BlueXPのバックアップとリカバリに関するドキュメント

BlueXP backup and recovery

NetApp
April 18, 2024

目次

BlueXPのバックアップとリカバリに関するドキュメント

リリースノート

BlueXPのバックアップとリカバリの最新情報

BlueXPのバックアップとリカバリの新機能をご紹介します。

2024年4月4日

ランサムウェアスキャンを有効または無効にする機能

以前は、バックアップポリシーでランサムウェアの検出を有効にすると、最初のバックアップの作成時とバックアップのリストア時に自動的にスキャンが実行されていました。以前はすべてのSnapshotコピーがスキャンされており、スキャンを無効にすることはできませんでした。

このリリースでは、[Advanced Settings]ページのオプションを使用して、最新のSnapshotコピーに対するランサムウェアスキャンを有効または無効にできるようになりました。有効にすると、スキャンはデフォルトで毎週実行されます。

詳細については、次の情報を参照してください。

- "バックアップ設定の管理"
- "ONTAPボリュームのポリシーを管理します。"
- "オブジェクトへのバックアップポリシーの設定"

2024年3月12日

クラウドバックアップからオンプレミスの**ONTAP**ボリュームへの「迅速なリストア」が可能

クラウドストレージからオンプレミスのONTAPデスティネーションボリュームへのボリュームの_クイックリストア_を実行できるようになりました。以前は、Cloud Volumes ONTAPシステムにのみクイックリストアを実行できました。迅速なリストアは、ボリュームへのアクセスをできるだけ早く提供する必要があるディザスタリカバリ環境に最適です。迅速なリストアは、フルボリュームリストアよりもはるかに高速です。クラウドSnapshotからONTAPデスティネーションボリュームにメタデータをリストアします。ソースは、AWS S3、Azure Blob、Google Cloud Services、NetApp StorageGRIDのいずれかです。

オンプレミスのONTAPデスティネーションシステムでONTAPバージョン9.14.1以降が実行されている必要があります。

これは、検索とリストアのプロセスではなく、参照とリストアのプロセスを使用して実行できます。

詳細については、を参照してください "バックアップファイルからONTAPデータを復元します"。

Snapshotコピーとレプリケーションコピーからファイルとフォルダをリストアする機能

以前は、AWS、Azure、Google Cloud Servicesのバックアップコピーからのみファイルとフォルダをリストアできました。ローカルSnapshotコピーとレプリケーションコピーからファイルとフォルダをリストアできるようになりました。

この機能は、参照とリストアのプロセスではなく、検索とリストアのプロセスを使用して実行できます。

2024年2月1日

仮想マシンの**BlueXP**バックアップとリカバリの機能拡張

- 代替保存場所への仮想マシンのリストアのサポート
- データストアの保護解除のサポート

2023年12月15日

ローカル**Snapshot**コピーとレプリケーション**Snapshot**コピーで使用できるレポート

以前は、バックアップコピーに関するレポートのみを生成できました。ローカルSnapshotコピーとレプリケーションSnapshotコピーに関するレポートも作成できるようになりました。

これらのレポートでは、次の操作を実行できます。

- 重要なデータが組織のポリシーに従って保護されていることを確認します。
- ボリュームグループのバックアップがスムーズに実行されたことを確認します。
- 本番環境のデータに対する保護の証明を提供

を参照してください "データ保護の適用範囲に関するレポートを作成します"。

ボリュームで並べ替えとフィルタリングに使用できるカスタムタグ付け

ONTAP 9.13.1以降では、カスタムタグをボリュームに追加できるようになりました。これにより、複数の作業環境内および複数の作業環境間でボリュームをグループ化できます。これにより、BlueXPのバックアップとリカバリのUIページでボリュームをソートしたり、レポートでフィルタリングしたりできます。

30日間保持されるバックアップをカタログ化

以前は、Catalog.zipのバックアップは7日間保持されていました。現在、それらは30日間保持されます。

を参照してください "ダークサイトでのBlueXPのバックアップとリカバリデータのリストア"。

2023年10月23日

バックアップのアクティブ化中の**3-2-1**バックアップポリシーの作成

これまでは、Snapshot、レプリケーション、またはバックアップを開始する前にカスタムポリシーを作成する必要がありました。BlueXPのバックアップとリカバリのUIを使用して、バックアップのアクティブ化プロセスでポリシーを作成できるようになりました。

"ポリシーの詳細"。

ONTAPボリュームのオンデマンドのクイックリストアのサポート

BlueXPでは、クラウドストレージからCloud Volumes ONTAPシステムへボリュームの「クイックリストア」を実行できるようになりました。迅速なリストアは、ボリュームへのアクセスをできるだけ早く提供する必要があるディザスタリカバリ環境に最適です。クイックリストアでは、バックアップファイル全体をリストアするのではなく、バックアップファイルからボリュームにメタデータをリストアできます。

Cloud Volumes ONTAPデスティネーションシステムでONTAPバージョン9.13.0以降が実行されている必要があります。 "データのリストアに関する詳細情報"。

BlueXPのバックアップとリカバリのジョブモニタには、クイックリストアジョブの進捗状況も表示されます。

ジョブモニタでのスケジュール済みジョブのサポート

BlueXPのバックアップおよびリカバリジョブモニタでは、以前にスケジュールされたボリュームからオブジェクトストアへのバックアップおよびリストアジョブを監視しましたが、UIまたはAPIを使用してスケジュールされたローカルのSnapshot、レプリケーション、バックアップ、およびリストアジョブは監視しません。

BlueXPのバックアップとリカバリのジョブモニタに、ローカルのSnapshot、レプリケーション、オブジェクトストレージへのバックアップに関するスケジュール済みジョブが追加されました。

"更新されたジョブモニタの詳細"。

2023年10月13日

BlueXPのアプリケーション向けバックアップとリカバリの機能拡張（クラウドネイティブ）

- Microsoft SQL Serverデータベース
  - Amazon FSx for NetApp ONTAP上にあるMicrosoft SQL Serverデータベースのバックアップ、リストア、リカバリをサポート
  - すべての処理がREST APIでのみサポートされます。
- SAP HANAシステム
  - システムの更新時に、スクリプトではなくワークフローを使用してボリュームの自動マウントおよびアンマウントが実行されます。
  - 追加、削除、編集、削除、保守、 UIヲシヨウシタフラクインホストノアツフクレエト

アプリケーション向けの**BlueXP**のバックアップとリカバリの機能拡張（ハイブリッド）

- データロックとランサムウェア対策をサポート
- StorageGRIDからアーカイブ階層へのバックアップの移動をサポート
- MongoDB、MySQL、PostgreSQLの各アプリケーションデータをオンプレミスのONTAPシステムからAmazon Web Services、Microsoft Azure、Google Cloud Platform、StorageGRIDにバックアップできます。必要に応じてデータをリストアできます。

仮想マシンの**BlueXP**バックアップとリカバリの機能拡張

- コネクタプロキシ配置モデルのサポート

2023年9月11日

ONTAPデータの新しいポリシー管理

このリリースには、UI内で、ONTAPデータのオブジェクトストレージへのバックアップ用のカスタムSnapshotポリシー、レプリケーションポリシー、およびポリシーを作成する機能が含まれています。

"ポリシーの詳細"。

ONTAP S3オブジェクトストレージ内のボリュームからのファイルとフォルダのリストアのサポート

これまでは、ボリュームがONTAP S3オブジェクトストレージにバックアップされている場合、[Browse & Restore]機能を使用してファイルやフォルダをリストアすることはできませんでした。このリリースでは、この制限はなくなりました。

"データのリストアに関する詳細情報"。

最初に標準ストレージに書き込むのではなく、バックアップデータを即座にアーカイブ可能

これで、データを標準のクラウドストレージに書き込む代わりに、バックアップファイルをすぐにアーカイブストレージに送信できます。これは、クラウドバックアップからデータにアクセスする必要がほとんどないユーザや、テープバックアップ環境に取って代わるユーザに特に役立ちます。

SnapLockボリュームのバックアップとリストアのサポートの追加

バックアップとリカバリで、SnapLockコンプライアンスまたはSnapLockエンタープライズ保護モードを使用して設定されたFlexVolボリュームとFlexGroupボリュームの両方をバックアップできるようになりました。このサポートを実行するには、クラスタでONTAP 9.14以降が実行されている必要があります。ONTAPバージョン9.11.1以降では、SnapLock Enterpriseモードを使用したFlexVolボリュームのバックアップがサポートされています。以前のONTAPリリースでは、SnapLock保護ボリュームのバックアップはサポートされません。

"ONTAPデータの保護に関する詳細情報"。

2023年8月1日

- 重要なセキュリティ強化のため、パブリッククラウド環境内のバックアップとリカバリのリソースを管理するために、Connectorに追加のエンドポイントへのアウトバウンドインターネットアクセスが必要になりました。このエンドポイントがファイアウォールの[Allowed]リストに追加されていない場合は、UIに「Service Unavailable」または「Failed to determine service status」というエラーが表示されます。

  https://netapp-cloud-account.auth0.com

- Cloud Volumes ONTAPとBlueXPのバックアップとリカバリをバンドルできる「CVO Professional」パッケージを使用する場合、バックアップとリカバリのPAYGOサブスクリプションが必要になりました。これは以前は必要ありませんでした。対象となるCloud Volumes ONTAPシステムのバックアップとリカバリのサブスクリプション料金は発生しませんが、新しいボリュームでバックアップを設定する場合は必要です。

S3に設定された**ONTAP**システムでバケットへのボリュームのバックアップがサポートされるようになりました。

Simple Storage Service（S3）用に設定されたONTAPシステムを使用して、オブジェクトストレージにボリュームをバックアップできるようになりました。これは、オンプレミスのONTAPシステムとCloud Volumes ONTAPシステムの両方でサポートされます。この構成は、クラウド環境およびインターネットアクセスのないオンプレミス環境（「プライベート」モード展開）でサポートされます。

"詳細はこちら。"。

保護対象ボリュームの既存の**Snapshot**をバックアップファイルに含めることができるようになりました。

これまでは、（最新のSnapshotコピーから始めるのではなく）最初のバックアップファイルに読み書き可能ボリュームの既存のSnapshotコピーを含めることができました。読み取り専用ボリューム（データ保護ボリューム）の既存のSnapshotコピーがバックアップファイルに含まれていませんでした。「DP」ボリュームのバックアップファイルに古いSnapshotコピーを含めるように選択できるようになりました。

バックアップウィザードの最後に、これらの「既存のSnapshot」を選択するためのプロンプトが表示されます。

BlueXPのバックアップとリカバリでは、今後追加されるボリュームの自動バックアップはサポートされなくなります。

これまでは、バックアップウィザードのチェックボックスをオンにして、選択したバックアップポリシーをクラスタに追加するすべてのボリュームに適用できました。この機能は、ユーザーからのフィードバックとこの機能の使用不足に基づいて削除されました。クラスタに追加された新しいボリュームのバックアップは、手動で有効にする必要があります。

ジョブ監視ページが更新され、新機能が追加されました。

[Job Monitoring]ページに、3-2-1バックアップ戦略に関する詳細情報が表示されるようになりました。また、バックアップ戦略に関連する追加のアラート通知も提供されます。

[Backup lifecycle（バックアップライフサイクル）]タイプフィルタの名前が[Retention（保持）]に変更されました。このフィルタを使用して、バックアップのライフサイクルを追跡し、すべてのバックアップコピーの有効期限を特定します。「保持」ジョブタイプには、BlueXPのバックアップとリカバリで保護されているボリュームで開始されたSnapshot削除ジョブがすべてキャプチャされます。

"更新されたジョブモニタの詳細"。

2023年7月6日

BlueXPのバックアップとリカバリに、**Snapshot**コピーとレプリケートされたボリュームのスケジュール設定と作成が追加されました

BlueXPのバックアップとリカバリでは、3-2-1戦略を実装できるようになりました。この戦略では、ソースデータのコピーを2つのストレージシステムに3つ、クラウドに1つ配置できます。アクティベーションが完了すると、次のような状態になります。

- ソースシステム上のボリュームのSnapshotコピー
- 別のストレージシステムにレプリケートされたボリューム
- オブジェクトストレージ内のボリュームのバックアップ

"新しいフルスペクトルバックアップおよびリストア機能の詳細については、こちらをご覧ください"。

この新機能は、環境リカバリ処理にも対応しています。リストア処理は、Snapshotコピー、レプリケートされたボリューム、またはクラウド内のバックアップファイルから実行できます。これにより、リカバリのコストや速度など、リカバリ要件を満たすバックアップファイルを柔軟に選択できます。

この新機能とユーザインターフェイスは、ONTAP 9.8以降を実行するクラスタでのみサポートされます。クラスタに以前のバージョンのソフトウェアがインストールされている場合は、以前のバージョンのBlueXPバックアップとリカバリを引き続き使用できます。ただし、最新の機能を利用するには、サポートされているバー

ジョンのONTAPにアップグレードすることを推奨します。古いバージョンのソフトウェアを引き続き使用するには、次の手順に従います。

1. [* Volumes （ボリューム）] タブで、 [* Backup Settings （バックアップ設定）] を選択します。
2. [_Backup Settings]ページで、*[Display the previous BlueXP backup and recovery version]*のラジオボタンをクリックします。

   その後、以前のバージョンのソフトウェアを使用して古いクラスタを管理できます。

オブジェクトストレージにバックアップするためのストレージコンテナを作成できます

オブジェクトストレージにバックアップファイルを作成すると、デフォルトでは、バックアップおよびリカバリサービスによってオブジェクトストレージにバケットが作成されます。特定の名前を使用したり、特殊なプロパティを割り当てたりする場合は、バケットを自分で作成できます。独自のバケットを作成する場合は、アクティブ化ウィザードを開始する前にバケットを作成する必要があります。 "オブジェクトストレージバケットの作成方法について説明します"。

この機能は、StorageGRIDシステムにバックアップファイルを作成する場合は現在サポートされていません。

2023年7月4日

BlueXPのアプリケーション向けバックアップとリカバリの機能拡張（クラウドネイティブ）

- SAP HANAシステム
  - Azure NetApp Filesセカンダリ保護が有効な非データボリュームおよびグローバル非データボリュームの接続とコピーリストアをサポートします
- Oracleデータベース
  - Azure NetApp Files上のOracleデータベースを別の場所にリストアできます
  - Azure NetApp Files上のOracleデータベースのバックアップのOracle Recovery Manager（RMAN）カタログ化をサポートします
  - データベースホストをメンテナンスモードにしてメンテナンスタスクを実行できます

アプリケーション向けの**BlueXP**のバックアップとリカバリの機能拡張（ハイブリッド）

- 別の場所へのリストアをサポートします
- Oracleデータベースのバックアップをマウントできます
- GCPからアーカイブ層へのバックアップの移動をサポートします

BlueXPの仮想マシンのバックアップとリカバリの機能拡張（ハイブリッド）

- NFSおよびVMFSタイプのデータストアの保護をサポートします
- SnapCenter Plug-in for VMware vSphereホストの登録を解除できます
- 最新のデータストアとバックアップの更新と検出がサポートされます

2023年6月5日

FlexGroupボリュームは、**DataLock**とランサムウェア対策を使用してバックアップおよび保護できます

クラスタでONTAP 9.13.1以降が実行されている場合、FlexGroupボリュームのバックアップポリシーでDataLockとランサムウェア対策を使用できるようになりました。

新しいレポート機能

[Reports]タブでバックアップインベントリレポートを生成できるようになりました。このレポートには、特定のアカウント、作業環境、またはSVMインベントリのすべてのバックアップが含まれます。Data Protection Job Activityレポートを作成することもできます。このレポートには、Snapshot、バックアップ、クローニング、およびリストアの各処理に関する情報が表示され、サービスレベルアグリーメントの監視に役立ちます。を参照してください "データ保護の適用範囲に関するレポートを作成します"。

ジョブモニタの機能拡張

[Job Monitor]ページで、_backup lifecycle_をジョブタイプとして確認できるようになりました。これにより、バックアップライフサイクル全体を追跡できます。BlueXPタイムラインでは、すべての処理の詳細を確認することもできます。を参照してください "バックアップジョブとリストアジョブのステータスを監視します"。

一致しないポリシーラベルに関する追加の通知アラート

新しいバックアップアラート「Backup files were not created because Snapshot policy labels do not match」が追加されました。バックアップポリシーで定義された_label_inにSnapshotポリシーにmatching_label_inがない場合、バックアップファイルは作成されません。欠落しているラベルをボリュームSnapshotポリシーに追加するには、System ManagerまたはONTAP CLIを使用する必要があります。

"BlueXPのバックアップとリカバリから送信されるアラートをすべて確認します"。

ダークサイトの**BlueXP**の重要なバックアップファイルとリカバリファイルを自動でバックアップ

インターネットアクセスのないサイト（「プライベートモード」環境）でBlueXPのバックアップとリカバリを使用している場合、BlueXPのバックアップとリカバリの情報はローカルコネクタシステムにのみ格納されます。この新機能では、BlueXPの重要なバックアップ/リカバリデータが接続されたStorageGRIDシステムのバケットに自動的にバックアップされるため、必要に応じてこのデータを新しいコネクタにリストアできます。 "詳細はこちら。"

2023年5月8日

アーカイブストレージとロックされたバックアップでフォルダレベルのリストア処理がサポートされるようになりました

バックアップファイルにDataLockおよびRansomware保護が設定されている場合、またはバックアップファイルがアーカイブストレージにある場合、クラスタでONTAP 9.13.1以降が実行されている場合にフォルダレベルのリストア処理がサポートされるようになりました。

ボリュームを**Google Cloud**にバックアップするときは、リージョン間およびプロジェクト間でお客様が管理するキーがサポートされます

顧客管理暗号化キー（CMEK）のプロジェクトとは別のプロジェクトにあるバケットを選択できるようになりました。 "お客様が管理する独自の暗号化キーの設定の詳細については、こちらをご覧ください"。

バックアップファイルで**AWS China**リージョンがサポートされるようになりました

クラスタでONTAP 9.12.1以降が実行されている場合、AWS China Beijing（cn-north-1）リージョンとNingxia（cn-northwest-1）リージョンがバックアップファイルのデスティネーションとしてサポートされるようになりました。

BlueXPコネクタに割り当てるIAMポリシーでは、all_Resource_sectionsの下にあるAWSリソース名「arn」を「aws」から「aws-cn」に変更する必要があります（例：「arn：aws-cn：s3：：：netapp-backup-*」）。を参照してください "Amazon S3 への Cloud Volumes ONTAP データのバックアップ" および "オンプレミスのONTAP データをAmazon S3にバックアップします" を参照してください。

ジョブモニタの機能拡張

ONTAP 9.13.1以降を実行しているオンプレミスのONTAP システムで、システム開始ジョブ（進行中のバックアップ処理など）を*[ジョブ監視]*タブで確認できるようになりました。以前のバージョンのONTAP では、ユーザが開始したジョブのみが表示されます。

2023年4月14日

BlueXPのアプリケーション向けバックアップとリカバリの機能拡張（クラウドネイティブ）

- SAP HANAデータベース
  - スクリプトベースのシステム更新をサポートします
  - Azure NetApp Files バックアップが設定されている場合は、Single-File-Snapshot-Restoreがサポートされます
  - プラグインのアップグレードをサポートします
- Oracleデータベース
  - root以外のsudoユーザ設定が簡易化され、プラグインの導入が強化されました
  - プラグインのアップグレードをサポートします
  - Azure NetApp Files 上のOracleデータベースの自動検出とポリシーベースの保護をサポートします
  - きめ細かなリカバリにより、Oracleデータベースを元の場所にリストアできます

アプリケーション向けの**BlueXP**のバックアップとリカバリの機能拡張（ハイブリッド）

- アプリケーション（ハイブリッド）向けのBlueXPのバックアップとリカバリは、SaaSコントロールプレーンから実行されます
- ハイブリッドREST APIが変更され、クラウドネイティブAPIと連携するようになりました。
- Eメール通知をサポートします

2023年4月4日

「制限付き」モードで**Cloud Volumes ONTAP** システムからクラウドにデータをバックアップする機能

これで、AWS、Azure、GCPの商用リージョンにインストールされているCloud Volumes ONTAP システムのデータを「制限モード」でバックアップできるようになりました。これを行うには、まず「制限された」商業地域にコネクタをインストールする必要があります。 "BlueXPの導入モードの詳細については、こちらをご覧

ください"。を参照してください "Amazon S3 への Cloud Volumes ONTAP データのバックアップ" および "Cloud Volumes ONTAP データをAzure Blobにバックアップしています"。

APIを使用して、オンプレミスの**ONTAP** ボリュームを**ONTAP S3**にバックアップする機能

APIの新機能を使用して、BlueXPのバックアップとリカバリを使用してボリュームSnapshotをONTAP S3にバックアップできます。この機能は、現時点ではオンプレミスのONTAP システムでのみ使用できます。詳細な手順については、ブログを参照してください "デスティネーションとしてのONTAP S3との統合"。

Azureストレージアカウントのゾーン冗長性の側面を**LRS**から**ZRS**に変更する機能

Cloud Volumes ONTAP システムからAzureストレージへのバックアップを作成する場合、BlueXPのバックアップとリカバリでは、コスト最適化のためにローカル冗長性（LRS）を使用してBlobコンテナがデフォルトでプロビジョニングされます。異なるゾーン間でデータを複製する場合は、この設定をZone redundancy（ZRS）に変更できます。Microsoftの手順を参照してください "ストレージアカウントの複製方法の変更"。

ジョブモニタの機能拡張

- ONTAP 9.13.0以降を実行しているCloud Volumes ONTAP システムでは、BlueXPのバックアップ/リカバリのUIとAPIでユーザが開始したバックアップ処理とリストア処理と、システムが開始したジョブ（進行中のバックアップ処理など）が[ジョブ監視]タブで利用できるようになりました。以前のバージョンのONTAP では、ユーザが開始したジョブのみが表示されます。
- すべてのジョブをレポートするためのCSVファイルをダウンロードできるほか、単一のジョブのJSONファイルをダウンロードして詳細を確認できるようになりました。 "詳細はこちら。"。
- 「Scheduled job failure」と「Restore job completes but with warnings」という2つの新しいバックアップジョブアラートが追加されました。 "BlueXPのバックアップとリカバリから送信されるアラートをすべて確認します"。

2023年3月9日

フォルダレベルのリストア処理に、すべてのサブフォルダとファイルが含まれるようになりました

以前は、フォルダをリストアしたときに、そのフォルダのファイルのみがリストアされました。サブフォルダやサブフォルダ内のファイルはリストアされませんでした。ONTAP 9.13.0以降を使用している場合は、選択したフォルダ内のすべてのサブフォルダとファイルが復元されます。これにより、トップレベルフォルダに複数のフォルダがネストされている場合に、時間とコストを大幅に節約できます。

アウトバウンド接続が制限されているサイトの**Cloud Volumes ONTAP**システムからデータをバックアップする機能

AWSおよびAzureの商用リージョンにインストールされているCloud Volumes ONTAP システムから、Amazon S3またはAzure Blobにデータをバックアップできるようになりました。これには、商用地域のLinuxホストに「制限モード」でコネクタをインストールし、そこにCloud Volumes ONTAPシステムを展開する必要があります。を参照してください "Amazon S3 への Cloud Volumes ONTAP データのバックアップ" および "Cloud Volumes ONTAP データをAzure Blobにバックアップしています"。

ジョブモニタに複数の機能拡張が追加されました

- [Job Monitoring]ページには高度なフィルタリング機能が追加され、時間、ワークロード（ボリューム、アプリケーション、仮想マシン、またはKubernetes）ごとにバックアップジョブとリストアジョブを検索できるようになりました。 ジョブタイプ、ステータス、作業環境、およびStorage VM。任意のリソース

（「application_3」など）を検索するフリーテキストを入力することもできます。 "詳細フィルタの使用方法を参照してください"。

- ONTAP 9.13.0以降を実行しているCloud Volumes ONTAP システムでは、BlueXPのバックアップ/リカバリのUIとAPIでユーザが開始したバックアップ処理とリストア処理と、システムが開始したジョブ（進行中のバックアップ処理など）が[ジョブ監視]タブで利用できるようになりました。以前のバージョンのCloud Volumes ONTAP システムおよびオンプレミスのONTAP システムでは、現時点ではユーザが開始したジョブのみが表示されます。

2023年2月6日

古いバックアップファイルを**StorageGRID** システムから**Azure**アーカイブストレージに移動する機能

これで、古いバックアップファイルをStorageGRID システムからAzureのアーカイブストレージに階層化できるようになりました。これにより、StorageGRID システムのスペースを解放し、古いバックアップファイルには低コストのストレージクラスを使用することでコストを削減できます。

この機能は、オンプレミスクラスタがONTAP 9.12.1以降を使用し、StorageGRID システムが11.4以降を使用している場合に使用できます。 "詳細はこちらをご覧ください"。

DataLockと**Ransomware**による保護は、**Azure Blob**でのバックアップファイルに対して設定できます

DataLockとRansomware Protectionは、Azure Blobに保存されたバックアップファイルでサポートされるようになりました。Cloud Volumes ONTAP またはオンプレミスONTAP システムでONTAP 9.12.1以降を実行している場合、バックアップファイルをロックしてスキャンし、ランサムウェアの可能性を検出できるようになりました。 "DataLockとランサムウェア防御を使用してバックアップを保護する方法については、こちらをご覧ください"。

FlexGroup ボリュームのバックアップとリストアの機能拡張

- FlexGroup ボリュームのリストア時に複数のアグリゲートを選択できるようになりました。前回のリリースでは、アグリゲートを1つしか選択できませんでした。
- FlexGroup ボリュームリストアがCloud Volumes ONTAP システムでサポートされるようになりました。前回のリリースでは、オンプレミスのONTAP システムにのみリストアできました。

Cloud Volumes ONTAP システムでは、古いバックアップを**Google**アーカイブストレージに移動できます

バックアップファイルは、最初にGoogle Standardストレージクラスで作成されます。BlueXPのバックアップとリカバリ機能を使用して、古いバックアップをGoogleアーカイブストレージに階層化し、コストをさらに最適化できるようになりました。前回のリリースでは、オンプレミスのONTAP クラスタでのみこの機能がサポートされていました。現在Google Cloudに導入されているCloud Volumes ONTAP システムがサポートされています。

ボリュームリストア処理で、ボリュームデータをリストアする**SVM**を選択できるようになりました

次に、ONTAP クラスタ内の別のStorage VMにボリュームデータをリストアします。これまでは、Storage VMを選択できませんでした。

MetroCluster 構成でのボリュームのサポートが強化されました

ONTAP 9.12.1 GA以降を使用している場合、MetroCluster 構成でプライマリシステムに接続しているときにバックアップがサポートされるようになりました。バックアップ構成全体がセカンダリシステムに転送される

ため、スイッチオーバー後もクラウドへのバックアップが自動的に続行されます。

"詳細については、「バックアップの制限」を参照してください"。

2023年1月9日

StorageGRID システムから**AWS S3**アーカイブストレージに古いバックアップファイルを移動する機能

これにより、StorageGRID システムの古いバックアップファイルをAWS S3のアーカイブストレージに階層化できるようになりました。これにより、StorageGRID システムのスペースを解放し、古いバックアップファイルには低コストのストレージクラスを使用することでコストを削減できます。AWS S3 GlacierまたはS3 Glacier Deep Archiveストレージにバックアップを階層化することもできます。

この機能は、オンプレミスクラスタでONTAP 9.12.1以降を使用し、StorageGRID システムで11.3以上を使用している場合に使用できます。 "詳細はこちらをご覧ください"。

Google Cloudのデータ暗号化に、お客様が管理する独自のキーを選択できます

ONTAP システムからGoogle Cloud Storageにデータをバックアップする際に、Googleが管理するデフォルトの暗号化キーを使用する代わりに、アクティベーションウィザードで、お客様が管理する独自のキーを選択してデータを暗号化できるようになりました。まずGoogleでお客様が管理する暗号化キーを設定し、BlueXPのバックアップとリカバリをアクティブ化する際に詳細を入力するだけです。

「ストレージ管理者」ロールは、サービスアカウントが**Google Cloud Storage**でバックアップを作成するために必要なくなりました

以前のリリースでは、BlueXPのバックアップとリカバリでGoogle Cloud Storageバケットにアクセスするためのサービスアカウントに「Storage Admin」ロールが必要でした。これで、一連の権限を減らしてサービスアカウントに割り当てるカスタムロールを作成できるようになりました。 "Google Cloud Storageでバックアップを準備する方法をご覧ください"。

インターネットにアクセスできないサイトで検索とリストアを使用してデータをリストアする機能がサポートされるようになりました

インターネットアクセスのないサイト（ダークサイトまたはオフラインサイトとも呼ばれます）のオンプレミスのONTAP クラスタからStorageGRID にデータをバックアップする場合は、必要に応じて検索とリストアのオプションを使用してデータをリストアできるようになりました。この機能を使用するには、BlueXPコネクタ(バージョン3.9.25以上)がオフラインサイトに配置されている必要があります。

"検索と復元を使用してONTAPデータを復元する方法"。
"コネクターをオフラインサイトにインストールする方法を参照してください"。

ジョブ監視結果ページを**.csv**レポートとしてダウンロードできるようになりました

[ジョブ監視]ページをフィルタリングして、必要なジョブとアクションを表示したら、そのデータの.csvファイルを生成してダウンロードできるようになりました。次に、情報を分析したり、組織内の他のユーザーにレポートを送信したりできます。 "「ジョブ監視レポートを生成する方法」を参照してください"。

2022年12月19日

Cloud Backup for Applicationsの機能強化

- SAP HANAデータベース
  - Azure NetApp Files 上にあるSAP HANAデータベースのポリシーベースのバックアップとリストアをサポートします
  - カスタムポリシーをサポート
- Oracleデータベース
  - ホストを追加してプラグインを自動的に導入
  - カスタムポリシーをサポート
  - Cloud Volumes ONTAP 上にあるOracleデータベースのポリシーベースのバックアップ、リストア、およびクローニングをサポートします
  - Amazon FSX for NetApp ONTAP 上に存在するOracleデータベースのポリシーベースのバックアップおよびリストアをサポートします
  - Connect and Copy方式を使用したOracleデータベースのリストアをサポートします
  - Oracle 21cをサポートします
  - クラウドネイティブのOracleデータベースのクローニングをサポート

Cloud Backup for Virtual Machinesの機能拡張

- 仮想マシン
  - オンプレミスのセカンダリストレージから仮想マシンをバックアップ
  - カスタムポリシーをサポート
  - では、Google Cloud Platform（GCP）をサポートしており、1つ以上のデータストアのバックアップに使用できます
  - Glacier、Deep Glacier、Azure Archiveなどの低コストのクラウドストレージをサポートします

2022年12月6日

必須コネクターアウトバウンドインターネットアクセスエンドポイントの変更

Cloud Backupの処理が変更されたため、クラウドバックアップの処理を成功させるには、次のコネクタエンドポイントを変更する必要があります。

古いエンドポイント	新しいエンドポイント
\ https://cloudmanager.cloud.netapp.com	\ https://api.bluexp.netapp.com
\ https://*.cloudmanager.cloud.netapp.com	\ https://*.api.bluexp.netapp.com

のすべてのエンドポイントのリストを参照してください "AWS"、 "Google Cloud"または "Azure" クラウド環境：

UIでの**Google**アーカイブストレージクラスの選択がサポートされます

バックアップファイルは、最初にGoogle Standardストレージクラスで作成されます。Cloud Backup UIを使用

して、特定の日数が経過した古いバックアップをGoogle Archiveストレージに階層化し、コストをさらに最適化できるようになりました。

この機能は、現在、ONTAP 9.12.1以降を使用するオンプレミスONTAP クラスタでサポートされています。現在、Cloud Volumes ONTAP システムでは使用できません。

FlexGroup ボリュームのサポート

Cloud BackupでFlexGroup ボリュームのバックアップとリストアがサポートされるようになりました。ONTAP 9.12.1以降を使用している場合は、FlexGroup ボリュームをパブリッククラウドストレージとプライベートクラウドストレージにバックアップできます。FlexVol ボリュームとFlexGroup ボリュームが含まれる作業環境がある場合、ONTAP ソフトウェアを更新すると、それらのシステム上の任意のFlexGroup をバックアップできます。

"サポートされるボリュームタイプの一覧を参照してください"。

バックアップのデータを**Cloud Volumes ONTAP** システムの特定のアグリゲートにリストアする機能

以前のリリースでは、データをオンプレミスのONTAP システムにリストアする場合にのみアグリゲートを選択できました。この機能は、Cloud Volumes ONTAP システムにデータをリストアする場合に使用できるようになりました。

2022年11月2日

古い**Snapshot**コピーをベースラインバックアップファイルにエクスポートできるようになりました

バックアップスケジュールのラベル（日単位、週単位など）に一致するボリュームのローカルSnapshotコピーが作業環境にある場合は、それらの履歴Snapshotをバックアップファイルとしてオブジェクトストレージにエクスポートできます。これにより、古いSnapshotコピーをベースラインバックアップコピーに移動することで、クラウドでバックアップを初期化できます。

このオプションは、作業環境でCloud Backupをアクティブ化する場合に使用できます。この設定は、あとでで変更することもできます "[詳細設定ページ"]。

これで、ソースシステムで不要になったボリュームのアーカイブに**Cloud Backup**を使用できるようになります

これで、ボリュームのバックアップ関係を削除できるようになります。これにより、新しいバックアップファイルの作成を停止してソースボリュームを削除し、既存のすべてのバックアップファイルを保持する場合に、アーカイブメカニズムを実現できます。これにより、必要に応じて、あとでソースストレージシステムからスペースを消去しながら、バックアップファイルからボリュームをリストアできるようになります。 "詳細をご確認ください"。

Cloud Backupのアラートを**E**メールおよび通知センターで受信するためのサポートが追加されました

Cloud Backupは、BlueXP Notificationサービスに統合されています。Cloud Backup通知を表示するには、BlueXPメニューバーの通知ベルをクリックします。また、システムにログインしていないときでも重要なシステムアクティビティを通知できるように、メールで通知を送信するようにBlueXPを構成することもできます。このEメールは、バックアップとリストアのアクティビティに注意する必要があるすべての受信者に送信できます。 "詳細をご確認ください"。

新しい**Advanced Settings**ページでは、クラスタレベルのバックアップ設定を変更できます

この新しいページでは、ONTAP システムごとにクラウドバックアップをアクティブ化するときに設定したクラスタレベルのバックアップ設定の多くを変更できます。「デフォルト」バックアップ設定として適用される一部の設定を変更することもできます。変更可能なバックアップ設定の完全なセットは、次のとおりです。

- ONTAP システムにオブジェクトストレージへのアクセス権を付与するストレージキー
- バックアップをオブジェクトストレージにアップロードするために割り当てられるネットワーク帯域幅
- 以降のボリュームの自動バックアップ設定（およびポリシー）
- アーカイブストレージクラス（AWSのみ）
- Snapshotコピーの履歴が最初のベースラインバックアップファイルに含まれているかどうか
- ソースシステムから「年次」スナップショットを削除するかどうか
- オブジェクトストレージに接続されているONTAP IPspace（アクティブ化時に誤って選択された場合）

"クラスタレベルのバックアップ設定の管理に関する詳細情報"。

オンプレミスコネクタを使用している場合に、検索とリストアを使用してバックアップファイルをリストアできるようになりました

以前のリリースでは、Connectorをオンプレミスに導入すると、バックアップファイルをパブリッククラウドに作成するためのサポートが追加されていました。このリリースでは、Connectorがオンプレミスに導入されている場合、Search & Restoreを使用してAmazon S3またはAzure Blobからバックアップをリストアできるようになりました。検索とリストアでは、StorageGRID システムからオンプレミスのONTAP システムへのバックアップのリストアもサポートされています。

現時点では、Google Cloud Storageからバックアップをリストアするために検索とリストアを使用する場合、ConnectorをGoogle Cloud Platformに導入する必要があります。

ジョブ監視ページが更新されました

には、次の更新が行われています "ジョブ監視ページ"：

- 「ワークロード」の列を使用して、ページをフィルタして、ボリューム、アプリケーション、仮想マシン、Kubernetesの各バックアップサービスのジョブを表示できます。
- 特定のバックアップジョブの詳細を表示するには、「ユーザ名」と「ジョブタイプ」の列を新たに追加します。
- [ジョブの詳細]ページには、メインジョブを完了するために実行中のすべてのサブジョブが表示されます。
- このページは15分ごとに自動的に更新されるため、常に最新のジョブステータスの結果が表示されます。また、[更新]ボタンをクリックすると、ページをすぐに更新できます。

AWSのクロスアカウントバックアップの機能拡張

Cloud Volumes ONTAP バックアップにソースボリュームに使用しているものとは異なるAWSアカウントを使用する場合は、デスティネーションのAWSアカウントクレデンシャルをBlueXPに追加し、「s3：PutBucketPolicy」および「s3：PutBucketOwnershipControls」権限をBlueXPに権限を提供するIAMロールに追加する必要があります。これまでは、AWSコンソールで多数の設定を行う必要がありましたが、これはもう必要ありません。

2022年9月28日

Cloud Backup for Applicationsの機能強化

- Google Cloud Platform（GCP）とStorageGRID をサポートし、アプリケーションと整合性のあるスナップショットをバックアップします
- カスタムポリシーを作成する
- アーカイブストレージをサポートします
- SAP HANAアプリケーションをバックアップ
- VMware環境のOracleおよびSQLアプリケーションをバックアップする
- オンプレミスのセカンダリストレージからアプリケーションをバックアップ
- バックアップの非アクティブ化
- SnapCenter サーバを登録解除します

Cloud Backup for Virtual Machinesの機能拡張

- では、StorageGRID を使用して1つ以上のデータストアをバックアップできます
- カスタムポリシーを作成する

2022年9月19日

DataLockと**Ransomware**による保護は、**StorageGRID** システムのバックアップファイルに対して設定できます

最後のリリースで導入された、Amazon S3バケットに格納されたバックアップ向けの_DataLockとRansomware Protection_forが含まれます。このリリースでは、StorageGRID システムに格納されたバックアップファイルのサポートが拡張されています。クラスタがONTAP 9.11.1以降を使用していて、StorageGRID システムがバージョン11.6.0.3以降を実行している場合、この新しいバックアップポリシーオプションを使用できます。 "DataLockとRansomwareによる保護でバックアップを保護する方法の詳細をご確認ください"。

バージョン3.9.22以降のソフトウェアがインストールされたコネクタを実行する必要があります。コネクタはオンプレミスにインストールする必要があり、インターネットにアクセスできるサイトまたはインターネットに接続できないサイトにインストールできます。

これで、バックアップファイルからフォルダレベルのリストアを実行できるようになりました

フォルダ（ディレクトリまたは共有）内のすべてのファイルにアクセスする必要がある場合は、バックアップファイルからフォルダをリストアできるようになりました。フォルダをリストアする方が、ボリューム全体をリストアするよりもはるかに効率的です。この機能は、ONTAP 9.11.1以降を使用している場合、Browse & RestoreメソッドとSearch & Restoreメソッドの両方を使用してリストア処理を実行するときに使用できます。この時点では、1つのフォルダのみを選択してリストアできます。そのフォルダのファイルのみがリストアされます。サブフォルダやサブフォルダ内のファイルはリストアされません。

アーカイブストレージに移動されたバックアップからファイルレベルのリストアを実行できるようになりました

以前は、アーカイブストレージに移動されたバックアップファイルからのみボリュームをリストアできました

（AWSおよびAzureのみ）。これらのアーカイブ済みバックアップファイルから個 々 のファイルをリストアできるようになりました。この機能は、ONTAP 9.11.1以降を使用している場合、Browse & RestoreメソッドとSearch & Restoreメソッドの両方を使用してリストア処理を実行するときに使用できます。

ファイルレベルのリストアで、元のソースファイルを上書きするオプションが追加されました

以前は、元のボリュームにリストアされたファイルは、「Restore_< file_name >」というプレフィックスの新しいファイルとして常にリストアされていました。ボリューム上の元の場所にファイルをリストアする際に、元のソースファイルを上書きできるようになりました。この機能は、参照およびリストア方法と検索およびリストア方法の両方を使用して、リストア処理を実行する場合に使用できます。

ドラッグアンドドロップして、**StorageGRID** システムへのクラウドバックアップを有効にします

状況に応じて "StorageGRID" バックアップ先がキャンバス上の作業環境として存在する場合、オンプレミスのONTAP 作業環境をデスティネーションにドラッグしてクラウドバックアップセットアップウィザードを開始できます。

既知の制限

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

ONTAPのバックアップとリストアの制限事項

レプリケーションの制限事項

- レプリケーション対象として一度に選択できるFlexGroupボリュームは1つだけです。FlexGroupボリュームごとにバックアップを個別にアクティブ化する必要があります。

  FlexVolボリュームに関する制限はありません。作業環境内のすべてのFlexVolボリュームを選択し、同じバックアップポリシーを割り当てることができます。

- では、次の機能がサポートされます "BlueXPレプリケーションサービス"ただし、BlueXPのバックアップとリカバリのレプリケーション機能を使用している場合は適用されません。
  - ボリュームAからボリュームBへ、およびボリュームBからボリュームCへのレプリケーションを行うカスケード構成はサポートされていませんサポートには、ボリュームAからボリュームBへのレプリケーションが含まれます
  - FSx for ONTAPシステムとの間でのデータのレプリケートはサポートされていません。
  - ボリュームの1回限りのレプリケーションを作成することはできません。
- オンプレミスのONTAPシステムからレプリケーションを作成する場合、ターゲットのCloud Volumes ONTAPシステムのONTAPのバージョンが9.8、9.9、または9.11の場合は、mirror-vaultポリシーのみが許可されます。

オブジェクトへのバックアップに関する制限事項

- バックアップポリシーにボリュームが割り当てられていないときにバックアップポリシーを作成または編集する場合、保持されるバックアップの最大数は1018です。ポリシーにボリュームを割り当てたら、ポリシーを編集して最大4、000個のバックアップを作成できます。

- DP ボリュームをバックアップする場合は、次の点に注意してください。
  - SnapMirrorラベルが設定された関係 `app_consistent` および `all_source_snapshot` クラウドにバックアップできない。
  - SnapMirrorデスティネーションボリュームでSnapshotのローカルコピーを作成する場合（使用するSnapMirrorラベルに関係なく）、これらのSnapshotはバックアップとしてクラウドに移動されません。この時点で、BlueXPのバックアップとリカバリでソースDPボリュームをバックアップできるように、目的のラベルを指定したSnapshotポリシーをソースDPボリュームに作成する必要があります。
- FlexGroup ボリュームのバックアップをアーカイブストレージに移動することはできません。
- クラスタでONTAP 9.13.1以降が実行されている場合、FlexGroupボリュームのバックアップでDataLockとランサムウェア対策を使用できます。
- SVM-DR ボリュームバックアップは、次の制限事項でサポートされます。
  - バックアップは ONTAP セカンダリからのみサポートされます。
  - ボリュームに適用されるSnapshotポリシーは、BlueXPのバックアップとリカバリで認識されるポリシー（日次、週次、月次など）のいずれかである必要があります デフォルトの「sm_created」ポリシー（*[すべてのSnapshotをミラーリング]*に使用）は認識されず、バックアップ可能なボリュームのリストにDPボリュームは表示されません。
- MetroCluster のサポート：
  - ONTAP 9.12.1 GA以上を使用している場合は、プライマリシステムに接続しているときにバックアップがサポートされます。バックアップ構成全体がセカンダリシステムに転送されるため、スイッチオーバー後もクラウドへのバックアップが自動的に続行されます。セカンダリシステムにバックアップを設定する必要はありません（実際には、セットアップは制限されています）。
  - ONTAP 9.12.0以前を使用している場合、バックアップはONTAPセカンダリシステムからのみサポートされます。
  - 現時点では、FlexGroup ボリュームのバックアップはサポートされていません。
- [今すぐバックアップ]ボタンを使用したアドホック・ボリューム・バックアップは’データ保護ボリュームではサポートされていません
- SM-BC 設定はサポートされません。
- ONTAP では、1つのボリュームから複数のオブジェクトストアへのSnapMirror関係のファンアウトはサポートされていません。そのため、この構成はBlueXPのバックアップおよびリカバリではサポートされていません。
- 現時点では、オブジェクトストアのWORM / ComplianceモードはAmazon S3、Azure、StorageGRID でサポートされています。これはDataLock機能と呼ばれ、クラウドプロバイダのインターフェイスではなく、BlueXPのバックアップとリカバリの設定を使用して管理する必要があります。

リストアの制限事項

これらの制限事項は、特に明記されていない限り、ファイルとフォルダをリストアするための検索とリストアおよび参照と復元の両方の方法に適用されます。

- ブラウズとリストアでは、一度に最大100個のファイルをリストアできます。
- 検索とリストアでは、一度に1つのファイルをリストアできます。
- ONTAP 9.13.0以降を使用している場合、[参照と復元]および[検索と復元]では、フォルダ内のすべてのファイルとサブフォルダとともにフォルダを復元できます。

9.11.1より前のバージョンのONTAP を使用している場合、リストア処理でリストアできるのは選択したフォルダとそのフォルダ内のファイルのみです。サブフォルダまたはサブフォルダ内のファイルはリストアされません。

9.11.1より前のバージョンのONTAP を使用している場合、フォルダのリストアはサポートされません。

- ディレクトリ/フォルダのリストアは、クラスタでONTAP 9.13.1以降が実行されている場合にのみアーカイブストレージに格納されたデータでサポートされます。
- DataLockを使用して保護されているデータについては、クラスタでONTAP 9.13.1以降が実行されている場合にのみ、ディレクトリ/フォルダのリストアがサポートされます。
- ディレクトリ/フォルダのリストアは、FlexGroup ボリュームのバックアップでは現在サポートされていません。
- レプリケーションやローカルスナップショットからのディレクトリ/フォルダのリストアは現在サポートされていません。
- FlexGroup ボリュームからFlexVol ボリューム、またはFlexVol ボリュームからFlexGroup ボリュームへのリストアはサポートされていません。
- リストアするファイルは、デスティネーションボリュームの言語と同じ言語を使用している必要があります。言語が異なる場合は、エラーメッセージが表示されます。
- AzureアーカイブストレージからStorageGRID システムにデータをリストアする場合、_High_restore優先度はサポートされません。
- クイックリストアの制限事項：
  - デスティネーションの場所は、ONTAP 9.13.0以降を使用するCloud Volumes ONTAPシステムである必要があります。
  - アーカイブストレージにあるバックアップではサポートされません。
  - FlexGroupボリュームは、クラウドバックアップの作成元のソースシステムでONTAP 9.12.1以降が実行されている場合にのみサポートされます。
  - SnapLockボリュームは、クラウドバックアップの作成元のソースシステムでONTAP 9.11.0以降が実行されている場合にのみサポートされます。

はじめに

BlueXPのバックアップとリカバリについて説明します

BlueXPのバックアップとリカバリサービスは、オンプレミスとクラウドの両方で、NetApp ONTAP データ、Kubernetesの永続的ボリューム、データベース、仮想マシンに効率的でセキュアな対費用効果の高いデータ保護を提供します。バックアップは自動的に生成され、パブリックまたはプライベートクラウドアカウントのオブジェクトストアに格納されます。

このサービスは、ブロックレベルの永久増分レプリケーションを実行し、すべてのストレージ効率を維持します。これにより、レプリケートされて格納されるデータの量が大幅に削減されます。さらに、保護されたデータに対してのみ料金が発生し、利用可能な最も低コストのストレージ階層が使用されるため、BlueXPのバックアップとリカバリの対費用効果が非常に高くなります。

必要に応じて、バックアップから同じ作業環境または別の作業環境に全面的に _ ボリューム _ をリストアできます。ONTAPデータをバックアップする場合は、バックアップからフォルダまたは1つ以上の_files_を同じ作業環境または異なる作業環境にリストアすることもできます。

"BlueXPのバックアップとリカバリの詳細については、こちらをご覧ください"。

バックアップとリカバリは、次の目的で使用できます。

- Cloud Volumes ONTAP システムとオンプレミスのONTAP システムからONTAP ボリュームのデータをバックアップおよびリストアします。 "詳細な機能については、こちらをご覧ください"。
- Kubernetes永続ボリュームのバックアップとリストア "詳細な機能については、こちらをご覧ください"。
- アプリケーション向けのBlueXPバックアップ/リカバリを使用して、オンプレミスのONTAP システムからアプリケーションと整合性のあるSnapshotをバックアップします。 "詳細な機能については、こちらをご覧ください"。
- VMware向けBlueXPバックアップ/リカバリを使用して、データストアをクラウドにバックアップし、仮想マシンをオンプレミスのvCenterにリストアします。 "詳細な機能については、こちらをご覧ください"。

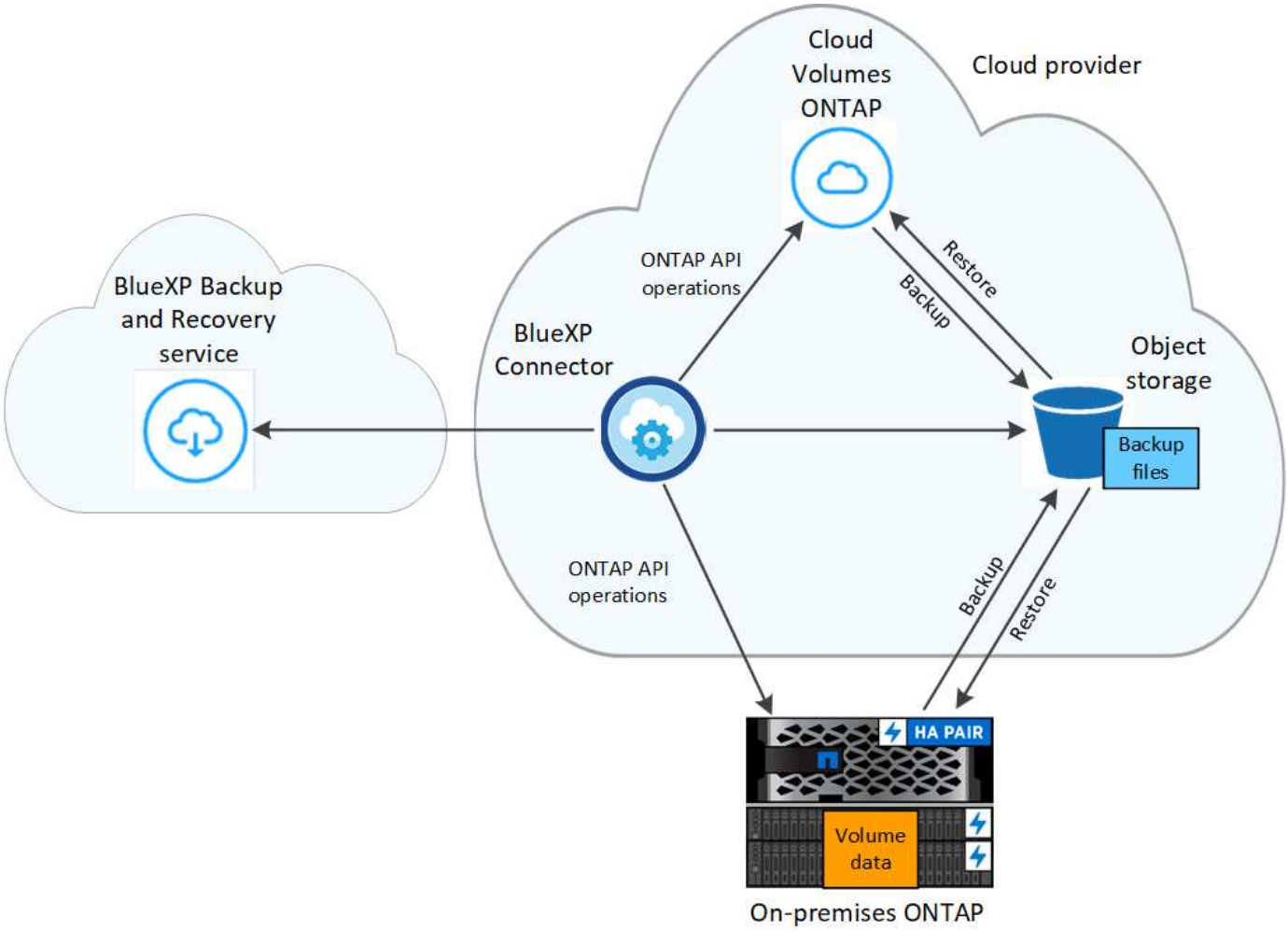
"簡単なデモをご覧ください"

> BlueXP Connectorがクラウドの行政機関やインターネットアクセスのないサイト（ダークサイト）に導入されている場合、BlueXPのバックアップとリカバリでサポートされるのはONTAP システムからのバックアップとリストアの処理のみです。このような導入方法を使用する場合、BlueXPのバックアップとリカバリでは、Kubernetesのクラスタ、アプリケーション、仮想マシンからのバックアップとリストアの処理はサポートされません。

BlueXPのバックアップとリカバリの仕組み

Cloud Volumes ONTAP またはオンプレミスのONTAP システムでBlueXPのバックアップとリカバリを有効にすると、データのフルバックアップが実行されます。ボリューム Snapshot はバックアップイメージに含まれません。初期バックアップ後は、追加のバックアップはすべて差分になります。つまり、変更されたブロックと新しいブロックのみがバックアップされます。これにより、ネットワークトラフィックを最小限に抑えることができます。

次の図は、コンポーネント間の関係を示しています。



バックアップの保管場所

バックアップコピーは、BlueXPがクラウドアカウントで作成したオブジェクトストアに格納されます。クラスタ/作業環境ごとに1つのオブジェクトストアがあり、BlueXPではこのオブジェクトストアの名前を次のように指定します。 `netapp-backup-clusteruuid`。このオブジェクトストアは削除しないでください。

- AWSでは、BlueXPによってが有効になります "Amazon S3 ブロックのパブリックアクセス機能" を S3 バケットに配置します。
- Azureでは、BlueXPは、BLOBコンテナ用のストレージアカウントを持つ新規または既存のリソースグループを使用します。BlueXP "BLOB データへのパブリックアクセスをブロックします" デフォルトでは
- GCPでは、Google Cloud Storageバケット用のストレージアカウントを持つ新規または既存のプロジェクトを使用します。
- StorageGRID では、オブジェクトストアバケットに既存のストレージアカウントが使用されます。
- ONTAP S3では、S3バケット用の既存のユーザアカウントが使用されます。

バックアップが作成されるタイミング

- 毎時バックアップは、毎時 5 分に開始されます。

- 日次バックアップは、毎日午前 0 時を過ぎた直後に開始されます。
- 週次バックアップは、日曜日の朝の午前 0 時を過ぎた直後に開始されます
- 月単位のバックアップは、毎月 1 日の午前 0 時を過ぎた直後に開始されます。
- 年単位のバックアップは、年の最初の日の午前0時を過ぎた直後に開始されます。

開始時間は、各ソース ONTAP システムで設定されているタイムゾーンに基づきます。UIからユーザが指定した時間にバックアップ処理をスケジュールすることはできません。詳細については、システムエンジニアにお問い合わせください。

バックアップコピーはネットアップアカウントに関連付けられています

バックアップコピーはに関連付けられます "ネットアップアカウント" BlueXPコネクタが配置されています。

同じネットアップアカウントに複数のコネクタがある場合は、各コネクタに同じバックアップのリストが表示されます。バックアップには、 Cloud Volumes ONTAP インスタンスとオンプレミスの ONTAP インスタンスに関連付けられたバックアップが含まれます。

BlueXPのバックアップとリカバリのライセンスをセットアップ

BlueXPバックアップ/リカバリのライセンスを取得するには、クラウドプロバイダから従量課金制（PAYGO）またはマーケットプレイスの年間サブスクリプションを購入するか、ネットアップからお客様所有のライセンスを使用（BYOL）する必要があります。作業環境でBlueXPのバックアップとリカバリをアクティブ化したり、本番環境のデータのバックアップを作成したり、バックアップデータを本番システムにリストアしたりするには、有効なライセンスが必要です。

さらに読む前に、いくつかのメモを記入してください。

- クラウドプロバイダのマーケットプレイスでCloud Volumes ONTAP システムの従量課金制（PAYGO）サブスクリプションにすでに登録している場合は、BlueXPのバックアップとリカバリも自動的に登録されます。再度サブスクライブする必要はありません。
- BlueXPのバックアップとリカバリのBring-your-own-license（BYOL）は、BlueXPアカウントに関連付けられているすべてのシステムで使用できるフローティングライセンスです。したがって、既存のBYOLライセンスで使用できるバックアップ容量が十分にある場合、別のBYOLライセンスを購入する必要はありません。
- BYOLライセンスを使用している場合は、PAYGOサブスクリプションもサブスクライブすることを推奨します。BYOLライセンスで許可されている数を超えるデータをバックアップした場合、またはライセンスの有効期限が切れた場合は、従量課金制サブスクリプションを通じてバックアップが続行され、サービスが中断されることはありません。
- オンプレミスの ONTAP データを StorageGRID にバックアップする場合は、 BYOL ライセンスが必要ですが、クラウドプロバイダのストレージスペースは無償です。

"BlueXPのバックアップとリカバリの使用に関連するコストの詳細をご確認ください。"

30 日間の無償トライアルをご利用いただけます

クラウドプロバイダのマーケットプレイスで従量課金制サブスクリプションに登録すると、BlueXPバックア

ップ/リカバリの30日間無償トライアルを利用できます。無料トライアルは、マーケットプレイスのリストに登録した時点から開始されます。Cloud Volumes ONTAPシステムの導入時にマーケットプレイスのサブスクリプション料金を支払ってから、10日後にBlueXPバックアップ/リカバリの無償トライアルを開始すると、残り20日間の無償トライアルを利用できます。

無料トライアルが終了すると、中断することなく自動的にPAYGOサブスクリプションに切り替えられます。BlueXPのバックアップとリカバリの使用を中止する場合は、をクリックします "作業環境からBlueXPバックアップおよびリカバリの登録を解除します" トライアルが終了する前に、請求は行われません。

BlueXPのバックアップとリカバリのPAYGOサブスクリプションを利用

従量課金制の場合、クラウドプロバイダにオブジェクトストレージのコストとネットアップのバックアップライセンスのコストを1時間単位で支払うことになります。無償トライアルを利用されている場合や、お客様が独自のライセンスを使用（ BYOL ）されている場合も、サブスクリプションを設定する必要があります。

- 登録することで、無償トライアルの終了後にサービスが中断されることがなくなります。トライアルが終了すると、バックアップしたデータの量に応じて1時間ごとに課金されます。
- BYOLライセンスで許可されている数を超えるデータをバックアップした場合は、従量課金制サブスクリプションを通じてデータのバックアップとリストアの処理を継続できます。たとえば、 BYOL ライセンスが 10TiB の場合、 10TiB を超える容量はすべて PAYGO サブスクリプションによって課金されます。

無償トライアル中やBYOLライセンスを超えていない場合は、従量課金制サブスクリプションから請求されることはありません。

BlueXPのバックアップとリカバリには、いくつかのPAYGOプランがあります。

- Cloud Volumes ONTAP データとオンプレミスのONTAP データをバックアップできる「クラウドバックアップ」パッケージ。
- Cloud Volumes ONTAP とBlueXPのバックアップとリカバリをバンドルできる「CVO Professional」パッケージです。これには、ライセンスを使用するCloud Volumes ONTAP システムのバックアップが無制限に含まれます（バックアップ容量はライセンス容量にはカウントされません）。このオプションでは、オンプレミスのONTAP データはバックアップできません。

  このオプションにはバックアップとリカバリのPAYGOサブスクリプションも必要ですが、対象となるCloud Volumes ONTAPシステムには料金は発生しません。

- 「CVO Edge Cache」パッケージは、「CVO Professional」パッケージと同じ機能を備えていますが、のサポートも含まれています "BlueXPのエッジキャッシング" サービスCloud Volumes ONTAP システムにプロビジョニングされた容量3TiBにつき、BlueXPエッジキャッシュエッジシステムを1つ導入することができます。このオプションはAzureとGoogleのマーケットプレイスで利用でき、オンプレミスのONTAP データをバックアップすることはできません。

"これらの容量ベースのライセンスパッケージの詳細については、こちらをご覧ください"。

以下のリンクから、クラウドプロバイダのマーケットプレイスからBlueXPバックアップ/リカバリのサブスクリプションに登録できます。

- AWS "価格の詳細については、BlueXP Marketplaceのサービスを参照してください"。
- Azure "価格の詳細については、BlueXP Marketplaceのサービスを参照してください"。
- Google Cloud "価格の詳細については、BlueXP Marketplaceのサービスを参照してください"。

年間契約を使用する

BlueXPのバックアップとリカバリの料金は、年単位の契約を購入して年単位で支払うことができます。期間は1年、2年、3年から選択できます。

市場で年間契約を結んでいるパートナー様の場合、BlueXPのバックアップとリカバリの消費量はすべてその契約に基づいて請求されます。BYOLでは、年単位のマーケットプレイス契約を組み合わせることはできません。

AWSを使用している場合は、で2つの年間契約が提供されます "AWS Marketplace のページ" Cloud Volumes ONTAPシステムとオンプレミスのONTAPシステムの場合：

- Cloud Volumes ONTAP データとオンプレミスの ONTAP データをバックアップできる「クラウドバックアップ」プラン。

  このオプションを使用する場合は、 Marketplace のページでサブスクリプションを設定してから、を設定します "サブスクリプションを AWS クレデンシャルに関連付けます"。BlueXPでAWSクレデンシャルに割り当てることができるアクティブなサブスクリプションは1つだけなので、この年間契約サブスクリプションを使用してCloud Volumes ONTAP システムの料金も支払う必要があります。

- Cloud Volumes ONTAP とBlueXPのバックアップとリカバリをバンドルできる「CVO Professional」プランこれには、ライセンスを使用するCloud Volumes ONTAP システムのバックアップが無制限に含まれます（バックアップ容量はライセンス容量にはカウントされません）。このオプションでは、オンプレミスのONTAP データはバックアップできません。

  を参照してください "Cloud Volumes ONTAP のライセンスに関するトピック" このライセンスオプションの詳細については、を参照してください。

  このオプションを使用する場合は、Cloud Volumes ONTAP 作業環境を作成するときに年間契約を設定し、AWS Marketplaceに登録するように要求するBlueXPを設定できます。

Azureを使用している場合は、 "Azure Marketplaceのページ" Cloud Volumes ONTAPシステムとオンプレミスのONTAPシステムの場合：

- Cloud Volumes ONTAP データとオンプレミスの ONTAP データをバックアップできる「クラウドバックアップ」プラン。

  このオプションを使用する場合は、 Marketplace のページでサブスクリプションを設定してから、を設定します "サブスクリプションをAzureクレデンシャルに関連付ける"。BlueXPでAzureクレデンシャルに割り当てることができるアクティブなサブスクリプションは1つだけなので、この年間契約サブスクリプションを使用してCloud Volumes ONTAPシステムの料金も支払う必要があります。

- Cloud Volumes ONTAP とBlueXPのバックアップとリカバリをバンドルできる「CVO Professional」プランこれには、ライセンスを使用するCloud Volumes ONTAP システムのバックアップが無制限に含まれます（バックアップ容量はライセンス容量にはカウントされません）。このオプションでは、オンプレミスのONTAP データはバックアップできません。

  を参照してください "Cloud Volumes ONTAP のライセンスに関するトピック" このライセンスオプションの詳細については、を参照してください。

  このオプションを使用する場合は、Cloud Volumes ONTAP作業環境の作成時に年間契約を設定でき、BlueXPからAzure Marketplaceへのサブスクライブを求めるメッセージが表示されます。

GCPを使用している場合は、ネットアップの営業担当者に連絡して年間契約を購入してください。この契約は、Google Cloud Marketplaceでのプライベートオファーとして利用できます。

ネットアップからプライベートオファーが提供されたら、BlueXPのバックアップとリカバリのアクティブ化時にGoogle Cloud Marketplaceからサブスクライブする際に年間プランを選択できます。

BlueXPのバックアップとリカバリのBYOLライセンスを使用

ネットアップが提供するお客様所有のライセンスには、 1 年、 2 年、 3 年の期間があります。バックアップ対象のソース ONTAP ボリュームの論理使用容量（ _Before_any 効率化）で計算され、保護するデータに対してのみ料金が発生します。この容量はフロントエンドテラバイト（ FETB ）とも呼ばれます。

BYOL BlueXPバックアップ/リカバリライセンスはフローティングライセンスで、BlueXPアカウントに関連付けられているすべてのシステムで合計容量が共有されます。ONTAP システムの場合は、CLIコマンドを実行して、必要な容量を概算できます `volume show -fields logical-used-by-afs` をクリックします。

BlueXPバックアップ/リカバリのBYOLライセンスをお持ちでない場合は、BlueXPの右下にあるチャットアイコンをクリックして購入してください。

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

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

BlueXPのバックアップとリカバリのライセンスファイルを入手します

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

インターネットにアクセスできないオンプレミスサイトでBlueXPのバックアップとリカバリを実行している（BlueXP Connectorを "プライベートモード"では、インターネットに接続されたシステムからライセンスファイルを取得する必要があります。プライベートモードのインストールでは、シリアル番号とNetApp Support Siteアカウントを使用してライセンスをアクティブ化することはできません。

作業を開始する前に

開始する前に、次の情報が必要です。

- BlueXPバックアップ/リカバリのシリアル番号

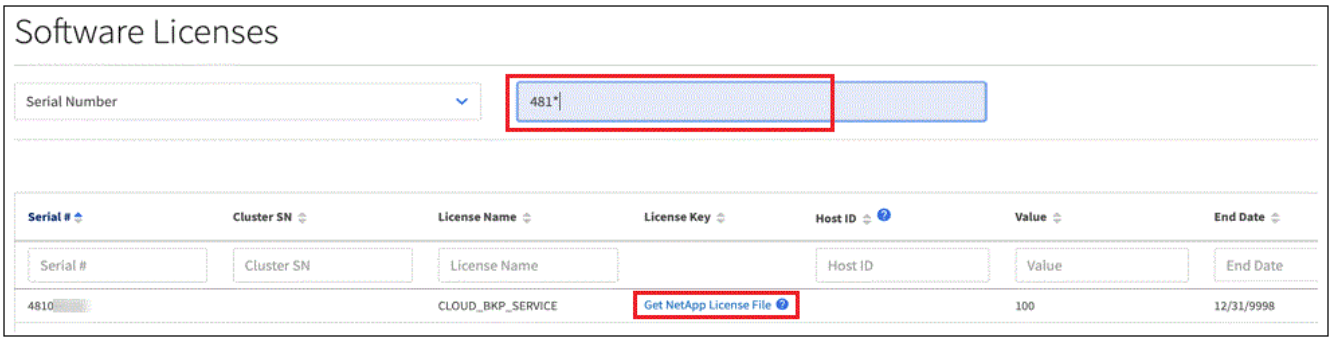
  この番号は、SOから確認するか、アカウントチームにお問い合わせください。

- BlueXPアカウントID

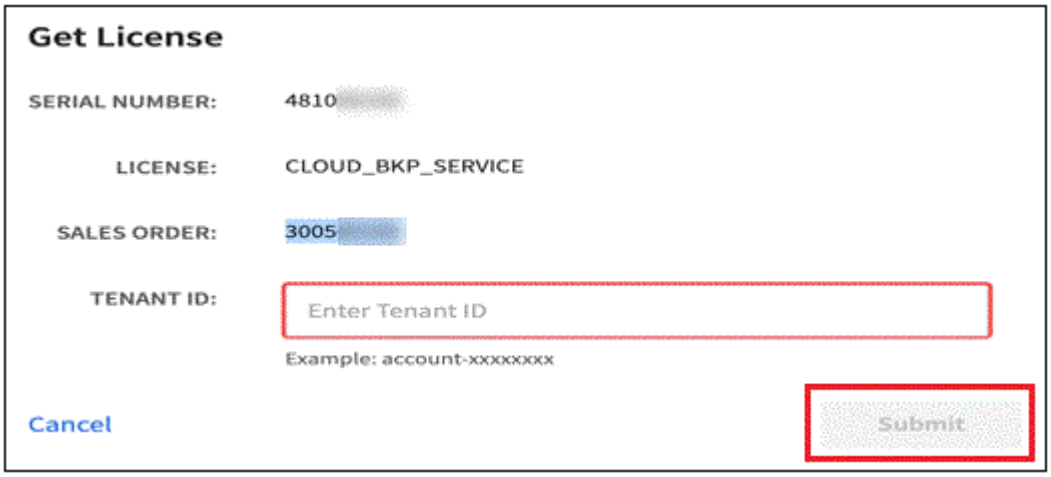
  BlueXPアカウントIDを確認するには、BlueXPの上部にある[**Account**]ドロップダウンを選択し、アカウントの横にある[**Manage Account**]をクリックします。アカウント ID は、 [概要] タブにあります。インターネットにアクセスできないプライベートモードのサイトでは、* account-DARKSITE1*を使用します。

手順

1. にサインインします "NetApp Support Site" [システム] 、 [ソフトウェアライセンス] の順にクリックします。
2. BlueXPバックアップ/リカバリライセンスのシリアル番号を入力します。



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



BlueXPのバックアップとリカバリの**BYOL**ライセンスをアカウントに追加します

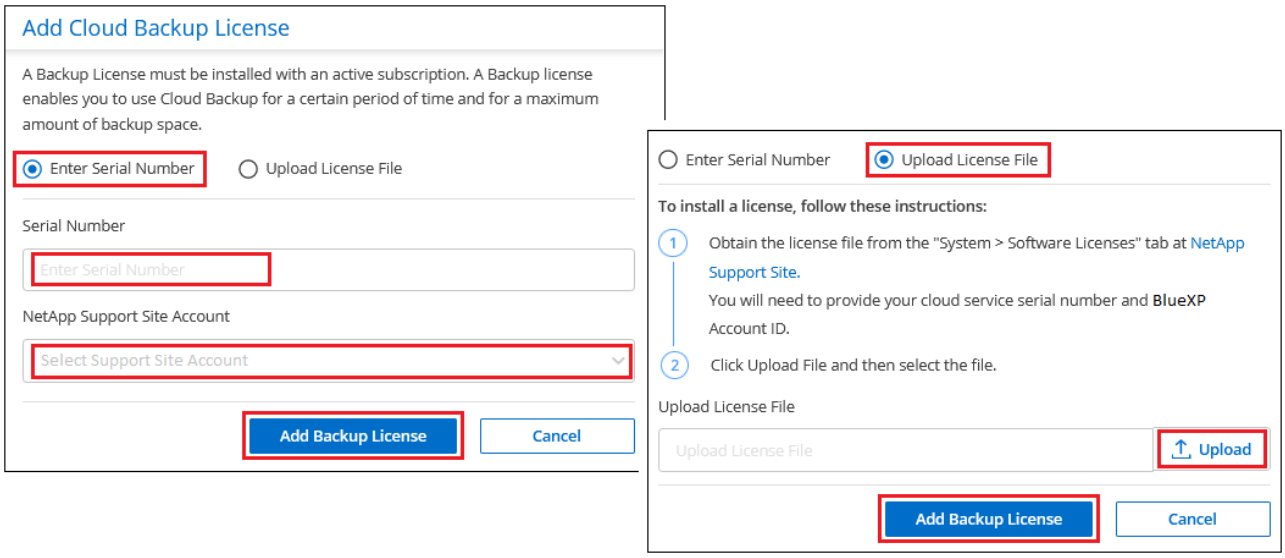
ネットアップアカウント用のBlueXPバックアップ/リカバリライセンスを購入したら、そのライセンスをBlueXPに追加する必要があります。

手順

1. BlueXPメニューから、「ガバナンス」>「デジタルウォレット」をクリックし、「データサービスライセンス」タブを選択します。
2. [ライセンスの追加] をクリックします。
3. _ ライセンスの追加 _ ダイアログで、ライセンス情報を入力し、 * ライセンスの追加 * をクリックします。
   - バックアップライセンスのシリアル番号があり、 NSS アカウントを知っている場合は、 * シリアル番号を入力 * オプションを選択してその情報を入力します。

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

- バックアップライセンスファイル（ダークサイトにインストールする場合に必要）がある場合は、 * ライセンスファイルのアップロード * オプションを選択し、プロンプトに従ってファイルを添付します。

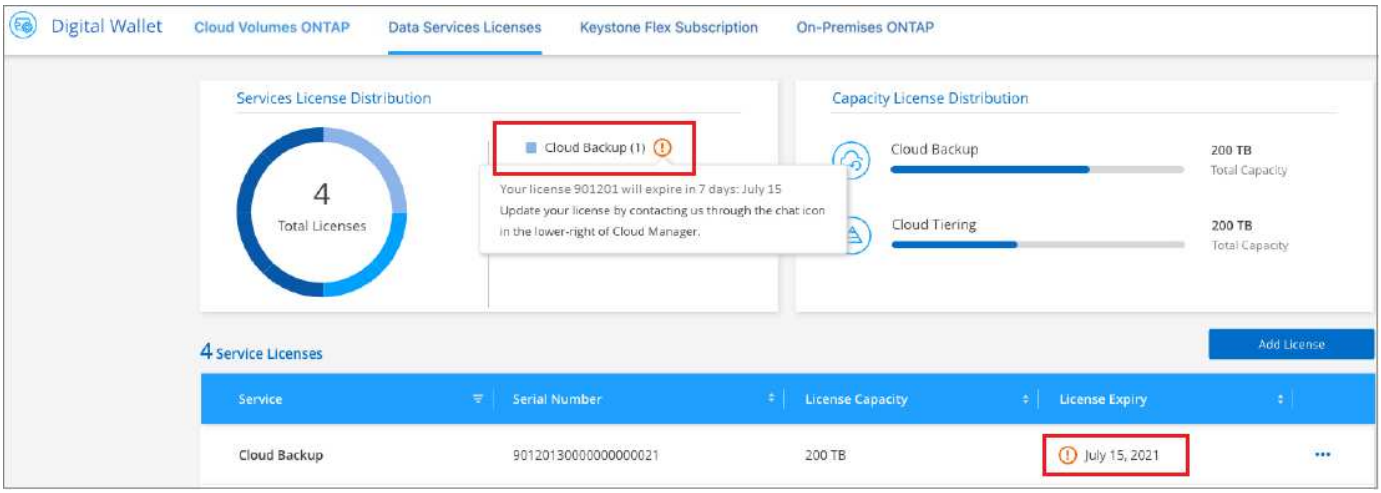


結果

BlueXPには、BlueXPのバックアップとリカバリをアクティブにするためのライセンスが追加されています。

BlueXPのバックアップとリカバリのBYOLライセンスを更新します

ライセンスで許可されている期間が終了期限に近づいている場合や、ライセンスで許可されている容量が上限に達している場合は、バックアップ UI に通知されます。このステータスは、BlueXPのデジタルウォレットページとにも表示されます "通知"。



BlueXPのバックアップとリカバリのライセンスは、有効期限が切れる前に更新できるため、データのバックアップとリストアが中断されることはありません。

手順

1. BlueXPの右下にあるチャットアイコンをクリックするか、サポートにお問い合わせください。特定のシリアル番号について、BlueXPバックアップ/リカバリライセンスの期間の延長や容量の追加をリクエストできます。

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

2. BlueXPがライセンスを自動的に更新できない場合(たとえば、ダークサイトにインストールされている場合)、ライセンスファイルを手動でアップロードする必要があります。
   a. 可能です ライセンスファイルをNetApp Support Siteから入手します。
   b. BlueXPデジタルウォレットページの[Data Services Licenses]タブで、をクリックします ••• アイコン"] 更新するサービスシリアル番号の場合は、 ［ * ライセンスの更新 * ］ をクリックします。

   ボタンを選択するスクリーンショット。"]

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

結果

BlueXPのライセンスが更新され、BlueXPのバックアップとリカバリが引き続きアクティブになります。

BYOL ライセンスに関する考慮事項

BlueXPのバックアップとリカバリのBYOLライセンスを使用している場合、バックアップするすべてのデータのサイズが容量の上限に近づいているかライセンスの有効期限に近づいているときに、BlueXPのユーザインターフェイスに警告が表示されます。次の警告が表示されます。

- バックアップがライセンスで許可された容量の 80% に達したとき、および制限に達したときに再度実行されます
- ライセンスの有効期限が切れる 30 日前と、ライセンスの有効期限が切れたあとに再度有効になります

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

BYOLライセンスの期限が切れると、次の2つのことが起こります。

- 使用しているアカウントにMarketplaceのPAYGOアカウントがある場合、バックアップサービスは引き続き実行されますが、PAYGOライセンスモデルに移行します。バックアップに使用されている容量に基づいて料金が発生します。
- 使用しているアカウントにMarketplaceアカウントがない場合、バックアップサービスは引き続き実行されますが、警告は引き続き表示されます。

BYOLサブスクリプションを更新すると、BlueXPによってライセンスが自動的に更新されます。BlueXPが安全なインターネット接続経由でライセンスファイルにアクセスできない場合(たとえば、ダークサイトにインストールされている場合)は、自分でファイルを取得してBlueXPに手動でアップロードできます。手順につい

ては、を参照してください "BlueXPのバックアップとリカバリのライセンスを更新する方法"。

PAYGO ライセンスに切り替えられたシステムは、自動的に BYOL ライセンスに戻されます。ライセンスなしで実行されていたシステムでは、警告が表示されなくなります。

データ保護を監視

データ保護の適用範囲に関するレポートを作成します

BlueXPのバックアップ/リカバリレポートを使用すると、組織で定義されたポリシーに従って重要なデータを確実に保護し、コンプライアンスニーズを監査できます。

BlueXPのバックアップとリカバリレポートを使用すると、次のことを実現できます。

- 運用の可視性:データ保護、バックアップ成功率、およびバックアップウィンドウとビジネスニーズとの整合性に関するサービスレベルアグリーメントを監視します。
- コンプライアンスと監査:内部および外部の監査プロセスで運用レポートと在庫レポートを使用して、コンプライアンスを継続的に監視します。

> レポートアクティビティはジョブ監視ログで監視されるため、すべてのアクティビティを監査できます。 "ジョブ監視について説明します"。

レポートの範囲

BlueXPのバックアップとリカバリのレポートには、次の情報が表示されます。

- コネクタの場所：オンプレミスまたはクラウド
- ソース：Cloud Volumes ONTAPボリューム、オンプレミスのONTAPボリューム、アプリケーション、Kubernetes永続ボリューム
- デスティネーション：任意のクラウドプロバイダ、NetApp StorageGRID、ONTAP S3
- * ONTAPバージョン*：9.13.0

バックアップインベントリレポートを作成します

BlueXPの[Backup and recovery Reports]タブでは、[Backup Inventory]レポートを作成してその内容をフィルタリングできます。Backup Inventoryレポートでは、特定のアカウント、作業環境、またはSVMインベントリのすべてのバックアップを表示できます。

Backup Inventoryレポートには、次の情報などが表示されます。

- アカウント、作業環境、およびSVM
- 保護されているボリュームと保護されていないボリューム
- バックアップターゲット
- バックアップポリシーが適用されました
- 暗号化形式（プロバイダ管理キーまたはユーザ管理キー）
- DataLockとランサムウェア対策のステータス（ガバナンス、コンプライアンス、なし）
- アーカイブ有効ステータス
- バックアップコピーの数

- バックアップ・タイプ（スケジュール・バックアップまたはユーザーが開始するアドホック・バックアップ）
- ストレージクラス
- Snapshot ラベル

Backup Inventoryレポートには、期限切れまたは失敗したバックアップ情報は含まれません。

レポートの上部には、次の情報を示すグラフが表示されます。

- 対象となるボリュームのうち、少なくとも1つのバックアップが含まれているボリュームの数
- アクティブでないボリュームとアクティブなボリュームの合計

Backup Inventoryレポートには、次のチャートが表示されます。

- ボリュームのバックアップステータス：選択した範囲について、保護されているボリュームと保護されていないボリュームとの比較が表示されます。
- バックアップ数別のボリューム：このボリュームで使用可能なバックアップコピーの数でボリュームをグループ化します。

手順

1. トップメニューから*[レポート]*を選択します。
2. [インベントリのバックアップ]*を選択します。
3. [レポートの作成]*を選択します。
4. アカウント、作業環境、およびSVMを選択します。

   複数の作業環境とSVMを選択できます。

5. 期間（[Last 24 hours]、[week]、または[month]）を選択します。
6. 選択したレポートに応じて、レポートのセクション（[Snapshot Policies]、[Replication Policies]、または[Backup Policies]）を確認します。
7. （オプション）ジョブステータスで結果をフィルタリングします。
8. （オプション）*[Download CSV]*を選択して、レポートの内容を.csv形式でエクスポートします。

Data Protection Job Activityレポートを作成します

プロアクティブな監視により、エコシステム内のすべてのリソースの監視に必要な労力を軽減できます。ONTAP 9.13.0以降では、Snapshot、バックアップ、クローニング、リストアの各処理に関する情報がデータ保護ジョブアクティビティレポートに表示されるようになりました。この情報は、SLAを監視したり、バックアップとリカバリの速度を追跡したりする際に使用できます。

レポート『環境BlueXP Backup and Recovery Operations for Cloud Volumes ONTAP、オンプレミス、アプリケーション、Kubernetes data』

Data Protection Job Activityレポートには、次の情報などが表示されます。

- アカウント、作業環境、およびSVM
- ジョブ・タイプ（バックアップまたはリストア）
- リソース名（ボリュームまたはアプリケーション）
- ジョブステータス
- 開始時刻と終了時刻と期間
- バックアップジョブのポリシー名
- バックアップジョブのSnapshotラベル

ページ上部のグラフには、次の情報が表示されます。

- タイプ別のジョブ
  - ONTAPボリュームのバックアップジョブとリストアジョブの数
  - アプリケーションのバックアップジョブとリストアジョブの数
  - 仮想マシンのバックアップジョブとリストアジョブの数
  - Kubernetesのバックアップジョブとリストアジョブの数
- 毎日のジョブアクティビティ

手順

1. トップメニューから*[レポート]*を選択します。
2. [データ保護ジョブアクティビティ]*を選択します。
3. [レポートの作成]*を選択します。
4. アカウント、作業環境、およびSVMを選択します。
5. 期間（[Last 24 hours]、[week]、または[month]）を選択します。
6. （オプション）ジョブステータス、ジョブタイプ（バックアップまたはリストア）、およびリソースで結果をフィルタリングします。
7. （オプション）*[Download CSV]*を選択して、レポートの内容を.csv形式でエクスポートします。

バックアップジョブとリストアジョブのステータスを監視します

開始したローカルSnapshot、レプリケーション、オブジェクトストレージへのバックアップジョブ、および開始したリストアジョブのステータスを監視できます。完了したジョブ、実行中のジョブ、または失敗したジョブを確認して、問題の診断と修正を行うことができます。BlueXP通知センターを使用すると、通知がEメールで送信されるように設定できるため、システムにログインしていないときでも重要なシステムアクティビティに関する通知を受け取ることができます。BlueXPタイムラインでは、UIまたはAPIを使用して開始したすべての操作の詳細を確認できます。

ジョブモニタでのジョブステータスの表示

[ジョブ監視]タブでは、Snapshot、レプリケーション、オブジェクトストレージへのバックアップ、およびリストア処理のすべてと現在のステータスのリストを表示できます。これには、Cloud Volumes ONTAP 、オンプレミスONTAP 、アプリケーション、仮想マシン、Kubernetesシステムからの運用が含まれます。各処理またはジョブには、一意の ID とステータスがあります。

ステータスは次のいずれかになります。

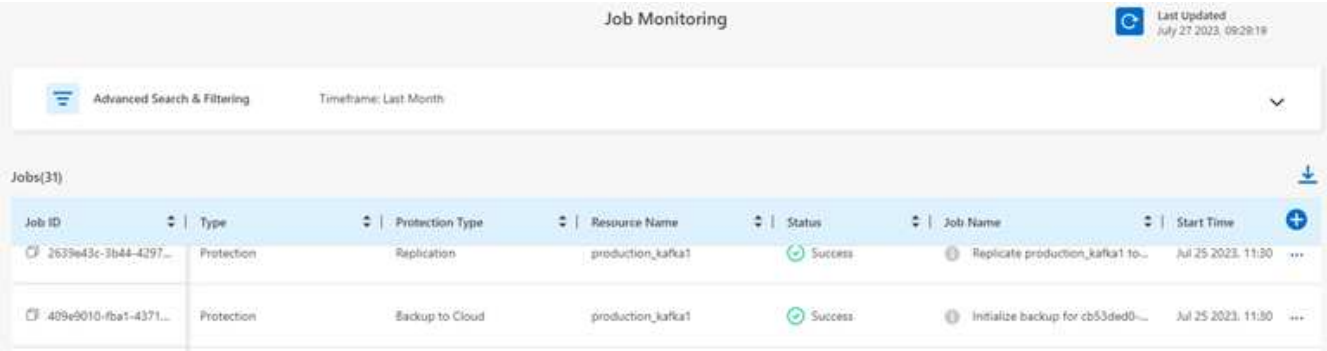
- 成功
- 実行中です
- キューに登録され
- 警告
- 失敗しました

BlueXPのバックアップとリカバリのUIおよびAPIから開始したSnapshot、レプリケーション、オブジェクトストレージへのバックアップ、リストア処理は、[Job Monitoring]タブで確認できます。

> ONTAP システムを9.13.xにアップグレードしたあとに、スケジュールされたバックアップ処理がジョブモニタに表示されない場合は、BlueXPのバックアップ/リカバリサービスを再起動する必要があります。 "BlueXPのバックアップとリカバリを再開する方法をご紹介します"。

手順

1. BlueXPメニューから、*Protection > Backup and recovery*を選択します。
2. [ジョブ監視]タブを選択します。



このスクリーンショットは、デフォルトの列見出しを示しています。

3. 列（Working Environment、SVM、ユーザ名、ワークロード、ポリシー名、 Snapshotラベル）、 。

ジョブのリストを検索してフィルタリングします

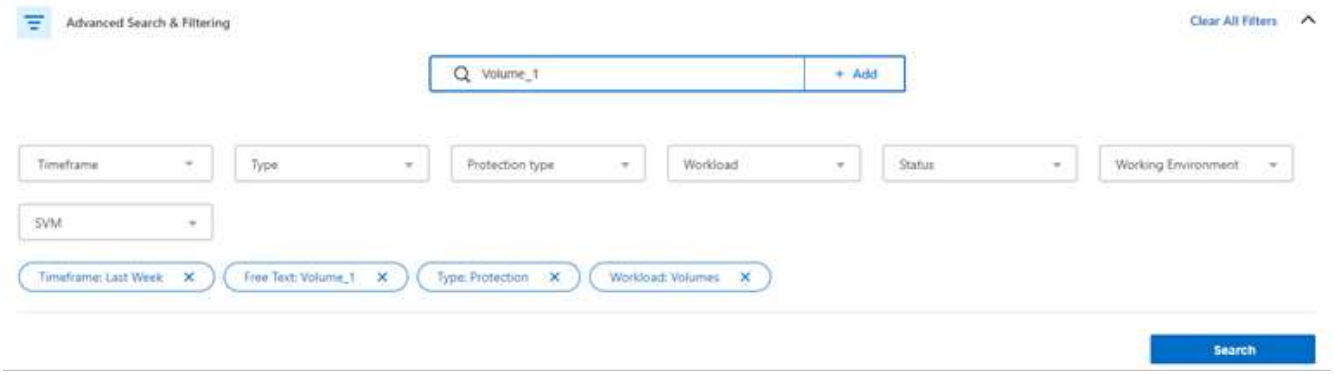
[Job Monitoring]ページでは、ポリシー、Snapshotラベル、処理のタイプ（保護、リストア、保持など）、保護のタイプ（ローカルSnapshot、レプリケーション、クラウドへのバックアップ）などの複数のフィルタを使用して処理をフィルタリングできます。

デフォルトでは、[Job Monitoring]ページには、過去24時間の保護ジョブとリカバリジョブが表示されます。タイムフレームは、タイムフレームフィルタを使用して変更できます。

手順

1. [ジョブ監視]タブを選択します。
2. 結果を別 々 にソートするには、各列見出しを選択して、ステータス、開始時間、リソース名などでソートします。
3. 特定のジョブを探している場合は、* Advanced Search & Filtering *領域を選択して、検索パネルを開きます。

   このパネルを使用して、任意のリソース（「volume 1」や「application 3」など）のフリーテキスト検索を入力します。ドロップダウンメニューの項目に基づいてジョブリストをフィルタすることもできます。



   このスクリーンショットは、「過去1週間」に「Volume_1」という名前のボリュームに対するすべての「Volume」「Backup」ジョブを検索する方法を示しています。

   ほとんどのフィルタはわかりやすいものです。「ワークロード」のフィルタを使用すると、次のカテゴリのジョブを表示できます。

   - ボリューム（Cloud Volumes ONTAPとオンプレミスのONTAPボリューム）
   - アプリケーション
   - 仮想マシン
   - Kubernetes

   - 特定の「SVM」内のデータを検索できるのは、最初に作業環境を選択した場合のみです。
   - [保護タイプ]フィルタを使用して検索できるのは、[保護]の[タイプ]を選択した場合のみです。

4. ページをすぐに更新するには、を選択します ボタンを押します。そうしないと、このページは15分ごとに更新され、常に最新のジョブステータス結果が表示されます。

ジョブの詳細を表示します

完了した特定のジョブに対応する詳細を表示できます。特定のジョブの詳細をJSON形式でエクスポートできます。

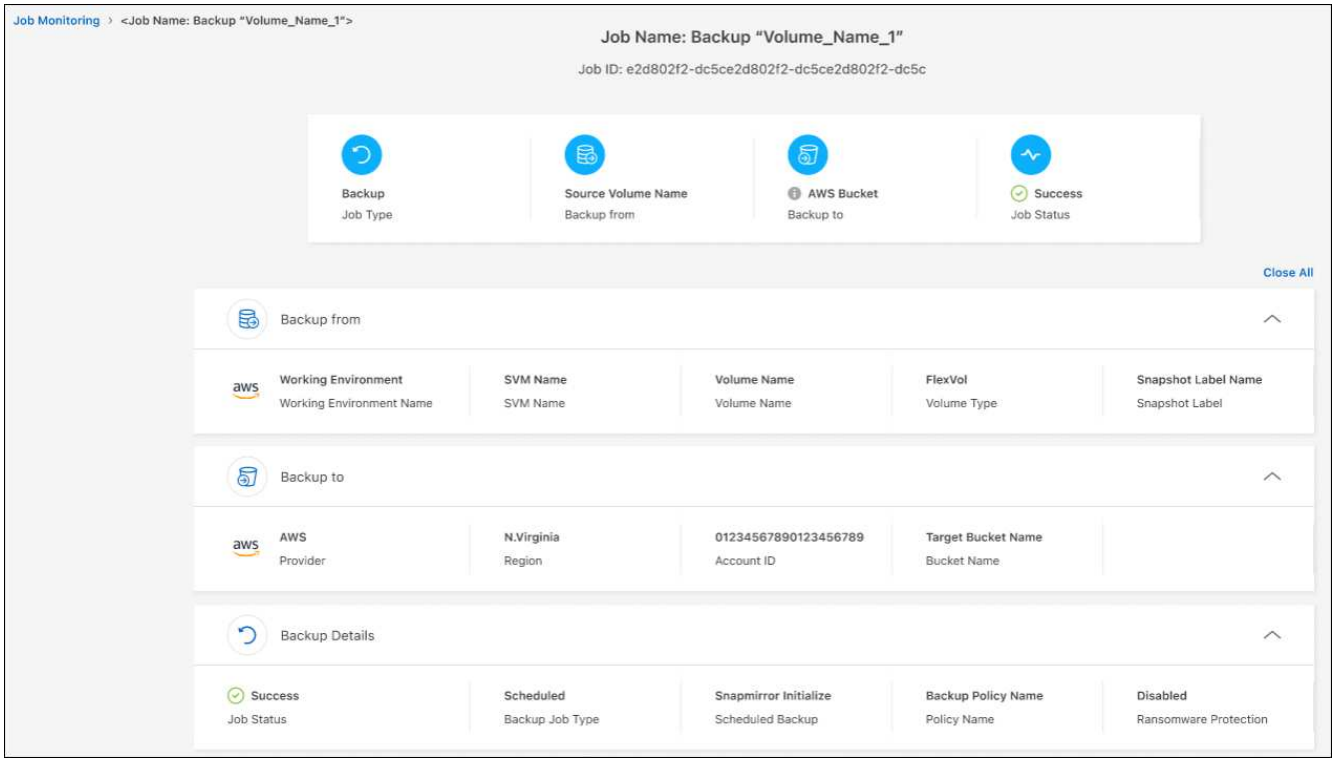
ジョブタイプ（スケジュール済みまたはオンデマンド）、SnapMirrorバックアップタイプ（初期または定期的）の開始時刻と終了時刻、期間、作業環境からオブジェクトストレージに転送されたデータの量、平均転送速度、ポリシー名、保持ロックの有効化、ランサムウェアスキャンの実行などの詳細を表示できます。 保護ソ

ースの詳細と保護ターゲットの詳細。

リストアジョブには、バックアップターゲットプロバイダ（Amazon Web Services、Microsoft Azure、Google Cloud、オンプレミス）、S3バケット名、 SVM名、ソースボリューム名、デスティネーションボリューム、Snapshotラベル、リカバリされたオブジェクト数、 ファイル名、ファイルサイズ、最終変更日、および完全なファイルパス。

手順

1. [ジョブ監視]タブを選択します。
2. ジョブの名前を選択します。
3. [Actions]メニューを選択します ••• [View Details]*を選択します。



Job Name: Backup "Volume_Name_1"

Job ID: e2d802f2-dc5ce2d802f2-dc5ce2d802f2-dc5c

4. 各セクションを展開して詳細を表示します。

ジョブ監視結果をレポートとしてダウンロードします

ジョブ監視のメインページの内容は、リファイン後にレポートとしてダウンロードできます。BlueXPのバックアップとリカバリでは.csvファイルが生成されてダウンロードされ、確認して必要に応じて他のグループに送信できます。.csvファイルには、最大10、000行のデータが含まれます。

[Job Monitoring Details]の情報から、単一のジョブの詳細を含むJSONファイルをダウンロードできます。

手順

1. [ジョブ監視]タブを選択します。
2. すべてのジョブのCSVファイルをダウンロードするには、を選択します ↓ ボタンをクリックし、ダウンロードディレクトリでファイルを見つけます。
3. 単一のジョブのJSONファイルをダウンロードするには、[Actions]メニューを選択します ••• ジョブの場合は、*[Download JSON File]*を選択し、ダウンロードディレクトリでファイルを探します。

保持（バックアップライフサイクル）ジョブの確認

保持（または_backup lifecycle _）フローの監視は、監査の完全性、説明責任、およびバックアップの安全性を支援します。バックアップのライフサイクルを追跡するために、すべてのバックアップコピーの有効期限を確認することができます。

バックアップライフサイクルジョブは、削除された、または削除対象のキューにあるすべてのSnapshotコピーを追跡します。ONTAP 9.13以降では、[Job Monitoring]ページで[Retention]というすべてのジョブタイプを確認できます。

「保持」ジョブタイプには、BlueXPのバックアップとリカバリで保護されているボリュームで開始されたSnapshot削除ジョブがすべてキャプチャされます。

手順

1. [ジョブ監視]タブを選択します。
2. [高度な検索とフィルタ（Advanced Search & Filtering）]領域を選択して、[検索（Search）]パネルを開きます。
3. ジョブ・タイプとして[Retention]を選択します。

BlueXP通知センターでバックアップとリストアのアラートを確認します

BlueXP通知センターでは、開始したバックアップジョブとリストアジョブの進捗状況が追跡されるため、処理が成功したかどうかを確認できます。

通知センターではアラートを確認できるだけでなく、特定のタイプの通知をEメールでアラートとして送信するようにBlueXPを設定することもできます。これにより、システムにログインしていないときでも重要なシステムアクティビティに関する情報を受け取ることができます。 "通知センターの詳細と、バックアップおよびリストア・ジョブに関するアラート・メールの送信方法について説明します"。

通知センターには、Snapshot、レプリケーション、クラウドへのバックアップ、リストアに関する多数のイベントが表示されますが、Eメールアラートがトリガーされるのは特定のイベントだけです。

処理のタイプ	イベント	アラートレベル	Eメール送信済み
アクティブ化	作業環境でバックアップとリカバリのアクティブ化に失敗しました	エラー	はい。
アクティブ化	作業環境のバックアップとリカバリの編集に失敗しました	エラー	はい。
ローカルSnapshot	BlueXPのバックアップとリカバリのアドホックSnapshot作成ジョブが失敗する	エラー	はい。
レプリケーション	BlueXPのバックアップとリカバリのアドホックレプリケーションジョブの失敗	エラー	はい。
レプリケーション	BlueXPのバックアップとリカバリのレプリケーションが一時停止するジョブが失敗する	エラー	いいえ
レプリケーション	BlueXPのバックアップ/リカバリレプリケーションのブレーキジョブの失敗	エラー	いいえ

処理のタイプ	イベント	アラートレベル	Eメール送信済み
レプリケーション	BlueXPのバックアップ/リカバリレプリケーションの再同期ジョブが失敗する	エラー	いいえ
レプリケーション	BlueXPのバックアップとリカバリのレプリケーションが停止するジョブが失敗する	エラー	いいえ
レプリケーション	BlueXPのバックアップ/リカバリレプリケーションの逆再同期ジョブが失敗する	エラー	はい。
レプリケーション	BlueXPのバックアップ/リカバリレプリケーションの削除ジョブが失敗する	エラー	はい。

ONTAP 9.13.0以降では、Cloud Volumes ONTAPシステムとオンプレミスONTAPシステムのすべてのアラートが表示されます。Cloud Volumes ONTAP 9.13.0およびオンプレミスのONTAPを搭載したシステムでは、「リストアジョブは完了しましたが、警告あり」に関連するアラートのみが表示されます。

デフォルトでは、「Critical」アラートと「Recommendation」アラートがすべてBlueXPアカウント管理者にEメールで送信されます。他のすべてのユーザと受信者は、通知メールを受信しないようにデフォルトで設定されています。ネットアップクラウドアカウントを使用しているBlueXPユーザや、バックアップとリストアのアクティビティに注意が必要なその他の受信者にEメールを送信できます。

BlueXPのバックアップとリカバリのEメールアラートを受け取るには、[Alerts and Notifications Settings]ページで通知の重大度タイプとして「Critical」、「Warning」、「Error」を選択する必要があります。

"バックアップジョブとリストアジョブに関するアラートEメールを送信する方法について説明します"。

手順

1. BlueXPのメニューバーで、を選択します）。
2. 通知を確認します。

BlueXPのタイムラインで処理のアクティビティを確認します

BlueXPタイムラインでは、バックアップとリストアの処理の詳細を確認して詳しい調査を行うことができます。BlueXPのタイムラインには、ユーザが開始したイベントとシステムが開始したイベントの詳細が表示され、UIまたはAPIを使用して開始されたアクションが表示されます。

"タイムラインと通知センターの違いについて説明します"。

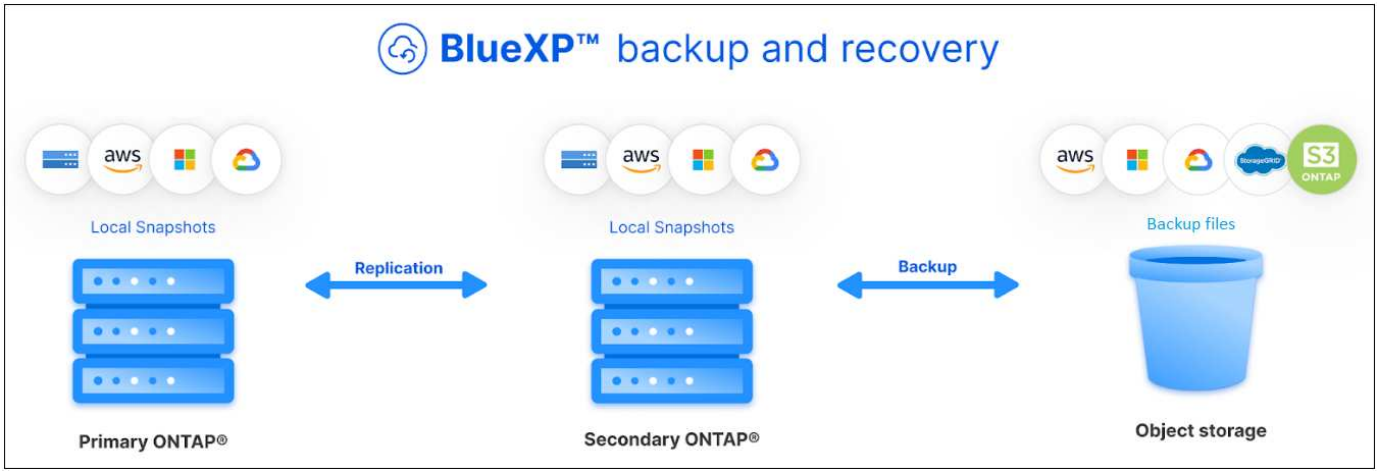
ONTAP データのバックアップとリストア

BlueXPのバックアップとリカバリを使用してONTAPボリュームのデータを保護します

BlueXPのバックアップとリカバリサービスは、ONTAPボリュームデータの保護と長期アーカイブのためのバックアップとリストア機能を提供します。3-2-1戦略では、ソースデータのコピーを2つの異なるストレージシステムに3つ、クラウドに1つ保持できます。

アクティブ化後、バックアップとリカバリによってブロックレベルの永久増分バックアップが作成され、別のONTAPクラスタとクラウド内のオブジェクトストレージに格納されます。ソースボリュームに加えて、次の機能があります。

- ソースシステム上のボリュームのSnapshotコピー
- 別のストレージシステムにレプリケートされたボリューム
- オブジェクトストレージ内のボリュームのバックアップ



BlueXPのバックアップとリカバリでは、ネットアップのSnapMirrorデータレプリケーションテクノロジを活用してSnapshotコピーを作成し、バックアップ先に転送することで、すべてのバックアップが完全に同期されます。

3-2-1アプローチの利点は次のとおりです。

- 複数のデータコピーを使用して、内部（内部）と外部のサイバーセキュリティの脅威に対する多層保護を実現します。
- 複数のメディアタイプにより、1つのメディアタイプの物理的または論理的な障害が発生した場合でもフェイルオーバーを実行できます。
- オンサイトコピーを使用すると、オンサイトコピーが危険にさらされた場合に備えて、オフサイトコピーを準備した状態で迅速にリストアできます。

必要に応じて、任意のバックアップコピーから、*volume*_全体、*a_folder*、または1つ以上の_files_を同じ作業環境または異なる作業環境にリストアできます。

の機能

レプリケーション機能：

- バックアップとディザスタリカバリをサポートするために、ONTAPストレージシステム間でデータをレプリケートします。
- 高い可用性を備えた信頼性の高い DR 環境を実現します。
- 2つのシステム間で事前共有キー（PSK）を使用して設定されたネイティブONTAP転送中暗号化。
- コピーされたデータは、書き込み可能にして使用できるようになるまで変更できません。
- 転送に失敗した場合、レプリケーションは自己回復型です。
- と比較した場合 "BlueXPレプリケーションサービス"BlueXPのバックアップとリカバリでのレプリケーションには、次の機能が含まれています。
  - 複数のFlexVolボリュームを一度にセカンダリシステムにレプリケートします。
  - UIを使用して、レプリケートされたボリュームをソースシステムまたは別のシステムにリストアします。
  - レプリケーションポリシーの管理

を参照してください "レプリケーションの制限事項" BlueXPのバックアップとリカバリでは使用できないレプリケーション機能のリストについては、を参照してください。

オブジェクトへのバックアップ機能：

- データボリュームの独立したコピーを低コストのオブジェクトストレージにバックアップできます。
- クラスタ内のすべてのボリュームに単一のバックアップポリシーを適用するか、または一意のリカバリポイント目標が設定されたボリュームに異なるバックアップポリシーを割り当てます。
- クラスタで今後作成されるすべてのボリュームに適用するバックアップポリシーを作成します。
- 書き換え不可のバックアップファイルを作成して、保持期間中にロックされて保護されるようにします。
- バックアップファイルをスキャンしてランサムウェア攻撃を受ける可能性があるかを調べ、感染したバックアップを自動的に削除/置換します。
- 古いバックアップファイルをアーカイブストレージに階層化してコストを削減します。
- ボリュームのバックアップを保持しながら不要なソースボリュームをアーカイブできるように、バックアップ関係を削除します。
- クラウドからクラウドへ、オンプレミスシステムからパブリッククラウドやプライベートクラウドへバックアップできます。
- バックアップデータは、転送中の AES-256 ビット暗号化と TLS 1.2 HTTPS 接続によって保護されます。
- クラウドプロバイダのデフォルトの暗号化キーを使用する代わりに、お客様が管理する独自のキーを使用してデータを暗号化します。
- 単一ボリュームで最大 4 、 000 個のバックアップがサポートされます。

リストア機能：

- ローカルのSnapshotコピー、レプリケートされたボリューム、またはオブジェクトストレージ内のバックアップされたボリュームから、特定の時点のデータをリストアします。

- ボリューム、フォルダ、または個々のファイルをソースシステムまたは別のシステムにリストアする。
- 別のサブスクリプション / アカウントを使用して、または別のリージョンにある作業環境にデータをリストアする。
- クラウドストレージからCloud Volumes ONTAPシステムまたはオンプレミスシステムにボリュームの_クイックリストア_を実行します。ボリュームへのアクセスをできるだけ早く提供する必要があるディザスタリカバリ環境に最適です。
- 元のACLを維持したまま、データを指定した場所に直接配置して、ブロックレベルでデータをリストアします。
- ファイルカタログの参照と検索により、単一ファイルのリストアに必要な個 々 のフォルダやファイルを簡単に選択できます。

バックアップとリストア処理でサポートされる作業環境

BlueXPのバックアップとリカバリは、ONTAP作業環境とパブリック/プライベートクラウドプロバイダをサポートします。

サポートされるバックアップ先

BlueXPのバックアップとリカバリを使用すると、パブリック/プライベートクラウドプロバイダでは、ONTAPボリュームを次のソース作業環境から次のセカンダリ作業環境やオブジェクトストレージにバックアップできます。Snapshotコピーはソースの作業環境に配置されます。

ソースの作業環境	セカンダリ作業環境（レプリケーション）	デスティネーションオブジェクトストア（バックアップ） ifdef：aws []
AWS の Cloud Volumes ONTAP	AWS の Cloud Volumes ONTAP オンプレミスの ONTAP システム	Amazon S3 endif：：aws[] ifdef：Azure []
Azure の Cloud Volumes ONTAP	Azure の Cloud Volumes ONTAP オンプレミスの ONTAP システム	Azure Blob の略 endif：：azure[] ifdef ::gcp[]
Google の Cloud Volumes ONTAP	Google の Cloud Volumes ONTAP オンプレミスの ONTAP システム	Google クラウドストレージ endif：GCP []

オンプレミスの ONTAP システム	Cloud Volumes ONTAP オンプレミスの ONTAP システム	ifdef：aws [] Amazon S3 endif：：aws[] ifdef：Azure [] Azure Blob の略 endif：：azure[] ifdef ::gcp[] Google クラウドストレージ endif：GCP [] NetApp StorageGRID ONTAP S3の略

サポートされるリストア先

セカンダリ作業環境（レプリケートされたボリューム）またはオブジェクトストレージ（バックアップファイル）にあるバックアップファイルから、ONTAPデータを次の作業環境にリストアできます。Snapshotコピーはソースの作業環境に存在し、同じシステムにのみリストアできます。

バックアップファイルの場所		デスティネーションの作業環境
オブジェクトストア（バックアップ）	セカンダリシステム（レプリケーション）	ifdef::aws[]
Amazon S3	AWS の Cloud Volumes ONTAP オンプレミスの ONTAP システム	AWS の Cloud Volumes ONTAP オンプレミスの ONTAP システム endif：：aws[] ifdef：Azure []
Azure Blob の略	Azure の Cloud Volumes ONTAP オンプレミスの ONTAP システム	Azure の Cloud Volumes ONTAP オンプレミスの ONTAP システム endif：：azure[] ifdef ::gcp[]
Google クラウドストレージ	Google の Cloud Volumes ONTAP オンプレミスの ONTAP システム	Google の Cloud Volumes ONTAP オンプレミスの ONTAP システム endif：GCP []

バックアップファイルの場所		デスティネーションの作業環境
NetApp StorageGRID	オンプレミスの ONTAP システム Cloud Volumes ONTAP	オンプレミスの ONTAP システム
ONTAP S3の略	オンプレミスの ONTAP システム Cloud Volumes ONTAP	オンプレミスの ONTAP システム

「オンプレミス ONTAP システム」とは、 FAS 、 AFF 、 ONTAP Select の各システムを指します。

サポートされるボリューム

BlueXPのバックアップとリカバリでは、次のタイプのボリュームがサポートされます。

- FlexVol 読み書き可能ボリューム
- FlexGroup ボリューム（ONTAP 9.12.1以降が必要）
- SnapLock Enterpriseボリューム（ONTAP 9.11.1以降が必要）
- SnapLock Complianceボリューム（ONTAP 9.14以降が必要）
- SnapMirrorデータ保護（DP）デスティネーションボリューム

の項を参照してください "バックアップとリストアの制限事項" を参照してください。

コスト

ONTAP システムでBlueXPのバックアップとリカバリを使用すると、リソース料金とサービス料金の2種類のコストが発生します。これらの料金はどちらも、サービスのオブジェクトへのバックアップ部分に適用されます。

Snapshotコピーやレプリケートされたボリュームの保存に必要なディスクスペース以外は、Snapshotコピーやレプリケートされたボリュームの作成に料金はかかりません。

- リソース料金 *

リソース料金は、オブジェクトストレージの容量、クラウドへのバックアップファイルの書き込みと読み取りのために、クラウドプロバイダに支払われます。

- オブジェクトストレージへのバックアップについては、クラウドプロバイダにオブジェクトストレージのコストを支払います。

  BlueXPのバックアップとリカバリではソースボリュームのストレージ効率化が維持されるため、クラウドプロバイダのオブジェクトストレージのコストであるdata_after_ ONTAP 効率化（重複排除と圧縮を適用したあとのデータ量が少ない場合）を支払う必要があります。

- 検索とリストアを使用してデータをリストアする場合、クラウドプロバイダによって特定のリソースがプロビジョニングされ、検索要求でスキャンされるデータ量には1TiBあたりのコストが関連付けられます。（これらのリソースは参照と復元には必要ありません）。
  - AWSでは、 "Amazon Athena" および "AWS 接着剤" リソースは新しいS3バケットに導入される。
  - Azureのでは "Azure Synapseワークスペース" および "Azure Data Lake Storageの略" データの格納と分析を行うためにストレージアカウントにプロビジョニングします。

- Googleでは、新しいバケットが導入され、が展開されます "Google Cloud BigQueryサービス" アカウント/プロジェクトレベルでプロビジョニングされます。
- アーカイブオブジェクトストレージに移動されたバックアップファイルからボリュームデータをリストアする場合は、クラウドプロバイダからGiB単位の読み出し料金と要求単位の料金を別途請求します。
- ボリュームデータのリストアプロセス中にバックアップファイルをスキャンしてランサムウェアを検出する場合（クラウドバックアップに対してDataLockとRansomware Protectionを有効にしている場合）は、クラウドプロバイダからの追加の出力コストも発生します。
- サービス料金 *

サービス料金はNetAppに支払われ、オブジェクトストレージへの_create_backupsと、それらのバックアップからのto_restore_volumes（ファイル）のコストの両方をカバーします。料金は、オブジェクトストレージで保護したデータに対してのみ発生します。これは、オブジェクトストレージにバックアップされるONTAPボリュームのソースの使用済み論理容量（ONTAPによる削減率）から計算されます。この容量はフロントエンドテラバイト（ FETB ）とも呼ばれます。

バックアップサービスの料金を支払う方法は 3 通りあります。1 つ目は、クラウドプロバイダを利用して月額料金を支払う方法です。2つ目のオプションは、年間契約を取得することです。3 つ目のオプションは、ネットアップからライセンスを直接購入することです。を参照してください ライセンス 詳細については、を参照してください

ライセンス

BlueXPのバックアップとリカバリには、次の消費モデルがあります。

- * BYOL *：ネットアップから購入したライセンス。任意のクラウドプロバイダで使用できます。
- * PAYGO *：クラウドプロバイダの市場から1時間ごとのサブスクリプション。
- * Annual *：クラウドプロバイダの市場から年間契約。

Backupライセンスは、オブジェクトストレージからのバックアップとリストアにのみ必要です。Snapshotコピーとレプリケートされたボリュームを作成するためのライセンスは必要ありません。

お客様所有のライセンスを使用

BYOLはタームベース（1、2、または3年）の_および_容量ベース（1TiB単位）です。ネットアップに料金を支払って、 1 年分のサービスを使用し、最大容量を指定した場合は「 10TiB 」とします。

サービスを有効にするためにBlueXPのデジタルウォレットページに入力したシリアル番号が表示されます。いずれかの制限に達すると、ライセンスを更新する必要があります。Backup BYOL ライセンス環境 では、に関連付けられているすべてのソースシステムがライセンスされます "BlueXPアカウント"。

"BYOL ライセンスの管理方法について説明します"。

従量課金制のサブスクリプション

BlueXPのバックアップとリカバリは、従量課金制モデルで従量課金制のライセンスを提供します。クラウドプロバイダの市場に登録すると、バックアップしたデータに対して1 GiB単位で料金が発生し、前払いによる支払いが発生しなくなります。クラウドプロバイダから月額料金で請求されます。

"従量課金制サブスクリプションの設定方法について説明します"。

PAYGOサブスクリプションに最初にサインアップしたときに、30日間の無償トライアルを利用できます。

年間契約

AWSを使用する場合は、1年、2年、3年の2年間契約を選択できます。

- Cloud Volumes ONTAP データとオンプレミスの ONTAP データをバックアップできる「クラウドバックアップ」プラン。
- Cloud Volumes ONTAP とBlueXPのバックアップとリカバリをバンドルできる「CVO Professional」プランこれには、このライセンスに基づいて Cloud Volumes ONTAP ボリュームのバックアップが無制限になることも含まれます（バックアップ容量はライセンスにはカウントされません）。

Azureをご利用の場合は、1年、2年、3年の2年間契約をご用意しています。

- Cloud Volumes ONTAP データとオンプレミスの ONTAP データをバックアップできる「クラウドバックアップ」プラン。
- Cloud Volumes ONTAP とBlueXPのバックアップとリカバリをバンドルできる「CVO Professional」プランこれには、このライセンスに基づいて Cloud Volumes ONTAP ボリュームのバックアップが無制限になることも含まれます（バックアップ容量はライセンスにはカウントされません）。

GCPを使用している場合は、ネットアップにプライベートオファーをリクエストし、BlueXPのバックアップとリカバリのアクティブ化中にGoogle Cloud Marketplaceからサブスクリプションを登録する際にプランを選択できます。

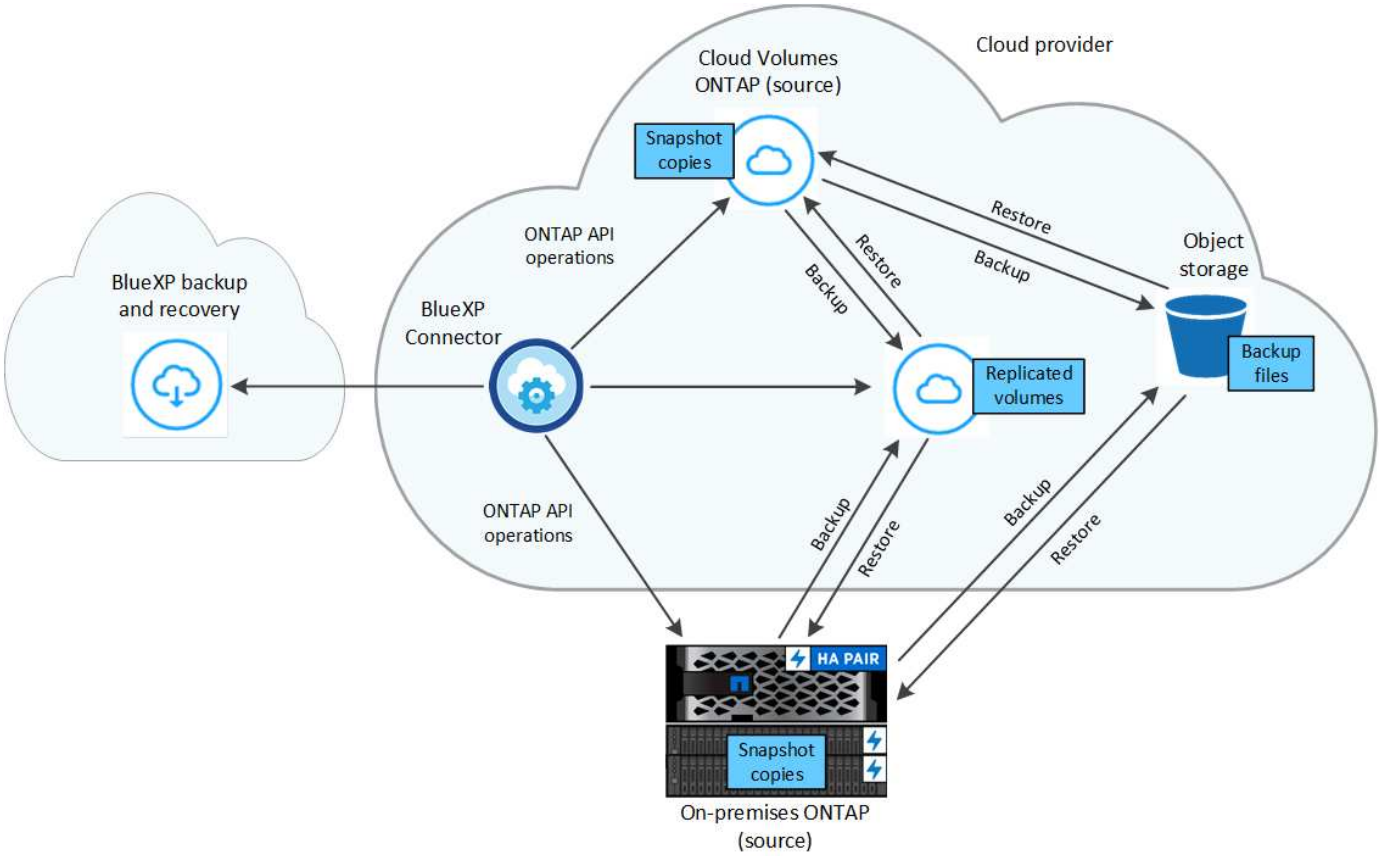
"年間契約の設定方法について説明します"。

BlueXPのバックアップとリカバリの仕組み

Cloud Volumes ONTAP またはオンプレミスのONTAP システムでBlueXPのバックアップとリカバリを有効にすると、データのフルバックアップが実行されます。初期バックアップ後は、追加のバックアップはすべて差分になります。つまり、変更されたブロックと新しいブロックのみがバックアップされます。これにより、ネットワークトラフィックを最小限に抑えることができます。オブジェクトストレージへのバックアップは、上に構築されます "NetApp SnapMirror Cloudテクノロジ"。

> クラウドプロバイダ環境から直接実行してクラウドバックアップファイルを管理または変更すると、ファイルが破損し、構成がサポートされない可能性があります。

次の図は、各コンポーネント間の関係を示しています。



この図は、ボリュームをCloud Volumes ONTAPシステムにレプリケートしているところを示していますが、ボリュームはオンプレミスのONTAPシステムにもレプリケートできます。

バックアップの保管場所

バックアップは、バックアップのタイプに基づいて別の場所に格納されます。

- _Snapshotコピー_を、ソースの作業環境のソースボリュームに配置します。
- _replicated volumes_セカンダリストレージシステム（Cloud Volumes ONTAPまたはオンプレミスのONTAPシステム）に配置します。
- _バックアップコピー_は、BlueXPがクラウドアカウントに作成するオブジェクトストアに格納されます。クラスタ/作業環境ごとに1つのオブジェクトストアがあり、BlueXPではオブジェクトストアに「NetApp-backup-clusteruuid」という名前が付けられます。このオブジェクトストアは削除しないでください。

[+]
** AWSではBlueXPがそれに対応します "Amazon S3 ブロックのパブリックアクセス機能" を S3 バケットに配置します。

[+]
** Azureでは、Blobコンテナ用のストレージアカウントを持つ新規または既存のリソースグループを使用します。BlueXP "BLOB データへのパブリックアクセスをブロックします" デフォルトでは

[+]
** GCPでは、BlueXPはGoogle Cloud Storageバケット用のストレージアカウントを持つ新規または既存のプロジェクトを使用します。

[+]
** StorageGRIDでは、BlueXPはS3バケットに既存のテナントアカウントを使用します。

[+]
** ONTAP S3では、BlueXPはS3バケットに既存のユーザアカウントを使用します。

あとでクラスタのデスティネーションオブジェクトストアを変更する場合は、が必要になります "作業環境のBlueXPバックアップとリカバリの登録を解除します"をクリックし、新しいクラウドプロバイダ情報を使用してBlueXPのバックアップとリカバリを有効にします。

カスタマイズ可能なバックアップスケジュールと保持設定

作業環境でBlueXPのバックアップとリカバリを有効にすると、選択したすべてのボリュームが選択したポリシーを使用してバックアップされます。Snapshotコピー、レプリケートされたボリューム、およびバックアップファイルに対して別 々 のポリシーを選択できます。Recovery Point Objective（RPO；目標復旧時点）が異なる特定のボリュームに異なるバックアップポリシーを割り当てる場合は、BlueXPのバックアップとリカバリがアクティブ化されたあとに、そのクラスタ用の追加のポリシーを作成してそれらのポリシーを他のボリュームに割り当てることができます。

すべてのボリュームについて、毎時、毎日、毎週、毎月、および毎年のバックアップの組み合わせを選択できます。オブジェクトへのバックアップについては、3カ月、1年、7年間のバックアップと保持を提供するシステム定義のポリシーのいずれかを選択することもできます。ONTAP System Manager または ONTAP CLI を使用してクラスタに作成したバックアップ保護ポリシーも選択内容として表示されます。これには、カスタムのSnapMirrorラベルを使用して作成したポリシーも含まれ

> ボリュームに適用されるSnapshotポリシーには、レプリケーションポリシーとオブジェクトへのバックアップポリシーで使用するラベルのいずれかが含まれている必要があります。一致するラベルが見つからない場合、バックアップファイルは作成されません。たとえば、「週単位」のレプリケートされたボリュームとバックアップファイルを作成する場合は、「週単位」のSnapshotコピーを作成するSnapshotポリシーを使用する必要があります。

カテゴリまたは間隔のバックアップの最大数に達すると、古いバックアップは削除されるため、常に最新のバックアップが保持されます（古いバックアップはスペースを消費し続けません）。

を参照してください "バックアップスケジュール" 使用可能なスケジュールオプションの詳細については、を参照してください。

できることに注意してください "ボリュームのオンデマンドバックアップを作成する" スケジュールバックアップから作成されたバックアップファイルに加え、いつでも Backup Dashboard からアクセスできます。

> データ保護ボリュームのバックアップの保持期間は、ソースの SnapMirror 関係の定義と同じです。API を使用して必要に応じてこの値を変更できます。

バックアップファイルの保護設定

クラスタでONTAP 9.11.1以降を使用している場合は、オブジェクトストレージ内のバックアップを削除やランサムウェア攻撃から保護できます。各バックアップポリシーでは、特定の期間にわたってバックアップファイルに適用可能な_DataLockとRansomware Protection_の セクションを提供しています。

- _DataLock_は'バックアップファイルの変更または削除を防止します
- _Ransomware protection_scanバックアップファイルをスキャンして、バックアップファイルの作成時とバックアップファイルのデータのリストア時にランサムウェア攻撃が発生した証拠を探します。

スケジュールされたランサムウェア対策スキャンはデフォルトで有効になっています。スキャン頻度のデフォルト設定は7日間です。スキャンは最新のSnapshotコピーに対してのみ実行されます。スケジュールされたスキャンを無効にして、コストを削減できます。[Advanced Settings]ページのオプションを使用して、最新のSnapshotコピーに対してスケジュールされたランサムウェアスキャンを有効または無効にできます。有効にすると、スキャンはデフォルトで毎週実行されます。このスケジュールを数日または数週間に変更したり、無効にしたりすることで、コストを節約できます。

バックアップの保持期間は、バックアップスケジュールの保持期間と同じに14日を足したものです。たとえば、_WEEKLY_BACKUPに_5_Copiesを適用すると、各バックアップファイルが5週間ロックされます。_6_個のコピーを保持したMonthly _バックアップは、各バックアップ・ファイルを6か月ロックします。

バックアップデスティネーションがAmazon S3、Azure Blob、NetApp StorageGRID の場合、現在サポートされています。その他のストレージプロバイダの送信先は今後のリリースで追加される予定です。

詳細については、次の情報を参照してください。

- "DataLockとランサムウェア対策の仕組み"。
- "[Advanced Settingsページでランサムウェア対策オプションを更新する方法"]。

アーカイブストレージにバックアップを階層化する場合は、DataLockを有効にできません。

古いバックアップファイル用のアーカイブストレージ

特定のクラウドストレージを使用している場合、一定期間経過した古いバックアップファイルを低コストのストレージクラス/アクセス階層に移動できます。また、標準のクラウドストレージに書き込まれることなく、バックアップファイルをすぐにアーカイブストレージに送信することもできます。DataLockを有効にした場合は、アーカイブストレージを使用できません。

- AWS では、バックアップは _Standard_storage クラスから開始し、 30 日後に _Standard-Infrequent Access_storage クラスに移行します。

  クラスタでONTAP 9.10.1以降を使用している場合は、BlueXPのバックアップとリカバリ用UIで、一定の日数が経過したら古いバックアップを_S3 Glacier_or_S3 Glacier Deep Archive_storageに階層化してコストをさらに最適化できます。 "AWS アーカイブストレージの詳細は、こちらをご覧ください"。

- Azure では、バックアップは _COOL アクセス層に関連付けられます。

  クラスタでONTAP 9.10.1以降を使用している場合は、コストをさらに最適化するために、BlueXPのバックアップとリカバリのUIで、古いバックアップを_azure Archive_storageに階層化することができます。 "Azure アーカイブストレージの詳細については、こちらをご覧ください"。

- GCP では、バックアップは _Standard_storage クラスに関連付けられます。

  クラスタでONTAP 9.12.1以降を使用している場合は、コストをさらに最適化するために、BlueXPのバックアップとリカバリのUIで、古いバックアップを_Archive_storageに階層化することができます。 "Googleアーカイブストレージの詳細をご覧ください"。

- StorageGRID では、バックアップは _Standard_storage クラスに関連付けられます。

  オンプレミスクラスタがONTAP 9.12.1以降を使用しており、StorageGRID システムが11.4以降を使用している場合は、古いバックアップファイルを特定の日数後にパブリッククラウドアーカイブストレージにアーカイブできます。現在、AWS S3 Glacier Deep ArchiveまたはAzure Archiveストレージ階層がサポー

トされています。 "StorageGRID からバックアップファイルをアーカイブする方法の詳細については、こちらをご覧ください"。

を参照してください "アーカイブストレージの設定" 古いバックアップファイルのアーカイブの詳細については、を参照してください。

FabricPool 階層化ポリシーに関する考慮事項

バックアップするボリュームがFabricPoolアグリゲートにあり、そのボリュームに以外の階層化ポリシーが割り当てられている場合は、注意が必要な事項がいくつかあります `none`：

- FabricPool 階層化ボリュームの最初のバックアップでは、（オブジェクトストアからの）ローカルおよびすべての階層化データを読み取る必要があります。バックアップ処理では、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は「再加熱」されません。

  この処理を実行すると、クラウドプロバイダからデータを読み取るコストが 1 回だけ増加する可能性があります。

  - 2 回目以降のバックアップは増分バックアップとなるため、影響はありません。
  - ボリュームの作成時に階層化ポリシーが割り当てられていた場合、この問題は表示されません。
- を割り当てる前に、バックアップによる影響を考慮してください `all` ボリュームへの階層化ポリシー。データはすぐに階層化されるため、BlueXPのバックアップとリカバリでは、ローカル階層ではなくクラウド階層からデータが読み取られます。バックアップの同時処理は、クラウドオブジェクトストレージへのネットワークリンクを共有するため、ネットワークリソースが最大限まで使用されなくなった場合にパフォーマンスが低下する可能性があります。この場合、複数のネットワークインターフェイス（ LIF ）をプロアクティブに設定して、この種類のネットワークの飽和を軽減することができます。

保護対策を計画しましょう

BlueXPのバックアップとリカバリサービスでは、ソースボリュームのコピーを最大3つ作成してデータを保護できます。ボリュームでこのサービスを有効にするときに選択できるオプションは多数あるため、準備ができるように選択内容を確認する必要があります。

次のオプションについて説明します。

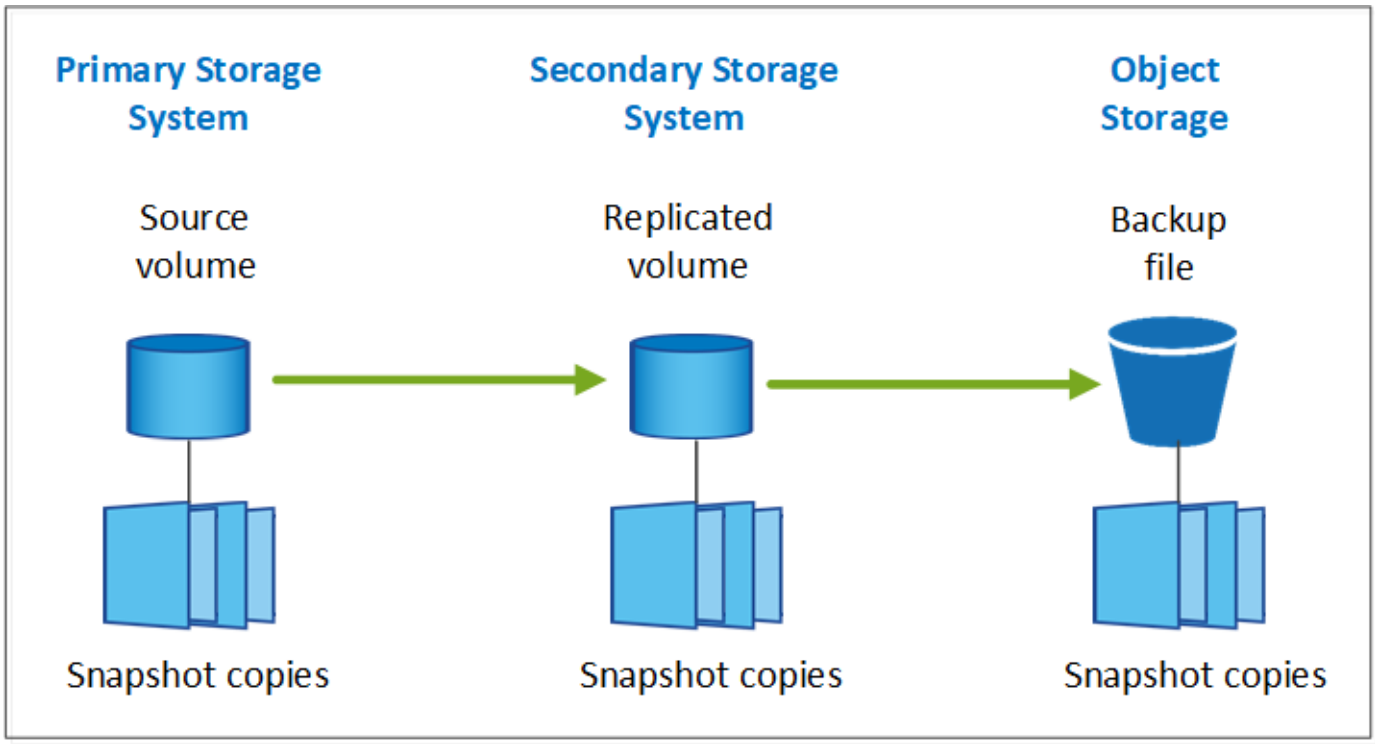
- 使用する保護機能（Snapshotコピー、レプリケートされたボリューム、クラウドへのバックアップ
- 使用するバックアップアーキテクチャ（ボリュームのカスケードバックアップまたはファンアウトバックアップ
- デフォルトのバックアップポリシーを使用するか、カスタムポリシーを作成する必要があるか
- 開始前にサービスでクラウドバケットを作成するか、オブジェクトストレージコンテナを作成するか
- 使用しているBlueXP Connector導入モード（標準モード、制限モード、プライベートモード）

どの保護機能を使用しますか

使用する機能を選択する前に、各機能の機能と提供する保護の種類について簡単に説明します。

バックアップタイプ	説明
スナップショット	ソースボリューム内のボリュームのポイントインタイムイメージをSnapshotコピーとして読み取り専用で作成します。Snapshotコピーを使用して、個 々 のファイルをリカバリしたり、ボリュームの内容全体をリストアしたりできます。
レプリケーション	データのセカンダリコピーを別のONTAPストレージシステムに作成し、セカンダリデータを継続的に更新します。データは最新の状態に維持され、必要なときにいつでも利用できます。
クラウドバックアップ	保護や長期アーカイブの目的で、データのバックアップをクラウドに作成します。必要に応じて、ボリューム、フォルダ、または個 々 のファイルをバックアップから同じ作業環境または異なる作業環境にリストアできます。

スナップショットはすべてのバックアップ方法の基礎であり、バックアップおよびリカバリサービスを使用するために必要です。Snapshot コピーは、ボリュームの読み取り専用のポイントインタイムイメージです。イメージには Snapshot コピーが最後に作成されたあとに発生したファイルへの変更だけが記録されるため、ストレージスペースは最小限しか消費せず、パフォーマンスのオーバーヘッドもわずかです。次の図に示すように、ボリューム上に作成されたSnapshotコピーを使用して、レプリケートされたボリュームとバックアップファイルがソースボリュームに加えられた変更と同期されます。



レプリケートされたボリュームを別のONTAPストレージシステムに作成し、バックアップファイルをクラウドに作成することもできます。または、レプリケートされたボリュームまたはバックアップファイルを作成するだけで選択できます。

要約すると、ONTAP作業環境内のボリュームに対して作成できる有効な保護フローは次のとおりです。

- ソースボリューム→ Snapshotコピー→レプリケートされたボリューム→バックアップファイル
- ソースボリューム→ Snapshotコピー→バックアップファイル
- ソースボリューム→ Snapshotコピー→レプリケートされたボリューム

レプリケートされたボリュームまたはバックアップファイルの初回作成時には、ソースデータのフルコピーが含まれます。これは_ベースライン転送_と呼ばれます。以降の転送では、ソースデータの差分コピー（Snapshot）のみが含まれます。

各種バックアップ方法の比較

次の表に、3つのバックアップ方法の一般的な比較を示します。オブジェクトストレージスペースは通常、オンプレミスのディスクストレージよりも安価ですが、クラウドからデータを頻繁にリストアする可能性がある場合は、クラウドプロバイダからの出力料金によって、削減量の一部を削減できます。クラウドのバックアップファイルからデータをリストアする頻度を特定する必要があります。

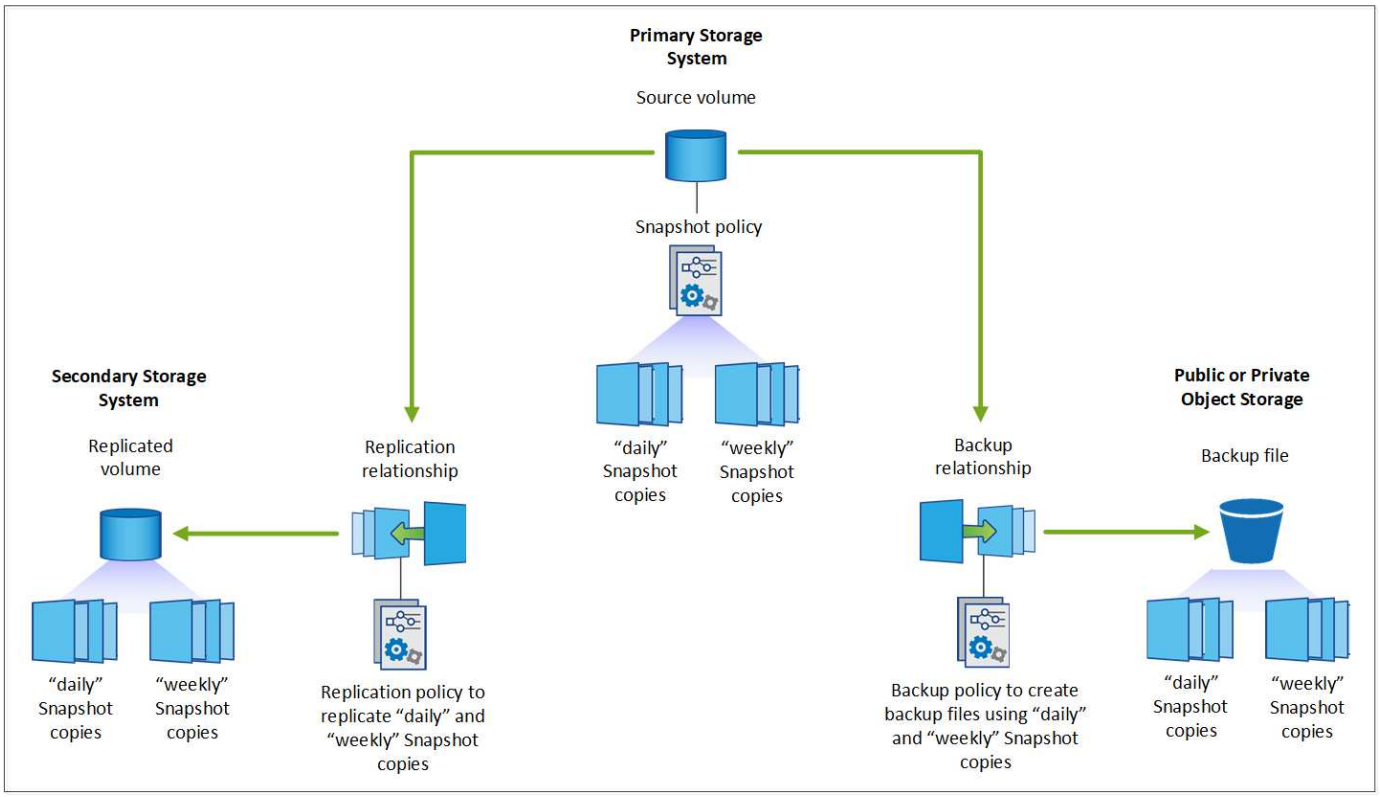
クラウドストレージでは、この条件に加えて、DataLockおよびRansomware Protection機能を使用する場合は追加のセキュリティオプションが提供されます。また、古いバックアップファイル用のアーカイブストレージクラスを選択することで、さらにコストを削減できます。 "DataLockとランサムウェアによる保護の詳細をご確認ください" および "アーカイブストレージの設定"。

バックアップタイプ	バックアップ速度	バックアップコスト	リストア速度	リストアコスト
スナップショット	高	低（ディスクスペース）	高	低
レプリケーション	中	中（ディスクスペース）	中	中（ネットワーク）
クラウドバックアップ	低	低（オブジェクトスペース）	低	高額（プロバイダ料金）

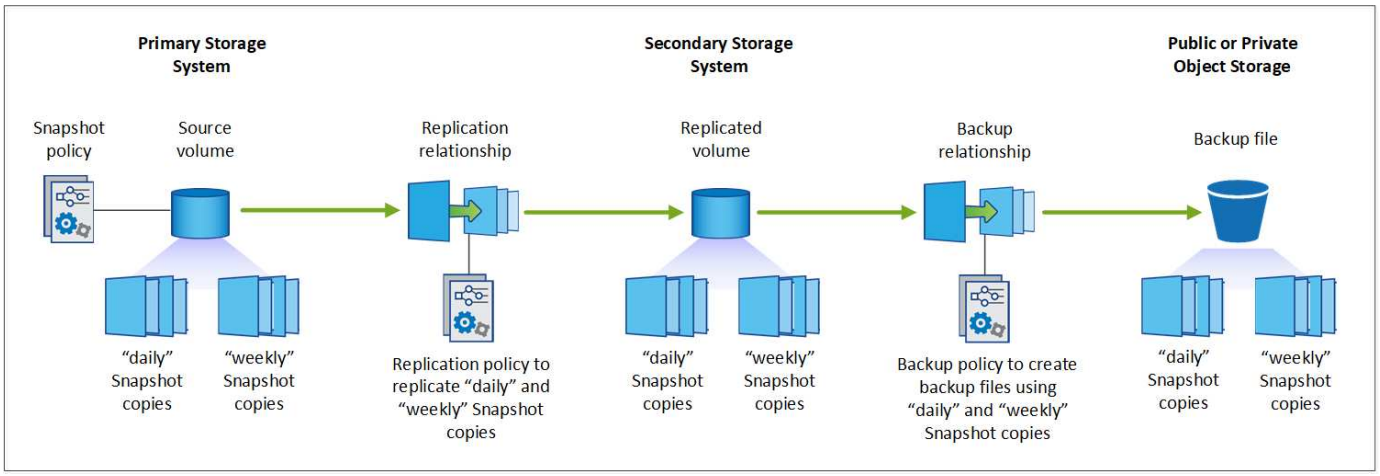
使用するバックアップアーキテクチャ

レプリケートされたボリュームとバックアップファイルの両方を作成する場合は、ファンアウトアーキテクチャまたはカスケードアーキテクチャを選択してボリュームをバックアップできます。

ファンアウト*アーキテクチャは、Snapshotコピーをデスティネーションストレージシステムとクラウド内のバックアップオブジェクトの両方に個別に転送します。



カスケード*アーキテクチャでは、Snapshotコピーが最初にデスティネーションストレージシステムに転送され、次にそのコピーがクラウド内のバックアップオブジェクトに転送されます。



さまざまなアーキテクチャの選択肢の比較

次の表は、ファンアウトアーキテクチャとカスケードアーキテクチャの比較を示しています。

ファンアウト	カスケード
Snapshotコピーが2つの異なるシステムに送信されるため、ソースシステムのパフォーマンスへの影響が小さい	Snapshotコピーは1回だけ送信されるため、ソースストレージシステムのパフォーマンスへの影響が少なくなります
ポリシー、ネットワーク、ONTAPの設定はすべてソースシステムで実行されるため、セットアップが簡単です	ネットワークとONTAPの設定も、セカンダリシステムから行う必要があります。

Snapshotコピー、レプリケーション、バックアップにデフォルトのポリシーを使用するか

NetAppのデフォルトポリシーを使用してバックアップを作成することも、カスタムポリシーを作成することもできます。アクティブ化ウィザードを使用してボリュームのバックアップとリカバリサービスを有効にする場合は、デフォルトのポリシーと、作業環境にすでに存在するその他のポリシー（Cloud Volumes ONTAPシステムまたはオンプレミスのONTAPシステム）を選択できます。既存のポリシーとは異なるポリシーを使用する場合は、アクティブ化ウィザードの開始前または使用中にポリシーを作成できます。

- デフォルトのSnapshotポリシーは、hourly、daily、およびweeklyのSnapshotコピーを作成し、hourlyのSnapshotコピーを6個、dailyを2個、weeklyを2個保持します。
- デフォルトのレプリケーションポリシーでは、日単位Snapshotコピーと週単位Snapshotコピーがレプリケートされ、日単位Snapshotコピーは7個、週単位Snapshotコピーは52個保持されます。
- デフォルトのバックアップポリシーでは、日単位Snapshotコピーと週単位Snapshotコピーがレプリケートされ、日単位Snapshotコピーは7個、週単位Snapshotコピーは52個保持されます。

レプリケーションまたはバックアップのカスタムポリシーを作成する場合は、ポリシーラベル（「daily」や「weekly」など）がSnapshotポリシーのラベルと一致している必要があります。一致していないと、レプリケートされたボリュームとバックアップファイルは作成されません。

BlueXPのバックアップとリカバリのUIで、Snapshot、レプリケーション、オブジェクトストレージへのバックアップポリシーを作成できます。の項を参照してください "新しいバックアップポリシーを追加しています" を参照してください。

BlueXPのバックアップリカバリを使用してカスタムポリシーを作成するだけでなく、System ManagerまたはONTAPコマンドラインインターフェイス（CLI）を使用することもできます。

"System Managerを使用してSnapshotポリシーを作成する"
"ONTAP CLIを使用したSnapshotポリシーの作成"
"System Managerを使用してレプリケーションポリシーを作成します"
"ONTAP CLIを使用してレプリケーションポリシーを作成します"
"System Managerを使用してバックアップポリシーを作成"
"ONTAP CLIを使用してバックアップポリシーを作成します"

注： System Managerを使用している場合は、レプリケーションポリシーのポリシータイプとして* Asynchronous を選択し、オブジェクトポリシーにバックアップする場合は Asynchronous と Back up to cloud *を選択します。

ここでは、カスタムポリシーを作成する場合に役立つONTAP CLIコマンドの例をいくつか示します。として_admin_vserver（Storage VM）を使用する必要があります `<vserver_name>` を参照してください。

Policy概要の略	コマンドを実行します
単純なSnapshotポリシー	`snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly`
クラウドへのシンプルなバックアップ	`snapmirror policy create -policy <policy_name> -transfer -priority normal -vserver <vserver_name> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

Policy概要の略	コマンドを実行します
DataLockとランサムウェア対策でクラウドにバックアップ	`snapmirror policy create -policy CloudBackupService-Enterprise -snapshot-lock-mode enterprise -vserver <vserver_name>` `snapmirror policy add-rule -policy CloudBackupService-Enterprise -retention-period 30days`
アーカイブストレージクラスを使用したクラウドへのバックアップ	`snapmirror policy create -vserver <vserver_name> -policy <policy_name> -archive-after-days <days> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`
別のストレージシステムへのシンプルなレプリケーション	`snapmirror policy create -policy <policy_name> -type async-mirror -vserver <vserver_name>` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

クラウドへのバックアップ関係に使用できるのはバックアップポリシーのみです。

ポリシーはどこに配置されていますか？

バックアップポリシーは、使用するバックアップアーキテクチャ（ファンアウトまたはカスケード）に応じてさまざまな場所に配置されます。レプリケーションポリシーとバックアップポリシーは同じようには設計されていません。2つのONTAPストレージシステムとオブジェクトへのバックアップでは、ストレージプロバイダがデスティネーションとして使用されるためです。

- Snapshotポリシーは常にプライマリストレージシステムに存在します。
- レプリケーションポリシーは常にセカンダリストレージシステムに存在します。
- オブジェクトへのバックアップポリシーは、ソースボリュームが配置されているシステム上に作成されます。これは、ファンアウト構成の場合はプライマリクラスタ、カスケード構成の場合はセカンダリクラスタです。

これらの違いを表に示します。

アーキテクチャ	スナップショットポリシー	レプリケーションポリシー	バックアップポリシー
ファンアウト	プライマリ	セカンダリ	プライマリ
カスケード	プライマリ	セカンダリ	セカンダリ

そのため、カスケードアーキテクチャを使用するときにカスタムポリシーを作成する場合は、レプリケートされたボリュームが作成されるセカンダリシステムにレプリケーションポリシーとオブジェクトへのバックアップポリシーを作成する必要があります。ファンアウトアーキテクチャを使用するときにカスタムポリシーを作成する場合は、複製されたボリュームが作成されるセカンダリシステムでレプリケーションポリシーを作成し、プライマリシステムでオブジェクトポリシーにバックアップする必要があります。

すべてのONTAPシステムに存在するデフォルトのポリシーを使用している場合は、すべて設定されていま

す。

独自のオブジェクトストレージコンテナを作成しますか

作業環境のオブジェクトストレージにバックアップファイルを作成すると、デフォルトでは、バックアップおよびリカバリサービスによって、設定したオブジェクトストレージアカウントにバックアップファイル用のコンテナ（バケットまたはストレージアカウント）が作成されます。AWSバケットまたはGCPバケットのデフォルトの名前は「netapp-backup-gp <uuid>」です。Azure BLOBストレージアカウントの名前は「netappbackup <uuid>」です。

特定のプレフィックスを使用したり、特別なプロパティを割り当てたりする場合は、オブジェクトプロバイダアカウントでコンテナを自分で作成できます。独自のコンテナを作成する場合は、アクティブ化ウィザードを開始する前にコンテナを作成する必要があります。コンテナは、ONTAPボリュームのバックアップファイルの格納専用に使用する必要があります。それ以外の目的に使用することはできません。バックアップアクティベーションウィザードは、選択したアカウントとクレデンシャル用にプロビジョニングされたコンテナを自動的に検出し、使用するコンテナを選択できるようにします。

バケットはBlueXPまたはクラウドプロバイダから作成できます。

- "BlueXPでAmazon S3バケットを作成"
- "BlueXPからAzure BLOBストレージアカウントを作成します"
- "BlueXPからGoogle Cloud Storageバケットを作成"

*注：*現時点では、StorageGRIDシステムまたはONTAP S3へのバックアップを作成するときに、独自のS3バケットを使用することはできません。

「netapp-backup-xxxxxx」以外のバケットプレフィックスを使用する場合は、コネクタIAMロールのS3権限を変更する必要があります。詳細については、AWS S3へのバックアップを作成する方法を参照してください。

詳細バケット設定

古いバックアップファイルをアーカイブストレージに移動する場合、またはDataLockおよびRansomware Protectionを有効にしてバックアップファイルをロックし、ランサムウェアの可能性がないかスキャンする場合は、特定の構成設定でコンテナを作成する必要があります。

- 現時点では、クラスタでONTAP 9.10.1以降のソフトウェアを使用している場合、独自のバケット上のアーカイブストレージはAWS S3ストレージでサポートされています。デフォルトでは、バックアップはS3_Standard_storageクラスで開始されます。適切なライフサイクルルールを使用してバケットを作成します。
  - バケットのスコープ全体のオブジェクトを30日後にS3_Standard-IA_に移動します。
  - 「smc_push_to_archive：true」タグのオブジェクトを_Glacier Flexible Retrieval_（旧S3 Glacier）に移動します。
- DataLockとランサムウェア対策は、クラスタでONTAP 9.11.1以降のソフトウェアを使用している場合はAWSストレージ、ONTAP 9.12.1以降のソフトウェアを使用している場合はAzureストレージでサポートされます。
  - AWSの場合、30日間の保持期間を使用してバケットのオブジェクトロックを有効にする必要があります。
  - Azureの場合は、バージョンレベルの変更不可をサポートするストレージクラスを作成する必要があります。

どの**BlueXP Connector**導入モードを使用していますか

すでにBlueXPを使用してストレージを管理している場合は、BlueXP Connectorがインストールされています。BlueXPのバックアップとリカバリで同じコネクタを使用する予定なら、準備は万端です。別のコネクタを使用する必要がある場合は、バックアップとリカバリの実装を開始する前に、コネクタをインストールする必要があります。

BlueXPには複数の導入モードが用意されており、ビジネスやセキュリティの要件に合わせてBlueXPを使用できます。_Standard modeは*BlueXP SaaS*レイヤを活用してすべての機能を提供しますが、*_restricted mode_and_private mode*は接続が制限されている組織で使用できます。

"BlueXPの導入モードの詳細については、こちらをご覧ください"。
"BlueXPの導入モードに関するビデオをご覧ください"。

完全なインターネット接続を備えたサイトのサポート

インターネットに完全に接続されたサイト（標準モード_または SaaSモード_とも呼ばれます）でBlueXPのバックアップとリカバリを使用する場合は、BlueXPで管理しているオンプレミスのONTAPシステムまたはCloud Volumes ONTAPシステムにレプリケートされたボリュームを作成できます。 また、サポートされている任意のクラウドプロバイダのオブジェクトストレージにバックアップファイルを作成できます。 "サポートされているバックアップ先の完全なリストを参照してください"。

有効なコネクタの場所のリストについては、バックアップファイルを作成するクラウドプロバイダの次のいずれかのバックアップ手順を参照してください。コネクタをLinuxマシンに手動でインストールするか、特定のクラウドプロバイダに導入する必要がある場合は、いくつかの制限事項があります。

- "Cloud Volumes ONTAP データを Amazon S3 にバックアップします"
- "オンプレミスの ONTAP データを Amazon S3 にバックアップ"
- "Cloud Volumes ONTAP データを Azure Blob にバックアップ"
- "オンプレミスの ONTAP データを Azure Blob にバックアップ"
- "Cloud Volumes ONTAP データを Google Cloud にバックアップ"
- "オンプレミスの ONTAP データを Google Cloud にバックアップ"
- "オンプレミスの ONTAP データを StorageGRID にバックアップ"
- "オンプレミスのONTAPをONTAP S3にバックアップ"

インターネット接続が制限されているサイトのサポート

BlueXPのバックアップとリカバリは、インターネット接続が制限されているサイト（_restricted mode_とも呼ばれます）でボリュームデータをバックアップするために使用できます。この場合は、制限されたリージョンにBlueXP Connectorを導入する必要があります。

- AWSの商用リージョンにインストールされているCloud Volumes ONTAP システムからAmazon S3にデータをバックアップできます。 "Cloud Volumes ONTAP データを Amazon S3 にバックアップします"。
- Azureの商用リージョンにインストールされているCloud Volumes ONTAP システムからAzure Blobにデータをバックアップできます。 "Cloud Volumes ONTAP データを Azure Blob にバックアップ"。

インターネットに接続されていないサイトをサポート

インターネットに接続されていないサイト（_private mode_or_dark_sitesとも呼ばれます）では、BlueXPのバックアップとリカバリを使用してボリュームデータをバックアップできます。この場合は、同じサイトのLinuxホストにBlueXP Connectorを導入する必要があります。

- ローカルのオンプレミスONTAP システムからローカルのStorageGRID システムにデータをバックアップできます。 "オンプレミスの ONTAP データを StorageGRID にバックアップ"。
- ローカルのオンプレミスONTAPシステムから、ローカルのオンプレミスONTAPシステムまたはS3オブジェクトストレージ用に構成されたCloud Volumes ONTAPシステムにデータをバックアップできます。 "オンプレミスのONTAPデータをONTAP S3にバックアップ"。
  ifdef：aws []

ONTAPボリュームのバックアップポリシーを管理します。

NetAppのデフォルトのバックアップポリシーを使用してバックアップを作成することも、カスタムポリシーを作成することもできます。ポリシーは、バックアップの頻度、バックアップが作成される時間、および保持されるバックアップファイルの数を制御します。

アクティブ化ウィザードを使用してボリュームのバックアップとリカバリサービスを有効にする場合は、デフォルトのポリシーと、作業環境にすでに存在するその他のポリシー（Cloud Volumes ONTAPシステムまたはオンプレミスのONTAPシステム）を選択できます。既存のポリシーとは異なるポリシーを使用する場合は、アクティブ化ウィザードの実行前または実行中にポリシーを作成できます。

デフォルトのバックアップポリシーについては、を参照してください。 "保護対策を計画しましょう"。

BlueXPのバックアップとリカバリでは、ONTAPデータのバックアップにSnapshot、レプリケーション、オブジェクトストレージへのバックアップの3種類が用意されています。ポリシーは、使用するアーキテクチャとバックアップのタイプに基づいて、さまざまな場所に配置されます。

アーキテクチャ	**Snapshot**ポリシーの格納場所	レプリケーションポリシーの格納場所	オブジェクトポリシーの格納場所へのバックアップ
ファンアウト	プライマリ	セカンダリ	プライマリ
カスケード	プライマリ	セカンダリ	セカンダリ

環境、設定、保護タイプに応じて、次のツールを使用してバックアップポリシーを作成します。

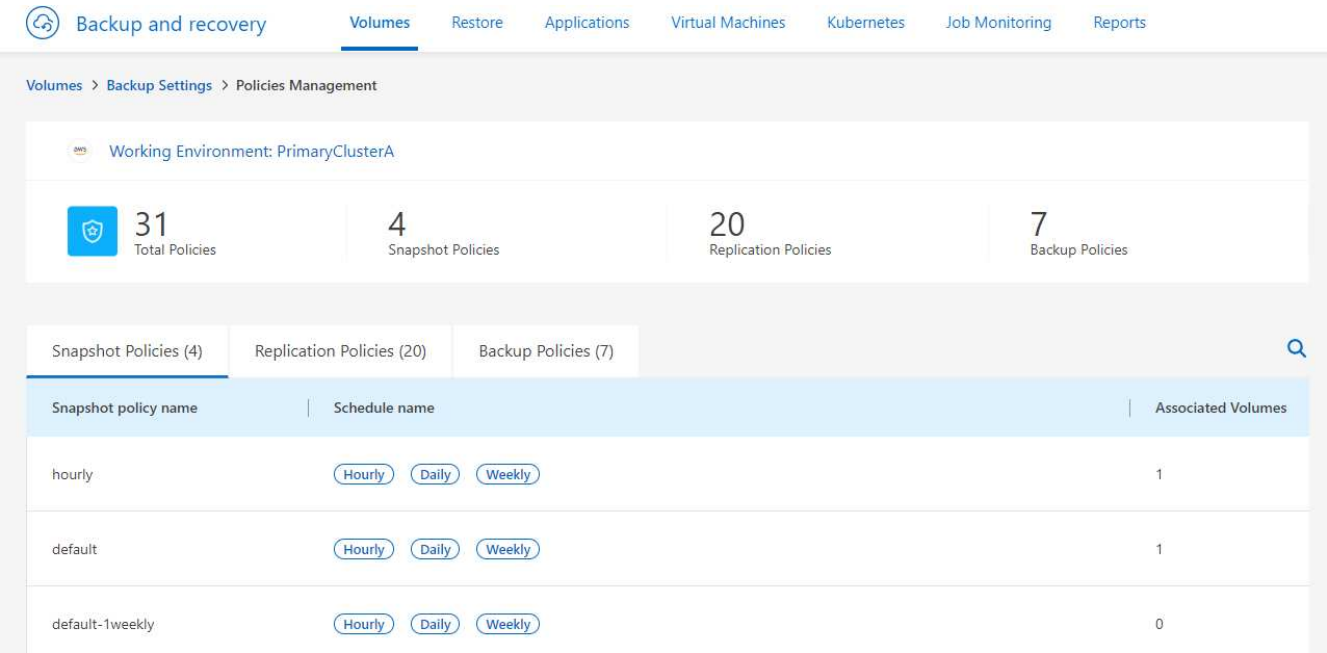
- BlueXPのUI
- System ManagerのUI
- ONTAP CLI

System Managerを使用している場合は、レプリケーションポリシーのポリシータイプとして* Asynchronous を選択し、オブジェクトポリシーにバックアップする場合は Asynchronous および Back up to cloud *を選択します。

作業環境のポリシーを表示する

1. BlueXP UIで、**[ボリューム]**>*[バックアップ設定]*を選択します。
2. [Backup Settings]ページで作業環境を選択し、**[Actions]***を選択します。 ••• アイコンをクリックし、[Policies management]*を選択します。

   [Policies]管理ページが表示されます。



   ページ"]

   Snapshotポリシーはデフォルトで表示されます。

3. 作業環境の他のポリシーを表示するには、**[レプリケーションポリシー]***または[バックアップポリシー]*を選択します。バックアップ計画に既存のポリシーを使用できる場合は、設定が完了します。特性の異なるポリシーが必要な場合は、このページから新しいポリシーを作成できます。

ポリシーの作成

Snapshotコピー、レプリケーション、オブジェクトストレージへのバックアップに関するポリシーを作成できます。

- Snapshotを開始する前にSnapshotポリシーを作成する
- [レプリケーションを開始する前にレプリケーションポリシーを作成する]
- [バックアップを開始する前に、オブジェクトストレージへのバックアップポリシーを作成する]

Snapshotを開始する前に**Snapshot**ポリシーを作成する

3-2-1戦略の一環として、*プライマリ*ストレージ・システム上にボリュームのSnapshotコピーを作成します。

ポリシー作成プロセスの一環として、スケジュールと保持を示すSnapshotラベルとSnapMirrorラベルを特定します。事前定義されたラベルを使用するか、独自のラベルを作成できます。

手順

1. BlueXP UIで、**[ボリューム]**>*[バックアップ設定]*を選択します。
2. [Backup Settings]ページで作業環境を選択し、**[Actions]***を選択します。 ••• アイコンをクリックし、[Policies management]*を選択します。

   [Policies]管理ページが表示されます。

3. [ポリシー]ページで、**[ポリシーの作成]**>*[Snapshotポリシーの作成]*を選択します。
4. ポリシー名を指定します。
5. Snapshotスケジュールを選択します。最大5つのラベルを設定できます。または、スケジュールを作成します。
6. スケジュールを作成する場合は、次の手順を実行します。
   a. 毎時、毎日、毎週、毎月、または毎年の頻度を選択します。
   b. スケジュールと保持を示すSnapshotラベルを指定します。
   c. スナップショットを作成するタイミングと頻度を入力します。
   d. Retention：保持するSnapshotの数を入力します。
7. 「 * Create * 」を選択します。

カスケードアーキテクチャを使用した**Snapshot**ポリシーの例

この例では、2つのクラスタを含むSnapshotポリシーを作成します。

1. クラスタ1：
   a. ポリシーページで[Cluster 1]を選択します。
   b. [Replication]セクションと[Backup to Object]ポリシーセクションは無視します。
   c. Snapshotポリシーを作成します。
2. クラスタ2：
   a. [Policy]ページで[Cluster 2]を選択します。
   b. [Snapshot policy]セクションは無視します。
   c. [Replication]および[Backup to]オブジェクトポリシーを設定します。

レプリケーションを開始する前にレプリケーションポリシーを作成する

3-2-1戦略には、別のストレージシステムにボリュームをレプリケートすることが含まれる場合があります。レプリケーションポリシーは*セカンダリ*ストレージシステムにあります。

手順

1. [ポリシー]ページで、**[ポリシーの作成]**>*[レプリケーションポリシーの作成]*を選択します。
2. [ポリシーの詳細]セクションで、ポリシー名を指定します。
3. 各ラベルの保持期間を示すSnapMirrorラベル（最大5つ）を指定します。
4. 転送スケジュールを指定します。

5. 「 * Create * 」を選択します。

バックアップを開始する前に、オブジェクトストレージへのバックアップポリシーを作成する

3-2-1の戦略には、ボリュームをオブジェクトストレージにバックアップすることが含まれます。

このストレージポリシーは、バックアップアーキテクチャに応じて、さまざまなストレージシステムの場所に配置されます。

- ファンアウト：プライマリストレージシステム
- カスケード：セカンダリストレージシステム

手順

1. [ポリシー管理]ページで、**[ポリシーの作成]**>*[バックアップポリシーの作成]*を選択します。
2. [ポリシーの詳細]セクションで、ポリシー名を指定します。
3. 各ラベルの保持期間を示すSnapMirrorラベル（最大5つ）を指定します。
4. 転送スケジュールやバックアップをアーカイブするタイミングなど、設定を指定します。
5. （オプション）一定の日数が経過した後に古いバックアップファイルを低コストのストレージクラスまたはアクセス階層に移動するには、* Archive オプションを選択し、データがアーカイブされるまでの経過日数を指定します。バックアップファイルをアーカイブストレージに直接送信するには、「**Archive after days**」に「 0 *」と入力します。

   "アーカイブストレージの設定に関する詳細情報"。

6. （オプション）バックアップが変更または削除されないように保護するには、*[DataLock & Ransomware protection]*オプションを選択します。

   クラスタでONTAP 9.11.1以降を使用している場合は、_DataLock_and_Ransomware protection_を設定することで、バックアップを削除から保護できます。

   "使用可能なDataLock設定の詳細については、こちらを参照してください"。

7. 「 * Create * 」を選択します。

ポリシーを編集します。

カスタムのSnapshot、レプリケーション、またはバックアップポリシーを編集できます。

バックアップポリシーの変更は、そのポリシーを使用しているすべてのボリュームに反映されます。

手順

1. [ポリシー管理]ページでポリシーを選択し、**[操作]** ••• アイコンをクリックし、*[ポリシーの編集]*を選択します。

   このプロセスは、レプリケーションポリシーとバックアップポリシーについても同じです。

2. [Edit Policy]ページで、変更を行います。

3. [保存（ Save ）] を選択します。

ポリシーを削除する

どのボリュームにも関連付けられていないポリシーも削除できます。

ボリュームに関連付けられているポリシーを削除する場合は、先にボリュームからポリシーを削除する必要があります。

手順

1. [ポリシー管理]ページでポリシーを選択し、**[操作]** ••• アイコンをクリックし、*[Snapshotポリシーの削除]*を選択します。
2. 「 * 削除」を選択します。

詳細については、こちらをご覧ください

System ManagerまたはONTAP CLIを使用してポリシーを作成する手順については、以下を参照してください。

"System Managerを使用してSnapshotポリシーを作成する"
"ONTAP CLIを使用したSnapshotポリシーの作成"
"System Managerを使用してレプリケーションポリシーを作成します"
"ONTAP CLIを使用してレプリケーションポリシーを作成します"
"System Managerを使用してオブジェクトストレージポリシーへのバックアップを作成する"
"ONTAP CLIを使用したオブジェクトストレージポリシーへのバックアップの作成"

オブジェクトへのバックアップポリシーのオプション

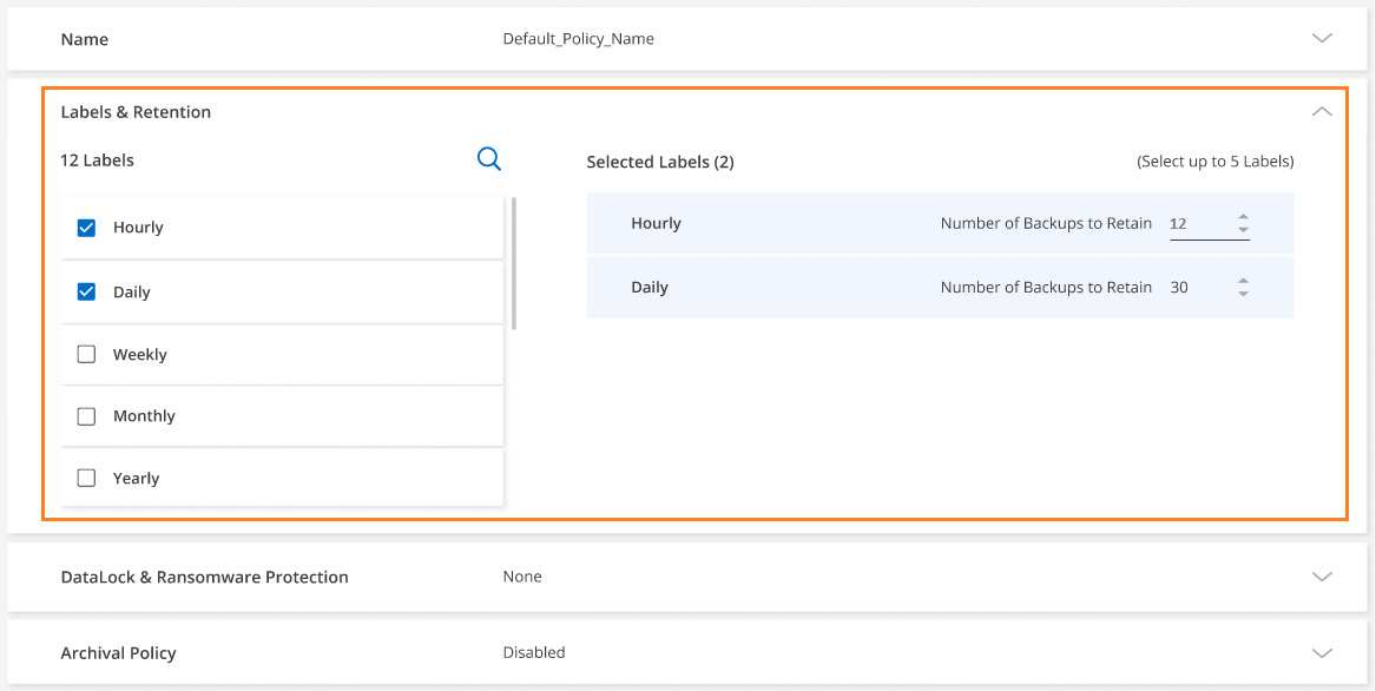
BlueXPのバックアップとリカバリでは、オンプレミスのONTAPシステムとCloud Volumes ONTAPシステムのさまざまな設定を使用してバックアップポリシーを作成できます。

> これらのポリシー設定は、オブジェクトストレージへのバックアップにのみ関連します。これらの設定は、Snapshotポリシーやレプリケーションポリシーには影響しません。Snapshotとレプリケーションについても、今後同様のポリシー設定が追加される予定です。

バックアップスケジュールのオプション

BlueXPのバックアップとリカバリでは、作業環境（クラスタ）ごとに一意のスケジュールで複数のバックアップポリシーを作成できます。RPO（目標復旧時点）が異なるボリュームには、異なるバックアップポリシーを割り当てることができます。

各バックアップポリシーには、バックアップファイルに適用可能な_Labels & Retention__というセクションがあります。ボリュームに適用されるSnapshotポリシーは、BlueXPのバックアップとリカバリで認識されるポリシーのいずれかである必要があります。そうでない場合、バックアップファイルは作成されません。



スケジュールには、ラベルと保持の値の2つの部分があります。

- 「* label *」は、ボリュームからバックアップファイルを作成（または更新）する頻度を定義します。次のタイプのラベルを選択できます。
  - 1つまたは* hourly 、 daily 、 weekly 、 monthly *の組み合わせを選択できます。 および*年単位*の期間。
  - システム定義のポリシーの中から、3カ月、1年、7年のバックアップと保持を提供するポリシーを1つ選択できます。
  - ONTAP System ManagerまたはONTAP CLIを使用してクラスタにカスタムのバックアップ保護ポリシーを作成した場合は、作成したポリシーを1つ選択できます。
- 「* retention *」の値は、各ラベル（期間）に保持するバックアップ・ファイルの数を定義します。カテゴリまたは間隔内で最大数のバックアップに達すると、古いバックアップは削除されるため、常に最新のバックアップが保持されます。これにより、廃止されたバックアップではクラウドのスペースが消費され続けることがないため、ストレージコストも削減されます。

たとえば、週7回*、月12回*のバックアップを作成するバックアップ・ポリシーを作成したとします。

- ボリュームのバックアップファイルは、週ごと、月ごとに1つずつ作成されます
- 8週間目には、最初の週次バックアップが削除され、8週間の新しい週次バックアップが追加されます（最大7週間ごとのバックアップを保持）。
- 13カ月目には、最初の月単位のバックアップが削除され、13カ月分に新しい月単位のバックアップが追加されます（最大12個の月単位のバックアップを保持）。

毎年のバックアップは、オブジェクトストレージに転送されたあとにソースシステムから自動的に削除されます。このデフォルト動作は変更できます "[詳細設定ページで設定します"] を参照してください。

DataLockとランサムウェア対策のオプション

BlueXPのバックアップとリカバリは、DataLockとランサムウェア対策をボリュームのバックアップに提供し

ます。これらの機能を使用すると、バックアップファイルをロックしてスキャンし、バックアップファイルでランサムウェアの可能性を検出できます。この設定はオプションで、クラスタのボリュームバックアップの保護を強化する場合にバックアップポリシーで定義できます。

これらの機能はどちらもバックアップファイルを保護するため、ランサムウェア攻撃がバックアップに試みられた場合にデータをリカバリするための有効なバックアップファイルを常に保持できます。また、バックアップを一定期間ロックして保持する必要がある規制要件にも対応すると便利です。[DataLock and Ransomware Protection]オプションを有効にすると、BlueXPのバックアップとリカバリのアクティブ化でプロビジョニングされるクラウドバケットでオブジェクトのロックとオブジェクトのバージョン管理が有効になります。

"詳細については、DataLockとRansomwareによる保護ブログをご覧ください"。

この機能では、ソースボリュームは保護されません。保護されるのは、ソースボリュームのバックアップのみです。ネットアップのソリューションを使用 "Cloud Insights およびCloud Secure"、またはの一部 "ONTAP が提供するアンチランサムウェア防御" ソースボリュームを保護します。

- DataLockとRansomware Protectionを使用する場合は、最初のバックアップポリシーを作成し、そのクラスタに対してBlueXPのバックアップとリカバリをアクティブ化するときに有効にすることができます。この機能は、BlueXPのバックアップとリカバリの詳細設定を使用してあとで有効にすることができます。
- DataLockとRansomware Protectionは、コスト削減のためにクラスタを設定したあとに無効にすることができます。
- BlueXPがボリュームデータをリストアするときにバックアップファイルをスキャンしてランサムウェアを検出すると、クラウドプロバイダからバックアップファイルの内容にアクセスするための追加の出力コストが発生します。

DataLockとは

DataLockは、バックアップファイルが一定期間変更または削除されないように保護します。これは_不変ストレージ_とも呼ばれます。この機能では、オブジェクトストレージプロバイダのテクノロジを「オブジェクトロック」に使用します。 バックアップファイルがロック（および保持）される期間は、DataLock保持期間と呼ばれます。定義したバックアップポリシーのスケジュールと保持設定に加え、14日間のバッファに基づいて設定されます。30日未満のDataLock保持ポリシーは、最小30日に切り上げられます。

古いバックアップは、バックアップポリシーの保持期間が終了した後ではなく、DataLockの保持期間が終了した後に削除されることに注意してください。

この機能の例をいくつか見てみましょう。

- 月単位のバックアップスケジュールを、保持期間が12の場合、各バックアップは、削除される12カ月（14日を足したもの）だけロックされます。
- 30日ごと、7週間ごと、12カ月ごとのバックアップを作成するバックアップポリシーを作成すると、ロックされた保持期間が3つになります。「30日ごと」のバックアップを44日間（30日と14日のバッファ）保持し、「7週間ごと」のバックアップを9週間（7週間と14日）保持し、「12カ月ごと」のバックアップを12カ月（さらに14日）保持します。
- 保持期間が24回の毎時バックアップスケジュールを作成する場合、バックアップは24時間ロックされると考えられることがあります。ただし、最低30日未満のため、各バックアップは44日間（30日と14日のバッファ）ロックされ、保持されます。

  この最後の例では、各バックアップファイルが44日間ロックされた場合、保持期間が時間あたり24回、保持ポリシーよりも多くのバックアップファイルが作成されます。通常、BlueXPのバックアップとリカバリ

で25番目のバックアップファイルが作成されると、最大保持数が24に維持されるように最も古いバックアップが削除されます（ポリシーに基づく）。この場合、DataLockの保持設定は、バックアップポリシーの保持設定よりも優先されます。これにより、バックアップファイルがオブジェクトストアに長期間保存されるため、ストレージのコストに影響する可能性があります。

ランサムウェアからの保護

ランサムウェア防御は、バックアップファイルをスキャンしてランサムウェア攻撃の兆候を探します。ランサムウェア攻撃の検出は、チェックサム比較を使用して実行されます。ランサムウェアの可能性が以前のバックアップファイルではなく新しいバックアップファイルで特定された場合、その新しいバックアップファイルはランサムウェア攻撃の兆候を示さない最新のバックアップファイルに置き換えられます。（ランサムウェア攻撃を受けていると特定されたファイルは、置き換えられてから1日後に削除されます）。

ランサムウェアスキャンは、バックアップとリストアのプロセスで3ポイント実行されます。

- バックアップファイルが作成されたとき。

  必要に応じてランサムウェアスキャンを有効または無効にすることができます。

  スキャンは、クラウドストレージに初めて書き込まれたとき、*次の*バックアップファイルが書き込まれたときに、バックアップファイルに対しては実行されません。たとえば、火曜日に週次バックアップのスケジュールが設定されている場合は、火曜日に14日にバックアップが作成されます。火曜日にもう1つバックアップが作成されます。ランサムウェアスキャンは、現時点で14日目からバックアップファイルで実行されています。

- バックアップファイルからデータをリストアする場合

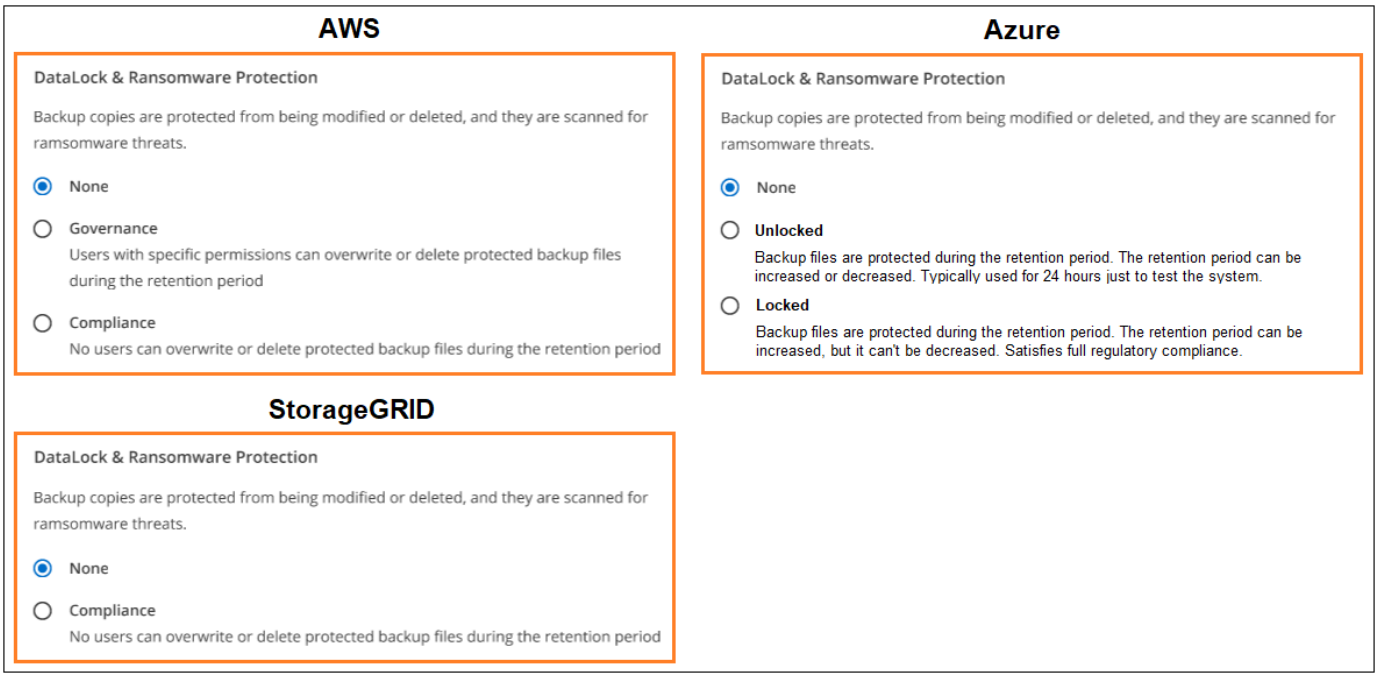
  バックアップファイルからデータをリストアする前にスキャンを実行するか、このスキャンをスキップするかを選択できます。

- 手動で実行する

  ランサムウェア攻撃からの保護スキャンは、いつでもオンデマンドで実行して、特定のバックアップファイルの健全性を確認できます。これは、特定のボリュームでランサムウェア問題 が実行されている場合に、そのボリュームのバックアップが影響を受けないことを確認するのに役立ちます。

DataLockとRansomware Protectionのオプション

各バックアップポリシーには、バックアップファイルに適用可能な_DataLockとRansomware Protection_に関する セクションが用意されています。



ランサムウェア対策スキャンはデフォルトで有効になっています。スキャン頻度のデフォルト設定は7日間です。スキャンは最新のSnapshotコピーに対してのみ実行されます。[Advanced Settings]ページのオプションを使用して、最新のSnapshotコピーに対するランサムウェアスキャンを有効または無効にできます。有効にすると、スキャンはデフォルトで7日ごとに実行されます。

を参照してください "[Advanced Settingsページでランサムウェア対策オプションを更新する方法"]。

各バックアップポリシーについて、次の設定から選択できます。

AWS

- なし（デフォルト）

  DataLock保護とランサムウェア防御は無効になっています。

- ガバナンス

  DataLockは_Governanceモードに設定されています。このモードでは、を使用します `s3:BypassGovernanceRetention` 権限（"以下を参照してください"）を使用すると、保持期間中にバックアップファイルを上書きまたは削除できます。ランサムウェア攻撃からの保護が有効

- コンプライアンス

  DataLockは_Compliion_modeに設定されており、保持期間中にユーザがバックアップファイルを上書きしたり削除したりすることはできません。ランサムウェア攻撃からの保護が有効

Azure

- なし（デフォルト）

  DataLock保護とランサムウェア防御は無効になっています。

- ロック解除

  バックアップファイルは保持期間中に保護されます。保持期間は増減できます。通常、システムのテストに24時間使用されます。ランサムウェア攻撃からの保護が有効

- ロックされています

  バックアップファイルは保持期間中に保護されます。保持期間は長くすることはできますが、短くすることはできません。完全なコンプライアンスを実現します。ランサムウェア攻撃からの保護が有効

StorageGRID

- なし（デフォルト）

  DataLock保護とランサムウェア防御は無効になっています。

- コンプライアンス

  DataLockは_Compliion_modeに設定されており、保持期間中にユーザがバックアップファイルを上書きしたり削除したりすることはできません。ランサムウェア攻撃からの保護が有効

サポートされている作業環境とオブジェクトストレージプロバイダ

以下のパブリッククラウドプロバイダとプライベートクラウドプロバイダでオブジェクトストレージを使用する際に、ONTAP ボリュームに対するDataLock保護とRansomware保護を有効にすることができます。クラウドプロバイダは今後のリリースで追加される予定です。

ソースの作業環境	バックアップファイルの保存先 ifdef：aws []
AWS の Cloud Volumes ONTAP	Amazon S3 endif：：aws[] ifdef：Azure []
Azure の Cloud Volumes ONTAP	Azure Blob の略 endif：：azure[] ifdef ::gcp[] endif：GCP []
オンプレミスの ONTAP システム	ifdef：aws [] Amazon S3 endif：：aws[] ifdef：Azure [] Azure Blob の略 endif：：azure[] ifdef ::gcp[] endif：GCP [] NetApp StorageGRID

要件

- AWSの場合：
  - クラスタでONTAP 9.11.1以降が実行されている必要があります
  - コネクタは、クラウドまたはオンプレミスに導入できます
  - 次のS3権限は、コネクタに権限を付与するIAMロールに含まれている必要があります。これらは、リソースarn：aws：s3：：：NetApp-backup-*」の「backupS3Policy」セクションに含まれています。

AWS S3権限

- S3 ： GetObjectVersionTagging
- S3 ： GetBucketObjectLockConfiguration
- S3：GetObjectVersionAcl
- S3 ： PutObjectTagging
- S3 ： DeleteObject
- S3 ： DeleteObjectTagging
- S3 ： GetObjectRetention
- S3 ： DeleteObjectVersionTagging
- S3 ： PutObject
- S3 ： GetObject
- S3 ： PutBucketObjectLockConfiguration
- S3 ： GetLifecycleConfiguration
- S3 ： GetBucketTagging
- S3 ： DeleteObjectVersion
- S3 ： ListBucketVersions
- S3 ： ListBucket
- S3 ： PutBucketTagging
- S3 ： GetObjectTagging
- S3 ： PutBucketVersioning
- S3 ： PutObjectVersionTagging
- S3 ： GetBucketVersioning
- S3 ： GetBucketAcl
- S3：Bypassガバナー 保持
- S3 ： PutObjectRetention
- S3 ： GetBucketLocation
- S3 ： GetObjectVersion

"必要な権限をコピーして貼り付けることができる、ポリシーの完全なJSON形式を表示します"。

- Azureの場合：
  - クラスタでONTAP 9.12.1以降が実行されている必要があります。
  - コネクタは、クラウドまたはオンプレミスに導入できます
- StorageGRID の場合：
  - クラスタでONTAP 9.11.1以降が実行されている必要があります

- StorageGRID システムで11.6.0.3以降が実行されている必要があります
- コネクタは、オンプレミスに導入する必要があります（インターネットにアクセスできるサイトまたはインターネットにアクセスできないサイトにインストールできます）。
- 次のS3権限は、コネクタに権限を提供するIAMロールに含める必要があります。

StorageGRID S3権限

- S3 ： GetObjectVersionTagging
- S3 ： GetBucketObjectLockConfiguration
- S3：GetObjectVersionAcl
- S3 ： PutObjectTagging
- S3 ： DeleteObject
- S3 ： DeleteObjectTagging
- S3 ： GetObjectRetention
- S3 ： DeleteObjectVersionTagging
- S3 ： PutObject
- S3 ： GetObject
- S3 ： PutBucketObjectLockConfiguration
- S3 ： GetLifecycleConfiguration
- S3 ： GetBucketTagging
- S3 ： DeleteObjectVersion
- S3 ： ListBucketVersions
- S3 ： ListBucket
- S3 ： PutBucketTagging
- S3 ： GetObjectTagging
- S3 ： PutBucketVersioning
- S3 ： PutObjectVersionTagging
- S3 ： GetBucketVersioning
- S3 ： GetBucketAcl
- S3 ： PutObjectRetention
- S3 ： GetBucketLocation
- S3 ： GetObjectVersion

制限事項

- バックアップポリシーでアーカイブストレージを設定している場合、DataLockとランサムウェアからの保護機能は使用できません。

- BlueXPのバックアップとリカバリをアクティブ化するときに選択するDataLockオプションを、そのクラスタのすべてのバックアップポリシーに使用する必要があります。
- 1つのクラスタで複数のDataLockモードを使用することはできません。
- DataLockを有効にすると、すべてのボリュームバックアップがロックされます。1つのクラスタに、ロックされたボリュームバックアップとロックされていないボリュームバックアップを混在させることはできません。
- DataLockとRansomwareによる保護は、DataLockとRansomwareによる保護が有効なバックアップポリシーを使用した新しいボリュームバックアップに適用されます。この機能は、[詳細設定]オプションを使用してあとで有効または無効にすることができます。
- FlexGroupボリュームでDataLockとランサムウェア対策を使用できるのは、ONTAP 9.13.1以降を使用している場合のみです。

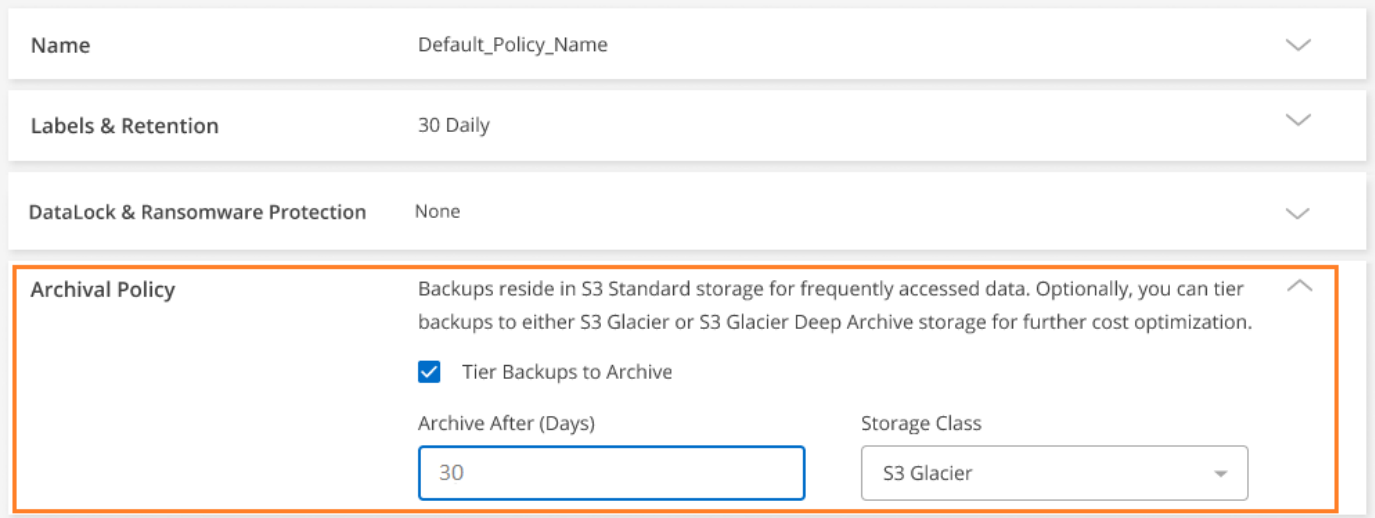
アーカイブストレージのオプション

AWS、Azure、Googleのクラウドストレージを使用している場合は、一定の日数が経過したら、古いバックアップファイルを低コストのアーカイブストレージクラスまたはアクセス階層に移動できます。また、標準のクラウドストレージに書き込まれることなく、バックアップファイルをすぐにアーカイブストレージに送信することもできます。「Archive after days」に「* 0 *」と入力するだけで、バックアップファイルをアーカイブストレージに直接送信できます。これは、クラウドバックアップからデータにアクセスする必要がほとんどないユーザや、テープの解決策にバックアップを取って代わるユーザに特に役立ちます。

アーカイブ層のデータには、必要なときにすぐにアクセスできないため、読み出しコストが高くなるため、バックアップファイルのアーカイブを決定する前に、バックアップファイルからデータをリストアする頻度を検討する必要があります。

- すべてのデータブロックをアーカイブクラウドストレージに送信するために「0」を選択した場合でも、メタデータブロックは常に標準のクラウドストレージに書き込まれます。
- DataLockを有効にしている場合、アーカイブストレージは使用できません。
- 「* 0 *日」（すぐにアーカイブ）を選択した後、アーカイブポリシーを変更することはできません。

各バックアップポリシーには、バックアップファイルに適用できる_Archival Policy_に関するセクションがあります。



- AWS では、バックアップは _Standard_storage クラスから開始し、 30 日後に _Standard-Infrequent Access_storage クラスに移行します。

  クラスタがONTAP 9.10.1以降を使用している場合は、古いバックアップをS3 Glacier Deep Archive_storageに階層化できます。 "AWS アーカイブストレージの詳細は、こちらをご覧ください"。

  - BlueXPのバックアップとリカバリをアクティブ化するときに最初のバックアップポリシーでアーカイブ階層を選択しない場合は、以降のポリシーでは_S3 Glacier_のみがアーカイブオプションになります。
  - 最初のバックアップポリシーで_S3 Glacier_を選択した場合は、そのクラスタの以降のバックアップポリシー用に_S3 Glacier Deep Archive_tierに変更できます。
  - 最初のバックアップポリシーで_S3 Glacier Deep Archive_を 選択した場合は、その階層がそのクラスタの今後のバックアップポリシーで使用できる唯一のアーカイブ階層になります。

- Azure では、バックアップは _COOL アクセス層に関連付けられます。

  ONTAP 9.10.1以降を使用しているクラスタでは、古いバックアップを_Azure Archive_storageに階層化できます。 "Azure アーカイブストレージの詳細については、こちらをご覧ください"。

- GCP では、バックアップは _Standard_storage クラスに関連付けられます。

  オンプレミスクラスタでONTAP 9.12.1以降を使用している場合は、コストをさらに最適化するために、BlueXPのバックアップとリカバリのUIで、古いバックアップを_Archive_storageに階層化することができます。 "Googleアーカイブストレージの詳細をご覧ください"。

- StorageGRID では、バックアップは _Standard_storage クラスに関連付けられます。

  オンプレミスクラスタがONTAP 9.12.1以降を使用しており、StorageGRID システムが11.4以降を使用している場合は、古いバックアップファイルをパブリッククラウドアーカイブストレージにアーカイブできます。

[+]
** AWSの場合、バックアップをAWS_S3 Glacier_or_S3 Glacier Deep Archive_storageに階層化できます。 "AWS アーカイブストレージの詳細は、こちらをご覧ください"。

[+]
** Azureの場合、古いバックアップを_Azure Archive_storageに階層化できます。 "Azure アーカイブストレージの詳細については、こちらをご覧ください"。

[+]
"StorageGRID からバックアップファイルをアーカイブする方法の詳細については、こちらをご覧ください"。

[Advanced Settings]ページでのオブジェクトストレージへのバックアップオプションの管理

[詳細設定]ページを使用して、ONTAPシステムごとにBlueXPのバックアップとリカバリをアクティブ化するときに設定した、クラスタレベルのオブジェクトストレージへのバックアップ設定を変更できます。「デフォルト」バックアップ設定として適用される一部の設定を変更することもできます。これには、オブジェクトストレージへのバックアップの転送速度の変更、Snapshotコピーの履歴をバックアップファイルとしてエクスポ

ートするかどうかの変更、作業環境でのランサムウェアスキャンの有効化または無効化が含まれます。

> これらの設定は、オブジェクトストレージへのバックアップでのみ使用できます。これらの設定は、Snapshotまたはレプリケーションの設定には影響しません。将来的には、同様のSnapshotとレプリケーションのクラスタレベルのレプリケーション設定が追加される予定です。

[Advanced Settings]ページでは、次のオプションを変更できます。

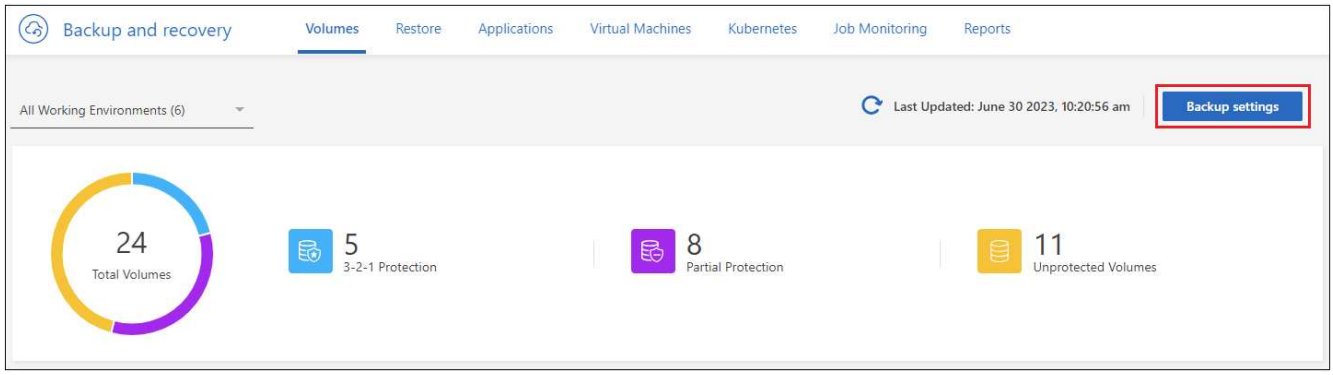
- [Max Transfer Rate]オプションを使用して、バックアップをオブジェクトストレージにアップロードするために割り当てられるネットワーク帯域幅の変更
  ifdef：aws []
- Snapshotコピー履歴をバックアップファイルとしてエクスポートし、将来のボリューム用の最初のベースラインバックアップファイルに含めるかどうかの変更
- 「年次」スナップショットをソースシステムから削除するかどうかを変更します
- 作業環境でのランサムウェアスキャンの有効化と無効化

クラスタレベルのバックアップの設定を表示します

それぞれの作業環境について、クラスタレベルのバックアップ設定を確認することができます。

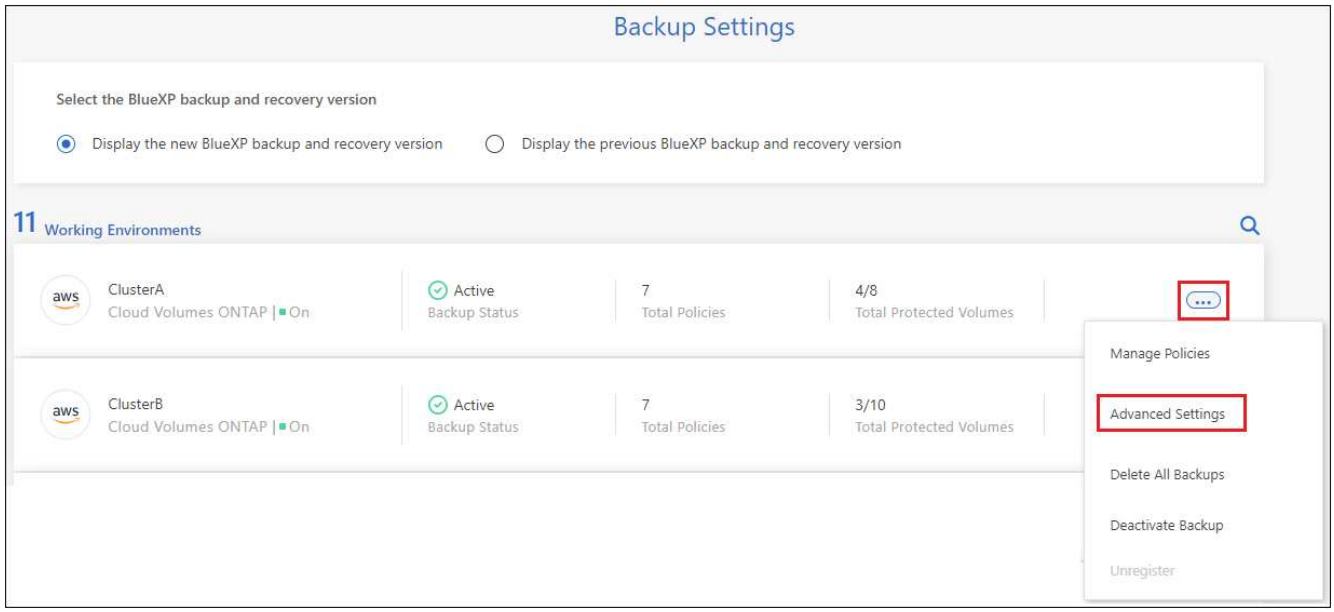
手順

1. BlueXPメニューから、*Protection > Backup and recovery*を選択します。
2. [* Volumes （ボリューム）] タブで、 [* Backup Settings （バックアップ設定）] を選択します。

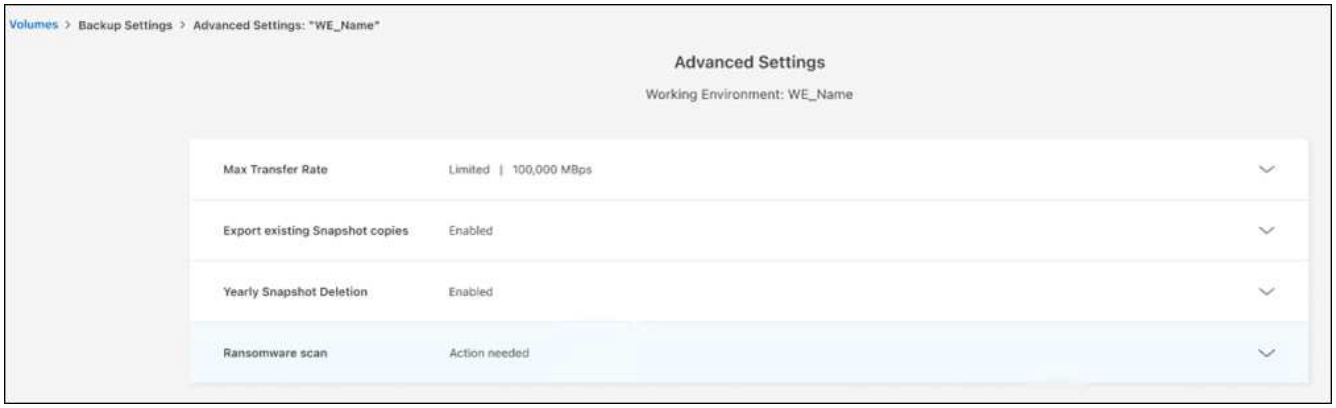


ボタンを示すスクリーンショット。"]

3. _ バックアップ設定ページ _ で、をクリックします ••• アイコン"] 作業環境では、*詳細設定*を選択します。



詳細設定ページには'その作業環境の現在の設定が表示されます



4. オプションを展開して変更を行います。

変更後のバックアップ処理では、すべて新しい値が使用されます。

一部のオプションは、ソースクラスタのONTAP のバージョン、およびバックアップの配置先クラウドプロバイダに基づいて使用できません。

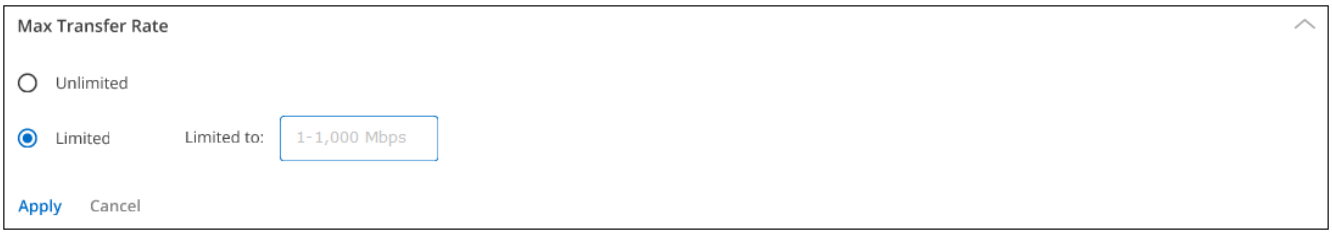
バックアップをオブジェクトストレージにアップロードするためのネットワーク帯域幅を変更する

作業環境でBlueXPのバックアップとリカバリをアクティブ化すると、デフォルトでは、ONTAP は無制限の帯域幅を使用して、作業環境内のボリュームからオブジェクトストレージにバックアップデータを転送できます。バックアップトラフィックが通常のユーザワークロードに影響している場合は、[Advanced Settings]ページの[Max Transfer Rate]オプションを使用して、転送中に使用されるネットワーク帯域幅を調整できます。

手順

1. [* Volumes （ボリューム）] タブで、 [* Backup Settings （バックアップ設定）] を選択します。
2. _ バックアップ設定ページ _ で、をクリックします ••• アイコン"] 作業環境では、*詳細設定*を選択します。

3. [Advanced Settings]ページで、[Max Transfer Rate]セクションを展開します。



4. 最大転送速度として1~1、000Mbpsの値を選択します。
5. [**Limited**]ラジオボタンを選択して使用できる最大帯域幅を入力するか、[*Unlimited *]を選択して制限がないことを示します。
6. * 適用 * を選択します。

この設定は、作業環境内のボリュームに対して設定可能な他のレプリケーション関係に割り当てられる帯域幅には影響しません。

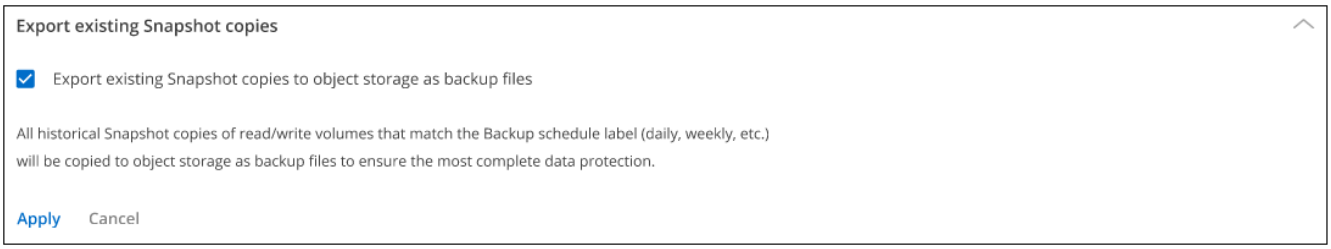
履歴**Snapshot**コピーをバックアップファイルとしてエクスポートするかどうかを変更します

この作業環境で使用しているバックアップスケジュールラベル（日次、週次など）に一致するボリュームのローカルSnapshotコピーがある場合は、それらの履歴Snapshotをバックアップファイルとしてオブジェクトストレージにエクスポートできます。これにより、古いSnapshotコピーをベースラインバックアップコピーに移動することで、クラウドでバックアップを初期化できます。

このオプションは、新しい読み取り/書き込みボリューム用の環境 の新しいバックアップファイルだけで、データ保護（DP）ボリュームではサポートされていません。

手順

1. [* Volumes （ボリューム）] タブで、 [* Backup Settings （バックアップ設定）] を選択します。
2. _ バックアップ設定ページ _ で、をクリックします ••• アイコン"] 作業環境では、*詳細設定*を選択します。
3. [詳細設定]ページで、*[既存のSnapshotコピーをエクスポート]*セクションを展開します。



4. 既存のSnapshotコピーをエクスポートするかどうかを選択します。
5. * 適用 * を選択します。

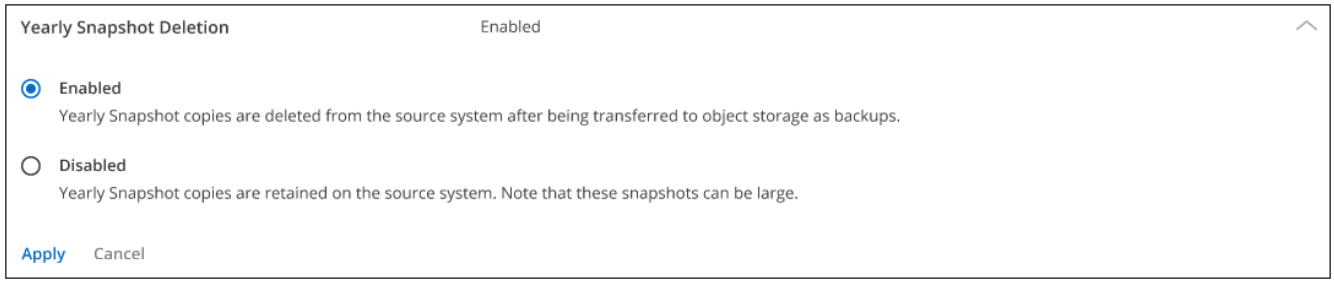
ソースシステムから「年次」スナップショットを削除するかどうかを変更します

いずれかのボリュームのバックアップポリシーで「年単位」のバックアップラベルを選択すると、作成されるSnapshotコピーのサイズが非常に大きくなります。デフォルトでは、これらの年単位のSnapshotは、オブ

ジェクトストレージに転送されたあとにソースシステムから自動的に削除されます。このデフォルト動作は、「年単位のSnapshotの削除」セクションから変更できます。

手順

1. [* Volumes （ボリューム）] タブで、 [* Backup Settings （バックアップ設定）] を選択します。
2. _ バックアップ設定ページ _ で、をクリックします ••• アイコン"] 作業環境では、*詳細設定*を選択します。
3. [Advanced Settings]ページで、*[Yearly Snapshot Deletion]*セクションを展開します。



ページの[Yearly Snapshots]エントリのスクリーンショット。"]

4. 毎年のSnapshotをソースシステムに保持する場合は、*[無効]*を選択します。
5. * 適用 * を選択します。

ランサムウェアスキャンを有効または無効にする

ランサムウェア対策スキャンはデフォルトで有効になっています。スキャン頻度のデフォルト設定は7日間です。スキャンは最新のSnapshotコピーに対してのみ実行されます。[Advanced Settings]ページのオプションを使用して、最新のSnapshotコピーに対するランサムウェアスキャンを有効または無効にできます。有効にすると、スキャンはデフォルトで7日ごとに実行されます。

ランサムウェアスキャンを有効にすると、クラウドプロバイダによっては追加料金が発生します。

を参照してください "ポリシーを管理する" ランサムウェア検出を実装するポリシーの管理の詳細については、を参照してください。

手順

1. [* Volumes （ボリューム）] タブで、 [* Backup Settings （バックアップ設定）] を選択します。
2. _ バックアップ設定ページ _ で、をクリックします ••• アイコン"] 作業環境では、*詳細設定*を選択します。
3. [Advanced Settings]ページで、*[Ransomware scan]*セクションを展開します。
4. Ransomware Scan *を有効または無効にします。

Cloud Volumes ONTAP データを Amazon S3 にバックアップします

Cloud Volumes ONTAP システムからAmazon S3へのボリュームデータのバックアップを開始するには、いくつかの手順を実行します。

クイックスタート

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

1 構成がサポートされていることを確認します

- AWSでCloud Volumes ONTAP 9.8以降を実行している（ONTAP 9.8P13以降を推奨）。
- バックアップを格納するストレージスペースに対する有効なクラウドプロバイダのサブスクリプションが必要です。
- に登録しておきます "BlueXP Marketplaceバックアップ製品"、 "AWS 年間契約"またはを購入したことが必要です "アクティブ化されます" ネットアップが提供するBlueXPバックアップ/リカバリのBYOLライセンス
- AWSにコネクタがインストールされている必要があります。
  - コネクタは、完全なインターネットアクセス(「標準モード」)または制限されたインターネット接続(「制限モード」)を備えたサイトにインストールできます。
  - BlueXP Connectorに権限を付与するIAMロールには、最新のからのS3権限が含まれています "BlueXPポリシー"。

2 **BlueXP**コネクタを準備します

AWSリージョンにすでにコネクタがデプロイされている場合は、設定は完了です。そうでない場合は、AWSにBlueXPコネクタをインストールしてCloud Volumes ONTAPデータをAWSにバックアップする必要があります。コネクタは、完全なインターネットアクセス(「標準モード」)または制限されたインターネット接続(「制限モード」)を備えたサイトにインストールできます。

BlueXPコネクタを準備します

3 ライセンス要件を確認

AWSとBlueXPの両方のライセンス要件を確認する必要があります。

[ライセンス要件を確認]。

4 ボリュームをレプリケートするための**ONTAP**ネットワークの要件を確認します

プライマリストレージシステムとセカンダリストレージシステムがONTAPのバージョンとネットワークの要件を満たしていることを確認します。

ボリュームをレプリケートするためのONTAPネットワークの要件を確認します。

5 **BlueXP**のバックアップとリカバリを有効にする

作業環境を選択し、右パネルのバックアップ/リカバリサービスの横にある*有効化>バックアップボリューム*をクリックします。

Cloud Volumes ONTAPでBlueXPのバックアップとリカバリを有効にする。

6 **ONTAP**ボリュームでバックアップをアクティブ化します

セットアップウィザードに従って、使用するレプリケーションポリシーとバックアップポリシー、およびバックアップするボリュームを選択します。

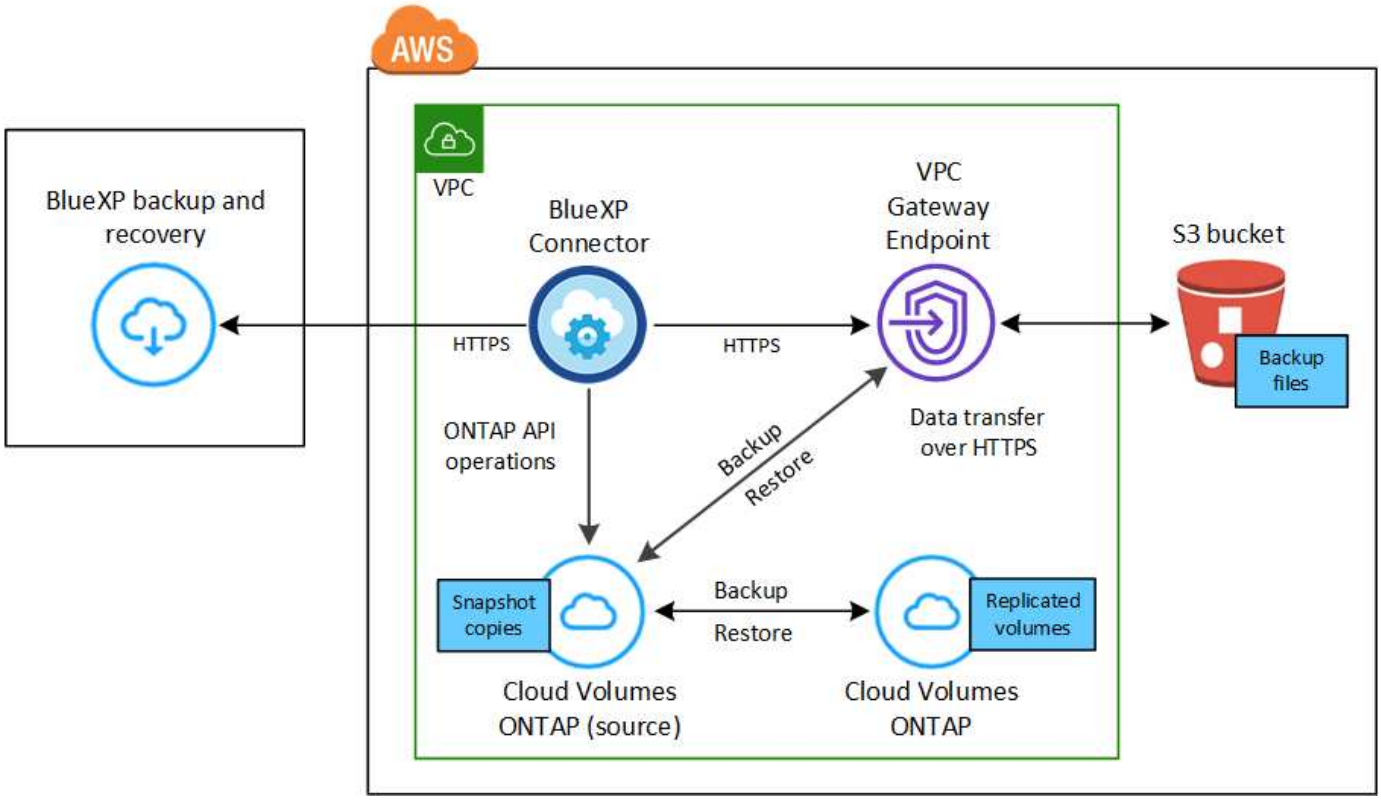
ONTAPボリュームでバックアップをアクティブ化します。

構成がサポートされていることを確認します

S3 へのボリュームのバックアップを開始する前に、次の要件を読み、サポートされている構成になっていることを確認してください。

次の図は、各コンポーネントとそれらの間の接続を示しています。

必要に応じて、パブリック接続またはプライベート接続を使用して、レプリケートされたボリュームのセカンダリONTAPシステムに接続することもできます。



VPCゲートウェイエンドポイントがすでにVPCに存在している必要があります。 "ゲートウェイエンドポイントの詳細については、こちらをご覧ください"。

サポートされる**ONTAP**のバージョン

ONTAP 9.8以上、ONTAP 9.8P13以降が推奨されます。

データ暗号化にお客様が管理するキーを使用するために必要な情報

デフォルトの Amazon S3 暗号化キーを使用する代わりに、アクティブ化ウィザードでお客様が管理する

データ暗号化キーを選択できます。この場合は、暗号化管理キーがすでに設定されている必要があります。 "独自のキーの使用方法を参照してください"。

ライセンス要件を確認

BlueXPのバックアップとリカバリのPAYGOライセンスの場合は、AWS MarketplaceでBlueXPサブスクリプションを購入して、Cloud Volumes ONTAP とBlueXPのバックアップとリカバリを導入できます。必要です "このBlueXPサブスクリプションを購読します" BlueXPのバックアップとリカバリを有効にする前に、BlueXPのバックアップとリカバリの課金は、このサブスクリプションを通じて行われます。

Cloud Volumes ONTAP データとオンプレミスの ONTAP データの両方をバックアップできる年間契約の場合は、から登録する必要があります "AWS Marketplace のページ" 次に "サブスクリプションを AWS クレデンシャルに関連付けます"。

Cloud Volumes ONTAP とBlueXPのバックアップとリカバリをバンドルできる年間契約の場合は、Cloud Volumes ONTAP 作業環境の作成時に年間契約を設定する必要があります。このオプションでは、オンプレミスのデータをバックアップすることはできません。

BlueXPのバックアップとリカバリのBYOLライセンスの場合は、ライセンスの期間と容量にわたってサービスを使用できるネットアップのシリアル番号が必要です。 "BYOL ライセンスの管理方法について説明します"。コネクタとCloud Volumes ONTAP システムをダークサイトに導入する場合は、BYOLライセンスを使用する必要があります。

また、バックアップを格納するストレージスペース用の AWS アカウントが必要です。

BlueXPコネクタを準備します

コネクタは、インターネットアクセスがフルまたは制限されているAWSリージョン（「標準」または「制限」モード）にインストールする必要があります。 "詳細については、BlueXPの導入モードを参照してください"。

- "コネクタについて説明します"
- "AWSでコネクタを標準モードで導入する（フルインターネットアクセス）"
- "制限モードでのコネクタの取り付け（制限されたアウトバウンドアクセス）"

コネクタの権限を確認または追加します

BlueXPに権限を付与するIAMロールには、最新ののS3権限が含まれている必要があります "BlueXPポリシー"。ポリシーにこれらの権限がすべて含まれていない場合は、を参照してください "AWS のドキュメント：「Editing IAM policies"。

ポリシーの具体的な権限を次に示します。

```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutBucketOwnershipControls"
                "s3:PutBucketPublicAccessBlock",
                "s3:PutEncryptionConfiguration",
                "s3:GetObjectVersionTagging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectVersionAcl",
                "s3:PutObjectTagging",
                "s3:DeleteObjectTagging",
                "s3:GetObjectRetention",
                "s3:DeleteObjectVersionTagging",
                "s3:PutBucketObjectLockConfiguration",
                "s3:DeleteObjectVersion",
                "s3:GetObjectTagging",
                "s3:PutBucketVersioning",
                "s3:PutObjectVersionTagging",
                "s3:GetBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:PutObjectRetention",
                "s3:GetObjectVersion",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
```

```
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
                "glue:BatchDeletePartition"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

AWS Chinaリージョンでバックアップを作成する場合は、IAMポリシーのall_Resource_sectionsの下にあるAWSリソース名「arn」を「aws」から「aws-cn」に変更する必要があります `arn:aws-cn:s3:::netapp-backup-*`。

必要な**AWS Cloud Volumes ONTAP** 権限

Cloud Volumes ONTAP システムでONTAP 9.12.1以降のソフトウェアを実行している場合は、作業環境に権限を付与するIAMロールに、BlueXPの最新のバックアップとリカバリに特化した新しいS3権限のセットを含める必要があります "Cloud Volumes ONTAP ポリシー"。

BlueXPバージョン3.9.23以降を使用してCloud Volumes ONTAP 作業環境を作成した場合、これらの権限はすでにIAMロールに含まれている必要があります。そうでない場合は、不足している権限を追加する必要があります。

サポートされている **AWS** リージョン

BlueXPのバックアップとリカバリは、すべてのAWSリージョンでサポートされます "Cloud Volumes ONTAP がサポートされている場合"（AWS GovCloudリージョンを含む）。

別の **AWS** アカウントでバックアップを作成する場合の必須のセットアップです

デフォルトでは、 Cloud Volumes ONTAP システムに使用されるアカウントと同じアカウントを使用してバックアップが作成されます。バックアップに別のAWSアカウントを使用する場合は、次の作業を行う必要があります。

- 権限「s3：PutBucketPolicy」と「s3：PutOwnershipControls」が、BlueXPコネクタに権限を付与するIAMロールに含まれていることを確認します。
- デスティネーションAWSアカウントのクレデンシャルをBlueXPに追加します。 "詳細については、「方法」を参照してください"。
- 2番目のアカウントのユーザクレデンシャルに次の権限を追加します。

```
"athena:StartQueryExecution",
"athena:GetQueryResults",
"athena:GetQueryExecution",
"glue:GetDatabase",
"glue:GetTable",
"glue:CreateTable",
"glue:CreateDatabase",
"glue:GetPartitions",
"glue:BatchCreatePartition",
"glue:BatchDeletePartition"
```

独自のバケットを作成します

デフォルトでは、サービスによってバケットが作成されます。独自のバケットを使用する場合は、バックアップアクティブ化ウィザードを開始する前にバケットを作成し、ウィザードでバケットを選択できます。

"独自のバケットの作成の詳細については、こちらをご覧ください"。

ボリュームをレプリケートするための**ONTAP**ネットワークの要件を確認します

BlueXPのバックアップとリカバリを使用してセカンダリONTAPシステムにレプリケートされたボリュームを作成する場合は、ソースシステムとデスティネーションシステムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワークの要件

- クラスタが社内にある場合は、社内ネットワークからクラウドプロバイダ内の仮想ネットワークへの接続が必要です。これは通常、 VPN 接続です。
- ONTAP クラスタは、サブネット、ポート、ファイアウォール、およびクラスタの追加要件を満たしている必要があります。

  Cloud Volumes ONTAPまたはオンプレミスのシステムにレプリケートできるため、オンプレミスのONTAPシステムのピアリング要件を確認してください。 "クラスタピアリングの前提条件については、ONTAP のドキュメントを参照してください"。

Cloud Volumes ONTAPネットワークの要件

- インスタンスのセキュリティグループに、必要なインバウンドおよびアウトバウンドのルールが含まれている必要があります。具体的には、 ICMP とポート 11104 および 11105 のルールが必要です。これらのルールは、事前定義されたセキュリティグループに含まれています。
- 異なるサブネットにある 2 つの Cloud Volumes ONTAP システム間でデータをレプリケートするには、サブネットを一緒にルーティングする必要があります（これがデフォルト設定です）。

Cloud Volumes ONTAPで**BlueXP**のバックアップとリカバリを有効にする

BlueXPのバックアップとリカバリは簡単に有効にできます。手順は、既存のCloud Volumes ONTAPシステムと新規のシステムのどちらを使用しているかによって多少異なります。

新しいシステムで**BlueXP**のバックアップとリカバリを有効にする

作業環境ウィザードでは、BlueXPのバックアップとリカバリがデフォルトで有効になります。このオプションは必ず有効にしておいてください。

を参照してください "AWS での Cloud Volumes ONTAP の起動" を Cloud Volumes ONTAP 参照してください。

手順

1. BlueXPのキャンバスで*を選択し、クラウドプロバイダを選択して[Add New]*を選択します。Cloud Volumes ONTAPの作成*を選択します。
2. クラウドプロバイダとして* Amazon Web Services *を選択し、単一のノードまたはHAシステムを選択します。
3. [詳細と資格情報] ページに入力します。
4. [サービス]ページで、サービスを有効のままにして*[続行]*を選択します。

5. ウィザードの各ページを設定し、システムを導入します。

結果

システムでBlueXPのバックアップとリカバリが有効になっている。これらのCloud Volumes ONTAPシステムでボリュームを作成したら、BlueXPのバックアップとリカバリとを起動します "保護する各ボリュームでバックアップをアクティブ化します"。

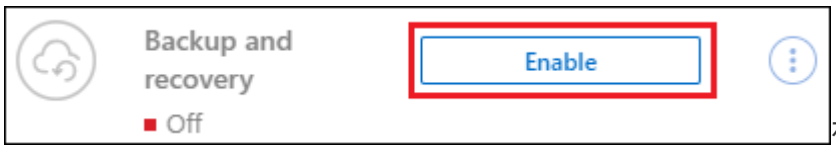
既存のシステムで**BlueXP**のバックアップとリカバリを有効にする

既存のシステムでBlueXPのバックアップとリカバリをいつでも作業環境から直接有効にできます。

手順

1. BlueXPのキャンバスで、作業環境を選択し、右側のパネルでバックアップとリカバリサービスの横にある*[有効化]*を選択します。

   バックアップのAmazon S3デスティネーションがCanvas上の作業環境として存在する場合は、クラスタをAmazon S3作業環境にドラッグしてセットアップウィザードを開始できます。



ボタンを示すスクリーンショット。"]

バックアップ設定の変更またはレプリケーションの追加については、を参照してください "ONTAP バックアップを管理します"。

ONTAPボリュームでバックアップをアクティブ化します

オンプレミスの作業環境からいつでも直接バックアップをアクティブ化できます。

ウィザードでは、次の主な手順を実行します。

- [バックアップするボリュームを選択します]
- [バックアップ戦略を定義します]
- [選択内容を確認します]

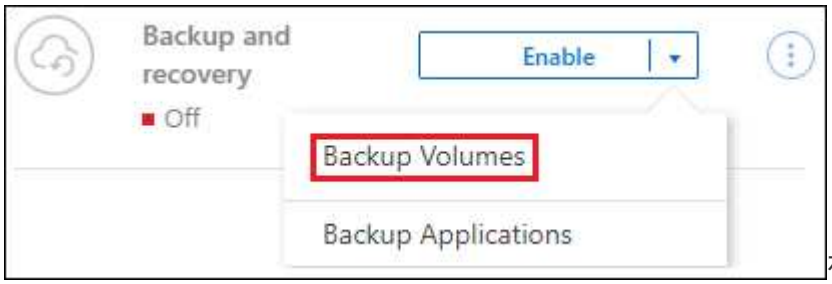
また可能です APIコマンドを表示します レビューステップでは、コードをコピーして、将来の作業環境のバックアップアクティベーションを自動化できます。

ウィザードを開始します

手順

1. 次のいずれかの方法でバックアップとリカバリのアクティブ化ウィザードにアクセスします。

   - BlueXPキャンバスで、作業環境を選択し、右パネルのバックアップとリカバリサービスの横にある*[有効化]>[ボリュームのバックアップ]*を選択します。

     ボタンのスクリーンショット。"]

     バックアップのAWSデスティネーションがCanvasの作業環境として存在する場合は、ONTAPクラスタをAWSオブジェクトストレージにドラッグできます。

   - [バックアップとリカバリ]バーで*を選択します。**[ボリューム]**タブで、[操作]* ••• 単一のボリューム（オブジェクトストレージへのレプリケーションまたはバックアップがまだ有効になっていないボリューム）に対して*[バックアップのアクティブ化]*を選択します。

   ウィザードの[Introduction]ページには、ローカルSnapshot、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で2番目のオプションを選択した場合は、1つのボリュームが選択された状態で[Define Backup Strategy]ページが表示されます。

2. 次のオプションに進みます。

   - BlueXPコネクタをすでにお持ちの場合は、これで準備は完了です。[次へ]*を選択します。
   - BlueXPコネクタをまだお持ちでない場合は、*[Add a Connector]*オプションが表示されます。を参照してください BlueXPコネクタを準備します。

バックアップするボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、Snapshotポリシー、レプリケーションポリシー、オブジェクトへのバックアップポリシーのうち1つ以上を含むボリュームです。

FlexVolボリュームとFlexGroupボリュームのどちらを保護するかを選択できますが、作業環境でバックアップをアクティブ化するときは、これらのボリュームを組み合わせて選択することはできません。方法を参照してください "作業環境内の追加ボリュームのバックアップをアクティブ化" （FlexVolまたはFlexGroup）初期ボリュームのバックアップの設定が完了したら、

> ⓘ
> - バックアップをアクティブ化できるのは、一度に1つのFlexGroupボリュームだけです。
> - 選択するボリュームのSnapLock設定は同じである必要があります。すべてのボリュームでSnapLock Enterpriseが有効になっているかSnapLockが無効になっている必要があります。（SnapLock Complianceモードのボリュームには、ONTAP 9.14以降が必要です）。

手順

選択したボリュームにSnapshotポリシーまたはレプリケーションポリシーがすでに適用されている場合は、あとで選択したポリシーで既存のポリシーが上書きされます。

1. [Select Volumes]ページで、保護するボリュームを選択します。
   - 必要に応じて、行をフィルタして、特定のボリュームタイプや形式などのボリュームのみを表示し、選択を容易にします。
   - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます（FlexGroupボリュームは一度に1つだけ選択できます）。既存のFlexVolボリュームをすべてバックアップするには、最初に1つのボリュームをオンにしてから、タイトル行のボックスをオンにします。（☑ Volume Name）。
   - 個々のボリュームをバックアップするには、各ボリュームのボックス（☑ Volume_1）。
2. 「 * 次へ * 」を選択します。

バックアップ戦略を定義します

バックアップ戦略を定義するには、次のオプションを設定します。

- 1つまたはすべてのバックアップオプション（ローカルSnapshot、レプリケーション、オブジェクトストレージへのバックアップ）が必要かどうか
- アーキテクチャ
- ローカルSnapshotポリシー
- レプリケーションのターゲットとポリシー

> ⓘ 選択したボリュームのSnapshotポリシーとレプリケーションポリシーがこの手順で選択したポリシーと異なる場合は、既存のポリシーが上書きされます。

- オブジェクトストレージ情報（プロバイダ、暗号化、ネットワーク、バックアップポリシー、エクスポートオプション）へのバックアップ。

手順

1. [Define backup strategy]ページで、次のいずれかまたはすべてを選択します。デフォルトでは、3つすべてが選択されています。
   - *ローカルSnapshot *：レプリケーションまたはオブジェクトストレージへのバックアップを実行する場合は、ローカルSnapshotを作成する必要があります。
   - レプリケーション：別のONTAPストレージシステムにレプリケートされたボリュームを作成します。

- バックアップ：ボリュームをオブジェクトストレージにバックアップします。

2. アーキテクチャ:レプリケーションとバックアップを選択した場合は'次のいずれかの情報フローを選択します
   - カスケード：情報は、プライマリストレージシステムからセカンダリストレージ、およびセカンダリストレージからオブジェクトストレージに流れます。
   - ファンアウト：プライマリストレージシステムからセカンダリ_および_に、プライマリストレージからオブジェクトストレージに情報が流れます。

     これらのアーキテクチャの詳細については、を参照してください "保護対策を計画しましょう"。

3. *ローカルSnapshot *：既存のSnapshotポリシーを選択するか、新しいSnapshotポリシーを作成します。

   Snapshotをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

   ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

   - ポリシーの名前を入力します。
   - 最大5つのスケジュール（通常は異なる周波数）を選択します。
   - 「 * Create * 」を選択します。

4. レプリケーション：次のオプションを設定します。
   - レプリケーションターゲット：デスティネーションの作業環境とSVMを選択します。必要に応じて、レプリケートするボリュームの名前に追加するデスティネーションアグリゲートとプレフィックスまたはサフィックスを選択します。
   - レプリケーションポリシー：既存のレプリケーションポリシーを選択するか作成します。

     カスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

     ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

     - ポリシーの名前を入力します。
     - 最大5つのスケジュール（通常は異なる周波数）を選択します。
     - 「 * Create * 」を選択します。

5. オブジェクトにバックアップ：*バックアップ*を選択した場合は、次のオプションを設定します。
   - プロバイダ：[Amazon Web Services]*を選択します。
   - プロバイダ設定：バックアップを保存するプロバイダの詳細と地域を入力します。

     バックアップの保存に使用するAWSアカウントを入力します。これは、 Cloud Volumes ONTAP システムが配置されているアカウントとは異なる場合があります。

     バックアップに別のAWSアカウントを使用する場合は、デスティネーションのAWSアカウントのクレデンシャルをBlueXPに追加し、「s3：PutBucketPolicy」および「s3：PutOwnerBucketshipControls」権限をBlueXPに付与するIAMロールに追加する必要があります。

     バックアップを保存するリージョンを選択します。これは、 Cloud Volumes ONTAP システムが配置

されているリージョンとは異なるリージョンにすることもできます。

新しいバケットを作成するか、既存のバケットを選択します。

- 暗号化キー：新しいバケットを作成した場合は、プロバイダから提供された暗号化キー情報を入力します。データの暗号化を管理するために、デフォルトのAWS暗号化キーを使用するか、AWSアカウントからお客様が管理する独自のキーを選択するかを選択します。（"独自の暗号化キーの使用方法を参照してください"）。

  独自の顧客管理キーを使用する場合は、キーボールトとキー情報を入力します。

  > 既存のバケットを選択した場合、暗号化情報はすでに使用可能なため、ここで入力する必要はありません。

- バックアップポリシー：オブジェクトストレージへの既存のバックアップポリシーを選択するか作成します。

  > バックアップをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

  ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

  - ポリシーの名前を入力します。
  - 最大5つのスケジュール（通常は異なる周波数）を選択します。
  - オブジェクトへのバックアップポリシーの場合は、DataLockとRansomware Protectionを設定します。DataLockとランサムウェア対策の詳細については、 "オブジェクトへのバックアップポリシーの設定"。
    - 「 * Create * 」を選択します。

- 既存の**Snapshot**コピーをバックアップコピーとしてオブジェクトストレージにエクスポート：この作業環境に、この作業環境に対して選択したバックアップスケジュールラベル（daily、weeklyなど）と一致するボリュームのローカルSnapshotコピーがある場合は、この追加のプロンプトが表示されます。ボリュームを最大限に保護するために、履歴Snapshotをすべてオブジェクトストレージにバックアップファイルとしてコピーする場合は、このチェックボックスをオンにします。

  i. 「 * 次へ * 」を選択します。

選択内容を確認します

これにより、選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. [Review]ページで、選択内容を確認します。
2. 必要に応じて、Snapshotポリシーのラベルをレプリケーションポリシーおよびバックアップポリシーのラベルと自動的に同期する*チェックボックスをオンにします。これにより、レプリケーションポリシーとバックアップポリシーのラベルに一致するラベルを持つSnapshotが作成されます。
3. [バックアップのアクティブ化]*を選択します。

結果

BlueXPのバックアップとリカバリで、ボリュームの初期バックアップが作成されます。レプリケートされた

ボリュームとバックアップファイルのベースライン転送には、プライマリストレージシステムのデータのフルコピーが含まれます。以降の転送には、Snapshotコピーに含まれるプライマリストレージシステムデータの差分コピーが含まれます。

レプリケートされたボリュームが、プライマリストレージボリュームと同期されるデスティネーションクラスタに作成されます。

入力したS3アクセスキーとシークレットキーで指定されたサービスアカウントにS3バケットが作成され、バックアップファイルがそこに格納されます。

ボリュームバックアップダッシュボードが表示され、バックアップの状態を監視できます。

を使用して、バックアップジョブとリストアジョブのステータスを監視することもできます "［ジョブ監視］パネル"。

APIコマンドを表示します

バックアップとリカバリのアクティブ化ウィザードで使用するAPIコマンドを表示し、必要に応じてコピーすることができます。これは、将来の作業環境でバックアップを自動的にアクティブ化する場合に必要になることがあります。

手順

1. バックアップとリカバリのアクティブ化ウィザードで、*[API要求の表示]*を選択します。
2. コマンドをクリップボードにコピーするには、*コピー*アイコンを選択します。

次の手順

- 可能です "バックアップファイルとバックアップポリシーを管理"。バックアップの開始と停止、バックアップの削除、バックアップスケジュールの追加と変更などが含まれます。
- 可能です "クラスタレベルのバックアップの設定を管理します"。これには、クラウドストレージへのアクセスにONTAP で使用するストレージキーの変更、オブジェクトストレージへのバックアップのアップロードに使用できるネットワーク帯域幅の変更、将来のボリュームに対する自動バックアップ設定の変更などが含まれます。
- また可能です "ボリューム、フォルダ、または個々のファイルをバックアップファイルからリストアする" AWS の Cloud Volumes ONTAP システムやオンプレミスの ONTAP システムに接続できます。

Cloud Volumes ONTAPのデータをAzure BLOBストレージにバックアップ

Cloud Volumes ONTAP システムからAzure BLOBストレージへのボリュームデータのバックアップを開始するには、いくつかの手順を実行します。

クイックスタート

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

1 構成がサポートされていることを確認します

- AzureでCloud Volumes ONTAP 9.8以降を実行している（ONTAP 9.8P13以降を推奨）。
- バックアップを格納するストレージスペースに対する有効なクラウドプロバイダのサブスクリプションが必要です。
- に登録しておきます "BlueXP Marketplaceバックアップ製品"またはを購入したことが必要です "アクティブ化されます" ネットアップが提供するBlueXPバックアップ/リカバリのBYOLライセンス

2 **BlueXP**コネクタを準備します

Azureリージョンにすでにコネクタがデプロイされている場合は、準備は完了です。そうでない場合は、AzureにBlueXPコネクタをインストールして、Cloud Volumes ONTAPのデータをAzure Blobストレージにバックアップする必要があります。コネクタは、完全なインターネットアクセス(「標準モード」)または制限されたインターネット接続(「制限モード」)を備えたサイトにインストールできます。

BlueXPコネクタを準備します

3 ライセンス要件を確認

AzureとBlueXPの両方のライセンス要件を確認する必要があります。

を参照してください [ライセンス要件を確認]。

4 ボリュームをレプリケートするための**ONTAP**ネットワークの要件を確認します

ソースシステムとデスティネーションシステムがONTAPのバージョンとネットワークの要件を満たしていることを確認します。

ボリュームをレプリケートするためのONTAPネットワークの要件を確認します。

5 **BlueXP**のバックアップとリカバリを有効にする

作業環境を選択し、右パネルのバックアップ/リカバリサービスの横にある*有効化>バックアップボリューム*をクリックします。

Cloud Volumes ONTAPでBlueXPのバックアップとリカバリを有効にする。

6 **ONTAP**ボリュームでバックアップをアクティブ化します

セットアップウィザードに従って、使用するレプリケーションポリシーとバックアップポリシー、およびバックアップするボリュームを選択します。

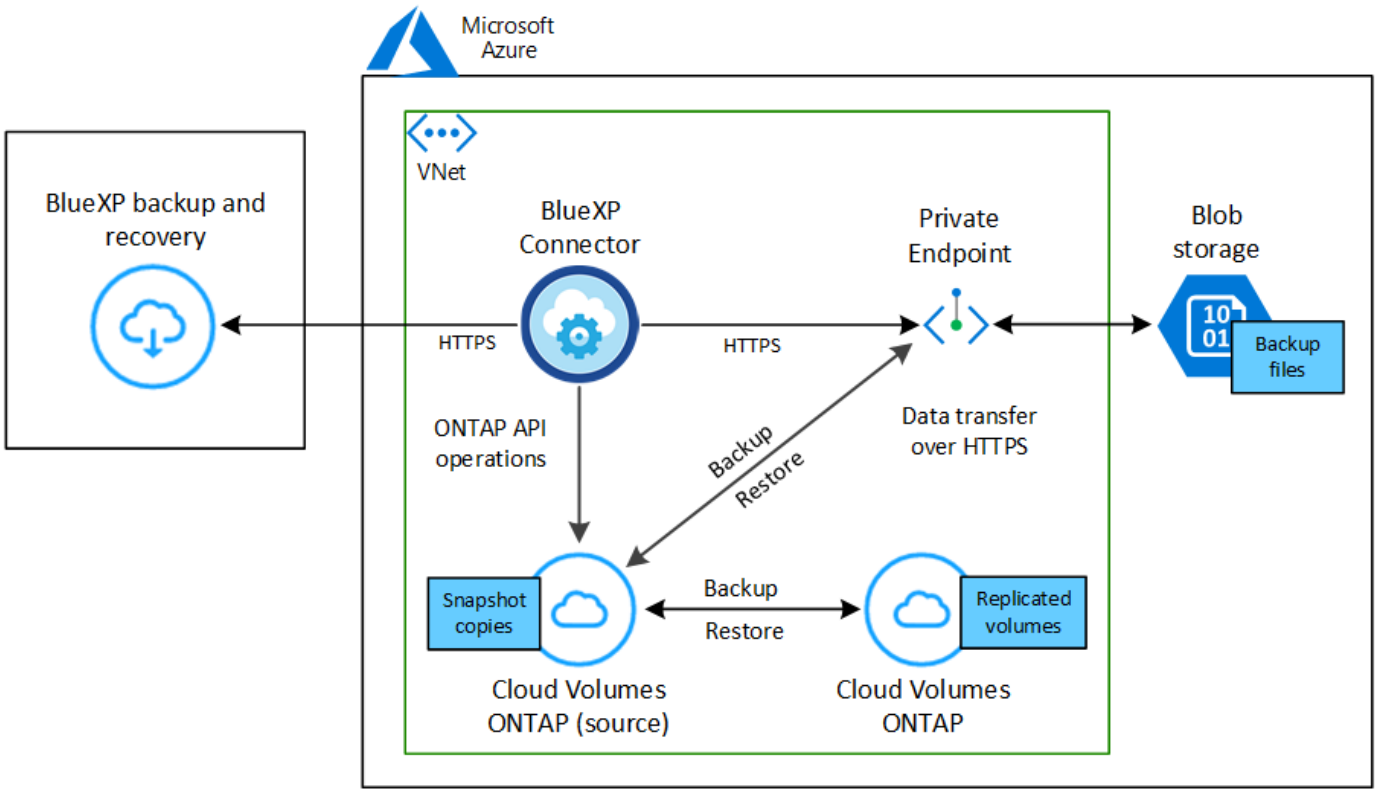
ONTAPボリュームでバックアップをアクティブ化します。

構成がサポートされていることを確認します

Azure Blob Storage へのボリュームのバックアップを開始する前に、次の要件を確認し、サポートされている構成であることを確認してください。

次の図は、各コンポーネントとそれらの間の接続を示しています。

必要に応じて、パブリック接続またはプライベート接続を使用して、レプリケートされたボリュームのセカンダリONTAPシステムに接続することもできます。



サポートされる**ONTAP**のバージョン

ONTAP 9.8以上、ONTAP 9.8P13以降が推奨されます。

サポートされている **Azure** リージョン

BlueXPのバックアップとリカバリは、Azureのすべてのリージョンでサポートされます "Cloud Volumes ONTAP がサポートされている場合"Azure Government リージョンを含む。

BlueXPのバックアップとリカバリでは、コストを最適化するために、デフォルトでLocal Redundancy（LRS）を使用してBlobコンテナがプロビジョニングされます。異なるゾーン間でデータを確実にレプリケートする場合は、BlueXPのバックアップとリカバリをアクティブ化したあとにこの設定をZone redundancy（ZRS）に変更できます。Microsoftの手順を参照してください "ストレージアカウントの複製方法の変更"。

別の **Azure** サブスクリプションでバックアップを作成するために必要なセットアップ

デフォルトでは、バックアップは Cloud Volumes ONTAP システムと同じサブスクリプションを使用して作成されます。バックアップに別の Azure サブスクリプションを使用する場合は、が必要です "Azure ポータルにログインして、 2 つのサブスクリプションをリンクできます"。

ライセンス要件を確認

BlueXPのバックアップとリカバリのPAYGOライセンスを使用している場合は、BlueXPのバックアップとリカバリを有効にする前に、Azure Marketplaceでサブスクリプションを購入する必要があります。BlueXPのバックアップとリカバリの課金は、このサブスクリプションを通じて行われます。 "作業環境ウィザードの[Details Credentialsページからサブスクライブできます。"^]。

BlueXPのバックアップとリカバリのBYOLライセンスの場合は、ライセンスの期間と容量にわたってサービスを使用できるネットアップのシリアル番号が必要です。 "BYOL ライセンスの管理方法について説明します"。コネクタとCloud Volumes ONTAP システムをダークサイト（「プライベートモード」）に導入する場合は、BYOLライセンスを使用する必要があります。

また、バックアップを格納するストレージスペースには、 Microsoft Azure サブスクリプションが必要です。

BlueXPコネクタを準備します

コネクタは、フルまたは制限されたインターネットアクセス(「標準」または「制限」モード)を持つAzureリージョンにインストールできます。 "詳細については、BlueXPの導入モードを参照してください"。

- "コネクタについて説明します"
- "Azureで標準モードでコネクタを導入する（フルインターネットアクセス）"
- "制限モードでのコネクタの取り付け（制限されたアウトバウンドアクセス）"

コネクタの権限を確認または追加します

BlueXPのバックアップとリカバリの検索とリストア機能を使用するには、コネクタがAzure Synapse WorkspaceとData Lake Storageアカウントにアクセスできるように、コネクタのロールに特定の権限が必要です。以下の権限を確認し、ポリシーを変更する必要がある場合は手順に従います。

を開始する前に

- Azure Synapse Analytics Resource Provider（"Microsoft.Synapse"）をサブスクリプションに登録する必要があります。 "このリソースプロバイダをサブスクリプションに登録する方法については、を参照してください"。リソースプロバイダを登録するには、Subscription * Owner または Contributor *である必要があります。
- コネクタとAzure Synapse SQLサービス間の通信には、ポート1433が開いている必要があります。

手順

1. Connector 仮想マシンに割り当てられているロールを特定します。
   a. Azureポータルで、仮想マシンサービスを開きます。
   b. Connector 仮想マシンを選択します。
   c. [設定] で、 [**Identity**] を選択します。
   d. [Azure role assignments]*を選択します。
   e. Connector 仮想マシンに割り当てられているカスタムロールをメモしておきます。
2. カスタムロールを更新します。
   a. Azure ポータルで、 Azure サブスクリプションを開きます。
   b. [Access control（IAM）]>[Roles]*を選択します。

c. カスタムロールの省略記号（...）を選択し、*[編集]*を選択します。

d. [json]*を選択し、次の権限を追加します。

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"ポリシーの完全な JSON 形式を表示します"

e. [* Review + update *] をクリックし、 [* Update *] をクリックします。

データ暗号化にお客様が管理するキーを使用するために必要な情報

Microsoft が管理するデフォルトの暗号化キーを使用する代わりに、アクティベーションウィザードで、お客様が管理する独自のキーを使用してデータを暗号化できます。この場合、Azureサブスクリプション、キーボールト名、およびキーが必要です。 "独自のキーの使用方法を参照してください"。

BlueXPのバックアップとリカバリでは、*Azure*アクセスポリシー_が権限モデルとしてサポートされます。現時点では、_*Azure Role-Based Access Control*（Azure RBAC）権限モデルはサポートされていません。

Azure BLOBストレージアカウントを作成します

デフォルトでは、サービスによってストレージアカウントが作成されます。独自のストレージアカウントを使用する場合は、バックアップアクティブ化ウィザードを開始する前にストレージアカウントを作成し、ウィザードでそれらのストレージアカウントを選択できます。

"独自のストレージアカウントの作成について詳しくは、こちらをご覧ください"。

ボリュームをレプリケートするための**ONTAP**ネットワークの要件を確認します

BlueXPのバックアップとリカバリを使用してセカンダリONTAPシステムにレプリケートされたボリュームを作成する場合は、ソースシステムとデスティネーションシステムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワークの要件

- クラスタが社内にある場合は、社内ネットワークからクラウドプロバイダ内の仮想ネットワークへの接続が必要です。これは通常、 VPN 接続です。
- ONTAP クラスタは、サブネット、ポート、ファイアウォール、およびクラスタの追加要件を満たしている必要があります。

  Cloud Volumes ONTAPまたはオンプレミスのシステムにレプリケートできるため、オンプレミスのONTAPシステムのピアリング要件を確認してください。 "クラスタピアリングの前提条件については、ONTAP のドキュメントを参照してください"。

Cloud Volumes ONTAPネットワークの要件

- インスタンスのセキュリティグループに、必要なインバウンドおよびアウトバウンドのルールが含まれている必要があります。具体的には、 ICMP とポート 11104 および 11105 のルールが必要です。これらのルールは、事前定義されたセキュリティグループに含まれています。
- 異なるサブネットにある 2 つの Cloud Volumes ONTAP システム間でデータをレプリケートするには、サブネットを一緒にルーティングする必要があります（これがデフォルト設定です）。

Cloud Volumes ONTAPで**BlueXP**のバックアップとリカバリを有効にする

BluXPのバックアップとリカバリを有効にするのは簡単です。手順は、既存のCloud Volumes ONTAPシステムと新規のシステムのどちらを使用しているかによって多少異なります。

新しいシステムで**BlueXP**のバックアップとリカバリを有効にする

作業環境ウィザードでは、BlueXPのバックアップとリカバリがデフォルトで有効になります。このオプションは必ず有効にしておいてください。

を参照してください "Azure で Cloud Volumes ONTAP を起動します" を Cloud Volumes ONTAP 参照してください。

> リソースグループの名前を選択する場合は、Cloud Volumes ONTAP を導入する際に* BlueXP のバックアップとリカバリを無効にしてください。の手順に従います 既存システムでBlueXPのバックアップとリカバリを有効にする BlueXPのバックアップとリカバリを有効にし、リソースグループを選択するには、次の手順を実行します。

手順

1. BlueXPのキャンバスで*を選択し、クラウドプロバイダを選択して[Add New]*を選択します。Cloud Volumes ONTAPの作成*を選択します。
2. クラウドプロバイダとして* Microsoft Azure *を選択し、単一のノードまたはHAシステムを選択します。
3. Azure クレデンシャルの定義ページで、クレデンシャル名、クライアント ID 、クライアントシークレット、およびディレクトリ ID を入力し、 * 続行 * をクリックします。
4. 詳細とクレデンシャルページに必要事項を入力し、 Azure Marketplace サブスクリプションが登録されていることを確認して、「 * Continue * 」をクリックします。
5. [サービス] ページで、サービスを有効のままにして、 [* 続行] をクリックします。

6. ウィザードの各ページを設定し、システムを導入します。

結果

システムでBlueXPのバックアップとリカバリが有効になっている。これらのCloud Volumes ONTAPシステムでボリュームを作成したら、BlueXPのバックアップとリカバリとを起動します "保護する各ボリュームでバックアップをアクティブ化します"。

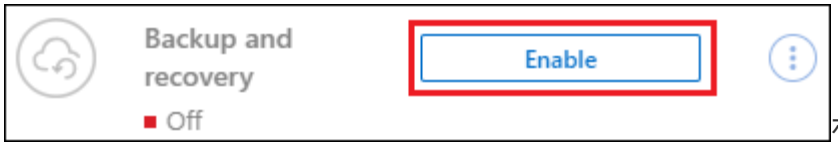
既存のシステムで**BlueXP**のバックアップとリカバリを有効にする

BlueXPのバックアップとリカバリは、いつでも作業環境から直接実行できます。

手順

1. BlueXPのキャンバスで、作業環境を選択し、右側のパネルでバックアップとリカバリサービスの横にある*[有効化]*を選択します。

   バックアップのAzure Blobデスティネーションが Canvas上に作業環境として存在する場合は、クラスタをAzure Blob Working環境にドラッグしてセットアップウィザードを開始できます。



ボタンのスクリーンショット。"]

2. ウィザードの各ページに必要な情報を入力して、BlueXPのバックアップとリカバリを導入します。
3. バックアップを開始する場合は、に進みます ONTAPボリュームでバックアップをアクティブ化します。

ONTAPボリュームでバックアップをアクティブ化します

オンプレミスの作業環境からいつでも直接バックアップをアクティブ化できます。

ウィザードでは、次の主な手順を実行します。

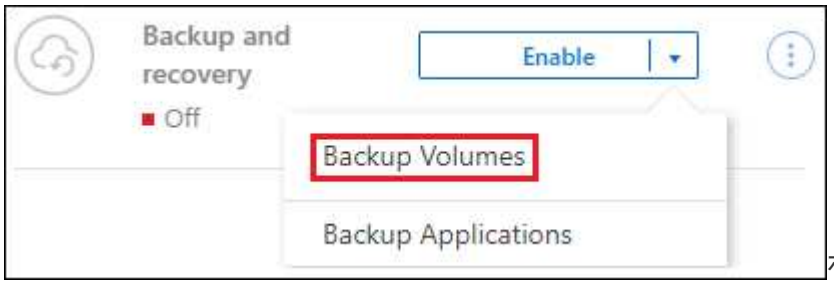
- [バックアップするボリュームを選択します]
- [バックアップ戦略を定義します]
- [選択内容を確認します]

また可能です APIコマンドを表示します レビューステップでは、コードをコピーして、将来の作業環境のバックアップアクティベーションを自動化できます。

ウィザードを開始します

手順

1. 次のいずれかの方法でバックアップとリカバリのアクティブ化ウィザードにアクセスします。
   - BlueXPキャンバスで、作業環境を選択し、右パネルのバックアップとリカバリサービスの横にある*[有効化]>[ボリュームのバックアップ]*を選択します。

     ボタンのスクリーンショット。"]

     バックアップのAzureデスティネーションがCanvasの作業環境として存在する場合は、ONTAPクラスタをAzure Blobオブジェクトストレージにドラッグできます。

   - [バックアップとリカバリ]バーで*を選択します。**[ボリューム]**タブで、[操作]* ••• アイコンをクリックし、（オブジェクトストレージへのレプリケーションまたはバックアップがまだ有効になっていない）単一のボリュームに対して*[バックアップのアクティブ化]*を選択します。

   ウィザードの[Introduction]ページには、ローカルSnapshot、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で2番目のオプションを選択した場合は、1つのボリュームが選択された状態で[Define Backup Strategy]ページが表示されます。

2. 次のオプションに進みます。
   - BlueXPコネクタをすでにお持ちの場合は、これで準備は完了です。[次へ]*を選択します。

- BlueXPコネクタをまだお持ちでない場合は、*[Add a Connector]*オプションが表示されます。を参照してください BlueXPコネクタを準備します。

バックアップするボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、Snapshotポリシー、レプリケーションポリシー、オブジェクトへのバックアップポリシーのうち1つ以上のポリシーが設定されているボリュームです。

FlexVolボリュームとFlexGroupボリュームのどちらを保護するかを選択できますが、作業環境でバックアップをアクティブ化するときは、これらのボリュームを組み合わせて選択することはできません。方法を参照してください "作業環境内の追加ボリュームのバックアップをアクティブ化" （FlexVolまたはFlexGroup）初期ボリュームのバックアップの設定が完了したら、

> - バックアップをアクティブ化できるのは、一度に1つのFlexGroupボリュームだけです。
> - 選択するボリュームのSnapLock設定は同じである必要があります。すべてのボリュームでSnapLock Enterpriseが有効になっているかSnapLockが無効になっている必要があります。（SnapLock Complianceモードのボリュームには、ONTAP 9.14以降が必要です）。

手順

選択したボリュームにSnapshotポリシーまたはレプリケーションポリシーがすでに適用されている場合は、あとで選択したポリシーで既存のポリシーが上書きされます。

1. [Select Volumes]ページで、保護するボリュームを選択します。
   - 必要に応じて、行をフィルタして、特定のボリュームタイプや形式などのボリュームのみを表示し、選択を容易にします。
   - 最初のボリュームを選択したら、[All FlexVol Volumes]を選択できます。（FlexGroupボリュームは一度に1つしか選択できません）。 既存のFlexVolボリュームをすべてバックアップするには、最初に1つのボリュームをオンにしてから、タイトル行のボックスをオンにします。（☑ Volume Name）。
   - 個々のボリュームをバックアップするには、各ボリュームのボックス（☑ Volume_1）。
2. 「 * 次へ * 」を選択します。

バックアップ戦略を定義します

バックアップ戦略を定義するには、次のオプションを設定します。

- 1つまたはすべてのバックアップオプション（ローカルSnapshot、レプリケーション、オブジェクトストレージへのバックアップ）が必要かどうか
- アーキテクチャ
- ローカルSnapshotポリシー
- レプリケーションのターゲットとポリシー

> 選択したボリュームのSnapshotポリシーとレプリケーションポリシーがこの手順で選択したポリシーと異なる場合は、既存のポリシーが上書きされます。

- オブジェクトストレージ情報（プロバイダ、暗号化、ネットワーク、バックアップポリシー、エクスポートオプション）へのバックアップ。

手順

1. [Define backup strategy]ページで、次のいずれかまたはすべてを選択します。デフォルトでは、3つすべてが選択されています。
   - *ローカルSnapshot *：レプリケーションまたはオブジェクトストレージへのバックアップを実行する場合は、ローカルSnapshotを作成する必要があります。
   - レプリケーション：別のONTAPストレージシステムにレプリケートされたボリュームを作成します。
   - バックアップ：ボリュームをオブジェクトストレージにバックアップします。
2. アーキテクチャ:レプリケーションとバックアップを選択した場合は'次のいずれかの情報フローを選択します
   - カスケード：情報は、プライマリストレージシステムからセカンダリストレージ、およびセカンダリストレージからオブジェクトストレージに流れます。
   - ファンアウト：プライマリストレージシステムからセカンダリ_および_に、プライマリストレージからオブジェクトストレージに情報が流れます。

     これらのアーキテクチャの詳細については、を参照してください "保護対策を計画しましょう"。
3. *ローカルSnapshot *：既存のSnapshotポリシーを選択するか、作成します。

   Snapshotをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

   ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

   - ポリシーの名前を入力します。
   - 最大5つのスケジュール（通常は異なる周波数）を選択します。
   - 「 * Create * 」を選択します。
4. レプリケーション：次のオプションを設定します。
   - レプリケーションターゲット：デスティネーションの作業環境とSVMを選択します。必要に応じて、レプリケートするボリュームの名前に追加するデスティネーションアグリゲートとプレフィックスまたはサフィックスを選択します。
   - レプリケーションポリシー：既存のレプリケーションポリシーを選択するか作成します。

     レプリケーションをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

     ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

     - ポリシーの名前を入力します。
     - 最大5つのスケジュール（通常は異なる周波数）を選択します。
     - 「 * Create * 」を選択します。
5. オブジェクトにバックアップ：*バックアップ*を選択した場合は、次のオプションを設定します。
   - プロバイダ：[Microsoft Azure]*を選択します。
   - プロバイダ設定：プロバイダの詳細を入力します。

バックアップを保存するリージョンを入力します。これは、 Cloud Volumes ONTAP システムが配置されているリージョンとは異なるリージョンにすることもできます。

新しいストレージアカウントを作成するか、既存のストレージアカウントを選択します。

バックアップの格納に使用するAzureサブスクリプションを入力します。これは、 Cloud Volumes ONTAP システムとは異なるサブスクリプションにすることもできます。バックアップに別の Azure サブスクリプションを使用する場合は、が必要です "Azure ポータルにログインして、 2 つのサブスクリプションをリンクできます"。

Blobコンテナを管理する独自のリソースグループを作成するか、リソースグループのタイプとグループを選択します。

> バックアップファイルが変更または削除されないように保護する場合は、ストレージアカウントが変更不可のストレージで作成され、30日間の保持期間を使用していることを確認してください。

> コストをさらに最適化するために古いバックアップファイルをAzure Archive Storageに階層化する場合は、ストレージアカウントに適切なライフサイクルルールが設定されていることを確認してください。

- 暗号化キー：新しいAzureストレージアカウントを作成した場合は、プロバイダから提供された暗号化キー情報を入力します。データの暗号化を管理するために、デフォルトのAzure暗号化キーを使用するか、Azureアカウントからお客様が管理する独自のキーを選択するかを選択します。

  独自の顧客管理キーを使用する場合は、キーボールトとキー情報を入力します。 "独自のキーの使用方法について説明します"。

  > 既存のMicrosoftストレージアカウントを選択した場合、暗号化情報はすでに使用可能なため、ここで入力する必要はありません。

- ネットワーク：IPspace、およびプライベートエンドポイントを使用するかどうかを選択します。プライベートエンドポイントはデフォルトで無効になっています。

  i. バックアップするボリュームが配置されている ONTAP クラスタ内の IPspace 。この IPspace のクラスタ間 LIF 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。

  ii. 必要に応じて、以前に設定したAzureプライベートエンドポイントを使用するかどうかを選択します。 "Azureプライベートエンドポイントの使用について説明します"。

- バックアップポリシー：既存のオブジェクトへのバックアップストレージポリシーを選択します。

  > バックアップをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

  ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

  - ポリシーの名前を入力します。
  - オブジェクトへのバックアップポリシーの場合は、DataLockとRansomware Protectionを設定します。DataLockとランサムウェア対策の詳細については、 "オブジェクトへのバックアップポリシーの設定"。

        - 最大5つのスケジュール（通常は異なる周波数）を選択します。
        - 「 * Create * 」を選択します。
    - 既存の**Snapshot**コピーをバックアップコピーとしてオブジェクトストレージにエクスポート：この作業環境に、この作業環境に対して選択したバックアップスケジュールラベル（daily、weeklyなど）と一致するボリュームのローカルSnapshotコピーがある場合は、この追加のプロンプトが表示されます。ボリュームを最大限に保護するために、履歴Snapshotをすべてオブジェクトストレージにバックアップファイルとしてコピーする場合は、このチェックボックスをオンにします。
        i. 「 * 次へ * 」を選択します。

選択内容を確認します

これにより、選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. [Review]ページで、選択内容を確認します。
2. 必要に応じて、Snapshotポリシーのラベルをレプリケーションポリシーおよびバックアップポリシーのラベルと自動的に同期する*チェックボックスをオンにします。これにより、レプリケーションポリシーとバックアップポリシーのラベルに一致するラベルを持つSnapshotが作成されます。
3. [バックアップのアクティブ化]*を選択します。

結果

BlueXPのバックアップとリカバリで、ボリュームの初期バックアップが作成されます。レプリケートされたボリュームとバックアップファイルのベースライン転送には、プライマリストレージシステムのデータのフルコピーが含まれます。以降の転送には、Snapshotコピーに含まれるプライマリストレージデータの差分コピーが含まれます。

レプリケートされたボリュームが、プライマリボリュームと同期されるデスティネーションクラスタに作成されます。

入力したリソースグループにBLOBストレージコンテナが作成され、バックアップファイルがそこに格納されます。

BlueXPのバックアップとリカバリでは、コストを最適化するために、デフォルトでLocal Redundancy（LRS）を使用してBlobコンテナがプロビジョニングされます。異なるゾーン間でデータを確実に複製する場合は、この設定をZone redundancy（ZRS）に変更できます。Microsoftの手順を参照してください "ストレージアカウントの複製方法の変更"。

ボリュームバックアップダッシュボードが表示され、バックアップの状態を監視できます。

を使用して、バックアップジョブとリストアジョブのステータスを監視することもできます "［ジョブ監視］パネル"。

APIコマンドを表示します

バックアップとリカバリのアクティブ化ウィザードで使用するAPIコマンドを表示し、必要に応じてコピーすることができます。これは、将来の作業環境でバックアップを自動的にアクティブ化する場合に必要になることがあります。

手順

1. バックアップとリカバリのアクティブ化ウィザードで、*[API要求の表示]*を選択します。
2. コマンドをクリップボードにコピーするには、*コピー*アイコンを選択します。

次の手順

- 可能です "バックアップファイルとバックアップポリシーを管理"。バックアップの開始と停止、バックアップの削除、バックアップスケジュールの追加と変更などが含まれます。
- 可能です "クラスタレベルのバックアップの設定を管理します"。これには、バックアップをオブジェクトストレージにアップロードするためのネットワーク帯域幅の変更、将来のボリュームに対する自動バックアップ設定の変更などが含まれます。
- また可能です "ボリューム、フォルダ、または個々のファイルをバックアップファイルからリストアする" Azure 内の Cloud Volumes ONTAP システムやオンプレミスの ONTAP システムへの接続に使用できます。

Cloud Volumes ONTAPデータをGoogle Cloud Storageにバックアップします

Cloud Volumes ONTAP システムからGoogle Cloud Storageへのボリュームデータのバックアップを開始するには、いくつかの手順を実行します。

クイックスタート

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

1 構成がサポートされていることを確認します

- GCPでCloud Volumes ONTAP 9.8以降を実行している（ONTAP 9.8P13以降を推奨）。
- バックアップを保存するストレージスペースの有効な GCP サブスクリプションがあります。
- Google Cloud Project に、事前定義された Storage Admin ロールを持つサービスアカウントがあります。
- に登録しておきます "BlueXP Marketplaceバックアップ製品"またはを購入したことが必要です "アクティブ化されます" ネットアップが提供するBlueXPバックアップ/リカバリのBYOLライセンス

2 **BlueXP**コネクタを準備します

コネクタがすでにGCPリージョンにデプロイされている場合は、すべて準備が完了しています。そうでない場合は、Cloud Volumes ONTAPデータをGoogle Cloud Storageにバックアップするために、GCPにBlueXPコネクタをインストールする必要があります。コネクタは、完全なインターネットアクセス(「標準モード」)または制限されたインターネット接続(「制限モード」)を備えたサイトにインストールできます。

BlueXPコネクタを準備します

3 ライセンス要件を確認

Google CloudとBlueXPの両方のライセンス要件を確認する必要があります。

[ライセンス要件を確認]。

4 ボリュームをレプリケートするための**ONTAP**ネットワークの要件を確認します

ソースシステムとデスティネーションシステムがONTAPのバージョンとネットワークの要件を満たしていることを確認します。

ボリュームをレプリケートするためのONTAPネットワークの要件を確認します。

5 **BlueXP**のバックアップとリカバリを有効にする

作業環境を選択し、右パネルのバックアップ/リカバリサービスの横にある*有効化>バックアップボリューム*をクリックします。

Cloud Volumes ONTAPでBlueXPのバックアップとリカバリを有効にする。

6 **ONTAP**ボリュームでバックアップをアクティブ化します

セットアップウィザードに従って、使用するレプリケーションポリシーとバックアップポリシー、およびバックアップするボリュームを選択します。

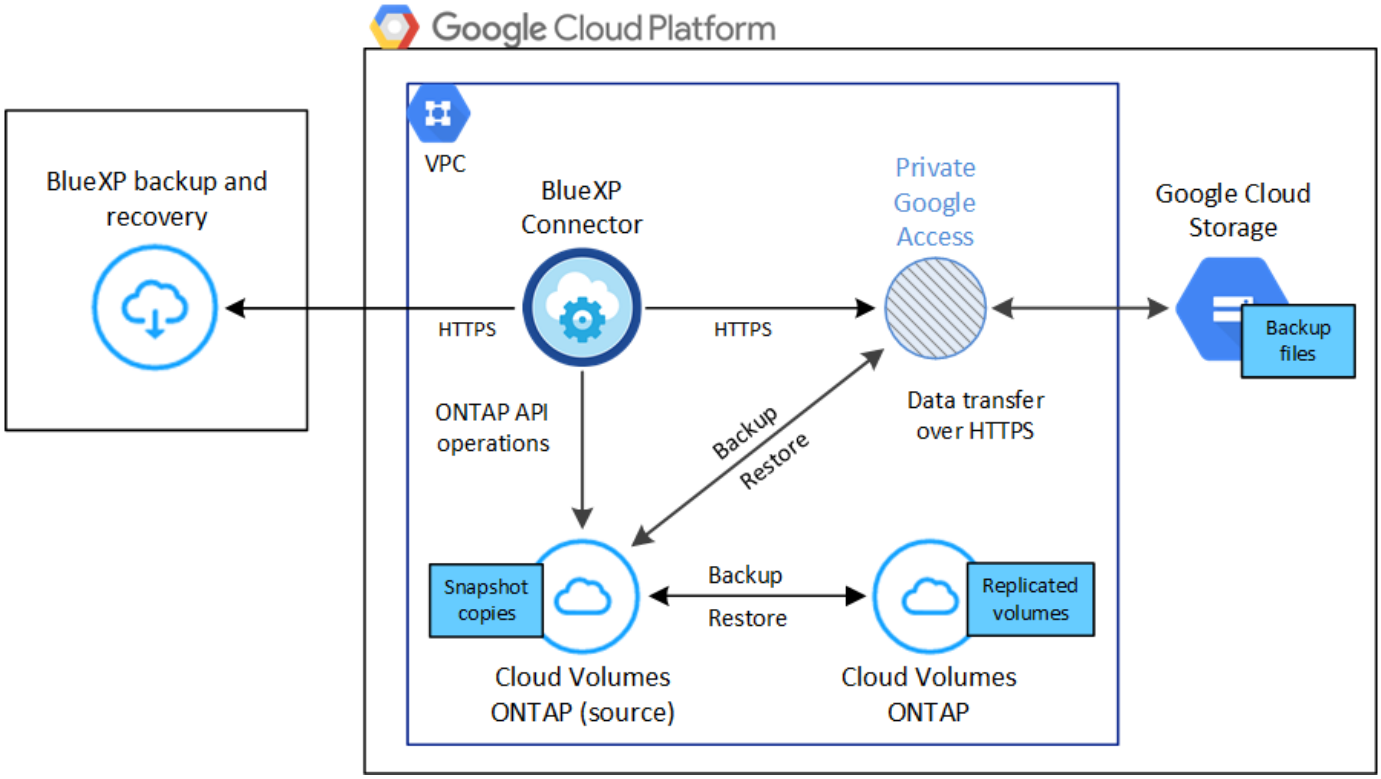
ONTAPボリュームでバックアップをアクティブ化します。

構成がサポートされていることを確認します

Google Cloud Storageへのボリュームのバックアップを開始する前に、次の要件を読み、サポートされる構成があることを確認してください。

次の図は、各コンポーネントとそれらの間の接続を示しています。

必要に応じて、パブリック接続またはプライベート接続を使用して、レプリケートされたボリュームのセカンダリONTAPシステムに接続することもできます。



サポートされる**ONTAP**のバージョン

ONTAP 9.8以上、ONTAP 9.8P13以降が推奨されます。

サポートされる **GCP** リージョン

BlueXPのバックアップとリカバリは、すべてのGCPリージョンでサポートされます "Cloud Volumes ONTAP がサポートされている場合"。

GCP サービスアカウント

事前定義された Storage Admin ロールを持つサービスアカウントが Google Cloud Project に必要です。 "サービスアカウントの作成方法について説明します"。

ライセンス要件を確認

BlueXPのバックアップとリカバリのPAYGOライセンスの場合は、Google MarketplaceでBlueXPサブスクリプションを購入して、Cloud Volumes ONTAP とBlueXPのバックアップとリカバリを導入できます。必要です "このBlueXPサブスクリプションを購読します" BlueXPのバックアップとリカバリを有効にする前に、BlueXPのバックアップとリカバリの課金は、このサブスクリプションを通じて行われます。 "作業環境ウィザードの[Details Credentialsページからサブスクライブできます。"^]。

BlueXPのバックアップとリカバリのBYOLライセンスの場合は、ライセンスの期間と容量にわたってサービスを使用できるネットアップのシリアル番号が必要です。 "BYOL ライセンスの管理方法について説明します"。

また、バックアップを保存するストレージスペースの Google サブスクリプションが必要です。

BlueXPコネクタを準備します

コネクタは、インターネットにアクセスできるGoogleリージョンにインストールする必要があります。

- "コネクタについて説明します"
- "Google Cloudにコネクタをデプロイします"

コネクタの権限を確認または追加します

BlueXPのバックアップとリカバリの「Search & Restore」機能を使用するには、コネクタがGoogle Cloud BigQueryサービスにアクセスできるように、コネクタのロールに特定の権限が必要です。以下の権限を確認し、ポリシーを変更する必要がある場合は手順に従います。

手順

1. を参照してください "Google Cloud Console の略"をクリックし、 * Roles * ページに移動します。
2. ページ上部のドロップダウンリストを使用して、編集するロールを含むプロジェクトまたは組織を選択します。
3. カスタムロールを選択します。
4. ロールの権限を更新するには、*[ロールの編集]*を選択します。
5. [権限の追加]*を選択して、次の新しい権限をロールに追加します。

```
bigquery.jobs.get
bigquery.jobs.list
bigquery.jobs.listAll
bigquery.datasets.create
bigquery.datasets.get
bigquery.jobs.create
bigquery.tables.get
bigquery.tables.getData
bigquery.tables.list
bigquery.tables.create
```

6. 編集したロールを保存するには、*[更新]*を選択します。

顧客が管理する暗号化キー（**CMEK**）の使用に必要な情報

Googleが管理するデフォルトの暗号化キーを使用する代わりに、お客様が管理する独自のキーを使用してデータを暗号化できます。クロスリージョンキーとクロスプロジェクトキーの両方がサポートされているため、CMEKキーのプロジェクトとは異なるバケット用のプロジェクトを選択できます。お客様が管理する独自のキーを使用する場合は、次の手順を実行します。

- アクティベーションウィザードでこの情報を追加できるように、キーリングとキー名が必要です。 "お客様が管理する暗号化キーの詳細については、こちらをご覧ください"。
- これらの必要な権限がコネクタの役割に含まれていることを確認する必要があります。

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- プロジェクトでGoogleの「Cloud Key Management Service（KMS）」APIが有効になっていることを確認する必要があります。を参照してください "Google Cloudドキュメント：APIの有効化" を参照してください。
- CMEKの考慮事項：*
- HSM（ハードウェアバックアップ）キーとソフトウェア生成キーの両方がサポートされます。
- 新しく作成またはインポートしたCloud KMSキーは両方サポートされます。
- リージョナルキーのみがサポートされます。グローバルキーはサポートされません。
- 現在、「対称暗号化/復号化」の目的のみがサポートされています。
- BlueXPのバックアップとリカバリによって、ストレージアカウントに関連付けられたサービスエージェントには、「CryptoKey encrypter/Decrypter（roles/cloudkms.cryptoKeyEncrypterDecrypter）」IAMロールが割り当てられます。

独自のバケットを作成します

デフォルトでは、サービスによってバケットが作成されます。独自のバケットを使用する場合は、バックアップアクティブ化ウィザードを開始する前にバケットを作成し、ウィザードでバケットを選択できます。

"独自のバケットの作成の詳細については、こちらをご覧ください"。

ボリュームをレプリケートするための**ONTAP**ネットワークの要件を確認します

BlueXPのバックアップとリカバリを使用してセカンダリONTAPシステムにレプリケートされたボリュームを作成する場合は、ソースシステムとデスティネーションシステムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワークの要件

- クラスタが社内にある場合は、社内ネットワークからクラウドプロバイダ内の仮想ネットワークへの接続が必要です。これは通常、 VPN 接続です。
- ONTAP クラスタは、サブネット、ポート、ファイアウォール、およびクラスタの追加要件を満たしている必要があります。

  Cloud Volumes ONTAPまたはオンプレミスのシステムにレプリケートできるため、オンプレミスのONTAPシステムのピアリング要件を確認してください。 "クラスタピアリングの前提条件については、ONTAP のドキュメントを参照してください"。

- インスタンスのセキュリティグループに、必要なインバウンドおよびアウトバウンドのルールが含まれている必要があります。具体的には、 ICMP とポート 11104 および 11105 のルールが必要です。これらのルールは、事前定義されたセキュリティグループに含まれています。
- 異なるサブネットにある 2 つの Cloud Volumes ONTAP システム間でデータをレプリケートするには、サブネットを一緒にルーティングする必要があります（これがデフォルト設定です）。

Cloud Volumes ONTAPでBlueXPのバックアップとリカバリを有効にする

BluXPのバックアップとリカバリを有効にするのは簡単です。手順は、既存のCloud Volumes ONTAPシステムと新規のシステムのどちらを使用しているかによって多少異なります。

新しいシステムで**BlueXP**のバックアップとリカバリを有効にする

作業環境のウィザードを完了して新しいCloud Volumes ONTAP システムを作成すると、BlueXPのバックアップとリカバリを有効にできます。

サービスアカウントがすでに設定されている必要があります。Cloud Volumes ONTAP システムの作成時にサービスアカウントを選択しなかった場合は、システムをオフにして、GCPコンソールからCloud Volumes ONTAP にサービスアカウントを追加する必要があります。

を参照してください "GCPでのCloud Volumes ONTAPの起動" を Cloud Volumes ONTAP 参照してください。

手順

1. BlueXPのキャンバスで*を選択し、クラウドプロバイダを選択して[Add New]*を選択します。Cloud Volumes ONTAPの作成*を選択します。
2. * 場所を選択 * ：「 * Google Cloud Platform * 」を選択します。
3. * タイプを選択 * ：「 * Cloud Volumes ONTAP * 」（シングルノードまたはハイアベイラビリティ）を選択します。
4. * 詳細と認証情報 * ：次の情報を入力します。

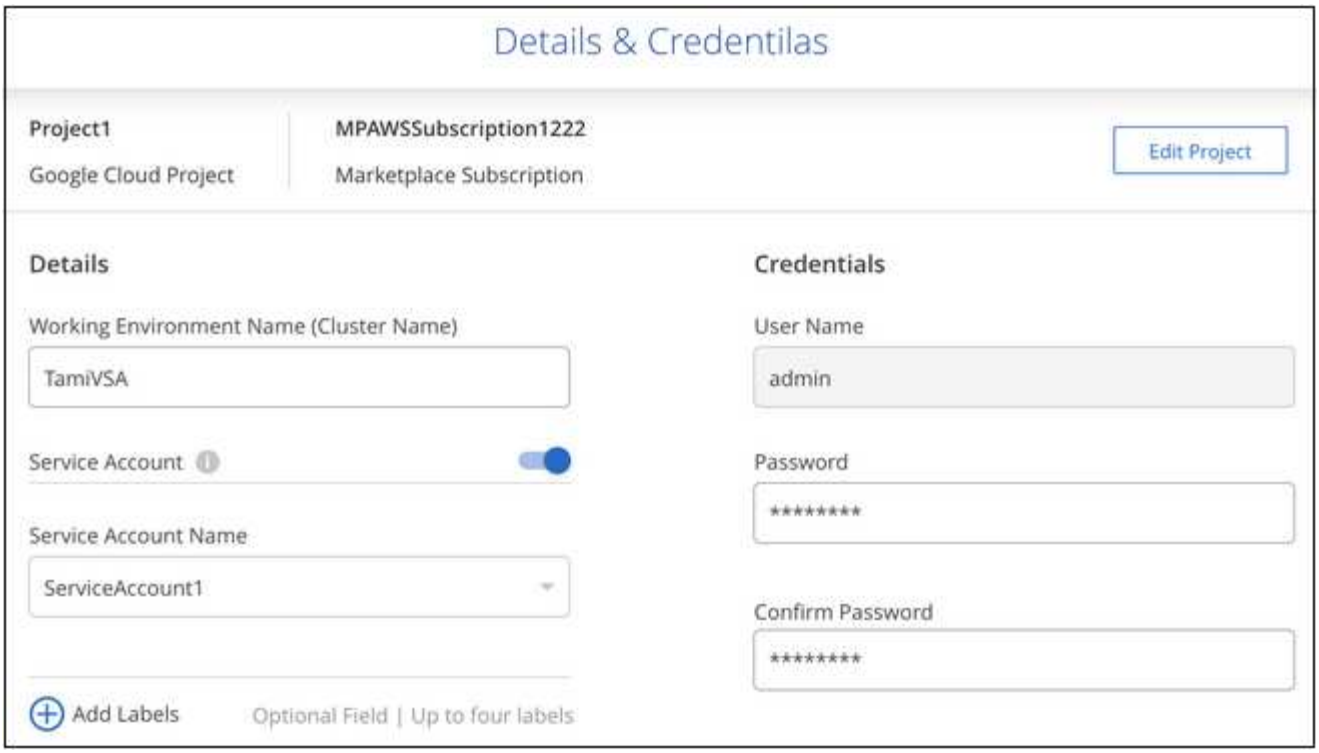
    a. 使用するプロジェクトがデフォルトのプロジェクト(コネクタが存在するプロジェクト)と異なる場合は、「*プロジェクトを編集」をクリックして新しいプロジェクトを選択します。

    b. クラスタ名を指定します。

    c. サービスアカウント * スイッチを有効にし、事前定義されたストレージ管理者ロールを持つサービスアカウントを選択します。これは、バックアップと階層化を有効にするために必要です。

    d. クレデンシャルを指定します。

    GCP Marketplace のサブスクリプションが登録されていることを確認します。



5. サービス：BlueXPのバックアップとリカバリサービスは有効なままにして、*[続行]*をクリックします。

6. ウィザードの各ページを設定し、システムを導入します を参照してください "GCPでのCloud Volumes ONTAPの起動"。

> バックアップ設定の変更またはレプリケーションの追加については、を参照してください "ONTAP バックアップを管理します"。

結果

システムでBlueXPのバックアップとリカバリが有効になっている。これらのCloud Volumes ONTAPシステムでボリュームを作成したら、BlueXPのバックアップとリカバリとを起動します "保護する各ボリュームでバックアップをアクティブ化します"。

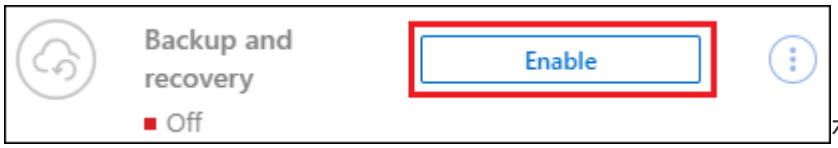
既存のシステムで**BlueXP**のバックアップとリカバリを有効にする

BlueXPのバックアップとリカバリは、いつでも作業環境から直接有効にできます。

手順

1. BlueXPのキャンバスで、作業環境を選択し、右側のパネルでバックアップとリカバリサービスの横にある*[有効化]*を選択します。

バックアップ先のGoogle Cloud StorageがCanvas上の作業環境として存在する場合は、クラスタをGoogle Cloud Storage作業環境にドラッグしてセットアップウィザードを開始できます。



ボタンのスクリーンショット。"]

バックアップ設定の変更またはレプリケーションの追加については、を参照してください "ONTAP バックアップを管理します"。

ONTAPボリュームでバックアップをアクティブ化します

オンプレミスの作業環境からいつでも直接バックアップをアクティブ化できます。

ウィザードでは、次の主な手順を実行します。

- [バックアップするボリュームを選択します]
- [バックアップ戦略を定義します]
- [選択内容を確認します]

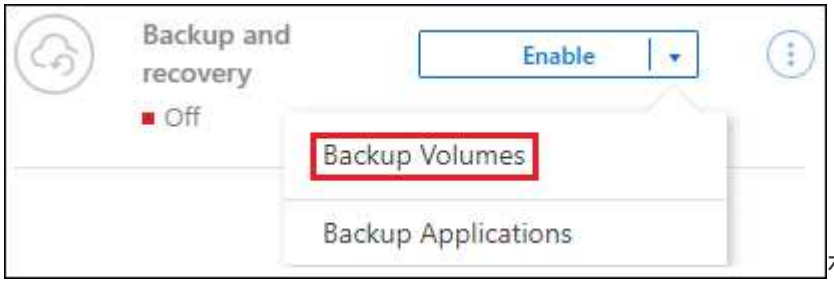
また可能です APIコマンドを表示します レビューステップでは、コードをコピーして、将来の作業環境のバックアップアクティベーションを自動化できます。

ウィザードを開始します

手順

1. 次のいずれかの方法でバックアップとリカバリのアクティブ化ウィザードにアクセスします。

   - BlueXPキャンバスで、作業環境を選択し、右パネルのバックアップとリカバリサービスの横にある*[有効化]>[ボリュームのバックアップ]*を選択します。

   ボタンのスクリーンショット。"]

   バックアップのGCPデスティネーションがCanvasの作業環境として存在する場合は、ONTAPクラスタをGCPオブジェクトストレージにドラッグできます。

   - [バックアップとリカバリ]バーで*を選択します。**[ボリューム]**タブで、[操作]* ••• アイコンをクリックし、（オブジェクトストレージへのレプリケーションまたはバックアップがまだ有効になっていない）単一のボリュームに対して*[バックアップのアクティブ化]*を選択します。

ウィザードの[Introduction]ページには、ローカルSnapshot、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で2番目のオプションを選択した場合は、1つのボリュームが選択された状態で[Define Backup Strategy]ページが表示されます。

2. 次のオプションに進みます。
    - BlueXPコネクタをすでにお持ちの場合は、これで準備は完了です。[次へ]*を選択します。
    - BlueXPコネクタをまだお持ちでない場合は、*[Add a Connector]*オプションが表示されます。を参照してください BlueXPコネクタを準備します。

バックアップするボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、Snapshotポリシー、レプリケーションポリシー、オブジェクトへのバックアップポリシーのうち1つ以上を含むボリュームです。

FlexVolボリュームとFlexGroupボリュームのどちらを保護するかを選択できますが、作業環境でバックアップをアクティブ化するときは、これらのボリュームを組み合わせて選択することはできません。方法を参照してください "作業環境内の追加ボリュームのバックアップをアクティブ化" （FlexVolまたはFlexGroup）初期ボリュームのバックアップの設定が完了したら、

- バックアップをアクティブ化できるのは、一度に1つのFlexGroupボリュームだけです。
- 選択するボリュームのSnapLock設定は同じである必要があります。すべてのボリュームでSnapLock Enterpriseが有効になっているかSnapLockが無効になっている必要があります。（SnapLock Complianceモードのボリュームには、ONTAP 9.14以降が必要です）。

手順

選択したボリュームにSnapshotポリシーまたはレプリケーションポリシーがすでに適用されている場合は、あとで選択したポリシーで既存のポリシーが上書きされます。

1. [Select Volumes]ページで、保護するボリュームを選択します。
    - 必要に応じて、行をフィルタして、特定のボリュームタイプや形式などのボリュームのみを表示し、選択を容易にします。
    - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます（FlexGroupボリュームは一度に1つだけ選択できます）。既存のFlexVolボリュームをすべてバックアップするには、最初に1つのボリュームをオンにしてから、タイトル行のボックスをオンにします。（☑ Volume Name）。
    - 個々のボリュームをバックアップするには、各ボリュームのボックス（☑ Volume_1）。
2. 「 * 次へ * 」を選択します。

バックアップ戦略を定義します

バックアップ戦略を定義するには、次のオプションを設定します。

- 1つまたはすべてのバックアップオプション（ローカルSnapshot、レプリケーション、オブジェクトストレージへのバックアップ）が必要かどうか
- アーキテクチャ
- ローカルSnapshotポリシー
- レプリケーションのターゲットとポリシー

選択したボリュームのSnapshotポリシーとレプリケーションポリシーがこの手順で選択したポリシーと異なる場合は、既存のポリシーが上書きされます。

- オブジェクトストレージ情報（プロバイダ、暗号化、ネットワーク、バックアップポリシー、エクスポートオプション）へのバックアップ。

手順

1. [Define backup strategy]ページで、次のいずれかまたはすべてを選択します。デフォルトでは、3つすべてが選択されています。
    - *ローカルSnapshot *：レプリケーションまたはオブジェクトストレージへのバックアップを実行する場合は、ローカルSnapshotを作成する必要があります。
    - レプリケーション：別のONTAPストレージシステムにレプリケートされたボリュームを作成します。
    - バックアップ：ボリュームをオブジェクトストレージにバックアップします。
2. アーキテクチャ:レプリケーションとバックアップを選択した場合は'次のいずれかの情報フローを選択します
    - カスケード：情報は、プライマリストレージシステムからセカンダリストレージ、およびセカンダリストレージからオブジェクトストレージに流れます。
    - ファンアウト：プライマリストレージシステムからセカンダリ_および_に、プライマリストレージからオブジェクトストレージに情報が流れます。

      これらのアーキテクチャの詳細については、を参照してください "保護対策を計画しましょう"。
3. *ローカルSnapshot *：既存のSnapshotポリシーを選択するか、作成します。

    バックアップをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

    ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

    - ポリシーの名前を入力します。
    - 最大5つのスケジュール（通常は異なる周波数）を選択します。
    - 「 * Create * 」を選択します。
4. レプリケーション：次のオプションを設定します。
    - レプリケーションターゲット：デスティネーションの作業環境とSVMを選択します。必要に応じて、レプリケートするボリュームの名前に追加するデスティネーションアグリゲートとプレフィックスまたはサフィックスを選択します。
    - レプリケーションポリシー：既存のレプリケーションポリシーを選択するか作成します。

      レプリケーションをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

      ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

      - ポリシーの名前を入力します。
      - 最大5つのスケジュール（通常は異なる周波数）を選択します。
      - 「 * Create * 」を選択します。
5. オブジェクトにバックアップ：*バックアップ*を選択した場合は、次のオプションを設定します。

- プロバイダ：* Google Cloud *を選択します。
- プロバイダ設定：バックアップを保存するプロバイダの詳細と地域を入力します。

  新しいバケットを作成するか、既存のバケットを選択します。

- 暗号化キー：新しいGoogleバケットを作成した場合は、プロバイダから提供された暗号化キー情報を入力します。データの暗号化を管理するために、デフォルトのGoogle Cloud暗号化キーを使用するか、Googleアカウントからお客様が管理する独自のキーを選択するかを選択します。

  独自の顧客管理キーを使用する場合は、キーボールトとキー情報を入力します。

  > 既存のGoogle Cloudバケットを選択した場合、暗号化情報はすでに使用可能なため、ここで入力する必要はありません。

- バックアップポリシー：オブジェクトストレージへの既存のバックアップポリシーを選択するか作成します。

  > バックアップをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

  ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

  - ポリシーの名前を入力します。
  - 最大5つのスケジュール（通常は異なる周波数）を選択します。
  - 「 * Create * 」を選択します。

- 既存の**Snapshot**コピーをバックアップコピーとしてオブジェクトストレージにエクスポート：この作業環境に、この作業環境に対して選択したバックアップスケジュールラベル（daily、weeklyなど）と一致するボリュームのローカルSnapshotコピーがある場合は、この追加のプロンプトが表示されます。ボリュームを最大限に保護するために、履歴Snapshotをすべてオブジェクトストレージにバックアップファイルとしてコピーする場合は、このチェックボックスをオンにします。

6. 「 * 次へ * 」を選択します。

選択内容を確認します

これにより、選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. [Review]ページで、選択内容を確認します。
2. 必要に応じて、Snapshotポリシーのラベルをレプリケーションポリシーおよびバックアップポリシーのラベルと自動的に同期する*チェックボックスをオンにします。これにより、レプリケーションポリシーとバックアップポリシーのラベルに一致するラベルを持つSnapshotが作成されます。
3. [バックアップのアクティブ化]*を選択します。

結果

BlueXPのバックアップとリカバリで、ボリュームの初期バックアップが作成されます。レプリケートされたボリュームとバックアップファイルのベースライン転送には、プライマリストレージシステムのデータのフルコピーが含まれます。以降の転送には、Snapshotコピーに含まれるプライマリストレージシステムデータの

差分コピーが含まれます。

レプリケートされたボリュームがデスティネーションクラスタに作成され、このボリュームはプライマリストレージシステムのボリュームと同期されます。

入力したGoogleアクセスキーとシークレットキーで指定されたサービスアカウントにGoogle Cloud Storageバケットが作成され、バックアップファイルがそこに保存されます。

バックアップは、デフォルトで_Standard_storageクラスに関連付けられています。低コストのNearlineクラス、_Coldline_クラス、または_Archive_storageクラスを使用できます。ただし、ストレージクラスの設定には、BlueXPのバックアップとリカバリのUIではなく、Googleを使用します。Google のトピックを参照してください "バケットのデフォルトのストレージクラスを変更する" を参照してください。

ボリュームバックアップダッシュボードが表示され、バックアップの状態を監視できます。

を使用して、バックアップジョブとリストアジョブのステータスを監視することもできます "［ジョブ監視］パネル"。

APIコマンドを表示します

バックアップとリカバリのアクティブ化ウィザードで使用するAPIコマンドを表示し、必要に応じてコピーすることができます。これは、将来の作業環境でバックアップを自動的にアクティブ化する場合に必要になることがあります。

手順

1. バックアップとリカバリのアクティブ化ウィザードで、*[API要求の表示]*を選択します。
2. コマンドをクリップボードにコピーするには、*コピー*アイコンを選択します。

次の手順

- 可能です "バックアップファイルとバックアップポリシーを管理"。バックアップの開始と停止、バックアップの削除、バックアップスケジュールの追加と変更などが含まれます。
- 可能です "クラスタレベルのバックアップの設定を管理します"。これには、バックアップをオブジェクトストレージにアップロードするためのネットワーク帯域幅の変更、将来のボリュームに対する自動バックアップ設定の変更などが含まれます。
- また可能です "ボリューム、フォルダ、または個々のファイルをバックアップファイルからリストアする" Google の Cloud Volumes ONTAP システムやオンプレミスの ONTAP システムに接続できます。

オンプレミスの **ONTAP** データを **Amazon S3** にバックアップ

オンプレミスのONTAPシステムからセカンダリストレージシステムおよびAmazon S3クラウドストレージへのボリュームデータのバックアップを開始するには、いくつかの手順を実行します。

「オンプレミスのONTAPシステム」には、FAS、AFF、ONTAP Selectシステムが含まれます。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。各手順の詳細については、このトピックの以降のセクションを参照してください。

1 使用する接続方法を特定します

オンプレミスのONTAP クラスタをパブリックインターネット経由でAWS S3に直接接続するか、VPNとAWS Direct Connectのどちらを使用してトラフィックをAWS S3にルーティングするかを選択します。

[接続方法を特定します]。

2 **BlueXP**コネクタを準備します

AWS VPCまたはオンプレミスにすでにコネクタが導入されている場合は、すべて設定されます。そうでない場合は、ONTAPデータをAWS S3ストレージにバックアップするためのBlueXPコネクタを作成する必要があります。また、コネクタのネットワーク設定をカスタマイズして AWS S3 に接続できるようにする必要があります。

コネクタの作成方法と、必要なネットワーク設定の定義方法について説明します。

3 ライセンス要件を確認

AWSとBlueXPの両方のライセンス要件を確認する必要があります。

を参照してください [ライセンス要件を確認]。

4 **ONTAP**クラスタを準備

BlueXPでONTAPクラスタを検出し、クラスタが最小要件を満たしていることを確認し、ネットワーク設定をカスタマイズしてクラスタをAWS S3に接続できるようにします。

ONTAPクラスタを準備する方法をご紹介します。

5 バックアップターゲットとして**Amazon S3**を準備します

ConnectorでS3バケットの作成と管理を行うための権限を設定します。また、オンプレミスのONTAP クラスタに対する権限を設定して、S3バケットに対してデータの読み取りと書き込みを行えるようにする必要があります。

必要に応じて、デフォルトの Amazon S3 暗号化キーを使用する代わりに、データ暗号化用に独自のカスタム管理キーを設定することもできます。 AWS S3環境でONTAPバックアップを受信できるようにする方法をご紹介します。

6 **ONTAP**ボリュームでバックアップをアクティブ化します

作業環境を選択し、右パネルのバックアップ/リカバリサービスの横にある*有効化>バックアップボリューム*をクリックします。次に、セットアップウィザードに従って、使用するレプリケーションポリシーとバックア

ップポリシー、およびバックアップするボリュームを選択します。

ONTAPボリュームでバックアップをアクティブ化します。

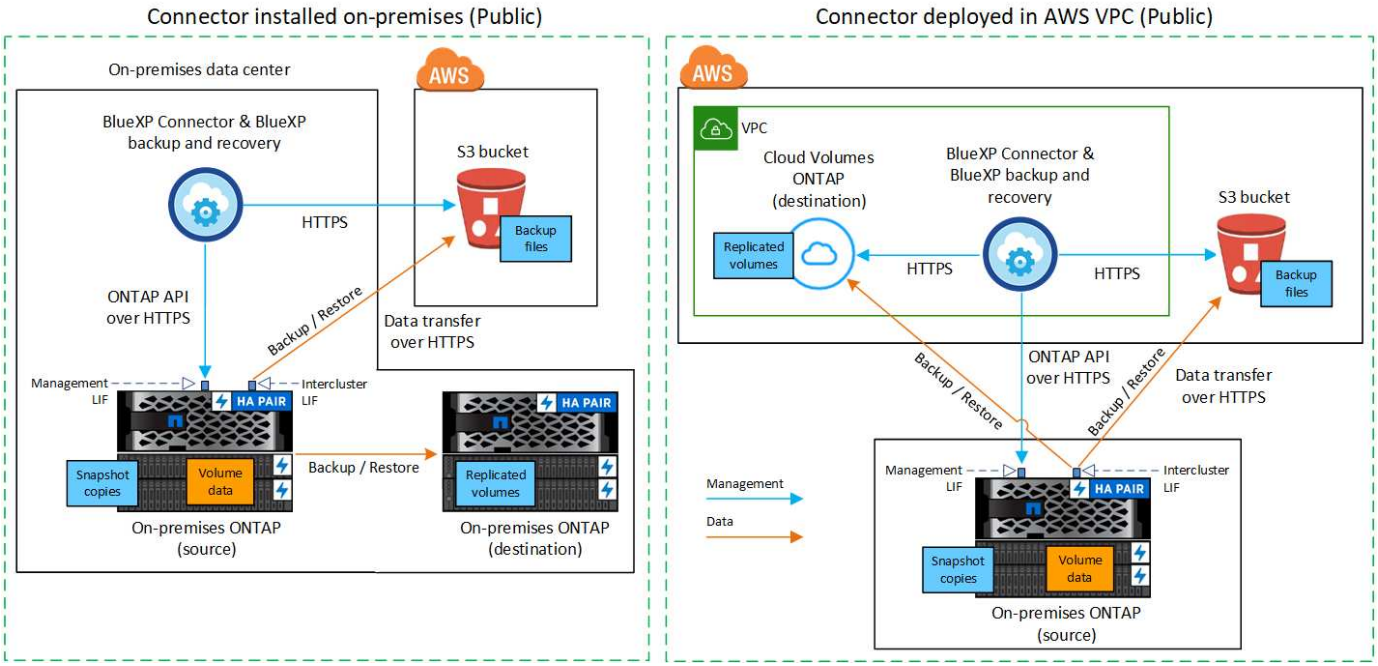
接続方法を特定します

オンプレミスのONTAPシステムからAWS S3へのバックアップを設定する場合は、どちらの接続方法を使用するかを選択してください。

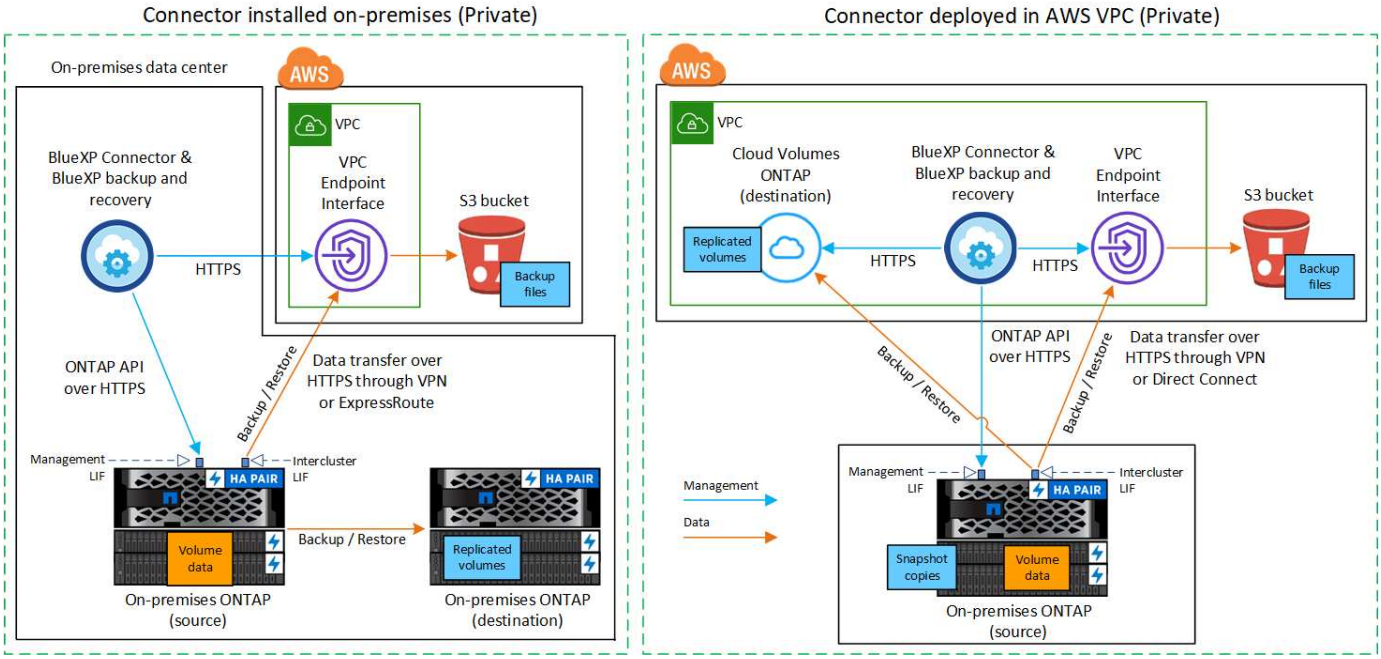
- パブリック接続-パブリックS3エンドポイントを使用して、ONTAPシステムをAWS S3に直接接続します。
- プライベート接続- VPNまたはAWS Direct Connectを使用し、プライベートIPアドレスを使用するVPCエンドポイントインターフェイスを介してトラフィックをルーティングします。

必要に応じて、パブリック接続またはプライベート接続を使用して、レプリケートされたボリュームのセカンダリONTAPシステムに接続することもできます。

次の図は、*パブリック接続*メソッドと、コンポーネント間の準備に必要な接続を示しています。オンプレミスにインストールしたコネクタや、AWS VPCに導入したコネクタを使用できます。



次の図は、*プライベート接続*メソッドと、コンポーネント間の準備に必要な接続を示しています。オンプレミスにインストールしたコネクタや、AWS VPCに導入したコネクタを使用できます。



BlueXPコネクタを準備します

BlueXPコネクタは'BlueXP機能の主要なソフトウェアですONTAP データのバックアップとリストアにはコネクタが必要です。

コネクタを作成または切り替えます

AWS VPCまたはオンプレミスにすでにコネクタが導入されている場合は、すべて設定されます。

そうでない場合は、ONTAPデータをAWS S3ストレージにバックアップするために、それらの場所の1つにコネクタを作成する必要があります。別のクラウドプロバイダに導入されているコネクタは使用できません。

- "コネクタについて説明します"
- "AWSにコネクタをインストールします"
- "コネクタをオンプレミスにインストールします"
- "AWS GovCloudリージョンにコネクタをインストールします"

  BlueXPのバックアップとリカバリは、コネクタがクラウドに導入されている場合はGovCloudリージョンでサポートされ、オンプレミスにインストールされている場合はサポートされません。また、AWS MarketplaceからConnectorを導入する必要があります。BlueXP SaaS Webサイトから政府機関のリージョンにコネクタを導入することはできません。

コネクタのネットワーク要件を準備

次のネットワーク要件が満たされていることを確認します。

- コネクタが取り付けられているネットワークで次の接続が有効になっていることを確認します。
  - ポート443を介してBlueXPバックアップおよびリカバリサービスとS3オブジェクトストレージへのHTTPS接続 ("エンドポイントのリストを参照してください")

- ONTAP クラスタ管理 LIF へのポート 443 経由の HTTPS 接続
- AWSおよびAWS GovCloud環境では、追加のインバウンドおよびアウトバウンドのセキュリティグループルールが必要です。を参照してください "AWS のコネクタのルール" を参照してください。

- "コネクタにS3バケットを管理する権限があることを確認します"。
- ONTAP クラスタからVPCへのDirect ConnectまたはVPN接続が確立されている状況で、コネクタとS3の間の通信をAWS内部ネットワーク（*プライベート*接続）のままにする場合は、S3へのVPCエンドポイントインターフェイスを有効にする必要があります。 VPC エンドポイントインターフェイスの設定方法を参照してください。

ライセンス要件を確認

AWSとBlueXPの両方のライセンス要件を確認する必要があります。

- クラスタでBlueXPのバックアップとリカバリをアクティブ化するには、AWSから従量課金制（PAYGO）のBlueXP Marketplaceサービスに登録するか、ネットアップからBlueXPバックアップとリカバリのBYOLライセンスを購入してアクティブ化する必要があります。これらのライセンスはアカウント用であり、複数のシステムで使用できます。
  - BlueXPのバックアップとリカバリのPAYGOライセンスを購入するには、のサブスクリプションが必要です "AWS Marketplaceで提供されるNetApp BlueXPサービス"。BlueXPのバックアップとリカバリの課金は、このサブスクリプションを通じて行われます。
  - BlueXPのバックアップとリカバリのBYOLライセンスの場合は、ライセンスの期間と容量にわたってサービスを使用できるネットアップのシリアル番号が必要です。 "BYOL ライセンスの管理方法について説明します"。
- バックアップを格納するオブジェクトストレージスペース用の AWS サブスクリプションが必要です。

サポートされている地域

すべてのリージョンで、オンプレミスシステムから Amazon S3 へのバックアップを作成できます "Cloud Volumes ONTAP がサポートされている場合"AWS GovCloud リージョンを含む。サービスのセットアップ時にバックアップを保存するリージョンを指定します。

ONTAPクラスタを準備

ソースのオンプレミスONTAPシステムと、セカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムを準備する必要があります。

ONTAPクラスタの準備では、次の手順を実行します。

- BlueXPでONTAPシステムを検出しましょう
- ONTAPのシステム要件を確認
- オブジェクトストレージにデータをバックアップするためのONTAPネットワークの要件を確認します
- ボリュームをレプリケートするためのONTAPネットワークの要件を確認します

BlueXPでONTAPシステムを検出しましょう

ソースのオンプレミスONTAPシステムとセカンダリのオンプレミスONTAPシステムまたはCloud Volumes ONTAPシステムの両方が、BlueXPキャンバスで利用可能である必要があります。

クラスタを追加するには、クラスタ管理 IP アドレスと admin ユーザアカウントのパスワードが必要です。"クラスタの検出方法について説明します"。

ONTAPのシステム要件を確認

次のONTAP要件が満たされていることを確認します。

- ONTAP 9.8以上、ONTAP 9.8P13以降が推奨されます。
- SnapMirror ライセンス（ Premium Bundle または Data Protection Bundle に含まれます）。

  注： BlueXPのバックアップとリカバリを使用する場合、「Hybrid Cloud Bundle」は必要ありません。

  方法をご確認ください "クラスタライセンスを管理します"。

- 時間とタイムゾーンが正しく設定されている。方法をご確認ください "クラスタ時間を設定します"。
- データをレプリケートする場合は、データをレプリケートする前に、ソースシステムとデスティネーションシステムで互換性のあるONTAPバージョンが実行されていることを確認する必要があります。

  "SnapMirror 関係に対して互換性のある ONTAP バージョンを表示します"。

オブジェクトストレージにデータをバックアップするための**ONTAP**ネットワークの要件を確認します

オブジェクトストレージに接続するシステムで、次の要件を設定する必要があります。

- ファンアウトバックアップアーキテクチャの場合は、_primary_systemで次の設定を行います。
- カスケードバックアップアーキテクチャの場合は、_secondary_systemで次の設定を行います。

次のONTAPクラスタネットワーク要件が必要です。

- クラスタには、コネクタからクラスタ管理 LIF へのインバウンド HTTPS 接続が必要です。
- クラスタ間 LIF は、バックアップ対象のボリュームをホストする各 ONTAP ノードに必要です。これらのクラスタ間 LIF がオブジェクトストアにアクセスできる必要があります。

  クラスタは、バックアップおよびリストア処理のために、インタークラスタ LIF から Amazon S3 ストレージへのポート 443 経由のアウトバウンド HTTPS 接続を開始します。ONTAP は、オブジェクトストレージとの間でデータの読み取りと書き込みを行います。オブジェクトストレージが開始されることはなく、応答するだけです。

- クラスタ間 LIF は、 ONTAP がオブジェクトストレージへの接続に使用する IPspace に関連付けられている必要があります。 "IPspace の詳細については、こちらをご覧ください"。

  BlueXPのバックアップとリカバリをセットアップするときに、使用するIPspaceを指定するように求められます。これらの LIF が関連付けられている IPspace を選択します。これは、「デフォルト」の IPspace または作成したカスタム IPspace です。

  「 default 」以外の IPspace を使用する場合は、オブジェクトストレージへのアクセスを取得するために静的ルートの作成が必要になることがあります。

  IPspace内のすべてのクラスタ間LIFがオブジェクトストアにアクセスできる必要があります。現在のIPspaceに対してこれを設定できない場合は、すべてのクラスタ間LIFがオブジェクトストアにアクセス

できる専用のIPspaceを作成する必要があります。

- ボリュームが配置されている Storage VM 用に DNS サーバが設定されている必要があります。方法を参照してください "SVM 用に DNS サービスを設定"。
- 必要に応じてファイアウォールルールを更新して、ONTAP からオブジェクトストレージへのBlueXPのバックアップおよびリカバリ接続（ポート443経由）、およびStorage VMからDNSサーバへの名前解決トラフィック（TCP / UDP）を許可します。
- AWSでS3接続にプライベートVPCインターフェイスエンドポイントを使用している場合は、HTTPS / 443を使用するために、S3エンドポイント証明書をONTAP クラスタにロードする必要があります。 VPC エンドポイントインターフェイスのセットアップ方法を参照して、 S3 証明書をロードしてください。
- "ONTAP クラスタにS3バケットへのアクセス権限があることを確認します"。

ボリュームをレプリケートするための**ONTAP**ネットワークの要件を確認します

BlueXPのバックアップとリカバリを使用してセカンダリONTAPシステムにレプリケートされたボリュームを作成する場合は、ソースシステムとデスティネーションシステムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワークの要件

- クラスタが社内にある場合は、社内ネットワークからクラウドプロバイダ内の仮想ネットワークへの接続が必要です。これは通常、 VPN 接続です。
- ONTAP クラスタは、サブネット、ポート、ファイアウォール、およびクラスタの追加要件を満たしている必要があります。

  Cloud Volumes ONTAPまたはオンプレミスのシステムにレプリケートできるため、オンプレミスのONTAPシステムのピアリング要件を確認してください。 "クラスタピアリングの前提条件については、ONTAP のドキュメントを参照してください"。

Cloud Volumes ONTAPネットワークの要件

- インスタンスのセキュリティグループに、必要なインバウンドおよびアウトバウンドのルールが含まれている必要があります。具体的には、 ICMP とポート 11104 および 11105 のルールが必要です。これらのルールは、事前定義されたセキュリティグループに含まれています。

バックアップターゲットとして**Amazon S3**を準備します

Amazon S3をバックアップターゲットとして準備するには、次の手順を実行します。

- S3権限を設定
- （オプション）独自のS3バケットを作成します。（必要に応じて、サービスによってバケットが作成されます）。
- （オプション）データ暗号化用にお客様が管理するAWSキーを設定します。
- （オプション）VPCエンドポイントインターフェイスを使用して、システムにプライベート接続を設定します。

S3 権限をセットアップする

次の 2 つの権限セットを設定する必要があります。

- S3バケットの作成と管理を行うコネクタの権限。
- オンプレミスの ONTAP クラスタの権限。 S3 バケットに対してデータの読み取りと書き込みを行うことができます。

手順

1. （最新のから）次の S3 権限を確認します "BlueXPポリシー"）は、コネクタに権限を付与する IAM ロールの一部です。表示されていない場合は、を参照してください "AWS のドキュメント：「 Editing IAM policies"。

```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutBucketOwnershipControls",
                "s3:PutBucketPublicAccessBlock",
                "s3:PutEncryptionConfiguration",
                "s3:GetObjectVersionTagging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectVersionAcl",
                "s3:PutObjectTagging",
                "s3:DeleteObjectTagging",
                "s3:GetObjectRetention",
                "s3:DeleteObjectVersionTagging",
                "s3:PutBucketObjectLockConfiguration",
                "s3:DeleteObjectVersion",
                "s3:GetObjectTagging",
                "s3:PutBucketVersioning",
                "s3:PutObjectVersionTagging",
                "s3:GetBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:PutObjectRetention",
                "s3:GetObjectVersion",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
```

```
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
                "glue:BatchDeletePartition"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        }
```

AWS Chinaリージョンでバックアップを作成する場合は、IAMポリシーのall_Resource_sectionsの下にあるAWSリソース名「arn」を「aws」から「aws-cn」に変更する必要があります `arn:aws-cn:s3:::netapp-backup-*`。

2. サービスをアクティブ化すると、バックアップウィザードからアクセスキーとシークレットキーの入力を求められます。これらのクレデンシャルは、 ONTAP がデータをバックアップして S3 バケットにリストアできるように ONTAP クラスタに渡されます。そのためには、以下の権限を持つ IAM ユーザを作成する必要があります。

   を参照してください "AWS ドキュメント：「 Creating a Role to Delegate Permissions to an IAM User"。

```
{
    "Version": "2012-10-17",
     "Statement": [
        {
           "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": "arn:aws:s3:::netapp-backup-*",
            "Effect": "Allow",
            "Sid": "backupPolicy"
        },
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

独自のバケットを作成します

デフォルトでは、サービスによってバケットが作成されます。独自のバケットを使用する場合は、バックアップアクティブ化ウィザードを開始する前にバケットを作成し、ウィザードでバケットを選択できます。

"独自のバケットの作成の詳細については、こちらをご覧ください"。

独自のバケットを作成する場合は、バケット名として「netapp-backup」を使用する必要があります。カスタム名を使用する必要がある場合は、を編集します `ontapcloud-instance-policy-netapp-backup` 既存のCVOにIAMRoleを割り当て、S3権限に次のリストを追加します。含める必要があります `"Resource": "arn:aws:s3:::*"` バケットに関連付ける必要があるすべての権限を割り当てます。

略称は「[
"S3：ListBucket"
"S3：GetBucketLocation"
]
リソース：arn：aws：s3：：：、
"Effect"："Allow"
}、
{
略称は「**[**
"S3：GetObject"、
"S3：PutObject"、
"S3：DeleteObject"、
"S3：ListAllMyBuckets"、
"S3：PutObjectTagging"、
"S3：GetObjectTagging"、
"S3：RestoreObject"、
"S3：GetBucketObjectLockConfiguration"、
"S3：GetObjectRetention"、
"S3：PutBucketObjectLockConfiguration"、
"S3：PutObjectRetention"
]
リソース：**arn：aws：s3**：：：、

データ暗号化用に、お客様が管理する**AWS**キーをセットアップ

デフォルトのAmazon S3暗号化キーを使用してオンプレミスクラスタとS3バケット間でやり取りされるデータを暗号化する場合は、デフォルトのインストールでそのタイプの暗号化が使用されるため、すべての暗号化キーが設定されます。

デフォルトのキーを使用するのではなく、お客様が管理する独自のキーをデータの暗号化に使用する場合は、BlueXPのバックアップとリカバリウィザードを開始する前に、暗号化に対応するキーをあらかじめ設定しておく必要があります。 "独自のキーの使用方法を参照してください"。

VPCエンドポイントインターフェイスを使用して、システムにプライベート接続を設定します

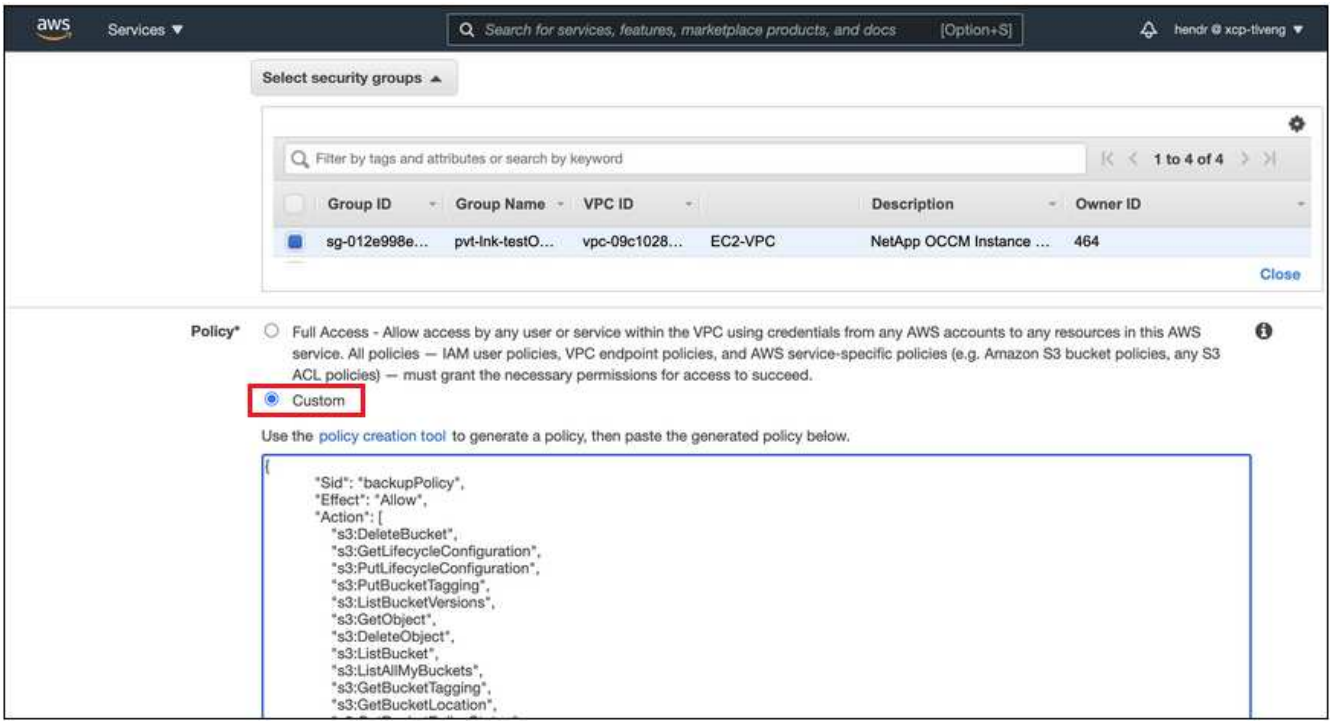
標準のパブリックインターネット接続を使用する場合は、すべてのアクセス権がコネクタによって設定され、他に必要な操作はありません。このタイプの接続がに表示されます "最初のダイアグラム"。

オンプレミスのデータセンターからVPCへのインターネット接続をよりセキュアにする場合は、バックアップアクティブ化ウィザードでAWS PrivateLink接続を選択できます。VPNまたはAWS Direct Connectを使用し

て、プライベートIPアドレスを使用するVPCエンドポイントインターフェイス経由でオンプレミスシステムに接続する場合は、この環境が必要です。このタイプの接続がに表示されます "2番目の図"。

手順

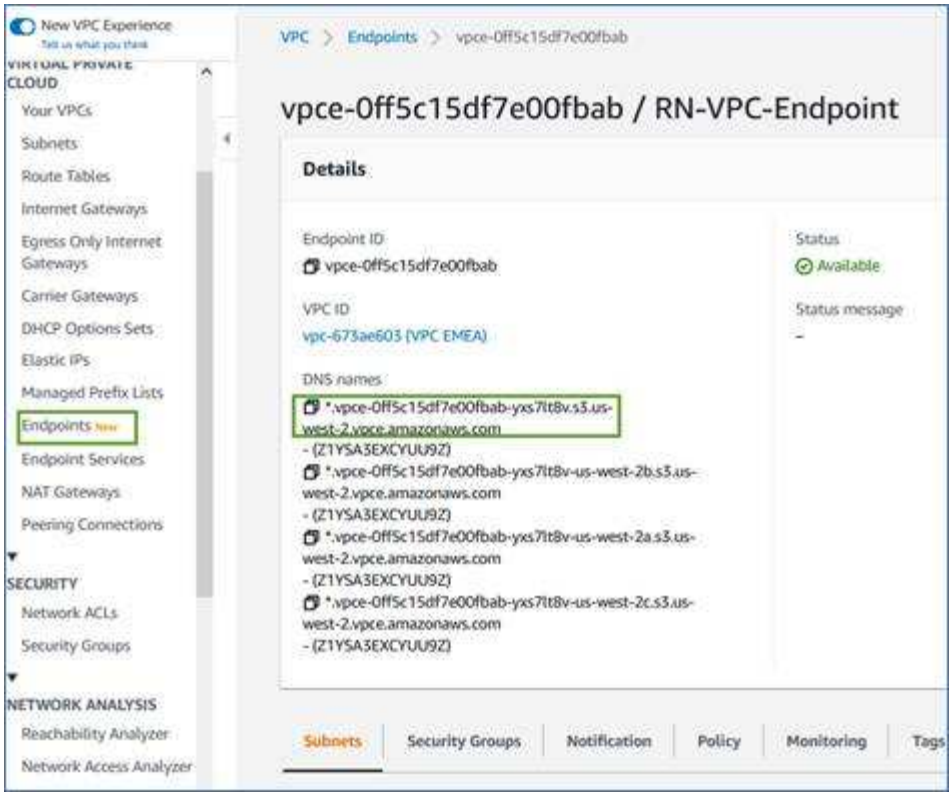
1. Amazon VPC コンソールまたはコマンドラインを使用して、インターフェイスエンドポイント設定を作成します。 "詳細については、AWS PrivateLink for Amazon S3を参照してください"。
2. BlueXPコネクタに関連付けられているセキュリティグループ設定を変更します。このポリシーを「Custom 」（「 Full Access 」から）に変更する必要があります。また、変更する必要があります バックアップポリシーから S3 権限を追加します 前に示したように、



プライベートエンドポイントとの通信にポート80（HTTP）を使用している場合は、すべて設定されています。クラスタでBlueXPのバックアップとリカバリを有効にすることができます。

ポート443（HTTPS）を使用してプライベートエンドポイントと通信する場合は、VPC S3エンドポイントから証明書をコピーし、次の4つの手順でONTAP クラスタに追加する必要があります。

3. AWS コンソールからエンドポイントの DNS 名を取得します。



4. VPC S3 エンドポイントから証明書を取得します。これは、で行います "BlueXPコネクタをホストしているVMにログインします" 実行するコマンドエンドポイントの DNS 名を入力するときは、先頭に「 * 」を追加して、「 * 」を置き換えます。

```
[ec2-user@ip-10-160-4-68 ~]$ openssl s_client -connect bucket.vpce-
0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443
-showcerts
```

5. このコマンドの出力から、 S3 証明書のデータ（ BEGIN / END CERTIFICATE タグを含む、との間のすべてのデータ）をコピーします。

```
Certificate chain
0 s:/CN=s3.us-west-2.amazonaws.com`
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
-----BEGIN CERTIFICATE-----
MIIM6zCCC9OgAwIBAgIQA7MGJ4FaDBR8uL0KR3oltTANBgkqhkiG9w0BAQsFADBG
…
…
GqvbOz/oO2NWLLFCqI+xmkLcMiPrZy+/6Af+HH2mLCM4EsI2b+IpBmPkriWnnxo=
-----END CERTIFICATE-----
```

6. ONTAP クラスタの CLI にログインし、次のコマンドを使用してコピーした証明書を適用します（代わりに独自の Storage VM 名を指定します）。

```
cluster1::> security certificate install -vserver cluster1 -type server-
ca
Please enter Certificate: Press <Enter> when done
```

ONTAPボリュームでバックアップをアクティブ化します

オンプレミスの作業環境からいつでも直接バックアップをアクティブ化できます。

ウィザードでは、次の主な手順を実行します。

- [バックアップするボリュームを選択します]
- [バックアップ戦略を定義します]
- [選択内容を確認します]

また可能です APIコマンドを表示します レビューステップでは、コードをコピーして、将来の作業環境のバックアップアクティベーションを自動化できます。

ウィザードを開始します

手順

1. 次のいずれかの方法でバックアップとリカバリのアクティブ化ウィザードにアクセスします。

   - BlueXPキャンバスで、作業環境を選択し、右パネルのバックアップとリカバリサービスの横にある*[有効化]>[ボリュームのバックアップ]*を選択します。

     バックアップのAmazon S3デスティネーションがCanvasの作業環境として存在する場合は、ONTAPクラスタをAmazon S3オブジェクトストレージにドラッグできます。

   - [バックアップとリカバリ]バーで*を選択します。**[**ボリューム**]**タブで、[操作]* ••• アイコンをクリックし、（オブジェクトストレージへのレプリケーションまたはバックアップがまだ有効になっていない）単一のボリュームに対して*[バックアップのアクティブ化]*を選択します。

   ウィザードの[Introduction]ページには、ローカルSnapshot、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で2番目のオプションを選択した場合は、1つのボリュームが選択された状態で[Define Backup Strategy]ページが表示されます。

2. 次のオプションに進みます。

   - BlueXPコネクタをすでにお持ちの場合は、これで準備は完了です。[次へ]*を選択します。
   - BlueXPコネクタをまだお持ちでない場合は、*[Add a Connector]*オプションが表示されます。を参照してください BlueXPコネクタを準備します。

バックアップするボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、Snapshotポリシー、レプリケーションポリシー、オブジェクトへのバックアップポリシーのうち1つ以上を含むボリュームです。

FlexVolボリュームとFlexGroupボリュームのどちらを保護するかを選択できますが、作業環境でバックアップをアクティブ化するときは、これらのボリュームを組み合わせて選択することはできません。方法を参照して

ください "作業環境内の追加ボリュームのバックアップをアクティブ化" （FlexVolまたはFlexGroup）初期ボリュームのバックアップの設定が完了したら、

> - バックアップをアクティブ化できるのは、一度に1つのFlexGroupボリュームだけです。
> - 選択するボリュームのSnapLock設定は同じである必要があります。すべてのボリュームでSnapLock Enterpriseが有効になっているかSnapLockが無効になっている必要があります。（SnapLock Complianceモードのボリュームには、ONTAP 9.14以降が必要です）。

手順

選択したボリュームにSnapshotポリシーまたはレプリケーションポリシーがすでに適用されている場合は、あとで選択したポリシーで既存のポリシーが上書きされます。

1. [Select Volumes]ページで、保護するボリュームを選択します。
   - 必要に応じて、行をフィルタして、特定のボリュームタイプや形式などのボリュームのみを表示し、選択を容易にします。
   - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます（FlexGroupボリュームは一度に1つだけ選択できます）。既存のFlexVolボリュームをすべてバックアップするには、最初に1つのボリュームをオンにしてから、タイトル行のボックスをオンにします。（☑ Volume Name）。
   - 個々のボリュームをバックアップするには、各ボリュームのボックス（☑ Volume_1）。
2. 「 * 次へ * 」を選択します。

バックアップ戦略を定義します

バックアップ戦略を定義するには、次のオプションを設定します。

- 1つまたはすべてのバックアップオプション（ローカルSnapshot、レプリケーション、オブジェクトストレージへのバックアップ）が必要かどうか
- アーキテクチャ
- ローカルSnapshotポリシー
- レプリケーションのターゲットとポリシー

> 選択したボリュームのSnapshotポリシーとレプリケーションポリシーがこの手順で選択したポリシーと異なる場合は、既存のポリシーが上書きされます。

- オブジェクトストレージ情報（プロバイダ、暗号化、ネットワーク、バックアップポリシー、エクスポートオプション）へのバックアップ。

手順

1. [Define backup strategy]ページで、次のいずれかまたはすべてを選択します。デフォルトでは、3つすべてが選択されています。
   - *ローカルSnapshot *：レプリケーションまたはオブジェクトストレージへのバックアップを実行する場合は、ローカルSnapshotを作成する必要があります。
   - レプリケーション：別のONTAPストレージシステムにレプリケートされたボリュームを作成します。
   - バックアップ：ボリュームをオブジェクトストレージにバックアップします。

2. アーキテクチャ:レプリケーションとバックアップを選択した場合は'次のいずれかの情報フローを選択します
   - カスケード：情報は、プライマリからセカンダリからオブジェクトストレージへ、セカンダリからオブジェクトストレージへと流れます。
   - ファンアウト：プライマリからセカンダリへ、プライマリからオブジェクトストレージへ、情報が流れます。

     これらのアーキテクチャの詳細については、を参照してください "保護対策を計画しましょう"。

3. *ローカルSnapshot *：既存のSnapshotポリシーを選択するか、ポリシーを作成します。

   Snapshotをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

4. ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。
   - ポリシーの名前を入力します。
   - 最大5つのスケジュール（通常は異なる周波数）を選択します。
     - オブジェクトへのバックアップポリシーの場合は、DataLockとRansomware Protectionを設定します。DataLockとランサムウェア対策の詳細については、 "オブジェクトへのバックアップポリシーの設定"。
   - 「 * Create * 」を選択します。
5. レプリケーション：次のオプションを設定します。
   - レプリケーションターゲット：デスティネーションの作業環境とSVMを選択します。必要に応じて、レプリケートするボリュームの名前に追加するデスティネーションアグリゲートとプレフィックスまたはサフィックスを選択します。
   - レプリケーションポリシー：既存のレプリケーションポリシーを選択するか、ポリシーを作成します。

     レプリケーションをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

     ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

     - ポリシーの名前を入力します。
     - 最大5つのスケジュール（通常は異なる周波数）を選択します。
     - 「 * Create * 」を選択します。
6. オブジェクトにバックアップ：*バックアップ*を選択した場合は、次のオプションを設定します。
   - プロバイダ：[Amazon Web Services]*を選択します。
   - プロバイダ設定：バックアップを保存するプロバイダの詳細とAWSリージョンを入力します。

     アクセスキーとシークレットキーは、 ONTAP クラスタに S3 バケットへのアクセスを付与するために作成した IAM ユーザ用のものです。

   - * Bucket *：既存のS3バケットを選択するか、新しいバケットを作成します。を参照してください "S3

バケットを追加"。

- 暗号化キー：新しいS3バケットを作成した場合は、プロバイダから提供された暗号化キー情報を入力します。データの暗号化を管理するために、デフォルトのAmazon S3暗号化キーを使用するか、AWSアカウントからお客様が管理する独自のキーを選択するかを選択します。

> 既存のバケットを選択した場合、暗号化情報はすでに使用可能なため、ここで入力する必要はありません。

- ネットワーク：IPspace、およびプライベートエンドポイントを使用するかどうかを選択します。プライベートエンドポイントはデフォルトで無効になっています。
  i. バックアップするボリュームが配置されている ONTAP クラスタ内の IPspace 。この IPspace のクラスタ間 LIF 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。
  ii. 必要に応じて、以前に設定した AWS PrivateLink を使用するかどうかを選択します。 "AWS PrivateLink for Amazon S3 の使用に関する詳細を参照してください"。
- バックアップポリシー：既存のバックアップポリシーを選択するか、ポリシーを作成します。

> バックアップをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

  - ポリシーの名前を入力します。
  - 最大5つのスケジュール（通常は異なる周波数）を選択します。
  - 「 * Create * 」を選択します。
- 既存の**Snapshot**コピーをバックアップコピーとしてオブジェクトストレージにエクスポート：この作業環境に、この作業環境に対して選択したバックアップスケジュールラベル（daily、weeklyなど）と一致するボリュームのローカルSnapshotコピーがある場合は、この追加のプロンプトが表示されます。ボリュームを最大限に保護するために、履歴Snapshotをすべてオブジェクトストレージにバックアップファイルとしてコピーする場合は、このチェックボックスをオンにします。

7. 「 * 次へ * 」を選択します。

選択内容を確認します

これにより、選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. [Review]ページで、選択内容を確認します。
2. 必要に応じて、Snapshotポリシーのラベルをレプリケーションポリシーおよびバックアップポリシーのラベルと自動的に同期する*チェックボックスをオンにします。これにより、レプリケーションポリシーとバックアップポリシーのラベルに一致するラベルを持つSnapshotが作成されます。
3. [バックアップのアクティブ化]*を選択します。

結果

BlueXPのバックアップとリカバリで、ボリュームの初期バックアップが作成されます。レプリケートされたボリュームとバックアップファイルのベースライン転送には、プライマリストレージシステムのデータのフルコピーが含まれます。以降の転送には、Snapshotコピーに含まれるプライマリデータの差分コピーが含まれ

ます。

レプリケートされたボリュームが、プライマリストレージボリュームと同期されるデスティネーションクラスタに作成されます。

入力したS3アクセスキーとシークレットキーで指定されたサービスアカウントにS3バケットが作成され、バックアップファイルがそこに格納されます。ボリュームバックアップダッシュボードが表示され、バックアップの状態を監視できます。

を使用して、バックアップジョブとリストアジョブのステータスを監視することもできます "［ジョブ監視］パネル"。

APIコマンドを表示します

バックアップとリカバリのアクティブ化ウィザードで使用するAPIコマンドを表示し、必要に応じてコピーすることができます。これは、将来の作業環境でバックアップを自動的にアクティブ化する場合に必要になることがあります。

手順

1. バックアップとリカバリのアクティブ化ウィザードで、*[API要求の表示]*を選択します。
2. コマンドをクリップボードにコピーするには、*コピー*アイコンを選択します。

次の手順

- 可能です "バックアップファイルとバックアップポリシーを管理"。バックアップの開始と停止、バックアップの削除、バックアップスケジュールの追加と変更などが含まれます。
- 可能です "クラスタレベルのバックアップの設定を管理します"。これには、クラウドストレージへのアクセスにONTAP で使用するストレージキーの変更、オブジェクトストレージへのバックアップのアップロードに使用できるネットワーク帯域幅の変更、将来のボリュームに対する自動バックアップ設定の変更などが含まれます。
- また可能です "ボリューム、フォルダ、または個々のファイルをバックアップファイルからリストアする" AWS の Cloud Volumes ONTAP システムやオンプレミスの ONTAP システムに接続できます。

オンプレミスの**ONTAP**データを**Azure Blob**ストレージにバックアップ

オンプレミスのONTAPシステムからセカンダリストレージシステムおよびAzure BLOBストレージへのボリュームデータのバックアップを開始するには、いくつかの手順を実行します。

「オンプレミスのONTAPシステム」には、FAS、AFF、ONTAP Selectシステムが含まれます。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。各手順の詳細については、このトピックの以降のセクションを参照してください。

1 使用する接続方法を特定します

オンプレミスのONTAPクラスタをパブリックインターネット経由でAzureに直接接続するか、VPNまたはAzure ExpressRouteを使用してプライベートVPCエンドポイントインターフェイス経由でAzureにトラフィックをルーティングするかを選択します。

[接続方法を特定します]。

2 **BlueXP**コネクタを準備します

Azure VNetまたはオンプレミスにコネクタがすでに導入されている場合は、すべて設定されます。そうでない場合は、ONTAPデータをAzure BLOBストレージにバックアップするためのBlueXPコネクタを作成する必要があります。また、コネクタがAzureに接続できるように、コネクタのネットワーク設定をカスタマイズする必要があります。

コネクタの作成方法と、必要なネットワーク設定の定義方法について説明します。

3 ライセンス要件を確認

AzureとBlueXPの両方のライセンス要件を確認する必要があります。

を参照してください [ライセンス要件を確認]。

4 **ONTAP**クラスタを準備

BlueXPでONTAPクラスタを検出し、クラスタが最小要件を満たしていることを確認し、ネットワーク設定をカスタマイズしてクラスタをAzureに接続できるようにします。

ONTAPクラスタを準備する方法をご紹介します。

5 バックアップターゲットとして**Azure Blob**を準備します

Azureバケットを作成および管理するためのコネクタの権限を設定します。また、オンプレミスのONTAPクラスタに権限を設定して、Azureバケットに対するデータの読み取りと書き込みを実行できるようにする必要があります。

必要に応じて、デフォルトのAzure暗号化キーを使用する代わりに、データ暗号化用に独自のカスタム管理キーを設定できます。 Azure環境でONTAPバックアップを受信できるようにする方法をご紹介します。

6 **ONTAP**ボリュームでバックアップをアクティブ化します

作業環境を選択し、右パネルのバックアップ/リカバリサービスの横にある*有効化>バックアップボリューム*をクリックします。次に、セットアップウィザードに従って、使用するレプリケーションポリシーとバックアップポリシー、およびバックアップするボリュームを選択します。

ONTAPボリュームでバックアップをアクティブ化します。

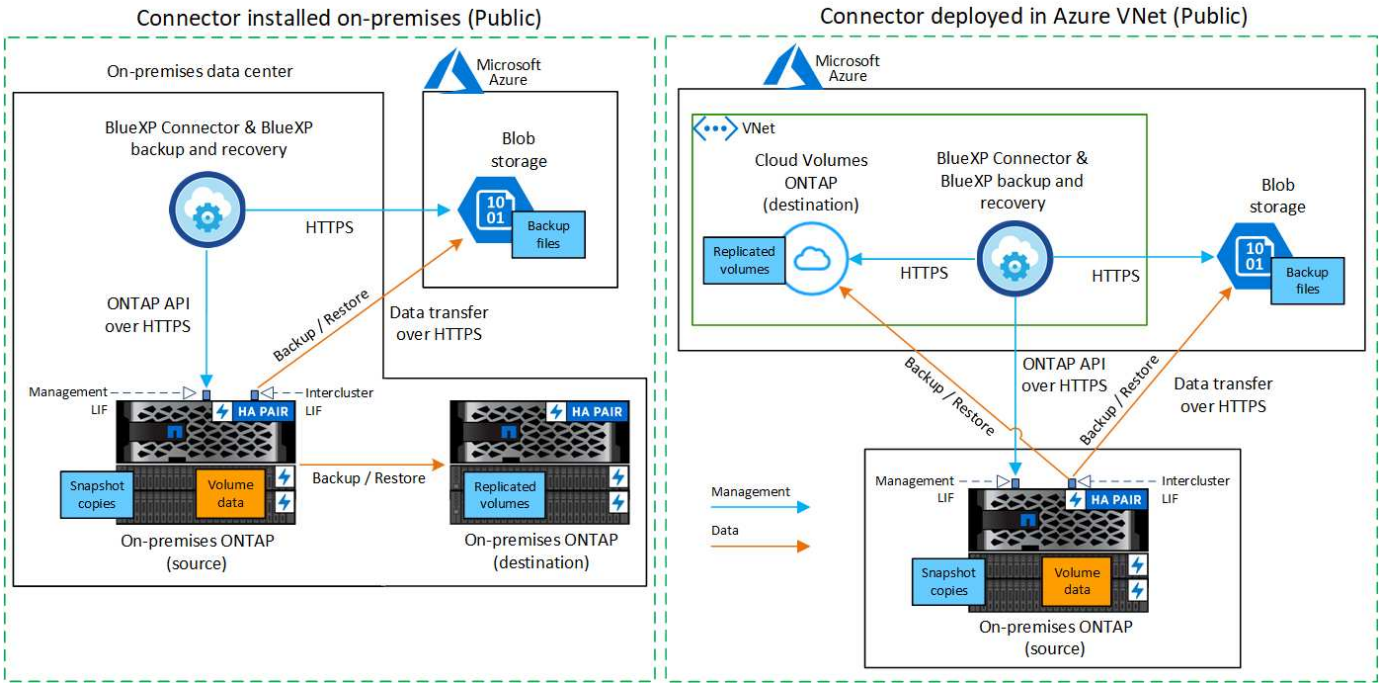
接続方法を特定します

オンプレミスのONTAPシステムからAzure Blobへのバックアップを構成する場合は、どちらの接続方法を使用するかを選択します。

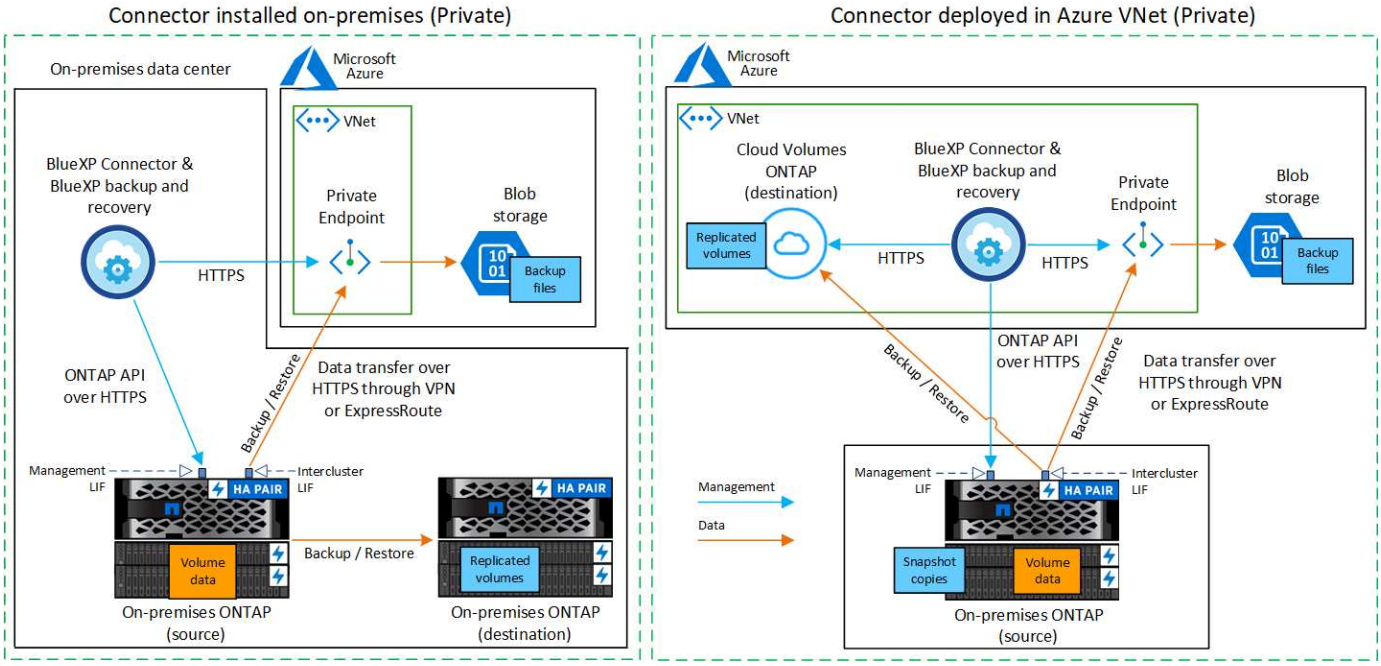
- パブリック接続-パブリックAzureエンドポイントを使用して、ONTAPシステムをAzure Blobストレージに直接接続します。
- プライベート接続- VPNまたはExpressRouteを使用し、プライベートIPアドレスを使用するVNetプライベートエンドポイントを介してトラフィックをルーティングします。

必要に応じて、パブリック接続またはプライベート接続を使用して、レプリケートされたボリュームのセカンダリONTAPシステムに接続することもできます。

次の図は、*パブリック接続*メソッドと、コンポーネント間の準備に必要な接続を示しています。オンプレミスにインストールしたコネクタやAzure VNetに導入したコネクタを使用できます。



次の図は、*プライベート接続*メソッドと、コンポーネント間の準備に必要な接続を示しています。オンプレミスにインストールしたコネクタやAzure VNetに導入したコネクタを使用できます。



BlueXPコネクタを準備します

BlueXPコネクタは'BlueXP機能の主要なソフトウェアですONTAP データのバックアップとリストアにはコネクタが必要です。

コネクタを作成または切り替えます

Azure VNetまたはオンプレミスにコネクタがすでに導入されている場合は、すべて設定されます。

そうでない場合は、いずれかの場所にコネクタを作成して、ONTAPデータをAzure BLOBストレージにバックアップする必要があります。別のクラウドプロバイダに導入されているコネクタは使用できません。

- "コネクタについて説明します"
- "Azureにコネクタをインストールします"
- "コネクタをオンプレミスにインストールします"
- "Azure Governmentリージョンにコネクタをインストールします"

  BlueXPのバックアップとリカバリは、コネクタがクラウドに導入されている場合はAzure Governmentのリージョンでサポートされ、オンプレミスにインストールされている場合はサポートされません。また、Azure MarketplaceからConnectorを導入する必要があります。BlueXP SaaS Webサイトから政府機関のリージョンにコネクタを導入することはできません。

コネクタのネットワークを準備します

コネクタに必要なネットワーク接続があることを確認します。

手順

1. コネクタが取り付けられているネットワークで次の接続が有効になっていることを確認します。
   - ポート443を介してBlueXPバックアップおよびリカバリサービスとBLOBオブジェクトストレージへのHTTPS接続 ("エンドポイントのリストを参照してください")

- ONTAP クラスタ管理 LIF へのポート 443 経由の HTTPS 接続
- BlueXPのバックアップとリカバリの検索とリストア機能を使用するには、コネクタとAzure Synapse SQLサービスの間の通信用にポート1433が開いている必要があります。
- AzureおよびAzure Government環境に追加のインバウンドセキュリティグループルールが必要です。を参照してください "Azure のコネクタのルール" を参照してください。

2. Azure ストレージへの VNet プライベートエンドポイントを有効化これは、ONTAP クラスタからVNetへのExpressRouteまたはVPN接続があり、コネクタとBLOBストレージ間の通信を仮想プライベートネットワーク（*プライベート*接続）で維持する場合に必要です。

コネクタの権限を確認または追加します

BlueXPのバックアップとリカバリの検索とリストア機能を使用するには、コネクタがAzure Synapse WorkspaceとData Lake Storageアカウントにアクセスできるように、コネクタのロールに特定の権限が必要です。以下の権限を確認し、ポリシーを変更する必要がある場合は手順に従います。

を開始する前に

Azure Synapse Analytics Resource Provider（"Microsoft.Synapse"）をサブスクリプションに登録する必要があります。 "このリソースプロバイダをサブスクリプションに登録する方法については、を参照してください"。リソースプロバイダを登録するには、Subscription * Owner または Contributor *である必要があります。

手順

1. Connector 仮想マシンに割り当てられているロールを特定します。
   a. Azure ポータルで、仮想マシンサービスを開きます。
   b. Connector 仮想マシンを選択します。
   c. で、[ID]*を選択します。
   d. [Azure role assignments]*を選択します。
   e. Connector 仮想マシンに割り当てられているカスタムロールをメモしておきます。
2. カスタムロールを更新します。
   a. Azure ポータルで、 Azure サブスクリプションを開きます。
   b. [Access control（IAM）]>[Roles]*を選択します。
   c. カスタムロールの省略記号（...）を選択し、*[編集]*を選択します。
   d. [json]*を選択し、次の権限を追加します。

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"ポリシーの完全な JSON 形式を表示します"

e. を選択し、[更新]*を選択します。

ライセンス要件を確認

AzureとBlueXPの両方のライセンス要件を確認する必要があります。

- クラスタでBlueXPのバックアップとリカバリをアクティブ化するには、Azureから従量課金制（PAYGO）のBlueXP Marketplaceサービスに登録するか、ネットアップからBlueXPバックアップとリカバリのBYOLライセンスを購入してアクティブ化する必要があります。これらのライセンスはアカウント用であり、複数のシステムで使用できます。
  - BlueXPのバックアップとリカバリのPAYGOライセンスを購入するには、のサブスクリプションが必要です "Azure Marketplaceで提供されるNetApp BlueXPサービス"。BlueXPのバックアップとリカバリの課金は、このサブスクリプションを通じて行われます。
  - BlueXPのバックアップとリカバリのBYOLライセンスの場合は、ライセンスの期間と容量にわたってサービスを使用できるネットアップのシリアル番号が必要です。 "BYOL ライセンスの管理方法について説明します"。
- バックアップを配置するオブジェクトストレージスペース用の Azure サブスクリプションが必要です。

サポートされている地域

すべての地域で、オンプレミスシステムから Azure Blob へのバックアップを作成できます "Cloud Volumes ONTAP がサポートされている場合"Azure Government リージョンを含む。サービスのセットアップ時にバックアップを保存するリージョンを指定します。

ONTAPクラスタを準備

ソースのオンプレミスONTAPシステムと、セカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムを準備する必要があります。

ONTAPクラスタの準備では、次の手順を実行します。

- BlueXPでONTAPシステムを検出しましょう
- ONTAPのシステム要件を確認
- オブジェクトストレージにデータをバックアップするためのONTAPネットワークの要件を確認します
- ボリュームをレプリケートするためのONTAPネットワークの要件を確認します

BlueXPでONTAPシステムを検出しましょう

ソースのオンプレミスONTAPシステムとセカンダリのオンプレミスONTAPシステムまたはCloud Volumes ONTAPシステムの両方が、BlueXPキャンバスで利用可能である必要があります。

クラスタを追加するには、クラスタ管理 IP アドレスと admin ユーザアカウントのパスワードが必要です。 "クラスタの検出方法について説明します"。

ONTAPのシステム要件を確認

次のONTAP要件が満たされていることを確認します。

- ONTAP 9.8以上、ONTAP 9.8P13以降が推奨されます。
- SnapMirror ライセンス（ Premium Bundle または Data Protection Bundle に含まれます）。

注： BlueXPのバックアップとリカバリを使用する場合、「Hybrid Cloud Bundle」は必要ありません。

方法をご確認ください "クラスタライセンスを管理します"。

- 時間とタイムゾーンが正しく設定されている。方法をご確認ください "クラスタ時間を設定します"。
- データをレプリケートする場合は、データをレプリケートする前に、ソースシステムとデスティネーションシステムで互換性のあるONTAPバージョンが実行されていることを確認する必要があります。

  "SnapMirror 関係に対して互換性のある ONTAP バージョンを表示します"。

オブジェクトストレージにデータをバックアップするための**ONTAP**ネットワークの要件を確認します

オブジェクトストレージに接続するシステムで、次の要件を設定する必要があります。

- ファンアウトバックアップアーキテクチャの場合は、_primary_systemで次の設定を行います。
- カスケードバックアップアーキテクチャの場合は、_secondary_systemで次の設定を行います。

次のONTAPクラスタネットワーク要件が必要です。

- ONTAP クラスタは、バックアップおよびリストア処理用に、クラスタ間 LIF から Azure Blob Storage へのポート 443 経由の HTTPS 接続を開始します。

  ONTAP は、オブジェクトストレージとの間でデータの読み取りと書き込みを行います。オブジェクトストレージが開始されることはなく、応答するだけです。

- ONTAP では、コネクタからクラスタ管理 LIF へのインバウンド接続が必要です。コネクタは Azure VNet 内に配置できます。
- クラスタ間 LIF は、バックアップ対象のボリュームをホストする各 ONTAP ノードに必要です。LIF は、ONTAP がオブジェクトストレージへの接続に使用する IPspace に関連付けられている必要があります。"IPspace の詳細については、こちらをご覧ください"。

  BlueXPのバックアップとリカバリをセットアップするときに、使用するIPspaceを指定するように求められます。各 LIF を関連付ける IPspace を選択する必要があります。これは、「デフォルト」の IPspace または作成したカスタム IPspace です。

- ノードとクラスタ間 LIF からオブジェクトストアにアクセスできます。
- ボリュームが配置されている Storage VM に DNS サーバが設定されている。方法を参照してください "SVM 用に DNS サービスを設定"。
- を使用しているIPspaceがデフォルトと異なる場合は、オブジェクトストレージにアクセスするための静的ルートの作成が必要になることがあります。
- 必要に応じてファイアウォールルールを更新して、ONTAP からオブジェクトストレージへのBlueXPバックアップ/リカバリサービス接続（ポート443経由）、およびStorage VMからDNSサーバへのポート53（TCP / UDP）経由の名前解決トラフィックを許可します。

ボリュームをレプリケートするための**ONTAP**ネットワークの要件を確認します

BlueXPのバックアップとリカバリを使用してセカンダリONTAPシステムにレプリケートされたボリュームを作成する場合は、ソースシステムとデスティネーションシステムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワークの要件

- クラスタが社内にある場合は、社内ネットワークからクラウドプロバイダ内の仮想ネットワークへの接続が必要です。これは通常、 VPN 接続です。
- ONTAP クラスタは、サブネット、ポート、ファイアウォール、およびクラスタの追加要件を満たしている必要があります。

  Cloud Volumes ONTAPまたはオンプレミスのシステムにレプリケートできるため、オンプレミスのONTAPシステムのピアリング要件を確認してください。 "クラスタピアリングの前提条件については、ONTAP のドキュメントを参照してください"。

Cloud Volumes ONTAPネットワークの要件

- インスタンスのセキュリティグループに、必要なインバウンドおよびアウトバウンドのルールが含まれている必要があります。具体的には、 ICMP とポート 11104 および 11105 のルールが必要です。これらのルールは、事前定義されたセキュリティグループに含まれています。

バックアップターゲットとして**Azure Blob**を準備します

1. Microsoftが管理するデフォルトの暗号化キーを使用する代わりに、アクティベーションウィザードで独自のカスタム管理キーを使用して、データ暗号化を行うことができます。この場合、 Azure サブスクリプション、キー・ボールト名、およびキーが必要です。 "独自のキーの使用方法について説明します"。

   Backup and Recoveryでは、権限モデルとして_AZUREアクセスポリシー_がサポートされていることに注意してください。現時点では、*Azure Role-Based Access Control*（Azure RBAC）権限モデルはサポートされていません。

2. オンプレミスのデータセンターから VNet へのパブリックインターネット経由での接続をより安全にするには、アクティブ化ウィザードで Azure Private Endpoint を設定するオプションがあります。この場合、この接続用の VNet とサブネットについて理解しておく必要があります。 "プライベートエンドポイントの使用方法の詳細については、を参照してください"。

Azure BLOBストレージアカウントを作成します

デフォルトでは、サービスによってストレージアカウントが作成されます。独自のストレージアカウントを使用する場合は、バックアップアクティブ化ウィザードを開始する前にストレージアカウントを作成し、ウィザードでそれらのストレージアカウントを選択できます。

"独自のストレージアカウントの作成について詳しくは、こちらをご覧ください"。

ONTAPボリュームでバックアップをアクティブ化します

オンプレミスの作業環境からいつでも直接バックアップをアクティブ化できます。

ウィザードでは、次の主な手順を実行します。

- [バックアップするボリュームを選択します]
- [バックアップ戦略を定義します]
- [選択内容を確認します]

また可能です APIコマンドを表示します レビューステップでは、コードをコピーして、将来の作業環境のバ

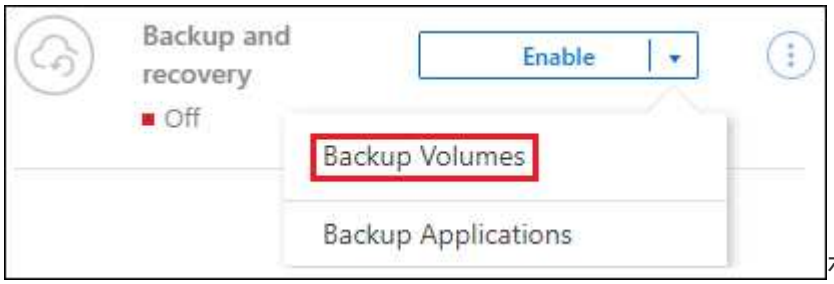
ックアップアクティベーションを自動化できます。

ウィザードを開始します

手順

1. 次のいずれかの方法でバックアップとリカバリのアクティブ化ウィザードにアクセスします。

   - BlueXPキャンバスで、作業環境を選択し、右パネルのバックアップとリカバリサービスの横にある*[有効化]>[ボリュームのバックアップ]*を選択します。



ボタンのスクリーンショット。"]

     バックアップのAzureデスティネーションがCanvasの作業環境として存在する場合は、ONTAPクラスタをAzure Blobオブジェクトストレージにドラッグできます。

   - [バックアップとリカバリ]バーで*を選択します。**[ボリューム]**タブで、[操作]* ••• アイコンをクリックし、（オブジェクトストレージへのレプリケーションまたはバックアップがまだ有効になっていない）単一のボリュームに対して*[バックアップのアクティブ化]*を選択します。

   ウィザードの[Introduction]ページには、ローカルSnapshot、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で2番目のオプションを選択した場合は、1つのボリュームが選択された状態で[Define Backup Strategy]ページが表示されます。

2. 次のオプションに進みます。

   - BlueXPコネクタをすでにお持ちの場合は、これで準備は完了です。[次へ]*を選択します。
   - BlueXPコネクタをまだお持ちでない場合は、*[Add a Connector]*オプションが表示されます。を参照してください BlueXPコネクタを準備します。

バックアップするボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、Snapshotポリシー、レプリケーションポリシー、オブジェクトへのバックアップポリシーのうち1つ以上を含むボリュームです。

FlexVolボリュームとFlexGroupボリュームのどちらを保護するかを選択できますが、作業環境でバックアップをアクティブ化するときは、これらのボリュームを組み合わせて選択することはできません。方法を参照してください "作業環境内の追加ボリュームのバックアップをアクティブ化" （FlexVolまたはFlexGroup）初期ボリュームのバックアップの設定が完了したら、

- バックアップをアクティブ化できるのは、一度に1つのFlexGroupボリュームだけです。
- 選択するボリュームのSnapLock設定は同じである必要があります。すべてのボリュームでSnapLock Enterpriseが有効になっているかSnapLockが無効になっている必要があります。（SnapLock Complianceモードのボリュームは現在サポートされていません。ONTAP 9.14以降が必要です。）

手順

選択したボリュームにSnapshotポリシーまたはレプリケーションポリシーがすでに適用されている場合は、あとで選択したポリシーで既存のポリシーが上書きされます。

1. [Select Volumes]ページで、保護するボリュームを選択します。
   - 必要に応じて、行をフィルタして、特定のボリュームタイプや形式などのボリュームのみを表示し、選択を容易にします。
   - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます（FlexGroupボリュームは一度に1つだけ選択できます）。既存のFlexVolボリュームをすべてバックアップするには、最初に1つのボリュームをオンにしてから、タイトル行のボックスをオンにします。（☑ Volume Name）。
   - 個々のボリュームをバックアップするには、各ボリュームのボックス（☑ Volume_1）。
2. 「 * 次へ * 」を選択します。

バックアップ戦略を定義します

バックアップ戦略を定義するには、次のオプションを設定します。

- 1つまたはすべてのバックアップオプション（ローカルSnapshot、レプリケーション、オブジェクトストレージへのバックアップ）が必要かどうか
- アーキテクチャ
- ローカルSnapshotポリシー
- レプリケーションのターゲットとポリシー

> ⓘ 選択したボリュームのSnapshotポリシーとレプリケーションポリシーがこの手順で選択したポリシーと異なる場合は、既存のポリシーが上書きされます。

- オブジェクトストレージ情報（プロバイダ、暗号化、ネットワーク、バックアップポリシー、エクスポートオプション）へのバックアップ。

手順

1. [Define backup strategy]ページで、次のいずれかまたはすべてを選択します。デフォルトでは、3つすべてが選択されています。
   - *ローカルSnapshot *：レプリケーションまたはオブジェクトストレージへのバックアップを実行する場合は、ローカルSnapshotを作成する必要があります。
   - レプリケーション：別のONTAPストレージシステムにレプリケートされたボリュームを作成します。
   - バックアップ：ボリュームをオブジェクトストレージにバックアップします。
2. アーキテクチャ:レプリケーションとバックアップを選択した場合は'次のいずれかの情報フローを選択します
   - カスケード：情報はプライマリからセカンダリへ、およびセカンダリからオブジェクトストレージへと流れます。
   - ファンアウト：プライマリからセカンダリへ、プライマリからオブジェクトストレージへ、情報が流れます。

     これらのアーキテクチャの詳細については、を参照してください "保護対策を計画しましょう"。

3. *ローカルSnapshot *：既存のSnapshotポリシーを選択するか、新しいSnapshotポリシーを作成します。

> Snapshotをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

- ポリシーの名前を入力します。
- 最大5つのスケジュール（通常は異なる周波数）を選択します。
- 「 * Create * 」を選択します。

4. レプリケーション：次のオプションを設定します。
   - レプリケーションターゲット：デスティネーションの作業環境とSVMを選択します。必要に応じて、レプリケートするボリュームの名前に追加するデスティネーションアグリゲートとプレフィックスまたはサフィックスを選択します。
   - レプリケーションポリシー：既存のレプリケーションポリシーを選択するか、新しいレプリケーションポリシーを作成します。

     > レプリケーションをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

     ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

     - ポリシーの名前を入力します。
     - 最大5つのスケジュール（通常は異なる周波数）を選択します。
     - 「 * Create * 」を選択します。

5. オブジェクトにバックアップ：*バックアップ*を選択した場合は、次のオプションを設定します。
   - プロバイダ：[Microsoft Azure]*を選択します。
   - プロバイダ設定：バックアップを保存するプロバイダの詳細と地域を入力します。

     新しいストレージアカウントを作成するか、既存のストレージアカウントを選択します。

     Blobコンテナを管理する独自のリソースグループを作成するか、リソースグループのタイプとグループを選択します。

     > バックアップファイルが変更または削除されないように保護する場合は、ストレージアカウントが変更不可のストレージで作成され、30日間の保持期間を使用していることを確認してください。

     > コストをさらに最適化するために古いバックアップファイルをAzure Archive Storageに階層化する場合は、ストレージアカウントに適切なライフサイクルルールが設定されていることを確認してください。

   - 暗号化キー：新しいAzureストレージアカウントを作成した場合は、プロバイダから提供された暗号化キー情報を入力します。データの暗号化を管理するために、デフォルトのAzure暗号化キーを使用するか、Azureアカウントからお客様が管理する独自のキーを選択するかを選択します。

独自の顧客管理キーを使用する場合は、キーボールトとキー情報を入力します。

> 既存のMicrosoftストレージアカウントを選択した場合、暗号化情報はすでに使用可能なため、ここで入力する必要はありません。

- ネットワーク：IPspace、およびプライベートエンドポイントを使用するかどうかを選択します。プライベートエンドポイントはデフォルトで無効になっています。
  i. バックアップするボリュームが配置されている ONTAP クラスタ内の IPspace 。この IPspace のクラスタ間 LIF 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。
  ii. 必要に応じて、以前に設定したAzureプライベートエンドポイントを使用するかどうかを選択します。 "Azureプライベートエンドポイントの使用について説明します"。
- バックアップポリシー：既存のオブジェクトストレージへのバックアップポリシーを選択するか、新しいポリシーを作成します。

> バックアップをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

  - ポリシーの名前を入力します。
  - 最大5つのスケジュール（通常は異なる周波数）を選択します。
  - オブジェクトへのバックアップポリシーの場合は、DataLockとRansomware Protectionを設定します。DataLockとランサムウェア対策の詳細については、 "オブジェクトへのバックアップポリシーの設定"。
  - 「 * Create * 」を選択します。
- 既存の**Snapshot**コピーをバックアップコピーとしてオブジェクトストレージにエクスポート：この作業環境に、この作業環境に対して選択したバックアップスケジュールラベル（daily、weeklyなど）と一致するボリュームのローカルSnapshotコピーがある場合は、この追加のプロンプトが表示されます。ボリュームを最大限に保護するために、履歴Snapshotをすべてオブジェクトストレージにバックアップファイルとしてコピーする場合は、このチェックボックスをオンにします。

6. 「 * 次へ * 」を選択します。

選択内容を確認します

これにより、選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. [Review]ページで、選択内容を確認します。
2. 必要に応じて、Snapshotポリシーのラベルをレプリケーションポリシーおよびバックアップポリシーのラベルと自動的に同期する*チェックボックスをオンにします。これにより、レプリケーションポリシーとバックアップポリシーのラベルに一致するラベルを持つSnapshotが作成されます。
3. [バックアップのアクティブ化]*を選択します。

結果

BlueXPのバックアップとリカバリで、ボリュームの初期バックアップが作成されます。レプリケートされたボリュームとバックアップファイルのベースライン転送には、プライマリストレージシステムのデータのフル

コピーが含まれます。以降の転送には、Snapshotコピーに含まれるプライマリストレージシステムデータの差分コピーが含まれます。

レプリケートされたボリュームが、プライマリボリュームと同期されるデスティネーションクラスタに作成されます。

入力したリソースグループにBLOBストレージアカウントが作成され、バックアップファイルがそこに格納されます。ボリュームバックアップダッシュボードが表示され、バックアップの状態を監視できます。

を使用して、バックアップジョブとリストアジョブのステータスを監視することもできます "［ジョブ監視］パネル"。

APIコマンドを表示します

バックアップとリカバリのアクティブ化ウィザードで使用するAPIコマンドを表示し、必要に応じてコピーすることができます。これは、将来の作業環境でバックアップを自動的にアクティブ化する場合に必要になることがあります。

手順

1. バックアップとリカバリのアクティブ化ウィザードで、*[API要求の表示]*を選択します。
2. コマンドをクリップボードにコピーするには、*コピー*アイコンを選択します。

次の手順

- 可能です "バックアップファイルとバックアップポリシーを管理"。バックアップの開始と停止、バックアップの削除、バックアップスケジュールの追加と変更などが含まれます。
- 可能です "クラスタレベルのバックアップの設定を管理します"。これには、バックアップをオブジェクトストレージにアップロードするためのネットワーク帯域幅の変更、将来のボリュームに対する自動バックアップ設定の変更などが含まれます。
- また可能です "ボリューム、フォルダ、または個々のファイルをバックアップファイルからリストアする" Azure 内の Cloud Volumes ONTAP システムやオンプレミスの ONTAP システムへの接続に使用できます。

オンプレミスの**ONTAP**データを**Google Cloud Storage**にバックアップ

オンプレミスのプライマリONTAPシステムからセカンダリストレージシステムおよびGoogle Cloud Storageへのボリュームデータのバックアップを開始するには、いくつかの手順を実行します。

「オンプレミスのONTAPシステム」には、FAS、AFF、ONTAP Selectシステムが含まれます。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。各手順の詳細については、このトピックの以降のセクションを参照してください。

1 使用する接続方法を特定します

オンプレミスのONTAPクラスタをパブリックインターネット経由でGoogle Cloud Storageに直接接続するか、VPNまたはGoogle Cloud Interconnectを使用してプライベートIPアドレスを使用するプライベートGoogle Accessインターフェイスを介してトラフィックをルーティングするかを選択します。

[接続方法を特定します]。

2 **BlueXP**コネクタを準備します

Google Cloud Platform VPCにコネクタがすでに導入されている場合は、すべて設定されます。そうでない場合は、ONTAPデータをGoogle Cloudストレージにバックアップするための**BlueXP**コネクタを作成する必要があります。また、コネクタがGoogle Cloudに接続できるように、コネクタのネットワーク設定をカスタマイズする必要があります。

コネクタの作成方法と、必要なネットワーク設定の定義方法について説明します。

3 ライセンス要件を確認

Google CloudとBlueXPの両方のライセンス要件を確認する必要があります。

を参照してください [ライセンス要件を確認]。

4 **ONTAP**クラスタを準備

BlueXPでONTAPクラスタを検出し、クラスタが最小要件を満たしていることを確認し、ネットワーク設定をカスタマイズしてクラスタをGoogle Cloudに接続できるようにします。

ONTAPクラスタを準備する方法をご紹介します。

5 バックアップターゲットとして**Google Cloud**を準備します

Google Cloudバケットを作成および管理するためのコネクタの権限を設定します。また、オンプレミスのONTAPクラスタでGoogle Cloudバケットに対するデータの読み取りと書き込みができるように、権限を設定する必要があります。

必要に応じて、Google Cloudのデフォルトの暗号化キーを使用する代わりに、データ暗号化用に独自のカスタム管理キーを設定できます。 Google Cloud環境でONTAPバックアップを受信できるようにする方法をご紹介します。

6 **ONTAP**ボリュームでバックアップをアクティブ化します

作業環境を選択し、右パネルのバックアップ/リカバリサービスの横にある*有効化>バックアップボリューム*をクリックします。次に、セットアップウィザードに従って、使用するレプリケーションポリシーとバックアップポリシー、およびバックアップするボリュームを選択します。

ONTAPボリュームでバックアップをアクティブ化します。

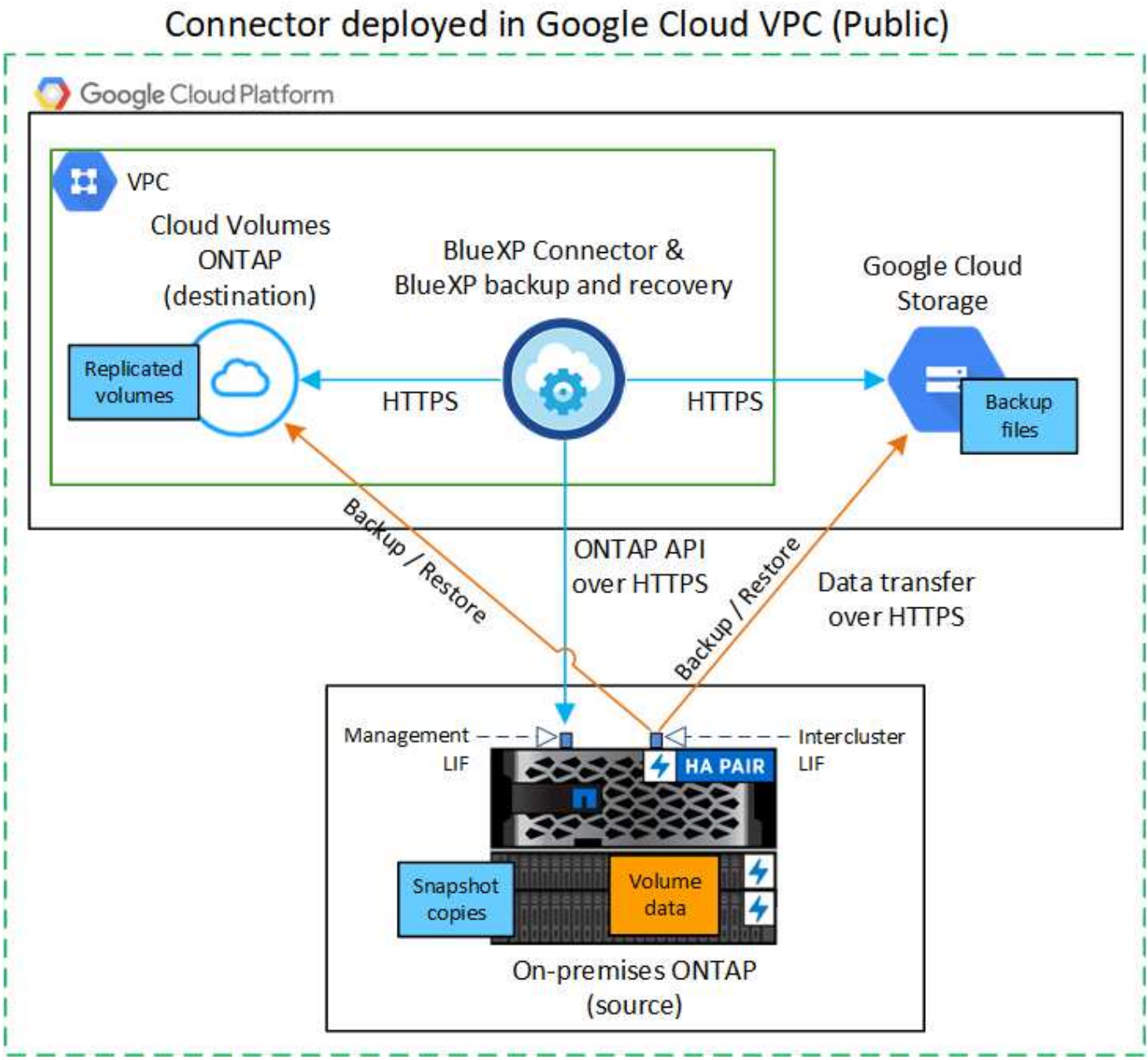
接続方法を特定します

オンプレミスのONTAPシステムからGoogle Cloud Storageへのバックアップを構成する場合は、どちらの接続方法を使用するかを選択します。

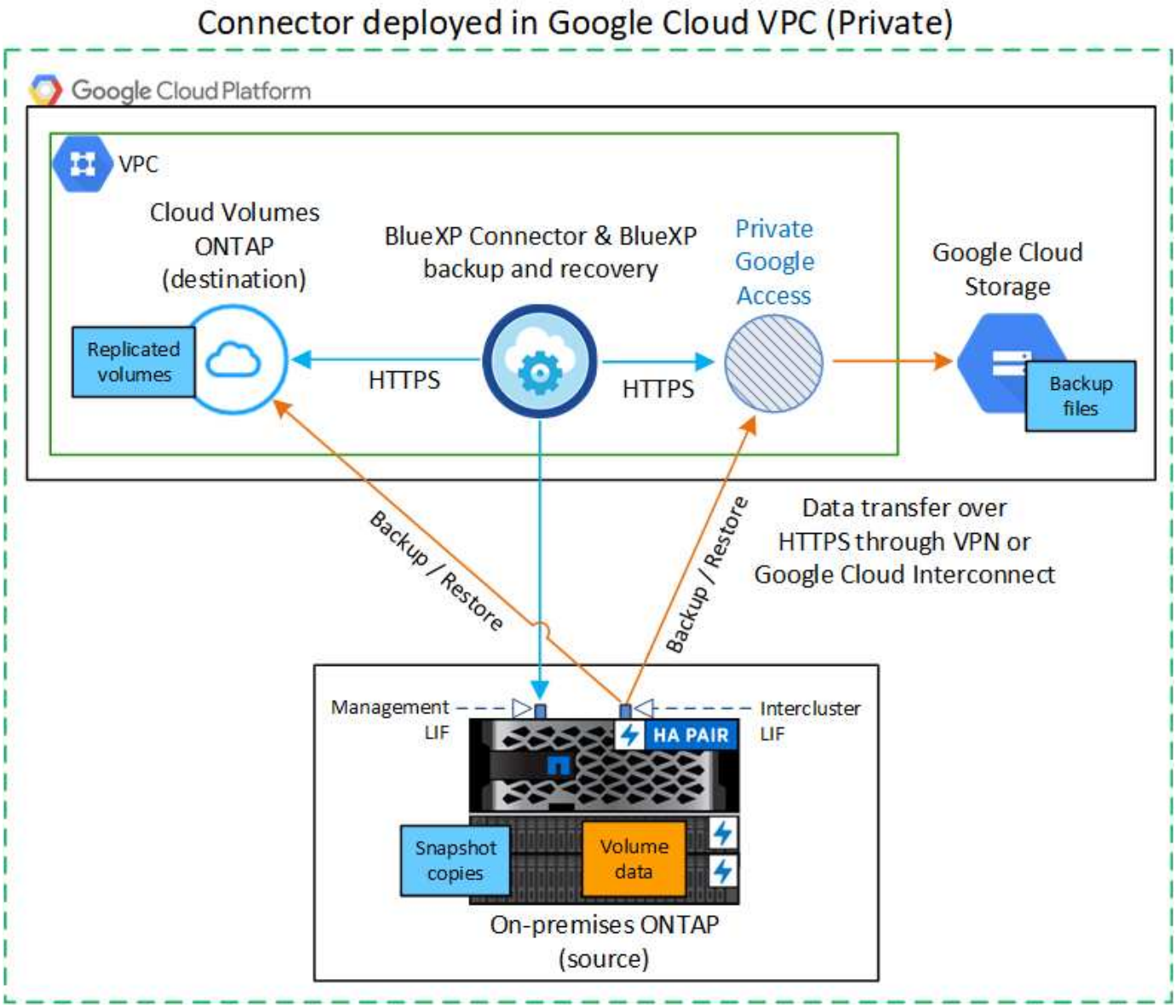
- パブリック接続-パブリックGoogleエンドポイントを使用して、ONTAPシステムをGoogle Cloud Storageに直接接続します。
- プライベート接続- VPNまたはGoogle Cloud Interconnectを使用し、プライベートIPアドレスを使用するプライベートGoogle Accessインターフェイスを介してトラフィックをルーティングします。

必要に応じて、パブリック接続またはプライベート接続を使用して、レプリケートされたボリュームのセカンダリONTAPシステムに接続することもできます。

次の図は、*パブリック接続*メソッドと、コンポーネント間の準備に必要な接続を示しています。コネクターはGoogle Cloud Platform VPCに展開する必要があります。



次の図は、*プライベート接続*メソッドと、コンポーネント間の準備に必要な接続を示しています。コネクターはGoogle Cloud Platform VPCに展開する必要があります。



BlueXPコネクタを準備します

BlueXPコネクタは'BlueXP機能の主要なソフトウェアですONTAP データのバックアップとリストアにはコネクタが必要です。

コネクタを作成または切り替えます

Google Cloud Platform VPCにコネクタがすでに導入されている場合は、すべて設定されます。

そうでない場合は、ONTAPデータをGoogle Cloud Storageにバックアップするためのコネクタをその場所に作成する必要があります。別のクラウドプロバイダやオンプレミスに導入されているコネクタは使用できません。

- "コネクタについて説明します"

- "GCPにコネクタを取り付けます"

コネクタのネットワークを準備します

コネクタに必要なネットワーク接続があることを確認します。

手順

1. コネクタが取り付けられているネットワークで次の接続が有効になっていることを確認します。
   - ポート443を介してBlueXPバックアップおよびリカバリサービスとGoogle Cloudストレージへのの HTTPS接続 ("エンドポイントのリストを参照してください")
   - ONTAP クラスタ管理 LIF へのポート 443 経由の HTTPS 接続
2. Connectorを展開するサブネットでプライベートGoogleアクセス（またはプライベートサービス接続）を有効にします。 "プライベート Google アクセス" または "Private Service Connectの略" ONTAP クラスタからVPCへの直接接続が確立されていて、ConnectorとGoogle Cloud Storage間の通信を仮想プライベートネットワーク（*プライベート*接続）のままにする場合に必要です。

   Googleの指示に従って、プライベートアクセスオプションを設定します。DNSサーバが参照するように設定されていることを確認します `www.googleapis.com` および `storage.googleapis.com` を正しい内部（プライベート）IPアドレスに割り当てます。

コネクタの権限を確認または追加します

BlueXPのバックアップとリカバリの「Search & Restore」機能を使用するには、コネクタがGoogle Cloud BigQueryサービスにアクセスできるように、コネクタのロールに特定の権限が必要です。以下の権限を確認し、ポリシーを変更する必要がある場合は手順に従います。

手順

1. を参照してください "Google Cloud Console の略"をクリックし、 * Roles * ページに移動します。
2. ページ上部のドロップダウンリストを使用して、編集するロールを含むプロジェクトまたは組織を選択します。
3. カスタムロールを選択します。
4. ロールの権限を更新するには、*[ロールの編集]*を選択します。
5. [権限の追加]*を選択して、次の新しい権限をロールに追加します。

```
bigquery.jobs.get
bigquery.jobs.list
bigquery.jobs.listAll
bigquery.datasets.create
bigquery.datasets.get
bigquery.jobs.create
bigquery.tables.get
bigquery.tables.getData
bigquery.tables.list
bigquery.tables.create
```

6. 編集したロールを保存するには、*[更新]*を選択します。

ライセンス要件を確認

- クラスタでBlueXPのバックアップとリカバリをアクティブ化するには、Googleから従量課金制（PAYGO）のBlueXP Marketplaceサービスに登録するか、ネットアップからBlueXPバックアップとリカバリのBYOLライセンスを購入してアクティブ化する必要があります。これらのライセンスはアカウント用であり、複数のシステムで使用できます。
  - BlueXPのバックアップとリカバリのPAYGOライセンスを購入するには、のサブスクリプションが必要です "Google Marketplaceで提供されているNetApp BlueXPサービス"。BlueXPのバックアップとリカバリの課金は、このサブスクリプションを通じて行われます。
  - BlueXPのバックアップとリカバリのBYOLライセンスの場合は、ライセンスの期間と容量にわたってサービスを使用できるネットアップのシリアル番号が必要です。 "BYOL ライセンスの管理方法について説明します"。
- バックアップを格納するオブジェクトストレージスペース用の Google サブスクリプションが必要です。

サポートされている地域

すべての地域で、オンプレミスシステムからGoogle Cloud Storageへのバックアップを作成できます "Cloud Volumes ONTAP がサポートされている場合"。サービスのセットアップ時にバックアップを保存するリージョンを指定します。

ONTAPクラスタを準備

ソースのオンプレミスONTAPシステムと、セカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムを準備する必要があります。

ONTAPクラスタの準備では、次の手順を実行します。

- BlueXPでONTAPシステムを検出しましょう
- ONTAPのシステム要件を確認
- オブジェクトストレージにデータをバックアップするためのONTAPネットワークの要件を確認します
- ボリュームをレプリケートするためのONTAPネットワークの要件を確認します

BlueXPでONTAPシステムを検出しましょう

ソースのオンプレミスONTAPシステムとセカンダリのオンプレミスONTAPシステムまたはCloud Volumes ONTAPシステムの両方が、BlueXPキャンバスで利用可能である必要があります。

クラスタを追加するには、クラスタ管理 IP アドレスと admin ユーザアカウントのパスワードが必要です。 "クラスタの検出方法について説明します"。

ONTAPのシステム要件を確認

次のONTAP要件が満たされていることを確認します。

- ONTAP 9.8以上、ONTAP 9.8P13以降が推奨されます。
- SnapMirror ライセンス（ Premium Bundle または Data Protection Bundle に含まれます）。

注： BlueXPのバックアップとリカバリを使用する場合、「Hybrid Cloud Bundle」は必要ありません。

方法をご確認ください "クラスタライセンスを管理します"。

- 時間とタイムゾーンが正しく設定されている。方法をご確認ください "クラスタ時間を設定します"。
- データをレプリケートする場合は、データをレプリケートする前に、ソースシステムとデスティネーションシステムで互換性のあるONTAPバージョンが実行されていることを確認する必要があります。

  "SnapMirror 関係に対して互換性のある ONTAP バージョンを表示します"。

オブジェクトストレージにデータをバックアップするための**ONTAP**ネットワークの要件を確認します

オブジェクトストレージに接続するシステムで、次の要件を設定する必要があります。

- ファンアウトバックアップアーキテクチャの場合は、_primary_systemで次の設定を行います。
- カスケードバックアップアーキテクチャの場合は、_secondary_systemで次の設定を行います。

次のONTAPクラスタネットワーク要件が必要です。

- ONTAPクラスタは、バックアップおよびリストア処理のために、インタークラスタLIFからGoogle Cloud Storageへのポート443経由でHTTPS接続を開始します。

  ONTAP は、オブジェクトストレージとの間でデータの読み取りと書き込みを行います。オブジェクトストレージが開始されることはなく、応答するだけです。

- ONTAP では、コネクタからクラスタ管理 LIF へのインバウンド接続が必要です。このコネクタは、Google Cloud Platform VPC 内に配置できます。
- クラスタ間 LIF は、バックアップ対象のボリュームをホストする各 ONTAP ノードに必要です。LIF は、ONTAP がオブジェクトストレージへの接続に使用する IPspace に関連付けられている必要があります。"IPspace の詳細については、こちらをご覧ください"。

  BlueXPのバックアップとリカバリをセットアップするときに、使用するIPspaceを指定するように求められます。各 LIF を関連付ける IPspace を選択する必要があります。これは、「デフォルト」の IPspace または作成したカスタム IPspace です。

- ノードのクラスタ間 LIF からオブジェクトストアにアクセスできます。
- ボリュームが配置されている Storage VM に DNS サーバが設定されている。方法を参照してください "SVM 用に DNS サービスを設定"。

  Private Google AccessまたはPrivate Service Connectを使用している場合は、DNSサーバーがポイントするように設定されていることを確認します `storage.googleapis.com` を正しい内部（プライベート）IPアドレスに割り当てます。

- をデフォルトとは異なる IPspace を使用している場合は、オブジェクトストレージへのアクセスを取得するために静的ルートの作成が必要になることがあります。
- 必要に応じてファイアウォールルールを更新して、ONTAP からオブジェクトストレージへのBlueXPのバックアップ/リカバリ接続（ポート443を経由）と、Storage VMからDNSサーバへのポート53（TCP / UDP）経由の名前解決トラフィックを許可します。

ボリュームをレプリケートするための**ONTAP**ネットワークの要件を確認します

BlueXPのバックアップとリカバリを使用してセカンダリONTAPシステムにレプリケートされたボリュームを作成する場合は、ソースシステムとデスティネーションシステムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワークの要件

- クラスタが社内にある場合は、社内ネットワークからクラウドプロバイダ内の仮想ネットワークへの接続が必要です。これは通常、 VPN 接続です。
- ONTAP クラスタは、サブネット、ポート、ファイアウォール、およびクラスタの追加要件を満たしている必要があります。

  Cloud Volumes ONTAPまたはオンプレミスのシステムにレプリケートできるため、オンプレミスのONTAPシステムのピアリング要件を確認してください。 "クラスタピアリングの前提条件については、ONTAP のドキュメントを参照してください"。

Cloud Volumes ONTAPネットワークの要件

- インスタンスのセキュリティグループに、必要なインバウンドおよびアウトバウンドのルールが含まれている必要があります。具体的には、 ICMP とポート 11104 および 11105 のルールが必要です。これらのルールは、事前定義されたセキュリティグループに含まれています。

バックアップターゲットとして**Google Cloud Storage**を準備します

バックアップターゲットとしてGoogle Cloud Storageを準備するには、次の手順を実行します。

- 権限を設定します。
- （オプション）独自のバケットを作成します。（必要に応じて、サービスによってバケットが作成されます）。
- （オプション）データ暗号化用の顧客管理キーを設定します

権限を設定します

バックアップを設定するときは、特定の権限を持つサービスアカウントのストレージアクセスキーを指定する必要があります。サービスアカウントを使用すると、BlueXPのバックアップとリカバリで、バックアップの格納に使用されるCloud Storageバケットを認証してアクセスできます。キーは、 Google Cloud Storage がリクエストを発行しているユーザーを認識できるようにするために必要です。

手順

1. を参照してください "Google Cloud Console の略"をクリックし、 * Roles * ページに移動します。
2. "新しいロールを作成します" 次の権限が必要です。

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. Google Cloud コンソールで、 "[サービスアカウント ページに移動します"^]。
4. クラウドプロジェクトを選択します。
5. [サービスアカウントの作成]*を選択し、必要な情報を入力します。
   a. * サービスアカウントの詳細 * ：名前と説明を入力します。
   b. このサービスアカウントにプロジェクトへのアクセス権を付与:作成したカスタムロールを選択します。
   c. 「 Done （完了）」を選択します。
6. に進みます "GCP Storage Settings （ GCP ストレージ設定）" サービスアカウントのアクセスキーを作成します。
   a. プロジェクトを選択し、* Interoperability *を選択します。まだ行っていない場合は、*相互運用性アクセスを有効にする*を選択します。
   b. で、[サービスアカウントのキーを作成する]を選択し、作成したサービスアカウントを選択して[キーの作成]*をクリックします。

      あとでバックアップサービスを設定するときに、BlueXPのバックアップとリカバリでキーを入力する必要があります。

独自のバケットを作成します

デフォルトでは、サービスによってバケットが作成されます。独自のバケットを使用する場合は、バックアップアクティブ化ウィザードを開始する前にバケットを作成し、ウィザードでバケットを選択できます。

"独自のバケットの作成の詳細については、こちらをご覧ください"。

データ暗号化用の顧客管理暗号化キー（**CMEK**）を設定します

Googleが管理するデフォルトの暗号化キーを使用する代わりに、お客様が管理する独自のキーを使用してデータを暗号化できます。クロスリージョンキーとクロスプロジェクトキーの両方がサポートされているため、CMEKキーのプロジェクトとは異なるバケット用のプロジェクトを選択できます。

お客様が管理する独自のキーを使用する場合は、次の手順を実行します。

- アクティベーションウィザードでこの情報を追加できるように、キーリングとキー名が必要です。 "お客様が管理する暗号化キーの詳細については、こちらをご覧ください"。
- これらの必要な権限がコネクタの役割に含まれていることを確認する必要があります。

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- プロジェクトでGoogleの「Cloud Key Management Service（KMS）」APIが有効になっていることを確認する必要があります。を参照してください "Google Cloudドキュメント：APIの有効化" を参照してください。
- CMEKの考慮事項：*
- HSM（ハードウェアバックアップ）キーとソフトウェア生成キーの両方がサポートされています。
- 新しく作成またはインポートしたCloud KMSキーは両方サポートされます。
- リージョンキーのみがサポートされています。グローバルキーはサポートされていません。
- 現在、「対称暗号化/復号化」の目的のみがサポートされています。
- BlueXPのバックアップとリカバリによって、ストレージアカウントに関連付けられたサービスエージェントには、「CryptoKey encrypter/Decrypter（roles/cloudkms.cryptoKeyEncrypterDecrypter）」IAMロールが割り当てられます。

ONTAPボリュームでバックアップをアクティブ化します

オンプレミスの作業環境からいつでも直接バックアップをアクティブ化できます。

ウィザードでは、次の主な手順を実行します。

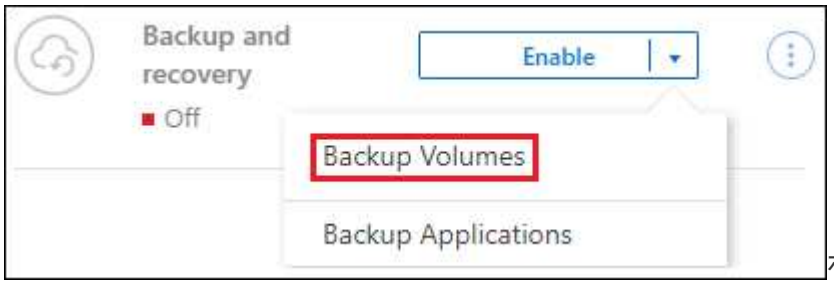
- [バックアップするボリュームを選択します]
- [バックアップ戦略を定義します]
- [選択内容を確認します]

また可能です APIコマンドを表示します レビューステップでは、コードをコピーして、将来の作業環境のバックアップアクティベーションを自動化できます。

ウィザードを開始します

手順

1. 次のいずれかの方法でバックアップとリカバリのアクティブ化ウィザードにアクセスします。
    - BlueXPキャンバスで、作業環境を選択し、右パネルのバックアップとリカバリサービスの横にある*[有効化]>[ボリュームのバックアップ]*を選択します。



ボタンのスクリーンショット。"]

バックアップ先のGoogle Cloud Storageがキャンバスの作業環境として存在する場合は、ONTAPクラスタをGoogle Cloudオブジェクトストレージにドラッグできます。

- [バックアップとリカバリ]バーで*を選択します。**[ボリューム]**タブで、[操作]* ••• アイコンをクリックし、（オブジェクトストレージへのレプリケーションまたはバックアップがまだ有効になっていない）単一のボリュームに対して*[バックアップのアクティブ化]*を選択します。。

ウィザードの[Introduction]ページには、ローカルSnapshot、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で2番目のオプションを選択した場合は、1つのボリュームが選択された状態で[Define Backup Strategy]ページが表示されます。

2. 次のオプションに進みます。
   - BlueXPコネクタをすでにお持ちの場合は、これで準備は完了です。[次へ]*を選択します。
   - BlueXPコネクタをまだお持ちでない場合は、*[Add a Connector]*オプションが表示されます。を参照してください BlueXPコネクタを準備します。

バックアップするボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、Snapshotポリシー、レプリケーションポリシー、オブジェクトへのバックアップポリシーのうち1つ以上を含むボリュームです。

FlexVolボリュームとFlexGroupボリュームのどちらを保護するかを選択できますが、作業環境でバックアップをアクティブ化するときは、これらのボリュームを組み合わせて選択することはできません。方法を参照してください "作業環境内の追加ボリュームのバックアップをアクティブ化" （FlexVolまたはFlexGroup）初期ボリュームのバックアップの設定が完了したら、

- バックアップをアクティブ化できるのは、一度に1つのFlexGroupボリュームだけです。
- 選択するボリュームのSnapLock設定は同じである必要があります。すべてのボリュームでSnapLock Enterpriseが有効になっているかSnapLockが無効になっている必要があります。（SnapLock Complianceモードのボリュームには、ONTAP 9.14以降が必要です）。

手順

選択したボリュームにSnapshotポリシーまたはレプリケーションポリシーがすでに適用されている場合は、あとで選択したポリシーで既存のポリシーが上書きされます。

1. [Select Volumes]ページで、保護するボリュームを選択します。
   - 必要に応じて、行をフィルタして、特定のボリュームタイプや形式などのボリュームのみを表示し、選択を容易にします。
   - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます（FlexGroupボリュームは一度に1つだけ選択できます）。既存のFlexVolボリュームをすべてバックアップするには、最初に1

つのボリュームをオンにしてから、タイトル行のボックスをオンにします。（☑ Volume Name）。

- 個々のボリュームをバックアップするには、各ボリュームのボックス（☑ Volume_1）。

2. 「* 次へ * 」を選択します。

バックアップ戦略を定義します

バックアップ戦略を定義するには、次のオプションを設定します。

- 1つまたはすべてのバックアップオプション（ローカルSnapshot、レプリケーション、オブジェクトストレージへのバックアップ）が必要かどうか
- アーキテクチャ
- ローカルSnapshotポリシー
- レプリケーションのターゲットとポリシー

> 選択したボリュームのSnapshotポリシーとレプリケーションポリシーがこの手順で選択したポリシーと異なる場合は、既存のポリシーが上書きされます。

- オブジェクトストレージ情報（プロバイダ、暗号化、ネットワーク、バックアップポリシー、エクスポートオプション）へのバックアップ。

手順

1. [Define backup strategy]ページで、次のいずれかまたはすべてを選択します。デフォルトでは、3つすべてが選択されています。
   - *ローカルSnapshot *：レプリケーションまたはオブジェクトストレージへのバックアップを実行する場合は、ローカルSnapshotを作成する必要があります。
   - レプリケーション：別のONTAPストレージシステムにレプリケートされたボリュームを作成します。
   - バックアップ：ボリュームをオブジェクトストレージにバックアップします。
2. アーキテクチャ:レプリケーションとバックアップを選択した場合は'次のいずれかの情報フローを選択します
   - カスケード：情報は、プライマリからセカンダリへ、およびセカンダリからオブジェクトストレージへと流れます。
   - ファンアウト：プライマリからセカンダリへ、プライマリからオブジェクトストレージへ、情報が流れます。

     これらのアーキテクチャの詳細については、を参照してください "保護対策を計画しましょう"。
3. *ローカルSnapshot *：既存のSnapshotポリシーを選択するか、新しいSnapshotポリシーを作成します。

   > Snapshotをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

   ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

   - ポリシーの名前を入力します。

- 最大5つのスケジュール（通常は異なる周波数）を選択します。
- 「 * Create * 」を選択します。

4. レプリケーション：次のオプションを設定します。
   - レプリケーションターゲット：デスティネーションの作業環境とSVMを選択します。必要に応じて、レプリケートするボリュームの名前に追加するデスティネーションアグリゲートとプレフィックスまたはサフィックスを選択します。
   - レプリケーションポリシー：既存のレプリケーションポリシーを選択するか、新しいレプリケーションポリシーを作成します。

     > レプリケーションをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

     ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

     - ポリシーの名前を入力します。
     - 最大5つのスケジュール（通常は異なる周波数）を選択します。
     - 「 * Create * 」を選択します。
5. オブジェクトにバックアップ：*バックアップ*を選択した場合は、次のオプションを設定します。
   - プロバイダ：* Google Cloud *を選択します。
   - プロバイダ設定：バックアップを保存するプロバイダの詳細と地域を入力します。

     新しいバケットを作成するか、すでに作成したバケットを選択します。

     > コストをさらに最適化するために古いバックアップファイルをGoogle Cloud Archiveストレージに階層化する場合は、バケットに適切なライフサイクルルールが設定されていることを確認してください。

     Google Cloudのアクセスキーとシークレットキーを入力します。

   - 暗号化キー：新しいGoogle Cloudストレージアカウントを作成した場合は、プロバイダから提供された暗号化キー情報を入力します。データの暗号化を管理するために、デフォルトのGoogle Cloud暗号化キーを使用するか、Google Cloudアカウントからお客様が管理する独自のキーを選択するかを選択します。

     > 既存のGoogle Cloudストレージアカウントを選択した場合、暗号化情報はすでに利用可能なため、ここで入力する必要はありません。

     独自のカスタマー管理キーを使用する場合は、キーリングとキー名を入力します。 "お客様が管理する暗号化キーの詳細については、こちらをご覧ください"。

   - ネットワーク：IPspaceを選択します。

     バックアップするボリュームが配置されている ONTAP クラスタ内の IPspace 。この IPspace のクラスタ間 LIF 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。

   - バックアップポリシー：既存のオブジェクトストレージへのバックアップポリシーを選択するか、新

しいポリシーを作成します。

> バックアップをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

- ポリシーの名前を入力します。
- 最大5つのスケジュール（通常は異なる周波数）を選択します。
- 「 * Create * 」を選択します。

◦ 既存の**Snapshot**コピーをバックアップコピーとしてオブジェクトストレージにエクスポート：この作業環境に、この作業環境に対して選択したバックアップスケジュールラベル（daily、weeklyなど）と一致するボリュームのローカルSnapshotコピーがある場合は、この追加のプロンプトが表示されます。ボリュームを最大限に保護するために、履歴Snapshotをすべてオブジェクトストレージにバックアップファイルとしてコピーする場合は、このチェックボックスをオンにします。

6. 「 * 次へ * 」を選択します。

選択内容を確認します

これにより、選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. [Review]ページで、選択内容を確認します。
2. 必要に応じて、Snapshotポリシーのラベルをレプリケーションポリシーおよびバックアップポリシーのラベルと自動的に同期する*チェックボックスをオンにします。これにより、レプリケーションポリシーとバックアップポリシーのラベルに一致するラベルを持つSnapshotが作成されます。
3. [バックアップのアクティブ化]*を選択します。

結果

BlueXPのバックアップとリカバリで、ボリュームの初期バックアップが作成されます。レプリケートされたボリュームとバックアップファイルのベースライン転送には、プライマリストレージシステムのデータのフルコピーが含まれます。以降の転送には、Snapshotコピーに含まれるプライマリストレージシステムデータの差分コピーが含まれます。

ソースボリュームと同期されるデスティネーションクラスタにレプリケートされたボリュームが作成されます。

Google Cloud Storageバケットは、入力したGoogleアクセスキーとシークレットキーで指定されたサービスアカウントに自動的に作成され、そこにバックアップファイルが格納されます。ボリュームバックアップダッシュボードが表示され、バックアップの状態を監視できます。

を使用して、バックアップジョブとリストアジョブのステータスを監視することもできます "［ジョブ監視］パネル"。

APIコマンドを表示します

バックアップとリカバリのアクティブ化ウィザードで使用するAPIコマンドを表示し、必要に応じてコピーすることができます。これは、将来の作業環境でバックアップを自動的にアクティブ化する場合に必要になることがあります。

手順

1. バックアップとリカバリのアクティブ化ウィザードで、*[API要求の表示]*を選択します。
2. コマンドをクリップボードにコピーするには、*コピー*アイコンを選択します。

次の手順

- 可能です "バックアップファイルとバックアップポリシーを管理"。バックアップの開始と停止、バックアップの削除、バックアップスケジュールの追加と変更などが含まれます。
- 可能です "クラスタレベルのバックアップの設定を管理します"。これには、クラウドストレージへのアクセスにONTAP で使用するストレージキーの変更、オブジェクトストレージへのバックアップのアップロードに使用できるネットワーク帯域幅の変更、将来のボリュームに対する自動バックアップ設定の変更などが含まれます。
- また可能です "ボリューム、フォルダ、または個々のファイルをバックアップファイルからリストアする" Google の Cloud Volumes ONTAP システムやオンプレミスの ONTAP システムに接続できます。

オンプレミスの**ONTAP**データを**ONTAP S3**にバックアップ

いくつかの手順を実行して、プライマリオンプレミスONTAPシステムからボリュームデータのバックアップを開始します。バックアップは、セカンダリONTAPストレージシステム（レプリケートされたボリューム）、S3サーバとして設定されたONTAPシステムのバケット（バックアップファイル）、またはその両方に送信できます。

オンプレミスのプライマリONTAPシステムは、FAS、AFF、ONTAP Selectのいずれかです。セカンダリONTAPシステムには、オンプレミスのONTAPまたはCloud Volumes ONTAPシステムを使用できます。オブジェクトストレージは、オンプレミスのONTAPシステムでも、Simple Storage Service（S3）オブジェクトストレージサーバを有効にしたCloud Volumes ONTAPシステムでもかまいません。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。各手順の詳細については、このトピックの以降のセクションを参照してください。

1 使用する接続方法を特定します

レプリケーションのためにプライマリオンプレミスのONTAPクラスタをセカンダリONTAPクラスタに接続し、オブジェクトストレージへのバックアップ用にS3サーバとして構成されたONTAPクラスタに接続する方法を確認します。

接続方法を特定します。

2 **BlueXP**コネクタを準備します

BlueXPコネクタをすでに導入している場合は、準備は完了です。そうでない場合は、ONTAPデータをONTAP S3にバックアップするためのBlueXPコネクタを作成する必要があります。また、コネクタのネットワーク設定をカスタマイズして、ONTAP S3に接続できるようにする必要があります。

コネクタの作成方法と、必要なネットワーク設定の定義方法について説明します。

3 ライセンス要件を確認

ONTAPシステムとBlueXPのバックアップとリカバリのライセンス要件を確認する必要があります。

ライセンス要件を確認

4 **ONTAP**クラスタを準備

BlueXPでプライマリとセカンダリのONTAPクラスタを検出し、クラスタが最小要件を満たしていることを確認し、ネットワーク設定をカスタマイズしてクラスタをONTAP S3オブジェクトストレージに接続できるようにします。

ONTAPクラスタを準備する方法をご紹介します。

5 バックアップターゲットとしての**ONTAP S3**の準備

コネクタがONTAP S3バケットを管理できるように、コネクタの権限を設定します。また、ソースのオンプレミスONTAPクラスタがONTAP S3バケットに対してデータの読み取りと書き込みを行えるように、権限を設定する必要があります。

ONTAP S3環境でONTAPバックアップを受信できるようにする方法を説明します。

6 **ONTAP**ボリュームでバックアップをアクティブ化します

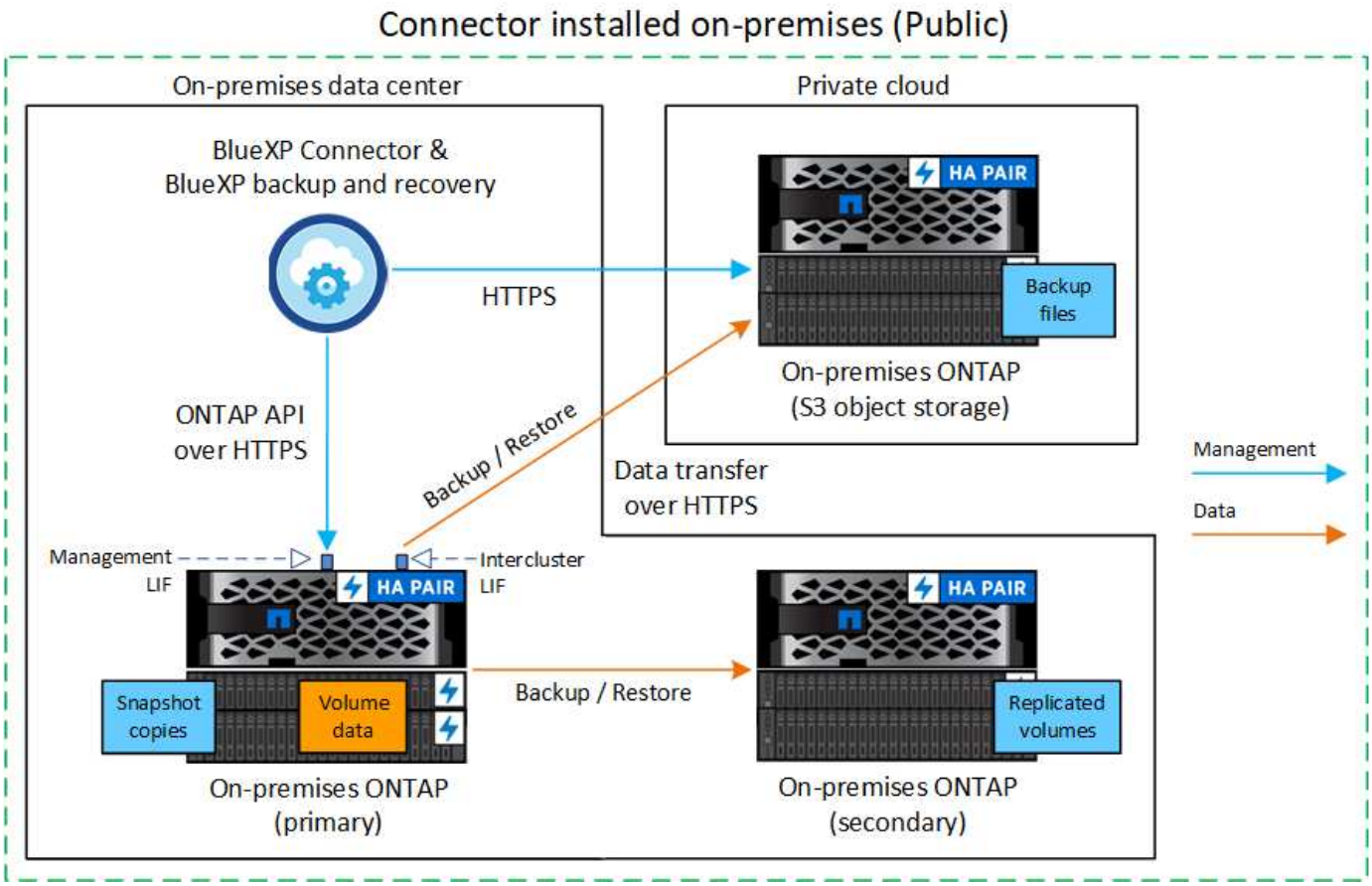
プライマリ作業環境を選択し、右パネルのバックアップとリカバリサービスの横にある*[有効化]>[ボリュームのバックアップ]*をクリックします。次に、セットアップウィザードに従って、バックアップするボリュームと、使用するSnapshotポリシー、レプリケーションポリシー、オブジェクトへのバックアップポリシーを選択します。

ONTAPボリュームでバックアップをアクティブ化します。

接続方法を特定します

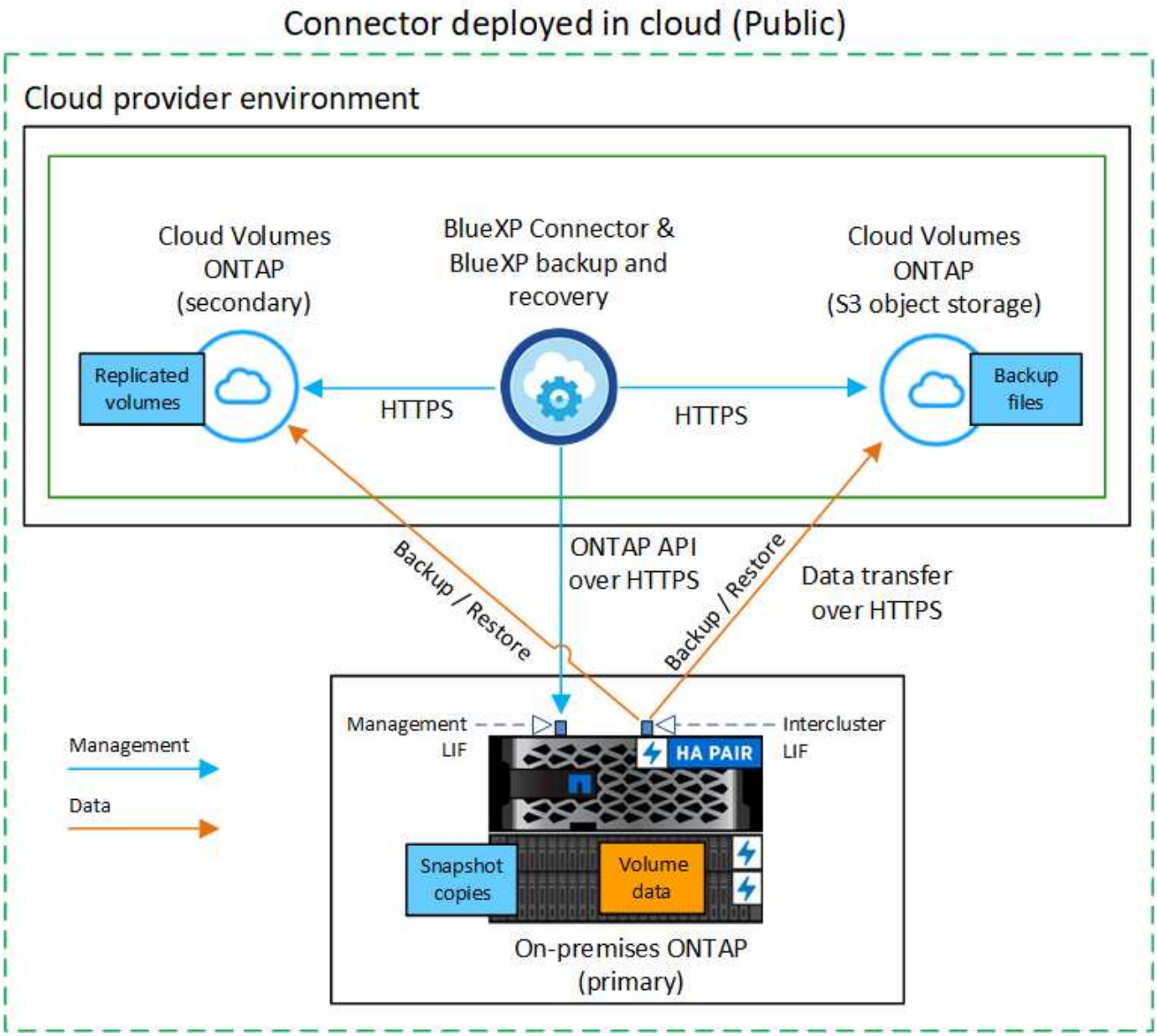
ONTAPシステムのS3バケットへのバックアップを作成できる設定は多数あります。以下に2つのシナリオを示します。

次の図は、S3用に設定されたオンプレミスのONTAPシステムにプライマリのオンプレミスONTAPシステムをバックアップする場合の各コンポーネントと、それらの間の接続を示しています。また、オンプレミスと同じ場所にあるセカンダリONTAPシステムに接続してボリュームをレプリケートしていることも示されています。



コネクタとプライマリオンプレミスのONTAPシステムを、インターネットにアクセスできないオンプレミスの場所にインストールする場合（「プライベート」モードの導入）は、ONTAP S3システムを同じオンプレミスのデータセンターに配置する必要があります。

次の図は、S3用に設定されたCloud Volumes ONTAPシステムにプライマリオンプレミスONTAPシステムをバックアップする場合の各コンポーネントと、それらの間の接続の準備を示しています。また、同じクラウドプロバイダ環境内のセカンダリCloud Volumes ONTAPシステムに接続してボリュームをレプリケートしていることも示されています。



このシナリオでは、Cloud Volumes ONTAPシステムが導入されているのと同じクラウドプロバイダ環境にコネクタを導入します。

BlueXPコネクタを準備します

BlueXPコネクタは'BlueXP機能の主要なソフトウェアですONTAP データのバックアップとリストアにはコネクタが必要です。

コネクタを作成または切り替えます

データをONTAP S3にバックアップする場合は、オンプレミスまたはクラウドでBlueXP Connectorを使用できる必要があります。新しいコネクタをインストールするか、現在選択されているコネクタがこれらの場所のいずれかにあることを確認する必要があります。オンプレミスコネクタは、インターネットアクセスの有無にかかわらず、サイトにインストールできます。

- "コネクタについて説明します"

- "クラウド環境へのコネクタのインストール"
- "インターネットにアクセスできる Linux ホストにコネクタをインストールしています"
- "インターネットにアクセスできない Linux ホストにコネクタをインストールしています"
- "コネクタ間の切り替え"

コネクタのネットワーク要件を準備

コネクタが取り付けられているネットワークで次の接続が有効になっていることを確認します。

- ポート443経由でONTAP S3サーバにHTTPS接続
- ポート443を介してソースのONTAPクラスタ管理LIFにHTTPS接続
- BlueXPのバックアップとリカバリへのポート443経由のアウトバウンドインターネット接続（「ダーク」サイトにコネクタがインストールされている場合は不要）

プライベートモード（ダークサイト）に関する考慮事項

BlueXPコネクタには、BlueXPのバックアップとリカバリ機能が組み込まれています。プライベートモードでインストールされている場合は、コネクタソフトウェアを定期的に更新して、新しい機能にアクセスする必要があります。を確認します "BlueXPのバックアップとリカバリの最新情報" にアクセスし、BlueXPのバックアップとリカバリの各リリースの新機能を確認してください。新しい機能を使用する場合は、手順~に従ってください "Connector ソフトウェアをアップグレードします"。

標準的なSaaS環境でBlueXPのバックアップとリカバリを使用すると、BlueXPのバックアップとリカバリの設定データがクラウドにバックアップされます。インターネットにアクセスできないサイトでBlueXPのバックアップとリカバリを使用すると、BlueXPのバックアップとリカバリの設定データがバックアップが格納されているONTAP S3バケットにバックアップされます。プライベートモードサイトでコネクタに障害が発生した場合は、できます "BlueXPのバックアップとリカバリのデータを新しいコネクタにリストアします"。

ライセンス要件を確認

クラスタでBlueXPのバックアップとリカバリをアクティブ化するには、ネットアップからBlueXPのバックアップとリカバリのBYOLライセンスを購入してアクティブ化する必要があります。オブジェクトストレージへのバックアップとリストアを対象としたライセンスです。Snapshotコピーやレプリケートされたボリュームの作成にライセンスは必要ありません。このライセンスはアカウント用であり、複数のシステムで使用できます。

ネットアップから提供されるシリアル番号を使用して、ライセンスの期間と容量にサービスを利用できるようにする必要があります。 "BYOL ライセンスの管理方法について説明します"。

ONTAP S3にファイルをバックアップする場合、PAYGOライセンスはサポートされません。

ONTAPクラスタを準備

ソースのオンプレミスONTAPシステムと、セカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムを準備する必要があります。

ONTAPクラスタの準備では、次の手順を実行します。

- BlueXPでONTAPシステムを検出しましょう

- ONTAPのシステム要件を確認
- オブジェクトストレージにデータをバックアップするためのONTAPネットワークの要件を確認します
- ボリュームをレプリケートするためのONTAPネットワークの要件を確認します

BlueXPで**ONTAP**システムを検出しましょう

ソースのオンプレミスONTAPシステムとセカンダリのオンプレミスONTAPシステムまたはCloud Volumes ONTAPシステムの両方が、BlueXPキャンバスで利用可能である必要があります。

クラスタを追加するには、クラスタ管理 IP アドレスと admin ユーザアカウントのパスワードが必要です。"クラスタの検出方法について説明します"。

ONTAPのシステム要件を確認

次のONTAP要件が満たされていることを確認します。

- ONTAP 9.8以上、ONTAP 9.8P13以降が推奨されます。
- SnapMirror ライセンス（ Premium Bundle または Data Protection Bundle に含まれます）。

  注： BlueXPのバックアップとリカバリを使用する場合、「Hybrid Cloud Bundle」は必要ありません。

  方法をご確認ください "クラスタライセンスを管理します"。

- 時間とタイムゾーンが正しく設定されている。方法をご確認ください "クラスタ時間を設定します"。
- データをレプリケートする場合は、データをレプリケートする前に、ソースシステムとデスティネーションシステムで互換性のあるONTAPバージョンが実行されていることを確認する必要があります。

  "SnapMirror 関係に対して互換性のある ONTAP バージョンを表示します"。

オブジェクトストレージにデータをバックアップするための**ONTAP**ネットワークの要件を確認します

オブジェクトストレージに接続するシステムが次の要件を満たしていることを確認する必要があります。

- ファンアウトバックアップアーキテクチャを使用する場合は、_primary_storageシステムで設定を行う必要があります。
- カスケードバックアップアーキテクチャを使用する場合は、_secondary_storageシステムで設定を行う必要があります。

  "バックアップアーキテクチャのタイプの詳細"。

次のONTAPクラスタネットワーク要件が必要です。

- ONTAPクラスタは、バックアップ処理とリストア処理のために、ユーザ指定のポートを介してクラスタ間LIFからONTAP S3サーバへのHTTPS接続を開始します。ポートはバックアップのセットアップ時に設定できます。

  ONTAP は、オブジェクトストレージとの間でデータの読み取りと書き込みを行います。オブジェクトストレージが開始されることはなく、応答するだけです。

- ONTAP では、コネクタからクラスタ管理 LIF へのインバウンド接続が必要です。
- クラスタ間 LIF は、バックアップ対象のボリュームをホストする各 ONTAP ノードに必要です。LIF は、ONTAP がオブジェクトストレージへの接続に使用する IPspace に関連付けられている必要があります。"IPspace の詳細については、こちらをご覧ください"。

  BlueXPのバックアップとリカバリをセットアップするときに、使用するIPspaceを指定するように求められます。各 LIF を関連付ける IPspace を選択する必要があります。これは、「デフォルト」の IPspace または作成したカスタム IPspace です。

- ノードのクラスタ間 LIF はオブジェクトストアにアクセスできます（コネクタが「ダーク」サイトに設置されている場合は不要）。
- ボリュームが配置されている Storage VM に DNS サーバが設定されている。方法を参照してください "SVM 用に DNS サービスを設定"。
- を使用しているIPspaceがデフォルトと異なる場合は、オブジェクトストレージにアクセスするための静的ルートの作成が必要になることがあります。
- 必要に応じてファイアウォールルールを更新して、指定したポート（通常はポート443）を介してONTAPからオブジェクトストレージへのBlueXPバックアップ/リカバリサービスの接続と、Storage VMからDNSサーバへのポート53（TCP / UDP）経由の名前解決トラフィックを許可します。

ボリュームをレプリケートするための**ONTAP**ネットワークの要件を確認します

BlueXPのバックアップとリカバリを使用してセカンダリONTAPシステムにレプリケートされたボリュームを作成する場合は、ソースシステムとデスティネーションシステムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワークの要件

- クラスタが社内にある場合は、社内ネットワークからクラウドプロバイダ内の仮想ネットワークへの接続が必要です。これは通常、 VPN 接続です。
- ONTAP クラスタは、サブネット、ポート、ファイアウォール、およびクラスタの追加要件を満たしている必要があります。

  Cloud Volumes ONTAPまたはオンプレミスのシステムにレプリケートできるため、オンプレミスのONTAPシステムのピアリング要件を確認してください。 "クラスタピアリングの前提条件については、ONTAP のドキュメントを参照してください"。

Cloud Volumes ONTAPネットワークの要件

- インスタンスのセキュリティグループに、必要なインバウンドおよびアウトバウンドのルールが含まれている必要があります。具体的には、 ICMP とポート 11104 および 11105 のルールが必要です。これらのルールは、事前定義されたセキュリティグループに含まれています。

バックアップターゲットとしての**ONTAP S3**の準備

オブジェクトストレージのバックアップに使用するSimple Storage Service（S3）オブジェクトストレージサーバをONTAPクラスタで有効にする必要があります。を参照してください "ONTAP S3のドキュメント" を参照してください。

*注：*このクラスタはBlueXP Canvasで検出できますが、S3オブジェクトストレージサーバではないため、ソースの作業環境をこのS3作業環境にドラッグアンドドロップしてバックアップのアクティブ化を開始するこ

とはできません。

このONTAPシステムは、次の要件を満たしている必要があります。

サポートされる**ONTAP**のバージョン

オンプレミスのONTAPシステムにはONTAP 9.8以降が必要です。
Cloud Volumes ONTAPシステムにはONTAP 9.9.1以降が必要です。

S3 クレデンシャル

ONTAP S3ストレージへのアクセスを制御するS3ユーザを作成しておく必要があります。 "詳細については、ONTAP S3のドキュメントを参照してください。"。

ONTAP S3へのバックアップをセットアップする際に、バックアップウィザードでユーザアカウントのS3アクセスキーとシークレットキーの入力を求められます。このユーザアカウントを使用して、BlueXPのバックアップとリカバリで、バックアップの格納に使用するONTAP S3バケットを認証し、アクセスすることができます。キーは、ONTAP S3が要求の送信者を認識するために必要です。

これらのアクセスキーは、次の権限を持つユーザに関連付ける必要があります。

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

ONTAPボリュームでバックアップをアクティブ化します

オンプレミスの作業環境からいつでも直接バックアップをアクティブ化できます。

ウィザードでは、次の主な手順を実行します。

- バックアップするボリュームを選択します
- バックアップ戦略とポリシーを定義
- 選択内容を確認します

また可能です APIコマンドを表示します レビューステップでは、コードをコピーして、将来の作業環境のバックアップアクティベーションを自動化できます。

ウィザードを開始します

手順

1. 次のいずれかの方法でバックアップとリカバリのアクティブ化ウィザードにアクセスします。
    - BlueXPキャンバスで、作業環境を選択し、右パネルのバックアップとリカバリサービスの横にある*[有効化]>[ボリュームのバックアップ]*を選択します。
    - [バックアップとリカバリ]バーで*を選択します。**[**ボリューム**]**タブで、[アクション（…）]オプションを選択し、（オブジェクトストレージへのレプリケーションまたはバックアップがまだ有効になって

いない）単一ボリュームに対して[バックアップのアクティブ化]*を選択します。

ウィザードの[Introduction]ページには、ローカルSnapshot、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で2番目のオプションを選択した場合は、1つのボリュームが選択された状態で[Define Backup Strategy]ページが表示されます。

2. 次のオプションに進みます。
   - BlueXPコネクタをすでにお持ちの場合は、これで準備は完了です。[次へ]*を選択します。
   - BlueXPコネクタがない場合は、*[Add a Connector]*オプションが表示されます。を参照してください BlueXPコネクタを準備します。

バックアップするボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、Snapshotポリシー、レプリケーションポリシー、オブジェクトへのバックアップポリシーのうち1つ以上を含むボリュームです。

FlexVolボリュームとFlexGroupボリュームのどちらを保護するかを選択できますが、作業環境でバックアップをアクティブ化するときは、これらのボリュームを組み合わせて選択することはできません。方法を参照してください "作業環境内の追加ボリュームのバックアップをアクティブ化" （FlexVolまたはFlexGroup）初期ボリュームのバックアップの設定が完了したら、

- バックアップをアクティブ化できるのは、一度に1つのFlexGroupボリュームだけです。
- 選択するボリュームのSnapLock設定は同じである必要があります。すべてのボリュームでSnapLock Enterpriseが有効になっているかSnapLockが無効になっている必要があります。（SnapLock Complianceモードのボリュームには、ONTAP 9.14以降が必要です）。

手順

選択したボリュームにSnapshotポリシーまたはレプリケーションポリシーがすでに適用されている場合は、あとで選択したポリシーで既存のポリシーが上書きされます。

1. [Select Volumes]ページで、保護するボリュームを選択します。
   - 必要に応じて、行をフィルタして、特定のボリュームタイプや形式などのボリュームのみを表示し、選択を容易にします。
   - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます（FlexGroupボリュームは一度に1つだけ選択できます）。既存のFlexVolボリュームをすべてバックアップするには、最初に1つのボリュームをオンにしてから、タイトル行のボックスをオンにします。（☑ Volume Name）。
   - 個々のボリュームをバックアップするには、各ボリュームのボックス（☑ Volume_1）。
2. 「 * 次へ * 」を選択します。

バックアップ戦略を定義します

バックアップ戦略を定義するには、次のオプションを設定する必要があります。

- 保護オプション：1つまたはすべてのバックアップオプション（ローカルSnapshot、レプリケーション、オブジェクトストレージへのバックアップ）を実装するかどうか
- アーキテクチャ：ファンアウトとカスケードのどちらのバックアップアーキテクチャを使用するか
- ローカルSnapshotポリシー

- レプリケーションのターゲットとポリシー
- オブジェクトストレージ情報（プロバイダ、暗号化、ネットワーク、バックアップポリシー、エクスポートオプション）へのバックアップ。

手順

1. [Define Backup Strategy]ページで、次のいずれかまたはすべてを選択します。デフォルトでは、3つすべてが選択されています。
   - *ローカルSnapshot *：ローカルSnapshotコピーを作成します。
   - レプリケーション：別のONTAPストレージシステムにレプリケートされたボリュームを作成します。
   - バックアップ：S3用に設定されたONTAPシステムのバケットにボリュームをバックアップします。
2. アーキテクチャ:レプリケーションとバックアップの両方を選択した場合は'次のいずれかの情報フローを選択します
   - カスケード：バックアップデータは、プライマリシステムからセカンダリシステムへと流れ、次にセカンダリシステムからオブジェクトストレージへと流れます。
   - ファンアウト：バックアップデータは、プライマリからセカンダリシステムへ、プライマリからオブジェクトストレージへのフローです。

     これらのアーキテクチャの詳細については、を参照してください "保護対策を計画しましょう"。
3. *ローカルSnapshot *：既存のSnapshotポリシーを選択するか、新しいSnapshotポリシーを作成します。

   Snapshotをアクティブ化する前にカスタムポリシーを作成する場合は、System ManagerまたはONTAP CLIを使用します。 `snapmirror policy create` コマンドを実行しますを参照してください。

   Snapshotをアクティブ化する前にこのサービスを使用してカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

   ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

   - ポリシーの名前を入力します。
   - 最大5つのスケジュール（通常は異なる周波数）を選択します。
   - 「 * Create * 」を選択します。
4. レプリケーション：*レプリケーション*を選択した場合は、次のオプションを設定します。
   - レプリケーションターゲット：デスティネーションの作業環境とSVMを選択します。必要に応じて、デスティネーションアグリゲート（FlexGroupボリュームの場合はアグリゲート）、およびレプリケートされたボリューム名に追加するプレフィックスまたはサフィックスを選択します。
   - レプリケーションポリシー：既存のレプリケーションポリシーを選択するか、新しいレプリケーションポリシーを作成します。

     ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

     - ポリシーの名前を入力します。
     - 最大5つのスケジュール（通常は異なる周波数）を選択します。

- 「 * Create * 」を選択します。

5. オブジェクトにバックアップ：*バックアップ*を選択した場合は、次のオプションを設定します。
   - プロバイダ：* ONTAP S3 *を選択します。
   - プロバイダ設定：S3サーバのFQDNの詳細、ポート、およびユーザのアクセスキーとシークレットキーを入力します。

     アクセスキーとシークレットキーは、 ONTAP クラスタに S3 バケットへのアクセスを付与するために作成したユーザ用のキーです。

   - ネットワーク：バックアップするボリュームが配置されているソースONTAPクラスタのIPspaceを選択します。この IPspace のクラスタ間 LIF 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（コネクタが「ダーク」サイトにインストールされている場合は不要です）。

     > 正しいIPspaceを選択すると、BlueXPのバックアップとリカバリでONTAPからONTAP S3オブジェクトストレージへの接続をセットアップできます。

   - バックアップポリシー：既存のバックアップポリシーを選択するか、新しいバックアップポリシーを作成します。

     > ポリシーはSystem ManagerまたはONTAP CLIで作成できます。ONTAP CLIを使用してカスタムポリシーを作成するには `snapmirror policy create` コマンド、を参照してください。。

     > UIを使用してバックアップをアクティブ化する前にカスタムポリシーを作成する方法については、を参照してください。 "ポリシーを作成する"。

     ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

     - ポリシーの名前を入力します。
     - 最大5つのスケジュール（通常は異なる周波数）を選択します。
     - オブジェクトへのバックアップポリシーの場合は、DataLockとRansomware Protectionを設定します。DataLockとランサムウェア対策の詳細については、 "オブジェクトへのバックアップポリシーの設定"。
     - 「 * Create * 」を選択します。

   - 既存の**Snapshot**コピーをバックアップファイルとしてオブジェクトストレージにエクスポート：この作業環境に、選択したバックアップスケジュールラベル（daily、weeklyなど）と一致するボリュームのローカルSnapshotコピーがある場合は、この追加のプロンプトが表示されます。ボリュームを最大限に保護するために、履歴Snapshotをすべてオブジェクトストレージにバックアップファイルとしてコピーする場合は、このチェックボックスをオンにします。
6. 「 * 次へ * 」を選択します。

選択内容を確認します

これにより、選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. [Review]ページで、選択内容を確認します。
2. 必要に応じて、Snapshotポリシーのラベルをレプリケーションポリシーおよびバックアップポリシーのラベルと自動的に同期する*チェックボックスをオンにします。これにより、レプリケーションポリシーとバックアップポリシーのラベルに一致するラベルを持つSnapshotが作成されます。ポリシーが一致しない場合、バックアップは作成されません。
3. [バックアップのアクティブ化]*を選択します。

結果

BlueXPのバックアップとリカバリで、ボリュームの初期バックアップが作成されます。レプリケートされたボリュームとバックアップファイルのベースライン転送には、ソースデータのフルコピーが含まれます。以降の転送には、Snapshotコピーに含まれるプライマリストレージデータの差分コピーが含まれます。

レプリケートされたボリュームが、プライマリストレージボリュームと同期されるデスティネーションクラスタに作成されます。

入力したS3アクセスキーとシークレットキーで指定されたサービスアカウントにS3バケットが作成され、バックアップファイルがそこに格納されます。

ボリュームバックアップダッシュボードが表示され、バックアップの状態を監視できます。

を使用して、バックアップジョブとリストアジョブのステータスを監視することもできます "［ジョブ監視］パネル"。

APIコマンドを表示します

バックアップとリカバリのアクティブ化ウィザードで使用するAPIコマンドを表示し、必要に応じてコピーすることができます。これは、将来の作業環境でバックアップを自動的にアクティブ化する場合に必要になることがあります。

手順

1. バックアップとリカバリのアクティブ化ウィザードで、*[API要求の表示]*を選択します。
2. コマンドをクリップボードにコピーするには、*コピー*アイコンを選択します。

次の手順

- 可能です "バックアップファイルとバックアップポリシーを管理"。バックアップの開始と停止、バックアップの削除、バックアップスケジュールの追加と変更などが含まれます。
- 可能です "クラスタレベルのバックアップの設定を管理します"。これには、バックアップをオブジェクトストレージにアップロードするためのネットワーク帯域幅の変更、将来のボリュームに対する自動バックアップ設定の変更などが含まれます。
- また可能です "ボリューム、フォルダ、または個々のファイルをバックアップファイルからリストアする" オンプレミスのONTAP システムへの移行をサポート

オンプレミスの **ONTAP** データを **StorageGRID** にバックアップ

オンプレミスのプライマリONTAPシステムからセカンダリストレージシステムおよびNetApp StorageGRIDシステムのオブジェクトストレージへのボリュームデータのバッ

クアップを開始するには、いくつかの手順を実行します。

「オンプレミスのONTAPシステム」には、FAS、AFF、ONTAP Selectシステムが含まれます。

クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。各手順の詳細については、このトピックの以降のセクションを参照してください。

1 使用する接続方法を特定します

オンプレミスのONTAPクラスタをパブリックインターネット経由でStorageGRIDに直接接続する方法、またはVPNを使用してプライベートVPCエンドポイントインターフェイスを介してトラフィックをStorageGRIDにルーティングするかどうかを確認します。

[接続方法を特定します]。

2 **BlueXP**コネクタを準備します

オンプレミスに既にコネクタがデプロイされている場合は、すべて準備が完了しています。そうでない場合は、ONTAPデータをStorageGRIDにバックアップするためのBlueXPコネクタを作成する必要があります。また、コネクタがStorageGRIDに接続できるように、コネクタのネットワーク設定をカスタマイズする必要があります。

コネクタの作成方法と、必要なネットワーク設定の定義方法について説明します。

3 ライセンス要件を確認

StorageGRIDとBlueXPの両方のライセンス要件を確認する必要があります。

を参照してください [ライセンス要件を確認]。

4 **ONTAP**クラスタを準備

BlueXPでONTAPクラスタを検出し、クラスタが最小要件を満たしていることを確認し、ネットワーク設定をカスタマイズしてクラスタをStorageGRIDに接続できるようにします。

ONTAPクラスタを準備する方法をご紹介します。

5 バックアップターゲットとして**StorageGRID**を準備します

StorageGRIDバケットを作成および管理するためのコネクタの権限を設定します。また、オンプレミスのONTAPクラスタでバケットに対するデータの読み取りと書き込みができるように権限を設定する必要があります。

必要に応じて、デフォルトのStorageGRID暗号化キーを使用する代わりに、データ暗号化用に独自のカスタム管理キーを設定できます。 StorageGRID環境でONTAPバックアップを受信できるようにする方法をご紹介します。

6 **ONTAP**ボリュームでバックアップをアクティブ化します

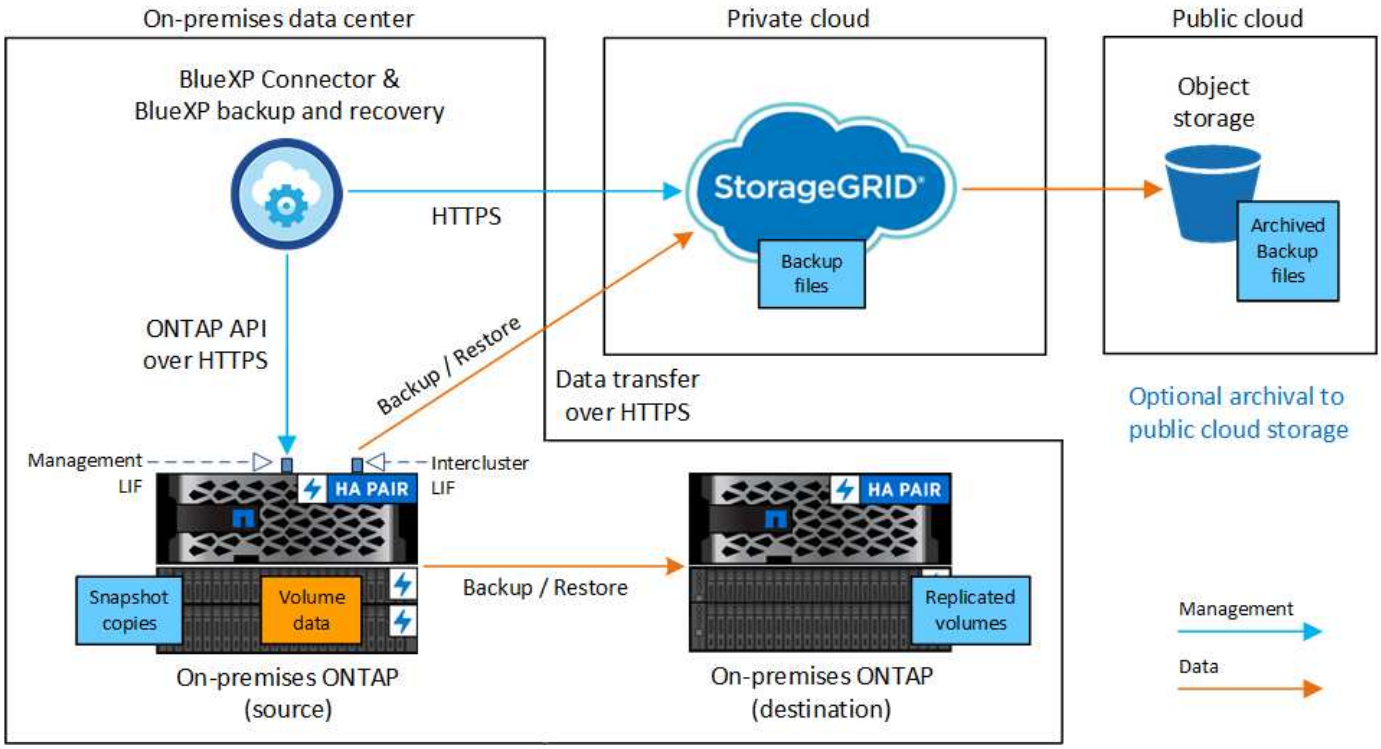
作業環境を選択し、右パネルのバックアップ/リカバリサービスの横にある*有効化>バックアップボリューム*をクリックします。次に、セットアップウィザードに従って、使用するレプリケーションポリシーとバックアップポリシー、およびバックアップするボリュームを選択します。

ONTAPボリュームでバックアップをアクティブ化します。

接続方法を特定します

次の図は、オンプレミスのONTAPシステムをStorageGRIDにバックアップする各コンポーネントと、それらのコンポーネント間の接続を示しています。

必要に応じて、オンプレミスの同じ場所にあるセカンダリONTAPシステムに接続してボリュームをレプリケートできます。



コネクタとオンプレミスのONTAPシステムを、インターネットにアクセスできないオンプレミスの場所（「ダークサイト」）にインストールする場合は、StorageGRIDシステムを同じオンプレミスのデータセンターに配置する必要があります。ダークサイトの構成では、古いバックアップファイルをパブリッククラウドにアーカイブすることはできません。

BlueXPコネクタを準備します

BlueXPコネクタは'BlueXP機能の主要なソフトウェアですONTAP データのバックアップとリストアにはコネクタが必要です。

コネクタを作成または切り替えます

データをStorageGRIDにバックアップする場合は、オンプレミスでBlueXP Connectorが使用可能である必要

があります。新しいコネクタをインストールするか、現在選択されているコネクタがオンプレミスにあることを確認する必要があります。コネクタは、インターネットに接続するかどうかに関係なく、サイトにインストールできます。

- "コネクタについて説明します"
- "インターネットにアクセスできる Linux ホストにコネクタをインストールしています"
- "インターネットにアクセスできない Linux ホストにコネクタをインストールしています"
- "コネクタ間の切り替え"

コネクタのネットワーク要件を準備

コネクタが取り付けられているネットワークで次の接続が有効になっていることを確認します。

- ポート443からStorageGRID ゲートウェイノードへのHTTPS接続
- ONTAP クラスタ管理 LIF へのポート 443 経由の HTTPS 接続
- BlueXPのバックアップとリカバリへのポート443経由のアウトバウンドインターネット接続（「ダーク」サイトにコネクタがインストールされている場合は不要）

プライベートモード（ダークサイト）に関する考慮事項

- BlueXPコネクタには、BlueXPのバックアップとリカバリ機能が組み込まれています。プライベートモードでインストールされている場合は、コネクタソフトウェアを定期的に更新して、新しい機能にアクセスする必要があります。を確認します "BlueXPのバックアップとリカバリの最新情報" にアクセスし、BlueXPのバックアップとリカバリの各リリースの新機能を確認してください。新しい機能を使用する場合は、手順~に従ってください "Connector ソフトウェアをアップグレードします"。

  新しいバージョンのBlueXPバックアップ/リカバリでは、オブジェクトストレージへのバックアップの作成に加えて、Snapshotコピーやレプリケートされたボリュームのスケジュール設定と作成を行うことができます。これには、バージョン3.9.31以降のBlueXP Connectorが必要です。したがって、すべてのバックアップを管理するために、この最新リリースを入手することをお勧めします。

- SaaS環境でBlueXPのバックアップとリカバリを使用すると、BlueXPのバックアップとリカバリの設定データがクラウドにバックアップされます。インターネットにアクセスできないサイトでBlueXPのバックアップとリカバリを使用すると、BlueXPのバックアップとリカバリの設定データがバックアップが格納されているStorageGRIDバケットにバックアップされます。プライベートモードサイトでコネクタに障害が発生した場合は、できます "BlueXPのバックアップとリカバリのデータを新しいコネクタにリストアします"。

ライセンス要件を確認

クラスタでBlueXPのバックアップとリカバリをアクティブ化するには、ネットアップからBlueXPのバックアップとリカバリのBYOLライセンスを購入してアクティブ化する必要があります。このライセンスはアカウント用であり、複数のシステムで使用できます。

ネットアップから提供されるシリアル番号を使用して、ライセンスの期間と容量にサービスを利用できるようにする必要があります。 "BYOL ライセンスの管理方法について説明します"。

PAYGO ライセンスは、ファイルを StorageGRID にバックアップする場合にはサポートされません。

ONTAPクラスタを準備

ソースのオンプレミスONTAPシステムと、セカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムを準備する必要があります。

ONTAPクラスタの準備では、次の手順を実行します。

- BlueXPでONTAPシステムを検出しましょう
- ONTAPのシステム要件を確認
- オブジェクトストレージにデータをバックアップするためのONTAPネットワークの要件を確認します
- ボリュームをレプリケートするためのONTAPネットワークの要件を確認します

BlueXPでONTAPシステムを検出しましょう

ソースのオンプレミスONTAPシステムとセカンダリのオンプレミスONTAPシステムまたはCloud Volumes ONTAPシステムの両方が、BlueXPキャンバスで利用可能である必要があります。

クラスタを追加するには、クラスタ管理 IP アドレスと admin ユーザアカウントのパスワードが必要です。"クラスタの検出方法について説明します"。

ONTAPのシステム要件を確認

次のONTAP要件が満たされていることを確認します。

- ONTAP 9.8以上、ONTAP 9.8P13以降が推奨されます。
- SnapMirror ライセンス（ Premium Bundle または Data Protection Bundle に含まれます）。

  注： BlueXPのバックアップとリカバリを使用する場合、「Hybrid Cloud Bundle」は必要ありません。

  方法をご確認ください "クラスタライセンスを管理します"。

- 時間とタイムゾーンが正しく設定されている。方法をご確認ください "クラスタ時間を設定します"。
- データをレプリケートする場合は、データをレプリケートする前に、ソースシステムとデスティネーションシステムで互換性のあるONTAPバージョンが実行されていることを確認する必要があります。

  "SnapMirror 関係に対して互換性のある ONTAP バージョンを表示します"。

オブジェクトストレージにデータをバックアップするためのONTAPネットワークの要件を確認します

オブジェクトストレージに接続するシステムで、次の要件を設定する必要があります。

- ファンアウトバックアップアーキテクチャを使用する場合は、_primary_storageシステムで次の設定を行う必要があります。
- カスケードバックアップアーキテクチャを使用する場合は、_secondary_storageシステムで次の設定を行う必要があります。

次のONTAPクラスタネットワーク要件が必要です。

- ONTAP クラスタは、バックアップおよびリストア処理のために、ユーザ指定のポートをクラスタ間LIFか

らStorageGRID ゲートウェイノードに介してHTTPS接続を開始します。ポートはバックアップのセットアップ時に設定できます。

ONTAP は、オブジェクトストレージとの間でデータの読み取りと書き込みを行います。オブジェクトストレージが開始されることはなく、応答するだけです。

- ONTAP では、コネクタからクラスタ管理 LIF へのインバウンド接続が必要です。コネクタは必ずオンプレミスに配置してください。
- クラスタ間 LIF は、バックアップ対象のボリュームをホストする各 ONTAP ノードに必要です。LIF は、ONTAP がオブジェクトストレージへの接続に使用する IPspace に関連付けられている必要があります。"IPspace の詳細については、こちらをご覧ください"。

  BlueXPのバックアップとリカバリをセットアップするときに、使用するIPspaceを指定するように求められます。各 LIF を関連付ける IPspace を選択する必要があります。これは、「デフォルト」の IPspace または作成したカスタム IPspace です。

- ノードのクラスタ間 LIF はオブジェクトストアにアクセスできます（コネクタが「ダーク」サイトに設置されている場合は不要）。
- ボリュームが配置されている Storage VM に DNS サーバが設定されている。方法を参照してください "SVM 用に DNS サービスを設定"。
- を使用しているIPspaceがデフォルトと異なる場合は、オブジェクトストレージにアクセスするための静的ルートの作成が必要になることがあります。
- 必要に応じてファイアウォールルールを更新して、指定したポート（通常はポート443）を介してONTAPからオブジェクトストレージへのBlueXPバックアップ/リカバリサービスの接続と、Storage VMからDNSサーバへのポート53（TCP / UDP）経由の名前解決トラフィックを許可します。

ボリュームをレプリケートするための**ONTAP**ネットワークの要件を確認します

BlueXPのバックアップとリカバリを使用してセカンダリONTAPシステムにレプリケートされたボリュームを作成する場合は、ソースシステムとデスティネーションシステムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワークの要件

- クラスタが社内にある場合は、社内ネットワークからクラウドプロバイダ内の仮想ネットワークへの接続が必要です。これは通常、 VPN 接続です。
- ONTAP クラスタは、サブネット、ポート、ファイアウォール、およびクラスタの追加要件を満たしている必要があります。

  Cloud Volumes ONTAPまたはオンプレミスのシステムにレプリケートできるため、オンプレミスのONTAPシステムのピアリング要件を確認してください。 "クラスタピアリングの前提条件については、ONTAP のドキュメントを参照してください"。

Cloud Volumes ONTAPネットワークの要件

- インスタンスのセキュリティグループに、必要なインバウンドおよびアウトバウンドのルールが含まれている必要があります。具体的には、 ICMP とポート 11104 および 11105 のルールが必要です。これらのルールは、事前定義されたセキュリティグループに含まれています。

バックアップターゲットとして**StorageGRID**を準備します

StorageGRID は、次の要件を満たす必要があります。を参照してください "StorageGRID のドキュメント" を参照してください。

サポートされている **StorageGRID** のバージョン

StorageGRID 10.3 以降がサポートされます。

DataLockとRansomware Protectionをバックアップに使用するには、StorageGRID システムでバージョン11.6.0.3以降が実行されている必要があります。

古いバックアップをクラウドアーカイブストレージに階層化するには、StorageGRID システムでバージョン11.3以降が実行されている必要があります。また、StorageGRID システムがBlueXPキャンバスで検出されている必要があります。

S3 クレデンシャル

StorageGRID ストレージへのアクセスを制御するS3テナントアカウントを作成しておく必要があります。"詳細については、StorageGRID のドキュメントを参照してください"。

StorageGRID へのバックアップを設定する際、テナントアカウントのS3アクセスキーとシークレットキーを入力するようにバックアップウィザードで求められます。テナントアカウントを使用すると、バックアップの格納に使用するStorageGRID バケットをBlueXPのバックアップとリカバリで認証してアクセスできるようになります。StorageGRID が誰が要求を行うかを認識できるようにするには、キーが必要です。

これらのアクセスキーは、次の権限を持つユーザに関連付ける必要があります。

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

オブジェクトのバージョン管理

オブジェクトストアバケットでは、StorageGRID オブジェクトのバージョン管理を手動で有効にしないでください。

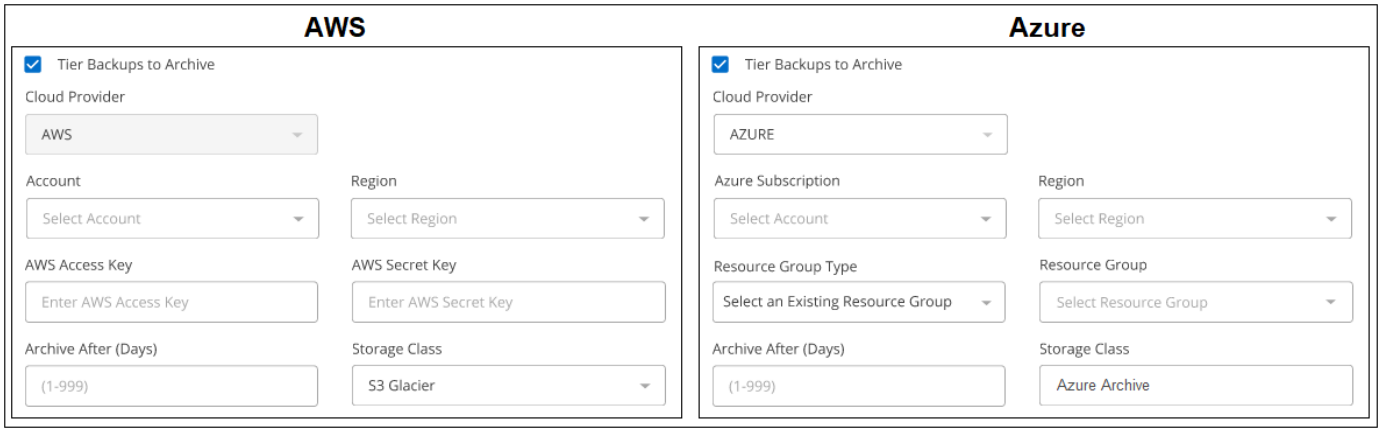
古いバックアップファイルをパブリッククラウドストレージにアーカイブする準備をします

古いバックアップファイルをアーカイブストレージに階層化すると、不要なバックアップに低コストのストレージクラスを使用することで、コストを削減できます。StorageGRID は、アーカイブストレージを提供しないオンプレミス（プライベートクラウド）の解決策 ですが、古いバックアップファイルをパブリッククラウドのアーカイブストレージに移動できます。この方法で使用した場合、クラウドストレージに階層化されたデータ、またはクラウドストレージから復元されたデータは、StorageGRID とクラウドストレージの間を移動します。BlueXPはこのデータ転送には関与しません。

現在のサポートでは、AWS_S3 Glacier Deep Archive_or_Azure Archive_storageにバックアップをアーカイブできます。

- ONTAP 要件*
- クラスタでONTAP 9.12.1以降が使用されている必要があります。
- StorageGRID 要件*
- StorageGRIDで11.4以降を使用している必要があります。
- StorageGRID はである必要があります "BlueXP Canvasで検出され、使用可能になりました"。
- Amazon S3の要件*
- アーカイブ済みバックアップを格納するストレージスペースには、Amazon S3アカウントを登録する必要があります。
- AWS S3 GlacierまたはS3 Glacier Deep Archiveストレージにバックアップを階層化することもできます。"AWSアーカイブ階層の詳細は、こちらをご覧ください"。
- StorageGRID には、バケットへのフルコントロールアクセスが必要です (`s3:*`) 。ただし、これができない場合は、バケットポリシーで次のS3権限をStorageGRID に付与する必要があります。
  - `s3:AbortMultipartUpload`
  - `s3:DeleteObject`
  - `s3:GetObject`
  - `s3:ListBucket`
  - `s3:ListBucketMultipartUploads`
  - `s3:ListMultipartUploadParts`
  - `s3:PutObject`
  - `s3:RestoreObject`
- Azure Blob要件*
- アーカイブ済みバックアップを格納するストレージスペースに対するAzureサブスクリプションに登録する必要があります。
- アクティブ化ウィザードでは、既存のリソースグループを使用して、バックアップを保存するBLOBコンテナを管理するか、新しいリソースグループを作成することができます。

クラスタのバックアップポリシーのアーカイブ設定を定義するときは、クラウドプロバイダのクレデンシャルを入力し、使用するストレージクラスを選択します。クラスタのバックアップをアクティブ化すると、BlueXPのバックアップとリカバリによってクラウドバケットが作成されます。AWSおよびAzureアーカイブストレージに必要な情報を次に示します。



選択したアーカイブポリシーの設定では、StorageGRID で情報ライフサイクル管理（ILM）ポリシーが生成され、「ルール」として追加されます。

- 既存のアクティブなILMポリシーがある場合は、新しいルールがILMポリシーに追加されてデータがアーカイブ階層に移動されます。
- 「ドラフト」状態の既存のILMポリシーがある場合は、新しいILMポリシーを作成およびアクティブ化できません。 "StorageGRID のILMポリシーとルールに関する詳細情報"。

ONTAPボリュームでバックアップをアクティブ化します

オンプレミスの作業環境からいつでも直接バックアップをアクティブ化できます。

ウィザードでは、次の主な手順を実行します。

- [バックアップするボリュームを選択します]
- [バックアップ戦略を定義します]
- [選択内容を確認します]

また可能です APIコマンドを表示します レビューステップでは、コードをコピーして、将来の作業環境のバックアップアクティベーションを自動化できます。

ウィザードを開始します

手順

1. 次のいずれかの方法でバックアップとリカバリのアクティブ化ウィザードにアクセスします。

    - BlueXPキャンバスで、作業環境を選択し、右パネルのバックアップとリカバリサービスの横にある*[有効化]>[ボリュームのバックアップ]*を選択します。

      バックアップのデスティネーションがキャンバスの作業環境として存在する場合は、ONTAPクラスタをオブジェクトストレージにドラッグできます。

    - [バックアップとリカバリ]バーで*を選択します。**[ボリューム]**タブで、[アクション（…）]オプションを選択し、（オブジェクトストレージへのレプリケーションまたはバックアップがまだ有効になっていない）単一ボリュームに対して[バックアップのアクティブ化]*を選択します。

    ウィザードの[Introduction]ページには、ローカルSnapshot、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で2番目のオプションを選択した場合は、1つのボリュームが選択さ

れた状態で[Define Backup Strategy]ページが表示されます。

2. 次のオプションに進みます。
   - BlueXPコネクタをすでにお持ちの場合は、これで準備は完了です。[次へ]*を選択します。
   - BlueXPコネクタをまだお持ちでない場合は、*[Add a Connector]*オプションが表示されます。を参照してください BlueXPコネクタを準備します。

バックアップするボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、Snapshotポリシー、レプリケーションポリシー、オブジェクトへのバックアップポリシーのうち1つ以上を含むボリュームです。

FlexVolボリュームとFlexGroupボリュームのどちらを保護するかを選択できますが、作業環境でバックアップをアクティブ化するときは、これらのボリュームを組み合わせて選択することはできません。方法を参照してください "作業環境内の追加ボリュームのバックアップをアクティブ化" （FlexVolまたはFlexGroup）初期ボリュームのバックアップの設定が完了したら、

- バックアップをアクティブ化できるのは、一度に1つのFlexGroupボリュームだけです。
- 選択するボリュームのSnapLock設定は同じである必要があります。すべてのボリュームでSnapLock Enterpriseが有効になっているかSnapLockが無効になっている必要があります。（SnapLock Complianceモードのボリュームには、ONTAP 9.14以降が必要です）。

手順

選択したボリュームにSnapshotポリシーまたはレプリケーションポリシーがすでに適用されている場合は、あとで選択したポリシーで既存のポリシーが上書きされます。

1. [Select Volumes]ページで、保護するボリュームを選択します。
   - 必要に応じて、行をフィルタして、特定のボリュームタイプや形式などのボリュームのみを表示し、選択を容易にします。
   - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます（FlexGroupボリュームは一度に1つだけ選択できます）。既存のFlexVolボリュームをすべてバックアップするには、最初に1つのボリュームをオンにしてから、タイトル行のボックスをオンにします。（☑ Volume Name）。
   - 個々のボリュームをバックアップするには、各ボリュームのボックス（☑ Volume_1）。
2. 「 * 次へ * 」を選択します。

バックアップ戦略を定義します

バックアップ戦略を定義するには、次のオプションを設定します。

- 1つまたはすべてのバックアップオプション（ローカルSnapshot、レプリケーション、オブジェクトストレージへのバックアップ）が必要かどうか
- アーキテクチャ
- ローカルSnapshotポリシー
- レプリケーションのターゲットとポリシー

> 選択したボリュームのSnapshotポリシーとレプリケーションポリシーがこの手順で選択したポリシーと異なる場合は、既存のポリシーが上書きされます。

- オブジェクトストレージ情報（プロバイダ、暗号化、ネットワーク、バックアップポリシー、エクスポートオプション）へのバックアップ。

手順

1. [Define backup strategy]ページで、次のいずれかまたはすべてを選択します。デフォルトでは、3つすべてが選択されています。
   - *ローカルSnapshot *：レプリケーションまたはオブジェクトストレージへのバックアップを実行する場合は、ローカルSnapshotを作成する必要があります。
   - レプリケーション：別のONTAPストレージシステムにレプリケートされたボリュームを作成します。
   - バックアップ：ボリュームをオブジェクトストレージにバックアップします。
2. アーキテクチャ:レプリケーションとバックアップの両方を選択した場合は'次のいずれかの情報フローを選択します
   - カスケード：情報はプライマリからセカンダリに流れ、次にセカンダリからオブジェクトストレージに流れます。
   - ファンアウト：プライマリからセカンダリへ、プライマリからオブジェクトストレージへ、情報が流れます。

     これらのアーキテクチャの詳細については、を参照してください "保護対策を計画しましょう"。
3. *ローカルSnapshot *：既存のSnapshotポリシーを選択するか、新しいSnapshotポリシーを作成します。

   > Snapshotをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

   ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

   - ポリシーの名前を入力します。
   - 最大5つのスケジュール（通常は異なる周波数）を選択します。
   - 「 * Create * 」を選択します。
4. レプリケーション：次のオプションを設定します。
   - レプリケーションターゲット：デスティネーションの作業環境とSVMを選択します。必要に応じて、レプリケートするボリュームの名前に追加するデスティネーションアグリゲートとプレフィックスまたはサフィックスを選択します。
   - レプリケーションポリシー：既存のレプリケーションポリシーを選択するか作成します。

     > レプリケーションをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

     ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

     - ポリシーの名前を入力します。

- 最大5つのスケジュール（通常は異なる周波数）を選択します。
- 「 * Create * 」を選択します。

5. オブジェクトにバックアップ：*バックアップ*を選択した場合は、次のオプションを設定します。
   - プロバイダー：* StorageGRID *を選択します。
   - プロバイダ設定：プロバイダゲートウェイノードのFQDNの詳細、ポート、アクセスキー、シークレットキーを入力します。

     アクセスキーとシークレットキーは、ONTAPクラスタにバケットへのアクセスを許可するために作成したIAMユーザのものです。

   - ネットワーク：バックアップするボリュームが配置されているONTAPクラスタのIPspaceを選択します。この IPspace のクラスタ間 LIF 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（コネクタが「ダーク」サイトにインストールされている場合は不要です）。

     > 正しいIPspaceを選択すると、BlueXPのバックアップとリカバリでONTAP からStorageGRID オブジェクトストレージへの接続をセットアップできます。

   - バックアップポリシー：既存のオブジェクトストレージへのバックアップポリシーを選択するか作成します。

     > バックアップをアクティブ化する前にカスタムポリシーを作成するには、を参照してください。 "ポリシーを作成する"。

     ポリシーを作成するには、*[新しいポリシーの作成]*を選択し、次の手順を実行します。

     - ポリシーの名前を入力します。
     - 最大5つのスケジュール（通常は異なる周波数）を選択します。
     - オブジェクトへのバックアップポリシーの場合は、DataLockとRansomware Protectionを設定します。DataLockとランサムウェア対策の詳細については、 "オブジェクトへのバックアップポリシーの設定"。

       クラスタがONTAP 9.11.1以降を使用している場合は、_DataLockとランサムウェアによる攻撃からバックアップを保護するように設定できます。_DataLock_バックアップファイルが変更または削除されないように保護し、_Ransomware Protection_バックアップファイルをスキャンしてバックアップファイル内のランサムウェア攻撃の証拠を探します。

     - 「 * Create * 」を選択します。

     クラスタがONTAP 9.12.1以降を使用しており、StorageGRID システムがバージョン11.4以降を使用している場合は、特定の日数が経過したあとに古いバックアップをパブリッククラウドのアーカイブ階層に階層化することを選択できます。現在、AWS S3 Glacier Deep ArchiveまたはAzure Archiveストレージ階層がサポートされています。 この機能を使用するためのシステムの設定方法を参照してください。

   - バックアップをパブリッククラウドに階層化：バックアップを階層化するクラウドプロバイダを選択し、プロバイダの詳細を入力します。

     新しいStorageGRIDクラスタを選択または作成します。StorageGRIDクラスタを作成してBlueXPで検出できるようにする方法については、を参照してください "StorageGRID のドキュメント"。

- 既存の**Snapshot**コピーをバックアップコピーとしてオブジェクトストレージにエクスポート：この作業環境に、この作業環境に対して選択したバックアップスケジュールラベル（daily、weeklyなど）と一致するボリュームのローカルSnapshotコピーがある場合は、この追加のプロンプトが表示されます。ボリュームを最大限に保護するために、履歴Snapshotをすべてオブジェクトストレージにバックアップファイルとしてコピーする場合は、このチェックボックスをオンにします。

6. 「 * 次へ * 」を選択します。

選択内容を確認します

これにより、選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. [Review]ページで、選択内容を確認します。
2. 必要に応じて、Snapshotポリシーのラベルをレプリケーションポリシーおよびバックアップポリシーのラベルと自動的に同期する*チェックボックスをオンにします。これにより、レプリケーションポリシーとバックアップポリシーのラベルに一致するラベルを持つSnapshotが作成されます。
3. [バックアップのアクティブ化]*を選択します。

結果

BlueXPのバックアップとリカバリで、ボリュームの初期バックアップが作成されます。レプリケートされたボリュームとバックアップファイルのベースライン転送には、ソースデータのフルコピーが含まれます。以降の転送には、Snapshotコピーに含まれるプライマリストレージデータの差分コピーが含まれます。

レプリケートされたボリュームが、プライマリストレージボリュームと同期されるデスティネーションクラスタに作成されます。

入力したS3アクセスキーとシークレットキーで指定されたサービスアカウントにS3バケットが作成され、バックアップファイルがそこに格納されます。

ボリュームバックアップダッシュボードが表示され、バックアップの状態を監視できます。

を使用して、バックアップジョブとリストアジョブのステータスを監視することもできます "［ジョブ監視］パネル"。

APIコマンドを表示します

バックアップとリカバリのアクティブ化ウィザードで使用するAPIコマンドを表示し、必要に応じてコピーすることができます。これは、将来の作業環境でバックアップを自動的にアクティブ化する場合に必要になることがあります。

手順

1. バックアップとリカバリのアクティブ化ウィザードで、*[API要求の表示]*を選択します。
2. コマンドをクリップボードにコピーするには、*コピー*アイコンを選択します。

次の手順

- 可能です "バックアップファイルとバックアップポリシーを管理"。バックアップの開始と停止、バックアップの削除、バックアップスケジュールの追加と変更などが含まれます。
- 可能です "クラスタレベルのバックアップの設定を管理します"。これには、バックアップをオブジェクト

ストレージにアップロードするためのネットワーク帯域幅の変更、将来のボリュームに対する自動バックアップ設定の変更などが含まれます。

- また可能です "ボリューム、フォルダ、または個々のファイルをバックアップファイルからリストアする" オンプレミスのONTAP システムへの移行をサポート

ONTAPシステムのバックアップを管理します

Cloud Volumes ONTAPシステムとオンプレミスのONTAPシステムのバックアップを管理するには、バックアップスケジュールの変更、ボリュームバックアップの有効化/無効化、バックアップの一時停止、バックアップの削除などを行います。これには、Snapshotコピー、レプリケートされたボリューム、オブジェクトストレージ内のバックアップファイルなど、すべてのタイプのバックアップが含まれます。

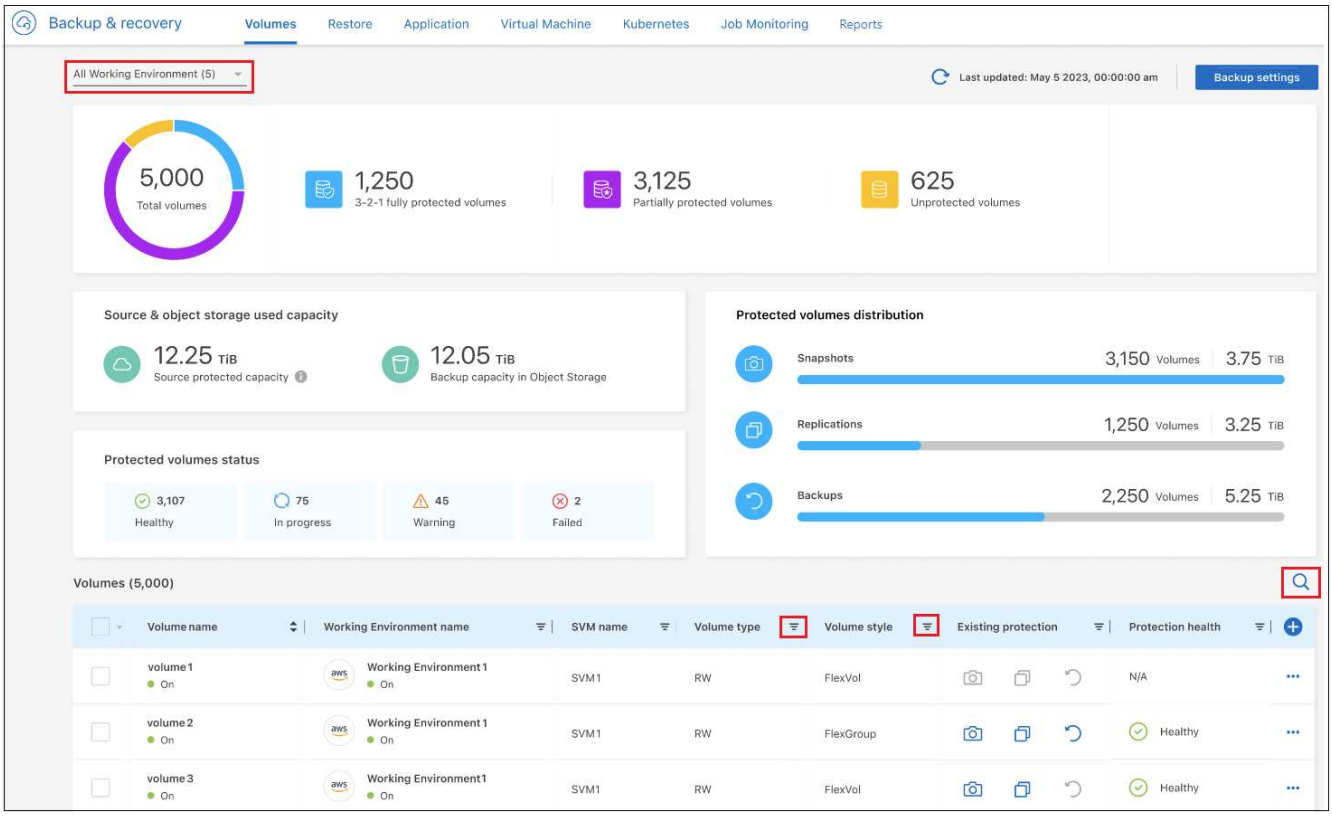
> ストレージシステム上で直接、またはクラウドプロバイダ環境からバックアップファイルを管理または変更しないでください。ファイルが破損し、サポートされていない構成になる可能性があります。

作業環境内のボリュームのバックアップステータスを表示します

[Volumes Backup]ダッシュボードでは、現在バックアップされているすべてのボリュームのリストを確認できます。これには、Snapshotコピー、レプリケートされたボリューム、オブジェクトストレージ内のバックアップファイルなど、すべてのタイプのバックアップが含まれます。現在バックアップされていない作業環境内のボリュームを表示することもできます。

手順

1. BlueXPメニューから、*Protection > Backup and recovery*を選択します。
2. [ボリューム]*タブをクリックして、Cloud Volumes ONTAPおよびオンプレミスのONTAPシステムのバックアップボリュームのリストを表示します。



3. 特定の作業環境で特定のボリュームを検索する場合は、作業環境とボリュームに基づいてリストを絞り込むことができます。検索フィルタを使用することも、ボリュームの形式（FlexVolまたはFlexGroup）やボリュームタイプなどに基づいて列をソートすることもできます。

   追加の列（アグリゲート、セキュリティ形式（WindowsまたはUNIX）、Snapshotポリシー、レプリケーションポリシー、およびバックアップポリシー）を表示するには、を選択します ⊕。

4. [Existing protection]列の保護オプションのステータスを確認します。3つのアイコンは、[Local Snapshot Copies]、[Replicated Volumes]、および[Backups in object storage]を表します。

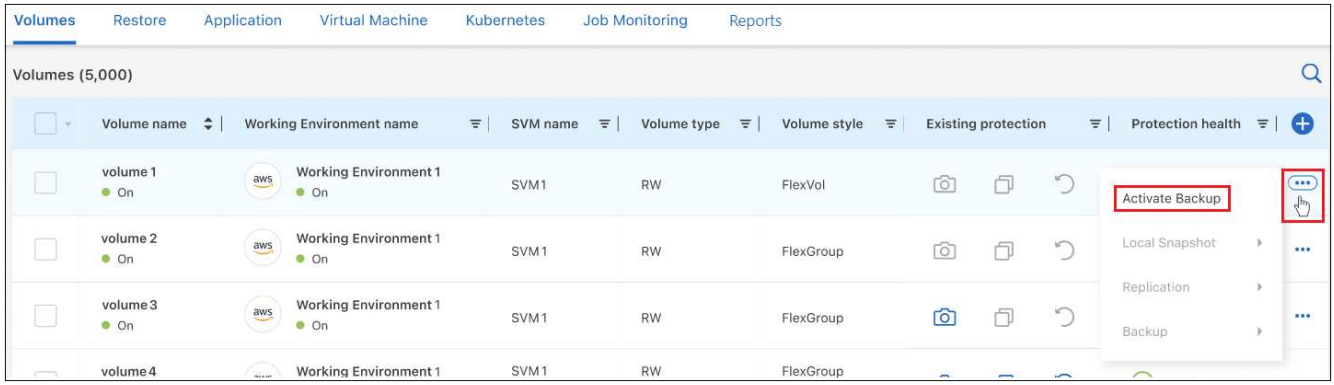
   各アイコンは、バックアップタイプがアクティブになっているときは青で、非アクティブになっているときはグレーで表示されます。各アイコンにカーソルを合わせると、使用されているバックアップポリシーや、各バックアップタイプのその他の関連情報を確認できます。

作業環境内の追加ボリュームでバックアップをアクティブ化します

BlueXPのバックアップとリカバリを初めて有効にしたときに作業環境内の一部のボリュームでのみバックアップをアクティブ化した場合は、あとで追加のボリュームのバックアップをアクティブ化できます。

手順

1. タブで、バックアップをアクティブ化するボリュームを指定し、**[操作]**メニューを選択します ••• 行の最後にある[バックアップのアクティブ化]*を選択します。



2. [*define backup strategy*]ページで、バックアップアーキテクチャを選択し、ローカルSnapshotコピー、レプリケートされたボリューム、バックアップファイルのポリシーとその他の詳細を定義します。この作業環境でアクティブ化した初期ボリュームのバックアップオプションの詳細については、を参照してください。次に、 [* 次へ *] をクリックします。
3. このボリュームのバックアップ設定を確認し、*[バックアップのアクティブ化]*をクリックします。

同一のバックアップ設定で複数のボリュームのバックアップを同時にアクティブ化する場合は、を参照してください 複数のボリュームのバックアップ設定を編集します を参照してください。

既存のボリュームに割り当てられているバックアップ設定を変更します

ポリシーが割り当てられている既存のボリュームに割り当てられているバックアップポリシーを変更することができます。ローカルSnapshotコピー、レプリケートされたボリューム、およびバックアップファイルのポリシーを変更できます。ボリュームに適用する新しいSnapshot、レプリケーション、またはバックアップポリシーがすでに存在している必要があります。

単一のボリュームのバックアップ設定を編集します

手順

1. タブで、ポリシーを変更するボリュームを特定し、**[操作]**メニューを選択します ••• 行の末尾に移動し、[バックアップ戦略の編集]*を選択します。

ボタンのスクリーンショット。"]

2. [バックアップ戦略の編集]ページで、ローカルSnapshotコピー、レプリケートされたボリューム、およびバックアップファイルの既存のバックアップポリシーを変更し、*[次へ]*をクリックします。

   このクラスタでBlueXPのバックアップとリカバリをアクティブ化するときに、初期バックアップポリシー

で_DataLockとRansomware Protection_forクラウドバックアップを有効にした場合は、DataLockで設定されている他のポリシーのみが表示されます。BlueXPのバックアップとリカバリをアクティブ化するときに_DataLockとRansomware Protection _を有効にしなかった場合は、DataLockが設定されていない他のクラウドバックアップポリシーのみが表示されます。

3. このボリュームのバックアップ設定を確認し、*[バックアップのアクティブ化]*をクリックします。

複数のボリュームのバックアップ設定を編集します

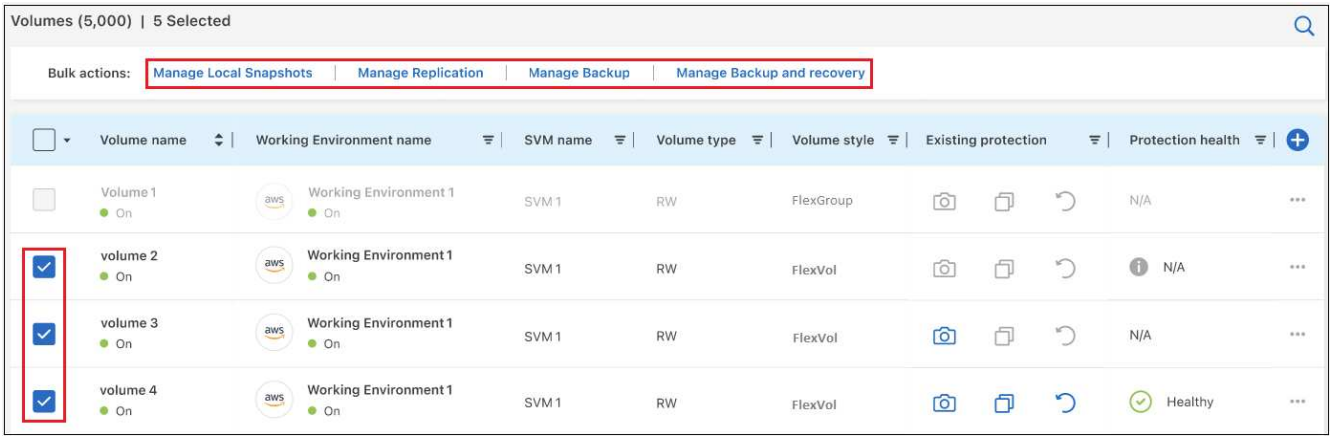
複数のボリュームで同じバックアップ設定を使用する場合は、複数のボリュームのバックアップ設定を同時にアクティブ化または編集できます。バックアップ設定がないボリューム、Snapshot設定のみ、クラウドへのバックアップ設定のみなどを選択し、さまざまなバックアップ設定を使用して、これらすべてのボリュームで一括変更を行うことができます。

複数のボリュームを使用する場合は、すべてのボリュームに次の共通の特性が必要です。

- 同じ作業環境
- 同じ形式（FlexVolまたはFlexGroupボリューム）
- 同じタイプ（読み書き可能またはデータ保護ボリューム）

手順

1. [ボリューム]*タブで、ボリュームが配置されている作業環境でフィルタします。
2. バックアップ設定を管理するすべてのボリュームを選択します。
3. 設定するバックアップアクションのタイプに応じて、[Bulk actions]メニューのボタンをクリックします。



ボタンのスクリーンショット。"]

バックアップ操作...	クリックするボタン
Snapshotバックアップの設定を管理します	ローカルスナップショットの管理
レプリケーションバックアップの設定を管理します	レプリケーションの管理
クラウドへのバックアップの設定を管理します	バックアップの管理
複数のタイプのバックアップ設定を管理します。このオプションでは、バックアップアーキテクチャも変更できます。	バックアップとリカバリの管理

4. 表示されたバックアップのページで、ローカルSnapshotコピー、レプリケートされたボリューム、またはバックアップファイルの既存のバックアップポリシーを変更し、*[保存]*をクリックします。

このクラスタでBlueXPのバックアップとリカバリをアクティブ化するときに、初期バックアップポリシーで_DataLockとRansomware Protection_forクラウドバックアップを有効にした場合は、DataLockで設定されている他のポリシーのみが表示されます。BlueXPのバックアップとリカバリをアクティブ化するときに_DataLockとRansomware Protection _を有効にしなかった場合は、DataLockが設定されていない他のクラウドバックアップポリシーのみが表示されます。

ボリュームの手動バックアップはいつでも作成できます

オンデマンドバックアップはいつでも作成することができ、ボリュームの現在の状態をキャプチャすることができます。これは、ボリュームに非常に重要な変更が加えられていて、そのデータを保護するために次回のスケジュールされたバックアップを待つ必要がない場合に便利です。また、この機能を使用して、現在バックアップされていないボリュームのバックアップを作成し、現在の状態をキャプチャすることもできます。

ボリュームのオブジェクトに対する一時的なSnapshotコピーまたはバックアップを作成できます。アドホックレプリケーションボリュームは作成できません。

バックアップ名にはタイムスタンプが含まれるため、他のスケジュールされたバックアップからオンデマンドバックアップを特定できます。

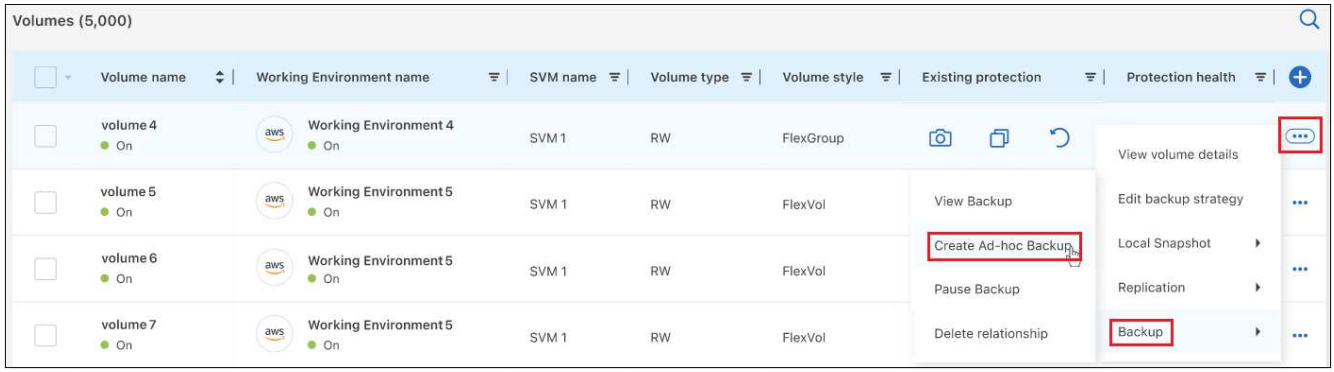
このクラスタでBlueXPのバックアップとリカバリをアクティブ化するときに_DataLockとRansomware Protection_を有効にした場合、オンデマンドバックアップにもDataLockが設定され、保持期間は30日になります。ランサムウェアスキャンはアドホックバックアップではサポートされていません。 "DataLockとランサムウェアによる保護の詳細をご確認ください"。

アドホックバックアップを作成する場合、ソースボリューム上にSnapshotが作成されることに注意してください。このSnapshotは通常のSnapshotスケジュールの一部ではないため、offのままになりません。バックアップの完了後に、このSnapshotをソースボリュームから手動で削除できます。これにより、このSnapshotに関連するブロックが解放されます。Snapshotの名前はで始まります `cbs-snapshot-adhoc-`。 "ONTAP CLIを使用してSnapshotを削除する方法を参照してください"。

オンデマンドボリュームバックアップは、データ保護ボリュームではサポートされません。

手順

1. [* Volumes （ボリューム）] タブで、をクリックします ••• アイコン"] ボリュームの*>[アドホックバックアップの作成]*を選択します。



ボタンのスクリーンショット。"]

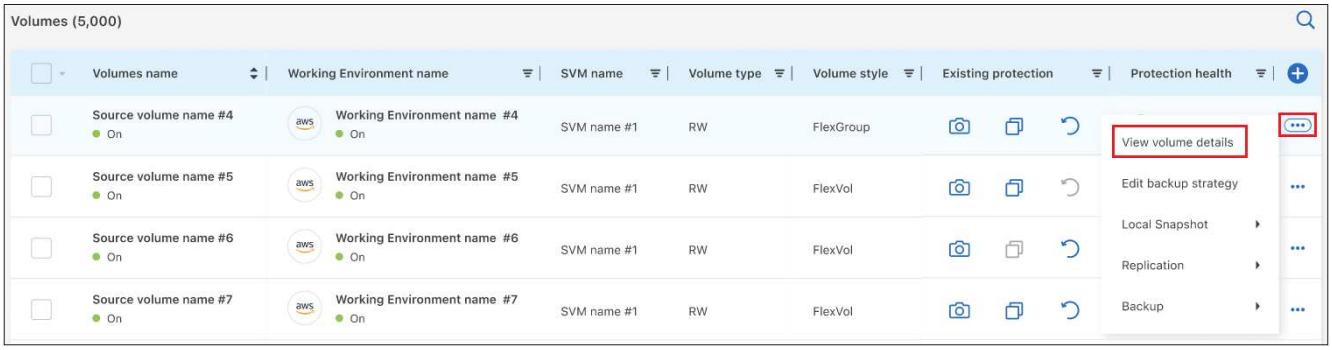
バックアップが作成されるまで、このボリュームの Backup Status 列には「 In Progress 」と表示されます。

各ボリュームのバックアップのリストを表示します

各ボリュームに存在するすべてのバックアップファイルのリストを表示できます。このページには、ソースボリューム、デスティネーションの場所、および前回作成されたバックアップの詳細、現在のバックアップポリシー、バックアップファイルのサイズなどのバックアップの詳細が表示されます。

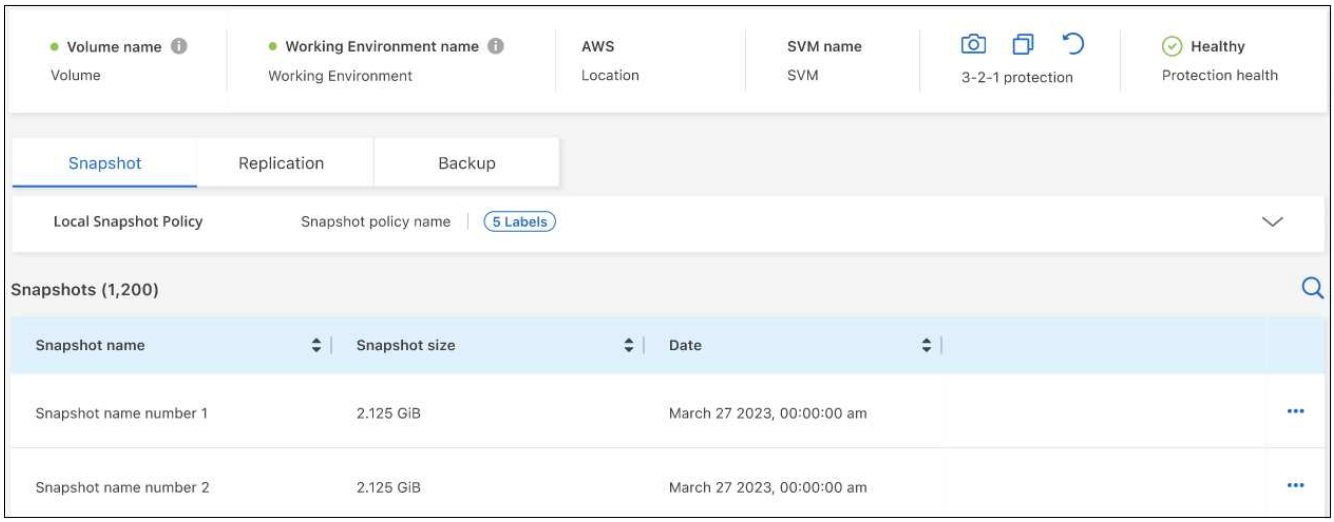
手順

1. [* Volumes （ボリューム）] タブで、をクリックします ••• アイコン"] を選択し、*[ボリュームの詳細を表示]*を選択します。



ボタンのスクリーンショット。"]

デフォルトでは、ボリュームの詳細とSnapshotコピーのリストが表示されます。



2. 、[Replication]、または[Backup]*を選択すると、各バックアップタイプのすべてのバックアップファイルのリストが表示されます。

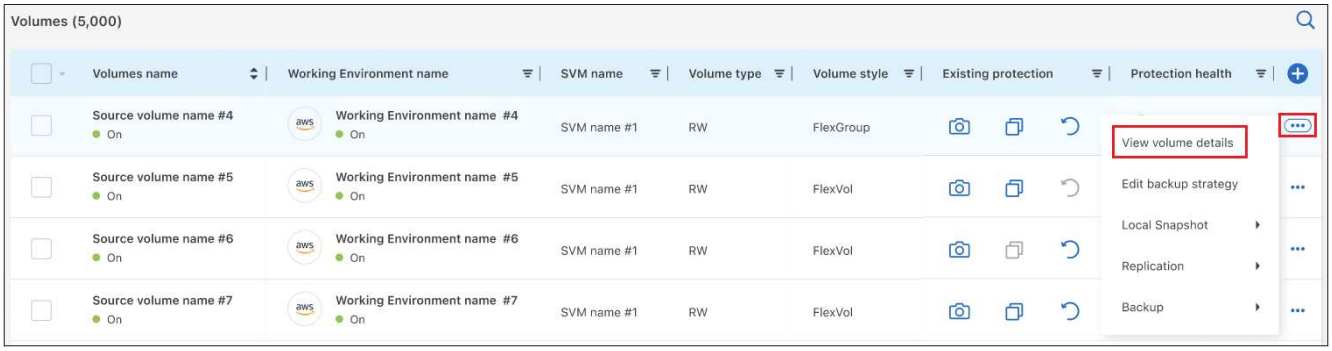
オブジェクトストレージ内のボリュームバックアップに対してランサムウェアスキャンを実行します

NetAppランサムウェア対策ソフトウェアは、バックアップファイルをスキャンして、オブジェクトファイルへのバックアップが作成されたときや、バックアップファイルのデータがリストアされたときに、ランサムウェア攻撃の証拠を探します。また、オンデマンドのランサムウェア対策スキャンをいつでも実行して、オブジェクトストレージ内の特定のバックアップファイルのユーザビリティを検証することもできます。これは、特定のボリュームでランサムウェア問題 が実行されている場合に、そのボリュームのバックアップが影響を受けないことを確認するのに役立ちます。

この機能は、ボリュームのバックアップがONTAP 9.11.1以降のシステムから作成された場合、およびオブジェクトへのバックアップポリシーで_DataLockとRansomware Protection_を有効にした場合にのみ使用できます。

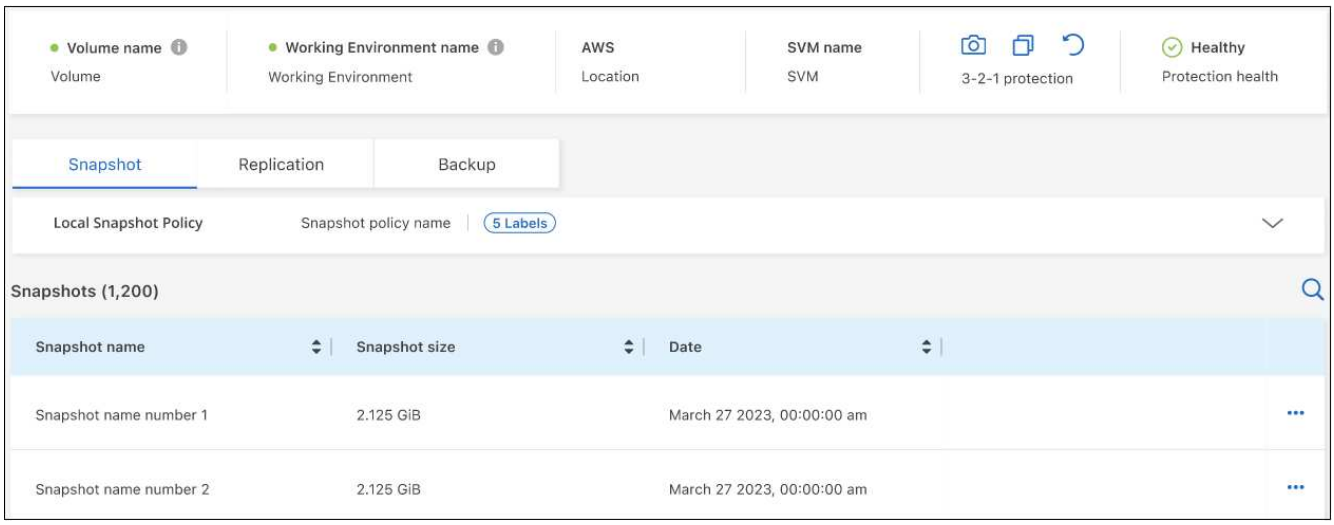
手順

1. [* Volumes （ボリューム）] タブで、をクリックします ••• アイコン"] を選択し、*[ボリュームの詳細を表示]*を選択します。



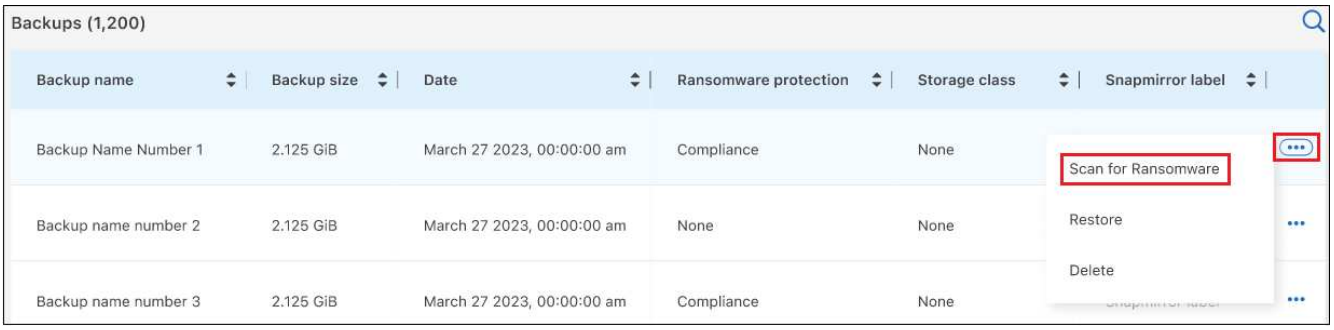
ボタンのスクリーンショット。"]

ボリュームの詳細が表示されます。



2. [バックアップ]*を選択すると、オブジェクトストレージ内のバックアップファイルのリストが表示されます。

3. をクリックします ••• アイコン"] ランサムウェアをスキャンするボリュームバックアップファイルの*[ランサムウェアをスキャン]*をクリックします。



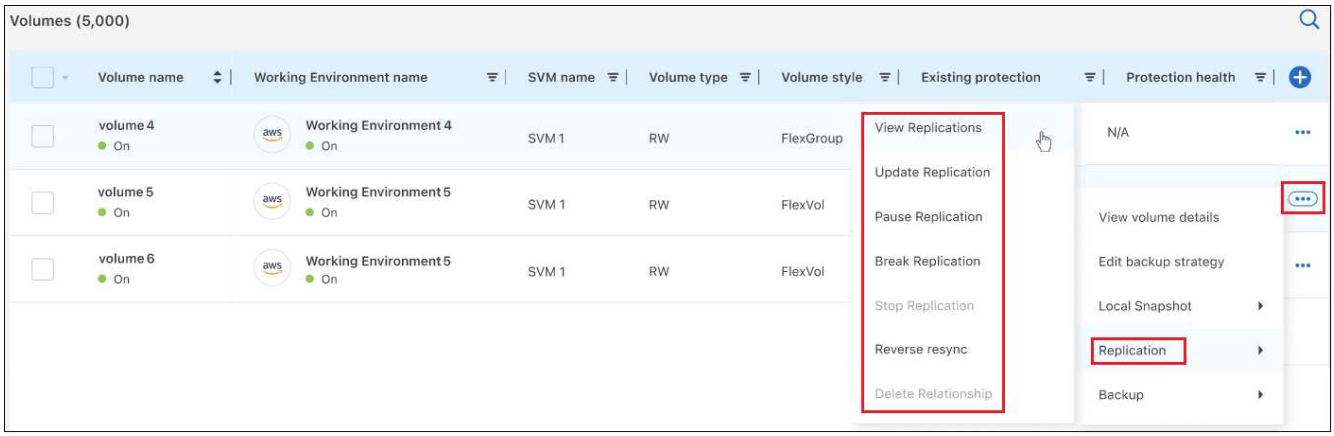
[Ransomware Protection]列には、スキャンが実行中であることが表示されます。

ソースボリュームとのレプリケーション関係を管理します

2つのシステム間にデータレプリケーションを設定したら、データレプリケーション関係を管理できます。

手順

1. [* Volumes （ボリューム）] タブで、をクリックします ••• アイコン"] をクリックし、*[レプリケーション]*オプションを選択します。使用可能なすべてのオプションが表示されます。
2. 実行するレプリケーションアクションを選択します。



アクションメニューで実行できる操作のリストを示すスクリーンショット。"]

次の表に、使用可能なアクションを示します。

アクション	説明
レプリケーションを表示します	ボリューム関係に関する詳細が表示されます。これには、転送情報、前回の転送情報、ボリュームに関する詳細、関係に割り当てられている保護ポリシーに関する情報が含まれます。
レプリケーションを更新します	差分転送を開始して、ソースボリュームと同期するデスティネーションボリュームを更新します。
レプリケーションの一時停止	デスティネーションボリュームを更新するには、Snapshotコピーの差分転送を一時停止します。増分更新を再開する場合は、後で再開できます。
レプリケーションを解除します	ソースボリュームとデスティネーションボリュームの間の関係を解除し、デスティネーションボリュームをデータアクセス用にアクティブ化します。これにより、ボリュームが読み取り/書き込み可能になります。 このオプションは通常、データの破損、偶発的な削除、オフライン状態などのイベントが原因でソースボリュームがデータを処理できない場合に使用します。 "ONTAP のドキュメントで、データアクセスのためのデスティネーションボリュームを設定し、ソースボリュームを再アクティブ化する方法について説明します"
レプリケーションを中止します	デスティネーションシステムへのこのボリュームのバックアップを無効にし、ボリュームのリストアも無効にします。既存のバックアップは削除されません。ソースボリュームとデスティネーションボリュームの間のデータ保護関係は削除されません。
リバース再同期	ソースボリュームとデスティネーションボリュームの役割を逆にします。元のソースボリュームの内容は、デスティネーションボリュームの内容によって上書きされます。これは、オフラインになったソースボリュームを再アクティブ化する場合に役立ちます。 前回のデータレプリケーションからソースボリュームが無効になったまでの間に元のソースボリュームに書き込まれたデータは保持されません。
関係の削除	ソースボリュームとデスティネーションボリューム間のデータ保護関係を削除します。つまり、ボリューム間でデータレプリケーションが行われなくなります。この処理では、デスティネーションボリュームはデータアクセス用にアクティブ化されません。つまり、デスティネーションボリュームは読み書き可能になりません。また、システム間に他のデータ保護関係がない場合は、クラスタピア関係と Storage VM （ SVM ）ピア関係も削除されます。

結果

操作を選択すると、関係がBlueXPによって更新されます。

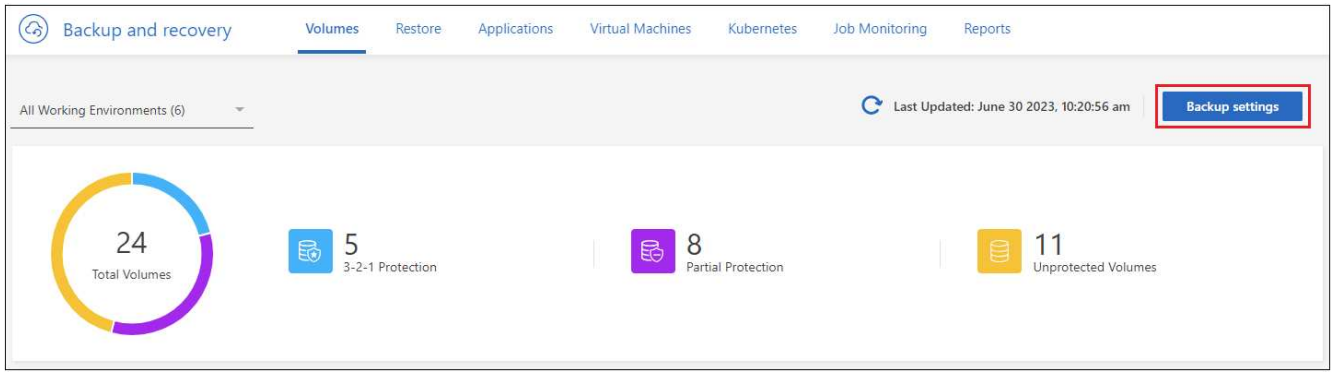
既存のクラウドバックアップポリシーを編集する

作業環境でボリュームに現在適用されているバックアップポリシーの属性を変更することができます。バックアップポリシーを変更すると、そのポリシーを使用している既存のすべてのボリュームが対象になります。

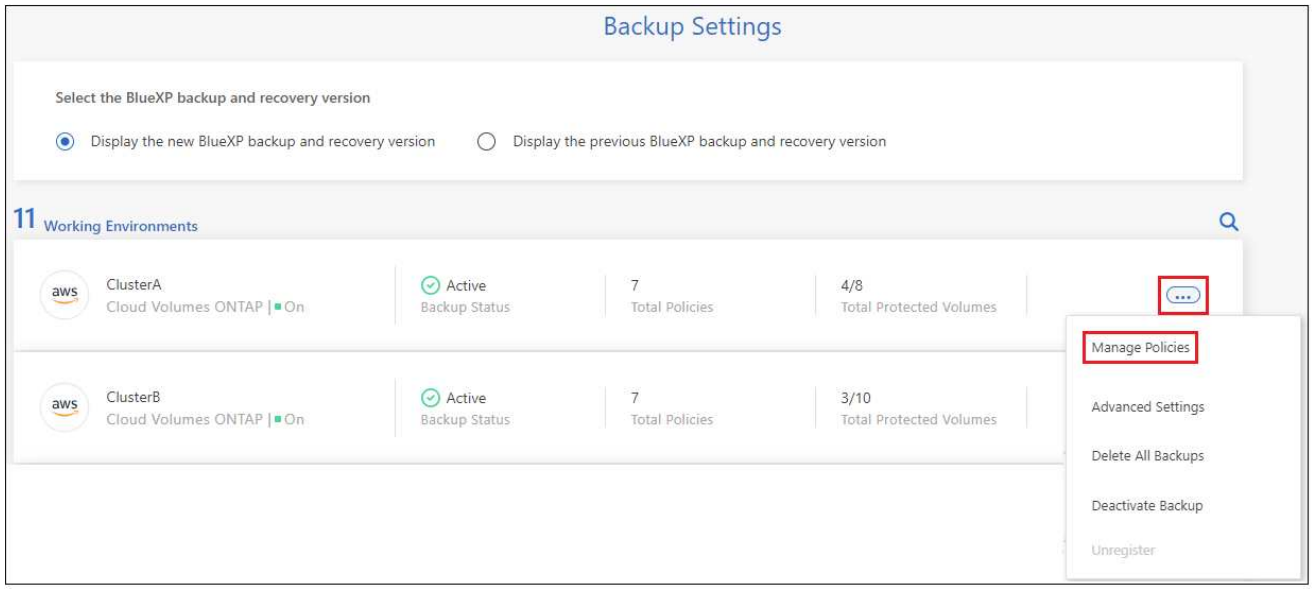
- このクラスタでBlueXPのバックアップとリカバリをアクティブ化するときに初期ポリシーで_DataLockとRansomware Protection_を有効にした場合は、編集するポリシーがすべて同じDataLock設定（ガバナンスまたはコンプライアンス）で構成されている必要があります。BlueXPのバックアップとリカバリをアクティブ化するときに_DataLockとRansomware Protection _を有効にしなかった場合は、ここでDataLockを有効にすることはできません。
- AWSでバックアップを作成するときに、BlueXPのバックアップとリカバリをアクティブ化するときに最初のバックアップポリシーで_S3 Glacier_or_S3 Glacier Deep Archive_を 選択した場合、バックアップポリシーの編集時に使用できる唯一のアーカイブ階層がその階層になります。最初のバックアップポリシーでアーカイブ階層を選択しなかった場合、ポリシーの編集時に_S3 Glacierが唯一のアーカイブオプションになります。

手順

1. [* Volumes （ボリューム）] タブで、 [* Backup Settings （バックアップ設定）] を選択します。

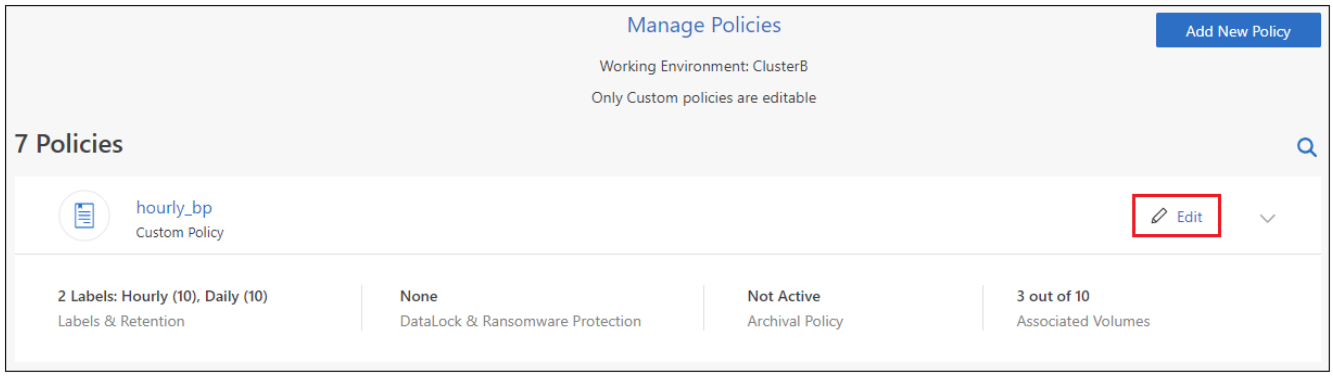


2. [Backup Settings_] ページで、をクリックします ••• アイコン"] ポリシー設定を変更する作業環境で、[ポリシーの管理]を選択します。

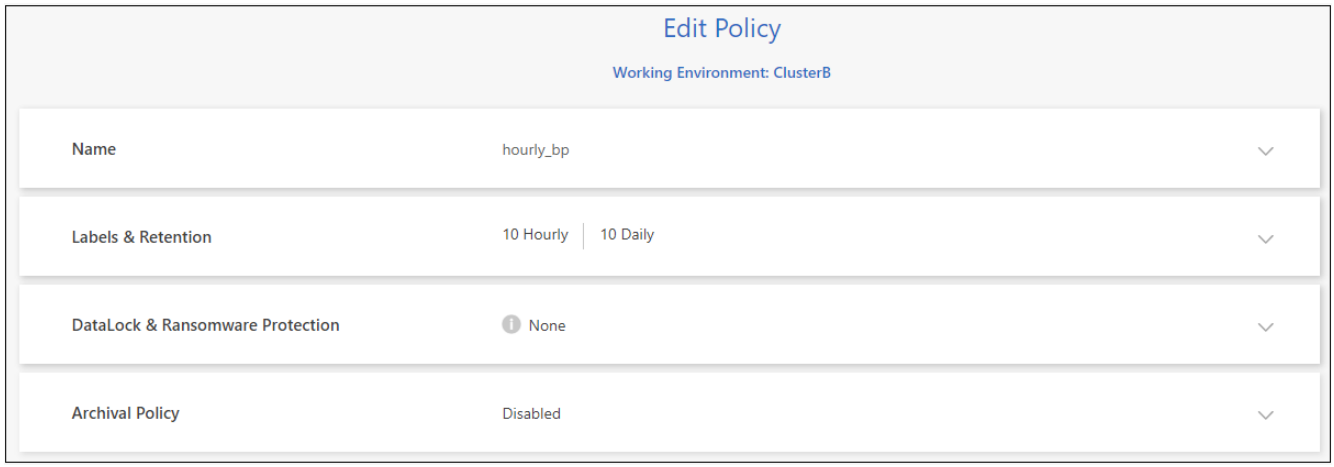


ページの [ポリシーの管理] オプションを示すスクリーンショット。"]

3. [ポリシーの管理]ページで、その作業環境で変更するバックアップポリシーの[編集]をクリックします。



4. [ポリシーの編集]ページで、をクリックします ⌄ [ラベルと保持期間]セクションを展開してスケジュールやバックアップの保持期間を変更するには'[保存]をクリックします



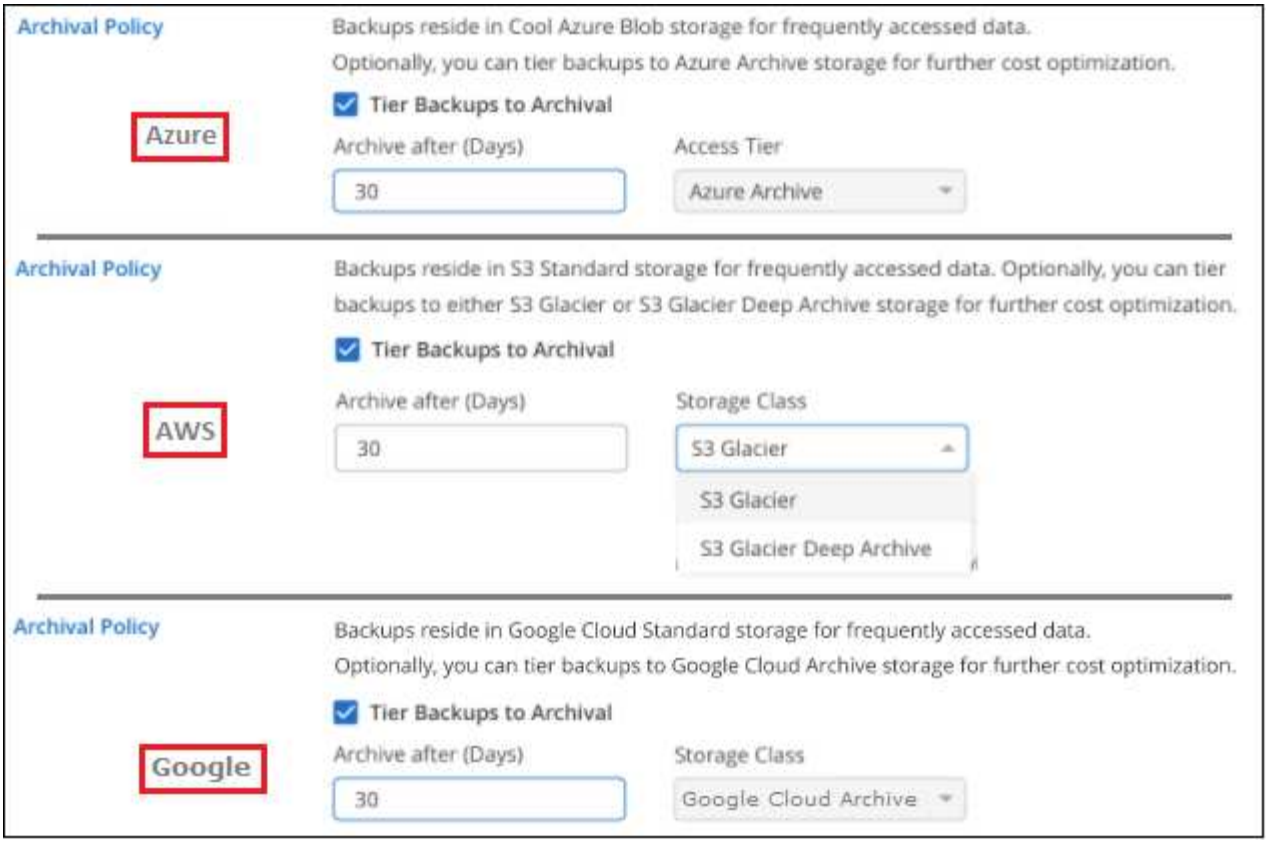
クラスタでONTAP 9.10.1以降が実行されている場合は、特定の日数が経過したバックアップをアーカイブストレージに階層化するかどうかを有効または無効にすることもできます。

"AWS アーカイブストレージの使用方法については、こちらをご覧ください"。

"Azure アーカイブストレージの使用方法については、こちらをご覧ください"。

"Googleアーカイブストレージの使用方法については、こちらをご覧ください"。（ONTAP 9.12.1が必要です）。

[+]



[+]
アーカイブへのバックアップの階層化を停止した場合、アーカイブストレージに階層化されたバックアップファイルはその階層に残ります。アーカイブされたバックアップファイルは自動的に標準階層に戻されません。新しいボリュームバックアップのみが標準階層に配置されます。

クラウドへの新しいバックアップポリシーを追加する

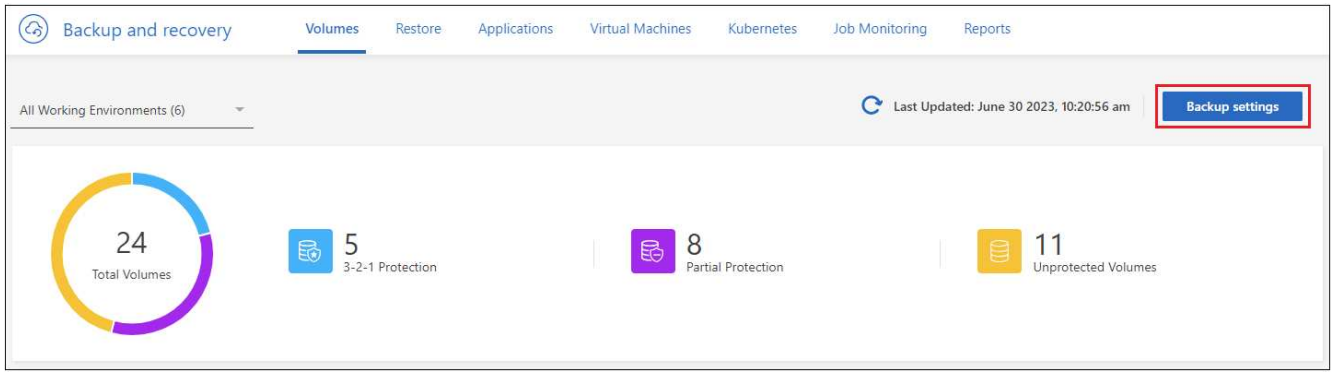
作業環境でBlueXPのバックアップとリカバリを有効にすると、最初に選択したすべてのボリュームが定義したデフォルトのバックアップポリシーを使用してバックアップされます。Recovery Point Objective （RPO；目標復旧時点）が異なるボリュームに対して異なるバックアップポリシーを割り当てる場合は、そのクラスタに追加のポリシーを作成し、そのポリシーを他のボリュームに割り当てることができます。

作業環境内の特定のボリュームに新しいバックアップポリシーを適用する場合は、最初にそのバックアップポリシーを作業環境に追加する必要があります。すると その作業環境内のボリュームにポリシーを適用します。

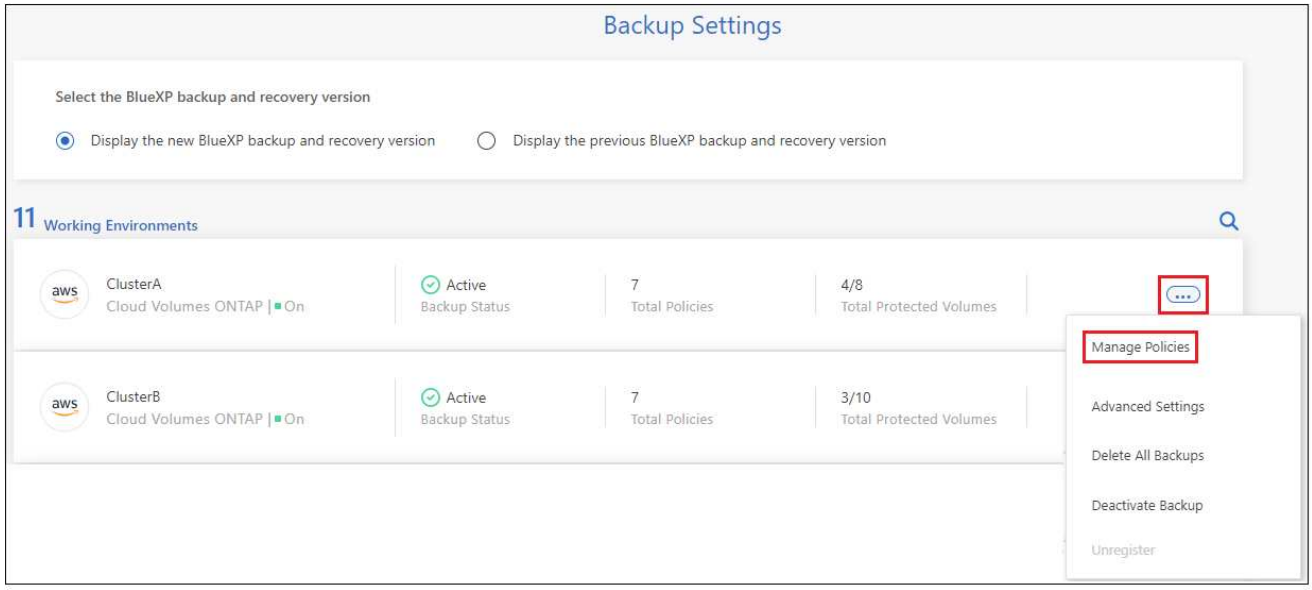
- このクラスタでBlueXPのバックアップとリカバリをアクティブ化するときに初期ポリシーで_DataLockとRansomware Protection_を有効にした場合は、追加のポリシーで同じDataLock設定（ガバナンスまたはコンプライアンス）を設定する必要があります。BlueXPのバックアップとリカバリをアクティブ化するときに_DataLockとRansomware Protection _を有効にしなかった場合は、DataLockを使用する新しいポリシーを作成できません。
- AWSでバックアップを作成するときに、BlueXPのバックアップとリカバリをアクティブ化するときに最初のバックアップポリシーで_S3 Glacier_or_S3 Glacier Deep Archive_を 選択した場合、その階層がそのクラスタの今後のバックアップポリシーで使用できる唯一のアーカイブ階層になります。最初のバックアップポリシーでアーカイブ階層を選択しなかった場合、以降のポリシーでは_S3 Glacierが唯一のアーカイブオプションになります。

手順

1. [* Volumes （ボリューム）] タブで、 [* Backup Settings （バックアップ設定）] を選択します。

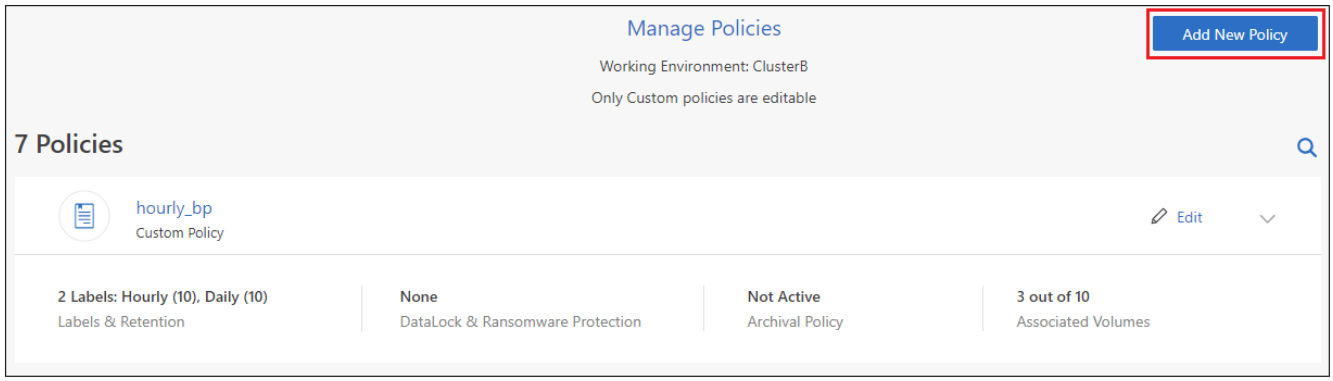


2. [Backup Settings_] ページで、をクリックします ••• アイコン"] 新しいポリシーを追加する作業環境で、 [ポリシーの管理] を選択します。



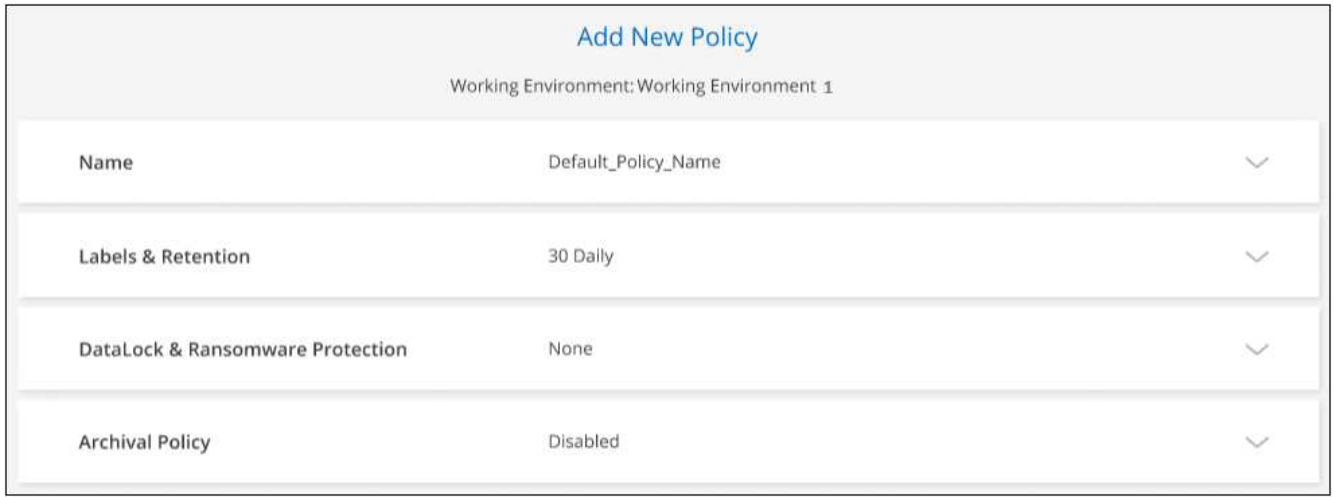
ページの [ポリシーの管理] オプションを示すスクリーンショット。"]

3. [ポリシーの管理] ページで、 [新しいポリシーの追加] をクリックします。



ページの [新しいポリシーの追加] ボタンを示すスクリーンショット。"]

4. [新しいポリシーの追加]ページで、をクリックします ⌄ [ラベルと保持期間]セクションを展開してスケジュールとバックアップの保持期間を定義するには'[保存]をクリックします



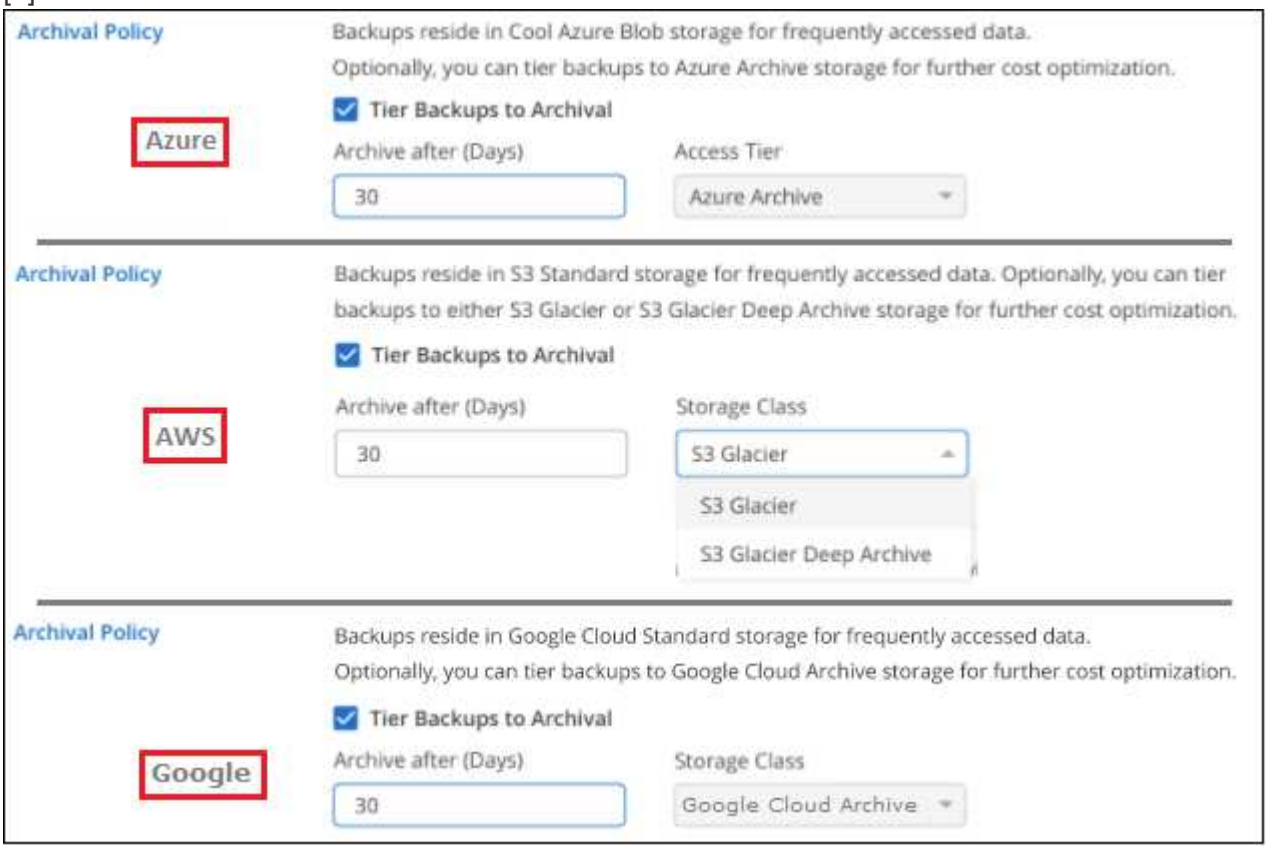
クラスタでONTAP 9.10.1以降が実行されている場合は、特定の日数が経過したバックアップをアーカイブストレージに階層化するかどうかを有効または無効にすることもできます。

"AWS アーカイブストレージの使用方法については、こちらをご覧ください"。

"Azure アーカイブストレージの使用方法については、こちらをご覧ください"。

"Googleアーカイブストレージの使用方法については、こちらをご覧ください"。（ONTAP 9.12.1が必要です）。

[+]



バックアップを削除します

BlueXPのバックアップとリカバリでは、1つのバックアップファイルを削除したり、ボリュームのすべてのバックアップを削除したり、作業環境内のすべてのボリュームのすべてのバックアップを削除したりできます。すべてのバックアップを削除するのは、不要になったバックアップや、ソースボリュームを削除したあとにすべてのバックアップを削除する場合などです。

DataLockとRansomwareによる保護を使用してロックしたバックアップファイルは削除できません。ロックされたバックアップファイルを1つ以上選択した場合、UIから[削除]オプションを使用できなくなります。

> バックアップがある作業環境またはクラスタを削除する場合は、システムを削除する前に * バックアップを削除する必要があります。システムを削除しても、BlueXPのバックアップとリカバリではバックアップは自動的に削除されません。また、システムの削除後にバックアップを削除する機能は現在UIでサポートされていません。残りのバックアップについては、引き続きオブジェクトストレージのコストが発生します。

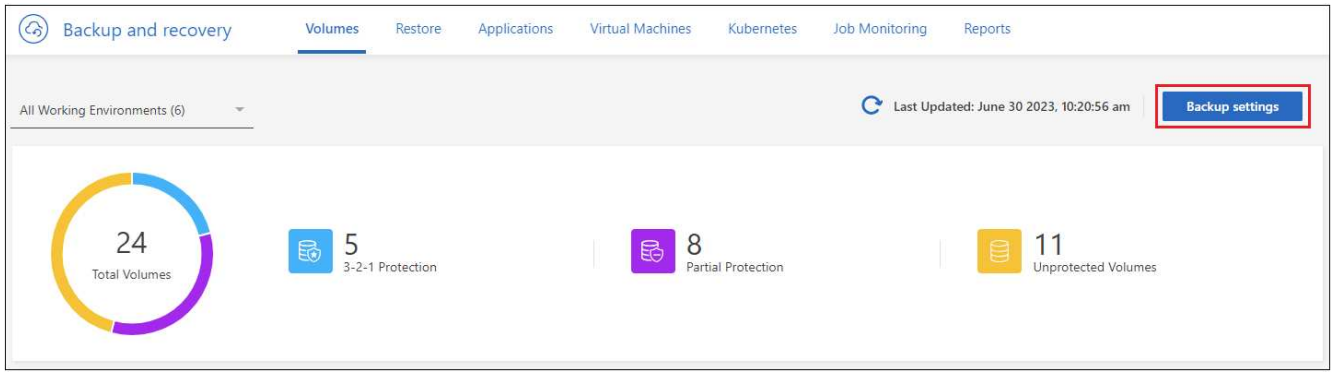
作業環境のすべてのバックアップファイルを削除します

作業環境のオブジェクトストレージ上のバックアップをすべて削除しても、この作業環境内のボリュームの以降のバックアップが無効になることはありません。作業環境ですべてのボリュームのバックアップの作成を停止するには、バックアップを非アクティブ化します ここで説明するようにします。

この処理は、Snapshotコピーやレプリケートされたボリュームには影響しません。これらのタイプのバックアップファイルは削除されません。

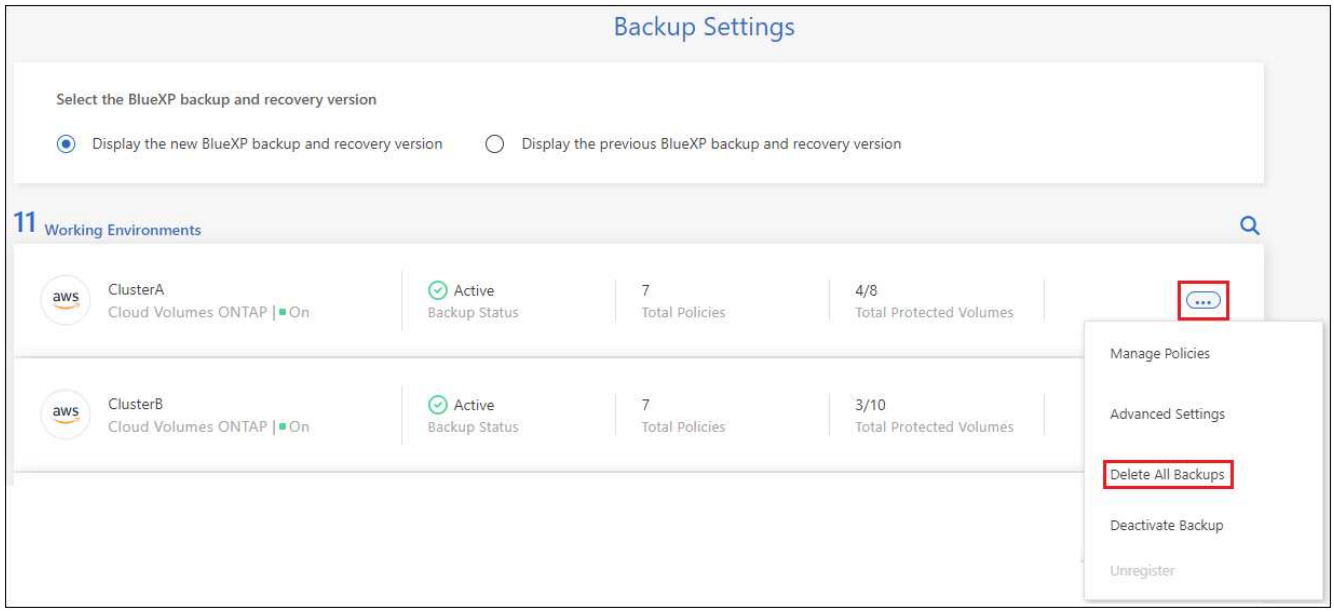
手順

1. [* Volumes （ボリューム）] タブで、 [* Backup Settings （バックアップ設定）] を選択します。



ボタンを示すスクリーンショット。"]

2. をクリックします ••• アイコン"] すべてのバックアップを削除する作業環境で、 * すべてのバックアップを削除 * を選択します。



ボタンを選択したスクリーンショット。"]

3. 確認ダイアログボックスで、作業環境の名前を入力し、 * 削除 * をクリックする。

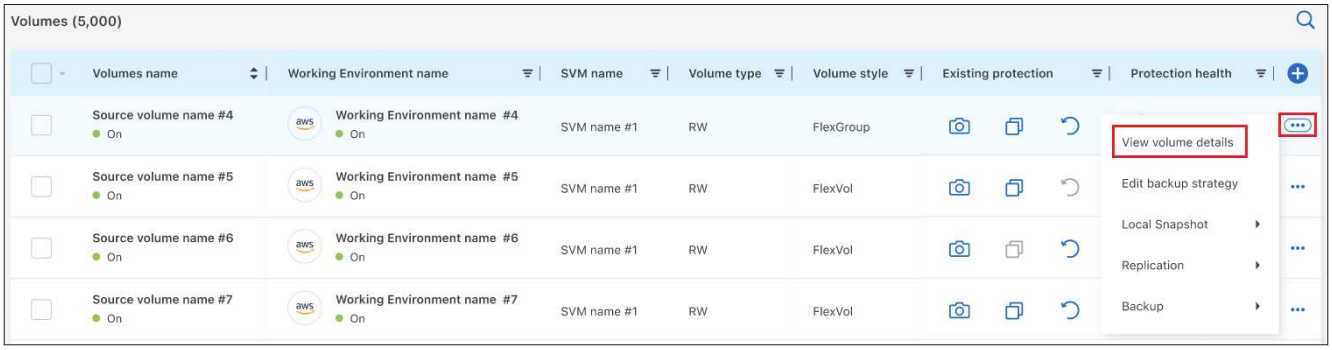
ボリュームのバックアップファイルを**1**つ削除します

不要になったバックアップファイルは1つだけ削除できます。これには、ボリュームのSnapshotコピーまたはオブジェクトストレージにあるバックアップの1つのバックアップが削除されます。

レプリケートされたボリューム（データ保護ボリューム）は削除できません。

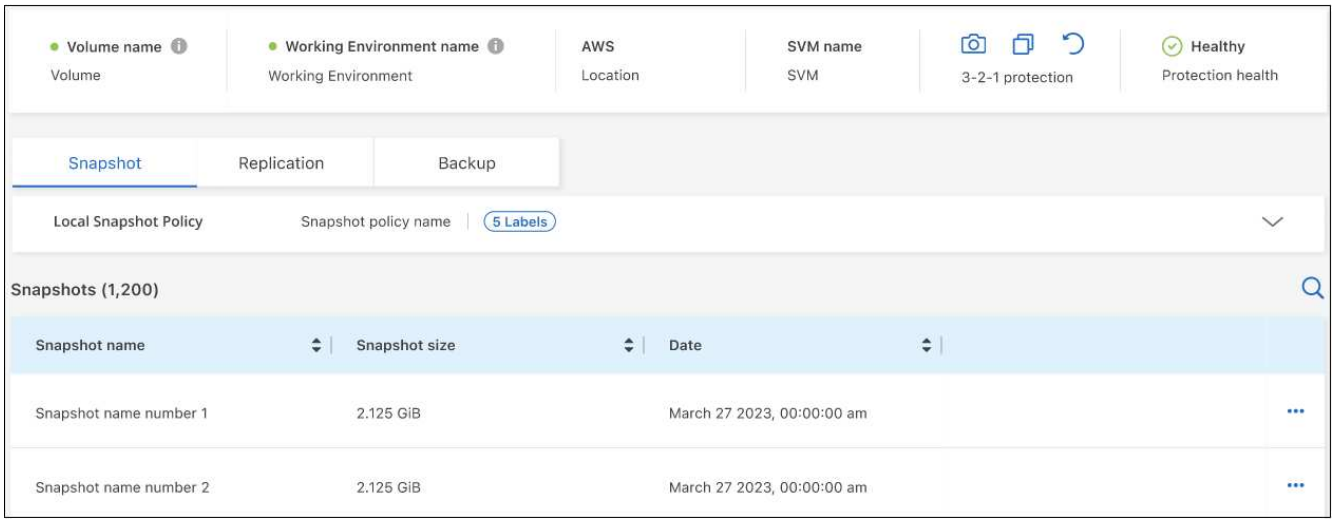
手順

1. [* Volumes （ボリューム）] タブで、をクリックします ••• アイコン"] を選択し、*[ボリュームの詳細を表示]*を選択します。



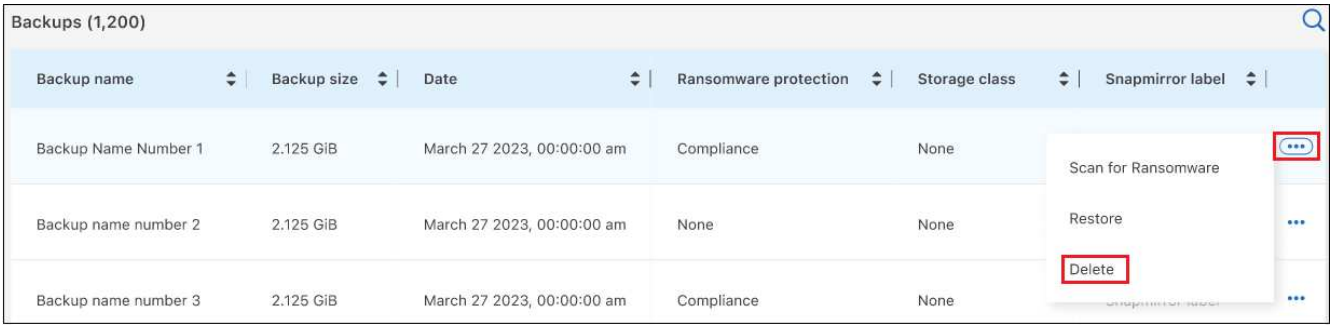
ボタンのスクリーンショット。"]

ボリュームの詳細が表示されます。* Snapshot 、 Replication 、または Backup *を選択すると、ボリュームのすべてのバックアップファイルのリストが表示されます。デフォルトでは、使用可能なSnapshotコピーが表示されます。



2. 削除するバックアップファイルのタイプを確認するには、* Snapshot または Backup *を選択します。

3. をクリックします ••• アイコン"] 削除するボリュームバックアップファイルに対して、 * 削除 * をクリックします。以下のスクリーンショットは、オブジェクトストレージ内のバックアップファイルからのものです。



4. 確認ダイアログボックスで、 * 削除 * をクリックします。

ボリュームのバックアップ関係を削除します

ボリュームのバックアップ関係を削除すると、新しいバックアップファイルの作成を中止してソースボリュームを削除し、既存のバックアップファイルはすべて保持する場合に、アーカイブのメカニズムを使用できます。これにより、必要に応じて、あとでソースストレージシステムからスペースを消去しながら、バックアップファイルからボリュームをリストアできるようになります。

ソースボリュームを削除する必要はありません。ボリュームのバックアップ関係を削除し、ソースボリュームを保持することができます。この場合、ボリュームのバックアップはあとで「アクティブ化」できます。この

場合も元のベースラインバックアップコピーが引き続き使用されます。新しいベースラインバックアップコピーは作成されず、クラウドにエクスポートされません。バックアップ関係を再アクティブ化すると、ボリュームにデフォルトのバックアップポリシーが割り当てられます。

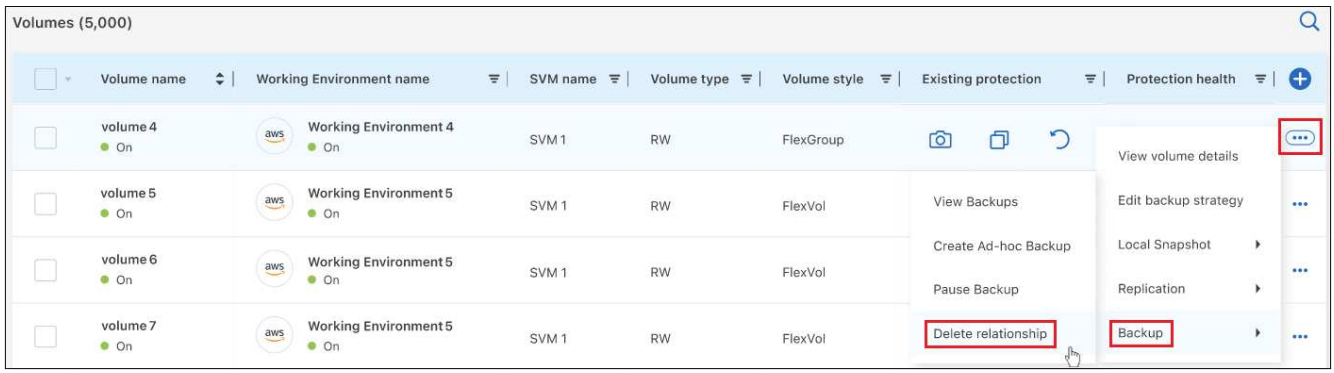
この機能は、システムでONTAP 9.12.1以降が実行されている場合にのみ使用できます。

BlueXPのバックアップとリカバリのユーザインターフェイスでソースボリュームを削除することはできません。ただし、Canvas、およびのVolume Detailsページを開くことはできます "そこからボリュームを削除します"。

> 関係を削除したあとでボリュームバックアップファイルを個別に削除することはできません。ただし、 "ボリュームのバックアップをすべて削除します" すべてのバックアップ・ファイルを削除する場合

手順

1. [* Volumes （ボリューム）] タブで、をクリックします ••• アイコン"] ソースボリュームの*>[関係の削除]* を選択します。



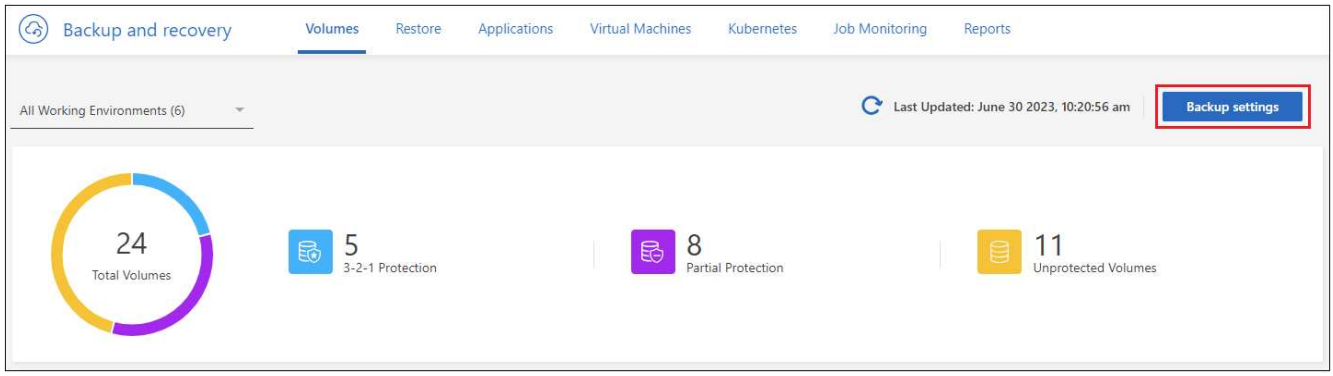
作業環境でBlueXPのバックアップとリカバリを非アクティブ化します

作業環境でBlueXPのバックアップとリカバリを無効にすると、システム上の各ボリュームのバックアップとボリュームのリストアも無効になります。既存のバックアップは削除されません。この作業環境からバックアップ・サービスの登録を解除することはありません。基本的には、すべてのバックアップおよびリストア処理を一定期間停止できます。

クラウドから引き続き課金されます が提供する容量のオブジェクトストレージコストのプロバイダ バックアップは自分以外で使用します バックアップを削除します。

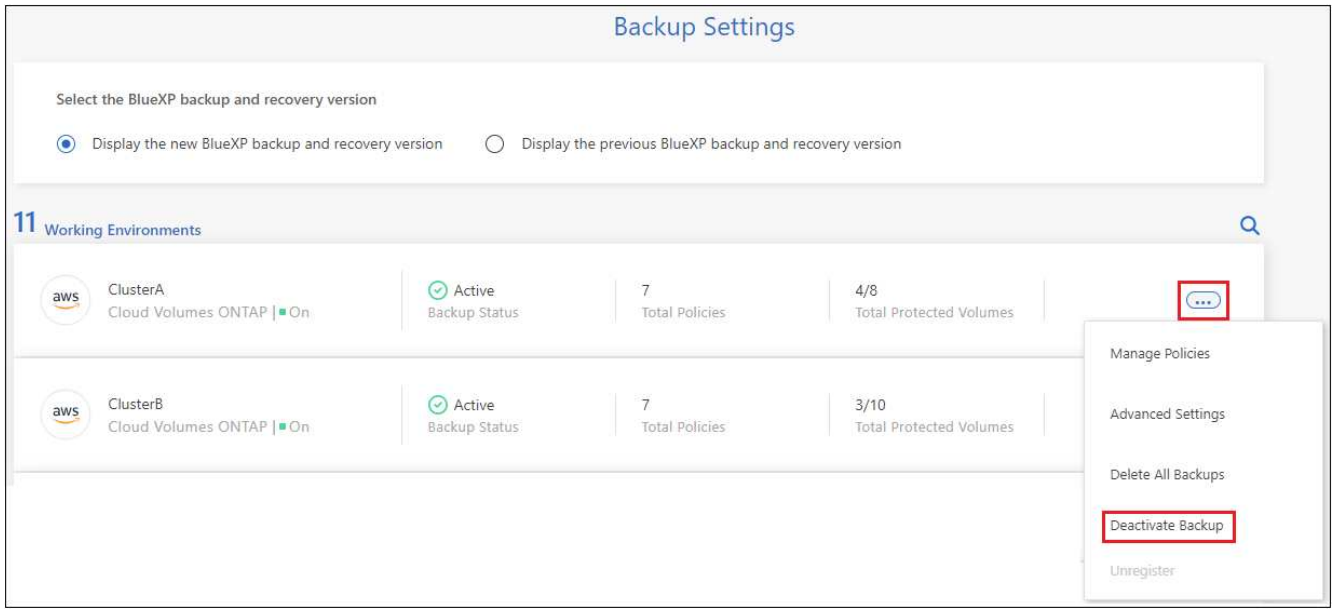
手順

1. [* Volumes （ボリューム）] タブで、 [* Backup Settings （バックアップ設定）] を選択します。



ボタンを示すスクリーンショット。"]

2. _ バックアップ設定ページ _ で、をクリックします ••• アイコン"] バックアップを無効にする作業環境で、 * バックアップを非アクティブ化 * を選択します。



3. 確認ダイアログボックスで、 * Deactivate * をクリックします。

> バックアップが無効になっている間は、その作業環境に対して * バックアップのアクティブ化 * ボタンが表示されます。このボタンは、作業環境でバックアップ機能を再度有効にする場合にクリックします。

作業環境のBlueXPバックアップとリカバリの登録を解除します

バックアップ機能の使用が不要になり、作業環境でのバックアップに対する課金を停止する場合は、作業環境のBlueXPバックアップ/リカバリの登録を解除できます。通常、この機能は、作業環境を削除する予定で、バックアップサービスをキャンセルする場合に使用します。

この機能は、クラスタバックアップの格納先のオブジェクトストアを変更する場合にも使用できます。作業環境のBlueXPバックアップ/リカバリの登録を解除したら、新しいクラウドプロバイダの情報を使用して、そのクラスタのBlueXPバックアップ/リカバリを有効にできます。

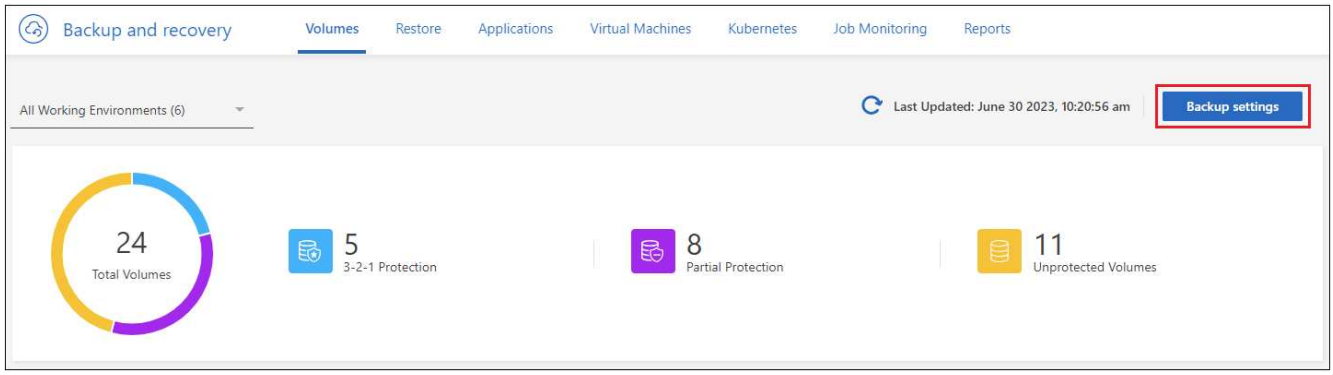
BlueXPのバックアップとリカバリの登録を解除する前に、次の手順をこの順序で実行する必要があります。

- 作業環境でBlueXPのバックアップとリカバリを非アクティブ化します
- その作業環境のバックアップをすべて削除します

登録解除オプションは、これら 2 つの操作が完了するまで使用できません。

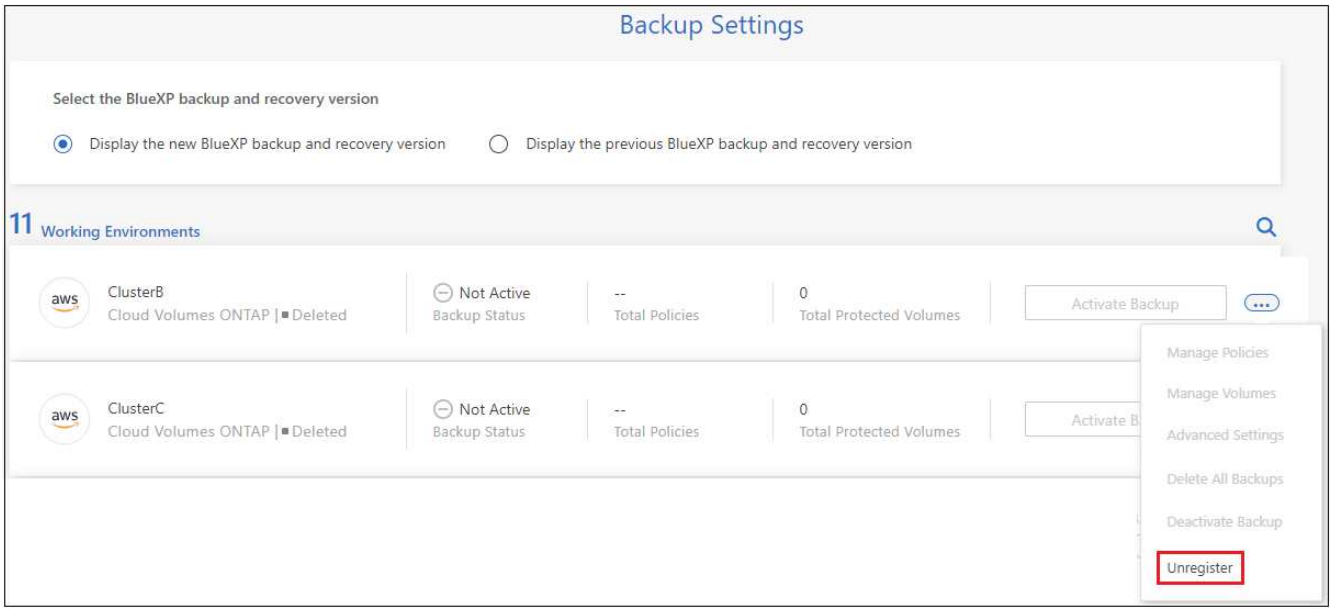
手順

1. [* Volumes （ボリューム）] タブで、 [* Backup Settings （バックアップ設定）] を選択します。



ボタンを示すスクリーンショット。"]

2. _ バックアップ設定ページ _ で、をクリックします ••• アイコン"] バックアップ・サービスの登録を解除する作業環境では、 * 登録解除 * を選択します。



3. 確認ダイアログボックスで、 * 登録解除 * をクリックします。

バックアップファイルから**ONTAP**データを復元します

ONTAPボリュームのデータは、バックアップを作成した場所（Snapshotコピー、レプリケートされたボリューム、オブジェクトストレージに格納されたバックアップ）からバックアップできます。これらのバックアップ先から特定の時点のデータをリストアできます。ONTAPボリューム全体をバックアップファイルからリストアすることも、少数の

ファイルのみをリストアする必要がある場合は、フォルダまたは個 々 のファイルをリストアすることもできます。

- 元の作業環境、同じクラウドアカウントを使用している別の作業環境、またはオンプレミスの ONTAP システムに * ボリューム * を（新しいボリュームとして）リストアできます。
- *フォルダ*を元の作業環境内のボリューム、同じクラウドアカウントを使用している別の作業環境内のボリューム、またはオンプレミスのONTAP システム上のボリュームにリストアできます。
- * files * は、元の作業環境内のボリューム、同じクラウドアカウントを使用している別の作業環境内のボリューム、またはオンプレミスの ONTAP システム上のボリュームにリストアできます。

バックアップファイルから本番環境のシステムにデータをリストアするには、有効なBlueXPバックアップ/リカバリライセンスが必要です。

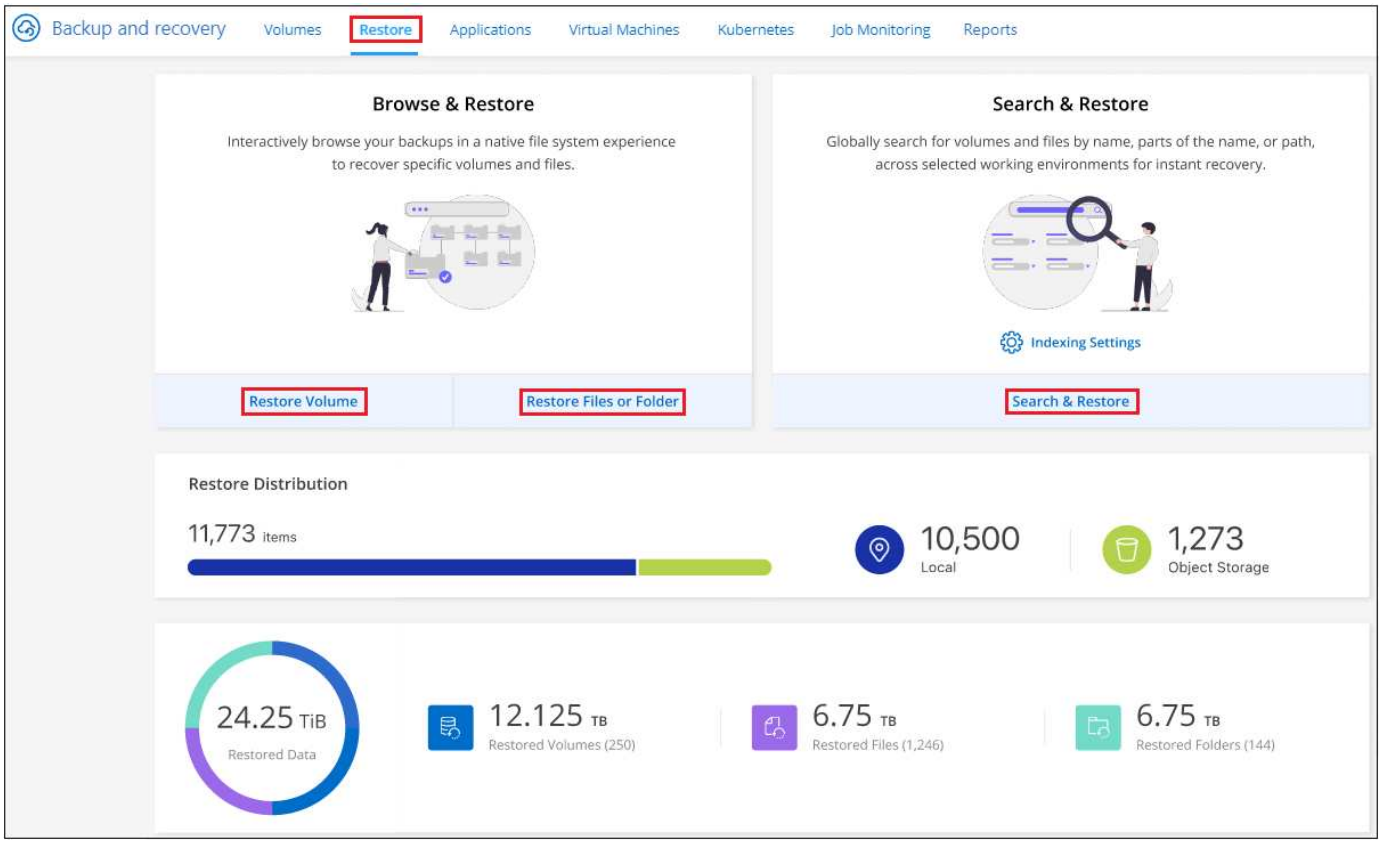
要約すると、ボリュームデータをONTAP作業環境にリストアするために使用できる有効なフローは次のとおりです。

- バックアップファイル→リストアされたボリューム
- レプリケートされたボリューム→リストアされたボリューム
- Snapshotコピー→リストアされたボリューム

リストアダッシュボード

リストアダッシュボードを使用して、ボリューム、フォルダ、およびファイルのリストア処理を実行できます。復元ダッシュボードにアクセスするには、BlueXPメニューの「バックアップと復元」をクリックし、次に「復元」タブをクリックします。をクリックすることもできます ボタン"] >*サービス・パネルからバックアップ/リカバリ・サービスのリストア・ダッシュボード*を表示します

> 少なくとも1つの作業環境でBlueXPのバックアップとリカバリをアクティブ化し、初期のバックアップファイルが存在している必要があります。



ダッシュボードには、[参照とリストア]または[検索とリストア]機能を使用するためのオプションが表示されます。"]

ご覧のように、リストアダッシュボードでは、 * 参照と復元 * と * 検索と復元 * の 2 つの異なる方法でバックアップファイルからデータを復元できます。

参照と復元と検索と復元を比較します

一般的に、先週または月から特定のボリューム、フォルダ、またはファイルを復元する必要がある場合には、*Browse &Restore*(参照と復元)を使用してください。また、ファイルの名前と場所、およびファイルが正常な状態で最後に作成された日付を確認できます。_検索と復元_は、通常、ボリューム、フォルダ、またはファイルを復元する必要があるときに適していますが、正確な名前、保存されているボリューム、または最後に良好な状態になった日付は覚えていません。

次の表に、2つの方法の機能比較を示します。

参照と復元	検索とリストア
フォルダ形式の構造を参照して、単一のバックアップファイル内のボリューム、フォルダ、またはファイルを検索します。	部分的または完全なボリューム名、部分的または完全なフォルダ/ファイル名、サイズ範囲、および追加の検索フィルタを使用して、*すべてのバックアップファイル*のボリューム、フォルダ、またはファイルを検索します。
ファイルが削除または名前変更されており、元のファイル名がわからない場合は、はファイルリカバリを処理しません	新しく作成 / 削除 / 名前変更されたディレクトリと新しく作成 / 削除 / 名前変更されたファイルを処理します

参照と復元	検索とリストア
クラウドプロバイダのリソースを追加する必要はありません	クラウドからリストアする場合は、アカウントごとにバケットとパブリッククラウドプロバイダのリソースが追加で必要になります。
クラウドプロバイダのコストを追加する必要はありません	クラウドからリストアする場合は、バックアップやボリュームをスキャンして検索結果を検索する際に追加コストが必要になります。
クイックリストアがサポートされています。	クイックリストアはサポートされていません。

この表には、バックアップファイルが配置されている場所に基づいて、有効なリストア処理のリストが表示されます。

バックアップタイプ	参照と復元			検索とリストア		
	ボリュームのリストア	ファイルの復元	フォルダの復元	ボリュームのリストア	ファイルの復元	フォルダの復元
Snapshot コピー	はい。	いいえ	いいえ	はい。	はい。	はい。
レプリケートされたボリューム	はい。	いいえ	いいえ	はい。	はい。	はい。
バックアップファイル	はい。	はい。	はい。	はい。	はい。	はい。

いずれかのリストア方式を使用する前に、固有のリソース要件に対応するように環境を設定しておく必要があります。これらの要件については、以降のセクションで説明します。

使用するリストア処理のタイプに応じた要件とリストア手順を確認します。

- 参照とリストアを使用したボリュームのリストア
- 参照と復元を使用したフォルダとファイルの復元
- 検索と復元を使用したボリューム、フォルダ、ファイルの復元

[参照と復元]を使用して**ONTAP**データを復元します

ボリューム、フォルダ、またはファイルのリストアを開始する前に、リストアするボリュームの名前、作業環境の名前、ボリュームが配置されているSVM、およびリストア元のバックアップファイルのおおよその日付を確認しておく必要があります。ONTAPデータは、Snapshotコピー、レプリケートされたボリューム、またはオブジェクトストレージに格納されているバックアップからリストアできます。

*注：*リストアするデータを含むバックアップファイルがアーカイブクラウドストレージ（ONTAP 9.10.1以降）にある場合、リストア処理に時間がかかり、コストがかかります。また、デスティネーションクラスタでボリュームのリストアにはONTAP 9.10.1以降、ファイルのリストアには9.11.1、Google Archive and StorageGRID には9.12.1、フォルダのリストアには9.13.1も実行されている必要があります。

"AWS アーカイブストレージからのリストアの詳細については、こちらをご覧ください"。

"Azure アーカイブストレージからのリストアの詳細については、こちらをご覧ください"。

"Googleのアーカイブストレージからのリストアの詳細については、こちらをご覧ください"。

> AzureアーカイブストレージからStorageGRID システムにデータをリストアする場合、優先度「高」はサポートされません。

サポートされている作業環境とオブジェクトストレージプロバイダの参照とリストア

セカンダリ作業環境（レプリケートされたボリューム）またはオブジェクトストレージ（バックアップファイル）にあるバックアップファイルから、ONTAPデータを次の作業環境にリストアできます。Snapshotコピーはソースの作業環境に存在し、同じシステムにのみリストアできます。

*注：*ボリュームは任意のタイプのバックアップファイルからリストアできますが、フォルダまたは個 々 のファイルは、現時点ではオブジェクトストレージのバックアップファイルからのみリストアできます。

オブジェクトストアから（バックアップ）	プライマリ（スナップショット）から	セカンダリ・システムから（レプリケーション）	デスティネーションの作業環境へ ifdef：aws []
Amazon S3	AWS の Cloud Volumes ONTAP オンプレミスの ONTAP システム	AWS の Cloud Volumes ONTAP オンプレミスの ONTAP システム endif：：aws[] ifdef：Azure []	Azure Blob の略
Azure の Cloud Volumes ONTAP オンプレミスの ONTAP システム	Azure の Cloud Volumes ONTAP オンプレミスの ONTAP システム endif：：azure[] ifdef ::gcp[]	Google クラウドストレージ	Google の Cloud Volumes ONTAP オンプレミスの ONTAP システム
Google の Cloud Volumes ONTAP オンプレミスの ONTAP システム endif：GCP []	NetApp StorageGRID	オンプレミスの ONTAP システム	オンプレミスの ONTAP システム Cloud Volumes ONTAP
オンプレミスのONTAPシステムへ	ONTAP S3の略	オンプレミスの ONTAP システム	オンプレミスの ONTAP システム Cloud Volumes ONTAP

参照と復元の場合、コネクタは次の場所にインストールできます。

- Amazon S3の場合、ConnectorはAWSまたは自社運用のどちらにも導入できます
- Azure Blobの場合は、Azureまたは自社運用環境に導入できます
- Google Cloud Storageの場合、ConnectorをGoogle Cloud Platform VPCに導入する必要があります
- StorageGRID の場合は、インターネットアクセスを使用するかどうかに関係なく、コネクタを社内に導入する必要があります
- ONTAP S3の場合、コネクタは社内環境（インターネットアクセスの有無にかかわらず）またはクラウドプロバイダ環境に導入できます。

「オンプレミス ONTAP システム」とは、 FAS 、 AFF 、 ONTAP Select の各システムを指します。

> システムのONTAP バージョンが9.13.1より前の場合、バックアップファイルにDataLock & Ransomwareが設定されていると、フォルダやファイルを復元できません。この場合、バックアップファイルからボリューム全体をリストアし、必要なファイルにアクセスできます。

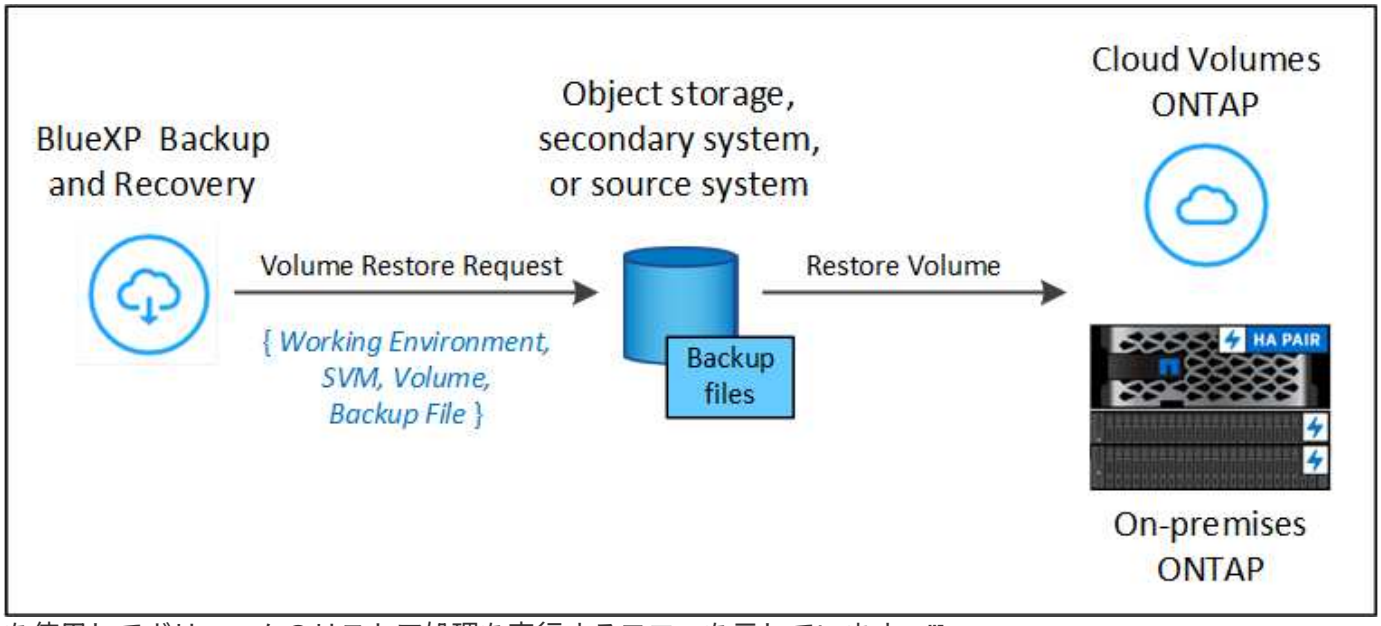
ブラウズおよびリストアを使用してボリュームをリストアします

バックアップファイルからボリュームをリストアすると、BlueXPのバックアップとリカバリでは、バックアップのデータを使用して_new_volumeが作成されます。オブジェクトストレージのバックアップを使用する場合は、元の作業環境内のボリューム、ソースの作業環境と同じクラウドアカウントにある別の作業環境、またはオンプレミスのONTAPシステムにデータをリストアできます。

ONTAP 9.13.0以降を使用してCloud Volumes ONTAPシステムにクラウドバックアップをリストアする場合、またはONTAP 9.14.1を実行しているオンプレミスのONTAPシステムにクラウドバックアップをリストアする場合は、_quick restore_operationを実行するオプションがあります。迅速なリストアは、ボリュームへのアクセスをできるだけ早く提供する必要があるディザスタリカバリ環境に最適です。クイックリストアでは、バックアップファイル全体をリストアするのではなく、バックアップファイルからボリュームにメタデータをリストアできます。高速リストアは、パフォーマンスやレイテンシの影響を受けやすいアプリケーションには推奨されません。また、アーカイブストレージ内のバックアップではサポートされません。

> クイックリストアは、クラウドバックアップの作成元のソースシステムでONTAP 9.12.1以降が実行されている場合にのみ、FlexGroupボリュームに対してサポートされます。また、SnapLockボリュームでサポートされるのは、ソースシステムでONTAP 9.11.0以降が実行されていた場合のみです。

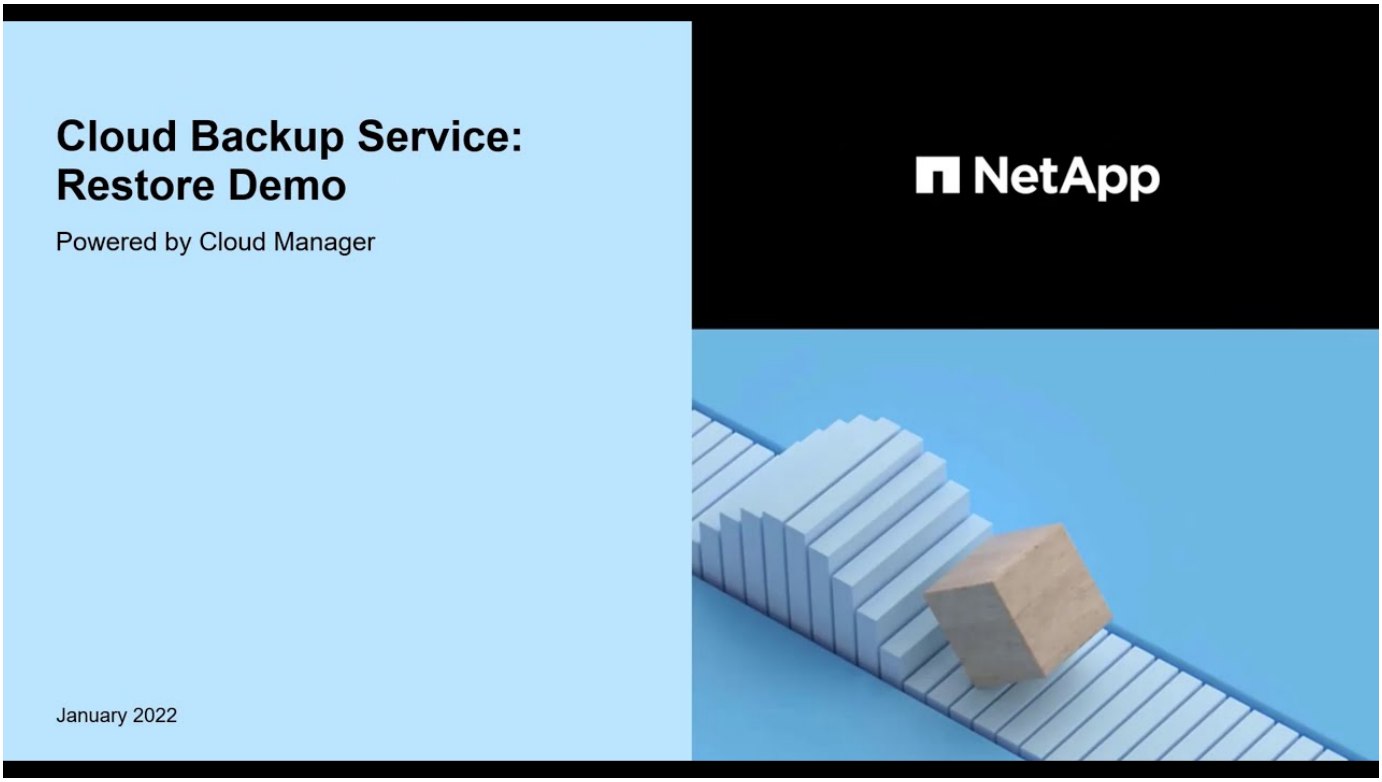
レプリケートされたボリュームからリストアする場合は、元の作業環境、Cloud Volumes ONTAPまたはオンプレミスのONTAPシステムにボリュームをリストアできます。



を使用してボリュームのリストア処理を実行するフローを示しています。"]

このように、ボリュームのリストアを実行するには、ソースの作業環境名、Storage VM、ボリューム名、およびバックアップファイルの日付を確認しておく必要があります。

次のビデオでは、ボリュームのリストア手順を簡単に紹介しています。



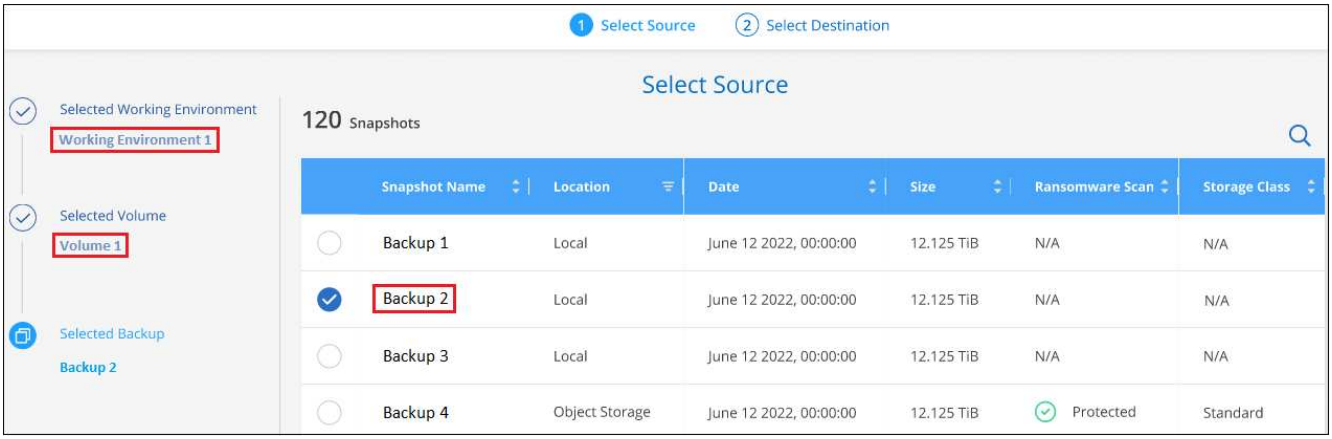
手順

1. BlueXPメニューから、*Protection > Backup and recovery*を選択します。
2. [* Restore * （復元）] タブをクリックすると、 [Restore Dashboard （復元ダッシュボード）] が表示されます。

3. [*Browse & Restore*] セクションで、 [* Restore Volume] をクリックします。

4. [ソースの選択] ページで ' リストアするボリュームのバックアップ・ファイルに移動しますリストア元の日付 / 時刻スタンプを含む * Working Environment * 、 * Volume * 、および * Backup * ファイルを選択します。

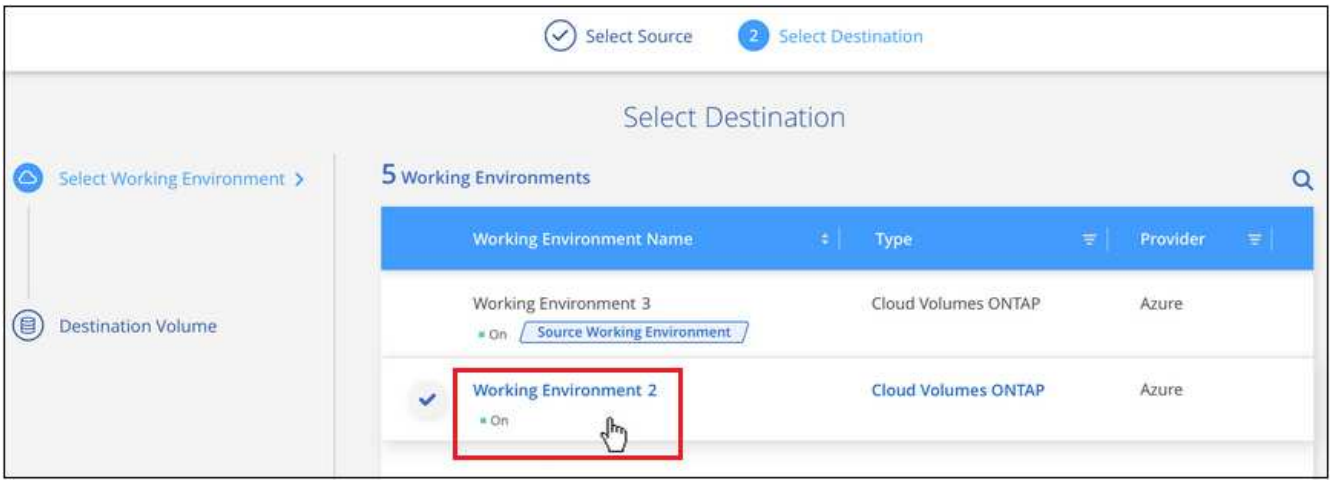
   [場所]列には、バックアップファイル（Snapshot）が*ローカル*（ソースシステム上のSnapshotコピー）、セカンダリ（セカンダリONTAPシステム上のレプリケートされたボリューム）、または*オブジェクトストレージ*（オブジェクトストレージ内のバックアップファイル）のいずれであるかが表示されます。リストアするファイルを選択します。



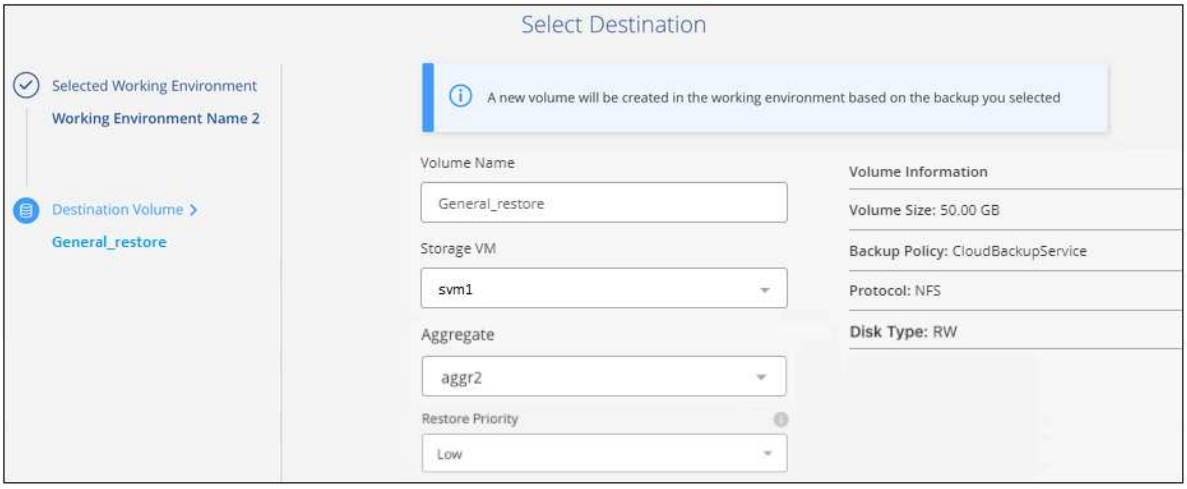
5. 「 * 次へ * 」をクリックします。

   オブジェクトストレージでバックアップファイルを選択し、そのバックアップに対してランサムウェア対策がアクティブになっている場合（バックアップポリシーでDataLockとRansomware Protectionを有効にしている場合）は、データをリストアする前に、バックアップファイルに対してランサムウェアスキャンを追加で実行するように求められます。バックアップファイルでランサムウェアをスキャンすることを推奨します。（バックアップファイルの内容にアクセスするために、クラウドプロバイダから追加の出力コストが発生します）。

6. [リストア先の選択] ページで、ボリュームをリストアする * 作業環境 * を選択します。



7. オブジェクトストレージからバックアップファイルをリストアするときに、オンプレミスのONTAPシステムを選択し、オブジェクトストレージへのクラスタ接続をまだ設定していない場合は、追加情報の入力を求めるプロンプトが表示されます。
   - Amazon S3 からリストアする場合、デスティネーションボリュームを配置する ONTAP クラスタ内の IPspace を選択し、 ONTAP クラスタに S3 バケットへのアクセスを許可するために作成したユーザのアクセスキーとシークレットキーを入力します。 さらに、必要に応じて、セキュアなデータ転送を行うためのプライベート VPC エンドポイントを選択できます。
     - Azure Blob からリストアする場合は、デスティネーションボリュームを配置する ONTAP クラスタ内の IPspace を選択し、オブジェクトストレージにアクセスする Azure サブスクリプションを選択します。また、 VNet とサブネットを選択して、データ転送を安全に行うプライベートエンドポイントを選択することもできます。
     - Google Cloud Storage からリストアする場合は、オブジェクトストレージ、バックアップが格納されているリージョン、およびデスティネーションボリュームが配置される ONTAP クラスタ内の IPspace にアクセスするために、 Google Cloud Project とアクセスキーとシークレットキーを選択します。
     - StorageGRID StorageGRID からリストアする場合は、StorageGRID サーバのFQDNとONTAP とのHTTPS通信に使用するポートを入力し、オブジェクトストレージへのアクセスに必要なアクセスキーとシークレットキー、およびデスティネーションボリュームを配置するONTAP クラスタのIPspaceを選択します。
     - ONTAP S3からリストアする場合は、ONTAP S3サーバのFQDNとONTAPがONTAP S3とのHTTPS通信に使用するポートを入力し、オブジェクトストレージへのアクセスに必要なアクセスキーとシークレットキーを選択します。 およびデスティネーションボリュームを配置するONTAPクラスタ内のIPspaceを指定します。
       a. リストアしたボリュームに使用する名前を入力し、ボリュームを配置するStorage VMとアグリゲートを選択します。FlexGroupボリュームをリストアする場合は、複数のアグリゲートを選択する必要があります。デフォルトでは、 * <source_volume_name> _ Restore * がボリューム名として使用されます。



ONTAP 9.13.0以降を使用するCloud Volumes ONTAPシステム、またはONTAP 9.14.1を実行するオンプレミスのONTAPシステムにオブジェクトストレージからバックアップをリストアする場合は、_quick restore_operationを実行するオプションがあります。

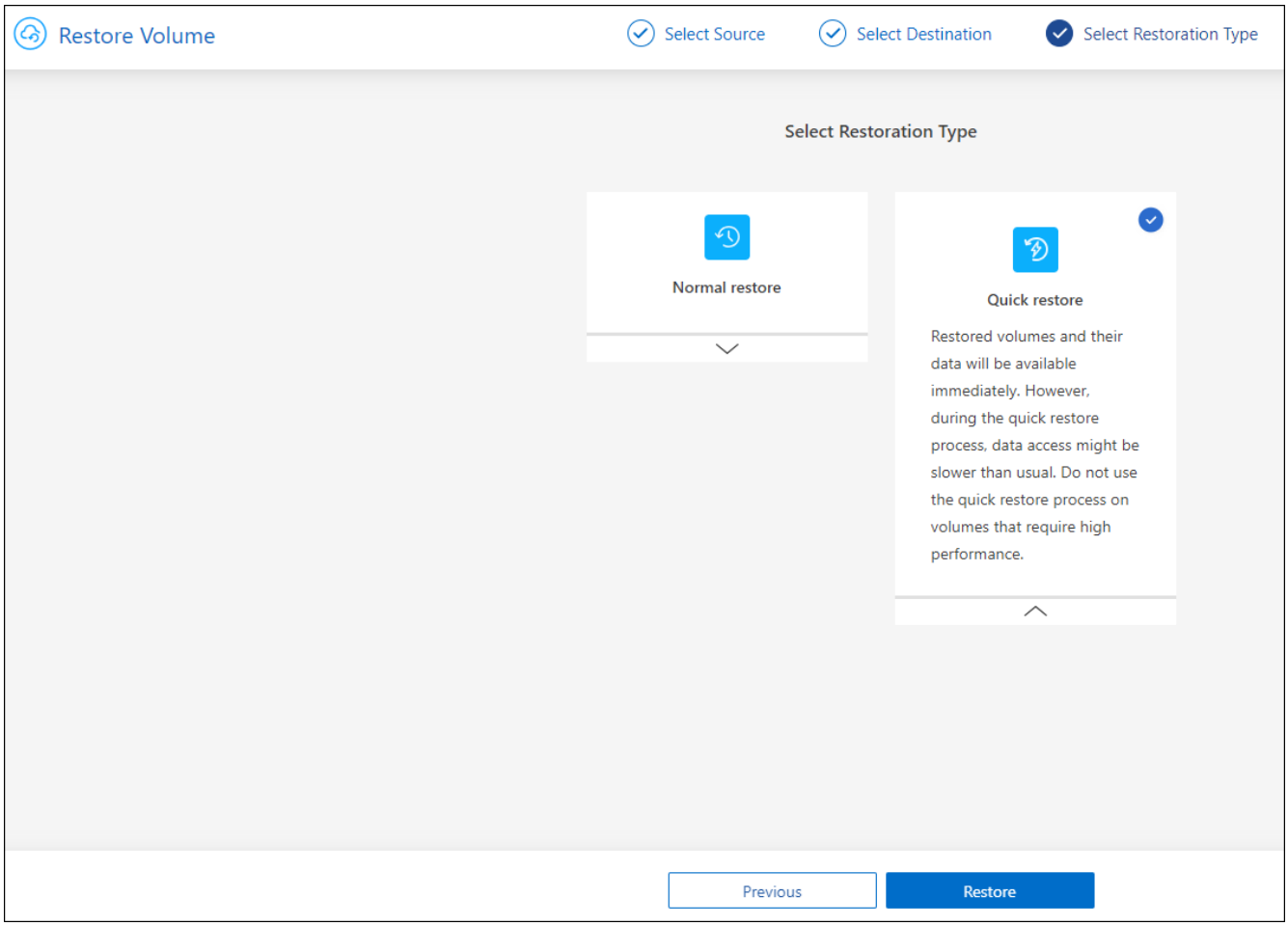
また、（ONTAP 9.10.1 以降で使用可能な）アーカイブストレージ階層にあるバックアップファイルからボリュームをリストアする場合は、リストア優先度を選択できます。

"AWS アーカイブストレージからのリストアの詳細については、こちらをご覧ください"。

"Azure アーカイブストレージからのリストアの詳細については、こちらをご覧ください"。

"Googleのアーカイブストレージからのリストアの詳細については、こちらをご覧ください"。Google Archiveストレージ階層内のバックアップファイルは、ほぼ即座にリストアされ、リストアの優先順位は不要です。

1. [次へ]*をクリックして、通常リストアとクイックリストアのどちらを実行するかを選択します。



- 通常のリストア：高いパフォーマンスが必要なボリュームでは、通常のリストアを使用します。リストアプロセスが完了するまでボリュームは使用できません。
- クイックリストア：リストアされたボリュームとデータはすぐに使用可能になります。高速リストアプロセスではデータへのアクセスが通常より遅くなる可能性があるため、ハイパフォーマンスが必要なボリュームではこのオプションを使用しないでください。

2. リストアの進行状況を確認できるように、 * リストア * をクリックするとリストアダッシュボードに戻ります。

結果

BlueXPのバックアップとリカバリでは、選択したバックアップに基づいて新しいボリュームが作成されます。

アーカイブストレージにあるバックアップファイルからボリュームをリストアする場合は、アーカイブ階層とリストアの優先順位によって数分から数時間かかることがあります。［ジョブ監視］タブをクリックすると、リストアの進行状況を確認できます。

ブラウズおよびリストアを使用して'フォルダとファイルをリストアします

ONTAP のバックアップから数ファイルしかリストアしない場合は、ボリューム全体をリストアするのではなく、フォルダまたは個々のファイルをリストアするように選択できます。フォルダとファイルは元の作業環境の既存のボリューム、または同じクラウドアカウントを使用している別の作業環境にリストアできます。また、フォルダやファイルをオンプレミスのONTAP システム上のボリュームにリストアすることもできます。

フォルダまたは個 々 のファイルは、現時点ではオブジェクトストレージ内のバックアップファイルからのみリストアできます。現在のところ、ローカルSnapshotコピーまたはセカンダリ作業環境（レプリケートされたボリューム）にあるバックアップファイルからのファイルとフォルダのリストアはサポートされていません。

複数のファイルを選択した場合は、選択したデスティネーションボリュームにすべてのファイルがリストアされます。したがって、ファイルを別のボリュームにリストアする場合は、リストアプロセスを複数回実行する必要があります。

ONTAP 9.13.0以降を使用している場合は、フォルダとそのフォルダ内のすべてのファイルおよびサブフォルダをリストアできます。9.13.0より前のバージョンのONTAP を使用している場合は、そのフォルダのファイルのみがリストアされます。サブフォルダまたはサブフォルダ内のファイルはリストアされません。

- バックアップファイルにDataLockおよびRansomware保護が設定されている場合、フォルダレベルのリストアはONTAP のバージョンが9.13.1以降の場合にのみサポートされます。以前のバージョンのONTAP を使用している場合は、バックアップファイルからボリューム全体をリストアし、必要なフォルダとファイルにアクセスできます。
- バックアップファイルがアーカイブストレージにある場合、フォルダレベルのリストアはONTAP のバージョンが9.13.1以降の場合にのみサポートされます。以前のバージョンのONTAP を使用している場合は、アーカイブされていない新しいバックアップファイルからフォルダをリストアできます。または、アーカイブされたバックアップからボリューム全体をリストアしてから、必要なフォルダとファイルにアクセスできます。

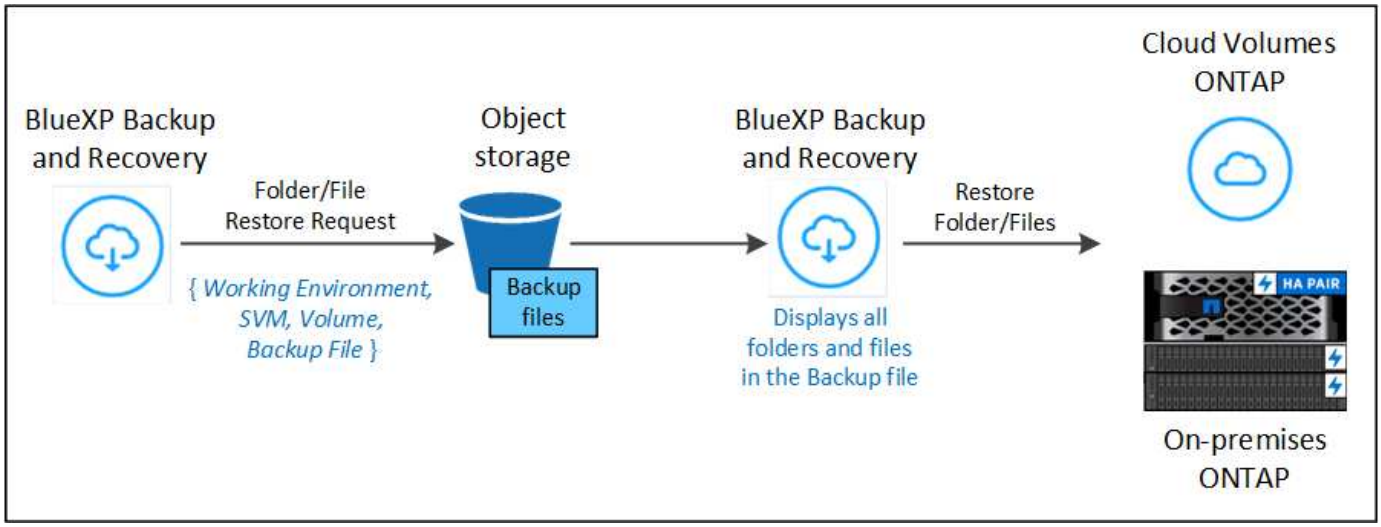
前提条件

- FILE _ RESTORE処理を実行するには、ONTAP のバージョンが9.6以降である必要があります。
- リストア処理を実行するには、ONTAP のバージョンが9.11.1以降である必要があります。データがアーカイブストレージにある場合、またはバックアップファイルでDataLockおよびランサムウェア対策を使用している場合は、ONTAP バージョン9.13.1が必要です。

フォルダおよびファイルのリストアプロセス

プロセスは次のようになります。

1. ボリュームのバックアップからフォルダまたは1つ以上のファイルを復元する場合は、*復元*タブをクリックし、_参照&復元_の下の*ファイルまたはフォルダの復元*をクリックします。
2. フォルダまたはファイルが存在するソースの作業環境、ボリューム、およびバックアップファイルを選択します。
3. BlueXPのバックアップとリカバリには、選択したバックアップファイル内のフォルダとファイルが表示されます。
4. バックアップからリストアするフォルダまたはファイルを選択します。
5. フォルダまたはファイル（作業環境、ボリューム、およびフォルダ）のリストア先を選択し、*リストア*をクリックします。
6. ファイルがリストアされます。

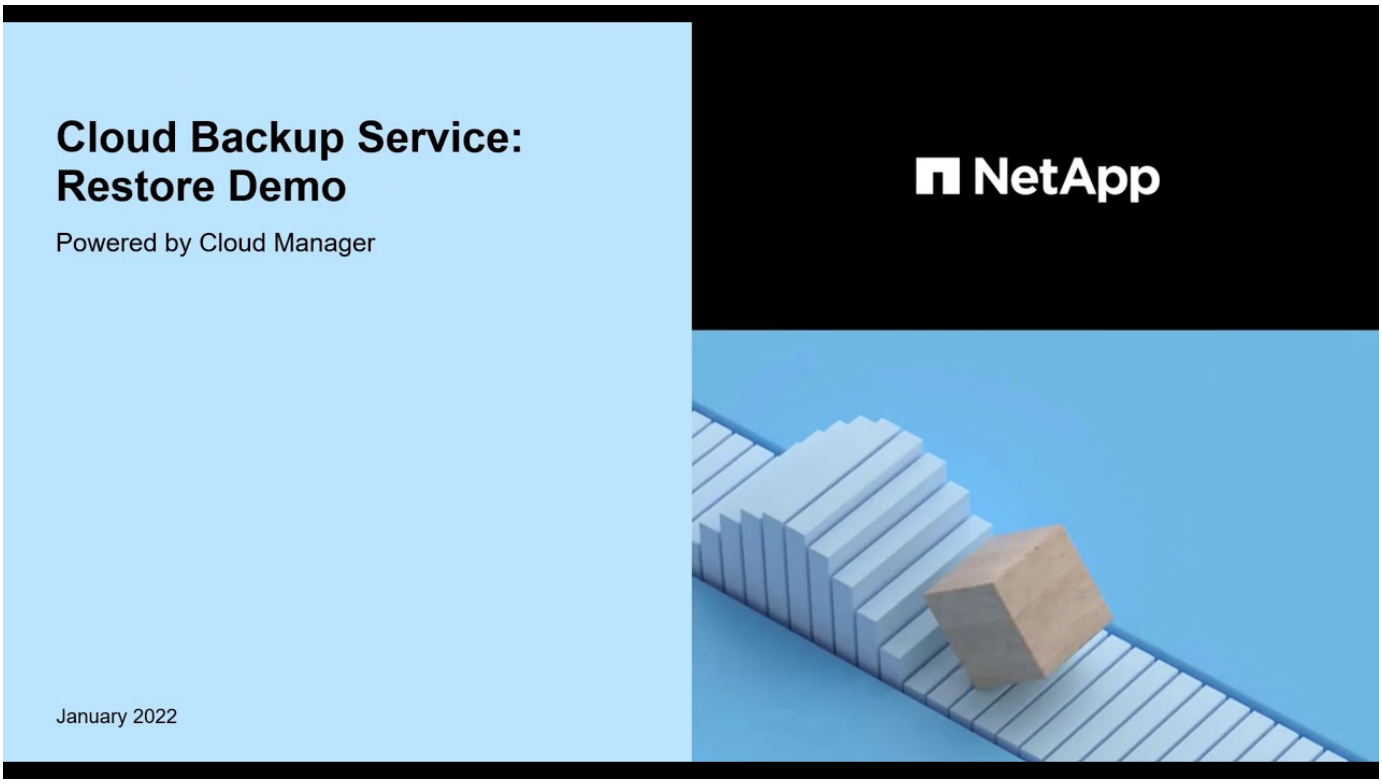


このように、フォルダまたはファイルのリストアを実行するには、作業環境名、ボリューム名、バックアップファイルの日付、およびフォルダ/ファイル名を知っている必要があります。

フォルダとファイルを復元します

ONTAP ボリュームのバックアップからボリュームにフォルダまたはファイルをリストアするには、次の手順を実行します。フォルダまたはファイルのリストアに使用するボリュームの名前とバックアップファイルの日付を確認しておく必要があります。この機能では、ライブブラウズを使用して、各バックアップファイル内のディレクトリとファイルのリストを表示できます。

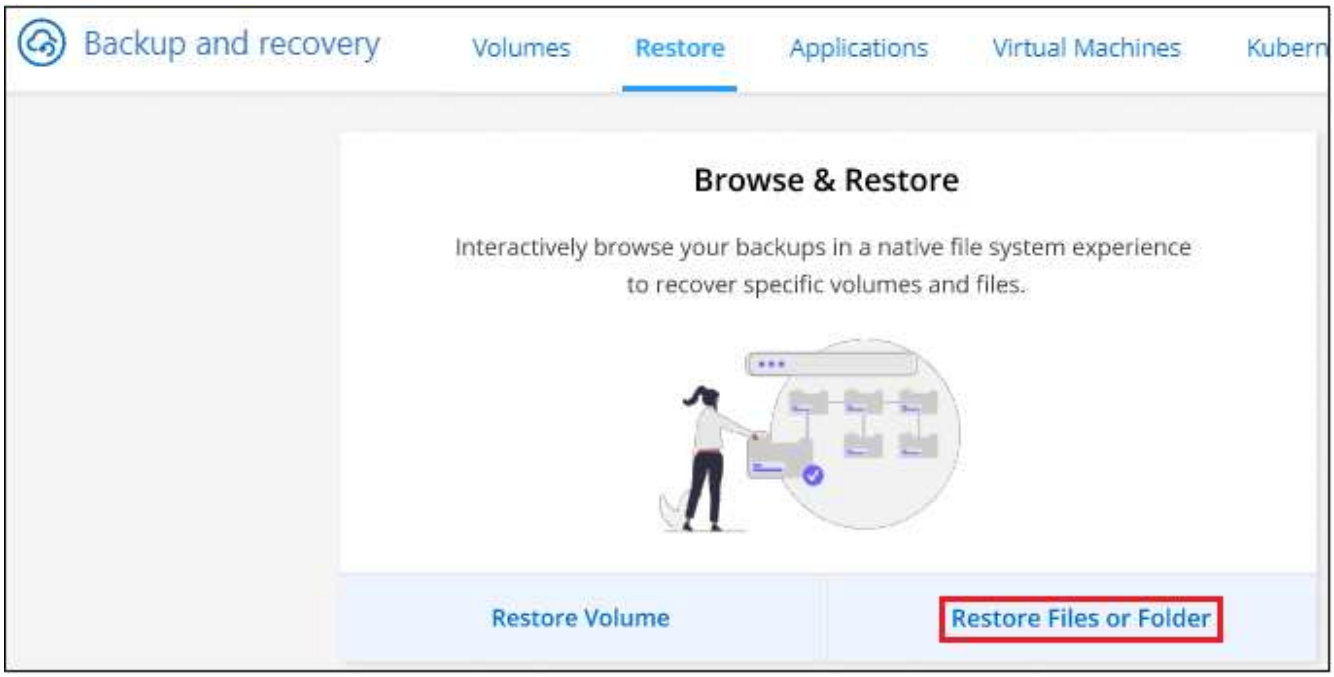
次のビデオでは、 1 つのファイルをリストアする手順を簡単に紹介します。



手順

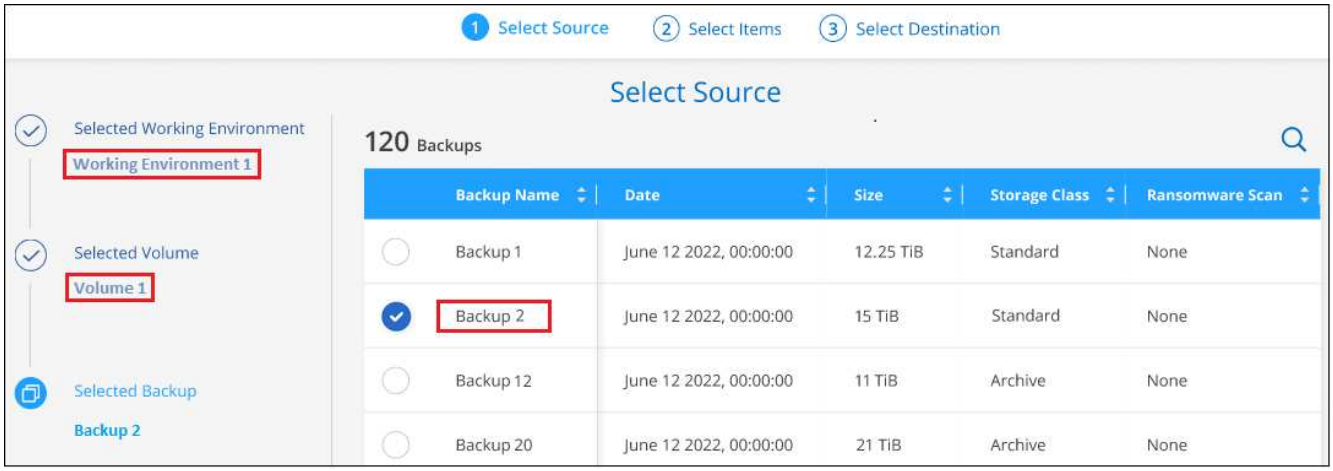
1. BlueXPメニューから、*Protection > Backup and recovery*を選択します。

2. [* Restore * （復元）] タブをクリックすると、 [Restore Dashboard （復元ダッシュボード）] が表示されます。
3. [参照と復元]セクションで、[ファイルまたはフォルダの復元]をクリックします。



ボタンを選択するスクリーンショット。"]

4. [ソースの選択]ページで'リストアするフォルダまたはファイルが格納されているボリュームのバックアップ・ファイルに移動しますファイルのリストア元の日付 / タイムスタンプを持つ * 作業環境 * 、 * ボリューム * 、および * バックアップ * を選択します。



5. 「*次へ」をクリックすると、ボリュームバックアップのフォルダとファイルのリストが表示されます。

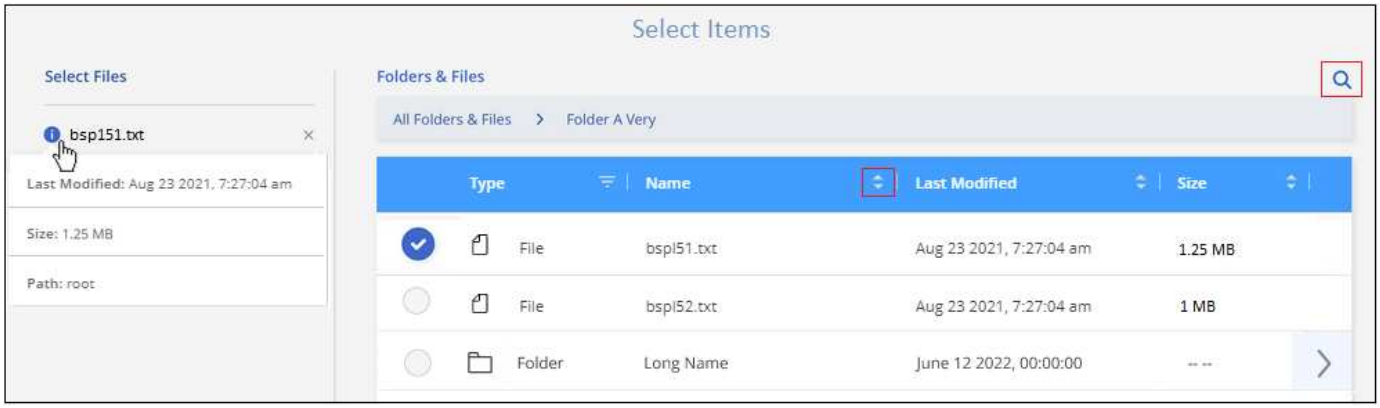
   アーカイブストレージ階層にあるバックアップファイルからフォルダまたはファイルをリストアする場合は、[Restore Priority]を選択できます。

"AWS アーカイブストレージからのリストアの詳細については、こちらをご覧ください"。

"Azure アーカイブストレージからのリストアの詳細については、こちらをご覧ください"。

"Googleのアーカイブストレージからのリストアの詳細については、こちらをご覧ください"。Google Archiveストレージ階層内のバックアップファイルは、ほぼ即座にリストアされ、リストアの優先順位は不要です。

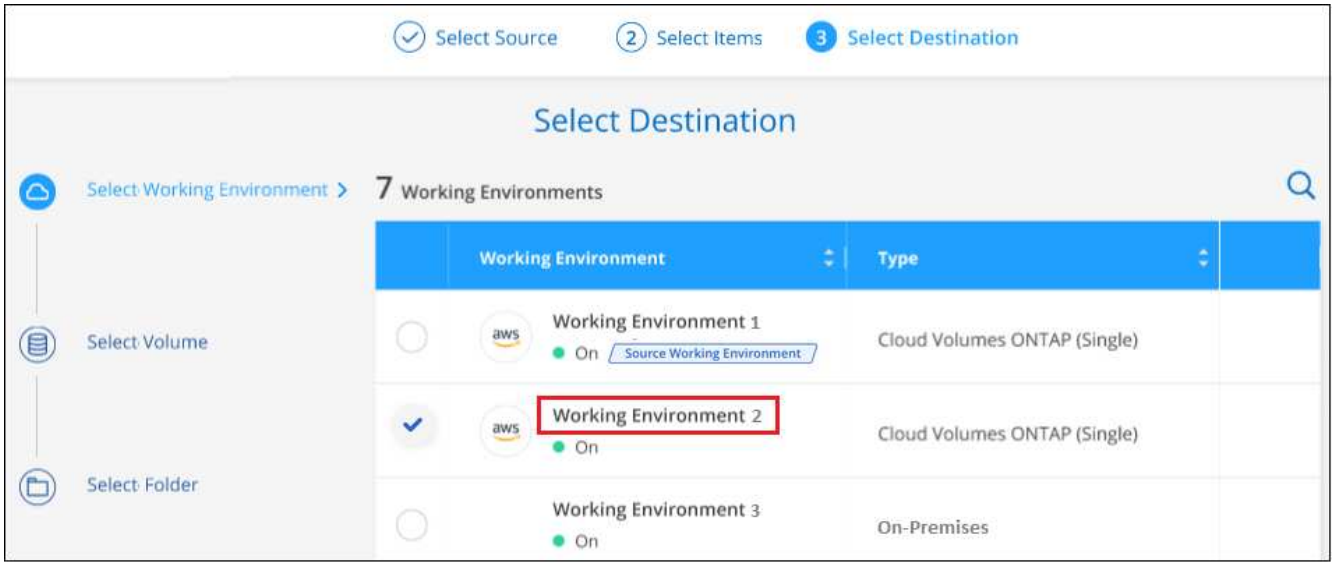
[+]
また、バックアップファイルに対してランサムウェア対策が有効になっている場合（バックアップポリシーでDataLockとRansomware Protectionを有効にした場合）は、データをリストアする前に、バックアップファイルに対してランサムウェアスキャンを追加で実行するように求められます。バックアップファイルでランサムウェアをスキャンすることを推奨します。（バックアップファイルの内容にアクセスするために、クラウドプロバイダから追加の出力コストが発生します）。

[+]


ページのスクリーンショット。"]

1. [アイテムの選択]ページで、復元するフォルダまたはファイルを選択し、[続行]をクリックします。アイテムの検索を支援するために、次の手順を実行します。
   - フォルダまたはファイル名が表示されている場合は、その名前をクリックします。
   - 検索アイコンをクリックしてフォルダまたはファイルの名前を入力すると、その項目に直接移動できます。
   - を使用して、フォルダ内の下位レベルに移動できます › 特定のファイルを検索するには、行の末尾にあるボタンをクリックします。

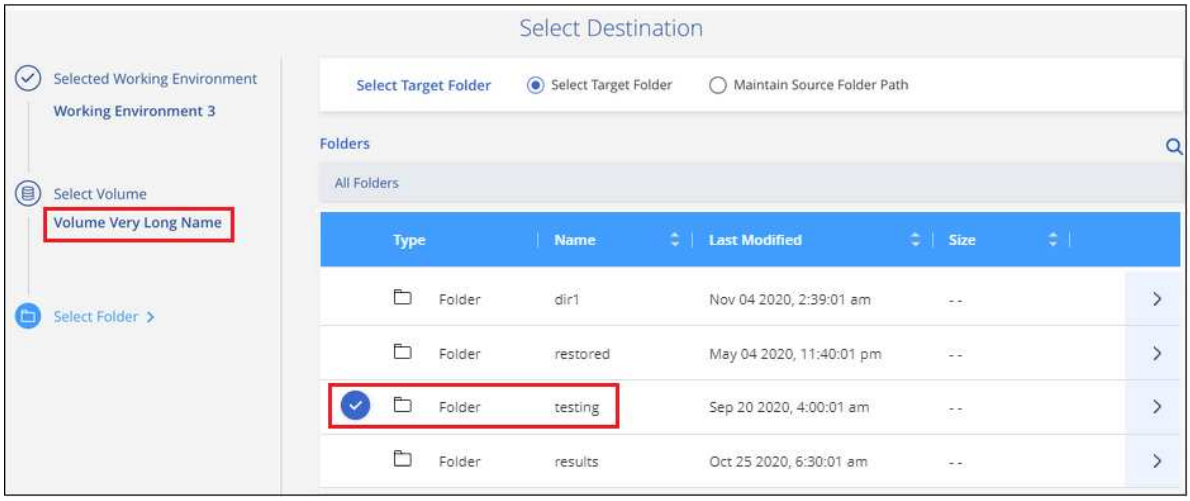
     ファイルを選択すると、ページの左側に追加され、選択済みのファイルが表示されます。必要に応じて、ファイル名の横にある * x * をクリックすると、このリストからファイルを削除できます。
2. [リストア先の選択]ページで、項目をリストアする*作業環境*を選択します。



オンプレミスクラスタを選択し、オブジェクトストレージへのクラスタ接続をまだ設定していない場合は、追加情報を入力するように求められます。

- Amazon S3 からリストアする場合は、デスティネーションボリュームが配置されている ONTAP クラスタの IPspace と、オブジェクトストレージへのアクセスに必要な AWS Access Key および Secret Key を入力します。クラスタへの接続にプライベートリンク設定を選択することもできます。
  - Azure Blob からリストアする場合は、デスティネーションボリュームが配置されている ONTAP クラスタ内の IPspace を入力します。クラスタへの接続にプライベートエンドポイントの設定を選択することもできます。
  - Google Cloud Storage からリストアする場合は、デスティネーションボリュームが配置されている ONTAP クラスタの IPspace と、オブジェクトストレージへのアクセスに必要なアクセスキーとシークレットキーを入力します。
  - StorageGRID StorageGRID からリストアする場合は、StorageGRID サーバのFQDNとONTAP とのHTTPS通信に使用するポートを入力し、オブジェクトストレージへのアクセスに必要なアクセスキーとシークレットキー、およびデスティネーションボリュームが配置されているONTAP クラスタのIPspaceを入力します。

    a. 次に、フォルダーまたはファイルを復元する*ボリューム*と*フォルダー*を選択します。



フォルダとファイルをリストアするときに、いくつかのオプションを選択できます。

- 上の図のように、 [ターゲットフォルダの選択] を選択した場合は、次のようになります。
  - 任意のフォルダを選択できます。
  - フォルダにカーソルを合わせて、をクリックできます › 行の末尾にあるサブフォルダをドリルダウンし、フォルダを選択します。
- ソースフォルダ/ファイルがある場所と同じ宛先作業環境およびボリュームを選択した場合は、「ソースフォルダパスを保持」を選択して、ソース構造内に存在していたのと同じフォルダにフォルダまたはファイルを復元できます。同じフォルダとサブフォルダがすべて存在している必要があります。フォルダは作成されません。ファイルを元の場所にリストアする場合は、ソースファイルを上書きするか、新しいファイルを作成するかを選択できます。

  a. リストアの進行状況を確認できるように、 * リストア * をクリックするとリストアダッシュボードに戻ります。また、*ジョブ監視*タブをクリックしてリストアの進捗状況を確認することもできます。

検索とリストアを使用した **ONTAP** データのリストア

検索とリストアを使用して、ONTAP バックアップファイルからボリューム、フォルダ、またはファイルをリストアできます。[Search & Restore]を使用すると、すべてのバックアップから特定のボリューム、フォルダ、またはファイルを検索し、リストアを実行できます。作業環境名、ボリューム名、ファイル名を正確に把握しておく必要はありません。すべてのボリュームバックアップファイルが検索されます。

検索処理では、ONTAPボリュームのすべてのローカルSnapshotコピー、セカンダリストレージシステム上のレプリケートされたすべてのボリューム、およびオブジェクトストレージに存在するすべてのバックアップファイルが検索されます。ローカルSnapshotコピーまたはレプリケートされたボリュームからデータをリストアする方が、オブジェクトストレージ内のバックアップファイルからリストアするよりも短時間でコストを抑えることができるため、これらの場所からデータをリストアすることもできます。

バックアップファイルからa_full volume__をリストアすると、BlueXPのバックアップとリカバリでは、バックアップのデータを使用して_new_volumeが作成されます。データは、元の作業環境のボリュームとして、ソースの作業環境と同じクラウドアカウントにある別の作業環境にリストアすることも、オンプレミスのONTAPシステムにリストアすることもできます。

_foldersまたはfiles_を元のボリュームの場所、同じ作業環境内の別のボリューム、同じクラウドアカウントを使用する別の作業環境、またはオンプレミスのONTAPシステム上のボリュームにリストアできます。

ONTAP 9.13.0以降を使用している場合は、フォルダとそのフォルダ内のすべてのファイルおよびサブフォルダをリストアできます。9.13.0より前のバージョンのONTAP を使用している場合は、そのフォルダのファイルのみがリストアされます。サブフォルダまたはサブフォルダ内のファイルはリストアされません。

リストアするボリュームのバックアップファイルがアーカイブストレージ（ONTAP 9.10.1以降で使用可能）にある場合、リストア処理にはより長い時間がかかり、追加コストが発生します。デスティネーションクラスタでも、ボリュームのリストアにはONTAP 9.10.1以降、ファイルのリストアには9.11.1、Google Archive and StorageGRID には9.12.1、フォルダのリストアには9.13.1が実行されている必要があります。

"AWS アーカイブストレージからのリストアの詳細については、こちらをご覧ください"。

"Azure アーカイブストレージからのリストアの詳細については、こちらをご覧ください"。

"Googleのアーカイブストレージからのリストアの詳細については、こちらをご覧ください"。

- オブジェクトストレージ内のバックアップファイルにDataLockおよびRansomware保護が設定されている場合、フォルダレベルのリストアはONTAPのバージョンが9.13.1以降の場合にのみサポートされます。以前のバージョンのONTAP を使用している場合は、バックアップファイルからボリューム全体をリストアし、必要なフォルダとファイルにアクセスできます。
- オブジェクトストレージ内のバックアップファイルがアーカイブストレージにある場合、フォルダレベルのリストアはONTAPのバージョンが9.13.1以降の場合にのみサポートされます。以前のバージョンのONTAP を使用している場合は、アーカイブされていない新しいバックアップファイルからフォルダをリストアできます。または、アーカイブされたバックアップからボリューム全体をリストアしてから、必要なフォルダとファイルにアクセスできます。
- AzureアーカイブストレージからStorageGRID システムにデータをリストアする場合、「High」リストア優先度はサポートされません。
- 現在、ONTAP S3オブジェクトストレージ内のボリュームからのフォルダのリストアはサポートされていません。

開始する前に、リストアするボリュームやファイルの名前や場所を把握しておく必要があります。

次のビデオでは、 1 つのファイルをリストアする手順を簡単に紹介します。

サポートされている作業環境とオブジェクトストレージプロバイダの検索とリストア

セカンダリ作業環境（レプリケートされたボリューム）またはオブジェクトストレージ（バックアップファイル）にあるバックアップファイルから、ONTAPデータを次の作業環境にリストアできます。Snapshotコピーはソースの作業環境に存在し、同じシステムにのみリストアできます。

*注：*ボリュームとファイルは任意のタイプのバックアップファイルからリストアできますが、フォルダは現時点ではオブジェクトストレージのバックアップファイルからのみリストアできます。

バックアップファイルの場所		デスティネーションの作業環境
オブジェクトストア（バックアップ）	セカンダリシステム（レプリケーション）	ifdef::aws[]
Amazon S3	AWS の Cloud Volumes ONTAP オンプレミスの ONTAP システム	AWS の Cloud Volumes ONTAP オンプレミスの ONTAP システム endif：：aws[] ifdef：Azure []
Azure Blob の略	Azure の Cloud Volumes ONTAP オンプレミスの ONTAP システム	Azure の Cloud Volumes ONTAP オンプレミスの ONTAP システム endif：：azure[] ifdef ::gcp[]
Google クラウドストレージ	Google の Cloud Volumes ONTAP オンプレミスの ONTAP システム	Google の Cloud Volumes ONTAP オンプレミスの ONTAP システム endif：GCP []
NetApp StorageGRID	オンプレミスの ONTAP システム Cloud Volumes ONTAP	オンプレミスの ONTAP システム
ONTAP S3の略	オンプレミスの ONTAP システム Cloud Volumes ONTAP	オンプレミスの ONTAP システム

検索と復元の場合、コネクタは次の場所にインストールできます。

- Amazon S3の場合、ConnectorはAWSまたは自社運用のどちらにも導入できます
- Azure Blobの場合は、Azureまたは自社運用環境に導入できます
- Google Cloud Storageの場合、ConnectorをGoogle Cloud Platform VPCに導入する必要があります
- StorageGRID の場合は、インターネットアクセスを使用するかどうかに関係なく、コネクタを社内に導入する必要があります
- ONTAP S3の場合、コネクタは社内環境（インターネットアクセスの有無にかかわらず）またはクラウドプロバイダ環境に導入できます。

「オンプレミス ONTAP システム」とは、 FAS 、 AFF 、 ONTAP Select の各システムを指します。

前提条件

- クラスタの要件：
  - ONTAP のバージョンは 9.8 以降である必要があります。
  - ボリュームが配置されている Storage VM （ SVM ）に設定済みのデータ LIF が必要です。
  - ボリュームでNFSが有効になっている必要があります（NFSとSMB / CIFSの両方のボリュームがサポートされています）。

- SVM で SnapDiff RPC サーバをアクティブ化する必要があります。作業環境でインデックス作成を有効にすると'BlueXPによって自動的に実行されます（SnapDiffは、Snapshotコピー間のファイルやディレクトリの相違を迅速に識別するテクノロジです）。

- AWS の要件：
  - BlueXPに権限を付与するユーザロールに、Amazon Athena、AWS Glue、およびAWS S3の特定の権限を追加する必要があります。 "すべての権限が正しく設定されていることを確認します"。

    以前に設定したコネクタでBlueXPのバックアップとリカバリをすでに使用している場合は、ここでBlueXPユーザロールにAthena権限とGlue権限を追加する必要があります。検索と復元に必要です。

- Azureの要件：
  - Azure Synapse Analytics Resource Provider（"Microsoft.Synapse"）をサブスクリプションに登録する必要があります。 "このリソースプロバイダをサブスクリプションに登録する方法については、を参照してください"。リソースプロバイダを登録するには、Subscription * Owner または Contributor *である必要があります。
  - 特定のAzure Synapse WorkspaceおよびData Lakeストレージアカウントの権限を、BlueXPに権限を付与するユーザーロールに追加する必要があります。 "すべての権限が正しく設定されていることを確認します"。

    以前に設定したコネクタでBlueXPのバックアップとリカバリをすでに使用している場合は、ここでBlueXPユーザロールにAzure Synapse WorkspaceとData Lake Storageアカウントの権限を追加する必要があります。検索と復元に必要です。

  - インターネットへのHTTP通信には、*プロキシサーバーなしでコネクターを設定する必要があります。コネクタにHTTPプロキシサーバを設定している場合は、検索と置換機能を使用できません。

- Google Cloudの要件：
  - 特定のGoogle BigQuery権限は、BlueXPに権限を付与するユーザーロールに追加する必要があります。 "すべての権限が正しく設定されていることを確認します"。

    以前に設定したコネクタでBlueXPのバックアップとリカバリをすでに使用している場合は、ここでBlueXPユーザロールにBigQuery権限を追加する必要があります。検索と復元に必要です。

- StorageGRIDおよびONTAP S3の要件：

  構成に応じて、検索とリストアの2つの方法が実装されています。

  - アカウントにクラウドプロバイダの資格情報がない場合は、インデックスカタログの情報がコネクタに保存されます。
  - プライベート（ダーク）サイトでコネクタを使用している場合、インデックスカタログ情報はコネクタに保存されます（コネクタのバージョン3.9.25以降が必要です）。
  - ある場合 "AWSクレデンシャル" または "Azure のクレデンシャル" アカウントでは、クラウドに展開されたコネクタと同様に、インデックスカタログがクラウドプロバイダに格納されます。（両方のクレデンシャルがある場合は、デフォルトでAWSが選択されます）。

    オンプレミスコネクタを使用している場合でも、コネクタ権限とクラウドプロバイダリソースの両方についてクラウドプロバイダの要件を満たしている必要があります。この実装を使用する場合は、前述のAWSとAzureの要件を参照してください。

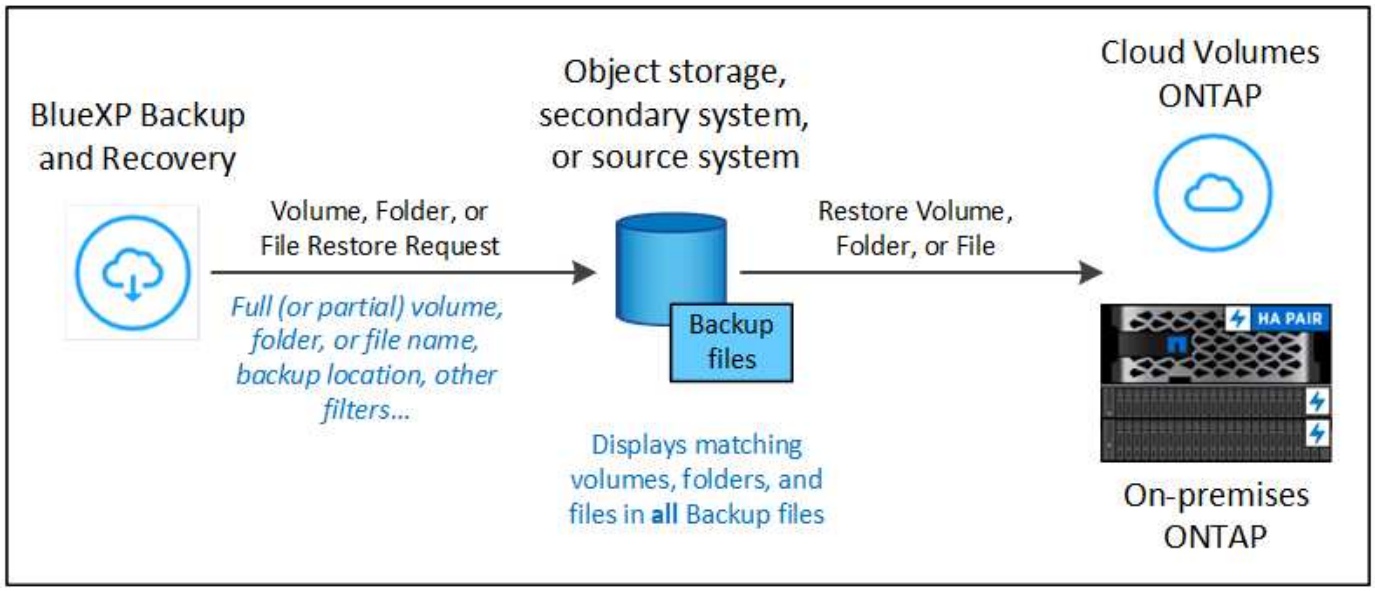
検索とリストアのプロセス

プロセスは次のようになります。

1. 検索とリストアを使用する前に、ボリュームデータのリストア元となる各ソース作業環境でインデックスの作成を有効にする必要があります。これにより、 Indexed Catalog は、すべてのボリュームのバックアップファイルを追跡できます。
2. ボリュームバックアップからボリュームまたはファイルを復元する場合は、 _ 検索と復元 _ で * 検索と復元 * をクリックします。
3. ボリューム、フォルダ、またはファイルの検索条件を、ボリューム名の一部または全体、ファイル名の一部または全体、バックアップの場所、サイズ範囲、作成日範囲、その他の検索フィルタで入力します。 [検索]*をクリックします。

   検索結果ページには、検索条件に一致するファイルまたはボリュームを含むすべての場所が表示されます。

4. ボリュームまたはファイルの復元に使用する場所の * すべてのバックアップの表示 * をクリックし、実際に使用するバックアップファイルの * 復元 * をクリックします。
5. ボリューム、フォルダ、またはファイルをリストアする場所を選択し、*リストア*をクリックします。
6. ボリューム、フォルダ、またはファイルがリストアされます。



ご覧のように、名前の一部を知っておくだけで、BlueXPのバックアップとリカバリでは、検索に一致するすべてのバックアップファイルが検索されます。

各作業環境でインデックスカタログを有効にします

検索とリストアを使用する前に、ボリュームまたはファイルのリストア元となる各ソース作業環境でインデックス作成を有効にする必要があります。これにより、インデックスカタログですべてのボリュームとすべてのバックアップファイルを追跡できるため、検索をすばやく効率的に実行できます。

この機能を有効にすると、BlueXPのバックアップとリカバリによって、ボリュームのSVMでSnapDiff v3が有効になり、次の処理が実行されます。

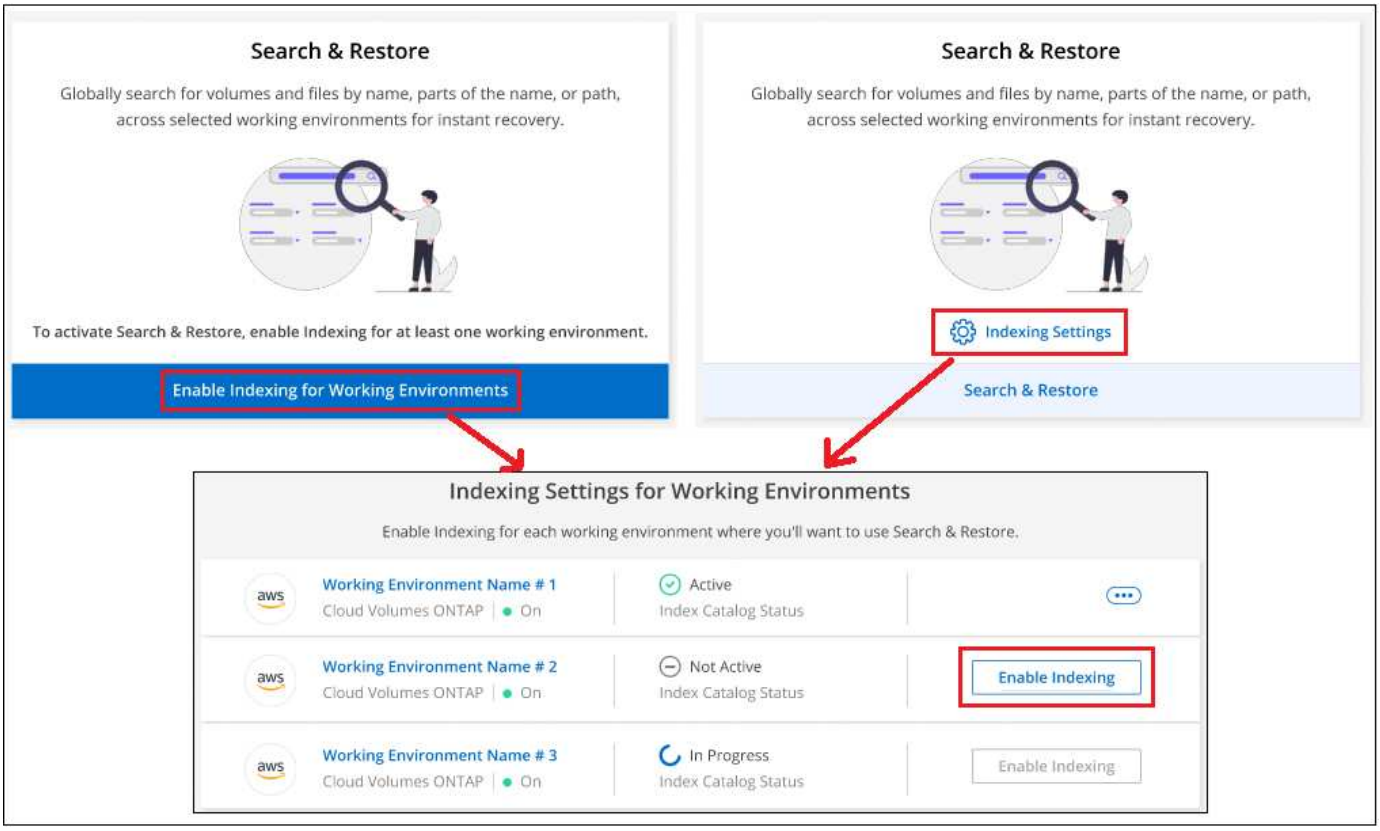
- AWSに格納されたバックアップについては、新しいS3バケットとがプロビジョニングされます "Amazon Athena インタラクティブクエリーサービス" および "AWS グルーサーバレスデータ統合サービス"。
- Azureに保存されているバックアップの場合、Azure Synapseワークスペースとデータレイクファイルシステムをワークスペースデータを格納するコンテナとしてプロビジョニングします。
- Google Cloudに保存されているバックアップの場合、新しいバケットとがプロビジョニングされます "Google Cloud BigQueryサービス" アカウント/プロジェクトレベルでプロビジョニングされます。
- StorageGRIDまたはONTAP S3に格納されたバックアップの場合、コネクタまたはクラウドプロバイダ環境にスペースがプロビジョニングされます。

作業環境でインデックス作成がすでに有効になっている場合は ' 次のセクションに進んでデータをリストアしてください

作業環境でインデックス作成を有効にするには：

- 作業環境にインデックスが作成されていない場合は、リストアダッシュボードの *Search&Restore* で * 作業環境でインデックス作成を有効にする * をクリックし、作業環境で * インデックス作成を有効にする * をクリックします。
- 少なくとも 1 つの作業環境にインデックスが作成されている場合は、リストアダッシュボードの *Search & Restore* で、 * インデックス設定 * をクリックし、作業環境で * インデックス作成を有効にする * をクリックします。

すべてのサービスがプロビジョニングされ、インデックスカタログがアクティブ化されると、作業環境は「アクティブ」と表示されます。



作業環境内のボリュームのサイズ、および3つすべてのバックアップ場所のバックアップファイルの数によっては、最初のインデックス作成プロセスに最大1時間かかることがあります。その後は、 1 時間ごとに差分変更を反映して透過的に更新され、最新の状態が維持されます。

検索とリストアを使用して'ボリューム'フォルダ'およびファイルをリストアします

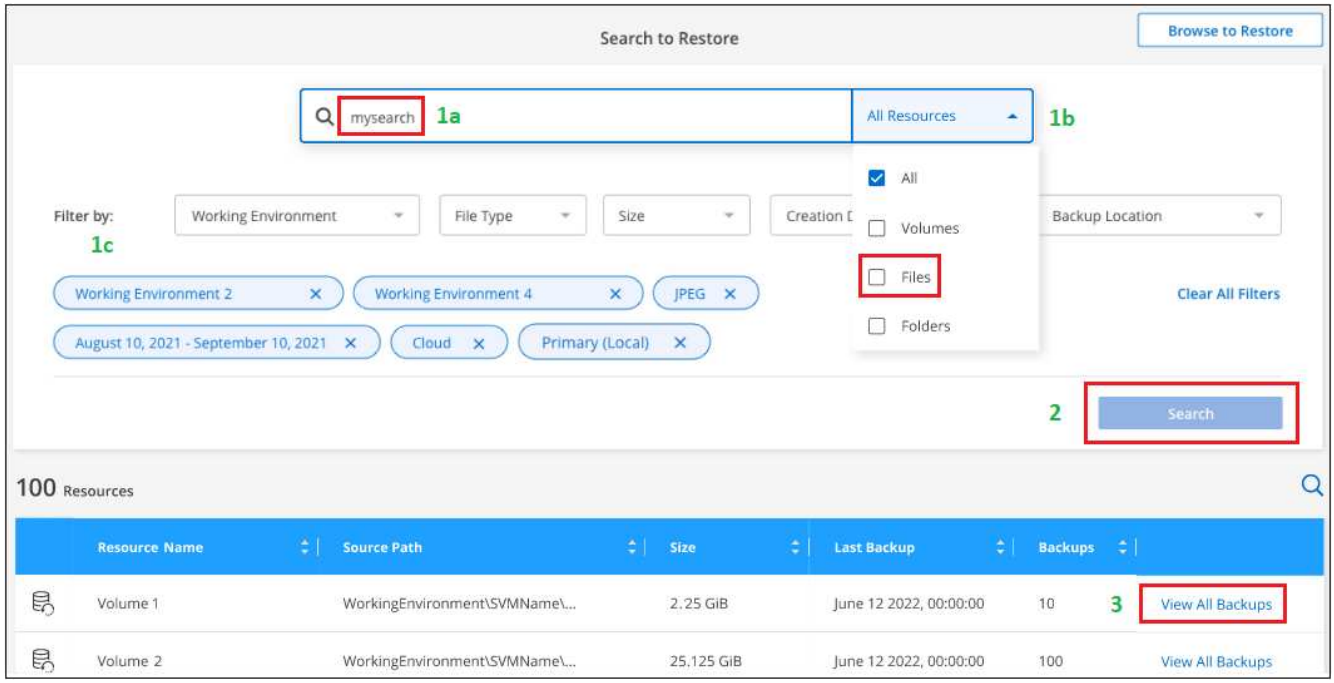
お先にどうぞ 作業環境のインデックス作成を有効にしましたでは、検索とリストアを使用して、ボリューム、フォルダ、およびファイルをリストアできます。これにより、幅広いフィルタを使用して、すべてのバックアップファイルからリストアするファイルまたはボリュームを検索できます。

手順

1. BlueXPメニューから、*Protection > Backup and recovery*を選択します。
2. [* Restore * （復元）] タブをクリックすると、 [Restore Dashboard （復元ダッシュボード）] が表示されます。
3. [検索と復元] セクションで、 [* 検索と復元 *] をクリックします。

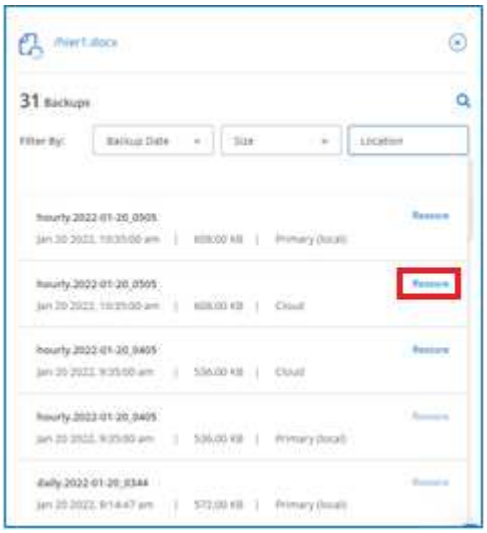
から[Search Restore]ボタンを選択するスクリーンショット。"]

4. [リストアする検索（Search to Restore）]ページから、次の
   a. _検索バー_で、ボリューム名、フォルダ名、またはファイル名の全体または一部を入力します。
   b. リソースのタイプとして、* Volumes 、 Files 、 Folders 、 All *を選択します。
   c. [*Filter by*]領域で、フィルタ条件を選択します。たとえば、データが存在する作業環境とファイルの種類（.jpegファイルなど）を選択できます。オブジェクトストレージ内の使用可能なSnapshotコピーまたはバックアップファイル内でのみ結果を検索する場合は、[Backup Location]のタイプを選択します。
5. [検索（ Search）]をクリックすると、検索結果（Search Results）領域に、検索に一致するファイル、フォルダ、またはボリュームを含むすべてのリソースが表示されます。



ページの検索条件と検索結果を示すスクリーンショット。"]

6. リストアするデータがあるリソースを探し、*[すべてのバックアップを表示]*をクリックして、一致するボリューム、フォルダ、またはファイルを含むすべてのバックアップファイルを表示します。



7. データのリストアに使用するバックアップファイルを探し、*[リストア]*をクリックします。

   検索結果には、検索対象のファイルを含むローカルボリュームのSnapshotコピーとリモートでレプリケートされたボリュームが含まれていることが示されます。リストアは、クラウドバックアップファイルから、Snapshotコピーから、またはレプリケートされたボリュームから選択できます。

8. ボリューム、フォルダ、またはファイルのリストア先を選択し、*リストア*をクリックします。
   - ボリュームについては、元の作業環境を選択するか、別の作業環境を選択できます。FlexGroupボリュームをリストアする場合は、複数のアグリゲートを選択する必要があります。
   - フォルダの場合は、元の場所にリストアすることも、作業環境、ボリューム、フォルダなどの別の場所を選択することもできます。

- ファイルの場合は、元の場所にリストアするか、作業環境、ボリューム、フォルダなどの別の場所を選択できます。元の場所を選択する場合は、ソースファイルを上書きするか、新しいファイルを作成するかを選択できます。

  オンプレミスの ONTAP システムを選択し、オブジェクトストレージへのクラスタ接続をまだ設定していない場合は、追加情報を入力するように求められます。

  - Amazon S3 からリストアする場合、デスティネーションボリュームを配置する ONTAP クラスタ内の IPspace を選択し、 ONTAP クラスタに S3 バケットへのアクセスを許可するために作成したユーザのアクセスキーとシークレットキーを入力します。 さらに、必要に応じて、セキュアなデータ転送を行うためのプライベート VPC エンドポイントを選択できます。 "これらの要件の詳細を参照してください"。
    - Azure Blobからリストアする場合は、デスティネーションボリュームを配置するONTAP クラスタ内のIPspaceを選択し、VNetとサブネットを選択してデータ転送を保護するプライベートエンドポイントを必要に応じて選択します。 "これらの要件の詳細を参照してください"。
    - Google Cloud Storageからリストアする場合は、デスティネーションボリュームを配置するONTAP クラスタ内のIPspaceと、オブジェクトストレージにアクセスするためのアクセスキーとシークレットキーを選択します。 "これらの要件の詳細を参照してください"。
    - StorageGRID StorageGRID からリストアする場合は、StorageGRID サーバのFQDNとONTAPとのHTTPS通信に使用するポートを入力し、オブジェクトストレージへのアクセスに必要なアクセスキーとシークレットキー、およびデスティネーションボリュームが配置されているONTAP クラスタのIPspaceを入力します。 "これらの要件の詳細を参照してください"。
    - ONTAP S3からリストアする場合は、ONTAP S3サーバのFQDNとONTAPがONTAP S3とのHTTPS通信に使用するポートを入力し、オブジェクトストレージへのアクセスに必要なアクセスキーとシークレットキーを選択します。 およびデスティネーションボリュームを配置するONTAPクラスタ内のIPspaceを指定します。 "これらの要件の詳細を参照してください"。

結果

ボリューム、フォルダ、またはファイルがリストアされ、リストアダッシュボードに戻り、リストア処理の進捗状況を確認できます。また、*ジョブ監視*タブをクリックしてリストアの進捗状況を確認することもできます。

リストアしたボリュームに対しては、を実行できます "この新しいボリュームのバックアップ設定を管理します" 必要に応じて。

オンプレミスのアプリケーションデータのバックアップとリストア

オンプレミスアプリケーションのデータを保護

アプリケーション向けのBlueXPバックアップ/リカバリ機能は、オンプレミスのONTAPプライマリからクラウドプロバイダに至るまで、アプリケーションと整合性のあるSnapshotを保護するためのデータ保護機能を提供します。

Oracle、Microsoft SQL、SAP HANA、MongoDB、MySQL、 オンプレミスのONTAPシステムからAmazon Web Services、Microsoft Azure、Google Cloud Platform、StorageGRIDに至るまで、PostgreSQLアプリケーションのデータをバックアップできます。

アプリケーションのBlueXPのバックアップとリカバリの詳細については、以下を参照してください。

- "BlueXPのバックアップ/リカバリ機能とSnapCenter を使用した、アプリケーション対応のバックアップ"
- "BlueXPの「Backup and Recovery for Applications」ポッドキャスト"

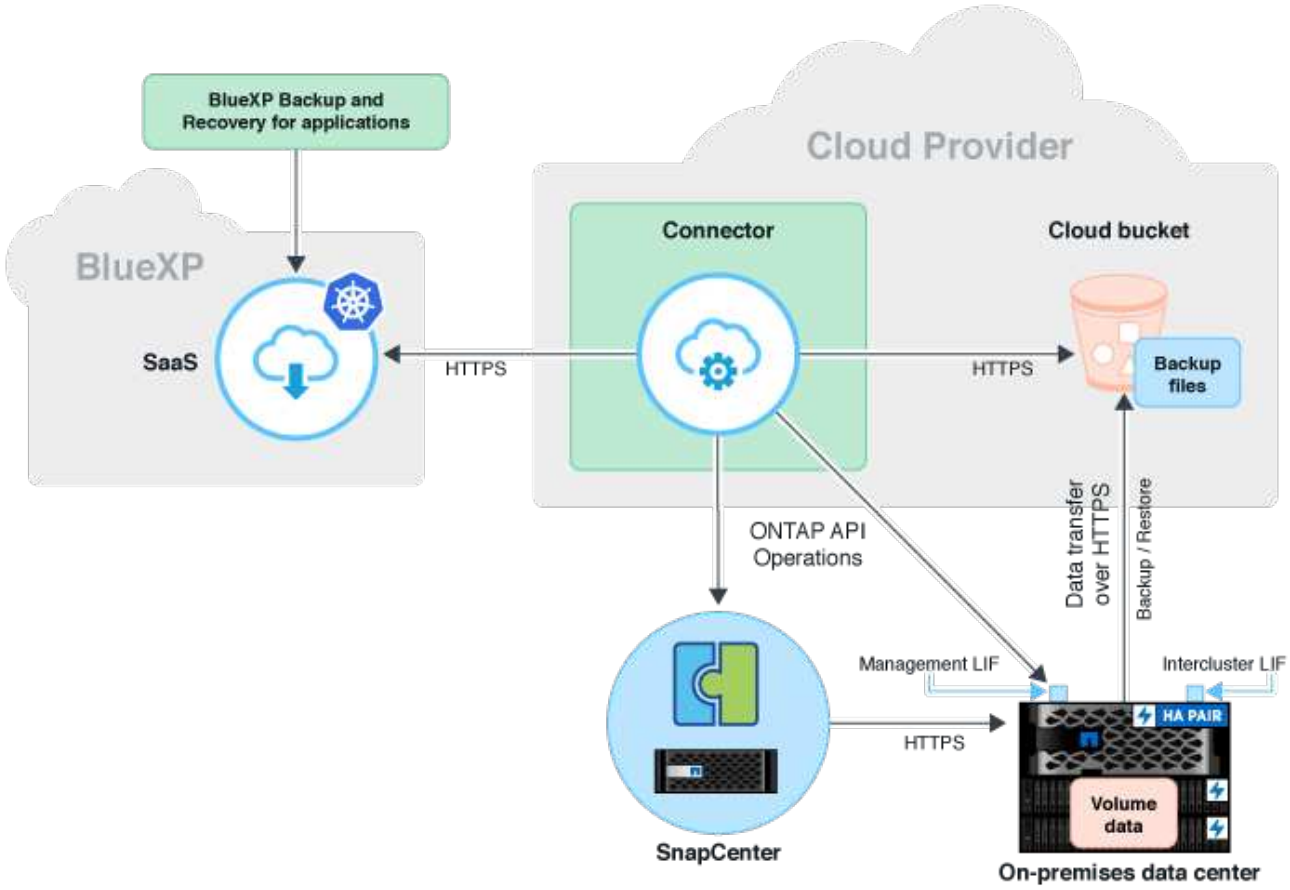
要件

クラウドプロバイダへのアプリケーションデータのバックアップを開始する前に、次の要件を読み、サポートされる構成があることを確認してください。

- ONTAP 9.8以降
- BlueXP
- SnapCenterサーバ4.6以降
  - 次の機能を使用する場合は、SnapCenterサーバ4.7以降を使用してください。
    - オンプレミスのセカンダリストレージからバックアップを保護
    - SAP HANAアプリケーションを保護
    - VMware環境上にあるOracleアプリケーションやSQLアプリケーションを保護
    - バックアップのストレージエクスポート
    - バックアップの非アクティブ化
    - SnapCenter サーバを登録解除します
  - 次の機能を使用する場合は、SnapCenterサーバ4.9以降を使用してください。
    - Oracleデータベースバックアップをマウントします
    - 代替ストレージにリストアします
  - MongoDB、MySQL、PostgreSQLのアプリケーションを保護する場合は、SnapCenter Server 4.9P1を使用する必要があります。
- SnapCenter サーバでは、各アプリケーションに使用可能なバックアップを少なくとも 1 つ用意する必要があります
- SnapCenterで、BlueXPのポリシーとラベルがない、または同じラベルのない日次、週次、または月次の

ポリシーを1つ以上設定

次の図は、クラウドにバックアップする場合の各コンポーネントと、それらの間の準備に必要な接続を示しています。



SnapCenter サーバを登録します

SnapCenterAdminロールのユーザだけが、SnapCenter サーバ4.6以降が実行されているホストを登録できます。BlueXPには複数のSnapCenter サーバホストを登録できます。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. [* 設定] ドロップダウンから、 [SnapCenter サーバ *] をクリックします。
3. [* SnapCenter サーバーの登録 *] をクリックします。
4. 次の情報を指定します。
   a. SnapCenter Server フィールドで、 SnapCenter サーバホストの FQDN または IP アドレスを指定します。
   b. [ポート]フィールドで、SnapCenter サーバホストが実行されているポート番号を指定します。

      SnapCenter サーバとBlueXPの間で通信するためには、ポートが開いていることを確認する必要があ

ります。

c. [タグ] フィールドで、 SnapCenter サーバーにタグを付けるサイト名、都市名、またはカスタム名を指定します。

   タグはカンマで区切って指定します。

d. Username and Password フィールドで、 SnapCenterAdmin ロールを持つユーザのクレデンシャルを指定します。

5. コネクター*ドロップダウンからコネクターを選択します。
6. [*Register] をクリックします。

完了後

[* バックアップと復元 **>** アプリケーション *] をクリックして、登録済み SnapCenter サーバ・ホストを使用して保護されているすべてのアプリケーションを表示します。デフォルトでは、アプリケーションは毎日午前0時に自動的に検出されます。

サポートされるアプリケーションとその構成は次のとおりです。

- Oracleデータベース：
  - フルバックアップ（データ+ログ）：少なくとも1つの日次、週次、または月次スケジュールで作成されます
  - SAN、NFS、VMDK - SAN、VMDK - NFS、RDM
- Microsoft SQL Server データベース：
  - スタンドアロン、フェイルオーバークラスタインスタンス、および可用性グループ
  - フルバックアップ：日単位、週単位、または月単位のスケジュールを少なくとも 1 つずつ設定して作成します
  - SAN、VMDK SAN、VMDK - NFS、RDM
- SAP HANAデータベース：
  - シングルコンテナ1.x
  - 複数のデータベースコンテナ2.x
  - HANAシステムレプリケーション（HSR）

    プライマリサイトとセカンダリサイトの両方に少なくとも1つのバックアップが必要です。プロアクティブな障害にするか、セカンダリへの遅延フェイルオーバーを行うかを選択できます。

  - HANAバイナリ、HANAアーカイブログボリューム、HANA共有ボリュームなどの非データボリューム（NDV）リソース
- MongoDB
- MySQL
- PostgreSQL

次のデータベースは表示されません。

- バックアップがないデータベース

- オンデマンドまたは毎時ポリシーのみのデータベース
- NVMe上にあるOracleデータベース

アプリケーションをバックアップするポリシーを作成する

アプリケーションデータをクラウドにバックアップするポリシーを作成する必要があります。

作業を開始する前に

- オブジェクトストアからアーカイブストレージにバックアップを移動する場合は、必要なバージョンのONTAPを使用していることを確認します。
  - Amazon Web Servicesを使用している場合は、ONTAP 9.10.1以降を使用している必要があります
  - Microsoft Azureを使用している場合は、ONTAP 9.10.1以降を使用している必要があります
  - Google Cloudを使用している場合は、ONTAP 9.12.1以降を使用してください
  - StorageGRIDを使用している場合は、ONTAP 9.12.1以降を使用してください。
- 各クラウドプロバイダにアーカイブアクセス階層を設定する必要があります。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. [設定]ドロップダウンから、[ポリシー>*ポリシーの作成*]をクリックします。
3. [ポリシーの詳細]セクションで、ポリシー名を指定します。
4. 保持セクションで、保持タイプの1つを選択し、保持するバックアップの数を指定します。
5. バックアップストレージソースとして、プライマリまたはセカンダリを選択します。
6. （オプション）コストを最適化するために一定の日数が経過したバックアップをオブジェクトストアからアーカイブストレージに移動する場合は、「*ティアBackup to Archival *」チェックボックスを選択します。
7. [作成（ Create ）] をクリックします。

アプリケーションに関連付けられているポリシーを編集または削除することはできません。

オンプレミスアプリケーションのデータを**Amazon Web Services**にバックアップ

いくつかの手順を実行して、ONTAP からAmazon Web Servicesにアプリケーションデータをバックアップします。

BlueXPは、データロックとランサムウェア対策をサポートしています。ONTAPクラスタがONTAP 9.11.1以降で実行されていて、アーカイブストレージを設定していない場合は、上書き、削除、ランサムウェアの脅威からバックアップを保護できます。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. をクリックします ••• アプリケーションに対応して、 * バックアップのアクティブ化 * をクリックします。
3. [ポリシーの割り当て] ページで、ポリシーを選択して [次へ *] をクリックします。
4. 作業環境を追加します。

   BlueXPで検出するクラスタ管理LIFを設定します。いずれかのアプリケーション用の作業環境を追加したら、同じ ONTAP クラスタにある他のすべてのアプリケーションでその作業環境を再利用できます。

   a. SVMを選択し、*作業環境の追加*をクリックします。
   b. 作業環境の追加ウィザードで、次の手順を実行します。
      i. クラスタ管理LIFのIPアドレスを指定します。
      ii. ONTAP クラスタユーザのクレデンシャルを指定してください。

         アプリケーション向けBlueXPのバックアップとリカバリでサポートされるのはクラスタ管理者のみです。
   c. * 作業環境の追加 * をクリックします。
5. クラウドプロバイダとして「* Amazon Web Services *」を選択します。
   a. AWS アカウントを指定します。
   b. AWS Access Key フィールドで、キーを指定します。
   c. AWS Secret Key フィールドで、パスワードを指定します。
   d. バックアップを作成するリージョンを選択します。
   e. IPスペースを指定してください。
   f. ポリシーでアーカイブストレージを設定している場合は、アーカイブ階層を選択します。

      アーカイブ階層は1回限りのアクティビティであり、あとから設定することはできないため、設定することを推奨します。
6. データロックとランサムウェア対策を設定
7. 詳細を確認し、 * バックアップのアクティブ化 * をクリックします。

オンプレミスアプリケーションのデータを**Microsoft Azure**にバックアップ

いくつかの手順を実行して、ONTAP からMicrosoft Azureにアプリケーションデータをバックアップします。

BlueXPは、データロックとランサムウェア対策をサポートしています。ONTAPクラスタがONTAP 9.12.1以降で実行されていて、アーカイブストレージを設定していない場合は、上書き、削除、ランサムウェアの脅威からバックアップを保護できます。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. をクリックします ••• アプリケーションに対応して、 * バックアップのアクティブ化 * をクリックします。
3. [ポリシーの割り当て] ページで、ポリシーを選択して [次へ *] をクリックします。
4. 作業環境を追加します。

   BlueXPで検出するクラスタ管理LIFを設定します。いずれかのアプリケーション用の作業環境を追加したら、同じ ONTAP クラスタにある他のすべてのアプリケーションでその作業環境を再利用できます。

   a. SVMを選択し、*作業環境の追加*をクリックします。
   b. 作業環境の追加ウィザードで、次の手順を実行します。
      i. クラスタ管理LIFのIPアドレスを指定します。
      ii. ONTAP クラスタユーザのクレデンシャルを指定してください。

         アプリケーション向けBlueXPのバックアップとリカバリでサポートされるのはクラスタ管理者のみです。
   c. * 作業環境の追加 * をクリックします。
5. クラウドプロバイダとして「* Microsoft Azure *」を選択します。
   a. Azure サブスクリプション ID を指定します。
   b. バックアップを作成するリージョンを選択します。
   c. 新しいリソースグループを作成するか、既存のリソースグループを使用してください。
   d. IPスペースを指定してください。
   e. ポリシーでアーカイブストレージを設定している場合は、アーカイブ階層を選択します。

      アーカイブ階層は1回限りのアクティビティであり、あとから設定することはできないため、設定することを推奨します。
6. データロックとランサムウェア対策を設定
7. 詳細を確認し、 * バックアップのアクティブ化 * をクリックします。

オンプレミスアプリケーションのデータを**Google Cloud Platform**にバックアップ

いくつかの手順を実行して、ONTAP からGoogle Cloud Platformにアプリケーションデータをバックアップします。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. をクリックします ••• アプリケーションに対応して、 * バックアップのアクティブ化 * をクリックします。
3. [ポリシーの割り当て] ページで、ポリシーを選択して [次へ *] をクリックします。

4. 作業環境を追加します。

   BlueXPで検出するクラスタ管理LIFを設定します。いずれかのアプリケーション用の作業環境を追加したら、同じ ONTAP クラスタにある他のすべてのアプリケーションでその作業環境を再利用できます。

   a. SVMを選択し、*作業環境の追加*をクリックします。
   b. 作業環境の追加ウィザードで、次の手順を実行します。
      i. クラスタ管理LIFのIPアドレスを指定します。
      ii. ONTAP クラスタユーザのクレデンシャルを指定してください。

         アプリケーション向けBlueXPのバックアップとリカバリでサポートされるのはクラスタ管理者のみです。

   c. * 作業環境の追加 * をクリックします。
5. クラウドプロバイダとして「* Google Cloud Platform *」を選択します。
   a. バックアップ用に Google Cloud Storage バケットを作成する Google Cloud Project を選択します。
   b. Google Cloud Access Keyフィールドで、キーを指定します。
   c. Google Cloud Secret Keyフィールドで、パスワードを指定します。
   d. バックアップを作成するリージョンを選択します。
   e. IPスペースを指定してください。
   f. アーカイブ階層を選択します。

      アーカイブ階層は1回限りのアクティビティであり、あとから設定することはできないため、設定することを推奨します。

6. 詳細を確認し、 * バックアップのアクティブ化 * をクリックします。

オンプレミスのアプリケーションデータを**StorageGRID** にバックアップ

アプリケーションデータをONTAP からStorageGRID にバックアップするには、いくつかの手順を実行します。

BlueXPは、データロックとランサムウェア対策をサポートしています。ONTAPクラスタがONTAP 9.11.1以降で実行されている場合、StorageGRIDシステムは11.6.0.3以降です。アーカイブストレージを設定していない場合は、上書き、削除、ランサムウェアの脅威からバックアップを保護できます。

作業を開始する前に

StorageGRID にデータをバックアップするときは、オンプレミスのコネクタが必要です。新しいコネクタをインストールするか、現在選択されているコネクタがオンプレミスにあることを確認する必要があります。コネクタは、インターネットに接続するかどうかに関係なく、サイトにインストールできます。

詳細については、を参照してください "StorageGRID のコネクタを作成します"。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. をクリックします ••• アプリケーションに対応して、 * バックアップのアクティブ化 * をクリックします。
3. [ポリシーの割り当て] ページで、ポリシーを選択して [次へ *] をクリックします。
4. 作業環境を追加します。

   BlueXPで検出するクラスタ管理LIFを設定します。いずれかのアプリケーション用の作業環境を追加したら、同じ ONTAP クラスタにある他のすべてのアプリケーションでその作業環境を再利用できます。

   a. SVMを選択し、*作業環境の追加*をクリックします。
   b. 作業環境の追加ウィザードで、次の手順を実行します。
      i. クラスタ管理LIFのIPアドレスを指定します。
      ii. ONTAP クラスタユーザのクレデンシャルを指定してください。

         アプリケーション向けBlueXPのバックアップとリカバリでサポートされるのはクラスタ管理者のみです。
   c. * 作業環境の追加 * をクリックします。
5. 「* StorageGRID *」を選択します。
   a. StorageGRID サーバのFQDNと、StorageGRID サーバが実行されているポートを指定します。

      FQDN：portの形式で詳細を入力します。
   b. [Access Key]フィールドで、キーを指定します。
   c. Secret Keyフィールドで、パスワードを指定します。
   d. IPスペースを指定してください。
   e. ポリシーでアーカイブストレージを設定している場合は、アーカイブ階層を指定します。

を選択した場合は	実行する手順
AWS	i. ドロップダウンからStorageGRIDを選択するか、StorageGRIDクラスタを追加します。 ii. AWS アカウントを指定します。 iii. AWS Access Key フィールドで、キーを指定します。 iv. AWS Secret Key フィールドで、パスワードを指定します。 v. バックアップを作成するリージョンを選択します。 vi. [保存（ Save ）] をクリックします。

を選択した場合は	実行する手順
Azure	i. ドロップダウンからStorageGRIDクラスタを選択するか、クラスタを追加します。 ii. Azure サブスクリプション ID を指定します。 iii. バックアップを作成するリージョンを選択します。 iv. 新しいリソースグループを作成するか、既存のリソースグループを使用してください。 v. [保存（ Save ）] をクリックします。

アーカイブ階層は1回限りのアクティビティであり、あとから設定することはできないため、設定することを推奨します。

6. データロックとランサムウェア対策を設定
7. 詳細を確認し、 * バックアップのアクティブ化 * をクリックします。

アプリケーションの保護を管理します

アプリケーションの保護を管理するには、ポリシーの表示、バックアップの表示、データベースレイアウト、ポリシー、リソースグループへの変更の確認、すべての処理の監視をBlueXP UIから実行します。

ポリシーを表示します

すべてのポリシーを表示できます。これらの各ポリシーについて、関連するすべてのアプリケーションの詳細を表示すると表示されます。

手順

1. [バックアップとリカバリ>*アプリケーション*]をクリックします。
2. [* 設定] ドロップダウンから、 [ポリシー *] をクリックします。
3. 詳細を表示するポリシーに対応する **View Details** をクリックします。

   関連するアプリケーションがリスト表示されます。

   アプリケーションに関連付けられているポリシーを編集または削除することはできません。

を実行して、クラウド拡張SnapCenter ポリシーを表示することもできます `Get-SmResources` SnapCenter のコマンドレット。
コマンドレットで使用できるパラメータとその説明は、Get-Helpコマンドnameで確認できます。

クラウド上のバックアップを表示します

クラウド上のバックアップは、BlueXP UIで確認できます。

手順

1. [バックアップとリカバリ>*アプリケーション*]をクリックします。
2. をクリックします ••• アプリケーションに対応して、 * 詳細を表示 * をクリックします。

> バックアップが表示されるまでの時間は、ONTAPのデフォルトのレプリケーションスケジュールによって異なります。

- Oracleデータベースの場合は、データバックアップとログバックアップの両方、各バックアップのSystem Change Number（SCN；システム変更番号）、各バックアップの終了日が表示されます。データバックアップのみを選択し、データベースを元の場所にリストアできます。データバックアップとログバックアップを別の場所にマウントできます。
- Microsoft SQL Server データベースの場合は、各バックアップのフルバックアップと終了日だけが表示されます。バックアップを選択して、元の場所または別の場所にデータベースをリストアできます。
- Microsoft SQL Serverインスタンスの場合は、そのインスタンスのデータベースのバックアップが表示されます。
- SAP HANAデータベースの場合は、各バックアップのデータバックアップと終了日だけが表示されます。バックアップを選択して、特定のホストでストレージのエクスポートを実行できます。
- MongoDB、MySQL、PostgreSQLでは、データバックアップと各バックアップの終了日のみが表示されます。バックアップを選択して、特定のホストでストレージのエクスポートを実行できます。

> クラウド保護を有効にする前に作成したバックアップはリストア対象として表示されません。

これらのバックアップは、を実行して確認することもできます `Get-SmBackup` SnapCenter のコマンドレット。
コマンドレットで使用できるパラメータとその説明は、Get-Helpコマンドnameで確認できます。

バックアップを無効にします

オブジェクトストアに移動されたバックアップは、SnapCenterとオブジェクトストアの両方から削除できます。

手順

1. [バックアップとリカバリ>*アプリケーション*]をクリックします。
2. をクリックします ••• アプリケーションに対応し、[Deactivate Backup]をクリックします。

   デフォルトではこのチェックボックスがオンになっており、オブジェクトストアに移動されたすべてのバックアップがSnapCenterとオブジェクトストアの両方から削除されます。

   チェックボックスをオフにすると、バックアップはオブジェクトストアにのみ保持されますが、アプリケーションレベルのリストアには使用できません。あとでこのアプリケーションのバックアップをアクティブ化すると、オブジェクトストアに保持されているバックアップはリストア対象のリストに表示されません。

3. [バックアップの非アクティブ化]*をクリックします。

データベースレイアウトの変更

ボリュームがデータベースに追加されると、SnapCenter サーバは、ポリシーおよびスケジュールに従って、新しいボリューム上のSnapshotに自動的にラベルを付けます。これらの新しいボリュームにはオブジェクトストアエンドポイントは設定されません。次の手順を実行してボリュームを更新する必要があります。

手順

1. [バックアップとリカバリ>*アプリケーション*]をクリックします。
2. [* 設定] ドロップダウンから、 [SnapCenter サーバ *] をクリックします。
3. をクリックします ••• アプリケーションをホストしている SnapCenter サーバーに対応し、 [更新] をクリックします。

   新しいボリュームが検出されます。

4. をクリックします ••• アプリケーションに対応し、 * 保護の更新 * をクリックして、新しいボリュームのクラウド保護を有効にします。
   - クラウドプロバイダの設定後にアプリケーションにストレージボリュームを追加すると、SnapCenter サーバは、アプリケーションが存在する新しいバックアップのラベルをSnapshotに付けます。
   - 削除したボリュームが他のアプリケーションで使用されていない場合は、オブジェクトストア関係を手動で削除する必要があります。
   - アプリケーションインベントリを更新すると、アプリケーションの現在のストレージレイアウトが反映されます。

ポリシーまたはリソースグループの変更

SnapCenter ポリシーまたはリソースグループに変更がある場合は、保護関係を更新する必要があります。

手順

1. [バックアップとリカバリ>*アプリケーション*]をクリックします。
2. をクリックします ••• アプリケーションに対応して、 [* 保護の更新 *] をクリックします。

SnapCenter サーバを登録解除します

手順

1. [バックアップとリカバリ>*アプリケーション*]をクリックします。
2. [* 設定] ドロップダウンから、 [SnapCenter サーバ *] をクリックします。
3. をクリックします ••• SnapCenter サーバーに対応して、*登録解除*をクリックします。

   デフォルトではこのチェックボックスがオンになっており、オブジェクトストアに移動されたすべてのバックアップがSnapCenterとオブジェクトストアの両方から削除されます。

   チェックボックスをオフにすると、バックアップはオブジェクトストアにのみ保持されますが、アプリケーションレベルのリストアには使用できません。あとでこのアプリケーションのバックアップをアクティブ化すると、オブジェクトストアに保持されているバックアップはリストア対象のリストに表示されません。

ジョブを監視します

すべてのクラウドバックアップ処理に対してジョブが作成されます。すべてのジョブと、各タスクの一部として実行されるすべてのサブタスクを監視できます。

手順

1. [バックアップとリカバリ>*ジョブ監視*]をクリックします。

   処理を開始すると、ジョブが開始されたことを示すウィンドウが表示されます。リンクをクリックするとジョブを監視できます。

2. プライマリタスクをクリックすると、これらの各サブタスクのサブタスクとステータスが表示されます。

CA 証明書を設定します

環境のセキュリティを強化する場合は、CA署名証明書を設定します。

BlueXP ConnectorでSnapCenterのCA署名証明書を設定します

SnapCenterの証明書を検証できるように、BlueXP ConnectorでSnapCenterのCA署名証明書を設定する必要があります。

作業を開始する前に

BlueXPコネクタで次のコマンドを実行して_<base_mount_path>_を取得する必要があります。

```
sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo
docker volume inspect | grep Mountpoint
```

手順

1. コネクタにログインします。
   ```
   cd <base_mount_path> mkdir -p server/certificate
   ```
2. ルートCAファイルと中間CAファイルを_<base_mount_path>/ server/certificate_directoryにコピーします。

   CAファイルは.pem形式である必要があります。

3. CRLファイルがある場合は、次の手順を実行します。
   a. `cd <base_mount_path> mkdir -p server/crl`
   b. <base_mount_path>ファイルを_CRL/server/crl_ディレクトリにコピーします。
4. cloudmanager_snapcenterに接続し、config.ymlのenableCACertをtrueに変更します。
   ```
   sudo docker exec -t cloudmanager_snapcenter sed -i 's/enableCACert:
   false/enableCACert: true/g' /opt/netapp/cloudmanager-
   snapcenter/config/config.yml
   ```
5. cloudmanager_snapcenterコンテナを再起動します。
   ```
   sudo docker restart cloudmanager_snapcenter
   ```

BlueXP ConnectorのCA署名証明書を設定します

SnapCenterで2way SSLが有効になっている場合、コネクタがSnapCenterに接続しているときにCA証明書を

クライアント証明書として使用するには、コネクタで次の手順を実行する必要があります。

作業を開始する前に

次のコマンドを実行して_<base_mount_path>_を取得する必要があります。

```
sudo docker volume ls | grep snapcenter_volume | awk {'print $2'} | xargs sudo
docker volume inspect | grep Mountpoint
```

手順

1. コネクタにログインします。
   ```
   cd <base_mount_path> mkdir -p client/certificate
   ```
2. CA署名証明書とキーファイルをコネクタの_<base_mount_path> / client/certificate_にコピーします。

   ファイル名はcertificate.pemとkey.pemである必要があります。certificate.pemには、中間CAやルートCAなどの証明書のチェーン全体が含まれている必要があります。

3. certificate.p12という名前でPKCS12形式の証明書を作成し、_<base_mount_path>/client/certificate__に保持してください。

   例：openssl pkcs12 -inkey key.pem -in certificate.pem -export-out certificate.p12

4. cloudmanager_snapcenterに接続し、config.ymlのsendCACertをtrueに変更します。
   ```
   sudo docker exec -t cloudmanager_snapcenter sed -i 's/sendCACert:
   false/sendCACert: true/g' /opt/netapp/cloudmanager-
   snapcenter/config/config.yml
   ```
5. cloudmanager_snapcenterコンテナを再起動します。
   ```
   sudo docker restart cloudmanager_snapcenter
   ```
6. SnapCenterで次の手順を実行して、コネクタから送信された証明書を検証します。
   a. SnapCenterサーバホストにログインします。
   b. **>**[検索の開始]*をクリックします。
   c. mmcと入力し、* Enter*キーを押します。
   d. 「 * はい * 」をクリックします。
   e. [ファイル]メニューの*[スナップインの追加と削除]*をクリックします。
   f. **>**[追加]**>**[コンピュータアカウント]**>**[次へ]*をクリックします。
   g. **>**[完了]*をクリックします。
   h. コンソールに追加するスナップインがない場合は、*[OK]*をクリックします。
   i. コンソールツリーで、*[証明書]*をダブルクリックします。
   j. [Trusted Root Certification Authorities]ストア*を右クリックします。
   k. をクリックして証明書をインポートし、[証明書のインポートウィザード]*の手順に従います。

オンプレミスアプリケーションのデータをリストア

Oracle データベースをリストアします

Oracleデータベースは元の場所にリストアすることも、別の場所にリストアすることもできます。RACデータベースの場合、バックアップが作成されたオンプレミスノードにデータがリストアされます。

制御ファイルのリストアを含むフルデータベースのみがサポートされます。アーカイブログが AFS 内にない場合は、リカバリに必要なアーカイブログが格納されている場所を指定する必要があります。

> single File Restore（SFR；単一ファイルリストア）はサポートされません。

- 手順 *

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. [* フィルター条件 *] フィールドで、フィルター * タイプ * を選択し、ドロップダウンから [* Oracle*] を選択します。
3. リストアするデータベースに対応する **View Details** をクリックし、 **Restore** をクリックします。
4. [Restore options]ページで、データベースファイルをリストアする場所を指定します。

状況	手順
元の場所にリストアします	a. [元の場所にリストア]*を選択します。 b. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。 c. 「 * 次へ * 」をクリックします。 d. データベースの状態をリストアおよびリカバリ処理の実行に必要な状態に変更する場合は、「* Database State *」を選択します。 データベースの状態は、高いレベルから順に、オープン、マウント済み、開始、シャットダウンがあります。 ◦ データベースの状態が上位で、リストア処理を実行するために下位の状態に変更する必要がある場合は、このチェックボックスを選択する必要があります。 ◦ リストア処理を実行するために、データベースの状態を低いレベルから高いレベルに変更する必要がある場合は、このチェックボックスをオンにしなくても自動的に状態が変更されます。 ◦ データベースが OPEN 状態で、リストアのためにデータベースが MOUNTED 状態である必要がある場合、データベースの状態はこのチェックボックスをオンにした場合にのみ変更されます。 e. リカバリの範囲を指定します。 ◦ 最後のトランザクションまでリカバリする場合は、*[すべてのログ]*を選択します。 ◦ 特定のSCNにリカバリする場合は、* Until SCN（System Change Number）*を選択します。 ◦ 特定のデータと時刻にリカバリする場合は、*[日付と時刻]*を選択します。 データベースホストのタイムゾーンの日付と時刻を指定する必要があります。 ◦ リカバリしない場合は*[リカバリなし]*を選択します。 f. アーカイブログがアクティブファイルシステムにない場合は、リカバリに必要なアーカイブログを格納する場所を指定する必要があります。 リカバリ後にデータベースを開く場合は、チェックボックスを選択します。 RAC セットアップでは、リカバリに使用され

状況	手順
別のストレージに一時的にリストアし、リストアしたファイルを元の場所にコピーします	a. [元の場所にリストア]*を選択します。 b. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。 c. [保存場所の変更]*を選択します。 [ストレージの場所の変更]*を選択した場合は、デスティネーションボリュームにサフィックスを追加できます。このチェックボックスをオンにしていない場合、デフォルトではデスティネーションボリュームに*_restore *が追加されます。 d. 「 * 次へ * 」をクリックします。 e. [ストレージマッピング]ページで、オブジェクトストアからリストアしたデータを一時的に格納する代替ストレージの場所の詳細を指定します。 オンプレミスのONTAPシステムを選択し、オブジェクトストレージへのクラスタ接続を設定していない場合は、オブジェクトストアに関する追加情報の入力を求められます。 f. 「 * 次へ * 」をクリックします。 g. データベースの状態をリストアおよびリカバリ処理の実行に必要な状態に変更する場合は、「* Database State *」を選択します。 データベースの状態は、高いレベルから順に、オープン、マウント済み、開始、シャットダウンがあります。 ◦ データベースの状態が上位で、リストア処理を実行するために下位の状態に変更する必要がある場合は、このチェックボックスを選択する必要があります。 ◦ リストア処理を実行するために、データベースの状態を低いレベルから高いレベルに変更する必要がある場合は、このチェックボックスをオンにしなくても自動的に状態が変更されます。 ◦ データベースが OPEN 状態で、リストアのためにデータベースが MOUNTED 状態である必要がある場合、データベースの状態はこのチェックボックスをオンにした場合にのみ変更されます。 h. リカバリの範囲を指定します。 最後のトランザクションまでリカバリする場合は、*[すべてのログ]*を選択します。

状況	手順
別の場所にリストアする	a. [別の場所にリストアする]*を選択します。 b. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。 c. 代替ストレージにリストアする場合は、次の手順を実行します。 i. [保存場所の変更]*を選択します。 [ストレージの場所の変更]*を選択した場合は、デスティネーションボリュームにサフィックスを追加できます。このチェックボックスをオンにしていない場合、デフォルトではデスティネーションボリュームに*_restore *が追加されます。 ii. 「 * 次へ * 」をクリックします。 iii. [ストレージマッピング]ページで、オブジェクトストアのデータをリストアする代替ストレージの場所の詳細を指定します。 d. 「 * 次へ * 」をクリックします。 e. [Destination host]ページで、データベースをマウントするホストを選択します。 i. （オプション）NAS環境の場合は、オブジェクトストアからリストアしたボリュームのエクスポート先となるホストのFQDNまたはIPアドレスを指定します。 ii. （オプション）SAN環境の場合は、オブジェクトストアからリストアしたボリュームのLUNをマッピングするホストのイニシエータを指定します。 f. 「 * 次へ * 」をクリックします。

5. 詳細を確認して、 * リストア * をクリックします。

[別の場所にリストア]オプションを指定すると、選択したバックアップが指定したホストにマウントされます。データベースは手動で起動する必要があります。

マウントしたバックアップは、アンマウントするまで再マウントできません。UIの* Unmount *オプションを使用して、バックアップをアンマウントできます。

Oracleデータベースを起動する方法については、を参照してください。 "ナレッジベースの記事"。

SQL Server データベースをリストアする

SQL Serverデータベースは元の場所にリストアすることも、別の場所にリストアすることもできます。

> Single File Restore（SFR；単一ファイルのリストア）、ログバックアップのリカバリ、および可用性グループの再シードはサポートされていません。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. [* フィルター条件 *] フィールドで、フィルター * タイプ * を選択し、ドロップダウンから * SQL* を選択します。
3. 「 * 詳細表示 * 」をクリックすると、使用可能なすべてのバックアップが表示されます。
4. バックアップを選択し、 * リストア * をクリックします。
5. [Restore options]ページで、データベースファイルをリストアする場所を指定します。

状況	手順
元の場所にリストアします	a. [元の場所にリストア]*を選択します。 b. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。 c. 「 * 次へ * 」をクリックします。
別のストレージに一時的にリストアし、リストアしたファイルを元の場所にコピーします	a. [元の場所にリストア]*を選択します。 b. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。 c. [保存場所の変更]*を選択します。 [ストレージの場所の変更]*を選択した場合は、デスティネーションボリュームにサフィックスを追加できます。このチェックボックスをオンにしていない場合、デフォルトではデスティネーションボリュームに*_restore *が追加されます。 d. 「 * 次へ * 」をクリックします。 e. [ストレージマッピング]ページで、オブジェクトストアからリストアしたデータを一時的に格納する代替ストレージの場所の詳細を指定します。 f. 「 * 次へ * 」をクリックします。

状況	手順
別の場所にリストアする	a. [別の場所にリストアする]*を選択します。 b. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。 c. 「 * 次へ * 」をクリックします。 d. [Destination host]ページで、ホスト名を選択し、データベース名を指定し（オプション）、インスタンスを選択し、リストアパスを指定します。 ⓘ 代替パスに指定するファイル拡張子は、元のデータベースファイルのファイル拡張子と同じにする必要があります。 e. 「 * 次へ * 」をクリックします。

状況	手順
別のストレージに一時的にリストアし、リストアしたファイルを別の場所にコピーする	a. [別の場所にリストアする]*を選択します。 b. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。 c. [保存場所の変更]*を選択します。 [ストレージの場所の変更]*を選択した場合は、デスティネーションボリュームにサフィックスを追加できます。このチェックボックスをオンにしていない場合、デフォルトではデスティネーションボリュームに*_restore *が追加されます。 d. 「 * 次へ * 」をクリックします。 e. [ストレージマッピング]ページで、オブジェクトストアからリストアしたデータを一時的に格納する代替ストレージの場所の詳細を指定します。 f. 「 * 次へ * 」をクリックします。 g. [Destination host]ページで、ホスト名を選択し、データベース名を指定し（オプション）、インスタンスを選択し、リストアパスを指定します。 ⓘ 代替パスに指定するファイル拡張子は、元のデータベースファイルのファイル拡張子と同じにする必要があります。 h. 「 * 次へ * 」をクリックします。

6. [Pre-operations]*選択で、次のいずれかのオプションを選択します。
   - [リストア時に同じ名前でデータベースを上書きする] を選択して、同じ名前でデータベースをリストアします。
   - データベースをリストアし、既存のレプリケーション設定を保持するには、「 * SQL データベースのレプリケーション設定を保持 * 」を選択します。
7. [Post-operations]セクションで、追加のトランザクションログをリストアするためのデータベースの状態を指定するには、次のいずれかのオプションを選択します。
   - 必要なすべてのバックアップを今すぐリストアする場合は、 [* Operational 、 but unavailable] を選択します。

     これはデフォルトの動作で、コミットされていないトランザクションをロールバックすることでデータベースを使用可能な状態にします。バックアップを作成するまで追加のトランザクションログはリストアできません。

- コミットされていないトランザクションをロールバックせずにデータベースを非稼働状態のままにするには、 [**Non-operational, but available**] を選択します。

  追加のトランザクションログをリストアできます。データベースはリカバリされるまで使用できません。

- データベースを読み取り専用モードのままにするには、「 * 読み取り専用モード」と「使用可能 * 」を選択します。

  コミットされていないトランザクションはロールバックされますが、ロールバックされた操作がスタンバイファイルに保存されるため、リカバリ前の状態に戻すことができます。

[ディレクトリを元に戻す] オプションが有効になっている場合は、さらに多くのトランザクションログがリストアされます。トランザクションログのリストア処理が失敗した場合は、変更をロールバックできます。詳細については、 SQL Server のマニュアルを参照してください。

8. 「 * 次へ * 」をクリックします。
9. 詳細を確認して、 * リストア * をクリックします。

SAP HANAデータベースをリストア

SAP HANAデータベースは任意のホストにリストアできます。

- 手順 *

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. フィールドで、フィルタ Type を選択し、ドロップダウンから HANA *を選択します。
3. リストアするデータベースに対応する **View Details** をクリックし、 **Restore** をクリックします。
4. [Restore options]ページで、次のいずれかを指定します。
   a. NAS環境の場合は、オブジェクトストアからリストアするボリュームのエクスポート先となるホストのFQDNまたはIPアドレスを指定します。
   b. SAN環境の場合、オブジェクトストアからリストアするボリュームのLUNをマッピングするホストのイニシエータを指定します。
5. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。
6. ソースストレージに十分なスペースがないか、ソースストレージが停止している場合は、*[ストレージの場所を変更]*を選択します。

   [ストレージの場所の変更]*を選択した場合は、デスティネーションボリュームにサフィックスを追加できます。このチェックボックスをオンにしていない場合、デフォルトではデスティネーションボリュームに*_restore *が追加されます。

7. 「 * 次へ * 」をクリックします。
8. [ストレージマッピング]ページで、オブジェクトストアからリストアしたデータを格納する代替ストレージの場所の詳細を指定します。
9. 「 * 次へ * 」をクリックします。
10. 詳細を確認して、 * リストア * をクリックします。

この処理では、指定したホスト上の選択したバックアップのストレージエクスポートのみが実行されます。ファイルシステムを手動でマウントし、データベースを起動する必要があります。ボリュームを利用したあと、ストレージ管理者はONTAP クラスタからボリュームを削除できます。

SAP HANAデータベースを起動する方法については、を参照してください。 "TR-4667：『Overview of SAP system copy workflow with SnapCenter 』" および "TR-4667：『Overview of SAP system clone workflow with SnapCenter 』"。

MongoDB、MySQL、PostgreSQLデータベースのリストア

MongoDB、MySQL、PostgreSQLのデータベースを任意のホストにリストアできます。

- 手順 *

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. フィールドで、フィルタ Type を選択し、ドロップダウンから MongoDB 、 MySQL 、または PostgreSQL *を選択します。
3. リストアするデータベースに対応する **View Details** をクリックし、 **Restore** をクリックします。
4. [Restore options]ページで、次のいずれかを指定します。
   a. NAS環境の場合は、オブジェクトストアからリストアするボリュームのエクスポート先となるホストのFQDNまたはIPアドレスを指定します。
   b. SAN環境の場合、オブジェクトストアからリストアするボリュームのLUNをマッピングするホストのイニシエータを指定します。
5. スナップショットがアーカイブストレージにある場合は、アーカイブストレージからデータをリストアする優先度を選択します。
6. ソースストレージに十分なスペースがないか、ソースストレージが停止している場合は、*[ストレージの場所を変更]*を選択します。

   [ストレージの場所の変更]*を選択した場合は、デスティネーションボリュームにサフィックスを追加できます。このチェックボックスをオンにしていない場合、デフォルトではデスティネーションボリュームに*_restore *が追加されます。

7. 「 * 次へ * 」をクリックします。
8. [ストレージマッピング]ページで、オブジェクトストアからリストアしたデータを格納する代替ストレージの場所の詳細を指定します。
9. 「 * 次へ * 」をクリックします。
10. 詳細を確認して、 * リストア * をクリックします。

この処理では、指定したホスト上の選択したバックアップのストレージエクスポートのみが実行されます。ファイルシステムを手動でマウントし、データベースを起動する必要があります。ボリュームを利用したあと、ストレージ管理者はONTAP クラスタからボリュームを削除できます。

クラウドネイティブアプリケーションデータのバックアップとリストア

クラウドネイティブアプリケーションのデータを保護

アプリケーション向けのBlueXPバックアップ/リカバリ機能は、NetAppクラウドストレージで実行されるアプリケーションに対して、アプリケーションと整合性のあるデータ保護機能を提供します。BlueXPのバックアップとリカバリでは、次のアプリケーションに対して、アプリケーションと整合性のある効率的なポリシーベースの保護を提供します。

- Amazon FSx for NetApp ONTAP 、Cloud Volumes ONTAP 、Azure NetApp Files 上にあるOracleデータベース
- Azure NetApp Files 上にあるSAP HANAシステム
- Amazon FSx for NetApp ONTAP上にあるMicrosoft SQL Serverデータベース

アーキテクチャ

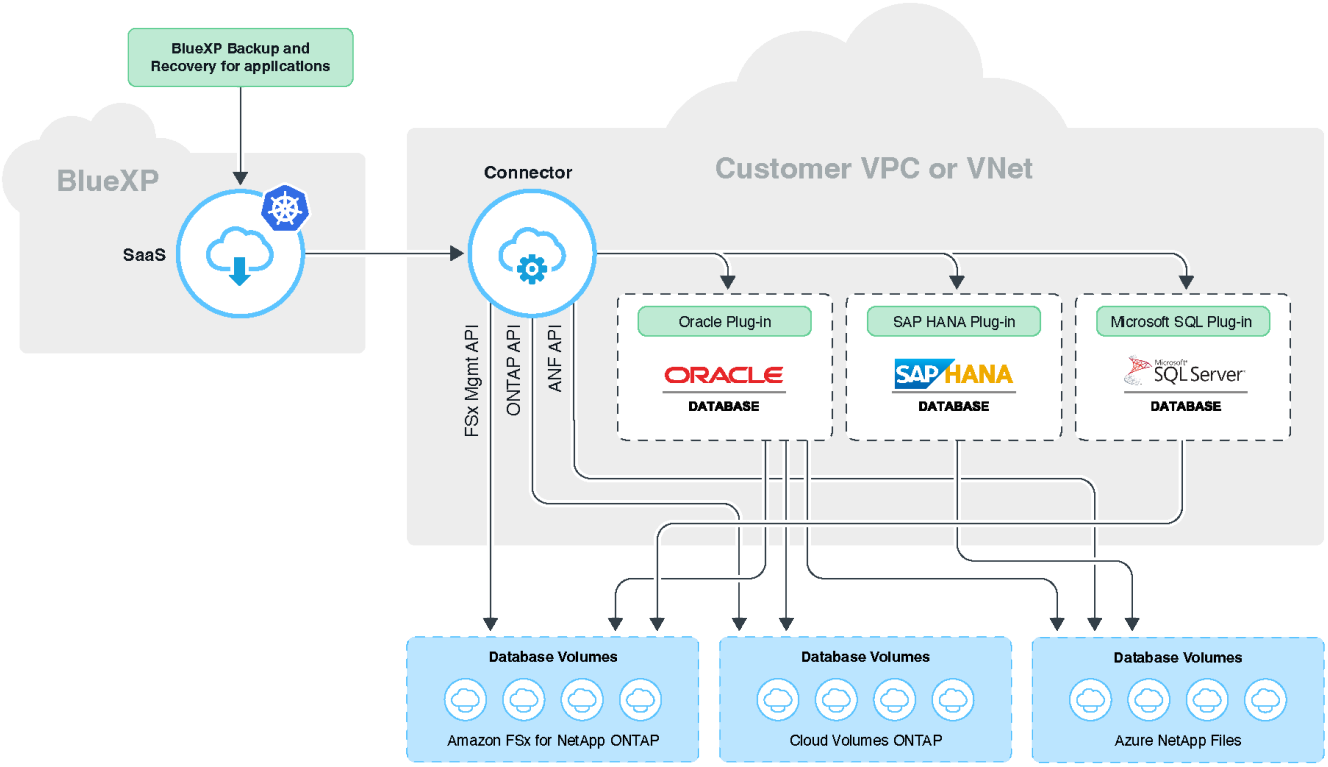
BlueXPのアプリケーション向けバックアップ/リカバリアーキテクチャには、次のコンポーネントが含まれています。

- BlueXPのバックアップとリカバリは、ネットアップがSaaSサービスとしてホストする一連のデータ保護サービスで、BlueXP SaaSプラットフォームを基盤としています。

  オーケストレーション機能を使用して、NetApp Cloud Storage上にあるアプリケーションのデータ保護ワークフローをオーケストレーションできます

- BlueXP UIはアプリケーション向けのデータ保護機能を提供し、BlueXP UIからアクセスできます。
- BlueXP Connectorは、クラウドネットワークで実行されるコンポーネントで、ストレージシステムやアプリケーション固有のプラグインと通信します。
- アプリケーション固有のプラグインは、各アプリケーションホストで実行され、データ保護処理の実行中にホストで実行されるデータベースと通信するコンポーネントです。

次の図は、各コンポーネントとその間の準備に必要な接続を示しています。



ユーザが開始した要求については、BlueXP UIがBlueXP SaaSと通信し、BlueXP UIは要求の検証時に同じ処理を行います。バックアップ、復元、クローンなどのワークフローを実行する要求がある場合、SaaSサービスはワークフローを開始し、必要に応じてコールをBlueXP Connectorに転送します。このコネクタは、ワークフロータスクの実行中にストレージシステムおよびアプリケーション固有のプラグインと通信します。

このコネクタは、アプリケーションと同じVPCまたはVNetに導入することも、別のVPCまたはVNetに導入することもできます。コネクタとアプリケーションが異なるネットワーク上にある場合は、コネクタとアプリケーションの間にネットワーク接続を確立する必要があります。

> 1つのBlueXPコネクタは、複数のストレージシステムおよび複数のアプリケーションプラグインと通信できます。コネクタとアプリケーションホストの間に接続がある限り、アプリケーションを管理するには単一のコネクタが必要です。

> BlueXP SaaSインフラは、リージョン内のアベイラビリティゾーンに障害が発生した場合の耐障害性を備えています。このフェイルオーバーは、新しいリージョンにフェイルオーバーすることで地域的な障害に対応します。そのため、2時間程度のダウンタイムが発生します。

Oracle データベースを保護します

の機能

- ホストを追加してプラグインを導入

  プラグインは、UIまたはスクリプトを使用して導入することも、手動で導入することもできます。

- Oracleデータベースの自動検出

- Amazon FSx for NetApp ONTAP 、Cloud Volumes ONTAP 、Azure NetApp Files 上にあるOracleデータベースをバックアップします
  - フル（データ+制御+アーカイブログファイル）バックアップ
  - オンデマンドバックアップ
  - システム定義またはカスタムのポリシーに基づいてスケジュールされたバックアップ

    ポリシーでは、毎時、毎日、毎週、毎月などの異なるスケジュール頻度を指定できます。バックアップの成功後に実行するポストスクリプトを指定して、Snapshotをセカンダリストレージにコピーすることもできます。
- Azure NetApp Files上のOracleデータベースのバックアップは、Oracle RMANを使用してカタログ化できます
- ポリシーに基づいてバックアップを保持する
- Amazon FSx for NetApp ONTAP 、Cloud Volumes ONTAP 、Azure NetApp Files にあるOracleデータベースのリストア
  - 指定したバックアップからOracleデータベース全体（データ・ファイル+制御ファイル）をリストアします
  - SCNまで、時間が経過するまで、使用可能なすべてのログ、およびリカバリオプションなしでOracleデータベースをリカバリする場合
- Azure NetApp Files上のOracleデータベースを別の場所にリストアしています
- Amazon FSx for NetApp ONTAP およびCloud Volumes ONTAP 上にあるOracleデータベースのソースホストまたは代替ターゲットホストへのクローニング
  - 基本的なワンクリッククローン
  - カスタムクローン仕様ファイルを使用した高度なクローニング
  - クローンエンティティ名は、自動生成することも、ソースと同一にすることもできます
  - クローン階層を表示します
  - クローンデータベースの削除
- バックアップ、リストア、クローニングなどのジョブを監視しています
- ダッシュボードに保護の概要を表示します
- E メールでアラートを送信する
- ホストプラグインをアップグレードします

制限

- Oracle 11gはサポートされません
- バックアップに対するマウント、カタログ化、検証の処理はサポートされていません
- では、RACおよびData GuardでのOracleはサポートされません
- Cloud Volumes ONTAP HAでは、ネットワークインターフェイスのIPアドレスのうち1つだけが使用されます。IPの接続がダウンした場合やIPにアクセスできない場合は、データ保護処理が失敗します。
- Amazon FSx for NetApp ONTAP またはCloud Volumes ONTAP のネットワークインターフェイスIPアドレスは、BlueXPのアカウントとリージョンで一意である必要があります。

SAP HANA データベースを保護します

の機能

- SAP HANAシステムを手動で追加
- SAP HANAデータベースのバックアップ
  - オンデマンドバックアップ（ファイルベースおよびSnapshotコピーベース）
  - システム定義またはカスタムのポリシーに基づいてスケジュールされたバックアップ

    ポリシーでは、毎時、毎日、毎週、毎月などの異なるスケジュール頻度を指定できます。

  - HANA System Replication（HSR；システムレプリケーション）対応
- ポリシーに基づいてバックアップを保持する
- 指定したバックアップからのSAP HANAデータベース全体のリストア
- HANA非データボリュームとグローバル非データボリュームのバックアップとリストア
- プリスクリプトとポストスクリプトでは、バックアップ処理とリストア処理に環境変数を使用できます
- 終了前のオプションを使用して、障害シナリオのアクションプランを作成します

制限

- HSR構成では、2ノードのHSRのみがサポートされます（1プライマリおよび1セカンダリ）。
- リストア処理中にポストスクリプトが失敗した場合、保持はトリガーされません

Microsoft SQL Serverデータベースの保護

の機能

- ホストを手動で追加してプラグインを導入する
- データベースの手動検出
- Amazon FSx for NetApp ONTAP上のSQL Serverインスタンスをバックアップ
  - オンデマンドバックアップ
  - ポリシーに基づくスケジュールされたバックアップ
  - Microsoft SQL Serverインスタンスのログバックアップ
- データベースを元の場所にリストア

制限

- バックアップはSQL Serverインスタンスに対してのみサポートされます。
- フェイルオーバークラスタインスタンス（FCI）構成はサポートされない
- BlueXP UIではSQLデータベース固有の処理がサポートされない

  Microsoft SQL Serverデータベース固有の処理は、すべてREST APIを実行して実行します。

- 別の場所へのリストアはサポートされていません

クラウドネイティブのOracleデータベースをバックアップ

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。

1 構成がサポートされていることを確認します

- オペレーティングシステム
  - RHEL 7.5以降および8.x
  - OL 7.5以降および8.x
  - SLES 15 SP4
- ネットアップのクラウドストレージ：
  - NetApp ONTAP 対応の Amazon FSX
  - Cloud Volumes ONTAP
  - Azure NetApp Files の特長
- ストレージレイアウト：
  - NFS v3およびv4.1（dNFSを含む）
  - ASMを使用するiSCSI（ASMFD、ASMLib、ASMUdev）

> Azure NetApp Files はSAN環境をサポートしていません。

- データベースレイアウト：Oracle StandardおよびOracle Enterprise Standalone（従来型およびマルチテナントCDBおよびPDB）
- データベースのバージョン：19cと21c

2 BlueXPにサインアップします

BlueXPにはWebベースのコンソールからアクセスできます。BlueXPの利用を開始するには、まず既存のNetApp Support Site クレデンシャルを使用するか、ネットアップクラウドログインアカウントを作成して登録します。詳細については、を参照してください "BlueXPにサインアップします"。

3 BlueXPにログインします

BlueXPに登録すると、Webベースのコンソールからログインできます。詳細については、を参照してください "BlueXPにログインします"。

4 BlueXPアカウントを管理します

ユーザー、サービスアカウント、ワークスペース、コネクタを管理することで、アカウントを管理できます。詳細については、を参照してください "BlueXPアカウントを管理します"。

ONTAP のFSXを設定します

BlueXPを使用してFSx for ONTAP 作業環境を作成し、ボリュームや追加のデータサービスを追加、管理する必要があります。また、AWSでコネクタを作成して、パブリッククラウド環境内のリソースとプロセスをBlueXPで管理できるようにする必要があります。

ONTAP 作業環境用のFSXを作成します

データベースがホストされているFSx for ONTAP 作業環境を作成する必要があります。詳細については、を参照してください "Amazon FSX for ONTAP の利用を開始しましょう" および "Amazon FSX for ONTAP 作業環境の作成と管理"。

FSx for ONTAP 作業環境は、BlueXPまたはAWSを使用して作成できます。AWSを使用してを作成した場合は、BlueXPのONTAP システム用FSXを検出する必要があります。

コネクタを作成します

アカウント管理者はAWSでコネクタを作成し、BlueXPでパブリッククラウド環境内のリソースとプロセスを管理する必要があります。

詳細については、を参照してください "BlueXPからAWSでコネクタを作成する"。

- FSx for ONTAP の作業環境とデータベースの管理には、同じコネクタを使用する必要があります。
- FSx for ONTAP の作業環境とデータベースが同じ仮想プライベートクラウド（VPC）内にある場合は、コネクタを同じVPCに導入できます。
- FSx for ONTAPの作業環境とデータベースが異なるVPCにある場合：
  - FSx for ONTAP でNAS（NFS）ワークロードが設定されている場合は、どちらかのVPCにコネクタを作成できます。
  - SANワークロードのみが設定されていて、NAS（NFS）ワークロードを使用する予定がない場合は、FSx for ONTAP システムが作成されたVPCにコネクタを作成する必要があります。

> NAS（NFS）ワークロードを使用する場合は、データベースVPCとAmazon VPC間のトランジットゲートウェイが必要です。フローティングIPアドレスであるNFS IPアドレスには、転送ゲートウェイ経由でのみ別のVPCからアクセスできます。VPCをピアリングしてフローティングIPアドレスにアクセスすることはできません。

コネクタを作成したら、**[**ストレージ**]**>* Canvas **>** My Working Environments **>**[Add Working Environment]*をクリックし、プロンプトに従って作業環境を追加します。
コネクタからOracleデータベースホストおよびFSx作業環境への接続が確立されていることを確認します。コネクタは、FSx作業環境のクラスタ管理IPアドレスに接続できる必要があります。

- **>** Canvas **>** My Working Environments **>**[作業環境の追加]*をクリックして、作業環境を追加します。

  コネクタからデータベースホストおよびFSx for ONTAP 作業環境への接続が確立されていることを確認します。コネクタは、FSx for ONTAP 作業環境のクラスタ管理IPアドレスに接続する必要があります。

- コネクター（Connector）>コネクターを管理（Manage Connectors）*をクリックし、コネクター名を選択して、コネクターIDをコピーします。

Cloud Volumes ONTAP を設定します

BlueXPを使用してCloud Volumes ONTAP 作業環境を作成し、ボリュームや追加のデータサービスを追加および管理する必要があります。また、BlueXPでパブリッククラウド環境内のリソースとプロセスを管理できるように、クラウド環境用のコネクタを作成する必要もあります。

Cloud Volumes ONTAP 作業環境を作成します

既存のCloud Volumes ONTAP システムを検出し、BlueXPに追加できます。詳細については、を参照してください "既存のCloud Volumes ONTAP システムをBlueXPに追加する"。

コネクタを作成します

クラウド環境向けCloud Volumes ONTAP の導入は、いくつかの手順で開始できます。詳細については、次のいずれかを参照してください。

- "AWS での Cloud Volumes ONTAP のクイックスタート"
- "Azure での Cloud Volumes ONTAP のクイックスタート"
- "Google Cloud の Cloud Volumes ONTAP のクイックスタート"

Cloud Volumes ONTAP 作業環境とデータベースの両方を管理するには、同じコネクタを使用する必要があります。

- Cloud Volumes ONTAP の作業環境とデータベースが同じVirtual Private Cloud（VPC；仮想プライベートクラウド）またはVNetにある場合は、コネクタを同じVPCまたはVNetに導入できます。
- Cloud Volumes ONTAP 作業環境があり、データベースが異なるVPCまたはVNetにある場合は、VPCまたはVNetがピアリングされていることを確認します。

Azure NetApp Files を設定します

BlueXPを使用してAzure NetApp Files 作業環境を作成し、ボリュームや追加のデータサービスを追加および管理する必要があります。Azureでコネクタを作成して、パブリッククラウド環境内のリソースとプロセスをBlueXPで管理できるようにすることも必要です。

Azure NetApp Files 作業環境を作成します

データベースがホストされているAzure NetApp Files 作業環境を作成する必要があります。詳細については、を参照してください "Azure NetApp Files の詳細をご覧ください" および "Azure NetApp Files 作業環境を作成します"。

コネクタを作成します

BlueXPのアカウント管理者は、Azureにコネクタを導入して、パブリッククラウド環境内のリソースとプロセ

スをBlueXPで管理できるようにする必要があります。

詳細については、を参照してください "BlueXPからAzureにコネクタを作成します"。

- コネクタからデータベースホストへの接続が確立されていることを確認します。
- Azure NetApp Files の作業環境とデータベースが同じ仮想ネットワーク（VNet）にある場合は、コネクタを同じVNetに導入できます。
- Azure NetApp Files 作業環境とデータベースが異なるVNetにあり、Azure NetApp Files でNAS（NFS）ワークロードが設定されている場合は、どちらかのVNetにコネクタを作成できます。

コネクタを作成したら、**[**ストレージ**]>*** Canvas **>[**マイ作業環境**]>[**作業環境の追加**]***をクリックして作業環境を追加します。

SnapCenter Plug-in for Oracleをインストールし、データベースホストを追加します

SnapCenter Plug-in for Oracleを各Oracleデータベースホストにインストールし、データベースホストを追加し、ホスト上のデータベースを検出して、ポリシーを割り当ててバックアップを作成する必要があります。

- データベースホストでSSHが有効になっている場合は、次のいずれかの方法でプラグインをインストールできます。
  - UIからSSHオプションを使用してプラグインをインストールし、ホストを追加します。 詳細はこちら。。
  - スクリプトを使用してプラグインをインストールし、手動オプションを使用してUIからホストを追加します。 詳細はこちら。。
- SSHが無効になっている場合は、プラグインを手動でインストールし、UIからmanualオプションを使用してホストを追加します。 詳細はこちら。。

前提条件

ホストを追加する前に、前提条件を満たしていることを確認する必要があります。

- 作業環境とコネクタを作成しておきます。
- コネクタがOracleデータベースホストに接続されていることを確認します。

  接続問題 を解決する方法については、を参照してください "BlueXP Connectorホストからアプリケーションデータベースホストへの接続を検証できませんでした"。

  コネクタが失われた場合、または新しいコネクタを作成した場合は、コネクタを既存のアプリケーションリソースに関連付ける必要があります。コネクタを更新する手順については、を参照してください "コネクタの詳細を更新します"。

- BlueXPユーザーに「アカウント管理者」の役割があることを確認します。
- データ保護処理用に、アプリケーションホストにroot以外の（sudo）アカウントが存在することを確認します。
- Java 11（64ビット）のOracle JavaまたはOpenJDKが各Oracleデータベースホストにインストールされていて、JAVA_HOME変数が適切に設定されていることを確認します。

- SSHベースのインストールを実行する場合は、コネクタでSSHポートへの通信が有効になっていることを確認します（デフォルト：22）。
- データ保護処理が機能するように、コネクタがプラグインポート（デフォルト：8145）との通信が有効になっていることを確認します。
- 最新バージョンのプラグインがインストールされていることを確認します。プラグインをアップグレードするには、を参照してください SnapCenter Plug-in for Oracle Databaseをアップグレードします。

SSHオプションを使用して**UI**からホストを追加します

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。

   ホストをすでに追加していて、別のホストを追加する場合は、**[**アプリケーション**]**>*[データベースの管理]*[追加]*をクリックし、手順5に進みます。

2. [アプリケーションの検出]をクリックします。
3. クラウドネイティブ*を選択し、*次へ*をクリックします。

   このアカウントのすべてのユーザに対してスケジュールされたデータ保護処理を実行するために、<accountid> SnapCenter System_Roleが割り当てられたサービスアカウント（*SnapCenter -account -system*）が作成されます。
   スケジュールされたバックアップ処理の実行には、サービスアカウント（_SnapCenter -account -<accountid> _）を使用します。サービスアカウントは絶対に削除しないでください。
   サービスアカウントを表示するには、**[**アカウント**]**>*[アカウントの管理]*[メンバー]*をクリックします。

4. アプリケーションタイプとして[Oracle]を選択します。
5. [Host details]ページで、次の手順を実行します。

   a. SSHを使用して*を選択します。
   b. プラグインをインストールするホストのFQDNまたはIPアドレスを指定します。

      コネクタがFQDNまたはIPアドレスを使用してデータベースホストと通信できることを確認します。

   c. プラグインパッケージのホストへのコピーに使用するroot以外のユーザ（sudo）を指定します。

      rootユーザはサポートされません。

   d. SSHとプラグインポートを指定します。

      デフォルトのSSHポートは22で、プラグインポートは8145です。

   プラグインをインストールしたら、アプリケーションホスト上のSSHポートを閉じることができます。SSHポートはデータ保護処理には必要ありません。

   a. コネクタを選択します。
   b. （オプション）コネクタとホストの間でキーレス認証が有効になっていない場合は、ホストとの通信に使用するSSH秘密鍵を指定する必要があります。

SSH秘密鍵はアプリケーション内のどこにも保存されず、他の操作にも使用されません。

c. 「 * 次へ * 」をクリックします。

6. [Configuration]ページで、次の手順を実行します。
   a. Oracleデータベースを実行しているLinuxマシンにログインして、Oracleデータベースホストでの SnapCenterユーザのsudoアクセスを設定します。
   b. BlueXP UIに表示されたテキストをコピーします。
   c. Linuxマシンで_/etc/sudoers.d/snapcenter_fileを作成し、コピーしたテキストを貼り付けます。
   d. BlueXP UIで、チェックボックスを選択し、*[次へ]*をクリックします。
7. 詳細を確認し、*[アプリケーションの検出]*をクリックします。
   - プラグインをインストールすると、検出処理が開始されます。
   - 検出処理が完了すると、ホスト上のすべてのデータベースが表示されます。データベースでOS認証が無効になっている場合は、*[設定]*をクリックしてデータベース認証を有効にします。詳細については、を参照してください Oracleデータベースのクレデンシャルを設定する。
   - すべてのホストを表示するには、[設定]をクリックし、[ホスト]を選択します。
   - [*設定]をクリックし、[*ポリシー]を選択して、組み込みポリシーを表示します。組み込みのポリシーを確認し、要件に合わせて編集するか、新しいポリシーを作成します。

手動オプションを使用して**UI**からホストを追加し、スクリプトを使用してプラグインをインストールします

Oracleホストのroot以外のユーザアカウントに対してSSHキーベースの認証を設定し、次の手順を実行してプラグインをインストールします。

作業を開始する前に

コネクタへのSSH接続が有効になっていることを確認します。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. [アプリケーションの検出]をクリックします。
3. クラウドネイティブ*を選択し、*次へ*をクリックします。

   このアカウントのすべてのユーザに対してスケジュールされたデータ保護処理を実行するために、<accountid> SnapCenter System_Roleが割り当てられたサービスアカウント（*SnapCenter -account -system*）が作成されます。
   スケジュールされたバックアップ処理の実行には、サービスアカウント（_SnapCenter -account -<accountid> _）を使用します。サービスアカウントは絶対に削除しないでください。
   サービスアカウントを表示するには、**[**アカウント**]**>*[アカウントの管理]*[メンバー]*をクリックします。

4. アプリケーションタイプとして[Oracle]を選択します。
5. [Host details]ページで、次の手順を実行します。
   a. [* Manual*]を選択します。
   b. プラグインがインストールされているホストのFQDNまたはIPアドレスを指定します。

コネクタがFQDNまたはIPアドレスを使用してデータベースホストと通信できることを確認します。

c. プラグインポートを指定します。

デフォルトポートは8145です。

d. プラグインパッケージのホストへのコピーに使用するroot以外のユーザ（sudo）を指定します。

e. コネクタを選択します。

f. チェックボックスを選択して、プラグインがホストにインストールされていることを確認します。

g. 「 * 次へ * 」をクリックします。

6. [Configuration]ページで、次の手順を実行します。

a. Oracleデータベースを実行しているLinuxマシンにログインして、Oracleデータベースホストでで SnapCenterユーザのsudoアクセスを設定します。

b. BlueXP UIに表示されたテキストをコピーします。

c. Linuxマシンで_/etc/sudoers.d/snapcenter_fileを作成し、コピーしたテキストを貼り付けます。

d. BlueXP UIで、チェックボックスを選択し、*[次へ]*をクリックします。

7. Connector VMにログインします。

8. コネクタに付属のスクリプトを使用してプラグインをインストールします。

```
sudo /var/lib/docker/volumes/service-manager-
2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh
--host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
--pluginport <plugin_port> --sshport <host_ssh_port>
```

古いコネクタを使用している場合は、次のコマンドを実行してプラグインをインストールします。

```
sudo
/var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plug
in_copy_and_install.sh --host <plugin_host> --username <host_user_name>
--sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
```

名前	説明	必須	デフォルト
plugin_hostの略	Oracleホストを指定します	はい。	-
host_user_nameを指定します	Oracleホストに対するSSH権限を持つSnapCenter ユーザを指定します	はい。	-
host_ssh_keyを指定します	SnapCenter ユーザのSSHキーを指定します。このキーは、Oracleホストへの接続に使用されます	はい。	-

名前	説明	必須	デフォルト
PLUGIN_PORT	プラグインで使用されるポートを指定します	いいえ	8145
host_ssh_portを指定します	OracleホストのSSHポートを指定します	いいえ	22

例：

- `sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --username snapcenter --sshkey /keys/netapp-ssh.ppk`
- `sudo /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host 10.0.1.1 --username snapcenter --sshkey /keys/netapp-ssh.ppk`

9. BlueXP UIで詳細を確認し、*[アプリケーションの検出]*をクリックします。
   - 検出処理が完了すると、ホスト上のすべてのデータベースが表示されます。データベースでOS認証が無効になっている場合は、*[設定]*をクリックしてデータベース認証を有効にします。詳細については、を参照してください Oracleデータベースのクレデンシャルを設定する。
   - すべてのホストを表示するには、[設定]をクリックし、[ホスト]を選択します。
   - [*設定]をクリックし、[*ポリシー]を選択して、組み込みポリシーを表示します。組み込みのポリシーを確認し、要件に合わせて編集するか、新しいポリシーを作成します。

手動オプションを使用して**UI**からホストを追加し、プラグインを手動でインストールします

Oracleデータベースホストで**SSH**キーベースの認証が有効になっていない場合は、次の手動手順を実行してプラグインをインストールし、manualオプションを使用してUIからホストを追加する必要があります。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
2. [アプリケーションの検出]をクリックします。
3. クラウドネイティブ*を選択し、*次へ*をクリックします。

   このアカウントのすべてのユーザに対してスケジュールされたデータ保護処理を実行するために、<accountid> SnapCenter System_Roleが割り当てられたサービスアカウント（*SnapCenter -account -system*）が作成されます。
   スケジュールされたバックアップ処理の実行には、サービスアカウント（_SnapCenter -account -<accountid> _）を使用します。サービスアカウントは絶対に削除しないでください。
   サービスアカウントを表示するには、**[**アカウント**]>***[アカウントの管理]*[メンバー]*をクリックします。

4. アプリケーションタイプとして[Oracle]を選択します。
5. [ホストの詳細]ページで、次の手順を実行します。
   a. [* Manual*]を選択します。
   b. プラグインがインストールされているホストのFQDNまたはIPアドレスを指定します。

FQDNまたはIPアドレスを使用して、コネクタがデータベースホストと通信できることを確認します。

c. プラグインポートを指定します。

デフォルトポートは8145です。

d. プラグインパッケージのホストへのコピーに使用するsudo非root（sudo）ユーザを指定します。

e. コネクタを選択します。

f. チェックボックスを選択して、プラグインがホストにインストールされていることを確認します。

g. 「 * 次へ * 」をクリックします。

6. [Configuration]ページで、次の手順を実行します。

a. Oracleデータベースを実行しているLinuxマシンにログインして、Oracleデータベースホストでの SnapCenterユーザのsudoアクセスを設定します。

b. BlueXP UIに表示されたテキストをコピーします。

c. Linuxマシンで_/etc/sudoers.d/snapcenter_fileを作成し、コピーしたテキストを貼り付けます。

d. BlueXP UIで、チェックボックスを選択し、*[次へ]*をクリックします。

7. Connector VMにログインします。

8. SnapCenter Linuxホストプラグインバイナリをダウンロードします。
```
sudo docker exec -it cloudmanager_scs_cloud curl -X GET
'http://127.0.0.1/deploy/downloadLinuxPlugin'
```

プラグインのバイナリは次の場所にあります。*cd /var/lib/docker/volumes/service-manager [1]-2_cloudmanager_SCS_cloud_volume/_data/$*（*sudo docker ps | grep -Po" cloudmanager_SCS_cloud*：。？***"|sed -e 's/**$//"| *cut-f2-d"*：*"*）*/sc-linux-host-plugin*

9. scpまたはその他の別の方法を使用して、上記のパスから各<non root user (sudo)> データベースホストの_/ home/oracle/.sc_netapp_pathに_snapcenter_linux_host_plugin_sc.bin_をコピーします。

10. root以外の（sudo）アカウントを使用してOracleデータベースホストにログインします。

11. ディレクトリを_/ home/home /<non root user> /.sc_netapp/_に変更し、次のコマンドを実行してバイナリの実行権限を有効にします。
```
chmod +x snapcenter_linux_host_plugin_scs.bin
```

12. OracleプラグインをsudO SnapCenter ユーザとしてインストールします。
```
./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root>
```

13. コネクタVMのcopy_certificate.pem_from_certificate/client/certificate/*path <base_mount_path>*をプラグインホストの/var/opt/snapcenter/spl/etc/にコピーします。

14. _/var/opt/snapcenter/spl/etcに移動し、keytoolコマンドを実行してcertificate.pemをインポートします。
```
keytool -import -alias agentcert -file certificate.pem -keystore keystore.jks
-deststorepass snapcenter -noprompt
```

15. SPLを再起動します。 `systemctl restart spl`

16. コネクタから次のコマンドを実行して、コネクタからプラグインに到達できることを確認します。
```
docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the
plug-in host>:<plug-in port>/PluginService/Version --cert
```

```
/config/client/certificate/certificate.pem --key
/config/client/certificate/key.pem
```

17. BlueXP UIで詳細を確認し、*[アプリケーションの検出]*をクリックします。
    - 検出処理が完了すると、ホスト上のすべてのデータベースが表示されます。データベースでOS認証が無効になっている場合は、*[設定]*をクリックしてデータベース認証を有効にします。詳細については、を参照してください Oracleデータベースのクレデンシャルを設定する。
    - すべてのホストを表示するには、[設定]をクリックし、[ホスト]を選択します。
    - [*設定]をクリックし、[*ポリシー]を選択して、組み込みポリシーを表示します。組み込みのポリシーを確認し、要件に合わせて編集するか、新しいポリシーを作成します。

Oracleデータベースのクレデンシャルを設定する

Oracleデータベースに対してデータ保護処理を実行する際に使用するデータベースクレデンシャルを設定する必要があります。

手順

1. データベースでOS認証が無効になっている場合は、*[設定]*をクリックしてデータベース認証を変更します。
2. ユーザ名、パスワード、およびポートの詳細を指定します。

   データベースがASMにある場合は、ASMも設定する必要があります。

   Oracleユーザにはsysdba権限が必要で、ASMユーザにはSYSASM権限が必要です。

3. [**Configure**] をクリックします。

SnapCenter Plug-in for Oracle Databaseをアップグレードします

最新の新機能や機能拡張を利用するには、SnapCenter Plug-in for Oracleをアップグレードする必要があります。BlueXP UIまたはコマンドラインを使用してアップグレードできます。

作業を開始する前に

- ホストで実行中の処理がないことを確認します。

手順

1. **>**[アプリケーション]**>**[ホスト]*をクリックします。
2. いずれかのホストでプラグインアップグレードを利用できるかどうかを[Overall Status]列で確認します。
3. UIまたはコマンドラインを使用してプラグインをアップグレードします。

UIを使用してアップグレードする	コマンドラインを使用してアップグレードします

a. をクリックします ••• ホストに対応し、*[プラグインのアップグレード]*をクリックします。
b. [Configuration]ページで、次の手順を実行します。
i. Oracleデータベースを実行しているLinuxマシンにログインして、Oracleデータベースホストで SnapCenterユーザのsudoアクセスを設定します。
ii. BlueXP UIに表示されたテキストをコピーします。
iii. Linuxマシンで_/etc/sudoers.d/snapcenter_fileを編集し、コピーしたテキストを貼り付けます。
iv. BlueXP UIで、チェックボックスを選択し、*[アップグレード]*をクリックします。
	a. コネクタVMにログインします。
	b. 次のスクリプトを実行します。
	`sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade`
	
	古いコネクタを使用している場合は、次のコマンドを実行してプラグインをアップグレードします。
	`sudo /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade`

クラウドネイティブの**Oracle**データベースをバックアップ

組み込みのポリシーまたは作成したポリシーを割り当てて、スケジュールされたバックアップまたはオンデマンドバックアップを作成できます。

ポリシーの作成時にカタログ化を有効にした場合は、Oracle Recovery Manager（RMAN）を使用してOracleデータベースバックアップをカタログ化することもできます。（RMAN）のカタログ化は、Azure NetApp Files上のデータベースでのみサポートされます。カタログ化されたバックアップは、あとでブロックレベルのリストア処理や表領域のポイントインタイムリカバリ処理に使用できます。カタログ化するためには、データベースの状態が少なくともマウント済み状態であることが必要です。

Oracleデータベースを保護するポリシーを作成します

組み込みのポリシーを編集しない場合は、ポリシーを作成できます。

- 手順 *

1. [アプリケーション]ページの[設定]ドロップダウンリストから、[ポリシー]を選択します。
2. ［ポリシーの作成］をクリックします。
3. ポリシー名を指定します。

4. （オプション）バックアップ名の形式を編集します。
5. スケジュールと保持の詳細を指定します。
6. スケジュールとして_daily_and_weekly_を 選択し、RMANカタログへの登録を有効にする場合は、*[Catalog backup with Oracle Recovery Manager（RMAN）]*を選択します。
7. （オプション）バックアップの成功後に実行するポストスクリプトのパスとタイムアウト値（Snapshotのセカンダリストレージへのコピーなど）を入力します。

   必要に応じて、引数を指定することもできます。

   ポストスクリプトは、_/var/opt/snapcenter/spl/scripts _というパスに保存する必要があります。

   POSTスクリプトは、一連の環境変数をサポートします。

環境変数	説明
SC_ORACLE_SID	OracleデータベースのSIDを指定します。
sc_hostの略	データベースのホスト名を指定します
SC_BACKUP_NAME	バックアップの名前を指定します。データバックアップ名とログバックアップ名は区切り文字で連結されます。
SC_BACKUP_POLICY_NAME	バックアップの作成に使用するポリシーの名前を指定します。
sc_primary_data_volume_full_pathを指定します	区切り文字として「、」を使用して連結されたデータボリュームパスを指定します。 Azure NetApp Filesボリュームの場合、情報はを使用して連結されます。 */subscriptions/｛subscription_id｝/resourceGroups/｛resource_group｝/providers/｛provider｝/netAppAccounts/｛anfaccount｝/capacityPools/｛capacity_pool｝/volumes/｛VolumeName｝*
sc_primary_archivelogs_volume_full_pathを指定します	区切り文字として「、」を使用して連結されたアーカイブログボリュームのパスを指定します。 Azure NetApp Filesの場合は、を使用して連結された情報 */subscriptions/｛subscription_id｝/resourceGroups/｛resource_group｝/providers/｛provider｝/netAppAccounts/｛anfaccount｝/capacityPools/｛capacity_pool｝/volumes/｛VolumeName｝*

1. [作成（ Create ）] をクリックします。

RMANカタログリポジトリを設定します

リカバリカタログデータベースをRMANカタログリポジトリとして設定できます。リポジトリを設定しない場合、デフォルトでは、ターゲット・データベースの制御ファイルがRMANカタログ・リポジトリになります。

作業を開始する前に

ターゲット・データベースをRMANカタログ・データベースに手動で登録する必要があります。

手順

1. [アプリケーション]ページで、をクリックします ••• >*詳細を表示*。
2. [Database details]セクションで、をクリックします RMANカタログリポジトリを設定するには、次の手順を実行します。
3. RMANを使用してバックアップをカタログ化するためのクレデンシャルと、カタログリカバリデータベースのTransparent Network Substrate（TNS）名を指定します。
4. [**Configure**] をクリックします。

Oracleデータベースのバックアップを作成します

組み込みのポリシーを割り当てるか、ポリシーを作成してデータベースに割り当てることができます。ポリシーを割り当てると、ポリシーで定義されたスケジュールに従ってバックアップが作成されます。

> Amazon FSx for NetApp ONTAP またはCloud Volumes ONTAP でASMディスクグループを作成する場合は、ディスクグループ間に共通のボリュームが存在しないことを確認してください。各ディスクグループに専用のボリュームを配置する必要があります。

- 手順 *

1. [アプリケーション]ページで、データベースがポリシーを使用して保護されていない場合は、[ポリシーの割り当て]をクリックします。

   データベースが1つ以上のポリシーを使用して保護されている場合は、をクリックして複数のポリシーを割り当てることができます ••• >*ポリシーの割り当て*。

2. ポリシーを選択し、* assign *をクリックします。

   バックアップは、ポリシーで定義されたスケジュールに従って作成されます。ポリシーでRMANカタログを有効にしている場合は、ワークフローの最後のバックアップでカタログ化処理が別のジョブとして起動されます。カタログ化の進捗状況はジョブモニタで確認できます。カタログ化が成功すると、*[バックアップの詳細]*に各バックアップのカタログのステータスが表示されます。

> スケジュールされたバックアップ処理の実行には、サービスアカウント（_SnapCenter -account-<account_id> _）を使用します。

Oracleデータベースのオンデマンドバックアップを作成する

ポリシーを割り当てたら、アプリケーションのオンデマンドバックアップを作成できます。

- 手順 *

1. [アプリケーション]ページで、をクリックします ••• アプリケーションに対応して、*オンデマンドバックアップ*をクリックします。
2. アプリケーションに複数のポリシーが割り当てられている場合は、ポリシーと保持階層を選択し、*[バックアップの作成]*をクリックします。

   ポリシーでRMANカタログを有効にしている場合は、ワークフローの最後のバックアップでカタログ化処理が別のジョブとして起動されます。カタログ化の進捗状況はジョブモニタで確認できます。カタログ化が成功すると、*[バックアップの詳細]*に各バックアップのカタログのステータスが表示されます。

制限

- では、FSXボリュームと重複する複数のASMディスクグループに存在するOracleデータベースの整合グループSnapshotはサポートされていません
- OracleデータベースがAmazon FSx for NetApp ONTAP またはCloud Volumes ONTAP 上にあり、ASM上に設定されている場合は、SVM名がFSxシステム全体で一意であることを確認してください。FSXシステム間でSVM名が同じ場合は、それらのSVM上にあるOracleデータベースのバックアップはサポートされません。
- 大規模なデータベース（250GB以上）をリストアしたあとに、同じデータベースでフルオンラインバックアップを実行すると、次のエラーメッセージが表示されて処理が失敗することがあります。

  ```
  failed with status code 500, error
  {\"error\":{\"code\":\"app_internal_error\",\"message\":\"Failed to create
  snapshot. Reason: Snapshot operation not allowed due to clones backed by
  snapshots. Try again after sometime.
  ```

  この問題 の修正方法については、以下を参照してください。 "Snapshotでバックアップされたクローンが原因で、Snapshot処理を実行できません"。

クラウドネイティブのSAP HANAデータベースをバックアップ

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。

1 構成がサポートされていることを確認します

- オペレーティングシステム
  - RHEL 7.6以降
  - SAP-HANA SPS07の場合はRHEL 8.1以降
  - SLES 12 SP5以降および15 SPXプラットフォームは、SAP HANAによって認定されています
- ネットアップクラウドストレージ：Azure NetApp Files
- ストレージレイアウト：データファイルとログファイルについては、Azureでサポートされるのはは NFSv4.1のみです。
- データベースレイアウト：

- シングルテナントまたは複数テナントのSAP HANAマルチテナントデータベースコンテナ（MDC）2.0SPS5、2.0SPS6、2.0SPS7
- SAP HANAシングルホストシステム、SAP HANAマルチホストシステム、HANAシステムレプリケーション

- データベースホスト上のSAP HANAプラグイン

2 **BlueXP**にサインアップします

BlueXPにはWebベースのコンソールからアクセスできます。BlueXPの利用を開始するには、まず既存のNetApp Support Site クレデンシャルを使用するか、ネットアップクラウドログインアカウントを作成して登録します。詳細については、を参照してください "BlueXPにサインアップします"。

3 **BlueXP**にログインします

BlueXPに登録すると、Webベースのコンソールからログインできます。詳細については、を参照してください "BlueXPにログインします"。

4 **BlueXP**アカウントを管理します

ユーザー、サービスアカウント、ワークスペース、コネクタを管理することで、アカウントを管理できます。詳細については、を参照してください "BlueXPアカウントを管理します"。

Azure NetApp Files を設定します

BlueXPを使用してAzure NetApp Files 作業環境を作成し、ボリュームや追加のデータサービスを追加および管理する必要があります。Azureでコネクタを作成して、パブリッククラウド環境内のリソースとプロセスをBlueXPで管理できるようにすることも必要です。

Azure NetApp Files 作業環境を作成します

データベースがホストされているAzure NetApp Files 作業環境を作成する必要があります。詳細については、を参照してください "Azure NetApp Files の詳細をご覧ください" および "Azure NetApp Files 作業環境を作成します"。

コネクタを作成します

BlueXPのアカウント管理者は、Azureにコネクタを導入して、パブリッククラウド環境内のリソースとプロセスをBlueXPで管理できるようにする必要があります。

詳細については、を参照してください "BlueXPからAzureにコネクタを作成します"。

- コネクタからデータベースホストへの接続が確立されていることを確認します。
- Azure NetApp Files の作業環境とデータベースが同じ仮想ネットワーク（VNet）にある場合は、コネクタを同じVNetに導入できます。
- Azure NetApp Files 作業環境とデータベースが異なるVNetにあり、Azure NetApp Files でNAS（NFS）ワークロードが設定されている場合は、どちらかのVNetにコネクタを作成できます。

コネクタを作成したら、**[ストレージ]>*** Canvas **>[マイ作業環境]>[作業環境の追加]***をクリックして作業環境を追加します。

SnapCenter Plug-in for SAP HANAをインストールし、データベースホストを追加します

各SAP HANAデータベースホストにSnapCenter Plug-in for SAP HANAをインストールする必要があります。SAP HANAホストでSSHキーベースの認証が有効になっているかどうかに応じて、いずれかの方法でプラグインをインストールできます。

- データベース・ホストでSSHが有効になっている場合は、SSHオプションを使用してプラグインをインストールできます。 詳細はこちら。。
- SSHが無効になっている場合は、プラグインを手動でインストールします。 詳細はこちら。。

前提条件

ホストを追加する前に、前提条件を満たしていることを確認する必要があります。

- 各SAP HANAデータベースホストにJava 11（64ビット）Oracle JavaまたはOpenJDKがインストールされていることを確認します。
- 作業環境を追加し、コネクタを作成しておく必要があります。
- コネクタがSAP HANAデータベースホストに接続されていることを確認します。

  接続問題 を解決する方法については、を参照してください "BlueXP Connectorホストからアプリケーションデータベースホストへの接続を検証できませんでした"。

  コネクタが失われた場合、または新しいコネクタを作成した場合は、コネクタを既存のアプリケーションリソースに関連付ける必要があります。コネクタを更新する手順については、を参照してください "コネクタの詳細を更新します"。

- BlueXPユーザーに「アカウント管理者」の役割があることを確認します。
- SnapCenter ユーザを作成し、root以外（sudo）ユーザにsudoを設定しておく必要があります。詳細については、を参照してください "SnapCenter ユーザにsudoを設定します。"
- データベースホストを追加する前に、SnapCenter Plug-in for SAP HANAをインストールしておく必要があります。
- SAP HANAデータベースホストを追加する場合は、HDBユーザストアキーを追加する必要があります。HDBセキュアユーザストアキーは、SAP HANAデータベースホストの接続情報をクライアントにセキュアに格納し、HDBSQLクライアントでセキュアなユーザストアキーを使用してSAP HANAデータベースホストに接続するために使用されます。
- HANA System Replication（HSR；システムレプリケーション）の場合、HANAシステムを保護するには、プライマリとセカンダリの両方のHANAシステムを手動で登録する必要があります。

  ホスト名は、HSRレプリケーションで使用されるホストのホスト名と同じである必要があります。

- SSHベースのインストールを実行する場合は、コネクタでSSHポートへの通信が有効になっていることを確認します（デフォルト：22）。

- データ保護処理が機能するように、コネクタがプラグインポート（デフォルト：8145）との通信が有効になっていることを確認します。
- 最新バージョンのプラグインがインストールされていることを確認します。プラグインをアップグレードするには、を参照してください SnapCenter Plug-in for SAP HANA Databaseをアップグレードします。

SnapCenter ユーザに**sudo**を設定します

プラグインをインストールするには、root以外のユーザ（sudo）を作成してください。

手順

1. Connector VMにログインします。
2. SnapCenter Linuxホストプラグインバイナリをダウンロードします。
   ```
   sudo docker exec -it cloudmanager_scs_cloud curl -X GET
   'http://127.0.0.1/deploy/downloadLinuxPlugin'
   ```
3. */var/lib/docker/volumes/service-manager-2_cloudmanager_SCS_cloud_volume/_data/$*（*sudo docker ps | grep -PO "cloudmanager_SCS_cloud:.*？にある *sudoer.txt* の内容をコピーします。***"|sed -e 's/$//"|*** *cut-f2-d"："*）*/sc-linux-host-plugin*
4. rootユーザアカウントを使用してSAP HANAシステムホストにログインします。
5. 手順3でコピーしたテキストを_/etc/sudoers.d/snapcenter_fileにコピーして、root以外のユーザにsudoアクセスを設定します。

   /etc/sudoers.d/snapcenter_fileに追加した行で、*<LINUXUSER>* _を*root*以外のユーザに、<USER_HOME_DIRECTORY> _を_HOME /<non-root-user> _に置き換えます。

スクリプトを使用してプラグインをインストールします

SAP HANAホストのroot以外のユーザアカウントに対してSSHキーベースの認証を設定し、次の手順を実行してプラグインをインストールします。

始める前に

コネクタへのSSH接続が有効になっていることを確認します。

手順

1. コネクタVMにログインします。
2. コネクタに付属のスクリプトを使用してプラグインをインストールします。
   ```
   sudo bash /var/lib/docker/volumes/service-manager-
   2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.sh
   --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
   --pluginport <plugin_port> --sshport <host_ssh_port>
   ```

   古いコネクタを使用している場合は、次のコマンドを実行してプラグインをインストールします。
   ```
   sudo
   /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_plug
   in_copy_and_install.sh --host <plugin_host> --username <host_user_name>
   --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
   ```

名前	説明	必須	デフォルト
plugin_hostの略	SAP HANAホストを指定します	はい。	-
host_user_nameを指定します	SAP HANAホストに対するSSH権限を持つSnapCenter ユーザを指定します	はい。	-
host_ssh_keyを指定します	SnapCenter ユーザのSSHキーを指定します。このキーは、SAP HANAホストへの接続に使用されます	はい。	-
PLUGIN_PORT	プラグインで使用されるポートを指定します	いいえ	8145
host_ssh_portを指定します	SAP HANAホストのSSHポートを指定します	いいえ	22

たとえば、'sudo bash /var/lib/docker/volumes/service-manager-2_cloudmanager_SCS_cloud_volume/_data/scripts/ linux_plugin_copy_and_install.sh --host 10.0.1.1 --username SnapCenter --sshkey/keys/netapp-ssh.ppkと入力します

プラグインをインストールしたら、インストールする必要があります SAP HANAデータベースホストを追加します。

プラグインを手動でインストールします

HANAホストでSSHキーベースの認証が有効になっていない場合は、以下の手動手順を実行してプラグインをインストールする必要があります。

- 手順 *
  1. コネクタVMにログインします。
  2. SnapCenter Linuxホストプラグインバイナリをダウンロードします。
     ```
     sudo docker exec -it cloudmanager_scs_cloud curl -X GET
     'http://127.0.0.1/deploy/downloadLinuxPlugin'
     ```
     プラグインのバイナリは次の場所にあります。*cd /var/lib/docker/volumes/service-manager-2_cloudmanager_SCS_cloud_volume/_data/$（sudo docker ps | grep -po "cloudmanager_SCS_cloud:.？* ***"\|sed -e 's/****$//'\| cut-f2-d"：*"）*/sc-linux-host-plugin*
  3. scpまたはその他の方法を使用して、各<non root user (sudo)> HANAデータベースホストの_/home/sapan/.sc_netapp_pathに上記のパスから_snapcenter_linux_host_plugin_sc.bin_をコピーします。
  4. root以外のアカウント（sudo）を使用してSAP HANAデータベースホストにログインします。

5. ディレクトリを_/ home/home /<non root user> /.sc_netapp/_に変更し、次のコマンドを実行してバイナリの実行権限を有効にします。
   ```
   chmod +x snapcenter_linux_host_plugin_scs.bin
   ```
6. sudo SnapCenter ユーザとしてSAP HANAプラグインをインストールします。
   ```
   ./snapcenter_linux_host_plugin_scs.bin -i silent -DSPL_USER=<non-root>
   ```
7. コネクタVMのcopy_certificate.pem_from_certificate/client/certificate/*path <base_mount_path>*をプラグインホストの/var/opt/snapcenter/spl/etc/にコピーします。
8. _/var/opt/snapcenter/spl/etcに移動し、keytoolコマンドを実行して証明書をインポートします。
   ```
   keytool -import -alias agentcert -file certificate.pem -keystore
   keystore.jks -deststorepass snapcenter -noprompt
   ```
9. SPLを再起動します。 `systemctl restart spl`
10. コネクタから次のコマンドを実行して、コネクタからプラグインに到達できることを確認します。
    ```
    docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the
    plug-in host>:<plug-in port>/PluginService/Version --cert
    config/client/certificate/certificate.pem --key
    /config/client/certificate/key.pem
    ```

プラグインをインストールしたら、インストールする必要があります SAP HANAデータベースホストを追加します。

SnapCenter Plug-in for SAP HANA Databaseをアップグレードします

最新の新機能や機能拡張を利用するには、SnapCenter Plug-in for SAP HANAデータベースをアップグレードする必要があります。

- 始める前に *
- ホストで実行中の処理がないことを確認します。
- 手順 *
  1. SnapCenter ユーザにsudoを設定します。詳細については、を参照してください SnapCenter ユーザにsudoを設定します。
  2. 次のスクリプトを実行します。
     ```
     /var/lib/docker/volumes/service-manager-
     2_cloudmanager_scs_cloud_volume/_data/scripts/linux_plugin_copy_and_install.
     sh --host <plugin_host> --username <host_user_name> --sshkey <host_ssh_key>
     --pluginport <plugin_port> --sshport <host_ssh_port> --upgrade
     ```

     古いコネクタを使用している場合は、次のコマンドを実行してプラグインをアップグレードします。
     ```
     /var/lib/docker/volumes/cloudmanager_scs_cloud_volume/_data/scripts/linux_pl
     ugin_copy_and_install.sh --host <plugin_host> --username <host_user_name>
     --sshkey <host_ssh_key> --pluginport <plugin_port> --sshport <host_ssh_port>
     --upgrade
     ```

SAP HANAデータベースホストを追加します

ポリシーを割り当ててバックアップを作成するには、SAP HANAデータベースホストを手動で追加する必要があります。SAP HANAデータベースホストの自動検出はサポートされていません。

- 手順 *

1. BlueXP * UIで、**[**保護**]**>***>**[アプリケーション]*を選択します。
2. [アプリケーションの検出]*を選択します。
3. Cloud Native **>** SAP HANA を選択し、 Next *を選択します。
4. [アプリケーション]ページで、*[システムの追加]*を選択します。
5. [システムの詳細*]ページで、次の操作を実行します。

   a. [System Type]で、[Multi-tenant database container]または[Global Non-Data Volumes]を選択します。

   b. SAP HANAシステムの名前を入力します。

   c. SAP HANA システムの SID を指定します。

   d. （任意）OSDBユーザを変更します。

   e. HANAシステムがHANAシステムレプリケーションで構成されている場合は、* HANA System Replication（HSR）System *を有効にします。

   f. [HDB Secure User Store Keys]*テキストボックスを選択して、ユーザストアキーの詳細を追加します。

      キー名、システムの詳細、ユーザー名、パスワードを指定し、*キーの追加*をクリックします。

   ユーザストアキーは削除または変更できます。

6. 「 * 次へ * 」を選択します。
7. [ホストの詳細]*ページで、次の操作を実行します。

   a. または[既存のホストを使用]*を選択します。

   b. または[Manual]*を選択します。

      [Manual]に、ホストのFQDNまたはIP、コネクタ、ユーザ名、SSHポート、プラグインポートを入力します。 必要に応じて、SSH秘密鍵を追加して検証します。

   SSHの場合は、ホストのFQDNまたはIP、コネクタ、ユーザ名、およびプラグインポートを入力します。

   a. 「 * 次へ * 」を選択します。

      1. [ホスト設定]ページで、設定要件を満たしているかどうかを確認します。

         確認するチェックボックスをオンにします。

      2. 「 * 次へ * 」を選択します。
      3. [ストレージフットプリント]ページで*[ストレージの追加]*を選択し、次の手順を実行します。

   b. 作業環境を選択し、ネットアップアカウントを指定します。

      左側のナビゲーションペインで、BlueXP * Canvas *を選択して新しい作業環境を追加します。

   c. 必要なボリュームを選択します。

d. [ストレージの追加]*を選択します。

    1. すべての詳細を確認し、*[システムの追加]*を選択します。

UIからSAP HANAシステムを変更または削除できます。

SAP HANAシステムを削除する前に、関連付けられているバックアップをすべて削除し、保護を解除する必要があります。

非データボリュームを追加します

マルチテナントデータベースコンテナタイプをSAP HANAシステムに追加したら、HANAシステムのデータボリューム以外のボリュームを追加できます。

使用可能な SAP HANA データベースを検出したあと、それらのリソースをリソースグループに追加してデータ保護処理を実行できます。

- 手順 *

    1. BlueXP* UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
    2. [アプリケーションの検出]をクリックします。
    3. Cloud Native **>** SAP HANA を選択し、 Next *をクリックします。
    4. [アプリケーション]ページで、をクリックします ••• 非データボリュームを追加するシステムに対応し、システム管理>*非データボリューム*を選択します。

グローバル非データボリュームの追加

マルチテナントデータベースコンテナタイプがSAP HANAシステムの追加後に、HANAシステムのグローバルデータボリューム以外のボリュームを追加できます。

- 手順 *

    1. BlueXP* UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
    2. [アプリケーションの検出]をクリックします。
    3. Cloud Native **>** SAP HANA を選択し、 Next *をクリックします。
    4. [アプリケーション]ページで、[システムの追加]をクリックします。
    5. [システムの詳細*]ページで、次の操作を実行します。

        a. System Type（システムタイプ）ドロップダウンから、* Global Non-Data Volume（グローバル非データボリューム）*を選択します。

        b. SAP HANAシステムの名前を入力します。

    6. 。[ホストの詳細]*ページで、次の操作を実行します。

        a. SAP HANAシステムの関連付けられたSIDを指定します。

        b. プラグインホストを選択します

        c. 「 * 次へ * 」をクリックします。

        d. すべての詳細を確認し、*システムの追加*をクリックします。

クラウドネイティブのSAP HANAデータベースをバックアップ

組み込みのポリシーまたは作成したポリシーを割り当てることで、バックアップを作成できます。

SAP HANAデータベースを保護するポリシーを作成します

組み込みポリシーを使用または編集しない場合は、ポリシーを作成できます。

1. [アプリケーション]ページの[設定]ドロップダウンリストから、[ポリシー]を選択します。
2. ［ポリシーの作成］をクリックします。
3. ポリシー名を指定します。
4. （オプション）Snapshotコピー名の形式を編集します。
5. ポリシータイプを選択します。
6. スケジュールと保持の詳細を指定します。
7. （任意）スクリプトを指定します。 "プリスクリプトとポストスクリプト"
8. [作成（ Create ）] をクリックします。

プリスクリプトとポストスクリプト

ポリシーの作成時にプリスクリプト、ポストスクリプト、および終了スクリプトを指定できます。 これらのスクリプトは、データ保護処理中にHANAホストで実行されます。

サポートされているスクリプトの形式は、.sh、Pythonスクリプト、perlスクリプトなどです。

プリスクリプトとポストスクリプトは、ホスト管理者がに登録する必要があります `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config` ファイル。

```
[root@scspa2622265001 etc]# cat allowed_commands.config
command: mount
command: umount
command: /mnt/scripts/pre_script.sh
command: /mnt/scripts/post_script.sh
```

環境変数

バックアップワークフローでは、プリスクリプトとポストスクリプトで次の環境変数を使用できます。

環境変数	説明
SID	リストア用に選択したHANAデータベースのシステムID
BackupNameの略	リストア処理用に選択されたバックアップ名

環境変数	説明
UserStoreKeyNames	HANAデータベース用にユーザストアキーを設定しました
OSDBUser	HANAデータベース用にOSDBUserを設定
実行します	スケジュールされたバックアップの場合のみ
schedule_type	スケジュールされたバックアップの場合のみ

SAP HANAデータベースのバックアップを作成します

組み込みポリシーを割り当てるか、ポリシーを作成してデータベースに割り当てることができます。ポリシーを割り当てると、ポリシーで定義されたスケジュールに従ってバックアップが作成されます。

- 始める前に *

SAP HANAデータベースホストを追加しておく必要があります。
"SAP HANAデータベースホストを追加します"

- このタスクについて *

HANAシステムレプリケーション（HSR）の場合、スケジュールされたバックアップジョブはプライマリHANAシステムに対してのみトリガーされ、システムがセカンダリHANAシステムにフェイルオーバーすると、既存のスケジュールによって現在のプライマリHANAシステムでバックアップがトリガーされます。ポリシーがプライマリとセカンダリの両方のHANAシステムに割り当てられていないと、フェイルオーバー後にスケジュールが失敗します。

複数のポリシーがHSRシステムに割り当てられている場合、プライマリとセカンダリの両方のHANAシステムでスケジュールされたバックアップトリガーと、セカンダリHANAシステムのバックアップは失敗します。

- 手順 *

1. [アプリケーション]ページで、データベースがポリシーを使用して保護されていない場合は、[ポリシーの割り当て]をクリックします。

   データベースは1つ以上のポリシーを使用して保護されていますが、必要に応じてをクリックして、さらにポリシーを割り当てることができます ••• >*ポリシーの割り当て*。

2. ポリシーを選択し、* assign *をクリックします。

   バックアップは、ポリシーで定義されたスケジュールに従って作成されます。

   スケジュールされたバックアップ処理の実行には、サービスアカウント（_SnapCenter -account-<account_id> _）を使用します。

SAP HANAデータベースのオンデマンドバックアップを作成する

ポリシーを割り当てたら、アプリケーションのオンデマンドバックアップを作成できます。

- 手順 *
  1. [アプリケーション]ページで、をクリックします ••• アプリケーションに対応して、*オンデマンドバックアップ*をクリックします。
  2. オンデマンドバックアップタイプを選択します。
  3. ポリシーベースのバックアップの場合、ポリシーと保持階層を選択し、*バックアップの作成*をクリックします。
  4. Snapshotコピーベースを1回選択するか、ファイルベースを選択して、次の手順を実行します。
     a. 保持値を選択し、バックアップ名を指定します。
     b. （任意）スクリプトおよびスクリプトのパスを指定します。

        詳細については、を参照してください "プリスクリプトとポストスクリプト"

     c. [バックアップの作成 *] をクリックします。

REST APIを使用してクラウドネイティブのSQL Serverデータベースをバックアップ

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。

1 構成がサポートされていることを確認します

- オペレーティングシステム
  - Windows * 2016
  - Windows 2019
  - Windows 2022
- NetAppクラウドストレージ：Amazon FSx for NetApp ONTAP
- ストレージレイアウト：SAN（iSCSI）

  NAS構成はサポートされていません。

- データベースのバージョン：
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2019
  - Microsoft SQL Server 2022
- データベース構成：
  - スタンドアロン

BlueXPにサインアップします

BlueXPにはWebベースのコンソールからアクセスできます。BlueXPの利用を開始するには、まず既存のNetApp Support Site クレデンシャルを使用するか、ネットアップクラウドログインアカウントを作成して登録します。詳細については、を参照してください "BlueXPにサインアップします"。

BlueXPにログインします

BlueXPに登録すると、Webベースのコンソールからログインできます。詳細については、を参照してください "BlueXPにログインします"。

BlueXPアカウントを管理します

ユーザー、サービスアカウント、ワークスペース、コネクタを管理することで、アカウントを管理できます。詳細については、を参照してください "BlueXPアカウントを管理します"。

ONTAP のFSXを設定します

BlueXPを使用してFSx for ONTAP 作業環境を作成し、ボリュームや追加のデータサービスを追加、管理する必要があります。また、AWSでコネクタを作成して、パブリッククラウド環境内のリソースとプロセスをBlueXPで管理できるようにする必要があります。

ONTAP 作業環境用のFSXを作成します

データベースがホストされているFSx for ONTAP 作業環境を作成する必要があります。詳細については、を参照してください "Amazon FSX for ONTAP の利用を開始しましょう" および "Amazon FSX for ONTAP 作業環境の作成と管理"。

FSx for ONTAP 作業環境は、BlueXPまたはAWSを使用して作成できます。AWSを使用してを作成した場合は、BlueXPのONTAP システム用FSXを検出する必要があります。

コネクタを作成します

アカウント管理者はAWSでコネクタを作成し、BlueXPでパブリッククラウド環境内のリソースとプロセスを管理する必要があります。

詳細については、を参照してください "BlueXPからAWSでコネクタを作成する"。

- FSx for ONTAP の作業環境とデータベースの管理には、同じコネクタを使用する必要があります。
- FSx for ONTAP の作業環境とデータベースが同じ仮想プライベートクラウド（VPC）内にある場合は、コネクタを同じVPCに導入できます。
- FSx for ONTAPの作業環境とデータベースが異なるVPCにある場合：
  - FSx for ONTAP でNAS（NFS）ワークロードが設定されている場合は、どちらかのVPCにコネクタを作成できます。
  - SANワークロードのみが設定されていて、NAS（NFS）ワークロードを使用する予定がない場合は、FSx for ONTAP システムが作成されたVPCにコネクタを作成する必要があります。

NAS（NFS）ワークロードを使用する場合は、データベースVPCとAmazon VPC間のトランジットゲートウェイが必要です。フローティングIPアドレスであるNFS IPアドレスには、転送ゲートウェイ経由でのみ別のVPCからアクセスできます。VPCをピアリングしてフローティングIPアドレスにアクセスすることはできません。

コネクタを作成したら、**[**ストレージ**]>*** Canvas **>** My Working Environments **>**[Add Working Environment]*をクリックし、プロンプトに従って作業環境を追加します。
コネクタからOracleデータベースホストおよびFSx作業環境への接続が確立されていることを確認します。コネクタは、FSx作業環境のクラスタ管理IPアドレスに接続できる必要があります。

- **>** Canvas **>** My Working Environments **>**[作業環境の追加]*をクリックして、作業環境を追加します。

  コネクタからデータベースホストおよびFSx for ONTAP 作業環境への接続が確立されていることを確認します。コネクタは、FSx for ONTAP 作業環境のクラスタ管理IPアドレスに接続する必要があります。

- コネクター（Connector）>コネクターを管理（Manage Connectors）*をクリックし、コネクター名を選択して、コネクターIDをコピーします。

SnapCenter Plug-in for SQL Serverのインストールとデータベースホストの追加

各SQLデータベースホストにSnapCenter Plug-in for SQL Serverをインストールし、データベースホストを追加し、データベースインスタンスを検出して、データベースインスタンスのクレデンシャルを設定する必要があります。

SnapCenter Plug-in for SQL Serverのインストール

プラグイン* snapcenter_service_windows_host_plugin.exe *をダウンロードしてから、サイレントインストーラコマンドを実行してデータベースホストにプラグインをインストールする必要があります。

作業を開始する前に

- 次の前提条件を満たしていることを確認する必要があります。
  - .Net 4.7.2がインストールされている
  - PowerShell 4.0がインストールされている
  - 5 GB以上のディスクスペースが利用可能です
  - 最小RAMサイズは4GBです。
- APIを実行してお客様へのオンボーディングを完了する必要があります。詳細については、以下を参照してください。 https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Tenant%20Registration/createTenant

手順

1. コネクタホストからAPIを実行してプラグインをダウンロードします。
   ```
   docker exec -it cloudmanager_scs_cloud curl
   'http://127.0.0.1/api/v2/pluginpackage/windows'
   ```

   ファイルの場所は、*/var/lib/docker/volumes/service-manager-2_cloudmanager_SCS_cloud_volume/_data/sc-windows-host-plugin/snapcenter_service_windows_host_plugin.exe*<agent_version>です。

2. scpまたはその他の代替方法を使用して、コネクタから各MSSQL Serverデータベースホストに_snapcenter_service_windows_host_plugin.exe _をコピーします。
3. プラグインをインストールします。
   '"C：//snapcenter_service_windows_host_plugin.exe"<install_folder>/silent/debuglog" C：//HA_Suite_Silent_Install_SCSQL_fresh.log <install_folder>"/log" C：//install_folder/"BI_SNAPCENTER_PORT=8145 ISFeatureInstall=SCSQL'
4. 自己署名証明書を_/var/lib/docker/volumes/service-manager-2_cloudmanager_SCS_cloud_volume/_data/client/certificate.pem_からMSSQL Serverデータベースホストにコピーします。

   デフォルトの証明書を使用しない場合は、自己署名証明書またはCA署名証明書を生成することもできます。
5. コネクタホストで、証明書を.pem形式から.crt形式に変換します。
   'openssl x509-outform der-in certificate.pem-out certificate.crt'
6. 証明書をダブルクリックして、* Personal および Trusted Root Certification Authorities *ストアに追加します。

SQL Serverデータベースホストの追加

ホストFQDNを使用してMSSQLデータベースホストを追加する必要があります。

' POST snapcenter.cloudmanager.cloud.netapp.com/api/v1/hosts'

詳細については、以下を参照してください。 https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Host%20Management/AddHosts

このAPIは、BlueXP UIの*[ジョブモニタ]*タブから追跡できるジョブを作成します。

パラメータ

名前	を入力します	必須
住所	文字列	正しいです
connector_id	文字列	正しいです
プラグインタイプ	文字列	正しいです
インストール方法	文字列	正しいです
PLUGIN_PORT	番号	正しいです
ユーザ名	文字列	正しいです

応答

APIが正常に実行されると、応答コード202が表示されます。

例

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

追加された**SQL Server**データベースホストの表示

このAPIを実行すると、追加されたすべてのSQL Serverデータベースホストを表示できます。

' snapcenter.cloudmanager.cloud.netapp.com/api/v1/hosts'を入手

詳細については、以下を参照してください。 https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Host%20Management/GetHosts

応答

APIが正常に実行されると、応答コード200が表示されます。

例

```
{
  "num_records": 1,
    "total_records": 1,
    "records": [
        {
            "id": "85bd4603-08f7-45f4-ba8e-a0b1e2a0f4d0",
            "addr": "scspa2722211001.rtp.openenglab.netapp.com",
            "status": "Running",
            "connector_id": "fBf8Iwbp4BscBfD02qBwWm6I03gGAesRclients",
            "plugin_port": 8145,
            "plugins": [
                {
                    "type": "mssql"
                }
            ],
            "os_type": "windows",
            "platform": "onprem",
            "username": "administrator",
            "operating_mode": "production"
        }
    ],
    "_links": {
        "next": {}
    }
}
```


データベースインスタンスの検出

このAPIを実行してホストIDを入力すると、すべてのMSSQLインスタンスを検出できます。

' POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances/discovery'

詳細については、以下を参照してください。 https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/MSSQLInstancesDiscoveryRequest

このAPIは、BlueXP UIの*[ジョブモニタ]*タブから追跡できるジョブを作成します。

パラメータ

名前	を入力します	必須
host_id	文字列	正しいです

応答

APIが正常に実行されると、応答コード202が表示されます。

例

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

検出されたデータベースインスタンスの表示

このAPIを実行すると、検出されたすべてのデータベースインスタンスを表示できます。

' snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances'を入手

詳細については、以下を参照してください。 https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/GetMSSQLInstancesRequest

応答

APIが正常に実行されると、応答コード200が表示されます。

例

```
{
    "num_records": 2,
    "total_records": 2,
    "records": [
        {
            "id": "953e66de-10d9-4fd9-bdf2-bf4b0eaabfd7",
            "name": "scspa2722211001\\NAMEDINSTANCE1",
            "host_id": "85bd4603-08f7-45f4-ba8e-a0b1e2a0f4d0",
            "status": "Running",
            "auth_mode": 0,
            "version": "",
            "is_clustered": false,
            "is_credentials_configured": false,
            "protection_mode": ""
        },
        {
            "id": "18e1b586-4c89-45bd-99c8-26268def787c",
            "name": "scspa2722211001",
            "host_id": "85bd4603-08f7-45f4-ba8e-a0b1e2a0f4d0",
            "status": "Stopped",
            "auth_mode": 0,
            "version": "",
            "is_clustered": false,
            "is_credentials_configured": false,
            "protection_mode": ""
        }
    ],
    "_links": {
        "next": {}
    }
}
```


データベースインスタンスのクレデンシャルの設定

このAPIを実行して、データベースインスタンスのクレデンシャルを検証および設定できます。

' POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql//api/mssql/credentials-configuration'

詳細については、以下を参照してください。 https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Instances/ConfigureCredentialRequest

このAPIは、BlueXP UIの*[ジョブモニタ]*タブから追跡できるジョブを作成します。

パラメータ

名前	を入力します	必須
host_id	文字列	正しいです
インスタンスID	文字列	正しいです
ユーザ名	文字列	正しいです
パスワード	文字列	正しいです
AUTH_MODE	文字列	正しいです

応答

APIが正常に実行されると、応答コード202が表示されます。

例

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

クラウドネイティブの**Microsoft SQL Server**データベースをバックアップ

作成したポリシーを割り当てて、スケジュールバックアップまたはオンデマンドバックアップを作成できます。

バックアップポリシーの作成

このAPIを実行してバックアップポリシーを作成できます。

' POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backup/policies'

詳細については、以下を参照してください。 https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Backup%20Policies/MSSQLBackupPolicyService_CreateMSSQLBackupPolicy

このAPIは、BlueXP UIの*[ジョブモニタ]*タブから追跡できるジョブを作成します。

パラメータ

名前	を入力します	必須
名前	文字列	正しいです
バックアップタイプ	文字列	正しいです
コピーのみのバックアップ	文字列	いいえ
is_system_defined	文字列	いいえ
backup_name_format	文字列	正しいです
schedule_type	文字列	正しいです
開始時刻	番号	正しいです
時間間隔	番号	正しいです
分間隔	番号	正しいです
保持タイプ	文字列	正しいです
保持数	番号	正しいです
終了時刻	番号	正しいです

応答

APIが正常に実行されると、応答コード201が表示されます。

例

```
{
    "_links": {
    "self": {
        "href": "/api/resourcelink"
      }
    }
}
```

SQLデータベースインスタンスへのポリシーの割り当て

このAPIを実行して、SQLデータベースインスタンスにポリシーを割り当てることができます。

' POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/instances/{id}/policy-assignment'

ここで、_id_は、DISCOVERデータベースインスタンスAPIを実行して取得したMSSQLインスタンスIDです。詳細については、を参照してください "データベースインスタンスの検出"。

ここでは、IDの配列を入力します。例：

```
[
  "c9f3e68d-1f9c-44dc-b9af-72a9dfc54320"
]
```

詳細については、以下を参照してください。 https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Policy%20Assignment/PostMSSQLInstanceAssignPolicyRequest

このAPIは、BlueXP UIの*[ジョブモニタ]*タブから追跡できるジョブを作成します。

応答

APIが正常に実行されると、応答コード202が表示されます。

例

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

オンデマンドバックアップの作成

このAPIを実行すると、オンデマンドバックアップを作成できます。

' POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups'

詳細については、以下を参照してください。 https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Backups/CreateMSSQLBackupRequest

このAPIは、BlueXP UIの*[ジョブモニタ]*タブから追跡できるジョブを作成します。

パラメータ

名前	を入力します	必須
ID これはMSSQLデータベースインスタンスのIDです。	文字列	正しいです
リソースタイプ	文字列	正しいです
policy_id	文字列	正しいです
schedule_type	文字列	正しいです

応答

APIが正常に実行されると、応答コード202が表示されます。

例

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

バックアップの表示

これらのAPIを実行すると、すべてのバックアップを一覧表示したり、特定のバックアップの詳細を表示したりできます。

' snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups'を入手

' snapcenter.cloudmanager.cloud.netapp.com/api/mssql/backups/{id}'を入手

詳細については、以下を参照してください。 https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Backups/MSSQLGetBackupsRequest

応答

APIが正常に実行されると、応答コード200が表示されます。

例

```
{
    "total_records": 1,
    "num_records": 1,
    "records": [
        {
            "backup_id": "602d7796-8074-43fc-a178-eee8c78566ac",
            "resource_id": "a779578d-cf78-46f3-923d-b9223255938c",
            "backup_name":
"Hourly_policy2_scspa2722211001_NAMEDINSTANCE1_2023_08_08_07_02_01_81269_0
",
            "policy_name": "policy2",
            "schedule_type": "Hourly",
            "start_time": "2023-08-08T07:02:10.203Z",
            "end_time": "0001-01-01T00:00:00Z",
            "backup_status": "success",
            "backup_type": "FullBackup"
        }
    ],
    "_links": {
        "next": {}
    }
}
```

クラウドネイティブのOracleデータベースをリストア

クラウドネイティブのOracleデータベースを元の場所にリストア

データ損失が発生した場合は、データファイル、制御ファイル、またはその両方を元の場所にリストアしてから、データベースをリカバリできます。

作業を開始する前に

Oracle 21cデータベースがstarted状態の場合、リストア処理は失敗します。データベースを正常にリストアするには、次のコマンドを実行する必要があります。

```
cp -f <ORACLE_HOME>/jdbc/lib/ojdbc8.jar
/opt/NetApp/snapcenter/spl/plugins/sco/lib/ojdbc8-8.jar
```

手順

1. をクリックします ••• リストアするデータベースに対応し、*[リストア]*をクリックします。
2. データベースのリストア先となるリストアポイントを選択し、*[元の場所にリストア]*をクリックします。

3. Restore Scopeセクションで、次の操作を実行します。

状況	手順
データ・ファイルだけをリストアする場合	[すべてのデータファイル]を選択します。
制御ファイルだけをリストアする場合	「制御ファイル」を選択します
データ・ファイルと制御ファイルの両方をリストアする場合	[すべてのデータファイル]および[制御ファイル]を選択します。

また、［強制的にインプレースリストア］チェックボックスをオンにすることもできます。

Amazon FSx for NetApp ONTAP またはCloud Volumes ONTAP SANレイアウトで、SnapCenter Plug-in for OracleがASMディスクグループにOracleデータファイル以外の外部ファイルを検出した場合は、接続とコピーのリストアが実行されます。外部ファイルには、次のタイプが1つ以上ある可能性があります。

- パラメータ
- パスワード
- アーカイブログ
- オンラインログ
- ASMパラメータファイル。

  [強制インプレースリストア]オプションは、パラメータ、パスワード、アーカイブ・ログ・タイプの外部ファイルを上書きします。[強制的にインプレースリストア*]オプションを選択した場合は、最新のバックアップを使用する必要があります。

4. リカバリ範囲セクションで、次の操作を実行します。

状況	手順
最後のトランザクションまでリカバリする場合	[* すべてのログ *] を選択します。
特定の System Change Number （ SCN ）までリカバリする場合	[Until SCN]*を選択し、SCNを指定します。
特定の日時にリカバリする	[* 日付と時刻 *] を選択します。
リカバリが不要である場合	「 * リカバリなし * 」を選択します。

選択したリカバリ範囲の[アーカイブ・ログ・ファイルの場所*]フィールドでは'リカバリに必要なアーカイブ・ログが格納されている場所を任意で指定できます

リカバリ後にデータベースを読み取り/書き込みモードで開く場合は、チェックボックスを選択します。

5. 「次へ」をクリックして詳細を確認します。

6. [* リストア] をクリックします。

クラウドネイティブの**Oracle**データベースを別の場所にリストア

データ損失が発生した場合、Azure NetApp FilesでのみOracleデータベースを別の場所にリストアできます。別の場所にすることも、同じホストにすることもできます。

作業を開始する前に

- Oracle 21cデータベースがstarted状態の場合、リストア処理は失敗します。データベースを正常にリストアするには、次のコマンドを実行する必要があります。
  ```
  cp -f <ORACLE_HOME>/jdbc/lib/ojdbc8.jar
  /opt/NetApp/snapcenter/spl/plugins/sco/lib/ojdbc8-8.jar
  ```
- 代替ホストのOracleバージョンが元のホストと同じであることを確認する必要があります。

このタスクについて

リストア処理の開始時に、Oracleホーム、最大ボリュームスループット、Oracle SID、およびデータベースクレデンシャル以外の構成を変更することはできません。

デフォルトでは、_until cancel_setをtrueに設定すると、フルリカバリが有効になります。

リストアされたデータベースのアーカイブログモードは、デフォルトではオフになっています。必要に応じて、アーカイブログモードを有効にして、アーカイブログをNetAppボリュームに保持できます。

手順

1. をクリックします ••• リストアするデータベースに対応し、*[リストア]*をクリックします。
2. データベースのリストア先となるリストアポイントを選択し、**[**別の場所にリストア**]**>*[次へ]*をクリックします。
3. [Configuration]ページで、代替場所、SID、ORACLE_Home、データベースクレデンシャル、およびストレージスループットの詳細を指定します。

   データベースクレデンシャルでOSユーザ認証が無効になっている場合は、リストアされたデータベースに同じホストまたはターゲットホストで接続するsysユーザのパスワードを指定する必要があります。

4. をクリックし、詳細を確認して[リストア]*をクリックします。

   リストア処理の進捗状況は、[Job Monitor]ページで確認できます。ジョブが完了したら、*[検出のリフレッシュ]*をクリックして、リストアされたデータベースを表示します。ただし、別の場所にリストアされたデータベースを保護することはできません。

クラウドネイティブの**SAP HANA**データベースをリストア

データ損失が発生した場合は、データファイルと非データファイルをリストアしてから、データベースをリカバリできます。

- 始める前に *
- SAP HANAシステムは停止状態である必要があります。

- SAP HANAシステムが稼働している場合は、システムを停止するプリスクリプトを指定できます。
- このタスクについて *
- ボリュームでANFバックアップを有効にすると、Single File SnapRestore処理が実行されます。
- 非データボリュームおよびグローバル非データボリュームの場合は、接続およびコピーリストア処理が実行されます。
  - 接続リストア処理とコピーリストア処理のQuality of Service（QoS；サービス品質）値は、データボリューム以外のボリュームまたはグローバルデータボリューム以外のボリュームのソースボリュームから取得されます。

> QoSは、タイプが「手動」の容量プールにのみ適用されます。

- 手順 *

1. をクリックします ••• リストアするデータベースに対応して、*詳細の表示*をクリックします。
2. をクリックします ••• リストアするデータバックアップに対応し、*[リストア]*をクリックします。
3. [* Restore System*（システムの復元）]ページで、スクリプトを入力します。 "プリスクリプトとポストスクリプト"

   リストアワークフローでは、プリスクリプトとポストスクリプトの一部として次の環境変数を使用できます。

環境変数	説明
SID	リストア用に選択したHANAデータベースのシステムID
BackupNameの略	リストア処理用に選択されたバックアップ名
UserStoreKeyNames	HANAデータベース用にユーザストアキーを設定しました
OSDBUser	HANAデータベース用にOSDBUserを設定

1. [* リストア] をクリックします。

次のステップ

リストアが完了したら、SAP HANAシステムを手動でリカバリするか、ポストスクリプトを指定してSAP HANAシステムのリカバリを実行します。

非データボリュームをリストアします

- このタスクについて *

接続とコピーのリストア処理については、Microsoft Azureポータルにアクセスしてボリュームを選択し、**[**編集**]***をクリックして[Snapshotパスを隠す]*を有効にします。

- 手順 *
  1. [**Applications**]ページで、ドロップダウンボックスから[Non-Data Volume]を選択します。
  2. をクリックします ••• リストアするバックアップに対応して、*リストア*をクリックします。

グローバルな非データボリュームをリストアします

- このタスクについて *

接続とコピーのリストア処理については、Microsoft Azureポータルにアクセスしてボリュームを選択し、**[**編集**]***をクリックして[Snapshotパスを隠す]*を有効にします。

- 手順 *
  1. [*アプリケーション]ページで、リストアするグローバル非データ・ボリュームをクリックします。
  2. をクリックします ••• リストアするグローバル非データボリュームに対応し、*リストア*をクリックします。

Microsoft SQL Serverテタヘスノリストア

Microsoft SQL Serverデータベースは同じホストにリストアできます。まずデータベースのリストを取得してから、データベースをリストアする必要があります。

データベースのリストを表示する

このAPIを実行すると、データベースのリストを表示できます。

' snapcenter.cloudmanager.cloud.netapp.com/api/mssql/databases'を入手

詳細については、以下を参照してください。 https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Databases/GetMSSQLDatabasesRequest

応答

APIが正常に実行されると、応答コード200が表示されます。

例

```
{
    "num_records": 3,
    "total_records": 3,
    "records": [
        {
            "id": "348901e5-aeaa-419f-88b1-80240de3b1fe",
            "name": "DB4",
            "hostname": "scspa2722211001.rtp.openenglab.netapp.com",
            "size": 0.078125,
            "instance_id": "454c8413-5351-41fc-88bf-f20fb050ec87",
            "instance": "scspa2722211001\\NAMEDINSTANCE1",
            "db_status": "Normal",
            "db_access": "eUndefined",
            "db_type": "User",
            "recovery_mode": "Full"
        },
        {
            "id": "c79d33ab-7322-4ed6-92f5-51ad7a6944e0",
            "name": "DB5",
            "hostname": "scspa2722211001.rtp.openenglab.netapp.com",
            "size": 0.078125,
            "instance_id": "454c8413-5351-41fc-88bf-f20fb050ec87",
            "instance": "scspa2722211001\\NAMEDINSTANCE1",
            "db_status": "Normal",
            "db_access": "eUndefined",
            "db_type": "User",
            "recovery_mode": "Full"
        },
        {
            "id": "40d6f35a-f4fb-48bc-8e0a-0ac93ddf0888",
            "name": "model",
            "hostname": "scspa2722211001.rtp.openenglab.netapp.com",
            "size": 0.015625,
            "instance_id": "454c8413-5351-41fc-88bf-f20fb050ec87",
            "instance": "scspa2722211001\\NAMEDINSTANCE1",
            "db_status": "Normal",
            "db_access": "eUndefined",
            "db_type": "System",
            "recovery_mode": "Full"
        }
    ],
    "_links": {
        "next": {}
    }
}
```

MSSQLデータベースのリストアとリカバリ

このAPIを実行してMSSQLデータベースを復元できます。

' POST snapcenter.cloudmanager.cloud.netapp.com/api/mssql/databases/{id}/restore'

ここで、_id_は、ビューデータベースAPIを実行して取得したMSSQLデータベースIDです。詳細については、を参照してください [データベースのリストを表示する]。

詳細については、以下を参照してください。 https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/MSSQL%20Database%20Restore/RestoreMSSQLDatabaseRequest

このAPIは、BlueXP UIの*[ジョブモニタ]*タブから追跡できるジョブを作成します。

パラメータ

名前	を入力します	必須
バックアップID	文字列	正しいです
上書きデータベース	ブール値	正しいです
retain_replication_settings	ブール値	いいえ
リカバリモード	文字列 サポートされている文字列は、*Operational*、*Nonoperational*、および_ReadOnly_です。	正しいです
undo_file_directory	文字列	正しいです
リストアタイプ	文字列	正しいです

応答

APIが正常に実行されると、応答コード202が表示されます。

例

```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  }
}
```

クラウドネイティブな**Oracle**データベースをクローニング

クローンの概念と要件

データベースのバックアップを使用して、Amazon FSx for NetApp ONTAP またはCloud Volumes ONTAP 上のOracleデータベースをソースデータベースホストまたは代替ホストにクローニングできます。バックアップはプライマリストレージシステムからクローニングできます。

データベースをクローニングする前に、クローンの概念を理解し、すべての要件を満たしていることを確認する必要があります。

Oracle データベースをクローニングするための要件

Oracle データベースをクローニングする前に、前提条件を満たしていることを確認する必要があります。

- データベースのバックアップを作成しておく必要があります。
  クローニング処理を正常に実行するには、オンラインデータとログバックアップが正常に作成されている必要があります。
- asm_diskstringパラメータでは、次の設定を行う必要があります。
  - AFD：* ASMFDを使用している場合
  - ORCL:* ASMlibを使用している場合
  - ASMUDEV <exact_device_location> を使用している場合は/dev/ASMUDEVを使用します
- 代替ホストでクローンを作成する場合、代替ホストは次の要件を満たす必要があります。
  - プラグインは代替ホストにインストールする必要があります。
  - Oracleソフトウェアは代替ホストにインストールする必要があります。
  - iSCSI SANストレージ上にあるデータベースのクローニングを行う場合は、クローンホストでストレージからLUNを検出できる必要があります。
    代替ホストにクローニングする場合は、ストレージと代替ホストの間にiSCSIセッションが確立されていることを確認します。
  - ソースデータベースが ASM データベースの場合は、次の手順を実行します。

- クローンを実行するホスト上で、 ASM インスタンスが稼働している必要があります。
- クローニングしたデータベースのアーカイブログファイルを専用のASMディスクグループに配置する場合は、クローン処理の前にASMディスクグループをプロビジョニングする必要があります。
- データディスクグループの名前は設定できますが、クローンを実行するホスト上の他のASMディスクグループに名前が使用されていないことを確認してください。
- ASMディスクグループにあるデータファイルは、クローンワークフローの一環としてプロビジョニングされます。

制限

- Azure NetApp Files 上にあるデータベースのクローニングはサポートされていません。
- qtreeにあるデータベースのクローニングはサポートされていません。
- クローンデータベースのバックアップはサポートされていません。
- Amazon FSx for NetApp ONTAPで日次自動バックアップが有効になっている場合、Amazon FSx for NetApp ONTAPではクローンボリューム上にバックアップが作成されるため、BlueXP UIからクローンボリュームを削除できません。
  FSx UIからボリュームのバックアップをすべて削除したあとにクローンボリュームを削除し、その後forceオプションを使用してBlueXP UIからクローンを削除する必要があります。

クローンメソッド

基本的な方法またはクローン仕様ファイルを使用して、クローンを作成できます。

基本的な方法でクローニングします

ソースデータベースと選択したバックアップを基に、デフォルトの設定でクローンを作成できます。

- データベースパラメータ、ホーム、およびOSユーザは、デフォルトでソースデータベースに設定されます。
- データファイルパスの名前は、選択した名前スキームに基づいて決まります。
- プリスクリプト、ポストスクリプト、およびSQLステートメントは指定できません。
- リカバリ・オプションは’デフォルトでは* Until cancel *であり’データ・バックアップに関連付けられたログ・バックアップをリカバリに使用します

仕様ファイルを使用してクローニングする

クローン仕様ファイルで設定を定義し、それを使用してデータベースをクローニングできます。仕様ファイルをダウンロードし、要件に合わせて変更してから、ファイルをアップロードできます。 "詳細はこちら。"。

仕様ファイルに定義されているさまざまなパラメーターと、変更可能なパラメーターは次のとおりです。

パラメータ	説明
control_files	クローンデータベースの制御ファイルの場所。 制御ファイルの数はソースデータベースと同じになります。 制御ファイルのパスを無効にする場合は、別の制御ファイルのパスを指定します。ファイルシステムまたはASMディスクグループがホストに存在する必要があります。
REDOログ	REDOログの場所、サイズ、Redoグループの数。 データベースをクローニングするには、少なくとも 2 つの REDO ログループが必要です。REDOログファイルのパスを上書きする場合は、ソースデータベースとは別のファイルシステムにREDOログファイルのパスをカスタマイズできます。ファイルシステムまたはASMディスクグループはホストに存在する必要があります。
ORACLE_VERSION	ターゲット・ホスト上のOracleのバージョン。
ORACLE_HOMEを参照してください	ターゲット・ホストのOracleホーム
enable_archive_log_mode	クローンデータベースのアーカイブログモードを制御します
databE_parameters	クローンデータベースのデータベースパラメータ
SQL_statements	クローニング後にデータベースで実行するSQLステートメント
os_user_detail	ターゲットクローンデータベースのOracle OSユーザ
databa_port	ホストでOS認証が無効な場合に、データベースとの通信に使用するポート。
asm_portのようになります	Create Clone入力にクレデンシャルが指定されている場合に、ASMデータベースとの通信に使用するポート。
skip_recovery	はリカバリ処理を実行しません。
Until SCN	指定したSystem Change Number（SCN）までデータベースをリカバリします。

パラメータ	説明
until _ time	指定した日時までデータベースをリカバリします。 指定できる形式は、_mm/dd/yyyy hh：mm：ss_です。
until _ cancel	クローニング対象として選択したデータバックアップに関連付けられたログバックアップをマウントすることでリカバリできます。 クローンデータベースは、欠落または破損したログファイルまでリカバリされます。
LOG_PATHS	クローンデータベースのリカバリに使用するアーカイブログパスの追加場所。
source_locationのコマンドを使用します	ソースデータベースホスト上のディスクグループまたはマウントポイントの場所。
clone_location	ソースの場所に対応するターゲットホストに作成する必要があるディスクグループまたはマウントポイントの場所。
location_type	asm_diskgroupまたはmountpointを指定できます。 値は、ファイルのダウンロード時に自動的に入力されます。このパラメータは編集しないでください。
pre_script	クローンを作成する前にターゲットホストで実行するスクリプト。
post_script	クローン作成後にターゲットホストで実行するスクリプト。
パス	クローンホスト上のスクリプトの絶対パス。 スクリプトは、/var/opt/snapcenter/spl/scriptsまたはこのパス内の任意のフォルダに保存してください。
タイムアウト	ターゲットホストで実行されているスクリプトに対して指定されたタイムアウト時間。
引数	スクリプトに指定された引数。

クローンの命名方式

クローンの命名スキームは、マウントポイントの場所と、クローニングされたデータベースのディスクグルー

プの名前を定義します。「同一」または「自動生成」のいずれかを選択できます。

同一の命名方式

クローンの命名方式として「* identical *」を選択した場合、クローニングされたデータベースのマウントポイントの場所とディスクグループの名前は、ソースデータベースと同じになります。

たとえば、ソースデータベースのマウントポイントが、クローンデータベースの_____oursourcedb/data_1、+DATA1_DG_である場合、SANのNFSとASMの両方のマウントポイントは同じままです。

- 制御ファイルやREDOファイルの数やパスなどの構成はソースと同じになります。

> REDOログまたは制御ファイルのパスがデータボリューム以外に存在する場合は、ターゲットホストにASMディスクグループまたはマウントポイントをプロビジョニングしておく必要があります。

- Oracle OSユーザとOracleバージョンはソースデータベースと同じになります。
- クローンストレージボリューム名は、sourceVolNameSCS_Clone_CurrentTimeStampNumberという形式になります。

  たとえば、ソースデータベース上のボリューム名が_sourceVolName_の場合、クローンボリューム名は_sourceVolNameSCS_Clone_1661420020304608825_になります。

> CurrentTimeStampNumber_はボリューム名に一意性を示します。

自動生成される命名方式

クローニングスキームとして*自動生成*を選択した場合、マウントポイントの場所とクローニングされたデータベースのディスクグループの名前にはサフィックスが付加されます。

- 基本的なクローニング方法を選択した場合、接尾辞に*クローンSID *が付加されます。
- 仕様ファイル方式を選択した場合、クローン仕様ファイルのダウンロード時に指定した*サフィックス*がサフィックスとして付加されます。

たとえば、ソースデータベースのマウントポイントが_/NetApp_sourcedb/data_1_and the * Clone SID * or * Suffix * is_HR_の場合、クローンデータベースのマウントポイントは_/NetApp_sourcedb/data_1_HR_に なります。

- 制御ファイルとREDOログファイルの数がソースと同じになります。
- すべてのREDOログファイルと制御ファイルは、クローニングされたデータマウントポイントまたはデータASMディスクグループのいずれかに配置されます。
- クローンストレージボリューム名は、sourceVolNameSCS_Clone_CurrentTimeStampNumberという形式になります。

  たとえば、ソースデータベース上のボリューム名が_sourceVolName_の場合、クローンボリューム名は_sourceVolNameSCS_Clone_1661420020304608825_になります。

> CurrentTimeStampNumber_はボリューム名に一意性を示します。

- NASマウントポイントの形式は、_SourceNASMountPoint_suffix_です。
- ASMディスクグループの形式は、_SourceDiskgroup_suffix_です。

> クローンディスクグループ内の文字数が25文字を超える場合は、_SC_hashCode_suffix_が付けられます。

データベースパラメータ

次のデータベース・パラメータの値は、クローンの命名方式に関係なく、ソース・データベースの値と同じになります。

- LOG_ARCH_FORMATの略
- audit_trail
- プロセス
- PGAアグリゲート・ターゲット
- remote_login_passwordfileを指定します
- undo_tablespace
- オープンカーソル
- SGAターゲット
- DB_BLOBK_SIZE

次のデータベースパラメータの値には、クローンのSIDに基づくサフィックスが付加されます。

- audit_file_dest = ｛sourcedatabase-parameteralue｝サフィックス
- LOG_ARCHIVE _ dest_1 = ｛sourcedatabase-oraclehome｝サフィックス

特定のプリスクリプトとポストスクリプトのクローニングでサポートされる事前定義された環境変数

データベースのクローニングの実行時にプリスクリプトとポストスクリプトを実行する場合は、サポートされる事前定義された環境変数を使用できます。

- sc_original_SIDには、ソースデータベースのSIDを指定します。
  このパラメータは、アプリケーションボリュームに対して入力されます。例：NFSB32
- sc_original_hostは、ソースホストの名前を指定します。
  このパラメータは、アプリケーションボリュームに対して入力されます。例
  ：asmrac1.gdl.englab.netapp.com
- SC_ORACLE_HOMEは’ターゲット・データベースのOracleホーム・ディレクトリのパスを指定します
  例： /ora01/app/oracle/product/18.1.0/db_1
- sc_backup_nameには、バックアップの名前を指定します。
  このパラメータは、アプリケーションボリュームに対して入力されます。例
  - データベースがARCHIVELOGモードで実行されていない場合：DATA @RG2_scspr2417819002_07-020-202021 _ 116.9267_0 | LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267 _1
  - データベースがARCHIVELOGモードで実行されている場合：DATA @RG2_scspr2417819002_07-020-20-220_1120_116.9267_0 | LOG @RG2_scspr2417819002_07-07-20-20-

220_112_112.16.48.9267_1、Rg2_scspr24002_06_24002_0.262.16002_0.262.16002_0.7_2.168.262.162.168.261_2.24002_0.21_2.168.262.168.262.168.262_0.7_2.24002_0.262.168.

- sc_original_os_userは、ソースデータベースのオペレーティングシステム所有者を指定します。
  例： oracle
- sc_original_os_groupは、ソースデータベースのオペレーティングシステムグループを指定します。
  例： oinstall
- sc_target_SIDには、クローンデータベースのSIDを指定します。
  PDB クローンワークフローの場合、このパラメータの値は事前定義されていません。このパラメータは、アプリケーションボリュームに対して入力されます。
  例： clonedb
- sc_target_hostは、データベースをクローニングするホストの名前を指定します。
  このパラメータは、アプリケーションボリュームに対して入力されます。例
  ：asmrac1.gdl.englab.netapp.com
- sc_target_os_userは、クローンデータベースのオペレーティングシステムの所有者を指定します。
  PDB クローンワークフローの場合、このパラメータの値は事前定義されていません。例： oracle
- sc_target_os_groupには、クローンデータベースのオペレーティングシステムグループを指定します。
  PDB クローンワークフローの場合、このパラメータの値は事前定義されていません。例： oinstall
- sc_target_db_portは、クローンデータベースのデータベースポートを指定します。
  PDB クローンワークフローの場合、このパラメータの値は事前定義されていません。例： 1521

サポートされるデリミタ

- @は、データベース名からデータを分離し、キーから値を分離するために使用されます。
  例：data@RG2_scspr2417819002_07-08-202021 _116.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267 _1
- |は、SC_backup_nameパラメータに2つのエンティティ間でデータを分離するために使用します。
  例：DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267 _0 | LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267 _1
- は、同じキーに対して一連の変数を区切るために使用します。
  例：data@RG2_scspr2417819002_07-02-20-20-220_116.9267_0|log@RG2_scspr2417819002_07-07-20-20-220_116.9267_1, RG2_scspr2417819002_07-02-21-2202.16_222.168.261_222.168.262_002_0.24002_0.262_0.261_2.168.262_0.172.168.262_0.264_002_0.172.168.262_0.7_122_0.262_0.262_0.262_0.262_0.262_

クラウドネイティブな**Oracle**データベースをクローニング

データベースのバックアップを使用して、Amazon FSx for NetApp ONTAP またはCloud Volumes ONTAP 上のOracleデータベースをソースデータベースホストまたは代替ホストにクローニングできます。

データベースをクローニングする理由には次のものがあります。

- アプリケーション開発のライフサイクルで、実装が必要な機能を、現在のデータベースの構造およびコンテンツを使用してテストするため。
- データの抽出と操作を行うツールを使用してデータウェアハウスにデータを取り込むため。
- 誤って削除または変更されたデータをリカバリするため。

作業を開始する前に

クローンの概念を理解し、すべての要件を満たしていることを確認する必要があります。 "詳細はこちら。"。

手順

1. をクリックします ••• クローニングするデータベースに対応し、*詳細の表示*をクリックします。
2. をクリックします ••• データバックアップに対応し、* Clone *をクリックします。
3. Clone Detailsページで、いずれかのクローンオプションを選択します。
4. 選択したオプションに応じて、次の操作を実行します。

選択した項目	手順
• 基本 *	a. クローンホストを選択します。 代替ホスト上にクローンを作成する場合は、ソース・データベース・ホストと同じバージョンの Oracle および OS を持つホストを選択します。 b. クローンの SID を指定します。 c. クローンの命名方式を選択します。 データベースをソースホストにクローニングすると、クローンの命名規則が自動生成されます。データベースを代替ホストにクローニングすると、クローンの命名規則が同一になります。 d. Oracleホームパスを指定します。 e. （任意）データベースクレデンシャルを指定します。 ◦ データベースクレデンシャル：OSユーザ認証が無効になっている場合は、sysユーザが同じホストまたはターゲットホスト上のクローンデータベースに接続するためのパスワードを指定する必要があります。 ◦ ASMクレデンシャル：ターゲットホストでOSユーザ認証が無効になっている場合は、ターゲットホストのASMインスタンスに接続するために、SYSASM特権ユーザのクレデンシャルを指定する必要があります。 ⓘ ターゲット・ホストでリスナーが稼働していることを確認します f. 「 * 次へ * 」をクリックします。 g. [* Clone*] をクリックします。

選択した項目	手順
仕様ファイル	a. [ファイルのダウンロード（Download File）]をクリックして、仕様ファイルをダウンロードします。 b. クローンの命名方式を選択します。 「自動生成」を選択した場合は、サフィックスを指定する必要があります。 c. 要件に応じて仕様ファイルを編集し、*参照*ボタンをクリックしてアップロードします。 d. クローンホストを選択します。 代替ホスト上にクローンを作成する場合は、ソース・データベース・ホストと同じバージョンの Oracle および OS を持つホストを選択します。 e. クローンの SID を指定します。 f. （任意）データベースクレデンシャルを指定します。 ◦ データベースクレデンシャル：OSユーザ認証が無効になっている場合は、sysユーザが同じホストまたはターゲットホスト上のクローンデータベースに接続するためのパスワードを指定する必要があります。 ◦ ASMクレデンシャル：ターゲットホストでOSユーザ認証が無効になっている場合は、ターゲットホストのASMインスタンスに接続するために、SYSASM特権ユーザのクレデンシャルを指定する必要があります。 ターゲット・ホストでリスナーが稼働していることを確認します g. 「 * 次へ * 」をクリックします。 h. [* Clone*] をクリックします。

5. をクリックします [フィルタ]の横にある[*クローニング・オプション>*クローン*]を選択して、クローンを表示します。

SAP HANAターゲットシステムを更新

SAP HANAソースシステムのデータを使用して、SAP HANAターゲットシステムの更新

を実行できます。これを使用して、現在の本番環境のデータをテストシステムに提供できます。BlueXPのバックアップとリカバリでは、ソースシステムからSnapshotコピーを選択し、そのSnapshotコピーに基づいて新しいAzure NetApp Filesボリュームを作成できます。サンプルのスクリプトを使用して、SAP HANAデータベースをリカバリするためにデータベースホストで必要な処理を実行します。

- 始める前に *
- 最初の更新処理を実行する前に、SAP HANAターゲットシステムをインストールする必要があります。
- ソースとターゲットのHANAシステムをBlueXPのバックアップとリカバリに手動で追加する必要があります。
- ソースシステムとターゲットシステムでSAP HANAデータベースのバージョンが同じであることを確認します。
- 使用する更新スクリプトを決定しておく必要があります。更新スクリプトは、解決策 テクニカルレポートで提供されています。

  "自動化スクリプトの例"

  更新スクリプトはカスタマイズできます。

- プリスクリプトとポストスクリプトでは、次の環境変数を使用できます。
  - cloned_volumes_mount_pathを指定します
  - <SOURCEVOLUME> の宛先
  - hana_database_typeを指定します
  - tenant_database_namesの略
- プラグインをバージョン3.0にアップグレードする必要があります。
- マウントパスは、ソースとターゲットの両方のSAP HANAシステムのデータボリュームで同じである必要があります。
- 最初の更新処理の前に、「/etc/fstab」ファイルにターゲットSAP HANAシステムのデータボリュームのエントリがないことを確認してください。
- このタスクについて *
- システム更新は、マルチテナントデータベースコンテナHANAシステムでのみサポートされます。
- 既存のポリシーはシステムの更新後に有効になります。
- 新しいボリュームには、<sourcevolumename> -<timestamp> という命名規則が適用されます
  - タイムスタンプの形式：<year> <month> <day> -<hour> <minute> <second>

    たとえば、ソースボリュームがvol1の場合、更新されるボリューム名はvol1-20230109-184501になります

> 新しいボリュームは、ターゲットボリュームと同じ容量プールに配置されます。

- ジャンクションパスはボリューム名と同じになります。
- 新しいボリュームの「最大スループット数」は、手動のQuality of Service（QoS；サービス品質）容量プ

ールを含むターゲットシステムのボリュームから選択されます。
自動QoS容量プールの場合、スループットはソースボリュームの容量で定義されます。

- システムの更新時に、スクリプトではなくワークフローを使用してボリュームの自動マウントおよびアンマウントが実行されます。
- 手順 *
  1. BlueXP UIで、[保護>*バックアップとリカバリ*>*アプリケーション*]をクリックします。
  2. [アプリケーション]ページで、をクリックします ••• アイコンをクリックして、更新するシステムに対応するアクションを選択し、*[システムの更新]*を選択します。
  3. [システムの更新]*ページで、次の操作を実行します。
     a. ソースシステムとSnapshotコピーを選択
     b. （オプション）新しいボリュームにアクセスできるエクスポートアドレスを入力します。
     c. （任意）Maximum storage throughput（MIB;最大ストレージスループット）を入力します。
     d. プリスクリプト、ポストスクリプト、およびエラーが発生したスクリプトパスを入力します。
     失敗時スクリプトは、システム更新処理が失敗した場合にのみ実行されます。
     e. [* 更新 *] をクリックします。

クラウドネイティブアプリケーションデータの保護を管理

ジョブを監視する

作業環境で開始されたジョブのステータスを監視できます。これにより、正常に完了したジョブ、現在実行中のジョブ、および失敗したジョブを表示できるため、問題を診断して修正できます。

> スケジュール済みジョブは、ジョブ完了時刻から5分（最大）後にBlueXPの[Job Monitor]ページに表示されます。

詳細については、を参照してください "ジョブステータスを監視します"。

Oracleデータベースホストのメンテナンス

管理者は、データベースホストを手動でメンテナンスモードにして、ホストでメンテナンスタスクを実行できます。アップグレード中はホストが自動的にメンテナンスモードになり、アップグレード後は自動的に本番モードに切り替わります。

ホストをメンテナンスモードにすると、オンデマンド処理が失敗し、スケジュールされたジョブがスキップされます。

> ホストをメンテナンスモードにする前に、そのホスト上のリソースに対するジョブが実行中かどうかを確認することはできません。

手順

1. BlueXP UIで、**[保護]>*>**[アプリケーション]*をクリックします
2. アプリケーションタイプとして* Oracle *を選択します。

3. >[ホスト]*をクリックします。
4. 次のいずれかを実行します。

状況	手順
ホストをメンテナンスモードにする	をクリックします ••• ホストに対応し、*[メンテナンスモードを有効にする]*を選択します。
ホストをメンテナンスモードから戻す	をクリックします ••• メンテナンス中のホストに対応し、*[メンテナンスモードを無効にする]*を選択します。

監査データ

APIを直接実行するか、UIを使用して、アプリケーション向けにBlueXPの外部に公開されているAPIのいずれかにAPI呼び出しを行うと、ヘッダー、ロール、要求の本文、 また、API情報はBlueXPのタイムラインに記録され、監査エントリはタイムラインに永久に保持されます。API呼び出しのステータスとエラー応答も、処理の完了後に監査されます。ジョブなどの非同期API応答の場合、ジョブIDも応答の一部としてログに記録されます。

アプリケーション向けBlueXPのバックアップ/リカバリでは、ホストIP、要求の本文、処理名、トリガー日時、一部のヘッダー、 およびAPIの動作状態。

バックアップの詳細を表示します

作成されたバックアップの総数、バックアップの作成に使用されたポリシー、データベースのバージョン、およびエージェントIDを表示できます。

手順

1. [バックアップとリカバリ>*アプリケーション*]をクリックします。
2. をクリックします ••• アプリケーションに対応して、 * 詳細を表示 * をクリックします。

> エージェントIDはコネクタに関連付けられています。SAP HANAホストの登録時に使用したコネクタが存在しない場合、新しいコネクタのエージェントIDが異なるため、そのアプリケーションの以降のバックアップは失敗します。ホストのコネクタIDを変更する必要があります。詳細については、を参照してください [コネクタの詳細を更新します]。

クローンを削除します

不要になったクローンは削除できます。

手順

1. をクリックします + [フィルターの基準]の隣にある[*複製オプション>*親の複製*]を選択します。
2. をクリックします ••• アプリケーションに対応して、 * 詳細を表示 * をクリックします。
3. Database Details（データベースの詳細）ページで、をクリックします + [フィルターの基準]の隣にあ

る[*クローン]を選択します。

4. をクリックします ••• 削除するクローンに対応し、* Delete *をクリックします。
5. （オプション）* force delete *チェックボックスを選択します。

コネクタの詳細を更新します

アプリケーションホストの登録時に使用されたコネクタが存在しないか破損している場合は、新しいコネクタを導入する必要があります。新しいコネクタを導入したら、* connector-update * APIを実行して、古いコネクタを使用して登録されているすべてのホストのコネクタの詳細を更新する必要があります。

OracleホストまたはSAP HANAホストのコネクタの詳細を更新したら、次の手順を実行してコネクタの詳細が正常に更新されたことを確認します。

手順

1. BlueXP Connector VMにログインし、次の手順を実行します。
   a. コネクタから次のコマンドを実行して、コネクタからプラグインに到達できることを確認します。
   ```
   docker exec -it cloudmanager_scs_cloud curl -ik https://<FQDN or IP of the
   plug-in host>:<plug-in port>/getVersion
   --cert/config/client/certificate/certificate.pem
   --key/config/client/certificate/key.pem
   ```
   b. ベースマウントパスを取得します。
   ```
   sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs
   sudo docker volume inspect | grep Mountpoint
   ```
   c. コネクタVMの_pem <base_mount_path>/client/certificate/*path*からプラグインホストの/var/opt/snapcenter/spl/etc/にcertificate.pemをコピーします。
2. プラグインホストにログインし、次の手順を実行します。
   a. _/var/opt/snapcenter/spl/etc _に移動し、keytoolコマンドを実行して証明書.pemファイルをインポートします。
   ```
   keytool -import -alias agentcert -file certificate.pem -keystore
   keystore.jks -deststorepass snapcenter -noprompt
   ```
   b. SPLを再起動します。 `systemctl restart spl`
   c. 次のいずれかを実行します。

使用する環境	手順
Oracleデータベースホスト	i. すべてのを確認します "前提条件" 達成された。 ii. >[アプリケーション]*をクリックします iii. をクリックします ••• アプリケーションに対応して、 * 詳細を表示 * をクリックします。 iv. コネクターID *を修正します。

使用する環境	手順
SAP HANAデータベースホスト	i. すべてのを確認します "前提条件" 達成された。 ii. 次のコマンドを実行します。 `curl --location --request PATCH 'https://snapcenter.cloudmanager.cloud.netapp.com/api/saphana/hosts/connector/update' \ --header 'x-account-id: <CM account-id>' \ --header 'Authorization: Bearer token' \ --header 'Content-Type: application/json' \ --data-raw '{ "old_connector_id": "Old connector id that no longer exists", "new_connector_id": "New connector Id"}'` すべてのホストにSnapCenter Plug-in for SAP HANAサービスがインストールされて実行されている場合や、すべてのホストに新しいコネクタからアクセスできる場合は、コネクタの詳細が更新されます。

CA署名証明書を設定します

環境のセキュリティを強化する場合は、CA署名証明書を設定します。

BlueXP ConnectorのCA署名証明書を設定します

コネクタは、自己署名証明書を使用してプラグインと通信します。自己署名証明書は、インストールスクリプトによってキーストアにインポートされます。自己署名証明書をCA署名証明書に置き換えるには、次の手順を実行します。

手順

1. コネクタがプラグインに接続しているときにCA証明書をクライアント証明書として使用するには、コネクタで次の手順を実行します。
   a. コネクタにログインします。
   b. 次のコマンドを実行して_<base_mount_path>_を取得します。
   `sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs`

```
sudo docker volume inspect | grep Mountpoint
```

c. コネクタの_<base_mount_path> /client/certificate_inにある既存のファイルをすべて削除します。

d. CA署名証明書とキーファイルをコネクタの_<base_mount_path> / client/certificate_にコピーします。

   ファイル名はcertificate.pemとkey.pemである必要があります。certificate.pemには、中間CAやルートCAなどの証明書のチェーン全体が含まれている必要があります。

e. certificate.p12という名前でPKCS12形式の証明書を作成し、_<base_mount_path>/client/certificate__に保持してください。

   例：openssl pkcs12 -inkey key.pem -in certificate.pem -export-out certificate.p12

2. プラグインホストで次の手順を実行して、コネクタから送信された証明書を検証します。

   a. プラグインホストにログインします。

   b. すべての中間CAとルートCAの証明書.pemと証明書をコネクタからプラグインホスト（*/var/opt/snapcenter/spl/etc/*）にコピーします。

      中間CA証明書とルートCA証明書の形式は.crt形式である必要があります。

   c. _/var/opt/snapcenter/spl/etc _に移動し、keytoolコマンドを実行して証明書.pemファイルをインポートします。
      ```
      keytool -import -alias agentcert -file certificate.pem -keystore
      keystore.jks -deststorepass snapcenter -noprompt
      ```

   d. ルートCAと中間証明書をインポートします。
      ```
      keytool -import -trustcacerts -keystore keystore.jks -storepass snapcenter
      -alias trustedca -file <certificate.crt>
      ```

      certificate.crtは、ルートCAと中間CAの証明書を参照します。

   e. SPLを再起動します。 `systemctl restart spl`

プラグインの**CA**署名証明書を設定します

CA証明書の名前は、プラグインホストのCloud Backupに登録されている名前と同じである必要があります。

手順

1. CA証明書を使用してプラグインをホストするには、プラグインホストで次の手順を実行します。

   a. SPLのkeystore _/var/opt/snapcenter/spl/etc _が格納されているフォルダに移動します。

   b. 証明書とキーの両方を持つ証明書のPKCS12形式を、alias_splkeystore._で作成します。

      certificate.pemには、中間CAやルートCAなどの証明書のチェーン全体が含まれている必要があります。

   例：openssl pkcs12 -inkey key.pem -in certificate.pem -export-out certificate.p12 -name splkeystore

   a. 上記の手順で作成したCA証明書を追加します。
      ```
      keytool -importkeystore -srckeystore certificate.p12 -srcstoretype pkcs12
      ```

```
-destkeystore keystore.jks -deststoretype JKS -srcalias splkeystore
-destalias splkeystore -noprompt
```

b. 証明書を確認します。
```
keytool -list -v -keystore keystore.jks
```

c. SPLを再起動します。 `systemctl restart spl`

2. コネクタで次の手順を実行して、コネクタがプラグインの証明書を確認できるようにします。

a. root以外のユーザとしてコネクタにログインします。

b. 次のコマンドを実行して_<base_mount_path>_を取得します。
```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs
sudo docker volume inspect | grep Mountpoint
```

c. serverディレクトリの下にあるルートCAファイルと中間CAファイルをコピーします。
```
cd <base_mount_path>
mkdir server
```

CAファイルはPEM形式である必要があります。

d. cloudmanager_scs_cloudに接続し、* enableCACert * in_config.yml_to * true *を変更します。
```
sudo docker exec -t cloudmanager_scs_cloud sed -i 's/enableCACert:
false/enableCACert: true/g' /opt/netapp/cloudmanager-scs-
cloud/config/config.yml
```

e. cloudmanager_scs_cloudコンテナを再起動します。
```
sudo docker restart cloudmanager_scs_cloud
```

REST APIにアクセスできます

アプリケーションをクラウドで保護するREST APIには、次のURLからアクセスできます。https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/。

REST APIにアクセスするには、フェデレーテッド認証を使用してユーザトークンを取得する必要があります。ユーザートークンの取得方法については、を参照してください "フェデレーテッド認証を使用してユーザトークンを作成します"。

仮想マシンのデータのバックアップとリストア

仮想マシンのデータを保護

BlueXPの仮想マシン向けバックアップ/リカバリ機能は、データストアのバックアップとリストアを通じてデータを保護します。

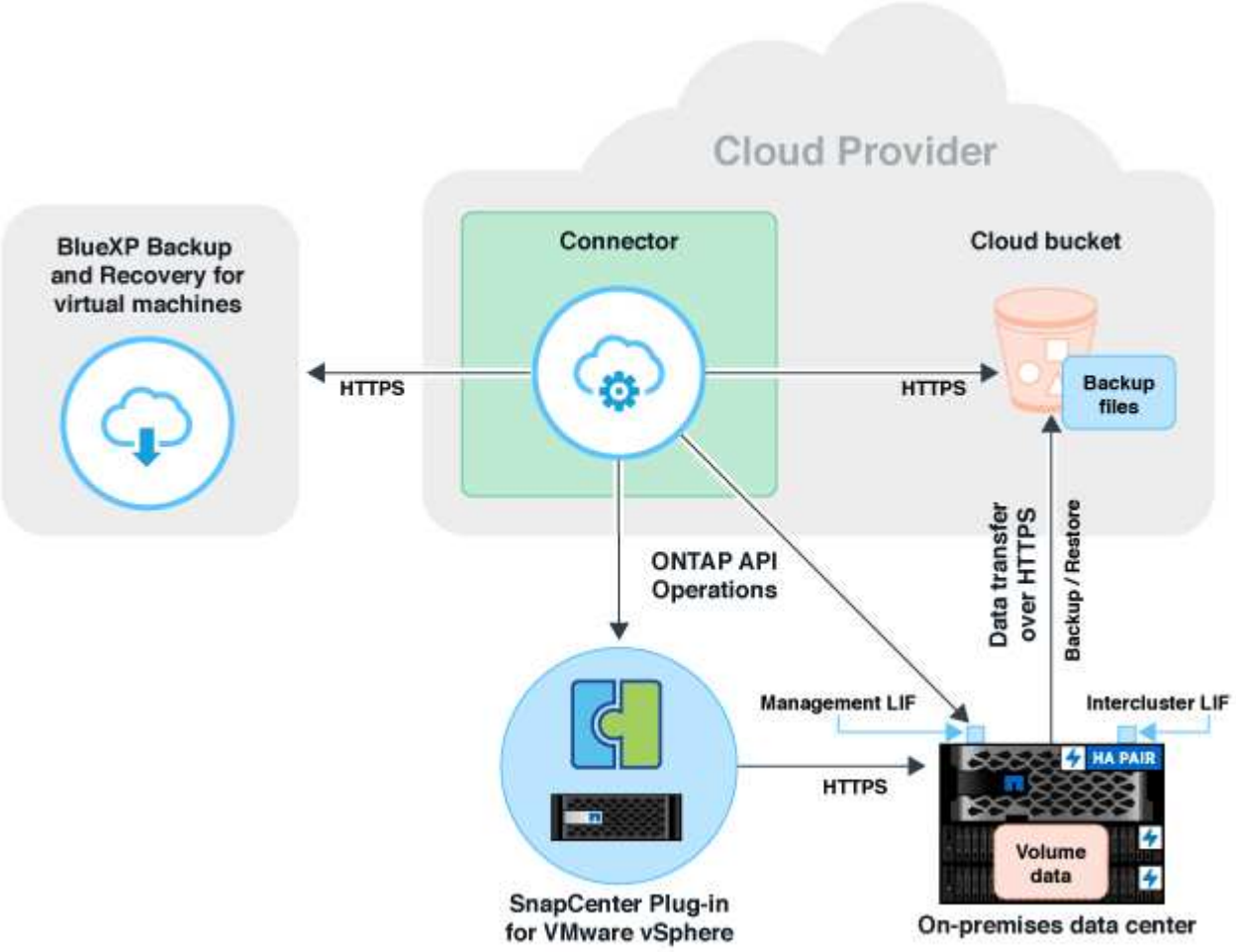
データストアをAmazon Web Services S3、Microsoft Azure Blob、Google Cloud Platform、StorageGRID にバックアップし、仮想マシンをオンプレミスのSnapCenter Plug-in for VMware vSphereホストにリストアできます。仮想マシン向けのBlueXPバックアップ/リカバリでは、コネクタプロキシ導入モデルもサポートされます。

作業を開始する前に

データストアと仮想マシンをクラウドプロバイダにバックアップする前に、次の要件を確認して、サポートされる構成があることを確認してください。

- VMware vSphere 4.6P1以降用のSnapCenter プラグイン
  - SnapCenter Plug-in for VMware vSphere 4.7P1以降を使用して、オンプレミスのセカンダリストレージからデータストアをバックアップする必要があります。
- ONTAP 9.8以降
- BlueXP
- NFSデータストアとVMFSデータストアがサポートされます。VVOLはサポートされません。
- VMFSをサポートするには、SnapCenter Plug-in for VMware vSphereホストが4.9以降で実行されている必要があります。SnapCenter Plug-in for VMware vSphereホストを以前のバージョンから4.9リリースにアップグレードした場合は、VMFSデータストアのバックアップを作成してください。
- VMware vSphere 4.6P1向けSnapCenter プラグインでは、少なくとも1つのバックアップを作成しておく必要があります。
- SnapCenter Plug-in for VMware vSphereで、BlueXPの仮想マシンポリシーと同じラベルまたは同じラベルの日単位、週単位、または月単位のポリシーが少なくとも1つ適用されます。
- 組み込みのポリシーの場合は、SnapCenter Plug-in for VMware vSphereとクラウドのデータストアでスケジュール階層を同じにする必要があります。
- FlexGroup ボリュームのバックアップとリストアはサポートされていないため、データストアにFlexGroup ボリュームがないことを確認してください。
- 必要なリソースグループで「*_ recent *」を無効にします。リソースグループに対して「*_ recent *」が有効になっている場合、これらのリソースグループのバックアップをクラウドへのデータ保護に使用できず、それ以降はリストア処理に使用できません。
- 仮想マシンのリストア先のデータストアに、VMDK、VMX、VMSDなどのすべての仮想マシンファイルのコピーを格納できるだけの十分なスペースがあることを確認してください。
- リストア先のデータストアに、リストア処理でエラーが発生した場合に、restore_xxx_xxxxxx_filename形式の古い仮想マシンファイルが存在しないことを確認してください。リストア処理を開始する前に古いファイルを削除してください。
- プロキシが設定されたコネクタを展開するには、すべての発信コネクタコールがプロキシサーバ経由でルーティングされることを確認します。

次の図は、各コンポーネントとその間の準備に必要な接続を示しています。



SnapCenter Plug-in for VMware vSphereホストを登録

表示するデータストアと仮想マシンについては、BlueXPでSnapCenter Plug-in for VMware vSphereホストを登録する必要があります。SnapCenter Plug-in for VMware vSphereホストを登録できるのは、管理者アクセス権を持つユーザだけです。

> BlueXPでは、複数のSnapCenter Plug-in for VMware vSphereホストを登録できます。ただし、登録後にSnapCenter Plug-in for VMware vSphereホストを削除することはできません。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*仮想マシン*]をクリックします。
2. [設定]ドロップダウンから、[* SnapCenter Plug-in for VMware vSphere*]をクリックします。
3. [* SnapCenter Plug-in for VMware vSphere*の登録]をクリックします。
4. 次の情報を指定します。
   a. SnapCenter Plug-in for VMware vSphereフィールドで、SnapCenter Plug-in for VMware vSphereホス

トのFQDNまたはIPアドレスを指定します。

b. [ポート]フィールドで、SnapCenter Plug-in for VMware vSphereホストが実行されているポート番号を指定します。

デフォルトの8144ポートで実行されているオンプレミスのSnapCenter Plug-in for VMware vSphereホストと、任意のクラウドプロバイダ（Amazon Web Services、Microsoft Azure、Google Cloud Platform）またはオンプレミスで実行されているBlueXPコネクタインスタンスの間で通信が開かれていることを確認する必要があります。

c. [Username]フィールドと[Password]フィールドに、管理者ロールを持つvCenterユーザのクレデンシャルを指定します。

5. [*Register] をクリックします。

◦ 終了後 *

>[仮想マシン]*をクリックして、登録済みのSnapCenter Plug-in for VMware vSphereホストを使用して保護されているすべてのデータストアと仮想マシンを表示します。

データストアをバックアップするポリシーを作成します

ポリシーを作成するか、BlueXPで使用可能な次の定義済みポリシーのいずれかを使用できます。

作業を開始する前に

- 事前定義されたポリシーを編集しない場合は、ポリシーを作成する必要があります。
- オブジェクトストアからアーカイブストレージにバックアップを移動するには、ONTAP 9.10.1以降を実行し、Amazon Web ServicesまたはMicrosoft Azureをクラウドプロバイダとして使用する必要があります。
- 各クラウドプロバイダにアーカイブアクセス階層を設定する必要があります。

このタスクについて

BlueXPでは、次の事前定義されたポリシーを使用できます。

ポリシー名	ラベル	保持値
1年間のLTR（長期保持）	毎日	366
5 年ごとの LTR	毎日	1830年
7 年ごとの LTR	毎週	370
10 年間の月単位 LTR	毎月	一二 〇

手順

1. [仮想マシン]ページの[設定]ドロップダウンリストから、[ポリシー]を選択します。
2. ［ポリシーの作成］をクリックします。

3. [ポリシーの詳細]セクションで、ポリシー名を指定します。
4. 保持セクションで、保持タイプの1つを選択し、保持するバックアップの数を指定します。
5. バックアップストレージソースとして、プライマリまたはセカンダリを選択します。
6. （オプション）コストを最適化するために一定の日数が経過したあとにバックアップをオブジェクトストアからアーカイブストレージに移動する場合は、「* Tier Backups to Archival *」チェックボックスをオンにし、バックアップをアーカイブするまでの日数を入力します。
7. [作成（ Create ）] をクリックします。

> データストアに関連付けられているポリシーを編集または削除することはできません。

データストアを**Amazon Web Services**にバックアップする

1つ以上のデータストアをAmazon Web Servicesにバックアップしてアーカイブすることで、ストレージ効率を高め、クラウドへの移行を促進できます。

データストアがアーカイブポリシーに関連付けられている場合は、アーカイブ階層を選択できます。サポートされているアーカイブ階層は、GlacierとGlacier Deepです。

作業を開始する前に

すべてのが満たされていることを確認します "要件" データストアをクラウドにバックアップする前に、

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*仮想マシン*]をクリックします。
2. をクリックします ••• バックアップするデータストアに対応して、*バックアップのアクティブ化*をクリックします。
3. [ポリシーの割り当て] ページで、ポリシーを選択して [次へ *] をクリックします。
4. 作業環境を追加します。

   BlueXPで検出するクラスタ管理LIFを設定します。いずれかのデータストアの作業環境を追加したら、同じONTAP クラスタにある他のすべてのデータストアでその環境を再利用できます。

   a. SVMに対応する* Add Working Environment *をクリックします。
   b. 作業環境の追加ウィザードで、次の手順を実行します。
      i. クラスタ管理LIFのIPアドレスを指定します。
      ii. ONTAP クラスタユーザのクレデンシャルを指定してください。
   c. * 作業環境の追加 * をクリックします。
5. Amazon Web Services *を選択してクラウドプロバイダとして設定します。
   a. AWS アカウントを指定します。
   b. AWS Access Keyフィールドで、データ暗号化のキーを指定します。
   c. AWS Secret Keyフィールドで、データ暗号化のパスワードを指定します。
   d. バックアップを作成するリージョンを選択します。

e. 作業環境として追加したクラスタ管理LIFのIPアドレスを指定します。

f. アーカイブ階層を選択します。

   アーカイブ層は1回限りのアクティビティであり、あとで設定することはできないため、設定することを推奨します。

6. 詳細を確認し、 * バックアップのアクティブ化 * をクリックします。

データストアを**Microsoft Azure**にバックアップする

SnapCenter Plug-in for VMware vSphereホストとBlueXPを統合することで、1つ以上のデータストアをMicrosoft Azureにバックアップできます。これにより、VM管理者はデータのバックアップとアーカイブを簡単かつ迅速に行えるようになり、ストレージ効率を高めてクラウドへの移行を促進できます。

データストアがアーカイブポリシーに関連付けられている場合は、アーカイブ階層を選択するオプションが表示されます。サポートされるアーカイブ層はAzure Archive Blob Storageです。

作業を開始する前に

すべてのが満たされていることを確認します "要件" データストアをクラウドにバックアップする前に、

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*仮想マシン*]をクリックします。
2. をクリックします ••• バックアップするデータストアに対応して、*バックアップのアクティブ化*をクリックします。
3. [ポリシーの割り当て] ページで、ポリシーを選択して [次へ *] をクリックします。
4. 作業環境を追加します。

   BlueXPで検出するクラスタ管理LIFを設定します。いずれかのデータストアの作業環境を追加したら、同じONTAP クラスタにある他のすべてのデータストアでその環境を再利用できます。

   a. SVMに対応する* Add Working Environment *をクリックします。
   b. 作業環境の追加ウィザードで、次の手順を実行します。
      i. クラスタ管理LIFのIPアドレスを指定します。
      ii. ONTAP クラスタユーザのクレデンシャルを指定してください。
   c. * 作業環境の追加 * をクリックします。
5. 「* Microsoft Azure *」を選択して、クラウドプロバイダとして設定します。
   a. Azure サブスクリプション ID を指定します。
   b. バックアップを作成するリージョンを選択します。
   c. 新しいリソースグループを作成するか、既存のリソースグループを使用します。
   d. 作業環境として追加したクラスタ管理LIFのIPアドレスを指定します。
   e. アーカイブ階層を選択します。

アーカイブ階層は1回限りのアクティビティであり、あとから設定することはできないため、設定することを推奨します。

6. 詳細を確認し、 * バックアップのアクティブ化 * をクリックします。

データストアを**Google Cloud Platform**にバックアップする

SnapCenter Plug-in for VMware vSphereホストとBlueXPを統合することで、1つ以上のデータストアをGoogle Cloud Platformにバックアップできます。これにより、VM管理者はデータのバックアップとアーカイブを簡単かつ迅速に行えるようになり、ストレージ効率を高めてクラウドへの移行を促進できます。

作業を開始する前に

すべてのが満たされていることを確認します "要件" データストアをクラウドにバックアップする前に、

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*仮想マシン*]をクリックします。
2. をクリックします ••• バックアップするデータストアに対応して、*バックアップのアクティブ化*をクリックします。
3. [ポリシーの割り当て] ページで、ポリシーを選択して [次へ *] をクリックします。
4. 作業環境を追加します。

   BlueXPで検出するクラスタ管理LIFを設定します。いずれかのデータストアの作業環境を追加したら、同じONTAP クラスタにある他のすべてのデータストアでその環境を再利用できます。

   a. SVMに対応する* Add Working Environment *をクリックします。
   b. 作業環境の追加ウィザードで、次の手順を実行します。
      i. クラスタ管理LIFのIPアドレスを指定します。
      ii. ONTAP クラスタユーザのクレデンシャルを指定してください。
   c. * 作業環境の追加 * をクリックします。
5. Google Cloud Platform *を選択して、クラウドプロバイダとして構成します。
   a. バックアップ用に Google Cloud Storage バケットを作成する Google Cloud Project を選択します。
   b. Google Cloud Access Keyフィールドで、キーを指定します。
   c. Google Cloud Secret Keyフィールドで、パスワードを指定します。
   d. バックアップを作成するリージョンを選択します。
   e. IPスペースを指定してください。
6. 詳細を確認し、 * バックアップのアクティブ化 * をクリックします。

データストアを**StorageGRID** にバックアップする

SnapCenter Plug-in for VMware vSphereホストをBlueXPに統合することで、1つ以上のデータストアをStorageGRID にバックアップできます。これにより、VM管理者はデー

タのバックアップとアーカイブを簡単かつ迅速に行えるようになり、ストレージ効率を高めてクラウドへの移行を促進できます。

作業を開始する前に

すべてのが満たされていることを確認します "要件" データストアをクラウドにバックアップする前に、

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*仮想マシン*]をクリックします。
2. をクリックします ••• バックアップするデータストアに対応して、*バックアップのアクティブ化*をクリックします。
3. [ポリシーの割り当て] ページで、ポリシーを選択して [次へ *] をクリックします。
4. 作業環境を追加します。

   BlueXPで検出するクラスタ管理LIFを設定します。いずれかのデータストアの作業環境を追加したら、同じONTAP クラスタにある他のすべてのデータストアでその環境を再利用できます。

   a. SVMに対応する* Add Working Environment *をクリックします。
   b. 作業環境の追加ウィザードで、次の手順を実行します。
      i. クラスタ管理LIFのIPアドレスを指定します。
      ii. ONTAP クラスタユーザのクレデンシャルを指定してください。
   c. * 作業環境の追加 * をクリックします。
5. 「* StorageGRID *」を選択します。
   a. ストレージサーバのIPを指定します。
   b. アクセスキーとシークレットキーを選択します。
6. 詳細を確認し、 * バックアップのアクティブ化 * をクリックします。

データストアと仮想マシンのデータの保護を管理します

データをバックアップおよびリストアする前に、ポリシー、データストア、および仮想マシンを表示できます。データベース、ポリシー、リソースグループの変更内容に応じて、BlueXP UIで更新内容を確認できます。

ポリシーを表示します

デフォルトの組み込みポリシーをすべて表示できます。これらの各ポリシーについて、詳細を表示すると、関連付けられているすべてのポリシーと仮想マシンが表示されます。

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*仮想マシン*]をクリックします。
2. [* 設定] ドロップダウンから、 [ポリシー *] をクリックします。
3. 詳細を表示するポリシーに対応する **View Details** をクリックします。

関連付けられているポリシーと仮想マシンが一覧表示されます。

データストアと仮想マシンを表示します

登録済みのSnapCenter Plug-in for VMware vSphereホストを使用して保護されているデータストアと仮想マシンが表示されます。

手順

1. BlueXP UIで、**Protection**>* Backup and recovery*>* Virtual Machines **>** Settings*>* SnapCenter Plug-in for VMware vSphere*の順にクリックします。
2. データストアおよび仮想マシンを表示するSnapCenter Plug-in for VMware vSphereホストをクリックします。

データストアの保護の解除

以前に保護されていたデータストアの保護を解除できます。クラウドバックアップを削除する場合や、クラウドへのバックアップを中止する場合は、データストアの保護を解除できます。データストアは、保護が解除されたあとに再度保護することができます。

手順

1. BlueXP UIで、[保護>*バックアップとリカバリ*>*仮想マシン*]をクリックします。
2. をクリックします ••• をクリックし、*[保護解除]*をクリックします。

SnapCenter Plug-in for VMware vSphereインスタンスを編集します

BlueXPでは、SnapCenter Plug-in for VMware vSphereホストの詳細を編集できます。

手順

1. BlueXP UIで、**Protection**>* Backup and recovery*>* Virtual Machines **>** Settings*>* SnapCenter Plug-in for VMware vSphere*の順にクリックします。
2. をクリックします ••• をクリックし、 * Edit * を選択します。
3. 必要に応じて詳細を変更します。
4. [保存（ Save ）] をクリックします。

リソースとバックアップを更新

アプリケーションに追加された最新のデータストアとバックアップを表示する場合は、リソースとバックアップを更新する必要があります。これにより、リソースとバックアップの検出が開始され、最新の詳細が表示されます。

1. [バックアップとリカバリ>*仮想マシン*]をクリックします。
2. [設定]ドロップダウンから、[* SnapCenter Plug-in for VMware vSphere*]をクリックします。
3. をクリックします ••• SnapCenter Plug-in for VMware vSphereホストに対応し、*[リソースとバックアップをリフレッシュ]*をクリックします。

ポリシーまたはリソースグループをリフレッシュ

ポリシーまたはリソースグループに変更がある場合は、保護関係を更新する必要があります。

1. [バックアップとリカバリ>*仮想マシン*]をクリックします。
2. をクリックします ••• データストアに対応し、*[保護をリフレッシュ]*をクリックします。

SnapCenter Plug-in for VMware vSphereホストの登録を解除します

SnapCenter Plug-in for VMware vSphereホストに関連付けられているすべてのデータストアと仮想マシンが保護されなくなります。

1. [バックアップとリカバリ>*仮想マシン*]をクリックします。
2. [設定]ドロップダウンから、[* SnapCenter Plug-in for VMware vSphere*]をクリックします。
3. をクリックします ••• SnapCenter Plug-in for VMware vSphereホストに対応し、*[登録解除]*をクリックします。

ジョブを監視します

BlueXPのすべてのバックアップ処理とリカバリ処理用のジョブが作成されます。すべてのジョブと、各タスクの一部として実行されるすべてのサブタスクを監視できます。

1. [バックアップとリカバリ>*ジョブ監視*]をクリックします。

   処理を開始すると、ジョブが開始されたことを示すウィンドウが表示されます。リンクをクリックするとジョブを監視できます。

2. プライマリタスクをクリックすると、これらの各サブタスクのサブタスクとステータスが表示されます。

仮想マシンのデータをクラウドからリストア

仮想マシンのデータをクラウドからオンプレミスのvCenterにリストアできます。仮想マシンは、バックアップが作成された場所とまったく同じ場所にリストアすることも、別の場所にリストアすることもできます。アーカイブポリシーを使用して仮想マシンをバックアップした場合は、アーカイブリストアの優先順位を設定できます。

複数のデータストアにまたがる仮想マシンはリストアできません。

作業を開始する前に

- すべてのが満たされていることを確認します "要件" 仮想マシンをクラウドからリストアする前に、
- 別の場所にリストアする場合は、次の手順を実行します。
  - ソースvCenterとデスティネーションvCenterがリンクモードであることを確認します。
  - ソースクラスタとデスティネーションクラスタの詳細が両方のSnapCenter Plug-in for VMware vSphereホストのBlueXPキャンバスとリンクモードのvCenterで追加されていることを確認します。
  - BlueXP Canvasの別の場所に対応するWorking Environment（WE）が追加されていることを確認します。

手順

1. BlueXP UIで、**[保護]>*>**[仮想マシン]**>** SnapCenter Plug-in for VMware vSphere *をクリックし、SnapCenter Plug-in for VMware vSphereホストを選択します。

ソース仮想マシンを別の場所（vMotion）に移動した場合にユーザがBlueXPからその仮想マシンのリストアをトリガーすると、バックアップが作成されたソースの場所に仮想マシンがリストアされます。

1. 仮想マシンを元の場所にリストアすることも、データストアまたは仮想マシンから別の場所にリストアすることもできます。

仮想マシンをリストアする対象	手順
データストアから元の場所	1. をクリックします ••• リストアするデータストアに対応し、*詳細の表示*をクリックします。 2. リストアするバックアップに対応する* Restore *をクリックします。 3. バックアップからリストアする仮想マシンを選択し、* Next *（次へ）をクリックします。 4. *オリジナル*が選択されていることを確認し、*続行*をクリックします。 5. アーカイブ設定が構成されたポリシーを使用して仮想マシンが保護されている場合は、**[**アーカイブリストア優先度**]***を選択し、[次へ]*をクリックします。 Amazon Web Servicesでサポートされているアーカイブリストアの優先度は、高、標準、および低です。また、Microsoft Azureでサポートされているアーカイブリストアの優先度は高および標準です。 6. 詳細を確認して、 * リストア * をクリックします。

仮想マシンをリストアする対象	手順
データストアカラヘツノバショ	1. をクリックします ••• リストアするデータストアに対応し、*詳細の表示*をクリックします。 2. リストアするバックアップに対応する* Restore * をクリックします。 3. バックアップからリストアする仮想マシンを選択し、* Next *（次へ）をクリックします。 4. [代替（Alternate）]*を選択します。 5. 代替のvCenter Server、ESXiホスト、データストア、およびネットワークを選択します。 6. リストア後にVMの名前を指定し、*[続行]*をクリックします。 7. アーカイブ設定が構成されたポリシーを使用して仮想マシンが保護されている場合は、**[**アーカイブリストア優先度**]***を選択し、[次へ]*をクリックします。 Amazon Web Servicesでサポートされているアーカイブリストアの優先度は、高、標準、および低です。また、Microsoft Azureでサポートされているアーカイブリストアの優先度は高および標準です。 8. 詳細を確認して、 * リストア * をクリックします。
仮想マシンから元の場所へ	1. をクリックします ••• リストアする仮想マシンに対応して、*リストア*をクリックします。 2. 仮想マシンのリストアに使用するバックアップを選択します。 3. *オリジナル*が選択されていることを確認し、*続行*をクリックします。 4. アーカイブ設定が構成されたポリシーを使用して仮想マシンが保護されている場合は、**[**アーカイブリストア優先度**]***を選択し、[次へ]*をクリックします。 Amazon Web Servicesでサポートされているアーカイブリストアの優先度は、高、標準、および低です。また、Microsoft Azureでサポートされているアーカイブリストアの優先度は高および標準です。 5. 詳細を確認して、 * リストア * をクリックします。

仮想マシンをリストアする対象	手順
仮想マシンから別の場所へ	1. をクリックします ••• リストアする仮想マシンに対応して、*リストア*をクリックします。 2. 仮想マシンのリストアに使用するバックアップを選択します。 3. [代替（Alternate）]*を選択します。 4. 代替のvCenter Server、ESXiホスト、データストア、およびネットワークを選択します。 5. リストア後にVMの名前を指定し、*[続行]*をクリックします。 6. アーカイブ設定が構成されたポリシーを使用して仮想マシンが保護されている場合は、**[**アーカイブリストア優先度**]***を選択し、[次へ]*をクリックします。 Amazon Web Servicesでサポートされているアーカイブリストアの優先度は、高、標準、および低です。また、Microsoft Azureでサポートされているアーカイブリストアの優先度は高および標準です。 7. 詳細を確認して、 * リストア * をクリックします。

Kubernetes データのバックアップとリストア

BlueXPのバックアップとリカバリを使用してKubernetesクラスタのデータを保護します

BlueXPのバックアップとリカバリは、Kubernetesクラスタデータの保護と長期アーカイブのためのバックアップとリストア機能を提供します。バックアップは自動的に生成され、パブリックまたはプライベートクラウドアカウントのオブジェクトストアに格納されます。

必要に応じて、バックアップから同じ作業環境または別の作業環境に全面的に _ ボリューム _ をリストアできます。

の機能

バックアップ機能：

- 永続ボリュームの独立したコピーを低コストのオブジェクトストレージにバックアップできます。
- クラスタ内のすべてのボリュームに単一のバックアップポリシーを適用するか、または一意のリカバリポイント目標が設定されたボリュームに異なるバックアップポリシーを割り当てます。
- バックアップデータは、転送中の AES-256 ビット暗号化と TLS 1.2 HTTPS 接続によって保護されます。
- 単一ボリュームで最大 4 、 000 個のバックアップがサポートされます。

リストア機能：

- 特定の時点からデータをリストアします。
- ボリュームをソースシステムまたは別のシステムにリストアします。
- 元の ACL を維持したまま、指定した場所にデータを直接配置して、ブロックレベルでデータをリストアします。

サポートされている Kubernetes 作業環境とオブジェクトストレージプロバイダ

BlueXPのバックアップとリカバリでは、Kubernetesボリュームを次の作業環境から次のパブリック/プライベートクラウドプロバイダのオブジェクトストレージにバックアップできます。

ソースの作業環境	バックアップファイルの保存先 ifdef：aws []
AWS の Kubernetes クラスタ	Amazon S3 endif：：aws[] ifdef：Azure []

Azure の Kubernetes クラスタ	Azure Blob の略 endif：：azure[] ifdef ::gcp[]
Google の Kubernetes クラスタ	Google クラウドストレージ endif：GCP []

Kubernetes バックアップファイルから次の作業環境にボリュームをリストアできます。

バックアップファイルの場所	デスティネーションの作業環境 ifdef：aws []
Amazon S3	AWS の Kubernetes クラスタ endif：：aws[] ifdef：Azure []
Azure Blob の略	Azure の Kubernetes クラスタ endif：：azure[] ifdef ::gcp[]
Google クラウドストレージ	Google の Kubernetes クラスタ endif：GCP []

コスト

BlueXPのバックアップとリカバリの使用に関連するコストには、リソース料金とサービス料金の2種類があります。

- リソース料金 *

クラウド内のオブジェクトストレージの容量については、リソースの料金がクラウドプロバイダに支払われます。BlueXPのバックアップとリカバリではソースボリュームのストレージ効率化が維持されるため、クラウドプロバイダのオブジェクトストレージのコストであるdata_after_ ONTAP 効率化（重複排除と圧縮を適用したあとのデータ量が少ない場合）を支払う必要があります。

- サービス料金 *

サービス料金はネットアップにお支払いいただき、バックアップの作成時とリストア時のコストの両方を負担させていただきます。保護するデータの料金は、オブジェクトストレージにバックアップされるボリュームのソースの使用済み論理容量（ ONTAP 効率化）で計算されます。この容量はフロントエンドテラバイト（ FETB ）とも呼ばれます。

バックアップサービスの料金を支払う方法は 2 つあります。1 つ目は、クラウドプロバイダを利用して月額料金を支払う方法です。2 つ目の選択肢は、ネットアップから直接ライセンスを購入することです。を参照してください ライセンス 詳細については、を参照してください

ライセンス

BlueXPのバックアップとリカバリには、従量課金制（PAYGO）とお客様所有のライセンスを使用（BYOL）の2つのライセンスオプションがあります。ライセンスをお持ちでない場合は、 30 日間の無償トライアルをご利用いただけます。

無償トライアルをご利用ください

30 日間の無償トライアルを使用すると、残りの無料試用日数が通知されます。無償トライアルが終了すると、バックアップは作成されなくなります。サービスを引き続き使用するには、サービスに登録するかライセンスを購入する必要があります。

サービスが無効になってもバックアップファイルは削除されません。バックアップを削除しないかぎり、バックアップで使用する容量のオブジェクトストレージのコストは引き続きクラウドプロバイダから請求されます。

従量課金制のサブスクリプション

BlueXPのバックアップとリカバリは、従量課金制モデルで従量課金制のライセンスを提供します。クラウドプロバイダの市場に登録した後は、バックアップされたデータに対して GB 単位の支払いを行います。つまり、前払いによる支払いはありません。クラウドプロバイダから月額料金で請求されます。

無償トライアルを利用されている場合や、お客様が独自のライセンスを使用（ BYOL ）されている場合も、サブスクリプションを設定する必要があります。

- 登録すると、無料トライアルの終了後にサービスが中断されることがなくなります。

  試用期間が終了すると、バックアップしたデータの量に応じて 1 時間ごとに課金されます。

- BYOL ライセンスで許可されている数を超えるデータをバックアップした場合、データバックアップは従量課金制サブスクリプションを使用して続行されます。

  たとえば、 10 TB の BYOL ライセンスがある場合、 10 TB を超える容量はすべて、 PAYGO サブスクリプションによって課金されます。

お客様は、無料トライアル期間中、または BYOL ライセンスを超えていない場合は、従量課金制サブスクリプションから料金を請求されることはありません。

"従量課金制サブスクリプションの設定方法について説明します"。

お客様所有のライセンスを使用

BYOL は、期間ベース（ 12 カ月、 24 カ月、 36 カ月）の _ と _ の容量ベースで、 1 TB 単位での増分に基づいています。ネットアップに料金を支払って、 1 年分のサービスを使用し、最大容量である 10TB を支払うことになります。

サービスを有効にするためにBlueXPのデジタルウォレットページに入力したシリアル番号が表示されます。いずれかの制限に達すると、ライセンスを更新する必要があります。Backup BYOL ライセンス環境 では、に

関連付けられているすべてのソースシステムがライセンスされます "BlueXPアカウント"。

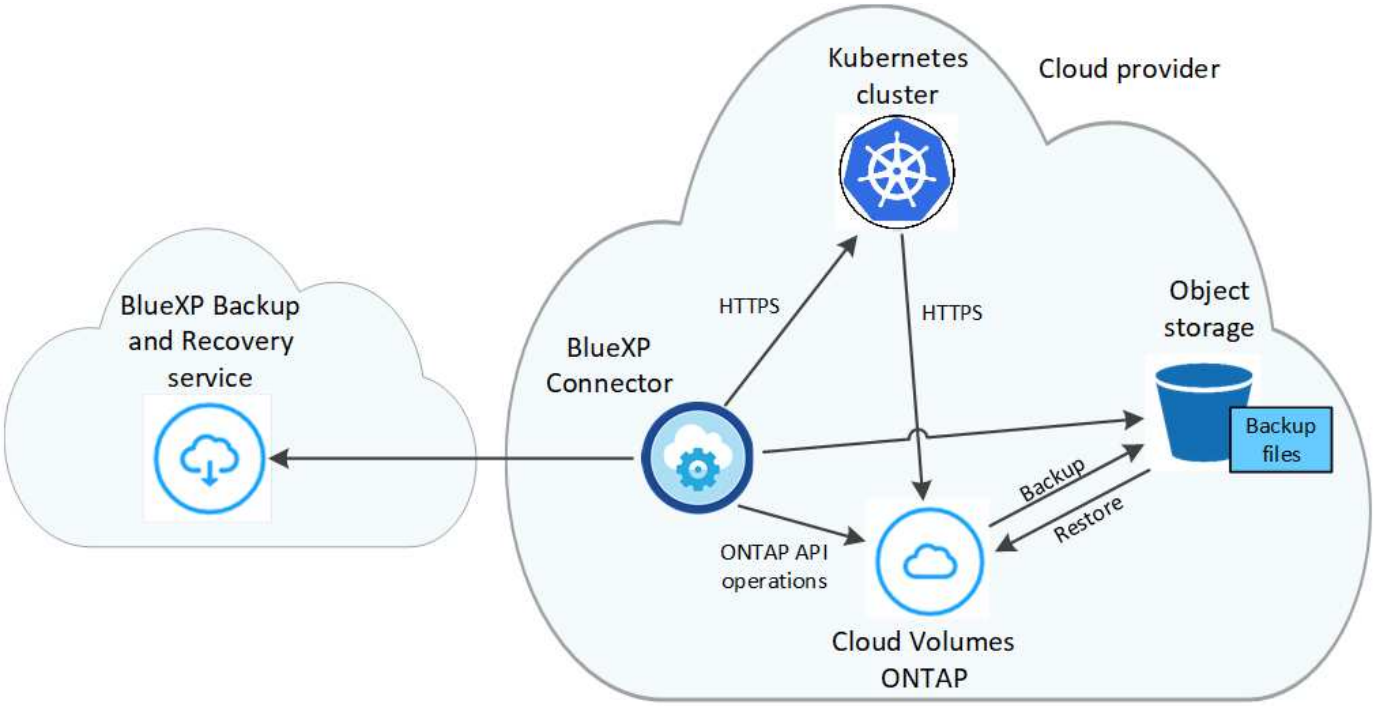
"BYOL ライセンスの管理方法について説明します"。

BlueXPのバックアップとリカバリの仕組み

KubernetesシステムでBlueXPのバックアップとリカバリを有効にすると、サービスによってデータのフルバックアップが実行されます。初期バックアップ後は、追加のバックアップはすべて差分になります。つまり、変更されたブロックと新しいブロックのみがバックアップされます。これにより、ネットワークトラフィックを最小限に抑えることができます。

> クラウドプロバイダ環境からバックアップファイルの管理や変更を直接行うと、ファイルが破損してサポートされない構成になる可能性があります。

次の図は、各コンポーネント間の関係を示しています。



サポートされるストレージクラスまたはアクセス階層

- AWS では、バックアップは _Standard_storage クラスから開始し、 30 日後に _Standard-Infrequent Access_storage クラスに移行します。
- Azure では、バックアップは _COOL アクセス層に関連付けられます。
- GCP では、バックアップはデフォルトで _Standard_storage クラスに関連付けられています。

クラスタごとにカスタマイズ可能なバックアップスケジュールと保持設定

作業環境でBlueXPのバックアップとリカバリを有効にすると、最初に選択したすべてのボリュームが定義したデフォルトのバックアップポリシーを使用してバックアップされます。Recovery Point Objective （ RPO ；目標復旧時点）が異なるボリュームに対して異なるバックアップポリシーを割り当てる場合は、そのクラスタに追加のポリシーを作成し、そのポリシーを他のボリュームに割り当てることができます。

すべてのボリュームについて、毎時、毎日、毎週、および毎月のバックアップを組み合わせて選択できます。

カテゴリまたは間隔のバックアップの最大数に達すると、古いバックアップは削除されるため、常に最新のバックアップが保持されます。

サポートされるボリューム

BlueXPのバックアップとリカバリでは永続ボリューム（PV）がサポートされます。

制限

- ポリシーにボリュームが割り当てられていない場合にバックアップポリシーを作成または編集するときは、バックアップの保持数を 1018 以下にする必要があります。回避策 では、ポリシーを作成するバックアップの数を減らすことができます。その後、ポリシーを編集して、ポリシーにボリュームを割り当てたあとで最大 4 、 000 個のバックアップを作成できます。
- Kubernetes ボリュームでは、 * 今すぐバックアップ * ボタンを使用したアドホックボリュームのバックアップはサポートされていません。

Kubernetes の永続ボリュームのデータを Amazon S3 にバックアップします

EKS Kubernetes クラスタ上の永続ボリュームから Amazon S3 ストレージへのデータのバックアップを開始するには、いくつかの手順を実行します。

クイックスタート

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

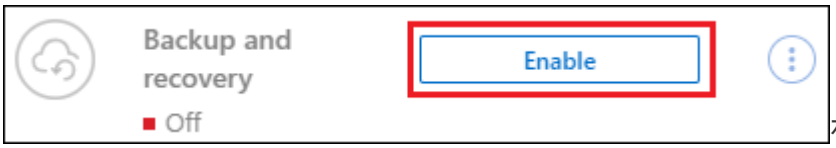
1 前提条件を確認する

- KubernetesクラスタがBlueXP作業環境として検出されました。
  - Trident がクラスタにインストールされている必要があります。 Trident のバージョンは 21.1 以降である必要があります。
  - バックアップする永続ボリュームの作成に使用されるすべての PVC で、「 snapshotPolicy 」が「 default 」に設定されている必要があります。
  - クラスタのバックエンドストレージに AWS で Cloud Volumes ONTAP が使用されている必要があります。
  - Cloud Volumes ONTAP システムで ONTAP 9.7P5 以降が実行されている必要があります。
- バックアップを格納するストレージスペースに対する有効なクラウドプロバイダのサブスクリプションが必要です。
- に登録しておきます "BlueXP Marketplaceバックアップ製品"、 "AWS 年間契約"またはを購入したことが必要です "アクティブ化されます" ネットアップが提供するBlueXPバックアップ/リカバリのBYOLライセンス
- BlueXP Connectorに権限を付与するIAMロールには、最新のからのS3権限が含まれています "BlueXPポリ

シー"。

2 既存の**Kubernetes**クラスタで**BlueXP**のバックアップとリカバリを有効にします

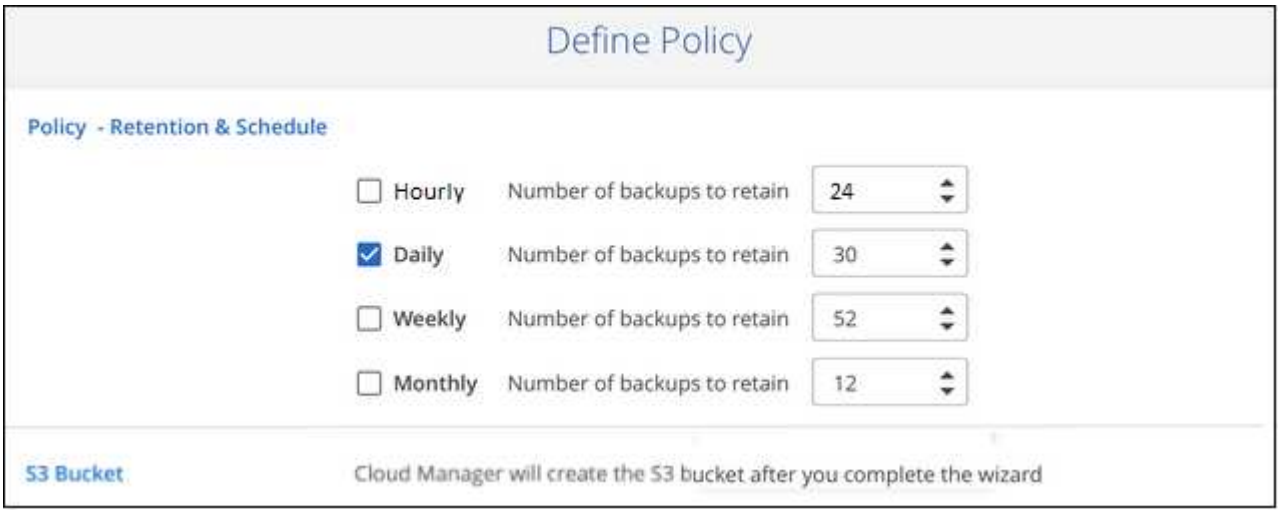
作業環境を選択し、右パネルでバックアップ/リカバリサービスの横にある*有効化*をクリックして、セットアップ・ウィザードに従います。



ボタンのスクリーンショット。"]

3 バックアップポリシーを定義

デフォルトポリシーでは、毎日ボリュームがバックアップされ、各ボリュームの最新の 30 個のバックアップコピーが保持されます。毎時、毎日、毎週、または毎月のバックアップに変更するか、システム定義のポリシーの中からオプションを追加する 1 つを選択します。保持するバックアップコピーの数を変更することもできます。



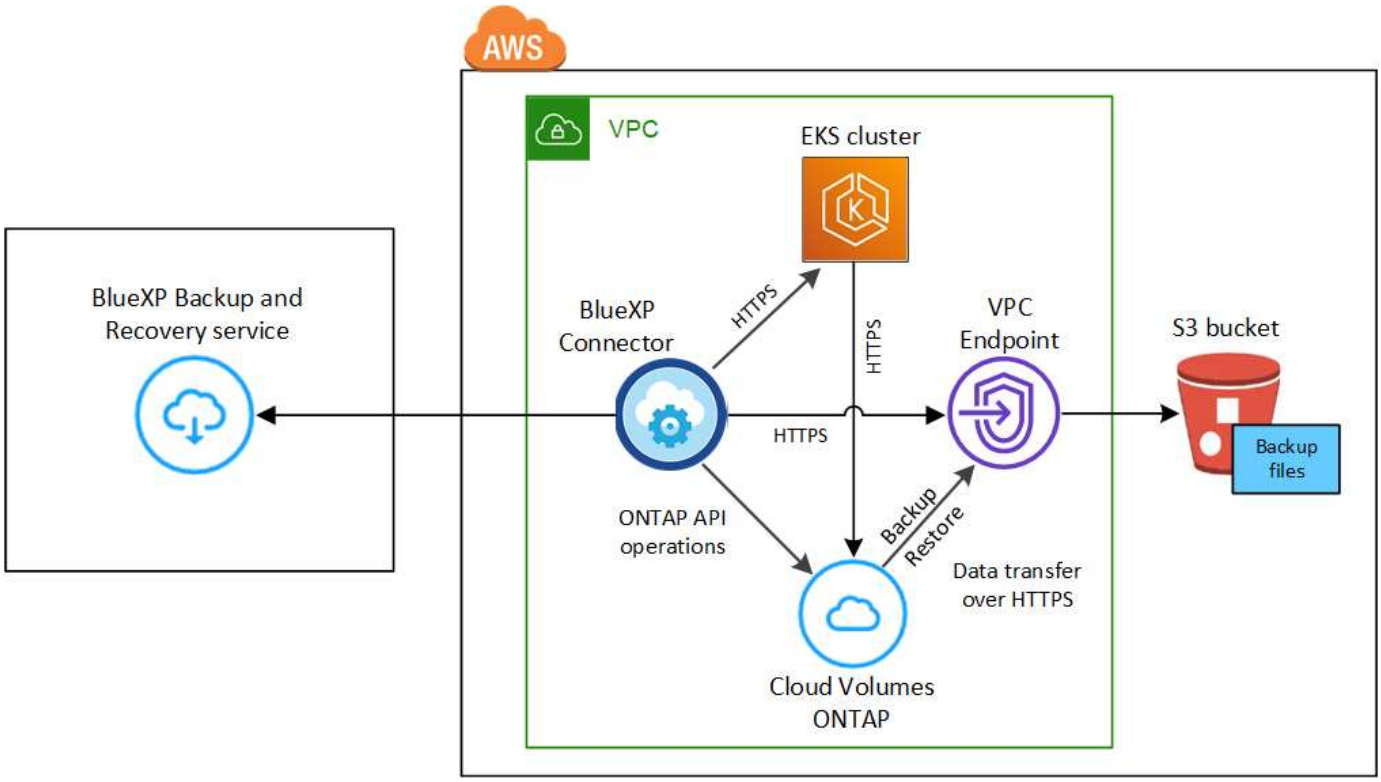
4 バックアップするボリュームを選択します

Select Volumes （ボリュームの選択）ページで、バックアップするボリュームを特定します。S3 バケットは、 Cloud Volumes ONTAP システムと同じ AWS アカウントおよびリージョンに自動的に作成され、バックアップファイルが格納されます。

要件

Kubernetes の永続ボリュームを S3 にバックアップする前に、次の要件を読み、サポートされている構成になっていることを確認してください。

次の図は、各コンポーネントとその間の準備に必要な接続を示しています。



VPC エンドポイントはオプションです。

Kubernetes クラスタの要件

- KubernetesクラスタがBlueXP作業環境として検出されました。 "Kubernetes クラスタの検出方法を参照してください"。
- Trident はクラスタにインストールされている必要があります。 Trident のバージョンは 21.1 以上である必要があります。を参照してください "Trident のインストール方法" または "Trident バージョンをアップグレードする方法"。
- クラスタのバックエンドストレージに AWS で Cloud Volumes ONTAP が使用されている必要があります。
- Cloud Volumes ONTAP システムはKubernetesクラスタと同じAWSリージョンに配置する必要があり、ONTAP 9.7P5以降を実行している必要があります（ONTAP 9.8P11以降を推奨）。

  オンプレミス環境の Kubernetes クラスタはサポートされていません。Cloud Volumes ONTAP システムを使用するクラウド環境では、 Kubernetes クラスタのみがサポートされます。

- バックアップする永続ボリュームの作成に使用されるすべての Persistent Volume Claim オブジェクトで、「 snapshotPolicy 」が「 default 」に設定されている必要があります。

  これは、を追加することによって、個 々 のPVCに対して行うことができます `snapshotPolicy` アノテーションの下：

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver
```

これは、特定のバックエンドストレージに関連付けられているすべてのPVCに対して実行できます `snapshotPolicy` フィールドのデフォルト値は、です `backend.json` ファイル：

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
  deletionPolicy: retain
```

ライセンス要件

BlueXPのバックアップとリカバリのPAYGOライセンスの場合は、AWS Marketplaceでサブスクリプションを購入してCloud Volumes ONTAP とBlueXPのバックアップとリカバリを導入できます。必要です "このBlueXPサブスクリプションを購読します" BlueXPのバックアップとリカバリを有効にする前に、BlueXP

のバックアップとリカバリの課金は、このサブスクリプションを通じて行われます。

Cloud Volumes ONTAP データとオンプレミスの ONTAP データの両方をバックアップできる年間契約の場合は、から登録する必要があります "AWS Marketplace のページ" 次に "サブスクリプションを AWS クレデンシャルに関連付けます"。

Cloud Volumes ONTAP とBlueXPのバックアップとリカバリをバンドルできる年間契約の場合は、Cloud Volumes ONTAP 作業環境の作成時に年間契約を設定する必要があります。このオプションでは、オンプレミスのデータをバックアップすることはできません。

BlueXPのバックアップとリカバリのBYOLライセンスの場合は、ライセンスの期間と容量にわたってサービスを使用できるネットアップのシリアル番号が必要です。 "BYOL ライセンスの管理方法について説明します"。

また、バックアップを格納するストレージスペース用の AWS アカウントが必要です。

サポートされている **AWS** リージョン

BlueXPのバックアップとリカバリは、すべてのAWSリージョンでサポートされます "Cloud Volumes ONTAP がサポートされている場合"。

AWS Backup 権限が必要です

BlueXPに権限を付与するIAMロールには、最新ののS3権限が含まれている必要があります "BlueXPポリシー"。

次に、このポリシーの特定の S3 権限を示します。

```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

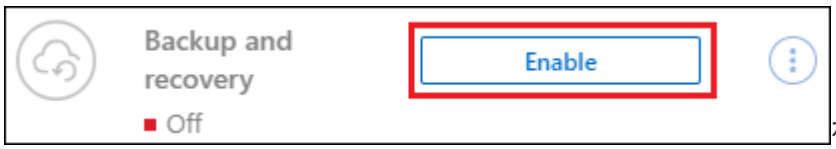
BlueXPのバックアップとリカバリを有効にする

BlueXPのバックアップとリカバリは、Kubernetes作業環境からいつでも直接実行できます。

手順

1. 作業環境を選択し、右パネルのバックアップ/リカバリサービスの横にある*有効化*をクリックします。

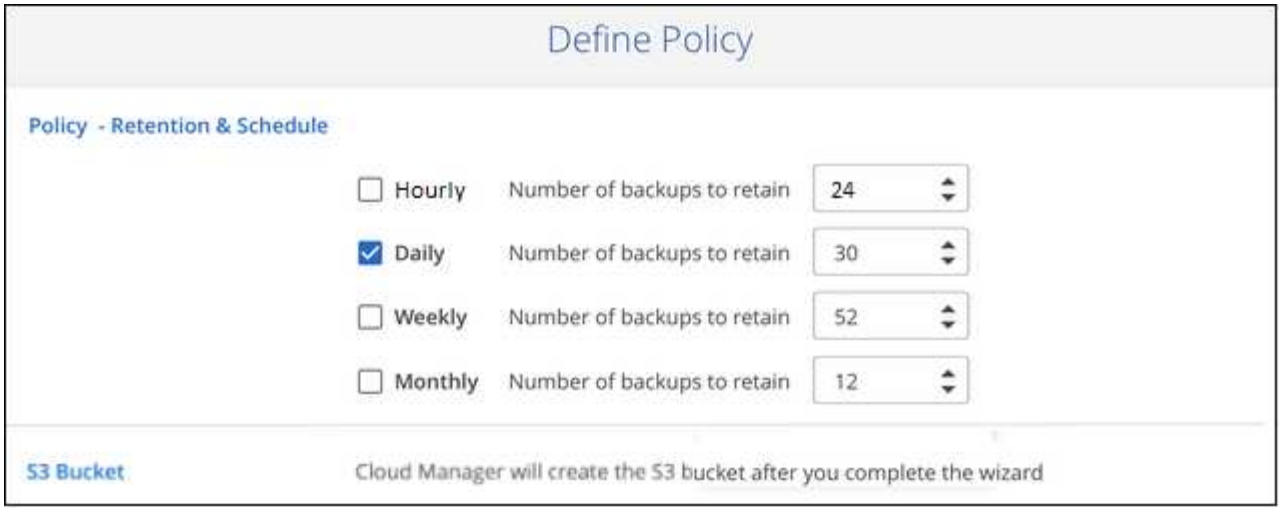
   バックアップのAmazon S3デスティネーションがCanvas上の作業環境として存在する場合は、KubernetesクラスタをAmazon S3作業環境にドラッグしてセットアップウィザードを開始できます。

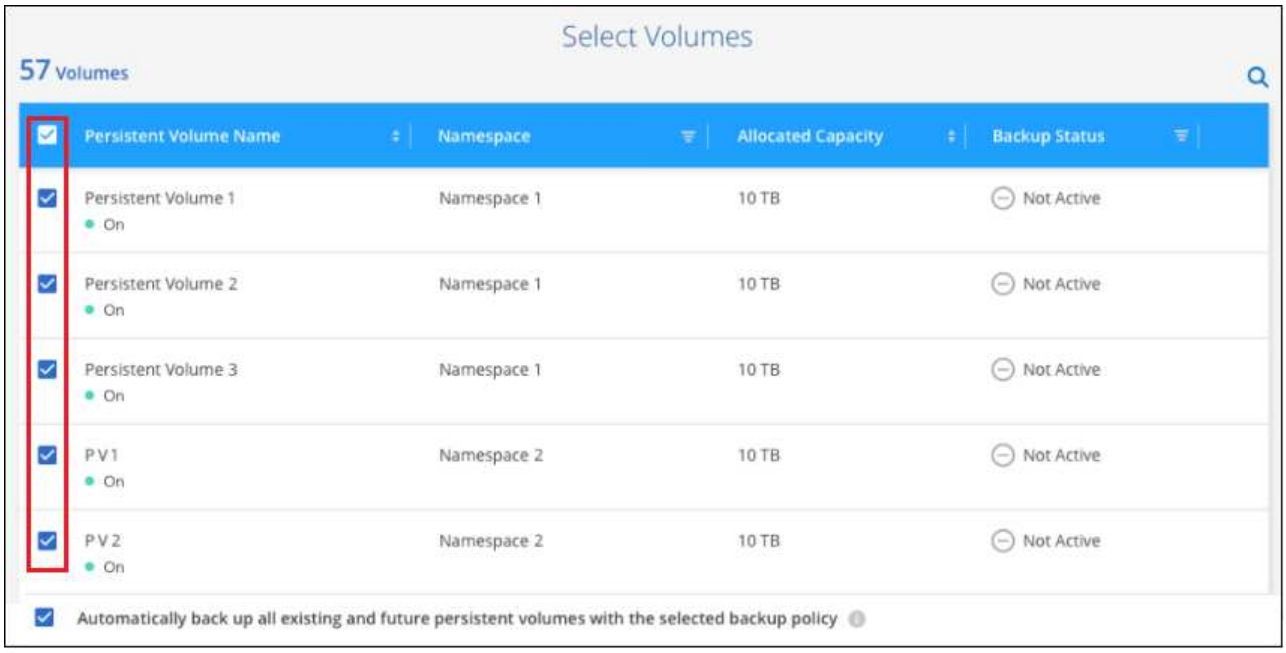
   ボタンのスクリーンショット。"]

2. バックアップポリシーの詳細を入力し、 * Next * をクリックします。

   バックアップスケジュールを定義して、保持するバックアップの数を選択できます。



3. バックアップする永続ボリュームを選択します。
   - すべてのボリュームをバックアップするには、タイトル行（ Volume Name ）。
   - 個々のボリュームをバックアップするには、各ボリュームのボックス（ Volume_1）。



4. 現在および将来のすべてのボリュームでバックアップを有効にする場合は、「今後のボリュームを自動的にバックアップします…一時保持」チェックボックスをオンのままにします。この設定を無効にした場合は、将来のボリュームのバックアップを手動で有効にする必要があります。
5. [バックアップをアクティブ化]*をクリックすると、選択した各ボリュームの初期バックアップの作成がBlueXPのバックアップとリカバリによって開始されます。

結果

S3 バケットは、 Cloud Volumes ONTAP システムと同じ AWS アカウントおよびリージョンに自動的に作成され、バックアップファイルが格納されます。

Kubernetes ダッシュボードが表示され、バックアップの状態を監視できます。

次の手順

可能です "ボリュームのバックアップを開始および停止したり、バックアップを変更したりできます スケジュール"。
また可能です "バックアップファイルからボリューム全体をリストアする" AWS の同じまたは別の Kubernetes クラスタ（同じリージョン内）上の新しいボリュームとして。

Kubernetes の永続ボリュームのデータを Azure BLOB ストレージにバックアップする

AKS Kubernetes クラスタ上の永続ボリュームから Azure BLOB ストレージへのデータのバックアップを開始するには、いくつかの手順を実行します。

クイックスタート

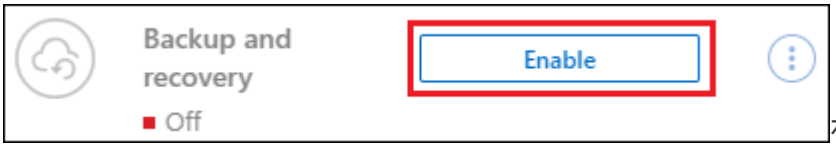
これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

1 前提条件を確認する

- KubernetesクラスタがBlueXP作業環境として検出されました。
  - Trident がクラスタにインストールされている必要があります。 Trident のバージョンは 21.1 以降である必要があります。
  - バックアップする永続ボリュームの作成に使用されるすべての PVC で、「 snapshotPolicy 」が「 default 」に設定されている必要があります。
  - クラスタのバックエンドストレージに Azure 上の Cloud Volumes ONTAP が使用されている必要があります。
  - Cloud Volumes ONTAP システムで ONTAP 9.7P5 以降が実行されている必要があります。
- バックアップを格納するストレージスペースに対する有効なクラウドプロバイダのサブスクリプションが必要です。
- に登録しておきます "BlueXP Marketplaceバックアップ製品"またはを購入したことが必要です "アクティブ化されます" ネットアップが提供するBlueXPバックアップ/リカバリのBYOLライセンス

2 既存の**Kubernetes**クラスタで**BlueXP**のバックアップとリカバリを有効にします

作業環境を選択し、右パネルでバックアップ/リカバリサービスの横にある*有効化*をクリックして、セットアップ・ウィザードに従います。



ボタンのスクリーンショット。"]

3 バックアップポリシーを定義

デフォルトポリシーでは、毎日ボリュームがバックアップされ、各ボリュームの最新の 30 個のバックアップ

コピーが保持されます。毎時、毎日、毎週、または毎月のバックアップに変更するか、システム定義のポリシーの中からオプションを追加する 1 つを選択します。保持するバックアップコピーの数を変更することもできます。

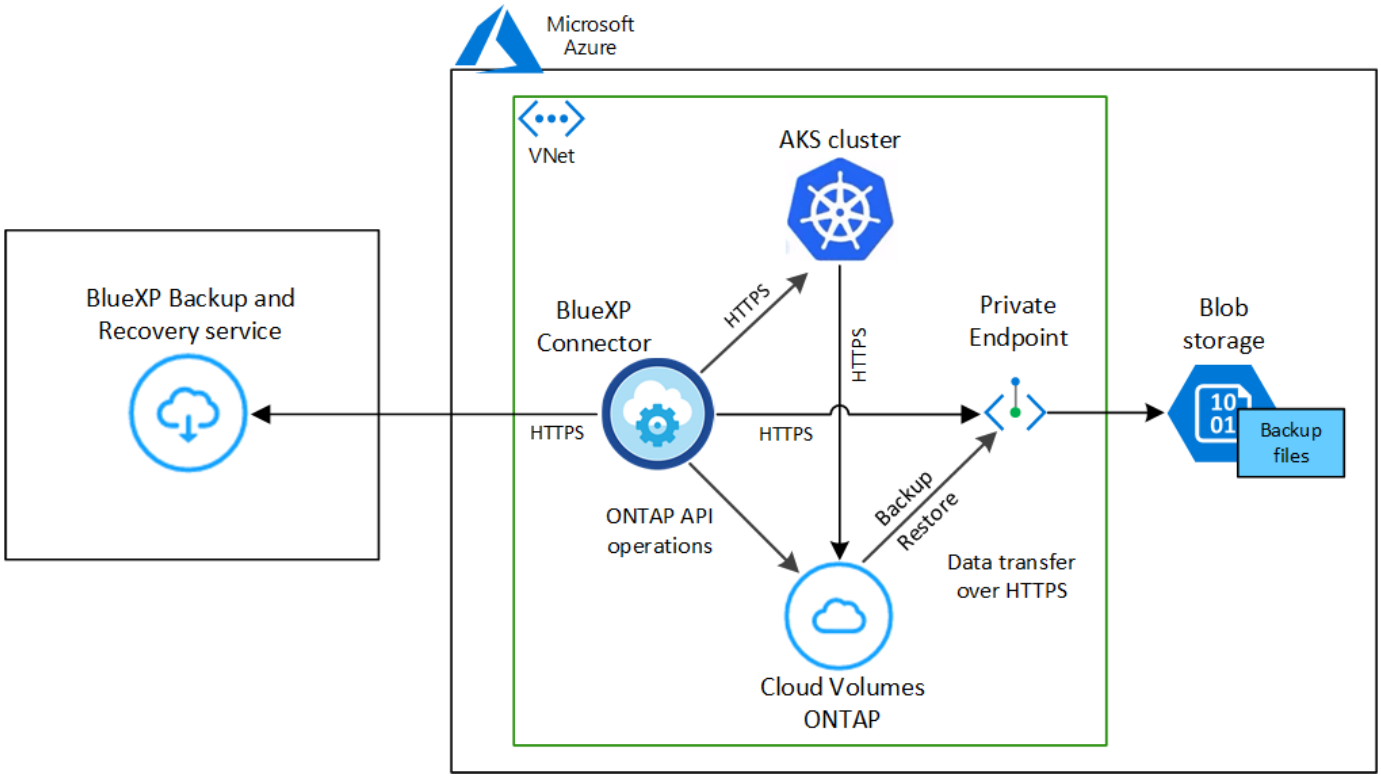
4 バックアップするボリュームを選択します

Select Volumes （ボリュームの選択）ページで、バックアップするボリュームを特定します。バックアップファイルは、 Cloud Volumes ONTAP システムと同じ Azure サブスクリプションとリージョンを使用して BLOB コンテナに格納されます。

要件

Kubernetes 永続ボリュームを BLOB ストレージにバックアップする前に、次の要件を読み、サポートされている構成であることを確認してください。

次の図は、各コンポーネントとその間の準備に必要な接続を示しています。



プライベートエンドポイントはオプションです。

Kubernetes クラスタの要件

- KubernetesクラスタがBlueXP作業環境として検出されました。 "Kubernetes クラスタの検出方法を参照してください"。
- Trident はクラスタにインストールされている必要があります。 Trident のバージョンは 21.1 以上である必要があります。を参照してください "Trident のインストール方法" または "Trident バージョンをアップグレードする方法"。
- クラスタのバックエンドストレージに Azure 上の Cloud Volumes ONTAP が使用されている必要があります。
- Cloud Volumes ONTAP システムはKubernetesクラスタと同じAzureリージョンに配置する必要があり、ONTAP 9.7P5以降を実行している必要があります（ONTAP 9.8P11以降を推奨）。

  オンプレミス環境の Kubernetes クラスタはサポートされていません。Cloud Volumes ONTAP システムを使用するクラウド環境では、 Kubernetes クラスタのみがサポートされます。

- バックアップする永続ボリュームの作成に使用されるすべての Persistent Volume Claim オブジェクトで、「 snapshotPolicy 」が「 default 」に設定されている必要があります。

  これは、を追加することによって、個 々 のPVCに対して行うことができます `snapshotPolicy` アノテーションの下：

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver
```

これは、特定のバックエンドストレージに関連付けられているすべてのPVCに対して実行できます `snapshotPolicy` フィールドのデフォルト値は、です `backend.json` ファイル：

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
  deletionPolicy: retain
```

ライセンス要件

BlueXPのバックアップとリカバリのPAYGOライセンスを使用している場合は、BlueXPのバックアップとリカバリを有効にする前に、Azure Marketplaceでサブスクリプションを購入する必要があります。BlueXPのバックアップとリカバリの課金は、このサブスクリプションを通じて行われます。 "作業環境ウィザード

の[Details Credentialsページからサブスクライブできます。"^]。

BlueXPのバックアップとリカバリのBYOLライセンスの場合は、ライセンスの期間と容量にわたってサービスを使用できるネットアップのシリアル番号が必要です。 "BYOL ライセンスの管理方法について説明します"。

また、バックアップを格納するストレージスペースには、 Microsoft Azure サブスクリプションが必要です。

サポートされている **Azure** リージョン

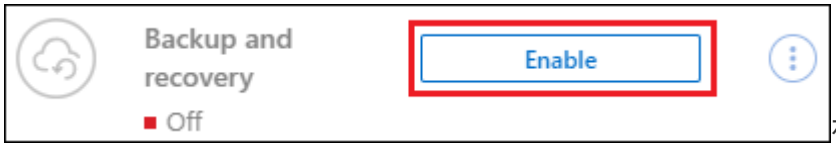
BlueXPのバックアップとリカバリは、Azureのすべてのリージョンでサポートされます "Cloud Volumes ONTAP がサポートされている場合"。

BlueXPのバックアップとリカバリを有効にする

BlueXPのバックアップとリカバリは、Kubernetes作業環境からいつでも直接実行できます。

手順

1. 作業環境を選択し、右パネルのバックアップ/リカバリサービスの横にある*有効化*をクリックします。

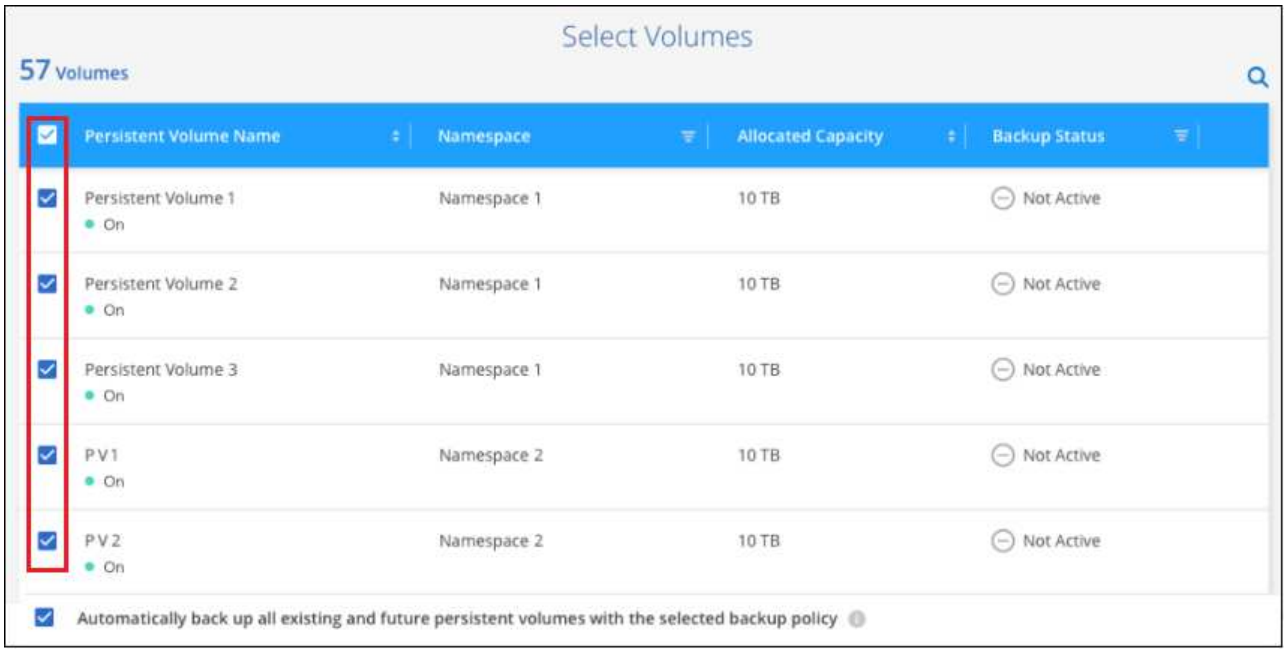


ボタンのスクリーンショット。"]

2. バックアップポリシーの詳細を入力し、 * Next * をクリックします。

   バックアップスケジュールを定義して、保持するバックアップの数を選択できます。

3. バックアップする永続ボリュームを選択します。
   - すべてのボリュームをバックアップするには、タイトル行（ Volume Name ）。
   - 個々のボリュームをバックアップするには、各ボリュームのボックス（ Volume_1 ）。



4. 現在および将来のすべてのボリュームでバックアップを有効にする場合は、「今後のボリュームを自動的にバックアップします…一時保持」チェックボックスをオンのままにします。この設定を無効にした場合は、将来のボリュームのバックアップを手動で有効にする必要があります。
5. [バックアップをアクティブ化]*をクリックすると、選択した各ボリュームの初期バックアップの作成がBlueXPのバックアップとリカバリによって開始されます。

結果

バックアップファイルは、 Cloud Volumes ONTAP システムと同じ Azure サブスクリプションとリージョンを使用して BLOB コンテナに格納されます。

Kubernetes ダッシュボードが表示され、バックアップの状態を監視できます。

次の手順

可能です "ボリュームのバックアップを開始および停止したり、バックアップを変更したりできます スケジュール"。
また可能です "バックアップファイルからボリューム全体をリストアする" Azure 内の同じまたは別の Kubernetes クラスタ（同じリージョン内）に新しいボリュームとして配置する必要があります。

Kubernetes の永続ボリュームのデータを Google Cloud ストレージにバックアップする

GKE Kubernetes クラスタ上の永続ボリュームから Google Cloud ストレージへのデータのバックアップを開始するには、いくつかの手順を実行します。

クイックスタート

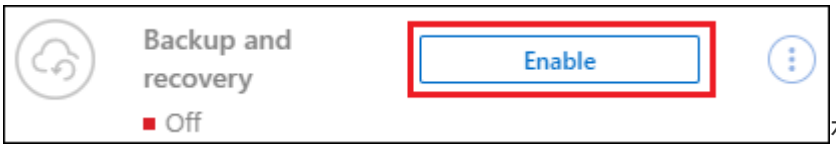
これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

1 前提条件を確認する

- KubernetesクラスタがBlueXP作業環境として検出されました。
  - Trident がクラスタにインストールされている必要があります。 Trident のバージョンは 21.1 以降である必要があります。
  - バックアップする永続ボリュームの作成に使用されるすべての PVC で、「 snapshotPolicy 」が「 default 」に設定されている必要があります。
  - クラスタは、そのバックエンドストレージに GCP 上の Cloud Volumes ONTAP を使用している必要があります。
  - Cloud Volumes ONTAP システムで ONTAP 9.7P5 以降が実行されている必要があります。
- バックアップを保存するストレージスペースの有効な GCP サブスクリプションがあります。
- Google Cloud Project に、事前定義された Storage Admin ロールを持つサービスアカウントがあります。
- に登録しておきます "BlueXP Marketplaceバックアップ製品"またはを購入したことが必要です "アクティブ化されます" ネットアップが提供するBlueXPバックアップ/リカバリのBYOLライセンス

2 既存の**Kubernetes**クラスタで**BlueXP**のバックアップとリカバリを有効にします

作業環境を選択し、右パネルでバックアップ/リカバリサービスの横にある*有効化*をクリックして、セットアップ・ウィザードに従います。



ボタンのスクリーンショット。"]

3 バックアップポリシーを定義

デフォルトポリシーでは、毎日ボリュームがバックアップされ、各ボリュームの最新の 30 個のバックアップコピーが保持されます。毎時、毎日、毎週、または毎月のバックアップに変更するか、システム定義のポリシーの中からオプションを追加する 1 つを選択します。保持するバックアップコピーの数を変更することもできます。

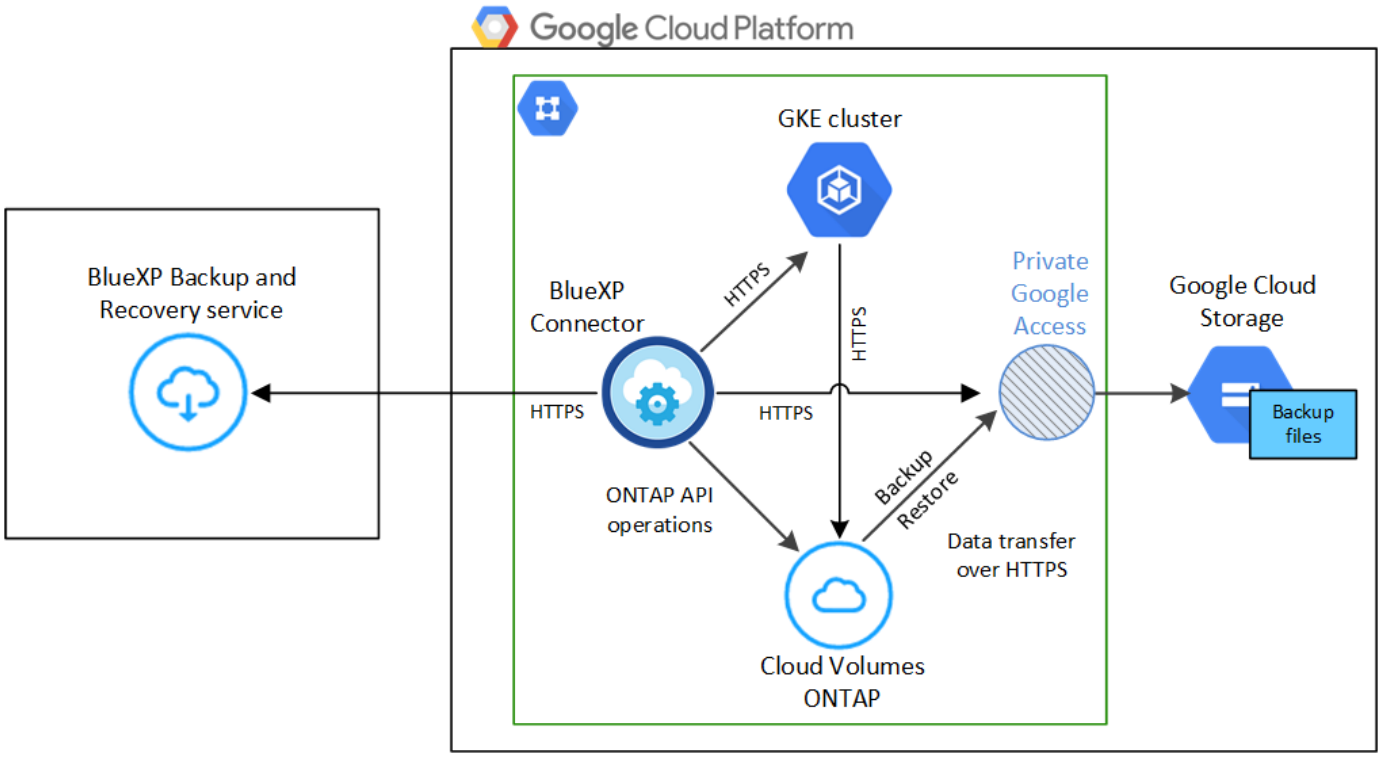
4 バックアップするボリュームを選択します

Select Volumes （ボリュームの選択）ページで、バックアップするボリュームを特定します。バックアップファイルは、 Cloud Volumes ONTAP システムと同じ GCP サブスクリプションとリージョンを使用して Google Cloud Storage バケットに格納されます。

要件

Kubernetes の永続ボリュームを Google Cloud ストレージにバックアップする前に、次の要件を確認し、サポートされている構成であることを確認してください。

次の図は、各コンポーネントとその間の準備に必要な接続を示しています。



プライベートエンドポイントはオプションです。

Kubernetes クラスタの要件

- KubernetesクラスタがBlueXP作業環境として検出されました。 "Kubernetes クラスタの検出方法を参照してください"。
- Trident はクラスタにインストールされている必要があります。 Trident のバージョンは 21.1 以上である必要があります。を参照してください "Trident のインストール方法" または "Trident バージョンをアップグレードする方法"。
- クラスタは、そのバックエンドストレージに GCP 上の Cloud Volumes ONTAP を使用している必要があります。
- Cloud Volumes ONTAP システムはKubernetesクラスタと同じGCPリージョンに配置し、ONTAP 9.7P5以降を実行している必要があります（ONTAP 9.8P11以降を推奨）。

  オンプレミス環境の Kubernetes クラスタはサポートされていません。Cloud Volumes ONTAP システムを使用するクラウド環境では、 Kubernetes クラスタのみがサポートされます。

- バックアップする永続ボリュームの作成に使用されるすべての Persistent Volume Claim オブジェクトで、「 snapshotPolicy 」が「 default 」に設定されている必要があります。

  これは、を追加することによって、個 々 のPVCに対して行うことができます `snapshotPolicy` アノテーションの下：

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver
```

  これは、特定のバックエンドストレージに関連付けられているすべてのPVCに対して実行できます `snapshotPolicy` フィールドのデフォルト値は、です `backend.json` ファイル：

```yaml
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
  deletionPolicy: retain
```

サポートされる **GCP** リージョン

BlueXPのバックアップとリカバリは、すべてのGCPリージョンでサポートされます "Cloud Volumes ONTAP がサポートされている場合"。

ライセンス要件

BlueXPのバックアップとリカバリのPAYGOライセンスの場合は、を使用したサブスクリプションです "GCPマーケットプレイス" は、BlueXPのバックアップとリカバリを有効にする前に必要です。BlueXPのバックアップとリカバリの課金は、このサブスクリプションを通じて行われます。 "作業環境ウィザードの[Details Credentialsページからサブスクライブできます。"^]。

BlueXPのバックアップとリカバリのBYOLライセンスの場合は、ライセンスの期間と容量にわたってサービスを使用できるネットアップのシリアル番号が必要です。 "BYOL ライセンスの管理方法について説明します"。

また、バックアップを保存するストレージスペースの Google サブスクリプションが必要です。

GCP サービスアカウント

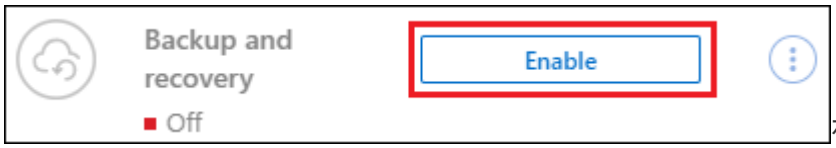
事前定義された Storage Admin ロールを持つサービスアカウントが Google Cloud Project に必要です。 "サービスアカウントの作成方法について説明します"。

BlueXPのバックアップとリカバリを有効にする

BlueXPのバックアップとリカバリは、Kubernetes作業環境からいつでも直接実行できます。

手順

1. 作業環境を選択し、右パネルのバックアップ/リカバリサービスの横にある*有効化*をクリックします。

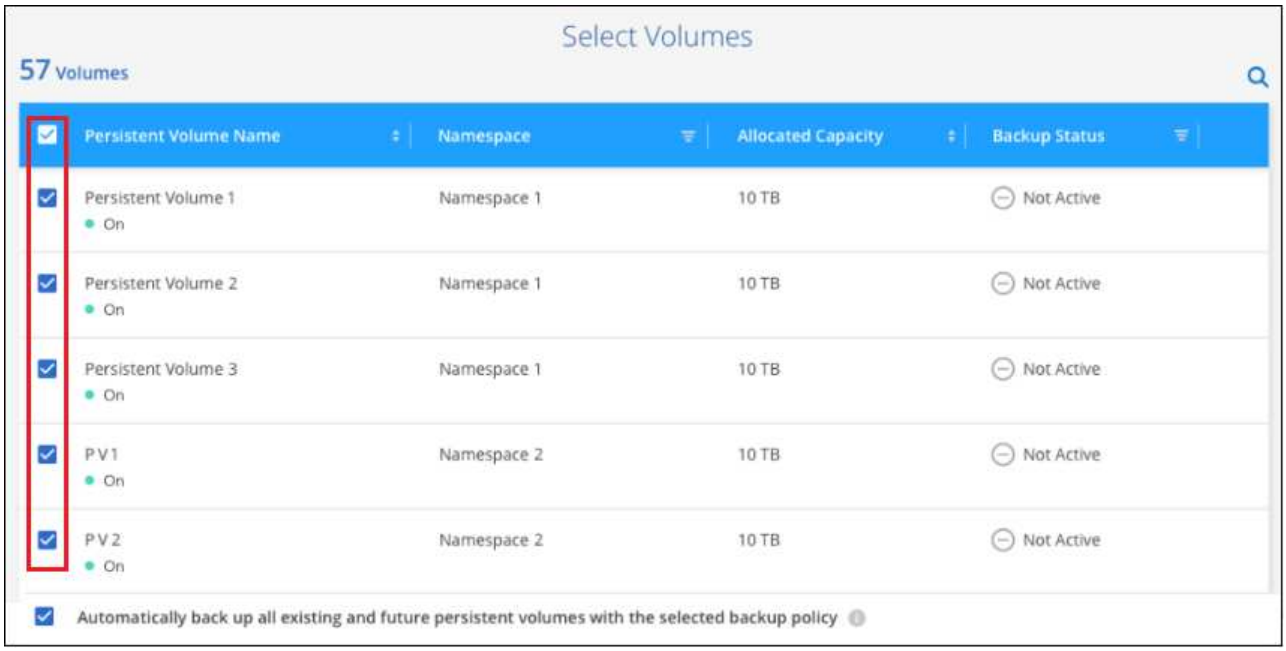


ボタンのスクリーンショット。"]

2. バックアップポリシーの詳細を入力し、 * Next * をクリックします。

   バックアップスケジュールを定義して、保持するバックアップの数を選択できます。

3. バックアップする永続ボリュームを選択します。
   - すべてのボリュームをバックアップするには、タイトル行（ Volume Name ）。
   - 個々のボリュームをバックアップするには、各ボリュームのボックス（ Volume_1 ）。



4. 現在および将来のすべてのボリュームでバックアップを有効にする場合は、「今後のボリュームを自動的にバックアップします…一時保持」チェックボックスをオンのままにします。この設定を無効にした場合

は、将来のボリュームのバックアップを手動で有効にする必要があります。

5. [バックアップをアクティブ化]*をクリックすると、選択した各ボリュームの初期バックアップの作成がBlueXPのバックアップとリカバリによって開始されます。

結果

バックアップファイルは、 Cloud Volumes ONTAP システムと同じ GCP サブスクリプションとリージョンを使用して Google Cloud Storage バケットに格納されます。

Kubernetes ダッシュボードが表示され、バックアップの状態を監視できます。

次の手順

可能です "ボリュームのバックアップを開始および停止したり、バックアップを変更したりできます スケジュール"。
また可能です "バックアップファイルからボリューム全体をリストアする" GCP 内の同じ Kubernetes クラスタまたは別の Kubernetes クラスタ（同じリージョン内）上の新しいボリュームです。

Kubernetes システムのバックアップの管理

Kubernetes システムのバックアップは、バックアップスケジュールの変更、ボリュームのバックアップの有効化 / 無効化、バックアップの削除などによって管理できます。

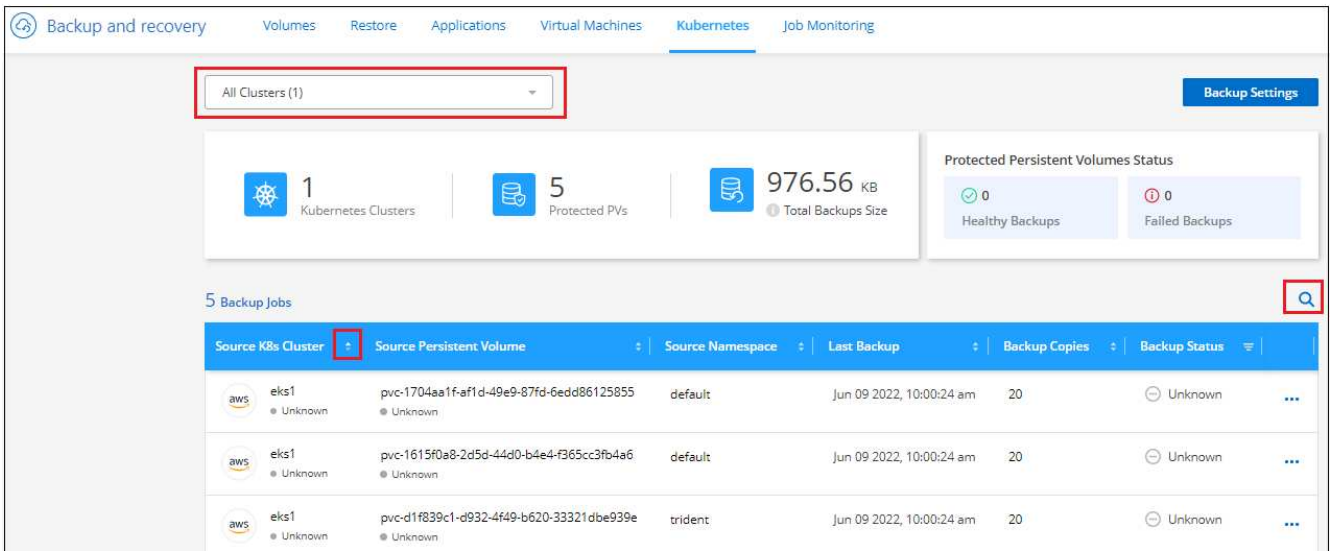
> バックアップファイルをクラウドプロバイダ環境から直接管理したり変更したりしないでください。ファイルが破損し、サポートされていない構成になる可能性があります。

バックアップしているボリュームを表示します

BlueXPのバックアップとリカバリで現在バックアップされているすべてのボリュームのリストを表示できます。

手順

1. BlueXPメニューから、*Protection > Backup and recovery*を選択します。
2. Kubernetes システムの永続ボリュームのリストを表示するには、 * Kubernetes * タブをクリックします。



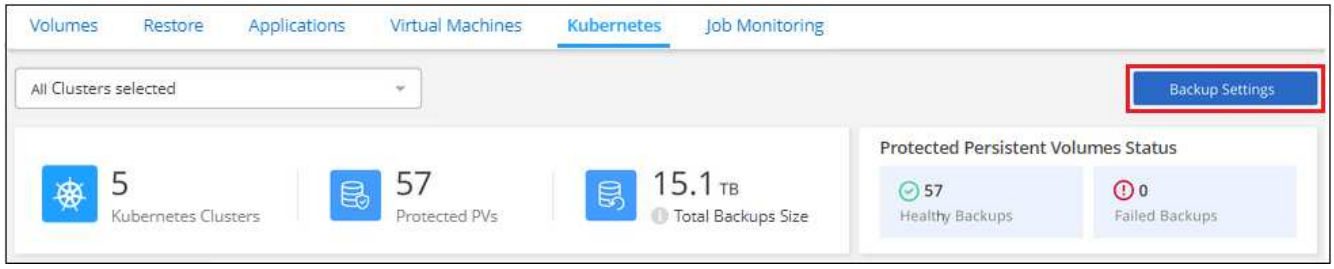
特定のクラスタの特定のボリュームを検索する場合は、クラスタおよびボリュームに基づいてリストを絞り込むか、検索フィルタを使用できます。

ボリュームのバックアップの有効化と無効化

ボリュームのバックアップコピーが不要で、バックアップの格納コストを抑える必要がない場合は、ボリュームのバックアップを停止できます。新しいボリュームがバックアップ中でない場合は、バックアップリストに追加することもできます。

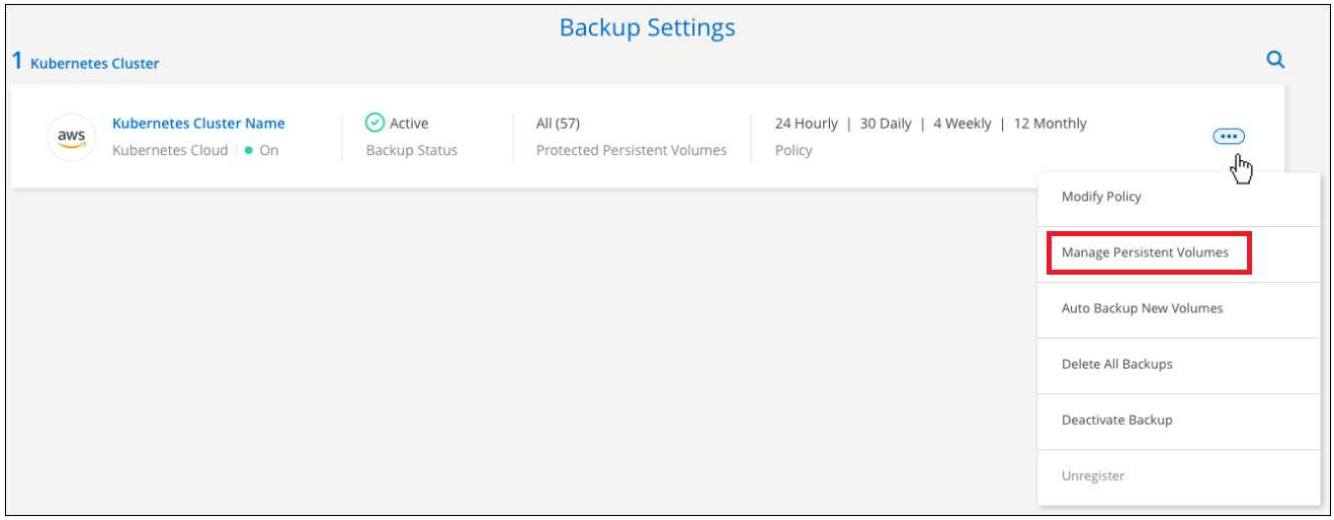
手順

1. [**Kubernetes ***] タブで、 [バックアップ設定 *] を選択します。



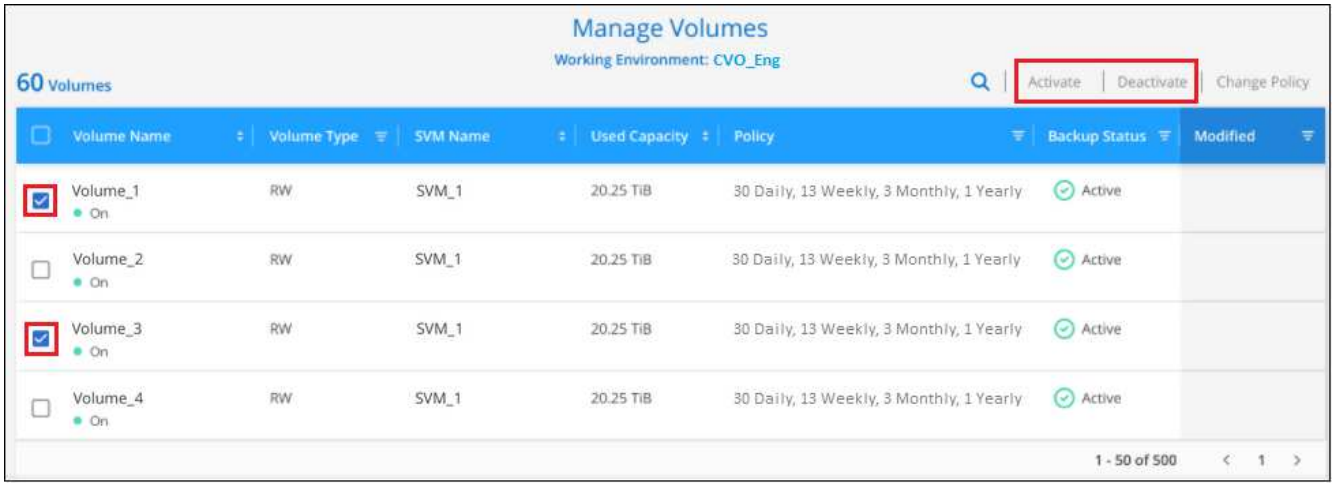
ボタンを示すスクリーンショット。"]

2. _ バックアップ設定ページ _ で、をクリックします ••• アイコン"] Kubernetesクラスタで、* Manage Persistent Volumes *を選択します。



ページの[永続ボリュームの管理]ボタンを示すスクリーンショット。"]

3. 変更するボリュームのチェックボックスを選択し、ボリュームのバックアップを開始するか停止するかに応じて、 [Activate * （アクティブ化 * ）] または [* Deactivate * （非アクティブ化 * ）] をクリックします。



4. [保存（ Save ）] をクリックして、変更をコミットします。

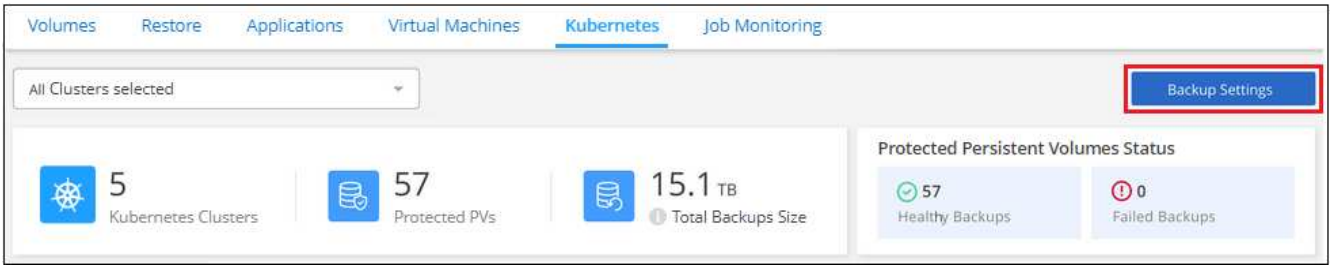
*注：*ボリュームのバックアップを停止した場合、バックアップが使用する容量のオブジェクトストレージのコストは引き続きクラウドプロバイダに課金されます バックアップを削除します。

既存のバックアップポリシーを編集する

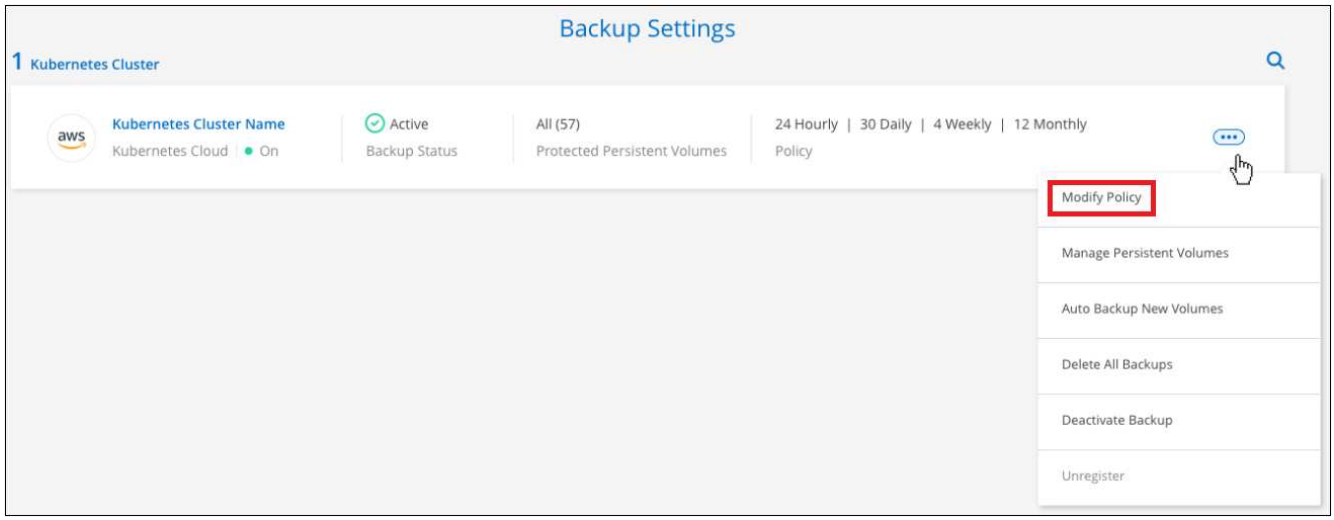
作業環境でボリュームに現在適用されているバックアップポリシーの属性を変更することができます。バックアップポリシーを変更すると、そのポリシーを使用している既存のすべてのボリュームが対象になります。

手順

1. **[Kubernetes *]** タブで、 **[** バックアップ設定 *] を選択します。



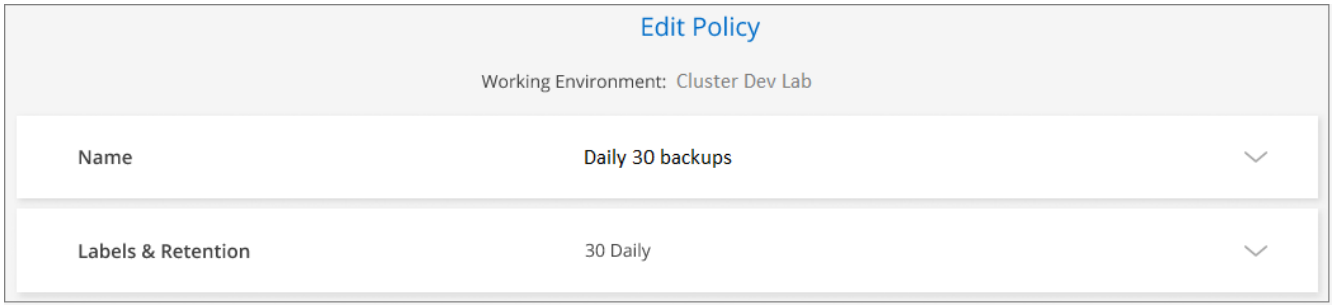
2. [Backup Settings_] ページで、をクリックします ••• アイコン"] 設定を変更する作業環境で、 [* ポリシーの管理 *] を選択します。



ページの [ポリシーの管理] オプションを示すスクリーンショット。"]

3. [ポリシーの管理] ページで、作業環境で変更するバックアップポリシーの [ポリシーの編集] をクリックします。

4. [ポリシーの編集] ページで、スケジュールとバックアップの保持を変更し、 [保存] をクリックします。



新しいボリュームに割り当てるバックアップポリシーの設定

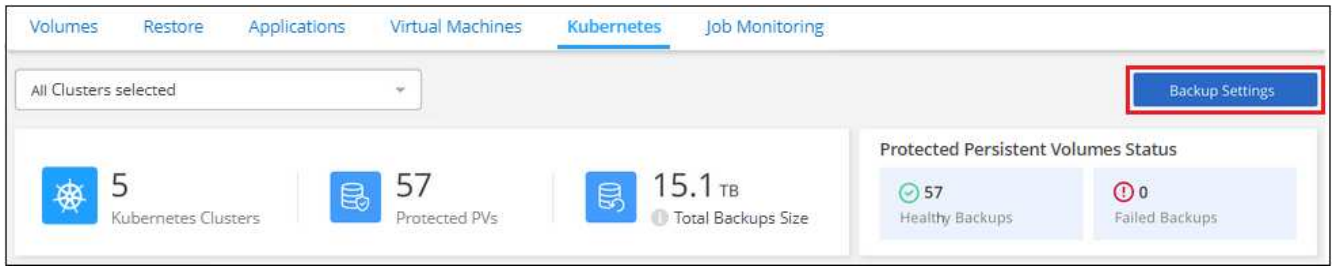
KubernetesクラスタでBlueXPのバックアップとリカバリを初めてアクティブ化したときに、新しく作成したボリュームにバックアップポリシーを自動的に割り当てるオプションを選択しなかった場合は、あとで_Backup Settings_pageでこのオプションを選択できます。新しく作成したボリュームにバックアップポリシーを割り当てると、すべてのデータを確実に保護できます。

ボリュームに適用するポリシーがすでに存在している必要があります。

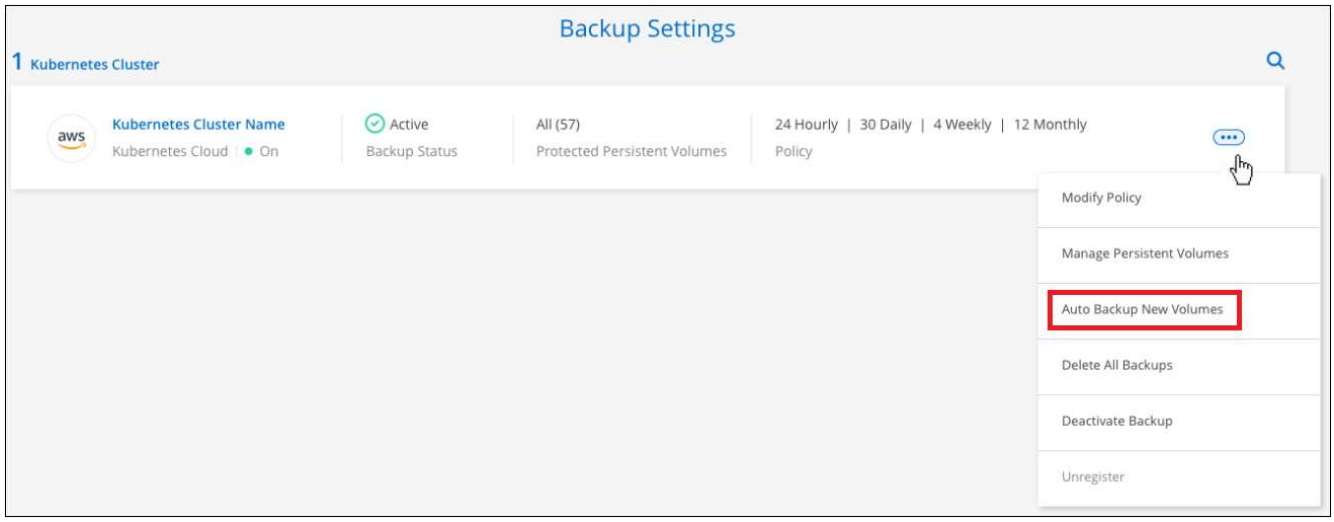
また、新しく作成したボリュームが自動的にバックアップされないようにするには、この設定を無効にします。その場合は、後でバックアップする特定のボリュームのバックアップを手動で有効にする必要があります。

手順

1. **[Kubernetes *]** タブで、 **[** バックアップ設定 *] を選択します。

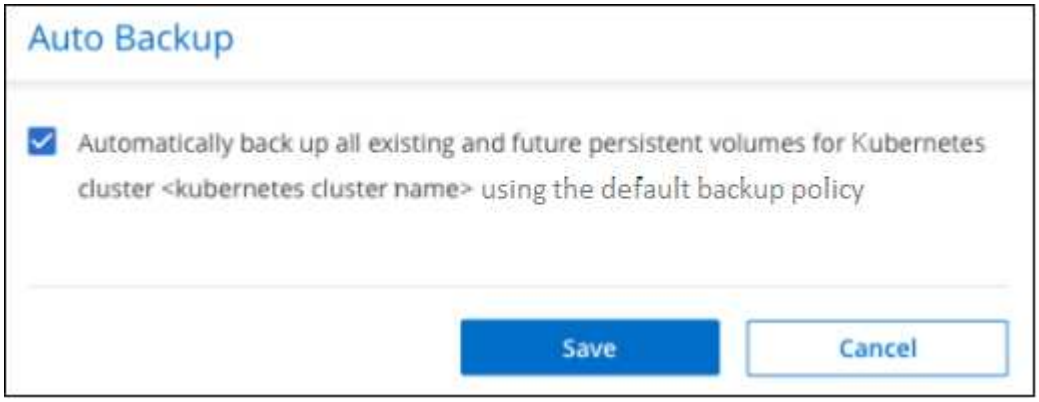


2. _ バックアップ設定ページ _ で、をクリックします ••• アイコン"] ボリュームが存在するKubernetesクラスタで、* Auto Backup New Volumes *を選択します。



ページで[新しいボリュームの自動バックアップ]オプションを選択したスクリーンショット。"]

3. [今後の永続ボリュームを自動的にバックアップする…]チェックボックスをオンにし、新しいボリュームに適用するバックアップポリシーを選択して、[保存]をクリックします。



結果

このバックアップポリシーは、このKubernetesクラスタで作成されるすべての新しいボリュームに適用され

ます。

各ボリュームのバックアップリストを表示します

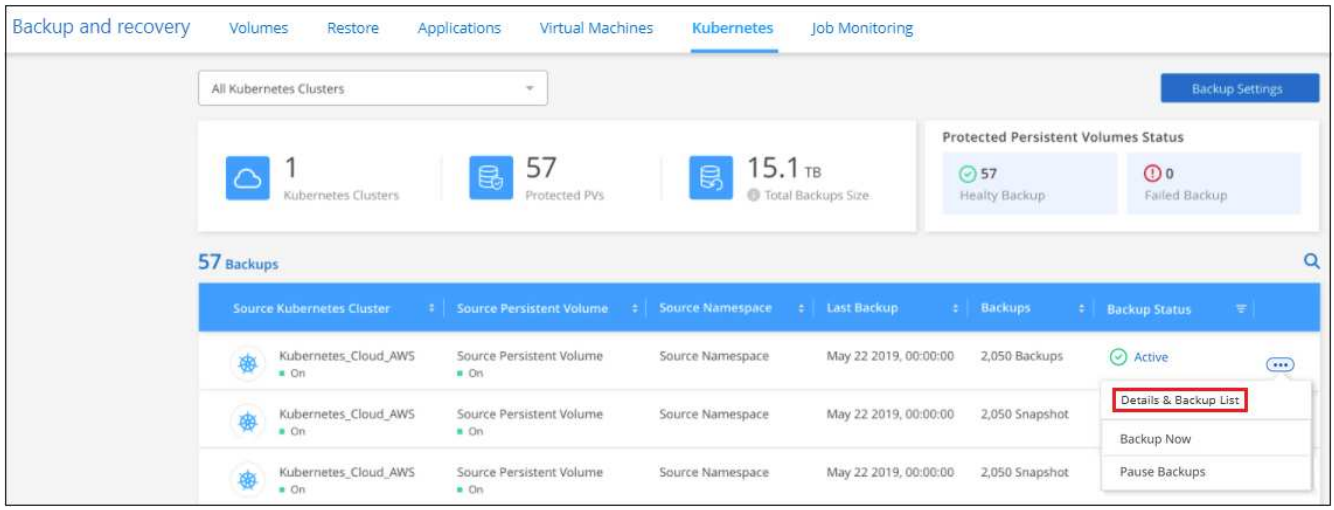
各ボリュームに存在するすべてのバックアップファイルのリストを表示できます。このページには、ソースボリューム、デスティネーションの場所、および前回作成されたバックアップの詳細、現在のバックアップポリシー、バックアップファイルのサイズなどのバックアップの詳細が表示されます。

このページでは、次のタスクも実行できます。

- ボリュームのすべてのバックアップファイルを削除します
- ボリュームの個々のバックアップファイルを削除する
- ボリュームのバックアップレポートをダウンロードします

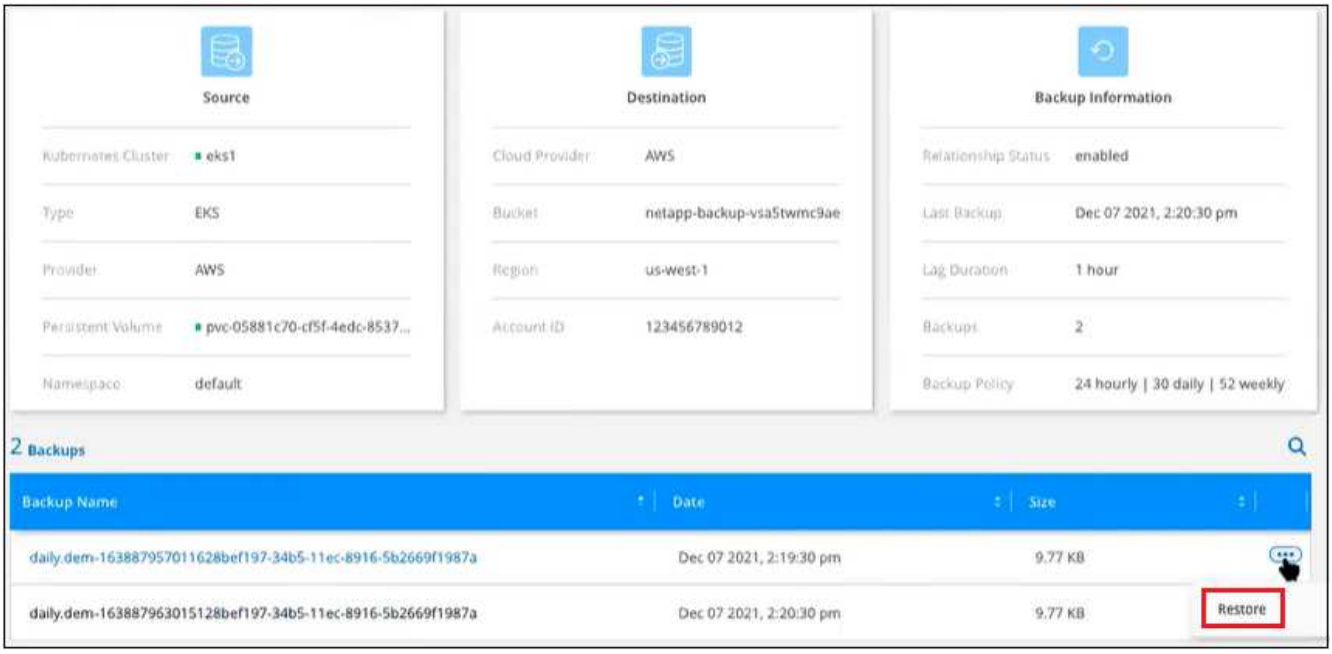
手順

1. [*Kubernetes *] タブで、をクリックします ••• アイコン"] をソースボリュームとして選択し、 * Details & Backup List * を選択します。



ボタンを示すスクリーンショット。"]

すべてのバックアップファイルのリストが、ソースボリューム、デスティネーションの場所、およびバックアップの詳細とともに表示されます。



バックアップを削除する

BlueXPのバックアップとリカバリでは、単一のバックアップファイルを削除したり、ボリュームのすべてのバックアップを削除したり、Kubernetesクラスタ内のすべてのボリュームのすべてのバックアップを削除したりできます。すべてのバックアップを削除するのは、不要になった場合やソースボリュームを削除したあとにすべてのバックアップを削除する場合などです。

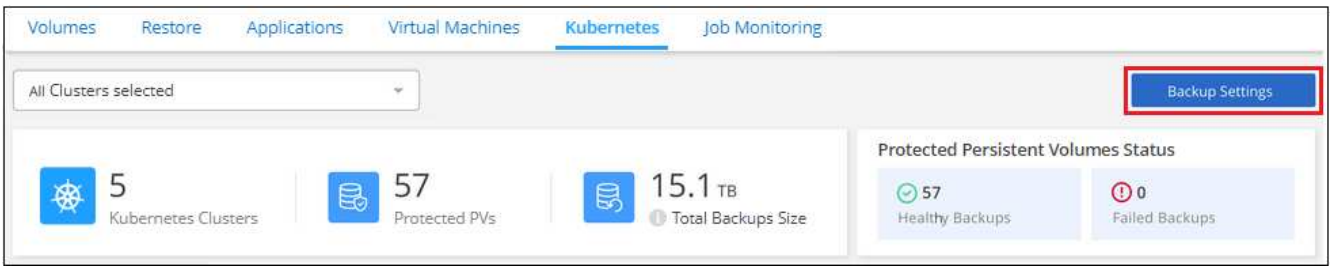
> バックアップがある作業環境またはクラスタを削除する場合は、システムを削除する前に * バックアップを削除する必要があります。システムを削除しても、BlueXPのバックアップとリカバリでバックアップが自動的に削除されることはなく、システムの削除後にバックアップを削除する機能は現在UIでサポートされていません。残りのバックアップについては、引き続きオブジェクトストレージのコストが発生します。

作業環境のすべてのバックアップファイルを削除する

作業環境のすべてのバックアップを削除しても、この作業環境のボリュームの以降のバックアップは無効になりません。作業環境ですべてのボリュームのバックアップの作成を停止するには、バックアップを非アクティブ化します ここで説明するようにします。

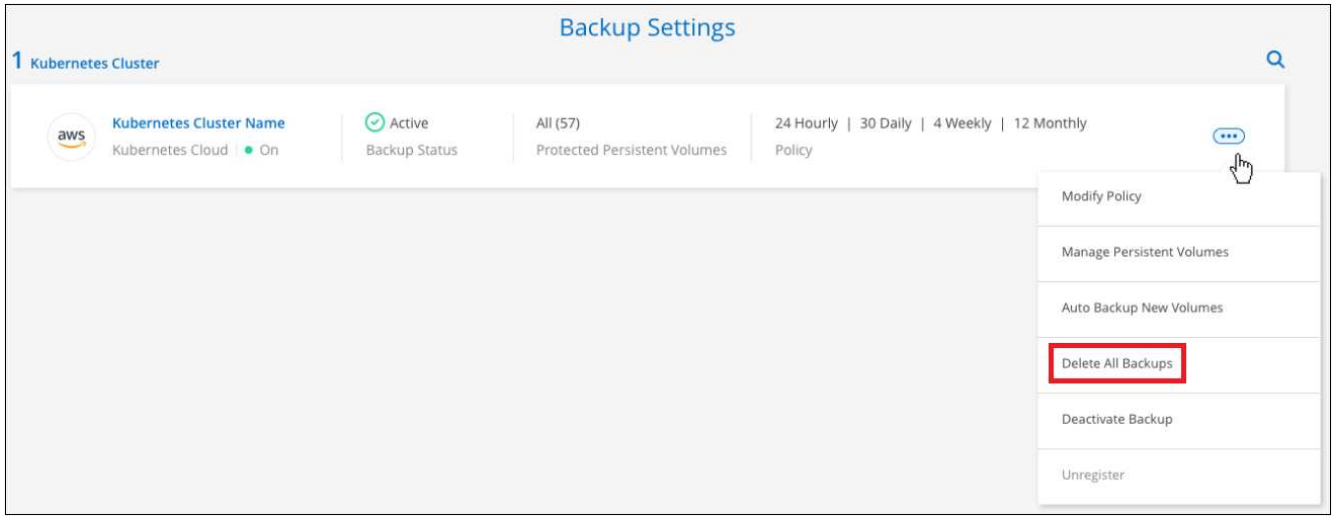
手順

1. [**Kubernetes ***] タブで、 [バックアップ設定 *] を選択します。



ボタンを示すスクリーンショット。"]

2. をクリックします ••• アイコン"] すべてのバックアップを削除する Kubernetes クラスタで、 * すべてのバックアップを削除 * を選択します。



ボタンを選択したスクリーンショット。"]

3. 確認ダイアログボックスで、作業環境の名前を入力し、 * 削除 * をクリックする。

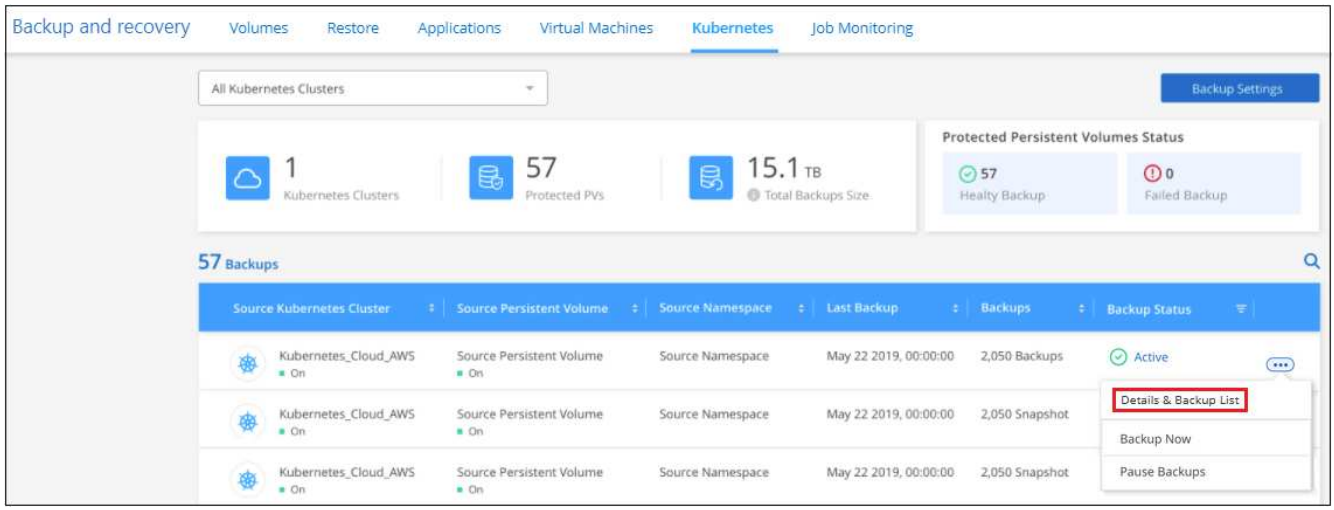
ボリュームのすべてのバックアップファイルを削除する

ボリュームのすべてのバックアップを削除すると、そのボリュームの以降のバックアップも無効になります。

可能です ボリュームのバックアップの作成を再開します ［ Manage Backups （バックアップの管理） ］ ページからいつでもアクセスできます。

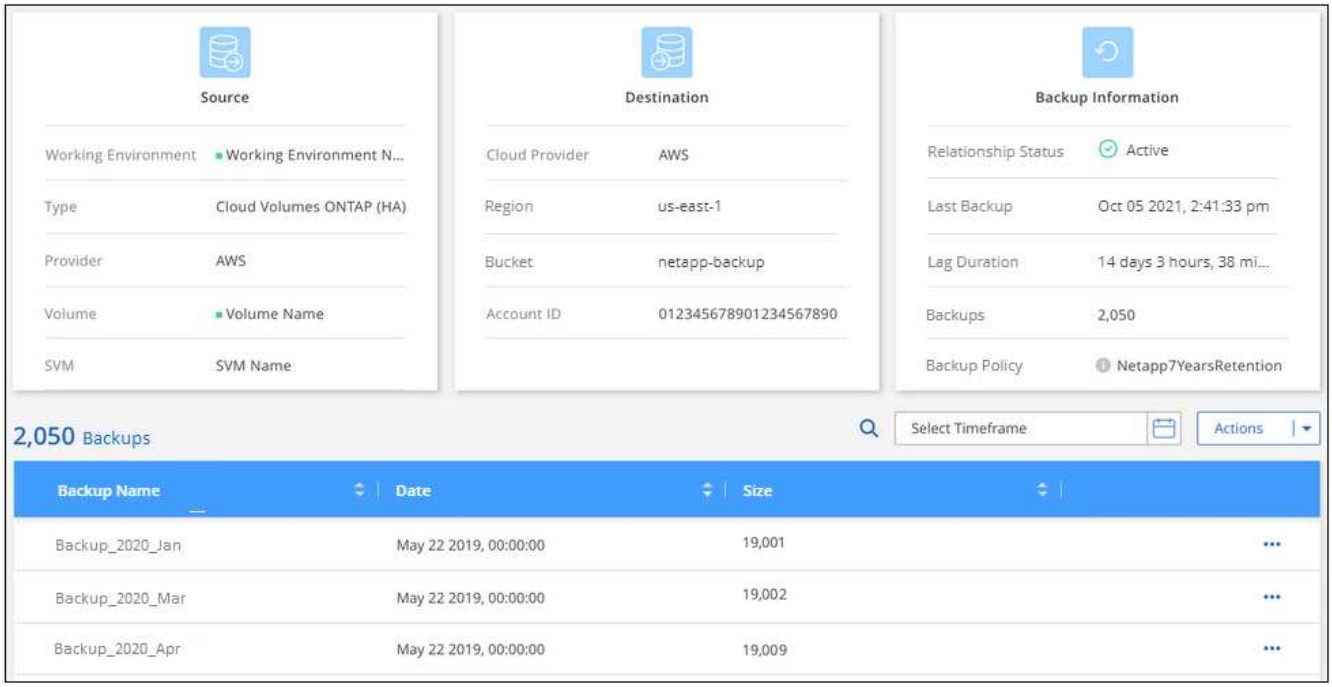
手順

1. [*Kubernetes *] タブで、をクリックします ••• アイコン"] をソースボリュームとして選択し、 * Details & Backup List * を選択します。



ボタンを示すスクリーンショット。"]

すべてのバックアップファイルのリストが表示されます。



2. [* アクション * > * すべてのバックアップを削除 *] をクリックします。

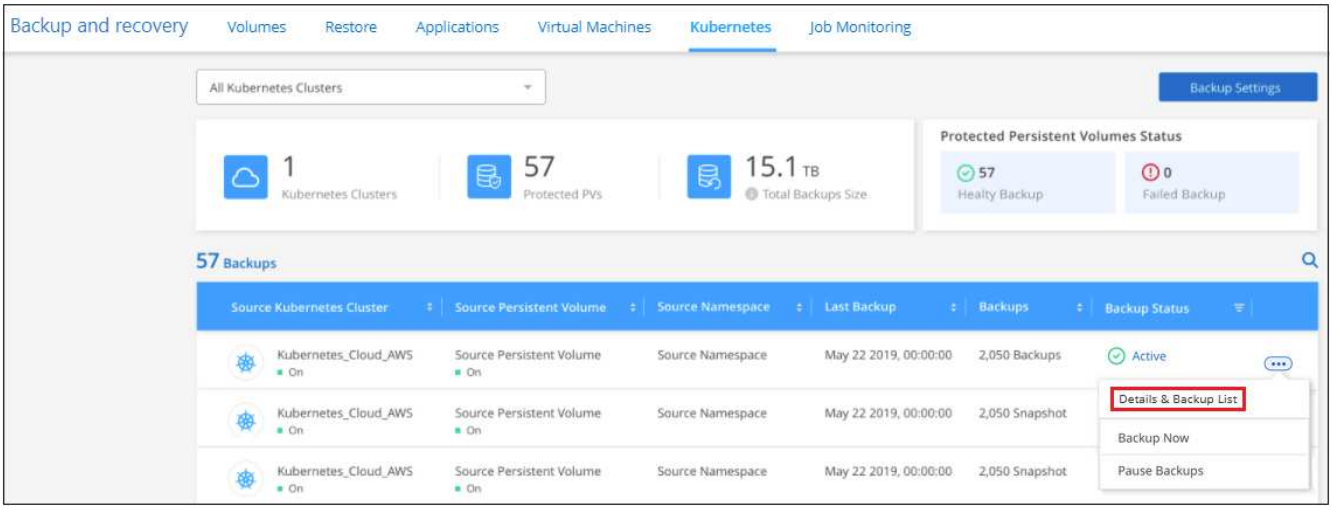
3. 確認ダイアログボックスで、ボリューム名を入力し、 * 削除 * をクリックします。

ボリュームの単一のバックアップファイルを削除する

バックアップファイルは 1 つだけ削除できます。この機能は、 ONTAP 9.8 以降のシステムでボリューム・バックアップを作成した場合にのみ使用できます。

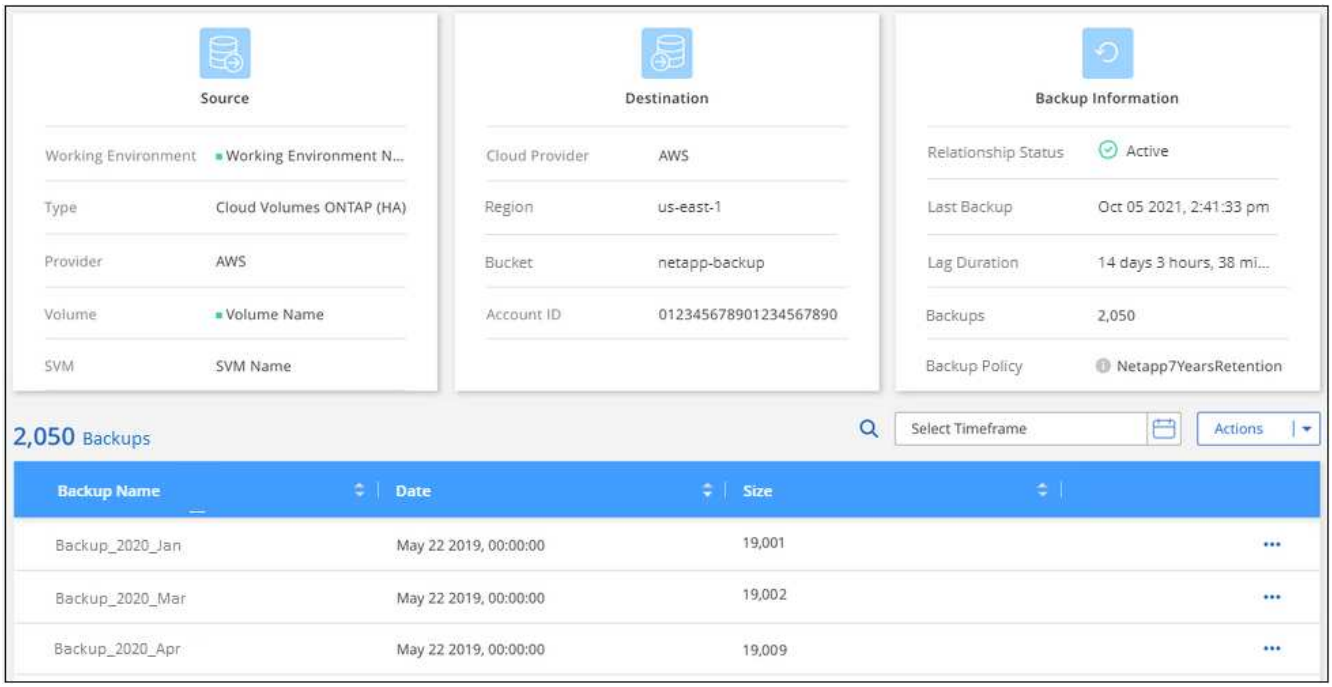
手順

1. [*Kubernetes *] タブで、をクリックします ••• アイコン"] をソースボリュームとして選択し、 * Details & Backup List * を選択します。

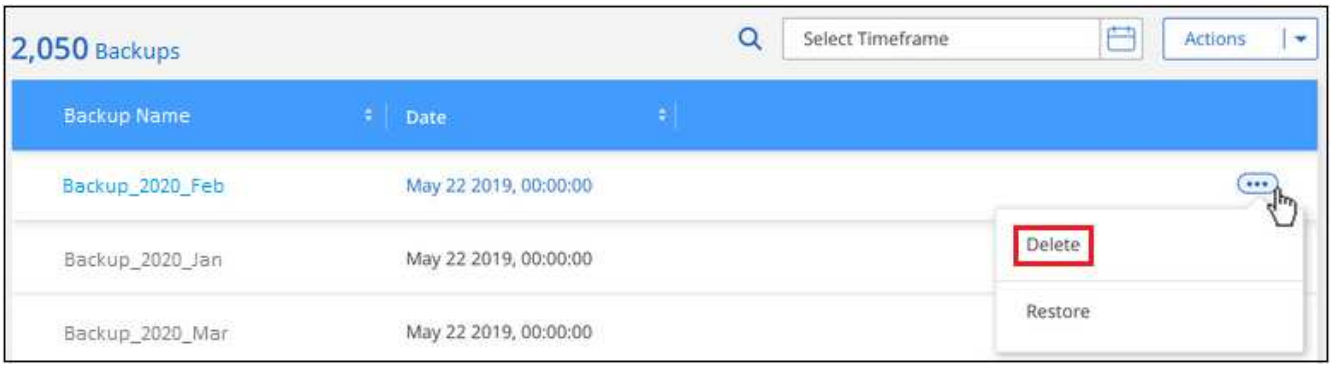


ボタンを示すスクリーンショット。"]

すべてのバックアップファイルのリストが表示されます。



2. をクリックします ••• アイコン"] 削除するボリュームバックアップファイルに対して、 * 削除 * をクリックします。



3. 確認ダイアログボックスで、 * 削除 * をクリックします。

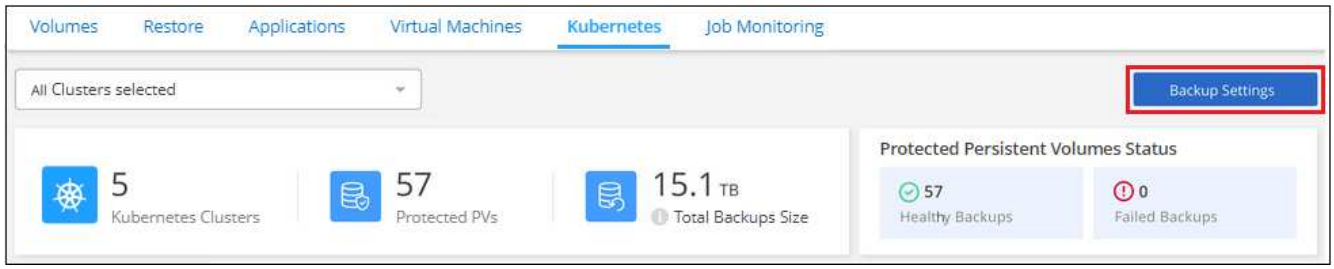
作業環境でのBlueXPのバックアップとリカバリの無効化

作業環境でBlueXPのバックアップとリカバリを無効にすると、システム上の各ボリュームのバックアップが無効になり、またボリュームをリストアする機能も無効になります。既存のバックアップは削除されません。この作業環境からバックアップ・サービスの登録を解除することはありません。基本的には、すべてのバックアップおよびリストア処理を一定期間停止できます。

クラウドから引き続き課金されます が提供する容量のオブジェクトストレージコストのプロバイダ バックアップは自分以外で使用します バックアップを削除します。

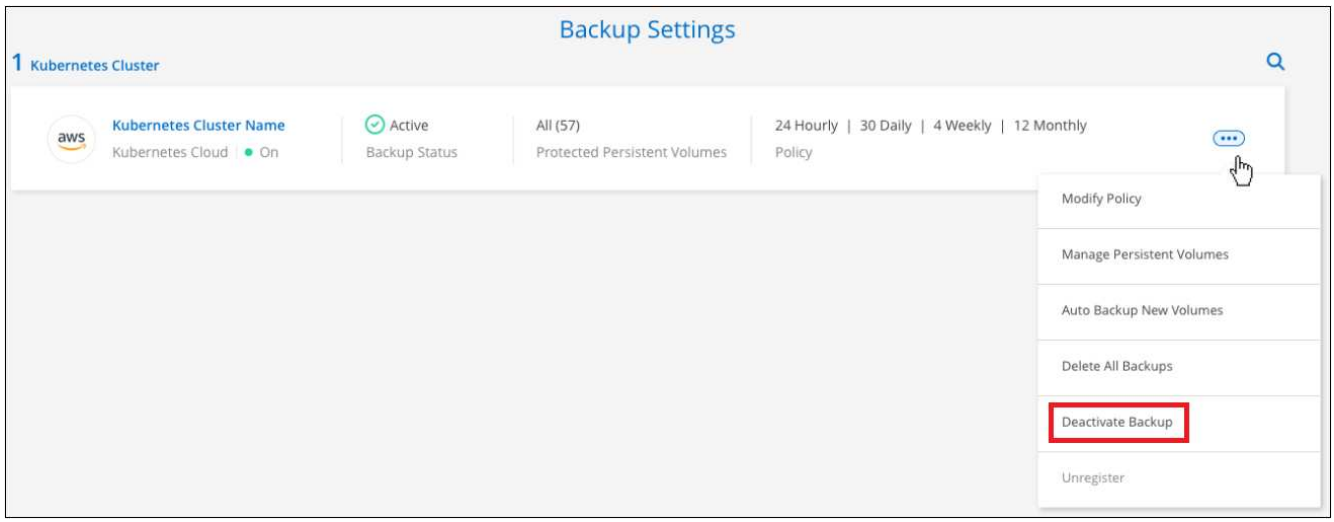
手順

1. [**Kubernetes ***] タブで、 [バックアップ設定 *] を選択します。



ボタンを示すスクリーンショット。"]

2. _ バックアップ設定ページ _ で、をクリックします ••• アイコン"] バックアップを無効にする作業環境または Kubernetes クラスタで、 * バックアップを非アクティブ化 * を選択します。



3. 確認ダイアログボックスで、 * Deactivate * をクリックします。

> バックアップが無効になっている間は、その作業環境に対して * バックアップのアクティブ化 * ボタンが表示されます。このボタンは、作業環境でバックアップ機能を再度有効にする場合にクリックします。

作業環境のBlueXPバックアップおよびリカバリの登録を解除します

バックアップ機能の使用が不要になり、作業環境でのバックアップに対する課金を停止する場合は、作業環境のBlueXPバックアップ/リカバリの登録を解除できます。通常、この機能は、 Kubernetes クラスタを削除する予定でバックアップサービスをキャンセルする場合に使用します。

この機能は、クラスタバックアップの格納先のオブジェクトストアを変更する場合にも使用できます。作業環境のBlueXPバックアップ/リカバリの登録を解除したら、新しいクラウドプロバイダの情報を使用して、そのクラスタのBlueXPバックアップ/リカバリを有効にできます。

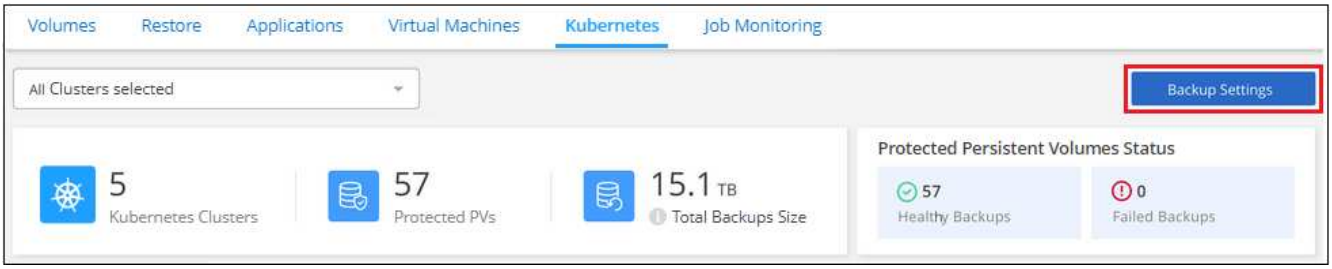
BlueXPのバックアップとリカバリの登録を解除する前に、次の手順をこの順序で実行する必要があります。

- 作業環境でBlueXPのバックアップとリカバリを非アクティブ化します
- その作業環境のバックアップをすべて削除します

登録解除オプションは、これら 2 つの操作が完了するまで使用できません。

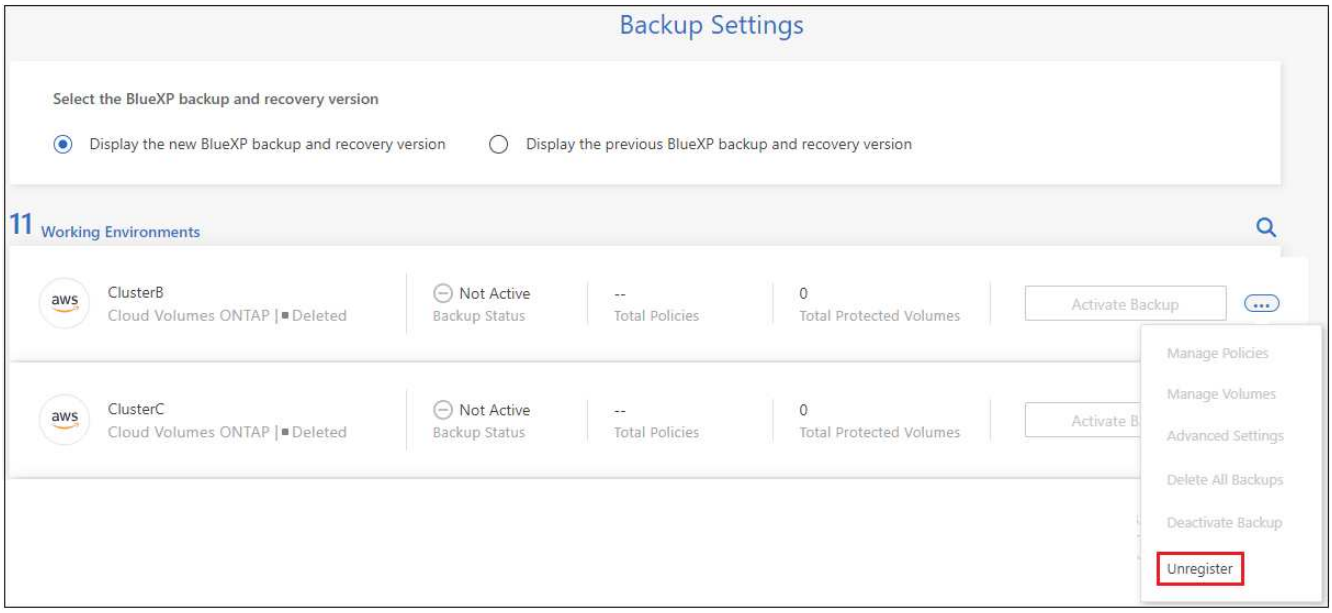
手順

1. **[Kubernetes *]** タブで、 **[** バックアップ設定 *] を選択します。



ボタンを示すスクリーンショット。"]

2. _ バックアップ設定ページ _ で、をクリックします ••• アイコン"] バックアップサービスの登録を解除する Kubernetes クラスタで、 * 登録解除 * を選択します。



3. 確認ダイアログボックスで、 * 登録解除 * をクリックします。

バックアップファイルからの Kubernetes データのリストア

バックアップは、特定の時点のデータをリストアできるように、クラウドアカウントのオブジェクトストアに格納されます。Kubernetes の永続ボリューム全体を、保存したバックアップファイルからリストアできます。

永続ボリュームは、（新しいボリュームとして）同じ作業環境または同じクラウドアカウントを使用している別の作業環境にリストアできます。

サポートされている作業環境とオブジェクトストレージプロバイダ

Kubernetes バックアップファイルから次の作業環境にボリュームをリストアできます。

バックアップファイルの場所	デスティネーションの作業環境 ifdef：aws []
Amazon S3	AWS の Kubernetes クラスタ endif：：aws[] ifdef：Azure []
Azure Blob の略	Azure の Kubernetes クラスタ endif：：azure[] ifdef ::gcp[]
Google クラウドストレージ	Google の Kubernetes クラスタ endif：GCP []

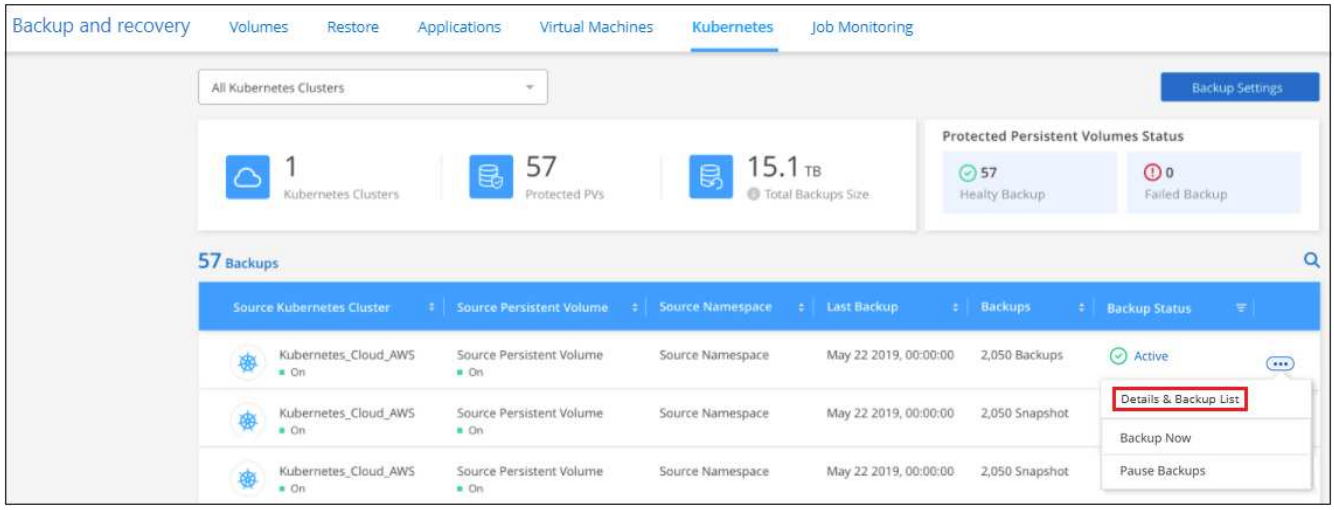
Kubernetes バックアップファイルからのボリュームのリストア

バックアップファイルから永続ボリュームを復元すると、BlueXPはバックアップのデータを使用して_new_volumeを作成します。データは、同じ Kubernetes クラスタ内のボリューム、またはソースの Kubernetes クラスタと同じクラウドアカウントにある別の Kubernetes クラスタにリストアできます。

開始する前に、リストアするボリュームの名前と、新規にリストアされたボリュームの作成に使用するバックアップファイルの日付を確認しておく必要があります。

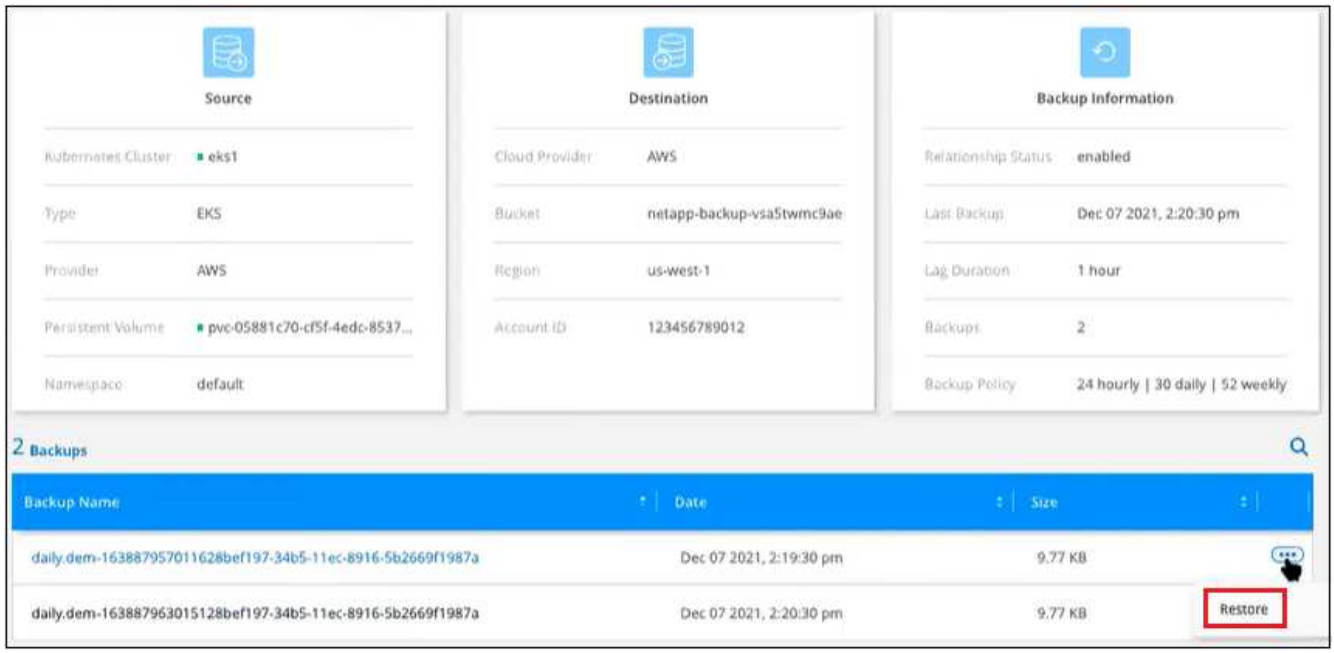
手順

1. BlueXPメニューから、*Protection > Backup and recovery*を選択します。
2. [*Kubernetes *] タブをクリックすると、 [Kubernetes Dashboard] が表示されます。



3. リストアするボリュームを選択し、をクリックします ••• アイコン"]をクリックし、*詳細とバックアップリスト*をクリックします。

   そのボリュームのすべてのバックアップファイルと、ソースボリューム、デスティネーションの場所、およびバックアップの詳細が表示されます。



4. 日付 / タイムスタンプに基づいてリストアする特定のバックアップファイルを選択し、をクリックします ••• アイコン"]をクリックし、次に * Restore * を実行します。

5. Select Destination_page で、ボリュームをリストアする *Kubernetes cluster_where* を選択します。 _ *Namespace* _ 、 _ *Storage Class* 、および new_Persistent ボリューム name _ 。

6. リストア * をクリックすると、 Kubernetes ダッシュボードに戻り、リストア処理の進捗状況を確認できます。

結果

BlueXPは、選択したバックアップに基づいて、Kubernetesクラスタに新しいボリュームを作成します。可能です "この新しいボリュームのバックアップ設定を管理します" 必要に応じて。

BlueXPのバックアップとリカバリ用API

Web UIから利用できるBlueXPのバックアップとリカバリ機能は、RESTful APIからも利用できます。

BlueXPのバックアップとリカバリでは、次の10のカテゴリのエンドポイントが定義されています。

- バックアップ-クラウドリソースとオンプレミスリソースのバックアップ処理を管理し、バックアップデータの詳細を取得します
- カタログ-クエリに基づいて、インデックス付きカタログ検索を管理します（検索とリストア）。
- クラウド-さまざまなクラウドプロバイダリソースに関する情報をBlueXPから取得します
- job - BlueXPデータベースのジョブ詳細エントリを管理します
- ライセンス-作業環境のライセンスの有効性をBlueXPから取得します
- Ransomware scan -ランサムウェアスキャンを特定のバックアップファイルで開始します
- Restore -ボリューム、ファイル、およびフォルダレベルのリストア処理を実行できます
- SFR -単一ファイルレベルのリストア処理（参照とリストア）用にバックアップファイルからファイルを取得します。
- StorageGRID - StorageGRID サーバの詳細を取得し、StorageGRID サーバを検出できます
- 作業環境-バックアップポリシーを管理し、作業環境に関連付けられたデスティネーションオブジェクトストアを設定します

はじめに

BlueXPのバックアップとリカバリAPIの使用を開始するには、ユーザトークン、BlueXPアカウントID、およびBlueXPコネクタIDを取得する必要があります。

API呼び出しを行うときは、Authorizationヘッダーにユーザートークンを、x-agent-idヘッダーにBlueXPコネクタIDを追加します。APIでBlueXPアカウントIDを使用する必要があります。

手順

1. NetApp BlueXP Webサイトからユーザートークンを取得します

   次のリンクからリフレッシュトークンを生成してください。https://services.cloud.netapp.com/refresh-token/.リフレッシュトークンは、ユーザートークンを生成するために使用する英数字文字列です。

```
curl --location --request POST 'https://netapp-cloud-
account.auth0.com/oauth/token?=' \
--header 'Content-Type: application/json' \
-d '{
    "grant_type": "refresh_token",
    "refresh_token": "JxaVHn9cGkX92aPVCkhat3zxxxxxwsC9qMl_pLHkZtsVA",
    "client_id": "Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC"
}'
```

BlueXP Webサイトのユーザートークンには有効期限がありますAPI 応答には、トークンの有効期限を示す「 expires_in 」フィールドが含まれています。トークンを更新するには、もう一度このAPIを呼び出す必要があります。

2. BlueXPアカウントIDを取得します

```
GET 'https://api.bluexp.netapp.com/tenancy/account' -H 'authority:
api.bluexp.netapp.com'
Header:
-H 'accept: application/json'
-H 'accept-language: en-GB,en;q=0.9'
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR.........
```

このAPIは、次のような応答を返します。アカウントIDを取得するには、*[0].[accountPublicId]*の出力を解析します。

```
 [{"accountPublicId":"account-
i6vJXvZW","accountName":"rashidn","isSaas":true,"isGov":false,"isPrivate
PreviewEnabled":false,"is3rdPartyServicesEnabled":false,"accountSerial":
"96064469711530003565","userRole":"Role-1"}.........
. BlueXPコネクタIDを含むx-agent-idを取得します。
```

```
GET curl 'https://api.services.cloud.netapp.com/occm/list-occms/account-
OOnAR4ZS?excludeStandalone=true&source=saas' \
Header:
  -H 'authority: api.services.cloud.netapp.com' \
  -H 'accept: application/json' \
  -H 'accept-language: en-GB,en;q=0.9' \
  -H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5............
```

このAPIは、次のような応答を返します。エージェントIDを取得するには、*occcm.[0].[agent].[AgentID]*の出力を解析します。

```
{"occms":[{"account":"account-
OOnAR4ZS","accountName":"cbs","occm":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Z",
"agentId":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Z","status":"ready","occmName"
:"cbsgcpdevcntsg-
asia","primaryCallbackUri":"http://34.93.197.21","manualOverrideUris":[]
,"automaticCallbackUris":["http://34.93.197.21","http://34.93.197.21/occ
mui","https://34.93.197.21","https://34.93.197.21/occmui","http://10.138
.0.16","http://10.138.0.16/occmui","https://10.138.0.16","https://10.138
.0.16/occmui","http://localhost","http://localhost/occmui","http://local
host:1337","http://localhost:1337/occmui","https://localhost","https://l
ocalhost/occmui","https://localhost:1337","https://localhost:1337/occmui
"],"createDate":"1652120369286","agent":{"useDockerInfra":true,"network"
:"default","name":"cbsgcpdevcntsg-
asia","agentId":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Zclients","provider":"gc
p","systemId":"a3aa3578-bfee-4d16-9e10-
```


APIを使用した例

次の例は、AzureクラウドのEast-US-2リージョンで、日単位、時間単位、週単位のラベルが180日に設定された新しいポリシーを使用して、作業環境でBlueXPのバックアップとリカバリをアクティブ化するAPI呼び出しを示しています。これにより、作業環境でのバックアップのみが有効になり、ボリュームはバックアップされません。

API要求

BlueXPアカウントIDが使用されていることがわかります `account-DpTFcxN3`、BlueXPコネクタID `iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients`およびユーザートークン `Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwkeMwHc4ValobjUmju2x0xUH48g` をクリックします。

```
curl --location --request POST
'https://api.bluexp.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v3/backup/working-
environment/VsaWorkingEnvironment-99hPYEgk' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwk
eMwHc4ValobjUmju2x0xUH48g' \
--data-raw '{
    "provider":"AZURE",
    "backup-policy": {
      "archive-after-days": 180,
      "rule": [
        {
          "label": "hourly",
          "retention": "2"
        },
        {
          "label": "daily",
          "retention": "30"
        },
        {
          "label": "weekly",
          "retention": "52"
        }
      ]
    },
    "ip-space": "Default",
    "region": "eastus2",
    "azure": {
      "resource-group": "rn-test-backup-rg",
      "subscription": "3beb4dd0-25d4-464f-9bb0-303d7cf5c0c2"
    }
  }'
```

応答は、監視可能なジョブ**ID**です。

```
{
 "job-id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a"
}
```

応答を監視します。

```
curl --location --request GET
'https://api.bluexp.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v1/job/1b34b6f6-8f43-40fb-9a52-
485b0dfe893a' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…hE9ss2Nub
K6wZRHUdSaORI7JvcOorUhJ8srqdiUiW6MvuGIFAQIh668of2M3dLbhVDBe8BBMtsa939UGnJx
7Qz6Eg'
```

応答。

```
{
    "job": [
        {
            "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
            "type": "backup-working-environment",
            "status": "PENDING",
            "error": "",
            "time": 1651852160000
        }
    ]
}
```

「**status**」が「**completed**」になるまで監視します。

```
{
    "job": [
        {
            "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
            "type": "backup-working-environment",
            "status": "COMPLETED",
            "error": "",
            "time": 1651852160000
        }
    ]
}
```

API リファレンス

BlueXPの各バックアップとリカバリAPIのドキュメントは、から入手できます https://docs.netapp.com/us-en/bluexp-automation/cbs/overview.html。

参照

AWS S3 アーカイブストレージクラスおよびリストアの読み出し時間

BlueXPのバックアップとリカバリは、2つのS3アーカイブストレージクラスとほとんどのリージョンをサポートしています。

BlueXPのバックアップとリカバリでサポートされるS3アーカイブストレージクラス

バックアップファイルが最初に作成されるときは、 S3_Standard_storage に格納されています。この階層は、アクセス頻度の低いデータを格納するために最適化されていますが、すぐにアクセスすることもできます。30 日経過すると、バックアップは S3_Standard - Infrequent Access_storage クラスに移行してコストを削減します。

ソースクラスタで ONTAP 9.10.1 以降が実行されている場合は、特定の日数（通常は 30 日以上）が経過したあとに S3 Glacier Deep Archive_storage にバックアップを階層化して、コストをさらに最適化することができます。これを「0」または1～999日に設定できます。「0」日に設定した場合、後で1～999日に変更することはできません。

これらの階層のデータは、必要なときにすぐにアクセスすることはできず、取得コストが高くなるため、アーカイブされたバックアップファイルからデータをリストアする頻度を考慮する必要があります。についてのセクションを参照してください アーカイブストレージからのデータのリストア。

- BlueXPのバックアップとリカバリをアクティブ化するときに最初のバックアップポリシーでアーカイブ階層を選択しない場合は、以降のポリシーでは_S3 Glacier_のみがアーカイブオプションになります。
- 最初のバックアップポリシーで_S3 Glacier_を選択した場合は、そのクラスタの以降のバックアップポリシー用に_S3 Glacier Deep Archive_tierに変更できます。
- 最初のバックアップポリシーで_S3 Glacier Deep Archive_を 選択した場合は、その階層がそのクラスタの今後のバックアップポリシーで使用できる唯一のアーカイブ階層になります。

このタイプのライフサイクルルールを使用してBlueXPのバックアップとリカバリを設定する場合は、AWSアカウントでバケットをセットアップするときにライフサイクルルールを設定しないでください。

"S3 ストレージクラスについて説明します"。

アーカイブストレージからのデータのリストア

古いバックアップファイルをアーカイブストレージに保存すると、標準または標準の IA ストレージよりもはるかに低コストですが、リストア処理のためにアーカイブストレージ内のバックアップファイルからデータにアクセスすると、時間がかかり、コストがかかります。

Amazon S3 Glacier と **Amazon S3 Glacier Deep Archive** からデータをリストアするのにどれくらいのコストがかかりますか。

Amazon S3 Glacier からデータを読み出すときは 3 つのリストア優先度を選択でき、 Amazon S3 Glacier Deep Archive からデータを読み出すときは 2 つのリストア優先度を選択できます。S3 Glacier Deep Archive のコストは S3 Glacier よりも低く：

アーカイブ階層	優先度とコストを復元します		
	* 高 *	* 標準 *	* 低 *
* S3 Glacier *	高速な読み出し、コストの最大化	取得速度が低下し、コストが削減されます	読み出しに時間がかかり、コストを最小限に抑えます
* S3 Glacier Deep Archive *		高速な読み出し、コストの増大	取得速度が遅く、コストが最も低い

各メソッドには、 GB 単位の取得料金とリクエストごとの料金が異なります。AWS リージョン別の S3 Glacier の詳細な価格設定については、を参照してください "Amazon S3 の価格設定ページ"。

Amazon S3 Glacier にアーカイブされているオブジェクトのリストアにはどれくらいの時間がかかりますか。

リストアの合計時間は、次の 2 つの要素で構成されます。

- * 取得時間 * ：アーカイブからバックアップファイルを取得して標準ストレージに保存する時間。これは、「水和」時間と呼ばれることもあります。取得時間は、選択したリストア優先度によって異なります。

アーカイブ階層	優先度と取得時間のリストア		
	* 高 *	* 標準 *	* 低 *
* S3 Glacier *	3 ～ 5 分	3 ～ 5 時間	5～12時間
* S3 Glacier Deep Archive *		12時間	48時間

- * リストア時間 * ： Standard ストレージのバックアップファイルからデータをリストアする時間。アーカイブ層を使用しない場合、この時間は標準ストレージから直接実行される通常のリストア処理と同じです。

Amazon S3 Glacier と S3 Glacier Deep Archive の読み出しオプションの詳細については、を参照してください "これらのストレージクラスに関する Amazon FAQ"。

Azure のアーカイブ階層およびリストアの読み出し時間

BlueXPのバックアップとリカバリでは、1つのAzureアーカイブアクセス階層とほとんどのリージョンがサポートされます。

BlueXPのバックアップとリカバリでサポートされるAzure Blobアクセス階層

バックアップファイルが最初に作成されるときは、 _Cool _ アクセス層に保存されます。この階層は、アクセス頻度の低いデータを格納するために最適化されていますが、必要に応じてすぐにアクセスできます。

ソースクラスタで ONTAP 9.10.1 以降が実行されている場合は、コストをさらに最適化するために、特定の日数（通常は 30 日以上）後に _Cool _To Azure Archive_storage からバックアップを階層化することを選択できます。この階層のデータは、必要なときにすぐにアクセスすることはできず、取得コストが高くなるため、アーカイブされたバックアップファイルからデータをリストアする頻度を考慮する必要があります。次のセクション About を参照してください アーカイブストレージからのデータのリストア。

このタイプのライフサイクルルールを使用してBlueXPのバックアップとリカバリを設定する場合は、Azureアカウントでコンテナをセットアップするときにライフサイクルルールを設定しないでください。

"Azure Blob アクセス階層の概要について説明します"。

アーカイブストレージからのデータのリストア

古いバックアップファイルをアーカイブストレージに保存するのは Cool ストレージよりもはるかに安価ですが、リストア処理用に Azure Archive のバックアップファイルからデータにアクセスするには時間がかかり、コストも高くなります。

Azure Archive からデータをリストアするのにどれくらいのコストがかかりますか？

Azure Archive からデータを取得する際に選択できるリストア優先度は 2 つあります。

- * 高い * ：高速な読み出し、コストの増大
- * 標準 * ：読み出し速度が遅く、コストが削減されます

各メソッドには、 GB 単位の取得料金とリクエストごとの料金が異なります。Azure リージョン別の Azure Archive の詳細な価格設定については、を参照してください "Azure の料金体系のページです"。

> 高優先度は、AzureからStorageGRID システムにデータをリストアする場合はサポートされていません。

Azure Archive にアーカイブされたデータをリストアするのにどれくらいの時間がかかりますか。

リストア時間は次の 2 つの要素で構成されます。

- * 取得時間 * ：アーカイブされたバックアップファイルを Azure Archive から取得して Cool Storage に保存する時間。これは、「水和」時間と呼ばれることもあります。読み出し時間は、選択したリストア優先度によって異なります。
  - * 高 * ： 1 時間未満
  - * 標準 * ： 15 時間以内
- * リストア時間 * ： Cool ストレージ内のバックアップファイルからデータをリストアする時間。この時間は、アーカイブ層を使用しないクールストレージからの一般的なリストア処理と同じです。

Azure Archive の読み出しオプションの詳細については、を参照してください "Azure に関する FAQ です"。

Googleアーカイブストレージクラスとリストアの読み出し時間

BlueXPのバックアップとリカバリは、1つのGoogleアーカイブストレージクラスとほとんどのリージョンでサポートされます。

BlueXPのバックアップとリカバリでサポートされるGoogleアーカイブストレージクラス

バックアップファイルが最初に作成されるときは、_Standard_storageに保存されます。この階層は、アクセス頻度の低いデータを格納するために最適化されていますが、すぐにアクセスすることもできます。

オンプレミスクラスタでONTAP 9.12.1以降を使用している場合は、コストをさらに最適化するために、BlueXPのバックアップとリカバリのUIで、古いバックアップを_Archive_storageに階層化することができます。この階層のデータには高い読み出しコストが必要なため、アーカイブされたバックアップファイルからデータをリストアする頻度を考慮する必要があります。についてのセクションを参照してください アーカイブストレージからのデータのリストア。

このタイプのライフサイクルルールを使用してBlueXPのバックアップとリカバリを設定する場合は、Googleアカウントでバケットをセットアップするときにライフサイクルルールを設定しないでください。

"Googleのストレージクラスについて説明します"。

アーカイブストレージからのデータのリストア

古いバックアップファイルをアーカイブストレージに保存すると、標準ストレージよりもはるかに低コストですが、リストア処理のためにアーカイブストレージ内のバックアップファイルからデータにアクセスすると、所要時間が若干長くなり、コストが増大します。

Google Archiveからデータを復元するのにどのくらいのコストがかかりますか。

地域別のGoogle Cloud Storageの詳細な価格設定については、を参照してください "Google Cloud Storageの価格設定ページ"。

Google Archiveにアーカイブされているオブジェクトをリストアするのにどれくらいの時間がかかりますか。

リストアの合計時間は、次の 2 つの要素で構成されます。

- 取得時間：アーカイブからバックアップファイルを取得して標準ストレージに保存する時間。これは、「水和」時間と呼ばれることもあります。他のクラウドプロバイダが提供する「最低目的」のストレージソリューションとは異なり、データには数ミリ秒でアクセスできます。
- * リストア時間 * ： Standard ストレージのバックアップファイルからデータをリストアする時間。アーカイブ層を使用しない場合、この時間は標準ストレージから直接実行される通常のリストア処理と同じです。

Azure でマルチアカウントアクセスのバックアップを設定する

BlueXPのバックアップとリカバリでは、ソースCloud Volumes ONTAP ボリュームの場所とは異なるAzureアカウントにバックアップファイルを作成できます。どちらのアカウントも、BlueXP Connectorがインストールされているアカウントとは異なる場合があります。

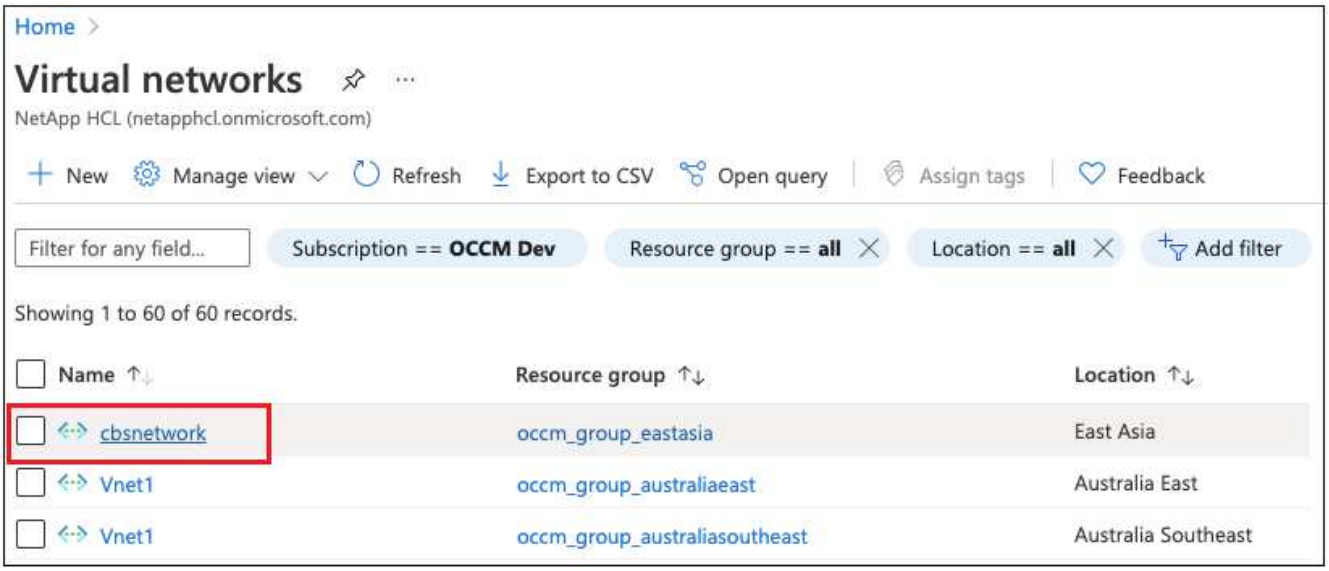
これらの手順は、を実行している場合にのみ必要です "Cloud Volumes ONTAP データの Azure BLOB ストレージへのバックアップ"。

この方法で設定を行うには、次の手順を実行します。

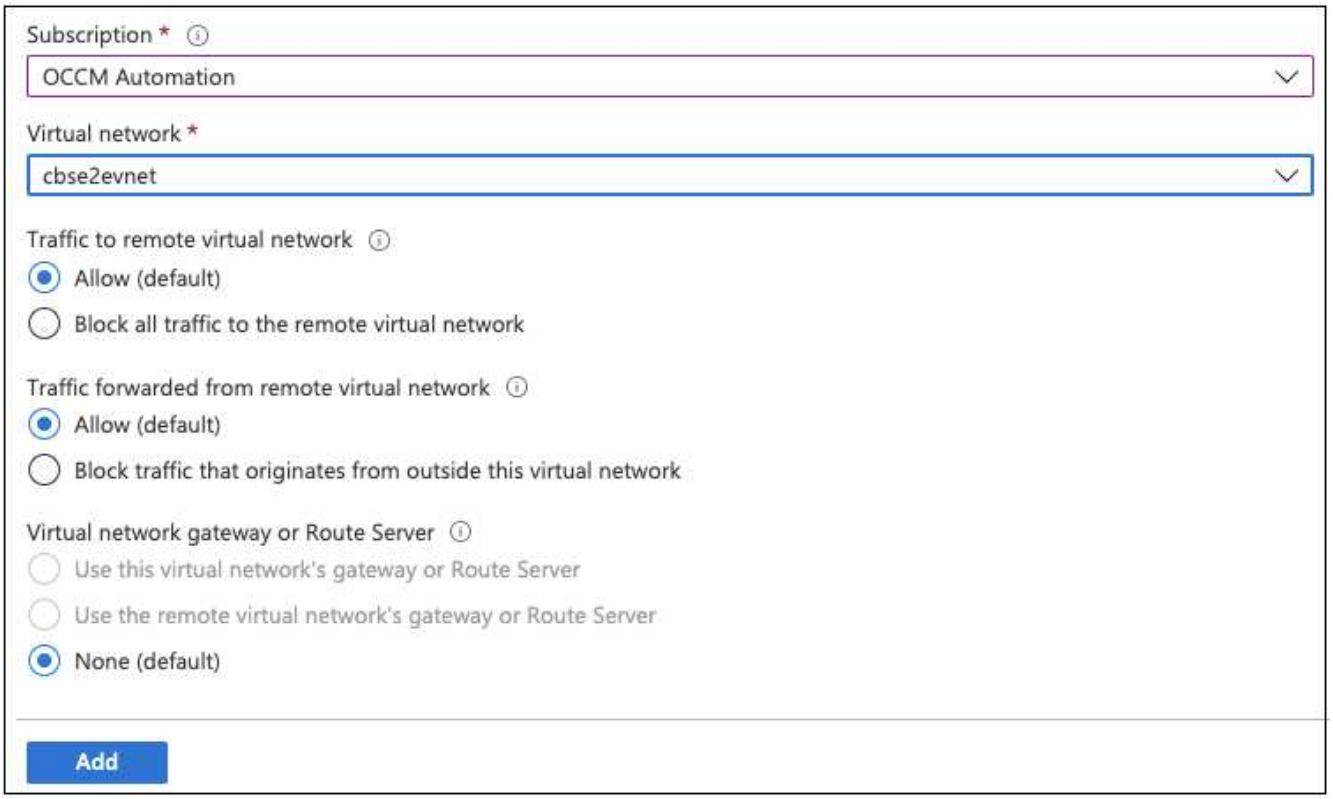
アカウント間の **VNet** ピアリングを設定します

BlueXPで別のアカウント/リージョンでCloud Volumes ONTAP システムを管理する場合は、VNetピアリングを設定する必要があることに注意してください。ストレージアカウントの接続に VNet ピアリングは必要ありません。

1. Azure ポータルにログインし、ホームから仮想ネットワークを選択します。
2. サブスクリプション 1 として使用するサブスクリプションを選択し、ピアリングを設定する VNet 上でクリックします。

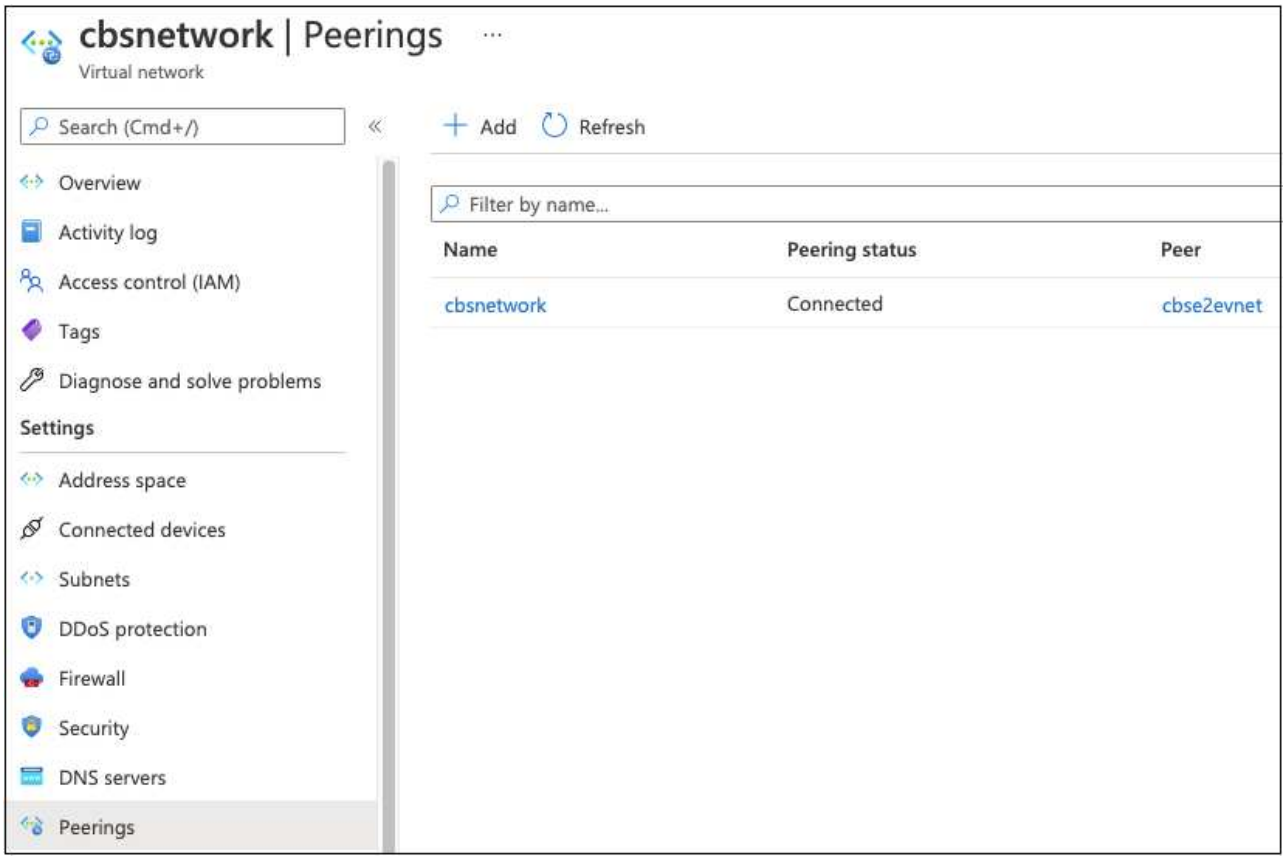


3. **cbsnetwork** を選択し、左パネルから **peerings** をクリックし、 * Add * をクリックします。



4. ピアリングページで次の情報を入力し、 * 追加 * をクリックします。
   - このネットワークのピアリングリンク名：ピアリング接続を識別する任意の名前を指定できます。
   - リモート仮想ネットワークピアリングリンク名：リモート VNet を識別するための名前を入力します。

- すべての選択をデフォルト値のままにします。
- [サブスクリプション] で、サブスクリプション 2 を選択します。
- 仮想ネットワーク：ピアリングを設定するサブスクリプション 2 の仮想ネットワークを選択します。



5. サブスクリプション 2 VNet 内で同じ手順を実行し、サブスクリプション 1 のサブスクリプションおよびリモート VNet の詳細を指定します。

Subscription *
OCCM Dev

Virtual network *
cbsnetwork

Traffic to remote virtual network
- (●) Allow (default)
- ( ) Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network
- (●) Allow (default)
- ( ) Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server
- ( ) Use this virtual network's gateway or Route Server
- ( ) Use the remote virtual network's gateway or Route Server
- (●) None (default)

Add

ピアリング設定が追加されます。

cbse2evnet | Peerings
Virtual network

Search (Cmd+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings

Address space
Connected devices
Subnets
DDoS protection
Firewall
Security
DNS servers
Peerings

Add Refresh

Filter by name...

Name	Peering status	Peer
cbsnetworkpeer	Connected	cbsnetwork

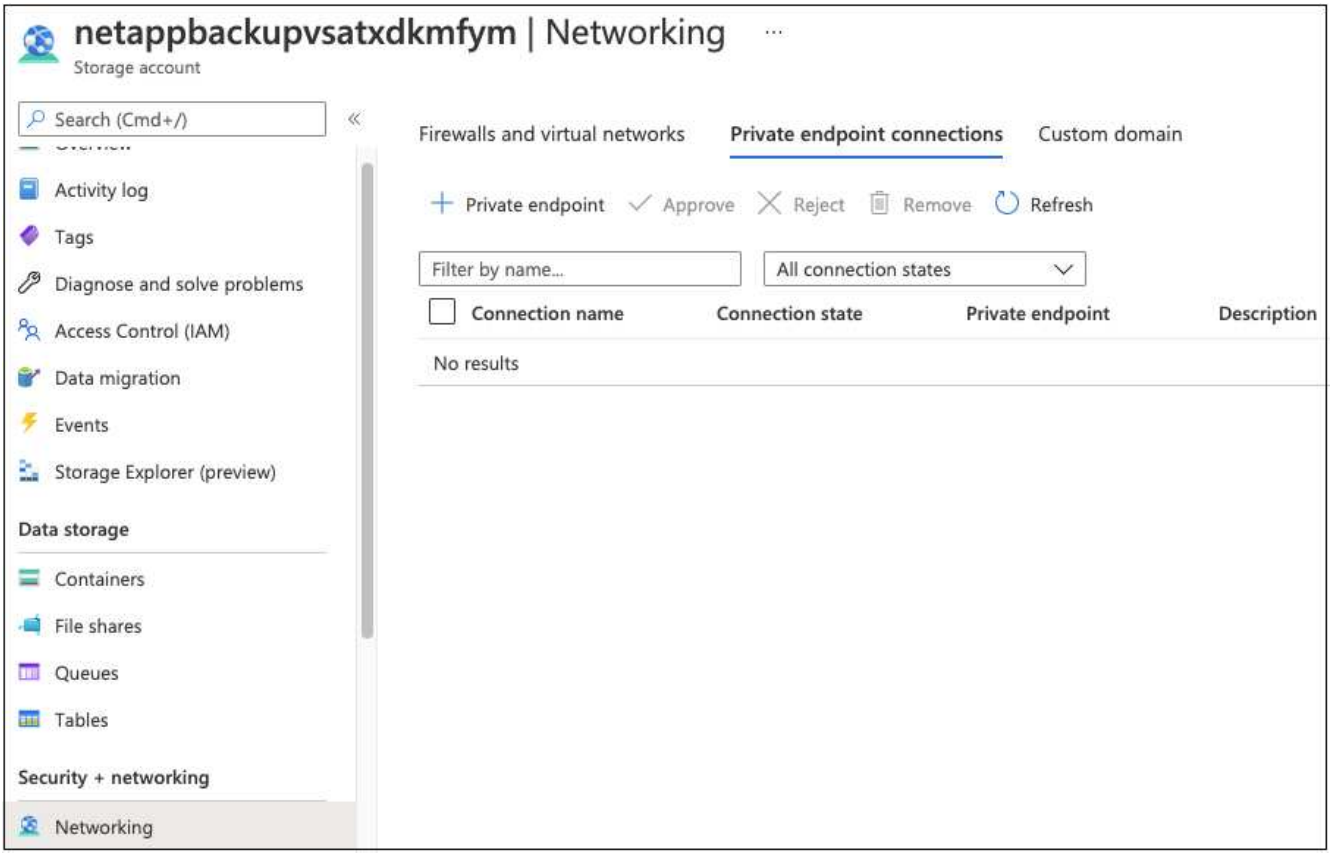
ストレージアカウントのプライベートエンドポイントを作成します

次に、ストレージアカウント用のプライベートエンドポイントを作成する必要があります。この例では、サブスクリプション 1 でストレージアカウントが作成され、 Cloud Volumes ONTAP システムはサブスクリプション 2 で実行されています。

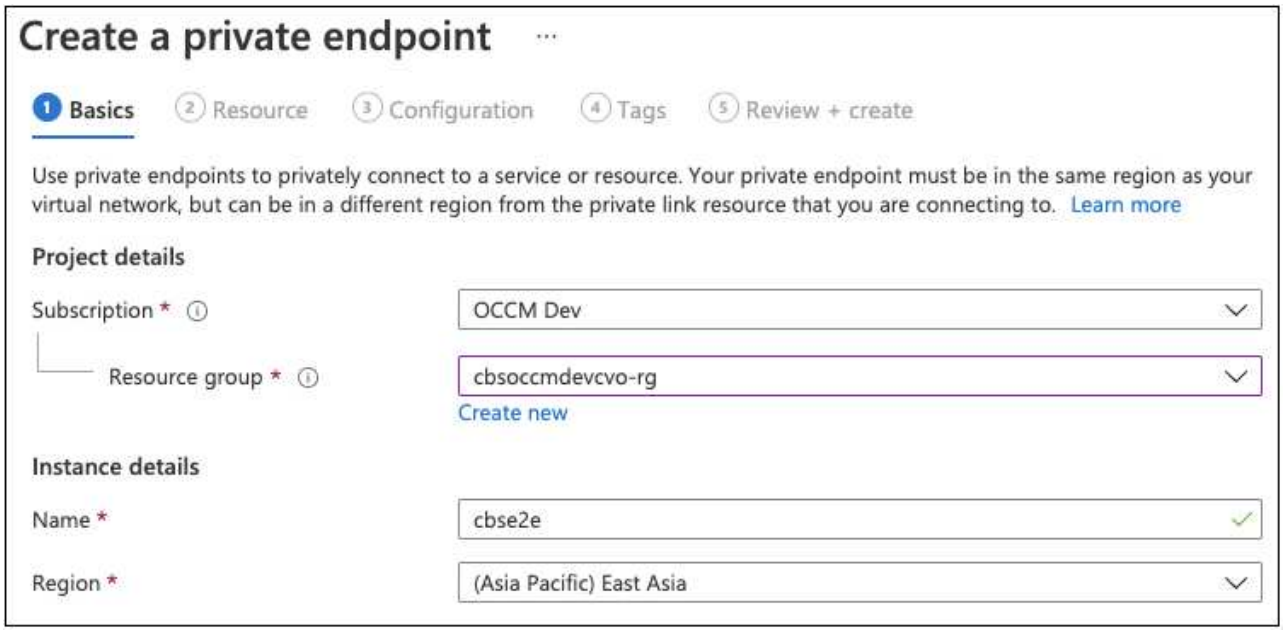
> 次の操作を実行するには、ネットワーク作成者の権限が必要です。

```
{
  "id": "/subscriptions/d333af45-0d07-4154-
943dc25fbbce1b18/providers/Microsoft.Authorization/roleDefinitions/4d97b98
b-1d4f-4787-a291-c67834d212e7",
  "properties": {
    "roleName": "Network Contributor",
    "description": "Lets you manage networks, but not access to them.",
    "assignableScopes": [
      "/"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/*/read",
          "Microsoft.Insights/alertRules/*",
          "Microsoft.Network/*",
          "Microsoft.ResourceHealth/availabilityStatuses/read",
          "Microsoft.Resources/deployments/*",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Support/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

1. [ストレージアカウント]>[ネットワーク]>[プライベートエンドポイント接続]に移動し、*+プライベートエンドポイント*をクリックします。

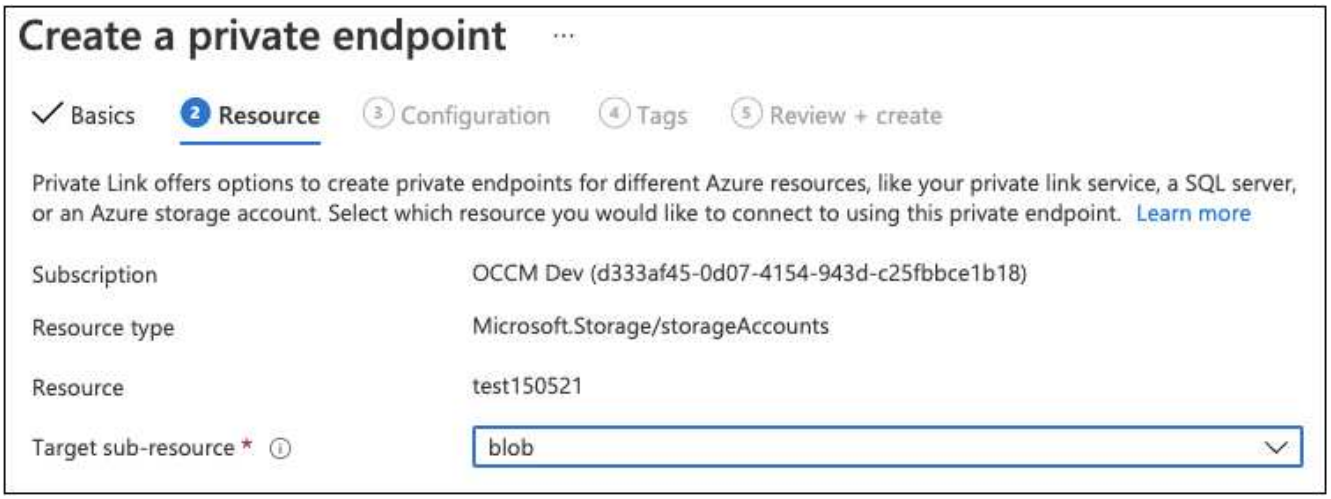


2. Private Endpoint_Basics_page で、次の手順を実行します。
   - サブスクリプション2（BlueXP ConnectorおよびCloud Volumes ONTAP システムが展開されている場所）とリソースグループを選択します。
   - エンドポイント名を入力します。
   - リージョンを選択します。



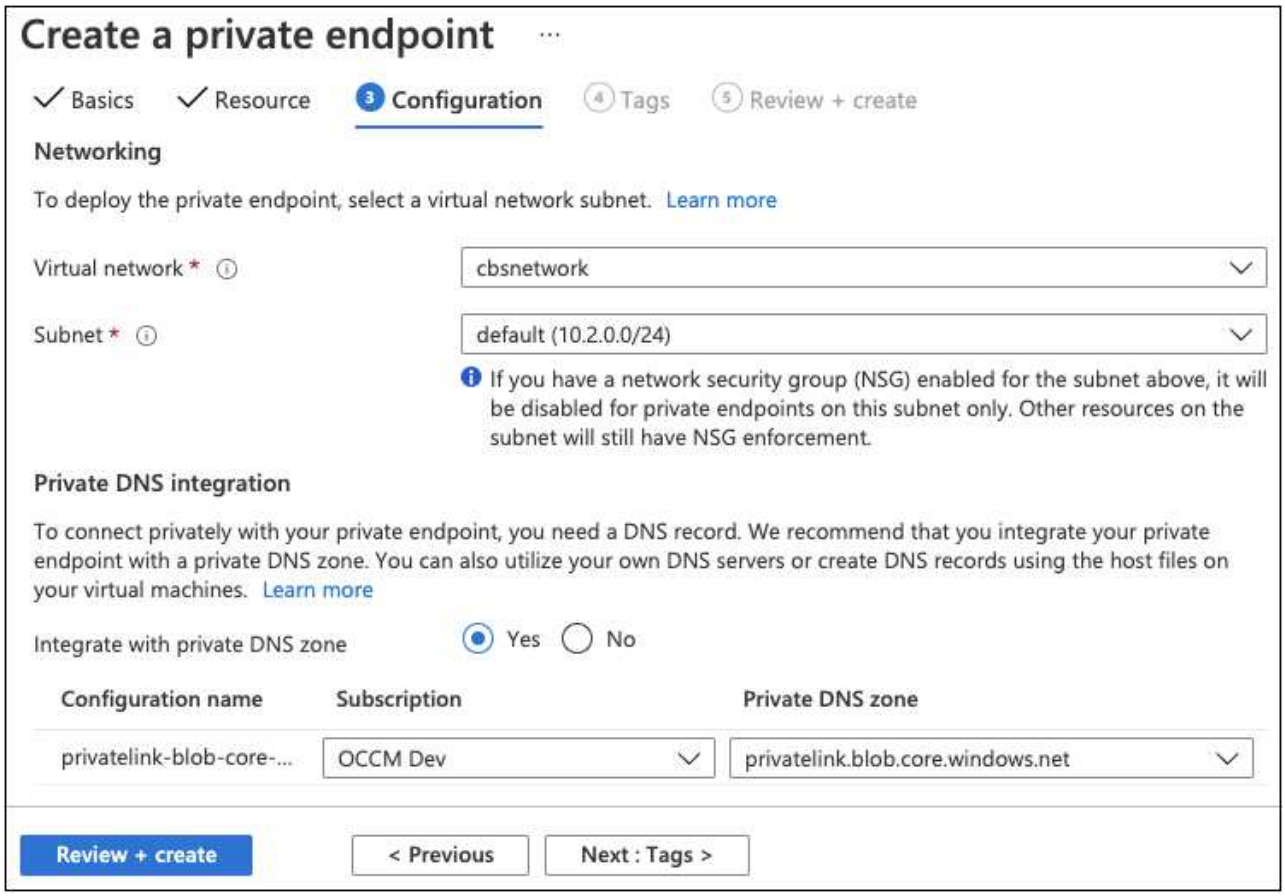
ページの詳細を示すスクリーンショット。"]

3. _Resource_page で ' ターゲットサブリソースとして *blob * を選択します



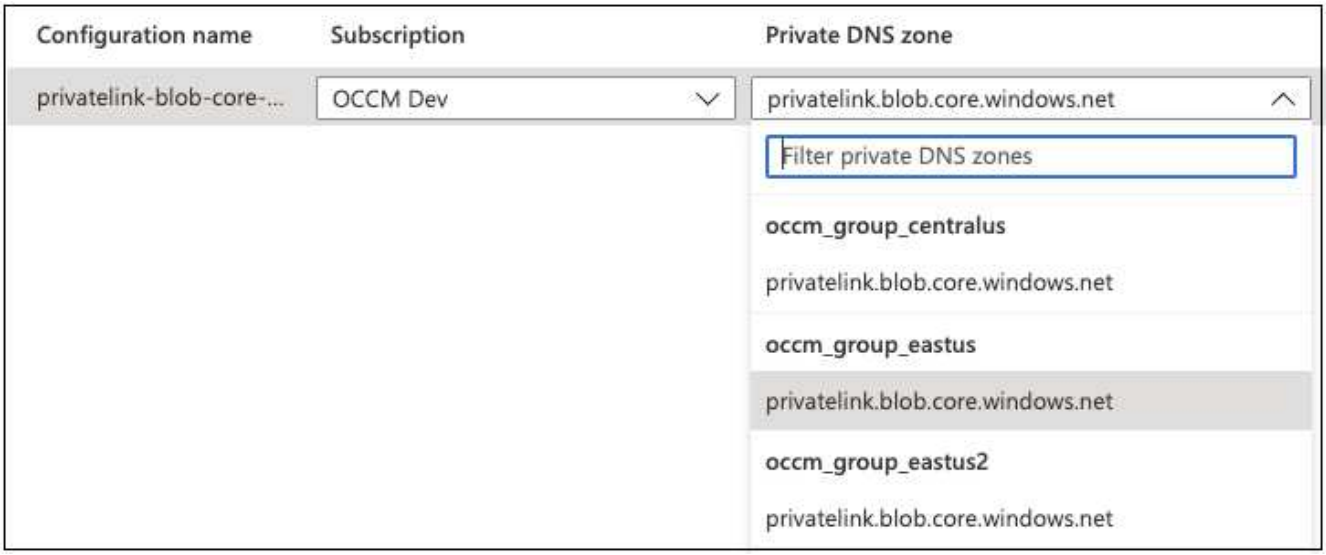
ページの詳細を示すスクリーンショット。"]

4. 設定ページで、次の操作を行います。
   - 仮想ネットワークとサブネットを選択します。
   - [はい *] ラジオボタンをクリックして、 [プライベート DNS ゾーンと統合] を選択します。



ページの詳細を示すスクリーンショット。"]

5. [プライベート DNS ゾーン] リストで、正しいリージョンからプライベートゾーンが選択されていることを確認し、 [* レビュー + 作成 *] をクリックします。



ページでのプライベートゾーンの選択を示すスクリーンショット。"]

これで、ストレージアカウント（サブスクリプション 1 ）は、サブスクリプション 2 で実行されている Cloud Volumes ONTAP システムにアクセスできます。

6. Cloud Volumes ONTAP システムでBlueXPのバックアップとリカバリの有効化をもう一度実行すると、成功します。

ダークサイトで**BlueXP**のバックアップとリカバリのデータをリストア

インターネットアクセスのないサイト（プライベートモード）でBlueXPのバックアップとリカバリを使用すると、BlueXPのバックアップとリカバリの設定データがバックアップが格納されているStorageGRIDまたはONTAP S3バケットにバックアップされます。将来、BlueXP Connectorホストシステムを搭載した問題を使用している場合は、新しいコネクタを導入して、BlueXPの重要なバックアップとリカバリデータをリストアできます。

BlueXPのバックアップとリカバリをクラウドプロバイダやインターネットにアクセスできる独自のホストシステムに導入されているSaaS環境で使用する場合は、BlueXPのバックアップとリカバリの重要な設定データがすべてクラウドにバックアップされて保護されます。コネクタ付きの問題がある場合は、新しいコネクタを作成して作業環境を追加するだけで、バックアップの詳細が自動的にリストアされます。

バックアップされるデータには次の2種類があります。

- BlueXPバックアップおよびリカバリデータベース-すべてのボリューム、バックアップファイル、バックアップポリシー、および設定情報のリストが格納されます。
- インデックス付きカタログ・ファイル-検索とリストア機能に使用される詳細なインデックスが含まれており、リストアするボリューム・データを検索する際に、検索を迅速かつ効率的に行うことができます。

このデータは1日1回午前0時にバックアップされ、各ファイルの最大7つのコピーが保持されます。コネクタが複数のオンプレミスONTAP作業環境を管理している場合、BlueXPのバックアップファイルとリカバリファイルは、最初にアクティブ化した作業環境のバケットに配置されます。

BlueXPのバックアップ/リカバリデータベースやインデックスカタログファイルにボリュームデータが含まれることはありません。

BlueXPのバックアップとリカバリのデータを新しいコネクタにリストア

オンプレミスコネクタで重大な障害が発生した場合は、新しいコネクタをインストールし、BlueXPのバックアップとリカバリのデータを新しいコネクタにリストアする必要があります。

BlueXPのバックアップとリカバリシステムを動作状態に戻すには、次の4つのタスクを実行する必要があります。

- 新しいBlueXPコネクタを取り付けます
- BlueXPのバックアップとリカバリデータベースをリストア
- インデックス付けされたカタログファイルを復元します
- すべてのオンプレミスONTAP システムとStorageGRID システムをBlueXP UIに再検出します

システムが正常に動作していることを確認したら、新しいバックアップファイルを作成することをお勧めします。

必要なもの

バックアップファイルが保存されているStorageGRIDまたはONTAP S3バケットから、最新のデータベースとインデックスのバックアップにアクセスする必要があります。

- BlueXPのバックアップとリカバリ用MySQLデータベースファイル

  このファイルはバケット内の次の場所にあります `netapp-backup-<GUID>/mysql_backup/`という名前が付けられています `CBS_DB_Backup_<day>_<month>_<year>.sql`。

- インデックス付きカタログバックアップのzipファイル

  このファイルはバケット内の次の場所にあります `netapp-backup-<GUID>/catalog_backup/`という名前が付けられています `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip`。

新しいオンプレミス**Linux**ホストに新しいコネクタをインストールします

新しいBlueXPコネクタをインストールするときは、元のコネクタにインストールしたものと同じリリースのソフトウェアをダウンロードしてください。BlueXPのバックアップとリカバリのデータベース構造を定期的に変更すると、新しいソフトウェアリリースと元のデータベースバックアップとの互換性がなくなる可能性があります。可能です "Backupデータベースをリストアした後、Connectorソフトウェアを最新バージョンにアップグレードします"。

1. "新しいオンプレミスLinuxホストにBlueXP Connectorをインストールします"
2. 作成した管理者ユーザー資格情報を使用してBlueXPにログインします。

BlueXPのバックアップとリカバリデータベースをリストア

1. バックアップの場所から新しいコネクタホストにMySQLバックアップをコピーします。次の例のファイル名「CBS_DB_Backup_23_05_2023.sql」を使用します。

2. 次のコマンドを使用して、MySQL Dockerコンテナにバックアップをコピーします。

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. 次のコマンドを使用してMySQLコンテナシェルを入力します。

```
docker exec -it ds_mysql_1 sh
```

4. コンテナシェルで、「env」を導入します。
5. MySQL DBのパスワードが必要なので、キー「mysql_root_password」の値をコピーします。
6. 次のコマンドを使用して、BlueXPのバックアップとリカバリのMySQL DBをリストアします。

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. 次のSQLコマンドを使用して、BlueXPのバックアップとリカバリのMySQL DBが正しくリストアされたことを確認します。

```
mysql -u root -p cloud_backup
```

パスワードを入力します。

```
mysql> show tables;
mysql> select * from volume;
```

表示されているボリュームが、元の環境に存在していたボリュームと同じかどうかを確認します。

インデックス付けされたカタログファイルを復元します

1. インデックスカタログバックアップzipファイル（例のファイル名「Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip」を使用）をバックアップの場所から「/opt/application/netapp/cbs」フォルダの新しいコネクタホストにコピーします。
2. 次のコマンドを使用して、「Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip」ファイルを解凍します。

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. *ls *コマンドを実行して、フォルダ"catalogdb1"が下のサブフォルダ"changes"と"snapshots"で作成されていることを確認します。

ONTAP クラスタと**StorageGRID** システムを検出

1. "オンプレミスのONTAP 作業環境をすべて検出できます" 以前の環境で使用できていたものです。これには、S3サーバとして使用しているONTAPシステムも含まれます。
2. "StorageGRID システムを検出"。

StorageGRID 環境の詳細を設定

を使用して元のコネクタセットアップを行ったときの、ONTAP の作業環境に関連付けられているStorageGRID システムの詳細を追加します "BlueXP API"。

これらの手順は、StorageGRID にデータをバックアップするONTAP システムごとに実行する必要があります。

1. 次のOAuth/token APIを使用して、認証トークンを抽出します。

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'User-Agent:
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:100101 Firefox/108.0'
-H 'Accept: application/json' -H 'Accept-Language: en-US,en;q=0.5' -H
'Accept-Encoding: gzip, deflate' -H 'Content-Type: application/json' -d
'{"username":admin@netapp.com,"password":"Netapp@123","grant_type":"pass
word"}
> '
```

このAPIは、次のような応答を返します。次のように、認証トークンを取得できます。


```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```


2. テナンシー/外部/リソースAPIを使用して、作業環境IDとX-Agent-IDを抽出します。

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

このAPIは、次のような応答を返します。「resourceIdentifier」の下の値は_WorkingEnvironment ID_を示し、「AgentID」の下の値は_x-agent-id_を示します。

3. 作業環境に関連付けられたStorageGRID システムの詳細を使用して、バックアップとリカバリのデータベースを更新します。StorageGRID の完全修飾ドメイン名と、次に示すアクセスキーおよびストレージキーを入力してください。

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

BlueXPのバックアップとリカバリの設定を確認

1. 各ONTAP 作業環境を選択し、右パネルのバックアップ/リカバリ・サービスの横にある*バックアップの表示*をクリックします。

   ボリュームに対して作成されたすべてのバックアップが表示されます。

2. リストア・ダッシュボードの[検索とリストア]セクションで、[インデックス設定]をクリックします。

   インデックスカタログが有効になっている作業環境が、以前に有効なままであることを確認します。

3. [検索と復元]ページで、いくつかのカタログ検索を実行して、インデックス付けされたカタログの復元が正常に完了したことを確認します。

BlueXPバックアップ/リカバリサービスを再起動します

場合によっては、BlueXPのバックアップとリカバリサービスの再起動が必要になることがあります。

BlueXPコネクタには、BlueXPのバックアップとリカバリ機能が組み込まれています。コネクタをクラウドにデプロイしたか、コネクタをLinuxシステムに手動でインストールしたかに応じて、サービスを再起動するためにさまざまな初期手順を実行する必要があります。

手順

1. コネクタが実行されているLinuxシステムに接続します。

コネクタの位置	手順
クラウドの導入	の手順に従ってください "コネクタLinux仮想マシンに接続しています" 使用しているクラウドプロバイダによって異なります。
手動インストール	Linuxシステムにログインします。

2. コマンドを入力してサービスを再起動します。

コネクタの位置	コマンドを実行します
クラウドの導入	`docker restart cloudmanager_cbs`
インターネットアクセスを使用した手動インストール	`docker restart cloudmanager_cbs`
インターネットにアクセスせずに手動でインストールします	`docker restart ds_cloudmanager_cbs_1`

知識とサポート

サポートに登録します

BlueXPとそのストレージソリューションおよびサービスに固有のテクニカルサポートを受けるには、サポート登録が必要です。Cloud Volumes ONTAPシステムの主要なワークフローを有効にするには、サポート登録も必要です。

サポートに登録しても、クラウドプロバイダのファイルサービスでNetAppのサポートは有効になりません。クラウドプロバイダのファイルサービスとそのインフラ、またはサービスを使用する解決策に関連するテクニカルサポートについては、該当する製品のBlueXPドキュメントの「困ったときは」を参照してください。

- "ONTAP 対応の Amazon FSX"
- "Azure NetApp Files の特長"
- "Cloud Volumes Service for Google Cloud"

サポート登録の概要

サポート資格を有効にする登録には、次の2つの形式があります。

- BlueXPアカウントIDサポートサブスクリプションの登録(BlueXPの[サポートリソース]ページにある20桁の960xxxxxxxxxシリアル番号)。

  これは、BlueXP内のすべてのサービスのシングルサポートサブスクリプションIDとして機能します。各BlueXPアカウントレベルのサポート契約が登録されている必要があります。

- クラウドプロバイダのマーケットプレイスでのサブスクリプションに関連付けられているCloud Volumes ONTAP のシリアル番号を登録している（909201xxxxxxxxのシリアル番号）。

  これらのシリアル番号は、通常PAY_GOシリアル番号と呼ばれ、Cloud Volumes ONTAP の導入時にBlueXPによって生成されます。

両方のタイプのシリアル番号を登録することで、サポートチケットのオープンやケースの自動生成などの機能を利用できます。登録を完了するには、以下の手順でNetApp Support Site（NSS）アカウントをBlueXPに追加してください。

NetAppサポートに**BlueXP**アカウントを登録します

サポートに登録してサポート利用資格をアクティブ化するには、BlueXPアカウントの1人のユーザがNetApp Support SiteアカウントをBlueXPログインに関連付ける必要があります。ネットアップサポートへの登録方法は、NetApp Support Site （NSS）アカウントがあるかどうかによって異なります。

NSSアカウントをお持ちの既存のお客様

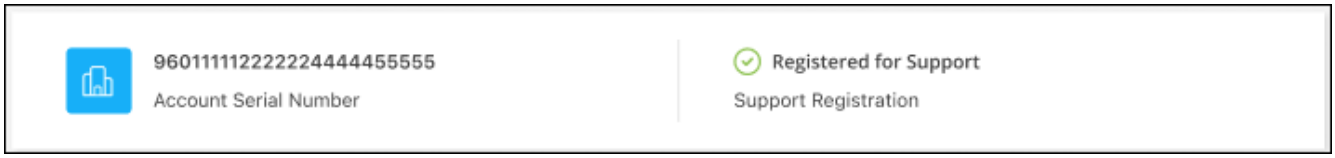
NSSアカウントをお持ちのネットアップのお客様は、BlueXPからサポートに登録するだけで済みます。

手順

1. BlueXPコンソールの右上で、[設定]アイコンを選択し、*[クレデンシャル]*を選択します。

2. [ユーザクレデンシャル]*を選択します。
3. [NSSクレデンシャルの追加]*を選択し、NetApp Support Site（NSS）認証プロンプトに従います。
4. 登録プロセスが正常に完了したことを確認するには、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。

   [リソース]ページに、アカウントがサポートに登録されていることが表示されます。

   他のBlueXPユーザにNetApp Support Siteアカウントが関連付けられていない場合、このサポート登録ステータスは表示されません。ただし、BlueXPアカウントがサポートに登録されていないわけではありません。アカウント内の1人のユーザーがこれらの手順を実行している限り、アカウントは登録されています。

NSSアカウントを持たない既存のお客様

NetAppの既存のお客様で、ライセンスとシリアル番号は_NO_NSSアカウントしかお持ちでない場合は、NSSアカウントを作成してBlueXPログインに関連付ける必要があります。

手順

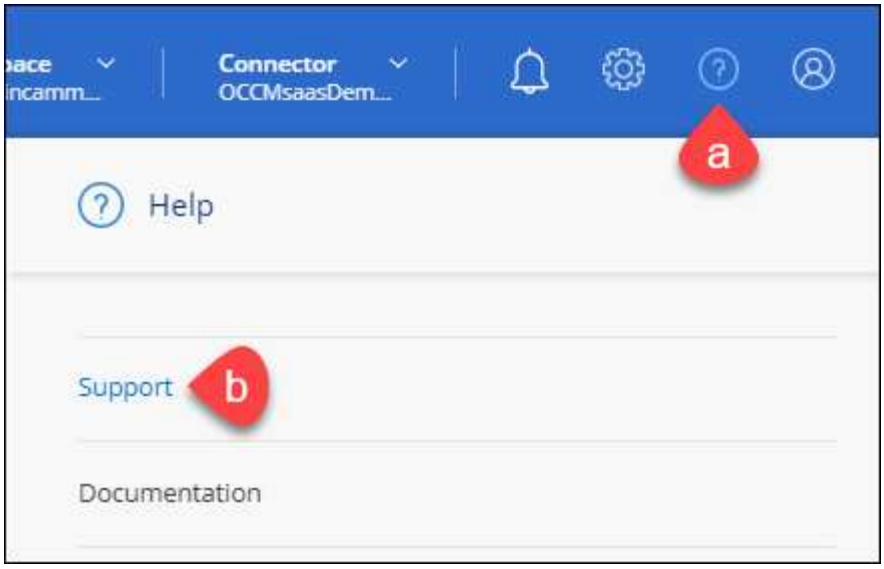
1. を実行してNetApp Support Site アカウントを作成します "NetApp Support Site ユーザー登録フォーム"
   a. 適切なユーザレベルを選択してください。通常は*ネットアップのお客様/エンドユーザ*がこれに該当します。
   b. 必ず、上記のシリアル番号フィールドに使用されているBlueXPアカウントのシリアル番号(960xxxx)をコピーしてください。これにより、アカウント処理が高速化されます。
2. の手順を実行して、新しいNSSアカウントをBlueXPログインに関連付けます NSSアカウントをお持ちの既存のお客様。

ネットアップのソリューションを初めて導入する場合は

ネットアップ製品を初めてご利用になり、NSSアカウントをお持ちでない場合は、以下の手順に従ってください。

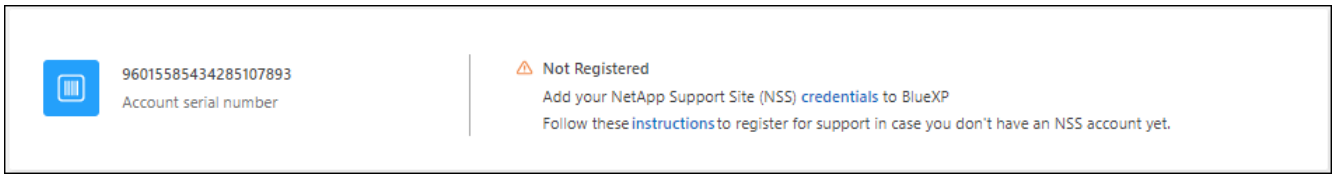
手順

1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。



メニューのスクリーンショット。サポートは最初に表示されるオプションです"]

2. サポート登録ページでアカウントIDのシリアル番号を確認します。



メニューのスクリーンショット。サポートは最初に表示されるオプションです"]

3. に移動します "ネットアップサポート登録サイト" 「ネットアップ登録のお客様ではありません」を選択します。
4. 必須フィールドに入力します（赤いアスタリスクのフィールド）。
5. [製品ライン（Product Line ）]フィールドで、[Cloud Manager *]を選択し、該当する課金プロバイダーを選択します。
6. 上記の手順2からアカウントのシリアル番号をコピーし、セキュリティチェックを完了して、ネットアップのグローバルデータプライバシーポリシーを確認します。

   この安全なトランザクションを完了するために、メールボックスに電子メールがすぐに送信されます。確認メールが数分で届かない場合は、必ずスパムフォルダを確認してください。

7. Eメールからアクションを確認します。

   確認ではネットアップにリクエストが送信され、NetApp Support Site アカウントを作成することを推奨します。

8. を実行してNetApp Support Site アカウントを作成します "NetApp Support Site ユーザー登録フォーム"
   a. 適切なユーザレベルを選択してください。通常は*ネットアップのお客様/エンドユーザ*がこれに該当します。
   b. シリアル番号フィールドには、上記のアカウントのシリアル番号（960xxxx）を必ずコピーしてください。これにより、アカウント処理が高速化されます。

完了後

このプロセスについては、ネットアップからご連絡ください。これは、新規ユーザ向けの1回限りのオンボーディング演習です。

NetApp Support Siteアカウントを作成したら、の手順を実行してアカウントをBlueXPログインに関連付けます NSSアカウントをお持ちの既存のお客様。

Cloud Volumes ONTAPサポートのためにNSSクレデンシャルを関連付けます

NetApp Support Siteで次の主要なワークフローを有効にするには、BlueXPアカウントにクレデンシャルを関連付ける必要がCloud Volumes ONTAPあります。

- 従量課金制のCloud Volumes ONTAPシステムのサポートを登録しています

  お使いのシステムのサポートを有効にし、ネットアップのテクニカルサポートリソースにアクセスするには、 NSS アカウントを用意する必要があります。

- お客様所有のライセンスを使用（BYOL）する場合のCloud Volumes ONTAP の導入

  ライセンスキーをBlueXPでアップロードし、購入した契約期間のサブスクリプションを有効にするには、NSSアカウントを提供する必要があります。これには、期間の更新の自動更新も含まれます。

- Cloud Volumes ONTAP ソフトウェアを最新リリースにアップグレードしています

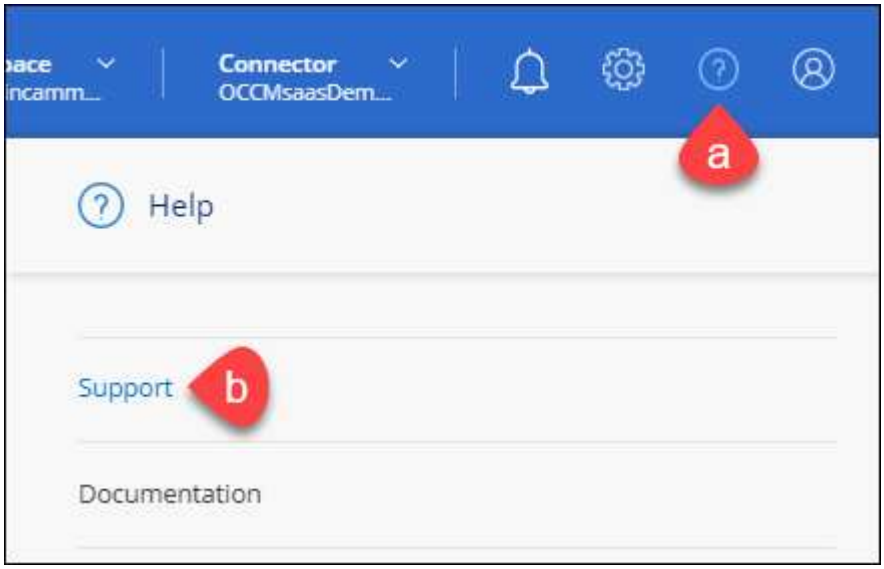
NSSクレデンシャルをBlueXPアカウントに関連付ける方法は、BlueXPユーザログインに関連付けられたNSSアカウントとは異なります。

これらのNSSクレデンシャルは、特定のBlueXPアカウントIDに関連付けられています。BlueXPアカウントに属するユーザは、*[サポート]>[NSS管理]*からこれらのクレデンシャルにアクセスできます。

- お客様レベルのアカウントをお持ちの場合は、1つ以上のNSSアカウントを追加することもできます。
- パートナーアカウントまたはリセラーアカウントをお持ちの場合は、1つ以上のNSSアカウントを追加することはできますが、お客様レベルのアカウントと一緒に追加することはできません。

手順

1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。



メニューのスクリーンショット。

サポートは最初に表示されるオプションです"]

2. [NSS Management]>[Add NSS Account]*を選択します。
3. プロンプトが表示されたら、*続行*を選択してMicrosoftログインページにリダイレクトします。

   NetAppでは、サポートとライセンスに固有の認証サービスのIDプロバイダとしてMicrosoftエントラIDを使用します。

4. ログインページで、NetApp Support Siteの登録 E メールアドレスとパスワードを入力して認証プロセスを実行します。

   これらのアクションにより、BlueXPはライセンスのダウンロード、ソフトウェアのアップグレード検証、および将来のサポート登録などの目的でNSSアカウントを使用できます。

   次の点に注意してください。

   - NSSアカウントは、お客様レベルのアカウントである必要があります（ゲストアカウントや一時アカウントではありません）。複数のお客様レベルのNSSアカウントを設定できます。
   - NSSアカウントがパートナーレベルのアカウントの場合、作成できるNSSアカウントは1つだけです。お客様レベルのNSSアカウントを追加しようとすると、パートナーレベルのアカウントが存在する場合は、次のエラーメッセージが表示されます。

     「別のタイプのNSSユーザーがすでに存在するため、このアカウントではNSS顧客タイプは許可されていません。」

   既存のお客様レベルのNSSアカウントがあり、パートナーレベルのアカウントを追加しようとする場合も同様です。

   - ログインに成功すると、ネットアップはNSSのユーザ名を保存します。

     これはシステムによって生成されたIDで、電子メールにマッピングされます。[**NSS Management**]ページで、から電子メールを表示できます ••• メニュー。

   - ログイン認証情報トークンを更新する必要がある場合は、の[認証情報の更新*]オプションも使用できます ••• メニュー。

     このオプションを使用すると、再度ログインするように求められます。これらのアカウントのトークンは90日後に期限切れになります。このことを通知する通知が投稿されます。

ヘルプを表示します

ネットアップでは、BlueXPとその クラウド サービス をさまざまな方法でサポートしています。ナレッジベース（ KB ）記事やコミュニティフォーラムなど、 24 時間 365 日利用可能な幅広いセルフサポートオプションをご用意しています。サポート登録には、Web チケット処理によるリモートテクニカルサポートが含まれます。

クラウドプロバイダのファイルサービスのサポート

クラウドプロバイダのファイルサービスとそのインフラ、またはサービスを使用する解決策に関連するテクニカルサポートについては、該当する製品のBlueXPドキュメントの「困ったときは」を参照してください。

- "ONTAP 対応の Amazon FSX"
- "Azure NetApp Files の特長"
- "Cloud Volumes Service for Google Cloud"

BlueXPおよびそのストレージソリューションとサービスに固有のテクニカルサポートを受けるには、以下に記載されているサポートオプションを使用してください。

セルフサポートオプションを使用します

次のオプションは、 1 日 24 時間、週 7 日間無料でご利用いただけます。

- ドキュメント

  現在表示しているBlueXPのマニュアル。

- "ナレッジベース"

  BlueXPナレッジベースで問題のトラブルシューティングに役立つ記事を検索します。

- "コミュニティ"

  BlueXPコミュニティに参加して、進行中のディスカッションをフォローしたり、新しいディスカッションを作成したりできます。

ネットアップサポートと一緒にケースを作成します

上記のセルフサポートオプションに加え、サポートを有効にしたあとで問題が発生した場合は、ネットアップサポートの担当者と相談して解決できます。

始める前に

- [ケースの作成]*機能を使用するには、最初にNetApp Support SiteクレデンシャルをBlueXPログインに関連付ける必要があります。 "BlueXPログインに関連付けられているクレデンシャルの管理方法について説明します"。
- シリアル番号のあるONTAPシステムのケースをオープンする場合は、そのシステムのシリアル番号にNSSアカウントを関連付ける必要があります。

手順

1. BlueXPで、*[ヘルプ]>[サポート]*を選択します。
2. [**Resources**]ページで、[Technical Support]で次のいずれかのオプションを選択します。

   a. 電話で誰かと話をしたい場合は、*[電話]*を選択します。netapp.comのページに移動し、電話番号が表示されます。

   b. [ケースの作成]*を選択して、NetAppサポートスペシャリストとのチケットをオープンします。

      - **Service**:問題 が関連付けられているサービスを選択します。たとえば、サービス内のワークフローまたは機能を備えたテクニカルサポート問題 に固有のBlueXPなどです。
      - 作業環境：ストレージに該当する場合は、* Cloud Volumes ONTAP *または*オンプレミス*を選択し、関連する作業環境を選択します。

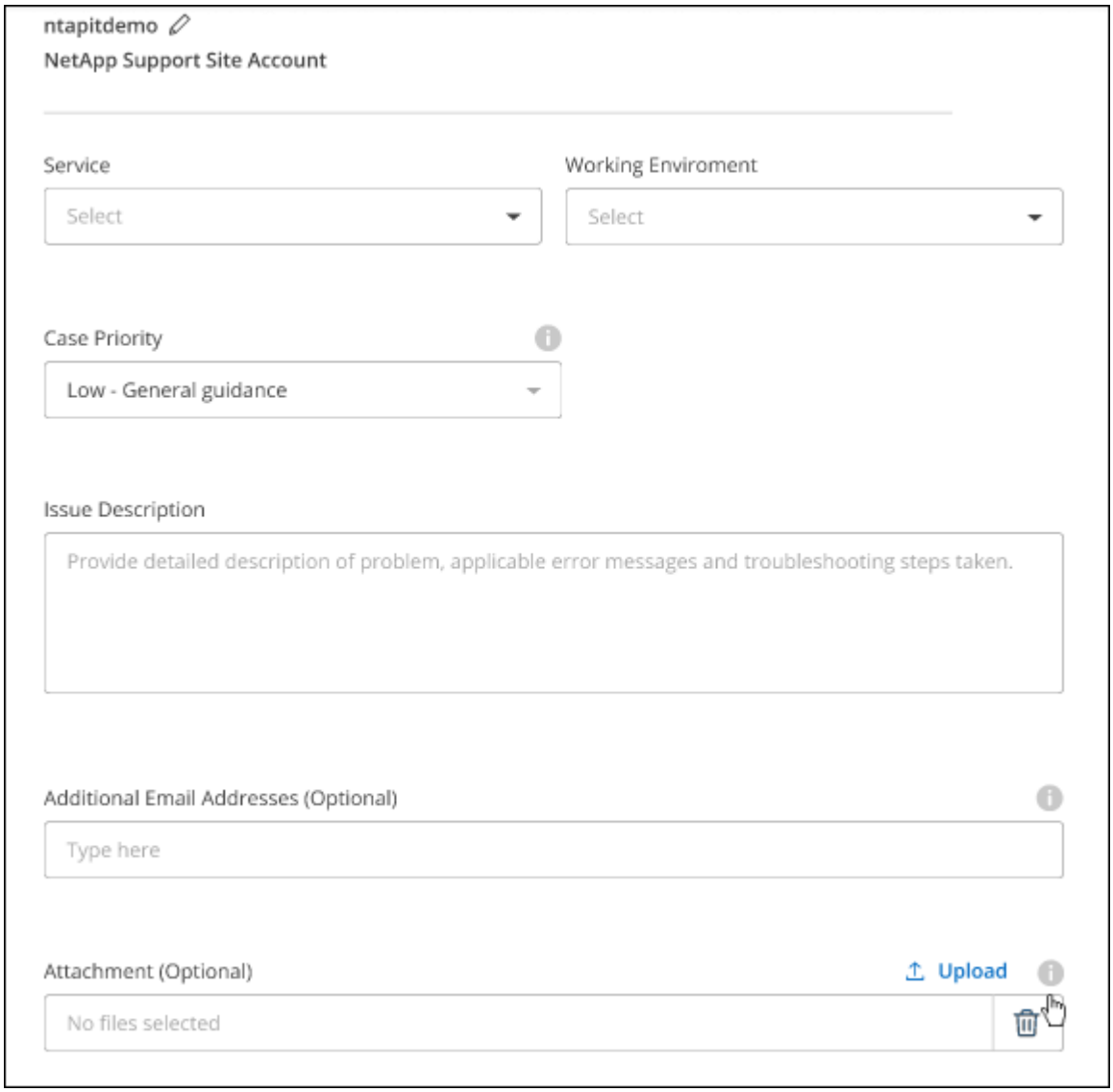
作業環境のリストは、サービスの上部バナーで選択したBlueXPアカウント、ワークスペース、コネクタの範囲内にあります。

- ケース優先度：ケースの優先度を選択します。優先度は、[低]、[中]、[高]、[クリティカル]のいずれかになります。

  これらの優先度の詳細を確認するには、フィールド名の横にある情報アイコンの上にマウスポインタを合わせます。

- *事象の説明 *：実行したエラーメッセージやトラブルシューティング手順など、問題の詳細な概要 を入力します。
- その他のメールアドレス：この問題 を他のユーザーに知らせる場合は、追加のメールアドレスを入力します。
- 添付ファイル（オプション）：一度に1つずつ、最大5つの添付ファイルをアップロードできます。

  添付ファイルはファイルあたり25 MBに制限されています。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、 doc/docx、xls/xlsx、およびcsv。



完了後

ポップアップにサポートケース番号が表示されます。ネットアップのサポート担当者がケースを確認し、すぐに対応させていただきます。

サポートケースの履歴を確認するには、*[設定]>[タイムライン]*を選択し、「サポートケースの作成」というアクションを検索します。 右端のボタンをクリックすると、アクションを展開して詳細を表示できます。

ケースを作成しようとすると、次のエラーメッセージが表示される場合があります。

"選択したサービスに対してケースを作成する権限がありません"

このエラーは、NSSアカウントとそれに関連付けられているレコードの会社が、BlueXPアカウントのシリアル番号(例960xxxx）または動作環境のシリアル番号。次のいずれかのオプションを使用して、サポートを受けることができます。

- 製品内のチャットを使用します
- テクニカル以外のケースをに送信します https://mysupport.netapp.com/site/help

サポートケースの管理（プレビュー）

アクティブなサポートケースと解決済みのサポートケースは、BlueXPから直接表示および管理できます。NSSアカウントと会社に関連付けられたケースを管理できます。

ケース管理はプレビューとして使用できます。今後のリリースでは、この点をさらに改良し、機能を強化する予定です。製品内のチャットでご意見をお寄せください。

次の点に注意してください。

- ページ上部のケース管理ダッシュボードには、次の2つのビューがあります。
  - 左側のビューには、指定したユーザNSSアカウントによって過去3カ月間にオープンされたケースの総数が表示されます。
  - 右側のビューには、ユーザのNSSアカウントに基づいて、過去3カ月間にオープンしたケースの総数が会社レベルで表示されます。

  テーブルの結果には、選択したビューに関連するケースが反映されます。
- 目的の列を追加または削除したり、[優先度]や[ステータス]などの列の内容をフィルタリングしたりできます。他の列には、並べ替え機能だけがあります。

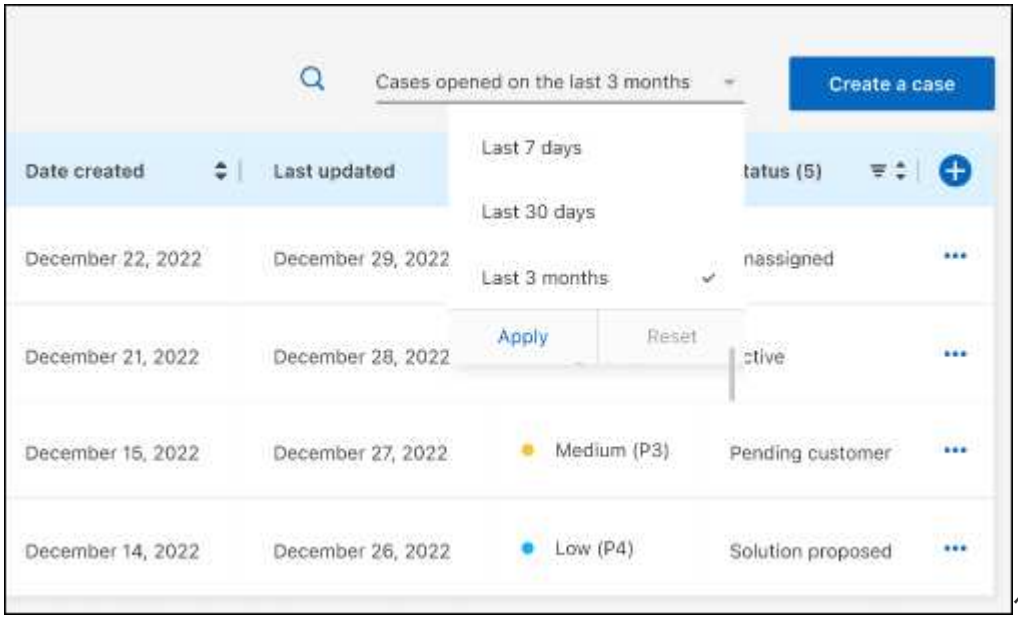
  詳細については、以下の手順を参照してください。
- ケースごとに、ケースノートを更新したり、ステータスが「Closed」または「Pending Closed」でないケースをクローズしたりすることができます。

手順

1. BlueXPで、*[ヘルプ]>[サポート]*を選択します。
2. [ケース管理]*を選択し、プロンプトが表示されたらNSSアカウントをBlueXPに追加します。

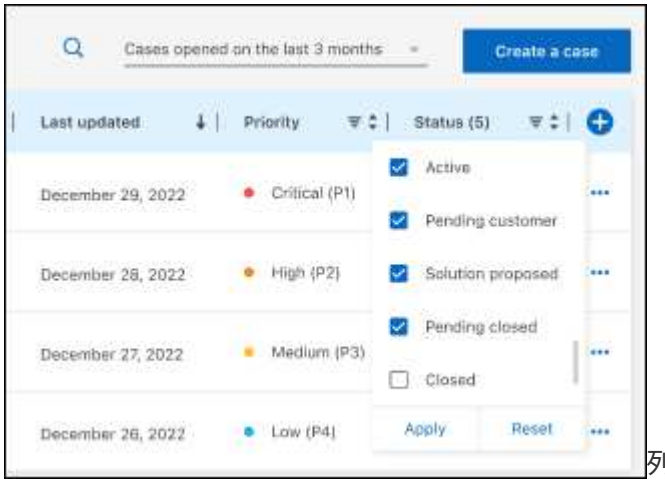
   ケース管理*ページには、BlueXPユーザアカウントに関連付けられたNSSアカウントに関連するオープンケースが表示されます。これは、* NSS管理*ページの上部に表示されるNSSアカウントと同じです。

3. 必要に応じて、テーブルに表示される情報を変更します。
    - [Organization’s Cases]*で[View]*を選択すると、会社に関連付けられているすべてのケースが表示されます。
    - 正確な日付範囲を選択するか、別の期間を選択して、日付範囲を変更します。



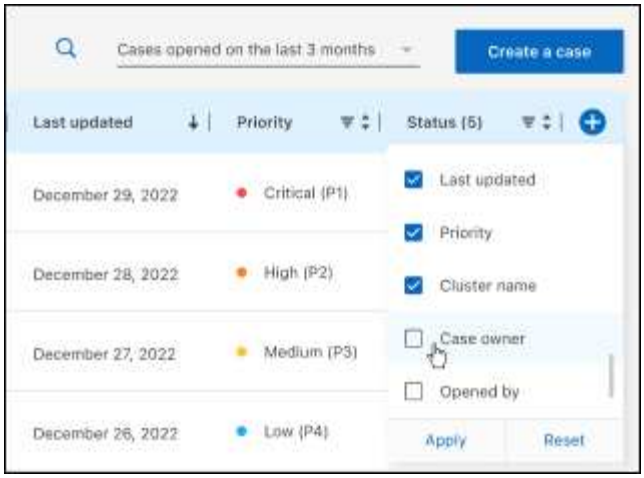
ページのテーブルの上にあるオプションのスクリーンショット。正確な日付範囲、または過去7日、30日、または3カ月を選択できます。"]

    - 列の内容をフィルタリングします。



列のフィルタオプションのスクリーンショット。[Active]や[Closed]など、特定のステータスに一致するケースを除外できます。"]

    - テーブルに表示される列を変更するには、 次に、表示する列を選択します。

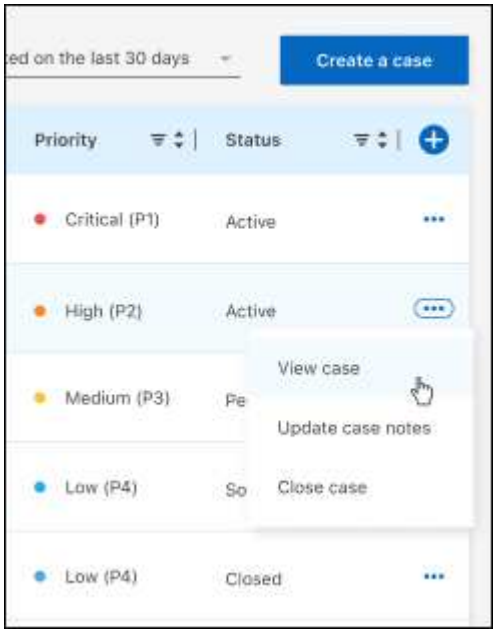


4. 既存のケースを管理するには、 ••• 使用可能なオプションのいずれかを選択します。

   - ケースの表示:特定のケースの詳細を表示します。
   - ケースノートの更新：問題の詳細を入力するか、*ファイルのアップロード*を選択して最大5つのファイルを添付します。

     添付ファイルはファイルあたり25 MBに制限されています。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、 doc/docx、xls/xlsx、およびcsv。

   - ケースをクローズ：ケースをクローズする理由の詳細を入力し、*ケースをクローズ*を選択します。



法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp 、 NetApp のロゴ、および NetApp の商標ページに記載されているマークは、 NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシーポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

- "BlueXPに関する注意事項"
- "BlueXPのバックアップとリカバリについて説明します"
- "Single File Restore に関する注意事項を参照してください"