AWS を始めましょう

Cloud Manager 3.8

NetApp
March 25, 2024

目次

AWS を始めましょう

Cloud Volumes ONTAP for AWS での作業の開始

いくつかの手順で、 Cloud Volumes ONTAP for AWS を使い始めましょう。

コネクタを作成します

を持っていなければ "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"。

最初の Cloud Volumes ONTAP 作業環境を作成する際、まだコネクタがない場合は、 Cloud Manager からコネクタの導入を求められます。

構成を計画

Cloud Manager には、ワークロードの要件に応じた事前設定パッケージが用意されています。または、独自の設定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。"。

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インターネットアクセスを有効にして、コネクタと Cloud Volumes ONTAP が複数のエンドポイントに接続できるようにします。

   コネクタはアウトバウンドのインターネットアクセスがないと Cloud Volumes ONTAP を管理できないため、この手順は重要です。アウトバウンド接続を制限する必要がある場合は、のエンドポイントのリストを参照してください "コネクタと Cloud Volumes ONTAP"。

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"。

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。"。

Cloud Manager 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

- "評価中"
- "Cloud Manager からコネクタを作成します"
- "AWS Marketplace から Connector を起動する"
- "Linux ホストへの Connector ソフトウェアのインストール"
- "Cloud Manager が AWS 権限を使用して実行する処理"

AWS での Cloud Volumes ONTAP 構成の計画

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。

ライセンスタイプの選択

Cloud Volumes ONTAP には、従量課金制とお客様所有のライセンスを使用（ BYOL ）の 2 種類の料金プランがあります。従量課金制の場合は、 Explore 、 Standard 、 Premium の 3 つのライセンスから選択できます。ライセンスごとに容量とコンピューティングのオプションが異なります。

"AWS の Cloud Volumes ONTAP 9.7 でサポートされている構成"

ストレージの制限を理解する

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 の Cloud Volumes ONTAP 9.7 でのストレージの制限"

AWS でのシステムのサイジング

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

汎用 SSD は、 Cloud Volumes ONTAP で最も一般的なディスクタイプです。EBS ディスクのユースケースについては、を参照してください "AWS ドキュメント：「 EBS Volume Types"。

EBS ディスクサイズ

Cloud Volumes ONTAP システムを起動するとき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 Cloud Manager で管理できます"必要に応じて "アグリゲートを自分で作成する"、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 TB 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"。

AWS での Cloud Volumes ONTAP システムのサイジングに関する詳細については、次のビデオを参照してください。

[] | *https://img.youtube.com/vi/GELcXmOuYPw/maxresdefault.jpg*

Flash Cache をサポートする構成を選択しています

AWS の一部の Cloud Volumes ONTAP 構成にはローカルの NVMe ストレージが含まれており、 Cloud Volumes ONTAP はパフォーマンスを向上させるために _Flash Cache _ として使用します。 "Flash Cache の詳細については、こちらをご覧ください"。

AWS ネットワーク情報ワークシート

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。

Cloud Volumes ONTAP のネットワーク情報

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 **AZS** 内の **HA** ペアのネットワーク情報

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	

書き込み速度の選択

Cloud Manager では、シングルノードの Cloud Volumes ONTAP システム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。

通常の書き込み速度と高速書き込み速度の差

通常の書き込み速度を選択すると、データはディスクに直接書き込まれるため、計画外のシステム停止が発生した場合にデータが失われる可能性が低くなります。

高速書き込みを選択すると、データはディスクに書き込まれる前にメモリにバッファされるため、書き込みパフォーマンスが向上します。このキャッシュにより、計画外のシステム停止が発生した場合にデータが失われる可能性があります。

計画外のシステム停止が発生した場合に失われる可能性があるデータの量は、最後の 2 つの整合ポイントの範囲です。整合ポイントとは、バッファされたデータをディスクに書き込むことです。整合ポイントは、書き込みログがいっぱいになったとき、または 10 秒後（どちらか早い方）に発生します。ただし、 AWS EBS ボリュームのパフォーマンスは、整合ポイントの処理時間に影響を与える可能性があります。

高速書き込みを使用する場合

高速書き込みは、ワークロードに高速書き込みパフォーマンスが必要な場合に最適です。また、予期しないシステム停止が発生した場合にも、データ損失のリスクに耐えることができます。

高速書き込みを使用する場合の推奨事項

高速書き込みを有効にする場合は、アプリケーション層で書き込み保護を確保する必要があります。

ボリューム使用プロファイルの選択

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。Cloud Manager でボリュームを作成する場合は、これらの機能を有効にするプロファイルを選択するか、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

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 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 ）"。

IP アドレスの数

Cloud Manager から Cloud Volumes ONTAP に次の数の IP アドレスが AWS で割り当てられます。

- 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

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。"

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**

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"。

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

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。

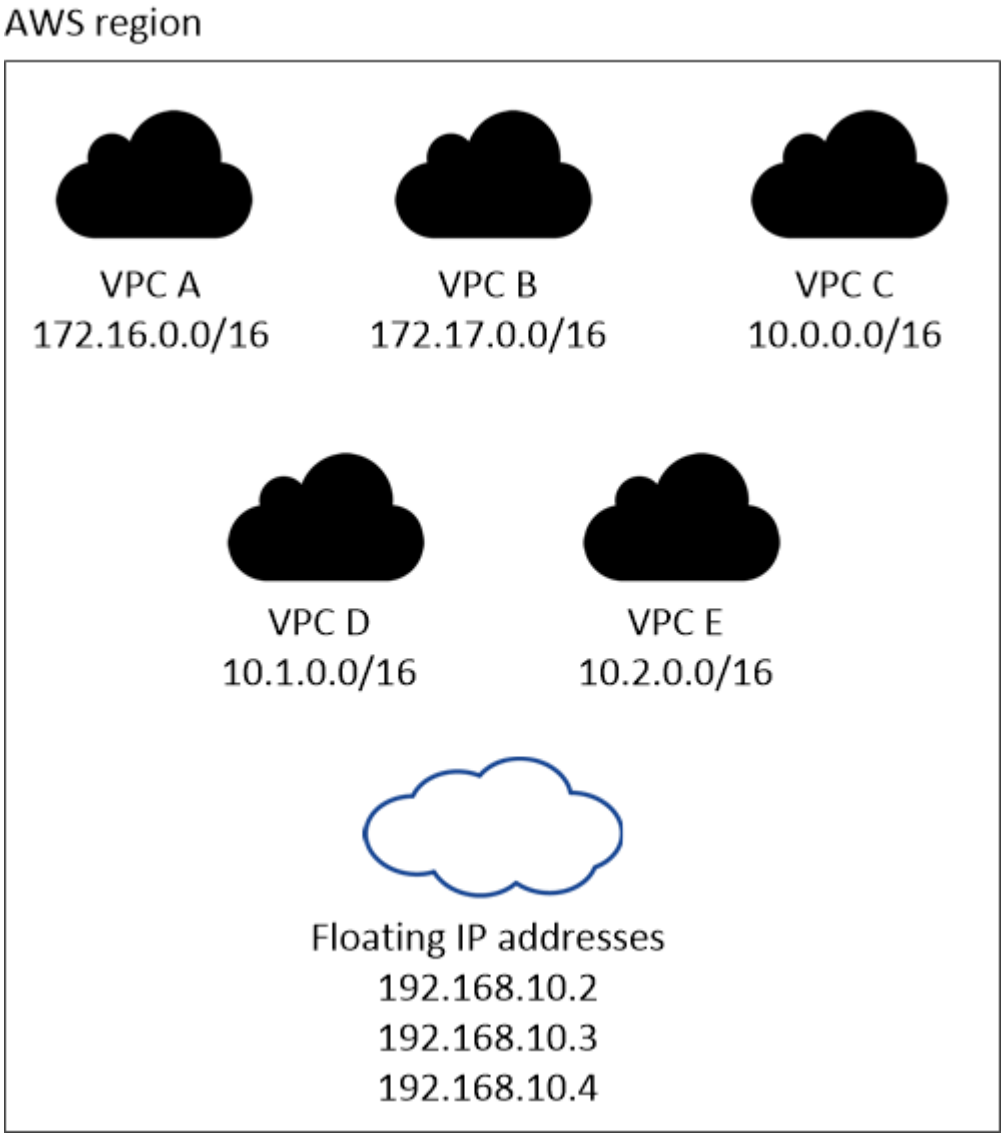
SnapCenter for Windows または SnapDrive を HA ペアで使用する場合は、 SVM 管理 LIF 用にフローティング IP アドレスが必要です。システムの導入時に IP アドレスを指定しなかった場合は、あとで LIF を作成できます。詳細については、を参照してください "Cloud Volumes ONTAP のセットアップ"。

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

Cloud Manager でフローティング IP アドレスを指定したあと、それらのフローティング 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必要があります。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"。

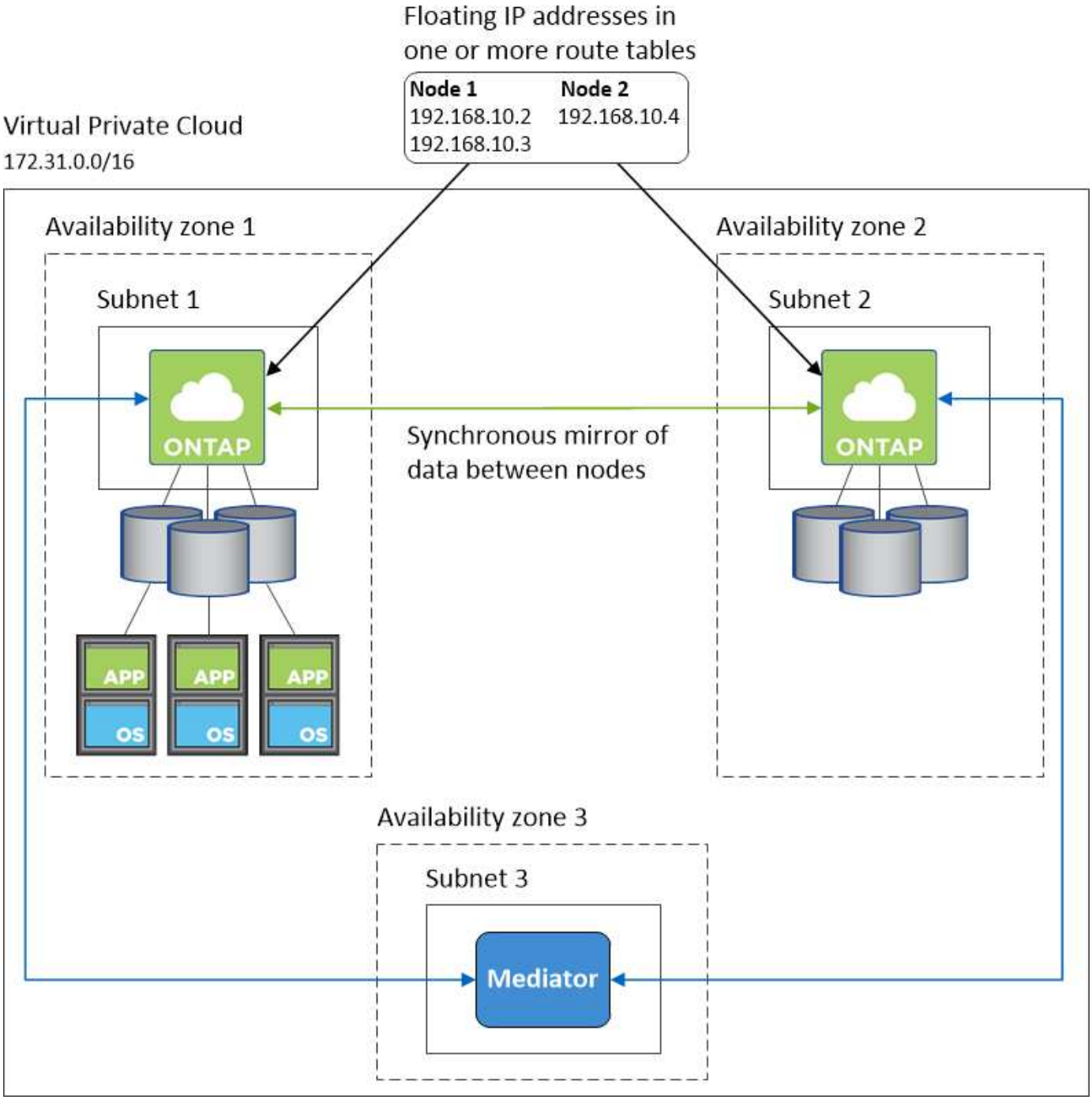
ネットアップの管理ツールとの連携

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、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。

エンドポイント	目的
AWS サービス（ amazonaws.com ）： • 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 ） 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。"	Cloud Manager で Cloud Volumes ONTAP を AWS に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://repo.cloud.support.netapp.com	Cloud Manager の依存関係のダウンロードに使用します。
\ http://repo.mysql.com/	MySQL のダウンロードに使用します。
¥ 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	Cloud Manager は、マニフェスト、テンプレート、 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。
\ 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。

エンドポイント	目的
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。
\ https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	S3 へのバックアップを許可するユーザのリストに AWS アカウント ID を追加します。
¥ https://support.netapp.com/aods/asupmessage ¥ https://support.netapp.com/asupprod/post/1.0/postAsup	ネットアップ AutoSupport との通信：
¥ 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://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）。
¥ https://packages.cloud.google.com/yum ¥ https://github.com/NetApp/trident/releases/download/	Cloud Volumes ONTAP システムを Kubernetes クラスタに接続するために必要です。エンドポイントを使用して NetApp Trident をインストールできます。
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。 • https://repo1.maven.org/maven2 です • https://oss.sonType.org/content/repository を参照してください • https://repo.typafe.org にアクセスします 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。 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。 • 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 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。

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**

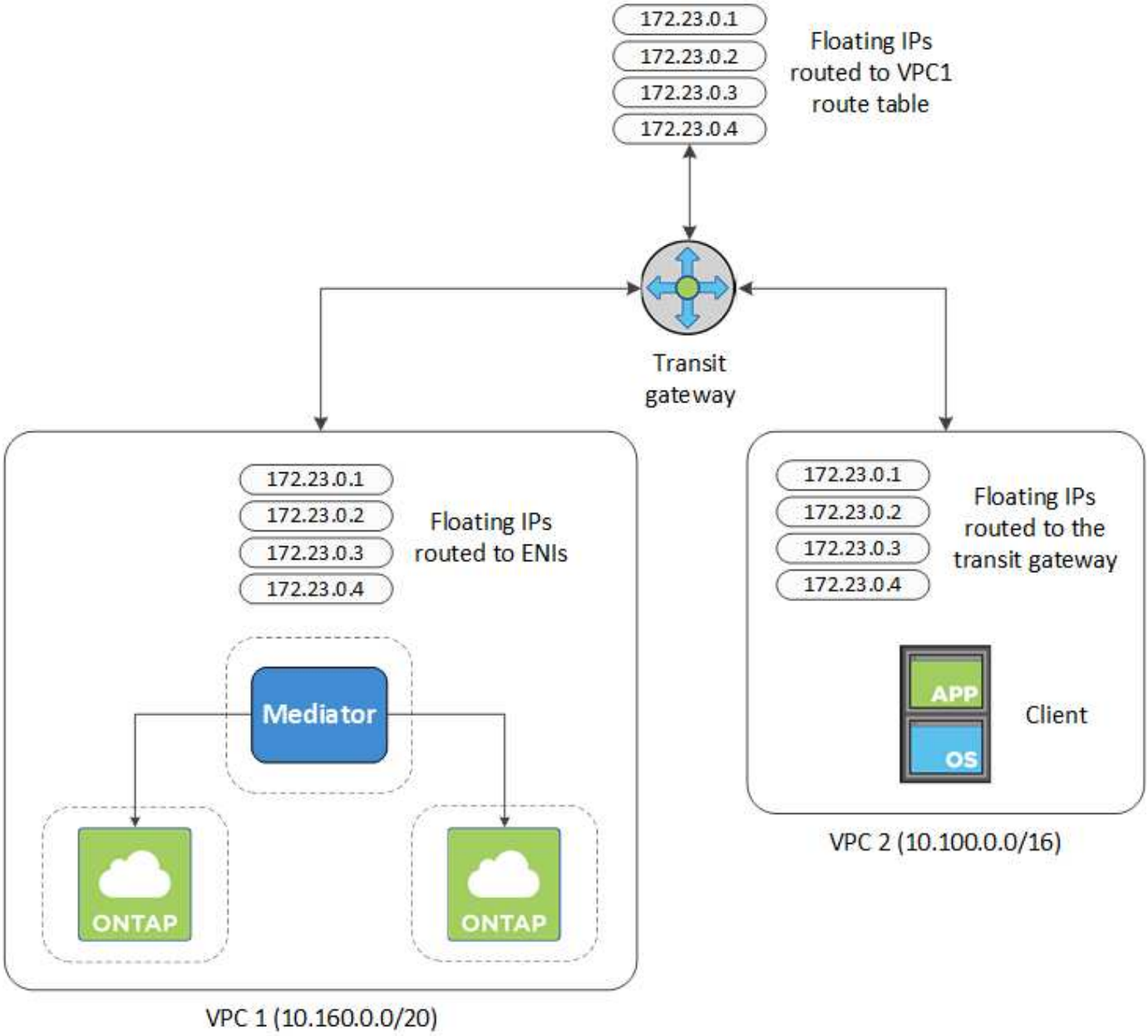
へのアクセスを有効にするために、 AWS 転送ゲートウェイを設定します HA ペアの 1 つ "フローティング IP アドレス" HA ペアが存在する VPC の外部から

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。

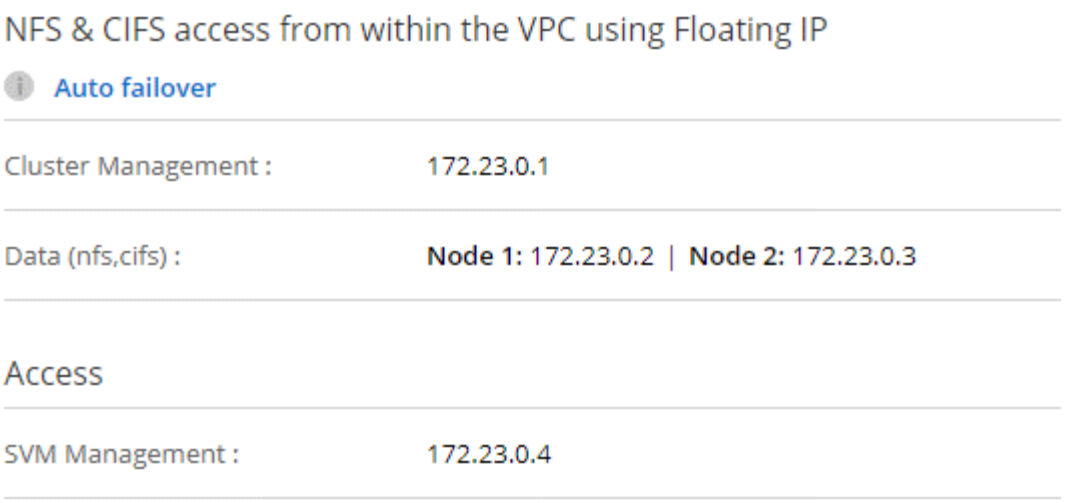


以下に、同様の構成を設定する手順を示します。

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. 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。



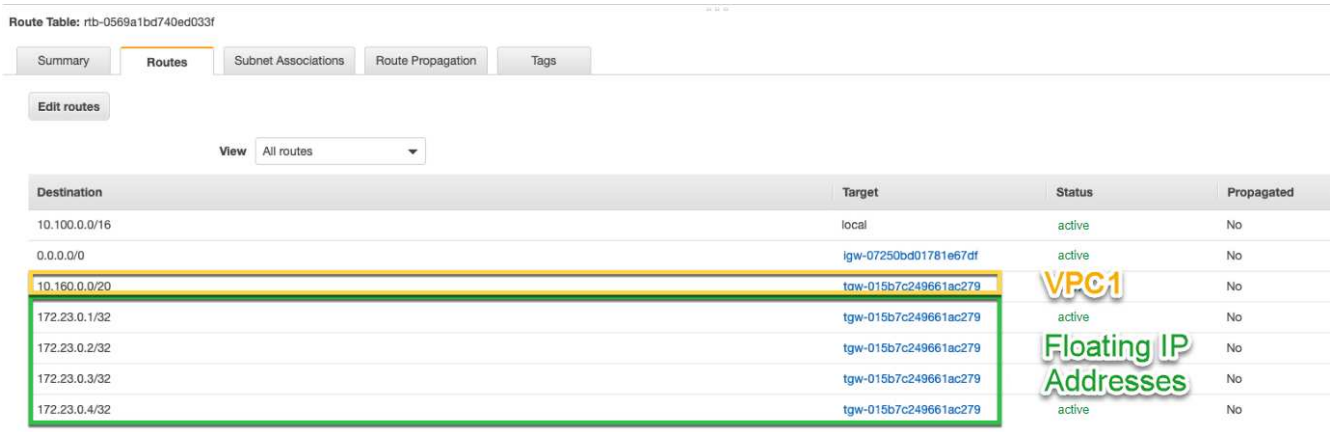
次の図は、中継ゲートウェイのルートテーブルを示しています。このルートには、 2 つの VPC の CIDR ブロックへのルートと、 Cloud Volumes ONTAP で使用される 4 つのフローティング IP アドレスが含まれます。

3. 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。

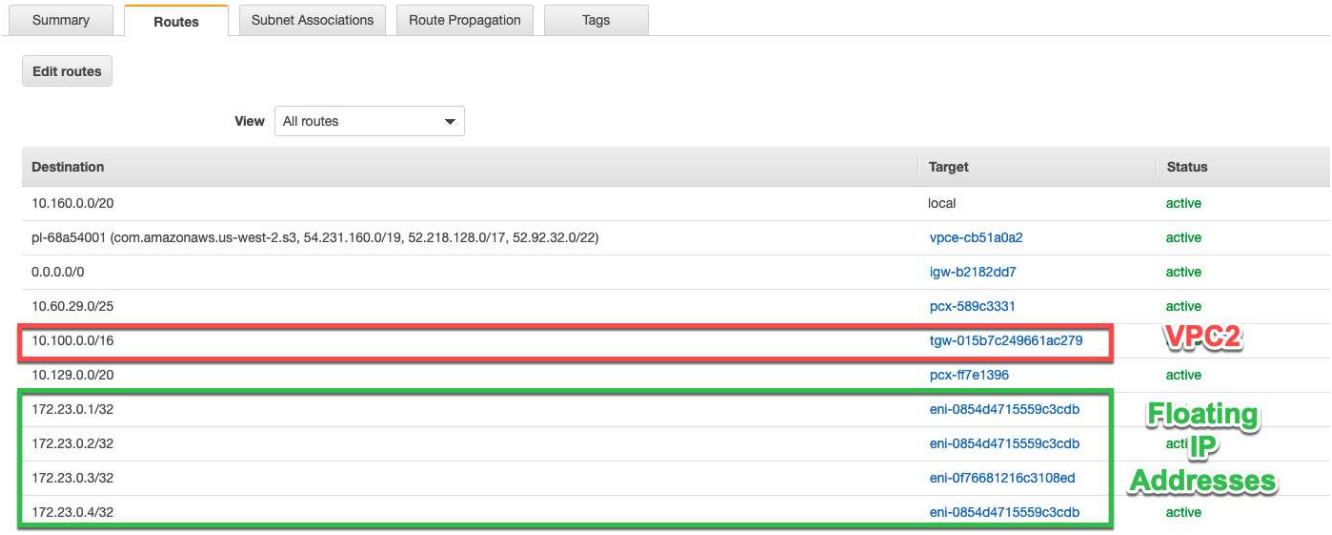
      次の図は、 VPC 1 へのルートとフローティング IP アドレスを含む VPC 2 のルートテーブルを示しています。



4. 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。

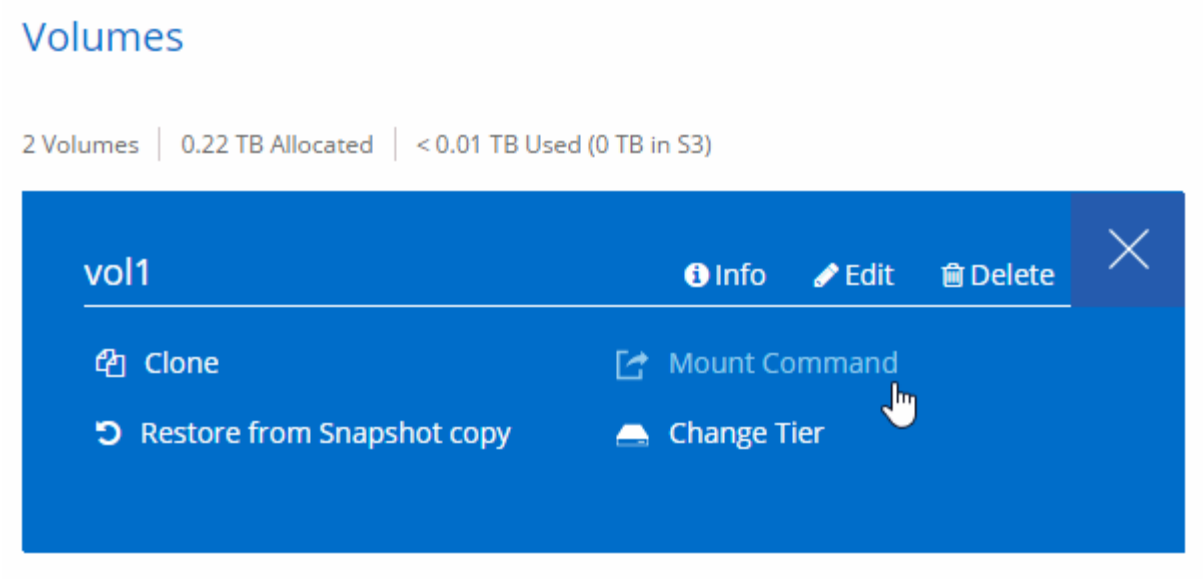
   VPC 間のルーティングが完了するため、この手順は重要です。

   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。



5. 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。



- 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
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

プロトコル	ポート	目的
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モニタ
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モニタ
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 ）
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

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
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への HTTP アクセスを提供します Cloud Compliance からのユーザインターフェイスと接続
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 Compliance 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
クラウドコンプライアンス	HTTP	80	Cloud Compliance インスタンス	Cloud Volumes ONTAP 向けクラウドコンプライアンス

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。Cloud Manager および Cloud Volumes ONTAP と同じ AWS アカウントにすることも、別の AWS アカウントにすることもできます。

   "AWS ドキュメント：「 Customer Master Keys （ CMK ；カスタマーマスターキー）」"

2. 各 CMK のキーポリシーを変更します。変更するには、 Cloud Manager に a_key user_権限 を付与する IAM ロールを追加します。

   IAM ロールをキーユーザとして追加すると、 Cloud Volumes ONTAP で CMK を使用する権限が Cloud Manager に付与されます。

   "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。

   a. 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。

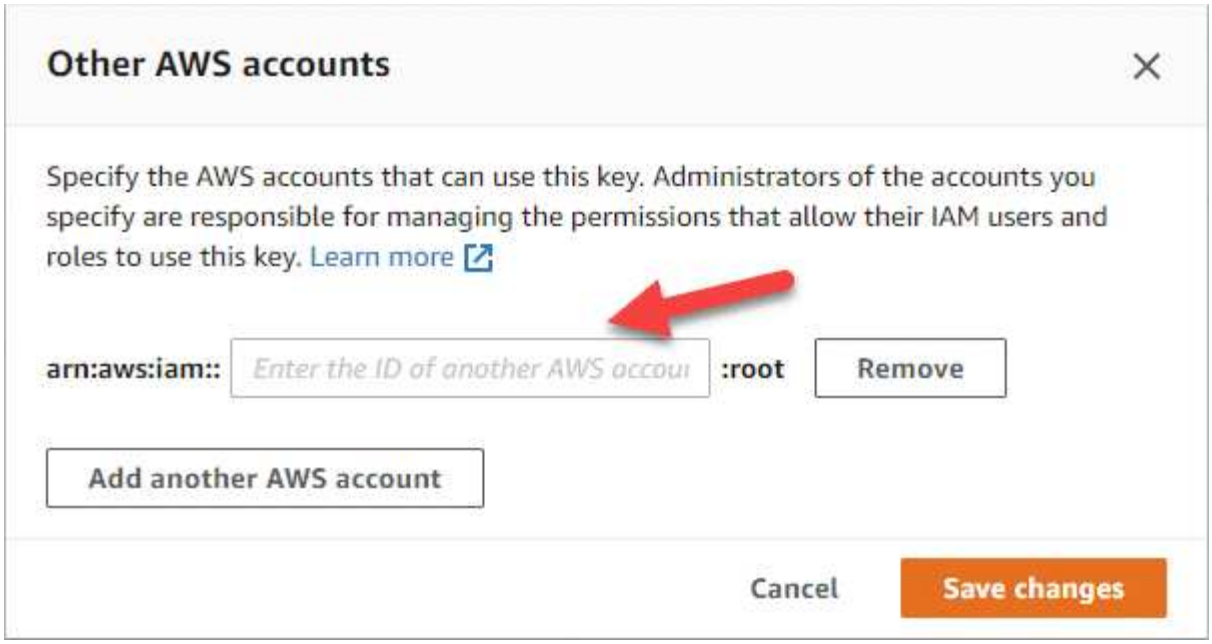
   b. キーを選択します。

   c. General configuration * ペインで、キーの ARN をコピーします。

      Cloud Volumes ONTAP システムの作成時には、 Cloud Manager の ARN の指定が必要になります。

   d. その他の AWS アカウント * ペインで、 Cloud Manager 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、 Cloud Manager が配置されているアカウントです。Cloud Manager が AWS にインストールされていない場合、 Cloud Manager に AWS アクセスキーを指定したアカウントになります。



e. 次に、 Cloud Manager 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。

f. 以下の権限を含む IAM ポリシーを作成します。

g. Cloud Manager に権限を付与する IAM ロールまたは IAM ユーザにポリシーを関連付けます。

次のポリシーは、 Cloud Manager 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 ドキュメント：「外部 AWS アカウントによる CMK へのアクセスの許可"。

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。

AWS でのシングルノード Cloud Volumes ONTAP システムの起動

Cloud Volumes ONTAP を AWS で起動する場合は、 Cloud Manager で新しい作業環境を作成する必要があります。

作業を開始する前に

- 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"。

> コネクタを作成するには、アカウント管理者である必要があります。最初の Cloud Volumes ONTAP 作業環境を作成する際、まだコネクタがない場合はコネクタの作成を求めるメッセージが表示されます。

- "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"。
- 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"。
- BYOL システムを起動する場合は、 20 桁のシリアル番号（ライセンスキー）が必要です。
- CIFS を使用する場合は、 DNS と Active Directory を設定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 in AWS のネットワーク要件"。

このタスクについて

作業環境を作成した直後に、 Cloud Manager は指定された vPC でテストインスタンスを起動して接続を確認します。成功すると、 Cloud Manager はすぐにインスタンスを終了し、 Cloud Volumes ONTAP システムの導入を開始します。Cloud Manager が接続を確認できない場合、作業環境の作成は失敗します。テストインスタンスは、 t2.nano （デフォルトの vPC テナンシーの場合）または m3.medium （専用の vPC テナンシーの場合）のいずれかです。

手順

1. [作業環境] ページで、 [* 作業環境の追加 *] をクリックし、画面の指示に従います。
2. * 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。
3. * 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。

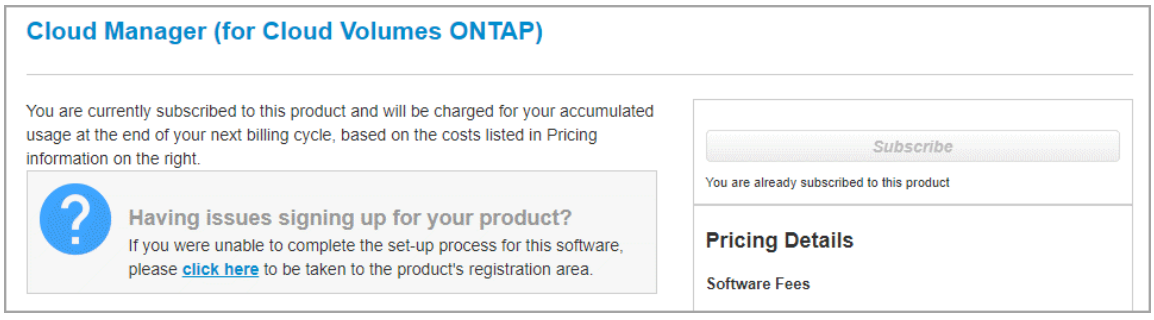
フィールド	説明
作業環境名	Cloud Manager は、作業環境名を使用して、 Cloud Volumes ONTAP システムと Amazon EC2 インスタンスの両方に名前を付けます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。

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。Cloud Manager は、 Cloud Volumes ONTAP インスタンスおよびインスタンスに関連付けられた各 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 "AWS ドキュメント：「 Tagging your Amazon EC2 Resources"。
ユーザ名とパスワード	これらは、 Cloud Volumes ONTAP クラスタ管理アカウントのクレデンシャルです。これらのクレデンシャルを使用して、 OnCommand System Manager またはその CLI を使用して Cloud Volumes ONTAP に接続できます。
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。[サブスクリプションの追加] をクリックして、選択した資格情報をサブスクリプションに関連付けます。従量課金制の Cloud Volumes ONTAP システムを作成するには、 AWS Marketplace から Cloud Volumes ONTAP へのサブスクリプションに関連付けられている AWS クレデンシャルを選択する必要があります。お客様が作成した Cloud Volumes ONTAP 9.6 以降の PAYGO システムと、有効にしたアドオン機能ごとに、このサブスクリプションから料金が請求されます。"Cloud Manager 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"。

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。

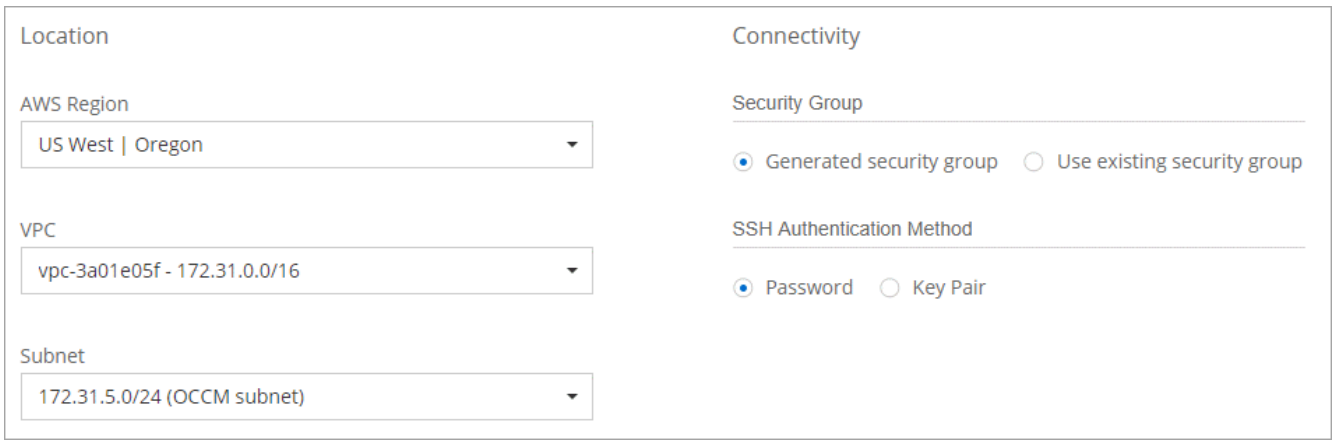
► https://docs.netapp.com/ja-jp/occm38//media/video_subscribing_aws.mp4 *(video)*

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。以下のメッセージが表示された場合は、 * ここをクリック * リンクをクリックして Cloud Central にアクセスし、処理を完了してください。



4. * 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。
   - "Cloud Compliance の詳細はこちらをご覧ください"。
   - "クラウドへのバックアップの詳細については、こちらをご覧ください"。
   - "モニタリングの詳細"。
5. * Location & Connectivity * ： AWS の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。

次の図は、入力済みのページを示しています。



6. * 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の詳細を確認してください"。

7. * ライセンスとサポートサイトのアカウント * ：従量課金制または BYOL のどちらを使用するかを指定し、 NetApp Support Site のアカウントを指定します。

   ライセンスの仕組みについては、を参照してください "ライセンス"。

   NetApp Support Site のアカウントは、従量課金制の場合は任意ですが、 BYOL システムの場合は必須です。 "ネットアップサポートサイトのアカウントを追加する方法について説明します"。

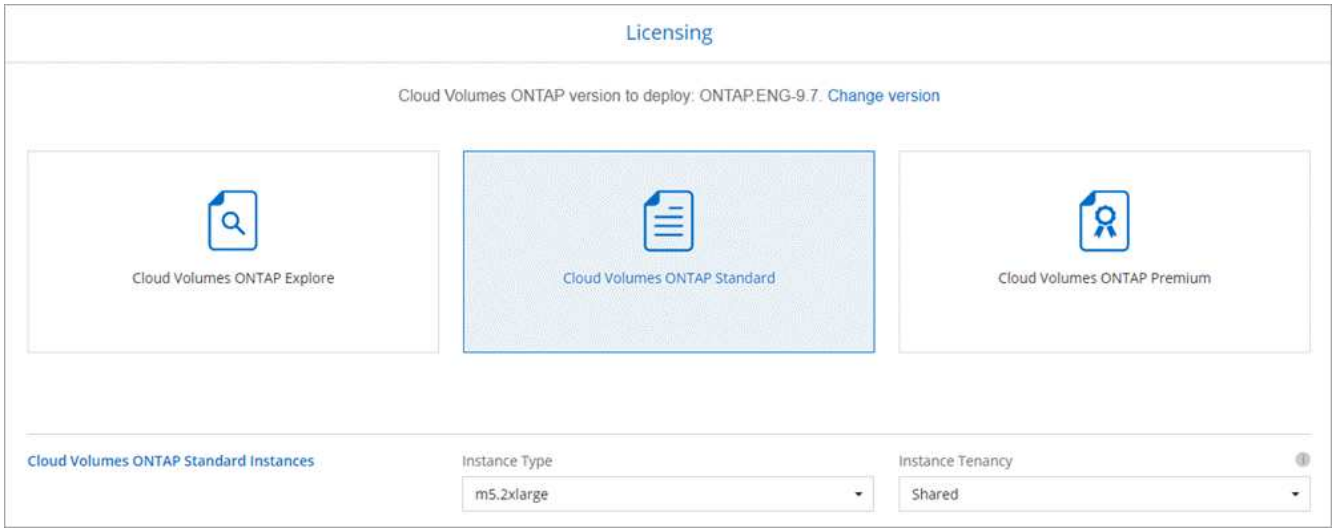
8. * 構成済みパッケージ * ： Cloud Volumes ONTAP をすばやく起動するパッケージを 1 つ選択するか、 * 独自の構成を作成 * をクリックします。

   いずれかのパッケージを選択した場合は、ボリュームを指定してから、設定を確認して承認するだけで済みます。

9. * IAM Role * ： Cloud Manager でロールを作成する場合は、デフォルトのオプションを使用してください。

   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"。

10. * ライセンス * ：必要に応じて Cloud Volumes ONTAP のバージョンを変更し、ライセンス、インスタンスタイプ、インスタンステナンシーを選択します。



インスタンスの起動後に必要な変更があった場合は、後でライセンスまたはインスタンスタイプを変更できます。

選択したバージョンで新しいリリース候補、一般的な可用性、またはパッチリリースが利用可能な場合は、作業環境の作成時に Cloud Manager によって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 9.6 RC1 と 9.6 GA を選択した場合、更新が行われます。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。

11. * 基盤となるストレージリソース * ：初期アグリゲートの設定を選択します。ディスクタイプ、各ディスクのサイズ、データの階層化を有効にするかどうかを指定します。

    次の点に注意してください。

    - ディスクタイプは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。
    - ディスクサイズは、最初のアグリゲート内のすべてのディスクと、シンプルプロビジョニングオプションを使用したときに Cloud Manager によって作成される追加のアグリゲートに適用されます。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。

      ディスクの種類とサイズの選択については、を参照してください "AWS でのシステムのサイジング"。

    - 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"。

12. * Write Speed & WORM * ：「 * Normal * 」または「 * High * write speed 」を選択し、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。

    書き込み速度の選択はシングルノードシステムでのみサポートされます。

    "書き込み速度の詳細については、こちらをご覧ください。"。

    データの階層化が有効になっていると、 WORM を有効にできません。

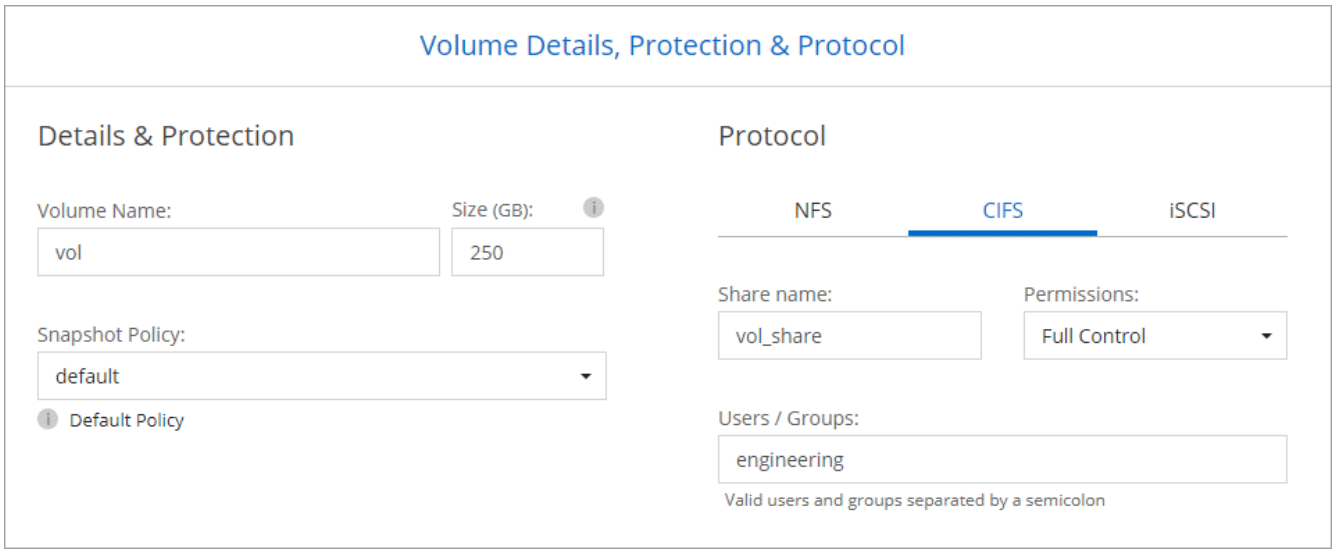
"WORM ストレージの詳細については、こちらをご覧ください。"。

13. * 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。

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、 Cloud Manager 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、 Cloud Manager 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。



14. * 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 "Cloud Manager API 開発者ガイド" を参照してください。

15. * 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"。

16. * 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、 Cloud Manager で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 Manager が Cloud Volumes ONTAP インスタンスを起動します。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

Cloud Volumes ONTAP HA ペアを AWS で起動する場合は、 Cloud Manager で HA 作業環境を作成する必要があります。

作業を開始する前に

- 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"。

  コネクタを作成するには、アカウント管理者である必要があります。最初の Cloud Volumes ONTAP 作業環境を作成する際、まだコネクタがない場合はコネクタの作成を求めるメッセージが表示されます。

- "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"。
- 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"。
- BYOL ライセンスを購入した場合は、ノードごとに 20 桁のシリアル番号（ライセンスキー）が必要です。
- CIFS を使用する場合は、 DNS と Active Directory を設定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 in AWS のネットワーク要件"。

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、 Cloud Manager は指定された vPC でテストインスタンスを起動して接続を確認

します。成功すると、 Cloud Manager はすぐにインスタンスを終了し、 Cloud Volumes ONTAP システムの導入を開始します。Cloud Manager が接続を確認できない場合、作業環境の作成は失敗します。テストインスタンスは、 t2.nano （デフォルトの vPC テナンシーの場合）または m3.medium （専用の vPC テナンシーの場合）のいずれかです。

手順

1. [作業環境] ページで、 [* 作業環境の追加 *] をクリックし、画面の指示に従います。
2. * 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。
3. * 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。

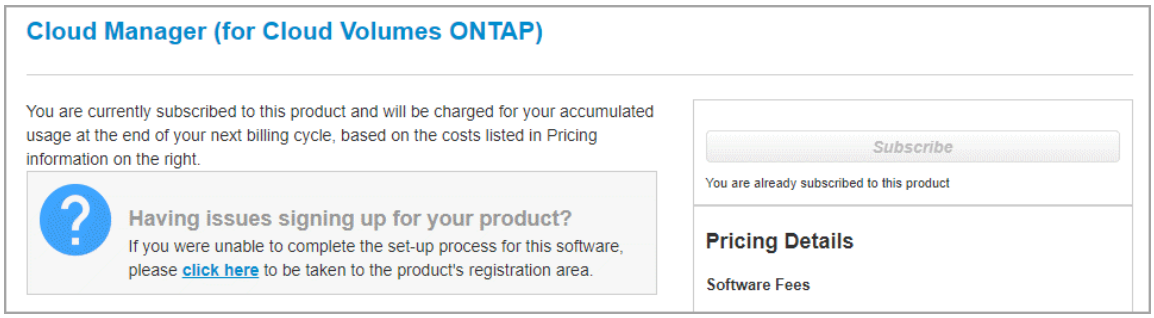
   このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
作業環境名	Cloud Manager 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。Cloud Manager は、 Cloud Volumes ONTAP インスタンスおよびインスタンスに関連付けられた各 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 "AWS ドキュメント：「 Tagging your Amazon EC2 Resources"。
ユーザ名とパスワード	これらは、 Cloud Volumes ONTAP クラスタ管理アカウントのクレデンシャルです。これらのクレデンシャルを使用して、 OnCommand System Manager またはその CLI を使用して Cloud Volumes ONTAP に接続できます。
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。[サブスクリプションの追加] をクリックして、選択した資格情報をサブスクリプションに関連付けます。従量課金制の Cloud Volumes ONTAP システムを作成するには、 AWS Marketplace から Cloud Volumes ONTAP へのサブスクリプションに関連付けられている AWS クレデンシャルを選択する必要があります。お客様が作成した Cloud Volumes ONTAP 9.6 以降の PAYGO システムと、有効にしたアドオン機能ごとに、このサブスクリプションから料金が請求されます。"Cloud Manager 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"。

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。

► https://docs.netapp.com/ja-jp/occm38//media/video_subscribing_aws.mp4 *(video)*

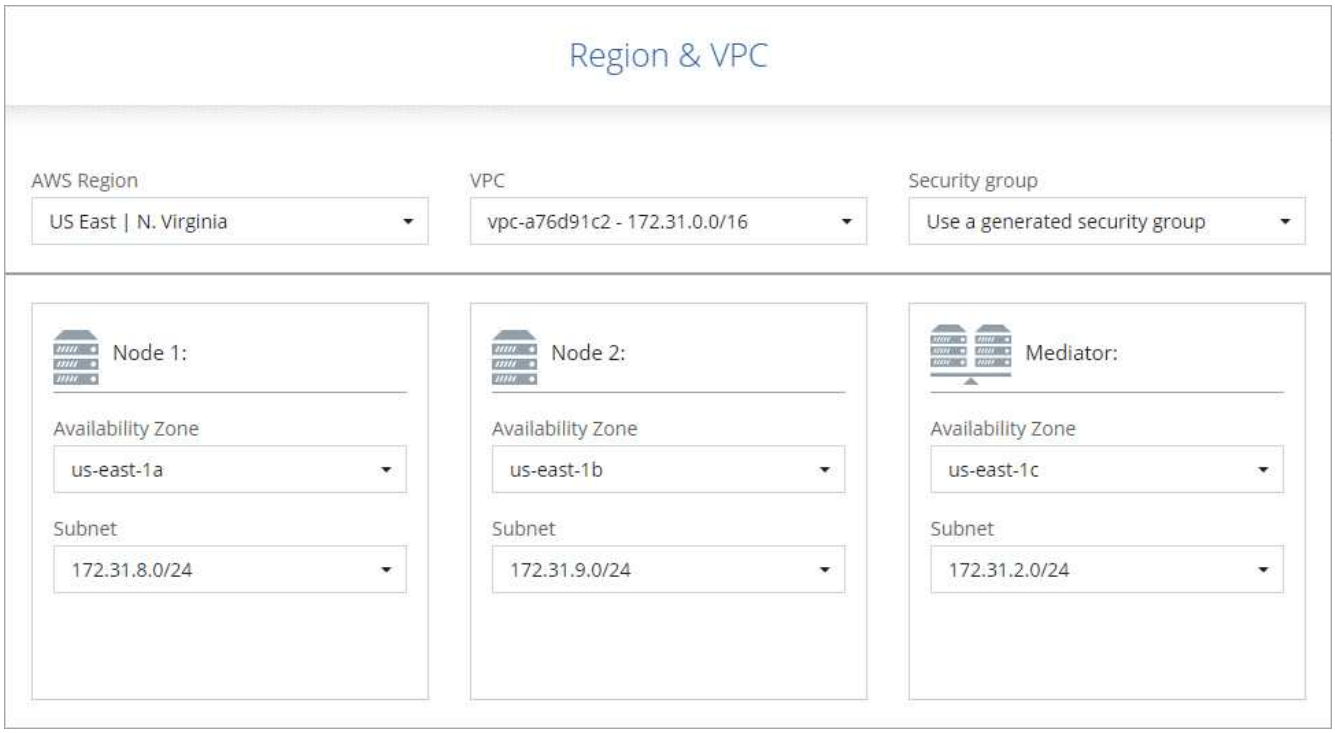
複数の IAM ユーザが同じ AWS アカウントで作業する場合は、各ユーザにサブスクライブする必要があります。最初のユーザがサブスクライブすると、次の図に示すように、 AWS Marketplace から後続のユーザに登録済みであることが通知されます。AWS_account_ のサブスクリプションが設定されている間、各 IAM ユーザは、そのサブスクリプションに自分自身を関連付ける必要があります。以下のメッセージが表示された場合は、 * ここをクリック * リンクをクリックして Cloud Central にアクセスし、処理を完了してください。



4. * 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。
   - "Cloud Compliance の詳細はこちらをご覧ください"。
   - "クラウドへのバックアップの詳細については、こちらをご覧ください"。
   - "モニタリングの詳細"。
5. *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"。
6. * Region & VPC * ： 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。

   次の図は、複数の AZ 構成に対応するページを示しています。



7. * 接続と SSH 認証 * ： HA ペアとメディエーターの接続方法を選択します。
8. * 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"。
9. * 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"。
10. * 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"。

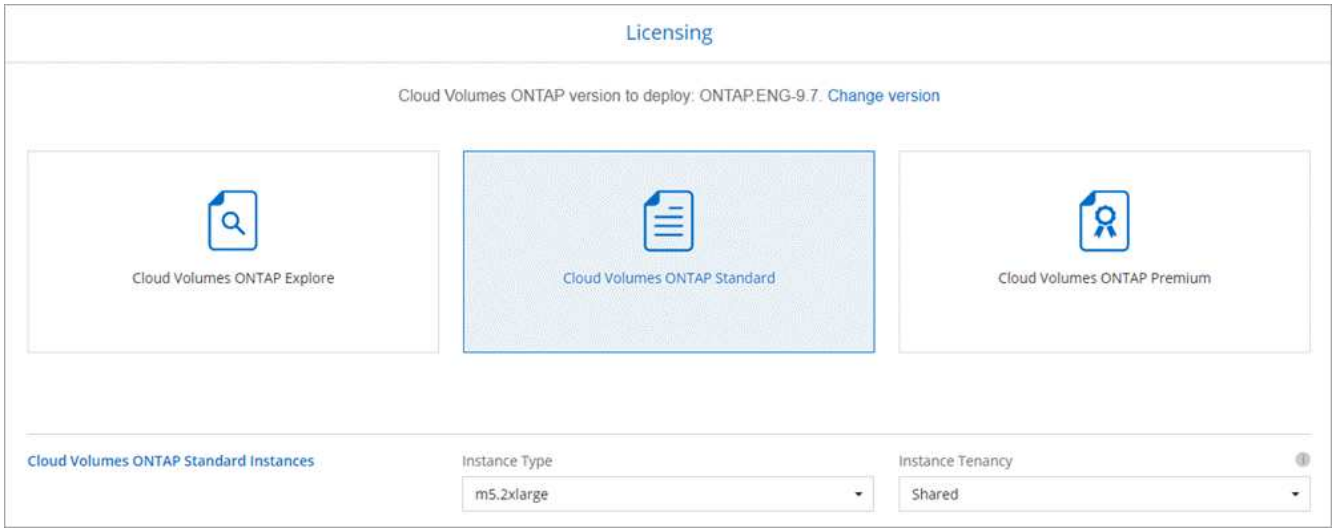
    "サポートされている暗号化テクノロジの詳細を確認してください"。
11. * ライセンスとサポートサイトのアカウント * ：従量課金制または BYOL のどちらを使用するかを指定し、 NetApp Support Site のアカウントを指定します。

    ライセンスの仕組みについては、を参照してください "ライセンス"。

    NetApp Support Site のアカウントは、従量課金制の場合は任意ですが、 BYOL システムの場合は必須です。 "ネットアップサポートサイトのアカウントを追加する方法について説明します"。
12. * 構成済みパッケージ * ： Cloud Volumes ONTAP システムをすばやく起動するには、パッケージを 1 つ選択するか、 * 独自の構成を作成 * をクリックします。

    いずれかのパッケージを選択した場合は、ボリュームを指定してから、設定を確認して承認するだけで済みます。
13. * IAM Role * ：デフォルトのオプションをそのまま使用し、 Cloud Manager で役割を作成する必要があります。

    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"。
14. * ライセンス * ：必要に応じて Cloud Volumes ONTAP のバージョンを変更し、ライセンス、インスタンスタイプ、インスタンステナンシーを選択します。



インスタンスの起動後に必要な変更があった場合は、後でライセンスまたはインスタンスタイプを変更できます。

選択したバージョンで新しいリリース候補、一般的な可用性、またはパッチリリースが利用可能な場合は、作業環境の作成時に Cloud Manager によって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 9.6 RC1 と 9.6 GA を選択した場合、更新が行われます。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。

15. * 基盤となるストレージリソース * ：初期アグリゲートの設定を選択します。ディスクタイプ、各ディスクのサイズ、データの階層化を有効にするかどうかを指定します。

    次の点に注意してください。

    - ディスクタイプは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。
    - ディスクサイズは、最初のアグリゲート内のすべてのディスクと、シンプルプロビジョニングオプションを使用したときに Cloud Manager によって作成される追加のアグリゲートに適用されます。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。

      ディスクの種類とサイズの選択については、を参照してください "AWS でのシステムのサイジング"。

    - 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"。

16. * WORM * ：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。

    データの階層化が有効になっていると、 WORM を有効にできません。

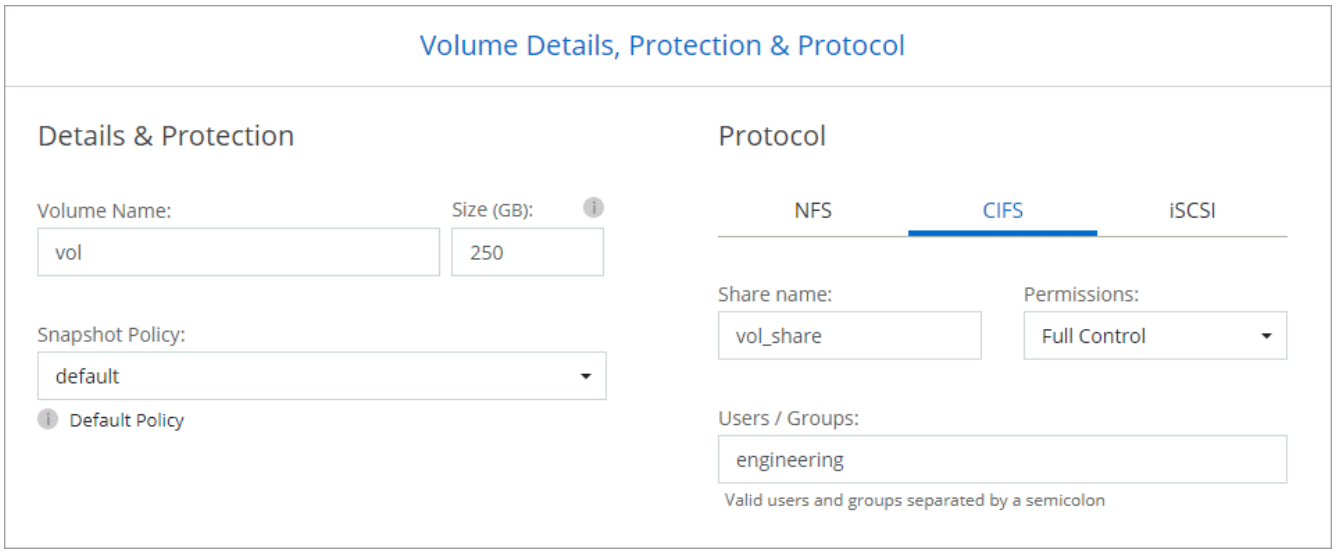
    "WORM ストレージの詳細については、こちらをご覧ください。"。

17. * 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。

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、 Cloud Manager 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、 Cloud Manager 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。



18. * 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 "Cloud Manager API 開発者ガイド" を参照してください。

19. * 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"。

20. * 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、 Cloud Manager で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 Manager が Cloud Volumes ONTAP HA ペアを起動します。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。

著作権に関する情報

商標に関する情報