# Cloud Volumes ONTAP in AWS のネットワーク要件

## Cloud Manager

Ben Cammett
May 12, 2021

# 目次

# Cloud Volumes ONTAP in AWS のネットワーク要件

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

## Cloud Volumes ONTAP の一般的な要件

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 から 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 AWS 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 の設定方法について説明します"。

**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

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 ）"。

**IP** アドレスの数

- シングルノード： IP アドレス × 6
- 単一の AZ にまたがる HA ペア： 15 個のアドレス
- 複数の AZ にまたがる HA ペア： 15 または 16 個の IP アドレス

Cloud Manager は、単一のノードシステム上に SVM 管理 LIF を作成しますが、単一の AZ 内の HA ペア上には作成しません。複数の AZ にまたがる HA ペア上に SVM 管理 LIF を作成するかどうかを選択できます。

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

セキュリティグループ

Cloud Manager ではセキュリティグループを作成する必要がないため、セキュリティグループを作成する必要はありません。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"。

**Cloud Volumes ONTAP** から **AWS S3** への接続によるデータ階層化

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。"

他のネットワーク内の **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（ Azure VNet や企業ネットワークなど）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**

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"。

# 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、これらの要件を確認する必要があります。これは、 Cloud Manager でネットワークの詳細を入力する必要があるためです。

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

可用性ゾーン

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

**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

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。

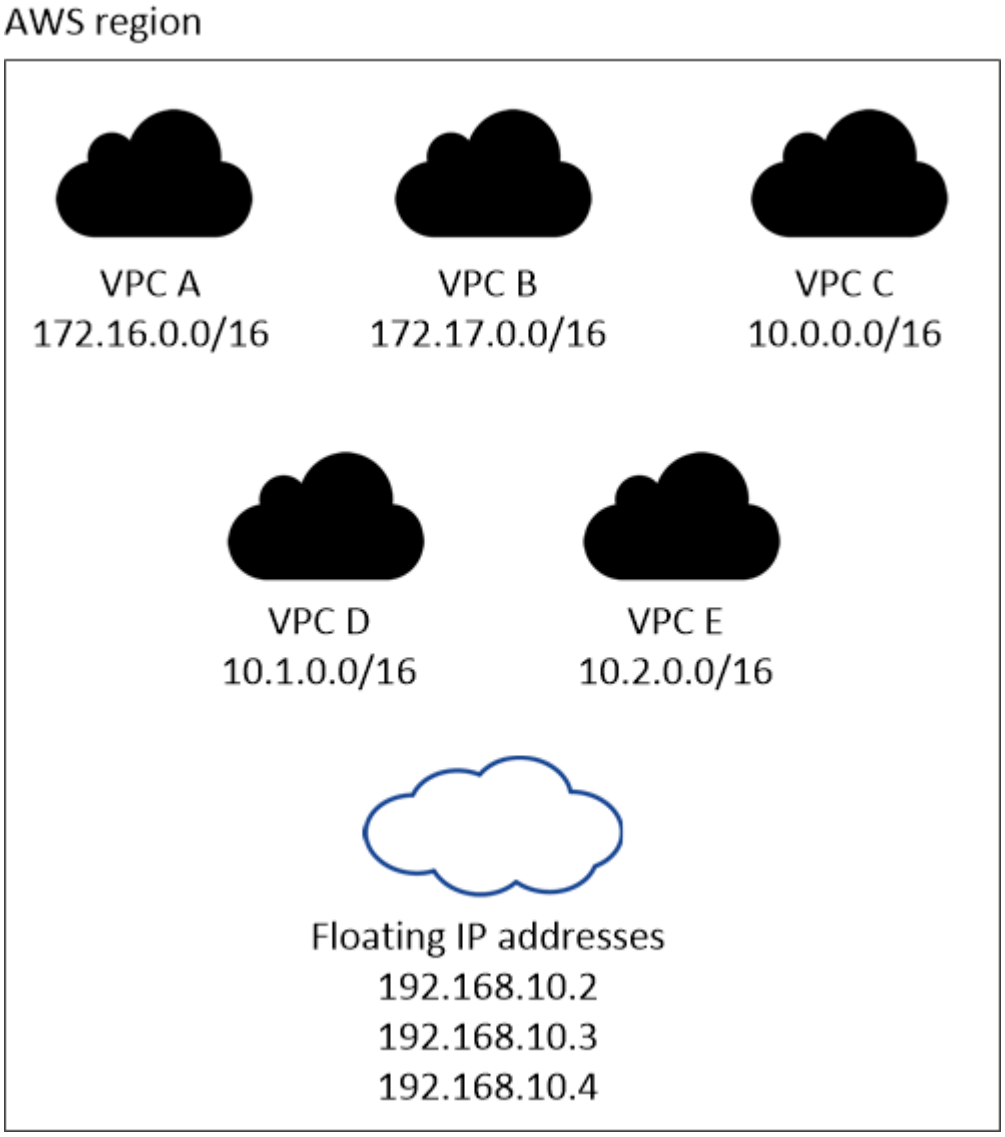
SnapCenter for Windows または SnapDrive を HA ペアで使用する場合は、 SVM 管理 LIF 用にフローティング IP アドレスが必要です。システムの導入時に IP アドレスを指定しなかった場合は、あとで LIF を作成できます。詳細については、を参照してください "Cloud Volumes ONTAP のセットアップ"。

Cloud Volumes ONTAP HA 作業環境を作成するときに、 Cloud Manager 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。Cloud Manager は、システムの起動時に IP アドレスを HA ペアに割り当てます。

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。




Cloud Manager は、 iSCSI アクセス用と、 VPC 外のクライアントからの NAS アクセス用に、自動的に静的 IP アドレスを作成します。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**

"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

vPC （メインルートテーブル）内のサブネットのルートテーブルが 1 つだけの場合、 Cloud Manager はそのルートテーブルにフローティング IP アドレスを自動的に追加します。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。

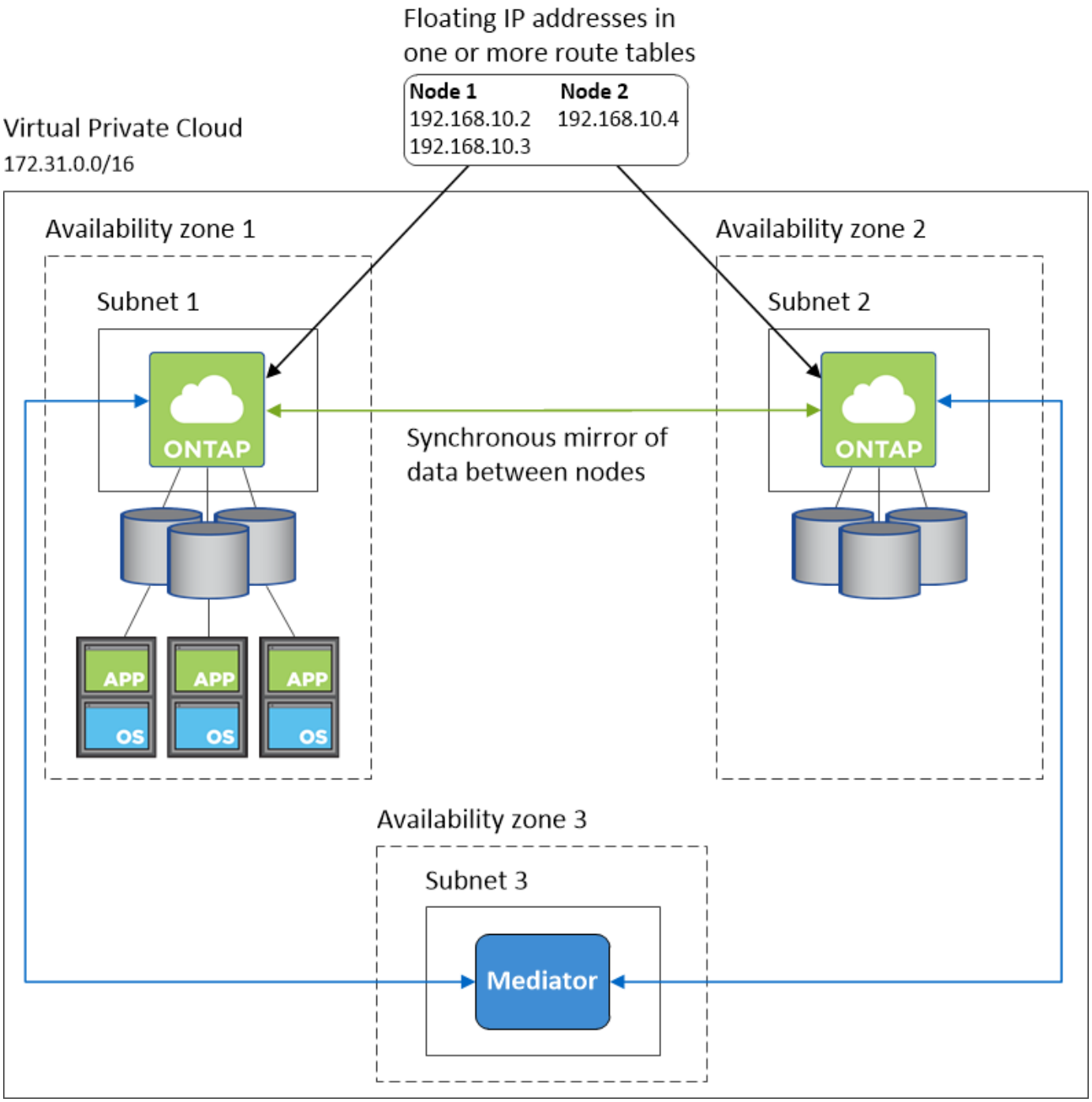
ルーティングテーブルの詳細については、を参照してください "AWS のドキュメント：「 Route Tables"。

ネットアップの管理ツールとの連携

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、アクティブ / パッシブ構成として動作する AWS の最適な HA 構成を示しています。




# コネクタの要件

コネクタがパブリッククラウド環境内のリソースやプロセスを管理できるように、ネットワークを設定します。最も重要なステップは、さまざまなエンドポイントへのアウトバウンドインターネットアクセスを確保することです。

ネットワークでインターネットへのすべての通信にプロキシサーバを使用している場合は、[ 設定 ] ページでプロキシサーバを指定できます。を参照してください "プロキシサーバを使用するようにコネクタを設定します"。

## ターゲットネットワークへの接続

コネクタには、 Cloud Volumes ONTAP を導入する VPC および VNet へのネットワーク接続が必要です。

たとえば、企業ネットワークにコネクタを設置する場合は、 Cloud Volumes ONTAP を起動する VPC または VNet への VPN 接続を設定する必要があります。

## アウトバウンドインターネットアクセス

Connector では、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するためにアウトバウンドインターネットアクセスが必要です。コネクタは、 AWS でリソースを管理する際に次のエンドポイントに接続します。

VPC がネットワークアクセス制御リスト（ ACL ）を使用してトラフィックをフィルタリングする場合は、アウトバウンドとインバウンドの両方のトラフィックに対してこれらのエンドポイントを有効にしてください。

| エンドポイント | 目的 |
| --- | --- |
| AWS サービス（ amazonaws.com ）：<br>• クラウド形成<br>• 柔軟なコンピューティングクラウド（ EC2 ）<br>• キー管理サービス（ KMS ）<br>• セキュリティトークンサービス（ STS ）<br>• シンプルなストレージサービス（ S3 ）<br>正確なエンドポイントは、 Cloud Volumes ONTAP を導入する地域によって異なります。 "詳細については、 AWS のマニュアルを参照してください。" | AWS に Cloud Volumes ONTAP を導入して管理できるようにします。 |
| \ https://api.services.cloud.netapp.com:443 | NetApp Cloud Central への API 要求。 |
| \ https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com | ソフトウェアイメージ、マニフェスト、およびテンプレートにアクセスできます。 |
| ¥ https://cognito-idp.us-east-1.amazonaws.com ¥ https://cognito-identity.us-east-1.amazonaws.com ¥ https://sts.amazonaws.com ¥ https://cloud-support-netapp-com-accelerated.s3.amazonaws.com | コネクタがマニフェスト、テンプレート、および Cloud Volumes ONTAP アップグレードイメージにアクセスしてダウンロードできるようにします。 |
| \ https://cloudmanagerinfraprod.azurecr.io | Docker を実行しているインフラのコンテナコンポーネントのソフトウェアイメージにアクセスでき、 Cloud Manager とのサービス統合のためのソリューションを提供します。 |
| \ https://kinesis.us-east-1.amazonaws.com | ネットアップが監査レコードからデータをストリーミングできるようにします。 |

| エンドポイント | 目的 |
| --- | --- |
| \ https://cloudmanager.cloud.netapp.com | Cloud Central アカウントを含む Cloud Manager サービスとの通信。 |
| https://netapp-cloud-account.auth0.com | NetApp Cloud Central との通信により、ユーザ認証を一元的に行うことができます。 |
| support.netapp.com:443<br>https://mysupport.netapp.com | ネットアップ AutoSupport との通信：コネクタは support.netapp.com:443 と通信し、https://mysupport.netapp.com にリダイレクトされます。 |
| ¥ https://support.netapp.com/svcgw ¥ https://support.netapp.com/ServiceGW/entitlement ¥ https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com ¥ https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com | システムライセンスとサポート登録を行うためのネットアップとの通信 |
| ¥ https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com ¥ https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com ¥ https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com | ネットアップがサポートの問題のトラブルシューティングに必要な情報を収集できるようにします。 |
| \ https://ipa-signer.cloudmanager.netapp.com | Cloud Manager でライセンスを生成できます（ Cloud Volumes ONTAP 用の FlexCache ライセンスなど）。 |
| 次のようなさまざまなサードパーティの場所があります。<br>• https://repo1.maven.org/maven2 です<br>• https://oss.sonType.org/content/repository を参照してください<br>• \ https://repo.typesafe.com<br>サードパーティの所在地は変更される可能性があります。 | アップグレード時に、 Cloud Manager はサードパーティの依存関係に対応する最新のパッケージをダウンロードします。 |

SaaS ユーザインターフェイスからほとんどのタスクを実行する必要がありますが、ローカルユーザインターフェイスは引き続きコネクタで使用できます。Web ブラウザを実行するマシンは、次のエンドポイントに接続する必要があります。

| エンドポイント | 目的 |
| --- | --- |
| コネクタホスト | Cloud Manager コンソールをロードするには、 Web ブラウザでホストの IP アドレスを入力する必要があります。<br><br>クラウドプロバイダへの接続に応じて、ホストに割り当てられたプライベート IP またはパブリック IP を使用できます。<br><br>• プライベート IP は、 VPN とがある場合に機能します 仮想ネットワークへの直接アクセス<br>• パブリック IP は、あらゆるネットワークシナリオで機能します<br><br>いずれの場合も、セキュリティグループのルールで許可された IP またはサブネットからのアクセスのみを許可することで、ネットワークアクセスを保護する必要があります。 |
| ¥ https://auth0.com ¥ https://cdn.auth0.com ¥ https://netapp-cloud-account.auth0.com ¥ https://services.cloud.netapp.com | Web ブラウザはこれらのエンドポイントに接続し、 NetApp Cloud Central を介してユーザ認証を一元化します。 |
| \ https://widget.intercom.io | 製品内でのチャットにより、ネットアップのクラウドエキスパートと会話できます。 |