



データソースでスキャンをアクティブ化します

Cloud Manager

NetApp
April 08, 2021

This PDF was generated from https://docs.netapp.com/us-en/occm/task_getting_started_compliance.html on April 08, 2021. Always check docs.netapp.com for the latest.

目次

データソースでスキャンをアクティブ化します	1
『 Getting started with Cloud Compliance for Cloud Volumes ONTAP 、 On-Premises ONTAP 、 or Azure NetApp Files 』	1
Cloud Compliance for Amazon S3 の利用を開始してください	9
データベーススキーマをスキャンしています	15
OneDrive アカウントをスキャンしています	19

データソースでスキャンをアクティブ化します

『 Getting started with Cloud Compliance for Cloud Volumes ONTAP 、 On-Premises ONTAP 、 or Azure NetApp Files 』

Cloud Compliance for Cloud Volumes ONTAP 、 オンプレミスの ONTAP システム、 Azure NetApp Files の導入を開始するには、いくつかの手順を実行します。

クイックスタート

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

目的のデータが含まれているデータソースを検出します をクリックしてください

ボリュームをスキャンするには、 Cloud Manager で作業環境にシステムを追加する必要があります。

- Cloud Volumes ONTAP システムの場合、これらの作業環境はすでに Cloud Manager で使用可能になっている必要があります
- オンプレミスの ONTAP システムでは、 ["ONTAP クラスタは Cloud Manager で検出する必要があります"](#)
- Azure NetApp Files の場合、 ["構成を検出するには、 Cloud Manager が設定されている必要があります"](#)。

Cloud Compliance インスタンスを導入します

["Cloud Manager に Cloud Compliance を導入"](#) インスタンスが展開されていない場合。

作業環境で **Cloud Compliance** を有効にし、を選択します スキャンするボリューム

コンプライアンス * をクリックし、 * 構成 * タブを選択して、特定の作業環境でボリュームのコンプライアンススキャンを有効にします。

ボリュームへのアクセスを確認

Cloud Compliance が有効になったので、ボリュームにアクセスできることを確認します。

- クラウドコンプライアンスインスタンスには、各 Cloud Volumes ONTAP サブネット、 Azure NetApp Files サブネット、 オンプレミスの ONTAP システムへのネットワーク接続が必要です。
- Cloud Volumes ONTAP のセキュリティグループは、クラウドコンプライアンスインスタンスからのインバウンド接続を許可する必要があります。
- 次のポートが Cloud Compliance インスタンスに対して開いていることを確認します。
 - NFS –ポート 111 および 2049 。
 - CIFS の場合 - ポート 139 および 445
- NFS ボリュームのエクスポートポリシーで、 Cloud Compliance インスタンスからのアクセスを許可する必要があります。

- CIFS ボリュームをスキャンするには、Cloud Compliance で Active Directory のクレデンシャルが必要です。

コンプライアンス * > * スキャン設定 * > * CIFS クレデンシャルの編集 * をクリックし、クレデンシャルを入力します。

スキャンするボリュームを管理します

スキャンするボリュームを選択または選択解除すると、Cloud Compliance によるスキャンが開始または停止します。

スキャンするデータソースを検出しています

スキャンするデータソースがまだ Cloud Manager 環境にない場合は、ここでキャンバスに追加できます。

Cloud Volumes ONTAP システムは、Cloud Manager のキャンバスですでに使用できるようになっている必要があります。オンプレミスの ONTAP システムには、が必要です ["これらのクラスタは Cloud Manager で検出されます"](#)。Azure NetApp Files の場合は、["構成を検出するには、Cloud Manager が設定されている必要があります"](#)。

Cloud Compliance インスタンスの導入

["Cloud Compliance の導入"](#) インスタンスが展開されていない場合。

Cloud Volumes ONTAP やオンプレミスの ONTAP システムをスキャンする場合、クラウドまたはオンプレミスの場所に Cloud Compliance を導入できます。

Azure NetApp Files ボリュームをスキャンする際にはクラウドに Cloud Compliance を導入し、スキャンするボリュームと同じリージョンに導入する必要があります。

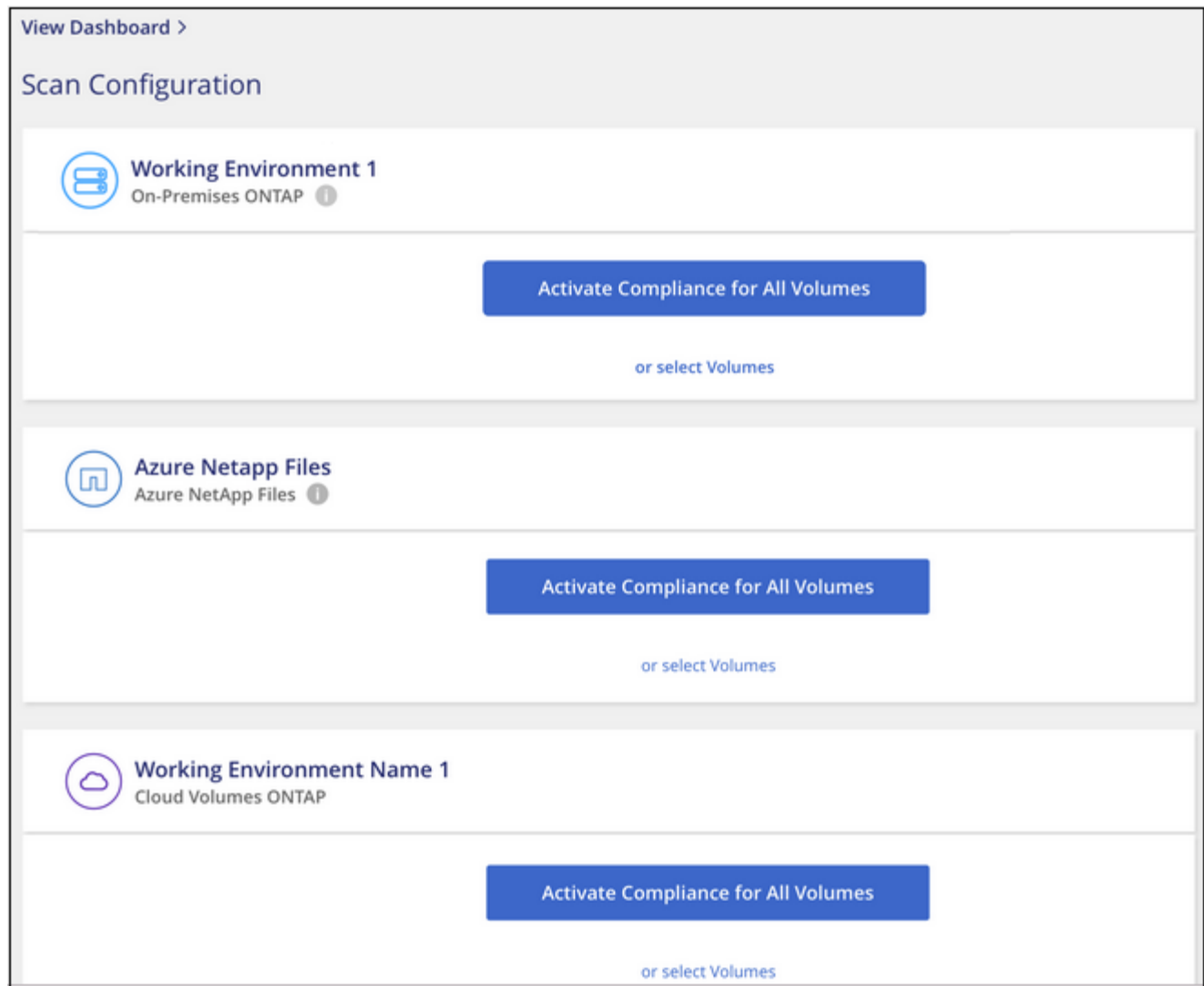
作業環境での Cloud Compliance の有効化

Cloud Volumes ONTAP システム（AWS および Azure）、オンプレミスの ONTAP クラスタ、および Azure NetApp Files で Cloud Compliance を有効にすることができます。



オンプレミス ONTAP システムで次の手順を実行すると、オンプレミス ONTAP システム上のボリュームが直接スキャンされます。すでにオンプレミスからバックアップファイルを作成している場合 ["クラウドバックアップ"](#)ではなく、クラウド内のバックアップファイルに対してコンプライアンススキャンを実行できます。に進みます [オンプレミスの ONTAP システムからバックアップファイルをスキャンする](#) バックアップファイルをスキャンしてボリュームをスキャンします。

1. Cloud Manager の上部で、* Compliance * をクリックし、* Configuration * タブを選択します。



- 作業環境内のすべてのボリュームをスキャンするには、 * すべてのボリュームのコンプライアンスをアクティブ化 * をクリックします。

作業環境内の特定のボリュームのみをスキャンするには、 * をクリックするか、 Volumes （ボリューム） * を選択して、スキャンするボリュームを選択します。

を参照してください [ボリュームのコンプライアンススキャンの有効化と無効化](#) を参照してください。

Cloud Compliance によって、作業環境で選択したボリュームのスキャンが開始されます。結果は、 Cloud Compliance ダッシュボードで最初のスキャンが完了するとすぐに表示されます。所要時間はデータ量によって異なります。数分から数時間かかる場合もあります。

Cloud Compliance がボリュームにアクセスできることの確認

ネットワーク、セキュリティグループ、およびエクスポートポリシーを確認して、 Cloud Compliance がボリュームにアクセスできることを確認します。CIFS ボリュームにアクセスできるようにするには、 Cloud Compliance に CIFS クレデンシャルを指定する必要があります。

手順

- クラウドコンプライアンスインスタンスと、 Cloud Volumes ONTAP 、 Azure NetApp Files 、またはオン

プレミスの ONTAP クラスターのボリュームを含む各ネットワークとの間にネットワーク接続が確立されていることを確認します。

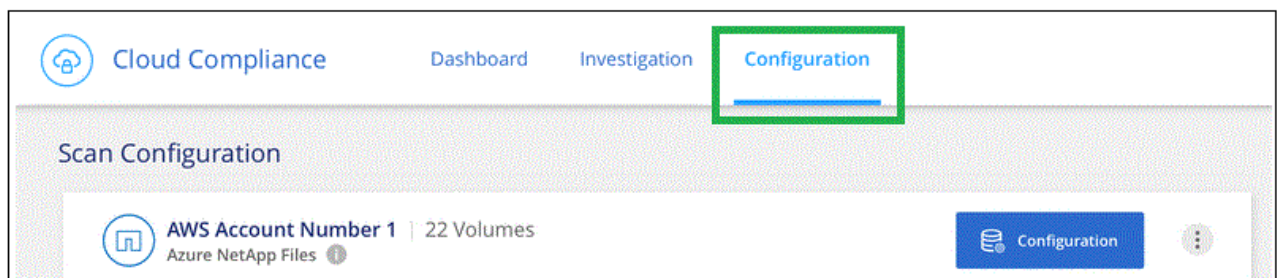


Azure NetApp Files の場合、Cloud Compliance は Cloud Manager と同じリージョンにあるボリュームのみをスキャンできます。

2. Cloud Volumes ONTAP のセキュリティグループがクラウドコンプライアンスインスタンスからのインバウンドトラフィックを許可していることを確認してください。

Cloud Compliance インスタンスの IP アドレスからのトラフィックのセキュリティグループを開くか、仮想ネットワーク内からのすべてのトラフィックのセキュリティグループを開くことができます。

3. 次のポートが Cloud Compliance インスタンスに対して開いていることを確認します。
 - NFS –ポート 111 および 2049。
 - CIFS の場合 - ポート 139 および 445
4. NFS ボリュームのエクスポートポリシーに Cloud Compliance インスタンスの IP アドレスが含まれていて、各ボリュームのデータにアクセスできることを確認します。
5. CIFS を使用する場合は、Active Directory クレデンシャルを使用して Cloud Compliance を提供し、CIFS ボリュームをスキャンできるようにします。
 - a. Cloud Manager の上部で、* Compliance * をクリックします。
 - b. [* 構成 *] タブをクリックします。



ボタンを示す [遵守] タブのスクリーンショット。"]

- c. 各作業環境について、* CIFS 資格情報の編集 * をクリックし、クラウド・コンプライアンスがシステム上の CIFS ボリュームにアクセスするために必要なユーザー名とパスワードを入力します。

クレデンシャルは読み取り専用ですが、管理者のクレデンシャルを指定することで、Cloud Compliance は昇格された権限が必要なデータを読み取ることができます。クレデンシャルは Cloud Compliance インスタンスに保存されます。

クレデンシャルを入力すると、すべての CIFS ボリュームが認証されたことを示すメッセージが表示されます。

< Back

Scan Status

Cloud Volumes ONTAP

Name:
Newdatastore

Volumes:

12 Continuously Scanning

8 Not Scanning

View Details

CIFS Credentials Status:

Valid CIFS credentials for all accessible volumes

Edit CIFS Credentials

6. `_Scan Configuration_page` で、 `* View Details *` をクリックして、各 CIFS および NFS ボリュームのステータスを確認し、エラーを修正します。

たとえば、次の図は 3 つのボリュームを示しています。1 つは Cloud Compliance インスタンスとボリュームの間のネットワーク接続の問題が原因で Cloud Compliance がスキャンできないボリュームです。

< 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...

ボリュームのコンプライアンススキャンの有効化と無効化

作業環境内のボリュームのスキャンは、`Scan Configuration` ページからいつでも停止または開始できます。すべてのボリュームをスキャンすることを推奨します。

< 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 checked="" 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	

終了：	手順：
ボリュームのスキャンを無効にします	音量スライダを左に動かします
すべてのボリュームのスキャンを無効にします	[すべてのボリュームのコンプライアンスを有効にする *] スライダを左に移動します
ボリュームのスキャンを有効にします	音量スライダを右に動かします
すべてのボリュームのスキャンを有効にします	[すべてのボリュームのコンプライアンスを有効にする *] スライダを右に移動します



作業環境に追加した新しいボリュームは、すべてのボリュームのコンプライアンスのアクティブ化 * 設定が有効になっている場合にのみ自動的にスキャンされます。この設定を無効にすると、作業環境で作成する新しいボリュームごとにスキャンを有効にする必要があります。

オンプレミスの ONTAP システムからバックアップファイルをスキャンする

Cloud Compliance でオンプレミスの ONTAP システム上のボリュームを直接スキャンしない場合は、2021 年 1 月にリリースされる新しいベータ機能によって、オンプレミスの ONTAP ボリュームから作成されたバックアップファイルに対してコンプライアンススキャンを実行できます。したがって、を使用してバックアップファイルを既に作成している場合にも同様です ["クラウドバックアップ"](#)この新機能を使用して、バックアップファイルに対してコンプライアンススキャンを実行できます。

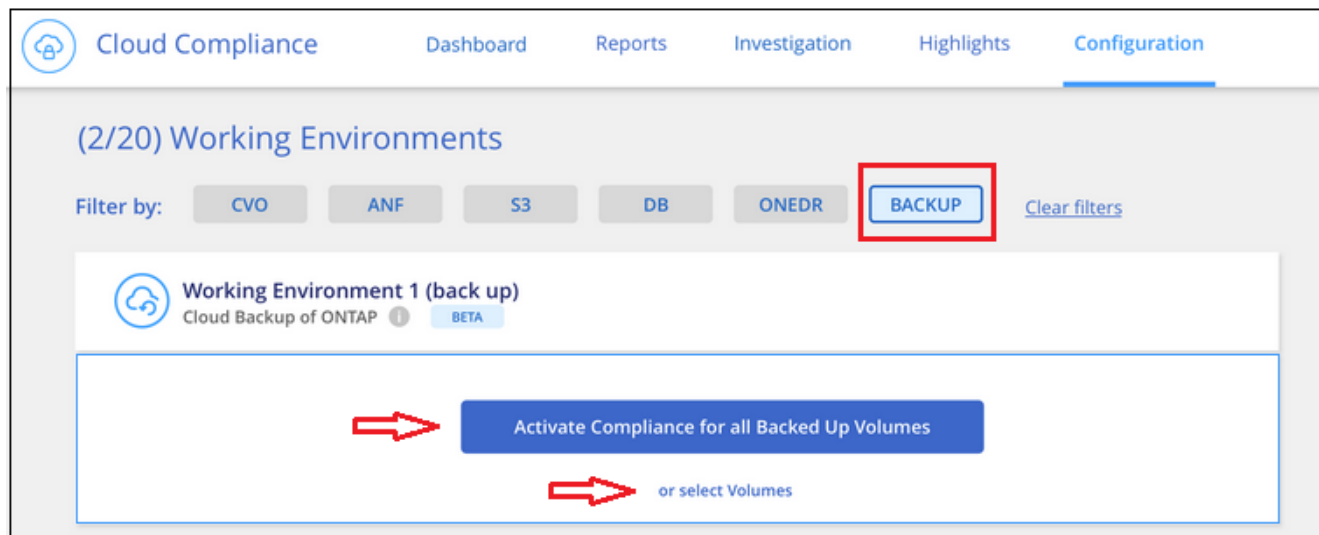
バックアップファイルで実行したコンプライアンススキャンは * 無料 * - Cloud Compliance サブスクリプションやライセンスは不要です。

- ・注：コンプライアンスがバックアップファイルをスキャンする場合、バックアップファイルへのアクセスには、リストアインスタンスから付与された権限が使用されます。通常、ファイルをアクティブにリストアしていない場合はリストアインスタンスの電源がオフになりますが、バックアップファイルをスキャンするときはオンのままになります。を参照してください ["Restore インスタンスに関する詳細情報"](#)。

オンプレミスの ONTAP システムからバックアップファイルをスキャンする場合は、次の手順を実行します。

1. Cloud Manager の上部で、* Compliance * をクリックし、* Configuration * タブを選択します。
2. 作業環境のリストで、フィルタのリストから * backup * ボタンをクリックします。

バックアップファイルがあるオンプレミスの ONTAP 作業環境がすべて表示されます。オンプレミスシステムにバックアップファイルがない場合、作業環境は表示されません。



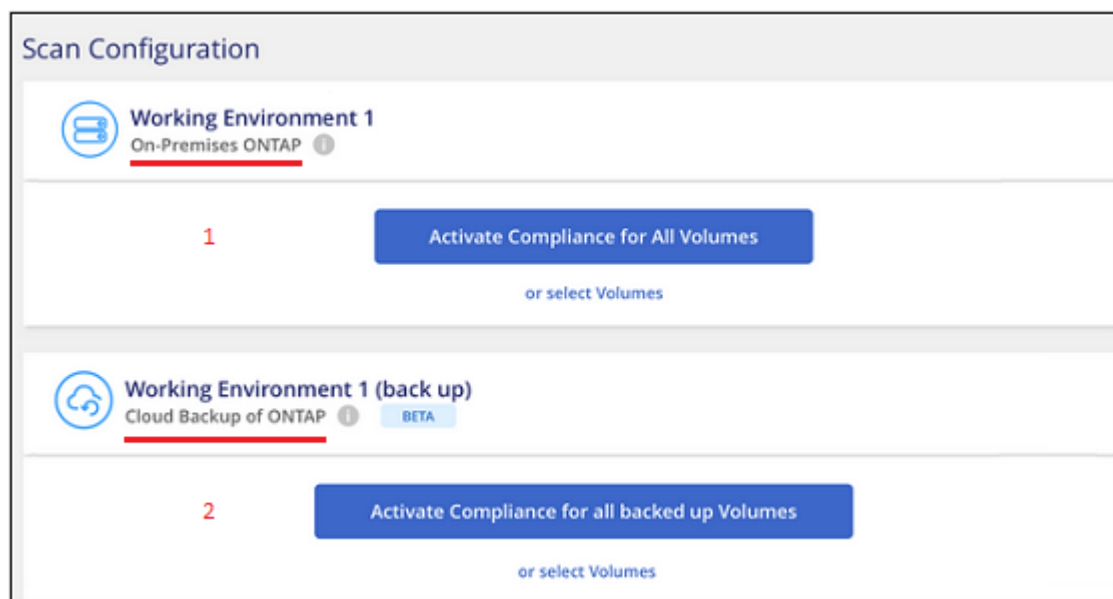
3. 作業環境でバックアップされたすべてのボリュームをスキャンするには、 * すべてのバックアップされたボリュームのコンプライアンスをアクティブ化 * をクリックします。

作業環境でバックアップされた特定のボリュームのみをスキャンするには、 * をクリックするか、Volumes（ボリューム）を選択し、スキャンするバックアップファイル（ボリューム）を選択します。

を参照してください [ボリュームのコンプライアンススキャンの有効化と無効化](#) を参照してください。

オンプレミスボリュームをスキャンするか、それらのボリュームのバックアップをスキャンするか

作業環境のリスト全体を表示すると、ファイルをバックアップしている場合は、オンプレミスクラスタごとに2つのリストが表示されます。



最初の項目はオンプレミスクラスタと実際のボリュームです。2 つ目は、同じオンプレミスクラスタのバックアップファイルです。

オンプレミスシステム上のボリュームをスキャンする最初のオプションを選択します。2 番目のオプションを選択して、対象のボリュームからバックアップファイルをスキャンします。同じクラスタのオンプレミスボリ

ユーモとバックアップファイルの両方をスキャンしないでください。

データ保護ボリュームをスキャンしています

デフォルトでは、データ保護（ DP ）ボリュームは外部から公開されておらず、 Cloud Compliance はアクセスできないため、スキャンされません。オンプレミスの ONTAP システムまたは Cloud Volumes ONTAP システムからの SnapMirror 処理のデスティネーションボリュームです。

最初は、ボリュームリストでこれらのボリュームを **Type* DP *** でスキャンしていないステータス * および必要なアクション **_* DP ボリュームへのアクセスを有効にします ***。

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	

これらのデータ保護ボリュームをスキャンする場合は、次の手順を実行します。

1. ページ上部の *** DP ボリュームへのアクセスを有効にする *** ボタンをクリックします。
2. 確認メッセージを確認し、もう一度「 *** DP ボリュームへのアクセスを有効にする *** 」をクリックします。
 - ソース ONTAP システムで最初に NFS ボリュームとして作成されたボリュームが有効になります。
 - ソース ONTAP システムで最初に CIFS ボリュームとして作成されたボリュームでは、それらの DP ボリュームをスキャンするために CIFS クレデンシャルを入力する必要があります。Cloud Compliance で CIFS ボリュームをスキャンするためにすでに Active Directory クレデンシャルを入力している場合は、それらのクレデンシャルを使用するか、別の管理者クレデンシャルを指定することができます。

Provide Active Directory Credentials

☒ Use existing CIFS Scanning Credentials (user1@domain2) ☐ Use Custom Credentials

Active Directory Domain DNS IP Address

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Compliance. The shares' export policies will allow access only from the Cloud Compliance instance. [Learn More](#)

Provide Active Directory Credentials

☐ Use existing CIFS Scanning Credentials (user1@domain2) ☒ Use Custom Credentials

Username Password

Active Directory Domain DNS IP Address

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Compliance. The shares' export policies will allow access only from the Cloud Compliance instance. [Learn More](#)

3. スキャンする各 DP ボリュームをアクティブ化します **他のボリュームも有効にした場合と同じです** をクリックするか、すべてのボリュームでコンプライアンスのアクティブ化 *** コントロール** を使用して、すべて

の DP ボリュームを含むすべてのボリュームを有効にします。

有効にすると、コンプライアンスのためにアクティブ化された各 DP ボリュームから NFS 共有が作成され、スキャンすることができます。共有のエクスポートポリシーでは、Cloud Compliance インスタンスからのアクセスのみが許可されます。

- 注： DP ボリュームへのアクセスを最初に有効にしたときに CIFS データ保護ボリュームがなかった場合は、一部のボリュームを追加すると、CIFS DP へのアクセスを有効にするボタン * がスキャン設定ページの上に表示されます。このボタンをクリックして、CIFS DP ボリュームへのアクセスを有効にする CIFS クレデンシャルを追加します。

Cloud Compliance for Amazon S3 の利用を開始してください

Cloud Compliance では、Amazon S3 バケットをスキャンして、S3 オブジェクトストレージに格納されている個人データや機密データを特定できます。Cloud Compliance は、ネットアップソリューション用に作成されたバケットであるかどうかに関係なく、アカウント内の任意のバケットをスキャンできます。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

クラウド環境で **S3** の要件を設定します

クラウド環境が Cloud Compliance の要件を満たしていることを確認します。たとえば、IAM ロールの準備と Cloud Compliance から S3 への接続の設定を行います。 [すべてのリストを参照してください](#)。

Cloud Compliance インスタンスを導入します

"[Cloud Compliance の導入](#)" インスタンスが展開されていない場合。

S3 作業環境でコンプライアンスをアクティブ化します

Amazon S3 作業環境を選択し、* 準拠の有効化 * をクリックして、必要な権限を含む IAM ロールを選択します。

スキャンするバケットを選択します

スキャンするバケットを選択すると、Cloud Compliance でスキャンが開始されます。

S3 の前提条件の確認

S3 バケットのスキャンに固有の要件を次に示します。

Cloud Compliance インスタンス用の **IAM** ロールを設定します

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

Cloud Compliance から Amazon S3 への接続を提供

VPC エンドポイントを作成するときは、Cloud Compliance インスタンスに対応するリージョン、VPC、およびルーティングテーブルを選択してください。S3 エンドポイントへのトラフィックを有効にする発信 HTTPS ルールを追加するには、セキュリティグループも変更する必要があります。そうしないと、Cloud Compliance は S3 サービスに接続できません。

問題が発生した場合は、を参照してください ["AWS のサポートナレッジセンター：ゲートウェイ VPC エンドポイントを使用して S3 バケットに接続できないのはなぜですか。"](#)

別の方法として、NAT ゲートウェイを使用して接続を提供する方法があります。



インターネット経由で S3 にアクセスするためにプロキシを使用することはできません。

Cloud Compliance インスタンスの導入

["Cloud Manager に Cloud Compliance を導入"](#) インスタンスが展開されていない場合。

この AWS アカウントで S3 バケットが Cloud Manager で自動的に検出されて Amazon S3 作業環境に表示されるように、AWS コネクタにインスタンスを導入する必要があります。

- 注： * オンプレミスの場所に Cloud Compliance を導入することは、現在 S3 バケットのスキャンではサポートされていません。

S3 作業環境でのコンプライアンスのアクティブ化

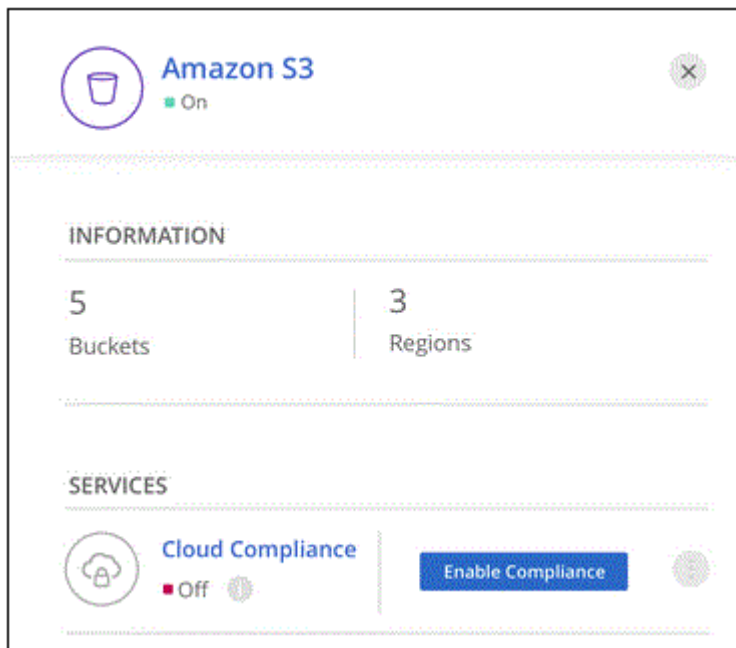
前提条件を確認したら、Amazon S3 で Cloud Compliance を有効にします。

手順

1. Cloud Manager の上部にある * Canvas * をクリックします。
2. Amazon S3 作業環境を選択します。



3. 右側のペインで、 * コンプライアンスを有効にする * をクリックします。



4. プロンプトが表示されたら、の Cloud Compliance インスタンスに IAM ロールを割り当てます [必要な権限](#)。

Assign an AWS IAM Role for Cloud Compliance

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

Select IAM Role

NetAppCloudCompliance

VPC Endpoint for Amazon S3 Required

A VPC endpoint to the Amazon S3 service is required so Cloud Compliance can securely scan the data.

Alternatively, ensure that the Cloud Compliance instance has direct access to the internet via a NAT Gateway or Internet Gateway.

Free for the 1st TB

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

Enable ComplianceCancel

5. [コンプライアンスを有効にする] をクリックします。



また、作業環境のコンプライアンススキャンを有効にすることもできます。 をクリックして、[スキャン設定] ページからアクセスします。 ボタンを押して、*コンプライアンスを有効にする* を選択します。

Cloud Manager によって、インスタンスに IAM ロールが割り当てられます。

S3 バケットでの準拠スキャンの有効化と無効化

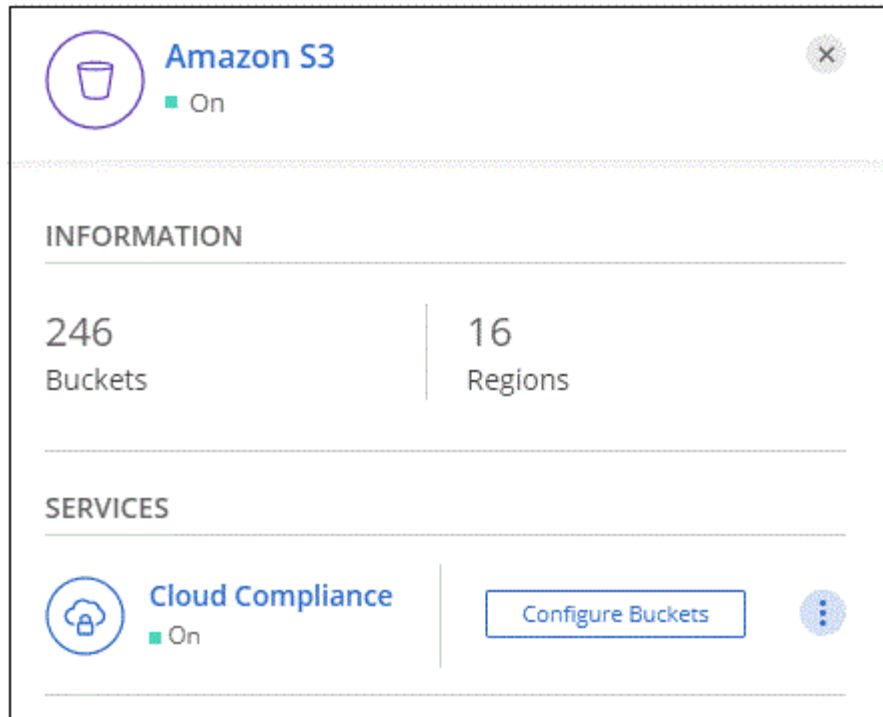
Cloud Manager で Amazon S3 の Cloud Compliance が有効になったら、次の手順でスキャンするバケットを設定します。

スキャンする S3 バケットを含む AWS アカウントで Cloud Manager を実行している場合は、そのバケットが検出され、Amazon S3 作業環境に表示されます。

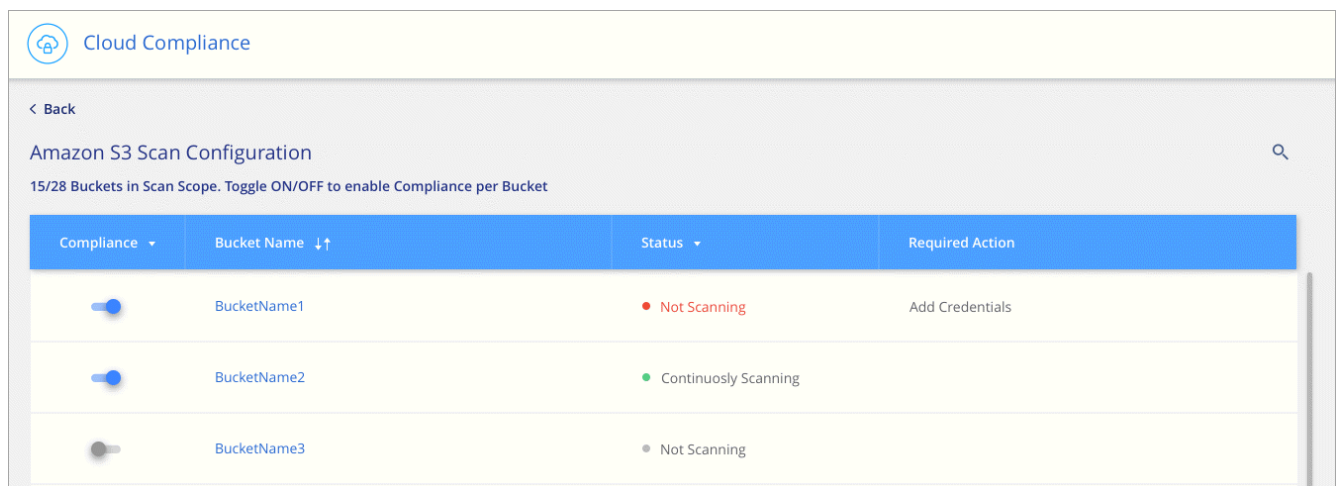
Cloud Compliance も同様です [別々の AWS アカウントにある S3 バケットをスキャンします](#)。

手順

1. Amazon S3 作業環境を選択します。
2. 右側のペインで、*バケットの設定* をクリックします。



3. スキャンするバケットで準拠を有効にします。



Cloud Compliance で、有効にした S3 バケットのスキャンが開始されます。エラーが発生した場合は、エラーを修正するために必要なアクションとともに、[ステータス] 列に表示されます。

追加の **AWS** アカウントからバケットをスキャンする

別の AWS アカウントを使用している S3 バケットをスキャンするには、そのアカウントからロールを割り当てて、既存の Cloud Compliance インスタンスにアクセスします。

手順

1. S3 バケットをスキャンするターゲット AWS アカウントに移動し、* 別の AWS アカウント * を選択して IAM ロールを作成します。

Create role





1

2

3

4


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 

必ず次の手順を実行してください。

- Cloud Compliance インスタンスが存在するアカウントの ID を入力します。
- 最大 CLI / API セッション期間 * を 1 時間から 12 時間に変更し、変更を保存してください。
- Cloud Compliance IAM ポリシーを関連付けます。必要な権限があることを確認します。

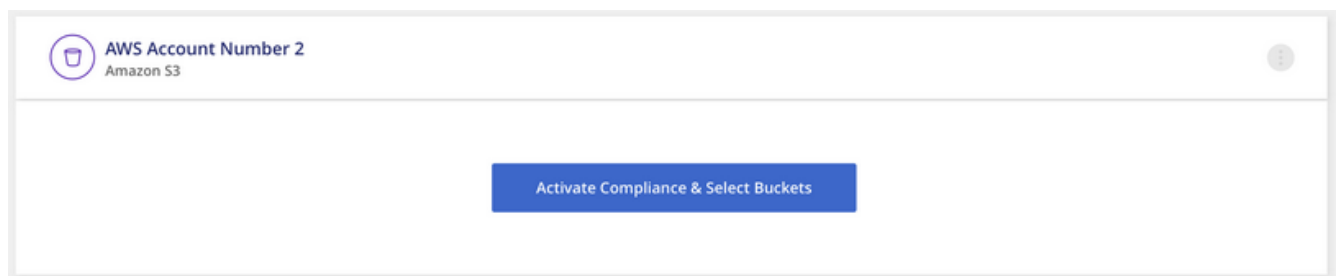
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject",
        "s3:HeadBucket"
      ],
      "Resource": "*"
    }
  ]
}
```

2. Cloud Compliance インスタンスが存在するソース AWS アカウントに移動し、インスタンスに関連付けられている IAM ロールを選択します。
 - a. 最大 CLI / API セッション期間 * を 1 時間から 12 時間に変更し、変更を保存してください。
 - b. [* ポリシーの適用 *] をクリックし、[ポリシーの作成 *] をクリックします。
 - c. 「STS : AssumeRole」アクションと、ターゲットアカウントで作成したロールの ARN を含むポリシーを作成します。


```
{
  "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/*"
      ]
    }
  ]
}
```

Cloud Compliance インスタンスのプロファイルアカウントで追加の AWS アカウントにアクセスできるようになりました。

3. Amazon S3 Scan Configuration * ページに移動し、新しい AWS アカウントが表示されます。Cloud Compliance が新しいアカウントの作業環境を同期し、この情報を表示するまでに数分かかることがあります。



4. [Activate Compliance & Select Buckets] をクリックして、スキャンするバケットを選択します。

Cloud Compliance によって、有効にした新しい S3 バケットのスキャンが開始されます。

データベーススキーマをスキャンしています

Cloud Compliance でデータベーススキーマのスキャンを開始するには、いくつかの手順

を実行します。

クイックスタート

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

データベースの前提条件を確認する

データベースがサポートされていること、およびデータベースへの接続に必要な情報があることを確認します。

Cloud Compliance インスタンスを導入します

"[Cloud Compliance の導入](#)" インスタンスが展開されていない場合。

データベースサーバを追加します

アクセスするデータベースサーバを追加します。

スキーマを選択します

スキャンするスキーマを選択します。

前提条件の確認

Cloud Compliance を有効にする前に、次の前提条件を確認し、サポートされている構成であることを確認してください。

サポートされるデータベース

Cloud Compliance では、次のデータベースからスキーマをスキャンできます。

- MongoDB
- MySQL
- Oracle の場合
- PostgreSQL
- SAP HANA のサポート
- SQL Server (MSSQL)



統計収集機能 * は、データベースで有効にする必要があります *。

データベースの要件

Cloud Compliance インスタンスに接続されたデータベースは、ホストされている場所に関係なくすべてスキャンできます。データベースに接続するには、次の情報が必要です。

- IP アドレスまたはホスト名
- ポート

- サービス名（ Oracle データベースにアクセスする場合のみ）
- スキーマへの読み取りアクセスを許可するクレデンシャル

ユーザー名とパスワードを選択する場合は、スキャンするすべてのスキーマとテーブルに対する完全な読み取り権限を持つユーザーを選択することが重要です。必要なすべての権限を持つ専用のユーザを Cloud Compliance システムに作成することを推奨します。

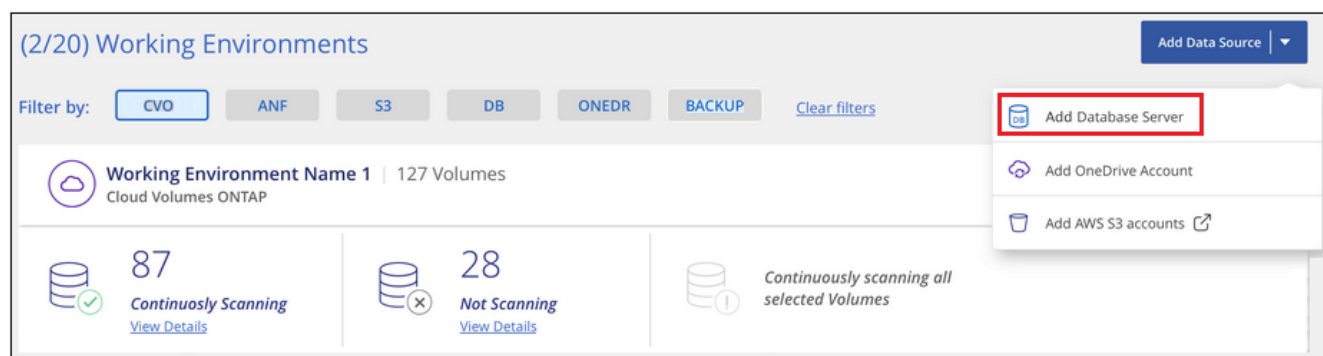
- 注： MongoDB では、読み取り専用の管理者ロールが必要です。

データベースサーバを追加しています

が必要です "[Cloud Manager に Cloud Compliance のインスタンスを導入済みである](#)".

スキーマが存在するデータベース・サーバを追加します。

1. [作業環境の構成] ページで、 [* データソースの追加 > データベースサーバーの追加 *] をクリックします。



2. データベースサーバを識別するために必要な情報を入力します。
 - a. データベースタイプを選択します。
 - b. データベースに接続するポートおよびホスト名または IP アドレスを入力します。
 - c. Oracle データベースの場合は、サービス名を入力します。
 - d. Cloud Compliance がサーバにアクセスできるように、クレデンシャルを入力します。
 - e. [Add DB Server*] をクリックします。

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
<input type="text"/>	<input type="text"/>
Port	Service Name
<input type="text"/>	<input type="text"/>

Credentials

Username	Password
<input type="text"/>	<input type="text"/>

ページのスクリー

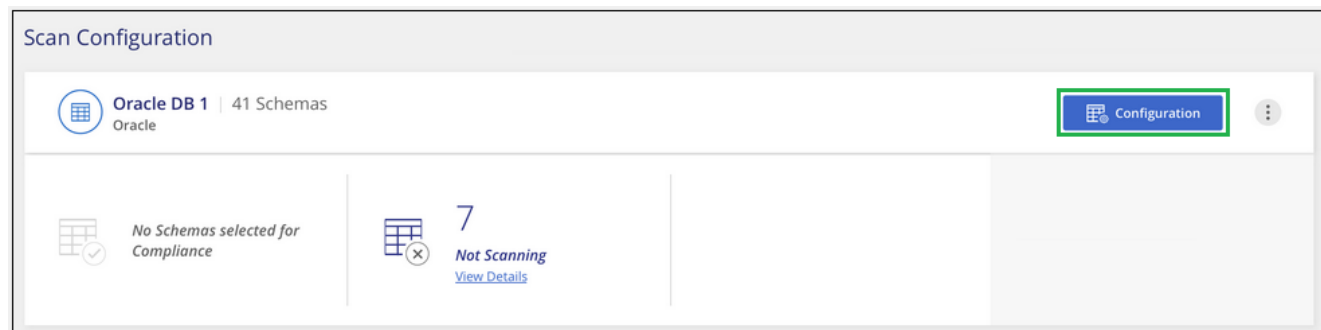
ンショット。"]

データベースが作業環境のリストに追加されます。

データベーススキーマでの準拠スキャンの有効化と無効化

スキーマのスキャンは、いつでも停止または開始できます。

1. _Scan Configuration_page から、設定するデータベースの **Configuration** ボタンをクリックします。



2. スライダを右に移動して、スキャンするスキーマを選択します。

'Working Environment Name' Scan Configuration			
28/28 Schemas selected for compliance scan		<input type="text"/> Edit Credentials	
Compliance	Schema Name	Status	Required Action
<input 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	

ページのスクリーンショット。"]

Cloud Compliance によって、有効にしたデータベーススキーマのスキャンが開始されます。エラーが発生した場合は、エラーを修正するために必要なアクションとともに、[ステータス]列に表示されます。

OneDrive アカウントをスキャンしています

Cloud Compliance を使って OneDrive フォルダ内のファイルのスキャンを開始するには、いくつかの手順を実行します。

クイックスタート

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

OneDrive の前提条件を確認します

OneDrive アカウントにログインするための管理者資格情報があることを確認してください。

Cloud Compliance インスタンスを導入します

"Cloud Compliance の導入" インスタンスが展開されていない場合。

OneDrive アカウントを追加します

Admin ユーザクレデンシャルを使用して、アクセスする OneDrive アカウントにログインし、新しい作業環境として追加します。

ユーザを追加します

スキャンする OneDrive アカウントからユーザーのリストを追加します。一度に最大 100 人のユーザを追加できます。

前提条件の確認

Cloud Compliance を有効にする前に、次の前提条件を確認し、サポートされている構成であることを確認してください。

OneDrive の要件

すべてのユーザファイルに読み取りアクセスを提供する OneDrive for Business アカウントの管理者ログインクレデンシャルが必要です。

OneDrive フォルダをスキャンするすべてのユーザーに対して、電子メールアドレスの行区切りリストが必要です。

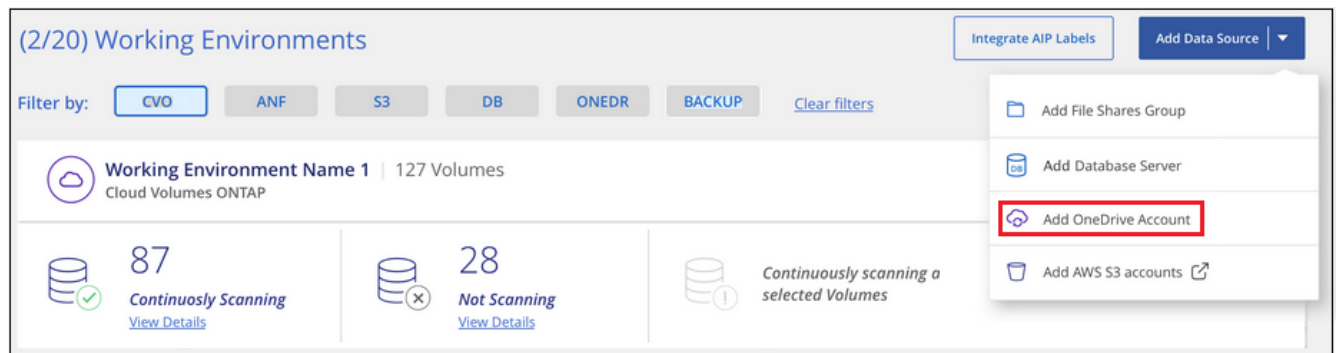
OneDrive アカウントを追加します

が必要です "[Cloud Manager に Cloud Compliance のインスタンスを導入済みである](#)"。

ユーザファイルが存在する OneDrive アカウントを追加します。

手順

1. [作業環境の構成] ページで、[* データソースの追加 >]、[OneDrive アカウントの追加 *] の順にクリックします。



ボタンをクリックできる [スキャン構成] ページのスクリーンショット。"]

2. [OneDrive アカウントの追加] ダイアログで、[* OneDrive にサインイン] をクリックします。
3. 表示される Microsoft ページで、OneDrive アカウントを選択し、必要な管理者ユーザーとパスワードを入力してから、* 同意する * をクリックして、Cloud Compliance がこのアカウントからデータを読み取れることを許可します。

OneDrive アカウントが作業環境の一覧に追加されます。

OneDrive ユーザーをコンプライアンススキャンに追加する

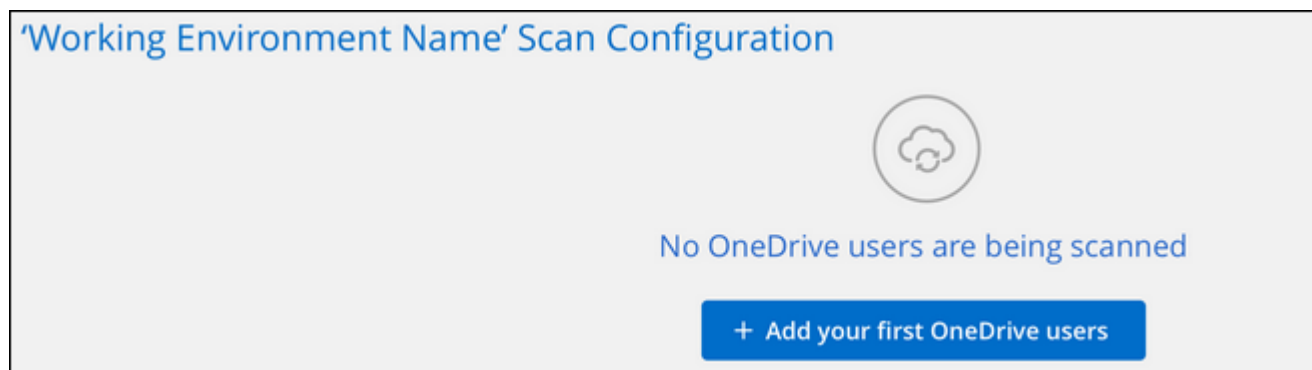
個々の OneDrive ユーザまたはすべての OneDrive ユーザを追加して、ファイルを Cloud Compliance でスキャンすることができます。

手順

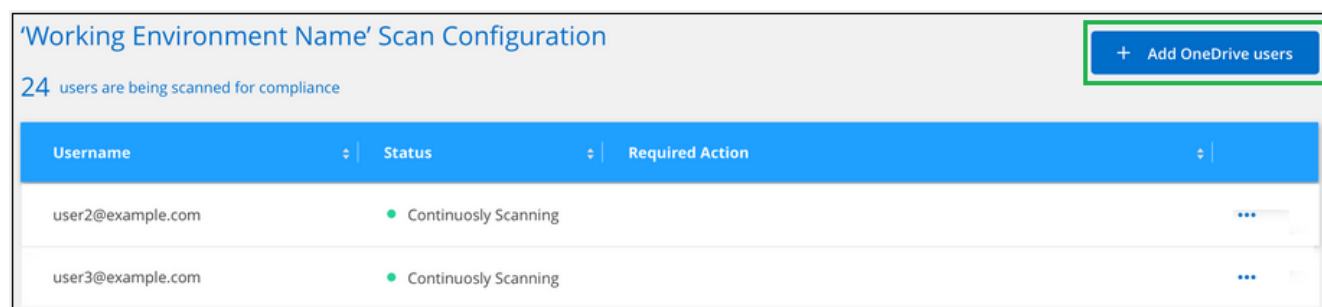
1. [スキャン構成] ページで、OneDrive アカウントの [* 構成 *] ボタンをクリックします。



2. この OneDrive アカウントに初めてユーザーを追加する場合は、[* 最初の OneDrive ユーザーを追加する *] をクリックします。



OneDrive アカウントからユーザーを追加する場合は、[* OneDrive ユーザーの追加 *] をクリックします。



ボタンを示すスクリーンショット。"]

3. ファイルをスキャンするユーザーの電子メールアドレスを 1 行に 1 つ追加し（セッションあたり最大 100 件）、[ユーザーの追加] をクリックします。

Add OneDrive users

Provide a list of OneDrive users for Cloud Compliance to scan their data, line-separated. You can add up to 100 users at a time.

Type or paste below the OneDrive user accounts to add

User Accounts

user@example.com

user@example.com

user@example.com

user@example.com

user@example.com

user@example.com

user@example.com

Add Users

Cancel

ページのスクリーンショット。"]

確認ダイアログに、追加されたユーザの数が表示されます。

ダイアログに追加できなかったユーザが表示される場合は、この情報を記録して問題を解決します。修正した E メールアドレスを使用してユーザを再追加できる場合もあります。

Cloud Compliance によるスキャンが開始され、追加したユーザのファイルがスキャンされます。結果はダッシュボードやその他の場所に表示されます。

OneDrive ユーザーをコンプライアンススキャンから削除します

ユーザが会社から退出した場合や、E メールアドレスが変更された場合、個々の OneDrive ユーザがいつでもファイルをスキャンできないようにすることができます。[構成] ページで [OneDrive ユーザーの削除] をクリックします。

'Working Environment Name' Scan Configuration

+ Add OneDrive users

24 users are being scanned for compliance

Username	Status	Required Action
user1@example.com	Continuously Scanning	<div>Remove OneDrive User</div>

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.