データソースでスキャンをアクティブ化します

BlueXP classification

NetApp
April 03, 2024

目次

データソースでスキャンをアクティブ化します

BlueXPでCloud Volumes ONTAP とオンプレミスのONTAP を分類してみましょう

いくつかの手順を実行して、BlueXPの分類を使用してCloud Volumes ONTAP ボリュームとオンプレミスONTAP ボリューム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。

1 スキャンするデータソースを検出します

ボリュームをスキャンする前に、システムをBlueXPの作業環境として追加する必要があります。

- Cloud Volumes ONTAP システムでは、これらの作業環境はBlueXPですでに使用可能になっています
- オンプレミスの ONTAP システムでは、 "BlueXPはONTAP クラスタを検出する必要があります"

2 **BlueXP**分類インスタンスを導入します

"BlueXP分類を導入します" インスタンスが展開されていない場合。

3 **BlueXP**分類を有効にし、スキャンするボリュームを選択します

[Configuration]*タブを選択し、特定の作業環境のボリュームのコンプライアンススキャンをアクティブ化します。

4 ボリュームへのアクセスを確認

BlueXPの分類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。

- BlueXP分類インスタンスには、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で、BlueXP分類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BlueXP分類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の場合は、
  - CIFSポート139および445の場合。
- NFSボリュームエクスポートポリシーでは、BlueXP分類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。

- BlueXPの分類では、CIFSボリュームのスキャンにActive Directoryの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。

5 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、BlueXP分類によってスキャンが開始または停止されます。

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BlueXP環境にない場合は、この時点でキャンバスに追加できます。

お使いのCloud Volumes ONTAP システムは、BlueXPのキャンバスですでに使用できるはずです。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BlueXPで検出されます"。

BlueXP分類インスタンスの導入

導入されているインスタンスがない場合は、BlueXP分類を導入します。

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 "BlueXPの分類機能をクラウドに導入します" 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"。

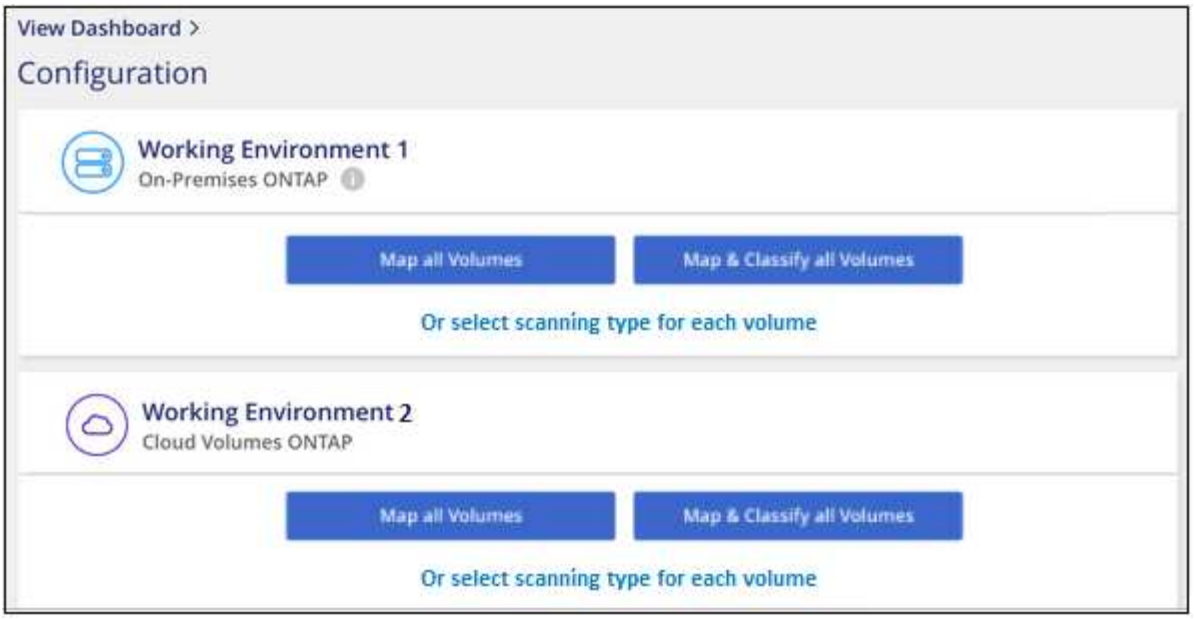
インターネットにアクセスできないダークサイトにインストールされているオンプレミスの ONTAP システムをスキャンする場合は、を実行する必要があります "インターネットアクセスのないオンプレミスと同じ場所にBlueXPの分類を導入します"。また、BlueXPコネクタがオンプレミスの同じ場所に配置されている必要があります。

インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

作業環境でBlueXPの分類を有効にする

BlueXPの分類は、サポートされている任意のクラウドプロバイダのCloud Volumes ONTAP システムとオンプレミスのONTAP クラスタで有効にすることができます。

1. BlueXPの左ナビゲーションメニューで、* Governance > Classification 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. 確認のダイアログボックスで、*[承認]*をクリックして、BlueXP分類でボリュームのスキャンを開始します。

結果

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、BlueXPの分類による初回スキャンが終了するとすぐに[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。

- BlueXPの分類では「最終アクセス時間」を元のタイムスタンプに戻すことができないため、CIFSでは属性の書き込み権限やNFSでの書き込み権限がない場合、デフォルトではボリューム内のファイルはスキャンされません。最終アクセス時間をリセットしても構わない場合は、*をクリックするか、各ボリュームのスキャンタイプ*を選択します。表示されるページで設定を有効にすると、権限に関係なくBlueXP分類でボリュームがスキャンされます。
- BlueXPは、1つのボリュームに含まれるファイル共有を1つだけスキャンします。ボリュームに複数の共有がある場合は、それらの他の共有を共有グループとして個別にスキャンする必要があります。 "BlueXPの分類に関するこの制限の詳細を参照してください"。

BlueXPの分類でボリュームにアクセスできることを確認する

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チェックして、BlueXPの分類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、BlueXPの分類にCIFSクレデンシャルを指定する必要があります。

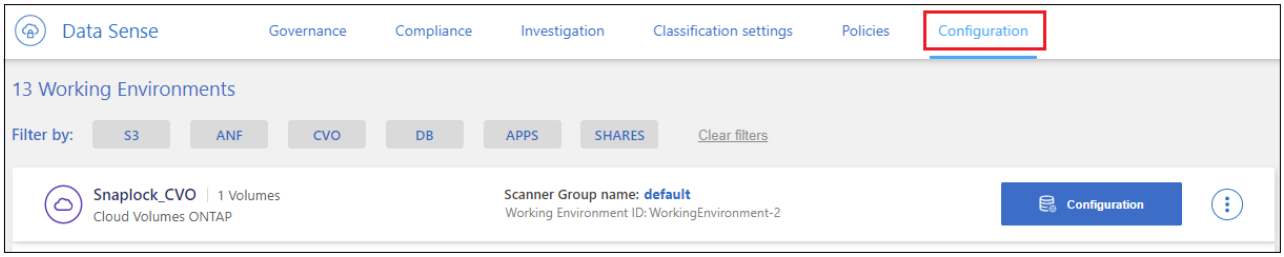
手順

1. BlueXP分類インスタンスと、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。
2. Cloud Volumes ONTAP のセキュリティグループがBlueXP分類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。

   BlueXP分類インスタンスの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. BlueXP分類インスタンスに対して次のポートが開いていることを確認します。
   - NFSポート111および2049の場合は、
   - CIFSポート139および445の場合。
4. NFSボリュームエクスポートポリシーにBlueXP分類インスタンスのIPアドレスが含まれていることを確認して、各ボリュームのデータにアクセスできるようにします。
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、BlueXPにActive Directoryクレデンシャルを指定してください。

   a. BlueXPの左ナビゲーションメニューで、* Governance > Classification をクリックし、 Configuration * タブを選択します。

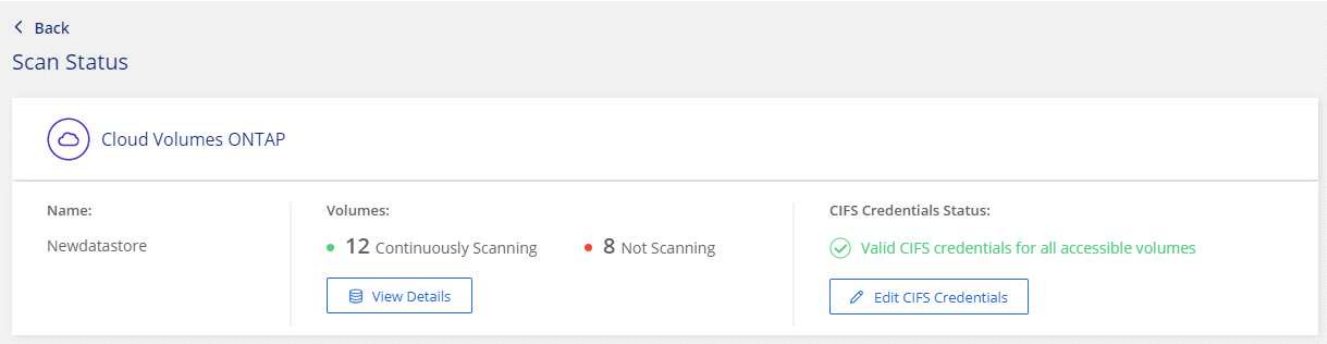
   ボタンを示す [遵守] タブのスクリーンショット。"]

   b. 各作業環境について、*[CIFSクレデンシャルの編集]*をクリックし、BlueXPでシステムのCIFSボリュームにアクセスするために必要なユーザ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、adminクレデンシャルを指定すると、昇格された権限が必要なデータをBlueXP分類で確実に読み取ることができます。クレデンシャルはBlueXP分類インスタンスに格納されます。

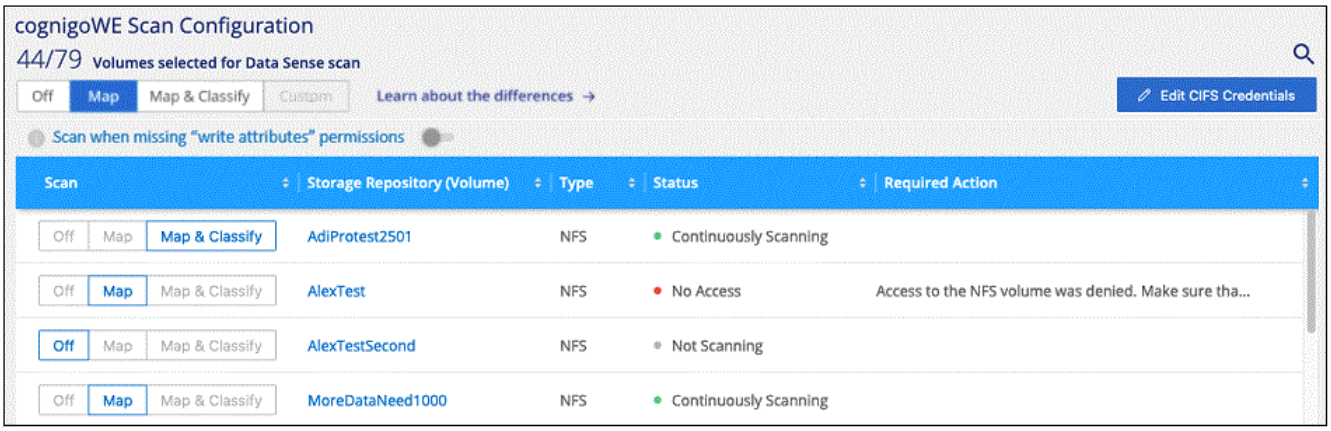
   BlueXPの分類スキャンでファイルの「最終アクセス日時」が変更されないようにするには、CIFSではWrite Attributes権限、NFSではwrite権限を持つことを推奨します。可能であれば、すべてのファイルに対する権限を持つ組織内の親グループにActive Directory構成ユーザーを含めることをお勧めします。

   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。そのうちの1つは、BlueXP分類インスタンスとボリュームの間のネットワーク接続に問題があるため、BlueXP分類でスキャンできません。

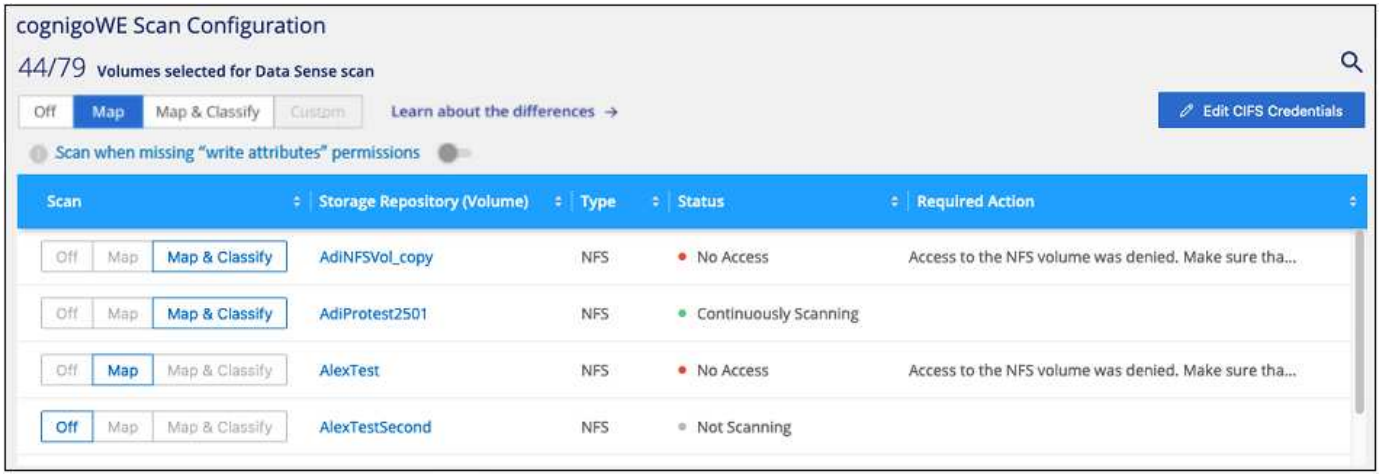


   ページのスクリーンショット。4つのボリュームが表示されています。そのうちの1つはBlueXPで分類されたボリュームとボリュームの間のネットワーク接続が原因でスキャンされていません。"]

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。

「属性の書き込み」権限がない場合にスキャンする*のページ上部のスイッチは、デフォルトでは無効になっています。つまり、BlueXPの分類にCIFSの属性への書き込み権限やNFSの書き込み権限がない場合、BlueXPの分類では「最終アクセス時間」を元のタイムスタンプに戻すことができないため、ファイルはスキャンされません。最終アクセス時間がリセットされても構わない場合は、スイッチをオンにすると、権限に関係なくすべてのファイルがスキャンされます。 "詳細はこちら。"。



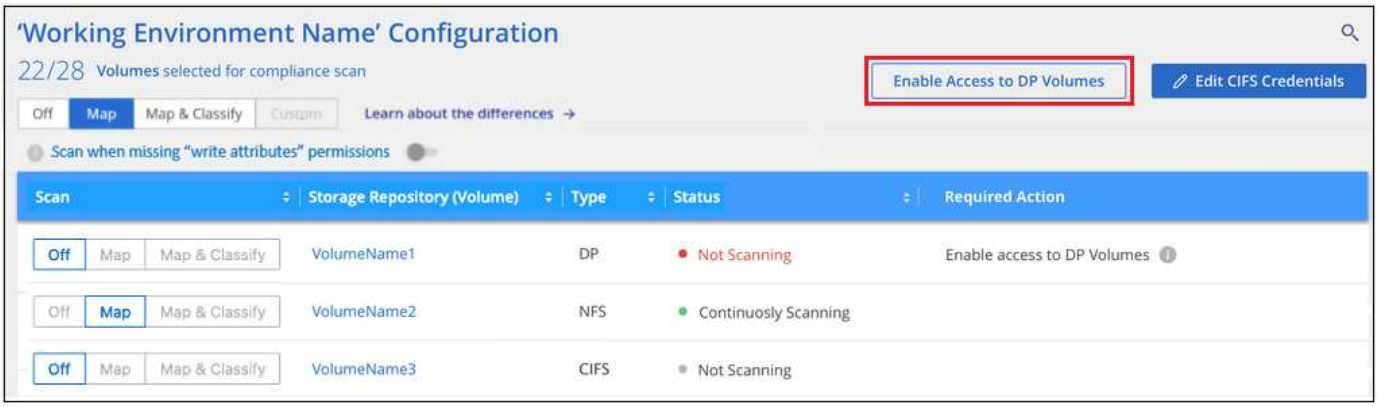
終了：	手順：
ボリュームに対してマッピングのみのスキャンを有効にします	ボリューム領域で、 * マップ * をクリックします
ボリュームでフルスキャンを有効にします	ボリューム領域で、 * マップと分類 * をクリックします
ボリュームのスキャンを無効にします	ボリューム領域で、 * オフ * をクリックします
すべてのボリュームでマッピングのみのスキャンを有効にします	見出し領域で、 * マップ * をクリックします
すべてのボリュームでフルスキャンを有効にします	見出し領域で、 * マップと分類 * をクリックします
すべてのボリュームでスキャンを無効にします	見出し領域で、 * Off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

データ保護（DP）ボリュームは外部に公開されず、BlueXPの分類ではアクセスできないため、デフォルトでは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。

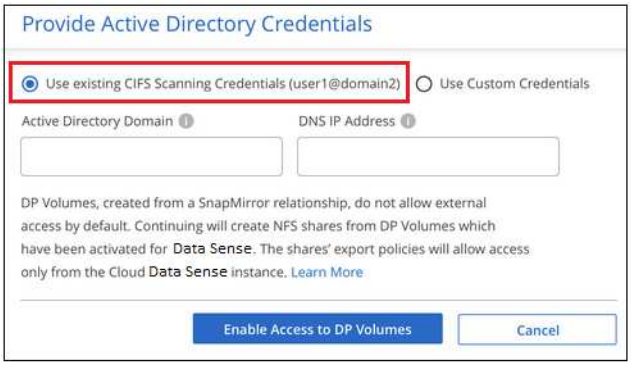
最初は、ボリュームリストでこれらのボリュームを *Type* * DP * でスキャンしていないステータス * および必要なアクション _ * DP ボリュームへのアクセスを有効にします * 。

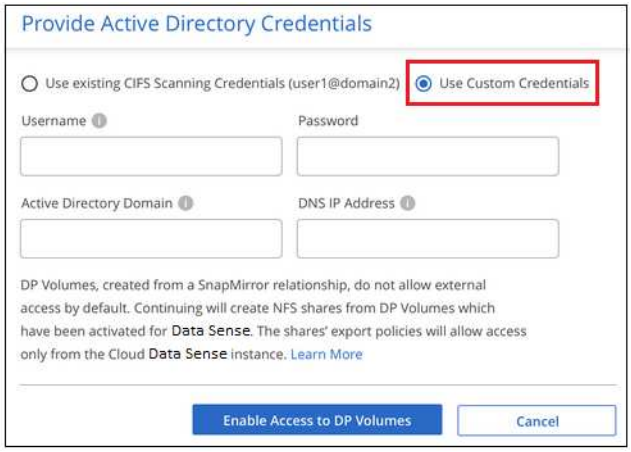


手順

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。Active Directory クレデンシャルを入力してBlueXP分類でCIFSボリュームをスキャンできるようにした場合は、それらのクレデンシャルを使用することも、別の管理者クレデンシャルのセットを指定することもできます。





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。

結果

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。共有のエクスポートポリシーでは、BlueXP分類インスタンスからのみアクセスが許可されます。

- 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。

BlueXPでAzure NetApp Files の分類を開始します

いくつかの手順を実行して、Azure NetApp Files 向けBlueXPの分類を開始してください。

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。

1 スキャンする**Azure NetApp Files** システムを検出します

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、BlueXPを設定する必要があります"。

2 **BlueXP**分類インスタンスを導入します

"BlueXPでBlueXP分類を導入します" インスタンスが展開されていない場合。

3 **BlueXP**分類を有効にし、スキャンするボリュームを選択します

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。

4 ボリュームへのアクセスを確認

BlueXPの分類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。

- BlueXP分類インスタンスには、各Azure NetApp Files サブネットへのネットワーク接続が必要です。
- 次のポートがBlueXP分類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は、BlueXP分類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。
- BlueXPの分類では、CIFSボリュームのスキャンにActive Directoryの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。

5 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、BlueXP分類によってスキャンが開始または停止されます。

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 システムが作業環境としてまだBlueXPにない場合は、この時点でキャンバスに追加できます。

"BlueXPでAzure NetApp Files システムを検出する方法を参照してください"。

BlueXP分類インスタンスの導入

"BlueXP分類を導入します" インスタンスが展開されていない場合。

Azure NetApp Files ボリュームのスキャン時にBlueXP分類がクラウドに導入され、スキャンするボリュームと同じリージョンに導入されている必要があります。

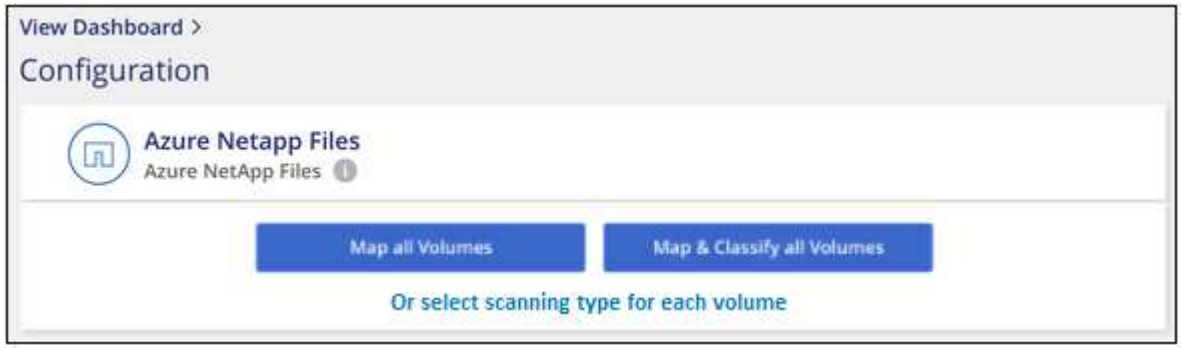
*注：*現時点では、Azure NetApp Files ボリュームのスキャン時にBlueXPの分類をオンプレミスに導入することはできません。

インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

作業環境で**BlueXP**の分類を有効にする

Azure NetApp Files ボリュームでBlueXP分類を有効にすることができます。

1. BlueXPの左ナビゲーションメニューで、* Governance > Classification 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. 確認のダイアログボックスで、*[承認]*をクリックして、BlueXP分類でボリュームのスキャンを開始します。

結果

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、BlueXPの分類による初回スキャンが終了するとすぐに[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。

- BlueXPの分類では「最終アクセス時間」を元のタイムスタンプに戻すことができないため、CIFSでは属性の書き込み権限やNFSでの書き込み権限がない場合、デフォルトではボリューム内のファイルはスキャンされません。最終アクセス時間をリセットしても構わない場合は、*をクリックするか、各ボリュームのスキャンタイプ*を選択します。表示されるページで設定を有効にすると、権限に関係なくBlueXP分類でボリュームがスキャンされます。
- BlueXPは、1つのボリュームに含まれるファイル共有を1つだけスキャンします。ボリュームに複数の共有がある場合は、それらの他の共有を共有グループとして個別にスキャンする必要があります。 "BlueXPの分類に関するこの制限の詳細を参照してください"。

BlueXPの分類でボリュームにアクセスできることを確認する

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チェックして、BlueXPの分類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、BlueXPの分類にCIFSクレデンシャルを指定する必要があります。

手順

1. BlueXP分類インスタンスと、Azure NetApp Files 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 では、BlueXPの分類でスキャンできるのはBlueXPと同じリージョンにあるボリュームのみです。

2. BlueXP分類インスタンスに対して次のポートが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ボリュームエクスポートポリシーにBlueXP分類インスタンスのIPアドレスが含まれていることを確認して、各ボリュームのデータにアクセスできるようにします。
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、BlueXPにActive Directoryクレデンシャルを指定してください。
   a. BlueXPの左ナビゲーションメニューで、* Governance > Classification をクリックし、 Configuration * タブを選択します。

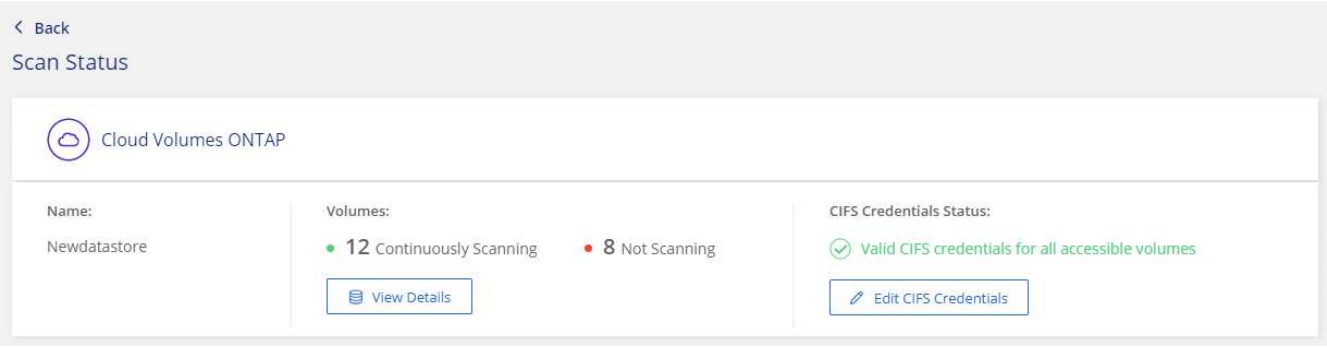
ボタンを示す [遵守] タブのスクリーンショット。"]

b. 各作業環境について、*[CIFSクレデンシャルの編集]*をクリックし、BlueXPでシステムのCIFSボリュームにアクセスするために必要なユーザ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、adminクレデンシャルを指定すると、昇格された権限が必要なデータをBlueXP分類で確実に読み取ることができます。クレデンシャルはBlueXP分類インスタンスに格納されます。

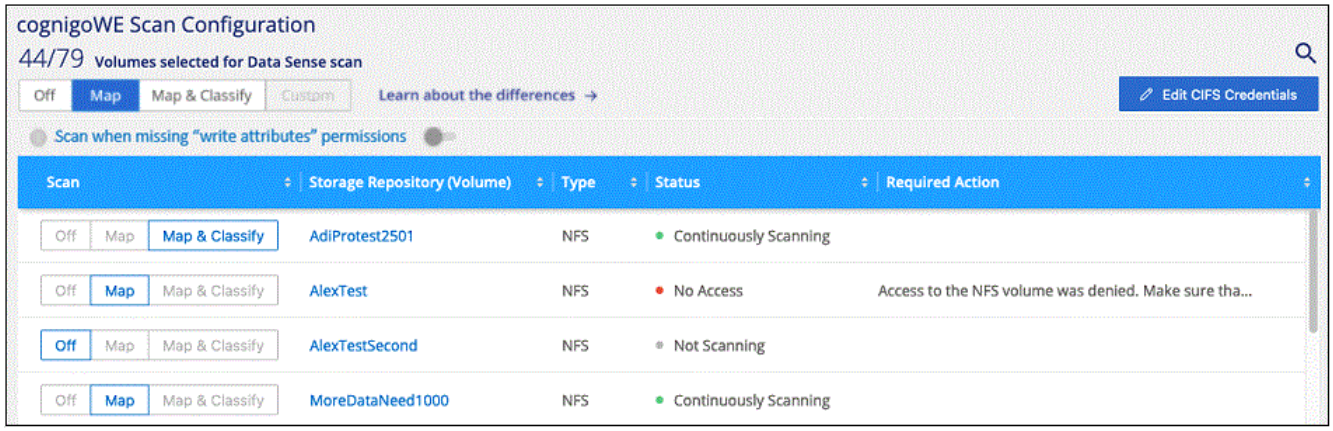
BlueXPの分類スキャンでファイルの「最終アクセス日時」が変更されないようにするには、CIFSではWrite Attributes権限、NFSではwrite権限を持つことを推奨します。可能であれば、すべてのファイルに対する権限を持つ組織内の親グループにActive Directory構成ユーザーを含めることをお勧めします。

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。そのうちの1つは、BlueXP分類インスタンスとボリュームの間のネットワーク接続に問題があるため、BlueXP分類でスキャンできません。

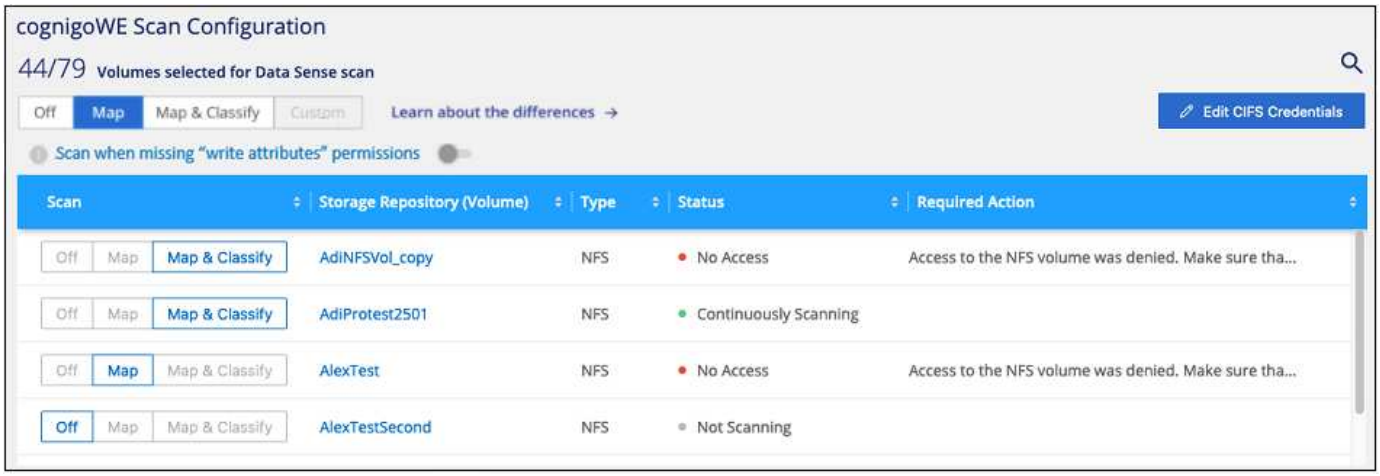


ページのスクリーンショット。4つのボリュームが表示されています。そのうちの1つはBlueXPで分類されたボリュームとボリュームの間のネットワーク接続が原因でスキャンされていません。"]

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。

「属性の書き込み」権限がない場合にスキャンする*のページ上部のスイッチは、デフォルトでは無効になっています。つまり、BlueXPの分類にCIFSの属性への書き込み権限やNFSの書き込み権限がない場合、BlueXPの分類では「最終アクセス時間」を元のタイムスタンプに戻すことができないため、ファイルはスキャンされません。最終アクセス時間がリセットされても構わない場合は、スイッチをオンにすると、権限に関係なくすべてのファイルがスキャンされます。 "詳細はこちら。"。



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

終了：	手順：
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。

BlueXPでAmazon FSx for ONTAP を分類しましょう

いくつかの手順を実行して、BlueXPに分類されたAmazon FSx for ONTAP ボリュームのスキャンを開始してください。

作業を開始する前に

- BlueXP分類を導入して管理するには、AWSにアクティブ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で、BlueXP分類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。

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

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"。

2 **BlueXP**分類インスタンスを導入します

"BlueXPでBlueXP分類を導入します" インスタンスが展開されていない場合。

3 **BlueXP**分類を有効にし、スキャンするボリュームを選択します

[Configuration]*タブを選択し、特定の作業環境のボリュームのコンプライアンススキャンをアクティブ化します。

4 ボリュームへのアクセスを確認

BlueXPの分類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。

- BlueXP分類インスタンスには、FSx for ONTAP の各サブネットへのネットワーク接続が必要です。
- 次のポートがBlueXP分類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は、BlueXP分類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。
- BlueXPの分類では、CIFSボリュームのスキャンにActive Directoryの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。

5 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、BlueXP分類によってスキャンが開始または停止されます。

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BlueXPにない場合は、この時点でキャンバスに追加できます。

"BlueXPでONTAP ファイルシステムのFSXを検出または作成する方法を参照してください"。

BlueXP分類インスタンスの導入

"BlueXP分類を導入します" インスタンスが展開されていない場合。

BlueXP分類は、Connector for AWSおよびスキャンするFSxボリュームと同じAWSネットワークに導入する必要があります。

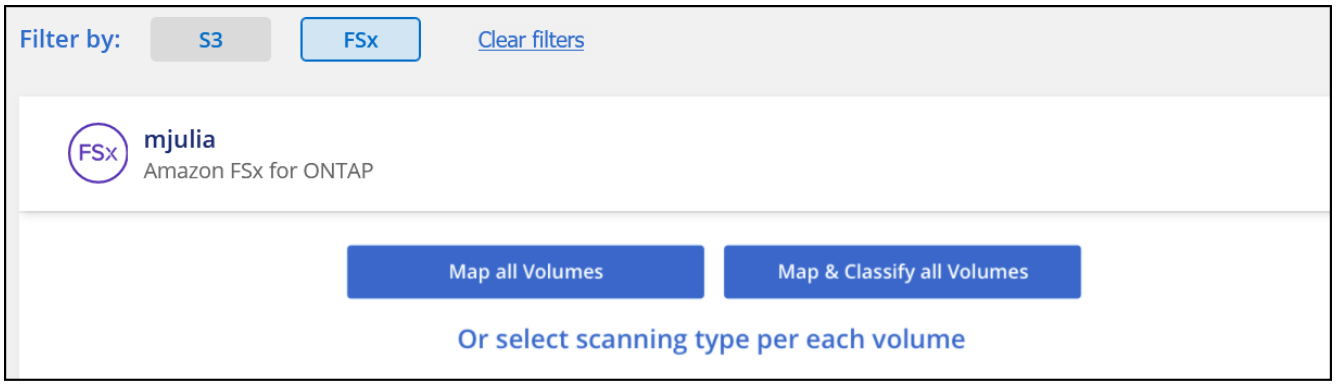
注： FSxボリュームのスキャン時にオンプレミス環境へのBlueXP分類の導入は現在サポートされていません。

インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

作業環境で**BlueXP**の分類を有効にする

FSx for ONTAP ボリュームに対してBlueXPの分類を有効にすることができます。

1. BlueXPの左ナビゲーションメニューで、* Governance > Classification 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. 確認のダイアログボックスで、*[承認]*をクリックして、BlueXP分類でボリュームのスキャンを開始します。

結果

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、BlueXPの分類による初回スキャンが終了するとすぐに[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。

- BlueXPの分類では「最終アクセス時間」を元のタイムスタンプに戻すことができないため、CIFSでは属性の書き込み権限やNFSでの書き込み権限がない場合、デフォルトではボリューム内のファイルはスキャンされません。最終アクセス時間をリセットしても構わない場合は、*をクリックするか、各ボリュームのスキャンタイプ*を選択します。表示されるページで設定を有効にすると、権限に関係なくBlueXP分類でボリュームがスキャンされます。
- BlueXPは、1つのボリュームに含まれるファイル共有を1つだけスキャンします。ボリュームに複数の共有がある場合は、それらの他の共有を共有グループとして個別にスキャンする必要があります。 "BlueXPの分類に関するこの制限の詳細を参照してください"。

BlueXPの分類でボリュームにアクセスできることを確認する

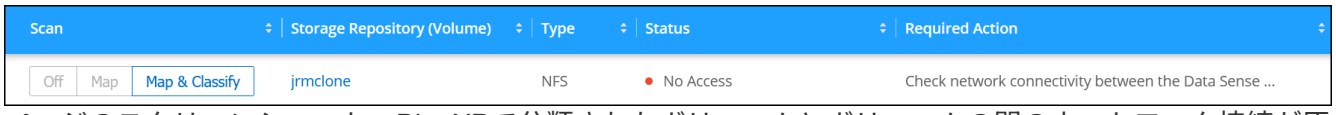
ネットワーク、セキュリティグループ、およびエクスポートポリシーをチェックして、BlueXPの分類でボリュームへのアクセスが許可されていることを確認します。

CIFSボリュームにアクセスできるように、BlueXPの分類にCIFSクレデンシャルを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、BlueXP分類インスタンスとボリュームの間のネットワーク接続に問題があるために、ボリュームBlueXP分類をスキャンできないことを示しています。



ページのスクリーンショット。BlueXPで分類されたボリュームとボリュームの間のネットワーク接続が原因でボリュームがスキャンされていないことが示されています。"]

2. BlueXP分類インスタンスと、FSx for ONTAP 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。

> FSx for ONTAP では、BlueXPの分類でスキャンできるのはBlueXPと同じリージョンのボリュームのみです。

3. 次のポートがBlueXP分類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ボリュームエクスポートポリシーにBlueXP分類インスタンスのIPアドレスが含まれていることを確認して、各ボリュームのデータにアクセスできるようにします。
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、BlueXPにActive Directoryクレデンシャルを指定してください。

   a. BlueXPの左ナビゲーションメニューで、* Governance > Classification をクリックし、 Configuration * タブを選択します。

   b. 各作業環境について、*[CIFSクレデンシャルの編集]*をクリックし、BlueXPでシステムのCIFSボリュームにアクセスするために必要なユーザ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、adminクレデンシャルを指定すると、昇格された権限が必要なデータをBlueXP分類で確実に読み取ることができます。クレデンシャルはBlueXP分類インスタンスに格納されます。

      BlueXPの分類スキャンでファイルの「最終アクセス日時」が変更されないようにするには、CIFSではWrite Attributes権限、NFSではwrite権限を持つことを推奨します。可能であれば、すべてのファイルに対する権限を持つ組織内の親グループにActive Directory構成ユーザーを含めることをお勧めします。

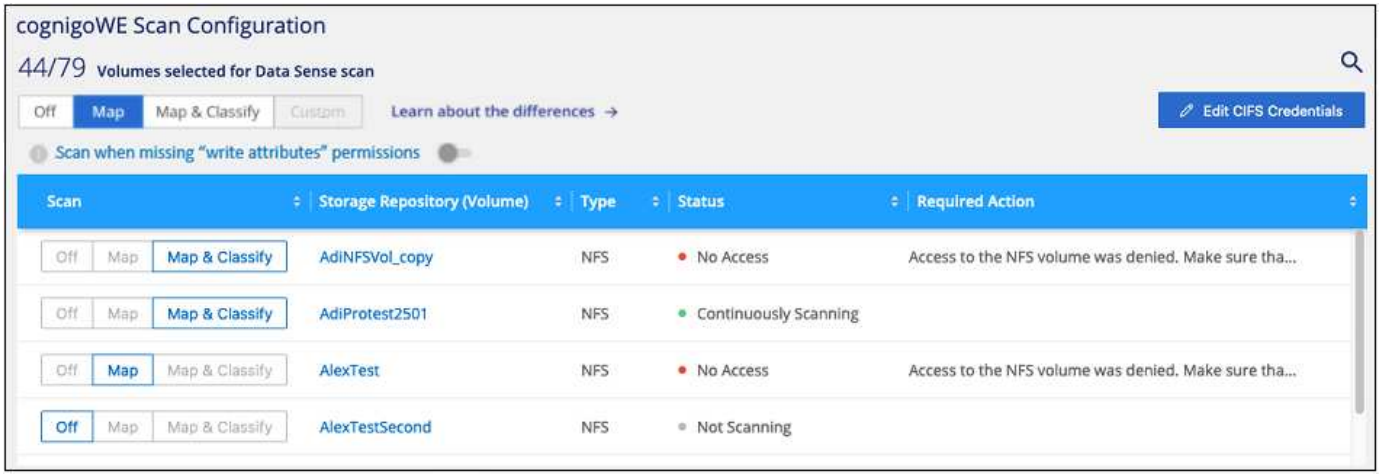
   クレデンシャルを入力すると、すべての CIFS ボリュームが認証されたことを示すメッセージが表示されます。

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。

「属性の書き込み」権限がない場合にスキャンする*のページ上部のスイッチは、デフォルトでは無効になっています。つまり、BlueXPの分類にCIFSの属性への書き込み権限やNFSの書き込み権限がない場合、BlueXP

の分類では「最終アクセス時間」を元のタイムスタンプに戻すことができないため、ファイルはスキャンされません。最終アクセス時間がリセットされても構わない場合は、スイッチをオンにすると、権限に関係なくすべてのファイルがスキャンされます。 "詳細はこちら。"。



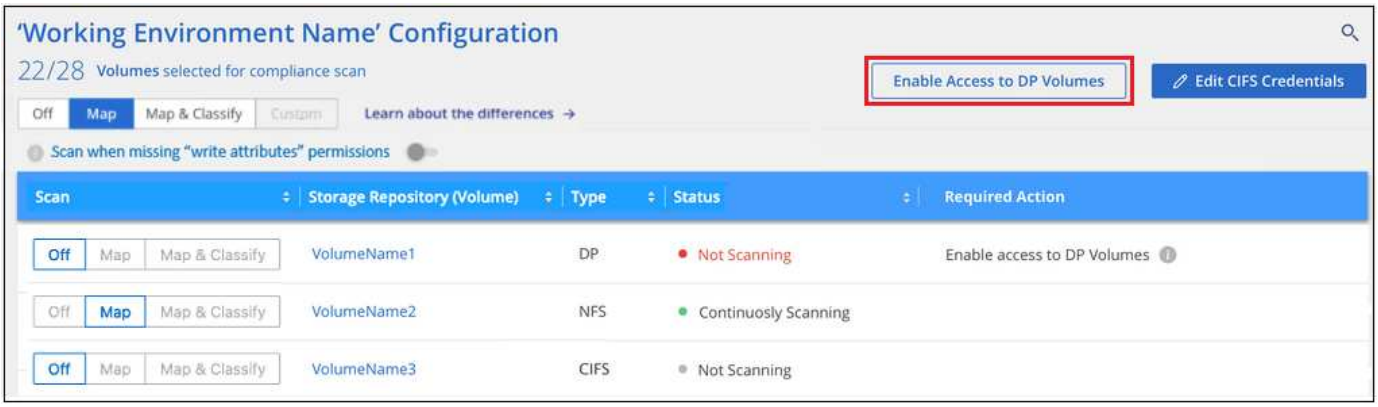
終了：	手順：
ボリュームに対してマッピングのみのスキャンを有効にします	ボリューム領域で、 * マップ * をクリックします
ボリュームでフルスキャンを有効にします	ボリューム領域で、 * マップと分類 * をクリックします
ボリュームのスキャンを無効にします	ボリューム領域で、 * オフ * をクリックします
すべてのボリュームでマッピングのみのスキャンを有効にします	見出し領域で、 * マップ * をクリックします
すべてのボリュームでフルスキャンを有効にします	見出し領域で、 * マップと分類 * をクリックします
すべてのボリュームでスキャンを無効にします	見出し領域で、 * Off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

データ保護（DP）ボリュームは外部に公開されず、BlueXPの分類ではアクセスできないため、デフォルトでは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。

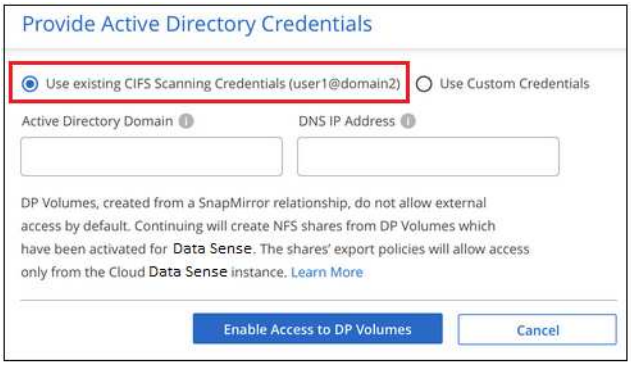
最初は、ボリュームリストでこれらのボリュームを *Type* DP * でスキャンしていないステータス * および必要なアクション _ * DP ボリュームへのアクセスを有効にします * 。

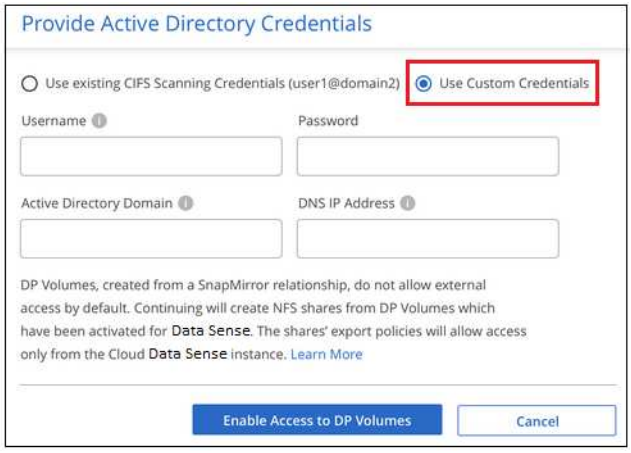


手順

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。Active Directoryクレデンシャルを入力してBlueXP分類でCIFSボリュームをスキャンできるようにした場合は、それらのクレデンシャルを使用することも、別の管理者クレデンシャルのセットを指定することもできます。





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。

結果

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。共有のエクスポートポリシーでは、BlueXP分類インスタンスからのみアクセスが許可されます。

- 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。

BlueXPでAmazon S3の分類を開始します

BlueXPの分類では、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た個人データと機密データを特定できます。BlueXPの分類では、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。

1. クラウド環境で **S3** の要件を設定します

お使いのクラウド環境がBlueXPの分類要件を満たしていることを確認します。これには、IAMロールの準備やBlueXPの分類からS3への接続の設定などが含まれます。 すべてのリストを参照してください。

2. **BlueXP**分類インスタンスを導入します

"BlueXP分類を導入します" インスタンスが展開されていない場合。

3. **S3**作業環境で**BlueXP**分類をアクティブ化します

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。

4. 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、BlueXPの分類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。

BlueXP分類インスタンス用の**IAM**ロールを設定します

BlueXPの分類には、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BlueXPの分類を有効にすると、IAMロールを選択するように求められます。

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

BlueXP分類から**Amazon S3**への接続を提供します

BlueXPの分類にはAmazon S3への接続が必要です。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、BlueXP分類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、BlueXPの分類から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。

BlueXP分類インスタンスの導入

"BlueXPでBlueXP分類を導入します" 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、BlueXP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： S3バケットのスキャン時にオンプレミス環境へのBlueXP分類の導入は現在サポートされていません。

インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

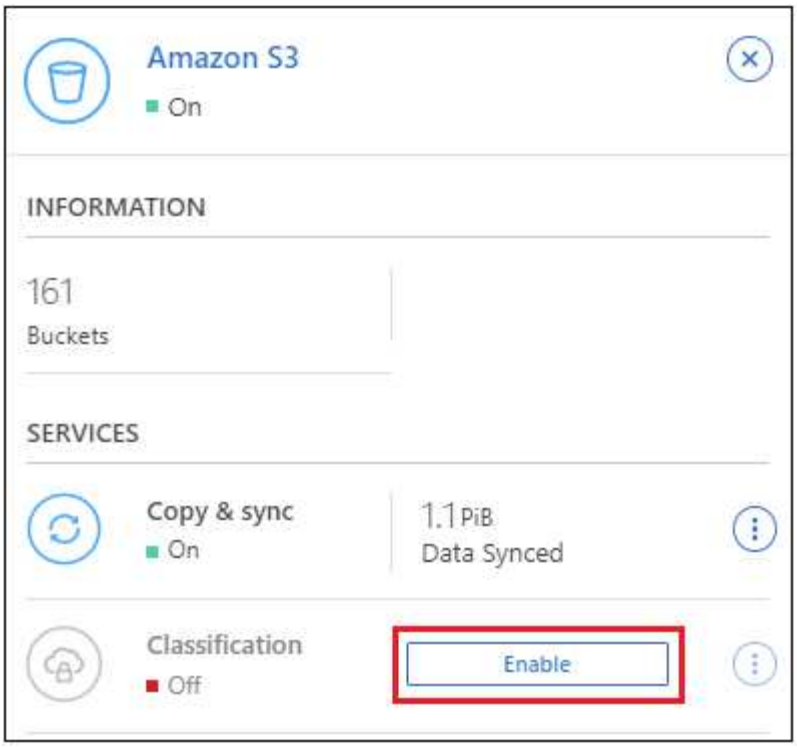
S3作業環境でBlueXP分類をアクティブ化します

前提条件を確認したら、Amazon S3でBlueXPの分類を有効にします。

手順

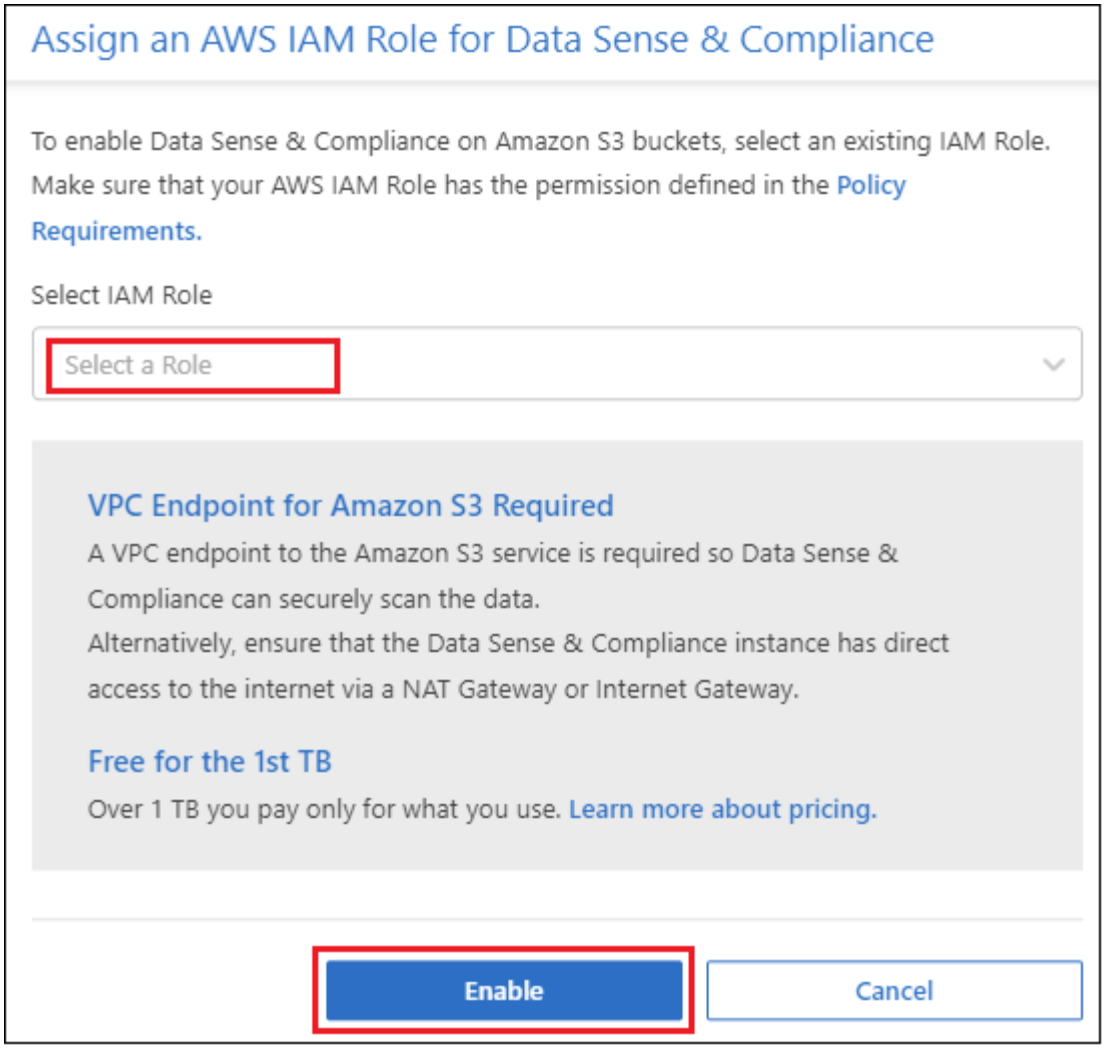
1. BlueXPの左ナビゲーションメニューから、*Storage > Canvas *をクリックします。
2. Amazon S3 作業環境を選択します。

3. 右側の[サービス]ペインで、[分類]の横にある*[有効化]*をクリックします。



パネルでBlueXP分類サービスを有効にするスクリーンショット"]

4. プロンプトが表示されたら、を含むBlueXP分類インスタンスにIAMロールを割り当てます 必要な権限。



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 ⋮ ボタンをクリックし、*[BlueXP分類のアクティブ化]*を選択します。

結果

BlueXPは、インスタンスにIAMロールを割り当てます。

S3 バケットでの準拠スキャンの有効化と無効化

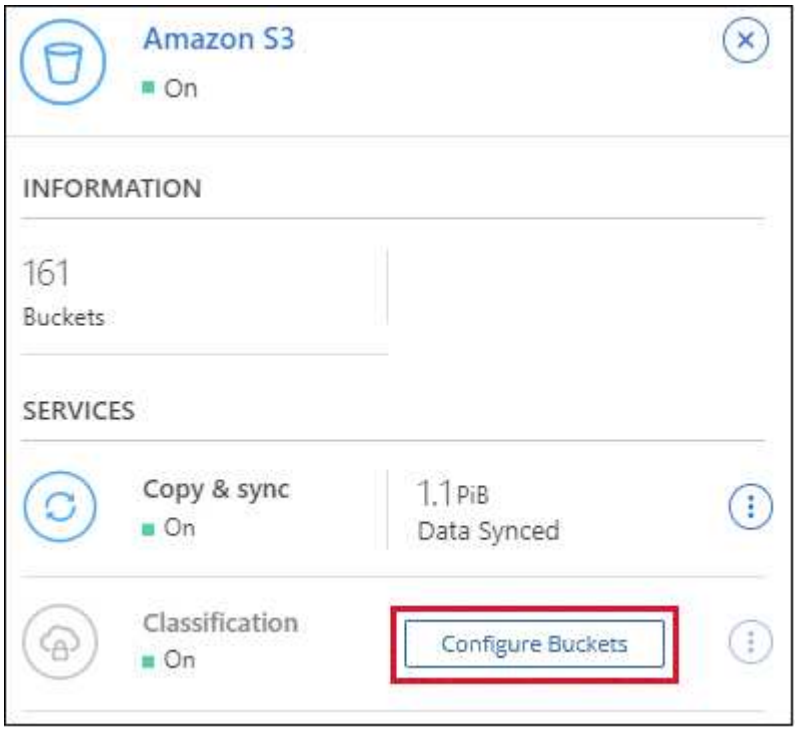
Amazon S3でBlueXPの分類を有効にしたら、次にスキャンするバケットを設定します。

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

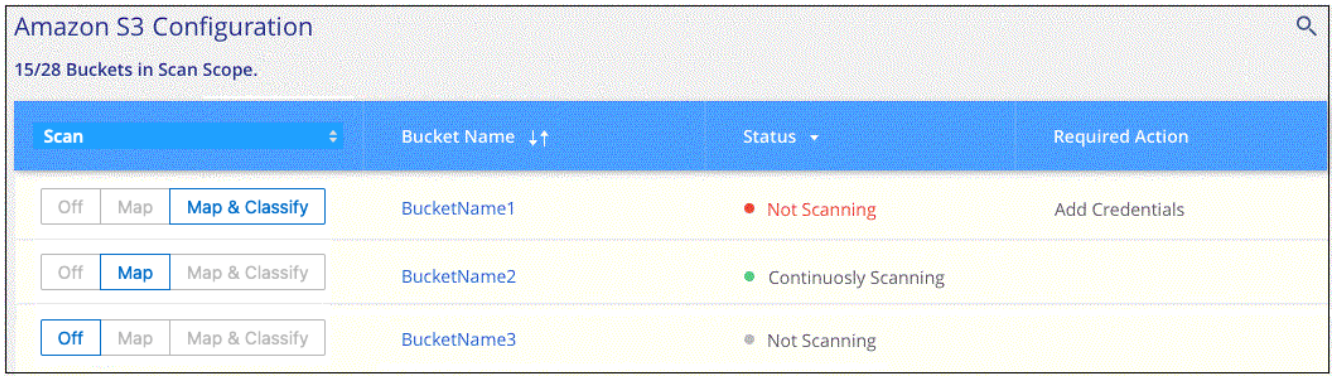
BlueXPに分類することもできます 別々の AWS アカウントにある S3 バケットをスキャンします。

手順

1. Amazon S3 作業環境を選択します。
2. 右側の[Services]ペインで、*[Configure Buckets]*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。



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

結果

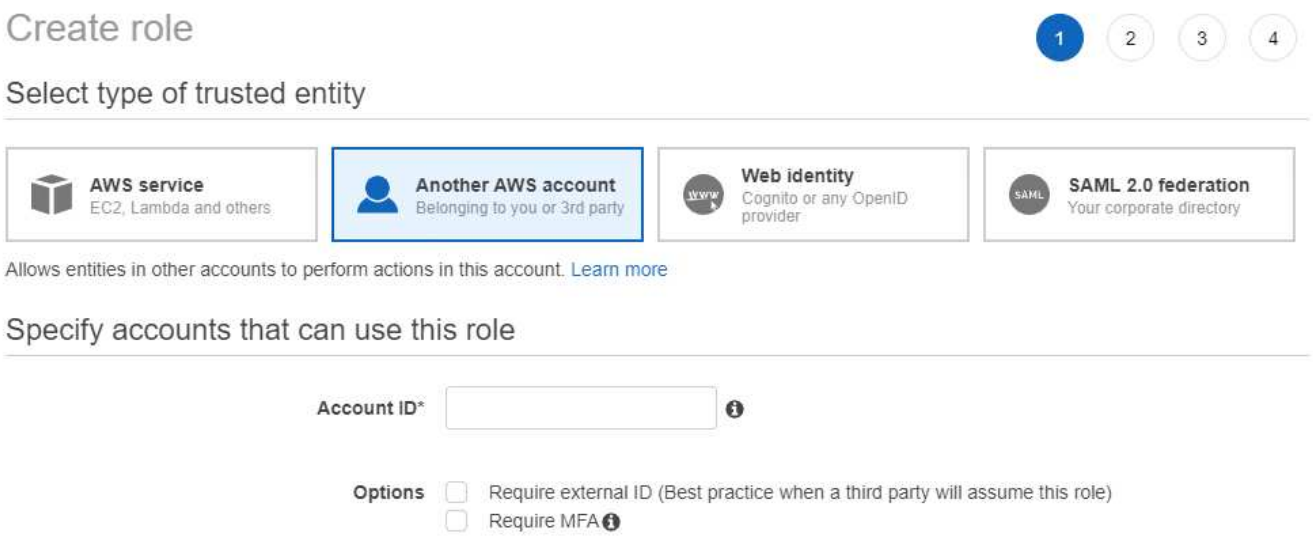
BlueXPの分類で、有効にしたS3バケットのスキャンが開始されます。エラーが発生した場合は、エラーを修正するために必要なアクションとともに、 [ステータス] 列に表示されます。

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アカウントにある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BlueXP分類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。



必ず次の手順を実行してください。

- BlueXP分類インスタンスが配置されているアカウントの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。
- BlueXP分類IAMポリシーを適用します。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": "*"
      },
  ]
}
```

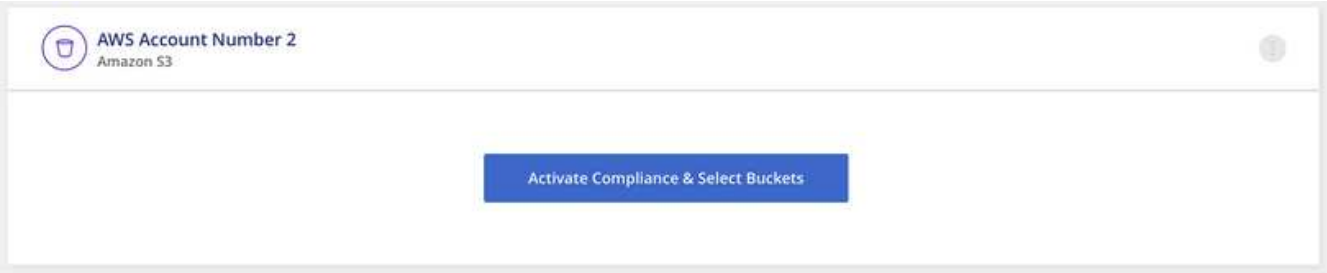
2. BlueXP分類インスタンスが配置されているソースAWSアカウントに移動し、インスタンスに関連付けられているIAMロールを選択します。
   a. 最大 CLI / API セッション期間 * を 1 時間から 12 時間に変更し、変更を保存してください。
   b. [* ポリシーの適用 *] をクリックし、 [ポリシーの作成 *] をクリックします。
   c. 「 STS ： AssumeRole 」アクションを含むポリシーを作成し、ターゲットアカウントで作成したロ

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/*"
            ]
        }
    ]
}
```

BlueXP分類インスタンスのプロファイルアカウントから、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。BlueXPの分類によって新しいアカウントの作業環境が同期され、この情報が表示されるまでに数分かかることがあります。



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

結果

BlueXPの分類で、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のスキャン

いくつかの手順を実行して、BlueXPの分類を使用したデータベーススキーマのスキャンを開始します。

データベーススキャンを有効にすると、すべてのデータソースでデータベースの特定の列に基づいて識別される一意の識別子を追加できます。これは_Data Fusionフィーチャーと呼ばれます。 "データベースからカスタム個人データ識別子を追加する方法"。

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。

1. 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。

2. **BlueXP**分類インスタンスを導入します

"BlueXP分類を導入します" インスタンスが展開されていない場合。

3. 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。

4. 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。

前提条件を確認する

BlueXPの分類を有効にする前に、次の前提条件を確認して、サポートされる構成が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

BlueXPの分類では、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

BlueXP分類インスタンスに接続されているデータベースは、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を選択することが重要です。BlueXP分類システム専用のユーザを作成し、必要なすべての権限を設定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。

BlueXP分類インスタンスを導入します

導入されているインスタンスがない場合は、BlueXP分類を導入します。

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 "BlueXPの分類機能をクラウドに導入します" 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にBlueXPの分類を導入します"。

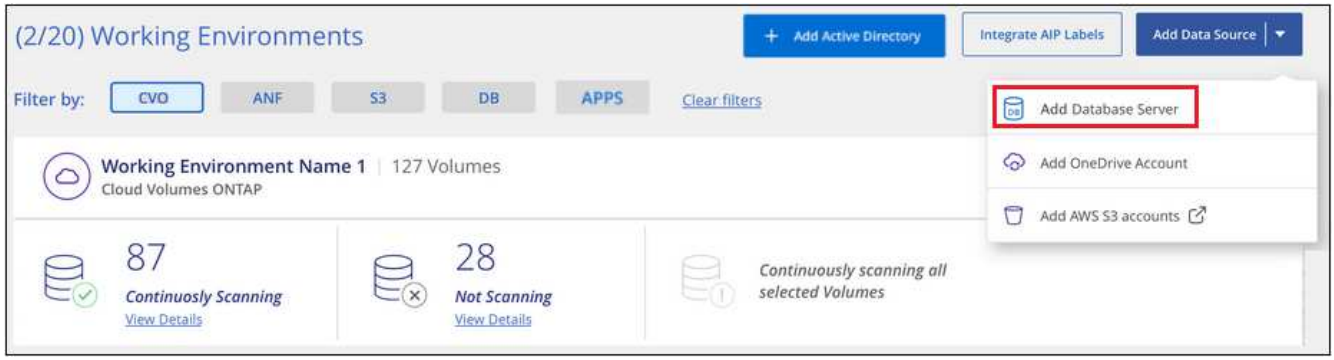
インターネットにアクセスできないダークサイトにインストールされているデータベーススキーマをスキャンする場合は、が必要です "インターネットアクセスのないオンプレミスと同じ場所にBlueXPの分類を導入します"。また、BlueXPコネクタがオンプレミスの同じ場所に配置されている必要があります。

インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

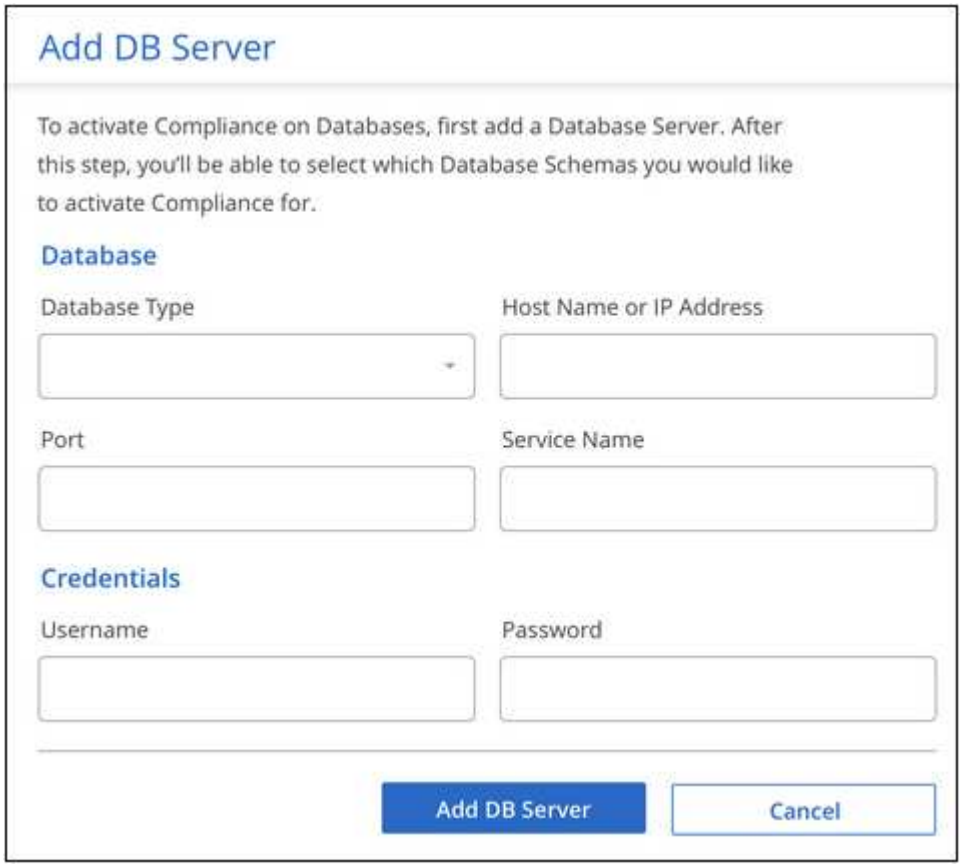
データベースサーバを追加します

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. クレデンシャルを入力して、BlueXP分類からサーバにアクセスできるようにします。
   e. [Add DB Server*] をクリックします。



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。

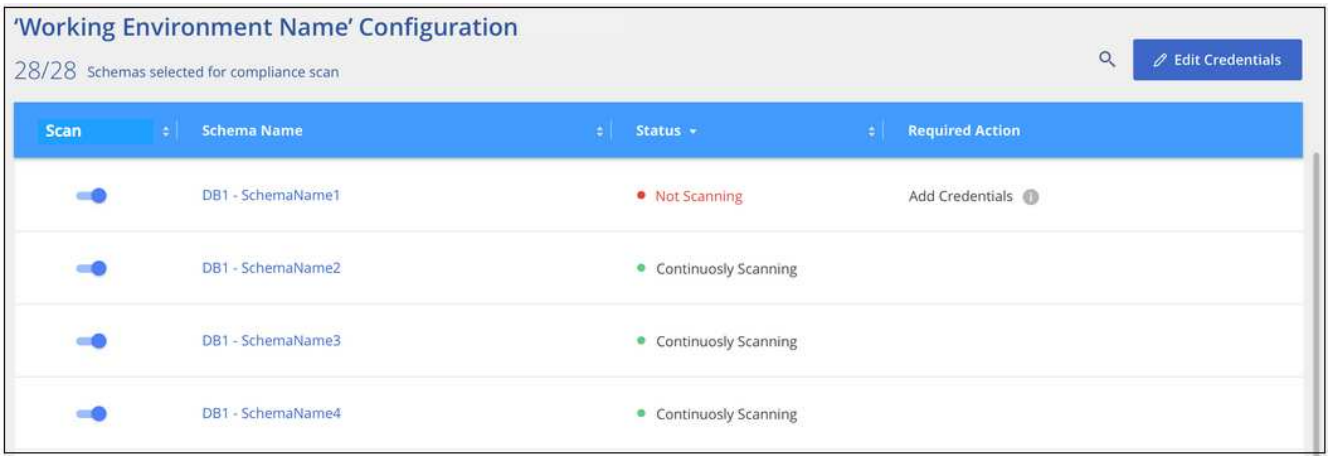
データベーススキーマでのコンプライアンススキャンの有効化と無効化

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。

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。



ページのスクリーンショット。"]

結果

BlueXPの分類で、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。

BlueXPの分類では、データベースが1日に1回スキャンされます。データベースは、他のデータソースのように継続的にスキャンされるわけではありません。

OneDrive アカウントをスキャンしています

BlueXP分類を使用して、ユーザーの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。

1 **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。

2 **BlueXP**分類インスタンスを導入します

"BlueXP分類を導入します" インスタンスが展開されていない場合。

3 **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。

4 ユーザを追加して、スキャンのタイプを選択します

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

BlueXPの分類を有効にする前に、次の前提条件を確認して、サポートされる構成があることを確認してください。

- ユーザの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。

BlueXP分類インスタンスの導入

導入されているインスタンスがない場合は、BlueXP分類を導入します。

BlueXPには次のように分類できます "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"。

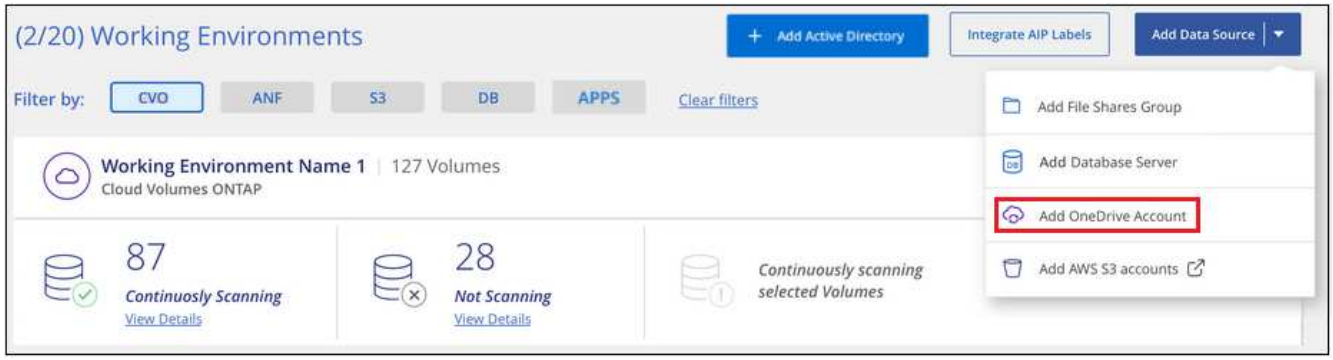
インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

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. 表示された[Microsoft]ページで、OneDriveアカウントを選択して必要な管理者ユーザとパスワードを入力し、*[同意する]*をクリックしてBlueXP分類によるこのアカウントからのデータの読み取りを許可します。

OneDrive アカウントが作業環境の一覧に追加されます。

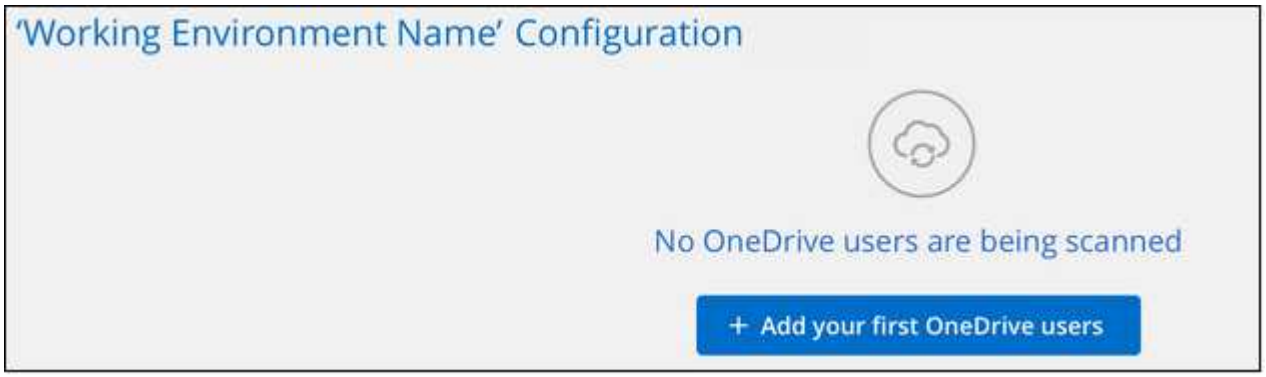
OneDrive ユーザーをコンプライアンススキャンに追加する

個 々 のOneDriveユーザまたはすべてのOneDriveユーザを追加して、BlueXPの分類によってファイルがスキャンされるようにすることができます。

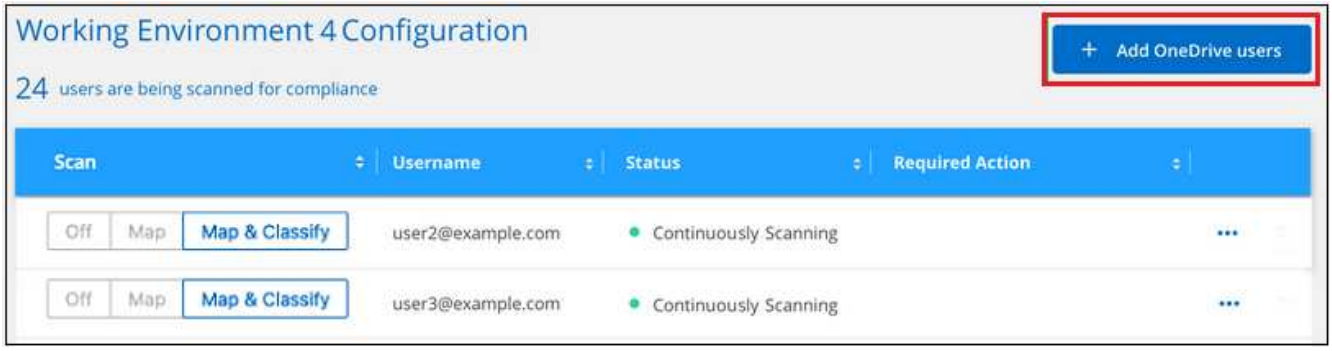
手順

1. [*Configuration*] ページで、 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。

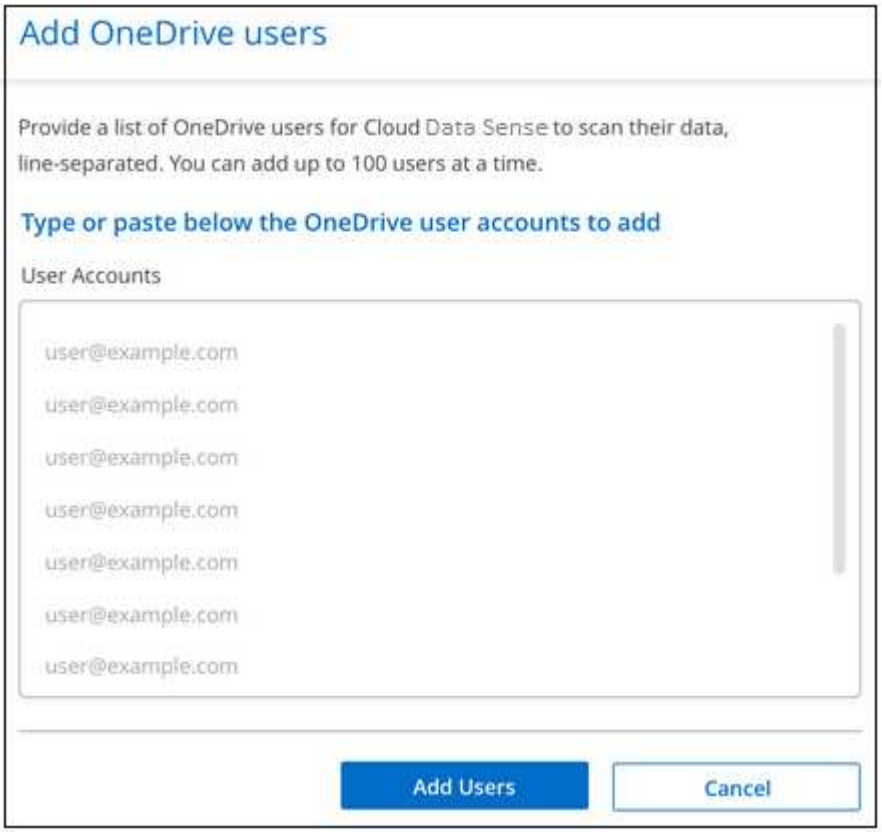


OneDrive アカウントからユーザーを追加する場合は、 [* OneDrive ユーザーの追加 *] をクリックします。



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

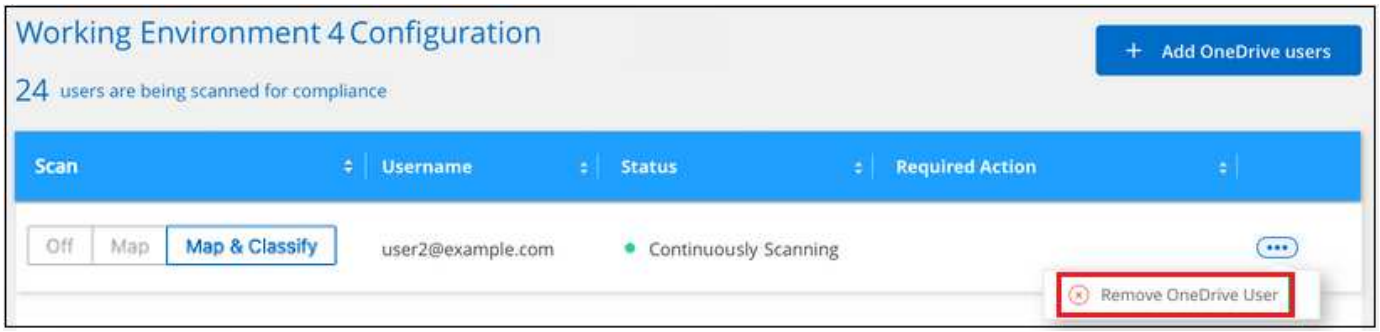
終了：	手順：
ユーザファイルのスキャンを無効にします	[* Off *] をクリックします

結果

BlueXPの分類により、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と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。



できることに注意してください "BlueXPの分類からOneDriveアカウント全体を削除します" OneDriveアカウントからユーザーデータをスキャンする必要がなくなった場合。

SharePoint アカウントをスキャンしています

BlueXPで分類されたSharePoint OnlineアカウントとSharePointオンプレミスアカウント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。

1 **SharePoint**の前提条件を確認する

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

2 **BlueXP**分類インスタンスを導入します

"BlueXP分類を導入します" インスタンスが展開されていない場合。

3 **SharePoint**アカウントにログインします

資格のあるユーザクレデンシャルを使用して、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。

4 スキャンする**SharePoint**サイトの**URL**を追加します

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、アカウントごとに合計1,000個のサイトを追加できます。

SharePoint の要件を確認する

SharePointアカウントでBlueXP分類をアクティブ化する準備ができていることを確認するには、次の前提条件を確認してください。

- 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ユーザーのログイン資格情報が必要です。
  - SharePoint Onlineの場合、管理者以外のアカウントを使用できますが、スキャンするすべてのSharePointサイトにアクセスするには、そのユーザーに権限が必要です。
- SharePoint On-Premiseについては、SharePoint ServerのURLも必要です。
- 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。

BlueXP分類インスタンスの導入

導入されているインスタンスがない場合は、BlueXP分類を導入します。

- SharePoint Onlineでは、BlueXPは次のように分類できます "クラウドに導入"。
- オンプレミスのSharePointの場合は、BlueXPの分類をインストールできます "インターネットにアクセスできるオンプレミスの場所" または "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"。

インターネットにアクセスできないサイトにBlueXP分類がインストールされている場合は、インターネットにアクセスできない同じサイトにもBlueXP Connectorをインストールする必要があります。 "詳細はこちら。"。

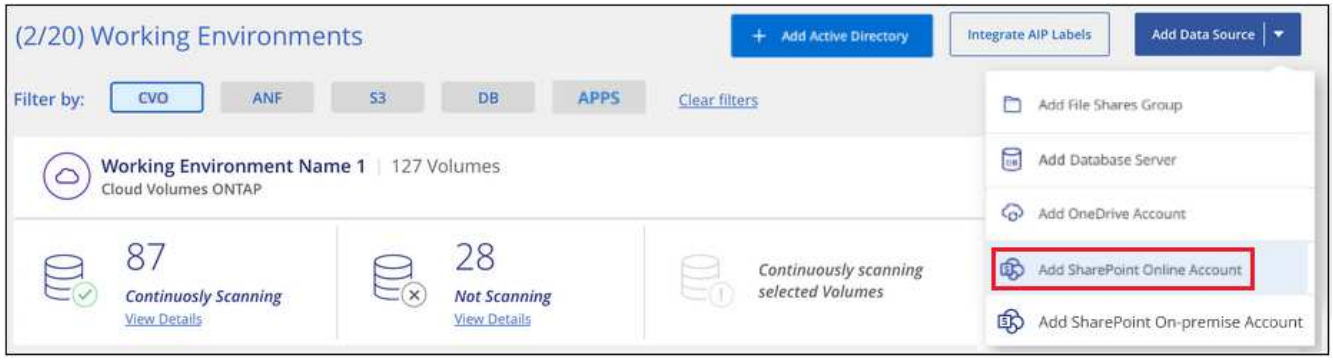
インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

SharePoint Onlineアカウントを追加する

ユーザーファイルが存在するSharePoint Online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。



ボタンをクリックできる[構成]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. 表示された[Microsoft]ページで、SharePointアカウントを選択してユーザとパスワード（管理者ユーザまたはSharePointサイトにアクセスできる他のユーザ）を入力し、*[同意する]*をクリックしてBlueXP分類によるこのアカウントからのデータの読み取りを許可します。

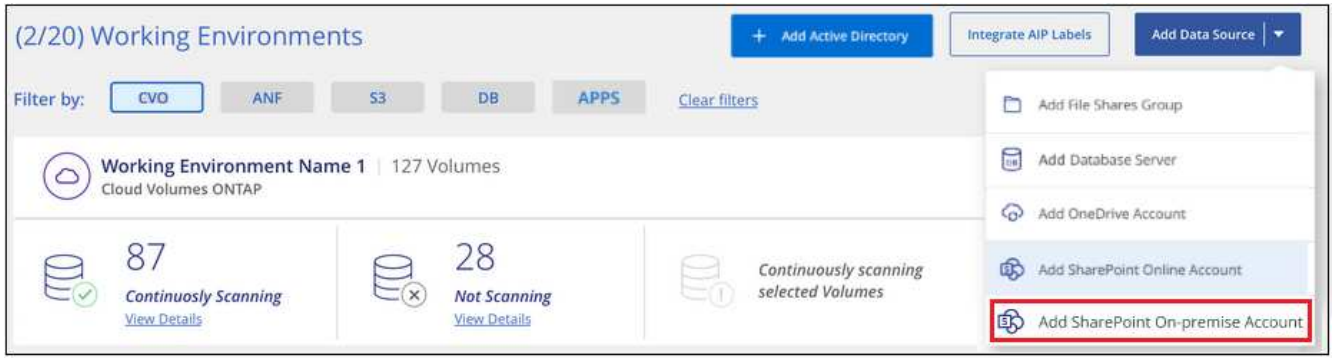
SharePoint Onlineアカウントが作業環境のリストに追加されます。

SharePointオンプレミスアカウントを追加する

ユーザーファイルが存在するSharePointオンプレミスアカウントを追加します。

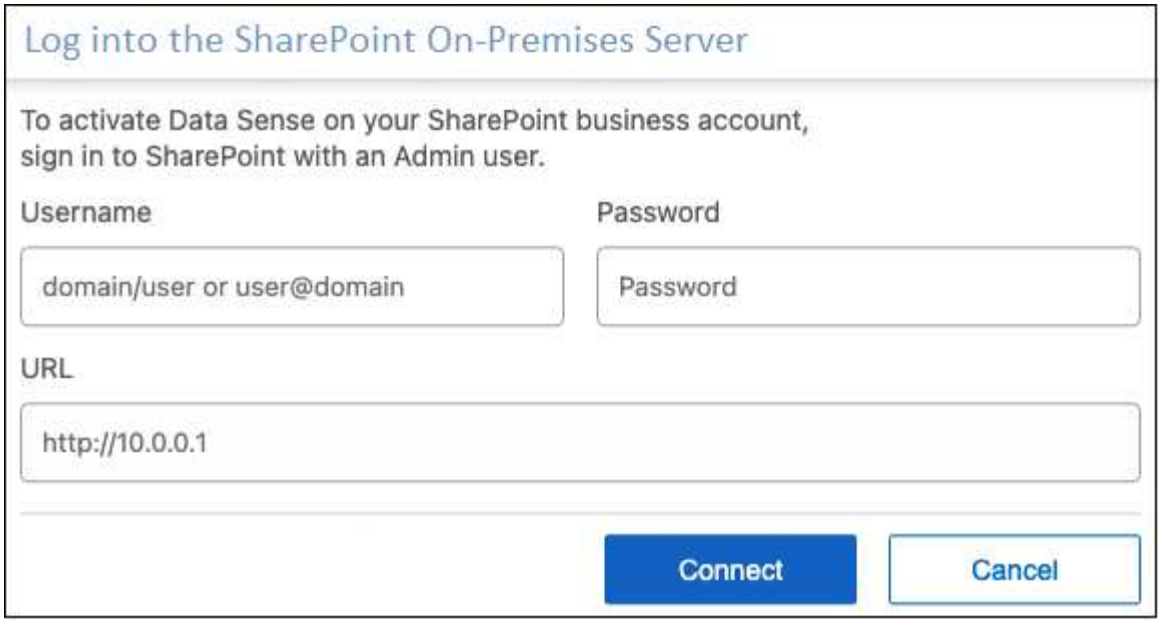
手順

1. [作業環境の構成]ページで、[データソースの追加>* SharePointオンプレミスアカウントの追加*]をクリックします。



ボタンをクリックできる[構成]ページのスクリーンショット。"]

2. [SharePoint On-Premise Server]ダイアログで、次の情報を入力します。
   - 「domain/user」または「user@domain」の形式の管理ユーザとadminパスワード
   - SharePoint ServerのURL



3. [接続] をクリックします。

SharePointのオンプレミスアカウントが作業環境のリストに追加されます。

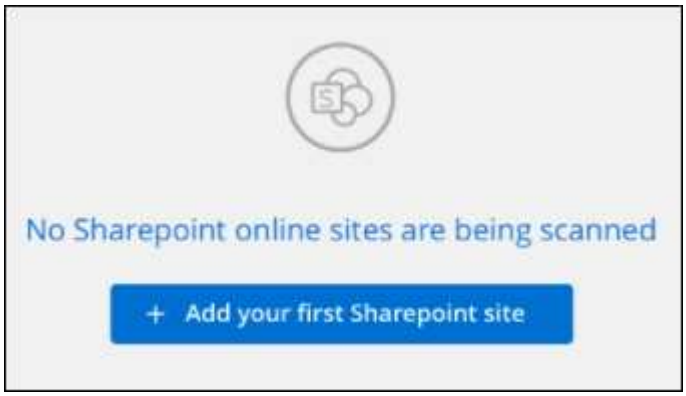
SharePoint サイトをコンプライアンススキャンに追加する

個 々 のSharePointサイトを追加することも、アカウントに最大1、000のSharePointサイトを追加して、関連するファイルがBlueXPの分類によってスキャンされるようにすることもできます。SharePoint OnlineサイトとSharePointオンプレミスサイトのどちらを追加する場合でも、手順は同じです。

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。

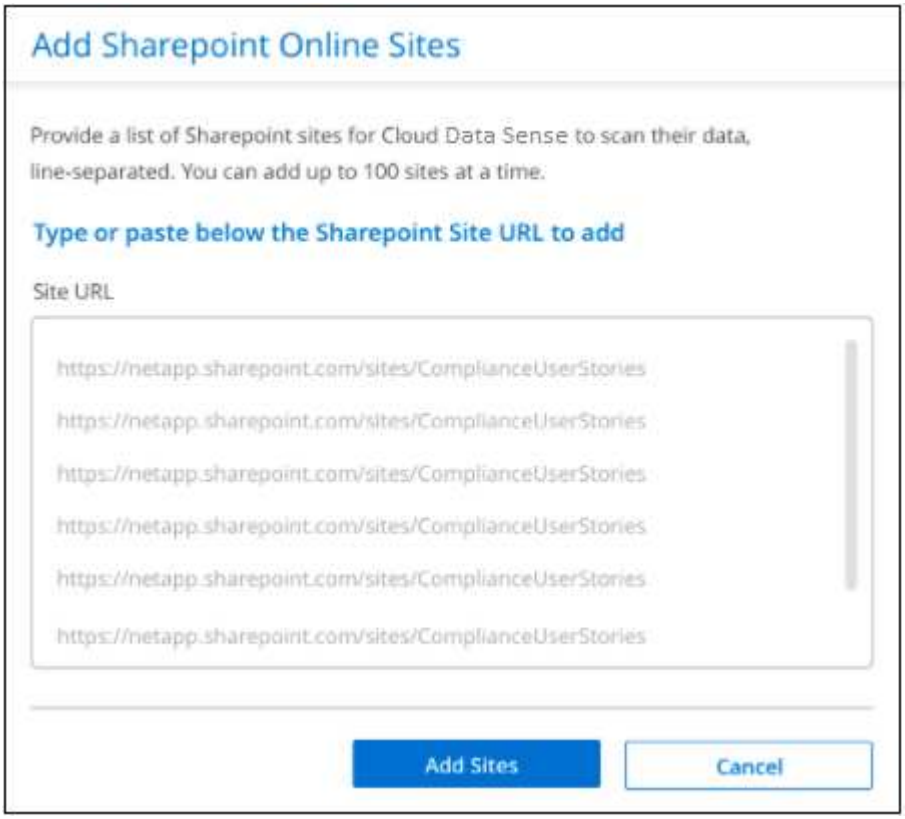


ボタンを示すスクリーンショット。"]

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。



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. このアカウントに100を超えるサイトを追加する必要がある場合は、[SharePointサイトの追加]*をもう一度クリックして、このアカウントのすべてのサイトを追加します(アカウントごとに合計1,000サイトまで)。
5. 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。

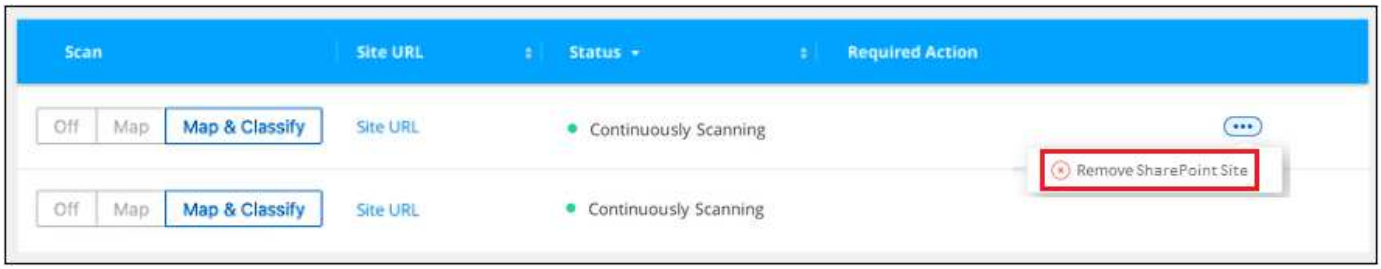
終了：	手順：
ファイルのマッピングのみのスキャンを有効にします	[* マップ *] をクリックします
ファイルのフルスキャンを有効にします	[マップと分類 *] をクリックします
ファイルのスキャンを無効にします	[* Off *] をクリックします

結果

BlueXPの分類により、追加したSharePointサイト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と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。



できることに注意してください "BlueXP分類からSharePointアカウント全体を削除します" SharePointアカウントからユーザーデータをスキャンする必要がなくなった場合。

Googleドライブアカウントをスキャンしています

BlueXP分類を使用してGoogleドライブアカウントのユーザ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。

1 **Google**ドライブの前提条件を確認します

Googleドライブ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ます。

2 **BlueXP**分類を導入します

"BlueXP分類を導入します" インスタンスが展開されていない場合。

Googleドライブアカウントにログインします

Adminユーザのクレデンシャルを使用して、アクセスするGoogle Driveアカウントにログインし、新しいデータソースとして追加します。

ユーザファイルのスキャンタイプを選択します

ユーザファイルで実行するスキャンのタイプ（マッピングまたはマッピングおよび分類）を選択します。

Googleドライブの要件を確認する

次の前提条件を確認して、Google DriveアカウントでBlueXPの分類を有効にする準備ができていることを確認してください。

- ユーザのファイルへの読み取りアクセスを提供するGoogle Drive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

現在の制限

BlueXPの次の分類機能は、現在Google Driveファイルではサポートされていません。

- [データ調査]ページでファイルを表示している場合、ボタンバーのアクションはアクティブになりません。ファイルのコピー、移動、削除などはできません。
- Googleドライブ内のファイル内で権限を識別できないため、［調査］ページに権限情報は表示されません。

BlueXP分類の導入

導入されているインスタンスがない場合は、BlueXP分類を導入します。

BlueXPには次のように分類できます "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"。

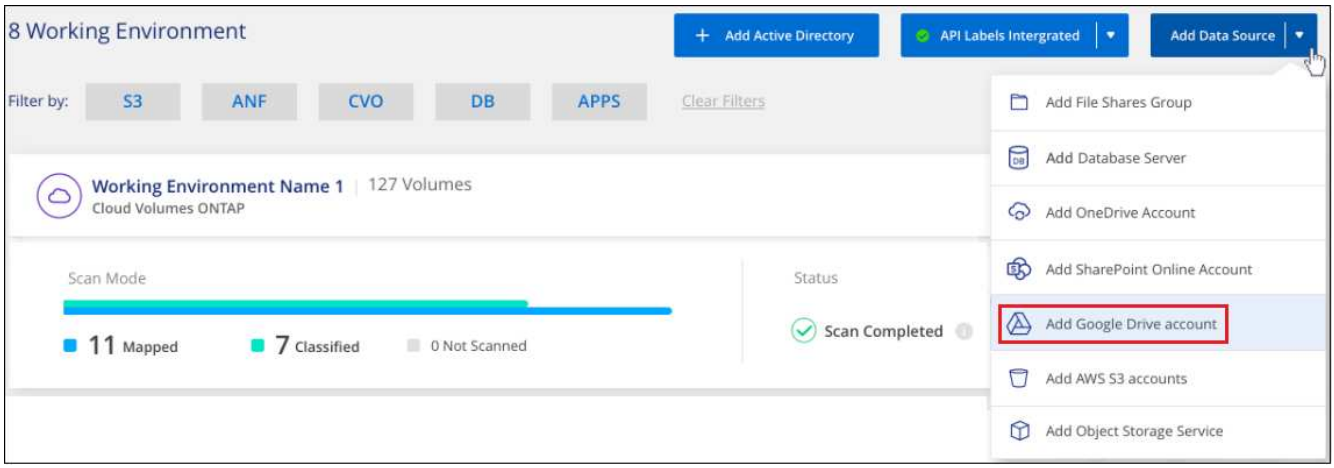
インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

Google Drive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Googleドライブアカウントを追加します。複数のユーザーからファイルをスキャンする場合は、ユーザーごとにこの手順を実行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>* Googleドライブアカウントの追加*]をクリックします。



2. [Googleドライブアカウントの追加]ダイアログで、[Googleドライブへのサインイン*]をクリックします。
3. 表示された[Google]ページで、Google Driveアカウントを選択して必要な管理者ユーザとパスワードを入力し、*[同意する]*をクリックしてBlueXP分類によるこのアカウントからのデータの読み取りを許可します。

Googleドライブアカウントが作業環境のリストに追加されます。

ユーザデータのスキャンタイプを選択しています

BlueXPで分類されるユーザのデータに対して実行するスキャンのタイプを選択します。

手順

1. _Configuration_pageで、Google Driveアカウントの* Configuration *ボタンをクリックします。

2. Google Driveアカウントのファイルに対して、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

結果

BlueXPの分類により、追加したGoogle Driveアカウント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と他の場所に表示されます。

Googleドライブアカウントをコンプライアンススキャンから削除しています

1人のユーザーのGoogleドライブファイルのみが1つのGoogleドライブアカウントの一部であるため、ユーザーのGoogleドライブアカウントからのファイルのスキャンを停止する場合は、次の手順を実行します "BlueXP分類からGoogle Driveアカウントを削除します"。

ファイル共有をスキャンしています

ネットアップ以外のNFSまたはCIFSファイル共有のスキャンをBlueXPで直接開始するには、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。

1 ファイル共有の前提条件を確認する

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。

2 **BlueXP**分類インスタンスを導入します

"BlueXP分類を導入します" インスタンスが展開されていない場合。

3 ファイル共有を保持するグループを作成します

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。

4 ファイル共有をグループに追加します

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

BlueXPの分類を有効にする前に、次の前提条件を確認して、サポートされる構成があることを確認してください。

- 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。ほとんどの場合、これらはネットアップ以外のストレージシステムに存在するファイル共有です。ただし、古いNetApp 7-Modeストレージシ

ステムのCIFS共有はファイル共有としてスキャンできます。

BlueXPの分類では、7-Modeシステムから権限や「最終アクセス時間」を抽出することはできません。また、7-ModeシステムのLinuxバージョンとCIFS共有の問題 は既知のものであるため、NTLM認証が有効なSMB v1のみを使用するように共有を設定する必要があります。

- BlueXP分類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。
- 次のポートがBlueXP分類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
- DFS（Distributed File System）共有を通常のCIFS共有として追加できます。ただし、BlueXPの分類では、共有が複数のサーバ/ボリュームを1つのCIFS共有として組み合わせて構築されていることを認識していないため、別のサーバ/ボリュームにあるフォルダ/共有の1つだけを環境というメッセージが表示された場合に、共有に関する権限や接続のエラーが表示されることがあります。
- 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。BlueXPの分類で昇格された権限が必要なデータをスキャンする必要がある場合に備えて、管理者クレデンシャルが推奨されます。

  BlueXPの分類スキャンでファイルの「最終アクセス日時」が変更されないようにするには、CIFSではWrite Attributes権限、NFSではwrite権限を持つことを推奨します。可能であれば、すべてのファイルに対する権限を持つ組織内の親グループにActive Directory構成ユーザーを含めることをお勧めします。

- 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。

BlueXP分類インスタンスの導入

導入されているインスタンスがない場合は、BlueXP分類を導入します。

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 "BlueXPの分類機能をクラウドに導入します" 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にBlueXPの分類を導入します"。

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 "インターネットアクセスのないオンプレミスと同じ場所にBlueXPの分類を導入します"。また、BlueXPコネクタがオンプレミスの同じ場所に配置されている必要があります。

インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

ファイル共有のグループを作成します

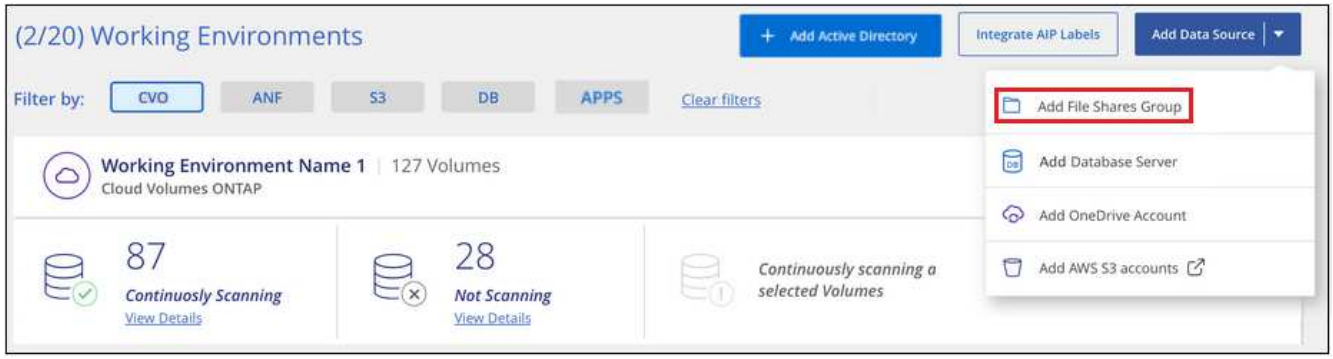
ファイル共有を追加する前に、「 group 」というファイル共有を追加する必要があります。グループはスキャンするファイル共有のコンテナであり、グループ名はそれらのファイル共有の作業環境名として使用されます。

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して、それらの共有内のファイルがBlueXPの分類でスキャンされるようにします。共有は、の形式で追加します `<host_name>:/<share_path>`。

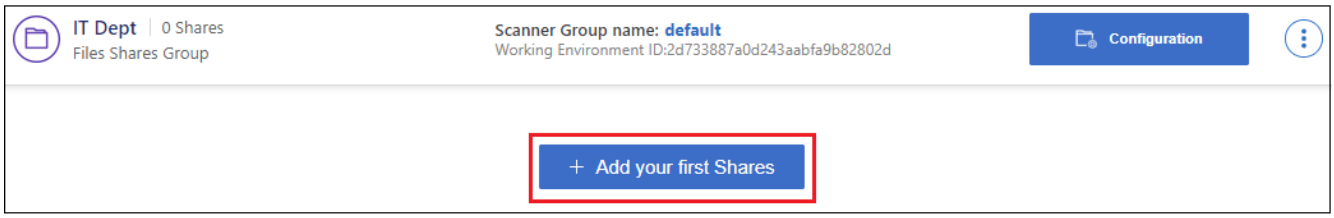
個々のファイル共有を追加することも、スキャンするファイル共有を 1 行で区切って指定することもできます。一度に最大 100 個の共有を追加できます。

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。



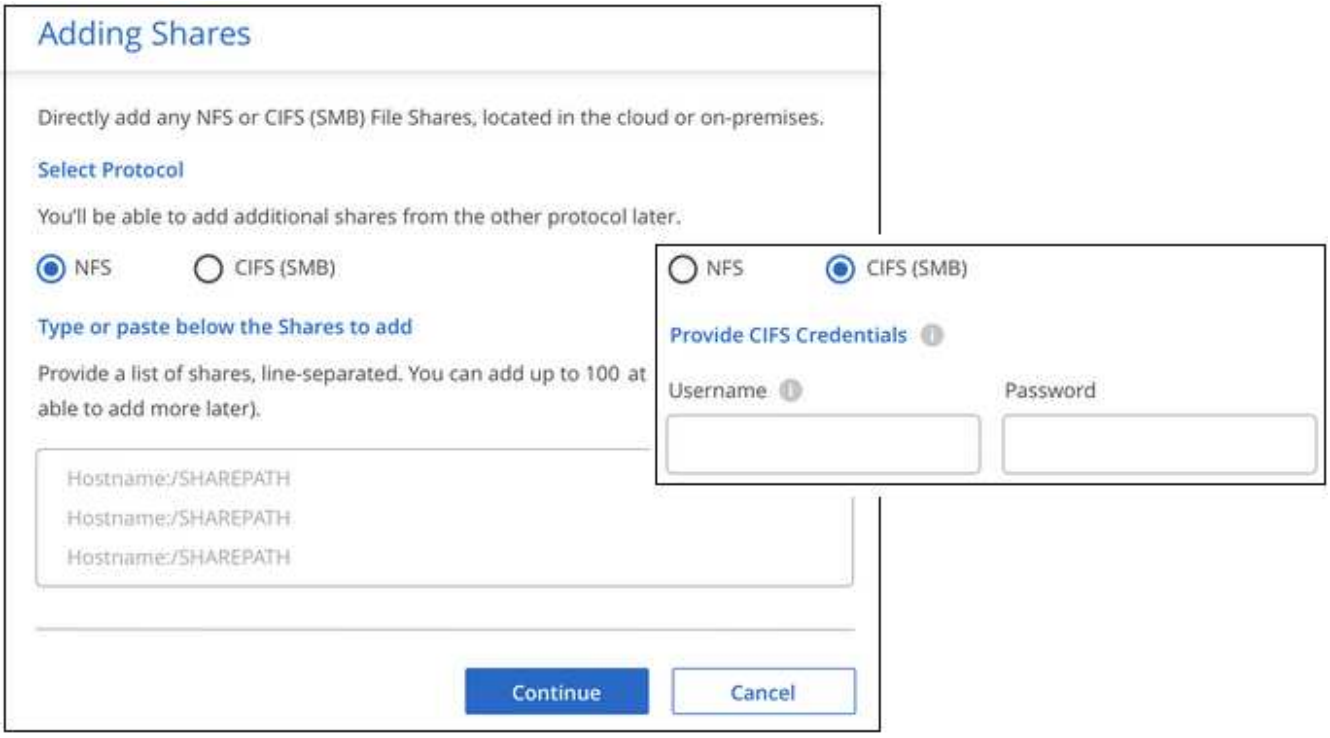
ボタンを示すスクリーンショット。"]

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

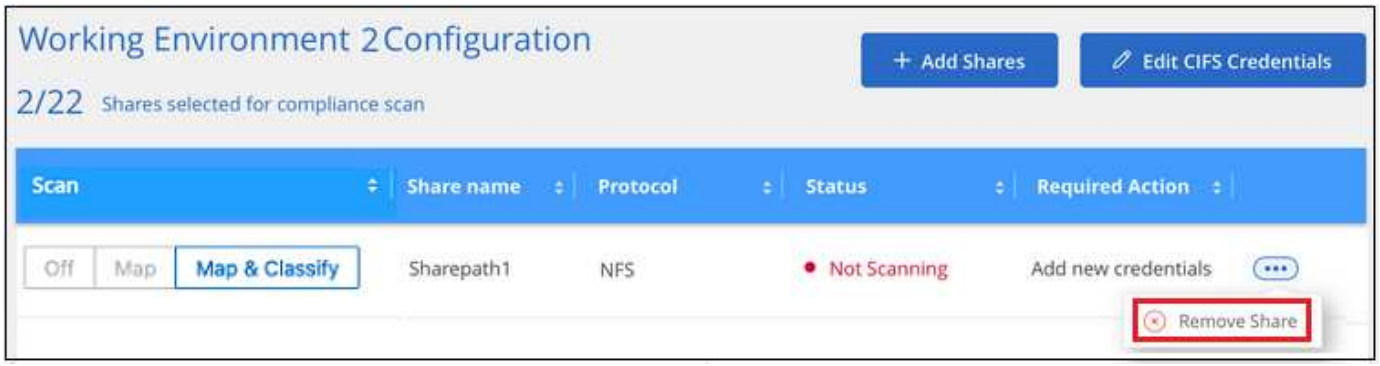
「属性の書き込み」権限がない場合にスキャンする*のページ上部のスイッチは、デフォルトでは無効になっています。つまり、BlueXPの分類にCIFSの属性への書き込み権限やNFSの書き込み権限がない場合、BlueXPの分類では「最終アクセス時間」を元のタイムスタンプに戻すことができないため、ファイルはスキャンされません。最終アクセス時間がリセットされても構わない場合は、スイッチをオンにすると、権限に関係なくすべてのファイルがスキャンされます。 "詳細はこちら。"。

結果

BlueXPの分類により、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、結果がダッシュボードと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

いくつかの手順を実行して、BlueXPの分類を使用してオブジェクトストレージ内のデータの直接スキャンを開始します。BlueXPの分類では、Simple Storage Service（S3）プロトコルを使用する任意のオブジェクトストレージサービスのデータをスキャンできます。これには、NetApp StorageGRID 、IBM Cloud Object Store、Linode、B2クラウドストレージ、Amazon S3などが含まれます。

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。

1. オブジェクトストレージの前提条件を確認する

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。

BlueXP分類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のアクセスキーとシークレットキーが必要です。

2. **BlueXP**分類インスタンスを導入します

"BlueXP分類を導入します" インスタンスが展開されていない場合。

3. オブジェクトストレージサービスを追加します

オブジェクトストレージサービスをBlueXP分類に追加します。

4. 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、BlueXPの分類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

BlueXPの分類を有効にする前に、次の前提条件を確認して、サポートされる構成があることを確認してください。

- 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。
- BlueXP分類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のアクセスキーとシークレットキーが必要です。

BlueXP分類インスタンスの導入

導入されているインスタンスがない場合は、BlueXP分類を導入します。

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 "BlueXPの分類機能をクラウドに導入します" 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にBlueXPの分類を導入します"。

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 "インターネットアクセスのないオンプレミスと同じ場所にBlueXPの分類を導入します"。また、BlueXPコネクタがオンプレミスの同じ場所に配置されている必要があります。

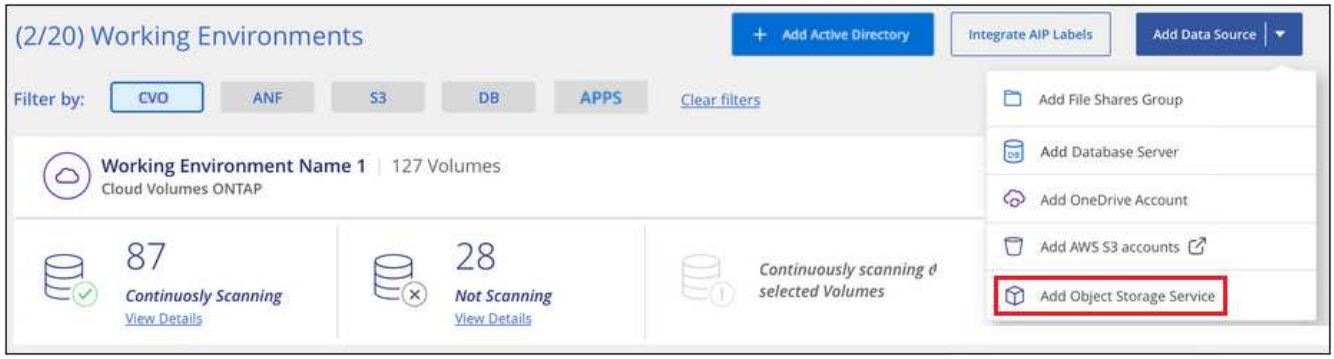
インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

オブジェクトストレージサービスを**BlueXP**分類に追加しています

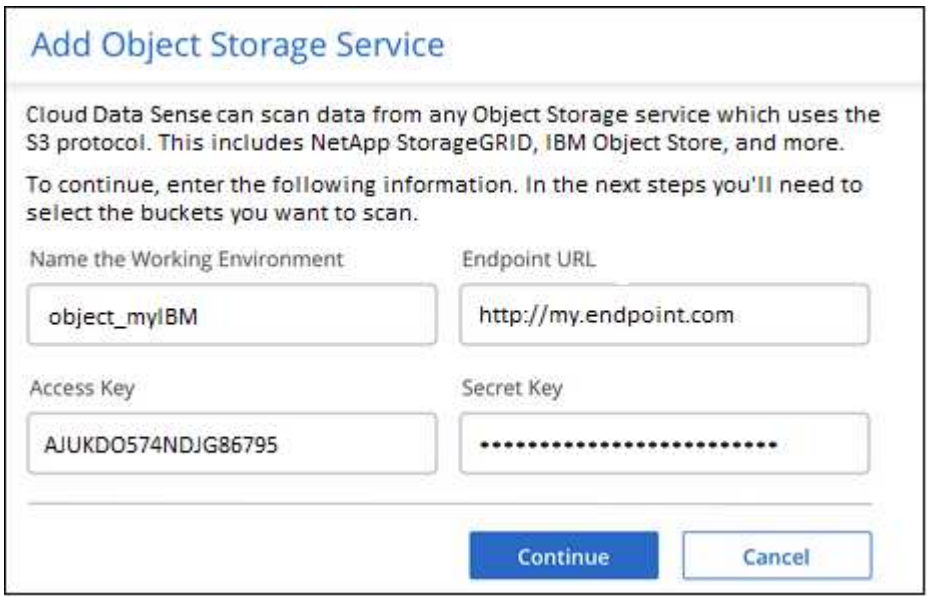
オブジェクトストレージサービスを追加します。

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. [Access Key]と[Secret Key]を入力して、BlueXPの分類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します。



結果

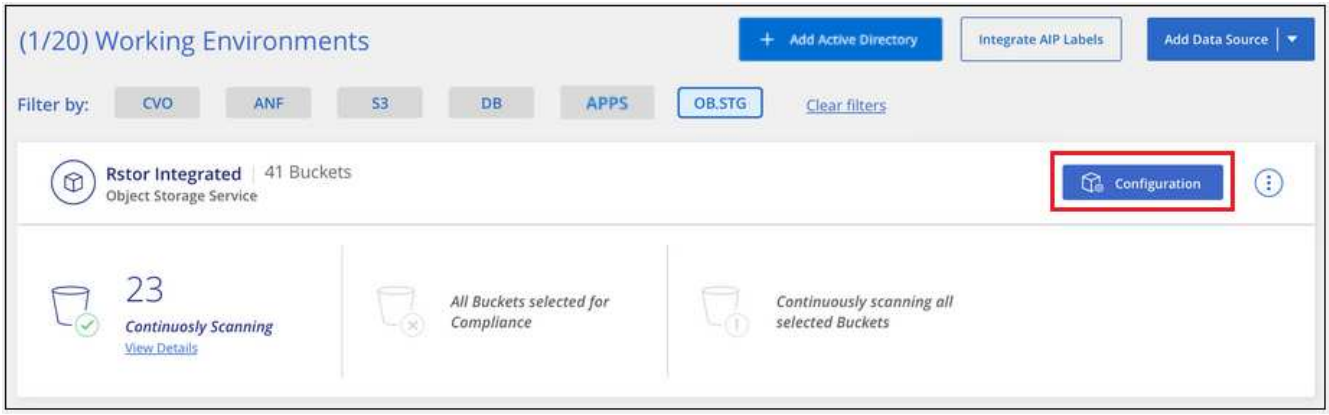
新しいオブジェクトストレージサービスが作業環境のリストに追加されます。

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

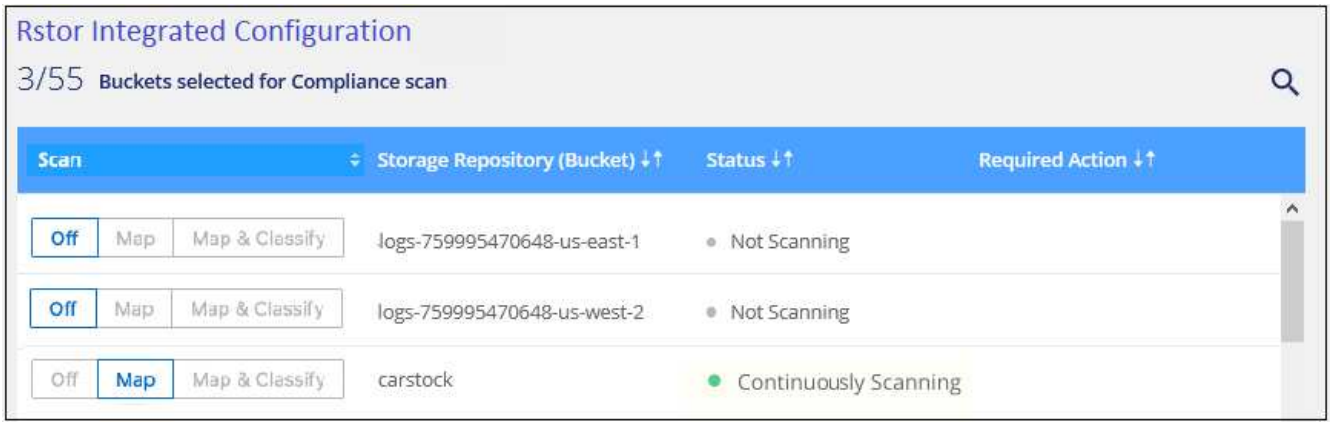
オブジェクトストレージサービスでBlueXPの分類を有効にしたら、次の手順でスキャンするバケットを設定します。BlueXPの分類により、該当するバケットが検出され、作成した作業環境に表示されます。

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。



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

結果

BlueXPの分類で、有効にした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。