



Activez la numérisation sur vos sources de données

Cloud Manager 3.8

NetApp
March 25, 2024

Sommaire

- Activez la numérisation sur vos sources de données 1
 - Mise en route de Cloud Compliance pour Cloud Volumes ONTAP et Azure NetApp Files 1
 - Mise en route de Cloud Compliance pour Amazon S3 5
 - Analyse des schémas de base de données..... 13
 - Une analyse des données ONTAP sur site avec Cloud Compliance à l'aide de SnapMirror..... 16

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**.

The screenshot displays the 'Scan Configuration' page in Cloud Manager. At the top left, there is a 'View Dashboard >' link. At the top right, there is a link 'How to add AWS accounts to scan S3' with an external link icon. The main content area is divided into three sections, each representing a different environment:

- AWS Account Number 1** (Amazon S3): This section includes a text instruction: 'To enable Compliance for Amazon S3 on this AWS account or other, go to [Working Environment tab](#), select the Amazon S3 cloud and activate Compliance from the right hand panel.'
- Azure Netapp Files** (Azure NetApp Files): This section features a prominent blue button labeled 'Activate Compliance for All Volumes' and a smaller link 'or select Volumes' below it.
- Working Environment Name 1** (Cloud Volumes ONTAP): This section also features a prominent blue button labeled 'Activate Compliance for All Volumes' and a smaller link 'or select Volumes' below it.

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.

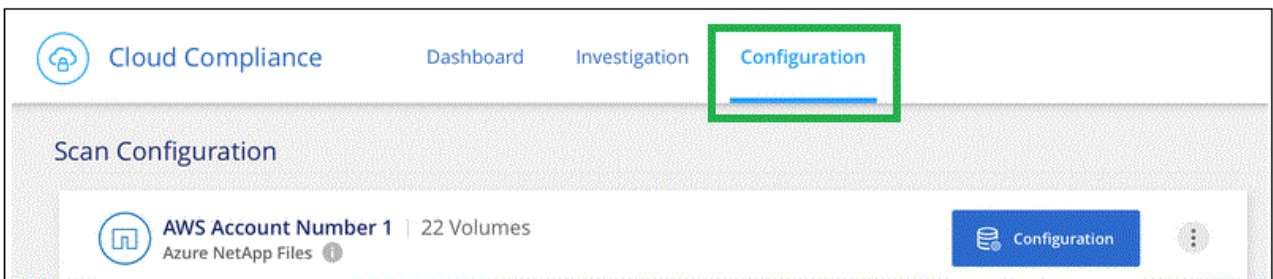


Pour Azure NetApp Files, Cloud Compliance ne peut analyser que les volumes qui se trouvent dans la même région que Cloud Manager.

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.

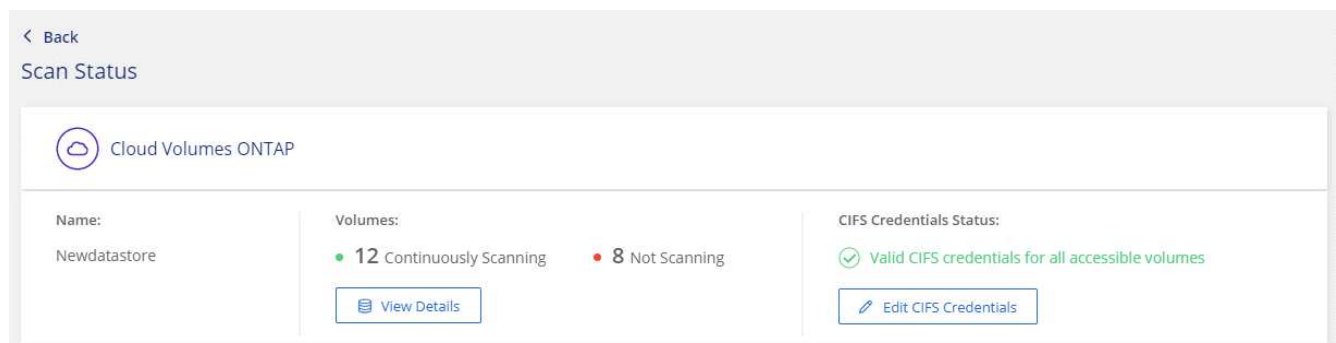
3. Assurez-vous que les règles d'exportation de volume NFS incluent l'adresse IP de l'instance Cloud Compliance afin que les services IT puissent accéder aux données de chaque volume.
4. Si vous utilisez CIFS, fournissez Cloud Compliance avec des identifiants Active Directory pour qu'il puisse analyser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

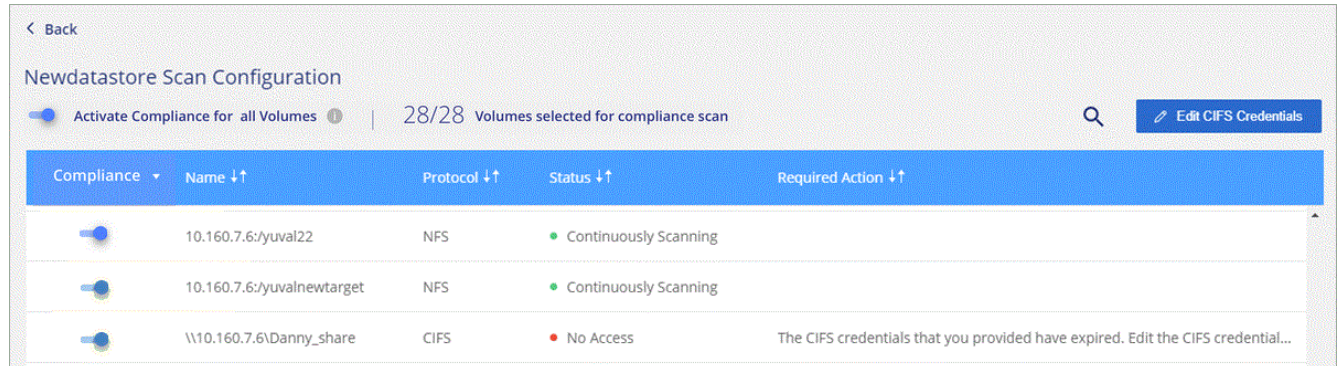
Une fois les informations d'identification saisies, un message indiquant que tous les volumes CIFS ont été authentifiés avec succès s'affiche.



5. Sur la page *Scan Configuration*, cliquez sur **View Details** pour vérifier l'état de chaque volume CIFS et

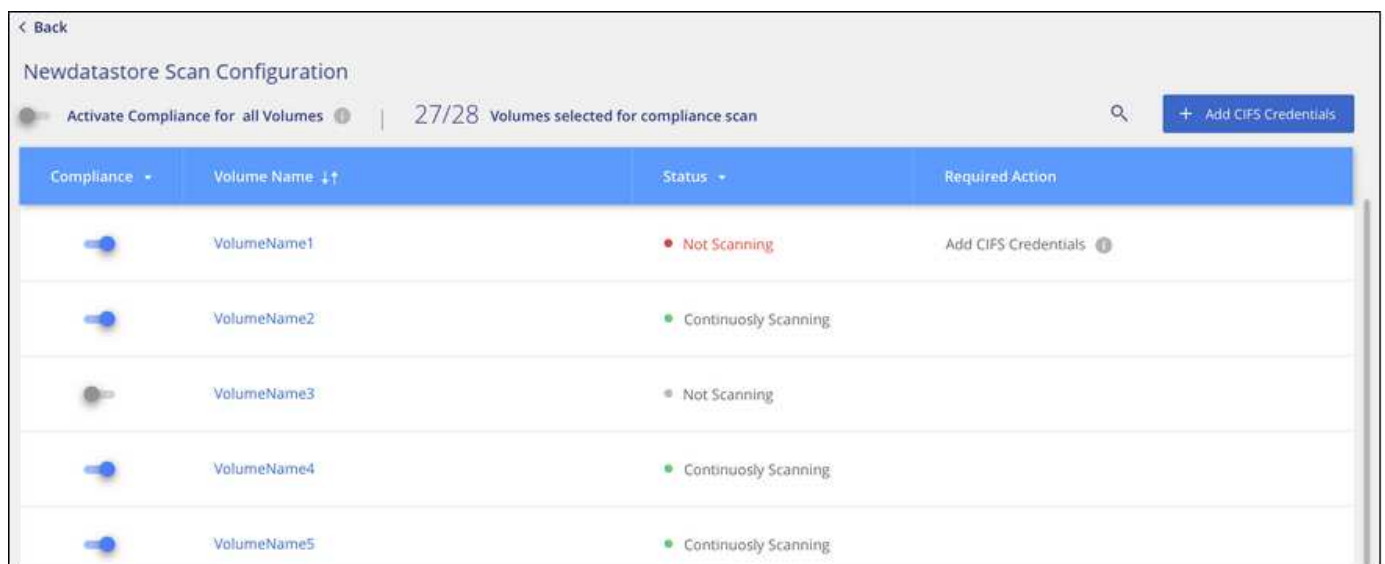
NFS et corriger les erreurs éventuelles.

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.



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.



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.](#)



2 Déployez l'instance Cloud Compliance

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



3 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.



4 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

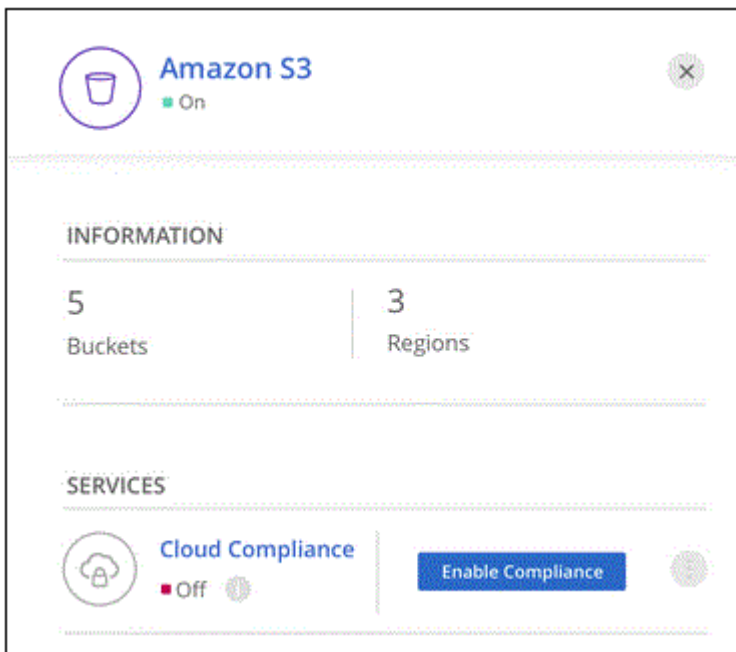
Activez Cloud Compliance sur Amazon S3 après avoir vérifié les prérequis.

Étapes

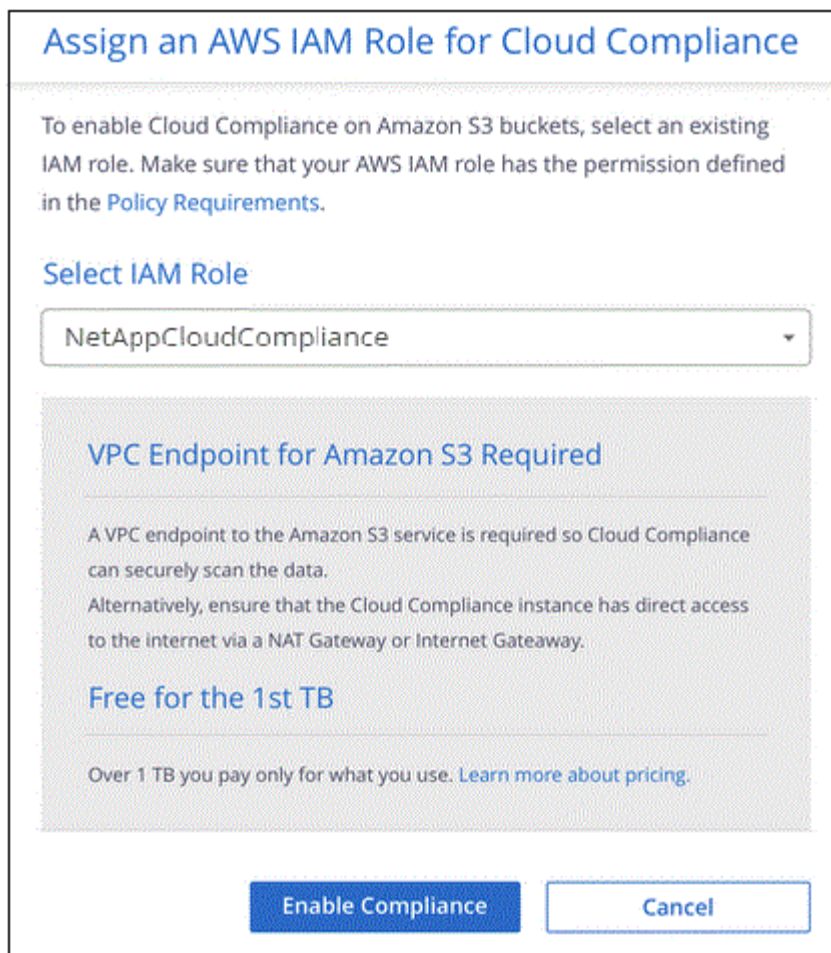
1. En haut de Cloud Manager, cliquez sur **environnements de travail**.
2. Sélectionnez l'environnement de travail Amazon S3.



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

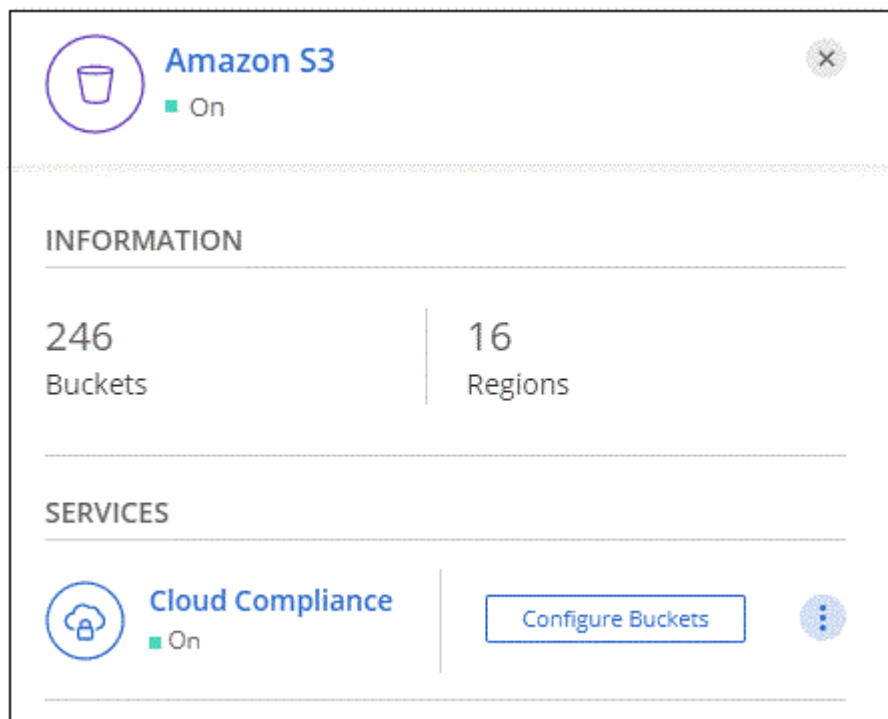
Une fois que Cloud Manager active Cloud Compliance sur Amazon S3, l'étape suivante consiste à configurer les compartiments à analyser.

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.

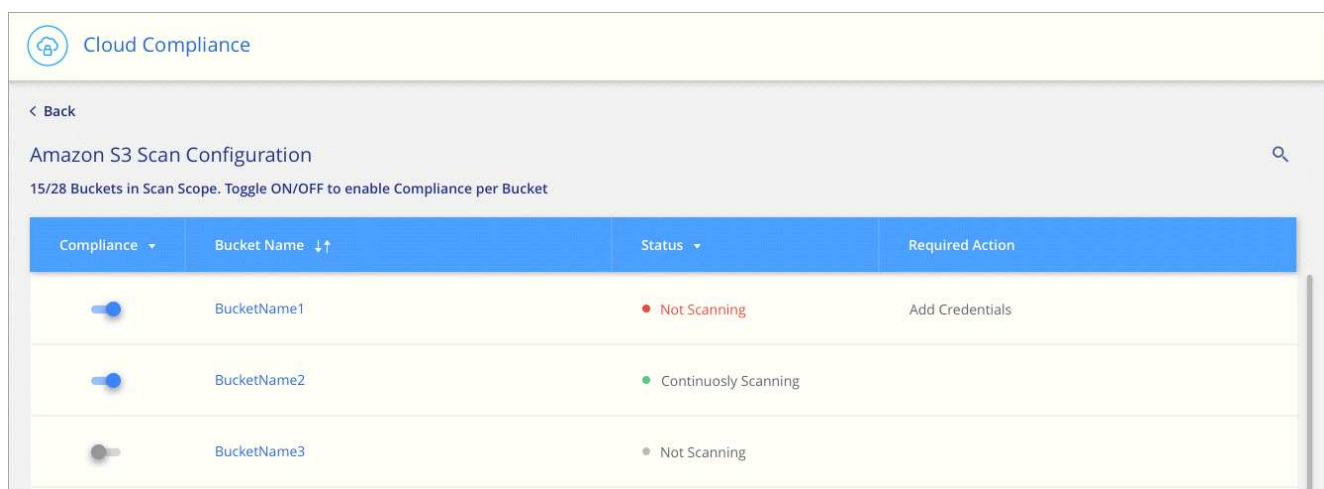
Cloud Compliance l'est également [Analysez les compartiments S3 qui se trouvent dans différents comptes AWS](#).

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.

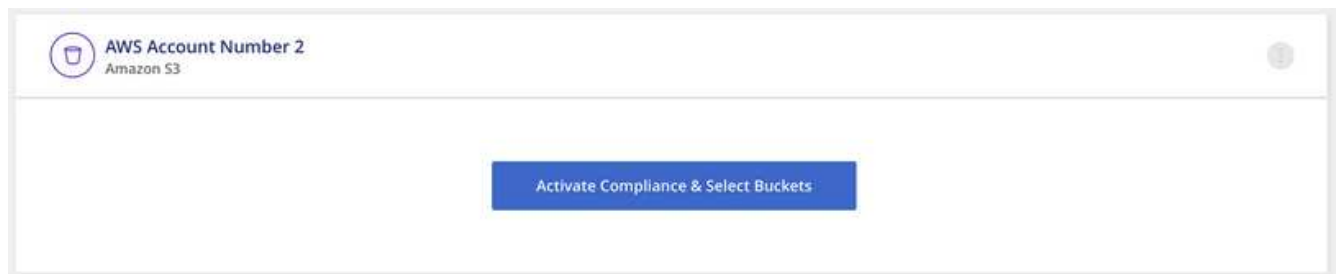
```

{
  "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.

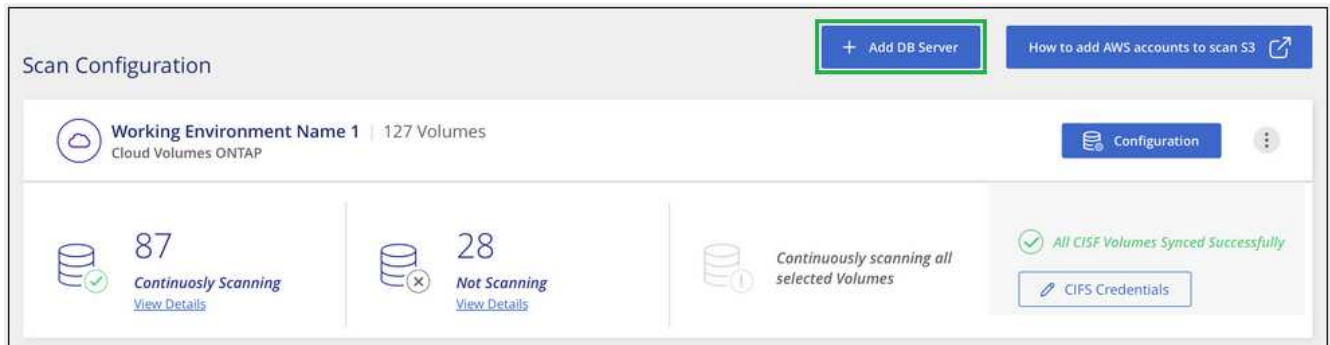
Remarque : pour MongoDB, un rôle d'administrateur en lecture seule est requis.

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

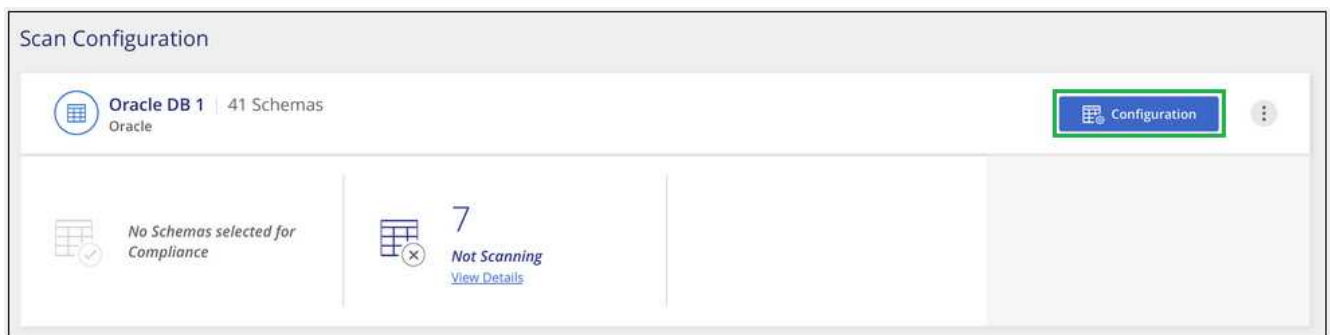
Username Password

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			
28/28 Schemas selected for compliance scan		<input type="button" value="Edit Credentials"/>	
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.

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.