はじめに
BlueXP classification

NetApp
April 03, 2024

目次

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。

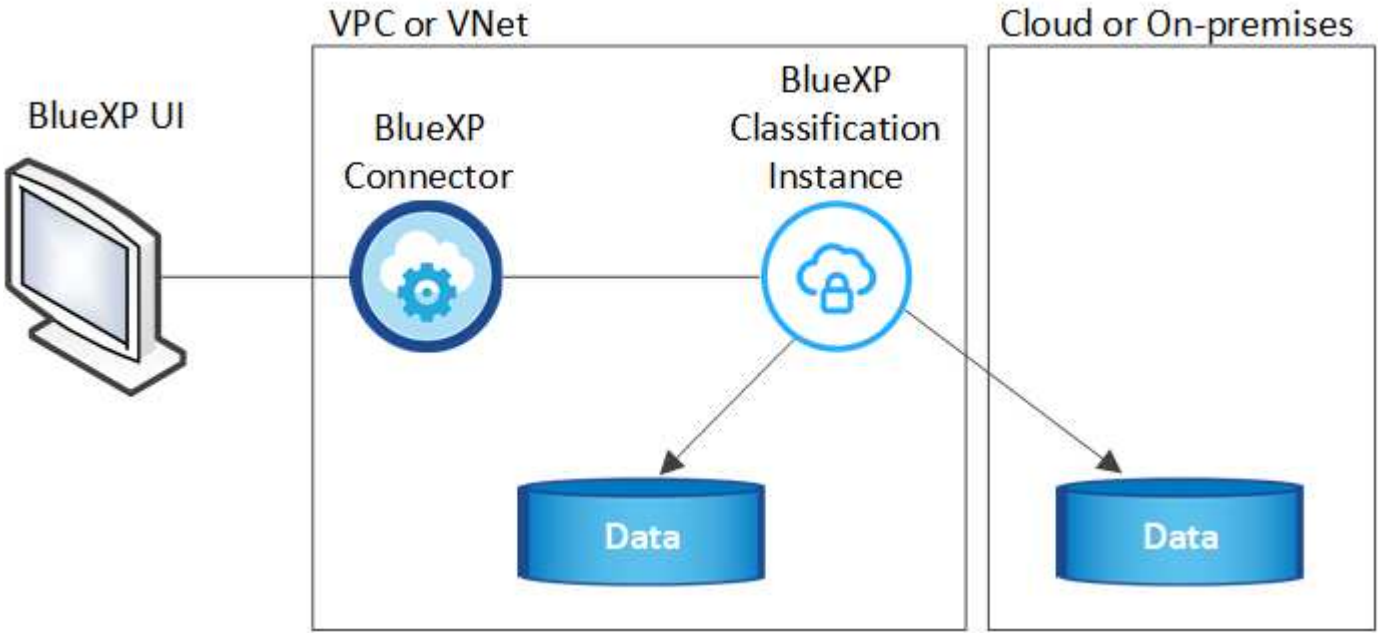
データ転送コスト

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。

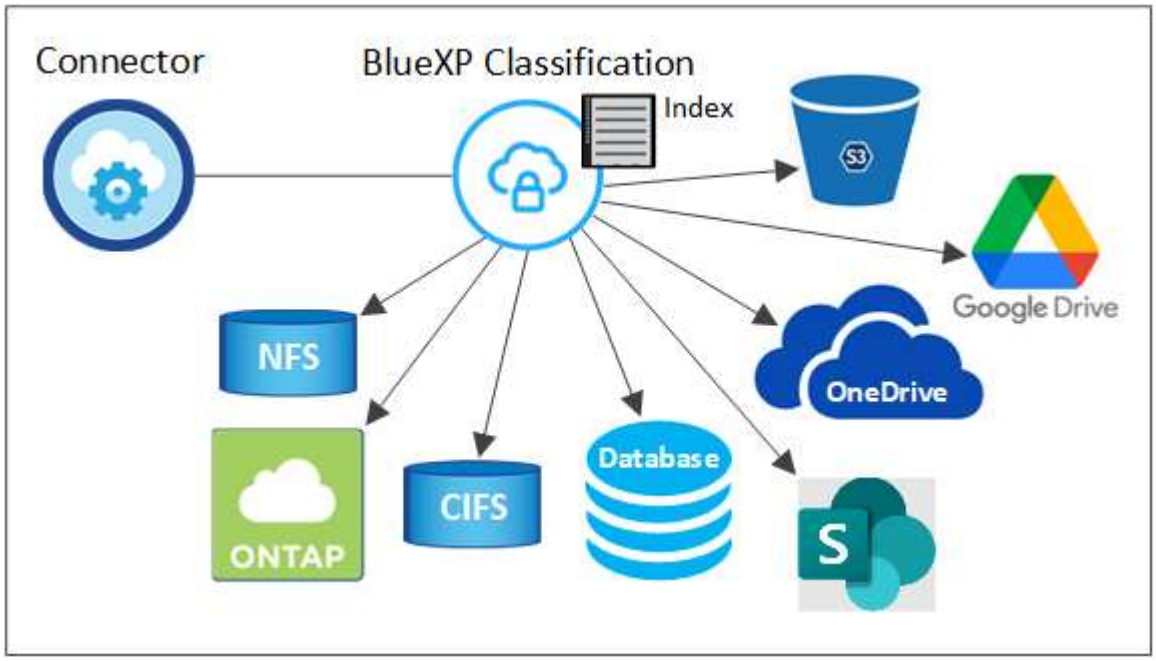
1. BlueXPでBlueXP分類のインスタンスを導入します。
2. 1つ以上のデータソースで、概要レベルのマッピングまたは詳細レベルのスキャンを有効にします。
3. BlueXPの分類では、AI学習プロセスを使用してデータがスキャンされます。
4. 提供されているダッシュボードとレポートツールを使用して、コンプライアンスとガバナンスの取り組みを支援します。

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

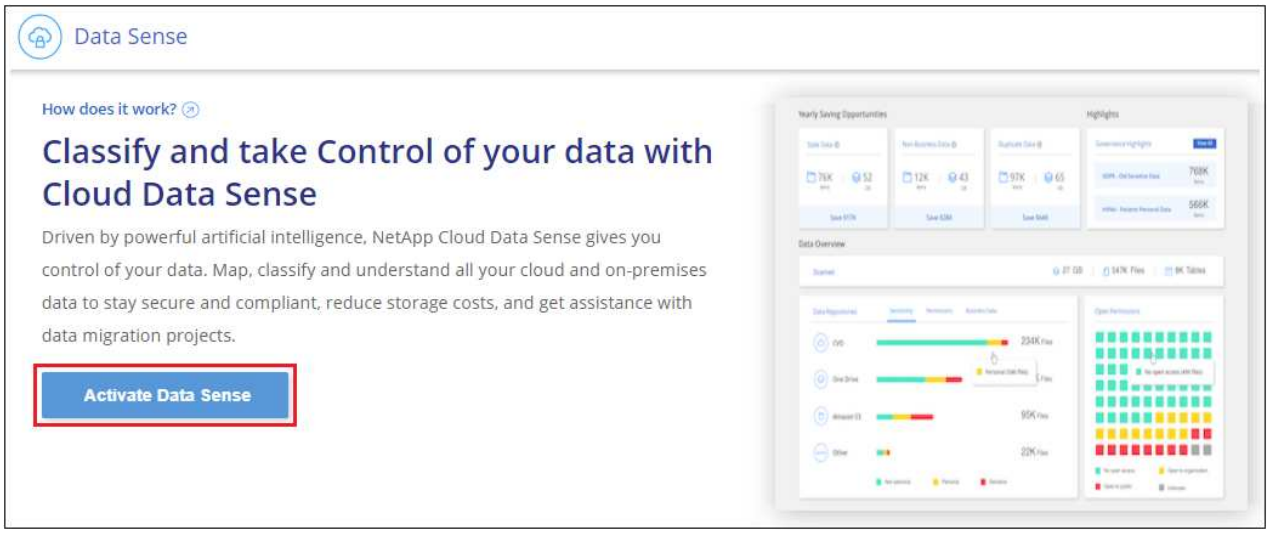
BlueXP分類のインスタンスをクラウドに導入するには、次の手順を実行します。コネクタはインスタンスをクラウドに導入し、そのインスタンスにBlueXP分類ソフトウェアをインストールします。

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。



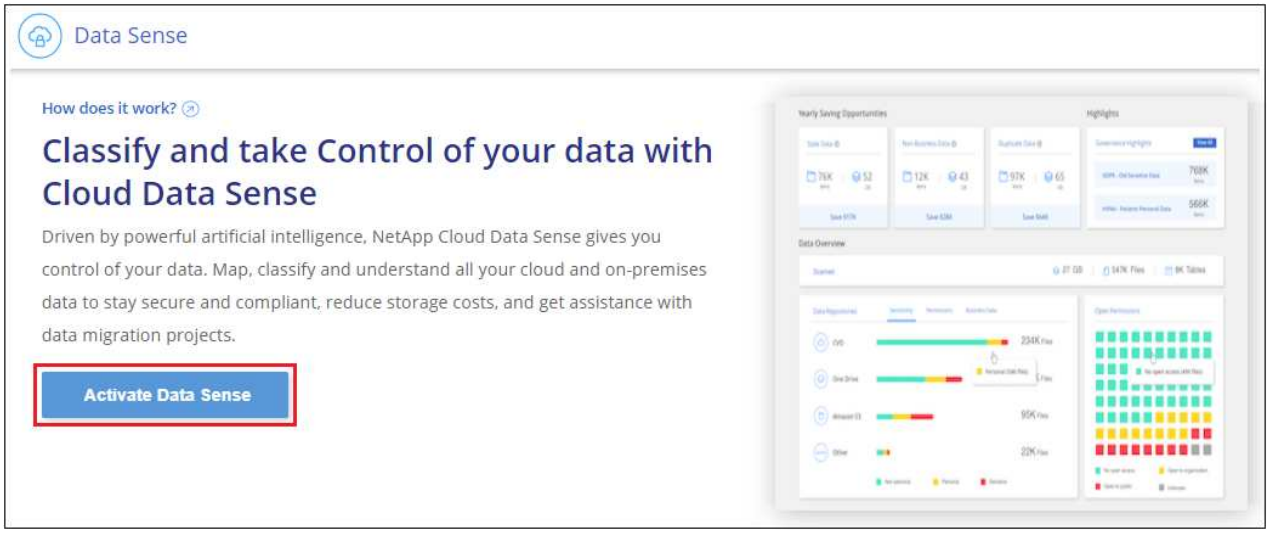
2. [データセンスを活動化（ Activate Data sense ）] をクリックし
3. [*Installation*]ページで、*[Deploy]>[Deploy]*をクリックして「Large」インスタンスサイズを使用し、クラウド導入ウィザードを開始します。
4. 導入手順が完了すると、ウィザードに進捗状況が表示されます。問題が発生した場合は、停止して入力を求められます。

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。

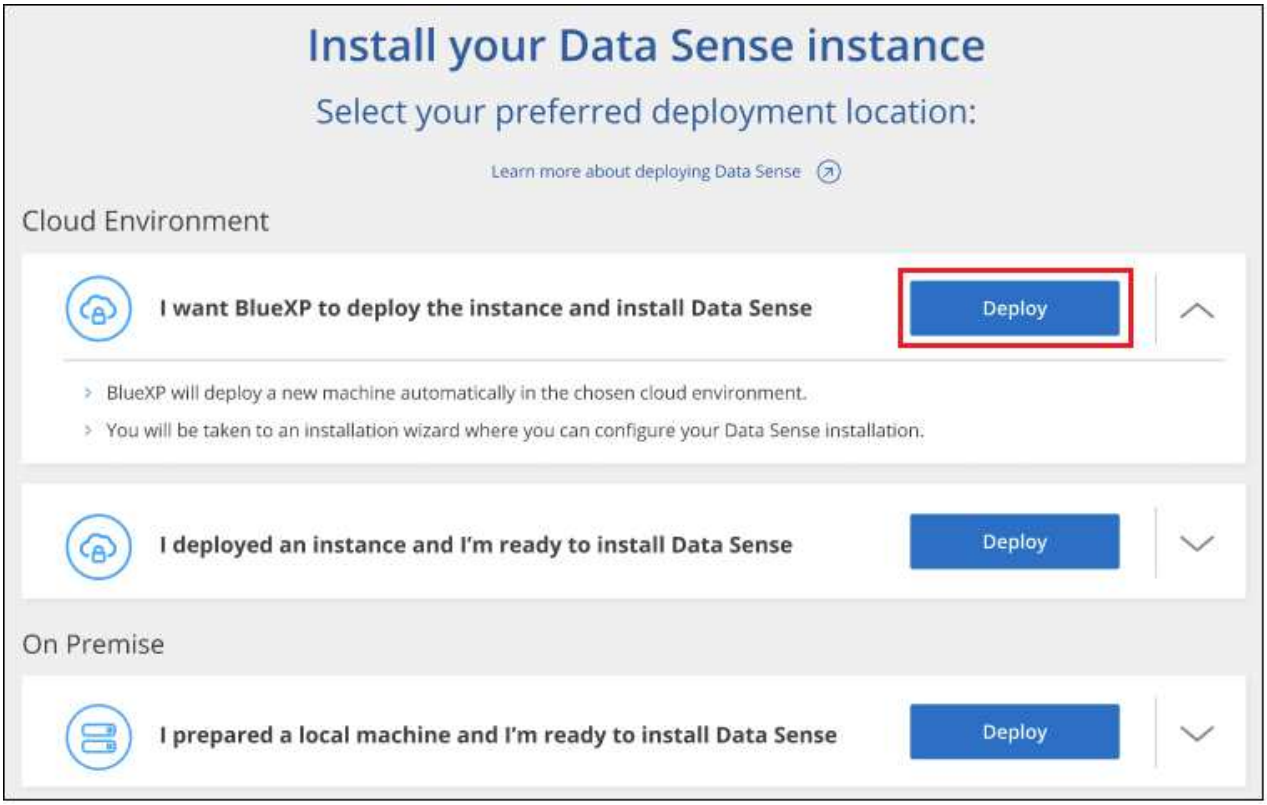
Azureへの導入

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。



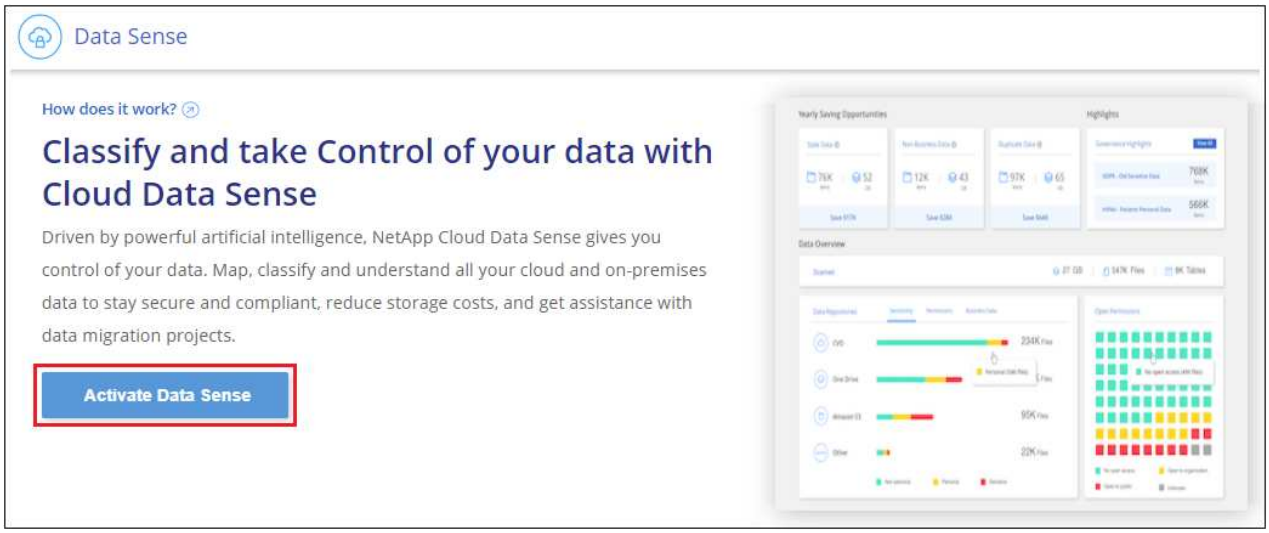
4. 導入手順が完了すると、ウィザードに進捗状況が表示されます。問題が発生した場合は、停止して入力を求められます。

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。

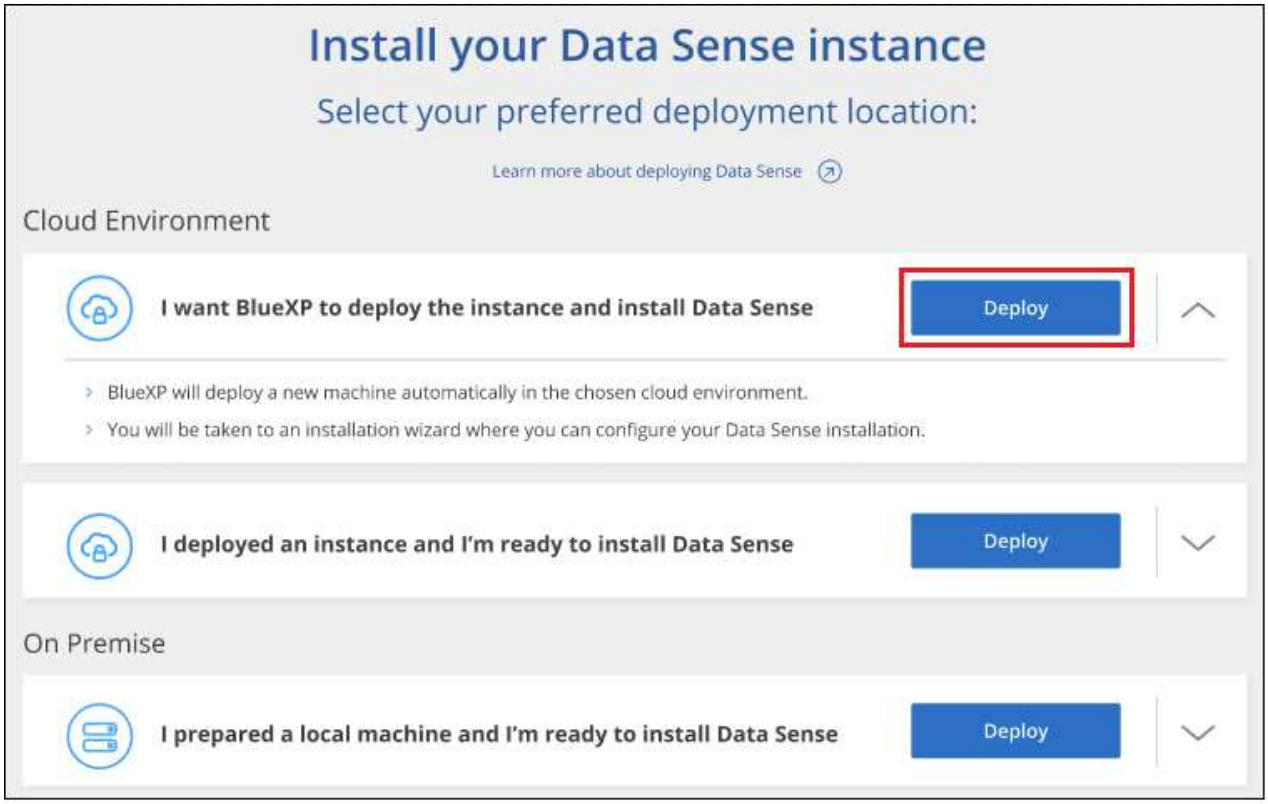
Google Cloudに導入

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。

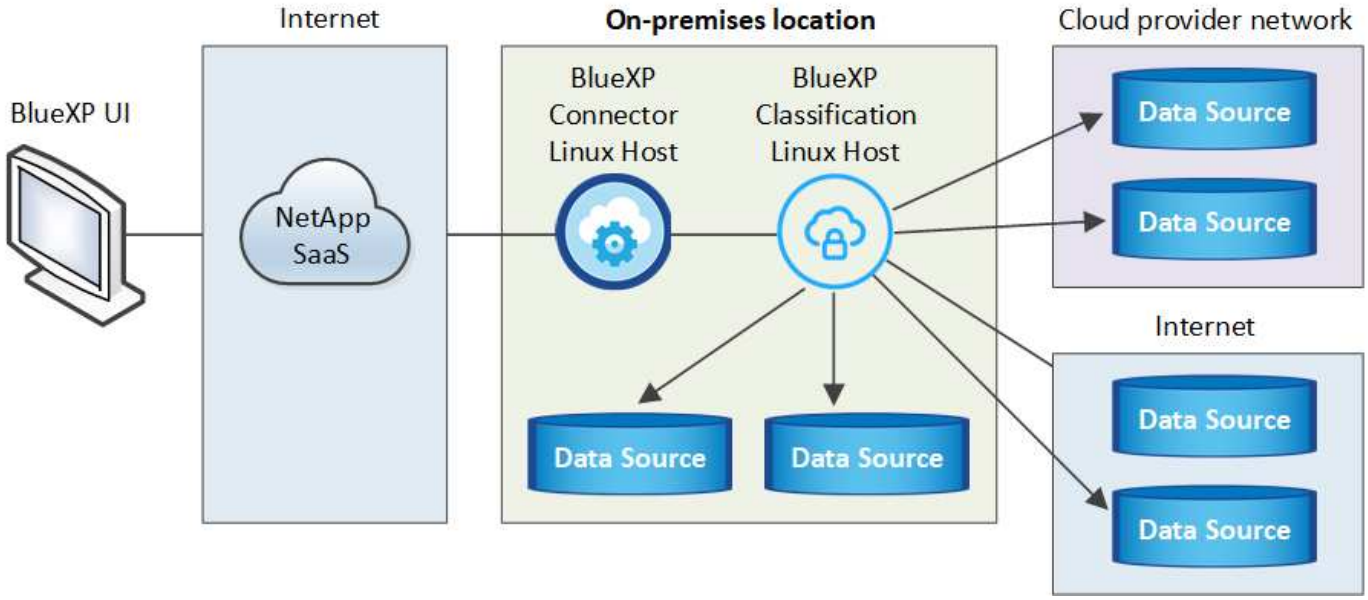
インターネットにアクセスできるホストに**BlueXP**分類をインストールします

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。

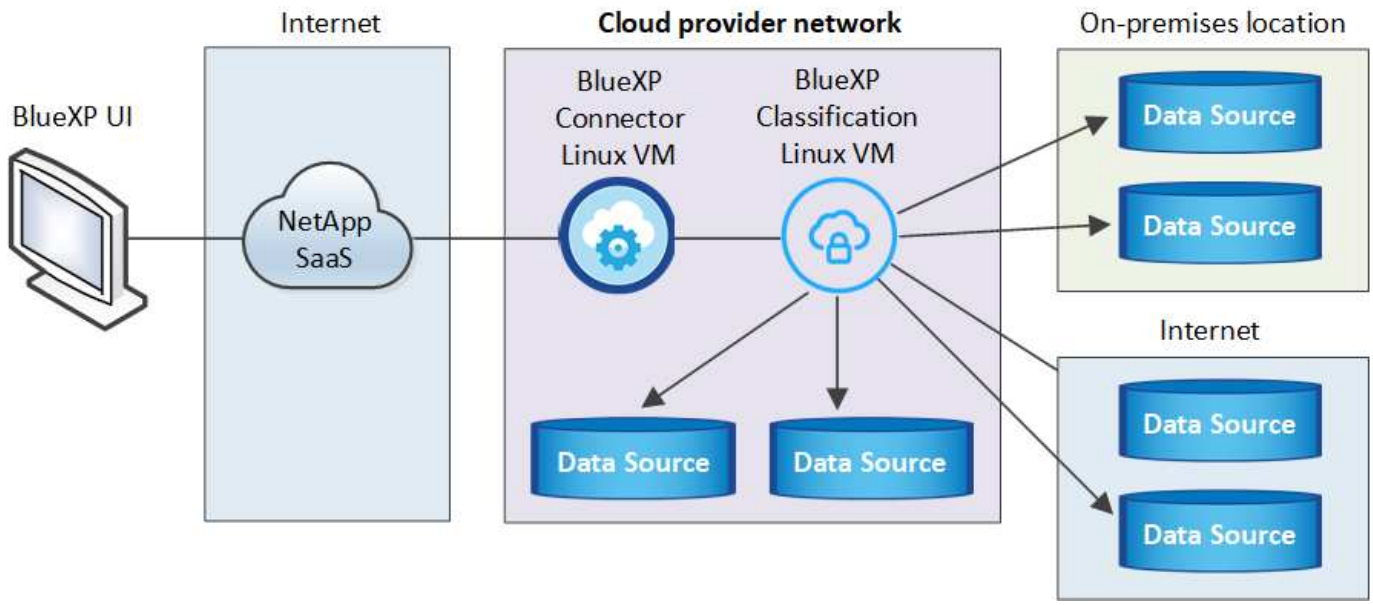
オンプレミス環境は、同じくオンプレミスにあるBlueXP分類インスタンスを使用してオンプレミスのONTAPシステムをスキャンする場合に適したオプションですが、これは必須ではありません。どのインストール方法を選択しても、ソフトウェアはまったく同じように機能します。

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。

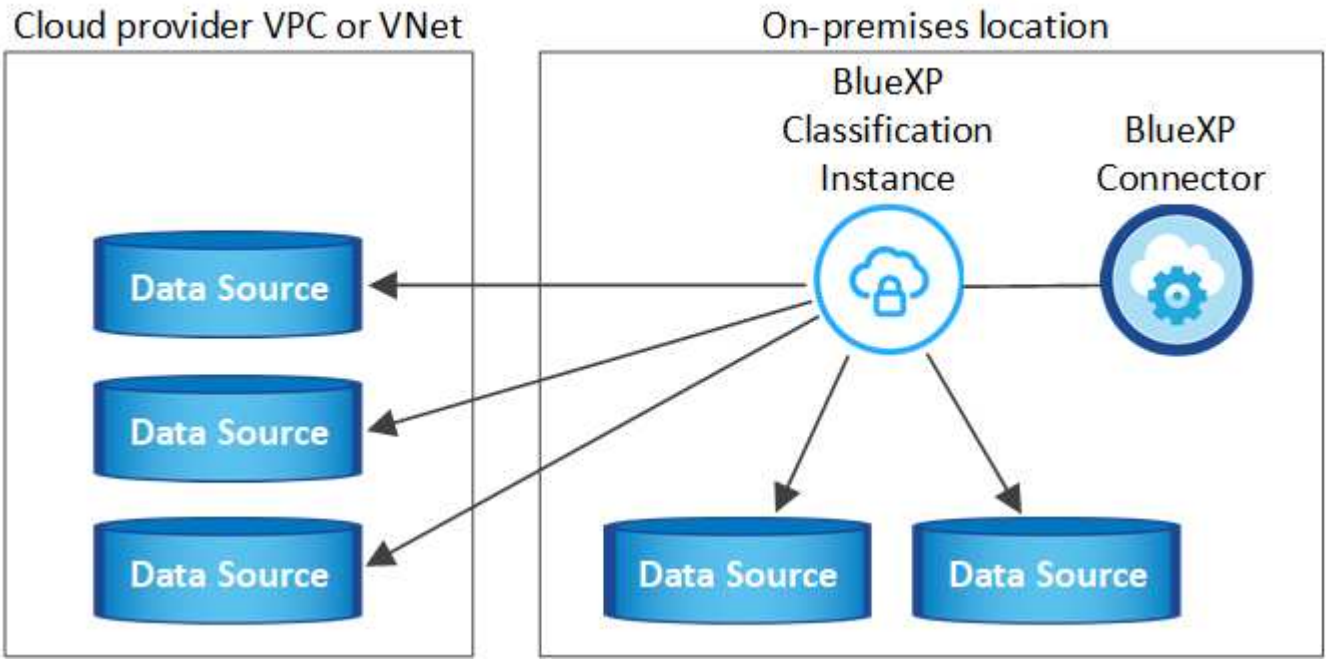
接続タイプ	ポート	説明
コネクタ<> BlueXPの分類	8080（TCP）、443（TCP）、および80	コネクタのファイアウォールルールまたはルーティングルールで、ポート443を介したBlueXP分類インスタンスとの間のインバウンドおよびアウトバウンドトラフィックを許可する必要があります。ポート8080が開いていることを確認し、BlueXPでインストールの進行状況を確認します。
Connector <> ONTAP cluster（NAS）	443（TCP）	BlueXPはHTTPSを使用してONTAP クラスタを検出しましたカスタムファイアウォールポリシーを使用する場合は、次の要件を満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 ）

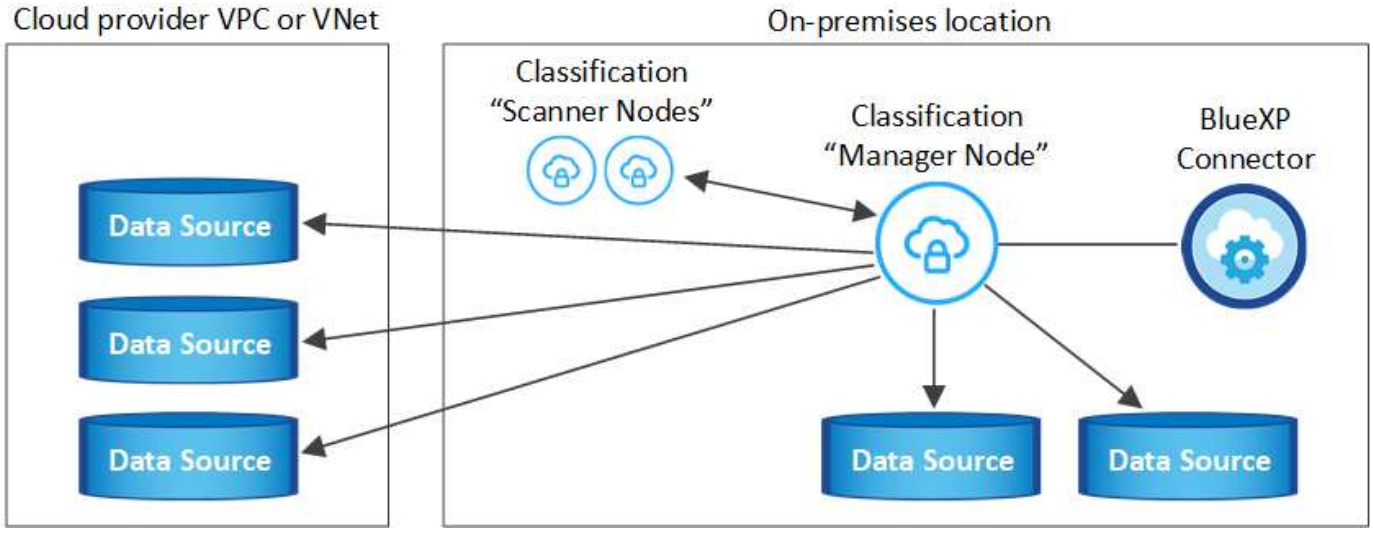
複数のBlueXP分類ホストを使用してデータソースのスキャンに必要な処理能力を提供している場合は、追加のポート/プロトコルを有効にする必要があります。 "追加のポート要件を参照してください"。

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。

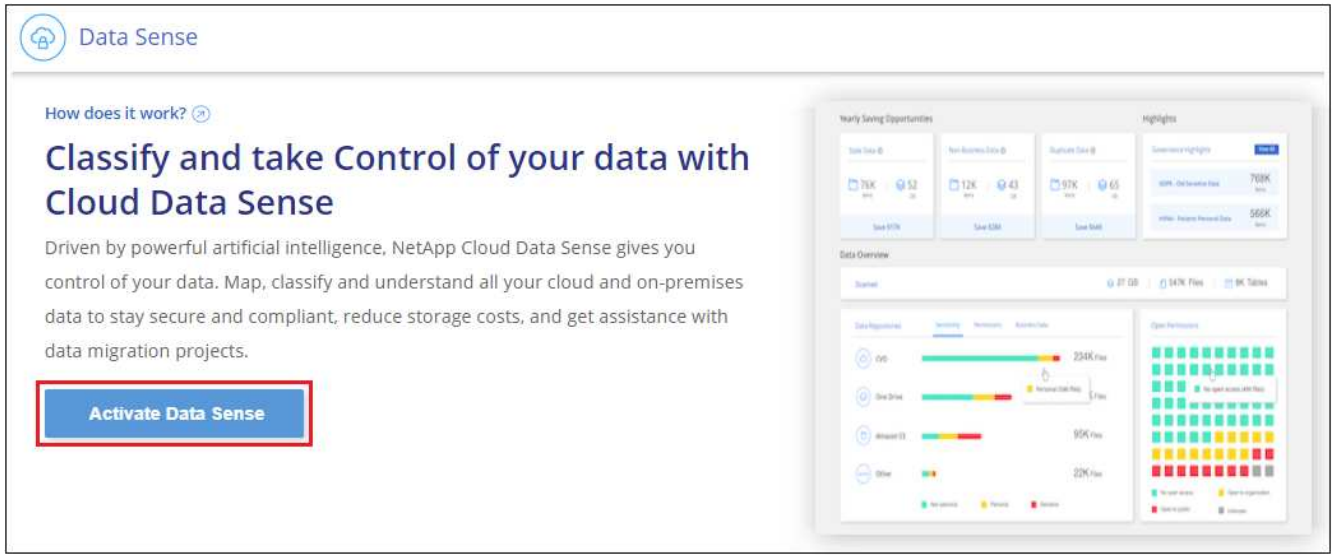
- オフライン環境が要件を満たしていることを確認します 権限と接続。

手順

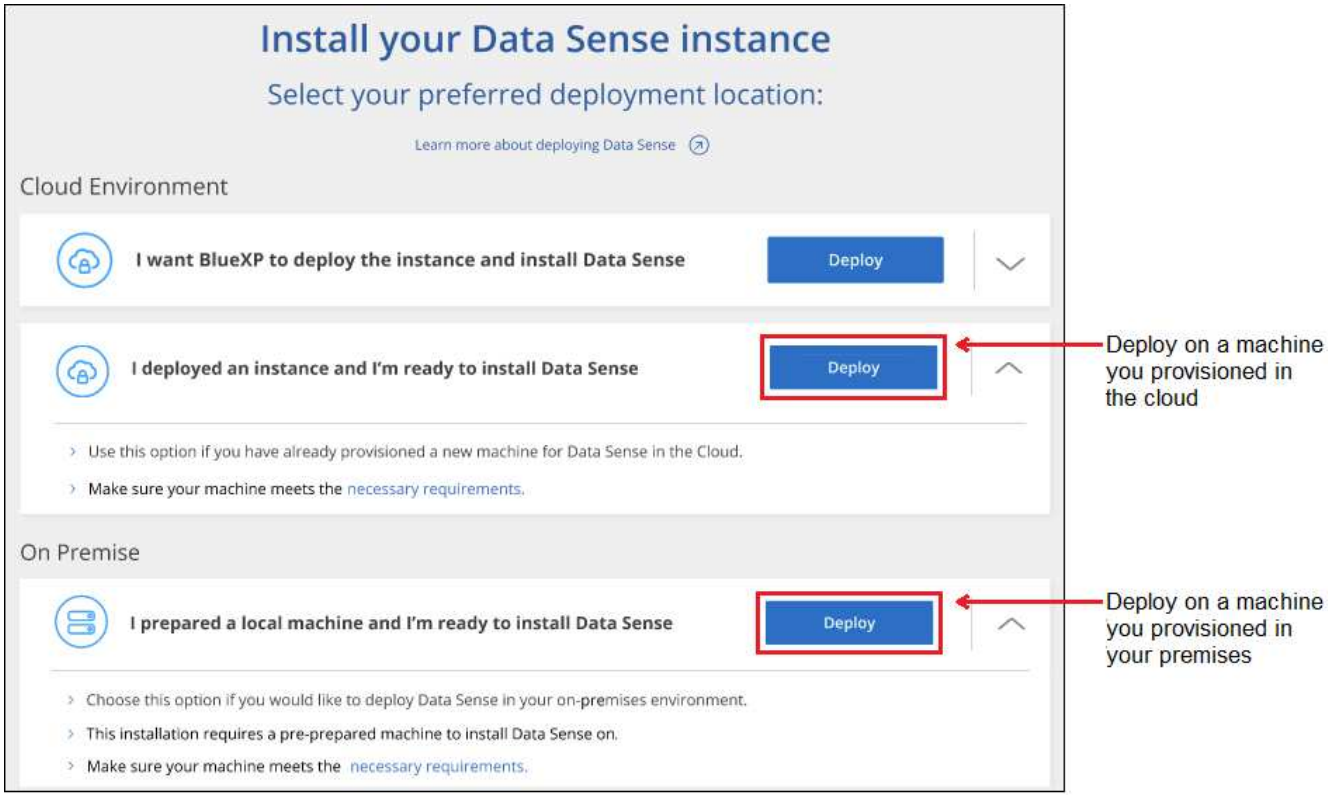
1. からBlueXP分類ソフトウェアをダウンロードします "ネットアップサポートサイト"。選択するファイルの名前は* DATASENSE-installer -<version> .tar.gz *です。
2. 使用する Linux ホストにインストーラファイルをコピーします (`cp またはその他の方法を使用) 。
3. ホストマシンでインストーラファイルを解凍します。次に例を示します。

```
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。

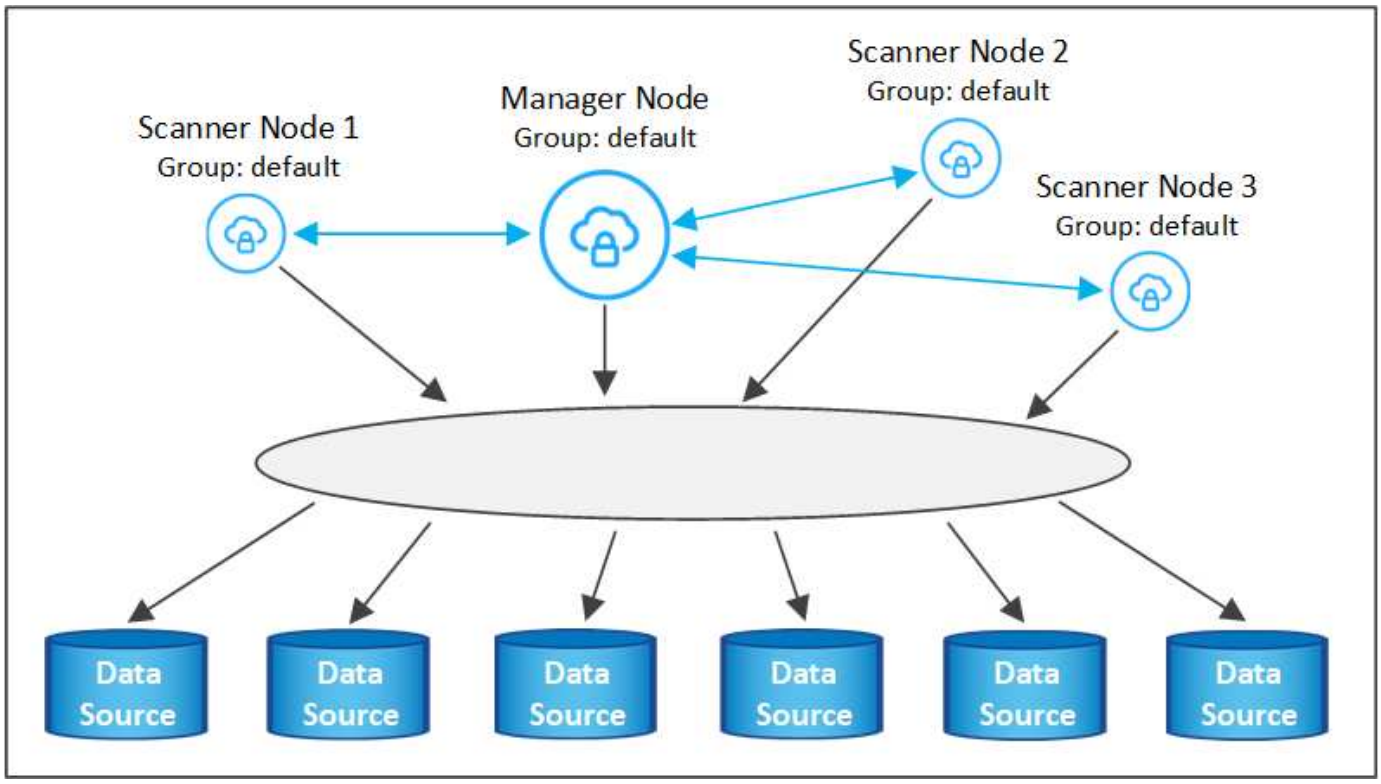
既存の環境にスキャナノードを追加する

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。

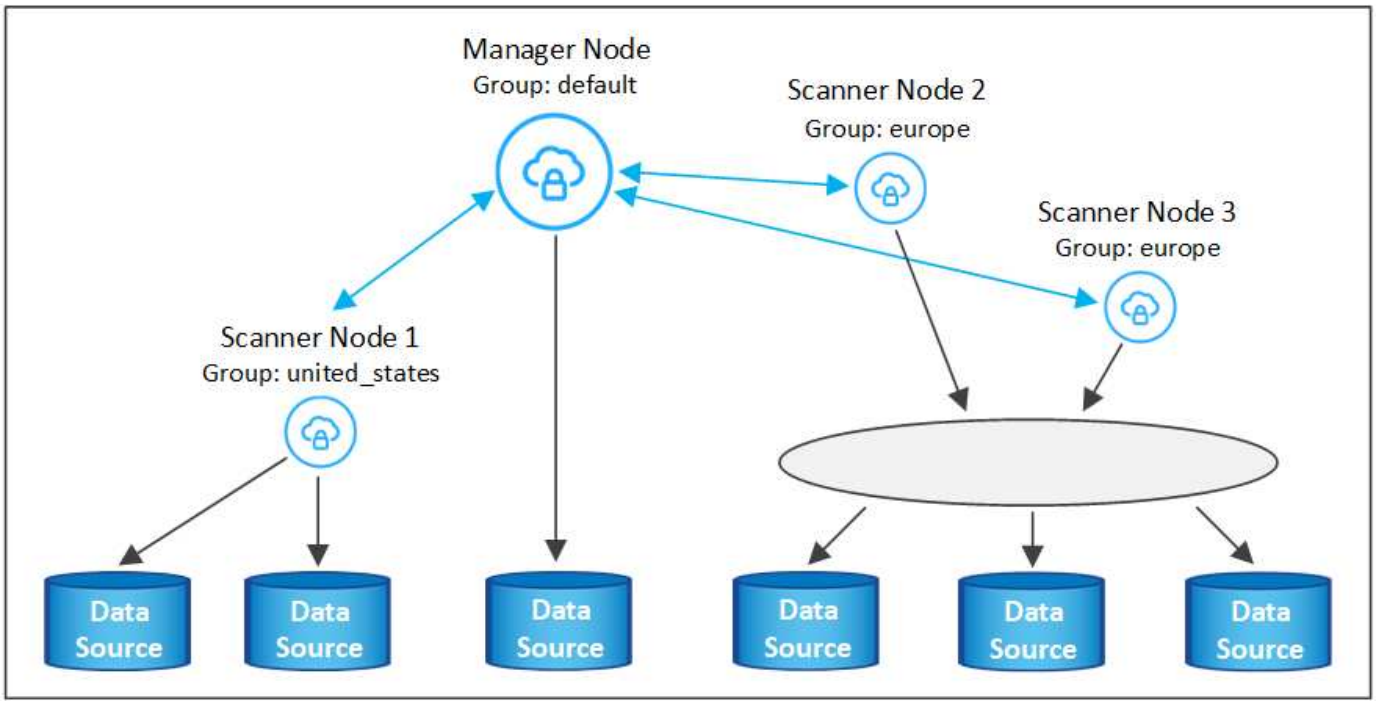
- すべてのデータソースのスキャンに使用するノードを追加します
- 特定のデータソース、または特定のデータソースグループ（通常は場所に基づく）のスキャンに役立つノードを追加する

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。

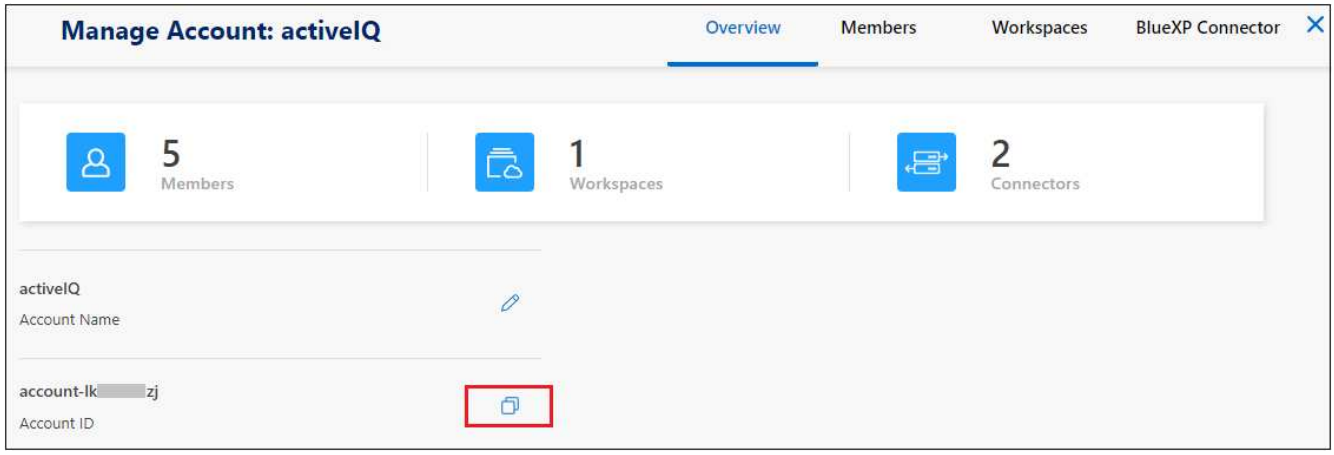
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp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

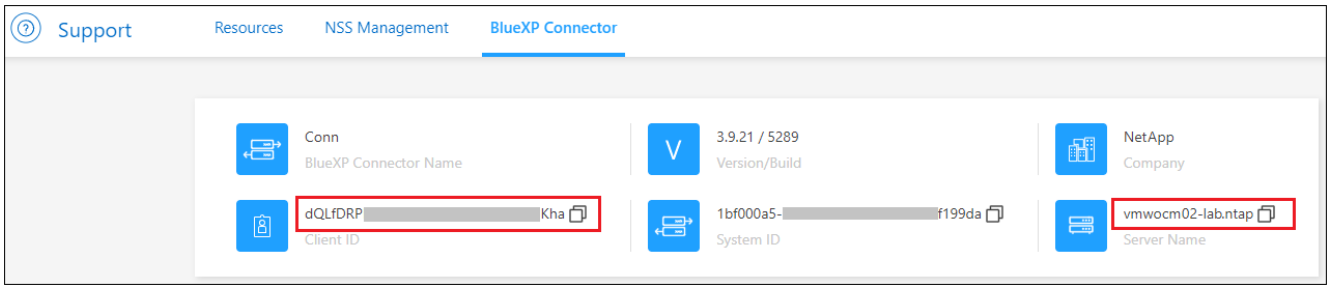
事前に必要な手順

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。

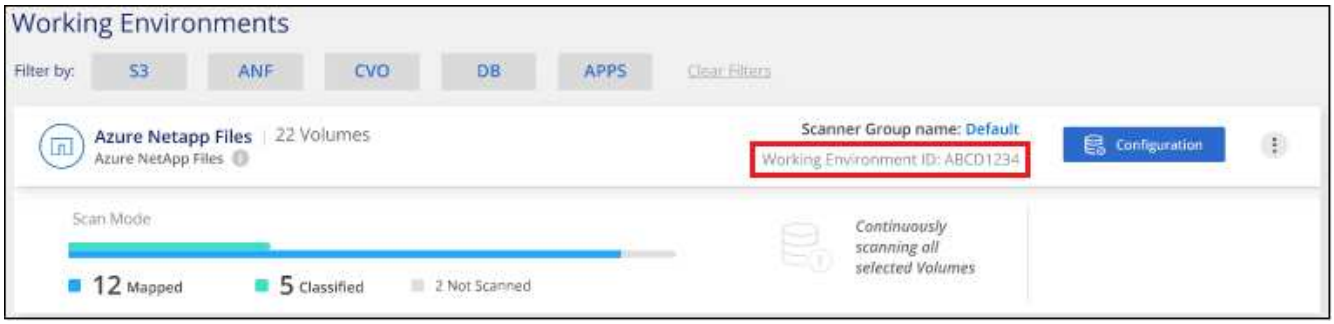
1. BlueXPのメニューバーで、*アカウント>アカウントの管理*をクリックします。



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。

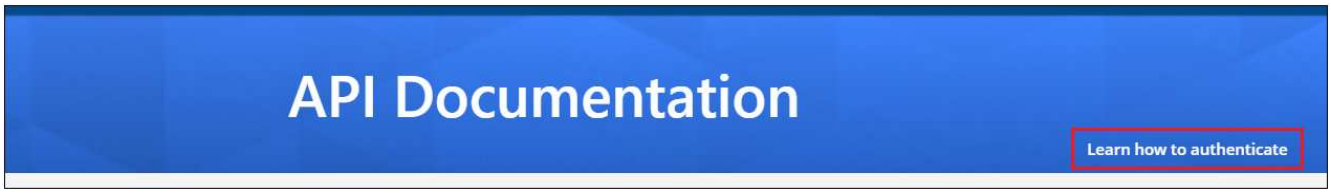


4. Connector_Client ID_と_サーバ名_をコピーします。
5. スキャナグループを使用する場合は、BlueXP分類の[設定]タブで、スキャナグループに追加する各作業環境の作業環境IDをコピーします。



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`

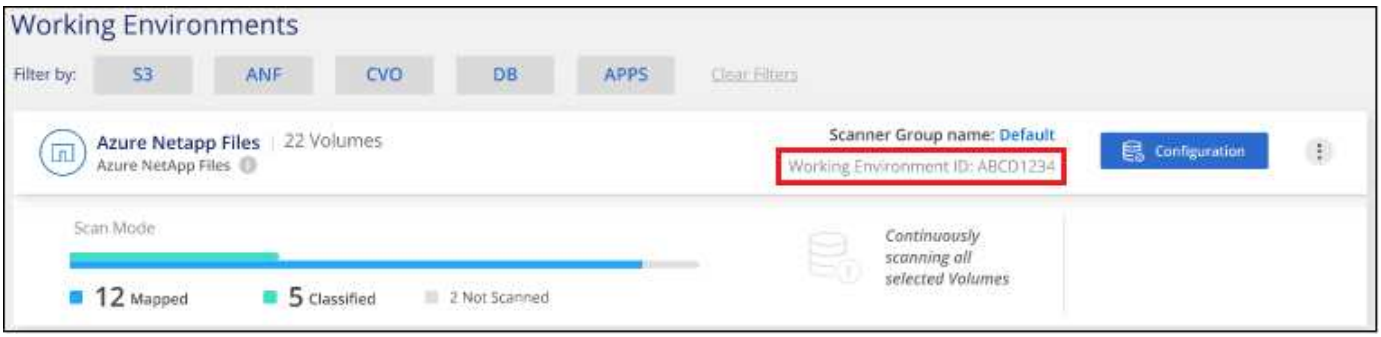
結果

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

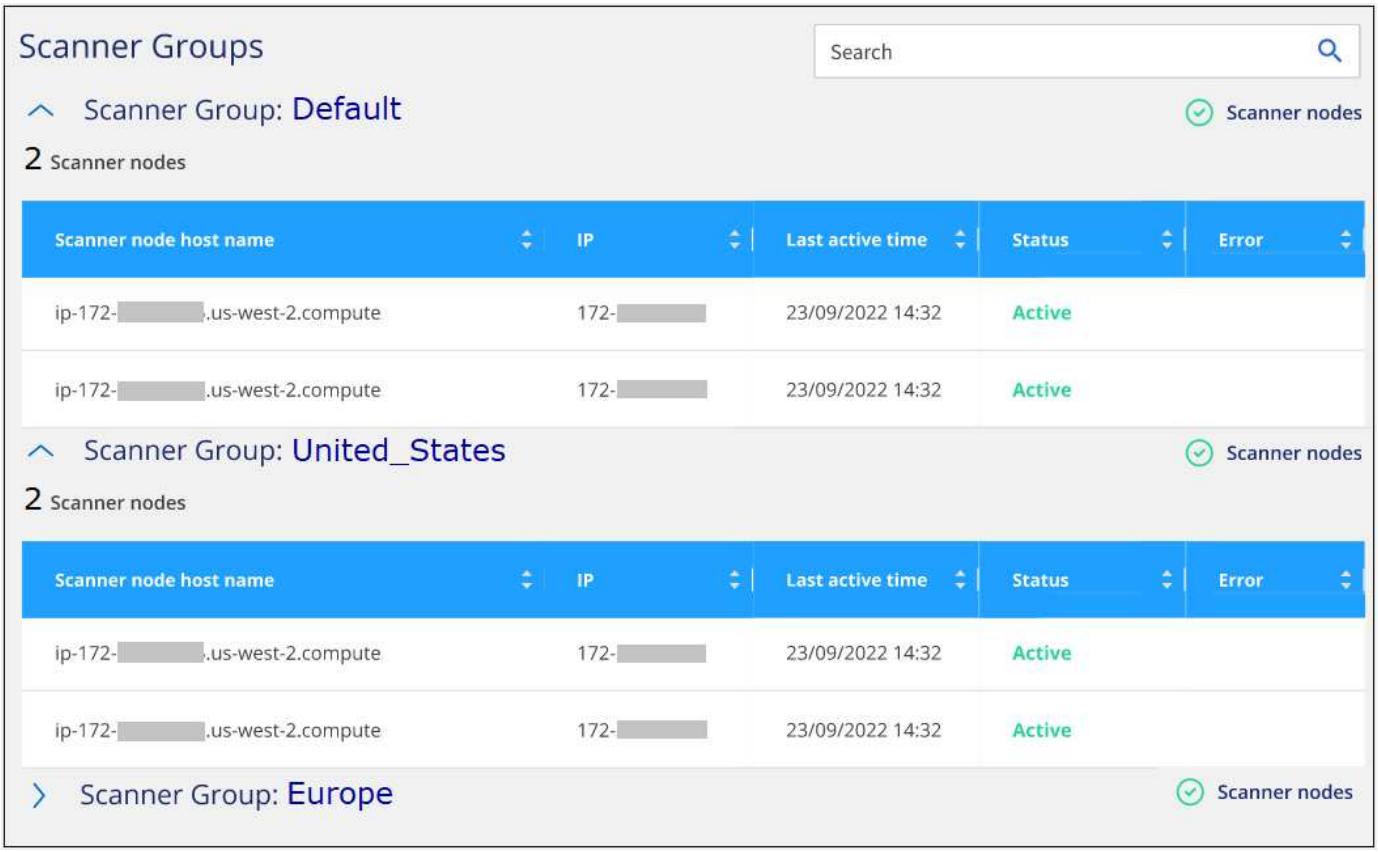
設定ページで、スキャンするデータソースを選択できます（まだ選択していない場合）。スキャナグループを作成した場合は、各データソースがそれぞれのグループのスキャナノードによってスキャンされます。

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。

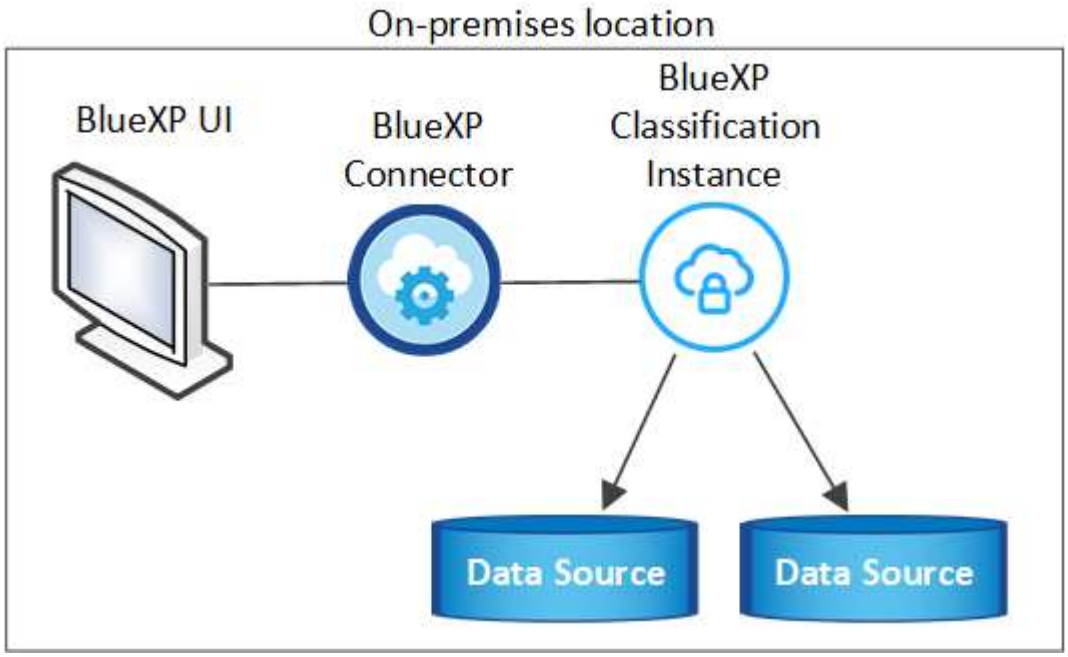
接続タイプ	ポート	説明
Connector <> ONTAP cluster（NAS）	443（TCP）	BlueXPはHTTPSを使用してONTAP クラスタを検出しましたカスタムファイアウォールポリシーを使用する場合は、次の要件を満たす必要があります。 • コネクタホストが、ポート 443 経由のアウトバウンド HTTPS アクセスを許可する必要があります。コネクタがクラウドにある場合、すべてのアウトバウンド通信は事前定義されたセキュリティグループによって許可されます。 • ONTAP クラスタでは、ポート 443 を介した着信 HTTPS アクセスが許可されている必要があります。デフォルトの「 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 ）

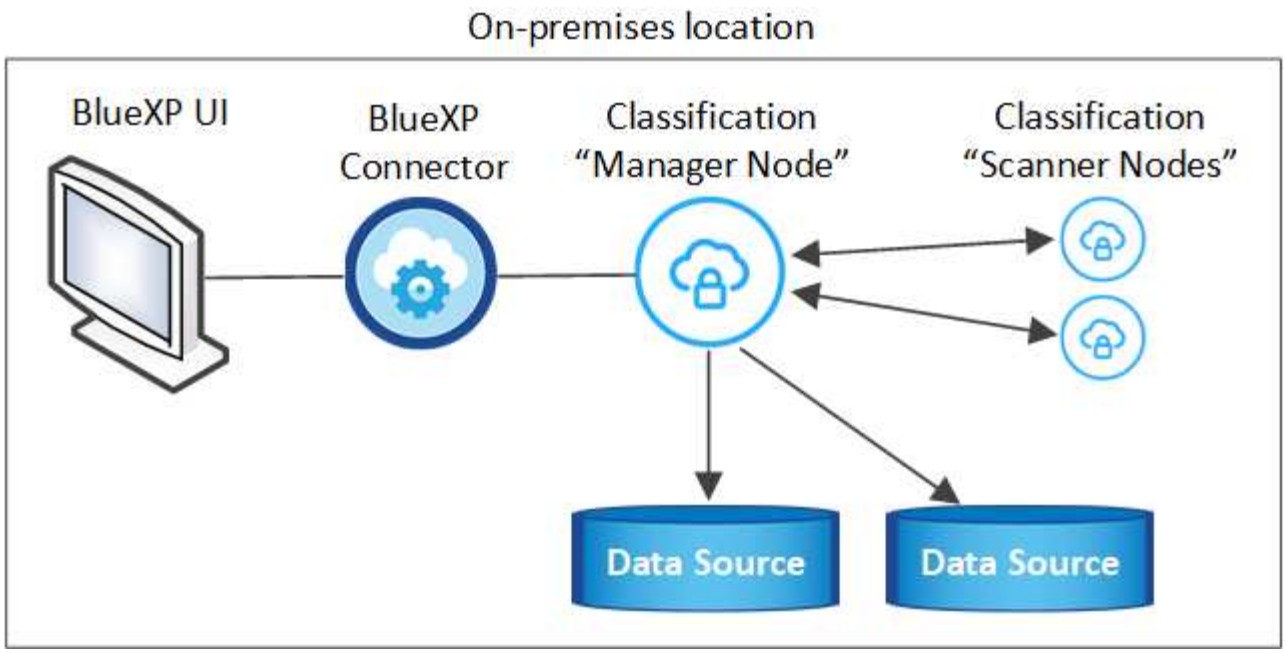
複数のBlueXP分類ホストを使用してデータソースのスキャンに必要な処理能力を提供している場合は、追加のポート/プロトコルを有効にする必要があります。 "追加のポート要件を参照してください"。

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。

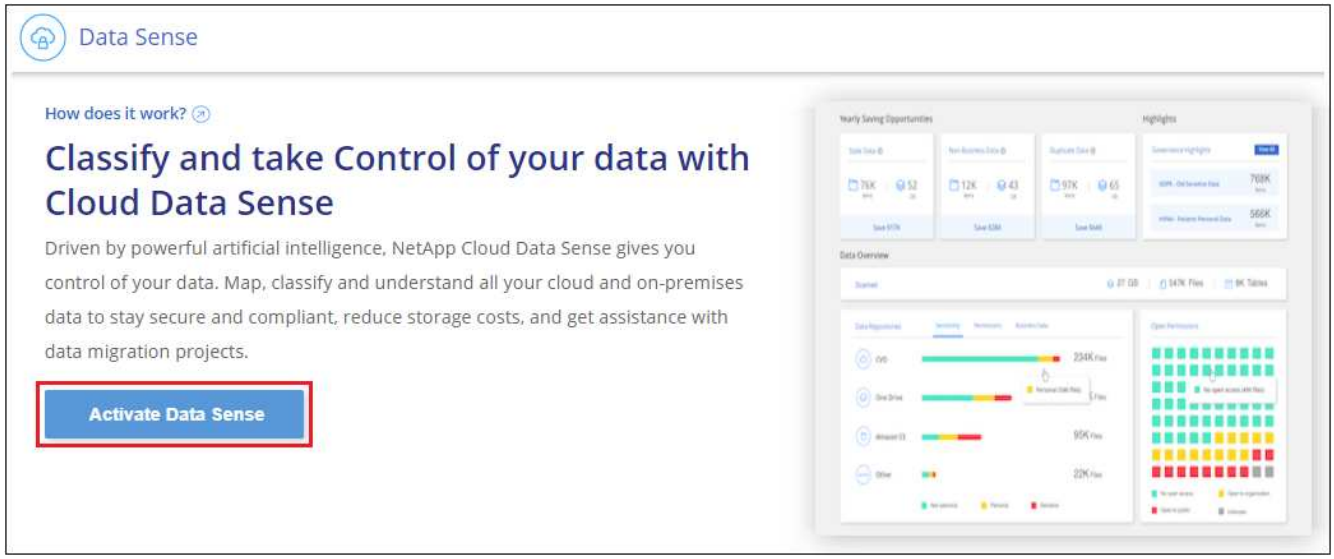
```
tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
```

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。

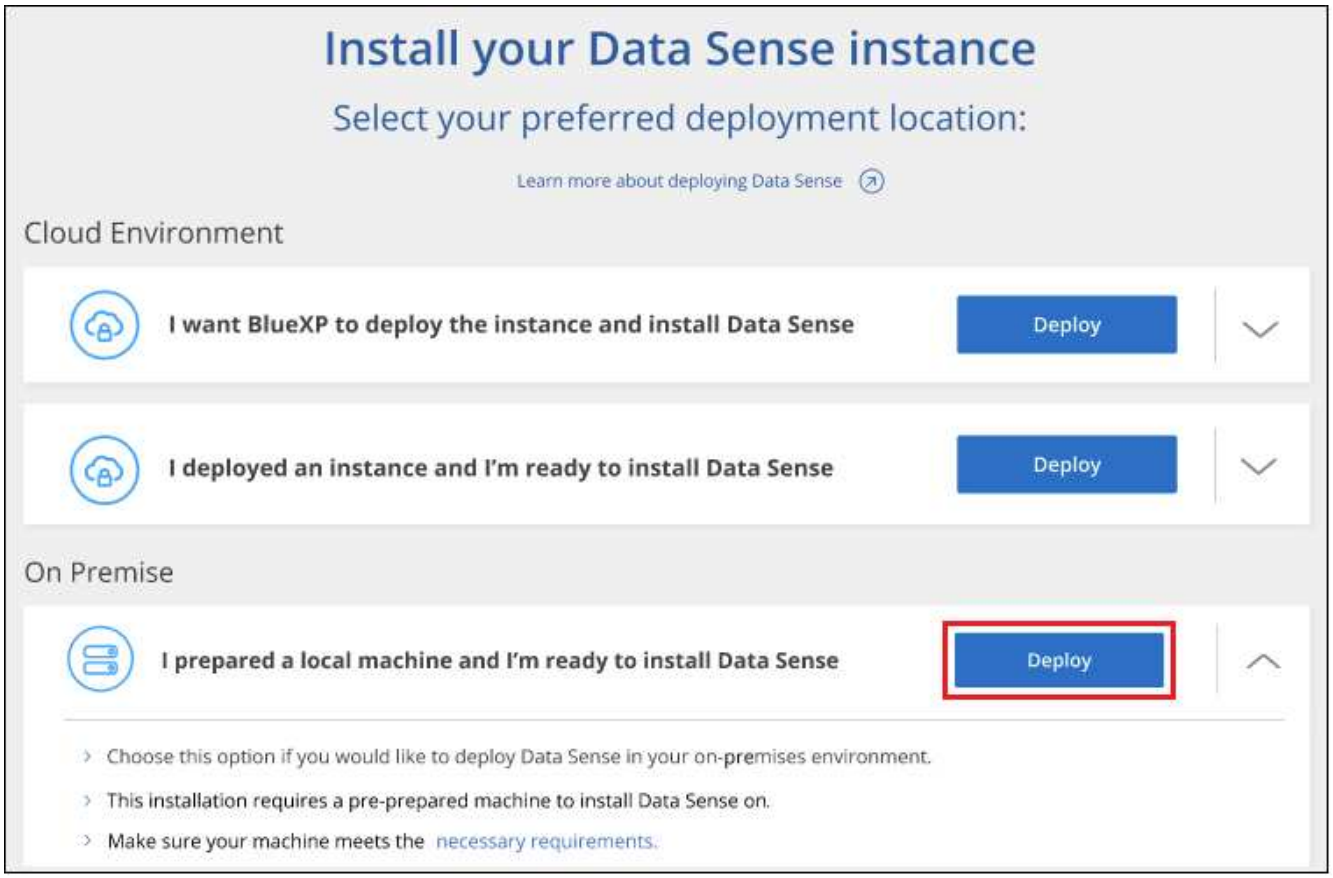
4. ホストマシンでインストールファイルを解凍します。次に例を示します。

```
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"。

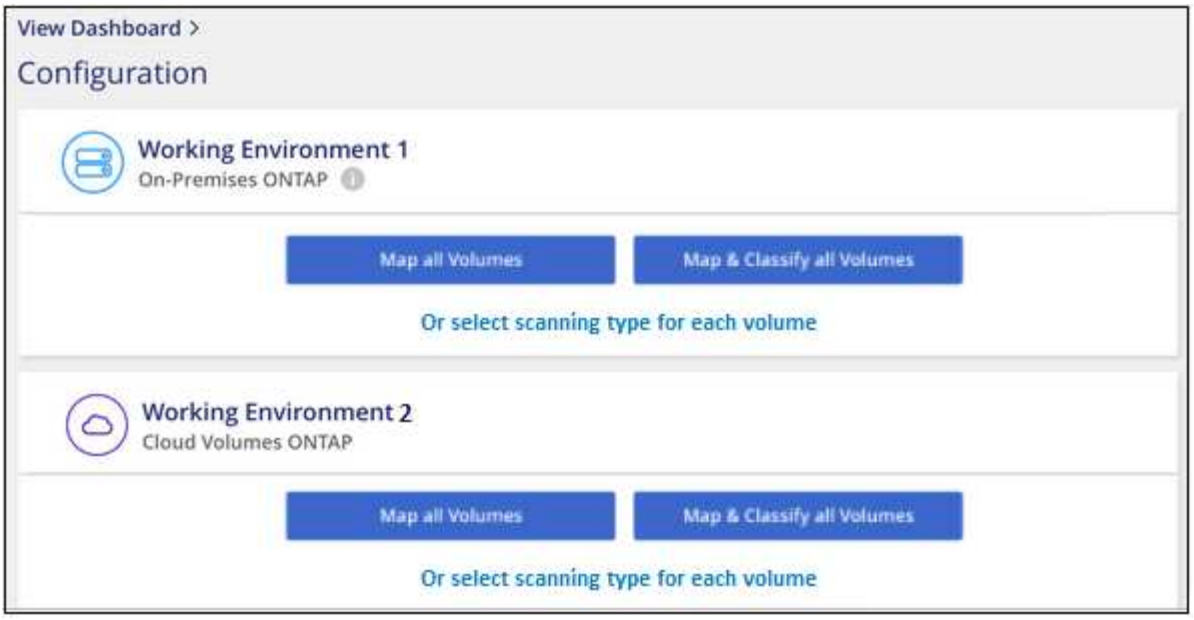
インターネットにアクセスできないダークサイトにインストールされているオンプレミスの ONTAP システムをスキャンする場合は、を実行する必要があります "インターネットアクセスのないオンプレミスと同じ場所にBlueXPの分類を導入します"。また、BlueXPコネクタがオンプレミスの同じ場所に配置されている必要があります。

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。

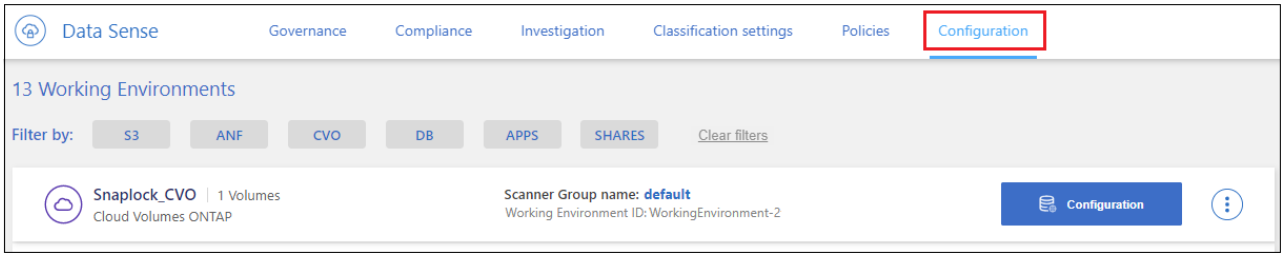
手順

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。

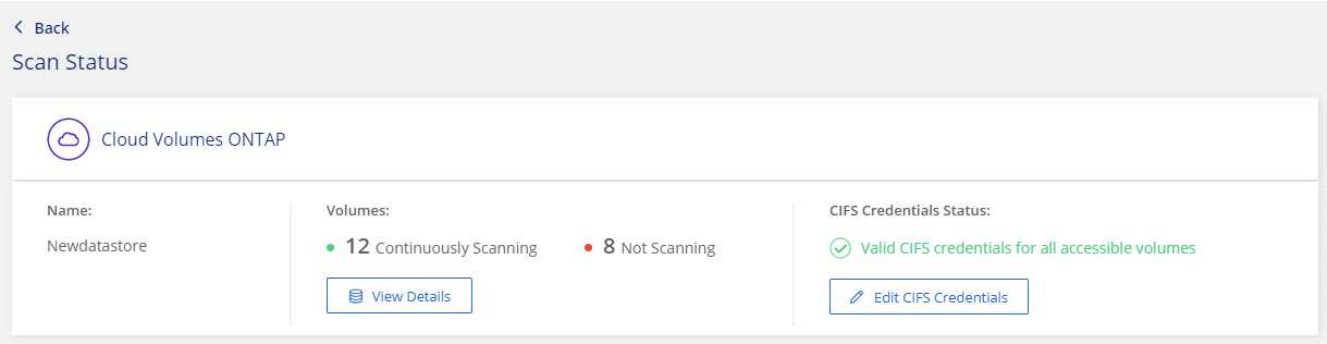
   ボタンを示す [遵守] タブのスクリーンショット。"]

   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。

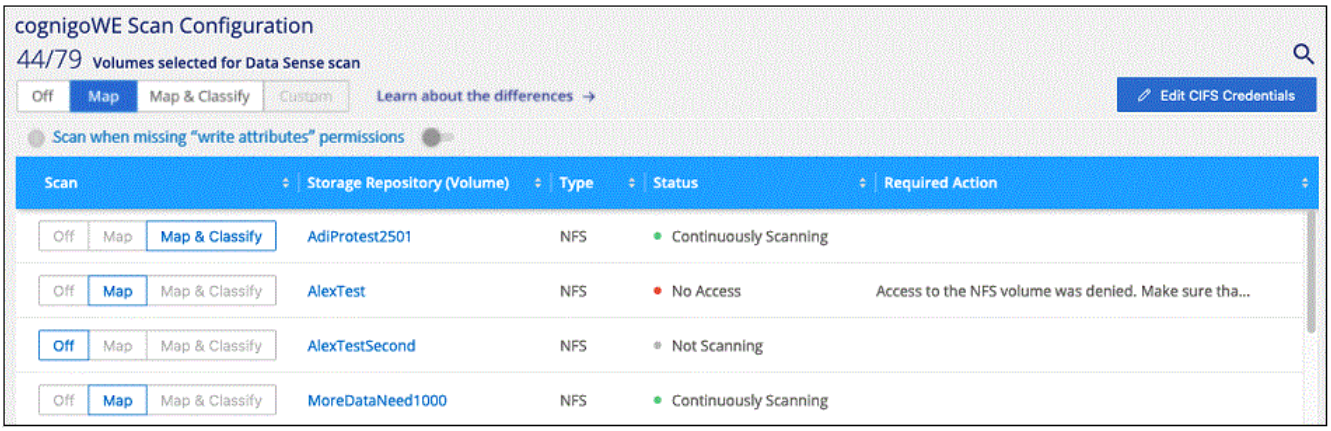
   BlueXPの分類スキャンでファイルの「最終アクセス日時」が変更されないようにするには、CIFSではWrite Attributes権限、NFSではwrite権限を持つことを推奨します。可能であれば、すべてのファイルに対する権限を持つ組織内の親グループにActive Directory構成ユーザーを含めることをお勧めします。

   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。

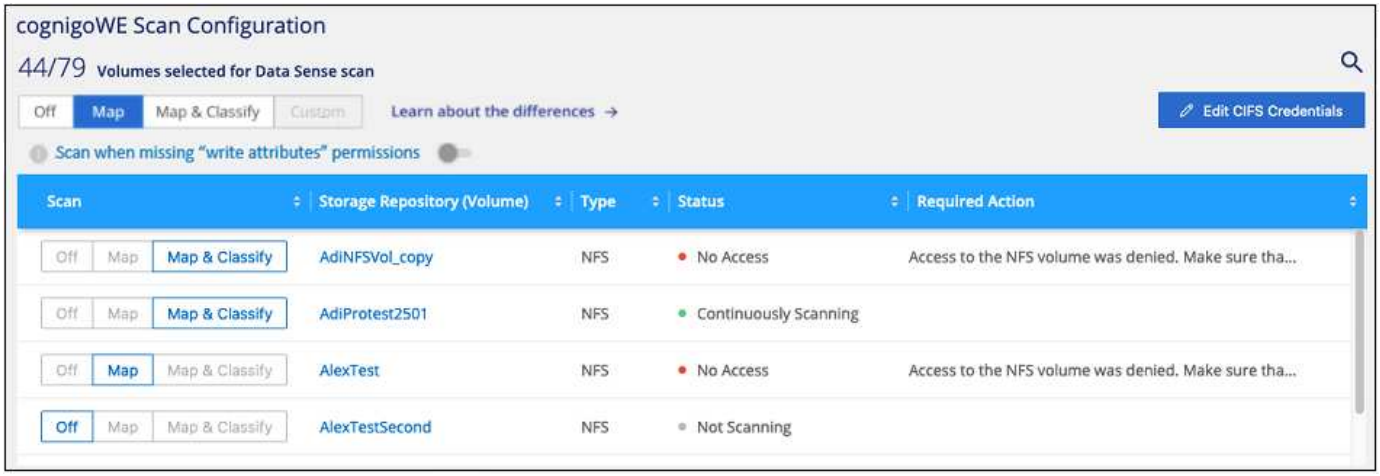


   ページのスクリーンショット。4つのボリュームが表示されています。そのうちの1つはBlueXPで分類されたボリュームとボリュームの間のネットワーク接続が原因でスキャンされていません。"]

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。"。



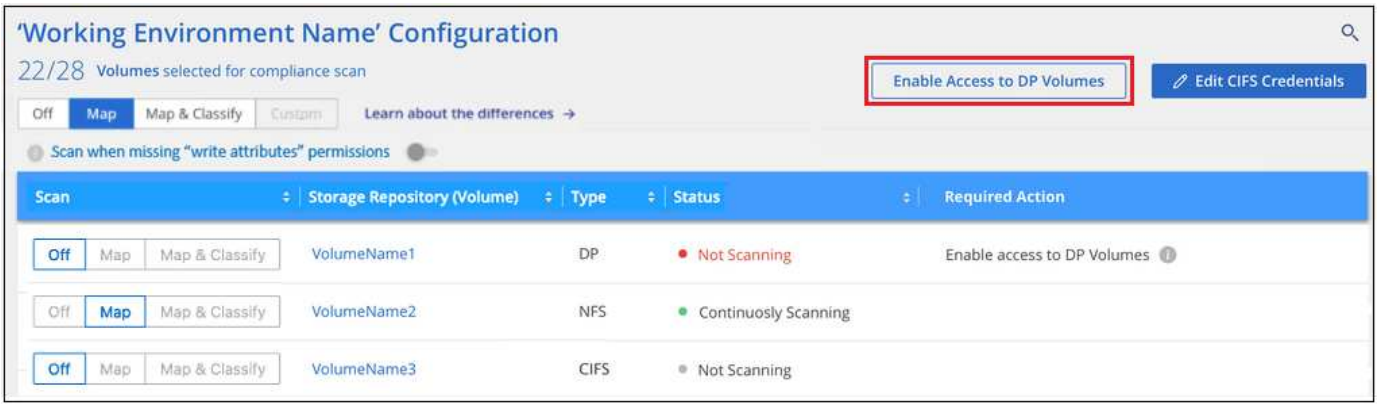
終了：	手順：
ボリュームに対してマッピングのみのスキャンを有効にします	ボリューム領域で、 * マップ * をクリックします
ボリュームでフルスキャンを有効にします	ボリューム領域で、 * マップと分類 * をクリックします
ボリュームのスキャンを無効にします	ボリューム領域で、 * オフ * をクリックします
すべてのボリュームでマッピングのみのスキャンを有効にします	見出し領域で、 * マップ * をクリックします
すべてのボリュームでフルスキャンを有効にします	見出し領域で、 * マップと分類 * をクリックします
すべてのボリュームでスキャンを無効にします	見出し領域で、 * Off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

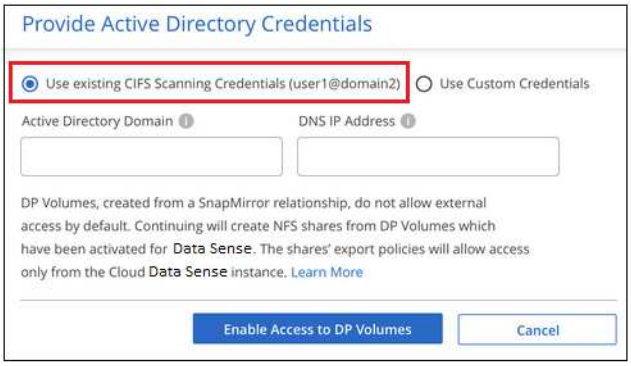
最初は、ボリュームリストでこれらのボリュームを *Type* * DP * でスキャンしていないステータス * および必要なアクション _ * DP ボリュームへのアクセスを有効にします * 。

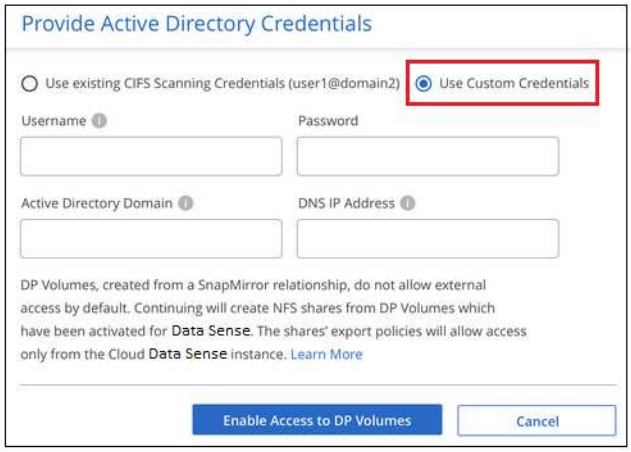


手順

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。

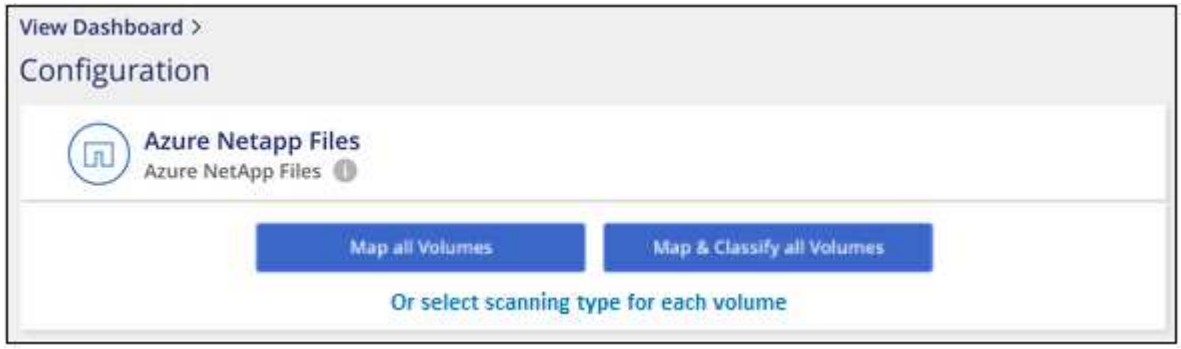
*注：*現時点では、Azure NetApp Files ボリュームのスキャン時にBlueXPの分類をオンプレミスに導入することはできません。

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。

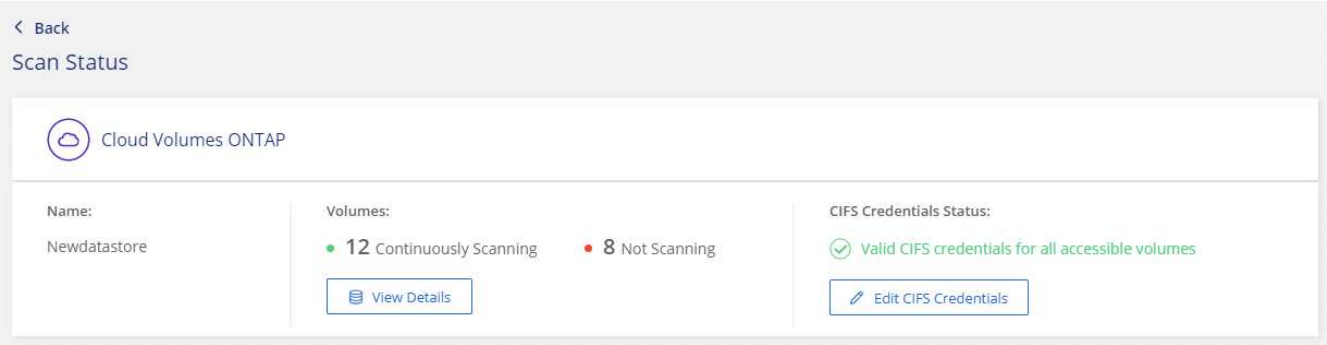
ボタンを示す [遵守] タブのスクリーンショット。"]

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。

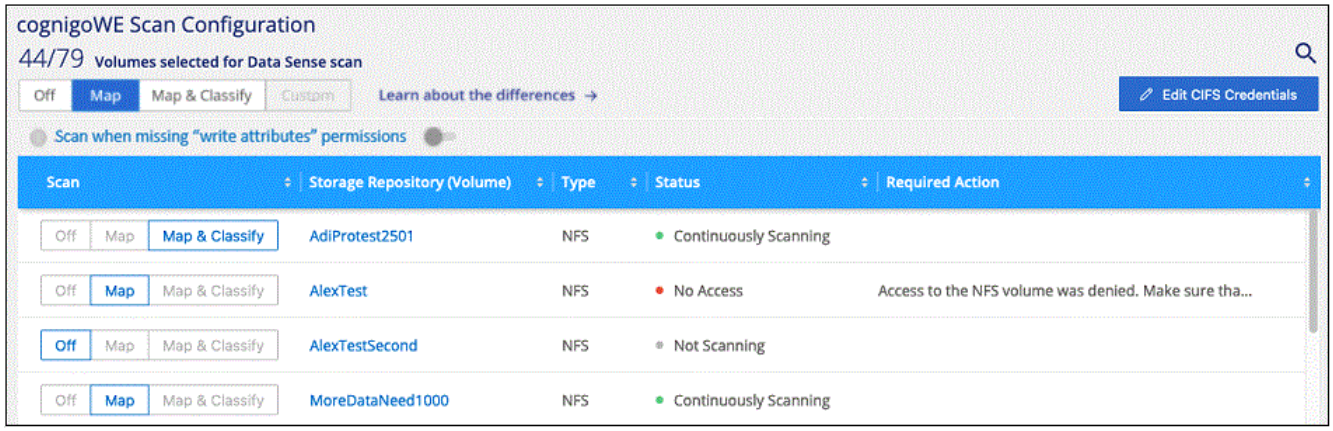
BlueXPの分類スキャンでファイルの「最終アクセス日時」が変更されないようにするには、CIFSではWrite Attributes権限、NFSではwrite権限を持つことを推奨します。可能であれば、すべてのファイルに対する権限を持つ組織内の親グループにActive Directory構成ユーザーを含めることをお勧めします。

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。

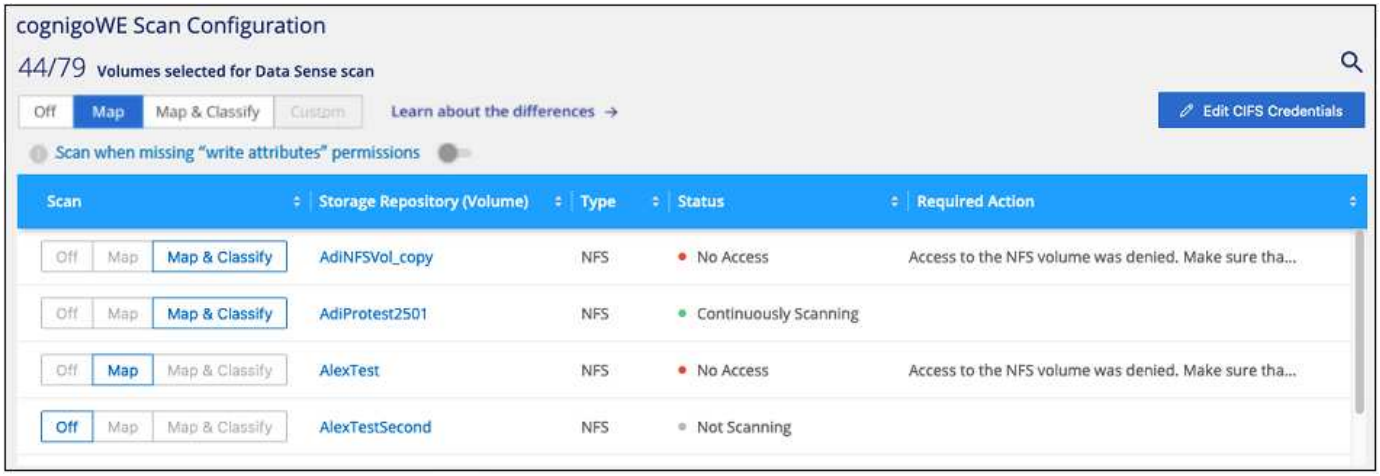


ページのスクリーンショット。4つのボリュームが表示されています。そのうちの1つはBlueXPで分類されたボリュームとボリュームの間のネットワーク接続が原因でスキャンされていません。"]

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。

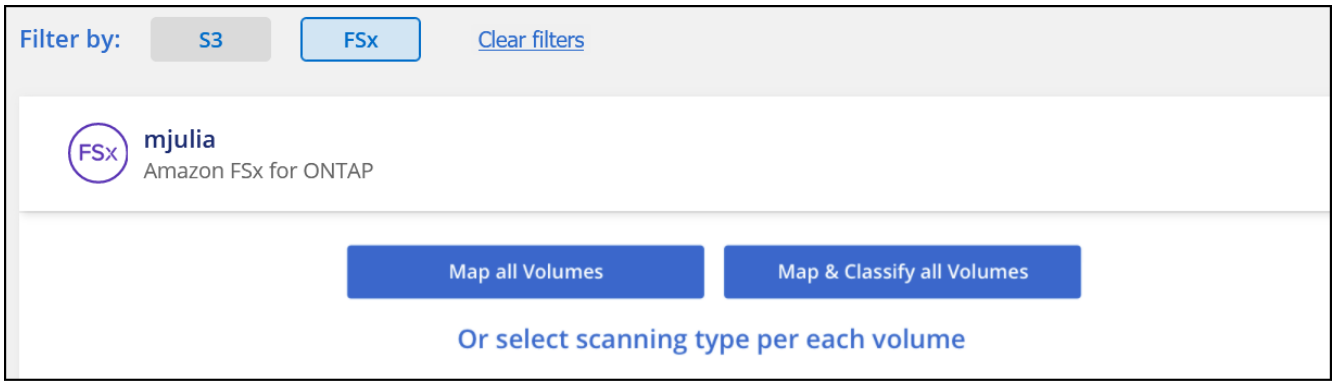
注： FSxボリュームのスキャン時にオンプレミス環境へのBlueXP分類の導入は現在サポートされていません。

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

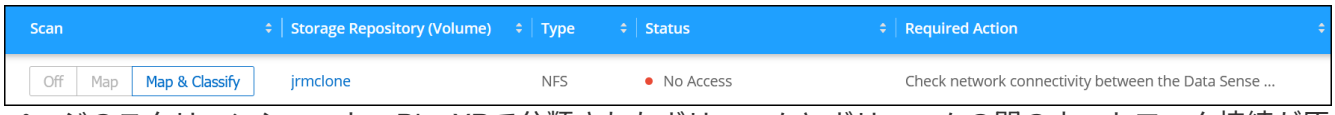
ネットワーク、セキュリティグループ、およびエクスポートポリシーをチェックして、BlueXPの分類でボリュームへのアクセスが許可されていることを確認します。

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。



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。

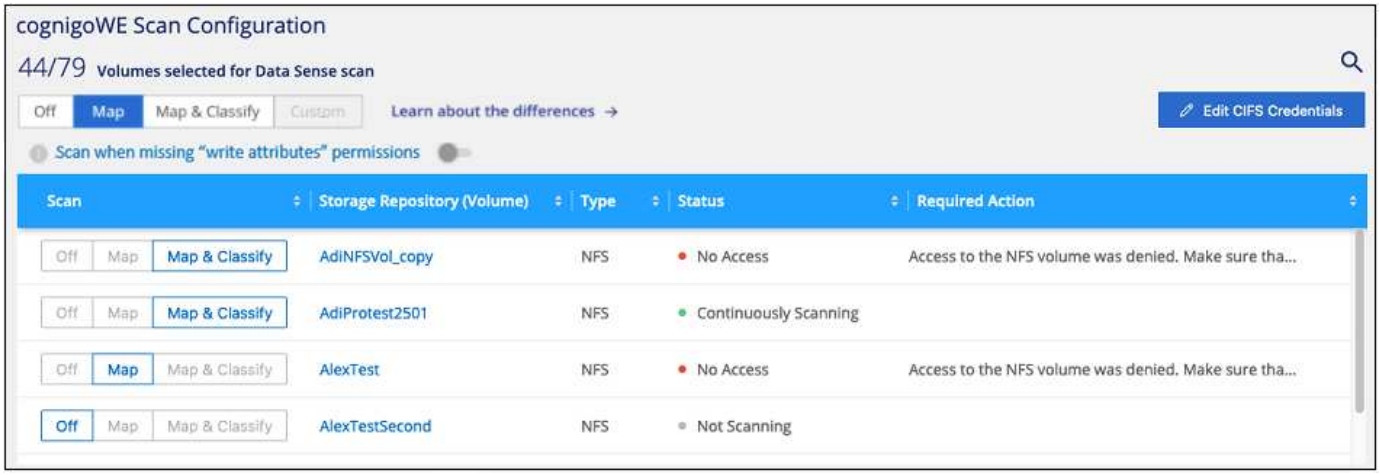
   クレデンシャルを入力すると、すべての CIFS ボリュームが認証されたことを示すメッセージが表示されます。

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。"。



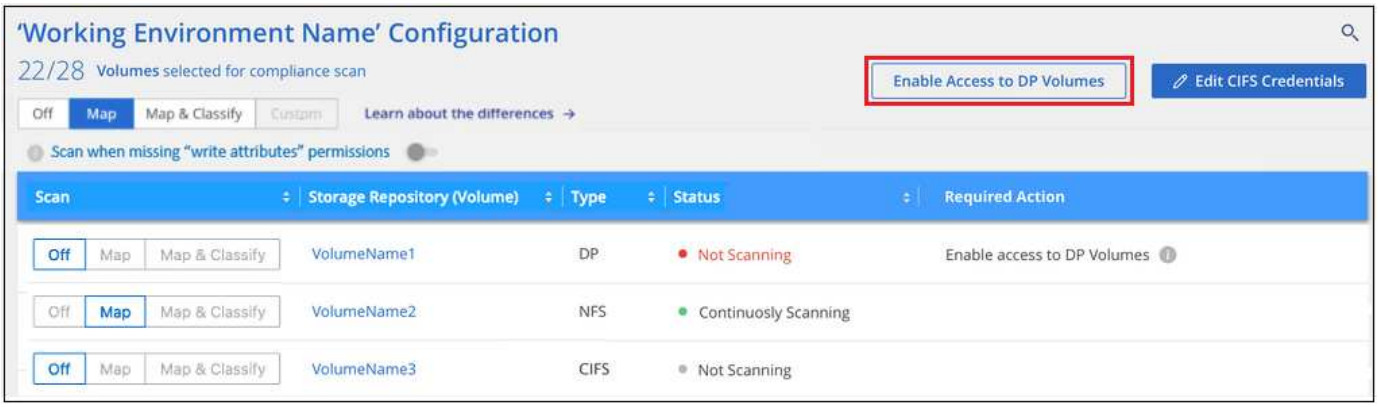
終了：	手順：
ボリュームに対してマッピングのみのスキャンを有効にします	ボリューム領域で、 * マップ * をクリックします
ボリュームでフルスキャンを有効にします	ボリューム領域で、 * マップと分類 * をクリックします
ボリュームのスキャンを無効にします	ボリューム領域で、 * オフ * をクリックします
すべてのボリュームでマッピングのみのスキャンを有効にします	見出し領域で、 * マップ * をクリックします
すべてのボリュームでフルスキャンを有効にします	見出し領域で、 * マップと分類 * をクリックします
すべてのボリュームでスキャンを無効にします	見出し領域で、 * Off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

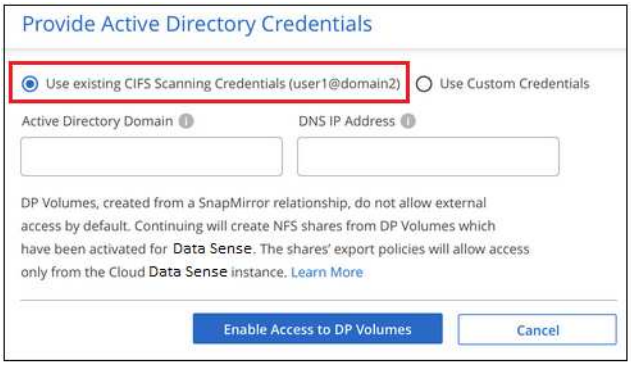
最初は、ボリュームリストでこれらのボリュームを *Type* * DP * でスキャンしていないステータス * および必要なアクション _ * DP ボリュームへのアクセスを有効にします * 。

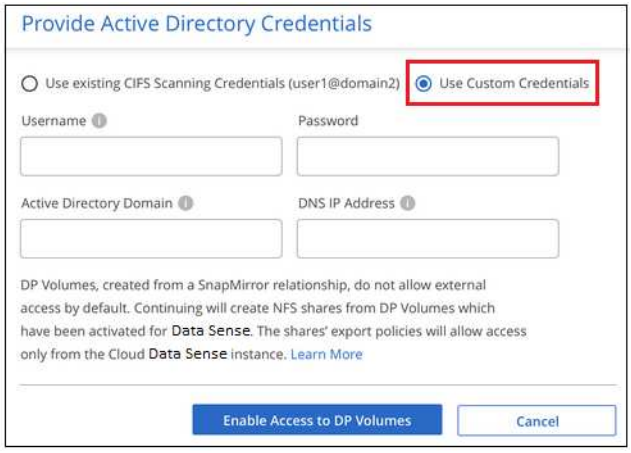


手順

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。

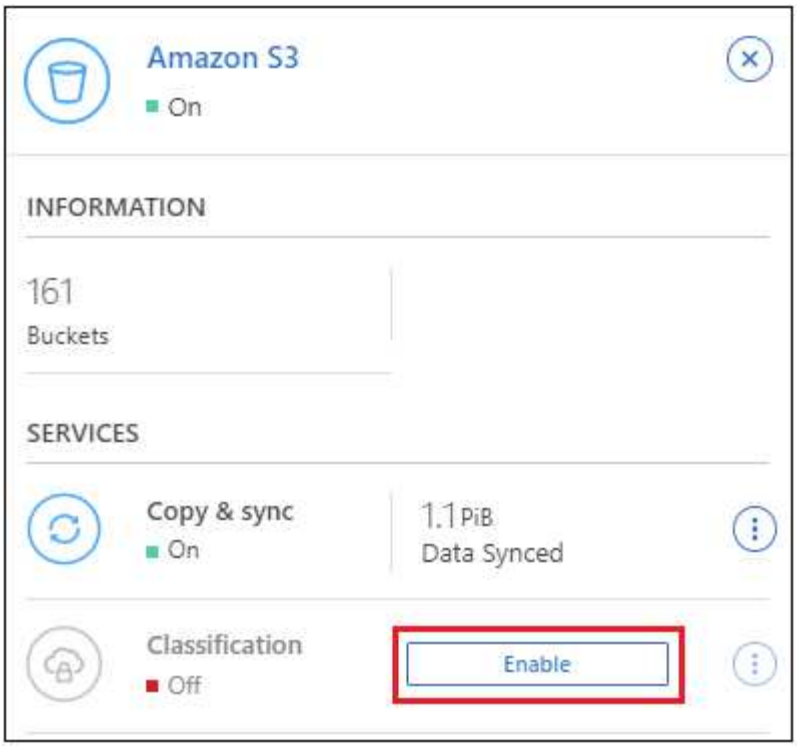
S3作業環境で**BlueXP**分類をアクティブ化します

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

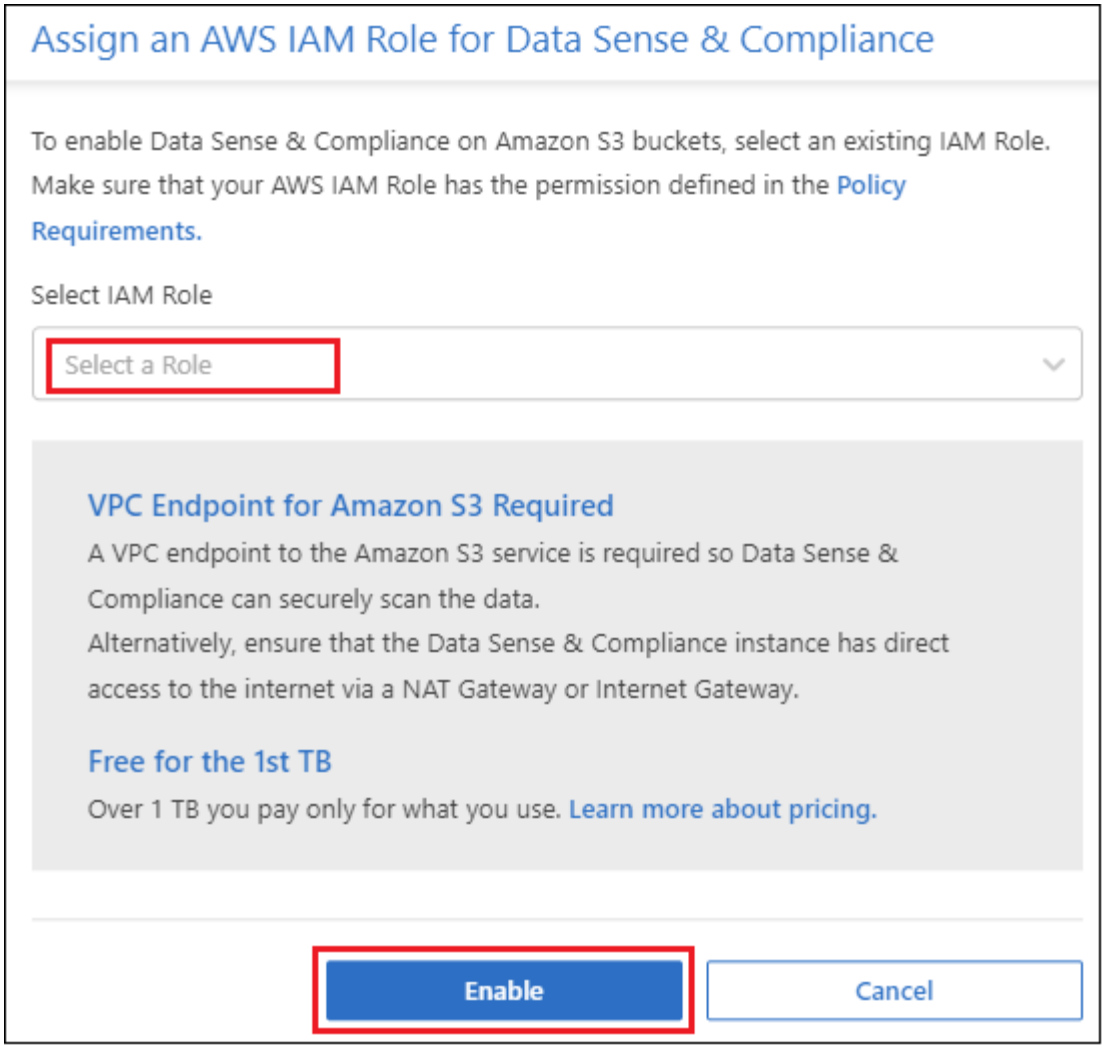
1. BlueXPの左ナビゲーションメニューから、*Storage > Canvas *をクリックします。
2. Amazon S3 作業環境を選択します。

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

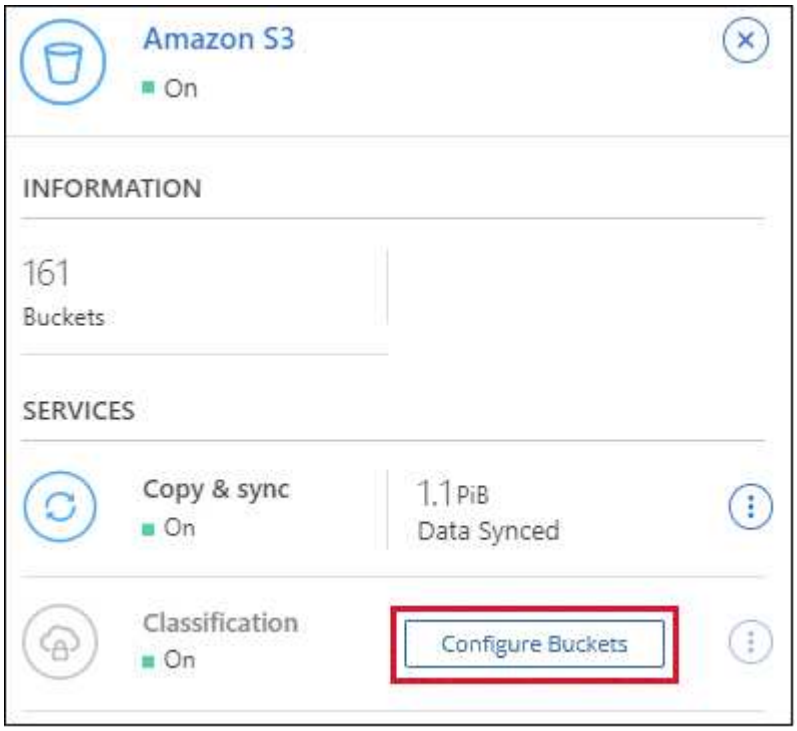
Amazon S3でBlueXPの分類を有効にしたら、次にスキャンするバケットを設定します。

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。

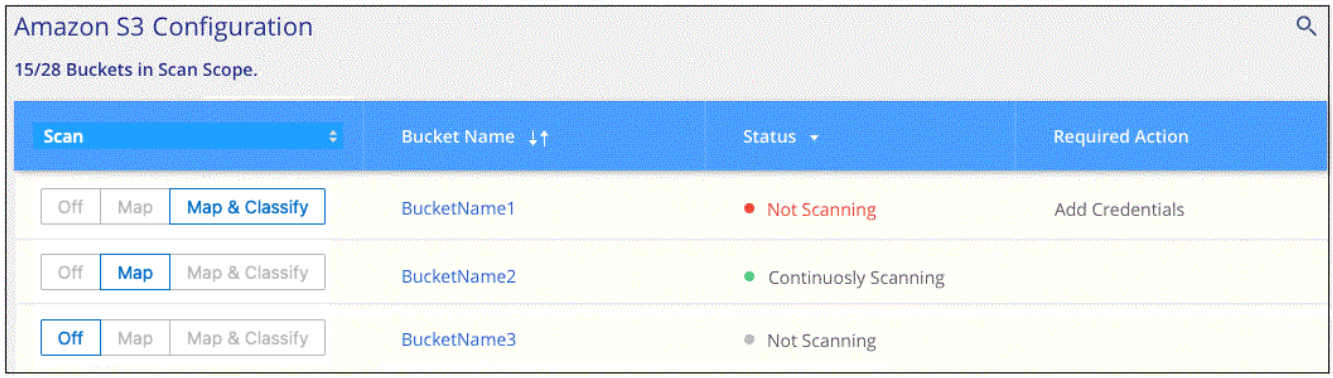
BlueXPに分類することもできます 別々の AWS アカウントにある S3 バケットをスキャンします。

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

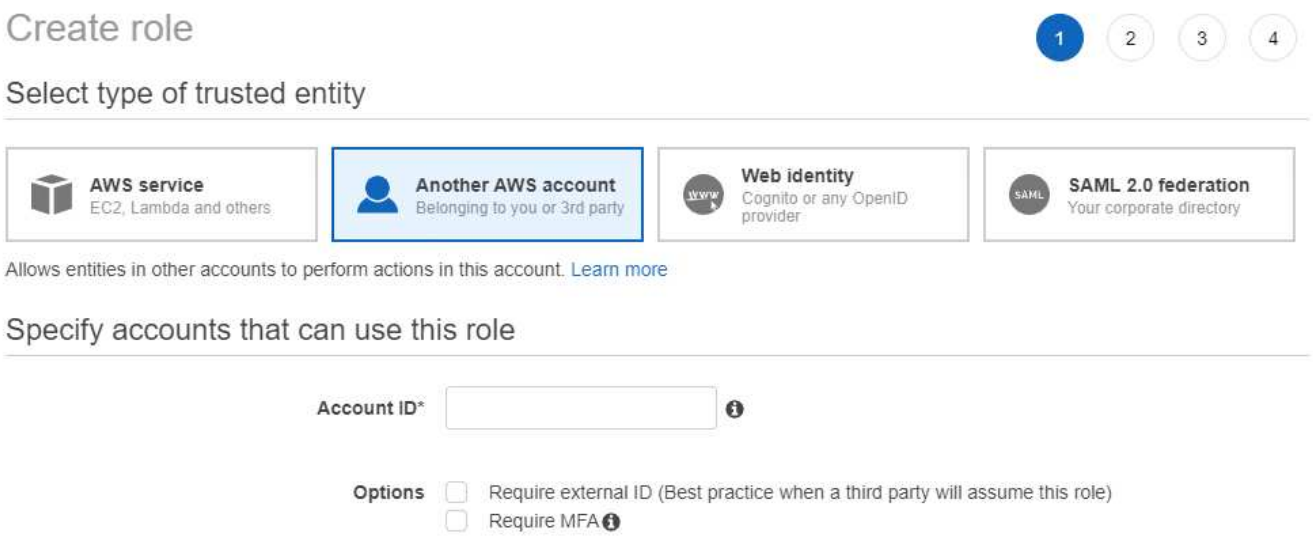
BlueXPの分類で、有効にしたS3バケットのスキャンが開始されます。エラーが発生した場合は、エラーを修正するために必要なアクションとともに、 [ステータス] 列に表示されます。

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

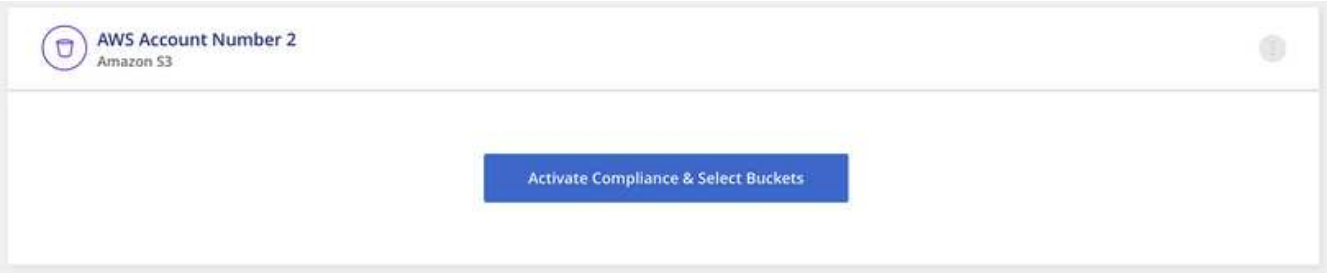
2. BlueXP分類インスタンスが配置されているソースAWSアカウントに移動し、インスタンスに関連付けられているIAMロールを選択します。
   a. 最大 CLI / API セッション期間 * を 1 時間から 12 時間に変更し、変更を保存してください。
   b. [* ポリシーの適用 *] をクリックし、 [ポリシーの作成 *] をクリックします。
   c. 「 STS ： AssumeRole 」アクションを含むポリシーを作成し、ターゲットアカウントで作成したロ

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"。

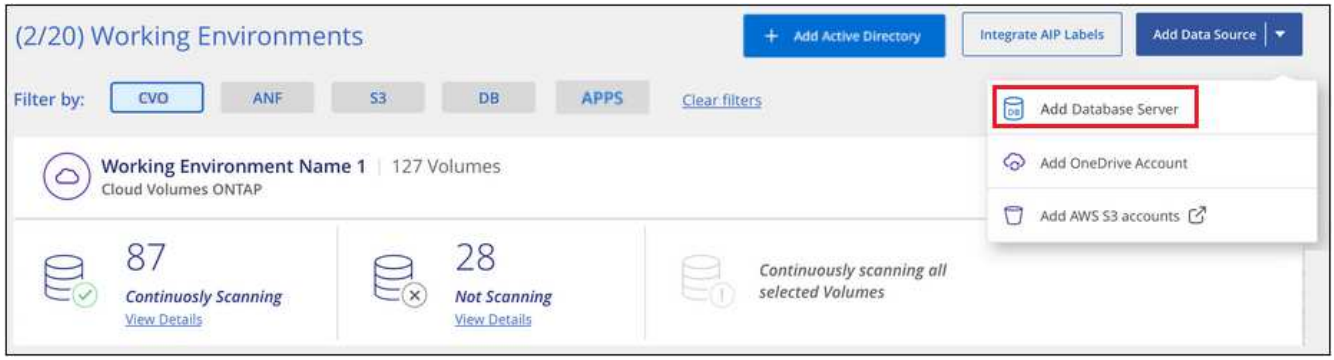
インターネットにアクセスできないダークサイトにインストールされているデータベーススキーマをスキャンする場合は、が必要です "インターネットアクセスのないオンプレミスと同じ場所にBlueXPの分類を導入します"。また、BlueXPコネクタがオンプレミスの同じ場所に配置されている必要があります。

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。

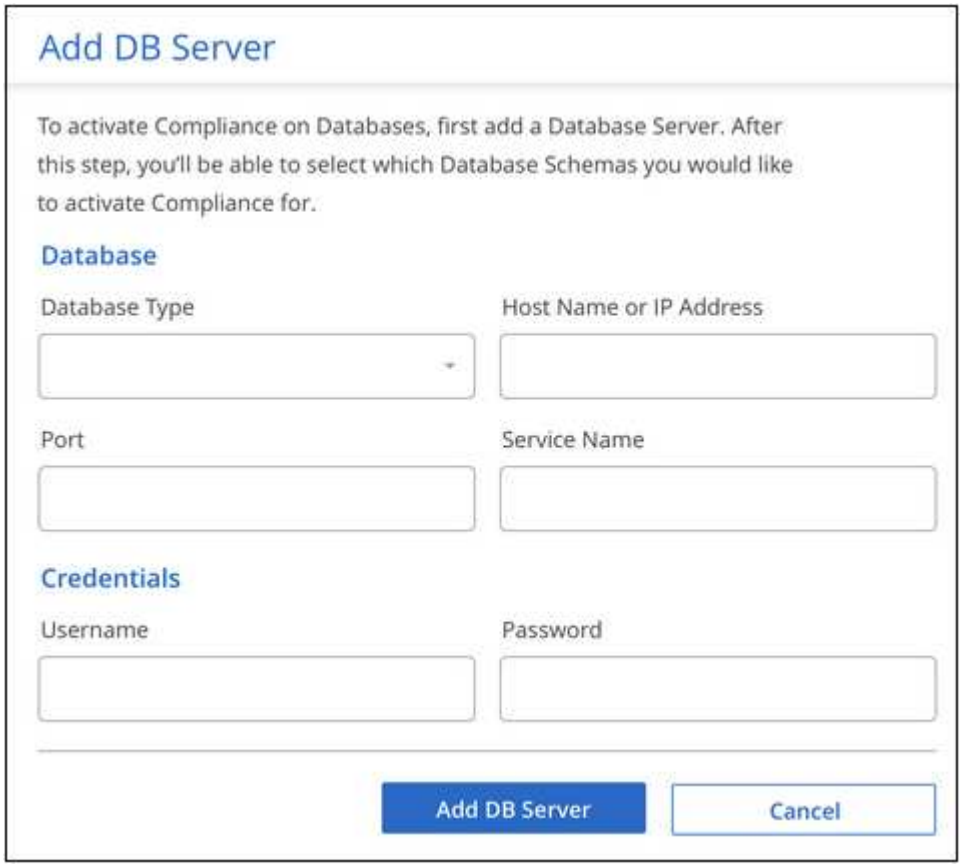
データベースサーバを追加します

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。

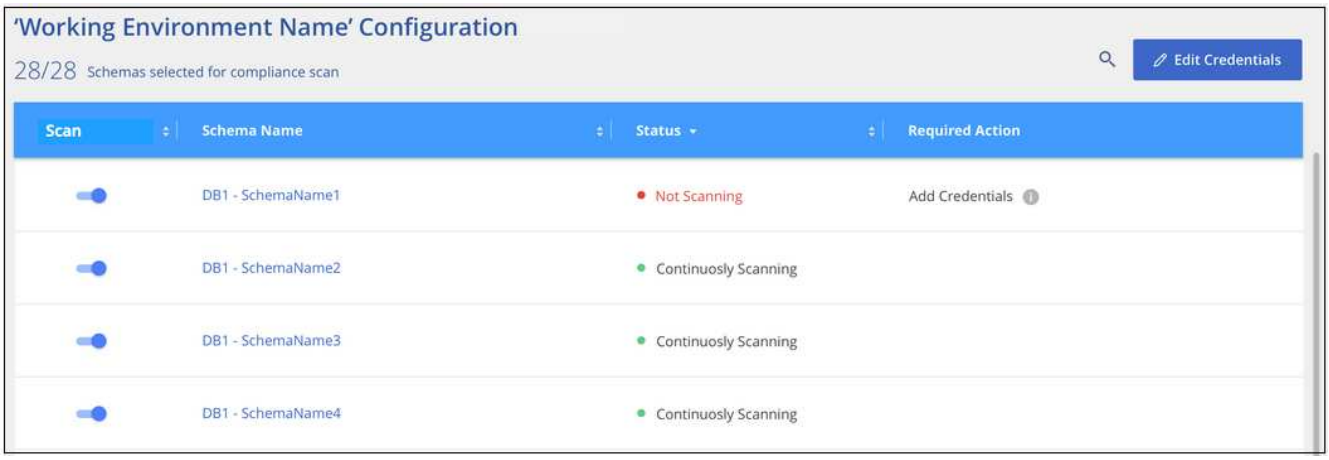
データベーススキーマでのコンプライアンススキャンの有効化と無効化

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"。

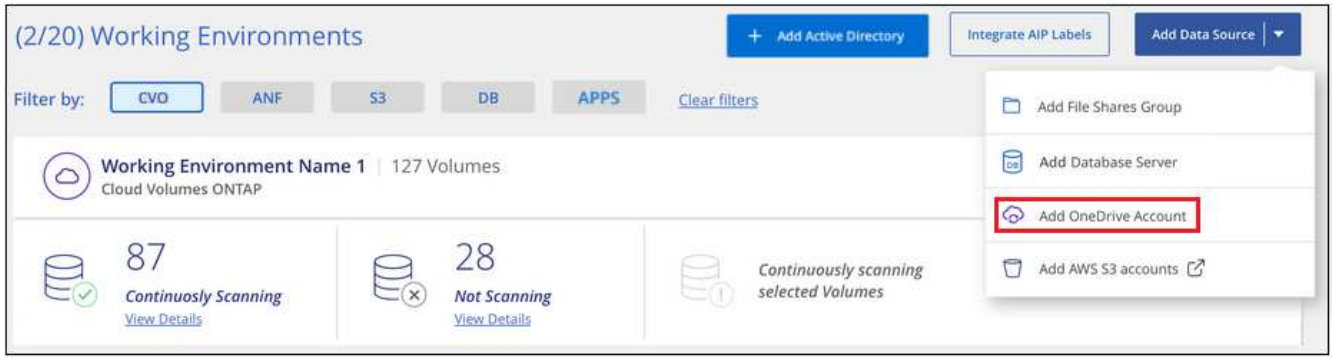
インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

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。

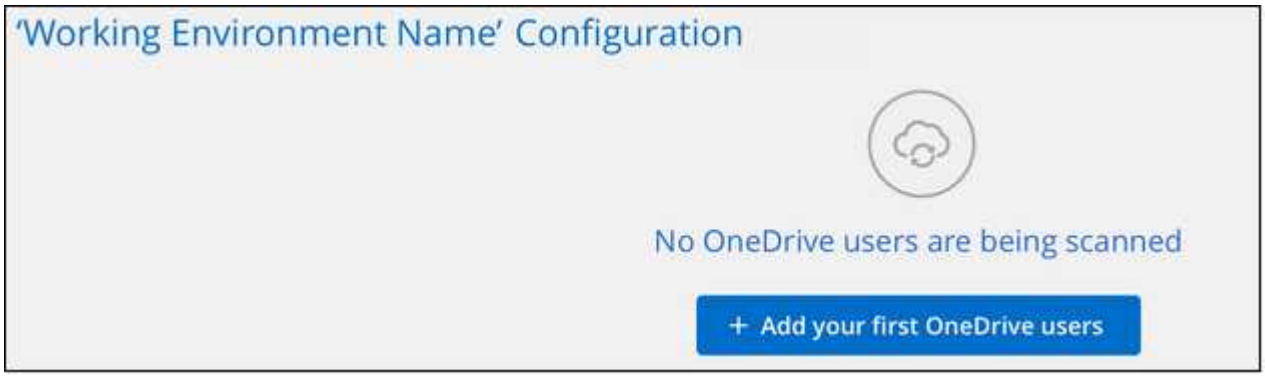
OneDrive ユーザーをコンプライアンススキャンに追加する

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。

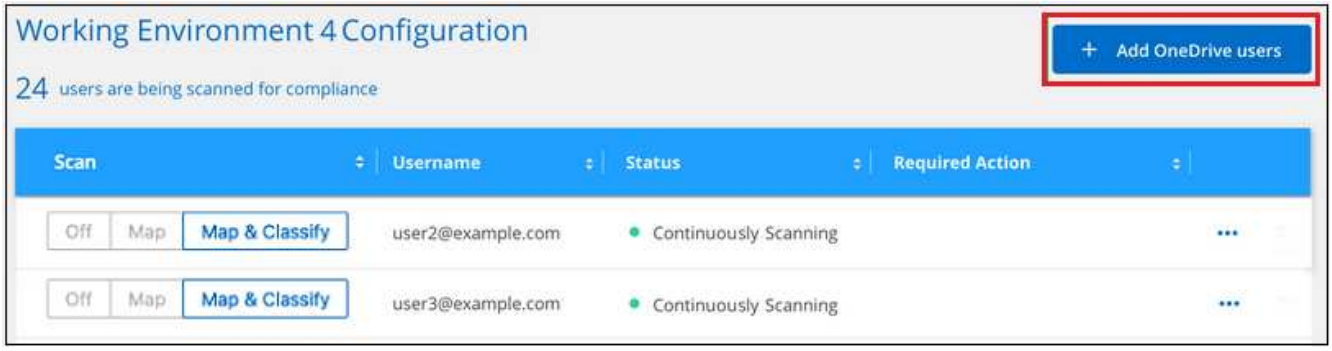
手順

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。

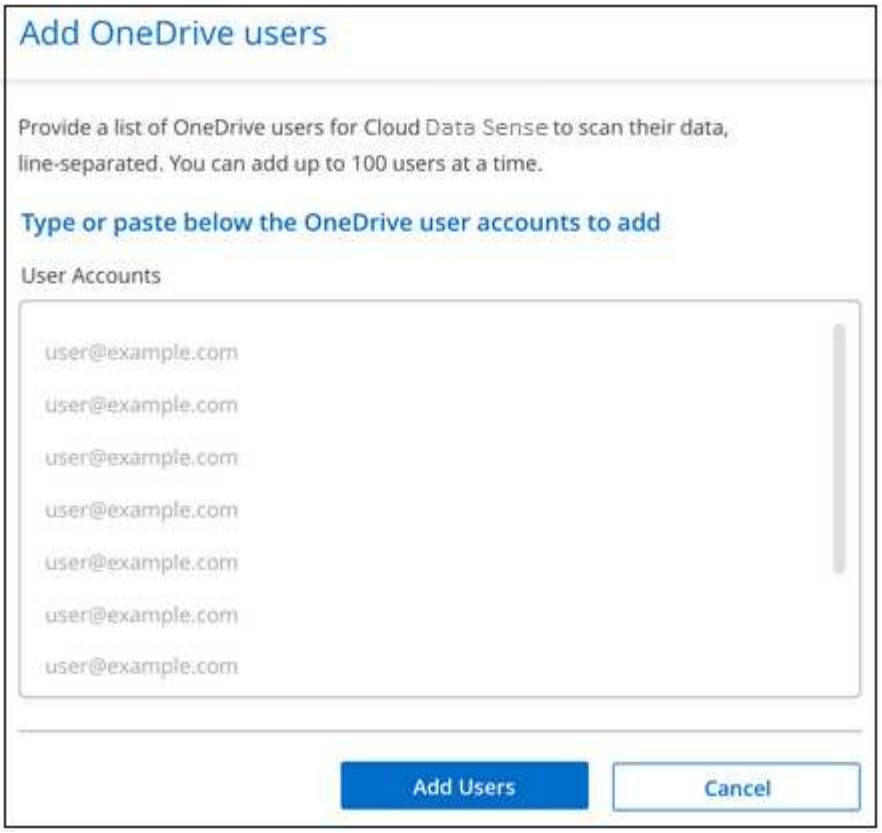


OneDrive アカウントからユーザーを追加する場合は、 [* OneDrive ユーザーの追加 *] をクリックします。



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

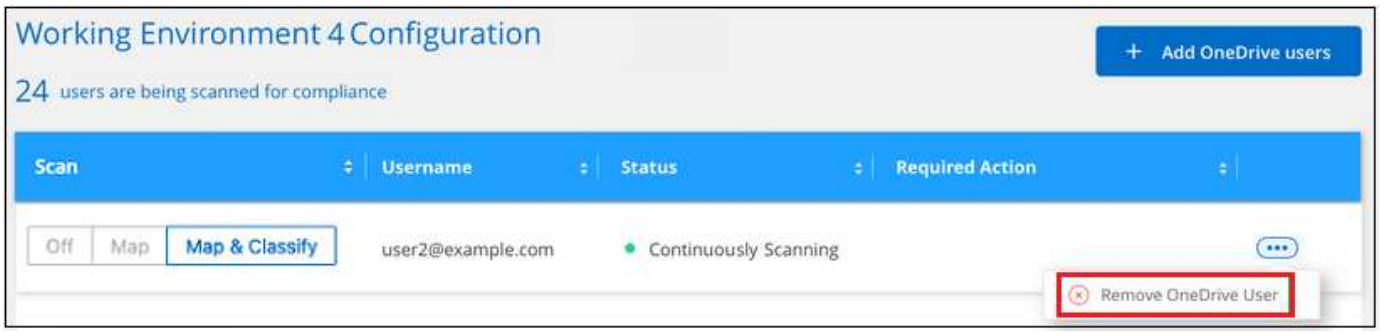
終了：	手順：
ユーザファイルのスキャンを無効にします	[* Off *] をクリックします

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。"。

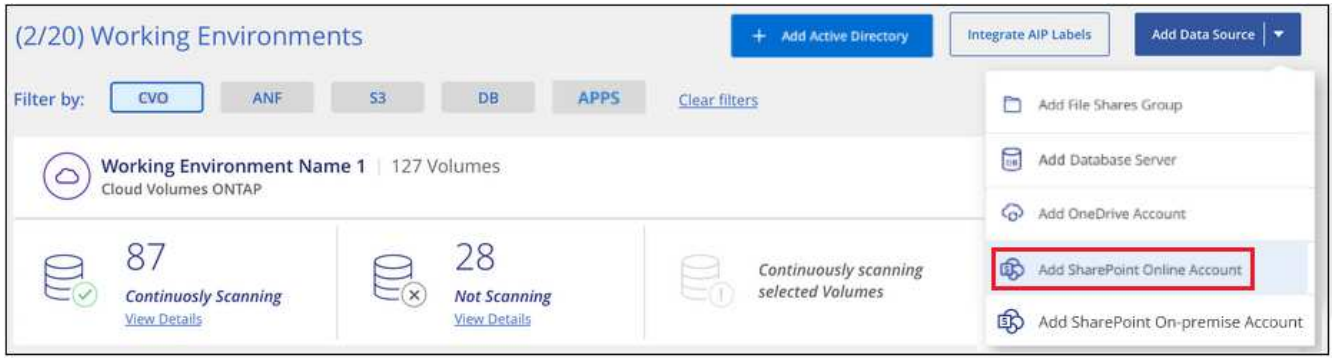
インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

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。

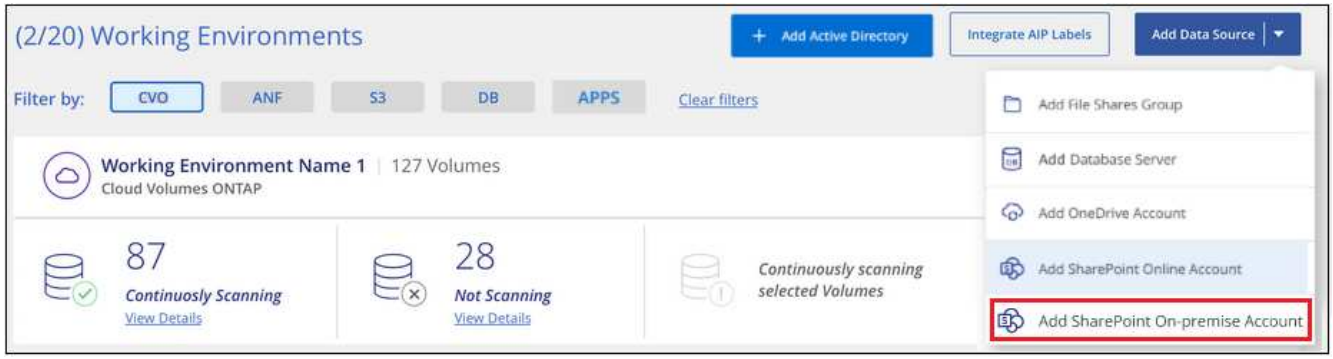
SharePoint Onlineアカウントが作業環境のリストに追加されます。

SharePointオンプレミスアカウントをSharePointオンプレミスアカウントを追加する

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

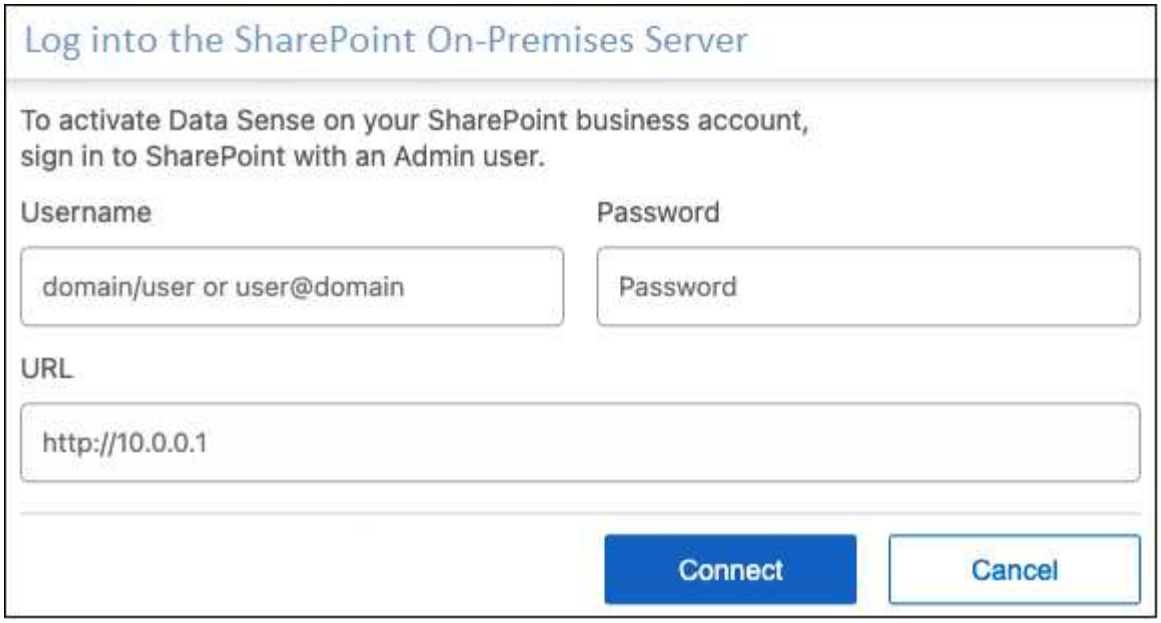
手順

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



ボタンをクリックできる[構成]ページのスクリーンショット。"]

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



3. [接続] をクリックします。

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

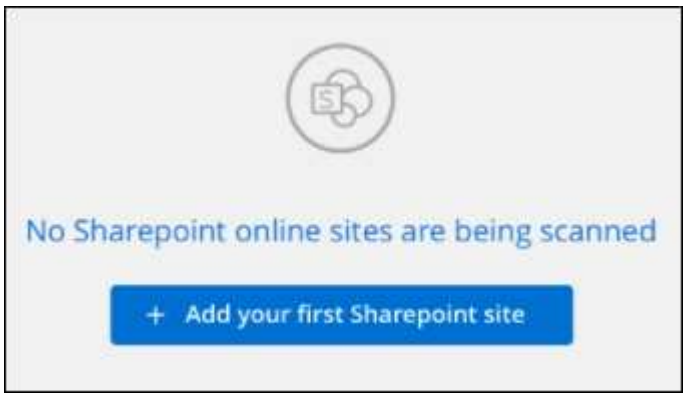
SharePoint サイトをコンプライアンススキャンに追加する

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

手順

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

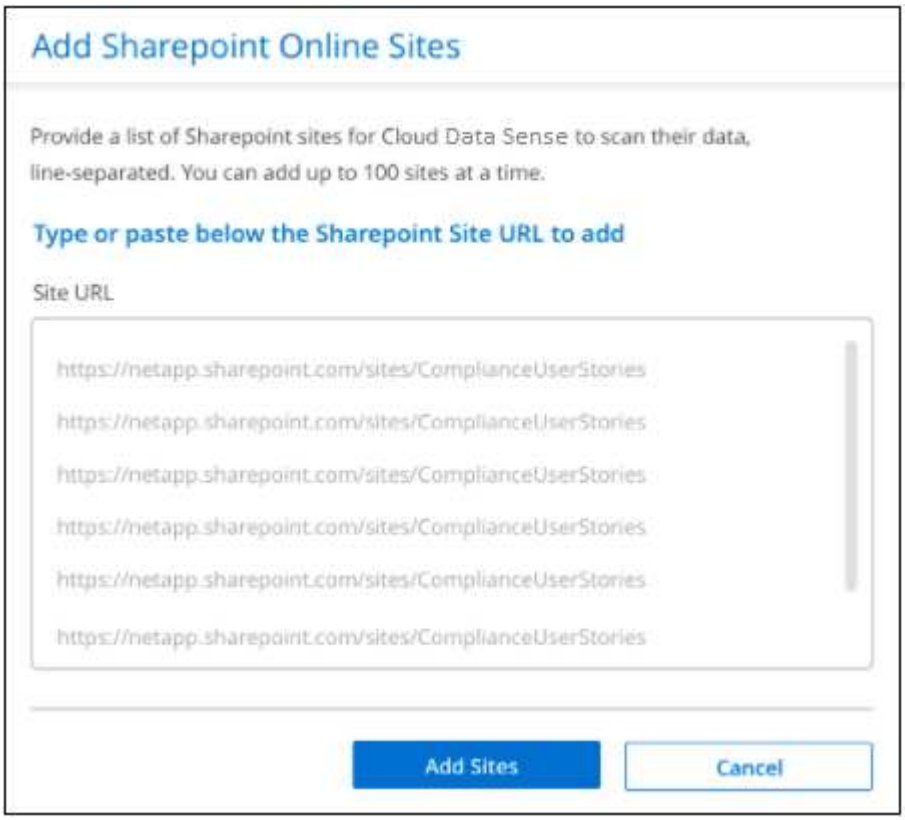
2. この SharePoint アカウントのサイトを初めて追加する場合は、 [* 最初の SharePoint サイトを追加する *] をクリックします。



ボタンを示すスクリーンショット。"]

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

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



確認ダイアログに追加されたサイトの数が表示されます。

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

4. このアカウントに100を超えるサイトを追加する必要がある場合は、[SharePointサイトの追加]*をもう一度クリックして、このアカウントのすべてのサイトを追加します(アカウントごとに合計1,000サイトまで)。
5. SharePoint サイト内のファイルに対して、マッピングのみのスキャン、またはマッピングと分類スキャンを有効にします。

終了：	手順：
ファイルのマッピングのみのスキャンを有効にします	[* マップ *] をクリックします

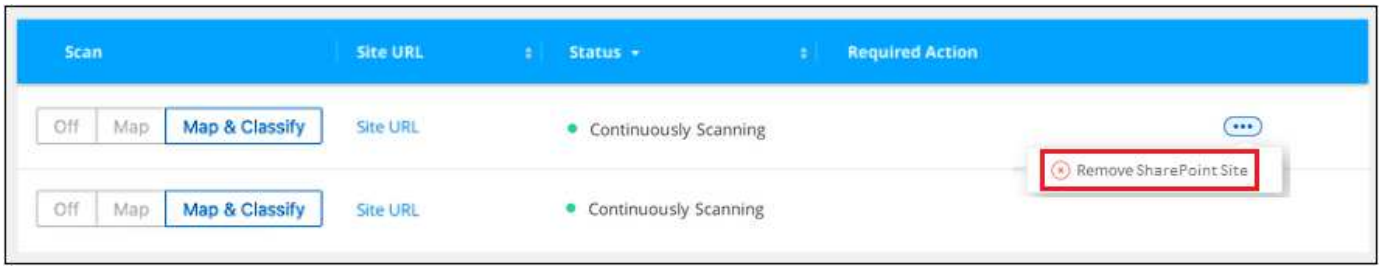
終了：	手順：
ファイルのフルスキャンを有効にします	[マップと分類 *] をクリックします
ファイルのスキャンを無効にします	[* Off *] をクリックします

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"。

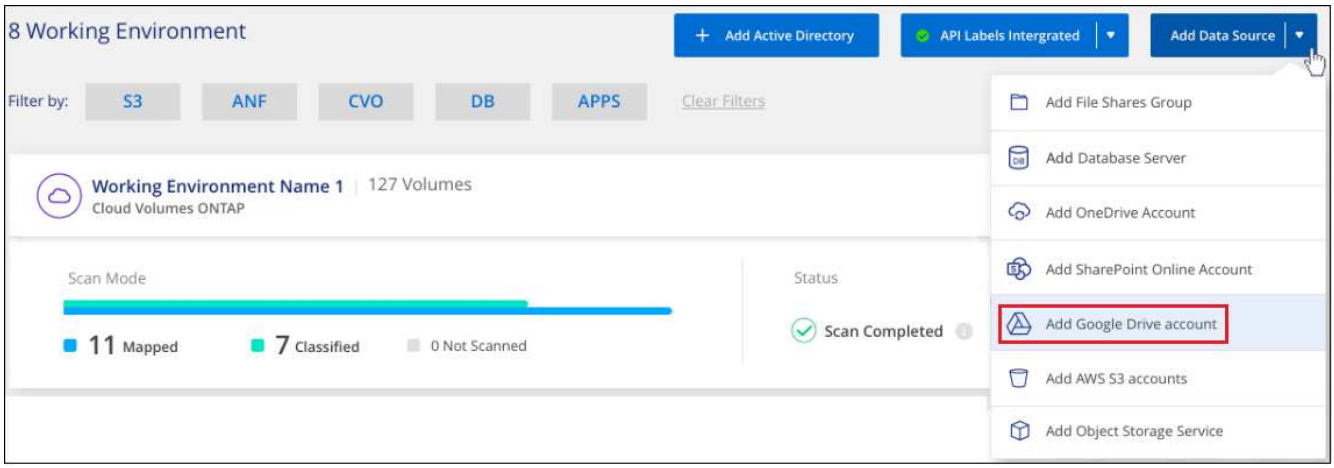
インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

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。

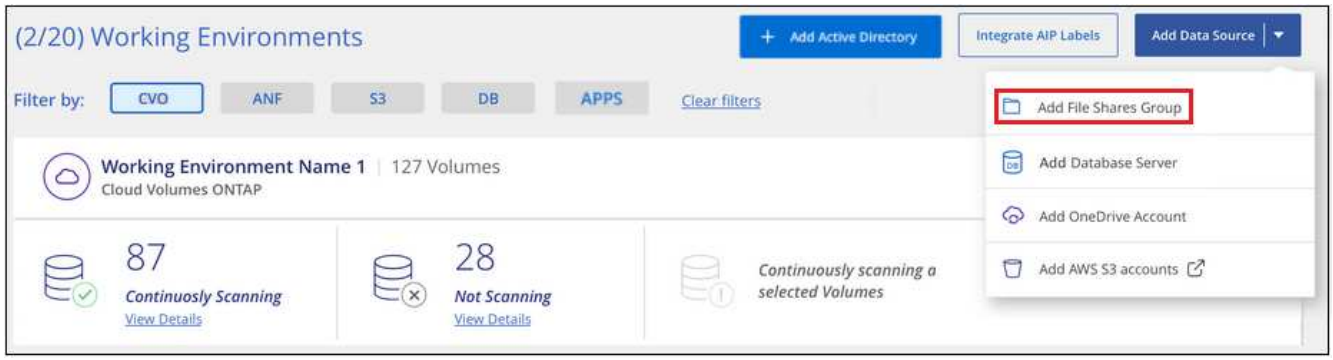
ファイル共有のグループを作成します

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>`。

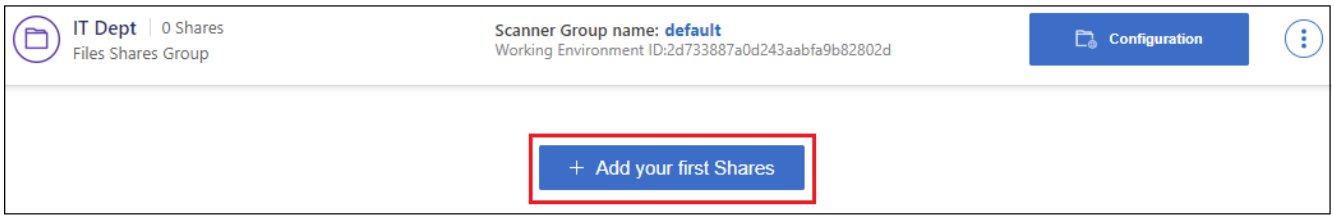
個々のファイル共有を追加することも、スキャンするファイル共有を 1 行で区切って指定することもできます。一度に最大 100 個の共有を追加できます。

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。



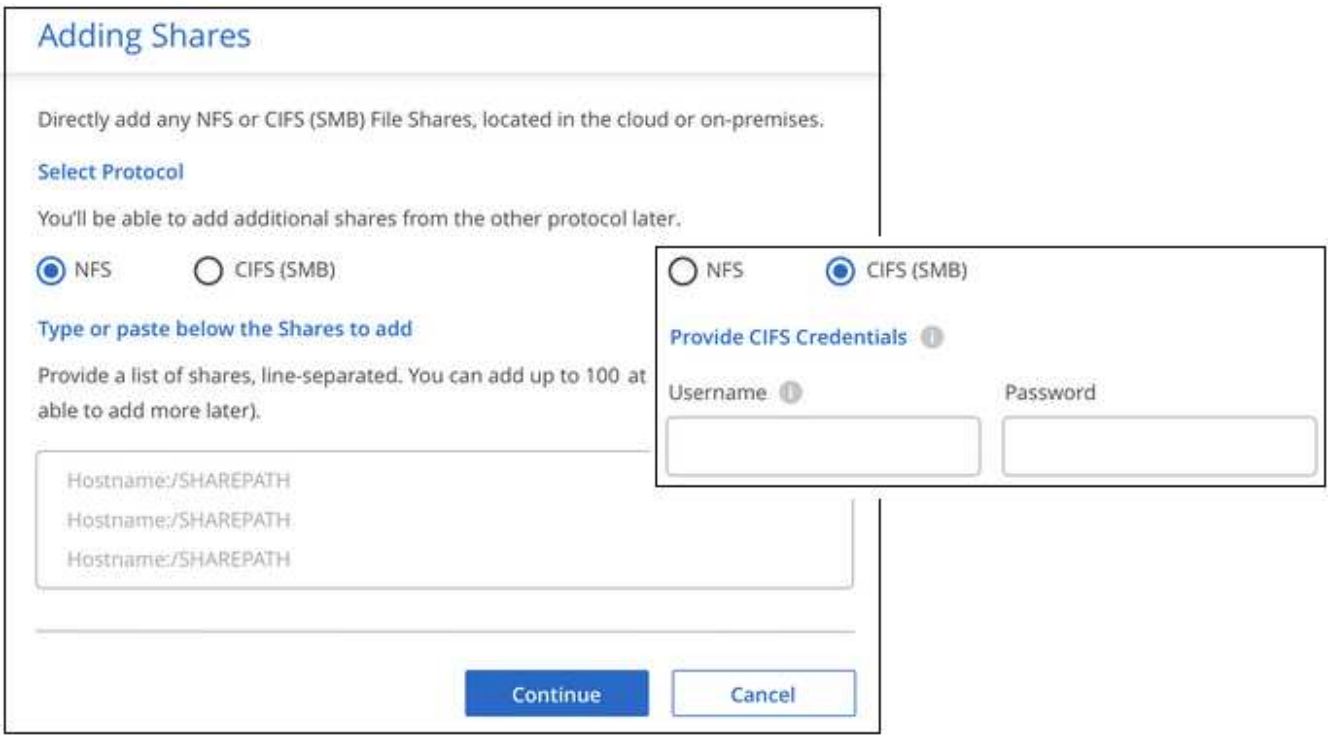
ボタンを示すスクリーンショット。"]

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

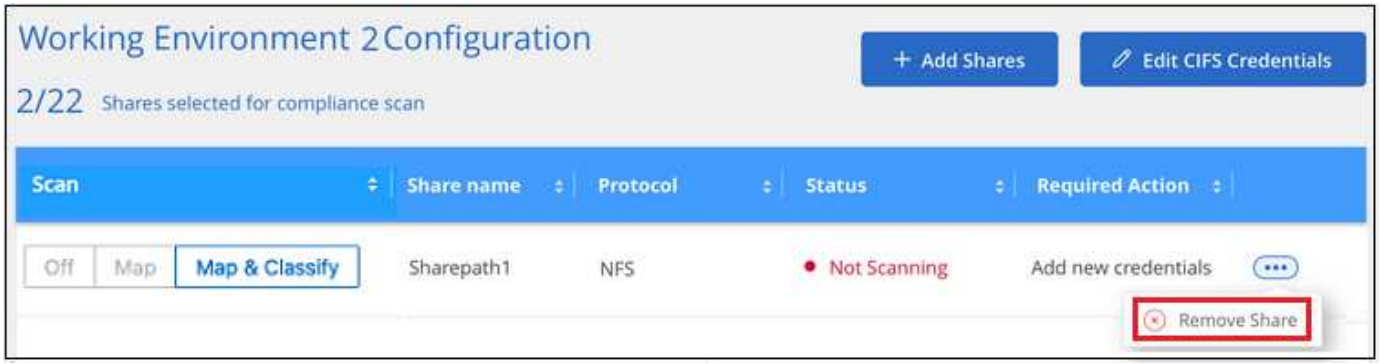
「属性の書き込み」権限がない場合にスキャンする*のページ上部のスイッチは、デフォルトでは無効になっています。つまり、BlueXPの分類にCIFSの属性への書き込み権限やNFSの書き込み権限がない場合、BlueXPの分類では「最終アクセス時間」を元のタイムスタンプに戻すことができないため、ファイルはスキャンされません。最終アクセス時間がリセットされても構わない場合は、スイッチをオンにすると、権限に関係なくすべてのファイルがスキャンされます。 "詳細はこちら。"。

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。

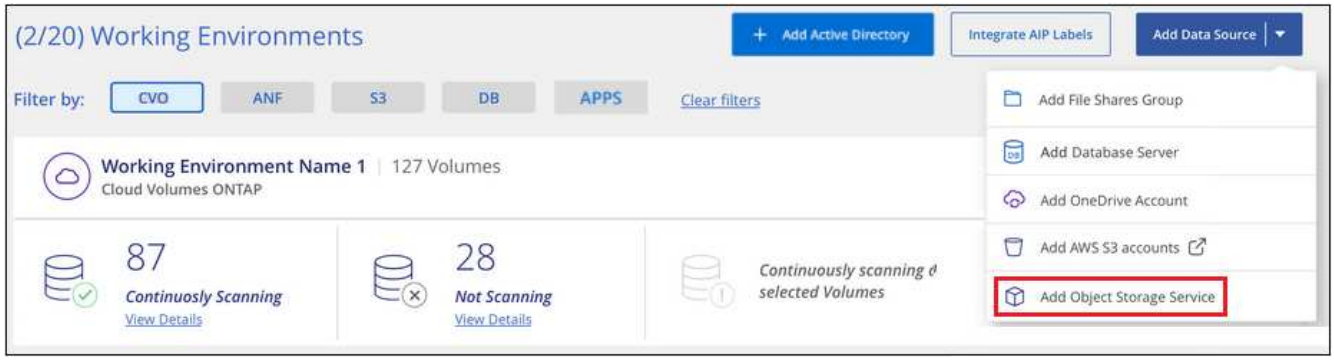
インスタンスがインターネットに接続されていれば、BlueXP分類ソフトウェアへのアップグレードは自動で実行されます。

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

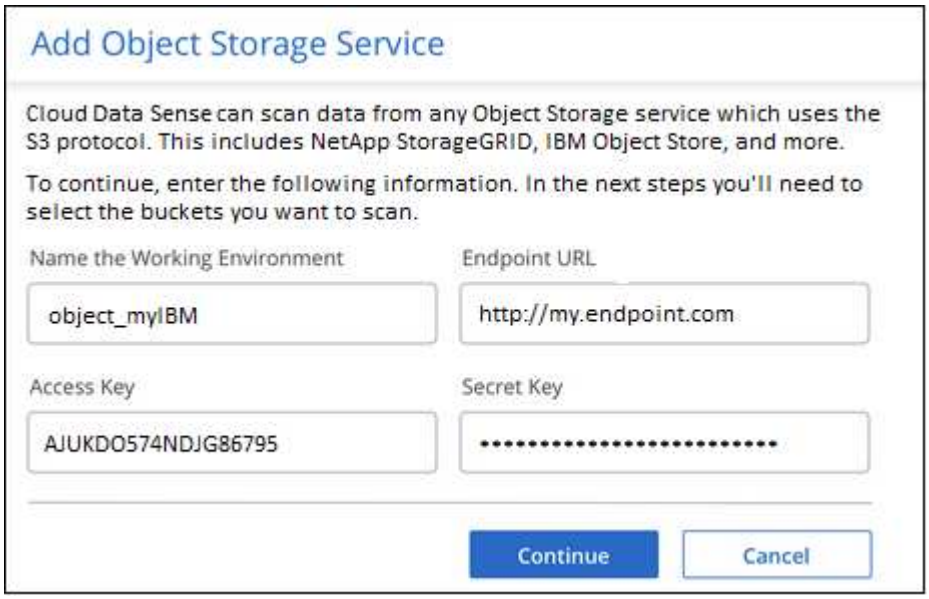
オブジェクトストレージサービスを追加します。

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

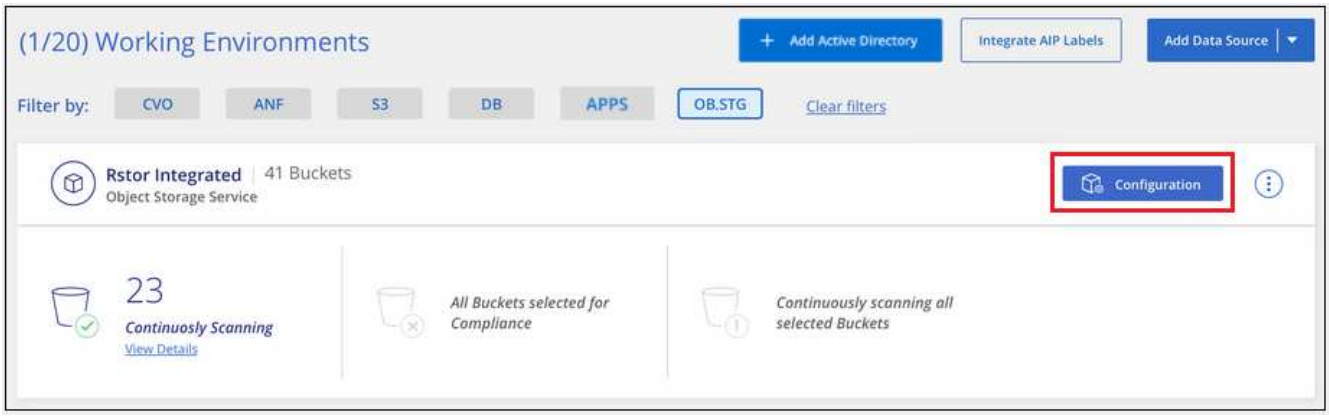
新しいオブジェクトストレージサービスが作業環境のリストに追加されます。

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

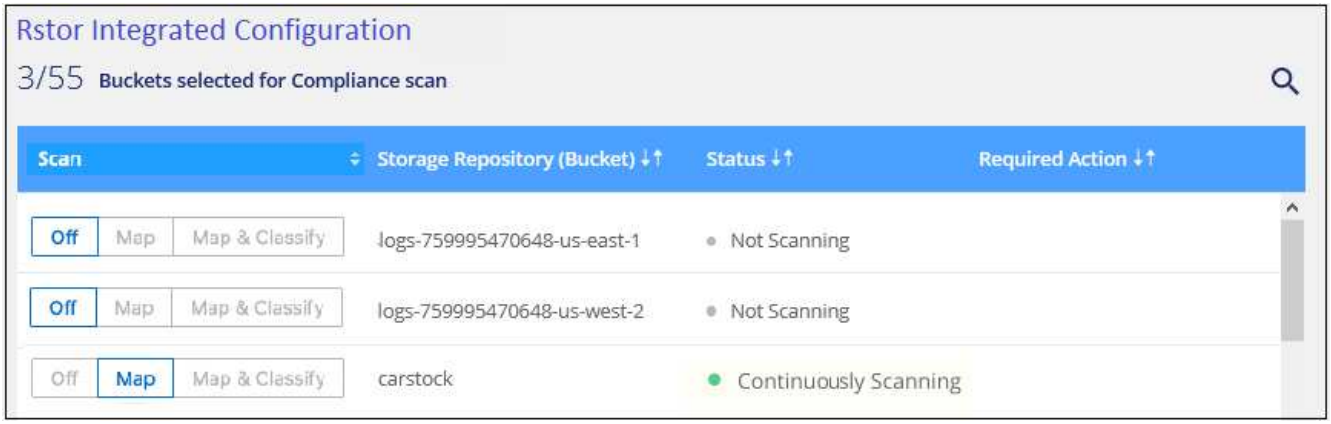
オブジェクトストレージサービスでBlueXPの分類を有効にしたら、次の手順でスキャンするバケットを設定します。BlueXPの分類により、該当するバケットが検出され、作成した作業環境に表示されます。

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

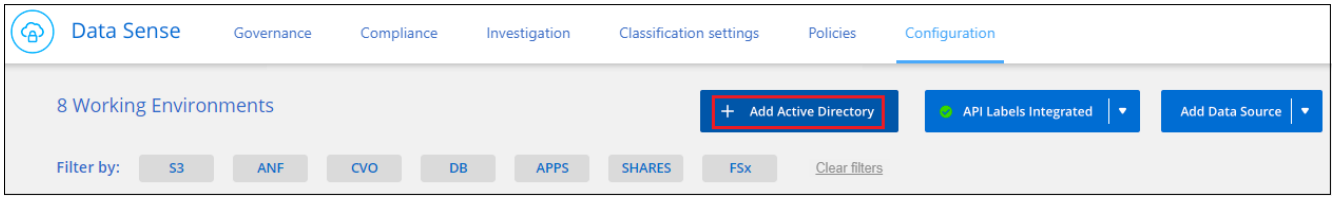
- サーバーにアクセスするためのユーザー名とパスワード
- ドメイン名（ Active Directory 名）
- セキュアな LDAP （ LDAPS ）を使用しているかどうか
- LDAP サーバポート（通常は LDAP では 389 、セキュア LDAP では 636 ）

- 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

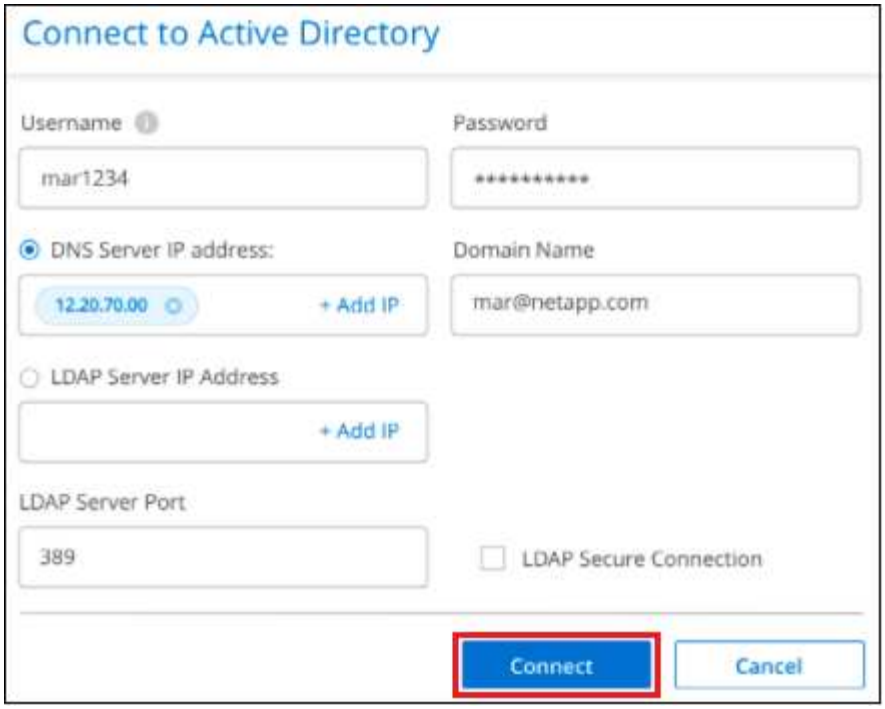
手順

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。

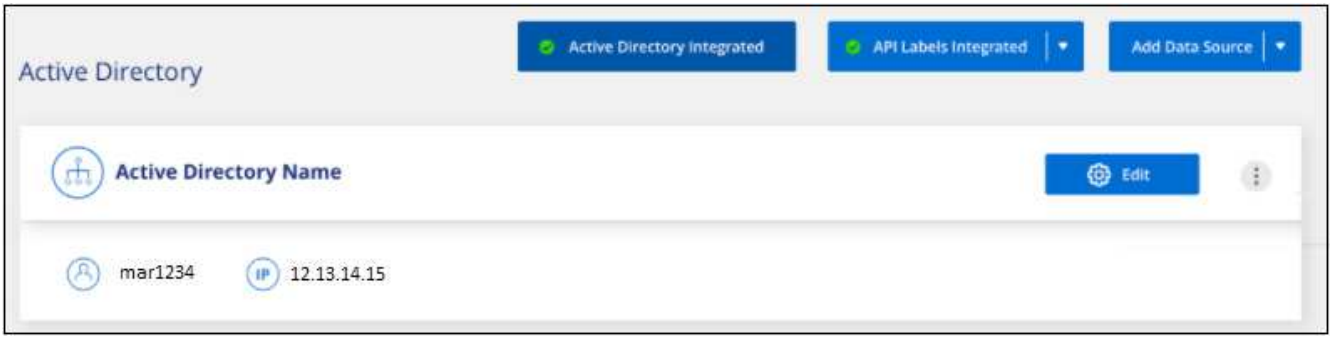


2. Active Directory への接続ダイアログで、 Active Directory の詳細を入力し、 * 接続 * をクリックします。

   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。

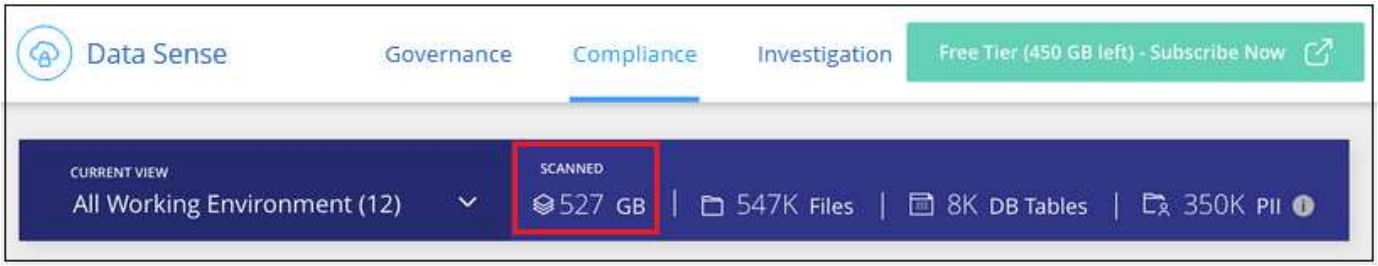
- クラウドプロバイダのマーケットプレイスでBlueXPの従量課金制（PAYGO）サブスクリプションにすでに登録している場合は、BlueXPの分類にも自動的に登録されます。再度サブスクライブする必要はありません。
- BlueXPの分類（Data Sense）であるBring-your-own-license（BYOL）は_floating_licenseです。このライセンスは、スキャンするワークスペース内のすべての作業環境とデータソースに使用できます。BlueXPデジタルウォレットには、アクティブなサブスクリプションが表示されます。
- スキャンされるデータの量は論理ファイルサイズに基づいて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

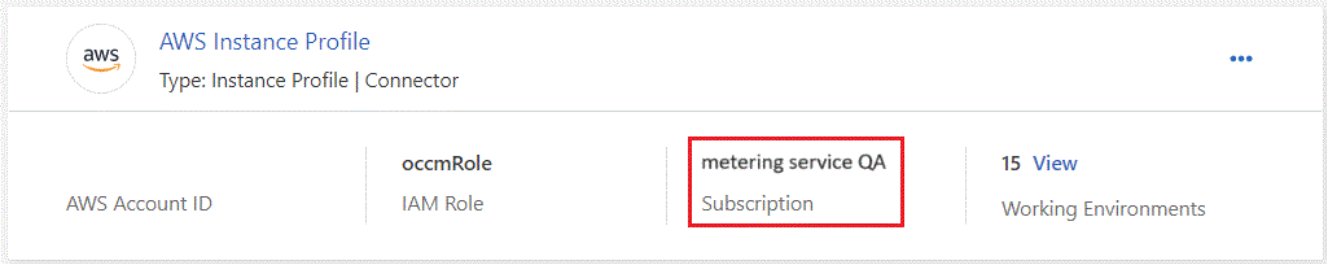
1. BlueXPコンソールの右上にある[設定]アイコンをクリックし、[資格情報*]を選択します。

アイコンを選択できます。"]

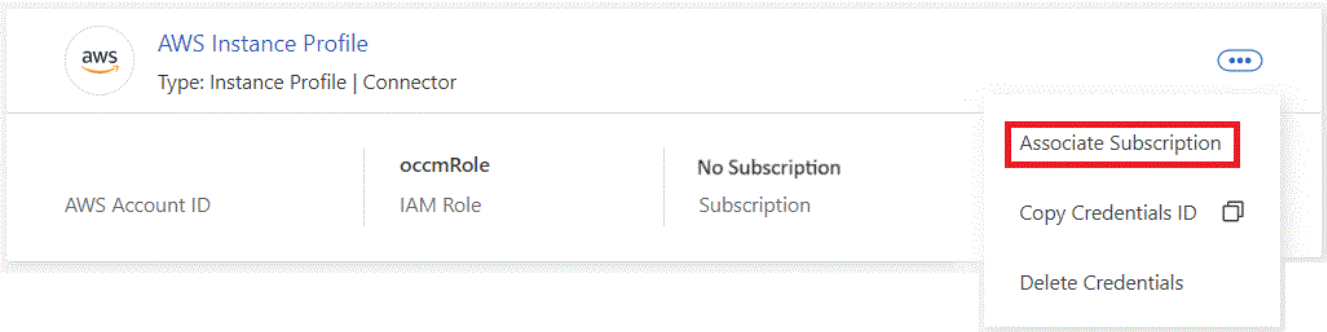
2. [Credentials]*をクリックし、AWSインスタンスプロファイル、Azure Managed Service Identity、またはGoogle Projectのクレデンシャルを検索します。

   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

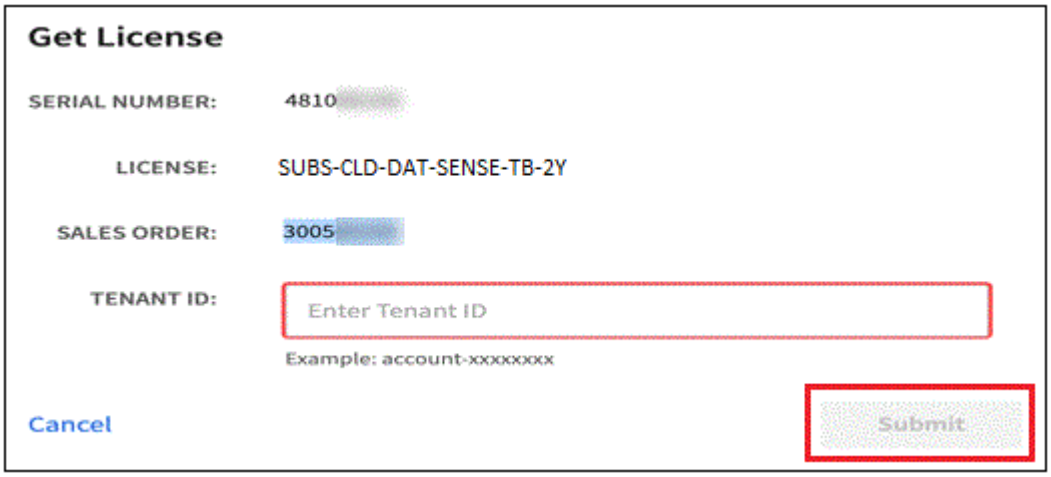
  BlueXPアカウントIDを確認するには、BlueXPの上部にある[**Account**]ドロップダウンを選択し、アカウン

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。

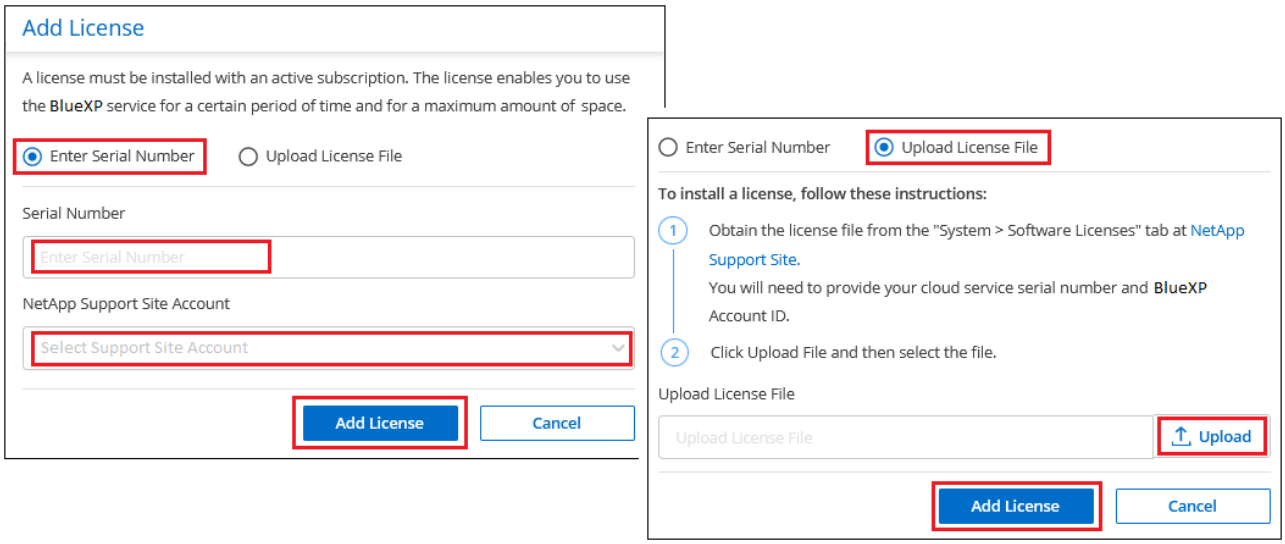
手順

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。



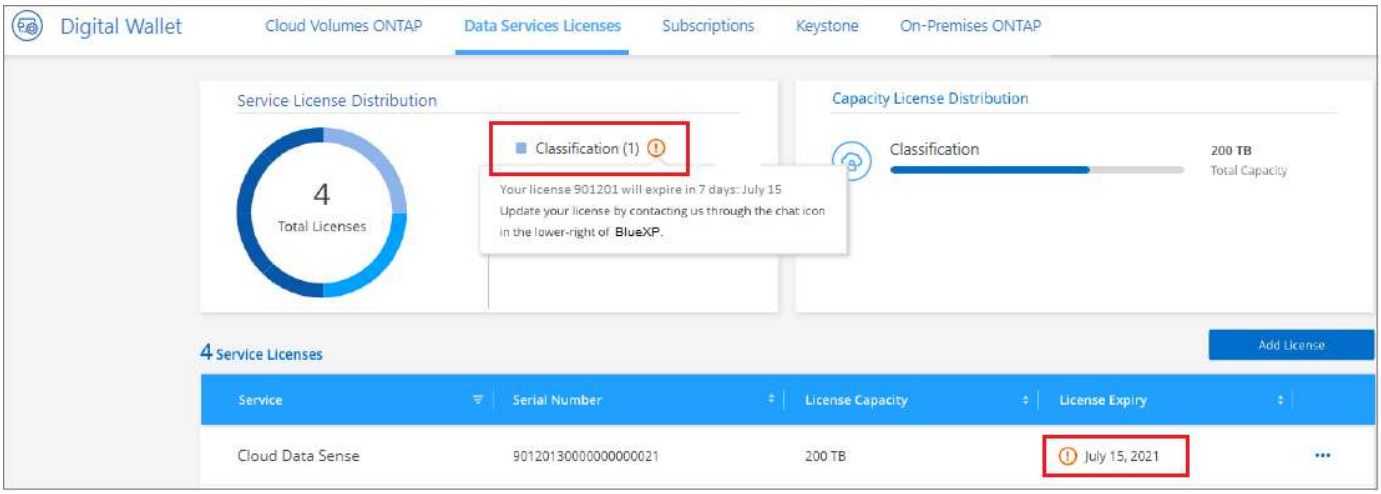
結果

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。