データソースのスキャンを有効にする

NetApp Data Classification

NetApp
February 11, 2026

目次

データソースのスキャンを有効にする

NetApp Data Classificationでデータソースをスキャン

NetApp Data Classification は、選択したリポジトリ内のデータ (ボリューム、データベース スキーマ、またはその他のユーザー データ) をスキャンして、個人データや機密データを識別します。次に、データ分類により組織のデータがマッピングされ、各ファイルが分類され、データ内の定義済みパターンが識別されます。スキャンの結果は、個人情報、機密個人情報、データ カテゴリ、およびファイル タイプのインデックスです。

最初のスキャンの後、データ分類はラウンドロビン方式でデータを継続的にスキャンし、増分変更を検出します。そのため、インスタンスを実行し続けることが重要です。

ボリューム レベルまたはデータベース スキーマ レベルでスキャンを有効または無効にすることができます。

マッピングスキャンと分類スキャンの違いは何ですか？

データ分類では、次の 2 種類のスキャンを実行できます。

- マッピングのみのスキャン は、データの概要のみを提供し、選択されたデータ ソースに対して実行されます。マッピングのみのスキャンでは、ファイルにアクセスして内部のデータを確認する必要がないため、マップおよび分類スキャンよりも時間がかかりません。最初にこれを実行して研究領域を特定し、次にそれらの領域に対してマップと分類のスキャンを実行することをお勧めします。
- マップと分類スキャン は、データの詳細なスキャンを提供します。

以下の表にいくつかの違いを示します。

特徴	スキャンをマップして分類する	マッピングのみのスキャン
スキャン速度	遅い	速い
料金	空き	空き
容量	500 TiB に制限されます*	500 TiB に制限されます*
ファイルの種類と使用容量の一覧	はい	はい
ファイル数と使用容量	はい	はい
ファイルの古さとサイズ	はい	はい
実行する能力"データマッピングレポート"	はい	はい
ファイルの詳細を表示するためのデータ調査ページ	はい	いいえ
ファイル内の名前を検索する	はい	いいえ
作成する"保存されたクエリ"カスタム検索結果を提供する	はい	いいえ
他のレポートを実行する機能	はい	いいえ
ファイルのメタデータを表示する機能**	いいえ	はい

{アスタリスク} データ分類では、スキャンできるデータの量に制限はありません。各コンソール エージェントは、500 TiB のデータのスキャンと表示をサポートします。500TiB以上のデータをスキャンするには、"別のコンソールエージェントをインストールする"それから"別のデータ分類インスタンスをデプロイする"。 + コンソール UI には、単一のコネクタからのデータが表示されます。複数のコンソールエージェントからデータを表示するヒントについては、"複数のコンソールエージェントを操作する" 。

{アスタリスク}{アスタリスク} マッピング スキャン中にファイルから次のメタデータが抽出されます。

- システム
- システムタイプ
- ストレージリポジトリ
- ファイル タイプ
- 使用済み容量
- ファイル数
- ファイル サイズ
- ファイル作成
- ファイルの最終アクセス
- ファイルの最終更新日時
- ファイル発見時刻
- 権限の抽出

ガバナンス ダッシュボードの違い:

特徴	マップと分類	マップ
古いデータ	はい	はい
非ビジネスデータ	はい	はい
重複したファイル	はい	はい
定義済みの保存済みクエリ	はい	いいえ
デフォルトの保存クエリ	はい	はい
DDAレポート	はい	はい
マッピングレポート	はい	はい
感度レベル検出	はい	いいえ
幅広い権限を持つ機密データ	はい	いいえ
オープン権限	はい	はい
データの時代	はい	はい
データのサイズ	はい	はい
カテゴリ	はい	いいえ
ファイルの種類	はい	はい

コンプライアンス ダッシュボードの違い:

特徴	マップと分類	マップ
個人情報	はい	いいえ
機密個人情報	はい	いいえ
プライバシーリスク評価レポート	はい	いいえ
HIPAAレポート	はい	いいえ
PCI DSSレポート	はい	いいえ

調査フィルターの違い:

特徴	マップと分類	マップ
保存されたクエリ	はい	はい
システムタイプ	はい	はい
システム	はい	はい
ストレージリポジトリ	はい	はい
ファイル タイプ	はい	はい
ファイル サイズ	はい	はい
作成時間	はい	はい
発見された時間	はい	はい
最終更新日	はい	はい
最終アクセス	はい	はい
オープン権限	はい	はい
ファイルディレクトリパス	はい	はい
カテゴリ	はい	いいえ
感度レベル	はい	いいえ
識別子の数	はい	いいえ
個人データ	はい	いいえ
機密性の高い個人データ	はい	いいえ
データ主体	はい	いいえ
重複	はい	はい
分類ステータス	はい	ステータスは常に「限られた洞察」です
スキャン分析イベント	はい	はい
ファイルハッシュ	はい	はい
アクセス権を持つユーザーの数	はい	はい
ユーザー/グループの権限	はい	はい
ファイルの所有者	はい	はい
ディレクトリタイプ	はい	はい

NetApp Data Classificationを使用してAmazon FSx for ONTAPボリュームをスキャンする

NetApp Data Classificationを使用してAmazon FSx for ONTAPボリュームをスキャンす

るには、いくつかの手順を実行します。

開始する前に

- データ分類を展開および管理するには、AWS にアクティブなコンソールエージェントが必要です。
- システムの作成時に選択したセキュリティ グループは、データ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。 FSx for ONTAPファイルシステムに接続された ENI を使用して関連付けられたセキュリティグループを見つけ、AWS マネジメント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 エラスティックネットワークインターフェース (ENI)"

- データ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 の場合 - ポート 111 および 2049。
  - CIFS の場合 - ポート 139 および 445。

データ分類インスタンスをデプロイする

"データ分類を展開する"インスタンスがまだデプロイされていない場合。

Data Classification は、AWS のコンソールエージェントおよびスキャンする FSx ボリュームと同じ AWS ネットワークにデプロイする必要があります。

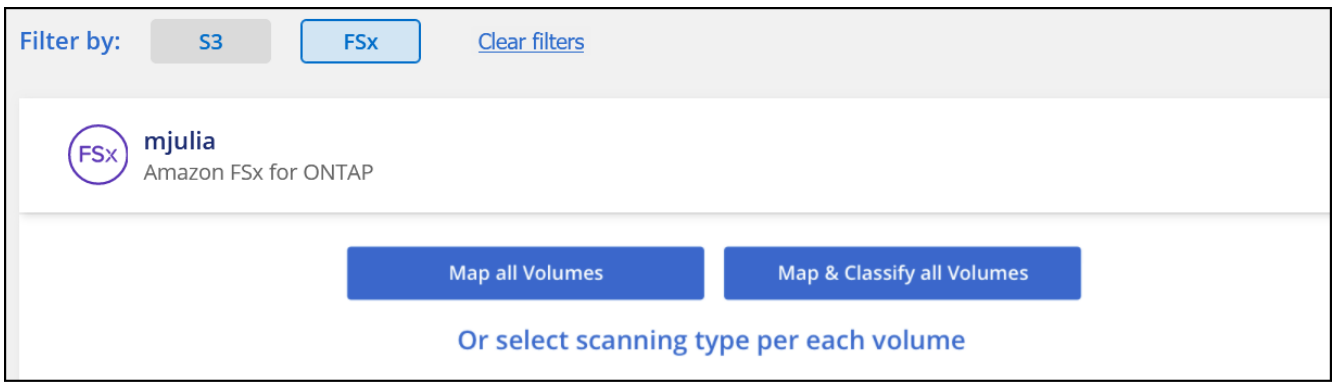
注意: FSx ボリュームをスキャンする場合、オンプレミスの場所でのデータ分類の展開は現在サポートされていません。

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

システムでデータ分類を有効にする

FSx for ONTAPボリュームのデータ分類を有効にすることができます。

1. NetApp Consoleから、*ガバナンス > 分類*を選択します。
2. データ分類メニューから、*構成*を選択します。



タブのスクリーンショット。"]

3. 各システム内のボリュームをスキャンする方法を選択します。"マッピングと分類スキャンについて学ぶ"：
   - 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」を選択します。
   - 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] を選択します。
   - 各ボリュームのスキャンをカスタマイズするには、[または各ボリュームのスキャン タイプを選択] を選択し、マップおよび/または分類するボリュームを選択します。
4. 確認ダイアログボックスで「承認」を選択すると、データ分類によってボリュームのスキャンが開始されます。

結果

データ分類は、システムで選択したボリュームのスキャンを開始します。データ分類が初期スキャンを完了するとすぐに、コンプライアンス ダッシュボードで結果を確認できるようになります。かかる時間はデータの量によって異なり、数分または数時間かかる場合があります。構成 メニューに移動し、システム構成 を選択すると、初期スキャンの進行状況を追跡できます。進行状況バーで各スキャンの進行状況を追跡します。進行状況バーの上にマウスを置くと、ボリューム内のファイルの合計数に対するスキャンされたファイルの数が表示されます。

- デフォルトでは、データ分類に CIFS での属性書き込み権限または NFS での書き込み権限がない場合、データ分類は「最終アクセス時刻」を元のタイムスタンプに戻すことができないため、システムはボリューム内のファイルをスキャンしません。最終アクセス時刻がリセットされても構わない場合は、「またはボリュームごとにスキャン タイプを選択」を選択します。表示されるページには、権限に関係なくデータ分類がボリュームをスキャンするように有効にできる設定があります。
- データ分類では、ボリューム下の 1 つのファイル共有のみをスキャンします。ボリューム内に複数の共有がある場合は、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。"このデータ分類の制限に関する詳細を見る" 。

データ分類がボリュームにアクセスできることを確認する

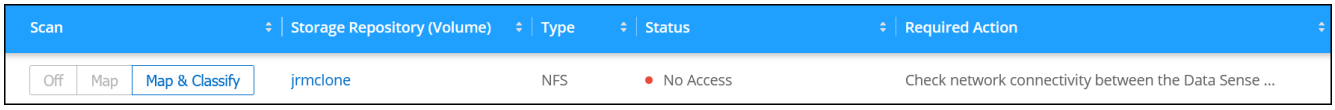
ネットワーク、セキュリティ グループ、エクスポート ポリシーをチェックして、データ分類がボリュームにアクセスできることを確認します。

CIFS ボリュームにアクセスできるようにするには、データ分類に CIFS 資格情報を提供する必要があります。

手順

1. データ分類メニューから、*構成*を選択します。
2. [構成] ページで [詳細の表示] を選択してステータスを確認し、エラーを修正します。

   たとえば、次の画像は、データ分類インスタンスとボリューム間のネットワーク接続の問題により、データ分類がスキャンできないボリュームを示しています。



3. Data Classification 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との間に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、データ分類はコンソールと同じリージョン内のボリュームのみをスキャンできます。

4. NFS ボリュームのエクスポート ポリシーにデータ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、Data Classification に Active Directory 資格情報を提供して、CIFS ボリュームをスキャンできるようにします。

   a. データ分類メニューから、*構成*を選択します。

   b. 各システムについて、「**CIFS** 資格情報の編集」を選択し、データ分類がシステム上の 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。

      資格情報は読み取り専用にすることができますが、管理者の資格情報を提供することで、データ分類は昇格された権限を必要とするすべてのデータを読み取ることができるようになります。資格情報は、データ分類インスタンスに保存されます。

      データ分類スキャンによってファイルの「最終アクセス時刻」が変更されないようにしたい場合は、ユーザーに CIFS での属性書き込み権限または NFS での書き込み権限を与えることをお勧めします。可能であれば、Active Directory ユーザーを、すべてのファイルへの権限を持つ組織内の親グループの一部として構成します。

   資格情報を入力すると、すべての CIFS ボリュームが正常に認証されたことを示すメッセージが表示されます。

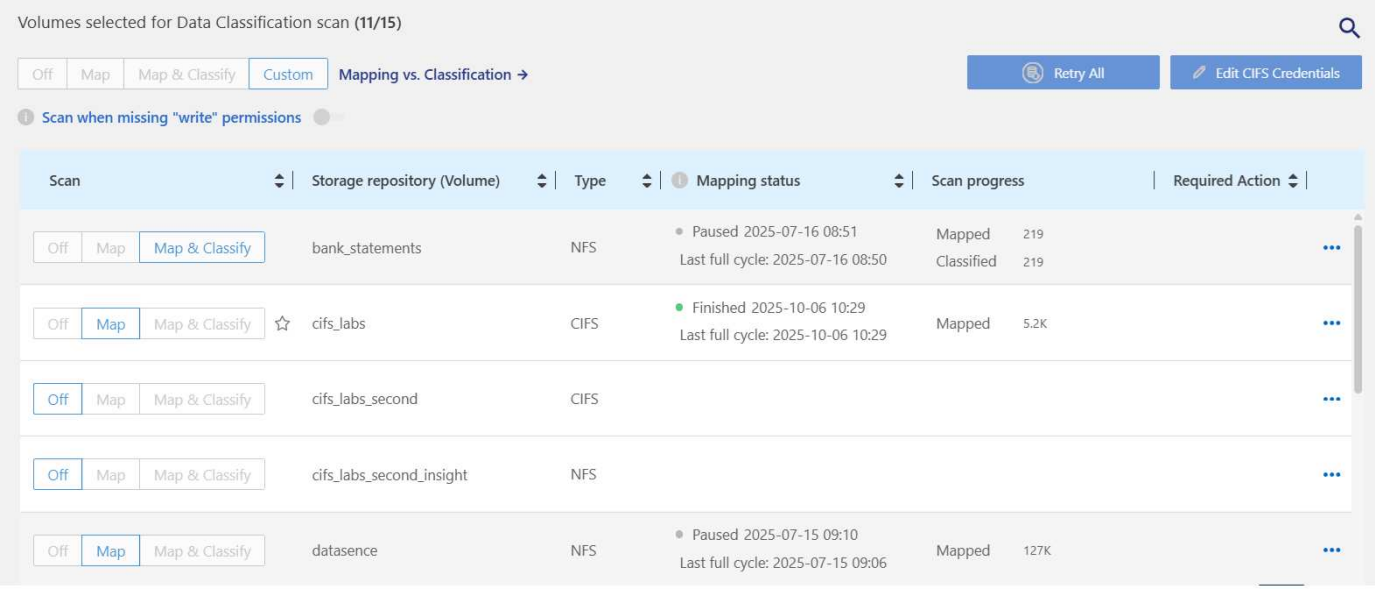
ボリュームのスキャンを有効または無効にする

構成ページからいつでも任意のシステムのスキャンを開始または停止できます。スキャンをマッピングのみのスキャンからマッピングと分類のスキャンに切り替えることも、その逆に切り替えることもできます。システム内のすべてのボリュームをスキャンすることをお勧めします。

システムに追加された新しいボリュームは、見出し領域で マップ または マップと分類 設定を選択した場合にのみ自動的にスキャンされます。見出し領域で カスタム または オフ に設定すると、システムに追加する新しいボリュームごとにマッピングや完全スキャンをアクティブ化する必要があります。

ページ上部の「書き込み権限がない場合にスキャンする」スイッチは、デフォルトで無効になっています。つまり、データ分類に CIFS での属性書き込み権限または NFS での書き込み権限がない場合、データ分類は「最終アクセス時刻」を元のタイムスタンプに戻すことができないため、システムはファイルをスキャンしません。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。"詳細情報"。

システムに追加された新しいボリュームは、見出し領域で マップ または マップと分類 設定を行った場合にのみ自動的にスキャンされます。すべてのボリュームの設定が カスタム または オフ の場合、追加する新しいボリュームごとにスキャンを手動で有効にする必要があります。



手順

1. データ分類メニューから、*構成*を選択します。
2. システムを選択し、*構成*を選択します。
3. すべてのボリュームのスキャンを有効または無効にするには、すべてのボリュームの上にある見出しで [マップ]、[マップと分類]、または [オフ] を選択します。

   個々のボリュームのスキャンを有効または無効にするには、リストでボリュームを見つけて、ボリューム名の横にある [マップ]、[マップと分類]、または [オフ] を選択します。

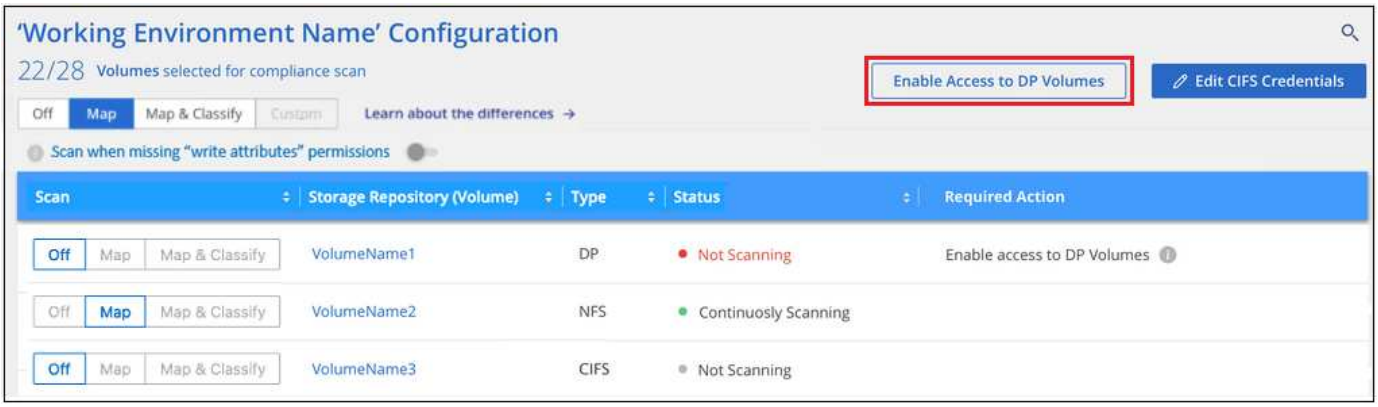
結果

スキャンを有効にすると、データ分類はシステムで選択したボリュームのスキャンを開始します。データ分類がスキャンを開始するとすぐに、コンプライアンス ダッシュボードに結果が表示され始めます。スキャンの完了時間はデータの量に応じて数分から数時間の範囲になります。

データ保護ボリュームをスキャンする

デフォルトでは、データ保護 (DP) ボリュームは外部に公開されておらず、データ分類ではアクセスできないため、スキャンされません。これらは、FSx for ONTAPファイル システムからのSnapMirror操作の宛先ボリュームです。

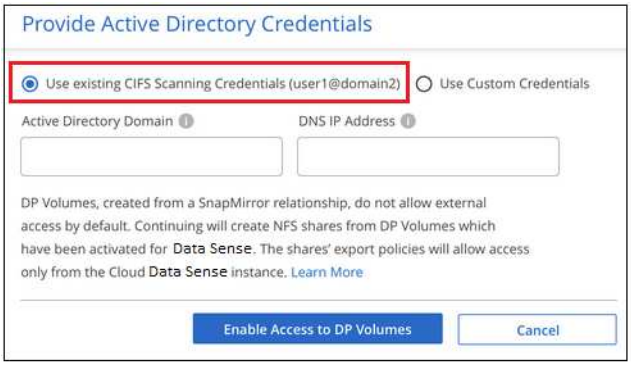
最初、ボリューム リストでは、これらのボリュームが、タイプ **DP**、ステータス スキャンなし、必要なアクション **DP** ボリュームへのアクセスを有効にする として識別されます。

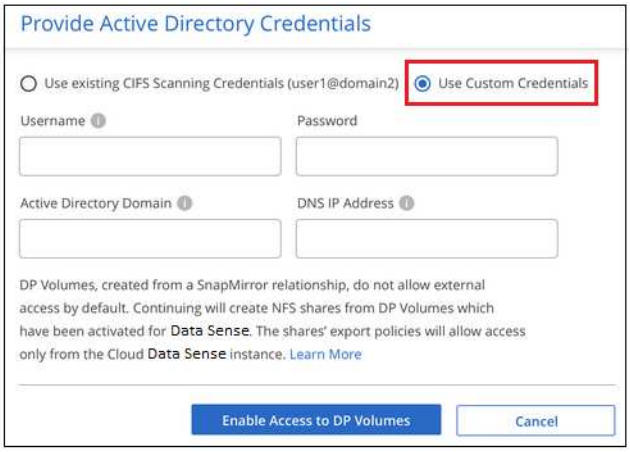


手順

これらのデータ保護ボリュームをスキャンする場合:

1. データ分類メニューから、*構成*を選択します。
2. ページの上部にある*DP ボリュームへのアクセスを有効にする*を選択します。
3. 確認メッセージを確認し、*DP ボリュームへのアクセスを有効にする*を再度選択します。
   - ソース FSx for ONTAPファイル 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 FSx for ONTAPファイル 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 認証情報を入力する必要があります。データ分類が CIFS ボリュームをスキャンできるように Active Directory 資格情報をすでに入力している場合は、その資格情報を使用することも、別の管理者資格情報セットを指定することもできます。





4. スキャンする各 DP ボリュームをアクティブ化します。

結果

有効にすると、データ分類はスキャン用にアクティブ化された各 DP ボリュームから NFS 共有を作成します。共有エクスポート ポリシーでは、データ分類インスタンスからのアクセスのみが許可されます。

最初に DP ボリュームへのアクセスを有効にしたときに CIFS データ保護ボリュームが存在せず、後でボリュームを追加すると、[構成] ページの上部に [**CIFS DP** へのアクセスを有効にする] ボタンが表示されます。このボタンを選択し、CIFS 資格情報を追加して、これらの CIFS DP ボリュームへのアクセスを有効にします。

Active Directory の資格情報は最初の CIFS DP ボリュームのストレージ VM にのみ登録されるため、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 に存在するボリュームには Active Directory 資格情報が登録されていないため、それらの DP ボリュームはスキャンされません。

NetApp Data Classificationを使用してAzure NetApp Filesボリュームをスキャンする

Azure NetApp FilesのNetApp Data Classificationを開始するには、いくつかの手順を完了します。

スキャンするAzure NetApp Filesシステムを検出します

スキャンするAzure NetApp FilesシステムがNetApp Consoleにシステムとしてまだ存在しない場合は、"システムページに追加します" 。

データ分類インスタンスをデプロイする

"データ分類を展開する"インスタンスがまだデプロイされていない場合。

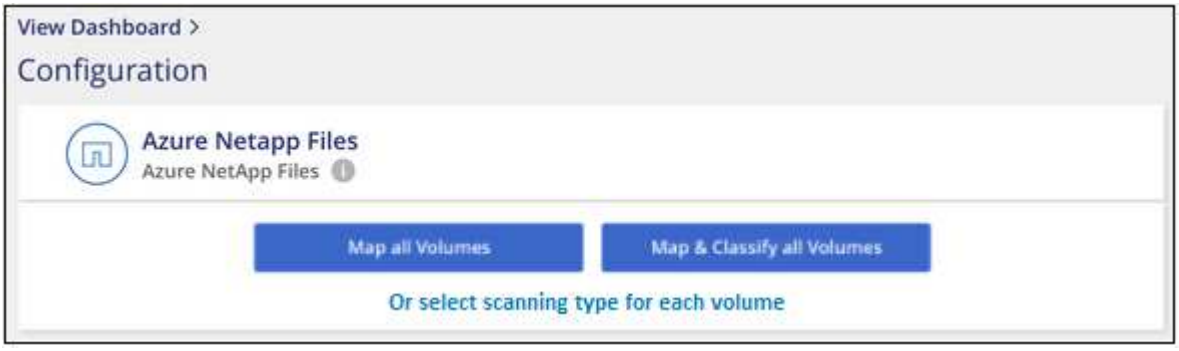
Azure NetApp Filesボリュームをスキャンするときは、データ分類をクラウドにデプロイする必要があり、スキャンするボリュームと同じリージョンにデプロイする必要があります。

注: Azure NetApp Filesボリュームをスキャンする場合、オンプレミスの場所でのデータ分類の展開は現在サポートされていません。

システムでデータ分類を有効にする

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

1. データ分類メニューから、*構成*を選択します。



タブのスクリーンショット。"]

2. 各システム内のボリュームをスキャンする方法を選択します。"マッピングと分類スキャンについて学ぶ" ：
   - 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」を選択します。
   - 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] を選択します。

◦ 各ボリュームのスキャンをカスタマイズするには、[または各ボリュームのスキャン タイプを選択] を選択し、マップするボリューム、またはマップして分類するボリュームを選択します。

見るボリュームのスキャンを有効または無効にする詳細については。

3. 確認ダイアログボックスで*承認*を選択します。

結果

データ分類は、システムで選択したボリュームのスキャンを開始します。データ分類が初期スキャンを完了するとすぐに、コンプライアンス ダッシュボードで結果を確認できます。かかる時間はデータの量によって異なり、数分または数時間かかる場合があります。構成 メニューに移動し、システム構成 を選択すると、初期スキャンの進行状況を追跡できます。データ分類では、スキャンごとに進行状況バーが表示されます。進行状況バーにマウスを移動すると、ボリューム内のファイルの合計数に対するスキャンされたファイルの数が表示されます。

- デフォルトでは、データ分類に CIFS での属性書き込み権限または NFS での書き込み権限がない場合、データ分類は「最終アクセス時刻」を元のタイムスタンプに戻すことができないため、システムはボリューム内のファイルをスキャンしません。最終アクセス時刻がリセットされても構わない場合は、「またはボリュームごとにスキャン タイプを選択」を選択します。表示されるページには、権限に関係なくデータ分類がボリュームをスキャンするように有効にできる設定があります。
- データ分類では、ボリューム下の 1 つのファイル共有のみをスキャンします。ボリューム内に複数の共有がある場合は、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。"データ分類の制限について学ぶ" 。

データ分類が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、エクスポート ポリシーをチェックして、データ分類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、Data Classification に CIFS 資格情報を提供する必要があります。

Azure NetApp Filesの場合、データ分類ではコンソールと同じリージョン内のボリュームのみをスキャンできます。

チェックリスト

- データ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との間にネットワーク接続があることを確認します。
- データ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 の場合 - 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 ポリシーにデータ分類インスタンスの 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ようにします。

手順

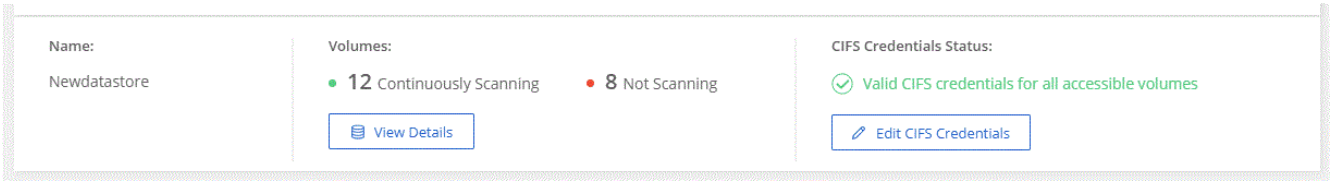
1. データ分類メニューから、*構成*を選択します。

   a. CIFS (SMB) を使用している場合は、Active Directory の資格情報が正しいことを確認してください。各システムについて、「**CIFS** 資格情報の編集」を選択し、データ分類がシステム上の 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。

資格情報は読み取り専用にすることができます。管理者の資格情報を提供することで、データ分類は昇格された権限を必要とするすべてのデータを読み取ることができるようになります。資格情報は、データ分類インスタンスに保存されます。

データ分類スキャンによってファイルの「最終アクセス時刻」が変更されないようにしたい場合は、ユーザーに CIFS での属性書き込み権限または NFS での書き込み権限を与えることをお勧めします。可能であれば、Active Directory ユーザーを、すべてのファイルへの権限を持つ組織内の親グループの一部として構成します。

資格情報を入力すると、すべての CIFS ボリュームが正常に認証されたことを示すメッセージが表示されます。



2. [構成] ページで [詳細の表示] を選択して、各 CIFS ボリュームと NFS ボリュームのステータスを確認します。必要に応じて、ネットワーク接続の問題などのエラーを修正します。

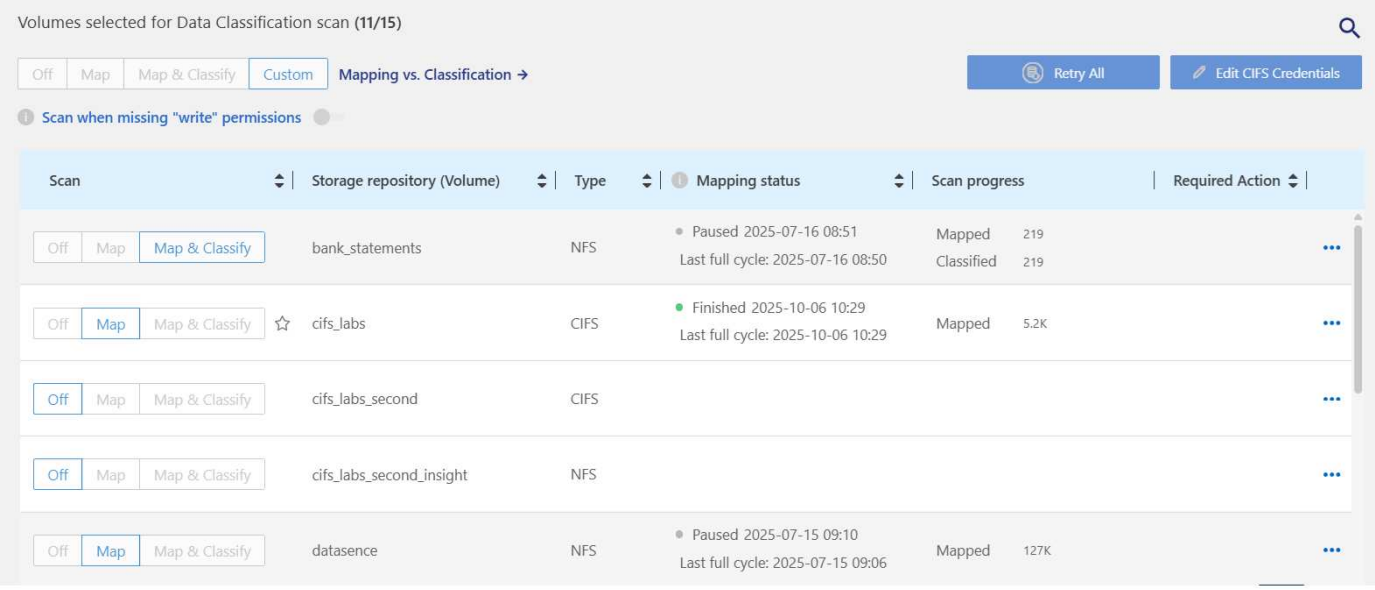
ボリュームのスキャンを有効または無効にする

構成ページからいつでも任意のシステムのスキャンを開始または停止できます。スキャンをマッピングのみのスキャンからマッピングと分類のスキャンに切り替えることも、その逆に切り替えることもできます。システム内のすべてのボリュームをスキャンすることをお勧めします。

システムに追加された新しいボリュームは、見出し領域で マップ または マップと分類 設定を選択した場合にのみ自動的にスキャンされます。見出し領域で カスタム または オフ に設定すると、システムに追加する新しいボリュームごとにマッピングや完全スキャンをアクティブ化する必要があります。

ページ上部の「書き込み権限がない場合にスキャンする」スイッチは、デフォルトで無効になっています。つまり、データ分類に CIFS での属性書き込み権限または NFS での書き込み権限がない場合、データ分類は「最終アクセス時刻」を元のタイムスタンプに戻すことができないため、システムはファイルをスキャンしません。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。"詳細情報"。

システムに追加された新しいボリュームは、見出し領域で マップ または マップと分類 設定を行った場合にのみ自動的にスキャンされます。すべてのボリュームの設定が カスタム または オフ の場合、追加する新しいボリュームごとにスキャンを手動で有効にする必要があります。



手順

1. データ分類メニューから、*構成*を選択します。
2. システムを選択し、*構成*を選択します。
3. すべてのボリュームのスキャンを有効または無効にするには、すべてのボリュームの上にある見出しで [マップ]、[マップと分類]、または [オフ] を選択します。

   個々のボリュームのスキャンを有効または無効にするには、リストでボリュームを見つけて、ボリューム名の横にある [マップ]、[マップと分類]、または [オフ] を選択します。

結果

スキャンを有効にすると、データ分類はシステムで選択したボリュームのスキャンを開始します。データ分類がスキャンを開始するとすぐに、コンプライアンス ダッシュボードに結果が表示され始めます。スキャンの完了時間はデータの量に応じて数分から数時間の範囲になります。

NetApp Data Classificationを使用してCloud Volumes ONTAPとオンプレミスのONTAPボリュームをスキャンします。

NetApp Data Classification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。

前提条件

データ分類を有効にする前に、サポートされている構成があることを確認してください。

- 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のONTAPシステムをスキャンする場合は、"クラウドでデータ分類を展開する"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、"インターネットにアクセスできないオンプレミスの同じ場所にデータ分類を展

開する"。これには、コンソール エージェントを同じオンプレミスの場所に展開する必要があります。

データ分類が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、エクスポート ポリシーをチェックして、データ分類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、データ分類に CIFS 資格情報を提供する必要があります。

チェックリスト

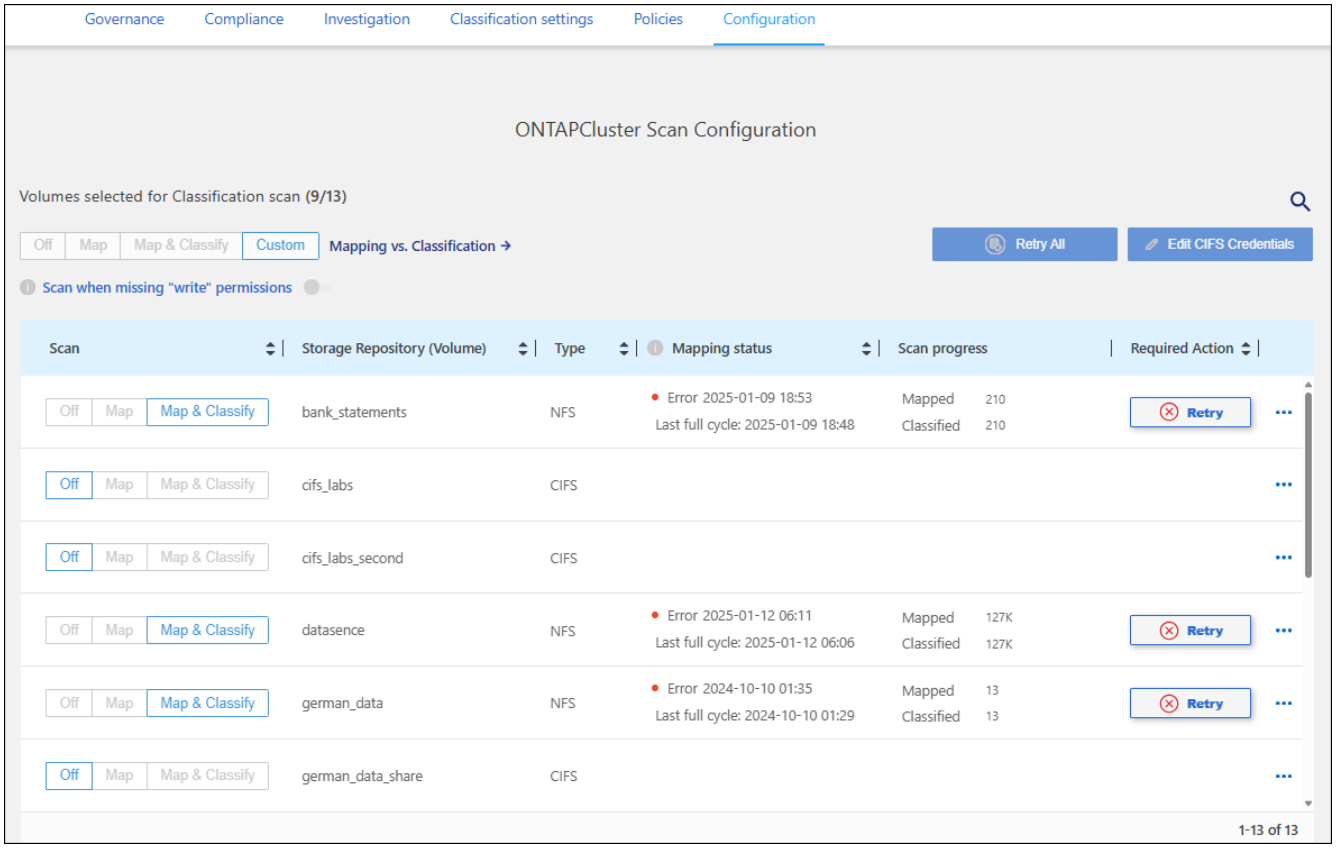
- Data Classification インスタンスと、 Cloud Volumes ONTAPまたはオンプレミスのONTAPクラスターのボリュームを含む各ネットワークとの間にネットワーク接続があることを確認します。
- Cloud Volumes ONTAPのセキュリティ グループが、データ分類インスタンスからの受信トラフィックを許可していることを確認します。

  データ分類インスタンスの IP アドレスからのトラフィックに対してセキュリティ グループを開くことも、仮想ネットワーク内からのすべてのトラフィックに対してセキュリティ グループを開くこともできます。

- NFS ボリューム エクスポート ポリシーにデータ分類インスタンスの 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ようにしていることを確認します。

手順

1. データ分類メニューから、*構成*を選択します。



タブのスクリーンショット。"]

2. CIFS を使用する場合は、Data Classification に Active Directory 資格情報を提供して、CIFS ボリュームをスキャンできるようにします。各システムについて、「**CIFS** 資格情報の編集」を選択し、データ分類が

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。

資格情報は読み取り専用にすることができますが、管理者の資格情報を提供することで、データ分類は昇格された権限を必要とするすべてのデータを読み取ることができるようになります。資格情報は、データ分類インスタンスに保存されます。

データ分類スキャンによってファイルの「最終アクセス時刻」が変更されないようにしたい場合は、ユーザーに CIFS での属性書き込み権限または NFS での書き込み権限を与えることをお勧めします。可能であれば、Active Directory ユーザーを、すべてのファイルへの権限を持つ組織内の親グループの一部として構成します。

資格情報を正しく入力した場合、すべての CIFS ボリュームが正常に認証されたことを確認するメッセージが表示されます。

3. [構成] ページで [構成] を選択し、各 CIFS ボリュームと 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。

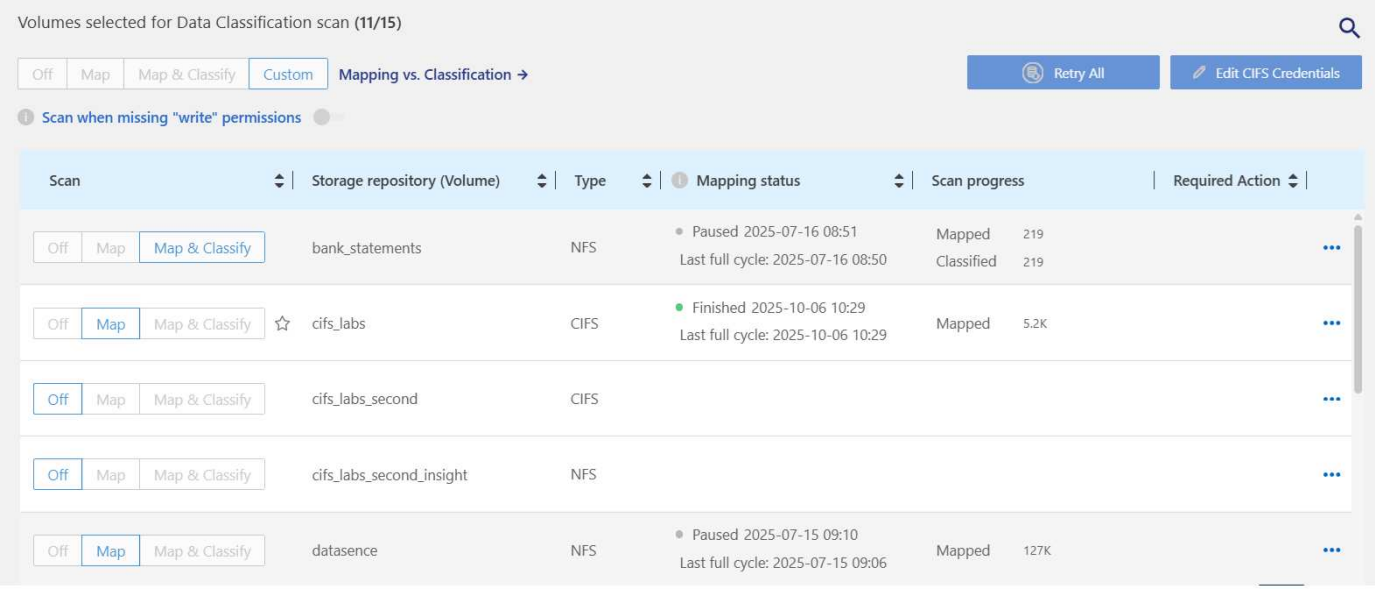
ボリュームのスキャンを有効または無効にする

構成ページからいつでも任意のシステムのスキャンを開始または停止できます。スキャンをマッピングのみのスキャンからマッピングと分類のスキャンに切り替えることも、その逆に切り替えることもできます。システム内のすべてのボリュームをスキャンすることをお勧めします。

システムに追加された新しいボリュームは、見出し領域で マップ または マップと分類 設定を選択した場合にのみ自動的にスキャンされます。見出し領域で カスタム または オフ に設定すると、システムに追加する新しいボリュームごとにマッピングや完全スキャンをアクティブ化する必要があります。

ページ上部の「書き込み権限がない場合にスキャンする」スイッチは、デフォルトで無効になっています。つまり、データ分類に CIFS での属性書き込み権限または NFS での書き込み権限がない場合、データ分類は「最終アクセス時刻」を元のタイムスタンプに戻すことができないため、システムはファイルをスキャンしません。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。"詳細情報"。

システムに追加された新しいボリュームは、見出し領域で マップ または マップと分類 設定を行った場合にのみ自動的にスキャンされます。すべてのボリュームの設定が カスタム または オフ の場合、追加する新しいボリュームごとにスキャンを手動で有効にする必要があります。



手順

1. データ分類メニューから、*構成*を選択します。
2. システムを選択し、*構成*を選択します。
3. すべてのボリュームのスキャンを有効または無効にするには、すべてのボリュームの上にある見出しで [マップ]、[マップと分類]、または [オフ] を選択します。

   個々のボリュームのスキャンを有効または無効にするには、リストでボリュームを見つけて、ボリューム名の横にある [マップ]、[マップと分類]、または [オフ] を選択します。

結果

スキャンを有効にすると、データ分類はシステムで選択したボリュームのスキャンを開始します。データ分類がスキャンを開始するとすぐに、コンプライアンス ダッシュボードに結果が表示され始めます。スキャンの完了時間はデータの量に応じて数分から数時間の範囲になります。

データ分類では、ボリューム下の 1 つのファイル共有のみをスキャンします。ボリューム内に複数の共有がある場合は、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。"このデータ分類の制限に関する詳細を見る" 。

NetApp Data Classificationでデータベーススキーマをスキャンする

NetApp Data Classificationを使用してデータベース 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。

前提条件を確認する

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

サポートされているデータベース

データ分類では、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
- PostgreSQL
- SAP HANA
- SQL サーバー (MSSQL)

データベースで統計収集機能が有効になっている必要があります。

データベース要件

ホストされている場所に関係なく、データ分類インスタンスに接続できるデータベースであればスキャンできます。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 データベースへのアクセスのみ）
- スキーマへの読み取りアクセスを許可する資格情報

  ユーザー名とパスワードを選択するときは、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名とパスワードを選択することが重要です。必要なすべての権限を持つデータ分類システム専用のユーザーを作成することをお勧めします。

MongoDB の場合、読み取り専用の管理者ロールが必要です。

データ分類インスタンスをデプロイする

インスタンスがまだデプロイされていない場合は、データ分類をデプロイします。

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、"クラウドでデータ分類を展開する"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データ分類を展開する"。

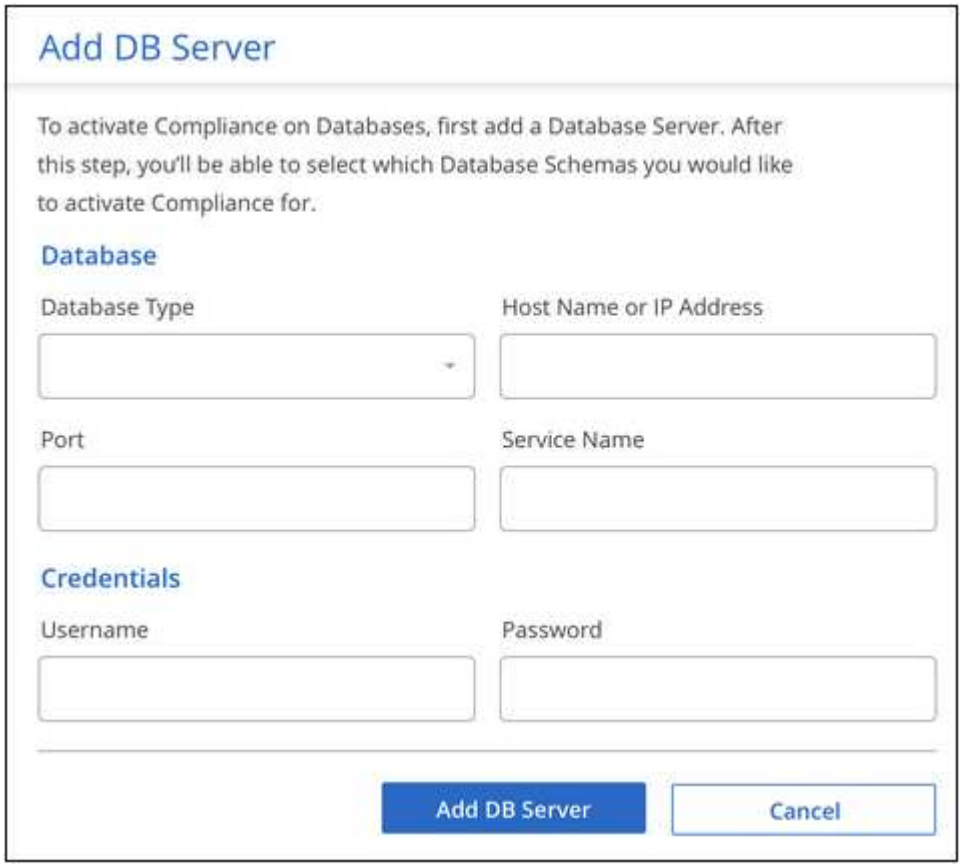
インターネットにアクセスできないダークサイトにインストールされているデータベーススキーマをスキャンする場合は、"インターネットにアクセスできないオンプレミスの同じ場所にデータ分類を展開する" 。これには、コンソール エージェントが同じオンプレミスの場所に展開されていることも必要です。

データベースサーバーを追加する

スキーマが存在するデータベース サーバーを追加します。

1. データ分類メニューから、*構成*を選択します。

2. 構成ページで、システムの追加 > *データベース サーバーの追加*を選択します。
3. データベース サーバーを識別するために必要な情報を入力します。
   a. データベースの種類を選択します。
   b. データベースに接続するためのポートとホスト名または 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. データ分類がサーバーにアクセスできるように資格情報を入力します。
   e. *DB サーバーの追加*を選択します。



データベースがシステムのリストに追加されます。

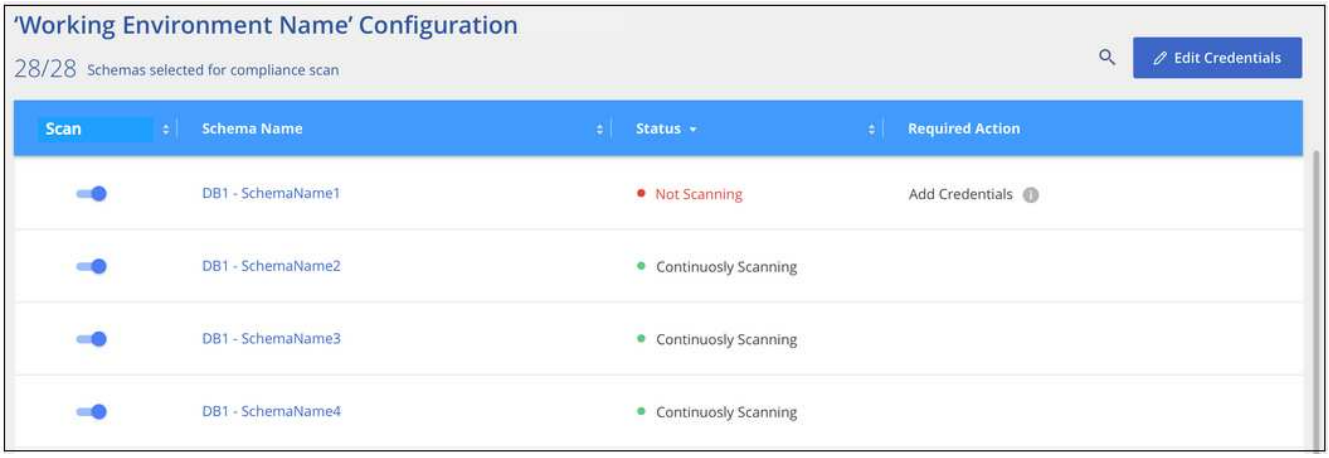
データベーススキーマのスキャンを有効または無効にする

スキーマの完全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 スキーマの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. 構成ページで、構成するデータベースの*構成*ボタンを選択します。

2. スライダーを右に移動して、スキャンするスキーマを選択します。



結果

データ分類は、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。構成 メニューに移動し、システム構成 を選択すると、初期スキャンの進行状況を追跡できます。各スキャンの進行状況は進行状況バーとして表示されます。進行状況バーにマウスを移動すると、ボリューム内のファイルの合計数に対するスキャンされたファイルの数を確認することもできます。エラーがある場合は、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。

データ分類では、データベースを 1 日に 1 回スキャンします。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。

NetApp Data Classificationを使用してGoogle Cloud NetApp Volumesをスキャンする

NetApp Data Classification は、システムとしてGoogle Cloud NetApp Volumes をサポートします。 Google Cloud NetApp Volumesシステムをスキャンする方法を学びます。

スキャンするGoogle Cloud NetApp Volumesシステムを検出します

スキャンしたいGoogle Cloud NetApp VolumesシステムがNetApp Consoleにシステムとしてまだ登録されていない場合は、"システムページに追加する" 。

データ分類インスタンスをデプロイする

"データ分類を展開する"インスタンスがまだデプロイされていない場合。

Google Cloud NetApp Volumesをスキャンするときは、データ分類をクラウドにデプロイする必要があり、スキャンするボリュームと同じリージョンにデプロイする必要があります。

注: Google Cloud NetApp Volumesをスキャンする場合、オンプレミスの場所でのデータ分類の展開は現在サポートされていません。

システムでデータ分類を有効にする

Google Cloud NetApp Volumesシステムでデータ分類を有効にすることができます。

1. データ分類メニューから、*構成*を選択します。
2. 各システム内のボリュームをスキャンする方法を選択します。"マッピングと分類スキャンについて学ぶ"：
   - 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」を選択します。
   - 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] を選択します。
   - 各ボリュームのスキャンをカスタマイズするには、[または各ボリュームのスキャン タイプを選択] を選択し、マップおよび/または分類するボリュームを選択します。

     見るボリュームのスキャンを有効または無効にする詳細については。
3. 確認ダイアログボックスで*承認*を選択します。

結果

データ分類は、システムで選択したボリュームのスキャンを開始します。データ分類が初期スキャンを完了するとすぐに、コンプライアンス ダッシュボードで結果を確認できます。かかる時間はデータの量によって異なり、数分から数時間かかります。初期スキャンの進行状況は、[構成] メニューの [システム構成] セクションで追跡できます。データ分類では、スキャンごとに進行状況バーが表示されます。進行状況バーにマウスを移動すると、ボリューム内のファイルの合計数に対するスキャンされたファイルの数を確認することもできます。

- デフォルトでは、データ分類に CIFS での属性書き込み権限または NFS での書き込み権限がない場合、データ分類は「最終アクセス時刻」を元のタイムスタンプに戻すことができないため、システムはボリューム内のファイルをスキャンしません。最終アクセス時刻がリセットされても構わない場合は、「またはボリュームごとにスキャン タイプを選択」を選択します。表示されるページには、権限に関係なくデータ分類がボリュームをスキャンするように有効にできる設定があります。
- データ分類では、ボリューム下の 1 つのファイル共有のみをスキャンします。ボリューム内に複数の共有がある場合は、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。"データ分類の制限について学ぶ"。

データ分類が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、エクスポート ポリシーを確認して、データ分類がボリュームにアクセスできることを確認します。 CIFS ボリュームの場合、データ分類に CIFS 資格情報を提供する必要があります。

Google Cloud NetApp Volumesの場合、データ分類ではコンソールと同じリージョン内のボリュームのみをスキャンできます。

チェックリスト

- データ分類インスタンスと、 Google Cloud NetApp Volumes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あることを確認します。
- データ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 の場合 - 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 ポリシーにデータ分類インスタンスの 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ようにします。

手順

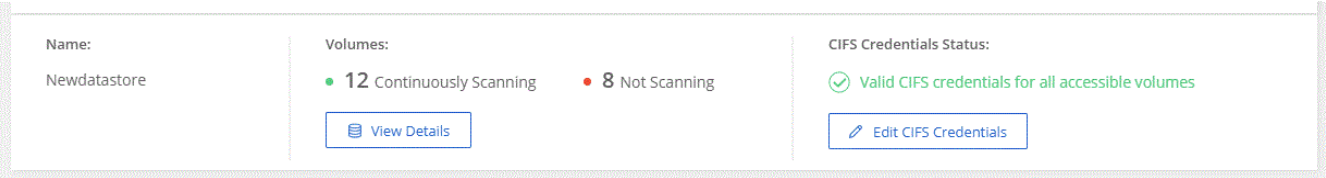
1. データ分類メニューから、*構成*を選択します。

   a. CIFS (SMB) を使用している場合は、Active Directory の資格情報が正しいことを確認してください。各システムについて、「**CIFS** 資格情報の編集」を選択し、データ分類がシステム上の 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。

      資格情報は読み取り専用にすることができますが、管理者の資格情報を提供することで、データ分類は昇格された権限を必要とするすべてのデータを読み取ることができるようになります。資格情報は、データ分類インスタンスに保存されます。

      データ分類スキャンによってファイルの「最終アクセス時刻」が変更されないようにしたい場合は、ユーザーに CIFS での属性書き込み権限または NFS での書き込み権限を与えることをお勧めします。可能であれば、Active Directory ユーザーを、すべてのファイルへの権限を持つ組織内の親グループの一部として構成します。

      資格情報を入力すると、すべての CIFS ボリュームが正常に認証されたことを示すメッセージが表示されます。



2. [構成] ページで [詳細の表示] を選択し、各 CIFS ボリュームと 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。

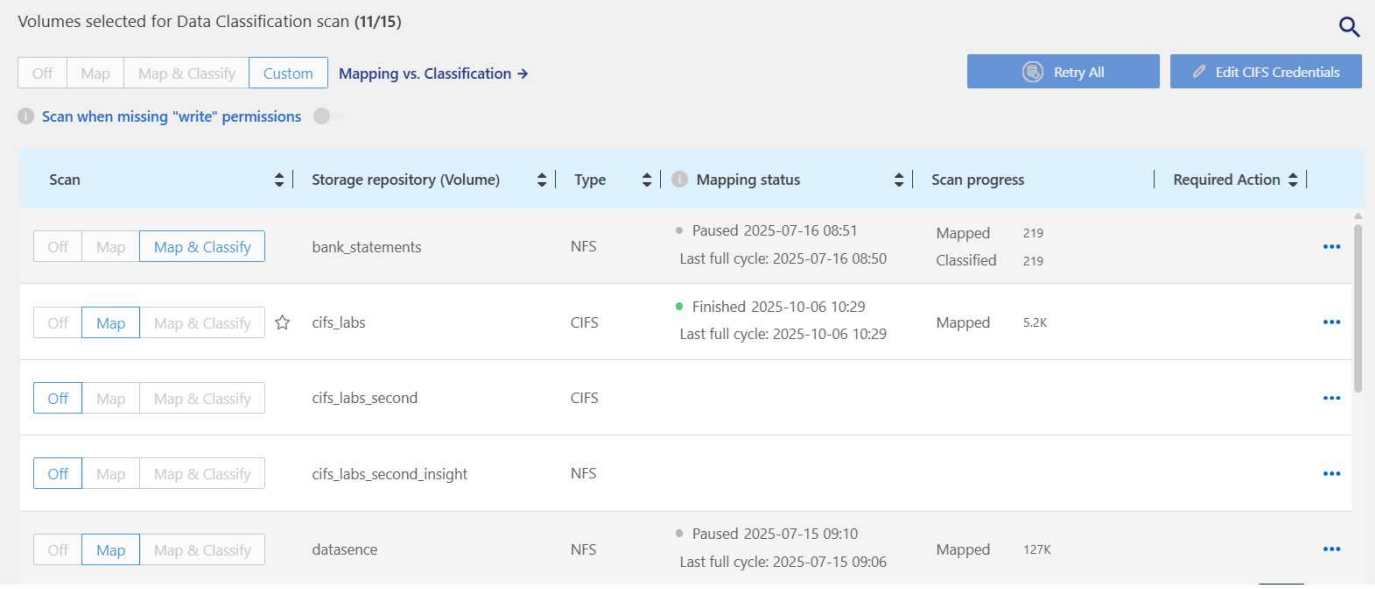
ボリュームのスキャンを有効または無効にする

構成ページからいつでも任意のシステムのスキャンを開始または停止できます。スキャンをマッピングのみのスキャンからマッピングと分類のスキャンに切り替えることも、その逆に切り替えることもできます。システム内のすべてのボリュームをスキャンすることをお勧めします。

システムに追加された新しいボリュームは、見出し領域で マップ または マップと分類 設定を選択した場合にのみ自動的にスキャンされます。見出し領域で カスタム または オフ に設定すると、システムに追加する新しいボリュームごとにマッピングや完全スキャンをアクティブ化する必要があります。

ページ上部の「書き込み権限がない場合にスキャンする」スイッチは、デフォルトで無効になっています。つまり、データ分類に CIFS での属性書き込み権限または NFS での書き込み権限がない場合、データ分類は「最終アクセス時刻」を元のタイムスタンプに戻すことができないため、システムはファイルをスキャンしません。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。"詳細情報"。

システムに追加された新しいボリュームは、見出し領域で マップ または マップと分類 設定を行った場合にのみ自動的にスキャンされます。すべてのボリュームの設定が カスタム または オフ の場合、追加する新しいボリュームごとにスキャンを手動で有効にする必要があります。



手順

1. データ分類メニューから、*構成*を選択します。
2. システムを選択し、*構成*を選択します。
3. すべてのボリュームのスキャンを有効または無効にするには、すべてのボリュームの上にある見出しで [マップ]、[マップと分類]、または [オフ] を選択します。

   個々のボリュームのスキャンを有効または無効にするには、リストでボリュームを見つけて、ボリューム名の横にある [マップ]、[マップと分類]、または [オフ] を選択します。

結果

スキャンを有効にすると、データ分類はシステムで選択したボリュームのスキャンを開始します。データ分類がスキャンを開始するとすぐに、コンプライアンス ダッシュボードに結果が表示され始めます。スキャンの完了時間はデータの量に応じて数分から数時間の範囲になります。

NetApp Data Classificationでファイル共有をスキャンする

ファイル共有をスキャンするには、まずNetApp Data Classificationでファイル共有グループを作成する必要があります。ファイル共有グループは、オンプレミスまたはクラウドでホストされる NFS または CIFS (SMB) 共有用です。

データ分類コア バージョンでは、 NetApp以外のファイル共有からのデータのスキャンはサポートされていません。

前提条件

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

- 共有は、クラウドやオンプレミスなど、どこにでもホストできます。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。
  - データ分類では、7-Mode システムから権限や「最終アクセス時刻」を抽出できません。
  - 一部の Linux バージョンと 7-Mode システム上の CIFS 共有の間に既知の問題があるため、NTLM 認証が有効になっている SMBv1 のみを使用するように共有を構成する必要があります。
- データ分類インスタンスと共有の間にはネットワーク接続が必要です。
- DFS (分散ファイル システム) 共有を通常の CIFS 共有として追加できます。データ分類では、共有が複数のサーバー/ボリューム上に構築され、単一の CIFS 共有として結合されていることを認識しないため、メッセージが実際には別のサーバー/ボリュームにあるフォルダー/共有の 1 つにのみ適用される場合でも、共有に関するアクセス許可または接続エラーが発生する可能性があります。
- 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 資格情報があることを確認します。データ分類で昇格された権限を必要とするデータをスキャンする必要がある場合は、管理者の資格情報が優先されます。

  データ分類スキャンによってファイルの「最終アクセス時刻」が変更されないようにしたい場合は、ユーザーに CIFS での属性書き込み権限または NFS での書き込み権限を与えることをお勧めします。可能であれば、Active Directory ユーザーを、すべてのファイルへの権限を持つ組織内の親グループの一部として構成します。

- グループ内のすべての CIFS ファイル共有では、同じ Active Directory 資格情報を使用する必要があります。
- NFS と CIFS (Kerberos または NTLM のいずれかを使用) の共有を混在させることができます。共有をグループに個別に追加する必要があります。つまり、プロトコルごとに 1 回ずつ、プロセスを 2 回完了する必要があります。
  - CIFS 認証タイプ (Kerberos と NTLM) が混在するファイル共有グループを作成することはできません。
- Kerberos 認証で CIFS を使用している場合は、提供された IP アドレスがデータ分類にアクセスできることを確認してください。 IP アドレスに到達できない場合は、ファイル共有を追加できません。

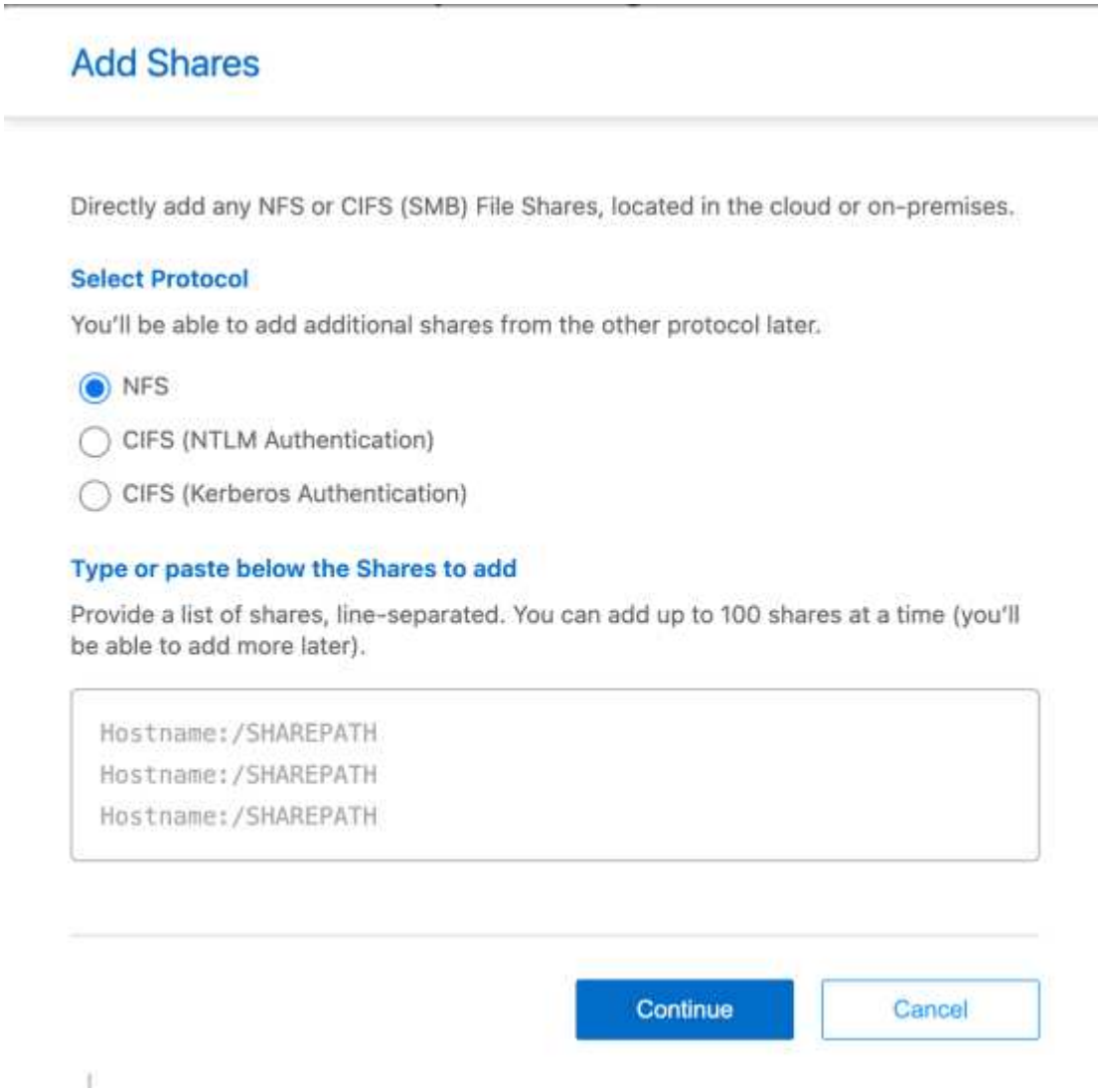
ファイル共有グループを作成する

グループにファイル共有を追加するときは、次の形式を使用する必要があります。
`<host_name>:/<share_path>` 。

ファイル共有を個別に追加することも、スキャンするファイル共有の行区切りリストを入力することもできます。一度に追加できる株式数は最大 100 です。

手順

1. データ分類メニューから、*構成*を選択します。
2. 構成ページで、システムの追加 > *ファイル共有グループの追加*を選択します。
3. [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] を選択します。
4. 追加するファイル共有のプロトコルを選択します。



   a. NTLM 認証を使用して CIFS 共有を追加する場合は、Active Directory の資格情報を入力して CIFS ボリュームにアクセスします。読み取り専用の資格情報はサポートされていますが、管理者の資格情報を使用してフルアクセスを提供することをお勧めします。 保存を選択します。

5. スキャンするファイル共有を追加します (1 行につき 1 つのファイル共有)。次に、[続行] を選択します。
6. 確認ダイアログに追加された共有数が表示されます。

   ダイアログに追加できなかった共有がリストされている場合は、問題を解決できるようにこの情報を取得します。問題が命名規則に関係する場合は、修正した名前で共有を再度追加できます。

7. ボリュームのスキャンを構成します。
    - ファイル共有でマッピングのみのスキャンを有効にするには、[マップ] を選択します。
    - ファイル共有の完全スキャンを有効にするには、[マップと分類] を選択します。
    - ファイル共有のスキャンを無効にするには、[オフ] を選択します。

> ページ上部の「「属性の書き込み」権限がない場合にスキャンする」スイッチは、デフォルトでは無効になっています。つまり、データ分類に CIFS での属性書き込み権限または NFS での書き込み権限がない場合、データ分類は「最終アクセス時刻」を元のタイムスタンプに戻すことができないため、システムはファイルをスキャンしません。+ *「属性の書き込み」権限がない場合にスキャン*を*オン*に切り替えると、スキャンは最終アクセス時刻をリセットし、権限に関係なくすべてのファイルをスキャンします。+ 最終アクセスタイムスタンプの詳細については、以下を参照してください。"データ分類のデータソースから収集されたメタデータ" 。

結果

データ分類は、追加したファイル共有内のファイルのスキャンを開始します。あなたはできるxref:#track-the-scanning-progressダッシュボードでスキャンの結果を表示します。

> Kerberos 認証を使用した CIFS 構成のスキャンが正常に完了しない場合は、[構成] タブでエラーを確認してください。

ファイル共有グループを編集する

ファイル共有グループを作成した後、CIFS プロトコルを編集したり、ファイル共有を追加および削除したりできます。

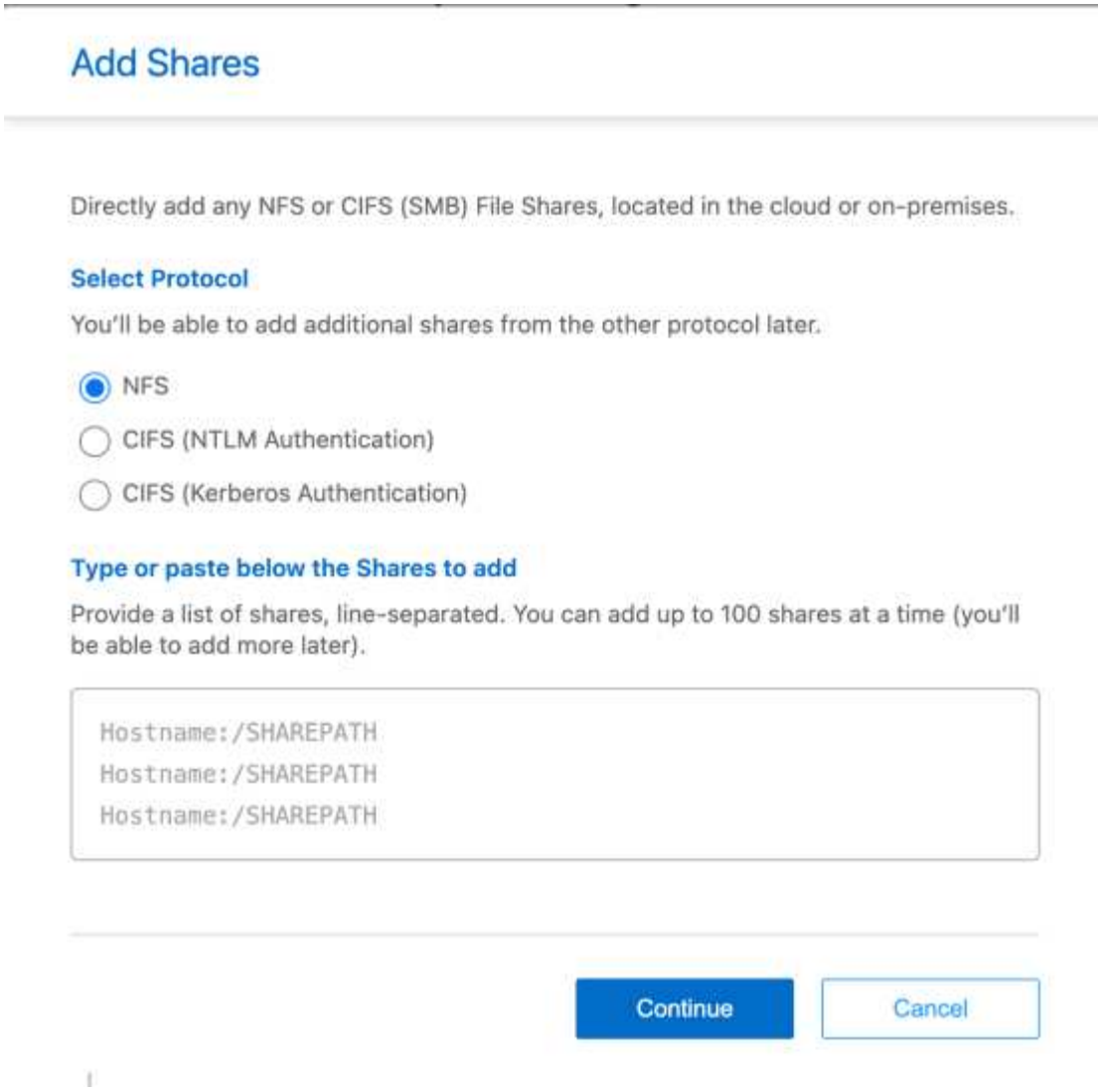
CIFSプロトコル設定を編集する

1. データ分類メニューから、*構成*を選択します。
2. [構成] ページで、変更するファイル共有グループを選択します。
3. **CIFS** 資格情報の編集 を選択します。

4. 認証方法を選択します: **NTLM** または **Kerberos**。
5. Active Directory の ユーザー名 と パスワード を入力します。
6. プロセスを完了するには、[保存] を選択します。

スキャンにファイル共有を追加する

1. データ分類メニューから、*構成*を選択します。
2. [構成] ページで、変更するファイル共有グループを選択します。
3. **+** 共有を追加 を選択します。
4. 追加するファイル共有のプロトコルを選択します。



すでに構成済みのプロトコルにファイル共有を追加する場合、変更は必要ありません。

2番目のプロトコルでファイル共有を追加する場合は、認証が適切に設定されていることを確認してください。"前提条件" 。

5. スキャンするファイル共有（1行につき1つのファイル共有）を次の形式で追加します。 `<host_name>:/<share_path>` 。
6. ファイル共有の追加を完了するには、[続行] を選択します。

スキャンからファイル共有を削除する

1. データ分類メニューから、*構成*を選択します。
2. ファイル共有を削除するシステムを選択します。
3. *構成*を選択します。
4. 設定ページからアクションを選択します ••• 削除するファイル共有の。
5. [アクション] メニューから、[共有を削除] を選択します。

スキャンの進行状況を追跡する

初期スキャンの進行状況を追跡できます。

1. 構成 メニューを選択します。
2. システム構成を選択します。
3. ストレージ リポジトリの場合は、スキャン進行状況列をチェックしてステータスを表示します。

NetApp Data ClassificationでStorageGRIDデータをスキャン

いくつかの手順を完了すると、 NetApp Data Classificationを使用してStorageGRID内のデータを直接スキャンし始めることができます。

StorageGRIDの要件を確認する

データ分類を有効にする前に、次の前提条件を確認して、サポートされてい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。
- データ分類がバケットにアクセスできるようにするには、 StorageGRIDからのアクセス キーとシークレット キーが必要です。

データ分類インスタンスをデプロイする

インスタンスがまだデプロイされていない場合は、データ分類をデプロイします。

インターネット経由でアクセス可能なStorageGRIDからデータをスキャンする場合は、"クラウドでデータ分類を展開する"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データ分類を展開する"。

インターネットにアクセスできない暗い場所にインストールされているStorageGRIDからデータをスキャンする場合は、"インターネットにアクセスできないオンプレミスの同じ場所にデータ分類を展開する" 。これには、コンソール エージェントが同じオンプレミスの場所に展開されていることも必要です。

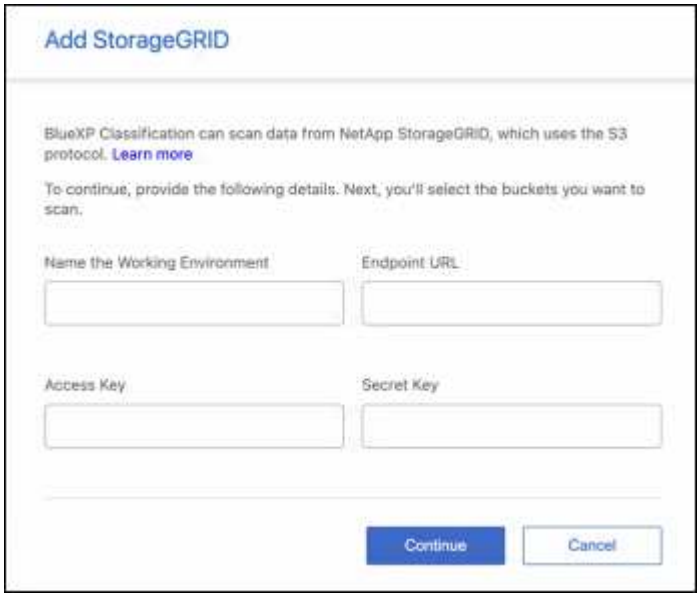
データ分類にStorageGRIDサービスを追加する

StorageGRIDサービスを追加します。

手順

1. データ分類メニューから、*構成*オプションを選択します。
2. 構成ページで、システムの追加 > * StorageGRIDの追加*を選択します。
3. 「StorageGRIDサービスの追加」ダイアログで、 StorageGRIDサービスの詳細を入力し、「続行」を選択します。
   a. システムに使用する名前を入力します。この名前は、接続先のStorageGRIDサービスの名前を反映する必要があります。
   b. オブジェクト ストレージ サービスにアクセスするためのエンドポイント URL を入力します。
   c. データ分類がStorageGRID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。



結果

StorageGRIDがシステムのリストに追加されます。

StorageGRIDバケットのスキャンを有効または無効にする

StorageGRIDでデータ分類を有効にした後、次のステップはスキャンするバケットを構成することです。データ分類はこれらのバケットを検出し、作成したシステムに表示します。

手順

1. 構成ページで、 StorageGRIDシステムを見つけます。
2. StorageGRIDシステム タイルで、[構成] を選択します。
3. スキャンを有効または無効にするには、次のいずれかの手順を実行します。
   - バケットでマッピングのみのスキャンを有効にするには、[マップ] を選択します。
   - バケットの完全スキャンを有効にするには、[マップと分類] を選択します。
   - バケットのスキャンを無効にするには、[オフ] を選択します。

結果

データ分類は、有効にしたバケットのスキャンを開始します。 構成 メニューに移動し、システム構成 を選択すると、初期スキャンの進行状況を追跡できます。各スキャンの進行状況は進行状況バーとして表示されます。進行状況バーにマウスを移動すると、ボリューム内のファイルの合計数に対するスキャンされたファイルの数を確認することもできます。エラーがある場合は、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。

著作権に関する情報

商標に関する情報