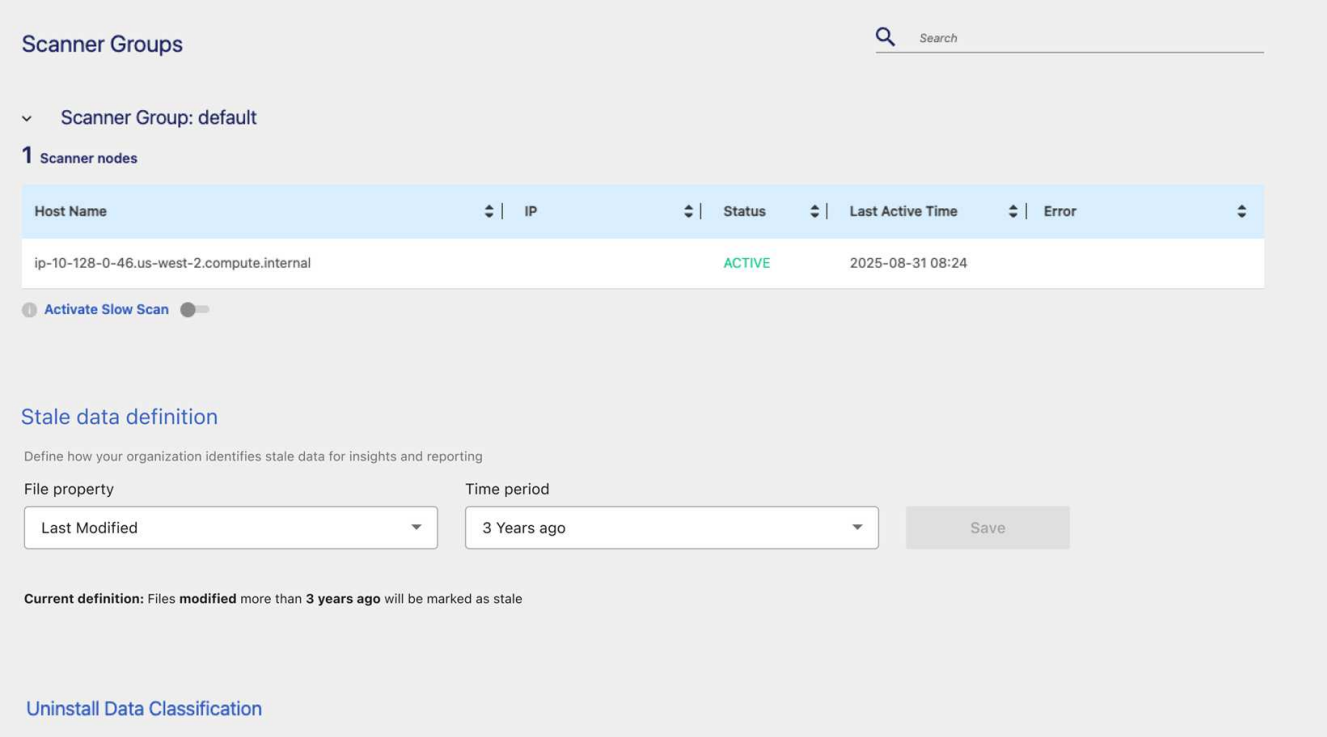
La NetApp Data Classification identifie les données obsolètes pour vous aider à repérer les opportunités d'économies et les risques de gouvernance. Étant donné que la définition des données obsolètes peut varier selon les contextes organisationnels, vous pouvez personnaliser la façon dont la classification des données définit les données obsolètes.

Les données obsolètes peuvent être définies en fonction de leur *dernier accès* ou de leur *dernière modification*. Les périodes sélectionnables vont de 6 mois à 10 ans.

Par défaut, les données sont considérées comme obsolètes si leur dernière modification remonte à trois ans.

Définir les données obsolètes

1. Dans Ransomware Resilience, sélectionnez **Configuration**.
2. Dans la page Configuration, faites défiler jusqu'à la section **Définition des données obsolètes**.
3. Dans le menu déroulant **Propriétés du fichier**, choisissez si vous souhaitez définir les données obsolètes en fonction de leur **Dernier accès** ou de leur **Dernière modification**.
4. Choisissez la période pour la définition des données obsolètes.



5. Sélectionnez **Enregistrer**.

Supprimer les sources de données de la NetApp Data Classification

Si nécessaire, vous pouvez empêcher NetApp Data Classification d'analyser un ou plusieurs systèmes, bases de données ou groupes de partage de fichiers.

Désactiver les analyses d'un système

Lorsque vous désactivez les analyses, Data Classification n'analyse plus les données du système et supprime les informations indexées de l'instance Data Classification. Les données du système lui-même ne sont pas supprimées.

1. Depuis la page *Configuration*, sélectionnez l'option bouton dans la ligne du système puis **Désactiver la classification des données**.

> Vous pouvez également désactiver les analyses d'un système à partir du panneau Services lorsque vous sélectionnez le système.

Supprimer une base de données de la classification des données

Si vous n'avez plus besoin d'analyser une certaine base de données, vous pouvez la supprimer de l'interface de classification des données et arrêter toutes les analyses.

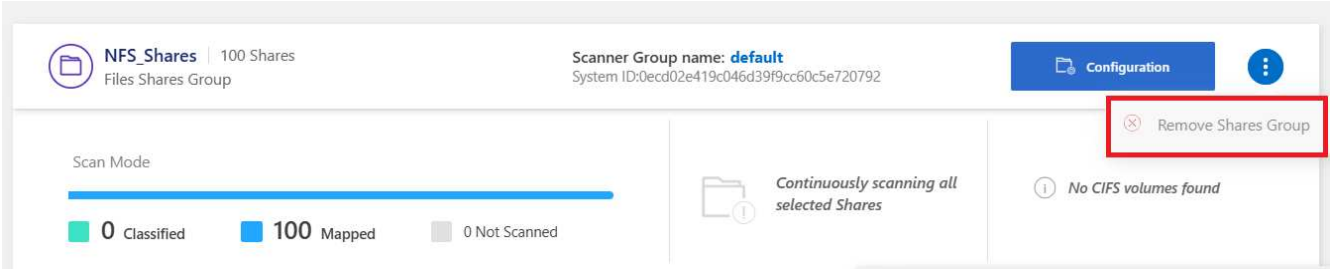
1. Depuis la page *Configuration*, sélectionnez l'option bouton dans la ligne de la base de données puis **Supprimer le serveur de base de données**.

Supprimer un groupe de partages de fichiers de la classification des données

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

Étapes

1. Depuis la page *Configuration*, sélectionnez l'option bouton dans la ligne du groupe de partages de fichiers puis **Supprimer le groupe de partages de fichiers**.



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

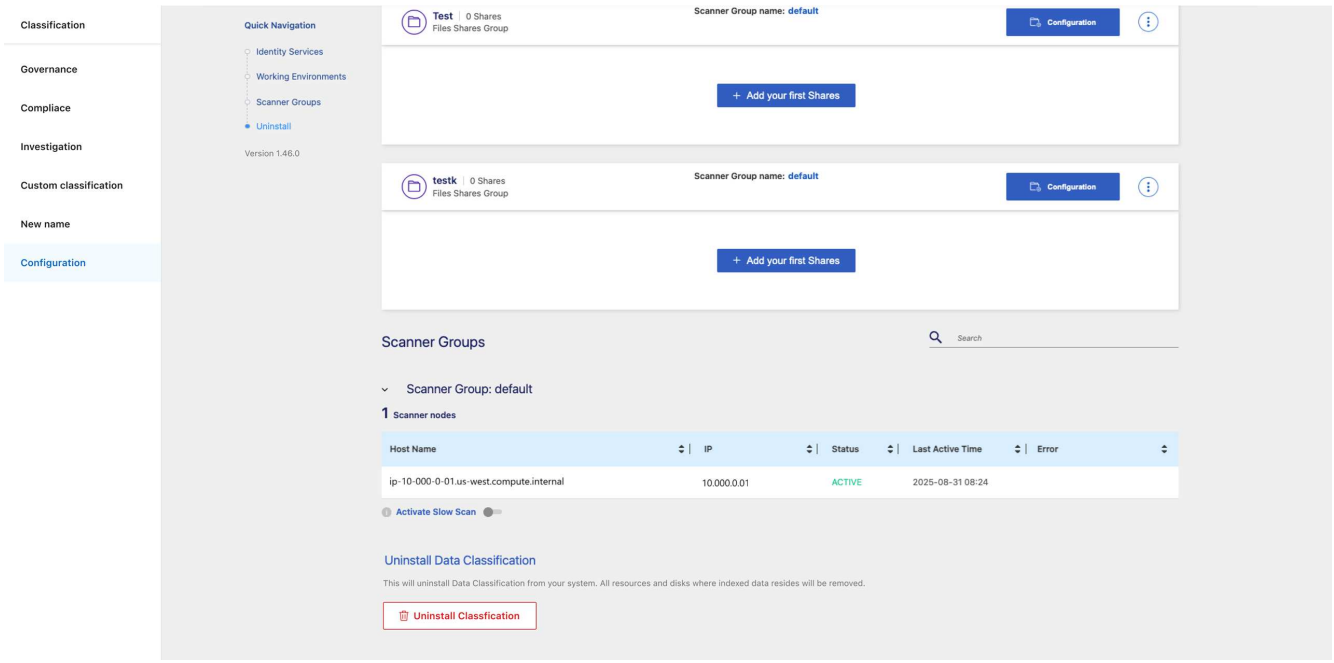
Désinstaller NetApp Data Classification

Vous pouvez désinstaller NetApp Data Classification pour résoudre les problèmes ou pour supprimer définitivement le logiciel de l'hôte. La suppression de l'instance supprime également les disques associés sur lesquels résident les données indexées, ce qui signifie que toutes les informations analysées par Data Classification seront définitivement supprimées.

Les étapes à suivre dépendent du fait que vous avez déployé la classification des données dans le cloud ou sur un hôte local.

Désinstaller Data Classification d'un fournisseur cloud

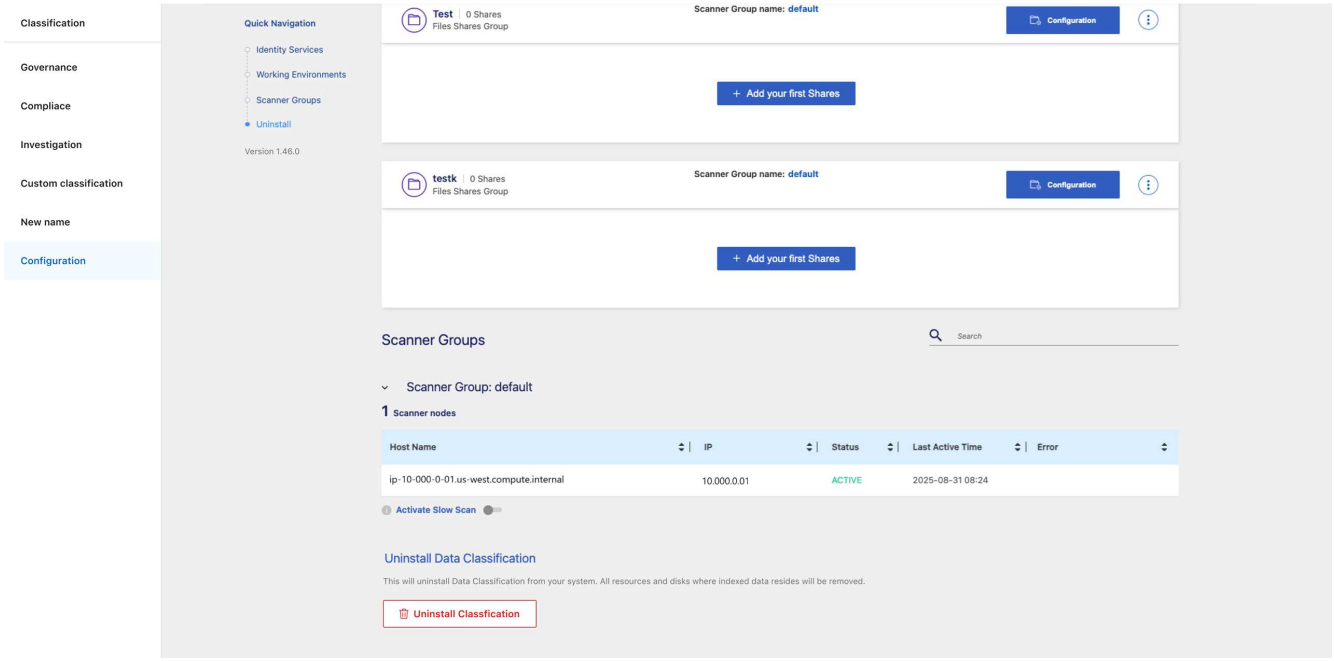
1. Dans Classification des données, sélectionnez **Configuration**.
2. Au bas de la page de configuration, sélectionnez **Désinstaller la classification**.



3. Dans la boîte de dialogue, saisissez « désinstaller » pour procéder à la déconnexion de l'instance de classification des données de l'agent de la console. Sélectionnez **Désinstaller** pour confirmer.
4. Dans la boîte de dialogue *Désinstaller la classification*, saisissez **uninstall** pour confirmer que vous souhaitez déconnecter l'instance de classification des données de l'agent de la console, puis sélectionnez **Désinstaller**.
5. Pour finaliser le processus de désinstallation, accédez à la console de votre fournisseur de cloud et supprimez l'instance de classification des données. L'instance est nommée *CloudCompliance* avec un hachage généré (UUID) concaténé. Par exemple : *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

Désinstaller la classification des données d'un déploiement sur site

1. Dans Classification des données, sélectionnez **Configuration**.
2. Au bas de la page de configuration, sélectionnez **Désinstaller la classification**.



3. Dans la boîte de dialogue, saisissez « désinstaller » pour procéder à la déconnexion de l'instance de classification des données de l'agent de la console. Sélectionnez **Désinstaller** pour confirmer.
4. Pour désinstaller le logiciel de l'hôte, exécutez le `cleanup.sh` script sur la machine hôte de classification des données, par exemple :

```
cleanup.sh
```

Le script est situé dans le `/install/light_probe/onprem_installer/cleanup.sh` annuaire. Découvrez comment"connectez-vous à la machine hôte de classification des données" .

Informations sur le copyright

Informations sur les marques commerciales