



ネットワークをセットアップします

Cloud Manager

NetApp
July 13, 2021

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 | 8 |
| AWS のセキュリティグループルール | 12 |

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

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。

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。

AWS region



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 |
|--|--|
| <p>AWS サービス（amazonaws.com）：</p> <ul style="list-style-type: none">• クラウド形成• 柔軟なコンピューティングクラウド（EC2）• キー管理サービス（KMS）• セキュリティトークンサービス（STS）• シンプルなストレージサービス（S3） <p>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。"</p> | <p>AWS に Cloud Volumes ONTAP を導入して管理できるようにします。</p> |
| <p>\ https://api.services.cloud.netapp.com:443</p> | <p>NetApp Cloud Central への API 要求。</p> |
| <p>\ https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</p> | <p>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。</p> |
| <p>¥ 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</p> | <p>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。</p> |
| <p>\ https://cloudmanagerinfraproduct.azurecr.io</p> | <p>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。</p> |
| <p>\ https://kinesis.us-east-1.amazonaws.com</p> | <p>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。</p> |

| 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 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。 <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 です • https://oss.sonatype.org/content/repository を参照してください • \ https://repo.typesafe.com 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 | <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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 • 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 <p>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。</p> |
| ¥ 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。 |

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

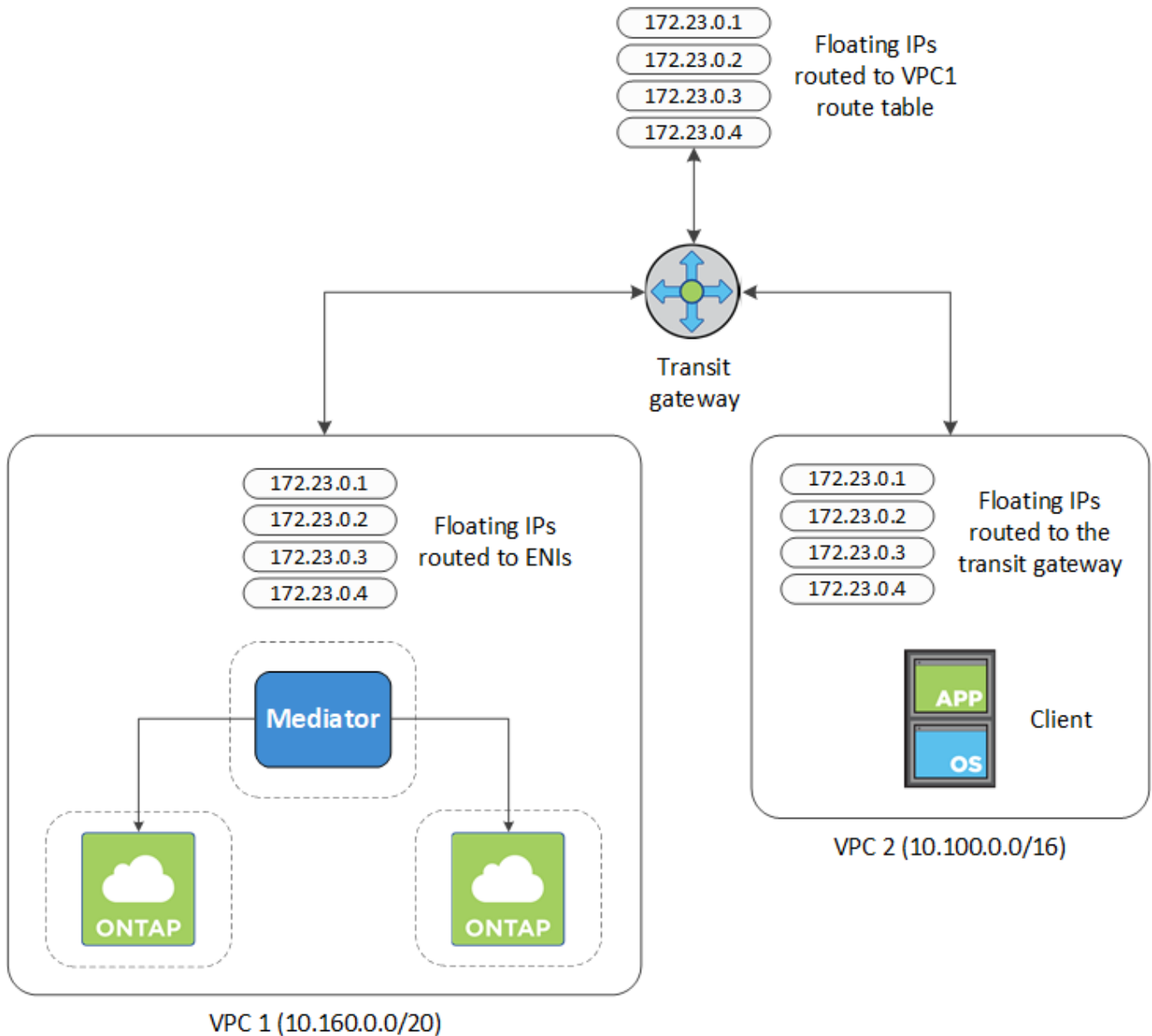
へのアクセスを有効にするために、AWS 転送ゲートウェイを設定します HA ペアの 1 つ **"フローティング IP アドレス"** HA ペアが存在する VPC の外部から

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、Cloud Manager の Working Environment Information ページで確認できま

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 | 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 | Floating | static | active |
| <input type="checkbox"/> | 172.23.0.3/32 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | IP | static | active |
| <input type="checkbox"/> | 172.23.0.4/32 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | Addresses | 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。

- 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。
- 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 | lgw-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。フローティング IP は、HA ペアの導入時に Cloud Manager によってルートテーブルに自動的に追加されます。

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 | lgw-b2182dd7 | active |
| 10.60.29.0/25 | pcx-589c3331 | active |
| 10.100.0.0/16 | tgw-015b7c249661ac279 | active |
| 10.129.0.0/20 | pcx-f7e1396 | 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
acti
IP
Addresses

6. 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。

Cloud Manager で正しい IP アドレスを確認するには、ボリュームを選択して * Mount command * をクリックします。

Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



7. 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"](#)

AWS のセキュリティグループルール

Cloud Manager で作成される AWS セキュリティグループには、コネクタと 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が含まれています。テスト目的でポートを参照したり、独自のセキュリティグループを使用したりする場合に使用します。

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

定義済みセキュリティグループのインバウンドルールの送信元は 0.0.0.0/0 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 |

| プロトコル | ポート | 目的 |
|-------|---------|---|
| HTTPS | 443 | 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 |
| 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 |

| 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、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) |
| 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) |

| サービス | プロトコル | ポート | ソース | 宛先 | 目的 |
|------------|------------|---------------|---------------------------------|-------------------|--------------------------------------|
| 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） |
| DHCP | UDP | 68 | ノード管理 LIF | DHCP | 初回セットアップ用の DHCP クライアント |
| DHCP | UDP | 67 | ノード管理 LIF | DHCP | DHCP サーバ |
| DNS | UDP | 53 | ノード管理 LIF とデータ LIF（ NFS、 CIFS ） | DNS | DNS |
| NDMP | TCP | 18600 ~ 18699 | ノード管理 LIF | 宛先サーバ | NDMP コピー |
| SMTP | TCP | 25 | ノード管理 LIF | メールサーバ | SMTP アラート。 AutoSupport に使用できます |
| SNMP | TCP | 161 | ノード管理 LIF | サーバを監視します | SNMP トラップによる監視 |
| | UDP | 161 | ノード管理 LIF | サーバを監視します | SNMP トラップによる監視 |
| | TCP | 162 | ノード管理 LIF | サーバを監視します | SNMP トラップによる監視 |
| | UDP | 162 | ノード管理 LIF | サーバを監視します | SNMP トラップによる監視 |
| SnapMirror | TCP | 11104 | クラスタ間 LIF | ONTAP クラスタ間 LIF | SnapMirror のクラスタ間通信セッションの管理 |
| | TCP | 11105 | クラスタ間 LIF | ONTAP クラスタ間 LIF | SnapMirror によるデータ転送 |
| syslog | UDP | 514 | ノード管理 LIF | syslog サーバ | syslog 転送メッセージ |

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

インバウンドルールの送信元は 0.0.0.0/0 です。

| プロトコル | ポート | 目的 |
|-------|------|--------------------------|
| SSH | 22 | HA メディエータへの SSH 接続 |
| TCP | 3000 | コネクタからの RESTful API アクセス |

アウトバウンドルール

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

基本的なアウトバウンドルール

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

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

高度なアウトバウンドルール

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

| プロトコル | ポート | 宛先 | 目的 |
|-------|-----|---------------|---------------------------|
| HTTP | 80 | 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 | AWS API サービス | ストレージのフェイルオーバーを支援します |
| UDP | 53 | AWS API サービス | 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 Mediator 内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。Cloud Manager は常にこのセキュリティグループを作成します。独自のオプションはありません。

インバウンドルール

事前定義されたセキュリティグループには、次の着信ルールが含まれています。

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

アウトバウンドルール

定義済みのセキュリティグループには、次の発信ルールが含まれます。

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

コネクタのルール

コネクタのセキュリティグループには、インバウンドとアウトバウンドの両方のルールが必要です。

インバウンドルール

| プロトコル | ポート | 目的 |
|-------|------|---|
| SSH | 22 | コネクタホストへの SSH アクセスを提供します |
| HTTP | 80 | クライアント Web ブラウザからローカルユーザインターフェイスへの HTTP アクセス、および Cloud Data Sense からの接続を提供します |
| HTTPS | 443 | クライアント Web ブラウザからローカルへの HTTPS アクセスを提供します ユーザインターフェイス |
| TCP | 3128 | AWS ネットワークで NAT やプロキシを使用していない場合に、Cloud Data Sense インスタンスにインターネットアクセスを提供します |

アウトバウンドルール

コネクタの事前定義された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

コネクタの事前定義された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 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固定ルールが必要な場合は、次の情報を使用して、コネクタによる発信通信に必要なポートだけを開くことができます。



送信元 IP アドレスは、コネクタホストです。

| サービス | プロトコル | ポート | 宛先 | 目的 |
|-------------------------|-------|------|---------------------------------------|---|
| Active Directory | TCP | 88 | Active Directory フォレスト | Kerberos V 認証 |
| | TCP | 139 | Active Directory フォレスト | NetBIOS サービスセッション |
| | TCP | 389 | Active Directory フォレスト | LDAP |
| | TCP | 445 | 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 | Active Directory フォレスト | Kerberos V パスワードの変更と設定（ SET_CHANGE） |
| | TCP | 749 | Active Directory フォレスト | Active Directory Kerberos v の変更と パスワードの設定（ RPCSEC_GSS） |
| | UDP | 137 | Active Directory フォレスト | NetBIOS ネームサービス |
| | UDP | 138 | Active Directory フォレスト | NetBIOS データグラムサービス |
| | UDP | 464 | Active Directory フォレスト | Kerberos キー管理 |
| API コールと AutoSupport | HTTPS | 443 | アウトバウンドインターネットおよび ONTAP クラスタ管理 LIF | AWS および ONTAP への API コール、 およびネットアップへの AutoSupport メッセージの送信 |
| API コール | TCP | 3000 | ONTAP クラスタ管理 LIF | ONTAP への API コール |
| | TCP | 8088 | S3 へのバックアップ | S3 へのバックアップを API で呼び出します |
| DNS | UDP | 53 | DNS | Cloud Manager による DNS 解決に使用されます |
| クラウドデータの意味 | HTTP | 80 | Cloud Data Sense インスタンス | Cloud Volumes ONTAP に最適なクラウドデータ |

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.