はじめに
Cloud Volumes ONTAP

NetApp
May 28, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/bluexp-cloud-volumes-ontap/concept-overview-cvo.html on May 28, 2024. Always check docs.netapp.com for the latest.

目次

はじめに

Cloud Volumes ONTAP の詳細をご覧ください

Cloud Volumes ONTAP を使用すると、データ保護、セキュリティ、コンプライアンスを強化しながら、クラウドストレージのコストとパフォーマンスを最適化できます。

Cloud Volumes ONTAP は、クラウドで ONTAP データ管理ソフトウェアを実行するソフトウェア型のストレージアプライアンスです。以下の主要機能を備えたエンタープライズクラスのストレージを提供します。

- ストレージの効率化

  組み込みのデータ重複排除、データ圧縮、シンプロビジョニング、クローニングを活用して、ストレージコストを最小限に抑えます。

- 高可用性

  クラウド環境で障害が発生した場合でも、エンタープライズクラスの信頼性と継続的な運用を確保できます。

- データ保護

  Cloud Volumes ONTAP は、業界をリードするネットアップのレプリケーションテクノロジである SnapMirror を利用してオンプレミスのデータをクラウドにレプリケートするため、セカンダリコピーを複数のユースケースに簡単に利用できます。

  また、Cloud Volumes ONTAP はBlueXPのバックアップとリカバリと統合することで、クラウド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の機能を提供します。

  "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"

- データの階層化

  アプリケーションをオフラインにすることなく、ハイパフォーマンスとローパフォーマンスのストレージプールをオンデマンドで切り替えます。

- アプリケーションの整合性

  NetApp SnapCenter を使用して、 NetApp Snapshot コピーの整合性を確保します。

  "SnapCenter の詳細については、こちらをご覧ください"

- データセキュリティ

  Cloud Volumes ONTAP は、データ暗号化をサポートし、ウィルスやランサムウェアからの保護を提供します。

- プライバシーコンプライアンスの管理

  BlueXPの分類機能と統合することで、データのコンテキストを把握し、機密データを特定できます。

"BlueXPの分類の詳細については、こちらをご覧ください"

ONTAP 機能のライセンスは、 Cloud Volumes ONTAP に含まれています。

"サポートされている Cloud Volumes ONTAP 構成を表示します"

"Cloud Volumes ONTAP の詳細については、こちらを参照してください"

新規導入でサポートされるバージョン

BlueXPでは'新しいCloud Volumes ONTAP 作業環境を作成するときに'いくつかの異なるONTAP バージョンから選択できます

それ以外のCloud Volumes ONTAP バージョンは、新規導入ではサポートされません。

AWS

シングルノード

- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- P5 9.7
- 9.5 P6.

HA ペア

- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3

- 9.10.1
- 9.9.1 P6
- 9.8
- P5 9.7
- 9.5 P6.

Azure

シングルノード

- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6
- 9.5 P6.

HA ペア

- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6

Google Cloud

シングルノード

- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- P5 9.7

HA ペア

- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

Amazon Web Services の利用を開始しましょう

AWS での Cloud Volumes ONTAP のクイックスタート

いくつかの手順で、 AWS で Cloud Volumes ONTAP を使い始めましょう。

コネクタを作成します

を持っていなければ "コネクタ" ただし、アカウント管理者がアカウントを作成する必要があります。 "AWS でコネクタを作成する方法について説明します"

インターネットアクセスを使用できないサブネットにCloud Volumes ONTAP を導入する場合は、コネクタを手動でインストールし、そのコネクタで実行されているBlueXPユーザインターフェイスにアクセスする必要があります。 "インターネットにアクセスできない場所にコネクタを手動でインストールする方法について説

明します"

2 構成を計画

BlueXPでは、ワークロード要件に合わせて事前設定されたパッケージを提供しています。また、独自の構成を作成することもできます。独自の設定を選択する場合は、使用可能なオプションを理解しておく必要があります。 "詳細はこちら。"。

3 ネットワークをセットアップします

1. VPC とサブネットがコネクタと Cloud Volumes ONTAP 間の接続をサポートしていることを確認します。
2. ターゲットVPCからのアウトバウンドのインターネットアクセスをNetApp AutoSupport で有効にします。

   インターネットにアクセスできない場所にCloud Volumes ONTAP を導入する場合は、この手順は必要ありません。

3. S3 サービスへの vPC エンドポイントをセットアップします。

   Cloud Volumes ONTAP から低コストのオブジェクトストレージにコールドデータを階層化する場合は、VPC エンドポイントが必要です。

"ネットワーク要件の詳細については、こちらをご覧ください"。

4 **AWS KMS** を設定します

Cloud Volumes ONTAP で Amazon 暗号化を使用する場合は、アクティブなカスタマーマスターキー（ CMK ）が存在することを確認する必要があります。また、コネクタに「 a_key user__ 」という権限を付与する IAM ロールを追加して、各 CMK のキーポリシーを変更する必要があります。 "詳細はこちら。"。

5 **BlueXP**を使用して**Cloud Volumes ONTAP** を起動します

[作業環境の追加] をクリックし、展開するシステムのタイプを選択して、ウィザードの手順を実行します。 "詳細な手順を参照してください"。

関連リンク

- "BlueXPからAWSにコネクタを作成します"
- "AWS Marketplace からコネクタを作成します"
- "コネクタをオンプレミスにインストールしてセットアップします"
- "Connector の AWS 権限"

AWSでCloud Volumes ONTAP 構成を計画

AWS に Cloud Volumes ONTAP を導入する場合は、ワークロードの要件に応じて事前設定されたシステムを選択するか、または独自の設定を作成できます。独自の設定を選択する場合は、使用可能なオプションを理解しておく必要があります。

Cloud Volumes ONTAP ライセンスを選択します

Cloud Volumes ONTAP には、いくつかのライセンスオプションがあります。それぞれのオプションで、ニーズに合った消費モデルを選択できます。

- "Cloud Volumes ONTAP のライセンスオプションについて説明します"
- "ライセンスの設定方法について説明します"

サポートされているリージョンを選択します

Cloud Volumes ONTAP はほとんどの AWS リージョンでサポートされています。 "サポートされているリージョンの完全なリストを表示します"。

新しい AWS リージョンは、それらのリージョンでリソースを作成および管理する前に有効にする必要があります。 "リージョンを有効にする方法について説明します"。

サポートされるローカルゾーンの選択

Cloud Volumes ONTAPは、シンガポールを含む一部のAWSローカルゾーンでサポートされています。ローカルゾーンの選択はオプションです。

"ローカルゾーンの完全なリストを表示する"。
ローカルゾーンでリソースを作成および管理するには、ローカルゾーンを有効にする必要があります。

"ローカルゾーンを有効にする方法"。

Phoenixはサポートされているローカルゾーンではありません。

サポートされているインスタンスを選択します

Cloud Volumes ONTAP では、選択したライセンスタイプに応じて、複数のインスタンスタイプがサポートされます。

"AWS で Cloud Volumes ONTAP がサポートされる構成"

ストレージの制限を確認

Cloud Volumes ONTAP システムの未フォーマット時の容量制限は、ライセンスに関連付けられています。追加の制限は、アグリゲートとボリュームのサイズに影響します。設定を計画する際には、これらの制限に注意する必要があります。

"AWS での Cloud Volumes ONTAP のストレージの制限"

AWSでシステムのサイズを設定します

Cloud Volumes ONTAP システムのサイジングを行うことで、パフォーマンスと容量の要件を満たすのに役立ちます。インスタンスタイプ、ディスクタイプ、およびディスクサイズを選択する際には、次の点に注意する必要があります。

インスタンスタイプ

- ワークロードの要件を、各 EC2 インスタンスタイプの最大スループットと IOPS に合わせます。

- 複数のユーザが同時にシステムに書き込む場合は、要求を管理するのに十分な CPU を備えたインスタンスタイプを選択します。
- 読み取りが多いアプリケーションがある場合は、十分な RAM が搭載されたシステムを選択します。
  - "AWS ドキュメント：「 Amazon EC2 Instance Types"
  - "AWS のドキュメント：「 Amazon EBS – Optimized instances"

EBS ディスクタイプ

EBS ディスクタイプの違いは次のとおりです。EBS ディスクのユースケースの詳細については、を参照してください "AWS ドキュメント：「 EBS Volume Types"。

- _General Purpose SSD （ GP3 ） _ ディスクは、幅広いワークロードに対してコストとパフォーマンスのバランスを取る最も低コストの SSD です。パフォーマンスは、 IOPS とスループットを基準に定義されます。GP3 ディスクは Cloud Volumes ONTAP 9.7 以降でサポートされています。

  GP3ディスクを選択すると、選択したディスクサイズに基づいて、gp2ディスクに相当するパフォーマンスを提供するデフォルトのIOPSとスループットの値がBlueXPによって設定されます。この値を増やすと、コストを高くしてもパフォーマンスを向上させることができますが、パフォーマンスが低下する可能性があるため、値を小さくすることはできません。つまり、デフォルト値をそのまま使用するか、値を大きくします。低くしないでください。 "GP3 ディスクとそのパフォーマンスについては、こちらをご覧ください"。

  Cloud Volumes ONTAP は、GP3ディスクを使用したAmazon EBS Elastic Volumes機能をサポートしています。 "Elastic Volumesのサポートに関する詳細情報"。

- _ 汎用 SSD （ gp2 ） _ ディスクは、幅広いワークロードに対してコストとパフォーマンスのバランスを取ります。パフォーマンスは IOPS の観点から定義されます。
- _Provisioned IOPS SSD （ io1 ） _disks は、コストが高くても最高のパフォーマンスが求められる重要なアプリケーション用です。

  Cloud Volumes ONTAP では、io1ディスクを使用したAmazon EBS Elastic Volumes機能がサポートされています。 "Elastic Volumesのサポートに関する詳細情報"。

- _Throughput Optimized HDD （ st1 ） _disks は、高速で安定したスループットを必要とする、アクセス頻度の高いワークロード用です。価格は低くなります。

  スループット最適化 HDD （ st1 ）を使用している場合、オブジェクトストレージへのデータの階層化は推奨されません。

EBS ディスクサイズ

をサポートしない構成を選択した場合 "Amazon EBS Elastic Volumes機能"を選択した場合、Cloud Volumes ONTAP システムの起動時に初期ディスクサイズを選択する必要があります。その後、次の操作を実行できます "システムの容量をBlueXPが管理できるようにします"必要に応じて "アグリゲートの作成は自分で行います"、次の点に注意してください。

- アグリゲート内のディスクはすべて同じサイズである必要があります。
- EBS ディスクのパフォーマンスはディスクサイズに依存します。サイズによって、 SSD ディスクのベースライン IOPS と最大バースト期間、および HDD ディスクのベースラインスループットとバーストスループットが決まります。

- 最終的には、必要なパフォーマンスを継続的に提供するディスクサイズを選択する必要があります。
- 4 TiB のディスクを 6 台使用するなど、大容量のディスクを選択した場合でも、 EC2 インスタンスの帯域幅が制限に達する可能性があるため、すべての IOPS が得られないことがあります。

  EBS ディスクのパフォーマンスの詳細については、を参照してください "AWS ドキュメント：「 EBS Volume Types"。

  前述したように、ディスクサイズの選択は、Amazon EBS Elastic Volumes機能をサポートするCloud Volumes ONTAP 構成ではサポートされていません。 "Elastic Volumesのサポートに関する詳細情報"。

デフォルトのシステムディスクを表示します

ユーザデータ用のストレージに加えて、BlueXPはCloud Volumes ONTAP システムデータ（ブートデータ、ルートデータ、コアデータ、NVRAM）用のクラウドストレージも購入します。計画を立てる場合は、 Cloud Volumes ONTAP を導入する前にこれらの詳細を確認すると役立つ場合があります。

"AWS で Cloud Volumes ONTAP システムデータのデフォルトディスクを表示する"。

コネクタにはシステムディスクも必要です。 "コネクタのデフォルト設定に関する詳細を表示します"。

AWSアウトポストに**Cloud Volumes ONTAP** を導入する準備をします

AWS Outpost を使用している場合は、 Working Environment ウィザードで Outpost VPC を選択して、その Outpost に Cloud Volumes ONTAP を導入できます。エクスペリエンスは、 AWS に存在する他の VPC と同じです。最初に、 AWS Outpost にコネクタを導入する必要があります。

指摘すべき制限事項はいくつかあります。

- でサポートされるのはシングルノードの Cloud Volumes ONTAP システムのみです 今回は
- Cloud Volumes で使用できる EC2 インスタンス ONTAP は、 Outpost で利用できる機能に限定されています
- 現時点では、汎用 SSD （ gp2 ）のみがサポートされます

ネットワーク情報を収集

AWS で Cloud Volumes ONTAP を起動する場合は、 VPC ネットワークの詳細を指定する必要があります。ワークシートを使用して、管理者から情報を収集できます。

単一の**AZ**における単一のノードまたは**HA**ペア

AWS 情報	あなたの価値
地域	
vPC	
サブネット	
セキュリティグループ（独自のグループを使用している場合）	

複数のAZにまたがるHAペアを作成します

AWS 情報	あなたの価値
地域	
vPC	
セキュリティグループ（独自のグループを使用している場合）	
ノード 1 の可用性ゾーン	
ノード 1 のサブネット	
ノード 2 の可用性ゾーン	
ノード 2 のサブネット	
メディエータ可用性ゾーン	
メディエータサブネット	
メディエータのキーペア	
クラスタ管理ポートのフローティング IP アドレス	
ノード 1 のデータの浮動 IP アドレス	
ノード 2 のデータの浮動 IP アドレス	
フローティング IP アドレスのルートテーブル	

書き込み速度を選択します

BlueXPでは、Cloud Volumes ONTAP の書き込み速度設定を選択できます。書き込み速度を選択する前に、高速書き込みを使用する場合の標準設定と高設定の違い、およびリスクと推奨事項を理解しておく必要があります。 "書き込み速度の詳細については、こちらをご覧ください。"。

ボリュームの使用プロファイルを選択してください

ONTAP には、必要なストレージの合計容量を削減できるストレージ効率化機能がいくつか搭載されています。BlueXPでボリュームを作成するときに、これらの機能を有効にするプロファイル、または無効にするプロファイルを選択できます。これらの機能の詳細については、使用するプロファイルを決定する際に役立ちます。

NetApp Storage Efficiency 機能には、次のようなメリットがあります。

シンプロビジョニング

物理ストレージプールよりも多くの論理ストレージをホストまたはユーザに提供します。ストレージスペースは、事前にストレージスペースを割り当てる代わりに、データの書き込み時に各ボリュームに動的に割り当てられます。

重複排除

同一のデータブロックを検索し、単一の共有ブロックへの参照に置き換えることで、効率を向上します。この手法では、同じボリュームに存在するデータの冗長ブロックを排除することで、ストレージ容量の要件を軽減します。

圧縮

プライマリ、セカンダリ、アーカイブストレージ上のボリューム内のデータを圧縮することで、データの格納に必要な物理容量を削減します。

ネットワークをセットアップします

Cloud Volumes ONTAP in AWS のネットワーク要件

BlueXPは、IPアドレス、ネットマスク、ルートなど、Cloud Volumes ONTAP のネットワークコンポーネントのセットアップを処理します。アウトバウンドのインターネットアクセスが可能であること、十分な数のプライベート IP アドレスを利用できること、適切な接続が確立されていることなどを確認する必要があります。

一般的な要件

AWS では、次の要件を満たす必要があります。

Cloud Volumes ONTAP ノードのアウトバウンドインターネットアクセス

Cloud Volumes ONTAP ノードには、NetApp AutoSupport へのアウトバウンドインターネットアクセスが必要です。ネットアップは、システムの健常性をプロアクティブに監視し、ネットアップテクニカルサポートにメッセージを送信します。

Cloud Volumes ONTAP が AutoSupport メッセージを送信できるように、ルーティングポリシーとファイアウォールポリシーで次のエンドポイントへの HTTP / HTTPS トラフィックを許可する必要があります。

- \ https://support.netapp.com/aods/asupmessage
- \ https://support.netapp.com/asupprod/post/1.0/postAsup

NAT インスタンスがある場合は、プライベートサブネットからインターネットへの HTTPS トラフィックを許可する着信セキュリティグループルールを定義する必要があります。

AutoSupport メッセージの送信にアウトバウンドのインターネット接続が使用できない場合、Cloud Volumes ONTAP システムは自動的にコネクタをプロキシサーバとして使用するように設定されます。唯一の要件は、コネクタのセキュリティグループがポート3128で_ inbound_connectionsを許可することです。コネクタを展開した後、このポートを開く必要があります。

Cloud Volumes ONTAP に厳密なアウトバウンドルールを定義した場合は、Cloud Volumes ONTAP セキュリティグループがポート3128で_OUTBOUND接続を許可する必要もあります。

アウトバウンドのインターネットアクセスが使用可能であることを確認したら、 AutoSupport をテストしてメッセージを送信できることを確認します。手順については、を参照してください "ONTAP のドキュメント：「 AutoSupport のセットアップ"。

AutoSupport メッセージを送信できないことがBlueXPから通知された場合は、 "AutoSupport 構成のトラブルシューティングを行います"。

HA メディエータのアウトバウンドインターネットアクセス

HA メディエータインスタンスは、 AWS EC2 サービスへのアウトバウンド接続を持っている必要があります。これにより、ストレージのフェイルオーバーを支援できます。接続を提供するには、パブリック IP アドレスを追加するか、プロキシサーバを指定するか、または手動オプションを使用します。

手動オプションには、 NAT ゲートウェイまたはターゲットサブネットから AWS EC2 サービスへのインターフェイス VPC エンドポイントを指定できます。VPC エンドポイントの詳細については、を参照してください "AWS ドキュメント：「 Interface VPC Endpoints 」（ AWS PrivateLink ）"。

プライベート IP アドレス

BlueXPは、必要な数のプライベートIPアドレスを自動的にCloud Volumes ONTAP に割り当てます。ネットワークに十分な数のプライベート IP アドレスがあることを確認する必要があります。

Cloud Volumes ONTAP 用に割り当てられるLIFの数は、シングルノードシステムとHAペアのどちらを導入するかによって異なります。LIF は、物理ポートに関連付けられた IP アドレスです。

シングルノードシステムの IP アドレス

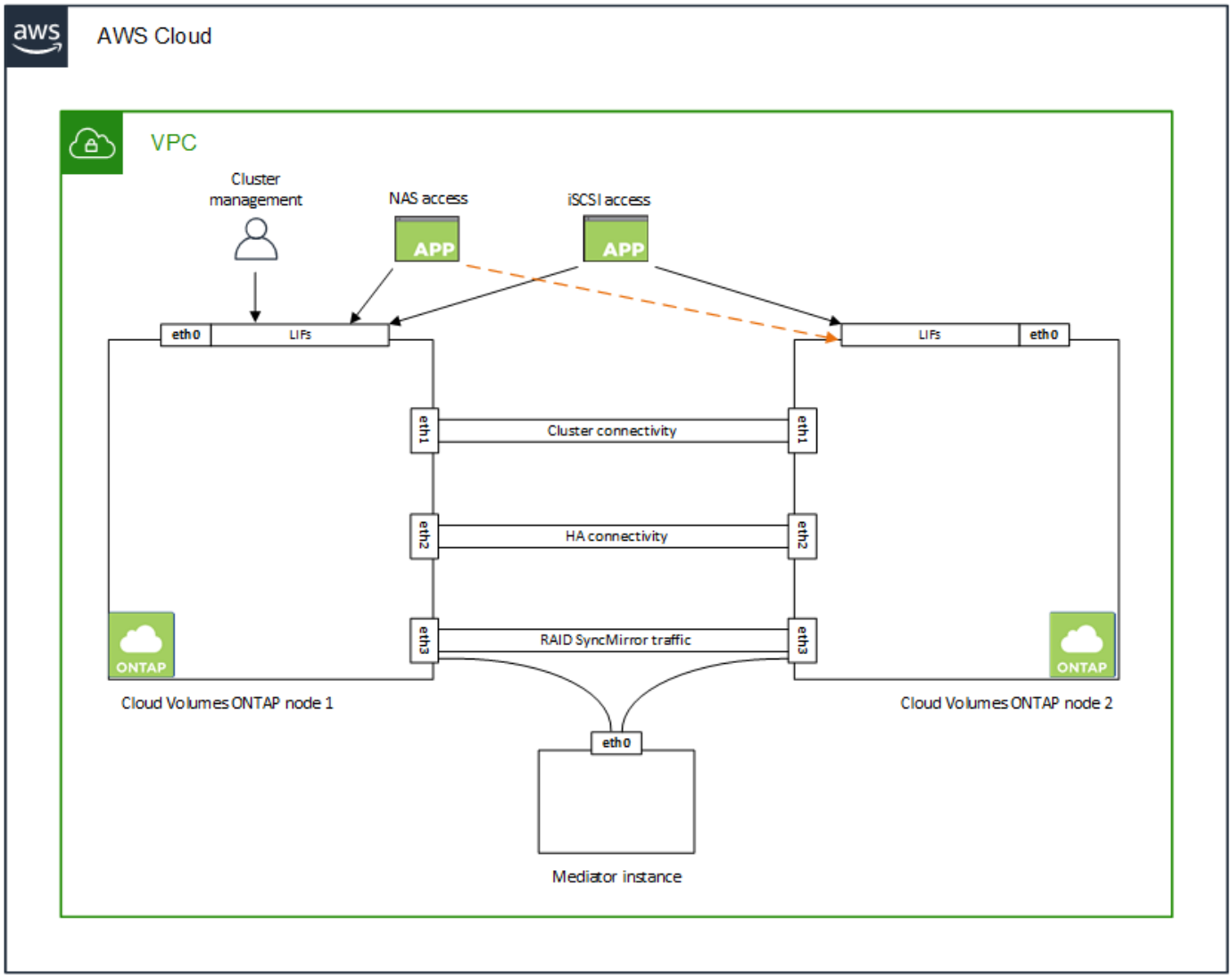
BlueXPでは、1つのノードシステムに6つのIPアドレスが割り当てられます。

次の表に、各プライベートIPアドレスに関連付けられているLIFの詳細を示します。

LIF	目的
クラスタ管理	クラスタ全体（ HA ペア）の管理。
ノード管理	ノードの管理。
クラスタ間	クラスタ間の通信、バックアップ、レプリケーション。
NAS データ	NAS プロトコルを使用したクライアントアクセス。
iSCSI データ	iSCSI プロトコルを使用したクライアントアクセス。システムでは、その他の重要なネットワークワークフローにも使用されます。このLIFは必須であり、削除することはできません。
Storage VM管理	Storage VM 管理 LIF は、 SnapCenter などの管理ツールで使用されます。

HA ペアの IP アドレス

HA ペアには、シングルノードシステムよりも多くの IP アドレスが必要です。次の図に示すように、これらの IP アドレスは異なるイーサネットインターフェイスに分散されています。



HA ペアに必要なプライベート IP アドレスの数は、選択する導入モデルによって異なります。A_SILE_AWS アベイラビリティゾーン（ AZ ）に導入する HA ペアには 15 個のプライベート IP アドレスが必要です。一方、 _multiple_AZs に導入する HA ペアには、 13 個のプライベート IP アドレスが必要です。

次の表に、各プライベート IP アドレスに関連付けられている LIF の詳細を示します。

単一の **AZ** にある **HA** ペアの **LIF**

LIF	インターフェイス	ノード	目的
クラスタ管理	eth0	ノード 1	クラスタ全体（ HA ペア）の管理。
ノード管理	eth0	ノード 1 とノード 2	ノードの管理。
クラスタ間	eth0	ノード 1 とノード 2	クラスタ間の通信、バックアップ、レプリケーション。
NAS データ	eth0	ノード 1	NAS プロトコルを使用したクライアントアクセス。

LIF	インターフェイス	ノード	目的
iSCSI データ	eth0	ノード 1 とノード 2	iSCSI プロトコルを使用したクライアントアクセス。システムでは、その他の重要なネットワークワークフローにも使用されます。これらのLIFは必須であり、削除しないでください。
クラスタ接続	Eth1	ノード 1 とノード 2	ノード間の通信およびクラスタ内でのデータの移動を可能にします。
HA 接続	eth2	ノード 1 とノード 2	フェイルオーバー時の 2 つのノード間の通信。
RSM iSCSI トラフィック	eth3	ノード 1 とノード 2	RAID SyncMirror iSCSI トラフィック、および 2 つの Cloud Volumes ONTAP ノードとメディエーター間の通信。
メディエーター	eth0	メディエーター	ストレージのテイクオーバーとギブバックのプロセスを支援するための、ノードとメディエーターの間の通信チャネル。

複数の **AZ** にまたがる **HA** ペア用の **LIF** です

LIF	インターフェイス	ノード	目的
ノード管理	eth0	ノード 1 とノード 2	ノードの管理。
クラスタ間	eth0	ノード 1 とノード 2	クラスタ間の通信、バックアップ、レプリケーション。
iSCSI データ	eth0	ノード 1 とノード 2	iSCSI プロトコルを使用したクライアントアクセス。また、ノード間でのフローティングIPアドレスの移行も管理します。これらのLIFは必須であり、削除しないでください。
クラスタ接続	Eth1	ノード 1 とノード 2	ノード間の通信およびクラスタ内でのデータの移動を可能にします。
HA 接続	eth2	ノード 1 とノード 2	フェイルオーバー時の 2 つのノード間の通信。
RSM iSCSI トラフィック	eth3	ノード 1 とノード 2	RAID SyncMirror iSCSI トラフィック、および 2 つの Cloud Volumes ONTAP ノードとメディエーター間の通信。
メディエーター	eth0	メディエーター	ストレージのテイクオーバーとギブバックのプロセスを支援するための、ノードとメディエーターの間の通信チャネル。

複数のアベイラビリティゾーンに導入すると、いくつかの LIF が関連付けられます "フローティング IP アドレス"AWS のプライベート IP 制限にはカウントされません。

セキュリティグループ

セキュリティグループを作成する必要はありません。BlueXPではセキュリティグループが自動的に作成され

ます。自分で使用する必要がある場合は、を参照してください "セキュリティグループのルール"。

コネクタに関する情報をお探しですか？ "コネクタのセキュリティグループルールを表示します"

データ階層化のための接続

EBS をパフォーマンス階層として使用し、 AWS S3 を容量階層として使用する場合は、 Cloud Volumes ONTAP が S3 に接続されていることを確認する必要があります。この接続を提供する最善の方法は、 S3 サービスへの vPC エンドポイントを作成することです。手順については、を参照してください "AWS のドキュメント：「 Creating a Gateway Endpoint"。

vPC エンドポイントを作成するときは、 Cloud Volumes ONTAP インスタンスに対応するリージョン、 vPC 、およびルートテーブルを必ず選択してください。S3 エンドポイントへのトラフィックを有効にする発信 HTTPS ルールを追加するには、セキュリティグループも変更する必要があります。そうしないと、 Cloud Volumes ONTAP は S3 サービスに接続できません。

問題が発生した場合は、を参照してください "AWS のサポートナレッジセンター：ゲートウェイ VPC エンドポイントを使用して S3 バケットに接続できないのはなぜですか。"

ONTAP システムへの接続

AWSのCloud Volumes ONTAP システムと他のネットワークのONTAP システムの間でデータをレプリケートするには、AWS VPCと他のネットワーク（社内ネットワークなど）の間にVPN接続が必要です。手順については、を参照してください "AWS ドキュメント：「 Setting Up an AWS VPN Connection"。

CIFS 用の **DNS** と **Active Directory**

CIFS ストレージをプロビジョニングする場合は、 AWS で DNS と Active Directory をセットアップするか、オンプレミスセットアップを AWS に拡張する必要があります。

DNS サーバは、 Active Directory 環境に名前解決サービスを提供する必要があります。デフォルトの EC2 DNS サーバを使用するように DHCP オプションセットを設定できます。このサーバは、 Active Directory 環境で使用される DNS サーバであってはなりません。

手順については、を参照してください "AWS ドキュメント：「 Active Directory Domain Services on the AWS Cloud ： Quick Start Reference Deployment"。

vPC共有

9.11.1リリース以降では、VPCを共有するAWSでCloud Volumes ONTAP HAペアがサポートされます。VPC共有を使用すると、他のAWSアカウントとサブネットを共有できます。この構成を使用するには、AWS環境をセットアップし、APIを使用してHAペアを導入する必要があります。

"共有サブネットにHAペアを導入する方法について説明します"。

複数の **AZ** にまたがる **HA** ペアに関する要件

複数の可用性ゾーン（ AZS ）を使用する Cloud Volumes ONTAP HA 構成には、 AWS ネットワークの追加要件が適用されます。HAペアを起動する前に、作業環境の作成時にBlueXPでネットワークの詳細を入力する必要があるため、これらの要件を確認してください。

HA ペアの仕組みについては、を参照してください "ハイアベイラビリティペア"。

可用性ゾーン

この HA 導入モデルでは、複数の AZS を使用してデータの高可用性を確保します。各 Cloud Volumes ONTAP インスタンスと、 HA ペア間の通信チャネルを提供するメディエータインスタンスには、専用の AZ を使用する必要があります。

サブネットが各アベイラビリティゾーンに存在する必要があります。

NAS データおよびクラスタ **/ SVM** 管理用のフローティング **IP** アドレス

複数の AZ に展開された HA configurations では、障害が発生した場合にノード間で移行するフローティング IP アドレスを使用します。VPC の外部からネイティブにアクセスすることはできません。ただし、その場合は除きます "AWS 転送ゲートウェイを設定します"。

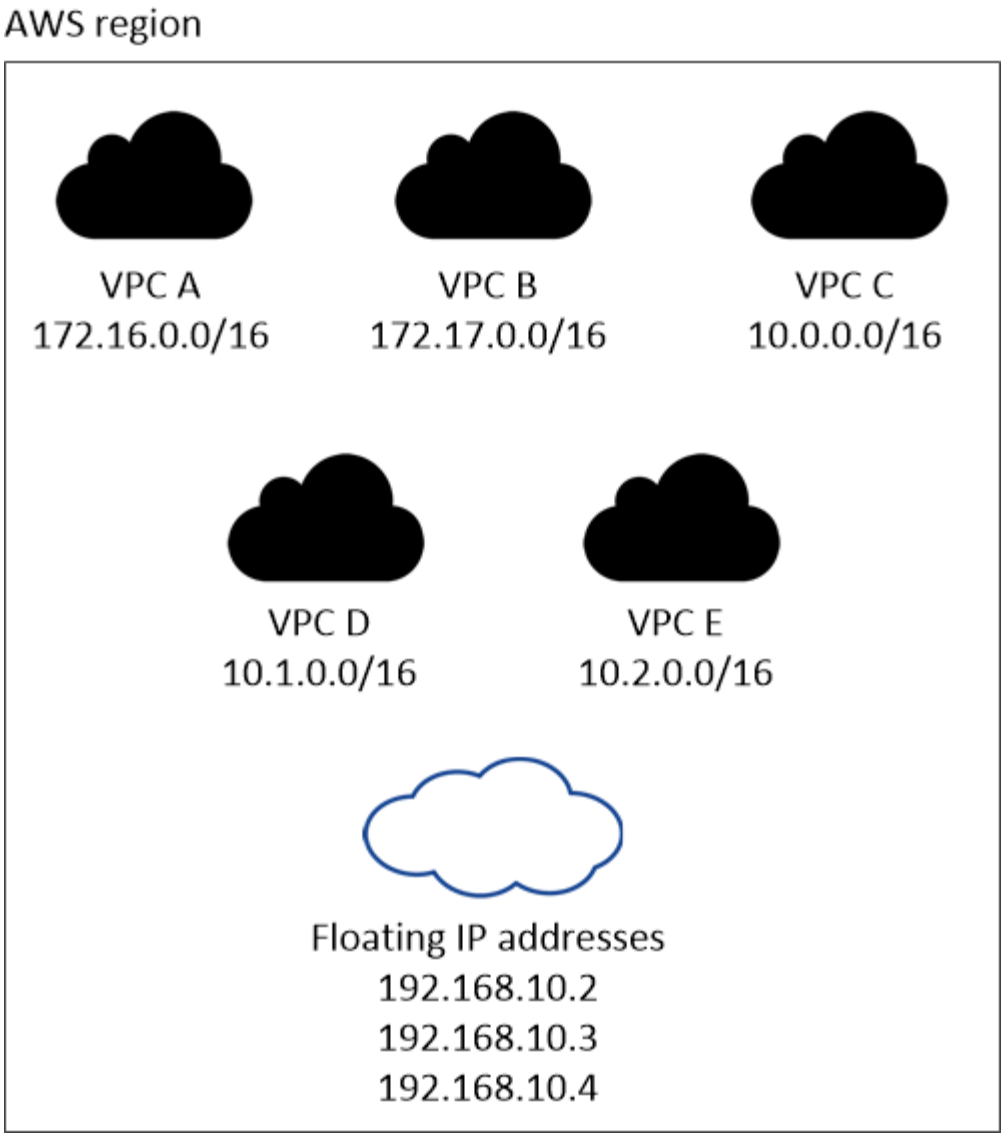
フローティング IP アドレスの 1 つはクラスタ管理用、 1 つはノード 1 の NFS/CIFS データ用、もう 1 つはノード 2 の NFS/CIFS データ用です。SVM 管理用の 4 つ目のフローティング IP アドレスはオプションです。

SnapCenter for Windows または SnapDrive を HA ペアで使用する場合は、 SVM 管理 LIF 用にフローティング IP アドレスが必要です。

Cloud Volumes ONTAP HA作業環境を作成する場合は、BlueXPでフローティングIPアドレスを入力する必要があります。システムの起動時に、HAペアにIPアドレスが割り当てられます。

フローティング IP アドレスは、 HA 構成を導入する AWS リージョン内のどの VPC の CIDR ブロックにも属していない必要があります。フローティング IP アドレスは、リージョン内の VPC の外部にある論理サブネットと考えてください。

次の例は、 AWS リージョンのフローティング IP アドレスと VPC の関係を示しています。フローティング IP アドレスはどの VPC の CIDR ブロックにも属しておらず、ルーティングテーブルを介してサブネットにルーティングできます。



BlueXPでは、VPCの外部にあるクライアントからのiSCSIアクセスとNASアクセスに対して、自動的に静的IPアドレスが作成されます。これらの種類の IP アドレスの要件を満たす必要はありません。

外部からのフローティング **IP** アクセスを可能にする中継ゲートウェイ **VPC**

必要に応じて、 "AWS 転送ゲートウェイを設定します" HA ペアが配置されている VPC の外部から HA ペアのフローティング IP アドレスにアクセスできるようにします。

ルートテーブル

BlueXPでフローティングIPアドレスを指定すると、フローティングIPアドレスへのルートを含むルートテーブルを選択するように求められます。これにより、 HA ペアへのクライアントアクセスが可能になります。

VPC内のサブネット用のルーティングテーブルが1つ（メインルーティングテーブル）だけの場合は、そのルーティングテーブルにフローティングIPアドレスが自動的に追加されます。ルーティングテーブルが複数ある場合は、 HA ペアの起動時に正しいルーティングテーブルを選択することが非常に重要です。そうしないと、一部のクライアントが Cloud Volumes ONTAP にアクセスできない場合があります。

たとえば、異なるルートテーブルに関連付けられた 2 つのサブネットがあるとします。ルーティングテー

ブル A を選択し、ルーティングテーブル B は選択しなかった場合、ルーティングテーブル A に関連付けられたサブネット内のクライアントは HA ペアにアクセスできますが、ルーティングテーブル B に関連付けられたサブネット内のクライアントはアクセスできません。

ルーティングテーブルの詳細については、を参照してください "AWS のドキュメント：「 Route Tables"。

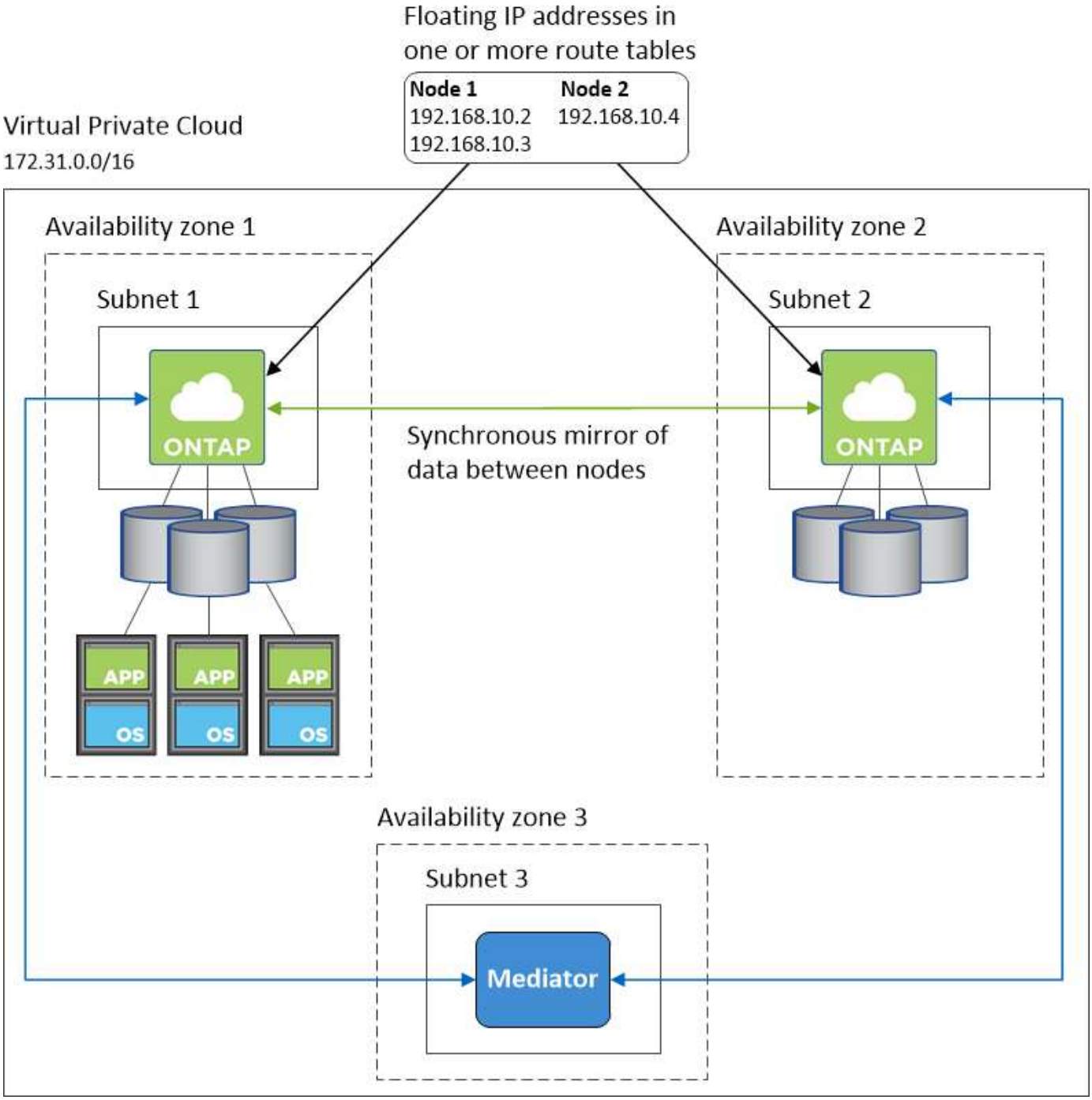
ネットアップの管理ツールとの連携

複数の AZ に展開された HA 構成でネットアップ管理ツールを使用するには、次の 2 つの接続オプションがあります。

1. ネットアップの管理ツールは、別の VPC とに導入できます "AWS 転送ゲートウェイを設定します"。ゲートウェイを使用すると、 VPC の外部からクラスタ管理インターフェイスのフローティング IP アドレスにアクセスできます。
2. NAS クライアントと同様のルーティング設定を使用して、同じ VPC にネットアップ管理ツールを導入できます。

HA 構成の例

次の図は、複数の AZ にまたがる HA ペアに固有のネットワークコンポーネントを示しています。 3 つのアベイラビリティゾーン、 3 つのサブネット、フローティング IP アドレス、およびルートテーブルです。



コネクタの要件

コネクタをまだ作成していない場合は、コネクタのネットワーク要件も確認してください。

- "コネクタのネットワーク要件を確認します"
- "AWSのセキュリティグループのルール"

での **HA** ペアの **AWS** 転送ゲートウェイのセットアップ 複数の **AZ**

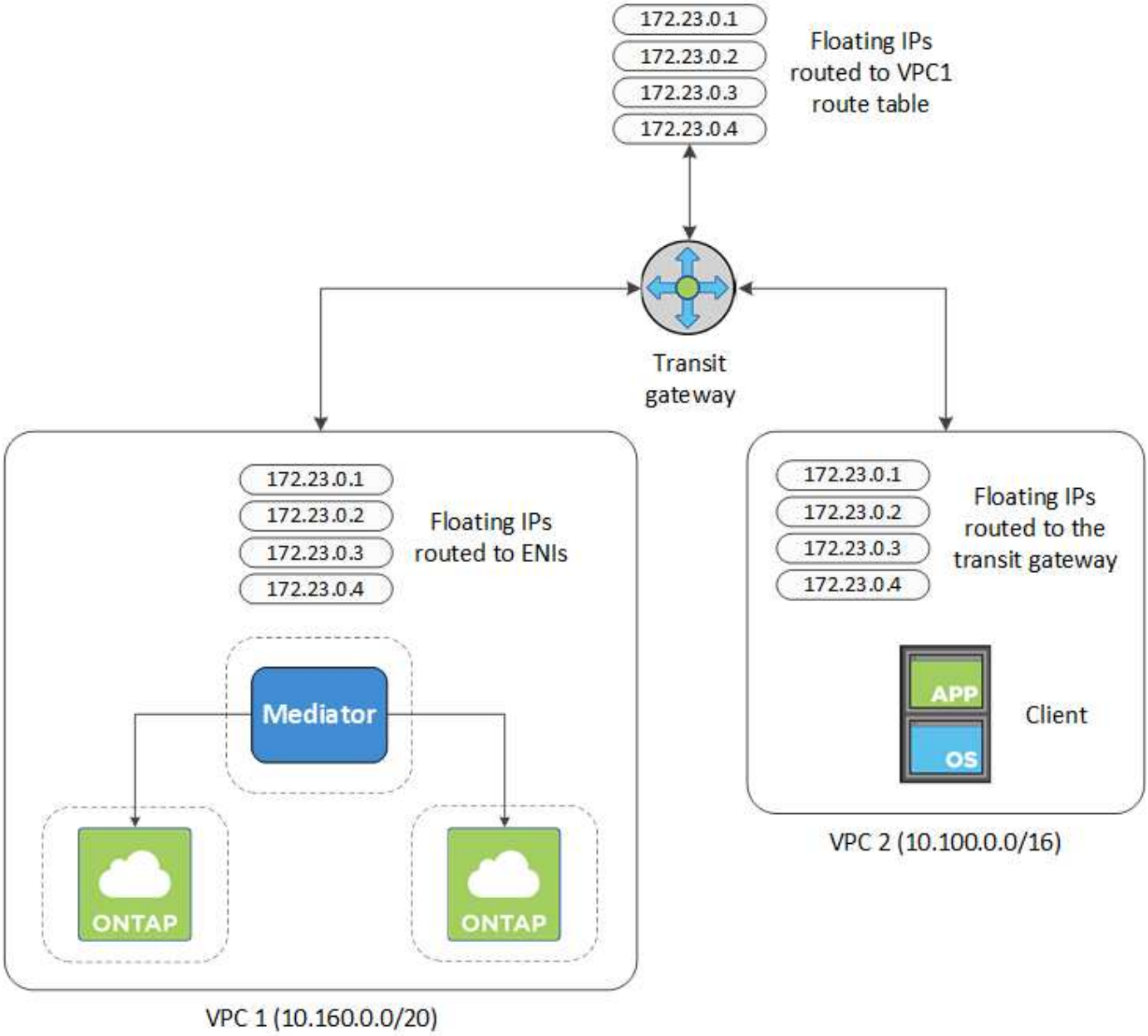
へのアクセスを有効にするために、 AWS 転送ゲートウェイを設定します HA ペアの 1 つ "フローティング IP アドレス" HA ペアが存在する VPC の外部から

Cloud Volumes ONTAP HA 構成が複数の AWS アベイラビリティゾーンに分散されている場合は、 VPC 内からの NAS データアクセス用にフローティング IP アドレスが必要です。これらのフローティング IP アドレスは、障害の発生時にノード間で移行できますが、 VPC の外部からネイティブにアクセスすることはできません。VPC の外部からのデータアクセスはプライベート IP アドレスで提供されますが、自動フェイルオーバーは提供されません。

クラスタ管理インターフェイスとオプションの SVM 管理 LIF にもフローティング IP アドレスが必要です。

AWS 転送ゲートウェイを設定すると、 HA ペアが配置された VPC の外部からフローティング IP アドレスにアクセスできるようになります。つまり、 VPC の外部にある NAS クライアントとネットアップの管理ツールからフローティング IP にアクセスできます。

以下に、トランジットゲートウェイによって接続された 2 つの VPC の例を示します。HA システムは 1 つの VPC に存在し、クライアントはもう一方の VPC に存在します。その後、フローティング IP アドレスを使用して NAS ボリュームをクライアントにマウントできます。

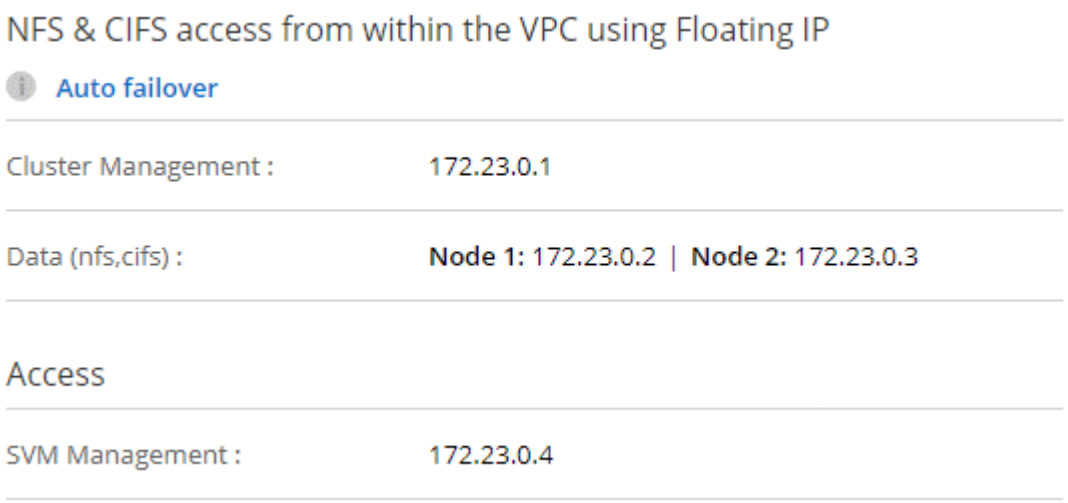


以下に、同様の構成を設定する手順を示します。

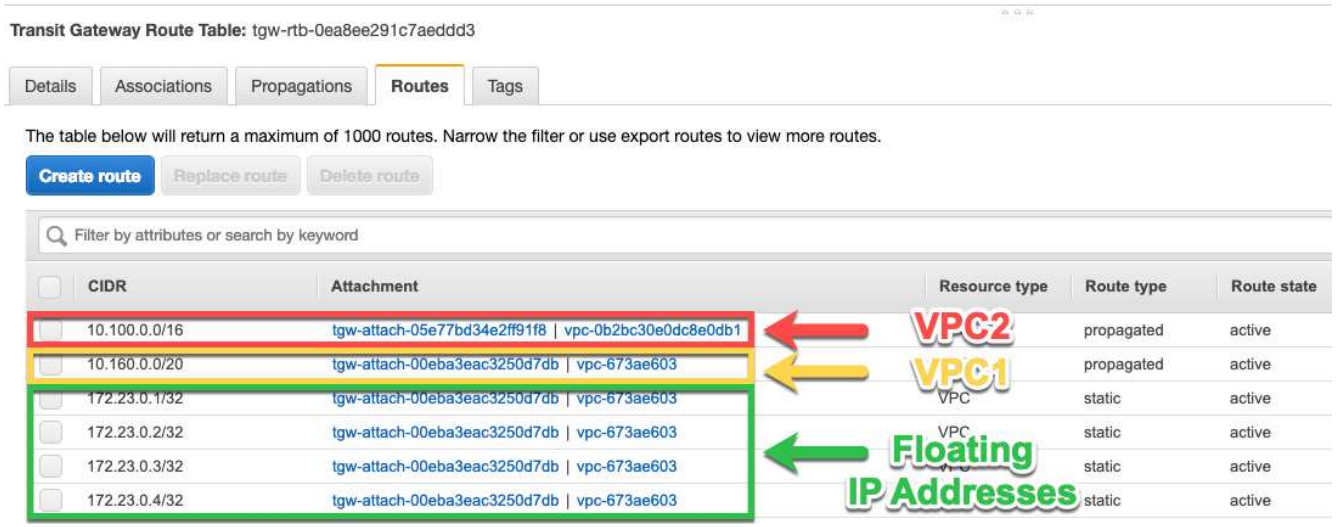
手順

1. "トランジットゲートウェイを作成し、 VPC をに接続します ゲートウェイ"。
2. VPC とトランジットゲートウェイルートテーブルを関連付ける。
   a. *VPC サービスで、 *Transit Gateway Route Tables * をクリックします。
   b. ルートテーブルを選択します。
   c. [*Associations] をクリックし、 [Create associations] を選択します。
   d. 関連付ける添付ファイル（ VPC ）を選択し、 * 関連付けの作成 * をクリックします。
3. HA ペアのフローティング IP アドレスを指定して、転送ゲートウェイのルートテーブルにルートを作成します。

   フローティングIPアドレスは、BlueXPの[作業環境情報]ページにあります。次に例を示します。



   次の図は、中継ゲートウェイのルートテーブルを示しています。このルートには、 2 つの VPC の CIDR ブロックへのルートと、 Cloud Volumes ONTAP で使用される 4 つのフローティング IP アドレスが含まれます。

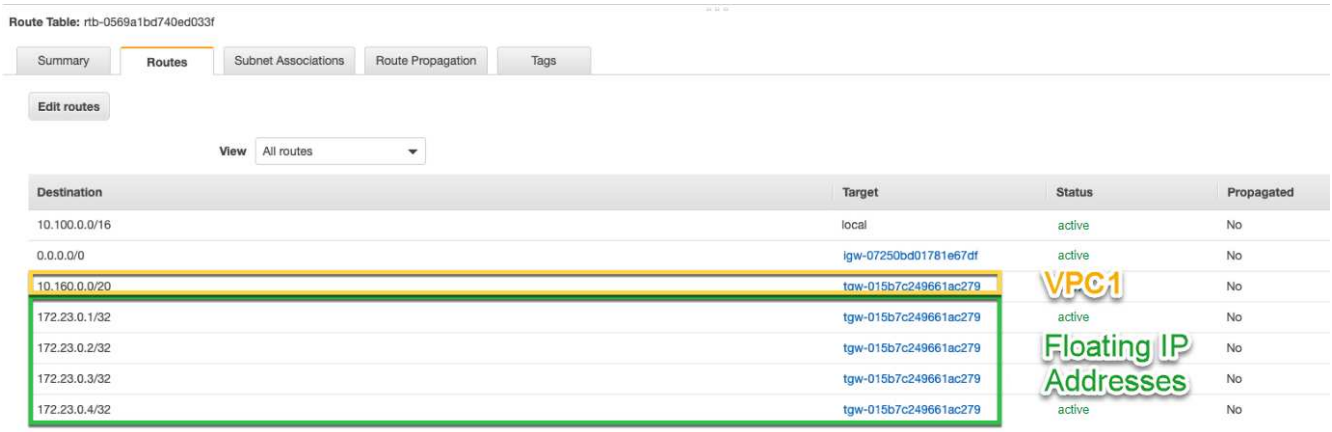


4. フローティング IP アドレスにアクセスする必要がある VPC のルーティングテーブルを変更します。

   a. フローティング IP アドレスにルートエントリを追加します。

   b. HA ペアが存在する VPC の CIDR ブロックにルートエントリを追加します。

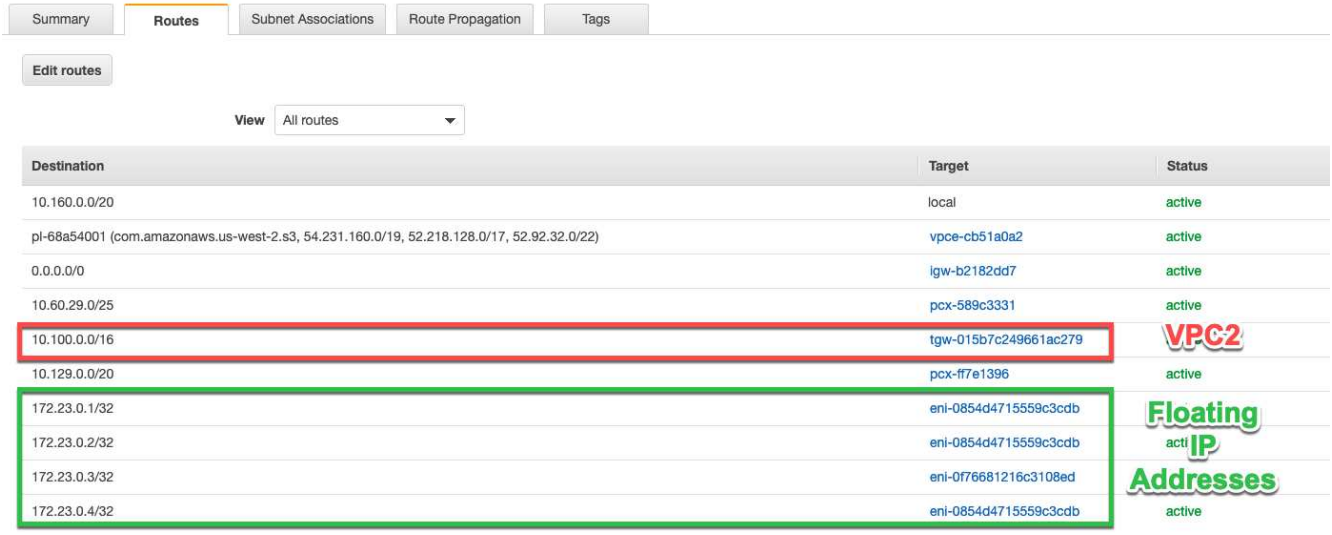
      次の図は、 VPC 1 へのルートとフローティング IP アドレスを含む VPC 2 のルートテーブルを示しています。



5. フローティング IP アドレスへのアクセスが必要な VPC へのルートを追加して、 HA ペアの VPC のルーティングテーブルを変更します。

   VPC 間のルーティングが完了するため、この手順は重要です。

   次の例は、 VPC 1 のルートテーブルを示しています。フローティング IP アドレスへのルートと、クライアントが配置されている VPC 2 へのルートが含まれます。BlueXPでは、HAペアを展開すると、フローティングIPがルートテーブルに自動的に追加されました。



6. VPCのすべてのトラフィックに対するセキュリティグループ設定を更新します。

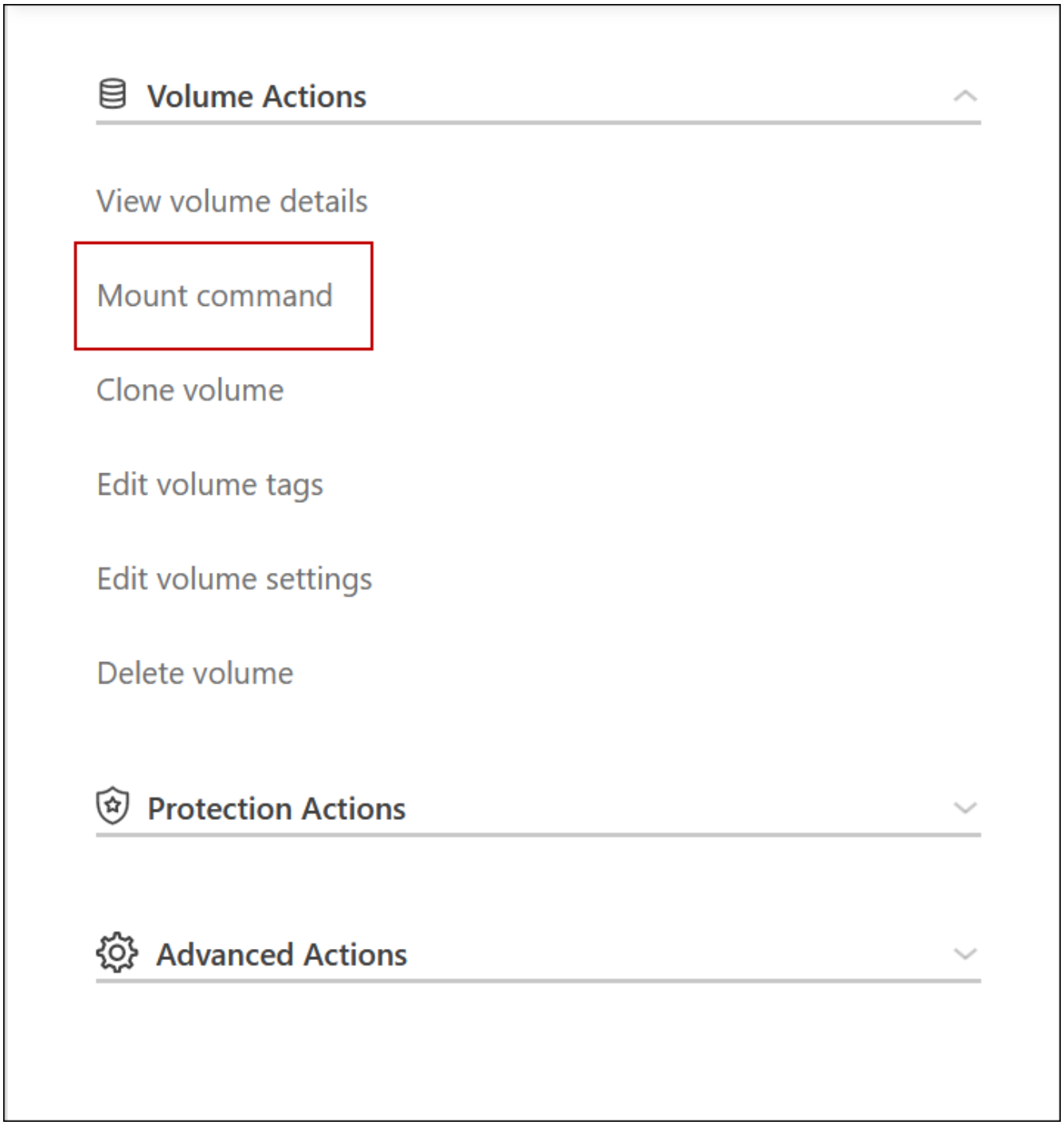
   a. [Virtual Private Cloud]で、*[サブネット]*をクリックします。

   b. [Route table]*タブをクリックし、HAペアのいずれかのフローティングIPアドレスに使用する環境を選択します。

c. [セキュリティグループ]*をクリックします。
d. [受信ルールの編集]*を選択します。
e. [ルールの追加]をクリックします。
f. [Type]で*[すべてのトラフィック]*を選択し、VPCのIPアドレスを選択します。
g. [ルールの保存]*をクリックして変更を適用します。

7. フローティング IP アドレスを使用して、ボリュームをクライアントにマウントします。

BlueXPで正しいIPアドレスを確認するには、BlueXPの[Manage Volumes]パネルにある*[Mount Command]*オプションを使用します。



8. NFS ボリュームをマウントする場合は、クライアント VPC のサブネットと一致するようにエクスポートポリシーを設定します。

   "ボリュームを編集する方法について説明します"。

   - 関連リンク *
   - "AWS におけるハイアベイラビリティペア"
   - "Cloud Volumes ONTAP in AWS のネットワーク要件"

HAペアを共有サブネットに導入します

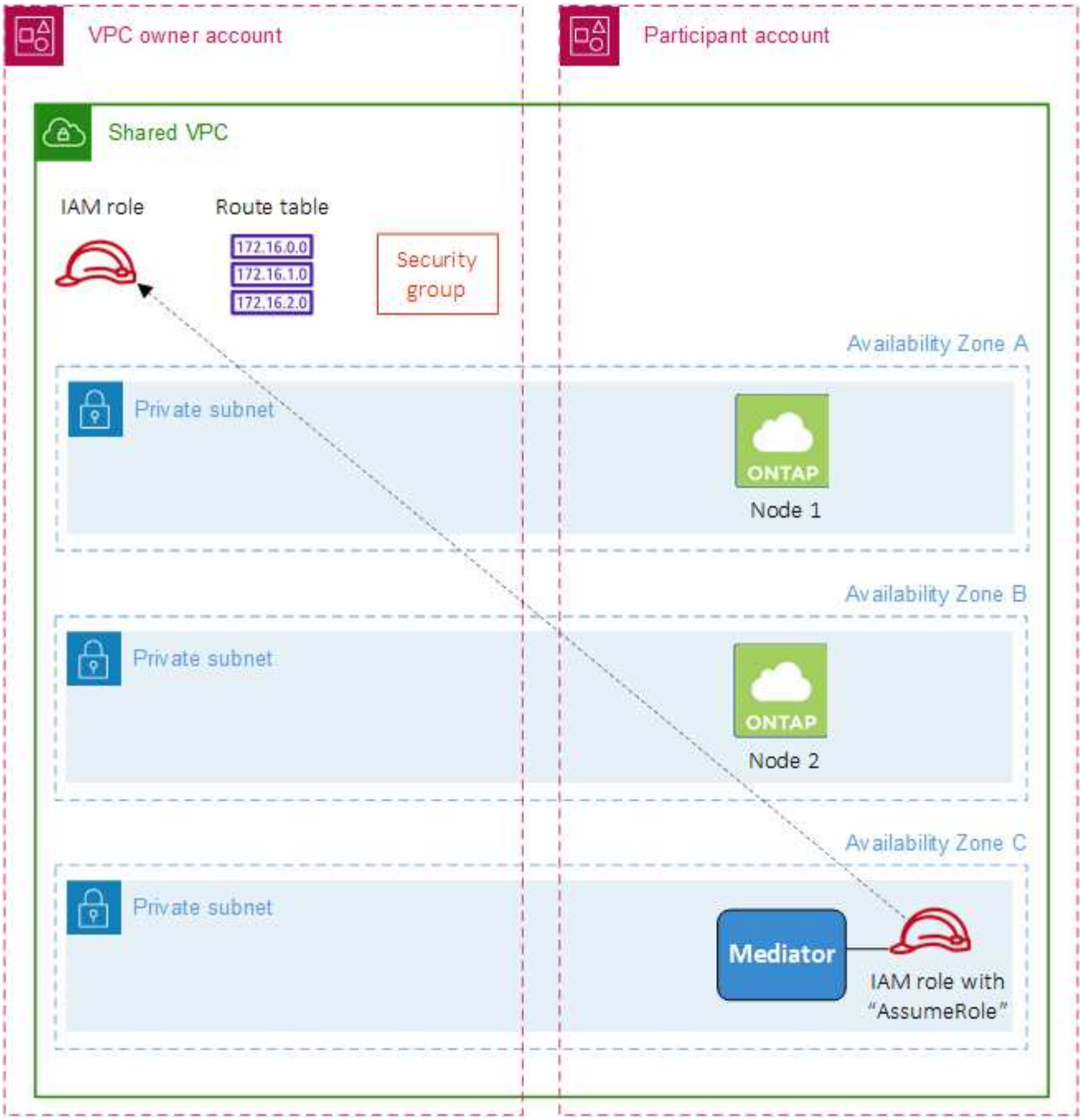
9.11.1リリース以降では、VPCを共有するAWSでCloud Volumes ONTAP HAペアがサポートされます。VPC共有を使用すると、他のAWSアカウントとサブネットを共有できます。この構成を使用するには、AWS環境をセットアップし、APIを使用してHAペアを導入する必要があります。

を使用 "vPC共有"Cloud Volumes ONTAP HA構成は、次の2つのアカウントに分散されます。

- ネットワークを所有するVPC所有者アカウント（VPC、サブネット、ルーティングテーブル、Cloud Volumes ONTAP セキュリティグループ）
- EC2インスタンスが共有サブネット（2つのHAノードとメディエーターを含む）に導入されている参加者アカウント

複数のアベイラビリティゾーンにまたがって導入されているCloud Volumes ONTAP HA構成の場合は、HAメディエーターからVPC所有者アカウントのルーティングテーブルに書き込むための特定の権限が必要です。メディエーターで想定できるIAMロールを設定して、これらの権限を指定する必要があります。

次の図は、この導入に関連するコンポーネントを示しています。



以下の手順で説明するように、サブネットを参加者アカウントと共有し、VPC所有者アカウント内にIAMロールとセキュリティグループを作成する必要があります。

Cloud Volumes ONTAP 作業環境を作成すると、自動的にIAMロールが作成され、メディエーターに関連付けられます。このロールは、VPC所有者アカウントで作成したIAMロールを前提としており、HAペアに関連付けられているルーティングテーブルを変更します。

手順

1. VPC所有者アカウントのサブネットを参加者アカウントと共有します。

   この手順は、HAペアを共有サブネットに導入するために必要です。

   "AWSドキュメント：サブネットを共有"

2. VPC所有者アカウントで、Cloud Volumes ONTAP のセキュリティグループを作成します。

   "Cloud Volumes ONTAP のセキュリティグループルールを参照してください"。HAメディエーターのセキュリティグループを作成する必要はありません。BlueXPはそのような機能を提供します。

3. VPC所有者アカウントで、次の権限を含むIAMロールを作成します。

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. BlueXP APIを使用して'新しいCloud Volumes ONTAP 作業環境を作成します

   次のフィールドを指定する必要があります。

   - "securityGroupId"

     「securityGroupId」フィールドには、VPC所有者アカウントで作成したセキュリティグループを指定する必要があります（上記の手順2を参照）。

   - "haParams"オブジェクトの"amereRoleArn"を想定します

     「仮定ロールアーn」フィールドには、VPC所有者アカウントで作成したIAMロールのARNを含める必要があります（上記の手順3を参照）。

     例：

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

   +
   "Cloud Volumes ONTAP APIについて説明します"

AWS のセキュリティグループルール

BlueXPでは、Cloud Volumes ONTAP が正常に動作するために必要なインバウンドとアウトバウンドのルールを含むAWSセキュリティグループが作成されます。テスト目的または独自のセキュリティグループを使用する場合は、ポートを参照してください。

Cloud Volumes ONTAP のルール

Cloud Volumes ONTAP のセキュリティグループには、インバウンドルールとアウトバウンドルールの両方が必要です。

インバウンドルール

作業環境を作成し、事前定義されたセキュリティグループを選択する場合、次のいずれかの範囲内でトラフィックを許可するように選択できます。

- 選択した**VPC**のみ：インバウンドトラフィックのソースは、Cloud Volumes ONTAP システムのVPCのサブネット範囲、およびコネクタが存在するVPCのサブネット範囲です。これが推奨されるオプションです。
- *すべてのVPC *：インバウンドトラフィックのソースは0.0.0.0/0のIP範囲です。

プロトコル	ポート	目的
すべての ICMP	すべて	インスタンスの ping を実行します
HTTP	80	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTP アクセス
HTTPS	443	コネクタへの接続と、クラスタ管理LIFのIPアドレスを使用したSystem Manager Web コンソールへのHTTPSアクセス
SSH	22	クラスタ管理 LIF またはノード管理 LIF の IP アドレスへの SSH アクセス
TCP	111	NFS のリモートプロシージャコール
TCP	139	CIFS の NetBIOS サービスセッション
TCP	161-162	簡易ネットワーク管理プロトコル
TCP	445	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
TCP	635	NFS マウント
TCP	749	Kerberos
TCP	2049	NFS サーバデーモン
TCP	3260	iSCSI データ LIF を介した iSCSI アクセス
TCP	4045	NFS ロックデーモン
TCP	4046	NFS のネットワークステータスモニタ
TCP	10000	NDMP を使用したバックアップ
TCP	11104	SnapMirror のクラスタ間通信セッションの管理
TCP	11105	クラスタ間 LIF を使用した SnapMirror データ転送
UDP	111	NFS のリモートプロシージャコール
UDP	161-162	簡易ネットワーク管理プロトコル
UDP	635	NFS マウント
UDP	2049	NFS サーバデーモン

プロトコル	ポート	目的
UDP	4045	NFS ロックデーモン
UDP	4046	NFS のネットワークステータスモニタ
UDP	4049	NFS rquotad プロトコル

アウトバウンドルール

Cloud Volumes 用の事前定義済みセキュリティグループ ONTAP は、すべての発信トラフィックをオープンします。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

Cloud Volumes ONTAP 用の定義済みセキュリティグループには、次のアウトバウンドルールが含まれています。

プロトコル	ポート	目的
すべての ICMP	すべて	すべての発信トラフィック
すべての TCP	すべて	すべての発信トラフィック
すべての UDP	すべて	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、 Cloud Volumes ONTAP による発信通信に必要なポートのみを開くことができます。

source は、 Cloud Volumes ONTAP システムのインターフェイス（ IP アドレス）です。

サービス	プロトコル	ポート	ソース	宛先	目的
Active Directory	TCP	88	ノード管理 LIF	Active Directory フォレスト	Kerberos V 認証
	UDP	137	ノード管理 LIF	Active Directory フォレスト	NetBIOS ネームサービス
	UDP	138	ノード管理 LIF	Active Directory フォレスト	NetBIOS データグラムサービス
	TCP	139	ノード管理 LIF	Active Directory フォレスト	NetBIOS サービスセッション
	TCP および UDP	389	ノード管理 LIF	Active Directory フォレスト	LDAP
	TCP	445	ノード管理 LIF	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	TCP	464	ノード管理 LIF	Active Directory フォレスト	Kerberos V パスワードの変更と設定（ SET_CHANGE ）
	UDP	464	ノード管理 LIF	Active Directory フォレスト	Kerberos キー管理
	TCP	749	ノード管理 LIF	Active Directory フォレスト	Kerberos V Change & Set Password （ RPCSEC_GSS ）
	TCP	88	データ LIF （ NFS 、 CIFS 、 iSCSI ）	Active Directory フォレスト	Kerberos V 認証
	UDP	137	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS ネームサービス
	UDP	138	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS データグラムサービス
	TCP	139	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS サービスセッション
	TCP および UDP	389	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	LDAP
	TCP	445	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	TCP	464	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	Kerberos V パスワードの変更と設定（ SET_CHANGE ）
	UDP	464	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	Kerberos キー管理
	TCP	749	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	Kerberos V Change & Set Password （ RPCSEC_GSS ）

サービス	プロトコル	ポート	ソース	宛先	目的
AutoSupport	HTTPS	443	ノード管理 LIF	support.netapp.com	AutoSupport （デフォルトは HTTPS ）
	HTTP	80	ノード管理 LIF	support.netapp.com	AutoSupport （転送プロトコルが HTTPS から HTTP に変更された場合のみ）
	TCP	3128	ノード管理 LIF	コネクタ	アウトバウンドのインターネット接続が使用できない場合に、コネクタのプロキシサーバを介してAutoSupport メッセージを送信する
S3 へのバックアップ	TCP	5010	クラスタ間 LIF	バックアップエンドポイントまたはリストアエンドポイント	S3 へのバックアップ処理とリストア処理 フィーチャー（ Feature ）
クラスタ	すべてのトラフィック	すべてのトラフィック	1 つのノード上のすべての LIF	もう一方のノードのすべての LIF	クラスタ間通信（ Cloud Volumes ONTAP HA のみ）
	TCP	3000	ノード管理 LIF	HA メディエータ	ZAPI コール（ Cloud Volumes ONTAP HA のみ）
	ICMP	1.	ノード管理 LIF	HA メディエータ	キープアライブ（ Cloud Volumes ONTAP HA のみ）
構成のバックアップ	HTTP	80	ノード管理 LIF	http://<connector-IP-address>/occm/offboxconfig	構成バックアップをコネクタに送信します。 "構成バックアップファイルについて説明します"。
DHCP	UDP	68	ノード管理 LIF	DHCP	初回セットアップ用の DHCP クライアント
DHCP	UDP	67	ノード管理 LIF	DHCP	DHCP サーバ
DNS	UDP	53	ノード管理 LIF とデータ LIF （ NFS 、 CIFS ）	DNS	DNS
NDMP	TCP	18600 ～ 18699	ノード管理 LIF	宛先サーバ	NDMP コピー
SMTP	TCP	25	ノード管理 LIF	メールサーバ	SMTP アラート。 AutoSupport に使用できます
SNMP	TCP	161	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	UDP	161	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	TCP	162	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	UDP	162	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視

サービス	プロトコル	ポート	ソース	宛先	目的
SnapMirror	TCP	11104	クラスタ間 LIF	ONTAP クラスタ間 LIF	SnapMirror のクラスタ間通信セッションの管理
	TCP	11105	クラスタ間 LIF	ONTAP クラスタ間 LIF	SnapMirror によるデータ転送
syslog	UDP	514	ノード管理 LIF	syslog サーバ	syslog 転送メッセージ

HA Mediator 外部セキュリティグループのルール

Cloud Volumes ONTAP HA Mediator 用に事前定義された外部セキュリティグループには、次のインバウンドルールとアウトバウンドルールが含まれています。

インバウンドルール

HAメディエーターの事前定義されたセキュリティグループには、次のインバウンドルールが含まれています。

プロトコル	ポート	ソース	目的
TCP	3000	コネクタのCIDR	コネクタからの RESTful API アクセス

アウトバウンドルール

HA メディエータの定義済みセキュリティグループは、すべての発信トラフィックを開きます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

HA Mediator 用の定義済みセキュリティグループには、次のアウトバウンドルールが含まれます。

プロトコル	ポート	目的
すべての TCP	すべて	すべての発信トラフィック
すべての UDP	すべて	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、 HA メディエータによる発信通信に必要なポートだけを開くことができます。

プロトコル	ポート	宛先	目的
HTTP	80	AWS EC2インスタンスのコネクタのIPアドレス	メディエーターのアップグレードをダウンロードします
HTTPS	443	ec2.amazonaws.com	ストレージのフェイルオーバーを支援します
UDP	53	ec2.amazonaws.com	ストレージのフェイルオーバーを支援します

ポート 443 および 53 を開く代わりに、ターゲットサブネットから AWS EC2 サービスへのインターフェイス VPC エンドポイントを作成できます。

HA構成の内部セキュリティグループに関するルール

Cloud Volumes ONTAP HA構成用に事前定義された内部セキュリティグループには、次のルールが含まれています。このセキュリティグループを使用すると、HAノード間、メディエーターとノード間の通信が可能になります。

BlueXPでは常にこのセキュリティグループが作成されます。独自のオプションはありません。

インバウンドルール

事前定義されたセキュリティグループには、次の着信ルールが含まれています。

プロトコル	ポート	目的
すべてのトラフィック	すべて	HA メディエータと HA ノード間の通信

アウトバウンドルール

定義済みのセキュリティグループには、次の発信ルールが含まれます。

プロトコル	ポート	目的
すべてのトラフィック	すべて	HA メディエータと HA ノード間の通信

コネクタのルール

"コネクタのセキュリティグループルールを表示します"

AWS KMS のセットアップ

Cloud Volumes ONTAP で Amazon 暗号化を使用する場合は、 AWS Key Management Service （ KMS ）を設定する必要があります。

手順

1. アクティブな Customer Master Key （ CMK ）が存在することを確認します。

   CMK は、 AWS 管理の CMK または顧客管理の CMK にすることができます。BlueXPやCloud Volumes ONTAP と同じAWSアカウントにすることも、別のAWSアカウントに含めることもできます。

   "AWS ドキュメント：「 Customer Master Keys （ CMK ；カスタマーマスターキー）」"

2. BlueXPに「a_key user__」権限を提供するIAMロールを追加して、各CMKのキーポリシーを変更します。

   IAMロールをキーユーザとして追加すると、Cloud Volumes ONTAP でCMKを使用するためのBlueXP権限が付与されます。

"AWS のドキュメント：「キーの編集"

3. CMK が別の AWS アカウントにある場合は、次の手順を実行します。

   a. CMK が存在するアカウントから KMS コンソールにアクセスします。

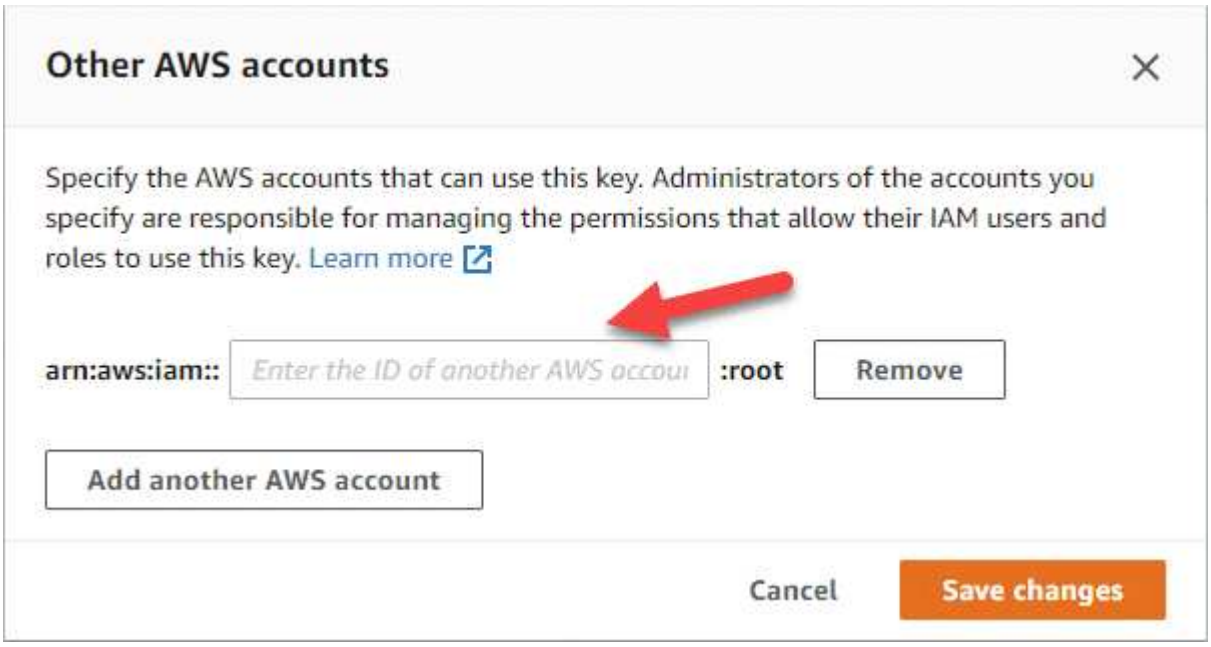
   b. キーを選択します。

   c. General configuration * ペインで、キーの ARN をコピーします。

      Cloud Volumes ONTAP システムを作成するときは、BlueXPにARNを提供する必要があります。

   d. [* Other AWS accounts （その他の**AWS**アカウント）]ペインで、BlueXPに権限を付与するAWSアカウントを追加します。

      ほとんどの場合、これはBlueXPが存在するアカウントです。BlueXPがAWSにインストールされていない場合は、BlueXPにAWSアクセスキーを提供したアカウントになります。



   e. 次に、BlueXPに権限を付与するAWSアカウントに切り替えて、IAMコンソールを開きます。

   f. 以下の権限を含む IAM ポリシーを作成します。

   g. このポリシーを、BlueXPに対する権限を提供するIAMロールまたはIAMユーザに関連付けます。

      次のポリシーは、BlueXPが外部AWSアカウントからCMKを使用するために必要な権限を提供します。「リソース」セクションで、リージョンとアカウント ID を必ず変更してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
このプロセスの詳細については、を参照してください "AWS のマニュアル：他のアカウントのユーザに KMS キーの使用を許可する"。

4. お客様が管理する CMK を使用している場合は、 Cloud Volumes ONTAP IAM ロールを a_key user_権限として追加して、 CMK のキーポリシーを変更します。

この手順は、 Cloud Volumes ONTAP でデータの階層化を有効にし、 S3 バケットに格納されているデータを暗号化する場合に必要です。

作業環境の作成時に IAM ロールが作成されるため、このステップの _ 導入後 _ Cloud Volumes ONTAP を実行する必要があります。（もちろん、既存の Cloud Volumes ONTAP IAM ロールを使用することもできるため、この手順を前に実行することもできます）。

"AWS のドキュメント：「キーの編集"

Cloud Volumes ONTAP 用のIAMロールを設定します

必要な権限を持つIAMロールを各Cloud Volumes ONTAP ノードに関連付ける必要があります。HAメディエーターについても同様です。BlueXPでIAMロールを作成するのが最も簡単ですが、自分の役割を使用することもできます。

このタスクはオプションです。Cloud Volumes ONTAP 作業環境を作成する場合、デフォルトでは、BlueXPでIAMロールを作成することができます。ビジネスのセキュリティポリシーでIAMロールの作成が手動で求められる場合は、次の手順を実行します。

AWS Secret Cloudでは、独自のIAMロールを指定する必要があります。 "C2SにCloud Volumes ONTAP を導入する方法を学習します"。

手順

1. AWS IAMコンソールに移動します。
2. 次の権限を含むIAMポリシーを作成します。
    - Cloud Volumes ONTAP ノードのベースポリシー

標準領域

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud（US）リージョン

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-us-gov:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Top Secret領域

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

シークレットリージョン

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

- Cloud Volumes ONTAP ノードのバックアップポリシー

  Cloud Volumes ONTAP システムでBlueXPのバックアップとリカバリを使用する場合は、ノードのIAMロールに次の2つ目のポリシーを含める必要があります。

標準領域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "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"
        }
    ]
}
```

GovCloud（US）リージョン

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov: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-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Top Secret領域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso: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-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

シークレットリージョン

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso-b: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-iso-b:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- HA メディエータ

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "sts:AssumeRole",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

3. IAMロールを作成し、作成したポリシーを関連付けます。

結果

新しいCloud Volumes ONTAP 作業環境を作成するときに選択できるIAMロールを設定できました。

詳細情報

- "AWSのドキュメント：「IAMポリシーの作成"
- "AWSのドキュメント：「IAMロールの作成"

AWSでCloud Volumes ONTAP のライセンスを設定

Cloud Volumes ONTAP で使用するライセンスオプションを決定したら、新しい作業環境を作成する際にそのライセンスオプションを選択する前に、いくつかの手順を実行する必要があります。

フリーミアム

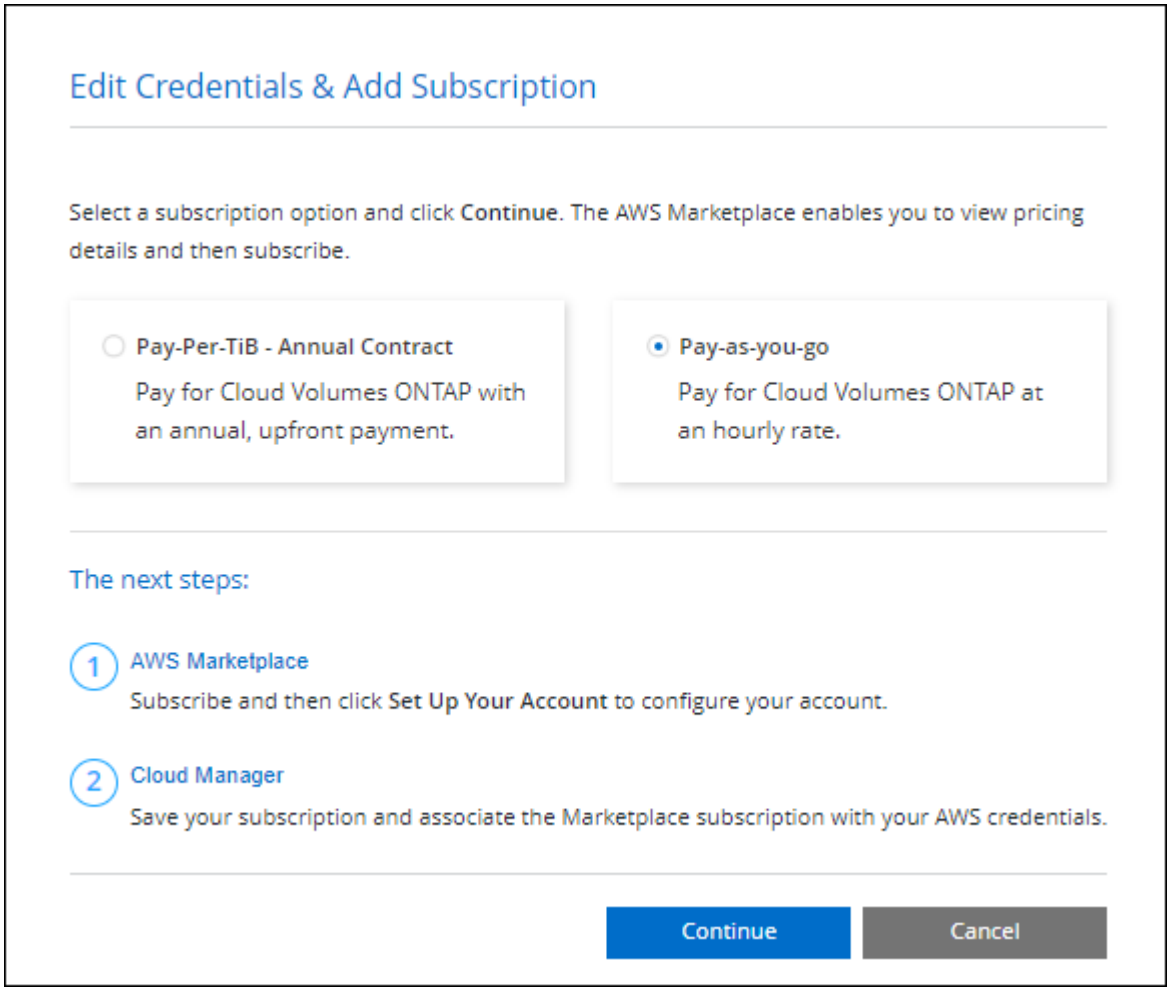
プロビジョニングされた容量が最大500GiBのCloud Volumes ONTAP を無料で使用するには、Freemium製品を選択してください。 "Freemium 製品の詳細をご覧ください"。

手順

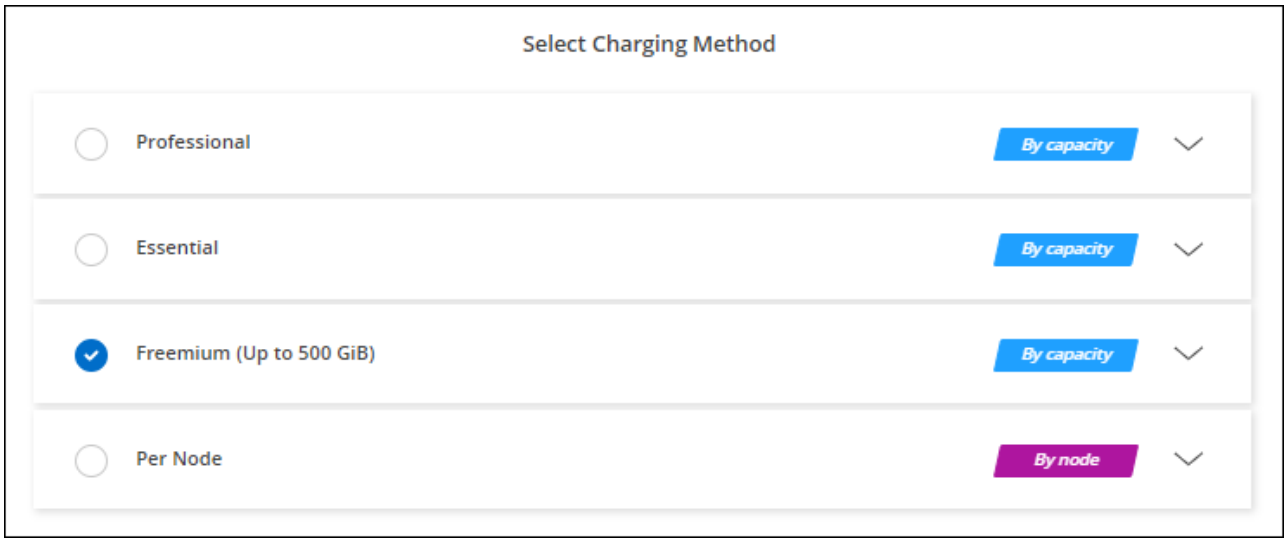
1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。

a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]>[サブスクリプションの追加]をクリックし、プロンプトに従ってAWS Marketplaceで従量課金制サービスに登録します。

プロビジョニング済み容量が500GiBを超えると、システムはに自動的に変換されないかぎり、マーケットプレイスのサブスクリプションを通じて料金が請求されることはありません "Essentials パッケージ"。



a. BlueXPに戻ったら、充電方法のページにアクセスして「* Freemium *」を選択します。



"ステップバイステップの手順を確認して、AWSでCloud Volumes ONTAP を起動してください"。

容量単位のライセンスです

容量単位のライセンスでは、 TiB 単位の Cloud Volumes ONTAP に対して料金を支払うことができます。容量ベースのライセンスは、パッケージ：Essentialsパッケージまたはプロフェッショナルパッケージの形式で提供されます。

Essentials パッケージと Professional パッケージには、次の消費モデルがあります。

- ネットアップから購入したライセンス（ BYOL ）
- AWS Marketplaceで提供する従量課金制（PAYGO）の1時間単位のサブスクリプション
- AWS Marketplaceからの年間契約

"容量単位のライセンスに関する詳細は、こちらをご覧ください"。

以降のセクションでは、これらの各消費モデルの使用方法について説明します。

BYOL

ネットアップからライセンスを購入（BYOL）して前払いし、任意のクラウドプロバイダにCloud Volumes ONTAP システムを導入できます。

手順

1. "ライセンスの取得については、ネットアップの営業部門にお問い合わせください"
2. "NetApp Support Site アカウントをBlueXPに追加します"

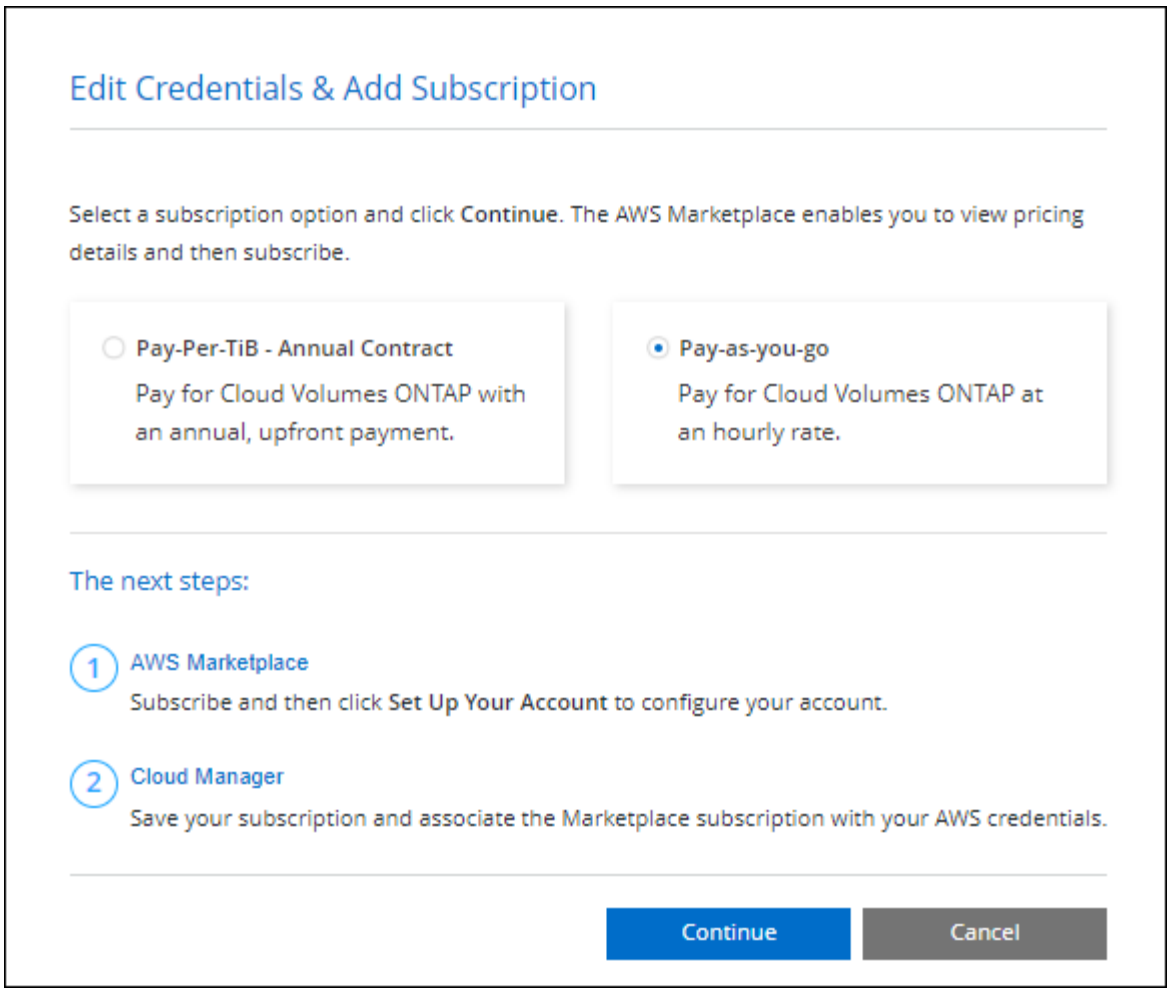
   BlueXPは、ネットアップのライセンスサービスを自動的に照会し、NetApp Support Site アカウントに関連付けられているライセンスの詳細を取得します。エラーがなければ、BlueXPは自動的にライセンスをデジタルウォレットに追加します。

   Cloud Volumes ONTAP でライセンスを使用するには、事前にBlueXPデジタルウォレットからライセンスを入手しておく必要があります。必要に応じて、を実行できます "ライセンスをBlueXPデジタルウォレットに手動で追加します"。

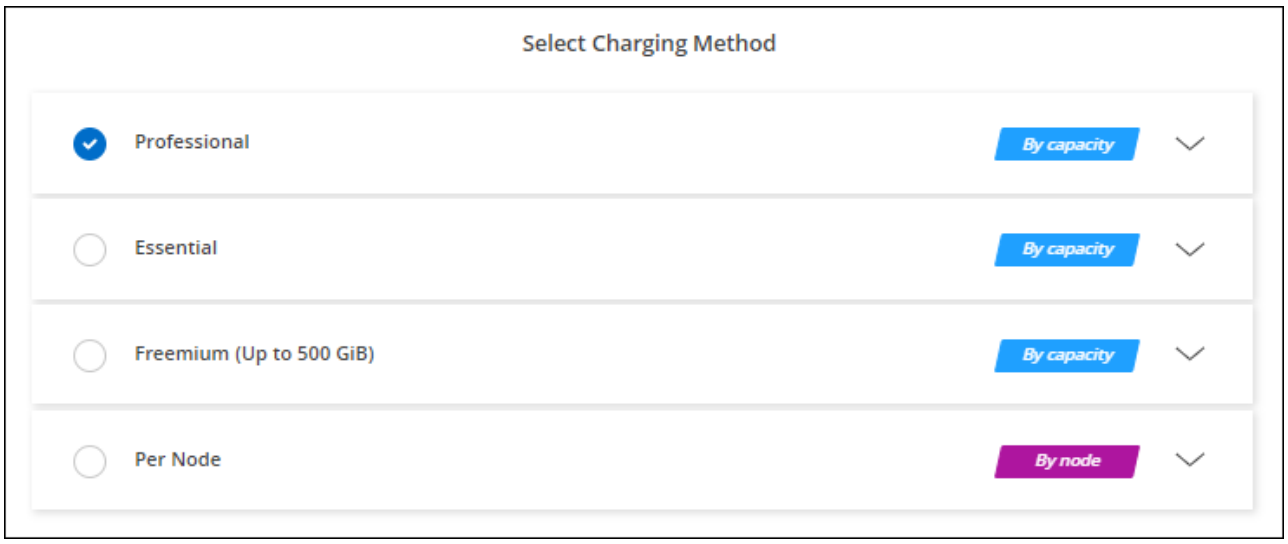
3. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。

   a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]>[サブスクリプションの追加]をクリックし、プロンプトに従ってAWS Marketplaceで従量課金制サービスに登録します。

      ネットアップから購入したライセンスには、最初に必ず料金が請求されますが、ライセンスで許可された容量を超えた場合や、ライセンスの期間が終了した場合は、マーケットプレイスで1時間ごとに料金が請求されます。



a. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



"ステップバイステップの手順を確認して、AWSでCloud Volumes ONTAP を起動してください"。

PAYGOサブスクリプション

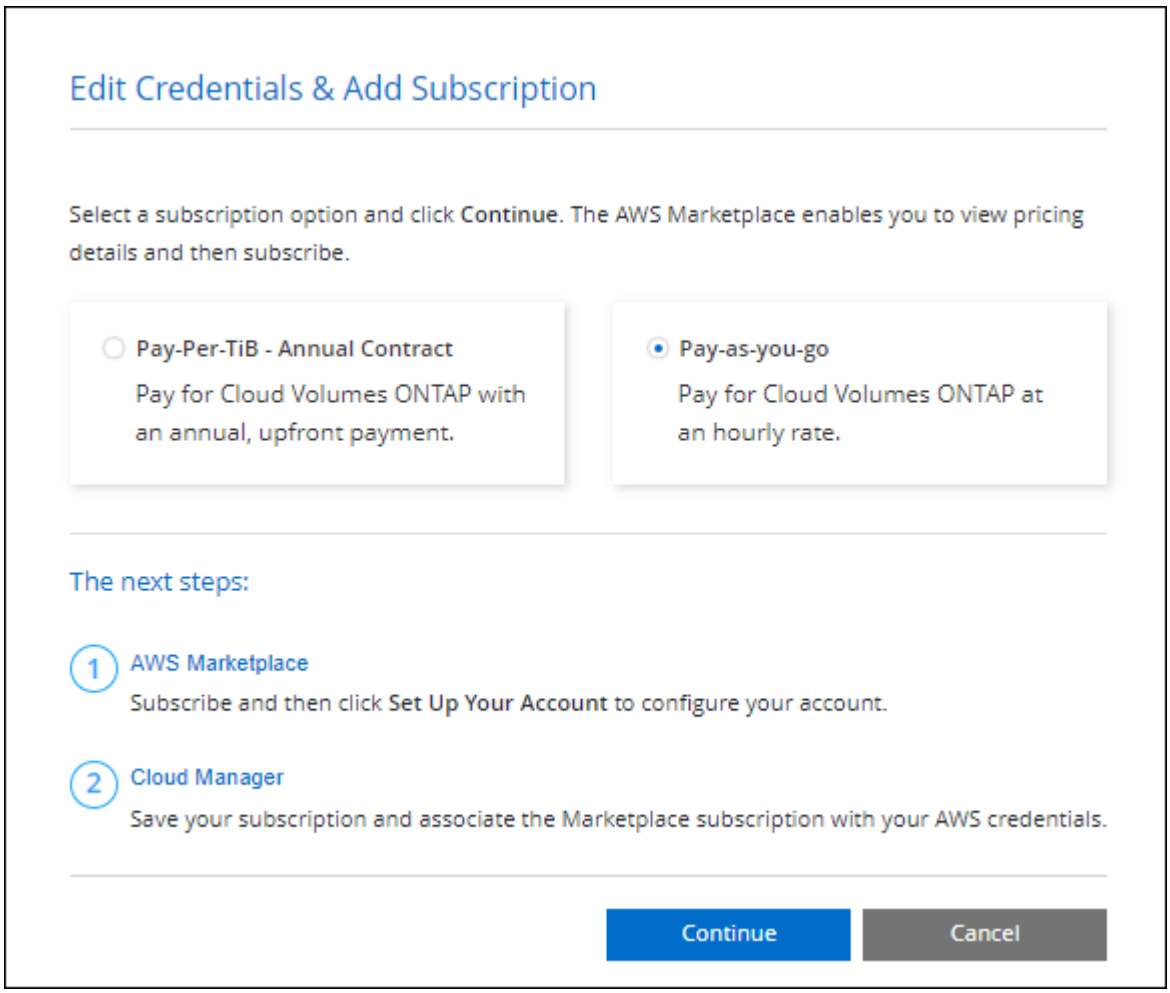
クラウドプロバイダのマーケットプレイスから提供されたサービスに登録すると、1時間ごとに料金が発生し

ます。

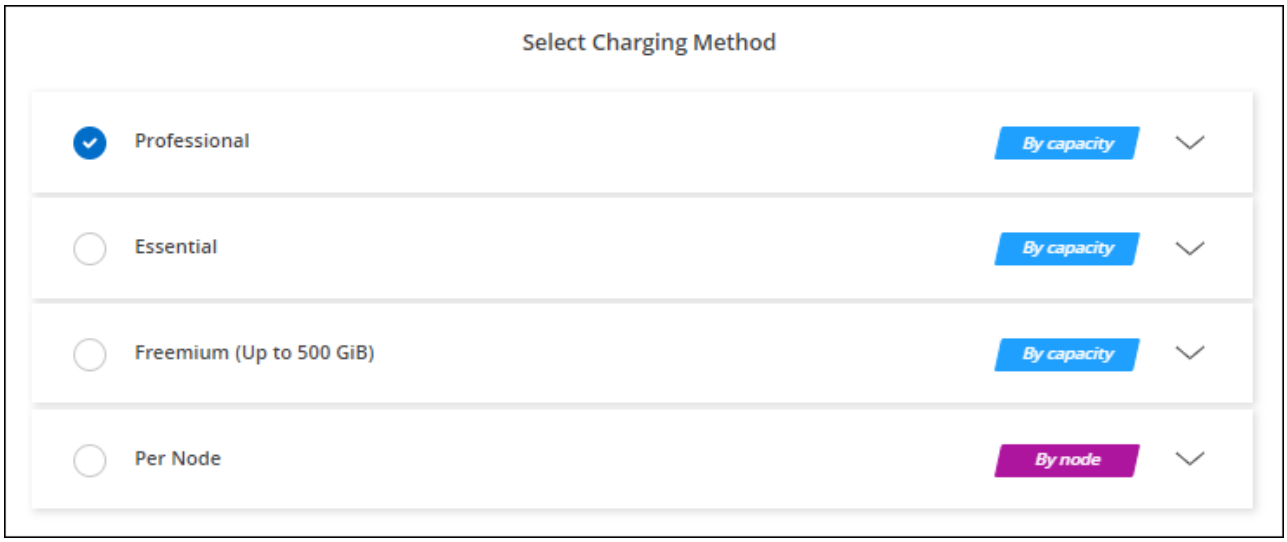
Cloud Volumes ONTAP 作業環境を作成すると、AWS Marketplaceで提供されている契約に登録するよう求めるメッセージが表示されます。このサブスクリプションは、充電のための作業環境に関連付けられます。同じサブスクリプションを追加の作業環境に使用できます。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]>[サブスクリプションの追加]をクリックし、プロンプトに従ってAWS Marketplaceで従量課金制サービスに登録します。



   b. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



"ステップバイステップの手順を確認して、AWSでCloud Volumes ONTAP を起動してください"。

AWSアカウントに関連付けられたAWS Marketplaceのサブスクリプションを管理するには、[設定]>[クレデンシャル]ページを使用します。 "AWSのアカウントとサブスクリプションの管理方法について説明します"

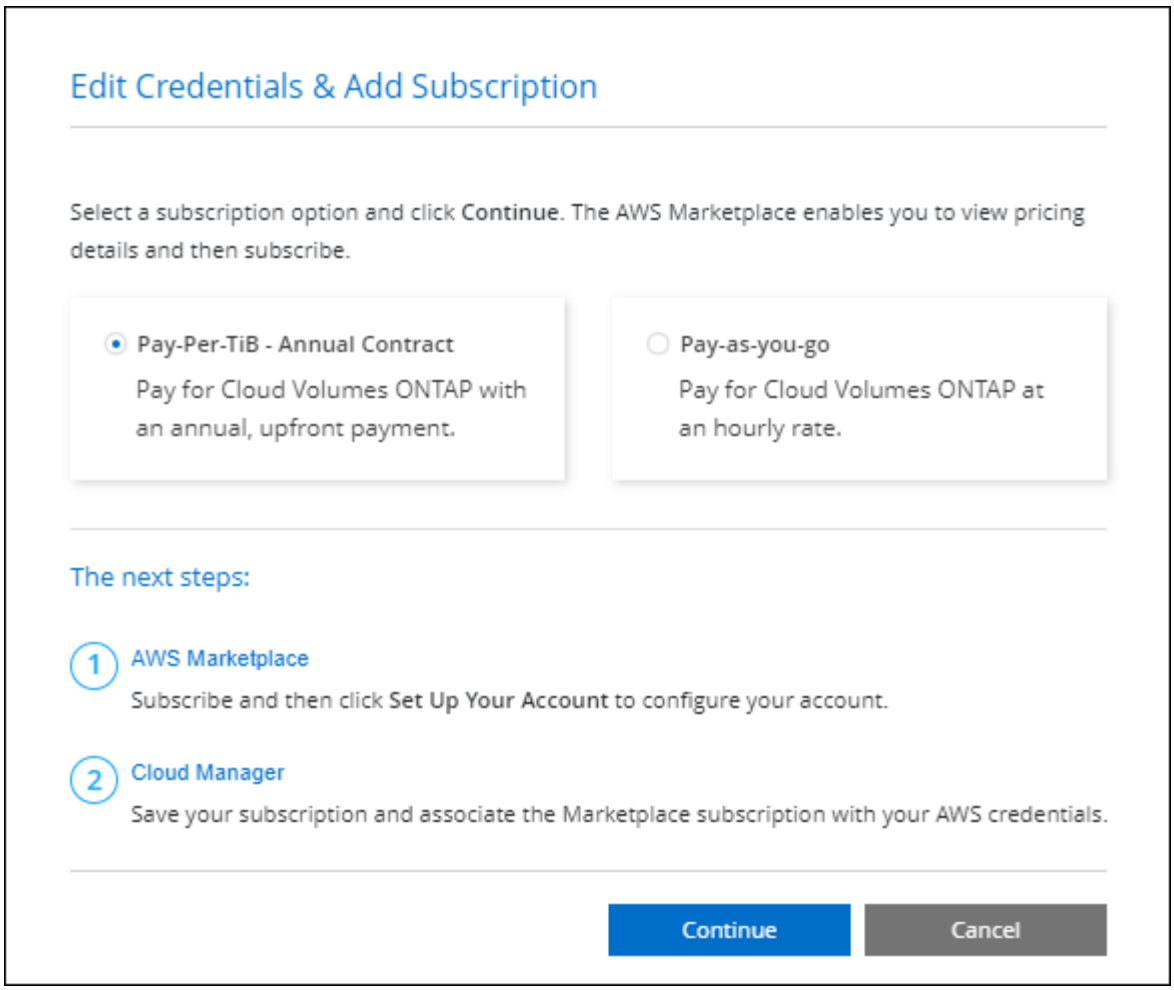
年間契約

クラウドプロバイダのマーケットプレイスから年間契約を購入することで、年間料金を支払うことができます。

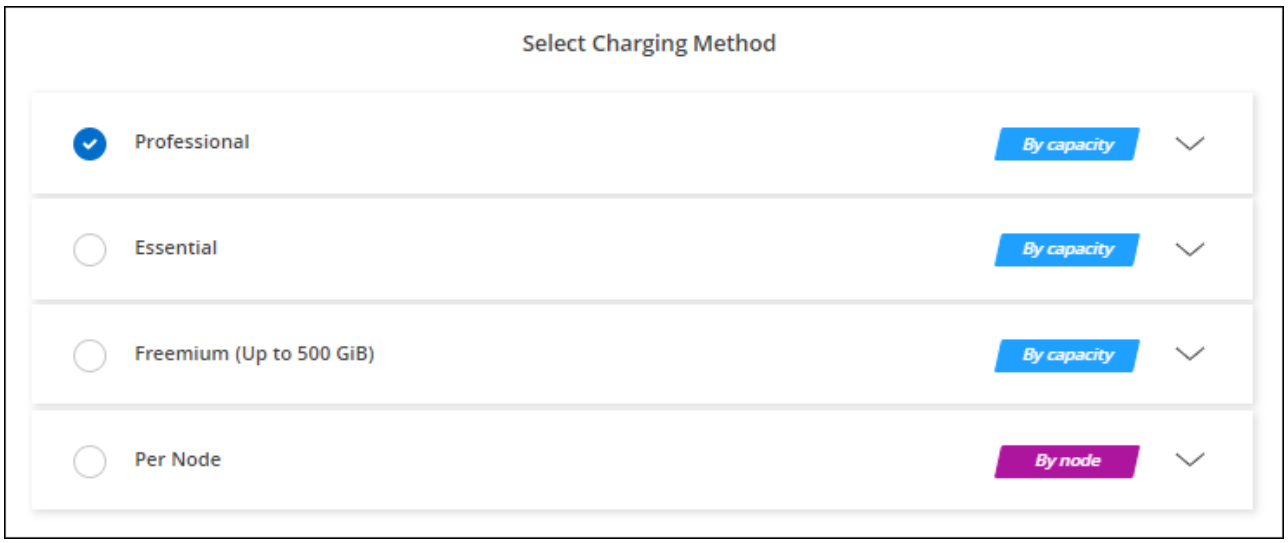
BlueXPでは、時間単位のサブスクリプションと同様に、AWS Marketplaceで提供されている年間契約を登録するよう求められます。

手順

1. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]>[サブスクリプションの追加]をクリックし、プロンプトに従ってAWS Marketplaceで年間契約をサブスクライブします。



b. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



"ステップバイステップの手順を確認して、AWSでCloud Volumes ONTAP を起動してください"。

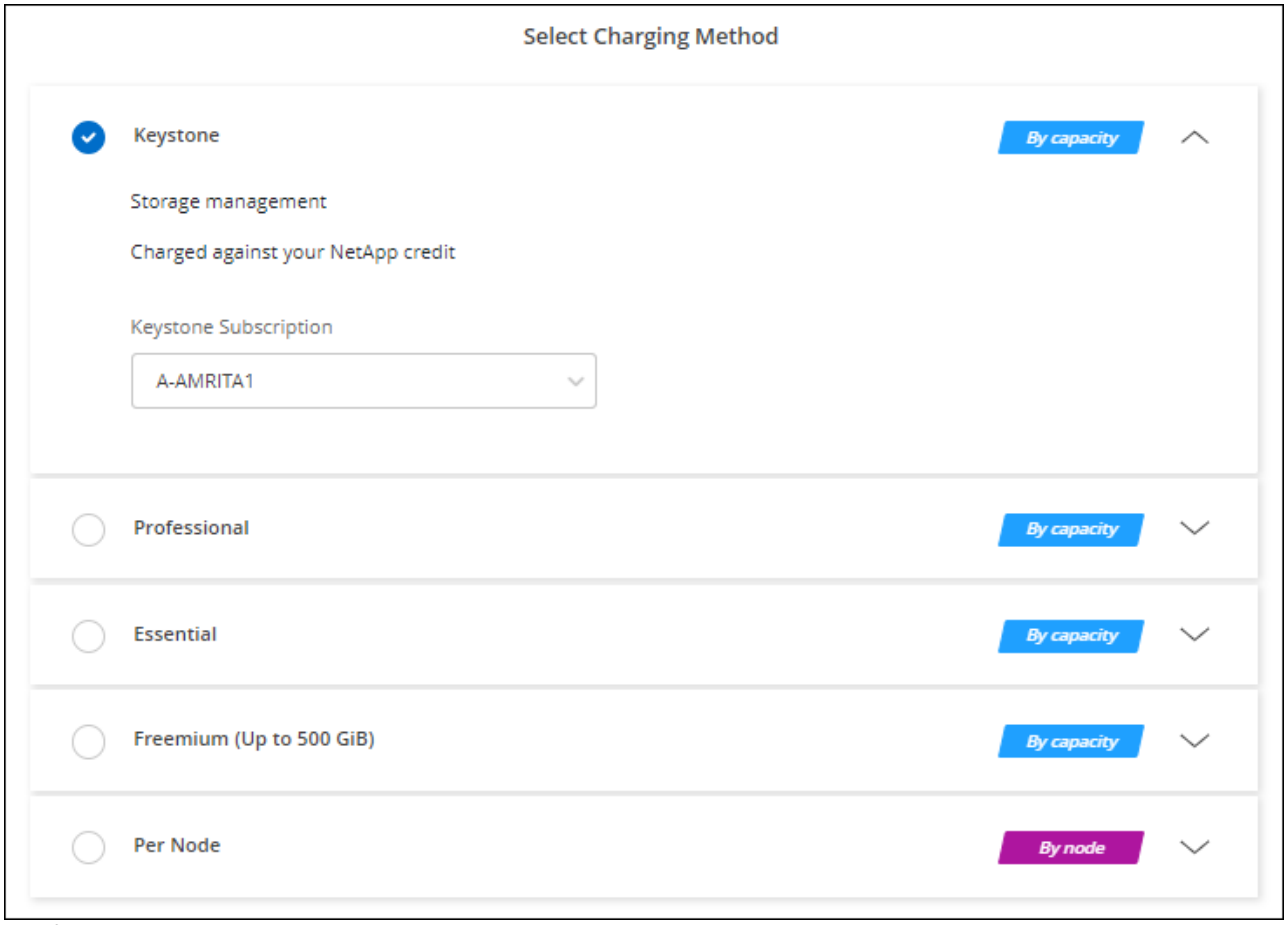
Keystoneサブスクリプション

Keystoneサブスクリプションは、ビジネスの成長に応じたサブスクリプションベースのサービスです。

"NetApp Keystone サブスクリプションの詳細については、こちらをご覧ください"。

手順

1. まだサブスクリプションをお持ちでない場合は、 "ネットアップにお問い合わせください"
2. mailto：ng-keystone-success@netapp.com [ネットアップにお問い合わせください]。1つ以上のKeystoneサブスクリプションでBlueXPユーザアカウントを承認する場合。
3. ネットアップがお客様のアカウントを許可したあと、 "Cloud Volumes ONTAP で使用するサブスクリプションをリンクします"。
4. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. 課金方法を選択するよう求められたら、Keystoneサブスクリプションの課金方法を選択します。



オプションのスクリーンショット。"]

"ステップバイステップの手順を確認して、AWSでCloud Volumes ONTAP を起動してください"。

AWS での Cloud Volumes ONTAP の起動

Cloud Volumes ONTAP は単一システム構成で起動することも、 AWS で HA ペアとして起動することもできます。

始める前に

作業環境を作成するには、次の作業が必要です。

- 稼働中のコネクタ。
  - を用意しておく必要があります "ワークスペースに関連付けられているコネクタ"。
  - "コネクタをで実行したままにする準備をしておく必要があります 常時"。
- 使用する構成についての理解。

  設定を選択し、管理者から AWS ネットワーク情報を取得して準備を完了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 "Cloud Volumes ONTAP 構成を計画"。
- Cloud Volumes ONTAP のライセンスを設定するために必要な事項を理解する。

  "ライセンスの設定方法について説明します"。
- CIFS 構成用の DNS と Active Directory

  詳細については、を参照してください "Cloud Volumes ONTAP in AWS のネットワーク要件"。

AWS でのシングルノード Cloud Volumes ONTAP システムの起動

AWSでCloud Volumes ONTAP を起動する場合は、BlueXPで新しい作業環境を作成する必要があります

このタスクについて

作業環境を作成した直後に、指定されたVPCでテストインスタンスを起動して接続を検証します。成功すると、すぐにインスタンスが終了し、Cloud Volumes ONTAP システムの導入が開始されます。BlueXPが接続を検証できない場合は'作業環境の作成に失敗しますテストインスタンスは、 t2.nano （デフォルトの vPC テナンシーの場合）または m3.medium （専用の vPC テナンシーの場合）のいずれかです。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. [[subscribe] キャンバスページで、 * 作業環境の追加 * をクリックし、プロンプトに従います。
3. * 場所を選択 * ：「 * Amazon Web Services * 」と「 * Cloud Volumes ONTAP シングルノード * 」を選択します。
4. プロンプトが表示されたら、 "コネクタを作成します"。
5. * 詳細とクレデンシャル * ：必要に応じて、 AWS のクレデンシャルとサブスクリプションを変更し、作業環境名を入力してタグを追加し、パスワードを入力します。

   このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

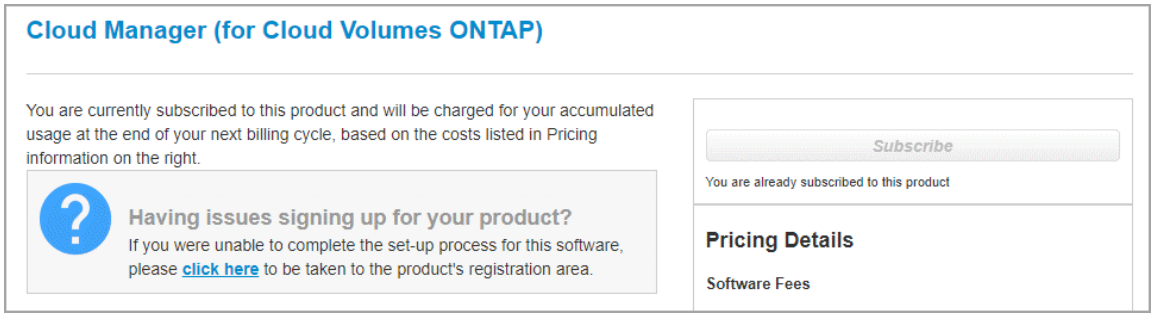
フィールド	説明
作業環境名	BlueXPでは、作業環境名を使用してCloud Volumes ONTAP システムとAmazon EC2インスタンスの両方に名前を付けます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。

フィールド	説明
タグを追加します	AWS タグは、 AWS リソースのメタデータです。BlueXPは、Cloud Volumes ONTAP インスタンスとそのインスタンスに関連付けられている各AWSリソースにタグを追加します。作業環境を作成するときに、ユーザインターフェイスから最大 4 つのタグを追加し、作成後にさらに追加できます。API では、作業環境の作成時にタグを 4 つに制限することはありません。タグの詳細については、を参照してください "AWS ドキュメント：「 Tagging your Amazon EC2 Resources"。
ユーザ名とパスワード	Cloud Volumes ONTAP クラスタ管理者アカウントのクレデンシャルです。このクレデンシャルを使用して、 System Manager またはその CLI から Cloud Volumes ONTAP に接続できます。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します
資格情報を編集します	このシステムを導入するアカウントに関連付けられている AWS クレデンシャルを選択します。この Cloud Volumes ONTAP システムで使用する AWS Marketplace サブスクリプションを関連付けることもできます。 Add Subscription * をクリックして、選択したクレデンシャルを新しい AWS Marketplace サブスクリプションに関連付けます。サブスクリプションは、年間契約の場合と、 Cloud Volumes ONTAP の料金を 1 時間ごとに支払う場合があります。 "BlueXPにAWSクレデンシャルを追加する方法について説明します"。

次のビデオでは、従量課金制の Marketplace サブスクリプションを AWS クレデンシャルに関連付ける方法を紹介します。

AWS MarketplaceでBlueXPにサブスクライブ

複数の IAM ユーザが同じ AWS アカウントで作業する場合は、各ユーザにサブスクライブする必要があります。最初のユーザがサブスクライブすると、次の図に示すように、 AWS Marketplace から後続のユーザに登録済みであることが通知されます。AWS_account_ のサブスクリプションが設定されている間、各 IAM ユーザは、そのサブスクリプションに自分自身を関連付ける必要があります。次のメッセージが表示されたら、[Click here *（ここをクリック）]リンクをクリックしてBlueXP Webサイトにアクセスし、プロセスを完了します。



6. * サービス *: サービスを有効にしておくか、 Cloud Volumes ONTAP で使用しない個々のサービスを無効にします。
   - "BlueXPの分類の詳細については、こちらをご覧ください"
   - "BlueXPのバックアップとリカバリの詳細については、こちらをご覧ください"

WORMとデータ階層化を活用する場合は、BlueXPのバックアップとリカバリを無効にし、バージョン9.8以降のCloud Volumes ONTAP 作業環境を導入する必要があります。

7. * 場所と接続 * ：に記録したネットワーク情報を入力します "AWS ワークシート"。

   次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
vPC	AWS Outpost を使用している場合は、 Outpost VPC を選択して、その Outpost に単一のノードの Cloud Volumes ONTAP システムを導入できます。エクスペリエンスは、 AWS に存在する他の VPC と同じです。
セキュリティグループが生成されました	BlueXPがセキュリティグループを生成するようにした場合は、トラフィックを許可する方法を選択する必要があります。 • 「* Selected VPC Only *」を選択した場合、インバウンドトラフィックのソースは、選択したVPCのサブネット範囲と、コネクタが存在するVPCのサブネット範囲です。これが推奨されるオプションです。 • どのVPC *も選択した場合、インバウンドトラフィックのソースは0.0.0.0/0のIP範囲になります。
既存のセキュリティグループを使用する	既存のファイアウォールポリシーを使用する場合は、必要なルールが含まれていることを確認してください。 "Cloud Volumes ONTAP のファイアウォールルールについて説明します"。

8. * データ暗号化 * ：データ暗号化なし、または AWS で管理する暗号化を選択します。

   AWS で管理する暗号化の場合は、アカウントまたは別の AWS アカウントから別の Customer Master Key （ CMK ；カスタマーマスターキー）を選択できます。

   Cloud Volumes ONTAP システムの作成後に AWS のデータ暗号化方式を変更することはできません。

   "Cloud 用の AWS KMS の設定方法については、こちらをご覧ください Volume ONTAP の略"。

   "サポートされている暗号化テクノロジの詳細を確認してください"。

9. * 充電方法と NSS アカウント * ：このシステムで使用する充電オプションを指定し、ネットアップサポートサイトのアカウントを指定します。
   - "Cloud Volumes ONTAP のライセンスオプションについて説明します"。
   - "ライセンスの設定方法について説明します"。
10. * Cloud Volumes ONTAP 構成 * （ AWS Marketplace の年間契約のみ）：デフォルトの構成を確認して「 * Continue * 」をクリックするか、「 * 構成の変更 * 」をクリックして独自の構成を選択します。

    デフォルトの設定を使用している場合、ボリュームを指定し、構成を確認および承認するだけで済みます。

11. 構成済みパッケージ：Cloud Volumes ONTAP をすばやく起動するパッケージを1つ選択するか、*構成の変更*をクリックして独自の構成を選択します。

いずれかのパッケージを選択した場合、ボリュームを指定し、構成を確認および承認するだけで済みます。

12. **IAM**の役割: BlueXPが役割を作成できるようにするには、既定のオプションをそのまま使用することをお勧めします。

    独自のポリシーを使用する場合は、それが満たされている必要があります "Cloud Volumes ONTAP ノードのポリシーの要件"。

13. ライセンス：必要に応じてCloud Volumes ONTAP のバージョンを変更し、インスタンスタイプとインスタンステナンシーを選択します。

    選択したバージョンで新しいリリース候補、一般提供、またはパッチリリースが利用可能な場合、作業環境の作成時にシステムがそのバージョンに更新されます。たとえば、Cloud Volumes ONTAP 9.10.1と9.10.1 P4が利用可能になっていれば、更新が実行されます。たとえば、 9.6 から 9.7 への更新など、あるリリースから別のリリースへの更新は行われません。

14. 基盤となるストレージリソース：ディスクタイプを選択し、基盤となるストレージを構成して、データの階層化を有効にするかどうかを選択します。

    次の点に注意してください。

    - ディスクタイプは最初のボリューム（およびアグリゲート）用です。以降のボリューム（およびアグリゲート）には別のディスクタイプを選択できます。
    - GP3またはio1ディスクを選択した場合、BlueXPはAWSのElastic Volumes機能を使用して、必要に応じて、基盤となるストレージディスク容量を自動的に増やします。初期容量はストレージのニーズに基づいて選択し、Cloud Volumes ONTAP の導入後に変更することができます。 "Elastic VolumesのAWSサポートの詳細については、こちらをご覧ください"。
    - gp2ディスクまたはst1ディスクを選択する場合、シンプルなプロビジョニングオプションを使用する場合、初期アグリゲートおよびBlueXPで作成される追加のアグリゲートのすべてのディスクサイズを選択できます。Advanced Allocation オプションを使用すると、異なるディスクサイズを使用するアグリゲートを作成できます。
    - ボリュームを作成または編集するときに、特定のボリューム階層化ポリシーを選択できます。
    - データの階層化を無効にすると、以降のアグリゲートで有効にすることができます。

      "データ階層化の仕組みをご確認ください"。

15. *書き込み速度とWORM *：

    a. 必要に応じて、「標準」または「高速」の書き込み速度を選択します。

       "書き込み速度の詳細については、こちらをご覧ください。"。

    b. 必要に応じて、Write Once、Read Many（WORM）ストレージをアクティブにします。

       Cloud Volumes ONTAP 9.7以前のバージョンでデータ階層化が有効になっている場合は、WORMを有効にすることはできません。Cloud Volumes ONTAP 9.8へのリバートまたはダウングレードは、WORMと階層化を有効にしたあとはブロックされます。

    "WORM ストレージの詳細については、こちらをご覧ください。"。

a. WORMストレージをアクティブ化する場合は、保持期間を選択します。

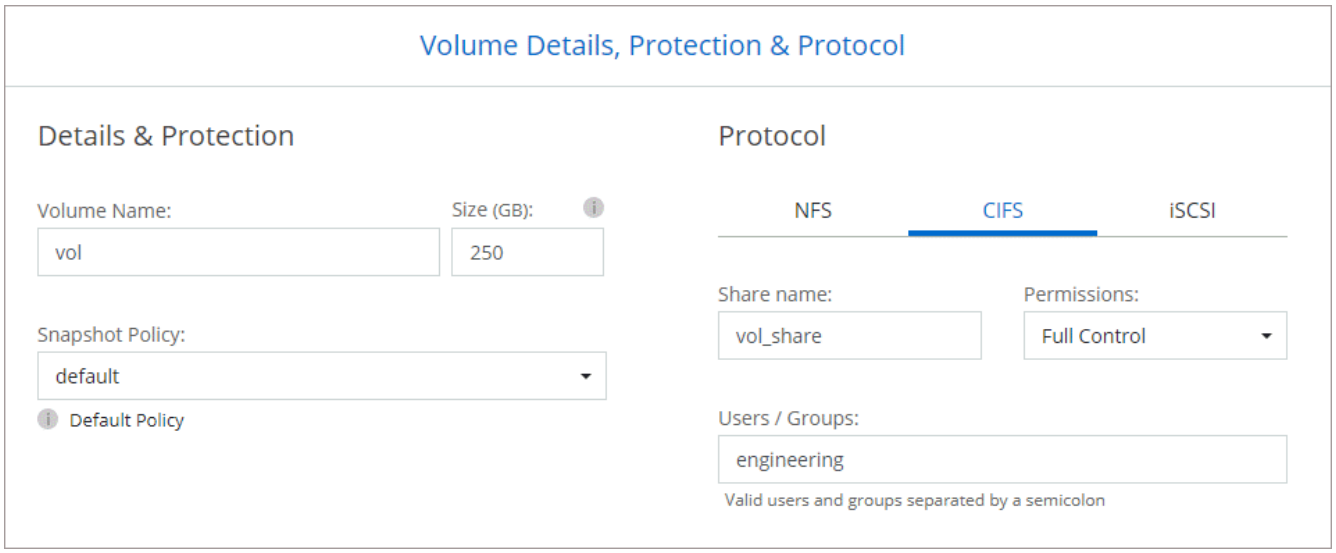
16. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

"サポートされるクライアントプロトコルおよびバージョンについて説明します"。

このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
サイズ	入力できる最大サイズは、シンプロビジョニングを有効にするかどうかによって大きく異なります。シンプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。
アクセス制御（ NFS のみ）	エクスポートポリシーは、ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、BlueXPはサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。
権限とユーザー / グループ（ CIFS のみ）	これらのフィールドを使用すると、ユーザおよびグループ（アクセスコントロールリストまたは ACL とも呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、 UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、 domain\username 形式でユーザのドメインを指定する必要があります。
スナップショットポリシー	Snapshot コピーポリシーは、自動的に作成される NetApp Snapshot コピーの頻度と数を指定します。NetApp Snapshot コピーは、パフォーマンスに影響を与えず、ストレージを最小限に抑えるポイントインタイムファイルシステムイメージです。デフォルトポリシーを選択することも、なしを選択することもできます。一時データには、 Microsoft SQL Server の tempdb など、 none を選択することもできます。
アドバンストオプション（ NFS のみ）	ボリュームの NFS バージョンを NFSv3 または NFSv4 のいずれかで選択してください。
イニシエータグループと IQN （ iSCSI のみ）	iSCSI ストレージターゲットは LUN （論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。イニシエータグループは、 iSCSI ホストのノード名のテーブルであり、どのイニシエータがどの LUN にアクセスできるかを制御します。iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（ NIC ）、ソフトウェアイニシエータを搭載した TOE カード、 CNA 、または専用の HBA を使用してネットワークに接続され、 iSCSI Qualified Name （ IQN ）で識別されます。iSCSIボリュームを作成すると、BlueXPによって自動的にLUNが作成されます。ボリュームごとに 1 つの LUN だけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、 "IQN を使用して、から LUN に接続します ホスト"。

次の図は、 CIFS プロトコルの [Volume] ページの設定を示しています。



17. * CIFS セットアップ * ： CIFS プロトコルを選択した場合は、 CIFS サーバをセットアップします。

フィールド	説明
DNS プライマリおよびセカンダリ IP アドレス	CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、 CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスロケーションレコード（ SRV ）が含まれている必要があります。
参加する Active Directory ドメイン	CIFS サーバを参加させる Active Directory （ AD ）ドメインの FQDN 。
ドメインへの参加を許可されたクレデンシャル	AD ドメイン内の指定した組織単位（ OU ）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。AWS Managed Microsoft AD を Cloud Volumes ONTAP の AD サーバとして設定する場合は、このフィールドに「 * OU=computers 、 OU=corp * 」と入力します。
DNS ドメイン	Cloud Volumes ONTAP Storage Virtual Machine （ SVM ）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。
NTP サーバ	Active Directory DNS を使用して NTP サーバを設定するには、「 Active Directory ドメインを使用」を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、 API を使用してください。を参照してください "BlueXP自動化ドキュメント" を参照してください。 NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

18. * 使用状況プロファイル、ディスクタイプ、階層化ポリシー * ：必要に応じて、 Storage Efficiency 機能を有効にするかどうかを選択し、ボリューム階層化ポリシーを編集します。

    詳細については、を参照してください "ボリューム使用率プロファイルについて" および "データ階層化の概要"。

19. * レビューと承認 *: 選択内容を確認して確認します。
    a. 設定の詳細を確認します。
    b. [詳細情報*]をクリックして、BlueXPが購入するサポートとAWSリソースの詳細を確認します。
    c. [* I understand … * （理解しています … * ）] チェックボックスを選択
    d. [Go*] をクリックします。

結果

Cloud Volumes ONTAP インスタンスが起動します。タイムラインで進行状況を追跡できます。

Cloud Volumes ONTAP インスタンスの起動時に問題が発生した場合は、障害メッセージを確認してください。また、作業環境を選択して、 [環境の再作成] をクリックすることもできます。

詳細については、を参照してください "NetApp Cloud Volumes ONTAP のサポート"。

完了後

- CIFS 共有をプロビジョニングした場合は、ファイルとフォルダに対する権限をユーザまたはグループに付与し、それらのユーザが共有にアクセスしてファイルを作成できることを確認します。
- ボリュームにクォータを適用する場合は、 System Manager または CLI を使用します。

  クォータを使用すると、ユーザ、グループ、または qtree が使用するディスク・スペースとファイル数を制限または追跡できます。

AWS での Cloud Volumes ONTAP HA ペアの起動

AWSでCloud Volumes ONTAP HAペアを起動するには、BlueXPでHA作業環境を作成する必要があります。

制限事項

現時点では、 AWS アウトポストで HA ペアがサポートされていません。

このタスクについて

作業環境を作成した直後に、指定されたVPCでテストインスタンスを起動して接続を検証します。成功すると、すぐにインスタンスが終了し、Cloud Volumes ONTAP システムの導入が開始されます。BlueXPが接続を検証できない場合は'作業環境の作成に失敗しますテストインスタンスは、 t2.nano （デフォルトの vPC テナンシーの場合）または m3.medium （専用の vPC テナンシーの場合）のいずれかです。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. Canvas ページで、 * Add Working Environment * をクリックし、画面の指示に従います。
3. 場所を選択：「* Amazon Web Services 」と「 Cloud Volumes ONTAP HA *」を選択します。

   一部のAWSローカルゾーンを使用できます。

   AWSローカルゾーンを使用する前に、ローカルゾーンを有効にし、AWSアカウントのローカルゾーンでサブネットを作成する必要があります。の*および[Extend your Amazon VPC to the Local Zone]*の手順に従います。 "AWSチュートリアル「Get Started Deploying Low Latency Applications with AWS Local Zones」"。

コネクタバージョン3.9.36以前を実行している場合は、AWS EC2コンソールのAWSコネクタロールにDescribeAvailabilityZones権限を追加する必要があります。

4. * 詳細とクレデンシャル * ：必要に応じて、 AWS のクレデンシャルとサブスクリプションを変更し、作業環境名を入力してタグを追加し、パスワードを入力します。

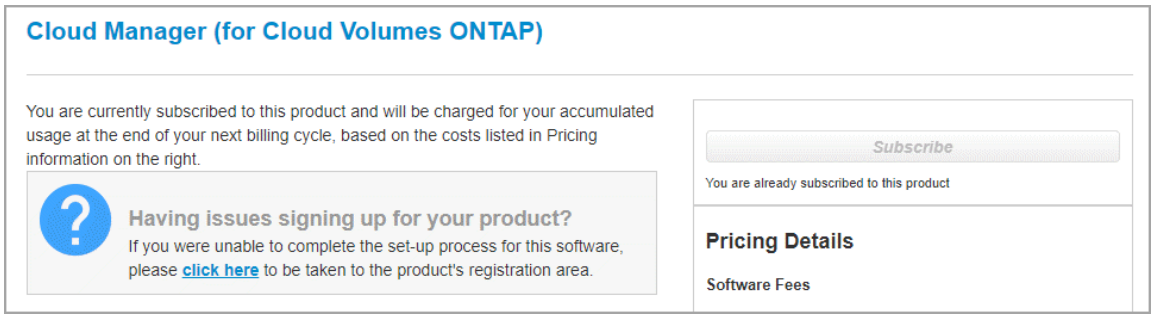
   このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
作業環境名	BlueXPでは、作業環境名を使用してCloud Volumes ONTAP システムとAmazon EC2インスタンスの両方に名前を付けます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。
タグを追加します	AWS タグは、 AWS リソースのメタデータです。BlueXPは、Cloud Volumes ONTAP インスタンスとそのインスタンスに関連付けられている各AWSリソースにタグを追加します。作業環境を作成するときに、ユーザインターフェイスから最大 4 つのタグを追加し、作成後にさらに追加できます。API では、作業環境の作成時にタグを 4 つに制限することはありません。タグの詳細については、を参照してください "AWS ドキュメント：「 Tagging your Amazon EC2 Resources"。
ユーザ名とパスワード	Cloud Volumes ONTAP クラスタ管理者アカウントのクレデンシャルです。このクレデンシャルを使用して、 System Manager またはその CLI から Cloud Volumes ONTAP に接続できます。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します
資格情報を編集します	この Cloud Volumes ONTAP システムで使用する AWS クレデンシャルと Marketplace サブスクリプションを選択します。 Add Subscription * をクリックして、選択したクレデンシャルを新しい AWS Marketplace サブスクリプションに関連付けます。サブスクリプションは、年間契約の場合と、 Cloud Volumes ONTAP の料金を 1 時間ごとに支払う場合があります。 NetApp （ BYOL ）からライセンスを直接購入した場合、 AWS サブスクリプションは必要ありません。 "BlueXPにAWSクレデンシャルを追加する方法について説明します"。

次のビデオでは、従量課金制の Marketplace サブスクリプションを AWS クレデンシャルに関連付ける方法を紹介します。

AWS MarketplaceでBlueXPにサブスクライブ

複数の IAM ユーザが同じ AWS アカウントで作業する場合は、各ユーザにサブスクライブする必要があります。最初のユーザがサブスクライブすると、次の図に示すように、 AWS Marketplace から後続のユーザに登録済みであることが通知されます。AWS_account_ のサブスクリプションが設定されている間、各 IAM ユーザは、そのサブスクリプションに自分自身を関連付ける必要があります。次のメッセージが表示されたら、[Click here *（ここをクリック）]リンクをクリックしてBlueXP Webサイトにアクセスし、プロセスを完了します。



5. * サービス *: この Cloud Volumes ONTAP システムで使用しない個々のサービスを有効または無効にしておきます。
   - "BlueXPの分類の詳細については、こちらをご覧ください"
   - "BlueXPのバックアップとリカバリの詳細については、こちらをご覧ください"

   WORMとデータ階層化を活用する場合は、BlueXPのバックアップとリカバリを無効にし、バージョン9.8以降のCloud Volumes ONTAP 作業環境を導入する必要があります。

6. *HA 導入モデル *: HA 構成を選択します。

   導入モデルの概要については、を参照してください "AWS での Cloud Volumes ONTAP HA"。

7. 場所と接続（単一AZ）または*リージョンとVPC *（複数のAZ）：AWSワークシートに記録したネットワーク情報を入力します。

   次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
セキュリティグループが生成されました	BlueXPがセキュリティグループを生成するようにした場合は、トラフィックを許可する方法を選択する必要があります。 • 「* Selected VPC Only *」を選択した場合、インバウンドトラフィックのソースは、選択したVPCのサブネット範囲と、コネクタが存在するVPCのサブネット範囲です。これが推奨されるオプションです。 • どのVPC *も選択した場合、インバウンドトラフィックのソースは0.0.0.0/0のIP範囲になります。
既存のセキュリティグループを使用する	既存のファイアウォールポリシーを使用する場合は、必要なルールが含まれていることを確認してください。 "Cloud Volumes ONTAP のファイアウォールルールについて説明します"。

8. * 接続と SSH 認証 * ： HA ペアとメディエーターの接続方法を選択します。

9. * フローティング IP * ：複数の AZ を選択した場合は、フローティング IP アドレスを指定します。

   IP アドレスは、その地域のすべての VPC の CIDR ブロックの外側にある必要があります。詳細については、を参照してください "複数の AZS での Cloud Volumes ONTAP HA の AWS ネットワーク要件"。

10. * ルートテーブル * ：複数の AZ を選択した場合は、フローティング IP アドレスへのルートを含むルーティングテーブルを選択します。

    複数のルートテーブルがある場合は、正しいルートテーブルを選択することが非常に重要です。そうしないと、一部のクライアントが Cloud Volumes ONTAP HA ペアにアクセスできない場合があります。ルーティングテーブルの詳細については、を参照してください "AWS のドキュメント：「 Route Tables"。

11. * データ暗号化 * ：データ暗号化なし、または AWS で管理する暗号化を選択します。

    AWS で管理する暗号化の場合は、アカウントまたは別の AWS アカウントから別の Customer Master Key （ CMK ；カスタマーマスターキー）を選択できます。

    Cloud Volumes ONTAP システムの作成後に AWS のデータ暗号化方式を変更することはできません。

    "Cloud 用の AWS KMS の設定方法については、こちらをご覧ください Volume ONTAP の略"。

    "サポートされている暗号化テクノロジの詳細を確認してください"。

12. * 充電方法と NSS アカウント * ：このシステムで使用する充電オプションを指定し、ネットアップサポートサイトのアカウントを指定します。

    - "Cloud Volumes ONTAP のライセンスオプションについて説明します"。
    - "ライセンスの設定方法について説明します"。

13. * Cloud Volumes ONTAP 構成 * （ AWS Marketplace の年間契約のみ）：デフォルトの構成を確認して「 * Continue * 」をクリックするか、「 * 構成の変更 * 」をクリックして独自の構成を選択します。

    デフォルトの設定を使用している場合、ボリュームを指定し、構成を確認および承認するだけで済みます。

14. * 構成済みパッケージ * （時間単位または BYOL のみ）： Cloud Volumes ONTAP をすばやく起動するパッケージを 1 つ選択するか、 * 構成の変更 * をクリックして独自の構成を選択します。

    いずれかのパッケージを選択した場合、ボリュームを指定し、構成を確認および承認するだけで済みます。

15. **IAM**の役割: BlueXPが役割を作成できるようにするには、既定のオプションをそのまま使用することをお勧めします。

    独自のポリシーを使用する場合は、それが満たされている必要があります "Cloud Volumes ONTAP ノードと HA のポリシー要件 メディエーター"。

16. ライセンス：必要に応じてCloud Volumes ONTAP のバージョンを変更し、インスタンスタイプとインスタンステナンシーを選択します。

選択したバージョンで新しいリリース候補、一般提供、またはパッチリリースが利用可能な場合、作業環境の作成時にシステムがそのバージョンに更新されます。たとえば、Cloud Volumes ONTAP 9.10.1と9.10.1 P4が利用可能になっていれば、更新が実行されます。たとえば、 9.6 から 9.7 への更新など、あるリリースから別のリリースへの更新は行われません。

17. 基盤となるストレージリソース：ディスクタイプを選択し、基盤となるストレージを構成して、データの階層化を有効にするかどうかを選択します。

    次の点に注意してください。

    - ディスクタイプは最初のボリューム（およびアグリゲート）用です。以降のボリューム（およびアグリゲート）には別のディスクタイプを選択できます。
    - GP3またはio1ディスクを選択した場合、BlueXPはAWSのElastic Volumes機能を使用して、必要に応じて、基盤となるストレージディスク容量を自動的に増やします。初期容量はストレージのニーズに基づいて選択し、Cloud Volumes ONTAP の導入後に変更することができます。 "Elastic Volumes のAWSサポートの詳細については、こちらをご覧ください"。
    - gp2ディスクまたはst1ディスクを選択する場合、シンプルなプロビジョニングオプションを使用する場合、初期アグリゲートおよびBlueXPで作成される追加のアグリゲートのすべてのディスクサイズを選択できます。Advanced Allocation オプションを使用すると、異なるディスクサイズを使用するアグリゲートを作成できます。
    - ボリュームを作成または編集するときに、特定のボリューム階層化ポリシーを選択できます。
    - データの階層化を無効にすると、以降のアグリゲートで有効にすることができます。

      "データ階層化の仕組みをご確認ください"。

18. *書き込み速度とWORM *：

    a. 必要に応じて、「標準」または「高速」の書き込み速度を選択します。

       "書き込み速度の詳細については、こちらをご覧ください。"。

    b. 必要に応じて、Write Once、Read Many（WORM）ストレージをアクティブにします。

       Cloud Volumes ONTAP 9.7以前のバージョンでデータ階層化が有効になっている場合は、WORMを有効にすることはできません。Cloud Volumes ONTAP 9.8へのリバートまたはダウングレードは、WORMと階層化を有効にしたあとはブロックされます。

    "WORM ストレージの詳細については、こちらをご覧ください。"。

    a. WORMストレージをアクティブ化する場合は、保持期間を選択します。

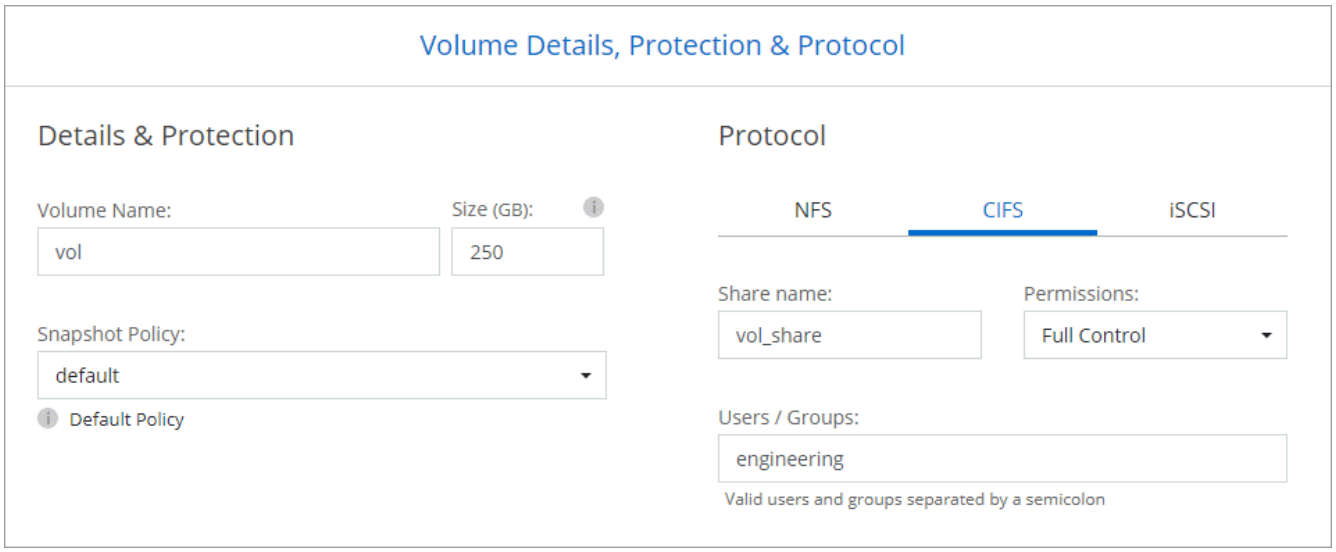
19. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

    "サポートされるクライアントプロトコルおよびバージョンについて説明します"。

    このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
サイズ	入力できる最大サイズは、シンプロビジョニングを有効にするかどうかによって大きく異なります。シンプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。
アクセス制御（ NFS のみ）	エクスポートポリシーは、ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、BlueXPはサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。
権限とユーザー / グループ（ CIFS のみ）	これらのフィールドを使用すると、ユーザおよびグループ（アクセスコントロールリストまたは ACL とも呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、 UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、 domain\username 形式でユーザのドメインを指定する必要があります。
スナップショットポリシー	Snapshot コピーポリシーは、自動的に作成される NetApp Snapshot コピーの頻度と数を指定します。NetApp Snapshot コピーは、パフォーマンスに影響を与えず、ストレージを最小限に抑えるポイントインタイムファイルシステムイメージです。デフォルトポリシーを選択することも、なしを選択することもできます。一時データには、 Microsoft SQL Server の tempdb など、 none を選択することもできます。
アドバンストオプション（ NFS のみ）	ボリュームの NFS バージョンを NFSv3 または NFSv4 のいずれかで選択してください。
イニシエータグループと IQN （ iSCSI のみ）	iSCSI ストレージターゲットは LUN （論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。イニシエータグループは、 iSCSI ホストのノード名のテーブルであり、どのイニシエータがどの LUN にアクセスできるかを制御します。iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（ NIC ）、ソフトウェアイニシエータを搭載した TOE カード、 CNA 、または専用の HBA を使用してネットワークに接続され、 iSCSI Qualified Name （ IQN ）で識別されます。iSCSIボリュームを作成すると、BlueXPによって自動的にLUNが作成されます。ボリュームごとに 1 つの LUN だけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、 "IQN を使用して、から LUN に接続します ホスト"。

次の図は、 CIFS プロトコルの [Volume] ページの設定を示しています。



20. * CIFS セットアップ * ： CIFS プロトコルを選択した場合は、 CIFS サーバをセットアップします。

フィールド	説明
DNS プライマリおよびセカンダリ IP アドレス	CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、 CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスロケーションレコード（ SRV ）が含まれている必要があります。
参加する Active Directory ドメイン	CIFS サーバを参加させる Active Directory （ AD ）ドメインの FQDN 。
ドメインへの参加を許可されたクレデンシャル	AD ドメイン内の指定した組織単位（ OU ）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。AWS Managed Microsoft AD を Cloud Volumes ONTAP の AD サーバとして設定する場合は、このフィールドに「 * OU=computers 、 OU=corp * 」と入力します。
DNS ドメイン	Cloud Volumes ONTAP Storage Virtual Machine （ SVM ）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。
NTP サーバ	Active Directory DNS を使用して NTP サーバを設定するには、「 Active Directory ドメインを使用」を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、 API を使用してください。を参照してください "BlueXP自動化ドキュメント" を参照してください。 NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

21. * 使用状況プロファイル、ディスクタイプ、階層化ポリシー * ：必要に応じて、 Storage Efficiency 機能を有効にするかどうかを選択し、ボリューム階層化ポリシーを編集します。

    詳細については、を参照してください "ボリュームの使用プロファイルを選択してください" および "データ階層化の概要"。

22. * レビューと承認 *: 選択内容を確認して確認します。
    a. 設定の詳細を確認します。
    b. [詳細情報*]をクリックして、BlueXPが購入するサポートとAWSリソースの詳細を確認します。
    c. [* I understand … * （理解しています … * ）] チェックボックスを選択
    d. [Go*] をクリックします。

結果

Cloud Volumes ONTAP HAペアが起動します。タイムラインで進行状況を追跡できます。

HA ペアの起動で問題が発生した場合は、障害メッセージを確認します。また、作業環境を選択して、 [環境の再作成] をクリックすることもできます。

詳細については、を参照してください "NetApp Cloud Volumes ONTAP のサポート"。

完了後

- CIFS 共有をプロビジョニングした場合は、ファイルとフォルダに対する権限をユーザまたはグループに付与し、それらのユーザが共有にアクセスしてファイルを作成できることを確認します。
- ボリュームにクォータを適用する場合は、 System Manager または CLI を使用します。

  クォータを使用すると、ユーザ、グループ、または qtree が使用するディスク・スペースとファイル数を制限または追跡できます。

AWS Secret CloudリージョンとTop Secret CloudリージョンにCloud Volumes ONTAPを導入

標準のAWSリージョンと同様に、BlueXPは "AWSシークレットクラウド" およびインチ "AWSのトップシークレットクラウド" クラウドストレージにエンタープライズクラスの機能を提供するCloud Volumes ONTAPを導入するには、次の手順を実行します。AWS Secret CloudとTop Secret Cloudは、米国Intelligence Community：このページの手順は、AWS Secret CloudおよびTop Secret Cloudリージョンのユーザにのみ適用されます。

作業を開始する前に

作業を開始する前に、AWS Secret CloudとTop Secret Cloudでサポートされているバージョンを確認し、BlueXPのプライベートモードについて学習してください。

- AWS Secret CloudおよびTop Secret Cloudでサポートされている次のバージョンを確認してください。
  - Cloud Volumes ONTAP 9.12.1 P2
  - コネクタのバージョン3.9.32

    Connectorは、AWSでCloud Volumes ONTAP を導入して管理するために必要なソフトウェアです。コネクタインスタンスにインストールされているソフトウェアからBlueXPにログインします。BlueXP向けのSaaS Webサイトは、AWS Secret CloudとTop Secret Cloudではサポートされていません。
- プライベートモードの詳細

  AWS Secret CloudおよびTop Secret Cloudでは、BlueXPは_privateモード_で動作します。プライベートモードでは、BlueXP SaaSレイヤへの接続はありません。BlueXPには、SaaSレイヤではなくコネクタからアクセスできるWebベースのコンソールからローカルにアクセスします。

  プライベートモードの動作の詳細については、を参照してください。 "BlueXPプライベート導入モード"。

手順**1**：ネットワークをセットアップする

Cloud Volumes ONTAP が適切に動作するように AWS ネットワークをセットアップします。

手順

1. コネクタインスタンスと Cloud Volumes ONTAP インスタンスを起動する VPC とサブネットを選択します。
2. VPC とサブネットがコネクタと Cloud Volumes ONTAP 間の接続をサポートしていることを確認します。
3. S3 サービスへの vPC エンドポイントをセットアップします。

Cloud Volumes ONTAP から低コストのオブジェクトストレージにコールドデータを階層化する場合は、VPC エンドポイントが必要です。

手順**2**：権限を設定する

AWSシークレットクラウドまたはトップシークレットクラウドでアクションを実行するために必要な権限をコネクタとCloud Volumes ONTAPに提供するIAMポリシーとロールを設定します。

次の項目について、 IAM ポリシーと IAM ロールを 1 つずつ用意する必要があります。

- コネクタインスタンス
- Cloud Volumes ONTAP インスタンス
- HAペアの場合は、Cloud Volumes ONTAPのHAメディエーターインスタンス（HAペアを導入する場合）

手順

1. AWS IAM コンソールに移動し、 * Policies * をクリックします。
2. コネクタインスタンスのポリシーを作成します。

AWS環境のS3バケットをサポートするために、これらのポリシーを作成します。あとでバケットを作成するときは、バケット名の先頭に「 `fabric-pool-`。この要件は、AWSシークレットクラウドリージョンとTop Secret Cloudリージョンの両方を環境にします。

シークレットリージョン

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
```

```
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
```

```
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Top Secret領域

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
```

```
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
```

```
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
```

```
        ]
}
```

3. Cloud Volumes ONTAP のポリシーを作成します。

シークレットリージョン

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Top Secret領域

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

HAペアについて、Cloud Volumes ONTAP HAペアを導入する場合は、HAメディエーターのポリシーを作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

4. タイプが Amazon EC2 の IAM ロールを作成し、前の手順で作成したポリシーを関連付けます。

   ロールを作成します。

   ポリシーと同様に、コネクタにはIAMロールが1つ、Cloud Volumes ONTAPノードにはIAMロールが1つ必要です。
   HAペアの場合：ポリシーと同様に、コネクタ用、Cloud Volumes ONTAPノード用、HAメディエーター用（HAペアを導入する場合）用にIAMロールが1つ必要です。

   ロールを選択します。

   コネクタインスタンスを起動するときに、コネクタ IAM ロールを選択する必要があります。Cloud Volumes ONTAPのIAMロールは、BlueXPでCloud Volumes ONTAP作業環境を作成するときに選択できます。
   HAペアの場合、BlueXPでCloud Volumes ONTAP作業環境を作成するときに、Cloud Volumes ONTAPのIAMロールとHAメディエーターを選択できます。

ステップ3：AWS KMSをセットアップする

Cloud Volumes ONTAPでAmazon暗号化を使用する場合は、AWSキー管理サービス（KMS）の要件が満たされていることを確認してください。

手順

1. アクティブな Customer Master Key （ CMK ；カスタマーマスターキー）がアカウントまたは別の AWS アカウントに存在することを確認します。

   CMK は、 AWS 管理の CMK または顧客管理の CMK にすることができます。

2. Cloud Volumes ONTAP を導入するアカウントとは別の AWS アカウントに CMK を配置する場合は、そのキーの ARN を取得する必要があります。

Cloud Volumes ONTAP システムを作成するときは、BlueXPにARNを提供する必要があります。

3. コネクタインスタンスのIAMロールをCMKのキーユーザのリストに追加します。

   これにより、Cloud Volumes ONTAP でCMKを使用するためのBlueXP権限が与えられます。

手順4：コネクタをインストールして**BlueXP**をセットアップする

BlueXPを使用してAWSにCloud Volumes ONTAPを導入する前に、BlueXP Connectorをインストールしてセットアップする必要があります。Connectorを使用すると、BlueXPは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ます（Cloud Volumes ONTAP を含む）。

手順

1. Privacy Enhanced Mail （ PEM ） Base-64 でエンコードされた X.509 形式の認証局（ CA ）が署名したルート証明書を取得する証明書を入手するには、組織のポリシーと手順を参照してください。

   > AWS Secret Cloudリージョンの場合は、 `NSS Root CA 2` 証明書、およびTop Secret Cloudの場合は、 `Amazon Root CA 4` 証明書。チェーン全体ではなく、これらの証明書のみをアップロードしてください。証明書チェーンのファイルが大きいため、アップロードに失敗する可能性があります。追加の証明書がある場合は、次の手順で説明するように、後でアップロードできます。

   セットアッププロセス中に証明書をアップロードする必要があります。BlueXPでは、HTTPS経由でAWSに要求を送信するときに信頼された証明書が使用されます。

2. コネクタインスタンスを起動します。
   a. AWS Intelligence Community MarketplaceのBlueXPのページにアクセスします。
   b. Custom Launch タブで、 EC2 コンソールからインスタンスを起動するオプションを選択します。
   c. プロンプトに従って、インスタンスを設定します。

      インスタンスを設定する際には、次の点に注意してください。

      - t3.xlarge をお勧めします。
      - 権限の設定時に作成したIAMロールを選択する必要があります。
      - デフォルトのストレージオプションはそのままにしておく必要があります。
      - コネクタに必要な接続方法は、 SSH 、 HTTP 、 HTTPS です。
3. コネクタインスタンスに接続されているホストからBlueXPをセットアップします。
   a. Web ブラウザを開き、と入力します https://ipaddress _ipaddress_は、コネクタをインストールしたLinuxホストのIPアドレスです。
   b. AWS サービスに接続するためのプロキシサーバを指定します。
   c. 手順 1 で取得した証明書をアップロードします。
   d. [新しいBlueXPのセットアップ]*を選択し、プロンプトに従ってシステムをセットアップします。
      - システムの詳細：コネクタの名前と会社名を入力します。

- * 管理者ユーザーの作成 * ：システムの管理者ユーザーを作成します。

  このユーザアカウントはシステム上でローカルに実行されます。BlueXPからはAuth0サービスに接続できません。

- 確認：詳細を確認し、使用許諾契約に同意して、*セットアップ*を選択します。

e. CA 署名証明書のインストールを完了するには、 EC2 コンソールからコネクタインスタンスを再起動します。

4. コネクタが再起動したら、セットアップウィザードで作成した管理者ユーザアカウントを使用してログインします。

手順**5**：（オプション）プライベートモード証明書をインストールする

この手順は、AWS Secret CloudリージョンとTop Secret Cloudリージョンではオプションであり、前の手順でインストールしたルート証明書以外の追加の証明書がある場合にのみ必要です。

手順

1. インストールされている既存の証明書を表示

   a. occmコンテナDocker ID（識別名「DS-occm-1」）を収集するには、次のコマンドを実行します。

   ```
   docker ps
   ```

   b. occmコンテナ内に入るには、次のコマンドを実行します。

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   c. 「trust_store_password」環境変数からパスワードを収集するには、次のコマンドを実行します。

   ```
   env
   ```

   d. 信頼ストアにインストールされているすべての証明書を一覧表示するには、次のコマンドを実行し、前の手順で収集したパスワードを使用します。

   ```
   keytool -list -v -keystore occm.truststore
   ```

2. 証明書を追加します。

   a. occmコンテナDocker ID（識別名「ds-occm-1」）を収集するには、次のコマンドを実行します。

   ```
   docker ps
   ```

   b. occmコンテナ内に入るには、次のコマンドを実行します。

```
docker exec -it <docker-id> /bin/sh
```

新しい証明書ファイルをに保存します。

c. 「trust_store_password」環境変数からパスワードを収集するには、次のコマンドを実行します。

```
env
```

d. 証明書を信頼ストアに追加するには、次のコマンドを実行し、前の手順のパスワードを使用します。

```
keytool -import -alias <alias-name> -file <certificate-file-name>
-keystore occm.truststore
```

e. 証明書がインストールされていることを確認するには、次のコマンドを実行します。

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

f. occmコンテナを終了するには、次のコマンドを実行します。

```
exit
```

g. occmコンテナをリセットするには、次のコマンドを実行します。

```
docker restart <docker-id>
```

手順**6**：**BlueXP**デジタルウォレットにライセンスを追加する

NetAppからライセンスを購入した場合は、新しいCloud Volumes ONTAPシステムを作成するときにライセンスを選択できるように、そのライセンスをBlueXPデジタルウォレットに追加する必要があります。デジタルウォレットは、これらのライセンスを未割り当てとして識別します。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. [*Node] Cloud Volumes ONTAP タブで、ドロップダウンから[*Node Based Licenses]を選択します。
3. [* 未割り当て * （ Unassigned * ）]
4. [未割り当てライセンスの追加] をクリックします。
5. ライセンスのシリアル番号を入力するか、ライセンスファイルをアップロードしてください。
6. ライセンスファイルがまだない場合は、netapp.comから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. にアクセスします "ネットアップライセンスファイルジェネレータ" をクリックし、NetApp Support Siteのクレデンシャルでログインします。

b. パスワードを入力し、製品を選択してシリアル番号を入力し、プライバシーポリシーを読み、同意したことを確認してから、 * Submit * をクリックします。

c. 電子メールまたは直接ダウンロードで serialnumber.nlf JSON ファイルを受信するかどうかを選択します。

7. [ライセンスの追加] をクリックします。

結果

BlueXPはデジタルウォレットにライセンスを追加します。ライセンスは、新しい Cloud Volumes ONTAP システムに関連付けるまでは未割り当てとみなされます。その後、ライセンスはデジタルウォレットの[BYOL]タブに移動します。

ステップ**7**：**BlueXP**から**Cloud Volumes ONTAP**を起動する

BlueXPで新しい作業環境を作成することで、AWS Secret CloudおよびTop Secret CloudでCloud Volumes ONTAPインスタンスを起動できます。

作業を開始する前に

HAペアの場合、HAメディエーターへのキーベースのSSH認証を有効にするには、キーペアが必要です。

手順

1. 作業環境ページで、 * 作業環境の追加 * をクリックします。
2. [Create]*で、Cloud Volumes ONTAPを選択します。

   HAの場合：*[作成]*で、[Cloud Volumes ONTAP]または[Cloud Volumes ONTAP HA]を選択します。

3. ウィザードの手順に従って、 Cloud Volumes ONTAP システムを起動します。

> ウィザードで選択を行う場合は、**[**サービス**]***で[Data Sense & Compliance]と[Backup to Cloud]を選択しないでください。**[Preconfigured Packages]***で**[Change Configuration]** Only]を選択し、他のオプションが選択されていないことを確認します。事前設定されたパッケージはAWS Secret CloudリージョンとTop Secret Cloudリージョンではサポートされておらず、選択するとデプロイに失敗します。

複数のアベイラビリティゾーンに**Cloud Volumes ONTAP HA**を導入する場合の注意事項

HAペアのウィザードを実行する際は、次の点に注意してください。

- 複数のアベイラビリティゾーン（AZ）にCloud Volumes ONTAP HAを導入する場合は、トランジットゲートウェイを設定する必要があります。を参照してください "AWS 転送ゲートウェイを設定します"。
- 公開時点でAWS Top Secret Cloudで利用可能なAZは2つしかなかったため、次のように構成を導入します。
  - ノード 1 ：アベイラビリティゾーン A
  - ノード 2 ：アベイラビリティゾーン B
  - メディエーター：アベイラビリティゾーン A または B

シングルノードと**HA**ノードの両方に**Cloud Volumes ONTAP**を導入する場合の注意事項

ウィザードを完了する際には、次の点に注意してください。

- 生成されたセキュリティグループを使用するには、デフォルトのオプションをそのままにしておく必要があります。

  事前定義されたセキュリティグループには、 Cloud Volumes ONTAP が正常に動作するために必要なルールが含まれています。独自の要件がある場合は、下のセキュリティグループのセクションを参照してください。

- AWS 環境の準備の際に作成した IAM ロールを選択する必要があります。
- 基盤となる AWS ディスクタイプは Cloud Volumes ONTAP の初期ボリューム用です。

  以降のボリュームでは、別のディスクタイプを選択できます。

- AWS ディスクのパフォーマンスはディスクサイズに依存します。

  必要なパフォーマンスを継続的に提供するディスクサイズを選択する必要があります。EBS のパフォーマンスの詳細については、 AWS のドキュメントを参照してください。

- ディスクサイズは、システム上のすべてのディスクのデフォルトサイズです。

  あとでサイズを変更する必要がある場合は、 Advanced allocation オプションを使用して、特定のサイズのディスクを使用するアグリゲートを作成できます。

結果

Cloud Volumes ONTAP インスタンスが起動します。タイムラインで進行状況を追跡できます。

手順**8**：データ階層化用のセキュリティ証明書をインストールする

AWS Secret CloudリージョンとTop Secret Cloudリージョンでデータの階層化を有効にするには、セキュリティ証明書を手動でインストールする必要があります。

作業を開始する前に

1. S3 バケットを作成する。

   バケット名の先頭にが付いていることを確認します。 `fabric-pool-`. 例えば `fabric-pool-testbucket`。

2. インストールしたルート証明書を保持します。 `step 4` 便利です。

手順

1. にインストールしたルート証明書からテキストをコピーします。 `step 4`。
2. CLIを使用してCloud Volumes ONTAPシステムにセキュアに接続します。
3. ルート証明書をインストールします。必要に応じて、 `ENTER` 複数回キーを押す：

```
security certificate install -type server-ca -cert-name <certificate-
name>
```

4. プロンプトが表示されたら、コピーしたテキスト全体を入力します。 `----- BEGIN CERTIFICATE -----` 終了： `----- END CERTIFICATE -----`。
5. あとで参照できるように、CA署名デジタル証明書のコピーを保管しておいてください。
6. CA名と証明書のシリアル番号は保持します。
7. AWS Secret CloudリージョンとTop Secret Cloudリージョン用のオブジェクトストアを設定します。 `set -privilege advanced -confirmations off`
8. オブジェクトストアを設定するには、このコマンドを実行します。

> すべてのAmazonリソース名（ARN）にサフィックスを付加 `-iso-b`など `arn:aws-iso-b`。たとえば、リソースにリージョンを含むARNが必要な場合、Top Secret Cloudには という命名規則を使用します。 `us-iso-b` をクリックします `-server` フラグ。AWS Secret Cloudの場合は `us-iso-b-1`。

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. オブジェクトストアが作成されたことを確認します。 `storage aggregate object-store show -instance`
10. オブジェクトストアをアグリゲートに接続します。この処理は、新しいアグリゲートごとに繰り返す必要があります。 `storage aggregate object-store attach -aggregate <aggr1> -object -store-name <S3Bucket>`

Microsoft Azure で利用を開始しましょう

Azure での Cloud Volumes ONTAP のクイックスタート

いくつかの手順で、 Cloud Volumes ONTAP for Azure を使い始めましょう。

1 コネクタを作成します

を持っていなければ "コネクタ" ただし、アカウント管理者がアカウントを作成する必要があります。 "Azure でコネクタを作成する方法について説明します"

インターネットアクセスを使用できないサブネットにCloud Volumes ONTAP を導入する場合は、コネクタを手動でインストールし、そのコネクタで実行されているBlueXPユーザインターフェイスにアクセスする必要があります。 "インターネットにアクセスできない場所にコネクタを手動でインストールする方法について説明します"

構成を計画

BlueXPでは、ワークロード要件に合わせて事前設定されたパッケージを提供しています。また、独自の構成を作成することもできます。独自の設定を選択する場合は、使用可能なオプションを理解しておく必要があります。 "詳細はこちら。"。

ネットワークをセットアップします

1. VNet とサブネットがコネクタと Cloud Volumes ONTAP 間の接続をサポートすることを確認します。
2. ターゲットVPCからのアウトバウンドのインターネットアクセスをNetApp AutoSupport で有効にします。

   インターネットにアクセスできない場所にCloud Volumes ONTAP を導入する場合は、この手順は必要ありません。

"ネットワーク要件の詳細については、こちらをご覧ください"。

BlueXPを使用して**Cloud Volumes ONTAP** を起動します

[作業環境の追加] をクリックし、展開するシステムのタイプを選択して、ウィザードの手順を実行します。 "詳細な手順を参照してください"。

関連リンク

- "BlueXPからコネクタを作成しています"
- "Azure Marketplace からコネクタを作成する"
- "Linux ホストへの Connector ソフトウェアのインストール"
- "BlueXPが権限を持って実行できること"

AzureでCloud Volumes ONTAP 構成を計画

Azure で Cloud Volumes ONTAP を導入する場合は、ワークロード要件に一致する事前設定済みのシステムを選択するか、または独自の設定を作成できます。独自の設定を選択する場合は、使用可能なオプションを理解しておく必要があります。

Cloud Volumes ONTAP ライセンスを選択します

Cloud Volumes ONTAP には、いくつかのライセンスオプションがあります。それぞれのオプションで、ニーズに合った消費モデルを選択できます。

- "Cloud Volumes ONTAP のライセンスオプションについて説明します"
- "ライセンスの設定方法について説明します"

サポートされているリージョンを選択します

Cloud Volumes ONTAP は、ほとんどの Microsoft Azure リージョンでサポートされています。 "サポートされているリージョンの完全なリストを表示します"。

サポートされている**VM**タイプを選択してください

Cloud Volumes ONTAP では、選択したライセンスタイプに応じて、複数の VM タイプがサポートされます。

"Azure で Cloud Volumes ONTAP がサポートされている構成"

ストレージの制限を確認

Cloud Volumes ONTAP システムの未フォーマット時の容量制限は、ライセンスに関連付けられています。追加の制限は、アグリゲートとボリュームのサイズに影響します。設定を計画する際には、これらの制限に注意する必要があります。

"Azure での Cloud Volumes ONTAP のストレージの制限"

Azureでシステムのサイズを設定します

Cloud Volumes ONTAP システムのサイジングを行うことで、パフォーマンスと容量の要件を満たすのに役立ちます。VM タイプ、ディスクタイプ、およびディスクサイズを選択する際には、次の点に注意してください。

仮想マシンのタイプ

でサポートされている仮想マシンタイプを確認します "Cloud Volumes ONTAP リリースノート" サポートされている各 VM タイプの詳細を確認します。各 VM タイプがサポートするデータディスクの数には制限があることに注意してください。

- "Azure のドキュメント：「汎用仮想マシンのサイズ"
- "Azure のドキュメント：「 Memory optimized virtual machine sizes"

シングルノードシステムの**Azure**ディスクタイプ

Cloud Volumes ONTAP 用のボリュームを作成する場合は、 ONTAP がディスクとして使用する基盤となるクラウドストレージを選択する必要があります。

シングルノードシステムでは、次の 3 種類の Azure Managed Disks を使用できます。

- _Premium SSD Managed Disks （プレミアム SSD 管理ディスク） - I/O 負荷の高いワークロードに高パフォーマンスを提供し、コストを高めます。
- _ 標準 SSD 管理ディスク _ 低 IOPS を必要とするワークロードに一貫したパフォーマンスを提供します。
- _Standard HDD Managed Disks_are a good choice if you need high iops and want to Reduce your costs （高 IOPS が必要なく、コストを削減したい場合に最適です。）

これらのディスクのユースケースの詳細については、を参照してください "Microsoft Azure のドキュメント：「 What disk types are available in Azure ？」"。

Azureの**HA**ペア構成のディスクタイプ

HAシステムでは、Premium SSD Shared Managed Disksを使用して、I/O負荷の高いワークロードのパフォーマンスを高コストで実現します。9.12.1リリースより前に作成されたHA配置では、Premiumページブロブが使用されます。

Azure のディスクサイズ

Cloud Volumes ONTAP インスタンスを起動するときは、アグリゲートのデフォルトのディスクサイズを選択する必要があります。BlueXPでは、このディスクサイズを最初のアグリゲート、およびシンプルなプロビジョニングオプションを使用したときに作成される追加のアグリゲートに使用します。別のディスクサイズを使用するアグリゲートを作成できます デフォルトでは、です "高度な割り当てオプションを使用する"。

アグリゲート内のディスクはすべて同じサイズである必要があります。

ディスクサイズを選択する際には、いくつかの要素を考慮する必要があります。ディスクサイズは、ストレージのコスト、アグリゲートに作成できるボリュームのサイズ、 Cloud Volumes ONTAP で使用可能な総容量、ストレージパフォーマンスに影響します。

Azure Premium ストレージのパフォーマンスは、ディスクサイズに依存します。ディスク容量が大きいほど、 IOPS とスループットが向上します。たとえば、 1 TiB のディスクを選択すると、 500 GiB のディスクよりも高いパフォーマンスを低コストで実現できます。

標準ストレージのディスクサイズにはパフォーマンスの違いはありません。必要な容量に基づいてディスクサイズを選択する必要があります。

ディスクサイズ別の IOPS とスループットについては、 Azure を参照してください。

- "Microsoft Azure ： Managed Disks の価格"
- "Microsoft Azure ： Page Blob の価格設定"

デフォルトのシステムディスクを表示します

ユーザデータ用のストレージに加えて、BlueXPはCloud Volumes ONTAP システムデータ（ブートデータ、ルートデータ、コアデータ、NVRAM）用のクラウドストレージも購入します。計画を立てる場合は、 Cloud Volumes ONTAP を導入する前にこれらの詳細を確認すると役立つ場合があります。

"Azure で、 Cloud Volumes ONTAP システムデータのデフォルトディスクを表示します"。

コネクタにはシステムディスクも必要です。 "コネクタのデフォルト設定に関する詳細を表示します"。

ネットワーク情報を収集

Cloud Volumes ONTAP を Azure に導入する場合は、仮想ネットワークの詳細を指定する必要があります。ワークシートを使用して、管理者から情報を収集できます。

Azure の情報	あなたの価値
地域	
仮想ネットワーク（ Vnet ）	
サブネット	
Network Security Group （独自のグループを使用している場合）	

書き込み速度を選択します

BlueXPでは、Cloud Volumes ONTAP の書き込み速度設定を選択できます。書き込み速度を選択する前に、高速書き込みを使用する場合の標準設定と高設定の違い、およびリスクと推奨事項を理解しておく必要があります。 "書き込み速度の詳細については、こちらをご覧ください。"。

ボリュームの使用プロファイルを選択してください

ONTAP には、必要なストレージの合計容量を削減できるストレージ効率化機能がいくつか搭載されています。BlueXPでボリュームを作成するときに、これらの機能を有効にするプロファイル、または無効にするプロファイルを選択できます。これらの機能の詳細については、使用するプロファイルを決定する際に役立ちます。

NetApp Storage Efficiency 機能には、次のようなメリットがあります。

シンプロビジョニング

物理ストレージプールよりも多くの論理ストレージをホストまたはユーザに提供します。ストレージスペースは、事前にストレージスペースを割り当てる代わりに、データの書き込み時に各ボリュームに動的に割り当てられます。

重複排除

同一のデータブロックを検索し、単一の共有ブロックへの参照に置き換えることで、効率を向上します。この手法では、同じボリュームに存在するデータの冗長ブロックを排除することで、ストレージ容量の要件を軽減します。

圧縮

プライマリ、セカンダリ、アーカイブストレージ上のボリューム内のデータを圧縮することで、データの格納に必要な物理容量を削減します。

Azure の Cloud Volumes ONTAP のネットワーク要件

Cloud Volumes ONTAP システムが適切に動作するように Azure ネットワークをセットアップします。

Cloud Volumes ONTAP の要件

Azure では、次のネットワーク要件を満たしている必要があります。

アウトバウンドインターネットアクセス

Cloud Volumes ONTAP ノードには、NetApp AutoSupport へのアウトバウンドインターネットアクセスが必要です。ネットアップは、システムの健常性をプロアクティブに監視し、ネットアップテクニカルサポートにメッセージを送信します。

Cloud Volumes ONTAP が AutoSupport メッセージを送信できるように、ルーティングポリシーとファイアウォールポリシーで次のエンドポイントへの HTTP / HTTPS トラフィックを許可する必要があります。

- \ https://support.netapp.com/aods/asupmessage
- \ https://support.netapp.com/asupprod/post/1.0/postAsup

AutoSupport メッセージの送信にアウトバウンドのインターネット接続が使用できない場合、Cloud Volumes

ONTAP システムは自動的にコネクタをプロキシサーバとして使用するように設定されます。唯一の要件は、コネクタのセキュリティグループがポート3128で_ inbound_connectionsを許可することです。コネクタを展開した後、このポートを開く必要があります。

Cloud Volumes ONTAP に厳密なアウトバウンドルールを定義した場合は、Cloud Volumes ONTAP セキュリティグループがポート3128で_OUTBOUND接続を許可する必要もあります。

アウトバウンドのインターネットアクセスが使用可能であることを確認したら、 AutoSupport をテストしてメッセージを送信できることを確認します。手順については、を参照してください "ONTAP のドキュメント：「 AutoSupport のセットアップ"。

AutoSupport メッセージを送信できないことがBlueXPから通知された場合は、 "AutoSupport 構成のトラブルシューティングを行います"。

IP アドレス

BlueXPは、必要な数のプライベートIPアドレスを自動的にAzureのCloud Volumes ONTAP に割り当てます。ネットワークに利用可能な十分な数のプライベートIPアドレスがあることを確認する必要があります。

Cloud Volumes ONTAP 用に割り当てられるLIFの数は、シングルノードシステムとHAペアのどちらを導入するかによって異なります。LIF は、物理ポートに関連付けられた IP アドレスです。SnapCenter などの管理ツールには、 SVM 管理 LIF が必要です。

> iSCSI LIFは、iSCSIプロトコルを介したクライアントアクセスを提供し、システムがその他の重要なネットワークワークフローに使用します。これらのLIFは必須であり、削除しないでください。

シングルノードシステムの IP アドレス

BlueXPは'1つのノードシステムに5つまたは6つのIPアドレスを割り当てます

- クラスタ管理IP
- ノード管理IP
- SnapMirror用のクラスタ間IP
- NFS / CIFS IP
- iSCSI IP

> iSCSI IPは、iSCSIプロトコルを使用したクライアントアクセスを提供します。システムでは、その他の重要なネットワークワークフローにも使用されます。このLIFは必須であり、削除することはできません。

- SVMの管理（オプション-デフォルトでは設定されていません）

HA ペアの IP アドレス

BlueXPでは、導入時に1ノードあたり4 NICにIPアドレスが割り当てられています。

BlueXPでは、HAペアにSVM管理LIFが作成されますが、Azureのシングルノードシステムには作成されません。

- NIC0 *
- ノード管理IP
- クラスタ間IP
- iSCSI IP

> iSCSI IPは、iSCSIプロトコルを使用したクライアントアクセスを提供します。システムでは、その他の重要なネットワークワークフローにも使用されます。このLIFは必須であり、削除することはできません。

- NIC1 *
- クラスタネットワークIP
- NIC2 *
- クラスタインターコネクトIP（HA IC）

NIC3

- Pageblob NIC IP (ディスクアクセス)

> NIC3は、ページBLOBストレージを使用するHA環境にのみ適用できます。

上記のIPアドレスは、フェイルオーバーイベントの際に移行されません。

また、4つのフロントエンドIP（FIPS）がフェイルオーバーイベント時に移行するように設定されています。これらのフロントエンドIPはロードバランサに存在します。

- クラスタ管理IP
- nodeAデータIP（NFS / CIFS）
- nodeBデータIP（NFS / CIFS）
- SVM管理IP

Azure サービスへのセキュアな接続

BlueXPでは、Cloud Volumes ONTAP とAzureページBLOBストレージアカウント間の接続用にAzure Private Linkがデフォルトで有効になっています。

ほとんどの場合、必要な操作は何もありません。BlueXPはAzure Private Linkを管理します。ただし、 Azure プライベート DNS を使用している場合は、構成ファイルを編集する必要があります。また、Azureのコネクタの場所に関する要件も把握しておく必要があります。

ビジネスニーズに応じて、プライベートリンク接続を無効にすることもできます。リンクを無効にすると、Cloud Volumes ONTAP はサービスエンドポイントを使用するように設定されます。

"Azureプライベートリンクまたはサービスエンドポイントでの Cloud Volumes ONTAP を使用する方法の詳細については、こちらをご覧ください"。

他の **ONTAP** システムへの接続

Azure内のCloud Volumes ONTAP システムと他のネットワーク内のONTAP システム間でデータをレプリケートするには、企業ネットワークなど、Azure VNetとその他のネットワーク間にVPN接続が必要です。

手順については、を参照してください "Microsoft Azure のドキュメント：「 Create a Site-to-Site connection in the Azure portal"。

HA インターコネクトのポート

Cloud Volumes ONTAP HA ペアには HA インターコネクトが含まれています。 HA インターコネクトを使用すると、各ノードはパートナーが機能しているかどうかを継続的に確認し、パートナーの不揮発性メモリのログデータをミラーリングできます。HA インターコネクトは、通信に TCP ポート 10006 を使用します。

デフォルトでは、 HA インターコネクト LIF 間の通信は開いており、このポートにはセキュリティグループのルールはありません。ただし、 HA インターコネクト LIF の間にファイアウォールを作成する場合は、 HA ペアが適切に動作するように、ポート 10006 の TCP トラフィックが開いていることを確認する必要があります。

Azure リソースグループには **HA** ペアが **1** つしかありません

Azure に導入する Cloud Volumes ONTAP HA ペアごとに、 _dedicated_resource グループを使用する必要があります。リソースグループでサポートされる HA ペアは 1 つだけです。

Azureリソースグループに2つ目のCloud Volumes ONTAP HAペアを導入しようとすると、接続の問題が発生します。

セキュリティグループのルール

BlueXPでは、Cloud Volumes ONTAP が正常に動作するために必要なインバウンドとアウトバウンドのルールを含むAzureセキュリティグループが作成されます。テスト目的または独自のセキュリティグループを使用する場合は、ポートを参照してください。

Cloud Volumes ONTAP のセキュリティグループには、インバウンドルールとアウトバウンドルールの両方が必要です。

コネクタに関する情報をお探しですか？ "コネクタのセキュリティグループルールを表示します"

シングルノードシステムのインバウンドルール

作業環境を作成し、事前定義されたセキュリティグループを選択する場合、次のいずれかの範囲内でトラフィックを許可するように選択できます。

- 選択した**VNet**のみ：インバウンドトラフィックのソースは、Cloud Volumes ONTAP システムのVNetのサブネット範囲およびコネクタが存在するVNetのサブネット範囲です。これが推奨されるオプションです。
- *すべてのVNet *：インバウンドトラフィックの送信元は0.0.0.0/0のIP範囲です。

優先順位と名前	ポートおよびプロトコル	ソースとデスティネーションの **2** つです	説明
1000 inbound_ssh	22 TCP	Any から Any	クラスタ管理 LIF またはノード管理 LIF の IP アドレスへの SSH アクセス
1001 INBOUND _http	80 TCP	Any から Any	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTP アクセス
1002 INBOUND _111_TCP	111 TCP	Any から Any	NFS のリモートプロシージャコール
1003 INBONED_111_UDP	111 UDP	Any から Any	NFS のリモートプロシージャコール
1004 INBOUND _139	139 TCP	Any から Any	CIFS の NetBIOS サービスセッション
1005 inbound_161-162_TCP	161-162 TCP	Any から Any	簡易ネットワーク管理プロトコル
1006 INBOUND _161-162_UDP	UDP 161-162	Any から Any	簡易ネットワーク管理プロトコル
1007 INBOUND _443	443 tcp	Any から Any	コネクタへの接続と、クラスタ管理LIFのIPアドレスを使用したSystem Manager Webコンソールへの HTTPSアクセス
1008 INBOUND _445	445 TCP	Any から Any	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
1009 INBOUND _635_TCP	635 TCP	Any から Any	NFS マウント
1010 INBOUND _635_UDP	635 UDP	Any から Any	NFS マウント
1011 INBOUND _749	749 TCP	Any から Any	Kerberos
1012 INBOUND _2049 _TCP	2049 TCP	Any から Any	NFS サーバデーモン
1013 INBOUND _2049 _UDP	2049 UDP	Any から Any	NFS サーバデーモン
1014 インバウンド _3260	3260 TCP	Any から Any	iSCSI データ LIF を介した iSCSI アクセス
1015 INBOUND _4045-4046_tcp の略	4045-4046 TCP	Any から Any	NFS ロックデーモンとネットワークステータスモニタ
1016 INBOUND _4045-4046_UDP	4045-4046 UDP	Any から Any	NFS ロックデーモンとネットワークステータスモニタ

優先順位と名前	ポートおよびプロトコル	ソースとデスティネーションの **2** つです	説明
1017 INBOUND _10000	10000 TCP	Any から Any	NDMP を使用したバックアップ
1018 INBOUND _11104-11105	11104-11105 TCP	Any から Any	SnapMirror によるデータ転送
3000 inbound_deny_all_tcp	任意のポート TCP	Any から Any	他のすべての TCP インバウンドトラフィックをブロックします
3001 INBOUND _DENY_ALL_UDP	任意のポート UDP	Any から Any	他のすべての UDP 着信トラフィックをブロックします
65000 AllowVnetInBound	任意のポート任意のプロトコル	VirtualNetwork	VNet 内からのインバウンドトラフィック
65001 AllowAzureLoad BalancerInBound の略	任意のポート任意のプロトコル	AzureLoadBalancer を任意のに設定します	Azure Standard Load Balancer からのデータトラフィック
65500 DenyAllInBound	任意のポート任意のプロトコル	Any から Any	他のすべてのインバウンドトラフィックをブロックする

HA システムのインバウンドルール

作業環境を作成し、事前定義されたセキュリティグループを選択する場合、次のいずれかの範囲内でトラフィックを許可するように選択できます。

- 選択した**VNet**のみ：インバウンドトラフィックのソースは、Cloud Volumes ONTAP システムのVNetのサブネット範囲およびコネクタが存在するVNetのサブネット範囲です。これが推奨されるオプションです。
- *すべてのVNet *：インバウンドトラフィックの送信元は0.0.0.0/0のIP範囲です。

HA システムのインバウンドデータトラフィックは Azure Standard Load Balancer を経由するため、シングルノードシステムよりもインバウンドルールが少なくなります。そのため、「 AllowAzureLoadBalancerInBound 」ルールに示されているように、ロードバランサからのトラフィックがオープンである必要があります。

優先順位と名前	ポートおよびプロトコル	ソースとデスティネーションの **2** つです	説明
100 インバウンド _ 443	443 ：任意のプロトコル	Any から Any	コネクタへの接続と、クラスタ管理LIFのIPアドレスを使用したSystem Manager Webコンソールへの HTTPSアクセス
101 INBOUND _111_TCP	111 すべてのプロトコル	Any から Any	NFS のリモートプロシージャコール
102 インバウンド _2049 _TCP	2049 任意のプロトコル	Any から Any	NFS サーバデーモン

優先順位と名前	ポートおよびプロトコル	ソースとデスティネーションの **2** つです	説明
111 inbound_ssh	22 すべてのプロトコル	Any から Any	クラスタ管理 LIF またはノード管理 LIF の IP アドレスへの SSH アクセス
121 INBOUND _53	53 任意のプロトコル	Any から Any	DNS と CIFS
65000 AllowVnetInBound	任意のポート任意のプロトコル	VirtualNetwork	VNet 内からのインバウンドトラフィック
65001 AllowAzureLoad BalancerInBound の略	任意のポート任意のプロトコル	AzureLoadBalancer を任意のに設定します	Azure Standard Load Balancer からのデータトラフィック
65500 DenyAllInBound	任意のポート任意のプロトコル	Any から Any	他のすべてのインバウンドトラフィックをブロックする

アウトバウンドルール

Cloud Volumes 用の事前定義済みセキュリティグループ ONTAP は、すべての発信トラフィックをオープンします。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

Cloud Volumes ONTAP 用の定義済みセキュリティグループには、次のアウトバウンドルールが含まれています。

ポート	プロトコル	目的
すべて	すべての TCP	すべての発信トラフィック
すべて	すべての UDP	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、 Cloud Volumes ONTAP による発信通信に必要なポートのみを開くことができます。

source は、 Cloud Volumes ONTAP システムのインターフェイス（ IP アドレス）です。

サービス	ポート	プロトコル	ソース	宛先	目的
Active Directory	88	TCP	ノード管理 LIF	Active Directory フォレスト	Kerberos V 認証
	137	UDP	ノード管理 LIF	Active Directory フォレスト	NetBIOS ネームサービス
	138	UDP	ノード管理 LIF	Active Directory フォレスト	NetBIOS データグラムサービス
	139	TCP	ノード管理 LIF	Active Directory フォレスト	NetBIOS サービスセッション
	389	TCP および UDP	ノード管理 LIF	Active Directory フォレスト	LDAP
	445	TCP	ノード管理 LIF	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	464	TCP	ノード管理 LIF	Active Directory フォレスト	Kerberos V パスワードの変更と設定（ SET_CHANGE ）
	464	UDP	ノード管理 LIF	Active Directory フォレスト	Kerberos キー管理
	749	TCP	ノード管理 LIF	Active Directory フォレスト	Kerberos V Change & Set Password （ RPCSEC_GSS ）
	88	TCP	データ LIF （ NFS 、 CIFS 、 iSCSI ）	Active Directory フォレスト	Kerberos V 認証
	137	UDP	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS ネームサービス
	138	UDP	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS データグラムサービス
	139	TCP	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS サービスセッション
	389	TCP および UDP	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	LDAP
	445	TCP	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	464	TCP	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	Kerberos V パスワードの変更と設定（ SET_CHANGE ）
	464	UDP	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	Kerberos キー管理
	749	TCP	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	Kerberos V Change & Set Password （ RPCSEC_GSS ）

サービス	ポート	プロトコル	ソース	宛先	目的
AutoSupport	HTTPS	443	ノード管理 LIF	support.netapp.com	AutoSupport （デフォルトは HTTPS ）
	HTTP	80	ノード管理 LIF	support.netapp.com	AutoSupport （転送プロトコルが HTTPS から HTTP に変更された場合のみ）
	TCP	3128	ノード管理 LIF	コネクタ	アウトバウンドのインターネット接続が使用できない場合に、コネクタのプロキシサーバを介してAutoSupport メッセージを送信する
構成のバックアップ	HTTP	80	ノード管理 LIF	http://<connector-IP-address>/occm/offboxconfig	構成バックアップをコネクタに送信します。 "構成バックアップファイルについて説明します"。
DHCP	68	UDP	ノード管理 LIF	DHCP	初回セットアップ用の DHCP クライアント
DHCP	67	UDP	ノード管理 LIF	DHCP	DHCP サーバ
DNS	53	UDP	ノード管理 LIF とデータ LIF （ NFS 、 CIFS ）	DNS	DNS
NDMP	18600 ～ 18699	TCP	ノード管理 LIF	宛先サーバ	NDMP コピー
SMTP	25	TCP	ノード管理 LIF	メールサーバ	SMTP アラート。 AutoSupport に使用できます
SNMP	161	TCP	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	161	UDP	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	162	TCP	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	162	UDP	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
SnapMirror	11104	TCP	クラスタ間 LIF	ONTAP クラスタ間 LIF	SnapMirror のクラスタ間通信セッションの管理
	11105	TCP	クラスタ間 LIF	ONTAP クラスタ間 LIF	SnapMirror によるデータ転送
syslog	514	UDP	ノード管理 LIF	syslog サーバ	syslog 転送メッセージ

コネクタの要件

コネクタをまだ作成していない場合は、コネクタのネットワーク要件も確認してください。

- "コネクタのネットワーク要件を確認します"
- "Azureのセキュリティグループルール"

Azure でお客様が管理するキーを使用するように Cloud Volumes ONTAP を設定します

データは、を使用して Azure の Cloud Volumes ONTAP で自動的に暗号化されます "Azure Storage Service Encryption の略" Microsoft が管理するキーを使用する場合：ただし、このページの手順に従って独自の暗号化キーを使用することもできます。

データ暗号化の概要

Cloud Volumes ONTAP データは、を使用して Azure で自動的に暗号化されます "Azure Storage Service Encryption の略"。デフォルトの実装では、 Microsoft が管理するキーが使用されます。セットアップは必要ありません。

Cloud Volumes ONTAP で顧客管理キーを使用する場合は、次の手順を実行する必要があります。

1. Azure で、キーヴォールトを作成し、そのヴォールトでキーを生成します
2. BlueXPから'APIを使用して'キーを使用するCloud Volumes ONTAP 作業環境を作成します

キーローテーション

キーの新しいバージョンを作成すると、 Cloud Volumes ONTAP では自動的に最新のキーバージョンが使用されます。

データの暗号化方法

BlueXPではディスク暗号化セットを使用します。これにより、ページブロブではなく管理対象ディスクを使用して暗号化キーを管理できます。新しいデータディスクでも同じディスク暗号化セットが使用されます。下位バージョンでは、顧客管理キーの代わりにMicrosoft管理キーが使用されます。

お客様が管理するキーを使用するように設定された Cloud Volumes ONTAP 作業環境を作成すると、 Cloud Volumes ONTAP データは次のように暗号化されます。

Cloud Volumes ONTAP 構成	キーの暗号化に使用されるシステムディスク	キーの暗号化に使用されるデータディスク
シングルノード	• ブート • コア • NVRAM	• root • データ
ページBLOBを含むAzure HA単一アベイラビリティゾーン	• ブート • コア • NVRAM	なし
共有管理対象ディスクを使用するAzure HA単一アベイラビリティゾーン	• ブート • コア • NVRAM	• root • データ

Cloud Volumes ONTAP 構成	キーの暗号化に使用されるシステムディスク	キーの暗号化に使用されるデータディスク
Azure HA：共有管理対象ディスクを使用する複数のアベイラビリティゾーン	• ブート • コア • NVRAM	• root • データ

Cloud Volumes ONTAP 用のすべての Azure ストレージアカウントは、お客様が管理するキーを使用して暗号化されます。作成時にストレージアカウントを暗号化する場合は、CVO作成要求でリソースのIDを作成して指定する必要があります。これは、すべてのタイプの導入に当てはまります。提供しない場合でもストレージアカウントは暗号化されますが、BlueXPはまずMicrosoftが管理するキー暗号化を使用してストレージアカウントを作成し、次にストレージアカウントを更新してお客様が管理するキーを使用するようにします。

ユーザーが割り当てた管理**ID**を作成します

ユーザーが割り当てた管理IDと呼ばれるリソースを作成することもできます。これにより、Cloud Volumes ONTAP作業環境の作成時にストレージアカウントを暗号化できます。キーボールトを作成してキーを生成する前に、このリソースを作成することをお勧めします。

リソースのIDは次のとおりです。 `userassignedidentity`。

手順

1. Azureで、Azureサービスに移動し、* Managed Identities *を選択します。
2. [作成（ Create ）] をクリックします。
3. 次の詳細を入力します。
   - サブスクリプション:サブスクリプションを選択します。コネクタサブスクリプションと同じサブスクリプションを選択することをお勧めします。
   - リソースグループ：既存のリソースグループを使用するか、新しいリソースグループを作成します。
   - リージョン：必要に応じて、コネクタと同じリージョンを選択します。
   - 名前:リソースの名前を入力します。
4. 必要に応じて、タグを追加します。
5. [作成（ Create ）] をクリックします。

キーボールトを作成し、キーを生成します

キーヴォールトは、 Cloud Volumes ONTAP システムを作成するときと同じ Azure サブスクリプションとリージョンに配置する必要があります。

あなたの場合 ユーザーが割り当てた管理IDを作成しました、キーヴォールトの作成時に、キーヴォールトのアクセスポリシーも作成する必要があります。

手順

1. "Azure サブスクリプションでキーヴォールトを作成します"。

   キーヴォールトの次の要件に注意してください。

- キーヴォールトは、 Cloud Volumes ONTAP システムと同じリージョンに配置する必要があります。
- 次のオプションを有効にする必要があります。
  - * Soft -delete *（このオプションはデフォルトで有効ですが、 DISABLE_NOT BE 無効にする必要があります）
  - * パージ保護 *
  - * Azure Disk Encryption for Volume Encryption *（シングルノードシステムの場合、または複数のゾーンのHAペアの場合）
- ユーザが割り当てた管理IDを作成した場合は、次のオプションを有効にする必要があります。
  - バックアップアクセスポリシー

2. バックアップアクセスポリシーを選択した場合は、[作成]をクリックしてキーバックアップのアクセスポリシーを作成します。そうでない場合は、手順3に進みます。
   a. 次の権限を選択します。
      - 取得
      - リスト
      - 復号化します
      - 暗号化
      - キーのラップを解除します
      - ラップキー
      - 検証
      - サインだ
   b. ユーザーが割り当てた管理ID（リソース）をプリンシパルとして選択します。
   c. アクセスポリシーを確認して作成します。
3. "キーボールトでキーを生成します"。

   キーに関する次の要件に注意してください。

   - キータイプは * rsa * である必要があります。
   - 推奨される RSA キー・サイズは **2048** ですが、それ以外のサイズもサポートされます。

暗号化キーを使用する作業環境を作成します

キーヴォールトを作成して暗号化キーを生成したら、そのキーを使用するように設定した新しい Cloud Volumes ONTAP システムを作成できます。これらの手順は、BlueXP APIを使用してサポートされています。

必要な権限

シングルノードのCloud Volumes ONTAP システムで顧客管理キーを使用する場合は、BlueXP Connectorに次の権限があることを確認します。

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"権限の最新のリストを表示します"

手順

1. 次のBlueXP API呼び出しを使用して、Azureサブスクリプション内の主要なボルトのリストを取得します。

   HA ペアの場合：「 GET /azure-ha/ma/metadata/vaults 」

   シングルノードの場合：「 GET /azure-vsa/metadata/vaults 」

   - name * および * resourcegroup * をメモします。次の手順でこれらの値を指定する必要があります。

   "この API 呼び出しの詳細を確認してください"。

2. 次のBlueXP API呼び出しを使用して、ボルト内のキーのリストを取得します。

   HA ペアの場合：「 GET /azure-ha/ma/metadata/keys - vault 」

   シングルノードの場合：「 get/azure-vsa/metadata/keys - vault 」

   - keyName * をメモします。次のステップで、その値（ボルト名とともに）を指定する必要があります。

   "この API 呼び出しの詳細を確認してください"。

3. 次のBlueXP API呼び出しを使用してCloud Volumes ONTAP システムを作成します

   a. HA ペアの場合：

      「 POST/Azure/HA/ 作業環境」

      要求の本文には次のフィールドを含める必要があります。

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

      を含めます "userAssignedIdentity": " userAssignedIdentityId" フィールド：ストレージアカウントの暗号化に使用するリソースを作成した場合。

"この API 呼び出しの詳細を確認してください"。

b. シングルノードシステムの場合：

「 POST/Azure/VSA/Working-Environments 」

要求の本文には次のフィールドを含める必要があります。

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

を含めます "userAssignedIdentity": " userAssignedIdentityId" フィールド：ストレージアカウントの暗号化に使用するリソースを作成した場合。

"この API 呼び出しの詳細を確認してください"。

結果

新しい Cloud Volumes ONTAP システムで、お客様が管理するキーを使用してデータを暗号化するように設定しておきます。

AzureでCloud Volumes ONTAP のライセンスをセットアップする

Cloud Volumes ONTAP で使用するライセンスオプションを決定したら、新しい作業環境を作成する際にそのライセンスオプションを選択する前に、いくつかの手順を実行する必要があります。

フリーミアム

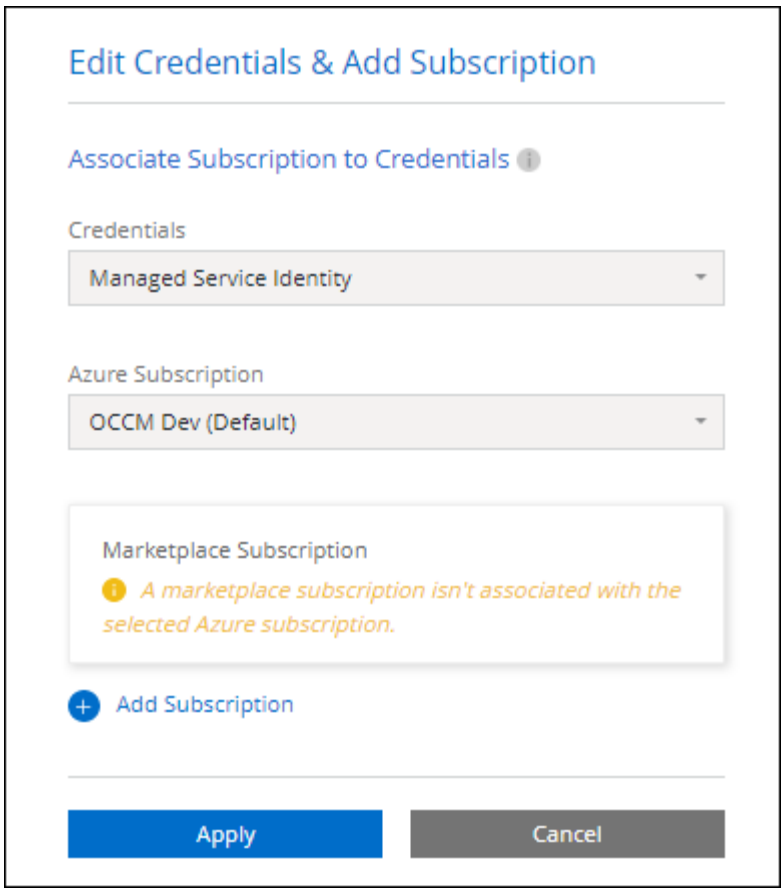
プロビジョニングされた容量が最大500GiBのCloud Volumes ONTAP を無料で使用するには、Freemium製品を選択してください。 "Freemium 製品の詳細をご覧ください"。

手順

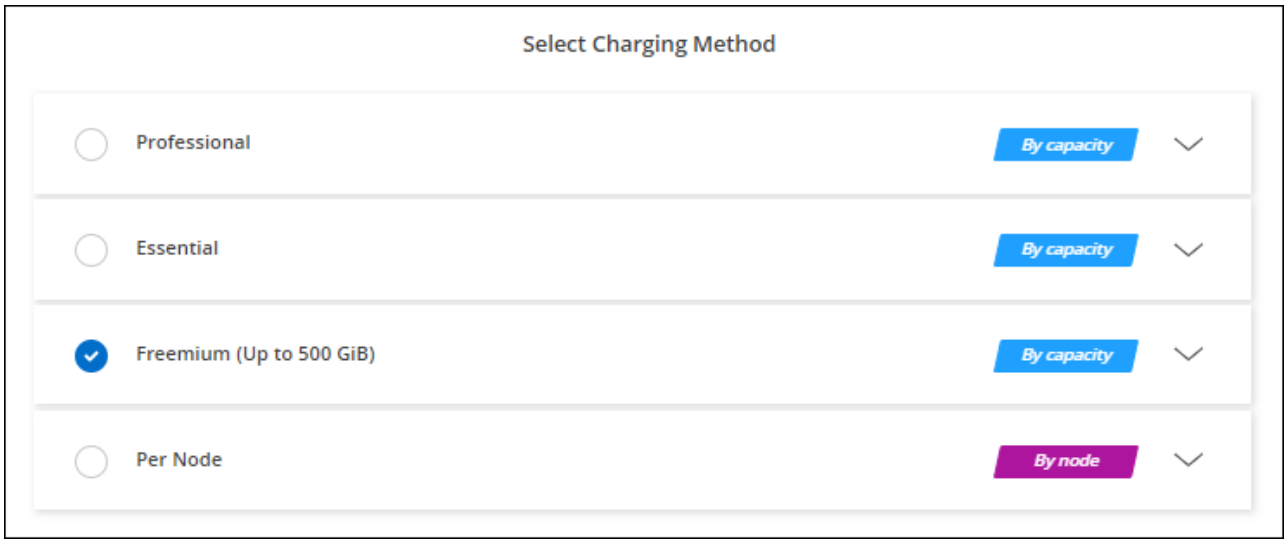
1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。

   a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってAzure Marketplaceで従量課金制サービスに登録します。

      プロビジョニング済み容量が500GiBを超えると、システムはに自動的に変換されないかぎり、マーケットプレイスのサブスクリプションを通じて料金が請求されることはありません "Essentials パッケージ"。



a. BlueXPに戻ったら、充電方法のページにアクセスして「* Freemium *」を選択します。



"ステップバイステップの手順を参照して、AzureでCloud Volumes ONTAP を起動してください"。

容量単位のライセンスです

容量単位のライセンスでは、 TiB 単位の Cloud Volumes ONTAP に対して料金を支払うことができます。容量ベースのライセンスは、パッケージ：Essentialsパッケージまたはプロフェッショナルパッケージの形式で提供されます。

Essentials パッケージと Professional パッケージには、次の消費モデルがあります。

- ネットアップから購入したライセンス（ BYOL ）
- Azure Marketplaceからの従量課金制（PAYGO）単位のサブスクリプション
- 年間契約

"容量単位のライセンスに関する詳細は、こちらをご覧ください"。

以降のセクションでは、これらの各消費モデルの使用方法について説明します。

BYOL

ネットアップからライセンスを購入（BYOL）して前払いし、任意のクラウドプロバイダにCloud Volumes ONTAP システムを導入できます。

手順

1. "ライセンスの取得については、ネットアップの営業部門にお問い合わせください"
2. "NetApp Support Site アカウントをBlueXPに追加します"

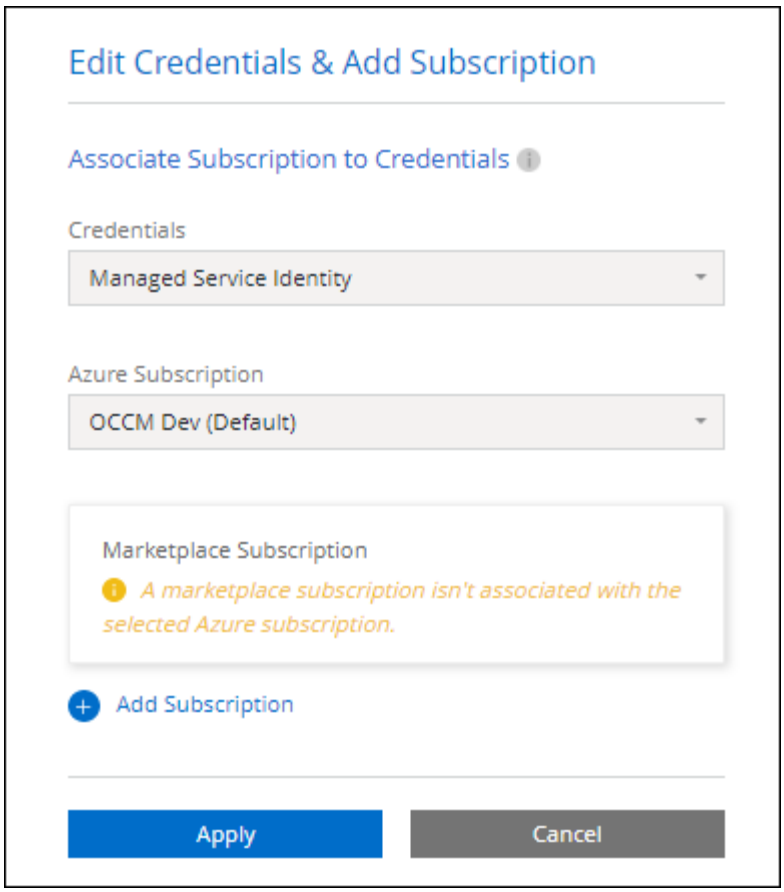
   BlueXPは、ネットアップのライセンスサービスを自動的に照会し、NetApp Support Site アカウントに関連付けられているライセンスの詳細を取得します。エラーがなければ、BlueXPは自動的にライセンスをデジタルウォレットに追加します。

   Cloud Volumes ONTAP でライセンスを使用するには、事前にBlueXPデジタルウォレットからライセンスを入手しておく必要があります。必要に応じて、を実行できます "ライセンスをBlueXPデジタルウォレットに手動で追加します"。

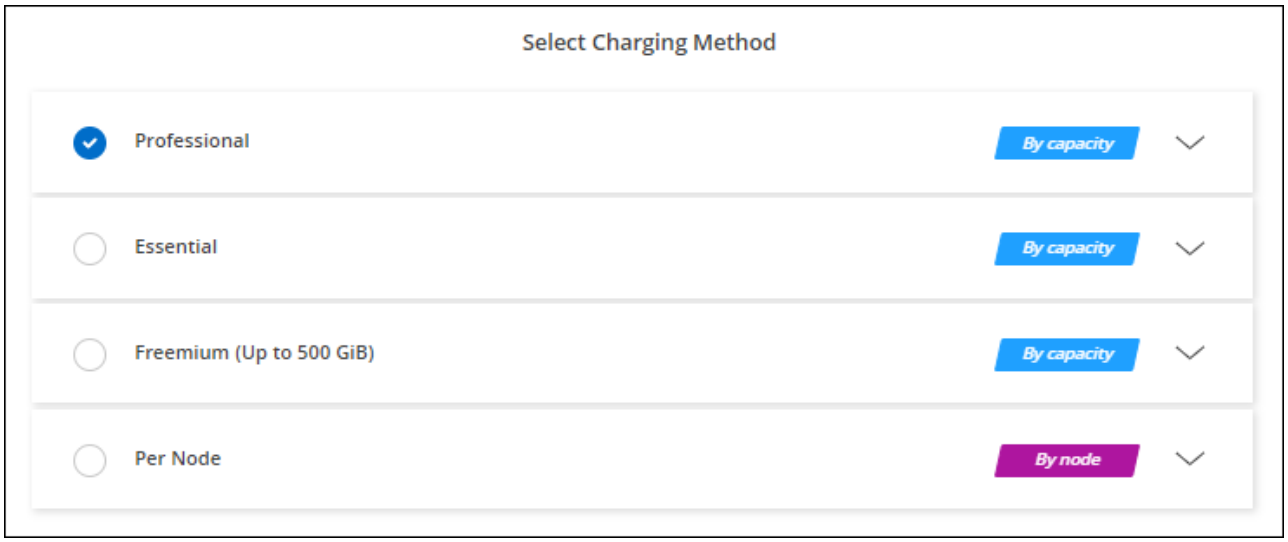
3. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。

   a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってAzure Marketplaceで従量課金制サービスに登録します。

      ネットアップから購入したライセンスには、最初に必ず料金が請求されますが、ライセンスで許可された容量を超えた場合や、ライセンスの期間が終了した場合は、マーケットプレイスで1時間ごとに料金が請求されます。



a. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



"ステップバイステップの手順を参照して、AzureでCloud Volumes ONTAP を起動してください"。

PAYGOサブスクリプション

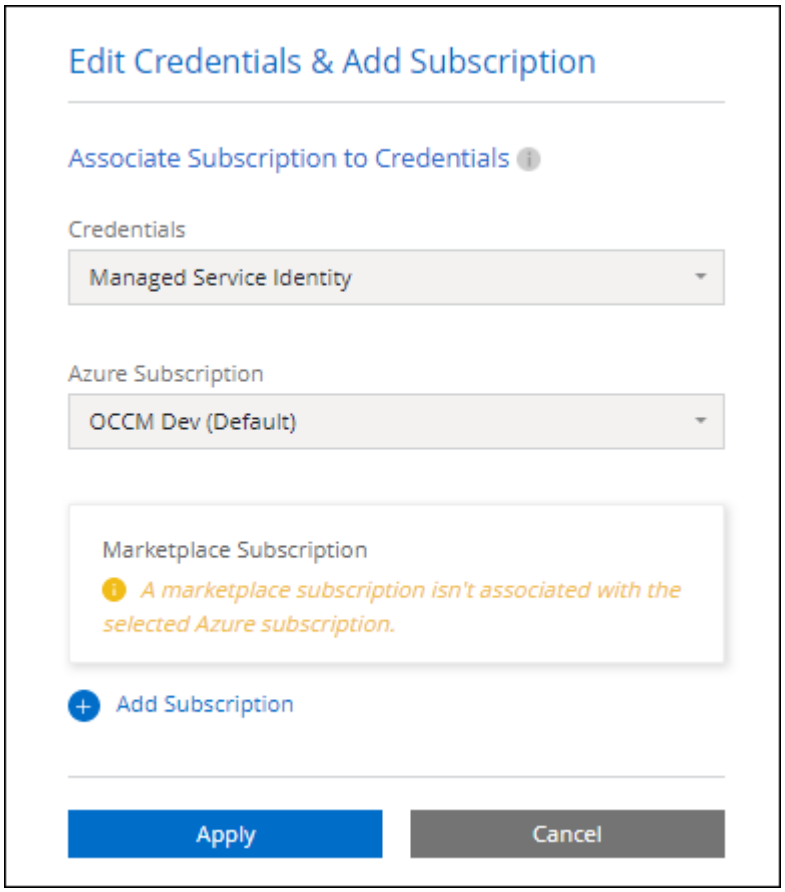
クラウドプロバイダのマーケットプレイスから提供されたサービスに登録すると、1時間ごとに料金が発生します。

Cloud Volumes ONTAP 作業環境を作成すると、Azure Marketplaceで提供されている契約に登録するよう求め

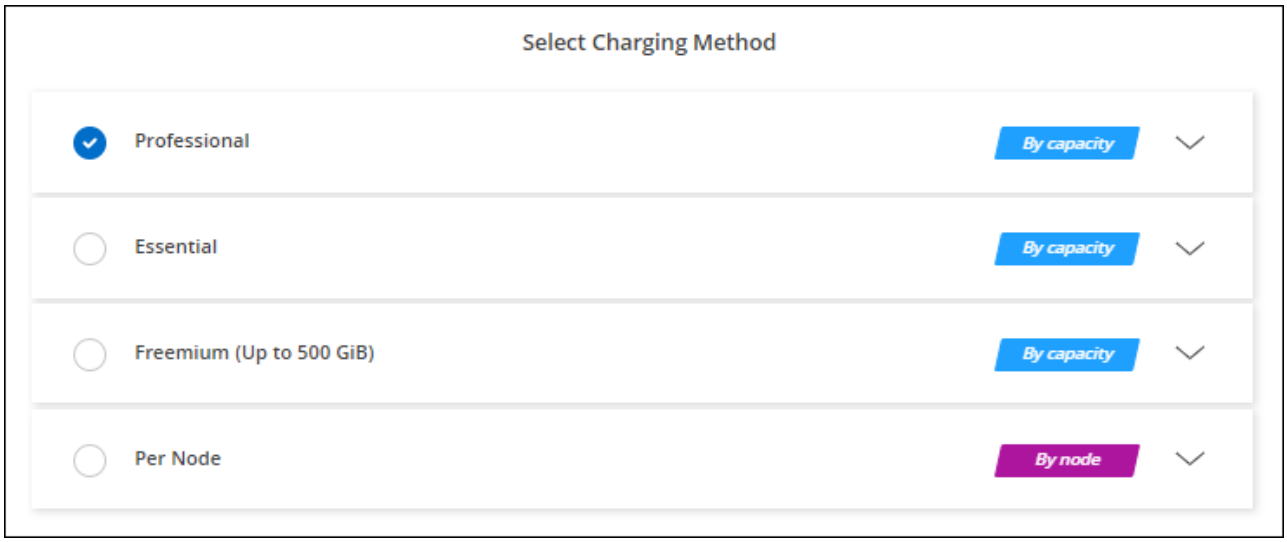
られます。このサブスクリプションは、充電のための作業環境に関連付けられます。同じサブスクリプションを追加の作業環境に使用できます。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってAzure Marketplaceで従量課金制サービスに登録します。



   b. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



"ステップバイステップの手順を参照して、AzureでCloud Volumes ONTAP を起動してください"。

Azureアカウントに関連付けられたAzure Marketplaceのサブスクリプションを管理するには、[設定]>[クレデンシャル]ページを使用します。 "Azureのアカウントとサブスクリプションの管理方法について説明します"

年間契約

年間契約を購入することで、Cloud Volumes ONTAP の年間料金をお支払いいただけます。

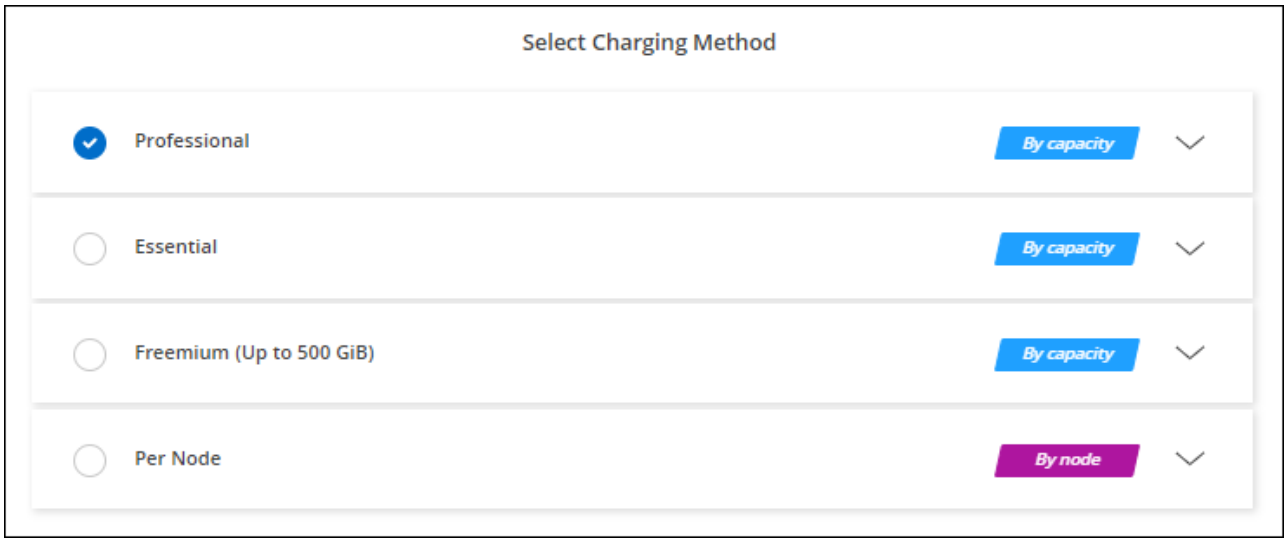
手順

1. 年間契約を購入するには、ネットアップの営業担当者にお問い合わせください。

   この契約は、Azure Marketplaceで_private_offerとして提供されます。

   ネットアップがお客様とプライベートオファーを共有したあとは、Azure Marketplaceでの作業環境の作成時にサブスクリプションするときに、年間プランを選択できます。

2. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. [詳細と資格情報]ページで、[資格情報の編集]>[サブスクリプションの追加]>[続行*]をクリックします。
   b. Azureポータルで、Azureアカウントと共有している年間プランを選択し、* Subscribe *をクリックします。
   c. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



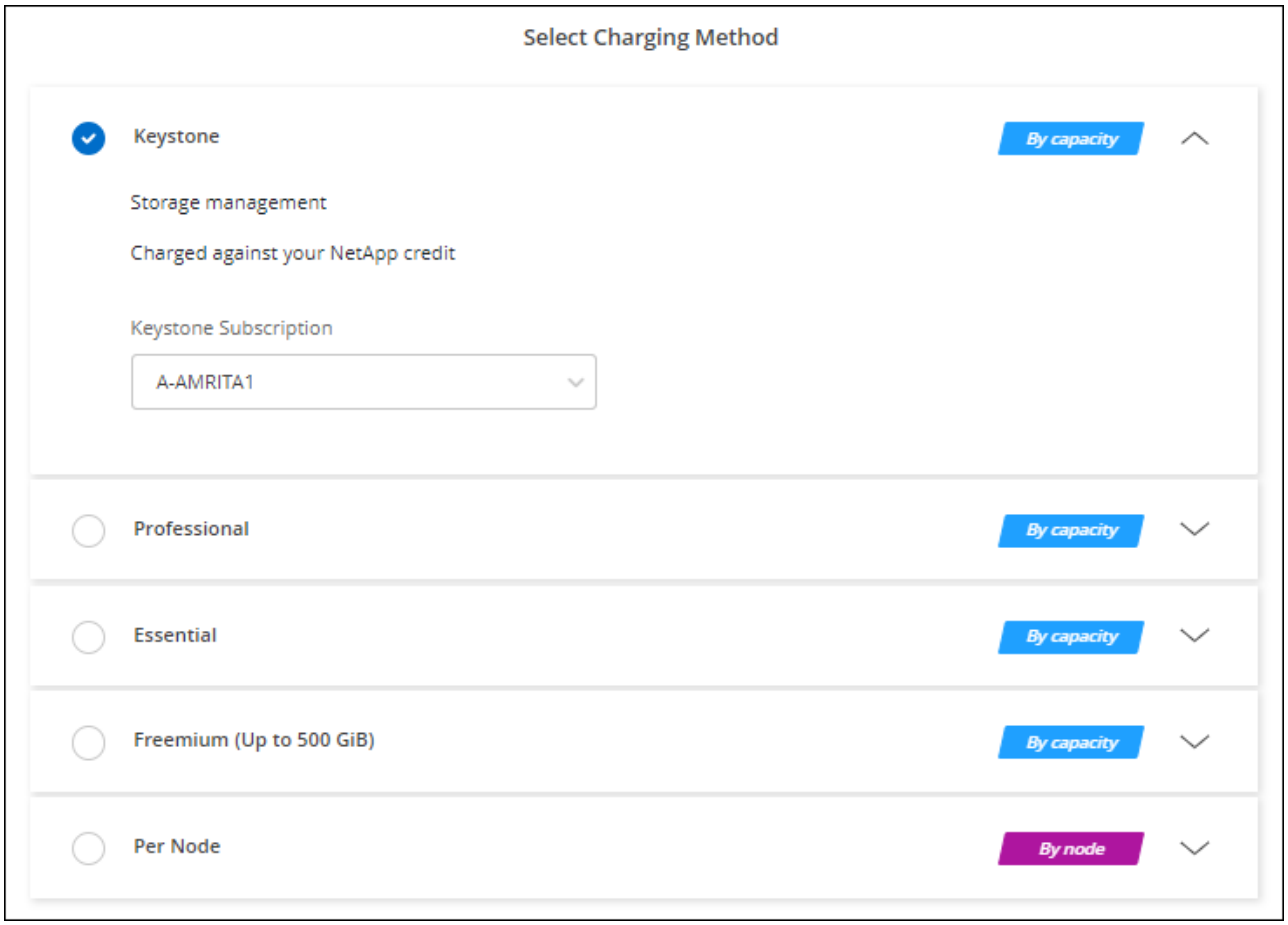
"ステップバイステップの手順を参照して、AzureでCloud Volumes ONTAP を起動してください"。

Keystoneサブスクリプション

Keystoneサブスクリプションは、ビジネスの成長に応じたサブスクリプションベースのサービスです。
"NetApp Keystone サブスクリプションの詳細については、こちらをご覧ください"。

手順

1. まだサブスクリプションをお持ちでない場合は、 "ネットアップにお問い合わせください"
2. mailto：ng-keystone-success@netapp.com [ネットアップにお問い合わせください]。1つ以上のKeystoneサブスクリプションでBlueXPユーザアカウントを承認する場合。
3. ネットアップがお客様のアカウントを許可したあと、 "Cloud Volumes ONTAP で使用するサブスクリプションをリンクします"。
4. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. 課金方法を選択するよう求められたら、Keystoneサブスクリプションの課金方法を選択します。



オプションのスクリーンショット。"]

"ステップバイステップの手順を参照して、AzureでCloud Volumes ONTAP を起動してください"。

Azureでハイアベイラビリティモードを有効にします

Microsoft Azureの高可用性モードを有効にして、計画外のフェイルオーバー時間を短縮し、NFSv4でCloud Volumes ONTAP がサポートされるようにする必要があります。

Cloud Volumes ONTAP 9.10.1リリースから、Microsoft Azureで実行されるCloud Volumes ONTAP HAペアの計画外フェイルオーバー時間が短縮され、NFSv4がサポートされるようになりました。これらの機能拡張をCloud Volumes ONTAP で使用できるようにするには、Azureサブスクリプションでハイアベイラビリティ機能を有効にする必要があります。

Azureサブスクリプションでこの機能を有効にする必要がある場合、「Action Required」メッセージにこれらの詳細が表示されます。

次の点に注意してください。

- Cloud Volumes ONTAP HA ペアの高可用性に問題はありません。この Azure 機能は、 ONTAP と連携して動作し、計画外のフェイルオーバーによって発生する NFS プロトコルのアプリケーション停止時間を短縮します。
- この機能を有効にしても、 Cloud Volumes ONTAP HA ペアの処理は中断されません。
- Azure サブスクリプションでこの機能を有効にしても、他の VM で原因の問題は発生しません。

「Owner」権限があるAzureユーザは、Azure CLIからこの機能を有効にできます。

手順

1. "Azure PortalからAzure Cloud Shellにアクセスします"
2. ハイアベイラビリティモード機能を登録します。

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. 必要に応じて、機能が登録されたことを確認します。

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Azure CLIから次のような結果が返されることを確認します。

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

Azure で Cloud Volumes ONTAP を起動します

BlueXPでCloud Volumes ONTAP 作業環境を作成することで、Azureで単一ノードシステムまたはHAペアを起動できます。

必要なもの

作業環境を作成するには、次の作業が必要です。

- 稼働中のコネクタ。
  - を用意しておく必要があります "ワークスペースに関連付けられているコネクタ"。
  - "コネクタをで実行したままにする準備をしておく必要があります 常時"。
- 使用する構成についての理解。

設定を選択し、ネットワーク管理者から Azure ネットワーク情報を入手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 "Cloud Volumes ONTAP 構成を計画"。

- Cloud Volumes ONTAP のライセンスを設定するために必要な事項を理解する。

  "ライセンスの設定方法について説明します"。

このタスクについて

BlueXPはAzureでCloud Volumes ONTAP システムを作成すると、リソースグループ、ネットワークインターフェイス、ストレージアカウントなどのいくつかのAzureオブジェクトを作成します。ウィザードの最後にあるリソースの概要を確認できます。

> データ損失の可能性があります
>
> Cloud Volumes ONTAP システムごとに新しい専用のリソースグループを使用することを推奨します。
>
> データ損失のリスクがあるため、既存の共有リソースグループに Cloud Volumes ONTAP を導入することは推奨されません。導入に失敗したり削除したりした場合に、共有リソースグループからCloud Volumes ONTAP リソースを削除できますが、Azureユーザが誤って共有リソースグループからCloud Volumes ONTAP リソースを削除する可能性があります。

Azureでのシングルノード**Cloud Volumes ONTAP** システムの起動

AzureでシングルノードのCloud Volumes ONTAP システムを起動する場合は、BlueXPでシングルノードの作業環境を作成する必要があります。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. [[subscribe] キャンバスページで、 * 作業環境の追加 * をクリックし、プロンプトに従います。
3. 場所を選択：「* Microsoft Azure 」および「 Cloud Volumes ONTAP シングルノード*」を選択します。
4. プロンプトが表示されたら、 "コネクタを作成します"。
5. * 詳細とクレデンシャル * ：必要に応じて Azure のクレデンシャルとサブスクリプションを変更し、クラスタ名を指定し、タグを追加し、クレデンシャルを指定することもできます。

   次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
作業環境名	BlueXPでは、作業環境名を使用して、Cloud Volumes ONTAP システムとAzure仮想マシンの両方に名前が付けられます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。
リソースグループタグ	タグは、 Azure リソースのメタデータです。このフィールドにタグを入力すると、Cloud Volumes ONTAP システムに関連付けられているリソースグループにタグが追加されます。作業環境を作成するときに、ユーザインターフェイスから最大 4 つのタグを追加し、作成後にさらに追加できます。API では、作業環境の作成時にタグを 4 つに制限することはありません。タグの詳細については、を参照してください "Microsoft Azure のドキュメント：「 Using tags to organize your Azure resources"。

フィールド	説明
ユーザ名とパスワード	Cloud Volumes ONTAP クラスタ管理者アカウントのクレデンシャルです。このクレデンシャルを使用して、 System Manager またはその CLI から Cloud Volumes ONTAP に接続できます。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します
資格情報を編集します	この Cloud Volumes ONTAP システムで使用する別の Azure クレデンシャルと別の Azure サブスクリプションを選択できます。従量課金制 Cloud Volumes ONTAP システムを導入するには、選択した Azure サブスクリプションに Azure Marketplace サブスクリプションを関連付ける必要があります。 "クレデンシャルを追加する方法について説明します"。

次のビデオでは、 Marketplace サブスクリプションを Azure サブスクリプションに関連付ける方法を紹介します。

Azure MarketplaceでBlueXPにサブスクライブ

6. * サービス *: サービスを有効にしておくか、 Cloud Volumes ONTAP で使用しない個々のサービスを無効にします。
   - "BlueXPの分類の詳細については、こちらをご覧ください"
   - "BlueXPのバックアップとリカバリの詳細については、こちらをご覧ください"

   WORMとデータ階層化を活用する場合は、BlueXPのバックアップとリカバリを無効にし、バージョン9.8以降のCloud Volumes ONTAP 作業環境を導入する必要があります。

7. 場所：リージョン、アベイラビリティゾーン、VNet、およびサブネットを選択し、チェックボックスを選択してコネクタとターゲットの場所間のネットワーク接続を確認します。

   シングルノードシステムの場合は、 Cloud Volumes ONTAP を導入するアベイラビリティゾーンを選択できます。AZを選択しない場合は、BlueXPによってそのAZが選択されます。

8. 接続性:新しいリソースグループまたは既存のリソースグループを選択し、事前定義されたセキュリティグループを使用するか、独自のリソースグループを使用するかを選択します。

   次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
リソースグループ	Cloud Volumes ONTAP の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。Cloud Volumes ONTAP には、新しい専用のリソースグループを使用することを推奨します。既存の共有リソースグループに Cloud Volumes ONTAP を導入することは可能ですが、データ損失のリスクがあるため推奨されません。詳細については、上記の警告を参照してください。 使用している Azure アカウントにが割り当てられている場合 "必要な権限"では、展開に失敗したり削除されたりした場合、Cloud Volumes ONTAP リソースがリソースグループから削除されます。

フィールド	説明
セキュリティグループが生成されました	BlueXPがセキュリティグループを生成するようにした場合は、トラフィックを許可する方法を選択する必要があります。 • 「選択したVNetのみ」を選択した場合のインバウンドトラフィックのソースは、選択したVNetのサブネット範囲およびコネクタが存在するVNetのサブネット範囲です。これが推奨されるオプションです。 • 「すべてのVNet *」を選択した場合、インバウンドトラフィックの送信元は0.0.0.0/0のIP範囲になります。
既存のを使用します	既存のセキュリティグループを選択する場合は、 Cloud Volumes ONTAP の要件を満たす必要があります。 "デフォルトのセキュリティグループを表示します"。

9. * 充電方法と NSS アカウント * ：このシステムで使用する充電オプションを指定し、ネットアップサポートサイトのアカウントを指定します。
   - "Cloud Volumes ONTAP のライセンスオプションについて説明します"。
   - "ライセンスの設定方法について説明します"。
10. * 構成済みパッケージ * ： Cloud Volumes ONTAP システムを迅速に導入するパッケージを 1 つ選択するか、 * 独自の構成を作成 * をクリックします。

    いずれかのパッケージを選択した場合は、ボリュームを指定してから、設定を確認して承認するだけで済みます。

11. ライセンス：必要に応じてCloud Volumes ONTAP のバージョンを変更し、仮想マシンのタイプを選択します。

    選択したバージョンで新しいリリース候補、一般提供、またはパッチリリースが利用可能な場合、作業環境の作成時にシステムがそのバージョンに更新されます。たとえば、Cloud Volumes ONTAP 9.10.1と9.10.1 P4が利用可能になっていれば、更新が実行されます。たとえば、 9.6 から 9.7 への更新など、あるリリースから別のリリースへの更新は行われません。

12. * Azure Marketplaceからサブスクライブ*：BlueXPでCloud Volumes ONTAPのプログラムによる導入を有効にできなかった場合は、このページが表示されます。画面に表示される手順に従います。を参照してください "Marketplace製品のプログラムによる導入" を参照してください。
13. * 基盤となるストレージリソース * ：初期アグリゲートの設定を選択します。ディスクタイプ、各ディスクのサイズ、 BLOB ストレージへのデータ階層化を有効にするかどうかを指定します。

    次の点に注意してください。

    - ディスクタイプは初期ボリューム用です。以降のボリュームでは、別のディスクタイプを選択できます。
    - シンプルなプロビジョニングオプションを使用した場合、ディスクサイズは、初期アグリゲートのすべてのディスクと、BlueXPで作成される追加のアグリゲートのサイズです。Advanced Allocation オプションを使用すると、異なるディスクサイズを使用するアグリゲートを作成できます。

      ディスクの種類とサイズの選択については、を参照してください "Azure でのシステムのサイジング

"。

- ボリュームを作成または編集するときに、特定のボリューム階層化ポリシーを選択できます。
- データの階層化を無効にすると、以降のアグリゲートで有効にすることができます。

"データ階層化の詳細については、こちらをご覧ください。"。

14. *書き込み速度とWORM *：

a. 必要に応じて、「標準」または「高速」の書き込み速度を選択します。

"書き込み速度の詳細については、こちらをご覧ください。"。

b. 必要に応じて、Write Once、Read Many（WORM）ストレージをアクティブにします。

このオプションは、特定のVMタイプに対してのみ使用できます。サポートされるVMタイプについては、を参照してください "HAペアのライセンスでサポートされる構成"。

Cloud Volumes ONTAP 9.7以前のバージョンでデータ階層化が有効になっている場合は、WORMを有効にすることはできません。Cloud Volumes ONTAP 9.8へのリバートまたはダウングレードは、WORMと階層化を有効にしたあとはブロックされます。

"WORM ストレージの詳細については、こちらをご覧ください。"。

a. WORMストレージをアクティブ化する場合は、保持期間を選択します。

15. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

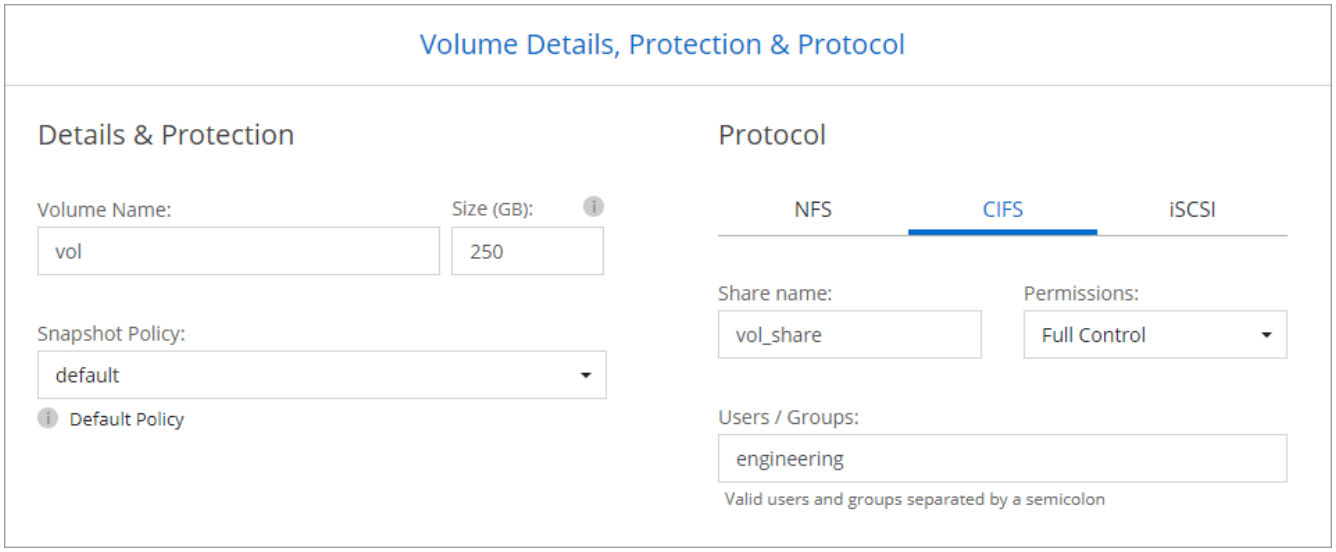
"サポートされるクライアントプロトコルおよびバージョンについて説明します"。

このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
サイズ	入力できる最大サイズは、シンプロビジョニングを有効にするかどうかによって大きく異なります。シンプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。
アクセス制御（ NFS のみ）	エクスポートポリシーは、ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、BlueXPはサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。
権限とユーザー / グループ（ CIFS のみ）	これらのフィールドを使用すると、ユーザおよびグループ（アクセスコントロールリストまたは ACL とも呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、 UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、 domain\username 形式でユーザのドメインを指定する必要があります。

フィールド	説明
スナップショットポリシー	Snapshot コピーポリシーは、自動的に作成される NetApp Snapshot コピーの頻度と数を指定します。NetApp Snapshot コピーは、パフォーマンスに影響を与えず、ストレージを最小限に抑えるポイントインタイムファイルシステムイメージです。デフォルトポリシーを選択することも、なしを選択することもできます。一時データには、 Microsoft SQL Server の tempdb など、 none を選択することもできます。
アドバンストオプション（ NFS のみ）	ボリュームの NFS バージョンを NFSv3 または NFSv4 のいずれかで選択してください。
イニシエータグループと IQN （ iSCSI のみ）	iSCSI ストレージターゲットは LUN （論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。イニシエータグループは、 iSCSI ホストのノード名のテーブルであり、どのイニシエータがどの LUN にアクセスできるかを制御します。iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（ NIC ）、ソフトウェアイニシエータを搭載した TOE カード、 CNA 、または専用の HBA を使用してネットワークに接続され、 iSCSI Qualified Name （ IQN ）で識別されます。iSCSIボリュームを作成すると、BlueXPによって自動的にLUNが作成されます。ボリュームごとに 1 つの LUN だけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、 "IQN を使用して、から LUN に接続します ホスト"。

次の図は、 CIFS プロトコルの [Volume] ページの設定を示しています。



16. * CIFS セットアップ * ： CIFS プロトコルを選択した場合は、 CIFS サーバをセットアップします。

フィールド	説明
DNS プライマリおよびセカンダリ IP アドレス	CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、 CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスロケーションレコード（ SRV ）が含まれている必要があります。
参加する Active Directory ドメイン	CIFS サーバを参加させる Active Directory （ AD ）ドメインの FQDN 。
ドメインへの参加を許可されたクレデンシャル	AD ドメイン内の指定した組織単位（ OU ）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。

フィールド	説明
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。Azure AD ドメインサービスを Cloud Volumes ONTAP の AD サーバとして設定するには、このフィールドに「 * OU=AADDC computers* 」または「 * OU=AADDC Users* 」と入力します。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure のドキュメント：「 Create an Organizational Unit （ OU ；組織単位） in an Azure AD Domain Services managed domain"^]
DNS ドメイン	Cloud Volumes ONTAP Storage Virtual Machine （ SVM ）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。
NTP サーバ	Active Directory DNS を使用して NTP サーバを設定するには、「 Active Directory ドメインを使用」を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、 API を使用してください。を参照してください "BlueXP自動化ドキュメント" を参照してください。 NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

17. * 使用状況プロファイル、ディスクタイプ、階層化ポリシー * ： Storage Efficiency 機能を有効にするかどうかを選択し、必要に応じてボリューム階層化ポリシーを変更します。

    詳細については、を参照してください "ボリューム使用率プロファイルについて" および "データ階層化の概要"。

18. * レビューと承認 *: 選択内容を確認して確認します。
    a. 設定の詳細を確認します。
    b. [詳細情報*]をクリックして、BlueXPが購入するサポートとAzureリソースの詳細を確認します。
    c. [* I understand … * （理解しています … * ）] チェックボックスを選択
    d. [Go*] をクリックします。

結果

BlueXPがCloud Volumes ONTAP システムを導入しましたタイムラインで進行状況を追跡できます。

Cloud Volumes ONTAP システムの導入で問題が発生した場合は、障害メッセージを確認してください。作業環境を選択し、 * 環境の再作成 * をクリックすることもできます。

詳細については、を参照してください "NetApp Cloud Volumes ONTAP のサポート"。

完了後

- CIFS 共有をプロビジョニングした場合は、ファイルとフォルダに対する権限をユーザまたはグループに付与し、それらのユーザが共有にアクセスしてファイルを作成できることを確認します。
- ボリュームにクォータを適用する場合は、 System Manager または CLI を使用します。

  クォータを使用すると、ユーザ、グループ、または qtree が使用するディスク・スペースとファイル数を制限または追跡できます。

AzureでのCloud Volumes ONTAP HAペアの起動

AzureでCloud Volumes ONTAP HAペアを起動するには、BlueXPでHA作業環境を作成する必要があります。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. [[subscribe] キャンバスページで、 * 作業環境の追加 * をクリックし、プロンプトに従います。
3. プロンプトが表示されたら、 "コネクタを作成します"。
4. * 詳細とクレデンシャル * ：必要に応じて Azure のクレデンシャルとサブスクリプションを変更し、クラスタ名を指定し、タグを追加し、クレデンシャルを指定することもできます。

   次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
作業環境名	BlueXPでは、作業環境名を使用して、Cloud Volumes ONTAP システムとAzure仮想マシンの両方に名前が付けられます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。
リソースグループタグ	タグは、 Azure リソースのメタデータです。このフィールドにタグを入力すると、Cloud Volumes ONTAP システムに関連付けられているリソースグループにタグが追加されます。作業環境を作成するときに、ユーザインターフェイスから最大 4 つのタグを追加し、作成後にさらに追加できます。API では、作業環境の作成時にタグを 4 つに制限することはありません。タグの詳細については、を参照してください "Microsoft Azure のドキュメント：「 Using tags to organize your Azure resources"。
ユーザ名とパスワード	Cloud Volumes ONTAP クラスタ管理者アカウントのクレデンシャルです。このクレデンシャルを使用して、 System Manager またはその CLI から Cloud Volumes ONTAP に接続できます。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します
資格情報を編集します	この Cloud Volumes ONTAP システムで使用する別の Azure クレデンシャルと別の Azure サブスクリプションを選択できます。従量課金制 Cloud Volumes ONTAP システムを導入するには、選択した Azure サブスクリプションに Azure Marketplace サブスクリプションを関連付ける必要があります。 "クレデンシャルを追加する方法について説明します"。

   次のビデオでは、 Marketplace サブスクリプションを Azure サブスクリプションに関連付ける方法を紹介します。

   Azure MarketplaceでBlueXPにサブスクライブ

5. * サービス *: サービスを有効にしておくか、 Cloud Volumes ONTAP で使用しない個々のサービスを無効にします。
   - "BlueXPの分類の詳細については、こちらをご覧ください"
   - "BlueXPのバックアップとリカバリの詳細については、こちらをご覧ください"

   WORMとデータ階層化を活用する場合は、BlueXPのバックアップとリカバリを無効にし、バージョン9.8以降のCloud Volumes ONTAP 作業環境を導入する必要があります。

6. * HA導入モデル*：
   a. 単一アベイラビリティゾーン*または*複数のアベイラビリティゾーン*を選択します。
   b. 場所と接続（単一AZ）および*地域と接続*（複数のAZ）
      - 単一のAZの場合は、リージョン、VNet、およびサブネットを選択します。
      - 複数のAZについて、リージョン、VNet、サブネット、ノード1のゾーン、およびノード2のゾーンを選択します。
   c. [ネットワーク接続を検証しました…]*]チェックボックスを選択します。
7. 接続性:新しいリソースグループまたは既存のリソースグループを選択し、事前定義されたセキュリティグループを使用するか、独自のリソースグループを使用するかを選択します。

   次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
リソースグループ	Cloud Volumes ONTAP の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。Cloud Volumes ONTAP には、新しい専用のリソースグループを使用することを推奨します。既存の共有リソースグループに Cloud Volumes ONTAP を導入することは可能ですが、データ損失のリスクがあるため推奨されません。詳細については、上記の警告を参照してください。 Azure に導入する Cloud Volumes ONTAP HA ペアごとに専用のリソースグループを使用する必要があります。リソースグループでサポートされる HA ペアは 1 つだけです。Azureリソースグループに2つ目のCloud Volumes ONTAP HAペアを導入しようとすると、接続の問題が発生します。 使用している Azure アカウントにが割り当てられている場合 "必要な権限"では、展開に失敗したり削除されたりした場合、Cloud Volumes ONTAP リソースがリソースグループから削除されます。
セキュリティグループが生成されました	BlueXPがセキュリティグループを生成するようにした場合は、トラフィックを許可する方法を選択する必要があります。 • 「選択したVNetのみ」を選択した場合のインバウンドトラフィックのソースは、選択したVNetのサブネット範囲およびコネクタが存在するVNetのサブネット範囲です。これが推奨されるオプションです。 • 「すべてのVNet *」を選択した場合、インバウンドトラフィックの送信元は0.0.0.0/0のIP範囲になります。
既存のを使用します	既存のセキュリティグループを選択する場合は、 Cloud Volumes ONTAP の要件を満たす必要があります。 "デフォルトのセキュリティグループを表示します"。

8. * 充電方法と NSS アカウント * ：このシステムで使用する充電オプションを指定し、ネットアップサポートサイトのアカウントを指定します。
   ◦ "Cloud Volumes ONTAP のライセンスオプションについて説明します"。

- "ライセンスの設定方法について説明します"。

9. 構成済みパッケージ：Cloud Volumes ONTAP システムを迅速に導入するパッケージを1つ選択するか、*構成の変更*をクリックします。

   いずれかのパッケージを選択した場合は、ボリュームを指定してから、設定を確認して承認するだけで済みます。

10. ライセンス：必要に応じてCloud Volumes ONTAP のバージョンを変更し、仮想マシンのタイプを選択します。

    選択したバージョンで新しいリリース候補、一般提供、またはパッチリリースが利用可能な場合、作業環境の作成時にシステムがそのバージョンに更新されます。たとえば、Cloud Volumes ONTAP 9.10.1と9.10.1 P4が利用可能になっていれば、更新が実行されます。たとえば、 9.6 から 9.7 への更新など、あるリリースから別のリリースへの更新は行われません。

11. * Azure Marketplaceからサブスクライブ*：BlueXPでCloud Volumes ONTAP のプログラムによる導入を有効にできなかった場合は、以下の手順に従ってください。

12. * 基盤となるストレージリソース * ：初期アグリゲートの設定を選択します。ディスクタイプ、各ディスクのサイズ、 BLOB ストレージへのデータ階層化を有効にするかどうかを指定します。

    次の点に注意してください。

    - シンプルなプロビジョニングオプションを使用した場合、ディスクサイズは、初期アグリゲートのすべてのディスクと、BlueXPで作成される追加のアグリゲートのサイズです。Advanced Allocation オプションを使用すると、異なるディスクサイズを使用するアグリゲートを作成できます。

      ディスク・サイズの選択については、を参照してください "Azureでシステムのサイズを設定します"。

    - ボリュームを作成または編集するときに、特定のボリューム階層化ポリシーを選択できます。
    - データの階層化を無効にすると、以降のアグリゲートで有効にすることができます。

      "データ階層化の詳細については、こちらをご覧ください。"。

13. *書き込み速度とWORM *：

    a. 必要に応じて、「標準」または「高速」の書き込み速度を選択します。

       "書き込み速度の詳細については、こちらをご覧ください。"。

    b. 必要に応じて、Write Once、Read Many（WORM）ストレージをアクティブにします。

       このオプションは、特定のVMタイプに対してのみ使用できます。サポートされるVMタイプについては、を参照してください "HAペアのライセンスでサポートされる構成"。

       Cloud Volumes ONTAP 9.7以前のバージョンでデータ階層化が有効になっている場合は、WORMを有効にすることはできません。Cloud Volumes ONTAP 9.8へのリバートまたはダウングレードは、WORMと階層化を有効にしたあとはブロックされます。

    "WORM ストレージの詳細については、こちらをご覧ください。"。

a. WORMストレージをアクティブ化する場合は、保持期間を選択します。

14. ストレージと**WORM**へのセキュアな通信：Azureストレージアカウントへの**HTTPS**接続を有効にするかどうかを選択し、必要に応じてWrite Once Read Many（WORM）ストレージをアクティブ化します。

    HTTPS接続は、Cloud Volumes ONTAP 9.7のHAペアからAzureページBLOBストレージアカウントに確立されます。このオプションを有効にすると、書き込みパフォーマンスに影響する可能性があります。作業環境の作成後に設定を変更することはできません。

    "WORM ストレージの詳細については、こちらをご覧ください。"。

    データの階層化が有効になっていると、 WORM を有効にできません。

    "WORM ストレージの詳細については、こちらをご覧ください。"。

15. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

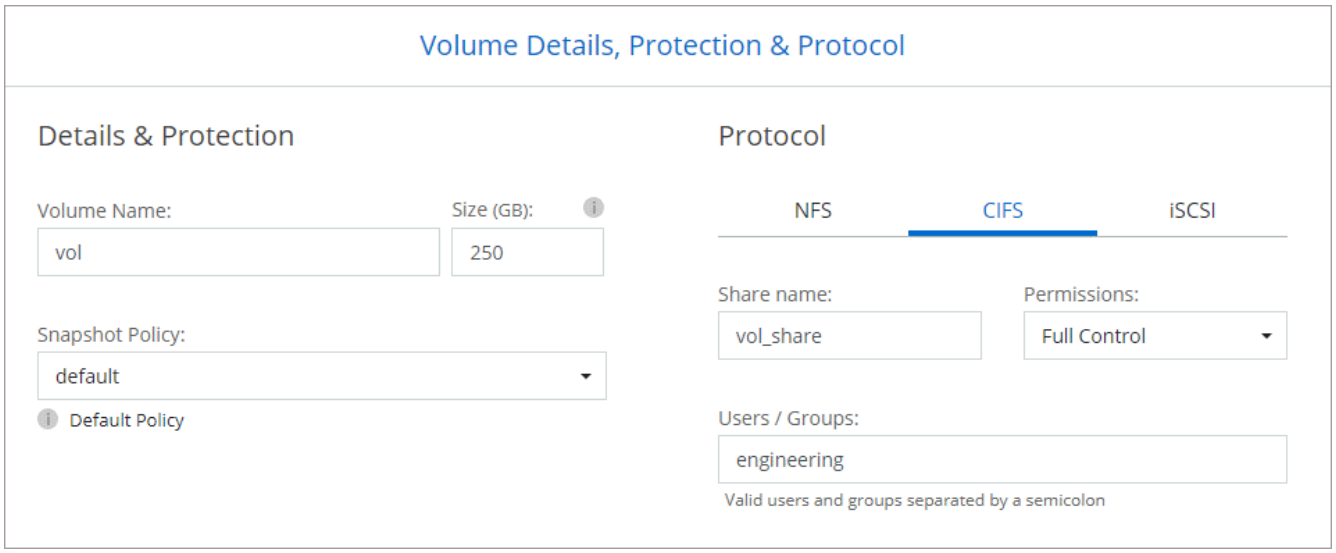
    "サポートされるクライアントプロトコルおよびバージョンについて説明します"。

    このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
サイズ	入力できる最大サイズは、シンプロビジョニングを有効にするかどうかによって大きく異なります。シンプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。
アクセス制御（ NFS のみ）	エクスポートポリシーは、ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、BlueXPはサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。
権限とユーザー / グループ（ CIFS のみ）	これらのフィールドを使用すると、ユーザおよびグループ（アクセスコントロールリストまたは ACL とも呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、 UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、 domain\username 形式でユーザのドメインを指定する必要があります。
スナップショットポリシー	Snapshot コピーポリシーは、自動的に作成される NetApp Snapshot コピーの頻度と数を指定します。NetApp Snapshot コピーは、パフォーマンスに影響を与えず、ストレージを最小限に抑えるポイントインタイムファイルシステムイメージです。デフォルトポリシーを選択することも、なしを選択することもできます。一時データには、 Microsoft SQL Server の tempdb など、 none を選択することもできます。
アドバンストオプション（ NFS のみ）	ボリュームの NFS バージョンを NFSv3 または NFSv4 のいずれかで選択してください。

フィールド	説明
イニシエータグループと IQN （ iSCSI のみ）	iSCSI ストレージターゲットは LUN （論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。イニシエータグループは、 iSCSI ホストのノード名のテーブルであり、どのイニシエータがどの LUN にアクセスできるかを制御します。iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（ NIC ）、ソフトウェアイニシエータを搭載した TOE カード、 CNA 、または専用の HBA を使用してネットワークに接続され、 iSCSI Qualified Name （ IQN ）で識別されます。iSCSIボリュームを作成すると、BlueXPによって自動的にLUNが作成されます。ボリュームごとに 1 つの LUN だけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、 "IQN を使用して、から LUN に接続します ホスト"。

次の図は、 CIFS プロトコルの [Volume] ページの設定を示しています。



16. * CIFS セットアップ * ： CIFS プロトコルを選択した場合は、 CIFS サーバをセットアップします。

フィールド	説明
DNS プライマリおよびセカンダリ IP アドレス	CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、 CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスロケーションレコード（ SRV ）が含まれている必要があります。
参加する Active Directory ドメイン	CIFS サーバを参加させる Active Directory （ AD ）ドメインの FQDN 。
ドメインへの参加を許可されたクレデンシャル	AD ドメイン内の指定した組織単位（ OU ）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。

フィールド	説明
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。Azure AD ドメインサービスを Cloud Volumes ONTAP の AD サーバとして設定するには、このフィールドに「 * OU=AADDC computers* 」または「 * OU=AADDC Users* 」と入力します。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure のドキュメント：「 Create an Organizational Unit （ OU ；組織単位） in an Azure AD Domain Services managed domain"^]
DNS ドメイン	Cloud Volumes ONTAP Storage Virtual Machine （ SVM ）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。
NTP サーバ	Active Directory DNS を使用して NTP サーバを設定するには、「 Active Directory ドメインを使用」を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、 API を使用してください。を参照してください "BlueXP自動化ドキュメント" を参照してください。 NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

17. * 使用状況プロファイル、ディスクタイプ、階層化ポリシー * ： Storage Efficiency 機能を有効にするかどうかを選択し、必要に応じてボリューム階層化ポリシーを変更します。

    詳細については、を参照してください "ボリュームの使用プロファイルを選択してください" および "データ階層化の概要"。

18. * レビューと承認 *: 選択内容を確認して確認します。
    a. 設定の詳細を確認します。
    b. [詳細情報*]をクリックして、BlueXPが購入するサポートとAzureリソースの詳細を確認します。
    c. [* I understand … * （理解しています … * ）] チェックボックスを選択
    d. [Go*] をクリックします。

結果

BlueXPがCloud Volumes ONTAP システムを導入しましたタイムラインで進行状況を追跡できます。

Cloud Volumes ONTAP システムの導入で問題が発生した場合は、障害メッセージを確認してください。作業環境を選択し、 * 環境の再作成 * をクリックすることもできます。

詳細については、を参照してください "NetApp Cloud Volumes ONTAP のサポート"。

完了後

- CIFS 共有をプロビジョニングした場合は、ファイルとフォルダに対する権限をユーザまたはグループに付与し、それらのユーザが共有にアクセスしてファイルを作成できることを確認します。
- ボリュームにクォータを適用する場合は、 System Manager または CLI を使用します。

  クォータを使用すると、ユーザ、グループ、または qtree が使用するディスク・スペースとファイル数を制限または追跡できます。

Google Cloud で始めましょう

Google Cloud の Cloud Volumes ONTAP のクイックスタート

Cloud Volumes ONTAP for Google Cloudの使用を開始するには、いくつかの手順を実行します。


コネクタを作成します

を持っていなければ "コネクタ" ただし、アカウント管理者がアカウントを作成する必要があります。
"Google Cloud でコネクタを作成する方法について説明します"

インターネットアクセスを使用できないサブネットにCloud Volumes ONTAP を導入する場合は、コネクタを手動でインストールし、そのコネクタで実行されているBlueXPユーザインターフェイスにアクセスする必要があります。 "インターネットにアクセスできない場所にコネクタを手動でインストールする方法について説明します"


構成を計画

BlueXPでは、ワークロード要件に合わせて事前設定されたパッケージを提供しています。また、独自の構成を作成することもできます。独自の設定を選択する場合は、使用可能なオプションを理解しておく必要があります。

"構成の計画の詳細については、こちらをご覧ください"。


ネットワークをセットアップします

1. VPC とサブネットがコネクタと Cloud Volumes ONTAP 間の接続をサポートしていることを確認します。
2. データの階層化を有効にする場合は、 "プライベート Google アクセス用の Cloud Volumes ONTAP サブネットを設定します"。
3. HA ペアを導入する場合は、それぞれ独自のサブネットを持つ 4 つの VPC があることを確認します。
4. 共有 VPC を使用する場合は、コネクタサービスアカウントに _Compute Network User_role を指定します。
5. ターゲットVPCからのアウトバウンドのインターネットアクセスをNetApp AutoSupport で有効にします。

   インターネットにアクセスできない場所にCloud Volumes ONTAP を導入する場合は、この手順は必要ありません。

"ネットワーク要件の詳細については、こちらをご覧ください"。


サービスアカウントを設定します

Cloud Volumes ONTAP には、 2 つの目的で Google Cloud サービスアカウントが必要です。1 つ目は、を有効にする場合です "データの階層化" Google Cloud でコールドデータを低コストのオブジェクトストレージに階層化すること。2 つ目は、を有効にした場合です "BlueXPのバックアップとリカバリ" ボリュームを低コス

トのオブジェクトストレージにバックアップできます。

1 つのサービスアカウントを設定して、両方の目的に使用できます。サービスアカウントには * Storage Admin * ロールが必要です。

"詳細な手順を参照してください"。

5 Google Cloud API を有効にします

"プロジェクトで次の Google Cloud API を有効にします"。これらの API は、コネクタと Cloud Volumes ONTAP を導入するために必要です。

- Cloud Deployment Manager V2 API
- クラウドロギング API
- Cloud Resource Manager API の略
- Compute Engine API
- ID およびアクセス管理（ IAM ） API

6 BlueXPを使用してCloud Volumes ONTAP を起動します

[作業環境の追加] をクリックし、展開するシステムのタイプを選択して、ウィザードの手順を実行します。 "詳細な手順を参照してください"。

関連リンク

- "BlueXPからコネクタを作成しています"
- "Linux ホストへの Connector ソフトウェアのインストール"
- "BlueXPがGoogle Cloud権限で実行する機能"

Google CloudでCloud Volumes ONTAP 構成を計画する

Google Cloud に Cloud Volumes ONTAP を導入する場合は、ワークロードの要件に合わせて事前設定されたシステムを選択するか、または独自の設定を作成できます。独自の設定を選択する場合は、使用可能なオプションを理解しておく必要があります。

Cloud Volumes ONTAP ライセンスを選択します

Cloud Volumes ONTAP には、いくつかのライセンスオプションがあります。それぞれのオプションで、ニーズに合った消費モデルを選択できます。

- "Cloud Volumes ONTAP のライセンスオプションについて説明します"
- "ライセンスの設定方法について説明します"

サポートされているリージョンを選択します

Cloud Volumes ONTAP は、ほとんどの Google Cloud リージョンでサポートされています。 "サポートされているリージョンの完全なリストを表示します"。

サポートされているマシンタイプを選択してください

Cloud Volumes ONTAP では、選択したライセンスタイプに応じて、複数のマシンタイプがサポートされます。

"GCP の Cloud Volumes ONTAP でサポートされている構成"

ストレージの制限を確認

Cloud Volumes ONTAP システムの未フォーマット時の容量制限は、ライセンスに関連付けられています。追加の制限は、アグリゲートとボリュームのサイズに影響します。設定を計画する際には、これらの制限に注意する必要があります。

"GCP の Cloud Volumes ONTAP でのストレージの制限"

GCPでシステムのサイズを設定します

Cloud Volumes ONTAP システムのサイジングを行うことで、パフォーマンスと容量の要件を満たすのに役立ちます。マシンタイプ、ディスクタイプ、およびディスクサイズを選択する際には、次の点に注意してください。

マシンのタイプ

でサポートされているマシンタイプを確認します "Cloud Volumes ONTAP リリースノート" 次に、サポートされている各マシンタイプについて Google の詳細を確認します。ワークロードの要件を、マシンタイプの vCPU とメモリの数と一致させます。各 CPU コアは、ネットワークパフォーマンスを向上させることに注意してください。

詳細については、以下を参照してください。

- "Google Cloud ドキュメント： N1 標準マシンタイプ"
- "Google Cloud のドキュメント：「 Performance"

GCP ディスクタイプ

Cloud Volumes ONTAP 用のボリュームを作成する際には、 Cloud Volumes ONTAP がディスクに使用する基盤となるクラウドストレージを選択する必要があります。ディスクタイプは次のいずれかです。

- _ゾーン SSD 永続ディスク _ ： SSD 永続ディスクは、ランダム IOPS が高いワークロードに最適です。
- _ゾーン バランシング永続ディスク _ ：これらの SSD は、 GB あたりの IOPS を下げて、パフォーマンスとコストのバランスを取ります。
- _Zonal 標準パーシステントディスク _ ：標準パーシステントディスクは経済的で、シーケンシャルな読み取り / 書き込み処理に対応できます。

  詳細については、を参照してください "Google Cloud のドキュメント：「ゾーン永続ディスク（標準および SSD ）」"。

GCP ディスクサイズ

Cloud Volumes ONTAP システムを導入する際には、初期ディスクサイズを選択する必要があります。システムの容量をBlueXPで管理できるようになりますが、自分でアグリゲートを作成する場合は、次の点に注意してください。

- アグリゲート内のディスクはすべて同じサイズである必要があります。
- パフォーマンスを考慮しながら、必要なスペースを判断します。
- パーシステントディスクのパフォーマンスは、システムで使用可能なディスクサイズと vCPU の数に応じて自動的に拡張されます。

  詳細については、以下を参照してください。

  - "Google Cloud のドキュメント：「ゾーン永続ディスク（標準および SSD ）」"
  - "Google Cloud のドキュメント：「 Optimizing Persistent Disk and Local SSD Performance"

デフォルトのシステムディスクを表示します

ユーザデータ用のストレージに加えて、BlueXPはCloud Volumes ONTAP システムデータ（ブートデータ、ルートデータ、コアデータ、NVRAM）用のクラウドストレージも購入します。計画を立てる場合は、 Cloud Volumes ONTAP を導入する前にこれらの詳細を確認すると役立つ場合があります。

- "Cloud Volumes ONTAP システムデータ用のデフォルトディスクを Google Cloud で表示します"。
- "Google Cloud のドキュメント：リソースクォータ"

  Google Cloud Compute Engine では、リソース使用量にクォータが適用されるため、 Cloud Volumes ONTAP を導入する前に制限に達していないことを確認する必要があります。

コネクタにはシステムディスクも必要です。 "コネクタのデフォルト設定に関する詳細を表示します"。

ネットワーク情報を収集

GCP で Cloud Volumes ONTAP を導入する場合は、仮想ネットワークの詳細を指定する必要があります。ワークシートを使用して、管理者から情報を収集できます。

- シングルノードシステム * のネットワーク情報

GCP 情報	あなたの価値
地域	
ゾーン	
vPC ネットワーク	
サブネット	
ファイアウォールポリシー（独自のポリシーを使用している場合）	

- 複数ゾーン内の HA ペアのネットワーク情報 *

GCP 情報	あなたの価値
地域	

GCP 情報	あなたの価値
ノード 1 のゾーン	
ノード 2 のゾーン	
メディエーターのゾーン	
vPC-0 およびサブネット	
vPC-1 とサブネット	
vPC-2 およびサブネット	
vPC-3 とサブネット	
ファイアウォールポリシー（独自のポリシーを使用している場合）	

- 単一ゾーン内の HA ペアのネットワーク情報 *

GCP 情報	あなたの価値
地域	
ゾーン	
vPC-0 およびサブネット	
vPC-1 とサブネット	
vPC-2 およびサブネット	
vPC-3 とサブネット	
ファイアウォールポリシー（独自のポリシーを使用している場合）	

書き込み速度を選択します

BlueXPを使用すると、Google Cloudのハイアベイラビリティ（HA）ペアを除き、Cloud Volumes ONTAP の書き込み速度設定を選択できます。書き込み速度を選択する前に、高速書き込みを使用する場合の標準設定と高設定の違い、およびリスクと推奨事項を理解しておく必要があります。 "書き込み速度の詳細については、こちらをご覧ください。"。

ボリュームの使用プロファイルを選択してください

ONTAP には、必要なストレージの合計容量を削減できるストレージ効率化機能がいくつか搭載されています。BlueXPでボリュームを作成するときに、これらの機能を有効にするプロファイル、または無効にするプロファイルを選択できます。これらの機能の詳細については、使用するプロファイルを決定する際に役立ちます。

NetApp Storage Efficiency 機能には、次のようなメリットがあります。

シンプロビジョニング

物理ストレージプールよりも多くの論理ストレージをホストまたはユーザに提供します。ストレージスペースは、事前にストレージスペースを割り当てる代わりに、データの書き込み時に各ボリュームに動的に

割り当てられます。

重複排除

同一のデータブロックを検索し、単一の共有ブロックへの参照に置き換えることで、効率を向上します。この手法では、同じボリュームに存在するデータの冗長ブロックを排除することで、ストレージ容量の要件を軽減します。

圧縮

プライマリ、セカンダリ、アーカイブストレージ上のボリューム内のデータを圧縮することで、データの格納に必要な物理容量を削減します。

Google CloudでのCloud Volumes ONTAP のネットワーク要件

Cloud Volumes ONTAP システムが正常に動作するように、Google Cloudネットワークをセットアップします。

HA ペアを導入する場合は、を実行します "Google CloudでのHAペアの仕組みをご確認ください"。

Cloud Volumes ONTAP の要件

Google Cloudでは、次の要件を満たす必要があります。

シングルノードシステムに固有の要件

シングルノードシステムを導入する場合は、ネットワークが次の要件を満たしていることを確認してください。

1つのVPC

シングルノードシステムにはVirtual Private Cloud（VPC；仮想プライベートクラウド）が1つ必要です。

プライベート IP アドレス

BlueXPは、Google Cloudのシングルノードシステムに3つまたは4つのプライベートIPアドレスを割り当てます。

Cloud Volumes ONTAP を API を使用して導入する場合、 Storage VM （ SVM ）管理 LIF の作成をスキップし、次のフラグを指定できます。

'kipsvmManagementLIF ： true

LIF は、物理ポートに関連付けられた IP アドレスです。SnapCenter などの管理ツールには、Storage VM （ SVM ）管理 LIF が必要です。

HAペアに固有の要件

HAペアを導入する場合は、ネットワークが次の要件を満たしていることを確認します。

1つまたは複数のゾーン

複数のゾーンまたは単一のゾーンに HA 構成を導入することで、データの高可用性を確保できます。HAペアを作成すると、複数のゾーンまたは単一のゾーンを選択するように求められます。

- 複数のゾーン（推奨）

  3 つのゾーンに HA 構成を導入することで、ゾーン内で障害が発生した場合の継続的なデータ可用性を確保できます。書き込みパフォーマンスは、単一のゾーンを使用する場合に比べてわずかに低くなりますが、最小のパフォーマンスです。

- シングルゾーン

  Cloud Volumes ONTAP HA 構成では、単一のゾーンに導入する場合は分散配置ポリシーを使用します。このポリシーにより、 HA 構成がゾーン内の単一点障害から保護されます。障害の切り分けに別々のゾーンを使用する必要はありません。

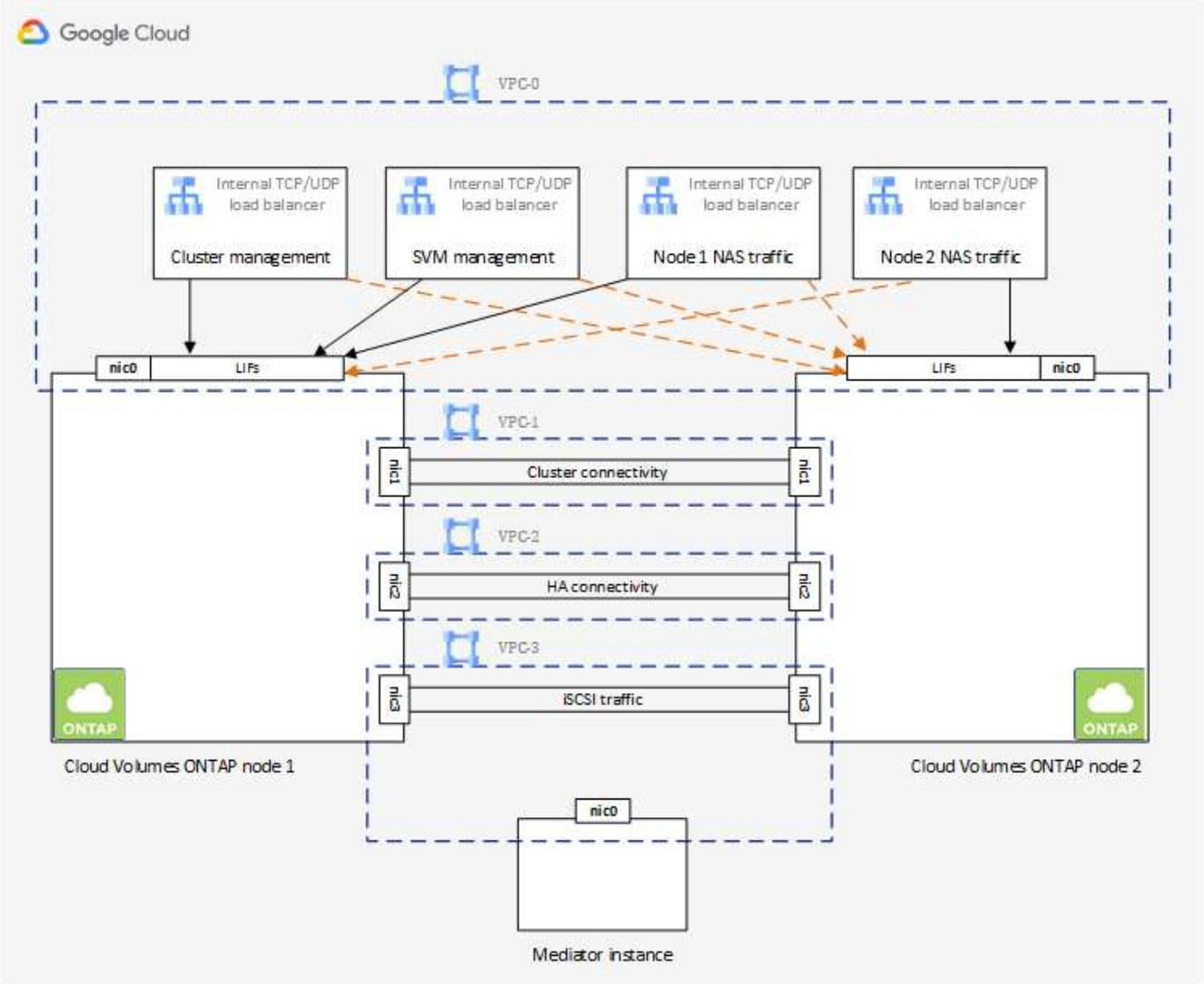
  この導入モデルでは、ゾーン間にデータ出力料金が発生しないため、コストが削減されます。

4つの仮想プライベートクラウド

HA 構成には、 4 つの Virtual Private Cloud （ VPC ；仮想プライベートクラウド）が必要です。Google Cloudでは各ネットワークインターフェイスを別 々 のVPCネットワークに配置する必要があるため、VPCは4つ必要です。

HAペアを作成するときに、4つのVPCを選択するように要求されます。

- vPC-0 ：データおよびノードへのインバウンド接続
- vPC-1 、 VPC -2 、および VPC -3 ：ノードと HA メディエーター間の内部通信



サブネット

VPC ごとにプライベートサブネットが必要です。

コネクタを VPC 0 に配置する場合は、サブネットで Private Google Access を有効にして API にアクセスし、データの階層化を有効にする必要があります。

これらの VPC 内のサブネットには、個別の CIDR 範囲が必要です。CIDR 範囲を重複させることはできません。

プライベート **IP** アドレス

BlueXPは、必要な数のプライベートIPアドレスをGoogle CloudのCloud Volumes ONTAP に自動的に割り当てます。ネットワークに十分なプライベートアドレスがあることを確認する必要があります。

Cloud Volumes ONTAP 用に割り当てられるLIFの数は、シングルノードシステムとHAペアのどちらを導入するかによって異なります。LIF は、物理ポートに関連付けられた IP アドレスです。SnapCenter などの管理ツールには、 SVM 管理 LIF が必要です。

- シングルノード BlueXPでは、1つのノードシステムに4つのIPアドレスが割り当てられます。

- ノード管理 LIF
- クラスタ管理 LIF
- iSCSI データ LIF

> iSCSI LIFは、iSCSIプロトコルを介したクライアントアクセスを提供し、システムがその他の重要なネットワークワークフローに使用します。これらのLIFは必須であり、削除しないでください。

- NAS LIF

  Cloud Volumes ONTAP を API を使用して導入する場合、 Storage VM （ SVM ）管理 LIF の作成をスキップし、次のフラグを指定できます。

'kipsvmManagementLIF ： true

- * HAペア* BlueXPは、12~13個のIPアドレスをHAペアに割り当てます。
  - ノード管理LIF×2（e0a）
  - クラスタ管理LIF（e0a）×1
  - iSCSI LIF×2（e0a）

> iSCSI LIFは、iSCSIプロトコルを介したクライアントアクセスを提供し、システムがその他の重要なネットワークワークフローに使用します。これらのLIFは必須であり、削除しないでください。

  - NAS LIF（e0a）×1または2
  - クラスタLIF×2（e0b）
  - HAインターコネクトIPアドレス×2（e0c）
  - RSM iSCSI IPアドレス×2（e0d）

    Cloud Volumes ONTAP を API を使用して導入する場合、 Storage VM （ SVM ）管理 LIF の作成をスキップし、次のフラグを指定できます。

'kipsvmManagementLIF ： true

内部ロードバランサ

BlueXPでは、Cloud Volumes ONTAP HAペアへの着信トラフィックを管理するGoogle Cloud内部ロードバランサ（TCP/UDP）が自動的に4つ作成されます。セットアップは必要ありませんネットワークトラフィックを通知し、セキュリティ上の問題を緩和するだけで、この要件が満たされることがわかりました。

クラスタ管理用のロードバランサで、 1 つは Storage VM （ SVM ）管理用、もう 1 つはノード 1 への NAS トラフィック用、もう 1 つはノード 2 への NAS トラフィック用です。

各ロードバランサの設定は次のとおりです。

- 共有プライベート IP アドレス × 1

- グローバル健全性チェック 1 回

  デフォルトでは、ヘルスチェックで使用されるポートは 63001 、 63002 、および 63003 です。

- 地域 TCP バックエンドサービス × 1
- 地域 UDP バックエンドサービス × 1
- 1 つの TCP 転送ルール
- 1 つの UDP 転送ルール
- グローバルアクセスは無効です

  グローバルアクセスはデフォルトでは無効になっていますが、展開後に有効にすることができます。クロスリージョントラフィックのレイテンシが大幅に高くなるため、この機能は無効にしました。誤ってリージョン間にマウントすることが原因でマイナスの体験が得られないようにしたいと考えていました。このオプションを有効にすることは、ビジネスニーズに固有のものです。

共有 **VPC**

Cloud Volumes ONTAP とコネクタは、 Google Cloud の共有 VPC とスタンドアロンの VPC でサポートされます。

シングルノードシステムの場合は、 VPC は共有 VPC またはスタンドアロン VPC のどちらかになります。

HA ペアの場合は、 4 つの VPC が必要です。これらの各 VPC は、共有またはスタンドアロンのどちらかにすることができます。たとえば、 VPC は VPC を共有化し、 VPC は VPC 1 、 VPC は 2 、 VPC は 3 で構成されることになります。

共有 VPC を使用すると、複数のプロジェクトの仮想ネットワークを設定し、一元管理できます。ホストプロジェクト _ で共有 VPC ネットワークをセットアップし、 Connector および Cloud Volumes ONTAP 仮想マシンインスタンスをサービスプロジェクト _ で導入できます。 "Google Cloud のドキュメント：「 Shared VPC Overview"。

"Connector の導入でカバーされている必要な共有 VPC の権限を確認します"

VPC でのパケットミラーリング

"パケットミラーリング" Cloud Volumes ONTAPを導入するGoogle Cloudサブネットで無効にする必要があります。パケットミラーリングがイネーブルの場合、 Cloud Volumes ONTAP は正常に動作しません。

アウトバウンドインターネットアクセス

Cloud Volumes ONTAP では、ネットアップAutoSupport へのアウトバウンドのインターネットアクセスが必要です。ネットアップは、システムの健常性をプロアクティブに監視し、ネットアップテクニカルサポートにメッセージを送信します。

Cloud Volumes ONTAP が AutoSupport メッセージを送信できるように、ルーティングポリシーとファイアウォールポリシーで次のエンドポイントへの HTTP / HTTPS トラフィックを許可する必要があります。

- \ https://support.netapp.com/aods/asupmessage
- \ https://support.netapp.com/asupprod/post/1.0/postAsup

AutoSupport メッセージの送信にアウトバウンドのインターネット接続が使用できない場合、Cloud Volumes ONTAP システムは自動的にコネクタをプロキシサーバとして使用するように設定されます。唯一の要件は、コネクタのファイアウォールがポート3128上の_INBOUND接続を許可することです。コネクタを展開した後、このポートを開く必要があります。

Cloud Volumes ONTAP に厳密なアウトバウンドルールを定義した場合は、Cloud Volumes ONTAP ファイアウォールがポート3128で_OUTBOUND接続を許可することも必要です。

アウトバウンドのインターネットアクセスが使用可能であることを確認したら、 AutoSupport をテストしてメッセージを送信できることを確認します。手順については、を参照してください "ONTAP のドキュメント：「 AutoSupport のセットアップ"。

HA ペアを使用している場合、 HA メディエーターではアウトバウンドのインターネットアクセスは必要ありません。

AutoSupport メッセージを送信できないことがBlueXPから通知された場合は、 "AutoSupport 構成のトラブルシューティングを行います"。

ファイアウォールルール

ファイアウォールルールを作成する必要はありません。BlueXPはファイアウォールルールを作成します。独自のファイアウォールを使用する必要がある場合は、以下のファイアウォールルールを参照してください。

HA 構成には、次の 2 組のファイアウォールルールが必要です。

- VPC -0 の HA コンポーネントのルールセット。これらのルールにより、 Cloud Volumes ONTAP へのデータアクセスが可能になります。 詳細はこちら。。
- VPC -1 、 VPC -2 、および VPC -3 の HA コンポーネントに関するもう 1 つのルールセット。これらのルールは、 HA コンポーネント間のインバウンド通信とアウトバウンド通信に対してオープンです。詳細はこちら。。

コールドデータを Google Cloud Storage バケットに階層化する場合は、 Cloud Volumes ONTAP が配置されているサブネットをプライベート Google Access 用に設定する必要があります（ HA ペアを使用している場合、これは VPC 0 のサブネットです）。手順については、を参照してください "Google Cloud のドキュメント：「 Configuring Private Google Access"。

BlueXPでデータの階層化を設定するために必要な追加手順については'を参照してください "コールドデータを低コストのオブジェクトストレージに階層化する"。

他のネットワーク内の **ONTAP** システムへの接続

Google Cloud内のCloud Volumes ONTAP システムと他のネットワーク内のONTAP システムの間でデータをレプリケートするには、VPCと他のネットワーク（たとえば、社内ネットワーク）の間にVPN接続が必要です。

手順については、を参照してください "Google Cloud のドキュメント：「 Cloud VPN Overview"。

ファイアウォールルール

BlueXPは、Cloud Volumes ONTAP が正常に動作するために必要なインバウンドとアウトバウンドのルールを含むGoogle Cloudファイアウォールルールを作成します。テスト目的や独自のファイアウォールルールを使用する場合は、ポートを参照してください。

Cloud Volumes ONTAP のファイアウォールルールには、インバウンドとアウトバウンドの両方のルールが必要です。HA 構成を導入する場合は、 VPC 0 の Cloud Volumes ONTAP のファイアウォールルールを以下に示します。

HA 構成には、次の 2 組のファイアウォールルールが必要です。

- VPC -0 の HA コンポーネントのルールセット。これらのルールにより、 Cloud Volumes ONTAP へのデータアクセスが可能になります。
- VPC -1 、 VPC -2 、および VPC -3 の HA コンポーネントに関するもう 1 つのルールセット。これらのルールは、 HA コンポーネント間のインバウンド通信とアウトバウンド通信に対してオープンです。 詳細はこちら。。

コネクタに関する情報をお探しですか？ "コネクタのファイアウォールルールを表示します"

インバウンドルール

作業環境を作成する場合、展開時に定義済みファイアウォールポリシーのソースフィルタを選択できます。

- 選択した**VPC**のみ：インバウンドトラフィックのソースフィルタは、Cloud Volumes ONTAP システムのVPCのサブネット範囲、およびコネクタが存在するVPCのサブネット範囲です。これが推奨されるオプションです。
- *すべてのVPC *：インバウンドトラフィックのソースフィルタは0.0.0.0/0のIP範囲です。

独自のファイアウォールポリシーを使用する場合は、Cloud Volumes ONTAP と通信する必要のあるすべてのネットワークを追加し、内部のGoogleロードバランサが正常に機能するように両方のアドレス範囲を追加してください。これらのアドレスは 130.211.0.0/22 および 35.191.0.0/16 です。詳細については、を参照してください "Google Cloud ドキュメント：ロードバランサファイアウォールルール"。

プロトコル	ポート	目的
すべての ICMP	すべて	インスタンスの ping を実行します
HTTP	80	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTP アクセス
HTTPS	443	コネクタへの接続と、クラスタ管理LIFのIPアドレスを使用したSystem Manager Web コンソールへのHTTPSアクセス
SSH	22	クラスタ管理 LIF またはノード管理 LIF の IP アドレスへの SSH アクセス
TCP	111	NFS のリモートプロシージャコール
TCP	139	CIFS の NetBIOS サービスセッション
TCP	161-162	簡易ネットワーク管理プロトコル
TCP	445	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
TCP	635	NFS マウント
TCP	749	Kerberos
TCP	2049	NFS サーバデーモン

プロトコル	ポート	目的
TCP	3260	iSCSI データ LIF を介した iSCSI アクセス
TCP	4045	NFS ロックデーモン
TCP	4046	NFS のネットワークステータスモニタ
TCP	10000	NDMP を使用したバックアップ
TCP	11104	SnapMirror のクラスタ間通信セッションの管理
TCP	11105	クラスタ間 LIF を使用した SnapMirror データ転送
TCP	63001-63050	プローブポートをロードバランシングして、どのノードが正常であるかを判断します（ HA ペアの場合のみ必要）
UDP	111	NFS のリモートプロシージャコール
UDP	161-162	簡易ネットワーク管理プロトコル
UDP	635	NFS マウント
UDP	2049	NFS サーバデーモン
UDP	4045	NFS ロックデーモン
UDP	4046	NFS のネットワークステータスモニタ
UDP	4049	NFS rquotad プロトコル

アウトバウンドルール

Cloud Volumes 用の事前定義済みセキュリティグループ ONTAP は、すべての発信トラフィックをオープンします。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

Cloud Volumes ONTAP 用の定義済みセキュリティグループには、次のアウトバウンドルールが含まれています。

プロトコル	ポート	目的
すべての ICMP	すべて	すべての発信トラフィック
すべての TCP	すべて	すべての発信トラフィック
すべての UDP	すべて	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、 Cloud Volumes ONTAP による発信通信に必要なポートのみを開くことができます。

source は、 Cloud Volumes ONTAP システムのインターフェイス（ IP アドレス）です。

サービス	プロトコル	ポート	ソース	宛先	目的
Active Directory	TCP	88	ノード管理 LIF	Active Directory フォレスト	Kerberos V 認証
	UDP	137	ノード管理 LIF	Active Directory フォレスト	NetBIOS ネームサービス
	UDP	138	ノード管理 LIF	Active Directory フォレスト	NetBIOS データグラムサービス
	TCP	139	ノード管理 LIF	Active Directory フォレスト	NetBIOS サービスセッション
	TCP および UDP	389	ノード管理 LIF	Active Directory フォレスト	LDAP
	TCP	445	ノード管理 LIF	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	TCP	464	ノード管理 LIF	Active Directory フォレスト	Kerberos V パスワードの変更と設定（ SET_CHANGE ）
	UDP	464	ノード管理 LIF	Active Directory フォレスト	Kerberos キー管理
	TCP	749	ノード管理 LIF	Active Directory フォレスト	Kerberos V Change & Set Password （ RPCSEC_GSS ）
	TCP	88	データ LIF （ NFS 、 CIFS 、 iSCSI ）	Active Directory フォレスト	Kerberos V 認証
	UDP	137	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS ネームサービス
	UDP	138	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS データグラムサービス
	TCP	139	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS サービスセッション
	TCP および UDP	389	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	LDAP
	TCP	445	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	TCP	464	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	Kerberos V パスワードの変更と設定（ SET_CHANGE ）
	UDP	464	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	Kerberos キー管理
	TCP	749	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	Kerberos V Change & Set Password （ RPCSEC_GSS ）

サービス	プロトコル	ポート	ソース	宛先	目的
AutoSupport	HTTPS	443	ノード管理 LIF	support.netapp.com	AutoSupport （デフォルトは HTTPS ）
	HTTP	80	ノード管理 LIF	support.netapp.com	AutoSupport （転送プロトコルが HTTPS から HTTP に変更された場合のみ）
	TCP	3128	ノード管理 LIF	コネクタ	アウトバウンドのインターネット接続が使用できない場合に、コネクタのプロキシサーバを介してAutoSupport メッセージを送信する
クラスタ	すべてのトラフィック	すべてのトラフィック	1 つのノード上のすべての LIF	もう一方のノードのすべての LIF	クラスタ間通信（ Cloud Volumes ONTAP HA のみ）
構成のバックアップ	HTTP	80	ノード管理 LIF	http://<connector-IP-address>/occm/offboxconfig	構成バックアップをコネクタに送信します。 "構成バックアップファイルについて説明します"。
DHCP	UDP	68	ノード管理 LIF	DHCP	初回セットアップ用の DHCP クライアント
DHCP	UDP	67	ノード管理 LIF	DHCP	DHCP サーバ
DNS	UDP	53	ノード管理 LIF とデータ LIF （ NFS 、 CIFS ）	DNS	DNS
NDMP	TCP	18600 ～ 18699	ノード管理 LIF	宛先サーバ	NDMP コピー
SMTP	TCP	25	ノード管理 LIF	メールサーバ	SMTP アラート。 AutoSupport に使用できます
SNMP	TCP	161	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	UDP	161	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	TCP	162	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	UDP	162	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
SnapMirror	TCP	11104	クラスタ間 LIF	ONTAP クラスタ間 LIF	SnapMirror のクラスタ間通信セッションの管理
	TCP	11105	クラスタ間 LIF	ONTAP クラスタ間 LIF	SnapMirror によるデータ転送
syslog	UDP	514	ノード管理 LIF	syslog サーバ	syslog 転送メッセージ

VPC -1、VPC -2、およびVPC -3のルール

Google Cloudでは、4つのVPC間にHA構成が導入されます。VPC -0 の HA 構成に必要なファイアウォールルール はです Cloud Volumes ONTAP については上記のリストを参照してください。

一方、BlueXPでVPC -1、VPC -2、およびVPC -3のインスタンスに対して作成される定義済みのファイアウォールルールにより、_All_protocolsとポートでの入力通信が可能になります。これらのルールに従って、 HA ノード間の通信が可能になります。

HA ノードから HA メディエーターへの通信は、ポート 3260 （ iSCSI ）を介して行われます。

> Google Cloudの新しいHAペア環境で高速な書き込み速度を有効にするには、VPC-1、VPC-2、およびVPC-3のMaximum Transmission Unit（MTU；最大伝送ユニット）が8、896バイト以上必要です。既存のVPC-1、VPC-2、およびVPC-3を8、896バイトのMTUにアップグレードする場合は、設定プロセス中にこれらのVPCを使用している既存のHAシステムをすべてシャットダウンする必要があります。

コネクタの要件

コネクタをまだ作成していない場合は、コネクタのネットワーク要件も確認してください。

- "コネクタのネットワーク要件を確認します"
- "Google Cloudのファイアウォールルール"

GCP での VPC サービスコントロールの計画

Google Cloud環境をVPC Service Controlsでロックダウンする場合は、BlueXPとCloud Volumes ONTAP がGoogle Cloud APIとどのように連携するか、またBlueXPとCloud Volumes ONTAP を展開するためのサービス境界を構成する方法について理解しておく必要があります。

vPC サービスコントロールを使用すると、信頼できる境界外の Google 管理サービスへのアクセスを制御し、信頼できない場所からのデータアクセスをブロックし、不正なデータ転送のリスクを軽減できます。 "Google Cloud VPC Service Controls の詳細をご覧ください"。

ネットアップサービスと VPC サービスコントロールの通信方法

BlueXPは、Google Cloud APIと直接通信します。これは、Google Cloudの外部の外部IPアドレス（たとえば、api.services.cloud.netapp.comから）、またはBlueXPコネクタに割り当てられた内部アドレスからGoogle Cloud内でトリガーされます。

コネクタの配置スタイルによっては、サービスの境界に対して特定の例外を設定する必要があります。

イメージ

Cloud Volumes ONTAP とBlueXPはどちらも、ネットアップが管理するGCP内のプロジェクトのイメージを使用します。組織内でホスティングされていない画像の使用をブロックするポリシーがある場合、これはBlueXP ConnectorおよびCloud Volumes ONTAP の展開に影響を与える可能性があります。

手動インストールでもコネクタを手動で導入できますが、 Cloud Volumes ONTAP プロジェクトからイメージを取得する必要があります。Connector と Cloud Volumes ONTAP を導入するには、許可されたリストを指定

する必要があります。

コネクタの配置

コネクタを導入するユーザーは、 projectId_NetApp-cloudmanager_and the project Number_14190056516_ でホストされているイメージを参照できる必要があります。

Cloud Volumes ONTAP の導入

- BlueXPサービスアカウントは、projectId_NetApp-cloudmanager_and the project number_14190056516_ でホストされているイメージをサービスプロジェクトから参照する必要があります。
- デフォルトの Google API サービスエージェントのサービスアカウントは、 projectId_NetApp-cloudmanager_and the project number_14190056516_ サービスプロジェクトからホストされているイメージを参照する必要があります。

VPC サービスコントロールを使用してこれらのイメージをプルするために必要なルールの例を次に示します。

vPC サービスは境界ポリシーを制御します

ポリシーでは、 VPC Service Controls ルールセットの例外が許可されます。ポリシーの詳細については、を参照してください "GCP VPC Service Controls Policy Documentation を参照してください"。

BlueXPで必要なポリシーを設定するには、組織内のVPC Service Controls Perimeterに移動し、次のポリシーを追加します。各フィールドは、 VPC の [Service Controls Policy] ページで指定されたオプションと一致する必要があります。また、 * すべての * ルールが必要であり、 * または * パラメーターをルールセットで使用する必要があります。

入力規則

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

または

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

または

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

出力ルール

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

上記のプロジェクト番号は、コネクタと Cloud Volumes ONTAP のイメージを格納するためにネットアップが使用する project_name cloudmanager_used です。

データ階層化とバックアップ用のサービスアカウントを作成します

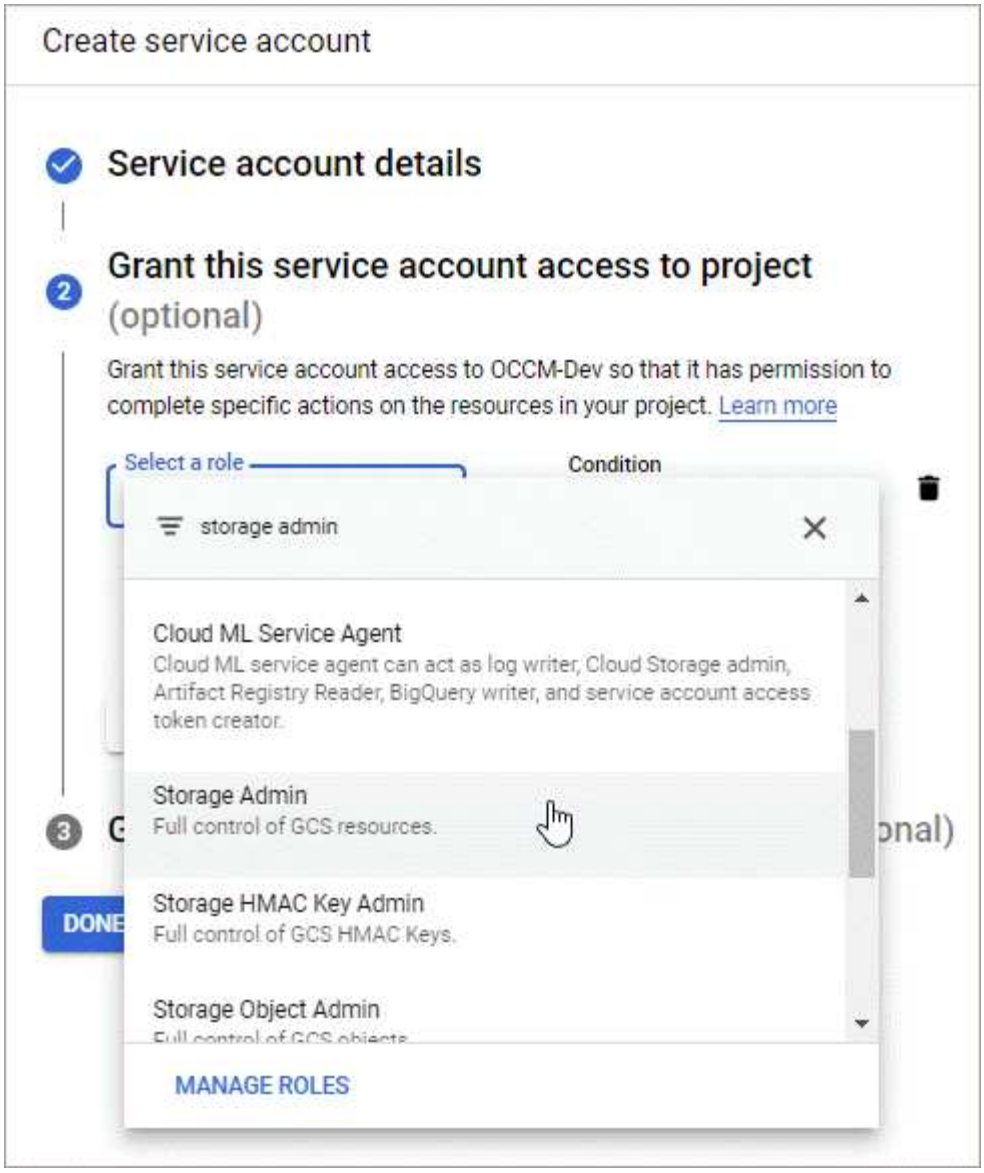
Cloud Volumes ONTAP には、 2 つの目的で Google Cloud サービスアカウントが必要です。1 つ目は、を有効にする場合です "データの階層化" Google Cloud でコールドデータを低コストのオブジェクトストレージに階層化すること。2 つ目は、を有効にした場合です "BlueXPのバックアップとリカバリ" ボリュームを低コストのオブジェクトストレージにバックアップできます。

Cloud Volumes ONTAP では、このサービスアカウントを使用して、階層化データ用のバケットとバックアップ用のバケットにアクセスして管理します。

1 つのサービスアカウントを設定して、両方の目的に使用できます。サービスアカウントには * Storage Admin * ロールが必要です。

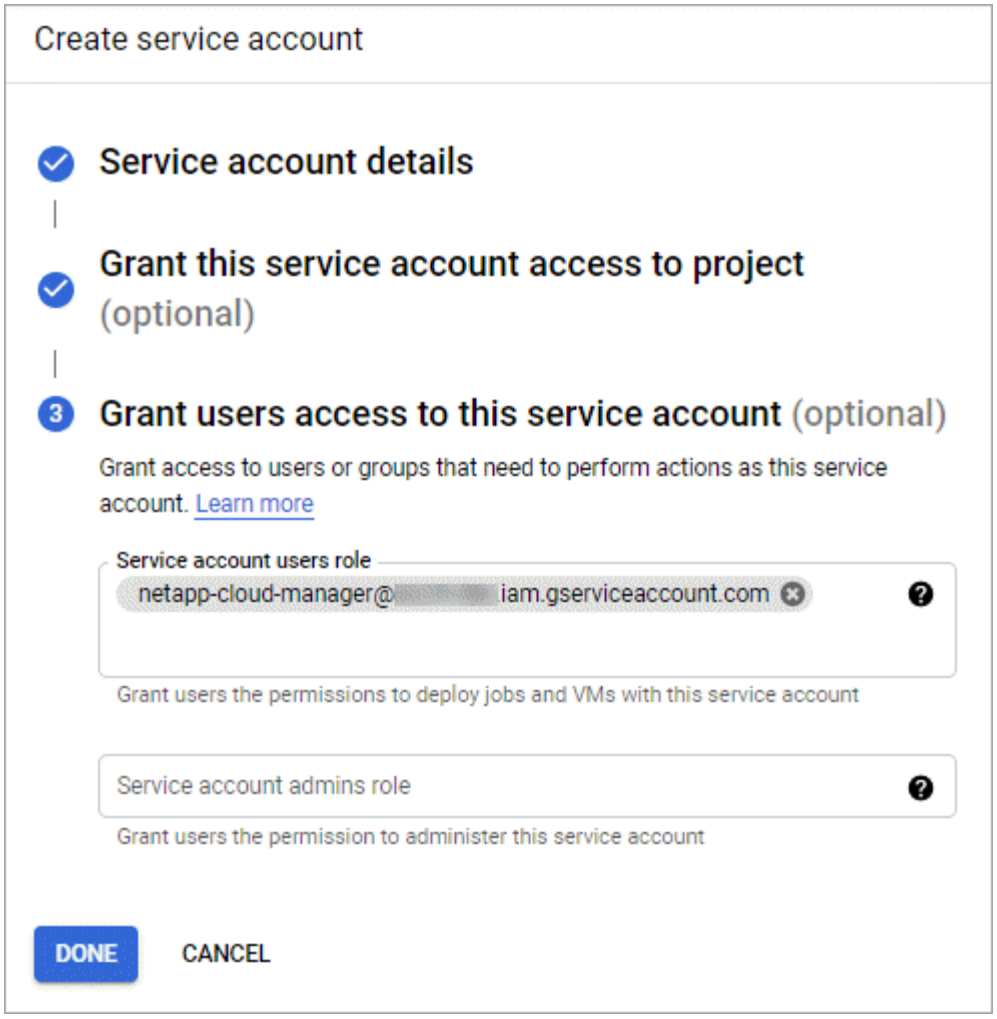
手順

1. 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"^]。
2. プロジェクトを選択します。
3. [サービスアカウントの作成] をクリックし、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を許可 * ： * ストレージ管理者 * の役割を選択します。



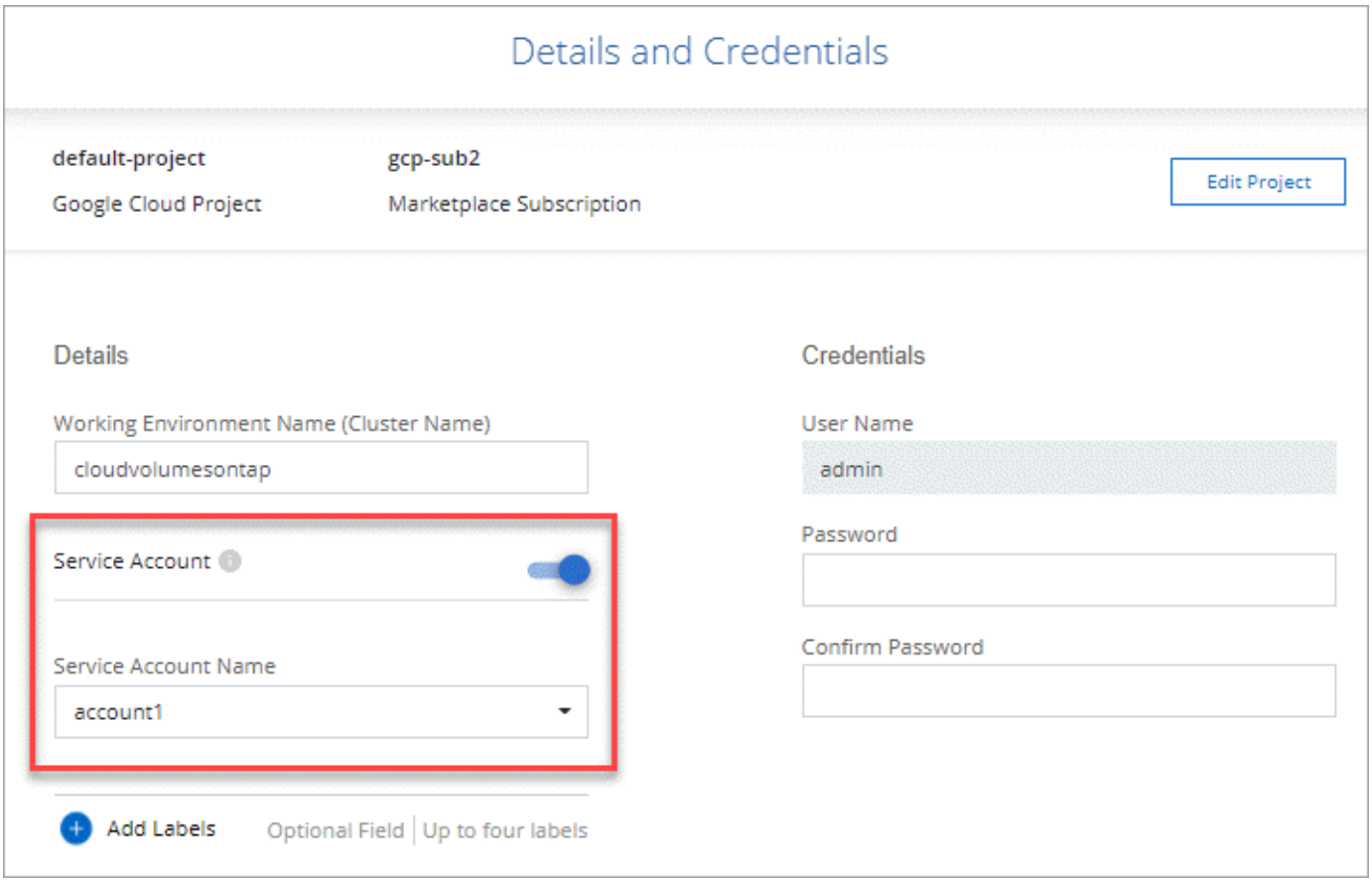
c. * このサービスアカウントへのアクセス権をユーザーに付与 *: Connector サービスアカウントを A_Service アカウント User_ としてこの新しいサービスアカウントに追加します。

この手順はデータ階層化にのみ必要です。BlueXPのバックアップとリカバリには必要ありません。



次の手順

サービスアカウントは、 Cloud Volumes ONTAP 作業環境の作成後に選択する必要があります。



ページのスクリーンショット。"]

お客様が管理する暗号化キーを **Cloud Volumes ONTAP** で使用する

Google Cloud Storageでは、データがディスクに書き込まれる前に常に暗号化されますが、BlueXP APIを使用して、_お客様が管理する暗号化キー_を使用するCloud Volumes ONTAP システムを作成できます。これらは、 Cloud Key Management Service を使用して GCP で生成および管理するキーです。

手順

1. キーが格納されているプロジェクトで、BlueXP Connectorサービスアカウントがプロジェクトレベルで正しいアクセス許可を持っていることを確認します。

   権限は、で提供されています "デフォルトでは、Connectorサービスアカウントの権限です"、ただし、Cloud Key Management Serviceに別のプロジェクトを使用する場合は適用できません。

   権限は次のとおりです。

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. のサービスアカウントを確認します "Google Compute Engine Service Agent" キーに対する Cloud KMS の

暗号化 / 復号化権限があることを確認します。

サービスアカウントの名前は、「 service-[SERVICE_PROJECT_NUMBER_@compute-system.iam.gserviceaccount.com 」という形式で指定します。

"Google Cloud のドキュメント：「 Using IAM with Cloud KMS - Granting roles on a resource"

3. 「 /GCP/VSA/meta/META/GCP-encryption-keys 」 API 呼び出しの get コマンドを呼び出すか、 GCP コンソールのキーで「 Copy Resource Name 」を選択して、キーの「 id 」を取得します。
4. お客様が管理する暗号化キーを使用し、データをオブジェクトストレージに階層化する場合、BlueXPは、永続ディスクの暗号化に使用されるのと同じキーを使用しようとします。キーを使用するには、まず Google Cloud Storage バケットを有効にする必要があります。

   a. 次の手順に従って、 Google Cloud Storage サービスエージェントを検索します "Google Cloud ドキュメント：「 Getting the Cloud Storage service agent"。

   b. 暗号化キーに移動し、 Cloud KMS 暗号化 / 復号化権限を持つ Google Cloud Storage サービスエージェントを割り当てます。

   詳細については、を参照してください "Google Cloud のドキュメント：「 Using customer-managed encryption keys"

5. 作業環境を作成するときは、 API 要求で "GcpEncryption" パラメータを使用します。

   ◦ 例 *

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-1/cryptoKeys/generatedkey1"
  }
```

を参照してください "BlueXP自動化ドキュメント" "GcpEncryption" パラメータの使用方法の詳細については、を参照してください。

Google CloudでCloud Volumes ONTAP のライセンスを設定します

Cloud Volumes ONTAP で使用するライセンスオプションを決定したら、新しい作業環境を作成する際にそのライセンスオプションを選択する前に、いくつかの手順を実行する必要があります。

フリーミアム

プロビジョニングされた容量が最大500GiBのCloud Volumes ONTAP を無料で使用するには、Freemium製品を選択してください。 "Freemium 製品の詳細をご覧ください"。

手順

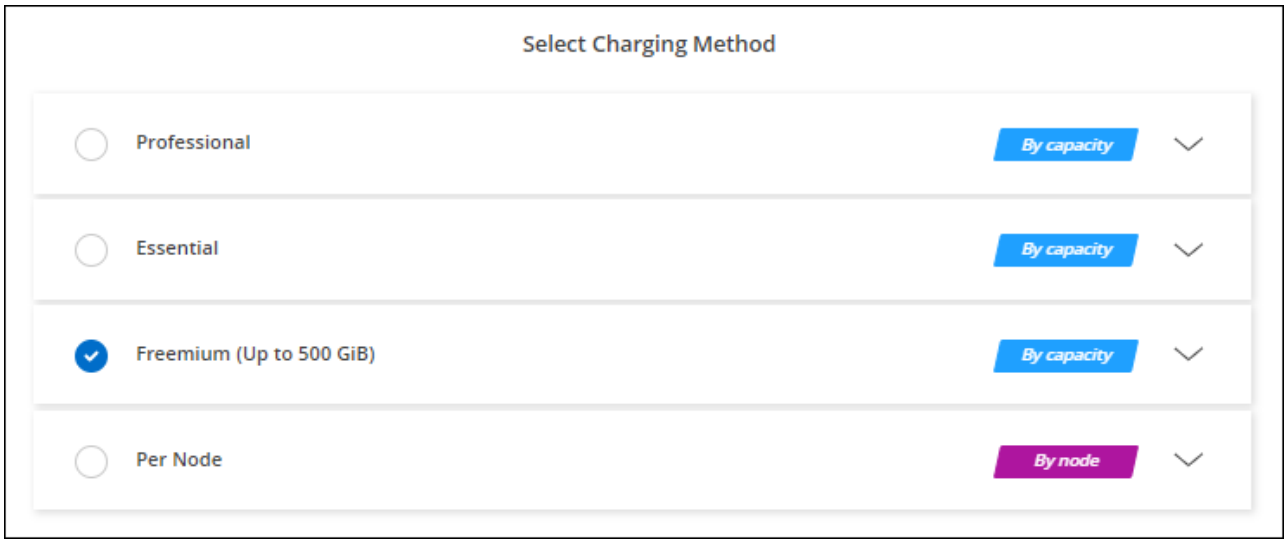
1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。

   a. [詳細と資格情報]ページで、[資格情報の編集]、[サブスクリプションの追加]の順にクリックし、プロン

プトに従ってGoogle Cloud Marketplaceでの従量課金制サービスに登録します。

プロビジョニング済み容量が500GiBを超えると、システムはに自動的に変換されないかぎり、マーケットプレイスのサブスクリプションを通じて料金が請求されることはありません "Essentials パッケージ"。

b. BlueXPに戻ったら、充電方法のページにアクセスして「* Freemium *」を選択します。



"Google CloudでCloud Volumes ONTAP を起動するための詳細な手順を表示します"。

容量単位のライセンスです

容量単位のライセンスでは、 TiB 単位の Cloud Volumes ONTAP に対して料金を支払うことができます。容量ベースのライセンスは、パッケージ：Essentialsパッケージまたはプロフェッショナルパッケージの形式で提供されます。

Essentials パッケージと Professional パッケージには、次の消費モデルがあります。

- ネットアップから購入したライセンス（ BYOL ）
- Google Cloud Marketplaceから1時間単位の従量課金制（PAYGO）サブスクリプション
- 年間契約

"容量単位のライセンスに関する詳細は、こちらをご覧ください"。

以降のセクションでは、これらの各消費モデルの使用方法について説明します。

BYOL

ネットアップからライセンスを購入（BYOL）して前払いし、任意のクラウドプロバイダにCloud Volumes ONTAP システムを導入できます。

手順

1. "ライセンスの取得については、ネットアップの営業部門にお問い合わせください"
2. "NetApp Support Site アカウントをBlueXPに追加します"

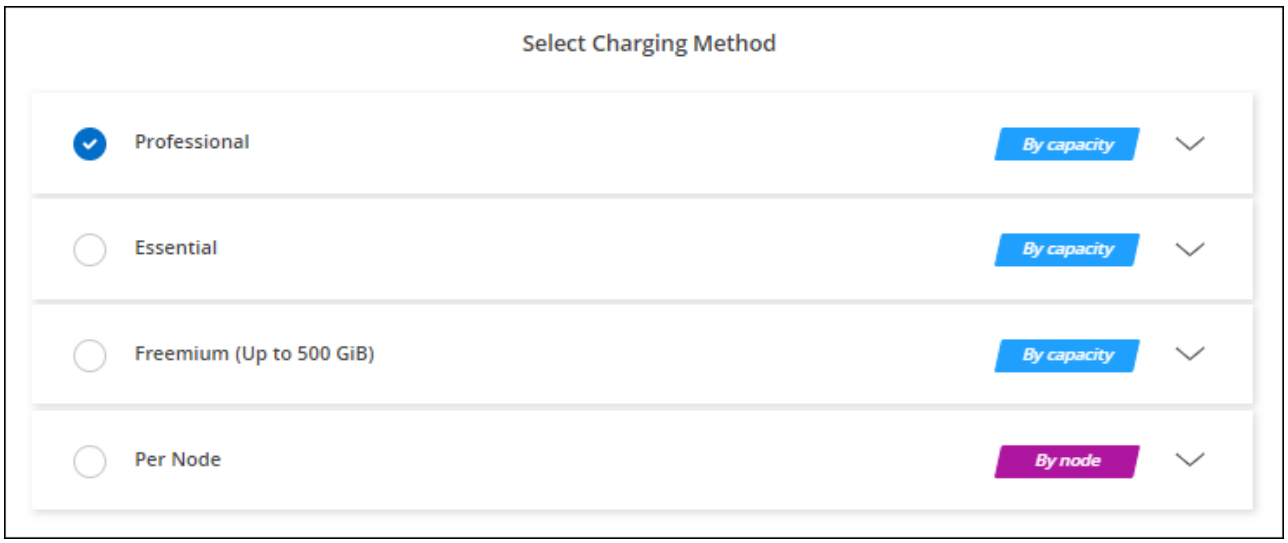
BlueXPは、ネットアップのライセンスサービスを自動的に照会し、NetApp Support Site アカウントに関連付けられているライセンスの詳細を取得します。エラーがなければ、BlueXPは自動的にライセンスをデジタルウォレットに追加します。

Cloud Volumes ONTAP でライセンスを使用するには、事前にBlueXPデジタルウォレットからライセンスを入手しておく必要があります。必要に応じて、を実行できます "ライセンスをBlueXPデジタルウォレットに手動で追加します"。

3. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. [詳細と資格情報]ページで、[資格情報の編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってGoogle Cloud Marketplaceでの従量課金制サービスに登録します。

      ネットアップから購入したライセンスには、最初に必ず料金が請求されますが、ライセンスで許可された容量を超えた場合や、ライセンスの期間が終了した場合は、マーケットプレイスで1時間ごとに料金が請求されます。

   b. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



"Google CloudでCloud Volumes ONTAP を起動するための詳細な手順を表示します"。

PAYGOサブスクリプション

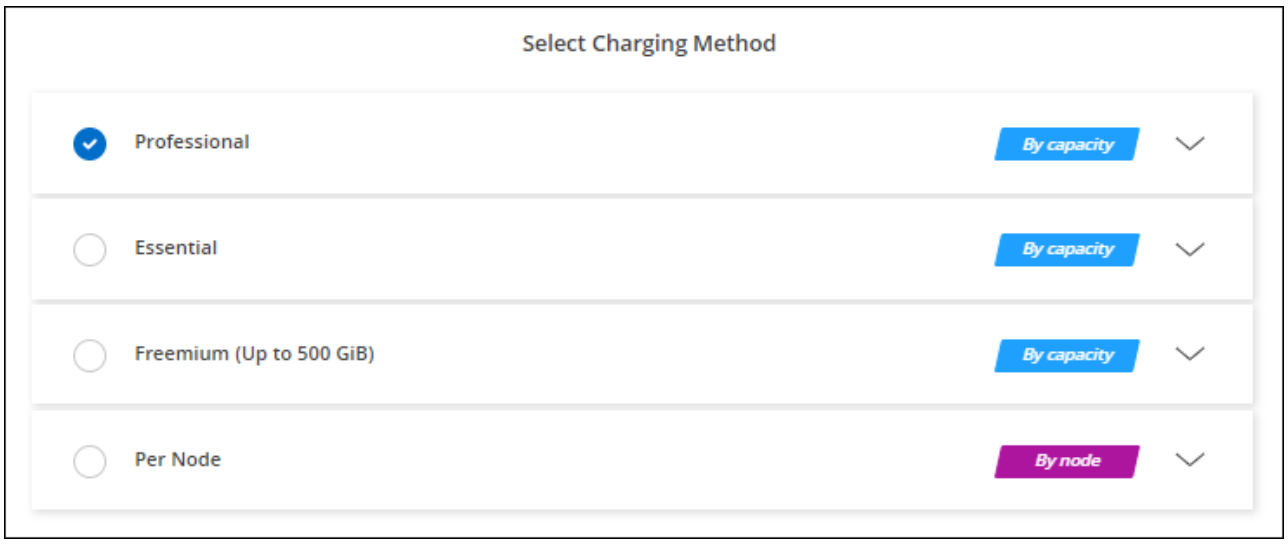
クラウドプロバイダのマーケットプレイスから提供されたサービスに登録すると、1時間ごとに料金が発生します。

Cloud Volumes ONTAP 作業環境を作成すると、Google Cloud Marketplaceで提供されている契約を購読するように求めるメッセージが表示されます。このサブスクリプションは、充電のための作業環境に関連付けられます。同じサブスクリプションを追加の作業環境に使用できます。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. [詳細と資格情報]ページで、[資格情報の編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってGoogle Cloud Marketplaceでの従量課金制サービスに登録します。

b. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



"Google CloudでCloud Volumes ONTAP を起動するための詳細な手順を表示します"。

アカウントに関連付けられたGoogle Cloud Marketplaceのサブスクリプションは、[設定]>[クレデンシャル]ページで管理できます。 "Google Cloudのクレデンシャルとサブスクリプションを管理する方法について説明します"

年間契約

年間契約を購入することで、Cloud Volumes ONTAP の年間料金をお支払いいただけます。

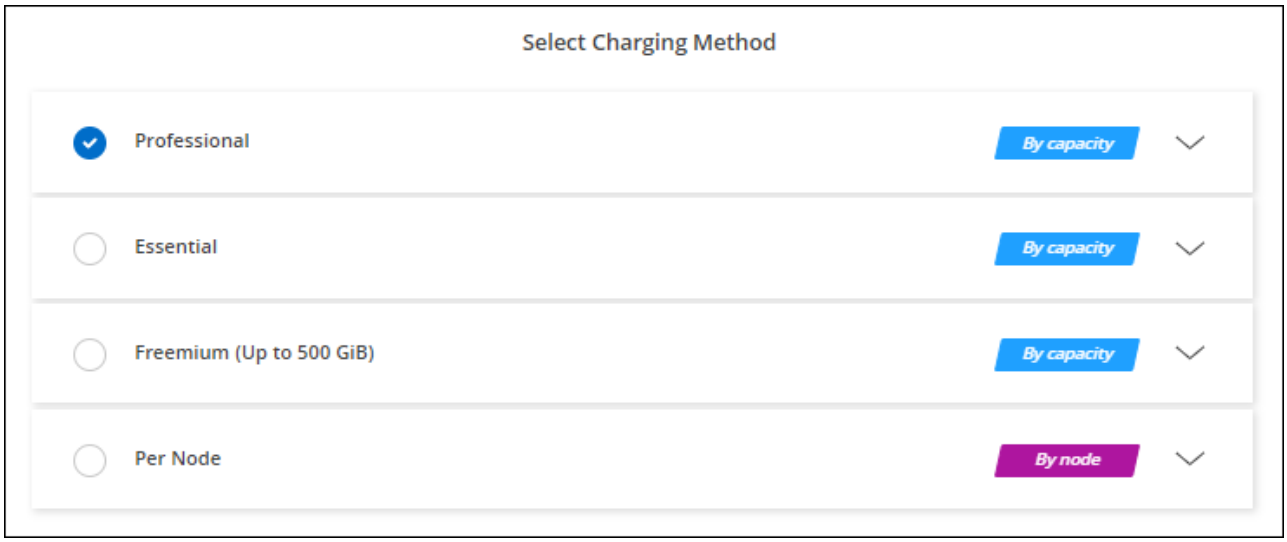
手順

1. 年間契約を購入するには、ネットアップの営業担当者にお問い合わせください。

   この契約は、Google Cloud Marketplaceで_private_offerとして提供されます。

   ネットアップがプライベートオファーを共有した後は、作業環境の作成中にGoogle Cloud Marketplaceから登録するときに、年間プランを選択できます。

2. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. [詳細と資格情報]ページで、[資格情報の編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってGoogle Cloud Marketplaceで年間プランを購読します。
   b. Google Cloudで、アカウントと共有されている年間プランを選択し、[**Subscribe**]をクリックします。
   c. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



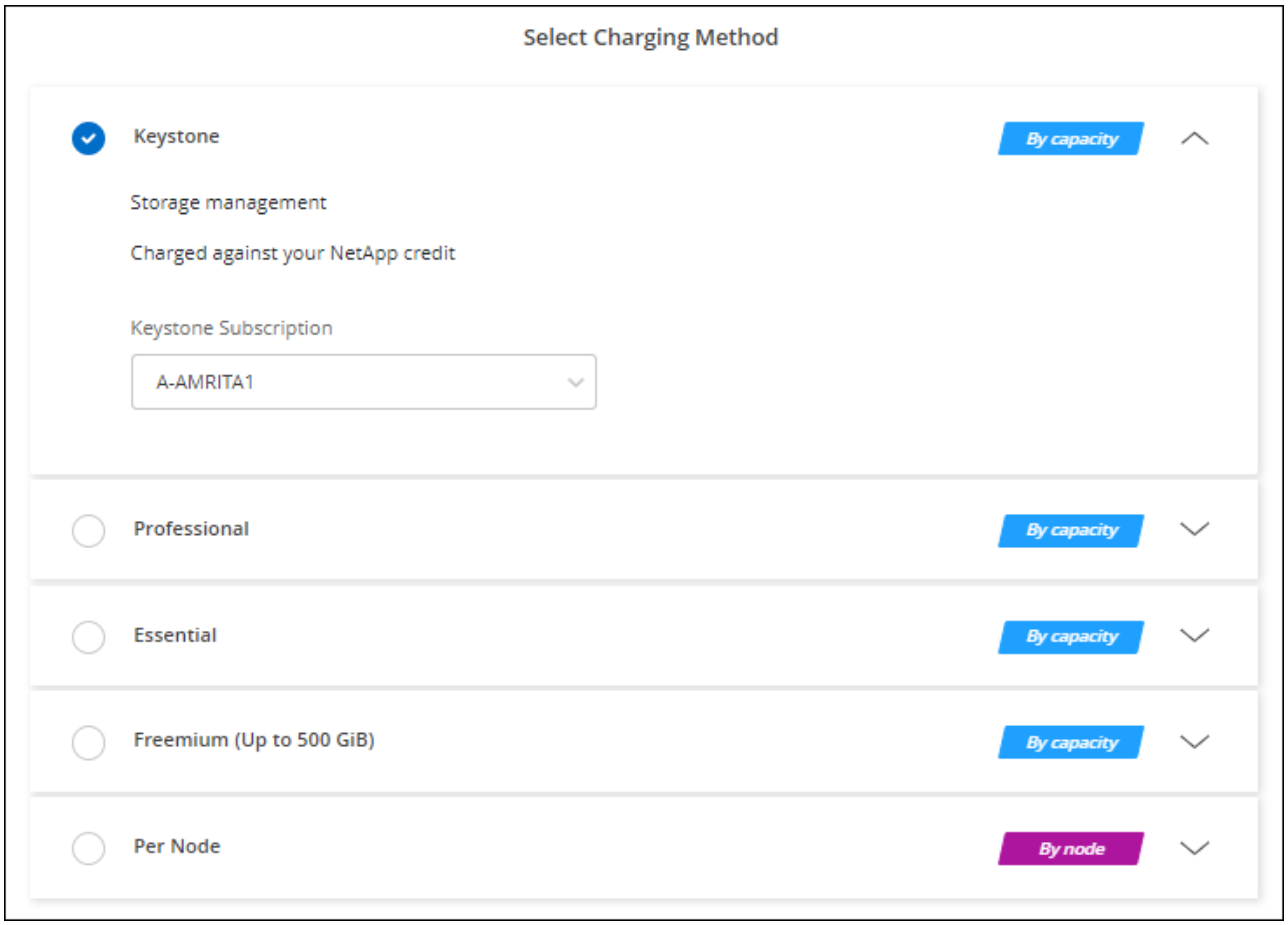
"Google CloudでCloud Volumes ONTAP を起動するための詳細な手順を表示します"。

Keystoneサブスクリプション

Keystoneサブスクリプションは、ビジネスの成長に応じたサブスクリプションベースのサービスです。
"NetApp Keystone サブスクリプションの詳細については、こちらをご覧ください"。

手順

1. まだサブスクリプションをお持ちでない場合は、 "ネットアップにお問い合わせください"
2. mailto：ng-keystone-success@netapp.com [ネットアップにお問い合わせください]。1つ以上のKeystoneサブスクリプションでBlueXPユーザアカウントを承認する場合。
3. ネットアップがお客様のアカウントを許可したあと、 "Cloud Volumes ONTAP で使用するサブスクリプションをリンクします"。
4. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. 課金方法を選択するよう求められたら、Keystoneサブスクリプションの課金方法を選択します。



オプションのスクリーンショット。"]

"Google CloudでCloud Volumes ONTAP を起動するための詳細な手順を表示します"。

Google Cloud で Cloud Volumes ONTAP を起動しています

Cloud Volumes ONTAP は、シングルノード構成またはGoogle CloudのHAペアとして起動できます。

始める前に

作業環境を作成するには、次の作業が必要です。

- 稼働中のコネクタ。
  - を用意しておく必要があります "ワークスペースに関連付けられているコネクタ"。
  - "コネクタをで実行したままにする準備をしておく必要があります 常時"。
  - コネクタに関連付けられているサービスアカウント "必要な権限がある必要があります"
- 使用する構成についての理解。

  構成を選択し、管理者からGoogle Cloudネットワーク情報を入手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 "Cloud Volumes ONTAP 構成を計画"。

- Cloud Volumes ONTAP のライセンスを設定するために必要な事項を理解する。

"ライセンスの設定方法について説明します"。

- Google Cloud API はとする必要があります "プロジェクトで有効にします"：
  - Cloud Deployment Manager V2 API
  - クラウドロギング API
  - Cloud Resource Manager API の略
  - Compute Engine API
  - ID およびアクセス管理（ IAM ） API

Google Cloudでのシングルノードシステムの起動

BlueXPで作業環境を作成し、Cloud Volumes ONTAP をGoogle Cloudで起動します。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. [[subscribe] キャンバスページで、 * 作業環境の追加 * をクリックし、プロンプトに従います。
3. * 場所を選択 * ：「 * Google Cloud * 」と「 * Cloud Volumes ONTAP * 」を選択します。
4. プロンプトが表示されたら、 "コネクタを作成します"。
5. 詳細と認証情報：プロジェクトを選択し、クラスタ名を指定します。必要に応じてサービスアカウントを選択し、ラベルを追加し、クレデンシャルを指定することもできます。

   次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
作業環境名	BlueXPは、作業環境名を使用して、Cloud Volumes ONTAP システムとGoogle Cloud VMインスタンスの両方に名前を付けます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。
サービスアカウント名	を使用する場合は "データの階層化" または "BlueXPのバックアップとリカバリ" Cloud Volumes ONTAP では、 * サービスアカウント * を有効にして、事前定義されたストレージ管理者ロールが割り当てられたサービスアカウントを選択する必要があります。 "サービスアカウントの作成方法について説明します"。
ラベルを追加します	ラベルは、Google Cloudリソースのメタデータです。BlueXPは、システムに関連付けられているCloud Volumes ONTAP システムとGoogle Cloudリソースにラベルを追加します。作業環境の作成時にユーザインターフェイスからラベルを 4 つまで追加し、その後追加することができます。API では、作業環境の作成時にラベルを 4 つに制限することはありません。ラベルの詳細については、を参照してください "Google Cloud のドキュメント：「 Labeling Resources"。
ユーザ名とパスワード	Cloud Volumes ONTAP クラスタ管理者アカウントのクレデンシャルです。このクレデンシャルを使用して、 System Manager またはその CLI から Cloud Volumes ONTAP に接続できます。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します

フィールド	説明
プロジェクトを編集します	Cloud Volumes ONTAP を配置するプロジェクトを選択します。既定のプロジェクトは、BlueXPが存在するプロジェクトです。 ドロップダウンリストに他のプロジェクトが表示されない場合は、まだBlueXPサービスアカウントを他のプロジェクトに関連付けていません。Google Cloud コンソールに移動し、 IAM サービスを開き、プロジェクトを選択します。BlueXPロールを持つサービスアカウントをそのプロジェクトに追加しますプロジェクトごとにこの手順を繰り返す必要があります。 これは、BlueXP用に設定したサービスアカウントです。 "このページで説明されているように"。 [サブスクリプションの追加] をクリックして、選択した資格情報をサブスクリプションに関連付けます。 従量課金制のCloud Volumes ONTAP システムを作成するには、Google Cloud MarketplaceからCloud Volumes ONTAP へのサブスクリプションに関連付けられているGoogle Cloudプロジェクトを選択する必要があります。

次のビデオでは、従量課金制のMarketplaceサブスクリプションをGoogle Cloudプロジェクトに関連付ける方法を紹介します。または、の手順に従って、に登録します "MarketplaceサブスクリプションとGoogle Cloudクレデンシャルの関連付け" セクション。

Google Cloud MarketplaceからBlueXPにサブスクライブ

6. * サービス * ：このシステムで使用するサービスを選択します。BlueXPのバックアップとリカバリを選択するか、BlueXPの階層化を使用するには、ステップ3でサービスアカウントを指定しておく必要があります。

   WORMとデータ階層化を活用する場合は、BlueXPのバックアップとリカバリを無効にし、バージョン9.8以降のCloud Volumes ONTAP 作業環境を導入する必要があります。

7. 場所と接続性：場所を選択し、ファイアウォールポリシーを選択して、データ階層化のためのGoogle Cloudストレージへのネットワーク接続を確認します。

   次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
接続の検証	コールドデータをGoogle Cloud Storageバケットに階層化するには、Cloud Volumes ONTAP が配置されているサブネットをプライベートGoogleアクセス用に構成する必要があります。手順については、を参照してください "Google Cloud のドキュメント：「 Configuring Private Google Access"。

フィールド	説明
ファイアウォールポリシーが生成されました	BlueXPがファイアウォールポリシーを生成するようにした場合は、トラフィックを許可する方法を選択する必要があります。 • 「* Selected VPC Only *」を選択した場合、インバウンドトラフィックのソースフィルタは、選択したVPCのサブネット範囲とコネクタが存在するVPCのサブネット範囲になります。これが推奨されるオプションです。 • どのVPC *も選択した場合、インバウンドトラフィックのソースフィルタは0.0.0.0/0のIP範囲になります。
既存のファイアウォールポリシーを使用する	既存のファイアウォールポリシーを使用する場合は、必要なルールが含まれていることを確認してください。リンク：https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/reference-networking-gcp.html#firewall-rules[Learn Cloud Volumes ONTAPのファイアウォールルールについて^]。

8. * 充電方法と NSS アカウント * ：このシステムで使用する充電オプションを指定し、ネットアップサポートサイトのアカウントを指定します。
   - "Cloud Volumes ONTAP のライセンスオプションについて説明します"。
   - "ライセンスの設定方法について説明します"。
9. * 構成済みパッケージ * ： Cloud Volumes ONTAP システムを迅速に導入するパッケージを 1 つ選択するか、 * 独自の構成を作成 * をクリックします。

   いずれかのパッケージを選択した場合は、ボリュームを指定してから、設定を確認して承認するだけで済みます。
10. ライセンス：必要に応じてCloud Volumes ONTAP バージョンを変更し、マシンタイプを選択します。

    選択したバージョンで新しいリリース候補、一般提供、またはパッチリリースが利用可能な場合、作業環境の作成時にシステムがそのバージョンに更新されます。たとえば、Cloud Volumes ONTAP 9.10.1と9.10.1 P4が利用可能になっていれば、更新が実行されます。たとえば、 9.6 から 9.7 への更新など、あるリリースから別のリリースへの更新は行われません。
11. * 基盤となるストレージリソース * ：初期アグリゲートの設定、つまりディスクタイプと各ディスクのサイズを選択します。

    ディスクタイプは初期ボリューム用です。以降のボリュームでは、別のディスクタイプを選択できます。

    シンプルなプロビジョニングオプションを使用した場合、ディスクサイズは、初期アグリゲートのすべてのディスクと、BlueXPで作成される追加のアグリゲートのサイズです。Advanced Allocation オプションを使用すると、異なるディスクサイズを使用するアグリゲートを作成できます。

    ディスクの種類とサイズの選択については、を参照してください "Google Cloudでシステムをサイジングする"。
12. * Flash Cache、書き込み速度、WORM * ：
    a. 必要に応じて、「Flash Cache」*を有効にします。

Cloud Volumes ONTAP 9.13.1以降では、n2-standard-16、n2-standard-32、n2-standard-48、およびn2-standard-64インスタンスタイプで_Flash Cache_が サポートされます。導入後にFlash Cacheを無効にすることはできません。

b. 必要に応じて、「標準」または「高速」の書き込み速度を選択します。

"書き込み速度の詳細については、こちらをご覧ください。"。

「* High * write speed」オプションを使用すると、高速な書き込み速度と最大伝送ユニット（MTU）8、896バイトを使用できます。また、MTUが8、896の場合は、導入環境でVPC-1、VPC-2、およびVPC-3を選択する必要があります。VPC-1、VPC-2、およびVPC-3の詳細については、を参照してください "VPC -1、VPC -2、およびVPC -3のルール"。

c. 必要に応じて、Write Once、Read Many（WORM）ストレージをアクティブにします。

Cloud Volumes ONTAP 9.7以前のバージョンでデータ階層化が有効になっている場合は、WORMを有効にすることはできません。Cloud Volumes ONTAP 9.8へのリバートまたはダウングレードは、WORMと階層化を有効にしたあとはブロックされます。

"WORM ストレージの詳細については、こちらをご覧ください。"。

a. WORMストレージをアクティブ化する場合は、保持期間を選択します。

13. * Google Cloud Platformでのデータ階層化*：最初のアグリゲートでデータの階層化を有効にするかどうかを選択し、階層化されたデータのストレージクラスを選択してから、事前に定義されたストレージ管理者ロール（Cloud Volumes ONTAP 9.7以降で必要）を持つサービスアカウントを選択します。または、Google Cloudアカウントを選択します（Cloud Volumes ONTAP 9.6に必要）。

次の点に注意してください。

- Cloud Volumes ONTAP インスタンスでサービスアカウントを設定します。このサービスアカウントは、 Google Cloud Storage バケットへのデータ階層化の権限を提供します。Connectorサービスアカウントを階層化サービスアカウントのユーザーとして追加してください。追加しないと、BlueXPから選択できません
- Google Cloudアカウントの追加については、を参照してください "9.6でのデータ階層化用にGoogle Cloudアカウントを設定および追加します"。
- ボリュームを作成または編集するときに、特定のボリューム階層化ポリシーを選択できます。
- データの階層化を無効にすると、以降のアグリゲートで有効にすることができますが、システムの電源をオフにして、Google Cloudコンソールからサービスアカウントを追加する必要があります。

"データ階層化の詳細については、こちらをご覧ください。"。

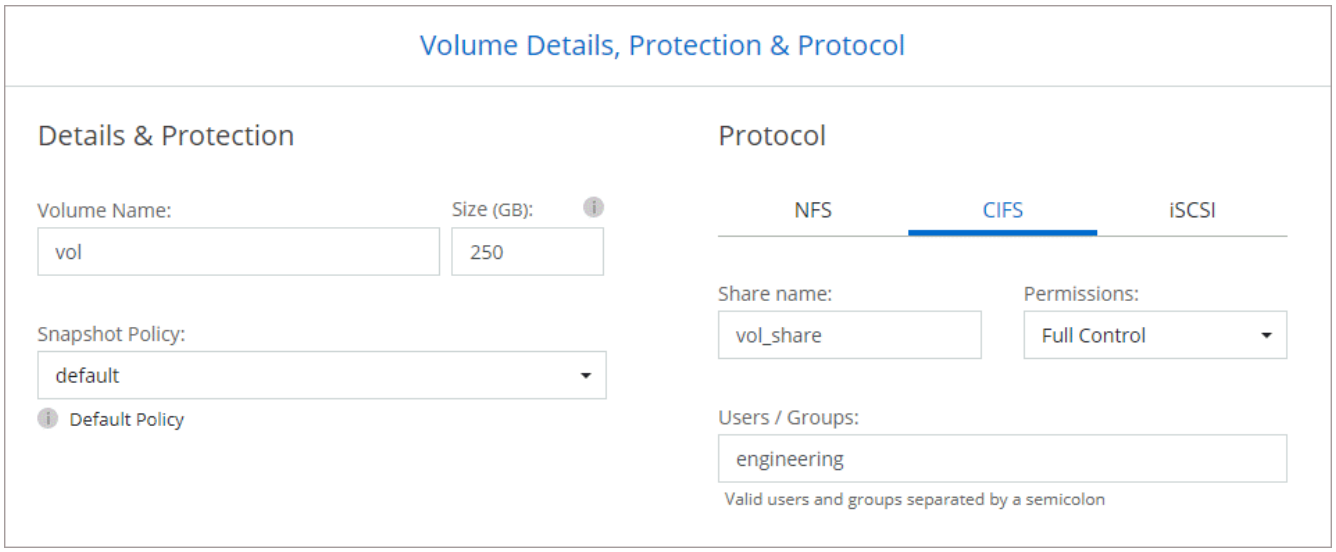
14. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

"サポートされるクライアントプロトコルおよびバージョンについて説明します"。

このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
サイズ	入力できる最大サイズは、シンプロビジョニングを有効にするかどうかによって大きく異なります。シンプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。
アクセス制御（ NFS のみ）	エクスポートポリシーは、ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、BlueXPはサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。
権限とユーザー / グループ（ CIFS のみ）	これらのフィールドを使用すると、ユーザおよびグループ（アクセスコントロールリストまたは ACL とも呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、 UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、 domain\username 形式でユーザのドメインを指定する必要があります。
スナップショットポリシー	Snapshot コピーポリシーは、自動的に作成される NetApp Snapshot コピーの頻度と数を指定します。NetApp Snapshot コピーは、パフォーマンスに影響を与えず、ストレージを最小限に抑えるポイントインタイムファイルシステムイメージです。デフォルトポリシーを選択することも、なしを選択することもできます。一時データには、 Microsoft SQL Server の tempdb など、 none を選択することもできます。
アドバンストオプション（ NFS のみ）	ボリュームの NFS バージョンを NFSv3 または NFSv4 のいずれかで選択してください。
イニシエータグループと IQN （ iSCSI のみ）	iSCSI ストレージターゲットは LUN （論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。イニシエータグループは、 iSCSI ホストのノード名のテーブルであり、どのイニシエータがどの LUN にアクセスできるかを制御します。iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（ NIC ）、ソフトウェアイニシエータを搭載した TOE カード、 CNA 、または専用の HBA を使用してネットワークに接続され、 iSCSI Qualified Name （ IQN ）で識別されます。iSCSIボリュームを作成すると、BlueXPによって自動的にLUNが作成されます。ボリュームごとに 1 つの LUN だけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、 "IQN を使用して、から LUN に接続します ホスト"。

次の図は、 CIFS プロトコルの [Volume] ページの設定を示しています。



15. * CIFS セットアップ * ： CIFS プロトコルを選択した場合は、 CIFS サーバをセットアップします。

フィールド	説明
DNS プライマリおよびセカンダリ IP アドレス	CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、 CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスロケーションレコード（ SRV ）が含まれている必要があります。Google Managed Active Directory を設定している場合は、デフォルトで 169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.x.x の IP アドレスを使用して AD にアクセスできます。
参加する Active Directory ドメイン	CIFS サーバを参加させる Active Directory （ AD ）ドメインの FQDN 。
ドメインへの参加を許可されたクレデンシャル	AD ドメイン内の指定した組織単位（ OU ）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。Google Managed Microsoft AD を Cloud Volumes ONTAP の AD サーバとして設定するには、このフィールドに「 * OU=computers 、 OU=Cloud 」と入力します。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud ドキュメント：「 Organizational Units in Google Managed Microsoft AD"^]
DNS ドメイン	Cloud Volumes ONTAP Storage Virtual Machine （ SVM ）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。
NTP サーバ	Active Directory DNS を使用して NTP サーバを設定するには、「 Active Directory ドメインを使用」を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、 API を使用してください。を参照してください "BlueXP自動化ドキュメント" を参照してください。 NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

16. * 使用状況プロファイル、ディスクタイプ、階層化ポリシー * ： Storage Efficiency 機能を有効にするかどうかを選択し、必要に応じてボリューム階層化ポリシーを変更します。

    詳細については、を参照してください "ボリュームの使用プロファイルを選択してください" および "データ階層化の概要"。

17. * レビューと承認 *: 選択内容を確認して確認します。
    a. 設定の詳細を確認します。
    b. サポートの詳細とBlueXPが購入するGoogle Cloudのリソースを確認するには、[詳細情報*]をクリックします。
    c. [* I understand … * （理解しています … * ）] チェックボックスを選択
    d. [Go*] をクリックします。

結果

BlueXPがCloud Volumes ONTAP システムを導入しましたタイムラインで進行状況を追跡できます。

Cloud Volumes ONTAP システムの導入で問題が発生した場合は、障害メッセージを確認してください。作業環境を選択し、 * 環境の再作成 * をクリックすることもできます。

詳細については、を参照してください "NetApp Cloud Volumes ONTAP のサポート"。

完了後

- CIFS 共有をプロビジョニングした場合は、ファイルとフォルダに対する権限をユーザまたはグループに付与し、それらのユーザが共有にアクセスしてファイルを作成できることを確認します。
- ボリュームにクォータを適用する場合は、 System Manager または CLI を使用します。

  クォータを使用すると、ユーザ、グループ、または qtree が使用するディスク・スペースとファイル数を制限または追跡できます。

Google CloudでのHAペアの起動

BlueXPで作業環境を作成し、Cloud Volumes ONTAP をGoogle Cloudで起動します。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. Canvas ページで、 * Add Working Environment * をクリックし、画面の指示に従います。
3. * 場所を選択 * ：「 * Google Cloud * 」と「 * Cloud Volumes ONTAP HA * 」を選択します。
4. * 詳細と認証情報 * ：プロジェクトを選択し、クラスタ名を指定します。必要に応じてサービスアカウントを選択し、ラベルを追加し、クレデンシャルを指定することもできます。

   次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
作業環境名	BlueXPは、作業環境名を使用して、Cloud Volumes ONTAP システムとGoogle Cloud VMインスタンスの両方に名前を付けます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。
サービスアカウント名	を使用する場合は "BlueXPの階層化" または "BlueXPのバックアップとリカバリ" サービスを利用するには、 * Service Account * スイッチを有効にし、事前定義された Storage Admin ロールが割り当てられたサービスアカウントを選択する必要があります。
ラベルを追加します	ラベルは、Google Cloudリソースのメタデータです。BlueXPは、システムに関連付けられているCloud Volumes ONTAP システムとGoogle Cloudリソースにラベルを追加します。作業環境の作成時にユーザインターフェイスからラベルを 4 つまで追加し、その後追加することができます。API では、作業環境の作成時にラベルを 4 つに制限することはありません。ラベルの詳細については、を参照してください "Google Cloud のドキュメント：「 Labeling Resources"。

フィールド	説明
ユーザ名とパスワード	Cloud Volumes ONTAP クラスタ管理者アカウントのクレデンシャルです。このクレデンシャルを使用して、 System Manager またはその CLI から Cloud Volumes ONTAP に接続できます。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します
プロジェクトを編集します	Cloud Volumes ONTAP を配置するプロジェクトを選択します。既定のプロジェクトは、BlueXPが存在するプロジェクトです。 ドロップダウンリストに他のプロジェクトが表示されない場合は、まだBlueXPサービスアカウントを他のプロジェクトに関連付けていません。Google Cloud コンソールに移動し、 IAM サービスを開き、プロジェクトを選択します。BlueXPロールを持つサービスアカウントをそのプロジェクトに追加しますプロジェクトごとにこの手順を繰り返す必要があります。 これは、BlueXP用に設定したサービスアカウントです。 "このページで説明されているように"。 [サブスクリプションの追加] をクリックして、選択した資格情報をサブスクリプションに関連付けます。 従量課金制のCloud Volumes ONTAP システムを作成するには、Google Cloud MarketplaceからCloud Volumes ONTAP へのサブスクリプションに関連付けられているGoogle Cloudプロジェクトを選択する必要があります。

次のビデオでは、従量課金制のMarketplaceサブスクリプションをGoogle Cloudプロジェクトに関連付ける方法を紹介します。 または、の手順に従って、に登録します "Marketplaceサブスクリプションとの関連付け" セクション。

Google Cloud MarketplaceからBlueXPにサブスクライブ

5. * サービス * ：このシステムで使用するサービスを選択します。BlueXPのバックアップとリカバリを選択するか、BlueXP階層化を使用するには、ステップ3でサービスアカウントを指定しておく必要があります。

   WORMとデータ階層化を活用する場合は、BlueXPのバックアップとリカバリを無効にし、バージョン9.8以降のCloud Volumes ONTAP 作業環境を導入する必要があります。

6. *HA 配置モデル *: HA 構成用に複数のゾーン (推奨) または単一ゾーンを選択します。次に、リージョンとゾーンを選択します。

   "HA 導入モデルの詳細については、こちらをご覧ください"。

7. * 接続 * ： HA 構成の場合は 4 つの VPC 、各 VPC のサブネットを選択し、ファイアウォールポリシーを選択します。

   "ネットワーク要件の詳細については、こちらをご覧ください"。

   次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
ポリシーが生成されました	BlueXPがファイアウォールポリシーを生成するようにした場合は、トラフィックを許可する方法を選択する必要があります。 • 「* Selected VPC Only *」を選択した場合、インバウンドトラフィックのソースフィルタは、選択したVPCのサブネット範囲とコネクタが存在するVPCのサブネット範囲になります。これが推奨されるオプションです。 • どのVPC *も選択した場合、インバウンドトラフィックのソースフィルタは0.0.0.0/0のIP範囲になります。
既存のを使用します	既存のファイアウォールポリシーを使用する場合は、必要なルールが含まれていることを確認してください。 "Cloud Volumes ONTAP のファイアウォールルールについて説明します"。

8. * 充電方法と NSS アカウント * ：このシステムで使用する充電オプションを指定し、ネットアップサポートサイトのアカウントを指定します。
   - "Cloud Volumes ONTAP のライセンスオプションについて説明します"。
   - "ライセンスの設定方法について説明します"。
9. * 構成済みパッケージ * ： Cloud Volumes ONTAP システムを迅速に導入するパッケージを 1 つ選択するか、 * 独自の構成を作成 * をクリックします。

   いずれかのパッケージを選択した場合は、ボリュームを指定してから、設定を確認して承認するだけで済みます。
10. ライセンス：必要に応じてCloud Volumes ONTAP バージョンを変更し、マシンタイプを選択します。

    選択したバージョンで新しいリリース候補、一般提供、またはパッチリリースが利用可能な場合、作業環境の作成時にシステムがそのバージョンに更新されます。たとえば、Cloud Volumes ONTAP 9.10.1と9.10.1 P4が利用可能になっていれば、更新が実行されます。たとえば、 9.6 から 9.7 への更新など、あるリリースから別のリリースへの更新は行われません。
11. * 基盤となるストレージリソース * ：初期アグリゲートの設定、つまりディスクタイプと各ディスクのサイズを選択します。

    ディスクタイプは初期ボリューム用です。以降のボリュームでは、別のディスクタイプを選択できます。

    シンプルなプロビジョニングオプションを使用した場合、ディスクサイズは、初期アグリゲートのすべてのディスクと、BlueXPで作成される追加のアグリゲートのサイズです。Advanced Allocation オプションを使用すると、異なるディスクサイズを使用するアグリゲートを作成できます。

    ディスクの種類とサイズの選択については、を参照してください "Google Cloudでシステムをサイジングする"。
12. * Flash Cache、書き込み速度、WORM * ：
    a. 必要に応じて、「Flash Cache」*を有効にします。

Cloud Volumes ONTAP 9.13.1以降では、n2-standard-16、n2-standard-32、n2-standard-48、およびn2-standard-64インスタンスタイプで_Flash Cache_が サポートされます。導入後にFlash Cacheを無効にすることはできません。

b. 必要に応じて、「標準」または「高速」の書き込み速度を選択します。

"書き込み速度の詳細については、こちらをご覧ください。"。

インスタンスタイプn2-standard-16、n2-standard-32、n2-standard-48、およびn2-standard-64では、* High * write speedオプションを使用して、高速の書き込み速度とより高いMaximum Transmission Unit（MTU；最大伝送ユニット）8、896バイトを使用できます。また、MTUが8、896の場合は、導入環境でVPC-1、VPC-2、およびVPC-3を選択する必要があります。高速の書き込み速度とMTU 8、896は機能に依存し、設定されたインスタンス内で個別に無効にすることはできません。VPC-1、VPC-2、およびVPC-3の詳細については、を参照してください "VPC -1、VPC -2、およびVPC -3のルール"。

c. 必要に応じて、Write Once、Read Many（WORM）ストレージをアクティブにします。

Cloud Volumes ONTAP 9.7以前のバージョンでデータ階層化が有効になっている場合は、WORMを有効にすることはできません。Cloud Volumes ONTAP 9.8へのリバートまたはダウングレードは、WORMと階層化を有効にしたあとはブロックされます。

"WORM ストレージの詳細については、こちらをご覧ください。"。

a. WORMストレージをアクティブ化する場合は、保持期間を選択します。

13. * Google Cloudでのデータ階層化*：最初のアグリゲートでデータの階層化を有効にするかどうかを選択し、階層化データのストレージクラスを選択してから、定義済みのStorage Adminロールを持つサービスアカウントを選択します。

次の点に注意してください。

- Cloud Volumes ONTAP インスタンスでサービスアカウントを設定します。このサービスアカウントは、 Google Cloud Storage バケットへのデータ階層化の権限を提供します。Connectorサービスアカウントを階層化サービスアカウントのユーザーとして追加してください。追加しないと、BlueXPから選択できません。
- ボリュームを作成または編集するときに、特定のボリューム階層化ポリシーを選択できます。
- データの階層化を無効にすると、以降のアグリゲートで有効にすることができますが、システムの電源をオフにして、Google Cloudコンソールからサービスアカウントを追加する必要があります。

"データ階層化の詳細については、こちらをご覧ください。"。

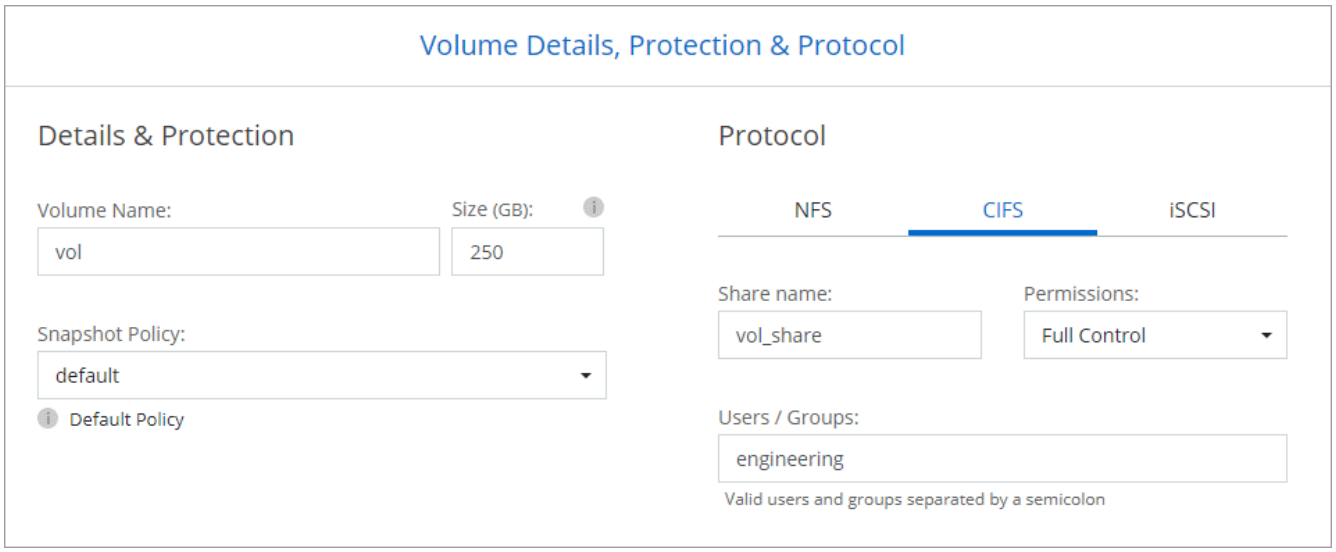
14. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

"サポートされるクライアントプロトコルおよびバージョンについて説明します"。

このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
サイズ	入力できる最大サイズは、シンプロビジョニングを有効にするかどうかによって大きく異なります。シンプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。
アクセス制御（ NFS のみ）	エクスポートポリシーは、ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、BlueXPはサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。
権限とユーザー / グループ（ CIFS のみ）	これらのフィールドを使用すると、ユーザおよびグループ（アクセスコントロールリストまたは ACL とも呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、 UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、 domain\username 形式でユーザのドメインを指定する必要があります。
スナップショットポリシー	Snapshot コピーポリシーは、自動的に作成される NetApp Snapshot コピーの頻度と数を指定します。NetApp Snapshot コピーは、パフォーマンスに影響を与えず、ストレージを最小限に抑えるポイントインタイムファイルシステムイメージです。デフォルトポリシーを選択することも、なしを選択することもできます。一時データには、 Microsoft SQL Server の tempdb など、 none を選択することもできます。
アドバンストオプション（ NFS のみ）	ボリュームの NFS バージョンを NFSv3 または NFSv4 のいずれかで選択してください。
イニシエータグループと IQN （ iSCSI のみ）	iSCSI ストレージターゲットは LUN （論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。イニシエータグループは、 iSCSI ホストのノード名のテーブルであり、どのイニシエータがどの LUN にアクセスできるかを制御します。iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（ NIC ）、ソフトウェアイニシエータを搭載した TOE カード、 CNA 、または専用の HBA を使用してネットワークに接続され、 iSCSI Qualified Name （ IQN ）で識別されます。iSCSIボリュームを作成すると、BlueXPによって自動的にLUNが作成されます。ボリュームごとに 1 つの LUN だけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、 "IQN を使用して、から LUN に接続します ホスト"。

次の図は、 CIFS プロトコルの [Volume] ページの設定を示しています。



15. * CIFS セットアップ * ： CIFS プロトコルを選択した場合は、 CIFS サーバをセットアップします。

フィールド	説明
DNS プライマリおよびセカンダリ IP アドレス	CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、 CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスロケーションレコード（ SRV ）が含まれている必要があります。Google Managed Active Directory を設定している場合は、デフォルトで 169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.x.x の IP アドレスを使用して AD にアクセスできます。
参加する Active Directory ドメイン	CIFS サーバを参加させる Active Directory （ AD ）ドメインの FQDN 。
ドメインへの参加を許可されたクレデンシャル	AD ドメイン内の指定した組織単位（ OU ）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。Google Managed Microsoft AD を Cloud Volumes ONTAP の AD サーバとして設定するには、このフィールドに「 * OU=computers 、 OU=Cloud 」と入力します。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud ドキュメント：「 Organizational Units in Google Managed Microsoft AD"^]
DNS ドメイン	Cloud Volumes ONTAP Storage Virtual Machine （ SVM ）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。
NTP サーバ	Active Directory DNS を使用して NTP サーバを設定するには、「 Active Directory ドメインを使用」を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、 API を使用してください。を参照してください "BlueXP自動化ドキュメント" を参照してください。 NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

16. * 使用状況プロファイル、ディスクタイプ、階層化ポリシー * ： Storage Efficiency 機能を有効にするかどうかを選択し、必要に応じてボリューム階層化ポリシーを変更します。

    詳細については、を参照してください "ボリュームの使用プロファイルを選択してください" および "データ階層化の概要"。

17. * レビューと承認 *: 選択内容を確認して確認します。
    a. 設定の詳細を確認します。
    b. サポートの詳細とBlueXPが購入するGoogle Cloudのリソースを確認するには、[詳細情報*]をクリックします。
    c. [* I understand … * （理解しています … * ）] チェックボックスを選択
    d. [Go*] をクリックします。

結果

BlueXPがCloud Volumes ONTAP システムを導入しましたタイムラインで進行状況を追跡できます。

Cloud Volumes ONTAP システムの導入で問題が発生した場合は、障害メッセージを確認してください。作業環境を選択し、 * 環境の再作成 * をクリックすることもできます。

詳細については、を参照してください "NetApp Cloud Volumes ONTAP のサポート"。

完了後

- CIFS 共有をプロビジョニングした場合は、ファイルとフォルダに対する権限をユーザまたはグループに付与し、それらのユーザが共有にアクセスしてファイルを作成できることを確認します。
- ボリュームにクォータを適用する場合は、 System Manager または CLI を使用します。

  クォータを使用すると、ユーザ、グループ、または qtree が使用するディスク・スペースとファイル数を制限または追跡できます。

Google Cloud Platformイメージの検証

Google Cloudの画像検証の概要

Google Cloudのイメージ検証機能は、ネットアップの高度なセキュリティ要件に準拠しています。このタスク用に特別に生成された秘密鍵を使用して、途中でイメージに署名するためのイメージを生成するスクリプトに変更が加えられました。からダウンロードできるGoogle Cloud用の署名済みダイジェストとパブリック証明書を使用して、GCPイメージの整合性を検証できます "NSS" 特定のリリースの場合。

Google Cloudイメージの検証は、Cloud Volumes ONTAP ソフトウェアバージョン9.13.0以降でサポートされています。

Google Cloudで画像をRAW形式に変換します

新しいインスタンスの導入、アップグレード、または既存のイメージで使用されているイメージは、を通じてクライアントと共有されます "NetApp Support Site （NSS）"。署名済みダイジェストと証明書は、NSSポータルからダウンロードできます。ネットアップサポートが共有しているイメージに対応する、適切なリリースのダイジェストと証明書をダウンロードしていることを確認してください。たとえば、9.13.0イメージには、9.13.0署名付きダイジェストとNSSで使用できる証明書があります。

この手順が必要なのはなぜですか？

Google Cloudからの画像は直接ダウンロードできません。署名済みダイジェストと証明書と照合してイメージを検証するには、2つのファイルを比較してイメージをダウンロードするメカニズムが必要です。これを行うには、画像をdisk.raw形式にエクスポート/変換し、結果をGoogle Cloudのストレージバケットに保存する必要があります。disk.rawファイルは、処理中にtarredおよびgzipされます。

ユーザ/サービスアカウントには、次の操作を実行するための権限が必要です。

- Googleストレージバケットへのアクセス

- Google Storageバケットに書き込みます
- クラウドビルドジョブの作成（エクスポートプロセスで使用）
- 目的の画像へのアクセス
- イメージのエクスポートタスクを作成します

イメージを検証するには、disk.raw形式に変換してからダウンロードする必要があります。

Google Cloudのコマンドラインを使用して、**Google Cloud**イメージをエクスポートします

Cloud Storageにイメージをエクスポートする場合は、を使用することを推奨します "gcloud compute images exportコマンド"。このコマンドは、提供されたイメージを取得し、tarredおよびgzipされるdisk.rawファイルに変換します。生成されたファイルは保存先URLに保存され、ダウンロードして検証することができます。

この処理を実行するには、ユーザ/アカウントに目的のバケットへのアクセスと書き込み、イメージのエクスポート、およびクラウドビルド（Googleがイメージのエクスポートに使用）の権限が必要です。

- gcloud *を使用してGoogle Cloudイメージをエクスポートします

をクリックしてスクリプトを表示します

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

圧縮されたファイルを抽出します

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

を参照してください "画像のエクスポートに関するGoogle Cloudドキュメント" Google Cloudを使用して画像をエクスポートする方法の詳細については、を参照してください。

画像署名の検証

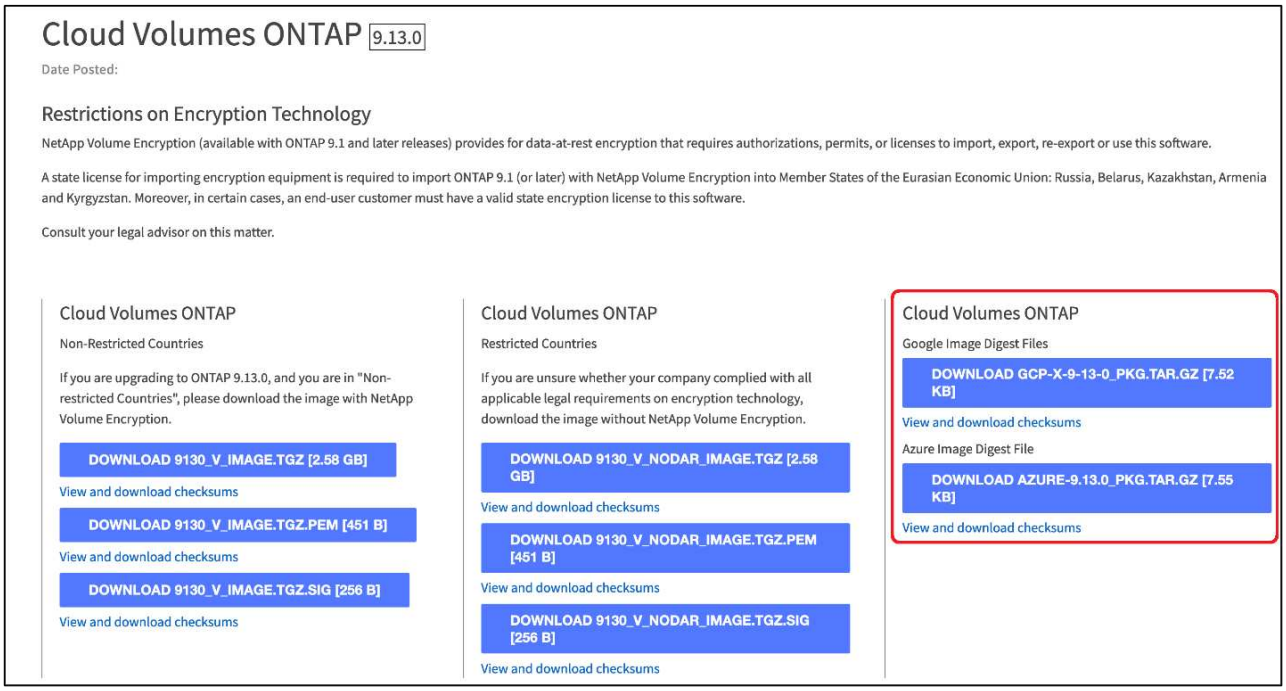
Google Cloudの署名済みイメージを検証します

エクスポートされたGoogle Cloud署名済みイメージを確認するには、NSSからイメージダイジェストファイルをダウンロードして、disk.rawファイルとダイジェストファイルの内容を検証する必要があります。

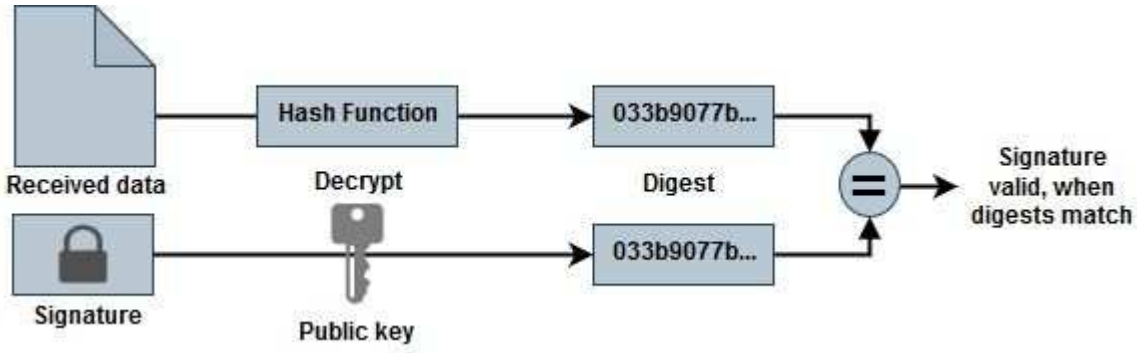
署名済み画像検証ワークフローの概要

以下は、Google Cloudの署名付き画像検証ワークフロープロセスの概要です。

- から "NSS"次のファイルを含むGoogle Cloudアーカイブをダウンロードします。
  - 署名付きダイジェスト（.sig）
  - 公開鍵（.pem）を含む証明書
  - 証明書チェーン（.pem）



- 変換されたdisk.rawファイルをダウンロードします
- 証明書チェーンを使用して証明書を検証します
- 証明書に公開鍵が含まれていることを使用して、署名済みダイジェストを検証します
  - 公開鍵を使用して署名済みダイジェストを復号化し、イメージファイルのダイジェストを抽出します
  - ダウンロードしたdisk.rawファイルのダイジェストを作成します
  - 2つのダイジェストファイルを比較して検証します



OpenSSLを使用した**disk.raw**ファイルおよびダイジェストファイルの内容の検証

Google Cloudでダウンロードしたdisk.rawファイルを、で使用できるダイジェストファイルの内容と照合して確認できます "NSS" OpenSSLを使用しています。

イメージがLinux、Mac OS、およびWindowsマシンと互換性があるかどうかを検証するOpenSSLコマンド。

手順

1. OpenSSLを使用して証明書を確認します。

をクリックしてスクリプトを表示します

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
          e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
          22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
          38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
          fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
          bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. ダウンロードしたdisk.rawファイル、署名、および証明書をディレクトリに配置します。
3. OpenSSLを使用して証明書から公開鍵を抽出します。
4. 抽出した公開鍵を使用して署名を復号化し、ダウンロードしたdisk.rawファイルの内容を確認します。

をクリックしてスクリプトを表示します

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。