



ネットワークをセットアップします

Cloud Volumes ONTAP

NetApp
May 28, 2024

目次

ネットワークをセットアップします	1
Cloud Volumes ONTAP in AWS のネットワーク要件	1
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	10
HAペアを共有サブネットに導入します	15
AWS のセキュリティグループルール	17

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/aods/asupmessage)
- [\ https://support.netapp.com/asupprod/post/1.0/postAsup](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

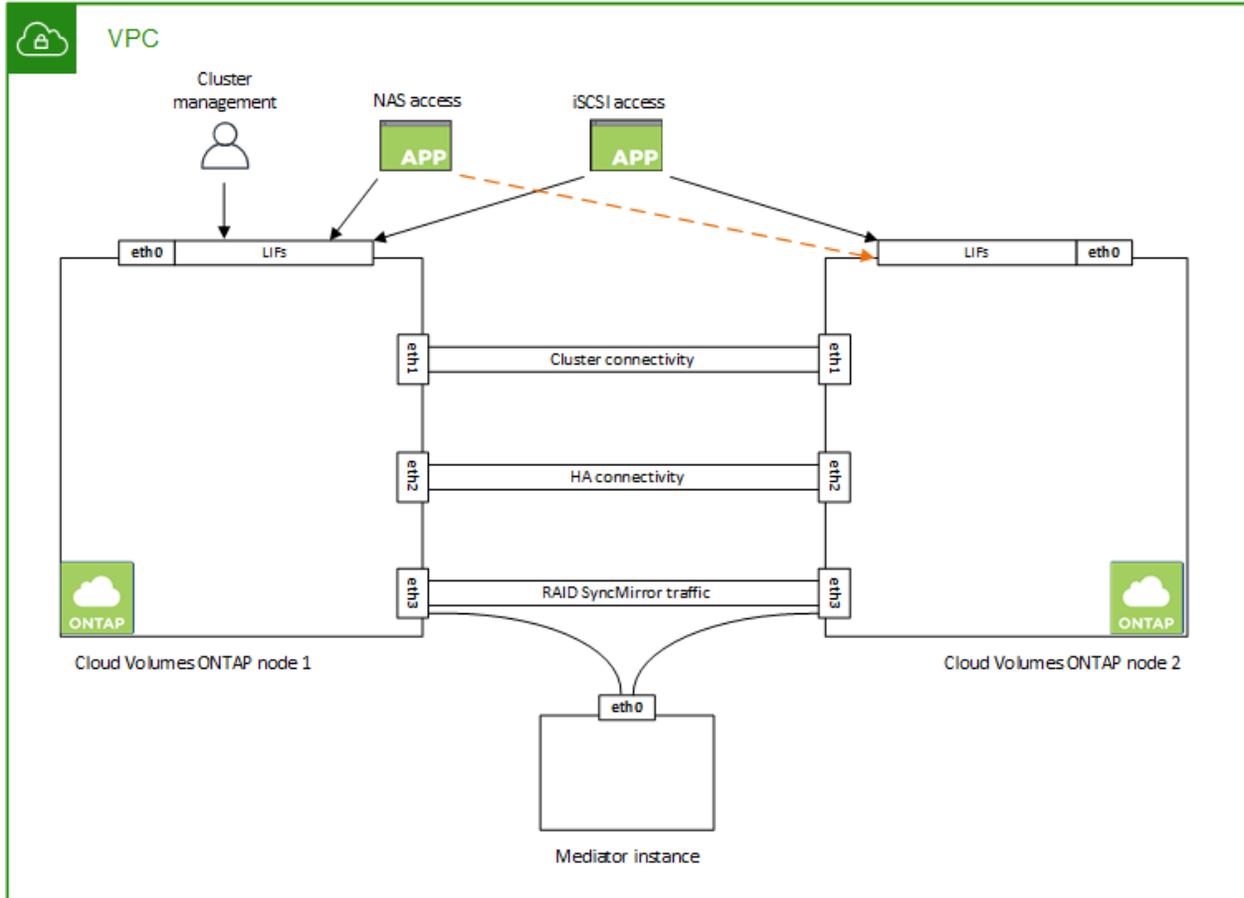
BlueXPでは、1つのノードシステムに6つのIPアドレスが割り当てられます。

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。
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。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。



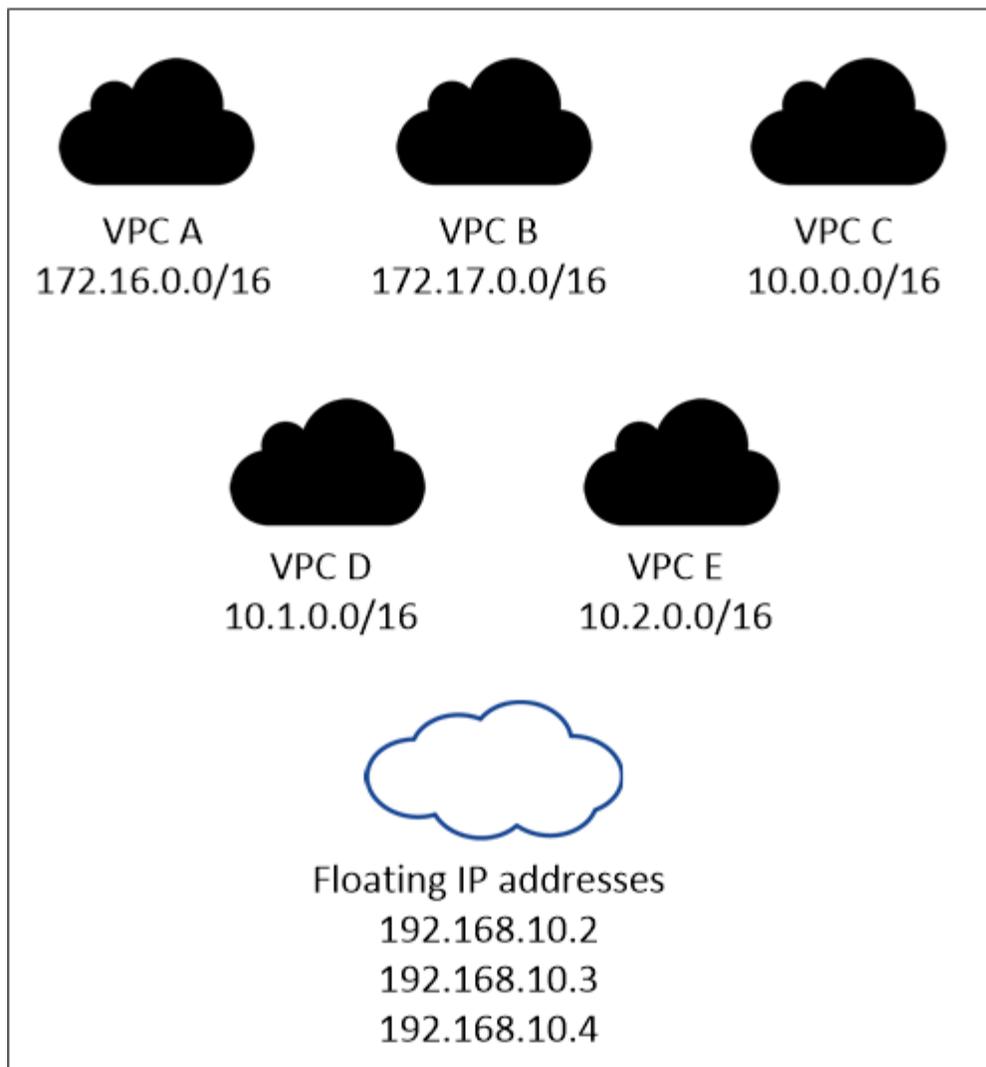
SnapCenter for Windows または SnapDrive を HA ペアで使用する場合は、SVM 管理 LIF 用にフローティング IP アドレスが必要です。

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」](#)。

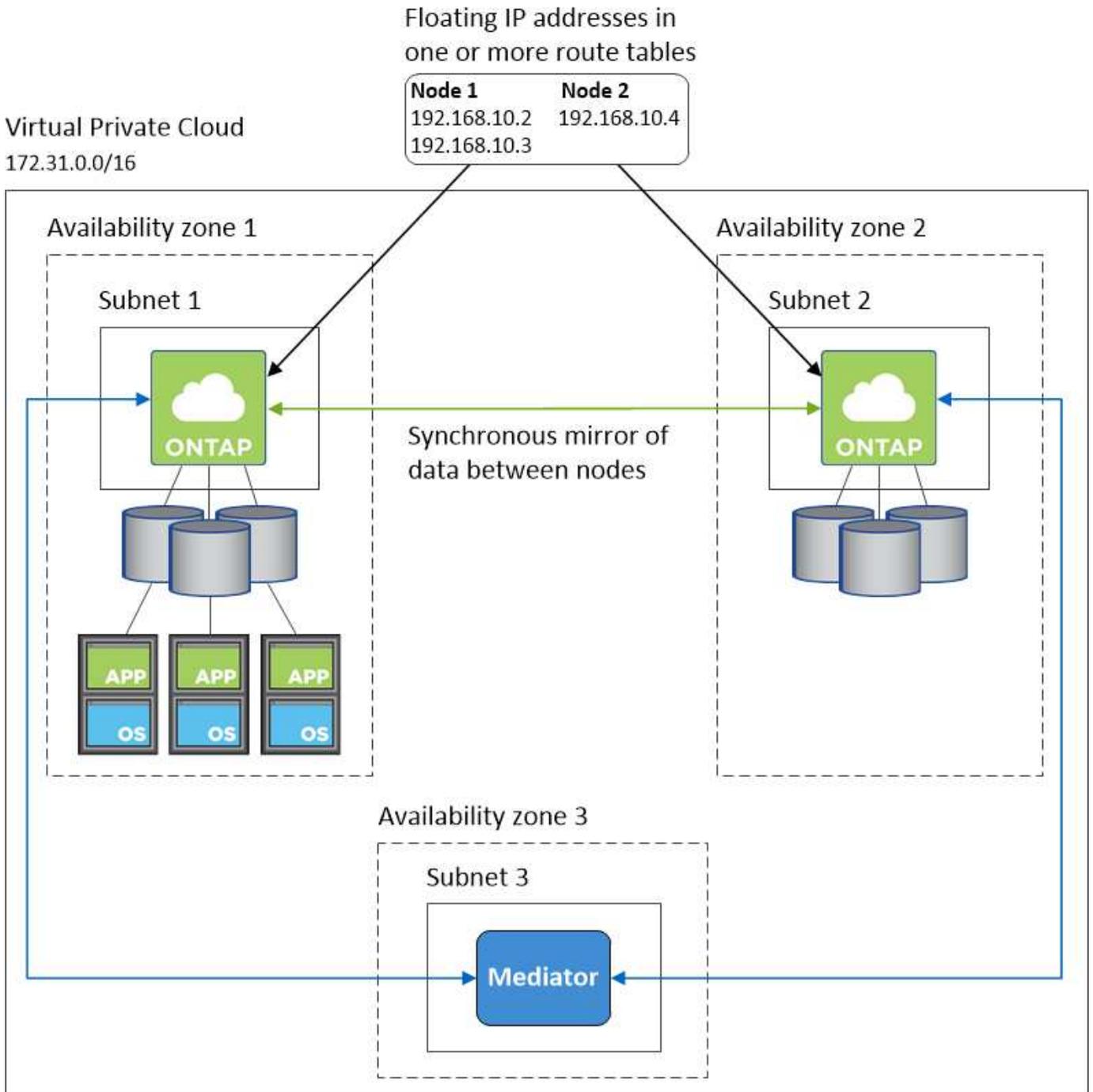
ネットアップの管理ツールとの連携

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

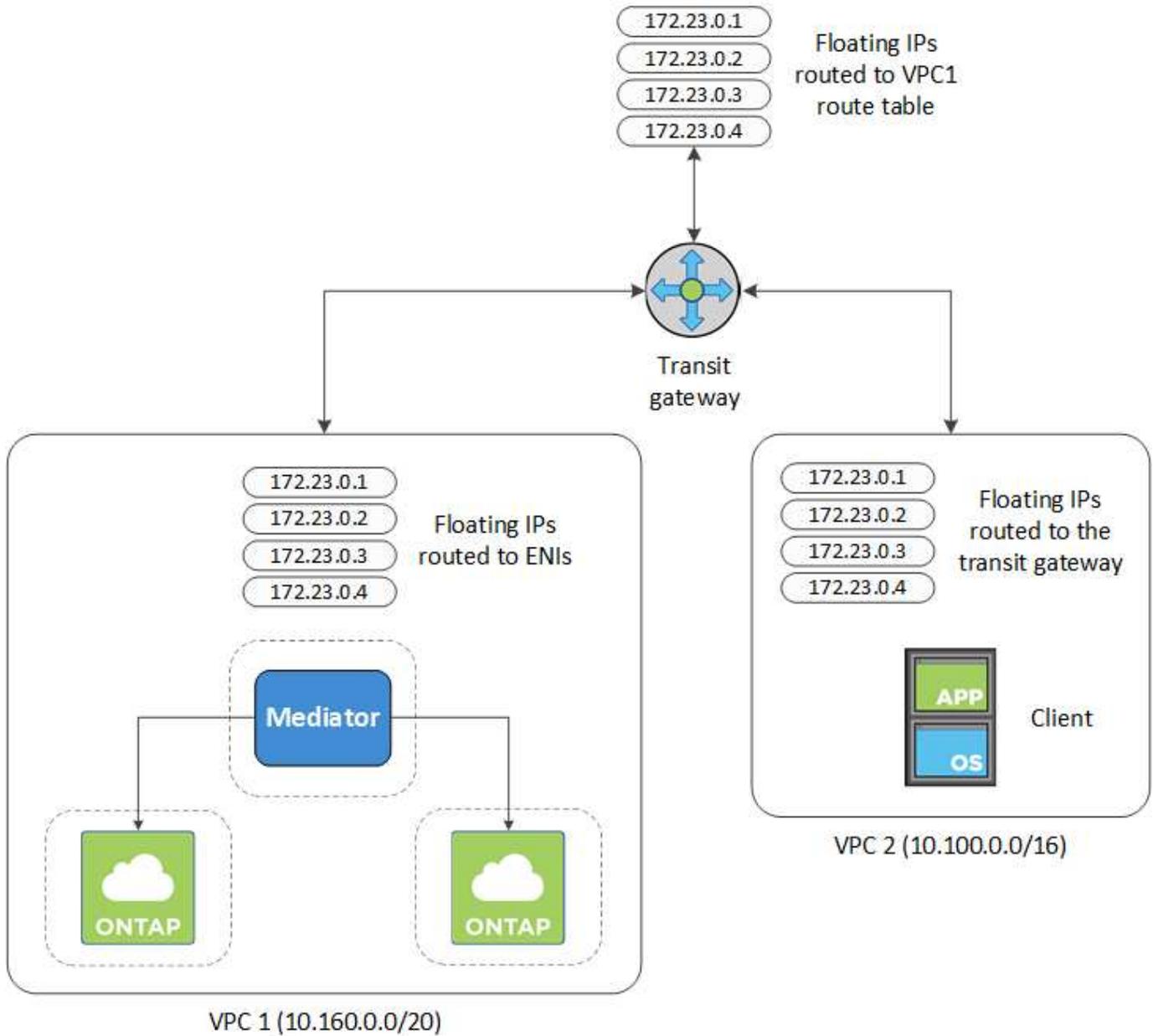
へのアクセスを有効にするために、AWS 転送ゲートウェイを設定します HA ペアの 1 つ "フローティング IP アドレス" HA ペアが存在する VPC の外部から

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 route Delete route

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 VPC	propagated	active
<input type="checkbox"/>	10.160.0.0/20	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC1 VPC	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

Annotations: Red arrow points to VPC2 route, Yellow arrow points to VPC1 route, Green arrow points to Floating IP Addresses (rows 3-6).

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、VPC1へのルートとフローティングIPアドレスを含むVPC2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

- 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

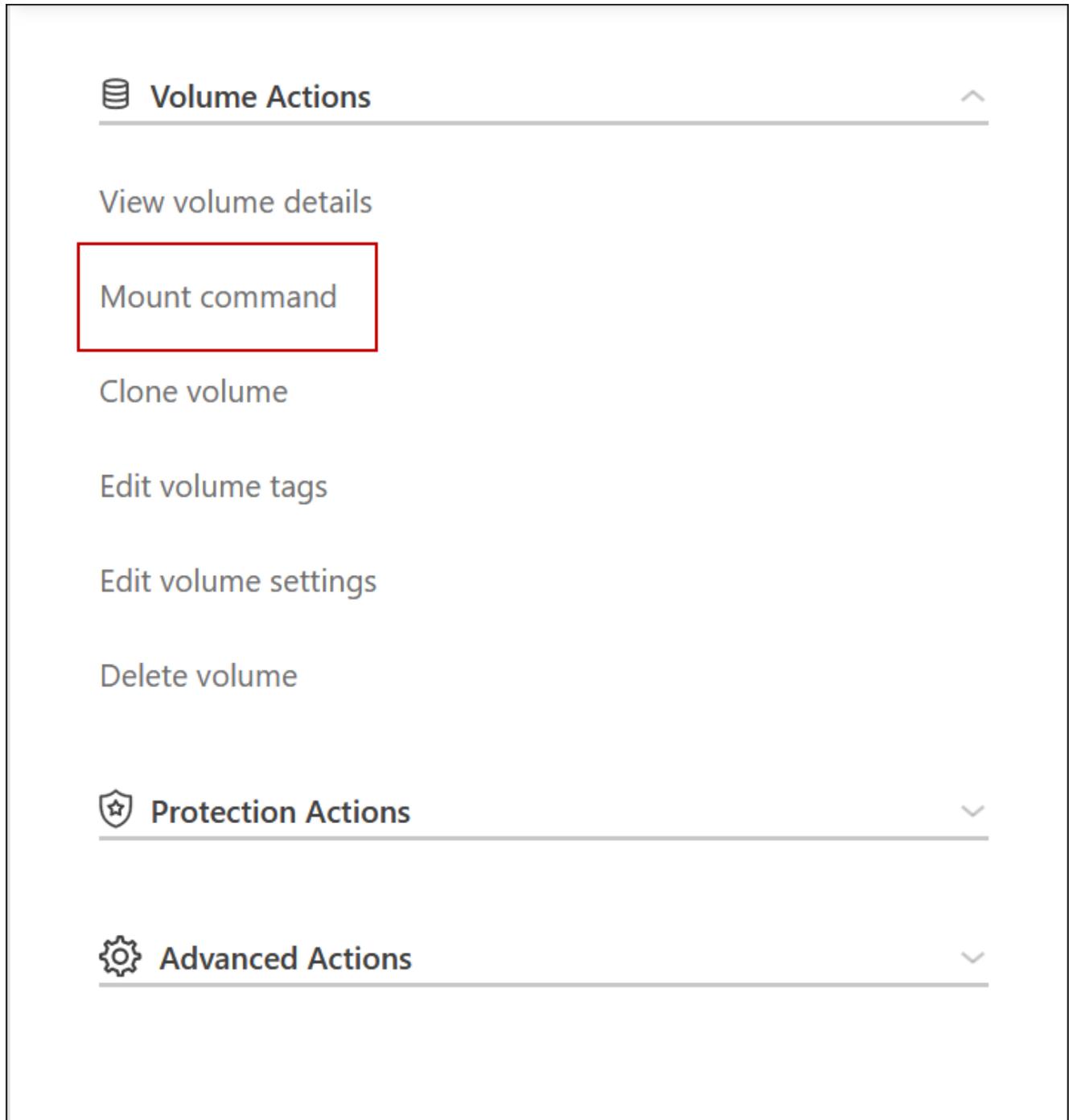
View All routes

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

- 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。
 - [Virtual Private Cloud] で、*[サブネット]* をクリックします。
 - [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。
 - [セキュリティグループ]* をクリックします。
 - [受信ルールの編集]* を選択します。
 - [ルールの追加] をクリックします。
 - [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。
 - [ルールの保存]* をクリックして変更を適用します。
- 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

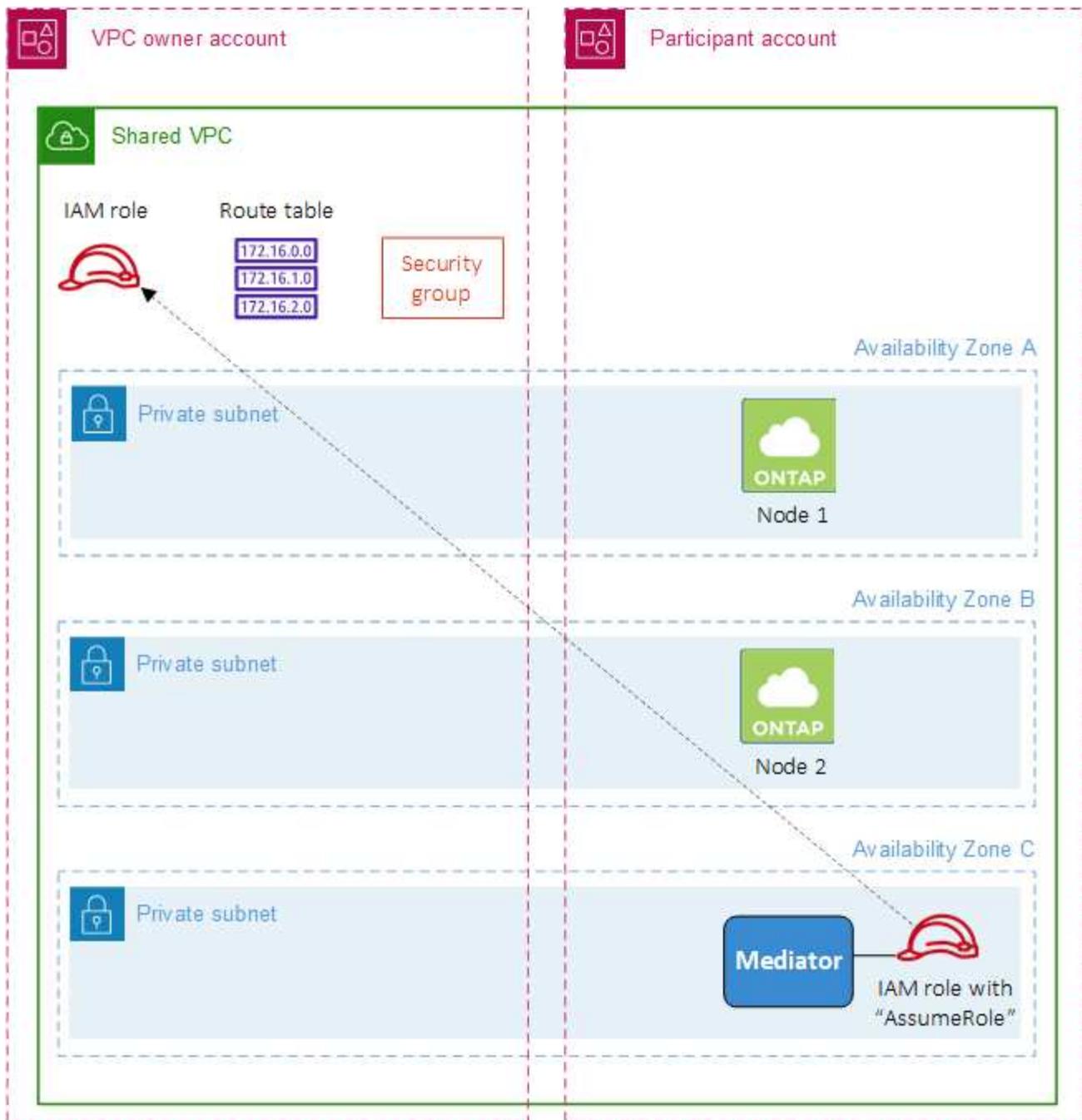
9.11.1リリース以降では、VPCを共有するAWSでCloud Volumes ONTAP HAペアがサポートされます。VPC共有を使用すると、他のAWSアカウントとサブネットを共有できます。この構成を使用するには、AWS環境をセットアップし、APIを使用してHAペアを導入する必要があります。

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 メディエ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、メディア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 メディアーターと 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 メディアーターと 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"

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权を有し、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权については、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。