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

Cloud Manager

Tom Onacki, Ben Cammett
March 15, 2021

目次

『 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。

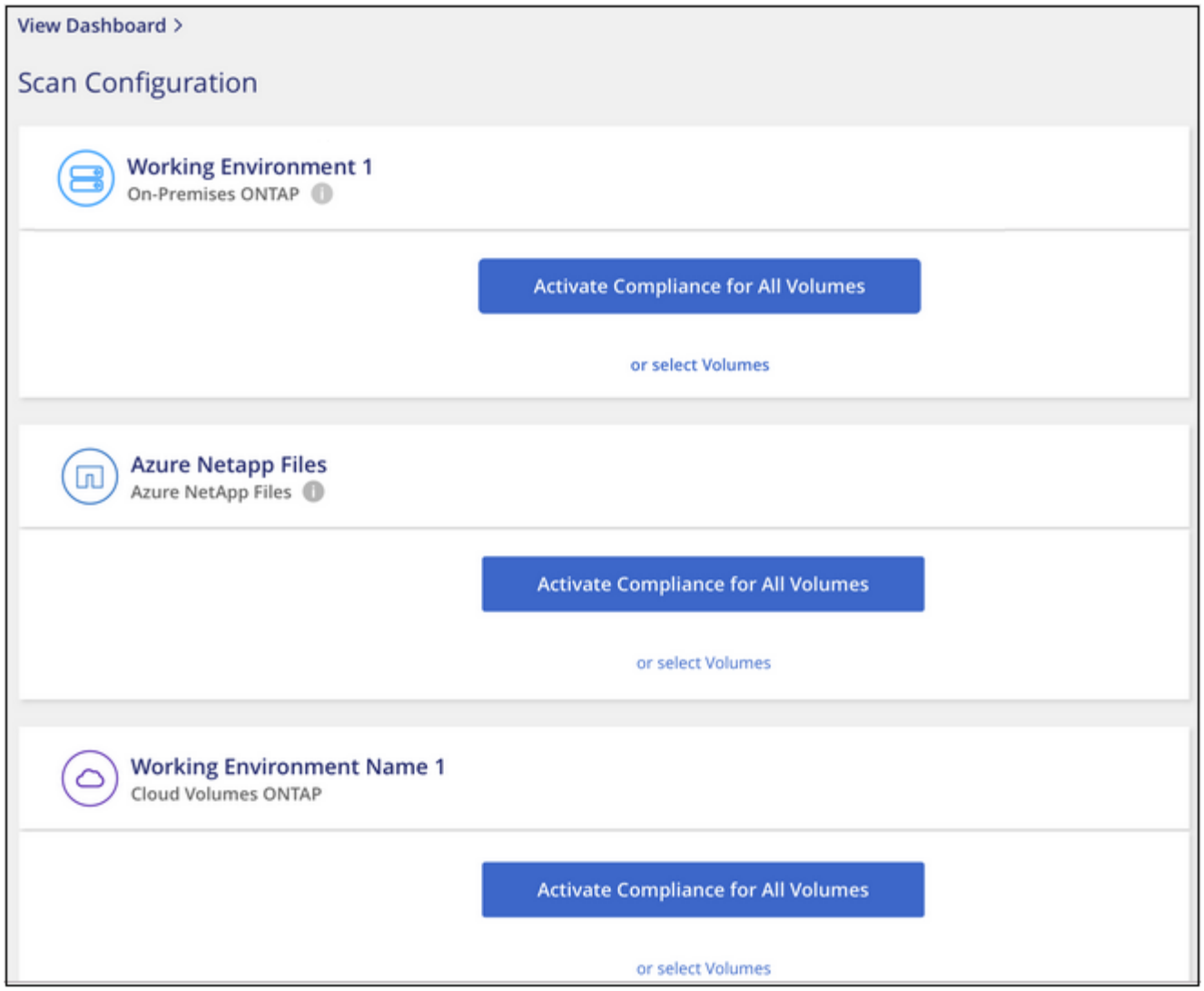
Azure NetApp Files ボリュームをスキャンする際にはクラウドに Cloud Compliance を導入し、スキャンするボリュームと同じリージョンに導入する必要があります。

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　を使用しています "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。



2. 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

1. 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。

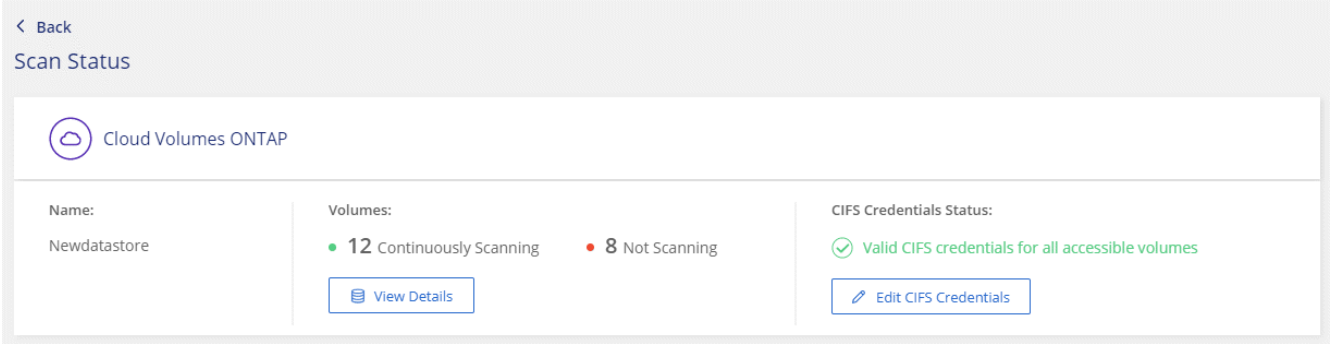
3. 次のポートが Cloud Compliance インスタンスに対して開いていることを確認します。
   - NFS –ポート 111 および 2049 。
   - CIFS の場合 - ポート 139 および 445
4. NFS ボリュームのエクスポートポリシーに Cloud Compliance インスタンスの IP アドレスが含まれていて、各ボリュームのデータにアクセスできることを確認します。
5. CIFS を使用する場合は、 Active Directory クレデンシャルを使用して Cloud Compliance を提供し、 CIFS ボリュームをスキャンできるようにしま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

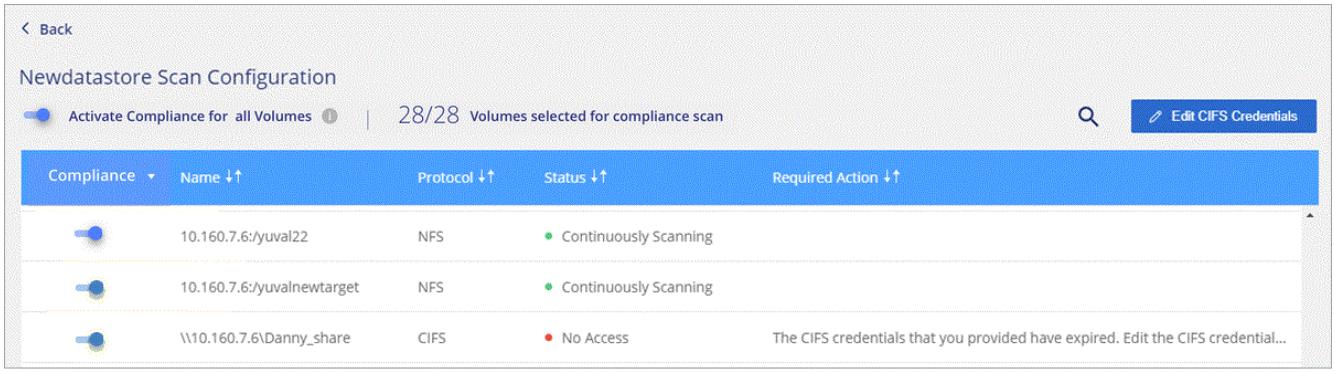
      クレデンシャルは読み取り専用ですが、管理者のクレデンシャルを指定することで、　Cloud Compliance　は昇格された権限が必要なデータを読み取ることができます。クレデンシャルは　Cloud Compliance インスタンスに保存されます。

      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。



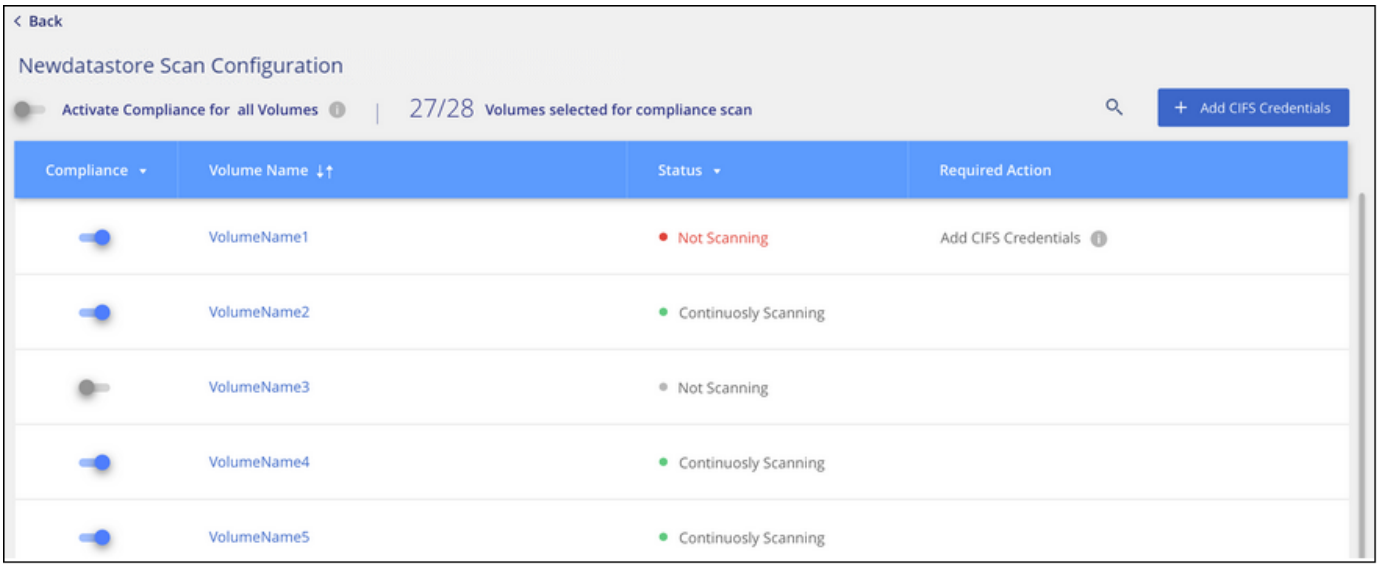
6. _Scan Configuration_page で、 * View Details * をクリックして、各 CIFS および NFS ボリュームのステータスを確認し、エラーを修正します。

   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。



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。



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 *] スライダをに移動します 左
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 *] スライダをに移動します 権利

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。

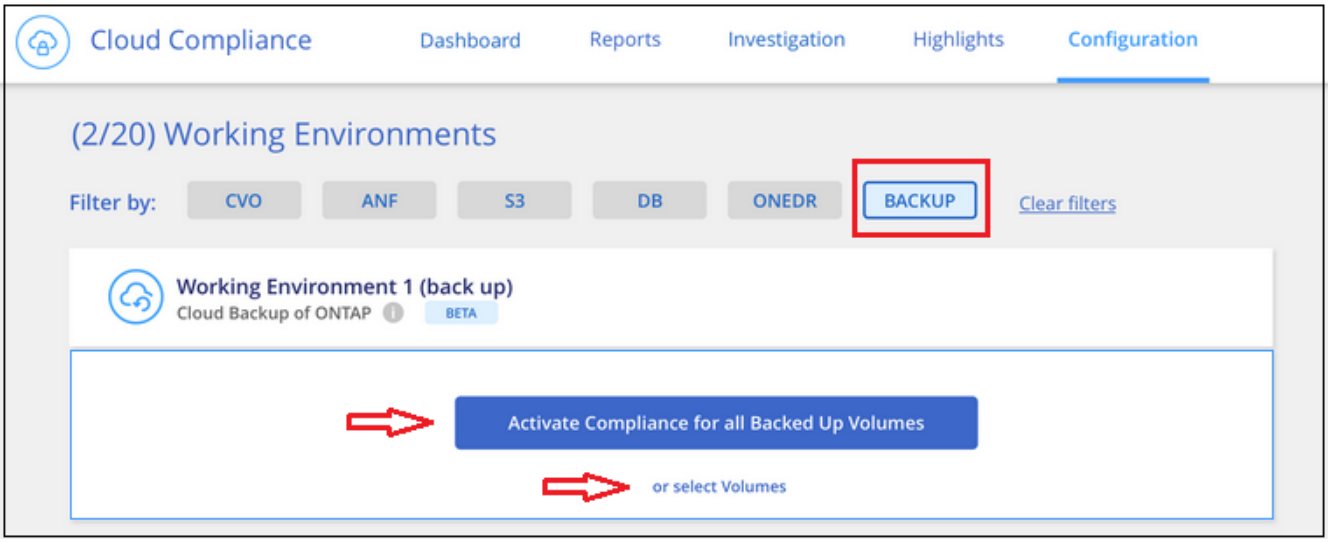
バックアップファイルで実行したコンプライアンススキャンは * 無料 * - Cloud Compliance サブスクリプションやライセンスは不要です。

- 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。



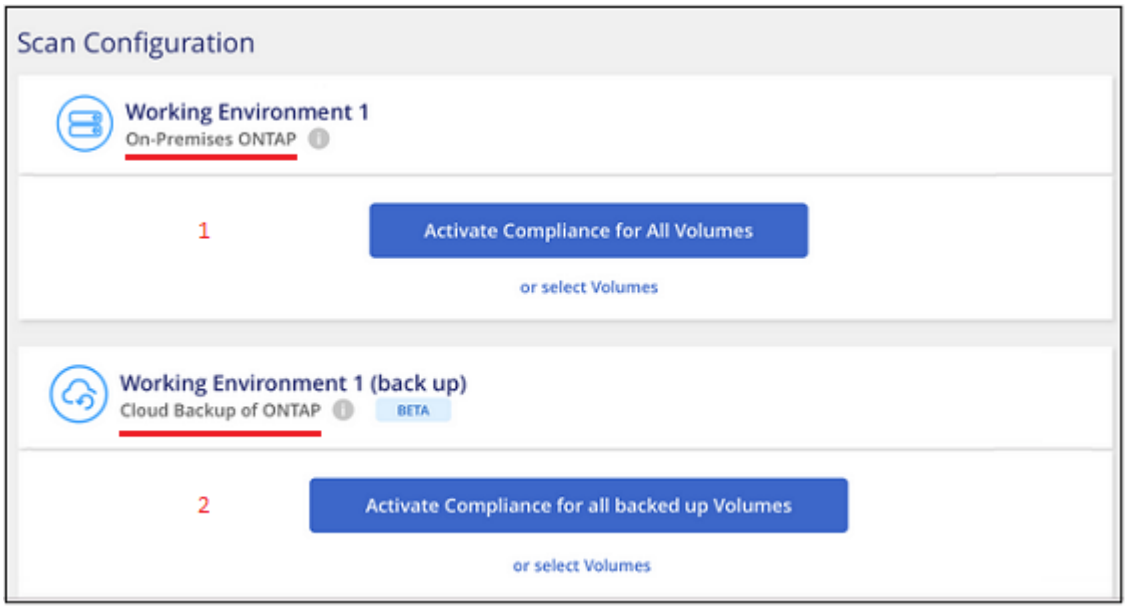
3. 作業環境でバックアップされたすべてのボリュームをスキャンするには、 * すべてのバックアップされたボリュームのコンプライアンスをアクティブ化 * をクリックします。

   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。

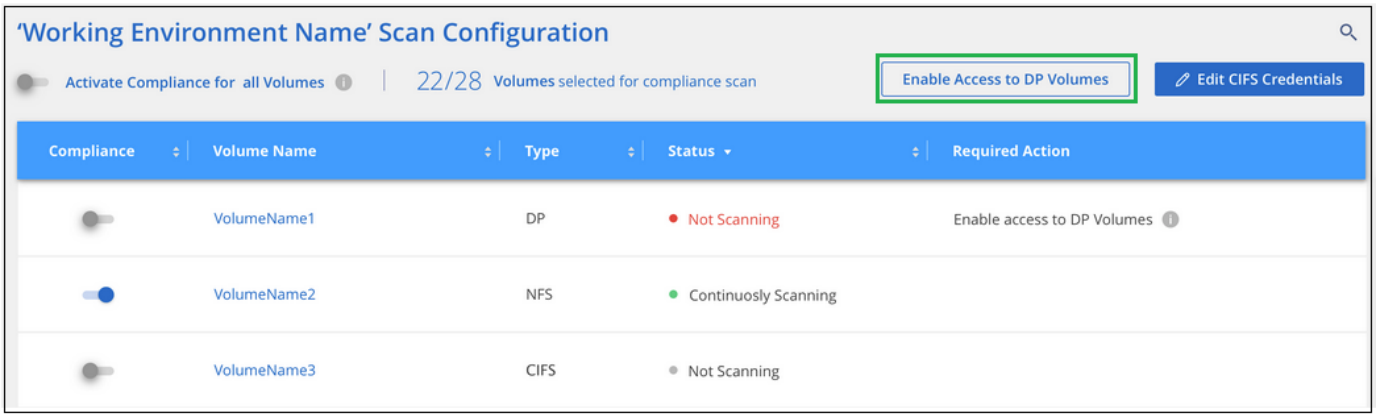
オンプレミスシステム上のボリュームをスキャンする最初のオプションを選択します。2 番目のオプションを選択して、対象のボリュームからバックアップファイルをスキャンします。同じクラスタのオンプレミスボリ

ューム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

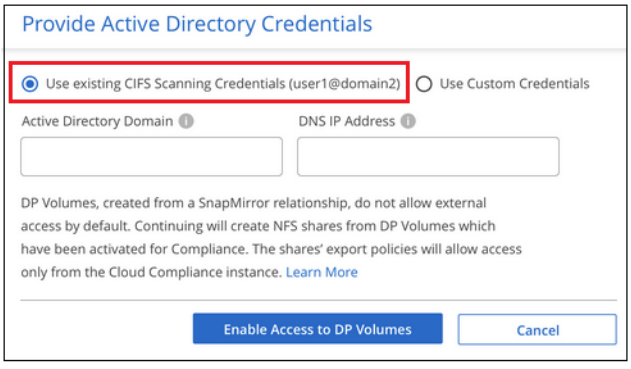
デフォルトでは、データ保護（ DP ）ボリュームは外部から公開されておらず、 Cloud Compliance はアクセスできないため、スキャンされません。オンプレミスの ONTAP システムまたは Cloud Volumes ONTAP システムからの SnapMirror 処理のデスティネーションボリュームです。

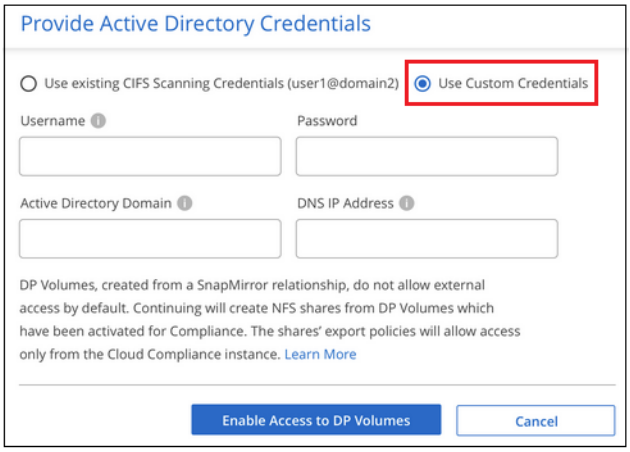
最初は、ボリュームリストでこれらのボリュームを *Type* DP * でスキャンしていないステータス * および必要なアクション _ * DP ボリュームへのアクセスを有効にします * 。



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。





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。