開始する
BlueXP classification

NetApp
January 03, 2025

目次

開始する

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。

重要

2024年5月にバージョン1.31から、BlueXPのコア機能としてBlueXPの分類が追加料金なしで利用できるようになりました。分類ライセンスまたはサブスクリプションは必要ありません。また、BlueXPの分類機能もNetAppストレージシステムに重点を置いているため、一部の未使用の機能やあまり使用されていない機能は廃止されました。

"廃止された機能の一覧を見る"です。

旧バージョン1.30以前を使用していたユーザーは、サブスクリプションが期限切れになるまでそのバージョンを引き続き使用できます。

特徴

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"です。

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。

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の問題を自動的に検出するには、_Policies_を使用します。これにより、セキュリティ担当者はすぐに対処できます。

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。
- アクセス頻度の低いデータを特定して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"です。 "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"です。

サポートされている作業環境とデータソース

BlueXPは、次のタイプの作業環境と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。

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
- StorageGRID
- Azure NetApp Files
- Amazon FSx for ONTAP
- Google Cloud NetAppボリューム

データソース

- NetAppファイル共有
- 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
  - PostgreSQL
  - SAP HANA
  - SQL Server （ MSSQL ）

BlueXPの分類では、NFSバージョン3.x、4.0、4.1、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の分類機能を無料で使用できるようになりました。分類ライセンスや有料サブスクリプションは必要ありません。

インフラコスト

- 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 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。

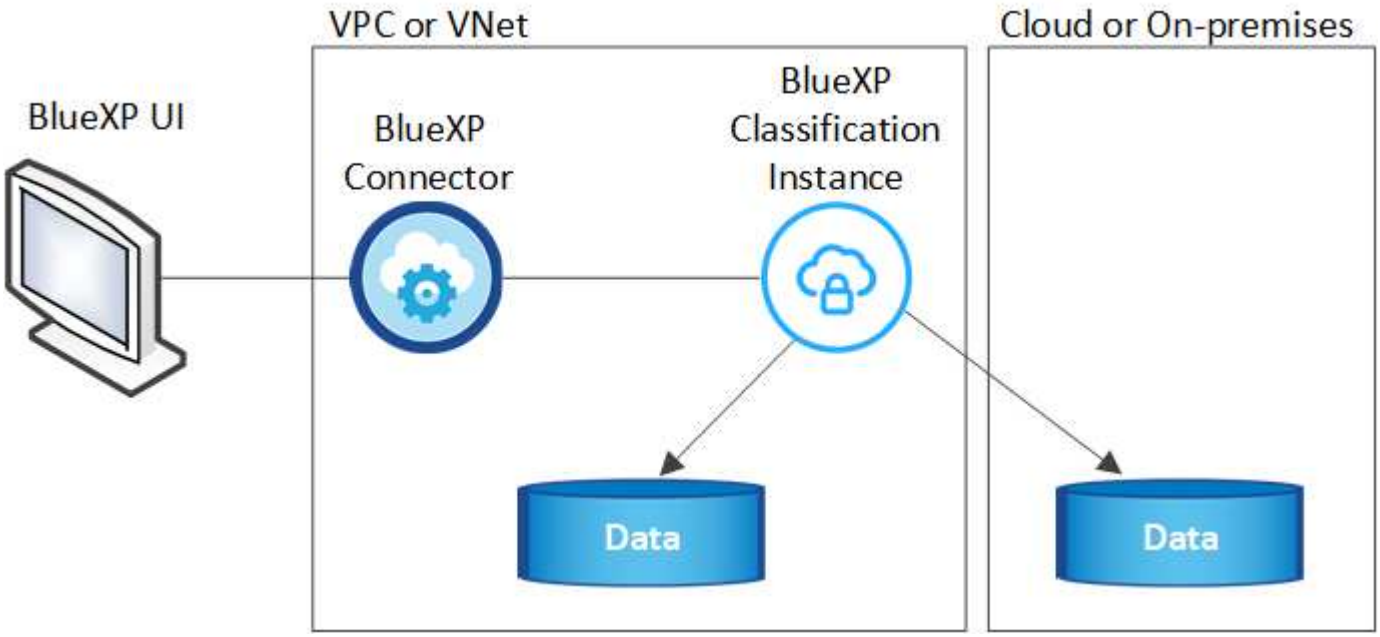
データ転送コスト

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 システムなどのデータソースが_ different_アベイラビリティゾーンまたはリージョンにある場合、データ転送のコストはクラウドプロバイダから請求されます。詳細については、次のリンクを参照してください。

- "AWS：Amazon Elastic Compute Cloud（Amazon EC2）の価格設定"
- "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 分類は500GiBのgp2ディスクを搭載したで実行され "m6i.4xlargeインスタンス"ます。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 分類は、ディスクが500GiBのAで実行され"Standard_D16s_v3 VM"ます。オペレーティングシステムのイメージはUbuntu 22.04です。
- GCPでは、BlueXP 分類は500GiB標準永続ディスクを備えた上で実行され"N2-standard-16 VM"ます。オペレーティングシステムのイメージはUbuntu 22.04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"です。
- インスタンスの名前は *CloudCompliancy_with* で、生成されたハッシュ（ *UUID* ）を連結しています。例：*_CloudCompliion-16bb6564-38ad-40802-9a92-36f5fd2f71c7*
- 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。

さまざまなインスタンスタイプに導入

BlueXP 分類は、CPUとRAMの数が少ないシステムに導入できます。

システムサイズ	仕様	制限事項
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。

AzureまたはGCPにBlueXP 分類を導入する際に、より小さいインスタンスタイプを使用する場合は、ng-contact-data-sense@ NetApp .comまでEメールで支援を要請してください。

BlueXPの分類の仕組み

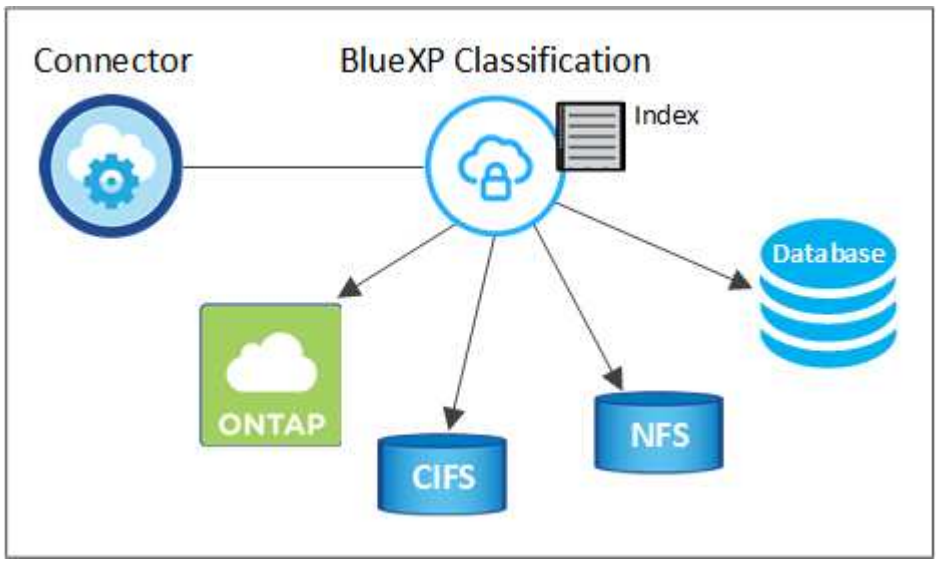
BlueXPの分類の概要は次のようになります。

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、データベーススキーマ、その他のユーザデータ）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、ボリュームレベルまたはデータベーススキーマレベルで有効または無効にすることができます。

マッピングスキャンと分類スキャンの違いは何ですか

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。

機能	分類	マッピング
スキャン速度	遅い	高速
価格設定	無料	無料
容量	最大500TB	最大500TB

機能	分類	マッピング
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
カスタム検索結果を提供する作成"ポリシー"	はい	いいえ
他のレポートを実行できます	はい	いいえ
ファイルからメタデータを表示する機能*	いいえ	はい

*マッピングスキャン中に、次のメタデータがファイルから抽出されます。

- 作業環境
- 作業環境のタイプ
- ストレージリポジトリ
- ファイルタイプ
- 使用済み容量
- ファイル数
- ファイルサイズ
- ファイル作成
- ファイルの最終アクセス
- ファイルの最終変更日
- ファイル検出時刻
- 権限の抽出

ガバナンスダッシュボードの違い：

機能	マッピングと分類	マップ
古いデータ	はい	はい
ビジネス以外のデータ	はい	はい
重複ファイル	はい	はい
事前定義済みポリシー	はい	いいえ
カスタムポリシー	はい	はい
DDAレポート	はい	はい
マッピングレポート	はい	はい
感度レベル検出	はい	いいえ
幅広い権限を持つ機密データ	はい	いいえ
オープンアクセス権	はい	はい
データの使用年数	はい	はい
データのサイズ	はい	はい
カテゴリ	はい	いいえ
ファイルの種類	はい	はい

コンプライアンスダッシュボードの違い：

機能	マッピングと分類	マップ
個人情報	はい	いいえ
機密性の高い個人情報	はい	いいえ
プライバシーリスクアセスメントレポート	はい	いいえ
HIPAAレポート	はい	いいえ
PCI DSS レポート	はい	いいえ

調査フィルタの違い：

機能	マッピングと分類	マップ
ポリシー	はい	はい
作業環境のタイプ	はい	はい
作業環境	はい	はい
ストレージリポジトリ	はい	はい
ファイルタイプ	はい	はい
ファイルサイズ	はい	はい
時刻を作成しました	はい	はい
検出時刻	はい	はい
最終更新日	はい	はい
最終アクセス	はい	はい
オープンアクセス権	はい	はい
ファイルディレクトリパス	はい	はい
カテゴリ	はい	いいえ
感度レベル	はい	いいえ
IDの数	はい	いいえ
個人データ	はい	いいえ
機密性の高い個人データ	はい	いいえ
データ主体	はい	いいえ
重複	はい	はい
分類ステータス	はい	ステータスは常に「限定的なインサイト」です。
スキャン分析イベント	はい	はい
ファイルハッシュ	はい	はい
アクセス権を持つユーザの数	はい	はい
ユーザ/グループの権限	はい	はい
ファイルの所有者	はい	はい
ディレクトリタイプ	はい	はい

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では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1日に15~40TiBのデータをスキャンできます。

BlueXP 分類によって分類される情報

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*ファイルについて：ファイルの種類、サイズ、作成日、変更日など。
- 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の個人識別情報(PII)。"個人データの詳細については、こちらをご覧ください"です。
- 機密性の高い個人データ: GDPRおよび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、民族起源、政治的意見などの特別な種類の機密個人情報(SPii)。"機密性の高い個人データの詳細をご覧ください"です。
- カテゴリ: BlueXP 分類は、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"です。
- **types**: BlueXP 分類では、スキャンしたデータをファイルの種類別に分類します。"タイプの詳細については、こちらをご覧ください"です。
- 名前エンティティ認識: BlueXP 分類は、AIを使用してドキュメントから人の自然な名前を抽出します。"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"です。

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。

ネットワークに関する厳しい要件がある場合は、を"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"参照してください。

BlueXP 分類でのユーザロール

各ユーザに割り当てられたロールは、BlueXP 内およびBlueXP 分類内で異なる機能を提供します。詳細については、次を参照してください。

- "BlueXP IAMロール"（標準モードでBlueXP を使用している場合）
- "BlueXP アカウントノロール"（制限モードまたはプライベートモードでBlueXP を使用する場合）

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"です。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。
- "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"です。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、BlueXP SaaSレイヤに接続されません。

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、可能であることに注意して"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"ください。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 コネクターの作成

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

ネットワーク内のLinuxホストやクラウド内のLinuxホストにも対応できます "コネクタをオンプレミスにインストールします"。

2 前提条件の確認

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です。

3 Deploy BlueXP Classification

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。

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。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"を参照してください "AWS でコネクタを作成する"。ほとんどの場合、BlueXP 分類をアクティブ化する前にコネクタが設定されている可能性があります。ほとんどの場合、コネクタを今すぐ設定する必要がある場合があります。 "BlueXPの機能にはコネクタが必要です"

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またはAmazon FSx for ONTAPバケットで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。

これらのクラウドコネクタを使用すると、オンプレミスのONTAPシステム、NetAppファイル共有、データベースをスキャンできます。

ネットワーク内またはクラウド内のLinuxホストでも実行できます "コネクタをオンプレミスにインストールします"。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。

ご覧のとおり、使用する必要がある状況がある場合があり "複数のコネクタ"ます。

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。

"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"です。

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。最新のBlueXP 権限については、を参照し "ネットアップが提供するポリシー"てください。

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。詳細は、を参照してください "AWS のコネクターのルール"。

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。詳細は、を参照してください "Azure のコネクタのルール"。

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"です。

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"

BlueXPの分類機能をクラウドに導入します

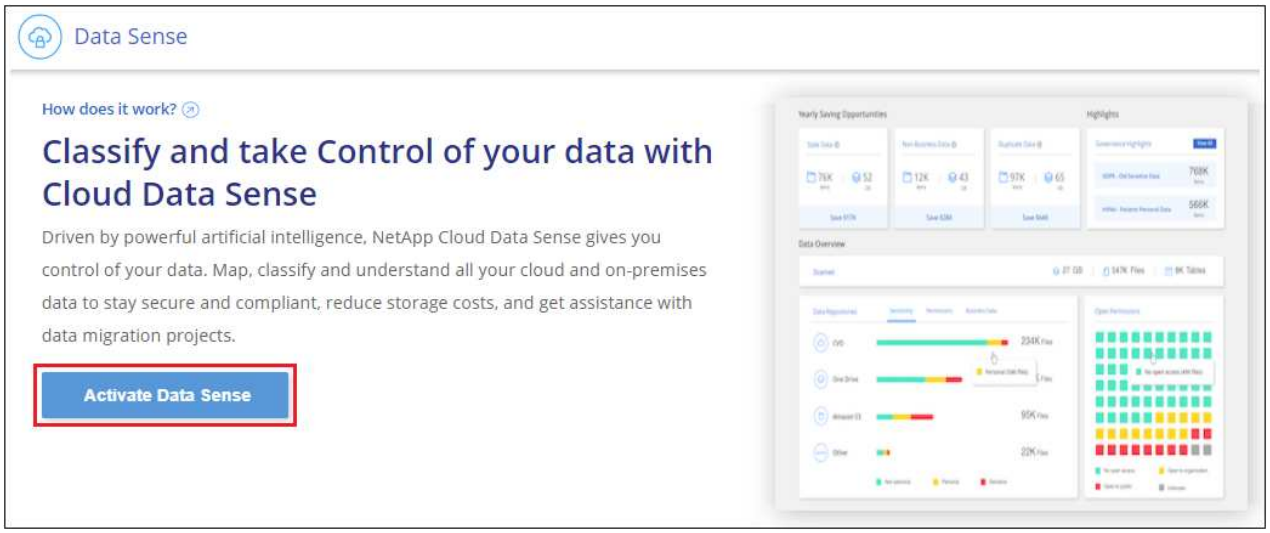
BlueXP分類のインスタンスをクラウドに導入するには、次の手順を実行します。コネクタはインスタンスをクラウドに導入し、そのインスタンスにBlueXP分類ソフトウェアをインストールします。

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 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。



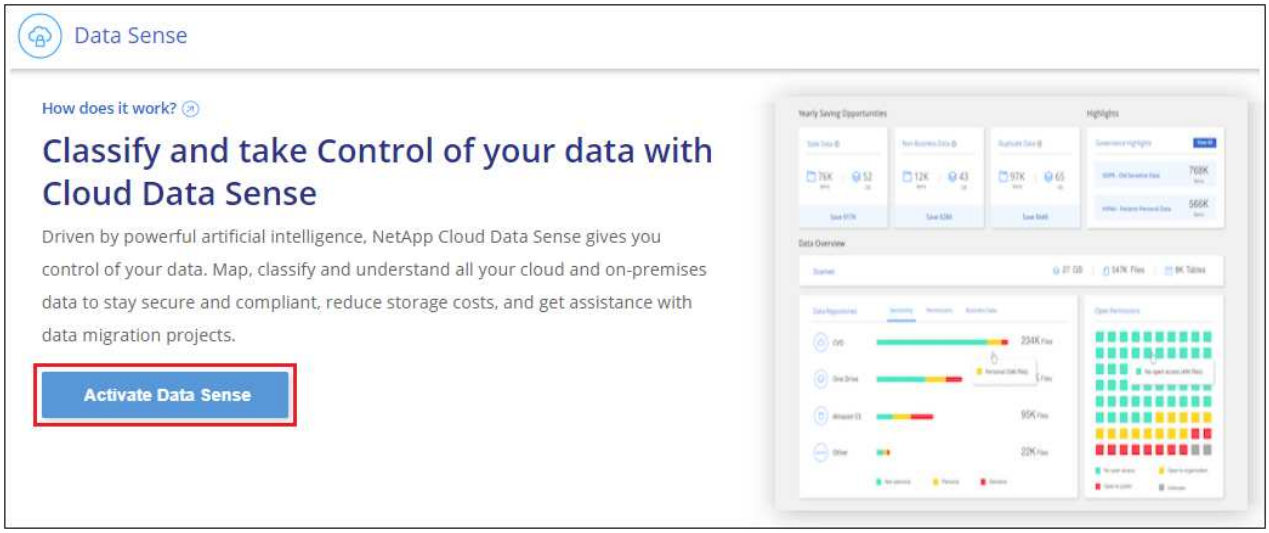
2. [データセンスを活動化（ Activate Data sense ）] をクリックし
3. [*Installation*]ページで、*[Deploy]>[Deploy]*をクリックして「Large」インスタンスサイズを使用し、クラウド導入ウィザードを開始します。
4. 導入手順が完了すると、ウィザードに進捗状況が表示されます。問題が発生した場合は、停止して入力を求められます。

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。

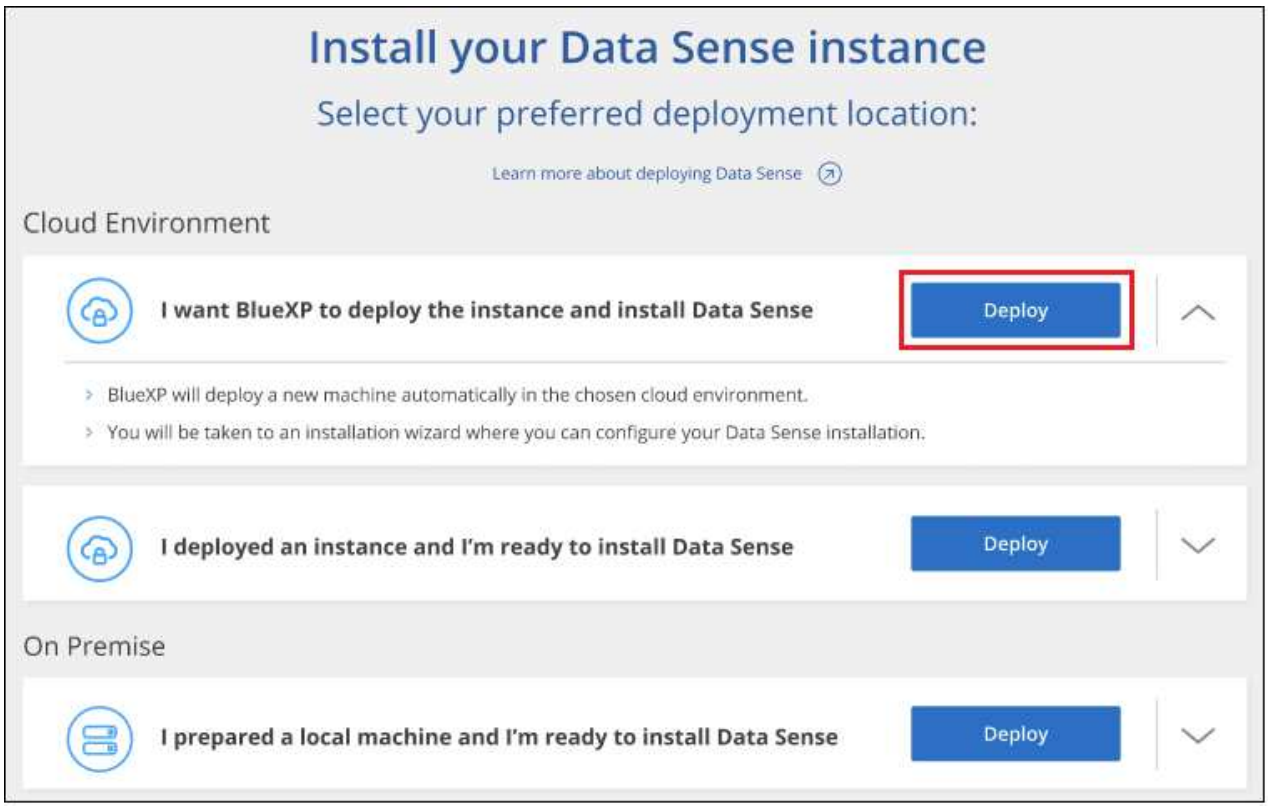
Azureへの導入

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。



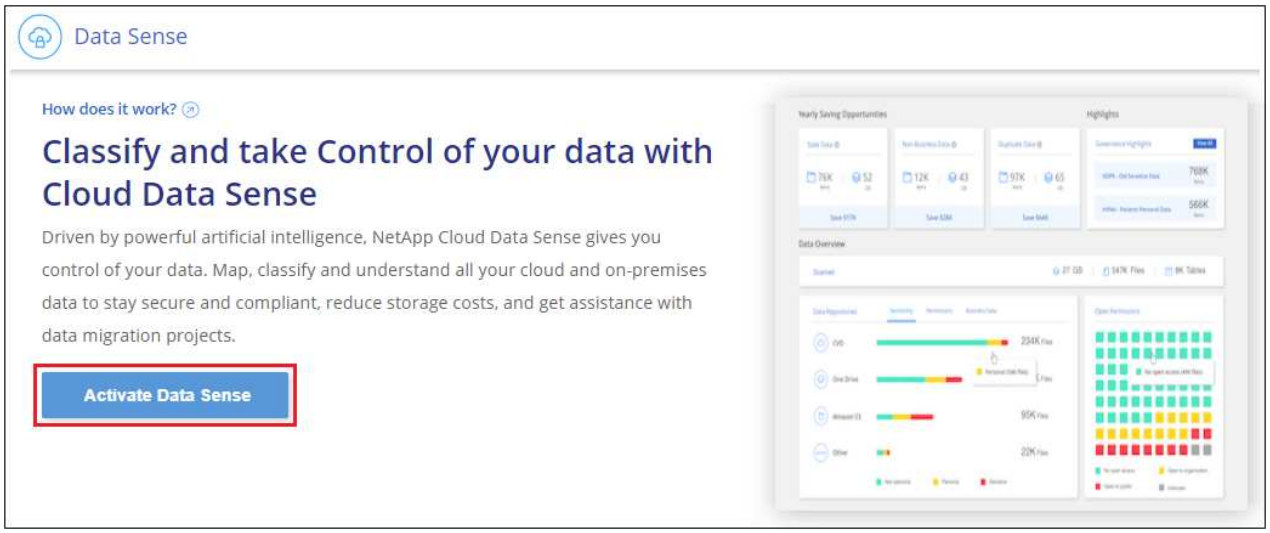
4. 導入手順が完了すると、ウィザードに進捗状況が表示されます。問題が発生した場合は、停止して入力を求められます。

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。

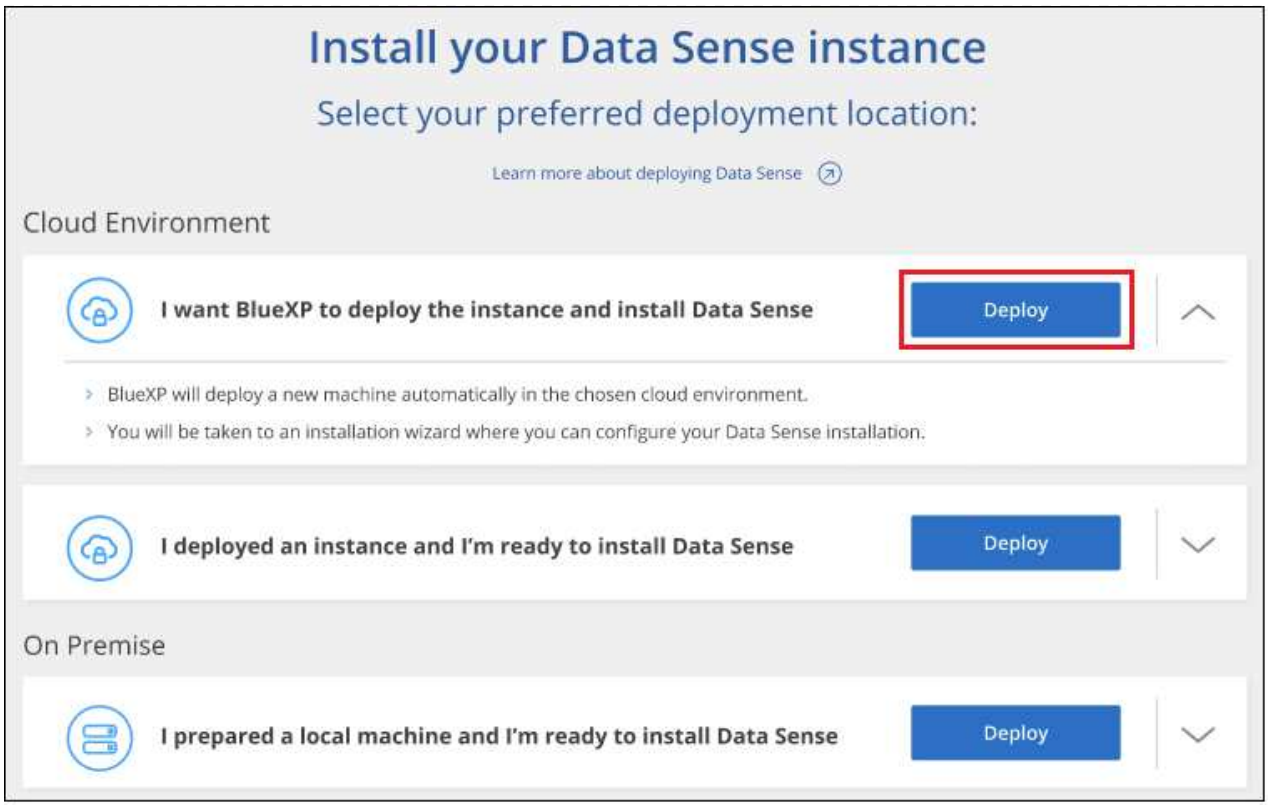
Google Cloudに導入

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。

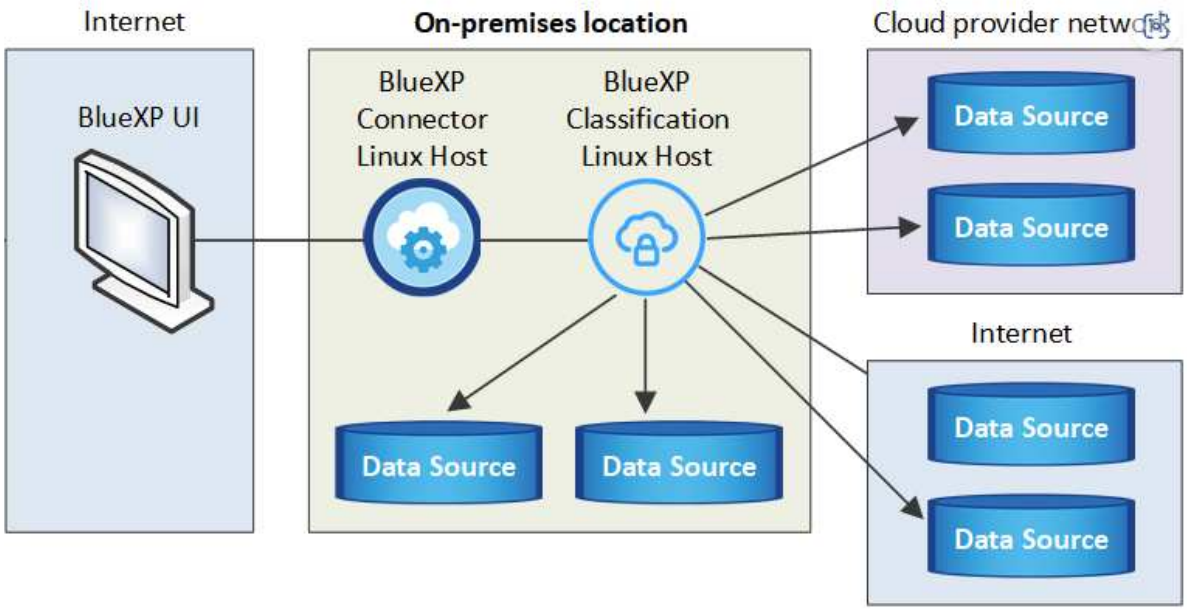
インターネットにアクセスできるホストに**BlueXP**分類をインストールします

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。

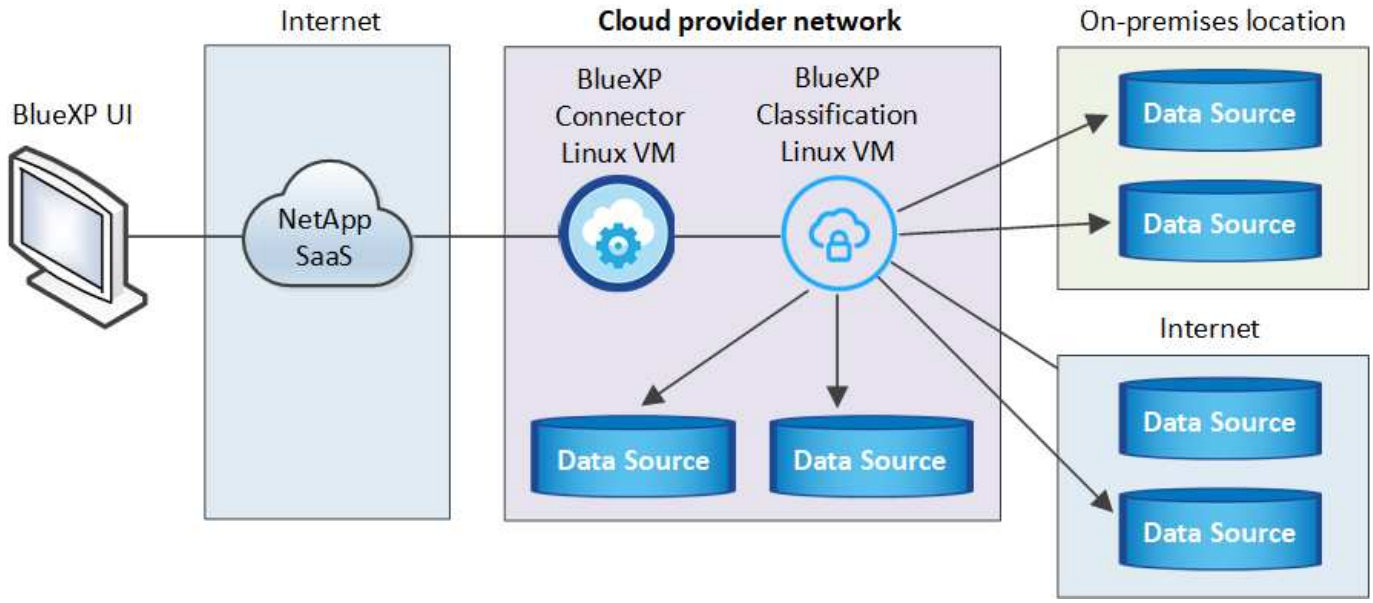
オンプレミス環境は、同じくオンプレミスにあるBlueXP分類インスタンスを使用してオンプレミスのONTAPシステムをスキャンする場合に適したオプションですが、これは必須ではありません。どのインストール方法を選択しても、ソフトウェアはまったく同じように機能します。

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"です。

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。



レガシーバージョン1.30以前で、複数のホストにBlueXP 分類をインストールする必要がある場合は、を参照してください"インターネットアクセスのない複数のホストにBlueXP分類をインストールする"。

あなたもできます"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にBlueXPの分類をインストールします"。

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 コネクターの作成

コネクタがない場合、 "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。、 "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"を参照してください "AWS でコネクタを作成する"。

2 前提条件の確認

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です。

また、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** 分類のダウンロードと導入

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。

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 分類をアクティブ化する前にコネクタが設定されている可能性があります。ほとんどの場合、コネクタを今すぐ設定する必要がある場合があります。 "BlueXPの機能にはコネクタが必要です"

クラウドプロバイダ環境で作成する方法については、、 "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"を参照してください "AWS 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またはAmazon FSx for ONTAPで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、NetAppファイル共有、データベースアカウントは、次のいずれかのクラウドコネクタを使用してスキャンできます。

ネットワーク内のLinuxホストやクラウド内のLinuxホストにも使用できます "コネクタをオンプレミスに導入"。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。

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、これら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	SSDが1TiB、または-100GiBが/opt-895GiBが/var/lib/dockerで-5GiBが/tmpで利用可能
大きい	CPU×16	64GBのRAM	500GiB SSDオン/または-100GiBオン/opt-395GiBオン/var/lib/dockerまたはPodman/var/lib/containersまたはPodman/var/lib/containersの場合は-5GiBオン/tmp

- 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。
  - * Amazon Elastic Compute Cloud（Amazon EC2）インスタンスタイプ*：「m6i.4xlarge」を推奨します。"追加のAWSインスタンスタイプを参照してください"です。
  - * 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"です。
  - **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"です。
- * 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
    - Ubuntu 22.04（BlueXP分類バージョン1.23以降が必要）
    - Ubuntu 24.04（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、9.4
- * 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"です。
- Podmanバージョン4以降。Podmanをインストールするには、と入力し (`sudo yum install podman netavark -y`ます）。

- Pythonバージョン3.6以降。 "インストール手順を確認します"です。
  - * 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。
  - * firewalldの考慮事項*：を使用する場合は `firewalld`、BlueXP 分類をインストールする前に有効にすることをお勧めします。次のコマンドを実行して、BlueXP 分類と互換性があるようにを設定し`firewalld`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
```

+
設定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ります `firewalld`。

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。

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://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

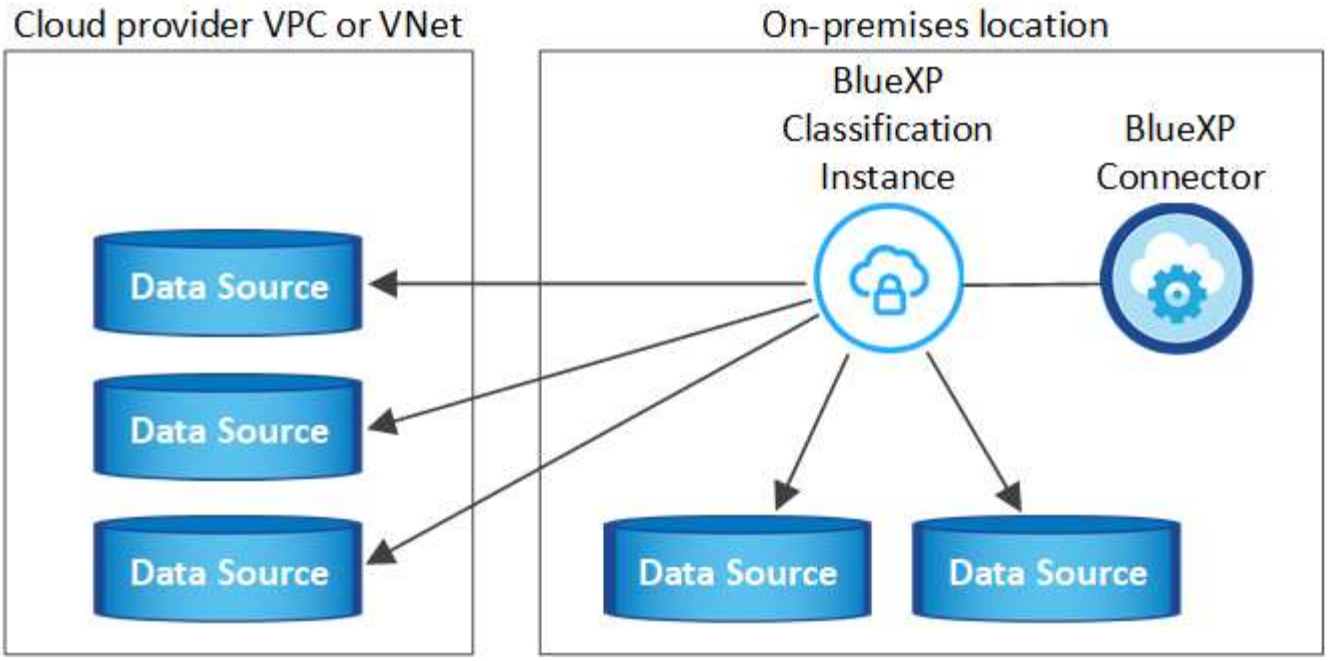
コネクタ、BlueXP分類、Active Directory、データソースの間の通信に必要なすべてのポートが開いていることを確認する必要があります。

接続タイプ	ポート	製品説明
コネクタ<> BlueXPの分類	8080（TCP）、443（TCP）、および80。9000	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。Linuxホストでファイアウォールが使用されている場合は、Ubuntuサーバ内の内部プロセスにポート9000が必要です。
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。

接続タイプ	ポート	製品説明
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。
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 ）

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です。



BlueXP 分類を導入する前の要件については、および前提条件の確認を参照してくださいLinux ホストシステムの準備。

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、クラウドおよびさまざまなデータソースに別 々 のコネクタとBlueXP 分類のインスタンスをデプロイする必要があり "コネクタを切り替えます"ます。

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"を参照して、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 `/opt/netapp/install_logs/` ます。"詳細はこちら"です。

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。
- 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。

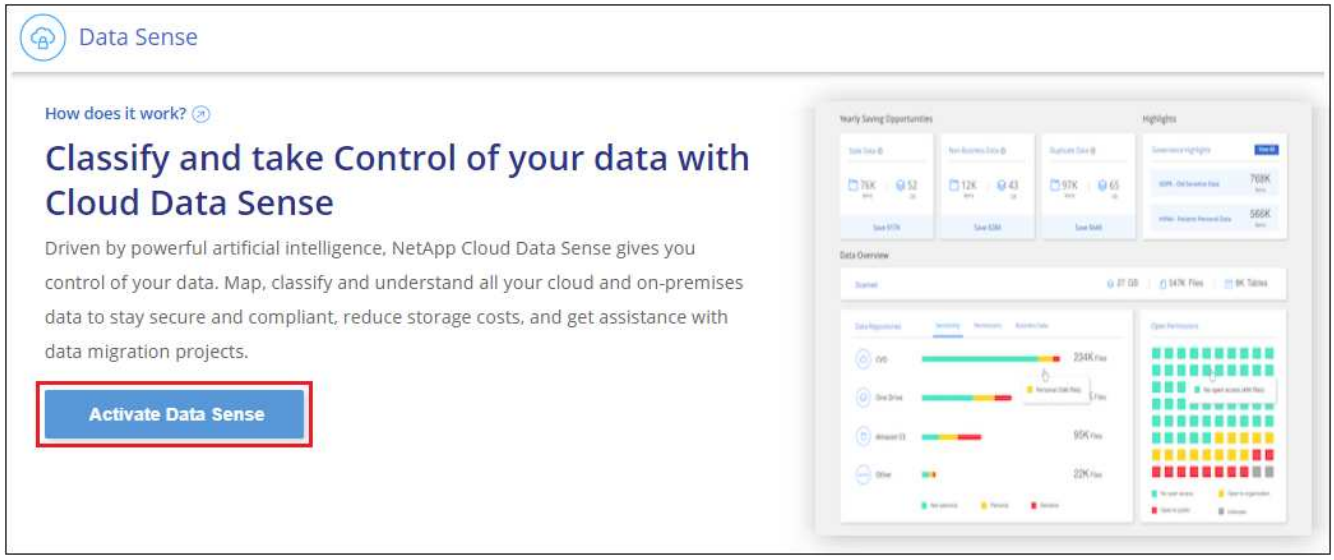
- オフライン環境が要件を満たしていることを確認します権限と接続。

手順

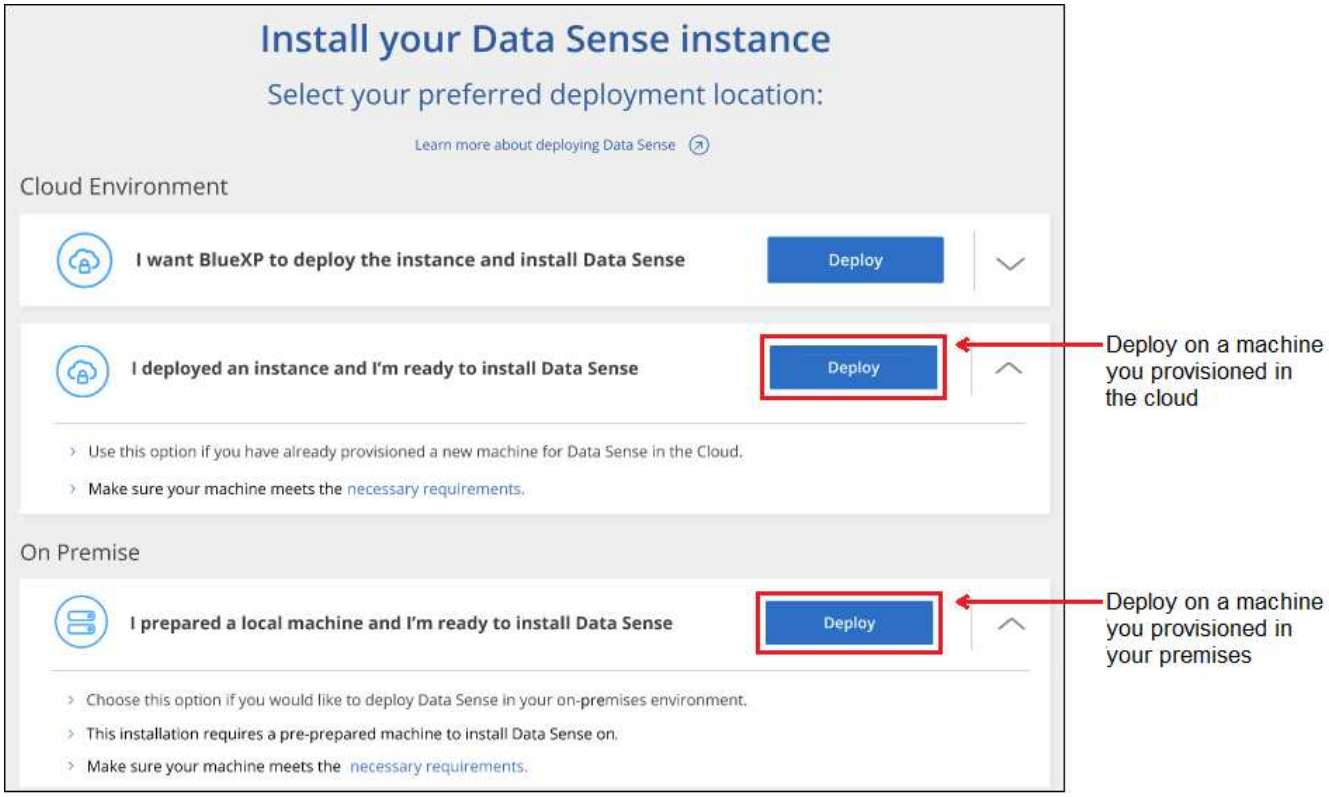
1. からBlueXP 分類ソフトウェアをダウンロードし "NetAppサポートサイト"ます。選択するファイルの名前は* DATASENSE-installer -<version> .tar.gz *です。
2. 使用するLinuxホストにインストーラファイルをコピーします（またはその他の方法を使用 `scp`）。
3. ホストマシンでインストーラファイルを解凍します。次に例を示します。

```
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（例：）をコピーし`sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq`てテキストファイルに貼り付け、後で使用できるようにします。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。

   インストーラは事前チェックを実行して、インストールを正常に完了するためのシステム要件とネットワーク要件が満たされていることを確認します。 "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 分かかる場合があります。

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

設定ページで、スキャンするデータソースを選択できます。

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。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では、BlueXP SaaSレイヤには接続されません。

"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。"です。

また、可能であることに注意して"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"ください。

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"です。

> レガシーバージョン1.30以前で、複数のホストにBlueXP 分類をインストールする必要がある場合は、を参照してください"インターネットアクセスのない複数のホストにBlueXP分類をインストールする"。

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

現時点では、BlueXPの分類がプライベートモードで導入されている場合、Cloud Volumes ONTAP、Azure NetApp Files、FSx for ONTAPのアカウントのスキャンはサポートされていません。

制限事項

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。

- 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
- 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。各リリースの新機能とその機能が必要かどうかを確認するには、を確認して"BlueXPの分類に関するリリースノート"ください。その後、およびの手順に従うことができます "BlueXP Connectorをアップグレードします"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** コネクタの取り付け

プライベートモードでコネクタをインストールしていない場合は、今すぐLinuxホストにインストールし "コネクタを配置します"ます。

2 **BlueXP** 分類の前提条件を確認する

Linuxシステムがを満たしていることホストの要件、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権限と接続ます。

3 **BlueXP** 分類のダウンロードと導入

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。

BlueXPコネクタを取り付けます

プライベートモードでBlueXP Connectorをインストールしていない場合は、オフラインサイトのLinuxホストにインストールし "コネクタを配置します"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。

- 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、これら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	SSDが1TiB、または-100GiBが/opt-895GiBが/var/lib/dockerで-5GiBが/tmpで利用可能

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
大きい	CPU×16	64GBのRAM	500GiB SSDオン/または-100GiBオン/opt-395GiBオン/var/lib/dockerまたはPodman/var/lib/containersまたはPodman/var/lib/containersの場合は-5GiBオン/tmp

- 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。
  - * Amazon Elastic Compute Cloud（Amazon EC2）インスタンスタイプ*：「m6i.4xlarge」を推奨します。"追加のAWSインスタンスタイプを参照してください"です。
  - * 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"です。
  - **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"です。
- * 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
    - Ubuntu 22.04（BlueXP分類バージョン1.23以降が必要）
    - Ubuntu 24.04（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、9.4
- * 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"です。
    - Podmanバージョン4以降。Podmanをインストールするには、と入力し (`sudo yum install

podman netavark -y`ます）。

- Pythonバージョン3.6以降。 "インストール手順を確認します"です。
  - * 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。
  - * firewalldの考慮事項*：を使用する場合は `firewalld`、BlueXP 分類をインストールする前に有効にすることをお勧めします。次のコマンドを実行して、BlueXP 分類と互換性があるようにを設定し`firewalld`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
```

    設定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ります `firewalld`。

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。最新のBlueXP 権限については、を参照し "ネットアップが提供するポリシー"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

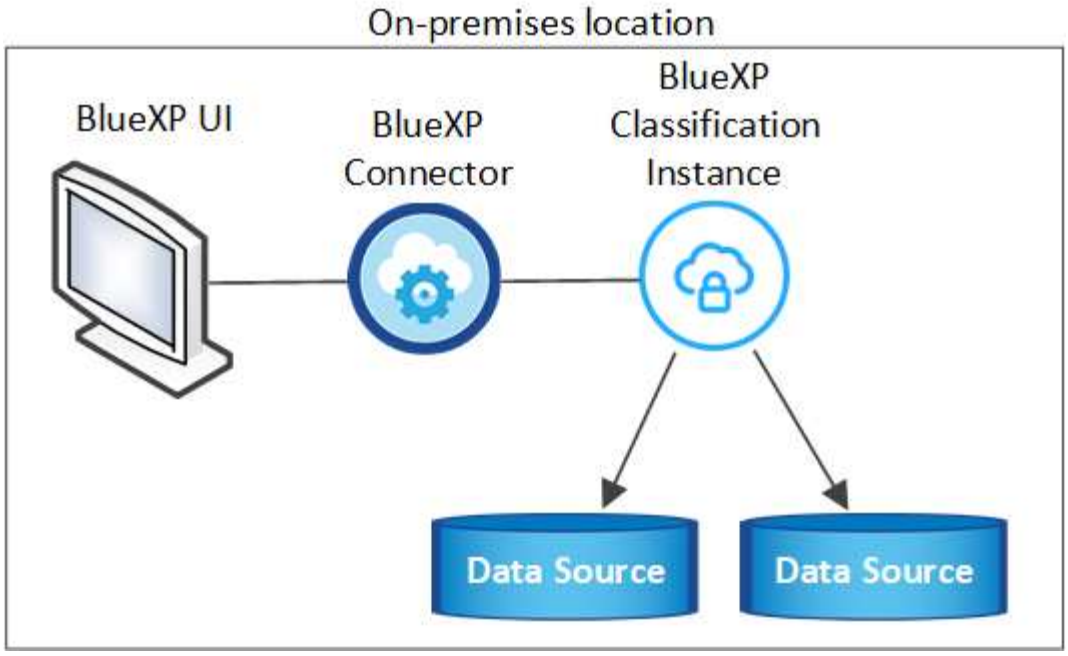
コネクタ、BlueXP分類、Active Directory、データソースの間の通信に必要なすべてのポートが開いていることを確認する必要があります。

接続タイプ	ポート	製品説明
コネクタ<> BlueXPの分類	8080（TCP）、6000（TCP）、443（TCP）、および80。9000	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。 • Linuxホストでファイアウォールが使用されている場合は、Ubuntuサーバ内の内部プロセスにポート9000が必要です。
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。

接続タイプ	ポート	製品説明
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。
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 ）
Linuxホストでファイアウォールを使用する場合	9000	Ubuntuサーバ内の内部プロセスに必要です。

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。



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`/opt/netapp/install_logs/`ます。"詳細はこちら"です。

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。
- 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では、からBlueXP 分類ソフトウェアをダウンロードし "NetAppサポートサイト"ます。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。

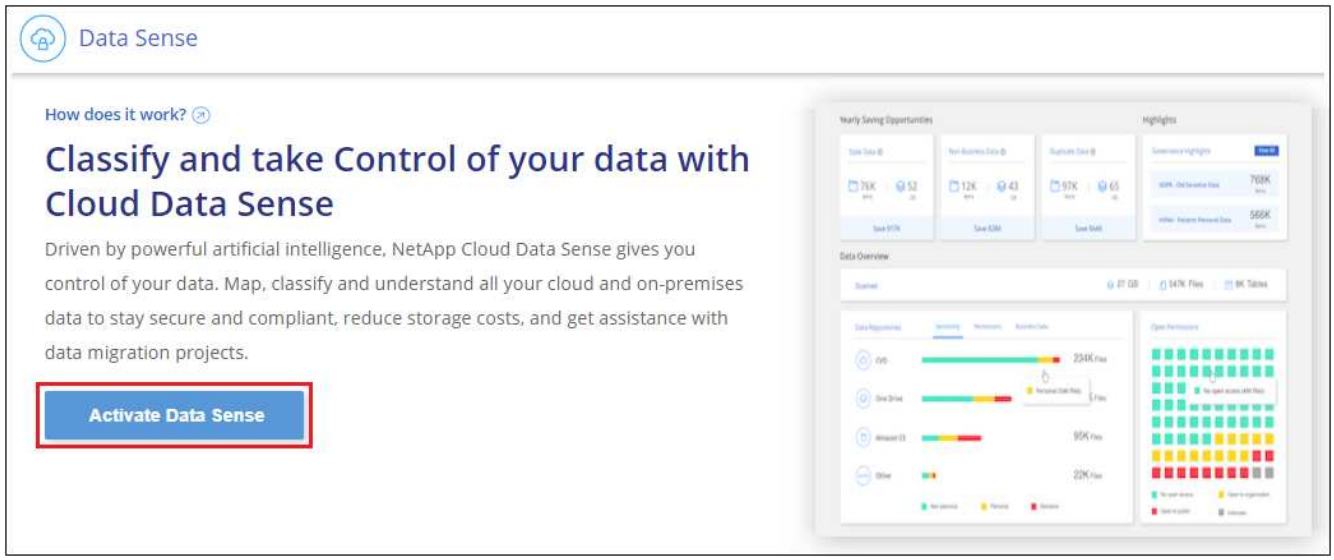
   ```
   tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
   ```

   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。

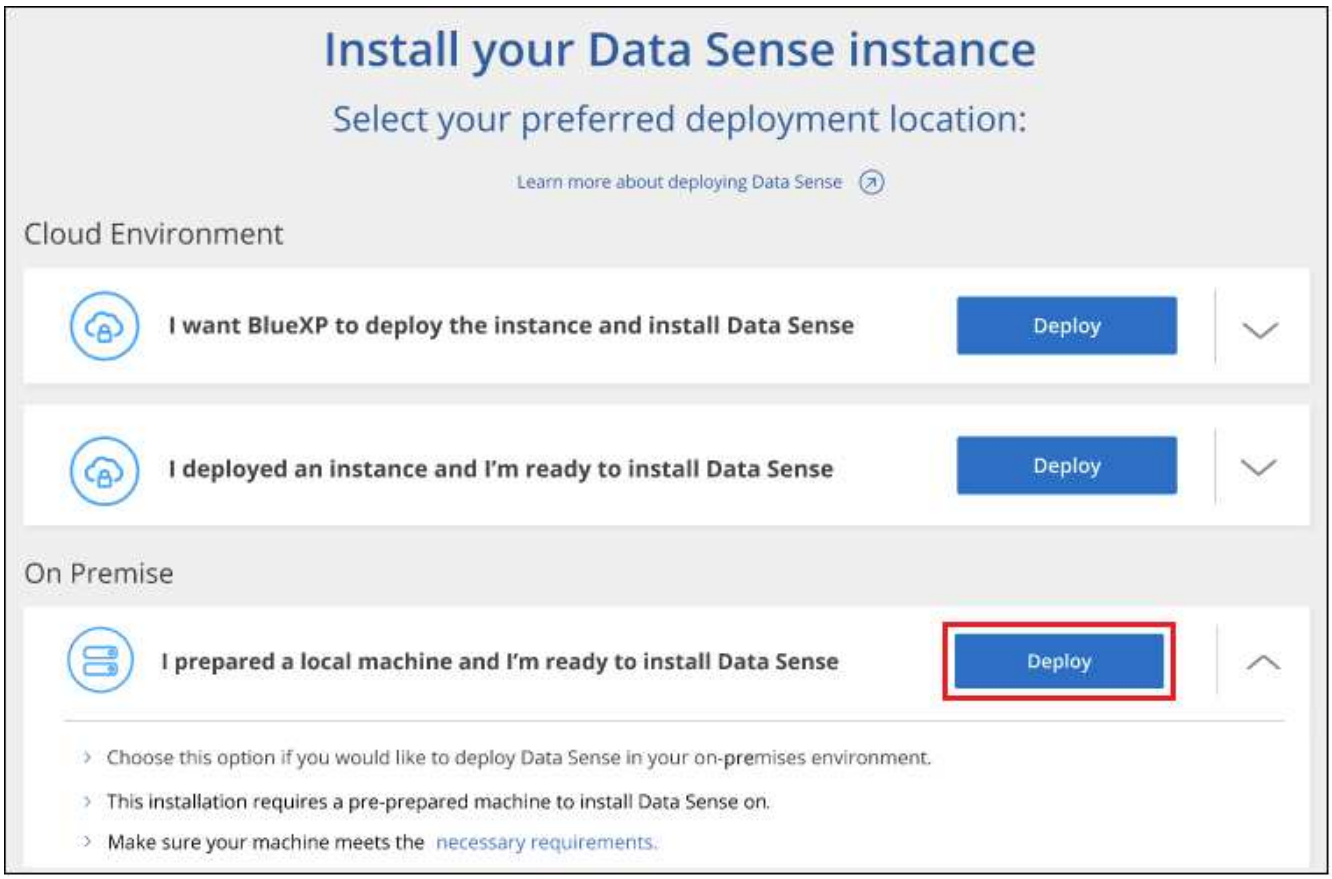
4. ホストマシンでインストールファイルを解凍します。次に例を示します。

```
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（例：）をコピー

し `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq --darksite`てテキストファイルに貼り付け、後で使用できるようにします。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 分かかる場合があります。

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

[Configuration]ページでは、スキャンするローカルとを"データベース"選択できます"オンプレミスの ONTAP クラスタ"。

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。

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お勧めします。 "コネクタのアップグレード手順を参照してください"です。
- 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では、からBlueXP 分類ソフトウェアをダウンロードし "NetAppサポートサイト"ます。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。

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。

ネットワーク内のLinuxホストまたはクラウド内のLinuxホストに配置できます "コネクタをオンプレミスにインストールします"。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、、 "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"を参照してください "AWS 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、これら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	SSDが1TiB、または-100GiBが/opt-895GiBが/var/lib/dockerで-5GiBが/tmpで利用可能

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
大きい	CPU×16	64GBのRAM	500GiB SSDオン/または-100GiBオン/opt-395GiBオン/var/lib/dockerまたはPodman/var/lib/containersまたはPodman/var/lib/containersの場合は-5GiBオン/tmp

- 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。
  - * Amazon Elastic Compute Cloud（Amazon EC2）インスタンスタイプ*：「m6i.4xlarge」を推奨します。"追加のAWSインスタンスタイプを参照してください"です。
  - * 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"です。
  - **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"です。
- * 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
    - Ubuntu 22.04（BlueXP分類バージョン1.23以降が必要）
    - Ubuntu 24.04（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、9.4
- * 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"です。
    - Podmanバージョン4以降。Podmanをインストールするには、と入力し (`sudo yum install

podman netavark -y`ます）。

- Pythonバージョン3.6以降。 "インストール手順を確認します"です。
  - * 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。
  - * firewalldの考慮事項*：を使用する場合は `firewalld`、BlueXP 分類をインストールする前に有効にすることをお勧めします。次のコマンドを実行して、BlueXP 分類と互換性があるようにを設定し`firewalld`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
```

+
設定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ります `firewalld`。

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://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	製品説明
コネクタ<> BlueXPの分類	8080（TCP）、443（TCP）、および80。9000	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。Linuxホストでファイアウォールが使用されている場合は、Ubuntuサーバ内の内部プロセスにポート9000が必要です。
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 classification Prerequisitesスクリプトをダウンロードします "NetApp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（またはその他の方法を使用 `scp`）。
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ディレクトリ内の `/opt/netapp/install_logs`という名前のファイルに書き込まれ `prerequisites-test-<timestamp>.log`ます。

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 分類によるAzure NetApp Filesボリュームのスキャン

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。


スキャンする**Azure NetApp Files**システムの検出

Azure NetApp Filesボリュームをスキャンする前に、を参照してください "構成を検出するには、BlueXPを設定する必要があります"。


BlueXP 分類インスタンスの導入

"BlueXPでBlueXP分類を導入します"インスタンスがまだデプロイされていない場合。


BlueXP 分類を有効にし、スキャンするボリュームを選択

コンプライアンス * をクリックし、 * 構成 * タブを選択して、特定の作業環境でボリュームのコンプライアンススキャンを有効にします。


ボリュームへのアクセスを確保

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 の場合 - ポート 111 および 2049
  - CIFS の場合 - ポート 139 および 445
- NFSボリュームエクスポートポリシーでは、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。


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"です。

BlueXP分類インスタンスを導入します

"BlueXP分類を導入します"インスタンスがまだデプロイされていない場合。

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。

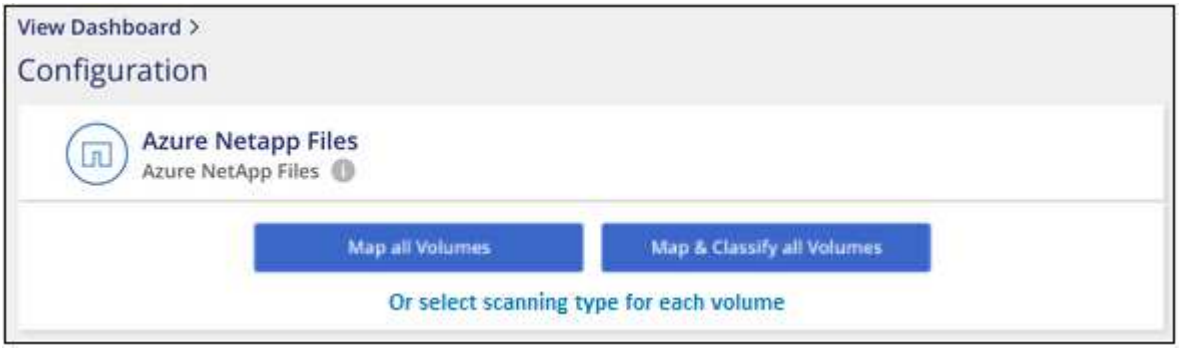
*注：*現時点では、Azure NetApp Files ボリュームのスキャン時にBlueXPの分類をオンプレミスに導入することはできません。

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。

作業環境での**BlueXP** 分類の有効化

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。

     詳細は、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 。

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"です。

BlueXP 分類でボリュームにアクセスできることを確認する

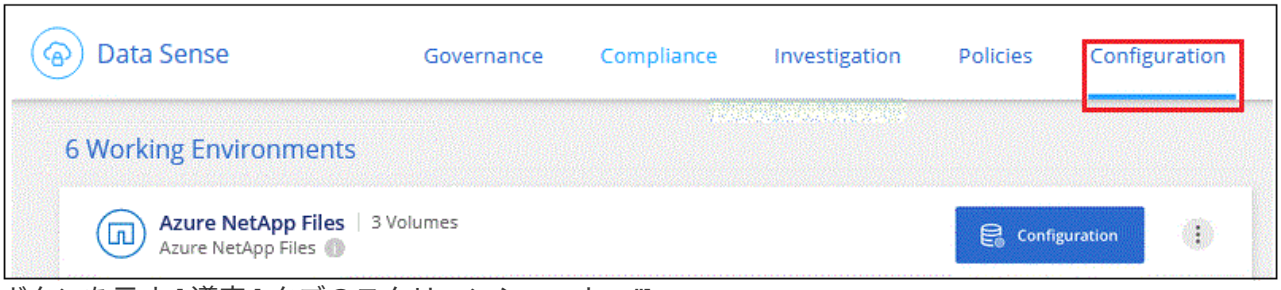
ネットワーク、セキュリティグループ、およびエクスポートポリシーをチェックして、BlueXPの分類でボリュームにアクセスできることを確認します。CIFSボリュームにアクセスできるように、BlueXPの分類にCIFSクレデンシャルを指定する必要があります。

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 の場合 - 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。"]

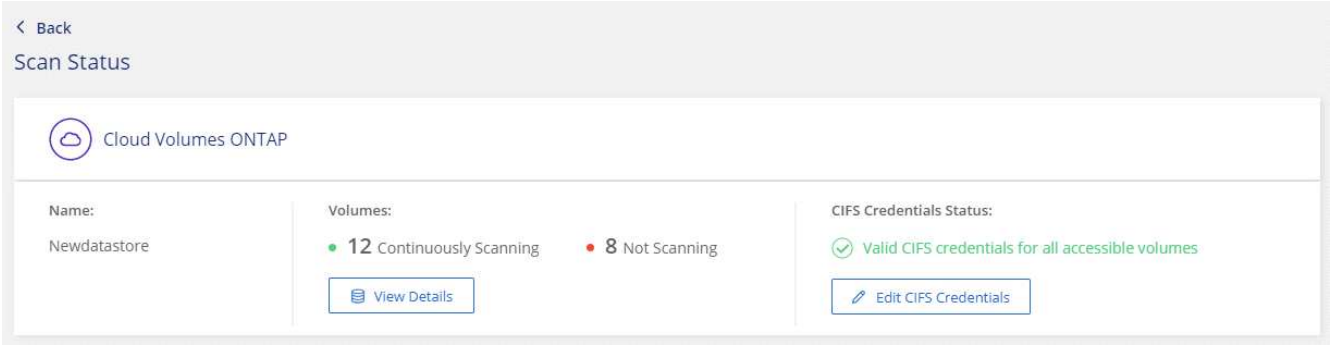
   b. 各作業環境について、*[CIFSクレデンシャルの編集]*をクリックし、BlueXPでシステムのCIFSボリュームにアクセスするために必要なユーザ名とパスワードを入力します。

      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。

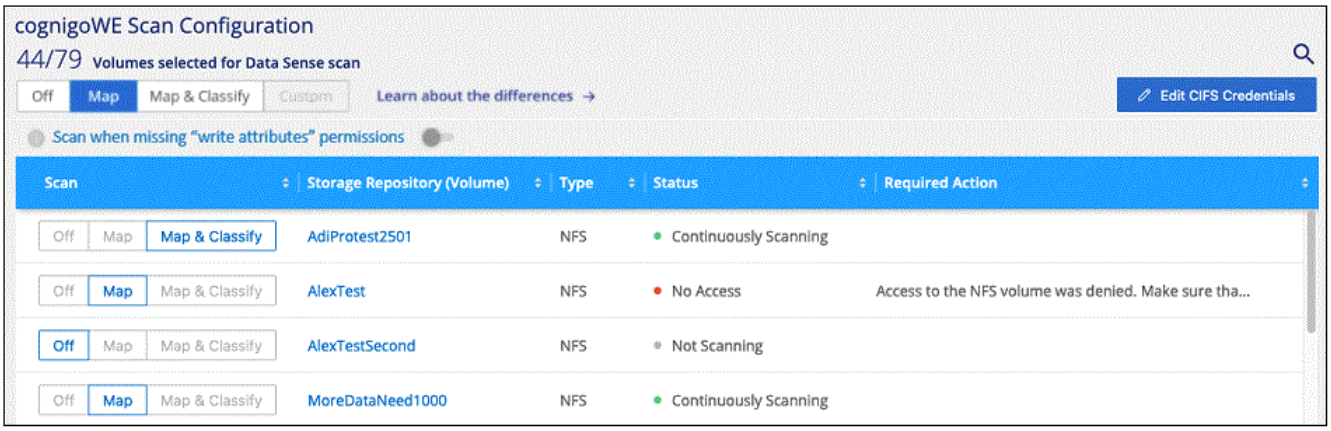
BlueXPの分類スキャンでファイルの「最終アクセス日時」が変更されないようにするには、CIFSではWrite Attributes権限、NFSではwrite権限を持つことを推奨します。可能であれば、すべてのファイルに対する権限を持つ組織内の親グループにActive Directory構成ユーザーを含めることをお勧めします。

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。



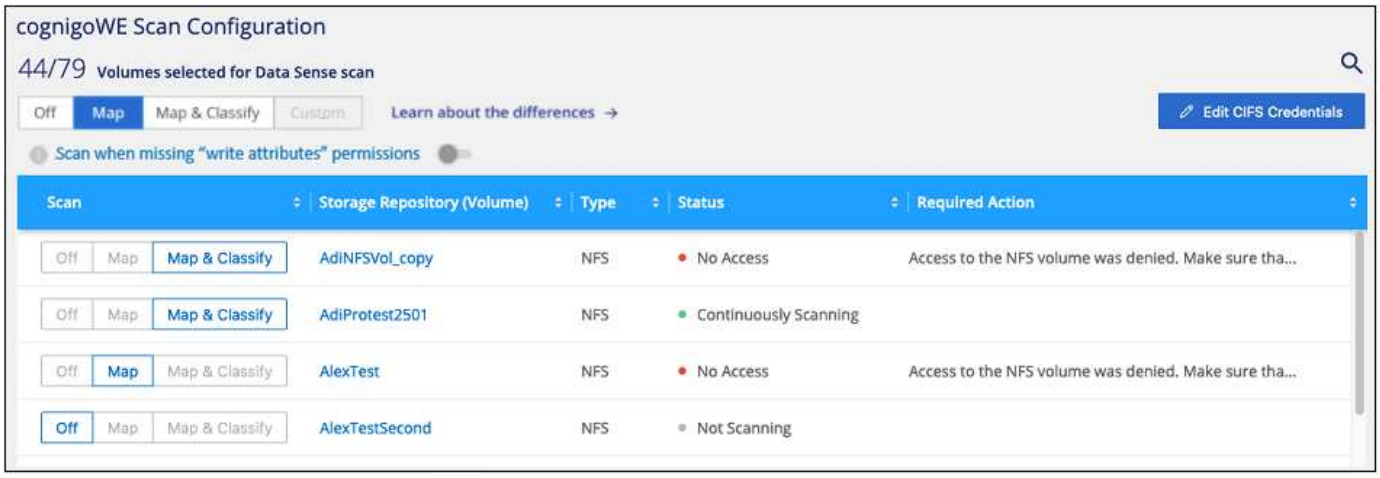
ページのスクリーンショット。4つのボリュームが表示されています。そのうちの1つはBlueXPで分類されたボリュームとボリュームの間のネットワーク接続が原因でスキャンされていません。"]

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"です。



宛先：	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。

BlueXP 分類を使用してAmazon FSx for ONTAPボリュームをスキャン

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。

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**FSx for ONTAP**ファイルシステムを確認します

FSx for ONTAPボリュームをスキャンする前に、を参照してください "ボリュームが設定された FSX 作業環境が必要です"。

2 **BlueXP** 分類インスタンスの導入

"BlueXPでBlueXP分類を導入します"インスタンスがまだデプロイされていない場合。

3 **BlueXP** 分類を有効にし、スキャンするボリュームを選択

[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保

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 の場合 - ポート 111 および 2049
  - CIFS の場合 - ポート 139 および 445
- NFSボリュームエクスポートポリシーでは、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**FSx for ONTAP**ファイルシステムを検出します

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"です。

BlueXP分類インスタンスを導入します

"BlueXP分類を導入します"インスタンスがまだデプロイされていない場合。

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。

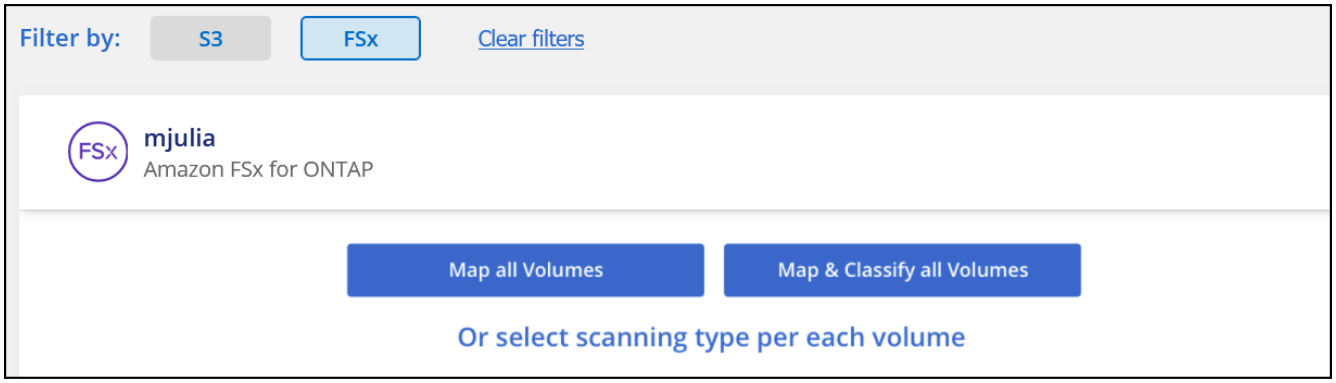
注： FSxボリュームのスキャン時にオンプレミス環境へのBlueXP分類の導入は現在サポートされていません。

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。

作業環境での**BlueXP** 分類の有効化

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。

     詳細については、ボリュームで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"です。

BlueXP 分類でボリュームにアクセスできることを確認する

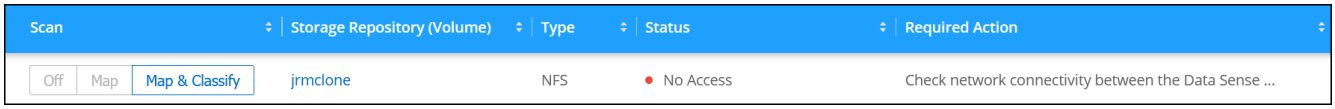
ネットワーク、セキュリティグループ、およびエクスポートポリシーをチェックして、BlueXPの分類でボリュームへのアクセスが許可されていることを確認します。

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 の場合 - 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。

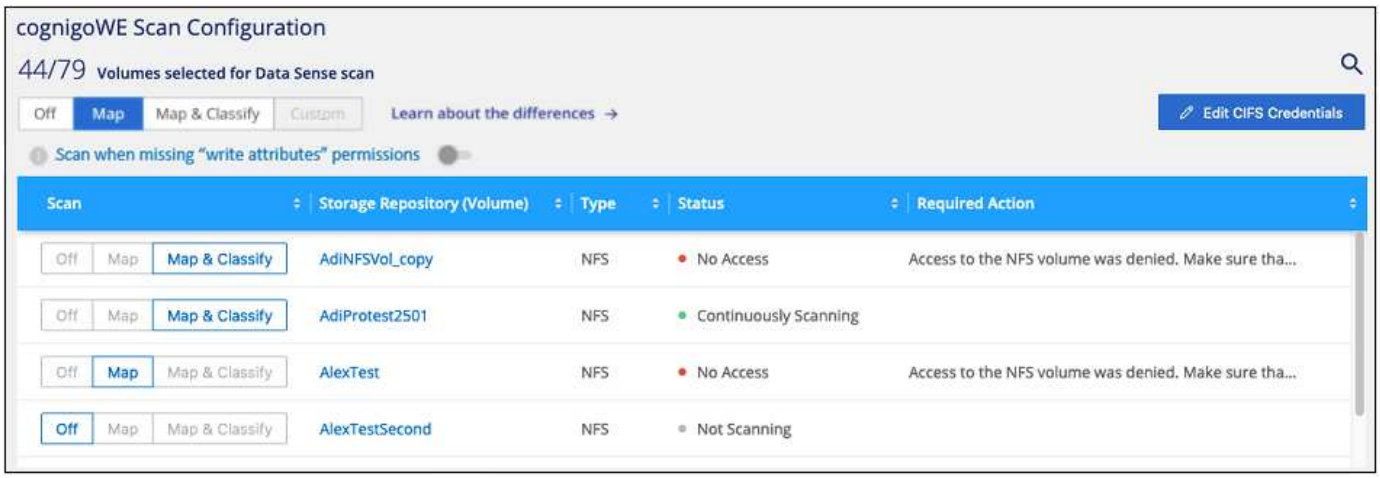
BlueXPの分類スキャンでファイルの「最終アクセス日時」が変更されないようにするには、CIFSではWrite Attributes権限、NFSではwrite権限を持つことを推奨します。可能であれば、すべてのファイルに対する権限を持つ組織内の親グループにActive Directory構成ユーザーを含めることをお勧めします。

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"です。



宛先：	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

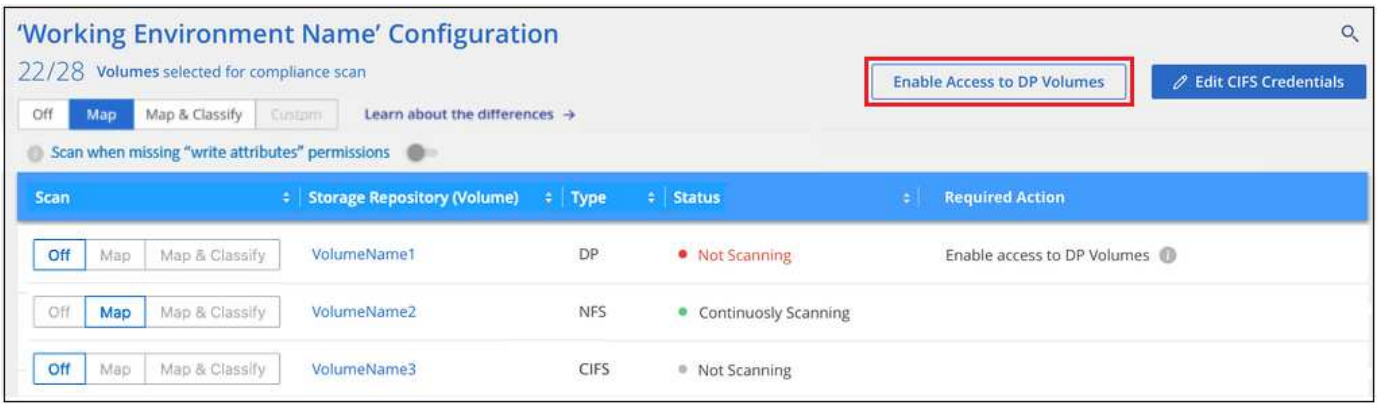
宛先：	手順：
すべてのボリュームでスキャンを無効にします	見出し領域で、 * Off * をクリックします

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する

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。

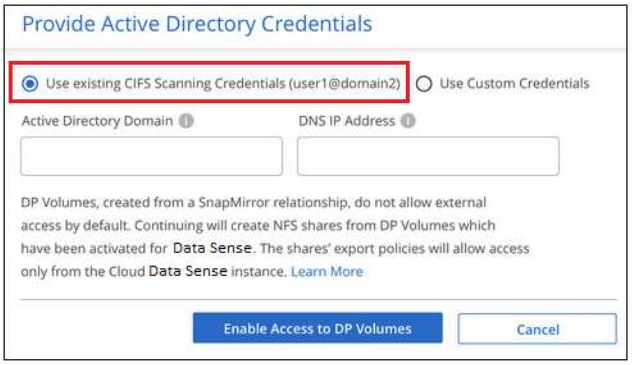
最初は、ボリュームリストでこれらのボリュームを *Type* DP * でスキャンしていないステータス * および必要なアクション _ * DP ボリュームへのアクセスを有効にします * 。

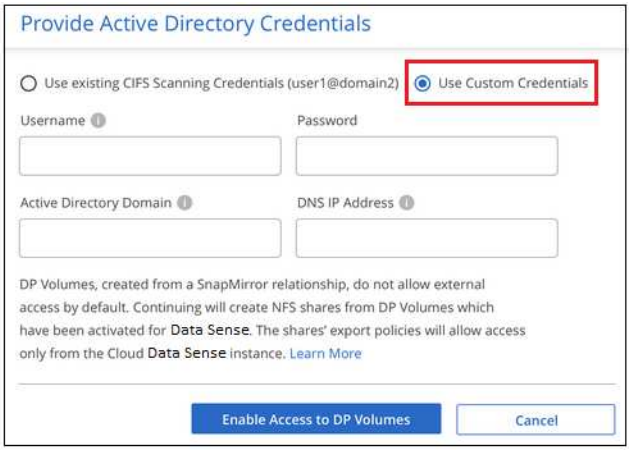


手順

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。

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 分類を使用してCloud Volumes ONTAPとオンプレミスのONTAPボリュームをスキャン

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する

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システムについては、 "BlueXPはONTAP クラスタを検出する必要があります"

2 BlueXP 分類インスタンスの導入

"BlueXP分類を導入します"インスタンスがまだデプロイされていない場合。

3 BlueXP 分類を有効にし、スキャンするボリュームを選択

[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保

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。
  - 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 "これらのクラスタはBlueXPで検出されます"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Cloud Volumes ONTAPシステムとオンプレミスのONTAPシステムをスキャンする場合は、またはを実行できます"BlueXPの分類機能をクラウドに導入します""インターネットにアクセスできるオンプレミスの場所"。

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

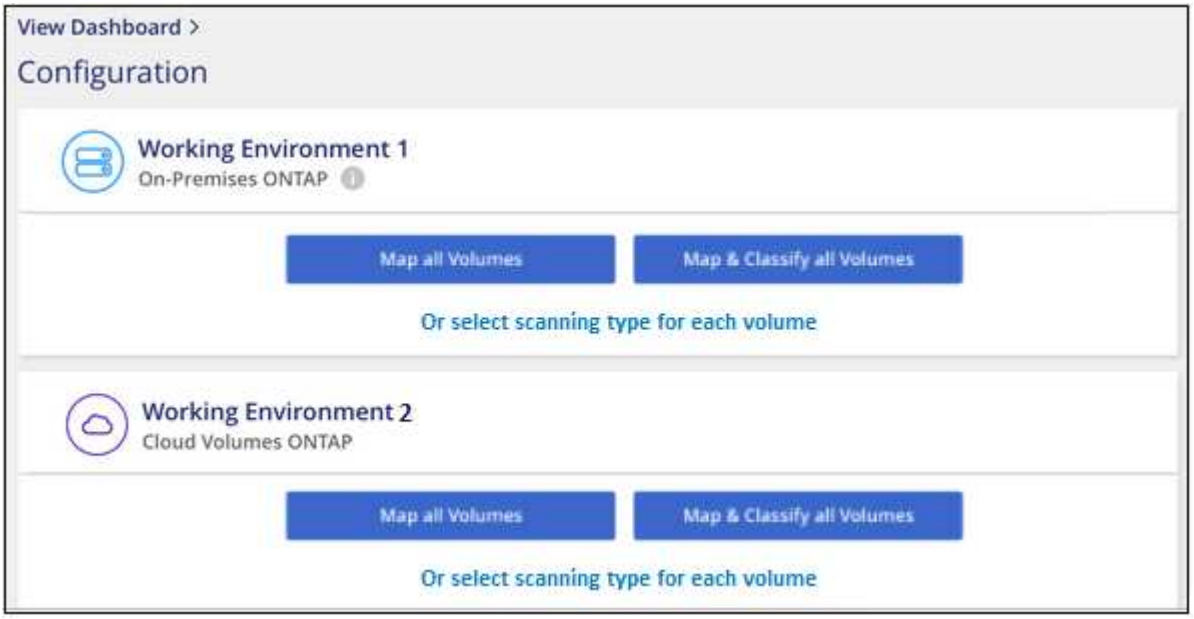
にBlueXPの分類を導入します"。また、BlueXPコネクタがオンプレミスの同じ場所に配置されている必要があります。

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。

作業環境での**BlueXP** 分類の有効化

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。

     詳細は、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 。

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"です。

BlueXP 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。

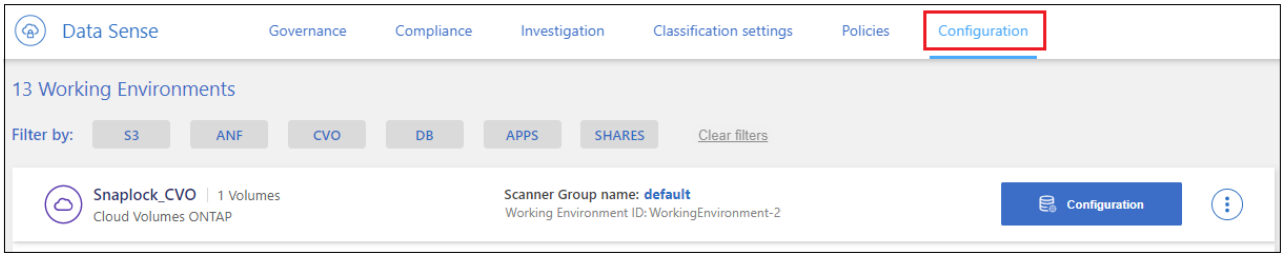
手順

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。
   - 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。"]

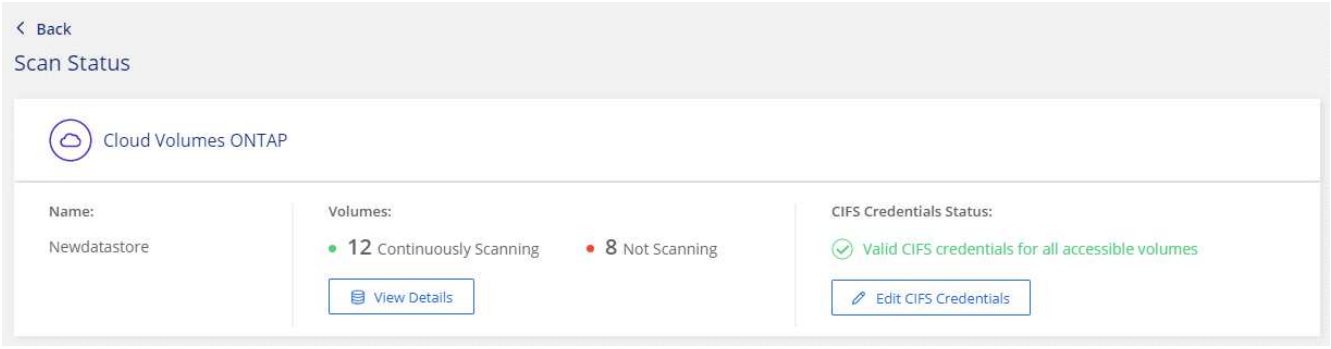
   b. 各作業環境について、*[CIFSクレデンシャルの編集]*をクリックし、BlueXPでシステムのCIFSボリュームにアクセスするために必要なユーザ名とパスワードを入力します。

   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。

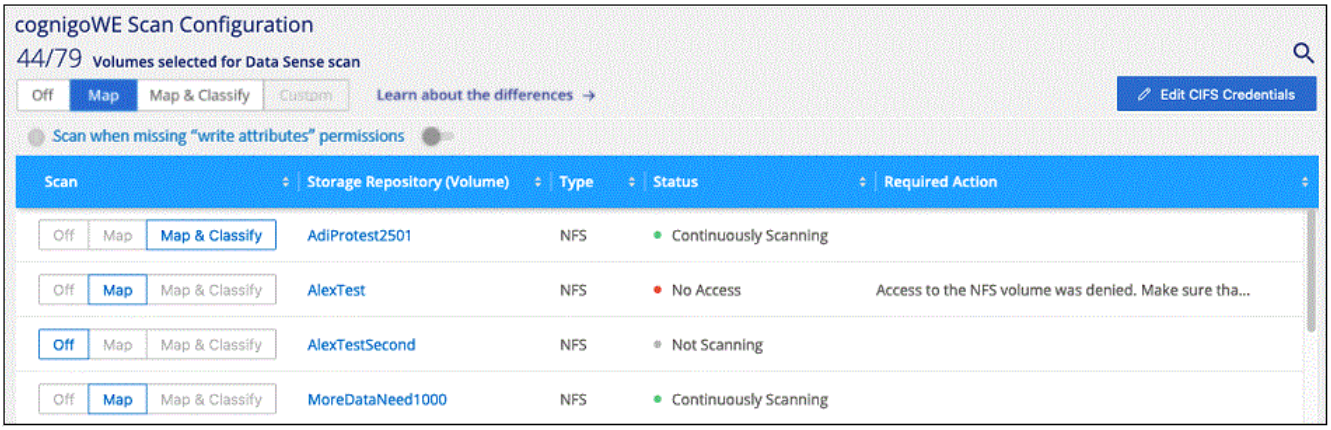
BlueXPの分類スキャンでファイルの「最終アクセス日時」が変更されないようにするには、CIFSではWrite Attributes権限、NFSではwrite権限を持つことを推奨します。可能であれば、すべてのファイルに対する権限を持つ組織内の親グループにActive Directory構成ユーザーを含めることをお勧めします。

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。



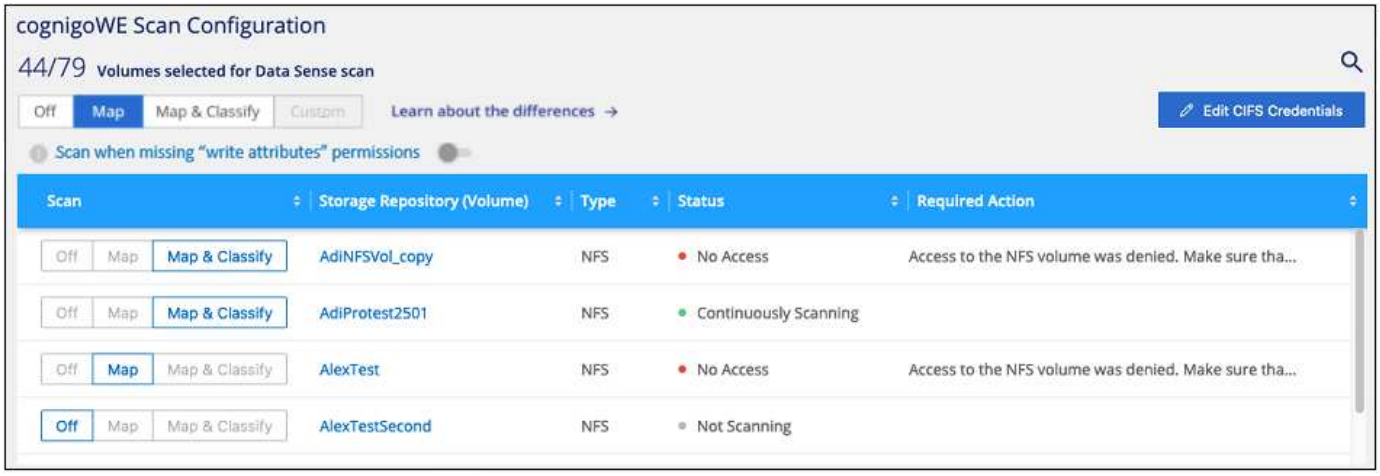
ページのスクリーンショット。4つのボリュームが表示されています。そのうちの1つはBlueXPで分類されたボリュームとボリュームの間のネットワーク接続が原因でスキャンされていません。"]

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"です。



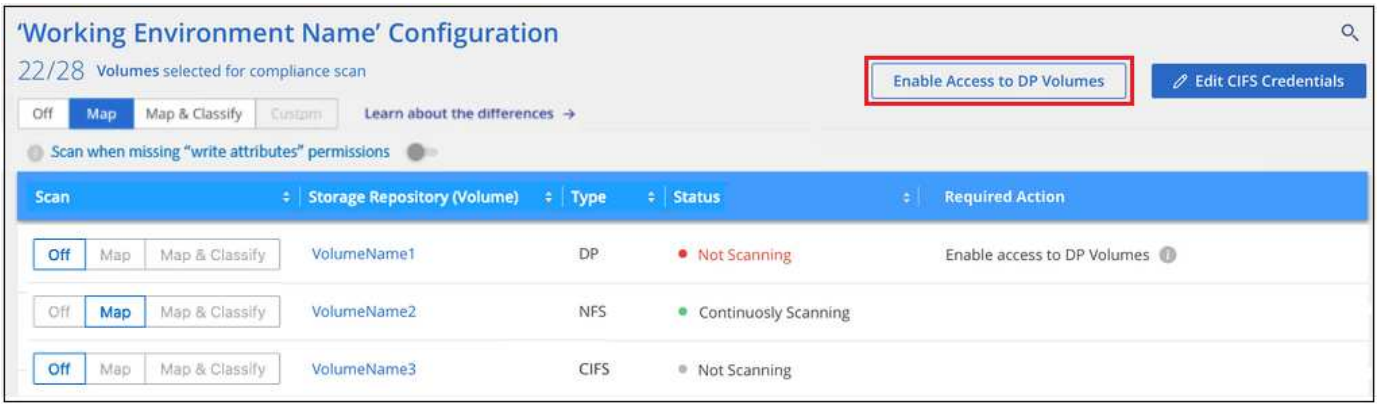
宛先：	手順：
ボリュームに対してマッピングのみのスキャンを有効にします	ボリューム領域で、 * マップ * をクリックします
ボリュームでフルスキャンを有効にします	ボリューム領域で、 * マップと分類 * をクリックします
ボリュームのスキャンを無効にします	ボリューム領域で、 * オフ * をクリックします
すべてのボリュームでマッピングのみのスキャンを有効にします	見出し領域で、 * マップ * をクリックします
すべてのボリュームでフルスキャンを有効にします	見出し領域で、 * マップと分類 * をクリックします
すべてのボリュームでスキャンを無効にします	見出し領域で、 * Off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

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。

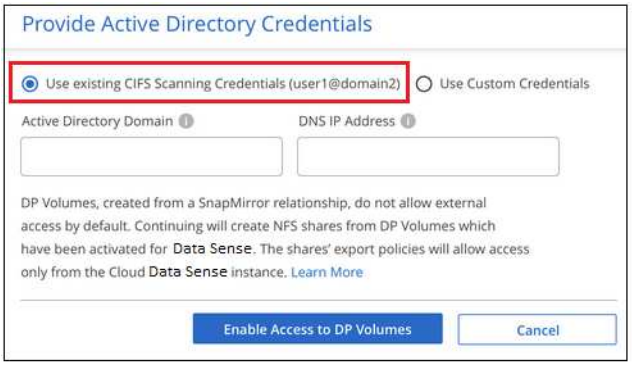
最初は、ボリュームリストでこれらのボリュームを *Type* * DP * でスキャンしていないステータス * および必要なアクション _ * DP ボリュームへのアクセスを有効にします * 。

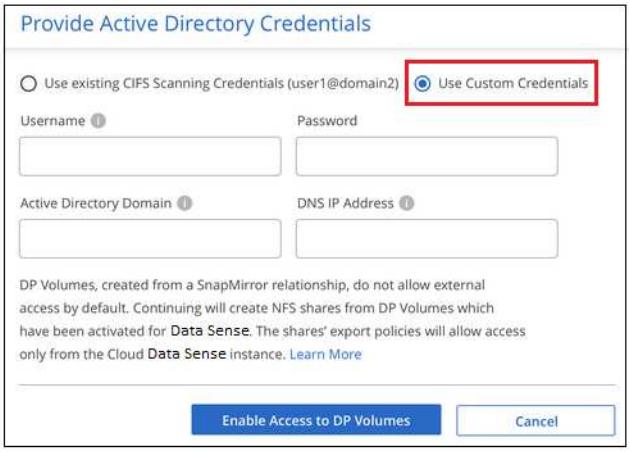


手順

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。

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 分類を使用した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。

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の確認

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 分類インスタンスの導入

"BlueXP分類を導入します"インスタンスがまだデプロイされていない場合。

3 データベースサーバの追加

アクセスするデータベースサーバを追加します。

4 スキーマの選択

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
- PostgreSQL

- SAP HANA
- 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、またはを使用できます"BlueXPの分類機能をクラウドに導入します""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"。

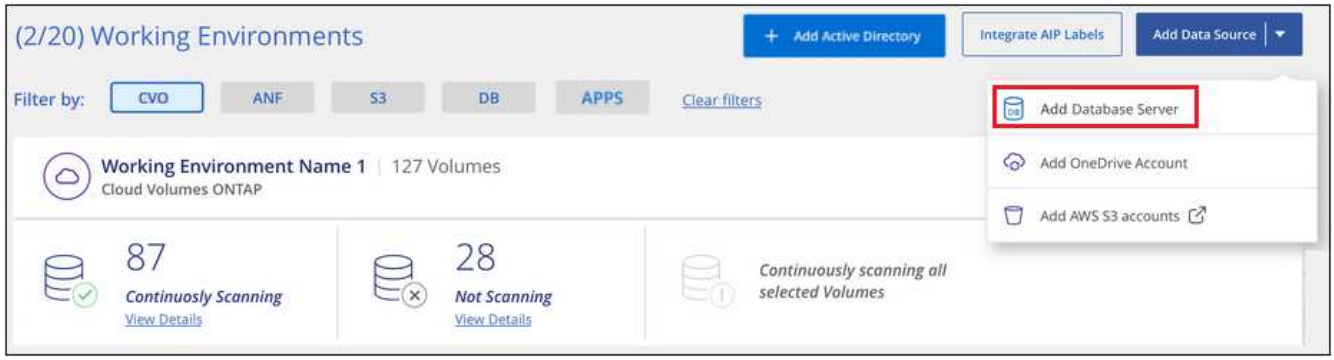
インターネットにアクセスできないダークサイトにインストールされているデータベーススキーマをスキャンする場合は、を実行する必要があります"インターネットアクセスのないオンプレミスと同じ場所にBlueXPの分類を導入します"。また、BlueXPコネクタがオンプレミスの同じ場所に配置されている必要があります。

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。

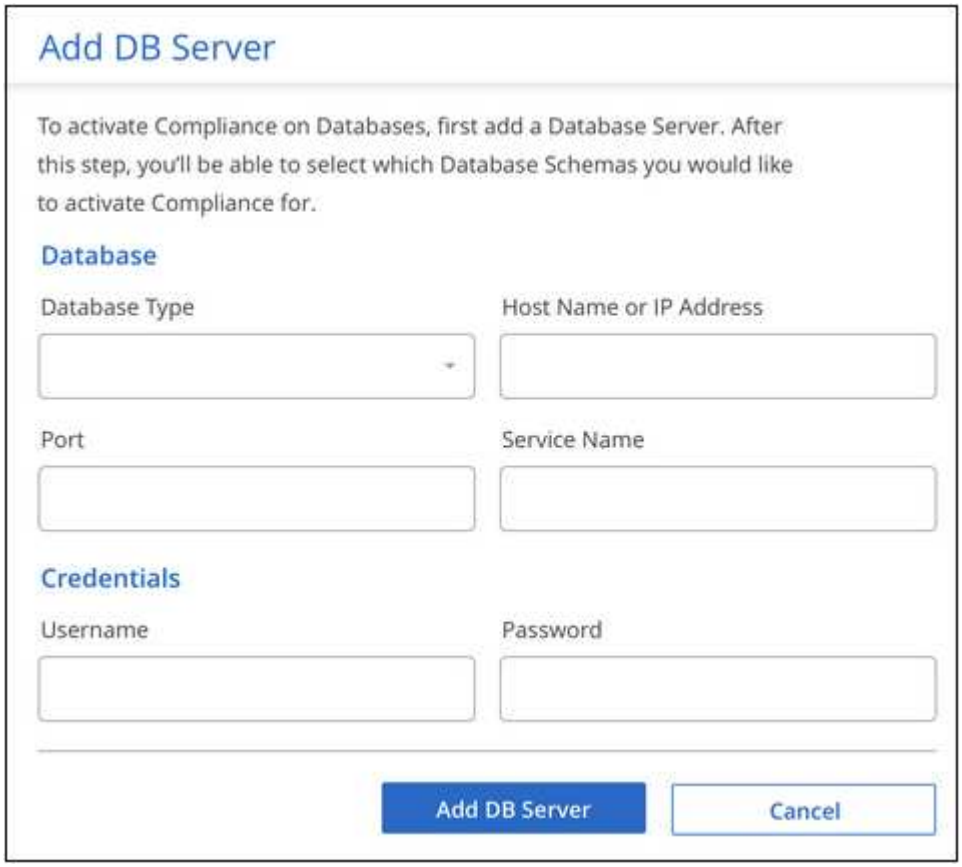
データベースサーバを追加します

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。

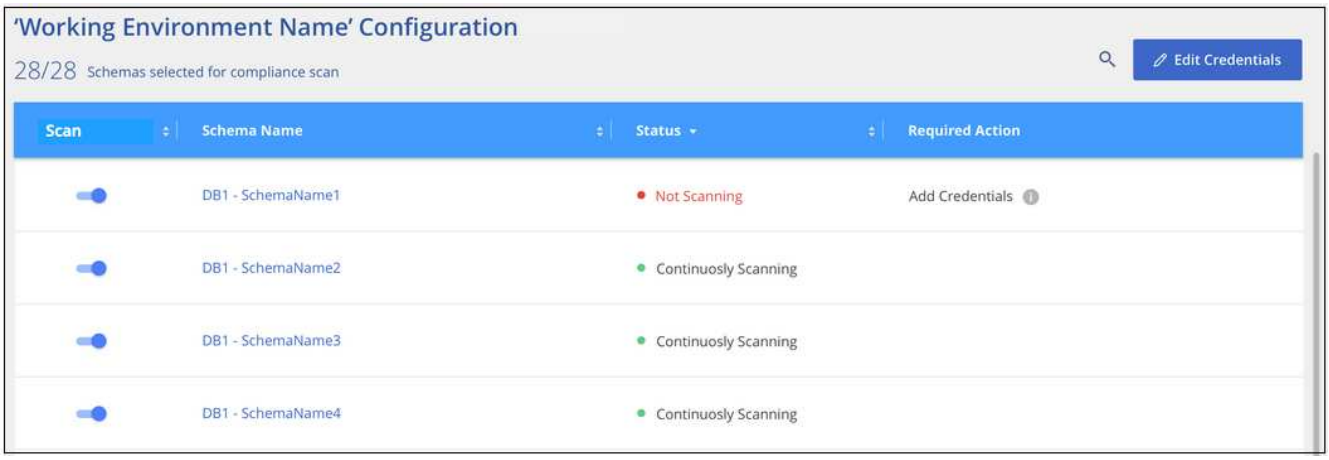
データベーススキーマでのコンプライアンススキャンの有効化と無効化

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。

BlueXP 分類によるファイル共有のスキャン

いくつかの手順を実行して、Google Cloud NetApp VolumeおよびNetApp 7-ModeシステムからNFSまたはCIFSファイル共有のスキャンを開始します。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。

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

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の確認

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 分類インスタンスの導入

"BlueXP分類を導入します"インスタンスがまだデプロイされていない場合。

3 ファイル共有を保持するグループを作成する

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 グループにファイル共有を追加します。

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。

- 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。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システムの一部の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 の場合 - 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をの形式で指定する必要があり `<host_name>:/<share_path>`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化されます。

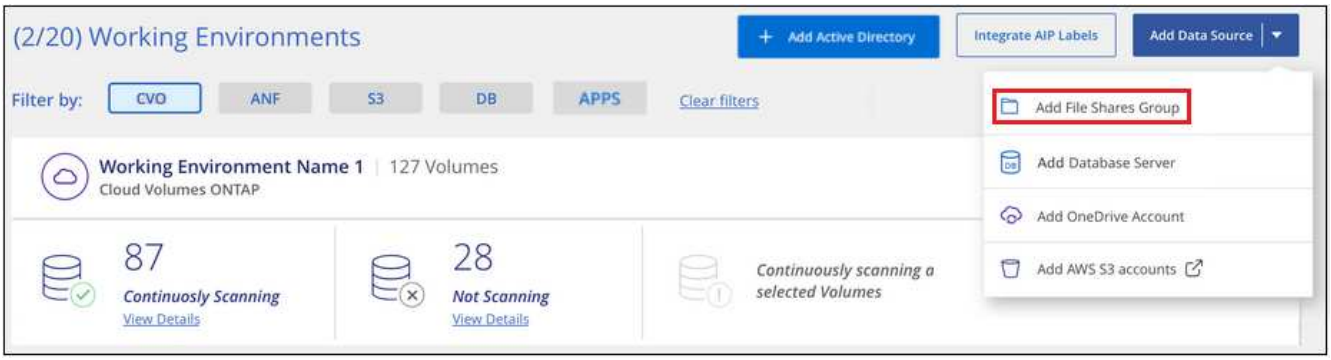
ファイル共有用のグループを作成する

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。

グループにファイル共有を追加する

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 `<host_name>:/<share_path>`ます。

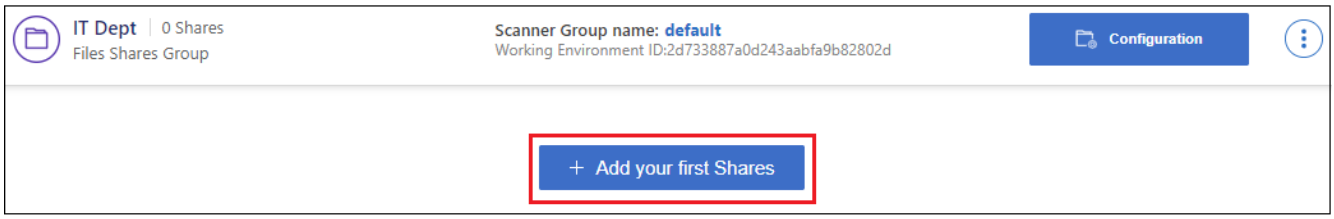
個々のファイル共有を追加することも、スキャンするファイル共有を 1 行で区切って指定することもできます。一度に最大 100 個の共有を追加できます。

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。



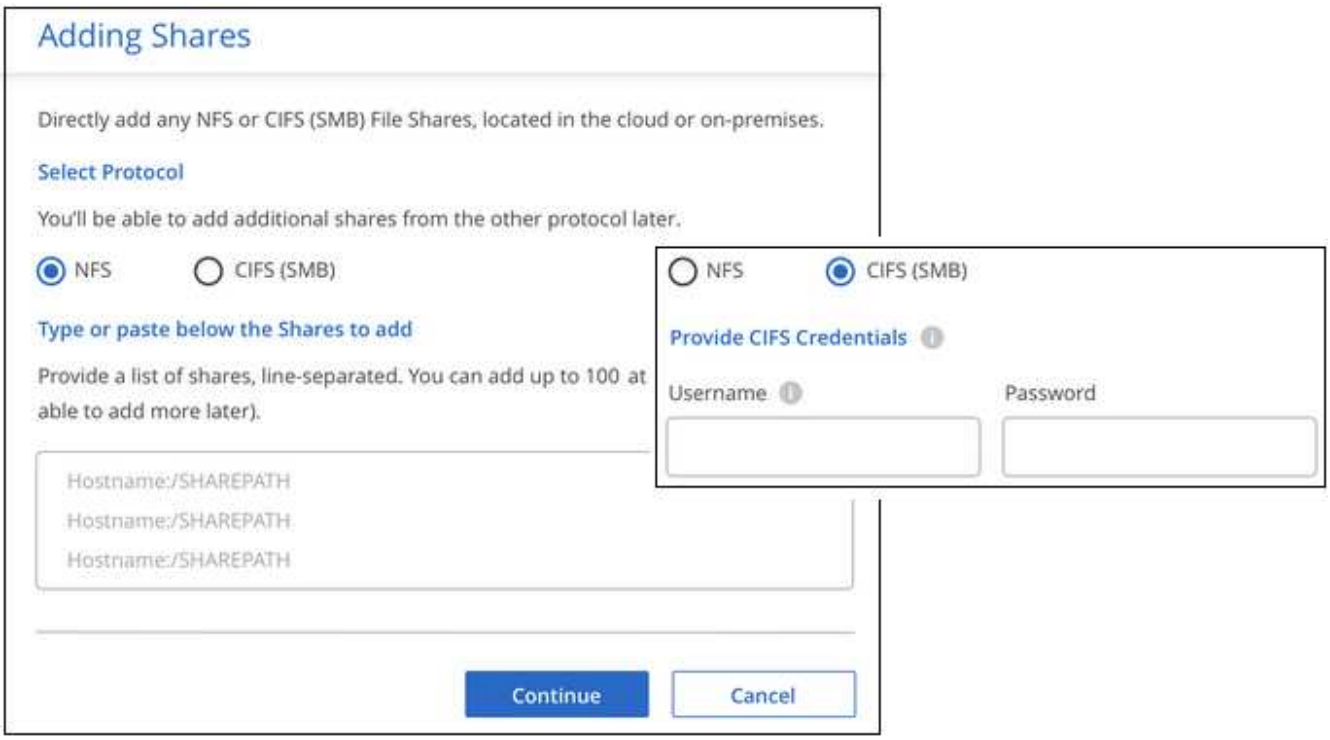
ボタンを示すスクリーンショット。"]

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。

宛先：	手順：
ファイル共有でマッピングのみのスキャンを有効にします	[* マップ *] をクリックします
ファイル共有でフルスキャンを有効にします	[マップと分類 *] をクリックします
ファイル共有でのスキャンを無効にします	[* Off *] をクリックします

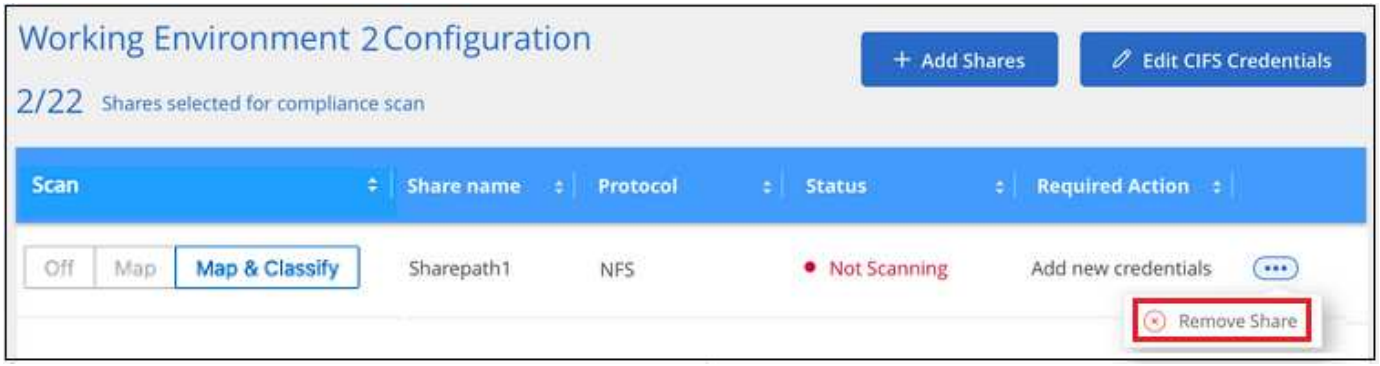
「属性の書き込み」権限がない場合にスキャンする*のページ上部のスイッチは、デフォルトでは無効になっています。つまり、BlueXPの分類にCIFSの属性への書き込み権限やNFSの書き込み権限がない場合、BlueXPの分類では「最終アクセス時間」を元のタイムスタンプに戻すことができないため、ファイルはスキャンされません。最終アクセス時間がリセットされても構わない場合は、スイッチをオンにすると、権限に関係なくすべてのファイルがスキャンされます。"詳細"です。

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。

コンプライアンススキャンからファイル共有を削除する

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。



BlueXP 分類を使用したStorageGRIDデータのスキャン

いくつかの手順を実行して、BlueXP 分類を使用してStorageGRID内のデータの直接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 **StorageGRID**の前提条件の確認

StorageGRIDサービスに接続するには、エンドポイントの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、StorageGRIDのアクセスキーとシークレットキーが必要です。

2 **BlueXP** 分類インスタンスの導入

"BlueXP分類を導入します"インスタンスがまだデプロイされていない場合。

3 **StorageGRID**サービスの追加

StorageGRID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

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。

StorageGRID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。

- 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、StorageGRID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StorageGRIDからデータをスキャンする場合は"BlueXPの分類機能をクラウドに導入します"、またはを使用できます"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StorageGRIDからデータ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。

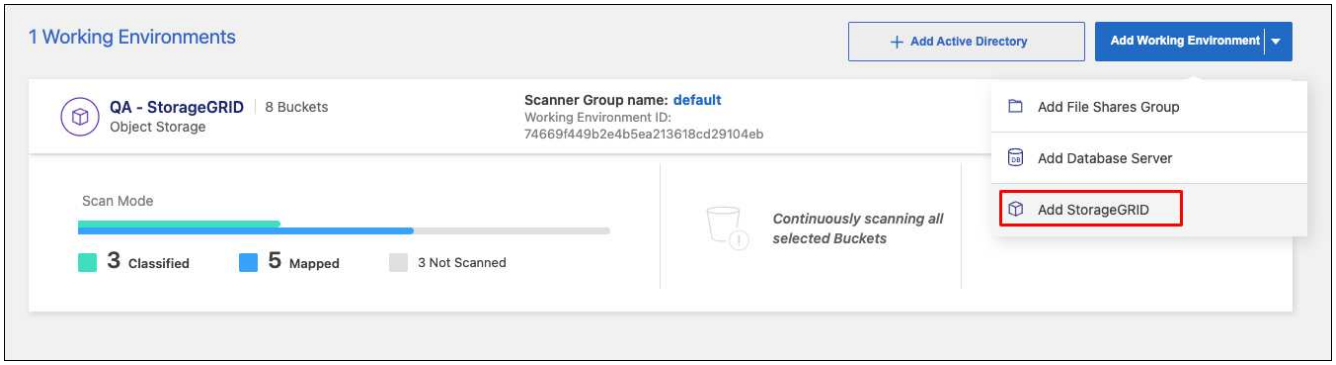
インスタンスがインターネットに接続されていれば、BlueXP 分類ソフトウェアへのアップグレードは自動化されます。

StorageGRIDサービスをBlueXP 分類に追加する

StorageGRIDサービスを追加します。

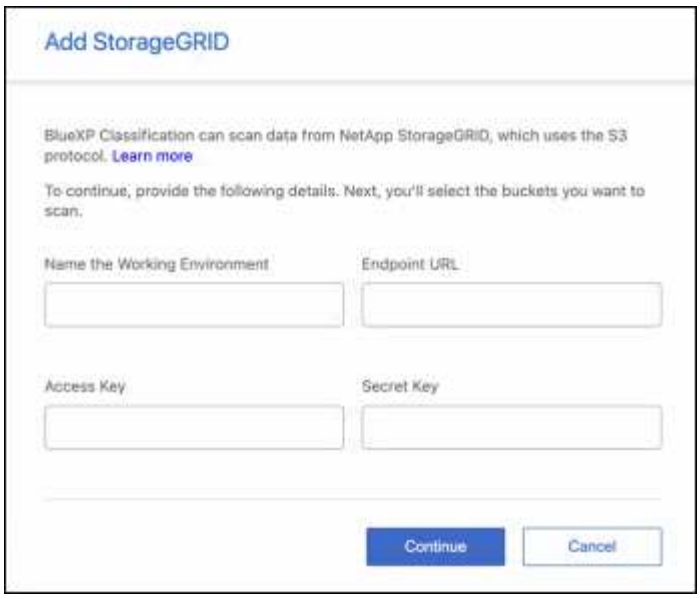
手順

1. [Working Environments Configuration]ページで、**[Add Data Source]**>*[Add StorageGRID *をクリックします。



ボタンをクリックできる[Scan Configuration（スキャン設定）]ページのスクリーンショット。"]

2. [Add StorageGRID Service]ダイアログで、StorageGRID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StorageGRIDサービスの名前が反映されている必要があります。
   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. BlueXP 分類がStorageGRID内のバケットにアクセスできるように、[Access Key]と[Secret Key]を入力します。



結果

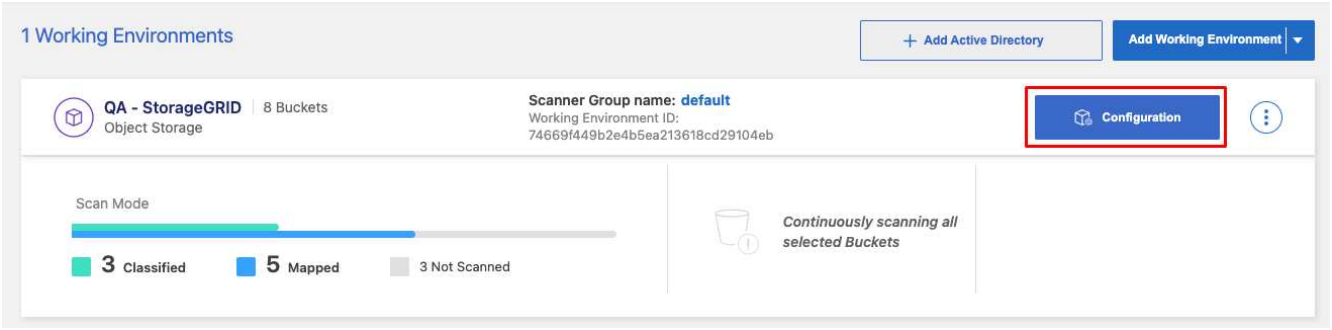
StorageGRIDが作業環境のリストに追加されます。

StorageGRIDバケットでコンプライアンススキャンを有効または無効にする

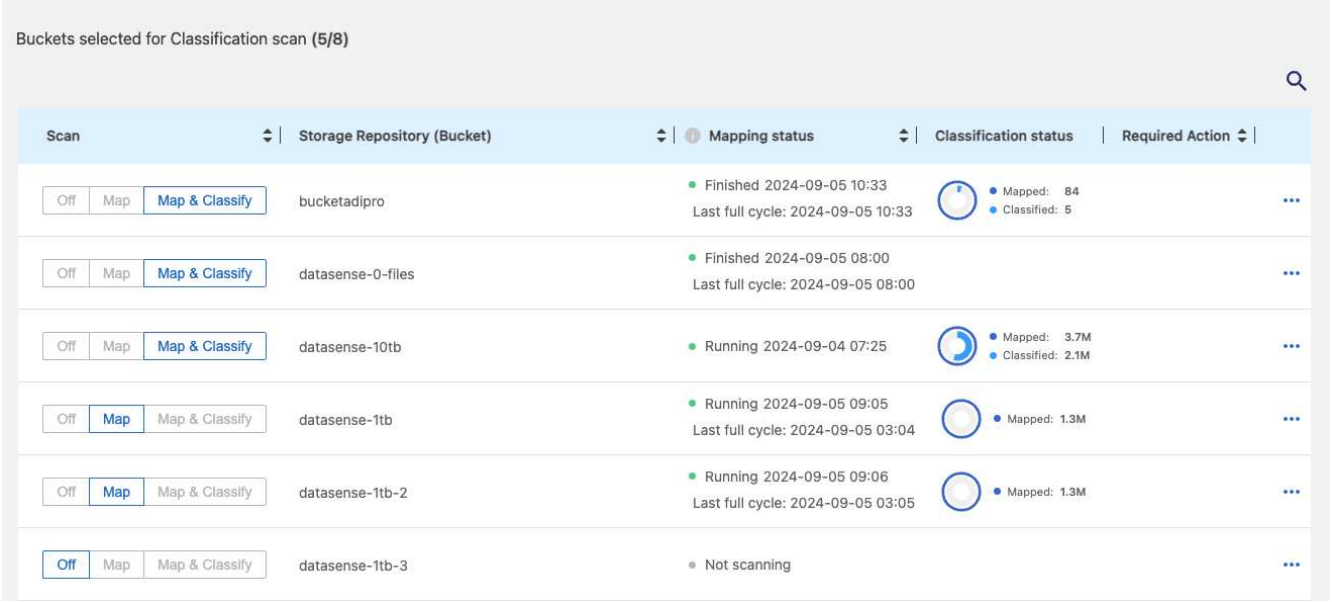
StorageGRIDでBlueXP 分類を有効にしたら、次の手順でスキャンするバケットを設定します。BlueXPの分類により、該当するバケットが検出され、作成した作業環境に表示されます。

手順

1. [Configuration]ページで、StorageGRID作業環境から*[Configuration]*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。



宛先：	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するActive Directoryは、ここで入力するグローバルActive Directory資格情報とは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。

- [File Owner]を使用すると、[Investigation]ペインでファイルのメタデータの結果を確認できます"フィルタ"。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。
- [すべての権限を表示]ボタンをクリックすると、各ファイルとディレクトリが表示されます"フルファイル権限"。
- では"ガバナンスダッシュボード"、[開く権限（Open Permissions）]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
- FSX for ONTAP の略
- OneDriveアカウントとSharePointアカウント（旧バージョン1.30以前の場合）

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/ファイル共有で、BlueXPの分類スキャンによってファイルの「最終アクセス日時」が変更されないようにするには、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

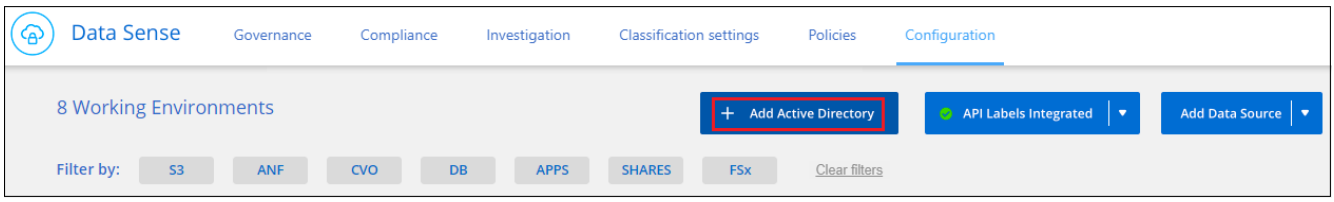
    または

  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	デスティネーション	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

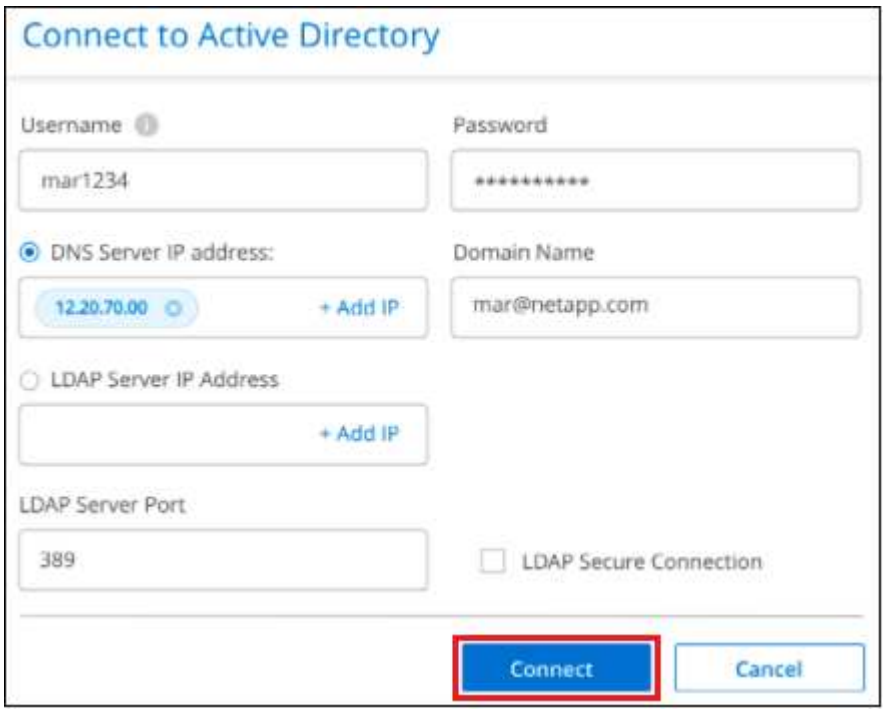
手順

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。

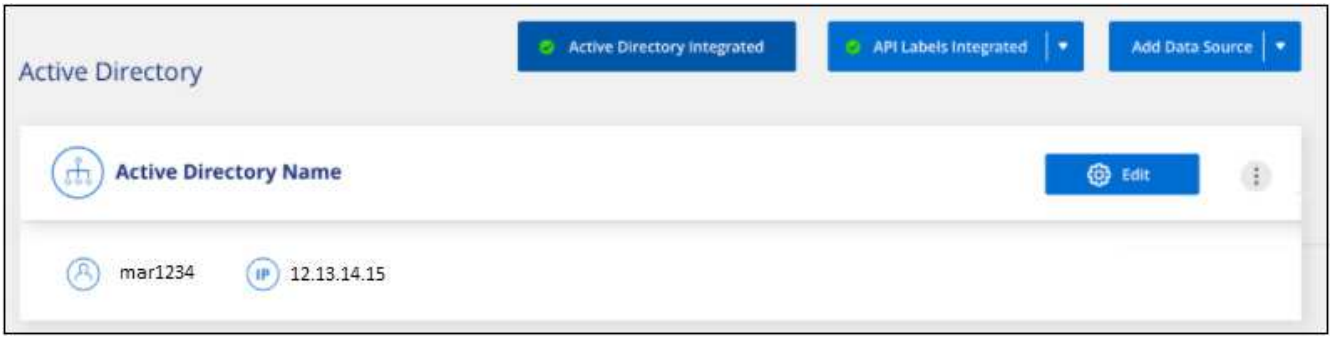


2. Active Directory への接続ダイアログで、 Active Directory の詳細を入力し、 * 接続 * をクリックします。

   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。

不要になった統合を削除するには、ボタンをクリックして* Active Directoryの削除*をクリックし ボタン"]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"です。

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"です。

"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"です。

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？

いいえ。BlueXPにはREST APIはありません。

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"です。

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"です。

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"です。

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"です。

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"です。

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"です。

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"です。

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"です。

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"です。

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。詳細については、およびを参照してください "BlueXP分類インスタンス" "BlueXP分類の導入" 。

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"です。

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"です。

> 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の分類の設定ページでは、個 々 の作業環境、データベース、またはファイル共有グループがスキャンされないように設定できます。

"詳細"です。

> 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、データの分析情報が得られます。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"です。

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"です。

ONTAPボリュームにある**Snapshot**はスキャンされますか？

いいえ。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、BlueXP 分類ではSnapshotはスキャンされません。

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。

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。

を参照して "サポートされている作業環境とデータソース"

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。

*注*この情報は、旧バージョン1.30以前のBlueXP 分類にのみ関連します。

- 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
- 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

を参照して "サポートされている作業環境とデータソース"

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, .DICOM, .DOC, .DOCX, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX,
Docs, Sheets, and 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 分類はメタデータのみをスキャンします。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：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、BlueXP 分類スキャンを実行します。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 分類は、個人情報(PII)や機密性の高い個人情報(SPII)など、多くの種類の個人データを識別することができます。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 ユーザには、権限に応じて表示できる作業環境の情報のみが表示されます。

また、特定のユーザーがBlueXP 分類設定を管理する機能を持たずにBlueXP 分類スキャン結果のみを表示できるようにする場合は、それらのユーザーに*分類ビューア*ロール（標準モードでBlueXP を使用している場合）または*コンプライアンスビューア*ロール（制限モードでBlueXP を使用している場合）を割り当てることができます。

"詳細"です。

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ています。これは、NetAppと非NetAppの関係者がそれを読み取ること

ができないことを意味します。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はBlueXPのコア機能であり、料金は発生しません。

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のCloud Volumes ONTAPまたはAmazon FSx for ONTAPで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 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、NetAppファイル共有、データベースのデータをスキャンする場合は、これらのクラウドのいずれかでコネクタを使用できます。

したがって、これらの多くの場所にデータがある場合は、を使用する必要があり "複数のコネクタ"ます。

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。ネットワーク内のLinuxホストまたはクラウド内のホストに配置できます "コネクタをオンプレミスに導入"。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。できます "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。"です。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？

"クラウドに導入"次の場合：

- 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。

"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"です。

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。システム要件およびインストールの詳細については、を参照してください"BlueXPの分類をオンプレミスに導入"。

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。あなたは完全に安全なサイトのためにできます"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にBlueXPを分類して導入します"。

著作権に関する情報

商標に関する情報