



データソースでスキャンをアクティブ化します Cloud Data Sense

NetApp
April 11, 2022

目次

データソースでスキャンをアクティブ化します	1
Cloud Volumes ONTAP とオンプレミス ONTAP	
向けのクラウドデータサービスの導入を開始する方法をご紹介します	1
Azure NetApp Files 向けクラウドデータセンスの導入を開始する方法をご確認ください	7
Amazon FSX for ONTAP のクラウドデータセンスを今すぐ始めましょう	11
Amazon S3 向けのクラウドデータセンスの導入	16
データベーススキーマをスキャンしています	22
OneDrive アカウントをスキャンしています	26
SharePoint アカウントをスキャンしています	30
ファイル共有をスキャンしています	33
S3 プロトコルを使用するオブジェクトストレージをスキャンしています	37

データソースでスキャンをアクティブ化します

Cloud Volumes ONTAP とオンプレミス ONTAP 向けのクラウドデータサービスの導入を開始する方法をご紹介します

Cloud Data Sense を使用して、Cloud Volumes ONTAP とオンプレミスの ONTAP ボリューム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。

ボリュームをスキャンする前に、Cloud Manager でシステムを作業環境として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"](#)

["クラウドデータの導入センス"](#) インスタンスが展開されていない場合。

[* データセンス *] 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。

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

- クラウドデータセンスインスタンスには、各 Cloud Volumes ONTAP サブネットまたはオンプレミスの 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、データセ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。
- これらのポートが Data Sense 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 ボリュームエクスポートポリシーで、データセンス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、Active Directory クレデンシャルが必要です。

コンプライアンス * > * 構成 * > * 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選択または選択解除すると、Cloud Data Sense で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 で検出されません"](#)。

Cloud Data Sense インスタンスの導入

導入済みのインスタンスがない場合は Cloud Data Sense を導入

インターネット経由でアクセス可能な Cloud Volumes ONTAP およびオンプレミス ONTAP システムをスキャンする場合は、を実行します ["クラウドにクラウドデータセンスを導入"](#) または ["インターネットにアクセスできるオンプレミスの場所"](#)。

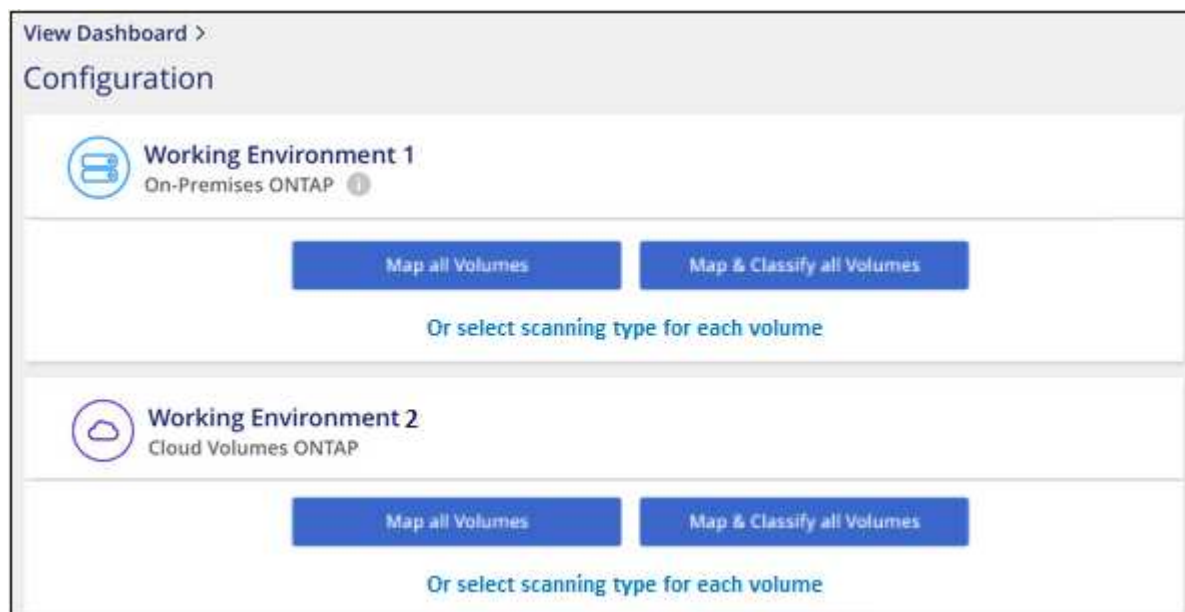
インターネットにアクセスできないデータサイトにインストールされているオンプレミスの ONTAP システムをスキャンする場合は、を実行する必要があります ["クラウドデータセンスは、インターネットにアクセスできないオンプレミス環境に導入できます"](#)。そのため、Cloud Manager Connector をオンプレミスと同じ場所に導入する必要があります。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

作業環境でクラウドデータを有効に活用

クラウドデータセンスは、Cloud Volumes ONTAP システム（AWS、Azure、GCP）とオンプレミスの ONTAP クラスタで有効にすることができます。

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



クリーンショット。"]

タブのス

2. 各作業環境でボリュームをスキャンする方法を選択します。 ["マッピングおよび分類スキャンについて説明します"](#)：

- すべてのボリュームをマップするには、* すべてのボリュームをマップ * をクリックします。
- すべてのボリュームをマップして分類するには、* すべてのボリュームをマップして分類 * をクリックします。
- 各ボリュームのスキャンをカスタマイズするには、「*」をクリックするか、各ボリュームのスキャンタイプを選択してから、マッピングまたは分類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。

3. 確認ダイアログボックスで、[* 承認] をクリックして、ボリュームのスキャンを開始するデータセンスを設定します。

Cloud Data Sense により、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 Data Sense が最初のスキャンを完了するとすぐに Compliance ダッシュボードに表示されます。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 Data Sense がボリュームにアクセスできることの確認

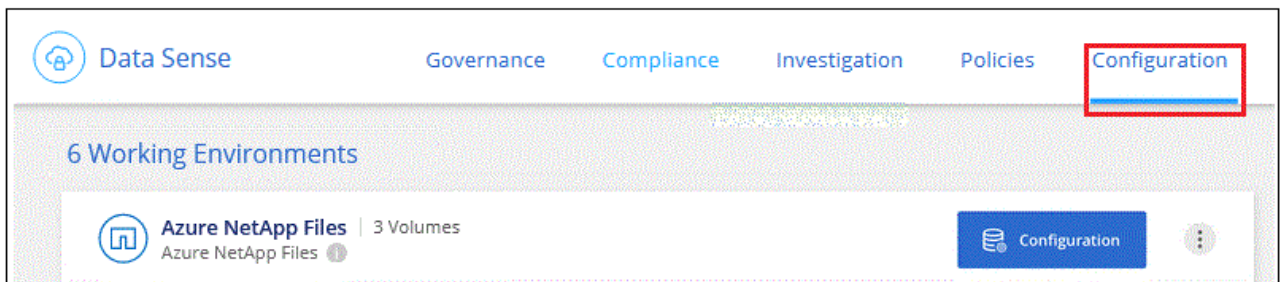
ネットワーク、セキュリティグループ、およびエクスポートポリシーを確認して、Cloud Data Sense でボリュームにアクセスできることを確認します。CIFS ボリュームにアクセスできるようにするには、CIFS クレデンシャルをデータセン스에指定する必要があります。

手順

1. クラウドデータセンスインスタンスと、Cloud Volumes ONTAP 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。
2. Cloud Volumes ONTAP のセキュリティグループがデータセ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ます。

データセンスインスタンスの 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. 次のポートがデータセンス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、各ボリュームのデータにアクセスできるように Data sense インスタンスの IP アドレスが含まれていることを確認します。
5. CIFS を使用する場合は、CIFS ボリュームをスキャンできるように、Active Directory クレデンシャルを使用したデータセンスを設定します。
 - a. Cloud Manager の上部で、* Data Sense * をクリックします。
 - b. [* 構成 *] タブをクリックします。

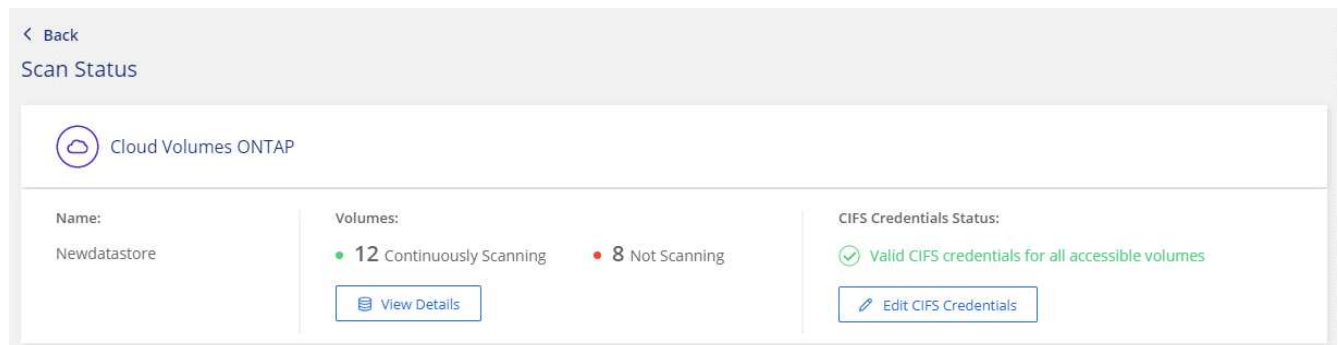


ボタンを示す [遵守] タブのスクリーンショット。"]

- c. 各作業環境について、* CIFS 資格情報の編集 * をクリックし、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。

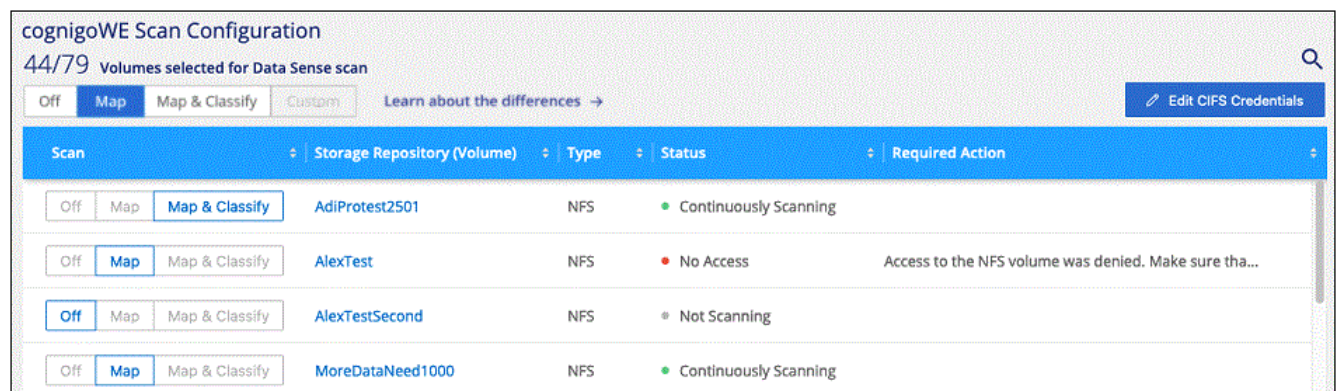
クレデンシャルは読み取り専用ですが、管理者のクレデンシャルを指定することで、データセンスは昇格された権限が必要なデータを読み取ることができます。クレデンシャルは Cloud Data Sense インスタンスに保存されます。

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。



6. _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 4 つのボリュームを示しています。1 つは、データセンス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クラウドデータセンスでスキャンできないボリュームです。



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

設定ページからは、作業環境でマッピング専用スキャンまたはマッピングおよび分類スキャンをいつでも開始

または停止できます。マッピングのみのスキャンからマッピングおよび分類スキャンに変更することもできます。また、マッピングのみのスキャンからマッピングおよび分類スキャンに変更することもできます。すべてのボリュームをスキャンすることを推奨します。

cognigoWE Scan Configuration						
44/79 Volumes selected for Data Sense scan						
<div> Off Map Map & Classify Custom Learn about the differences → Edit CIFS Credentials </div>						
Scan	Storage Repository (Volume)	Type	Status	Required Action		
Off Map Map & Classify	AdiNFSVol_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...		
Off Map Map & Classify	AdiProtest2501	NFS	Continuously Scanning			
Off Map Map & Classify	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...		
Off Map Map & Classify	AlexTestSecond	NFS	Not Scanning			
Off Map Map & Classify	MoreDataNeed1000	NFS	Continuously Scanning			

終了：	手順：
ボリュームに対してマッピングのみのスキャンを有効にします	ボリューム領域で、* マップ * をクリックします
ボリュームでフルスキャンを有効にします	ボリューム領域で、* マップと分類 * をクリックします
ボリュームのスキャンを無効にします	ボリューム領域で、* オフ * をクリックします
すべてのボリュームでマッピングのみのスキャンを有効にします	見出し領域で、* マップ * をクリックします
すべてのボリュームでフルスキャンを有効にします	見出し領域で、* マップと分類 * をクリックします
すべてのボリュームでスキャンを無効にします	見出し領域で、* Off * をクリックします



作業環境に追加された新しいボリュームは、見出し領域で * Map * または * Map & Classify * の設定を行った場合にのみ自動的にスキャンされます。見出し領域で * Custom * または * Off * に設定すると、作業環境に追加する新しいボリュームごとに、マッピングまたはフルスキャンを有効にする必要があります。

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、クラウドデータセンスで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 *。

'Working Environment Name' Configuration

22/28 Volumes selected for compliance scan

Enable Access to DP Volumes [Edit CIFS Credentials](#)

Off **Map** Map & Classify Custom [Learn about the differences](#) →

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

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 * 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 Data Sense で CIFS ボリュームをスキャンするためにすでに Active Directory の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できます。また、別の管理クレデンシャルを指定することもできます。

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 Data Sense. The shares' export policies will allow access only from the Cloud Data Sense instance. [Learn More](#)

Enable Access to DP Volumes Cancel

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 Data Sense. The shares' export policies will allow access only from the Cloud Data Sense instance. [Learn More](#)

Enable Access to DP Volumes Cancel

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](#)。

有効にすると、スキャン対象としてアクティブ化された各 DP ボリュームから NFS 共有が作成されます。共有エクスポートポリシーでは、データセンス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い場合は、あとで追加しても、CIFS DP の有効化ボタン * が設定ページの上部に表示されます。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。



Active Directory クレデンシャルは、最初の CIFS DP ボリュームの Storage VM にのみ登録されているため、その SVM 上のすべての DP ボリュームがスキャンされます。他の SVM 上のボリュームには Active Directory クレデンシャルが登録されないため、これらの DP ボリュームはスキャンされません。

Azure NetApp Files 向けクラウドデータセンスの導入を開始する方法をご確認ください

Azure NetApp Files 向けクラウドデータセンス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。

Azure NetApp Files ボリュームをスキャンする前に、["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 Manager に Cloud Data Sense を導入"](#) インスタンスが展開されていない場合。

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。

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

- クラウドデータセンスインスタンスには、各 Azure NetApp Files サブネットへのネットワーク接続が必要です。
- これらのポートが Data Sense 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 ボリュームエクスポートポリシーで、データセンス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、Active Directory クレデンシャルが必要です。

コンプライアンス * > * 構成 * > * 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選択または選択解除すると、Cloud Data Sense でスキャンが開始または停止します。

スキャンする Azure NetApp Files システムを検出しています

スキャンする Azure NetApp Files システムがまだ作業環境として Cloud Manager にはない場合は、この時点でキャンバスに追加できます。

["Cloud Manager で Azure NetApp Files システムを検出する方法をご覧ください"](#)。

Cloud Data Sense インスタンスの導入

["クラウドデータの導入センス"](#) インスタンスが展開されていない場合。

Azure NetApp Files ボリュームをスキャンするときは、データセンスをクラウドに導入する必要があります。また、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。

- ・注：* オンプレミスの場所にクラウドデータセンスを導入することは、Azure NetApp Files ボリュームのスキャンでは現在サポートされていません。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

作業環境でクラウドデータを有効に活用

Azure NetApp Files ボリュームでクラウドデータセンスを有効にすることができます。

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



タブのスク

リーンショット。"]

2. 各作業環境でボリュームをスキャンする方法を選択します。"[マッピングおよび分類スキャンについて説明します](#)"：
 - すべてのボリュームをマップするには、* すべてのボリュームをマップ * をクリックします。
 - すべてのボリュームをマップして分類するには、* すべてのボリュームをマップして分類 * をクリックします。
 - 各ボリュームのスキャンをカスタマイズするには、「*」をクリックするか、各ボリュームのスキャンタイプを選択してから、マッピングまたは分類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。

3. 確認ダイアログボックスで、[* 承認] をクリックして、ボリュームのスキャンを開始するデータセンスを設定します。

Cloud Data Sense により、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 Data Sense が最初のスキャンを完了するとすぐに Compliance ダッシュボードに表示されます。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 Data Sense 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 Data Sense で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、CIFS クレデンシャルをデータセン스에指定する必要があります。

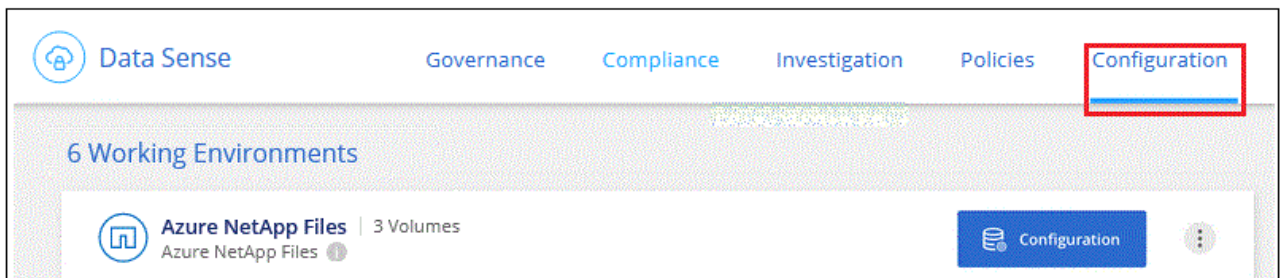
手順

1. クラウドデータセンシブインスタンスと、Azure NetApp Files 用のボリュームを含む各ネットワーク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 Data Sense 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. 次のポートがデータセンシブ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
3. NFS ボリュームのエクスポートポリシーに、各ボリュームのデータにアクセスできるように Data sense インスタンスの IP アドレスが含まれていることを確認します。
4. CIFS を使用する場合は、CIFS ボリュームをスキャンできるように、Active Directory クレデンシャルを使用したデータセンシブを設定します。
 - a. Cloud Manager の上部で、* Data Sense * をクリックします。
 - b. [* 構成 *] タブをクリックします。

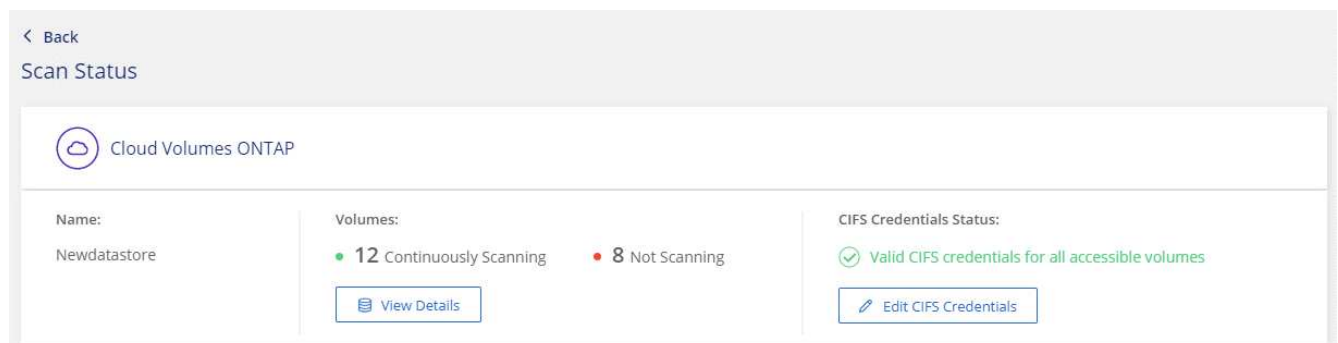


ボタンを示す [遵守] タブのスクリーンショット。"]

- c. 各作業環境について、* CIFS 資格情報の編集 * をクリックし、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、データセンシブ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 Data Sense 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。



5. 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 4 つのボリュームを示しています。1 つは、データセンシブ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クラウドデータセンスでスキャンできないボリュームです。

cognitoWE Scan Configuration				
44/79 Volumes selected for Data Sense scan				
<div>OffMapMap & ClassifyCustom</div> <div>Learn about the differences →</div> <div>Edit CIFS Credentials</div>				
Scan	Storage Repository (Volume)	Type	Status	Required Action
OffMapMap & Classify	AdiProtest2501	NFS	Continuously Scanning	
OffMapMap & Classify	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
OffMapMap & Classify	AlexTestSecond	NFS	Not Scanning	
OffMapMap & Classify	MoreDataNeed1000	NFS	Continuously Scanning	

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

設定ページからは、作業環境でマッピング専用スキャンまたはマッピングおよび分類スキャンをいつでも開始または停止できます。マッピングのみのスキャンからマッピングおよび分類スキャンに変更することもできます。また、マッピングのみのスキャンからマッピングおよび分類スキャンに変更することもできます。すべてのボリュームをスキャンすることを推奨します。

cognitoWE Scan Configuration				
44/79 Volumes selected for Data Sense scan				
<div>OffMapMap & ClassifyCustom</div> <div>Learn about the differences →</div> <div>Edit CIFS Credentials</div>				
Scan	Storage Repository (Volume)	Type	Status	Required Action
OffMapMap & Classify	AdiNFSVol_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
OffMapMap & Classify	AdiProtest2501	NFS	Continuously Scanning	
OffMapMap & Classify	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
OffMapMap & Classify	AlexTestSecond	NFS	Not Scanning	
OffMapMap & Classify	MoreDataNeed1000	NFS	Continuously Scanning	

終了：	手順：
ボリュームに対してマッピングのみのスキャンを有効にします	ボリューム領域で、 * マップ * をクリックします
ボリュームでフルスキャンを有効にします	ボリューム領域で、 * マップと分類 * をクリックします
ボリュームのスキャンを無効にします	ボリューム領域で、 * オフ * をクリックします
すべてのボリュームでマッピングのみのスキャンを有効にします	見出し領域で、 * マップ * をクリックします
すべてのボリュームでフルスキャンを有効にします	見出し領域で、 * マップと分類 * をクリックします
すべてのボリュームでスキャンを無効にします	見出し領域で、 * Off * をクリックします



作業環境に追加された新しいボリュームは、見出し領域で * Map * または * Map & Classify * の設定を行った場合にのみ自動的にスキャンされます。見出し領域で * Custom * または * Off * に設定すると、作業環境に追加する新しいボリュームごとに、マッピングまたはフルスキャンを有効にする必要があります。

Amazon FSX for ONTAP のクラウドデータセンスを今すぐ始めましょう

クラウドデータセンスを使用した Amazon FSX for ONTAP ボリューム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。

作業を開始する前に

- データセンスを導入および管理するには、AWS にアクティブなコネクタが必要です。
- 作業環境の作成時に選択したセキュリティグループは、Cloud Data Sense インスタンスからのトラフィックを許可する必要があります。関連付けられたセキュリティグループは、FSX for ONTAP ファイルシステムに接続されている ENI を使用して検索し、AWS 管理コンソールを使用して編集できます。

"Linux インスタンス用の AWS セキュリティグループ"

"Windows インスタンス用の AWS セキュリティグループ"

"AWS Elastic Network Interface (ENI) "

クイックスタート

以下の手順を実行してすぐに作業を開始するか、下にスクロールして詳細を確認してください。

FSX で ONTAP ボリュームをスキャンする前に、**"ボリュームが設定された FSX 作業環境が必要です"**。

"Cloud Manager に Cloud Data Sense を導入" インスタンスが展開されていない場合。

[* データセンス *] 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。

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

- クラウドデータセンスインスタンスには、ONTAP サブネットの各 FSX へのネットワーク接続が必要です。
- 次のポートがデータセンス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 ボリュームエクスポートポリシーで、データセンス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、Active Directory クレデンシャルが必要です。+ コンプライアンス * > * 構成 * > * 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選択または選択解除すると、Cloud Data Sense でスキャンが開始または停止します。

スキャンする **ONTAP** ファイルシステムの **FSX** を検出します

スキャンする FSX for ONTAP ファイルシステムが作業環境としてまだ Cloud Manager にはない場合は、この時点でキャンバスに追加できます。

"Cloud Manager で ONTAP ファイルシステムの FSX を検出または作成する方法については、[を参照してください](#)。"

Cloud Data Sense インスタンスの導入

"クラウドデータの導入センス" インスタンスが展開されていない場合。

Connector for AWS とスキャン対象の FSX ボリュームと同じ AWS ネットワークに Data Sense を導入する必要があります。

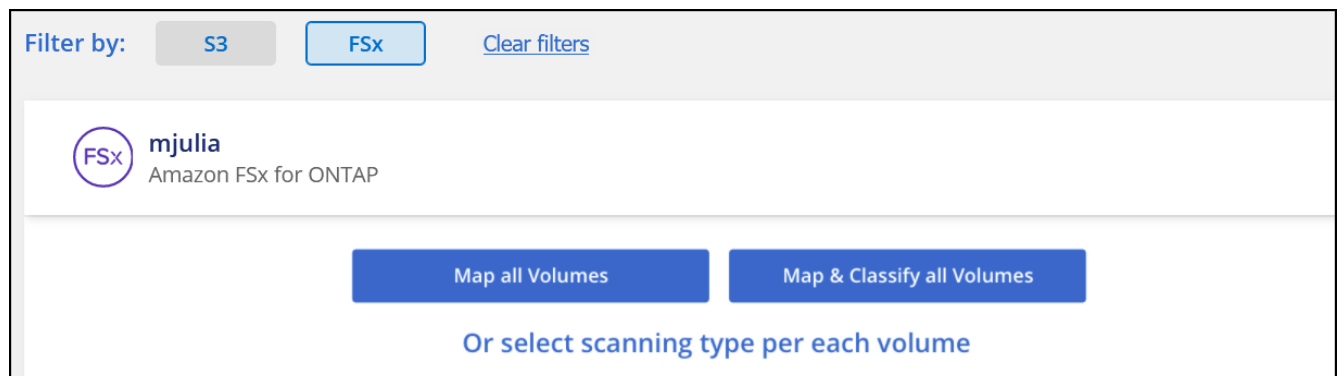
- ・注：* オンプレミスの場所にクラウドデータセンスを導入することは、現在 FSX ボリュームのスキャンではサポートされていません。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

作業環境でクラウドデータを有効に活用

ONTAP ボリュームの FSX に対してクラウドデータセンスを有効にすることができます。

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



タブのスクリーンショット。"]

2. 各作業環境でボリュームをスキャンする方法を選択します。"[マッピングおよび分類スキャンについて説明します](#)"：
 - すべてのボリュームをマップするには、* すべてのボリュームをマップ * をクリックします。
 - すべてのボリュームをマップして分類するには、* すべてのボリュームをマップして分類 * をクリックします。
 - 各ボリュームのスキャンをカスタマイズするには、「*」をクリックするか、各ボリュームのスキャンタイプを選択してから、マッピングまたは分類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。

3. 確認ダイアログボックスで、[* 承認] をクリックして、ボリュームのスキャンを開始するデータセンスを設定します。

Cloud Data Sense により、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 Data Sense が最初のスキャンを完了するとすぐに Compliance ダッシュボードに表示されます。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 Data Sense 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 Data Sense で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、CIFS クレデンシャルをデータセン스에指定する必要があります。

手順

1. _Configuration_page で、**View Details** をクリックして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、データセンス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、ボリュームの Cloud Data Sense によるスキャンができないことを示しています。

Scan	Storage Repository (Volume)	Type	Status	Required Action
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	jrmclone	NFS	● No Access	Check network connectivity between the Data Sense ...

2. クラウドデータセンスインスタンスと各ネットワークの間に、FSX for ONTAP のボリュームを含むネットワーク接続があることを確認します。



FSX for ONTAP の場合、Cloud Data Sense は Cloud Manager と同じリージョンのボリュームのみをスキャンできます。

3. 次のポートがデータセンス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 Data Sense 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、CIFS ボリュームをスキャンできるように、Active Directory クレデンシャルを使用したデータセンスを設定します。
 - a. Cloud Manager の上部で、* Data Sense * をクリックします。
 - b. [* 構成 *] タブをクリックします。
 - c. 各作業環境について、* CIFS 資格情報の編集 * をクリックし、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、データセンス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 Data Sense 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。

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

設定ページからは、作業環境でマッピング専用スキャンまたはマッピングおよび分類スキャンをいつでも開始または停止できます。マッピングのみのスキャンからマッピングおよび分類スキャンに変更することもできます。また、マッピングのみのスキャンからマッピングおよび分類スキャンに変更することもできます。すべてのボリュームをスキャンすることを推奨します。

cognigoWE Scan Configuration						
44/79 Volumes selected for Data Sense scan						
<div>Off Map Map & Classify Custom Learn about the differences → Edit CIFS Credentials</div>						
Scan	Storage Repository (Volume)	Type	Status	Required Action		
Off Map Map & Classify	AdiNFSVol_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...		
Off Map Map & Classify	AdiProtest2501	NFS	Continuously Scanning			
Off Map Map & Classify	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...		
Off Map Map & Classify	AlexTestSecond	NFS	Not Scanning			
Off Map Map & Classify	MoreDataNeed1000	NFS	Continuously Scanning			

終了：	手順：
ボリュームに対してマッピングのみのスキャンを有効にします	ボリューム領域で、* マップ * をクリックします
ボリュームでフルスキャンを有効にします	ボリューム領域で、* マップと分類 * をクリックします
ボリュームのスキャンを無効にします	ボリューム領域で、* オフ * をクリックします
すべてのボリュームでマッピングのみのスキャンを有効にします	見出し領域で、* マップ * をクリックします
すべてのボリュームでフルスキャンを有効にします	見出し領域で、* マップと分類 * をクリックします
すべてのボリュームでスキャンを無効にします	見出し領域で、* Off * をクリックします



作業環境に追加された新しいボリュームは、見出し領域で * Map * または * Map & Classify * の設定を行った場合にのみ自動的にスキャンされます。見出し領域で * Custom * または * Off * に設定すると、作業環境に追加する新しいボリュームごとに、マッピングまたはフルスキャンを有効にする必要があります。

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、クラウドデータセンスでアクセスできないため、スキャンされません。これは、ONTAP ファイルシステムの FSX 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 *。

Scan	Storage Repository (Volume)	Type	Status	Required Action
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	VolumeName1	DP	Not Scanning	Enable access to DP Volumes ⓘ
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	VolumeName2	NFS	Continuously Scanning	
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map & Classify"/>	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 * 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。
 - ONTAP ファイルシステムのソース FSX で NFS ボリュームとして最初に作成されたボリュームが有効になります。
 - ONTAP ファイルシステム用のソース FSX で CIFS ボリュームとして最初に作成されたボリュームでは、これらの 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 Data Sense で CIFS ボリュームをスキャンするためにすでに Active Directory の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できます。また、別の管理クレデンシャルを指定することもできます。

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 Data Sense. The shares' export policies will allow access only from the Cloud Data Sense 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 Data Sense. The shares' export policies will allow access only from the Cloud Data Sense 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。**

有効にすると、スキャン対象としてアクティブ化された各 DP ボリュームから NFS 共有が作成されます。共有エクスポートポリシーでは、データセンシブ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い場合は、あとで追加しても、CIFS DP の有効化ボタン * が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。



Active Directory クレデンシャルは、最初の CIFS DP ボリュームの Storage VM にのみ登録されているため、その SVM 上のすべての DP ボリュームがスキャンされます。他の SVM 上のボリュームには Active Directory クレデンシャルが登録されないため、これらの DP ボリュームはスキャンされません。

Amazon S3 向けのクラウドデータセンスの導入

Cloud Data Sense 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することができます。Cloud Data Sense は、NetApp 解決策用に作成されたバケット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。

IAM ロールの準備やデータセンスから S3 への接続の設定など、クラウド環境がクラウドデータセンスの要件を満たしていることを確認します。 [すべてのリストを参照してください](#)。

"クラウドデータの導入センス" インスタンスが展開されていない場合。

Amazon S3 作業環境を選択し、* Enable * 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すると、Cloud Data Sense によって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 Data Sense インスタンス用の IAM ロールを設定する

Cloud Data Sense では、アカウント内の S3 バケットに接続してスキャンするための権限が必要です。以下の権限を含む IAM ロールを設定します。Amazon S3 作業環境でデータの意味を有効にすると、Cloud Manager から IAM ロールを選択するよう求められます。

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

Cloud Data Sense から Amazon S3 への接続を提供する

Cloud Data Sense は Amazon S3 への接続を必要としている。この接続を確立する最善の方法は、VPC エンドポイントを介して S3 サービスに接続することです。手順については、を参照してください ["AWS のドキュメント：「Creating a Gateway Endpoint」](#)。

VPC エンドポイントを作成するときは、Cloud Data Sense 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、データセンスで 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 Data Sense インスタンスの導入

"Cloud Manager に Cloud Data Sense を導入" インスタンスが展開されていない場合。

AWS に導入されているコネクタを使用してインスタンスを導入する必要があります。これにより、Cloud Manager はこの AWS アカウント内の S3 バケットを自動的に検出し、Amazon S3 作業環境に表示します。

- ・注：* クラウドデータセンスをオンプレミスの場所に導入することは、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。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

S3 作業環境でのデータセンスのアクティブ化

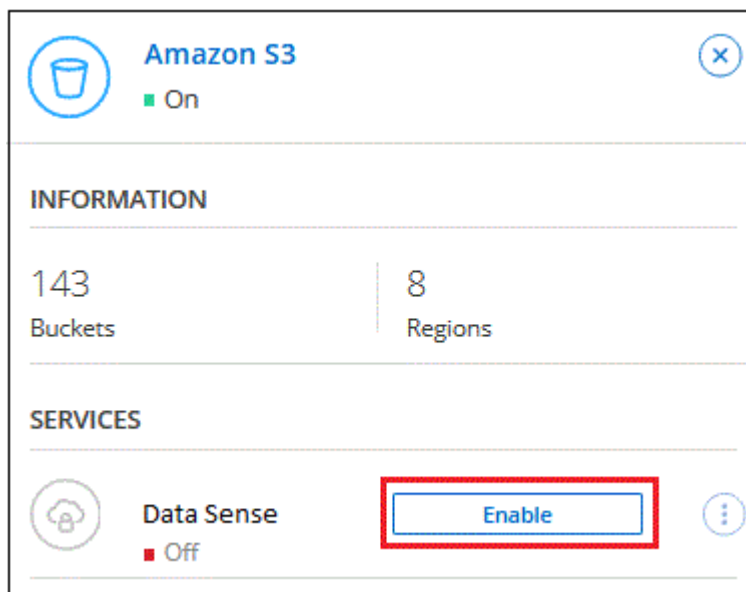
前提条件を確認したら、Amazon S3 で Cloud Data Sense を有効にします。

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 [データセンス] ペインで、[Enable] をクリックします。



4. プロンプトが表示されたら、を持つ Cloud Data Sense 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 Data Sense

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

Select IAM Role

occm

VPC Endpoint for Amazon S3 Required

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

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

Free for the 1st TB


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

Enable

Cancel

5. **[Enable]** 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 Configuration ページでをクリックします  ボタンを押して、[データセンスを活動化（Activate Data Sense）] を選択

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 が Amazon S3 で Cloud Data Sense を有効にしたら、次の手順でスキャンするバケットを設定します。

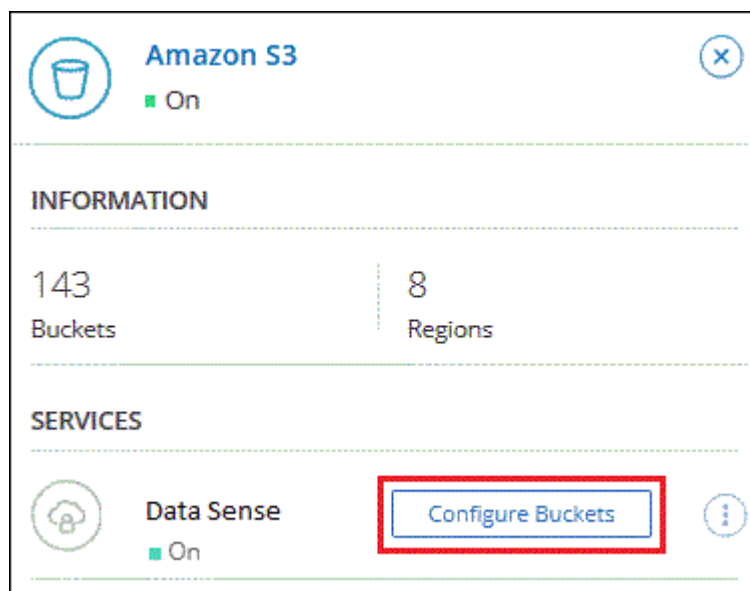
スキャンする S3 バケットを含む AWS アカウントで Cloud Manager を実行している場合は、そのバケットが検出され、Amazon S3 作業環境に表示されます。

クラウドデータセンスも可能です [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. バケットでマッピング専用スキャン、またはマッピングスキャンと分類スキャンを有効にします。

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

終了：	手順：
バケットでマッピングのみのスキャンを有効にする	[* マップ *] をクリックします
バケットでフルスキャンを有効にします	[マップと分類 *] をクリックします
バケットに対するスキャンを無効にする	[* Off *] をクリックします

Cloud Data Sense は、有効にした S3 バケットのスキャンを開始します。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既存の Cloud Data Sense インスタンスにアクセスするロールを割り当てます。

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 Data Sense 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。
- クラウドデータセンス 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"
      ],
      "Resource": "*"
    }
  ]
}
```

2. データセンス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」アクションを含むポリシーを作成し、ターゲットアカウントで作成したロールの ARN を指定します。

```
{
  "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 Data Sense インスタンスプロファイルアカウントが追加の 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 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 Data Sense 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場合があります。



4. [Activate Data Sense & 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 Data Sense は、有効にした新しい S3 バケットのスキャンを開始します。

データベーススキーマをスキャンしています

Cloud Data Sense 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。

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。

"クラウドデータの導入センス" インスタンスが展開されていない場合。

アクセスするデータベースサーバを追加します。

スキャンするスキーマを選択します。

前提条件の確認

Cloud Data Sense 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ます。

サポートされるデータベース

Cloud Data Sense 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。

- Amazon リレーショナルデータベースサービス（Amazon RDS）
- 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 Data Sense インスタンスに接続されているデータベースは、どこでホストしているかに関係なく、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クラウドデータセンスシステム専用のユーザを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。

Cloud Data Sense インスタンスの導入

導入済みのインスタンスがない場合は Cloud Data Sense を導入

インターネット経由でアクセス可能なデータベーススキーマをスキャンする場合は、を実行します ["クラウドにクラウドデータセンスを導入"](#) または ["インターネットにアクセス可能なオンプレミスの場所にデータセンスを導入"](#)。

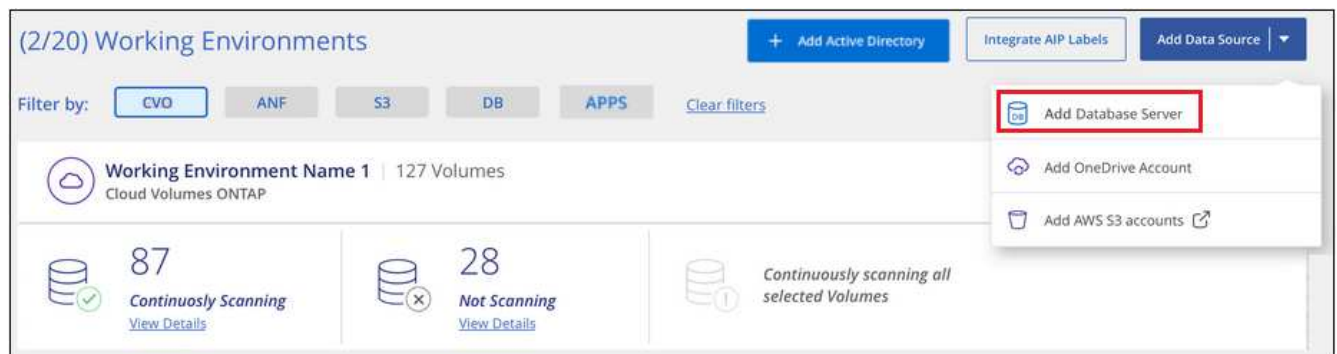
インターネットにアクセスできないダークサイトにインストールされているデータベーススキーマをスキャンする場合は、が必要です ["クラウドデータセンスは、インターネットにアクセスできないオンプレミス環境に導入できます"](#)。そのため、 Cloud Manager Connector をオンプレミスと同じ場所に導入する必要があります。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

データベースサーバを追加しています

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 Data Sense 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

Port

Service Name

Credentials

Username

Password

Add DB Server **Cancel**

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

スキーマのフルスキャンは、いつでも停止または開始できます。



データベーススキーマに対してマッピングのみのスキャンを選択するオプションはありません。

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

Configuration

Oracle DB 1 | 41 Schemas
Oracle

Configuration

No Schemas selected for Compliance

7
Not Scanning
[View Details](#)

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' Configuration			
28/28 Schemas selected for compliance scan		<input type="text"/> Edit Credentials	
Scan	Schema Name	Status	Required Action
<input type="checkbox"/>	DB1 - SchemaName1	Not Scanning	Add Credentials ⓘ
<input type="checkbox"/>	DB1 - SchemaName2	Continuously Scanning	
<input type="checkbox"/>	DB1 - SchemaName3	Continuously Scanning	
<input type="checkbox"/>	DB1 - SchemaName4	Continuously Scanning	

ページのスクリーンショット。"]

Cloud Data Sense は、有効にしたデータベーススキーマのスキャンを開始します。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

いくつかの手順を実行して、クラウドデータセンスを使用した OneDrive フォルダのファイルのスキャンを開始します。

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。

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。

"クラウドデータの導入センス" インスタンスが展開されていない場合。

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。

スキャンするユーザのリストを OneDrive アカウントから追加し、スキャンのタイプを選択します。一度に最大 100 人のユーザを追加できます。

OneDrive の要件を確認する

Cloud Data Sense 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ます。

- 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。

Cloud Data Sense インスタンスの導入

導入済みのインスタンスがない場合は Cloud Data Sense を導入

データセンスは、のいずれかです ["クラウドに導入"](#) または ["インターネットにアクセスできるオンプレミスの場所"](#)。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

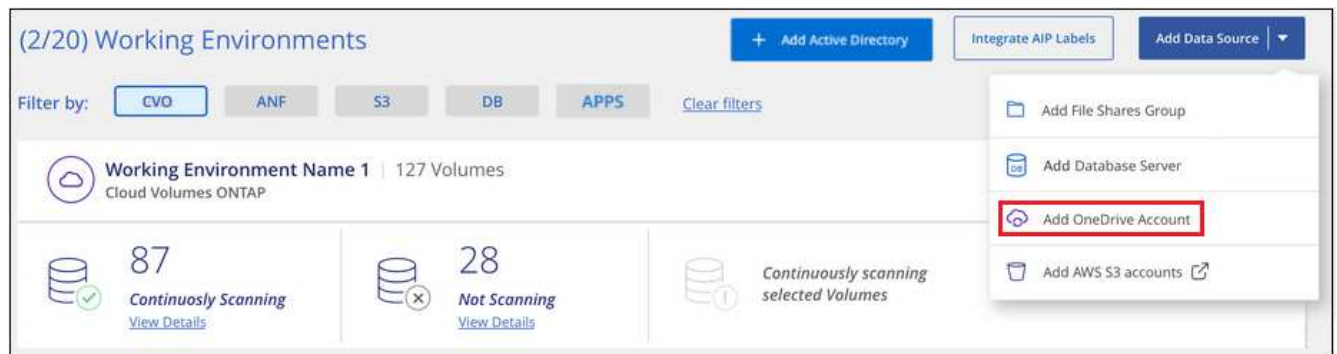
データセンスは、の場合もあります ["インターネットにアクセスできないオンプレミスの場所に導入されている"](#)。ただし、ローカルの OneDrive ファイルをスキャンするには、いくつかの一部のエンドポイントへのインターネットアクセスを提供する必要があります。 ["必要なエンドポイントのリストを参照してください"](#)。

OneDrive アカウントを追加します

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、[Accept] をクリックして、Cloud Data Sense がこのアカウントからデータを読み取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 ユーザーまたはすべての OneDrive ユーザーを追加して、ファイルを Cloud Data Sense でスキャンすることができます。

手順

1. [Configuration] 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。



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。

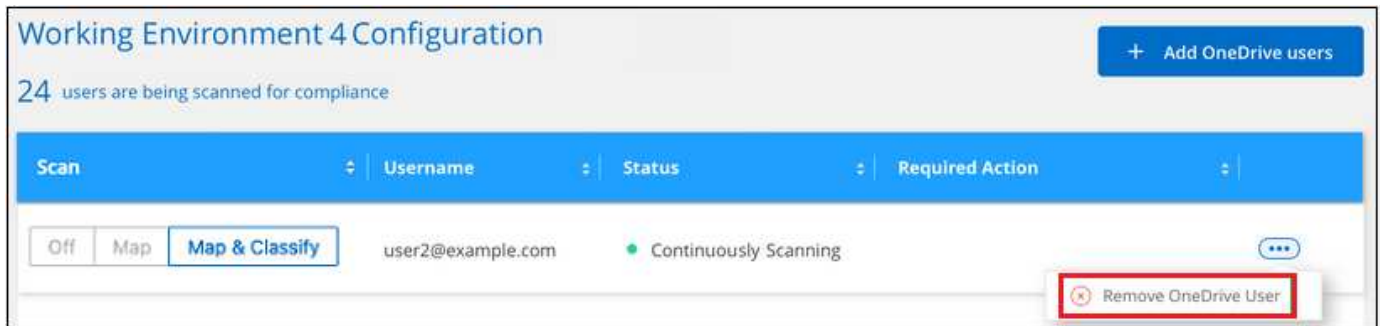
4. ユーザファイルに対して、マッピング専用スキャン、またはマッピングおよび分類スキャンをイネーブルにします。

終了：	手順：
ユーザファイルに対してマッピングのみのスキャンを有効にします	[* マップ *] をクリックします
ユーザファイルのフルスキャンを有効にします	[マップと分類 *] をクリックします
ユーザファイルのスキャンを無効にします	[* Off *] をクリックします

Cloud Data Sense によって、追加したユーザのファイルのスキャンが開始され、その結果が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。



SharePoint アカウントをスキャンしています

Cloud Data Sense を使用して、SharePoint アカウント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。

SharePoint アカウントにログインするための管理者資格情報があり、スキャンする SharePoint サイトの URL があることを確認します。

"クラウドデータの導入センス" インスタンスが展開されていない場合。

管理者ユーザーの資格情報を使用して、アクセスする SharePoint アカウントにログインし、新しいデータソース / 作業環境として追加します。

SharePoint アカウントでスキャンする SharePoint サイト URL のリストを追加し、スキャンの種類を選択します。一度に最大 100 個の URL を追加できます。

SharePoint の要件を確認する

以下の前提条件を確認して、SharePoint アカウントで Cloud Data Sense を有効にする準備ができていることを確認します。

- すべての SharePoint サイトへの読み取りアクセスを提供する SharePoint 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。
- スキャンするすべてのデータについて、SharePoint サイトの URL の行区切りリストが必要です。

Cloud Data Sense インスタンスの導入

導入済みのインスタンスがない場合は Cloud Data Sense を導入

データセンスは、のいずれかです "クラウドに導入" または "インターネットにアクセスできるオンプレミスの場所"。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

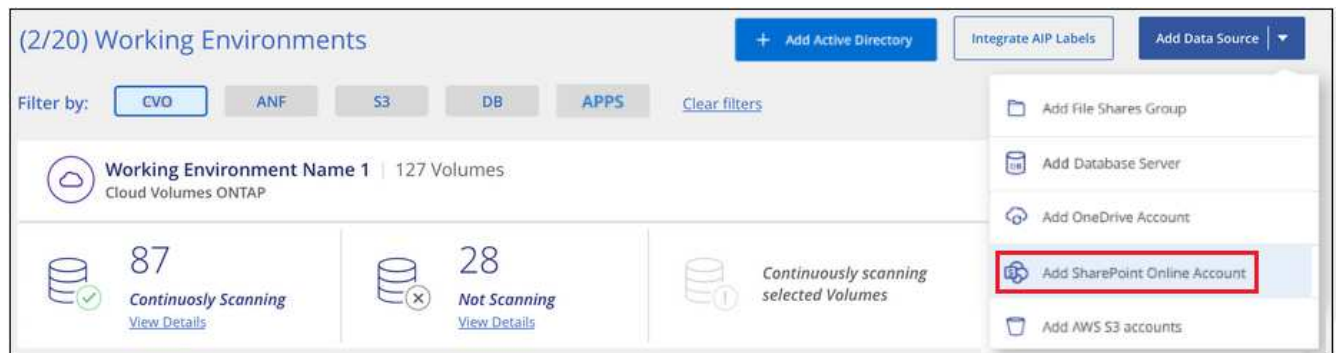
データセンシティブなデータは、の場合もあります "インターネットにアクセスできないオンプレミスの場所に導入されている"。ただし、ローカルの SharePoint ファイルをスキャンするには、いくつかの選択したエンドポイントへのインターネットアクセスを提供する必要があります。"必要なエンドポイントのリストを参照してください"。

SharePoint アカウントを追加しています

ユーザーファイルが存在する SharePoint 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 > SharePoint Online アカウントの追加 *] をクリックします。



ページのスクリーンショット。"]

2. [SharePoint Online アカウントの追加] ダイアログで、[* SharePoint にサインインする *] をクリックします。
3. 表示される Microsoft ページで、SharePoint 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、*Accept * をクリックして Cloud Data Sense 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。

SharePoint アカウントが作業環境のリストに追加されます。

SharePoint サイトをコンプライアンススキャンに追加する

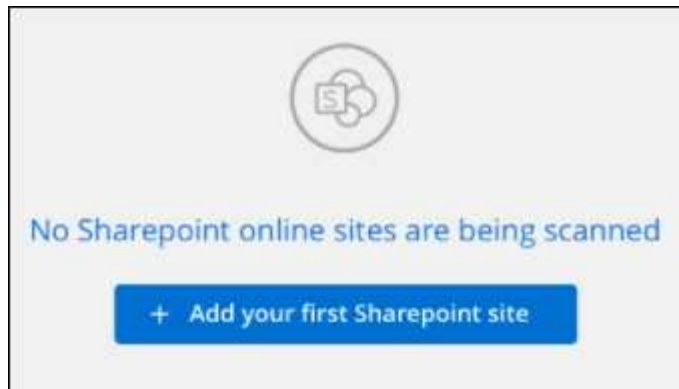
個々の SharePoint サイト、またはアカウント内のすべての SharePoint サイトを追加して、関連するファイルが Cloud Data Sense によってスキャンされるようにすることができます。

手順

1. [Configuration] ページで、SharePoint アカウントの [Configuration] ボタンをクリックします。



2. この SharePoint アカウントのサイトを初めて追加する場合は、[* 最初の SharePoint サイトを追加する *] をクリックします。



ボタンを示すスクリーンショット。"]

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



3. スキャンするファイルがあるサイトの URL を 1 行に 1 つ追加し（セッションあたり最大 100 URL ）、[サイトの追加] をクリックします。

 A screenshot of a dialog box titled "Add Sharepoint Online Sites". The text inside says "Provide a list of Sharepoint sites for Cloud Data Sense to scan their data, line-separated. You can add up to 100 sites at a time." Below this, it says "Type or paste below the Sharepoint Site URL to add". There is a text input area labeled "Site URL" containing six identical lines of the URL "https://netapp.sharepoint.com/sites/ComplianceUserStories". At the bottom of the dialog, there are two buttons: "Add Sites" and "Cancel".

確認ダイアログに追加されたサイトの数が表示されます。

ダイアログに追加できなかったサイトが表示された場合は、問題を解決できるようにこの情報を記録します。場合によっては、URL を修正してサイトを再追加することができます。

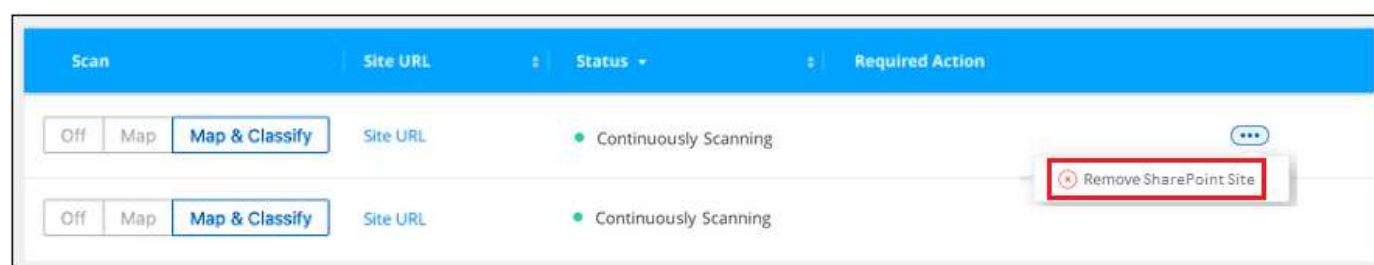
4. SharePoint サイト内のファイルに対して、マッピングのみのスキャン、またはマッピングと分類スキャンを有効にします。

終了：	手順：
ファイルのマッピングのみのスキャンを有効にします	[* マップ *] をクリックします
ファイルのフルスキャンを有効にします	[マップと分類 *] をクリックします
ファイルのスキャンを無効にします	[* Off *] をクリックします

Cloud Data Sense によって、追加した SharePoint サイトのファイルのスキャンが開始され、結果がダッシュボードやその他の場所に表示されます。

SharePoint サイトをコンプライアンススキャンから削除します

今後 SharePoint サイトを削除する場合や、SharePoint サイト内のファイルをスキャンしない場合は、個々の SharePoint サイトのファイルがいつでもスキャンされないようにすることができます。[構成] ページで [SharePoint サイトの削除] をクリックします。



ファイル共有をスキャンしています

NetApp 以外の NFS または CIFS ファイル共有を Cloud Data Sense で直接スキャンするには、いくつかの手順を実行します。これらのファイル共有は、オンプレミスでもクラウドでもかまいません。

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。

CIFS （SMB）共有の場合は、共有にアクセスするためのクレデンシャルがあることを確認しておきます。

"クラウドデータの導入センス" インスタンスが展開されていない場合。

このグループは、スキャンするファイル共有のコンテナであり、これらのファイル共有の作業環境名として使用されます。

スキャンするファイル共有のリストを追加し、スキャンのタイプを選択します。一度に最大 100 個のファイ

ル共有を追加できます。

ファイル共有の要件の確認

Cloud Data Sense 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ます。

- 共有は、クラウド内やオンプレミスなど、どこでもホストできます。ネットアップ以外のストレージシステム上のファイル共有です。
- データセンスインスタンスと共有の間にネットワーク接続が必要です。
- これらのポートが Data Sense 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
- 追加する共有のリストは、「<host_name> : /<share_path>`」の形式で指定する必要があります。共有は個別に入力することも、スキャンするファイル共有の行区切りリストを指定することもできます。
- CIFS （SMB）共有の場合は、共有への読み取りアクセスを提供する Active Directory クレデンシャルがあることを確認します。管理者クレデンシャルが推奨されるのは、Cloud Data Sense で管理者権限が必要なデータをスキャンする必要がある場合です。

Cloud Data Sense インスタンスの導入

導入済みのインスタンスがない場合は Cloud Data Sense を導入

インターネット経由でアクセス可能な、ネットアップ以外の NFS または CIFS ファイル共有をスキャンする場合は、を実行します ["クラウドにクラウドデータセンスを導入"](#) または ["インターネットにアクセス可能なオンプレミスの場所にデータセンスを導入"](#)。

インターネットにアクセスできないダークサイトにインストールされているネットアップ以外の NFS または CIFS ファイル共有をスキャンする場合は、が必要です ["クラウドデータセンスは、インターネットにアクセスできないオンプレミス環境に導入できます"](#)。そのため、Cloud Manager Connector をオンプレミスと同じ場所に導入する必要があります。

Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

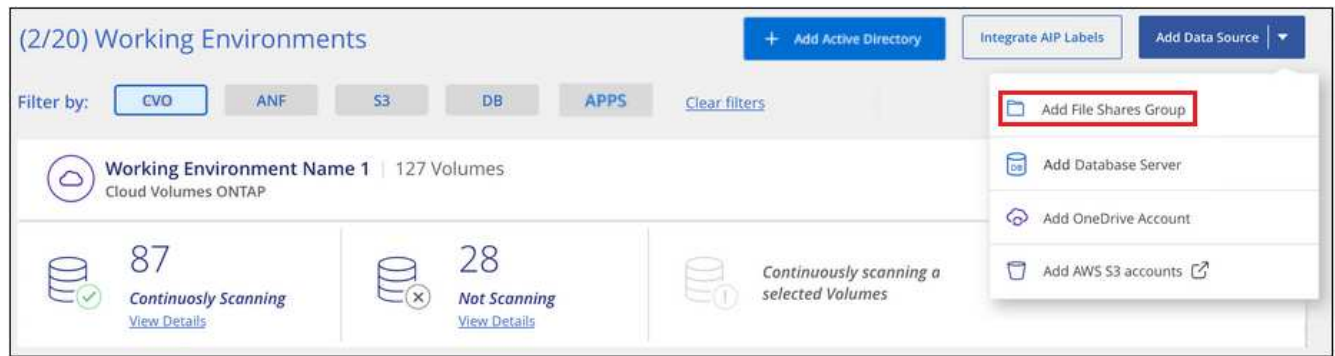
ファイル共有のグループを作成します

ファイル共有を追加する前に、「group」というファイル共有を追加する必要があります。グループはスキャンするファイル共有のコンテナであり、グループ名はそれらのファイル共有の作業環境名として使用されます。

同じグループ内に NFS 共有と CIFS 共有を混在させることはできますが、1つのグループ内のすべての CIFS ファイル共有で同じ Active Directory クレデンシャルを使用する必要があります。異なるクレデンシャルを使用する CIFS 共有を追加する場合は、一意のクレデンシャルセットごとに個別のグループを作成する必要があります。

手順

1. [作業環境の構成] ページで、[* データソースの追加 > ファイル共有グループの追加 *] をクリックします。



2. [ファイル共有グループの追加] ダイアログで、共有グループの名前を入力し、[続行] をクリックします。

新しいファイル共有グループが作業環境のリストに追加されます。

グループへのファイル共有の追加

ファイル共有グループにファイル共有を追加すると、これらの共有内のファイルが Cloud Data Sense によってスキャンされます。共有は、「<host_name> : /<share_path>」の形式で追加します。

個々のファイル共有を追加することも、スキャンするファイル共有を 1 行で区切って指定することもできます。一度に最大 100 個の共有を追加できます。

NFS 共有と CIFS 共有を 1 つのグループに追加する場合は、NFS 共有を追加してから CIFS 共有を再度追加するまで、このプロセスを 2 回実行する必要があります。

手順

1. 作業環境ページで、ファイル共有グループの * 構成 * ボタンをクリックします。



2. このファイル共有グループのファイル共有を初めて追加する場合は、* 最初の共有を追加 * をクリックします。



ボタンを

示すスクリーンショット。"]

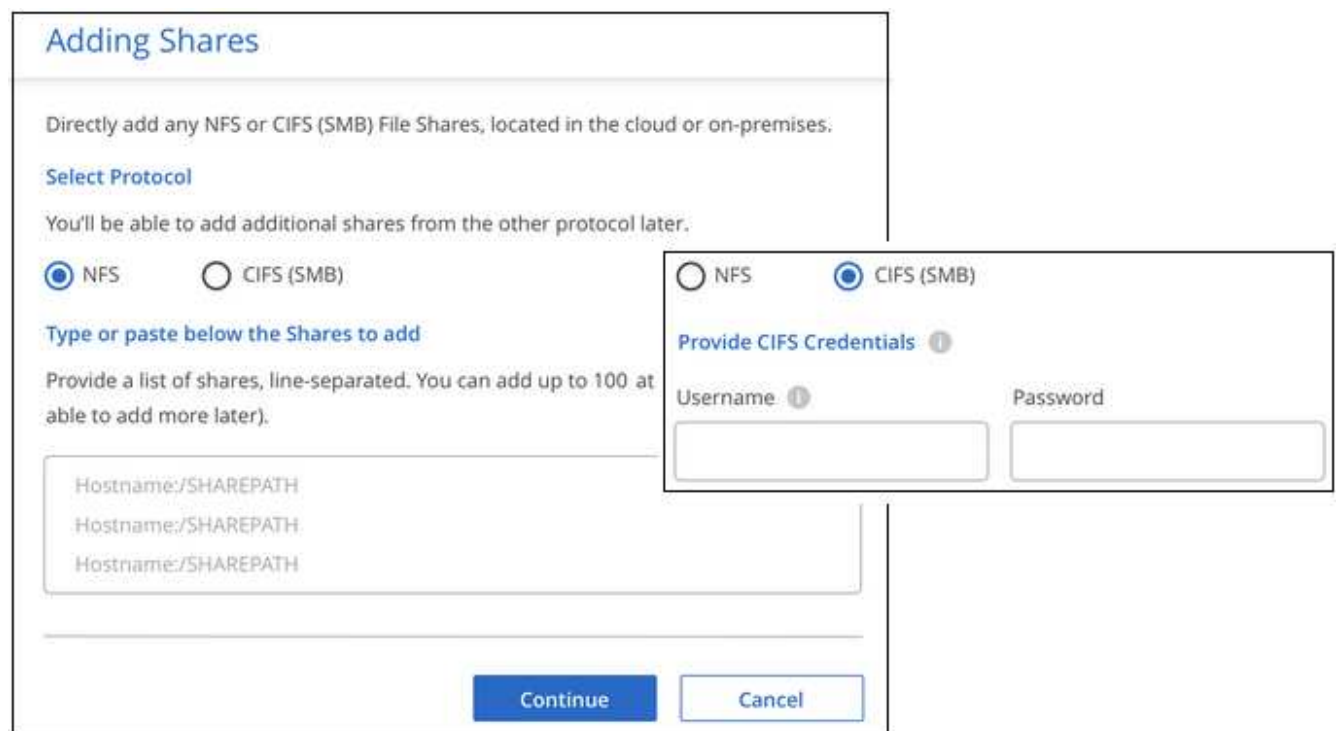
既存のグループにファイル共有を追加する場合は、* 共有の追加 * をクリックします。



ボタンを示すスクリーンショット。"]

3. 追加するファイル共有のプロトコルを選択し、スキャンするファイル共有を 1 行に 1 つ追加して、「* Continue *」をクリックします。

CIFS（SMB）共有を追加する場合は、共有への読み取りアクセスを提供する Active Directory クレデンシャルを入力する必要があります。admin クレデンシャルが優先されます。



追加された共有の数が確認ダイアログに表示されます。

ダイアログに追加できなかった共有が表示された場合は、問題を解決できるようにこの情報を記録しておきます。修正したホスト名または共有名を使用して共有を再追加できる場合があります。

4. 各ファイル共有で、マッピング専用スキャン、またはマッピングスキャンと分類スキャンを有効にします。

終了：	手順：
ファイル共有でマッピングのみのスキャンを有効にします	[* マップ *] をクリックします
ファイル共有でフルスキャンを有効にします	[マップと分類 *] をクリックします
ファイル共有でのスキャンを無効にします	[* Off *] をクリックします

Cloud Data Sense によって、追加したファイル共有内のファイルのスキャンが開始され、その結果がダッシュボードやその他の場所に表示されます。

準拠スキャンからのファイル共有の削除

特定のファイル共有をスキャンする必要がなくなった場合は、個々のファイル共有を削除して、ファイルがいつでもスキャンされるようにすることができます。[構成] ページで [共有の削除] をクリックします。



S3 プロトコルを使用するオブジェクトストレージをスキャンしています

Cloud Data Sense で、オブジェクトストレージ内のデータ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。データセンスは、Simple Storage Service (S3) プロトコルを使用する任意の Object Storage サービスからデータをスキャンできます。具体的には、NetApp StorageGRID、IBM Cloud Object Store、Azure Blob (MinIO を使用)、Linode、B2 Cloud Storage、Amazon S3 などです。

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。

オブジェクトストレージサービスに接続するには、エンドポイント URL が必要です。

Cloud Data Sense でバケットにアクセスできるように、オブジェクトストレージプロバイダからアクセスキーとシークレットキーを入手する必要があります。

"クラウドデータの導入センス" インスタンスが展開されていない場合。

オブジェクトストレージサービスをクラウドデータセンスに追加します。

スキャンするバケットを選択すると、Cloud Data Sense によってスキャンが開始されます。

オブジェクトストレージ要件の確認

Cloud Data Sense 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ます。

- オブジェクトストレージサービスに接続するには、エンドポイント URL が必要です。
- データセンスでバケットにアクセスできるようにするには、オブジェクトストレージプロバイダからアクセスキーとシークレットキーを取得する必要があります。
- Azure Blob のサポートにはを使用する必要があります ["MinIO サービス"](#)。

Cloud Data Sense インスタンスの導入

導入済みのインスタンスがない場合は Cloud Data Sense を導入

インターネット経由でアクセス可能な S3 オブジェクトストレージからデータをスキャンする場合は、を実行します ["クラウドにクラウドデータセンスを導入"](#) または ["インターネットにアクセス可能なオンプレミスの場所にデータセンスを導入"](#)。

インターネットにアクセスできないダークサイトにインストールされている S3 オブジェクトストレージからデータをスキャンする場合は、が必要です ["クラウドデータセンスは、インターネットにアクセスできないオンプレミス環境に導入できます"](#)。そのため、Cloud Manager Connector をオンプレミスと同じ場所に導入する必要があります。

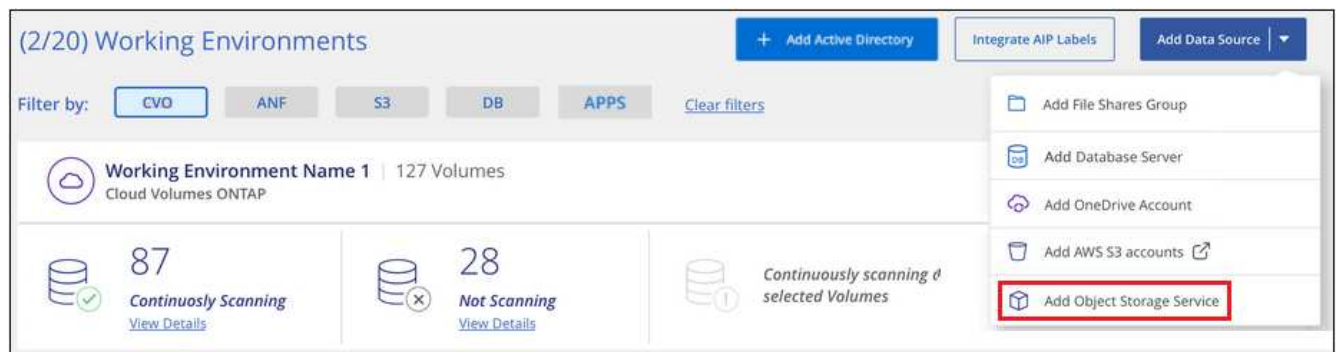
Data Sense ソフトウェアへのアップグレードは、インスタンスがインターネットに接続されている限り自動化されます。

Cloud Data Sense へのオブジェクトストレージサービスの追加

オブジェクトストレージサービスを追加します。

手順

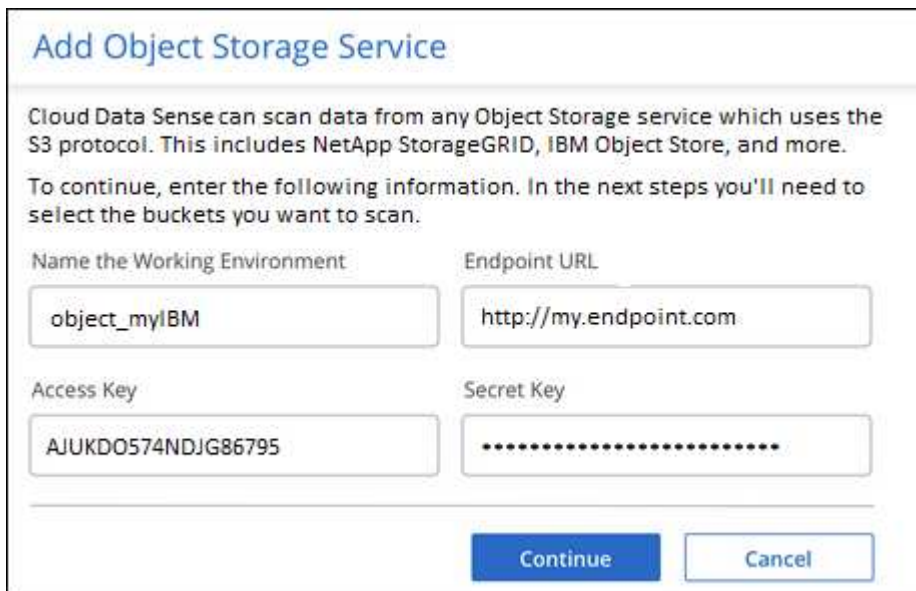
1. [作業環境の構成] ページで、[* データソースの追加 > オブジェクトストレージサービスの追加 *] をクリックします。



2. Add Object Storage Service ダイアログで、オブジェクトストレージサービスの詳細を入力し、* Continue * をクリックします。
 - a. 作業環境に使用する名前を入力します。この名前には、接続先のオブジェクトストレージサービスの

名前を指定する必要があります。

- b. エンドポイントの URL を入力してオブジェクトストレージサービスにアクセスします。
- c. Cloud Data Sense がオブジェクトストレージ内のバケットにアクセスできるように、アクセスキーとシークレットキーを入力します。



The dialog box is titled "Add Object Storage Service". It contains the following text: "Cloud Data Sense can scan data from any Object Storage service which uses the S3 protocol. This includes NetApp StorageGRID, IBM Object Store, and more. To continue, enter the following information. In the next steps you'll need to select the buckets you want to scan." Below this text are four input fields: "Name the Working Environment" with the value "object_myIBM", "Endpoint URL" with the value "http://my.endpoint.com", "Access Key" with the value "AJUKDO574NDJG86795", and "Secret Key" with a masked value "*****". At the bottom are two buttons: "Continue" and "Cancel".

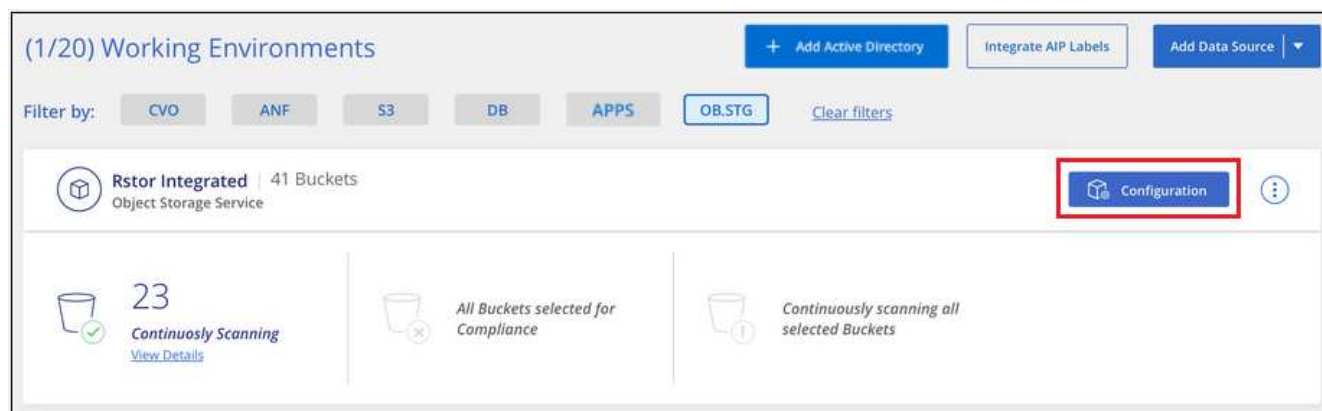
新しいオブジェクトストレージサービスが作業環境のリストに追加されます。

オブジェクトストレージバケットでの準拠スキャンの有効化と無効化

オブジェクトストレージサービスで Cloud Data Sense を有効にしたら、次の手順でスキャンするバケットを設定します。Data Sense は、これらのバケットを検出し、作成した作業環境に表示します。

手順

1. 設定ページで、Object Storage Service 作業環境の * 設定 * をクリックします。



2. バケットでマッピング専用スキャン、またはマッピングスキャンと分類スキャンを有効にします。

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

終了：	手順：
バケットでマッピングのみのスキャンを有効にする	[* マップ *] をクリックします
バケットでフルスキャンを有効にします	[マップと分類 *] をクリックします
バケットに対するスキャンを無効にする	[* Off *] をクリックします

Cloud Data Sense は、有効にしたバケットのスキャンを開始します。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。

Copyright Information

Copyright © 2022 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.