



Améliorez la confidentialité des données

Cloud Manager 3.8

NetApp
March 25, 2024

Sommaire

- Améliorez la confidentialité des données 1
- Découvrez Cloud Compliance 1
- Commencez 5
- La visibilité et le contrôle des données privées 28
- Affichage des rapports de conformité 42
- Réponse à une demande d'accès à un sujet de données 47
- Désactivation de Cloud Compliance 49
- Questions les plus fréquemment posées concernant Cloud Compliance 50

Améliorez la confidentialité des données

Découvrez Cloud Compliance

Cloud Compliance est un service de confidentialité et de conformité des données conçu pour Cloud Manager qui analyse les volumes, les compartiments Amazon S3 et les bases de données afin d'identifier les données personnelles et sensibles qui résident dans ces fichiers. Avec la technologie d'intelligence artificielle (IA), Cloud Compliance aide les entreprises à comprendre le contexte des données et à identifier les données sensibles.

["Découvrez les utilisations de Cloud Compliance"](#).

Caractéristiques

Cloud Compliance fournit plusieurs outils qui vous aideront dans vos efforts de conformité. Vous pouvez utiliser Cloud Compliance pour :

- Identifier les informations à caractère personnel
- Identifier une vaste gamme d'informations sensibles, conformément aux réglementations en matière de confidentialité RGPD, CCPA, PCI et HIPAA
- Répondre aux demandes d'accès aux données (DSAR, Data Subject Access Requests)

Environnements de travail et sources de données pris en charge

Cloud Compliance peut analyser les données à partir de plusieurs types de sources :

- Cloud Volumes ONTAP dans AWS
- Cloud Volumes ONTAP dans Azure
- Azure NetApp Files
- Amazon S3
- Bases de données résidant où que vous soyez (elles ne nécessitent pas que la base de données réside dans un environnement de travail)

Remarque : pour Azure NetApp Files, Cloud Compliance peut analyser tous les volumes se trouvant dans la même région que Cloud Manager.

Le coût

- Le coût d'utilisation de la conformité dans le cloud dépend de la quantité de données à analyser. Depuis le 7 octobre 2020, les 1 premiers To de données analysés par Cloud Compliance dans un espace de travail Cloud Manager sont gratuits. Cela inclut les données des volumes Cloud Volumes ONTAP, des volumes Azure NetApp Files, des compartiments Amazon S3 et des schémas de base de données. Un abonnement à AWS ou Azure Marketplace est nécessaire pour poursuivre l'analyse des données après ce point. Voir ["tarifs"](#) pour plus d'informations.

["Découvrez comment vous inscrire"](#).

- L'installation de Cloud Compliance nécessite le déploiement d'une instance cloud, ce qui entraîne des frais supplémentaires du fournisseur cloud sur lequel elle est déployée. Voir la [type d'instance déployé pour chaque fournisseur cloud](#)
- Cloud Compliance requiert que vous ayez déployé un connecteur. Dans la plupart des cas, vous disposez déjà d'un connecteur en raison des autres services et stockages que vous utilisez dans Cloud Manager. L'instance de connecteur entraîne des frais supplémentaires du fournisseur cloud sur lequel elle est déployée. Voir la "[type d'instance déployé pour chaque fournisseur cloud](#)".

Coûts de transfert de données

Les coûts de transfert de données dépendent de votre configuration. Si l'instance Cloud Compliance et la source de données se trouvent dans la même zone de disponibilité et la même région, aucun coût de transfert de données n'est observé. Mais si la source de données, telle qu'un cluster Cloud Volumes ONTAP ou un compartiment S3, se trouve dans une zone ou une région *différente* disponibilité, vous serez facturé par votre fournisseur cloud pour les coûts de transfert de données. Consultez ces liens pour en savoir plus :

- ["AWS : tarification Amazon EC2"](#)
- ["Microsoft Azure : détails de la tarification de la bande passante"](#)

Fonctionnement de Cloud Compliance

À un niveau élevé, Cloud Compliance fonctionne comme ceci :

1. Vous déployez une instance de Cloud Compliance dans Cloud Manager.
2. Vous l'activez sur un ou plusieurs environnements de travail, ou sur vos bases de données.
3. Cloud Compliance analyse les données à l'aide d'un processus de formation d'IA.
4. Dans Cloud Manager, vous cliquez sur **Compliance** et utilisez le tableau de bord et les outils de reporting fournis pour vous aider dans vos efforts de conformité.

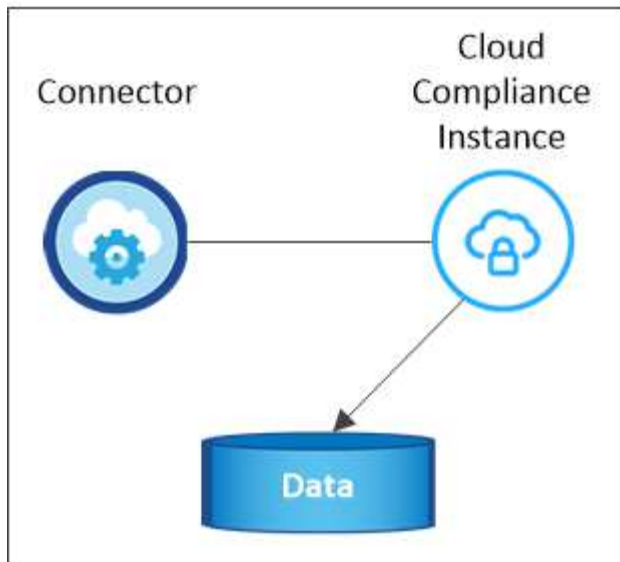
Instance Cloud Compliance

Lorsque vous activez Cloud Compliance, Cloud Manager déploie une instance Cloud Compliance dans le même sous-réseau que le connecteur. "[En savoir plus sur les connecteurs.](#)"



Si le connecteur est installé sur site, il déploie l'instance Cloud Compliance dans le même VPC ou vNet que le premier système Cloud Volumes ONTAP de la demande.

VPC or VNet



Notez les points suivants sur l'instance :

- Dans Azure, Cloud Compliance s'exécute sur une machine virtuelle standard_D16s_v3 avec un disque de 512 Go.
- Dans AWS, Cloud Compliance s'exécute sur une instance m5.4xlarge avec un disque GP2 de 500 Go.

Dans les régions où m5.4xlarge n'est pas disponible, Cloud Compliance s'exécute sur une instance m4.4xlarge.



La modification ou le redimensionnement du type d'instance/de VM n'est pas prise en charge. Vous devez utiliser la taille fournie.

- L'instance s'appelle *CloudCompliance* avec un hachage (UUID) généré concaténé. Par exemple : *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Une seule instance Cloud Compliance est déployée par connecteur.
- Les mises à niveau du logiciel Cloud Compliance sont automatisées ; vous n'avez plus à vous inquiéter.

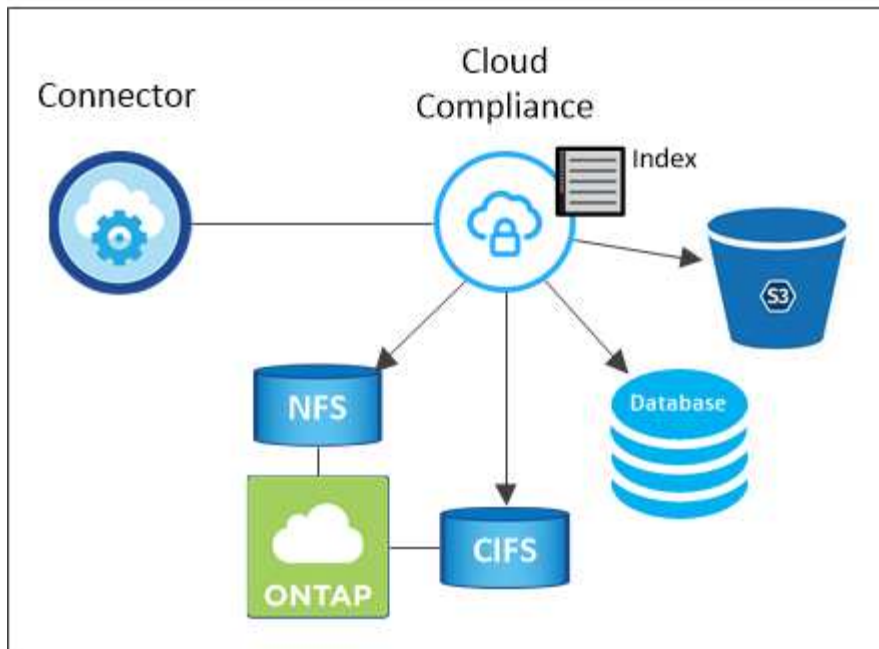


L'instance doit rester en cours d'exécution en permanence car Cloud Compliance analyse les données en continu.

Fonctionnement des acquisitions

Une fois que vous avez activé Cloud Compliance et sélectionné les volumes, compartiments ou schémas de base de données que vous souhaitez numériser, il commence immédiatement à analyser les données pour identifier les données personnelles et sensibles. Il mappe les données de votre organisation, classe chaque fichier et identifie et extrait des entités et des modèles prédéfinis dans les données. Cette analyse permet d'obtenir un index des données personnelles, des données personnelles sensibles et des catégories de données.

Cloud Compliance se connecte aux données comme tout autre client en montant les volumes NFS et CIFS. Les volumes NFS sont automatiquement accessibles en lecture seule, tandis que vous devez fournir des identifiants Active Directory pour analyser les volumes CIFS.



Après l'analyse initiale, Cloud Compliance analyse en continu chaque volume pour détecter les modifications incrémentielles (c'est pourquoi il est important de maintenir l'exécution de l'instance).

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

Informations index par Cloud Compliance

Cloud Compliance collecte, index et attribue des catégories aux données non structurées (fichiers). Les données index Cloud Compliance incluent les éléments suivants :

Métadonnées standard

Cloud Compliance collecte des métadonnées standard sur les fichiers : le type de fichier, sa taille, ses dates de création et de modification, etc.

Données personnelles

Informations personnelles identifiables telles que les adresses électroniques, les numéros d'identification ou les numéros de carte de crédit. ["En savoir plus sur les données personnelles"](#).

Données personnelles sensibles

Des types spéciaux d'informations sensibles, comme les données de santé, l'origine ethnique ou les opinions politiques, tels que définis par le RGPD et d'autres réglementations sur la confidentialité. ["En savoir plus sur les données personnelles sensibles"](#).

Catégories

Cloud Compliance divise les données analysées et les divise en plusieurs types de catégories. Les catégories sont des rubriques basées sur l'analyse par IA du contenu et des métadonnées de chaque fichier. ["En savoir plus sur les catégories"](#).

Reconnaissance de l'entité de nom

Cloud Compliance utilise l'IA pour extraire les noms des personnes physiques des documents. ["Découvrez comment répondre aux demandes d'accès aux données"](#).

Présentation du réseau

Cloud Manager déploie l'instance Cloud Compliance avec un groupe de sécurité qui active les connexions HTTP entrantes à partir de l'instance de connecteur.

Lorsque vous utilisez Cloud Manager en mode SaaS, la connexion à Cloud Manager est assurée par HTTPS. Les données privées envoyées entre votre navigateur et l'instance Cloud Compliance sont sécurisées par un chiffrement de bout en bout, ce qui signifie que NetApp et des tiers ne peuvent pas les lire.

Si vous devez utiliser l'interface utilisateur locale plutôt que l'interface utilisateur SaaS pour quelque raison que ce soit, vous pouvez toujours ["Accédez à l'interface utilisateur locale"](#).

Les règles sortantes sont complètement ouvertes. Un accès Internet est nécessaire pour installer et mettre à niveau le logiciel Cloud Compliance et pour envoyer des metrics d'utilisation.

Si vous avez des exigences de mise en réseau strictes, ["Découvrez les terminaux contacts par Cloud Compliance"](#).

Accès des utilisateurs aux informations de conformité

Le rôle attribué à chaque utilisateur donne accès à différentes fonctionnalités dans Cloud Manager et dans Cloud Compliance :

- **Les administrateurs de compte** peuvent gérer les paramètres de conformité et afficher les informations de conformité pour tous les environnements de travail.
- **Les administrateurs d'espace de travail** peuvent gérer les paramètres de conformité et afficher les informations de conformité uniquement pour les systèmes auxquels ils ont des autorisations d'accès. Si un administrateur d'espace de travail ne parvient pas à accéder à un environnement de travail dans Cloud Manager, il ne peut pas voir les informations de conformité de l'environnement de travail dans l'onglet conformité.
- Les utilisateurs disposant du rôle **Cloud Compliance Viewer** peuvent uniquement afficher les informations de conformité et générer des rapports pour les systèmes auxquels ils sont autorisés à accéder. Ces utilisateurs ne peuvent pas activer/désactiver la lecture des volumes, compartiments ou schémas de base de données.

["En savoir plus sur les rôles de Cloud Manager"](#) et comment ["ajoutez des utilisateurs avec des rôles spécifiques"](#).

Commencez

Déployez Cloud Compliance

Suivez quelques étapes pour déployer l'instance Cloud Compliance dans votre espace de travail Cloud Manager.

Démarrage rapide

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



Créer un connecteur

Si vous n'avez pas encore de connecteur, créez-en un dans Azure ou AWS. Voir "[Création d'un connecteur dans AWS](#)" ou "[Création d'un connecteur dans Azure](#)".



Passer en revue les prérequis

Assurez-vous que votre environnement cloud peut répondre aux conditions préalables, dont 16 vCPU pour l'instance Cloud Compliance, l'accès Internet sortant pour l'instance, la connectivité entre le connecteur et Cloud Compliance sur le port 80, etc. [Voir la liste complète](#).



Déployez Cloud Compliance

Lancez l'assistant d'installation pour déployer l'instance Cloud Compliance dans Cloud Manager.



Abonnez-vous au service Cloud Compliance

Les 1 premiers To de données analysés par Cloud Compliance dans Cloud Manager sont gratuits. Un abonnement à AWS ou Azure Marketplace est nécessaire pour poursuivre l'analyse des données après ce point.

Création d'un connecteur

Si vous n'avez pas encore de connecteur, créez-en un dans Azure ou AWS. Voir "[Création d'un connecteur dans AWS](#)" ou "[Création d'un connecteur dans Azure](#)". Dans la plupart des cas, un connecteur sera probablement configuré avant d'essayer d'activer Cloud Compliance, car la plupart du temps "[Les fonctionnalités de Cloud Manager nécessitent un connecteur](#)", mais il y a des cas où vous devez en configurer un maintenant.

Il existe certains cas où vous devez utiliser un connecteur dans AWS ou Azure pour Cloud Compliance.

- Pour analyser les données dans Cloud Volumes ONTAP dans AWS ou dans des compartiments AWS S3, vous utilisez un connecteur dans AWS.
- Pour analyser les données dans Cloud Volumes ONTAP dans Azure ou dans Azure NetApp Files, vous utilisez un connecteur dans Azure.
- Les bases de données peuvent être scannées à l'aide d'un connecteur.

Comme vous pouvez le voir, il peut y avoir des situations où vous devez utiliser "[Plusieurs connecteurs](#)".



Si vous envisagez d'analyser Azure NetApp Files, vous devez vous assurer que vous déployez dans la même région que les volumes que vous souhaitez analyser.

Vérification des prérequis

Avant de déployer Cloud Compliance, consultez les conditions préalables suivantes pour vous assurer que la configuration est prise en charge.

Activer l'accès Internet sortant

Cloud Compliance requiert un accès Internet sortant. Si votre réseau virtuel utilise un serveur proxy pour l'accès Internet, assurez-vous que l'instance Cloud Compliance dispose d'un accès Internet sortant pour contacter les points de terminaison suivants. Notez que Cloud Manager déploie l'instance Cloud Compliance dans le même sous-réseau que le connecteur.

Terminaux	Objectif
https://cloudmanager.cloud.netapp.com	Communication avec le service Cloud Manager, notamment les comptes Cloud Central.
https://netapp-cloud-account.auth0.com https://auth0.com	Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs.
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Permet à Cloud Compliance d'accéder aux manifestes et aux modèles, à l'envoi de journaux et de metrics, et de les télécharger.

Assurez-vous que Cloud Manager dispose des autorisations requises

Assurez-vous que Cloud Manager dispose des autorisations nécessaires pour déployer des ressources et créer des groupes de sécurité pour l'instance Cloud Compliance. Vous trouverez les dernières autorisations Cloud Manager dans "[Règles fournies par NetApp](#)".

Vérifiez les limites de vos CPU virtuels

Assurez-vous que la limite de vCPU de votre fournisseur de cloud permet de déployer une instance de 16 cœurs. Vous devez vérifier la limite de CPU virtuels pour la famille d'instances appropriée dans la région où Cloud Manager fonctionne.

Dans AWS, la famille d'instances est *On-Demand Standard instances*. Dans Azure, la famille d'instances est *Standard D5v3 Family*.

Pour plus de détails sur les limites des CPU virtuels, consultez les documents suivants :

- "[Documentation AWS : limites du service Amazon EC2](#)"
- "[Documentation Azure : quotas de vCPU de machine virtuelle](#)"

Assurez-vous que Cloud Manager peut accéder à Cloud Compliance

Assurez la connectivité entre le connecteur et l'instance Cloud Compliance. Le groupe de sécurité du connecteur doit autoriser le trafic entrant et sortant via le port 80 vers et depuis l'instance Cloud Compliance.

Cette connexion permet le déploiement de l'instance Cloud Compliance et vous permet d'afficher des informations dans l'onglet conformité.

Configurer la découverte de Azure NetApp Files

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

Assurez-vous que vous pouvez assurer que Cloud Compliance est en cours d'exécution

L'instance Cloud Compliance doit rester active pour analyser vos données en continu.

Assurez la connectivité du navigateur Web à Cloud Compliance

Une fois que Cloud Compliance est activé, assurez-vous que les utilisateurs accèdent à l'interface Cloud Manager à partir d'un hôte connecté à l'instance Cloud Compliance.

L'instance Cloud Compliance utilise une adresse IP privée pour s'assurer que les données indexées ne sont pas accessibles sur Internet. Par conséquent, le navigateur Web que vous utilisez pour accéder à Cloud Manager doit disposer d'une connexion à cette adresse IP privée. Cette connexion peut s'établir directement auprès d'AWS ou d'Azure (par exemple, un VPN), ou depuis un hôte situé dans le même réseau que l'instance Cloud Compliance.

Déploiement de l'instance Cloud Compliance

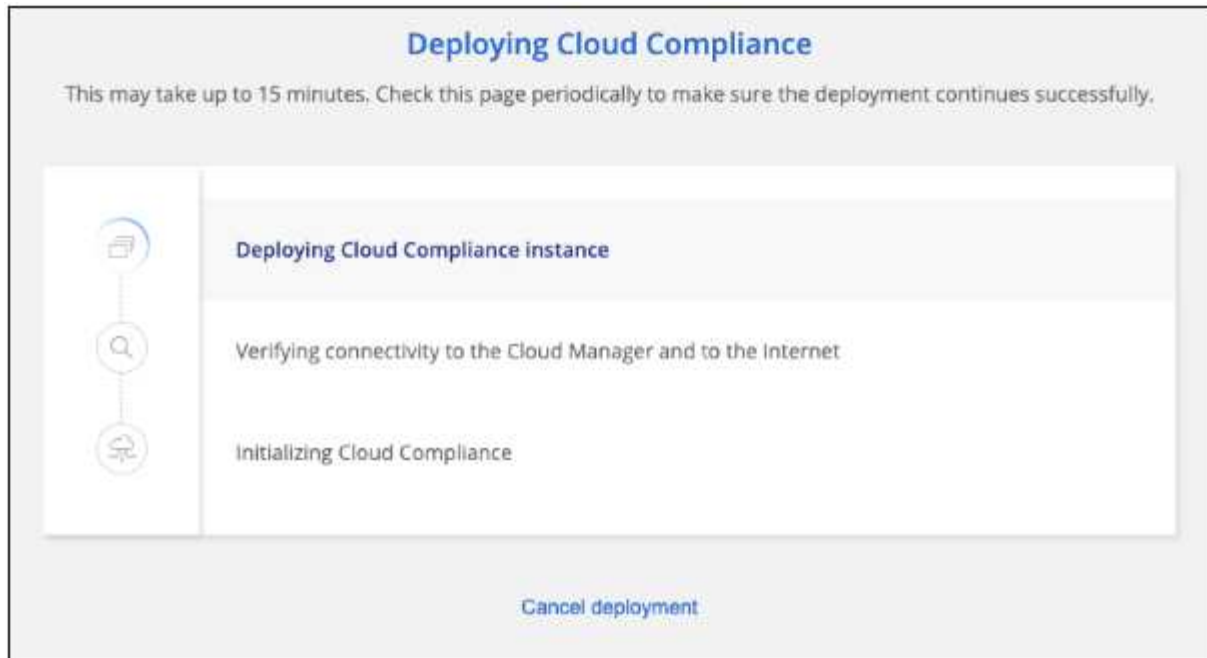
Vous déployez une instance de Cloud Compliance pour chaque instance Cloud Manager.

Étapes

1. Dans Cloud Manager, cliquez sur **Cloud Compliance**.
2. Cliquez sur **Activer Cloud Compliance** pour démarrer l'assistant de déploiement.

The screenshot shows the Azure portal interface for Cloud Compliance. The top navigation bar includes 'Working Environment', 'Compliance', 'Replication', 'Kubernetes', 'Backup & Restore', 'Monitoring', and 'Timeline'. The 'Compliance' section is active, displaying a 'Cloud Compliance' header and a 'How does it work?' link. The main content area features a section titled 'Always-on Privacy & Compliance Controls' with a description: 'Automated controls for data privacy regulations such as the GDPR, CCPA and more. Driven by powerful artificial intelligence algorithms, Cloud Compliance gets your business application data and cloud environments privacy ready.' Below this is a blue 'Activate Cloud Compliance' button. On the right, a 'Compliance Status' widget shows a 'Data Distribution' chart with 75% Non-Sensitive, 20% Personal, and 5% Sensitive Personal data. Below the chart, it shows 28,000 Personal Files and 7,000 Sensitive Personal Files, with sub-categories like Email Address, Credit Card, Health, and Ethnicity, each with 2,700 files.

3. L'assistant affiche la progression au fur et à mesure des étapes de déploiement. Il s'arrête et demande des commentaires s'il n'y a pas de problème.



4. Lorsque l'instance est déployée, cliquez sur **Continuer la configuration** pour accéder à la page *Scan Configuration*.

Résultat

Cloud Manager déploie l'instance Cloud Compliance dans votre fournisseur cloud.

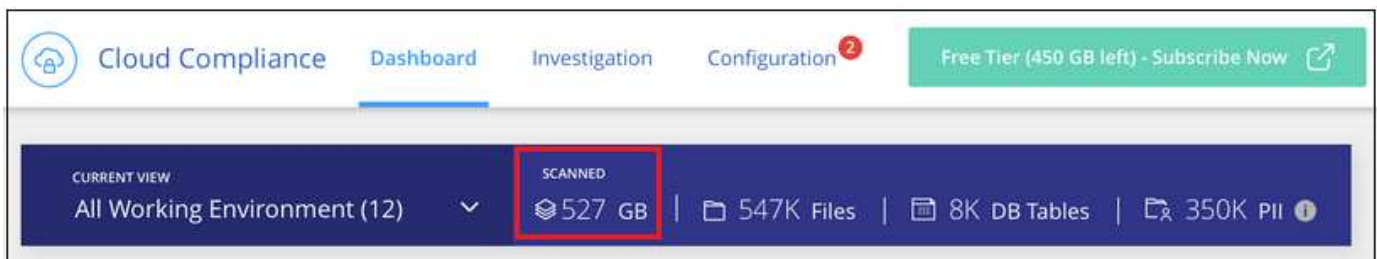
Et la suite

Dans la page Configuration de la numérisation, vous pouvez sélectionner les environnements de travail, les volumes et les compartiments que vous souhaitez rechercher pour la conformité. Vous pouvez également vous connecter à un serveur de base de données afin de scanner des schémas de base de données spécifiques. Activez Cloud Compliance sur l'une de ces sources de données.

Abonnement au service Cloud Compliance

Les 1 premiers To de données analysés par Cloud Compliance dans un espace de travail Cloud Manager sont gratuits. Un abonnement à AWS ou Azure Marketplace est nécessaire pour poursuivre l'analyse des données après ce point.

Vous pouvez vous abonner à tout moment et vous ne serez facturé que lorsque la quantité de données dépasse 1 To. La quantité totale de données analysées à partir du tableau de bord de conformité cloud est toujours visible. Et le bouton *Subscribe Now* permet de vous abonner facilement lorsque vous êtes prêt.



Remarque : si vous êtes invité par Cloud Compliance à vous abonner, mais que vous disposez déjà d'un abonnement Azure, vous utilisez probablement l'ancien abonnement **Cloud Manager** et vous devez passer au nouvel abonnement **NetApp Cloud Manager**. Voir [Modification du nouveau plan NetApp Cloud Manager dans](#)

[Azure](#) pour plus d'informations.

Étapes

Ces étapes doivent être effectuées par un utilisateur qui a le rôle *Account Admin*.

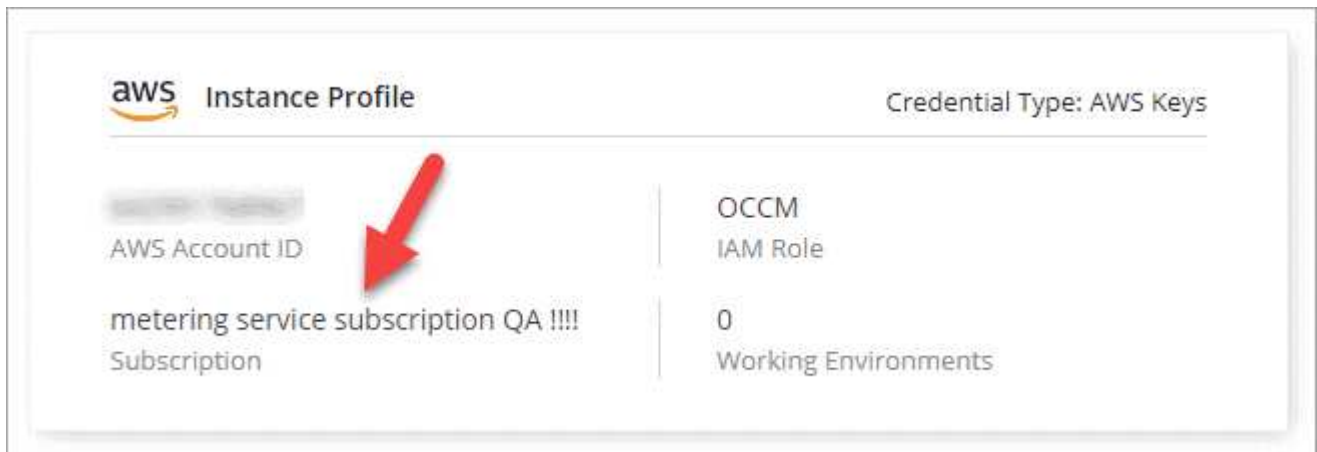
1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.



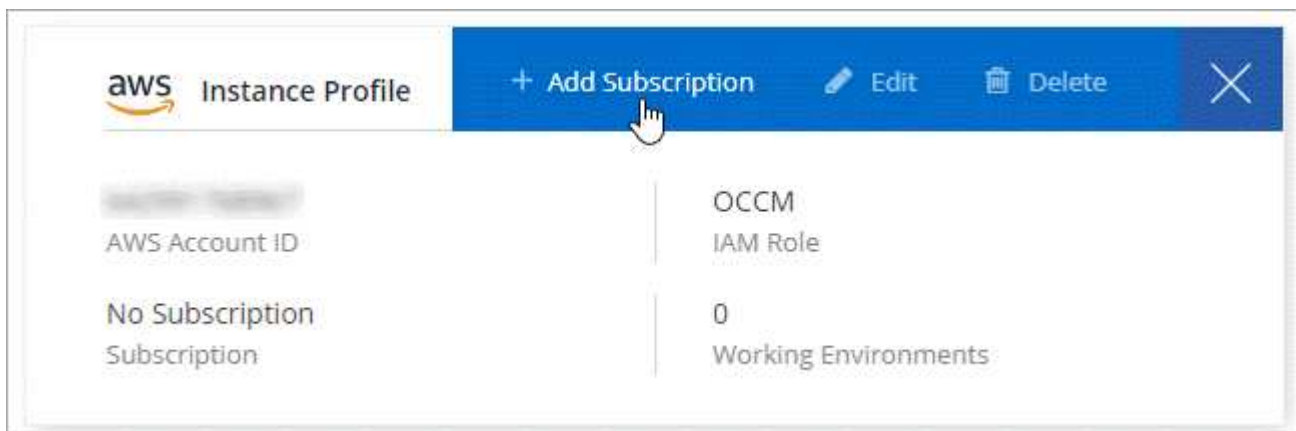
2. Recherchez les identifiants du profil d'instance AWS ou de l'identité de service géré Azure.

L'abonnement doit être ajouté au profil d'instance ou à l'identité de service géré. La charge ne fonctionnera pas autrement.

Si vous avez déjà un abonnement, alors vous êtes tout configuré - il n'y a rien d'autre que vous devez faire.



3. Si vous n'avez pas encore d'abonnement, passez le curseur sur les informations d'identification et cliquez sur le menu d'action.
4. Cliquez sur **Ajouter un abonnement**.



5. Cliquez sur **Ajouter un abonnement**, cliquez sur **Continuer** et suivez les étapes.

Découvrez dans la vidéo comment associer un abonnement Marketplace à un abonnement AWS :

► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_aws.mp4 (video)

La vidéo suivante explique comment associer un abonnement Marketplace à un abonnement Azure :

► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_azure.mp4 (video)

Modification du nouveau plan Cloud Manager dans Azure

Cloud Compliance a été ajouté à l'abonnement Azure Marketplace nommé **NetApp Cloud Manager** au 7 octobre 2020. Si vous disposez déjà de l'abonnement d'Azure **Cloud Manager** d'origine, il ne vous permettra pas d'utiliser Cloud Compliance.

Suivez ces étapes et sélectionnez le nouvel abonnement **NetApp Cloud Manager**, puis supprimez l'ancien abonnement **Cloud Manager**.



Si votre abonnement existant a été délivré avec une offre privée spéciale, vous devez contacter NetApp afin de pouvoir émettre une nouvelle offre privée spéciale avec conformité incluse.

Étapes

Ces étapes sont similaires à l'ajout d'un nouvel abonnement comme décrit ci-dessus, mais varient en quelques endroits.

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.
2. Recherchez les informations d'identification pour l'identité de service géré Azure pour laquelle vous souhaitez modifier l'abonnement et passez le curseur sur les informations d'identification, puis cliquez sur **associer l'abonnement**.

Les détails de votre abonnement Marketplace actuel s'affichent.

3. Cliquez sur **Ajouter un abonnement**, cliquez sur **Continuer** et suivez les étapes. Vous êtes redirigé vers le portail Azure pour créer votre abonnement.
4. Veillez à sélectionner le plan **NetApp Cloud Manager** qui donne accès à Cloud Compliance et non **Cloud Manager**.
5. Suivez les étapes de la vidéo pour associer un abonnement Marketplace à un abonnement Azure :

► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_azure.mp4 (video)

6. Revenez à Cloud Manager, sélectionnez le nouvel abonnement et cliquez sur **Associate**.
7. Pour vérifier que votre abonnement a changé, passez le curseur sur « i » ci-dessus dans la carte d'informations d'identification.

Vous pouvez désormais annuler votre abonnement précédent sur le portail Azure.

8. Sur le portail Azure, accédez à Software as a Service (SaaS), sélectionnez l'abonnement, puis cliquez sur **Unsubscribe**.

Activez la numérisation sur vos sources de données

Mise en route de Cloud Compliance pour Cloud Volumes ONTAP et Azure NetApp Files

Découvrez comment utiliser Cloud Compliance pour Cloud Volumes ONTAP ou Azure NetApp Files en quelques étapes.

Démarrage rapide

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



Déployez l'instance Cloud Compliance

"[Déployez Cloud Compliance dans Cloud Manager](#)" si aucune instance n'est déjà déployée.



Intégrez Cloud Compliance dans vos environnements de travail

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



Vérifiez l'accès aux volumes

Lorsque Cloud Compliance est activé, assurez-vous que le service informatique peut accéder aux volumes.

- L'instance Cloud Compliance doit disposer d'une connexion réseau à chaque sous-réseau Cloud Volumes ONTAP ou sous-réseau Azure NetApp Files.
- Les groupes de sécurité pour Cloud Volumes ONTAP doivent autoriser les connexions entrantes depuis l'instance Cloud Compliance.
- Les règles d'exportation de volumes NFS doivent autoriser l'accès à partir de l'instance Cloud Compliance.
- Pour analyser les volumes CIFS, Cloud Compliance a besoin d'identifiants Active Directory.

Cliquez sur **Cloud Compliance** > **Scan Configuration** > **Edit CIFS Credentials** et indiquez les informations d'identification. Ces identifiants peuvent être en lecture seule, mais fournir des informations d'identification administrateur garantit que Cloud Compliance peut lire les données qui requièrent des autorisations élevées.



Configurez les volumes à analyser

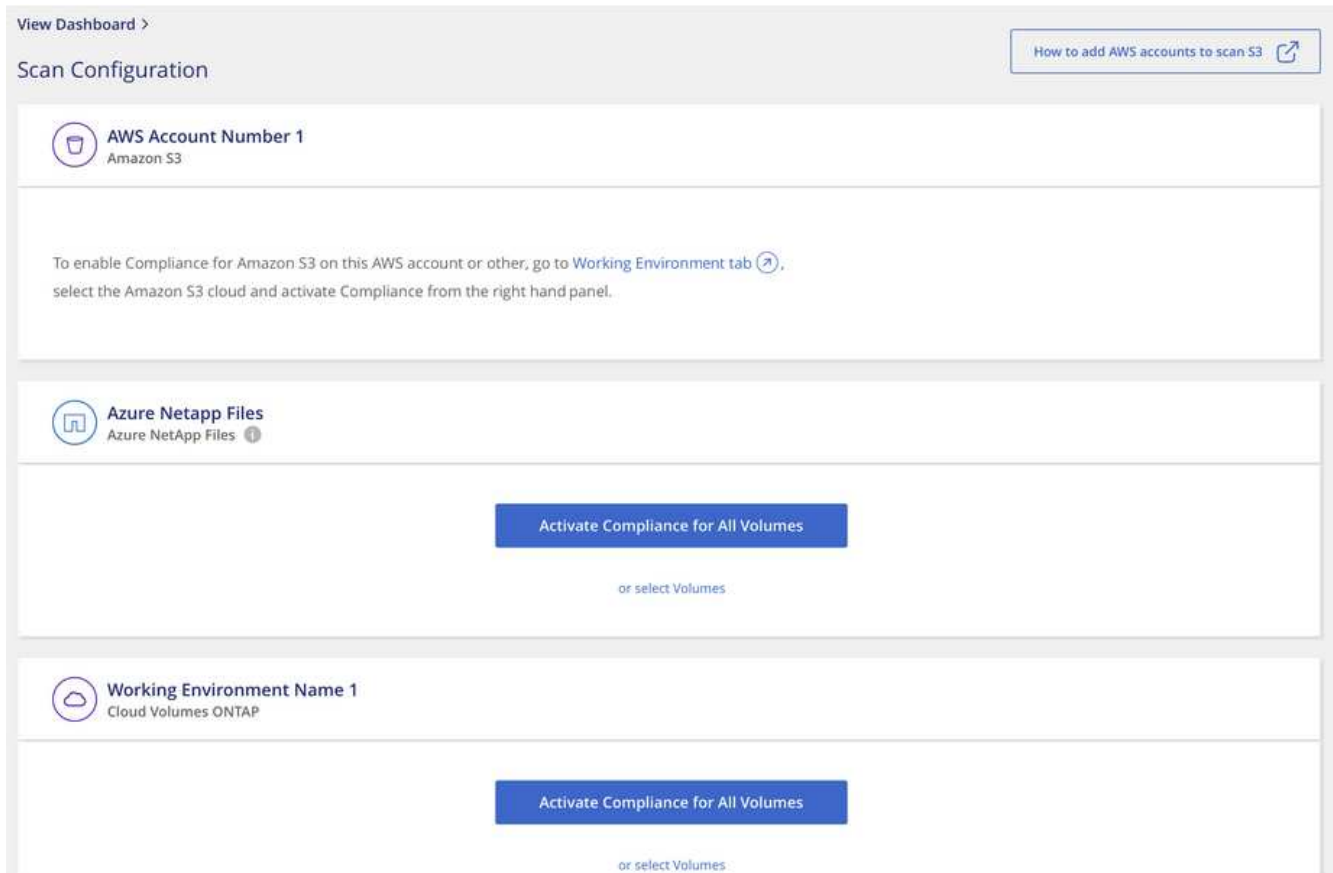
Sélectionnez les volumes que vous souhaitez analyser et Cloud Compliance commence à les analyser.

Déploiement de l'instance Cloud Compliance

"[Déployez Cloud Compliance dans Cloud Manager](#)" si aucune instance n'est déjà déployée.

Activation de la conformité cloud dans vos environnements de travail

1. En haut de Cloud Manager, cliquez sur **Cloud Compliance**, puis sélectionnez l'onglet **Configuration**.



2. Pour analyser tous les volumes d'un environnement de travail, cliquez sur **Activer la conformité pour tous les volumes**.

Pour analyser uniquement certains volumes dans un environnement de travail, cliquez sur **ou sélectionnez volumes**, puis choisissez les volumes que vous souhaitez analyser.

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

Résultat

Cloud Compliance commence l'analyse des données sur chaque environnement de travail. Les résultats seront disponibles dans le tableau de bord de conformité dès que Cloud Compliance termine les analyses initiales. Le temps nécessaire dépend de la quantité de données—il peut être de quelques minutes ou heures.

Vérification de l'accès aux volumes par Cloud Compliance

Assurez-vous que Cloud Compliance peut accéder aux volumes en vérifiant vos groupes de sécurité et vos règles d'exportation. Vous devez fournir des identifiants CIFS à Cloud Compliance pour pouvoir accéder aux volumes CIFS.

Étapes

1. Vérifiez qu'il existe une connexion réseau entre l'instance Cloud Compliance et chaque réseau qui inclut des volumes pour Cloud Volumes ONTAP ou Azure NetApp Files.



Pour Azure NetApp Files, Cloud Compliance ne peut analyser que les volumes qui se trouvent dans la même région que Cloud Manager.

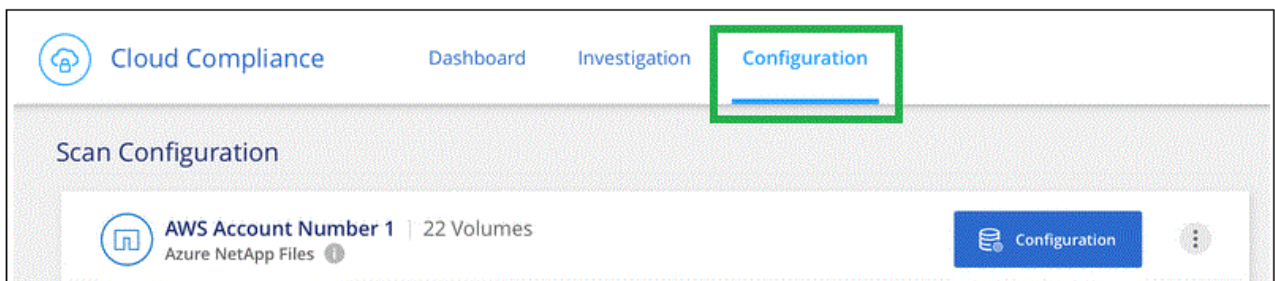
2. Assurez-vous que le groupe de sécurité pour Cloud Volumes ONTAP autorise le trafic entrant depuis l'instance Cloud Compliance.

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

3. Assurez-vous que les règles d'exportation de volume NFS incluent l'adresse IP de l'instance Cloud Compliance afin que les services IT puissent accéder aux données de chaque volume.
4. Si vous utilisez CIFS, fournissez Cloud Compliance avec des identifiants Active Directory pour qu'il puisse analyser les volumes CIFS.

a. En haut de Cloud Manager, cliquez sur **Cloud Compliance**.

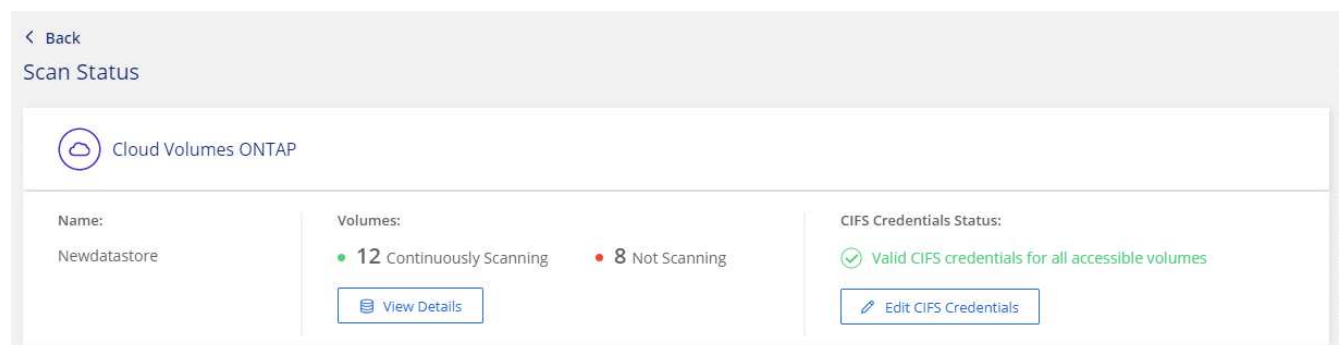
b. Cliquez sur l'onglet **Configuration**.



- c. Pour chaque environnement de travail, cliquez sur **Modifier les informations d'identification CIFS** et entrez le nom d'utilisateur et le mot de passe requis par Cloud Compliance pour accéder aux volumes CIFS sur le système.

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

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 *Scan 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 trois volumes dont l'un ne peut pas se numériser en raison de problèmes de connectivité réseau entre l'instance Cloud Compliance et le volume.

< Back

Newdatastore Scan Configuration

Activate Compliance for all Volumes ⓘ | 28/28 Volumes selected for compliance scan 🔍 [Edit CIFS Credentials](#)

Compliance ▾	Name ↑↓	Protocol ↑↓	Status ↑↓	Required Action ↑↓
<input checked="" type="checkbox"/>	10.160.7.6:yuval22	NFS	● Continuously Scanning	
<input checked="" type="checkbox"/>	10.160.7.6:yuvalnewtarget	NFS	● Continuously Scanning	
<input checked="" type="checkbox"/>	\\10.160.7.6\Danny_share	CIFS	● No Access	The CIFS credentials that you provided have expired. Edit the CIFS credential...

Activation et désactivation des analyses de conformité sur les volumes

Vous pouvez arrêter ou démarrer la numérisation de volumes dans un environnement de travail à tout moment à partir de la page Configuration de la numérisation. Nous vous recommandons de scanner tous les volumes.

< Back

Newdatastore Scan Configuration

Activate Compliance for all Volumes ⓘ | 27/28 Volumes selected for compliance scan 🔍 [+ Add CIFS Credentials](#)

Compliance ▾	Volume Name ↑↓	Status ▾	Required Action
<input type="checkbox"/>	VolumeName1	● Not Scanning	Add CIFS Credentials ⓘ
<input checked="" type="checkbox"/>	VolumeName2	● Continuously Scanning	
<input type="checkbox"/>	VolumeName3	● Not Scanning	
<input checked="" type="checkbox"/>	VolumeName4	● Continuously Scanning	
<input checked="" type="checkbox"/>	VolumeName5	● Continuously Scanning	

À :	Procédez comme suit :
Désactiver la recherche d'un volume	Déplacez le curseur de volume vers la gauche
Désactiver l'analyse de tous les volumes	Déplacez le curseur Activer la conformité pour tous les volumes vers la gauche
Activer la recherche d'un volume	Déplacez le curseur de volume vers la droite
Activer la recherche de tous les volumes	Déplacez le curseur Activer la conformité pour tous les volumes vers la droite



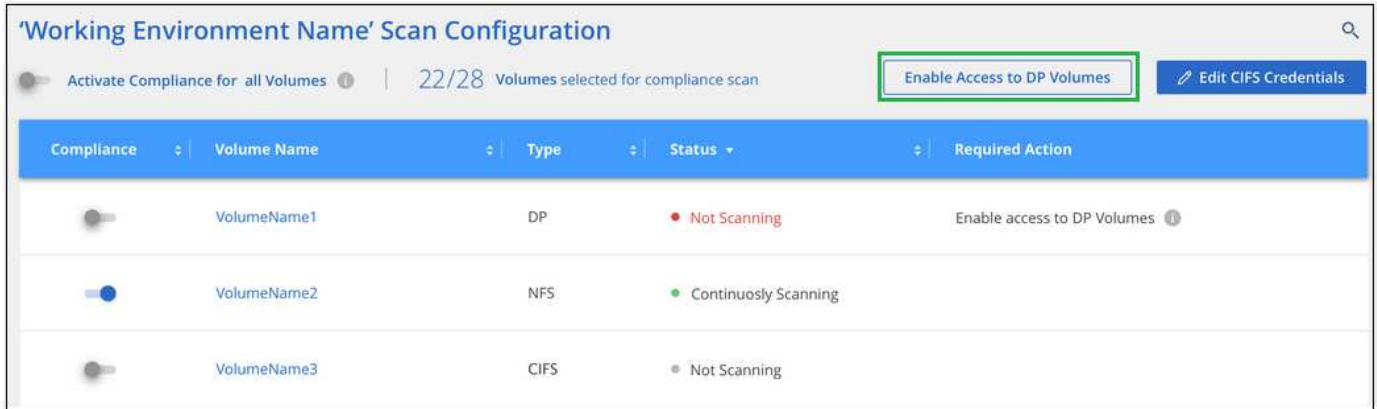
Les nouveaux volumes ajoutés à l'environnement de travail sont automatiquement analysés uniquement lorsque le paramètre **Activer la conformité pour tous les volumes** est activé. Lorsque ce paramètre est désactivé, vous devez activer la numérisation sur chaque nouveau volume créé dans l'environnement de travail.

Analyse des volumes de protection des données

Par défaut, les volumes de protection des données (DP) ne sont pas analysés parce qu'ils ne sont pas

exposés à des ressources externes et que Cloud Compliance ne peut pas y accéder. Ces volumes sont généralement les volumes de destination des opérations SnapMirror à partir d'un cluster ONTAP sur site.

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



Compliance	Volume Name	Type	Status	Required Action
<input type="checkbox"/>	VolumeName1	DP	Not Scanning	Enable access to DP Volumes
<input checked="" type="checkbox"/>	VolumeName2	NFS	Continuously Scanning	
<input type="checkbox"/>	VolumeName3	CIFS	Not Scanning	

Étapes

Pour analyser ces volumes de protection des données :

1. Cliquez sur le bouton **Activer l'accès aux volumes DP** en haut de la page.
2. Activez chaque volume DP que vous souhaitez analyser ou utilisez le contrôle **Activer la conformité pour tous les volumes** pour activer tous les volumes, y compris tous les volumes DP.

Une fois activé, Cloud Compliance crée un partage NFS à partir de chaque volume DP activé pour la conformité, afin de pouvoir l'analyser. Les règles d'exportation de partage n'autorisent l'accès qu'à partir de l'instance Cloud Compliance.



Seuls les volumes initialement créés en tant que volumes NFS dans le système ONTAP source sont affichés dans la liste des volumes. Les volumes source qui ont été créés initialement en tant que CIFS n'apparaissent pas actuellement dans Cloud Compliance.

Mise en route de Cloud Compliance pour Amazon S3

Cloud Compliance peut analyser vos compartiments Amazon S3 pour identifier les données personnelles et sensibles qui résident dans le stockage objet S3. Cloud Compliance peut analyser n'importe quel compartiment du compte, quel que soit son origine 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 de Cloud Compliance, y compris la préparation d'un rôle IAM et la configuration de la connectivité Cloud Compliance vers S3. [Voir la liste complète.](#)



Déployez l'instance Cloud Compliance

"Déployez Cloud Compliance dans Cloud Manager" si aucune instance n'est déjà déployée.



Activez la conformité sur votre environnement de travail S3

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



Sélectionnez les compartiments à numériser

Sélectionnez les compartiments que vous souhaitez analyser et Cloud Compliance 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 Compliance

Cloud Compliance doit disposer 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. Cloud Manager vous invite à sélectionner un rôle IAM lorsque vous activez Cloud Compliance dans l'environnement de travail Amazon S3.

```

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

```

Connectivité entre Cloud Compliance et Amazon S3

Cloud Compliance 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 Compliance. 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, Cloud Compliance 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 Compliance

["Déployez Cloud Compliance dans Cloud Manager"](#) si aucune instance n'est déjà déployée.

Vous devez déployer l'instance dans un connecteur AWS, pour que Cloud Manager détecte automatiquement les compartiments S3 dans ce compte AWS et les affiche dans un environnement de travail Amazon S3.

Activation de la conformité sur votre environnement de travail S3

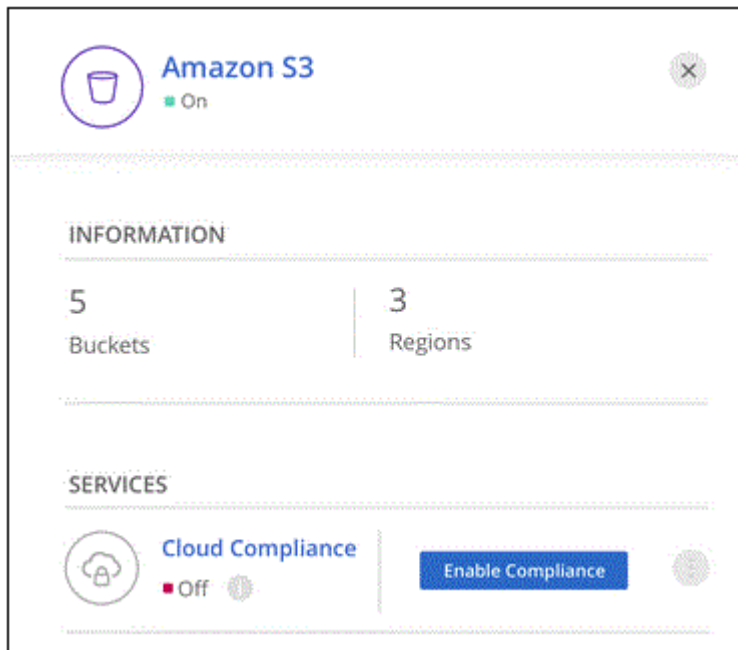
Activez Cloud Compliance sur Amazon S3 après avoir vérifié les prérequis.

Étapes

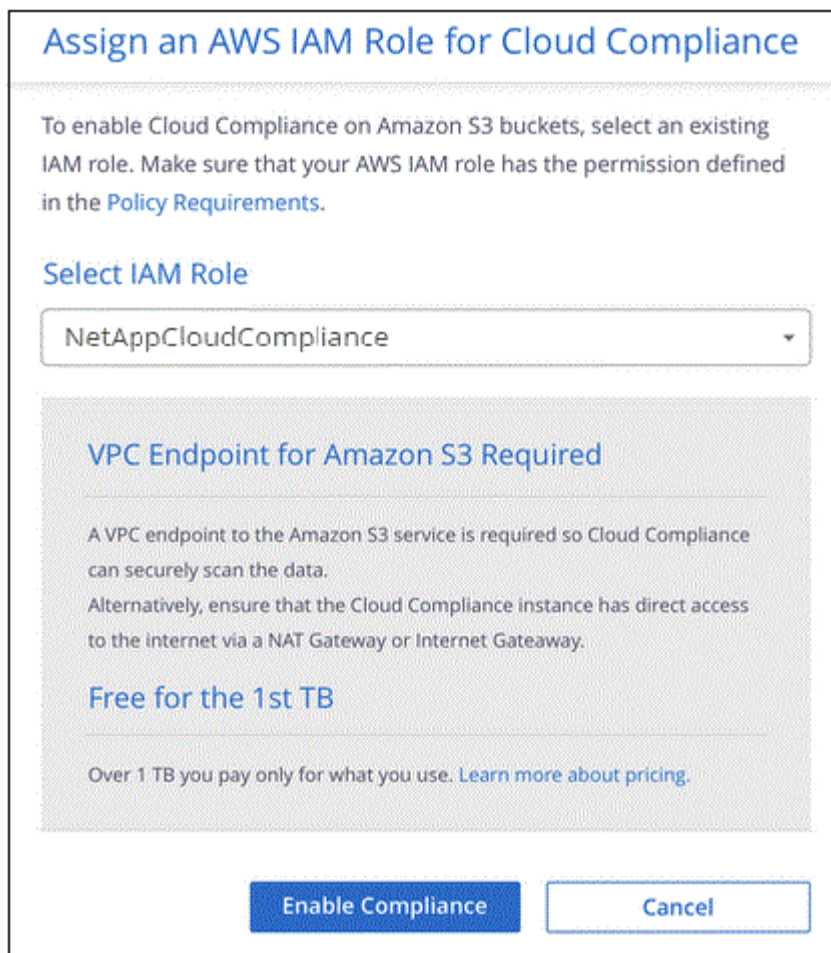
1. En haut de Cloud Manager, cliquez sur **environnements de travail**.
2. Sélectionnez l'environnement de travail Amazon S3.



3. Dans le volet de droite, cliquez sur **Activer la conformité**.




4. Lorsque vous y êtes invité, attribuez un rôle IAM à l'instance Cloud Compliance qui possède [les autorisations requises](#).



5. Cliquez sur **Activer la conformité**.



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

Résultat

Cloud Manager attribue le rôle IAM à l'instance.

Activation et désactivation des analyses de conformité dans les compartiments S3

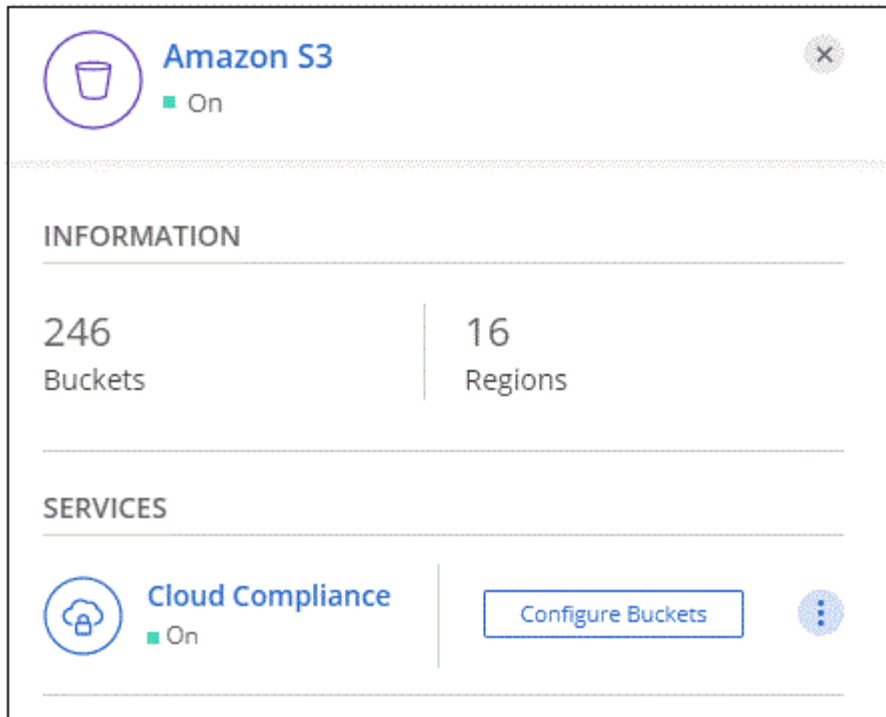
Une fois que Cloud Manager active Cloud Compliance sur Amazon S3, l'étape suivante consiste à configurer les compartiments à analyser.

Lorsque Cloud Manager s'exécute sur le compte AWS possédant les compartiments S3 que vous souhaitez analyser, il détecte ces compartiments et les affiche dans un environnement de travail Amazon S3.

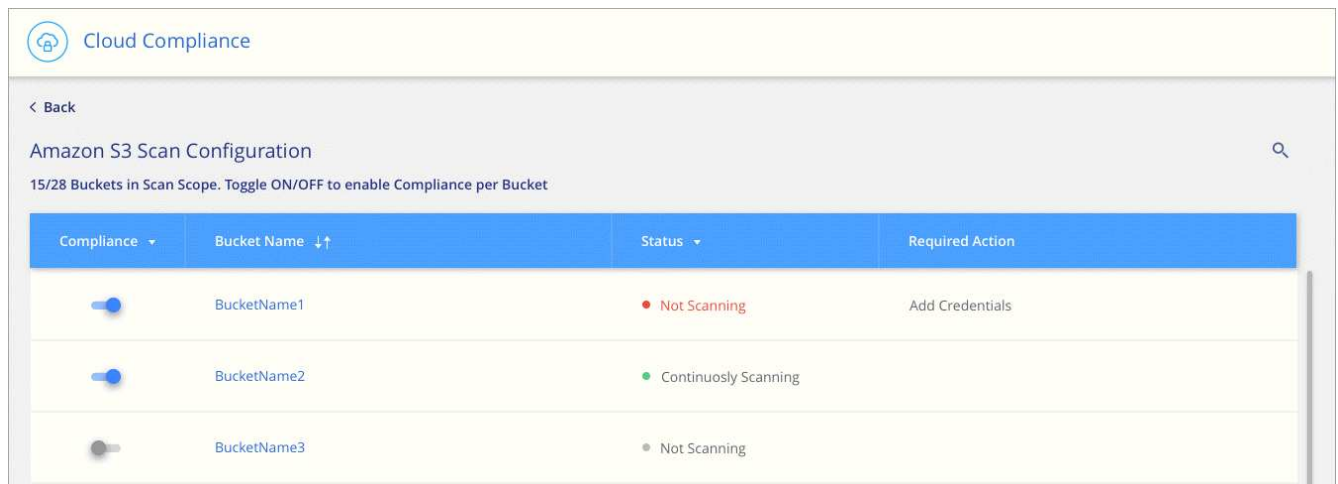
Cloud Compliance l'est également [Analysez les compartiments S3 qui se trouvent dans différents comptes AWS](#).

Étapes

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



3. Activez la conformité sur les compartiments à numériser.



Résultat

Cloud Compliance commence l'analyse des compartiments S3 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 analyser les compartiments S3 qui se trouvent dans un autre compte AWS, vous pouvez attribuer un rôle à partir de ce compte pour accéder à l'instance Cloud Compliance 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 Compliance.
- Modifiez la durée * maximale de la session CLI/API* de 1 heure à 12 heures et enregistrez cette modification.
- Joignez la politique IAM de conformité aux solutions cloud. Assurez-vous qu'il dispose des autorisations requises.

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

2. Accédez au compte AWS source où réside l'instance Cloud Compliance 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 l'ARN du rôle que vous avez créé dans le compte cible.

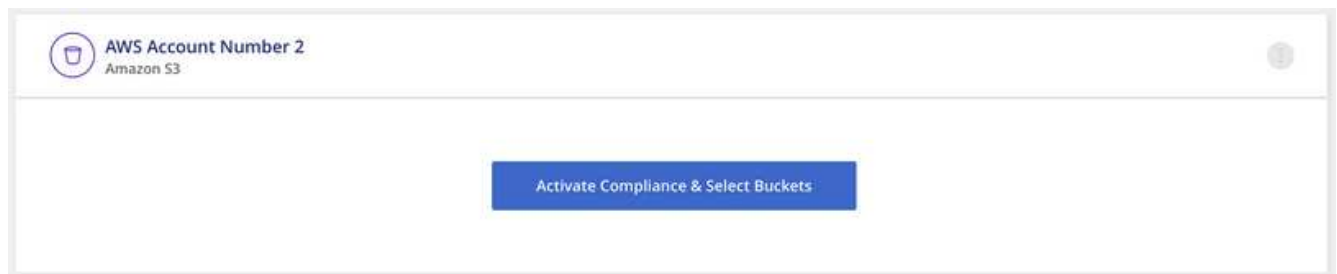

```

{
  "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 de profil d'instance Cloud Compliance a désormais accès au compte AWS supplémentaire.

3. Accédez à la page **Amazon S3 Scan Configuration** et le nouveau compte AWS s'affiche. Notez que Cloud Compliance peut mettre quelques minutes à synchroniser l'environnement de travail du nouveau compte et afficher ces informations.



4. Cliquez sur **Activer la conformité et sélectionnez les rubriques** et sélectionnez les rubriques que vous souhaitez numériser.

Résultat

Cloud Compliance commence l'analyse des nouveaux compartiments S3 activés.

Analyse des schémas de base de données

Suivez quelques étapes pour commencer à analyser vos schémas de base de données

avec Cloud Compliance.

Démarrage rapide

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



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.



Déployez l'instance Cloud Compliance

"[Déployez Cloud Compliance dans Cloud Manager](#)" si aucune instance n'est déjà déployée.



Ajoutez le serveur de base de données

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



Sélectionnez les schémas

Sélectionnez les schémas à numériser.

Vérification des prérequis

Avant d'activer Cloud Compliance, lisez les conditions préalables suivantes pour vous assurer que la configuration est prise en charge.

Bases de données prises en charge

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

- MongoDB
- 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 connecté à l'instance Cloud Compliance 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 Compliance avec toutes les autorisations requises.

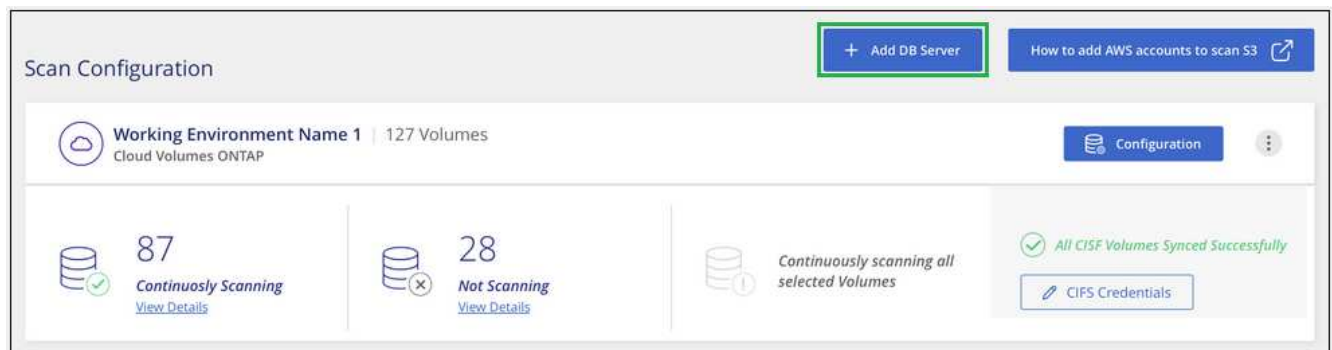
Remarque : pour MongoDB, un rôle d'administrateur en lecture seule est requis.

Ajout du serveur de base de données

Vous devez avoir "[Déploiement d'une instance de Cloud Compliance dans Cloud Manager](#)".

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

1. Dans la page *Scan Configuration*, cliquez sur le bouton **Add DB Server**.



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 pour que Cloud Compliance 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

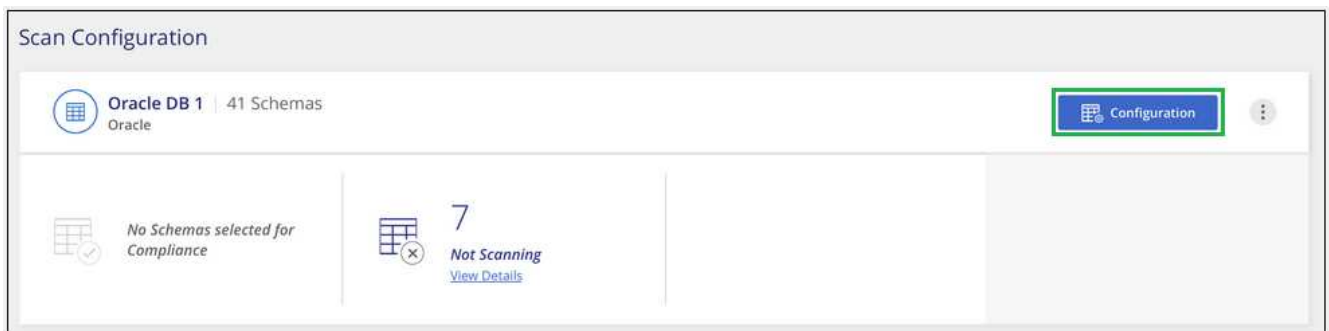
Password

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

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

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

1. Dans la page *Scan 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' Scan Configuration			
Compliance	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 Compliance 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.

Suppression d'une base de données de Cloud Manager

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

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



Une analyse des données ONTAP sur site avec Cloud Compliance à l'aide de SnapMirror

Vous pouvez analyser les données ONTAP sur site avec Cloud Compliance en répliquant les données NFS ou CIFS sur site vers un environnement de travail Cloud Volumes ONTAP, puis en assurant la conformité. Il n'est pas possible de numériser les données directement à partir d'un environnement de travail ONTAP sur site.

Vous devez avoir "[Déploiement d'une instance de Cloud Compliance dans Cloud Manager](#)".

Étapes

1. Depuis Cloud Manager, créez une relation SnapMirror entre le cluster ONTAP sur site et Cloud Volumes ONTAP.
 - a. "[Découvrez le cluster sur site dans Cloud Manager](#)".
 - b. "[Créez une réplication SnapMirror entre le cluster ONTAP sur site et Cloud Volumes ONTAP depuis](#)

Cloud Manager".

2. Pour les volumes DP créés à partir de volumes SMB source, depuis l'interface de ligne de commande ONTAP, configurez les volumes de destination SMB pour l'accès aux données. (Cette opération n'est pas requise pour les volumes NFS, car l'accès aux données est activé automatiquement via Cloud Compliance.)
 - a. ["Créer un partage SMB sur le volume de destination"](#).
 - b. ["Appliquez les ACL appropriées sur le partage SMB au volume de destination"](#).
3. Depuis Cloud Manager, activez Cloud Compliance dans l'environnement de travail Cloud Volumes ONTAP qui contient les données SnapMirror :
 - a. Cliquez sur **environnements de travail**.
 - b. Sélectionnez l'environnement de travail qui contient les données SnapMirror et cliquez sur **Activer la conformité**.

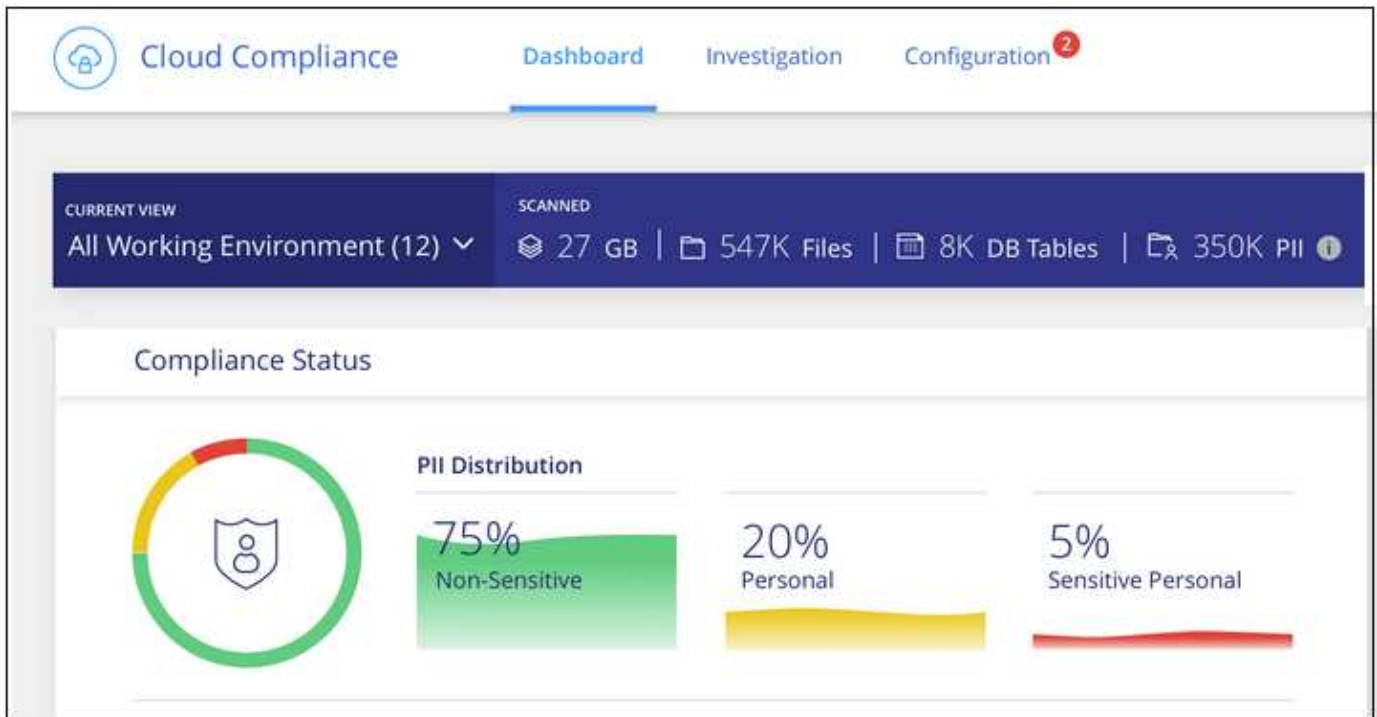
["Cliquez ici pour obtenir de l'aide sur l'activation de Cloud Compliance sur un système Cloud Volumes ONTAP"](#).
 - c. Cliquez sur le bouton **Activer l'accès aux volumes DP** en haut de la page *Scan Configuration*.
 - d. Activez chaque volume DP que vous souhaitez analyser ou utilisez le contrôle **Activer la conformité pour tous les volumes** pour activer tous les volumes, y compris tous les volumes DP.

Voir ["Analyse des volumes de protection des données"](#) Pour plus d'informations sur l'analyse des volumes DP.

La visibilité et le contrôle des données privées

Prenez le contrôle de vos données privées en affichant les détails sur les données personnelles et les données personnelles sensibles de votre organisation. Vous pouvez également consulter les catégories et les types de fichiers que Cloud Compliance trouve dans vos données.

Par défaut, le tableau de bord Cloud Compliance affiche les données de conformité pour tous les environnements en travail et toutes les bases de données.



Si vous ne souhaitez voir des données que pour certains environnements de travail, [sélectionnez ces environnements de travail](#).

Données personnelles

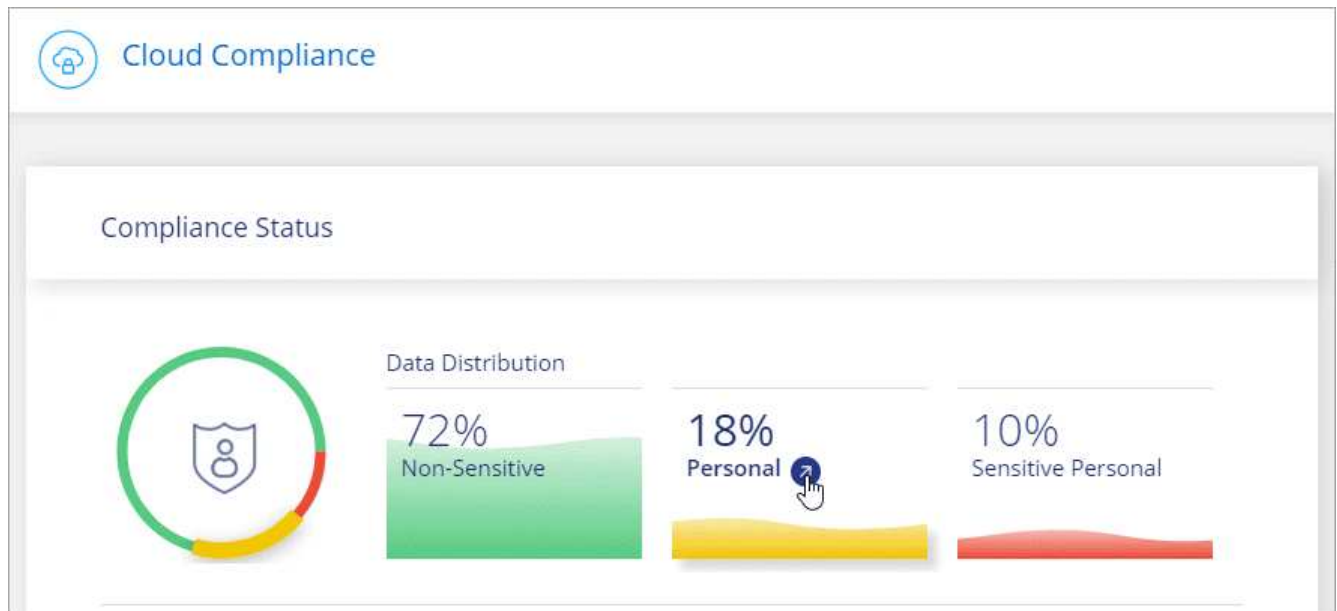
Cloud Compliance identifie automatiquement des mots, des chaînes et des motifs spécifiques (Regex) dans les données. Par exemple, les renseignements d'identification personnelle (RP), les numéros de carte de crédit, les numéros de sécurité sociale, les numéros de compte bancaire, etc. [Voir la liste complète](#).

Pour certains types de données personnelles, Cloud Compliance utilise *proximité validation* pour valider ses résultats. La validation se produit en recherchant un ou plusieurs mots clés prédéfinis à proximité des données personnelles trouvées. Par exemple, Cloud Compliance identifie un secteur public américain Numéro de sécurité sociale (SSN) comme numéro de sécurité sociale s'il y a un mot de proximité, par exemple, *SSN* ou *social Security*. [La liste ci-dessous](#) Indique quand Cloud Compliance utilise la validation de proximité.

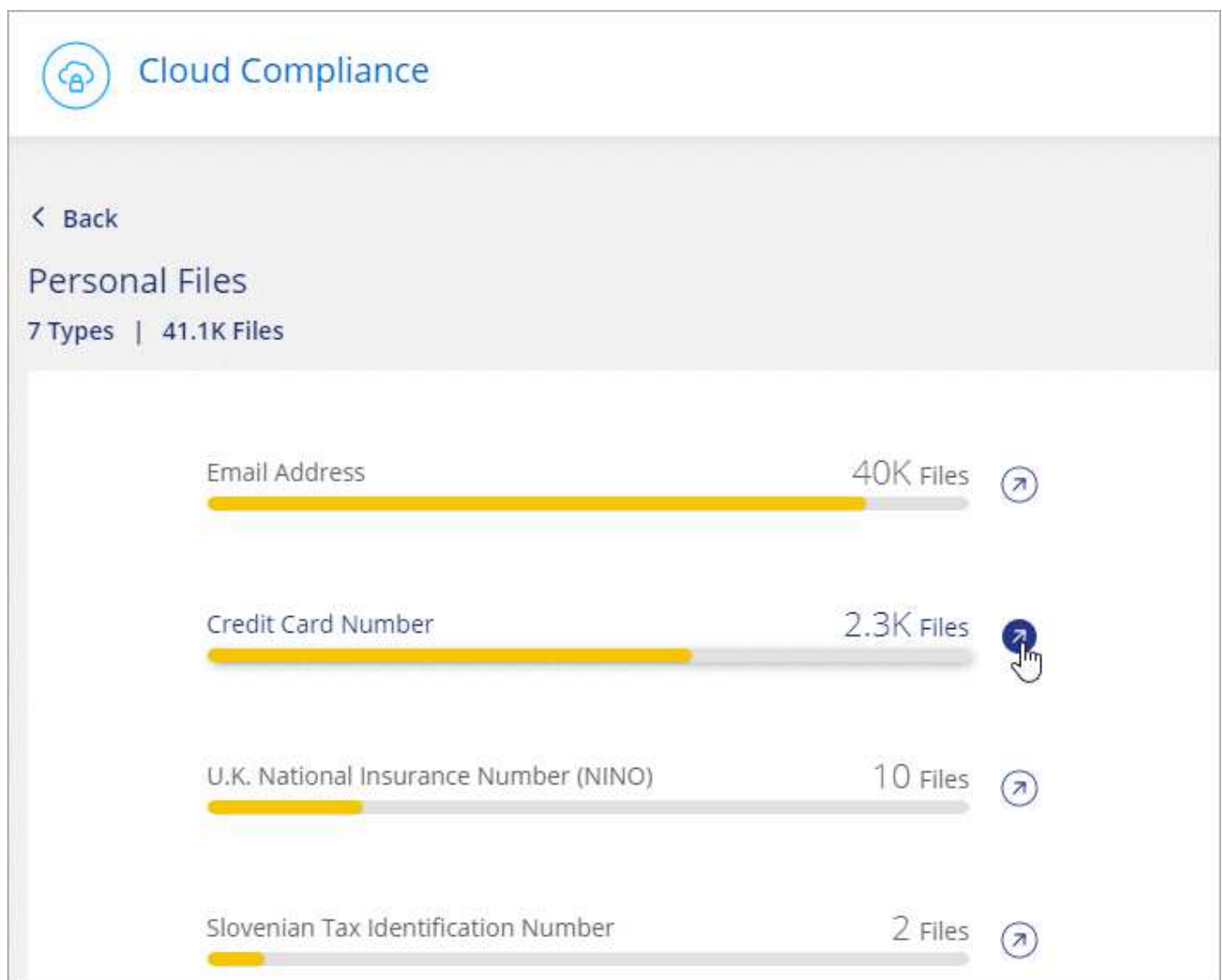
Affichage des fichiers contenant des données personnelles

Étapes

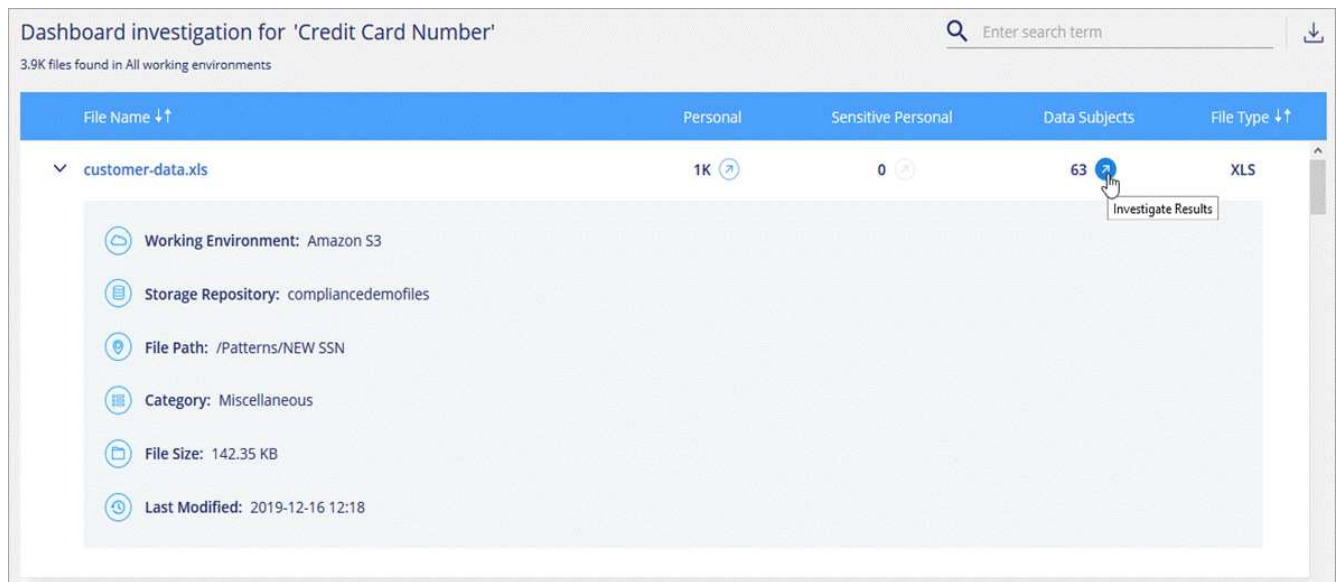
1. En haut de Cloud Manager, cliquez sur **Cloud Compliance** et cliquez sur l'onglet **Dashboard**.
2. Pour examiner les détails de toutes les données personnelles, cliquez sur l'icône en regard du pourcentage de données personnelles.



3. Pour examiner les détails d'un type spécifique de données personnelles, cliquez sur **Afficher tout**, puis cliquez sur l'icône **étudier les résultats** pour un type spécifique de données personnelles.

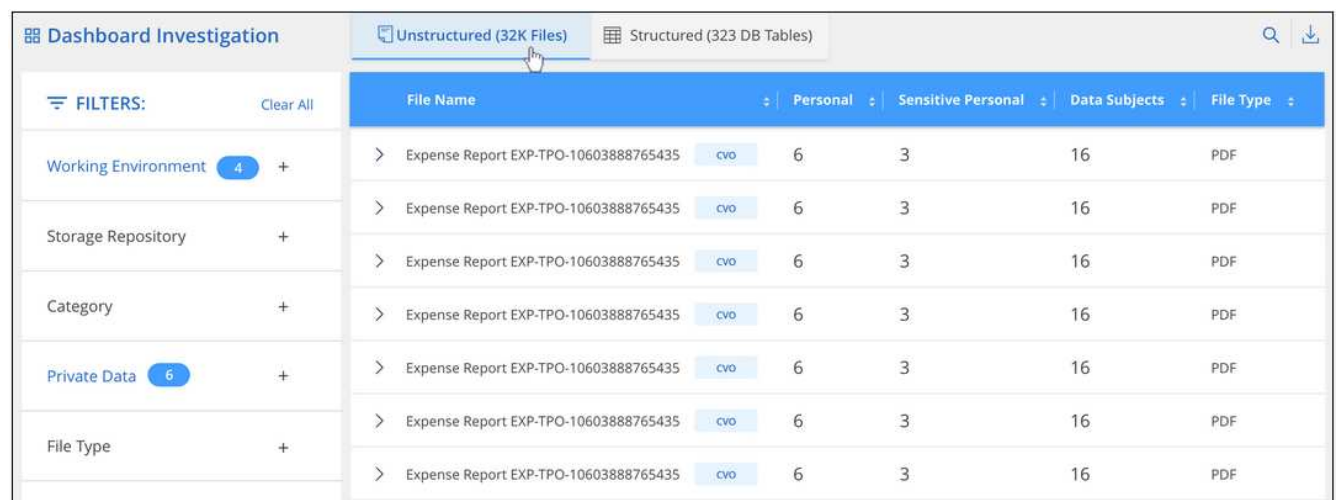


- Examinez les données en recherchant, en triant, en développant les détails d'un fichier spécifique, en cliquant sur **Informez Results** pour afficher les informations masquées ou en téléchargeant la liste de fichiers.



- Vous pouvez également filtrer le contenu de la page d'enquête pour n'afficher que les résultats que vous souhaitez voir. Les onglets de niveau supérieur permettent d'afficher des données à partir de fichiers (données non structurées) ou de bases de données (données structurées).

Vous disposez ensuite de filtres pour l'environnement de travail, le référentiel de stockage, la catégorie, les données privées, le type de fichier, Dernière modification date, et si les autorisations d'accès de l'objet S3 sont ouvertes pour l'accès public.



Types de données personnelles

Les données personnelles contenues dans les dossiers peuvent être des données personnelles générales ou des identifiants nationaux. La troisième colonne indique si Cloud Compliance utilise ou non [validation de proximité](#) pour valider ses résultats pour l'identificateur.

Type	Identificateur	Validation de proximité ?
Généralités	Adresse électronique	Non
	Numéro de carte de crédit	Non
	Numéro IBAN (Numéro de compte bancaire international)	Non

Type	Identificateur	Validation de proximité ?
Identifiants nationaux	Carte d'identité belge (Numero National)	Oui.
	ID brésilien (CPF)	Oui.
	ID bulgare (UCN)	Oui.
	Permis de conduire californien	Oui.
	ID croate (OIB)	Oui.
	Chypre Numéro d'identification fiscale (TIC)	Oui.
	Tchèque/slovaque ID	Oui.
	ID danois (RCP)	Oui.
	ID néerlandais (BSN)	Oui.
	ID estonien	Oui.
	ID finlandais (HETU)	Oui.
	Numéro d'identification fiscale (SPI)	Oui.
	Numéro d'identification fiscale allemand (identifiant Steierliche)	Oui.
	Pièce d'identité grecque	Oui.
	Numéro d'identification fiscale hongrois	Oui.
	Irish ID (PPS)	Oui.
	ID israélien	Oui.
	Numéro d'identification fiscal italien	Oui.
	Carte d'identité lettone	Oui.
	Carte d'identité lituanienne	Oui.
	Luxembourg ID	Oui.
	Identifiant maltais	Oui.
	ID polonais (PESEL)	Oui.
	Numéro d'identification fiscale portugais (FNI)	Oui.
	ID roumain (CNP)	Oui.
	ID slovène (EMSO)	Oui.
	Carte d'identité sud-africaine	Oui.
	Numéro d'identification fiscale espagnol	Oui.
	Carte d'identité suédoise	Oui.
	ROYAUME-UNI ID (NINO)	Oui.
Numéro de sécurité sociale des États-Unis (SSN)	Oui.	

Données personnelles sensibles

Cloud Compliance identifie automatiquement les types particuliers de données sensibles, conformément aux réglementations en matière de confidentialité, notamment "[Les articles 9 et 10 du RGPD](#)". Par exemple, des renseignements concernant la santé d'une personne, son origine ethnique ou son orientation sexuelle. [Voir la liste complète](#).

Cloud Compliance exploite l'intelligence artificielle (IA), le traitement du langage naturel (NLP), le machine learning (ML) et l'informatique cognitive (CC) pour comprendre la signification du contenu balayé afin d'extraire les entités et de les catégoriser en conséquence.

Par exemple, une catégorie de données sensibles du RGPD est l'origine ethnique. Du fait de ses capacités NLP, Cloud Compliance a la différence entre une phrase qui lit « George est mexicain » (en indiquant des données sensibles comme indiqué à l'article 9 du RGPD), et « George mange de la nourriture mexicaine ».

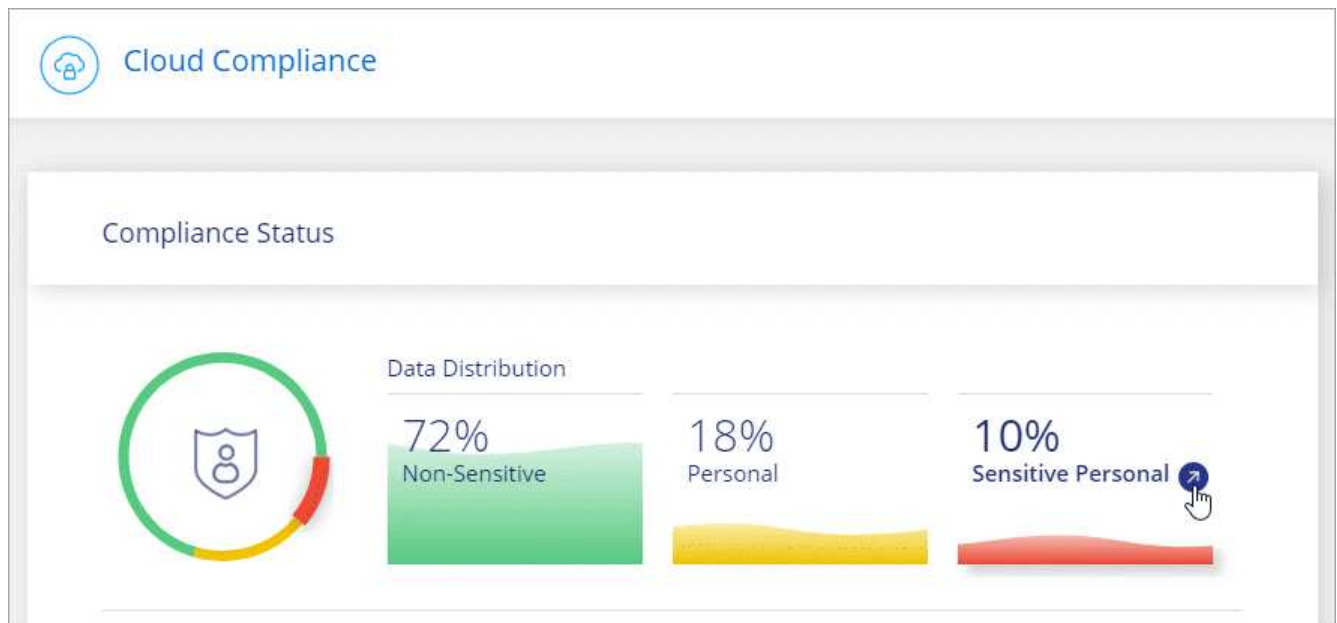


Seul l'anglais est pris en charge lors de la recherche de données personnelles sensibles. La prise en charge d'autres langues sera ajoutée ultérieurement.

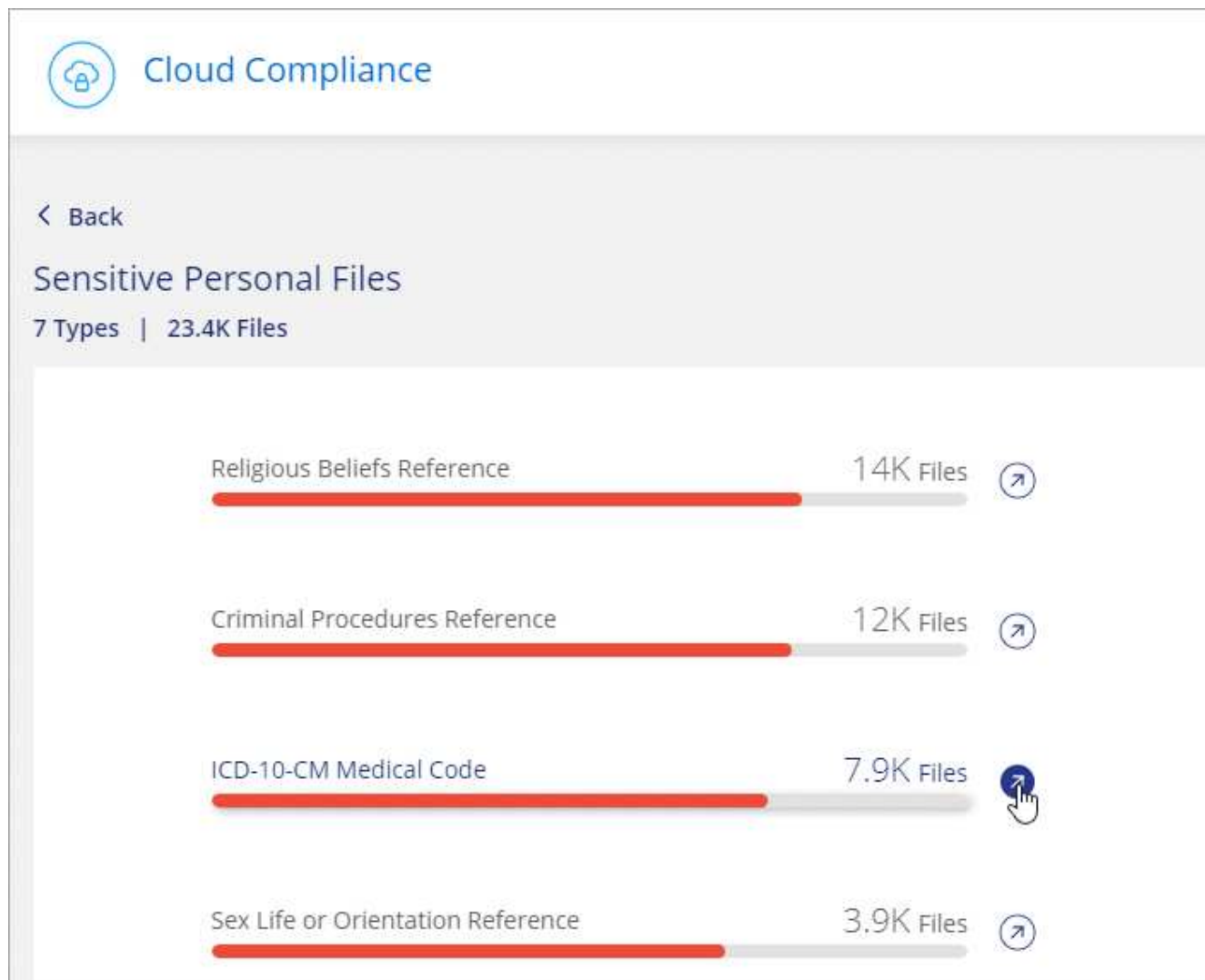
Affichage des fichiers contenant des données personnelles sensibles

Étapes

1. En haut de Cloud Manager, cliquez sur **Cloud Compliance**.
2. Pour examiner les détails de toutes les données personnelles sensibles, cliquez sur l'icône en regard du pourcentage de données personnelles sensibles.



3. Pour examiner les détails d'un type spécifique de données personnelles sensibles, cliquez sur **Afficher tout**, puis cliquez sur l'icône **enquêter sur les résultats** pour un type spécifique de données personnelles sensibles.



- Examinez les données en recherchant, en triant, en développant les détails d'un fichier spécifique, en cliquant sur **Informez Results** pour afficher les informations masquées ou en téléchargeant la liste de fichiers.

Types de données personnelles sensibles

Les données personnelles sensibles que Cloud Compliance peut trouver dans les fichiers sont les suivantes :

Référence des procédures pénales

Données concernant les condamnations pénales et les infractions d'une personne physique.

Référence ethnique

Données concernant l'origine raciale ou ethnique d'une personne physique.

Référence santé

Données concernant la santé d'une personne physique.

Codes médicaux ICD-9-cm

Codes utilisés dans l'industrie médicale et de la santé.

Codes médicaux ICD-10-cm

Codes utilisés dans l'industrie médicale et de la santé.

Références philosophiques

Données concernant les croyances philosophiques d'une personne naturelle.

Croyances religieuses

Données concernant les croyances religieuses d'une personne naturelle.

Référence de la vie sexuelle ou de l'orientation

Données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Catégories

Cloud Compliance divise les données analysées et les divise en plusieurs types de catégories. Les catégories sont des rubriques basées sur l'analyse par IA du contenu et des métadonnées de chaque fichier. [Voir la liste des catégories.](#)

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

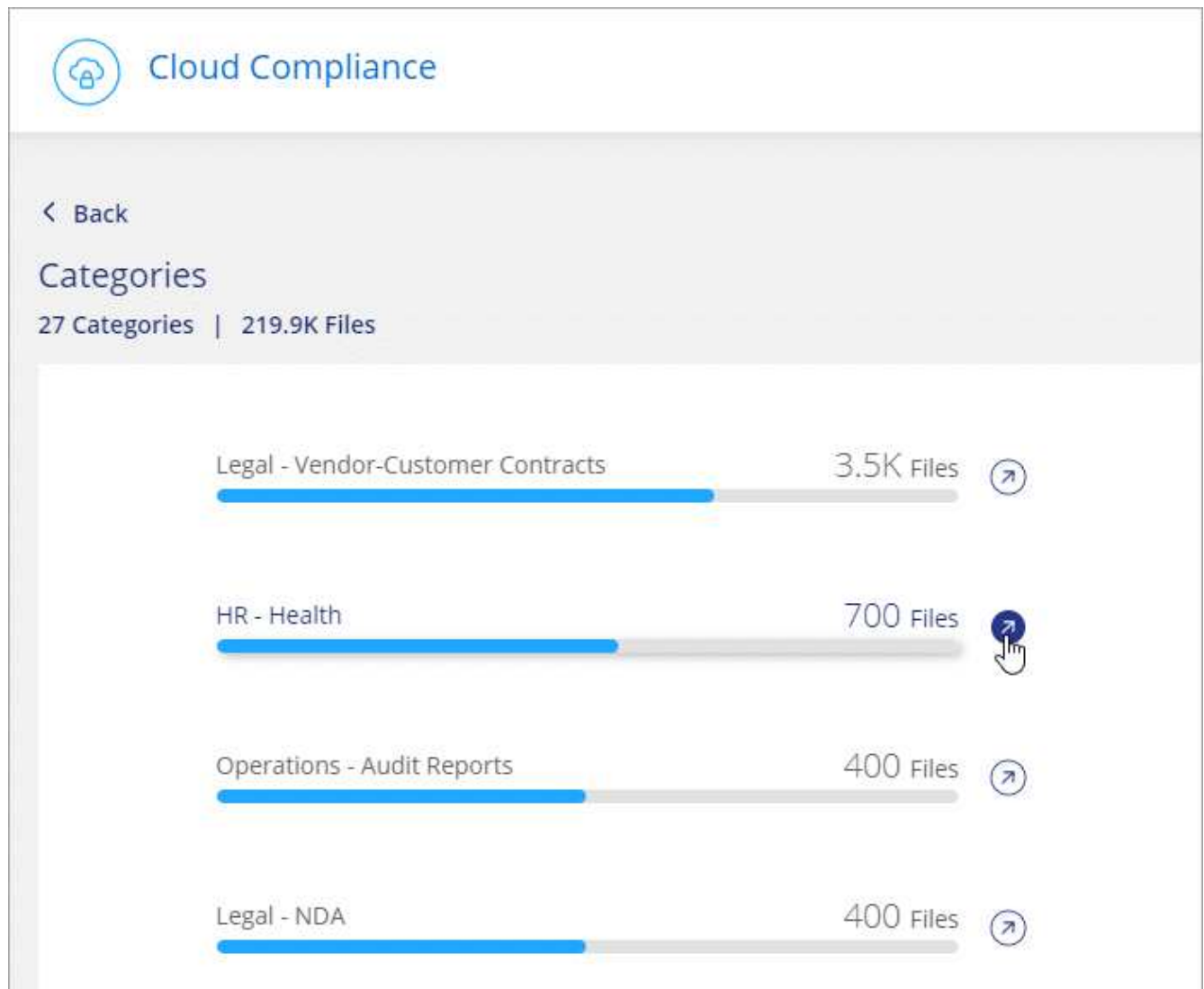


Seul l'anglais est pris en charge pour les catégories. La prise en charge d'autres langues sera ajoutée ultérieurement.

Affichage des fichiers par catégories

Étapes

1. En haut de Cloud Manager, cliquez sur **Cloud Compliance**.
2. Cliquez sur l'icône **Inquiétude Results** pour l'une des 4 catégories les plus importantes directement à partir de l'écran principal, ou cliquez sur **Afficher tout**, puis cliquez sur l'icône de l'une des catégories.



3. Examinez les données en recherchant, en triant, en développant les détails d'un fichier spécifique, en cliquant sur **Informez Results** pour afficher les informations masquées ou en téléchargeant la liste de fichiers.

Types de catégories

NetApp Cloud Compliance classe vos données comme suit :

Finances

- Bilans
- Bons de commande
- Factures
- Rapports trimestriels

RH

- Vérifications des antécédents
- Plans de rémunération
- Contrats employés

- Évaluations des employés
- Santé
- Reprend

Légal

- NDAS
- Contrats fournisseur-client

Marketing

- Campagnes
- Conférences

Exploitation

- Rapports d'audit

Ventes

- Commandes

Administratifs

- RFI
- RFP
- CAHIER DES CHARGES
- Formation

Assistance

- Plaintes et tickets

Catégories de métadonnées

- Données applicatives
- Archiver les fichiers
- Audio
- Données d'applications d'entreprise
- Fichiers CAO
- Code
- Base de données et fichiers d'index
- Fichiers de conception
- Données d'application de messagerie
- Exécutables
- Données d'applications financières
- Données d'application de santé
- Images
- Journaux
- Documents divers

- Présentations diverses
- Feuilles de calcul diverses
- Vidéos

Types de fichiers

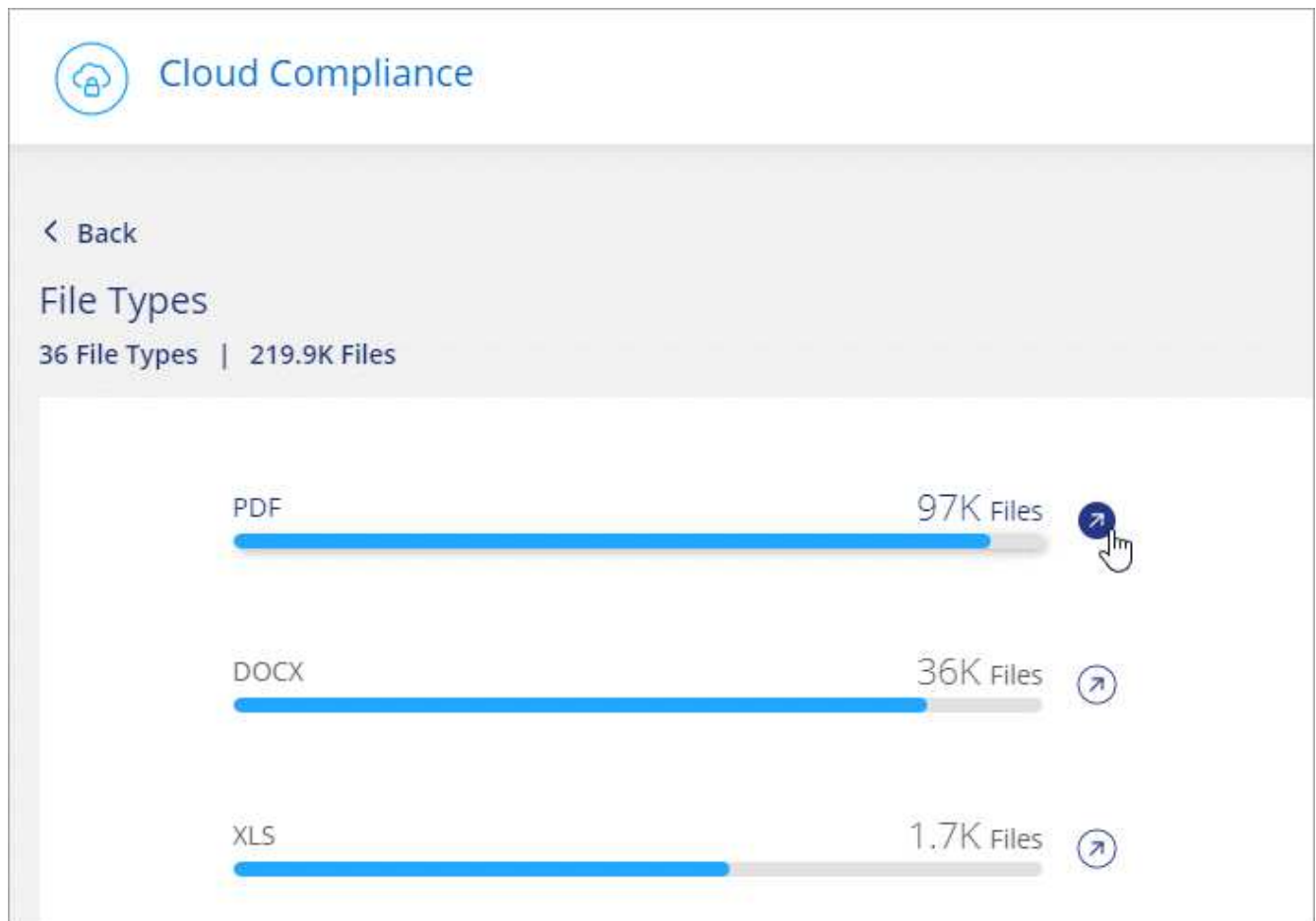
Cloud Compliance réduit les données analysées et les divise par type de fichier. La vérification de vos types de fichiers peut vous aider à contrôler vos données sensibles car il se peut que certains types de fichiers ne soient pas stockés correctement. [Voir la liste des types de fichiers.](#)

Par exemple, vous pouvez stocker des fichiers CAO qui contiennent des informations très sensibles sur votre organisation. S'ils ne sont pas sécurisés, vous pouvez prendre le contrôle des données sensibles en limitant les autorisations ou en déplaçant les fichiers vers un autre emplacement.

Affichage des types de fichiers

Étapes

1. En haut de Cloud Manager, cliquez sur **Cloud Compliance**.
2. Cliquez sur l'icône **étudier les résultats** pour l'un des 4 types de fichiers les plus importants directement à partir de l'écran principal ou cliquez sur **Afficher tout**, puis cliquez sur l'icône correspondant à l'un des types de fichiers.



3. Examinez les données en recherchant, en triant, en développant les détails d'un fichier spécifique, en cliquant sur **Informez Results** pour afficher les informations masquées ou en téléchargeant la liste de

fichiers.

Types de fichiers

Cloud Compliance analyse les informations relatives aux catégories et aux métadonnées de tous les fichiers, et affiche tous les types de fichiers dans la section types de fichiers du tableau de bord.

Mais lorsque Cloud Compliance détecte des informations à caractère personnel (PII) ou lorsqu'il effectue une recherche DSAR, seuls les formats de fichier suivants sont pris en charge : .PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF ET .JSON.

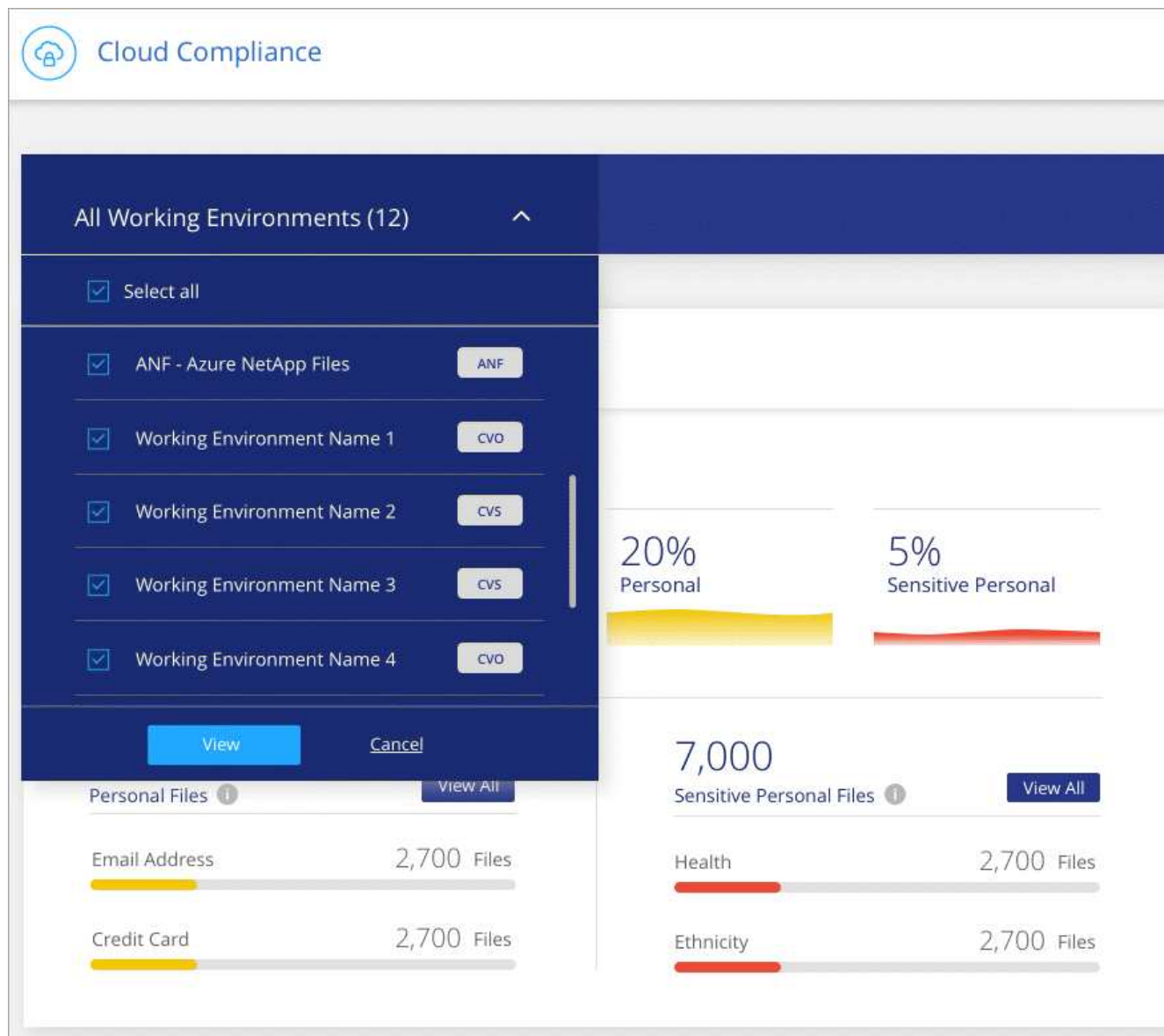
Affichage des données d'environnements de travail spécifiques

Vous pouvez filtrer le contenu du tableau de bord Cloud Compliance pour consulter les données de conformité pour tous les environnements de travail et bases de données, ou pour des environnements de travail spécifiques uniquement.

Lorsque vous filtrez le tableau de bord, Cloud Compliance évalue les données de conformité et les rapports aux environnements de travail que vous avez sélectionnés.

Étapes

1. Cliquez sur la liste déroulante du filtre, sélectionnez les environnements de travail pour lesquels vous souhaitez afficher les données, puis cliquez sur **Afficher**.



Exactitude des informations trouvées

NetApp ne peut garantir une précision de 100 % des données personnelles et des données personnelles sensibles que Cloud Compliance identifie. Vous devez toujours valider les informations en examinant les données.

Le tableau ci-dessous indique l'exactitude des informations fournies par Cloud Compliance à partir des résultats de nos tests. Nous la décomposent par *Precision* et *rappel*:

Précision

La probabilité que Cloud Compliance trouve a été identifiée correctement. Par exemple, un taux de précision de 90 % pour les données personnelles signifie que 9 fichiers sur 10 identifiés comme contenant des renseignements personnels, contiennent en fait des renseignements personnels. 1 fichier sur 10 serait un faux positif.

Rappel

La probabilité que Cloud Compliance trouve ce qu'il faut. Par exemple, un taux de rappel de 70 % pour les données personnelles signifie que Cloud Compliance peut identifier 7 fichiers sur 10 qui contiennent

réellement des données personnelles dans votre entreprise. Cloud Compliance manquerait 30 % des données et n'apparaîtra pas dans le tableau de bord.

Cloud Compliance est une version sous contrôle de disponibilité. Nous améliorons en permanence la précision de nos résultats. Ces améliorations seront automatiquement disponibles dans les prochaines versions de Cloud Compliance.

Type	Précision	Rappel
Données personnelles - général	90 à 95 %	60 à 80 %
Données personnelles - identificateurs de pays	30 à 60 %	40 à 60 %
Données personnelles sensibles	80 à 95 %	20 à 30 %
Catégories	90 à 97 %	60 à 80 %

Ce qui est inclus dans chaque rapport de liste de fichiers (fichier CSV)

À partir de chaque page Investigation, vous pouvez télécharger des listes de fichiers (au format CSV) qui incluent des détails sur les fichiers identifiés. S'il y a plus de 10,000 résultats, seuls les 10,000 meilleurs apparaissent dans la liste.

Chaque liste de fichiers comprend les informations suivantes :

- Nom du fichier
- Type d'emplacement
- Environnement de travail
- Référentiel de stockage
- Protocole
- Chemin des fichiers
- Type de fichier
- Catégorie
- Informations personnelles
- Informations personnelles sensibles
- Date de détection de suppression

Une date de détection de suppression identifie la date à laquelle le fichier a été supprimé ou déplacé. Cela vous permet d'identifier le moment où des fichiers sensibles ont été déplacés. Les fichiers supprimés ne font pas partie du nombre de fichiers qui s'affiche dans le tableau de bord ou sur la page Investigation. Les fichiers n'apparaissent que dans les rapports CSV.

Affichage des rapports de conformité

Cloud Compliance fournit des rapports qui vous aideront à mieux comprendre l'état du programme de confidentialité des données de votre entreprise.

Par défaut, le tableau de bord Cloud Compliance affiche les données de conformité pour tous les environnements en travail et toutes les bases de données. Si vous souhaitez afficher des rapports contenant

des données pour certains environnements de travail uniquement, [sélectionnez ces environnements de travail](#).



NetApp ne peut garantir une précision de 100 % des données personnelles et des données personnelles sensibles que Cloud Compliance identifie. Vous devez toujours valider les informations en examinant les données.

Rapport d'évaluation des risques pour la confidentialité

Le rapport d'évaluation des risques pour la protection de la vie privée fournit une vue d'ensemble de l'état des risques pour la confidentialité de votre organisation, conformément aux réglementations en matière de confidentialité, telles que le Règlement sur la protection de la vie privée et l'ACFPC. Le rapport contient les informations suivantes :

Statut de conformité

A [indice de gravité](#) et la distribution des données, qu'elles soient non sensibles, personnelles ou sensibles.

Présentation de l'évaluation

Une ventilation des types de données personnelles ainsi que des catégories de données.

Sujets de données dans cette évaluation

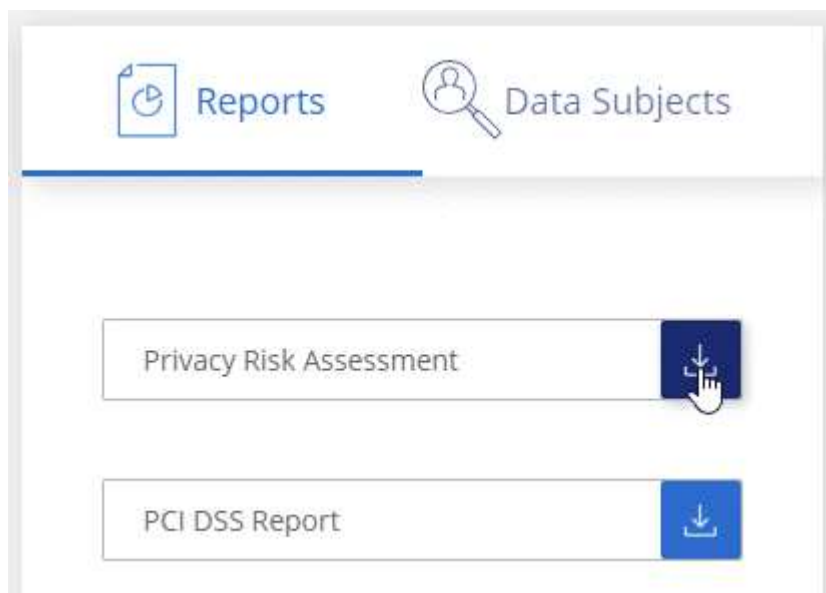
Nombre de personnes, par lieu, pour lesquelles des identificateurs nationaux ont été trouvés.

Génération du rapport d'évaluation des risques pour la confidentialité

Accédez à l'onglet conformité pour générer le rapport.

Étapes

1. En haut de Cloud Manager, cliquez sur **Cloud Compliance**.
2. Sous **Rapports**, cliquez sur l'icône de téléchargement en regard de **évaluation des risques pour la vie privée**.



Résultat

Cloud Compliance génère un rapport PDF que vous pouvez consulter et envoyer à d'autres groupes si nécessaire.

Indice de gravité

Cloud Compliance calcule le score de gravité pour le rapport d'évaluation des risques liés à la confidentialité, sur la base de trois variables :

- Pourcentage de données personnelles sur toutes les données.
- Le pourcentage de données personnelles sensibles hors de toutes les données.
- Le pourcentage de fichiers qui incluent des sujets de données, déterminé par des identificateurs nationaux tels que les ID nationaux, les numéros de sécurité sociale et les numéros d'identification fiscale.

La logique utilisée pour déterminer le score est la suivante :

Indice de gravité	Logique
0	Les trois variables sont exactement 0 %
1	L'une des variables est supérieure à 0 %
2	L'une des variables est supérieure à 3 %
3	Deux des variables sont supérieures à 3 %
4	Trois des variables sont supérieures à 3 %
5	L'une des variables est supérieure à 6 %
6	Deux des variables sont supérieures à 6 %
7	Trois des variables sont supérieures à 6 %
8	L'une des variables est supérieure à 15 %
9	Deux des variables sont supérieures à 15 %
10	Trois des variables sont supérieures à 15 %

Rapport PCI DSS

Le rapport PCI DSS (Payment Card Industry Data Security Standard) peut vous aider à identifier la distribution des informations de carte de crédit dans vos dossiers. Le rapport contient les informations suivantes :

Présentation

Combien de fichiers contiennent des informations de carte de crédit et dans quels environnements de travail.

Le cryptage

Le pourcentage de fichiers contenant des informations de carte de crédit sur des environnements de travail cryptés ou non cryptés. Ces informations sont spécifiques à Cloud Volumes ONTAP.

Protection contre les ransomwares

Le pourcentage de fichiers contenant des informations de carte de crédit sur des environnements de travail où la protection par ransomware est activée ou non. Ces informations sont spécifiques à Cloud Volumes ONTAP.

La conservation

Délai de la dernière modification des fichiers. Ceci est utile car vous ne devez pas conserver les informations de carte de crédit plus longtemps que vous n'avez besoin de les traiter.

Distribution des informations de carte de crédit

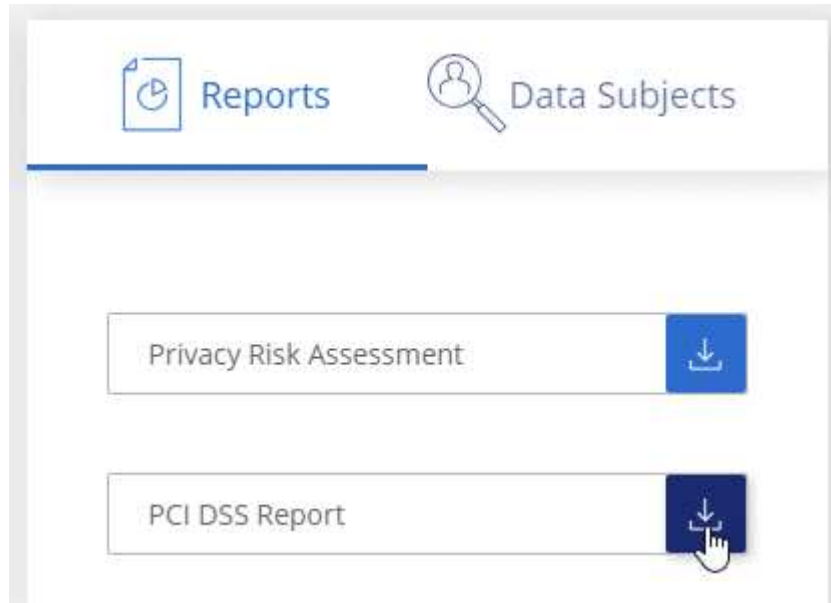
Les environnements de travail où les informations de carte de crédit ont été trouvées et où le chiffrement et la protection contre les ransomwares sont activés.

Génération du rapport PCI DSS

Accédez à l'onglet conformité pour générer le rapport.

Étapes

1. En haut de Cloud Manager, cliquez sur **Cloud Compliance**.
2. Sous **Rapports**, cliquez sur l'icône de téléchargement en regard de **PCI DSS Report**.



Résultat

Cloud Compliance génère un rapport PDF que vous pouvez consulter et envoyer à d'autres groupes si nécessaire.

Rapport HIPAA

Le rapport HIPAA (Health Insurance Portability and Accountability Act) peut vous aider à identifier les fichiers contenant des informations sur la santé. Il est conçu pour aider votre organisation à respecter les lois HIPAA sur la protection des données personnelles. Les informations fournies par Cloud Compliance sont les suivantes :

- Modèle de référence de santé
- Code médical ICD-10-cm
- Code médical ICD-9-cm
- RH – catégorie Santé
- Catégorie données d'application de santé

Le rapport contient les informations suivantes :

Présentation

Combien de fichiers contiennent des informations sur l'état de santé et dans quels environnements de travail.

Le cryptage

Le pourcentage de fichiers contenant des informations de santé sur des environnements de travail chiffrés ou non cryptés. Ces informations sont spécifiques à Cloud Volumes ONTAP.

Protection contre les ransomwares

Le pourcentage de fichiers contenant des informations d'état sur des environnements de travail qui n'ont pas ou qui sont sur lesquels une protection par ransomware est activée. Ces informations sont spécifiques à Cloud Volumes ONTAP.

La conservation

Délai de la dernière modification des fichiers. Ceci est utile parce que vous ne devez pas conserver les renseignements sur la santé plus longtemps que vous n'avez besoin de les traiter.

Distribution des renseignements sur la santé

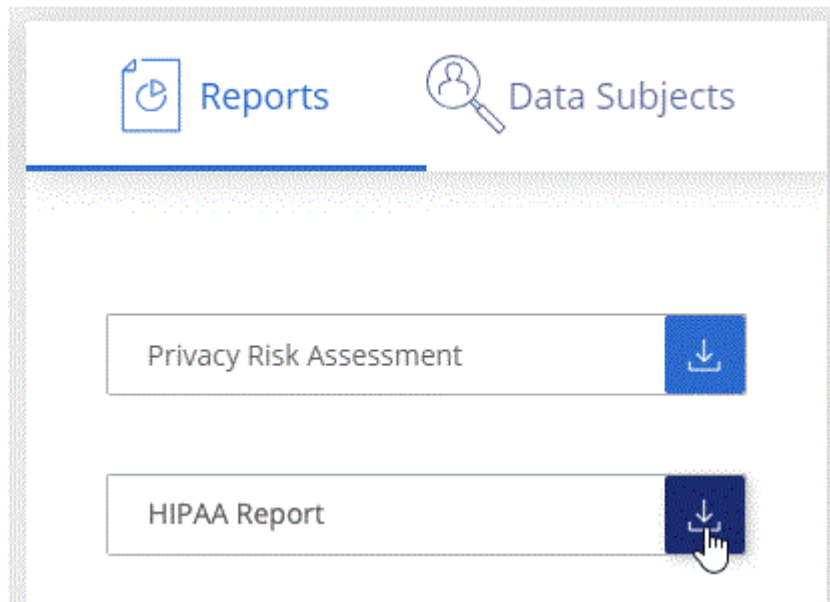
Les environnements de travail dans lesquels les informations de santé ont été trouvées et si le chiffrement et la protection par ransomware sont activés.

Génération du rapport HIPAA

Accédez à l'onglet conformité pour générer le rapport.

Étapes

1. En haut de Cloud Manager, cliquez sur **Cloud Compliance**.
2. Sous **Rapports**, cliquez sur l'icône de téléchargement en regard de **Rapport HIPAA**.



Résultat

Cloud Compliance génère un rapport PDF que vous pouvez consulter et envoyer à d'autres groupes si nécessaire.

Sélection des environnements de travail pour les rapports

Vous pouvez filtrer le contenu du tableau de bord Cloud Compliance pour consulter les données de conformité pour tous les environnements de travail et bases de données, ou pour des environnements de travail spécifiques uniquement.

Lorsque vous filtrez le tableau de bord, Cloud Compliance évalue les données de conformité et les rapports aux environnements de travail que vous avez sélectionnés.

Étapes

1. Cliquez sur la liste déroulante du filtre, sélectionnez les environnements de travail pour lesquels vous souhaitez afficher les données, puis cliquez sur **Afficher**.

The screenshot displays the Cloud Compliance interface. A filter selection menu is open, showing a list of working environments with checkboxes and buttons for each. The main dashboard area shows a summary of data for the selected environments, including a bar chart for Personal Files (20%) and Sensitive Personal Files (5%), and a table of file counts for various categories.

Category	Count
Personal Files	7,000
Sensitive Personal Files	1,400
Email Address	2,700
Credit Card	2,700
Health	2,700
Ethnicity	2,700

Réponse à une demande d'accès à un sujet de données

Répondez à une demande d'accès aux données (DSAR, Data Subject Access Request) en recherchant le nom complet ou l'identifiant connu d'un sujet (par exemple une adresse

e-mail), puis en téléchargeant un rapport. Ce rapport est conçu pour aider votre entreprise à respecter le RGPD ou les autres lois similaires sur la confidentialité des données.



NetApp ne peut garantir une précision de 100 % des données personnelles et des données personnelles sensibles que Cloud Compliance identifie. Vous devez toujours valider les informations en examinant les données.

Qu'est-ce qu'une demande d'accès aux données ?

Les réglementations en matière de confidentialité, telles que le RGPD européen, accordent à des sujets de données (clients ou employés, par exemple) le droit d'accéder à leurs données personnelles. Lorsqu'un sujet de données demande cette information, elle est appelée DSAR (Data Subject Access request). Les organisations sont tenues de répondre à ces demandes "sans délai excessif" et au plus tard dans un mois après réception.

En quoi Cloud Compliance peut-il vous aider à répondre à un SAR ?

Lorsque vous effectuez une recherche dans un sujet de données, Cloud Compliance trouve tous les fichiers dont le nom ou l'identifiant de cette personne est présent. Cloud Compliance vérifie les dernières données pré-indexées pour le nom ou l'identifiant. Il ne lance pas de nouvelle acquisition.

Une fois la recherche terminée, vous pouvez télécharger la liste des fichiers d'un rapport de demande d'accès aux données. Le rapport rassemble les informations issues des données et les place en termes juridiques que vous pouvez renvoyer à la personne.

Recherche de sujets de données et téléchargement de rapports

Recherchez le nom complet ou l'identifiant connu du sujet de données, puis téléchargez un rapport de liste de fichiers ou un rapport DSAR. Vous pouvez effectuer une recherche par "[tout type d'informations personnelles](#)".

Seul l'anglais est pris en charge lors de la recherche des noms des sujets de données. La prise en charge d'autres langues sera ajoutée ultérieurement.

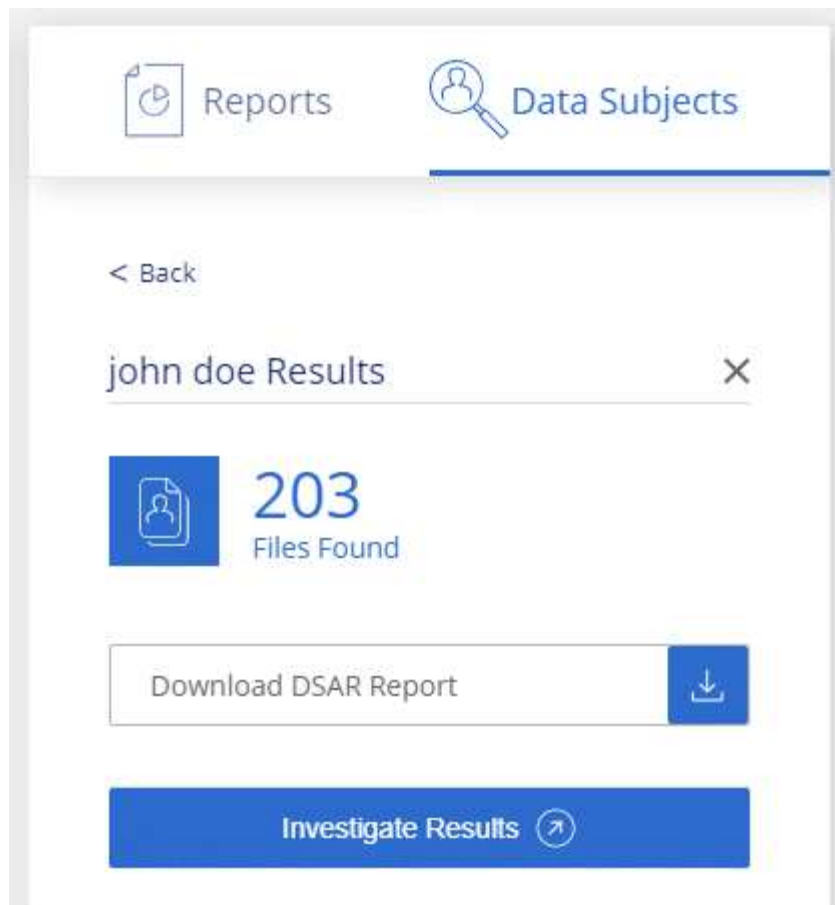


La recherche de sujet de données n'est pas prise en charge actuellement dans les bases de données.

Étapes

1. En haut de Cloud Manager, cliquez sur **Cloud Compliance**.
2. Cliquez sur **sujets de données**.
3. Recherchez le nom complet ou l'identifiant connu du sujet de données.

Voici un exemple qui montre une recherche du nom *john Doe*:



4. Choisissez l'une des options disponibles :

- **Télécharger le rapport DSAR** : réponse officielle à la demande d'accès que vous pouvez envoyer au sujet des données. Ce rapport contient des informations générées automatiquement en fonction des données que Cloud Compliance trouve sur le sujet des données et qui sont conçues pour être utilisées comme modèle. Vous devez remplir le formulaire et le revoir en interne avant de l'envoyer au sujet des données.
- **Étudier les résultats** : une page qui vous permet d'examiner les données en recherchant, en triant, en développant les détails d'un fichier spécifique et en téléchargeant la liste de fichiers.



S'il y a plus de 10,000 résultats, seuls les 10,000 premiers apparaissent dans la liste de fichiers.

Désactivation de Cloud Compliance

Si nécessaire, vous pouvez empêcher Cloud Compliance de scanner un ou plusieurs environnements de travail ou bases de données. Vous pouvez également supprimer l'instance Cloud Compliance si vous ne souhaitez plus utiliser Cloud Compliance avec vos environnements de travail.

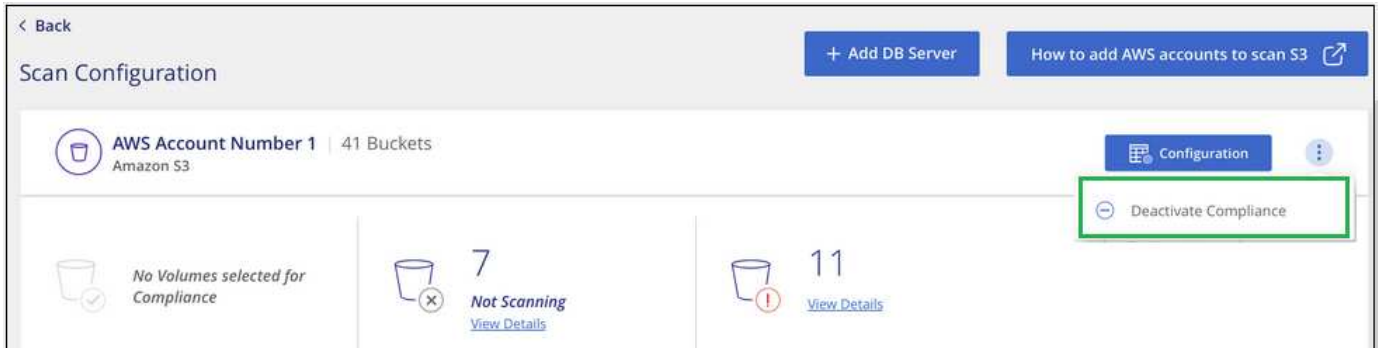
Désactivation des analyses de conformité pour un environnement de travail

Lorsque vous désactivez les analyses, Cloud Compliance ne analyse plus les données du système et supprime les informations de conformité indexées de l'instance Cloud Compliance (les données de

l'environnement de travail ou de la base de données elle-même ne sont pas supprimées).

Étapes

Dans la page *Scan Configuration*, cliquez sur le bouton  Dans la ligne de l'environnement de travail, puis cliquez sur **Désactiver la conformité**.



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

Suppression de l'instance Cloud Compliance

Vous pouvez supprimer l'instance Cloud Compliance si vous ne souhaitez plus utiliser Cloud Compliance. La suppression de l'instance supprime également les disques associés où résident les données indexées.

Étape

1. Accédez à la console de votre fournisseur cloud et supprimez l'instance Cloud Compliance.

L'instance s'appelle *CloudCompliance* avec un hachage (UUID) généré concaténé. Par exemple :
CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7

Questions les plus fréquemment posées concernant Cloud Compliance

Cette FAQ peut vous aider si vous cherchez simplement une réponse rapide à une question.

En quoi consiste la conformité cloud ?

Cloud Compliance est une offre cloud qui utilise la technologie d'intelligence artificielle (IA) pour aider les entreprises à comprendre le contexte des données et à identifier les données sensibles dans l'ensemble des configurations Azure NetApp Files, les systèmes Cloud Volumes ONTAP hébergés sur AWS ou Azure, des compartiments Amazon S3 et des bases de données.

Cloud Compliance fournit des paramètres prédéfinis (par exemple, des types d'informations sensibles et des catégories) pour respecter les nouvelles réglementations en matière de conformité des données en matière de confidentialité et de sensibilité des données, notamment le RGPD, la loi CCPA, HIPAA.

Pourquoi utiliser Cloud Compliance ?

Avec Cloud Compliance, vous pouvez :

- Respectez les réglementations en matière de conformité et de confidentialité des données.
- Respectez les règles de conservation des données.
- Localiser et créer facilement des rapports sur des données spécifiques en réponse à des sujets de données, conformément aux exigences du RGPD, de la loi CCPA, de l'HIPAA et d'autres réglementations en matière de confidentialité des données.

Quelles sont les utilisations courantes de Cloud Compliance ?

- Identifier les informations à caractère personnel
- Identifier une vaste portée des informations sensibles, conformément aux réglementations du RGPD et de la loi CCPA sur la confidentialité.
- Respectez les nouvelles réglementations sur la confidentialité des données, ainsi que celles à venir.

["Pour en savoir plus sur les utilisations de Cloud Compliance"](#).

Quels types de données peuvent être analysés avec Cloud Compliance ?

Cloud Compliance prend en charge l'analyse des données non structurées via les protocoles NFS et CIFS gérés par Cloud Volumes ONTAP et Azure NetApp Files. Cloud Compliance permet également d'analyser les données stockées dans des compartiments Amazon S3.

En outre, Cloud Compliance peut analyser les bases de données qui se trouvent n'importe où, ce qui n'est pas nécessaire de les gérer par Cloud Manager.

["Découvrez le fonctionnement des acquisitions"](#).

Quels sont les fournisseurs de cloud pris en charge ?

Cloud Compliance fonctionne avec Cloud Manager et prend actuellement en charge AWS et Azure. Votre entreprise peut ainsi bénéficier d'une visibilité unifiée sur la confidentialité des données entre les différents fournisseurs de cloud. La prise en charge de Google Cloud Platform (GCP) sera bientôt ajoutée.

Comment accéder à Cloud Compliance ?

Cloud Compliance est exécuté et géré via Cloud Manager. Vous pouvez accéder aux fonctionnalités Cloud Compliance à partir de l'onglet **Compliance** de Cloud Manager.

Comment fonctionne Cloud Compliance ?

Cloud Compliance déploie une autre couche d'intelligence artificielle avec votre système Cloud Manager et vos systèmes de stockage. Il analyse ensuite les données sur des volumes, des compartiments, des bases de données et indexe les informations exploitables qui se trouvent.

["Découvrez le fonctionnement de Cloud Compliance"](#).

Combien coûte Cloud Compliance ?

Le coût d'utilisation de la conformité dans le cloud dépend de la quantité de données à analyser. Les 1 premiers To de données analysés par Cloud Compliance dans un espace de travail Cloud Manager sont gratuits. Un abonnement à AWS ou Azure Marketplace est nécessaire pour poursuivre l'analyse des données après ce point. Voir ["tarifs"](#) pour plus d'informations.

À quelle fréquence Cloud Compliance analyse-t-il mes données ?

Les données évoluent fréquemment. Cloud Compliance les analyse en continu, sans affecter les données. Alors que l'analyse initiale de vos données peut prendre plus de temps, les analyses suivantes ne scannent que les modifications incrémentielles, ce qui réduit les temps d'analyse du système.

["Découvrez le fonctionnement des acquisitions"](#).

Cloud Compliance offre-t-il des rapports ?

Oui. Les informations communiquées par Cloud Compliance peuvent s'avérer utiles pour les autres parties prenantes dans votre entreprise. Nous vous permettons de générer des rapports pour partager les informations exploitables.

Les rapports suivants sont disponibles pour Cloud Compliance :

Rapport d'évaluation des risques pour la confidentialité

Fournit des informations sur la confidentialité à partir de vos données et un score de risque lié à la confidentialité. ["En savoir plus >>"](#).

Rapport de demande d'accès au sujet des données

Vous permet d'extraire un rapport de tous les fichiers contenant des informations concernant le nom spécifique ou l'identifiant personnel d'un sujet de données. ["En savoir plus >>"](#).

Rapport PCI DSS

Vous aide à identifier la distribution des informations de carte de crédit dans vos dossiers. ["En savoir plus >>"](#).

Rapport HIPAA

Vous aide à identifier la distribution de l'information sur la santé dans vos dossiers. ["En savoir plus >>"](#).

Rapports sur un type d'information spécifique

Des rapports sont disponibles, incluant des détails sur les fichiers identifiés qui contiennent des données personnelles et des données personnelles sensibles. Vous pouvez également voir les fichiers dérépartis par catégorie et par type de fichier. ["En savoir plus >>"](#).

Quel type d'instance ou de machine virtuelle est requis pour Cloud Compliance ?

- Dans Azure, Cloud Compliance s'exécute sur une machine virtuelle standard_D16s_v3 avec un disque de 512 Go.
- Dans AWS, Cloud Compliance s'exécute sur une instance m5.4xlarge avec un disque GP2 de 500 Go.

Dans les régions où m5.4xlarge n'est pas disponible, Cloud Compliance s'exécute sur une instance m4.4xlarge.



La modification ou le redimensionnement du type d'instance/de VM n'est pas prise en charge. Vous devez utiliser la taille par défaut fournie.

["Découvrez le fonctionnement de Cloud Compliance"](#).

Les performances d'acquisition varient-elles ?

Les performances d'analyse peuvent varier en fonction de la bande passante réseau et de la taille moyenne des fichiers dans votre environnement cloud.

Quels types de fichiers sont pris en charge ?

Cloud Compliance analyse les informations relatives aux catégories et aux métadonnées de tous les fichiers, et affiche tous les types de fichiers dans la section types de fichiers du tableau de bord.

Lorsque Cloud Compliance détecte des informations à caractère personnel (PII) ou lorsqu'il effectue une recherche DSAR, seuls les formats de fichier suivants sont pris en charge : .PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF ET .JSON.

Comment activer Cloud Compliance ?

Il vous faut tout d'abord déployer une instance de Cloud Compliance dans Cloud Manager. Une fois l'instance en cours d'exécution, vous pouvez l'activer sur les environnements de travail et les bases de données existants à partir de l'onglet **Compliance** ou en sélectionnant un environnement de travail spécifique.

["Découvrez comment démarrer"](#).



L'activation de Cloud Compliance entraîne une analyse initiale immédiate. Les résultats de conformité s'affichent peu de temps après.

Comment désactiver Cloud Compliance ?

Vous pouvez désactiver Cloud Compliance à partir de la page Working Environments après avoir sélectionné un environnement de travail individuel.

["En savoir plus >>"](#).



Pour supprimer complètement l'instance Cloud Compliance, vous pouvez supprimer manuellement l'instance Cloud Compliance du portail de votre fournisseur cloud.

Que se passe-t-il si le Tiering des données est activé sur Cloud Volumes ONTAP ?

Vous pouvez activer Cloud Compliance sur un système Cloud Volumes ONTAP qui transfère les données inactives vers un stockage objet. Si le Tiering est activé, Cloud Compliance analyse toutes les données qui se trouvent sur des disques et les données inactives envoyées vers le stockage objet.

L'analyse de conformité ne chauffe pas les données inactives : elles restent inactives et hiérarchisées vers le stockage objet.

Puis-je utiliser Cloud Compliance pour analyser le stockage ONTAP sur site ?

La numérisation des données directement à partir d'un environnement de travail ONTAP sur site n'est pas prise en charge. Mais vous pouvez analyser vos données ONTAP sur site en répliquant les données NFS ou CIFS sur un environnement de travail Cloud Volumes ONTAP puis en activant la conformité sur ces volumes. Nous prévoyons d'assurer la conformité cloud avec d'autres offres cloud telles que Cloud Volumes Service.

["En savoir plus >>"](#).

Cloud Compliance peut-il envoyer des notifications à mon entreprise ?

Non, mais vous pouvez télécharger des rapports de statut que vous pouvez partager en interne dans votre entreprise.

Puis-je personnaliser le service en fonction des besoins de mon entreprise ?

Cloud Compliance vous fournit des informations exploitables prêtes à l'emploi pour vos données. Ces informations peuvent être extraites et utilisées en fonction des besoins de votre entreprise.

Est-il possible de limiter les informations de conformité cloud à des utilisateurs spécifiques ?

Oui, Cloud Compliance est entièrement intégré avec Cloud Manager. Les utilisateurs de Cloud Manager ne peuvent voir que les informations relatives aux environnements de travail qu'ils peuvent afficher en fonction de leurs privilèges d'espace de travail.

En outre, si vous souhaitez autoriser certains utilisateurs à simplement afficher les résultats d'analyse de Cloud Compliance sans pouvoir gérer les paramètres Cloud Compliance, vous pouvez attribuer à ces utilisateurs le rôle *Cloud Compliance Viewer*.

["En savoir plus >>"](#).

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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