



ネットワークをセットアップします

Cloud Volumes ONTAP

NetApp
July 03, 2022

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 | 9 |
| HAペアを共有サブネットに導入します | 13 |
| AWS のセキュリティグループルール | 15 |

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 Manager は、IP アドレス、ネットマスク、ルートなど、Cloud Volumes ONTAP 用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 ノードでは、ネットアップ AutoSupport にメッセージを送信するために、アウトバウンドインターネットアクセスが必要です。ネットアップ AutoSupport は、ストレージの健全性をプロアクティブに監視します。

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

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

必要な数のプライベート IP アドレスが Cloud Manager から Cloud Volumes ONTAP に自動的に割り当てられます。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 に対して Cloud Manager が割り当てる 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

Cloud Manager は、1 つのノードシステムに 6 つの IP アドレスを割り当てます。

- クラスタ管理 LIF
- ノード管理 LIF
- クラスタ間 LIF
- NAS データ LIF
- iSCSI データ LIF
- Storage VM 管理 LIF

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。 |
| クラスタ接続 | Eth1 | ノード 1 とノード 2 | ノード間の通信およびクラスタ内でのデータの移動を可能にします。 |
| HA 接続 | eth2 | ノード 1 とノード 2 | フェイルオーバー時の 2 つのノード間の通信。 |
| RSM iSCSI トラフィック | eth3 | ノード 1 とノード 2 | RAID SyncMirror iSCSI トラフィック、および 2 つの Cloud Volumes ONTAP ノードとメディエーター間の通信。 |
| メディエーター | eth0 | メディエーター | ストレージのテイクオーバーとギブバックのプロセスを支援するための、ノードとメディエーターの間の通信チャンネル。 |

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。 |
| クラスタ接続 | Eth1 | ノード 1 とノード 2 | ノード間の通信およびクラスタ内でのデータの移動を可能にします。 |
| HA 接続 | eth2 | ノード 1 とノード 2 | フェイルオーバー時の 2 つのノード間の通信。 |
| RSM iSCSI トラフィック | eth3 | ノード 1 とノード 2 | RAID SyncMirror iSCSI トラフィック、および 2 つの Cloud Volumes ONTAP ノードとメディエーター間の通信。 |

| 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

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"](#)。

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 Cloud Manager でネットワークの詳細を入力する必要があるため、これらの要件を確認しておく必要があります。

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。

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

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

Cloud Manager 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ティングテーブルを選択するよう求められます。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（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

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

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

HA 構成の例

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



コネクタの要件

コネクタ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。

| エンドポイント | 目的 |
|--|---|
| \ https://support.netapp.com | ライセンス情報を取得し、ネットアップサポートに AutoSupport メッセージを送信するため。 |
| \ https://*.cloudmanager.cloud.netapp.com | Cloud Manager 内で SaaS の機能やサービスを提供できます。 |
| ¥ https://cloudmanagerinfraproduct.azurecr.io ¥ https://*.blob.core.windows.net | をクリックして、Connector と Docker コンポーネントをアップグレードします。 |

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、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 | 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 |

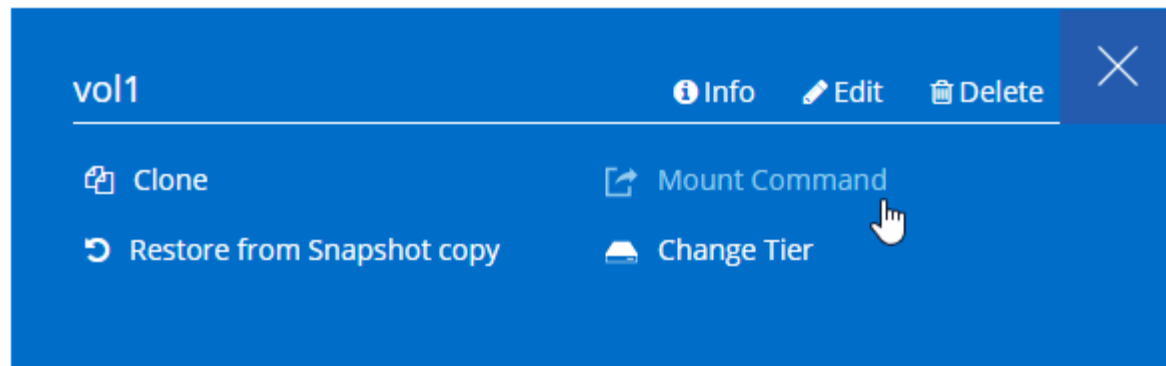
VPC2
Floating
act IP
Addresses

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"](#)

HAペアを共有サブネットに導入します

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

を使用 ["VPC共有"](#)Cloud Volumes ONTAP HA構成は、次の2つのアカウントに分散されます。

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

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

次の図は、この導入に関連するコンポーネントを示しています。



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

Cloud Volumes ONTAP の作業環境を作成すると、Cloud ManagerによってIAMロールが自動的に作成されて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。クラウドマネージャーがそれを実現します。

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. Cloud Manager 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

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 |
| 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 |

| プロトコル | ポート | 目的 |
|-------|------|-------------------|
| 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） |
| 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） |
| 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構成の内部セキュリティグループに関するルール

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

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 |

| プロトコル | ポート | 目的 |
|----------|-----|--------------|
| 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 |
|----------------------|-------|------|------------------------------------|--|
| 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 | API が AWS や ONTAP、クラウドデータ検知、ランサムウェアサービス、ネットアップへの AutoSupport メッセージの送信を呼び出します |
| API コール | TCP | 3000 | ONTAP HA メディエーター | ONTAP HA メディエーターとの通信 |
| | 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 |

著作権情報

Copyright © 2022 NetApp, Inc. All rights reserved. 米国で印刷されていますこのドキュメントは著作権によって保護されています。画像媒体、電子媒体、および写真複写、記録媒体などの機械媒体など、いかなる形式および方法による複製も禁止します。テープ媒体、または電子検索システムへの保管-著作権所有者の書面による事前承諾なし。

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、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、いかなる場合でも、間接的、偶発的、特別、懲罰的、またはまたは結果的損害（代替品または代替サービスの調達、使用の損失、データ、利益、またはこれらに限定されないものを含みますが、これらに限定されません。）ただし、契約、厳格責任、または本ソフトウェアの使用に起因する不法行為（過失やその他を含む）のいずれであっても、かかる損害の可能性について知らされていた場合でも、責任の理論に基づいて発生します。

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、またはその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り特許、その他の国の特許、および出願中の特許。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7103（1988 年 10 月）および FAR 52-227-19（1987 年 6 月）の Rights in Technical Data and Computer Software（技術データおよびコンピュータソフトウェアに関する諸権利）条項の（c）（1）（ii）項、に規定された制限が適用されます。

商標情報

NetApp、NetAppのロゴ、に記載されているマーク <http://www.netapp.com/TM> 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。