



Activez la numérisation sur vos sources de données

Cloud Data Sense

NetApp
December 12, 2022

Table des matières

- Activez la numérisation sur vos sources de données 1
 - Mise en route de Cloud Data Sense pour Cloud Volumes ONTAP et ONTAP sur site 1
 - Mise en route de Cloud Data Sense for Azure NetApp Files 7
 - Lancez-vous avec Cloud Data Sense for Amazon FSX pour ONTAP 12
 - Mise en route de Cloud Data Sense pour Amazon S3 17
 - Analyse des schémas de base de données 25
 - En analysant les comptes OneDrive 28
 - Analyse des comptes SharePoint 32
 - Numérisation de comptes Google Drive 37
 - Analyse des partages de fichiers 39
 - Analyse du stockage objet à l'aide du protocole S3 44

Activez la numérisation sur vos sources de données

Mise en route de Cloud Data Sense pour Cloud Volumes ONTAP et ONTAP sur site

Procédez comme suit pour commencer à analyser les volumes ONTAP Cloud Volumes ONTAP et sur site à l'aide de Cloud Data SENSE.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

Découvrez les sources de données que vous souhaitez analyser

Avant de pouvoir numériser des volumes, vous devez ajouter les systèmes en tant qu'environnements de travail dans BlueXP :

- Pour les systèmes Cloud Volumes ONTAP, ces environnements de travail devraient déjà être disponibles dans BlueXP
- Pour les systèmes ONTAP sur site, ["BlueXP doit découvrir les clusters ONTAP"](#)

2

Déployez l'instance Cloud Data SENSE

["Déployez des données adaptées au cloud"](#) si aucune instance n'est déjà déployée.

3

Activez Cloud Data SENSE et sélectionnez les volumes à analyser

Cliquez sur **Data Sense**, sélectionnez l'onglet **Configuration** et activez les analyses de conformité pour les volumes dans des environnements de travail spécifiques.

4

Vérifiez l'accès aux volumes

Lorsque Cloud Data SENSE est activé, assurez-vous qu'il peut accéder à tous les volumes.

- L'instance Cloud Data Sense doit être connectée réseau à chaque sous-réseau Cloud Volumes ONTAP ou système ONTAP sur site.
- Les groupes de sécurité pour Cloud Volumes ONTAP doivent autoriser les connexions entrantes à partir de l'instance de détection de données.
- Assurez-vous que ces ports sont ouverts à l'instance de détection de données :
 - Pour NFS – ports 111 et 2049.
 - Pour CIFS – ports 139 et 445.
- Les règles d'exportation de volumes NFS doivent autoriser l'accès à partir de l'instance Data Sense.

- La détection de données a besoin des identifiants Active Directory pour analyser les volumes CIFS.

Cliquez sur **Compliance > Configuration > Modifier les informations d'identification CIFS** et fournissez les informations d'identification.

5

Gérer les volumes à analyser

Sélectionnez ou désélectionnez les volumes que vous souhaitez scanner et Cloud Data SENSE démarre ou arrête l'acquisition.

Recherche des sources de données que vous souhaitez analyser

Si les sources de données que vous souhaitez numériser ne se trouvent pas déjà dans votre environnement BlueXP, vous pouvez les ajouter au canevas pour le moment.

Vos systèmes Cloud Volumes ONTAP devraient déjà être disponibles dans la zone de travail de BlueXP. Dont vous avez besoin avec les systèmes ONTAP sur site "[BlueXP découvre ces clusters](#)".

Déploiement de l'instance Cloud Data Sense

Déployez Cloud Data si aucune instance n'est déjà déployée.

Si vous numérisez des systèmes Cloud Volumes ONTAP et ONTAP sur site accessibles via Internet, vous pouvez "[Déployez les données du cloud dans le cloud](#)" ou "[dans un emplacement sur site avec accès à internet](#)".

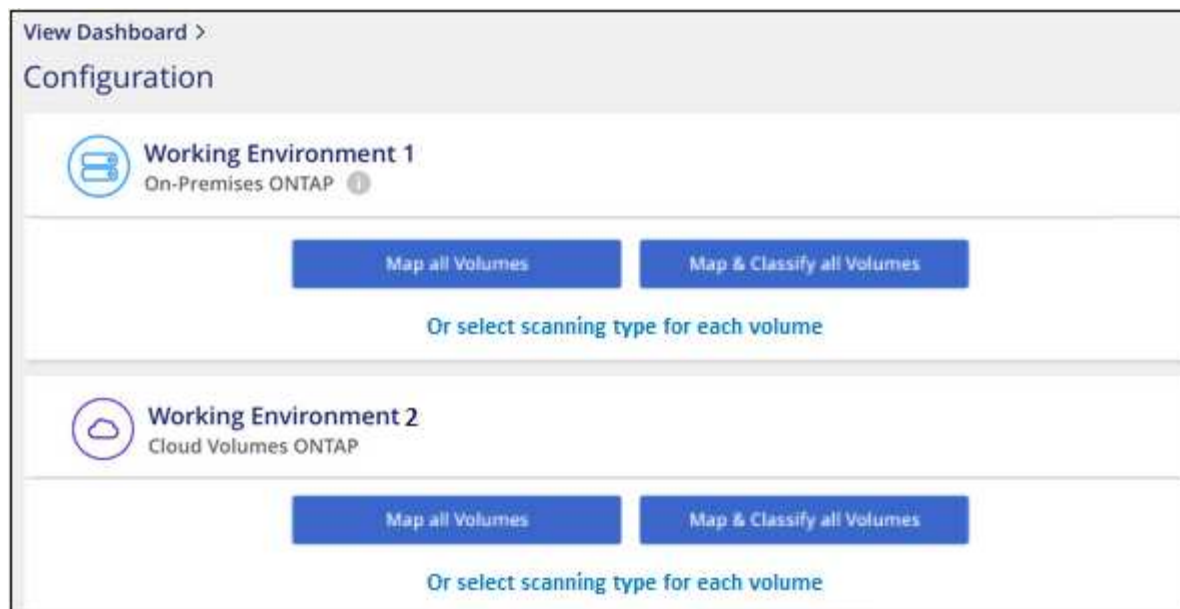
Si vous numérisez des systèmes ONTAP sur site qui ont été installés sur un site sombre et ne disposant pas d'accès à Internet, vous devez le faire "[Déployez les données cloud sur site qui ne disposent pas d'un accès Internet](#)". Cela nécessite également que le connecteur BlueXP soit déployé dans le même emplacement sur site.

Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

Activation des données cloud dans vos environnements de travail

Vous pouvez activer Cloud Data Sense sur les systèmes Cloud Volumes ONTAP dans n'importe quel fournisseur cloud pris en charge et dans des clusters ONTAP sur site.

1. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**, puis sélectionnez l'onglet **Configuration**.



2. Sélectionnez le mode de numérisation des volumes dans chaque environnement de travail. "[En savoir plus sur les acquisitions de mappage et de classification](#)":

- Pour mapper tous les volumes, cliquez sur **mapper tous les volumes**.
- Pour mapper et classer tous les volumes, cliquez sur **cartographier et classer tous les volumes**.
- Pour personnaliser la numérisation de chaque volume, cliquez sur **ou sélectionnez le type de numérisation pour chaque volume**, puis choisissez les volumes que vous souhaitez mapper et/ou classer.

Voir [Activation et désactivation des analyses de conformité sur les volumes](#) pour plus d'informations.

3. Dans la boîte de dialogue de confirmation, cliquez sur **approuver** pour que Data Sense commence à analyser vos volumes.

Résultat

Cloud Data SENSE commence à analyser les volumes que vous avez sélectionnés dans l'environnement de travail. Les résultats seront disponibles dans le tableau de bord de conformité dès que Cloud Data SENSE aura terminé les analyses initiales. Le temps nécessaire dépend de la quantité de données—il peut être de quelques minutes ou heures.

Vérifier que le sens des données cloud a accès aux volumes

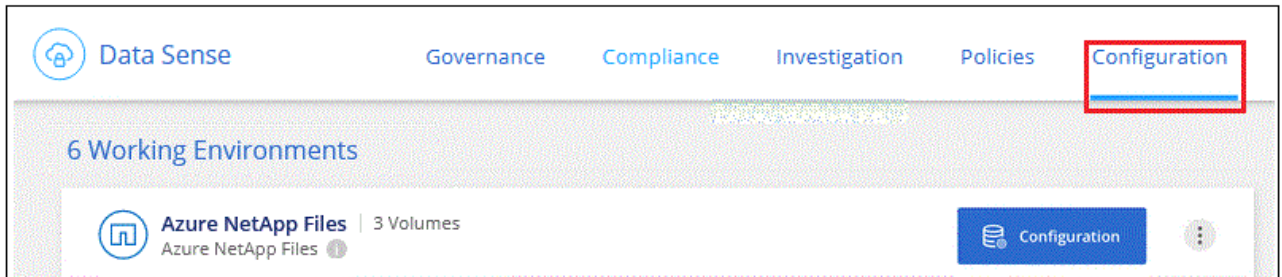
Assurez-vous que Cloud Data est capable d'accéder aux volumes en vérifiant vos groupes de sécurité et vos règles d'exportation. Vous devez fournir un « logique de données » avec des identifiants CIFS pour pouvoir accéder aux volumes CIFS.

Étapes

1. Assurez-vous qu'il existe une connexion réseau entre l'instance Cloud Data Sense et chaque réseau incluant des volumes pour les clusters Cloud Volumes ONTAP ou ONTAP sur site.
2. Assurez-vous que le groupe de sécurité pour Cloud Volumes ONTAP autorise le trafic entrant à partir de l'instance de détection de données.

Vous pouvez soit ouvrir le groupe de sécurité pour le trafic à partir de l'adresse IP de l'instance de détection de données, soit ouvrir le groupe de sécurité pour tout le trafic à partir du réseau virtuel.

3. Assurez-vous que les ports suivants sont ouverts à l'instance de détection de données :
 - Pour NFS – ports 111 et 2049.
 - Pour CIFS – ports 139 et 445.
4. Assurez-vous que les règles d'exportation de volume NFS incluent l'adresse IP de l'instance Data Sense afin qu'elle puisse accéder aux données sur chaque volume.
5. Si vous utilisez le protocole CIFS, fournissez Data Sense avec des identifiants Active Directory afin qu'il puisse analyser les volumes CIFS.
 - a. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**, puis sélectionnez l'onglet **Configuration**.

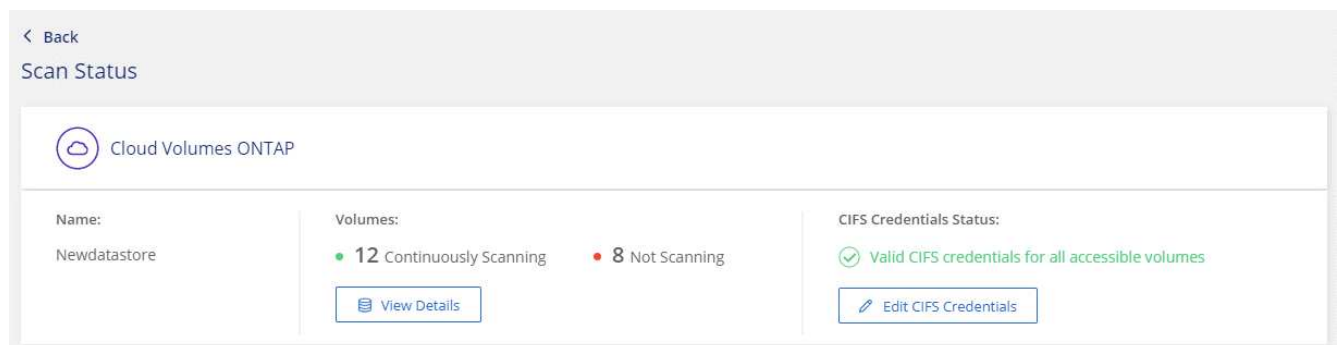


- b. Pour chaque environnement de travail, cliquez sur **Modifier les informations d'identification CIFS** et entrez le nom d'utilisateur et le mot de passe dont Data Sense a besoin pour accéder aux volumes CIFS sur le système.

Les informations d'identification peuvent être en lecture seule, mais fournir des informations d'identification admin garantit que Data Sense peut lire toutes les données qui requièrent des autorisations élevées. Les identifiants sont stockés sur l'instance Cloud Data Sense.

Si vous voulez vous assurer que vos fichiers “dernières heures d'accès” sont inchangés par les analyses de classification de détection de données, nous recommandons à l'utilisateur de disposer de l'autorisation Write Attributes. Si possible, nous vous recommandons de faire en sorte que l'utilisateur configuré Active Directory fasse partie d'un groupe parent de l'organisation qui dispose des autorisations pour tous les fichiers.

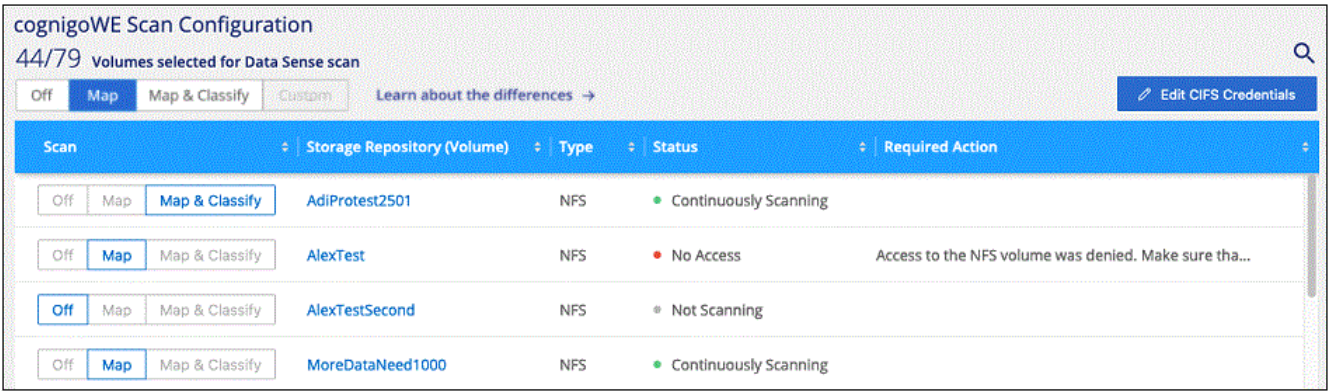
Une fois les informations d'identification saisies, un message indiquant que tous les volumes CIFS ont été authentifiés avec succès s'affiche.



6. Sur la page *Configuration*, cliquez sur **View Details** pour vérifier l'état de chaque volume CIFS et NFS et corriger les erreurs éventuelles.

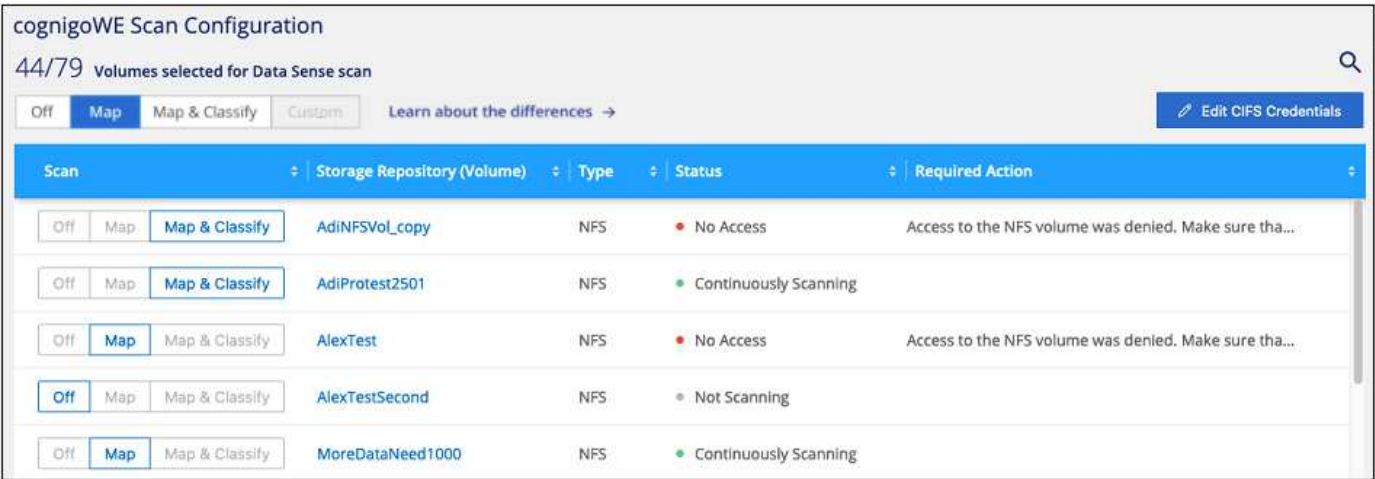
L'image suivante montre par exemple quatre volumes dont l'un des types de données cloud n'est pas capable de se scanner en raison de problèmes de connectivité réseau entre l'instance Data Sense et le

volume.



Activation et désactivation des analyses de conformité sur les volumes

Vous pouvez démarrer ou arrêter des analyses de mappage uniquement, ou des analyses de mappage et de classification, dans un environnement de travail à tout moment à partir de la page Configuration. Vous pouvez également passer des acquisitions avec mappage uniquement à des acquisitions avec mappage et classification, et inversement. Nous vous recommandons de scanner tous les volumes.



À :	Procédez comme suit :
Activez les acquisitions avec mappage uniquement sur un volume	Dans la zone du volume, cliquez sur Map
Activer la numérisation complète sur un volume	Dans la zone de volume, cliquez sur carte et classement
Désactiver la numérisation sur un volume	Dans la zone du volume, cliquez sur Off
Activez les analyses de mappage uniquement sur tous les volumes	Dans la zone d'en-tête, cliquez sur carte
Activez l'analyse complète sur tous les volumes	Dans la zone d'en-tête, cliquez sur carte et classement
Désactiver l'analyse de tous les volumes	Dans la zone d'en-tête, cliquez sur Off



Les nouveaux volumes ajoutés à l'environnement de travail sont automatiquement analysés uniquement lorsque vous avez défini le paramètre **Map** ou **Map & Classify** dans la zone d'entête. Lorsque vous sélectionnez **personnalisé** ou **Désactivé** dans la zone de titre, vous devez activer le mappage et/ou la numérisation complète sur chaque nouveau volume que vous ajoutez à l'environnement de travail.

Analyse des volumes de protection des données

Par défaut, les volumes DP ne sont pas analysés parce qu'ils ne sont pas exposés en externe et que Cloud Data SENSE ne peut pas y accéder. Il s'agit des volumes de destination des opérations SnapMirror depuis un système ONTAP sur site ou à partir d'un système Cloud Volumes ONTAP.

Initialement, la liste de volumes identifie ces volumes comme *Type DP* avec *Status Not Scanning* et la *Required action Enable Access to DP volumes*.

The screenshot shows the 'Working Environment Name' Configuration page. At the top, there's a search bar and a button 'Enable Access to DP Volumes' (highlighted with a red box). Below the search bar, there's a section for 'Volumes selected for compliance scan' with tabs for 'Off', 'Map', 'Map & Classify', and 'Custom'. The 'Map' tab is selected. Below this is a table with columns: 'Scan', 'Storage Repository (Volume)', 'Type', 'Status', and 'Required Action'. The table lists three volumes: 'VolumeName1' (Type: DP, Status: Not Scanning, Required Action: Enable access to DP Volumes), 'VolumeName2' (Type: NFS, Status: Continuously Scanning), and 'VolumeName3' (Type: CIFS, Status: Not Scanning). Each row has buttons for 'Off', 'Map', and 'Map & Classify'.

Étapes

Pour analyser ces volumes de protection des données :

1. Cliquez sur **Activer l'accès aux volumes DP** en haut de la page.
2. Vérifiez le message de confirmation et cliquez à nouveau sur **Activer l'accès aux volumes DP**.
 - Les volumes initialement créés en tant que volumes NFS dans le système ONTAP source sont activés.
 - Pour les volumes initialement créés en tant que volumes CIFS dans le système ONTAP source, vous devez entrer des identifiants CIFS pour scanner ces volumes DP. Si vous avez déjà saisi les informations d'identification Active Directory afin que Cloud Data SENSE puisse analyser des volumes CIFS, vous pouvez utiliser ces informations d'identification ou spécifier un autre ensemble d'informations d'identification Admin.

The screenshot shows the 'Provide Active Directory Credentials' dialog box. It has two radio buttons: 'Use existing CIFS Scanning Credentials (user1@domain2)' (selected and highlighted with a red box) and 'Use Custom Credentials'. Below the radio buttons are fields for 'Active Directory Domain' and 'DNS IP Address'. At the bottom, there are buttons for 'Enable Access to DP Volumes' and 'Cancel'. A message at the bottom states: 'DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Data Sense. The shares' export policies will allow access only from the Cloud Data Sense instance. Learn More'.

The screenshot shows the 'Provide Active Directory Credentials' dialog box. It has two radio buttons: 'Use existing CIFS Scanning Credentials (user1@domain2)' and 'Use Custom Credentials' (selected and highlighted with a red box). Below the radio buttons are fields for 'Username' and 'Password'. Below these are fields for 'Active Directory Domain' and 'DNS IP Address'. At the bottom, there are buttons for 'Enable Access to DP Volumes' and 'Cancel'. A message at the bottom states: 'DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Data Sense. The shares' export policies will allow access only from the Cloud Data Sense instance. Learn More'.

3. Activez chaque volume DP que vous souhaitez analyser [de la même façon que vous avez activé d'autres volumes](#).

Résultat

Une fois activée, Cloud Data Sense crée un partage NFS à partir de chaque volume DP activé pour l'analyse. Les règles d'exportation de partage autorisent uniquement l'accès à partir de l'instance de détection de données.

Remarque : si vous ne aviez pas de volumes de protection des données CIFS lorsque vous avez activé l'accès initial aux volumes DP, puis en ajoutant d'autres, le bouton **Activer l'accès à CIFS DP** s'affiche en haut de la page Configuration. Cliquez sur ce bouton et ajoutez des identifiants CIFS pour permettre l'accès à ces volumes CIFS DP.



Les identifiants Active Directory sont uniquement enregistrés dans la machine virtuelle de stockage du premier volume CIFS DP, de sorte que tous les volumes DP de ce SVM soient analysés. Les volumes résidant sur d'autres SVM ne seront pas enregistrés pour les identifiants Active Directory, de sorte que ces volumes DP ne seront pas analysés.

Mise en route de Cloud Data Sense for Azure NetApp Files

Suivez ces quelques étapes pour commencer à utiliser Cloud Data Sense for Azure NetApp Files.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

Découvrez les systèmes Azure NetApp Files que vous souhaitez analyser

Avant de pouvoir analyser des volumes Azure NetApp Files, "[BlueXP doit être configuré pour détecter la configuration](#)".

2

Déployez l'instance Cloud Data SENSE

"[Déployez Cloud Data Sense dans BlueXP](#)" si aucune instance n'est déjà déployée.

3

Activez Cloud Data SENSE et sélectionnez les volumes à analyser

Cliquez sur **Compliance**, sélectionnez l'onglet **Configuration** et activez les analyses de conformité pour les volumes dans des environnements de travail spécifiques.

4

Vérifiez l'accès aux volumes

Lorsque Cloud Data SENSE est activé, assurez-vous qu'il peut accéder à tous les volumes.

- L'instance Cloud Data SENSE doit disposer d'une connexion réseau à chaque sous-réseau Azure NetApp Files.

- Assurez-vous que ces ports sont ouverts à l'instance de détection de données :
 - Pour NFS – ports 111 et 2049.
 - Pour CIFS – ports 139 et 445.
- Les règles d'exportation de volumes NFS doivent autoriser l'accès à partir de l'instance Data Sense.
- La détection de données a besoin des identifiants Active Directory pour analyser les volumes CIFS.

Cliquez sur **Compliance > Configuration > Modifier les informations d'identification CIFS** et fournissez les informations d'identification.

5

Gérer les volumes à analyser

Sélectionnez ou désélectionnez les volumes que vous souhaitez scanner et Cloud Data SENSE démarre ou arrête l'acquisition.

Détection du système Azure NetApp Files que vous souhaitez numériser

Si le système Azure NetApp Files que vous voulez numériser n'est pas déjà dans BlueXP comme environnement de travail, vous pouvez l'ajouter au canevas pour le moment.

["Découvrez comment découvrir le système Azure NetApp Files dans BlueXP".](#)

Déploiement de l'instance Cloud Data Sense

["Déployez des données adaptées au cloud"](#) si aucune instance n'est déjà déployée.

Il est nécessaire de déployer Data Sense dans le cloud lors de l'analyse des volumes Azure NetApp Files, et il doit être déployé dans la même région que les volumes que vous souhaitez analyser.

Remarque : le déploiement de Cloud Data Sense dans un emplacement sur site n'est pas pris en charge actuellement lors de l'analyse de volumes Azure NetApp Files.

Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

Activation des données cloud dans vos environnements de travail

Vous pouvez activer Cloud Data SENSE sur vos volumes Azure NetApp Files.

1. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**, puis sélectionnez l'onglet **Configuration**.



2. Sélectionnez le mode de numérisation des volumes dans chaque environnement de travail. ["En savoir plus sur les acquisitions de mappage et de classification"](#):
 - Pour mapper tous les volumes, cliquez sur **mapper tous les volumes**.
 - Pour mapper et classer tous les volumes, cliquez sur **cartographier et classer tous les volumes**.
 - Pour personnaliser la numérisation de chaque volume, cliquez sur **ou sélectionnez le type de numérisation pour chaque volume**, puis choisissez les volumes que vous souhaitez mapper et/ou classer.

Voir [Activation et désactivation des analyses de conformité sur les volumes](#) pour plus d'informations.
3. Dans la boîte de dialogue de confirmation, cliquez sur **approuver** pour que Data Sense commence à analyser vos volumes.

Résultat

Cloud Data SENSE commence à analyser les volumes que vous avez sélectionnés dans l'environnement de travail. Les résultats seront disponibles dans le tableau de bord de conformité dès que Cloud Data SENSE aura terminé les analyses initiales. Le temps nécessaire dépend de la quantité de données—il peut être de quelques minutes ou heures.

Vérifier que le sens des données cloud a accès aux volumes

Assurez-vous que Cloud Data est capable d'accéder aux volumes en vérifiant vos groupes de sécurité et vos règles d'exportation. Vous devez fournir un « logique de données » avec des identifiants CIFS pour pouvoir accéder aux volumes CIFS.

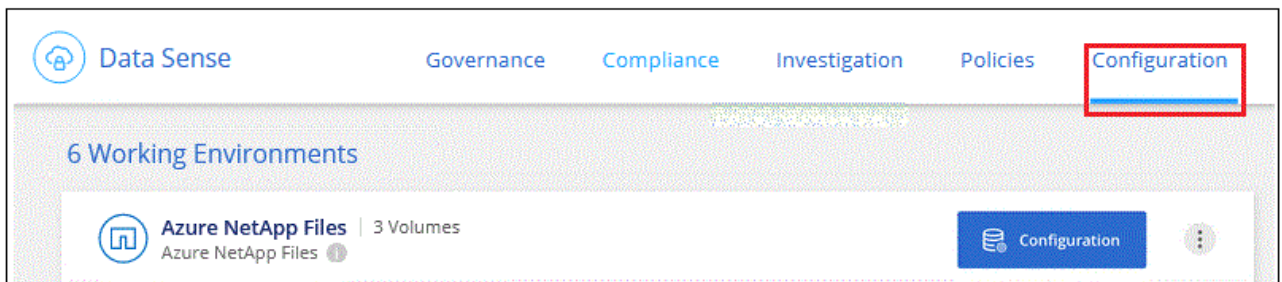
Étapes

1. Vérifiez qu'il existe une connexion réseau entre l'instance Cloud Data Sense et chaque réseau incluant des volumes pour Azure NetApp Files.



Pour Azure NetApp Files, Cloud Data SENSE ne peut analyser que les volumes se trouvant dans la même région que BlueXP.

2. Assurez-vous que les ports suivants sont ouverts à l'instance de détection de données :
 - Pour NFS – ports 111 et 2049.
 - Pour CIFS – ports 139 et 445.
3. Assurez-vous que les règles d'exportation de volume NFS incluent l'adresse IP de l'instance Data Sense afin qu'elle puisse accéder aux données sur chaque volume.
4. Si vous utilisez le protocole CIFS, fournissez Data Sense avec des identifiants Active Directory afin qu'il puisse analyser les volumes CIFS.
 - a. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**, puis sélectionnez l'onglet **Configuration**.

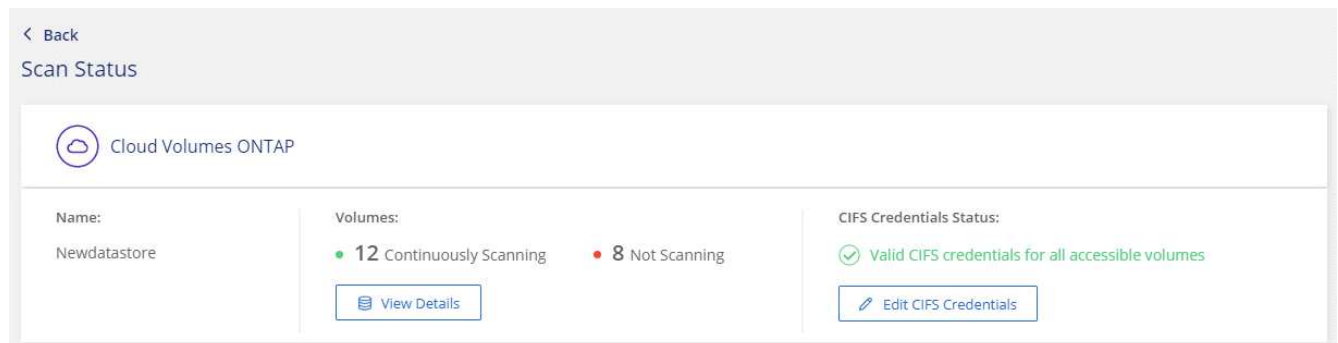


- b. Pour chaque environnement de travail, cliquez sur **Modifier les informations d'identification CIFS** et entrez le nom d'utilisateur et le mot de passe dont Data Sense a besoin pour accéder aux volumes CIFS sur le système.

Les informations d'identification peuvent être en lecture seule, mais fournir des informations d'identification admin garantit que Data Sense peut lire toutes les données qui requièrent des autorisations élevées. Les identifiants sont stockés sur l'instance Cloud Data Sense.

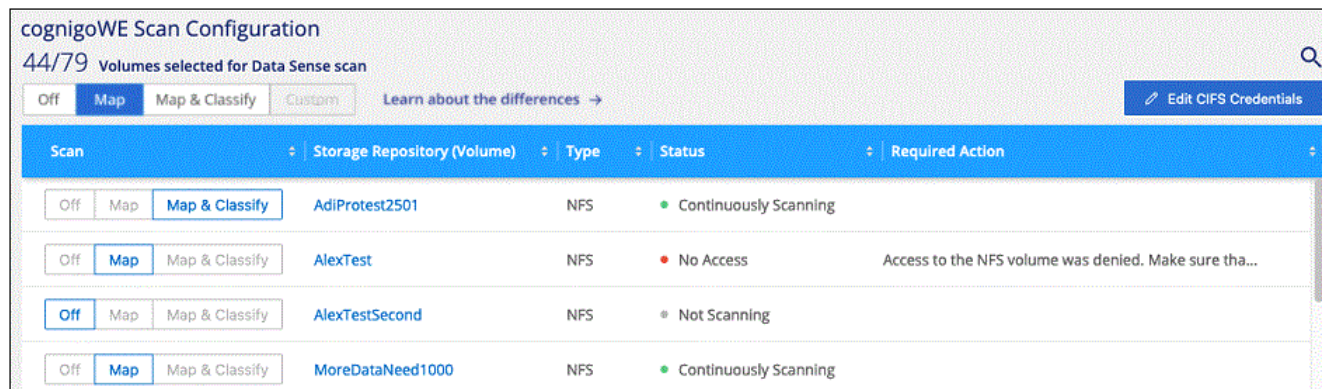
Si vous voulez vous assurer que vos fichiers "dernières heures d'accès" sont inchangés par les analyses de classification de détection de données, nous recommandons à l'utilisateur de disposer de l'autorisation Write Attributes. Si possible, nous vous recommandons de faire en sorte que l'utilisateur configuré Active Directory fasse partie d'un groupe parent de l'organisation qui dispose des autorisations pour tous les fichiers.

Une fois les informations d'identification saisies, un message indiquant que tous les volumes CIFS ont été authentifiés avec succès s'affiche.



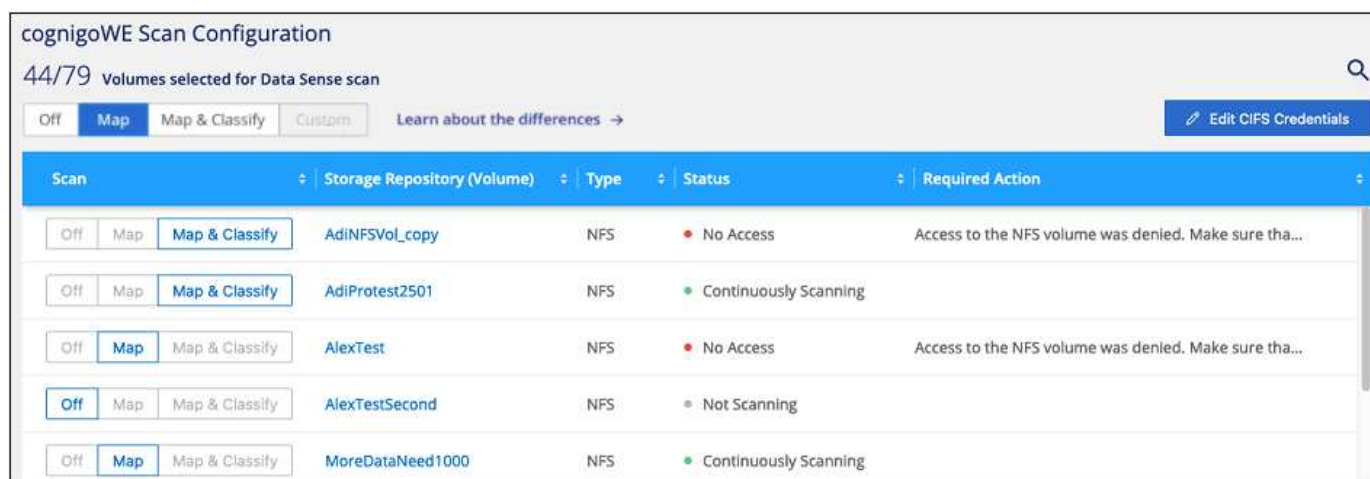
5. Sur la page *Configuration*, cliquez sur **View Details** pour vérifier l'état de chaque volume CIFS et NFS et corriger les erreurs éventuelles.

L'image suivante montre par exemple quatre volumes dont l'un des types de données cloud n'est pas capable de se scanner en raison de problèmes de connectivité réseau entre l'instance Data Sense et le volume.



Activation et désactivation des analyses de conformité sur les volumes

Vous pouvez démarrer ou arrêter des analyses de mappage uniquement, ou des analyses de mappage et de classification, dans un environnement de travail à tout moment à partir de la page Configuration. Vous pouvez également passer des acquisitions avec mappage uniquement à des acquisitions avec mappage et classification, et inversement. Nous vous recommandons de scanner tous les volumes.



À :	Procédez comme suit :
Activez les acquisitions avec mappage uniquement sur un volume	Dans la zone du volume, cliquez sur Map
Activer la numérisation complète sur un volume	Dans la zone de volume, cliquez sur carte et classement
Désactiver la numérisation sur un volume	Dans la zone du volume, cliquez sur Off
Activez les analyses de mappage uniquement sur tous les volumes	Dans la zone d'en-tête, cliquez sur carte
Activez l'analyse complète sur tous les volumes	Dans la zone d'en-tête, cliquez sur carte et classement
Désactiver l'analyse de tous les volumes	Dans la zone d'en-tête, cliquez sur Off



Les nouveaux volumes ajoutés à l'environnement de travail sont automatiquement analysés uniquement lorsque vous avez défini le paramètre **Map** ou **Map & Classify** dans la zone d'entête. Lorsque vous sélectionnez **personnalisé** ou **Désactivé** dans la zone de titre, vous devez activer le mappage et/ou la numérisation complète sur chaque nouveau volume que vous ajoutez à l'environnement de travail.

Lancez-vous avec Cloud Data Sense for Amazon FSX pour ONTAP

Suivez quelques étapes pour commencer l'analyse d'Amazon FSX pour les volumes ONTAP avec Cloud Data Sense.

Avant de commencer

- Vous avez besoin d'un connecteur actif dans AWS pour déployer et gérer Data Sense.
- Le groupe de sécurité que vous avez sélectionné lors de la création de l'environnement de travail doit autoriser le trafic à partir de l'instance Cloud Data SENSE. Vous pouvez trouver le groupe de sécurité associé à l'aide de l'ENI connecté au système de fichiers FSX pour 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 flexibles AWS \(ENI\)"](#)

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler vers le bas pour obtenir plus de détails.

1

Découvrez le FSX pour les systèmes de fichiers ONTAP que vous souhaitez analyser

Avant de pouvoir analyser FSX pour des volumes ONTAP, ["Vous devez disposer d'un environnement de travail FSX avec des volumes configurés"](#).

2

Déployez l'instance Cloud Data SENSE

["Déployez Cloud Data Sense dans BlueXP"](#) si aucune instance n'est déjà déployée.

3

Activez Cloud Data SENSE et sélectionnez les volumes à analyser

Cliquez sur **Data Sense**, sélectionnez l'onglet **Configuration** et activez les analyses de conformité pour les volumes dans des environnements de travail spécifiques.

4

Vérifiez l'accès aux volumes

Lorsque Cloud Data SENSE est activé, assurez-vous qu'il peut accéder à tous les volumes.

- L'instance Cloud Data SENSE doit disposer d'une connexion réseau à chaque sous-réseau FSX pour ONTAP.
- Assurez-vous que les ports suivants sont ouverts à l'instance de détection de données :
 - Pour NFS – ports 111 et 2049.
 - Pour CIFS – ports 139 et 445.
- Les règles d'exportation de volumes NFS doivent autoriser l'accès à partir de l'instance Data Sense.
- La détection de données a besoin des identifiants Active Directory pour analyser les volumes CIFS. + cliquez sur **conformité > Configuration > Modifier les informations d'identification CIFS** et fournissez les informations d'identification.

5

Gérer les volumes à analyser

Sélectionnez ou désélectionnez les volumes que vous souhaitez analyser et Cloud Data SENSE démarre ou arrête l'acquisition.

Détection du système de fichiers FSX pour ONTAP que vous souhaitez numériser

Si le système de fichiers FSX pour ONTAP que vous souhaitez numériser n'est pas déjà dans BlueXP comme environnement de travail, vous pouvez l'ajouter au canevas à ce moment.

["Découvrez comment découvrir ou créer le système de fichiers FSX pour ONTAP dans BlueXP".](#)

Déploiement de l'instance Cloud Data Sense

["Déployez des données adaptées au cloud"](#) si aucune instance n'est déjà déployée.

Vous devez déployer Data Sense dans le même réseau AWS que le connecteur pour AWS et les volumes FSX que vous souhaitez analyser.

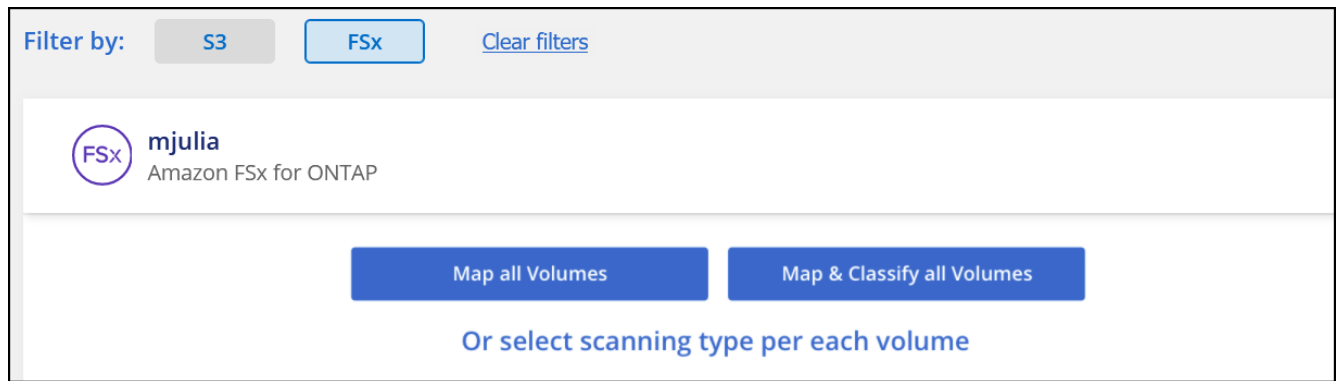
Remarque : le déploiement de Cloud Data SENSE dans un emplacement sur site n'est pas pris en charge actuellement lors de l'analyse de volumes FSX.

Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

Activation des données cloud dans vos environnements de travail

Vous pouvez activer Cloud Data Sense pour FSX pour les volumes ONTAP.

1. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**, puis sélectionnez l'onglet **Configuration**.



2. Sélectionnez le mode de numérisation des volumes dans chaque environnement de travail. "[En savoir plus sur les acquisitions de mappage et de classification](#)":

- Pour mapper tous les volumes, cliquez sur **mapper tous les volumes**.
- Pour mapper et classer tous les volumes, cliquez sur **cartographier et classer tous les volumes**.
- Pour personnaliser la numérisation de chaque volume, cliquez sur **ou sélectionnez le type de numérisation pour chaque volume**, puis choisissez les volumes que vous souhaitez mapper et/ou classer.

Voir [Activation et désactivation des analyses de conformité sur les volumes](#) pour plus d'informations.

3. Dans la boîte de dialogue de confirmation, cliquez sur **approuver** pour que Data Sense commence à analyser vos volumes.

Résultat

Cloud Data SENSE commence à analyser les volumes que vous avez sélectionnés dans l'environnement de travail. Les résultats seront disponibles dans le tableau de bord de conformité dès que Cloud Data SENSE aura terminé les analyses initiales. Le temps nécessaire dépend de la quantité de données—il peut être de quelques minutes ou heures.

Vérifier que le sens des données cloud a accès aux volumes

Assurez-vous que Cloud Data peut détecter l'accès aux volumes en vérifiant vos groupes de sécurité et vos règles de mise en réseau et d'exportation.

Vous devez fournir un « logique de données » avec des identifiants CIFS pour pouvoir accéder aux volumes CIFS.

Étapes

1. Sur la page *Configuration*, cliquez sur **Afficher les détails** pour vérifier l'état et corriger les erreurs.

Par exemple, l'image suivante montre qu'un volume Cloud Data SENSE ne peut pas se scanner en raison de problèmes de connectivité réseau entre l'instance Data Sense et le volume.

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	jrmclone	NFS	● No Access	Check network connectivity between the Data Sense ...

2. Vérifiez qu'il existe une connexion réseau entre l'instance Cloud Data Sense et chaque réseau incluant des volumes pour FSX pour ONTAP.



Pour FSX pour ONTAP, Cloud Data SENSE ne peut analyser les volumes que dans la même région que BlueXP.

3. Assurez-vous que les ports suivants sont ouverts à l'instance de détection de données.
 - Pour NFS – ports 111 et 2049.
 - Pour CIFS – ports 139 et 445.
4. Assurez-vous que les règles d'exportation de volume NFS incluent l'adresse IP de l'instance Data Sense afin qu'elle puisse accéder aux données sur chaque volume.
5. Si vous utilisez le protocole CIFS, fournissez Data Sense avec des identifiants Active Directory afin qu'il puisse analyser les volumes CIFS.
 - a. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**, puis sélectionnez l'onglet **Configuration**.
 - b. Pour chaque environnement de travail, cliquez sur **Modifier les informations d'identification CIFS** et entrez le nom d'utilisateur et le mot de passe dont Data Sense a besoin pour accéder aux volumes CIFS sur le système.

Les informations d'identification peuvent être en lecture seule, mais fournir des informations d'identification admin garantit que Data Sense peut lire toutes les données qui requièrent des autorisations élevées. Les identifiants sont stockés sur l'instance Cloud Data Sense.

Si vous voulez vous assurer que vos fichiers "dernières heures d'accès" sont inchangés par les analyses de classification de détection de données, nous recommandons à l'utilisateur de disposer de l'autorisation Write Attributes. Si possible, nous vous recommandons de faire en sorte que l'utilisateur configuré Active Directory fasse partie d'un groupe parent de l'organisation qui dispose des autorisations pour tous les fichiers.

Une fois les informations d'identification saisies, un message indiquant que tous les volumes CIFS ont été authentifiés avec succès s'affiche.

Activation et désactivation des analyses de conformité sur les volumes

Vous pouvez démarrer ou arrêter des analyses de mappage uniquement, ou des analyses de mappage et de classification, dans un environnement de travail à tout moment à partir de la page Configuration. Vous pouvez également passer des acquisitions avec mappage uniquement à des acquisitions avec mappage et classification, et inversement. Nous vous recommandons de scanner tous les volumes.

cognitoWE Scan Configuration

44/79 Volumes selected for Data Sense scan

OffMapMap & ClassifyCustom

Learn about the differences →

Edit CIFS Credentials

Scan	Storage Repository (Volume)	Type	Status	Required Action
<div>OffMapMap & Classify</div>	AdiNFSVol_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
<div>OffMapMap & Classify</div>	AdiProtest2501	NFS	Continuously Scanning	
<div>OffMapMap & Classify</div>	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
<div>OffMapMap & Classify</div>	AlexTestSecond	NFS	Not Scanning	
<div>OffMapMap & Classify</div>	MoreDataNeed1000	NFS	Continuously Scanning	

À :	Procédez comme suit :
Activez les acquisitions avec mappage uniquement sur un volume	Dans la zone du volume, cliquez sur Map
Activer la numérisation complète sur un volume	Dans la zone de volume, cliquez sur carte et classement
Désactiver la numérisation sur un volume	Dans la zone du volume, cliquez sur Off
Activez les analyses de mappage uniquement sur tous les volumes	Dans la zone d'en-tête, cliquez sur carte
Activez l'analyse complète sur tous les volumes	Dans la zone d'en-tête, cliquez sur carte et classement
Désactiver l'analyse de tous les volumes	Dans la zone d'en-tête, cliquez sur Off



Les nouveaux volumes ajoutés à l'environnement de travail sont automatiquement analysés uniquement lorsque vous avez défini le paramètre **Map** ou **Map & Classify** dans la zone d'en-tête. Lorsque vous sélectionnez **personnalisé** ou **Désactivé** dans la zone de titre, vous devez activer le mappage et/ou la numérisation complète sur chaque nouveau volume que vous ajoutez à l'environnement de travail.

Analyse des volumes de protection des données

Par défaut, les volumes DP ne sont pas analysés parce qu'ils ne sont pas exposés en externe et que Cloud Data SENSE 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 de volumes identifie ces volumes comme *Type DP* avec *Status Not Scanning* et la *Requited action Enable Access to DP volumes*.

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	VolumeName1	DP	Not Scanning	Enable access to DP Volumes ⓘ
Off Map Map & Classify	VolumeName2	NFS	Continuously Scanning	
Off Map Map & Classify	VolumeName3	CIFS	Not Scanning	

Étapes

Pour analyser ces volumes de protection des données :

1. Cliquez sur **Activer l'accès aux volumes DP** en haut de la page.
2. Vérifiez le message de confirmation et cliquez à nouveau sur **Activer l'accès aux volumes DP**.
 - Les volumes initialement créés en tant que volumes NFS dans le système de fichiers FSX source pour ONTAP sont activés.
 - Les volumes initialement créés en tant que volumes CIFS dans le système de fichiers FSX source pour

ONTAP nécessitent que vous saisiez des informations d'identification CIFS pour scanner ces volumes DP. Si vous avez déjà saisi les informations d'identification Active Directory afin que Cloud Data Sense puisse analyser des volumes CIFS, vous pouvez utiliser ces informations d'identification ou spécifier un autre ensemble d'informations d'identification Admin.

The image shows two versions of the 'Provide Active Directory Credentials' dialog box. The left version has the radio button for 'Use existing CIFS Scanning Credentials (user1@domain2)' selected. The right version has the radio button for 'Use Custom Credentials' selected, and it includes input fields for 'Username', 'Password', 'Active Directory Domain', and 'DNS IP Address'. Both versions include a warning about DP Volumes and 'Enable Access to DP Volumes' and 'Cancel' buttons.

3. Activez chaque volume DP que vous souhaitez analyser [de la même façon que vous avez activé d'autres volumes](#).

Résultat

Une fois activée, Cloud Data Sense crée un partage NFS à partir de chaque volume DP activé pour l'analyse. Les règles d'exportation de partage autorisent uniquement l'accès à partir de l'instance de détection de données.

Remarque : si vous ne aviez pas de volumes de protection des données CIFS lorsque vous avez activé l'accès initial aux volumes DP, puis en ajoutant d'autres, le bouton **Activer l'accès à CIFS DP** s'affiche en haut de la page Configuration. Cliquez sur ce bouton et ajoutez des identifiants CIFS pour permettre l'accès à ces volumes CIFS DP.



Les identifiants Active Directory sont uniquement enregistrés dans la machine virtuelle de stockage du premier volume CIFS DP, de sorte que tous les volumes DP de ce SVM soient analysés. Les volumes résidant sur d'autres SVM ne seront pas enregistrés pour les identifiants Active Directory, de sorte que ces volumes DP ne seront pas analysés.

Mise en route de Cloud Data Sense pour Amazon S3

Cloud Data Sense peut analyser vos compartiments Amazon S3 pour identifier les données personnelles et sensibles qui résident dans le stockage objet S3. Cloud Data Sense peut scanner n'importe quel compartiment du compte, indépendamment de sa création pour une solution NetApp.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

Configurez les exigences S3 dans votre environnement cloud

Assurez-vous que votre environnement cloud répond aux exigences du Cloud Data SENSE, notamment la préparation d'un rôle IAM et la configuration de la connectivité depuis Data Sense vers S3. [Voir la liste complète](#).

2

Déployez l'instance Cloud Data SENSE

"[Déployez des données adaptées au cloud](#)" si aucune instance n'est déjà déployée.

3

Activation de Data Sense dans votre environnement de travail S3

Sélectionnez l'environnement de travail Amazon S3, cliquez sur **Activer** et sélectionnez un rôle IAM qui inclut les autorisations requises.

4

Sélectionnez les compartiments à numériser

Sélectionnez les compartiments que vous souhaitez analyser et Cloud Data SENSE commence à les analyser.

Vérification des prérequis S3

Les exigences suivantes sont spécifiques à l'analyse des compartiments S3.

Configurez un rôle IAM pour l'instance Cloud Data Sense

Cloud Data SENSE a besoin d'autorisations pour se connecter aux compartiments S3 de votre compte et pour les analyser. Configurez un rôle IAM qui inclut les autorisations répertoriées ci-dessous. BlueXP vous invite à sélectionner un rôle IAM lorsque vous activez Data Sense dans l'environnement de travail Amazon S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}
```

Connectivité entre le maillage Cloud Data Sense et Amazon S3

Cloud Data SENSE a besoin d'une connexion à Amazon S3. Pour assurer cette connexion, le meilleur moyen consiste à utiliser un terminal VPC pour le service S3. Pour obtenir des instructions, reportez-vous à la section ["Documentation AWS : création d'un terminal de passerelle"](#).

Lorsque vous créez le point de terminaison VPC, veillez à sélectionner la région, le VPC et la table de routage correspondant à l'instance Cloud Data Sense. Vous devez également modifier le groupe de sécurité pour ajouter une règle HTTPS sortante qui active le trafic vers le terminal S3. Dans le cas contraire, Data Sense ne peut pas se connecter au service S3.

Si vous rencontrez des problèmes, reportez-vous à la section ["Centre de connaissances du support AWS : pourquoi ne puis-je pas me connecter à un compartiment S3 à l'aide d'un terminal VPC de passerelle ?"](#)

Une alternative consiste à fournir la connexion à l'aide d'une passerelle NAT.



Vous ne pouvez pas utiliser de proxy pour accéder à S3 sur Internet.

Déploiement de l'instance Cloud Data Sense

["Déployez Cloud Data Sense dans BlueXP"](#) si aucune instance n'est déjà déployée.

Vous devez déployer l'instance à l'aide d'un connecteur déployé dans AWS. BlueXP détecte automatiquement les compartiments S3 dans ce compte AWS et les affiche dans un environnement de travail Amazon S3.

Remarque : le déploiement de Cloud Data SENSE dans un emplacement sur site n'est pas pris en charge actuellement lors de l'analyse des compartiments S3.

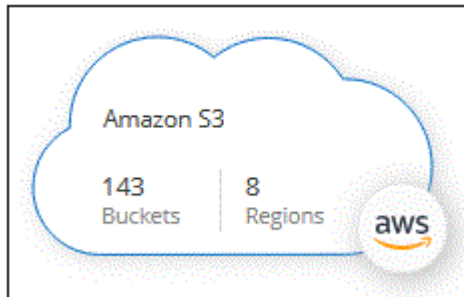
Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

Activation de Data Sense dans votre environnement de travail S3

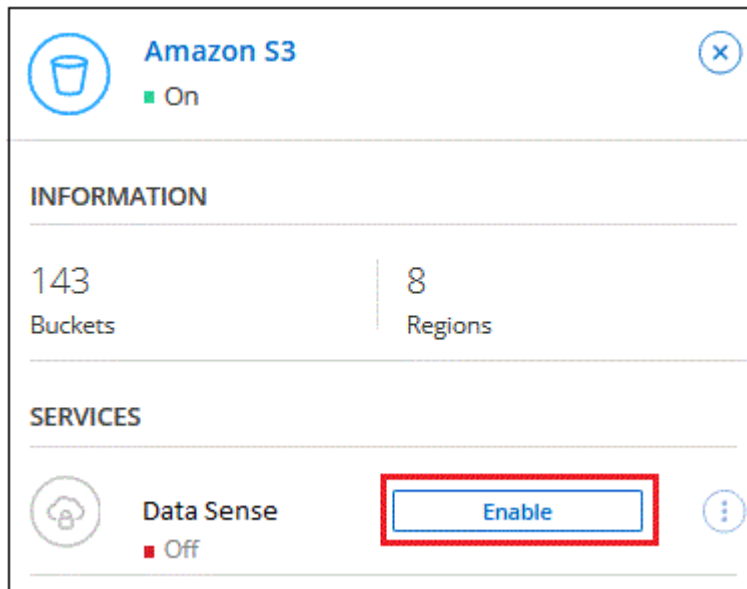
Activez Cloud Data SENSE sur Amazon S3 après avoir vérifié les prérequis.

Étapes

1. Dans le menu de navigation de gauche de BlueXP, cliquez sur **stockage > Canvas**.
2. Sélectionnez l'environnement de travail Amazon S3.



3. Dans le volet de détection de données situé à droite, cliquez sur **Activer**.



4. Attribuez un rôle IAM à l'instance Cloud Data SENSE qui dispose de [les autorisations requises](#).

Assign an AWS IAM Role for Cloud Data Sense

To enable **Cloud Data Sense** on Amazon S3 buckets, select an existing IAM Role. Make sure that your AWS IAM Role has the permission defined in the [Policy Requirements](#).

Select IAM Role

occm

▼

VPC Endpoint for Amazon S3 Required

A VPC endpoint to the Amazon S3 service is required so **Data Sense** can securely scan the data.

Alternatively, ensure that the **Data Sense** instance has direct access to the internet via a NAT Gateway or Internet Gateway.

Free for the 1st TB


Over 1 TB you pay only for what you use. [Learn more about pricing.](#)

Enable

Cancel

5. Cliquez sur **Activer**.



Vous pouvez également activer les analyses de conformité pour un environnement de travail à partir de la page Configuration en cliquant sur  Et en sélectionnant **Activer détection de données**.

Résultat

BlueXP affecte le rôle IAM à l'instance.

Activation et désactivation des analyses de conformité dans les compartiments S3

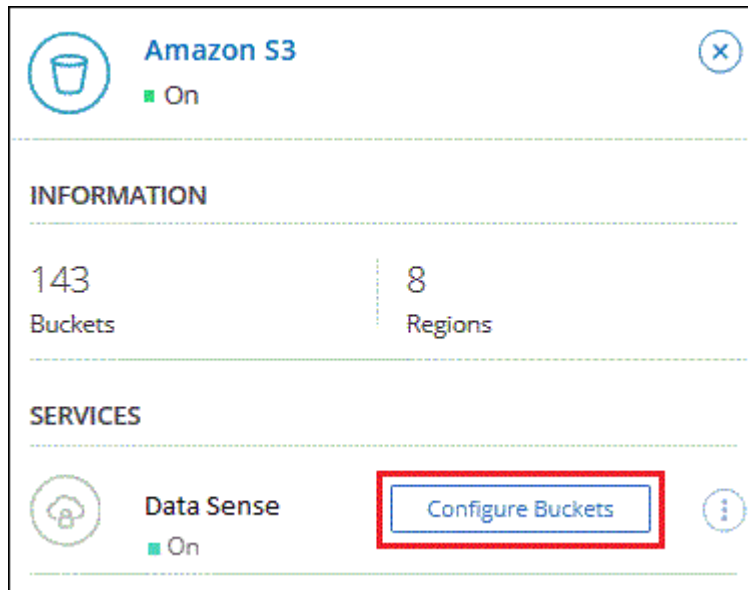
Une fois que BlueXP a activé Cloud Data Sense sur Amazon S3, l'étape suivante consiste à configurer les compartiments que vous souhaitez numériser.

Lorsque BlueXP est exécuté dans le compte AWS doté des compartiments S3 que vous souhaitez analyser, il détecte ces compartiments et les affiche dans un environnement de travail Amazon S3.

Cloud Data Sense peut également être [Analysez les compartiments S3 qui se trouvent dans différents comptes AWS](#).

Étapes

1. Sélectionnez l'environnement de travail Amazon S3.
2. Dans le volet de droite, cliquez sur **configurer les rubriques**.



3. Activez les analyses de mappage uniquement ou les analyses de mappage et de classification sur vos compartiments.

Amazon S3 Configuration			
15/28 Buckets in Scan Scope.			
Scan	Bucket Name	Status	Required Action
Off Map Map & Classify	BucketName1	● Not Scanning	Add Credentials
Off Map Map & Classify	BucketName2	● Continuosly Scanning	
Off Map Map & Classify	BucketName3	● Not Scanning	

À :	Procédez comme suit :
Activez les acquisitions avec mappage uniquement sur un compartiment	Cliquez sur carte
Activer les acquisitions complètes sur un compartiment	Cliquez sur carte et classement
Désactiver l'acquisition sur un godet	Cliquez sur Off

Résultat

Cloud Data Sense commence l'analyse des compartiments S3 que vous avez activés. En cas d'erreur, elles apparaîtront dans la colonne État, ainsi que l'action requise pour corriger l'erreur.

Analyse des compartiments à partir de comptes AWS supplémentaires

Pour scanner les compartiments S3 qui se trouvent dans un autre compte AWS, vous devez attribuer un rôle à partir de ce compte pour accéder à l'instance Cloud Data Sense existante.



Étapes

1. Accédez au compte AWS cible où vous voulez analyser les compartiments S3 et créer un rôle IAM en sélectionnant **un autre compte AWS**.

Create role




Select type of trusted entity

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID*

- Options**
- ☐ Require external ID (Best practice when a third party will assume this role)
 - ☐ Require MFA 

Assurez-vous de faire ce qui suit :

- Entrez l'ID du compte sur lequel réside l'instance Cloud Data SENSE.
- Modifiez la durée * maximale de la session CLI/API* de 1 heure à 12 heures et enregistrez cette modification.
- Joignez la politique IAM de détection des données cloud. Assurez-vous qu'il dispose des autorisations requises.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

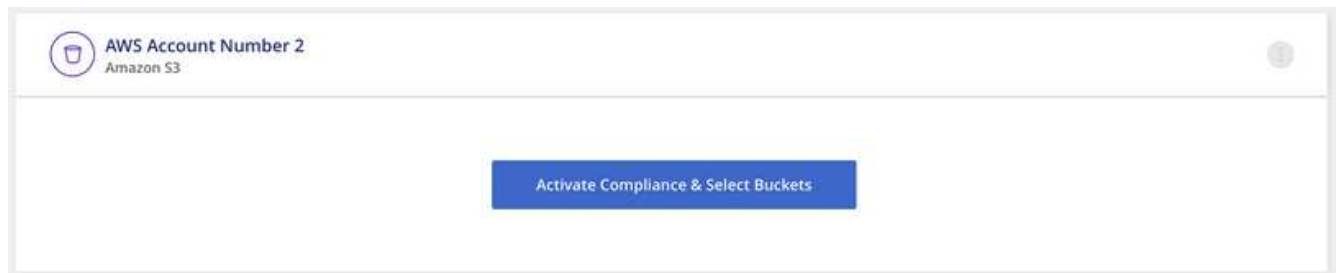
2. Accédez au compte AWS source sur lequel réside l'instance Data Sense et sélectionnez le rôle IAM associé à l'instance.
 - a. Modifiez la durée * maximale de la session CLI/API* de 1 heure à 12 heures et enregistrez cette modification.
 - b. Cliquez sur **attacher des stratégies**, puis sur **Créer une stratégie**.

- c. Créez une stratégie qui inclut l'action « sts:AssumeRole » et spécifiez l'ARN du rôle que vous avez créé dans le compte cible.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-ID>:role/<ADDITIONAL_ROLE_NAME>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}
```

Le compte d'instance Cloud Data SENSE a désormais accès au compte AWS supplémentaire.

3. Accédez à la page **Amazon S3 Configuration** et le nouveau compte AWS s'affiche. Notez que la synchronisation de l'environnement de travail du nouveau compte peut prendre quelques minutes avec Cloud Data Sense.



4. Cliquez sur **Activer la détection des données et sélectionnez les rubriques** et sélectionnez les rubriques que vous souhaitez numériser.

Résultat

Cloud Data Sense commence l'analyse des nouveaux compartiments S3 que vous avez activés.

Analyse des schémas de base de données

Suivez quelques étapes pour commencer à scanner vos schémas de base de données à l'aide de Cloud Data Sense.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

Vérifiez les prérequis de la base de données

Assurez-vous que votre base de données est prise en charge et que vous disposez des informations nécessaires pour vous connecter à la base de données.

2

Déployez l'instance Cloud Data SENSE

"[Déployez des données adaptées au cloud](#)" si aucune instance n'est déjà déployée.

3

Ajoutez le serveur de base de données

Ajoutez le serveur de base de données auquel vous souhaitez accéder.

4

Sélectionnez les schémas

Sélectionnez les schémas à numériser.

Vérification des prérequis

Avant d'activer le Cloud Data sens, lisez les conditions préalables suivantes pour vérifier que la configuration est prise en charge.

Bases de données prises en charge

Cloud Data SENSE peut scanner des schémas à partir des bases de données suivantes :

- Amazon Relational Database Service (Amazon RDS)
- MongoDB
- MySQL
- Oracle
- PostgreSQL
- SAP HANA
- Serveur SQL (MSSQL)



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

Configuration requise pour les bases de données

Toutes les bases de données connectée à l'instance Cloud Data SENSE peuvent être analysées, quel que soit l'endroit où elles sont hébergées. Pour vous connecter à la base de données, il vous suffit de disposer des informations suivantes :

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

Lorsque vous choisissez un nom d'utilisateur et un mot de passe, il est important de choisir un nom qui dispose des autorisations de lecture complètes pour tous les schémas et tables que vous souhaitez numériser. Nous vous recommandons de créer un utilisateur dédié pour le système Cloud Data SENSE avec toutes les autorisations requises.

Remarque : pour MongoDB, un rôle d'administrateur en lecture seule est requis.

Déploiement de l'instance Cloud Data Sense

Déployez Cloud Data si aucune instance n'est déjà déployée.

Si vous numérisez des schémas de base de données accessibles via Internet, vous pouvez "[Déployez les données du cloud dans le cloud](#)" ou "[Déployer Data Sense dans un emplacement sur site avec accès Internet](#)".

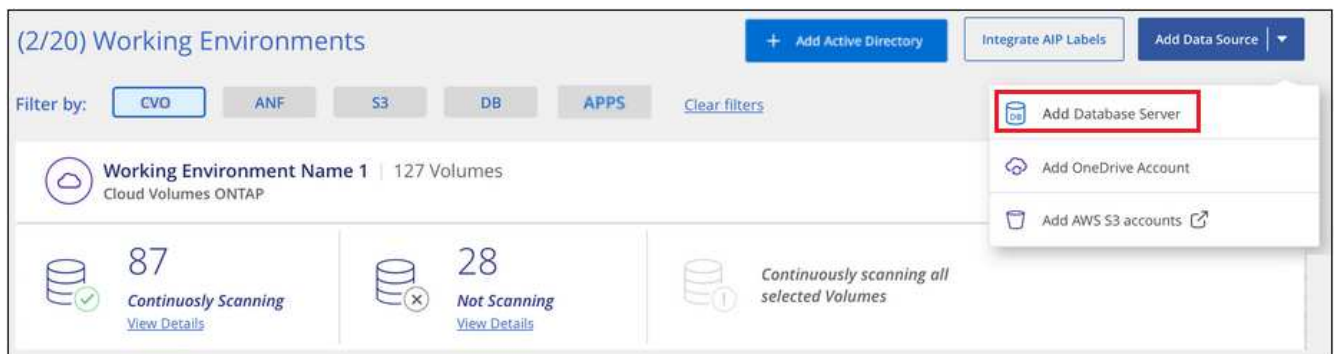
Si vous numérisez des schémas de base de données qui ont été installés sur un site sombre sans accès à Internet, vous devez le faire "[Déployez les données cloud sur site qui ne disposent pas d'un accès Internet](#)". Cela nécessite également que le connecteur BlueXP soit déployé dans le même emplacement sur site.

Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

Ajout du serveur de base de données

Ajoutez le serveur de base de données où se trouvent les schémas.

1. Dans la page Configuration des environnements de travail, cliquez sur **Ajouter une source de données > Ajouter un serveur de base de données**.



2. Entrez 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. Entrez les identifiants afin que Cloud Data SENSE puisse accéder au serveur.
- e. Cliquez sur **Ajouter serveur DB**.

Add DB Server

To activate Compliance on Databases, first add a Database Server. After this step, you'll be able to select which Database Schemas you would like to activate Compliance for.

Database

Database Type

Host Name or IP Address

Port

Service Name

Credentials

Username

Password

Add DB Server

Cancel

La base de données est ajoutée à la liste des environnements de travail.

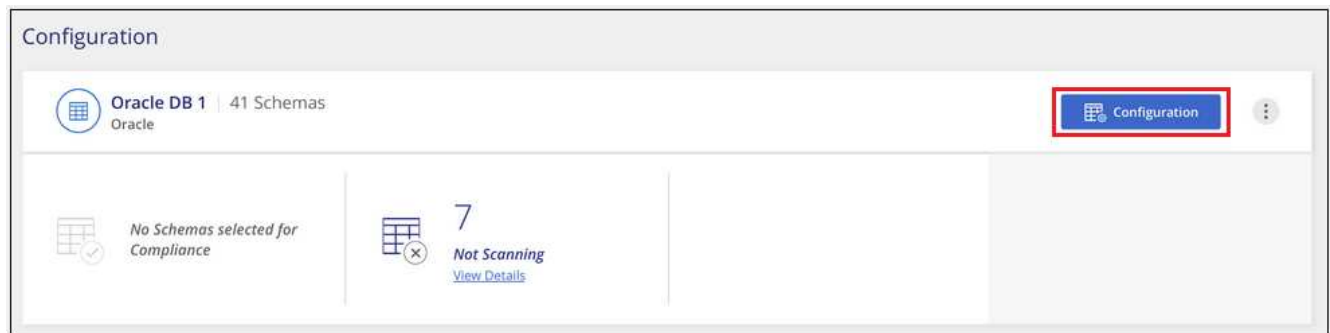
Activation et désactivation des analyses de conformité sur les schémas de base de données

Vous pouvez arrêter ou démarrer la numérisation complète de vos schémas à tout moment.



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

1. Dans la page *Configuration*, cliquez sur le bouton **Configuration** de la base de données à configurer.



2. Sélectionnez les schémas à numériser en déplaçant le curseur vers la droite.

'Working Environment Name' Configuration

28/28 Schemas selected for compliance scan 🔍 Edit Credentials

Scan	Schema Name	Status	Required Action
<input checked="" type="checkbox"/>	DB1 - SchemaName1	Not Scanning	Add Credentials ⓘ
<input checked="" type="checkbox"/>	DB1 - SchemaName2	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName3	Continuously Scanning	
<input checked="" type="checkbox"/>	DB1 - SchemaName4	Continuously Scanning	

Résultat

Cloud Data SENSE commence à analyser les schémas de base de données que vous avez activés. S'il y a des erreurs, elles apparaîtront dans la colonne État, ainsi que l'action requise pour corriger l'erreur.

En analysant les comptes OneDrive

Procédez comme suit pour lancer la numérisation des fichiers dans les dossiers OneDrive de votre utilisateur avec Cloud Data Sense.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

Vérifiez les prérequis OneDrive

Assurez-vous que vous disposez des informations d'identification Admin pour vous connecter au compte OneDrive.

2

Déployez l'instance Cloud Data SENSE

"Déployez des données adaptées au cloud" si aucune instance n'est déjà déployée.

3

Ajoutez le compte OneDrive

À l'aide des informations d'identification utilisateur Admin, connectez-vous au compte OneDrive auquel vous souhaitez accéder afin qu'il soit ajouté en tant que nouvel environnement de travail.

4

Ajoutez les utilisateurs et sélectionnez le type de numérisation

Ajoutez la liste des utilisateurs du compte OneDrive que vous souhaitez numériser et sélectionnez le type de numérisation. Vous pouvez ajouter jusqu'à 100 utilisateurs à la fois.

Vérification des exigences OneDrive

Avant d'activer le Cloud Data sens, lisez les conditions préalables suivantes pour vérifier que la configuration est prise en charge.

- Vous devez disposer des informations d'identification d'administrateur pour le compte OneDrive entreprise qui permet d'accéder en lecture aux fichiers de l'utilisateur.
- Vous aurez besoin d'une liste séparée en ligne des adresses e-mail pour tous les utilisateurs dont vous souhaitez numériser les dossiers OneDrive.

Déploiement de l'instance Cloud Data Sense

Déployez Cloud Data si aucune instance n'est déjà déployée.

Il peut y avoir un sens des données "[déploiement dans le cloud](#)" ou "[dans un emplacement sur site avec accès à internet](#)".

Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

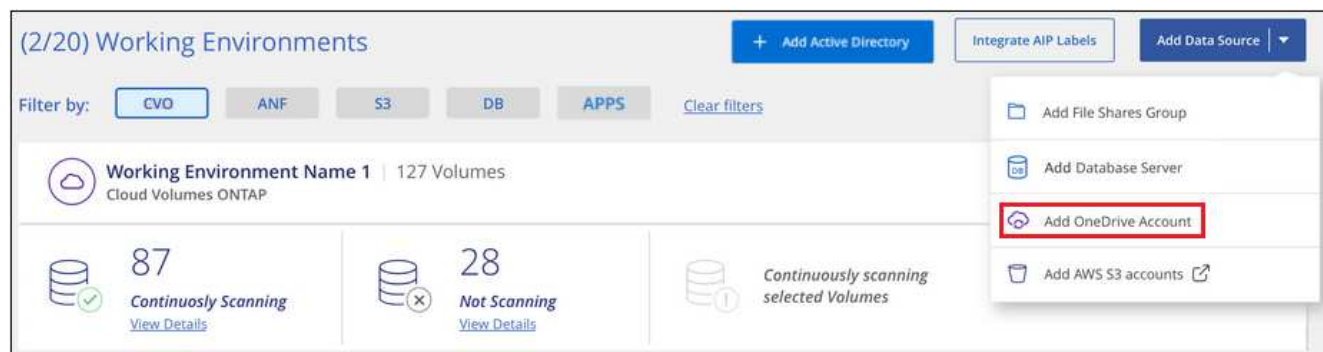
Il est également possible de détecter des données "[déploiement dans un emplacement sur site qui ne dispose pas d'un accès internet](#)". Cependant, vous devez fournir un accès Internet à quelques points de terminaison sélectionnés pour analyser vos fichiers OneDrive locaux. "[Voir la liste des points finaux requis ici](#)".

Ajout du compte OneDrive

Ajoutez le compte OneDrive où résident les fichiers utilisateur.

Étapes

1. Dans la page Configuration des environnements de travail, cliquez sur **Ajouter une source de données > Ajouter un compte OneDrive**.



2. Dans la boîte de dialogue Ajouter un compte OneDrive, cliquez sur **connexion à OneDrive**.
3. Dans la page Microsoft qui s'affiche, sélectionnez le compte OneDrive et entrez l'utilisateur et le mot de passe d'administration requis, puis cliquez sur **Accept** pour permettre à Cloud Data SENSE de lire les données de ce compte.

Le compte OneDrive est ajouté à la liste des environnements de travail.

Ajout d'utilisateurs OneDrive aux analyses de conformité

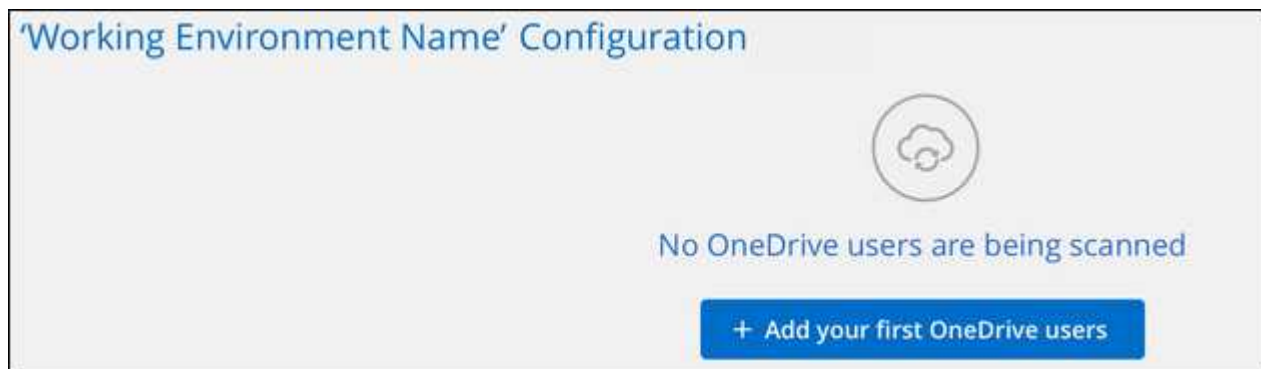
Vous pouvez ajouter des utilisateurs OneDrive individuels ou tous vos utilisateurs OneDrive, de sorte que leurs fichiers soient analysés par Cloud Data Sense.

Étapes

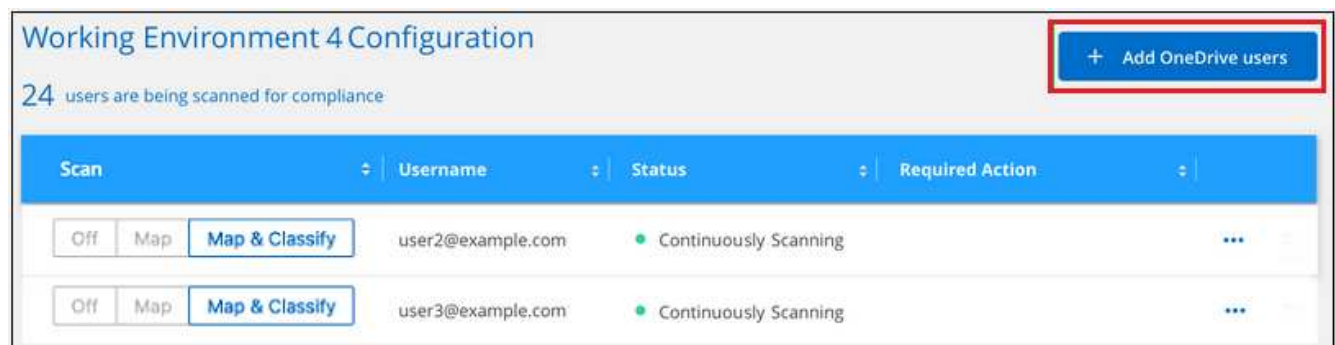
1. Dans la page *Configuration*, cliquez sur le bouton **Configuration** du compte OneDrive.



2. S'il s'agit de la première fois que vous ajoutez des utilisateurs pour ce compte OneDrive, cliquez sur **Ajouter vos premiers utilisateurs OneDrive**.

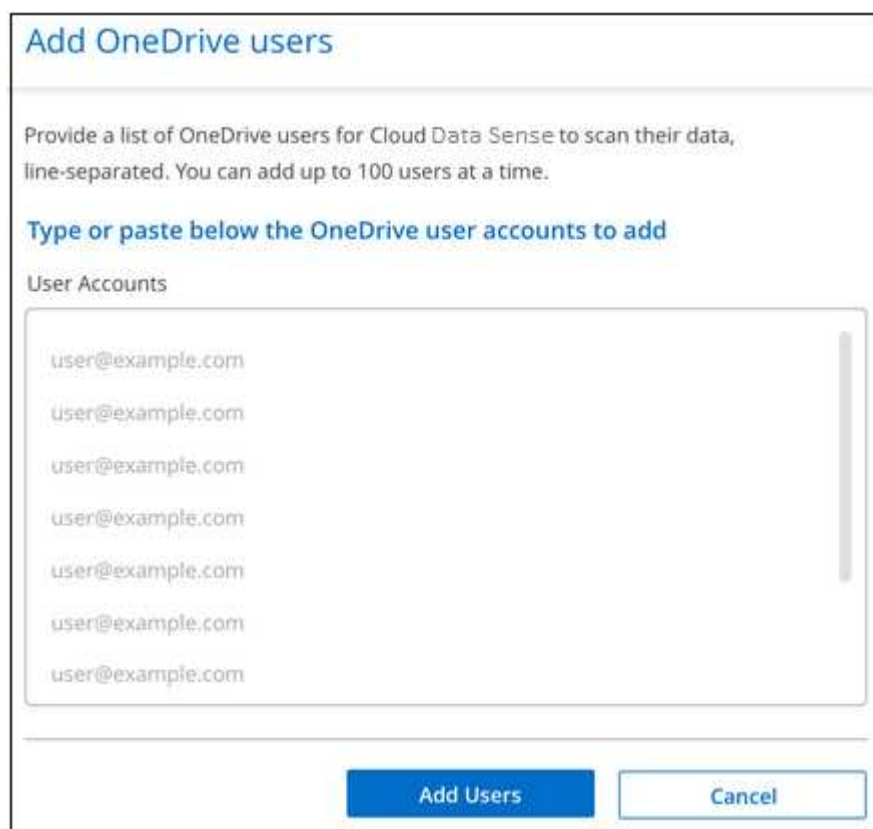


Si vous ajoutez des utilisateurs supplémentaires à partir d'un compte OneDrive, cliquez sur **Ajouter des utilisateurs OneDrive**.



3. Ajoutez les adresses e-mail des utilisateurs dont vous souhaitez numériser les fichiers - une adresse e-

mail par ligne (jusqu'à 100 par session) - et cliquez sur **Ajouter utilisateurs**.



Une boîte de dialogue de confirmation affiche le nombre d'utilisateurs ajoutés.

Si la boîte de dialogue répertorie tous les utilisateurs qui n'ont pas pu être ajoutés, capturez ces informations pour résoudre le problème. Dans certains cas, vous pouvez ajouter à nouveau l'utilisateur avec une adresse e-mail corrigée.

4. Activez les analyses de mappage uniquement, ou les analyses de mappage et de classification, sur les fichiers utilisateur.

À :	Procédez comme suit :
Activer les analyses de mappage uniquement sur les fichiers utilisateur	Cliquez sur carte
Activer les analyses complètes sur les fichiers utilisateur	Cliquez sur carte et classement
Désactiver la numérisation sur les fichiers utilisateur	Cliquez sur Off

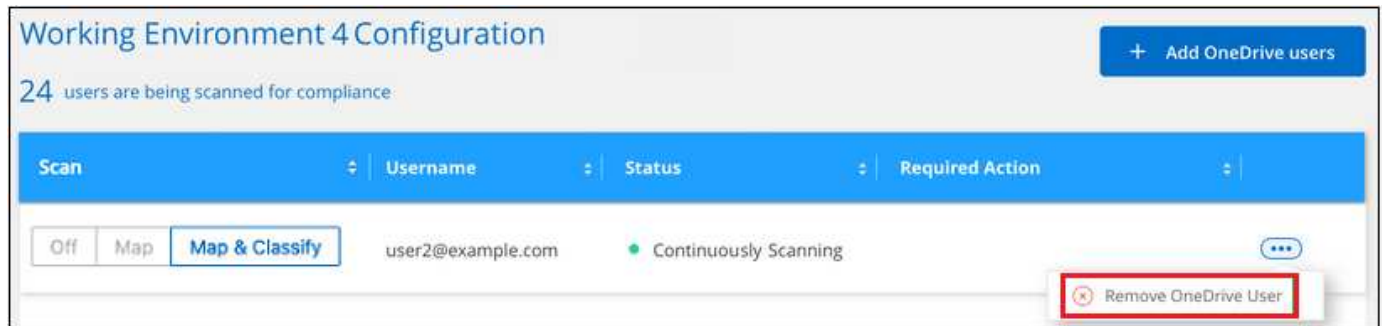
Résultat

Cloud Data SENSE commence à analyser les fichiers pour les utilisateurs que vous avez ajoutés, et les résultats sont affichés dans le tableau de bord et à d'autres emplacements.

Suppression d'un utilisateur OneDrive des analyses de conformité

Si des utilisateurs quittent l'entreprise ou si leur adresse e-mail change, vous pouvez supprimer à tout moment les utilisateurs OneDrive de faire analyser leurs fichiers. Il vous suffit de cliquer sur **Supprimer l'utilisateur**

OneDrive dans la page de configuration.



Notez que vous pouvez "[Supprimez l'ensemble du compte OneDrive de Data Sense](#)" Si vous ne souhaitez plus numériser de données utilisateur à partir du compte OneDrive.

Analyse des comptes SharePoint

Suivez quelques étapes pour commencer à analyser les fichiers de vos comptes sur site SharePoint Online et SharePoint avec Cloud Data Sense.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

Consultez les prérequis pour SharePoint

Assurez-vous que vous disposez des informations d'identification Admin pour vous connecter au compte SharePoint et que vous disposez des URL des sites SharePoint que vous souhaitez analyser.

2

Déployez l'instance Cloud Data SENSE

"[Déployez des données adaptées au cloud](#)" si aucune instance n'est déjà déployée.

3

Connectez-vous au compte SharePoint

À l'aide des informations d'identification utilisateur Admin, connectez-vous au compte SharePoint auquel vous souhaitez accéder afin qu'il soit ajouté en tant que nouvelle source de données/environnement de travail.

4

Ajoutez les URL du site SharePoint à analyser

Ajoutez la liste des URL du site SharePoint que vous souhaitez analyser dans le compte SharePoint et sélectionnez le type de numérisation. Vous pouvez ajouter jusqu'à 100 URL à la fois.

Révision des exigences SharePoint

Lisez les conditions préalables suivantes pour vous assurer que vous êtes prêt à activer Cloud Data SENSE sur un compte SharePoint.

- Vous devez disposer des informations d'identification d'administrateur pour le compte SharePoint qui fournissent un accès en lecture à tous les sites SharePoint.
- Pour les solutions SharePoint sur site, vous aurez également besoin de l'URL de SharePoint Server.
- Vous aurez besoin d'une liste séparée en plusieurs lignes des URL du site SharePoint pour toutes les données que vous souhaitez analyser.

Déploiement de l'instance Cloud Data Sense

Déployez Cloud Data si aucune instance n'est déjà déployée.

- Pour SharePoint Online, il est possible de détecter les données ["déploiement dans le cloud"](#) ou ["installé dans un emplacement sur site avec accès à internet"](#).

Il est également possible de détecter des données ["déploiement dans un emplacement sur site qui ne dispose pas d'un accès internet"](#). Cependant, vous devrez fournir un accès Internet à quelques points de terminaison sélectionnés pour analyser vos fichiers SharePoint Online. ["Voir la liste des points finaux requis ici"](#).

- Dans le cas d'une solution SharePoint sur site, Data Sense peut être installé ["dans un emplacement sur site avec accès à internet"](#) ou ["dans un emplacement sur site qui ne dispose pas d'un accès internet"](#).

Lorsque Data SENSE est installé sur un site sans accès à Internet, le connecteur BlueXP doit également être installé sur ce même site sans accès à Internet. ["En savoir plus >>"](#).

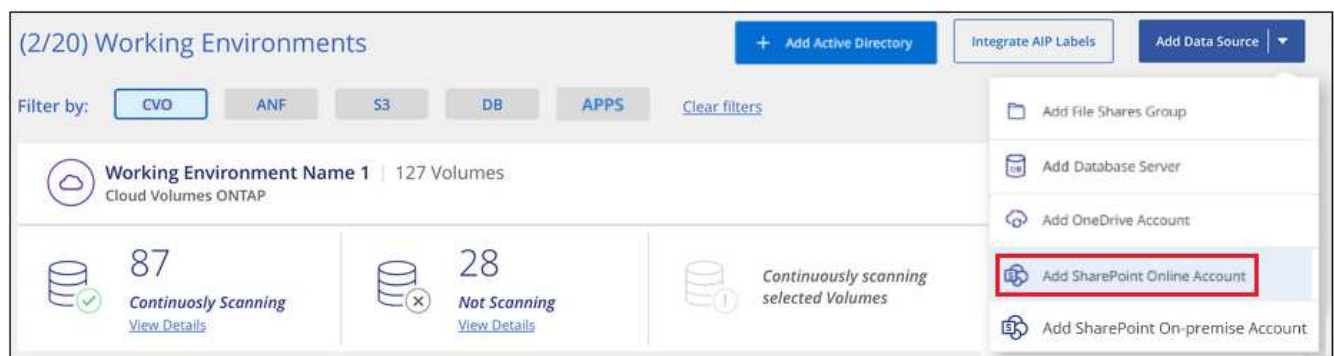
Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

Ajout d'un compte SharePoint Online

Ajoutez le compte SharePoint Online où se trouvent les fichiers utilisateur.

Étapes

1. Dans la page Configuration des environnements de travail, cliquez sur **Ajouter une source de données >** **Ajouter un compte SharePoint en ligne**.



2. Dans la boîte de dialogue Ajouter un compte SharePoint en ligne, cliquez sur **se connecter à SharePoint**.
3. Dans la page Microsoft qui s'affiche, sélectionnez le compte SharePoint et entrez l'utilisateur et le mot de passe d'administration requis, puis cliquez sur **Accept** pour permettre à Cloud Data SENSE de lire les données de ce compte.

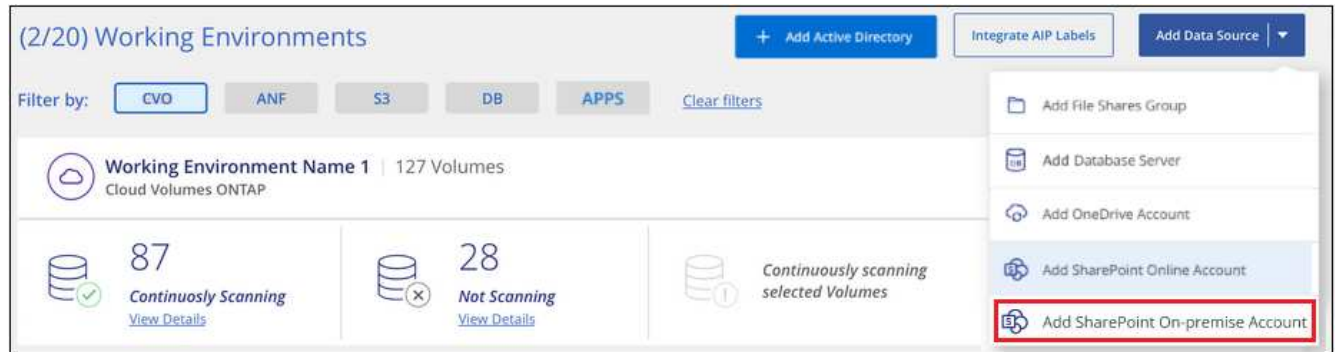
Le compte SharePoint Online est ajouté à la liste des environnements de travail.

Ajout d'un compte SharePoint sur site

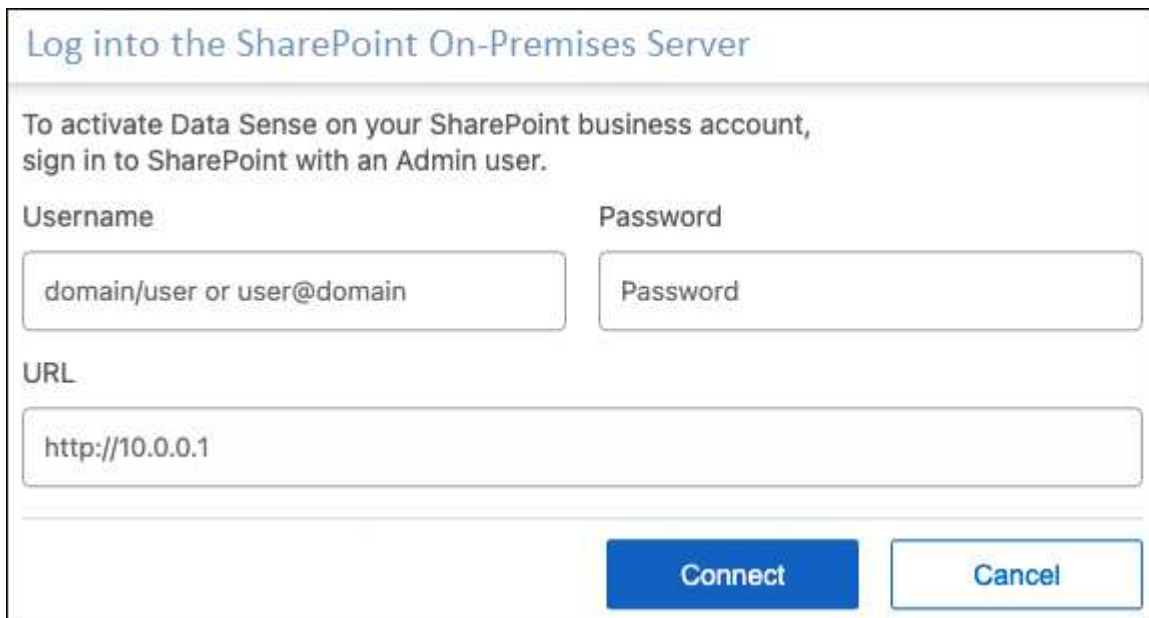
Ajoutez le compte SharePoint sur site où résident les fichiers utilisateur.

Étapes

1. Dans la page Configuration des environnements de travail, cliquez sur **Ajouter une source de données** > **Ajouter un compte SharePoint sur site**.



2. Dans la boîte de dialogue se connecter à SharePoint On-Premise Server, entrez les informations suivantes :
 - Admin user au format « domain/user » ou « user@domain », et le mot de passe admin
 - URL du serveur SharePoint

The screenshot shows the 'Log into the SharePoint On-Premises Server' dialog box. The title is 'Log into the SharePoint On-Premises Server'. Below the title, there's a message: 'To activate Data Sense on your SharePoint business account, sign in to SharePoint with an Admin user.' Below this message, there are three input fields: 'Username' with a placeholder 'domain/user or user@domain', 'Password' with a placeholder 'Password', and 'URL' with a placeholder 'http://10.0.0.1'. At the bottom right, there are two buttons: 'Connect' and 'Cancel'.

3. Cliquez sur **connexion**.

Le compte sur site SharePoint est ajouté à la liste des environnements de travail.

Ajout de sites SharePoint aux analyses de conformité

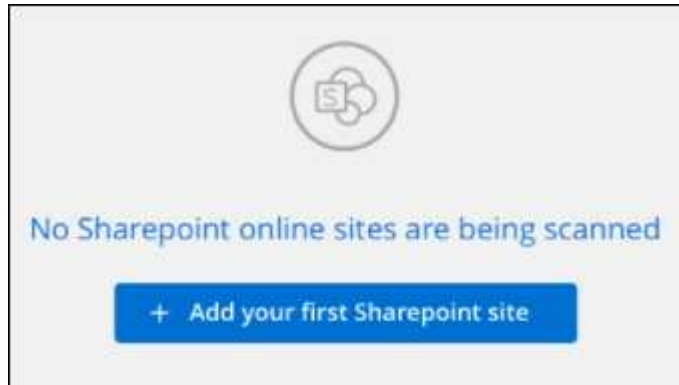
Vous pouvez ajouter des sites SharePoint individuels ou tous les sites SharePoint du compte, de sorte que les fichiers associés soient analysés par Cloud Data Sense. Les étapes sont identiques lors de l'ajout de sites SharePoint Online ou SharePoint sur site.

Étapes

1. Dans la page *Configuration*, cliquez sur le bouton **Configuration** du compte SharePoint.



2. Si c'est la première fois que vous ajoutez des sites pour ce compte SharePoint, cliquez sur **Ajouter votre premier site SharePoint**.



Si vous ajoutez des utilisateurs supplémentaires à partir d'un compte SharePoint, cliquez sur **Ajouter des sites SharePoint**.



3. Ajoutez les URL des sites dont vous voulez numériser les fichiers - une URL par ligne (jusqu'à 100 maximum par session) - et cliquez sur **Ajouter des sites**.

Une boîte de dialogue de confirmation affiche le nombre de sites ajoutés.

Si la boîte de dialogue répertorie des sites qui n'ont pas pu être ajoutés, capturez ces informations pour résoudre le problème. Dans certains cas, vous pouvez ajouter à nouveau le site avec une URL corrigée.

4. Activez les analyses de mappage uniquement, ou les analyses de mappage et de classification, sur les fichiers des sites SharePoint.

À :	Procédez comme suit :
Activer les analyses de mappage uniquement sur les fichiers	Cliquez sur carte
Activez les analyses complètes sur les fichiers	Cliquez sur carte et classement
Désactiver la numérisation sur les fichiers	Cliquez sur Off

Résultat

Cloud Data SENSE commence à analyser les fichiers des sites SharePoint que vous avez ajoutés, et les résultats sont affichés dans le tableau de bord et à d'autres emplacements.

Suppression d'un site SharePoint des analyses de conformité

Si vous supprimez un site SharePoint à l'avenir ou décidez de ne pas analyser les fichiers d'un site SharePoint, vous pouvez supprimer chaque site SharePoint de la façon dont ses fichiers sont analysés à tout moment. Il vous suffit de cliquer sur **Supprimer le site SharePoint** dans la page Configuration.

Scan	Site URL	Status	Required Action
Off Map Map & Classify	Site URL	Continuously Scanning	...
Off Map Map & Classify	Site URL	Continuously Scanning	Remove SharePoint Site

Notez que vous pouvez "[Supprimez tout le compte SharePoint de Data Sense](#)" Si vous ne souhaitez plus analyser les données utilisateur du compte SharePoint.

Numérisation de comptes Google Drive

Procédez comme suit pour lancer la numérisation des fichiers utilisateur dans vos comptes Google Drive avec Cloud Data Sense.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

Consultez les conditions préalables à Google Drive

Assurez-vous que vous disposez des informations d'identification Admin pour vous connecter au compte Google Drive.

2

Déployez des données adaptées au cloud

"[Déployez des données adaptées au cloud](#)" si aucune instance n'est déjà déployée.

3

Connectez-vous au compte Google Drive

À l'aide des informations d'identification utilisateur Admin, connectez-vous au compte Google Drive auquel vous souhaitez accéder afin qu'il soit ajouté en tant que nouvelle source de données.

4

Sélectionnez le type de numérisation des fichiers utilisateur

Sélectionnez le type de numérisation que vous souhaitez effectuer sur les fichiers utilisateur : mappage ou mappage et classification.

Vérification de la configuration requise pour Google Drive

Consultez les conditions préalables suivantes pour vous assurer que vous êtes prêt à activer Cloud Data SENSE sur un compte Google Drive.

- Vous devez disposer des informations d'identification Admin pour le compte Google Drive qui fournissent un accès en lecture aux fichiers de l'utilisateur

Restrictions actuelles

Les fonctions suivantes de détection de données ne sont pas prises en charge actuellement avec les fichiers Google Drive :

- Lorsque vous affichez des fichiers dans la page recherche de données, les actions de la barre de boutons ne sont pas actives. Vous ne pouvez copier, déplacer, supprimer, etc. Aucun fichier.
- Les autorisations ne peuvent pas être identifiées dans les fichiers de Google Drive. Aucune information d'autorisation n'est donc affichée dans la page Investigation.

Déployer des solutions Cloud Data est logique

Déployez Cloud Data si aucune instance n'est déjà déployée.

Il peut y avoir un sens des données "déploiement dans le cloud" ou "dans un emplacement sur site avec accès à internet".

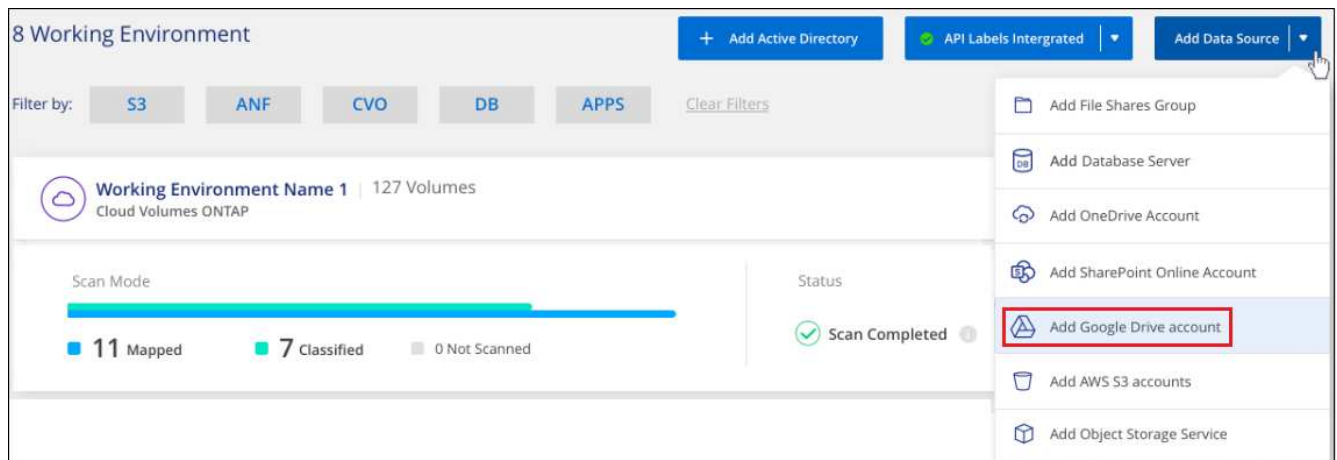
Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

Ajout du compte Google Drive

Ajoutez le compte Google Drive où résident les fichiers utilisateur. Si vous souhaitez analyser des fichiers de plusieurs utilisateurs, vous devez exécuter cette étape pour chaque utilisateur.

Étapes

1. Dans la page Configuration des environnements de travail, cliquez sur **Ajouter une source de données > Ajouter un compte Google Drive**.



2. Dans la boîte de dialogue Ajouter un compte Google Drive, cliquez sur **Connectez-vous à Google Drive**.
3. Sur la page Google qui s'affiche, sélectionnez le compte Google Drive et entrez l'utilisateur et le mot de passe d'administration requis, puis cliquez sur **Accept** pour permettre à Cloud Data SENSE de lire les données de ce compte.

Le compte Google Drive est ajouté à la liste des environnements de travail.

Sélection du type de numérisation des données utilisateur

Sélectionnez le type d'analyse que Cloud Data SENSE effectuera sur les données de l'utilisateur.

Étapes

- 1. Dans la page *Configuration*, cliquez sur le bouton **Configuration** du compte Google Drive.



- 2. Activez les analyses de mappage uniquement, ou les analyses de mappage et de classification, sur les fichiers du compte Google Drive.



À :	Procédez comme suit :
Activer les analyses de mappage uniquement sur les fichiers	Cliquez sur carte
Activez les analyses complètes sur les fichiers	Cliquez sur carte et classement
Désactiver la numérisation sur les fichiers	Cliquez sur Off

Résultat

Cloud Data SENSE commence à analyser les fichiers du compte Google Drive que vous avez ajouté et les résultats sont affichés dans le tableau de bord et à d'autres emplacements.

Suppression d'un compte Google Drive des analyses de conformité

Étant donné que les fichiers Google Drive d'un seul utilisateur font partie d'un seul compte Google Drive, si vous voulez arrêter de numériser des fichiers à partir du compte Google Drive d'un utilisateur, alors vous devriez "[Supprimez le compte Google Drive de Data Sense](#)".

Analyse des partages de fichiers

Procédez comme suit pour lancer l'analyse des partages de fichiers NFS ou CIFS non NetApp directement avec Cloud Data SENSE. Ces partages de fichiers peuvent résider sur site ou dans le cloud.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.



Vérifiez les conditions préalables au partage de fichiers

Pour les partages CIFS (SMB), assurez-vous que vous disposez des identifiants pour accéder aux partages.

2

Déployez l'instance Cloud Data SENSE

"Déployez des données adaptées au cloud" si aucune instance n'est déjà déployée.

3

Créez un groupe pour conserver les partages de fichiers

Le groupe est un conteneur pour les partages de fichiers que vous souhaitez analyser et il est utilisé comme nom d'environnement de travail pour ces partages de fichiers.

4

Ajoutez les partages de fichiers et sélectionnez les partages à analyser

Ajoutez la liste des partages de fichiers que vous souhaitez numériser et sélectionnez le type de numérisation. Vous pouvez ajouter jusqu'à 100 partages de fichiers à la fois.

Vérification des exigences relatives au partage de fichiers

Avant d'activer le Cloud Data sens, lisez les conditions préalables suivantes pour vérifier que la configuration est prise en charge.

- Ils peuvent être hébergés partout, y compris dans le cloud ou sur site. Il s'agit de partages de fichiers qui résident sur des systèmes de stockage non NetApp.
- Il faut une connectivité réseau entre l'instance Data Sense et les partages.
- Assurez-vous que ces ports sont ouverts à l'instance de détection de données :
 - Pour NFS – ports 111 et 2049.
 - Pour CIFS – ports 139 et 445.
- Vous aurez besoin de la liste des partages que vous souhaitez ajouter au format `<host_name>:/<share_path>`. Vous pouvez entrer les partages individuellement ou fournir une liste séparée par des lignes des partages de fichiers que vous souhaitez scanner.
- Pour les partages CIFS (SMB), assurez-vous que vous disposez des identifiants Active Directory qui fournissent un accès en lecture aux partages. Les identifiants d'administrateur sont à privilégier dans le cas où Cloud Data SENSE doit analyser toutes les données qui exigent des autorisations élevées.

Si vous voulez vous assurer que vos fichiers "dernières heures d'accès" sont inchangés par les analyses de classification de détection de données, nous recommandons à l'utilisateur de disposer de l'autorisation Write Attributes. Si possible, nous vous recommandons de faire en sorte que l'utilisateur configuré Active Directory fasse partie d'un groupe parent de l'organisation qui dispose des autorisations pour tous les fichiers.

Déploiement de l'instance Cloud Data Sense

Déployez Cloud Data si aucune instance n'est déjà déployée.

Si vous scannez des partages de fichiers NFS ou CIFS non NetApp accessibles via Internet, vous pouvez "Déployez les données du cloud dans le cloud" ou "Déployer Data Sense dans un emplacement sur site avec accès Internet".

Si vous scannez des partages de fichiers NFS ou CIFS non NetApp installés dans un site sombre qui n'offrent pas d'accès à Internet, vous devez le faire "[Déployez les données cloud sur site qui ne disposent pas d'un accès Internet](#)". Cela nécessite également que le connecteur BlueXP soit déployé dans le même emplacement sur site.

Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

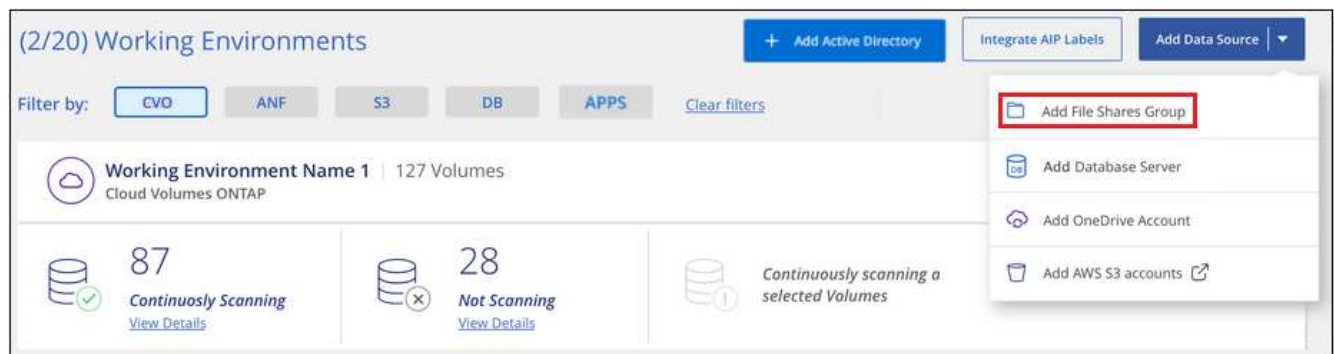
Création du groupe pour les partages de fichiers

Vous devez ajouter un « groupe » de partages de fichiers avant de pouvoir ajouter vos partages de fichiers. Le groupe est un conteneur pour les partages de fichiers que vous souhaitez analyser et le nom du groupe est utilisé comme nom d'environnement de travail pour ces partages de fichiers.

Vous pouvez mélanger des partages NFS et CIFS dans le même groupe, mais tous les partages de fichiers CIFS d'un groupe doivent utiliser les mêmes informations d'identification Active Directory. Si vous prévoyez d'ajouter des partages CIFS qui utilisent des identifiants différents, vous devez créer un groupe distinct pour chaque ensemble unique d'informations d'identification.

Étapes

1. Dans la page Configuration des environnements de travail, cliquez sur **Ajouter une source de données > Ajouter un groupe de partages de fichiers**.



2. Dans la boîte de dialogue Ajouter un groupe de partages de fichiers, entrez le nom du groupe de partages et cliquez sur **Continuer**.

Le nouveau groupe de partages de fichiers est ajouté à la liste des environnements de travail.

Ajout de partages de fichiers à un groupe

Vous ajoutez des partages de fichiers au groupe de partages de fichiers afin que les fichiers de ces partages soient analysés par Cloud Data Sense. Vous ajoutez les partages au format `<host_name>:/<share_path>`.

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

Lorsque vous ajoutez à la fois des partages NFS et CIFS au sein d'un seul groupe, vous devez recommencer le processus à deux reprises, après avoir ajouté des partages NFS, puis à nouveau en ajoutant les partages CIFS.

Étapes

1. Dans la page *Working Environments*, cliquez sur le bouton **Configuration** pour le groupe de partages de fichiers.



2. Si c'est la première fois que vous ajoutez des partages de fichiers pour ce groupe de partages de fichiers, cliquez sur **Ajouter vos premiers partages**.



Si vous ajoutez des partages de fichiers à un groupe existant, cliquez sur **Ajouter des partages**.



3. Sélectionnez le protocole pour les partages de fichiers que vous ajoutez, ajoutez les partages de fichiers que vous souhaitez analyser - un partage de fichiers par ligne - et cliquez sur **Continuer**.

Lors de l'ajout de partages CIFS (SMB), vous devez entrer les identifiants Active Directory qui fournissent un accès en lecture aux partages. Les identifiants d'administrateur sont privilégiés.

Une boîte de dialogue de confirmation affiche le nombre de partages ajoutés.

Si la boîte de dialogue répertorie tous les partages qui n'ont pas pu être ajoutés, capturez ces informations pour résoudre le problème. Dans certains cas, vous pouvez ajouter à nouveau le partage avec un nom d'hôte ou un nom de partage corrigé.

4. Activez les analyses de mappage uniquement, ou les analyses de mappage et de classification, sur chaque partage de fichiers.

À :	Procédez comme suit :
Activez les analyses de mappage uniquement sur les partages de fichiers	Cliquez sur carte
Activez les analyses complètes sur les partages de fichiers	Cliquez sur carte et classement
Désactiver l'analyse sur les partages de fichiers	Cliquez sur Off

Résultat

Cloud Data Sense commence à analyser les fichiers dans les partages de fichiers que vous avez ajoutés, et les résultats sont affichés dans le Tableau de bord et à d'autres emplacements.

Suppression d'un partage de fichiers des analyses de conformité

Si vous n'avez plus besoin d'analyser certains partages de fichiers, vous pouvez supprimer chaque partage de fichiers de l'analyse de leurs fichiers à tout moment. Il vous suffit de cliquer sur **Supprimer le partage** dans la page Configuration.



Analyse du stockage objet à l'aide du protocole S3

Suivez quelques étapes pour commencer à analyser les données dans le stockage objet directement avec Cloud Data Sense. La fonction Data Sense peut analyser les données depuis n'importe quel service de stockage objet utilisant le protocole simple Storage Service (S3). Notamment NetApp StorageGRID, IBM Cloud Object Store, Azure Blob (via MiniO), Linode, B2 Cloud Storage, Amazon S3, et bien plus encore.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

Examiner les prérequis en matière de stockage objet

Vous devez disposer de l'URL du terminal pour vous connecter au service de stockage objet.

Vous devez disposer de la clé d'accès et de la clé secrète du fournisseur de stockage objet pour que le Cloud Data SENSE puisse accéder aux compartiments.

2

Déployez l'instance Cloud Data SENSE

"[Déployez des données adaptées au cloud](#)" si aucune instance n'est déjà déployée.

3

Ajoutez le service de stockage objet

Ajoutez le service de stockage objet au sens des données dans le cloud.

4

Sélectionnez les compartiments à numériser

Sélectionnez les compartiments que vous souhaitez analyser et Cloud Data SENSE commence à les analyser.

Examen des besoins en stockage objet

Avant d'activer le Cloud Data sens, lisez les conditions préalables suivantes pour vérifier que la configuration est prise en charge.

- Vous devez disposer de l'URL du terminal pour vous connecter au service de stockage objet.
- Vous devez disposer de la clé d'accès et de la clé secrète du fournisseur de stockage objet afin que Data Sense puisse accéder aux compartiments.
- La prise en charge d'Azure Blob requiert que vous utilisiez le "Service MiniO".

Déploiement de l'instance Cloud Data Sense

Déployez Cloud Data si aucune instance n'est déjà déployée.

Si vous analysant des données à partir du stockage objet S3 accessible via Internet, vous pouvez "[Déployez les données du cloud dans le cloud](#)" ou "[Déployer Data Sense dans un emplacement sur site avec accès Internet](#)".

Si vous analysant les données à partir du stockage objet S3 qui a été installé dans un site sombre mais qui n'a pas d'accès à Internet, vous devez "[Déployez les données cloud sur site qui ne disposent pas d'un accès Internet](#)". Cela nécessite également que le connecteur BlueXP soit déployé dans le même emplacement sur site.

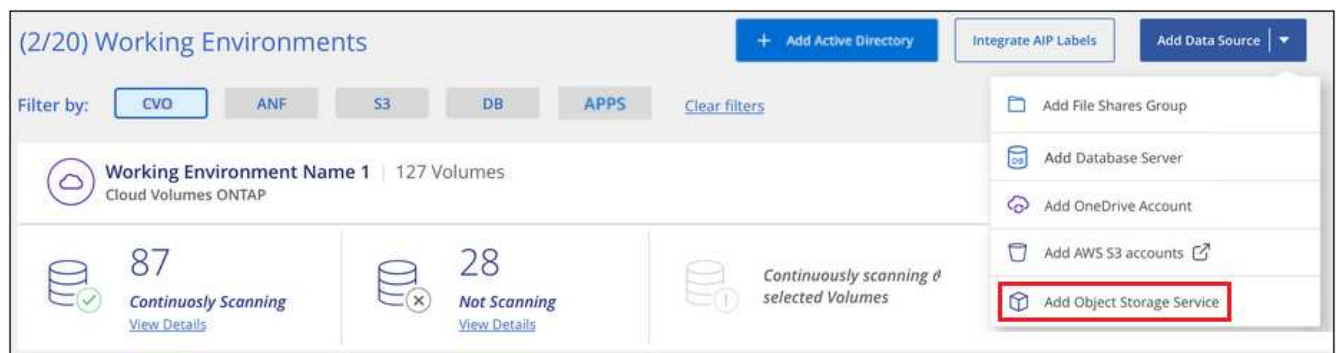
Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

Ajout du service de stockage objet au sens Cloud Data

Ajoutez le service de stockage objet.

Étapes

1. Dans la page Configuration des environnements de travail, cliquez sur **Ajouter une source de données > Ajouter un service de stockage d'objet**.



2. Dans la boîte de dialogue Ajouter un service de stockage objet, entrez les détails du service de stockage objet et cliquez sur **Continuer**.
 - a. Entrez le nom que vous souhaitez utiliser pour l'environnement de travail. Ce nom doit correspondre au nom du service de stockage objet auquel vous vous connectez.
 - b. Entrez l'URL du point final pour accéder au service de stockage d'objets.
 - c. Entrez la clé d'accès et la clé secrète pour que le cloud Data SENSE puisse accéder aux compartiments du stockage objet.

Add Object Storage Service

Cloud Data Sense can scan data from any Object Storage service which uses the S3 protocol. This includes NetApp StorageGRID, IBM Object Store, and more.

To continue, enter the following information. In the next steps you'll need to select the buckets you want to scan.

Name the Working Environment	Endpoint URL
<input type="text" value="object_myIBM"/>	<input type="text" value="http://my.endpoint.com"/>
Access Key	Secret Key
<input type="text" value="AJUKD0574NDJG86795"/>	<input type="text" value="....."/>

Résultat

Le nouveau service de stockage objet est ajouté à la liste des environnements de travail.

Activation et désactivation des analyses de conformité dans les compartiments de stockage objet

Une fois que vous avez activé le contrôle des données dans le cloud sur votre service de stockage objet, l'étape suivante consiste à configurer les compartiments à analyser. Data Sense détecte ces compartiments et les affiche dans l'environnement de travail que vous avez créé.

Étapes

1. Dans la page Configuration, cliquez sur **Configuration** dans l'environnement de travail Object Storage Service.

(1/20) Working Environments

Filter by: CVO ANF S3 DB APPS **OB.STG** [Clear filters](#)

Rstor Integrated | 41 Buckets

Configuration

23 Continuously Scanning [View Details](#)

All Buckets selected for Compliance

Continuously scanning all selected Buckets

2. Activez les analyses de mappage uniquement ou les analyses de mappage et de classification sur vos compartiments.

Rstor Integrated Configuration			
3/55 Buckets selected for Compliance scan			
Scan	Storage Repository (Bucket) ↓↑	Status ↓↑	Required Action ↓↑
Off Map Map & Classify	logs-759995470648-us-east-1	● Not Scanning	
Off Map Map & Classify	logs-759995470648-us-west-2	● Not Scanning	
Off Map Map & Classify	carstock	● Continuously Scanning	

À :	Procédez comme suit :
Activez les acquisitions avec mappage uniquement sur un compartiment	Cliquez sur carte
Activer les acquisitions complètes sur un compartiment	Cliquez sur carte et classement
Désactiver l'acquisition sur un godet	Cliquez sur Off

Résultat

Cloud Data Sense commence l'analyse des compartiments que vous avez activés. En cas d'erreur, elles apparaîtront dans la colonne État, ainsi que l'action requise pour corriger l'erreur.

Informations sur le copyright

Copyright © 2022 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.