



# Amazon Web Services の利用を開始しましょう Cloud Volumes ONTAP

NetApp  
May 28, 2024

# 目次

Amazon Web Services の利用を開始しましょう .....	1
AWS での Cloud Volumes ONTAP のクイックスタート .....	1
AWSでCloud Volumes ONTAP 構成を計画 .....	2
ネットワークをセットアップします .....	6
AWS KMS のセットアップ .....	27
Cloud Volumes ONTAP 用のIAMロールを設定します .....	30
AWSでCloud Volumes ONTAP のライセンスを設定 .....	39
AWS での Cloud Volumes ONTAP の起動 .....	46
AWS Secret CloudリージョンとTop Secret CloudリージョンにCloud Volumes ONTAPを導入 .....	60

# 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。

1

コネクタを作成します

を持っていない場合は ["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 ユーザー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、システムの健全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。

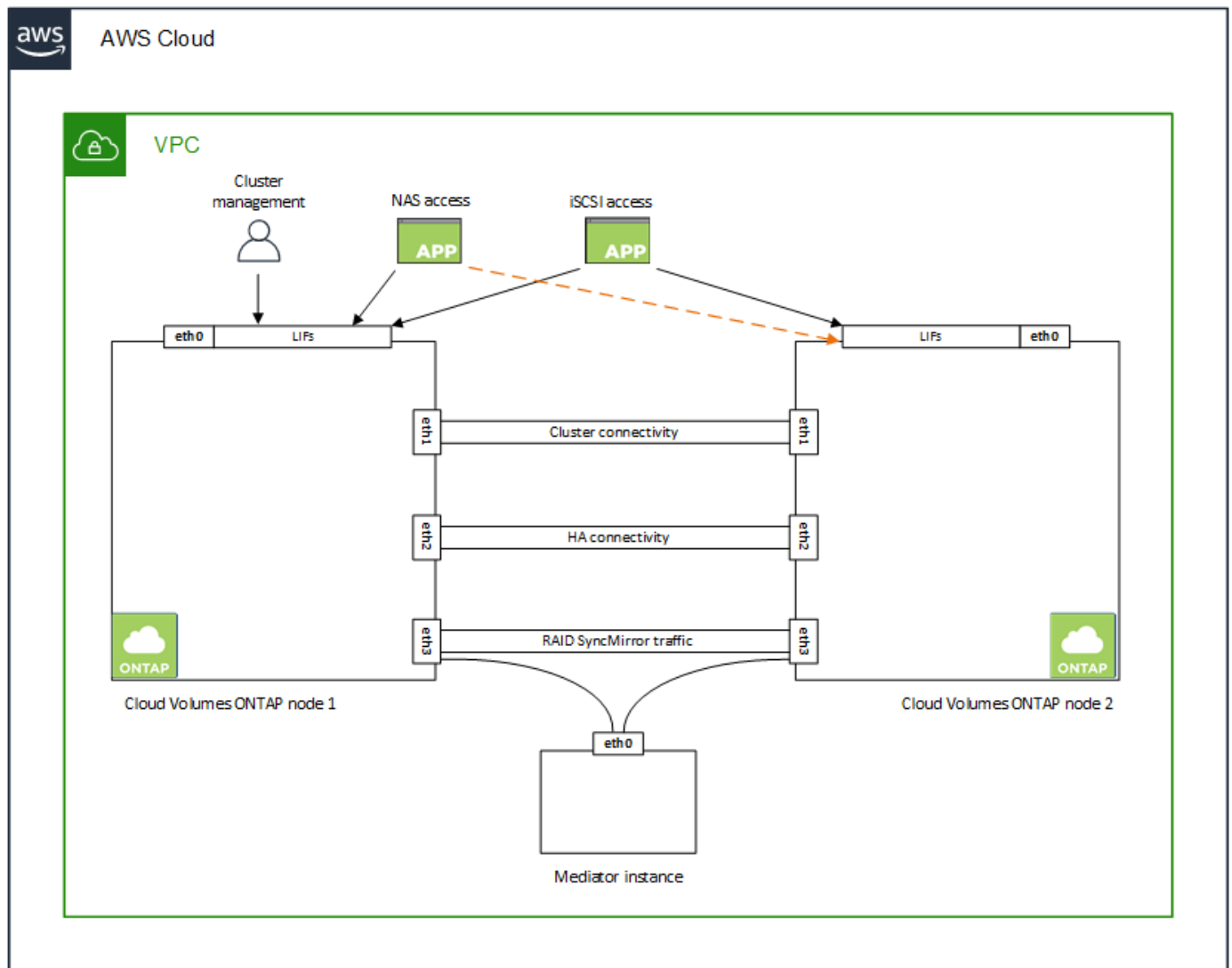
次の表に、各プライベートIPアドレスに関連付けられているLIFの詳細を示します。

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。

LIF	目的
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。
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 ノードとメディアエーター間の通信。
メディアエーター	eth0	メディアエーター	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、ノードとメディアエーターの間の通信チャンネル。

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 ノードとメディアエーター間の通信。

LIF	インターフェイス	ノード	目的
メディアエーター	eth0	メディアエーター	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、ノードとメディアエーターの間の通信チャンネル。



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ります。そのため、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ア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。



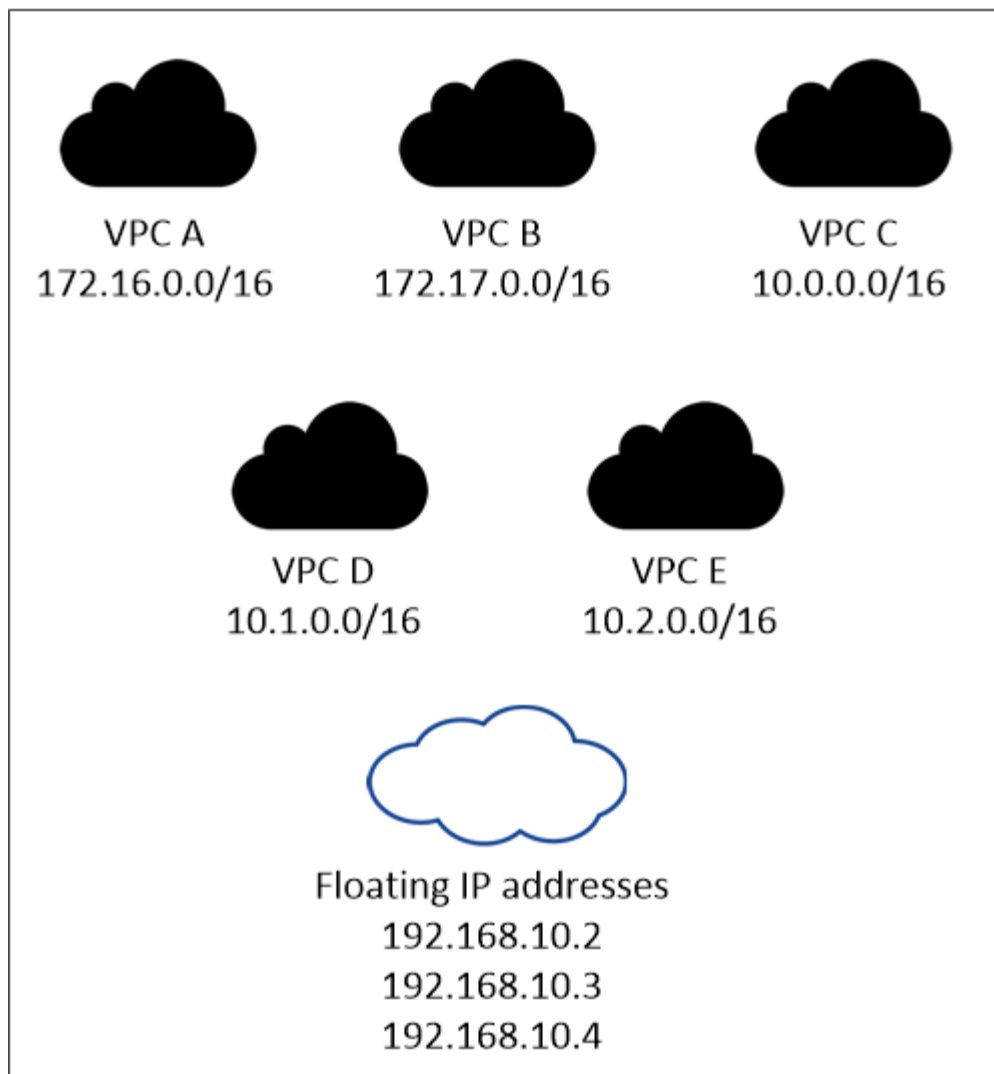
SnapCenter for Windows または SnapDrive を HA ペアで使用する場合は、SVM 管理 LIF 用にフローティング IP アドレスが必要です。

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。

## AWS region



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」](#)。

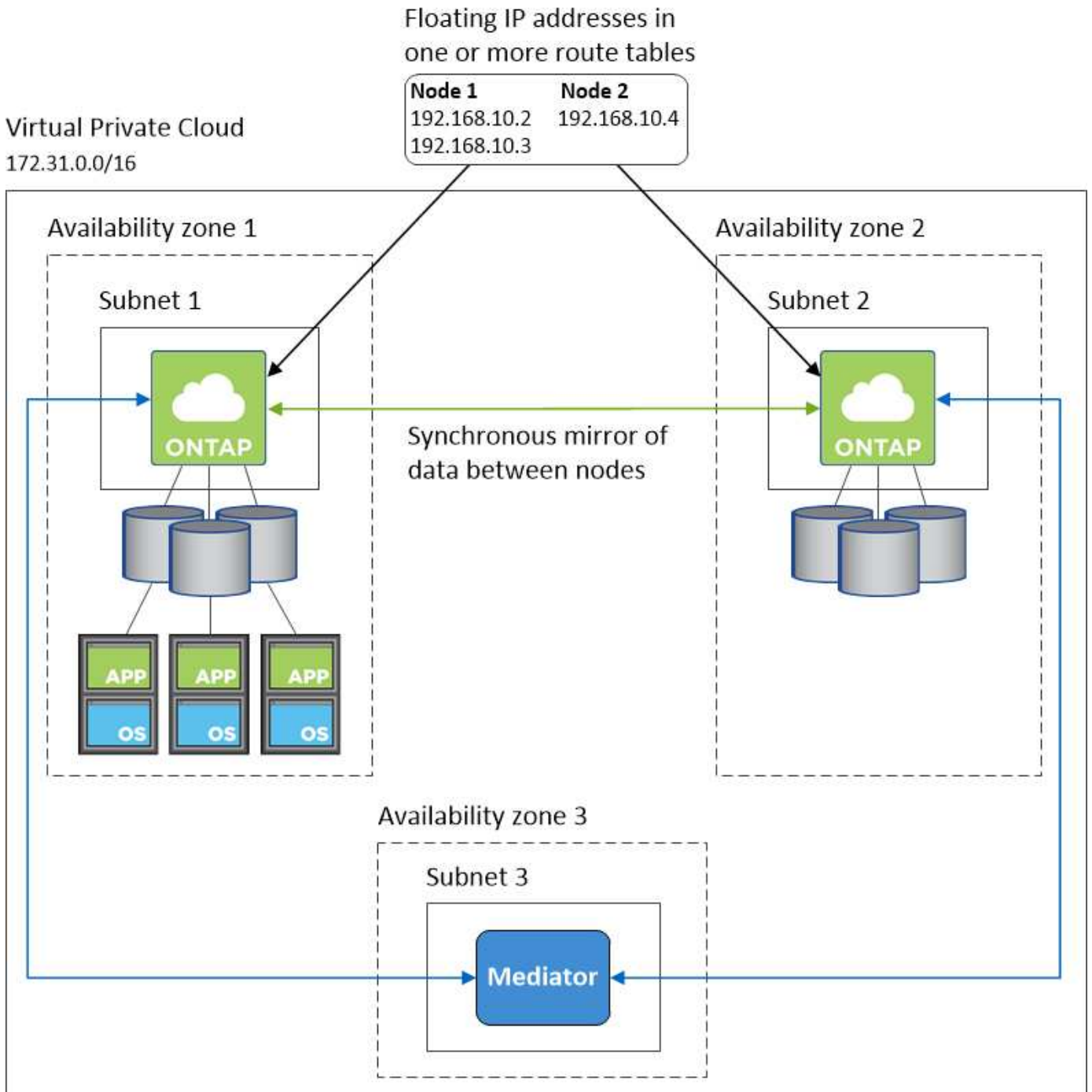
### ネットアップの管理ツールとの連携

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 Availability Zones、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

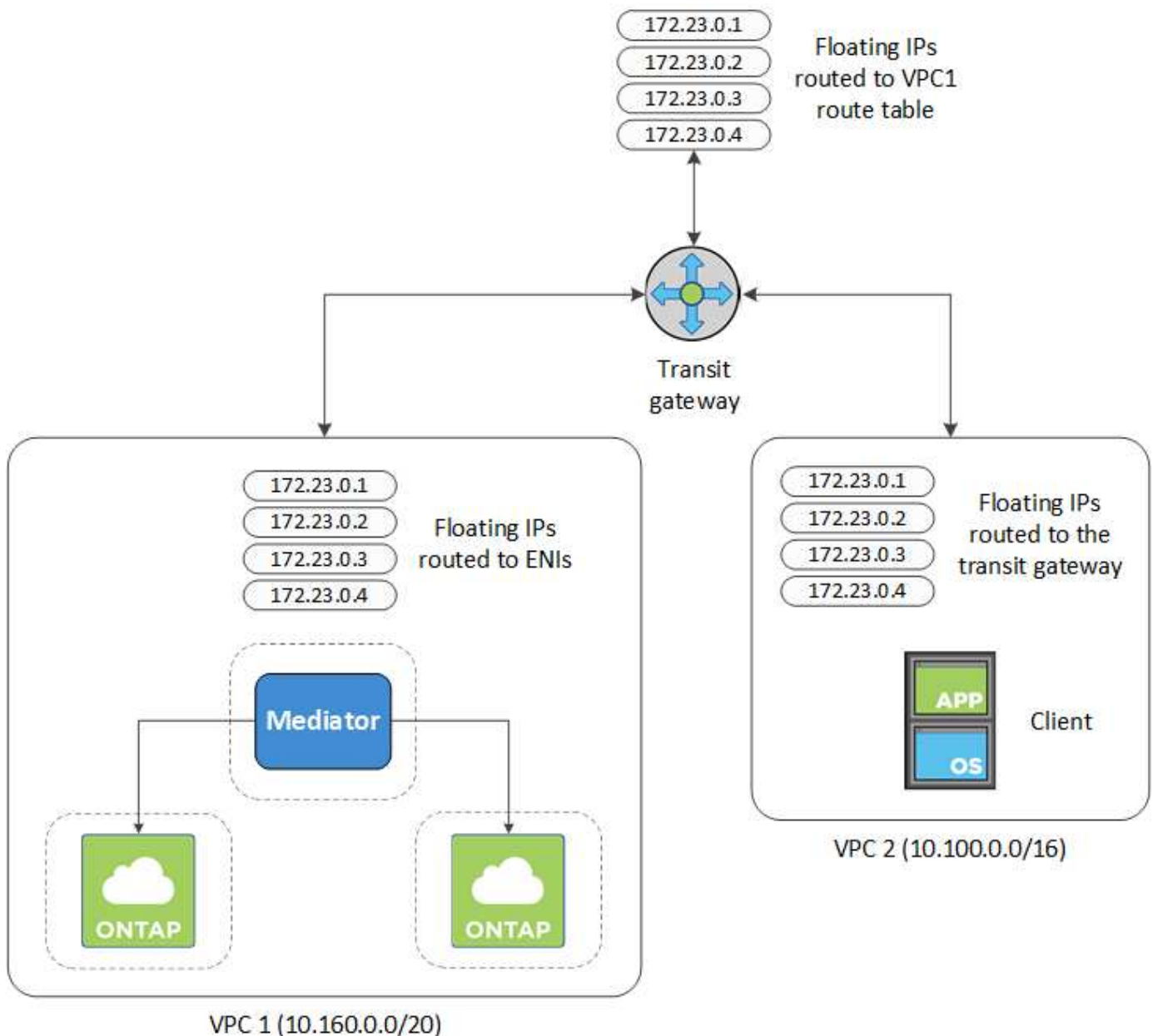


Cloud Volumes ONTAP HA 構成が複数の AWS アベイラビリティゾーンに分散されている場合は、VPC 内からの NAS データアクセス用にフローティング IP アドレスが必要です。これらのフローティング IP アドレスは、障害の発生時にノード間で移行できますが、VPC の外部からネイティブにアクセスすることはできません。VPC の外部からのデータアクセスはプライベート IP アドレスで提供されますが、自動フェイルオーバーは提供されません。

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。

## NFS & CIFS access from within the VPC using Floating IP

 Auto failover

Cluster Management : 172.23.0.1

Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

### Access

SVM Management : 172.23.0.4

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。

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aeddd3

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route

Replace routes

Delete routes

Filter by attributes or search by keyword

<input type="checkbox"/>	CIDR	Attachment	Resource type	Route type	Route state
<input type="checkbox"/>	10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8   vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
<input type="checkbox"/>	10.160.0.0/20	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC1	propagated	active
<input type="checkbox"/>	172.23.0.1/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.2/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.3/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.4/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active

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。

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	igw-07250bd01781e67df	active	No
10.160.0.0/20	tgw-015b7c249661ac279	active	No
172.23.0.1/32	tgw-015b7c249661ac279	active	No
172.23.0.2/32	tgw-015b7c249661ac279	active	No
172.23.0.3/32	tgw-015b7c249661ac279	active	No
172.23.0.4/32	tgw-015b7c249661ac279	active	No

VPC1 Floating IP Addresses

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。

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

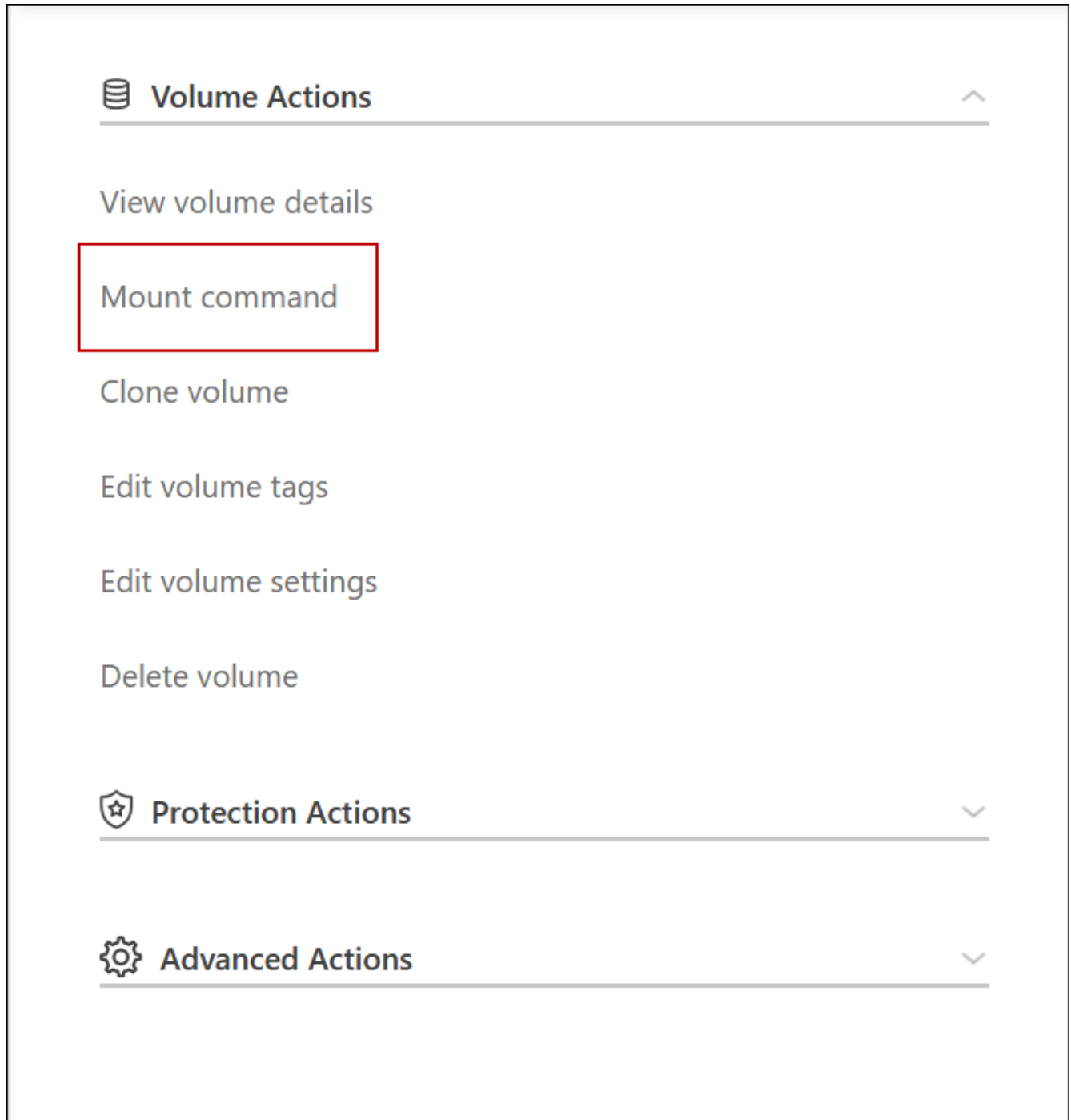
Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	igw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-ff7e1396	active
172.23.0.1/32	eni-0854d4715559c3cdb	active
172.23.0.2/32	eni-0854d4715559c3cdb	active
172.23.0.3/32	eni-0f76681216c3108ed	active
172.23.0.4/32	eni-0854d4715559c3cdb	active

VPC2 Floating IP Addresses

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

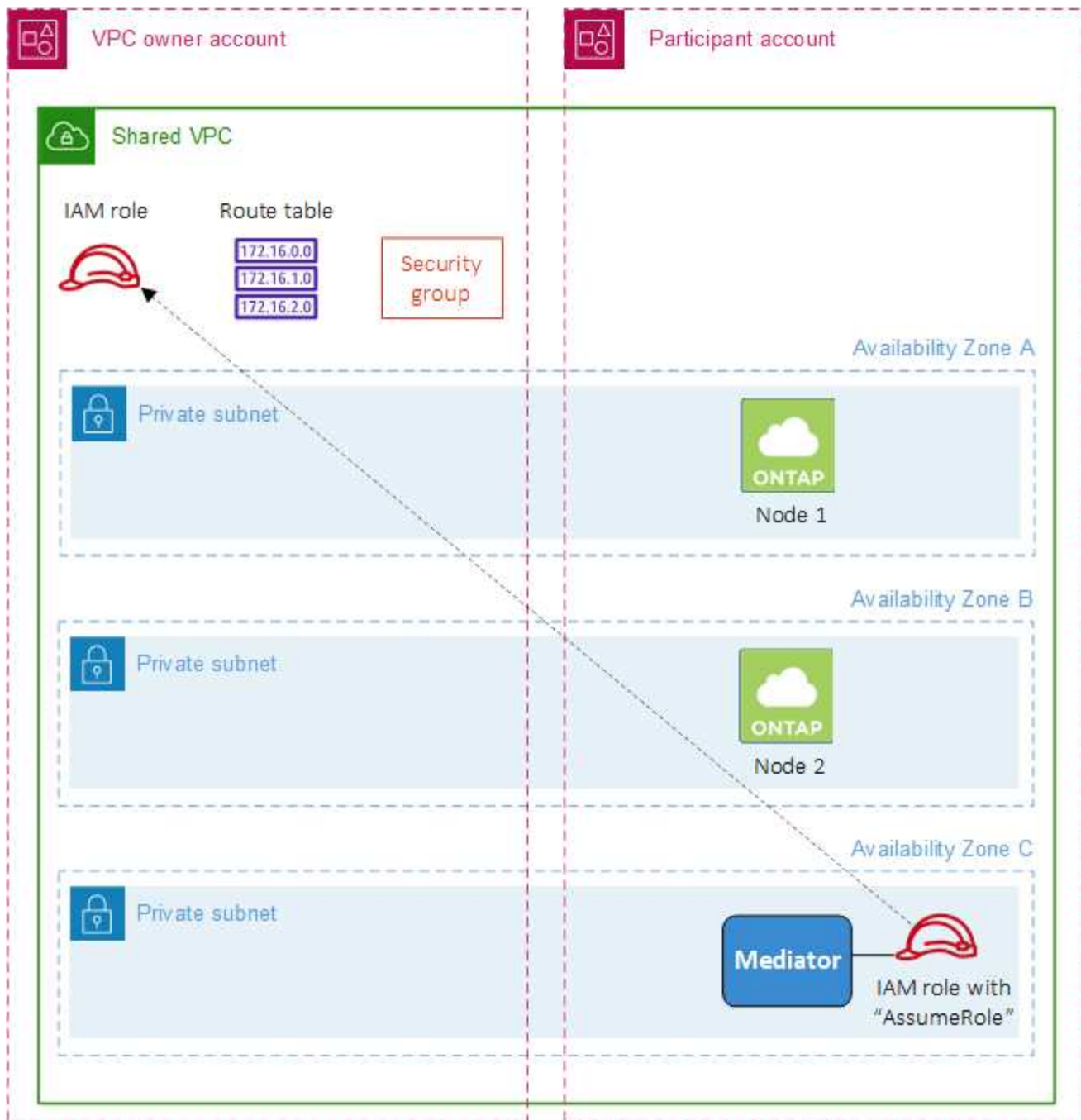
9.11.1リリース以降では、VPCを共有するAWSでCloud Volumes ONTAP HAペアがサポートされます。VPC共有を使用すると、他のAWSアカウントとサブネットを共有できます。この構成を使用するには、AWS環境をセットアップし、APIを使用してHAペアを導入する必要があります。

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ノードとメディアエーターを含む）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メディアエーターから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。メディア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メディア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"assumeRoleArn"を想定します

「仮定ロールアーン」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マニタ
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マニタ
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	1110 4	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	1110 5	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メディア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 メディアーター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 メディアーター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	メディア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ネットフェイス 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、メディア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 メディアエータと 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 メディアエータと 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」"

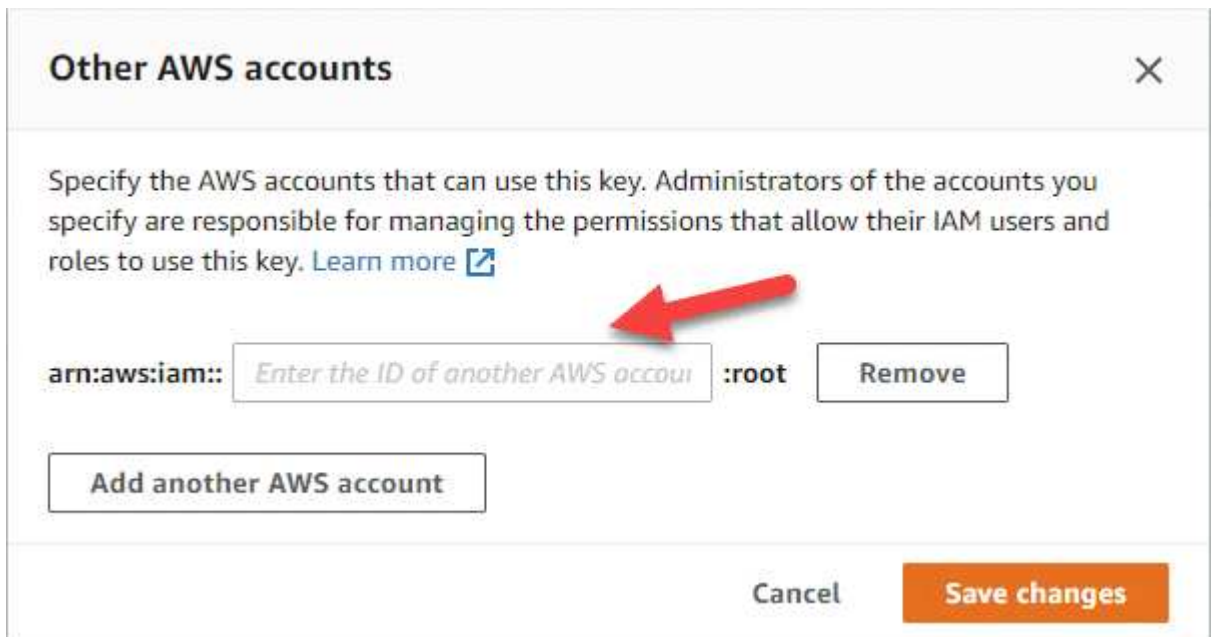
3. CMK が別の AWS アカウントにある場合は、次の手順を実行します。

- 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。
- キーを選択します。
- 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。

- [\* 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。



- 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。
- 以下の権限を含む IAM ポリシーを作成します。
- 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ーに 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メディア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、システムは自動的に変換されないかぎり、マーケットプレー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"。

**Edit Credentials & Add Subscription**

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract  
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go  
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 AWS Marketplace**  
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**  
Save your subscription and associate the Marketplace subscription with your AWS credentials.

**Continue** **Cancel**

- 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。

**Select Charging Method**

Professional **By capacity** ▾

Essential **By capacity** ▾

Freemium (Up to 500 GiB) **By capacity** ▾

Per Node **By node** ▾

"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。

## Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract

Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go

Pay for Cloud Volumes ONTAP at an hourly rate.

### The next steps:

1 AWS Marketplace

Subscribe and then click **Set Up Your Account** to configure your account.

2 Cloud Manager

Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue

Cancel

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。

### Select Charging Method

<input checked="" type="radio"/> Professional	By capacity	▼
<input type="radio"/> Essential	By capacity	▼
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity	▼
<input type="radio"/> Per Node	By node	▼

"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

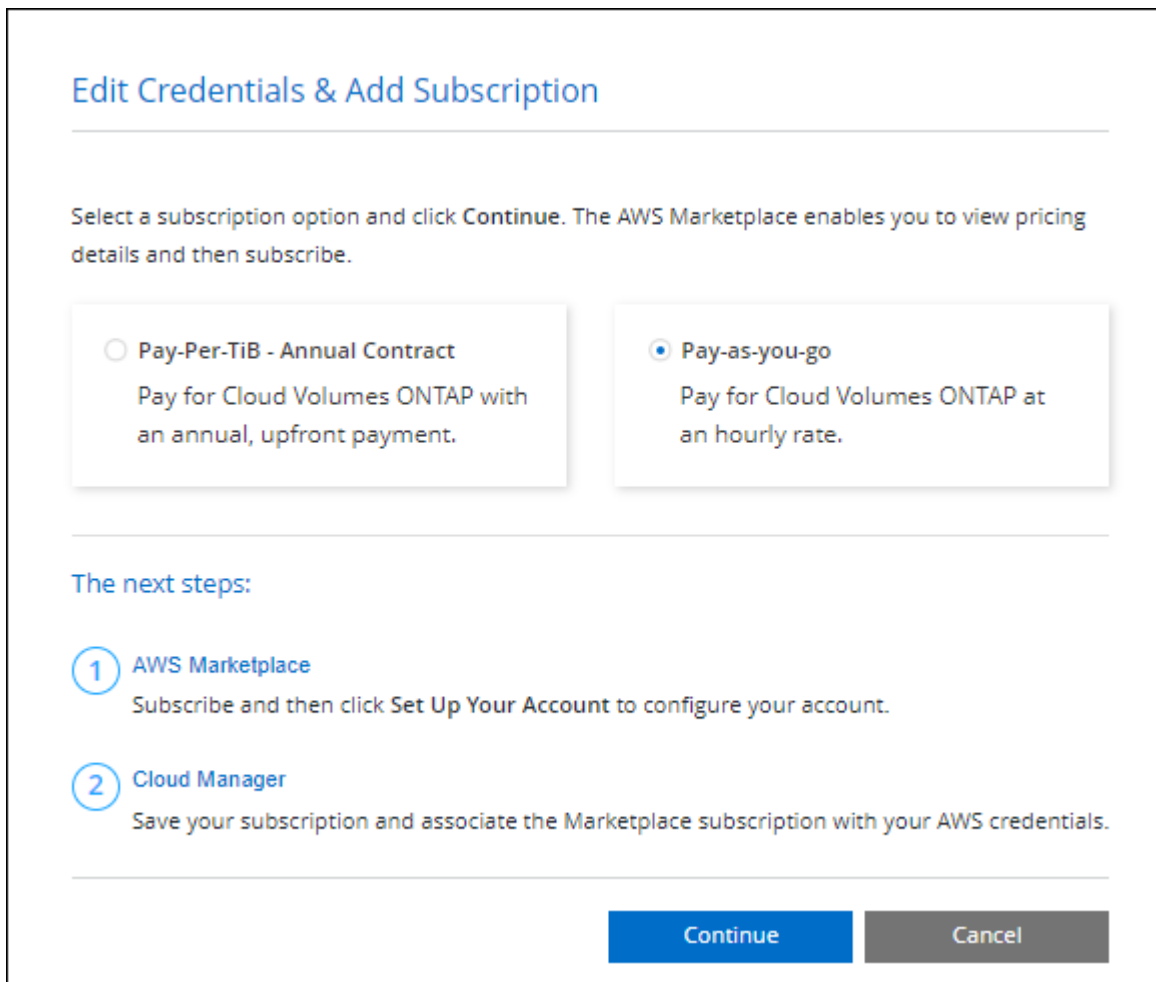
クラウドプロバイダのマーケットプレイスから提供されたサービスに登録すると、1時間ごとに料金が発生し

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。



**Edit Credentials & Add Subscription**

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

**Pay-Per-TiB - Annual Contract**  
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

**Pay-as-you-go**  
Pay for Cloud Volumes ONTAP at an hourly rate.

**The next steps:**

① **AWS Marketplace**  
Subscribe and then click **Set Up Your Account** to configure your account.

② **Cloud Manager**  
Save your subscription and associate the Marketplace subscription with your AWS credentials.

**Continue** **Cancel**

- 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。

### Select Charging Method

<input checked="" type="radio"/> Professional	By capacity	▼
<input type="radio"/> Essential	By capacity	▼
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity	▼
<input type="radio"/> Per Node	By node	▼

"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。

## Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

**Pay-Per-TiB - Annual Contract**  
 Pay for Cloud Volumes ONTAP with an annual, upfront payment.

**Pay-as-you-go**  
 Pay for Cloud Volumes ONTAP at an hourly rate.

---

**The next steps:**

- 1 **AWS Marketplace**  
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 **Cloud Manager**  
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue
Cancel

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。

### Select Charging Method

<input checked="" type="radio"/>	Professional	By capacity	▼
<input type="radio"/>	Essential	By capacity	▼
<input type="radio"/>	Freemium (Up to 500 GiB)	By capacity	▼
<input type="radio"/>	Per Node	By node	▼

"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。

Select Charging Method

Keystone By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1

Professional By capacity v

Essential By capacity v

Freemium (Up to 500 GiB) By capacity v

Per Node By node v

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 テナンスーの場合）または m3.medium（専用のvPC テナンスーの場合）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 " <a href="#">AWS ドキュメント：「Tagging your Amazon EC2 Resources」</a> "。
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に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。  <a href="#">"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"</a> 。

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。



**Cloud Manager (for Cloud Volumes ONTAP)**

---

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

**?** **Having issues signing up for your product?**  
If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

Subscribe

You are already subscribed to this product

**Pricing Details**

Software Fees

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。 <ul style="list-style-type: none"> <li>「* 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。</li> <li>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。</li> </ul>
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。 <a href="#">"Cloud Volumes ONTAP のファイアウォールルールについて説明します"</a> 。

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ー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、ユーザーおよびグループ (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 ユーザーまたはグループ、UNIX ユーザーまたはグループを指定できます。ドメインの Windows ユーザー名を指定する場合は、domain\username 形式でユーザー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、" <a href="#">"IQN を使用して、から LUN に接続します ホスト"</a> "。

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。

**Volume Details, Protection & Protocol**

Details & Protection	Protocol
Volume Name: <input style="width: 200px;" type="text" value="vol"/> Size (GB): <input style="width: 80px;" type="text" value="250"/>	NFS <b>CIFS</b> iSCSI
Snapshot Policy: <input style="width: 150px;" type="text" value="default"/>	Share name: <input style="width: 150px;" type="text" value="vol_share"/> Permissions: <input style="width: 150px;" type="text" value="Full Control"/>
<input type="checkbox"/> Default Policy	Users / Groups: <input style="width: 200px;" type="text" value="engineering"/> <p style="font-size: small;">Valid users and groups separated by a semicolon</p>

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	<p>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 <a href="#">"BlueXP自動化ドキュメント"</a> を参照してください。</p> <p>NTP サーバは、CIFS サーバを作成するときのみ設定できます。CIFS サーバを作成したあとで設定することはできません。</p>

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 テナンスーの場合）または m3.medium（専用のvPC テナンスーの場合）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。

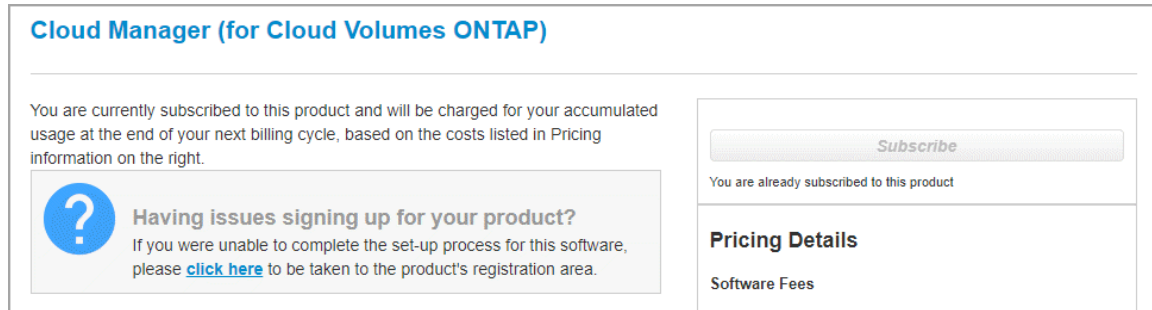
フィールド	説明
作業環境名	BlueXPでは、作業環境名を使用してCloud Volumes ONTAP システムとAmazon EC2インスタンスの両方に名前を付けます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。
タグを追加します	AWS タグは、AWS リソースのメタデータです。BlueXPは、Cloud Volumes ONTAP インスタンスとそのインスタンスに関連付けられている各AWSリソースにタグを追加します。作業環境を作成するときに、ユーザインターフェイスから最大 4 つのタグを追加し、作成後にさらに追加できます。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 " <a href="#">AWS ドキュメント：「Tagging your Amazon EC2 Resources」</a> "。
ユーザ名とパスワード	Cloud Volumes ONTAP クラスター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。  <a href="#">"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"</a> 。

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	<p>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。</p> <ul style="list-style-type: none"> <li>• 「* 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。</li> <li>• 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。</li> </ul>
既存のセキュリティグループを使用する	<p>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。 "<a href="#">Cloud Volumes ONTAP のファイアウォールルールについて説明します</a>".</p>

8. \* 接続と SSH 認証 \* : HA ペアとメディア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ー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。
アドバンスドオプション（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。

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy:

Default Policy

#### Protocol

NFS
  CIFS
  iSCSI

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

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 <a href="#">"BlueXP自動化ドキュメント"</a> 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せん。

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メディア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メディア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メディアエーター用（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メディア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 `<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a> _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ー"** 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.nif 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メディア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
  - メディアーター：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。



バケット名の先頭が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>

## 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。