BlueXPの分類に関するドキュメント

BlueXP classification

NetApp
April 03, 2024

目次

BlueXPの分類に関するドキュメント

リリースノート

BlueXP分類の新機能

BlueXP分類の新機能（Cloud Data Sense）をご紹介します。

2024年4月1日（バージョン1.30）

RHEL v8.8および**v9.3 BlueXP**の分類のサポートの追加

このリリースでは、以前サポートされていた9.xに加えて、Red Hat Enterprise Linux v8.8およびv9.3がサポートされます。9.xにはDockerエンジンではなくPodmanが必要です。これは、手動でオンプレミスにBlueXPをインストールした場合にも当てはまります。

次のオペレーティングシステムでは、Podmanコンテナエンジンを使用する必要があります。また、BlueXP分類バージョン1.30以降（Red Hat Enterprise Linuxバージョン8.8、9.0、9.1、9.2、9.3）が必要です。

の詳細を確認してください "BlueXPの分類環境の概要"。

監査ログ収集をアクティブ化するオプションが削除されました

監査ログ収集をアクティブ化するオプションが無効になりました。

スキャン速度の向上

セカンダリスキャナノードでのスキャンパフォーマンスが改善されました。スキャンの処理能力を高める必要がある場合は、スキャナノードを追加できます。詳細については、を参照してください "インターネットにアクセスできるホストにBlueXP分類をインストールします"。

ジドウアップグレード

インターネットにアクセスできるシステムにBlueXP分類を導入している場合は、システムが自動的にアップグレードされます。以前は、最後のユーザアクティビティから特定の時間が経過したあとにアップグレードが実行されていました。このリリースでは、現地時間が午前1時から午前5時の場合、BlueXPの分類が自動的にアップグレードされます。ローカル時間がこの時間外の場合は、最後のユーザアクティビティから特定の時間が経過したあとにアップグレードが実行されます。詳細については、を参照してください "インターネットにアクセスできるLinuxホストにインストールします"。

インターネットアクセスを使用せずにBlueXP分類を導入した場合は、手動でアップグレードする必要があります。詳細については、を参照してください "インターネットアクセスのないLinuxホストにBlueXP分類をインストールする"。

2024年3月4日（バージョン1.29）

特定のデータソースディレクトリにあるスキャンデータを除外できるようになりました。

BlueXPの分類で、特定のデータソースディレクトリにあるスキャンデータを除外する場合は、BlueXPの分類で処理する構成ファイルにこれらのディレクトリ名を追加します。この機能を使用すると、不要なディレクトリや、個人データの誤検出結果が返されるディレクトリのスキャンを回避できます。

"詳細はこちら。"。

特大規模インスタンスのサポートが認定されました

BlueXPの分類で2億5、000万を超えるファイルをスキャンする必要がある場合は、クラウド環境またはオンプレミス環境で特大規模なインスタンスを使用できます。このタイプのシステムは、最大5億個のファイルをスキャンできます。

"詳細はこちら。"。

2024年1月10日（バージョン1.27）

調査ページの結果に、項目の合計数に加えて合計サイズが表示されるようになりました。

[Investigation]ページでフィルタ処理された結果に、ファイルの合計数に加えてアイテムの合計サイズが表示されるようになりました。これは、ファイルの移動、ファイルの削除などを行うときに役立ちます。

追加のグループ**ID**を**[Open to Organization]**として設定します。

グループに最初にその権限が設定されていなかった場合に、BlueXPの分類から直接、NFSのグループIDを「Open to Organization」とみなされるように設定できるようになりました。これらのグループIDが添付されているファイルおよびフォルダは、[Investigation Details]ページで[Open to Organization]として表示されます。方法を参照してください "追加のグループIDを「組織にオープン」として追加"。

2023年12月14日（バージョン1.26.6）

このリリースには、いくつかのマイナーな機能拡張が含まれ

また、次のオプションも一時的に削除されました。

- 監査ログ収集をアクティブ化するオプションが無効になりました。を参照してください "ファイルアクセスイベントを監視および管理します"。
- ディレクトリ調査中に、ディレクトリごとの個人識別情報（PII）データの数を計算するオプションは使用できません。を参照してください "組織に保存されているデータを調査します"。
- Azure Information Protection（AIP）ラベルを使用してデータを統合するオプションが無効になりました。を参照してください "プライベートデータを整理します"。

2023年11月6日（バージョン1.26.3）

このリリースで解決された問題は次のとおりです。

- システムによってスキャンされたファイル数をダッシュボードに表示する際の不一致を修正しました。
- 名前とメタデータに特殊文字が含まれるファイルとディレクトリを処理およびレポートすることで、スキャンの動作が改善されました。

2023年10月4日（バージョン1.26）

RHELバージョン**9**での**BlueXP**分類のオンプレミスインストールのサポート

Red Hat Enterprise Linuxバージョン8および9は、BlueXP分類のインストールに必要なDockerエンジンをサポートしていません。コンテナインフラとしてPodmanバージョン4以降を使用したRHEL 9.0、9.1、9.2でのBlueXP分類のインストールがサポートされるようになりました。最新バージョンのRHELを使用する必要がある環境では、Podmanを使用する際にBlueXP分類（バージョン1.26以降）をインストールできるようになりました。

現時点では、RHEL 9.xを使用している場合、ダークサイトのインストールや分散スキャン環境（マスターノードとリモートスキャナノードを使用）はサポートされていません。

2023年9月5日（バージョン1.25）

小規模および中規模の導入が一時的に利用できない

現時点では、BlueXP分類のインスタンスをAWSに導入する場合、*[Deploy]>[Configuration]*を選択してSmallまたはMedium sizedインスタンスを選択するオプションは使用できません。[Deploy]>[Deploy]*を選択して、大きなインスタンスサイズを使用してインスタンスを導入することもできます。

[Investigation Results]ページから最大**100,000**項目にタグを適用

これまでは、[Investigation Results]ページ（20項目）で一度に1つのページにタグを適用することしかできませんでした。[調査結果（Investigation Results）]ページで*すべての*項目を選択し、すべての項目（一度に最大100,000項目）にタグを適用できるようになりました。 "方法を参照してください"。

最小ファイルサイズが**1MB**の重複ファイルを特定する

BlueXPの分類では、ファイルが50MB以上の場合にのみ重複ファイルが特定されます。1MBで始まる重複ファイルを識別できるようになりました。[Investigation]ページフィルタの[File Size]と[Duplicates]を使用して、環境内で特定のサイズのファイルが重複しているかどうかを確認できます。

2023年7月17日（バージョン1.24）

BlueXPの分類では、ドイツの**2**つの新しいタイプの個人データが特定されています。

BlueXPの分類では、次のタイプのデータを含むファイルを特定して分類できます。

- ドイツ語ID（Personalausweisnummer）
- ドイツ社会保障番号（Sozialversicherungsnummer）

"BlueXPの分類によってデータから特定できるすべてのタイプの個人データを確認できます"。

BlueXPの分類は制限モードとプライベートモードで完全にサポートされています。

インターネットアクセスがないサイト（プライベートモード）とアウトバウンドのインターネットアクセスが制限されているサイト（制限モード）で、BlueXPの分類が完全にサポートされるようになりました。 "コネクタのBlueXP導入モードの詳細"。

BlueXP分類のプライベートモードインストールをアップグレードするときにバージョンをスキップする機能

シーケンシャルでなくても、新しいバージョンのBlueXP分類にアップグレードできるようになりました。つ

まり、BlueXPの分類を1つのバージョンにアップグレードするという現行の制限は不要になりました。この機能は、バージョン1.24以降で該当します。

BlueXP分類**API**を利用できるようになりました

BlueXP分類APIを使用すると、スキャンするデータに関する操作の実行、クエリの作成、情報のエクスポートを行うことができます。Swaggerを使用して対話型ドキュメントを利用できます。ドキュメントは、調査、コンプライアンス、ガバナンス、構成など、複数のカテゴリに分かれています。各カテゴリは、BlueXP分類用UIのタブを表しています。

"BlueXP分類APIの詳細"。

2023年6月6日（バージョン1.23）

データ主体名の検索で日本語がサポートされるようになりました

データ主体アクセス要求（DSAR）に応答して、被験者の名前を検索する際に日本語名を入力できるようになりました。を生成できます "Data Subject Access Request レポート" 結果の情報を使用して。に日本語の名前を入力することもできます "[Data Investigationページの[Data Subject]フィルタ"] サブジェクト名を含むファイルを識別します。

Ubuntuがサポート対象の**Linux**ディストリビューションになり、**BlueXP**分類をインストールできるようになりました

Ubuntu 22.04は、BlueXPのサポート対象オペレーティングシステムとして認定されています。BlueXP分類は、ネットワーク内のUbuntu Linuxホストにインストールすることも、バージョン1.23のインストーラを使用している場合はクラウドのLinuxホストにインストールすることもできます。 "Ubuntuがインストールされているホストに BlueXP分類をインストールする方法を参照してください"。

新しい**BlueXP**分類のインストールでは、**Red Hat Enterprise Linux 8.6**および**8.7**はサポートされなくなりました

Red Hatでは前提条件であるDockerがサポートされなくなるため、新規導入ではこれらのバージョンはサポートされません。RHEL 8.6または8.7で既存のBlueXP分類マシンを実行している場合、NetAppでは引き続き構成がサポートされます。

BlueXPの分類は、**ONTAP**システムから**FPolicy**イベントを受信する**FPolicy**コレクタとして設定できます

作業環境内のボリュームで検出されたファイルアクセスイベントについて、BlueXP分類システムでファイルアクセス監査ログの収集を有効にすることができます。BlueXPの分類では、次のタイプのFPolicyイベントと、ファイルに対してアクションを実行したユーザ（Create、Read、Write、Delete、Rename、 所有者/権限を変更し、SACL/DACLを変更します。 "ファイルアクセスイベントを監視および管理する方法を参照してください"。

ダークサイトで**Data Sense BYOL**ライセンスがサポートされるようになりました

ダークサイトのBlueXPデジタルウォレットにData Sense BYOLライセンスをアップロードして、ライセンスの残量が少なくなったときに通知を受け取ることができます。 "Data Sense BYOLライセンスの入手方法とアップロード方法をご確認ください"。

2023年4月3日（バージョン1.22）

新しいデータ検出評価レポート

Data Discovery Assessment Reportでは、スキャンされた環境の概要を分析して、システムの調査結果を強調し、懸念領域と潜在的な修復手順を示します。このレポートの目的は、データガバナンスの懸念、データセキュリティの危険性、データセットのデータコンプライアンスギャップに対する認識を高めることです。 "Data Discovery Assessment Reportを生成して使用する方法を説明します"。

クラウド内の小規模インスタンスに**BlueXP**の分類機能を導入できます

AWS環境のBlueXP ConnectorからBlueXPの分類を導入する際に、デフォルトのインスタンスよりも小さい2つのインスタンスタイプから選択できるようになりました。小規模な環境をスキャンする場合は、クラウドコストを節約できます。ただし、小さいインスタンスを使用する場合はいくつかの制限があります。 "使用可能なインスタンスタイプと制限事項を参照してください"。

BlueXPの分類をインストールする前に、スタンドアロンスクリプトを使用して**Linux**システムを認定できるようになりました

BlueXP分類インストールとは別に、Linuxシステムがすべての前提条件を満たしていることを確認する場合は、前提条件のみをテストするスクリプトをダウンロードできます。 "LinuxホストでBlueXPのインストール準備が完了しているかどうかを確認する方法を説明します"。

2023年3月7日（バージョン1.21）

BlueXPの分類**UI**から独自のカスタムカテゴリを追加する新機能

BlueXPの分類で独自のカスタムカテゴリを追加できるようになりました。これにより、それらのカテゴリに該当するファイルがBlueXPの分類で識別されます。BlueXPには多くの種類があります "事前定義されたカテゴリ"そのため、この機能を使用すると、カスタムカテゴリを追加して、組織固有の情報がデータ内のどこにあるかを特定できます。

"詳細はこちら。"。

BlueXPの分類**UI**からカスタムキーワードを追加できるようになりました

BlueXPの分類では、今後のスキャンでBlueXPの分類によって特定されるカスタムキーワードを追加できます。ただし、BlueXP分類Linuxホストにログインし、コマンドラインインターフェイスを使用してキーワードを追加する必要がありました。今回のリリースでは、BlueXPの分類UIでカスタムキーワードを追加できるようになり、キーワードの追加や編集が非常に簡単になりました。

"BlueXPの分類UIからカスタムキーワードを追加する方法については、こちらをご覧ください"。

「最終アクセス時間」が変更されるときに、**BlueXP**の分類*がファイルをスキャンすることはできません

デフォルトでは、BlueXPの分類に適切な「書き込み」権限がないと、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、ボリューム内のファイルはスキャンされません。ただし、最終アクセス時刻がファイルの元の時刻にリセットされていてもかまわない場合は、[設定]ページでこの動作を無効にして、権限に関係なくBlueXPの分類でボリュームがスキャンされるようにすることができます。

この機能と併せて、「Scan Analysis Event」という新しいフィルタが追加され、BlueXPの分類で最終アクセ

ス時刻を元に戻すことができなかったために分類されなかったファイルや、BlueXPの分類で最終アクセス時刻を元に戻すことができなかったにもかかわらず分類されたファイルを表示できるようになりました。

"「最終アクセス時間のタイムスタンプ」とBlueXPの分類に必要な権限について詳しくは、こちらをご覧ください"。

BlueXPは、**3**つの新しいタイプの個人データを分類しています

BlueXPの分類では、次のタイプのデータを含むファイルを特定して分類できます。

- ボツワナIDカード（Omang）番号
- ボツワナパスポート番号
- シンガポール国民登録IDカード（NRIC）

"BlueXPの分類によってデータから特定できるすべてのタイプの個人データを確認できます"。

ディレクトリの機能が更新されました

- データ調査レポートの[Light CSV Report]オプションに、ディレクトリからの情報が含まれるようになりました。
- [Last Accessed]時間フィルタに、ファイルとディレクトリの両方の最終アクセス時刻が表示されるようになりました。

インストールの機能拡張

- インターネットアクセスがないサイト（ダークサイト）用のBlueXP分類インストーラで、インストールを成功させるためにシステムとネットワークの要件が満たされていることを確認するための事前チェックが実行されるようになりました。
- インストール監査ログファイルは保存され、に書き込まれます `/ops/netapp/install_logs`。

2023年2月5日（バージョン1.20）

任意の**E**メールアドレスにポリシーベースの通知**E**メールを送信できます

以前のバージョンのBlueXP分類では、特定のクリティカルポリシーが結果を返したときに、アカウントのBlueXPユーザにEメールアラートを送信できました。この機能を使用すると、オンラインでないときにデータを保護するための通知を受け取ることができます。また、ポリシーから、BlueXPアカウントに登録されていない最大20個の電子メールアドレスを持つ他のユーザーに電子メールアラートを送信することもできます。

"ポリシーの結果に基づいて電子メールアラートを送信する方法については、こちらをご覧ください"。

BlueXPの分類**UI**から個人用パターンを追加できるようになりました

BlueXPの分類では、カスタムの「個人データ」を追加できるようになりました。BlueXPの分類で今後のスキャンで特定できるようになります。ただし、BlueXP分類Linuxホストにログインし、コマンドラインを使用してカスタムパターンを追加する必要がありました。このリリースでは、BlueXPの分類UIで正規表現を使用して個人用パターンを追加できるようになり、カスタムパターンの追加と編集が非常に簡単になりました。

"BlueXPの分類UIからカスタムパターンを追加する方法については、こちらをご覧ください"。

BlueXPの分類を使用して**1**、**500**万個のファイルを移動できます

これまで、BlueXPの分類では、最大100、000個のソースファイルを任意のNFS共有に移動できました。一度に最大1,500万個のファイルを移動できるようになりました。 "BlueXPによる分類を使用したソースファイルの移動の詳細については、こちらをご覧ください"。

SharePoint Onlineファイルへのアクセス権を持つユーザーの数を表示する機能

フィルタ「アクセス権を持つユーザー数」で、SharePoint Onlineリポジトリに保存されているファイルがサポートされるようになりました。これまでは、CIFS共有上のファイルのみがサポートされていました。現時点では、Active DirectoryベースでないSharePointグループはこのフィルタにカウントされません。

新しい「部分的成功」ステータスがアクションステータスパネルに追加されました

新しい「Partial Success」ステータスは、BlueXPの分類処理が完了し、一部の項目が失敗し、一部の項目が成功したことを示します（100個のファイルを移動または削除する場合など）。さらに、「終了」ステータスが「成功」に変更されました。以前は、「終了」ステータスに成功した処理と失敗した処理が表示されることがありました。現在、「Success」ステータスは、すべての項目に対するすべてのアクションが成功したことを意味します。 "アクションステータスパネルの表示方法を参照してください"。

2023年1月9日（バージョン1.19）

機密データが含まれ、過度に許容されるファイルのグラフを表示する機能

Governanceダッシュボードには、機密データ（機密性の高い個人データと機密性の高い個人データの両方を含む）を含むファイルのヒートマップを提供するnew_sensitive DataおよびWide Permissive_areaが追加されています。これにより、機密データを含むリスクがある場所を確認できます。 "詳細はこちら。"。

Data Investigationページでは、**3**つの新しいフィルタを使用できます

[データ調査]ページに表示する結果を絞り込むための新しいフィルタを使用できます。

- 「アクセス権を持つユーザの数」フィルタは、特定の数のユーザに対して開かれているファイルやフォルダを表示します。数値の範囲を選択して結果を絞り込むことができます。たとえば、51~100ユーザがアクセスできるファイルを確認できます。
- 「作成日時」、「検出日時」、「最終変更日時」、「最終アクセス日時」の各フィルタを使用して、事前に定義された日範囲だけを選択するのではなく、カスタムの日付範囲を作成できるようになりました。たとえば、「作成日時」が6か月を超えているファイルや、「最終更新日時」が「過去10日間」の日付になっているファイルを探すことができます。
- 「ファイルパス」フィルタで、フィルタリングされたクエリ結果から除外するパスを指定できるようになりました。対象に含めるデータと除外するデータの両方のパスを入力すると、BlueXPの分類によって、対象に含めるパス内のすべてのファイルが最初に検出され、除外するパスからファイルが削除されて結果が表示されます。

"データの調査に使用できるすべてのフィルタのリストを確認します"。

BlueXPの分類では、日本の個人番号を識別できます

BlueXPの分類では、日本語の個人番号（「マイナンバー」とも呼ばれます）を含むファイルを特定して分類できます。これには、個人用電話番号と会社用電話番号の両方が含まれます。 "BlueXPの分類によってデータから特定できるすべてのタイプの個人データを確認できます"。

既知の制限

既知の制限事項には、このリリースの製品でサポートされていない機能、またはこのリリースと正しく相互運用できない機能が記載されています。これらの制限事項を慎重に確認してください

BlueXP分類リリースで一時的に削除されたオプション

2023年12月（バージョン1.26.6）リリースでは、次のオプションが一時的に削除されました。

- 監査ログ収集をアクティブ化するオプションが無効になりました。
- ディレクトリ調査中に、ディレクトリごとの個人識別情報（PII）データの数を計算するオプションは使用できません。
- Azure Information Protection（AIP）ラベルを使用してデータを統合するオプションが無効になりました。

BlueXPの分類スキャンの制限事項

BlueXPの分類では、ボリュームの下にある共有は**1**つだけスキャンされます

1つのボリュームに複数のファイル共有がある場合は、最上位階層の共有がスキャンされます。たとえば、次のような共有があるとします。

- /A
- /A/B
- /C
- /D/E

その後、/A内のデータがスキャンされます。/Cおよび/Dのデータはスキャンされません。

回避策

ボリューム内のすべての共有からデータをスキャンしていることを確認する回避策があります。次の手順を実行します。

1. 作業環境で、スキャンするボリュームを追加します。
2. BlueXPの分類によるボリュームのスキャンが完了したら、_Data Investigation_pageに移動し、どの共有がスキャンされているかを確認するフィルタを作成します。

   「Working Environment Name」および「Directory Type = Share」でデータをフィルタリングして、どの共有がスキャンされているかを確認します。

3. ボリューム内に存在する共有の完全なリストを取得して、スキャンされていない共有を確認します。
4. "残りの共有を共有グループに追加します"。

   次のように、すべての共有を個別に追加する必要があります。

```
/C
/D
```

5. 複数の共有を含む作業環境内のボリュームごとに、次の手順を実行します。

はじめに

BlueXPの分類について説明します

BlueXPの分類（Cloud Data Sense）は、BlueXP向けのデータガバナンスサービスです。オンプレミスとクラウドの社内データソースをスキャンしてデータのマッピングと分類を行い、個人情報を特定します。これにより、セキュリティとコンプライアンスのリスクを軽減し、ストレージコストを削減し、データ移行プロジェクトを支援できます。

の機能

BlueXPの分類では、人工知能（AI）、自然言語処理（NLP）、機械学習（ML）を使用してスキャンされるコンテンツを把握し、エンティティを抽出し、それに応じてコンテンツを分類します。これにより、BlueXPでは次の機能が提供されます。

"BlueXP分類のユースケースの詳細については、こちらをご覧ください"。

コンプライアンスを維持

BlueXPには、コンプライアンスへの取り組みに役立ついくつかのツールが用意されています。BlueXPの分類を使用すると、次の処理を実行できます。

- 個人識別情報（ PII ）を識別します。
- GDPR、CCPA、PCI、HIPAAの各プライバシー規制の要件に応じて、機密性の高い個人情報の範囲を特定します。
- 名前または電子メールアドレスに基づいてデータサブジェクトアクセス要求（dsar）に応答します。
- データベースの一意の識別子が他のリポジトリのファイルに含まれているかどうかを特定します。基本的には、BlueXPの分類スキャンで特定された「個人データ」の独自のリストを作成します。
- ファイルに特定のPIIが含まれている場合は、電子メールで特定のユーザーに通知します（を使用してこの基準を定義します "ポリシー"）では、アクションプランを決定することができます。

セキュリティの強化

BlueXPでは、犯罪目的でアクセスされるリスクのあるデータを分類して特定できます。BlueXPの分類を使用すると、次の処理を実行できます。

- 組織全体またはパブリックに公開されているオープンな権限を持つすべてのファイルとディレクトリ（共有およびフォルダ）を特定します。
- 初期の専用の場所以外に存在する機密データを特定します。
- データ保持ポリシーに準拠
- 新しいセキュリティ問題をセキュリティスタッフに自動的に通知して、ただちに対処できるようにするには、_Policies_を使用します。
- カスタムタグをファイルに追加し（「移動が必要」など）、BlueXPユーザーを割り当てて、ユーザーがファイルの更新を所有できるようにします。

- 表示と変更 "Azure Information Protection （ AIP ） ラベル" ファイルに保存できます。

ストレージ使用量を最適化

BlueXPは、ストレージの総所有コスト（TCO）に役立つツールを備えています。BlueXPの分類を使用すると、次の処理を実行できます。

- 重複データやビジネス以外のデータを特定することで、ストレージ効率を向上させます。この情報を使用して、特定のファイルを移動するか削除するかを決定できます。
- 安全でないようであるか、ストレージシステムに残すのにリスクが高すぎるファイル、または重複として識別されたファイルを削除してください。_Policies_を使用すると'特定の条件に一致するファイルを自動的に削除できます
- アクセス頻度の低いデータを低コストのオブジェクトストレージに階層化できるため、ストレージコストを削減できます。 "Cloud Volumes ONTAP システムからの階層化の詳細については、こちらをご覧ください"。 "オンプレミスのONTAP システムからの階層化の詳細については、こちらをご覧ください"。

データ移行を高速化

BlueXPの分類を使用すると、オンプレミスのデータをパブリッククラウドやプライベートクラウドに移行する前にスキャンできます。BlueXPの分類を使用すると、次の処理を実行できます。

- データのサイズ、および移動前に機密情報が含まれているデータがないかどうかを確認する。
- ソースデータを（25種類以上の基準に基づいて）フィルタリングして、必要なファイルのみを宛先に移動できるようにします。不要なデータは移動されません。
- 必要なデータのみをクラウドリポジトリに自動的かつ継続的に移動、コピー、同期

サポートされているデータソース

BlueXPの分類では、次のタイプのデータソースから構造化データと非構造化データをスキャンして分析できます。

ネットアップ：

- Cloud Volumes ONTAP （ AWS 、 Azure 、 GCP に導入）
- オンプレミスの ONTAP クラスタ
- StorageGRID
- Azure NetApp Files の特長
- ONTAP 対応の Amazon FSX
- Cloud Volumes Service for Google Cloud

ネットアップ以外：

- Dell EMC Isilon の
- Pure Storageの略
- Nutanix
- その他のストレージベンダー

クラウド：

- Amazon S3
- Google クラウドストレージ
- OneDrive
- SharePoint Online
- SharePointオンプレミス（SharePoint Server）
- Googleドライブ

データベース：

- 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 ）

BlueXPの分類では、NFSバージョン3.xとCIFSバージョン1.x、2.0、2.1、3.0がサポートされます。

コスト

- BlueXPの分類を使用するコストは、スキャンするデータの量によって異なります。BlueXPワークスペースでBlueXPの分類によってスキャンされる最初の1TBのデータは30日間無料です。これには、すべての作業環境とデータソースのすべてのデータが含まれます。この時点以降もデータのスキャンを続行するには、 AWS 、 Azure 、 GCP Marketplace 、またはネットアップの BYOL ライセンスのサブスクリプションが必要です。を参照してください "価格設定" を参照してください。

  "BlueXPのライセンスを取得する方法について説明します"。

- BlueXPをクラウドにインストールするにはクラウドインスタンスを導入する必要があるため、導入先のクラウドプロバイダから料金が請求されます。を参照してください 各クラウドに導入されるインスタンスのタイプ プロバイダ。BlueXP分類をオンプレミスシステムにインストールすればコストはかかりません。
- BlueXPに分類されるためには、BlueXPコネクタが導入されている必要があります。多くの場合、BlueXPで使用している他のストレージとサービスのためにコネクタが既に存在します。Connector インスタンスを使用すると、導入先のクラウドプロバイダから料金が発生します。を参照してください "クラウドプロバイダごとに導入されるインスタンスのタイプ"。コネクタをオンプレミスシステムにインストールしても、コストはかかりません。

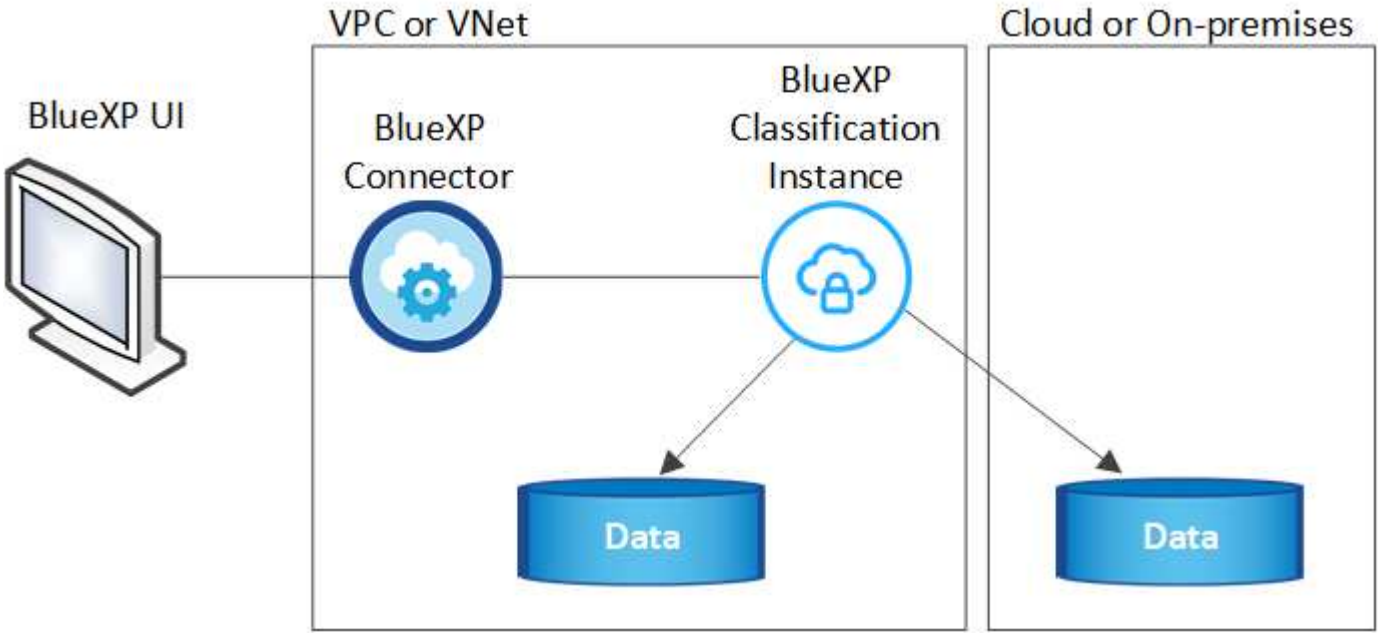
データ転送コスト

データ転送のコストは設定によって異なります。BlueXP分類インスタンスとデータソースが同じアベイラビリティゾーンとリージョンにある場合、データ転送コストは発生しません。ただし、 Cloud Volumes ONTAP システムや S3 バケットなどのデータソースが _different _Availability Zone またはリージョンにある場合は、クラウドプロバイダにデータ転送コストが請求されます。詳細については、次のリンクを参照してください。

- "AWS ： Amazon EC2 価格設定"
- "Microsoft Azure ： Bandwidth Pricing Details 』"
- "Google Cloud ：ストレージ転送サービスの価格"

BlueXP分類インスタンス

BlueXP分類をクラウドに導入すると、BlueXPはコネクタと同じサブネットにインスタンスを導入します。 "コネクタの詳細については、こちらをご覧ください。"



デフォルトのインスタンスについては、次の点に注意してください。

- AWSでは、BlueXPの分類はで実行されます "m6i.4xlargeインスタンス" 500GiBのgp2ディスクを使用した場合。オペレーティングシステムイメージは Amazon Linux 2 です。AWSに導入した場合、少量のデータをスキャンする場合は、インスタンスサイズを小さくすることができます。
- Azureでは、BlueXPの分類はで実行されます "Standard_D16s_v3 VM" 500GiBのディスクオペレーティングシステムイメージは CentOS 7.9 です。
- GCPでは、BlueXPの分類はで実行されます "N2-standard-16 VM" 500GiB Standard永続ディスクを使用した場合。オペレーティングシステムイメージは CentOS 7.9 です。
- デフォルトのインスタンスを使用できない地域では、BlueXPの分類は別のインスタンスで実行されます。"別のインスタンスタイプを参照してください"。
- インスタンスの名前は *CloudCompliancy_with* で、生成されたハッシュ（ *UUID* ）を連結しています。例： *_CloudCompliion-16bb6564-38ad-40802-9a92-36f5fd2f71c7*
- コネクタごとに導入されるBlueXP分類インスタンスは1つだけです。

BlueXPの分類は、オンプレミスのLinuxホストや希望するクラウドプロバイダのホストに導入することもできます。どのインストール方法を選択しても、ソフトウェアはまったく同じように機能します。インスタンスにインターネットアクセスがあれば、BlueXP分類ソフトウェアのアップグレードは自動で実行されます。

BlueXPの分類ではデータが継続的にスキャンされるため、インスタンスは常に実行されたままにしておく必要があります。

小さいインスタンスタイプを使用しています

CPUとRAMの数が少ないシステムにBlueXPの分類を導入することもできますが、使用するシステムにはいくつかの制限があります。

システムサイズ	仕様	制限
特大	CPU×32、128GB RAM、1TiB SSD	最大5億個のファイルをスキャンできます。
Large （デフォルト）	CPU×16、64GB RAM、500GiB SSD	最大2億5、000万個のファイルをスキャンできます。
中	CPU×8、32GB RAM、200GiB SSD	スキャンに時間がかかり、スキャンできるファイルは最大 100 万個です。
小規模	CPU×8、16GB RAM、100GiB SSD	「中」と同じ制限に加えて、特定する機能 "データ主体名" 内部ファイルは無効です。

AWSのクラウドにBlueXPの分類を導入する場合は、大規模、中規模、小規模のインスタンスを選択できます。AzureまたはGCPにBlueXPの分類を導入する際に、これらの代替システムのいずれかを使用する場合は、ng-contact-data-sense@netapp.comまでEメールで支援を要請してください。これらの他のクラウド構成を導入するには、お客様と協力する必要があります。

BlueXPの分類をオンプレミスに導入する場合は、別の仕様のLinuxホストを使用するだけです。ネットアップにお問い合わせいただく必要はありません。

BlueXPの分類の仕組み

BlueXPの分類の概要は次のようになります。

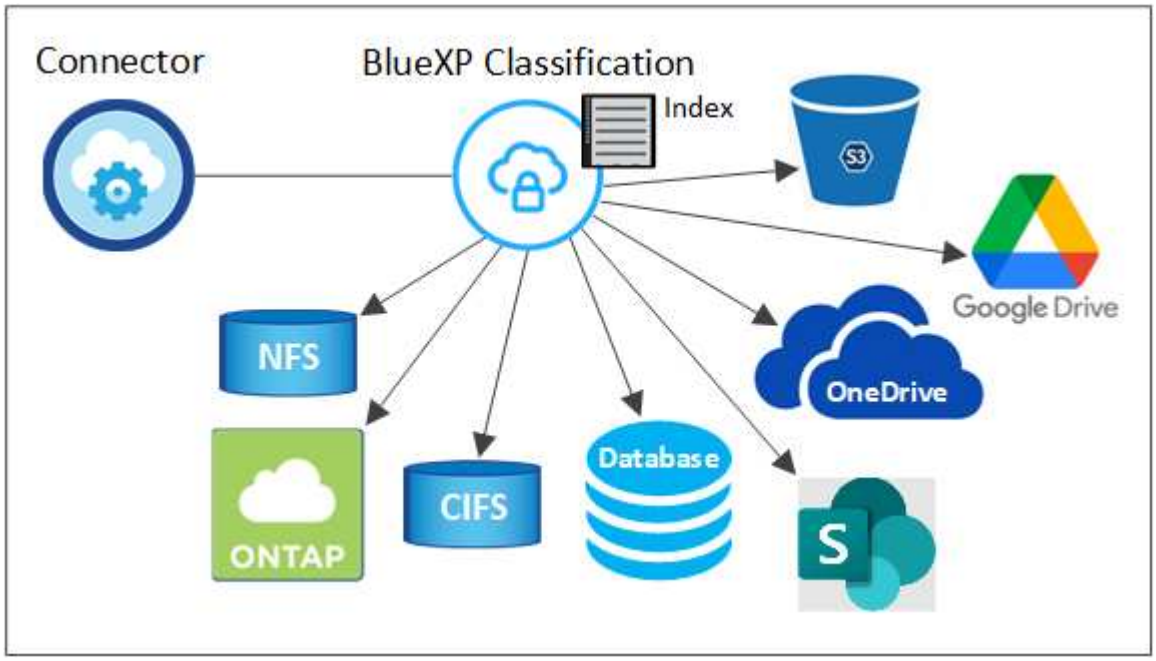
1. BlueXPでBlueXP分類のインスタンスを導入します。
2. 1つ以上のデータソースで、概要レベルのマッピングまたは詳細レベルのスキャンを有効にします。
3. BlueXPの分類では、AI学習プロセスを使用してデータがスキャンされます。
4. 提供されているダッシュボードとレポートツールを使用して、コンプライアンスとガバナンスの取り組みを支援します。

スキャンの動作

BlueXPの分類を有効にしてスキャンするリポジトリ（ボリューム、バケット、データベーススキーマ、OneDriveまたはSharePointのユーザデータ）を選択すると、すぐにデータのスキャンが開始され、個人データと機密データが特定されます。ほとんどの場合、バックアップ、ミラー、DRサイトではなく、本番環境のライブデータのスキャンに重点を置いてください。次に、BlueXPの分類によって組織データがマッピングされ、各ファイルが分類され、データ内のエンティティと事前定義されたパターンが特定されて抽出されます。スキャンの結果は、個人情報、機密性の高い個人情報、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。

BlueXPは、他のクライアントと同様に、NFSボリュームとCIFSボリュームをマウントすることでデータに接

続します。NFS ボリュームには読み取り専用で自動的にアクセスされますが、 CIFS ボリュームをスキャンするためには Active Directory のクレデンシャルを指定する必要があります。



初回スキャン後、BlueXPの分類ではラウンドロビン方式でデータが継続的にスキャンされ、差分の変更が検出されます（そのため、インスタンスを常に実行しておくことが重要です）。

スキャンは、ボリュームレベル、バケットレベル、データベーススキーマレベル、 OneDrive ユーザレベル、SharePoint サイトレベルで有効または無効にできます。

マッピングスキャンと分類スキャンの違いは何ですか

BlueXPの分類を使用すると、選択したデータソースに対して一般的な「マッピング」スキャンを実行できます。マッピングではデータの概要のみが示され、分類ではデータの詳細なスキャンが提供されます。データソースでは、ファイルにアクセスしてデータを参照できないため、マッピングは短時間で完了します。

多くのユーザは、この機能を気に入っています。たとえば、より多くの調査が必要なデータソースをすばやくスキャンして特定したうえで、必要なデータソースやボリュームに対してのみ分類スキャンを有効にする必要があるからです。

次の表に、いくつかの相違点を示します。

フィーチャー（ **Feature** ）	分類	マッピング
スキャン速度	遅い	高速
ファイルタイプと使用済み容量のリスト	はい。	はい。
ファイル数と使用済み容量	はい。	はい。
ファイルの経過時間とサイズ	はい。	はい。
を実行する機能 "データマッピングレポート"	はい。	はい。
[データ調査] ページでファイルの詳細を確認します	はい。	いいえ
ファイル内の名前を検索します	はい。	いいえ

フィーチャー（ **Feature** ）	分類	マッピング
作成 "ポリシー" カスタムの検索結果が表示されます	はい。	いいえ
AIP ラベルおよびステータスタグを使用してデータを分類します	はい。	いいえ
ソースファイルをコピー、削除、および移動します	はい。	いいえ
他のレポートを実行できます	はい。	いいえ

BlueXPの分類によるデータのスキャン速度

スキャン速度は、ネットワークレイテンシ、ディスクレイテンシ、ネットワーク帯域幅、環境のサイズ、およびファイル配信サイズによって左右されます。

- マッピングスキャンを実行する場合、BlueXPの分類では、スキャナノードごとに1日に100~150TiBのデータをスキャンできます。
- 分類スキャンを実行する場合、BlueXPの分類では、スキャナノードごとに1日あたり15~40TiBのデータをスキャンできます。

"データをスキャンするための複数のスキャナノードの導入の詳細については、こちらをご覧ください"。

BlueXPの分類の指標となる情報

BlueXPの分類では、データ（ファイル）の収集とインデックス作成が行われ、カテゴリが割り当てられます。BlueXP分類のインデックスには、次のデータが含まれています。

標準メタデータ

BlueXPは分類されるため、ファイルの種類、サイズ、作成日や変更日など、ファイルに関する標準的なメタデータが収集されます。

個人データ

メールアドレス、識別番号、クレジットカード番号など、個人を特定できる情報。 "個人データの詳細については、こちらをご覧ください"。

機密性の高い個人データ

GDPR やその他のプライバシー規制で定義されている、健康データ、民族的起源、政治的見解などの機密情報の特殊な種類。 "機密性の高い個人データの詳細をご覧ください"。

カテゴリ

BlueXPは、スキャンしたデータをさまざまなカテゴリに分類します。カテゴリは、各ファイルのコンテンツとメタデータの AI 分析に基づくトピックです。 "カテゴリの詳細については、こちらをご覧ください"。

タイプ（ **Types** ）

BlueXPは、スキャンしたデータをファイルタイプ別に分類して分類します。 "タイプの詳細については、こちらをご覧ください"。

名前エンティティ認識

BlueXPの分類では、AIを使用してドキュメントから自然人の名前を抽出します。 "データ主体のアクセスリクエストへの対応について説明します"。

ネットワークの概要

BlueXPでは、コネクタインスタンスからのインバウンドHTTP接続を可能にするセキュリティグループとともにBlueXP分類インスタンスを導入します。

SaaSモードでBlueXPを使用している場合、BlueXPへの接続はHTTPS経由で提供され、ブラウザとBlueXP分類インスタンスの間で送信されるプライベートデータは、TLS 1.2を使用したエンドツーエンドの暗号化で保護されます。つまり、NetAppやサードパーティはデータを読み取ることができません。

アウトバウンドルールは完全にオープンです。BlueXP分類ソフトウェアのインストールとアップグレード、使用状況の指標の送信には、インターネットアクセスが必要です。

ネットワーク要件が厳しい場合は、 "BlueXP分類の連絡先となるエンドポイントについて説明します"。

コンプライアンス情報へのユーザアクセス

各ユーザに割り当てられたロールは、BlueXPとBlueXPで異なる機能を提供します。

- * アカウント管理者 * は、コンプライアンス設定を管理し、すべての作業環境のコンプライアンス情報を表示できます。
- * ワークスペース管理者 * は、アクセス権を持つシステムについてのみ、コンプライアンス設定を管理し、コンプライアンス情報を表示できます。ワークスペース管理者がBlueXPの作業環境にアクセスできない場合、BlueXPの分類タブには作業環境のコンプライアンス情報が表示されません。
- コンプライアンスビューア * の役割を持つユーザーは、アクセス権を持つシステムのコンプライアンス情報を表示し、レポートを生成することのみができます。これらのユーザは、ボリューム、バケット、または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ことはできません。これらのユーザーは、ファイルのコピー、移動、または削除もできません。

"BlueXPの役割の詳細をご覧ください" そして方法 "特定のロールのユーザを追加します"。

BlueXP分類を導入します

BlueXPのどの分類環境を使用すればよいですか？

BlueXP分類はさまざまな方法で導入できます。ニーズに合った方法を確認します。

BlueXPは次の方法で分類されます。

- "BlueXPを使用してクラウドに導入"。BlueXPでは、BlueXPコネクタと同じクラウドプロバイダネットワークにBlueXP分類インスタンスが導入されます。
- "インターネットにアクセスできるLinuxホストにインストールします"。ネットワーク内のLinuxホスト、またはインターネットにアクセスできるクラウド内のLinuxホストにBlueXP分類をインストールします。このタイプのインストールは、同じくオンプレミスにあるBlueXP分類インスタンスを使用してオンプレミスのONTAPシステムをスキャンする場合に適したオプションですが、これは必須ではありません。
- "インターネットにアクセスできないオンプレミスサイトのLinuxホストにインストール"は、_privateモードとも呼ばれます。_インストールスクリプトを使用するこのタイプのインストールは、安全なサイトに適しています。

インターネットにアクセスできるLinuxホストへのインストールと、インターネットにアクセスできないLinux

ホストへのオンプレミスインストールの両方で、インストールスクリプトを使用します。システムと環境が前提条件を満たしているかどうかが確認されます。前提条件を満たしている場合は、インストールが開始されます。BlueXP分類のインストールとは別に前提条件を確認する場合は、前提条件のみをテストする別のソフトウェアパッケージをダウンロードできます。

を参照してください "LinuxホストでBlueXP分類をインストールできる状態になっていることを確認します"。

BlueXPを使用してBlueXP分類をクラウドに導入します

BlueXP分類をクラウドに導入するには、いくつかの手順を実行します。BlueXPでは、BlueXPコネクタと同じクラウドプロバイダネットワークにBlueXP分類インスタンスが導入されます。

また、次のことも可能です "インターネットにアクセスできるLinuxホストにBlueXP分類をインストールします"。このタイプのインストールは、同じくオンプレミスにあるBlueXP分類インスタンスを使用してオンプレミスのONTAP システムをスキャンする場合に適したオプションですが、これは必須ではありません。どのインストール方法を選択しても、ソフトウェアはまったく同じように機能します。

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 コネクタを作成します

コネクタがない場合は、ここでコネクタを作成します。を参照してください "AWS でコネクタを作成する"、"Azure でコネクタを作成する"または "GCP でコネクタを作成する"。

また可能です "コネクタをオンプレミスにインストールします" ネットワーク内のLinuxホストまたはクラウド内のLinuxホスト。

2 前提条件を確認する

環境が前提条件を満たしていることを確認します。これには、インスタンスのアウトバウンドインターネットアクセス、コネクタとBlueXPのポート443経由の分類間の接続などが含まれます。 すべてのリストを参照してください。

3 **BlueXP**分類を導入します

インストールウィザードを起動して、BlueXP分類インスタンスをクラウドに導入します。

4 **BlueXP**分類サービスにサブスクライブします

BlueXPで分類されてスキャンされる最初の1TBのデータは、30日間無料です。その時点以降もデータのスキャンを続行するには、クラウドプロバイダMarketplaceまたはネットアップのBYOLライセンスを通じてBlueXPサブスクリプションが必要です。

コネクタを作成します

コネクタがない場合は、クラウドプロバイダでコネクタを作成します。を参照してください "AWS でコネクタを作成する" または "Azure でコネクタを作成する"または "GCP でコネクタを作成する"。ほとんどの場合、BlueXPの分類をアクティブ化する前にコネクタがセットアップされていることがほとんどです "BlueXPの機能にはコネクタが必要です"ただし、ここで設定する必要がある場合もあります。

特定のクラウドプロバイダに導入されているコネクタを使用する必要がある場合は、次のような状況があります。

- AWSのCloud Volumes ONTAP 、Amazon FSx for ONTAP 、またはAWS S3バケット内のデータをスキャンする場合は、AWSのコネクタを使用します。
- AzureのCloud Volumes ONTAP またはAzure NetApp Files でデータをスキャンする場合は、Azureのコネクタを使用します。
  - Azure NetApp Files の場合は、スキャンするボリュームと同じ領域に配置する必要があります。
- GCP の Cloud Volumes ONTAP でデータをスキャンする場合は、 GCP のコネクタを使用します。

オンプレミスのONTAP システム、ネットアップ以外のファイル共有、汎用のS3オブジェクトストレージ、データベース、OneDriveフォルダ、SharePointアカウント、Googleドライブアカウントは、これらのクラウドコネクタのいずれかを使用している場合にスキャンできます。

また、次のことも可能です "コネクタをオンプレミスにインストールします" 自社ネットワーク内またはクラウド内の Linux ホストBlueXP分類をオンプレミスにインストールすることを計画している一部のユーザは、コネクタをオンプレミスにインストールすることもできます。

ご覧のように、を使用する必要がある状況もあります "複数のコネクタ"。

政府機関によるサポート

BlueXPの分類は、コネクタが政府機関のリージョン（AWS GovCloud、Azure Gov、Azure DoD）に導入されている場合にサポートされます。この方法で導入した場合、BlueXPには次の制限があります。

- OneDriveアカウント、SharePointアカウント、Googleドライブアカウントはスキャンできません。
- Microsoft Azure Information Protection（AIP）ラベル機能を統合できません。

"政府地域へのコネクタの配置の詳細については、を参照してください"。

前提条件を確認する

BlueXPの分類をクラウドに導入する前に、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。BlueXP分類をクラウドに導入する場合、コネクタと同じサブネットに配置されます。

BlueXPの分類からアウトバウンドのインターネットアクセスを有効にします

BlueXPの分類にはアウトバウンドのインターネットアクセスが必要です。仮想ネットワークまたは物理ネットワークでインターネットアクセスにプロキシサーバを使用している場合は、次のエンドポイントに接続するためのアウトバウンドのインターネットアクセスがBlueXP分類インスタンスにあることを確認してください。プロキシは非透過である必要があります。現在、透過プロキシはサポートされていません。

AWS、Azure、GCPのいずれにBlueXP分類を導入するかに応じて、次の表を参照してください。

AWSに必要なエンドポイント

エンドポイント	目的
\ https://api.bluexp.netapp.com	ネットアップアカウントを含むBlueXPサービスとの通信
¥ https://netapp-cloud-account.auth0.com ¥ https://auth0.com	BlueXP Webサイトとの通信により、ユーザ認証を一元化。
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com \ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/ \ https://dseasb33srnrn.cloudfront.net/ \ https://production.cloudflare.docker.com/	ソフトウェアイメージ、マニフェスト、およびテンプレートにアクセスできます。
\ https://kinesis.us-east-1.amazonaws.com	ネットアップが監査レコードからデータをストリーミングできるようにします。
¥ https://cognito-idp.us-east-1.amazonaws.com ¥ https://cognito-identity.us-east-1.amazonaws.com ¥ https://user-feedback-store-prod.s3.us-west-2.amazonaws.com ¥ https://customer-data-production.s3.us-west-2.amazonaws.com	BlueXPでは、マニフェストやテンプレートへのアクセスとダウンロード、ログや指標の送信が可能です。

Azureに必要なエンドポイント

エンドポイント	目的
\ https://api.bluexp.netapp.com	ネットアップアカウントを含むBlueXPサービスとの通信
¥ https://netapp-cloud-account.auth0.com ¥ https://auth0.com	BlueXP Webサイトとの通信により、ユーザ認証を一元化。
https://support.compliance.api.bluexp.netapp.com/\ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/\ https://dseasb33srnrn.cloudfront.net/\ https://production.cloudflare.docker.com/	ソフトウェアイメージ、マニフェスト、テンプレートへのアクセス、およびログとメトリックの送信を提供します。
\ https://support.compliance.api.bluexp.netapp.com/	ネットアップが監査レコードからデータをストリーミングできるようにします。

GCPに必要なエンドポイント

エンドポイント	目的
\ https://api.bluexp.netapp.com	ネットアップアカウントを含むBlueXPサービスとの通信
¥ https://netapp-cloud-account.auth0.com ¥ https://auth0.com	BlueXP Webサイトとの通信により、ユーザ認証を一元化。

エンドポイント	目的
https://support.compliance.api.bluexp.netapp.com/\ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/\ https://dseasb33srnrn.cloudfront.net/\ https://production.cloudflare.docker.com/	ソフトウェアイメージ、マニフェスト、テンプレートへのアクセス、およびログとメトリックの送信を提供します。
\ https://support.compliance.api.bluexp.netapp.com/	ネットアップが監査レコードからデータをストリーミングできるようにします。

BlueXPに必要な権限があることを確認します

BlueXPにリソースを導入し、BlueXP分類インスタンスのセキュリティグループを作成する権限があることを確認します。BlueXPの最新の権限は、で確認できます "ネットアップが提供するポリシー"。

BlueXPコネクタから**BlueXP**分類にアクセスできることを確認します

コネクタとBlueXP分類インスタンスが接続されていることを確認します。コネクタのセキュリティグループで、ポート443を介したBlueXP分類インスタンスとの間のインバウンドおよびアウトバウンドトラフィックを許可する必要があります。この接続により、BlueXP分類インスタンスを導入し、[Compliance]タブと[Governance]タブに情報を表示できます。BlueXPの分類は、AWSとAzureの政府機関のリージョンでサポートされます。

AWSおよびAWS GovCloud環境では、追加のインバウンドおよびアウトバウンドのセキュリティグループルールが必要です。を参照してください "AWS のコネクタのルール" を参照してください。

AzureおよびAzure Government環境には、追加のインバウンドおよびアウトバウンドのセキュリティグループルールが必要です。を参照してください "Azure のコネクタのルール" を参照してください。

BlueXPの分類を継続して実行できることを確認します

データを継続的にスキャンするには、BlueXP分類インスタンスを引き続き使用する必要があります。

Webブラウザから**BlueXP**に接続できることを確認します

BlueXPの分類を有効にしたら、ユーザがBlueXPの分類インスタンスに接続されているホストからBlueXPインターフェイスにアクセスできるようにします。

BlueXP分類インスタンスでは、プライベートIPアドレスを使用して、インデックス化されたデータにインターネットからアクセスできないようにします。そのため、BlueXPへのアクセスに使用するWebブラウザには、そのプライベートIPアドレスへの接続が必要です。この接続は、クラウドプロバイダへの直接接続（VPNなど）から行うことも、BlueXP分類インスタンスと同じネットワーク内のホストから行うこともできます。

vCPU の制限を確認してください

クラウドプロバイダのvCPU制限で、必要な数のコアを含むインスタンスの導入が許可されていることを確認してください。BlueXPを実行している地域の関連するインスタンスファミリのvCPU制限を確認する必要があります。 "必要なインスタンスタイプを参照してください"。

vCPU の制限の詳細については、次のリンクを参照してください。

- "AWS のドキュメント： Amazon EC2 サービスクォータ"

- "Azure のドキュメント：「仮想マシンの vCPU クォータ"
- "Google Cloud のドキュメント：リソースクォータ"

CPUとRAMの数が少ないAWSクラウド環境のインスタンスにBlueXP分類を導入できますが、これらのシステムの使用には制限があります。を参照してください "小さいインスタンスタイプを使用しています" を参照してください。

BlueXPの分類機能をクラウドに導入します

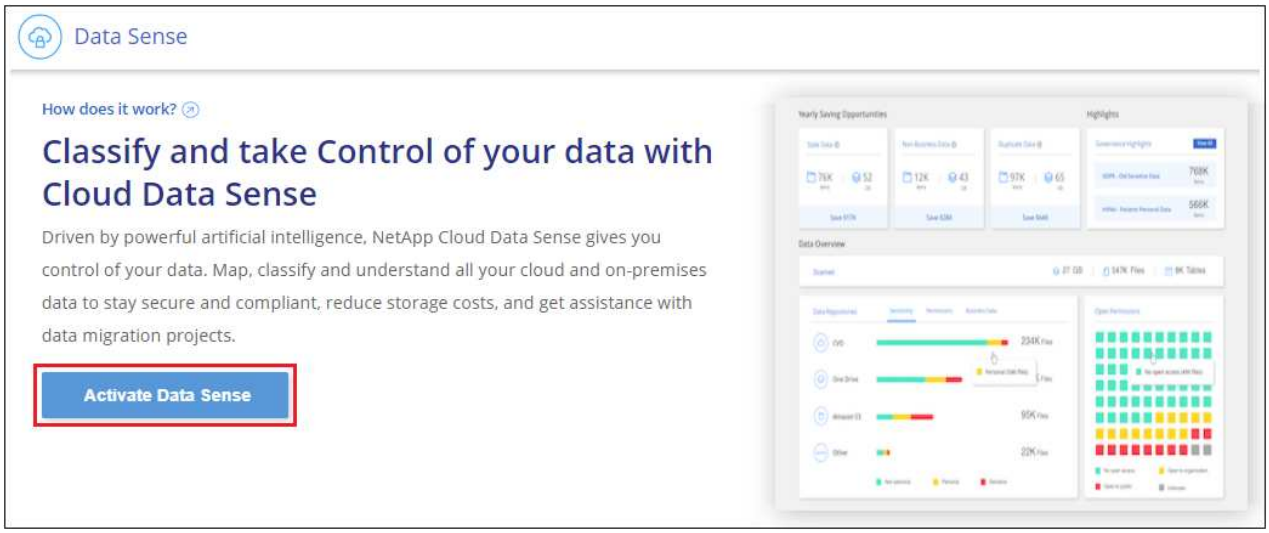
BlueXP分類のインスタンスをクラウドに導入するには、次の手順を実行します。コネクタはインスタンスをクラウドに導入し、そのインスタンスにBlueXP分類ソフトウェアをインストールします。

AWS環境でBlueXPコネクタからBlueXPの分類を導入する場合は、デフォルトのインスタンスサイズを選択するか、2つの小さいインスタンスタイプから選択できます。 "使用可能なインスタンスタイプと制限事項を参照してください"。デフォルトのインスタンスタイプを使用できない地域では、BlueXPの分類はで実行されます "代替インスタンスタイプ"。

AWSに導入

手順

1. BlueXPの左ナビゲーションメニューで、* Governance > Classification *をクリックします。



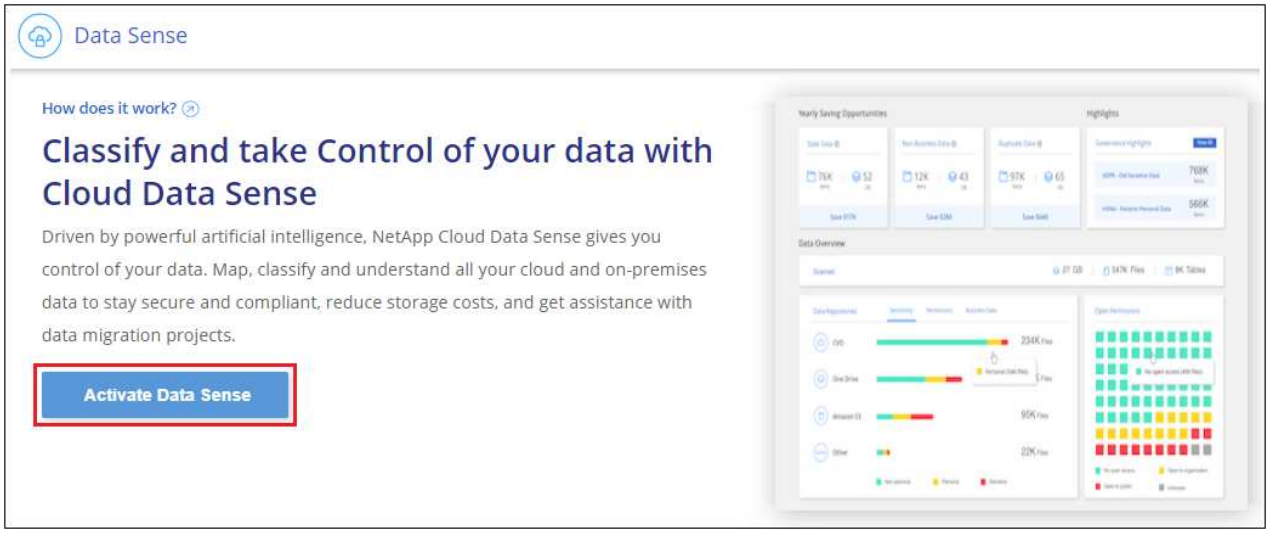
2. [データセンスを活動化（ Activate Data sense ）] をクリックし
3. [*Installation*]ページで、*[Deploy]>[Deploy]*をクリックして「Large」インスタンスサイズを使用し、クラウド導入ウィザードを開始します。
4. 導入手順が完了すると、ウィザードに進捗状況が表示されます。問題が発生した場合は、停止して入力を求められます。

5. インスタンスが導入され、BlueXP分類がインストールされたら、*[構成に進む]*をクリックして_Configuration_pageに移動します。

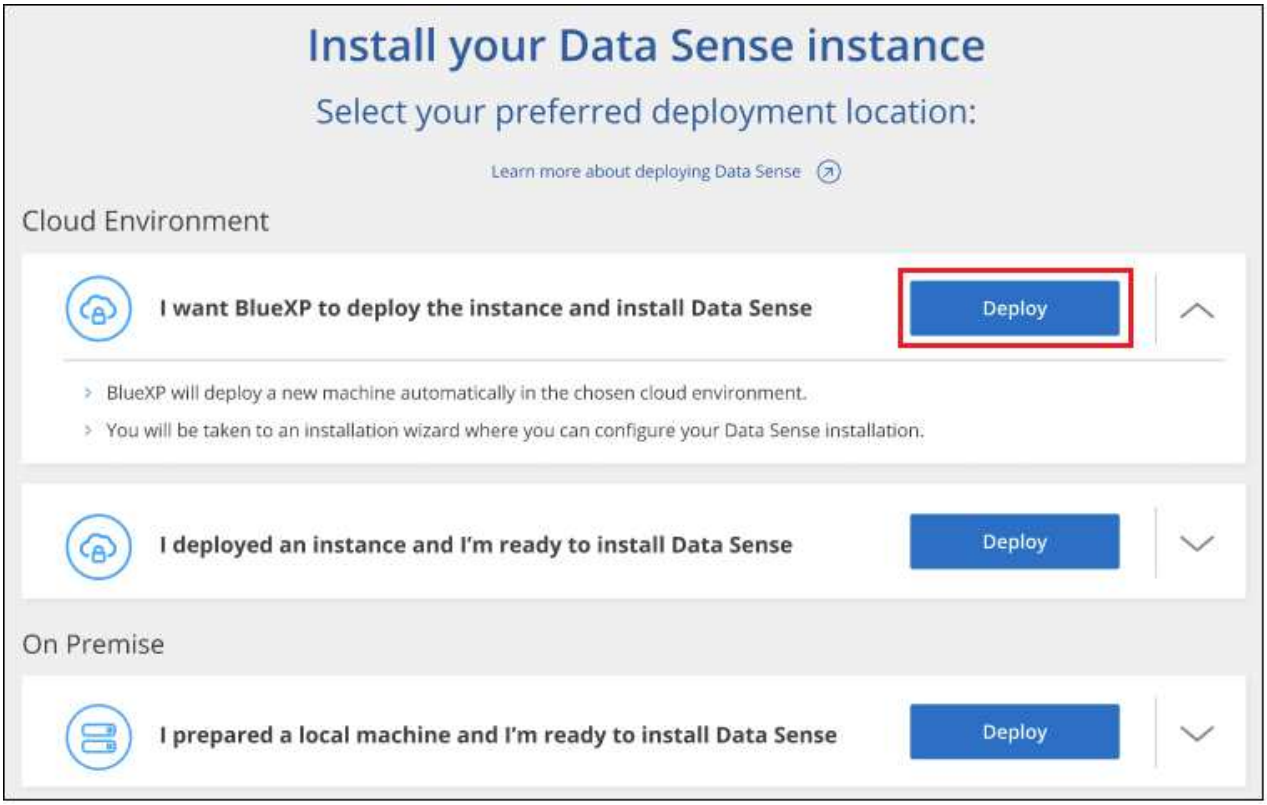
Azureへの導入

手順

1. BlueXPの左ナビゲーションメニューで、* Governance > Classification *をクリックします。
2. [データセンスを活動化（ Activate Data sense ）] をクリックし



3. [* Deploy*]をクリックして、クラウド導入ウィザードを開始します。



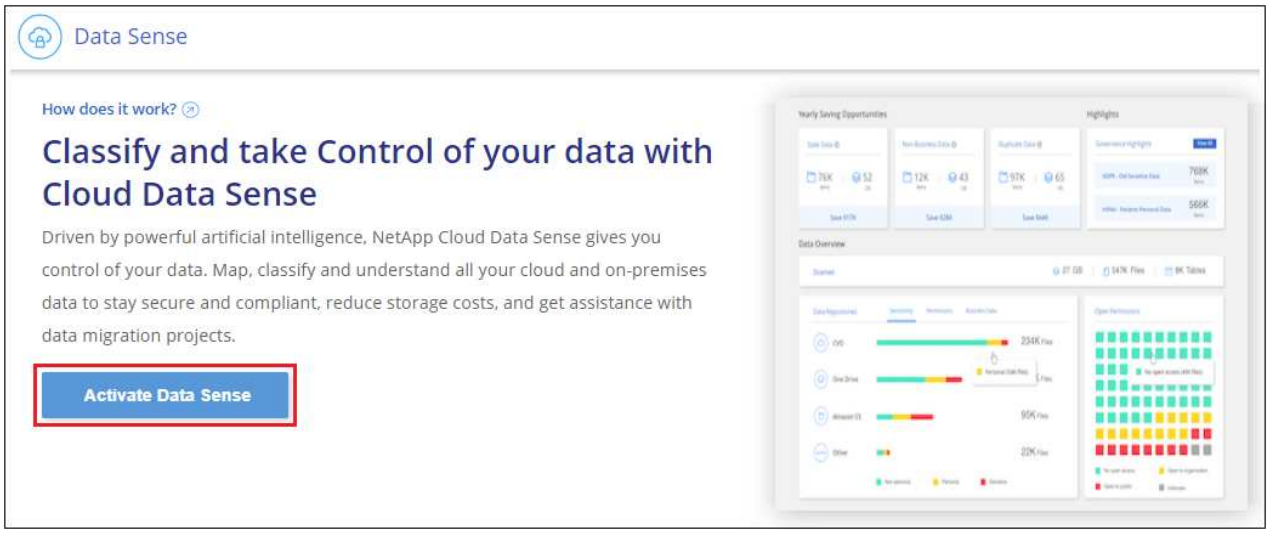
4. 導入手順が完了すると、ウィザードに進捗状況が表示されます。問題が発生した場合は、停止して入力を求められます。

5. インスタンスが導入され、BlueXP分類がインストールされたら、*[構成に進む]*をクリックして_Configuration_pageに移動します。

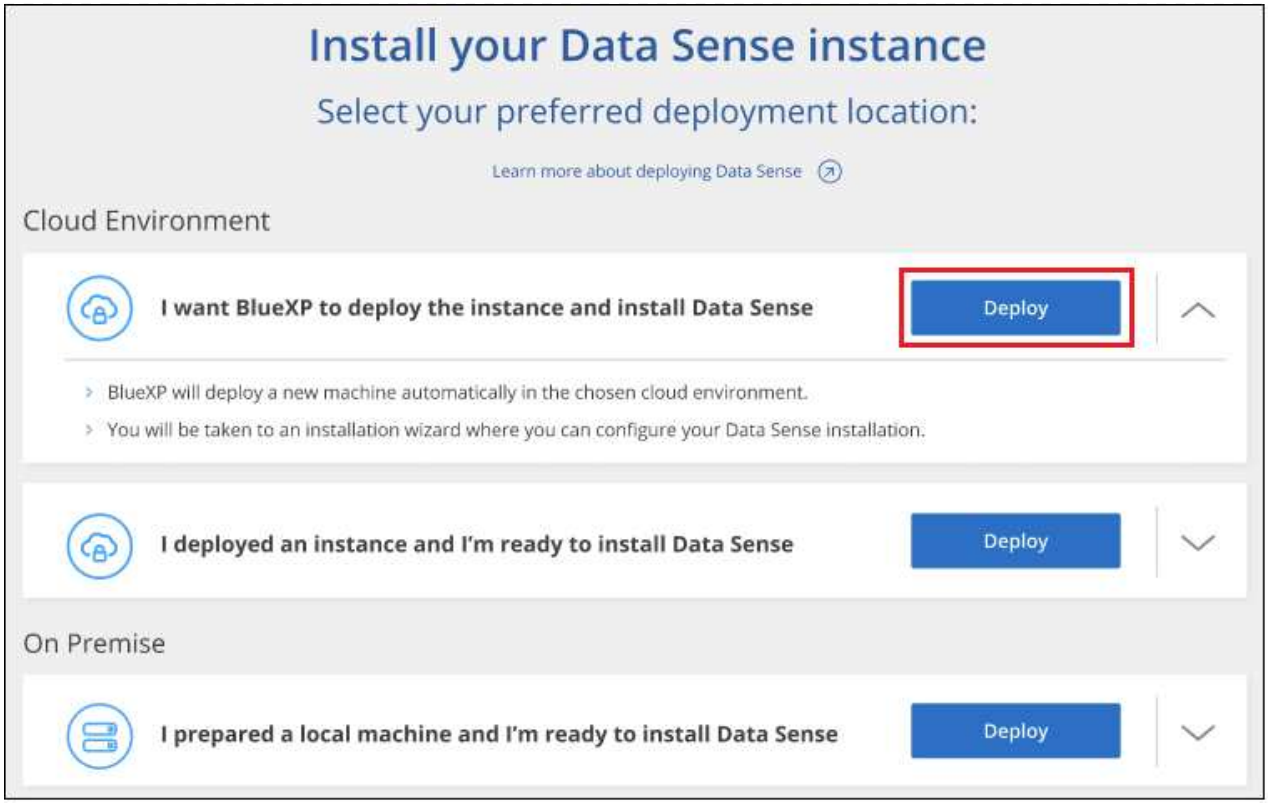
Google Cloudに導入

手順

1. BlueXPの左ナビゲーションメニューで、* Governance > Classification *をクリックします。
2. [データセンスを活動化（ Activate Data sense ）] をクリックし



3. [* Deploy*]をクリックして、クラウド導入ウィザードを開始します。



4. 導入手順が完了すると、ウィザードに進捗状況が表示されます。問題が発生した場合は、停止して入力を求められます。

5. インスタンスが導入され、BlueXP分類がインストールされたら、*[構成に進む]*をクリックして_Configuration_pageに移動します。

結果

BlueXPは、BlueXP分類インスタンスをクラウドプロバイダに導入します。

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

次のステップ

設定ページで、スキャンするデータソースを選択できます。

また可能です "BlueXP分類用のライセンスをセットアップ" 現時点では、30日間の無料トライアルが終了するまで、料金はかかりません。

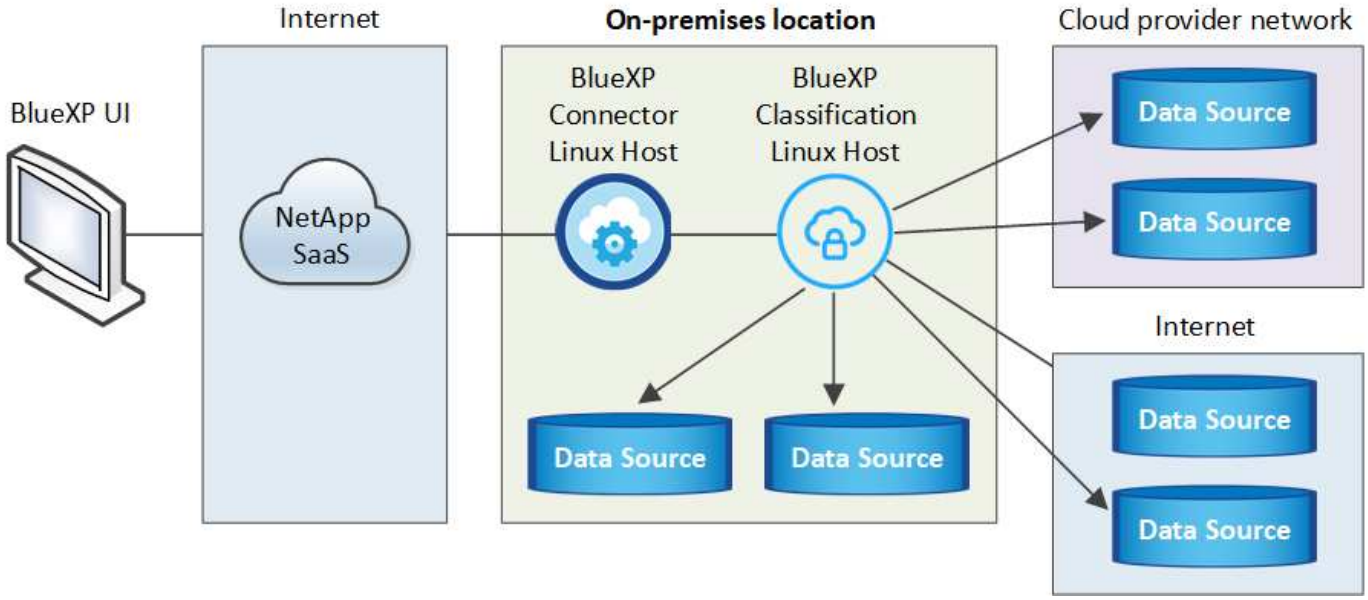
インターネットにアクセスできるホストに**BlueXP**分類をインストールします

いくつかの手順を実行して、ネットワーク内のLinuxホスト、またはインターネットにアクセスできるクラウド内のLinuxホストにBlueXP分類をインストールします。このインストールの一環として、Linuxホストをネットワークまたはクラウドに手動で導入する必要があります。

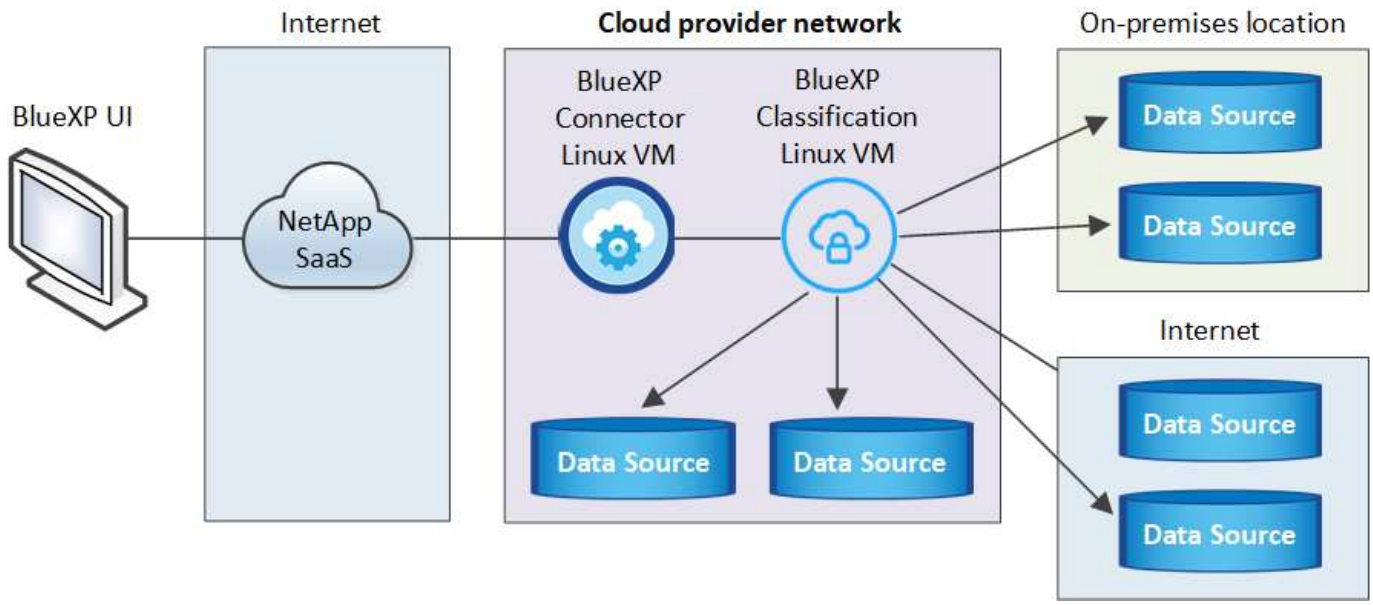
オンプレミス環境は、同じくオンプレミスにあるBlueXP分類インスタンスを使用してオンプレミスのONTAPシステムをスキャンする場合に適したオプションですが、これは必須ではありません。どのインストール方法を選択しても、ソフトウェアはまったく同じように機能します。

BlueXPの分類インストールスクリプトでは、まず、システムと環境が必要な前提条件を満たしているかどうかが確認されます。前提条件がすべて満たされている場合は、インストールが開始されます。BlueXP分類のインストールとは別に前提条件を確認する場合は、前提条件のみをテストする別のソフトウェアパッケージをダウンロードできます。 "LinuxホストでBlueXPのインストール準備が完了しているかどうかを確認する方法を説明します"。

社内_のLinuxホスト_への一般的なインストールには、次のコンポーネントと接続があります。



cloud_内のLinuxホストへの一般的なインストールには、次のコンポーネントと接続があります。



ペタバイト規模のデータをスキャンする大規模な構成では、複数のホストを含めて処理能力を追加できます。複数のホストシステムを使用する場合、プライマリシステムは_Manager node_と呼ばれ、追加の処理能力を提供する追加システムは_Scanner Node_と 呼ばれます。

また、次のことも可能です "インターネットにアクセスできないオンプレミスサイトにBlueXPの分類をインストールします" 完全にセキュアなサイトに。

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 コネクタを作成します

コネクタがない場合は、 "コネクタをオンプレミスに導入" ネットワーク内のLinuxホスト、またはクラウド内のLinuxホスト。

クラウドプロバイダを使用してコネクタを作成することもできます。を参照してください "AWS でコネクタを作成する"、 "Azure でコネクタを作成する"または "GCP でコネクタを作成する"。

2 前提条件を確認する

環境が前提条件を満たしていることを確認します。これには、インスタンスのアウトバウンドインターネットアクセス、コネクタとBlueXPのポート443経由の分類間の接続などが含まれます。 すべてのリストを参照してください。

とを満たす Linux システムも必要です 次の要件があります。

3 **BlueXP**分類をダウンロードして導入

NetApp Support Site からCloud BlueXP分類ソフトウェアをダウンロードし、使用するLinuxホストにインストーラファイルをコピーします。インストールウィザードを起動し、画面の指示に従ってBlueXP分類インスタ

ンスを導入します。

4 **BlueXP**分類サービスにサブスクライブします

BlueXPで分類されてスキャンされる最初の1TBのデータは、30日間無料です。そのあともデータのスキャンを続行するには、クラウドプロバイダ Marketplace またはネットアップの BYOL ライセンスのサブスクリプションが必要です。

コネクタを作成します

BlueXPをインストールして使用するには、BlueXPコネクタが必要です。ほとんどの場合、BlueXPの分類をアクティブ化する前にコネクタがセットアップされていることがほとんどです "BlueXPの機能にはコネクタが必要です"ただし、ここで設定する必要がある場合もあります。

クラウドプロバイダ環境で作成する場合は、を参照してください "AWS でコネクタを作成する"、 "Azure でコネクタを作成する"または "GCP でコネクタを作成する"。

特定のクラウドプロバイダに導入されているコネクタを使用する必要がある場合は、次のような状況があります。

- AWSのCloud Volumes ONTAP 、Amazon FSx for ONTAP 、またはAWS S3バケット内のデータをスキャンする場合は、AWSのコネクタを使用します。
- AzureのCloud Volumes ONTAP またはAzure NetApp Files でデータをスキャンする場合は、Azureのコネクタを使用します。

  Azure NetApp Files の場合は、スキャンするボリュームと同じ領域に配置する必要があります。

- GCP の Cloud Volumes ONTAP でデータをスキャンする場合は、 GCP のコネクタを使用します。

オンプレミスのONTAP システムでは、ネットアップ以外のファイル共有、汎用のS3オブジェクトストレージ、データベース、OneDriveフォルダ、SharePointアカウント、Googleドライブアカウントを、これらのクラウドコネクタのいずれかを使用してスキャンできます。

また、次のことも可能です "コネクタをオンプレミスに導入" ネットワーク内のLinuxホストまたはクラウド内のLinuxホスト。BlueXP分類をオンプレミスにインストールすることを計画している一部のユーザは、コネクタをオンプレミスにインストールすることもできます。

ご覧のように、を使用する必要がある状況もあります "複数のコネクタ"。

BlueXP分類をインストールするときは、コネクタシステムのIPアドレスまたはホスト名が必要です。この情報は、コネクタをオンプレミスにインストールした場合に表示されます。コネクタがクラウドに導入されている場合は、BlueXPコンソールで[ヘルプ]アイコンをクリックし、[サポート**]**を選択して、**[** BlueXPコネクタ*]をクリックします。

Linux ホストシステムを準備

BlueXP分類ソフトウェアは、特定のオペレーティングシステム要件、RAM要件、ソフトウェア要件などを満たすホストで実行する必要があります。Linuxホストは、自社ネットワークまたはクラウドに配置できます。

BlueXPの分類を継続して実行できることを確認します。BlueXP分類マシンは、データを継続的にスキャンするためにオンのままにする必要があります。

- BlueXPの分類は、他のアプリケーションと共有するホストではサポートされません。専用のホストである必要があります。
- オンプレミスでホストシステムを構築する場合は、BlueXP分類スキャンを実行するデータセットのサイズに応じて、3つのシステムサイズの中から選択できます。

システムサイズ	**CPU**	**RAM**（スワップメモリを無効にする必要があります）	ディスク
特大	CPU×32	128GBのRAM	1TiB SSDオン/または -100GiBは/optで利用可能 -895GiBを/var/lib/dockerで使用可能 -5GiB（/tmp
大きい	16 CPU	64GBのRAM	500GiB SSDオン/、または -100GiBは/optで利用可能 -395GiBは/var/lib/dockerで使用可能 -5GiB（/tmp
中	8 CPU	32GBのRAM	200GiB SSDオン/、または -50GiBは/optで利用可能 -145GiBは/var/lib/dockerで使用可能 -5GiB（/tmp
小さい	8 CPU	16GB の RAM	100GiB SSDオン/、または -50GiBは/optで利用可能 -45GiBは/var/lib/dockerで使用可能 -5GiB（/tmp

小規模なシステムを使用する場合は制限があることに注意してください。を参照してください "小さいインスタンスタイプを使用しています" を参照してください。

- BlueXP分類インストール用にコンピューティングインスタンスをクラウドに導入する場合は、上記の「大規模」システム要件を満たすシステムを推奨します。
  - * AWS EC2インスタンスタイプ*：「m6i.4xlarge」を推奨します。 "その他のAWSインスタンスタイプを参照してください"。
  - * Azure VMのサイズ*：「Standard_D16s_v3」を推奨します。 "その他のAzureインスタンスタイプを参照してください"。
  - **GCP**マシンタイプ:「n2-standard-16」をお勧めします。 "追加のGCPインスタンスタイプを参照してください"。
- * UNIXフォルダ権限*：次の最小UNIX権限が必要です。

フォルダ	最小権限
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/dockerを使用します	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- * オペレーティング・システム * ：
  - 次のオペレーティングシステムでは、Dockerコンテナエンジンを使用する必要があります。
    - Red Hat Enterprise Linuxバージョン7.8および7.9
    - CentOSバージョン7.8および7.9
    - Ubuntu 22.04（BlueXP分類バージョン1.23以降が必要）
  - 次のオペレーティングシステムでは、Podmanコンテナエンジンを使用する必要があります。また、BlueXP分類バージョン1.30以降が必要です。
    - Red Hat Enterprise Linuxバージョン8.8、9.0、9.1、9.2、9.3

      RHEL 8.xおよびRHEL 9.xを使用している場合、次の機能は現在サポートされていません。

      - タアクサイトテノセツチ
      - 分散スキャン（マスタースキャナノードとリモートスキャナノードを使用）
- * Red Hat Subscription Management * ：ホストはRed Hat Subscription Managementに登録されている必要があります。登録されていない場合、システムはインストール時に必要なサードパーティ製ソフトウェアを更新するためのリポジトリにアクセスできません。
- その他のソフトウェア：BlueXP分類をインストールする前に、次のソフトウェアをホストにインストールする必要があります。
  - 使用しているOSに応じて、次のいずれかのコンテナエンジンをインストールする必要があります。
    - Docker Engineバージョン19.3.1以降。 "インストール手順を確認します"。

      "こちらのビデオをご覧ください" では、CentOSへのDockerのインストールの簡単なデモをご覧ください。

    - Podmanバージョン4以降。Podmanをインストールするには、システムパッケージを更新します。（`sudo yum update -y`）をクリックし、Podmanをインストールします。（`sudo yum install netavark -y`）。
- Pythonバージョン3.6以降。 "インストール手順を確認します"。
  - * NTPに関する考慮事項*：NetAppでは、ネットワークタイムプロトコル（NTP）サービスを使用するようにBlueXP分類システムを設定することを推奨しています。BlueXP分類システムとBlueXP Connectorシステムの間で時刻が同期されている必要があります。
  - ファイアウォールの考慮事項:使用を計画している場合 `firewalld`は、`BlueXP`分類をインストールする前に有効にすることを推奨します。次のコマンドを実行して設定します `firewalld` BlueXPと互換性があることを確認します。

    ```
    firewall-cmd --permanent --add-service=http
    firewall-cmd --permanent --add-service=https
    firewall-cmd --permanent --add-port=80/tcp
    firewall-cmd --permanent --add-port=8080/tcp
    firewall-cmd --permanent --add-port=443/tcp
    firewall-cmd --reload
    ```

追加のBlueXP分類ホストをスキャナノードとして使用する場合は、この時点でプライマリシステムに次のルールを追加してください。

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

+
を有効または更新するたびに、DockerまたはPodmanを再起動する必要があることに注意してください。
`firewalld` 設定：

BlueXP分類ホストシステムのIPアドレスは、インストール後に変更することはできません。

BlueXPの分類からアウトバウンドのインターネットアクセスを有効にします

BlueXPの分類にはアウトバウンドのインターネットアクセスが必要です。仮想ネットワークまたは物理ネットワークでインターネットアクセスにプロキシサーバを使用している場合は、次のエンドポイントに接続するためのアウトバウンドのインターネットアクセスがBlueXP分類インスタンスにあることを確認してください。

エンドポイント	目的
\ https://api.bluexp.netapp.com	ネットアップアカウントを含むBlueXPサービスとの通信
¥ https://netapp-cloud-account.auth0.com ¥ https://auth0.com	BlueXP Webサイトとの通信により、ユーザ認証を一元化。
https://support.compliance.api.bluexp.netapp.com/\ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/\ https://dseasb33srnrn.cloudfront.net/\ https://production.cloudflare.docker.com/	ソフトウェアイメージ、マニフェスト、テンプレートへのアクセス、およびログとメトリックの送信を提供します。
\ https://support.compliance.api.bluexp.netapp.com/	ネットアップが監査レコードからデータをストリーミングできるようにします。
https://github.com/docker https://download.docker.com	Dockerのインストールに必要なパッケージを提供します。
http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	CentOSのインストールに必要なパッケージを提供します。
http://packages.ubuntu.com/ http://archive.ubuntu.com	Ubuntuのインストールに必要なパッケージを提供します。

必要なすべてのポートが有効になっていることを確認します

コネクタ、BlueXP分類、Active Directory、データソースの間の通信に必要なすべてのポートが開いていることを確認する必要があります。

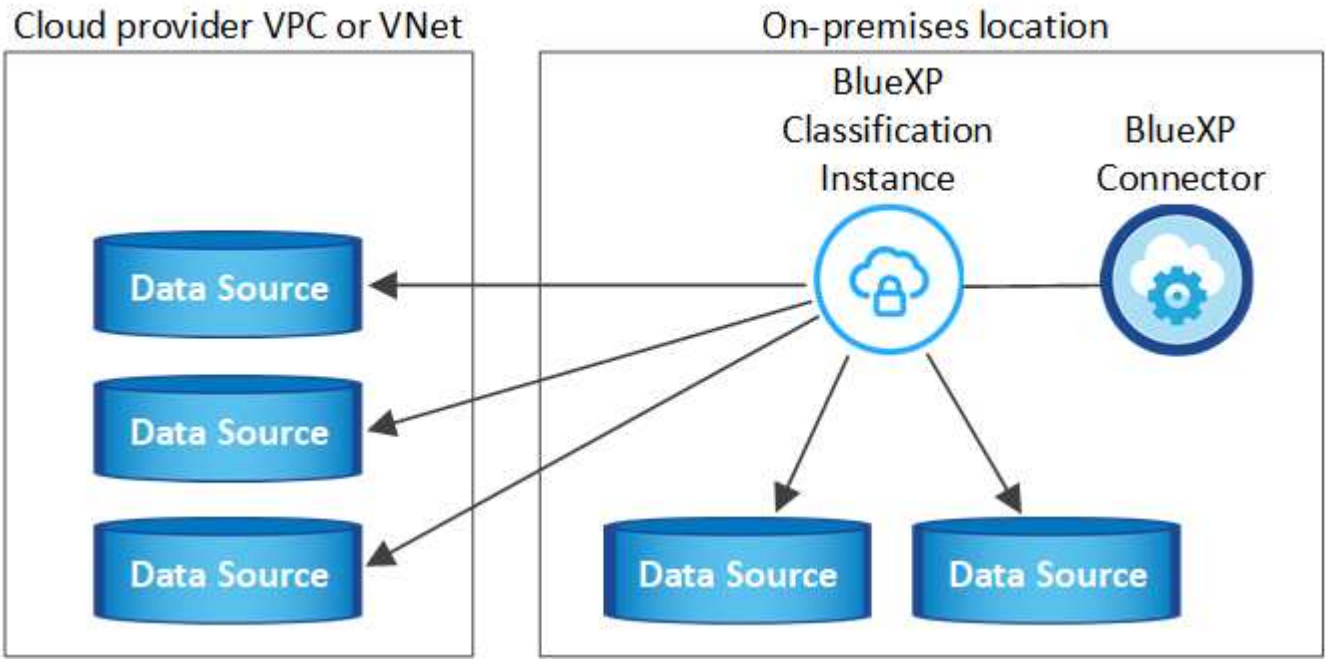
接続タイプ	ポート	説明
コネクタ<> BlueXPの分類	8080（TCP）、443（TCP）、および80	コネクタのファイアウォールルールまたはルーティングルールで、ポート443を介したBlueXP分類インスタンスとの間のインバウンドおよびアウトバウンドトラフィックを許可する必要があります。ポート8080が開いていることを確認し、BlueXPでインストールの進行状況を確認します。
Connector <> ONTAP cluster（NAS）	443（TCP）	BlueXPはHTTPSを使用してONTAP クラスタを検出しましたカスタムファイアウォールポリシーを使用する場合は、次の要件を満たす必要があります。 • コネクタホストが、ポート 443 経由のアウトバウンド HTTPS アクセスを許可する必要があります。コネクタがクラウド内にある場合、すべてのアウトバウンド通信は、事前定義されたファイアウォールまたはルーティングルールによって許可されます。 • ONTAP クラスタでは、ポート 443 を介した着信 HTTPS アクセスが許可されている必要があります。デフォルトの「 mgmt 」ファイアウォールポリシーでは、すべての IP アドレスからの着信 HTTPS アクセスが許可されます。このデフォルトポリシーを変更した場合、または独自のファイアウォールポリシーを作成した場合は、 HTTPS プロトコルをそのポリシーに関連付けて、Connector ホストからのアクセスを有効にする必要があります。
BlueXP分類<> ONTAP クラスタ	• nfs-111（TCP \ UDP）および2049（TCP \ UDP）の場合 • CIFS-139（TCP\UDP）および445（TCP\UDP）の場合	BlueXPの分類には、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 のファイアウォールまたはルーティングルールで、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-111と2049の場合は同じです • CIFS/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。

接続タイプ	ポート	説明
BlueXPの分類<> Active Directory	389（TCPおよびUDP）、636（TCP）、3268（TCP）、および3269（TCP）	社内のユーザに対して Active Directory がすでに設定されている必要があります。また、BlueXPの分類では、CIFSボリュームをスキャンするためにActive Directoryのクレデンシャルが必要です。 Active Directory の次の情報が必要です。 • DNS サーバの IP アドレス、または複数の IP アドレス • サーバーのユーザー名とパスワード • ドメイン名（Active Directory 名） • セキュアな LDAP （ LDAPS ）を使用しているかどうか • LDAP サーバポート（通常は LDAP では 389 、セキュア LDAP では 636 ）

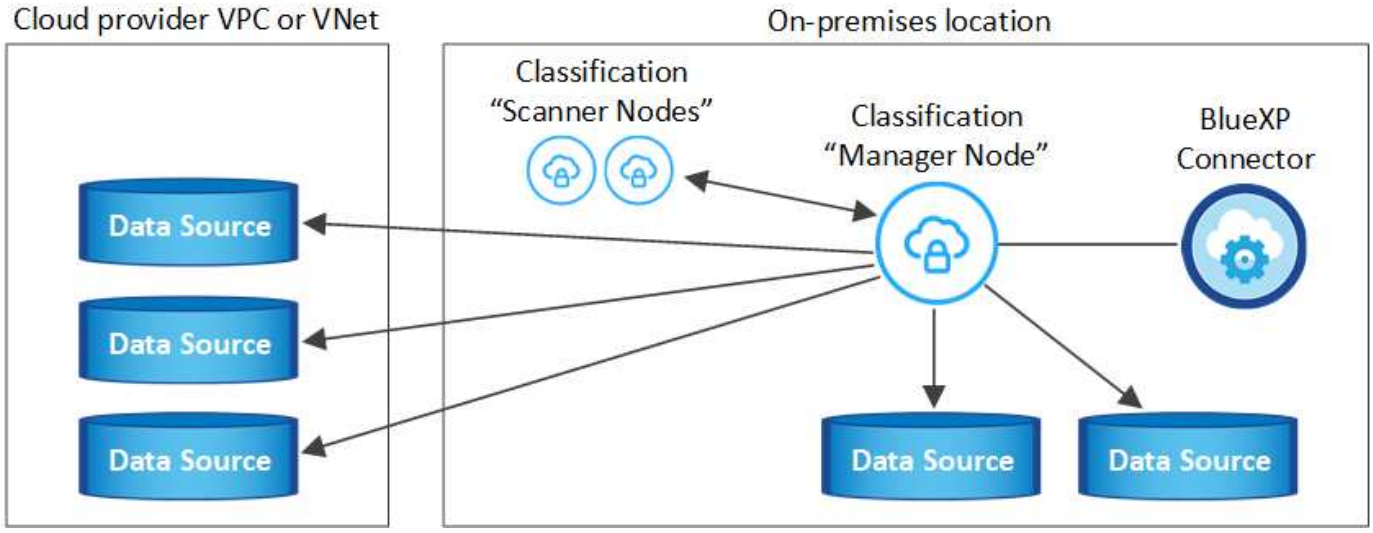
複数のBlueXP分類ホストを使用してデータソースのスキャンに必要な処理能力を提供している場合は、追加のポート/プロトコルを有効にする必要があります。 "追加のポート要件を参照してください"。

Linuxホストに**BlueXP**分類をインストールします

一般的な構成では、ソフトウェアを 1 台のホストシステムにインストールします。 これらの手順を参照してください。



ペタバイト規模のデータをスキャンする大規模な構成では、複数のホストを含めて処理能力を追加できます。これらの手順を参照してください。



を参照してください Linux ホストシステムの準備 および 前提条件の確認 では、BlueXPに分類を導入する前のすべての要件について説明します。

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。

> 現在、BlueXPの分類では、S3バケット、Azure NetApp Files 、FSx for ONTAP がオンプレミスにインストールされている場合はスキャンできません。このような場合は、BlueXP分類のコネクタとインスタンスを別 々 にクラウドとに導入する必要があります "コネクタを切り替えます" データソースごとに異なる。

一般的な構成でのシングルホストインストール

要件を確認し、BlueXP分類ソフトウェアをオンプレミスの単一のホストにインストールする場合は、以下の手順に従ってください。

"こちらのビデオをご覧ください" をクリックして、BlueXP分類のインストール方法を確認してください。

BlueXP分類をインストールすると、すべてのインストールアクティビティがログに記録されます。インストール中に問題が発生した場合は、インストール監査ログの内容を表示できます。に書き込まれます。`/opt/netapp/install_logs/`。 "詳細はこちら"。

必要なもの

- Linux システムがを満たしていることを確認します ホストの要件。
- システムに前提条件となる2つのソフトウェアパッケージ（Docker EngineまたはPodman、およびPython 3）がインストールされていることを確認します。
- Linux システムに対する root 権限があることを確認してください。
- インターネットへのアクセスにプロキシを使用している場合：
  - プロキシサーバー情報(IPアドレスまたはホスト名、接続ポート、接続スキーム: httpsまたはhttp、ユーザー名とパスワード)が必要です。
  - プロキシでTLS代行受信を実行している場合は、TLS CA証明書が格納されているBlueXP分類Linuxシステムのパスを確認しておく必要があります。
  - プロキシは非透過である必要があります。現在、透過プロキシはサポートされていません。

- ユーザはローカルユーザである必要があります。ドメインユーザはサポートされません。

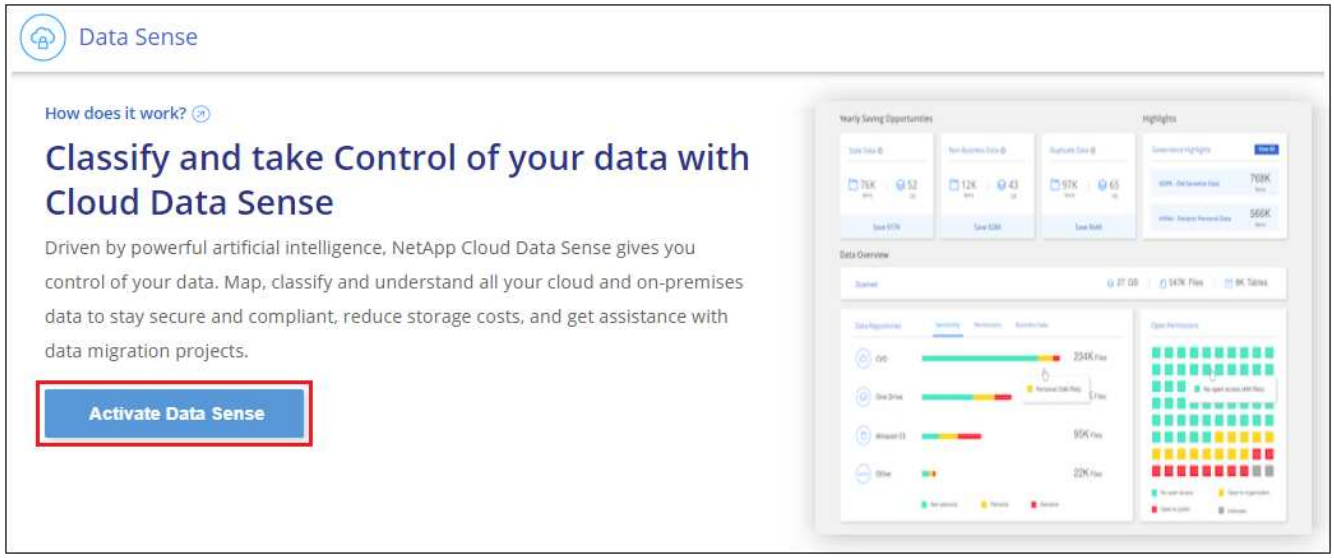
- オフライン環境が要件を満たしていることを確認します 権限と接続。

手順

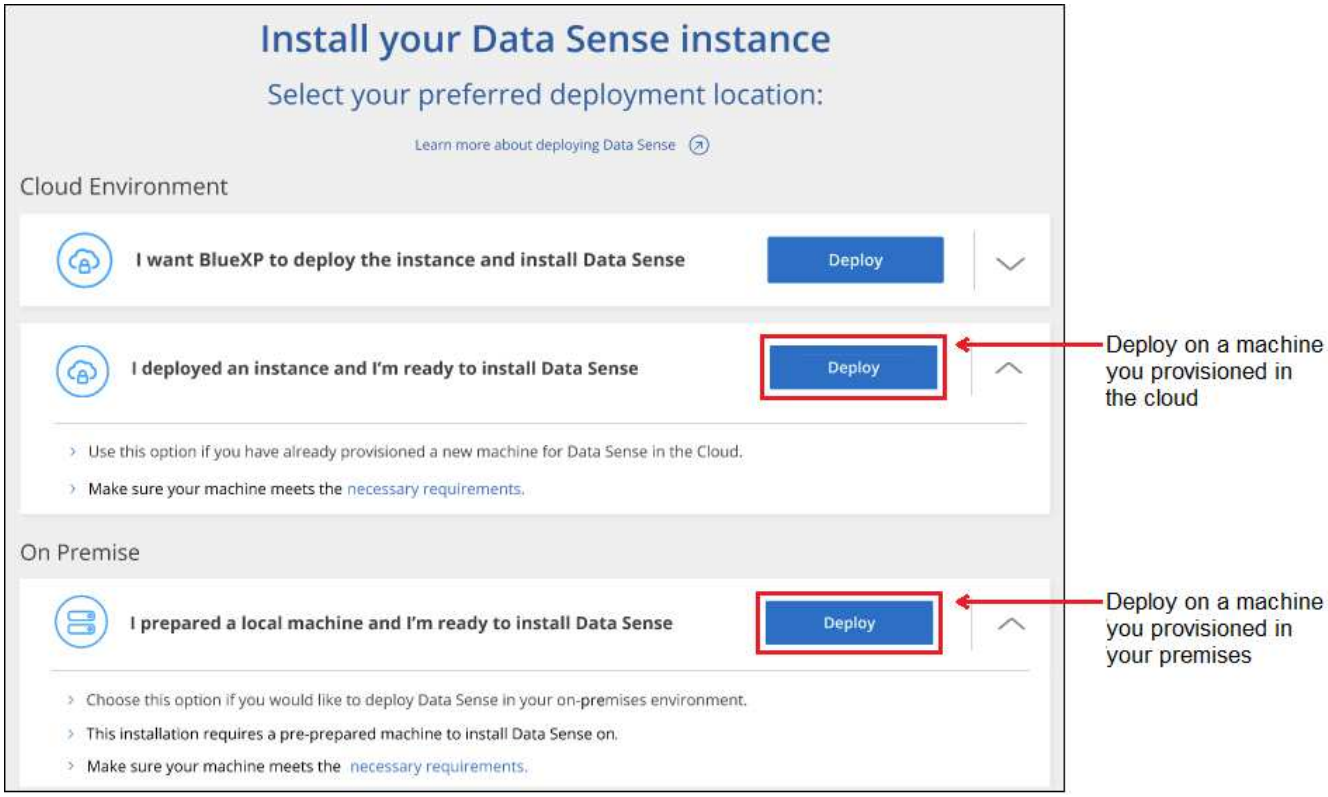
1. からBlueXP分類ソフトウェアをダウンロードします "ネットアップサポートサイト"。選択するファイルの名前は* DATASENSE-installer -<version> .tar.gz *です。
2. 使用する Linux ホストにインストーラファイルをコピーします (`cp またはその他の方法を使用) 。
3. ホストマシンでインストーラファイルを解凍します。次に例を示します。

```
tar -xzf DATASENSE-INSTALLER-V1.25.0.tar.gz
```

4. BlueXPでは、* Governance > Classification *を選択します。
5. [データセンスを活動化（ Activate Data sense ）] をクリックし



6. クラウドで準備したインスタンスとオンプレミスで準備したインスタンスのどちらにBlueXP分類をインストールするかに応じて、該当する*[Deploy]*ボタンをクリックしてBlueXP分類のインストールを開始します。



7. 「_Deploy Data Sense on Premises」ダイアログが表示されます。提供されたコマンドをコピーします（例： `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq`）をクリックし、後で使用できるようにテキストファイルに貼り付けます。次に*[閉じる]*をクリックしてダイアログを閉じます。
8. ホストマシンで、コピーしたコマンドを入力して一連のプロンプトに従います。または、必要なすべてのパラメータをコマンドライン引数として指定することもできます。

   インストールを正常に完了するには、インストーラによって事前チェックが実行され、システムとネットワークの要件が満たされていることが確認されます。 "こちらのビデオをご覧ください" 事前チェックのメッセージとその影響を理解する。

プロンプトに従ってパラメータを入力します。	完全なコマンドを入力します。
a. 手順7でコピーしたコマンドを貼り付けます。 `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token>` （オンプレミス以外の）クラウドインスタンスにインストールする場合は、を追加します `--manual-cloud-install <cloud_provider>`。 b. コネクタシステムからアクセスできるように、BlueXP分類ホストマシンのIPアドレスまたはホスト名を入力します。 c. BlueXPコネクタホストマシンのIPアドレスまたはホスト名を入力して、BlueXP分類システムからアクセスできるようにします。 d. プロンプトが表示されたら、プロキシの詳細を入力BlueXPコネクタですでにプロキシを使用している場合は、BlueXPの分類ではコネクタで使用されるプロキシが自動的に使用されるため、ここでもう一度入力する必要はありません。	または、必要なホストパラメータとプロキシパラメータを指定して、コマンド全体を事前に作成することもできます。 `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --manual-cloud-install <cloud_provider> --proxy-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy-user <proxy_user> --proxy-password <proxy_password> --cacert-folder-path <ca_cert_dir>`

変数値：

- _account_id _ = ネットアップアカウント ID
- *client_id*=コネクタクライアントID（クライアントIDがない場合は、接尾辞「clients」を追加）
- *user_token*= JWTユーザーアクセストークン
- *DS_HOST*= BlueXP分類LinuxシステムのIPアドレスまたはホスト名。
- *cm_host*= BlueXPコネクタシステムのIPアドレスまたはホスト名。
- *cloud_provider*=クラウドインスタンスにインストールする場合は、クラウドプロバイダに応じて「AWS」、「Azure」、または「GCP」を入力します。
- *proxy_host* = ホストがプロキシサーバの背後にある場合は、プロキシサーバの IP 名またはホスト名。
- *proxy_port*= プロキシサーバに接続するポート（デフォルトは 80 ）です。
- *proxy_scheme*= 接続方式： https または http （デフォルト http ）。
- *proxy_user*= ベーシック認証が必要な場合、プロキシサーバに接続するための認証されたユーザ。ローカルユーザドメインユーザである必要があります。サポートされていません。
- *proxy_password* = 指定したユーザ名のパスワード。
- *ca_cert_dir*=追加のTLS CA証明書バンドルを含むBlueXP分類Linuxシステムのパス。プロキシが TLS 代行受信を実行している場合にのみ必要です。

結果

BlueXP分類インストーラは、パッケージをインストールして登録し、BlueXP分類をインストールします。インストールには 10~20 分かかります。

ホストマシンとコネクタインスタンスの間にポート8080経由で接続が確立されている場合は、BlueXPのBlue XPの分類タブでインストールの進捗状況を確認できます。

次のステップ

設定ページで、スキャンするデータソースを選択できます。

また可能です "BlueXP分類用のライセンスをセットアップ" 現時点では、30日間の無料トライアルが終了するまで、料金はかかりません。

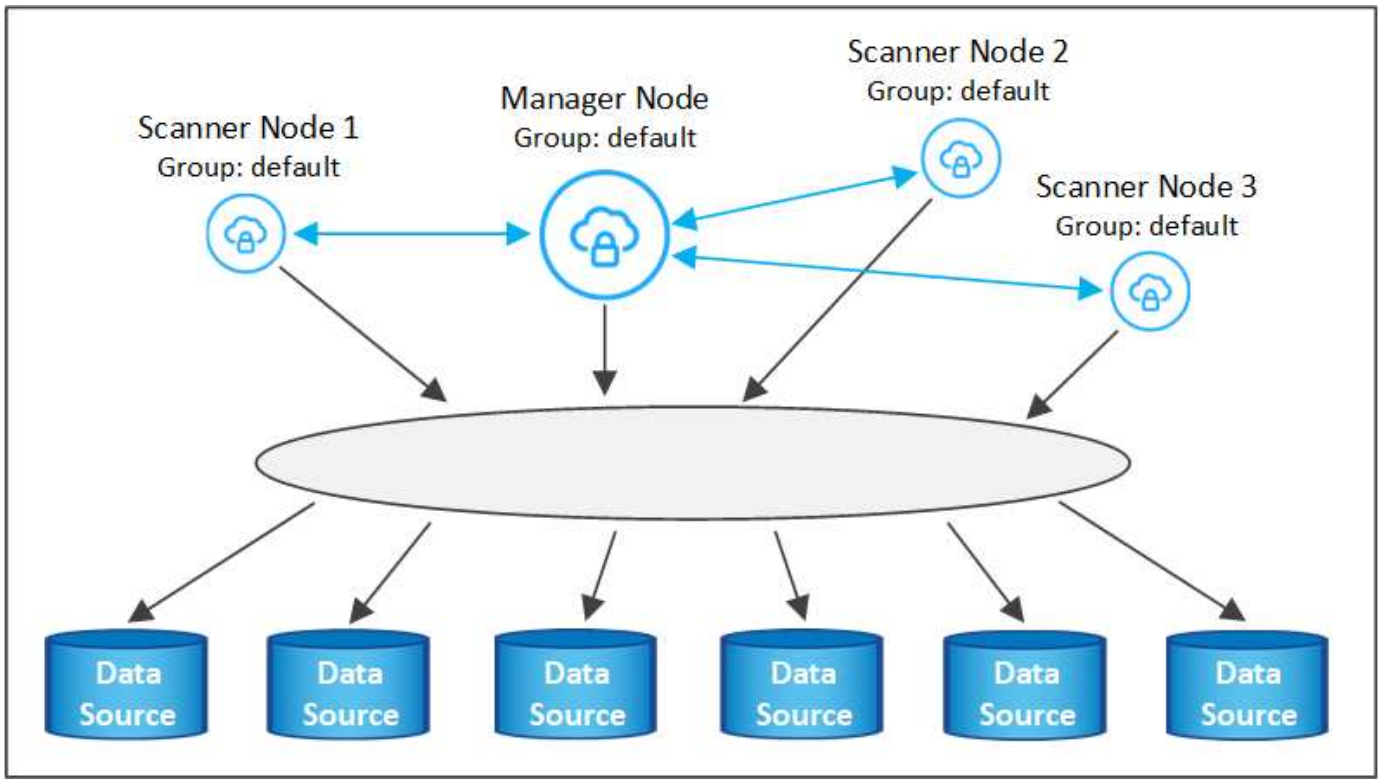
既存の環境にスキャナノードを追加する

データソースのスキャンに必要なスキャン処理能力が増えた場合は、スキャナノードを追加することができます。マネージャノードをインストールした直後にスキャナノードを追加することも、後でスキャナノードを追加することもできます。たとえば、1つのデータソースのデータ量が6カ月後に2倍または3倍になったことがわかった場合は、データスキャンに役立つ新しいスキャナノードを追加できます。

スキャナノードを追加するには、次の2つの方法があります。

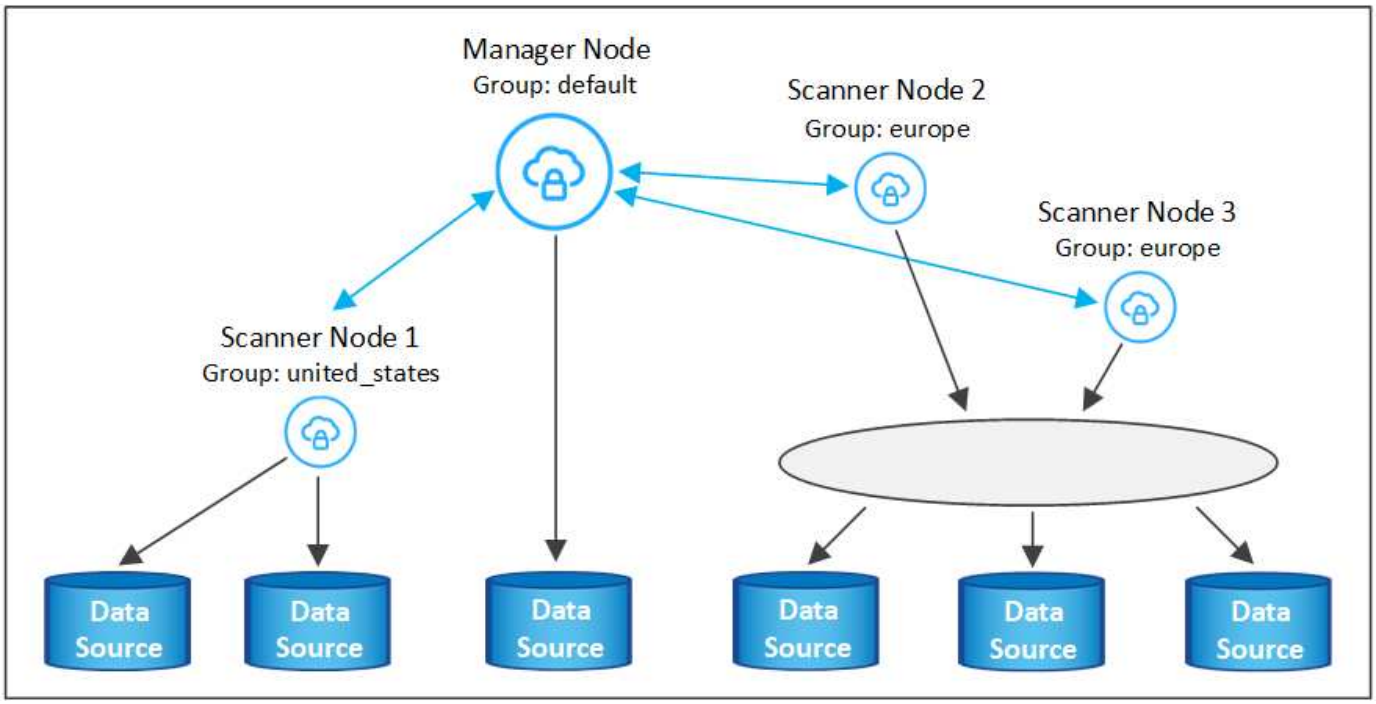
- すべてのデータソースのスキャンに使用するノードを追加します
- 特定のデータソース、または特定のデータソースグループ（通常は場所に基づく）のスキャンに役立つノードを追加する

デフォルトでは、追加した新しいスキャナノードはすべて、スキャンリソースの一般的なプールに追加されます。これを「デフォルトスキャナグループ」と呼びます。次の図では、6つすべてのデータソースからすべてのデータをスキャンする「デフォルト」グループに、1つのManagerノードと3つのスキャナノードがあります。



スキャナノードがデータソースに物理的に近いデータソースでスキャンするデータソースがある場合は、スキャナノードまたはスキャナノードのグループを定義して、特定のデータソースまたはデータソースのグループをスキャンできます。次の図では、1つのマネージャーノードと3つのスキャナーノードがあります。

- Managerノードは「デフォルト」グループにあり、1つのデータソースをスキャンしています
- スキャナノード1は「United States」グループに属し、2つのデータソースをスキャンしています
- スキャナノード2および3は「ヨーロッパ」グループに属し、3つのデータソースのスキャンタスクを共有します



BlueXPの分類スキャナグループは、データが格納される個別の地理的領域として定義できます。BlueXP分類スキャナノードは世界中に複数導入でき、ノードごとにスキャナグループを選択できます。このようにすると、各スキャナノードは最も近いデータをスキャンします。スキャナノードがデータに近いほど、データのスキャン時のネットワークレイテンシができるだけ低減されるため、データの読み取り速度が向上します。

BlueXPの分類に追加するスキャナグループとその名前を選択できます。BlueXPの分類では、「Europe」という名前のスキャナグループにマッピングされたノードがヨーロッパに導入されるわけではありません。

追加のBlueXP分類スキャナノードをインストールするには、次の手順を実行します。

1. スキャナノードとして機能するLinuxホストシステムを準備します
2. これらのLinuxシステムにデータセンスソフトウェアをダウンロードします
3. Managerノードでコマンドを実行して、スキャナノードを特定します
4. 次の手順に従って、スキャナノードにソフトウェアを展開します（また、特定のスキャナノードに対してオプションで「スキャナグループ」を定義します）。
5. スキャナグループを定義した場合は、Managerノードで次の手順を実行します。
   a. 「Working _environment To _ scanner _group_config.yml」ファイルを開き、各スキャナグループでスキャンされる作業環境を定義します
   b. 次のスクリプトを実行して、このマッピング情報をすべてのスキャナノードに登録します。
   `update_we_scanner_group_from_config_file.sh`

必要なもの

- スキャナノードのすべてのLinuxシステムがを満たしていることを確認します ホストの要件。
- システムに前提条件となる2つのソフトウェアパッケージ（Docker EngineまたはPodman、およびPython 3）がインストールされていることを確認します。
- Linux システムに対する root 権限があることを確認してください。
- 環境が要件を満たしていることを確認します 権限と接続。
- 追加するスキャナノードホストのIPアドレスを確認しておく必要があります。
- BlueXP Classification Managerノードのホストシステムの IPアドレスが必要です
- コネクタシステムのIPアドレスまたはホスト名、ネットアップアカウントID、コネクタクライアントID、およびユーザアクセストークンが必要です。スキャナグループを使用する場合は、アカウントの各データソースの作業環境IDを確認しておく必要があります。この情報を取得するには、以下の*必要条件ステップ*を参照してください。
- すべてのホストで次のポートとプロトコルを有効にする必要があります。

ポート	プロトコル	説明
2377	TCP	クラスタ管理通信
7946	tcp 、 udp です	ノード間通信
4789	UDP	オーバーレイネットワークトラフィック
50	ESP	暗号化された IPsec オーバーレイネットワーク（ ESP ）トラフィック
111	tcp 、 udp です	ホスト間でファイルを共有するための NFS サーバ（各スキャナノードからマネージャノードに必要）
2049	tcp 、 udp です	ホスト間でファイルを共有するための NFS サーバ（各スキャナノードからマネージャノードに必要）

- 使用するポート `firewalld` BlueXP分類マシンでは、BlueXP分類をインストールする前に有効にすることを推奨します。次のコマンドを実行して設定します `firewalld` BlueXPと互換性があることを確認します。

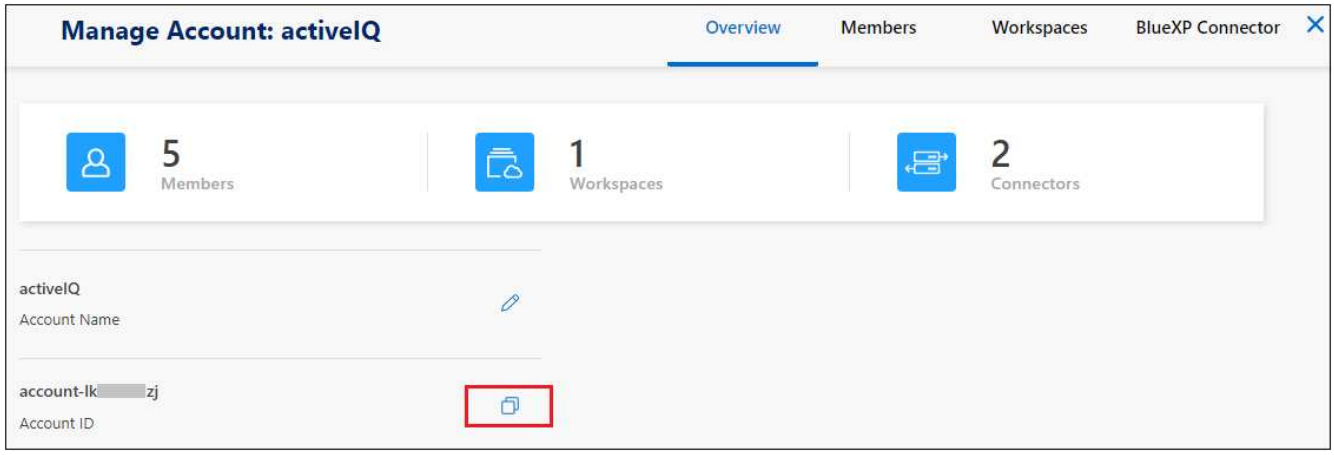
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
firewall-cmd --reload
```

を有効または更新するたびに、DockerまたはPodmanを再起動する必要があることに注意してください。`firewalld` 設定：

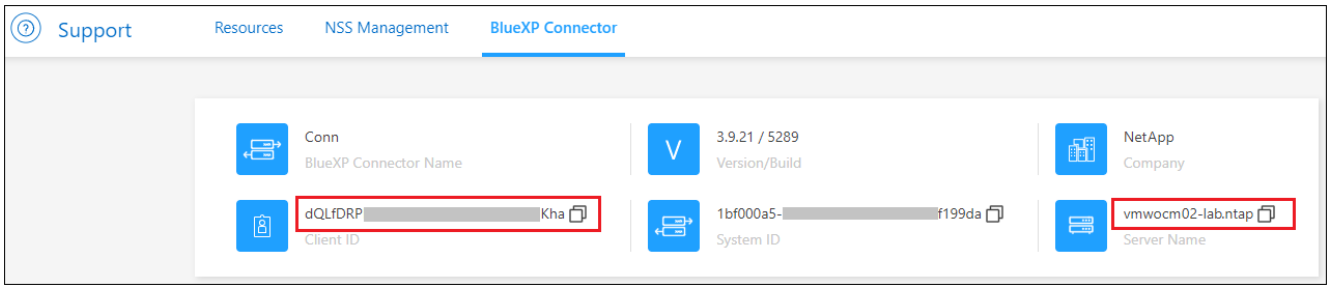
事前に必要な手順

次の手順に従って、スキャナノードの追加に必要なネットアップアカウントID、コネクタクライアントID、コネクタサーバ名、およびユーザアクセストークンを取得します。

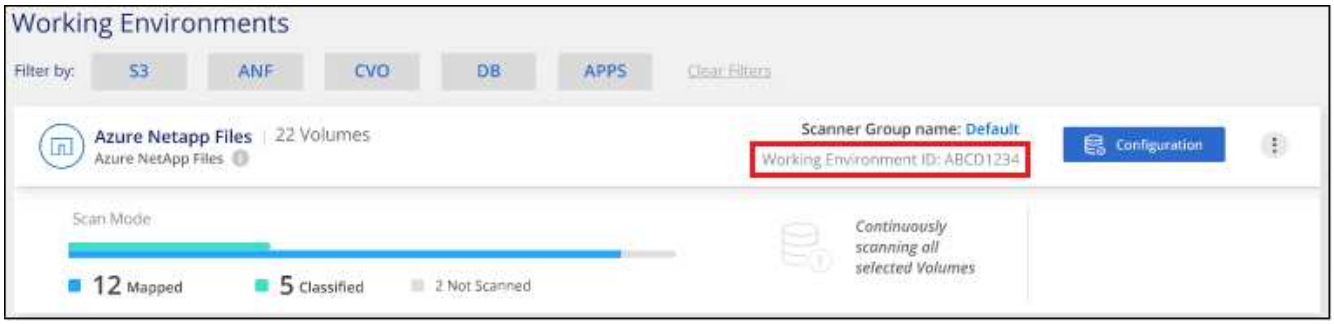
1. BlueXPのメニューバーで、*アカウント>アカウントの管理*をクリックします。



2. _アカウントID_をコピーします。
3. BlueXPメニューバーで、[ヘルプ]>[サポート]>[BlueXPコネクタ*]をクリックします。

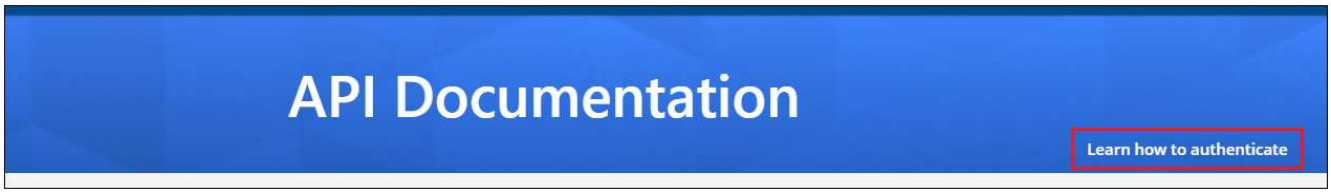


4. Connector_Client ID_と_サーバ名_をコピーします。
5. スキャナグループを使用する場合は、BlueXP分類の[設定]タブで、スキャナグループに追加する各作業環境の作業環境IDをコピーします。



ページに表示されるWorking Environment IDのスクリーンショット。"]

6. にアクセスします "APIドキュメント開発者ハブ" [**Learn how to authenticate**(認証方法を確認する)]をクリック



7. 「ユーザー名」と「パスワード」パラメータのアカウント管理者のユーザー名とパスワードを使用して、認証手順に従ってください。
8. 次に、応答から_access token_をコピーします。

手順

1. BlueXP Classification Managerノードで、スクリプト「add_scanner_node.sh」を実行します。たとえば、次のコマンドはスキャナノードを2つ追加します。

   ```
   sudo ./add_scanner_node.sh -a <account_id> -c <client_id> -m <cm_host> -h
   <ds_manager_ip> -n <node_private_ip_1,node_private_ip_2> -t <user_token>
   ```

   変数値：

   - _account_id _ = ネットアップアカウント ID
   - *client_id*=コネクタクライアントID（前提条件ステップでコピーしたクライアントIDに接尾辞「clients」を追加）
   - *cm_host*=コネクタシステムのIPアドレスまたはホスト名
   - *DS_manager_IP*= BlueXP Classification Managerノードシステムのプライベートアドレス
   - *node_private_IP*= BlueXP分類スキャナノードシステムのIPアドレス（複数のスキャナノードIPはカンマで区切ります）
   - *user_token*= JWTユーザーアクセストークン
2. add_scanner_nodeスクリプトが完了する前に、スキャナノードに必要なインストールコマンドを示すダイアログが表示されます。コマンドをコピーします（例： `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF1s35212 -u red95467j`）を入力し、テキストファイルに保存します。
3. 各 * スキャナノードホストで：
   a. データセンスインストーラファイル(**DATASENSE-installer -<version> .tar.gz**)をホストマシンにコピーします(scpなどの方法を使用)。
   b. インストーラファイルを解凍します。
   c. 手順2でコピーしたコマンドを貼り付けて実行します。
   d. スキャナノードを「スキャナグループ」に追加する場合は、パラメータ*-r <scanner_group_name>*をコマンドに追加します。それ以外の場合は、スキャナノードが「デフォルト」グループに追加されます。

      すべてのスキャナノードでインストールが完了し、それらのノードがマネージャノードに参加したら、「add_scanner_node.sh」スクリプトも終了します。インストールには10~20分かかることがあります。
4. スキャナグループにスキャナノードを追加した場合は、マネージャノードに戻り、次の2つのタスクを実行します。

a. 「/opt/netapp/config/custom _configuration/working_environment_to_scanner_group_config.yml」ファイルを開き、スキャナグループが特定の作業環境をスキャンするマッピングを入力します。データソースごとに_Working Environment ID_が必要になります。たとえば、次のエントリでは、2つの作業環境を「ヨーロッパ」スキャナグループに、2つを「United States」スキャナグループに追加します。

```
scanner_groups:
 europe:
   working_environments:
     - "working_environment_id1"
     - "working_environment_id2"
 united_states:
   working_environments:
     - "working_environment_id3"
     - "working_environment_id4"
```

リストに追加されていない作業環境は、「デフォルト」グループによってスキャンされます。「デフォルト」グループには、少なくとも1つのマネージャまたはスキャナノードが必要です。

b. 次のスクリプトを実行して、このマッピング情報をすべてのスキャナノードに登録します。
`/opt/netapp/Datasense/tools/update_we_scanner_group_from_config_file.sh`

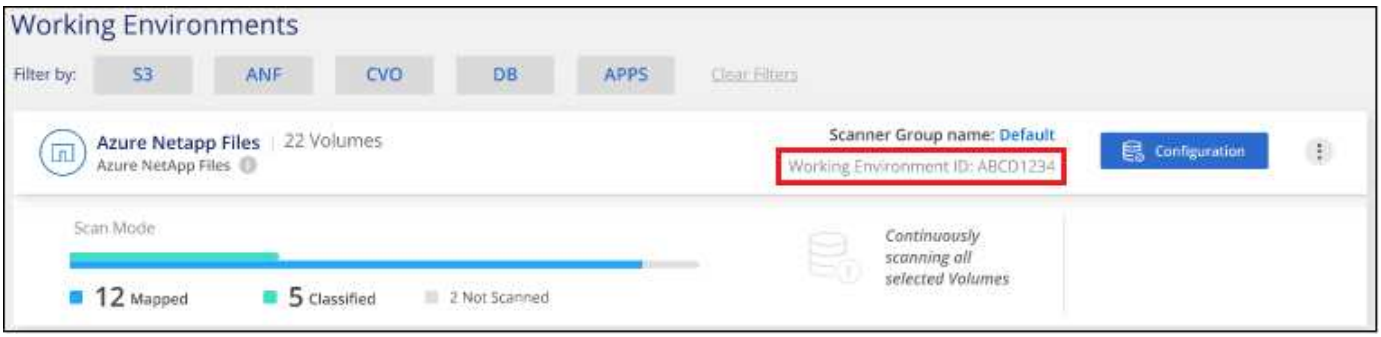
結果

BlueXPの分類は、ManagerノードとScannerノードで設定され、すべてのデータソースがスキャンされます。

次のステップ

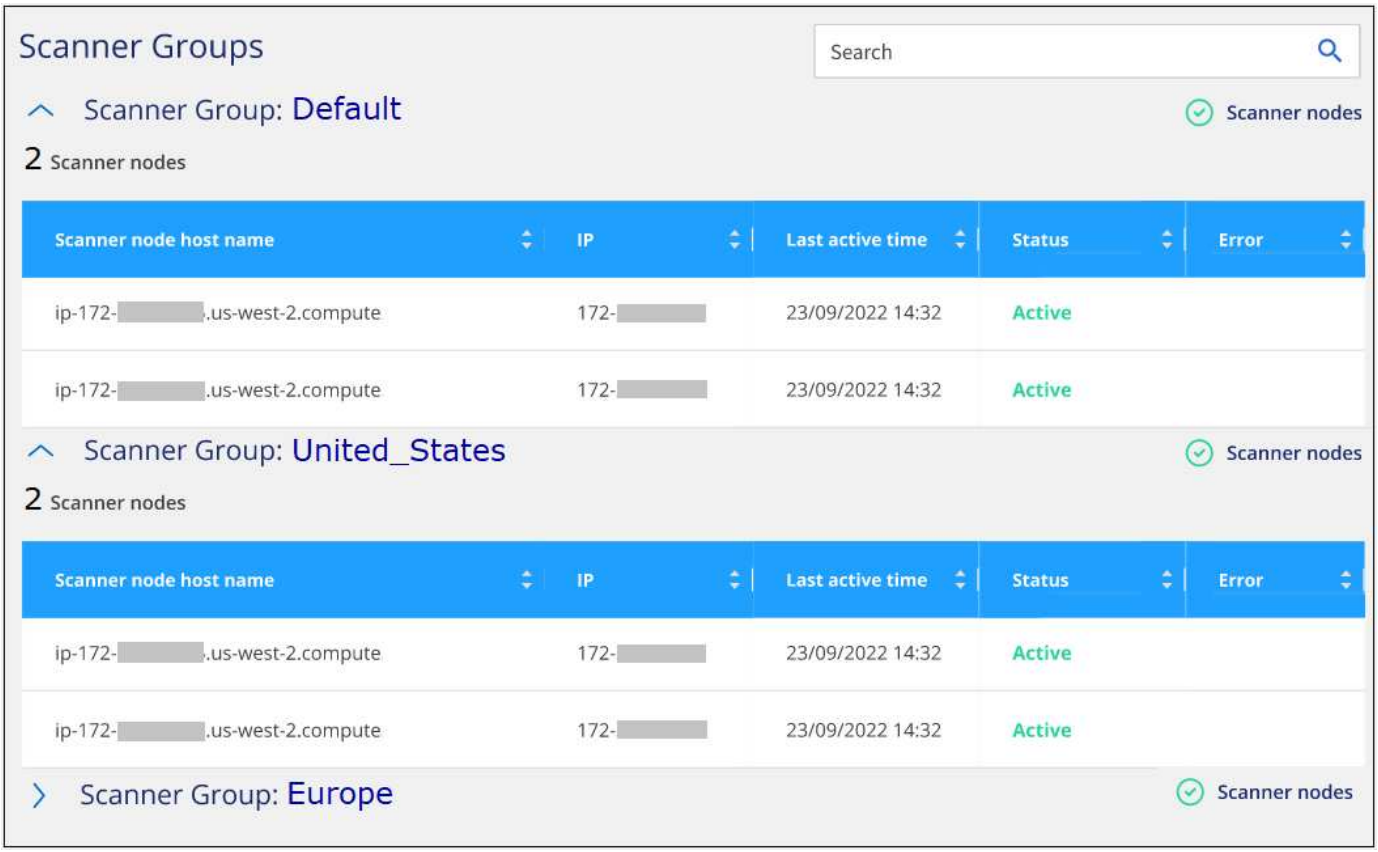
設定ページで、スキャンするデータソースを選択できます（まだ選択していない場合）。スキャナグループを作成した場合は、各データソースがそれぞれのグループのスキャナノードによってスキャンされます。

各作業環境のスキャナグループ名は、設定ページに表示されます。



ページに表示されるWorking Environment IDのスクリーンショット。"]

また、すべてのスキャナグループのリスト、および[設定]ページの下部にあるグループ内の各スキャナノードのIPアドレスとステータスを表示することもできます。



可能です "BlueXP分類用のライセンスをセットアップ" 現時点では、30日間の無料トライアルが終了するまで、料金はかかりません。

大規模構成向けのマルチホストインストール

ペタバイト規模のデータをスキャンする大規模な構成では、複数のホストを含めて処理能力を追加できます。複数のホストシステムを使用する場合、プライマリシステムは _Managernode_name と呼ばれ、追加の処理能力を提供する追加システムは _Scanner Node_と 呼ばれます。

複数のオンプレミスホストにBlueXP分類ソフトウェアを同時にインストールする場合は、次の手順に従います。この方法で複数のホストを導入する場合、「スキャナグループ」は使用できません。

必要なもの

- Manager ノードと Scanner ノードのすべての Linux システムが、を満たしていることを確認します ホストの要件。
- システムに前提条件となる2つのソフトウェアパッケージ（DockerまたはPodman Engine、およびPython 3）がインストールされていることを確認します。
- Linux システムに対する root 権限があることを確認してください。
- 環境が要件を満たしていることを確認します 権限と接続。
- 使用するスキャナノードホストの IP アドレスを確認しておく必要があります。
- すべてのホストで次のポートとプロトコルを有効にする必要があります。

ポート	プロトコル	説明
2377	TCP	クラスタ管理通信

ポート	プロトコル	説明
7946	tcp 、 udp です	ノード間通信
4789	UDP	オーバーレイネットワークトラフィック
50	ESP	暗号化された IPsec オーバーレイネットワーク（ ESP ）トラフィック
111	tcp 、 udp です	ホスト間でファイルを共有するための NFS サーバ（各スキャナノードからマネージャノードに必要）
2049	tcp 、 udp です	ホスト間でファイルを共有するための NFS サーバ（各スキャナノードからマネージャノードに必要）

手順

1. の手順 1~7 を実行します シングルホストインストール マネージャーノード。
2. 手順 8 で示したように、インストーラからプロンプトが表示されたら、一連のプロンプトに必要な値を入力するか、必要なパラメータをコマンドライン引数としてインストーラに指定することができます。

   シングルホストのインストールで使用できる変数に加えて、新しいオプション * -n <Node_IP> * を使用してスキャナノードの IP アドレスを指定します。複数のスキャナノードの IP はカンマで区切って指定します。

   たとえば、次のコマンドは3つのスキャナノードを追加します。
   ```
   sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host
   <ds_host> --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --proxy
   -host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme>
   --proxy-user <proxy_user> --proxy-password <proxy_password>
   ```
3. マネージャノードのインストールが完了する前に、スキャナノードに必要なインストールコマンドがダイアログに表示されます。コマンドをコピーします（例： `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`）を入力し、テキストファイルに保存します。
4. 各 * スキャナノードホストで：
   a. データセンスインストーラファイル(**DATASENSE-installer -<version> .tar.gz**)をホストマシンにコピーします(scpなどの方法を使用)。
   b. インストーラファイルを解凍します。
   c. 手順 3 でコピーしたコマンドを貼り付けて実行します。

      すべてのスキャナノードでインストールが完了し、それらのノードがマネージャノードに参加したら、マネージャノードのインストールも完了します。

結果

BlueXP分類インストーラがパッケージのインストールを完了し、インストールを登録します。インストールには 10~20 分かかります。

次のステップ

設定ページで、スキャンするデータソースを選択できます。

また可能です "BlueXP分類用のライセンスをセットアップ" 現時点では、30日間の無料トライアルが終了する

まで、料金はかかりません。

インターネットアクセスのない**Linux**ホストに**BlueXP**分類をインストールする

インターネットアクセスがないオンプレミスサイト（_private mode_とも呼ばれます）のLinuxホストにBlueXP分類をインストールするには、いくつかの手順を実行します。このタイプのインストールは、セキュアなサイトに最適です。

"BlueXP ConnectorとBlueXPの分類のさまざまな導入モードについて説明します。"。

また、次のことも可能です "インターネットにアクセスできるオンプレミスサイトにBlueXPの分類を導入します"。

BlueXPの分類インストールスクリプトでは、まず、システムと環境が必要な前提条件を満たしているかどうかが確認されます。前提条件がすべて満たされている場合は、インストールが開始されます。BlueXP分類のインストールとは別に前提条件を確認する場合は、前提条件のみをテストする別のソフトウェアパッケージをダウンロードできます。 "LinuxホストでBlueXPのインストール準備が完了しているかどうかを確認する方法を説明します"。

サポートされているデータソース

プライベートモード（「オフライン」または「ダーク」サイトと呼ばれることもある）がインストールされている場合、BlueXPの分類では、オンプレミスサイトに対してローカルなデータソースのデータしかスキャンできません。現時点では、BlueXPでは次の*ローカル*データソースをスキャンできます。

- オンプレミスの ONTAP システム
- データベーススキーマ
- SharePointオンプレミスアカウント(SharePoint Server)
- ネットアップ以外の NFS または CIFS ファイル共有
- Simple Storage Service （ S3 ）プロトコルを使用するオブジェクトストレージ

現在、Cloud Volumes ONTAP、Azure NetApp Files、FSx for ONTAP、AWS S3、Googleドライブのスキャンはサポートされていません。 BlueXP分類がプライベートモードで導入されている場合は、OneDriveまたはSharePoint Onlineアカウント。

制限

BlueXPのほとんどの分類機能は、インターネットアクセスのないサイトに導入した場合に機能します。ただし、インターネットアクセスを必要とする特定の機能はサポートされていません。たとえば、次のような機能があります。

- Microsoft Azure Information Protection （ AIP ）ラベルの管理
- 特定の重要なポリシーの結果が返されたときに、BlueXPユーザーに電子メールアラートを送信する
- 異なるユーザーのBlueXPロールの設定(アカウント管理者やCompliance Viewerなど)
- BlueXPのコピーと同期を使用したソースファイルのコピーと同期
- ユーザからのフィードバックを受け取る
- BlueXPからの自動ソフトウェアアップグレード

BlueXP ConnectorとBlueXPのどちらも、新機能を有効にするために定期的な手動アップグレードが必要になります。BlueXP分類バージョンは、BlueXP分類UIページの下部で確認できます。を確認します "BlueXPの分類に関するリリースノート" 各リリースの新機能と、それらの機能が必要かどうかを確認できます。次に、の手順を実行します "BlueXP Connectorをアップグレードします" および BlueXP分類ソフトウェアをアップグレードします。

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 **BlueXP**コネクタを取り付けます

プライベートモードでコネクタがインストールされていない場合は、 "コネクタを配置します" Linux ホストの場合は、

2 **BlueXP**の分類の前提条件を確認します

Linux システムがを満たしていることを確認します ホストの要件必要なソフトウェアがすべてインストールされていること、およびオフライン環境が要件を満たしていることを確認します 権限と接続。

3 **BlueXP**分類をダウンロードして導入

NetApp Support Site からBlueXP分類ソフトウェアをダウンロードし、使用するLinuxホストにインストーラファイルをコピーします。インストールウィザードを起動し、画面の指示に従ってBlueXP分類インスタンスを導入します。

4 **BlueXP**分類サービスにサブスクライブします

BlueXPで分類されてスキャンされる最初の1TBのデータは、30日間無料です。そのあともデータのスキャンを続行するには、ネットアップの BYOL ライセンスが必要です。

BlueXPコネクタを取り付けます

BlueXP Connectorがプライベートモードでインストールされていない場合は、 "コネクタを配置します" オフラインサイトの Linux ホスト

Linux ホストシステムを準備

BlueXP分類ソフトウェアは、特定のオペレーティングシステム要件、RAM要件、ソフトウェア要件などを満たすホストで実行する必要があります。

- BlueXPの分類は、他のアプリケーションと共有するホストではサポートされません。専用のホストである必要があります。
- オンプレミスでホストシステムを構築する場合は、BlueXP分類スキャンを実行するデータセットのサイズに応じて、3つのシステムサイズの中から選択できます。

システムサイズ	**CPU**	**RAM**（スワップメモリを無効にする必要があります）	ディスク
特大	CPU×32	128GBのRAM	1TiB SSDオン/または -100GiBは/optで利用可能 -895GiBを/var/lib/dockerで使用可能 -5GiB（/tmp
大きい	16 CPU	64GBのRAM	500GiB SSDオン/、または -100GiBは/optで利用可能 -395GiBは/var/lib/dockerで使用可能 -5GiB（/tmp
中	8 CPU	32GBのRAM	200GiB SSDオン/、または -50GiBは/optで利用可能 -145GiBは/var/lib/dockerで使用可能 -5GiB（/tmp
小さい	8 CPU	16GB の RAM	100GiB SSDオン/、または -50GiBは/optで利用可能 -45GiBは/var/lib/dockerで使用可能 -5GiB（/tmp

小規模なシステムを使用する場合は制限があることに注意してください。を参照してください "小さいインスタンスタイプを使用しています" を参照してください。

- BlueXP分類インストール用にコンピューティングインスタンスをクラウドに導入する場合は、上記の「大規模」システム要件を満たすシステムを推奨します。
  - * AWS EC2インスタンスタイプ*：「m6i.4xlarge」を推奨します。 "その他のAWSインスタンスタイプを参照してください"。
  - * Azure VMのサイズ*：「Standard_D16s_v3」を推奨します。 "その他のAzureインスタンスタイプを参照してください"。
  - **GCP**マシンタイプ:「n2-standard-16」をお勧めします。 "追加のGCPインスタンスタイプを参照してください"。
- * UNIXフォルダ権限*：次の最小UNIX権限が必要です。

フォルダ	最小権限
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/dockerを使用します	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- * オペレーティング・システム * ：
  - 次のオペレーティングシステムでは、Dockerコンテナエンジンを使用する必要があります。
    - Red Hat Enterprise Linuxバージョン7.8および7.9

    - CentOSバージョン7.8および7.9
    - Ubuntu 22.04（BlueXP分類バージョン1.23以降が必要）
  - 次のオペレーティングシステムでは、Podmanコンテナエンジンを使用する必要があります。また、BlueXP分類バージョン1.30以降が必要です。
    - Red Hat Enterprise Linuxバージョン8.8、9.0、9.1、9.2、9.3

      RHEL 8.xおよびRHEL 9.xを使用している場合、次の機能は現在サポートされていません。

      - タアクサイトテノセツチ
      - 分散スキャン（マスタースキャナノードとリモートスキャナノードを使用）
- * Red Hat Subscription Management *：ホストはRed Hat Subscription Managementに登録されている必要があります。登録されていない場合、システムはインストール時に必要なサードパーティ製ソフトウェアを更新するためのリポジトリにアクセスできません。
- その他のソフトウェア：BlueXP分類をインストールする前に、次のソフトウェアをホストにインストールする必要があります。
  - 使用しているOSに応じて、次のいずれかのコンテナエンジンをインストールする必要があります。
    - Docker Engineバージョン19.3.1以降。 "インストール手順を確認します"。

      "こちらのビデオをご覧ください" では、CentOSへのDockerのインストールの簡単なデモをご覧ください。

    - Podmanバージョン4以降。Podmanをインストールするには、システムパッケージを更新します。（`sudo yum update -y`）をクリックし、Podmanをインストールします。（`sudo yum install netavark -y`）。
- Pythonバージョン3.6以降。 "インストール手順を確認します"。
  - * NTPに関する考慮事項*：NetAppでは、ネットワークタイムプロトコル（NTP）サービスを使用するようにBlueXP分類システムを設定することを推奨しています。BlueXP分類システムとBlueXP Connectorシステムの間で時刻が同期されている必要があります。
  - ファイアウォールの考慮事項:使用を計画している場合 `firewalld`は、`BlueXP`分類をインストールする前に有効にすることを推奨します。次のコマンドを実行して設定します `firewalld` BlueXPと互換性があることを確認します。

    ```
    firewall-cmd --permanent --add-service=http
    firewall-cmd --permanent --add-service=https
    firewall-cmd --permanent --add-port=80/tcp
    firewall-cmd --permanent --add-port=8080/tcp
    firewall-cmd --permanent --add-port=443/tcp
    firewall-cmd --reload
    ```

    を有効または更新するたびに、DockerまたはPodmanを再起動する必要があることに注意してください。 `firewalld` 設定：

BlueXP分類ホストシステムのIPアドレスは、インストール後に変更することはできません。

BlueXPと**BlueXP**の分類の前提条件を確認

BlueXPに分類を導入する前に、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。

- BlueXP分類インスタンスのリソースを導入し、セキュリティグループを作成するための権限がコネクタに割り当てられていることを確認します。BlueXPの最新の権限は、で確認できます "ネットアップが提供するポリシー"。
- BlueXPの分類を継続して実行できることを確認します。データを継続的にスキャンするには、BlueXP分類インスタンスを引き続き使用する必要があります。
- WebブラウザからBlueXPに接続できることを確認します。BlueXPの分類を有効にしたら、ユーザがBlueXPの分類インスタンスに接続されているホストからBlueXPインターフェイスにアクセスできるようにします。

  BlueXP分類インスタンスでは、プライベートIPアドレスを使用して、インデックス化されたデータに他のユーザがアクセスできないようにします。そのため、BlueXPへのアクセスに使用するWebブラウザには、そのプライベートIPアドレスへの接続が必要です。この接続は、BlueXP分類インスタンスと同じネットワーク内のホストから行うことができます。

必要なすべてのポートが有効になっていることを確認します

コネクタ、BlueXP分類、Active Directory、データソースの間の通信に必要なすべてのポートが開いていることを確認する必要があります。

接続タイプ	ポート	説明
コネクタ<> BlueXPの分類	8080（TCP）、6000（TCP）、443（TCP）、および80	コネクタのセキュリティグループで、ポート6000および443を介したBlueXP分類インスタンスとの間のインバウンドおよびアウトバウンドトラフィックを許可する必要があります。 • BlueXPのBYOLライセンスをダークサイトで使用するには、ポート6000が必要です。 • インストールの進捗状況をBlueXPで確認できるように、ポート8080が開いている必要があります。

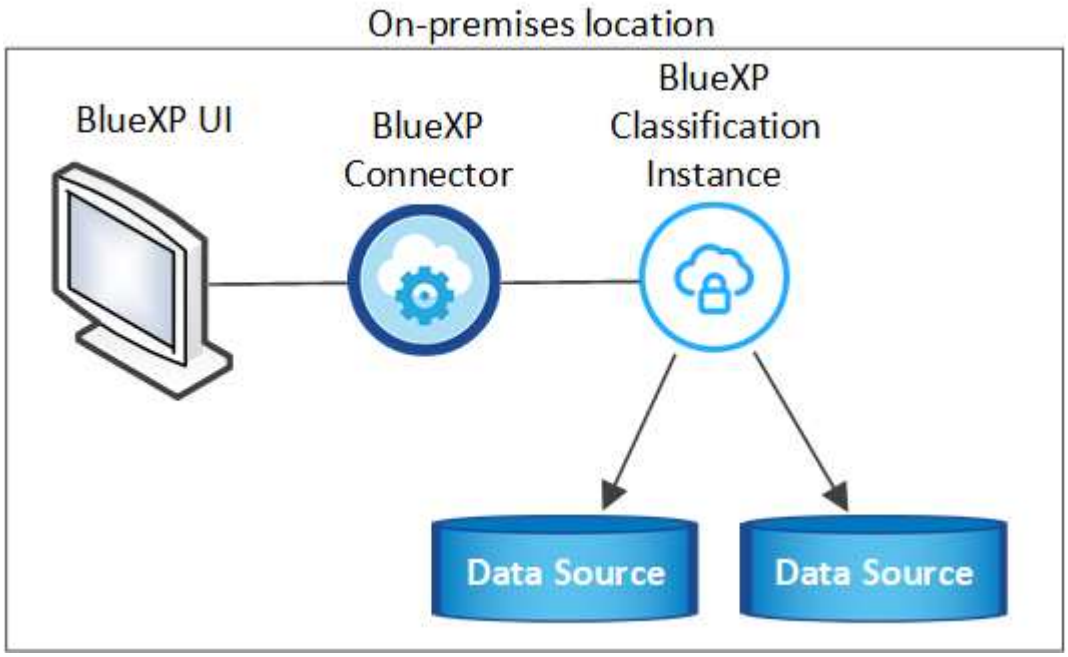
接続タイプ	ポート	説明
Connector <> ONTAP cluster（NAS）	443（TCP）	BlueXPはHTTPSを使用してONTAP クラスタを検出しましたカスタムファイアウォールポリシーを使用する場合は、次の要件を満たす必要があります。 • コネクタホストが、ポート 443 経由のアウトバウンド HTTPS アクセスを許可する必要があります。コネクタがクラウドにある場合、すべてのアウトバウンド通信は事前定義されたセキュリティグループによって許可されます。 • ONTAP クラスタでは、ポート 443 を介した着信 HTTPS アクセスが許可されている必要があります。デフォルトの「 mgmt 」ファイアウォールポリシーでは、すべての IP アドレスからの着信 HTTPS アクセスが許可されます。このデフォルトポリシーを変更した場合、または独自のファイアウォールポリシーを作成した場合は、 HTTPS プロトコルをそのポリシーに関連付けて、Connector ホストからのアクセスを有効にする必要があります。
BlueXP分類<> ONTAP クラスタ	• nfs-111（TCP \ UDP）および2049（TCP \ UDP）の場合 • CIFS-139（TCP\UDP）および445（TCP\UDP）の場合	BlueXPの分類には、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-111と2049の場合は同じです • CIFS/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。

接続タイプ	ポート	説明
BlueXPの分類<> Active Directory	389（TCPおよびUDP）、636（TCP）、3268（TCP）、および3269（TCP）	社内のユーザに対して Active Directory がすでに設定されている必要があります。また、BlueXPの分類では、CIFSボリュームをスキャンするためにActive Directoryのクレデンシャルが必要です。 Active Directory の次の情報が必要です。 • DNS サーバの IP アドレス、または複数の IP アドレス • サーバーのユーザー名とパスワード • ドメイン名（ Active Directory 名） • セキュアな LDAP （ LDAPS ）を使用しているかどうか • LDAP サーバポート（通常は LDAP では 389 、セキュア LDAP では 636 ）

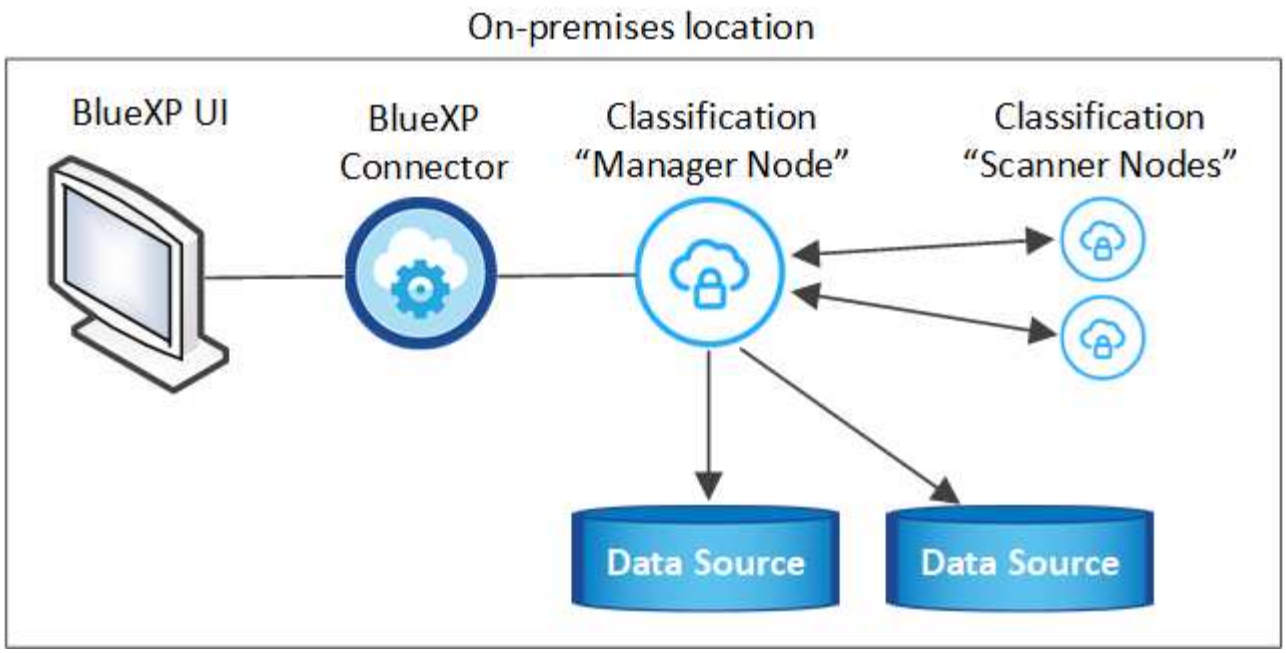
複数のBlueXP分類ホストを使用してデータソースのスキャンに必要な処理能力を提供している場合は、追加のポート/プロトコルを有効にする必要があります。 "追加のポート要件を参照してください"。

オンプレミスの**Linux**ホストに**BlueXP**分類をインストールします

一般的な構成では、ソフトウェアを 1 台のホストシステムにインストールします。 "これらの手順を参照してください"。



ペタバイト規模のデータをスキャンする大規模な構成では、複数のホストを含めて処理能力を追加できます。 "これらの手順を参照してください"。



一般的な構成でのシングルホストインストール

オフライン環境の単一のオンプレミスホストにBlueXP分類ソフトウェアをインストールする場合は、次の手順に従います。

BlueXP分類をインストールすると、すべてのインストールアクティビティがログに記録されます。インストール中に問題が発生した場合は、インストール監査ログの内容を表示できます。に書き込まれます。`/opt/netapp/install_logs/`。 "詳細はこちら"。

必要なもの

- Linux システムがを満たしていることを確認します ホストの要件。
- 前提条件となる2つのソフトウェアパッケージ（Docker EngineまたはPodman、およびPython 3）がインストールされていることを確認します。
- Linux システムに対する root 権限があることを確認してください。
- オフライン環境が要件を満たしていることを確認します 権限と接続。

手順

1. インターネットが設定されたシステムの場合は、からBlueXP分類ソフトウェアをダウンロードします "ネットアップサポートサイト"。選択するファイルの名前は * DataSense - offline-bundle-<version>.tar.gz * です。
2. プライベートモードで使用するLinuxホストにインストーラバンドルをコピーします。
3. ホストマシンでインストーラバンドルを解凍します。次に例を示します。

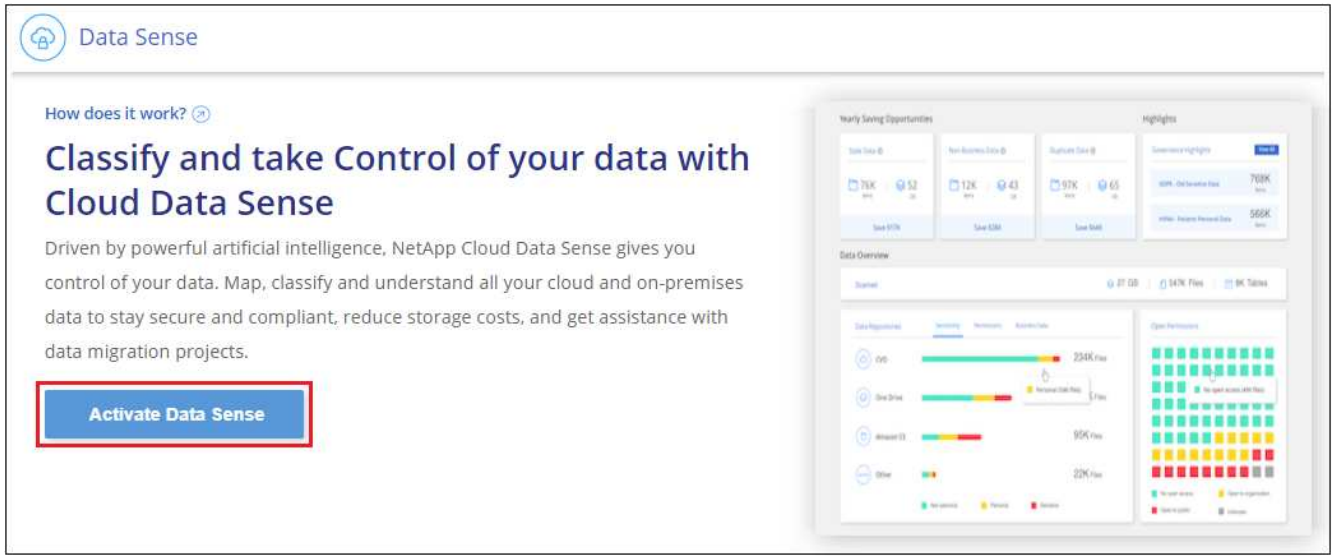
```
tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
```

これにより、必要なソフトウェアと実際のインストールファイル* cc_onpm_installer.tar.gz *が抽出されます。

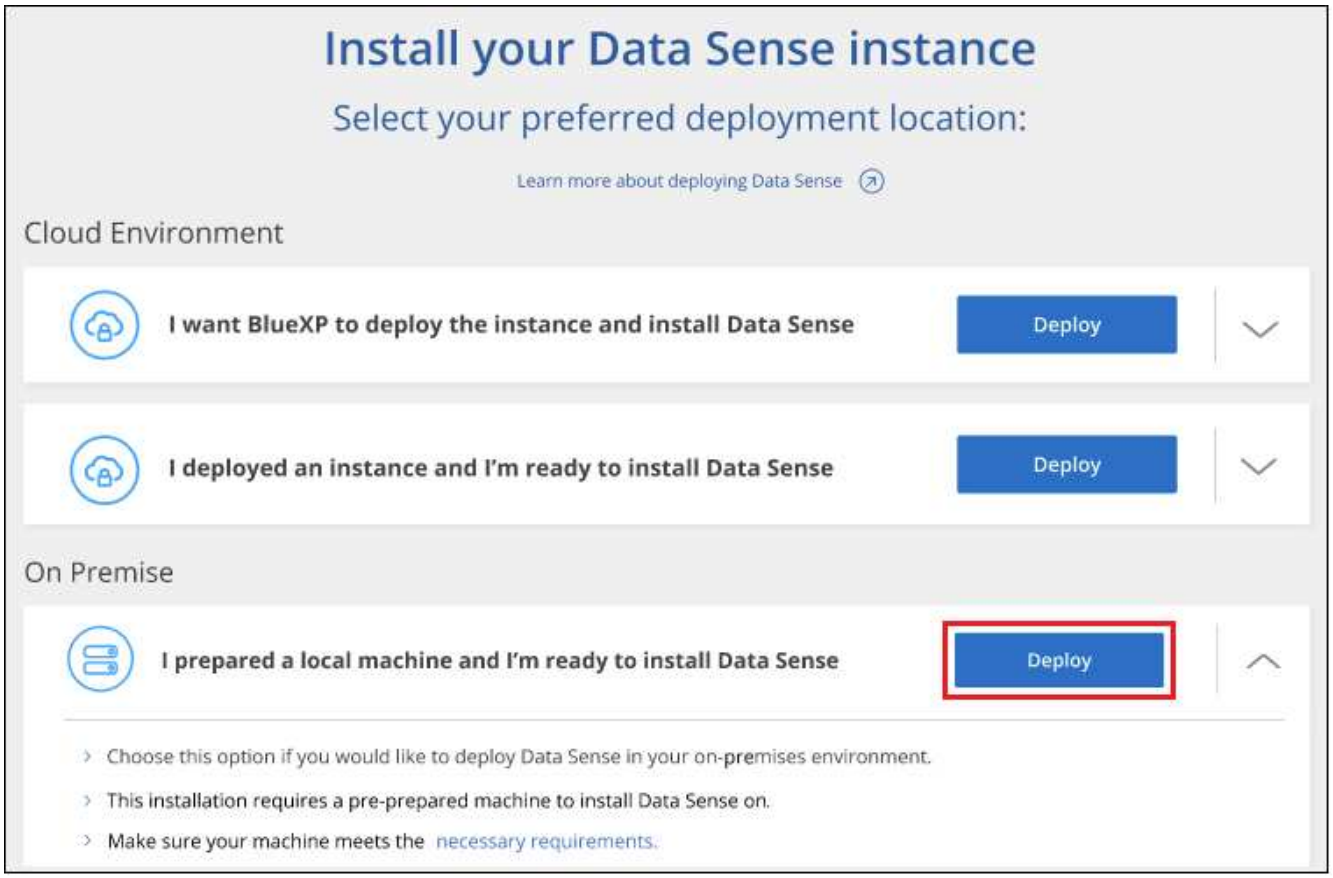
4. ホストマシンでインストールファイルを解凍します。次に例を示します。

```
tar -xzf cc_onprem_installer.tar.gz
```

5. BlueXPを起動し、「ガバナンス」＞「分類」と選択します。
6. [データセンスを活動化（ Activate Data sense ）] をクリックし



7. [Deploy]*をクリックしてオンプレミスのインストールを開始します。



8. 「_Deploy Data Sense on Premises」ダイアログが表示されます。提供されたコマンドをコピーします（例： `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq --darksite`）をクリックし、後で使用できるようにテキストファイルに貼り付けます。次に*[閉じる]*をクリックしてダイアログを閉じます。
9. ホストマシンで、コピーしたコマンドを入力して一連のプロンプトに従います。または、必要なすべてのパラメータをコマンドライン引数として指定することもできます。

   インストールを正常に完了するには、インストーラによって事前チェックが実行され、システムとネットワークの要件が満たされていることが確認されます。

プロンプトに従ってパラメータを入力します。	完全なコマンドを入力します。
a. 手順8でコピーした情報を貼り付けます。 `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --darksite` b. コネクタシステムからアクセスできるように、BlueXP分類ホストマシンのIPアドレスまたはホスト名を入力します。 c. BlueXPコネクタホストマシンのIPアドレスまたはホスト名を入力して、BlueXP分類システムからアクセスできるようにします。	または、必要なホストパラメータを指定して、コマンド全体を事前に作成することもできます。 `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --no-proxy --darksite`

   変数値：

   - _account_id _ = ネットアップアカウント ID
   - *client_id*=コネクタクライアントID（クライアントIDがない場合は、接尾辞「clients」を追加）
   - *user_token*= JWTユーザーアクセストークン
   - *DS_HOST*= BlueXP分類システムのIPアドレスまたはホスト名。
   - *cm_host*= BlueXPコネクタシステムのIPアドレスまたはホスト名。

結果

BlueXP分類インストーラは、パッケージをインストールして登録し、BlueXP分類をインストールします。インストールには 10~20 分かかります。

ホストマシンとコネクタインスタンスの間にポート8080経由で接続が確立されている場合は、BlueXPのBlueXPの分類タブでインストールの進捗状況を確認できます。

次のステップ

設定ページからローカルを選択できます "オンプレミスの ONTAP クラスタ" および "データベース" をスキャンします。

また可能です "BlueXP分類用のBYOLライセンスをセットアップ" （この時点ではBlueXPのデジタルウォレットページから）。30日間の無料トライアルが終了するまで、料金はかかりません。

大規模構成向けのマルチホストインストール

ペタバイト規模のデータをスキャンする大規模な構成では、複数のホストを含めて処理能力を追加できます。

複数のホストシステムを使用する場合、プライマリシステムは _Managernode_name と呼ばれ、追加の処理能力を提供する追加システムは _Scanner Node_と 呼ばれます。

オフライン環境の複数のオンプレミスホストにBlueXP分類ソフトウェアをインストールする場合は、次の手順に従います。

必要なもの

- Manager ノードと Scanner ノードのすべての Linux システムが、を満たしていることを確認します ホストの要件。
- 前提条件となる2つのソフトウェアパッケージ（Docker EngineまたはPodman、およびPython 3）がインストールされていることを確認します。
- Linux システムに対する root 権限があることを確認してください。
- オフライン環境が要件を満たしていることを確認します 権限と接続。
- 使用するスキャナノードホストの IP アドレスを確認しておく必要があります。
- すべてのホストで次のポートとプロトコルを有効にする必要があります。

ポート	プロトコル	説明
2377	TCP	クラスタ管理通信
7946	tcp 、 udp です	ノード間通信
4789	UDP	オーバーレイネットワークトラフィック
50	ESP	暗号化された IPsec オーバーレイネットワーク（ ESP ）トラフィック
111	tcp 、 udp です	ホスト間でファイルを共有するための NFS サーバ（各スキャナノードからマネージャノードに必要）
2049	tcp 、 udp です	ホスト間でファイルを共有するための NFS サーバ（各スキャナノードからマネージャノードに必要）

手順

1. から手順 1~8 を実行します "シングルホストインストール" マネージャーノード。
2. 手順 9 に示すように、インストーラからプロンプトが表示されたら、一連のプロンプトで必要な値を入力するか、必要なパラメータをコマンドライン引数としてインストーラに指定することができます。

   シングルホストのインストールで使用できる変数に加えて、新しいオプション * -n <Node_IP> * を使用してスキャナノードの IP アドレスを指定します。複数のノードの IP をカンマで区切って指定します。

   たとえば、次のコマンドは3つのスキャナノードを追加します。
   ```
   sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host
   <ds_host> --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --no
   -proxy --darksite
   ```
3. マネージャノードのインストールが完了する前に、スキャナノードに必要なインストールコマンドがダイアログに表示されます。コマンドをコピーします（例： `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`）を入力し、テキストファイルに保存します。
4. 各 * スキャナノードホストで：

a. データセンスインストーラファイル（* cc_onpm_installer.tar.gz *）をホストマシンにコピーします。

b. インストーラファイルを解凍します。

c. 手順 3 でコピーしたコマンドを貼り付けて実行します。

すべてのスキャナノードでインストールが完了し、それらのノードがマネージャノードに参加したら、マネージャノードのインストールも完了します。

結果

BlueXP分類インストーラがパッケージのインストールを完了し、インストールを登録します。インストールには 15 〜 25 分かかる場合があります。

次のステップ

設定ページからローカルを選択できます "オンプレミスの ONTAP クラスタ" および local です "データベース" をスキャンします。

また可能です "BlueXP分類用のBYOLライセンスをセットアップ" （この時点ではBlueXPのデジタルウォレットページから）。30日間の無料トライアルが終了するまで、料金はかかりません。

BlueXP分類ソフトウェアをアップグレードします

BlueXPの分類ソフトウェアは定期的に新機能で更新されるため、定期的に新しいバージョンをチェックして、最新のソフトウェアや機能を使用しているかどうかを確認する必要があります。自動的にアップグレードを実行するためのインターネット接続がないため、BlueXP分類ソフトウェアは手動でアップグレードする必要があります。

作業を開始する前に

- BlueXP Connectorソフトウェアを最新バージョンにアップグレードすることを推奨します。 "コネクタのアップグレード手順を参照してください"。
- BlueXP分類バージョン1.24以降では、ソフトウェアの将来のバージョンへのアップグレードを実行できます。

  BlueXP分類ソフトウェアで1.24より前のバージョンが実行されている場合、一度にアップグレードできるメジャーバージョンは1つだけです。たとえば、バージョン1.21.xがインストールされている場合は、1.22.xにのみアップグレードできます。いくつかのメジャーバージョンがサポートされている場合は、ソフトウェアを何度もアップグレードする必要があります。

手順

1. インターネットが設定されたシステムの場合は、からBlueXP分類ソフトウェアをダウンロードします "ネットアップサポートサイト"。選択するファイルの名前は * DataSense - offline-bundle-<version>.tar.gz * です。
2. BlueXP分類がインストールされているダークサイトのLinuxホストにソフトウェアバンドルをコピーします。
3. ホストマシンでソフトウェアバンドルを解凍します。次に例を示します。

```
tar -xvf DataSense-offline-bundle-v1.25.0.tar.gz
```

これにより、インストールファイル* cc_onpm_installer.tar.gz *が抽出されます。

4. ホストマシンでインストールファイルを解凍します。次に例を示します。

```
tar -xzf cc_onprem_installer.tar.gz
```

これにより、アップグレードスクリプト * START_ダーク site_upgrade.sh * および必要なサードパーティ製ソフトウェアが抽出されます。

5. ホストマシンでアップグレードスクリプトを実行します。次に例を示します。

```
start_darksite_upgrade.sh
```

結果

ホストでBlueXP分類ソフトウェアがアップグレードされます。更新には 5 〜 10 分かかる場合があります。

大規模な構成をスキャンするために複数のホストシステムにBlueXP分類を導入している場合は、スキャナノードでアップグレードする必要はありません。

BlueXP分類UIページの下部でバージョンを確認すると、ソフトウェアが更新されたことを確認できます。

Linuxホストで**BlueXP**分類をインストールできる状態になっていることを確認します

LinuxホストにBlueXPの分類を手動でインストールする前に、ホストでスクリプトを実行して、BlueXPの分類をインストールするための前提条件がすべて揃っていることを確認することができます。このスクリプトは、ネットワーク内のLinuxホストまたはクラウド内のLinuxホストで実行できます。ホストはインターネットに接続することも、インターネットにアクセスできないサイト（a_dark site_）に配置することもできます。

BlueXP分類インストールスクリプトには、前提条件となるテストスクリプトも含まれています。ここで説明するスクリプトは、BlueXP分類のインストールスクリプトとは別にLinuxホストを検証するユーザ向けに設計されています。

はじめに

次のタスクを実行します。

1. BlueXPコネクタがまだインストールされていない場合は、必要に応じてインストールします。テストスクリプトはコネクタをインストールせずに実行できますが、コネクタとBlueXP分類ホストマシンの間の接続がチェックされるため、コネクタを用意することを推奨します。
2. ホストマシンを準備し、すべての要件を満たしていることを確認します。
3. BlueXP分類ホストマシンからのアウトバウンドインターネットアクセスを有効にします。
4. すべてのシステムで必要なすべてのポートが有効になっていることを確認します。
5. 前提条件テストスクリプトをダウンロードして実行します。

コネクタを作成します

BlueXPをインストールして使用するには、BlueXPコネクタが必要です。ただし、コネクタを使用せずに前提条件スクリプトを実行することはできます。

可能です "コネクタをオンプレミスにインストールします" ネットワーク内のLinuxホストまたはクラウド内のLinuxホスト。BlueXP分類をオンプレミスにインストールすることを計画している一部のユーザは、コネクタをオンプレミスにインストールすることもできます。

クラウドプロバイダ環境でコネクタを作成するには、を参照してください "AWS でコネクタを作成する"、"Azure でコネクタを作成する"または "GCP でコネクタを作成する"。

前提条件スクリプトを実行するときに、コネクタシステムのIPアドレスまたはホスト名が必要になります。この情報は、コネクタをオンプレミスにインストールした場合に表示されます。コネクタがクラウドに導入されている場合は、BlueXPコンソールで[ヘルプ]アイコンをクリックし、[サポート**]**を選択して、**[** BlueXPコネクタ*]をクリックします。

ホストの要件を確認

BlueXP分類ソフトウェアは、特定のオペレーティングシステム要件、RAM要件、ソフトウェア要件などを満たすホストで実行する必要があります。

- BlueXPの分類は、他のアプリケーションと共有するホストではサポートされません。専用のホストである必要があります。
- オンプレミスでホストシステムを構築する場合は、BlueXP分類スキャンを実行するデータセットのサイズに応じて、3つのシステムサイズの中から選択できます。

システムサイズ	**CPU**	**RAM**（スワップメモリを無効にする必要があります）	ディスク
特大	CPU×32	128GBのRAM	1TiB SSDオン/または -100GiBは/optで利用可能 -895GiBを/var/lib/dockerで使用可能 -5GiB（/tmp
大きい	16 CPU	64GBのRAM	500GiB SSDオン/、または -100GiBは/optで利用可能 -395GiBは/var/lib/dockerで使用可能 -5GiB（/tmp
中	8 CPU	32GBのRAM	200GiB SSDオン/、または -50GiBは/optで利用可能 -145GiBは/var/lib/dockerで使用可能 -5GiB（/tmp
小さい	8 CPU	16GB の RAM	100GiB SSDオン/、または -50GiBは/optで利用可能 -45GiBは/var/lib/dockerで使用可能 -5GiB（/tmp

小規模なシステムを使用する場合は制限があることに注意してください。を参照してください "小さいインスタンスタイプを使用しています" を参照してください。

- BlueXP分類インストール用にコンピューティングインスタンスをクラウドに導入する場合は、上記の「大規模」システム要件を満たすシステムを推奨します。
  - * AWS EC2インスタンスタイプ*：「m6i.4xlarge」を推奨します。 "その他のAWSインスタンスタイプを参照してください"。
  - * Azure VMのサイズ*：「Standard_D16s_v3」を推奨します。 "その他のAzureインスタンスタイプを参照してください"。
  - **GCP**マシンタイプ:「n2-standard-16」をお勧めします。 "追加のGCPインスタンスタイプを参照してください"。
- * UNIXフォルダ権限*：次の最小UNIX権限が必要です。

フォルダ	最小権限
/tmp	`rwxrwxrwt`
/opt	`rwxr-xr-x`
/var/lib/dockerを使用します	`rwx------`
/usr/lib/systemd/system	`rwxr-xr-x`

- * オペレーティング・システム * ：
  - 次のオペレーティングシステムでは、Dockerコンテナエンジンを使用する必要があります。
    - Red Hat Enterprise Linuxバージョン7.8および7.9
    - CentOSバージョン7.8および7.9
    - Ubuntu 22.04（BlueXP分類バージョン1.23以降が必要）
  - 次のオペレーティングシステムでは、Podmanコンテナエンジンを使用する必要があります。また、BlueXP分類バージョン1.30以降が必要です。
    - Red Hat Enterprise Linuxバージョン8.8、9.0、9.1、9.2、9.3

      RHEL 8.xおよびRHEL 9.xを使用している場合、次の機能は現在サポートされていません。

      - タアクサイトテノセツチ
      - 分散スキャン（マスタースキャナノードとリモートスキャナノードを使用）
- * Red Hat Subscription Management *：ホストはRed Hat Subscription Managementに登録されている必要があります。登録されていない場合、システムはインストール時に必要なサードパーティ製ソフトウェアを更新するためのリポジトリにアクセスできません。
- その他のソフトウェア：BlueXP分類をインストールする前に、次のソフトウェアをホストにインストールする必要があります。
  - 使用しているOSに応じて、次のいずれかのコンテナエンジンをインストールする必要があります。
    - Docker Engineバージョン19.3.1以降。 "インストール手順を確認します"。

      "こちらのビデオをご覧ください" では、CentOSへのDockerのインストールの簡単なデモをご覧ください。

    - Podmanバージョン4以降。Podmanをインストールするには、システムパッケージを更新します。（`sudo yum update -y`）をクリックし、Podmanをインストールします。（`sudo yum`

install netavark -y）。

- Pythonバージョン3.6以降。 "インストール手順を確認します"。
  - * NTPに関する考慮事項*：NetAppでは、ネットワークタイムプロトコル（NTP）サービスを使用するようにBlueXP分類システムを設定することを推奨しています。BlueXP分類システムとBlueXP Connectorシステムの間で時刻が同期されている必要があります。
  - ファイアウォールの考慮事項:使用を計画している場合 `firewalld`は、`BlueXP`分類をインストールする前に有効にすることを推奨します。次のコマンドを実行して設定します `firewalld` BlueXPと互換性があることを確認します。

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

BlueXP分類ホストを（分散モデルで）スキャナノードとして使用する場合は、この時点でプライマリシステムに次のルールを追加します。

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

+
を有効または更新するたびに、DockerまたはPodmanを再起動する必要があることに注意してください。
`firewalld` 設定：

BlueXPの分類からアウトバウンドのインターネットアクセスを有効にします

BlueXPの分類にはアウトバウンドのインターネットアクセスが必要です。仮想ネットワークまたは物理ネットワークでインターネットアクセスにプロキシサーバを使用している場合は、次のエンドポイントに接続するためのアウトバウンドのインターネットアクセスがBlueXP分類インスタンスにあることを確認してください。

このセクションは、インターネットに接続されていないサイトにインストールされているホストシステムには必要ありません。

エンドポイント	目的
\ https://api.bluexp.netapp.com	ネットアップアカウントを含むBlueXPサービスとの通信
¥ https://netapp-cloud-account.auth0.com ¥ https://auth0.com	BlueXP Webサイトとの通信により、ユーザ認証を一元化。

エンドポイント	目的
https://support.compliance.api.bluexp.netapp.com/\ https://hub.docker.com \ https://auth.docker.io \ https://registry-1.docker.io \ https://index.docker.io/\ https://dseasb33srnrn.cloudfront.net/\ https://production.cloudflare.docker.com/	ソフトウェアイメージ、マニフェスト、テンプレートへのアクセス、およびログとメトリックの送信を提供します。
\ https://support.compliance.api.bluexp.netapp.com/	ネットアップが監査レコードからデータをストリーミングできるようにします。
https://github.com/docker https://download.docker.com	Dockerのインストールに必要なパッケージを提供します。
http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	CentOSのインストールに必要なパッケージを提供します。
http://packages.ubuntu.com/ http://archive.ubuntu.com	Ubuntuのインストールに必要なパッケージを提供します。

必要なすべてのポートが有効になっていることを確認します

コネクタ、BlueXP分類、Active Directory、データソースの間の通信に必要なすべてのポートが開いていることを確認する必要があります。

接続タイプ	ポート	説明
コネクタ<> BlueXPの分類	8080（TCP）、443（TCP）、および80	コネクタのファイアウォールルールまたはルーティングルールで、ポート443を介したBlueXP分類インスタンスとの間のインバウンドおよびアウトバウンドトラフィックを許可する必要があります。ポート8080が開いていることを確認し、BlueXPでインストールの進行状況を確認します。
Connector <> ONTAP cluster（NAS）	443（TCP）	BlueXPはHTTPSを使用してONTAP クラスタを検出しましたカスタムファイアウォールポリシーを使用する場合は、コネクタホストでポート443経由のアウトバウンドHTTPSアクセスを許可する必要があります。コネクタがクラウド内にある場合、すべてのアウトバウンド通信は、事前定義されたファイアウォールまたはルーティングルールによって許可されます。

BlueXPの分類の前提条件スクリプトを実行します

BlueXPの分類の前提条件スクリプトを実行するには、次の手順を実行します。

"こちらのビデオをご覧ください" 前提条件スクリプトの実行方法と結果の解釈方法を確認します。

必要なもの

- Linux システムがを満たしていることを確認します ホストの要件。
- システムに前提条件となる2つのソフトウェアパッケージ（Docker EngineまたはPodman、およびPython 3）がインストールされていることを確認します。
- Linux システムに対する root 権限があることを確認してください。

手順

1. からBlueXPの分類のPrerequisitesスクリプトをダウンロードします "ネットアップサポートサイト"。選択するファイルの名前は* standalone-pre-requisite-tester-tester*<version> です。
2. 使用するLinuxホストにファイルをコピーします（を使用） `scp` またはその他の方法を使用してください）。
3. スクリプトを実行する権限を割り当てます。

```
chmod +x standalone-pre-requisite-tester-v1.25.0
```

4. 次のコマンドを使用してスクリプトを実行します。

```
./standalone-pre-requisite-tester-v1.25.0 <--darksite>
```

   インターネットにアクセスできないホストでスクリプトを実行する場合にのみ、「--darksite」オプションを追加します。ホストがインターネットに接続されていない場合、一部の前提条件テストがスキップされます。

5. BlueXP分類ホストマシンのIPアドレスの入力を求められます。
   - IPアドレスまたはホスト名を入力します。
6. BlueXP Connectorがインストールされているかどうかを確認するメッセージが表示されます。
   - コネクタが取り付けられていない場合は、「* N *」と入力します。
   - コネクタが取り付けられている場合は、「* Y *」と入力します。をクリックし、テストスクリプトで接続をテストできるように、BlueXPコネクタのIPアドレスまたはホスト名を入力します。
7. このスクリプトでは、システムに対してさまざまなテストが実行され、処理が進むにつれて結果が表示されます。終了すると、セッションのログがという名前のファイルに書き込まれます `prerequisites-test-<timestamp>.log` をクリックします `/opt/netapp/install_logs`。

結果

すべての前提条件テストが正常に実行されたら、準備ができたらBlueXP分類をホストにインストールできます。

問題が検出された場合は、「推奨」または「必須」に分類され、修正が必要です。通常、推奨される問題は、BlueXPの分類のスキャンとカテゴリ化のタスクの実行に時間がかかる原因となる項目です。これらの項目は修正する必要はありませんが、対処する必要があります。

「必須」の問題がある場合は、問題を修正してから、前提条件テストスクリプトを再度実行する必要があります。

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"。

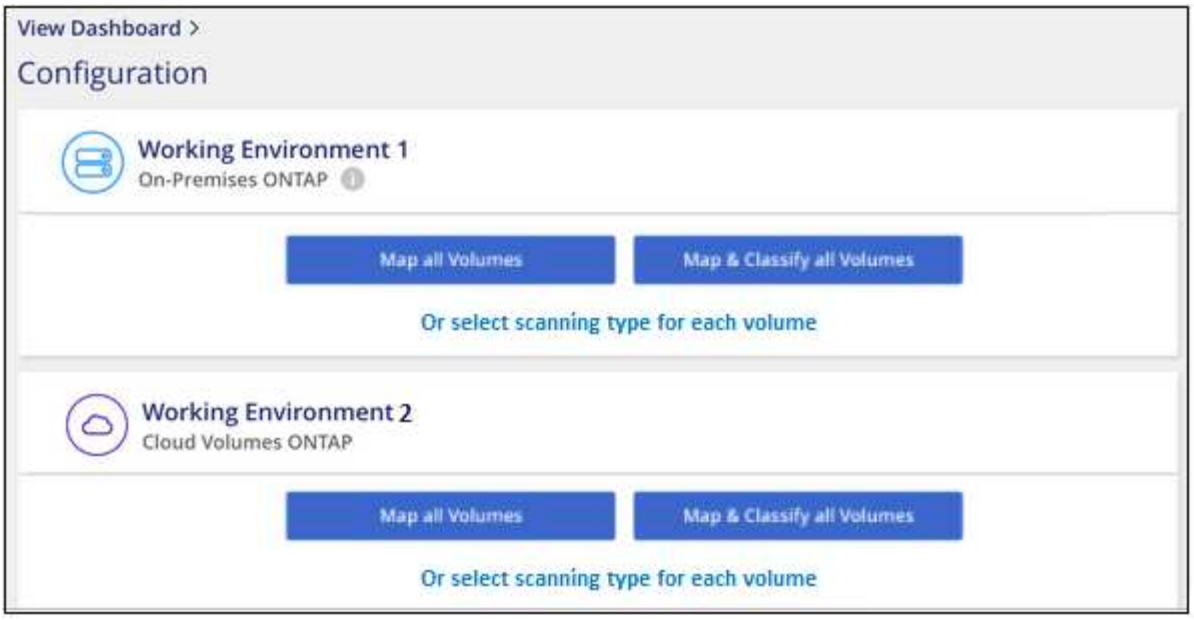
インターネットにアクセスできないダークサイトにインストールされているオンプレミスの ONTAP システムをスキャンする場合は、を実行する必要があります "インターネットアクセスのないオンプレミスと同じ場所にBlueXPの分類を導入します"。また、BlueXPコネクタがオンプレミスの同じ場所に配置されている必要があります。

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。

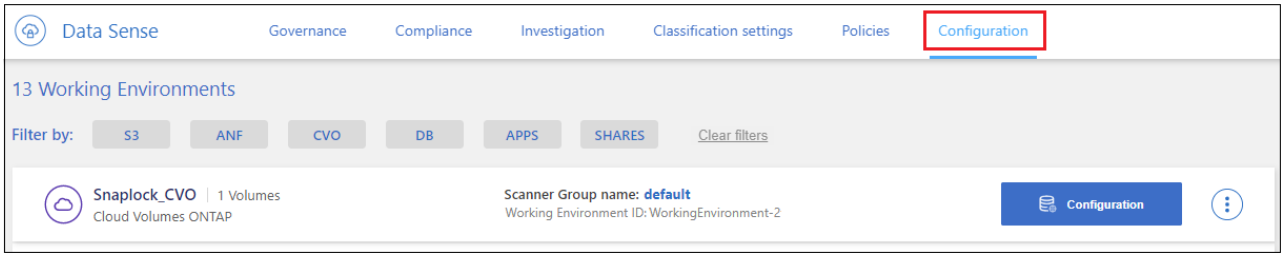
手順

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。

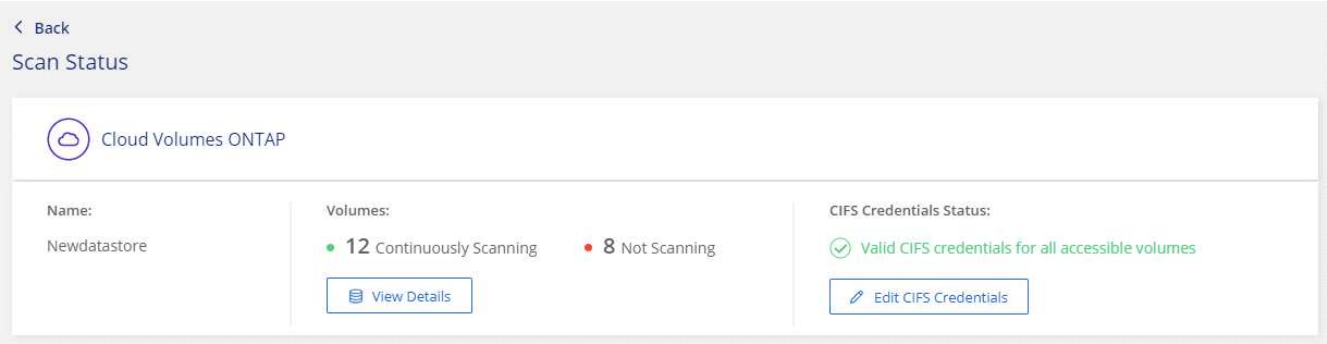
   ボタンを示す [遵守] タブのスクリーンショット。"]

   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。

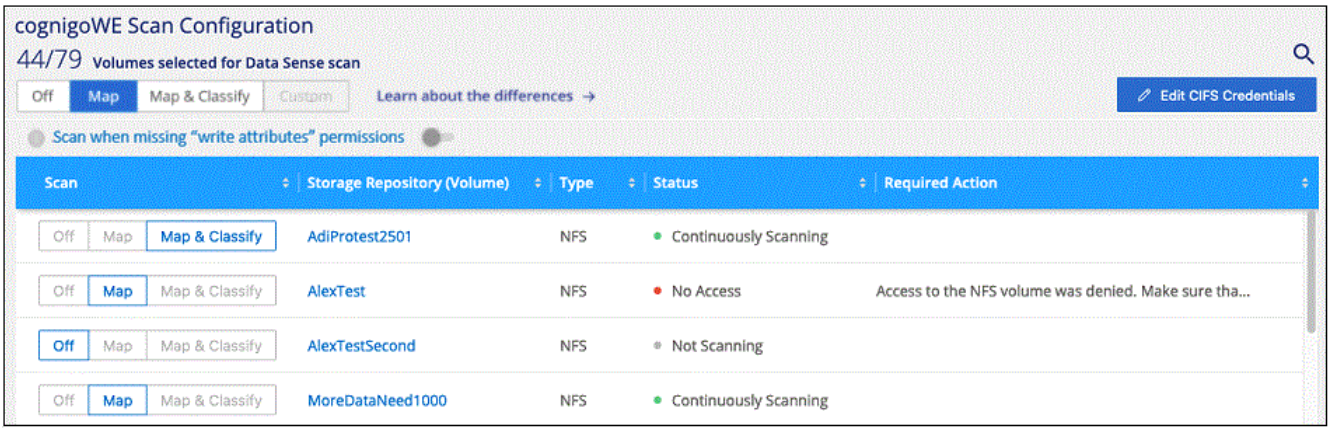
   BlueXPの分類スキャンでファイルの「最終アクセス日時」が変更されないようにするには、CIFSではWrite Attributes権限、NFSではwrite権限を持つことを推奨します。可能であれば、すべてのファイルに対する権限を持つ組織内の親グループにActive Directory構成ユーザーを含めることをお勧めします。

   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。

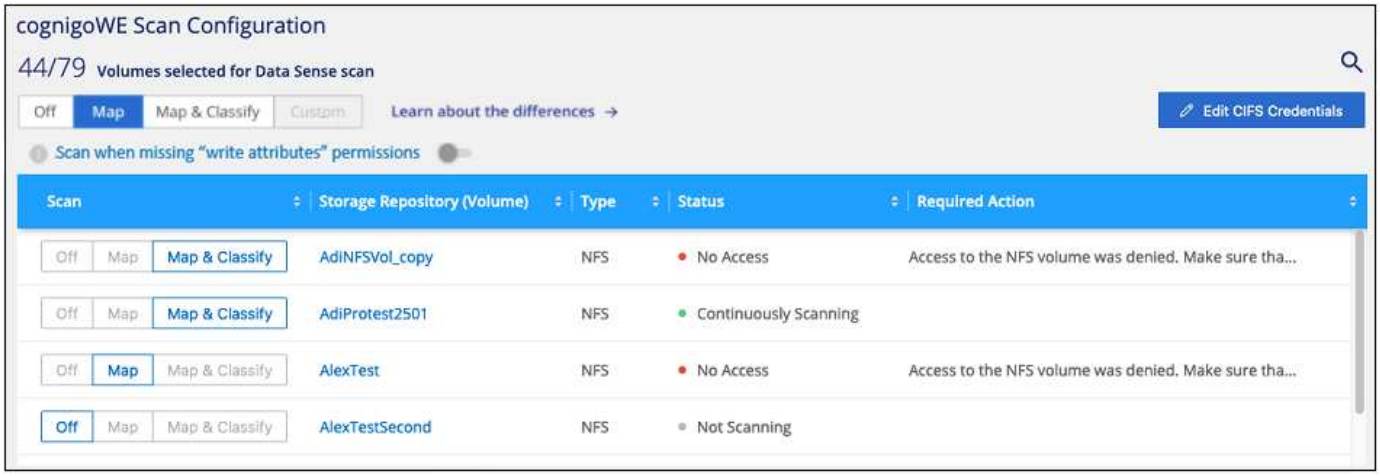


   ページのスクリーンショット。4つのボリュームが表示されています。そのうちの1つはBlueXPで分類されたボリュームとボリュームの間のネットワーク接続が原因でスキャンされていません。"]

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。"。



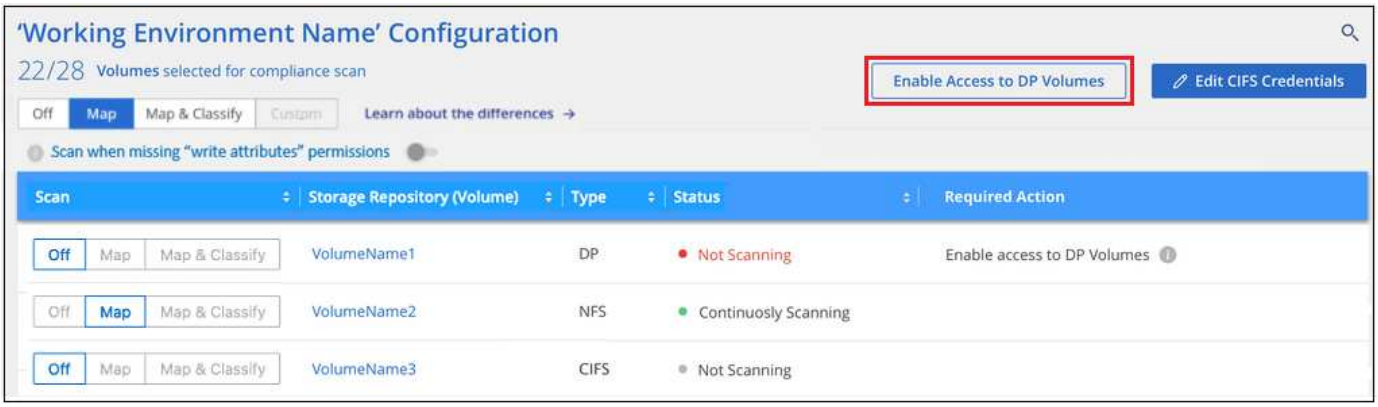
終了：	手順：
ボリュームに対してマッピングのみのスキャンを有効にします	ボリューム領域で、 * マップ * をクリックします
ボリュームでフルスキャンを有効にします	ボリューム領域で、 * マップと分類 * をクリックします
ボリュームのスキャンを無効にします	ボリューム領域で、 * オフ * をクリックします
すべてのボリュームでマッピングのみのスキャンを有効にします	見出し領域で、 * マップ * をクリックします
すべてのボリュームでフルスキャンを有効にします	見出し領域で、 * マップと分類 * をクリックします
すべてのボリュームでスキャンを無効にします	見出し領域で、 * Off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

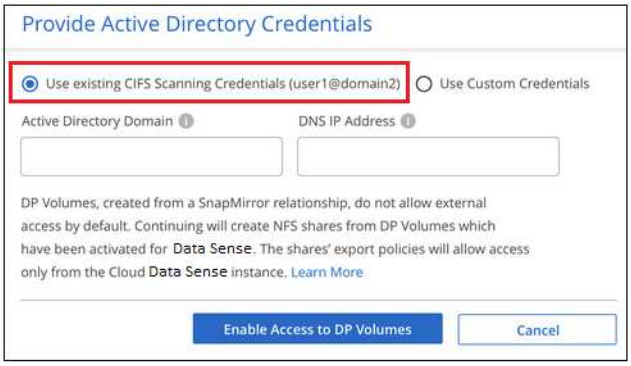
最初は、ボリュームリストでこれらのボリュームを *Type* * DP * でスキャンしていないステータス * および必要なアクション _ * DP ボリュームへのアクセスを有効にします * 。

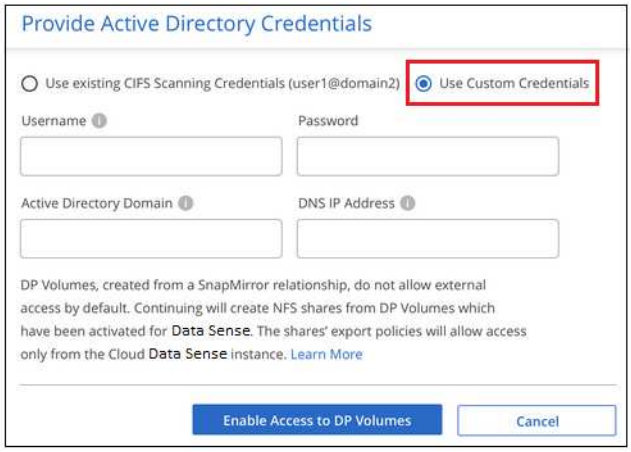


手順

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。

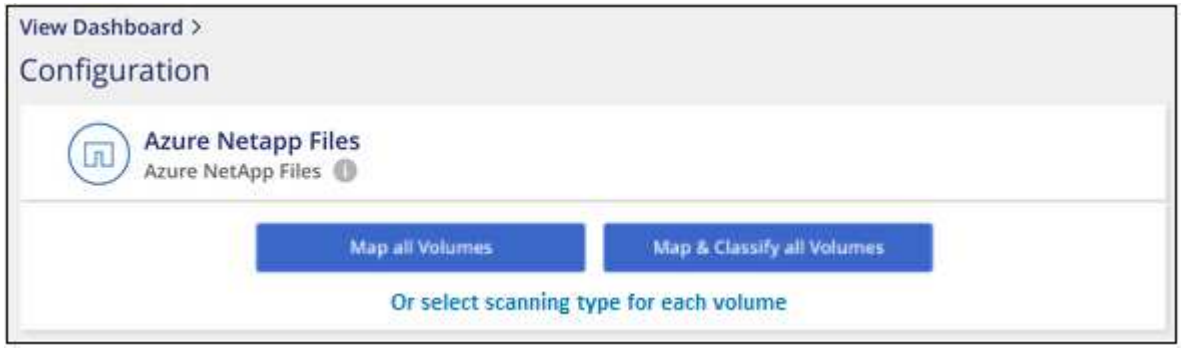
*注：*現時点では、Azure NetApp Files ボリュームのスキャン時にBlueXPの分類をオンプレミスに導入することはできません。

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。

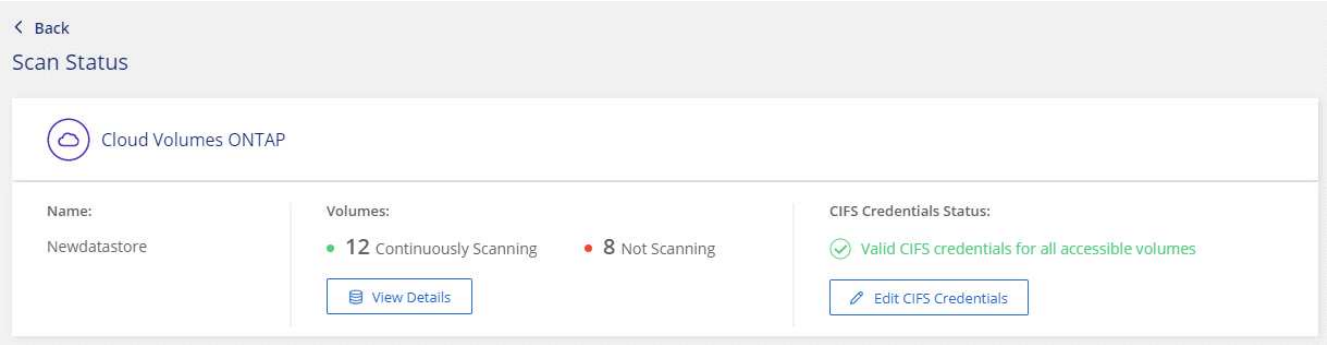
ボタンを示す [遵守] タブのスクリーンショット。"]

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。

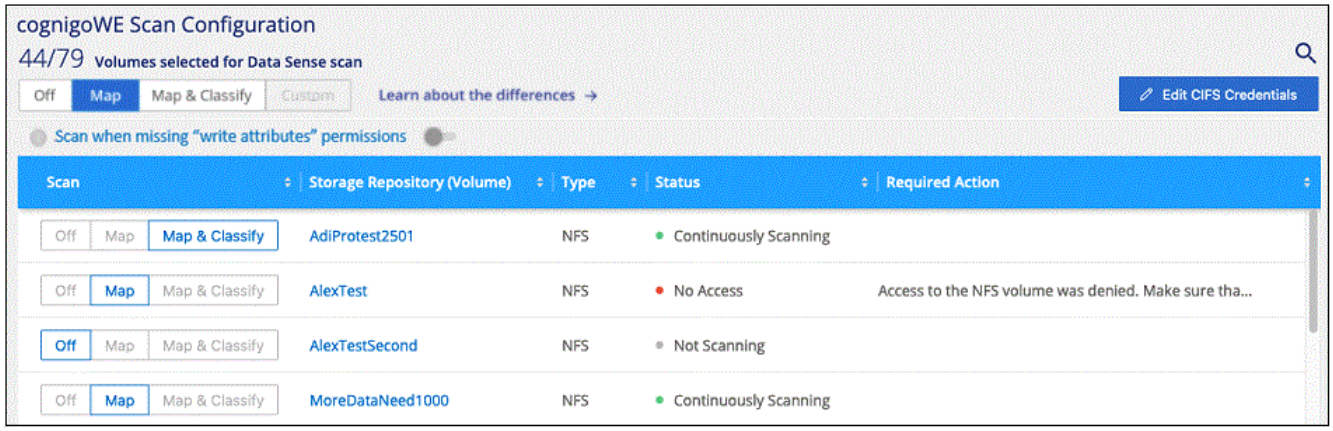
BlueXPの分類スキャンでファイルの「最終アクセス日時」が変更されないようにするには、CIFSではWrite Attributes権限、NFSではwrite権限を持つことを推奨します。可能であれば、すべてのファイルに対する権限を持つ組織内の親グループにActive Directory構成ユーザーを含めることをお勧めします。

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。

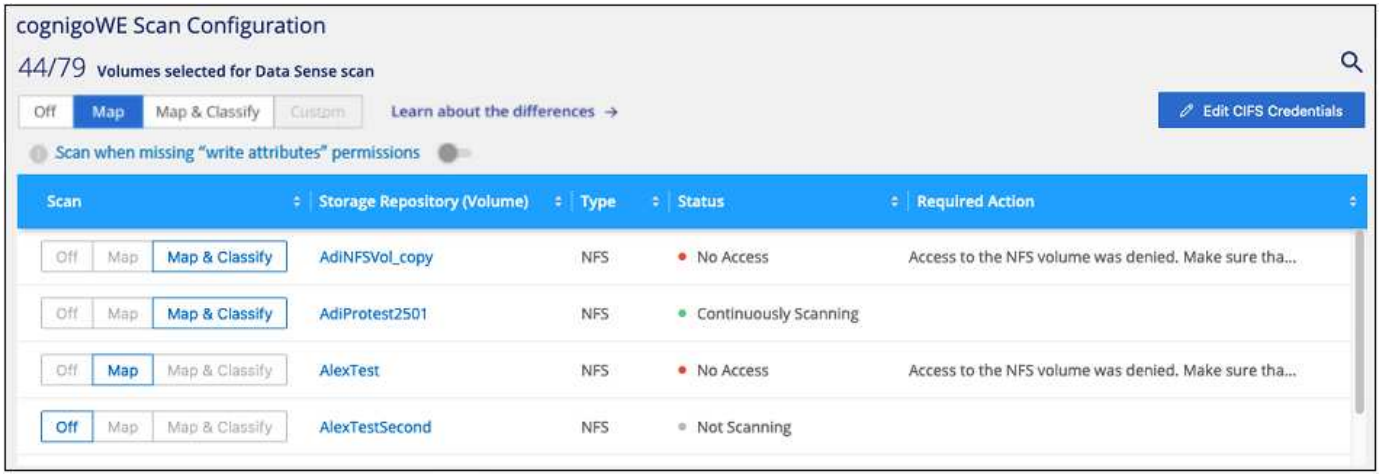


ページのスクリーンショット。4つのボリュームが表示されています。そのうちの1つはBlueXPで分類されたボリュームとボリュームの間のネットワーク接続が原因でスキャンされていません。"]

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。

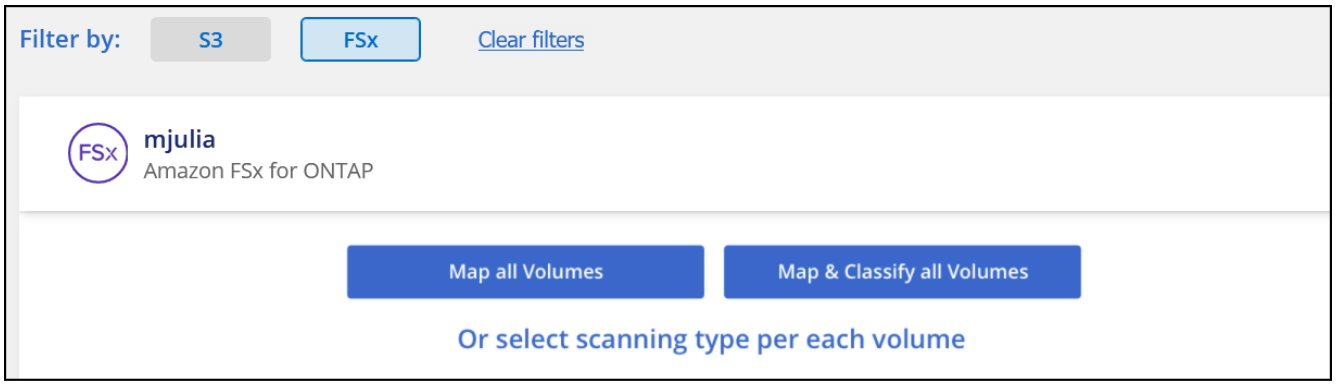
注： FSxボリュームのスキャン時にオンプレミス環境へのBlueXP分類の導入は現在サポートされていません。

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。

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	jrmclone	NFS	No Access	Check network connectivity between the Data Sense ...

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。

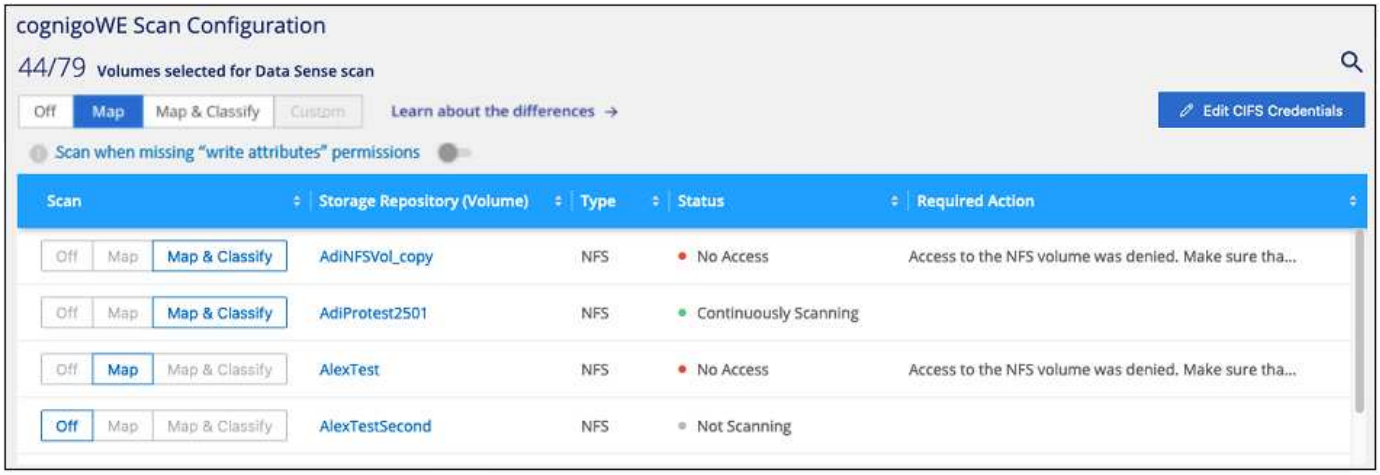
   クレデンシャルを入力すると、すべての CIFS ボリュームが認証されたことを示すメッセージが表示されます。

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。"。



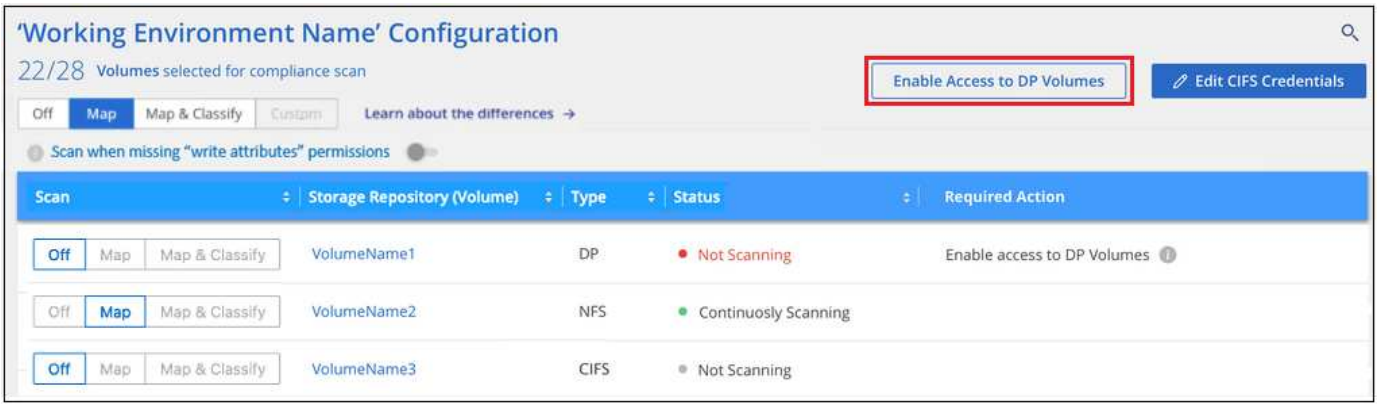
終了：	手順：
ボリュームに対してマッピングのみのスキャンを有効にします	ボリューム領域で、 * マップ * をクリックします
ボリュームでフルスキャンを有効にします	ボリューム領域で、 * マップと分類 * をクリックします
ボリュームのスキャンを無効にします	ボリューム領域で、 * オフ * をクリックします
すべてのボリュームでマッピングのみのスキャンを有効にします	見出し領域で、 * マップ * をクリックします
すべてのボリュームでフルスキャンを有効にします	見出し領域で、 * マップと分類 * をクリックします
すべてのボリュームでスキャンを無効にします	見出し領域で、 * Off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

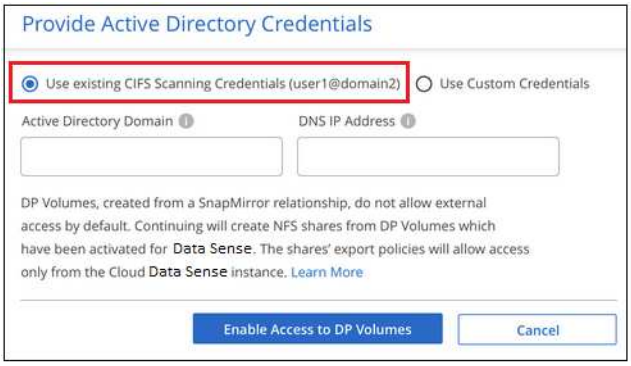
最初は、ボリュームリストでこれらのボリュームを *Type* * DP * でスキャンしていないステータス * および必要なアクション _ * DP ボリュームへのアクセスを有効にします * 。

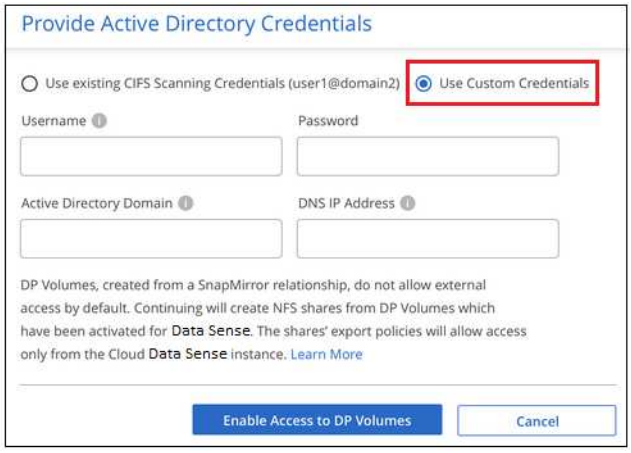


手順

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。

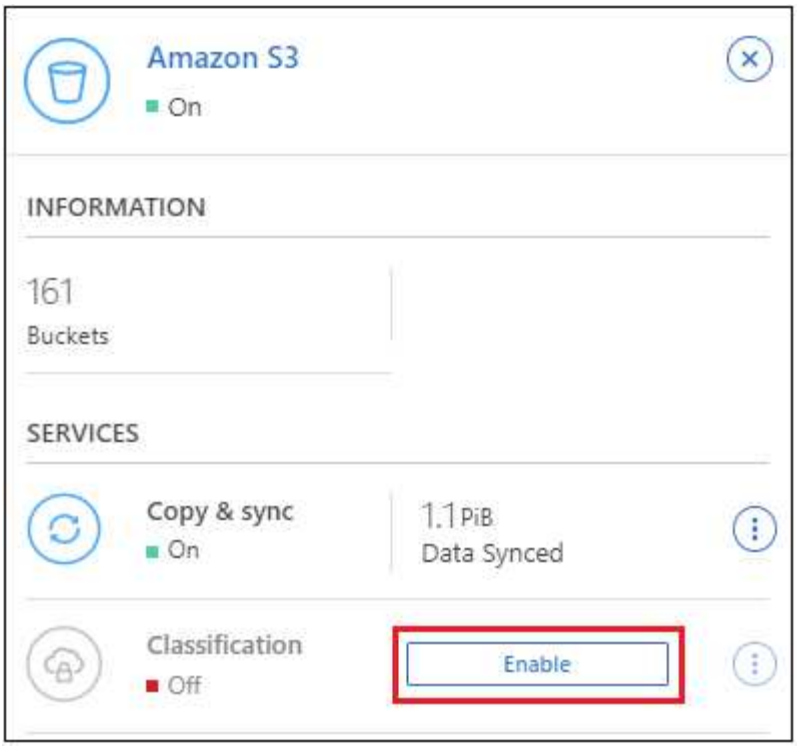
S3作業環境で**BlueXP**分類をアクティブ化します

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

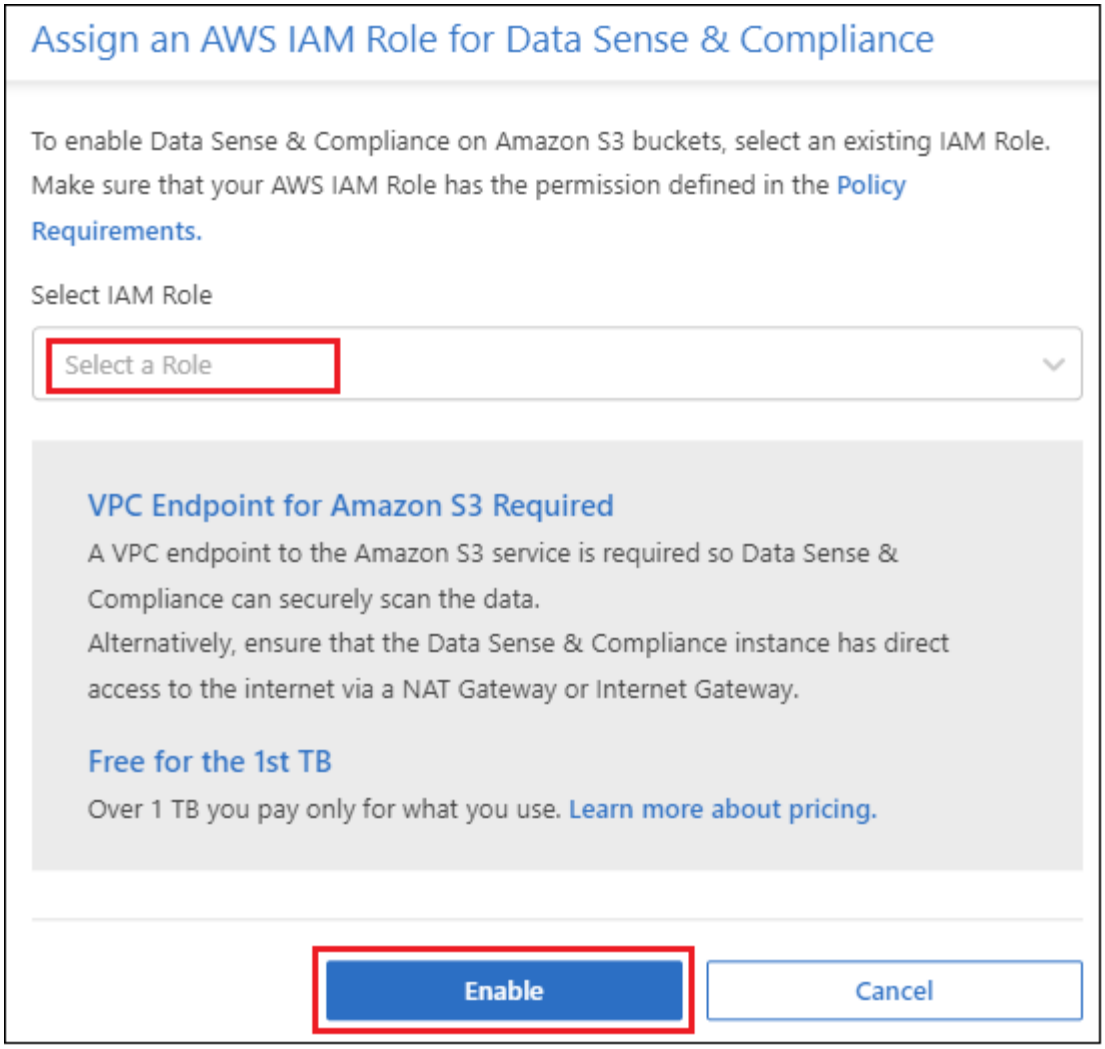
1. BlueXPの左ナビゲーションメニューから、*Storage > Canvas *をクリックします。
2. Amazon S3 作業環境を選択します。

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

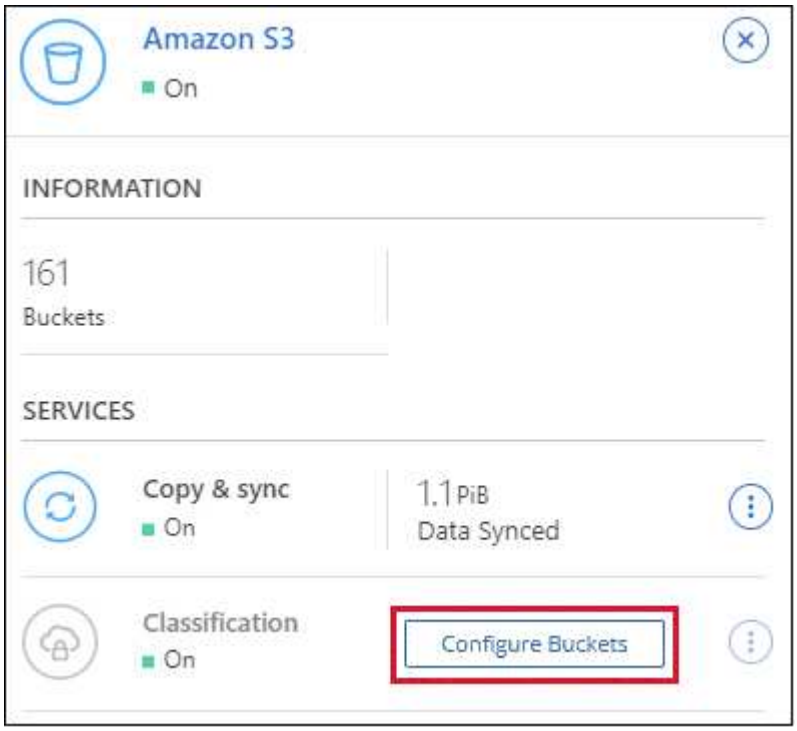
Amazon S3でBlueXPの分類を有効にしたら、次にスキャンするバケットを設定します。

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。

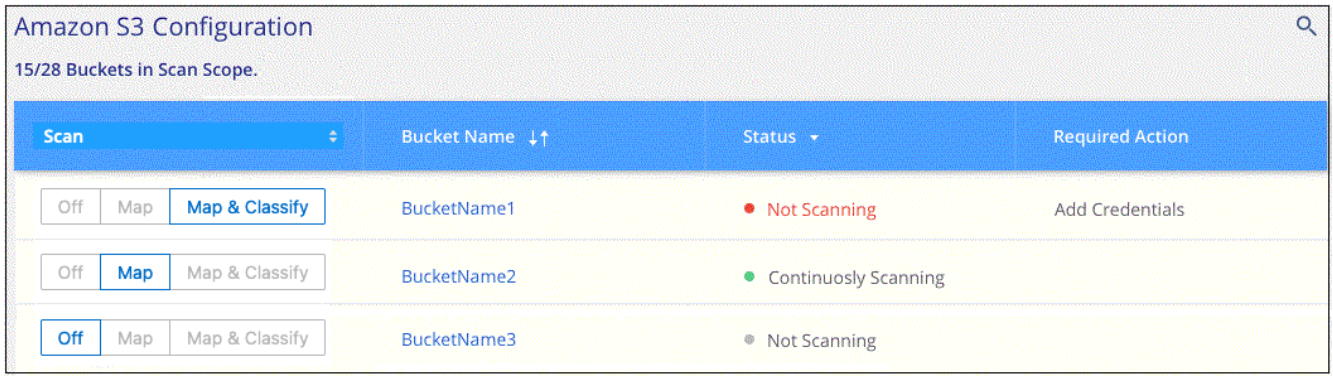
BlueXPに分類することもできます 別々の AWS アカウントにある S3 バケットをスキャンします。

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

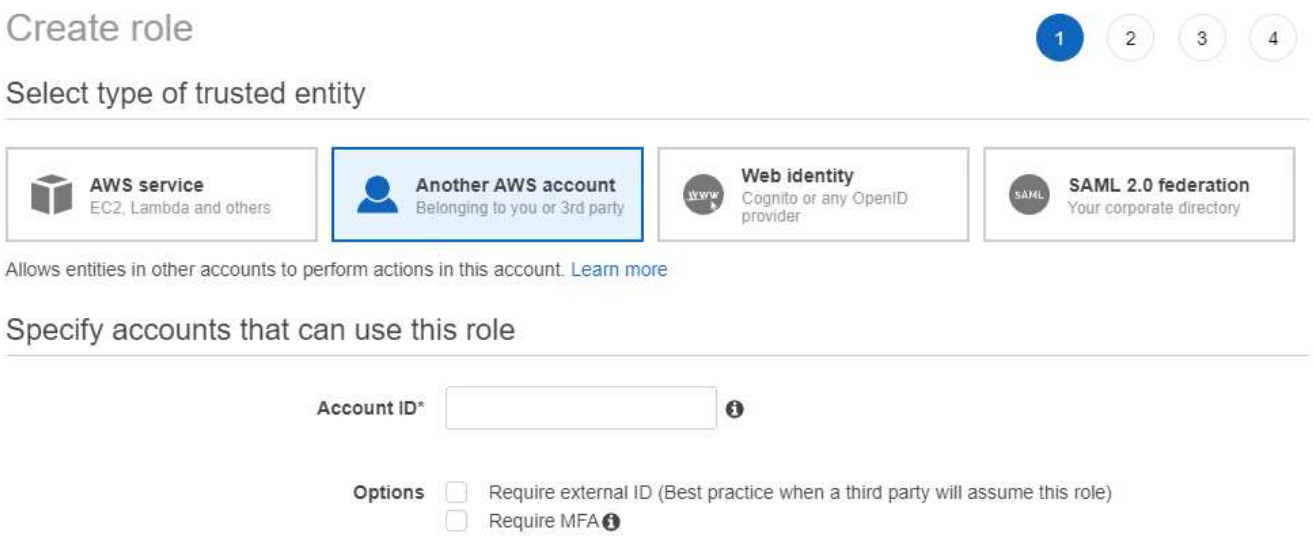
BlueXPの分類で、有効にしたS3バケットのスキャンが開始されます。エラーが発生した場合は、エラーを修正するために必要なアクションとともに、 [ステータス] 列に表示されます。

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": "*"
      },
  ]
}
```

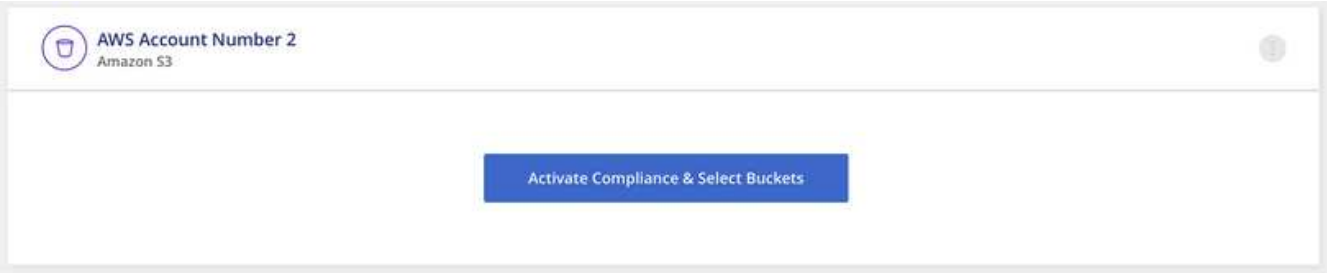
2. BlueXP分類インスタンスが配置されているソースAWSアカウントに移動し、インスタンスに関連付けられているIAMロールを選択します。
   a. 最大 CLI / API セッション期間 * を 1 時間から 12 時間に変更し、変更を保存してください。
   b. [* ポリシーの適用 *] をクリックし、 [ポリシーの作成 *] をクリックします。
   c. 「 STS ： AssumeRole 」アクションを含むポリシーを作成し、ターゲットアカウントで作成したロ

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"。

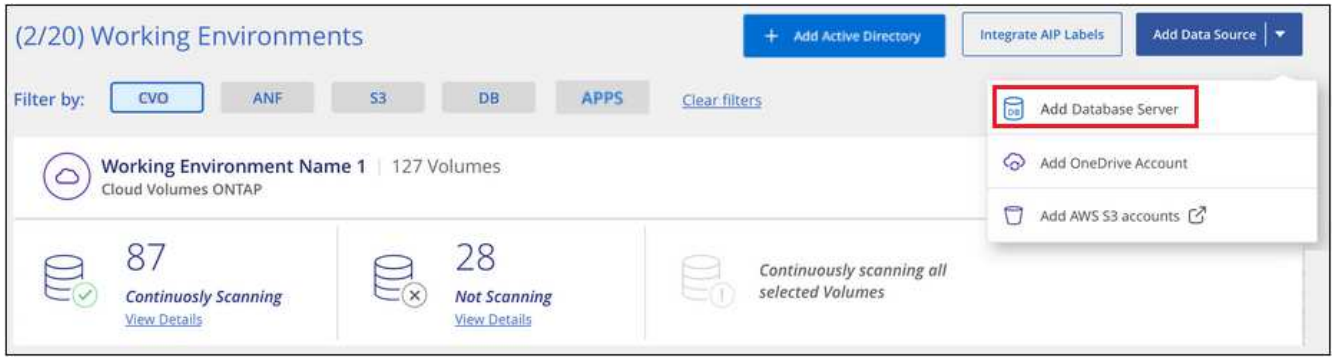
インターネットにアクセスできないダークサイトにインストールされているデータベーススキーマをスキャンする場合は、が必要です "インターネットアクセスのないオンプレミスと同じ場所にBlueXPの分類を導入します"。また、BlueXPコネクタがオンプレミスの同じ場所に配置されている必要があります。

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。

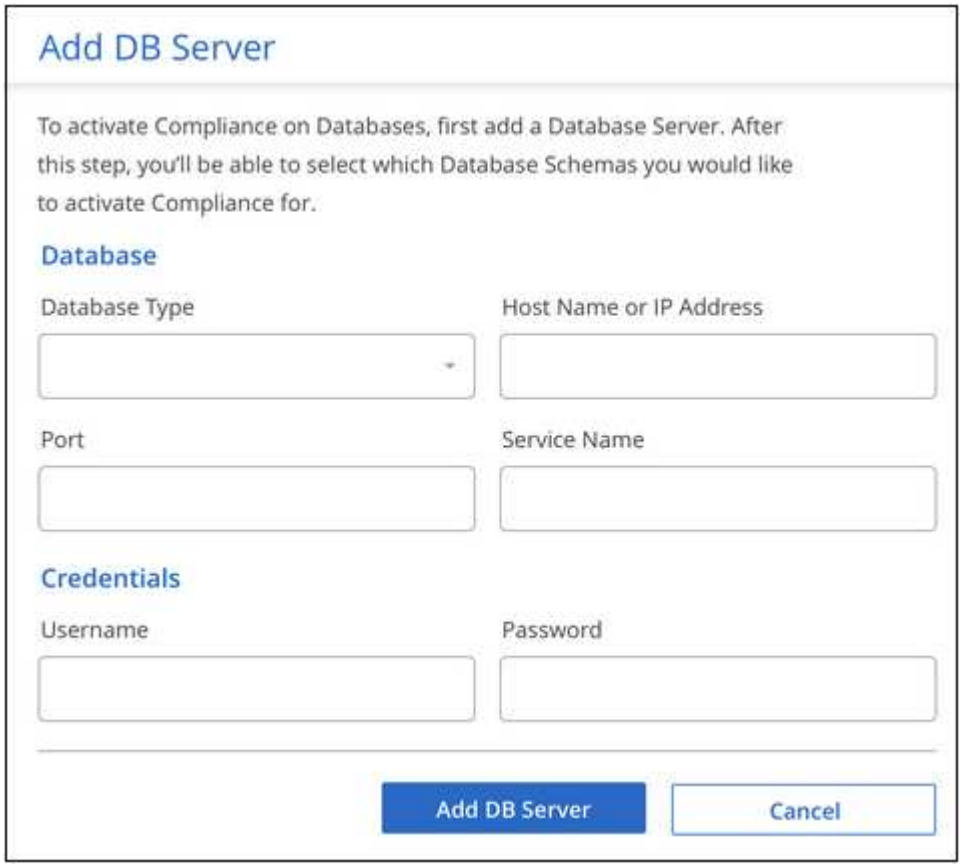
データベースサーバを追加します

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。

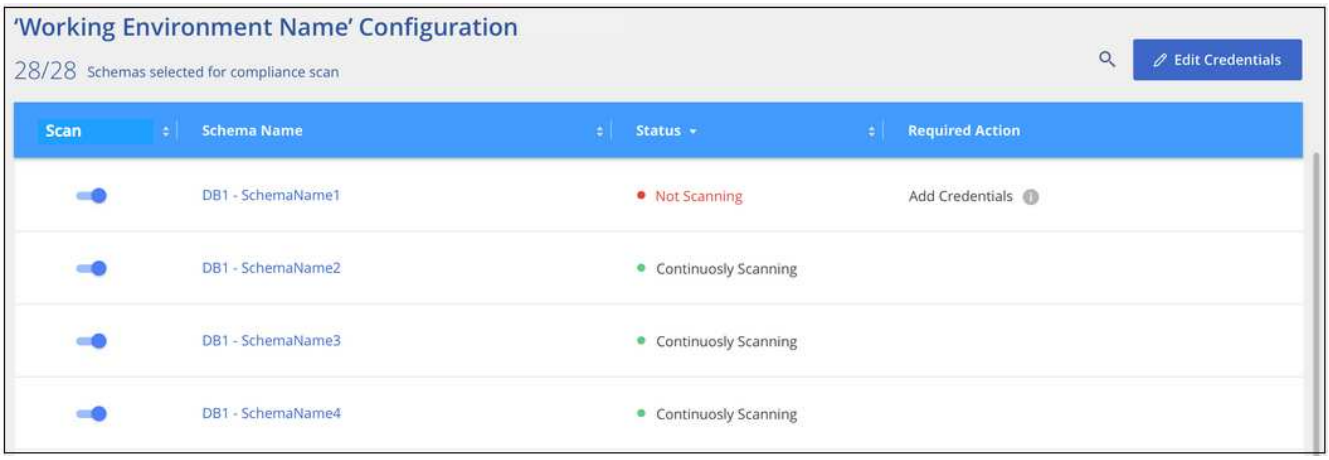
データベーススキーマでのコンプライアンススキャンの有効化と無効化

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"。

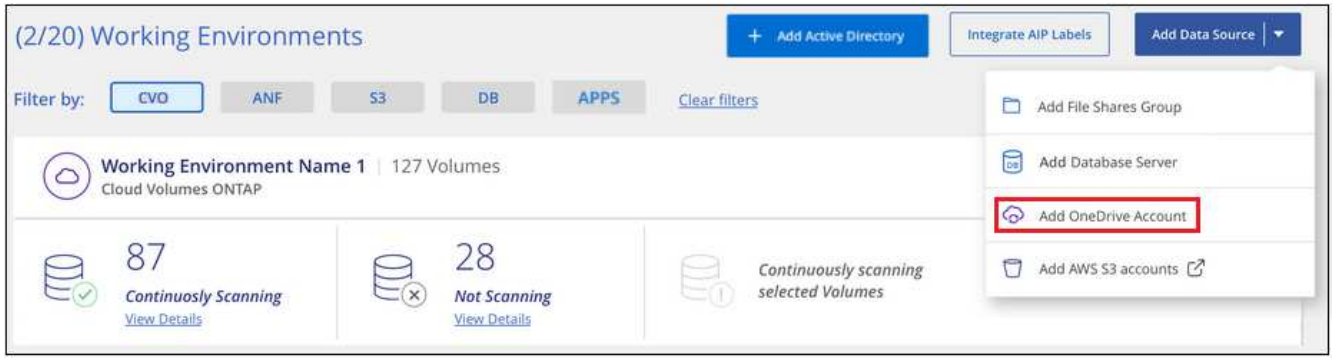
インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

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。

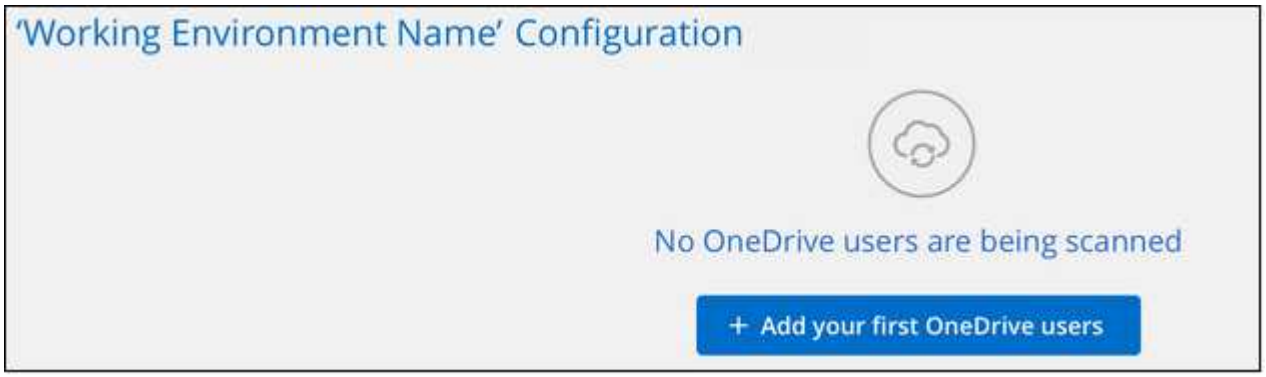
OneDrive ユーザーをコンプライアンススキャンに追加する

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。

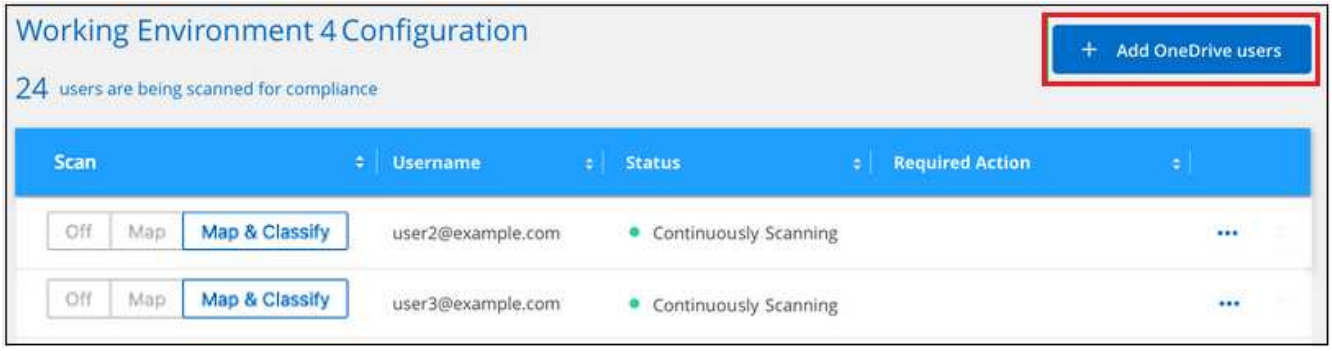
手順

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。

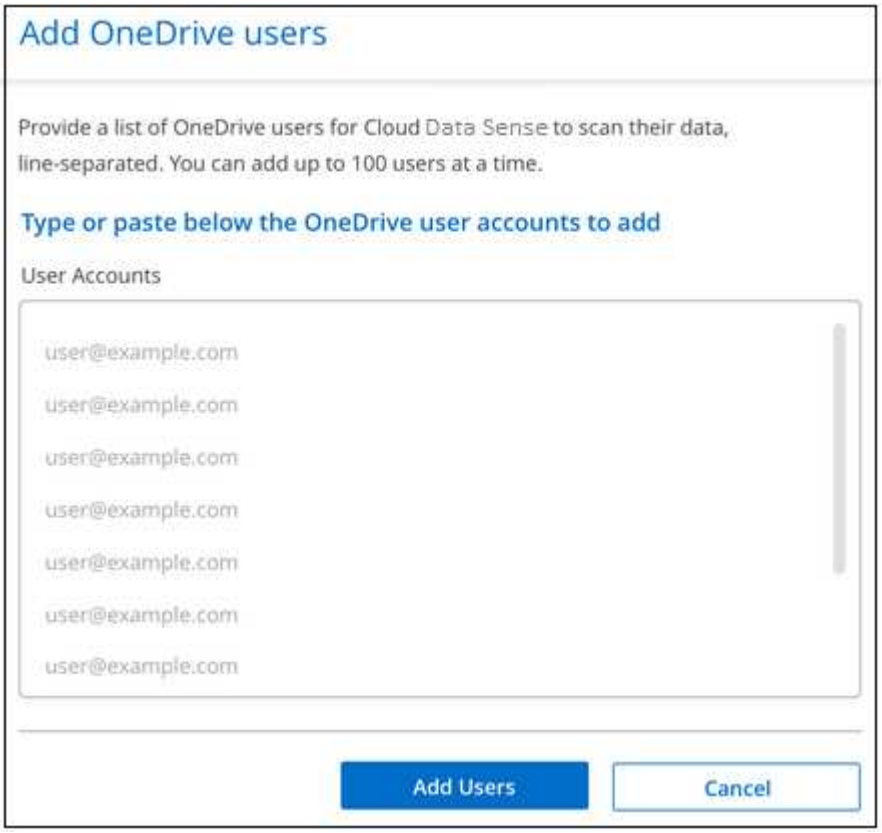


OneDrive アカウントからユーザーを追加する場合は、 [* OneDrive ユーザーの追加 *] をクリックします。



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

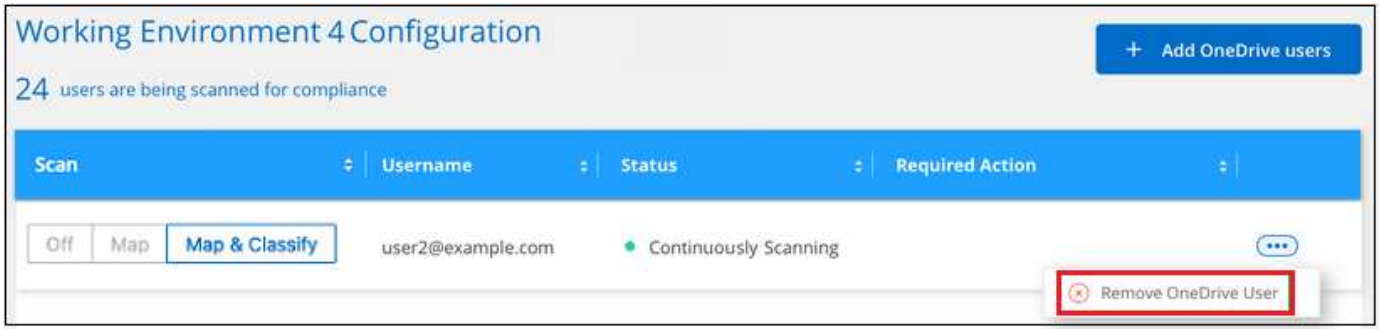
終了：	手順：
ユーザファイルのスキャンを無効にします	[* Off *] をクリックします

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。"。

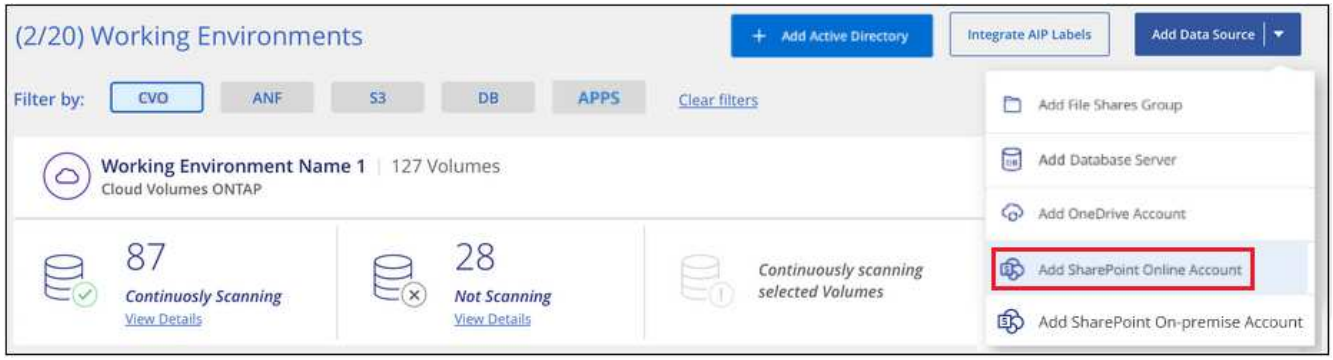
インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

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。

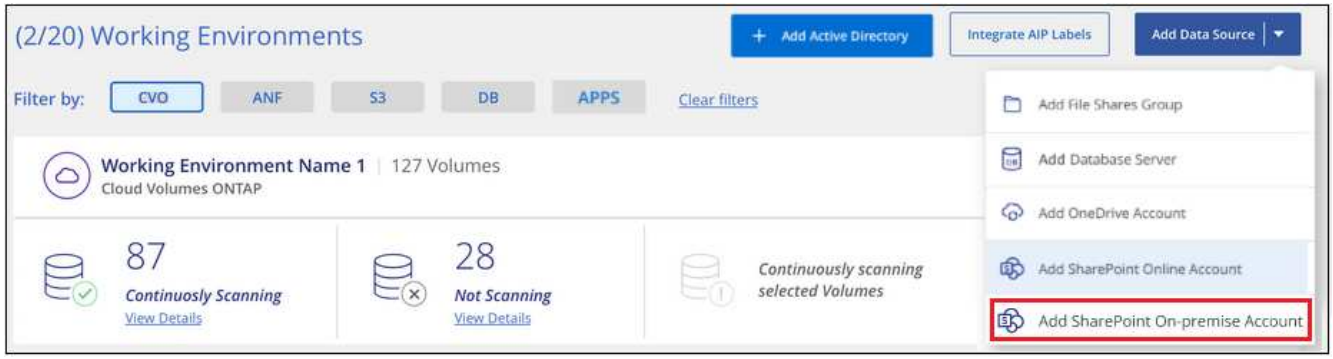
SharePoint Onlineアカウントが作業環境のリストに追加されます。

SharePointオンプレミスアカウントをSharePoint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。

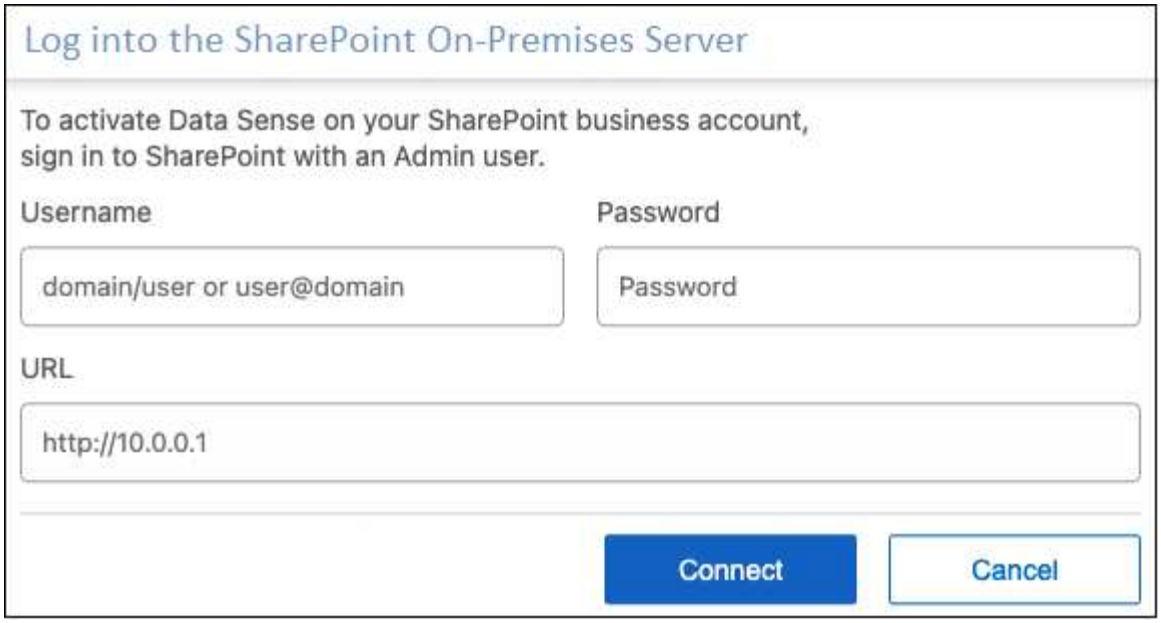
手順

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。

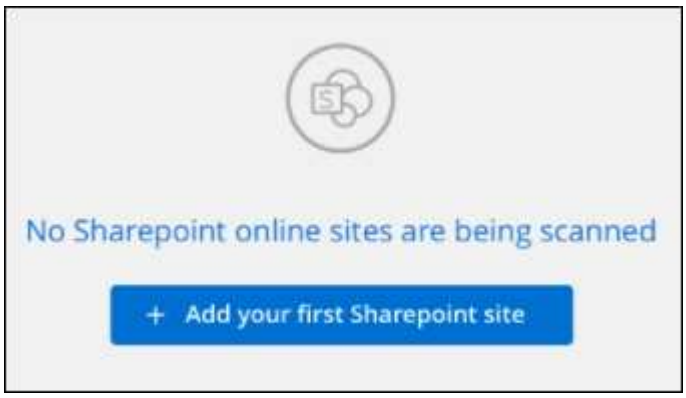
SharePoint サイトをコンプライアンススキャンに追加する

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。

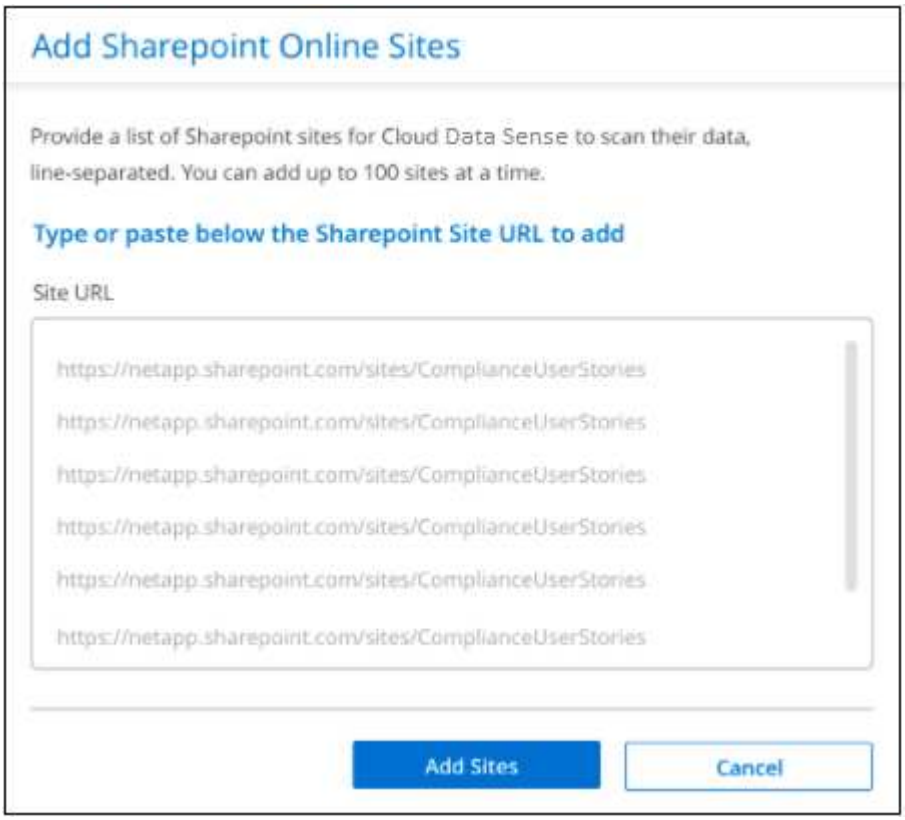
2. この SharePoint アカウントのサイトを初めて追加する場合は、 [* 最初の SharePoint サイトを追加する *] をクリックします。



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

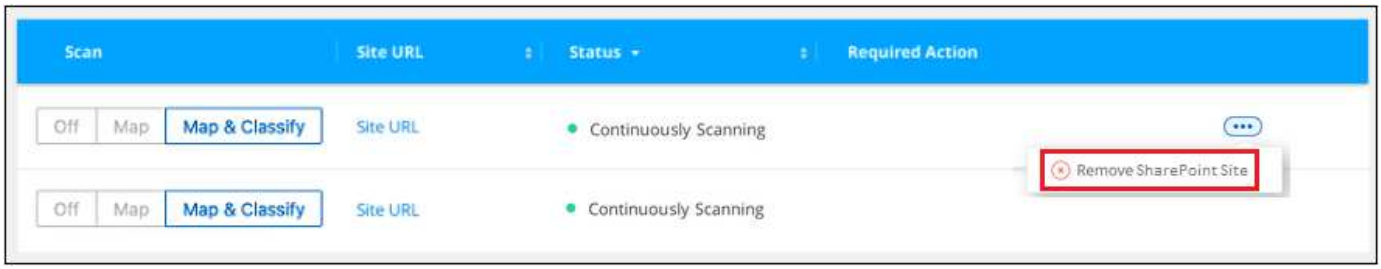
終了：	手順：
ファイルのフルスキャンを有効にします	[マップと分類 *] をクリックします
ファイルのスキャンを無効にします	[* Off *] をクリックします

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。

3 **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。

4 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"。

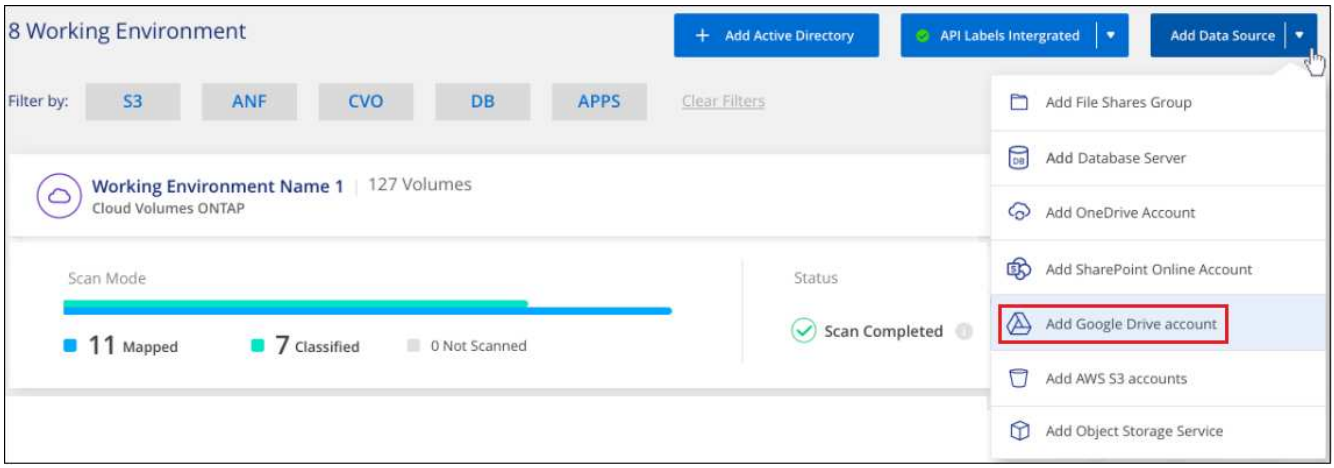
インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

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。

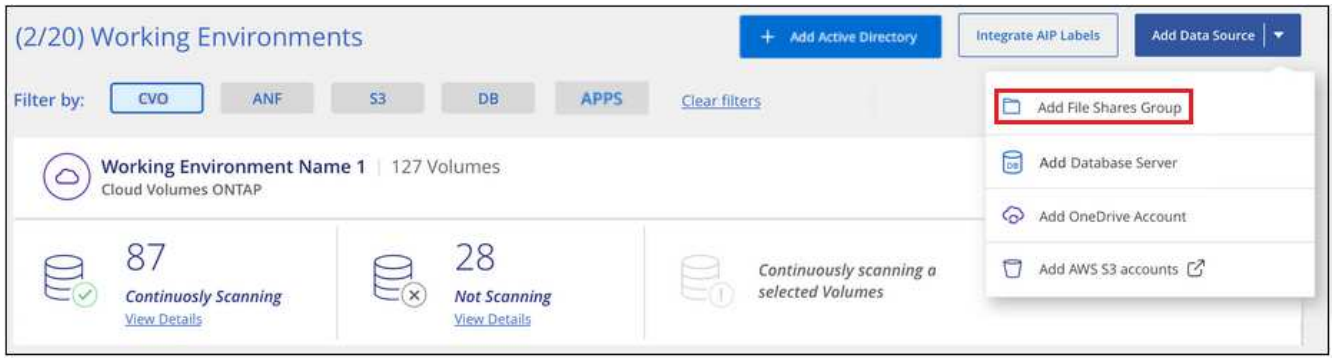
ファイル共有のグループを作成します

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>`。

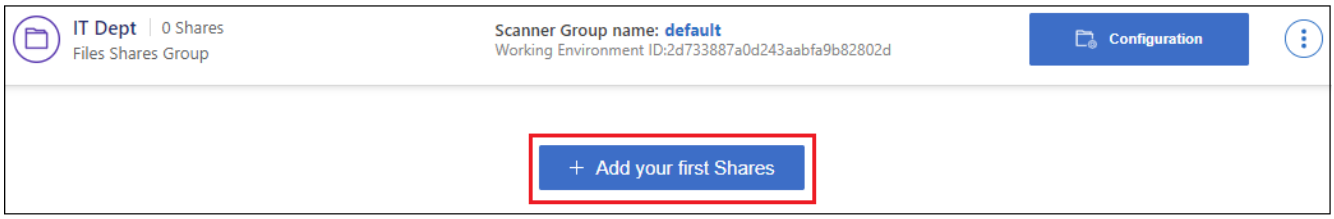
個々のファイル共有を追加することも、スキャンするファイル共有を 1 行で区切って指定することもできます。一度に最大 100 個の共有を追加できます。

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。



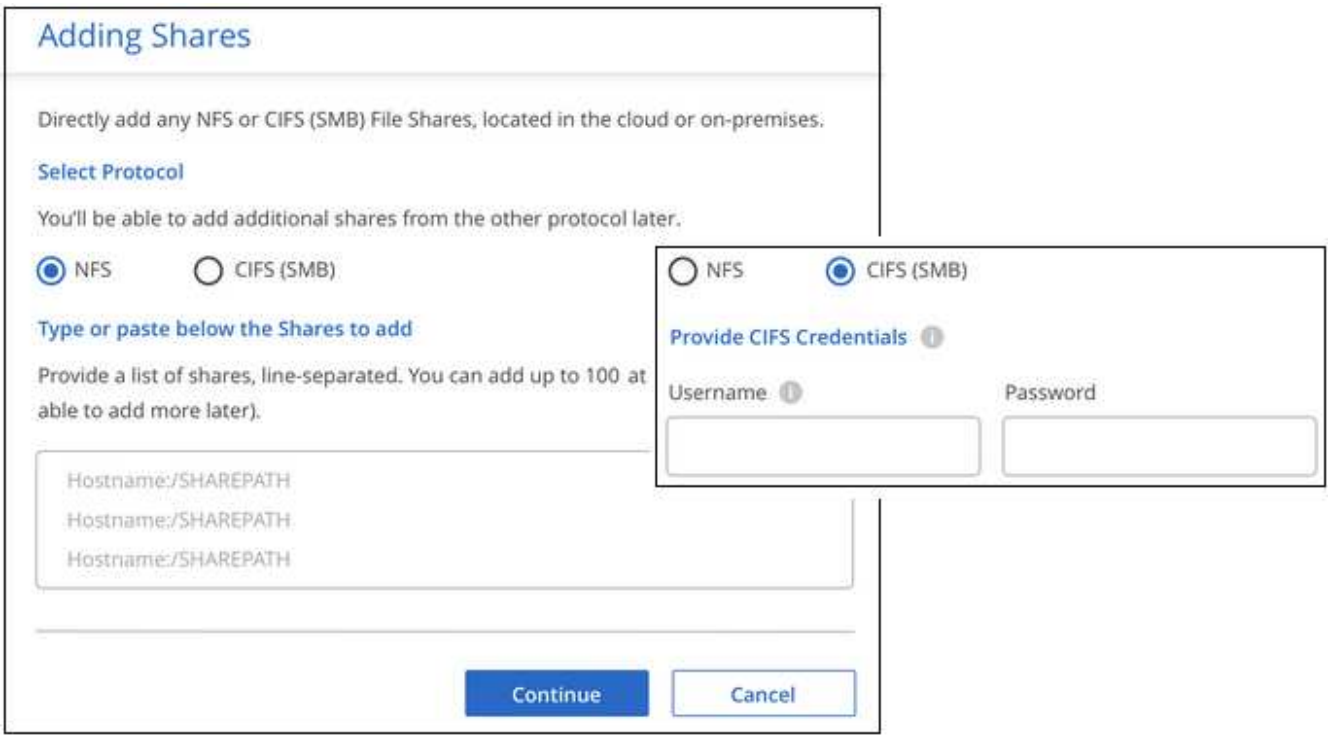
ボタンを示すスクリーンショット。"]

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

終了：	手順：
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

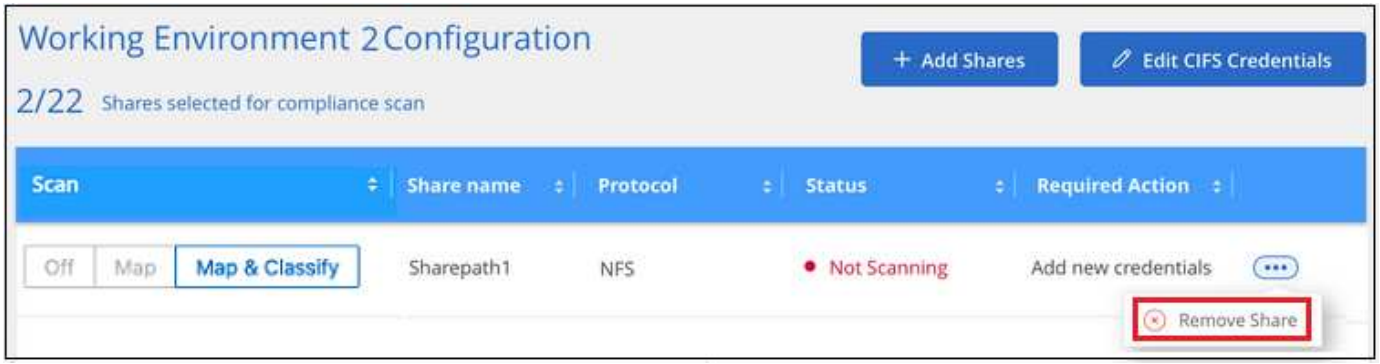
「属性の書き込み」権限がない場合にスキャンする*のページ上部のスイッチは、デフォルトでは無効になっています。つまり、BlueXPの分類にCIFSの属性への書き込み権限やNFSの書き込み権限がない場合、BlueXPの分類では「最終アクセス時間」を元のタイムスタンプに戻すことができないため、ファイルはスキャンされません。最終アクセス時間がリセットされても構わない場合は、スイッチをオンにすると、権限に関係なくすべてのファイルがスキャンされます。 "詳細はこちら。"。

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。

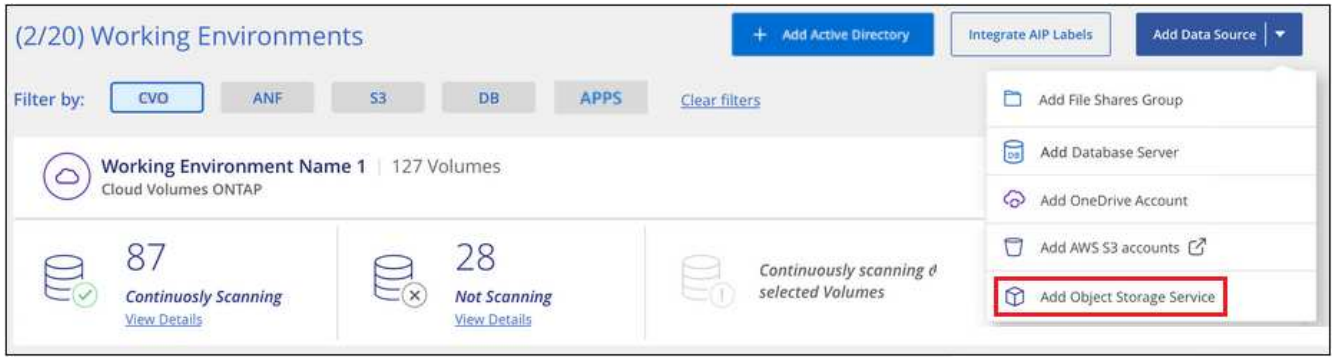
インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

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

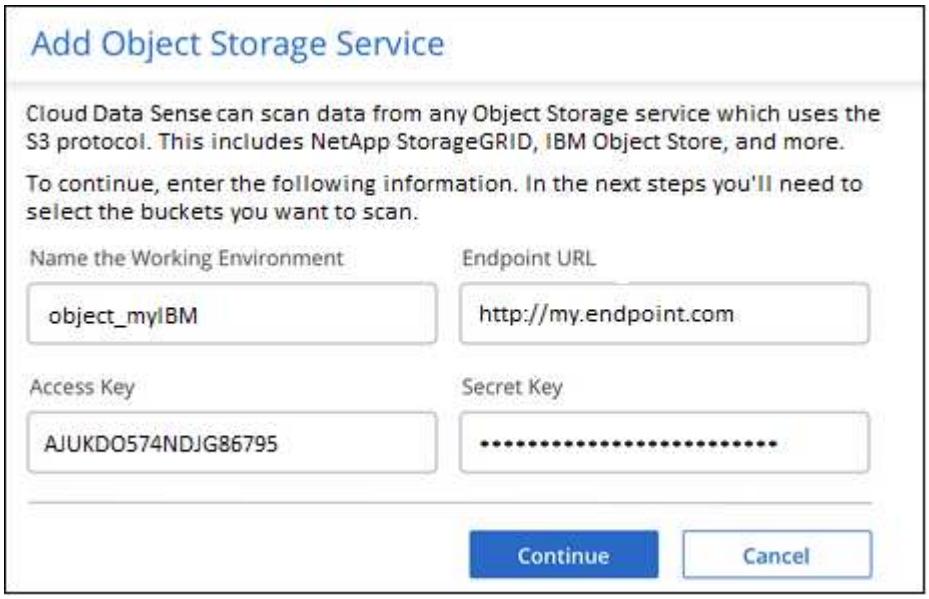
オブジェクトストレージサービスを追加します。

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

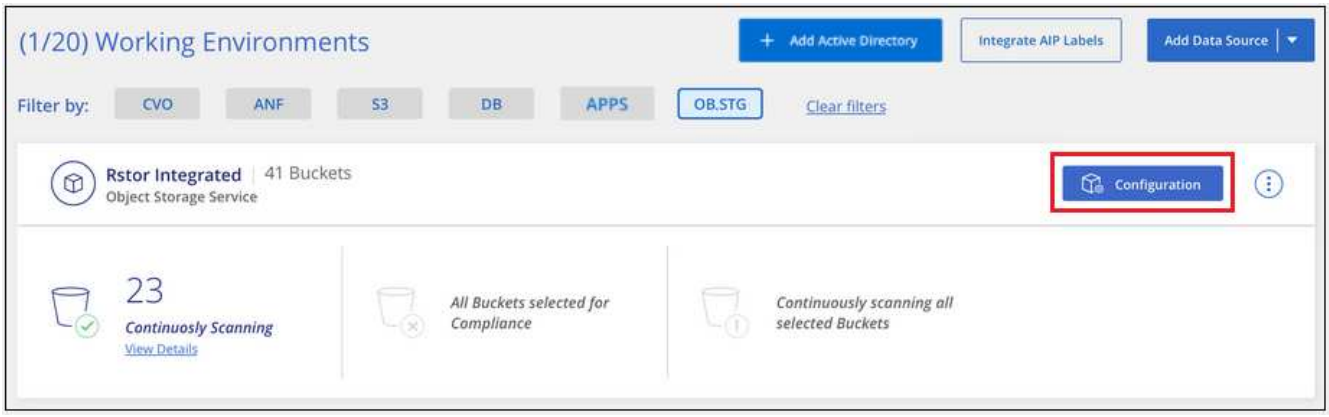
新しいオブジェクトストレージサービスが作業環境のリストに追加されます。

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

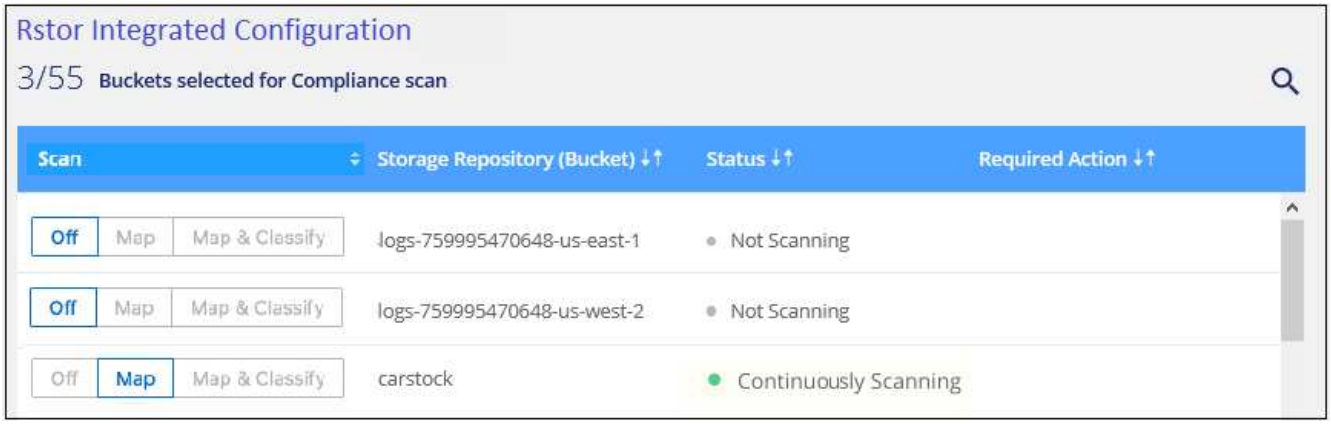
オブジェクトストレージサービスでBlueXPの分類を有効にしたら、次の手順でスキャンするバケットを設定します。BlueXPの分類により、該当するバケットが検出され、作成した作業環境に表示されます。

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。

Active DirectoryをBlueXPに統合しましょう

グローバルなActive DirectoryとBlueXPの分類を統合すると、BlueXPの分類で報告されるファイル所有者や、どのユーザやグループがファイルにアクセスできるかについての結果を強化できます。

BlueXPでCIFSボリュームをスキャンするためには、特定のデータソース（以下を参照）を設定するときにActive Directoryのクレデンシャルを入力する必要があります。この統合により、BlueXPの分類に、それらのデータソースに存在するデータのファイル所有者と権限の詳細が表示されます。これらのデータソースに対して入力した Active Directory は、ここで入力したグローバル Active Directory クレデンシャルと異なる場合があります。BlueXPの分類では、統合されているすべてのActive Directoryでユーザと権限の詳細が確認されます。

この統合により、BlueXPでは次の場所で追加情報 が提供されます。

- 「ファイル所有者」を使用できます。 "フィルタ" [調査]ペインで、ファイルのメタデータの結果を確認できます。SID （セキュリティ ID ）を含むファイル所有者ではなく、実際のユーザ名が入力されます。
- を参照してください "フルファイル権限" [すべてのアクセス許可の表示]ボタンをクリックしたときに、各ファイルおよびディレクトリについて、
- を参照してください "ガバナンスダッシュボード"を選択すると、 [アクセス許可] パネルに、データに関するより詳細な情報が表示されます。

ローカルユーザの SID および不明なドメインの SID は、実際のユーザ名に変換されません。

サポートされているデータソース

Active DirectoryとBlueXPの統合では、次のデータソースからデータを識別できます。

- オンプレミスの ONTAP システム
- Cloud Volumes ONTAP
- Azure NetApp Files の特長
- FSX for ONTAP の略
- ネットアップ以外のCIFSファイル共有（NFSファイル共有は除く）
- OneDrive アカウント
- SharePoint アカウント

データベーススキーマ、Googleドライブアカウント、Amazon S3アカウント、またはSimple Storage Service（S3）プロトコルを使用するオブジェクトストレージからユーザと権限の情報を識別することはできません。

Active Directoryサーバへの接続

BlueXPの分類を導入し、データソースでスキャンをアクティブ化したら、BlueXPの分類をActive Directoryに統合できます。Active Directory には、 DNS サーバの IP アドレスまたは LDAP サーバの IP アドレスを使用してアクセスできます。

Active Directoryクレデンシャルは読み取り専用ですが、管理者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。

CIFSボリューム/ファイル共有の場合、BlueXPの分類スキャンでファイルの「最終アクセス日時」に変更がないことを確認するには、ユーザにWrite Attributes権限を付与することを推奨します。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。

要件

- 社内のユーザに対して Active Directory がすでに設定されている必要があります。
- Active Directory の次の情報が必要です。
  - DNS サーバの IP アドレス、または複数の IP アドレス

または

LDAP サーバの IP アドレス、または複数の IP アドレス

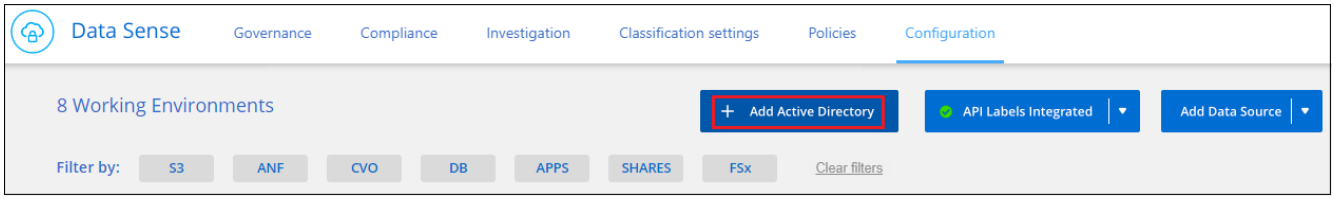
- サーバーにアクセスするためのユーザー名とパスワード
- ドメイン名（ Active Directory 名）
- セキュアな LDAP （ LDAPS ）を使用しているかどうか
- LDAP サーバポート（通常は LDAP では 389 、セキュア LDAP では 636 ）

- BlueXP分類インスタンスによるアウトバウンド通信用に、次のポートが開いている必要があります。

プロトコル	ポート	宛先	目的
TCP および UDP	389	Active Directory	LDAP
TCP	636	Active Directory	LDAP over SSL
TCP	3268	Active Directory	グローバルカタログ
TCP	3269	Active Directory	SSL 経由のグローバルカタログ

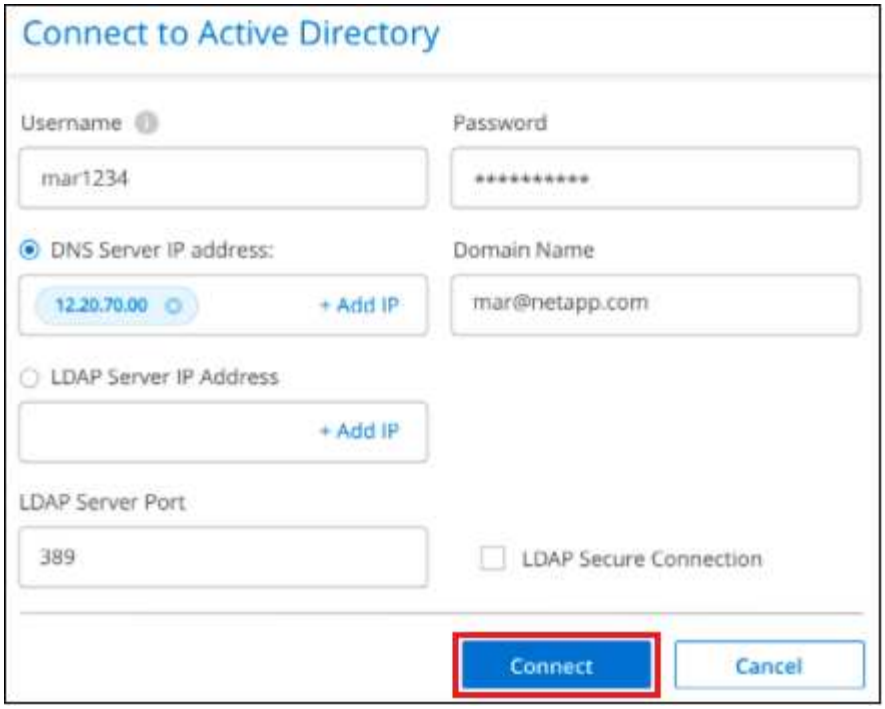
手順

1. BlueXPの分類の設定ページで、* Active Directoryの追加*をクリックします。

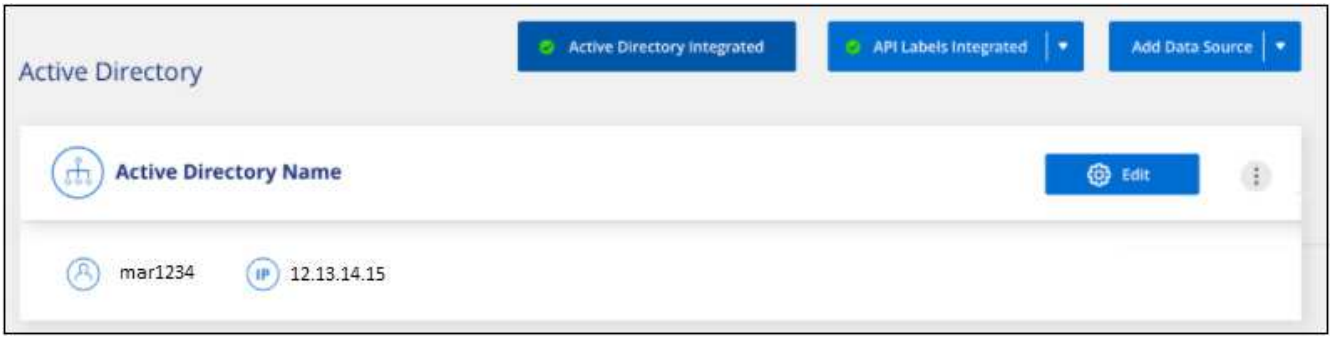


2. Active Directory への接続ダイアログで、 Active Directory の詳細を入力し、 * 接続 * をクリックします。

   必要に応じて、 * IP の追加 * をクリックすると、複数の IP アドレスを追加できます。



BlueXPはActive Directoryに分類され、[設定]ページに新しいセクションが追加されました。



Active Directory統合の管理

Active Directory 統合の値を変更する必要がある場合は、 * Edit * ボタンをクリックして変更を行います。

不要になった統合は、をクリックして削除することもできます ボタン"] ボタンをクリックして、 * Active Directory を削除 * をクリックします。

BlueXP分類用のライセンスをセットアップ

BlueXPワークスペースでBlueXPの分類によってスキャンされる最初の1TBのデータは30日間無料です。そのあとも引き続きデータをスキャンするには、ネットアップのBYOLライセンス、またはクラウドプロバイダのマーケットプレイスからのサブスクリプションが必要です。

さらに読む前に、いくつかのメモを記入してください。

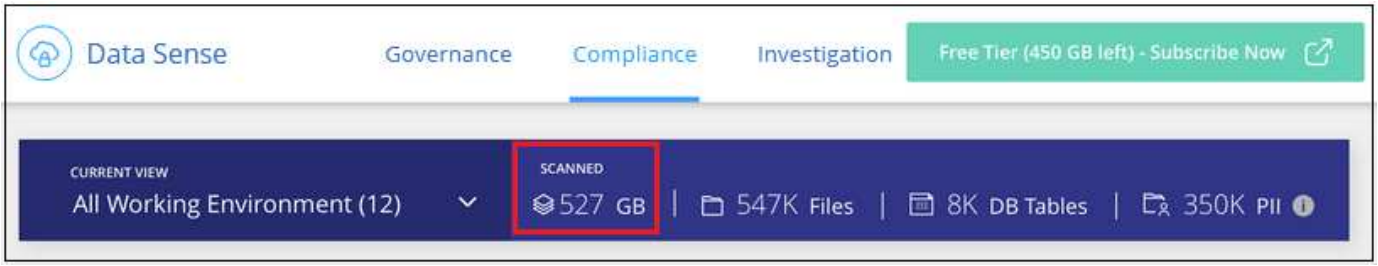
- クラウドプロバイダのマーケットプレイスでBlueXPの従量課金制（PAYGO）サブスクリプションにすでに登録している場合は、BlueXPの分類にも自動的に登録されます。再度サブスクライブする必要はありません。
- BlueXPの分類（Data Sense）であるBring-your-own-license（BYOL）は_floating_licenseです。このライセンスは、スキャンするワークスペース内のすべての作業環境とデータソースに使用できます。BlueXPデジタルウォレットには、アクティブなサブスクリプションが表示されます。
- スキャンされるデータの量は論理ファイルサイズに基づいて計算され、Storage Efficiency機能は使用されません。

"BlueXPの分類に関連するライセンスとコストの詳細については、こちらをご覧ください"。

30 日間の無償トライアルをご利用いただけます

BlueXPワークスペースでは、BlueXPの分類によってスキャンされる最大1TBのデータを対象とした30日間の無償トライアルを利用できます。その後もデータのスキャンを継続するには、NetAppからBYOLライセンスを購入するか、クラウドプロバイダのマーケットプレイスからサブスクリプションに登録する必要があります。

いつでも購読できます。30日間の試用期間が終了するか、データ量が1TBを超えるまでは、料金は発生しません。スキャンされているデータの合計量は、BlueXPの分類Governance Dashboardでいつでも確認できます。また、 [今すぐサブスクライブ] ボタンを使用すると、準備が整ったときに簡単にサブスクライブできます。



ボタン。"]

BlueXP分類のPAYGOサブスクリプションを使用

クラウドプロバイダのマーケットプレイスで提供されている従量課金制サブスクリプションを使用すると、Cloud Volumes ONTAPシステムや多くのBlueXPサービス（BlueXP分類など）のライセンスを取得できます。BlueXP分類が1つのサブスクリプションで1時間ごとにスキャンしているデータの量に応じて、クラウドプロバイダに料金を支払います。

登録することで、無償トライアルの終了後にサービスが中断されることがなくなります。トライアルが終了すると、スキャンしているデータの量に応じて1時間ごとに課金されます。無料トライアル中は、月額プランから課金されることはありません。

手順

これらの手順は、 _Account Admin_role 権限を持つユーザが実行する必要があります。

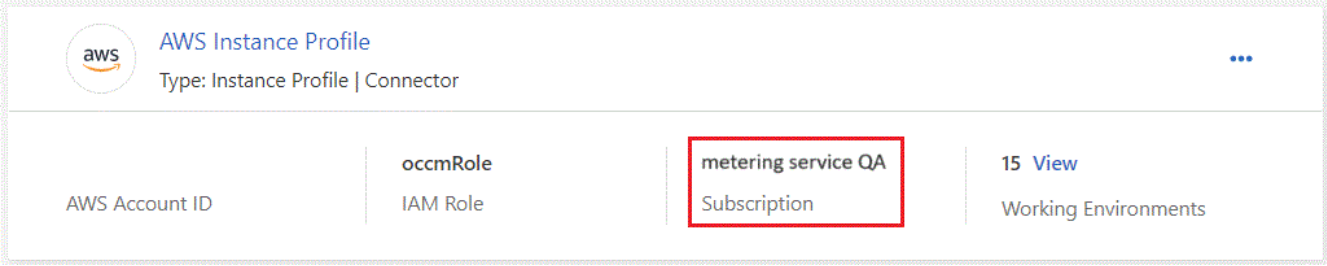
1. BlueXPコンソールの右上にある[設定]アイコンをクリックし、[資格情報*]を選択します。

アイコンを選択できます。"]

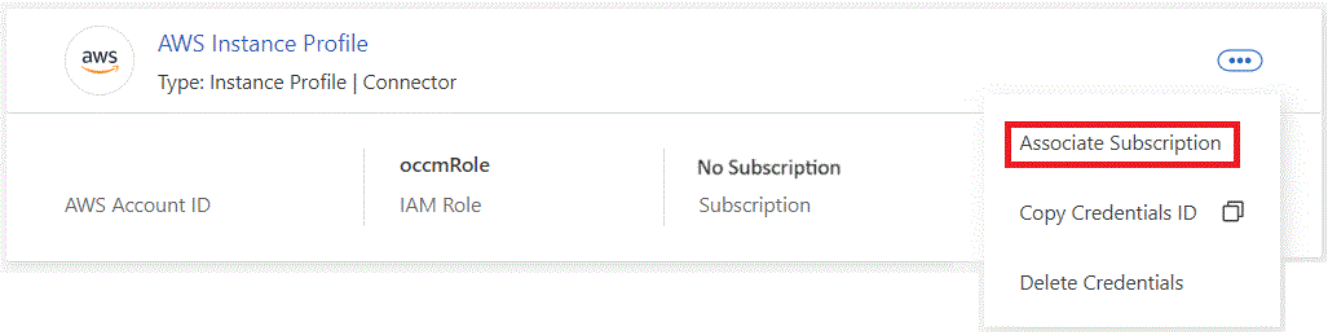
2. [Credentials]*をクリックし、AWSインスタンスプロファイル、Azure Managed Service Identity、またはGoogle Projectのクレデンシャルを検索します。

   サブスクリプションは、インスタンスプロファイル、マネージドサービス ID 、または Google プロジェクトに追加する必要があります。充電ができない。

   以下のAWS向けBlueXPサブスクリプションをすでにお持ちの場合は、設定が完了しています。他に必要なことはありません。



3. まだサブスクリプションをお持ちでない場合は、アクションメニューをクリックして*サブスクリプションの関連付け*をクリックします。



4. 既存のサブスクリプションを選択し、 [* アソシエイト *] をクリックするか、 [* サブスクリプションの追加 *] をクリックして、手順を実行します。

   次のビデオでは、を関連付ける方法を示します "AWS Marketplace" AWS サブスクリプションへのサブスクリプション：

   ▶ https://docs.netapp.com/ja-jp/bluexp-classification//media/video_subscribing_aws.mp4 *(video)*

   次のビデオでは、を関連付ける方法を示します "Azure Marketplace で入手できます" Azure サブスクリプションへのサブスクリプション：

   ▶ https://docs.netapp.com/ja-jp/bluexp-classification//media/video_subscribing_azure.mp4 *(video)*

   次のビデオでは、を関連付ける方法を示します "Google Cloud Marketplace" GCP サブスクリプションへのサブスクリプション：

   ▶ https://docs.netapp.com/ja-jp/bluexp-classification//media/video_subscribing_gcp.mp4 *(video)*

年間契約を使用する

BlueXP分類の料金は、年単位の契約を購入して年単位で支払います。期間は1年、2年、3年から選択できます。

市場で年間契約を結んでいるパートナー様は、BlueXPの分類データスキャンの料金がその契約に対して請求されます。BYOLでは、年単位のマーケットプレイス契約を組み合わせることはできません。

- AWS "価格の詳細については、BlueXP Marketplaceのサービスを参照してください"。
- Azure "価格の詳細については、BlueXP Marketplaceのサービスを参照してください"。
- Google Cloud：年間契約の購入については、NetAppの営業担当者にお問い合わせください。この契約は、Google Cloud Marketplaceでのプライベートオファーとして利用できます。NetAppからプライベートオファーが提供されたら、BlueXPの分類をアクティブ化する際にGoogle Cloud Marketplaceからサブスクライブする際に年間プランを選択できます。

BlueXP分類のBYOLライセンスを使用

ネットアップが提供するお客様所有のライセンスには、 1 年、 2 年、 3 年の期間があります。BYOL BlueXP分類（Data Sense）ライセンスは_floating_licenseです。このライセンスでは、*すべての*作業環境とデータソースで合計容量が共有されるため、初期ライセンスの取得や更新が容易になります。

BlueXP分類ライセンスをお持ちでない場合は、弊社までお問い合わせください。

- mailto ： ng-contact-data-sense@netapp.com ？ subject = ライセンス [ライセンスを購入するために電子メールを送信] 。
- ライセンスをリクエストするには、BlueXPの右下にあるチャットアイコンをクリックします。

必要に応じて、使用しないCloud Volumes ONTAP の未割り当てのノードベースライセンスがある場合は、同じ金額、同じ有効期限のBlueXP分類ライセンスに変換できます。 "詳細については、こちらをご覧ください"。

BlueXPデジタルウォレットを使用して、BlueXP分類のBYOLライセンスを管理します。BlueXPデジタルウォレットから、新しいライセンスの追加、既存ライセンスの更新、ライセンスステータスの表示を行うことができます。

BlueXP分類ライセンスファイルを入手します

BlueXP分類（Data Sense）ライセンスを購入したら、BlueXP分類のシリアル番号とNetApp Support Site（NSS）アカウントを入力するか、NetAppライセンスファイル（NLF）をアップロードして、BlueXPでライセンスをアクティブ化します。次の手順は、 NLF ライセンスファイルを取得する方法を示しています。

インターネットにアクセスできないオンプレミスサイトのホストにBlueXP分類を導入している（つまりBlueXPコネクタを "プライベートモード"では、インターネットに接続されたシステムからライセンスファイルを取得する必要があります。プライベートモードのインストールでは、シリアル番号とNSSアカウントを使用してライセンスをアクティブ化することはできません。

作業を開始する前に

開始する前に、次の情報が必要です。

- BlueXP分類のシリアル番号

  この番号は、SOから確認するか、アカウントチームにお問い合わせください。

- BlueXPアカウントID

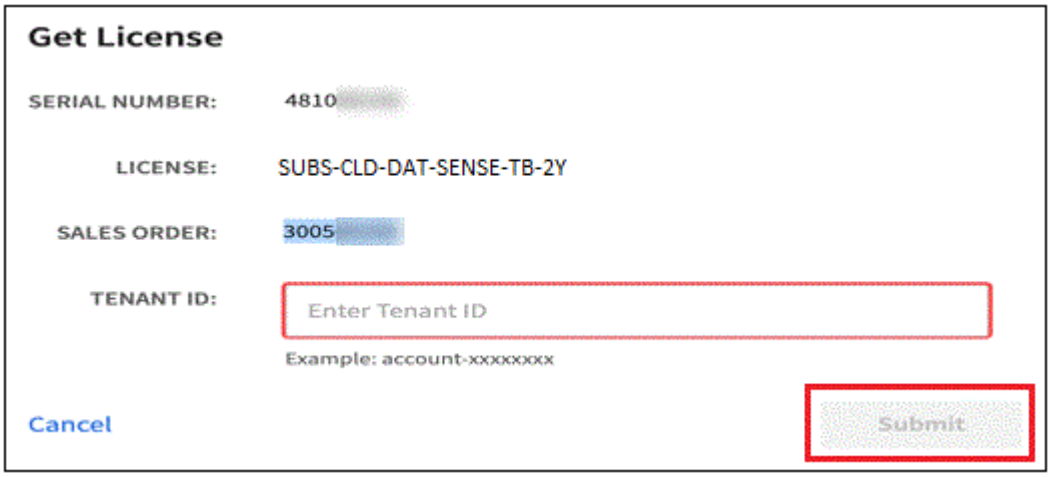
  BlueXPアカウントIDを確認するには、BlueXPの上部にある[**Account**]ドロップダウンを選択し、アカウン

トの横にある[**Manage Account**]をクリックします。アカウント ID は、 [概要] タブにあります。インターネットにアクセスできないプライベートモードのサイトでは、* account-DARKSITE1*を使用します。

手順

1. にサインインします "ネットアップサポートサイト" [システム] 、 [ソフトウェアライセンス] の順にクリックします。
2. BlueXP分類ライセンスのシリアル番号を入力します。

3. [ライセンスキー]列の*[Get NetApp License File]*をクリックします。
4. BlueXPアカウントID (これはサポートサイトではテナントIDと呼ばれます)を入力し'[**Submit**]をクリックしてライセンスファイルをダウンロードします



BlueXP分類の**BYOL**ライセンスをアカウントに追加します

BlueXPアカウント用のBlueXP分類（Data Sense）ライセンスを購入したら、BlueXP分類サービスを使用するにはライセンスをBlueXPに追加する必要があります。

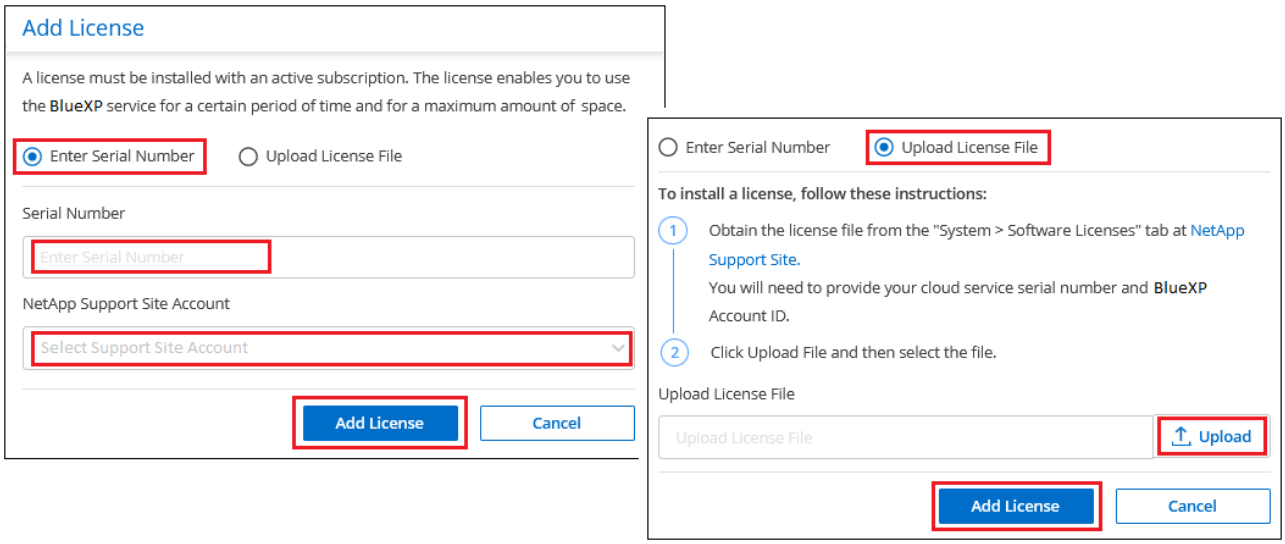
手順

1. BlueXPメニューから、「ガバナンス」>「デジタルウォレット」をクリックし、「データサービスライセンス」タブを選択します。
2. [ライセンスの追加] をクリックします。
3. _ ライセンスの追加 _ ダイアログで、ライセンス情報を入力し、 * ライセンスの追加 * をクリックします。

- BlueXP分類ライセンスのシリアル番号があり、NSSアカウントがわかっている場合は、*[シリアル番号の入力]*オプションを選択してその情報を入力します。

  お使いのNetApp Support Siteのアカウントがドロップダウンリストにない場合は、 "NSSアカウントをBlueXPに追加します"。

- BlueXP分類ライセンスファイル（ダークサイトにインストールされている場合に必要）がある場合は、*[Upload License File]*オプションを選択し、プロンプトに従ってファイルを添付します。



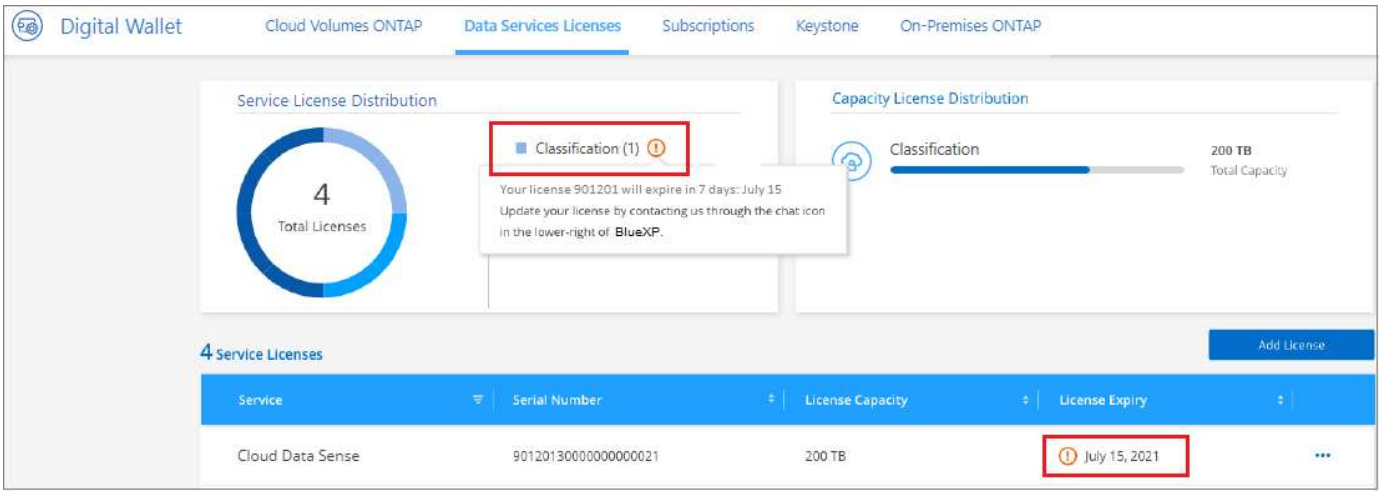
結果

BlueXPにライセンスが追加され、BlueXP分類サービスがアクティブになります。

BlueXP分類のBYOLライセンスを更新します

ライセンス期間が有効期限に近づいている場合、またはライセンス容量が上限に達している場合は、分類UIで通知されます。

このステータスは、BlueXPのデジタルウォレットや "通知"。



BlueXP分類ライセンスは、有効期限が切れる前に更新できるため、スキャンしたデータへのアクセスが中断されることはありません。

手順

1. BlueXPの右下にあるチャットアイコンをクリックして、特定のシリアル番号のCloud Data Senseライセンスの期間延長または追加容量をリクエストします。mailto ： ng-contact-data-sense@netapp.com ？subject= Licensing [ライセンスの更新をリクエストするメールを送信] もできます。

   ライセンスの料金を支払ってNetApp Support Site に登録すると、BlueXPデジタルウォレット内のライセンスが自動的に更新され、[Data Services Licenses]ページに5~10分後に変更が反映されます。

2. BlueXPがライセンスを自動的に更新できない場合(たとえば、ダークサイトにインストールされている場合)、ライセンスファイルを手動でアップロードする必要があります。

   a. 可能です ライセンスファイルをネットアップサポートサイトから入手します。

   b. BlueXPデジタルウォレットページの[Data Services Licenses]タブで、をクリックします ••• アイコン"] 更新するサービスシリアル番号の場合は、 [* ライセンスの更新 *] をクリックします。

   ボタンを選択するスクリーンショット。"]

   c. _Update License_page で、ライセンスファイルをアップロードし、 * ライセンスの更新 * をクリックします。

結果

BlueXPのライセンスが更新され、BlueXP分類サービスが引き続きアクティブになります。

BYOL ライセンスに関する考慮事項

BlueXP分類（Data Sense）BYOLライセンスを使用している場合、スキャンするすべてのデータのサイズが容量の上限に近づいているかライセンスの有効期限に近づいているときに、BlueXPの分類UIとBlueXPのデジタルウォレットUIに警告が表示されます。次の警告が表示されます。

- スキャンするデータ量がライセンスで許可された容量の 80% に達したとき、および制限に達したときに再度スキャンします
- ライセンスの有効期限が切れる 30 日前と、ライセンスの有効期限が切れたあとに再度有効になります

これらの警告が表示された場合は、BlueXPインターフェイスの右下にあるチャットアイコンを使用してライセンスを更新してください。

ライセンスの有効期限が切れた場合、またはBYOLの上限に達した場合でも、BlueXPの分類は引き続き実行されますが、ダッシュボードへのアクセスはブロックされるため、スキャンしたデータに関する情報を表示できません。スキャンするボリューム数を減らして容量の使用量をライセンスの上限までにする場合は、_Configuration_page だけを使用できます。

BYOLライセンスを更新すると、BlueXPデジタルウォレットのライセンスが自動的に更新され、すべてのダッシュボードにフルアクセスできるようになります。BlueXPが安全なインターネット接続経由でライセンスファイルにアクセスできない場合(たとえば、ダークサイトにインストールされている場合)は、自分でファイルを取得してBlueXPに手動でアップロードできます。手順については、を参照してください BlueXP分類ライセンスを更新する方法。

> 使用しているアカウントがBYOLライセンスとPAYGOサブスクリプションの両方を所有している場合、BYOLライセンスの有効期限が切れた時点でBlueXP classification_はPAYGOサブスクリプションに移行しません。BYOL ライセンスを更新する必要があります。

BlueXPの分類に関するよくある質問

この FAQ は、質問に対する簡単な回答を探している場合に役立ちます。

BlueXP分類サービス

次の質問は、BlueXPの分類について一般的に理解していることを示しています。

BlueXPの分類とは何ですか？

BlueXPは、人工知能（AI）ベースのテクノロジを使用して、データのコンテキストを把握し、ストレージシステム全体で機密データを特定できるクラウドサービスです。システムには、BlueXP Canvasに追加した作業環境や、BlueXPの分類でネットワーク経由でアクセスできるさまざまな種類のデータソースを使用できます。 "以下の一覧を参照してください"。

BlueXPは分類されるため、事前定義されたパラメータ（機密情報のタイプやカテゴリなど）を使用して、データプライバシーと機密性に関する新しいデータコンプライアンス規制（GDPR、CCPA、HIPAAなど）に対応できます。

BlueXPの分類の仕組み

BlueXPは、人工知能のもう1つのレイヤを、BlueXPシステムやストレージシステムとともに導入します。次に、ボリューム、バケット、データベース、その他のストレージアカウントのデータをスキャンして、見つか

ったデータ分析のインデックスを作成します。BlueXPの分類では、正規表現とパターンマッチングを中心に構築されている他のソリューションとは異なり、人工知能と自然言語処理の両方が活用されます。

BlueXPの分類では、AIを使用してデータのコンテキストを把握し、正確な検出と分類を実現します。AIは、最新のデータタイプと拡張性を考慮して設計されているため、この目的はAIによって推進されます。また、データコンテキストを理解して、強力で正確な検出と分類を提供します。

"BlueXPの分類の仕組みについて詳しくは、こちらをご覧ください"。

BlueXPに分類される一般的なユースケースを教えてください。

- 個人識別情報（ PII ）を識別します。
- GDPR 、 CCPA 、 HIPAA 、その他のデータプライバシー規制の要件に応じて、データ主体に応じて特定のデータを容易に検索し、レポートを作成できます。
- データプライバシーに関する新しい規制や今後の規制に対応できます。
- データコンプライアンスやプライバシーの規制に準拠
- 従来型システムからクラウドへデータを移行
- データ保持ポリシーに準拠

"BlueXP分類のユースケースの詳細については、こちらをご覧ください"。

BlueXPのアーキテクチャはどうですか？

BlueXPはクラウドかオンプレミスかを問わず、単一のサーバ（クラスタ）を任意の場所に導入できます。サーバは標準プロトコルでデータソースに接続し、同じサーバにも導入されているElasticsearchクラスタの結果をインデックス化します。これにより、マルチクラウド環境、クロスクラウド環境、プライベートクラウド環境、オンプレミス環境をサポートできます。

サポートされているクラウドプロバイダを教えてください。

BlueXPの分類はBlueXPの一部として機能し、AWS、Azure、GCPをサポートします。これにより、異なるクラウドプロバイダ間で統一されたプライバシー可視性を実現できます。

BlueXPには**REST API**がありますか？また、他社製ツールと連携できますか？

BlueXPは、サービスのREST API機能をサポートしています。BlueXPの管理が推奨されない場合は、REST APIを使用してBlueXPの分類などのサービスを使用することもできます。すべてのユーザアクションには、サードパーティのシステムと統合できるREST APIがあります。を参照してください "BlueXP分類API" を参照してください。

BlueXPの分類はマーケットプレイスを通じて提供されますか？

はい。BlueXPとBlueXPの分類は、AWS、Azure、GCPのマーケットプレイスで提供されています。

BlueXPの分類スキャンと分析

ここでは、BlueXPの分類スキャンのパフォーマンスとユーザが利用できる分析について説明します。

BlueXPの分類では、どのくらいの頻度でデータがスキャンされますか？

データの最初のスキャンには少し時間がかかることがありますが、その後のスキャンでは増分変更のみが検査されるため、システムスキャン時間が短縮されます。BlueXPの分類では、データがラウンドロビン方式で継続的にスキャンされ、一度に6つのリポジトリがスキャンされるため、変更されたすべてのデータが非常に迅速に分類されます。

"スキャンの仕組みを説明します"。

BlueXPの分類では、データベースが1日に1回しかスキャンされません。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。

データスキャンは、ストレージシステムとデータにほとんど影響を与えません。ただし、影響がごくわずかであっても問題が発生する場合は、「低速」スキャンを実行するようにBlueXPの分類を設定できます。 "スキャン速度を下げる方法を参照してください"。

BlueXPの分類を使用してデータを検索できますか。

BlueXPは、幅広い検索機能を備えており、接続されているすべてのソースから特定のファイルやデータを簡単に検索できます。BlueXPの分類機能を使用すると、メタデータに反映される情報よりも詳細な情報を検索できます。言語に依存しないサービスで、ファイルを読み取ったり、名前やIDなどの機密データの種類を多数分析したりすることもできます。たとえば、構造化データストアと非構造化データストアの両方を検索して、企業ポリシーに違反してデータベースからユーザファイルに漏れた可能性のあるデータを見つけることができます。検索は後で保存できます。ポリシーを作成して、設定した頻度で結果を検索してアクションを実行できます。

対象となるファイルが見つかったら、タグ、作業環境アカウント、バケット、ファイルパス、 カテゴリ（分類から）、ファイルサイズ、最終変更、権限ステータス、重複、 感度レベル、個人データ、ファイル内の機密データタイプ、所有者、ファイルタイプ、ファイルサイズ、作成時刻、 ファイルハッシュ、注意を求めているユーザーにデータが割り当てられたかどうかなど。フィルタを適用して、適切でないスクリーンアウト特性を適用できます。BlueXPの分類では、適切な権限があればファイルの移動や削除を許可するRBACも用意されています。適切な権限がない場合は、適切な権限を持つ組織内のユーザーにタスクを割り当てることができます。

BlueXPの分類では、どのような種類の分析が可能ですか？

データソースを視覚的に表現したり、リレーションシップを定義して視覚的に表現したりできます。たとえば、企業内のすべてのデータソース（オンプレミスのシステム、データベース、ファイル共有、S3ストア、OneDrive、 など）。データのコピー、移動、削除、管理が可能になり、ストレージコストを最適化してリスクを軽減できます。ユーザは、どのような機密データが公開されるかを確認することでリスクを軽減でき、強力なデータ保護を実現するための権限を管理するジョブを作成できます。BlueXPの分類では、すべてのタイプのデータも分類されるため、管理者はデータをタイプ別に調査し、そのデータに対してどのようなアクションが実行されたか、いつ実行されたかを確認できます。

BlueXPの分類ではレポートが提供されますか？

はい。BlueXPの分類によって提供される情報は、組織内の他の関係者に関連性があるため、レポートを生成して分析情報を共有できます。BlueXPの分類で使用できるレポートは次のとおりです。

プライバシーリスクアセスメントレポート

データからプライバシーに関する情報を収集し、プライバシーリスクスコアを取得します。 "詳細はこちら。"。

Data Subject Access Request レポート

データ主体の特定の名前または個人IDに関する情報を含むすべてのファイルのレポートを抽出できます "詳細はこちら。"。

PCI DSS レポート

クレジットカード情報のファイルへの配布を識別するのに役立ちます。 "詳細はこちら。"。

HIPAA レポート

健常性情報がファイルにどのように分散されているかを確認できます。 "詳細はこちら。"。

データマッピングレポート

作業環境内のファイルのサイズと数について説明します。これには、使用容量、データの経過時間、データのサイズ、ファイルタイプが含まれます。 "詳細はこちら。"。

Data Discovery Assessmentレポート

スキャンされた環境の高度な分析を行い、システムの調査結果を強調し、懸念すべき領域と潜在的な修復手順を示します。 "学習モード"。

特定の情報タイプに関するレポート

個人データや機密性の高い個人データを含む、特定されたファイルの詳細を含むレポートを利用できます。カテゴリおよびファイルタイプ別に分類されたファイルを表示することもできます。 "詳細はこちら。"。

スキャンのパフォーマンスは変化しますか？

スキャンのパフォーマンスは、環境内のネットワーク帯域幅と平均ファイルサイズによって異なります。また、（クラウドまたはオンプレミスの）ホストシステムのサイズ特性にも左右されます。を参照してください "BlueXP分類インスタンス" および "BlueXP分類の導入" を参照してください。

新しいデータソースを最初に追加するときに、「分類」のフルスキャンではなく「マッピング」スキャンのみを実行するように選択することもできます。データソースでは、ファイルにアクセスしてデータを参照できないため、マッピングは短時間で完了します。 "マッピングスキャンと分類スキャンの違いを参照してください"。

BlueXPの分類管理とプライバシー

ここでは、BlueXPの分類とプライバシー設定の管理方法について説明します。

BlueXPの分類を有効にする方法を教えてください。

まず、BlueXP分類のインスタンスをBlueXPまたはオンプレミスシステムに導入する必要があります。インスタンスが実行されると、*[設定]*タブから、または特定の作業環境を選択して、既存の作業環境、データベース、およびその他のデータソースに対してサービスを有効にできます。

"開始方法をご確認ください"。

> データソースでBlueXPの分類をアクティブ化すると、すぐに初回スキャンが実行されます。スキャン結果はすぐ後に表示されます。

BlueXPの分類を無効にする方法を教えてください。

BlueXPの分類設定ページでは、個 々 の作業環境、データベース、ファイル共有グループ、OneDriveアカウント、またはSharePointアカウントをスキャンして、BlueXPの分類を無効にすることができます。

"詳細はこちら。"。

> BlueXP分類インスタンスを完全に削除するには、クラウドプロバイダのポータルまたはオンプレミスの場所からBlueXP分類インスタンスを手動で削除します。

組織のニーズに合わせてサービスをカスタマイズできますか。

BlueXPは分類されているため、すぐに使用できる分析情報をデータに提供します。これらの分析情報を抽出して、組織のニーズに活用できます。

さらに、BlueXPの分類では、BlueXPの分類によってスキャンで識別される「個人データ」のカスタムリストを追加することができます。これにより、機密性の高いデータが_all_組織のファイル内のどこにあるかを全体的に把握できます。

- スキャンするデータベースの特定の列に基づいて一意の識別子を追加できます。この* Data Fusion *を呼び出します。
- テキストファイルからカスタムキーワードを追加できます。
- カスタムパターンは、正規表現（regex）を使用して追加できます。

"詳細はこちら。"。

特定のディレクトリのスキャンデータを除外するようにサービスに指示することはできますか**?**

はい。BlueXPの分類で、特定のデータソースディレクトリにあるスキャンデータを除外するには、そのリストを分類エンジンに指定します。この変更を適用すると、BlueXPの分類によって、指定したディレクトリ内のスキャンデータが除外されます。

"詳細はこちら。"。

ONTAPボリュームにある**Snapshot**コピーはスキャンされますか？

いいえBlueXPの分類ではSnapshotはスキャンされません。これは、コンテンツがボリューム内のコンテンツと同じであるためです。

ONTAP ボリュームでデータ階層化が有効になっている場合、どうなりますか？

BlueXPの分類では、コールドデータがオブジェクトストレージに階層化されたボリュームをスキャンするときに、ローカルディスクにあるデータとオブジェクトストレージに階層化されたコールドデータのすべてのデータがスキャンされます。これは、階層化を実装する他社製品にも当てはまります。

スキャンによってコールドデータが加熱されることはなく、コールドデータはオブジェクトストレージに残ります。

BlueXPの分類から組織に通知を送信できますか？

はい。ポリシー機能と組み合わせることで、BlueXPユーザー(毎日、毎週、または毎月)、またはポリシーが結

果を返したときに電子メールアラートを送信して、データを保護するための通知を受け取ることができます。の詳細を確認してください "ポリシー"。

また、 [ガバナンス] ページと [調査] ページからステータスレポートをダウンロードして、組織内で共有することもできます。

BlueXPの分類は、ファイルに埋め込まれた**AIP**ラベルでも機能しますか？

はい。サブスクライブ済みの場合は、BlueXP分類でスキャンするファイルでAIPラベルを管理できます "Azure 情報保護（ AIP ）"。既にファイルに割り当てられているラベルを表示したり、ファイルにラベルを追加したり、既存のラベルを変更したりできます。

"詳細はこちら。"。

ソースシステムとデータタイプのタイプ

スキャン可能なストレージのタイプ、およびスキャンするデータのタイプに関連する情報を次に示します。

BlueXPでは、どのようなデータソースをスキャンできますか？

BlueXPの分類では、BlueXP Canvasに追加した作業環境や、BlueXPの分類がネットワーク経由でアクセスできるさまざまな種類の構造化/非構造化データソースのデータをスキャンできます。

- 作業環境： *
- Cloud Volumes ONTAP （ AWS 、 Azure 、 GCP に導入）
- オンプレミスの ONTAP クラスタ
- Azure NetApp Files の特長
- ONTAP 対応の Amazon FSX
- Amazon S3
- データソース： *
- ネットアップ以外のファイル共有
- オブジェクトストレージ（ S3 プロトコルを使用）
- データベース（Amazon RDS、MongoDB、MySQL、Oracle、PostgreSQL、 SAP HANA、SQL Serverなど）
- OneDrive アカウント
- SharePoint Onlineアカウントとオンプレミスアカウント
- Googleドライブアカウント

BlueXPの分類では、NFSバージョン3.xとCIFSバージョン1.x、2.0、2.1、3.0がサポートされます。

政府機関に導入した場合、制限はありますか？

BlueXPの分類は、コネクタが政府機関のリージョン（AWS GovCloud、Azure Gov、Azure DoD）（「制限モード」とも呼ばれます）に導入されている場合にサポートされます。この方法で導入した場合、BlueXPには次の制限があります。

- OneDriveアカウント、SharePointアカウント、Googleドライブアカウントはスキャンできません。
- Microsoft Azure Information Protection（AIP）ラベル機能を統合できません。

インターネットにアクセスできないサイトに**BlueXP**分類をインストールすると、どのようなデータソースをスキャンできますか？

BlueXPの分類では、オンプレミスサイトのローカルなデータソースのデータのみをスキャンできます。この時点で、BlueXPの分類では、「プライベートモード」（「ダーク」サイトとも呼ばれます）で次のローカルデータソースをスキャンできます。

- オンプレミスの ONTAP システム
- データベーススキーマ
- SharePointオンプレミスアカウント(SharePoint Server)
- ネットアップ以外の NFS または CIFS ファイル共有
- Simple Storage Service （ S3 ）プロトコルを使用するオブジェクトストレージ

サポートされているファイルタイプはどれですか。

BlueXPの分類は、すべてのファイルをスキャンしてカテゴリやメタデータの分析情報を取得し、ダッシュボードの[File Types]セクションにすべてのファイルタイプを表示します。

BlueXPの分類でPersonal Identifiable Information（PII）が検出された場合、またはDSAR検索が実行された場合、サポートされるファイル形式は次のとおりです。

「+.csv」、「.dcm」、「.dom」、「.DOC」、「.DOCX」、 .json、.pdf、.PPTX、.rtf、.TXT、 .XLS、.xlsx、Docs、Sheets、Slides +`

BlueXPの分類では、どのような種類のデータやメタデータがキャプチャされますか？

BlueXPの分類を使用すると、一般的な「マッピング」スキャンまたは完全な「分類」スキャンをデータソースに対して実行できます。マッピングではデータの概要のみが示され、分類ではデータの詳細なスキャンが提供されます。データソースでは、ファイルにアクセスしてデータを参照できないため、マッピングは短時間で完了します。

- データマッピングスキャン：

  BlueXPの分類では、メタデータのみがスキャンされます。これは、全体的なデータ管理とガバナンス、プロジェクトの迅速な範囲設定、非常に大規模な環境、優先順位付けに役立ちます。データマッピングはメタデータに基づいており、*高速*スキャンとみなされます。

  高速スキャンの後、データマッピングレポートを生成できます。このレポートは、企業データソースに保存されているデータの概要を示しており、リソースの使用率、移行、バックアップ、セキュリティ、コンプライアンスの各プロセスに関する決定に役立ちます。

- データ分類（ディープ）スキャン。

  BlueXPの分類では、環境全体で標準プロトコルと読み取り専用権限を使用してスキャンが実行されます。一部のファイルは、ビジネスに関連する機密データ、プライベート情報、ランサムウェアに関連する問題の有無をチェックして開きます。

フルスキャン後は、[Data Investigation]ページでのデータの表示と絞り込み、ファイル内の名前の検索、ソースファイルのコピー、移動、削除など、データに適用できるBlueXPの分類機能が多数用意されています。

BlueXPの分類では、ファイル名、権限、作成日時、最終アクセス、最終変更日時などのメタデータがキャプチャされます。これには、[Data Investigation Details]ページおよび[Data Investigation Reports]に表示されるすべてのメタデータが含まれます。

BlueXPの分類では、個人データや機密性の高い個人データなど、さまざまなタイプのプライベートデータを特定できます。プライベートデータの詳細については、を参照してください。 "BlueXPの分類でスキャンされるプライベートデータのカテゴリ"。

BlueXPの分類情報を特定のユーザに限定できますか。

はい。BlueXPはBlueXPに完全に統合されています。BlueXPユーザーは'ワークスペース権限に応じて表示可能な作業環境の情報のみを表示できます

また、BlueXPの分類設定を管理せずに、特定のユーザにBlueXPの分類スキャン結果だけを表示させる場合は、それらのユーザにCloud Compliance Viewerロールを割り当てることができます。

"詳細はこちら。"。

ブラウザと**BlueXP**の分類の間で送信されたプライベートデータに誰でもアクセスできますか？

いいえブラウザとBlueXP分類インスタンスの間で送信されるプライベートデータは、TLS 1.2を使用したエンドツーエンドの暗号化で保護されます。つまり、NetAppやサードパーティはデータを読み取ることができません。BlueXPの分類では、アクセスをリクエストして承認しないかぎり、ネットアップとデータや結果が共有されることはありません。

スキャンされたデータは環境内に保持されます。

機密データはどのように処理されますか？

NetAppは機密データにアクセスできず、UIに表示されません。機密データはマスクされます。たとえば、クレジットカード情報用に最後の4つの数字が表示されます。

データはどこに保存されていますか？

スキャン結果は、BlueXP分類インスタンス内のElasticsearchに保存されます。

データへのアクセス方法

BlueXPの分類では、Elasticsearchに格納されたデータにAPI呼び出しを通じてアクセスします。API呼び出しは認証を必要とし、AES-128を使用して暗号化されます。Elasticsearchに直接アクセスするにはrootアクセスが必要です。

ライセンスとコスト

ここでは、BlueXPを使用するためのライセンスとコストについて説明します。

BlueXPの分類にはどれくらいのコストがかかりますか？

BlueXPの分類を使用するコストは、スキャンするデータの量によって異なります。BlueXPワークスペースでBlueXPの分類によってスキャンされる最初の1TBのデータは30日間無料です。いずれかの制限に達すると、データのスキャンを続行するために次のいずれかが必要になります。

- クラウドプロバイダからのBlueXP Marketplaceへのサブスクリプション、または
- ネットアップが提供するお客様所有のライセンス（BYOL）

を参照してください "価格設定" を参照してください。

BYOLの容量制限に達した場合はどうなりますか？

BYOLの容量が上限に達すると、BlueXPの分類は引き続き実行されますが、ダッシュボードへのアクセスはブロックされるため、スキャンしたデータに関する情報を表示できません。スキャンするボリューム数を減らして容量の使用率をライセンスの上限まで下げる場合は、設定ページのみが表示されます。BlueXPの分類にフルアクセスできるようにするには、BYOLライセンスを更新する必要があります。

コネクタの展開

次の質問は、BlueXPコネクタに関連しています。

コネクタは何ですか？

Connectorは、クラウドアカウントまたはオンプレミスのいずれかのコンピューティングインスタンス上で実行されるソフトウェアで、BlueXPでクラウドリソースを安全に管理できます。BlueXP分類を使用するには、コネクタを導入する必要があります。

コネクタはどこに取り付ける必要がありますか？

- AWS 、 Amazon FSX for ONTAP 、または AWS S3 バケット内の Cloud Volumes ONTAP のデータをスキャンするときは、 AWS のコネクタを使用します。
- Azure または Azure NetApp Files で Cloud Volumes ONTAP 内のデータをスキャンする場合は、 Azure のコネクタを使用します。
- GCP の Cloud Volumes ONTAP でデータをスキャンする場合は、 GCP のコネクタを使用します。
- オンプレミスのONTAP システム、ネットアップ以外のファイル共有、汎用のS3オブジェクトストレージ、データベース、OneDriveフォルダ、SharePointアカウント、Google Driveアカウント内のデータをスキャンする場合、これらのクラウド環境ではコネクタを使用できます。

そのため、これらの場所の多くにデータがある場合は、を使用する必要があります "複数のコネクタ"。

BlueXPの分類ではクレデンシャルへのアクセスが必要ですか？

BlueXPの分類自体はストレージクレデンシャルを取得しません。代わりに、BlueXPコネクタ内に格納されます。

BlueXPはデータプレーンのクレデンシャル（CIFSクレデンシャルなど）を使用して共有をマウントしてからスキャンを実行します。

コネクタを自分のホストに導入できますか。

はい。可能です "コネクタをオンプレミスに導入" ネットワーク内のLinuxホストまたはクラウド内のホスト。BlueXP分類をオンプレミスに導入する予定の場合は、コネクタもオンプレミスにインストールすることを推奨しますが、必須ではありません。

サービスとコネクタ間の通信に**HTTP**が使用されていますか？

はい。BlueXPはHTTPを使用してBlueXPコネクタと通信します。

インターネットにアクセスできないセキュアなサイトはどうでしょうか。

はい、サポートされています。可能です "インターネットにアクセスできないオンプレミスのLinuxホストにコネクタを導入します"。 "これは「プライベートモード」とも呼ばれます。"。その後、オンプレミスのONTAPクラスタとその他のローカルデータソースを検出し、BlueXPの分類を使用してデータをスキャンできます。

BlueXPクラシフィケーション環境

ここでは、個別のBlueXP分類インスタンスに関連する質問を示します。

BlueXPの分類では、どのような導入モデルがサポートされますか？

BlueXPを使用すると、オンプレミス、クラウド、ハイブリッド環境など、ほぼすべての場所でシステムのスキャンとレポートを実行できます。BlueXPは通常、SaaSモデルを使用して導入されます。このモデルでは、BlueXPインターフェイスを介してサービスが有効になり、ハードウェアやソフトウェアのインストールは必要ありません。このクリックアンドランの導入モードであっても、データストアがオンプレミスとパブリッククラウドのどちらにあるかに関係なく、データ管理を実行できます。

BlueXPの分類には、どのようなタイプのインスタンスや**VM**が必要ですか？

いつ "クラウドに導入"：

- AWSでは、BlueXPの分類は、500GiBのgp2ディスクを含むm6i.4xlargeインスタンスで実行されます。導入時に小さいインスタンスタイプを選択できます。
- Azureでは、BlueXPの分類は、ディスクが500GiBのStandard_D16s_v3 VMで実行されます。
- GCPでは、BlueXPの分類は、500GiB Standard永続ディスクを搭載したn2-standard-16 VMで実行されます。

CPUとRAMの数が少ないシステムにBlueXPの分類を導入できますが、これらのシステムを使用する場合は制限があります。を参照してください "小さいインスタンスタイプを使用しています" を参照してください。

"BlueXPの分類の仕組みについて詳しくは、こちらをご覧ください"。

BlueXP分類を独自のホストに導入できますか。

はい。ネットワークまたはクラウドでインターネットにアクセスできるLinuxホストにBlueXP分類ソフトウェアをインストールできます。すべてが同じように動作し、BlueXPを使用してスキャン設定と結果を引き続き管理できます。を参照してください "BlueXPの分類をオンプレミスに導入" を参照してください。

インターネットにアクセスできないセキュアなサイトはどうでしょうか。

はい、サポートされています。可能です "インターネットにアクセスできないオンプレミスサイトにBlueXPを分類して導入します" 完全にセキュアなサイトに。

BlueXP分類を使用

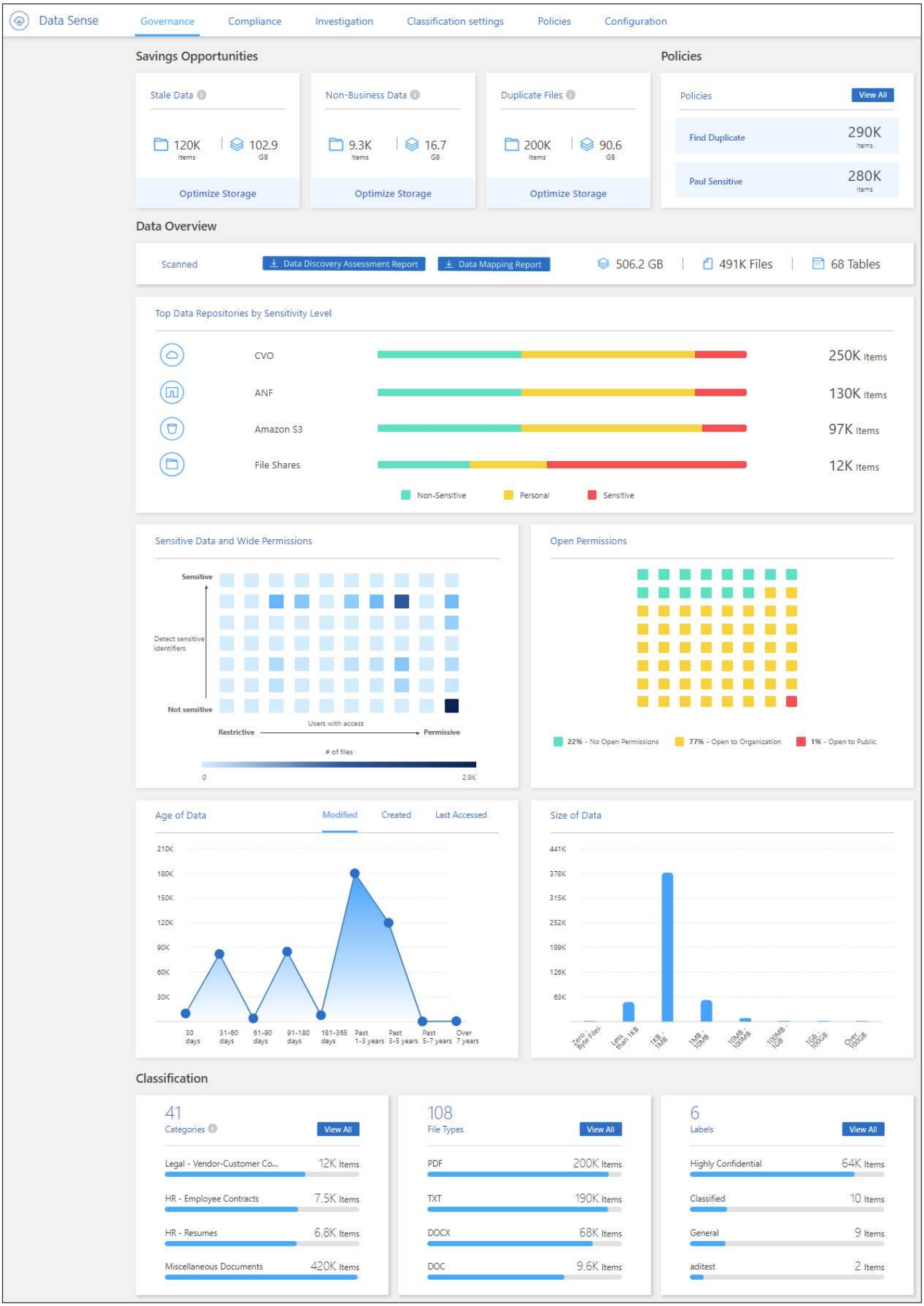
組織に保存されているデータに関するガバナンスの詳細を表示する

組織のストレージリソース上のデータに関連するコストを管理できます。BlueXPは分類されるため、システム内の古いデータ、ビジネス以外のデータ、重複ファイル、大容量ファイルの量が特定されるため、一部のファイルを削除するか、低コストのオブジェクトストレージに階層化するかを判断できます。

さらに、オンプレミスの場所からクラウドにデータを移行する予定の場合は、データのサイズと、データを移動する前に機密情報が含まれているかどうかを確認できます。

Governance ダッシュボード

Governance ダッシュボードには情報が表示されるため、ストレージリソースに保存されているデータの効率性を高め、コストを管理できます。


Data Sense
Governance
Compliance
Investigation
Classification settings
Policies
Configuration
Savings Opportunities
Stale Data
120K Items
102.9 GB
Optimize Storage
Non-Business Data
9.3K Items
16.7 GB
Optimize Storage
Duplicate Files
200K Items
90.6 GB
Optimize Storage
Policies
Policies
View All
Find Duplicate 290K Items
Paul Sensitive 280K Items
Data Overview
Scanned
Data Discovery Assessment Report
Data Mapping Report
506.2 GB
491K Files
68 Tables
Top Data Repositories by Sensitivity Level
CVO 250K Items
ANF 130K Items
Amazon S3 97K Items
File Shares 12K Items
Non-Sensitive
Personal
Sensitive
Sensitive Data and Wide Permissions
Sensitive
Detect sensitive identifiers
Not sensitive
Users with access
Restrictive
Permissive
# of files
0
2.9K
Open Permissions
22% - No Open Permissions
77% - Open to Organization
1% - Open to Public
Age of Data
Modified
Created
Last Accessed
210K
180K
150K
120K
90K
60K
30K
30 days
31-60 days
61-90 days
91-180 days
181-365 days
Past 1-3 years
Past 3-5 years
Past 5-7 years
Over 7 years
Size of Data
441K
378K
315K
252K
189K
126K
63K
Zero Byte Files
Less than 1KB
1KB - 1MB
1MB - 10MB
10MB - 100MB
100MB - 1GB
1GB - 10GB
Over 10GB
Classification
41
Categories
View All
Legal - Vendor-Customer Co... 12K Items
HR - Employee Contracts 7.5K Items
HR - Resumes 6.8K Items
Miscellaneous Documents 420K Items
108
File Types
View All
PDF 200K Items
TXT 190K Items
DOCX 68K Items
DOC 9.6K Items
6
Labels
View All
Highly Confidential 64K Items
Classified 10 Items
General 9 Items
aditest 2 Items

機会の節約

_Saving Opportunities 領域内の項目を調査して、削除または階層化してより安価なオブジェクトストレージにする必要があるデータがないかどうかを確認できます。各項目をクリックすると、 ［ 調査 ］ ページにフィルタリングされた結果が表示されます。

- **Stale Data**- 3 年前に最後に変更されたデータ。
- * ビジネス以外のデータ * - カテゴリまたはファイルタイプに基づいて、ビジネスに関連していないと見なされるデータ。これには、次のもの
  - アプリケーションデータ
  - 音声
  - 実行可能ファイル
  - イメージ
  - ログ
  - ビデオ
  - その他（一般的な「その他」カテゴリ）
- * 重複ファイル * - スキャンしているデータソース内の他の場所に複製されているファイル。 "表示される重複ファイルの種類を確認します"。

  注

  いずれかのデータソースでデータ階層化が実装されている場合は、オブジェクトストレージにすでに存在する古いデータを_Stale Data_categoryで特定できます。

検索結果が最も多いポリシーです

[_Policies]領域では、結果の数が最も多いポリシーがリストの先頭に表示されます。[調査]ページに結果を表示するには、ポリシーの名前をクリックします。[すべて表示 *] をクリックして、使用可能なすべてのポリシーのリストを表示します。

をクリックします "こちらをご覧ください" ポリシーの詳細については、を参照してください。

データの概要

Data Overview_Sectionには、スキャンされるすべてのデータの概要が表示されます。ボタンをクリックして、使用容量、経過時間、データサイズ、すべての作業環境およびデータソースのファイルタイプを含むデータマッピングレポートをダウンロードします。を参照してください データマッピングレポート 詳細については、を参照してください。

データの機密性に基づいて上位のデータリポジトリが表示されます

_Top Data Repositories by Sensitivity Level_領域には、最も機密性の高い項目を含む上位4つのデータリポジトリ（作業環境およびデータソース）が表示されます。各作業環境の棒グラフは、次のように分割されています。

- 機密性のないデータ
- 個人データ

- 機密性の高い個人データ

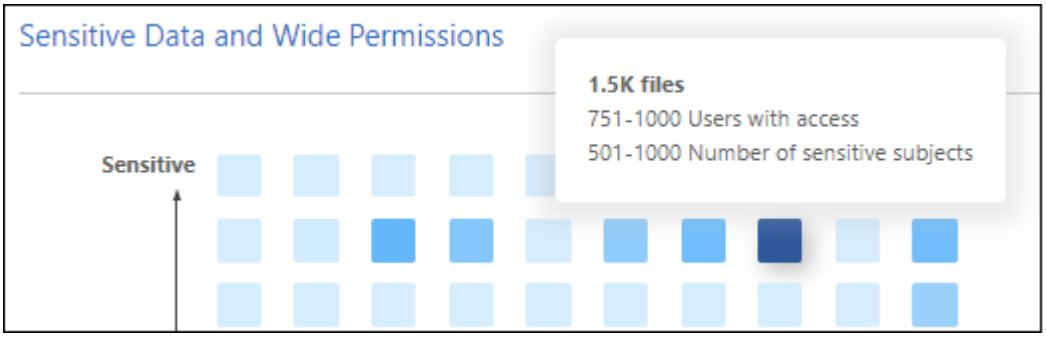
各セクションにカーソルを合わせると、各カテゴリの項目の総数を確認できます。

各領域をクリックすると、 [調査] ページにフィルタリングされた結果が表示され、詳細を調査できます。

機密性と幅広い権限に基づいてリストされたデータ

_Sensitive DataおよびWide Permissions_領域には、機密データ（機密性の高い個人データと機密性の高い個人データの両方を含む）が含まれ、過度に許容されるファイルのヒートマップが表示されます。これにより、機密データを含むリスクがある場所を確認できます。

ファイルは、X軸（最小から最大）上のファイルへのアクセス権を持つユーザの数、およびY軸（最小から最大）上のファイル内の機密識別子の数に基づいて評価されます。ブロックは、X軸とY軸のアイテムに一致するファイルの数を表します。明るい色のブロックは適切で、ファイルにアクセスできるユーザーが少なく、ファイルごとの機密識別子が少なくなります。濃いブロックは、調査する項目です。たとえば、下の画面には、濃い青色のブロックのマウスオーバーテキストが表示されます。751-100ユーザがアクセスできるファイルが1、500個あり、ファイルごとに501-100の機密識別子があることが示されています。



[調査]ページで、影響を受けるファイルのフィルタリングされた結果を表示するには、対象となるブロックをクリックします。これにより、詳細な調査が可能になります。

アイデンティティサービスをBlueXP分類に統合していない場合、このパネルにデータは表示されません。"Active DirectoryサービスとBlueXPの分類を統合する方法をご紹介します"。

> このパネルでは、CIFS共有、OneDrive、SharePointのデータソースのファイルをサポートしています。現在、データベース、Googleドライブ、Amazon S3、汎用オブジェクトストレージはサポートされていません。

オープンアクセス権のタイプ別に一覧表示されるデータ

Open Permissions 領域には、スキャンされるすべてのファイルに存在する各タイプの権限の割合が表示されます。このチャートには、次の種類の権限が表示されます。

- オープンアクセス権がありません
- 組織に開く（ Open to Organization ）
- [パブリック] に移動します
- 不明なアクセスです

各セクションにカーソルを合わせると、各カテゴリのファイルの総数が表示されます。各領域をクリックする

と、 [調査] ページにフィルタリングされた結果が表示され、詳細を調査できます。

データの経過時間とデータのサイズのグラフ

_Age および _Size_Graphs の項目を調査して、削除または階層化してコストの低いオブジェクトストレージにする必要のあるデータがないかどうかを確認することができます。

グラフの特定のポイントにカーソルを合わせると、そのカテゴリのデータの経過時間やサイズの詳細を確認できます。クリックすると、その年齢またはサイズの範囲でフィルタされたすべてのファイルが表示されます。

- *Age of Data グラフ *- データが作成された時刻、アクセスされた最終時刻、またはデータが変更された最終時刻に基づいてデータを分類します。
- * データサイズグラフ * - サイズに基づいてデータを分類します。

注

いずれかのデータソースでデータ階層化が実装されている場合は、オブジェクトストレージにすでに存在する古いデータをData_graphの_Ageで特定できます。

最も識別されているデータ分類

_Classification_area には ' 最も識別されたリストが表示されます "カテゴリ"、 "ファイルの種類"および "AIP ラベル" をスキャンしたデータに保存します。

カテゴリ

カテゴリを使用すると、保有している情報の種類を表示して、データの状況を把握することができます。たとえば、「履歴書」や「従業員契約書」などのカテゴリには機密データを含めることができます。結果を調査すると、従業員契約が安全でない場所に保存されていることがわかります。その後、その問題を修正できます。

を参照してください "カテゴリ別にファイルを表示します" を参照してください。

ファイルの種類

ファイルタイプを確認すると、特定のファイルタイプが正しく保存されない可能性があるため、機密データを制御するのに役立ちます。

を参照してください "ファイルタイプを表示しています" を参照してください。

AIP ラベル

Azure Information Protection （ AIP ）に加入している場合は、コンテンツにラベルを適用することで、ドキュメントとファイルを分類して保護できます。ファイルに割り当てられている最も使用されている AIP ラベルを確認すると、ファイルで最も使用されているラベルを確認できます。

を参照してください "AIP ラベル" を参照してください。

データマッピングレポート

データマッピングレポートには、企業データソースに保存されているデータの概要が表示され、移行、バックアップ、セキュリティ、コンプライアンスの各プロセスの決定に役立ちます。このレポートには、まずすべての作業環境とデータソースの概要が表示され、次に各作業環境の内訳が表示されます。

このレポートには次の情報が含まれます。

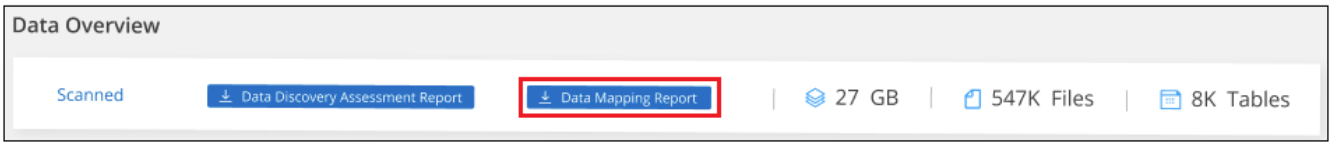
カテゴリ	説明
使用容量	すべての作業環境：各作業環境のファイル数と使用済み容量が表示されます。単一の作業環境の場合：容量が最も多いファイルが表示されます。
データの経過時間	ファイルが作成されたとき、最終変更されたとき、または最後にアクセスされたときのグラフとグラフが 3 つ表示されます。特定の日付範囲に基づいて、ファイル数とその使用済み容量が表示されます。
データのサイズ	作業環境の特定のサイズ範囲内に存在するファイルの数を示します。
ファイルの種類	作業環境に保存されているファイルタイプごとのファイルの総数と使用容量が表示されます。

データマッピングレポートの生成

このレポートは、BlueXPの[ガバナンス]タブで生成します。

手順

1. BlueXPメニューで、* Governance > Classification *をクリックします。
2. をクリックし、[データマッピングレポート]*ボタンをクリックします。



結果

BlueXPの分類によってPDFレポートが生成されます。このレポートを確認して、必要に応じて他のグループに送信できます。

レポートのサイズが1MBを超える場合は、BlueXP分類インスタンスにPDFファイルが保持され、正確な場所に関するポップアップメッセージが表示されます。BlueXP分類がオンプレミスのLinuxマシンまたはクラウドに導入したLinuxマシンにインストールされている場合は、PDFファイルに直接移動できます。BlueXP分類をクラウドに導入したら、BlueXP分類インスタンスにSSHでアクセスしてPDFファイルをダウンロードする必要があります。 "「分類インスタンスのデータにアクセスする方法」を参照してください"。

BlueXPの分類ページの上部にあるをクリックすると、レポートの最初のページに表示される会社名をカスタマイズできます ボタン"] [会社名の変更]をクリックします。次回レポートを生成するときに、新しい名前が含まれます。

Data Discovery Assessment Reportの略

Data Discovery Assessment Reportでは、スキャンされた環境の概要を分析して、システムの調査結果を強調し、懸念領域と潜在的な修復手順を示します。結果は、データのマッピングと分類の両方に基づいています。このレポートの目的は、データセットの次の3つの重要な側面についての認知度を高めることです。

フィーチャー（ **Feature** ）	説明
データガバナンスの懸念	所有しているすべてのデータと、コストを節約するためにデータ量を削減できる可能性のある領域の詳細な画像。
データセキュリティのリスク	広範なアクセス権限により、内部または外部の攻撃からデータにアクセスできる領域。
データコンプライアンスのギャップ	お客様の個人情報または機密性の高い個人情報が、セキュリティとDSAR（データ主体アクセス要求）の両方の目的で保管されている場所。

評価後、このレポートでは次のことが可能な領域を特定します。

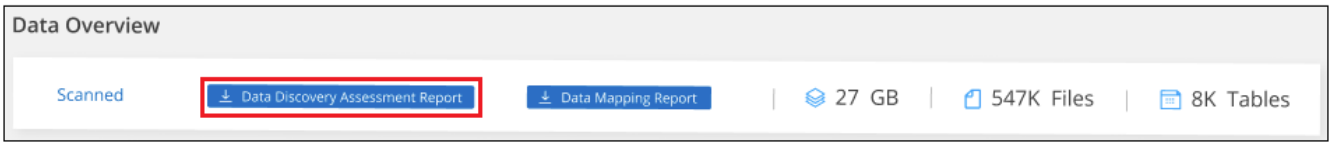
- 保持ポリシーを変更したり、特定のデータ（古いデータ、重複データ、ビジネス以外のデータ）を移動または削除したりすることで、ストレージコストを削減
- グローバルグループ管理ポリシーを改訂して、幅広い権限を持つデータを保護します
- PIIをより安全なデータストアに移動することで、個人情報または機密性の高い個人情報を含むデータを保護します

データ検出評価レポートの生成

このレポートは、BlueXPの[ガバナンス]タブで生成します。

手順

1. BlueXPメニューで、* Governance > Classification *をクリックします。
2. Governance（ガバナンス）をクリックし、 Data Discovery Assessment Report（データ検出評価レポート）*ボタンをクリックします。



結果

BlueXPの分類によってPDFレポートが生成されます。このレポートを確認して、必要に応じて他のグループに送信できます。

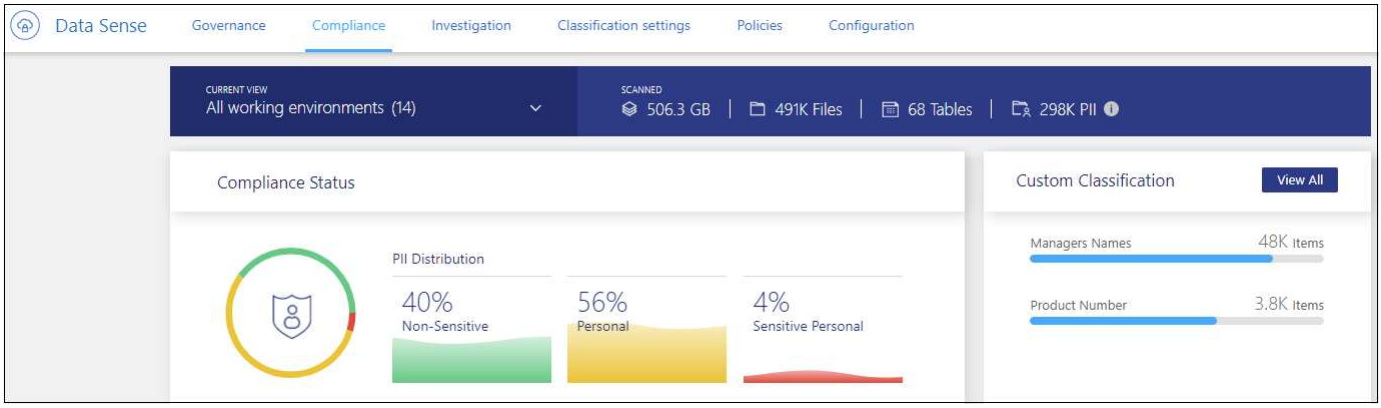
BlueXPの分類ページの上部にあるをクリックすると、レポートの最初のページに表示される会社名をカスタマイズできます ボタン"] [会社名の変更]をクリックします。次回レポートを生成するときに、新しい名前が含まれます。

組織に保存されているデータに関するコンプライアンスの詳細を表示する

組織内の個人データと機密性の高い個人データに関する詳細を表示することで、個人データを管理できます。BlueXPで分類されたデータのカテゴリやファイルタイプを確認することで、データを可視化することもできます。

このセクションで説明する機能は、データソースに対して完全な分類スキャンを実行することを選択した場合にのみ使用できます。マッピングのみのスキャンを実行したデータソースでは、ファイルレベルの詳細は表示されません。

デフォルトでは、BlueXPの分類ダッシュボードには、すべての作業環境とデータベースのコンプライアンスデータが表示されます。



一部の作業環境のデータだけを表示する場合は、 それらの作業環境を選択します。

また、 [データ調査] ページから結果をフィルタリングして、結果のレポートを CSV ファイルとしてダウンロードすることもできます。を参照してください "[データ調査 ページでデータをフィルタリングします"] を参照してください。

個人データを含むファイルを表示する

BlueXPの分類では、データ内の特定の単語、文字列、パターン（正規表現）が自動的に識別されます。たとえば、個人識別情報（ PII ）、クレジットカード番号、社会保障番号、銀行口座番号、パスワード、 その他。"すべてのリストを参照してください"。BlueXPの分類では、個 々 のファイル、ディレクトリ（共有とフォルダ）内のファイル、およびデータベーステーブルでこのような情報が識別されます。

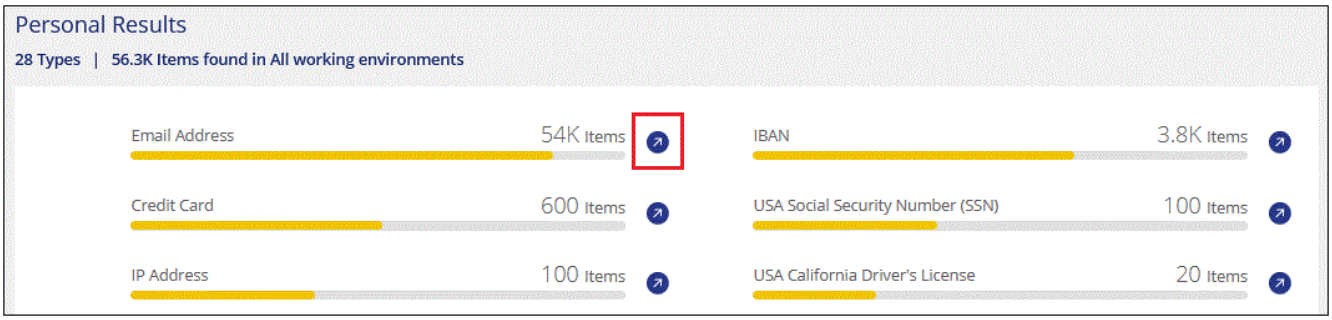
また、スキャン対象のデータベースサーバを追加した場合、 Data Fusion の機能を使用してファイルをスキャンし、データベースから一意の識別子がこれらのファイルまたは他のデータベースのいずれに存在するかを特定できます。を参照してください "Data Fusion を使用して個人データ識別子を追加する" を参照してください。

BlueXPの分類では、一部のタイプの個人データについて、*proximity validation_*を使用して検出結果が検証されます。検証は、見つかった個人データに近接した *1* つまたは複数の定義済みキーワードを検索することによって行われます。たとえば、*BlueXP*は米国を表しますソーシャルセキュリティ番号（ *SSN* ）は、 *IT* の横に近接語（ *_SSN_or_social security* など）が表示されている場合、 SSN として表示されます。 "個人データのテーブル" は、BlueXPの分類で近接検証を使用する状況を示しています。

手順

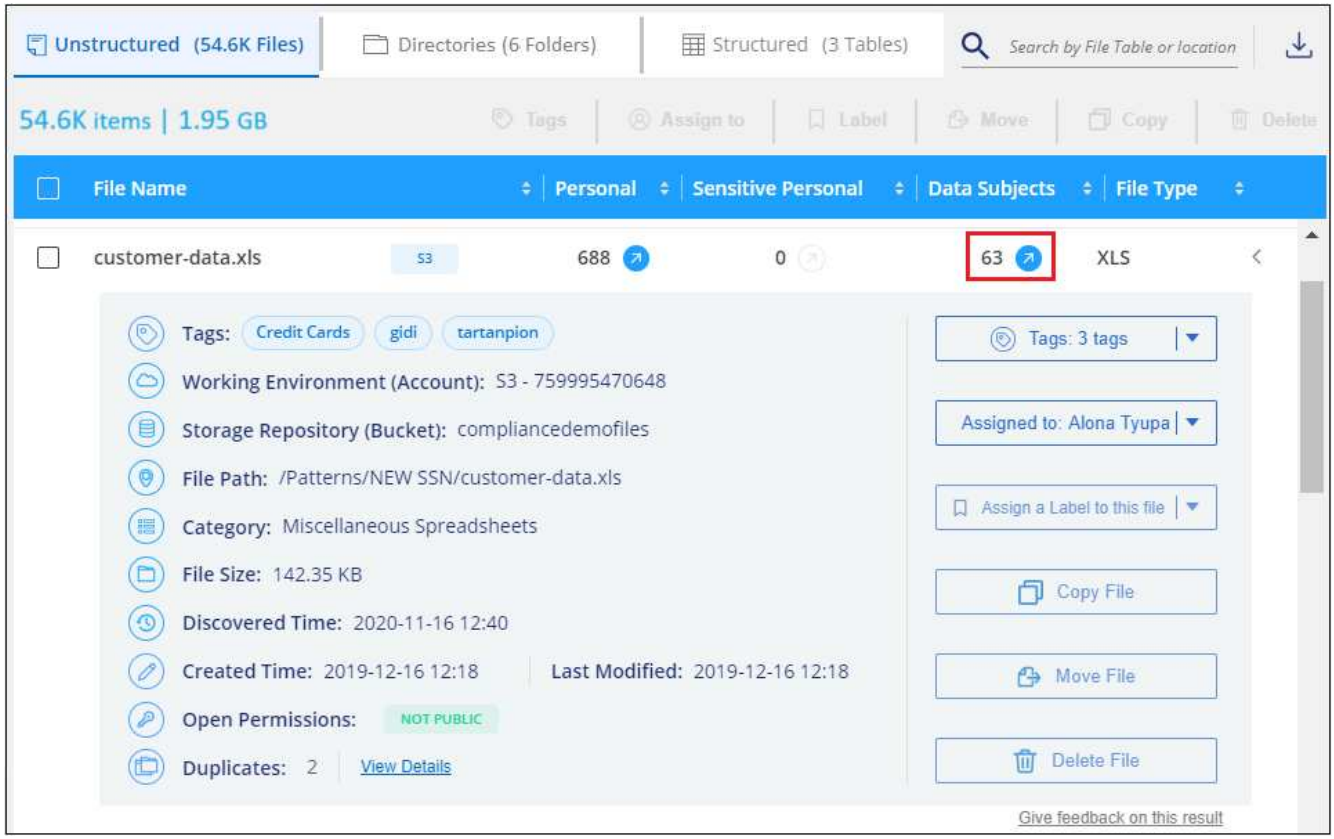
1. BlueXPの左ナビゲーションメニューで、* Governance > Classification をクリックし、 Compliance *タブをクリックします。
2. すべての個人データの詳細を調査するには、個人データの割合の横にあるアイコンをクリックします。

3. 特定の種類の個人データの詳細を調査するには、 [* すべて表示 *] をクリックしてから、特定の種類の個人データの [調査結果 *] アイコン（電子メールアドレスなど）をクリックします。

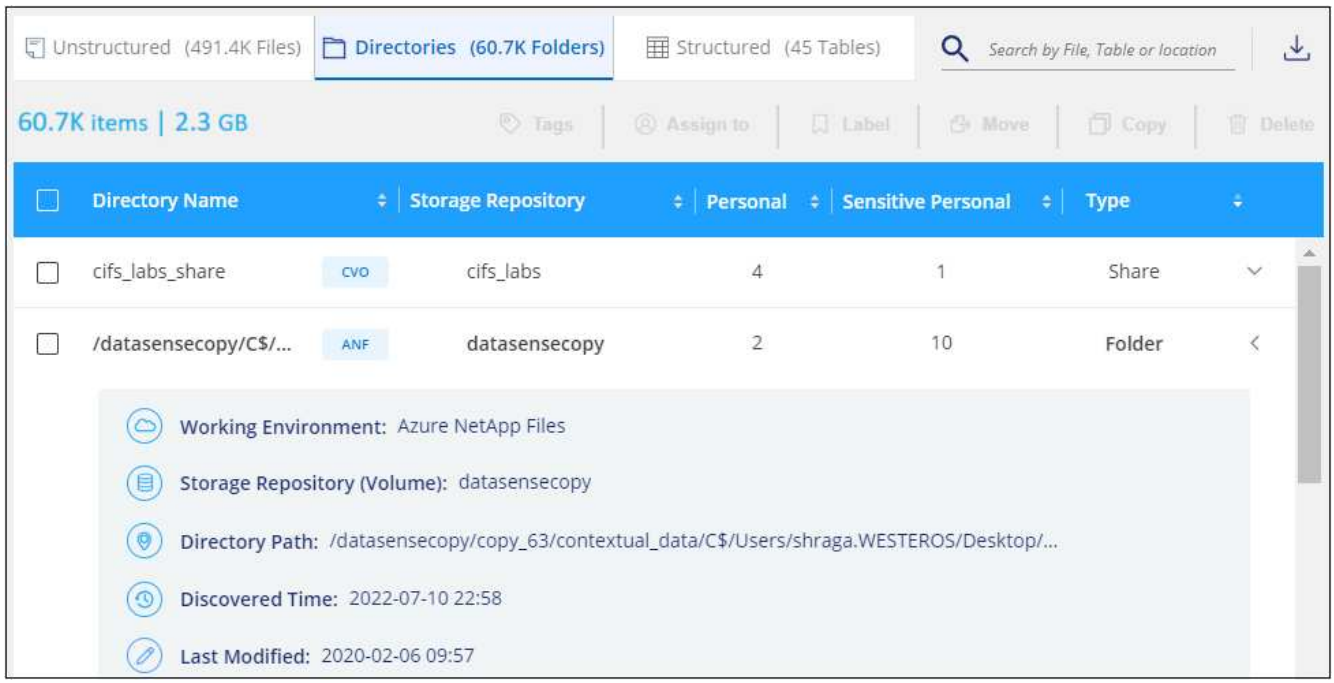


4. 特定のファイルの検索、ソート、詳細の展開、 * 調査結果 * をクリックしてマスクされた情報を表示、またはファイルリストをダウンロードして、データを調査します。

   以下の2つのスクリーンショットは、個々のファイルに保存されている個人データを示しています。これらのデータは、ディレクトリ（共有およびフォルダ）内のファイルに保存されています。[構造化*]タブを選択して、データベース内で検出された個人データを表示することもできます。



をクリックした後にファイルで見つかった詳細情報のスクリーンショット。"]



をクリックした後にディレクトリで見つかった詳細情報のスクリーンショット。"]

機密性の高い個人データを含むファイルを表示する

BlueXPは、などのプライバシー規制で定義されている特別な種類の機密個人情報を自動的に識別します "GDPR の第 9 、 10 記事"。たとえば、人の健康、民族の起源、性的指向に関する情報などです。 "すべてのリストを参照してください"。BlueXPの分類では、個 々 のファイル、ディレクトリ（共有とフォルダ）内の

ファイル、およびデータベーステーブルでこのような情報が識別されます。

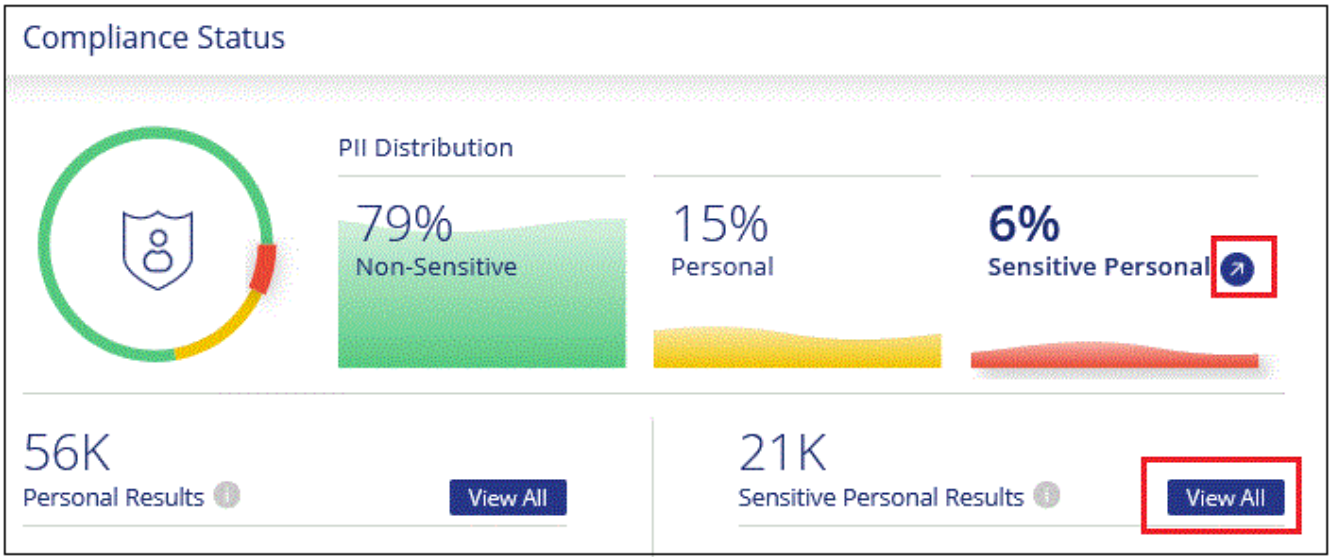
BlueXPは、人工知能（AI）、自然言語処理（NLP）、機械学習（ML）、コグニティブコンピューティング（CC）を使用してスキャンするコンテンツの意味を理解し、エンティティを抽出して適切に分類します。

たとえば、機密性の高い GDPR データカテゴリの 1 つは民族起源です。自然言語処理能力を備えたBlueXPの分類では、「George is Mexican」（GDPR第9条に規定されている機密データを示しています）と「George is Eating Mexican food」（ジョージはメキシコ料理を食べています）の違いを区別できます。

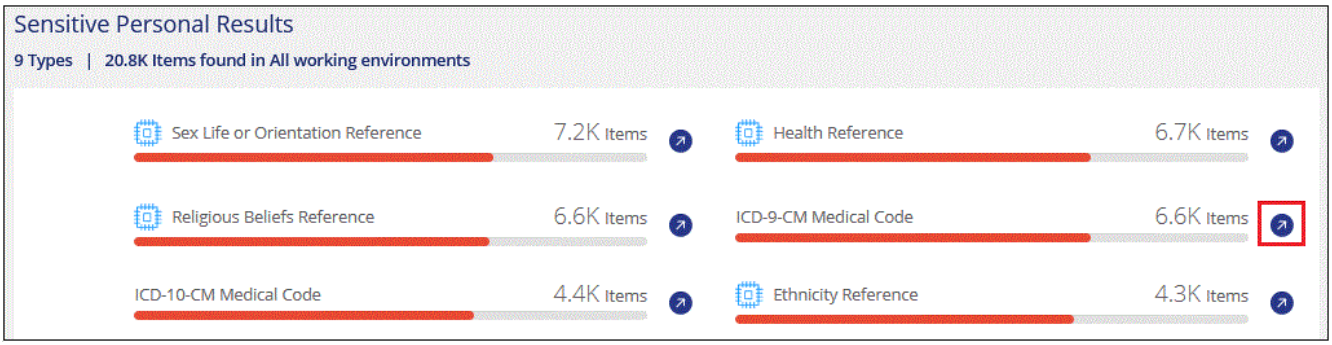
> 機密性の高い個人データをスキャンする場合は、英語のみがサポートされます。言語のサポートは、あとで追加されます。

手順

1. BlueXPの左ナビゲーションメニューで、* Governance > Classification をクリックし、 Compliance *タブをクリックします。
2. 機密性の高い個人データの詳細を調べるには、個人データの割合の横にあるアイコンをクリックします。



3. 特定のタイプの機密個人データの詳細を調べるには、 [* すべて表示 *] をクリックし、特定のタイプの機密個人データの [調査結果 *] アイコンをクリックします。



4. 特定のファイルの検索、ソート、詳細の展開、 * 調査結果 * をクリックしてマスクされた情報を表示、またはファイルリストをダウンロードして、データを調査します。

カテゴリ別にファイルを表示

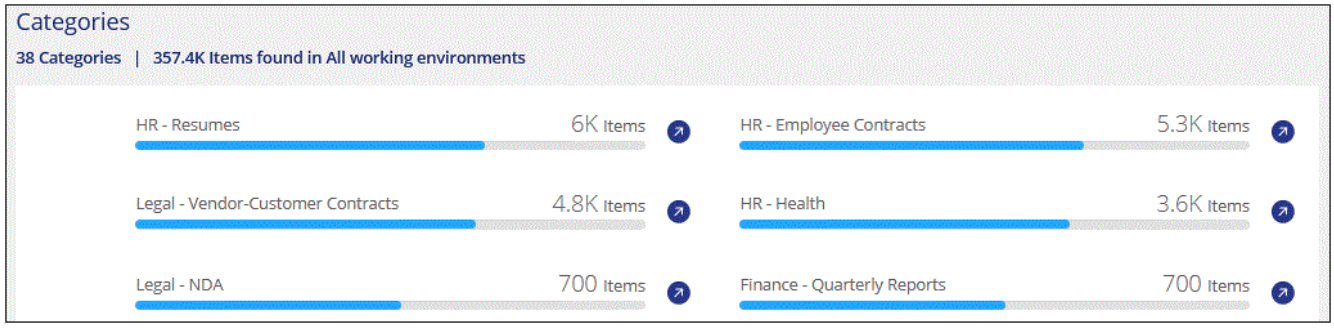
BlueXPは、スキャンしたデータをさまざまなカテゴリに分類します。カテゴリは、各ファイルのコンテンツとメタデータの AI 分析に基づくトピックです。 "カテゴリのリストを参照してください"。

カテゴリを使用すると、保有している情報の種類を表示して、データの状況を把握することができます。たとえば、履歴書や従業員契約などのカテゴリには機密データを含めることができます。結果を調査すると、従業員契約が安全でない場所に保存されていることがわかります。その後、その問題を修正できます。

> 英語、ドイツ語、およびスペイン語は、カテゴリでサポートされています。言語のサポートは、あとで追加されます。

手順

1. BlueXPの左ナビゲーションメニューで、* Governance > Classification をクリックし、 Compliance *タブをクリックします。
2. メイン画面から上位 4 つのカテゴリのいずれかの * 調査結果 * アイコンを直接クリックするか、 * すべて表示 * をクリックして、いずれかのカテゴリのアイコンをクリックします。



3. 特定のファイルの検索、ソート、詳細の展開、 * 調査結果 * をクリックしてマスクされた情報を表示、またはファイルリストをダウンロードして、データを調査します。

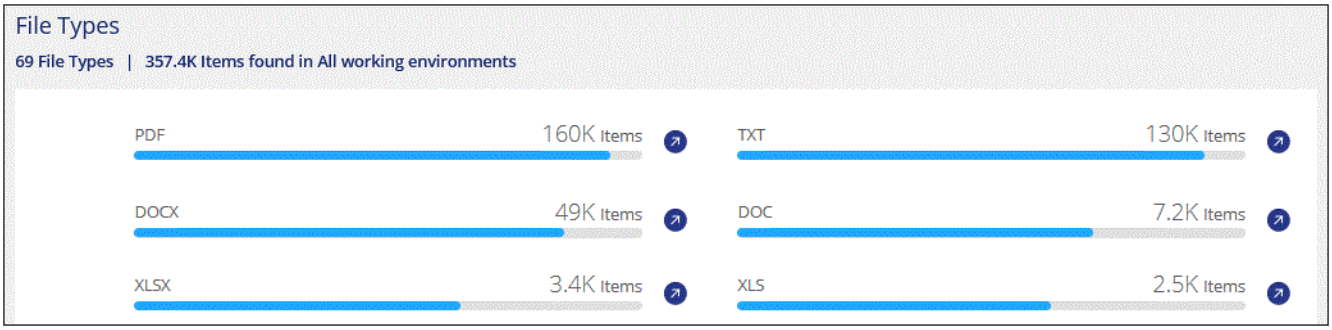
ファイルタイプ別のファイルの表示

BlueXPは、スキャンしたデータをファイルタイプ別に分類して分類します。ファイルタイプを確認すると、特定のファイルタイプが正しく保存されない可能性があるため、機密データを制御するのに役立ちます。 "ファイルタイプのリストを参照してください"。

たとえば ' 組織に関する非常に機密性の高い情報を含む CAD ファイルを保存する場合がありますセキュリティで保護されていない場合は、権限を制限するか、ファイルを別の場所に移動することで、機密データを制御できます。

手順

1. BlueXPの左ナビゲーションメニューで、* Governance > Classification をクリックし、 Compliance *タブをクリックします。
2. メイン画面で上位 4 つのファイルタイプのうちの 1 つに対応する * 調査結果 * アイコンをクリックするか、 * すべて表示 * をクリックして、任意のファイルタイプのアイコンをクリックします。



3. 特定のファイルの検索、ソート、詳細の展開、 * 調査結果 * をクリックしてマスクされた情報を表示、またはファイルリストをダウンロードして、データを調査します。

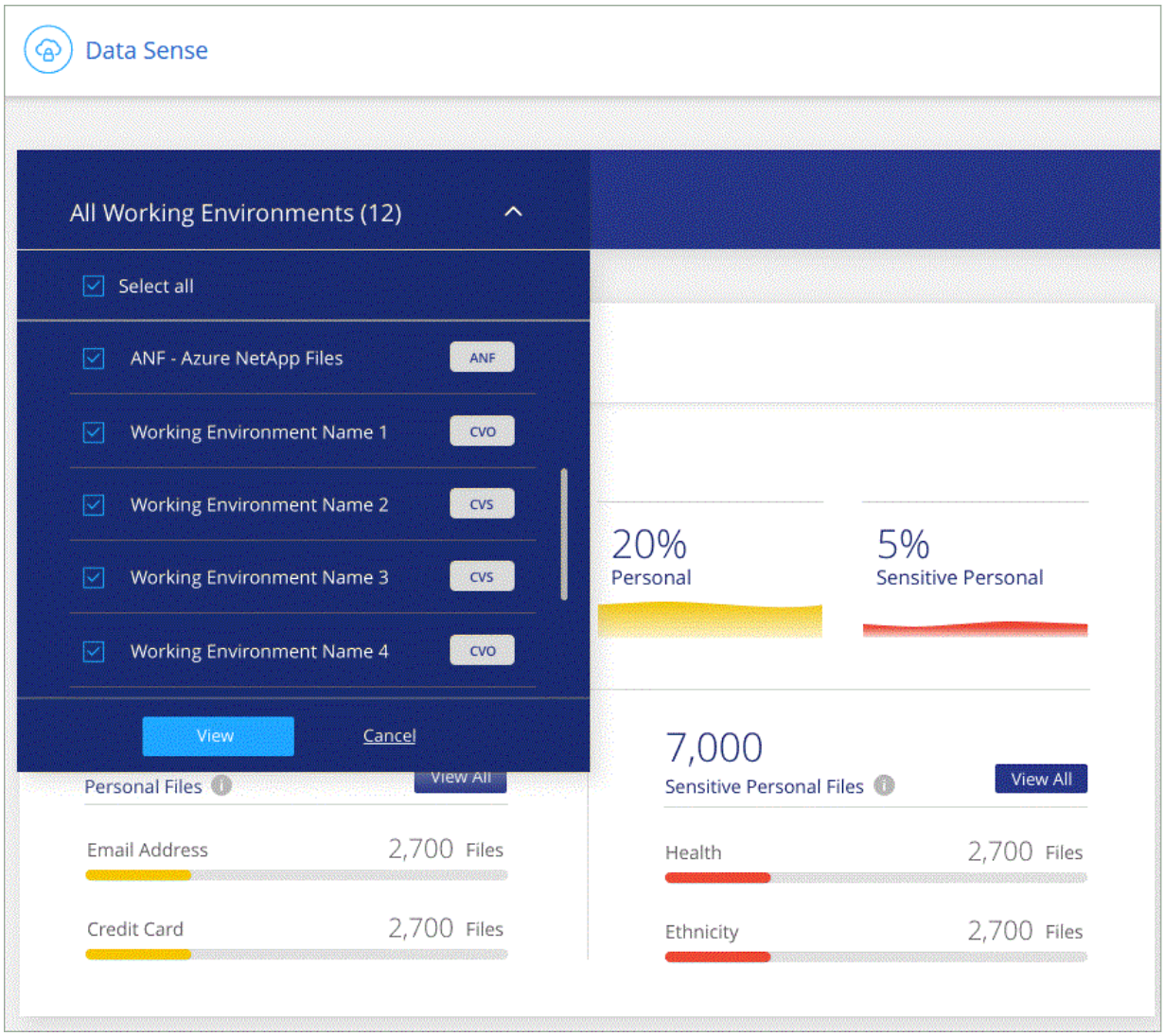
特定の作業環境のダッシュボードデータを表示する

BlueXPの分類ダッシュボードの内容をフィルタリングして、すべての作業環境とデータベース、または特定の作業環境のコンプライアンスデータを表示できます。

ダッシュボードをフィルタすると、BlueXPの分類によって、選択した作業環境のみに準拠データとレポートの範囲が限定されます。

手順

1. フィルタドロップダウンをクリックし、データを表示する作業環境を選択して、 * 表示 * をクリックします。



プライベートデータのカテゴリ

BlueXPの分類によってボリューム、Amazon S3バケット、データベース、OneDriveフォルダ、SharePointアカウントなど、さまざまな種類のプライベートデータを特定できます。 およびGoogleドライブアカウント。以下のカテゴリを参照してください。

> 国別ID番号や医療用IDなど、他のプライベートデータタイプを識別するためにBlueXPの分類が必要な場合は、ng-contact-data-sense@netapp.comまでリクエストをEメールで送信してください。

個人データの種類

ファイルに含まれる個人データは、一般的な個人データまたは国 ID です。次の表の3列目は、BlueXPの分類でが使用されているかどうかを示しています "近接性検証" 識別子の調査結果を検証します。

これらの項目を認識できる言語が表に示されています。

ファイル内にある個人データのリストに追加できます。データベースサーバをスキャンする場合、_Data

Fusion _機能を使用すると、データベーステーブルの列を選択して、BlueXP分類のスキャンで検索する追加の識別子を選択できます。また、カスタムキーワードをテキストファイルから追加したり、正規表現を使用してカスタムパターンを追加したりすることもできます。を参照してください "BlueXPの分類スキャンに個人データ識別子を追加します" を参照してください。

を入力します	識別子	近接性検証：	英語	ドイツ語	スペイン語	フランス語	日本語
全般	クレジットカード番号	いいえ	✓	✓	✓		✓
	データ主体	いいえ	✓	✓	✓		
	E メールアドレス	いいえ	✓	✓	✓		✓
	IBAN番号（国際銀行口座番号）	いいえ	✓	✓	✓		✓
	IP アドレス	いいえ	✓	✓	✓		✓
	パスワード	はい。	✓	✓	✓		✓

を入力します	識別子	近接性検証：	英語	ドイツ語	スペイン語	フランス語	日本語
国家識別番号							
150							

を入力します	識別子	近接性検証	英語	ドイツ語	スペイン語	フランス語	日本語
	ギリシャ ID	はい。	✓	✓	✓		
	ハンガリー語税識別番号	はい。	✓	✓	✓		
	アイルランド ID （ PPS ）	はい。	✓		✓		
	イスラエルの身分証明書	はい。	✓	✓	✓		
	イタリアの税識別番号	はい。	✓	✓	✓		
	日本の個人識別番号（個人および会社）	はい。	✓	✓	✓		✓
	ラトビア ID	はい。	✓	✓	✓		
	リトアニア ID	はい。	✓	✓	✓		
	ルクセンブルク iD	はい。	✓	✓	✓		
	マルタ ID	はい。	✓	✓	✓		
	National Health Service （ NHS ）番号	はい。	✓	✓	✓		
	ニュージーランド銀行口座	はい。	✓	✓	✓		
	ニュージーランド・ドライバー・ライセンス	はい。	✓	✓	✓		
	ニュージーランドIRD番号（税ID）	はい。	✓	✓	✓		
	ニュージーランドNHI（National Health Index）番号	はい。	✓	✓	✓		
	ニュージーランドパスポート番号	はい。	✓	✓	✓		
	ポーランド ID （ PESEL ）	はい。	✓	✓	✓		
	ポルトガル語税識別番号（ NIF ）	はい。	✓	✓	✓		
	ルーマニア語 ID （ CNP ）	はい。	✓	✓	✓		
	シンガポール国民登録IDカード（NRIC）	はい。	✓	✓	✓		
	スロベニア語 ID （ EMSO ）	はい。	✓	✓	✓		
	南アフリカ ID	はい。	✓	✓	✓		
	スペイン語税識別番号	はい。	✓	✓	✓		
	スウェーデン語 ID	はい。	✓	✓	✓		
	Texas Driver’s License	はい。	✓	✓	✓		
	英国ID （ニーノ）	はい。	✓	✓	✓		
	米国カリフォルニア州運転免許証	はい。	✓	✓	✓		
	USAインディアナ運転免許証	はい。	✓	✓	✓		
	米国ニューヨーク運転免許証	はい。	✓	✓	✓		
	米国社会保障番号（ SSN ）	はい。	✓	✓	✓		

機密性の高い個人データのタイプ

BlueXPの分類でファイルに含まれる機密性の高い個人データには、次のリストが含まれます。

このカテゴリの項目は、現時点では英語でのみ認識されます。

刑事手続きの参照
　天然人の犯罪に関するデータ。

『民族リファレンス』を参照してください
　自然な人の人種または民族の起源に関するデータ。

健全性リファレンス
　自然な人の健康に関するデータ。

ICD-9-CM Medical Codes
　医療および医療業界で使用されるコード。

ICD-10-CM Medical Codes
　医療および医療業界で使用されるコード。

哲学の信仰の参照
　自然な人の哲学的信条に関するデータ。

政治的見解参照
　自然界の政治的意見に関するデータ。

宗教的信条参照
　自然な人の宗教的信条に関するデータ。

性別生命または方向の参照
　自然な人の性生活や性的指向に関するデータ。

カテゴリのタイプ

BlueXPの分類では、データは次のように分類されます。

これらのカテゴリのほとんどは、英語、ドイツ語、スペイン語で認識されます。

カテゴリ	を入力します	英語	ドイツ語	スペイン語
財務	貸借対照表	✓	✓	✓
	注文書	✓	✓	✓
	請求書	✓	✓	✓
	四半期ごとのレポート	✓	✓	✓

カテゴリ	を入力します	英語	ドイツ語	スペイン語
時間	バックグラウンドチェック	✓		✓
	報酬プラン	✓	✓	✓
	従業員の契約	✓		✓
	従業員レビュー	✓		✓
	健常性	✓		✓
	再開します	✓	✓	✓
法律	NDAS	✓	✓	✓
	ベンダー - お客様との契約	✓	✓	✓
マーケティング	キャンペーン	✓	✓	✓
	会議	✓	✓	✓
処理	監査レポート	✓	✓	✓
営業	SO 番号	✓	✓	
サービス	RFI （ RFI ）	✓		✓
	RFP	✓		✓
	SOW の作成	✓	✓	✓
	トレーニング	✓	✓	✓
サポート	苦情やチケット	✓	✓	✓

次のメタデータも分類され、同じサポート対象言語で識別されます。

- アプリケーションデータ
- アーカイブファイル
- 音声
- ビジネスアプリケーションデータ
- CAD ファイル
- コード
- 壊れています
- データベースおよびインデックス・ファイル
- BlueXPの分類：パンくずリスト
- デザインファイル（ Design Files ）
- E メールアプリケーションデータ
- 暗号化（エントロピースコアが高いファイル）
- 実行可能ファイル
- 財務アプリケーションデータ

- ヘルスアプリケーションデータ
- イメージ
- ログ
- その他の文書
- その他のプレゼンテーション
- その他のスプレッドシート
- その他 " 不明 "
- パスワードで保護されたファイル
- 構造化データ
- ビデオ
- 0 バイトのファイル

ファイルのタイプ

BlueXPの分類は、すべてのファイルをスキャンしてカテゴリやメタデータの分析情報を取得し、ダッシュボードの[File Types]セクションにすべてのファイルタイプを表示します。

ただし、BlueXPの分類でPersonal Identifiable Information（PII）が検出された場合や、DSAR検索が実行された場合は、次のファイル形式のみがサポートされます。

「+.csv」、「.dcm」、「.dom」、「.DOC」、「.DOCX」、 .json、.pdf、.PPTX、.rtf、.TXT、 .XLS、.xlsx、Docs、Sheets、Slides +`

見つかった情報の正確性

ネットアップは、BlueXPの分類によって特定される個人データや機密性の高い個人データの正確性を100%保証することはできません。必ずデータを確認して情報を検証してください。

ネットアップのテストに基づいて、BlueXPで分類された情報の正確さを次の表に示します。精度 _ と _ リコール _ で分解します。

精度（ **Precision** ）

BlueXPの分類で検出された内容が正しく特定された可能性。たとえば、個人データの正確な割合が 90% の場合、個人情報を含むと識別された 10 個中 9 個のファイルに個人情報が実際に含まれていることを意味します。10 個のファイルのうち 1 個はフォールスポジティブです。

取り消し

BlueXPで分類して何が必要かを判断できる確率。たとえば、個人データのリコール率が70%の場合、BlueXPの分類では、組織内の個人情報が実際に含まれているファイルの10個中7個を特定できます。BlueXPの分類ではデータの30%が失われ、ダッシュボードには表示されません。

私たちは、常に結果の正確さを改善しています。これらの改善点は、今後のBlueXP分類リリースで自動的に提供される予定です。

を入力します	精度（ **Precision** ）	取り消し
個人データ - 一般	90% ~ 95%	60% ～ 80%
個人データ - 国 ID	30% ~ 60%	40% ~ 60%
機密性の高い個人データ	80% ~ 95%	20% ~ 30%
カテゴリ	90% ~ 97%	60% ～ 80%

組織に保存されているデータを調査します

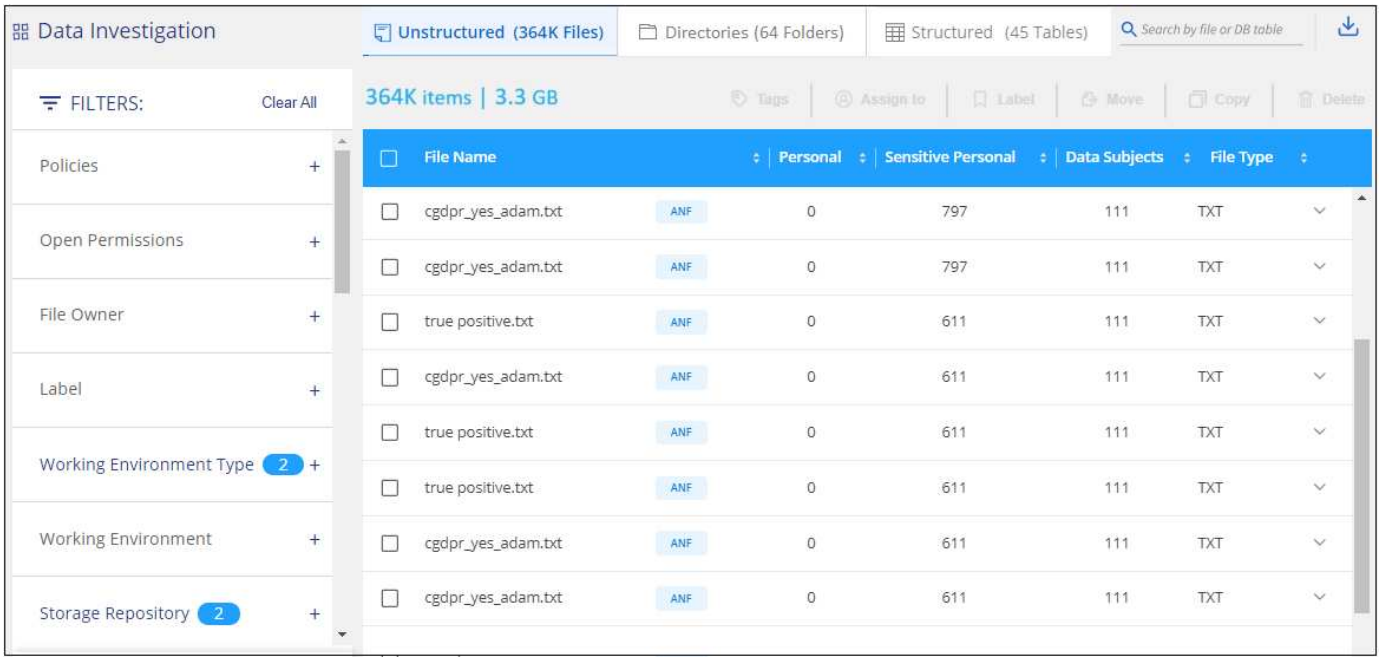
[データ調査]ページで詳細を表示すると、組織のデータを調査できます。このページには、ガバナンスダッシュボードやコンプライアンスダッシュボードなど、BlueXPの分類UIのさまざまな領域から移動できます。

> このセクションで説明する機能は、データソースに対して完全な分類スキャンを実行することを選択した場合にのみ使用できます。マッピングのみのスキャンを実行したデータソースでは、ファイルレベルの詳細は表示されません。

[Data Investigation]ページでのデータのフィルタリング

調査ページの内容をフィルタリングして、表示する結果のみを表示できます。これは非常に強力な機能です。データをリファインした後、ページ上部のボタンバーを使用して、ファイルのコピー、ファイルの移動、ファイルへのタグまたはAIPラベルの追加など、さまざまなアクションを実行できます。

ページをリファインした後で、そのページの内容をレポートとしてダウンロードする場合は、をクリックします ボタン"] ボタンを押します。 データ調査レポートの詳細については、こちらをご覧ください。



- トップレベルのタブでは、ファイル（非構造化データ）、ディレクトリ（フォルダおよびファイル共有）、またはデータベース（構造化データ）のデータを表示できます。
- 各列の上部にあるコントロールを使用して、結果を数値またはアルファベット順に並べ替えることができ

ます。

- 左側のペインフィルタを使用すると、以降のセクションで説明する属性を選択して、結果を絞り込むことができます。

感度と内容でデータをフィルタリングします

データに含まれている機密情報の量を表示するには、次のフィルタを使用します。

フィルタ	詳細
カテゴリ	を選択します "カテゴリのタイプ"。
感度レベル	感度レベルを選択します。個人レベル、個人レベル、または非機密レベルを選択します。
IDの数	検出された機密識別子のファイルごとの範囲を選択します。個人データと機密性の高い個人データが含まれます。ディレクトリでフィルタリングする場合、BlueXPの分類では、各フォルダ（およびサブフォルダ）内のすべてのファイルに一致するものが合計されます。 注: 2023年12月(バージョン1.26.6)リリースでは、ディレクトリごとの個人識別情報(PII)データの数を計算するオプションが一時的に削除されました。
個人データ	を選択します "個人データの種類"。
機密性の高い個人データ	を選択します "機密性の高い個人データのタイプ"。
データの件名	データ主体のフルネームまたは既知の識別子を入力します "データ主体の詳細については、こちらをご覧ください"。

ユーザの所有者とユーザの権限でデータをフィルタリングします

次のフィルタを使用して、ファイルの所有者とデータにアクセスするための権限を表示します。

フィルタ	詳細
[アクセス許可] を開きます	データ内およびフォルダ/共有内の権限のタイプを選択します。
ユーザ / グループの権限	1つ以上のユーザ名またはグループ名を選択するか、または名前の一部を入力してください。
ファイルの所有者	ファイル所有者名を入力します。
アクセス権を持つユーザの数	1つまたは複数のカテゴリ範囲を選択して、特定の数のユーザーに対してどのファイルおよびフォルダが開かれているかを表示します。

時間でデータをフィルタリングします

次のフィルタを使用して、条件に基づいてデータを表示します。

フィルタ	詳細
作成時刻（ Created Time ）	ファイルを作成したときの期間を選択します。カスタムの期間を指定して、検索結果をさらに絞り込むこともできます。

フィルタ	詳細
検出時刻	BlueXPの分類でファイルが検出された期間を選択します。カスタムの期間を指定して、検索結果をさらに絞り込むこともできます。
最終更新日	ファイルが最後に変更された時間範囲を選択します。カスタムの期間を指定して、検索結果をさらに絞り込むこともできます。
最後にアクセスした	ファイルまたはディレクトリ（CIFSまたはNFSのみ）が最後にアクセスされた時間範囲を選択します。カスタムの期間を指定して、検索結果をさらに絞り込むこともできます。BlueXP分類でスキャンされるファイルの種類については、BlueXP分類でファイルがスキャンされるのはこれが最後です。 BlueXPの分類では、SharePoint Online、SharePointオンプレミス（SharePoint Server）、OneDrive、Google Drive、Amazon S3の各データソースから「最終アクセス時刻」は抽出されません。

メタデータでデータをフィルタリングします

次のフィルタを使用して、場所、サイズ、およびディレクトリまたはファイルタイプに基づいてデータを表示します。

フィルタ	詳細
ファイルパス	クエリに含めるか除外するパスの一部または全部を20個まで入力します。対象パスと除外パスの両方を入力すると、対象パス内のすべてのファイルが最初に検出され、除外パスからファイルが削除されて結果が表示されます。このフィルタで「*」を使用しても効果はなく、特定のフォルダをスキャンから除外することはできません。設定された共有の下にあるすべてのディレクトリとファイルがスキャンされます。
ディレクトリタイプ（Directory Type）	ディレクトリタイプとして「共有」または「フォルダ」を選択します。
ファイルタイプ	を選択します "ファイルのタイプ"。
ファイルサイズ	ファイルサイズの範囲を選択します。
ファイル・ハッシュ	ファイルのハッシュを入力し、名前が異なる場合でも特定のファイルを検索します。

ストレージタイプでデータをフィルタリングします

ストレージタイプ別にデータを表示するには、次のフィルタを使用します。

フィルタ	詳細
作業環境タイプ（ Working Environment Type ）	作業環境のタイプを選択します。OneDrive、SharePoint、Google Driveは、[アプリ]に分類されます。
作業環境名	特定の作業環境を選択します。
ストレージリポジトリ	ボリュームやスキーマなどのストレージリポジトリを選択します。

タグ、ラベル、割り当てられたユーザ、およびポリシーでデータをフィルタリングします

AIPラベルまたはタグでデータを表示するには、次のフィルタを使用します。

フィルタ	詳細
ポリシー	ポリシーを選択します。実行します "こちらをご覧ください" をクリックして、既存のポリシーのリストを表示し、独自のカスタムポリシーを作成します。
ラベル	選択するオプション "AIP ラベル" ファイルに割り当てられます。
タグ	選択するオプション "タグ" ファイルに割り当てられます。
割り当て先	ファイルが割り当てられているユーザーの名前を選択します。

分析ステータスでデータをフィルタリングします

次のフィルタを使用して、BlueXPの分類スキャンステータス別にデータを表示します。

フィルタ	詳細
解析ステータス（Analysis Status）	オプションを選択して、[最初のスキャン保留中]、[スキャン完了]、[再スキャン保留中]、または[スキャンに失敗しました]のファイルのリストを表示します。
スキャン分析イベント	BlueXPの分類で最終アクセス時刻を復元できなかったために分類されなかったファイルを表示するか、BlueXPの分類で最終アクセス時刻を復元できなかったにもかかわらず分類されたファイルを表示するかを選択します。

"「最終アクセス時刻」のタイムスタンプの詳細を参照してください" スキャン分析イベントを使用してフィルタリングするときに[Investigation]ページに表示される項目の詳細については、を参照してください。

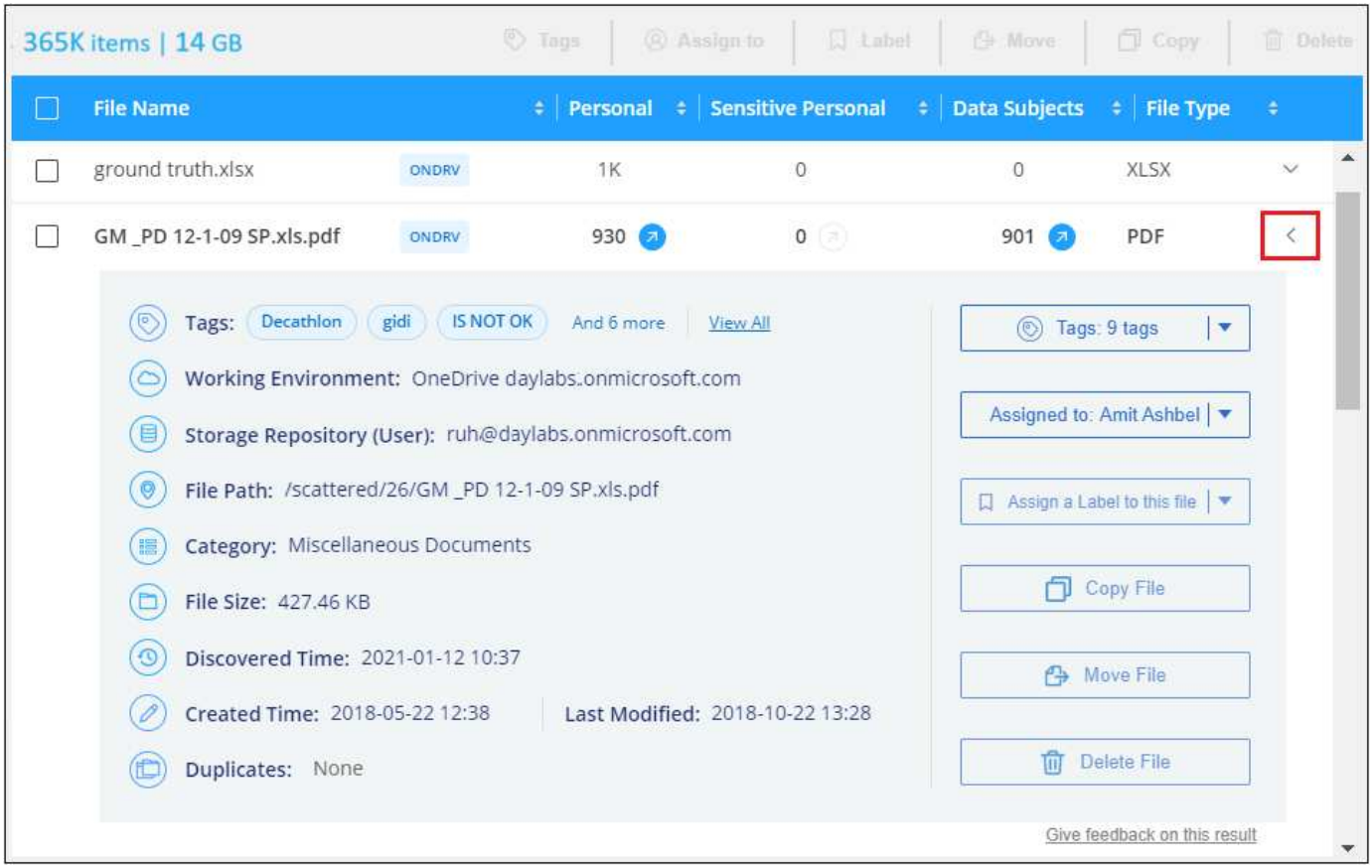
重複でデータをフィルタリングします

ストレージ内で複製されているファイルを表示するには、次のフィルタを使用します。

フィルタ	詳細
重複	リポジトリ内でファイルを複製するかどうかを選択します。

ファイルメタデータの表示

[データ調査結果] ペインで、をクリックできます ⌄ をクリックすると、単一のファイルについてファイルのメタデータが表示されます。



ページのファイルのメタデータの詳細を示すスクリーンショット。"]

ファイルが存在する作業環境とボリュームを表示するだけでなく、メタデータには、ファイル権限、ファイルの所有者、このファイルの重複がないかどうか、および AIP ラベルが割り当てられている場合など、より多くの情報が表示されます "BlueXPに統合されたAIPです"）。この情報は、を計画している場合に役立ちます "ポリシーを作成します" データのフィルタリングに使用できるすべての情報が表示されます。

すべてのデータソースについて、すべての情報が表示されるわけではなく、そのデータソースに適した情報だけが表示されることに注意してください。たとえば、ボリューム名、権限、および AIP ラベルは、データベースファイルには関係ありません。

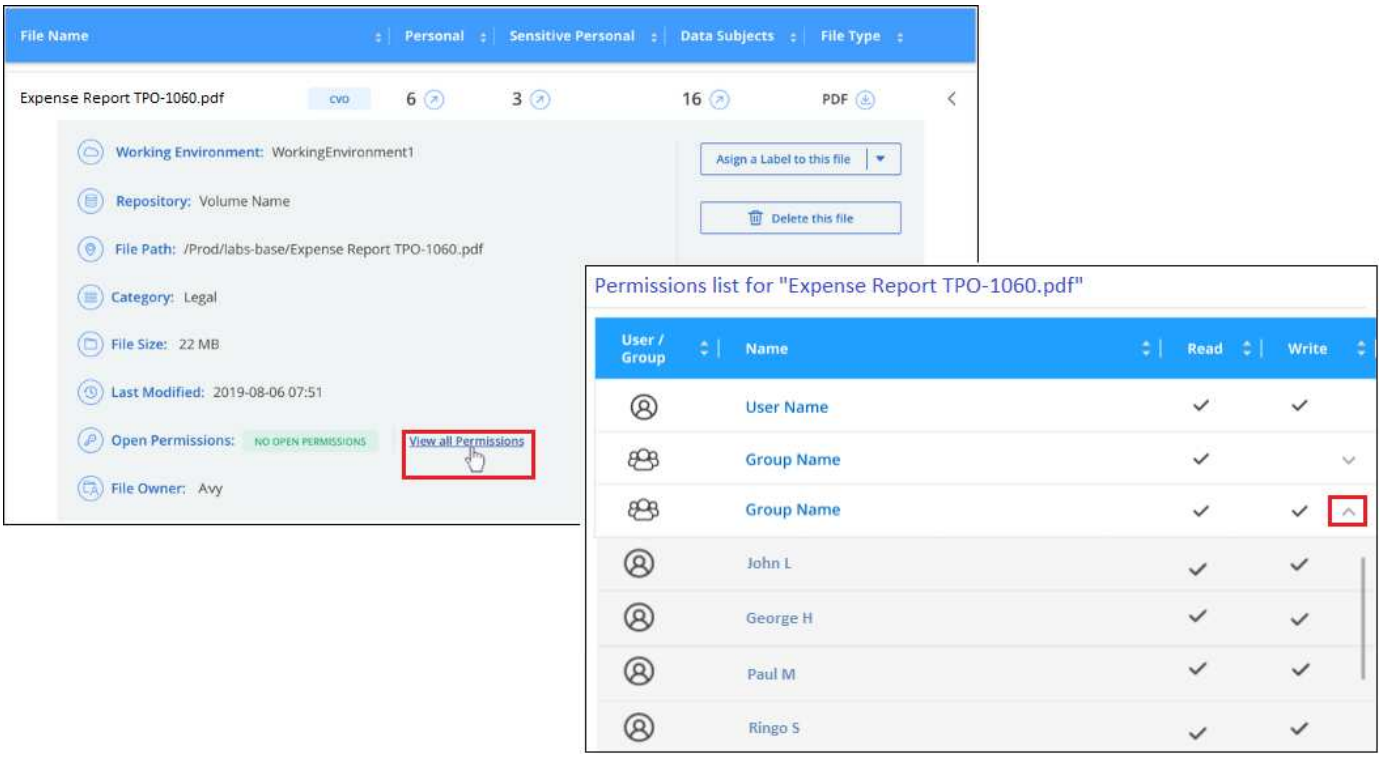
単一のファイルの詳細を表示する場合は、ファイルに対していくつかの操作を実行できます。

- ファイルは任意の NFS 共有に移動またはコピーできます。を参照してください "ソースファイルを NFS 共有に移動しています" および "ソースファイルを NFS 共有にコピーしています" を参照してください。
- ファイルを削除できます。を参照してください "ソースファイルを削除しています" を参照してください。
- ファイルに特定のステータスを割り当てることができます。を参照してください "タグの適用" を参照してください。
- このファイルをBlueXPユーザーに割り当てることで、ファイルに対して実行する必要があるフォローアップアクションを実行できます。を参照してください "ファイルへのユーザの割り当て" を参照してください。
- AIPラベルをBlueXPに統合した場合は、このファイルにラベルを割り当てることができます。また、すでに存在する場合は別のラベルに変更することもできます。を参照してください "AIP ラベルを手動で割り当てる" を参照してください。

ファイルおよびディレクトリの権限を表示する

ファイルまたはディレクトリへのアクセス権を持つすべてのユーザーまたはグループのリスト、およびそれらが持っているアクセス権のタイプを表示するには、*すべてのアクセス権を表示*をクリックします。このボタンは、CIFS共有、SharePoint Online、SharePoint On-Premise、OneDriveのデータに対してのみ使用できます。

ユーザ名とグループ名の代わりにSID（セキュリティ識別子）が表示される場合は、Active DirectoryをBlueXPに統合する必要があります。 "詳細については、「方法」を参照してください"。



をクリックできます をクリックすると、グループの一部であるユーザのリストが表示されます。

さらに、 ユーザまたはグループの名前をクリックすると、[調査]ページにそのユーザまたはグループの名前が表示され、[ユーザ/グループの権限]フィルタに入力されます。これにより、そのユーザまたはグループがアクセスできるすべてのファイルとディレクトリを表示できます。

ストレージシステム内の重複ファイルのチェック

重複ファイルがストレージシステムに保存されているかどうかを確認できます。これは、ストレージスペースを節約できる領域を特定する場合に便利です。また、特定の権限や機密情報を持つファイルが、ストレージシステム内で不必要に重複しないようにすることもできます。

1MB以上で、個人情報または機密情報を含むすべてのファイル（データベースを除く）が比較され、重複がないかどうかが確認されます。[Investigation]ページフィルタの[File Size]と[Duplicates]を使用して、環境内で特定のサイズ範囲のどのファイルが重複しているかを確認できます。

BlueXPの分類では、ハッシュテクノロジを使用して重複ファイルが特定されます。ハッシュコードが別のファイルと同じファイルがある場合、ファイル名が異なる場合でも、ファイルが完全に重複していることを100% 確認できます。

重複ファイルのリストをダウンロードし、ストレージ管理者に送信して、削除可能なファイルをユーザが判別

できるようにします。または "ファイルを削除します" 特定のバージョンのファイルが不要であることが確信できる場合は、自分自身で実行します。

重複ファイルをすべて表示

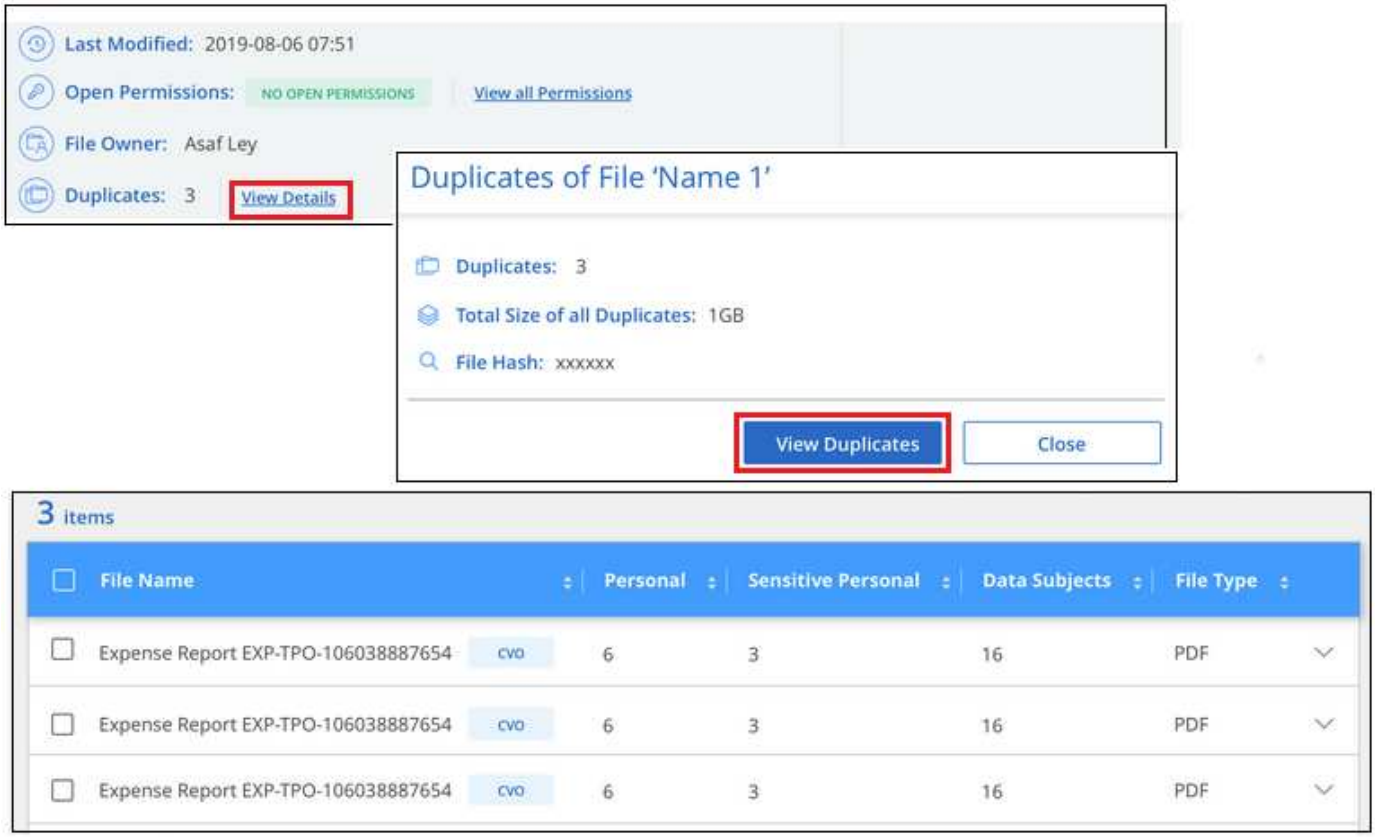
スキャンする作業環境およびデータソースで複製されているすべてのファイルのリストが必要な場合は、 [データの調査] ページで、 [重複] > [重複しているもの] というフィルタを使用できます。

複製されたすべてのファイルが結果ページに表示されます。

特定のファイルが重複しているかどうかを表示する

1 つのファイルに重複があるかどうかを確認するには、 [データ調査結果] ペインでをクリックします ⌄ をクリックすると、単一のファイルについてファイルのメタデータが表示されます。特定のファイルが重複している場合、この情報は _Duplicats_field の横に表示されます。

重複したファイルとその場所のリストを表示するには、 [* 詳細の表示 *] をクリックします。次のページで、 [重複の表示 *] をクリックして、 [調査] ページでファイルを表示します。



このページで指定されている「ファイルハッシュ」値を使用して、 ［ 調査 ］ ページに直接入力すると、特定の重複ファイルをいつでも検索できます。また、ポリシーで使用することもできます。

データ調査レポート

Data Investigation Reportは、Data Investigationページのフィルタリングされた内容をダウンロードしたものです。

レポートには、次の2つの形式があります。

- ローカルマシンに保存できる.csvファイル。

  このレポートには、最大10,000行のデータを含めることができます。

- NFS共有にエクスポートする.jsonファイルとして指定します。

  25万行を超えるデータがある場合は、追加の.jsonファイルが作成されます。

  ファイル共有にエクスポートする場合は、BlueXPの分類にエクスポートアクセス用の正しい権限が割り当てられていることを確認してください。

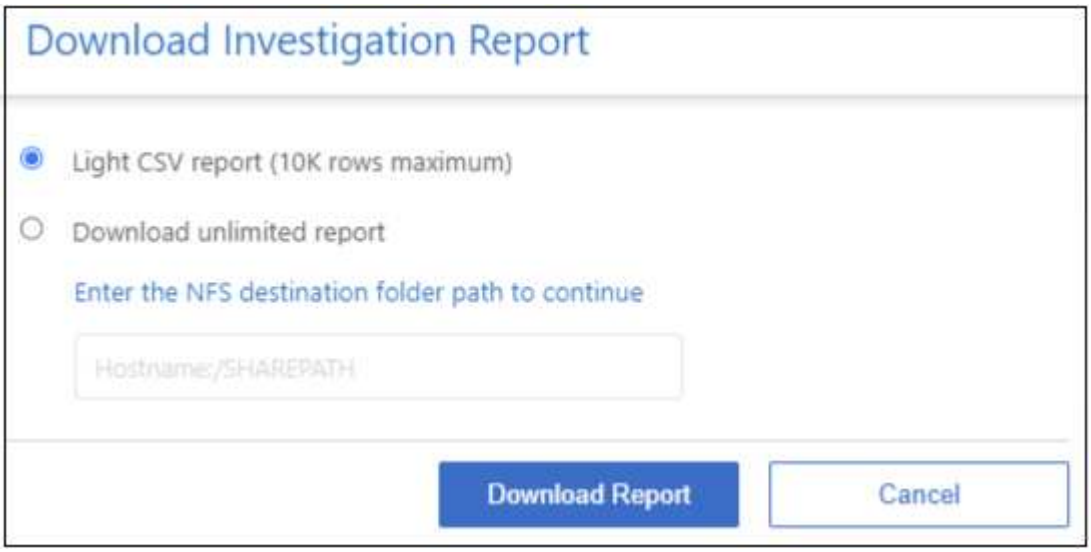
BlueXPの分類でファイル（非構造化データ）、ディレクトリ（フォルダとファイル共有）、データベース（構造化データ）をスキャンしている場合は、最大3つのレポートファイルをダウンロードできます。

データ調査レポートの生成

手順

1. [データ調査]ページで、をクリックします ボタン"] ボタンをクリックします。
2. データの.csvレポートと.jsonレポートのどちらをダウンロードするかを選択し、*レポートのダウンロード*をクリックします。

   JSONレポートを選択するときは、レポートをダウンロードするNFS共有の名前を「<host_name>：/<share_path>`」の形式で入力します。



結果

レポートをダウンロード中であることを示すメッセージがダイアログに表示されます。

JSONレポートの生成の進捗状況は、で確認できます "[アクションステータス（ Actions Status ） パネル"]。

各データ調査レポートに含まれる情報

非構造化ファイルデータレポート*には、ファイルに関する次の情報が含まれています。

- ファイル名
- 場所のタイプ
- 作業環境の名前
- ストレージリポジトリ（ボリューム、バケット、共有など）
- リポジトリタイプ
- ファイルパス
- ファイルタイプ
- ファイルサイズ（MB）
- 時刻を作成しました
- 最終更新日
- 最後にアクセスした
- ファイルの所有者
- カテゴリ
- 個人情報
- 機密性の高い個人情報
- オープンアクセス権
- スキャン分析エラー
- 削除の検出日

  削除の検出日は、ファイルが削除または移動された日付を示します。これにより、機密ファイルがいつ移動されたかを識別できます。削除されたファイルは、ダッシュボードまたは [調査] ページに表示されるファイル番号カウントの一部ではありません。ファイルは CSV レポートにのみ表示されます。

非構造化ディレクトリデータレポート*には、フォルダおよびファイル共有に関する次の情報が含まれています。

- 作業環境のタイプ
- 作業環境の名前
- ディレクトリ名
- ストレージリポジトリ（フォルダ、ファイル共有など）
- ディレクトリ所有者
- 時刻を作成しました
- 検出時刻
- 最終更新日
- 最後にアクセスした
- オープンアクセス権
- ディレクトリタイプ

構造化データレポート*には、データベーステーブルに関する次の情報が含まれています。

- DB テーブル名
- 場所のタイプ
- 作業環境の名前
- ストレージリポジトリ（スキーマなど）
- 列数
- 行数
- 個人情報
- 機密性の高い個人情報

プライベートデータを整理します

BlueXPの分類では、プライベートデータをさまざまな方法で管理、整理できます。これにより、最も重要なデータを簡単に確認できます。

- に登録している場合は "Azure 情報保護（ AIP ）" ファイルを分類して保護するには、BlueXPの分類を使用してAIPラベルを管理します。

> 2023年12月（v1.26.6）リリースでは、Azure Information Protection（AIP）ラベルを使用してデータを統合するオプションが一時的に削除されました。

- 組織または特定の種類のフォローアップのためにマークするファイルにタグを追加できます。
- BlueXPユーザーを特定のファイルまたは複数のファイルに割り当てることで、ユーザーがファイルの管理を担当できるようになります。
- 「ポリシー」機能を使用すると、 1 つのボタンをクリックして簡単に結果を表示できるように、独自のカスタム検索クエリを作成できます。
- 特定の重要なポリシーの結果が返された場合は、BlueXPユーザーまたはその他の電子メールアドレスに電子メールアラートを送信できます。

> このセクションで説明する機能は、データソースに対して完全な分類スキャンを実行することを選択した場合にのみ使用できます。マッピングのみのスキャンを実行したデータソースでは、ファイルレベルの詳細は表示されません。

タグまたはラベルを使用する必要がありますか？

以下は、BlueXPの分類タギングとAzure Information Protectionのラベル付けの比較です。

タグ	ラベル
ファイルタグはBlueXPに統合された分類機能です。	Azure Information Protection （ AIP ）に加入している必要があります。

タグ	ラベル
タグはBlueXP分類データベースにのみ保存され、ファイルには書き込まれません。ファイル、アクセス日時または変更日時は変更されません。	ラベルはファイルの一部であり、ラベルが変更されるとファイルが変更されます。この変更によって、アクセス日時や変更日時も変更されます。
1 つのファイルに複数のタグを設定できます。	1 つのファイルに 1 つのラベルを付けることができます。
このタグは、BlueXPの内部分類アクション（コピー、移動、削除、ポリシーの実行、 など	ファイルを読み取ることができる他のシステムでは、ラベルを確認できます。このラベルは、自動化のために使用できます。
ファイルにタグが設定されているかどうかを確認するために使用される API 呼び出しは 1 つだけです。	

AIP ラベルを使用してデータを分類します

サブスクライブ済みの場合は、BlueXP分類でスキャンするファイルでAIPラベルを管理できます "Azure 情報保護（ AIP ）"。AIP を使用すると、コンテンツにラベルを適用することで、ドキュメントやファイルを分類して保護できます。BlueXPでは、ファイルにすでに割り当てられているラベルの表示、ファイルへのラベルの追加、既存のラベルの変更を行うことができます。

BlueXPの分類では、.DOC、.DOCX、.PDF、.PPTX、.XLSの各ファイルタイプでAIPラベルがサポートされます。 .XLSX。

- 現在、 30MB を超えるファイルのラベルは変更できません。OneDrive、SharePoint 、Google Driveアカウントの場合、最大ファイルサイズは4 MBです。
- AIPに存在しないラベルがファイルに含まれている場合、BlueXPの分類ではラベルのないファイルとみなされます。
- 政府機関の地域、またはインターネットアクセスのないオンプレミスの場所（ダークサイトとも呼ばれます）にBlueXPの分類を導入している場合は、AIPラベル機能を使用できません。

ワークスペースに**AIP**ラベルを統合

AIPラベルを管理するには、既存のAzureアカウントにサインインして、AIPラベル機能をBlueXPの分類に統合する必要があります。有効にすると、すべてのファイルの AIP ラベルを管理できます "データソース" を選択します。

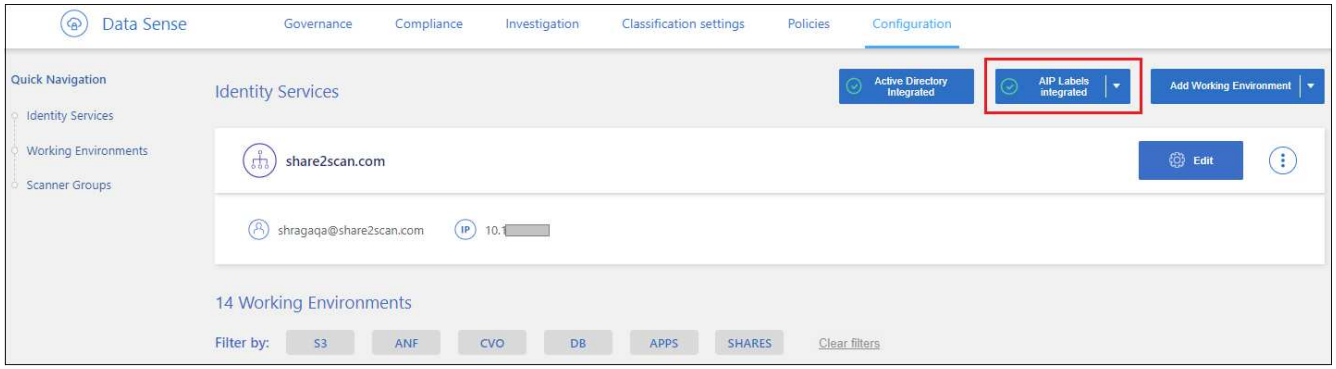
要件

- アカウントと Azure Information Protection のライセンスが必要です。
- Azure アカウントのログインクレデンシャルが必要です。
- Amazon S3 バケット内のファイルのラベルを変更する場合は、権限「 3 ： PutObject 」が IAM ロールに含まれていることを確認します。を参照してください "IAM ロールを設定します"。

手順

1. BlueXPの分類の[設定]ページで、*[Integrate AIP Labels]*をクリックします。

2. [Integrate AIP Labels （ AIP ラベルの統合）] ダイアログで、 [* Sign in to Azure* （ Azure にサインイン）]
3. 表示される Microsoft ページで、アカウントを選択し、必要なクレデンシャルを入力します。
4. BlueXPの分類タブに戻り、「_AIP Labels were integrated successfully with the account <account_name>_」というメッセージが表示されます。
5. [* 閉じる] をクリックすると、ページの上部に「 *AIP* ラベル *integrated_* 」というテキストが表示されます。



結果

AIP ラベルは、 ［ 調査 ］ ページの結果ペインで表示および割り当てることができます。また、ポリシーを使用して AIP ラベルをファイルに割り当てることもできます。

ファイル内の**AIP**ラベルの表示

ファイルに割り当てられている現在の AIP ラベルを表示できます。

[データ調査結果] ペインで、をクリックします ⌄ をクリックします。

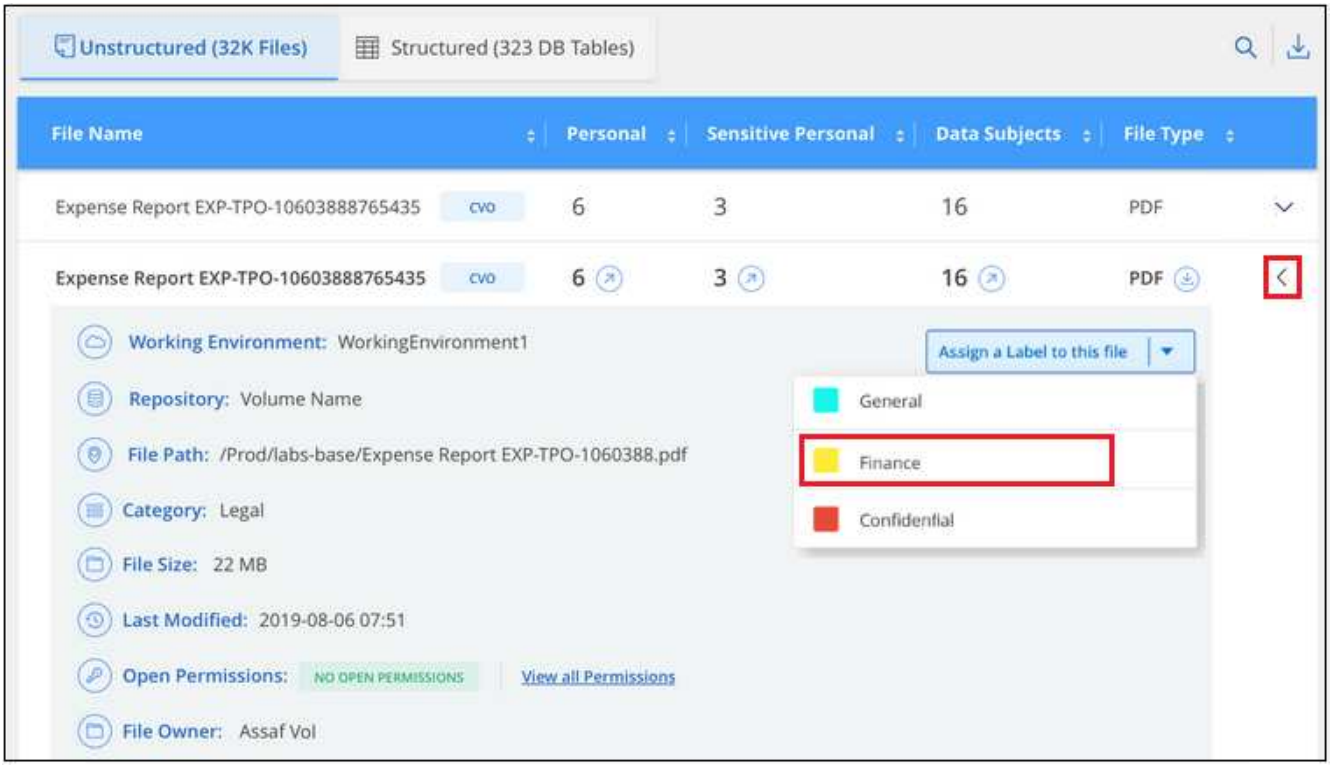
AIPラベルの手動割り当て

BlueXPの分類を使用して、ファイルのAIPラベルを追加、変更、削除できます。

AIP ラベルを 1 つのファイルに割り当てる手順は、次のとおりです。

手順

1. [データ調査結果] ペインで、をクリックします をクリックします。



ページのファイルのメタデータの詳細を示すスクリーンショット。"]

2. [* このファイルにラベルを割り当て *] をクリックして、ラベルを選択します。

   ラベルがファイルメタデータに表示されます。

AIPラベルを複数のファイルに割り当てる手順は、次のとおりです。AIPラベルは、一度に最大20個のファイル（UIの1ページ）に割り当てることができます。

手順

1. [データ調査結果] ペインで、ラベル付けするファイルを選択します。

ページの [ラベル] ボタン。"]

- 個々のファイルを選択するには、各ファイル（ Volume_1）。
- 現在のページのすべてのファイルを選択するには、タイトル行（ File Name ）。

2. ボタンバーの * Label * をクリックし、 AIP ラベルを選択します。

AIP ラベルが、選択したすべてのファイルのメタデータに追加されます。

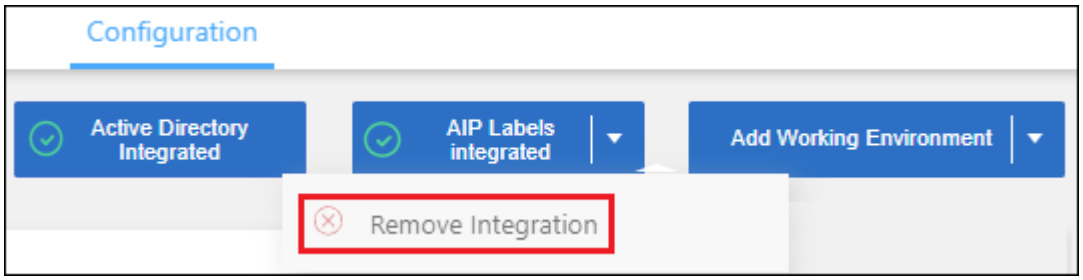
AIP統合の削除

ファイル内のAIPラベルを管理する必要がなくなった場合は、BlueXPの分類インターフェイスからAIPアカウントを削除できます。

BlueXPの分類を使用して追加したラベルは変更されません。ファイルに存在するラベルは、現在存在しているラベルのままになります。

手順

1. _Configuration_page で、 *AIP ラベル統合 > 統合の削除 * をクリックします。



2. 確認ダイアログで、 [統合の削除（ Remove Integration ）] をクリックします。

タグを適用してスキャンしたファイルを管理

特定の種類のフォローアップでマークするファイルにタグを追加できます。たとえば、重複するファイルがいくつか見つかった場合に、それらのファイルを 1 つ削除する必要がありますが、削除するファイルを確認する必要があります。このファイルに「削除するチェック」というタグを追加すると、このファイルに何らかの調査と将来のアクションが必要であることがわかります。

BlueXPでは、ファイルに割り当てられているタグの表示、ファイルに対するタグの追加と削除、名前の変更や既存のタグの削除を行うことができます。

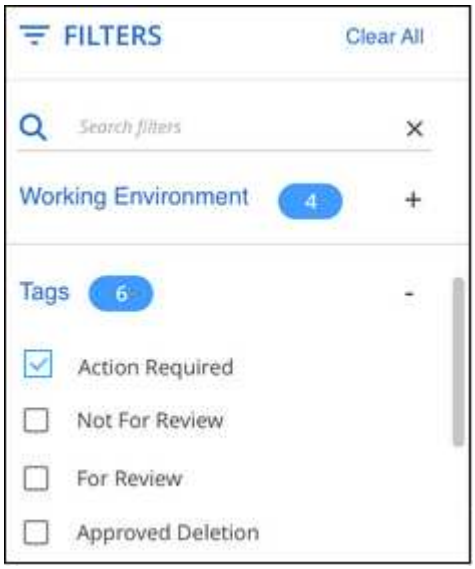
AIP ラベルがファイルメタデータの一部であるのと同じ方法で、タグがファイルに追加されないことに注意してください。このタグはBlueXPユーザのみがBlueXP分類を使用して確認できるため、ファイルを削除する必要があるかどうか、または何らかのフォローアップが必要かどうかを確認できます。

> BlueXPで分類されたファイルに割り当てられたタグは、リソース（ボリュームや仮想マシンインスタンスなど）に追加できるタグとは関係ありません。BlueXPの分類タグはファイルレベルで適用されます。

特定のタグが適用されているファイルを表示する

特定のタグが割り当てられているすべてのファイルを表示できます。

1. BlueXP分類の*[Investigation]*タブをクリックします。
2. [データ調査] ページで、 [フィルタ] ペインの [* タグ] をクリックし、必要なタグを選択します。



ペインからタグを選択する方法を示すスクリーンショット。"]

[調査結果] ペインには、これらのタグが割り当てられているすべてのファイルが表示されます。

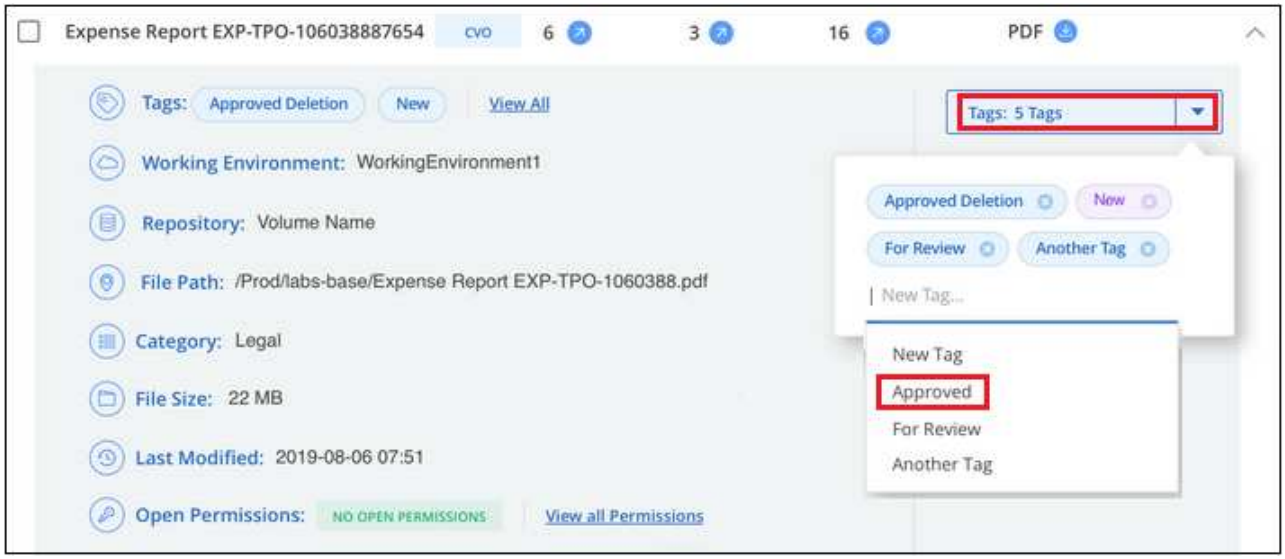
ファイルへのタグの割り当て

タグは、単一のファイルまたはファイルのグループに追加できます。

タグを 1 つのファイルに追加するには：

手順

1. [データ調査結果] ペインで、をクリックします をクリックします。
2. [* タグ * （ * Tags * ）] フィールドをクリックすると、現在割り当てられているタグが表示されます。
3. タグを追加します。
   - 既存のタグを割り当てるには、「 * 新しいタグ … 」フィールドをクリックして、タグの名前を入力します。探しているタグが表示されたら、そのタグを選択して * Enter * を押します。
   - 新しいタグを作成してファイルに割り当てるには、 [新しいタグ …] * フィールドをクリックし、新しいタグの名前を入力して、 **Enter** キーを押します。



ページでファイルにタグを割り当てる方法を示すスクリーンショット。"]

タグがファイルメタデータに表示されます。

複数のファイルにタグを追加するには：

手順

1. [データ調査結果] ペインで、タグを付けるファイルを選択します。

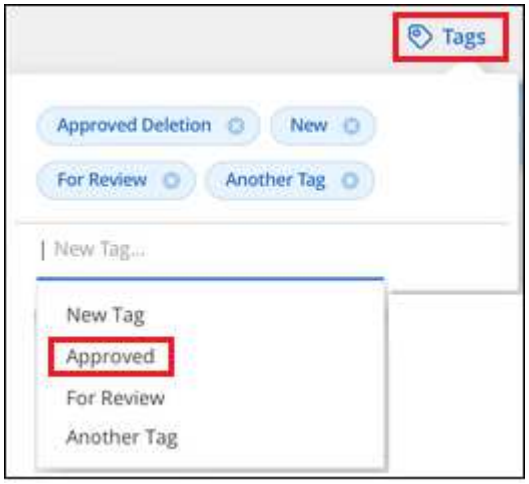
ページから、タグを付けるファイルの選択方法と [タグ] ボタンを示すスクリーンショット。"]

   - 個々のファイルを選択するには、各ファイル（ Volume_1）。
   - 現在のページのすべてのファイルを選択するには、タイトル行（ File Name ）。

- すべてのページのすべてのファイルを選択するには、タイトル行（ File Name ）をクリックし、ポップアップメッセージにと入力します All 20 Items on this page selected Select all Items in list (63K Items)をクリックし、リスト（ xxx 項目）のすべての項目を選択 * をクリックします。

  一度に最大100,000個のファイルにタグを適用できます。

2. ボタンバーで * タグ * をクリックすると、現在割り当てられているタグが表示されます。
3. タグを追加します。
   - 既存のタグを割り当てるには、「 * 新しいタグ … 」フィールドをクリックして、タグの名前を入力します。探しているタグが表示されたら、そのタグを選択して * Enter * を押します。
   - 新しいタグを作成してファイルに割り当てるには、 [新しいタグ …] * フィールドをクリックし、新しいタグの名前を入力して、 **Enter** キーを押します。



ページで複数のファイルにタグを割り当てる方法を示すスクリーンショット。"]

4. 確認ダイアログでタグの追加を承認し、選択したすべてのファイルのメタデータにタグを追加します。

ファイルからタグを削除

不要になったタグは削除できます。

既存のタグの * x * をクリックするだけです。

複数のファイルを選択した場合、タグはすべてのファイルから削除されます。

特定のファイルを管理するためのユーザの割り当て

BlueXPユーザーを特定のファイルまたは複数のファイルに割り当てることができるため、ユーザーはファイルに対して実行する必要があるフォローアップアクションを実行できます。この機能は、多くの場合、カスタムステータスタグをファイルに追加する機能で使用されます。

たとえば、特定の個人データを含むファイルで、読み取りおよび書き込みアクセス（オープン権限）を大量に許可する場合などです。したがって、 Status タグ「 Change permissions 」を割り当て、このファイルをユーザー「 Joan Smith 」に割り当てて、問題の修正方法を決定することができます。問題を修正すると、 Status

タグが「 Completed 」に変更されることがあります。

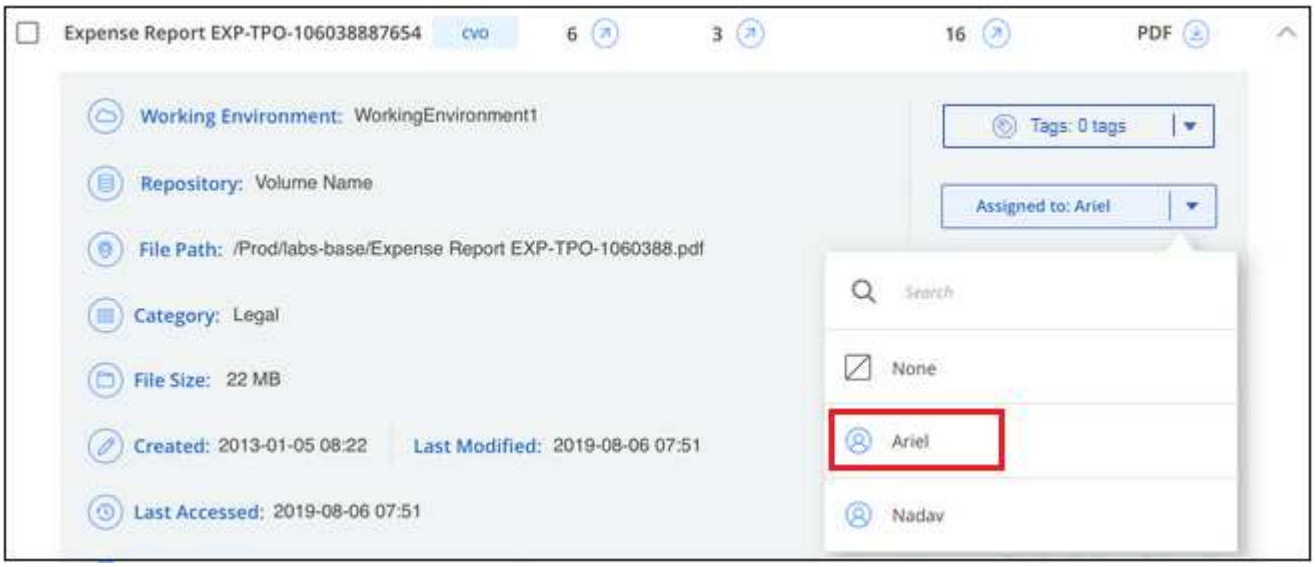
ユーザ名はファイルメタデータの一部としてファイルに追加されるわけではなく、BlueXPユーザがBlueXP分類を使用している場合にのみ表示されます。

[調査] ページの新しいフィルタを使用すると、 [割り当て先] フィールドに同じユーザーを持つすべてのファイルを簡単に表示できます。

ユーザを単一のファイルに割り当てる手順は、次のとおりです。

手順

1. [データ調査結果] ペインで、をクリックします をクリックします。
2. [**Assigned To**] フィールドをクリックして、ユーザ名を選択します。



ページでファイルにユーザーを割り当てる方法を示すスクリーンショット。"]

ユーザ名がファイルメタデータに表示されます。

ユーザーを複数のファイルに割り当てるには、次の手順を実行します。一度に最大20個のファイルにユーザを割り当てることができます（UIの1ページ）。

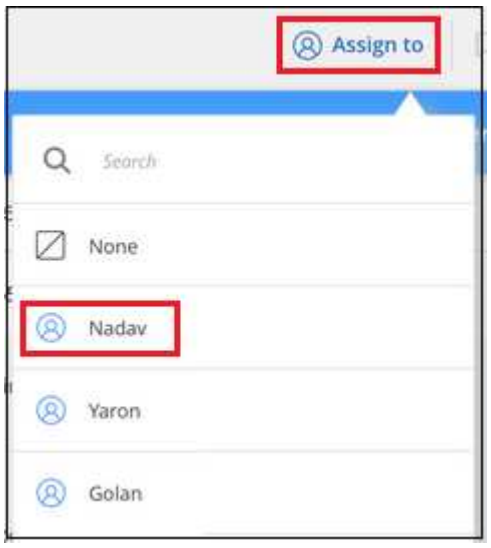
手順

1. [データ調査結果] ペインで、ユーザーに割り当てるファイルを選択します。

ページから、ユーザーに割り当てるファイルの選択方法と [割り当て先] ボタンを示すスクリーンショット。"]

- 個々のファイルを選択するには、各ファイル（ Volume_1）。
- 現在のページのすべてのファイルを選択するには、タイトル行（ File Name ）。

2. ボタンバーで * Assign to * をクリックし、ユーザー名を選択します。



ページでユーザーを複数のファイルに割り当てる方法を示すスクリーンショット。"]

選択したすべてのファイルのメタデータにユーザが追加されます。

データにポリシーを割り当てます

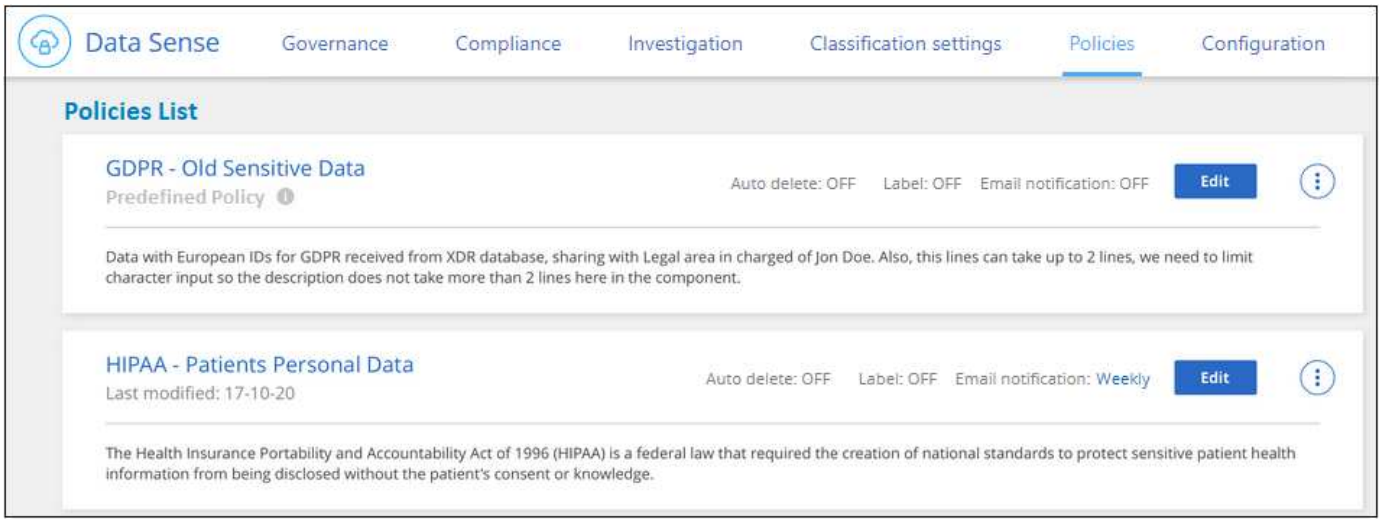
ポリシーは、よく要求されるコンプライアンスクエリーの [調査] ページで検索結果を表示するカスタムフィルタのお気に入りリストのようなものです。BlueXPは分類されており、一般的なお客様の要望に基づいて一連のポリシーが事前定義されています。組織固有の検索結果を提供するカスタムポリシーを作成できます。

ポリシーには次の機能があります。

- 事前定義されたポリシー ユーザの要求に基づいて作成されます
- 独自のカスタムポリシーを作成できます
- ポリシーの結果を含む [調査] ページを起動します ワンクリックで
- 特定の重要なポリシーが結果を返すときに、BlueXPユーザーやその他の電子メールアドレスに電子メールアラートを送信して、データを保護するための通知を受け取ることができます
- AIP の割り当て（ Azure 情報保護） 定義された条件に一致するすべてのファイルに自動的にラベルを付けます ポリシー内
- 特定のポリシーで結果が返されたときにファイルを自動的に削除して（ 1 日に 1 回）、データを自動的に保護できます

コンプライアンスダッシュボードの*[ポリシー]*タブには、BlueXP分類のこのインスタンスで使用可能な事前

定義済みポリシーとカスタムポリシーがすべて表示されます。

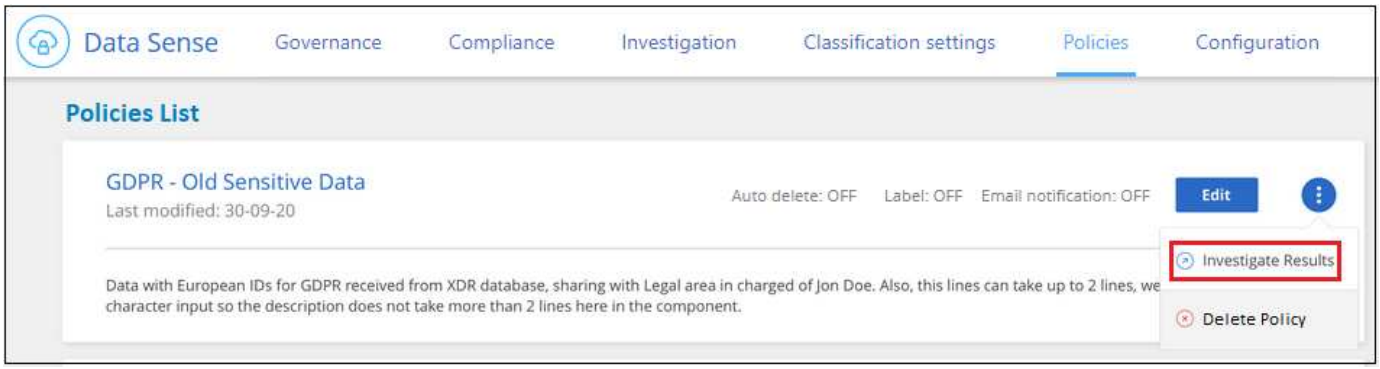


タブのスクリーンショット。"]

さらに、 [調査] ページの [フィルタ] リストにポリシーが表示されます。

[Investigation]ページでのポリシー結果の表示

[調査] ページでポリシーの結果を表示するには、をクリックします ボタン"] ボタンをクリックして特定のポリシーを選択し、 * 調査結果 * を選択します。



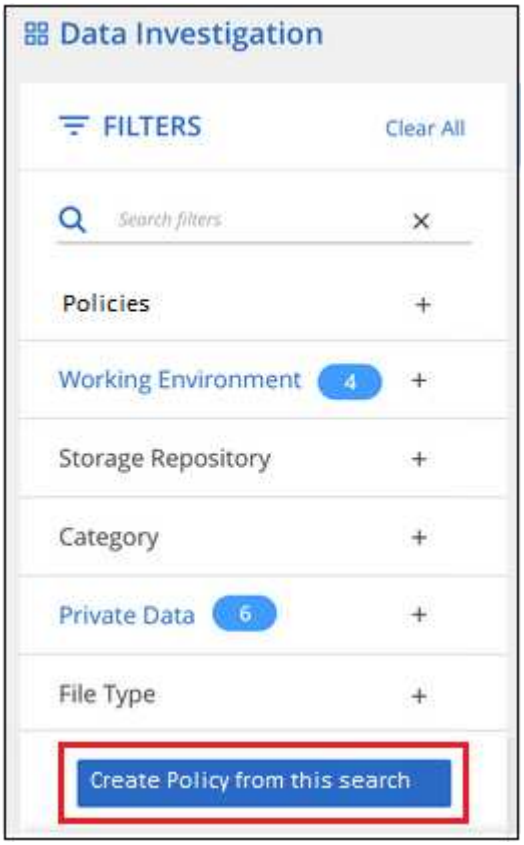
カスタムポリシーの作成

組織固有の検索結果を提供する独自のカスタムポリシーを作成できます。検索条件に一致するすべてのファイルとディレクトリ（共有とフォルダ）の結果が返されます。

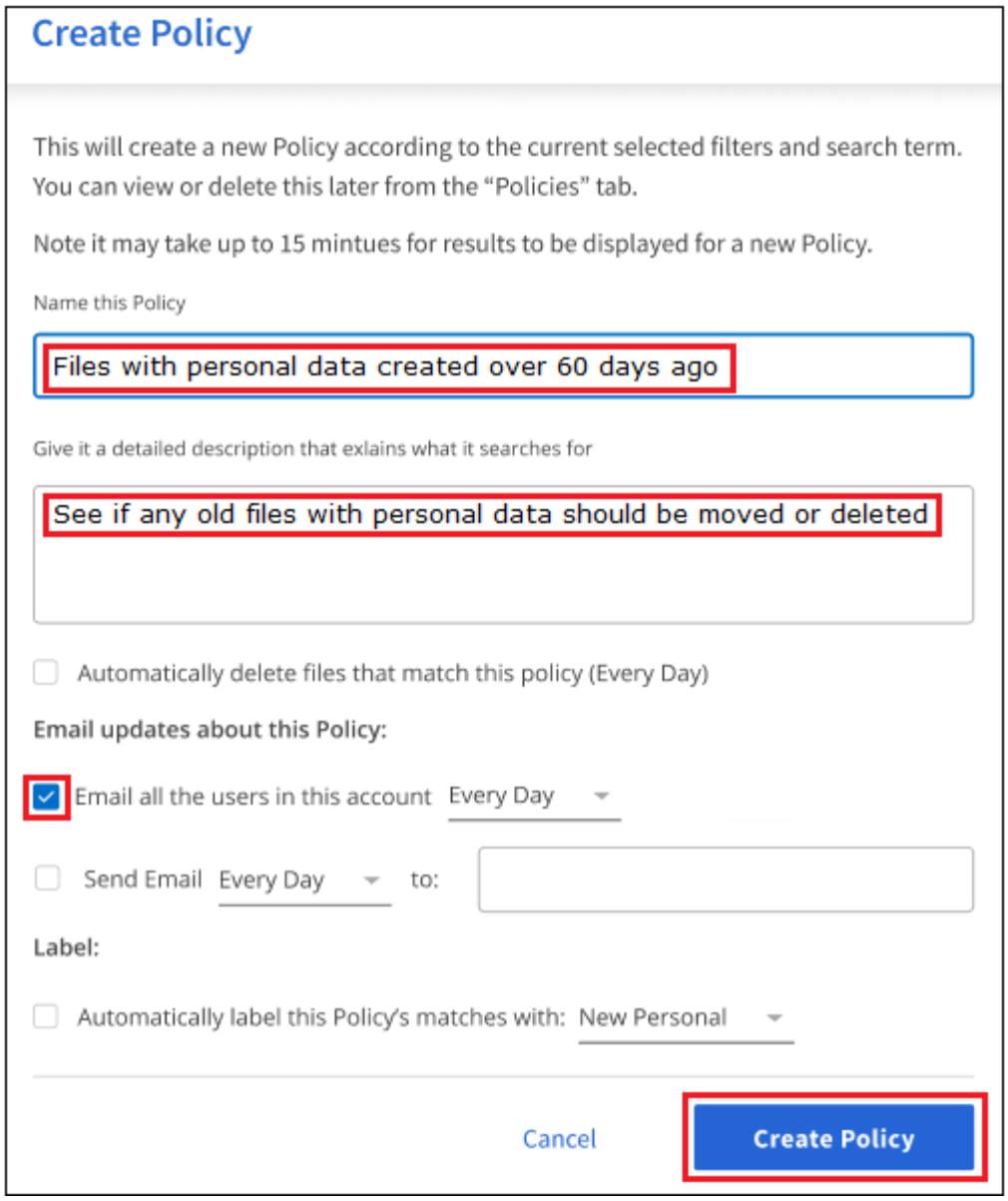
データを削除し、ポリシーの結果に基づいてAIPラベルを割り当てるアクションは、ファイルに対してのみ有効です。検索条件に一致するディレクトリは、自動的に削除することも、AIPラベルを割り当てることもできません。

手順

1. [データ調査] ページで、使用するすべてのフィルタを選択して検索を定義します。を参照してください "[データ調査 ページでデータをフィルタリングします"^] を参照してください。
2. 必要な方法でフィルタ特性をすべて設定したら、 [この検索からポリシーを作成する *] をクリックします。



3. ポリシーに名前を付け、そのポリシーで実行できるその他のアクションを選択します。
   a. 一意の名前と説明を入力します。
   b. 必要に応じて、このチェックボックスをオンにすると、ポリシーのパラメータに一致するファイルが自動的に削除されます。の詳細を確認してください ポリシーを使用してソースファイルを削除しています。
   c. 必要に応じて、アカウントのBlueXPユーザーに通知メールを送信する場合は、このチェックボックスをオンにして、メールの送信間隔を選択します。の詳細を確認してください ポリシーの結果に基づいて E メールアラートを送信する。
   d. 必要に応じて、他のユーザに通知Eメールを送信する場合はチェックボックスをオンにし、Eメールアドレスを20個まで入力して、Eメールの送信間隔を選択します。
   e. 必要に応じて、このチェックボックスをオンにすると、ポリシーパラメータに一致するファイルに AIP ラベルが自動的に割り当てられ、ラベルが選択されます。（AIP ラベルがすでに統合されている場合のみ。の詳細を確認してください "AIP ラベル". ）
   f. [ポリシーの作成 *] をクリックします。



結果

[ポリシー] タブに新しいポリシーが表示されます。

準拠していないデータが見つかった場合にEメールアラートを送信

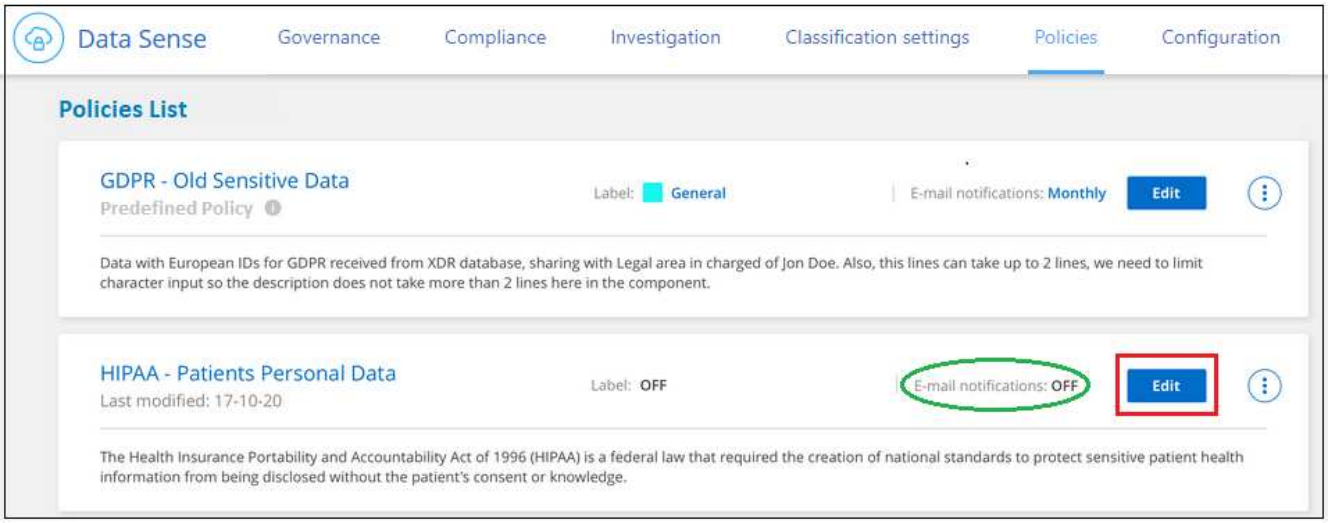
BlueXPの分類では、特定の重要なポリシーで結果が返されたときにアカウントのBlueXPユーザにEメールアラートを送信できるため、データを保護するための通知を受け取ることができます。E メール通知は、日単位、週単位、または月単位で送信することができます。また、BlueXPアカウントではなく、最大20個のメールアドレスに電子メールアラートを送信することもできます。

この設定は、ポリシーの作成時または任意のポリシーの編集時に設定できます。

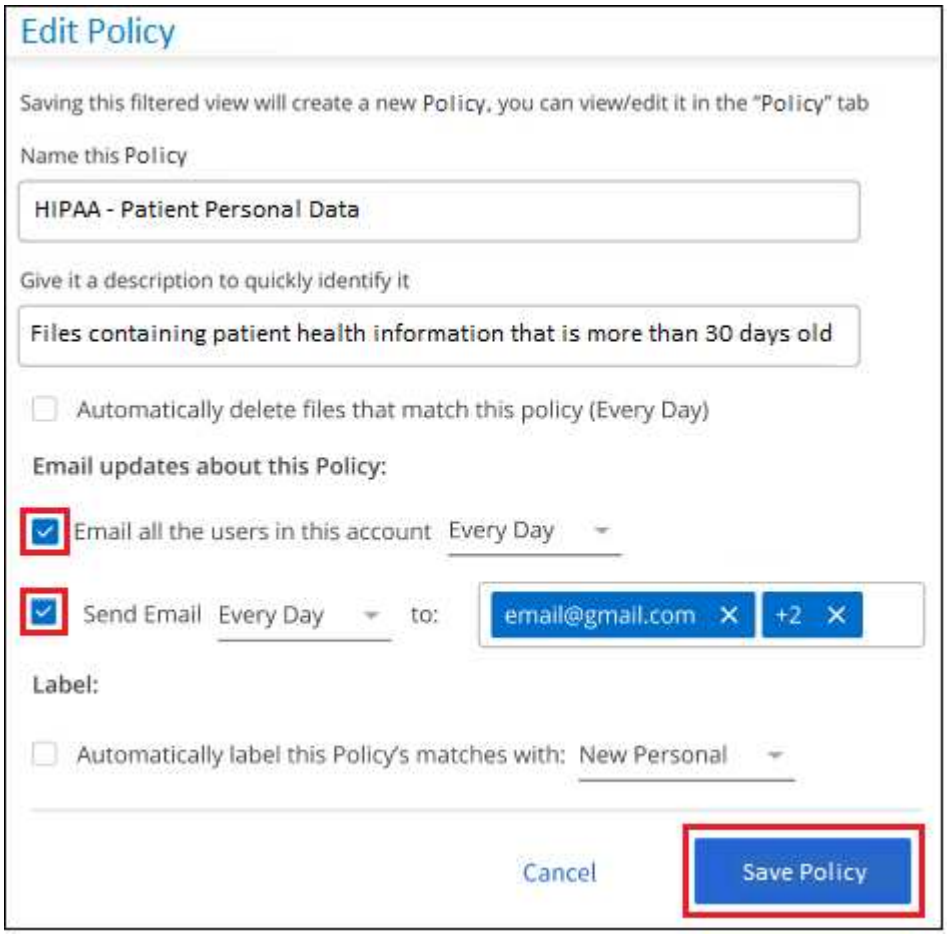
既存のポリシーにメールの更新を追加するには、次の手順を実行します。

手順

1. [ポリシーリスト] ページで、電子メール設定を追加（または変更）するポリシーの [編集 *] をクリックします。



2. Edit Policyページで、次の手順を実行します。
   a. BlueXPアカウントのユーザーに通知メールを送信する場合は、[このアカウントのすべてのユーザーに電子メールを送信する]チェックボックスをオンにし、電子メールの送信間隔を選択します(たとえば、**Every Day**)。
   b. 他のユーザに通知メールを送信する場合は、[電子メールの送信]チェックボックスをオンにし、電子メールを送信する間隔を選択して、最大20個の電子メールアドレスを入力します。



3. ［* ポリシーの保存 *］ をクリックすると、電子メールの送信間隔が ［ ポリシー概要 ］ に表示されます。

結果

最初の電子メールは、ポリシーからの結果がある場合に送信されます。ただし、ポリシーの条件を満たすファイルがある場合に限ります。通知メールに個人情報は送信されません。E メールには、ポリシーの条件に一致するファイルがあり、ポリシーの結果へのリンクが記載されています。

ポリシーを使用したソースファイルの自動削除

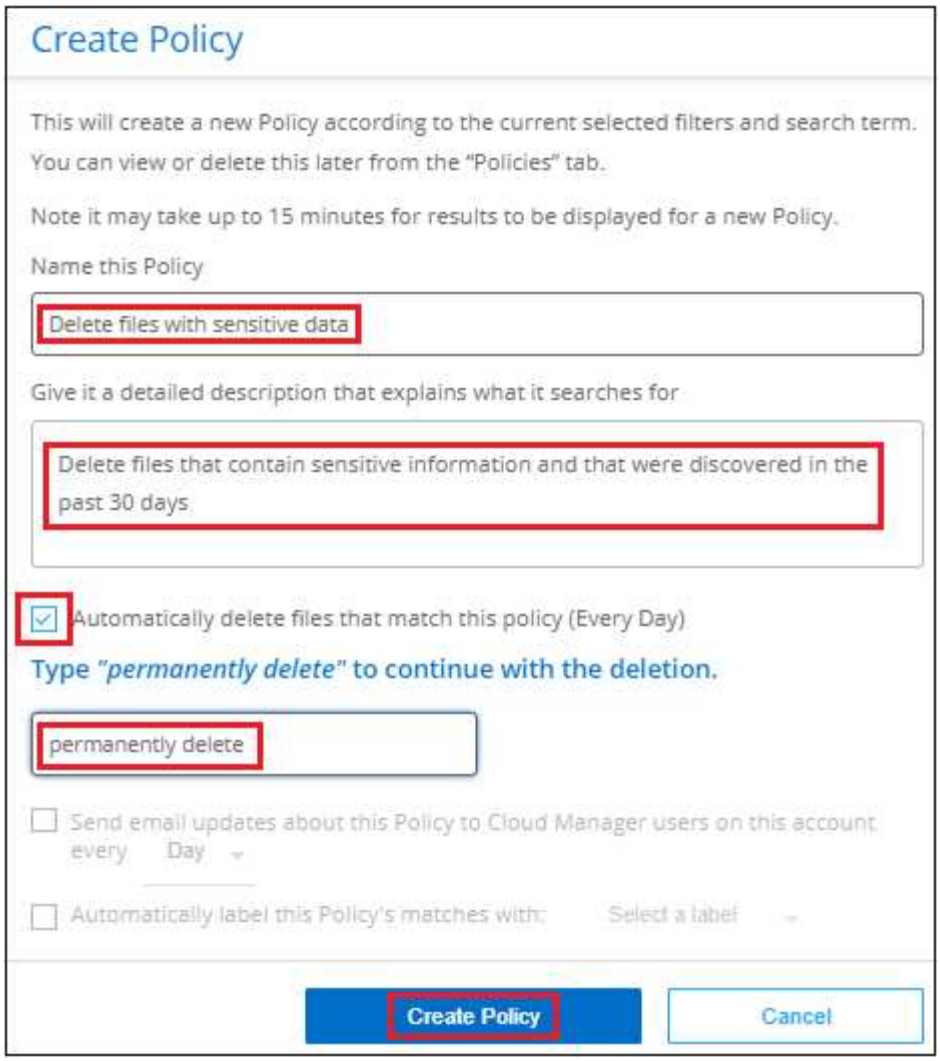
カスタムポリシーを作成して、ポリシーに一致するファイルを削除できます。たとえば、過去30日間にBlueXPの分類によって検出された機密情報を含むファイルを削除できます。

ファイルを自動的に削除するポリシーを作成できるのはアカウント管理者だけです。

ポリシーに一致するすべてのファイルは、 1 日に 1 回完全に削除されます。

手順

1. [データ調査] ページで、使用するすべてのフィルタを選択して検索を定義します。を参照してください "[データ調査 ページでデータをフィルタリングします"^] を参照してください。
2. 必要な方法でフィルタ特性をすべて設定したら、 [この検索からポリシーを作成する *] をクリックします。
3. ポリシーに名前を付け、そのポリシーで実行できるその他のアクションを選択します。
   a. 一意の名前と説明を入力します。
   b. このポリシーに一致するファイルを自動的に削除する] チェックボックスをオンにし、「 * permanently delete * 」と入力して、このポリシーによってファイルが完全に削除されることを確認します。
   c. [ポリシーの作成 *] をクリックします。



結果

[ポリシー] タブに新しいポリシーが表示されます。ポリシーに一致するファイルは、ポリシーの実行時に 1 日に 1 回削除されます。

で削除されたファイルのリストを確認できます "[アクションステータス（ Actions Status ） パネル"]。

ポリシーを使用した**AIP**ラベルの自動割り当て

AIP ラベルは、ポリシーの条件を満たすすべてのファイルに割り当てることができます。ポリシーの作成時に AIP ラベルを指定することも、ポリシーの編集時にラベルを追加することもできます。

BlueXPで分類されたファイルがスキャンされると、ラベルがファイルに追加または更新され続けます。

ラベルがすでにファイルに適用されているかどうか、およびラベルの分類レベルによって、ラベルを変更するときに次のアクションが実行されます。

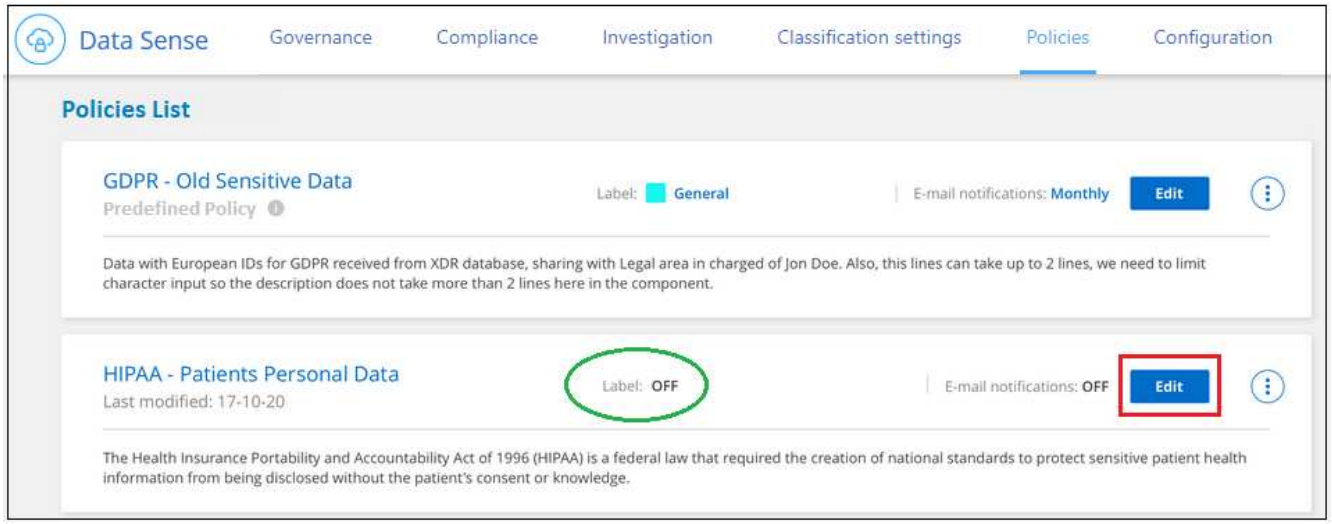
ファイルの内容	作業
にはラベルがありません	ラベルが追加されます
下位レベルの分類の既存のラベルがあります	上位レベルのラベルが追加されます

ファイルの内容	作業
より高いレベルの分類の既存のラベルがあります	上位レベルのラベルが保持されます
手動とポリシーの両方でラベルが割り当てられます	上位レベルのラベルが追加されます
2 つのポリシーによって 2 つの異なるラベルが割り当てられます	上位レベルのラベルが追加されます

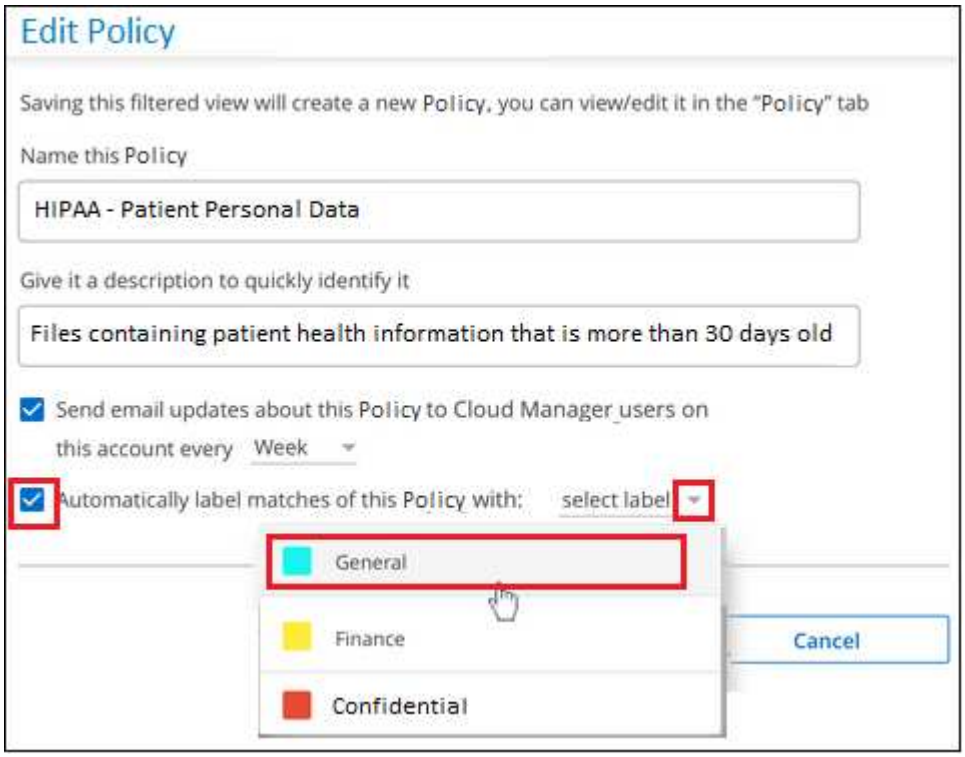
AIP ラベルを既存のポリシーに追加する手順は、次のとおりです。

手順

1. [ポリシーリスト] ページで、 AIP ラベルを追加（または変更）するポリシーの **Edit** をクリックします。



2. [ポリシーの編集] ページで、 [ポリシー] パラメータに一致するファイルの自動ラベルを有効にするチェックボックスをオンにして、ラベル（ **General** など）を選択します。



3. [ポリシーの保存 *] をクリックすると、 [ポリシー概要] にラベルが表示されます。

> ポリシーにラベルが設定されていても、ラベルが AIP から削除されている場合、ラベル名はオフになり、ラベルは割り当てられなくなります。

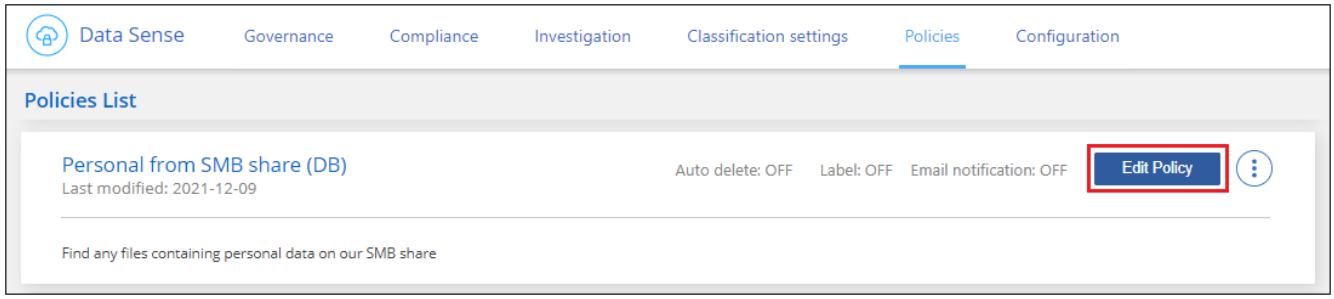
ポリシーの編集

前の手順で作成した既存のポリシーの条件を変更できます。これは、特定のパラメータを追加または削除するためにクエリ（フィルタを使用して定義した項目）を変更する場合に特に便利です。

定義済みポリシーでは、電子メール通知が送信されるかどうか、およびAIPラベルが追加されるかどうかだけを変更できます。その他の値は変更できません。

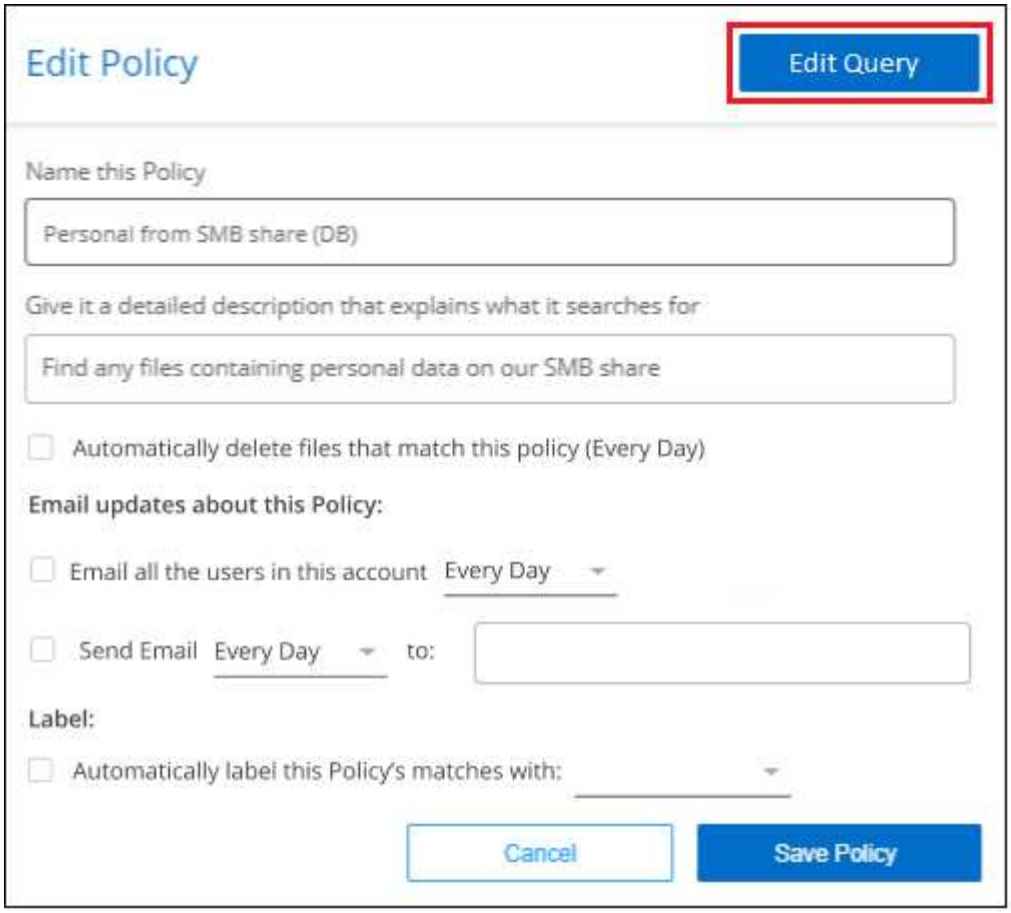
手順

1. [ポリシーリスト]ページで、変更するポリシーの*Edit*をクリックします。



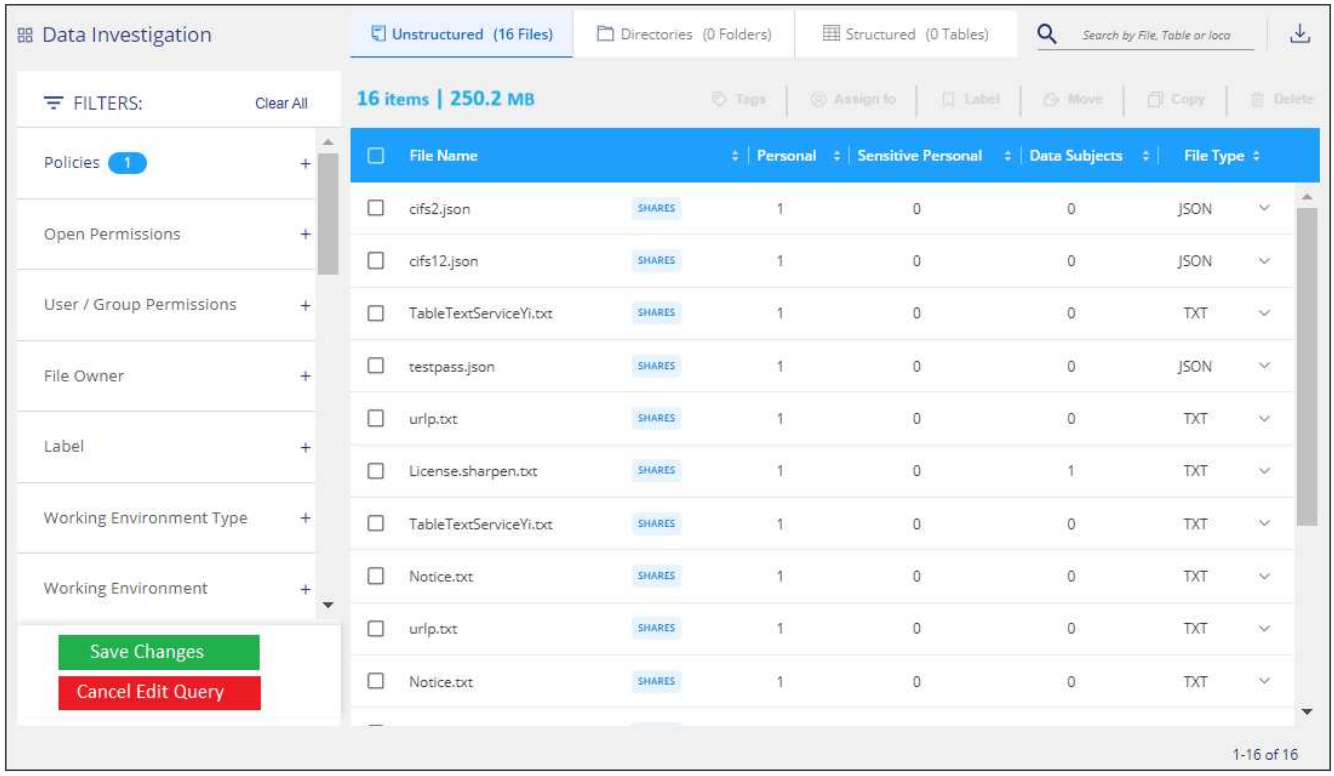
2. このページの項目（名前、概要 、電子メール通知が送信されているかどうか、およびAIPラベルが追加されているかどうか）を変更する場合は、変更を行って*ポリシーの保存*をクリックします。

   保存されたクエリのフィルタを変更する場合は、[クエリの編集]をクリックします。



ページの[クエリの編集]ボタンを選択するスクリーンショット。"]

3. そのクエリーを定義する[調査]ページで、フィルタを追加、削除、またはカスタマイズしてクエリーを編集し、[変更の保存*]をクリックします。



結果

ポリシーはただちに変更されます。そのポリシーに定義されたアクションは、電子メールの送信、AIPラベルの追加、またはファイルの削除のいずれかが、次の内部で実行されます。

ポリシーの削除

作成したカスタムポリシーが不要になった場合は削除できます。事前定義されたポリシーは削除できません。

ポリシーを削除するには、をクリックします ボタン"] ボタンをクリックして特定のポリシーを削除し、確認ダイアログでもう一度 ［* ポリシーの削除 *］ をクリックします。

事前定義されたポリシーのリスト

BlueXPは分類され、次のシステム定義のポリシーが提供されます。

名前	説明	ロジック
S3公開プライベートデータ	個人または機密性の高い個人情報を含む S3 オブジェクト。オープンなパブリック読み取りアクセスが許可されます。	S3 Public となり、個人情報または機密情報が含まれます
PCI DSS - 30日間の古いデータ	クレジットカード情報を含むファイル。最終更新日は 30 日前です。	クレジットカードと最終変更日が 30 日以上含まれます
HIPAA：30日間のデータを停滞させます	ヘルス情報が含まれるファイル。最終更新日は 30 日前です。	健康データを含む（ HIPAA レポートと同様に定義されている） そして、最終変更日は 30 日です
プライベートデータ：7年以上前に停滞しています	個人情報または機密性の高い個人情報を含むファイル。最終更新日は 7 年前に変更されました。	個人情報または機密性の高い個人情報を含むファイル。最終更新日は 7 年前に変更されました
GDPR -欧州市民	EU加盟国の市民の5つ以上のIDを含むファイル、またはEU加盟国の市民のIDを含むDBテーブル。	（1）EU市民またはDBテーブルの5つ以上の識別子を含むファイル。列の15%を超える行と、1つの国のEU識別子が含まれています。（欧州諸国のいずれかの国の識別子。ブラジル、カリフォルニア、米国 SSN 、イスラエル、南アフリカを含まない）
CCPA -カリフォルニア州在住	この識別子を持つ10を超えるカリフォルニアドライバのライセンス識別子またはDBテーブルを含むファイル。	カリフォルニアドライバのライセンスIDが10個を超えるファイル、またはカリフォルニアドライバのライセンスを含むDBテーブルが含まれているファイル
データ主体名-高リスク	50 を超えるデータ主体名を持つファイル。	50 を超えるデータ主体名を持つファイル
Eメールアドレス-リスクが高くなっています	E メールアドレスが 50 を超えるファイル、または E メールアドレスを含む行の 50% を超える DB 列	E メールアドレスが 50 を超えるファイル、または E メールアドレスを含む行の 50% を超える DB 列
個人データ-高いリスク	個人データ識別子が 20 個を超えるファイル、または個人データ識別子を含む行の 50% を超える DB 列。	20 以上の個人用のファイル、または個人を含む行の 50% を超える DB 列を持つファイル

名前	説明	ロジック
機密性の高い個人データ-高いリスク	機密性の高い個人データ識別子が 20 を超えるファイル、または機密性の高い個人データを含む行の 50% を超える DB 列。	機密性の高い個人用のファイル、または機密性の高い個人を含む行の 50% 以上を含む DB 列

プライベートデータを管理

BlueXPは、さまざまな方法でプライベートデータを管理できます。一部の機能を使用すると、データの移行準備が簡単になります。また、他の機能を使用してデータを変更することもできます。

- 特定のデータのコピーを作成して別の NFS の場所に移動する場合は、デスティネーションの NFS 共有にファイルをコピーできます。
- ONTAP ボリュームを新しいボリュームにクローニングしたり、選択したファイルだけをソースボリュームから新しいクローンボリュームに含めたりできます。これは、データを移行する際に元のボリュームから特定のファイルを除外する場合に便利です。
- ソースリポジトリから特定の保存先にあるディレクトリにファイルをコピーして同期できます。これは、ソースファイルに対して何らかの最終的なアクティビティが行われている間に、あるソースシステムから別のソースシステムにデータを移行する場合に便利です。
- BlueXP分類でスキャンするソースファイルを任意のNFS共有に移動できます。
- 安全でないようであるか危険すぎると思われるファイルを削除して、ストレージシステムに残すことも、重複として識別したファイルを削除することもできます。

> - このセクションで説明する機能は、データソースに対して完全な分類スキャンを実行することを選択した場合にのみ使用できます。マッピングのみのスキャンを実行したデータソースでは、ファイルレベルの詳細は表示されません。
> - Google Driveアカウントのデータでは、現時点でこれらの機能を使用することはできません。

ソースファイルをコピーします

BlueXP分類でスキャンしている任意のソースファイルをコピーできます。実行しようとしている処理に応じて、次の 3 種類のコピー処理があります。

- * 同一または異なるボリュームまたはデータソースからデスティネーション NFS 共有にファイル * をコピーします。

  これは、特定のデータのコピーを作成して別の NFS の場所に移動する場合に便利です。

- * ONTAP ボリュームのクローンを同じアグリゲート内の新しいボリュームに作成します。新しいクローンボリュームには、ソースボリュームから選択されたファイルのみを含めます。

  これは、データを移行する際に元のボリュームから特定のファイルを除外する場合に便利です。このアクションではを使用します "NetApp FlexClone" ボリュームをすばやく複製し、 * 選択しなかったファイルを削除する機能。

- * 単一のソースリポジトリ（ ONTAP ボリューム、 S3 バケット、 NFS 共有など）から特定のデスティネーション（ターゲット）にあるディレクトリにファイルをコピーして同期します。

  これは、あるソースシステムから別のシステムにデータを移行する場合に便利です。最初のコピーの後、設定したスケジュールに基づいて変更されたデータが同期されます。このアクションではを使用します "NetApp BlueXPのコピーと同期" データをソースからターゲットにコピーおよび同期する機能。

ソースファイルを**NFS**共有にコピーする

BlueXP分類でスキャンしているソースファイルは、任意のNFS共有にコピーできます。NFS共有をBlueXPに統合する必要はありません。選択したすべてのファイルがコピーされるNFS共有の名前を指定するだけです `<host_name>:/<share_path>`。

データベースに存在するファイルはコピーできません。

要件

- ファイルをコピーするには、アカウント管理者またはワークスペース管理者の役割が必要です。
- ファイルをコピーするには、デスティネーションNFS共有でBlueXP分類インスタンスからのアクセスが許可されている必要があります。
- 一度に1～100,000個のファイルをコピーできます。

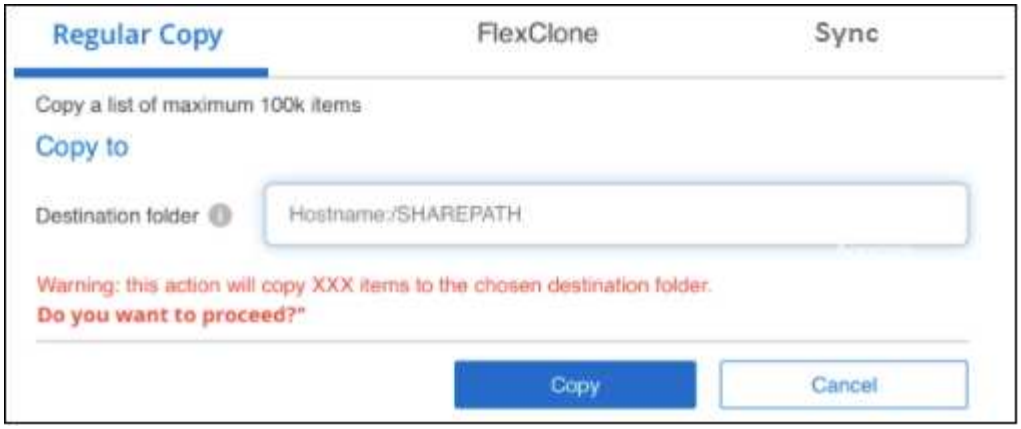
手順

1. [データ調査結果] ペインで、コピーするファイルを選択し、 [* コピー] をクリックします。

ページからコピーするファイルを選択する方法と、 [コピー] ボタンを示すスクリーンショット。"]

   - 個々のファイルを選択するには、各ファイル（ Volume_1）。
   - 現在のページのすべてのファイルを選択するには、タイトル行（ File Name ）。
   - すべてのページのすべてのファイルを選択するには、タイトル行（ File Name ）をクリックし、ポップアップメッセージにと入力します All 20 Items on this page selected Select all Items in list (63K Items)をクリックし、リスト（ xxx 項目）のすべての項目を選択 * をクリックします。

2. _ ファイルのコピー _ ダイアログで * 標準コピー * タブを選択します。



3. 選択したすべてのファイルをコピーする NFS 共有の名前を「 <host_name> ： /<share_path>` 」の形式で入力し、「 * Copy * 」をクリックします。

   コピー処理のステータスを示すダイアログが表示されます。

コピー処理の進捗状況はで確認できます "[アクションステータス（ Actions Status ） パネル"]。

ファイルのメタデータの詳細を表示するときに、個々のファイルをコピーすることもできます。[ファイルのコピー] をクリックします。

ページのファイルのメタデータ詳細から [ファイルのコピー] ボタンを選択したことを示すスクリーンショット。"]

新しいボリュームへのボリュームデータのクローニング

BlueXPでスキャンしている既存のONTAP ボリュームは、netapp_FlexClone_functionalityを使用してクローニングできます。これにより、選択したファイルのみを含めて、ボリュームをすばやく複製できます。この機能は、データを移行する際に元のボリュームから特定のファイルを除外する場合や、テスト用にボリュームのコピーを作成する場合に便利です。

新しいボリュームは、ソースボリュームと同じアグリゲート内に作成されます。このタスクを開始する前に、アグリゲート内にこの新しいボリューム用の十分なスペースがあることを確認してください。必要に応じて、ストレージ管理者にお問い合わせください。

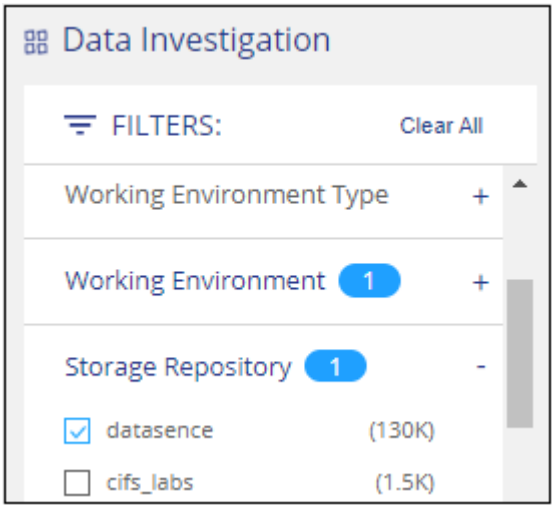
- 注： * FlexGroup ボリュームは FlexClone でサポートされていないため、クローンを作成できません。

要件

- ファイルをコピーするには、アカウント管理者またはワークスペース管理者の役割が必要です。
- 少なくとも20個のファイルを選択する必要があります。
- 選択したファイルはすべて同じボリュームにあり、ボリュームがオンラインである必要があります。
- ボリュームは、 Cloud Volumes ONTAP またはオンプレミスの ONTAP システムから選択する必要があります。他のデータソースは現在サポートされていません。
- クラスタに FlexClone ライセンスがインストールされている必要があります。このライセンスは、 Cloud Volumes ONTAP システムにデフォルトでインストールされます。

手順

1. [データ調査] ペインで、 1 つの * 作業環境 * と 1 つの * ストレージリポジトリ * を選択してフィルタを作成し、すべてのファイルが同じ ONTAP ボリュームにあることを確認します。



新しいボリュームにクローニングするファイルだけが表示されるように、他のフィルタを適用します。

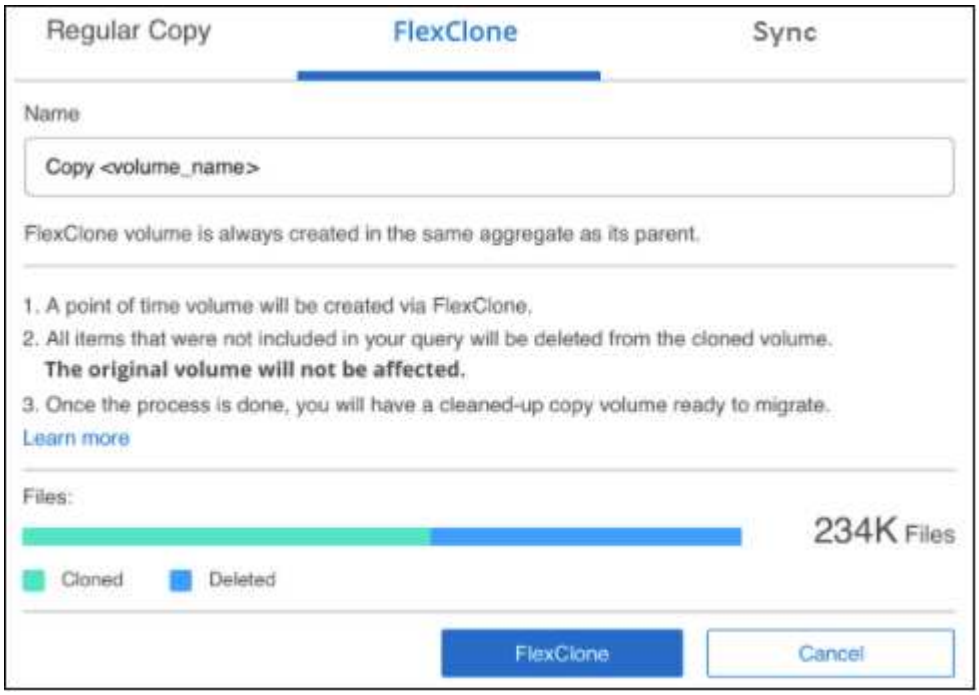
2. ［調査結果］ ペインで、複製するファイルを選択し、 ［* コピー *］ をクリックします。

ページからコピーするファイルを選択する方法と、 [コピー] ボタンを示すスクリーンショット。"]

   - 個々のファイルを選択するには、各ファイル（ Volume_1）。
   - 現在のページのすべてのファイルを選択するには、タイトル行（ File Name ）。
   - すべてのページのすべてのファイルを選択するには、タイトル行（ File Name ）をクリックし、ポップアップメッセージにと入力します All 20 Items on this page selected Select all Items in list (63K Items)をク

リックし、リスト（ xxx 項目）のすべての項目を選択 * をクリックします。

3. _ ファイルのコピー _ ダイアログで * FlexClone * タブを選択します。このページには、ボリュームからクローニングされるファイル（選択したファイル）の総数と、クローンボリュームに含まれている / 削除されていないファイル（選択しなかったファイル）の数が表示されます。



4. 新しいボリュームの名前を入力し、 * FlexClone * をクリックします。

   クローン処理のステータスを示すダイアログが表示されます。

結果

新しいクローンボリュームは、ソースボリュームと同じアグリゲート内に作成されます。

クローニング処理の進捗状況はで確認できます "[アクションステータス（ Actions Status ） パネル"]。

ソースボリュームが配置されている作業環境でBlueXPの分類を有効にしたときに最初に*[すべてのボリュームをマッピングして分類]*を選択した場合は、新しいクローンボリュームが自動的にスキャンされます。最初にこれらのいずれかを使用しなかった場合は、この新しいボリュームをスキャンする必要があります "ボリュームのスキャンを手動で有効にします"。

ソースファイルをターゲットシステムにコピーして同期する

BlueXP分類でスキャンしているソースファイルを、サポートされている非構造化データソースから特定のターゲットデスティネーションの場所にあるディレクトリにコピーできます ("BlueXPのコピーと同期でサポートされるターゲットの場所"）。最初のコピー後、ファイル内で変更されたデータは、設定したスケジュールに基づいて同期されます。

これは、あるソースシステムから別のシステムにデータを移行する場合に便利です。このアクションではを使用します "NetApp BlueXPのコピーと同期" データをソースからターゲットにコピーおよび同期する機能。

> データベース、 OneDrive アカウント、 SharePoint アカウントにあるファイルはコピーおよび同期できません。

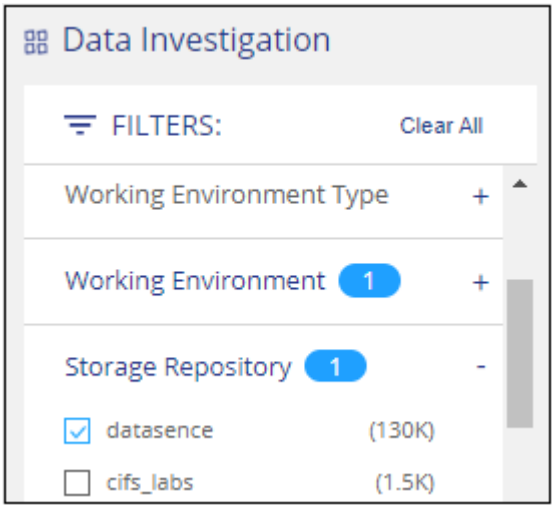
要件

- ファイルをコピーして同期するには、アカウント管理者またはワークスペース管理者の役割が必要です。
- 少なくとも20個のファイルを選択する必要があります。
- 選択したファイルはすべて、同じソースリポジトリ（ ONTAP ボリューム、 S3 バケット、 NFS 共有、 CIFS 共有など）にある必要があります。
- BlueXPのコピーおよび同期サービスをアクティブ化し、ソースシステムとターゲットシステム間でファイルを転送するためのデータブローカーを少なくとも1つ設定する必要があります。から、BlueXPのコピーと同期の要件を確認します "Quick Start 概要 の略"。

  BlueXPのコピーおよび同期サービスでは、同期関係ごとにサービス料金が別途発生します。データブローカーをクラウドに導入した場合はリソース料金が発生します。

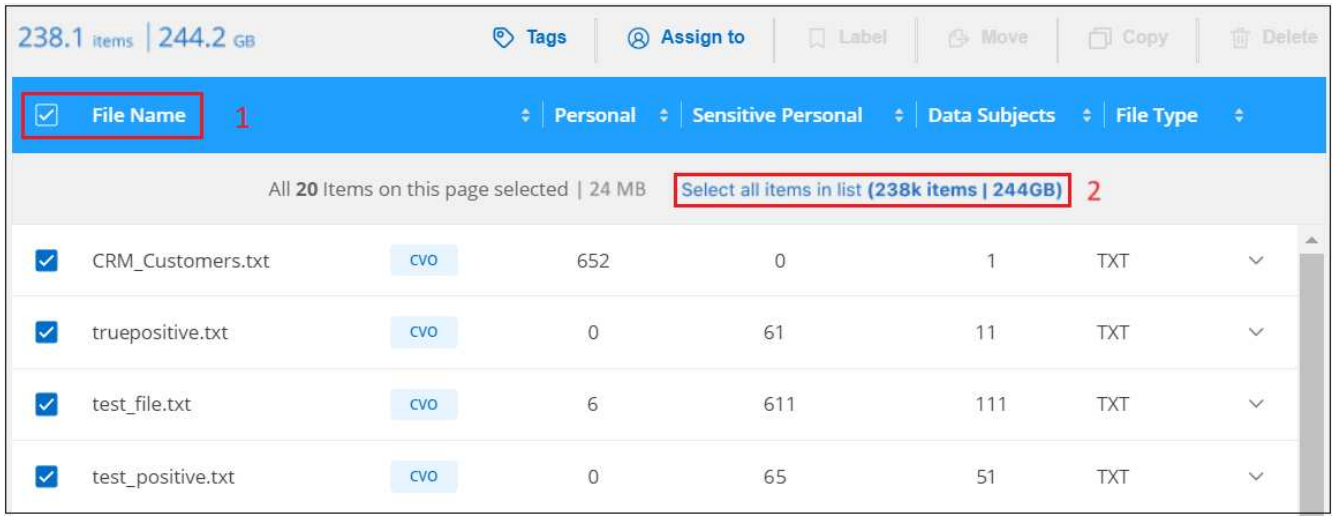
手順

1. [データの調査] ペインで、 1 つの * 作業環境 * と 1 つの * ストレージリポジトリ * を選択してフィルタを作成し、すべてのファイルが同じリポジトリにあることを確認します。



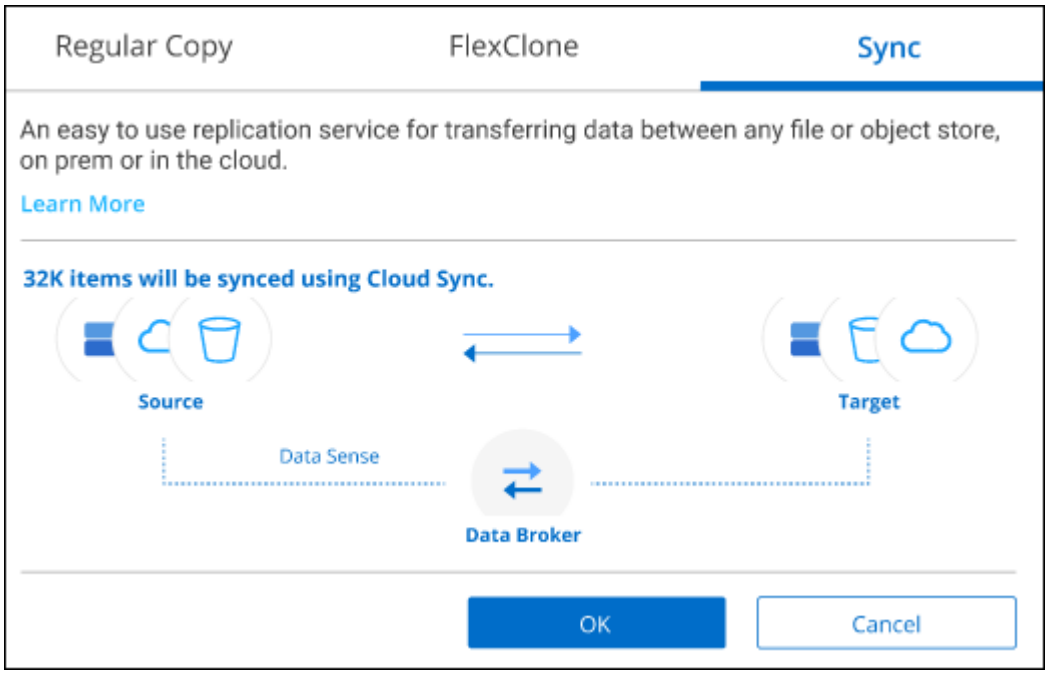
   他のフィルタを適用して、コピー先システムに同期するファイルだけが表示されるようにします。

2. [調査結果] ウィンドウ枠で、タイトル行のボックスをオンにして、すべてのページのすべてのファイルを選択します（ File Name ）をクリックし、ポップアップメッセージに入力します All 20 Items on this page selected Select all Items in list (63K Items) [リスト内のすべての項目を選択（ * xxx 項目）] をクリックし、 [* コピー *] をクリックします。



ページからコピーするファイルを選択する方法と、 [コピー] ボタンを示すスクリーンショット。"]

3. _ ファイルのコピー _ ダイアログで * 同期 * タブを選択します。



ダイアログを示すスクリーンショットで、 [同期] オプションを選択できます。"]

4. 選択したファイルを保存先に同期してもよい場合は、「 * OK * 」をクリックします。

   BlueXPのコピーと同期のUIがBlueXPで開きます。

   同期関係を定義するよう求められます。ソースシステムには、BlueXPの分類で選択したリポジトリとファイルがあらかじめ設定されています。

5. ターゲットシステムを選択し、使用するデータブローカーを選択（または作成）する必要があります。から、BlueXPのコピーと同期の要件を確認します "Quick Start 概要 の略"。

結果

ファイルはターゲットシステムにコピーされ、定義したスケジュールに基づいて同期されます。1 回限りの同期を選択した場合、ファイルは 1 回だけコピーされ、同期されます。定期的な同期を選択した場合は、スケ

ジュールに基づいてファイルが同期されます。フィルタを使用して作成したクエリに一致する新しいファイルがソースシステムによって追加されると、これらの _new_files がコピー先にコピーされ、後で同期されることに注意してください。

BlueXPの分類から起動すると、通常のBlueXPのコピー処理と同期処理の一部が無効になることに注意してください。

- 「ソース上のファイルを削除」または「ターゲット上のファイルを削除」ボタンは使用できません。
- レポートの実行が無効になっています。

ソースファイルを**NFS**共有に移動する

BlueXP分類でスキャンするソースファイルを任意のNFS共有に移動できます。NFS共有をBlueXPの分類と統合する必要はありません。

必要に応じて、移動したファイルの場所にブレッドクラムファイルを残すことができます。ブレッドクラムファイルは、ファイルが元の場所から移動された理由をユーザーが理解するのに役立ちます。移動された各ファイルについて、システムは「<filename>-ブレッドクラム-<date>.txt」という名前のソース位置にブレッドクラムファイルを作成します。ダイアログボックスで、ブレッドクラムファイルに追加されるテキストを追加して、ファイルが移動された場所とファイルを移動したユーザを示すことができます。

ソースファイルのサブディレクトリ構造は、ファイルの移動時に移動先の共有に再作成されるため、ファイルの移動元がわかりやすくなります。同じ名前のファイルがコピー先に存在する場合、そのファイルは移動されません。

データベースに存在するファイルは移動できません。

要件

- ファイルを移動するには、アカウント管理者またはワークスペース管理者の役割が必要です。
- ソースファイルは、オンプレミスのONTAP 、Cloud Volumes ONTAP 、Azure NetApp Files 、ファイル共有、SharePoint Onlineのデータソースに配置できます。
- 一度に移動できるファイルの最大数は1、500万です。
- 50 MB以下のファイルのみが移動されます。
- デスティネーションNFS共有で、BlueXP分類インスタンスのIPアドレスからのアクセスを許可する必要があります。

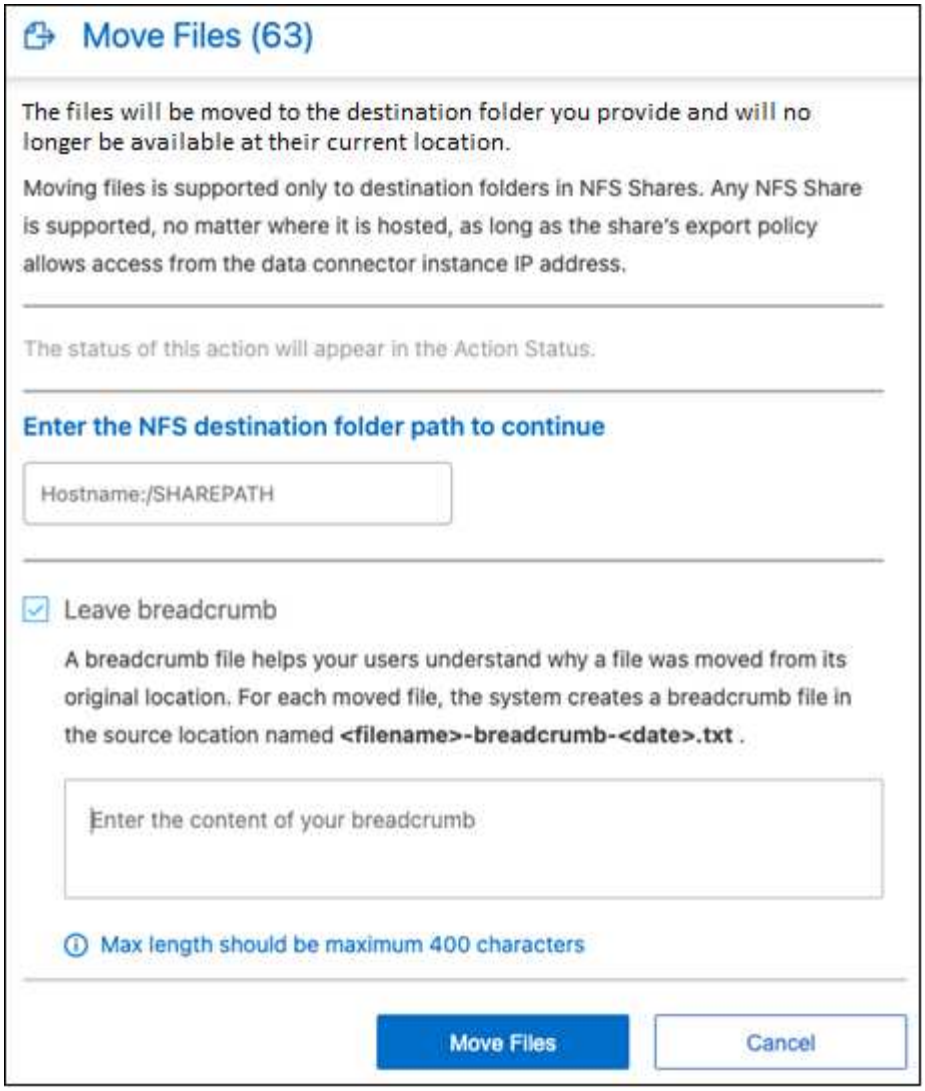
手順

1. [データ調査結果] ペインで、移動するファイルを選択します。

ページから [移動] ボタンをクリックします。"]

- 個々のファイルを選択するには、各ファイル（ Volume_1）。
- 現在のページのすべてのファイルを選択するには、タイトル行（ File Name ）。
- すべてのページのすべてのファイルを選択するには、タイトル行（ File Name ）をクリックし、ポップアップメッセージにと入力します All 20 Items on this page selected Select all Items in list (63K Items)をクリックし、リスト（ xxx 項目）のすべての項目を選択 * をクリックします。

2. ボタンバーで、 * 移動 * をクリックします。



3. _Move Files_Dialogに、選択したすべてのファイルを移動するNFS共有の名前を「<host_name>：/<share_path>`」の形式で入力します。
4. ブレッドクラムファイルを残す場合は、_ブレッドクラム履歴_ボックスをオンにします。ダイアログボックスにテキストを入力して、ファイルが移動された場所、ファイルを移動したユーザー、およびファイルが移動された理由などのその他の情報を指定できます。
5. 「ファイルの移動」をクリックします。

ファイルのメタデータの詳細を表示するときに、個々のファイルを移動することもできます。「 * ファイルを移動 * 」をクリックします。

ページのファイルのメタデータ詳細から [ファイルの移動] ボタンを選択したことを示すスクリーンショット。"]

ソースファイルを削除します

ストレージ・システムに残すのに安全でない ' またはリスクが高すぎるソース・ファイルを完全に削除したり ' 重複として識別したソース・ファイルを削除したりすることができますこの操作は永続的であり、元に戻すことも復元することもできません。

［調査］ペインから手動でファイルを削除することも、手動でファイルを削除することもできます "ポリシーを使用して自動的に作成"。

> データベースに存在するファイルは削除できません。その他のすべてのデータソースがサポートされます。

ファイルを削除するには、次の権限が必要です。

- NFSデータの場合-書き込み権限でエクスポートポリシーを定義する必要があります。
- CIFSデータの場合- CIFSクレデンシャルに書き込み権限が必要です。
- S3 データの場合 - IAM ロールに次の権限を含める必要があります。「 3 ： DeleteObject 」

ソースファイルを手動で削除する

要件

- ファイルを削除するには、アカウント管理者またはワークスペース管理者の役割が必要です。
- 一度に削除できるファイルの最大数は 100 、 000 です。

手順

1. [データ調査結果] ペインで、削除するファイルを選択します。

ページの [削除] ボタン。"]

- 個々のファイルを選択するには、各ファイル（ Volume_1）。
- 現在のページのすべてのファイルを選択するには、タイトル行（ File Name ）。
- すべてのページのすべてのファイルを選択するには、タイトル行（ File Name ）をクリックし、ポップアップメッセージにと入力します All 20 Items on this page selected Select all Items in list (63K Items)をクリックし、リスト（ xxx 項目）のすべての項目を選択 * をクリックします。

2. ボタンバーで、 * 削除 * をクリックします。
3. 削除操作は永続的であるため ' 後続の _Delete File_Dialog に「 * permanently delete * 」と入力し ' * ファイルの削除 * をクリックする必要があります

削除処理の進捗状況はで確認できます "[アクションステータス（ Actions Status ） パネル"]。

ファイルのメタデータの詳細を表示するときに、個々のファイルを削除することもできます。[ファイルの削除] をクリックします。

ページのファイルのメタデータ詳細から [ファイルの削除] ボタンを選択したことを示すスクリーンショット。"]

コンプライアンスレポートを表示する

BlueXPの分類では、組織のデータプライバシープログラムのステータスを詳しく把握するために使用できるレポートが提供されます。

BlueXPの分類ダッシュボードには、デフォルトで、すべての作業環境、データベース、データソースのコン

プライアンスとガバナンスのデータが表示されます。一部の作業環境のデータのみを含むレポートを表示する場合は、 それらの作業環境を選択します。

- このセクションで説明するレポートは、データソースに対して完全な分類スキャンを実行することを選択した場合にのみ使用できます。マッピング専用スキャンを実行したデータソースでは、データマッピングレポートのみが生成されます。
- ネットアップは、BlueXPの分類によって特定される個人データや機密性の高い個人データの正確性を100%保証することはできません。必ずデータを確認して情報を検証してください。

プライバシーリスク評価レポート

プライバシーリスクアセスメントレポートには、GDPRやCCPAなどのプライバシー規制に必要な、組織のプライバシーリスクステータスの概要が記載されています。このレポートには次の情報が含まれます。

準拠ステータス

A 重要度スコア 機密性、個人、機密性の高い個人のいずれであっても、データの配信は可能です。

評価の概要

検出された個人データの種類とデータのカテゴリの内訳。

この評価のデータ主体

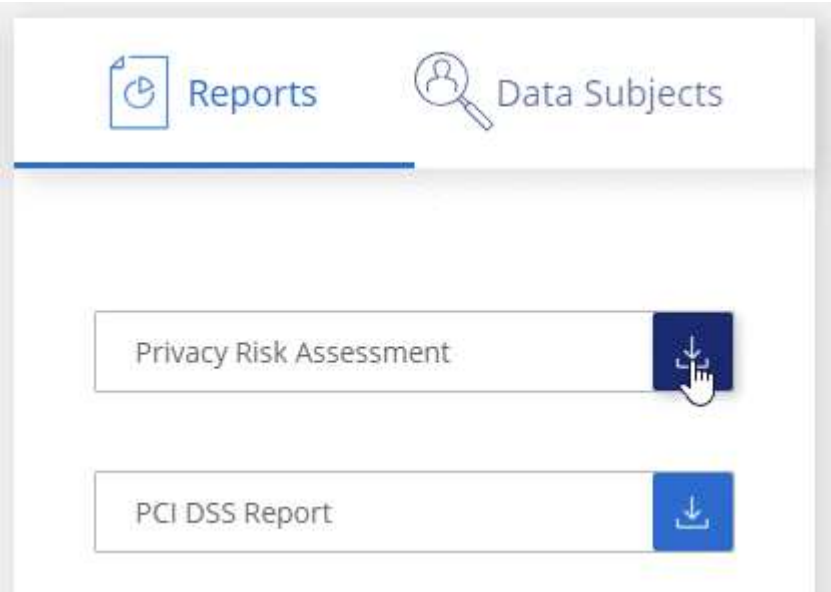
国 ID が見つかった場所別の人の数。

プライバシーリスクアセスメントレポートの生成

コンプライアンスタブに移動してレポートを生成します。

手順

1. BlueXPメニューで、* Governance > Classification *をクリックします。
2. **[Compliance]** をクリックし、 **[*Reports]** の下にある **[*Privacy Risk Assessment]** の横にあるダウンロードアイコンをクリックします。



タブのスクリーンショット。[レポート]

ペインに、[プライバシーリスクアセスメント]をクリックできることが示されています。"]

結果

BlueXPの分類によってPDFレポートが生成されます。このレポートを確認して、必要に応じて他のグループに送信できます。

重要度スコア

BlueXPの分類では、プライバシーリスク評価レポートの重大度スコアが、次の3つの変数に基づいて計算されます。

- すべてのデータの個人データの割合。
- すべてのデータの機密性の高い個人データの割合。
- データ主体を含むファイルの割合。国 ID 、社会保障番号、税務 ID 番号などの国 ID によって決定されます。

スコアの決定に使用されるロジックは次のとおりです。

重要度スコア	ロジック
0	3 つの変数はすべて 0% です
1.	変数の 1 つが 0% を超えています
2.	変数の 1 つが 3% を超えています
3.	2 つの変数が 3% を超えています
4.	3 つの変数が 3% を超えています
5.	変数の 1 つが 6% を超えています
6.	2 つの変数が 6% を超えています
7.	3 つの変数が 6% を超えています
8.	変数の 1 つが 15% を超えています
9.	2 つの変数が 15% を超えています
10.	3 つの変数が 15% を超えています

PCI DSS レポート

Payment Card Industry Data Security Standard （ PCI DSS ） Report は、クレジットカード情報のファイルへの配布を識別するのに役立ちます。このレポートには次の情報が含まれます。

概要

クレジットカード情報を含むファイル数と、作業環境。

暗号化

暗号化された作業環境または暗号化されていない作業環境にあるクレジットカード情報を含むファイルの割合。この情報は Cloud Volumes ONTAP に固有のものです。

ランサムウェアからの保護

ランサムウェアからの保護が有効になっている、または有効になっていない作業環境でのクレジットカード情報を含むファイルの割合。この情報は Cloud Volumes ONTAP に固有のものです。

保持

ファイルが最後に変更された期間。これは、クレジットカード情報を処理するよりも長く保持する必要がないために役立ちます。

クレジットカード情報の配布

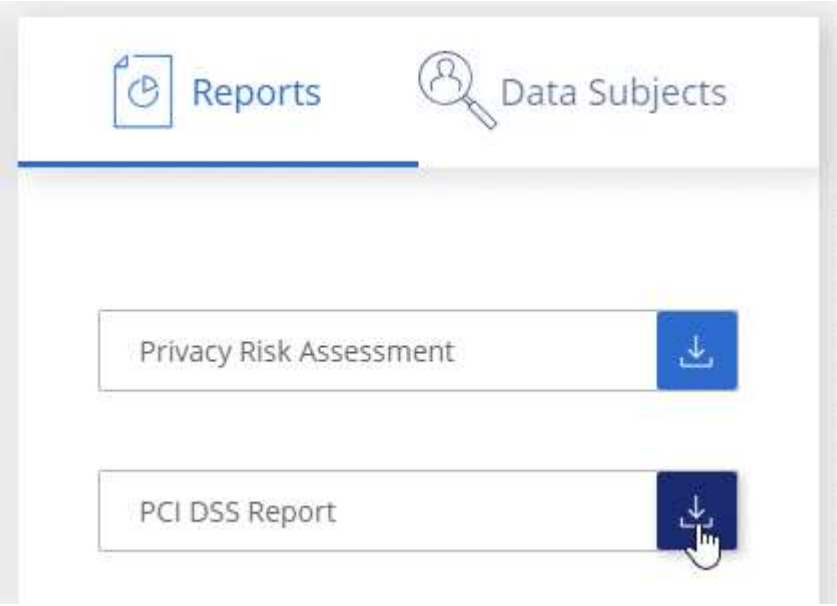
クレジットカード情報が見つかった作業環境、および暗号化とランサムウェアによる保護が有効になっているかどうか。

PCI DSSレポートの生成

コンプライアンスタブに移動してレポートを生成します。

手順

1. BlueXPメニューで、* Governance > Classification *をクリックします。
2. [* コンプライアンス *] をクリックし、 [* レポート] の下の [* PCI DSS レポート *] の横にあるダウンロード・アイコンをクリックします。



タブのスクリーンショット。[レポート]ペインに、[プライバシーリスクアセスメント]をクリックできることが示されています。"]

結果

BlueXPの分類によってPDFレポートが生成されます。このレポートを確認して、必要に応じて他のグループに送信できます。

HIPAA レポート

Health Insurance Portability and Accountability Act （ HIPAA ：医療保険の携行性と責任に関する法律）レポートは、健康に関する情報を含むファイルを特定するのに役立ちます。HIPAAデータプライバシー法を遵守するという組織の要件を支援するように設計されています。BlueXPの分類では、次のような情報が検索されます。

- ヘルス参照パターン
- ICD-10-CM 医療コード
- ICD-9-CM 医療コード
- HR -健全性カテゴリ
- ヘルスアプリケーションデータカテゴリ

このレポートには次の情報が含まれます。

概要

ヘルス情報が含まれているファイルの数と、作業環境。

暗号化

暗号化された作業環境または暗号化されていない作業環境にあるヘルス情報を含むファイルの割合。この情報は Cloud Volumes ONTAP に固有のものです。

ランサムウェアからの保護

ランサムウェアからの保護が有効になっている、または有効になっていない作業環境でのヘルス情報を含むファイルの割合。この情報は Cloud Volumes ONTAP に固有のものです。

保持

ファイルが最後に変更された期間。健常性の情報は、処理するまでに時間がかかることがないため、この方法が便利です。

健康情報の配布

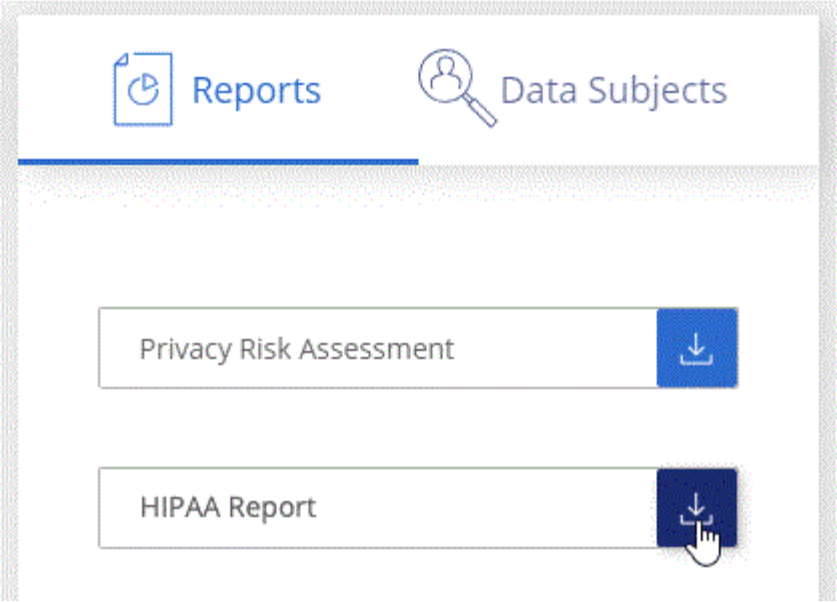
健常性の情報が見つかった作業環境、および暗号化とランサムウェアによる保護が有効になっているかどうか。

HIPAAレポートの生成

コンプライアンスタブに移動してレポートを生成します。

手順

1. BlueXPメニューで、* Governance > Classification *をクリックします。
2. [**Compliance]** をクリックし、 **[*Reports**] の下にある [**HIPAA Report**] の横にあるダウンロードアイコンをクリックします。



結果

BlueXPの分類によってPDFレポートが生成されます。このレポートを確認して、必要に応じて他のグループに送信できます。

データ主体アクセス要求とは

欧州 GDPR などのプライバシー規制により、データ主体（お客様や従業員など）は個人データにアクセスする権利が付与されます。データ主体がこの情報を要求すると ' これは dsar (データ主体アクセス要求) と呼ばれます組織は、これらの要求に「期日前に」、受領後 1 か月以内に対応する必要があります。

dsarに応答するには、件名のフルネームまたは既知の識別子(電子メールアドレスなど)を検索し、レポートをダウンロードします。このレポートは、企業が GDPR や同様のデータプライバシー法を遵守する必要がある場合に役立つように作成されています。

BlueXPの分類は**DSAR**への対応にどのように役立ちますか？

データ主体の検索を実行すると、BlueXPの分類によって、そのユーザの名前または識別子が含まれているファイル、バケット、OneDrive、SharePointアカウントがすべて検出されます。BlueXPの分類では、インデックスが事前に設定された最新のデータで名前や識別子がチェックされます。新しいスキャンは開始されません。

検索が完了したら、 Data Subject Access Request レポートのファイルリストをダウンロードできます。このレポートでは、データから得た情報を集約して、利用者に返すことができる法的条件にします。

> 現時点では、データベース内でのデータの件名検索はサポートされていません。

データ主体の検索とレポートのダウンロード

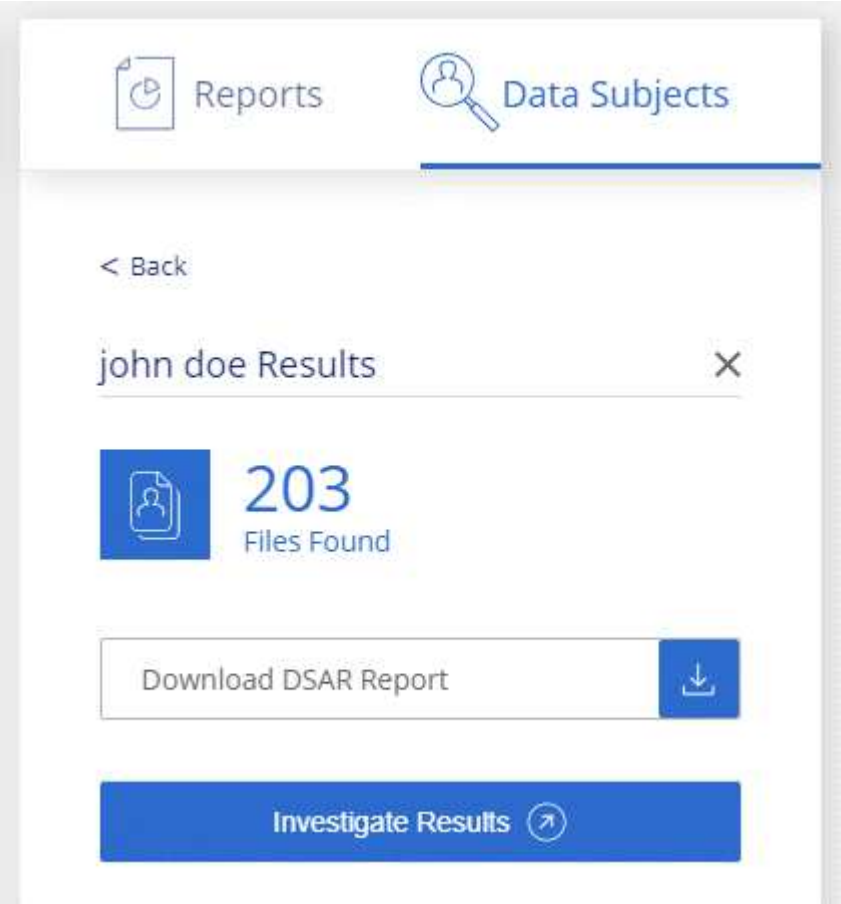
データ主体のフルネームまたは既知の識別子を検索し、ファイルリストレポートまたは dsar レポートをダウンロードします。で検索できます "個人情報の種類"。

> データ主体の名前を検索する際には、英語、ドイツ語、日本語、スペイン語がサポートされています。言語のサポートは、あとで追加されます。

手順

1. BlueXPメニューで、* Governance > Classification *をクリックします。
2. [* データ主体 *] をクリックします。
3. データ主体のフルネームまたは既知の識別子を検索します

   次の例では、 name *John doe*: を検索しています。



4. 次のいずれかのオプションを選択します。
   - **Download dsar Report**: アクセス要求に対する正式な応答で、データ主体に送信できます。このレポートには、対象データについてBlueXPで分類されたデータに基づいて自動的に生成される情報が含まれ、テンプレートとして使用できるように設計されています。データ主体に送信する前に、フォームに必要事項を記入して内部で確認してください。
   - * 調査結果 * ：特定のファイルの検索、ソート、詳細の展開、およびファイルリストのダウンロードによってデータを調査できるページ。

     10 、 000 件を超える結果がある場合は、ファイルリストに上位 10 、 000 件のみが表示されます。

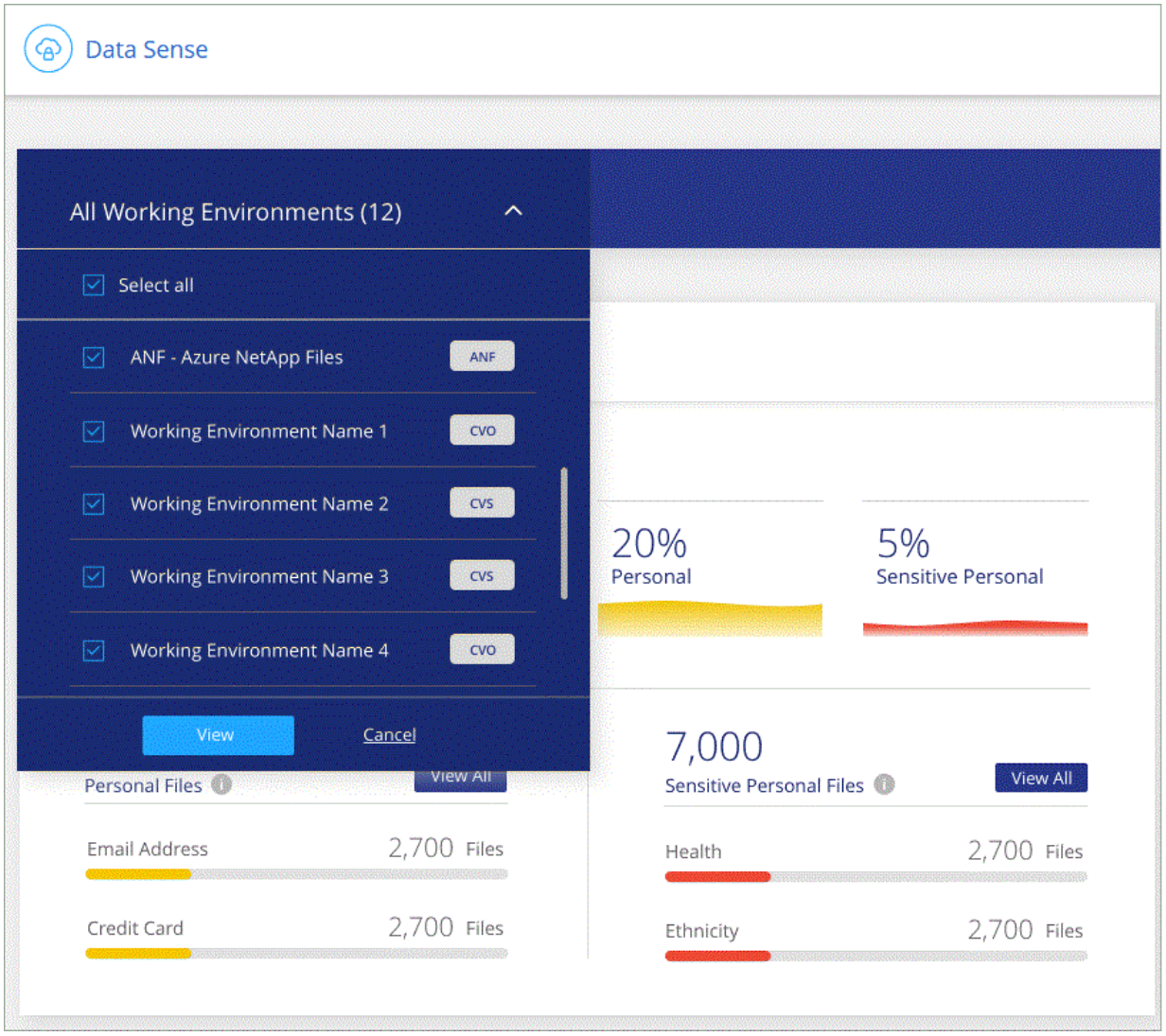
レポートの作業環境を選択

BlueXPの分類[Compliance]ダッシュボードの内容をフィルタリングして、すべての作業環境とデータベース、または特定の作業環境のコンプライアンスデータを表示できます。

ダッシュボードをフィルタすると、BlueXPの分類によって、選択した作業環境のみに準拠データとレポートの範囲が限定されます。

手順

1. フィルタドロップダウンをクリックし、データを表示する作業環境を選択して、 * 表示 * をクリックします。



BlueXPの分類を管理します

BlueXPの分類スキャンに個人データ識別子を追加

BlueXPの分類では、今後のスキャンでBlueXPの分類によって特定される「個人データ」のカスタムリストを追加するためのさまざまな方法が用意されています。これにより、機密性の高いデータが_all_組織のファイル内のどこにあるかを全体的に把握できます。

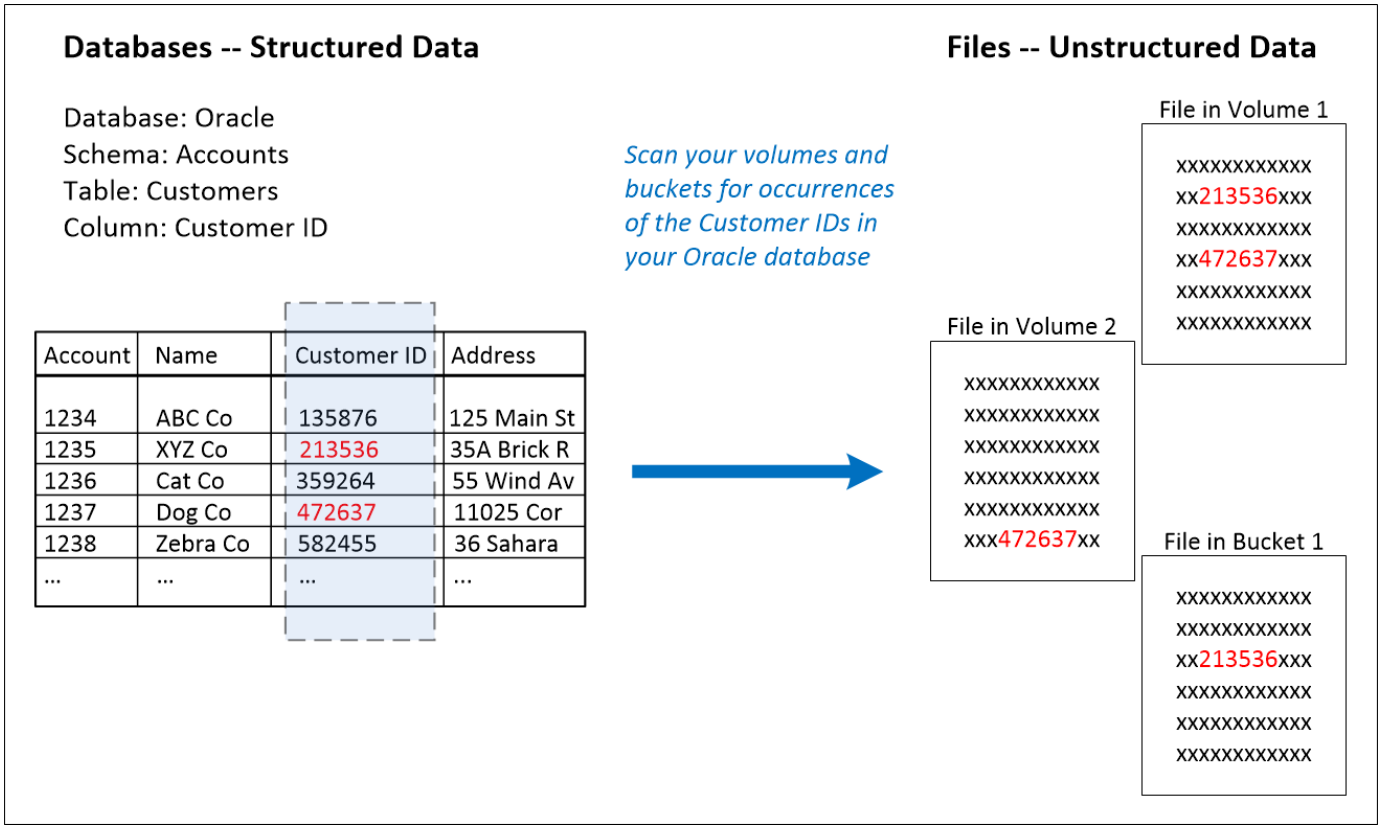
- スキャンするデータベース内の特定の列に基づいて一意の識別子を追加できます。
- テキストファイルからカスタムキーワードを追加できます。これらの単語はデータ内で識別されます。
- 正規表現（regex）を使用してパーソナルパターンを追加できます。既存の定義済みパターンに正規表現が追加されます。
- カスタムカテゴリを追加して、データ内の特定のカテゴリの情報を特定できます。

カスタムスキャン条件を追加するこれらのメカニズムはすべて、すべての言語でサポートされています。

> このセクションで説明する機能は、データソースに対して完全な分類スキャンを実行することを選択した場合にのみ使用できます。マッピングのみのスキャンを実行したデータソースでは、ファイルレベルの詳細は表示されません。

データベースからカスタムの個人データ識別子を追加します

Data Fusion _という機能を使用すると、組織のデータをスキャンして、データベースからの一意の識別子が他のいずれかのデータソースに存在するかどうかを確認できます。データベーステーブルで特定の列を選択することで、BlueXPのスキャンで検索される追加の識別子を選択できます。たとえば、次の図は、データ Fusion を使用してボリューム、バケット、およびデータベースをスキャンし、 Oracle データベースからすべての顧客 ID が出現する状況を示しています。



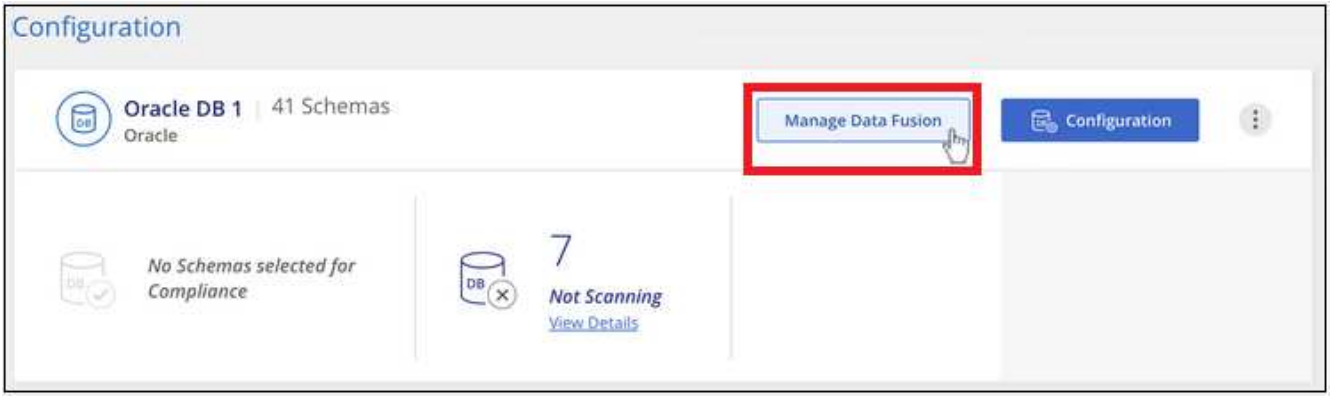
このように、 2 つのボリュームと 1 つの S3 バケットにそれぞれ一意の顧客 ID が見つかりました。データベーステーブル内の一致も識別されます。

独自のデータベースをスキャンするため、データが保存されている言語に関係なく、今後のBlueXP分類スキャンでデータを識別するために使用されることに注意してください。

手順

が必要です "データベースサーバを少なくとも 1 つ追加しました" データFusion ソースを追加する前に、をBlueXPの分類に追加する必要があります。

1. [構成] ページで、ソースデータが存在するデータベースの [データ Fusion の管理] をクリックします。

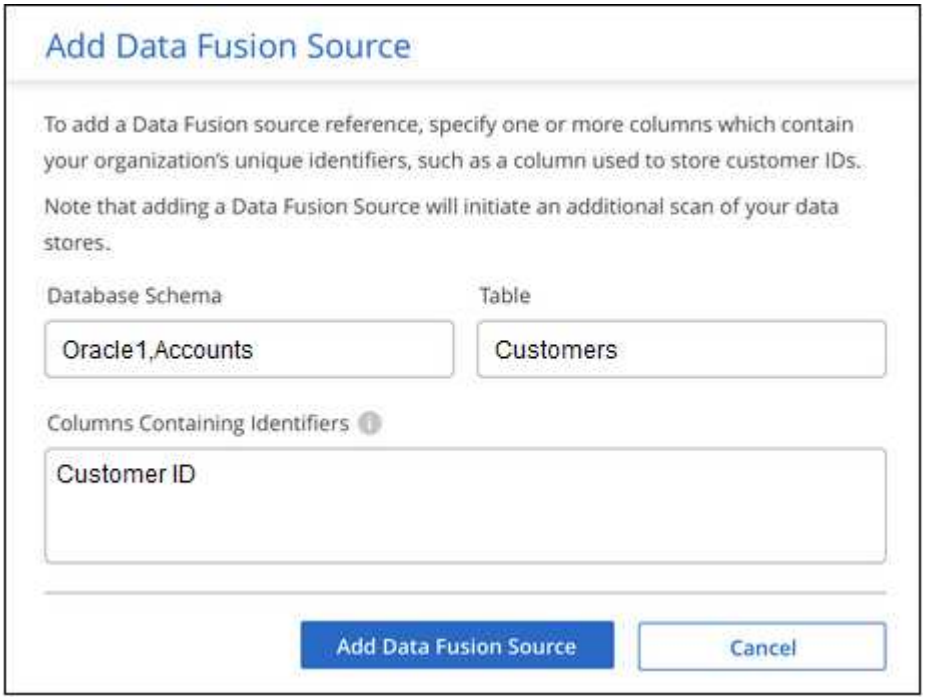


ボタンを選択するスクリーンショット。"]

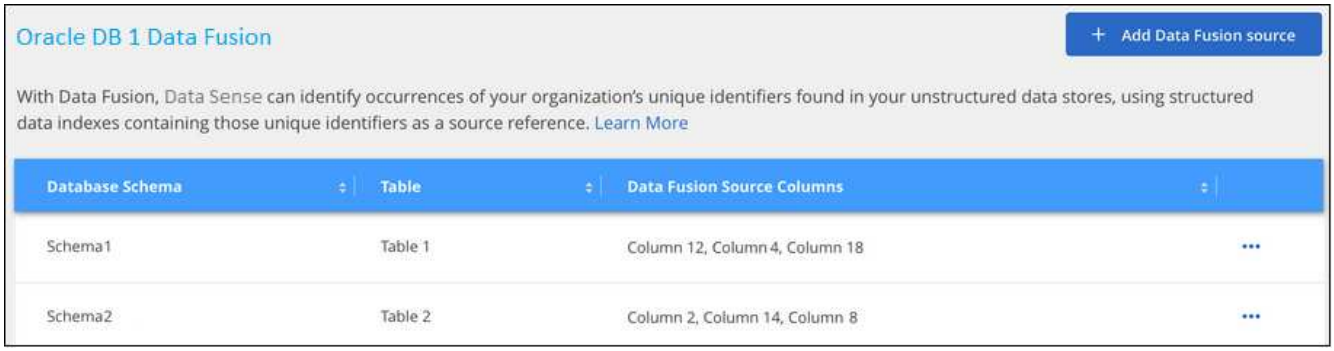
2. 次のページで [Add Data Fusion source*] をクリックします。
3. [Add Data Fusion Source_] ページで、次の手順を実行します。

a. ドロップダウンメニューからデータベーススキーマを選択します。
b. そのスキーマにテーブル名を入力します。
c. 使用する一意の識別子を含む列を入力します。

複数の列を追加する場合は、各列名またはテーブルビュー名を別々の行に入力します。

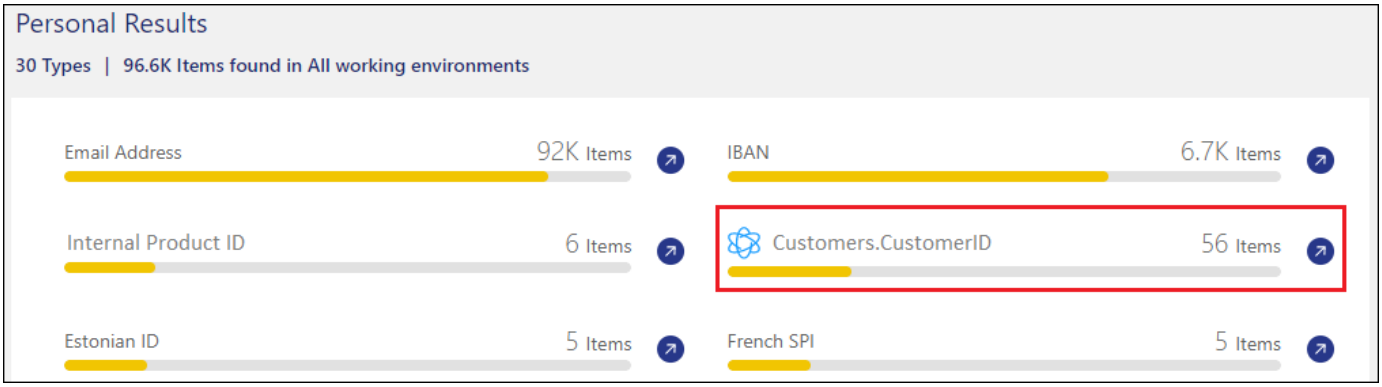


4. [Add Data Fusion Source*] をクリックします。



結果

次のスキャンの後、この新しい情報は、［個人の結果］セクションの［コンプライアンスダッシュボード］と［個人データ］フィルタの［調査］ページに表示されます。分類子に使用した名前がフィルタリストに表示されます。例： `Customers.CustomerID`。



Data Fusion ソースを削除します

特定の Data Fusion ソースを使用してファイルをスキャンしない場合は、 Data Fusion インベントリページからソース行を選択し、 ［* データ Fusion ソースの削除 *］ をクリックします。

単語のリストからカスタムキーワードを追加します

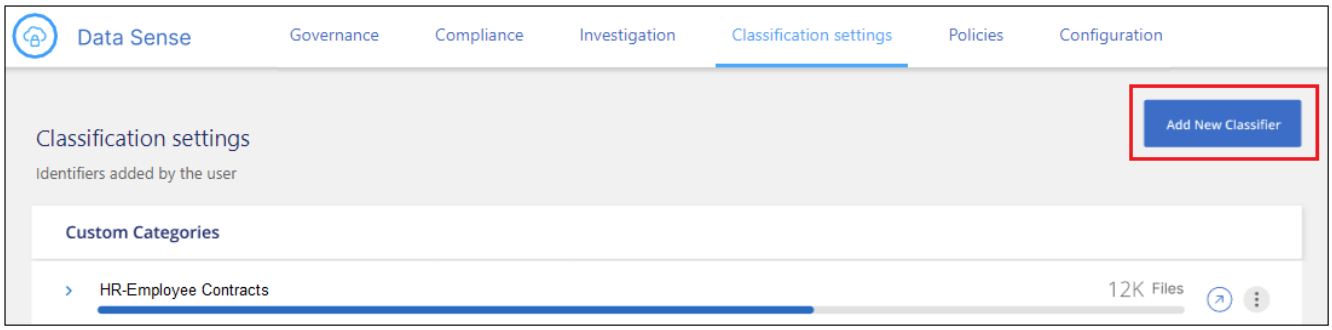
BlueXPの分類にカスタムキーワードを追加すると、その情報がデータ内のどこにあるかがわかるようになります。キーワードを追加するには、BlueXPの分類で認識したい単語を1つずつ入力します。これらのキーワードは、BlueXPの分類ですでに使用されている定義済みの既存のキーワードに追加され、結果は個人のパターンセクションに表示されます。

たとえば、すべてのファイルで内部製品名が言及されている場所を確認して、これらの名前が安全でない場所でアクセスできないようにすることができます。

カスタムキーワードを更新すると、BlueXP分類によってすべてのデータソースのスキャンが再開されます。スキャンが完了すると、BlueXP分類コンプライアンスダッシュボードの[Personal Results]セクションと[Investigation]ページの[Personal Data]フィルタに新しい結果が表示されます。

手順

1. [_Classification settings]タブで*[Add New Classifier]*をクリックし、_Add Custom Classifier_wizardを起動します。

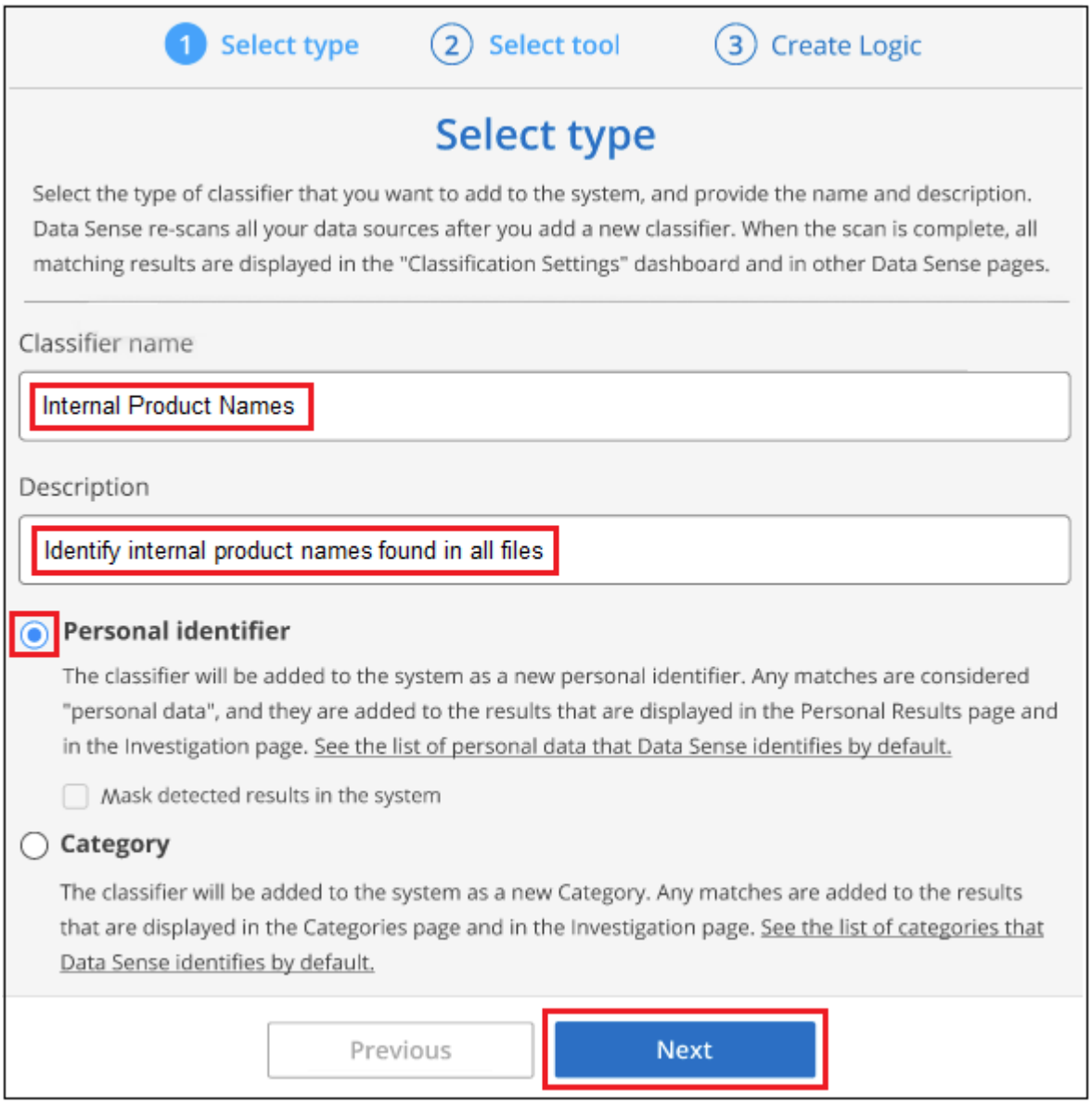


2. [タイプの選択]ページで、分類子の名前を入力し、短い概要 を入力して、[**Personal identifier**]を選択し、[

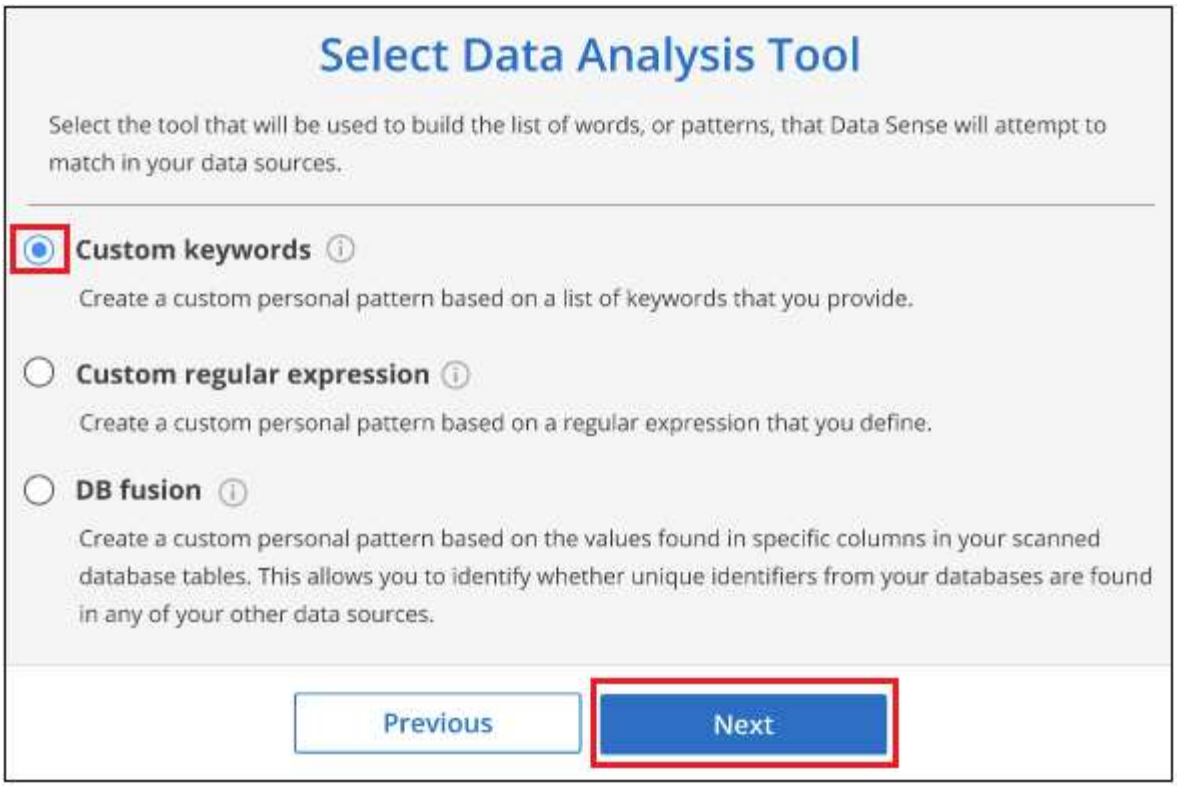
次へ*]をクリックします。

入力した名前は、BlueXP分類UIに分類子の要件に一致するスキャン済みファイルの見出しとして表示され、[Investigation]ページにフィルタの名前として表示されます。

また、「システムで検出された結果をマスク」のチェックボックスをオンにして、UIに完全な結果が表示されないようにすることもできます。たとえば、クレジットカード番号や類似の個人データを完全に非表示にする場合があります(マスクは次のようにUIに表示されます:"**********" 3434)。



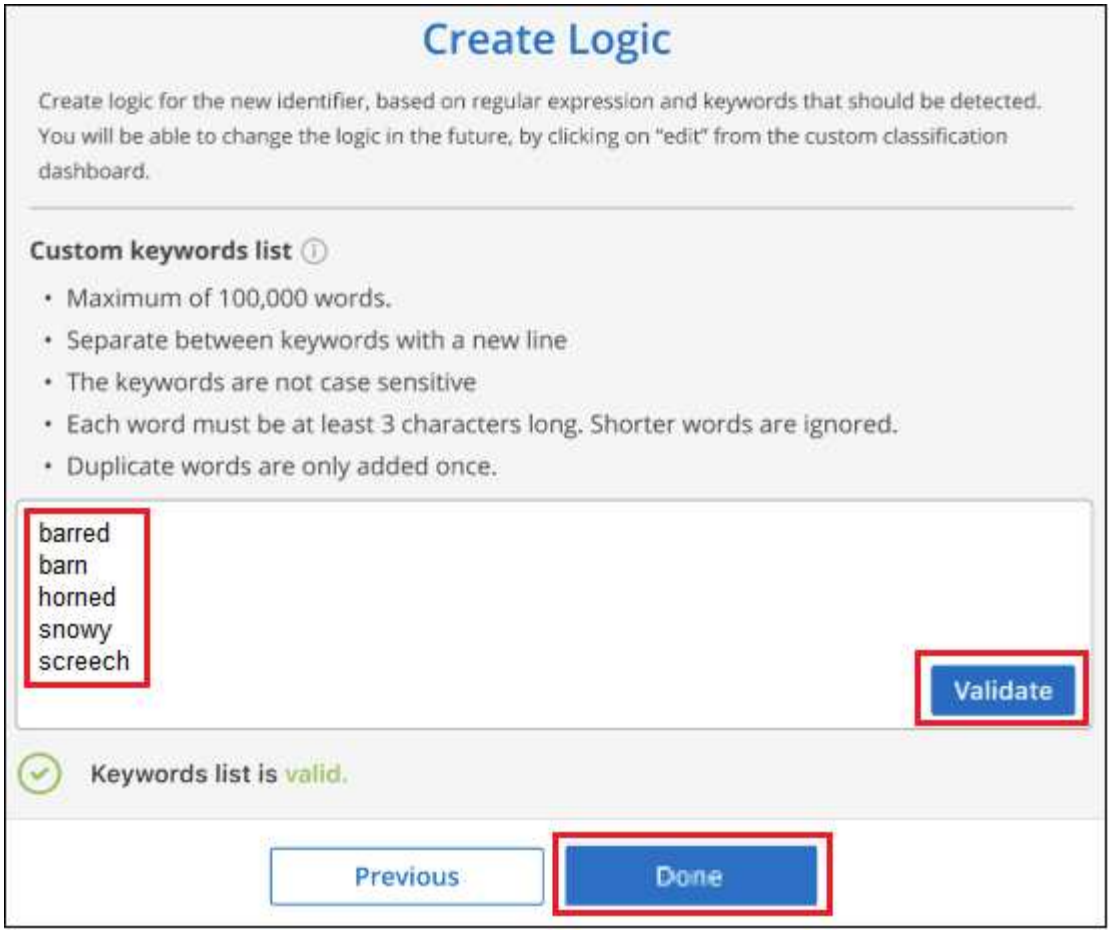
3. [データ分析ツールの選択]ページで、分類子の定義に使用する方法として*を選択し、[次へ]*をクリックします。



を選択したスクリーンショット。"]

4. [*Create Logic*]ページで、認識するキーワード（各単語を別 々 の行に入力）を入力し、*[Validate]*をクリックします。

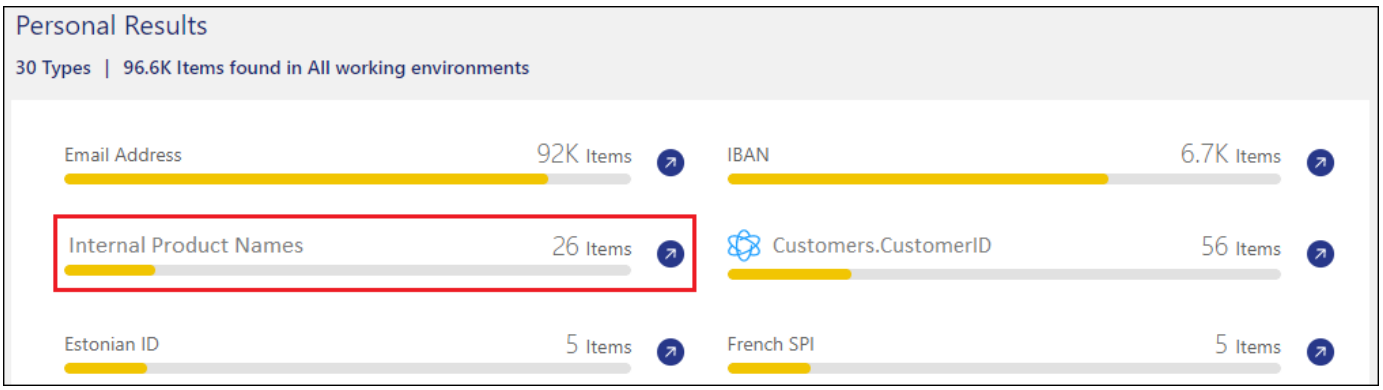
   下のスクリーンショットは、内部の製品名(さまざまな種類のフクロウ)を示しています。これらの項目に対するBlueXPの分類検索では、大文字と小文字は区別されません。



5. [完了]*をクリックすると、BlueXPの分類によってデータの再スキャンが開始されます。

結果

スキャンが完了すると、コンプライアンスダッシュボードの[個人結果]セクションと[個人データ]フィルタの[調査]ページに、この新しい情報が結果に含まれます。



ペインにカスタムキーワードの結果の例を示すスクリーンショット。"]

ご覧のように、分類子の名前が個人結果パネルの名前として使用されます。このようにして、さまざまなキーワードグループをアクティブ化し、各グループの結果を表示できます。

正規表現を使用してカスタムの個人データ識別子を追加する

カスタム正規表現（regex）を使用して、データ内の特定の情報を識別するためのパーソナルパターンを追加

できます。これにより、新しいカスタム正規表現を作成して、システムにまだ存在しない新しい個人情報要素を特定できます。正規表現は、BlueXPの分類ですでに使用されている既存の定義済みパターンに追加され、結果は[Personal Patterns]セクションに表示されます。

たとえば、すべてのファイルで内部製品IDが記載されている場所を確認できます。製品IDに明確な構造が含まれている場合、たとえば、201で始まる12桁の数値であれば、カスタム正規表現機能を使用してファイル内で検索できます。この例の正規表現は*\b201\d｛9｝\b *です。

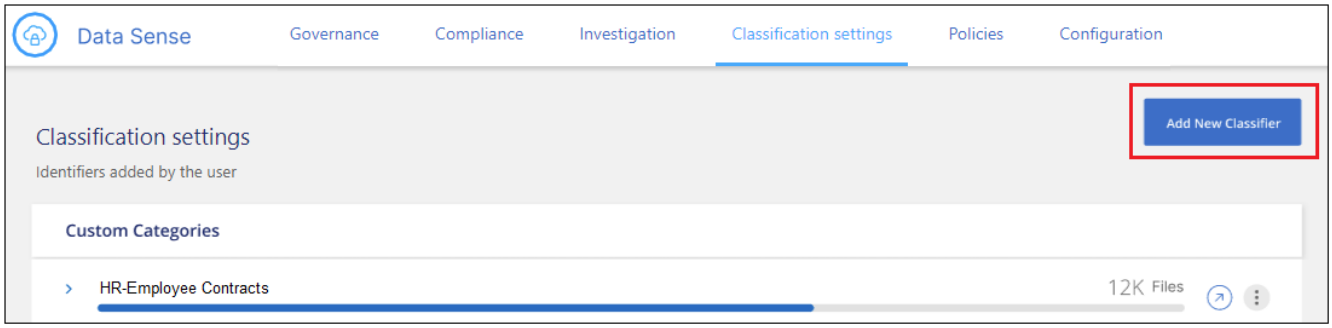
正規表現を追加すると、BlueXPの分類によってすべてのデータソースのスキャンが再開されます。スキャンが完了すると、BlueXP分類コンプライアンスダッシュボードの[Personal Results]セクションと[Investigation]ページの[Personal Data]フィルタに新しい結果が表示されます。

正規表現の作成についてサポートが必要な場合は、を参照してください。 "正規表現101"。フレーバーに「* Python *」を選択すると、BlueXPの分類が正規表現と一致する結果のタイプが表示されます。。 "Python Regex Testerページ" パターンをグラフィカルに表示することもできます。

> 現在、正規表現を作成するときにパターンフラグを使用することは許可されていません。これは、"/"を使用しないことを意味します。

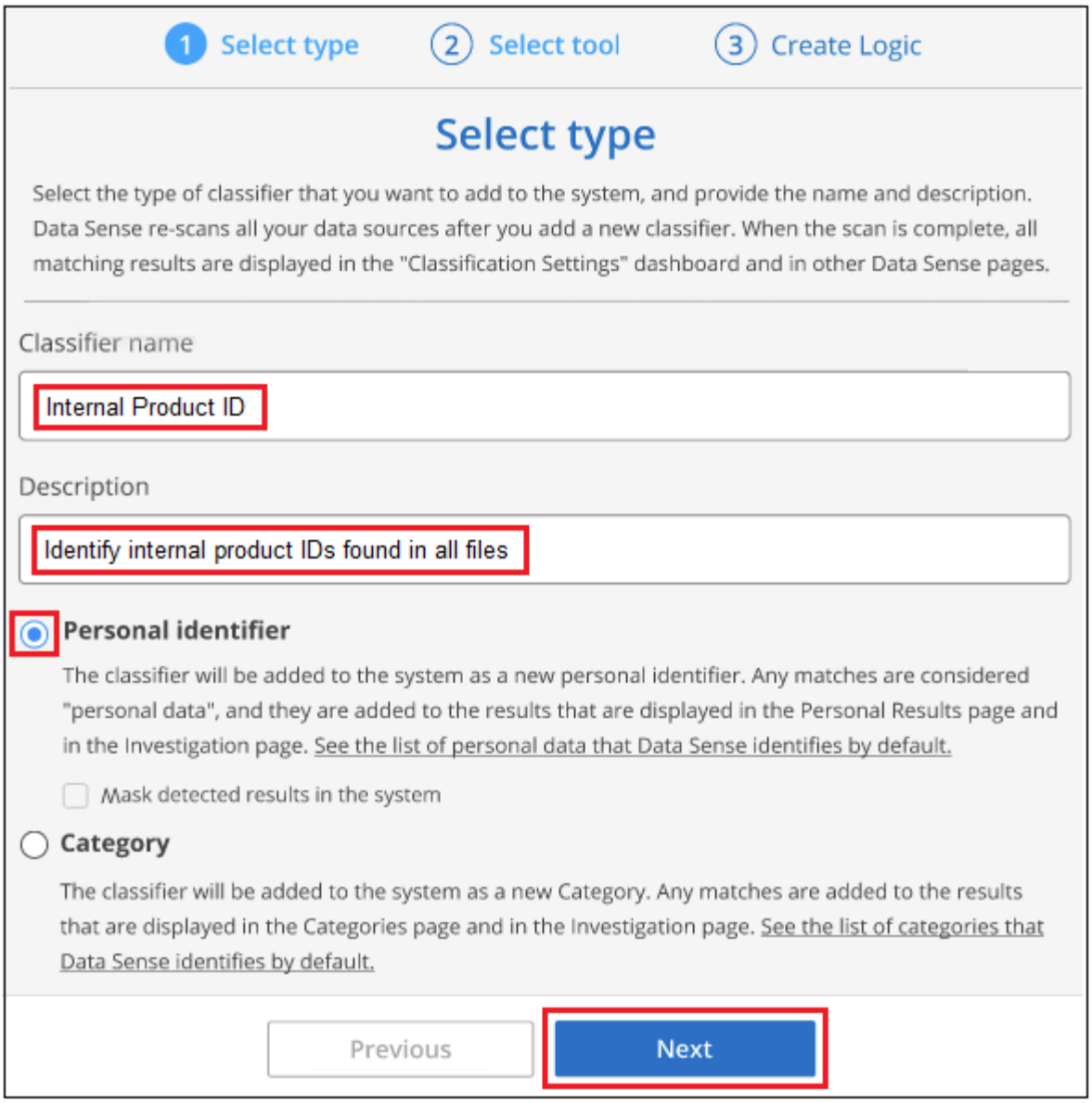
手順

1. [_Classification settings]タブで*[Add New Classifier]*をクリックし、_Add Custom Classifier_wizardを起動します。

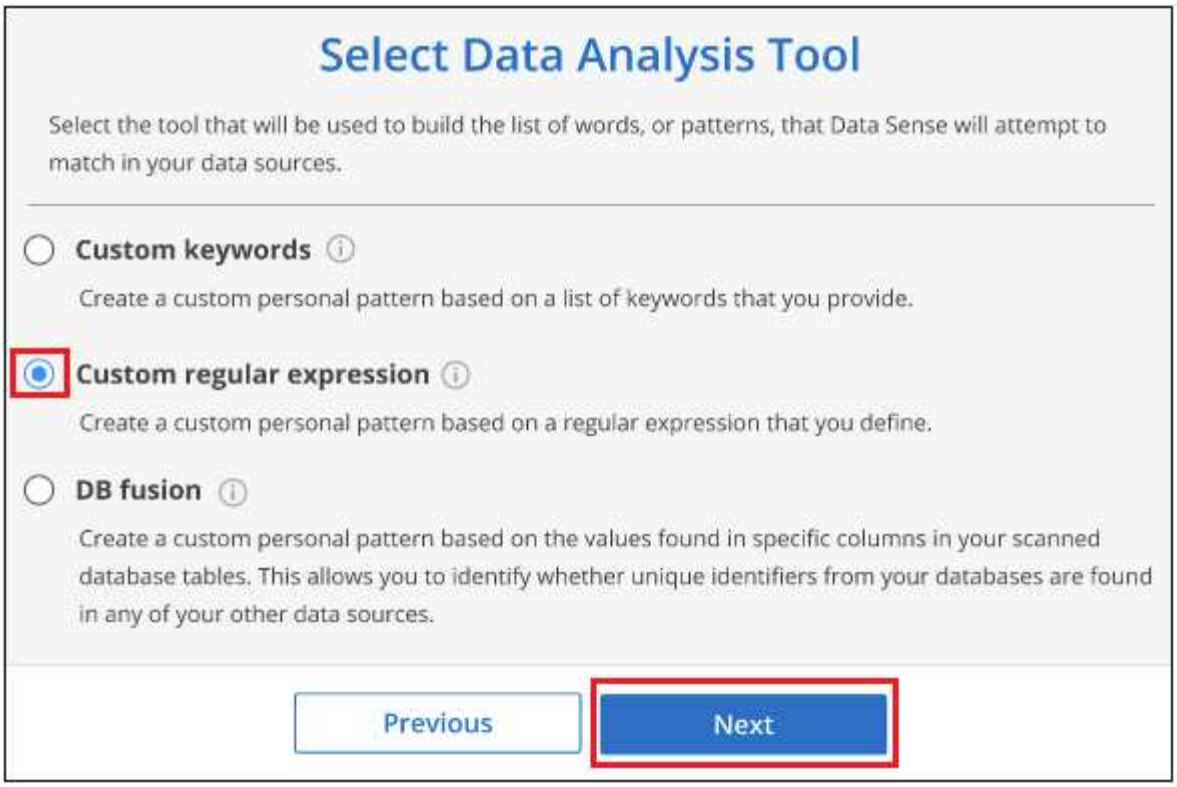


2. [タイプの選択]ページで、分類子の名前を入力し、短い概要 を入力して、[**Personal identifier**]を選択し、[次へ*]をクリックします。

   入力した名前は、BlueXP分類UIに分類子の要件に一致するスキャン済みファイルの見出しとして表示され、[Investigation]ページにフィルタの名前として表示されます。また、「システムで検出された結果をマスク」のチェックボックスをオンにして、UIに完全な結果が表示されないようにすることもできます。たとえば、クレジットカード番号全体または類似の個人データを非表示にする場合などです。

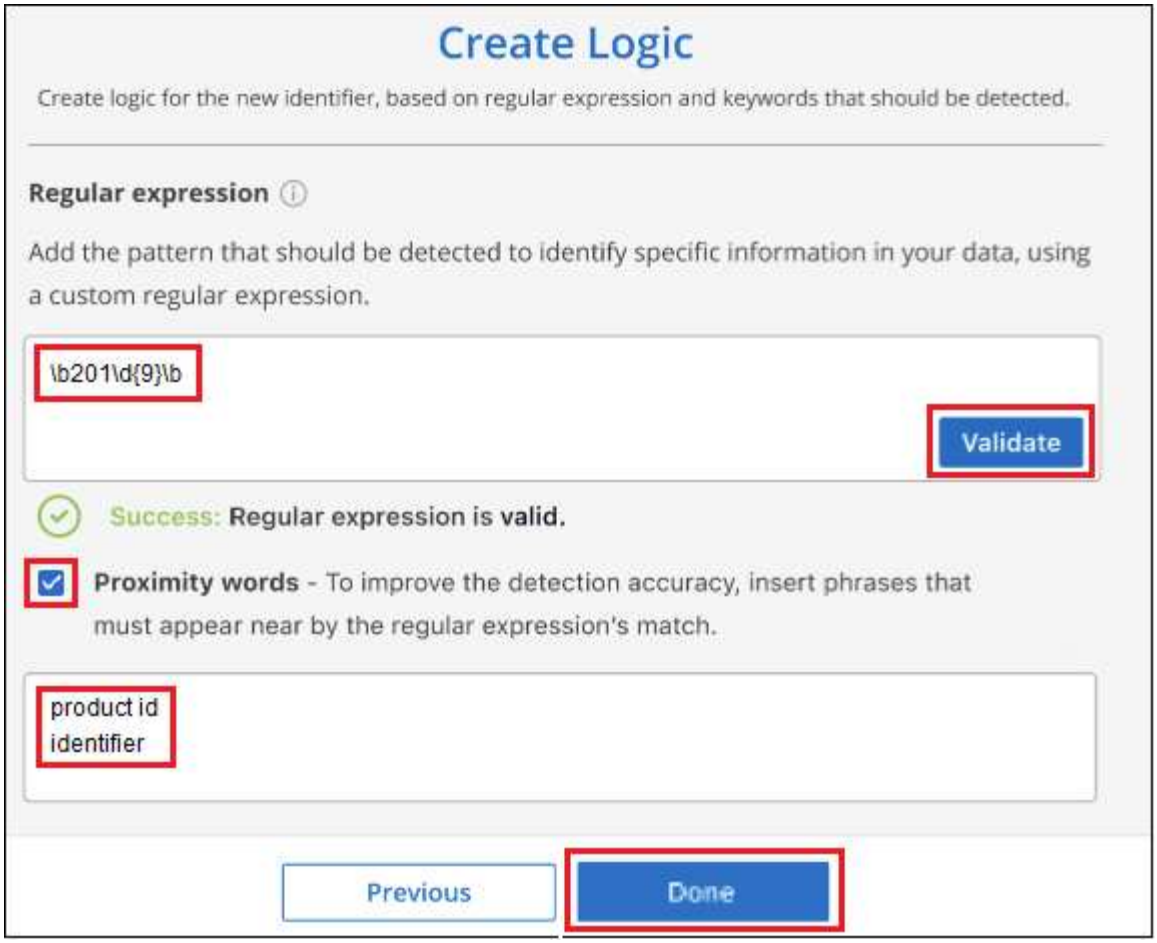


3. [データ分析ツールの選択]ページで、分類子の定義に使用するメソッドとして[カスタム正規表現*]を選択し、[次へ*]をクリックします。



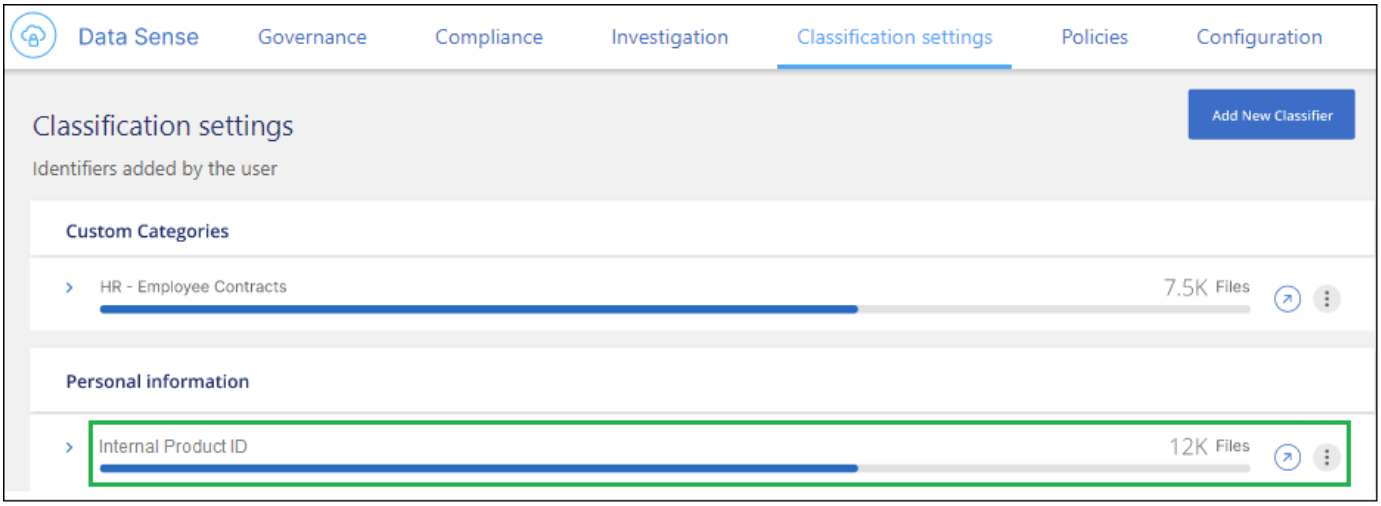
が選択されていることを示すスクリーンショット。"]

4. Create Logic_pageで、正規表現と近接文字を入力し、* Done *をクリックします。
   a. 正規表現は任意に入力できます。[検証]*ボタンをクリックして、BlueXPで正規表現が有効かどうか、また正規表現が広すぎないかどうか（返される結果が多すぎないかどうか）が検証されます。
   b. 必要に応じて、近接キーワードを入力して結果の精度を高めることができます。検索対象のパターンの300文字以内（検出されたパターンの前または後）に検索されるのが一般的な単語です。単語またはフレーズをそれぞれ別の行に入力します。



結果

分類子が追加され、BlueXPの分類によってすべてのデータソースの再スキャンが開始されます。カスタム分類子ページに戻り'新しい分類子に一致するファイルの数を確認できますすべてのデータソースをスキャンした結果は、スキャンする必要があるファイルの数によってはしばらく時間がかかります。



カスタムカテゴリを追加します

BlueXPは、スキャンしたデータをさまざまなカテゴリに分類して分類します。カテゴリは、各ファイルのコンテンツとメタデータの人工知能分析に基づくトピックです。 "事前定義されたカテゴリのリストを参照して

ください"。

カテゴリを使用すると、保有している情報の種類を表示して、データの状況を把握することができます。たとえば、_resumes_or_employee contracts_のようなカテゴリには、機密データが含まれている場合があります。結果を調査すると、従業員契約が安全でない場所に保存されていることがわかります。その後、その問題を修正できます。

BlueXPの分類にカスタムカテゴリを追加すると、データ資産に固有の情報のカテゴリがデータのどこにあるかを特定できます。特定するデータのカテゴリを含む「トレーニング」ファイルを作成して各カテゴリを追加し、BlueXPの分類でそれらのファイルをスキャンしてAIで「学習」し、データソース内のそのデータを識別できるようにします。これらのカテゴリは、BlueXPの分類ですでに識別されている既存の事前定義されたカテゴリに追加され、[カテゴリ]セクションに結果が表示されます。

たとえば、必要に応じて削除できるように、.gz形式の圧縮インストールファイルがファイル内のどこにあるかを確認することができます。

カスタムカテゴリを更新すると、BlueXPの分類によってすべてのデータソースのスキャンが再開されます。スキャンが完了すると、BlueXP分類コンプライアンスダッシュボードの[カテゴリ]セクションと[カテゴリ]フィルタの[調査]ページに新しい結果が表示されます。 "カテゴリ別にファイルを表示する方法を参照してください"。

必要なもの

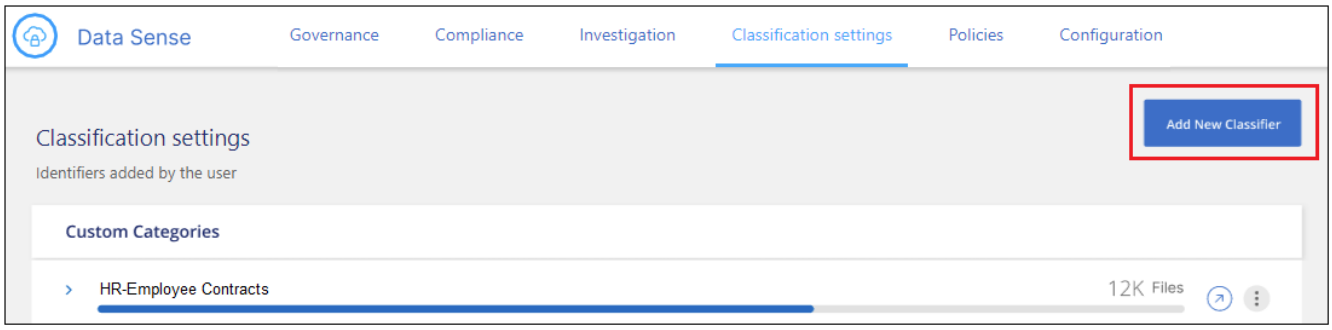
BlueXPの分類で認識するデータカテゴリのサンプルを含むトレーニングファイルを少なくとも25個作成する必要があります。次のファイルタイプがサポートされています。

```
.CSV, .DOC, .DOCX, .GZ, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX, Docs,
Sheets, and Slides
```

ファイルは100バイト以上である必要があり、BlueXPの分類でアクセスできるフォルダに配置されている必要があります。

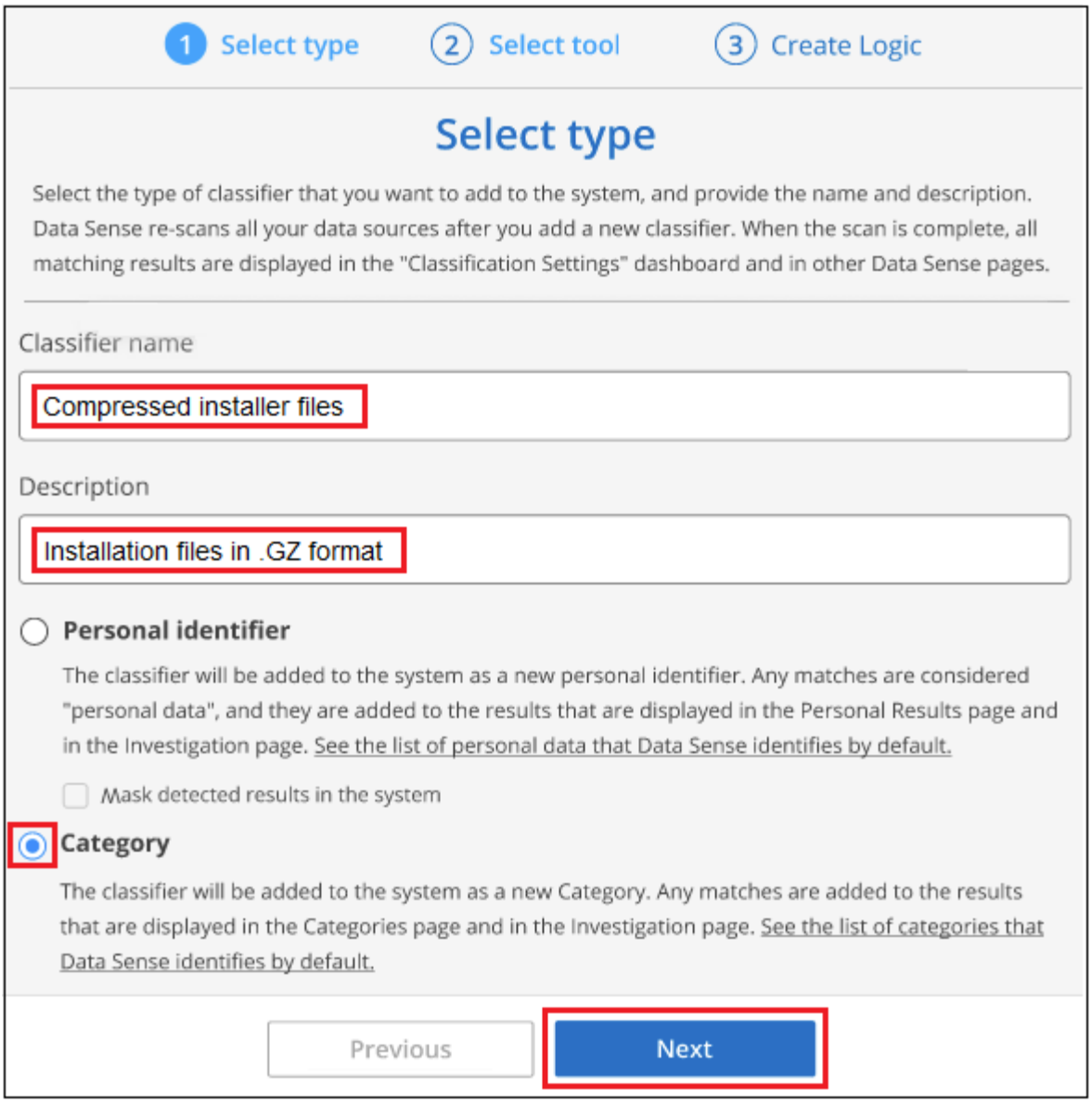
手順

1. [_Classification settings]タブで*[Add New Classifier]*をクリックし、_Add Custom Classifier_wizardを起動します。

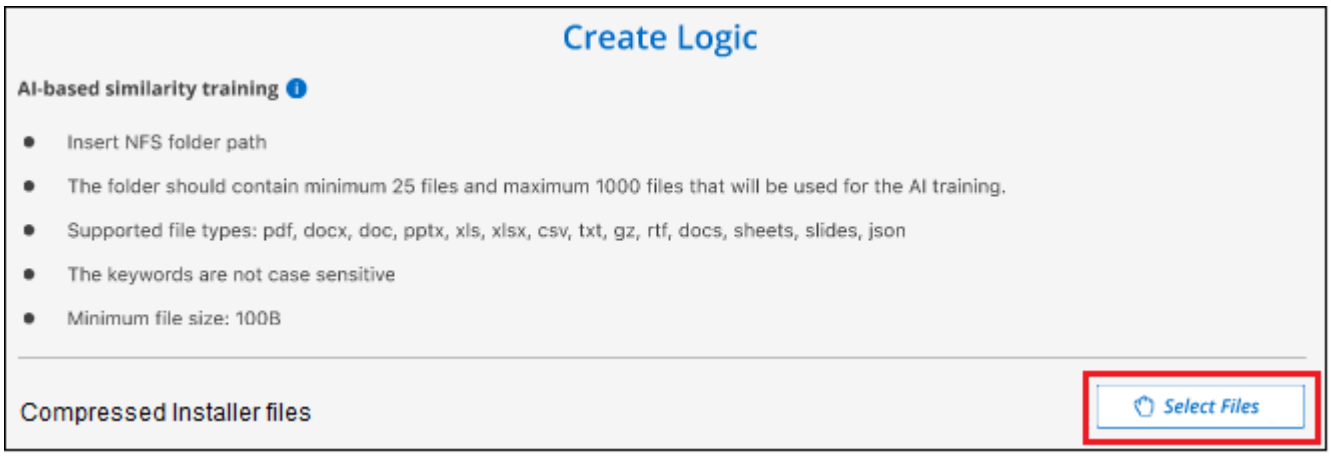


2. [*Select type*]ページで、分類子の名前を入力し、簡単な概要 を入力して*を選択し、[Next]*をクリックします。

   入力した名前が、定義しているデータのカテゴリに一致するスキャン済みファイルの見出しとしてBlueXP分類UIに表示され、[Investigation]ページにフィルタの名前として表示されます。



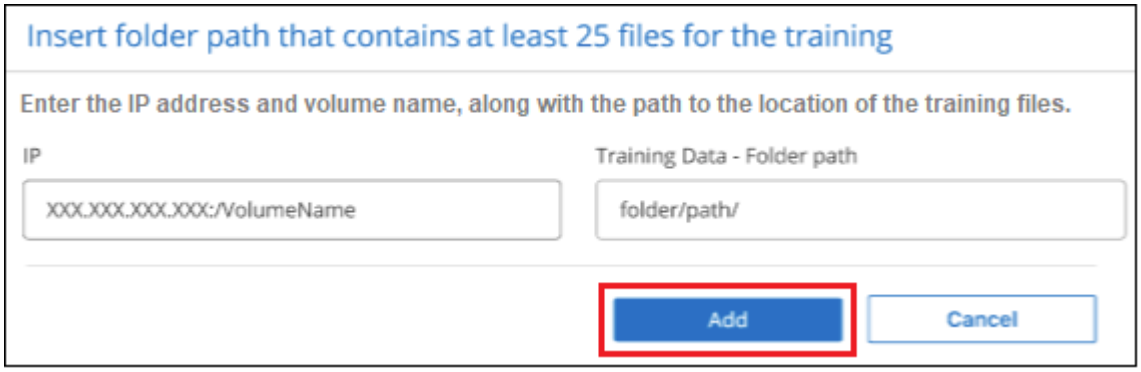
3. [*Create Logic*]ページで、学習ファイルが準備されていることを確認し、*[ファイルの選択]*をクリックします。



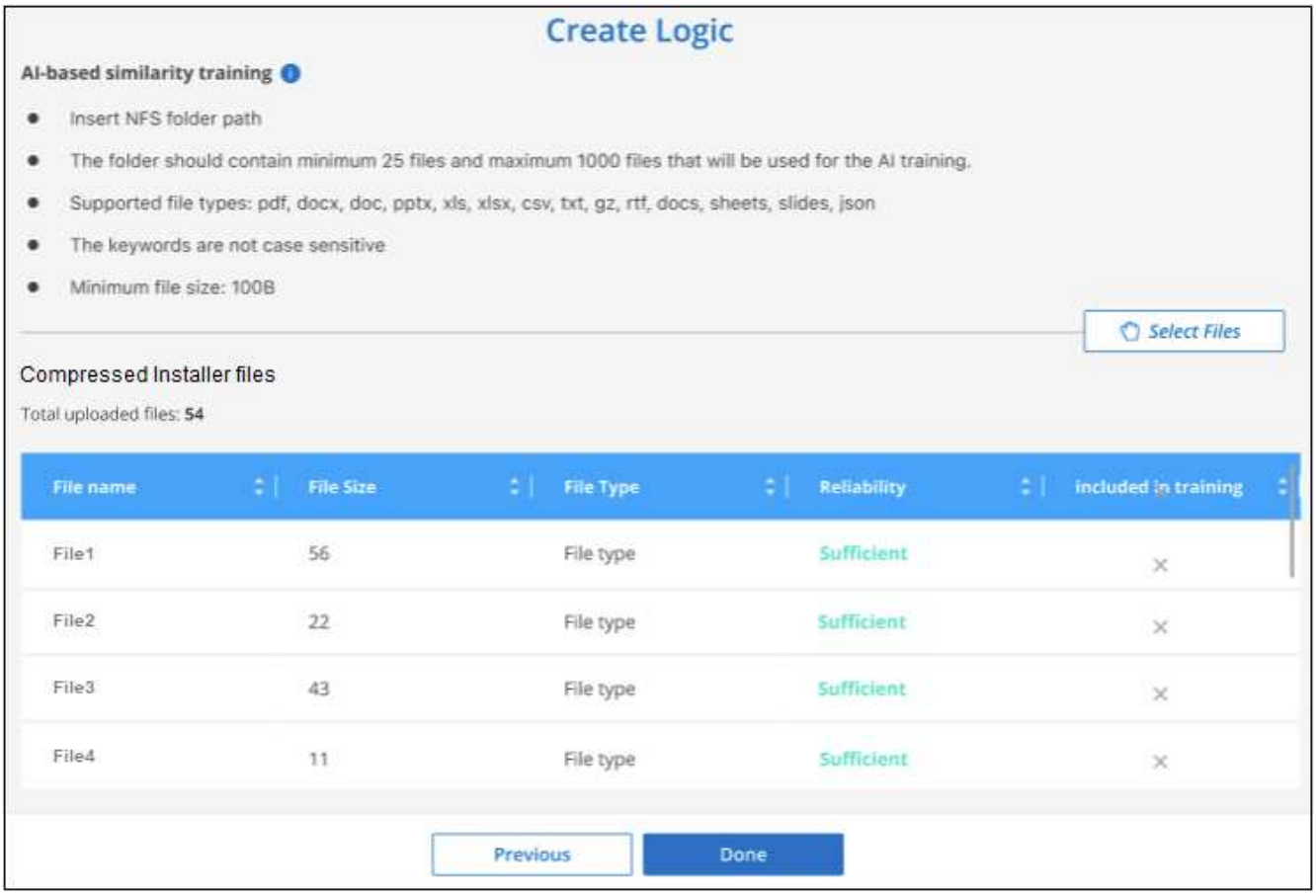
ページのスクリーンショット。BlueXPの分類に使用するデータを含むファイルを追加します。"]

4. ボリュームのIPアドレスとトレーニングファイルが格納されているパスを入力し、*[追加]*をクリックしま

す。



5. トレーニングファイルがBlueXPの分類で認識されたことを確認します。要件を満たしていないトレーニングファイルを削除するには、* x *をクリックします。[完了]*をクリックします。

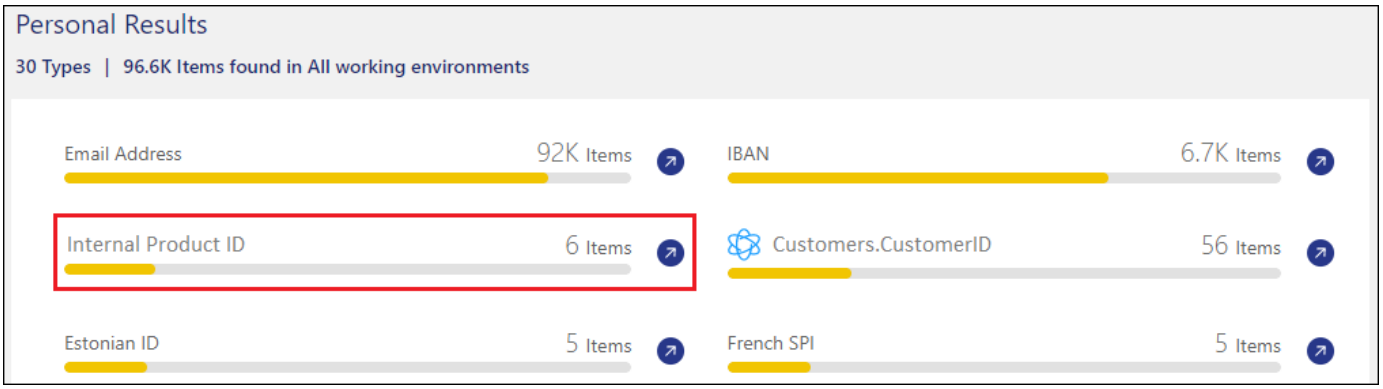


結果

トレーニングファイルの定義に従って新しいカテゴリが作成され、BlueXPの分類に追加されます。その後、BlueXPで分類が開始され、すべてのデータソースが再スキャンされて、この新しいカテゴリに該当するファイルが特定されます。[Custom Classifiers]ページに戻り、新しいカテゴリに一致するファイルの数を確認できます。すべてのデータソースをスキャンした結果は、スキャンする必要があるファイルの数によってはしばらく時間がかかります。

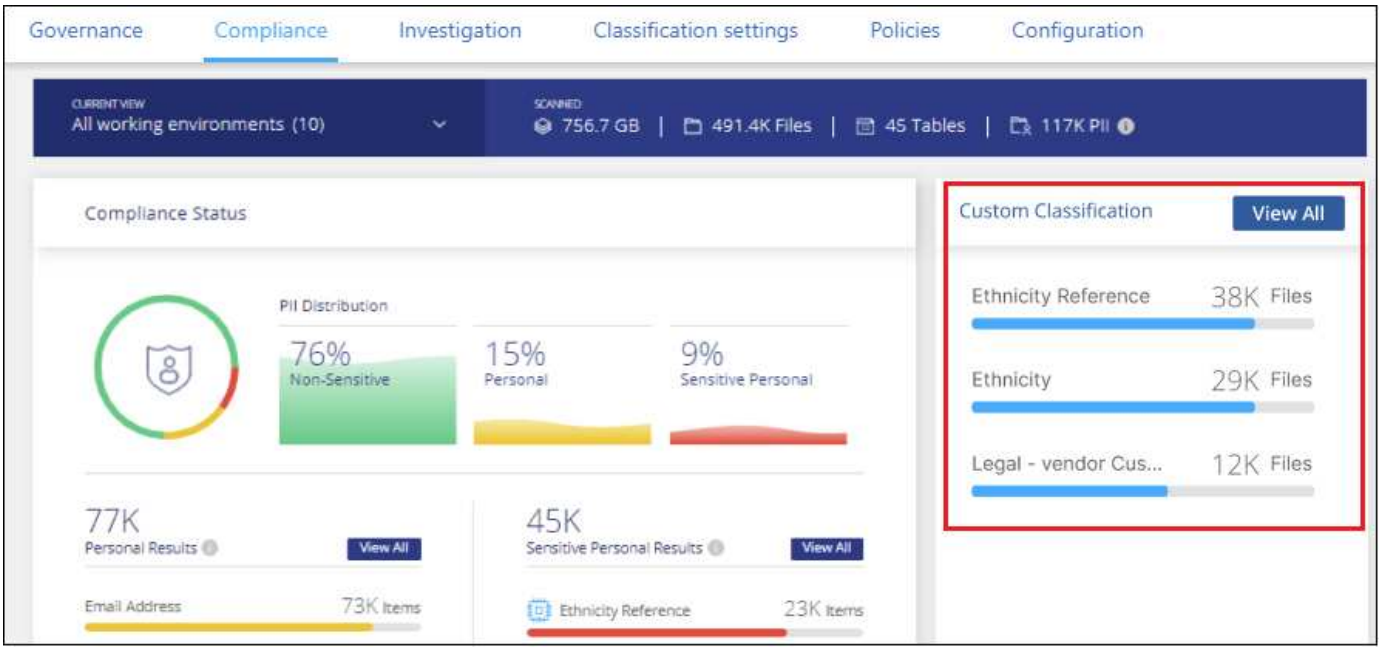
カスタム分類子の結果を表示します

コンプライアンスダッシュボードおよび［調査］ページで、任意のカスタム分類子の結果を表示できます。たとえば、このスクリーンショットは、「個人の結果」セクションの下のコンプライアンスダッシュボードに表示されている、一致した情報を示しています。



をクリックします ボタンをクリックすると、詳細な結果が[調査]ページに表示されます。

さらに、カスタム分類子の結果はすべて[カスタム分類子]タブに表示され、上位6つのカスタム分類子の結果が[コンプライアンスダッシュボード]に表示されます。

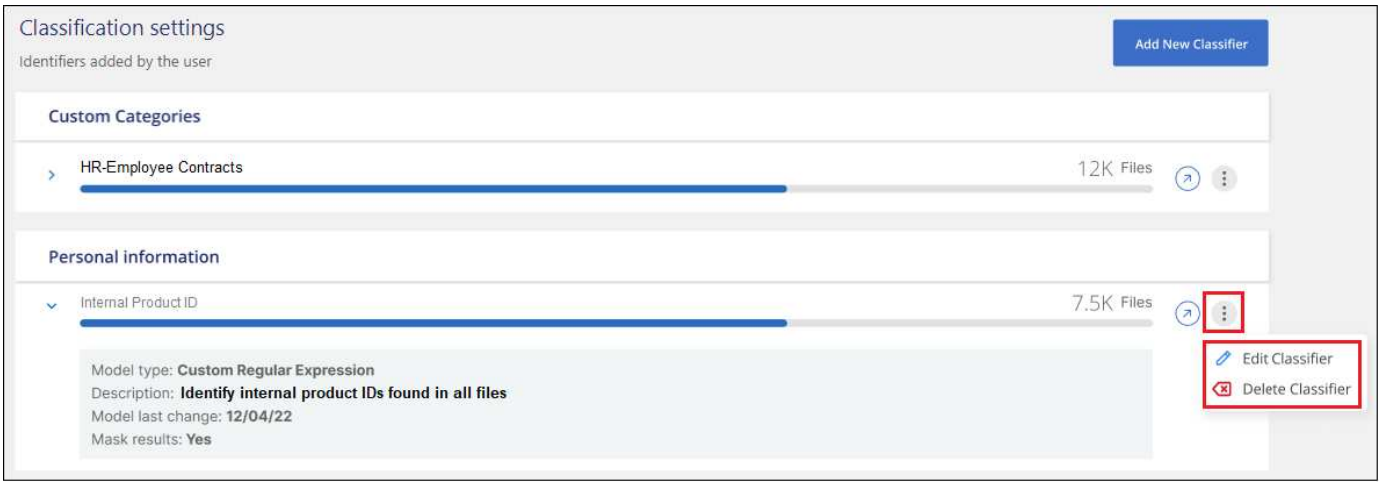


カスタム分類子を管理します

作成したカスタム分類子は、*Edit Classifier*ボタンを使用して変更できます。

現時点では、Data Fusion分類子を編集することはできません。

あとで、追加したカスタムパターンをBlueXPの分類で特定する必要がないと判断した場合は、*[Delete Classifier]*ボタンを使用して各項目を削除できます。



ページのスクリーンショット。"]

BlueXPの分類スキャンから特定のディレクトリを除外する

BlueXPの分類で、特定のデータソースディレクトリにあるスキャンデータを除外するには、これらのディレクトリ名を構成ファイルに追加します。この変更を適用すると、BlueXP分類エンジンによってディレクトリ内のスキャンデータが除外されます。

BlueXPの分類は、ボリュームの内容と同じであるため、ボリュームSnapshotデータのスキャンを除外するようにデフォルトで設定されています。

この機能は、BlueXP分類バージョン1.29以降（2024年3月以降）で使用できます。

サポートされているデータソース

BlueXPの分類スキャンから特定のディレクトリを除外することは、次のデータソースのNFS共有とCIFS共有でサポートされます。

- オンプレミスのONTAP
- Cloud Volumes ONTAP
- NetApp ONTAP 対応の Amazon FSX
- Azure NetApp Files の特長
- 一般的なファイル共有

スキャン対象から除外するディレクトリを定義する

分類のスキャン対象からディレクトリを除外するには、構成ファイルを編集してスクリプトを実行できるように、BlueXP分類システムにログインする必要があります。方法を参照してください "BlueXP分類システムにログインする" ソフトウェアを手動でLinuxマシンにインストールしたか、インスタンスをクラウドに導入したかによって異なります。

- BlueXP分類システムごとに最大50個のディレクトリパスを除外できます。
- ディレクトリパスを除外すると、スキャン時間に影響することがあります。

手順

1. BlueXP分類システムで、「/opt/netapp/config/custom _configuration」に移動してファイルを開きます。`data_provider.yaml`。
2. 「data_providers」セクションの「exclude：」行の下に、除外するディレクトリパスを入力します。例：

   ```
   exclude:
   - "folder1"
   - "folder2"
   ```

   このファイルの他の内容は変更しないでください。

3. 変更をファイルに保存します。
4. 「/opt/netapp/Datasense/tools/customer _configuration/data_providers」に移動し、次のスクリプトを実行します。

   ```
   update_data_providers_from_config_file.sh
   ```

   このコマンドは、スキャンから除外するディレクトリを分類エンジンにコミットします。

結果

以降のデータスキャンでは、指定したディレクトリのスキャンが除外されます。

除外リストの項目を追加、編集、または削除するには、同じ手順を実行します。修正された除外リストは、スクリプトを実行して変更をコミットすると更新されます。

例

構成**1**：

名前の任意の場所に"folder1"を含むすべてのフォルダは、すべてのデータソースから除外されます。

```
data_providers:
   exclude:
   - "folder1"
```

除外するパスの想定される結果：

- /CVO1/folder1
- /CVO1/folder1name
- /CVO1/folder10
- /CVO1/*フォルダ1
- /CVO1/+ folder1name
- /CVO1/notfolder10

- /CVO22/フォルダ1
- /CVO22/folder1name
- /CVO22/フォルダ10

除外されないパスの例：

- /CVO1/*フォルダ
- /CVO1/foldername
- /CVO22/* folder20

構成**2**：

名前の先頭にのみ「* folder1」を含むすべてのフォルダは除外されます。

```
data_providers:
   exclude:
   - "\\*folder1"
```

除外するパスの想定される結果：

- /CVO /*フォルダ1
- /CVO /* folder1name
- /CVO /*フォルダ10

除外されないパスの例：

- /CVO/フォルダ1
- /cvo/folder1name
- /CVO / NOT * folder10

構成**3**：

データソース「CVO22」内の名前の任意の場所に「folder1」を含むすべてのフォルダは除外されます。

```
data_providers:
   exclude:
   - "CVO22/folder1"
```

除外するパスの想定される結果：

- /CVO22/フォルダ1
- /CVO22/folder1name
- /CVO22/フォルダ10

除外されないパスの例：

- /CVO1/folder1
- /CVO1/folder1name

- /CVO1/folder10

フォルダ名の特殊文字のエスケープ

次の特殊文字のいずれかを含むフォルダ名があり、そのフォルダ内のデータをスキャン対象から除外する場合は、フォルダ名の前にエスケープシーケンス\\を使用する必要があります。

```
 ., +, *, ?, ^, $, (, ), [, ], {, }, |
例：
```

ソース内のパス： `/project/*not_to_scan`

EXCLUDEファイルの構文： `"\\*not_to_scan"`

現在の除外リストを表示する

内容は可能である `data_provider.yaml` の実行後に実際にコミットされたものとは異なる構成ファイル `update_data_providers_from_config_file.sh` スクリプト：BlueXPの分類スキャンの対象から除外したディレクトリの現在のリストを表示するには、「/opt/netapp/Datasense/tools/customer _configuration/data_providers」で次のコマンドを実行します。

```
get_data_providers_configuration.sh
```

コンプライアンスアクションのステータスを表示します

100個のファイルの移動や削除など、多くのファイルで［調査結果］ペインから非同期アクションを実行する場合は、このプロセスに時間がかかることがあります。これらのアクションのステータスは、_Action Status_Paneで監視できるので、すべてのファイルにいつ適用されたかを知ることができます。

これにより、正常に完了した操作、現在実行中の操作、および失敗した操作を確認できるため、問題を診断して修正できます。単一ファイルの移動など、短時間で完了する短時間の処理は、[操作][ステータス]ペインには表示されません。

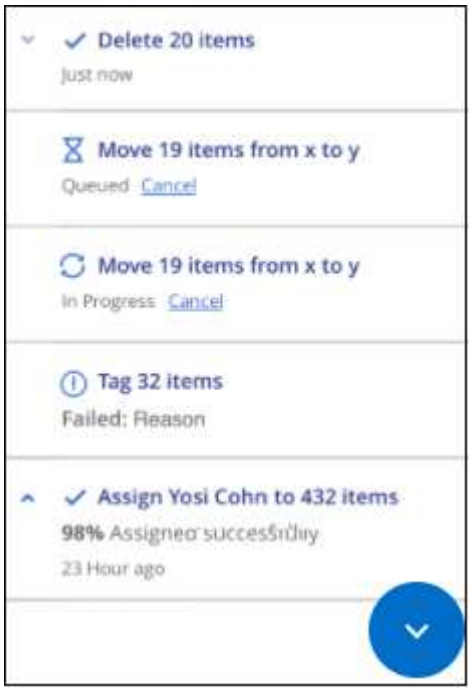
ステータスは次のいずれかになります。

- 成功- BlueXPの分類アクションが完了し、すべての項目が成功しました。
- 部分的に成功- BlueXPの分類処理が完了し、一部の項目が失敗して一部が成功しました。
- In Progress -処理はまだ実行中です。
- Queued -処理が開始されていません。
- Cancelled -処理はキャンセルされました。
- failed -処理に失敗しました。

ステータスが「 Queued 」または「 In Progress 」のアクションはすべてキャンセルできます。

手順

1. BlueXP分類UIの右下には、[操作][ステータス]*ボタンが表示されます  。
2. このボタンをクリックすると、最新の 20 件のアクションが表示されます。



アクションの名前をクリックすると、その操作に対応する詳細を表示できます。

追加のグループIDを組織に対してオープンとして定義する

グループID（GID）がNFSファイル共有内のファイルまたはフォルダに添付される場合、グループIDはファイルまたはフォルダに対する権限（組織に対して開かれているかどうかなど）を定義します。一部のグループID（GID）に「組織を開く」権限レベルが設定されていない場合は、その権限をGIDに追加して、そのGIDが添付されているファイルやフォルダが「組織に対して開かれている」とみなされるようにすることができます。

この変更を行ってBlueXPの分類でファイルやフォルダが再スキャンされると、これらのグループIDが関連付けられているファイルやフォルダには、[調査の詳細]ページにこの権限が表示され、ファイルの権限を表示しているレポートにも表示されます。

この機能をアクティブ化するには、構成ファイルを編集してスクリプトを実行できるように、BlueXP分類システムにログインする必要があります。方法を参照してください "BlueXP分類システムにログインする" ソフトウェアを手動でLinuxマシンにインストールしたか、インスタンスをクラウドに導入したかによって異なります。

「組織に開く」権限をグループIDに追加する

このタスクを開始する前に、グループID番号（GID）が必要です。

手順

1. BlueXP分類システムで、「/opt/netapp/config/custom _configuration」に移動してファイルを開きます。`data_provider.yaml`。
2. 「organization_group_ids:[]」行にグループIDを追加します。例：

   ```
   organization_group_ids: [1014, 1015, 21, 2021, 1013, 2020, 1018, 1019]
   ```

   このファイルの他の内容は変更しないでください。

3. 変更をファイルに保存します。
4. 「/opt/netapp/Datasense/tools/customer _configuration/data_providers」に移動し、次のスクリプトを実行します。

   ```
   update_data_providers_from_config_file.sh
   ```

   このコマンドは、変更されたグループID権限を分類エンジンにコミットします。

結果

その後のデータスキャンでは、これらのグループIDが「組織に対して開かれている」と添付されているファイルまたはフォルダが特定されます。

次の手順を使用して、グループIDのリストを編集したり、過去に追加したグループIDを削除したりできます。変更したグループIDのリストは、スクリプトを実行して変更をコミットすると更新されます。

現在のグループ**ID**のリストを表示する

内容は可能である `data_provider.yaml` の実行後に実際にコミットされたものとは異なる構成ファイル `update_data_providers_from_config_file.sh` スクリプト：BlueXPの分類に追加したグループIDの現在のリストを表示するには、「/opt/netapp/Datasense/tools/customer _configuration/data_providers」から次のコマンドを実行します。

```
get_data_providers_configuration.sh
```

BlueXPの分類アクションの履歴を監査します

BlueXPの分類では、BlueXPの分類でスキャンするすべての作業環境とデータソースのファイルに対して実行された管理アクティビティがログに記録されます。BlueXPの分類では、BlueXP分類インスタンスを導入する際のアクティビティも記録されます。

BlueXP分類監査ログファイルの内容を表示したり、ファイルをダウンロードして、どのファイルが変更されたか、いつ変更されたかを確認したりできます。たとえば、発行された要求、要求の時刻、ファイルが削除された場合のソースの場所、ファイルが移動された場合のソースとデスティネーションの場所などの詳細を確認できます。

ログファイルの内容

監査ログの各行には、次の形式で情報が表示されます。

```
<full date> | <status> | ds_audit_logger | <module> | 0 | 0 | File <full file
path> deleted from device <device path> - <result>
```

- 日付と時刻-イベントの完全なタイムスタンプ
- Status -情報、警告
- アクションタイプ（削除、コピー、移動、ポリシーの作成、ポリシーの更新、 ファイルの再スキャン、JSONレポートのダウンロードなど）
- ファイル名（ファイルに関連するアクションの場合）
- アクションの詳細-何が行われたか：アクションによって異なります
  - ポリシー名
  - 移動元と移動先のデータ用
  - コピー元およびコピー先の場合
  - tag-tag nameを指定します
  - をクリックします
  - Eメールアラートの場合- Eメールアドレス/アカウント

たとえば、ログファイルの次の行は、コピー処理が成功し、コピー処理が失敗した場合を示しています。

```
2022-06-06 15:23:08,910 | INFO | ds_audit_logger | es_scanned_file | 237 |
49 | Copy file /CIFS_share/data/dop1/random_positives.tsv from device
10.31.133.183 (type: SMB_SHARE) to device 10.31.130.133:/export_reports
(NFS_SHARE) - SUCCESS
2022-06-06 15:23:08,968 | WARNING | ds_audit_logger | es_scanned_file |
239 | 153 | Copy file /CIFS_share/data/compliance-netapp.tar.gz from
device 10.31.133.183 (type: SMB_SHARE) to device
10.31.130.133:/export_reports (NFS_SHARE) - FAILURE
```

ログファイルの場所

管理監査ログファイルは、BlueXP分類マシンの次の場所にあります。 `/opt/netapp/audit_logs/`

インストール監査ログファイルがに書き込まれます `/opt/netapp/install_logs/`

各ログファイルのサイズは最大で10MBです。この制限に達すると、新しいログファイルが開始されます。ログファイルの名前は「DataSense _ audit.log」、「DataSense _ audit.log.1」、「DataSense _ audit.log.2」などです。システムに保持されるログファイルの最大数は100です。古いログファイルは、最大数に達すると自動的に削除されます。

ログファイルへのアクセス

ログファイルにアクセスするには、BlueXP分類システムにログインする必要があります。方法を参照してください "BlueXP分類システムにログインする" ソフトウェアを手動でLinuxマシンにインストールしたか、インスタンスをクラウドに導入したかによって異なります。

BlueXPの分類スキャン速度が低下します

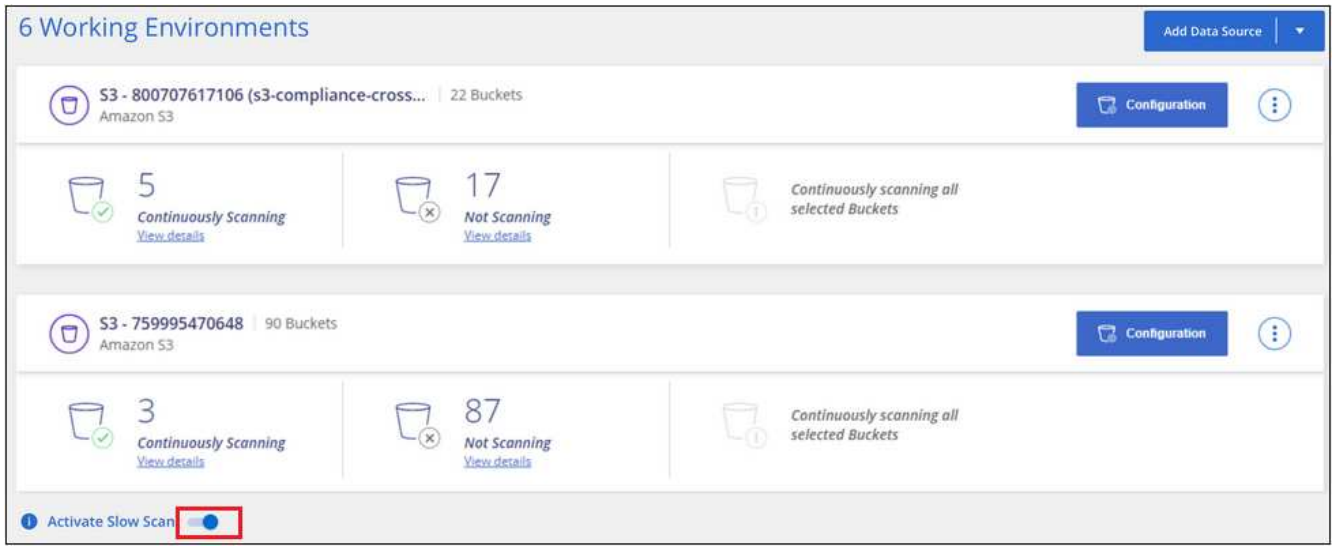
データスキャンは、ストレージシステムとデータにほとんど影響を与えません。ただし、影響がごくわずかであっても問題が発生する場合は、「低速」スキャンを実行するようにBlueXPの分類を設定できます。

有効にすると、すべてのデータソースで低速スキャンが使用されます。 1 つの作業環境またはデータソースで低速スキャンを設定することはできません。

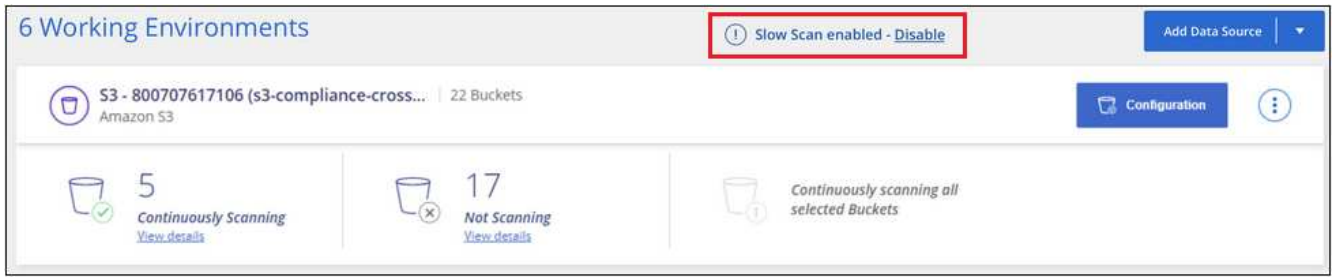
データベースのスキャン中は、スキャン速度を下げることはできません。

手順

1. _Configuration_page の下部から、スライダを右に動かして低速スキャンを有効にします。



設定ページの上部には、低速スキャンが有効になっていることが示されます。



2. このメッセージの * 無効 * をクリックすると、低速スキャンを無効にできます。

BlueXP分類からデータソースを削除しています

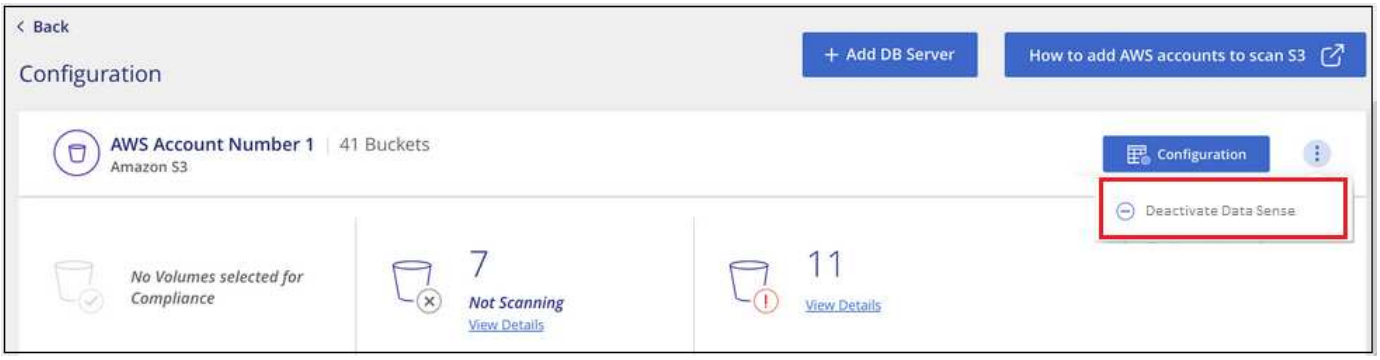
必要に応じて、BlueXPの分類によって1つ以上の作業環境、データベース、ファイル共有グループ、OneDriveアカウント、Google Driveアカウント、 またはSharePointアカウント。

データソースが削除されると、データスキャンの課金が停止します。

作業環境のコンプライアンススキャンを非アクティブにします

スキャンを非アクティブ化すると、BlueXPの分類によって作業環境のデータがスキャンされなくなり、インデックス化されたコンプライアンス分析情報がBlueXPの分類インスタンスから削除されます（作業環境自体のデータは削除されません）。

1. [*Configuration*] ページで、をクリックします ボタン"] ボタンをクリックして作業環境を選択し、 [* データセンスを非活動化 * （ Deactivate Data Sense * ）] をクリックします。



を選択できるアクションアイコンのスクリーンショット。このオプションは、キャンバスページから作業環境を選択した後で使用できます。"]

> 作業環境を選択するときに、サービスパネルから作業環境のコンプライアンススキャンを無効にすることもできます。

BlueXP分類からデータベースを削除しています

特定のデータベースのスキャンが不要になった場合は、BlueXPの分類インターフェイスからそのデータベースを削除して、すべてのスキャンを停止できます。

1. [*Configuration*] ページで、をクリックします ボタン"] ボタンをクリックし、 * DB サーバの削除 * をクリックします。

OneDrive、SharePoint、Google DriveのアカウントをBlueXP分類から削除する

特定のOneDriveアカウント、特定のSharePointアカウント、またはGoogle Driveアカウントからユーザファイルをスキャンする必要がなくなった場合は、BlueXP分類インターフェイスからアカウントを削除して、すべてのスキャンを停止できます。

手順

1. [*Configuration*] ページで、をクリックします ⋮ ボタン"] OneDrive、SharePoint、Google Driveアカウントの行にあるボタンをクリックし、* OneDriveアカウントの削除*、* SharePointアカウントの削除*、または* Googleドライブアカウントの削除*をクリックします。

ページから [OneDrive を削除] ボタンのスクリーンショット。"]

2. 確認ダイアログで * アカウントの削除 * をクリックします。

BlueXP分類からファイル共有のグループを削除しています

ファイル共有グループのユーザファイルをスキャンする必要がなくなった場合は、BlueXPの分類インターフェイスからファイル共有グループを削除して、すべてのスキャンを停止できます。

手順

1. [*Configuration*] ページで、をクリックします ⋮ ボタン"] [ファイル共有グループ] の行にあるボタンをクリックし、 [* ファイル共有グループの削除 *] をクリックします。

2. 確認ダイアログで * 共有のグループを削除 * をクリックします。

BlueXP分類をアンインストールしています

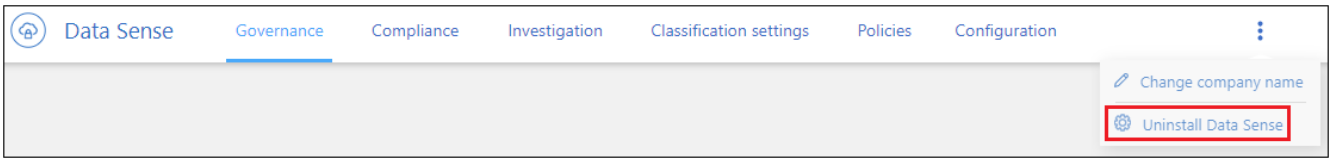
BlueXP分類ソフトウェアをアンインストールして、問題をトラブルシューティングしたり、ホストからソフトウェアを完全に削除したりできます。インスタンスを削除すると、インデックス付きデータが格納されている関連ディスクも削除されます。BlueXP分類によってスキャンされたすべての情報が完全に削除されます。

使用する必要がある手順は、BlueXPの分類をクラウドとオンプレミスのどちらのホストのどちらに導入したかによって異なります。

クラウド環境から**BlueXP**分類をアンインストールします

BlueXP分類を使用する必要がなくなった場合は、クラウドプロバイダ環境からBlueXP分類インスタンスをアンインストールして削除できます。

1. BlueXPの分類ページの上部にあるをクリックします ボタン"] 次に、[データセンスのアンインストール]をクリックします。



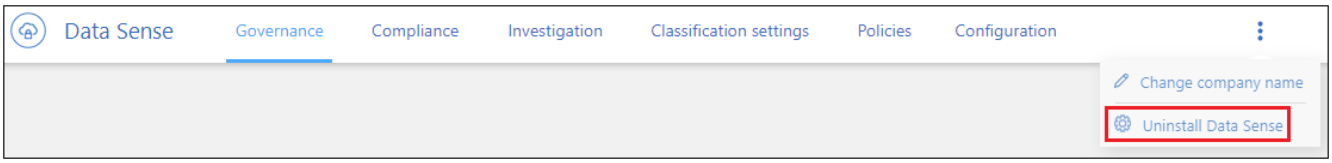
2. [*Uninstall Data Sense*]ダイアログで、「* uninstall 」と入力して**BlueXP**コネクタから**BlueXP**分類インスタンスを切断することを確認し、[アンインストール]*をクリックします。
3. クラウドプロバイダのコンソールに移動し、BlueXP分類インスタンスを削除します。インスタンスの名前は *CloudCompliancy_with* で、生成されたハッシュ（ *UUID* ）を連結しています。例： *_CloudCompliion-16bb6564-38ad-40802-9a92-36f5fd2f71c7*

   これにより、BlueXPの分類によって収集されたインスタンスと関連するすべてのデータが削除されます。

オンプレミス環境から**BlueXP**分類をアンインストールします

BlueXP分類を使用する必要がなくなった場合や、問題 の再インストールが必要な場合は、ホストからBlueXPをアンインストールできます。

1. BlueXPの分類ページの上部にあるをクリックします ボタン"] 次に、[データセンスのアンインストール]をクリックします。



2. [*Uninstall Data Sense*]ダイアログで、「* uninstall 」と入力して**BlueXP**コネクタから**BlueXP**分類インス

タンスを切断することを確認し、[アンインストール]*をクリックします。

3. ホストからソフトウェアをアンインストールするには、 `cleanup.sh` ホストマシン上のスクリプト。例：

```
cleanup.sh
```

方法を参照してください "BlueXP分類ホストマシンにログインします。"。

参照

サポートされるBlueXP分類インスタンスタイプ

BlueXP分類ソフトウェアは、特定のオペレーティングシステム要件、RAM要件、ソフトウェア要件などを満たすホストで実行する必要があります。BlueXPの分類をクラウドに導入する場合、すべての機能を利用するには「大規模」のシステムを使用することを推奨します。

CPUとRAMの数が少ないシステムにBlueXPの分類を導入することもできますが、使用するシステムにはいくつかの制限があります。 "これらの制限事項について説明します"。

次の表で、BlueXP分類をインストールするリージョンで「Default」とマークされたシステムが使用できない場合は、表の次のシステムが導入されます。

AWSインスタンスタイプ

システムサイズ	仕様	インスタンスタイプ
特大	CPU×32、128GB RAM、1TiB GP3 SSD	"m6i.8xlarge" （デフォルト）
大規模	CPU×16、64GB RAM、500GiB SSD	"m6i.4xlarge" （デフォルト）M6A.4xlarge m5a.4xlarge m5.4xlarge m4.4xlarge
中	CPU×8、32GB RAM、200GiB SSD	"m6i.2xlarge" （デフォルト）M6A.2xlarge m5a.2xlarge m5.2xlarge m4.2xlarge
小規模	CPU×8、16GB RAM、100GiB SSD	"c6a.2xlarge" （デフォルト）C5a.2xlarge c5.2xlarge c4.2xlarge

Azureインスタンスタイプ

システムサイズ	仕様	インスタンスタイプ
特大	CPU×32、128GB RAM、OSディスク（2、048GiB、最小250MB/秒のスループット）、データディスク（1TiB SSD、最小750MB/秒のスループット）	"STANDARD_D32_v3" （デフォルト）
大規模	CPU×16、64GB RAM、500GiB SSD	"Standard_D16s_v3" （デフォルト）

GCPインスタンスタイプ

システムサイズ	仕様	インスタンスタイプ
大規模	CPU×16、64GB RAM、500GiB SSD	"N2-standard-16" （デフォルト）n2d-standard-16 n1-standard-16

データソースから収集されたメタデータ

BlueXPの分類では、データソースや作業環境からのデータに対して分類スキャンを実行する際に、特定のメタデータが収集されます。BlueXPの分類では、データを分類するために必要なメタデータのほとんどにアクセスできますが、一部のソースでは必要なデータにアクセスできない場合があります。

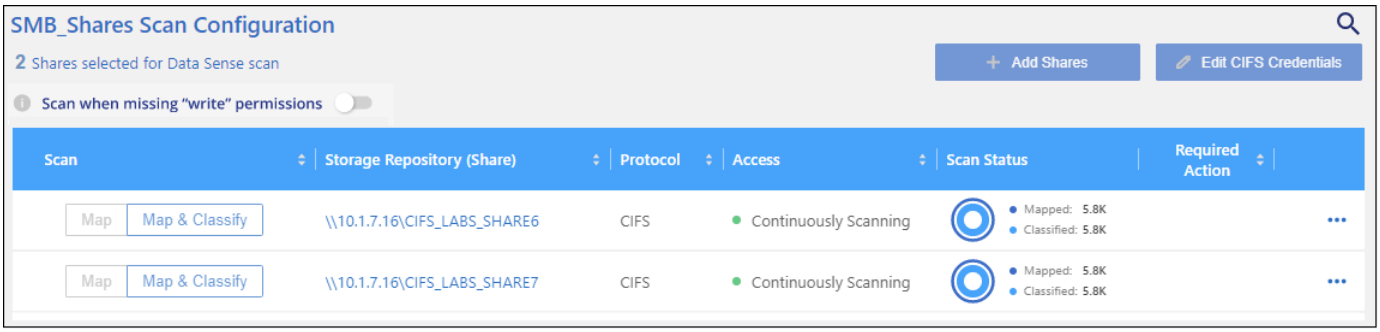
	メタデータ	* CIFS *	* NFS *
タイムスタンプ	作成時間	利用可能	使用不可（Linuxではサポート対象外）
	最終アクセス時間	利用可能	利用可能
	最終変更時刻	利用可能	利用可能
* 権限 *	権限を開く	「Everyone」グループにファイルへのアクセス権がある場合は、「組織に対して開く」と見なされます。	「その他」にファイルへのアクセス権がある場合、「組織に対して開く」と見なされます。
	ユーザー/グループアクセス_	ユーザおよびグループの情報はLDAPから取得されます	使用不可（NFSユーザは通常、サーバ上でローカルに管理されるため、各サーバで同じユーザのUIDを別 々 に設定できます）

- BlueXPの分類では、SharePoint Online、SharePointオンプレミス（SharePoint Server）、OneDrive、Google Drive、Amazon S3、データベースのデータソースから「最終アクセス時刻」は抽出されません。
- 古いバージョンのWindows OS（Windows 7やWindows 8など）では、システムのパフォーマンスに影響を与える可能性があるため、デフォルトで「最終アクセス時刻」属性の収集が無効になります。この属性が収集されない場合は、「最終アクセス日時」に基づくBlueXPの分類分析が影響を受けます。これらの古いWindowsシステムでは、必要に応じて最終アクセス時間の収集を有効にすることができます。

最終アクセス時間のタイムスタンプ

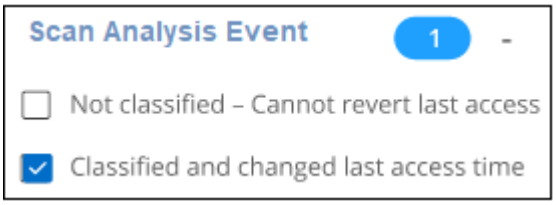
BlueXPの分類でファイル共有からデータが抽出されると、オペレーティングシステムはそのデータにアクセスしているとみなし、それに応じて「最終アクセス時間」が変更されます。BlueXPの分類では、スキャンの完了後に最終アクセス時刻を元のタイムスタンプに戻します。BlueXPの分類にCIFSでは属性への書き込み権限、NFSでは書き込み権限がない場合、最終アクセス時間を元のタイムスタンプに戻すことはできません。SnapLock が設定されたONTAP ボリュームには読み取り専用権限が設定され、最終アクセス時間を元のタイムスタンプに戻すこともできません。

BlueXPの分類では「最終アクセス日時」を元のタイムスタンプに戻すことができないため、BlueXPの分類にこれらの権限がないとボリューム内のファイルはデフォルトでスキャンされません。ただし、最終アクセス時刻がファイルの元の時刻にリセットされていてもかまわない場合は、[設定]ページの下部にある*[書き込み属性]権限がない場合にスキャン]*スイッチをクリックすると、権限に関係なくBlueXPの分類でボリュームがスキャンされるようになります。



この機能は、オンプレミスのONTAP システム、Cloud Volumes ONTAP 、Azure NetApp Files 、FSx for ONTAP 、ネットアップ以外のファイル共有に適用されます。

[Investigation]ページには、_Scan Analysis Event_というフィルタがあります。BlueXPの分類では最終アクセス時刻を元に戻すことができなかったため、分類されなかったファイルを表示できます。 または、BlueXPの分類で最終アクセス時間を元に戻すことができなかったにもかかわらず、分類されたファイル。



フィルタの選択項目は次のとおりです。

- 「Not Classified — Cannot revert last access time」-書き込み権限がないために分類されなかったファイルが表示されます。
- 「Classified and updated last access time」-分類されたファイルと、BlueXPの分類で最終アクセス時刻を元の日付にリセットできなかったファイルが表示されます。このフィルタは、*「属性の書き込み」権限がない場合にスキャン*をオンにした環境にのみ適用されます。

必要に応じて、これらの結果をレポートにエクスポートして、権限が原因でスキャンされているファイル、またはスキャンされていないファイルを確認できます。 "詳細については、データ調査レポートを参照してください"。

BlueXP分類システムにログインする

場合によっては、ログファイルにアクセスしたり構成ファイルを編集したりするために、BlueXP分類システムへのログインが必要になることがあります。

BlueXP分類がオンプレミスのLinuxマシンまたはクラウドに導入したLinuxマシンにインストールされている場合は、構成ファイルとスクリプトに直接アクセスできます。

BlueXP分類をクラウドに導入する場合は、BlueXP分類インスタンスにSSHで接続する必要があります。システムにSSHするには、ユーザとパスワードを入力するか、BlueXPコネクタのインストール時に入力したSSHキーを使用します。SSHコマンドは次のとおりです。

```
 ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
* <path-to_The _ssh_key>= SSH認証キーの場所
* <machine_user>：
```

+
AWSの場合：**<ec2-user>**を使用します
Azureの場合：BlueXPインスタンス用に作成したユーザを使用します
** GCPの場合：BlueXPインスタンス用に作成されたユーザーを使用します

- <datasension_IP>=仮想マシンインスタンスのIPアドレス

クラウドのシステムにアクセスするには、セキュリティグループのインバウンドルールを変更する必要があります。詳細については、以下を参照してください。

- "AWSのセキュリティグループのルール"
- "Azureのセキュリティグループルール"
- "Google Cloudのファイアウォールルール"

BlueXP分類API

Web UIから使用できるBlueXPの分類機能は、Swagger APIからも使用できます。

BlueXPでは、UIのタブに対応する4つのカテゴリが定義されています。

- 調査
- コンプライアンス
- ガバナンス
- 設定

Swaggerドキュメントに記載されているAPIを使用して、検索、データの集約、スキャンの追跡、コピーや移動などのアクションの作成を行うことができます。

概要

APIでは、次の機能を実行できます。

- 情報のエクスポート
  - UIで使用可能なすべての情報をAPI経由でエクスポート可能（レポートを除く）
  - データはJSON形式でエクスポートされます（Splunkなどのサードパーティアプリケーションに簡単に解析してプッシュできます）。
- 「AND」および「OR」ステートメントを使用してクエリを作成したり、情報を含めたり除外したりすることができます。

  たとえば、FILES_without_Specific Personal Identifiable Information（PII）（UIでは使用できない機能）を検索できます。エクスポート操作の特定のフィールドを除外することもできます。

- アクションの実行
  - CIFSクレデンシャルの更新
  - アクションの表示とキャンセル
  - ディレクトリの再スキャン
  - ユーザーの削除、コピー、ラベル付け、データへの割り当て
  - ファイルのクローニングとコピー
  - データをエクスポートします

このAPIはセキュアで、UIと同じ認証方式を使用します。認証の詳細については、次のページを参照してください。 https://docs.netapp.com/us-en/bluexp-automation/platform/get_identifiers.html

Swagger APIリファレンスへのアクセス

Swaggerにアクセスするには、BlueXP分類インスタンスのIPアドレスが必要です。クラウド展開の場合は、パブリックIPアドレスを使用します。次に、次のエンドポイントにアクセスする必要があります。

https://<classification_ip>/documentation

APIを使用した例

次の例は、ファイルをコピーするAPI呼び出しを示しています。

API要求

[調査]タブにすべてのフィルタを表示するには、作業環境に関連するすべてのフィールドとオプションを最初に取得する必要があります。

```
curl -X GET "http://{classification_ip}/api/{classification_version}
/search/options?data_mode=ALL_EXTRACTABLE" -H "accept: application/json"
-H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR…… " -H "x-agent-id:
hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients"
```

応答

```
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "string",
      "is_rulable": true,
      "name": "string",
      "operators": [
        "EQUALS"
      ],
      "optional_values": [
```

```
        {}
      ],
      "secondary": {},
      "server_data": false,
      "type": "TEXT"
    }
  ]
}
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "POLICIES",
      "name": "Policies",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "EXTRACTION_STATUS_RANGE",
      "name": "Scan Analysis Status",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "SCAN_ANALYSIS_ERROR",
      "name": "Scan Analysis Event",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
```

```
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "PUBLIC_ACCESS",
      "name": "Open Permissions",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": true,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "USERS_PERMISSIONS_COUNT_RANGE",
      "name": "Number of Users with Access",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": true,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "USER_GROUP_PERMISSIONS",
      "name": "User / Group Permissions",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_OWNER",
      "name": "File Owner",
      "operators": [
        "EQUALS",
        "CONTAINS"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
```

```
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ENVIRONMENT_TYPE",
      "name": "Working Environment Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ENVIRONMENT",
      "name": "Working Environment",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "SCAN_TASK",
      "name": "Storage Repository",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_PATH",
      "name": "File / Directory Path",
      "operators": [
        "MULTI_CONTAINS",
        "MULTI_EXCLUDE"
      ],
      "server_data": true,
      "type": "MULTI_TEXT"
```

```
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_DASHBOARD_EXTRACTABLE",
      "field": "CATEGORY",
      "name": "Category",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_SENSITIVITY_LEVEL",
      "name": "Sensitivity Level",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "NUMBER_OF_IDENTIFIERS",
      "name": "Number of identifiers",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_PERSONAL",
      "name": "Personal Data",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
```

```
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_SENSITIVE",
      "name": "Sensitive Personal Data",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "DATA_SUBJECT",
      "name": "Data Subject",
      "operators": [
        "EQUALS",
        "CONTAINS"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "DIRECTORIES",
      "field": "DIRECTORY_TYPE",
      "name": "Directory Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "FILE_TYPE",
      "name": "File Type",
      "operators": [
        "IN",
        "NOT_IN"
```

```
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "FILE_SIZE_RANGE",
      "name": "File Size",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_CREATION_RANGE_RETENTION",
      "name": "Created Time",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "DISCOVERED_TIME_RANGE",
      "name": "Discovered Time",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_LAST_MODIFICATION_RETENTION",
      "name": "Last Modified",
      "operators": [
        "IN"
      ],
```

```
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_LAST_ACCESS_RANGE_RETENTION",
      "name": "Last Accessed",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "FILES",
      "field": "IS_DUPLICATE",
      "name": "Duplicates",
      "operators": [
        "EQUALS",
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "FILES",
      "field": "FILE_HASH",
      "name": "File Hash",
      "operators": [
        "EQUALS",
        "IN"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "USER_DEFINED_STATUS",
      "name": "Tags",
      "operators": [
        "IN",
        "NOT_IN"
```

```
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ASSIGNED_TO",
      "name": "Assigned to",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    }
  ]
}
```

この応答をリクエストパラメータで使用して、コピーする必要なファイルをフィルタリングします。

1つのアクションを複数の項目に適用できます。サポートされるアクションタイプは、移動、削除、コピー、割り当て先、FlexClone、 データのエクスポート、再スキャン、およびラベル付けを行います。

コピーアクションを作成します。

API要求

次のAPIはアクションAPIで、複数のアクションを作成できます。

```
curl -X POST "http://
{classification_ip}/api//{classification_version}/actions" -H "accept:
application/json" -H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR…… "
-H "x-agent-id: hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients " -H "Content-
Type: application/json" -d "{ \"action_type\": \"COPY\", \"data_mode\":
\"FILES\", \"policy_id\": 0, \"request_params\": { destination_nfs_path:
"{ontap_ip}:/{share_name} " },
\"requested_query\":{"condition":"AND","rules":[{"field":"ENVIRONMENT_TYPE
","operator":"IN","value":["ONPREM"]},{"field":"CATEGORY","operator":"IN",
"value":["21"]}]}}"
```

応答

応答ではActionオブジェクトが返されるため、GETおよびDELETE APIを使用してアクションのステータスを取得したり、アクションをキャンセルしたりできます。

```
{
  "action_type": "COPY",
  "creation_time": "2023-08-08T12:37:21.705Z",
  "data_mode": "FILES",
  "end_time": "2023-08-08T12:37:21.705Z",
  "estimated_time_to_complete": 0,
  "id": 0,
  "policy_id": 0,
  "policy_name": "string",
  "priority": 0,
  "request_params": {},
  "requested_query": {},
  "result": {
    "error_message": "string",
    "failed": 0,
    "in_progress": 0,
    "succeeded": 0,
    "total": 0
  },
  "start_time": "2023-08-08T12:37:21.705Z",
  "status": "QUEUED",
  "title": "string",
  "user_id": "string"
}
```

知識とサポート

サポートに登録します

BlueXPとそのストレージソリューションおよびサービスに固有のテクニカルサポートを受けるには、サポート登録が必要です。Cloud Volumes ONTAPシステムの主要なワークフローを有効にするには、サポート登録も必要です。

サポートに登録しても、クラウドプロバイダのファイルサービスでNetAppのサポートは有効になりません。クラウドプロバイダのファイルサービスとそのインフラ、またはサービスを使用する解決策に関連するテクニカルサポートについては、該当する製品のBlueXPドキュメントの「困ったときは」を参照してください。

- "ONTAP 対応の Amazon FSX"
- "Azure NetApp Files の特長"
- "Cloud Volumes Service for Google Cloud"

サポート登録の概要

サポート資格を有効にする登録には、次の2つの形式があります。

- BlueXPアカウントIDサポートサブスクリプションの登録(BlueXPの[サポートリソース]ページにある20桁の960xxxxxxxxxシリアル番号)。

  これは、BlueXP内のすべてのサービスのシングルサポートサブスクリプションIDとして機能します。各BlueXPアカウントレベルのサポート契約が登録されている必要があります。

- クラウドプロバイダのマーケットプレイスでのサブスクリプションに関連付けられているCloud Volumes ONTAP のシリアル番号を登録している（909201xxxxxxxxのシリアル番号）。

  これらのシリアル番号は、通常PAY_GOシリアル番号と呼ばれ、Cloud Volumes ONTAP の導入時にBlueXPによって生成されます。

両方のタイプのシリアル番号を登録することで、サポートチケットのオープンやケースの自動生成などの機能を利用できます。登録を完了するには、以下の手順でNetApp Support Site（NSS）アカウントをBlueXPに追加してください。

NetAppサポートに**BlueXP**アカウントを登録します

サポートに登録してサポート利用資格をアクティブ化するには、BlueXPアカウントの1人のユーザがNetApp Support SiteアカウントをBlueXPログインに関連付ける必要があります。ネットアップサポートへの登録方法は、NetApp Support Site （NSS）アカウントがあるかどうかによって異なります。

NSSアカウントをお持ちの既存のお客様

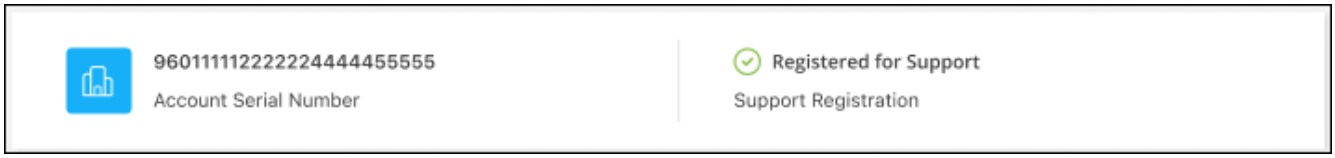
NSSアカウントをお持ちのネットアップのお客様は、BlueXPからサポートに登録するだけで済みます。

手順

1. BlueXPコンソールの右上で、[設定]アイコンを選択し、*[クレデンシャル]*を選択します。

2. [ユーザクレデンシャル]*を選択します。
3. [NSSクレデンシャルの追加]*を選択し、NetApp Support Site（NSS）認証プロンプトに従います。
4. 登録プロセスが正常に完了したことを確認するには、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。

   [リソース]ページに、アカウントがサポートに登録されていることが表示されます。

   他のBlueXPユーザにNetApp Support Siteアカウントが関連付けられていない場合、このサポート登録ステータスは表示されません。ただし、BlueXPアカウントがサポートに登録されていないわけではありません。アカウント内の1人のユーザーがこれらの手順を実行している限り、アカウントは登録されています。

NSSアカウントを持たない既存のお客様

NetAppの既存のお客様で、ライセンスとシリアル番号は_NO_NSSアカウントしかお持ちでない場合は、NSSアカウントを作成してBlueXPログインに関連付ける必要があります。

手順

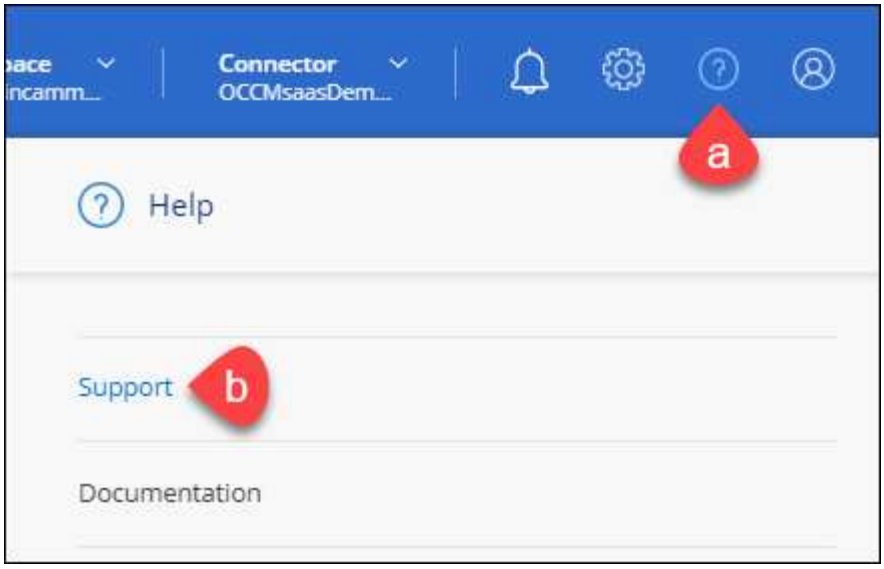
1. を実行してNetApp Support Site アカウントを作成します "NetApp Support Site ユーザー登録フォーム"
   a. 適切なユーザレベルを選択してください。通常は*ネットアップのお客様/エンドユーザ*がこれに該当します。
   b. 必ず、上記のシリアル番号フィールドに使用されているBlueXPアカウントのシリアル番号(960xxxx)をコピーしてください。これにより、アカウント処理が高速化されます。
2. の手順を実行して、新しいNSSアカウントをBlueXPログインに関連付けます NSSアカウントをお持ちの既存のお客様。

ネットアップのソリューションを初めて導入する場合は

ネットアップ製品を初めてご利用になり、NSSアカウントをお持ちでない場合は、以下の手順に従ってください。

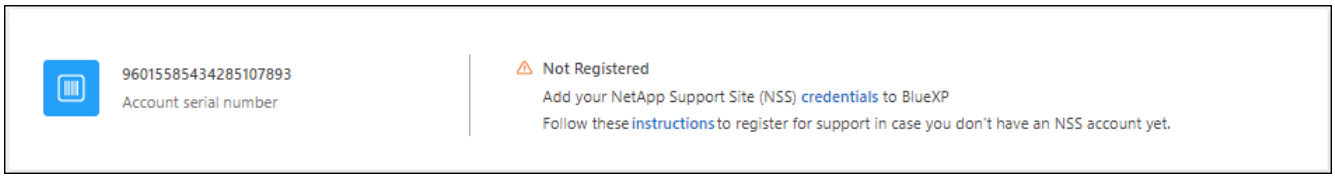
手順

1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。



メニューのスクリーンショット。サポートは最初に表示されるオプションです"]

2. サポート登録ページでアカウントIDのシリアル番号を確認します。



メニューのスクリーンショット。サポートは最初に表示されるオプションです"]

3. に移動します "ネットアップサポート登録サイト" 「ネットアップ登録のお客様ではありません」を選択します。
4. 必須フィールドに入力します（赤いアスタリスクのフィールド）。
5. [製品ライン（Product Line ）]フィールドで、[Cloud Manager *]を選択し、該当する課金プロバイダーを選択します。
6. 上記の手順2からアカウントのシリアル番号をコピーし、セキュリティチェックを完了して、ネットアップのグローバルデータプライバシーポリシーを確認します。

   この安全なトランザクションを完了するために、メールボックスに電子メールがすぐに送信されます。確認メールが数分で届かない場合は、必ずスパムフォルダを確認してください。

7. Eメールからアクションを確認します。

   確認ではネットアップにリクエストが送信され、NetApp Support Site アカウントを作成することを推奨します。

8. を実行してNetApp Support Site アカウントを作成します "NetApp Support Site ユーザー登録フォーム"
   a. 適切なユーザレベルを選択してください。通常は*ネットアップのお客様/エンドユーザ*がこれに該当します。
   b. シリアル番号フィールドには、上記のアカウントのシリアル番号（960xxxx）を必ずコピーしてください。これにより、アカウント処理が高速化されます。

完了後

このプロセスについては、ネットアップからご連絡ください。これは、新規ユーザ向けの1回限りのオンボーディング演習です。

NetApp Support Siteアカウントを作成したら、の手順を実行してアカウントをBlueXPログインに関連付けます NSSアカウントをお持ちの既存のお客様。

Cloud Volumes ONTAPサポートのためにNSSクレデンシャルを関連付けます

NetApp Support Siteで次の主要なワークフローを有効にするには、BlueXPアカウントにクレデンシャルを関連付ける必要がCloud Volumes ONTAPあります。

- 従量課金制のCloud Volumes ONTAPシステムのサポートを登録しています

  お使いのシステムのサポートを有効にし、ネットアップのテクニカルサポートリソースにアクセスするには、 NSS アカウントを用意する必要があります。

- お客様所有のライセンスを使用（BYOL）する場合のCloud Volumes ONTAP の導入

  ライセンスキーをBlueXPでアップロードし、購入した契約期間のサブスクリプションを有効にするには、NSSアカウントを提供する必要があります。これには、期間の更新の自動更新も含まれます。

- Cloud Volumes ONTAP ソフトウェアを最新リリースにアップグレードしています

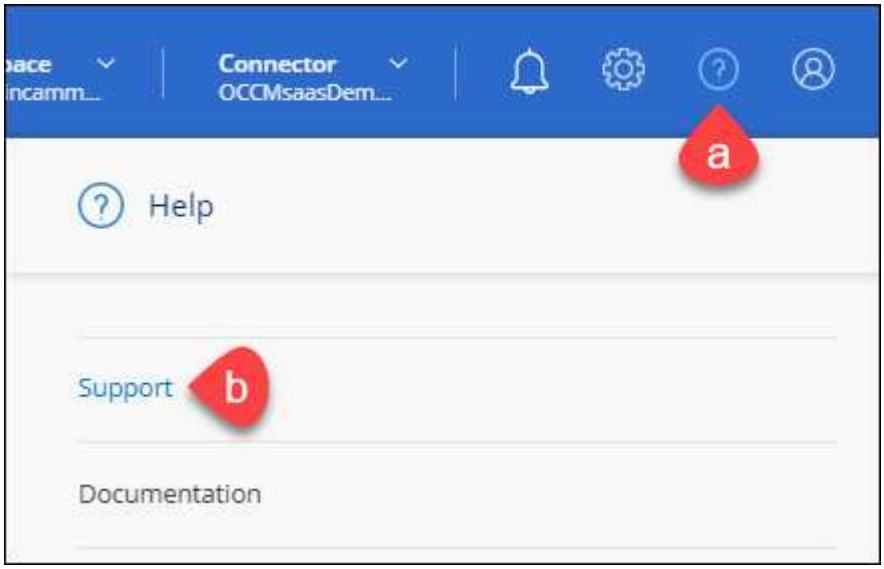
NSSクレデンシャルをBlueXPアカウントに関連付ける方法は、BlueXPユーザログインに関連付けられたNSSアカウントとは異なります。

これらのNSSクレデンシャルは、特定のBlueXPアカウントIDに関連付けられています。BlueXPアカウントに属するユーザは、*[サポート]>[NSS管理]*からこれらのクレデンシャルにアクセスできます。

- お客様レベルのアカウントをお持ちの場合は、1つ以上のNSSアカウントを追加することもできます。
- パートナーアカウントまたはリセラーアカウントをお持ちの場合は、1つ以上のNSSアカウントを追加することはできますが、お客様レベルのアカウントと一緒に追加することはできません。

手順

1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。



メニューのスクリーンショット。

サポートは最初に表示されるオプションです"]

2. [NSS Management]>[Add NSS Account]*を選択します。
3. プロンプトが表示されたら、*続行*を選択してMicrosoftログインページにリダイレクトします。

   NetAppでは、サポートとライセンスに固有の認証サービスのIDプロバイダとしてMicrosoftエントラIDを使用します。

4. ログインページで、ネットアップサポートサイトの登録 E メールアドレスとパスワードを入力して認証プロセスを実行します。

   これらのアクションにより、BlueXPはライセンスのダウンロード、ソフトウェアのアップグレード検証、および将来のサポート登録などの目的でNSSアカウントを使用できます。

   次の点に注意してください。

   - NSSアカウントは、お客様レベルのアカウントである必要があります（ゲストアカウントや一時アカウントではありません）。複数のお客様レベルのNSSアカウントを設定できます。
   - NSSアカウントがパートナーレベルのアカウントの場合、作成できるNSSアカウントは1つだけです。お客様レベルのNSSアカウントを追加しようとすると、パートナーレベルのアカウントが存在する場合は、次のエラーメッセージが表示されます。

     「別のタイプのNSSユーザーがすでに存在するため、このアカウントではNSS顧客タイプは許可されていません。」

   既存のお客様レベルのNSSアカウントがあり、パートナーレベルのアカウントを追加しようとする場合も同様です。

   - ログインに成功すると、ネットアップはNSSのユーザ名を保存します。

     これはシステムによって生成されたIDで、電子メールにマッピングされます。[**NSS Management**]ページで、から電子メールを表示できます ••• メニュー。

   - ログイン認証情報トークンを更新する必要がある場合は、の[認証情報の更新*]オプションも使用できます ••• メニュー。

     このオプションを使用すると、再度ログインするように求められます。これらのアカウントのトークンは90日後に期限切れになります。このことを通知する通知が投稿されます。

ヘルプを表示します

ネットアップでは、BlueXPとその クラウド サービス をさまざまな方法でサポートしています。ナレッジベース（ KB ）記事やコミュニティフォーラムなど、 24 時間 365 日利用可能な幅広いセルフサポートオプションをご用意しています。サポート登録には、Web チケット処理によるリモートテクニカルサポートが含まれます。

クラウドプロバイダのファイルサービスのサポート

クラウドプロバイダのファイルサービスとそのインフラ、またはサービスを使用する解決策に関連するテクニカルサポートについては、該当する製品のBlueXPドキュメントの「困ったときは」を参照してください。

- "ONTAP 対応の Amazon FSX"
- "Azure NetApp Files の特長"
- "Cloud Volumes Service for Google Cloud"

BlueXPおよびそのストレージソリューションとサービスに固有のテクニカルサポートを受けるには、以下に記載されているサポートオプションを使用してください。

セルフサポートオプションを使用します

次のオプションは、 1 日 24 時間、週 7 日間無料でご利用いただけます。

- ドキュメント

  現在表示しているBlueXPのマニュアル。

- "ナレッジベース"

  BlueXPナレッジベースで問題のトラブルシューティングに役立つ記事を検索します。

- "コミュニティ"

  BlueXPコミュニティに参加して、進行中のディスカッションをフォローしたり、新しいディスカッションを作成したりできます。

ネットアップサポートと一緒にケースを作成します

上記のセルフサポートオプションに加え、サポートを有効にしたあとで問題が発生した場合は、ネットアップサポートの担当者と相談して解決できます。

始める前に

- [ケースの作成]*機能を使用するには、最初にNetApp Support SiteクレデンシャルをBlueXPログインに関連付ける必要があります。 "BlueXPログインに関連付けられているクレデンシャルの管理方法について説明します"。
- シリアル番号のあるONTAPシステムのケースをオープンする場合は、そのシステムのシリアル番号にNSSアカウントを関連付ける必要があります。

手順

1. BlueXPで、*[ヘルプ]>[サポート]*を選択します。
2. [**Resources**]ページで、[Technical Support]で次のいずれかのオプションを選択します。

   a. 電話で誰かと話をしたい場合は、*[電話]*を選択します。netapp.comのページに移動し、電話番号が表示されます。

   b. [ケースの作成]*を選択して、NetAppサポートスペシャリストとのチケットをオープンします。

      - **Service**:問題 が関連付けられているサービスを選択します。たとえば、サービス内のワークフローまたは機能を備えたテクニカルサポート問題 に固有のBlueXPなどです。
      - 作業環境：ストレージに該当する場合は、* Cloud Volumes ONTAP *または*オンプレミス*を選択し、関連する作業環境を選択します。

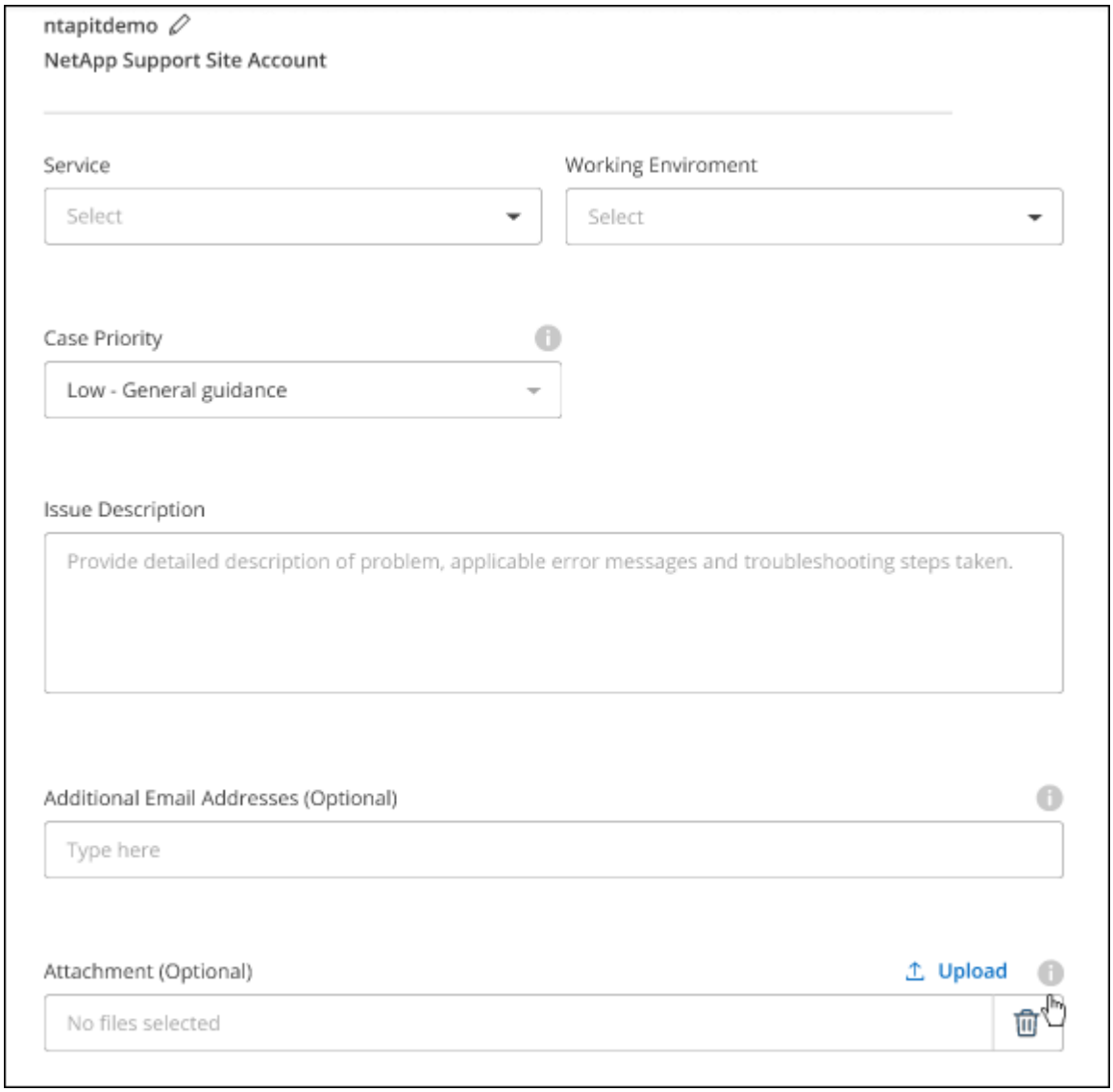
作業環境のリストは、サービスの上部バナーで選択したBlueXPアカウント、ワークスペース、コネクタの範囲内にあります。

- ケース優先度：ケースの優先度を選択します。優先度は、[低]、[中]、[高]、[クリティカル]のいずれかになります。

  これらの優先度の詳細を確認するには、フィールド名の横にある情報アイコンの上にマウスポインタを合わせます。

- *事象の説明 *：実行したエラーメッセージやトラブルシューティング手順など、問題の詳細な概要 を入力します。
- その他のメールアドレス：この問題 を他のユーザーに知らせる場合は、追加のメールアドレスを入力します。
- 添付ファイル（オプション）：一度に1つずつ、最大5つの添付ファイルをアップロードできます。

  添付ファイルはファイルあたり25 MBに制限されています。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、 doc/docx、xls/xlsx、およびcsv。



完了後

ポップアップにサポートケース番号が表示されます。ネットアップのサポート担当者がケースを確認し、すぐに対応させていただきます。

サポートケースの履歴を確認するには、*[設定]>[タイムライン]*を選択し、「サポートケースの作成」というアクションを検索します。 右端のボタンをクリックすると、アクションを展開して詳細を表示できます。

ケースを作成しようとすると、次のエラーメッセージが表示される場合があります。

"選択したサービスに対してケースを作成する権限がありません"

このエラーは、NSSアカウントとそれに関連付けられているレコードの会社が、BlueXPアカウントのシリアル番号(例960xxxx）または動作環境のシリアル番号。次のいずれかのオプションを使用して、サポートを受けることができます。

- 製品内のチャットを使用します
- テクニカル以外のケースをに送信します https://mysupport.netapp.com/site/help

サポートケースの管理（プレビュー）

アクティブなサポートケースと解決済みのサポートケースは、BlueXPから直接表示および管理できます。NSSアカウントと会社に関連付けられたケースを管理できます。

ケース管理はプレビューとして使用できます。今後のリリースでは、この点をさらに改良し、機能を強化する予定です。製品内のチャットでご意見をお寄せください。

次の点に注意してください。

- ページ上部のケース管理ダッシュボードには、次の2つのビューがあります。
  - 左側のビューには、指定したユーザNSSアカウントによって過去3カ月間にオープンされたケースの総数が表示されます。
  - 右側のビューには、ユーザのNSSアカウントに基づいて、過去3カ月間にオープンしたケースの総数が会社レベルで表示されます。

  テーブルの結果には、選択したビューに関連するケースが反映されます。
- 目的の列を追加または削除したり、[優先度]や[ステータス]などの列の内容をフィルタリングしたりできます。他の列には、並べ替え機能だけがあります。

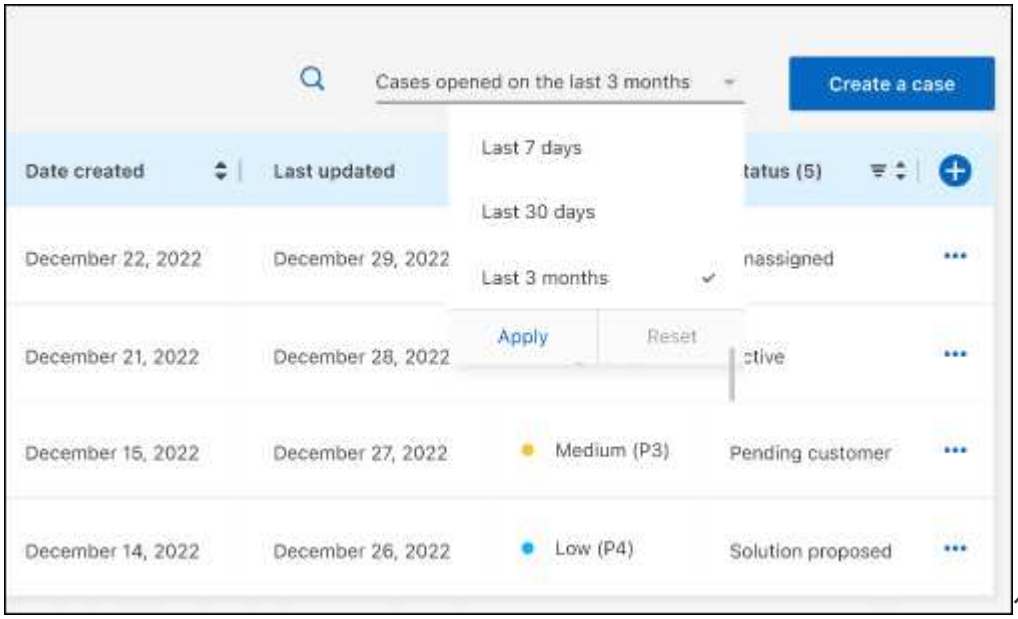
  詳細については、以下の手順を参照してください。
- ケースごとに、ケースノートを更新したり、ステータスが「Closed」または「Pending Closed」でないケースをクローズしたりすることができます。

手順

1. BlueXPで、*[ヘルプ]>[サポート]*を選択します。
2. [ケース管理]*を選択し、プロンプトが表示されたらNSSアカウントをBlueXPに追加します。

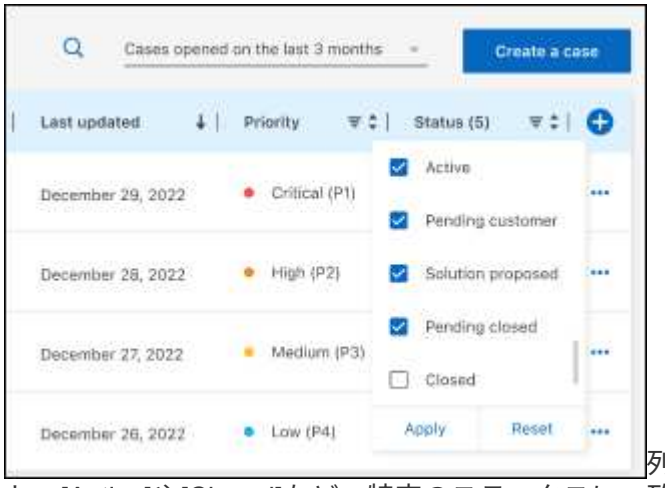
   ケース管理*ページには、BlueXPユーザアカウントに関連付けられたNSSアカウントに関連するオープンケースが表示されます。これは、* NSS管理*ページの上部に表示されるNSSアカウントと同じです。

3. 必要に応じて、テーブルに表示される情報を変更します。
    - [Organization’s Cases]*で[View]*を選択すると、会社に関連付けられているすべてのケースが表示されます。
    - 正確な日付範囲を選択するか、別の期間を選択して、日付範囲を変更します。



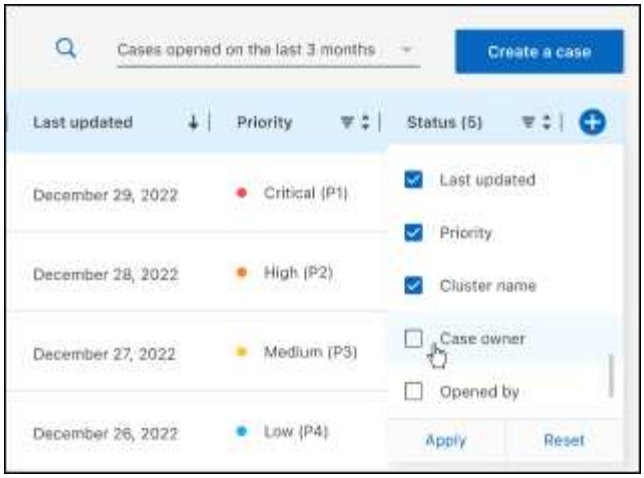
ページのテーブルの上にあるオプションのスクリーンショット。正確な日付範囲、または過去7日、30日、または3カ月を選択できます。"]

    - 列の内容をフィルタリングします。



列のフィルタオプションのスクリーンショット。[Active]や[Closed]など、特定のステータスに一致するケースを除外できます。"]

    - テーブルに表示される列を変更するには、 次に、表示する列を選択します。

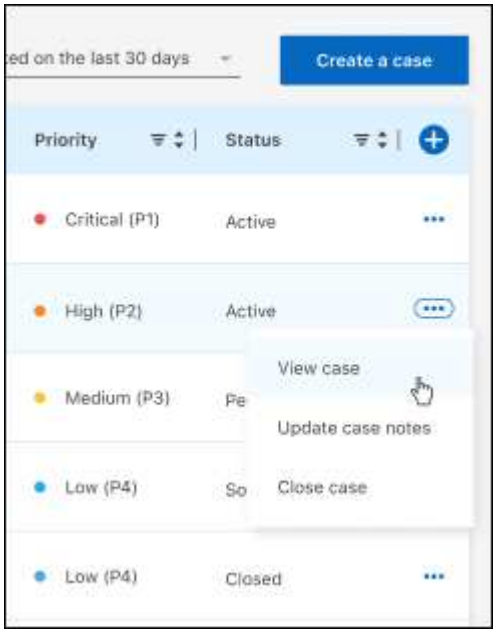


4. 既存のケースを管理するには、 ••• 使用可能なオプションのいずれかを選択します。

   - ケースの表示:特定のケースの詳細を表示します。
   - ケースノートの更新：問題の詳細を入力するか、*ファイルのアップロード*を選択して最大5つのファイルを添付します。

     添付ファイルはファイルあたり25 MBに制限されています。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、 doc/docx、xls/xlsx、およびcsv。

   - ケースをクローズ：ケースをクローズする理由の詳細を入力し、*ケースをクローズ*を選択します。



法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp 、 NetApp のロゴ、および NetApp の商標ページに記載されているマークは、 NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシーポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

- "BlueXPに関する注意事項"
- "BlueXPに分類されました"