Activer l'analyse sur vos sources de données

NetApp Data Classification

NetApp
February 11, 2026

Sommaire

Activer l’analyse sur vos sources de données

Analyser les sources de données avec la NetApp Data Classification

NetApp Data Classification analyse les données dans les référentiels (volumes, schémas de base de données ou autres données utilisateur) que vous sélectionnez pour identifier les données personnelles et sensibles. La classification des données cartographie ensuite vos données organisationnelles, catégorise chaque fichier et identifie des modèles prédéfinis dans les données. Le résultat de l’analyse est un index des informations personnelles, des informations personnelles sensibles, des catégories de données et des types de fichiers.

Après l’analyse initiale, Data Classification analyse en continu vos données de manière circulaire pour détecter les modifications incrémentielles. C’est pourquoi il est important de maintenir l’instance en cours d’exécution.

Vous pouvez activer et désactiver les analyses au niveau du volume ou au niveau du schéma de base de données.

Quelle est la différence entre les analyses de cartographie et de classification

Vous pouvez effectuer deux types d’analyses dans la classification des données :

- **Les analyses de cartographie uniquement** fournissent uniquement un aperçu de haut niveau de vos données et sont effectuées sur des sources de données sélectionnées. Les analyses de cartographie uniquement prennent moins de temps que les analyses de cartographie et de classification, car elles n’accèdent pas aux fichiers pour voir les données qu’ils contiennent. Vous souhaiterez peut-être procéder ainsi dans un premier temps pour identifier les domaines de recherche, puis effectuer une analyse de cartographie et de classification sur ces domaines.
- **Les analyses de cartographie et de classification** fournissent une analyse approfondie de vos données.

Le tableau ci-dessous montre certaines des différences :

Fonctionnalité	Cartographier et classer les scans	Analyses de cartographie uniquement
Vitesse de numérisation	Lent	Rapide
Tarifs	Gratuit	Gratuit
Capacité	Limité à 500 Tio*	Limité à 500 Tio*
Liste des types de fichiers et de la capacité utilisée	Oui	Oui
Nombre de fichiers et capacité utilisée	Oui	Oui
Âge et taille des fichiers	Oui	Oui
Capacité à exécuter un"Rapport de mappage des données"	Oui	Oui
Page d’enquête sur les données pour afficher les détails du fichier	Oui	Non

Fonctionnalité	Cartographier et classer les scans	Analyses de cartographie uniquement
Rechercher des noms dans les fichiers	Oui	Non
Créer"requêtes enregistrées" qui fournissent des résultats de recherche personnalisés	Oui	Non
Possibilité d'exécuter d'autres rapports	Oui	Non
Possibilité de voir les métadonnées des fichiers**	Non	Oui

* La classification des données n'impose pas de limite à la quantité de données qu'elle peut analyser. Chaque agent de console prend en charge l'analyse et l'affichage de 500 Tio de données. Pour scanner plus de 500 Tio de données,"installer un autre agent de console" alors"déployer une autre instance de classification des données" . + L'interface utilisateur de la console affiche les données d'un seul connecteur. Pour obtenir des conseils sur l'affichage des données de plusieurs agents de console, consultez"Travailler avec plusieurs agents de console" .

** Les métadonnées suivantes sont extraites des fichiers lors des analyses de mappage :

- Système
- Type de système
- Référentiel de stockage
- Type de fichier
- Capacité utilisée
- Nombre de fichiers
- Taille du fichier
- Création de fichier
- Dernier accès au fichier
- Fichier modifié pour la dernière fois
- Heure de découverte du fichier
- Extraction des autorisations

Différences entre les tableaux de bord de gouvernance :

Fonctionnalité	Cartographier et classer	Carte
Données obsolètes	Oui	Oui
Données non commerciales	Oui	Oui
Fichiers dupliqués	Oui	Oui
Requêtes enregistrées prédéfinies	Oui	Non
Requêtes enregistrées par défaut	Oui	Oui
Rapport DDA	Oui	Oui
Rapport de cartographie	Oui	Oui
Détection du niveau de sensibilité	Oui	Non
Données sensibles avec des autorisations étendues	Oui	Non
Autorisations ouvertes	Oui	Oui
L'âge des données	Oui	Oui
Taille des données	Oui	Oui
Catégories	Oui	Non
Types de fichiers	Oui	Oui

Différences entre les tableaux de bord de conformité :

Fonctionnalité	Cartographier et classer	Carte
Informations personnelles	Oui	Non
Informations personnelles sensibles	Oui	Non
Rapport d'évaluation des risques liés à la vie privée	Oui	Non
Rapport HIPAA	Oui	Non
Rapport PCI DSS	Oui	Non

Différences entre les filtres d'investigation :

Fonctionnalité	Cartographier et classer	Carte
Requêtes enregistrées	Oui	Oui
Type de système	Oui	Oui
Système	Oui	Oui
Référentiel de stockage	Oui	Oui
Type de fichier	Oui	Oui
Taille du fichier	Oui	Oui
Temps de création	Oui	Oui
Temps découvert	Oui	Oui
Dernière modification	Oui	Oui
Dernier accès	Oui	Oui
Autorisations ouvertes	Oui	Oui
Chemin du répertoire de fichiers	Oui	Oui
Catégorie	Oui	Non
Niveau de sensibilité	Oui	Non
Nombre d'identifiants	Oui	Non
Données personnelles	Oui	Non
Données personnelles sensibles	Oui	Non
Personne concernée	Oui	Non
Doublons	Oui	Oui
Statut de classification	Oui	Le statut est toujours « Informations limitées »
Événement d'analyse d'analyse	Oui	Oui
Hachage de fichier	Oui	Oui
Nombre d'utilisateurs avec accès	Oui	Oui
Autorisations utilisateur/groupe	Oui	Oui
Propriétaire du fichier	Oui	Oui
Type de répertoire	Oui	Oui

Analyser Amazon FSx pour les volumes ONTAP avec la NetApp Data Classification

Suivez quelques étapes pour analyser Amazon FSx pour les volumes ONTAP avec NetApp Data Classification.

Avant de commencer

- Vous avez besoin d'un agent de console actif dans AWS pour déployer et gérer la classification des données.
- Le groupe de sécurité que vous avez sélectionné lors de la création du système doit autoriser le trafic provenant de l'instance de classification des données. Vous pouvez trouver le groupe de sécurité associé à l'aide de l'ENI connecté au système de fichiers FSx for ONTAP et le modifier à l'aide de la console de gestion AWS.

  "Groupes de sécurité AWS pour les instances Linux"

  "Groupes de sécurité AWS pour les instances Windows"

  "Interfaces réseau élastiques AWS (ENI)"

- Assurez-vous que les ports suivants sont ouverts sur l'instance de classification des données :
  - Pour NFS – ports 111 et 2049.
  - Pour CIFS – ports 139 et 445.

Déployer l'instance de classification des données

"Déployer la classification des données"s'il n'y a pas déjà une instance déployée.

Vous devez déployer la classification des données sur le même réseau AWS que l'agent de console pour AWS et les volumes FSx que vous souhaitez analyser.

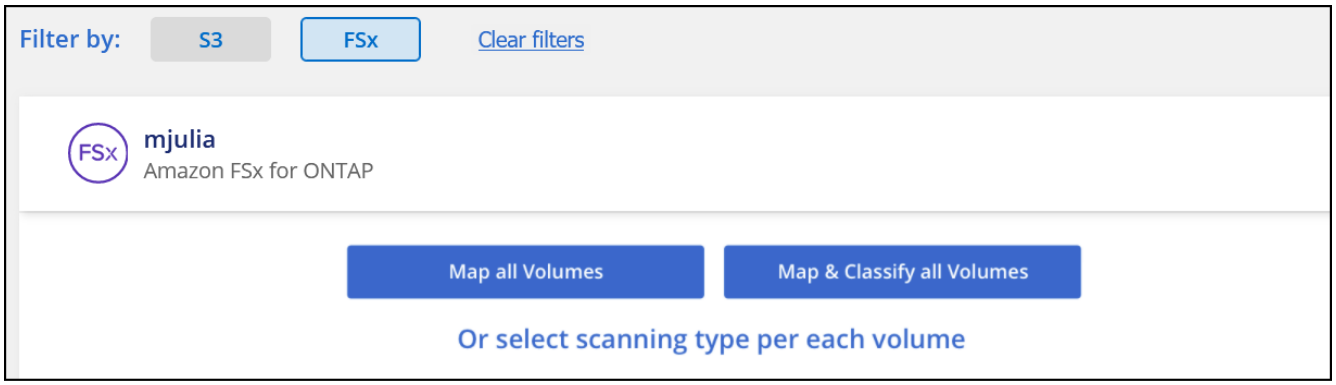
Remarque : le déploiement de la classification des données dans un emplacement local n'est actuellement pas pris en charge lors de l'analyse des volumes FSx.

Les mises à niveau du logiciel de classification des données sont automatisées tant que l'instance dispose d'une connexion Internet.

Activez la classification des données dans vos systèmes

Vous pouvez activer la classification des données pour les volumes FSx for ONTAP .

1. Depuis la NetApp Console, **Gouvernance > Classification**.
2. Dans le menu Classification des données, sélectionnez **Configuration**.



3. Sélectionnez la manière dont vous souhaitez analyser les volumes de chaque système. "En savoir plus sur les analyses de cartographie et de classification":

- Pour mapper tous les volumes, sélectionnez **Mapper tous les volumes**.
- Pour cartographier et classer tous les volumes, sélectionnez **Cartographier et classer tous les volumes**.
- Pour personnaliser l'analyse de chaque volume, sélectionnez **Ou sélectionnez le type d'analyse pour chaque volume**, puis choisissez les volumes que vous souhaitez mapper et/ou classer.

4. Dans la boîte de dialogue de confirmation, sélectionnez **Approuver** pour que la classification des données commence à analyser vos volumes.

Résultat

La classification des données commence à analyser les volumes que vous avez sélectionnés dans le système. Les résultats seront disponibles dans le tableau de bord de conformité dès que la classification des données aura terminé les analyses initiales. Le temps nécessaire dépend de la quantité de données : cela peut prendre quelques minutes ou quelques heures. Vous pouvez suivre la progression de l'analyse initiale en accédant au menu **Configuration** puis en sélectionnant la **Configuration système**. Suivez la progression de chaque analyse dans la barre de progression ; vous pouvez survoler la barre de progression pour voir le nombre de fichiers analysés par rapport au nombre total de fichiers dans le volume.

- Par défaut, si Data Classification ne dispose pas d'autorisations d'attributs d'écriture dans CIFS ou d'autorisations d'écriture dans NFS, le système n'analysera pas les fichiers de vos volumes car Data Classification ne peut pas rétablir l'« heure du dernier accès » à l'horodatage d'origine. Si vous ne vous souciez pas de savoir si la dernière heure d'accès est réinitialisée, sélectionnez **Ou sélectionnez le type d'analyse pour chaque volume**. La page résultante contient un paramètre que vous pouvez activer pour que la classification des données analyse les volumes quelles que soient les autorisations.
- La classification des données analyse un seul partage de fichiers sous un volume. Si vous avez plusieurs partages dans vos volumes, vous devrez analyser ces autres partages séparément en tant que groupe de partages. "Voir plus de détails sur cette limitation de classification des données" .

Vérifiez que la classification des données a accès aux volumes

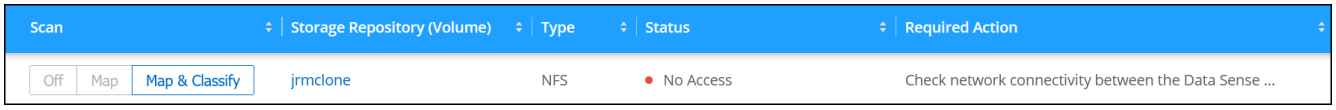
Assurez-vous que la classification des données peut accéder aux volumes en vérifiant votre réseau, vos groupes de sécurité et vos politiques d'exportation.

Vous devrez fournir à Data Classification les informations d'identification CIFS afin qu'il puisse accéder aux volumes CIFS.

Étapes

1. Dans le menu Classification des données, sélectionnez **Configuration**.
2. Sur la page Configuration, sélectionnez **Afficher les détails** pour vérifier l'état et corriger les erreurs.

   Par exemple, l'image suivante montre un volume que Data Classification ne peut pas analyser en raison de problèmes de connectivité réseau entre l'instance Data Classification et le volume.



3. Assurez-vous qu'il existe une connexion réseau entre l'instance de classification des données et chaque réseau qui inclut des volumes pour FSx pour ONTAP.

Pour FSx for ONTAP, la classification des données peut analyser les volumes uniquement dans la même région que la console.

4. Assurez-vous que les stratégies d'exportation de volume NFS incluent l'adresse IP de l'instance de classification des données afin qu'elle puisse accéder aux données sur chaque volume.
5. Si vous utilisez CIFS, fournissez à Data Classification les informations d'identification Active Directory afin qu'il puisse analyser les volumes CIFS.

   a. Dans le menu Classification des données, sélectionnez **Configuration**.
   b. Pour chaque système, sélectionnez **Modifier les informations d'identification CIFS** et saisissez le nom d'utilisateur et le mot de passe dont Data Classification a besoin pour accéder aux volumes CIFS sur le système.

      Les informations d'identification peuvent être en lecture seule, mais la fourniture d'informations d'identification d'administrateur garantit que la classification des données peut lire toutes les données nécessitant des autorisations élevées. Les informations d'identification sont stockées sur l'instance de classification des données.

      Si vous souhaitez vous assurer que les « dernières heures d'accès » de vos fichiers ne sont pas modifiées par les analyses de classification des données, il est recommandé que l'utilisateur dispose des autorisations d'écriture d'attributs dans CIFS ou des autorisations d'écriture dans NFS. Si possible, configurez l'utilisateur Active Directory en tant que membre d'un groupe parent de l'organisation disposant d'autorisations sur tous les fichiers.

   Après avoir saisi les informations d'identification, vous devriez voir un message indiquant que tous les volumes CIFS ont été authentifiés avec succès.

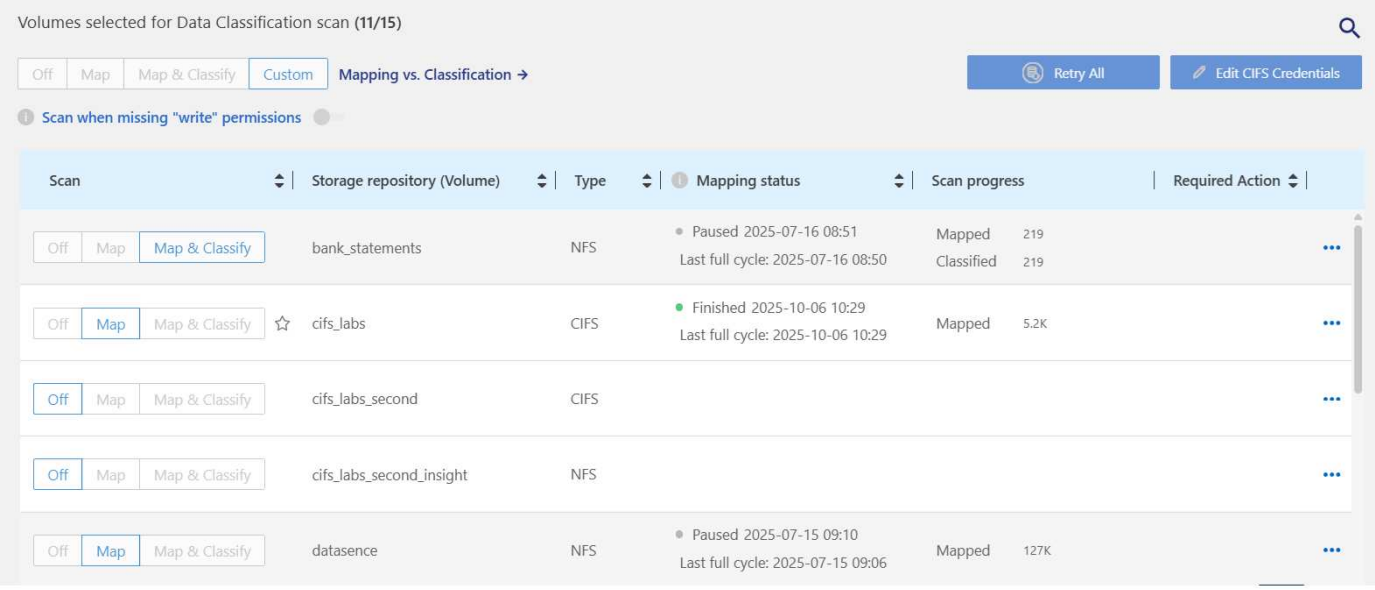
Activer et désactiver les analyses sur les volumes

Vous pouvez démarrer ou arrêter les analyses sur n'importe quel système à tout moment à partir de la page de configuration. Vous pouvez également passer d'analyses de cartographie uniquement à des analyses de cartographie et de classification, et vice-versa. Il est recommandé d'analyser tous les volumes d'un système.

Les nouveaux volumes ajoutés au système sont automatiquement analysés uniquement lorsque vous avez sélectionné le paramètre **Carte** ou **Carte et classification** dans la zone d'en-tête. Lorsque cette option est définie sur **Personnalisé** ou **Désactivé** dans la zone d'en-tête, vous devrez activer le mappage et/ou l'analyse complète sur chaque nouveau volume que vous ajoutez au système.

Le commutateur en haut de la page pour **Analyser en cas d'absence d'autorisations « d'écriture »** est désactivé par défaut. Cela signifie que si Data Classification ne dispose pas d'autorisations d'attributs d'écriture dans CIFS ou d'autorisations d'écriture dans NFS, le système n'analysera pas les fichiers car Data Classification ne peut pas rétablir l'« heure du dernier accès » à l'horodatage d'origine. Si vous ne vous souciez pas de savoir si la dernière heure d'accès est réinitialisée, activez l'interrupteur et tous les fichiers sont analysés quelles que soient les autorisations. "Apprendre encore plus".

Les nouveaux volumes ajoutés au système sont automatiquement analysés uniquement lorsque vous avez défini le paramètre **Carte** ou **Carte et classification** dans la zone d'en-tête. Lorsque le paramètre pour tous les volumes est **Personnalisé** ou **Désactivé**, vous devez activer l'analyse manuellement pour chaque nouveau volume que vous ajoutez.



Étapes

1. Dans le menu Classification des données, sélectionnez **Configuration**.
2. Choisissez un système, puis sélectionnez **Configuration**.
3. Pour activer ou désactiver les analyses pour tous les volumes, sélectionnez **Map**, **Map & Classify** ou **Off** dans l'en-tête au-dessus de tous les volumes.

   Pour activer ou désactiver les analyses de volumes individuels, recherchez les volumes dans la liste, puis sélectionnez **Map**, **Map & Classify** ou **Off** à côté du nom du volume.

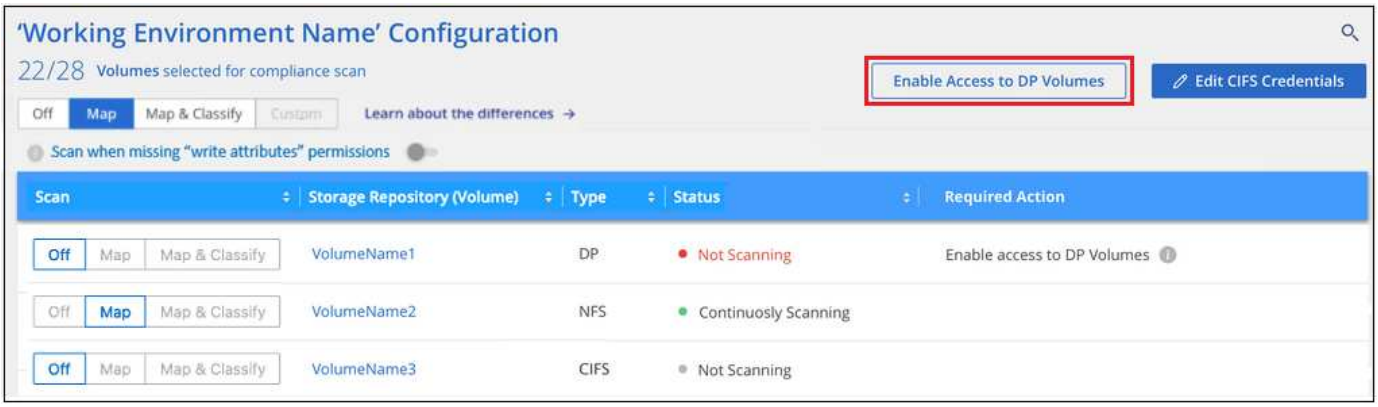
Résultat

Lorsque vous activez l'analyse, la classification des données démarre l'analyse des volumes que vous avez sélectionnés dans le système. Les résultats commencent à apparaître dans le tableau de bord Conformité dès que la classification des données démarre l'analyse. Le temps d'exécution de l'analyse dépend de la quantité de données, allant de quelques minutes à quelques heures.

Analyser les volumes de protection des données

Par défaut, les volumes de protection des données (DP) ne sont pas analysés car ils ne sont pas exposés en externe et Data Classification ne peut pas y accéder. Il s'agit des volumes de destination pour les opérations SnapMirror à partir d'un système de fichiers FSx pour ONTAP .

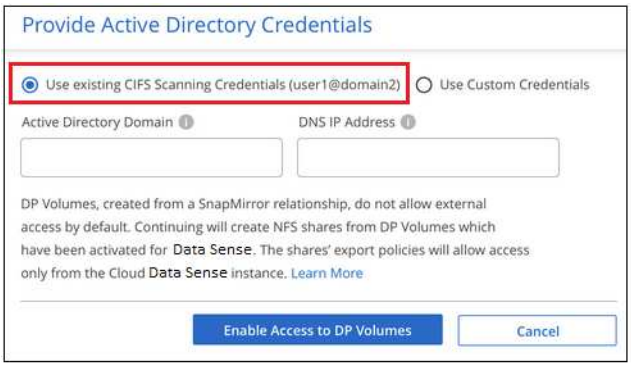
Initialement, la liste des volumes identifie ces volumes comme *Type* **DP** avec le *Statut* **Pas d'analyse** et l'*Action requise* **Activer l'accès aux volumes DP**.

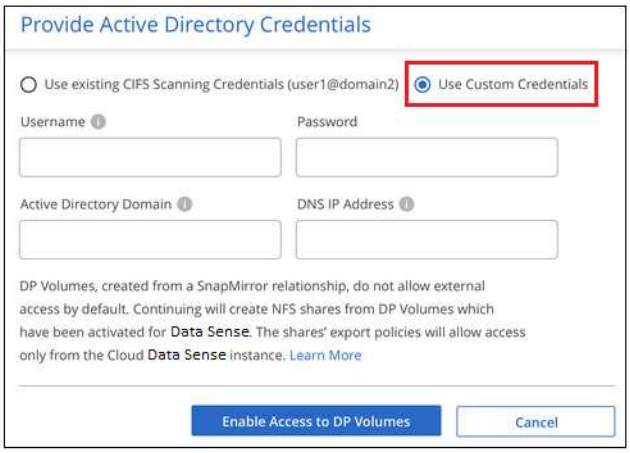


Étapes

Si vous souhaitez analyser ces volumes de protection des données :

1. Dans le menu Classification des données, sélectionnez **Configuration**.
2. Sélectionnez **Activer l'accès aux volumes DP** en haut de la page.
3. Vérifiez le message de confirmation et sélectionnez à nouveau **Activer l'accès aux volumes DP**.
   - Les volumes initialement créés en tant que volumes NFS dans le système de fichiers source FSx pour ONTAP sont activés.
   - Les volumes initialement créés en tant que volumes CIFS dans le système de fichiers source FSx for ONTAP nécessitent que vous saisissiez les informations d'identification CIFS pour analyser ces volumes DP. Si vous avez déjà saisi les informations d'identification Active Directory pour que la classification des données puisse analyser les volumes CIFS, vous pouvez utiliser ces informations d'identification ou spécifier un autre ensemble d'informations d'identification d'administrateur.





4. Activez chaque volume DP que vous souhaitez analyser.

Résultat

Une fois activée, la classification des données crée un partage NFS à partir de chaque volume DP activé pour l'analyse. Les politiques d'exportation de partage autorisent uniquement l'accès à partir de l'instance de classification des données.

Si vous n'aviez aucun volume de protection des données CIFS lorsque vous avez initialement activé l'accès aux volumes DP, et que vous en avez ajouté ultérieurement, le bouton **Activer l'accès à CIFS DP** apparaît en haut de la page de configuration. Sélectionnez ce bouton et ajoutez les informations d'identification CIFS pour activer l'accès à ces volumes CIFS DP.

Les informations d'identification Active Directory sont enregistrées uniquement dans la machine virtuelle de stockage du premier volume DP CIFS. Par conséquent, tous les volumes DP sur cette SVM seront analysés. Tous les volumes résidant sur d'autres SVM n'auront pas les informations d'identification Active Directory enregistrées, de sorte que ces volumes DP ne seront pas analysés.

Analyser les volumes Azure NetApp Files avec la NetApp Data Classification

Suivez quelques étapes pour démarrer avec NetApp Data Classification pour Azure NetApp Files.

Découvrez le système Azure NetApp Files que vous souhaitez analyser

Si le système Azure NetApp Files que vous souhaitez analyser n'est pas déjà présent dans la NetApp Console en tant que système,"ajoutez-le dans la page Systèmes" .

Déployer l'instance de classification des données

"Déployer la classification des données"s'il n'y a pas déjà une instance déployée.

La classification des données doit être déployée dans le cloud lors de l'analyse des volumes Azure NetApp Files et doit être déployée dans la même région que les volumes que vous souhaitez analyser.

Remarque : le déploiement de la classification des données dans un emplacement local n'est actuellement pas pris en charge lors de l'analyse des volumes Azure NetApp Files .

Activez la classification des données dans vos systèmes

Vous pouvez activer la classification des données sur vos volumes Azure NetApp Files .

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

2. Sélectionnez la manière dont vous souhaitez analyser les volumes de chaque système. "En savoir plus sur les analyses de cartographie et de classification":
   - Pour mapper tous les volumes, sélectionnez **Mapper tous les volumes**.
   - Pour cartographier et classer tous les volumes, sélectionnez **Cartographier et classer tous les volumes**.
   - Pour personnaliser l'analyse de chaque volume, sélectionnez **Ou sélectionnez le type d'analyse**

pour chaque volume, puis choisissez les volumes que vous souhaitez mapper ou mapper et classer.

VoirActiver ou désactiver les analyses sur les volumes pour plus de détails.

3. Dans la boîte de dialogue de confirmation, sélectionnez **Approuver**.

Résultat

La classification des données commence à analyser les volumes que vous avez sélectionnés dans le système. Les résultats sont disponibles dans le tableau de bord Conformité dès que la classification des données termine les analyses initiales. Le temps nécessaire dépend de la quantité de données : cela peut prendre quelques minutes ou quelques heures. Vous pouvez suivre la progression de l'analyse initiale en accédant au menu **Configuration** puis en sélectionnant la **Configuration système**. La classification des données affiche une barre de progression pour chaque analyse. Vous pouvez survoler la barre de progression pour voir le nombre de fichiers analysés par rapport au nombre total de fichiers dans le volume.

- Par défaut, si Data Classification ne dispose pas d'autorisations d'attributs d'écriture dans CIFS ou d'autorisations d'écriture dans NFS, le système n'analysera pas les fichiers de vos volumes car Data Classification ne peut pas rétablir l'« heure du dernier accès » à l'horodatage d'origine. Si vous ne vous souciez pas de savoir si la dernière heure d'accès est réinitialisée, sélectionnez **Ou sélectionnez le type d'analyse pour chaque volume**. La page résultante contient un paramètre que vous pouvez activer pour que la classification des données analyse les volumes quelles que soient les autorisations.
- La classification des données analyse un seul partage de fichiers sous un volume. Si vous avez plusieurs partages dans vos volumes, vous devrez analyser ces autres partages séparément en tant que groupe de partages. "En savoir plus sur cette limitation de classification des données" .

Vérifiez que la classification des données a accès aux volumes

Assurez-vous que la classification des données peut accéder aux volumes en vérifiant votre réseau, vos groupes de sécurité et vos politiques d'exportation. Vous devez fournir à Data Classification les informations d'identification CIFS afin qu'elle puisse accéder aux volumes CIFS.

Pour Azure NetApp Files, la classification des données ne peut analyser que les volumes dans la même région que la console.

Liste de contrôle

- Assurez-vous qu'il existe une connexion réseau entre l'instance de classification des données et chaque réseau qui inclut des volumes pour Azure NetApp Files.
- Assurez-vous que les ports suivants sont ouverts sur l'instance de classification des données :
  - Pour NFS – ports 111 et 2049.
  - Pour CIFS – ports 139 et 445.
- Assurez-vous que les stratégies d'exportation de volume NFS incluent l'adresse IP de l'instance de classification des données afin qu'elle puisse accéder aux données sur chaque volume.

Étapes

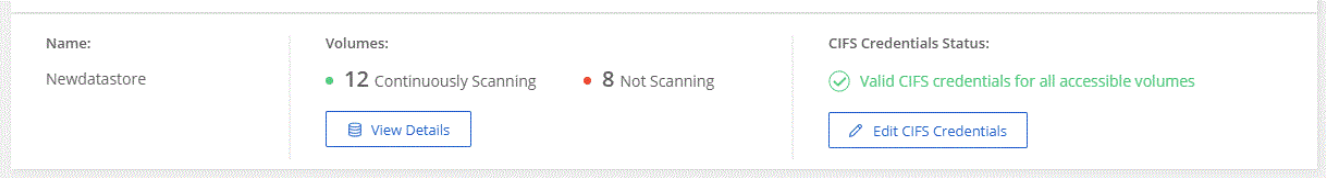
1. Dans le menu Classification des données, sélectionnez **Configuration**.

   a. Si vous utilisez CIFS (SMB), assurez-vous que les informations d'identification Active Directory sont correctes. Pour chaque système, sélectionnez **Modifier les informations d'identification CIFS**, puis saisissez le nom d'utilisateur et le mot de passe dont Data Classification a besoin pour accéder aux volumes CIFS sur le système.

Les informations d'identification peuvent être en lecture seule ; la fourniture d'informations d'identification d'administrateur garantit que Data Classification peut lire toutes les données nécessitant des autorisations élevées. Les informations d'identification sont stockées sur l'instance de classification des données.

Si vous souhaitez vous assurer que les « dernières heures d'accès » de vos fichiers ne sont pas modifiées par les analyses de classification des données, il est recommandé que l'utilisateur dispose des autorisations d'écriture d'attributs dans CIFS ou des autorisations d'écriture dans NFS. Si possible, configurez l'utilisateur Active Directory en tant que membre d'un groupe parent de l'organisation disposant d'autorisations sur tous les fichiers.

Après avoir saisi les informations d'identification, vous devriez voir un message indiquant que tous les volumes CIFS ont été authentifiés avec succès.



2. Sur la page Configuration, sélectionnez **Afficher les détails** pour vérifier l'état de chaque volume CIFS et NFS. Si nécessaire, corrigez les erreurs telles que les problèmes de connectivité réseau.

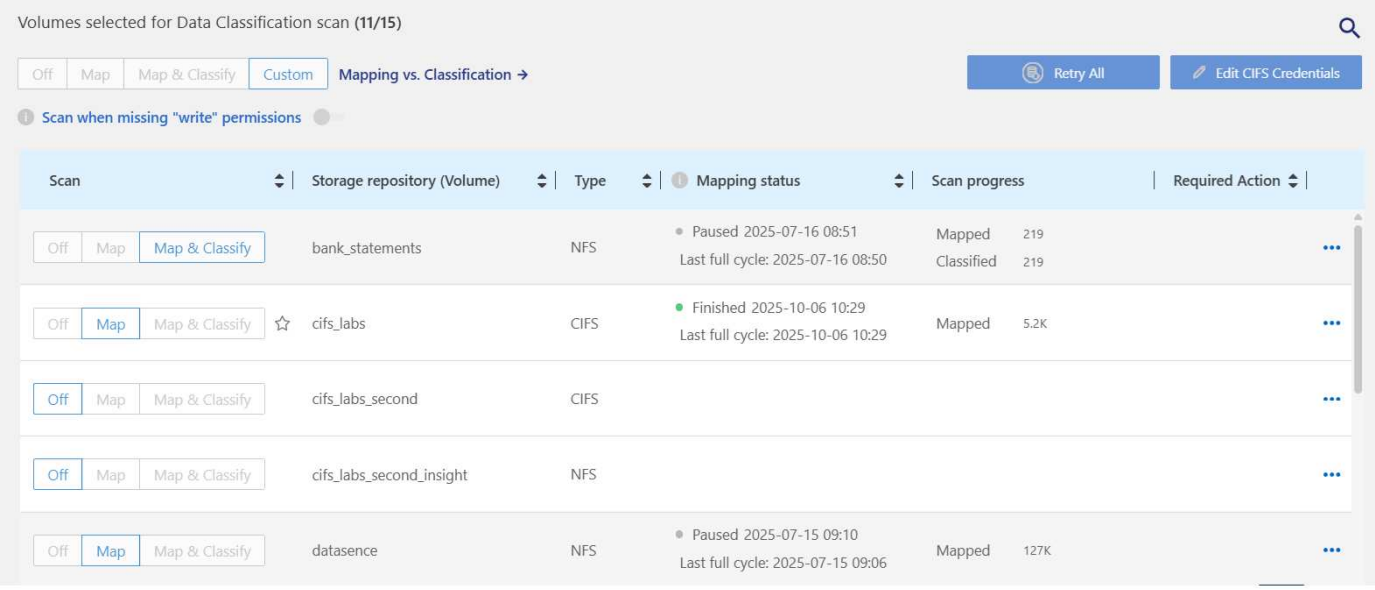
Activer ou désactiver les analyses sur les volumes

Vous pouvez démarrer ou arrêter les analyses sur n'importe quel système à tout moment à partir de la page de configuration. Vous pouvez également passer d'analyses de cartographie uniquement à des analyses de cartographie et de classification, et vice-versa. Il est recommandé d'analyser tous les volumes d'un système.

Les nouveaux volumes ajoutés au système sont automatiquement analysés uniquement lorsque vous avez sélectionné le paramètre **Carte** ou **Carte et classification** dans la zone d'en-tête. Lorsque cette option est définie sur **Personnalisé** ou **Désactivé** dans la zone d'en-tête, vous devrez activer le mappage et/ou l'analyse complète sur chaque nouveau volume que vous ajoutez au système.

Le commutateur en haut de la page pour **Analyser en cas d'absence d'autorisations « d'écriture »** est désactivé par défaut. Cela signifie que si Data Classification ne dispose pas d'autorisations d'attributs d'écriture dans CIFS ou d'autorisations d'écriture dans NFS, le système n'analysera pas les fichiers car Data Classification ne peut pas rétablir l'« heure du dernier accès » à l'horodatage d'origine. Si vous ne vous souciez pas de savoir si la dernière heure d'accès est réinitialisée, activez l'interrupteur et tous les fichiers sont analysés quelles que soient les autorisations. "Apprendre encore plus".

Les nouveaux volumes ajoutés au système sont automatiquement analysés uniquement lorsque vous avez défini le paramètre **Carte** ou **Carte et classification** dans la zone d'en-tête. Lorsque le paramètre pour tous les volumes est **Personnalisé** ou **Désactivé**, vous devez activer l'analyse manuellement pour chaque nouveau volume que vous ajoutez.



Étapes

1. Dans le menu Classification des données, sélectionnez **Configuration**.
2. Choisissez un système, puis sélectionnez **Configuration**.
3. Pour activer ou désactiver les analyses pour tous les volumes, sélectionnez **Map**, **Map & Classify** ou **Off** dans l'en-tête au-dessus de tous les volumes.

   Pour activer ou désactiver les analyses de volumes individuels, recherchez les volumes dans la liste, puis sélectionnez **Map**, **Map & Classify** ou **Off** à côté du nom du volume.

Résultat

Lorsque vous activez l'analyse, la classification des données démarre l'analyse des volumes que vous avez sélectionnés dans le système. Les résultats commencent à apparaître dans le tableau de bord Conformité dès que la classification des données démarre l'analyse. Le temps d'exécution de l'analyse dépend de la quantité de données, allant de quelques minutes à quelques heures.

Analysez les Cloud Volumes ONTAP et les volumes ONTAP sur site avec la NetApp Data Classification

Suivez quelques étapes pour commencer à analyser vos Cloud Volumes ONTAP et vos volumes ONTAP sur site à l'aide de NetApp Data Classification.

Prérequis

Avant d'activer la classification des données, assurez-vous que vous disposez d'une configuration prise en charge.

- Si vous numérisez des Cloud Volumes ONTAP et des systèmes ONTAP sur site accessibles via Internet, vous pouvez"déployer la classification des données dans le cloud" ou"dans un local équipé d'un accès Internet" .
- Si vous analysez des systèmes ONTAP sur site qui ont été installés sur un site sombre sans accès Internet, vous devez"déployer la classification des données dans le même emplacement sur site qui n'a pas d'accès Internet" . Cela nécessite que l'agent de console soit déployé dans le même emplacement sur

site.

Vérifiez que la classification des données a accès aux volumes

Assurez-vous que la classification des données peut accéder aux volumes en vérifiant votre réseau, vos groupes de sécurité et vos politiques d'exportation. Vous devrez fournir à Data Classification les informations d'identification CIFS afin qu'il puisse accéder aux volumes CIFS.

Liste de contrôle

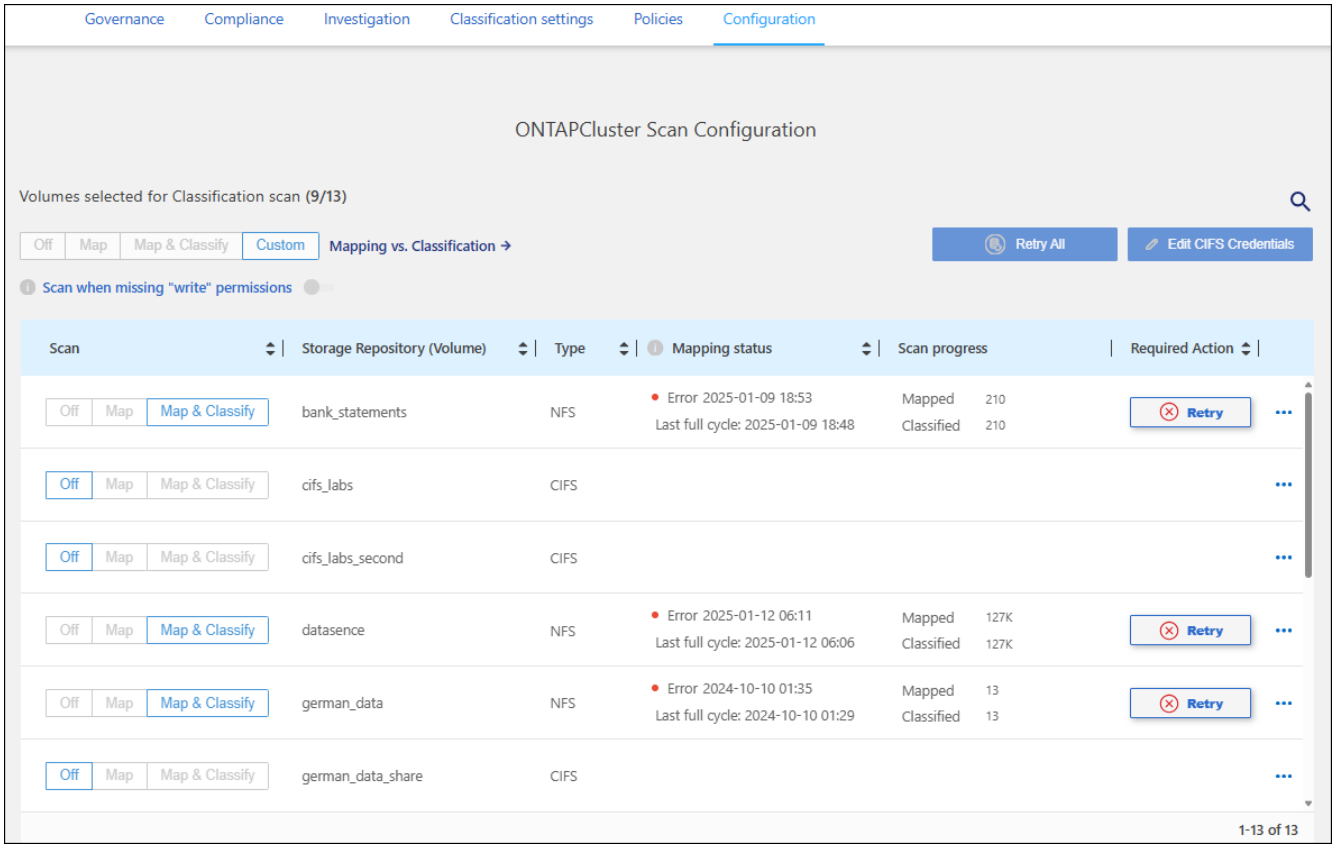
- Assurez-vous qu'il existe une connexion réseau entre l'instance de classification des données et chaque réseau qui inclut des volumes pour les clusters Cloud Volumes ONTAP ou ONTAP sur site.
- Assurez-vous que le groupe de sécurité pour Cloud Volumes ONTAP autorise le trafic entrant depuis l'instance de classification des données.

  Vous pouvez soit ouvrir le groupe de sécurité pour le trafic provenant de l'adresse IP de l'instance de classification des données, soit ouvrir le groupe de sécurité pour tout le trafic provenant de l'intérieur du réseau virtuel.

- Assurez-vous que les stratégies d'exportation de volume NFS incluent l'adresse IP de l'instance de classification des données afin qu'elle puisse accéder aux données sur chaque volume.

Étapes

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



2. Si vous utilisez CIFS, fournissez à Data Classification les informations d'identification Active Directory afin qu'il puisse analyser les volumes CIFS. Pour chaque système, sélectionnez **Modifier les informations d'identification CIFS** et saisissez le nom d'utilisateur et le mot de passe dont Data Classification a besoin pour accéder aux volumes CIFS sur le système.

Les informations d'identification peuvent être en lecture seule, mais la fourniture d'informations d'identification d'administrateur garantit que la classification des données peut lire toutes les données nécessitant des autorisations élevées. Les informations d'identification sont stockées sur l'instance de classification des données.

Si vous souhaitez vous assurer que les « dernières heures d'accès » de vos fichiers ne sont pas modifiées par les analyses de classification des données, il est recommandé que l'utilisateur dispose des autorisations d'écriture d'attributs dans CIFS ou des autorisations d'écriture dans NFS. Si possible, configurez l'utilisateur Active Directory en tant que membre d'un groupe parent de l'organisation disposant d'autorisations sur tous les fichiers.

Si vous avez correctement saisi les informations d'identification, un message confirme que tous les volumes CIFS ont été authentifiés avec succès.

3. Sur la page Configuration, sélectionnez **Configuration** pour vérifier l'état de chaque volume CIFS et NFS et corriger les erreurs éventuelles.

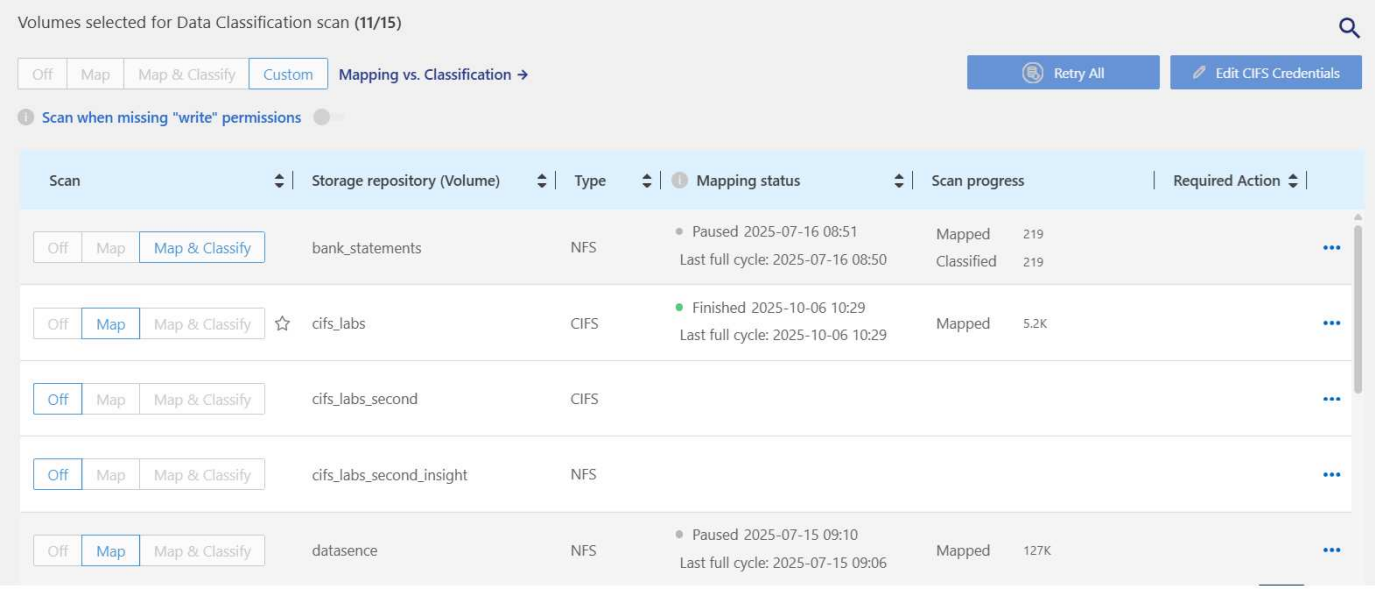
Activer ou désactiver les analyses sur les volumes

Vous pouvez démarrer ou arrêter les analyses sur n'importe quel système à tout moment à partir de la page de configuration. Vous pouvez également passer d'analyses de cartographie uniquement à des analyses de cartographie et de classification, et vice-versa. Il est recommandé d'analyser tous les volumes d'un système.

Les nouveaux volumes ajoutés au système sont automatiquement analysés uniquement lorsque vous avez sélectionné le paramètre **Carte** ou **Carte et classification** dans la zone d'en-tête. Lorsque cette option est définie sur **Personnalisé** ou **Désactivé** dans la zone d'en-tête, vous devrez activer le mappage et/ou l'analyse complète sur chaque nouveau volume que vous ajoutez au système.

Le commutateur en haut de la page pour **Analyser en cas d'absence d'autorisations « d'écriture »** est désactivé par défaut. Cela signifie que si Data Classification ne dispose pas d'autorisations d'attributs d'écriture dans CIFS ou d'autorisations d'écriture dans NFS, le système n'analysera pas les fichiers car Data Classification ne peut pas rétablir l'« heure du dernier accès » à l'horodatage d'origine. Si vous ne vous souciez pas de savoir si la dernière heure d'accès est réinitialisée, activez l'interrupteur et tous les fichiers sont analysés quelles que soient les autorisations. "Apprendre encore plus".

Les nouveaux volumes ajoutés au système sont automatiquement analysés uniquement lorsque vous avez défini le paramètre **Carte** ou **Carte et classification** dans la zone d'en-tête. Lorsque le paramètre pour tous les volumes est **Personnalisé** ou **Désactivé**, vous devez activer l'analyse manuellement pour chaque nouveau volume que vous ajoutez.



Étapes

1. Dans le menu Classification des données, sélectionnez **Configuration**.
2. Choisissez un système, puis sélectionnez **Configuration**.
3. Pour activer ou désactiver les analyses pour tous les volumes, sélectionnez **Map**, **Map & Classify** ou **Off** dans l'en-tête au-dessus de tous les volumes.

   Pour activer ou désactiver les analyses de volumes individuels, recherchez les volumes dans la liste, puis sélectionnez **Map**, **Map & Classify** ou **Off** à côté du nom du volume.

Résultat

Lorsque vous activez l'analyse, la classification des données démarre l'analyse des volumes que vous avez sélectionnés dans le système. Les résultats commencent à apparaître dans le tableau de bord Conformité dès que la classification des données démarre l'analyse. Le temps d'exécution de l'analyse dépend de la quantité de données, allant de quelques minutes à quelques heures.

La classification des données analyse un seul partage de fichiers sous un volume. Si vous avez plusieurs partages dans vos volumes, vous devrez analyser ces autres partages séparément en tant que groupe de partages. "Voir plus de détails sur cette limitation de classification des données" .

Analyser les schémas de base de données avec la NetApp Data Classification

Suivez quelques étapes pour commencer à analyser vos schémas de base de données avec NetApp Data Classification.

Réviser les prérequis

Passez en revue les conditions préalables suivantes pour vous assurer que vous disposez d'une configuration prise en charge avant d'activer la classification des données.

Bases de données prises en charge

La classification des données peut analyser les schémas des bases de données suivantes :

- Service de base de données relationnelle Amazon (Amazon RDS)
- MongoDB
- MySQL
- Oracle
- PostgreSQL
- SAP HANA
- Serveur SQL (MSSQL)

La fonctionnalité de collecte de statistiques **doit être activée** dans la base de données.

Exigences relatives à la base de données

Toute base de données connectée à l'instance de classification des données peut être analysée, quel que soit l'endroit où elle est hébergée. Vous avez juste besoin des informations suivantes pour vous connecter à la base de données :

- Adresse IP ou nom d'hôte
- Port
- Nom du service (uniquement pour l'accès aux bases de données Oracle)
- Informations d'identification permettant l'accès en lecture aux schémas

  Lors du choix d'un nom d'utilisateur et d'un mot de passe, il est important d'en choisir un qui dispose de toutes les autorisations de lecture sur tous les schémas et tables que vous souhaitez analyser. Nous vous recommandons de créer un utilisateur dédié au système de classification des données avec toutes les autorisations requises.

Pour MongoDB, un rôle d'administrateur en lecture seule est requis.

Déployer l'instance de classification des données

Déployez la classification des données s'il n'existe pas déjà d'instance déployée.

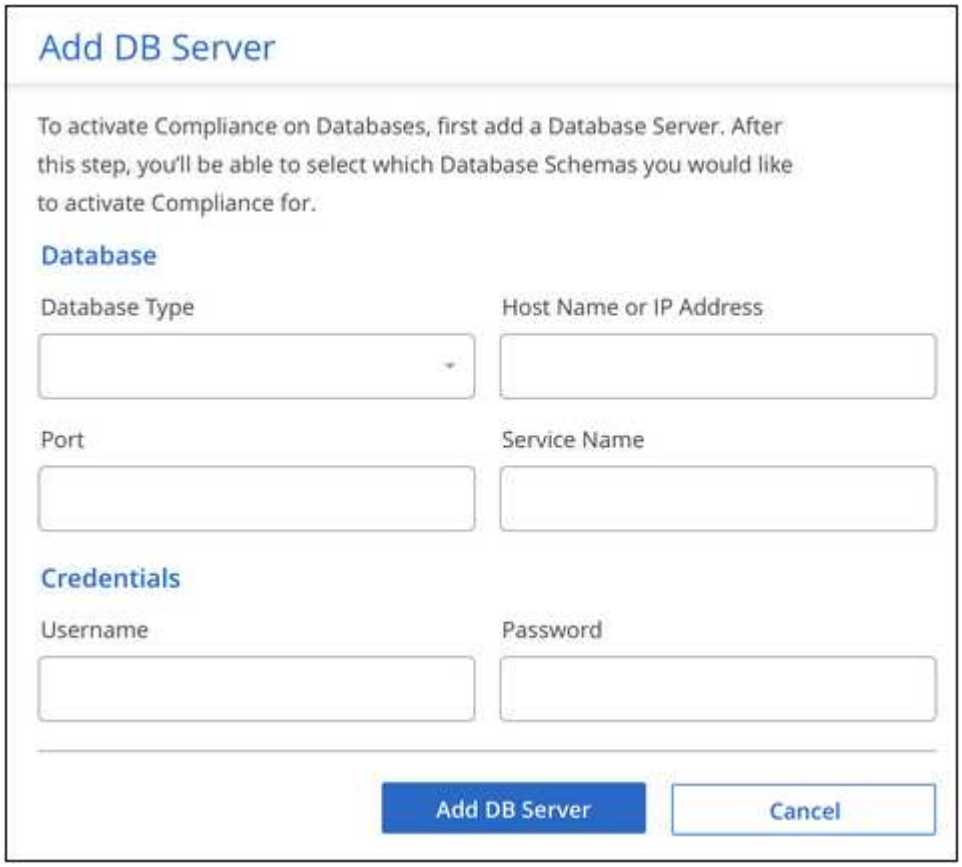
Si vous numérisez des schémas de bases de données accessibles sur Internet, vous pouvez"déployer la classification des données dans le cloud" ou"déployer la classification des données dans un emplacement sur site disposant d'un accès Internet" .

Si vous numérisez des schémas de base de données qui ont été installés sur un site sombre qui n'a pas d'accès Internet, vous devez"déployer la classification des données dans le même emplacement sur site qui n'a pas d'accès Internet" . Cela nécessite également que l'agent de console soit déployé dans le même emplacement sur site.

Ajouter le serveur de base de données

Ajoutez le serveur de base de données sur lequel résident les schémas.

1. Dans le menu Classification des données, sélectionnez **Configuration**.
2. Depuis la page Configuration, sélectionnez **Ajouter un système** > **Ajouter un serveur de base de données**.
3. Saisissez les informations requises pour identifier le serveur de base de données.
   a. Sélectionnez le type de base de données.
   b. Entrez le port et le nom d'hôte ou l'adresse IP pour vous connecter à la base de données.
   c. Pour les bases de données Oracle, entrez le nom du service.
   d. Saisissez les informations d'identification pour que Data Classification puisse accéder au serveur.
   e. Sélectionnez **Ajouter un serveur de base de données**.



La base de données est ajoutée à la liste des systèmes.

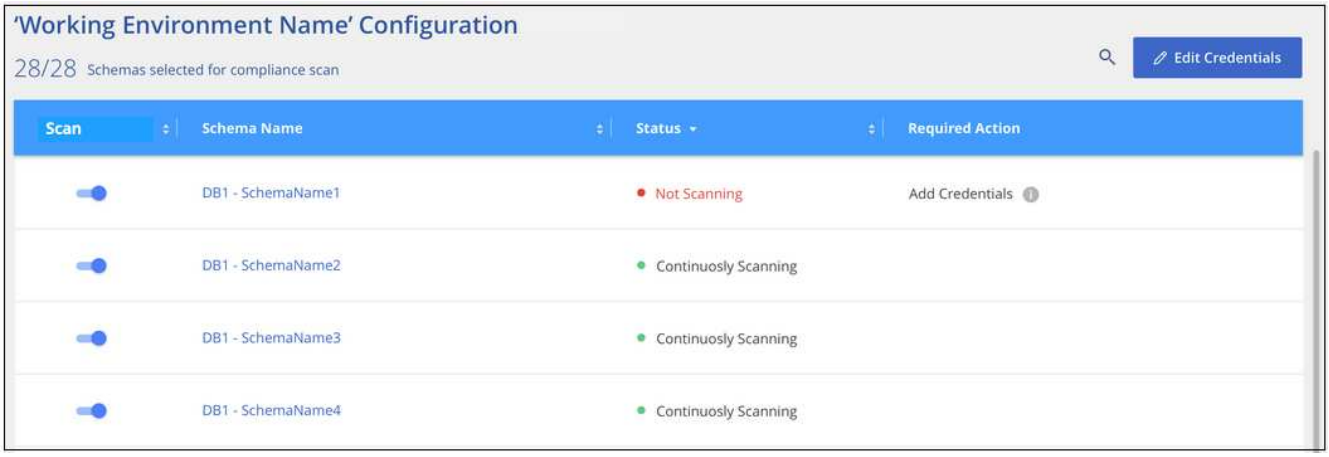
Activer et désactiver les analyses sur les schémas de base de données

Vous pouvez arrêter ou démarrer l'analyse complète de vos schémas à tout moment.

Il n'existe aucune option permettant de sélectionner des analyses de mappage uniquement pour les schémas de base de données.

1. Depuis la page Configuration, sélectionnez le bouton **Configuration** correspondant à la base de données que vous souhaitez configurer.

2. Sélectionnez les schémas que vous souhaitez analyser en déplaçant le curseur vers la droite.



Résultat

La classification des données commence à analyser les schémas de base de données que vous avez activés. Vous pouvez suivre la progression de l'analyse initiale en accédant au menu **Configuration** puis en sélectionnant la **Configuration système**. La progression de chaque analyse est affichée sous forme de barre de progression. Vous pouvez également survoler la barre de progression pour voir le nombre de fichiers analysés par rapport au nombre total de fichiers dans le volume. S'il y a des erreurs, elles apparaîtront dans la colonne Statut, à côté des actions requises pour corriger l'erreur.

Data Classification analyse vos bases de données une fois par jour ; les bases de données ne sont pas analysées en continu comme les autres sources de données.

Analyser les Google Cloud NetApp Volumes avec la NetApp Data Classification

NetApp Data Classification prend en charge Google Cloud NetApp Volumes en tant que système. Découvrez comment analyser votre système Google Cloud NetApp Volumes .

Découvrez le système Google Cloud NetApp Volumes que vous souhaitez analyser

Si le système Google Cloud NetApp Volumes que vous souhaitez analyser n'est pas déjà présent dans la NetApp Console en tant que système,"ajoutez-le à la page Systèmes" .

Déployer l’instance de classification des données

"Déployer la classification des données"s’il n’y a pas déjà une instance déployée.

La classification des données doit être déployée dans le cloud lors de l’analyse des Google Cloud NetApp Volumes et doit être déployée dans la même région que les volumes que vous souhaitez analyser.

Remarque : le déploiement de la classification des données dans un emplacement sur site n’est actuellement pas pris en charge lors de l’analyse des Google Cloud NetApp Volumes.

Activez la classification des données dans vos systèmes

Vous pouvez activer la classification des données sur votre système Google Cloud NetApp Volumes .

1. Dans le menu Classification des données, sélectionnez **Configuration**.
2. Sélectionnez la manière dont vous souhaitez analyser les volumes de chaque système. "En savoir plus sur les analyses de cartographie et de classification":
   - Pour mapper tous les volumes, sélectionnez **Mapper tous les volumes**.
   - Pour cartographier et classer tous les volumes, sélectionnez **Cartographier et classer tous les volumes**.
   - Pour personnaliser l’analyse de chaque volume, sélectionnez **Ou sélectionnez le type d’analyse pour chaque volume**, puis choisissez les volumes que vous souhaitez mapper et/ou classer.

     VoirActiver et désactiver les analyses sur les volumes pour plus de détails.
3. Dans la boîte de dialogue de confirmation, sélectionnez **Approuver**.

Résultat

La classification des données commence à analyser les volumes que vous avez sélectionnés dans le système. Les résultats sont disponibles dans le tableau de bord Conformité dès que la classification des données termine les analyses initiales. Le temps nécessaire dépend de la quantité de données : de quelques minutes à quelques heures. Vous pouvez suivre la progression de l’analyse initiale dans la section **Configuration système** du menu **Configuration**. La classification des données affiche une barre de progression pour chaque analyse. Vous pouvez également survoler la barre de progression pour voir le nombre de fichiers analysés par rapport au nombre total de fichiers dans le volume.

- Par défaut, si Data Classification ne dispose pas d’autorisations d’attributs d’écriture dans CIFS ou d’autorisations d’écriture dans NFS, le système n’analysera pas les fichiers de vos volumes car Data Classification ne peut pas rétablir l'« heure du dernier accès » à l’horodatage d’origine. Si vous ne vous souciez pas de savoir si la dernière heure d’accès est réinitialisée, sélectionnez **Ou sélectionnez le type d’analyse pour chaque volume**. La page résultante contient un paramètre que vous pouvez activer pour que la classification des données analyse les volumes quelles que soient les autorisations.
- La classification des données analyse un seul partage de fichiers sous un volume. Si vous avez plusieurs partages dans vos volumes, vous devez analyser ces autres partages séparément en tant que groupe de partages. "En savoir plus sur cette limitation de classification des données".

Vérifiez que la classification des données a accès aux volumes

Assurez-vous que la classification des données peut accéder aux volumes en vérifiant votre réseau, vos groupes de sécurité et vos politiques d’exportation. Pour les volumes CIFS, vous devez fournir une classification des données avec les informations d’identification CIFS.

Pour les Google Cloud NetApp Volumes, la classification des données ne peut analyser que les volumes situés dans la même région que la console.

Liste de contrôle

- Assurez-vous qu'il existe une connexion réseau entre l'instance de classification des données et chaque réseau qui inclut des volumes pour Google Cloud NetApp Volumes.
- Assurez-vous que les ports suivants sont ouverts sur l'instance de classification des données :
  - Pour NFS – ports 111 et 2049.
  - Pour CIFS – ports 139 et 445.
- Assurez-vous que les stratégies d'exportation de volume NFS incluent l'adresse IP de l'instance de classification des données afin qu'elle puisse accéder aux données sur chaque volume.

Étapes

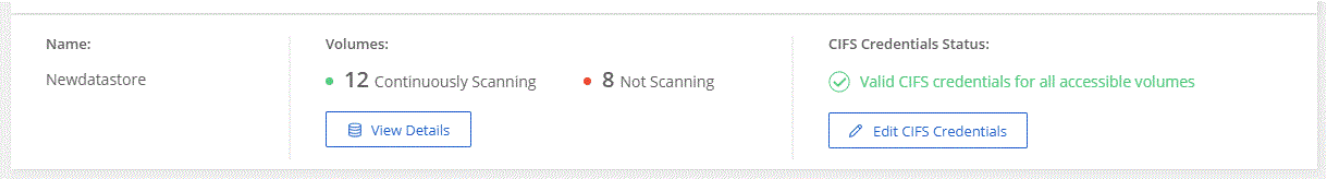
1. Dans le menu Classification des données, sélectionnez **Configuration**.

   a. Si vous utilisez CIFS (SMB), assurez-vous que les informations d'identification Active Directory sont correctes. Pour chaque système, sélectionnez **Modifier les informations d'identification CIFS**, puis saisissez le nom d'utilisateur et le mot de passe dont Data Classification a besoin pour accéder aux volumes CIFS sur le système.

      Les informations d'identification peuvent être en lecture seule, mais la fourniture d'informations d'identification d'administrateur garantit que la classification des données peut lire toutes les données nécessitant des autorisations élevées. Les informations d'identification sont stockées sur l'instance de classification des données.

      Si vous souhaitez vous assurer que les « dernières heures d'accès » de vos fichiers ne sont pas modifiées par les analyses de classification des données, il est recommandé que l'utilisateur dispose des autorisations d'écriture d'attributs dans CIFS ou des autorisations d'écriture dans NFS. Si possible, configurez l'utilisateur Active Directory en tant que membre d'un groupe parent de l'organisation disposant d'autorisations sur tous les fichiers.

      Après avoir saisi les informations d'identification, vous devriez voir un message indiquant que tous les volumes CIFS ont été authentifiés avec succès.



2. Sur la page Configuration, sélectionnez **Afficher les détails** pour vérifier l'état de chaque volume CIFS et NFS et corriger les erreurs éventuelles.

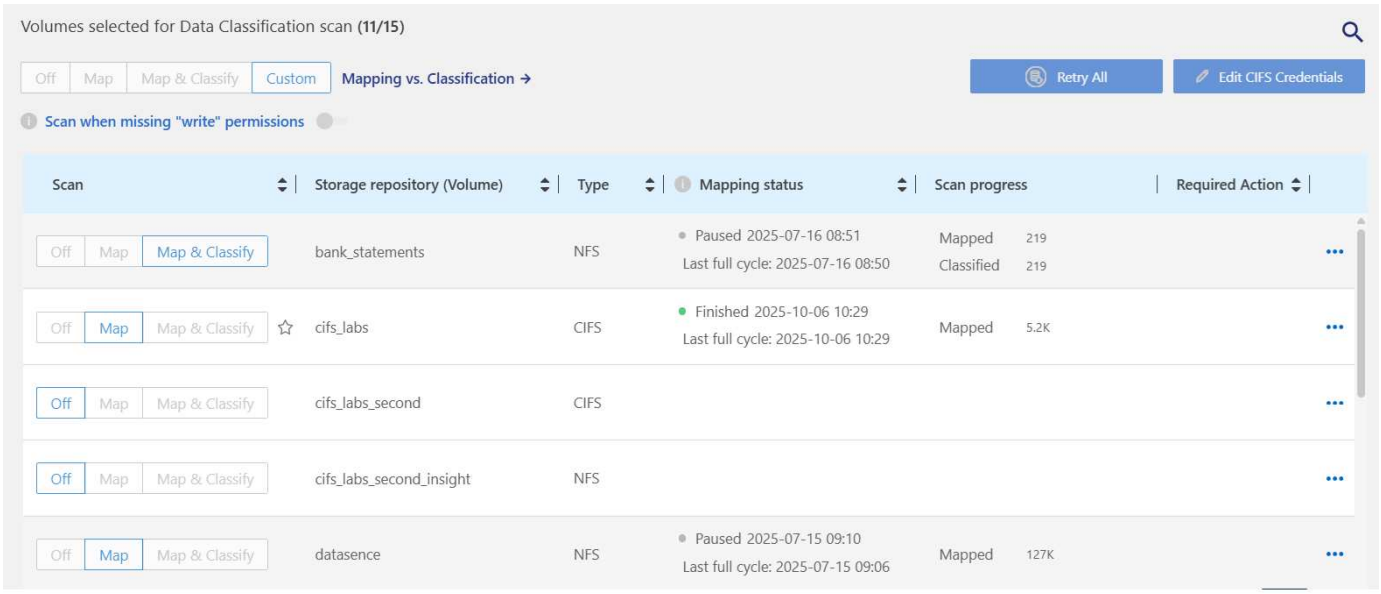
Activer et désactiver les analyses sur les volumes

Vous pouvez démarrer ou arrêter les analyses sur n'importe quel système à tout moment à partir de la page de configuration. Vous pouvez également passer d'analyses de cartographie uniquement à des analyses de cartographie et de classification, et vice-versa. Il est recommandé d'analyser tous les volumes d'un système.

Les nouveaux volumes ajoutés au système sont automatiquement analysés uniquement lorsque vous avez sélectionné le paramètre **Carte** ou **Carte et classification** dans la zone d'en-tête. Lorsque cette option est définie sur **Personnalisé** ou **Désactivé** dans la zone d'en-tête, vous devrez activer le mappage et/ou l'analyse complète sur chaque nouveau volume que vous ajoutez au système.

Le commutateur en haut de la page pour **Analyser en cas d'absence d'autorisations « d'écriture »** est désactivé par défaut. Cela signifie que si Data Classification ne dispose pas d'autorisations d'attributs d'écriture dans CIFS ou d'autorisations d'écriture dans NFS, le système n'analysera pas les fichiers car Data Classification ne peut pas rétablir l'« heure du dernier accès » à l'horodatage d'origine. Si vous ne vous souciez pas de savoir si la dernière heure d'accès est réinitialisée, activez l'interrupteur et tous les fichiers sont analysés quelles que soient les autorisations. "Apprendre encore plus".

Les nouveaux volumes ajoutés au système sont automatiquement analysés uniquement lorsque vous avez défini le paramètre **Carte** ou **Carte et classification** dans la zone d'en-tête. Lorsque le paramètre pour tous les volumes est **Personnalisé** ou **Désactivé**, vous devez activer l'analyse manuellement pour chaque nouveau volume que vous ajoutez.



Étapes

1. Dans le menu Classification des données, sélectionnez **Configuration**.
2. Choisissez un système, puis sélectionnez **Configuration**.
3. Pour activer ou désactiver les analyses pour tous les volumes, sélectionnez **Map**, **Map & Classify** ou **Off** dans l'en-tête au-dessus de tous les volumes.

   Pour activer ou désactiver les analyses de volumes individuels, recherchez les volumes dans la liste, puis sélectionnez **Map**, **Map & Classify** ou **Off** à côté du nom du volume.

Résultat

Lorsque vous activez l'analyse, la classification des données démarre l'analyse des volumes que vous avez sélectionnés dans le système. Les résultats commencent à apparaître dans le tableau de bord Conformité dès que la classification des données démarre l'analyse. Le temps d'exécution de l'analyse dépend de la quantité de données, allant de quelques minutes à quelques heures.

Analyser les partages de fichiers avec la NetApp Data Classification

Pour analyser les partages de fichiers, vous devez d'abord créer un groupe de partages de fichiers dans NetApp Data Classification. Les groupes de partages de fichiers sont destinés aux partages NFS ou CIFS (SMB) hébergés sur site ou dans le cloud.

L'analyse des données provenant de partages de fichiers non NetApp n'est pas prise en charge dans la version principale de la classification des données.

Prérequis

Passez en revue les conditions préalables suivantes pour vous assurer que vous disposez d'une configuration prise en charge avant d'activer la classification des données.

- Les actions peuvent être hébergées n'importe où, y compris dans le cloud ou sur site. Les partages CIFS des anciens systèmes de stockage NetApp 7-Mode peuvent être analysés en tant que partages de fichiers.
  - La classification des données ne peut pas extraire les autorisations ou la « dernière heure d'accès » des systèmes 7-Mode.
  - En raison d'un problème connu entre certaines versions Linux et les partages CIFS sur les systèmes 7-Mode, vous devez configurer le partage pour utiliser uniquement SMBv1 avec l'authentification NTLM activée.
- Une connectivité réseau est nécessaire entre l'instance de classification des données et les partages.
- Vous pouvez ajouter un partage DFS (Distributed File System) en tant que partage CIFS standard. Étant donné que la classification des données ne sait pas que le partage est basé sur plusieurs serveurs/volumes combinés en un seul partage CIFS, vous risquez de recevoir des erreurs d'autorisation ou de connectivité concernant le partage lorsque le message s'applique réellement uniquement à l'un des dossiers/partages situés sur un serveur/volume différent.
- Pour les partages CIFS (SMB), assurez-vous que vous disposez des informations d'identification Active Directory qui fournissent un accès en lecture aux partages. Les informations d'identification d'administrateur sont préférables au cas où la classification des données doit analyser des données nécessitant des autorisations élevées.

  Si vous souhaitez vous assurer que les « dernières heures d'accès » de vos fichiers ne sont pas modifiées par les analyses de classification des données, il est recommandé que l'utilisateur dispose des autorisations d'écriture d'attributs dans CIFS ou des autorisations d'écriture dans NFS. Si possible, configurez l'utilisateur Active Directory en tant que membre d'un groupe parent de l'organisation disposant d'autorisations sur tous les fichiers.

- Tous les partages de fichiers CIFS d'un groupe doivent utiliser les mêmes informations d'identification Active Directory.
- Vous pouvez mélanger les partages NFS et CIFS (en utilisant Kerberos ou NTLM). Vous devez ajouter les actions au groupe séparément. Autrement dit, vous devez effectuer le processus deux fois, une fois par protocole.
  - Vous ne pouvez pas créer un groupe de partage de fichiers qui mélange les types d'authentification CIFS (Kerberos et NTLM).
- Si vous utilisez CIFS avec l'authentification Kerberos, assurez-vous que l'adresse IP fournie est accessible

à la classification des données. Les partages de fichiers ne peuvent pas être ajoutés si l'adresse IP est inaccessible.

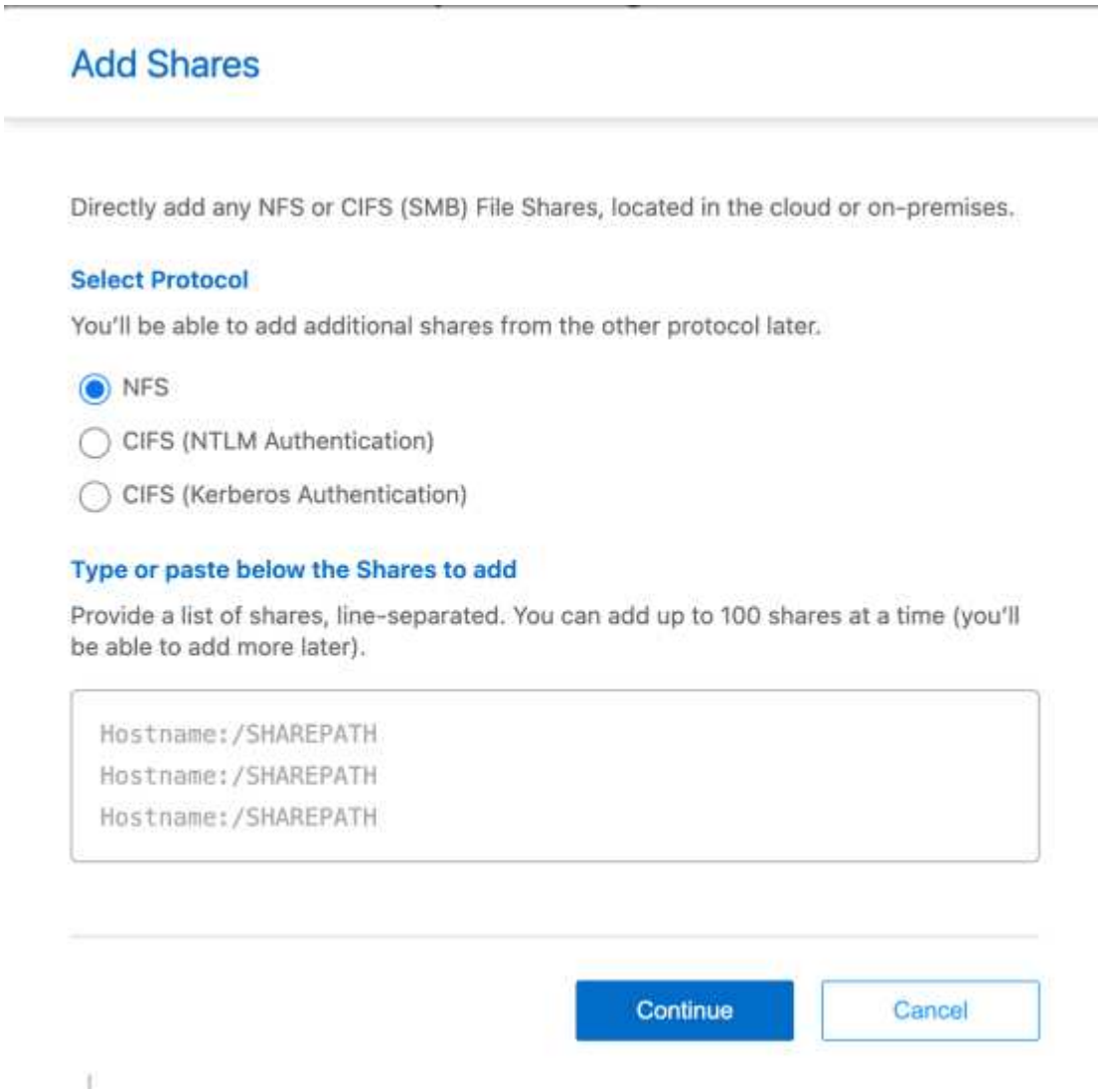
Créer un groupe de partage de fichiers

Lorsque vous ajoutez des partages de fichiers au groupe, vous devez utiliser le format `<host_name>:/<share_path>`.

Vous pouvez ajouter des partages de fichiers individuellement ou saisir une liste séparée par des lignes des partages de fichiers que vous souhaitez analyser. Vous pouvez ajouter jusqu'à 100 actions à la fois.

Étapes

1. Dans le menu Classification des données, sélectionnez **Configuration**.
2. Depuis la page Configuration, sélectionnez **Ajouter un système** > **Ajouter un groupe de partages de fichiers**.
3. Dans la boîte de dialogue Ajouter un groupe de partages de fichiers, saisissez le nom du groupe de partages, puis sélectionnez **Continuer**.
4. Sélectionnez le protocole pour les partages de fichiers que vous ajoutez.



a. Si vous ajoutez des partages CIFS avec l'authentification NTLM, entrez les informations d'identification

Active Directory pour accéder aux volumes CIFS. Bien que les informations d'identification en lecture seule soient prises en charge, il est recommandé de fournir un accès complet avec les informations d'identification d'administrateur. Sélectionnez **Enregistrer**.

5. Ajoutez les partages de fichiers que vous souhaitez analyser (un partage de fichiers par ligne). Sélectionnez ensuite **Continuer**.
6. Une boîte de dialogue de confirmation affiche le nombre de partages qui ont été ajoutés.

   Si la boîte de dialogue répertorie des partages qui n'ont pas pu être ajoutés, capturez ces informations afin de pouvoir résoudre le problème. Si le problème concerne une convention de dénomination, vous pouvez rajouter le partage avec un nom corrigé.

7. Configurer l'analyse sur le volume :
   - Pour activer les analyses de mappage uniquement sur les partages de fichiers, sélectionnez **Map**.
   - Pour activer les analyses complètes sur les partages de fichiers, sélectionnez **Mappez et classez**.
   - Pour désactiver l'analyse sur les partages de fichiers, sélectionnez **Désactivé**.

> Le commutateur en haut de la page pour **Analyser lorsque les autorisations « attributs d'écriture » sont manquantes** est désactivé par défaut. Cela signifie que si Data Classification ne dispose pas d'autorisations d'attributs d'écriture dans CIFS ou d'autorisations d'écriture dans NFS, le système n'analysera pas les fichiers car Data Classification ne peut pas rétablir l'« heure du dernier accès » à l'horodatage d'origine. + Si vous activez **Analyser en cas d'absence d'autorisations « attributs d'écriture »**, l'analyse réinitialise l'heure du dernier accès et analyse tous les fichiers, quelles que soient les autorisations. + Pour en savoir plus sur l'horodatage du dernier accès, voir"Métadonnées collectées à partir de sources de données dans la classification des données" .

Résultat

La classification des données commence à analyser les fichiers dans les partages de fichiers que vous avez ajoutés. Tu peuxSuivre la progression de la numérisation et afficher les résultats de l'analyse dans le **Tableau de bord**.

> Si l'analyse ne se termine pas correctement pour une configuration CIFS avec authentification Kerberos, vérifiez l'onglet **Configuration** pour détecter d'éventuelles erreurs.

Modifier un groupe de partage de fichiers

Après avoir créé un groupe de partages de fichiers, vous pouvez modifier le protocole CIFS ou ajouter et supprimer des partages de fichiers.

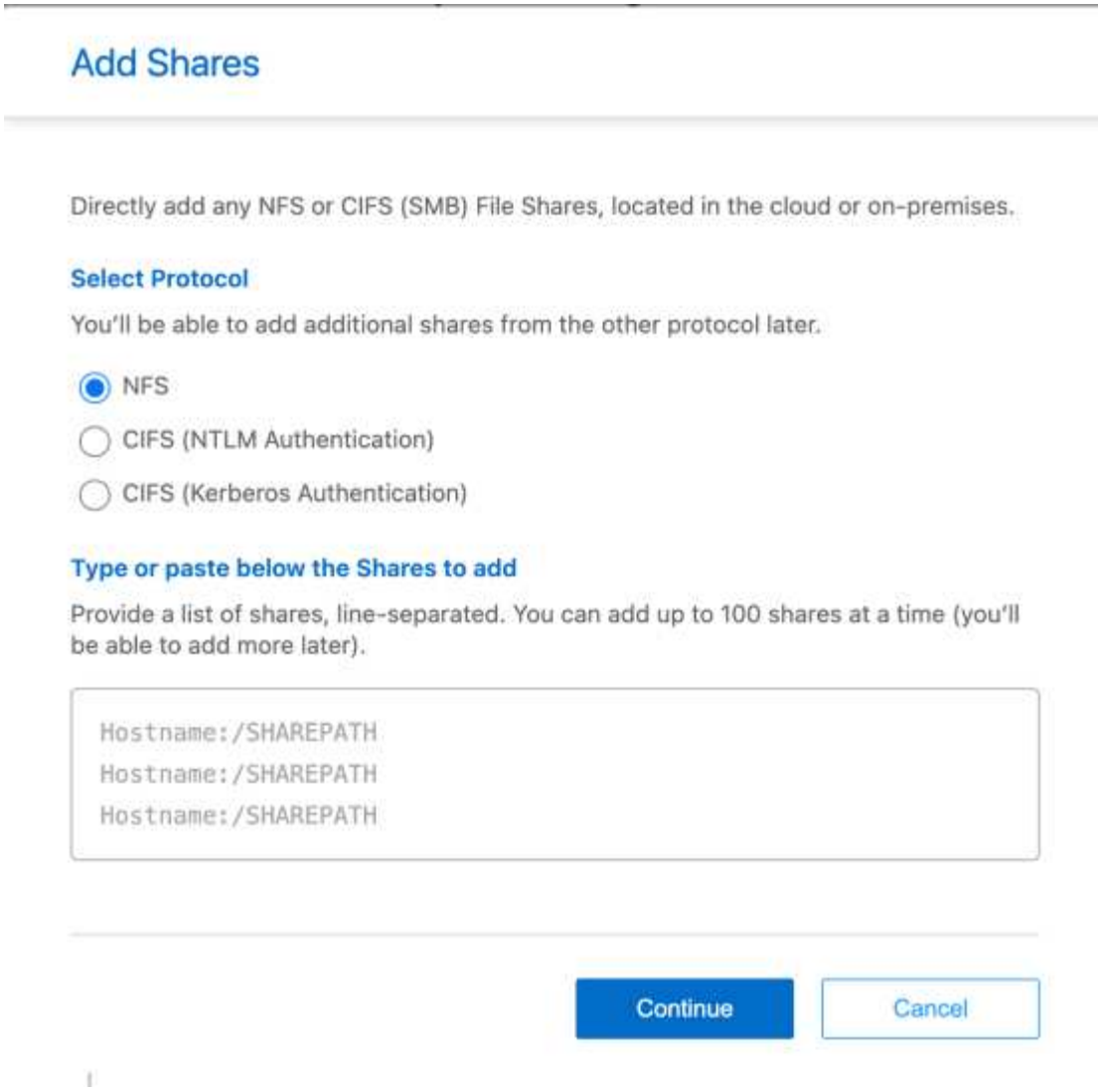
Modifier la configuration du protocole CIFS

1. Dans le menu Classification des données, sélectionnez **Configuration**.
2. Depuis la page Configuration, sélectionnez le groupe de partages de fichiers que vous souhaitez modifier.
3. Sélectionnez **Modifier les informations d'identification CIFS**.

4. Choisissez la méthode d'authentification : **NTLM** ou **Kerberos**.
5. Saisissez le **Nom d'utilisateur** et le **Mot de passe** d'Active Directory.
6. Sélectionnez **Enregistrer** pour terminer le processus.

Ajouter des partages de fichiers aux analyses

1. Dans le menu Classification des données, sélectionnez **Configuration**.
2. Depuis la page Configuration, sélectionnez le groupe de partages de fichiers que vous souhaitez modifier.
3. Sélectionnez **+ Ajouter des partages**.
4. Sélectionnez le protocole pour les partages de fichiers que vous ajoutez.



Si vous ajoutez des partages de fichiers à un protocole que vous avez déjà configuré, aucune modification n'est requise.

Si vous ajoutez des partages de fichiers avec un deuxième protocole, assurez-vous d'avoir correctement configuré l'authentification comme détaillé dans le"prérequis" .

5. Ajoutez les partages de fichiers que vous souhaitez analyser (un partage de fichiers par ligne) en utilisant le format `<host_name>:/<share_path>` .
6. Sélectionnez **Continuer** pour terminer l'ajout des partages de fichiers.

Supprimer un partage de fichiers des analyses

1. Dans le menu Classification des données, sélectionnez **Configuration**.
2. Sélectionnez le système dont vous souhaitez supprimer les partages de fichiers.
3. Sélectionnez **Configuration**.
4. Depuis la page Configuration, sélectionnez les Actions ••• pour le partage de fichiers que vous souhaitez supprimer.
5. Dans le menu Actions, sélectionnez **Supprimer le partage**.

Suivre la progression de la numérisation

Vous pouvez suivre la progression de l'analyse initiale.

1. Sélectionnez le menu **Configuration**.
2. Sélectionnez la **Configuration système**.
3. Pour le référentiel de stockage, vérifiez la colonne Progression de l'analyse pour afficher son état.

Analyser les données StorageGRID avec la NetApp Data Classification

Suivez quelques étapes pour commencer à analyser les données dans StorageGRID directement avec NetApp Data Classification.

Examiner les exigences de StorageGRID

Passez en revue les conditions préalables suivantes pour vous assurer que vous disposez d'une configuration prise en charge avant d'activer la classification des données.

- Vous devez disposer de l'URL du point de terminaison pour vous connecter au service de stockage d'objets.
- Vous devez disposer de la clé d'accès et de la clé secrète de StorageGRID afin que la classification des données puisse accéder aux buckets.

Déployer l'instance de classification des données

Déployez la classification des données s'il n'existe pas déjà d'instance déployée.

Si vous numérisez des données de StorageGRID accessibles sur Internet, vous pouvez"déployer la classification des données dans le cloud" ou"déployer la classification des données dans un emplacement sur site disposant d'un accès Internet" .

Si vous numérisez des données à partir de StorageGRID qui a été installé sur un site sombre qui n'a pas d'accès Internet, vous devez"déployer la classification des données dans le même emplacement sur site qui n'a pas d'accès Internet" . Cela nécessite également que l'agent de console soit déployé dans le même emplacement sur site.

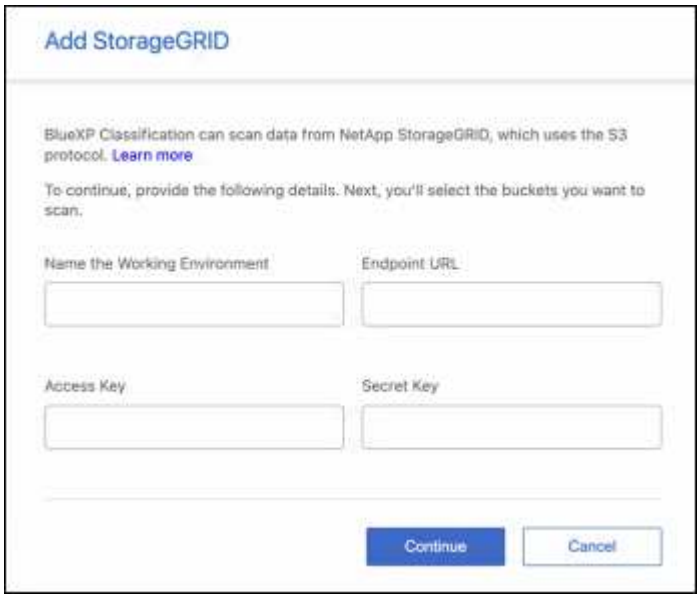
Ajoutez le service StorageGRID à la classification des données

Ajoutez le service StorageGRID .

Étapes

1. Dans le menu Classification des données, sélectionnez l'option **Configuration**.
2. Depuis la page Configuration, sélectionnez **Ajouter un système** > **Ajouter StorageGRID**.
3. Dans la boîte de dialogue Ajouter un service StorageGRID , saisissez les détails du service StorageGRID et sélectionnez **Continuer**.
   a. Entrez le nom que vous souhaitez utiliser pour le système. Ce nom doit refléter le nom du service StorageGRID auquel vous vous connectez.
   b. Saisissez l'URL du point de terminaison pour accéder au service de stockage d'objets.

c. Saisissez la clé d'accès et la clé secrète afin que la classification des données puisse accéder aux buckets dans StorageGRID.



Résultat

StorageGRID est ajouté à la liste des systèmes.

Activer et désactiver les analyses sur les buckets StorageGRID

Après avoir activé la classification des données sur StorageGRID, l'étape suivante consiste à configurer les buckets que vous souhaitez analyser. La classification des données découvre ces compartiments et les affiche dans le système que vous avez créé.

Étapes

1. Dans la page Configuration, recherchez le système StorageGRID .
2. Sur la mosaïque système StorageGRID , sélectionnez **Configuration**.
3. Effectuez l'une des étapes suivantes pour activer ou désactiver l'analyse :
   - Pour activer les analyses de mappage uniquement sur un bucket, sélectionnez **Carte**.
   - Pour activer les analyses complètes sur un bucket, sélectionnez **Cartographier et classer**.
   - Pour désactiver l'analyse sur un bucket, sélectionnez **Désactivé**.

Résultat

La classification des données commence à analyser les compartiments que vous avez activés. Vous pouvez suivre la progression de l'analyse initiale en accédant au menu **Configuration** puis en sélectionnant la **Configuration système**. La progression de chaque analyse est affichée sous forme de barre de progression. Vous pouvez également survoler la barre de progression pour voir le nombre de fichiers analysés par rapport au nombre total de fichiers dans le volume. S'il y a des erreurs, elles apparaîtront dans la colonne Statut, à côté de l'action requise pour corriger l'erreur.