Amazon Web Services の利用を開始しましょう Cloud Volumes ONTAP

NetApp
June 21, 2022

目次

Amazon Web Services の利用を開始しましょう

AWS での Cloud Volumes ONTAP のクイックスタート

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

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。

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。"。

<img src="https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-3.png" Alt="3"> ネットワークを設定します

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"。

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。"。

[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

- "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Cloud Volumes ONTAP 構成を計画

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。

Cloud Volumes ONTAP ライセンスを選択します

Cloud Volumes ONTAP には、いくつかのライセンスオプションがあります。それぞれのオプションで、ニーズに合った消費モデルを選択できます。

- "Cloud Volumes ONTAP のライセンスオプションについて説明します"
- "ライセンスの設定方法について説明します"

サポートされているリージョンを選択します

Cloud Volumes ONTAP はほとんどの AWS リージョンでサポートされています。 "サポートされているリージョンの完全なリストを表示します"。

新しい AWS リージョンは、それらのリージョンでリソースを作成および管理する前に有効にする必要があります。 "リージョンを有効にする方法について説明します"。

サポートされているインスタンスを選択します

Cloud Volumes ONTAP では、選択したライセンスタイプに応じて、複数のインスタンスタイプがサポートされます。

"AWS で Cloud Volumes ONTAP がサポートされる構成"

ストレージの制限を確認

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 での Cloud Volumes ONTAP のストレージの制限"

AWSでシステムのサイズを設定します

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

EBS ディスクタイプの違いは次のとおりです。EBS ディスクのユースケー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"。

- _General Purpose SSD （ GP3 ） _ ディスクは、幅広いワークロードに対してコストとパフォーマンスのバランスを取る最も低コストの SSD です。パフォーマンスは、 IOPS とスループットを基準に定義されます。GP3 ディスクは Cloud Volumes ONTAP 9.7 以降でサポートされています。

  GP3 ディスクを選択すると、 Cloud Manager はデフォルトの IOPS とスループットの値を入力し、選択したディスクサイズに基づいて gp2 ディスクに相当するパフォーマンスを提供します。この値を増やすと、コストを高くしてもパフォーマンスを向上させることができますが、パフォーマンスが低下する可能性があるため、値を小さくすることはできません。つまり、デフォルト値をそのまま使用するか、値を大きくします。低くしないでください。 "GP3 ディスクとそのパフォーマンスについては、こちらをご覧ください"。

  Cloud Volumes ONTAP は、GP3ディスクを使用したAmazon EBS Elastic Volumes機能をサポートしています。 "Elastic Volumesのサポートに関する詳細情報"。

- _ 汎用 SSD （ gp2 ） _ ディスクは、幅広いワークロードに対してコストとパフォーマンスのバランスを取ります。パフォーマンスは IOPS の観点から定義されます。
- _Provisioned IOPS SSD （ io1 ） _disks は、コストが高くても最高のパフォーマンスが求められる重要なアプリケーション用です。

  Cloud Volumes ONTAP では、io1ディスクを使用したAmazon EBS Elastic Volumes機能がサポートされています。 "Elastic Volumesのサポートに関する詳細情報"。

- _Throughput Optimized HDD （ st1 ） _disks は、高速で安定したスループットを必要とする、アクセス頻度の高いワークロード用です。価格は低くなります。

  スループット最適化 HDD （ st1 ）を使用している場合、オブジェクトストレージへのデータの階層化は推奨されません。

EBS ディスクサイズ

をサポートしない構成を選択した場合 "Amazon EBS Elastic Volumes機能"を選択した場合、Cloud Volumes ONTAP システムの起動時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 "アグリゲートの作成は自分で行います"、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 TiB 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"。

前述したように、ディスクサイズの選択は、Amazon EBS Elastic Volumes機能をサポートするCloud Volumes ONTAP 構成ではサポートされていません。 "Elastic Volumesのサポートに関する詳細情報"。

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。

デフォルトのシステムディスクを表示します

ユーザデータ用のストレージに加えて、 Cloud Manager は Cloud Volumes ONTAP システムデータ（ブートデータ、ルートデータ、コアデータ、 NVRAM ）用のクラウドストレージも購入します。計画を立てる場合は、 Cloud Volumes ONTAP を導入する前にこれらの詳細を確認すると役立つ場合があります。

"AWS で Cloud Volumes ONTAP システムデータのデフォルトディスクを表示する"。

コネクタにはシステムディスクも必要です。 "コネクタのデフォルト設定に関する詳細を表示します"。

AWSアウトポストにCloud Volumes ONTAP を導入する準備をします

AWS Outpost を使用している場合は、 Working Environment ウィザードで Outpost VPC を選択して、その Outpost に Cloud Volumes ONTAP を導入できます。エクスペリエンスは、 AWS に存在する他の VPC と同じです。最初に、 AWS Outpost にコネクタを導入する必要があります。

指摘すべき制限事項はいくつかあります。

- でサポートされるのはシングルノードの Cloud Volumes ONTAP システムのみです 今回は
- Cloud Volumes で使用できる EC2 インスタンス ONTAP は、 Outpost で利用できる機能に限定されています
- 現時点では、汎用 SSD （ gp2 ）のみがサポートされます

ネットワーク情報を収集

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。

単一の**AZ**における単一のノードまたは**HA**ペア

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**AZ**にまたがる**HA**ペアを作成します

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	

AWS 情報	あなたの価値
フローティング IP アドレスのルートテーブル	

書き込み速度を選択します

Cloud Manager では、 Cloud Volumes ONTAP の書き込み速度を選択できます。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。 "書き込み速度の詳細については、こちらをご覧ください。"。

ボリュームの使用プロファイルを選択してください

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 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

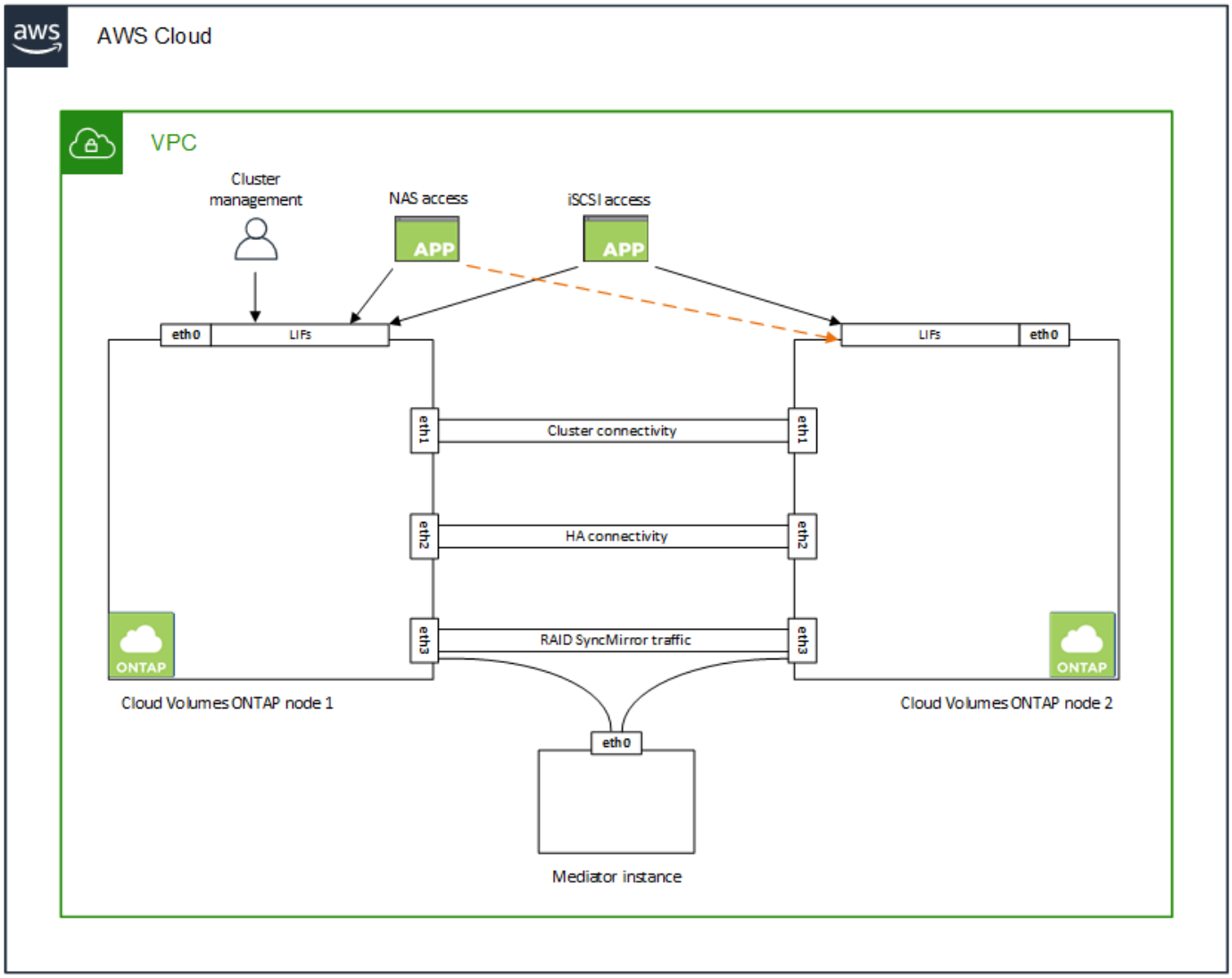
Cloud Manager は、 1 つのノードシステムに 6 つの IP アドレスを割り当てます。

- 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。

LIF	インターフェイス	ノード	目的
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。
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"。

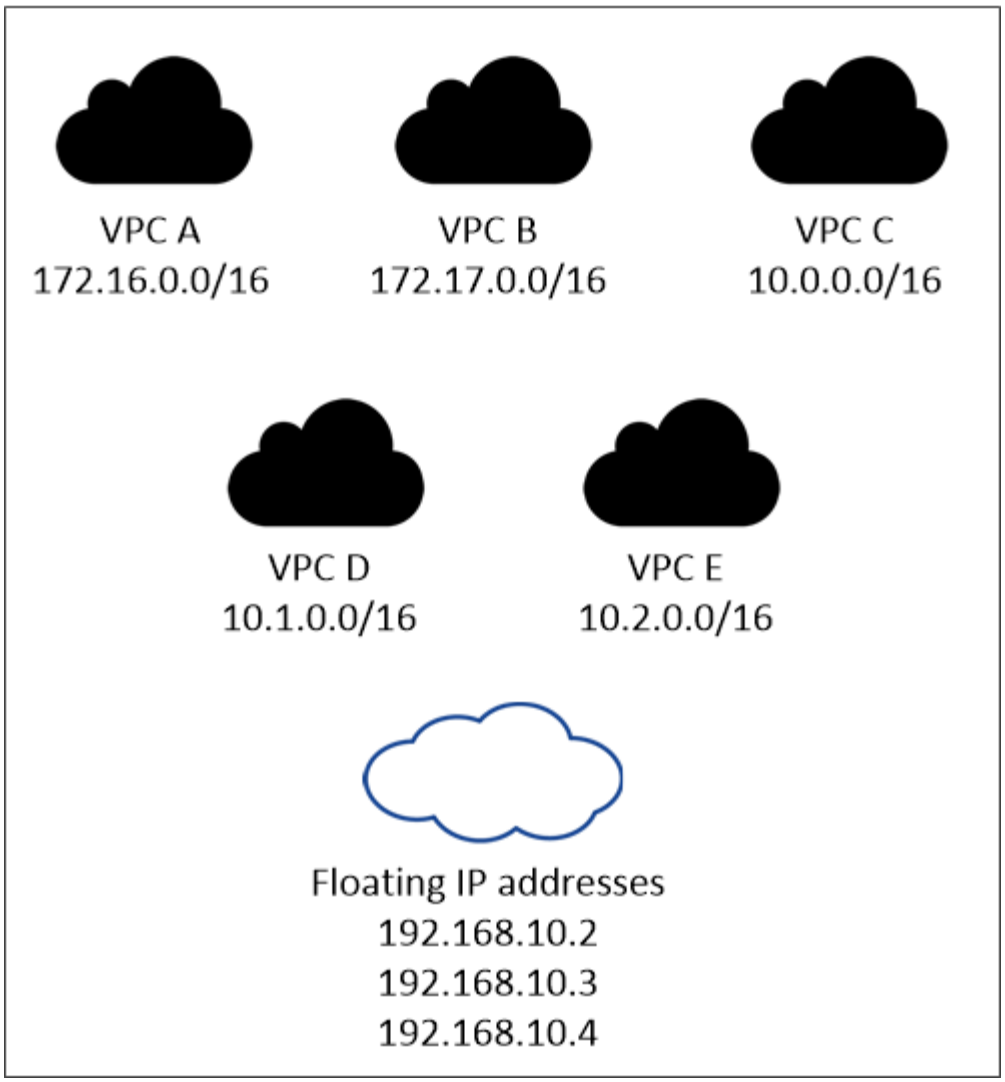
フローティング IP アドレスの 1 つはクラスタ管理用、 1 つはノード 1 の NFS/CIFS データ用、もう 1 つはノード 2 の NFS/CIFS データ用です。SVM 管理用の 4 つ目のフローティング IP アドレスはオプションです。

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。



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"。

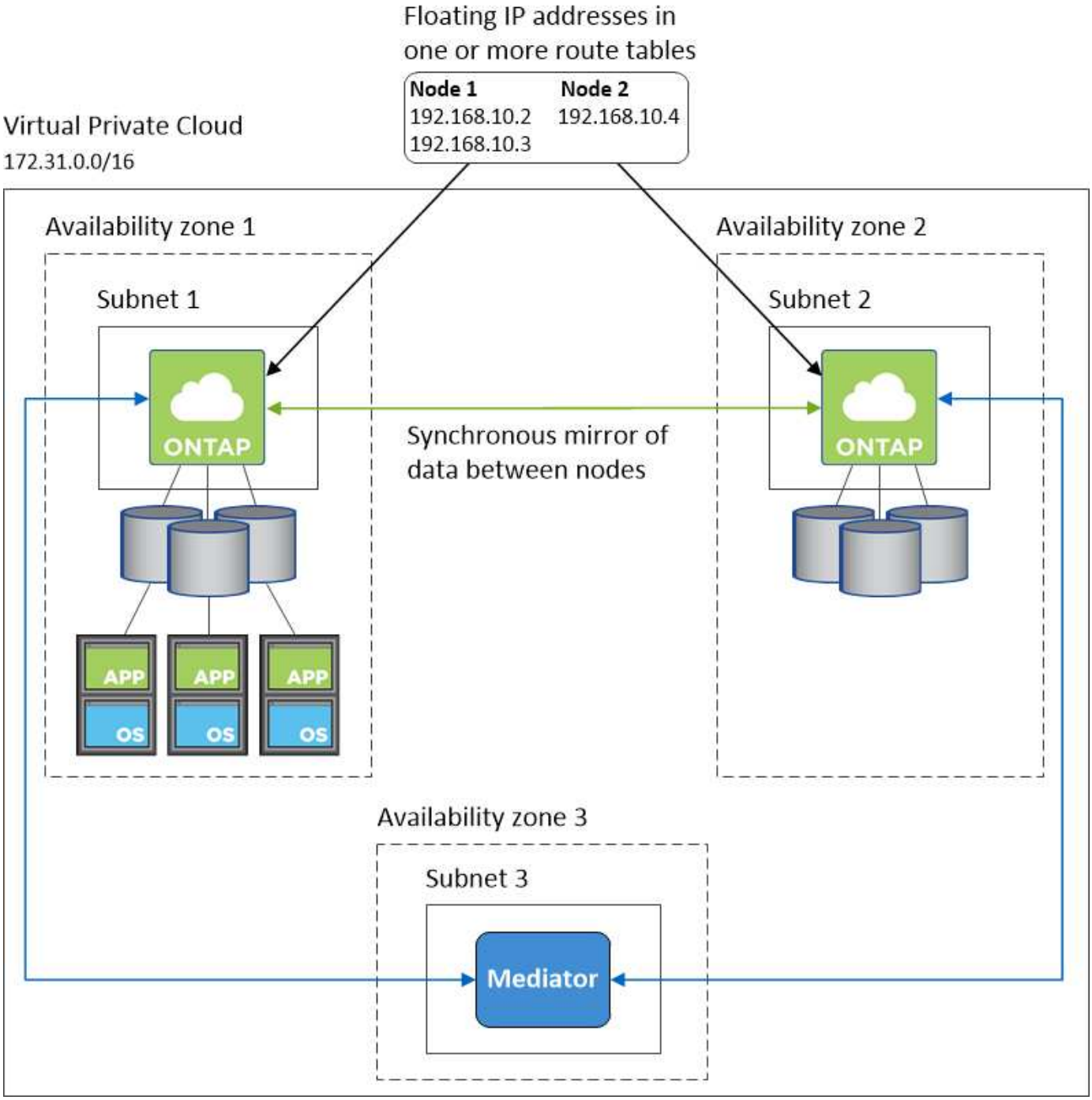
ネットアップの管理ツールとの連携

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://cloudmanagerinfraprod.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**

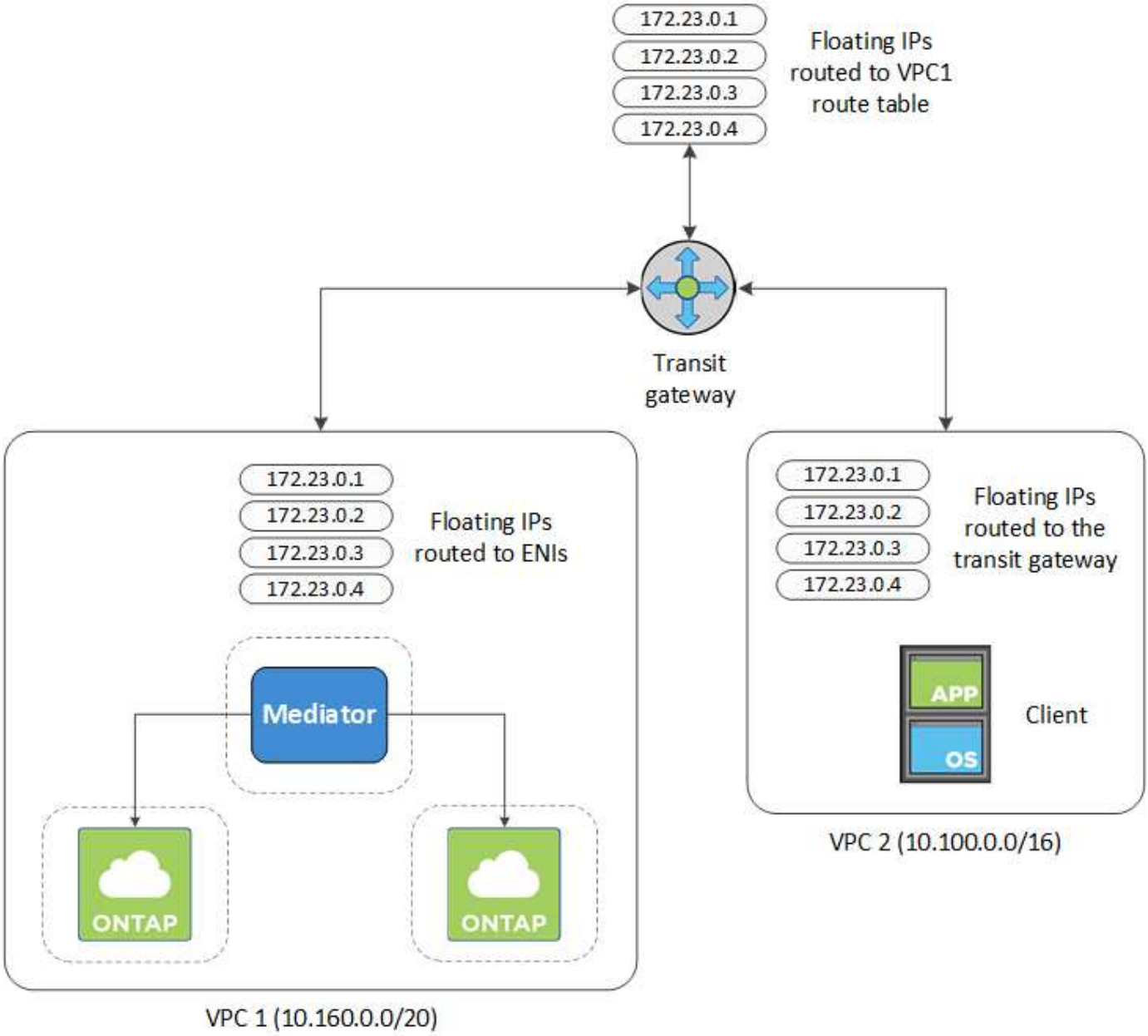
へのアクセスを有効にするために、 AWS 転送ゲートウェイを設定します HA ペアの 1 つ "フローティング IP アドレス" HA ペアが存在する VPC の外部から

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。



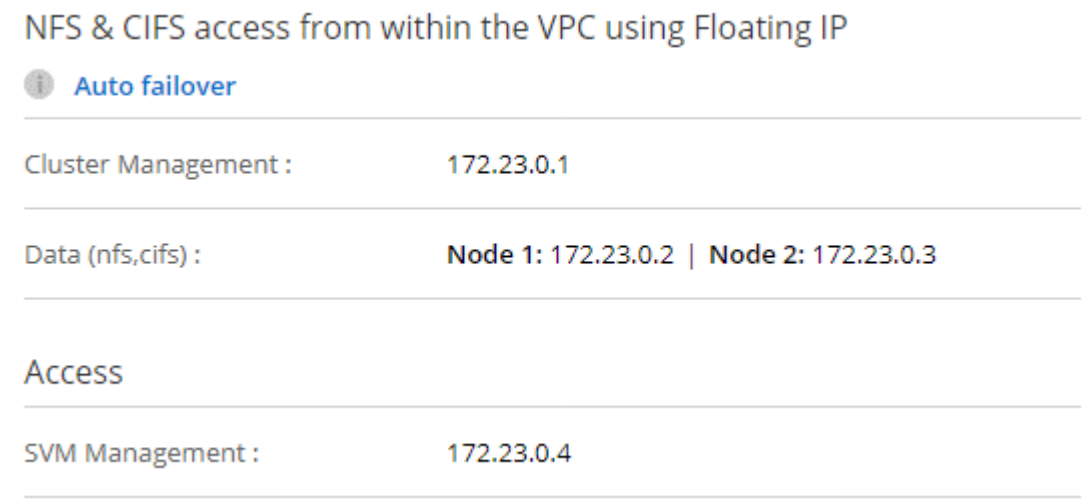
以下に、同様の構成を設定する手順を示します。

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。



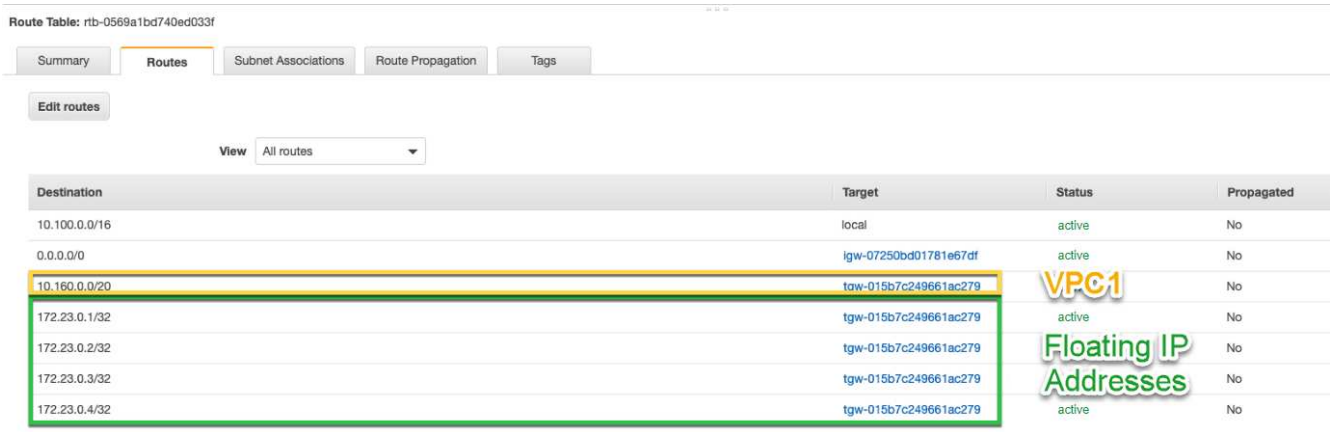
次の図は、中継ゲートウェイのルートテーブルを示しています。このルートには、 2 つの VPC の CIDR ブロックへのルートと、 Cloud Volumes ONTAP で使用される 4 つのフローティング IP アドレスが含まれます。

4. フローティング IP アドレスにアクセスする必要がある VPC のルーティングテーブルを変更します。

   a. フローティング IP アドレスにルートエントリを追加します。

   b. HA ペアが存在する VPC の CIDR ブロックにルートエントリを追加します。

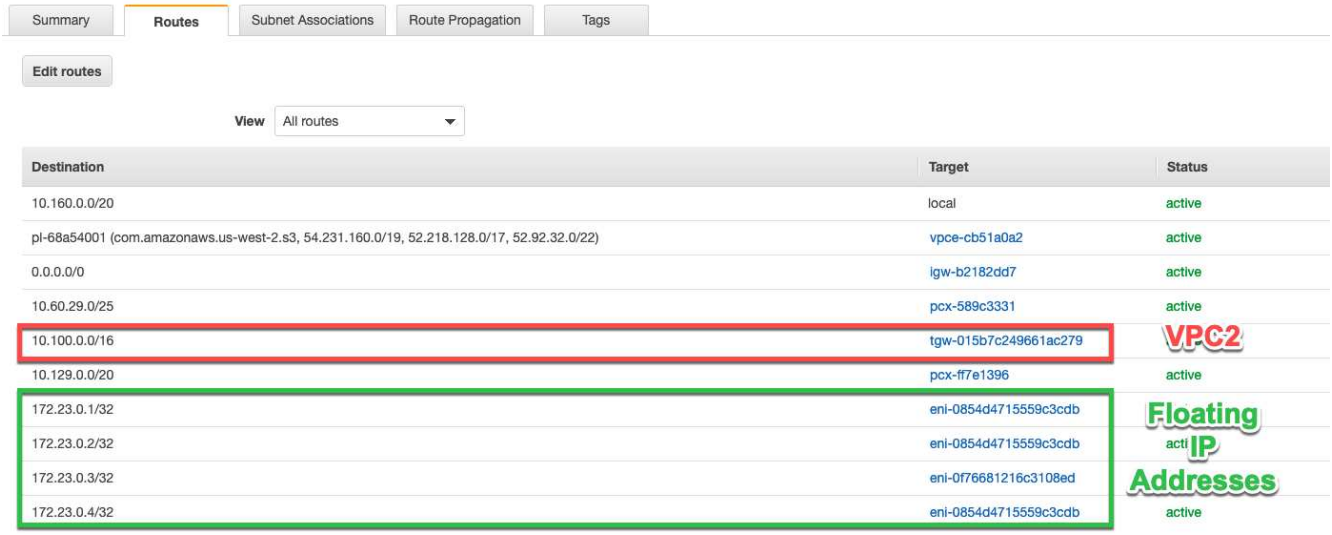
      次の図は、 VPC 1 へのルートとフローティング IP アドレスを含む VPC 2 のルートテーブルを示しています。



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。

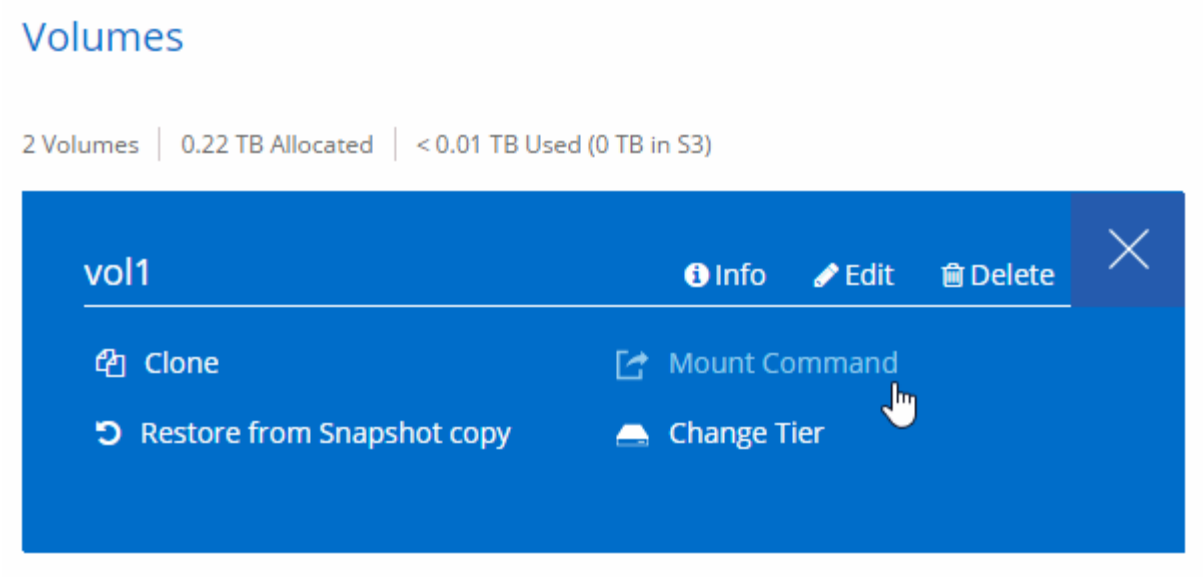
   VPC 間のルーティングが完了するため、この手順は重要です。

   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。



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。



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

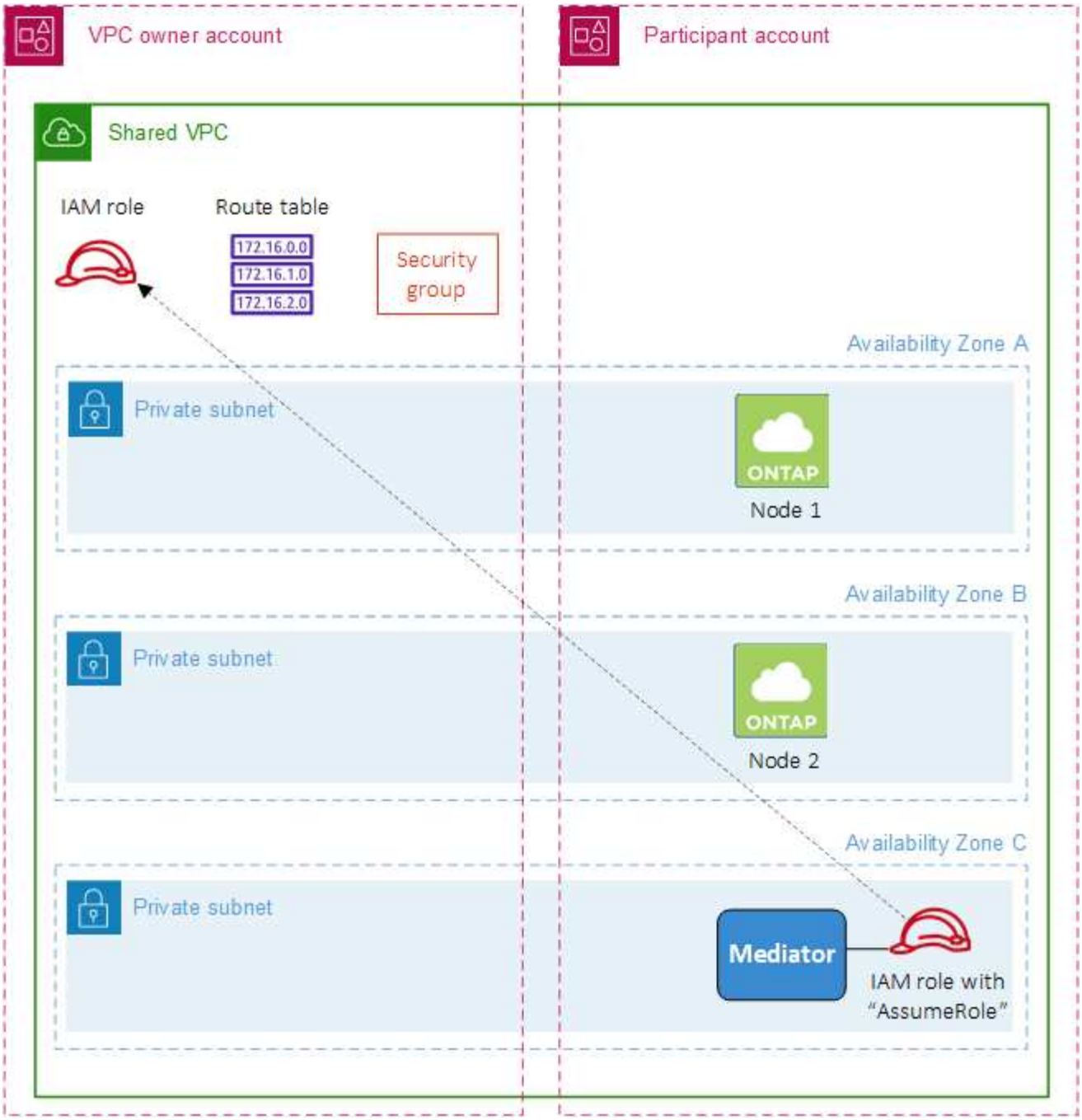
9.11.1リリース以降では、VPCを共有するAWSでCloud Volumes ONTAP HAペアがサポートされます。VPC共有を使用すると、他のAWSアカウントとサブネットを共有できます。この構成を使用するには、AWS環境をセットアップし、APIを使用してHAペアを導入する必要があります。

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. APIを使用して新しいCloud Volumes ONTAP 作業環境を作成し、「haParams」オブジェクトの「"haassereRoleArn"」フィールドを渡します。

   「仮定ロールアーn」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（前の手順を参照）。

   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 ）

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
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

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。

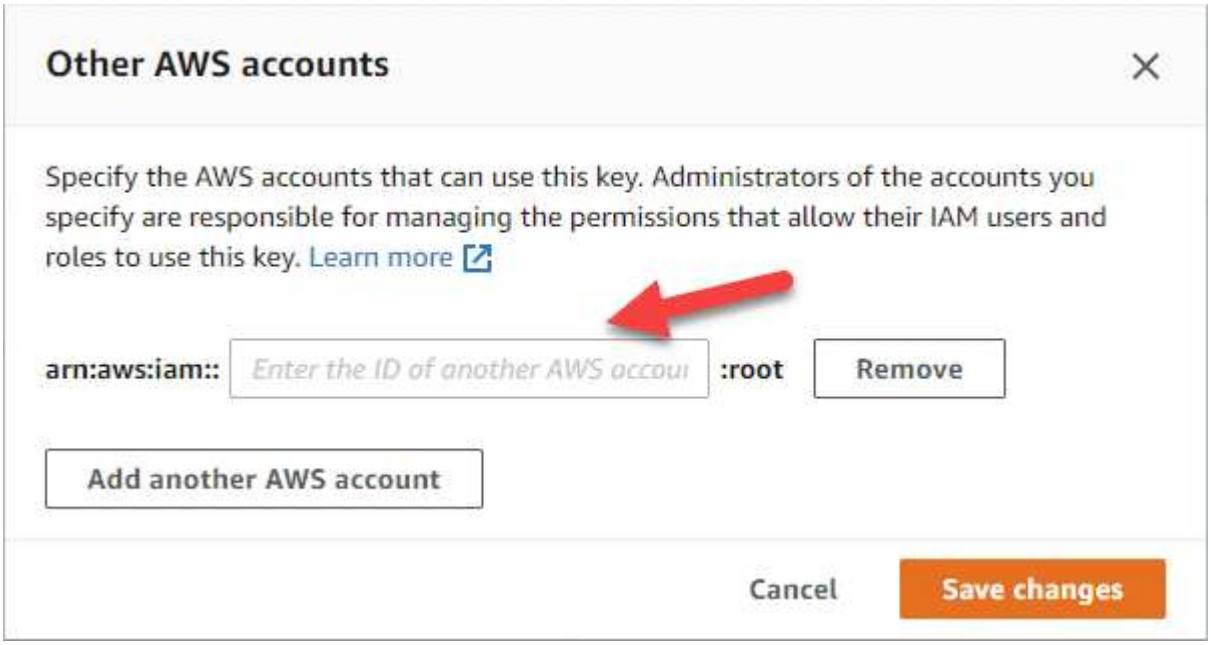
   b. キーを選択します。

   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 のマニュアル：他のアカウントのユーザに KMS キーの使用を許可する"。

4. お客様が管理する CMK を使用している場合は、 Cloud Volumes ONTAP IAM ロールを a_key user_権限

として追加して、 CMK のキーポリシーを変更します。

この手順は、 Cloud Volumes ONTAP でデータの階層化を有効にし、 S3 バケットに格納されているデータを暗号化する場合に必要です。

作業環境の作成時に IAM ロールが作成されるため、このステップの _ 導入後 _ Cloud Volumes ONTAP を実行する必要があります。（もちろん、既存の Cloud Volumes ONTAP IAM ロールを使用することもできるため、この手順を前に実行することもできます）。

"AWS のドキュメント：「キーの編集"

AWSでCloud Volumes ONTAP のライセンスを設定

Cloud Volumes ONTAP で使用するライセンスオプションを決定したら、新しい作業環境を作成する際にそのライセンスオプションを選択する前に、いくつかの手順を実行する必要があります。

フリーミアム

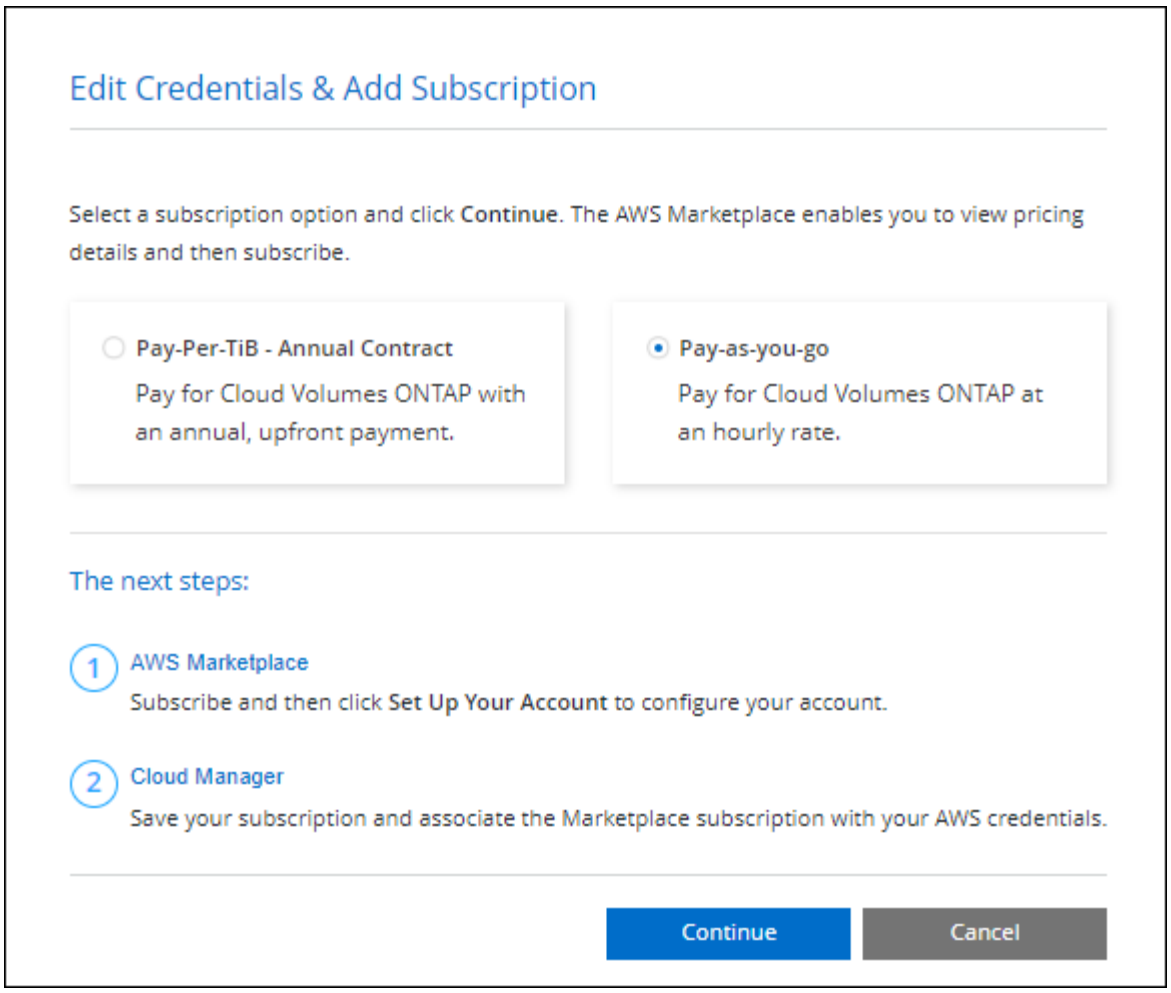
プロビジョニングされた容量が最大500GiBのCloud Volumes ONTAP を無料で使用するには、Freemium製品を選択してください。 "Freemium 製品の詳細をご覧ください"。

手順

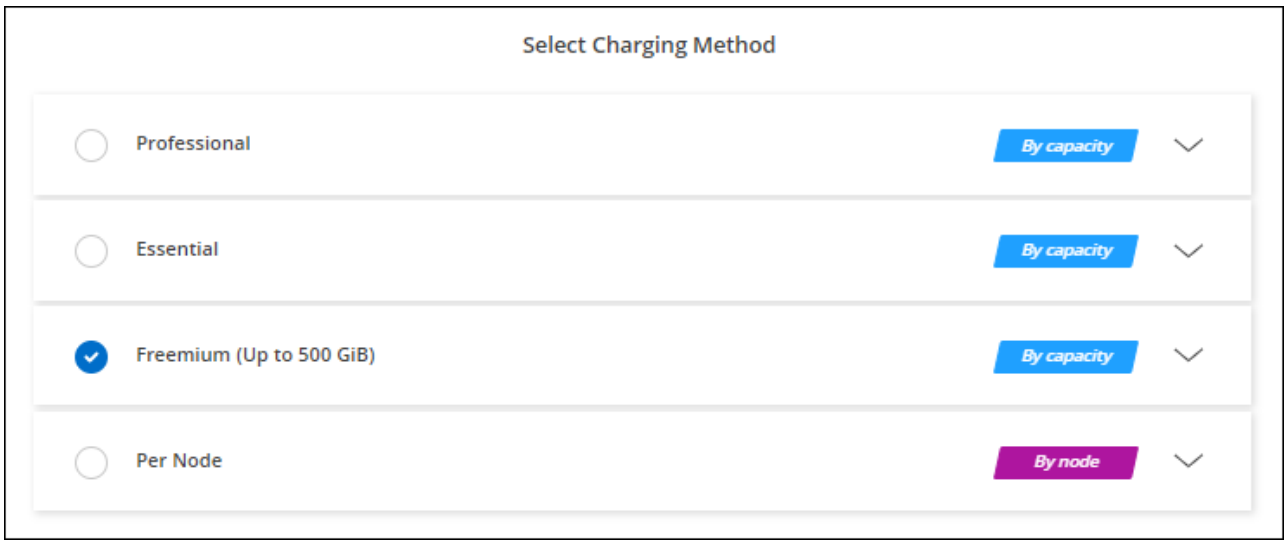
1. キャンバスページで、*作業環境の追加*をクリックし、Cloud Managerの手順に従います。

    a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]>[サブスクリプションの追加]をクリックし、プロンプトに従ってAWS Marketplaceで従量課金制サービスに登録します。

    プロビジョニング済み容量が500GiBを超えると、システムはに自動的に変換されないかぎり、マーケットプレイスのサブスクリプションを通じて料金が請求されることはありません "Essentials パッケージ"。



a. Cloud Managerに戻ったら、課金方法のページが表示されたら「* Freemium *」を選択します。



"ステップバイステップの手順を確認して、AWSでCloud Volumes ONTAP を起動してください"。

容量単位のライセンスです

容量単位のライセンスでは、 TiB 単位の Cloud Volumes ONTAP に対して料金を支払うことができます。容量

ベースのライセンスは、パッケージ：Essentialsパッケージまたはプロフェッショナルパッケージの形式で提供されます。

Essentials パッケージと Professional パッケージには、次の消費モデルがあります。

- ネットアップから購入したライセンス（ BYOL ）
- AWS Marketplaceで提供する従量課金制（PAYGO）の1時間単位のサブスクリプション
- AWS Marketplaceからの年間契約

"容量単位のライセンスに関する詳細は、こちらをご覧ください"。

以降のセクションでは、これらの各消費モデルの使用方法について説明します。

BYOL

ネットアップからライセンスを購入（BYOL）して前払いし、任意のクラウドプロバイダにCloud Volumes ONTAP システムを導入できます。

手順

1. "ライセンスの取得については、ネットアップの営業部門にお問い合わせください"
2. "Cloud Managerにネットアップサポートサイトのアカウントを追加します"

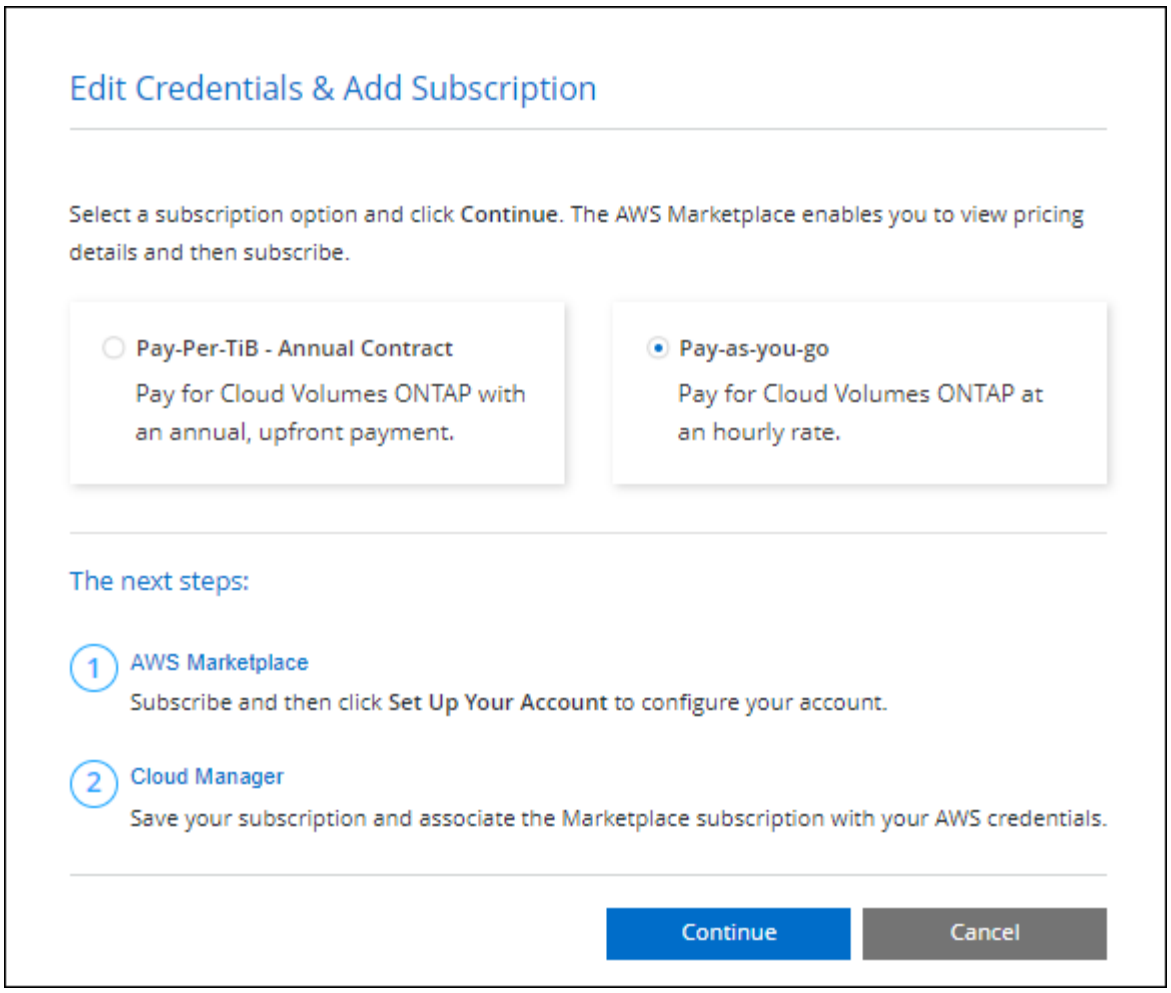
   Cloud Managerは、ネットアップのライセンスサービスを自動的に照会して、ネットアップサポートサイトのアカウントに関連付けられているライセンスに関する詳細を取得します。エラーがなければ、Cloud Managerはライセンスをデジタルウォレットに自動的に追加します。

   Cloud Volumes ONTAP で使用するには、ライセンスがデジタルウォレットから入手できる必要があります。必要に応じて、を実行できます "手動でライセンスをDigital Walletに追加します"。

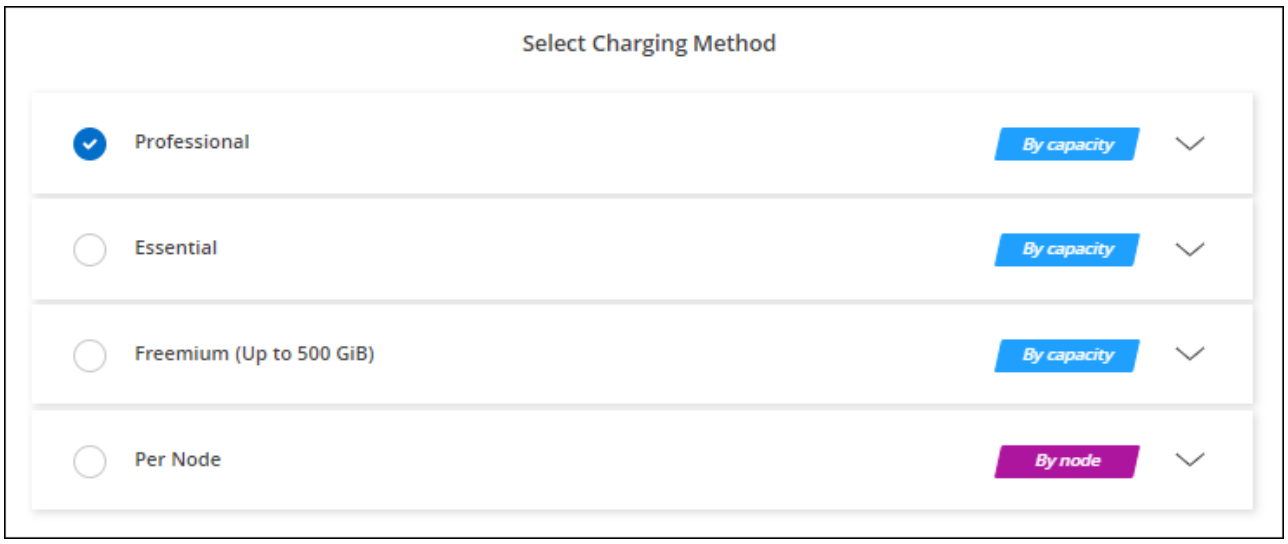
3. キャンバスページで、*作業環境の追加*をクリックし、Cloud Managerの手順に従います。

   a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]>[サブスクリプションの追加]をクリックし、プロンプトに従ってAWS Marketplaceで従量課金制サービスに登録します。

      ネットアップから購入したライセンスには、最初に必ず料金が請求されますが、ライセンスで許可された容量を超えた場合や、ライセンスの期間が終了した場合は、マーケットプレイスで1時間ごとに料金が請求されます。



a. Cloud Managerに戻ったら、課金方法のページで容量ベースのパッケージを選択します。



"ステップバイステップの手順を確認して、AWSでCloud Volumes ONTAP を起動してください"。

PAYGOサブスクリプション

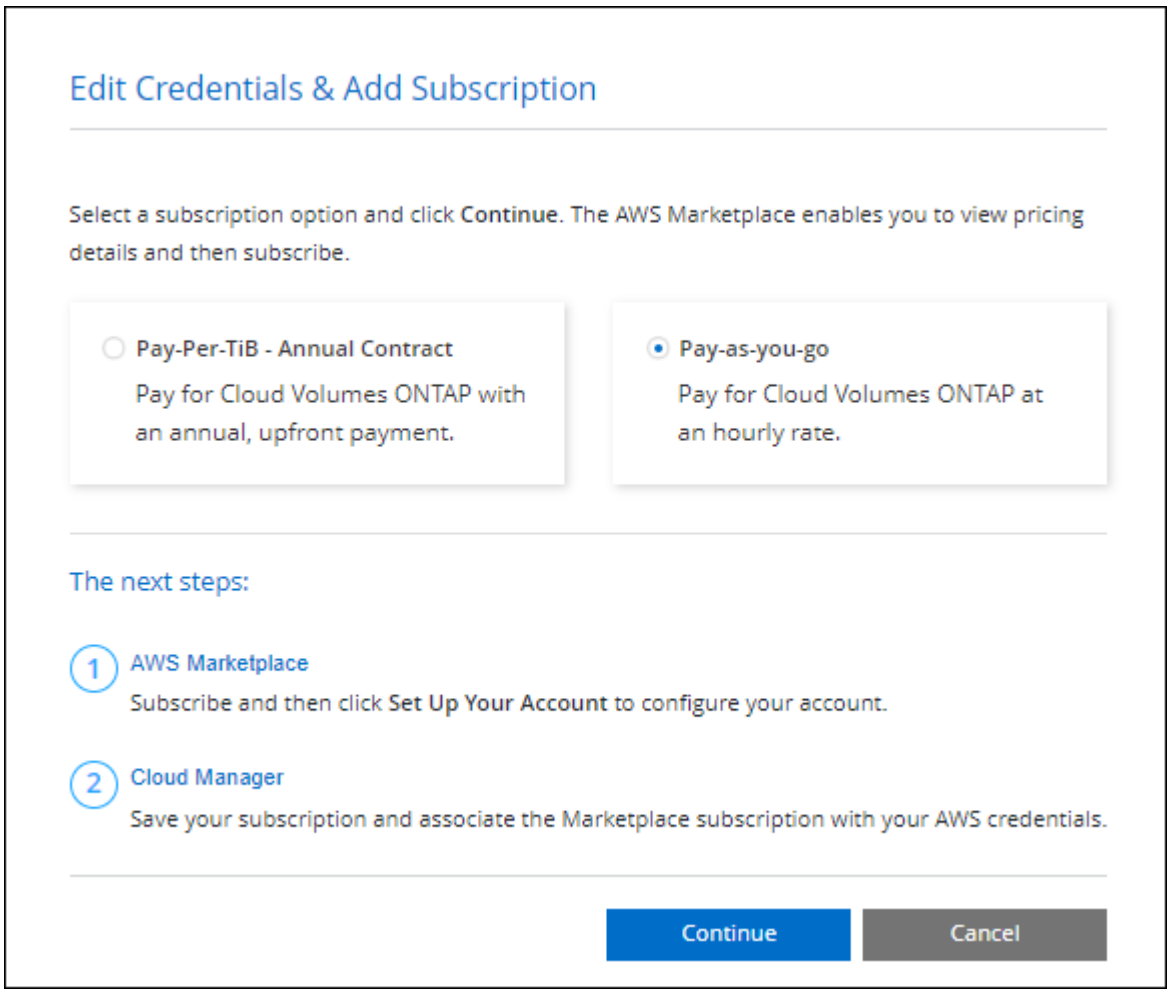
クラウドプロバイダのマーケットプレイスから提供されたサービスに登録すると、1時間ごとに料金が発生し

ます。

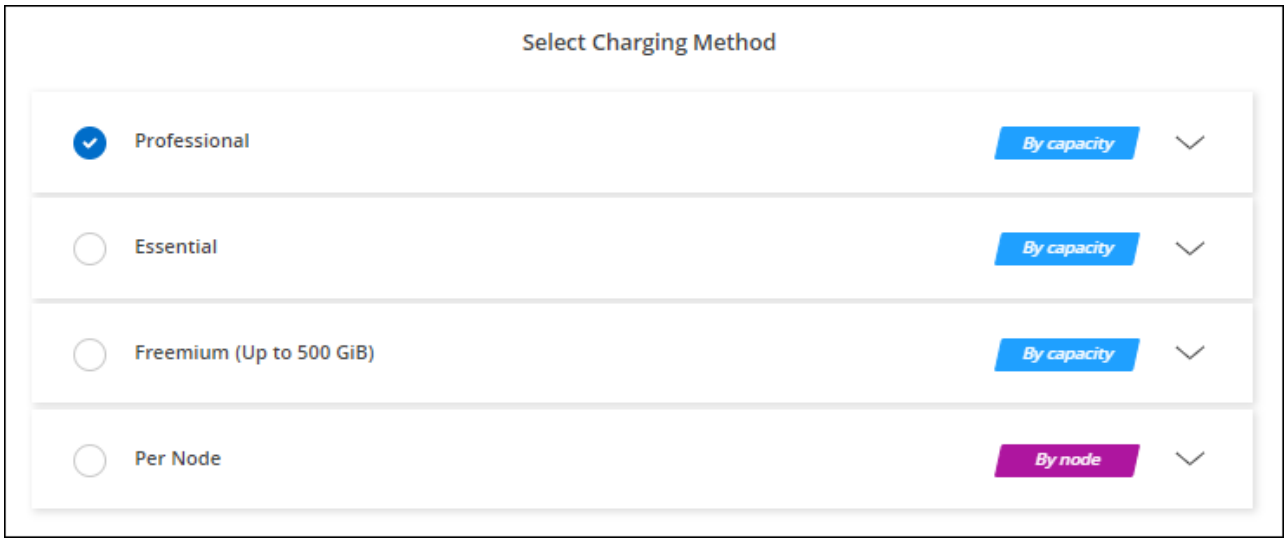
Cloud Volumes ONTAP 作業環境を作成すると、Cloud ManagerからAWS Marketplaceで提供されている契約に登録するよう求められます。このサブスクリプションは、充電のための作業環境に関連付けられます。同じサブスクリプションを追加の作業環境に使用できます。

手順

1. キャンバスページで、*作業環境の追加*をクリックし、Cloud Managerの手順に従います。
   a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]>[サブスクリプションの追加]をクリックし、プロンプトに従ってAWS Marketplaceで従量課金制サービスに登録します。



   b. Cloud Managerに戻ったら、課金方法のページで容量ベースのパッケージを選択します。



"ステップバイステップの手順を確認して、AWSでCloud Volumes ONTAP を起動してください"。

AWSアカウントに関連付けられたAWS Marketplaceのサブスクリプションを管理するには、[設定]>[クレデンシャル]ページを使用します。 "AWSのアカウントとサブスクリプションの管理方法について説明します"

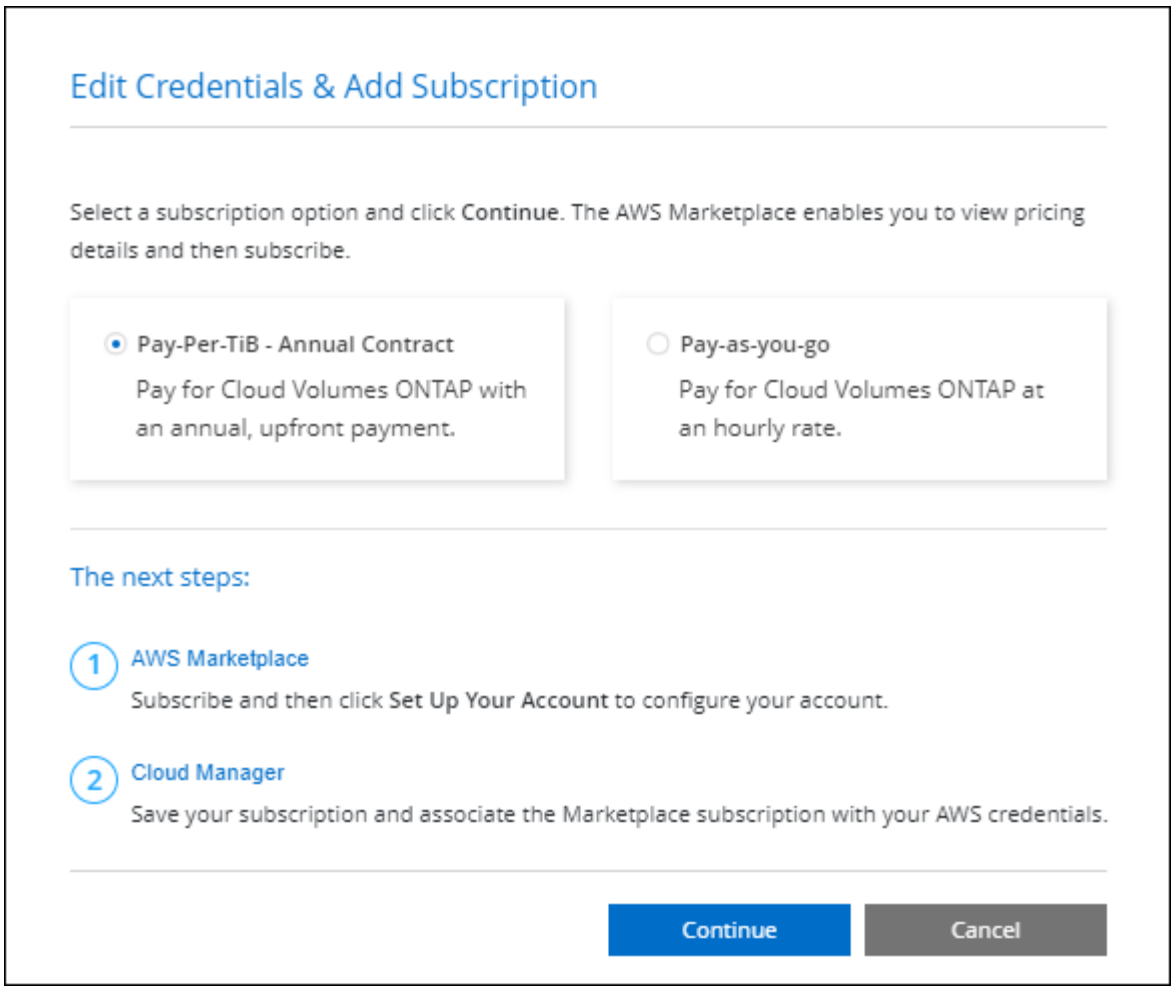
年間契約

クラウドプロバイダのマーケットプレイスから年間契約を購入することで、年間料金を支払うことができます。

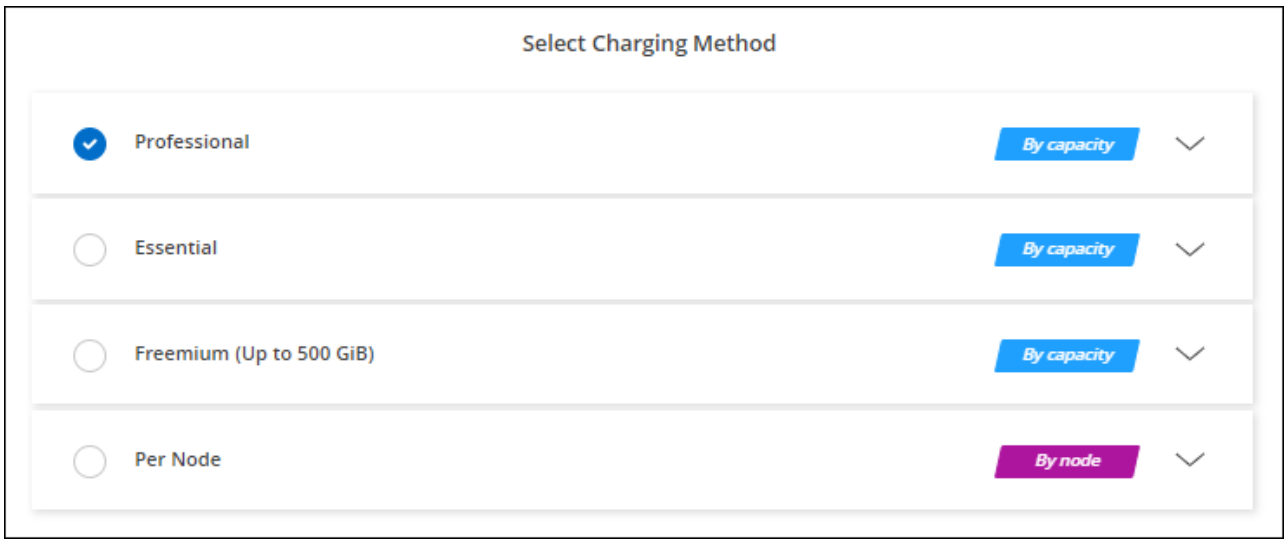
時間単位のサブスクリプションと同様に、Cloud Managerは、AWS Marketplaceで提供される年間契約をサブスクライブするよう求めます。

手順

1. キャンバスページで、*作業環境の追加*をクリックし、Cloud Managerの手順に従います。
    a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]>[サブスクリプションの追加]をクリックし、プロンプトに従ってAWS Marketplaceで年間契約をサブスクライブします。



b. Cloud Managerに戻ったら、課金方法のページで容量ベースのパッケージを選択します。



"ステップバイステップの手順を確認して、AWSでCloud Volumes ONTAP を起動してください"。

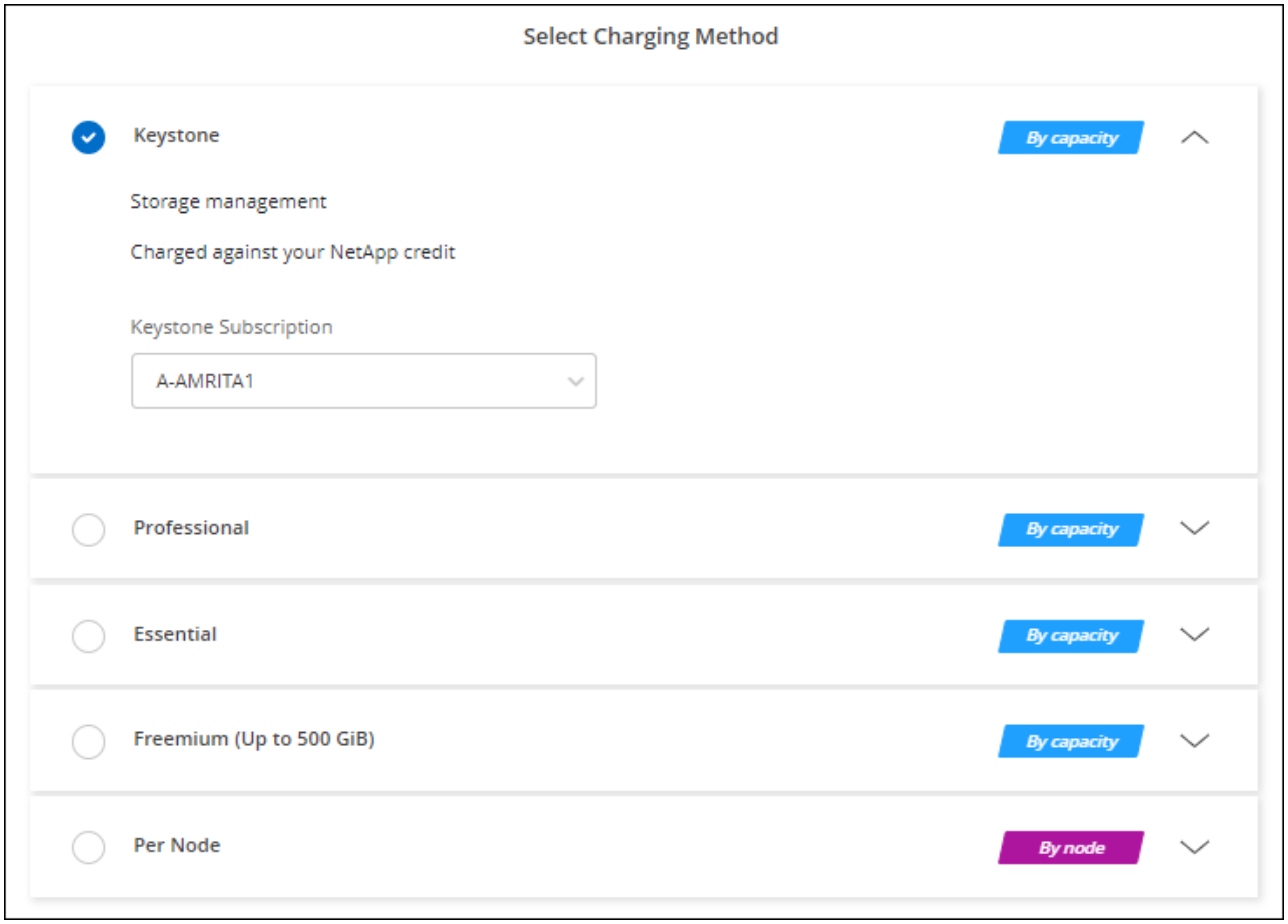
Keystone Flex サブスクリプション

Keystone Flexサブスクリプションは、ビジネスの成長に合わせて拡張できるサブスクリプションベースのサ

ービスです。 "Keystone Flex Subscriptions の詳細をご覧ください"。

手順

1. まだサブスクリプションをお持ちでない場合は、 "ネットアップにお問い合わせください"
2. mailto ： ng-keystone-success@netapp.com [ネットアップにお問い合わせください] 1 つ以上の Keystone Flex Subscriptions で Cloud Manager のユーザアカウントを承認します。
3. ネットアップがお客様のアカウントを許可したあと、 "Cloud Volumes ONTAP で使用するサブスクリプションをリンクします"。
4. キャンバスページで、*作業環境の追加*をクリックし、Cloud Managerの手順に従います。
   a. 充電方法を選択するように求められたら、Keystone Flexサブスクリプションの課金方法を選択します。



"ステップバイステップの手順を確認して、AWSでCloud Volumes ONTAP を起動してください"。

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。

始める前に

作業環境を作成するには、次の作業が必要です。

- 稼働中のコネクタ。
  - 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"。
- 使用する構成についての理解。

  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"。

- Cloud Volumes ONTAP のライセンスを設定するために必要な事項を理解する。

  "ライセンスの設定方法について説明します"。

- CIFS 構成用の DNS と Active Directory

  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"。

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. [[subscribe] キャンバスページで、 * 作業環境の追加 * をクリックし、プロンプトに従います。
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. プロンプトが表示されたら、 "コネクタを作成します"。
4. * 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。

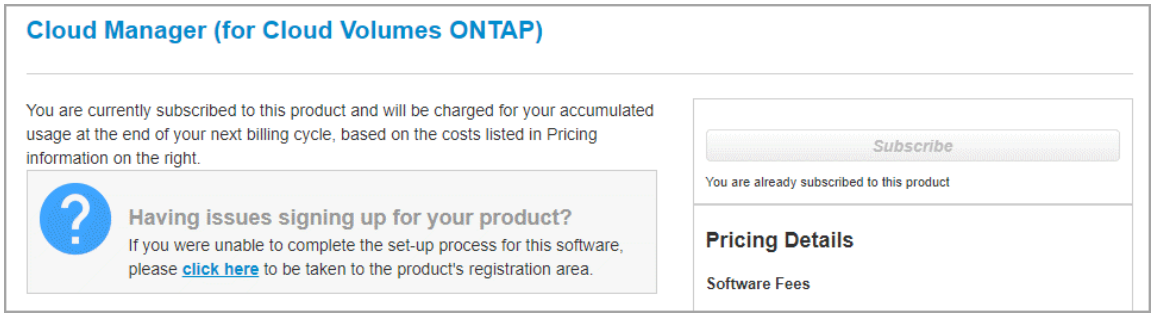
フィールド	説明
タグを追加します	AWS タグは、 AWS リソースのメタデータです。Cloud Manager は、 Cloud Volumes ONTAP インスタンスおよびインスタンスに関連付けられた各 AWS リソースにタグを追加します。作業環境を作成するときに、ユーザインターフェイスから最大 4 つのタグを追加し、作成後にさらに追加できます。API では、作業環境の作成時にタグを 4 つに制限することはありません。タグの詳細については、を参照してください "AWS ドキュメント：「 Tagging your Amazon EC2 Resources"。
ユーザ名とパスワード	Cloud Volumes ONTAP クラスタ管理者アカウントのクレデンシャルです。このクレデンシャルを使用して、 System Manager またはその CLI から Cloud Volumes ONTAP に接続できます。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します
資格情報を編集します	このシステムを導入するアカウントに関連付けられている AWS クレデンシャルを選択します。この Cloud Volumes ONTAP システムで使用する AWS Marketplace サブスクリプションを関連付けることもできます。Add Subscription * をクリックして、選択したクレデンシャルを新しい AWS Marketplace サブスクリプションに関連付けます。サブスクリプションは、年間契約の場合と、 Cloud Volumes ONTAP の料金を 1 時間ごとに支払う場合があります。https://docs.netapp.com/us-en/cloud-manager-setup-admin/task-adding-aws-accounts.html["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/cloud-manager-cloud-volumes-ontap//media/video_subscribing_aws.mp4

(video)

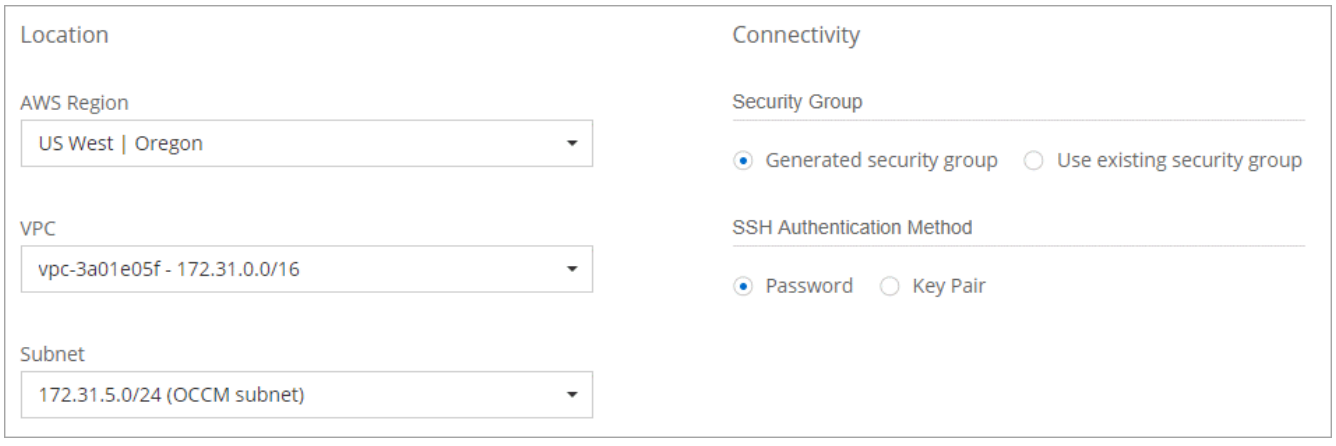
複数の IAM ユーザが同じ AWS アカウントで作業する場合は、各ユーザにサブスクライブする必要があります。最初のユーザがサブスクライブすると、次の図に示すように、 AWS Marketplace から後続のユーザに登録済みであることが通知されます。AWS_account_ のサブスクリプションが設定されている間、各 IAM ユーザは、そのサブスクリプションに自分自身を関連付ける必要があります。以下のメッセージが表示された場合は、 * ここをクリック * リンクをクリックして Cloud Central にアクセスし、処理を完了してください。



5. * 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。
   - "クラウドデータセンスの詳細をご確認ください"。
   - "Cloud Backup 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"。
6. * 場所と接続 * ：に記録したネットワーク情報を入力します "AWS ワークシート"。

   AWS Outpost を使用している場合は、 Outpost VPC を選択して、その Outpost に単一のノードの Cloud Volumes ONTAP システムを導入できます。エクスペリエンスは、 AWS に存在する他の VPC と同じです。

   次の図は、入力済みのページを示しています。



7. * 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"。

8. * 充電方法と NSS アカウント * ：このシステムで使用する充電オプションを指定し、ネットアップサポートサイトのアカウントを指定します。
   - "Cloud Volumes ONTAP のライセンスオプションについて説明します"。
   - "ライセンスの設定方法について説明します"。
9. * Cloud Volumes ONTAP 構成 * （ AWS Marketplace の年間契約のみ）：デフォルトの構成を確認して「 * Continue * 」をクリックするか、「 * 構成の変更 * 」をクリックして独自の構成を選択します。

   デフォルトの設定を使用している場合、ボリュームを指定し、構成を確認および承認するだけで済みます。
10. 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、*構成の変更*をクリックして独自の構成を選択します。

    いずれかのパッケージを選択した場合、ボリュームを指定し、構成を確認および承認するだけで済みます。
11. * IAM ロール * ： Cloud Manager にロールを割り当てるには、デフォルトのオプションを使用することを推奨します。

    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 ノードのポリシーの要件"。
12. ライセンス：必要に応じてCloud Volumes ONTAP のバージョンを変更し、インスタンスタイプとインスタンステナンシーを選択します。

    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 9.10.1と9.10.1 P4が利用可能になっていれば、更新が実行されます。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。
13. * 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"。

14. * 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。

"書き込み速度の詳細については、こちらをご覧ください。"。

Cloud Backup が有効になっている場合やデータ階層化が有効になっている場合は、 WORM を有効にすることはできません。

"WORM ストレージの詳細については、こちらをご覧ください。"。

15. * 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。

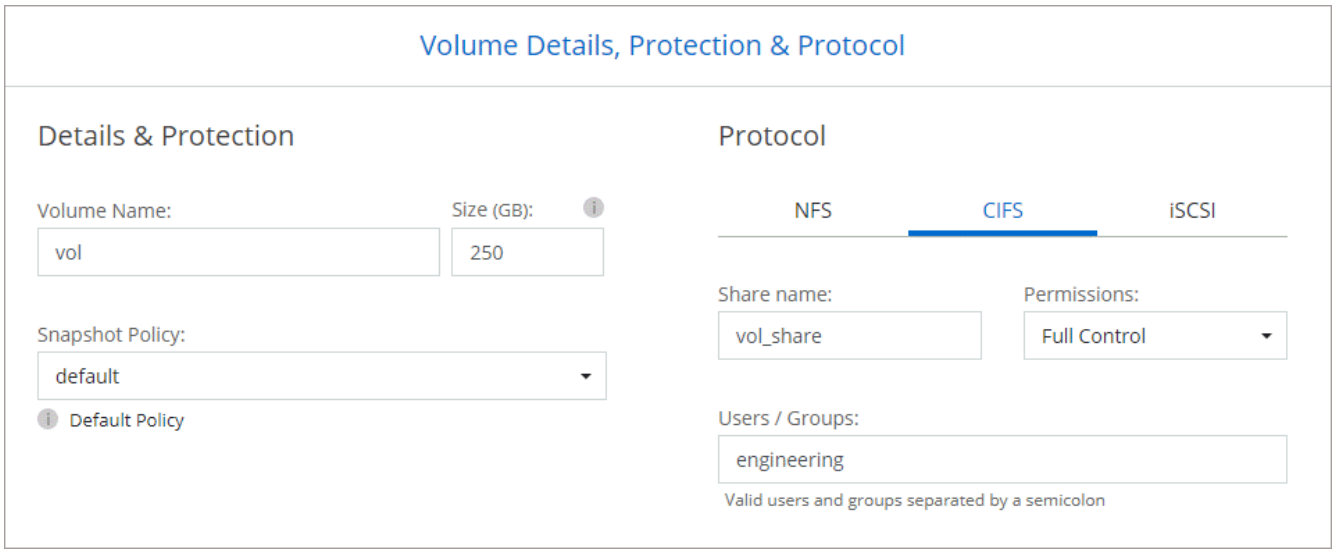
"サポートされるクライアントプロトコルおよびバージョンについて説明します"。

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。

フィールド	説明
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。



16. * 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。

フィールド	説明
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 自動化に関するドキュメント" を参照してください。NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

17. * 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"。

18. * 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。

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。

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。

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. Canvas ページで、 * Add Working Environment * 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。

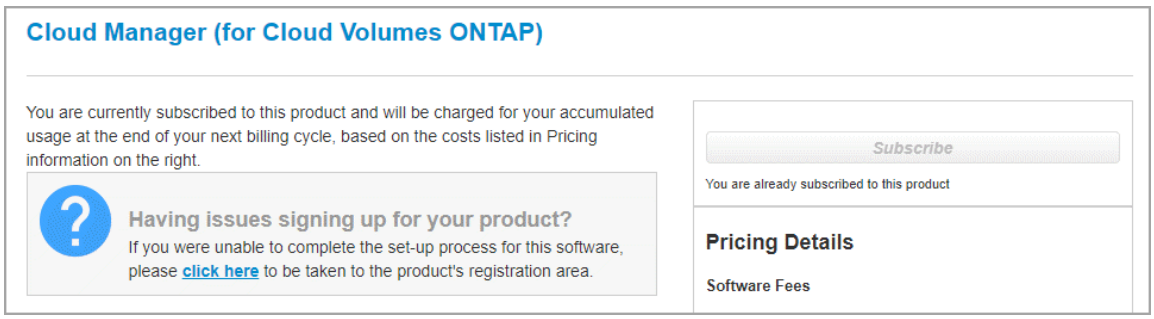
フィールド	説明
作業環境名	Cloud Manager は、作業環境名を使用して、 Cloud Volumes ONTAP システムと Amazon EC2 インスタンスの両方に名前を付けます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。
タグを追加します	AWS タグは、 AWS リソースのメタデータです。Cloud Manager は、 Cloud Volumes ONTAP インスタンスおよびインスタンスに関連付けられた各 AWS リソースにタグを追加します。作業環境を作成するときに、ユーザインターフェイスから最大 4 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	Cloud Volumes ONTAP クラスタ管理者アカウントのクレデンシャルです。このクレデンシャルを使用して、 System Manager またはその CLI から Cloud Volumes ONTAP に接続できます。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します
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。Add Subscription * をクリックして、選択したクレデンシャルを新しい AWS Marketplace サブスクリプションに関連付けます。サブスクリプションは、年間契約の場合と、 Cloud Volumes ONTAP の料金を 1 時間ごとに支払う場合があります。NetApp （ BYOL ）からライセンスを直接購入した場合、 AWS サブスクリプションは必要ありません。https://docs.netapp.com/us-en/cloud-manager-setup-admin/task-adding-aws-accounts.html["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/cloud-manager-cloud-volumes-ontap//media/video_subscribing_aws.mp4

(video)

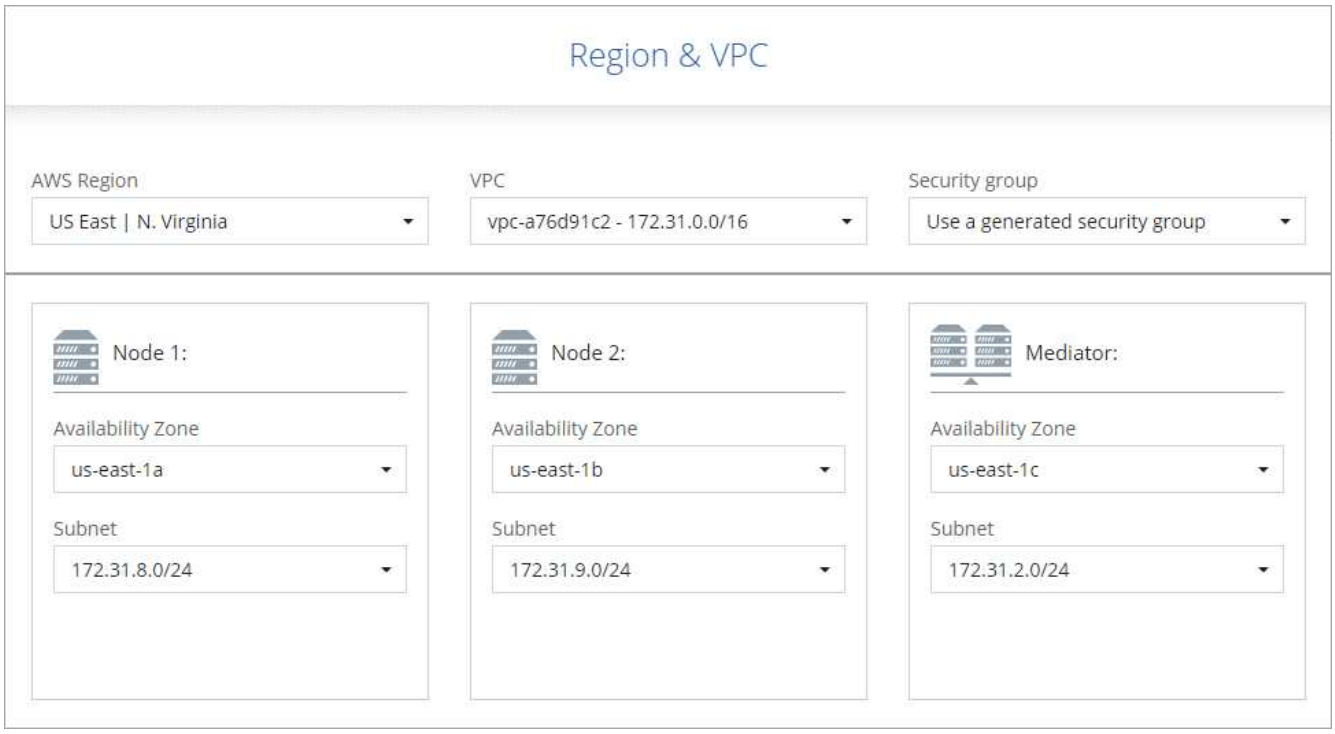
複数の IAM ユーザが同じ AWS アカウントで作業する場合は、各ユーザにサブスクライブする必要があります。最初のユーザがサブスクライブすると、次の図に示すように、 AWS Marketplace から後続のユーザに登録済みであることが通知されます。AWS_account_ のサブスクリプションが設定されている間、各 IAM ユーザは、そのサブスクリプションに自分自身を関連付ける必要があります。以下のメッセージが表示された場合は、 * ここをクリック * リンクをクリックして Cloud Central にアクセスし、処理を完了してください。



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。
   - "クラウドデータセンスの詳細をご確認ください"。
   - "Cloud Backup 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. * 充電方法と NSS アカウント * ：このシステムで使用する充電オプションを指定し、ネットアップサポートサイトのアカウントを指定します。
    - "Cloud Volumes ONTAP のライセンスオプションについて説明します"。
    - "ライセンスの設定方法について説明します"。

12. * Cloud Volumes ONTAP 構成 * （ AWS Marketplace の年間契約のみ）：デフォルトの構成を確認して「 * Continue * 」をクリックするか、「 * 構成の変更 * 」をクリックして独自の構成を選択します。

    デフォルトの設定を使用している場合、ボリュームを指定し、構成を確認および承認するだけで済みます。

13. * 構成済みパッケージ * （時間単位または BYOL のみ）： 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、 * 構成の変更 * をクリックして独自の構成を選択します。

    いずれかのパッケージを選択した場合、ボリュームを指定し、構成を確認および承認するだけで済みます。

14. * IAM ロール * ： Cloud Manager にロールを割り当てるには、デフォルトのオプションを使用することを推奨します。

    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"。

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

    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 9.10.1と9.10.1 P4が利用可能になっていれば、更新が実行されます。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。

16. * 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"。

17. * 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。

    "書き込み速度の詳細については、こちらをご覧ください。"。

    Cloud Backup が有効になっている場合やデータ階層化が有効になっている場合は、 WORM を有効にする

ことはできません。

"WORM ストレージの詳細については、こちらをご覧ください。"。

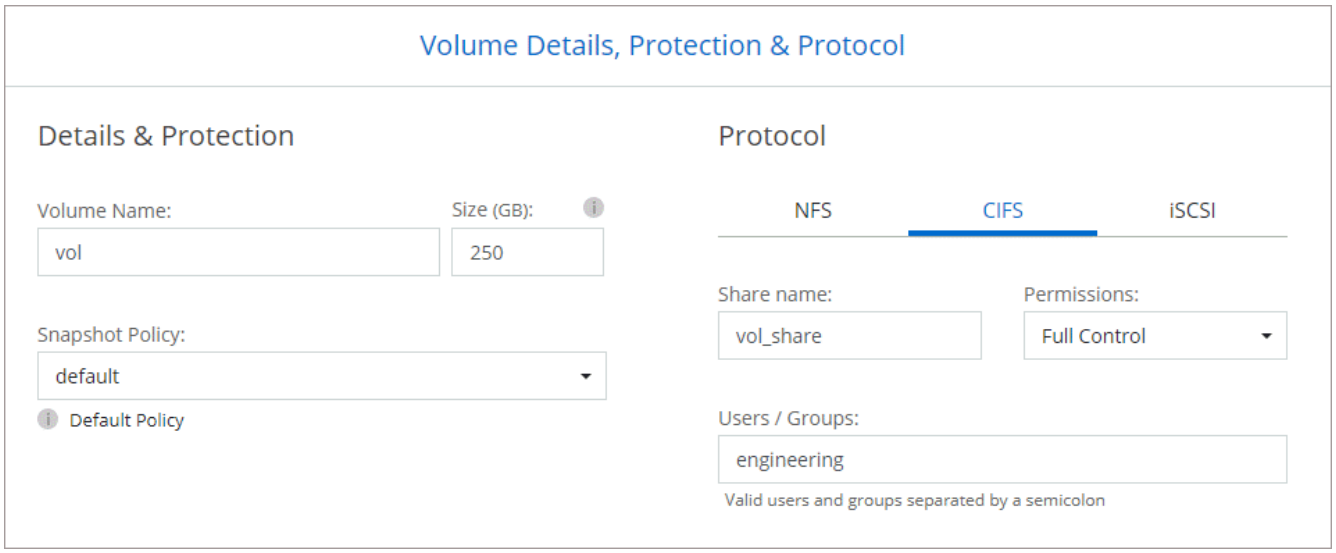
18. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

"サポートされるクライアントプロトコルおよびバージョンについて説明します"。

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。



19. * 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 自動化に関するドキュメント" を参照してください。NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

20. * 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"。

21. * 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。

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。

AWS C2S で Cloud Volumes ONTAP を使用する方法を確認します 環境

標準の AWS リージョンと同様に、で Cloud Manager を使用できます "AWS Commercial クラウドサービス（ C2S ）" Cloud Volumes ONTAP を導入する環境。クラウドストレージにエンタープライズクラスの機能を提供します。AWS C2S は米国に固有の閉じたリージョンですIntelligence Community 。このページの手順は、 AWS C2S リージョンユーザにのみ該当します。

C2S でサポートされている機能

C2S 環境の Cloud Manager から使用可能な機能は次のとおりです。

- Cloud Volumes ONTAP
- データレプリケーション
- 監査のスケジュール

Cloud Volumes ONTAP の場合は、シングルノードシステムまたは HA ペアを作成できます。どちらのライセンスオプションも使用できます。従量課金制とお客様所有のライセンス（ BYOL ）です。

S3 へのデータ階層化は、 C2S の Cloud Volumes ONTAP でもサポートされています。

制限

- ネットアップのどのクラウドサービスも Cloud Manager からは使用できません。

- C2S 環境ではインターネットにアクセスできないため、次の機能も使用できません。
  - NetApp Cloud Central との統合
  - Cloud Manager からのソフトウェアの自動アップグレード
  - NetApp AutoSupport
  - AWS の Cloud Volumes ONTAP リソースのコスト情報
- Freemiumライセンスは、C2S環境ではサポートされていません。

導入の概要

C2S で Cloud Volumes ONTAP を使用するにはいくつかの手順を実行します。

1. AWS 環境の準備

   これには、ネットワークの設定、 Cloud Volumes ONTAP への登録、権限の設定、および必要に応じて AWS KMS のセットアップが含まれます。

2. Connector のインストールと Cloud Manager のセットアップ

   Cloud Manager を使用して Cloud Volumes ONTAP を導入するには、コネクタを作成する必要があります。Connector を使用すると、 Cloud Manager でパブリッククラウド環境内のリソースとプロセス（ Cloud Volumes ONTAP を含む）を管理できます。

   Connector インスタンスにインストールされているソフトウェアから Cloud Manager にログインします。

3. Cloud Manager から Cloud Volumes ONTAP を起動しています。

以下に、各手順について説明します。

AWS 環境を準備

AWS 環境はいくつかの要件を満たす必要があります。

ネットワークをセットアップします

Cloud Volumes ONTAP 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。

手順

1. コネクタインスタンスと Cloud Volumes ONTAP インスタンスを起動する VPC とサブネットを選択します。
2. 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。
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。

Cloud Volumes ONTAP に登録します

Cloud Manager から Cloud Volumes ONTAP を導入するには、 Marketplace サブスクリプションが必要です。

手順

1. AWS Intelligence Community Marketplace にアクセスして、 Cloud Volumes ONTAP を検索します。
2. 導入を計画しているサービスを選択します。
3. 条件を確認し、 [**Accept**](同意する) をクリックします。
4. 導入を計画している場合は、他のサービスについても同じ手順を繰り返します。

   Cloud Volumes ONTAP インスタンスを起動するには、 Cloud Manager を使用する必要があります。Cloud Volumes ONTAP インスタンスを EC2 コンソールから起動しないでください。

権限を設定します

AWS Commercial クラウドサービス環境でアクションを実行するために必要な権限を Cloud Manager と Cloud Volumes ONTAP に提供する IAM ポリシーとロールを設定する。

次の項目について、 IAM ポリシーと IAM ロールを 1 つずつ用意する必要があります。

- コネクタインスタンス
- Cloud Volumes ONTAP インスタンス
- Cloud Volumes ONTAP HA メディエーターインスタンス （ HA ペアを導入する場合）

手順

1. AWS IAM コンソールに移動し、 * Policies * をクリックします。
2. コネクタインスタンスのポリシーを作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
```

```
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
```

```
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
```

```
            ]
        }
    ]
}
```

3. Cloud Volumes ONTAP のポリシーを作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

4. Cloud Volumes ONTAP HA ペアを導入する場合は、 HA メディエーターのポリシーを作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

5. タイプが Amazon EC2 の IAM ロールを作成し、前の手順で作成したポリシーを関連付けます。

   ポリシーと同様に、コネクタ用の IAM ロールが 1 つ、 Cloud Volumes ONTAP ノード用の IAM ロールが 1 つ、 HA メディエーター用の IAM ロールが 1 つ（ HA ペアを導入する場合）必要です。

   コネクタインスタンスを起動するときに、コネクタ IAM ロールを選択する必要があります。

   Cloud Volumes ONTAP の IAM ロールと HA メディエーターは、 Cloud Manager から Cloud Volumes ONTAP の作業環境を作成するときに選択できます。

AWS KMS を設定します

Cloud Volumes ONTAP で Amazon 暗号化を使用する場合は、 AWS Key Management Service の要件を満たしていることを確認します。

手順

1. アクティブな Customer Master Key （ CMK ；カスタマーマスターキー）がアカウントまたは別の AWS アカウントに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。

2. Cloud Volumes ONTAP を導入するアカウントとは別の AWS アカウントに CMK を配置する場合は、そのキーの ARN を取得する必要があります。

   Cloud Volumes ONTAP システムの作成時には、 Cloud Manager への ARN の提供が必要になります。

3. Cloud Manager インスタンス用の IAM ロールを CMK のキーユーザのリストに追加します。

   これにより、 Cloud Manager には、 Cloud Volumes ONTAP で CMK を使用する権限が与えられます。

Cloud Manager をインストールしてセットアップする

AWS で Cloud Volumes ONTAP システムを起動するには、まず AWS Marketplace から Connector インスタンスを起動してから、ログインして Cloud Manager をセットアップする必要があります。

手順

1. Privacy Enhanced Mail （ PEM ） Base-64 でエンコードされた X.509 形式の認証局（ CA ）が署名したルート証明書を取得する証明書を入手するには、組織のポリシーと手順を参照してください。

   セットアッププロセス中に証明書をアップロードする必要があります。Cloud Manager は、 HTTPS 経由で AWS に要求を送信する際に信頼された証明書を使用します。

2. コネクタインスタンスを起動します。
   a. AWS Intelligence Community Marketplace の Cloud Manager のページに移動します。
   b. Custom Launch タブで、 EC2 コンソールからインスタンスを起動するオプションを選択します。
   c. プロンプトに従って、インスタンスを設定します。

      インスタンスを設定する際には、次の点に注意してください。

      - t3.xlarge をお勧めします。
      - AWS 環境の準備の際に作成した IAM ロールを選択する必要があります。
      - デフォルトのストレージオプションはそのままにしておく必要があります。
      - コネクタに必要な接続方法は、 SSH 、 HTTP 、 HTTPS です。
3. コネクタインスタンスに接続されているホストから Cloud Manager をセットアップします。
   a. Web ブラウザを開き、次の URL を入力します。 http://ipaddress:80
   b. AWS サービスに接続するためのプロキシサーバを指定します。
   c. 手順 1 で取得した証明書をアップロードします。
   d. セットアップウィザードの手順に従って、 Cloud Manager をセットアップします。
      - * System Details * ： Cloud Manager インスタンスの名前を入力し、会社名を入力します。
      - * ユーザの作成 * ： Cloud Manager の管理に使用する管理者ユーザを作成します。
      - * レビュー * ：詳細を確認し、エンドユーザーライセンス契約を承認します。
   e. CA 署名証明書のインストールを完了するには、 EC2 コンソールからコネクタインスタンスを再起動します。
4. コネクタが再起動したら、セットアップウィザードで作成した管理者ユーザアカウントを使用してログインします。

Cloud Volumes ONTAP を起動します

Cloud Manager で新しい作業環境を作成することで、 AWS Commercial クラウドサービス環境で Cloud Volumes ONTAP インスタンスを起動できます。

必要なもの

- ライセンスを購入した場合は、ネットアップから受け取ったライセンスファイルが必要です。ライセンス

ファイルは JSON 形式の .NLF ファイルです。

- HA メディエーターへのキーベースの SSH 認証を有効にするには、キーペアが必要です。

手順

1. 作業環境ページで、 * 作業環境の追加 * をクリックします。
2. 作成（ Create ）で、 Cloud Volumes ONTAP または Cloud Volumes ONTAP HA を選択します。
3. ウィザードの手順に従って、 Cloud Volumes ONTAP システムを起動します。

   ウィザードを完了する際には、次の点に注意してください。

   - 複数のアベイラビリティゾーンに Cloud Volumes ONTAP HA を導入する場合は、公開時点で AWS Commercial クラウドサービス環境で使用可能な AZ は 2 つだけだったため、次のように構成を導入します。
     - ノード 1 ：アベイラビリティゾーン A
     - ノード 2 ：アベイラビリティゾーン B
     - メディエーター：アベイラビリティゾーン A または B
   - 生成されたセキュリティグループを使用するには、デフォルトのオプションをそのままにしておく必要があります。

     事前定義されたセキュリティグループには、 Cloud Volumes ONTAP が正常に動作するために必要なルールが含まれています。独自の要件がある場合は、下のセキュリティグループのセクションを参照してください。

   - AWS 環境の準備の際に作成した IAM ロールを選択する必要があります。
   - 基盤となる AWS ディスクタイプは Cloud Volumes ONTAP の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。

   - AWS 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。

     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。EBS のパフォーマンスの詳細については、 AWS のドキュメントを参照してください。

   - ディスクサイズは、システム上のすべてのディスクのデフォルトサイズです。

     あとでサイズを変更する必要がある場合は、 Advanced allocation オプションを使用して、特定のサイズのディスクを使用するアグリゲートを作成できます。

   - Storage Efficiency 機能を使用すると、ストレージ利用率を高めて、必要なストレージの総容量を減らすことができます。

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。

セキュリティグループのルール

Cloud Manager で作成されるセキュリティグループには、 Cloud Manager と Cloud Volumes ONTAP がクラウドで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。テスト目的ま

たは独自のセキュリティグループを使用する場合は、ポートを参照してください。

コネクタのセキュリティグループ

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への HTTP アクセスを提供します ユーザインターフェイス
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

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

Cloud Volumes ONTAP のセキュリティグループ

Cloud Volumes ONTAP ノード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
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

プロトコル	ポート	目的
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 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

HA メディエーターの外部セキュリティグループ

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ソースは、コネクタが存在する VPC からのトラフィックです。

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 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

HA メディエーターの内部セキュリティグループ

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