始めましょう
Cloud Volumes ONTAP

NetApp
February 26, 2026

目次

始めましょう

Cloud Volumes ONTAPについて学ぶ

Cloud Volumes ONTAP を使用すると、データ保護、セキュリティ、コンプライアンスを強化しながら、クラウド ストレージのコストとパフォーマンスを最適化できます。

Cloud Volumes ONTAPは、クラウドでONTAPデータ管理ソフトウェアを実行するソフトウェアのみのストレージ アプライアンスです。次の主要機能を備えたエンタープライズ グレードのストレージを提供します。

- ストレージ効率

  組み込みのデータ重複排除、データ圧縮、シン プロビジョニング、クローン作成を活用して、ストレージ コストを最小限に抑えます。

- 高可用性

  クラウド環境で障害が発生した場合でも、企業の信頼性と継続的な運用を確保します。

- データ保護

  Cloud Volumes ONTAP は、業界をリードする NetApp のレプリケーション テクノロジーであるSnapMirrorを活用してオンプレミスのデータをクラウドに複製するため、複数のユース ケースで使用できるセカンダリ コピーを簡単に作成できます。

  Cloud Volumes ONTAP はNetApp Backup and Recoveryとも統合されており、クラウド データの保護と長期アーカイブのためのバックアップおよび復元機能も提供します。

  "バックアップとリカバリの詳細"

- データ階層化

  アプリケーションをオフラインにすることなく、高パフォーマンスと低パフォーマンスのストレージ プールをオンデマンドで切り替えます。

- アプリケーションの一貫性

  NetApp SnapCenterを使用して、 NetApp Snapshot コピーの一貫性を確保します。

  "SnapCenterについて詳しくはこちら"

- Data security

  Cloud Volumes ONTAP はデータ暗号化をサポートし、ウイルスやランサムウェアからの保護を提供します。

- プライバシーコンプライアンス管理

  NetApp Data Classificationとの統合により、データのコンテキストを理解し、機密データを識別できるようになります。

"データ分類の詳細"

ONTAP機能のライセンスは、Cloud Volumes ONTAPに含まれています。

"サポートされているCloud Volumes ONTAP構成を表示する"

"Cloud Volumes ONTAPの詳細"

Cloud Volumes ONTAPデプロイメントでサポートされているONTAPバージョン

NetApp Consoleを使用すると、Cloud Volumes ONTAPシステムを追加するときに、複数の異なるONTAPバージョンから選択できます。

ここに記載されている以外の Cloud Volumes ONTAP バージョンは、新規導入には使用できません。ここでのリリースのパッチまたは汎用（一般提供）バージョンは、導入に使用可能な基本バージョンを表します。利用可能なパッチの詳細については、各リリースの "バージョン付きリリースノート"を参照してください。

アップグレードの詳細については、"サポートされているアップグレード パス"を参照してください。

AWS

シングル ノード

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

HAペア

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

Azure

シングル ノード

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

HAペア

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

Google Cloud

シングル ノード

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

HAペア

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

Amazon Web Servicesを始める

AWS でのCloud Volumes ONTAPのクイックスタート

数ステップで AWS のCloud Volumes ONTAPを使い始めましょう。

1 コンソールエージェントを作成する

もしあなたが "コンソールエージェント"まだ作成する必要があります。 "AWS でコンソールエージェントを作成する方法を学ぶ" 。

インターネット アクセスが利用できないサブネットにCloud Volumes ONTAPを展開する場合は、コンソール エージェントを手動でインストールし、そのコンソール エージェントで実行されているNetApp Consoleユーザー インターフェイスにアクセスする必要があることに注意してください。 "インターネットにアクセスできない場所にコンソールエージェントを手動でインストールする方法を学びます" 。

2 構成を計画する

コンソールでは、ワークロード要件に一致する事前構成済みのパッケージが提供されており、独自の構成を作成することもできます。独自の構成を選択する場合は、利用可能なオプションを理解する必要があります。 "詳細情報" 。

3 ネットワークを設定する

1. VPC とサブネットがコンソール エージェントと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. NetApp AutoSupportのターゲット 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ます。

   インターネットにアクセスできない場所にCloud Volumes ONTAPを展開する場合、この手順は必要ありません。

3. Amazon Simple Storage Service（Amazon S3）サービスへのVPCエンドポイントを設定します。

   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" 。

4 AWS KMSを設定する

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、コンソールエージェントに権限を提供する IAM ロールを キーユーザー として追加して、各 CMK のキーポリシーを変更する必要があります。"詳細情報" 。

5 コンソールを使用してCloud Volumes ONTAPを起動する

*システムの追加*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完了します。"

ステップバイステップの説明を読む" 。

関連リンク

- "AWS のコンソールエージェントを作成する"
- "AWS Marketplaceからコンソールエージェントを作成する"
- "オンプレミスでコンソールエージェントをインストールしてセットアップする"
- "コンソールエージェントのAWS権限"

AWS でCloud Volumes ONTAP構成を計画する

AWS にCloud Volumes ONTAP を導入する場合、ワークロード要件に一致する事前構成済みのシステムを選択することも、独自の構成を作成することもできます。独自の構成を選択する場合は、利用可能なオプションを理解する必要があります。

Cloud Volumes ONTAPライセンスを選択する

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。各オプションにより、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学ぶ"
- "ライセンスの設定方法を学ぶ"

サポートされている地域を選択してください

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地域の完全なリストを見る" 。

新しい AWS リージョンでリソースを作成および管理するには、その前に新しい AWS リージョンを有効にする必要があります。 "AWSドキュメント: リージョンを有効にする方法を学ぶ" 。

サポートされているローカルゾーンを選択してください

ローカルゾーンの選択はオプションです。 Cloud Volumes ONTAPは、シンガポールを含む一部の AWS ローカルゾーンでサポートされています。 AWS のCloud Volumes ONTAPは、単一のアベイラビリティーゾーンで高可用性 (HA) モードのみをサポートします。単一ノードの展開はサポートされていません。

> Cloud Volumes ONTAP は、 AWS ローカルゾーンでのデータ階層化とクラウド階層化をサポートしていません。さらに、 Cloud Volumes ONTAPに適合していないインスタンスを含むローカルゾーンはサポートされません。一例としてマイアミが挙げられますが、これはサポートされておらず、資格のない Gen6 インスタンスしかないため、ローカル ゾーンとして使用できません。

"AWSドキュメント: ローカルゾーンの完全なリストを見る" 。ローカル ゾーンでリソースを作成および管理するには、ローカル ゾーンを有効にする必要があります。

"AWS ドキュメント: AWS Local Zones の使用開始" 。

サポートされているインスタンスを選択してください

Cloud Volumes ONTAP は、選択したライセンス タイプに応じて、いくつかのインスタンス タイプをサポートします。

"AWS でサポートされているCloud Volumes ONTAPの構成"

ストレージ制限を理解する

Cloud Volumes ONTAPシステムの生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。構成を計画する際には、これらの制限に注意する必要があります。

"AWS のCloud Volumes ONTAPのストレージ制限"

AWS でシステムのサイズを決定する

Cloud Volumes ONTAPシステムのサイズを設定すると、パフォーマンスと容量の要件を満たすことができます。インスタンスタイプ、ディスクタイプ、ディスクサイズを選択する際には、いくつかの重要なポイント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 に合わせて調整します。
- 複数のユーザーが同時にシステムに書き込む場合は、リクエスト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。
- 主に読み取りを行うアプリケーションがある場合は、十分な RAM を搭載したシステムを選択してください。
  - "AWS ドキュメント: Amazon EC2 インスタンスタイプ"
  - "AWS ドキュメント: Amazon EBS 最適化インスタンス"

EBSのディスク タイプ

大まかに言えば、EBS ディスク タイプ間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、以下を参照してください。 "AWS ドキュメント: EBS ボリュームタイプ" 。

- 汎用 *SSD (gp3)* ディスクは、幅広いワークロードのコストとパフォーマンスのバランスが取れた最も低コストの SSD です。パフォーマンスは IOPS とスループットの観点から定義されます。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、 NetApp Consoleは、選択したディスク サイズに基づいて、gp2 ディスクと同等のパフォーマンスを提供するデフォルトの IOPS とスループットの値を入力します。値を大きくするとコストは高くなりますが、パフォーマンスが向上する可能性があります。ただし、値を小さくするとパフォーマンスが低下する可能性があるため、値はサポートされていません。つまり、デフォルト値をそのまま使用するか、値を増やします。下げないでください。 "AWSドキュメント: gp3ディスクとそのパフォーマンスについて詳しく知る" 。

  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ることに注意してください。"Elastic Volumesのサポートについて詳しくはこちら" 。

- 汎用 *SSD (gp2)* ディスクは、幅広いワークロードのコストとパフォーマンスのバランスを実現します。パフォーマンスは IOPS で定義されます。

- *Provisioned IOPS SSD (io1)* ディスクは、より高いコストで最高のパフォーマンスを必要とする重要なアプリケーション向けです。

  Cloud Volumes ONTAP は、 io1 ディスクを使用した Amazon EBS Elastic Volumes 機能をサポートしていることに注意してください。"Elastic Volumesのサポートについて詳しくはこちら" 。

- スループット最適化 *HDD (st1)* ディスクは、低価格で高速かつ一貫したスループットを必要とする、頻繁にアクセスされるワークロード向けです。

> Cloud Volumes ONTAPシステムがAWS Local Zoneにある場合、Amazon Simple Storage Service（Amazon S3）へのデータ階層化はサポートされません。これは、Local Zone外のAmazon S3バケットへのアクセスにはレイテンシが高くなり、Cloud Volumes ONTAPのアクティビティに影響を与えるためです。

EBSディスクサイズ

サポートされていない設定を選択した場合は、"Amazon EBS エラスティックボリューム機能" 、 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。その後は"コンソールでシステムの容量を管理します"ですが、もしあなたが"自分で集計を作成する"以下の点に注意してください。

- アグリゲート内のすべてのディスクは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 サイズに左右されます。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、必要な持続的なパフォーマンスを実現するディスク サイズを選択する必要があります。
- より大きなディスク (たとえば、4 TiB ディスク 6 台) を選択した場合でも、EC2 インスタンスが帯域幅制限に達する可能性があるため、すべての IOPS を取得できない可能性があります。

  EBSディスクパフォーマンスの詳細については、 "AWS ドキュメント: EBS ボリュームタイプ" 。

  前述のとおり、Amazon EBS Elastic Volumes 機能をサポートするCloud Volumes ONTAP構成では、ディスク サイズの選択はサポートされていません。"Elastic Volumesのサポートについて詳しくはこちら" 。

デフォルトのシステムディスクを表示する

コンソールは、ユーザー データ用のストレージに加えて、 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。計画のために、Cloud Volumes ONTAP を展開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 の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" 。

> コンソール エージェントにはシステム ディスクも必要です。 "コンソールエージェントのデフォルト構成の詳細を表示する" 。

AWS Outpost に**Cloud Volumes ONTAP**を導入する準備

AWS Outpost がある場合は、デプロイプロセス中に Outpost VPC を選択することで、その Outpost にCloud Volumes ONTAP をデプロイできます。エクスペリエンスは、AWS にある他の VPC と同じです。最初に

AWS Outpost にコンソールエージェントをデプロイする必要があることに注意してください。

指摘すべき制限がいくつかあります。

- 現時点では、単一ノードのCloud Volumes ONTAPシステムのみがサポートされています。
- Cloud Volumes ONTAPで使用できるEC2インスタンスは、Outpostで利用可能なものに限定されます。
- 現時点では汎用SSD（gp2）のみがサポートされています

ネットワーク情報を収集する

AWS でCloud Volumes ONTAP を起動するときは、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 **AZ** 内の単一ノードまたは **HA** ペア

AWSの情報	あなたの価値
リージョン	
VPC	
サブネット	
セキュリティ グループ (独自のものを使用する場合)	

複数の**AZ**における**HA**ペア

AWSの情報	あなたの価値
リージョン	
VPC	
セキュリティ グループ (独自のものを使用する場合)	
ノード1のアベイラビリティゾーン	
ノード1サブネット	
ノード2のアベイラビリティゾーン	
ノード2サブネット	
メディエーターの可用性ゾーン	
メディエーターサブネット	
仲介者の鍵ペア	
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のデータ用のフローティングIPアドレス	

AWSの情報	あなたの価値
ノード2のデータ用のフローティングIPアドレス	
フローティングIPアドレスのルートテーブル	

書き込み速度を選択する

コンソールでは、Cloud Volumes ONTAP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、標準設定と高速設定の違い、および高速書き込み速度を使用する場合のリスクと推奨事項を理解しておく必要があります。"書き込み速度について詳しくはこちら" 。

ボリューム使用プロファイルを選択する

ONTAPには、必要なストレージの総量を削減できるいくつかのストレージ効率機能が含まれています。コンソールでボリュームを作成するときに、これらの機能を有効にするプロファイルまたは無効にするプロファイルを選択できます。どのプロファイルを使用するかを決めるには、これらの機能について詳しく理解する必要があります。

NetAppストレージ効率機能には、次のような利点があります。

シンプロビジョニング

物理ストレージ プールに実際に存在するよりも多くの論理ストレージをホストまたはユーザーに提供します。ストレージ スペースを事前に割り当てるのではなく、データが書き込まれるときに各ボリュームにストレージ スペースが動的に割り当てられます。

重複排除

同一のデータ ブロックを見つけて、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。この手法は、同じボリューム内に存在する冗長なデータ ブロックを排除することで、ストレージ容量の要件を削減します。

圧縮

プライマリ、セカンダリ、アーカイブ ストレージのボリューム内のデータを圧縮することで、データの保存に必要な物理容量を削減します。

ネットワークを設定する

Cloud Volumes ONTAP用の AWS ネットワークを設定する

NetApp Consoleは、IP アドレス、ネットマスク、ルートなどのCloud Volumes ONTAP 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 アクセスが利用可能であること、十分なプライベート IP アドレスが利用可能であること、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。

一般要件

AWS で次の要件を満たしていることを確認してください。

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システムでは、さまざまな機能の外部エンドポイントにアクセスするために、アウトバウンド インターネット アクセスが必要です。厳格なセキュリティ要件を持つ環境でこれらのエンドポイントがブロックされている場合、 Cloud Volumes ONTAP は正常に動作しません。

コンソール エージェントは、日常的な操作のために複数のエンドポイントに接続します。使用されるエンドポイントの詳細については、以下を参照してください。 "コンソールエージェントから接続されたエンドポイントを表示する"そして "コンソールを使用するためのネットワークの準備"。

Cloud Volumes ONTAPエンドポイント

Cloud Volumes ONTAP はこれらのエンドポイントを使用してさまざまなサービスと通信します。

エンドポイント	適用対象	目的	展開モード	エンドポイントが利用できない場合の影響
https://netapp-cloud-account.auth0.com	認証	コンソールでの認証に使用されます。	標準モードと制限モード。	ユーザー認証が失敗し、次のサービスは利用できなくなります。 • Cloud Volumes ONTAPサービス • ONTAPサービス • プロトコルとプロキシサービス
https://api.bluexp.netapp.com/tenancy	賃貸借	コンソールからCloud Volumes ONTAPリソースを取得して、リソースとユーザーを承認するために使用されます。	標準モードと制限モード。	Cloud Volumes ONTAPリソースとユーザーは承認されていません。
https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	AutoSupportテレメトリ データをNetAppサポートに送信するために使用されます。	標準モードと制限モード。	AutoSupport情報は未配信のままです。

エンドポイント	適用対象	目的	展開モード	エンドポイントが利用できない場合の影響
AWSサービスの正確な商用エンドポイント（末尾に `amazonaws.com`）は、使用しているAWS リージョンによって異なります。参照 "詳細についてはAWSドキュメントをご覧ください"。	• クラウドフォーメーション • エラスティックコンピューティングクラウド (EC2) • アイデンティティとアクセス管理（IAM） • キー管理サービス (KMS) • セキュリティトークンサービス（STS） • Amazon Simple Storage Service（S3）	AWS サービスとの通信。	標準モードとプライベートモード。	Cloud Volumes ONTAP はAWS サービスと通信してAWS で特定の操作を実行することができません。
AWS サービスの正確な政府エンドポイントは、使用しているAWS リージョンによって異なります。エンドポイントには、 `amazonaws.com` そして `c2s.ic.gov`。参照 "AWS SDK"そして "AWS ドキュメント"詳細についてはこちらをご覧ください。	• クラウドフォーメーション • エラスティックコンピューティングクラウド (EC2) • アイデンティティとアクセス管理（IAM） • キー管理サービス (KMS) • セキュリティトークンサービス（STS） • シンプルストレージサービス（S3）	AWS サービスとの通信。	制限モード。	Cloud Volumes ONTAP はAWS サービスと通信してAWS で特定の操作を実行することができません。

HAメディエーターのアウトバウンドインターネットアクセス

HA メディエーターインスタンスには、ストレージフェイルオーバーを支援できるように、AWS EC2 サービスへの送信接続が必要です。接続を提供するには、パブリック IP アドレスを追加したり、プロキシ サーバーを指定したり、手動オプションを使用したりできます。

手動オプションとしては、ターゲットサブネットから AWS EC2 サービスへの NAT ゲートウェイまたはイン

ターフェース VPC エンドポイントが考えられます。 VPCエンドポイントの詳細については、 "AWS ドキュメント: インターフェイス VPC エンドポイント (AWS PrivateLink)" 。

NetApp Consoleエージェントのネットワークプロキシ構成

NetApp Consoleエージェントのプロキシ サーバー構成を使用して、 Cloud Volumes ONTAPからのアウトバウンド インターネット アクセスを有効にすることができます。コンソールは次の 2 種類のプロキシをサポートしています。

- 明示的なプロキシ: Cloud Volumes ONTAPからの送信トラフィックは、コンソール エージェントのプロキシ構成時に指定されたプロキシ サーバーの HTTP アドレスを使用します。管理者は、追加の認証のためにユーザー資格情報とルート CA 証明書を構成している場合もあります。明示的なプロキシにルートCA証明書が利用可能な場合は、必ず同じ証明書を取得して、 Cloud Volumes ONTAPシステムにアップロードしてください。 "ONTAP CLI: セキュリティ証明書のインストール"指示。
- 透過プロキシ: ネットワークは、 Cloud Volumes ONTAPからの送信トラフィックをコンソール エージェントのプロキシを介して自動的にルーティングするように構成されています。透過プロキシを設定する場合、管理者はプロキシ サーバーの HTTP アドレスではなく、 Cloud Volumes ONTAPからの接続用のルート CA 証明書のみを提供する必要があります。同じルートCA証明書を取得し、 Cloud Volumes ONTAPシステムにアップロードしてください。 "ONTAP CLI: セキュリティ証明書のインストール"指示。

プロキシサーバーの設定方法については、 "プロキシサーバーを使用するようにコンソールエージェントを構成する" 。

プライベート**IP**アドレス

コンソールは、必要な数のプライベート IP アドレスをCloud Volumes ONTAPに自動的に割り当てます。ネットワークに十分なプライベート IP アドレスが利用可能であることを確認する必要があります。

コンソールがCloud Volumes ONTAPに割り当てるLIFの数は、単一ノード システムを展開するか、HA ペアを展開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。

単一ノードシステムの**IP**アドレス

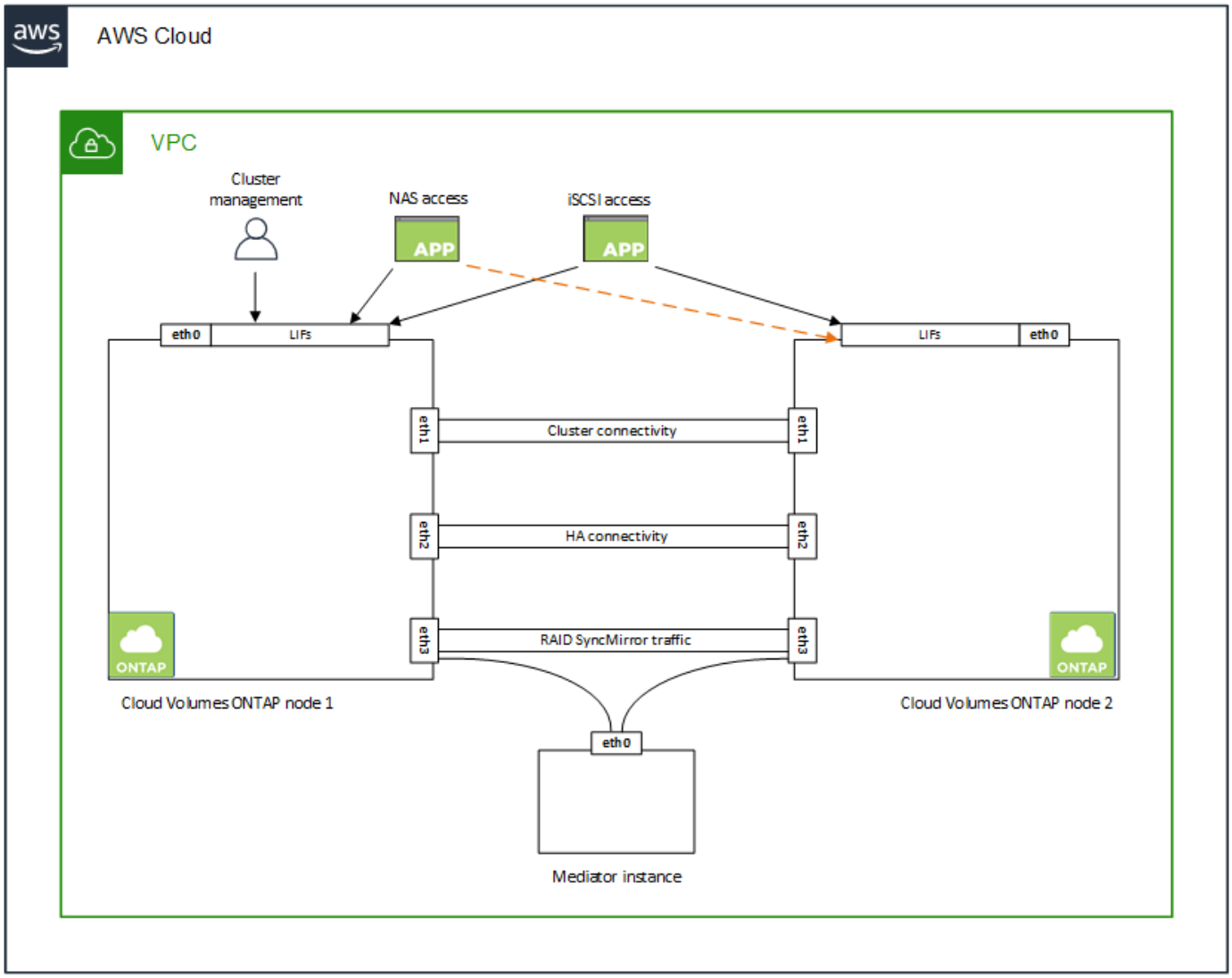
NetApp Console は、単一ノード システムに 6 つの IP アドレスを割り当てます。

次の表は、各プライベート IP アドレスに関連付けられている LIF の詳細を示しています。

LIF	目的
クラスタ管理	クラスタ全体（HA ペア）の管理。
ノード管理	ノードの管理。
インタークラスター	クラスター間の通信、バックアップ、およびレプリケーション。
NASデータ	NAS プロトコル経由のクライアント アクセス。
iSCSIデータ	iSCSI プロトコル経由のクライアント アクセス。システムでは他の重要なネットワーク ワークフローにも使用されます。この LIF は必須であり、削除しないでください。
ストレージVM管理	ストレージ 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 ペアでは、単一ノード 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、選択する展開モデルによって異なります。単一の AWS アベイラビリティゾーン (AZ) に展開された HA ペアには 15 個のプライベート IP アドレスが必要ですが、複数の AZ に展開された HA ペアには 13 個のプライベート IP アドレスが必要です。

次の表は、各プライベート IP アドレスに関連付けられている LIF の詳細を示しています。

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。
インタークラスター	eth0	ノード1とノード2	クラスター間の通信、バックアップ、およびレプリケーション。
NASデータ	eth0	ノード1	NAS プロトコル経由のクライアント アクセス。

LIF	インターフェイス	ノード	目的
iSCSIデータ	eth0	ノード1とノード2	iSCSI プロトコル経由のクライアント アクセス。システムでは他の重要なネットワーク ワークフローにも使用されます。これらの LIF は必須であり、削除しないでください。
クラスター接続	eth1	ノード1とノード2	ノードが相互に通信し、クラスター内でデータを移動できるようにします。
HA接続	eth2	ノード1とノード2	フェイルオーバーの場合の 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	ストレージの引き継ぎ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間の通信チャネル。

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。
インタークラスター	eth0	ノード1とノード2	クラスター間の通信、バックアップ、およびレプリケーション。
iSCSIデータ	eth0	ノード1とノード2	iSCSI プロトコル経由のクライアント アクセス。これらの LIF は、ノード間のフローティング IP アドレスの移行も管理します。これらの LIF は必須であり、削除しないでください。
クラスター接続	eth1	ノード1とノード2	ノードが相互に通信し、クラスター内でデータを移動できるようにします。
HA接続	eth2	ノード1とノード2	フェイルオーバーの場合の 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	ストレージの引き継ぎ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間の通信チャネル。

複数のアベイラビリティゾーンに展開する場合、複数のLIFが関連付けられます。"フローティングIPアドレス"これらは AWS 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

コンソールが自動的にセキュリティ グループを作成するので、セキュリティ グループを作成する必要はありません。独自のものを使用する必要がある場合は、"セキュリティグループルール" 。

コンソール エージェントに関する情報をお探しですか? "コンソールエージェントのセキュリティグループルールを表示する"

データ階層化のための接続

EBS をパフォーマンス層として、Amazon S3 を容量層として使用する場合は、Cloud Volumes ONTAP が S3 に接続し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、 "AWS ドキュメント: ゲートウェイエンドポイントの作成"を参照してください。

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、ルートテーブルを選択してください。また、セキュリティ グループを変更して、S3 エンドポイントへのトラフィックを有効にする送信 HTTPS ルールを追加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、 "AWS 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システム間でデータを複製するには、AWS VPC と他のネットワーク (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、 "AWS ドキュメント: AWS VPN 接続の設定" 。

CIFS 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 を設定するか、オンプレミスの設定を AWS に拡張する必要があります。

DNS サーバーは、Active Directory 環境に対して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 サーバーを使用するように DHCP オプション セットを設定できます。このサーバーは、Active Directory 環境で使用される DNS サーバーであってはなりません。

手順については、 "AWS ドキュメント: AWS クラウド上の Active Directory ドメインサービス: クイックスタートリファレンスデプロイ" 。

VPC共有

9.11.1 リリース以降、 Cloud Volumes ONTAP HA ペアは VPC 共有により AWS でサポートされるようになりました。 VPC 共有により、組織はサブネットを他の AWS アカウントと共有できるようになります。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 ペアをデプロイする必要があります。

"共有サブネットにHAペアを展開する方法を学ぶ" 。

複数の**AZ**における**HA**ペアの要件

複数のアベイラビリティーゾーン (AZ) を使用するCloud Volumes ONTAP HA 構成には、追加の AWS ネットワーク要件が適用されます。 Cloud Volumes ONTAPシステムを追加するときにコンソールにネットワークの詳細を入力する必要があるため、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。

HAペアの仕組みを理解するには、以下を参照してください。"ハイアベイラビリティ ペア" 。

アベイラビリティ ゾーン

この HA 展開モデルでは、複数の AZ を使用してデータの高可用性を確保します。各Cloud Volumes ONTAPインスタンスとメディエーター インスタンスには専用の AZ を使用する必要があります。これにより、HA ペア間の通信チャネルが提供されます。

各アベイラビリティーゾーンでサブネットが利用可能である必要があります。

NASデータとクラスタ/**SVM**管理用のフローティング**IP**アドレス

複数の AZ の HA 構成では、障害が発生した場合にノード間で移行されるフローティング IP アドレスが使用されます。 VPCの外部からはネイティブにアクセスできません。"AWSトランジットゲートウェイを設定する" 。

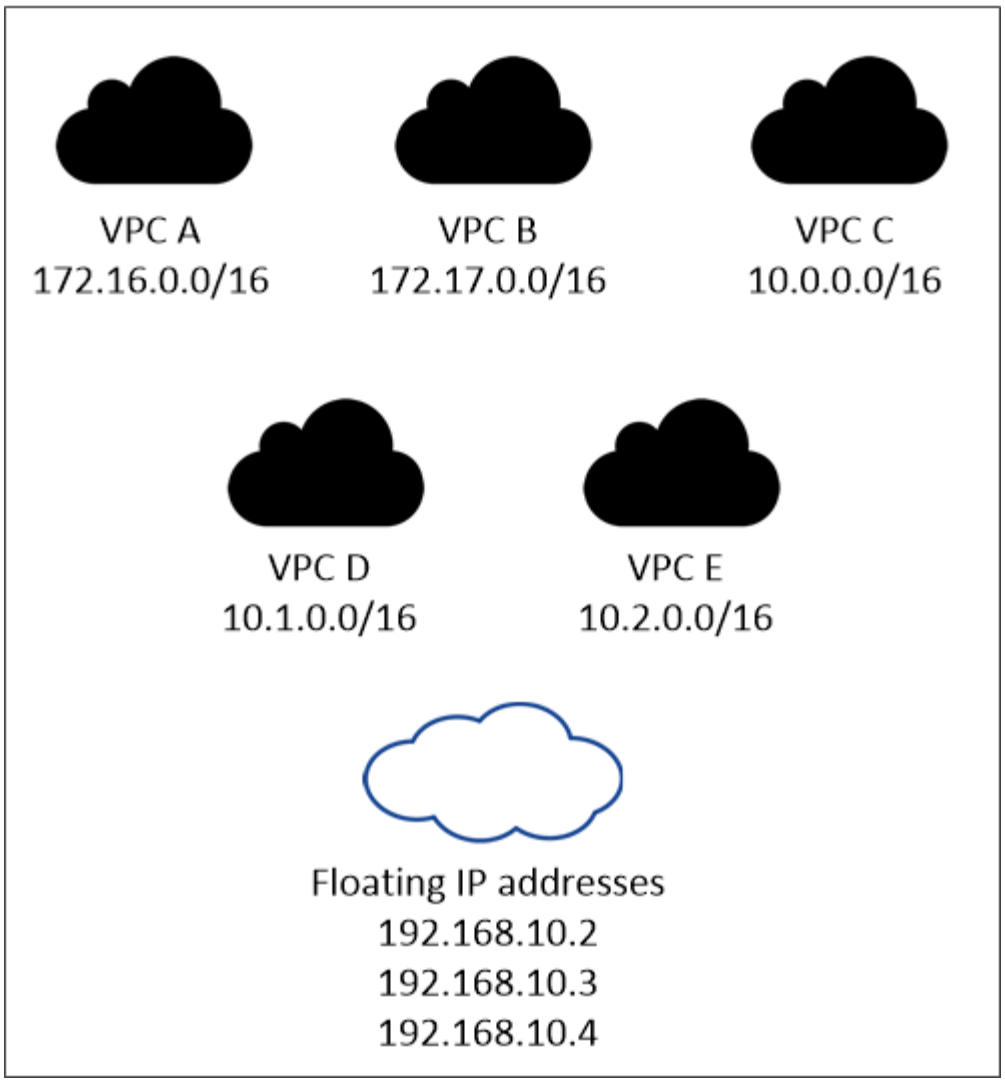
1 つのフローティング IP アドレスはクラスター管理用、1 つはノード 1 の NFS/CIFS データ用、もう 1 つはノード 2 の NFS/CIFS データ用です。 SVM 管理用の 4 番目のフローティング IP アドレスはオプションです。

HA ペアでSnapDrive for Windows またはSnapCenterを使用する場合は、SVM 管理 LIF にフローティング IP アドレスが必要です。

Cloud Volumes ONTAP HA システムを追加するときは、フローティング IP アドレスを入力する必要があります。コンソールは、システムを起動するときに、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 構成を展開する AWS リージョン内のすべての VPC の CIDR ブロックの外側にある必要があります。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 リージョン内のフローティング 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 アドレスはすべての VPC の CIDR ブロックの外側にありますが、ルートテーブルを通じてサブネットにルーティングできます。



コンソールは、iSCSI アクセスおよび VPC 外部のクライアントからの NAS アクセス用に静的 IP アドレスを自動的に作成します。これらのタイプの IP アドレスについては、いかなる要件も満たす必要はありません。

VPC 外部からのフローティング **IP** アクセスを可能にするトランジット ゲートウェイ

必要であれば、"AWSトランジットゲートウェイを設定する" HA ペアが存在する 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

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めるルート テーブルを選択するように求められます。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 内のサブネットにルート テーブルが 1 つだけある場合 (メイン ルート テーブル)、コンソールはフローティング IP アドレスをそのルート テーブルに自動的に追加します。ルート テーブルが複数ある場合は、HA ペアを起動するときに正しいルート 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にアクセスできなくなる可能性があります。

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場合があります。ルート テーブル A を選択し、ルート テーブル B を選択しない場合、ルート 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、ルート 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。

ルートテーブルの詳細については、 "AWS ドキュメント: ルートテーブル" 。

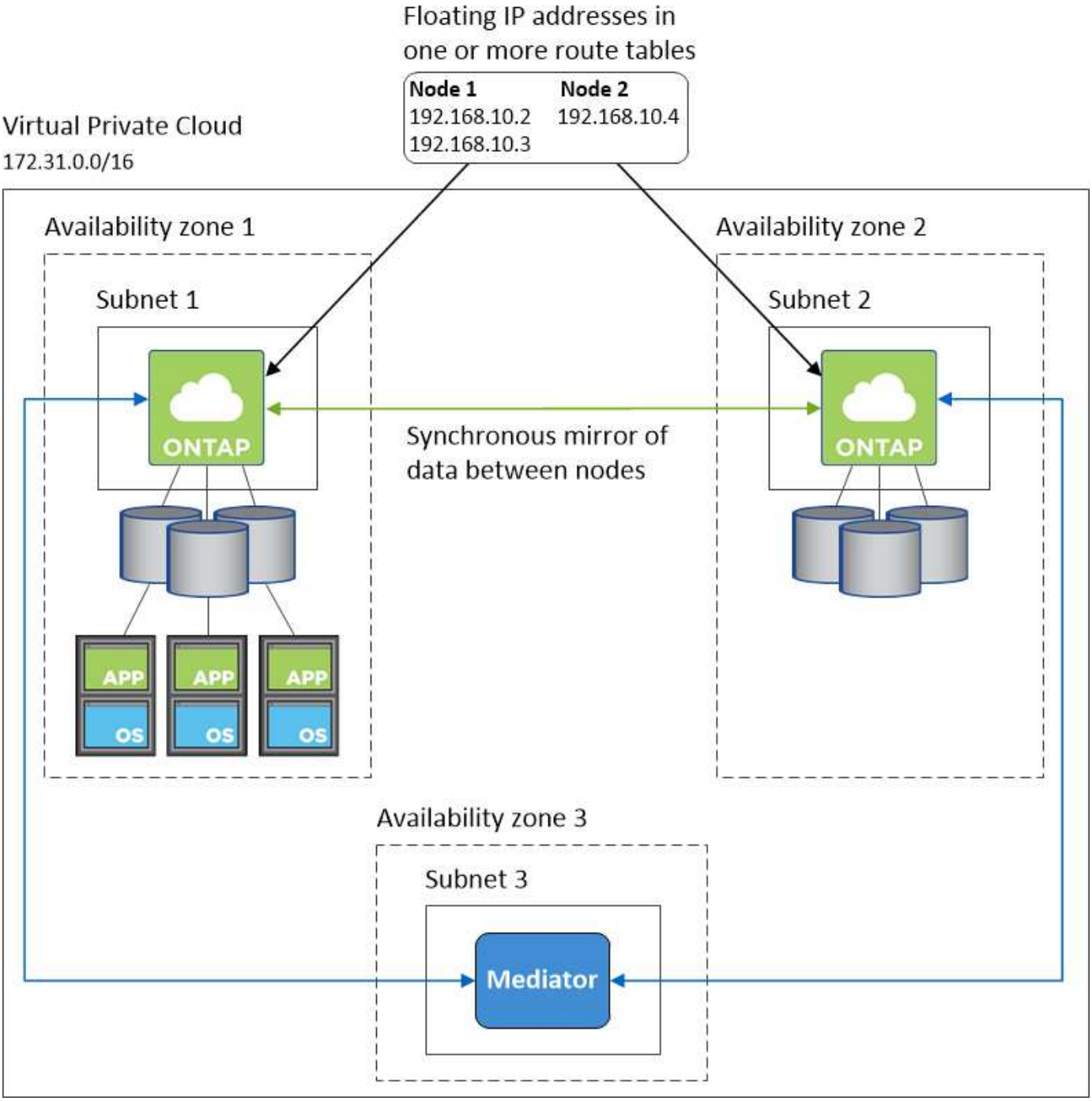
NetApp管理ツールへの接続

複数の AZ にある HA 構成でNetApp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. NetApp管理ツールを別のVPCに導入し、"AWSトランジットゲートウェイを設定する" 。ゲートウェイにより、VPC の外部からクラスター管理インターフェースのフローティング IP アドレスにアクセスできるようになります。
2. NAS クライアントと同様のルーティング構成を使用して、同じ VPC にNetApp管理ツールを展開します。

HA構成の例

次の図は、複数の AZ 内の HA ペアに固有のネットワーク コンポーネント (3 つのアベイラビリティー 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) を示しています。



コンソールエージェントの要件

コンソール エージェントをまだ作成していない場合は、ネットワーク要件を確認する必要があります。

- "コンソールエージェントのネットワーク要件を表示する"
- "AWSのセキュリティグループルール"

関連トピック

- "Cloud Volumes ONTAPのAutoSupport設定を確認する"
- "ONTAPの内部ポートについて学ぶ" 。

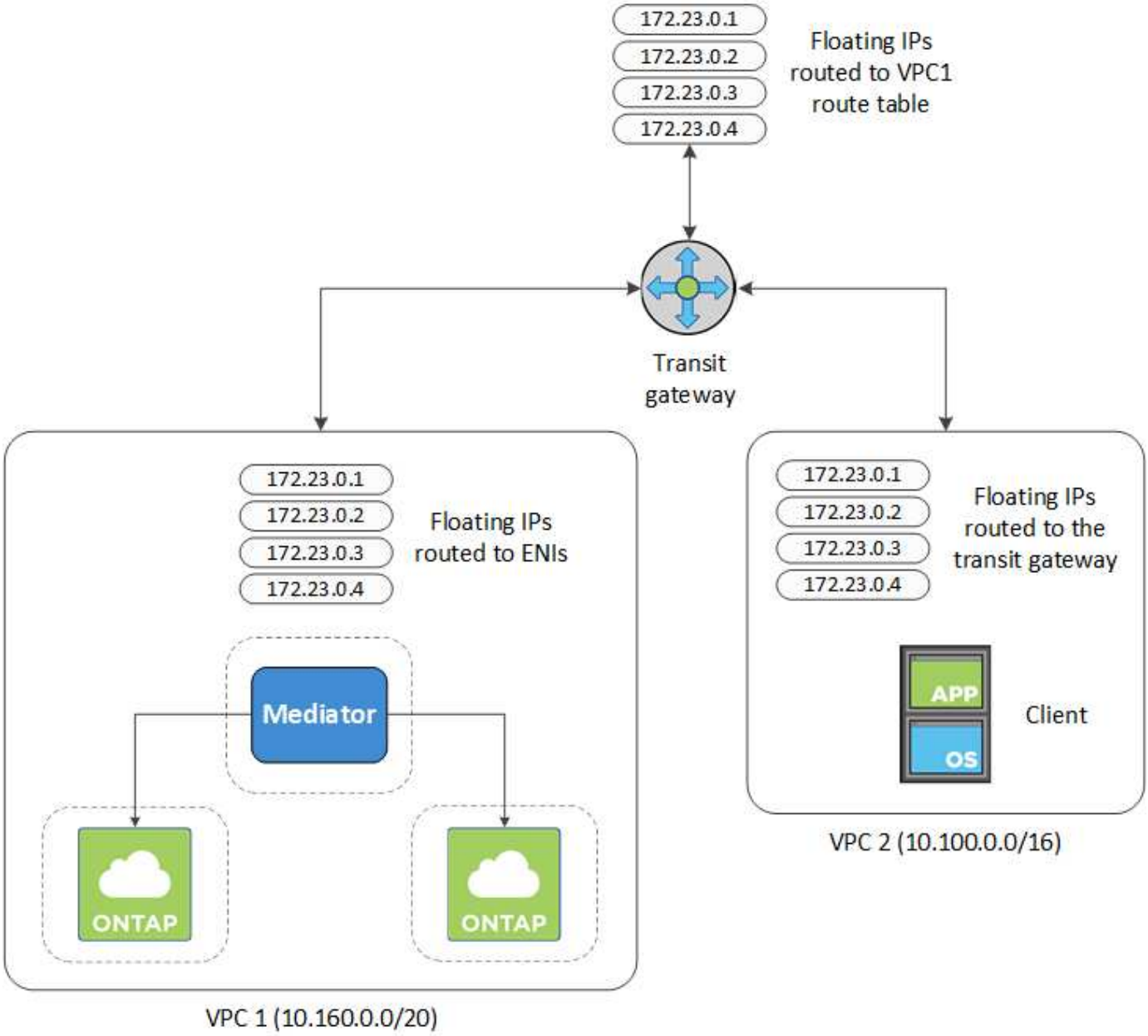
AWSトランジットゲートウェイを設定してHAペアのアクセスを有効にする"フローティングIPアドレス"HA ペアが存在する VPC の外部から。

Cloud Volumes ONTAP HA 構成が複数の AWS アベイラビリティーゾーンに分散されている場合、VPC 内からの NAS データ アクセスにはフローティング 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、障害が発生したときにノード間で移行できますが、VPC の外部からはネイティブにアクセスできません。個別のプライベート IP アドレスは VPC 外部からのデータ アクセスを提供しますが、自動フェイルオーバーは提供しません。

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 トランジットゲートウェイを設定すると、HA ペアが存在する VPC の外部からフローティング IP アドレスへのアクセスが可能になります。つまり、VPC 外部の NAS クライアントとNetApp管理ツールはフローティング IP にアクセスできます。

以下は、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 を示す例です。 HA システムは 1 つの VPC に存在し、クライアントは別の 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クライアントに NAS ボリュームをマウントできます。



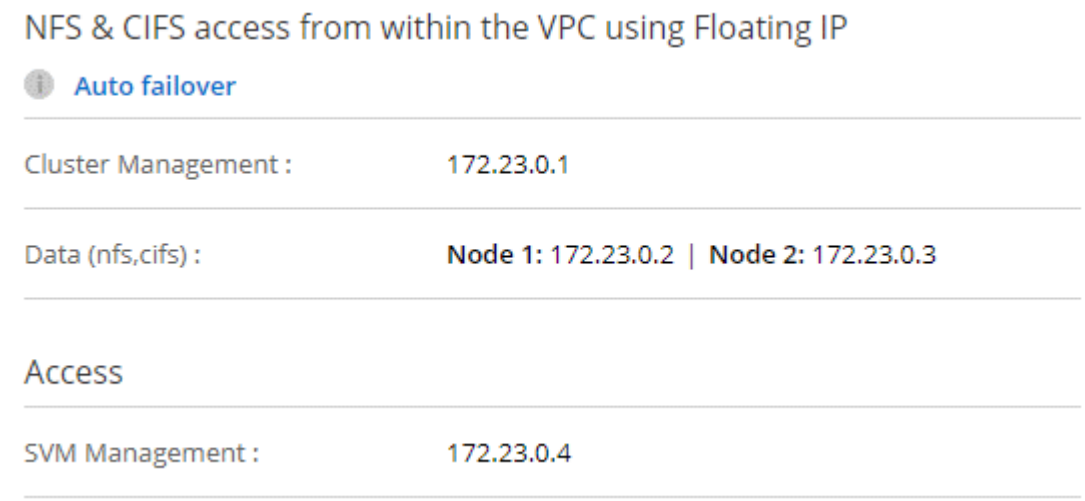
次の手順では、同様の構成を設定する方法を示します。

手順

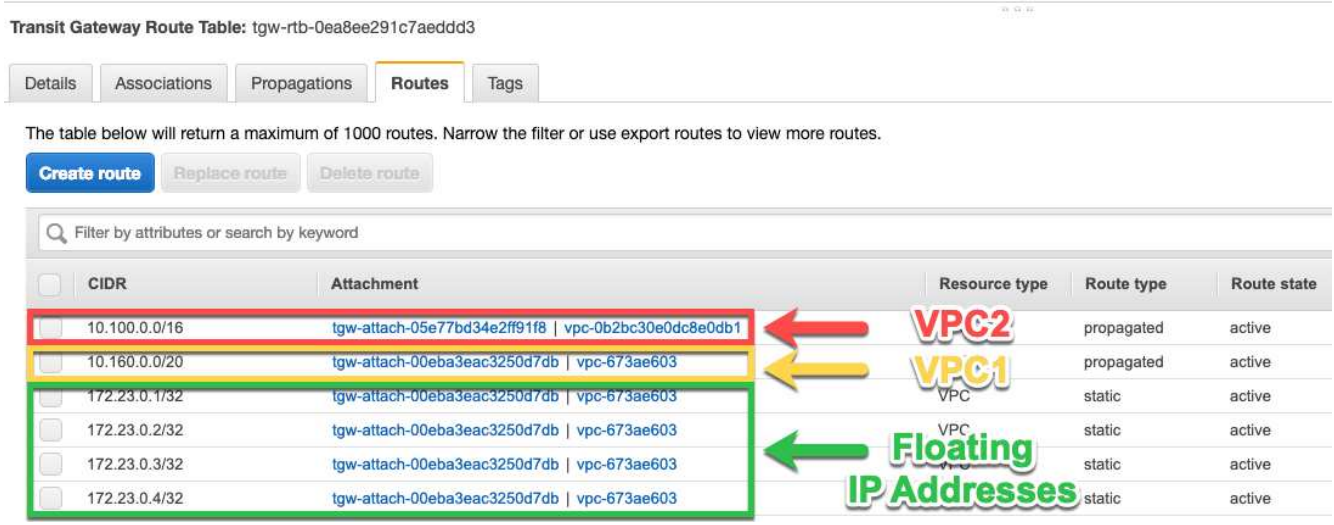
1. "トランジットゲートウェイを作成し、VPC をゲートウェイに接続する" 。
2. VPC をトランジット ゲートウェイ ルート テーブルに関連付けます。
   a. **VPC** サービスで、**Transit Gateway** ルート テーブル をクリックします。
   b. ルート テーブルを選択します。
   c. *関連付け*をクリックし、*関連付けの作成*を選択します。
   d. 関連付ける添付ファイル (VPC) を選択し、[関連付けの作成] をクリックします。
3. HA ペアのフローティング IP アドレスを指定して、トランジット ゲートウェイのルート テーブルにルートを作成します。

   フローティング IP アドレスは、 NetApp Consoleのシステム情報ページで確認できます。次に例を示しま

す。



次のサンプル画像は、トランジット ゲートウェイのルート テーブルを示しています。これには、Cloud Volumes ONTAPで使用される 2 つの VPC の CIDR ブロックと 4 つのフローティング IP アドレスへのルートが含まれます。

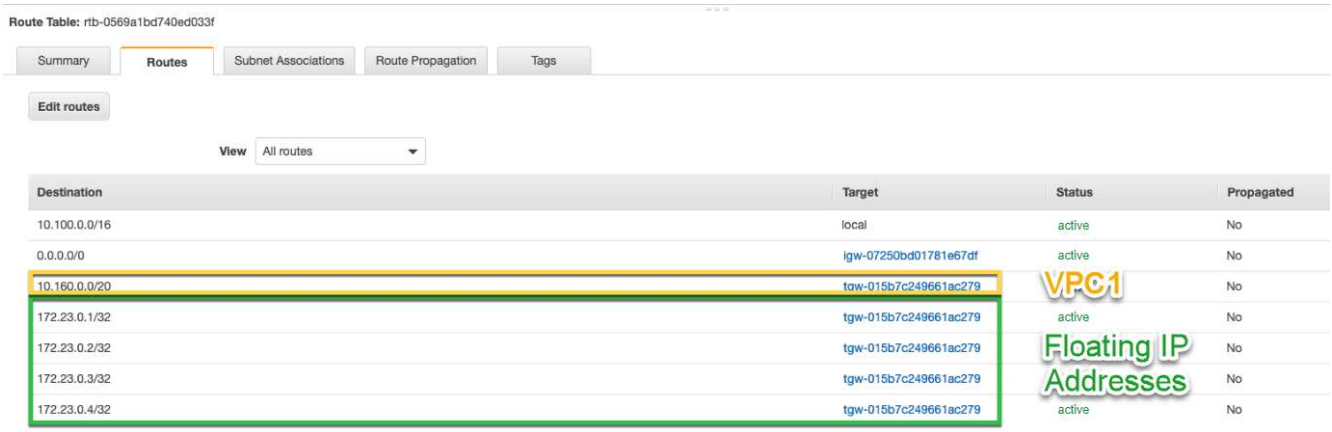


4. フローティング IP アドレスにアクセスする必要がある VPC のルート テーブルを変更します。

   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。

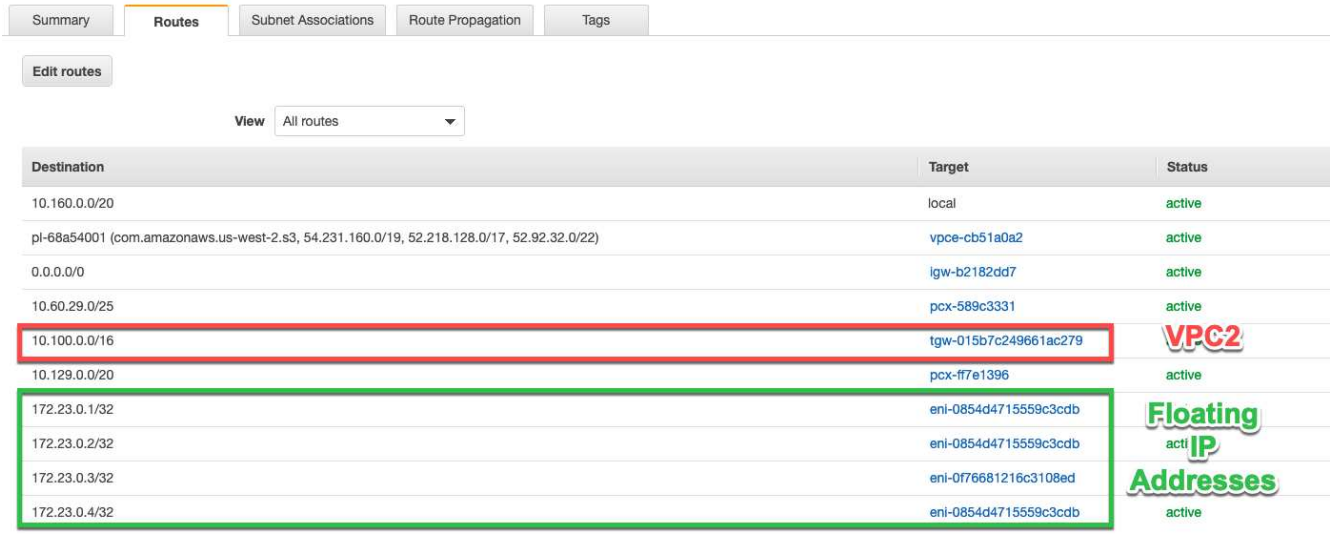
      次のサンプル画像は、VPC 1 へのルートとフローティング IP アドレスを含む VPC 2 のルートテーブルを示しています。



5. フローティング IP アドレスへのアクセスが必要な VPC にルートを追加して、HA ペアの VPC のルートテーブルを変更します。

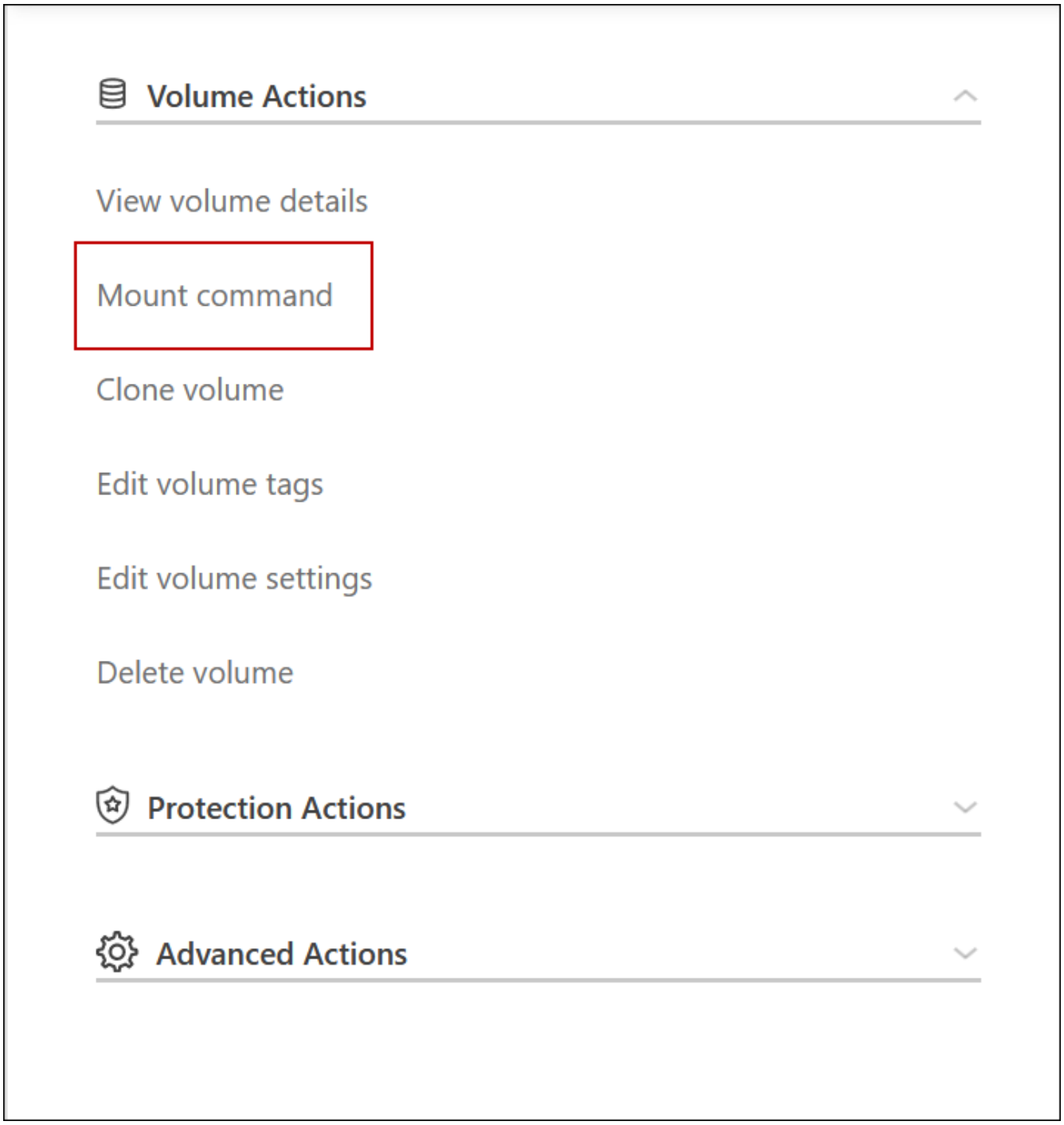
   このステップは、VPC 間のルーティングを完了するため重要です。

   次のサンプル画像は、VPC 1 のルート テーブルを示しています。これには、フローティング IP アドレスと、クライアントが存在する VPC 2 へのルートが含まれます。コンソールは、HA ペアを展開するときに、フローティング IP をルート テーブルに自動的に追加しました。



6. VPC のセキュリティ グループ設定をすべてのトラフィックに更新します。
   a. 仮想プライベートクラウドの下で、*サブネット*をクリックします。
   b. ルート テーブル タブをクリックし、HA ペアのフローティング IP アドレスの 1 つに対して目的の環境を選択します。
   c. *セキュリティ グループ*をクリックします。
   d. *受信規則の編集*を選択します。
   e. *ルールを追加*をクリックします。
   f. [タイプ] で [すべてのトラフィック] を選択し、VPC IP アドレスを選択します。
   g. 変更を適用するには、[ルールを保存] をクリックします。
7. 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。

コンソールの「ボリュームの管理」パネルの下にある マウント コマンド オプションを通じて、コンソールで正しい IP アドレスを見つけることができます。



8. 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。

   "ボリュームの編集方法を学ぶ" 。

関連リンク

- "AWSのハイアベイラビリティ ペア"

- "AWS におけるCloud Volumes ONTAPのネットワーク要件"

AWS共有サブネットに**Cloud Volumes ONTAP HA**ペアをデプロイする

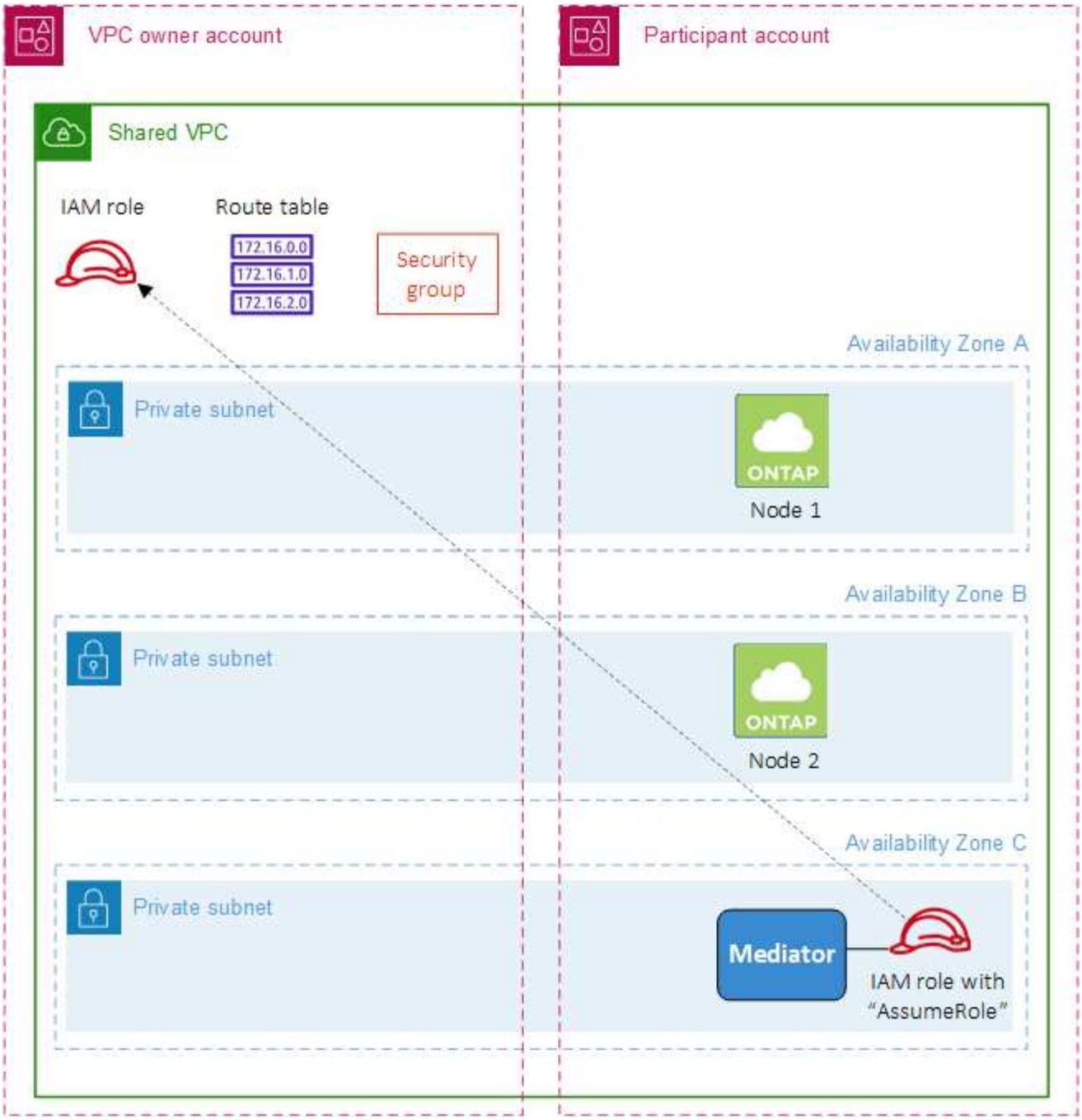
9.11.1 リリース以降、 Cloud Volumes ONTAP HA ペアは VPC 共有により AWS でサポートされるようになりました。 VPC 共有により、組織はサブネットを他の AWS アカウントと共有できるようになります。この構成を使用するには、AWS 環境をセットアップし、API を使用して HA ペアをデプロイする必要があります。

と "VPC共有"Cloud Volumes ONTAP HA 構成は 2 つのアカウントに分散されています。

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

複数のアベイラビリティーゾーンにまたがってデプロイされたCloud Volumes ONTAP HA 構成の場合、HA メディエーターには、VPC 所有者アカウントのルートテーブルに書き込むための特定の権限が必要です。メディエーターが引き受けることができる IAM ロールを設定して、これらの権限を付与する必要があります。

次の図は、この展開に関係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、参加者アカウントとサブネットを共有し、VPC 所有者アカウントに 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システムを作成すると、 NetApp Consoleによって IAM ロールが自動的に作成され、メディエーターにアタッチされます。このロールは、HA ペアに関連付けられたルートテーブルに変更を加えるために、VPC 所有者アカウントで作成した IAM ロールを引き継ぎます。

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、共有サブネットに HA ペアを展開するために必要です。

   "AWS ドキュメント: サブネットの共有"

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 メディエーター用のセキュリティ グループを作成する必要はありません。コンソールがそれを実行します。

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システムを作成します。

   次のフィールドを指定する必要があることに注意してください。

   - 「セキュリティグループID」

     「securityGroupId」フィールドには、VPC 所有者アカウントで作成したセキュリティ グループを指定する必要があります (上記の手順 2 を参照)。

   - 「haParams」オブジェクトの「assumeRoleArn」

     「assumeRoleArn」フィールドには、VPC 所有者アカウントで作成した IAM ロールの ARN を含める必要があります (上記の手順 3 を参照)。

     例えば：

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

+
"Cloud Volumes ONTAP APIについて学ぶ"

AWS の単一 **AZ** で**Cloud Volumes ONTAP HA** ペアの配置グループ作成を構成する

配置グループの作成に失敗すると、AWS 単一アベイラビリティゾーン (AZ) でのCloud Volumes ONTAP高可用性 (HA) デプロイメントが失敗し、ロールバックされる可能性があります。 Cloud Volumes ONTAPノードとメディエーターインスタンスが利用できない

場合は、配置グループの作成も失敗し、デプロイメントはロールバックされます。これを回避するには、配置グループの作成が失敗した場合でもデプロイメントが完了するように構成を変更します。

ロールバック プロセスをバイパスすると、 Cloud Volumes ONTAP のデプロイメント プロセスが正常に完了し、配置グループの作成が完了していないことが通知されます。

手順

1. SSH を使用してNetApp Consoleエージェント ホストに接続し、ログインします。
2. 移動先 `/opt/application/netapp/cloudmanager/docker_occm/data`。
3. 編集 `app.conf`の値を変更することで `rollback-on-placement-group-failure`パラメータに `false`。このパラメータのデフォルト値は `true`。

```
{
    "occm" : {
        "aws" : {
            "rollback-on-placement-group-failure" : false
        }
    }
}
```

4. ファイルを保存し、コンソール エージェントからログオフします。コンソール エージェントを再起動する必要はありません。

Cloud Volumes ONTAPの **AWS** セキュリティグループのインバウンドおよびアウトバウンドルール

NetApp Consoleは、 Cloud Volumes ONTAP が正常に動作するために必要なインバウンドルールとアウトバウンドルールを含む AWS セキュリティグループを作成します。テスト目的の場合、または独自のセキュリティ グループを使用する場合は、ポートを参照することをお勧めします。

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

Cloud Volumes ONTAPシステムを追加し、定義済みのセキュリティ グループを選択すると、次のいずれかの範囲内でトラフィックを許可することを選択できます。

- 選択した **VPC** のみ: 受信トラフィックのソースは、Cloud Volumes ONTAPシステムの VPC のサブネット範囲と、コンソール エージェントが存在する VPC のサブネット範囲です。これは推奨されるオプションです。
- すべての **VPC**: 受信トラフィックのソースは 0.0.0.0/0 IP 範囲です。

プロトコル	ポート	目的
すべてのICMP	全て	インスタンスにpingを実行する
HTTP	80	クラスタ管理LIFのIPアドレスを使用してONTAP System Manager WebコンソールにHTTPアクセスする
HTTPS	443	コンソールエージェントとの接続と、クラスタ管理LIFのIPアドレスを使用したONTAP 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 フレームを使用した TCP 経由の Microsoft SMB/CIFS
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 モニター
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 モニター
UDP	4049	NFS rquotadプロトコル

アウトバウンドルール

Cloud Volumes ONTAPの定義済みセキュリティ グループは、すべての送信トラフィックを開きます。それが許容できる場合は、基本的な送信ルールに従ってください。より厳格なルールが必要な場合は、高度な送信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の定義済みセキュリティ グループには、次の送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ICMP	全て	すべての送信トラフィック
すべてTCP	全て	すべての送信トラフィック
すべてUDP	全て	すべての送信トラフィック

高度なアウトバウンドルール

送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による送信通信に必要なポートのみを開くことができます。

ソースは、Cloud Volumes ONTAPシステム上のインターフェース (IP アドレス) です。

サービス	プロトコル	ポート	ソース	デスティネーション	目的
Active Directory	TCP	88	ノード管理LIF	アクティブディレクトリフォレスト	Kerberos V認証
	UDP	137	ノード管理LIF	アクティブディレクトリフォレスト	NetBIOSネーム サービス
	UDP	138	ノード管理LIF	アクティブディレクトリフォレスト	NetBIOSデータグラムサービス
	TCP	139	ノード管理LIF	アクティブディレクトリフォレスト	NetBIOSサービス セッション
	TCP とUDP	389	ノード管理LIF	アクティブディレクトリフォレスト	LDAP
	TCP	445	ノード管理LIF	アクティブディレクトリフォレスト	NetBIOS フレームを使用した TCP 経由の Microsoft SMB/CIFS
	TCP	464	ノード管理LIF	アクティブディレクトリフォレスト	Kerberos V パスワードの変更と設定 (SET_CHANGE)
	UDP	464	ノード管理LIF	アクティブディレクトリフォレスト	Kerberos鍵管理
	TCP	749	ノード管理LIF	アクティブディレクトリフォレスト	Kerberos V パスワードの変更と設定 (RPCSEC_GSS)
	TCP	88	データ LIF (NFS、CIFS、iSCSI)	アクティブディレクトリフォレスト	Kerberos V認証
	UDP	137	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	NetBIOSネーム サービス
	UDP	138	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	NetBIOSデータグラムサービス
	TCP	139	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	NetBIOSサービス セッション
	TCP とUDP	389	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	LDAP
	TCP	445	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	NetBIOS フレームを使用した TCP 経由の Microsoft SMB/CIFS
	TCP	464	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	Kerberos V パスワードの変更と設定 (SET_CHANGE)
	UDP	464	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	Kerberos鍵管理
	TCP	749	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	Kerberos V パスワードの変更と設定 (RPCSEC_GSS)

サービス	プロトコル	ポート	ソース	デスティネーション	目的
AutoSupport	HTTPS	443	ノード管理LIF	mysupport.netapp.com	AutoSupport （HTTPSがデフォルト）
	HTTP	80	ノード管理LIF	mysupport.netapp.com	AutoSupport （トランスポート プロトコルが HTTPS から HTTP に変更された場合のみ）
	TCP	3128	ノード管理LIF	コンソールエージェント	アウトバウンドインターネット接続が利用できない場合、コンソールエージェント上のプロキシサーバーを介してAutoSupportメッセージを送信する
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復元エンドポイント	S3へのバックアップ機能のバックアップと復元操作
クラスタ	すべてのトラフィック	すべてのトラフィック	すべてのLIFを1つのノードに	他のノード上のすべてのLIF	クラスタ間通信（Cloud Volumes ONTAP HAのみ）
	TCP	3000	ノード管理LIF	HA Mediator	ZAPI 呼び出し (Cloud Volumes ONTAP HA のみ)
	ICMP	1	ノード管理LIF	HA Mediator	キープアライブ（Cloud Volumes ONTAP HAのみ）
構成のバックアップ	HTTP	80	ノード管理LIF	http://<コンソールエージェントのIPアドレス>/occm/offboxconfig	構成のバックアップをコンソールエージェントに送信します。"ONTAPのドキュメント"
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	宛先サーバー	NDMPコピー
SMTP	TCP	25	ノード管理LIF	メール サーバ	SMTPアラートはAutoSupportに使用できます

サービス	プロトコル	ポート	ソース	デスティネーション	目的
SNMP	TCP	161	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	UDP	161	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	TCP	162	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	UDP	162	ノード管理LIF	監視サーバー	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メディエーター外部セキュリティグループのルール

Cloud Volumes ONTAP HA メディエーターの定義済み外部セキュリティ 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

HA メディエーターの定義済みセキュリティ グループには、次の受信ルールが含まれています。

プロトコル	ポート	ソース	目的
TCP	3000	コンソールエージェントのCIDR	コンソールエージェントからのRESTful APIアクセス

アウトバウンドルール

HA メディエーターの定義済みセキュリティ グループは、すべての送信トラフィックを開きます。それが許容できる場合は、基本的な送信ルールに従ってください。より厳格なルールが必要な場合は、高度な送信ルールを使用します。

基本的なアウトバウンドルール

HA メディエーターの定義済みセキュリティ グループには、次の送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TCP	全て	すべての送信トラフィック
すべてUDP	全て	すべての送信トラフィック

高度なアウトバウンドルール

送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 メディエーターによる送信通信に必要なポートのみを開くことができます。

プロトコル	ポート	デスティネーション	目的
HTTP	80	AWS EC2 インスタンス上のコンソールエージェントの 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
HTTPS	443	ec2.amazonaws.com	ストレージフェイルオーバーの支援
UDP	53	ec2.amazonaws.com	ストレージフェイルオーバーの支援

ポート 443 と 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構成内部セキュリティグループのルール

Cloud Volumes ONTAP HA 構成の定義済み内部セキュリティ 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 グループにより、HA ノード間およびメディエーターとノード間の通信が可能になります。

コンソールは常にこのセキュリティ グループを作成します。独自のものを使用するオプションはありません。

インバウンドルール

定義済みのセキュリティ グループには、次の受信規則が含まれています。

プロトコル	ポート	目的
すべてのトラフィック	全て	HAメディエーターと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、次の送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	全て	HAメディエーターとHAノード間の通信

コンソールエージェントのルール

"コンソールエージェントのセキュリティグループルールを表示する"

AWS で顧客管理キーを使用するようにCloud Volumes ONTAP を設定する

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. アクティブなカスタマー マスター キー (CMK) が存在することを確認します。

   CMK は、AWS 管理の CMK またはカスタマー管理の CMK にすることができます。これは、 NetApp Console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: カスタマーマスターキー (CMK)"

2. コンソールへの権限を提供する IAM ロールを キー ユーザー として追加して、各 CMK のキー ポリシーを変更します。

   Identity and Access Management (IAM) ロールをキーユーザーとして追加すると、コンソールにCloud Volumes ONTAPで CMK を使用する権限が付与されます。

   "AWS 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 コンソールに移動します。

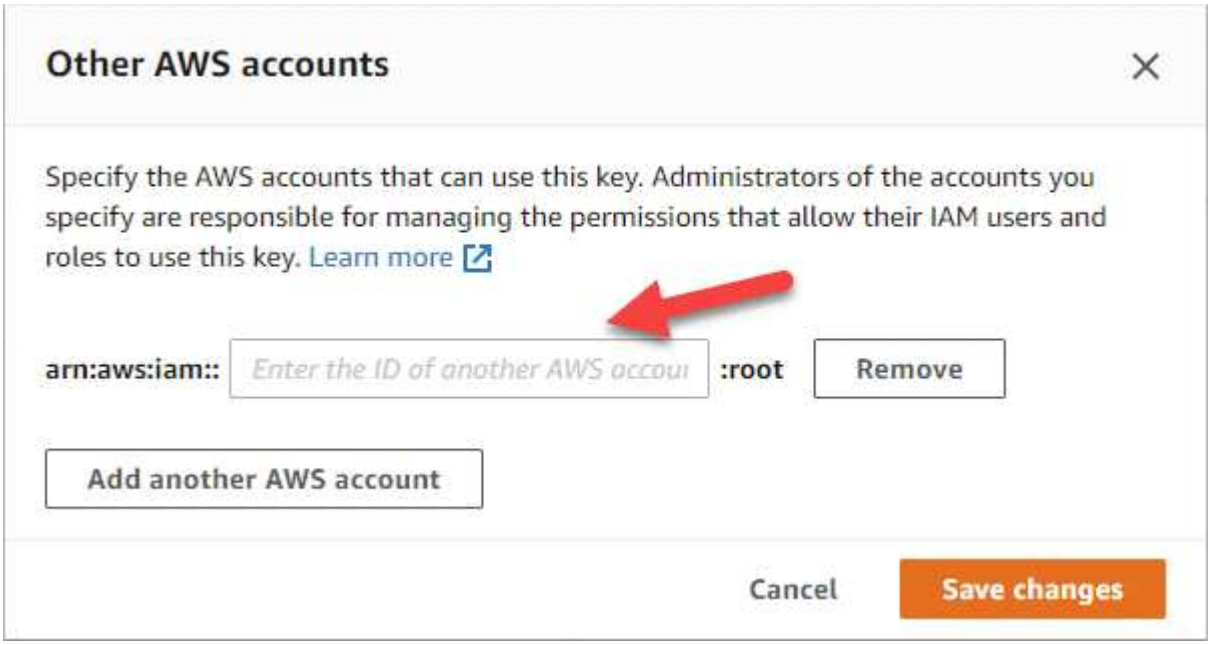
   b. キーを選択します。

   c. 一般設定 ペインで、キーの ARN をコピーします。

      Cloud Volumes ONTAPシステムを作成するときに、コンソールに ARN を提供する必要があります。

   d. その他の **AWS** アカウント ペインで、コンソールに権限を付与する AWS アカウントを追加します。

      通常、これはコンソールが展開されるアカウントです。コンソールが AWS にインストールされていない場合は、コンソールに AWS アクセスキーを提供したアカウントを使用します。



e. 次に、コンソールに権限を付与する AWS アカウントに切り替えて、IAM コンソールを開きます。

f. 以下にリストされている権限を含む IAM ポリシーを作成します。

g. コンソールに権限を提供する IAM ロールまたは IAM ユーザーにポリシーをアタッチします。

次のポリシーは、コンソールが外部 AWS アカウントの CMK を使用するために必要な権限を提供します。「リソース」セクションの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、 "AWSドキュメント: 他のアカウントのユーザーがKMSキーを使用できるようにする" 。

4. カスタマー管理の CMK を使用している場合は、 Cloud Volumes ONTAP IAM ロールを キー ユーザー 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 でデータ階層化を有効にし、Amazon Simple Storage Service（Amazon S3）バケットに保存されているデータを暗号化する場合に必要です。

Cloud Volumes ONTAPシステムを作成すると IAM ロールが作成されるため、 Cloud Volumes ONTAP をデプロイした後でこの手順を実行する必要があります。 (もちろん、既存のCloud Volumes ONTAP IAM ロールを使用するオプションもあるため、この手順を事前に実行することも可能です。)

"AWS ドキュメント: キーの編集"

Cloud Volumes ONTAPノードのAWS IAMロールを設定する

必要な権限を持つ AWS Identity and Access management (IAM) ロールを各Cloud Volumes ONTAPノードに添付する必要があります。HA メディエーターについても同様です。 NetApp Consoleで IAM ロールを作成するのが最も簡単ですが、独自のロールを使用することもできます。

このタスクはオプションです。 Cloud Volumes ONTAPシステムを作成する場合、デフォルトのオプションでは、コンソールによって IAM ロールが自動的に作成されます。会社のセキュリティ ポリシーにより IAM ロールを自分で作成する必要がある場合は、以下の手順に従ってください。

AWS Secret Cloud では独自の IAM ロールを提供する必要があります。"C2SでCloud Volumes ONTAPを展開する方法を学ぶ" 。

手順

1. AWS IAM コンソールに移動します。
2. 次の権限を含む IAM ポリシーを作成します。

   - Cloud Volumes ONTAPノードの基本ポリシー

標準地域

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

GovCloud（米国）リージョン

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

极秘地域

```
{
    "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"
    }]
}
```

秘密の地域

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

- Cloud Volumes ONTAPノードのバックアップポリシー

  Cloud Volumes ONTAPシステムでNetApp Backup and Recoveryを使用する予定の場合は、ノードのIAM ロールに以下に示す 2 番目のポリシーを含める必要があります。

標準地域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud（米国）リージョン

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

極秘地域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

秘密の地域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- HA Mediator

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

3. IAM ロールを作成し、作成したポリシーをロールにアタッチします。

結果

これで、新しいCloud Volumes ONTAPシステムを作成するときに選択できる IAM ロールが用意されました。

詳細情報

- "AWSドキュメント: IAMポリシーの作成"
- "AWSドキュメント: IAMロールの作成"

AWSでCloud Volumes ONTAPのライセンスを設定する

Cloud Volumes ONTAPで使用するライセンス オプションを決定したら、新しいシステムを作成するときにそのライセンス 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

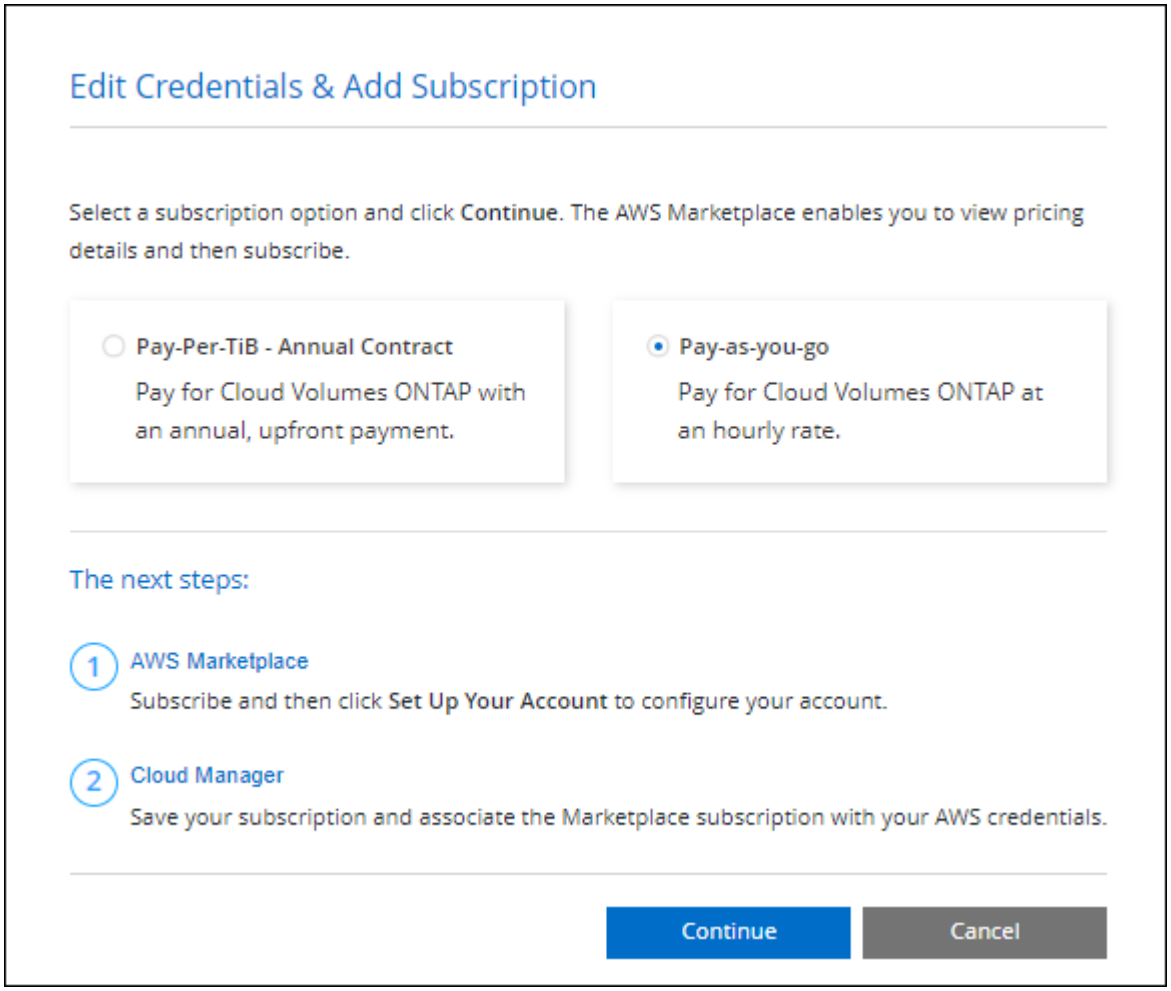
最大 500 GiB のプロビジョニング容量でCloud Volumes ONTAP を無料で使用するには、Freemium オファリングを選択してください。"フリーミアムプランの詳細" 。

手順

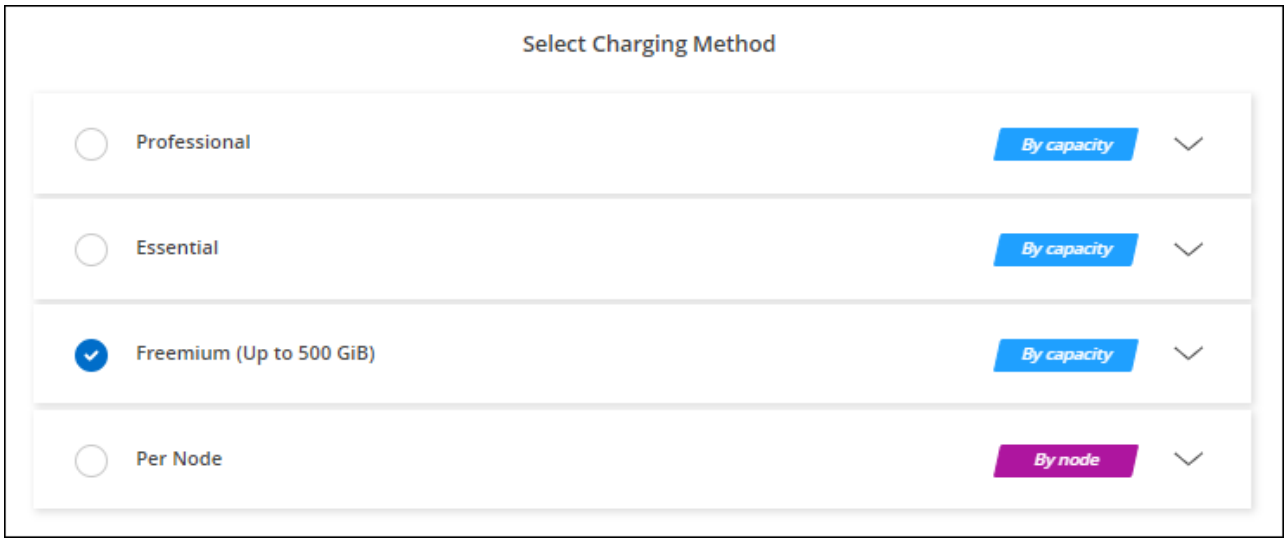
1. NetApp Consoleの左側のナビゲーション メニューから、ストレージ > 管理 を選択します。
2. *システム*ページで*システムの追加*をクリックし、手順に従います。

a. *詳細と認証情報*ページで、*認証情報の編集 > 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の従量課金制サービスにサブスクライブします。

プロビジョニングされた容量が500GiBを超えない限り、マーケットプレイスのサブスクリプションを通じて課金されることはありません。その時点で、システムは自動的に"エッセンシャルパッケージ"。



a. コンソールに戻ったら、課金方法のページにアクセスして「**Freemium**」を選択します。



"AWS でCloud Volumes ONTAP を起動するための手順をご覧ください" 。

容量ベースのライセンス

容量ベースのライセンスでは、容量 1 TiB ごとにCloud Volumes ONTAPの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、Essentials パッケージまたは Professional パッケージというパッケージ形式で提供されます。

Essentials および Professional パッケージは、次の消費モデルまたは購入オプションで利用できます。

- NetAppから購入したライセンス（BYOL）
- AWS Marketplace からの時間単位従量課金制 (PAYGO) サブスクリプション
- AWS Marketplaceからの年間契約

"容量ベースのライセンスについて詳しく見る" 。

次のセクションでは、それぞれの消費モデルを開始する方法について説明します。

BYOL

NetAppからライセンス (BYOL) を購入して前払いすることで、任意のクラウド プロバイダーにCloud Volumes ONTAPシステムを導入できます。

はBYOLライセンスの購入、延長、および更新を制限しています。 "Cloud Volumes ONTAPの BYOL ライセンスの利用制限" 。

手順

1. "ライセンスを取得するには、 NetApp の営業担当者にお問い合わせください。"
2. "NetAppサポートサイトのアカウントをコンソールに追加します"

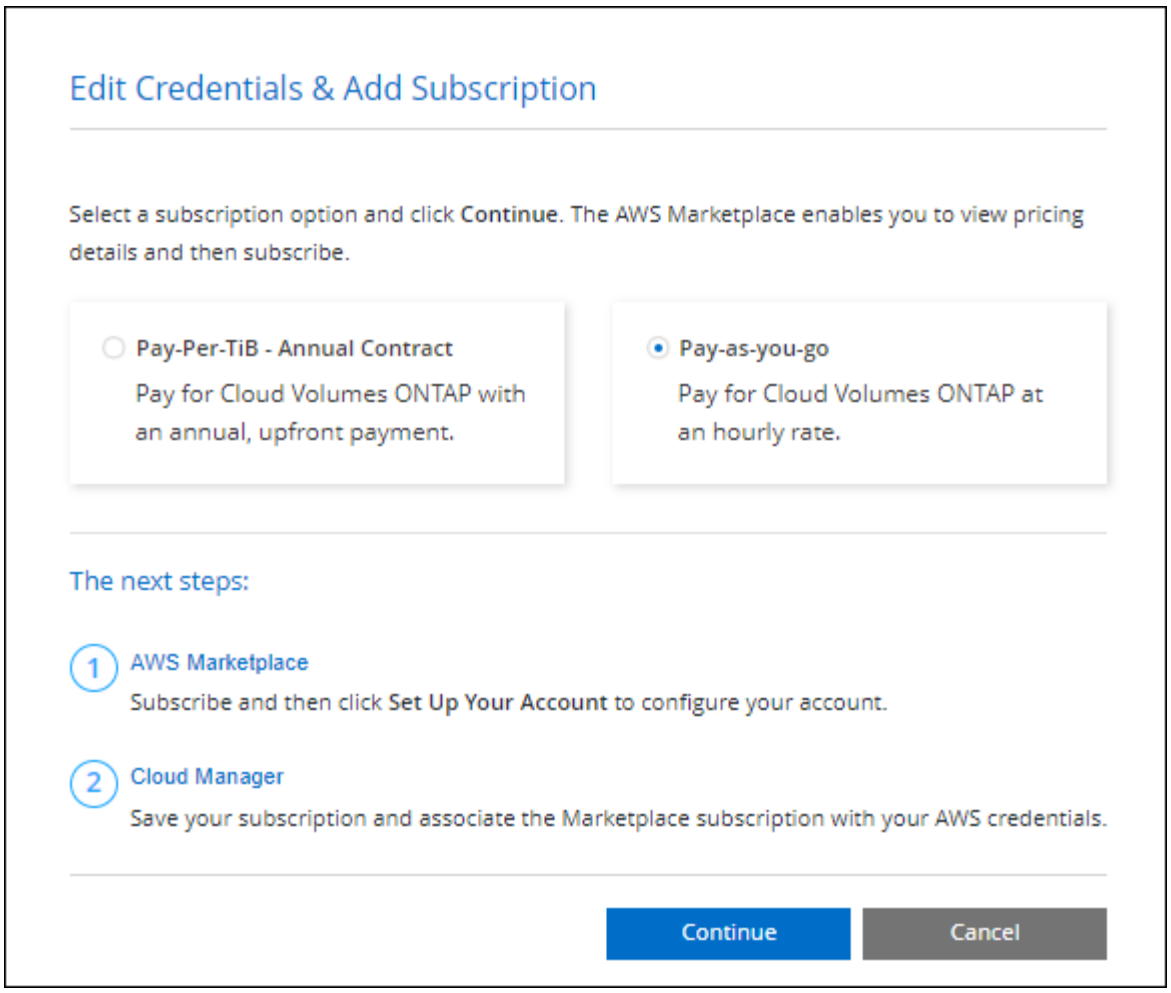
   コンソールは NetApp のライセンス サービスに自動的にクエリを実行し、 NetAppサポート サイト アカウントに関連付けられているライセンスの詳細を取得します。エラーがない場合、コンソールはライセンスを自動的にコンソールに追加します。

   Cloud Volumes ONTAPでライセンスを使用するには、コンソールからライセンスを利用できる必要があります。必要であれば、"コンソールにライセンスを手動で追加する" 。

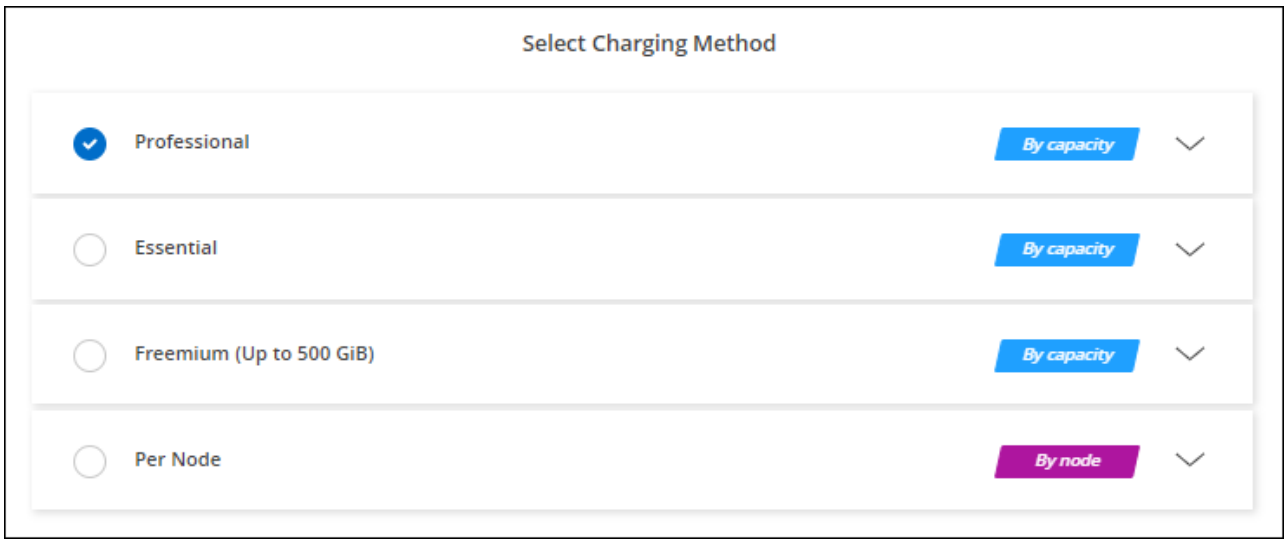
3. コンソールの システム ページで、システムの追加 をクリックし、手順に従います。

   a. *詳細と認証情報*ページで、*認証情報の編集 > 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の従量課金制サービスにサブスクライブします。

      NetAppから購入したライセンスに対しては常に最初に課金されますが、ライセンス容量を超えた場合、またはライセンスの有効期限が切れた場合は、マーケットプレイスの時間単位料金で課金されます。



a. コンソールに戻ったら、課金方法ページにアクセスして容量ベースのパッケージを選択します。



"AWS でCloud Volumes ONTAP を起動するための手順をご覧ください" 。

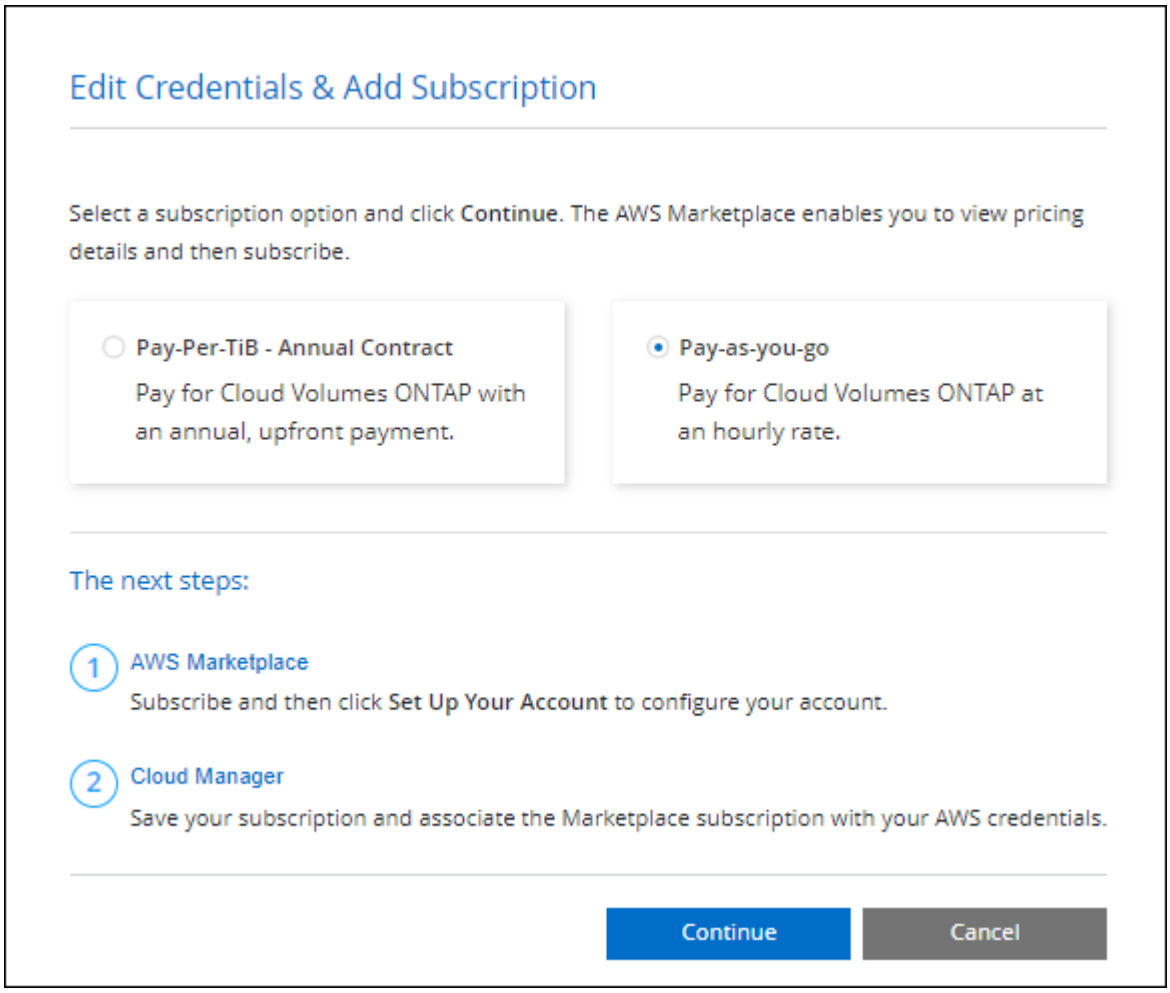
PAYGOサブスクリプション

クラウド プロバイダーのマーケットプレイスからのオファーをサブスクライブして、時間単位で支払います。

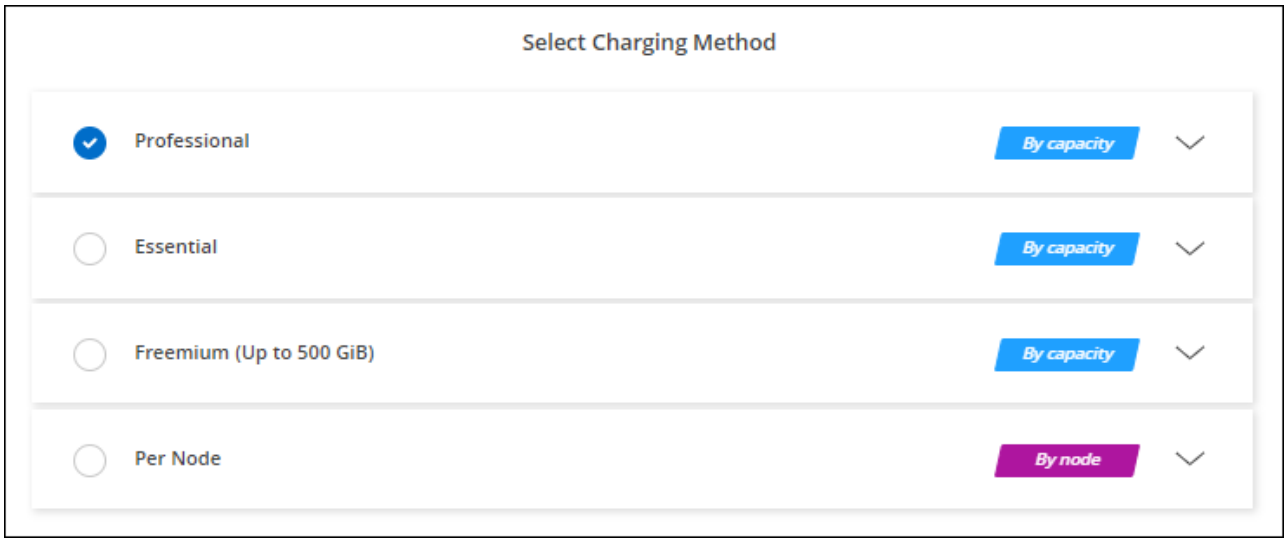
Cloud Volumes ONTAPシステムを作成すると、コンソールに AWS Marketplace で入手可能な契約にサブスクライブするように求めるプロンプトが表示されます。そのサブスクリプションは課金システムに関連付けられます。同じサブスクリプションを追加のCloud Volumes ONTAPシステムにも使用できます。

手順

1. 左側のナビゲーション メニューから、ストレージ > 管理 を選択します。
2. *システム*ページで*システムの追加*をクリックし、手順に従います。
   a. *詳細と認証情報*ページで、*認証情報の編集>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の従量課金制サービスにサブスクライブします。



   b. コンソールに戻ったら、課金方法ページにアクセスして容量ベースのパッケージを選択します。



"AWS でCloud Volumes ONTAP を起動するための手順をご覧ください" 。

AWS アカウントに関連付けられている AWS Marketplace サブスクリプションは、[設定] > [認証情報] ページから管理できます。 "AWSアカウントとサブスクリプションの管理方法を学ぶ"

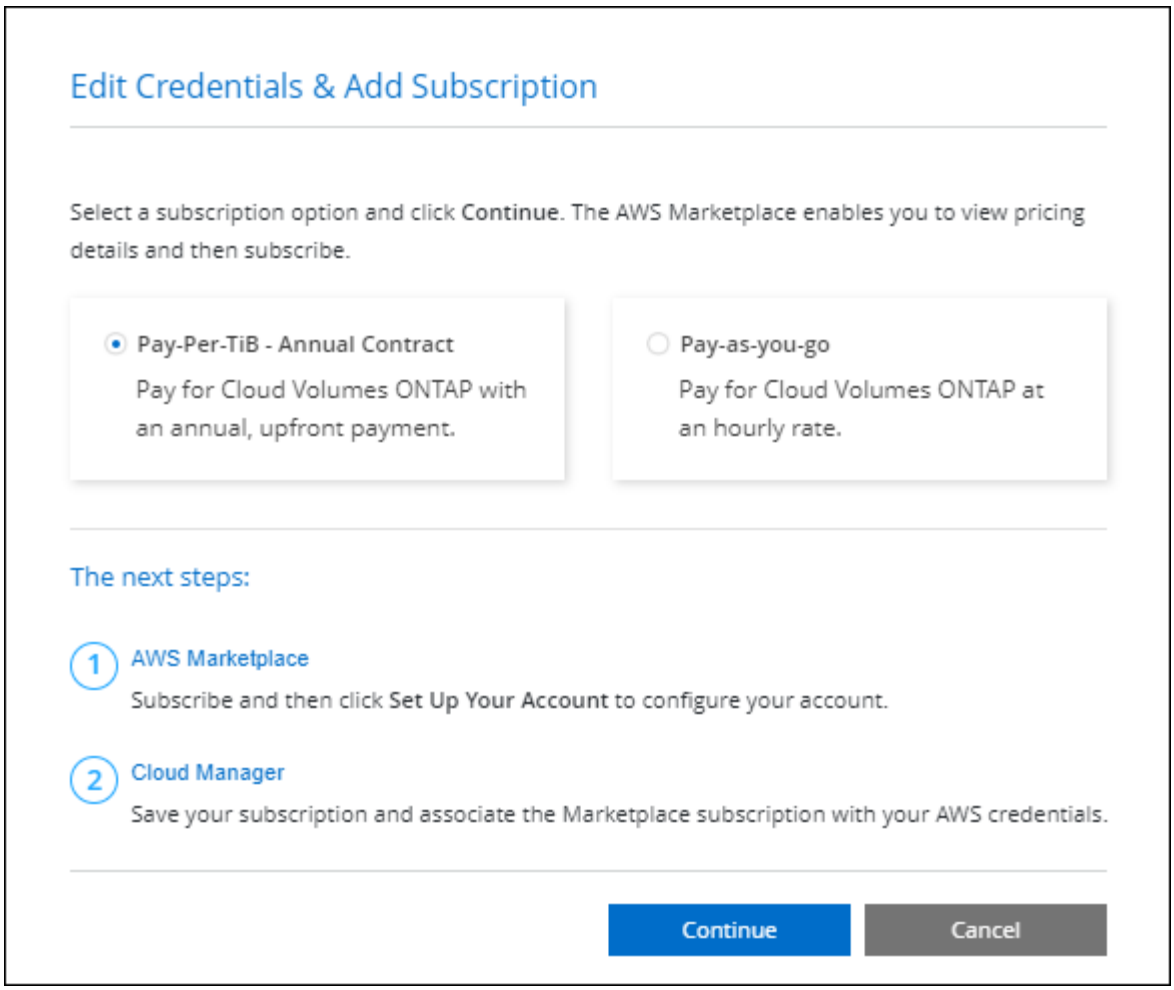
年間契約

クラウド プロバイダーのマーケットプレイスから年間契約を購入して、毎年支払います。

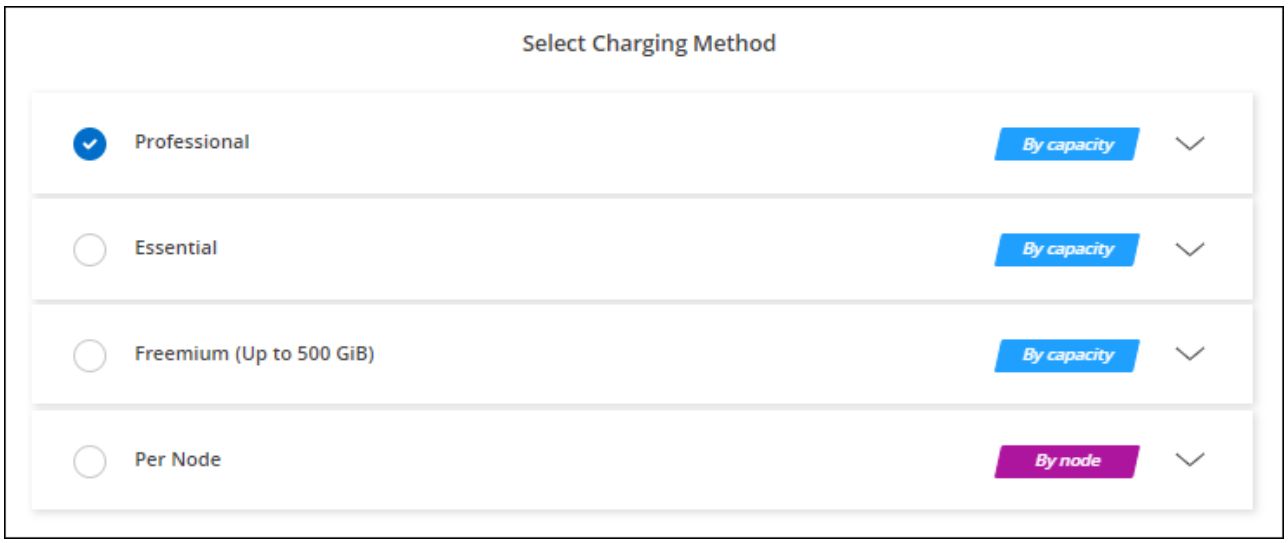
時間単位のサブスクリプションと同様に、コンソールでは、AWS Marketplace で利用可能な年間契約にサブスクライブするように求められます。

手順

1. *システム*ページで*システムの追加*をクリックし、手順に従います。
   a. *詳細と認証情報*ページで、*認証情報の編集 > 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. コンソールに戻ったら、課金方法ページにアクセスして容量ベースのパッケージを選択します。



"AWS でCloud Volumes ONTAP を起動するための手順をご覧ください" 。

Keystoneサブスクリプション

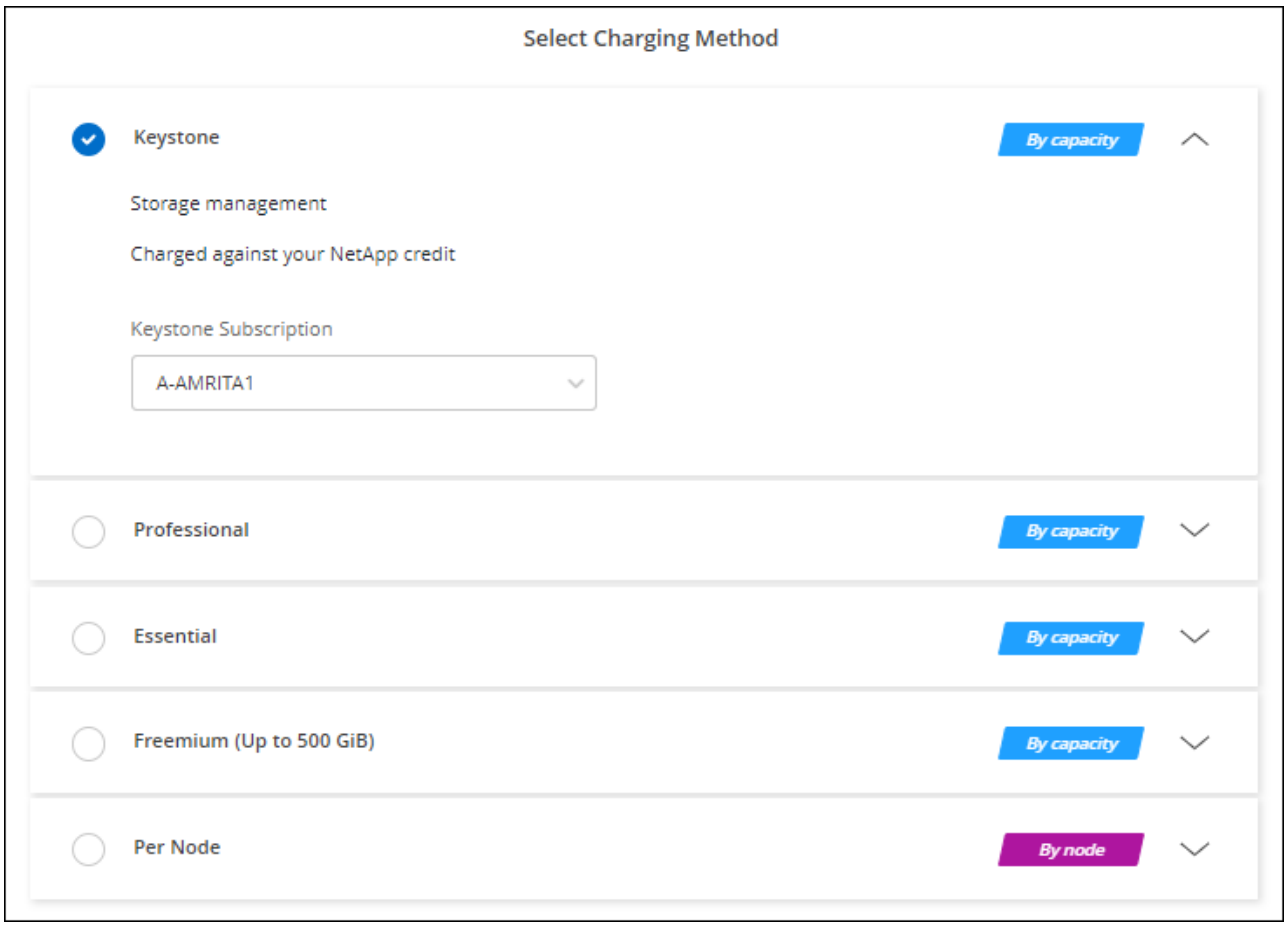
Keystoneサブスクリプションは、成長に応じて支払うサブスクリプション ベースのサービスです。"NetApp

Keystoneサブスクリプションの詳細" 。

手順

1. まだ購読していない場合は、 "ネットアップに連絡"
2. NetAppに問い合わせ して、1 つ以上のKeystoneサブスクリプションでユーザー アカウントを承認してください。
3. NetAppがアカウントを承認すると、"Cloud Volumes ONTAPで使用するためにサブスクリプションをリンクします" 。
4. *システム*ページで*システムの追加*をクリックし、手順に従います。

    a. 課金方法を選択するように求められたら、 Keystoneサブスクリプションの課金方法を選択します。



"AWS でCloud Volumes ONTAP を起動するための手順をご覧ください" 。

ノードベースのライセンス

ノードベースライセンスは、Cloud Volumes ONTAPの旧世代ライセンスです。ノードベースライセンスはNetApp （BYOL）から取得でき、特定のケースに限りライセンス更新に利用できます。詳細については、以下を参照してください。

- "ノードベースライセンスの提供終了"
- "ノードベースライセンスの提供終了"

- "ノードベースのライセンスを容量ベースのライセンスに変換する"

クイックデプロイメントを使用して**AWS**に**Cloud Volumes ONTAP**をデプロイする

単一ノードと高可用性 (HA) 構成の両方に対して、クイック デプロイメント メソッドを使用して、AWS にCloud Volumes ONTAP をデプロイできます。この簡素化されたプロセスにより、高度な方法と比較して展開手順が削減されます。また、1 ページにデフォルト値を自動的に設定し、ナビゲーションを最小限に抑えることで、ワークフローがより明確になります。

開始する前に

NetApp Consoleから AWS にCloud Volumes ONTAPシステムを追加するには、以下が必要です。

- 稼働中のコンソール エージェント。
  - あなたは "プロジェクトまたはワークスペースに関連付けられたコンソールエージェント"。
  - "コンソールエージェントを常に実行しておく必要があります" 。
- 使用する構成を理解すること。

  構成を選択し、管理者から AWS ネットワーク情報を取得して準備しておく必要があります。詳細については、"Cloud Volumes ONTAP構成の計画" 。
- Cloud Volumes ONTAPのライセンスを設定するために必要なことを理解していること。

  "ライセンスの設定方法を学ぶ" 。
- CIFS 構成用の DNS および Active Directory。

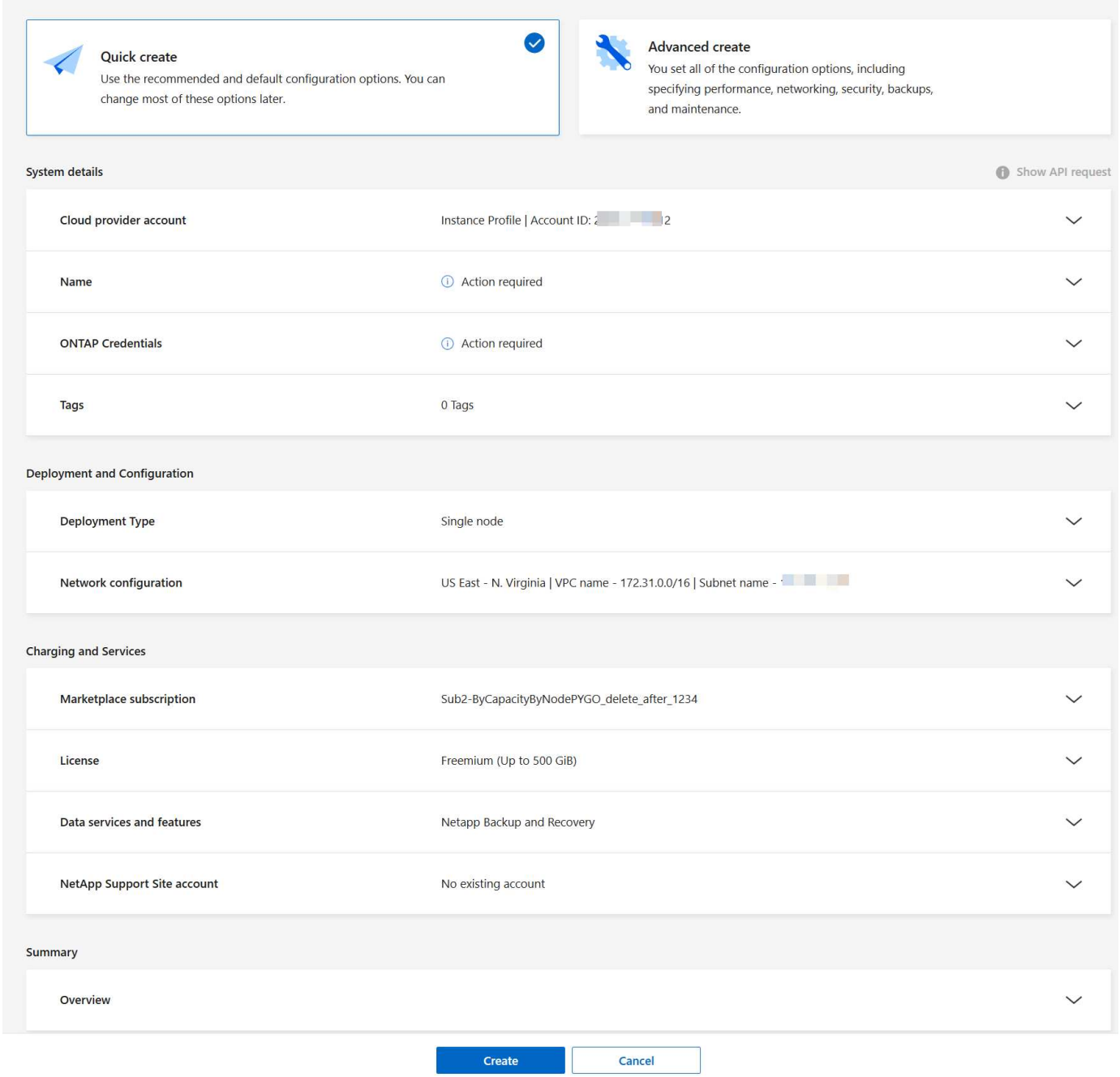
  詳細については、"AWS におけるCloud Volumes ONTAPのネットワーク要件" 。

タスク概要

Cloud Volumes ONTAPシステムを作成するとすぐに、 NetApp Console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。成功した場合、コンソールは直ちにインスタンスを終了し、システムの展開を開始します。コンソールが接続を確認できない場合、システム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 VPC テナンシーの場合)。

手順

1. 左側のナビゲーション メニューから、ストレージ > 管理 を選択します。
2. Canvas ページで、[システムの追加] をクリックし、指示に従います。
3. **Amazon Web Services** > * Cloud Volumes ONTAP* > *新規追加*を選択します。デフォルトでは*クイック作成*オプションが選択されています。



システムの詳細

1. クラウド プロバイダー アカウント: アカウントの詳細は、選択したコンソール エージェントに基づいて自動的に入力されます。複数のアカウントをお持ちの場合は、使用するアカウントを選択してください。コンソールエージェントが利用できない場合は、 "コンソールエージェントを作成する" 。
2. 名前: システム名。コンソールは、システム (クラスター) 名を使用して、 Cloud Volumes ONTAPシステムと Amazon EC2 インスタンスに名前を付けます。このオプションを選択した場合、定義済みのセキュリティ グループのプレフィックスとしても名前が使用されます。
3. * ONTAP認証情報* これらは、Cloud Volumes ONTAPクラスター管理者アカウントの認証情報です。これらの資格情報を使用して、 ONTAP System Manager またはONTAP CLI を介してCloud Volumes ONTAPに接続できます。デフォルトの *admin* ユーザー名をそのまま使用することも、カスタム ユーザー名に変更することもできます。
4. タグ AWS タグは、AWS リソースのメタデータです。コンソールは、Cloud Volumes ONTAPインスタン

スと、インスタンスに関連付けられている各 AWS リソースにタグを追加します。 Cloud Volumes ONTAPシステムを作成するときに、ユーザー インターフェイスから最大 15 個のタグを追加でき、作成後にさらにタグを追加できます。システムを作成するときに、API ではタグが 4 つに制限されないことに注意してください。タグの詳細については、 "AWS ドキュメント: Amazon EC2 リソースのタグ付け" 。

展開と構成

1. デプロイメント タイプ: 使用するデプロイメント タイプ (単一ノード、単一の可用性ゾーン (AZ) での高可用性 (HA)、または複数の AZ での HA) を選択します。
2. ネットワーク設定: 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" 。
   a. **AWS** リージョン: デフォルトでは、サブネット リソースを持つ VPC を持つ関連クラウド アカウントのリージョンが選択されます。
   b. **VPC**: サブネットを持つ AWS リージョンの VPC を入力します。サブネットがない場合、VPC のデフォルト値が選択されます。
   c. サブネット: 単一ノードのデプロイメントまたは単一 AZ 内の HA デプロイメントの場合にのみ、VPC のサブネットを選択できます。

高可用性

HA 構成を選択した場合は、次の情報を入力します。

単一**AZ**の**HA**

1. メディエーター アクセス: メディエーター アクセス情報を指定します。メディエーターは、HA ペアの健全性を監視し、障害発生時にクォーラムを提供する別のインスタンスです。キーペア名を指定して、メディエーターインスタンスが AWS EC2 サービスに接続できるようにし、接続方法を選択します。

複数の**AZ**での**HA**

1. アベイラビリティゾーンとメディエーター: 各ノードとメディエーターのアベイラビリティゾーン (AZ) と、 Cloud Volumes ONTAP HA ペアを展開する対応するサブネットを選択します。
2. フローティング **IP**: 複数の AZ を選択した場合は、NFS および CIFS サービスとクラスターおよび SVM 管理のフローティング IP アドレスを指定します。 IP アドレスは、リージョン内のすべての 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、"複数の AZ におけるCloud Volumes ONTAP HA の AWS ネットワーク要件" 。
3. メディエーター アクセス: メディエーター アクセス情報を指定します。メディエーターは、HA ペアの健全性を監視し、障害発生時にクォーラムを提供する別のインスタンスです。キーペア名を指定して、メディエーターインスタンスが AWS EC2 サービスに接続できるようにし、接続方法を選択します。
4. 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ト テーブルを選択します。ルート テーブルが複数ある場合は、正しいルート テーブルを選択することが重要です。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くなる可能性があります。ルートテーブルの詳細については、 "AWS ドキュメント: ルートテーブル" 。

充電とサービス

1. マーケットプレイス サブスクリプション: このCloud Volumes ONTAPシステムで使用する AWS マーケットプレイス サブスクリプションを選択します。
2. ライセンス: このCloud Volumes ONTAPシステムで使用するライセンスの種類を選択します。

Professional、Essential、Premium のライセンスから選択できます。さまざまなライセンスの詳細については、以下を参照してください。"Cloud Volumes ONTAPライセンスについて学ぶ" 。

3. データ サービスと機能: Cloud Volumes ONTAPで使用しないサービスを有効のままにするか、無効にします。
   - "NetAppの分類について詳しくはこちら"
   - "NetApp Backup and Recoveryの詳細"
   - "Cloud Volumes ONTAPの WORM ストレージについて学ぶ"

     WORM とデータ階層化を利用する場合は、バックアップとリカバリを無効にし、バージョン 9.8 以降のCloud Volumes ONTAPシステムを展開する必要があります。

   - * NetAppサポート サイト アカウント*: 複数のアカウントがある場合は、使用するアカウントを選択します。

まとめ

入力した詳細を確認または編集し、「作成」をクリックします。

導入プロセスが完了したら、AWS クラウドポータルでシステムによって生成されたCloud Volumes ONTAP構成、特にシステムタグを変更しないでください。これらの構成に変更を加えると、予期しない動作やデータ損失が発生する可能性があります。

関連リンク

- "Cloud Volumes ONTAP構成の計画"
- "高度なデプロイメントを使用して AWS にCloud Volumes ONTAPをデプロイする"

AWSでCloud Volumes ONTAPを起動

Cloud Volumes ONTAP は、単一システム構成で、または AWS の HA ペアとして起動できます。この方法では、クイック デプロイメント メソッドよりも多くの構成オプションと柔軟性を備えた高度なデプロイメント エクスペリエンスが提供されます。

開始する前に

始める前に以下のものが必要です。

- 稼働中のコンソール エージェント。
  - あなたは "システムに関連付けられたコンソールエージェント"。
  - "コンソールエージェントを常に実行しておく必要があります" 。
- 使用する構成を理解すること。

  構成を選択し、管理者から AWS ネットワーク情報を取得して準備しておく必要があります。詳細については、"Cloud Volumes ONTAP構成の計画" 。

- Cloud Volumes ONTAPのライセンスを設定するために必要なことを理解していること。

  "ライセンスの設定方法を学ぶ" 。

- CIFS 構成用の DNS および Active Directory。

  詳細については、"AWS におけるCloud Volumes ONTAPのネットワーク要件" 。

AWS でシングルノードのCloud Volumes ONTAPシステムを起動する

AWS でCloud Volumes ONTAPを起動する場合は、 NetApp Consoleで新しいシステムを作成する必要があります。

タスク概要

システムを作成するとすぐに、コンソールは指定された VPC でテストインスタンスを起動して接続を確認します。成功した場合、コンソールはインスタンスを直ちに終了し、 Cloud Volumes ONTAPシステムのデプロイを開始します。接続を検証できない場合、システム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 VPC テナンシーの場合)。

手順

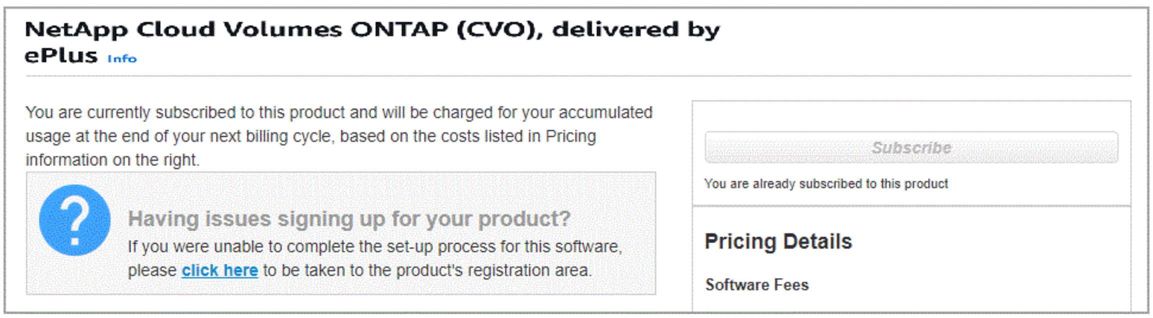
1. 左側のナビゲーション メニューから、ストレージ > 管理 を選択します。
2. *システム*ページで、*システムの追加*をクリックし、指示に従います。
3. **Amazon Web Services** と * Cloud Volumes ONTAP Single Node* を選択します。
4. *詳細作成*を選択します。デフォルトでは*クイック作成*モードが選択されているため、デフォルト値に関するメッセージが表示される場合があります。*続行*をクリックします。
5. プロンプトが表示されたら、 "コンソールエージェントを作成する" 。
6. 詳細と認証情報: オプションで AWS 認証情報とサブスクリプションを変更し、システム名を入力し、必要に応じてタグを追加して、パスワードを入力します。

   このページのいくつかのフィールドは説明不要です。次の表では、ガイダンスが必要になる可能性のあるフィールドについて説明します。

フィールド	説明
システム名	コンソールは、システム名を使用して、 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。このオプションを選択した場合、定義済みのセキュリティ グループのプレフィックスとしても名前が使用されます。
タグを追加する	AWS タグは、AWS リソースのメタデータです。コンソールは、Cloud Volumes ONTAPインスタンスと、インスタンスに関連付けられている各 AWS リソースにタグを追加します。システムを作成するときに、ユーザー インターフェイスから最大 4 つのタグを追加でき、システムの作成後にさらにタグを追加できます。システムを作成するときに、API ではタグが 4 つに制限されないことに注意してください。タグの詳細については、 "AWS ドキュメント: Amazon EC2 リソースのタグ付け" 。
ユーザ名とパスワード	これらは、Cloud Volumes ONTAPクラスター管理者アカウントの資格情報です。これらの資格情報を使用して、 ONTAP System Manager またはONTAP CLI を介してCloud Volumes ONTAPに接続できます。デフォルトの *admin* ユーザー名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。

フィールド	説明
資格情報の編集	このシステムをデプロイするアカウントに関連付けられている AWS 認証情報を選択します。このCloud Volumes ONTAPシステムで使用する AWS マーケットプレイス サブスクリプションを関連付けることもできます。「サブスクリプションを追加」をクリックすると、選択した認証情報が新しいAWSマーケットプレイスサブスクリプションに関連付けられます。サブスクリプションは年間契約または時間単位でCloud Volumes ONTAPをお支払いいただくことができます。NetApphttps://docs.netapp.com/us-en/bluexp-setup-admin/task-adding-aws-accounts.html["NetApp ConsoleにAWS認証情報を追加する方法を学びます"^] 。

複数の IAM ユーザーが同じ AWS アカウントで作業する場合は、各ユーザーがサブスクライブする必要があります。最初のユーザーがサブスクライブすると、AWS マーケットプレイスは、以下の画像に示すように、後続のユーザーにすでにサブスクライブしていることを通知します。 AWS アカウントにサブスクリプションが設定されている場合は、各 IAM ユーザーが自分自身をそのサブスクリプションに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コンソールの Web サイトに移動し、プロセスを完了してください。



7. サービス: サービスを有効のままにするか、 Cloud Volumes ONTAPで使用しない個々のサービスを無効にします。
   - "NetApp Data Classificationの詳細"
   - "NetApp Backup and Recoveryの詳細"

   WORM とデータ階層化を利用する場合は、バックアップとリカバリを無効にし、バージョン 9.8 以降のCloud Volumes ONTAPシステムを展開する必要があります。

8. 場所と接続: 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" 。

   次の表では、ガイダンスが必要になる可能性のあるフィールドについて説明します。

フィールド	説明
VPC	AWS Outpost がある場合は、Outpost VPC を選択して、その Outpost に単一ノードのCloud Volumes ONTAPシステムをデプロイできます。エクスペリエンスは、AWS にある他の VPC と同じです。

フィールド	説明
生成されたセキュリティグループ	コンソールでセキュリティ グループを生成させる場合は、トラフィックを許可する方法を選択する必要があります。 • 選択した **VPC** のみ を選択した場合、受信トラフィックのソースは、選択した VPC のサブネット範囲と、コンソール エージェントが存在する VPC のサブネット範囲になります。これは推奨されるオプションです。 • すべての **VPC** を選択した場合、受信トラフィックのソースは 0.0.0.0/0 IP 範囲になります。
既存のセキュリティグループを使用する	既存のファイアウォール ポリシーを使用する場合は、必要なルールが含まれていることを確認してください。"Cloud Volumes ONTAPのファイアウォールルールについて学ぶ" 。

9. データ暗号化: データ暗号化なし、または AWS 管理の暗号化を選択します。

   AWS 管理の暗号化の場合、自分のアカウントまたは別の AWS アカウントから別のカスタマーマスターキー (CMK) を選択できます。

   > Cloud Volumes ONTAPシステムを作成した後、AWS データ暗号化方法を変更することはできません。

   "Cloud Volumes ONTAP用の AWS KMS を設定する方法を学びます" 。

   "サポートされている暗号化技術の詳細" 。

10. 課金方法と **NSS** アカウント: このシステムで使用する課金オプションを指定し、 NetAppサポート サイト 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学ぶ" 。
    - "ライセンスの設定方法を学ぶ" 。

11. * Cloud Volumes ONTAP構成* (年間 AWS マーケットプレイス契約のみ): デフォルトの構成を確認して [続行] 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。

    デフォルト構成を維持する場合は、ボリュームを指定して、構成を確認して承認するだけです。

12. 事前構成済みパッケージ：いずれかのパッケージを選択してCloud Volumes ONTAP をすばやく起動するか、*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は、ボリュームを指定して構成を確認して承認するだけです。

13. **IAM** ロール: コンソールでロールを自動的に作成できるように、デフォルト オプションを維持するのが最適です。

    独自のポリシーを使用する場合は、次の条件を満たす必要があります。"Cloud Volumes ONTAPノードのポリシー要件" 。

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、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に対して新しいリリース候補、一般提供、またはパッチ リリースが利用可能な場合、コンソールはシステムの作成時にシステムをそのバージョンに更新します。たとえば、 Cloud Volumes ONTAP 9.13.1 を選択し、9.13.1 P4 が利用可能な場合は更新が行われます。更新は、あるリリースから別のリリース (たとえば、9.13 から 9.14) には行われません。

15. 基盤となるストレージ リソース: ディスク タイプを選択し、基盤となるストレージを構成し、データ階層化を有効のままにするかどうかを選択します。

    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 (およびアグリゲート) 用です。後続のボリューム (およびアグリゲート) には、異なるディスク タイプを選択できます。
    - gp3 または io1 ディスクを選択した場合、コンソールは AWS の Elastic Volumes 機能を使用して、必要に応じて基盤となるストレージ ディスク容量を自動的に増加します。ストレージのニーズに基づいて初期容量を選択し、 Cloud Volumes ONTAP の導入後に修正することができます。"AWS の Elastic Volumes のサポートについて詳しく見る" 。
    - gp2 または st1 ディスクを選択した場合は、初期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 オプションを使用するときにコンソールが作成する追加のアグリゲートのディスク サイズを選択できます。高度な割り当てオプションを使用して、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。
    - 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。
    - データ階層化を無効にした場合、後続の集約で有効にすることができます。

      "データ階層化の仕組みを学ぶ" 。

16. 書き込み速度と**WORM**:

    a. 必要に応じて、「通常」または「高速」の書き込み速度を選択します。

       "書き込み速度について詳しくはこちら" 。

    b. 必要に応じて、一度書き込み、何度も読み取り可能な (WORM) ストレージをアクティブ化します。

       Cloud Volumes ONTAPバージョン 9.7 以下でデータ階層化が有効になっている場合、WORM を有効にすることはできません。 WORM と階層化を有効にした後、 Cloud Volumes ONTAP 9.8 への復元またはダウングレードはブロックされます。

    "WORMストレージについて詳しくはこちら" 。

    a. WORM ストレージを有効にする場合は、保持期間を選択します。

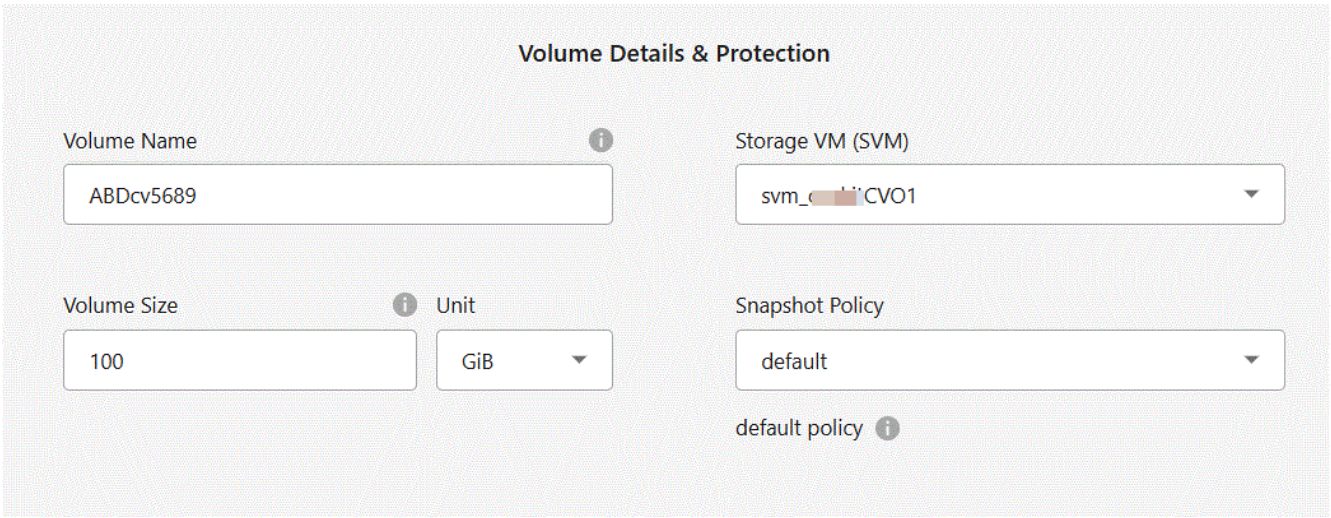
17. ボリュームの作成: 新しいボリュームの詳細を入力するか、[スキップ] をクリックします。

    "サポートされているクライアントプロトコルとバージョンについて学ぶ" 。

    このページのいくつかのフィールドは説明不要です。次の表では、ガイダンスが必要になる可能性のある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な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、コンソール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、ユーザーとグループの共有へのアクセス レベル (アクセス制御リストまたは ACL とも呼ばれます) を制御できます。ローカルまたはドメインの Windows ユーザーまたはグループ、あるいは UNIX ユーザーまたはグループを指定できます。ドメイン Windows ユーザー名を指定する場合は、domain\username の形式を使用してユーザーのドメインを含める必要があります。
スナップショットポリシー	スナップショット コピー ポリシーは、自動的に作成されるNetAppスナップショット コピーの頻度と数を指定します。NetAppスナップショット コピーは、パフォーマンスに影響を与えず、最小限のストレージしか必要としない、ポイントインタイム ファイル システム イメージです。デフォルトのポリシーを選択するか、ポリシーなしを選択できます。一時データの場合は none を選択できます (例: Microsoft SQL Server の場合は tempdb)。
詳細オプション（NFSのみ）	ボリュームの NFS バージョン (NFSv3 または NFSv4) を選択します。
イニシエーター 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供されます。イニシエーター グループは、iSCSI ホスト ノード名のテーブルであり、どのイニシエーターがどの 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 Ethernet ネットワーク アダプター (NIC)、ソフトウェア イニシエーターを備えた TCP オフロード エンジン (TOE) カード、統合ネットワーク アダプター (CNA)、または専用ホスト バス アダプター (HBA) を介してネットワークに接続し、iSCSI 修飾名 (IQN) によって識別されます。 iSCSI ボリュームを作成すると、コンソールによって LUN が自動的に作成されます。ボリュームごとに 1 つの LUN を作成するだけで簡単になるので、管理は不要です。ボリュームを作成したら、"IQNを使用してホストからLUNに接続します" 。

次の画像は、ボリューム作成ウィザードの最初のページを示しています。



18. **CIFS** セットアップ: CIFS プロトコルを選択した場合は、CIFS サーバー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 サーバーの名前解決を提供する DNS サーバーの IP アドレス。これらのDNSサーバには、Active DirectoryのLDAPサーバと、CIFSサーバが参加するドメインのドメイン コントローラを見つけるために必要なサービス 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 サーバーが参加する Active Directory (AD) ドメインの FQDN。
ドメインへの参加を許可された資格情報	AD ドメイン内の指定された組織単位 (OU) にコンピューターを追加するのに十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS server NetBIOS name	AD ドメイン内で一意の CIFS サーバー名。
組織単位	CIFS サーバーに関連付ける 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 サーバーとして設定する場合は、このフィールドに **OU=Computers,OU=corp** と入力する必要があります。
DNSドメイン	Cloud Volumes ONTAPストレージ仮想マシン (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 サーバーを構成するには、「**Active Directory** ドメインを使用する」を選択します。別のアドレスを使用して NTP サーバーを構成する必要がある場合は、API を使用する必要があります。参照 "NetApp Console自動化ドキュメント"詳細については。 NTP サーバーを設定できるのは、CIFS サーバーを作成するときだけであることに注意してください。 CIFS サーバーを作成した後は構成できません。

19. 使用プロファイル、ディスク タイプ、階層化ポリシー: ストレージ効率機能を有効にするかどうかを選択し、必要に応じて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、"ボリューム使用プロファイルの理解" 、"データ階層化の概要" 、 そして "KB: CVO ではどのようなインライン ストレージ効率機能がサポートされていますか?"

20. 確認と承認: 選択内容を確認して確定します。
    a. 構成の詳細を確認します。
    b. 詳細情報 をクリックすると、サポートとコンソールが購入する AWS リソースの詳細を確認できます。
    c. 理解しました... チェックボックスを選択します。
    d. [Go] をクリックします。

結果

コンソールはCloud Volumes ONTAPインスタンスを起動します。 *監査*ページで進捗状況を追跡できます。

Cloud Volumes ONTAPインスタンスの起動で問題が発生した場合は、失敗メッセージを確認してください。システムを選択して、「環境の再作成」をクリックすることもできます。

さらに詳しいヘルプについては、 "NetApp Cloud Volumes ONTAPサポート" 。

導入プロセスが完了したら、AWS クラウドポータルでシステムによって生成されたCloud Volumes ONTAP構成、特にシステムタグを変更しないでください。これらの構成に変更を加えると、予期しない動作やデータ損失が発生する可能性があります。

終了後の操作

- 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、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てください。
- ボリュームにクォータを適用する場合は、 ONTAP System Manager またはONTAP CLI を使用します。

  クォータを使用すると、ユーザー、グループ、または qtree が使用するディスク領域とファイル数を制限したり追跡したりできます。

AWSでCloud Volumes ONTAP HAペアを起動する

AWS でCloud Volumes ONTAP HA ペアを起動する場合は、コンソールで HA システムを作成する必要があります。

制限

現時点では、HA ペアは AWS Outposts ではサポートされていません。

タスク概要

Cloud Volumes ONTAPシステムを作成するとすぐに、コンソールは指定された VPC でテストインスタンスを起動して接続を確認します。成功した場合、コンソールはインスタンスを直ちに終了し、 Cloud Volumes ONTAPシステムのデプロイを開始します。接続を検証できない場合、システム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 VPC テナンシーの場合)。

手順

1. 左側のナビゲーション メニューから、ストレージ > 管理 を選択します。
2. *システム*ページで*システムの追加*をクリックし、指示に従います。
3. **Amazon Web Services** と * Cloud Volumes ONTAP HA* を選択します。

   いくつかの AWS ローカルゾーンが利用可能です。

   AWS Local Zones を使用する前に、Local Zones を有効にし、AWS アカウントの Local Zone にサブネットを作成する必要があります。 AWSローカルゾーンにオプトインする*とAmazon VPCをローカルゾーンに拡張する*の手順に従ってください。"AWS チュートリアル「AWS ローカルゾーンを使用した低レイテンシーアプリケーションのデプロイ開始」" 。

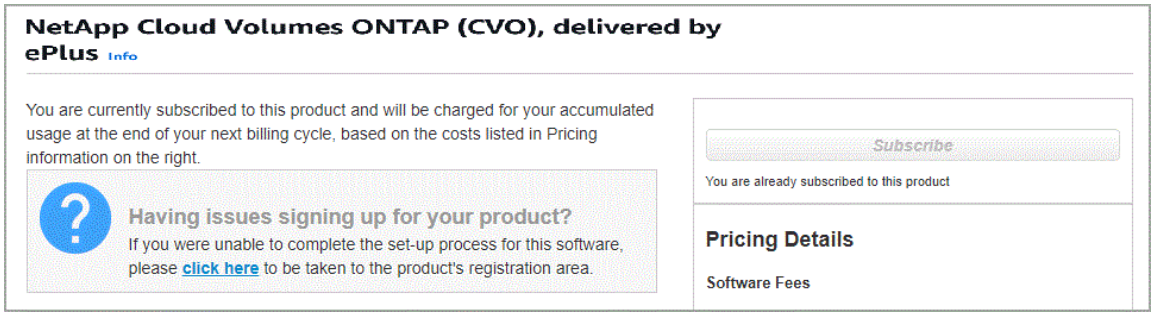
   コンソールエージェント3.9.36以前を実行している場合は、 `DescribeAvailabilityZones` AWS EC2 コンソールの AWS ロールへの権限。

4. 詳細と認証情報: オプションで AWS 認証情報とサブスクリプションを変更し、システム名を入力し、必要に応じてタグを追加して、パスワードを入力します。

   このページのいくつかのフィールドは説明不要です。次の表では、ガイダンスが必要になる可能性のあるフィールドについて説明します。

フィールド	説明
システム名	コンソールは、システム名を使用して、 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。このオプションを選択した場合、定義済みのセキュリティ グループのプレフィックスとしても名前が使用されます。
タグを追加する	AWS タグは、AWS リソースのメタデータです。コンソールは、Cloud Volumes ONTAPインスタンスと、インスタンスに関連付けられている各 AWS リソースにタグを追加します。システムを作成するときに、ユーザー インターフェイスから最大 4 つのタグを追加でき、システムの作成後にさらにタグを追加できます。システムを作成するときに、API ではタグが 4 つに制限されないことに注意してください。タグの詳細については、 "AWS ドキュメント: Amazon EC2 リソースのタグ付け" 。
ユーザ名とパスワード	これらは、Cloud Volumes ONTAPクラスター管理者アカウントの資格情報です。これらの資格情報を使用して、 ONTAP System Manager またはONTAP CLI を介してCloud Volumes ONTAPに接続できます。デフォルトの *admin* ユーザー名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。
資格情報の編集	このCloud Volumes ONTAPシステムで使用するAWS認証情報とマーケットプレイスサブスクリプションを選択してください。「サブスクリプションを追加」をクリックすると、選択した認証情報が新しいAWSマーケットプレイスサブスクリプションに関連付けられます。サブスクリプションは年間契約または時間単位でCloud Volumes ONTAPをお支払いいただくことができます。NetAppから直接ライセンスを購入された場合（ NetApp （Bring Your Own License）） 、AWSサブスクリプションは不要です。NetAppはBYOLライセンスの購入、延長、および更新を制限しています。 "Cloud Volumes ONTAP の BYOL ライセンスの利用制限" 。https://docs.netapp.com/us-en/bluexp-setup-admin/task-adding-aws-accounts.html["コンソールにAWS認証情報を追加する方法を学びます"^] 。

複数の IAM ユーザーが同じ AWS アカウントで作業する場合は、各ユーザーがサブスクライブする必要があります。最初のユーザーがサブスクライブすると、AWS マーケットプレイスは、以下の画像に示すように、後続のユーザーにすでにサブスクライブしていることを通知します。 AWS アカウントにサブスクリプションが設定されている場合は、各 IAM ユーザーが自分自身をそのサブスクリプションに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コンソールの Web サイトに移動し、プロセスを完了してくださ
い。



5. サービス: サービスを有効のままにするか、このCloud Volumes ONTAPシステムで使用しない個々のサービスを無効にします。
   - "NetApp Data Classificationの詳細"

◦ "バックアップとリカバリの詳細"

WORM とデータ階層化を利用する場合は、バックアップとリカバリを無効にし、バージョン 9.8 以降のCloud Volumes ONTAPシステムを展開する必要があります。

6. **HA** 展開モデル: HA 構成を選択します。

   展開モデルの概要については、以下を参照してください。"AWS 向けCloud Volumes ONTAP HA" 。

7. 場所と接続 (単一のアベイラビリティーゾーン (AZ)) または リージョンと **VPC** (複数の AZ): 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。

   次の表では、ガイダンスが必要になる可能性のあるフィールドについて説明します。

フィールド	説明
生成されたセキュリティグループ	コンソールでセキュリティ グループを生成させる場合は、トラフィックを許可する方法を選択する必要があります。 • 選択した **VPC** のみ を選択した場合、受信トラフィックのソースは、選択した VPC のサブネット範囲と、コンソール エージェントが存在する VPC のサブネット範囲になります。これは推奨されるオプションです。 • すべての **VPC** を選択した場合、受信トラフィックのソースは 0.0.0.0/0 IP 範囲になります。
既存のセキュリティグループを使用する	既存のファイアウォール ポリシーを使用する場合は、必要なルールが含まれていることを確認してください。"Cloud Volumes ONTAPのファイアウォールルールについて学ぶ" 。

8. 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。
9. 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、リージョン内のすべての 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、"複数の AZ におけるCloud Volumes ONTAP HA の AWS ネットワーク要件" 。

10. 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めるルートテーブルを選択します。

    ルート テーブルが複数ある場合は、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くなる可能性があります。ルートテーブルの詳細については、 "AWS ドキュメント: ルートテーブル" 。

11. データ暗号化: データ暗号化なし、または AWS 管理の暗号化を選択します。

    AWS 管理の暗号化の場合、自分のアカウントまたは別の AWS アカウントから別のカスタマーマスターキー (CMK) を選択できます。

    Cloud Volumes ONTAPシステムを作成した後、AWS データ暗号化方法を変更することはできません。

    "Cloud Volumes ONTAP用の AWS KMS を設定する方法を学びます" 。

"サポートされている暗号化技術の詳細" 。

12. 課金方法と **NSS** アカウント: このシステムで使用する課金オプションを指定し、 NetAppサポート サイト 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学ぶ" 。
    - "ライセンスの設定方法を学ぶ" 。
13. * Cloud Volumes ONTAP構成* (年間 AWS Marketplace 契約のみ): デフォルトの構成を確認して [続行] 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。

    デフォルト構成を維持する場合は、ボリュームを指定して、構成を確認して承認するだけです。
14. 事前構成済みパッケージ（時間単位またはBYOLのみ）：いずれかのパッケージを選択してCloud Volumes ONTAPをすばやく起動するか、*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は、ボリュームを指定して構成を確認して承認するだけです。
15. **IAM** ロール: コンソールでロールを自動的に作成できるように、デフォルト オプションを維持するのが最適です。

    独自のポリシーを使用する場合は、次の条件を満たす必要があります。"Cloud Volumes ONTAPノードとHAメディエーターのポリシー要件" 。
16. 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に対して新しいリリース候補、一般提供、またはパッチ リリースが利用可能な場合、コンソールはシステムの作成時にシステムをそのバージョンに更新します。たとえば、 Cloud Volumes ONTAP 9.13.1 を選択し、9.13.1 P4 が利用可能な場合は更新が行われます。更新は、あるリリースから別のリリース (たとえば、9.13 から 9.14) には行われません。
17. 基盤となるストレージ リソース: ディスク タイプを選択し、基盤となるストレージを構成し、データ階層化を有効のままにするかどうかを選択します。

    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 (およびアグリゲート) 用です。後続のボリューム (およびアグリゲート) には、異なるディスク タイプを選択できます。
    - gp3 または io1 ディスクを選択した場合、コンソールは AWS の Elastic Volumes 機能を使用して、必要に応じて基盤となるストレージ ディスク容量を自動的に増加します。ストレージのニーズに基づいて初期容量を選択し、 Cloud Volumes ONTAP の導入後に修正することができます。"AWS の Elastic Volumes のサポートについて詳しく見る" 。
    - gp2 または st1 ディスクを選択した場合は、初期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 オプションを使用するときにコンソールが作成する追加のアグリゲートのディスク サイズを選択できます。高度な割り当てオプションを使用して、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。
    - 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。
    - データ階層化を無効にした場合、後続の集約で有効にすることができます。

"データ階層化の仕組みを学ぶ" 。

18. 書き込み速度と**WORM**:

    a. 必要に応じて、「通常」または「高速」の書き込み速度を選択します。

    "書き込み速度について詳しくはこちら" 。

    b. 必要に応じて、一度書き込み、何度も読み取り可能な (WORM) ストレージをアクティブ化します。

    Cloud Volumes ONTAPバージョン 9.7 以下でデータ階層化が有効になっている場合、WORM を有効にすることはできません。 WORM と階層化を有効にした後、 Cloud Volumes ONTAP 9.8 への復元またはダウングレードはブロックされます。

"WORMストレージについて詳しくはこちら" 。

    a. WORM ストレージを有効にする場合は、保持期間を選択します。

19. 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。

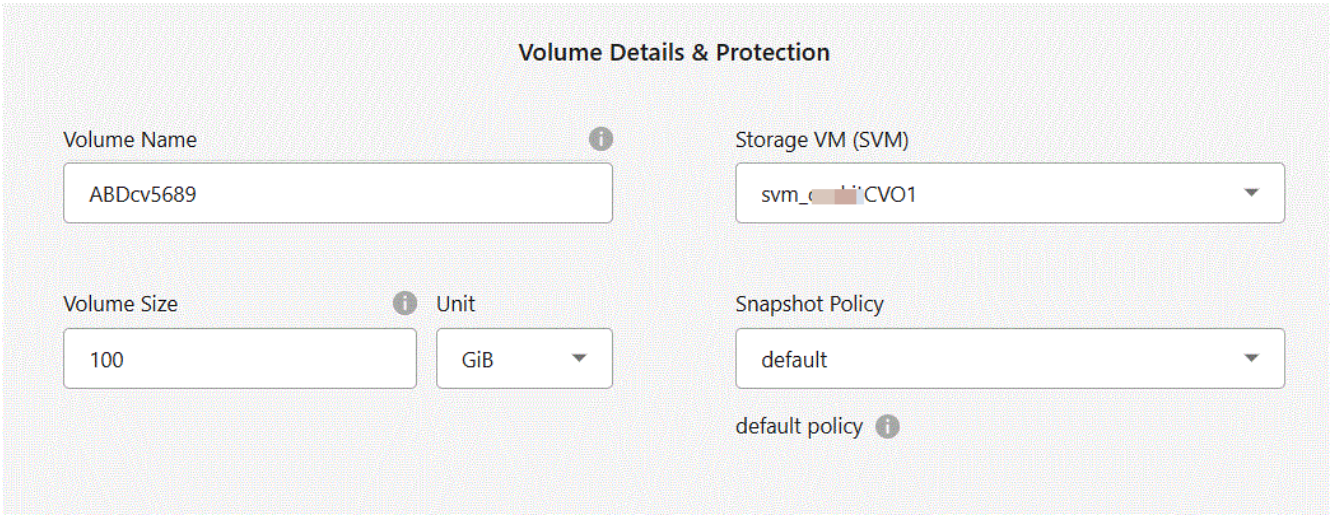
"サポートされているクライアントプロトコルとバージョンについて学ぶ" 。

このページのいくつかのフィールドは説明不要です。次の表では、ガイダンスが必要になる可能性のある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な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、コンソール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、ユーザーとグループの共有へのアクセス レベル (アクセス制御リストまたは ACL とも呼ばれます) を制御できます。ローカルまたはドメインの Windows ユーザーまたはグループ、あるいは UNIX ユーザーまたはグループを指定できます。ドメイン Windows ユーザー名を指定する場合は、domain\username の形式を使用してユーザーのドメインを含める必要があります。
スナップショットポリシー	スナップショット コピー ポリシーは、自動的に作成されるNetAppスナップショット コピーの頻度と数を指定します。NetAppスナップショット コピーは、パフォーマンスに影響を与えず、最小限のストレージしか必要としない、ポイントインタイム ファイル システム イメージです。デフォルトのポリシーを選択するか、ポリシーなしを選択できます。一時データの場合は none を選択できます (例: Microsoft SQL Server の場合は tempdb)。
詳細オプション（NFSのみ）	ボリュームの NFS バージョン (NFSv3 または NFSv4) を選択します。

フィールド	説明
イニシエーター 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供されます。イニシエーター グループは、iSCSI ホスト ノード名のテーブルであり、どのイニシエーターがどの 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 Ethernet ネットワーク アダプター (NIC)、ソフトウェア イニシエーターを備えた TCP オフロード エンジン (TOE) カード、統合ネットワーク アダプター (CNA)、または専用ホスト バス アダプター (HBA) を介してネットワークに接続し、iSCSI 修飾名 (IQN) によって識別されます。 iSCSI ボリュームを作成すると、コンソールによって LUN が自動的に作成されます。ボリュームごとに 1 つの LUN を作成するだけで簡単になるので、管理は不要です。ボリュームを作成したら、"IQNを使用してホストからLUNに接続します" 。

次の画像は、ボリューム作成ウィザードの最初のページを示しています。



20. **CIFS** セットアップ: CIFS プロトコルを選択した場合は、CIFS サーバー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 サーバーの名前解決を提供する DNS サーバーの IP アドレス。これらのDNSサーバには、Active DirectoryのLDAPサーバと、CIFSサーバが参加するドメインのドメイン コントローラを見つけるために必要なサービス 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 サーバーが参加する Active Directory (AD) ドメインの FQDN。
ドメインへの参加を許可された資格情報	AD ドメイン内の指定された組織単位 (OU) にコンピューターを追加するのに十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS server NetBIOS name	AD ドメイン内で一意の CIFS サーバー名。
組織単位	CIFS サーバーに関連付ける 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 サーバーとして設定する場合は、このフィールドに **OU=Computers,OU=corp** と入力する必要があります。

フィールド	説明
DNSドメイン	Cloud Volumes ONTAPストレージ仮想マシン (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 サーバーを構成するには、「**Active Directory** ドメインを使用する」を選択します。別のアドレスを使用して NTP サーバーを構成する必要がある場合は、API を使用する必要があります。参照 "NetApp Console自動化ドキュメント"詳細については。 NTP サーバーを設定できるのは、CIFS サーバーを作成するときだけであることに注意してください。 CIFS サーバーを作成した後は構成できません。

21. 使用プロファイル、ディスク タイプ、階層化ポリシー: ストレージ効率機能を有効にするかどうかを選択し、必要に応じて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、"ボリューム使用プロファイルを選択する"そして"データ階層化の概要"。

22. 確認と承認: 選択内容を確認して確定します。
    a. 構成の詳細を確認します。
    b. 詳細情報 をクリックすると、サポートとコンソールが購入する AWS リソースの詳細を確認できます。
    c. 理解しました... チェックボックスを選択します。
    d. [Go] をクリックします。

結果

コンソールはCloud Volumes ONTAP HA ペアを起動します。 *監査*ページで進捗状況を追跡できます。

HA ペアの起動時に問題が発生した場合は、失敗メッセージを確認してください。システムを選択して、「環境の再作成」をクリックすることもできます。

さらに詳しいヘルプについては、 "NetApp Cloud Volumes ONTAPサポート" 。

終了後の操作

- 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、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てください。
- ボリュームにクォータを適用する場合は、 ONTAP System Manager またはONTAP CLI を使用します。

  クォータを使用すると、ユーザー、グループ、または qtree が使用するディスク領域とファイル数を制限したり追跡したりできます。

> 導入プロセスが完了したら、AWS クラウドポータルでシステムによって生成されたCloud Volumes ONTAP構成、特にシステムタグを変更しないでください。これらの構成に変更を加えると、予期しない動作やデータ損失が発生する可能性があります。

関連リンク

- "Cloud Volumes ONTAP構成の計画"
- "クイックデプロイメントを使用してAWSにCloud Volumes ONTAPをデプロイする"

AWS Secret Cloud または AWS Top Secret Cloud にCloud Volumes ONTAP を導入する

標準のAWSリージョンと同様に、 NetApp Consoleは"AWS シークレットクラウド"そして"AWSトップシークレットクラウド"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するCloud Volumes ONTAPを導入します。 AWS Secret Cloud と Top Secret Cloud は、米国インテリジェンスコミュニティに固有のクローズドリージョンです。このページの手順は、AWS Secret Cloud および Top Secret Cloud リージョンのユーザーにのみ適用されます。

開始する前に

始める前に、AWS Secret Cloud と Top Secret Cloud でサポートされているバージョンを確認し、コンソールのプライベートモードについて学んでください。

- AWS Secret Cloud および Top Secret Cloud でサポートされている次のバージョンを確認します。
  - Cloud Volumes ONTAP 9.12.1 P2
  - コンソールエージェントのバージョン3.9.32

    AWS でCloud Volumes ONTAP をデプロイおよび管理するには、コンソール エージェントが必要です。コンソール エージェントのインスタンスにインストールされるソフトウェアからコンソールにログインします。コンソールの SaaS ウェブサイトは、AWS Secret Cloud および Top Secret Cloud ではサポートされていません。
- プライベートモードについて学ぶ

  AWS Secret Cloud および Top Secret Cloud では、コンソールは プライベート モード で動作します。プライベート モードでは、コンソールから SaaS レイヤーに接続できません。コンソール エージェントにアクセスできるローカルの Web ベースのアプリケーションを通じてコンソールにアクセスできます。

  プライベートモードの仕組みの詳細については、以下を参照してください。"コンソールのプライベート展開モード" 。

ステップ**1:** ネットワークを設定する

Cloud Volumes ONTAP が適切に動作するように AWS ネットワークを設定します。

手順

1. コンソール エージェントのインスタンスと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 とサブネットがコンソール エージェントと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. Amazon Simple Storage Service（Amazon S3）サービスへのVPCエンドポイントを設定します。

   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。

ステップ**2:** 権限を設定する

AWS Secret Cloud または Top Secret Cloud でアクションを実行するために必要な権限をコンソールエージェントとCloud Volumes ONTAP に付与する IAM ポリシーとロールを設定します。

次のそれぞれに対して IAM ポリシーと IAM ロールが必要です。

- コンソールエージェントのインスタンス
- Cloud Volumes ONTAPインスタンス
- HAペアの場合、 Cloud Volumes ONTAP HAメディエーターインスタンス（HAペアを展開する場合）

手順

1. AWS IAM コンソールに移動し、*ポリシー*をクリックします。
2. コンソール エージェントのインスタンスのポリシーを作成します。

> これらのポリシーは、AWS 環境内の S3 バケットをサポートするために作成します。後でバケットを作成するときに、バケット名に接頭辞が付けられていることを確認してください。 `fabric-pool-` 。この要件は、AWS Secret Cloud リージョンと Top Secret Cloud リージョンの両方に適用されます。

秘密の地域

```
{
    "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-b: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-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

極秘地域

```
{
    "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。

秘密の地域

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

極秘地域

```
{
    "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"
    }]
}
```

HA ペアの場合、 Cloud Volumes ONTAP HA ペアを展開する予定であれば、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": "*"
        }
    ]
}
```

4. ロールタイプが 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アタッチします。

   ロールを作成します。

   ポリシーと同様に、コンソール エージェント用に IAM ロールを 1 つ、 Cloud Volumes ONTAPノード用に IAM ロールを 1 つ用意する必要があります。 HA ペアの場合: ポリシーと同様に、コンソール エージェント用に 1 つの IAM ロール、 Cloud Volumes ONTAPノード用に 1 つ、HA メディエーター用に 1 つ (HA ペアを展開する場合) の IAM ロールが必要です。

   役割を選択してください:

   コンソール エージェントのインスタンスを起動するときに、コンソール エージェントの IAM ロールを選択する必要があります。コンソールからCloud Volumes ONTAPシステムを作成するときに、 Cloud Volumes ONTAPの IAM ロールを選択できます。 HA ペアの場合、 Cloud Volumes ONTAPシステムを作成するときに、 Cloud Volumes ONTAPと HA メディエーターの IAM ロールを選択できます。

ステップ**3: AWS KMS**を設定する

Cloud Volumes ONTAPで Amazon 暗号化を使用する場合は、AWS Key Management Service (KMS) の要件が満たされていることを確認してください。

手順

1. 自分のアカウントまたは別の AWS アカウントに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します。

   CMK は、AWS 管理の CMK またはカスタマー管理の CMK にすることができます。

2. CMK が、 Cloud Volumes ONTAPをデプロイする予定のアカウントとは別の AWS アカウントにある場合は、そのキーの ARN を取得する必要があります。

Cloud Volumes ONTAPシステムを作成するときは、コンソールに ARN を提供する必要があります。

3. インスタンスの IAM ロールを CMK のキーユーザーのリストに追加します。

   これにより、コンソールにCloud Volumes ONTAPで CMK を使用する権限が付与されます。

ステップ**4:** コンソールエージェントをインストールしてコンソールを設定する

コンソールを使用して AWS にCloud Volumes ONTAPをデプロイする前に、コンソール エージェントをインストールしてセットアップする必要があります。これにより、コンソールはパブリック クラウド環境 (Cloud Volumes ONTAPを含む) 内のリソースとプロセスを管理できるようになります。

手順

1. Privacy Enhanced Mail (PEM) Base-64 エンコード X.509 形式で証明機関 (CA) によって署名されたルート証明書を取得します。証明書を取得するための組織のポリシーと手順を参照してください。

   > AWS Secret Cloudリージョンの場合は、 `NSS Root CA 2`証明書、そしてTop Secret Cloud の場合は、 `Amazon Root CA 4`証明書。チェーン全体ではなく、これらの証明書のみをアップロードするようにしてください。証明書チェーンのファイルは大きいため、アップロードが失敗する可能性があります。追加の証明書がある場合は、次の手順で説明するように後でアップロードできます。

   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。コンソールは、HTTPS 経由で AWS にリクエストを送信するときに、信頼された証明書を使用します。

2. コンソール エージェントのインスタンスを起動します。
   a. コンソールの AWS Intelligence Community Marketplace ページに移動します。
   b. [カスタム起動] 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. 指示に従ってインスタンスを構成します。

      インスタンスを構成する際には、次の点に注意してください。

      - t3.xlarge をお勧めします。
      - 権限を設定するときに作成した 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 オプションを維持する必要があります。
      - コンソール エージェントに必要な接続方法は、SSH、HTTP、および HTTPS です。
3. インスタンスに接続しているホストからコンソールを設定します。
   a. ウェブブラウザを開いて入力してください https://ipaddressここで、ipaddress は、コンソール エージェントをインストールした Linux ホストの IP アドレスです。
   b. AWS サービスへの接続用のプロキシサーバーを指定します。
   c. 手順 1 で取得した証明書をアップロードします。
   d. 指示に従って新しいシステムをセットアップします。
      - システムの詳細: コンソール エージェントの名前と会社名を入力します。

- 管理者ユーザーの作成: システムの管理者ユーザーを作成します。

  このユーザー アカウントはシステム上でローカルに実行されます。コンソール経由で利用できる auth0 サービスへの接続がありません。

- 確認: 詳細を確認し、ライセンス契約に同意して、[セットアップ] を選択します。

e. CA 署名証明書のインストールを完了するには、EC2 コンソールからコンソールエージェントインスタンスを再起動します。

4. コンソール エージェントが再起動したら、セットアップ ウィザードで作成した管理者ユーザー アカウントを使用してログインします。

ステップ**5: (**オプション**)** プライベートモード証明書をインストールする

この手順は、AWS Secret Cloud および Top Secret Cloud リージョンではオプションであり、前の手順でインストールしたルート証明書とは別に追加の証明書がある場合にのみ必要です。

手順

1. 既存のインストールされている証明書を一覧表示します。

   a. occm コンテナの docker ID (識別名「ds-occm-1」) を収集するには、次のコマンドを実行します。

   ```
   docker ps
   ```

   b. occm コンテナ内に入るには、次のコマンドを実行します。

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   c. 「TRUST_STORE_PASSWORD」環境変数からパスワードを収集するには、次のコマンドを実行します。

   ```
   env
   ```

   d. トラストストアにインストールされているすべての証明書を一覧表示するには、次のコマンドを実行し、前の手順で収集したパスワードを使用します。

   ```
   keytool -list -v -keystore occm.truststore
   ```

2. 証明書を追加します。

   a. occm コンテナの docker ID (識別名「ds-occm-1」) を収集するには、次のコマンドを実行します。

   ```
   docker ps
   ```

   b. occm コンテナ内に入るには、次のコマンドを実行します。

```
docker exec -it <docker-id> /bin/sh
```

新しい証明書ファイルを内部に保存します。

c. 「TRUST_STORE_PASSWORD」環境変数からパスワードを収集するには、次のコマンドを実行します。

```
env
```

d. 証明書をトラストストアに追加するには、次のコマンドを実行し、前の手順のパスワードを使用します。

```
keytool -import -alias <alias-name> -file <certificate-file-name>
-keystore occm.truststore
```

e. 証明書がインストールされていることを確認するには、次のコマンドを実行します。

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

f. occm コンテナを終了するには、次のコマンドを実行します。

```
exit
```

g. occm コンテナをリセットするには、次のコマンドを実行します。

```
docker restart <docker-id>
```

ステップ**6:** コンソールにライセンスを追加する

NetAppからライセンスを購入した場合は、新しいCloud Volumes ONTAPシステムを作成するときにライセンスを選択できるように、コンソールに追加する必要があります。これらのライセンスは、新しいCloud Volumes ONTAPシステムに関連付けるまで未割り当てのままになります。

手順

1. 左側のナビゲーション メニューから、[**Licenses and subscriptions**] を選択します。
2. * Cloud Volumes ONTAP*パネルで、*表示*を選択します。
3. * Cloud Volumes ONTAP*タブで、*ライセンス>ノードベースのライセンス*を選択します。
4. *未割り当て*をクリックします。
5. *未割り当てのライセンスの追加*をクリックします。

6. ライセンスのシリアル番号を入力するか、ライセンス ファイルをアップロードします。
7. ライセンス ファイルがまだない場合は、netapp.com からライセンス ファイルを手動でアップロードする必要があります。
   a. に行く"NetApp License File Generator"NetAppサポート サイトの認証情報を使用してログインします。
   b. パスワードを入力し、製品を選択し、シリアル番号を入力し、プライバシー ポリシーを読んで同意したことを確認してから、[送信] をクリックします。
   c. serialnumber.NLF JSON ファイルを電子メールで受け取るか、直接ダウンロードするかを選択します。
8. *ライセンスの追加*をクリックします。

結果

コンソールは、新しいCloud Volumes ONTAPシステムに関連付けるまで、ライセンスを未割り当てとして追加します。ライセンスは、左側のナビゲーション メニューの *Licenses and subscriptions> Cloud Volumes ONTAP > 表示 > ライセンス * で確認できます。

ステップ**7:** コンソールから**Cloud Volumes ONTAP**を起動する

コンソールで新しいシステムを作成することにより、AWS Secret Cloud および Top Secret Cloud でCloud Volumes ONTAPインスタンスを起動できます。

開始する前に

HA ペアの場合、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. *システム*ページで、*システムの追加*をクリックします。
2. *作成*で、 Cloud Volumes ONTAPを選択します。

   HA の場合: 作成 で、 Cloud Volumes ONTAPまたはCloud Volumes ONTAP HA を選択します。

3. ウィザードの手順を完了して、 Cloud Volumes ONTAPシステムを起動します。

> ウィザードで選択を行う際は、[サービス] の [データ センス & コンプライアンス] と [クラウドへのバックアップ*] を選択しないでください。 *事前構成パッケージ*の下で、*構成の変更*のみを選択し、他のオプションを選択していないことを確認します。事前設定されたパッケージは AWS Secret Cloud および Top Secret Cloud リージョンではサポートされていないため、選択した場合、デプロイは失敗します。

Cloud Volumes ONTAP HAを複数のアベイラビリティゾーンに導入する場合の注意事項

HA ペアの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。

- Cloud Volumes ONTAP HA を複数のアベイラビリティーゾーン (AZ) にデプロイする場合は、トランジットゲートウェイを構成する必要があります。手順については、"AWSトランジットゲートウェイを設定する" 。
- 公開時点では AWS Top Secret Cloud で利用できる AZ は 2 つだけだったので、次のように構成を展開します。

- 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

Cloud Volumes ONTAPを単一ノードと**HA**ノードの両方に導入する場合の注意事項

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。

- 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 オプション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。独自のセキュリティ グループを使用する必要がある場合は、以下のセキュリティ グループのセクションを参照してください。

- AWS 環境を準備するときに作成した 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、初期のCloud Volumes ONTAPボリューム用です。

  後続のボリュームには異なるディスク 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左右されます。

  必要な持続的なパフォーマンスを実現するディスク サイズを選択する必要があります。 EBS 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。

  後で異なるサイズが必要になった場合は、詳細割り当て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。

結果

Cloud Volumes ONTAPインスタンスが起動します。 *監査*ページで進捗状況を追跡できます。

ステップ**8:** データ階層化のためのセキュリティ証明書をインストールする

AWS Secret Cloud および Top Secret Cloud リージョンでデータ階層化を有効にするには、セキュリティ証明書を手動でインストールする必要があります。

開始する前に

1. S3 バケットを作成します。

   バケット名に接頭辞が付いていることを確認してください `fabric-pool-.`例えば `fabric-pool-testbucket`。

2. インストールしたルート証明書を保管してください `step 4`ハンディ。

手順

1. インストールしたルート証明書からテキストをコピーします。 `step 4` 。

2. CLI を使用してCloud Volumes ONTAPシステムに安全に接続します。
3. ルート証明書をインストールします。押す必要があるかもしれません `ENTER`キーを複数回押す:

```
security certificate install -type server-ca -cert-name <certificate-
name>
```

4. プロンプトが表示されたら、コピーしたテキスト全体（およびを含む）を入力します。 `----- BEGIN CERTIFICATE -----`に `-----END CERTIFICATE -----`。
5. 将来の参照用に、CA 署名付きデジタル証明書のコピーを保管してください。
6. CA 名と証明書のシリアル番号を保持します。
7. AWS Secret Cloud および Top Secret Cloud リージョンのオブジェクト ストアを構成します。 `set -privilege advanced -confirmations off`
8. このコマンドを実行してオブジェクト ストアを構成します。

> すべてのAmazonリソース名（ARN）には、 `-iso-b` 、 のような `arn:aws-iso-b`。たとえば、リソースにリージョン付きのARNが必要な場合は、Top Secret Cloudでは次のような命名規則を使用します。 `us-iso-b`のために `-server`フラグ。 `AWS Secret Cloud`の場合は、 `us-iso-b-1`。

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. オブジェクト ストアが正常に作成されたことを確認します。 `storage aggregate object-store show -instance`
10. オブジェクト ストアをアグリゲートに接続します。これを新しい集計ごとに繰り返す必要があります。 `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`

Microsoft Azureを使い始める

Azure でのCloud Volumes ONTAP の展開オプションについて学習します

NetApp は、Azure にCloud Volumes ONTAP を展開するための 2 つのオプションを提供しています。 Cloud Volumes ONTAP は従来、導入とオーケストレーションにNetApp Consoleに依存しています。 Cloud Volumes ONTAP 9.16.1 以降では、Azure マーケットプレイスの直接展開を利用できます。これは、制限はあるものの強力なCloud Volumes ONTAP の機能とオプションのセットへのアクセスを提供する合理化されたプロセスです。

Azure マーケットプレイスからCloud Volumes ONTAP を直接デプロイする場合は、コンソール エージェント

をセットアップしたり、コンソール経由でCloud Volumes ONTAP をデプロイするために必要なその他のセキュリティおよびオンボーディング基準を満たしたりする必要はありません。 Azure マーケットプレイスでは、数回クリックするだけでCloud Volumes ONTAPを迅速に導入し、そのコア機能と機能を自分の環境で試すことができます。

Azure マーケットプレイスでのデプロイが完了すると、コンソールでこれらのシステムを検出できるようになります。検出後は、 Cloud Volumes ONTAPシステムとして管理し、コンソールのすべての機能を利用できます。。 "コンソールで展開されたシステムを検出する" 。

以下は 2 つのオプションの機能比較です。 Azure マーケットプレースを通じてデプロイされたスタンドアロン インスタンスの機能は、コンソールで検出された時点で変更されることに注意してください。

	Azureマーケットプレイス	**NetApp Console**
オンボーディング	より短く、より簡単で、直接導入に必要な準備は最小限	コンソールエージェントのインストールを含む、オンボーディングプロセスが長くなります
サポートされている仮想マシン（**VM**）の種類	Eds_v5 および Ls_v3 インスタンスタイプ	あらゆる種類の VM タイプ。https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html["Azureでサポートされている構成"^]
ライセンス	無料ライセンス	任意の容量ベースのライセンス。"Cloud Volumes ONTAPライセンス"
* NetAppサポート*	含まれません	ライセンスの種類に応じて利用可能
容量	500 GiB以下	構成により拡張可能
展開モデル	単一のアベイラビリティゾーン (AZ) での高可用性 (HA) モードの展開	単一ノードおよび HA モード、単一および複数の AZ 展開を含む、サポートされているすべての構成
サポートされているディスクタイプ	プレミアム SSD v2 マネージド ディスク	より幅広いサポート。"Cloud Volumes ONTAPのデフォルト設定"
書き込み速度（高速書き込みモード）	サポート対象外	構成に基づいてサポートされます。"Cloud Volumes ONTAPの書き込み速度について" 。
オーケストレーション機能	使用不可	ライセンスの種類に応じてNetApp Consoleから利用可能
サポートされるストレージ**VM**の数	展開ごとに1つ	構成に基づいた複数のストレージVM。"サポートされるストレージVMの数"
インスタンスタイプの変更	サポート対象外	サポート
* FabricPool の階層化*	サポート対象外	サポート

関連リンク

- Azure マーケットプレイスの直接展開:"AzureマーケットプレイスからCloud Volumes ONTAPをデプロイ

する"

- コンソール経由のデプロイメント:"Azure でのCloud Volumes ONTAPのクイック スタート"
- "NetApp Consoleのドキュメント"

NetApp Consoleで始める

Azure でのCloud Volumes ONTAPのクイック スタート

数ステップでCloud Volumes ONTAP for Azure を使い始めましょう。

1 コンソールエージェントを作成する

もしあなたが "コンソールエージェント"まだ作成する必要があります。 "Azure でコンソール エージェントを作成する方法を学びます"

インターネット アクセスが利用できないサブネットにCloud Volumes ONTAPを展開する場合は、コンソール エージェントを手動でインストールし、そのコンソール エージェントで実行されているNetApp Consoleにアクセスする必要があることに注意してください。 "インターネットにアクセスできない場所にコンソールエージェントを手動でインストールする方法を学びます"

2 構成を計画する

コンソールでは、ワークロード要件に一致する事前構成済みのパッケージが提供されており、独自の構成を作成することもできます。独自の構成を選択する場合は、利用可能なオプションを理解する必要があります。詳細については、"AzureでCloud Volumes ONTAPの構成を計画する" 。

3 ネットワークを設定する

1. VNet とサブネットがコンソール エージェントとCloud Volumes ONTAP間の接続をサポートすることを確認します。
2. NetApp AutoSupportのターゲット 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ます。

   インターネットにアクセスできない場所にCloud Volumes ONTAPを展開する場合、この手順は必要ありません。

"ネットワーク要件の詳細" 。

4 **Cloud Volumes ONTAP**を起動する

*システムの追加*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完了します。"ステップバイステップの説明を読む" 。

関連リンク

- "コンソールからコンソールエージェントを作成する"
- "Azure Marketplace からコンソール エージェントを作成する"

- "Linuxホストにコンソールエージェントソフトウェアをインストールする"
- "コンソールが権限を使って行うこと"

AzureでCloud Volumes ONTAPの構成を計画する

Azure にCloud Volumes ONTAP をデプロイする場合、ワークロード要件に一致する事前構成済みのシステムを選択することも、独自の構成を作成することもできます。独自の構成を選択する場合は、利用可能なオプションを理解する必要があります。

Cloud Volumes ONTAPライセンスを選択する

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。各オプションにより、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学ぶ"
- "ライセンスの設定方法を学ぶ"

サポートされている地域を選択してください

Cloud Volumes ONTAPは、ほとんどの Microsoft Azure 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地域の完全なリストを見る" 。

サポートされているVMタイプを選択してください

Cloud Volumes ONTAP は、選択したライセンス タイプに応じて、いくつかの VM タイプをサポートします。

"Azure でサポートされるCloud Volumes ONTAPの構成"

ストレージ制限を理解する

Cloud Volumes ONTAPシステムの生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。構成を計画する際には、これらの制限に注意する必要があります。

"Azure のCloud Volumes ONTAPのストレージ制限"

Azure でシステムのサイズを決定する

Cloud Volumes ONTAPシステムのサイズを設定すると、パフォーマンスと容量の要件を満たすことができます。 VM タイプ、ディスク タイプ、ディスク サイズを選択する際には、いくつかの重要なポイントに注意する必要があります。

仮想マシンの種類

サポートされている仮想マシンの種類については、 "Cloud Volumes ONTAPリリースノート"次に、サポートされている各 VM タイプの詳細を確認します。各 VM タイプは特定の数のデータ ディスクをサポートすることに注意してください。

- "Azure ドキュメント: 汎用仮想マシンのサイズ"
- "Azure ドキュメント: メモリ最適化された仮想マシンのサイズ"

単一ノード システムの **Azure** ディスク タイプ

Cloud Volumes ONTAPのボリュームを作成するときは、 Cloud Volumes ONTAP がディスクとして使用する基盤となるクラウド ストレージを選択する必要があります。

単一ノード システムでは、次の種類の Azure マネージド ディスクを使用できます：

- *Premium SSD* マネージド ディスク は、コストは高くなりますが、I/O 集中型のワークロードに高いパフォーマンスを提供します。
- *Premium SSD v2* マネージド ディスク は、Premium SSD マネージド ディスクと比較して、より低いレイテンシでより高いパフォーマンスを低コストで提供します。
- *Standard SSD Managed Disks* は、低い IOPS を必要とするワークロードに対して一貫したパフォーマンスを提供します。
- 高い IOPS を必要とせず、コストを削減したい場合は、*Standard HDD Managed Disks* が適しています。

これらのディスクの使用例の詳細については、以下を参照してください。 "Microsoft Azure ドキュメント: Azure ではどのようなディスク タイプが使用できますか?" 。

HA ペアを備えた **Azure** ディスク タイプ

HA システムでは、プレミアム SSD 共有マネージド ディスクが使用されます。どちらも、コストは高くなりますが、I/O 集中型のワークロードに対して高いパフォーマンスを提供します。 9.12.1 リリースより前に作成された HA デプロイメントでは、Premium ページ BLOB が使用されます。

Azure ディスクサイズ

Cloud Volumes ONTAPインスタンスを起動するときは、アグリゲートのデフォルトのディスク サイズを選択する必要があります。 NetApp Consoleは、初期アグリゲートと、シンプル プロビジョニング オプションを使用するときに作成される追加のアグリゲートにこのディスク サイズを使用します。デフォルトとは異なるディスクサイズを使用するアグリゲートを作成するには、"高度な割り当てオプションを使用する" 。

アグリゲート内のすべてのディスクは同じサイズである必要があります。

ディスク サイズを選択するときは、いくつかの要素を考慮する必要があります。ディスク サイズは、ストレージに支払う金額、アグリゲートで作成できるボリュームのサイズ、 Cloud Volumes ONTAPで使用できる合計容量、およびストレージ パフォーマンスに影響します。

Azure Premium Storage のパフォーマンスはディスク サイズに左右されます。ディスクが大きいほど、IOPS とスループットが向上します。たとえば、1 TiB ディスクを選択すると、コストは高くなりますが、500 GiB ディスクよりも優れたパフォーマンスが得られます。

標準ストレージでは、ディスク サイズ間でパフォーマンスの違いはありません。必要な容量に基づいてディスク サイズを選択する必要があります。

ディスク サイズ別の IOPS とスループットについては、Azure を参照してください。

- "Microsoft Azure: マネージド ディスクの価格"
- "Microsoft Azure: ページ BLOB の価格"

デフォルトのシステムディスクを表示する

コンソールは、ユーザー データ用のストレージに加えて、 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。計画のために、 Cloud Volumes ONTAP を展開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。

"Azure の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" 。

コンソール エージェントにはシステム ディスクも必要です。 "コンソールエージェントのデフォルト構成の詳細を表示する" 。

ネットワーク情報を収集する

Azure にCloud Volumes ONTAPをデプロイする場合は、仮想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。

Azure情報	あなたの価値
リージョン	
仮想ネットワーク (VNet)	
サブネット	
ネットワーク セキュリティ グループ (独自のものを使用している場合)	

書き込み速度を選択する

コンソールでは、Cloud Volumes ONTAP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、標準設定と高速設定の違い、および高速書き込み速度を使用する場合のリスクと推奨事項を理解しておく必要があります。"書き込み速度について詳しくはこちら" 。

ボリューム使用プロファイルを選択する

ONTAPには、必要なストレージの総量を削減できるいくつかのストレージ効率機能が含まれています。コンソールでボリュームを作成するときに、これらの機能を有効にするプロファイルまたは無効にするプロファイルを選択できます。どのプロファイルを使用するかを決めるには、これらの機能について詳しく理解する必要があります。

NetAppストレージ効率機能には、次のような利点があります。

シンプロビジョニング

物理ストレージ プールに実際に存在するよりも多くの論理ストレージをホストまたはユーザーに提供します。ストレージ スペースを事前に割り当てるのではなく、データが書き込まれるときに各ボリュームにストレージ スペースが動的に割り当てられます。

重複排除

同一のデータ ブロックを見つけて、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。この手法は、同じボリューム内に存在する冗長なデータ ブロックを排除することで、ストレージ容量の要件を削減します。

圧縮

プライマリ、セカンダリ、アーカイブ ストレージのボリューム内のデータを圧縮することで、データの保存に必要な物理容量を削減します。

Cloud Volumes ONTAP用の Azure ネットワークを設定する

NetApp Consoleは、IP アドレス、ネットマスク、ルートなどのCloud Volumes ONTAP 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 アクセスが利用可能であること、十分なプライベート IP アドレスが利用可能であること、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。

Cloud Volumes ONTAPの要件

Azure では次のネットワーク要件を満たす必要があります。

アウトバウンドインターネットアクセス

Cloud Volumes ONTAPシステムでは、さまざまな機能の外部エンドポイントにアクセスするために、アウトバウンド インターネット アクセスが必要です。厳格なセキュリティ要件を持つ環境でこれらのエンドポイントがブロックされている場合、 Cloud Volumes ONTAP は正常に動作しません。

コンソール エージェントは、日常的な操作のために複数のエンドポイントにも接続します。エンドポイントの詳細については、以下を参照してください。 "コンソールエージェントから接続されたエンドポイントを表示する"そして "コンソールを使用するためのネットワークの準備"。

Cloud Volumes ONTAPエンドポイント

Cloud Volumes ONTAP はこれらのエンドポイントを使用してさまざまなサービスと通信します。

エンドポイント	適用対象	目的	展開モード	利用できない場合の影響
https://netapp-cloud-account.auth0.com	認証	コンソールでの認証に使用されます。	標準モードと制限モード。	ユーザー認証が失敗し、次のサービスは利用できなくなります。 • Cloud Volumes ONTAPサービス • ONTAPサービス • プロトコルとプロキシサービス

エンドポイント	適用対象	目的	展開モード	利用できない場合の影響
https://vault.azure.net	キーボールト	カスタマー マネージド キー (CMK) を使用するときに、Azure Key Vault からクライアント シークレット キーを取得するために使用されます。	標準、制限、プライベートのモード。	Cloud Volumes ONTAPサービスは利用できません。
https://api.bluexp.netapp.com/tenancy	賃貸借	コンソールからCloud Volumes ONTAPリソースを取得して、リソースとユーザーを承認するために使用されます。	標準モードと制限モード。	Cloud Volumes ONTAPリソースとユーザーは承認されていません。
https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	AutoSupportテレメトリ データをNetAppサポートに送信するために使用されます。	標準モードと制限モード。	AutoSupport情報は未配信のままです。
https://management.azure.com https://login.microsoftonline.com https://bluexpinfraprod.eastus2.data.azurecr.io https://core.windows.net	パブリックリージョン	Azure サービスとの通信。	標準、制限、プライベートのモード。	Cloud Volumes ONTAP は、 Azure サービスと通信して Azure のコンソールの特定の操作を実行できません。
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	中国地域	Azure サービスとの通信。	標準、制限、プライベートのモード。	Cloud Volumes ONTAP は、 Azure サービスと通信して Azure のコンソールの特定の操作を実行できません。
https://management.microsoftazure.de https://login.microsoftonline.de https://blob.core.cloudapi.de https://core.cloudapi.de	ドイツ地域	Azure サービスとの通信。	標準、制限、プライベートのモード。	Cloud Volumes ONTAP は、 Azure サービスと通信して Azure のコンソールの特定の操作を実行できません。

エンドポイント	適用対象	目的	展開モード	利用できない場合の影響
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	政府地域	Azure サービスとの通信。	標準、制限、プライベートのモード。	Cloud Volumes ONTAP は、 Azure サービスと通信して Azure のコンソールの特定の操作を実行できません。
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	政府国防総省地域	Azure サービスとの通信。	標準、制限、プライベートのモード。	Cloud Volumes ONTAP は、 Azure サービスと通信して Azure のコンソールの特定の操作を実行できません。

NetApp Consoleエージェントのネットワークプロキシ構成

NetApp Consoleエージェントのプロキシ サーバー構成を使用して、 Cloud Volumes ONTAPからのアウトバウンド インターネット アクセスを有効にすることができます。コンソールは次の 2 種類のプロキシをサポートしています。

- 明示的なプロキシ: Cloud Volumes ONTAPからの送信トラフィックは、コンソール エージェントのプロキシ構成時に指定されたプロキシ サーバーの HTTP アドレスを使用します。管理者は、追加の認証のためにユーザー資格情報とルート CA 証明書を構成している場合もあります。明示的なプロキシにルートCA証明書が利用可能な場合は、必ず同じ証明書を取得して、 Cloud Volumes ONTAPシステムにアップロードしてください。 "ONTAP CLI: セキュリティ証明書のインストール"指示。
- 透過プロキシ: ネットワークは、 Cloud Volumes ONTAPからの送信トラフィックをコンソール エージェントのプロキシを介して自動的にルーティングするように構成されています。透過プロキシを設定する場合、管理者はプロキシ サーバーの HTTP アドレスではなく、 Cloud Volumes ONTAPからの接続用のルート CA 証明書のみを提供する必要があります。同じルートCA証明書を取得し、 Cloud Volumes ONTAPシステムにアップロードしてください。 "ONTAP CLI: セキュリティ証明書のインストール"指示。

プロキシサーバーの設定方法については、 "プロキシサーバーを使用するようにコンソールエージェントを構成する" 。

IPアドレス

コンソールは、Azure のCloud Volumes ONTAPに必要な数のプライベート IP アドレスを自動的に割り当てます。ネットワークに十分なプライベート IP アドレスが利用可能であることを確認する必要があります。

Cloud Volumes ONTAP に割り当てられる LIF の数は、単一ノード システムを導入するか HA ペア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。SVM 管理 LIF は、SnapCenter などの管理ツールに必要です。

iSCSI LIF は、iSCSI プロトコルを介したクライアント アクセスを提供し、システムによって他の重要なネットワーク ワークフローに使用されます。これらの LIF は必須であり、削除しないでください。

単一ノードシステムの**IP**アドレス

NetApp Console は、単一ノード システムに 5 つまたは 6 つの IP アドレスを割り当てます：

- クラスタ管理IP
- ノード管理IP
- SnapMirrorのクラスタ間 IP
- NFS/CIFS IP
- iSCSI IP

iSCSI IP は、iSCSI プロトコルを介したクライアント アクセスを提供します。これは、システムによって他の重要なネットワーク ワークフローにも使用されます。この LIF は必須であり、削除しないでください。

- SVM 管理 (オプション - デフォルトでは構成されていません)

HAペアの**IP**アドレス

コンソールは、展開中に 4 つの NIC (ノードあたり) に IP アドレスを割り当てます。

NetApp Console は HA ペア上に SVM 管理 LIF を作成しますが、Azure の単一ノード システム上には作成しないことに注意してください。

NIC0

- ノード管理IP
- クラスタ間IP
- iSCSI IP

iSCSI IP は、iSCSI プロトコルを介したクライアント アクセスを提供します。これは、システムによって他の重要なネットワーク ワークフローにも使用されます。この LIF は必須であり、削除しないでください。

NIC1

- クラスターネットワークIP

NIC2

- クラスタ相互接続 IP (HA IC)

NIC3

- Pageblob NIC IP (ディスクアクセス)

NIC3 は、ページ BLOB ストレージを使用する HA 展開にのみ適用されます。

上記の IP アドレスは、フェールオーバー イベントでは移行されません。

さらに、4 つのフロントエンド IP (FIP) がフェイルオーバー イベント時に移行するように構成されています。これらのフロントエンド IP はロードバランサー内に存在します。

- クラスタ管理IP
- NodeA データ IP (NFS/CIFS)
- NodeB データ IP (NFS/CIFS)
- SVM管理IP

Azure サービスへの安全な接続

デフォルトでは、コンソールは、 Cloud Volumes ONTAPと Azure ページ BLOB ストレージ アカウント間の接続に Azure プライベート リンクを有効にします。

ほとんどの場合、何もする必要はありません。コンソールが Azure Private Link を管理します。ただし、Azure プライベート DNS を使用する場合は、構成ファイルを編集する必要があります。 Azure 内のコンソール エージェントの場所に関する要件にも注意する必要があります。

ビジネスニーズに応じて、プライベートリンク接続を無効にすることもできます。リンクを無効にすると、コンソールは代わりにサービス エンドポイントを使用するようにCloud Volumes ONTAPを構成します。

"Cloud Volumes ONTAPで Azure Private Links またはサービス エンドポイントを使用する方法の詳細" 。

Azure VNet 暗号化のネットワーク

Cloud Volumes ONTAPは "Azure Virtual Network（VNet）暗号化"VNet内またはピアリングされたVNet間のVM間トラフィックの暗号化をサポートしています。この機能はAzure VNetレイヤーで設定され、Cloud Volumes ONTAPトポロジ（単一ノードまたはHA）から独立しています。

機能を有効にする前に、VM の NIC で高速ネットワークが有効になっていることを確認し、Azure VNet 暗号化の要件と制限事項を確認するだけで済みます。NetApp 管理対象ロードバランサオブジェクトを変更しないでください。

"Azure ドキュメント：VNet 暗号化と Accelerated Networking"。

他の**ONTAP**システムへの接続

Azure のCloud Volumes ONTAPシステムと他のネットワークのONTAPシステム間でデータを複製するには、Azure VNet と他のネットワーク (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、 "Microsoft Azure ドキュメント: Azure ポータルでサイト間接続を作成する" 。

HA相互接続用のポート

Cloud Volumes ONTAP HA ペアには HA 相互接続が含まれており、これにより各ノードはパートナーが機能しているかどうかを継続的に確認し、もう一方の不揮発性メモリのログ データをミラーリングできます。 HA 相互接続は通信に TCP ポート 10006 を使用します。

デフォルトでは、HA 相互接続 LIF 間の通信はオープンであり、このポートにはセキュリティ グループ ルールはありません。ただし、HA 相互接続 LIF 間にファイアウォールを作成する場合は、HA ペアが適切に動作できるように、TCP トラフィックがポート 10006 に対して開いていることを確認する必要があります。

Azure リソース グループには **HA** ペアが **1** つだけあります

Azure にデプロイするCloud Volumes ONTAP HA ペアごとに専用のリソース グループを使用する必要があります。リソース グループでは 1 つの HA ペアのみがサポートされます。

Azure リソース グループに 2 番目のCloud Volumes ONTAP HA ペアをデプロイしようとすると、コンソールで接続の問題が発生します。

セキュリティグループルール

コンソールは、Cloud Volumes ONTAP が正常に動作するためのインバウンド ルールとアウトバウンド ルールを含む Azure セキュリティ グループを作成します。 "コンソールエージェントのセキュリティグループルールを表示する" 。

Cloud Volumes ONTAPの Azure セキュリティ グループでは、ノード間の内部通信用に適切なポートが開いている必要があります。 "ONTAPの内部ポートについて学ぶ" 。

定義済みのセキュリティ グループを変更したり、カスタム セキュリティ グループを使用することはお勧めしません。ただし、必要な場合は、展開プロセスでCloud Volumes ONTAPシステムが独自のサブネット内でフルアクセス権を持つ必要があることに注意してください。デプロイが完了したら、ネットワーク セキュリティ グループを変更する場合は、クラスター ポートと HA ネットワーク ポートを開いたままにしておいてください。これにより、Cloud Volumes ONTAPクラスター内でのシームレスな通信 (ノード間の any-to-any 通信) が保証されます。

単一ノードシステムの受信ルール

Cloud Volumes ONTAPシステムを追加し、定義済みのセキュリティ グループを選択すると、次のいずれかの範囲内でトラフィックを許可することを選択できます。

- 選択した **VNet** のみ: 受信トラフィックのソースは、Cloud Volumes ONTAPシステムの VNet のサブネット範囲と、コンソール エージェントが存在する VNet のサブネット範囲です。これは推奨されるオプションです。
- すべての **VNet**: 受信トラフィックのソースは、0.0.0.0/0 IP 範囲です。
- 無効: このオプションは、ストレージ アカウントへのパブリック ネットワーク アクセスを制限し、 Cloud Volumes ONTAPシステムのデータ階層化を無効にします。セキュリティ規制やポリシーにより、同じ VNet 内であってもプライベート IP アドレスを公開しない場合は、このオプションが推奨されます。

優先順位と名前	ポートとプロトコル	送信元と送信先	説明
1000 受信SSH	22 TCP	任意対任意	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
1001 インバウンド_http	80 TCP	任意対任意	クラスタ管理LIFのIPアドレスを使用してONTAP System Manager WebコンソールにHTTPアクセスする

優先順位と名前	ポートとプロトコル	送信元と送信先	説明
1002 inbound_111_tcp	111 TCP	任意対任意	NFS のリモート プロシージャ コール
1003 inbound_111_udp	111 UDP	任意対任意	NFS のリモート プロシージャ コール
1004 inbound_139	139 TCP	任意対任意	CIFSのNetBIOSサービスセッション
1005 受信_161-162 _tcp	161-162 TCP	任意対任意	簡易ネットワーク管理プロトコル
1006 受信_161-162 _udp	161-162 UDP	任意対任意	簡易ネットワーク管理プロトコル
1007 inbound_443	443 TCP	任意対任意	コンソールエージェントとの接続と、クラスタ管理LIFのIPアドレスを使用したONTAP System Manager Webコンソールへの HTTPSアクセス
1008 inbound_445	445 TCP	任意対任意	NetBIOS フレームを使用した TCP 経由の Microsoft SMB/CIFS
1009 inbound_635_tcp	635 TCP	任意対任意	NFSマウント
1010 inbound_635_udp	635 UDP	任意対任意	NFSマウント
1011 inbound_749	749 TCP	任意対任意	Kerberos
1012 inbound_2049_tcp	2049 TCP	任意対任意	NFSサーバ デーモン
1013 inbound_2049_udp	2049 UDP	任意対任意	NFSサーバ デーモン
1014 inbound_3260	3260 TCP	任意対任意	iSCSI データ LIF を介した iSCSI アクセス
1015 受信_4045-4046_tcp	4045-4046 TCP	任意対任意	NFS ロックデーモンとネットワークステータスモニター
1016 受信_4045-4046_udp	4045-4046 UDP	任意対任意	NFS ロックデーモンとネットワークステータスモニター
1017 inbound_10000	10000 TCP	任意対任意	NDMPを使用したバックアップ
1018 着信_11104-11105	11104-11105 TCP	任意対任意	SnapMirrorデータ転送
3000 受信拒否 _all_tcp	任意のポート TCP	任意対任意	その他のTCP受信トラフィックをすべてブロックする
3001 受信拒否 _all_udp	任意のポートUDP	任意対任意	その他のUDP受信トラフィックをすべてブロックする

優先順位と名前	ポートとプロトコル	送信元と送信先	説明
65000 VnetInBound を許可する	任意のポート 任意のプロトコル	仮想ネットワークから仮想ネットワークへ	VNet 内からの受信トラフィック
65001 Azureロードバランサーの受信を許可する	任意のポート 任意のプロトコル	AzureLoadBalancer から Any	Azure Standard Load Balancer からのデータ トラフィック
65500 全受信拒否	任意のポート 任意のプロトコル	任意対任意	その他のすべての受信トラフィックをブロックする

HAシステムの受信ルール

Cloud Volumes ONTAPシステムを追加し、定義済みのセキュリティ グループを選択すると、次のいずれかの範囲内でトラフィックを許可することを選択できます。

- 選択した **VNet** のみ: 受信トラフィックのソースは、Cloud Volumes ONTAPシステムの VNet のサブネット範囲と、コンソール エージェントが存在する VNet のサブネット範囲です。これは推奨されるオプションです。
- すべての **VNet**: 受信トラフィックのソースは、0.0.0.0/0 IP 範囲です。

> HA システムでは、受信データ トラフィックが Azure Standard Load Balancer を経由するため、単一ノード システムよりも受信ルールが少なくなります。このため、ロードバランサーからのトラフィックは、「AllowAzureLoadBalancerInBound」ルールに示されているように、開いている必要があります。

- 無効: このオプションは、ストレージ アカウントへのパブリック ネットワーク アクセスを制限し、 Cloud Volumes ONTAPシステムのデータ階層化を無効にします。セキュリティ規制やポリシーにより、同じ VNet 内であってもプライベート IP アドレスを公開しない場合は、このオプションが推奨されます。

優先順位と名前	ポートとプロトコル	送信元と送信先	説明
100 inbound_443	443 任意のプロトコル	任意対任意	コンソールエージェントとの接続と、クラスタ管理LIFのIPアドレスを使用したONTAP System Manager Webコンソールへの HTTPSアクセス
101 inbound_111_tcp	111 任意のプロトコル	任意対任意	NFS のリモート プロシージャ コール
102 inbound_2049_tcp	2049 あらゆるプロトコル	任意対任意	NFSサーバ デーモン
111 受信SSH	22 あらゆるプロトコル	任意対任意	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
121 inbound_53	53 あらゆるプロトコル	任意対任意	DNSとCIFS
65000 VnetInBound を許可する	任意のポート 任意のプロトコル	仮想ネットワークから仮想ネットワークへ	VNet 内からの受信トラフィック

優先順位と名前	ポートとプロトコル	送信元と送信先	説明
65001 Azureロードバランサーの受信を許可する	任意のポート 任意のプロトコル	AzureLoadBalancer から Any	Azure Standard Load Balancer からのデータ トラフィック
65500 全受信拒否	任意のポート 任意のプロトコル	任意対任意	その他のすべての受信トラフィックをブロックする

アウトバウンドルール

Cloud Volumes ONTAPの定義済みセキュリティ グループは、すべての送信トラフィックを開きます。それが許容できる場合は、基本的な送信ルールに従ってください。より厳格なルールが必要な場合は、高度な送信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の定義済みセキュリティ グループには、次の送信ルールが含まれています。

ポート	プロトコル	目的
全て	すべてTCP	すべての送信トラフィック
全て	すべてUDP	すべての送信トラフィック

高度なアウトバウンドルール

送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による送信通信に必要なポートのみを開くことができます。

ソースは、Cloud Volumes ONTAPシステム上のインターフェース (IP アドレス) です。

サービス	ポート	プロトコル	ソース	デスティネーション	目的
Active Directory	88	TCP	ノード管理LIF	アクティブディレクトリフォレスト	Kerberos V認証
	137	UDP	ノード管理LIF	アクティブディレクトリフォレスト	NetBIOSネーム サービス
	138	UDP	ノード管理LIF	アクティブディレクトリフォレスト	NetBIOSデータグラムサービス
	139	TCP	ノード管理LIF	アクティブディレクトリフォレスト	NetBIOSサービス セッション
	389	TCPとUDP	ノード管理LIF	アクティブディレクトリフォレスト	LDAP
	445	TCP	ノード管理LIF	アクティブディレクトリフォレスト	NetBIOS フレームを使用した TCP 経由の Microsoft SMB/CIFS
	464	TCP	ノード管理LIF	アクティブディレクトリフォレスト	Kerberos V パスワードの変更と設定 (SET_CHANGE)
	464	UDP	ノード管理LIF	アクティブディレクトリフォレスト	Kerberos鍵管理
	749	TCP	ノード管理LIF	アクティブディレクトリフォレスト	Kerberos V パスワードの変更と設定 (RPCSEC_GSS)
	88	TCP	データ LIF (NFS、CIFS、iSCSI)	アクティブディレクトリフォレスト	Kerberos V認証
	137	UDP	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	NetBIOSネーム サービス
	138	UDP	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	NetBIOSデータグラムサービス
	139	TCP	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	NetBIOSサービス セッション
	389	TCPとUDP	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	LDAP
	445	TCP	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	NetBIOS フレームを使用した TCP 経由の Microsoft SMB/CIFS
	464	TCP	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	Kerberos V パスワードの変更と設定 (SET_CHANGE)
	464	UDP	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	Kerberos鍵管理
	749	TCP	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	Kerberos V パスワードの変更と設定 (RPCSEC_GSS)

サービス	ポート	プロトコル	ソース	デスティネーション	目的
AutoSupport	HTTPS	443	ノード管理LIF	mysupport.netapp.com	AutoSupport （HTTPSがデフォルト）
	HTTP	80	ノード管理LIF	mysupport.netapp.com	AutoSupport （トランスポート プロトコルが HTTPS から HTTP に変更された場合のみ）
	TCP	3128	ノード管理LIF	コンソールエージェント	アウトバウンドインターネット接続が利用できない場合、コンソールエージェント上のプロキシサーバーを介してAutoSupportメッセージを送信する
構成のバックアップ	HTTP	80	ノード管理LIF	http://<コンソールエージェントのIPアドレス>/occm/offboxconfig	構成のバックアップをコンソールエージェントに送信します。"ONTAPのドキュメント" 。
DHCP	68	UDP	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	67	UDP	ノード管理LIF	DHCP	DHCP サーバ
DNS	53	UDP	ノード管理LIFとデータLIF（NFS、CIFS）	DNS	DNS
NDMP	18600～18699	TCP	ノード管理LIF	宛先サーバー	NDMPコピー
SMTP	25	TCP	ノード管理LIF	メール サーバ	SMTPアラートはAutoSupportに使用できます
SNMP	161	TCP	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	161	UDP	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	162	TCP	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	162	UDP	ノード管理LIF	監視サーバー	SNMPトラップによる監視
SnapMirror	11104	TCP	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
	11105	TCP	クラスタ間LIF	ONTAPクラスタ間LIF	SnapMirrorデータ転送
syslog	514	UDP	ノード管理LIF	syslogサーバ	Syslog転送メッセージ

コンソールエージェントの要件

コンソール エージェントをまだ作成していない場合は、コンソール エージェントのネットワーク要件も確認する必要があります。

- "コンソールエージェントのネットワーク要件を表示する"

- "Azure のセキュリティ グループ ルール"

関連トピック

- "Cloud Volumes ONTAPのAutoSupport設定を確認する"
- "ONTAPの内部ポートについて学ぶ" 。

Azureで顧客管理キーを使用するように**Cloud Volumes ONTAP**を設定する

データは、Microsoft が管理するキーを使用した Azure Storage Service Encryption を使用して、Azure のCloud Volumes ONTAP上で自動的に暗号化されます。ただし、このページの手順に従って、代わりに独自の暗号化キーを使用することもできます。

データ暗号化の概要

Cloud Volumes ONTAPデータはAzureで自動的に暗号化されます。 "Azure Storage Service Encryption" 。デフォルトの実装では、Microsoft が管理するキーが使用されます。セットアップは必要ありません。

Cloud Volumes ONTAPでカスタマー管理キーを使用する場合は、次の手順を完了する必要があります。

1. Azure からキー コンテナーを作成し、そのコンテナー内にキーを生成します。
2. NetApp Consoleから、API を使用して、キーを使用するCloud Volumes ONTAPシステムを作成します。

データの暗号化方法

コンソールはディスク暗号化セットを使用します。これにより、ページ BLOB ではなく管理対象ディスクで暗号化キーを管理できるようになります。新しいデータ ディスクでも同じディスク暗号化セットが使用されます。下位バージョンでは、顧客管理キーではなく、Microsoft 管理キーが使用されます。

カスタマー管理キーを使用するように設定されたCloud Volumes ONTAPシステムを作成すると、 Cloud Volumes ONTAPデータは次のように暗号化されます。

Cloud Volumes ONTAP構成	キー暗号化に使用されるシステム ディスク	キー暗号化に使用されるデータ ディスク
シングル ノード	• ブート • コア • NVRAM	• ルート • データ
Azure HA 単一可用性ゾーンとページ BLOB	• ブート • コア • NVRAM	なし
共有マネージド ディスクを備えた Azure HA 単一可用性ゾーン	• ブート • コア • NVRAM	• ルート • データ

Cloud Volumes ONTAP構成	キー暗号化に使用されるシステムディスク	キー暗号化に使用されるデータディスク
共有マネージド ディスクを使用した Azure HA 複数可用性ゾーン	• ブート • コア • NVRAM	• ルート • データ

Cloud Volumes ONTAPのすべての Azure ストレージ アカウントは、顧客管理キーを使用して暗号化されます。ストレージ アカウントの作成中に暗号化する場合は、 Cloud Volumes ONTAP作成リクエストでリソースの ID を作成して提供する必要があります。これはすべてのタイプの展開に適用されます。指定しない場合でもストレージ アカウントは暗号化されますが、コンソールは最初に Microsoft 管理のキー暗号化を使用してストレージ アカウントを作成し、次にカスタマー マネージド キーを使用するようにストレージ アカウントを更新します。

Cloud Volumes ONTAPでのキーローテーション

暗号化キーを構成するときは、Azure ポータルを使用して自動キー ローテーションを設定し、有効にする必要があります。新しいバージョンの暗号化キーを作成して有効にすると、 Cloud Volumes ONTAP は暗号化に最新のキー バージョンを自動的に検出して使用できるようになり、手動による介入を必要とせずにデータの安全性が確保されます。

キーの構成とキーのローテーションの設定については、次の Microsoft Azure ドキュメントのトピックを参照してください。

- "Azure Key Vault で暗号化キーの自動ローテーションを構成する"
- "Azure PowerShell - カスタマーマネージドキーを有効にする"

> キーを設定したら、次の項目を選択したことを確認してください。 "自動回転を有効にする"これにより、 Cloud Volumes ONTAP は、以前のキーの有効期限が切れたときに新しいキーを使用できるようになります。 Azure ポータルでこのオプションを有効にしないと、 Cloud Volumes ONTAP は新しいキーを自動的に検出できず、ストレージのプロビジョニングで問題が発生する可能性があります。

ユーザー割り当てマネージド ID を作成する

ユーザー割り当てマネージド ID と呼ばれるリソースを作成するオプションがあります。これにより、Cloud Volumes ONTAPシステムを作成するときにストレージ アカウントを暗号化できるようになります。キー コンテナーを作成してキーを生成する前に、このリソースを作成することをお勧めします。

リソースの ID は次のとおりです: `userassignedidentity` 。

手順

1. Azure で、Azure サービスに移動し、マネージド **ID** を選択します。
2. *作成*をクリックします。
3. 以下の詳細を入力してください。
   - サブスクリプション: サブスクリプションを選択します。コンソール エージェントのサブスクリプションと同じサブスクリプションを選択することをお勧めします。
   - リソース グループ: 既存のリソース グループを使用するか、新しいリソース グループを作成します。

- リージョン: オプションで、コンソール エージェントと同じリージョンを選択します。
- 名前: リソースの名前を入力します。

4. 必要に応じてタグを追加します。
5. *作成*をクリックします。

キーコンテナーを作成し、キーを生成する

キー コンテナーは、Cloud Volumes ONTAPシステムを作成する予定の Azure サブスクリプションとリージョンに存在する必要があります。

もしあなたがユーザー割り当てマネージドIDを作成したキー コンテナーを作成するときに、キー コンテナーのアクセス ポリシーも作成する必要があります。

手順

1. "Azureサブスクリプションにキーコンテナーを作成する" 。

   キー コンテナーの次の要件に注意してください。

   - キー ボールトは、Cloud Volumes ONTAPシステムと同じリージョンに存在する必要があります。
   - 次のオプションを有効にする必要があります。
     - ソフト削除 (このオプションはデフォルトで有効になっていますが、無効にしないでください)
     - パージ保護
     - ボリューム暗号化のための **Azure Disk Encryption**（単一ノード システム、複数ゾーンの HA ペア、および HA 単一 AZ 展開の場合）

       Azure カスタマー管理暗号化キーを使用するには、キー コンテナーに対して Azure Disk Encryption が有効になっている必要があります。

   - ユーザー割り当てマネージド ID を作成した場合は、次のオプションを有効にする必要があります。
     - **Vault** アクセス ポリシー
2. [コンテナー アクセス ポリシー] を選択した場合は、[作成] をクリックして、キー コンテナーのアクセス ポリシーを作成します。そうでない場合は、手順 3 に進みます。
   a. 次の権限を選択します。
      - 得る
      - リスト
      - 解読する
      - 暗号化する
      - アンラップキー
      - ラップキー
      - 確認カクニン
      - サイン

b. ユーザーが割り当てたマネージド ID (リソース) をプリンシパルとして選択します。

c. アクセス ポリシーを確認して作成します。

3. "キーコンテナーにキーを生成する" 。

キーについては次の要件に注意してください。

- キータイプは **RSA** である必要があります。
- 推奨される RSA キー サイズは **2048** ですが、他のサイズもサポートされています。

暗号化キーを使用するシステムを作成する

キー ボールトを作成し、暗号化キーを生成したら、そのキーを使用するように構成された新しいCloud Volumes ONTAPシステムを作成できます。これらの手順は、API を使用することでサポートされます。

必要な権限

単一ノードのCloud Volumes ONTAPシステムでカスタマー管理キーを使用する場合は、コンソール エージェントに次の権限があることを確認してください。

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"最新の権限リストを表示する"

手順

1. 次の API 呼び出しを使用して、Azure サブスクリプション内のキー コンテナーの一覧を取得します。

HA ペアの場合: `GET /azure/ha/metadata/vaults`

単一ノードの場合: `GET /azure/vsa/metadata/vaults`

name と **resourceGroup** をメモします。次のステップでこれらの値を指定する必要があります。

"このAPI呼び出しの詳細" 。

2. 次の API 呼び出しを使用して、ボールト内のキーのリストを取得します。

HA ペアの場合: `GET /azure/ha/metadata/keys-vault`

単一ノードの場合: `GET /azure/vsa/metadata/keys-vault`

keyName をメモします。次の手順で、その値 (および Vault 名) を指定する必要があります。

"このAPI呼び出しの詳細" 。

3. 次の API 呼び出しを使用して、 Cloud Volumes ONTAPシステムを作成します。

   a. HA ペアの場合:

      `POST /azure/ha/working-environments`

      リクエスト本体には次のフィールドを含める必要があります。

      ```
      "azureEncryptionParameters": {
                    "key": "keyName",
                    "vaultName": "vaultName"
      }
      ```

      含める `"userAssignedIdentity": " userAssignedIdentityId"` このリソースをストレージ アカウントの暗号化に使用するために作成した場合は、このフィールドが必要です。

      "このAPI呼び出しの詳細" 。

   b. 単一ノード システムの場合：

      `POST /azure/vsa/working-environments`

      リクエスト本体には次のフィールドを含める必要があります。

      ```
      "azureEncryptionParameters": {
                    "key": "keyName",
                    "vaultName": "vaultName"
      }
      ```

      含める `"userAssignedIdentity": " userAssignedIdentityId"` このリソースをストレージ アカウントの暗号化に使用するために作成した場合は、このフィールドが必要です。

   "このAPI呼び出しの詳細" 。

結果

データ暗号化に顧客管理キーを使用するように設定された新しいCloud Volumes ONTAPシステムがあります。

AzureでCloud Volumes ONTAPのライセンスを設定する

Cloud Volumes ONTAPで使用するライセンス オプションを決定したら、新しいシステムを作成するときにそのライセンス 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

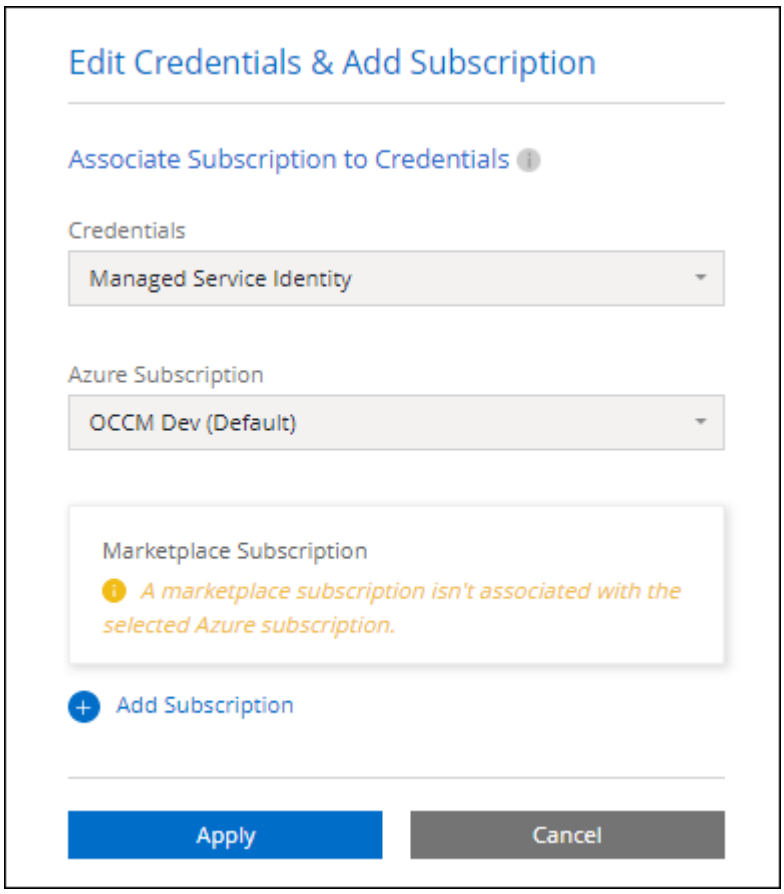
最大 500 GiB のプロビジョニング容量でCloud Volumes ONTAP を無料で使用するには、Freemium オファリングを選択してください。"フリーミアムプランの詳細" 。

手順

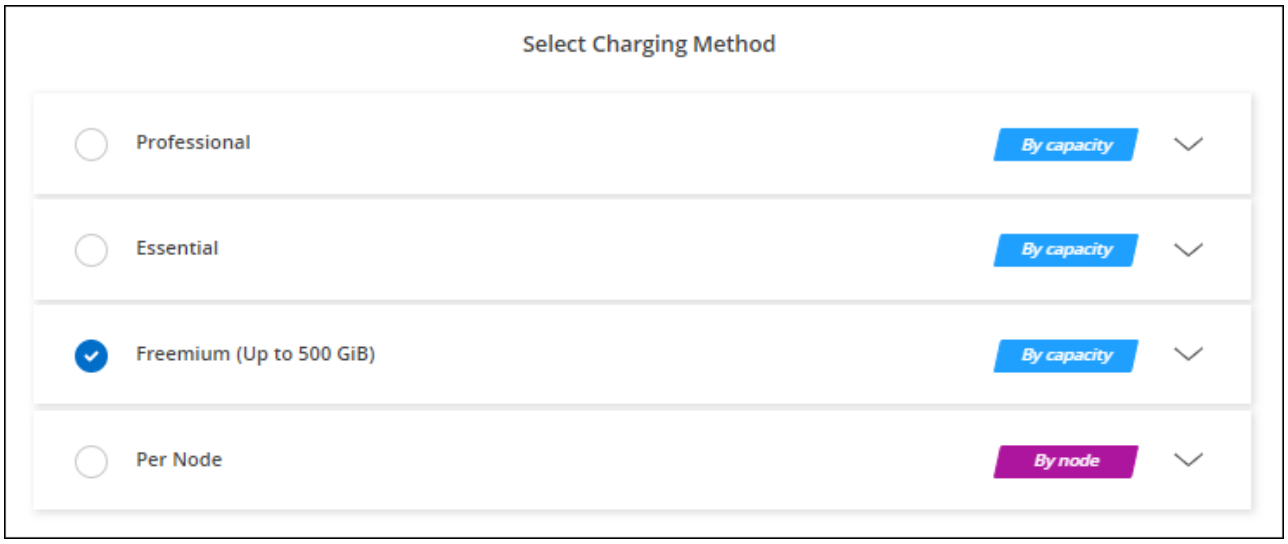
1. NetApp Consoleの左側のナビゲーション メニューから、ストレージ > 管理 を選択します。
2. *システム*ページで*システムの追加*をクリックし、手順に従います。

    a. *詳細と資格情報*ページで、*資格情報の編集 > 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 Azure Marketplace の従量課金制オファリングをサブスクライブします。

    プロビジョニングされた容量が500GiBを超えない限り、マーケットプレイスのサブスクリプションを通じて課金されることはありません。その時点で、システムは自動的に"エッセンシャルパッケージ"。



    a. コンソールに戻ったら、課金方法のページにアクセスして「**Freemium**」を選択します。



"AzureでCloud Volumes ONTAPを起動するための手順を見る" 。

容量ベースのライセンス

容量ベースのライセンスでは、容量 1 TiB ごとにCloud Volumes ONTAPの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、Essentials パッケージまたは Professional パッケージというパッケージ形式で提供されます。

Essentials および Professional パッケージは、次の消費モデルまたは購入オプションで利用できます。

- NetAppから購入したライセンス（BYOL）
- Azure Marketplace からの時間単位の従量課金制 (PAYGO) サブスクリプション
- 年間契約

"容量ベースのライセンスについて詳しく見る" 。

次のセクションでは、それぞれの消費モデルを開始する方法について説明します。

BYOL

NetAppからライセンス (BYOL) を購入して前払いすることで、任意のクラウド プロバイダーにCloud Volumes ONTAPシステムを導入できます。

はBYOLライセンスの購入、延長、および更新を制限しています。 "Cloud Volumes ONTAPのBYOL ライセンスの利用制限" 。

手順

1. "ライセンスを取得するには、 NetApp の営業担当者にお問い合わせください。"
2. "NetAppサポートサイトのアカウントをコンソールに追加します"

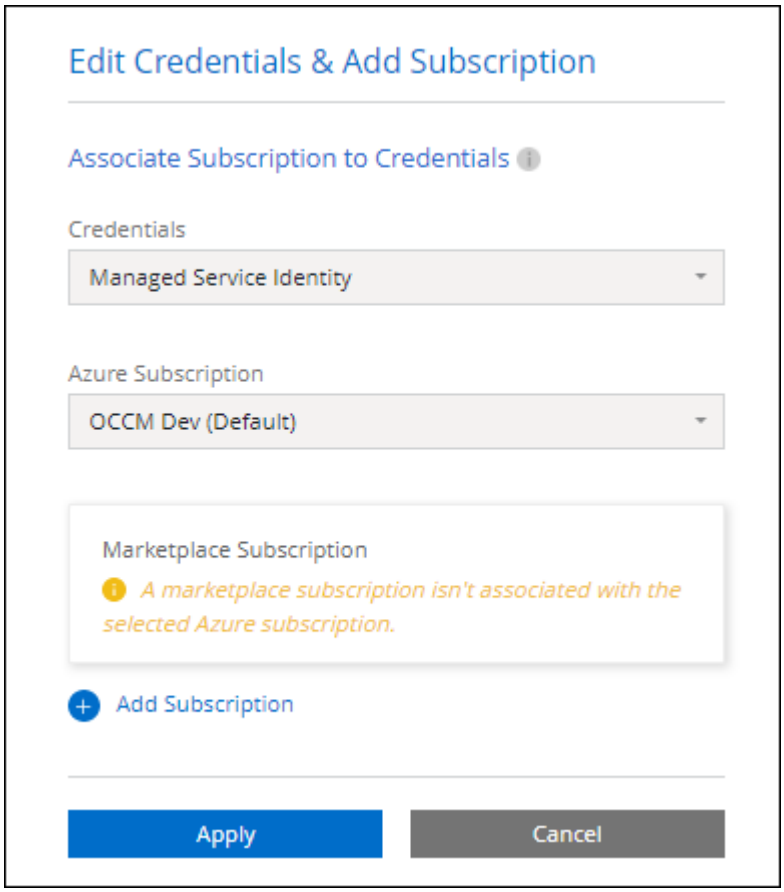
   コンソールは NetApp のライセンス サービスに自動的にクエリを実行し、 NetAppサポート サイト アカウントに関連付けられているライセンスの詳細を取得します。エラーがない場合、コンソールはライセンスを自動的にコンソールに追加します。

Cloud Volumes ONTAPでライセンスを使用するには、コンソールからライセンスを利用できる必要があります。必要であれば、"コンソールにライセンスを手動で追加する" 。

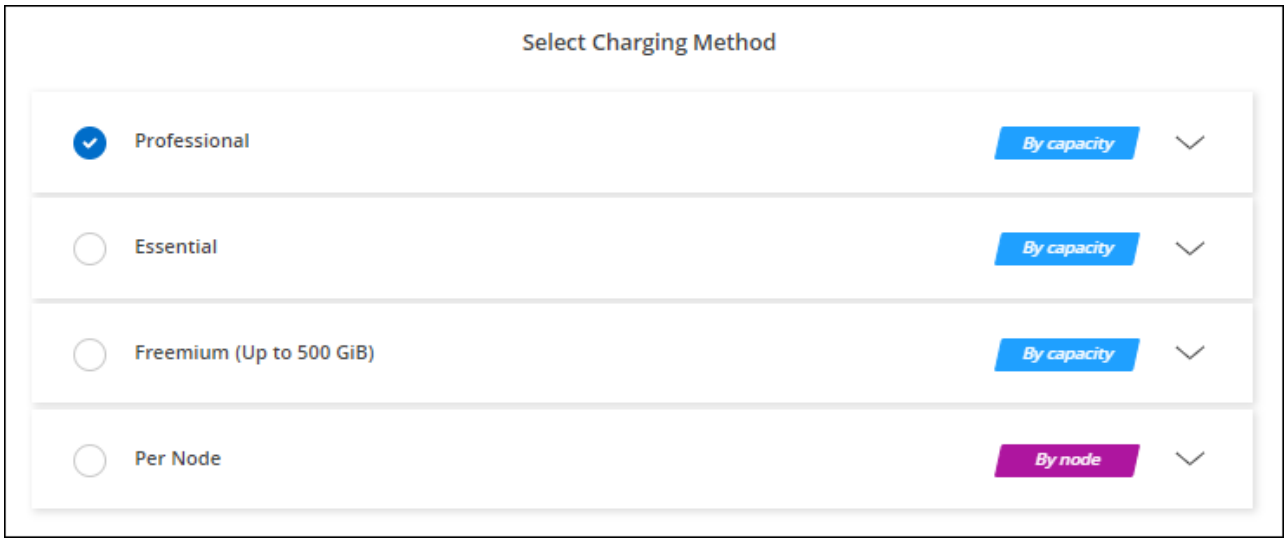
3. *システム*ページで*システムの追加*をクリックし、手順に従います。

   a. *詳細と資格情報*ページで、*資格情報の編集 > 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 Azure Marketplace の従量課金制オファリングをサブスクライブします。

      NetAppから購入したライセンスに対しては常に最初に課金されますが、ライセンス容量を超えた場合、またはライセンスの有効期限が切れた場合は、マーケットプレイスの時間単位料金で課金されます。



   a. コンソールに戻ったら、課金方法ページにアクセスして容量ベースのパッケージを選択します。



"AzureでCloud Volumes ONTAPを起動するための手順を見る" 。

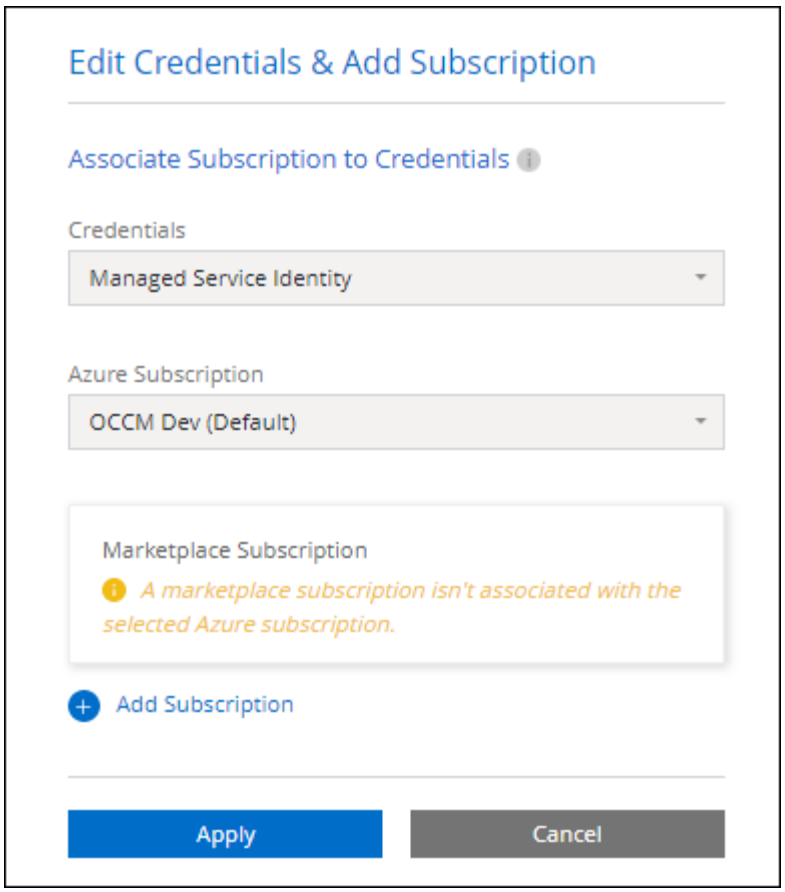
PAYGOサブスクリプション

クラウド プロバイダーのマーケットプレイスからのオファーをサブスクライブして、時間単位で支払います。

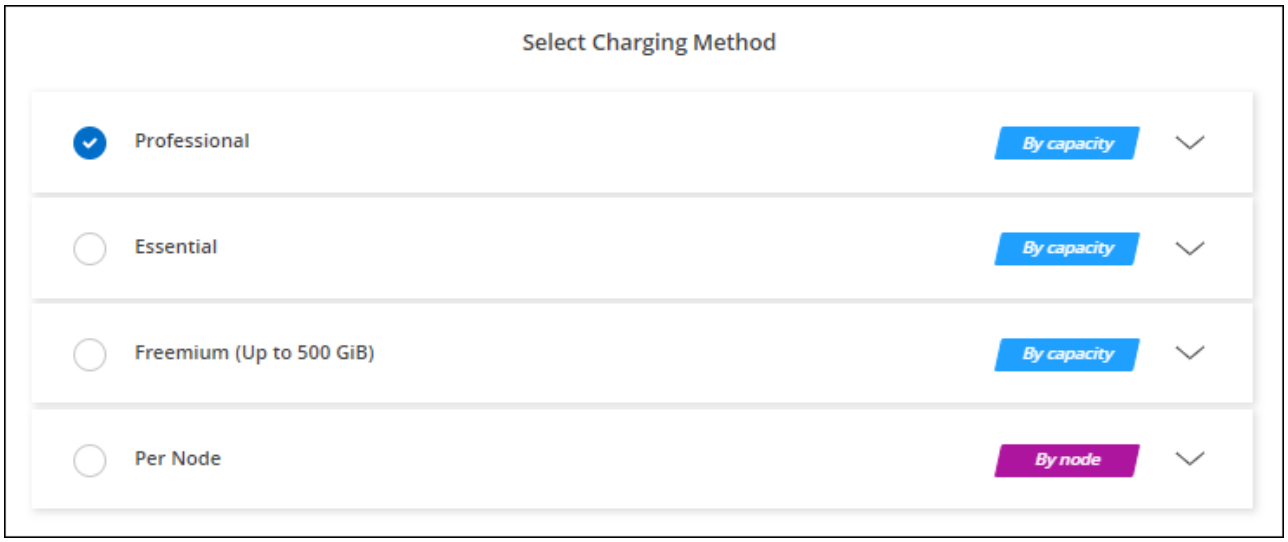
Cloud Volumes ONTAPシステムを作成すると、コンソールに、Azure Marketplace で利用可能な契約にサブスクライブするように求めるプロンプトが表示されます。そのサブスクリプションは課金システムに関連付けられます。同じサブスクリプションを追加のシステムにも使用できます。

手順

1. 左側のナビゲーション メニューから、ストレージ > 管理 を選択します。
2. *システム*ページで*システムの追加*をクリックし、手順に従います。
    a. *詳細と資格情報*ページで、*資格情報の編集 > 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 Azure Marketplace の従量課金制オファリングをサブスクライブします。



b. コンソールに戻ったら、課金方法ページにアクセスして容量ベースのパッケージを選択します。



"AzureでCloud Volumes ONTAPを起動するための手順を見る" 。

Azure アカウントに関連付けられている Azure Marketplace サブスクリプションは、[設定] > [資格情報] ページから管理できます。 "Azure アカウントとサブスクリプションを管理する方法を学びます"

年間契約

年間契約を購入して、 Cloud Volumes ONTAP の料金を毎年支払います。

手順

1. 年間契約を購入するには、 NetApp の営業担当者にお問い合わせください。

   契約は、Azure Marketplace でプライベート オファーとして利用できます。

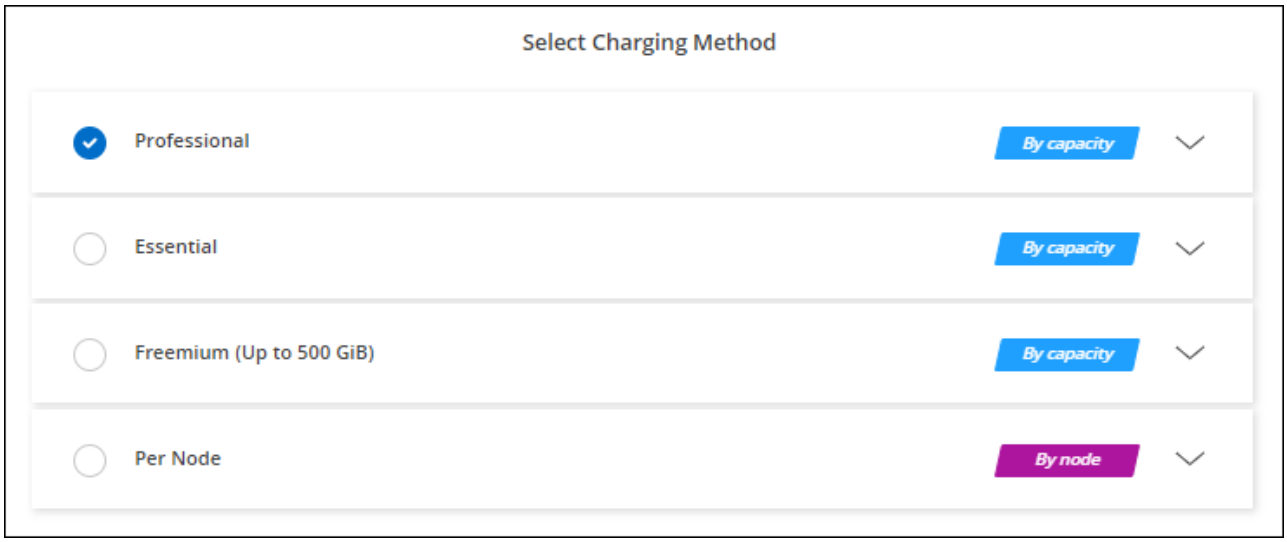
   NetApp がプライベート オファーを共有した後、システム作成中に Azure Marketplace からサブスクライブするときに年間プランを選択できます。

2. *システム*ページで*システムの追加*をクリックし、手順に従います。

   a. *詳細と資格情報*ページで、*資格情報の編集 > サブスクリプションの追加 > 続行*をクリックします。

   b. Azure ポータルで、Azure アカウントと共有された年間プランを選択し、[サブスクライブ] をクリックします。

   c. コンソールに戻ったら、課金方法ページにアクセスして容量ベースのパッケージを選択します。



"AzureでCloud Volumes ONTAPを起動するための手順を見る" 。

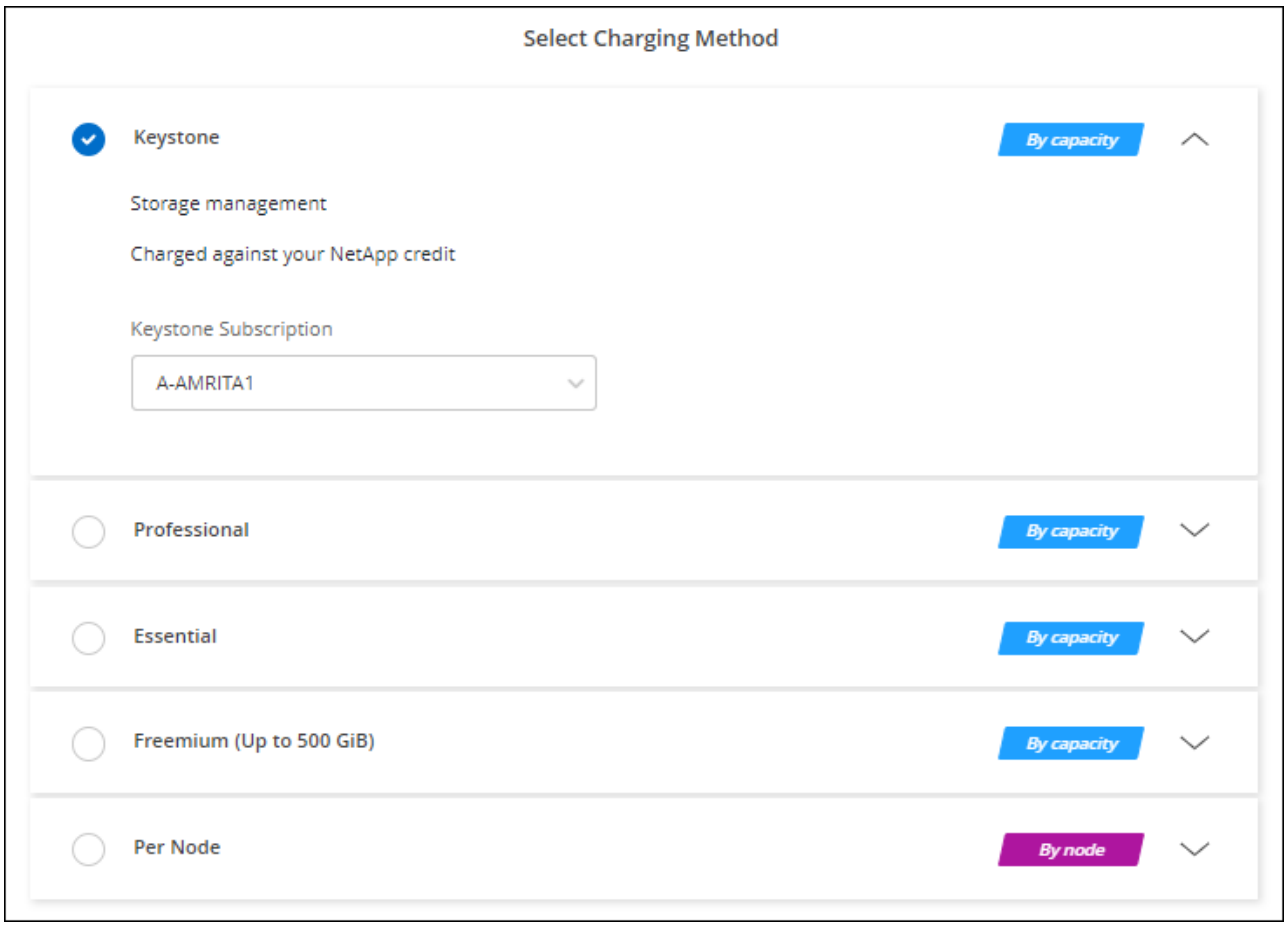
Keystoneサブスクリプション

Keystoneサブスクリプションは、成長に応じて支払うサブスクリプション ベースのサービスです。"NetApp Keystoneサブスクリプションの詳細" 。

手順

1. まだ購読していない場合は、 "ネットアップに連絡"
2. NetAppにお問い合わせください に連絡して、コンソールで 1 つ以上のKeystoneサブスクリプションを使用してユーザー アカウントを承認します。
3. NetAppがアカウントを承認すると、"Cloud Volumes ONTAPで使用するためにサブスクリプションをリンクします" 。
4. *システム*ページで*システムの追加*をクリックし、手順に従います。

a. 課金方法を選択するように求められたら、 Keystoneサブスクリプションの課金方法を選択します。



"AzureでCloud Volumes ONTAPを起動するための手順を見る" 。

ノードベースのライセンス

ノードベースライセンスは、Cloud Volumes ONTAPの旧世代ライセンスです。ノードベースライセンスはNetApp （BYOL）から取得でき、特定のケースに限りライセンス更新に利用できます。詳細については、以下を参照してください。

- "ノードベースライセンスの提供終了"
- "ノードベースライセンスの提供終了"
- "ノードベースのライセンスを容量ベースのライセンスに変換する"

Azureで**Cloud Volumes ONTAP**の高可用性モードを有効にする

予期しないフェイルオーバー時間を削減し、Cloud Volumes ONTAP の NFSv4 サポートを有効にするには、Microsoft Azure の高可用性（HA）モードを有効にする必要があります。このモードを有効にすると、Cloud Volumes ONTAP HA ノードは、CIFS および NFSv4 クライアントでの計画外のフェイルオーバー時に、低い（60 秒）復旧時間目標（RTO）を達成できます。

Cloud Volumes ONTAP 9.10.1 以降では、Microsoft Azure で実行されているCloud Volumes ONTAP HA ペア

の計画外のフェイルオーバー時間を短縮し、NFSv4 のサポートを追加しました。これらの拡張機能をCloud Volumes ONTAPで利用できるようにするには、Azure サブスクリプションで高可用性機能を有効にする必要があります。

タスク概要

NetApp Console は、Azure サブスクリプションで機能を有効にする必要がある場合、これらの詳細を表示します。次の点に注意してください：

- Cloud Volumes ONTAP HA ペアの高可用性に問題はありません。この Azure 機能はONTAPと連携して動作し、計画外のフェイルオーバー イベントによって発生する NFS プロトコルのクライアントで観測されるアプリケーション停止時間を短縮します。
- この機能を有効にしても、 Cloud Volumes ONTAP HA ペアは中断されません。
- Azure サブスクリプションでこの機能を有効にしても、他の VM に問題は発生しません。
- Cloud Volumes ONTAP は、 CIFS および NFS クライアント上のクラスターおよび SVM 管理 LIF のフェイルオーバー中に内部 Azure ロード バランサーを使用します。
- HA モードが有効になっている場合、コンソールは 12 時間ごとにシステムをスキャンして、Azure Load Balancer の内部ルールを更新します。

手順

Owner 権限を持つ Azure ユーザーは、Azure CLI からこの機能を有効にできます。

1. "Azure ポータルから Azure Cloud Shell にアクセスする"
2. 高可用性モード機能を登録します。

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. 必要に応じて、機能が登録されたことを確認します。

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Azure CLI は次のような結果を返すはずです。

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

関連リンク

1. "Microsoft Azure ドキュメント：高可用性ポートの概要"
2. "Microsoft Azure ドキュメント：Azure CLI の使用を開始する"

Azure でCloud Volumes ONTAPの VMOrchestratorZonalMultiFD を有効にする

ローカル冗長ストレージ（LRS）の単一アベイラビリティゾーン（AZ）にVMインスタンスを展開するには、Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD`サブスクリプションの機能。高可用性 (HA) モードでは、この機能により、同じ可用性ゾーン内の別々の障害ドメインにノードを展開することが容易になります。

この機能を有効にしないと、ゾーン展開は行われず、以前の LRS 非ゾーン展開が有効になります。

単一のアベイラビリティゾーンでのVMの展開については、以下を参照してください。"Azureのハイアベイラビリティ ペア" 。

「所有者」権限を持つユーザーとして次の手順を実行します。

手順

1. Azure ポータルから Azure Cloud Shell にアクセスします。詳細については、 "Microsoft Azure ドキュメント: Azure Cloud Shell の使用を開始する" 。
2. 登録する `Microsoft.Compute/VMOrchestratorZonalMultiFD`次のコマンドを実行して機能を有効にします。

   az account set -s <*Azure* サブスクリプション名または *ID*> az feature register --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute

3. 登録ステータスと出力サンプルを確認します。

```
az feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute { "id":
"/subscriptions/<ID>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestra
torZonalMultiFD", "name": "Microsoft.Compute/VMOrchestratorZonalMultiFD", "properties": { "state": "
登録済み" }, "type": "Microsoft.Features/providers/features" }
```

Azureで**Cloud Volumes ONTAP**を起動する

Azureで単一ノードシステムまたはHAペアを起動するには、NetApp ConsoleでCloud Volumes ONTAPシステムを作成します。

開始する前に

始める前に以下のものが必要です。

- 稼働中のコンソール エージェント。
  - あなたは "システムに関連付けられたコンソールエージェント"。
  - "コンソールエージェントを常に実行しておく必要があります" 。
- 使用する構成を理解すること。

  構成を計画し、管理者から必要な Azure ネットワークの詳細を入手する必要があります。詳細については、 "Cloud Volumes ONTAP構成の計画" 。
- Cloud Volumes ONTAPのライセンスを設定するために必要なことを理解していること。

  "ライセンスの設定方法を学ぶ" 。

タスク概要

コンソールが Azure にCloud Volumes ONTAPシステムを作成すると、リソース グループ、ネットワーク インターフェイス、ストレージ アカウントなどのいくつかの Azure オブジェクトが作成されます。ウィザードの最後にリソースの概要を確認できます。

データ損失の可能性

ベスト プラクティスは、各Cloud Volumes ONTAPシステムに新しい専用のリソース グループを使用することです。

データ損失のリスクがあるため、既存の共有リソース グループにCloud Volumes ONTAPをデプロイすることはお勧めしません。コンソールは、デプロイメントの失敗または削除の際に共有リソース グループからCloud Volumes ONTAPリソースを削除できますが、Azure ユーザーが誤って共有リソース グループからCloud Volumes ONTAPリソースを削除してしまう可能性があります。

Azure でシングルノードの**Cloud Volumes ONTAP**システムを起動する

Azure で単一ノードの Cloud Volumes ONTAP システムを起動する場合は、コンソールで単一ノード システムを作成する必要があります。

手順

1. 左側のナビゲーション メニューから、ストレージ > 管理 を選択します。
2. *システム*ページで、*システムの追加*をクリックし、指示に従います。
3. 場所の選択: **Microsoft Azure** と * Cloud Volumes ONTAP Single Node* を選択します。
4. プロンプトが表示されたら、 "コンソールエージェントを作成する" 。
5. 詳細と資格情報: 必要に応じて Azure の資格情報とサブスクリプションを変更し、クラスター名を指定し、必要に応じてタグを追加して、資格情報を指定します。

   次の表では、ガイダンスが必要になる可能性のあるフィールドについて説明します。

フィールド	説明
システム名	コンソールは、システム名を使用して、 Cloud Volumes ONTAPシステムと Azure 仮想マシンの両方に名前を付けます。このオプションを選択した場合、定義済みのセキュリティ グループのプレフィックスとしても名前が使用されます。
リソースグループタグ	タグは、Azure リソースのメタデータです。このフィールドにタグを入力すると、コンソールはそれらをCloud Volumes ONTAPシステムに関連付けられたリソース グループに追加します。システムを作成するときに、ユーザー インターフェイスから最大 4 つのタグを追加でき、システムの作成後にさらにタグを追加できます。システムを作成するときに、API ではタグが 4 つに制限されないことに注意してください。タグの詳細については、 "Microsoft Azure ドキュメント: タグを使用して Azure リソースを整理する" 。
ユーザ名とパスワード	これらは、Cloud Volumes ONTAPクラスター管理者アカウントの資格情報です。これらの資格情報を使用して、 ONTAP System Manager またはONTAP CLI を介してCloud Volumes ONTAPに接続できます。デフォルトの *admin* ユーザー名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。
資格情報の編集	このCloud Volumes ONTAPシステムで使用するために、異なる Azure 資格情報と異なる Azure サブスクリプションを選択できます。従量課金制のCloud Volumes ONTAPシステムを展開するには、Azure Marketplace サブスクリプションを選択した Azure サブスクリプションに関連付ける必要があります。 "資格情報を追加する方法を学ぶ" 。

6. サービス: Cloud Volumes ONTAPで使用する、または使用しないサービスを個別に有効または無効にします。
   - "NetApp Data Classificationの詳細"
   - "NetApp Backup and Recoveryの詳細"

   WORM とデータ階層化を利用する場合は、バックアップとリカバリを無効にし、バージョン 9.8 以降のCloud Volumes ONTAPシステムを展開する必要があります。

7. 場所: リージョン、可用性ゾーン、VNet、サブネットを選択し、チェックボックスをオンにして、コンソール エージェントとターゲットの場所間のネットワーク接続を確認します。

中国地域では、単一ノードの展開はCloud Volumes ONTAP 9.12.1 GA および 9.13.0 GA でのみサポートされます。これらのバージョンは、 Cloud Volumes ONTAPの以降のパッチとリリースにアップグレードできます。"Azureでサポートされています" 。中国地域で新しいバージョンのCloud Volumes ONTAPを展開する場合は、 NetAppサポートにお問い合わせください。中国地域ではNetAppから直接購入したライセンスのみがサポートされており、マーケットプレイスのサブスクリプションは利用できません。

8. 接続: 新しいリソース グループまたは既存のリソース グループを選択し、定義済みのセキュリティ グループを使用するか、独自のセキュリティ グループを使用するかを選択します。

   次の表では、ガイダンスが必要になる可能性のあるフィールドについて説明します。

フィールド	説明
Resource Group	Cloud Volumes ONTAPの新しいリソース グループを作成するか、既存のリソース グループを使用します。ベストプラクティスは、 Cloud Volumes ONTAP専用の新しいリソースグループを使用することです。 Cloud Volumes ONTAPを既存の共有リソース グループにデプロイすることは可能ですが、データ損失のリスクがあるためお勧めしません。詳細については上記の警告を参照してください。 使用しているAzureアカウントに "必要な権限"、コンソールは、デプロイメントの失敗または削除の場合に、リソース グループからCloud Volumes ONTAPリソースを削除します。
生成されたセキュリティ グループ	コンソールでセキュリティ グループを生成させる場合は、トラフィックを許可する方法を選択する必要があります。 • 選択した **VNet** のみ を選択した場合、受信トラフィックのソースは、選択した VNet のサブネット範囲と、コンソール エージェントが存在する VNet のサブネット範囲になります。これは推奨されるオプションです。 • すべての **VNet** を選択した場合、受信トラフィックのソースは 0.0.0.0/0 IP 範囲になります。
既存のものを使用する	既存のセキュリティ グループを選択する場合は、 Cloud Volumes ONTAP の要件を満たしている必要があります。"デフォルトのセキュリティ グループを表示する" 。

9. 課金方法と **NSS** アカウント: このシステムで使用する課金オプションを指定し、 NetAppサポート サイト 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学ぶ" 。
   - "ライセンスの設定方法を学ぶ" 。
10. 事前構成済みパッケージ: パッケージの 1 つを選択してCloud Volumes ONTAPシステムをすばやく展開するか、*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構成を確認し、承認するだけです。

11. ライセンス: 必要に応じてCloud Volumes ONTAP のバージョンを変更し、仮想マシンの種類を選択します。

選択したバージョンに対して新しいリリース候補、一般提供、またはパッチ リリースが利用可能な場合、 BlueXP は作業環境を作成するときにシステムをそのバージョンに更新します。たとえば、 Cloud Volumes ONTAP 9.16.1 P3 を選択し、9.16.1 P4 が利用可能な場合は更新が行われます。更新は、あるリリースから別のリリース (たとえば、9.15 から 9.16) には行われません。

12. **Azure Marketplace** からサブスクライブ: コンソールがCloud Volumes ONTAPのプログラムによるデプロイメントを有効にできなかった場合、このページが表示されます。画面に表示される手順に従ってください。 "マーケットプレイス製品のプログラムによる展開"詳細についてはこちらをご覧ください。
13. 基盤となるストレージ リソース: 初期集約の設定 (ディスク タイプ、各ディスクのサイズ、Blob ストレージへのデータ階層化を有効にするかどうか) を選択します。

    次の点に注意してください。

    - VNet 内でストレージ アカウントへのパブリック アクセスが無効になっている場合、 Cloud Volumes ONTAPシステムでデータ階層化を有効にすることはできません。詳細については、"セキュリティグループルール" 。
    - ディスク タイプは初期ボリューム用です。後続のボリュームには異なるディスク タイプを選択できます。
    - ディスク サイズは、初期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 オプションを使用するときにコンソールが作成する追加のアグリゲートのすべてのディスクに適用されます。高度な割り当てオプションを使用して、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、以下を参照してください。"Azure でのシステムのサイズ設定" 。
    - 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。
    - データ階層化を無効にした場合、後続の集約で有効にすることができます。

      "データ階層化の詳細" 。
14. 書き込み速度と**WORM**:

    a. 必要に応じて、「通常」または「高速」の書き込み速度を選択します。

       "書き込み速度について詳しくはこちら" 。

    b. 必要に応じて、一度書き込み、何度も読み取り可能な (WORM) ストレージをアクティブ化します。

       このオプションは特定の VM タイプでのみ使用できます。サポートされているVMタイプを確認するには、以下を参照してください。"HAペアのライセンスでサポートされる構成" 。

       Cloud Volumes ONTAPバージョン 9.7 以下でデータ階層化が有効になっている場合、WORM を有効にすることはできません。 WORM と階層化を有効にした後、 Cloud Volumes ONTAP 9.8 への復元またはダウングレードはブロックされます。

    "WORMストレージについて詳しくはこちら" 。

    a. WORM ストレージを有効にする場合は、保持期間を選択します。

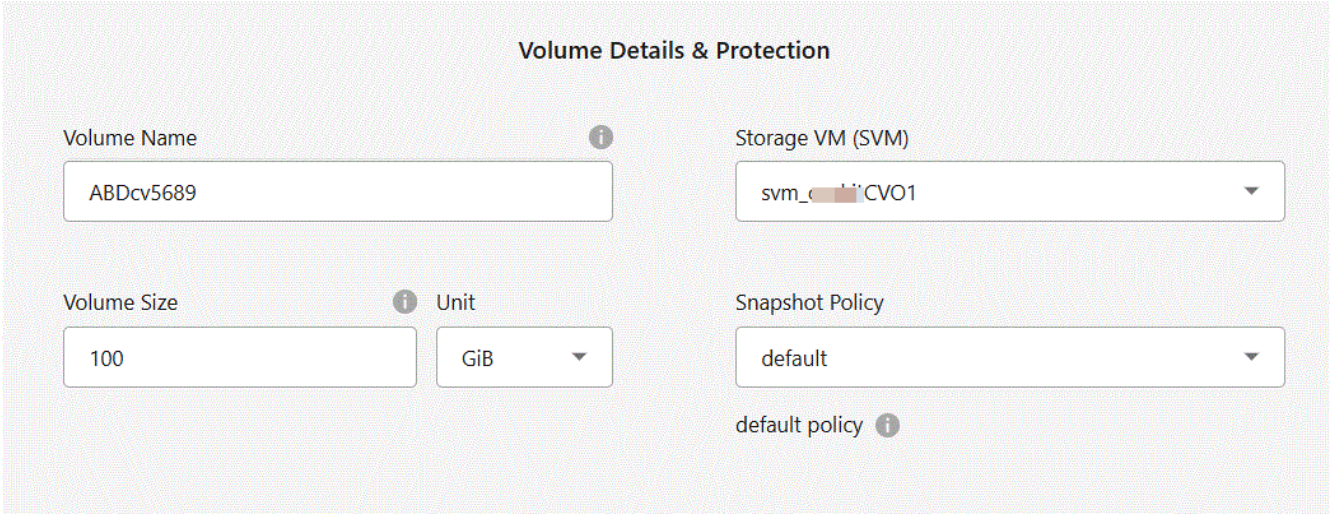
15. ボリュームの作成: 新しいボリュームの詳細を入力するか、[スキップ] をクリックします。

"サポートされているクライアントプロトコルとバージョンについて学ぶ" 。

このページのいくつかのフィールドは説明不要です。次の表では、ガイダンスが必要になる可能性のある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な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、コンソール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、ユーザーとグループの共有へのアクセス レベル (アクセス制御リストまたは ACL とも呼ばれます) を制御できます。ローカルまたはドメインの Windows ユーザーまたはグループ、あるいは UNIX ユーザーまたはグループを指定できます。ドメイン Windows ユーザー名を指定する場合は、domain\username の形式を使用してユーザーのドメインを含める必要があります。
スナップショットポリシー	スナップショット コピー ポリシーは、自動的に作成されるNetAppスナップショット コピーの頻度と数を指定します。NetAppスナップショット コピーは、パフォーマンスに影響を与えず、最小限のストレージしか必要としない、ポイントインタイム ファイル システム イメージです。デフォルトのポリシーを選択するか、ポリシーなしを選択できます。一時データの場合は none を選択できます (例: Microsoft SQL Server の場合は tempdb)。
詳細オプション（NFSのみ）	ボリュームの NFS バージョン (NFSv3 または NFSv4) を選択します。
イニシエーター 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供されます。イニシエーター グループは、iSCSI ホスト ノード名のテーブルであり、どのイニシエーターがどの 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 Ethernet ネットワーク アダプター (NIC)、ソフトウェア イニシエーターを備えた TCP オフロード エンジン (TOE) カード、統合ネットワーク アダプター (CNA)、または専用ホスト バス アダプター (HBA) を介してネットワークに接続し、iSCSI 修飾名 (IQN) によって識別されます。 iSCSI ボリュームを作成すると、コンソールによって LUN が自動的に作成されます。ボリュームごとに 1 つの LUN を作成するだけで簡単になるので、管理は不要です。ボリュームを作成したら、"IQNを使用してホストからLUNに接続します" 。

次の画像は、ボリューム作成ウィザードの最初のページを示しています。



16. **CIFS** セットアップ: CIFS プロトコルを選択した場合は、CIFS サーバー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 サーバーの名前解決を提供する DNS サーバーの IP アドレス。これらのDNSサーバには、Active DirectoryのLDAPサーバと、CIFSサーバが参加するドメインのドメイン コントローラを見つけるために必要なサービス 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 サーバーが参加する Active Directory (AD) ドメインの FQDN。
ドメインへの参加を許可された資格情報	AD ドメイン内の指定された組織単位 (OU) にコンピューターを追加するのに十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS server NetBIOS name	AD ドメイン内で一意の CIFS サーバー名。
組織単位	CIFS サーバーに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。 Azure AD Domain Services をCloud Volumes ONTAP の AD サーバーとして構成するには、このフィールドに **OU=AADDC Computers** または **OU=AADDC Users** を入力する必要があります。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure ドキュメント: Azure AD Domain Services マネージド ドメインに組織単位 (OU) を作成する"^]
DNSドメイン	Cloud Volumes ONTAPストレージ仮想マシン (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 サーバーを構成するには、「**Active Directory** ドメインを使用する」を選択します。別のアドレスを使用して NTP サーバーを構成する必要がある場合は、API を使用する必要があります。参照 "NetApp Console自動化ドキュメント"詳細については。 NTP サーバーを設定できるのは、CIFS サーバーを作成するときだけであることに注意してください。 CIFS サーバーを作成した後は構成できません。

17. 使用プロファイル、ディスク タイプ、階層化ポリシー: 必要に応じて、ストレージ効率機能を有効にするかどうか、およびボリューム階層化ポリシーを変更するかどうかを選択します。

    詳細については、"ボリューム使用プロファイルの理解"そして"データ階層化の概要"。

18. 確認と承認: 選択内容を確認して確定します。
    a. 構成の詳細を確認します。
    b. 詳細情報 をクリックすると、サポートとコンソールが購入する Azure リソースの詳細を確認できます。
    c. 理解しました... チェックボックスを選択します。
    d. [Go] をクリックします。

結果

コンソールはCloud Volumes ONTAPシステムを展開します。監査ページで進捗状況を追跡できます。

Cloud Volumes ONTAPシステムのデプロイ中に問題が発生した場合は、失敗メッセージを確認してください。システムを選択して、「環境の再作成」をクリックすることもできます。

さらに詳しいヘルプについては、 "NetApp Cloud Volumes ONTAPサポート" 。

> デプロイ プロセスが完了したら、Azure ポータルでシステムによって生成されたCloud Volumes ONTAP構成、特にシステム タグを変更しないでください。これらの構成に変更を加えると、予期しない動作やデータ損失が発生する可能性があります。

終了後の操作

- 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、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てください。
- ボリュームにクォータを適用する場合は、 ONTAP System Manager またはONTAP CLI を使用します。

  クォータを使用すると、ユーザー、グループ、または qtree が使用するディスク領域とファイル数を制限したり追跡したりできます。

AzureでCloud Volumes ONTAP HAペアを起動する

Azure でCloud Volumes ONTAP HA ペアを起動する場合は、コンソールで HA システムを作成する必要があります。

手順

1. 左側のナビゲーション メニューから、ストレージ > 管理 を選択します。
2. *システム*ページで、*システムの追加*をクリックし、指示に従います。
3. プロンプトが表示されたら、 "コンソールエージェントを作成する" 。
4. 詳細と資格情報: 必要に応じて Azure の資格情報とサブスクリプションを変更し、クラスター名を指定し、必要に応じてタグを追加して、資格情報を指定します。

   次の表では、ガイダンスが必要になる可能性のあるフィールドについて説明します。

フィールド	説明
システム名	コンソールは、システム名を使用して、 Cloud Volumes ONTAPシステムと Azure 仮想マシンの両方に名前を付けます。このオプションを選択した場合、定義済みのセキュリティ グループのプレフィックスとしても名前が使用されます。

フィールド	説明
リソースグループタグ	タグは、Azure リソースのメタデータです。このフィールドにタグを入力すると、コンソールはそれらをCloud Volumes ONTAPシステムに関連付けられたリソース グループに追加します。システムを作成するときに、ユーザー インターフェイスから最大 4 つのタグを追加でき、システムの作成後にさらにタグを追加できます。システムを作成するときに、API ではタグが 4 つに制限されないことに注意してください。タグの詳細については、 "Microsoft Azure ドキュメント: タグを使用して Azure リソースを整理する" 。
ユーザ名とパスワード	これらは、Cloud Volumes ONTAPクラスター管理者アカウントの資格情報です。これらの資格情報を使用して、 ONTAP System Manager またはONTAP CLI を介してCloud Volumes ONTAPに接続できます。デフォルトの *admin* ユーザー名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。
資格情報の編集	このCloud Volumes ONTAPシステムで使用するために、異なる Azure 資格情報と異なる Azure サブスクリプションを選択できます。従量課金制のCloud Volumes ONTAPシステムを展開するには、Azure Marketplace サブスクリプションを選択した Azure サブスクリプションに関連付ける必要があります。 "資格情報を追加する方法を学ぶ" 。

5. サービス: Cloud Volumes ONTAPで使用するかどうかに基づいて、個々のサービスを有効または無効にします。
   - "NetApp Data Classificationの詳細"
   - "NetApp Backup and Recoveryの詳細"

   WORM とデータ階層化を利用する場合は、バックアップとリカバリを無効にし、バージョン 9.8 以降のCloud Volumes ONTAPシステムを展開する必要があります。

6. **HA** 展開モデル:
   a. *単一のアベイラビリティーゾーン*または*複数のアベイラビリティーゾーン*を選択します。
      - 単一の可用性ゾーンの場合は、Azure リージョン、可用性ゾーン、VNet、サブネットを選択します。

        Cloud Volumes ONTAP 9.15.1 以降では、Azure の単一の可用性ゾーン (AZ) に HA モードで仮想マシン (VM) インスタンスをデプロイできます。このデプロイメントをサポートするゾーンとリージョンを選択する必要があります。ゾーンまたはリージョンがゾーン展開をサポートしていない場合は、LRS の以前の非ゾーン展開モードが適用されます。共有管理ディスクのサポートされている構成については、以下を参照してください。"共有マネージドディスクを使用した HA 単一アベイラビリティゾーン構成" 。
      - 複数の可用性ゾーンの場合は、リージョン、VNet、サブネット、ノード 1 のゾーン、ノード 2 のゾーンを選択します。

   b. ネットワーク接続を確認しました... チェックボックスを選択します。
7. 接続: 新しいリソース グループまたは既存のリソース グループを選択し、定義済みのセキュリティ グループを使用するか、独自のセキュリティ グループを使用するかを選択します。

   次の表では、ガイダンスが必要になる可能性のあるフィールドについて説明します。

フィールド	説明
Resource Group	Cloud Volumes ONTAPの新しいリソース グループを作成するか、既存のリソース グループを使用します。ベストプラクティスは、 Cloud Volumes ONTAP専用の新しいリソースグループを使用することです。 Cloud Volumes ONTAPを既存の共有リソース グループにデプロイすることは可能ですが、データ損失のリスクがあるためお勧めしません。詳細については上記の警告を参照してください。 Azure にデプロイするCloud Volumes ONTAP HA ペアごとに専用のリソース グループを使用する必要があります。リソース グループでは 1 つの HA ペアのみがサポートされます。 Azure リソース グループに 2 番目のCloud Volumes ONTAP HA ペアをデプロイしようとすると、コンソールで接続の問題が発生します。 使用しているAzureアカウントに "必要な権限"、コンソールは、デプロイメントの失敗または削除の場合に、リソース グループからCloud Volumes ONTAPリソースを削除します。
生成されたセキュリティ グループ	コンソールでセキュリティ グループを生成させる場合は、トラフィックを許可する方法を選択する必要があります。 • 選択した **VNet** のみ を選択した場合、受信トラフィックのソースは、選択した VNet のサブネット範囲と、コンソール エージェントが存在する VNet のサブネット範囲になります。これは推奨されるオプションです。 • すべての **VNet** を選択した場合、受信トラフィックのソースは 0.0.0.0/0 IP 範囲になります。
既存のものを使用する	既存のセキュリティ グループを選択する場合は、 Cloud Volumes ONTAP の要件を満たしている必要があります。"デフォルトのセキュリティ グループを表示する" 。

8. 課金方法と **NSS** アカウント: このシステムで使用する課金オプションを指定し、 NetAppサポート サイト 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学ぶ" 。
   - "ライセンスの設定方法を学ぶ" 。
9. 事前構成済みパッケージ: Cloud Volumes ONTAPシステムをすばやく展開するには、パッケージの 1 つを選択するか、[構成の変更] 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構成を確認し、承認するだけです。
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、仮想マシンの種類を選択します。

    選択したバージョンに対して新しいリリース候補、一般提供、またはパッチ リリースが利用可能な場合、コンソールは作成時にシステムをそのバージョンに更新します。たとえば、 Cloud Volumes ONTAP 9.13.1 を選択し、9.13.1 P4 が利用可能な場合は更新が行われます。更新は、あるリリースから別のリリース (たとえば、9.13 から 9.14) には行われません。

11. **Azure Marketplace** からサブスクライブ: コンソールでCloud Volumes ONTAPのプログラムによるデプロイメントを有効にできなかった場合は、次の手順に従います。
12. 基盤となるストレージ リソース: 初期集約の設定 (ディスク タイプ、各ディスクのサイズ、Blob ストレージへのデータ階層化を有効にするかどうか) を選択します。

    次の点に注意してください。

    - ディスク サイズは、初期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 オプションを使用するときにコンソールが作成する追加のアグリゲートのすべてのディスクに適用されます。高度な割り当てオプションを使用して、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。

      ディスクサイズの選択については、以下を参照してください。"Azure でシステムのサイズを決定する" 。

    - VNet 内でストレージ アカウントへのパブリック アクセスが無効になっている場合、 Cloud Volumes ONTAPシステムでデータ階層化を有効にすることはできません。詳細については、"セキュリティグループルール" 。
    - 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。
    - データ階層化を無効にした場合、後続の集約で有効にすることができます。

      "データ階層化の詳細" 。

    - Cloud Volumes ONTAP 9.15.0P1 以降、新しい高可用性ペアの展開では Azure ページ BLOB はサポートされなくなりました。現在、既存の高可用性ペアの展開で Azure ページ BLOB を使用している場合は、Edsv4 シリーズ VM および Edsv5 シリーズ VM の新しい VM インスタンス タイプに移行できます。

      "Azureでサポートされている構成の詳細" 。

13. 書き込み速度と**WORM**:

    a. 必要に応じて、「通常」または「高速」の書き込み速度を選択します。

       "書き込み速度について詳しくはこちら" 。

    b. 必要に応じて、一度書き込み、何度も読み取り可能な (WORM) ストレージをアクティブ化します。

       このオプションは特定の VM タイプでのみ使用できます。サポートされているVMタイプを確認するには、以下を参照してください。"HAペアのライセンスでサポートされる構成" 。

       Cloud Volumes ONTAPバージョン 9.7 以下でデータ階層化が有効になっている場合、WORM を有効にすることはできません。 WORM と階層化を有効にした後、 Cloud Volumes ONTAP 9.8 への復元またはダウングレードはブロックされます。

    "WORMストレージについて詳しくはこちら" 。

    a. WORM ストレージを有効にする場合は、保持期間を選択します。

14. ストレージと **WORM** への安全な通信: Azure ストレージ アカウントへの HTTPS 接続を有効にするかどうかを選択し、必要に応じて、一度書き込み、複数回読み取り (WORM) ストレージをアクティブ化します。

HTTPS 接続は、Cloud Volumes ONTAP 9.7 HA ペアから Azure ページ BLOB ストレージ アカウントへ行われます。このオプションを有効にすると書き込みパフォーマンスに影響する可能性があることに注意してください。システムを作成した後は設定を変更できません。

"WORMストレージについて詳しくはこちら" 。

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

"WORMストレージについて詳しくはこちら" 。

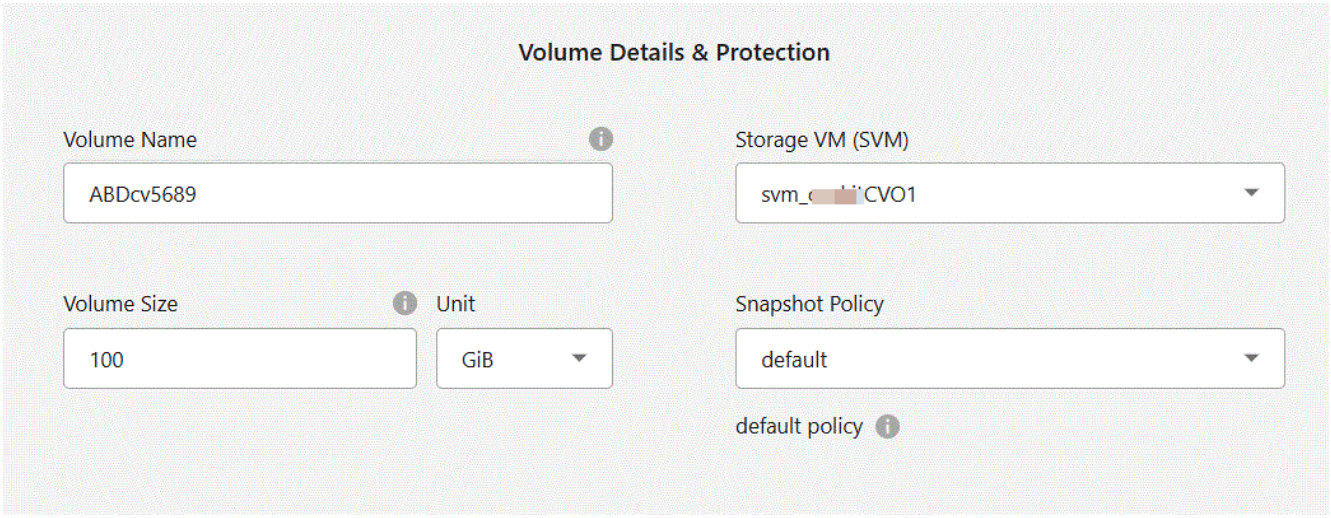
15. ボリュームの作成: 新しいボリュームの詳細を入力するか、[スキップ] をクリックします。

"サポートされているクライアントプロトコルとバージョンについて学ぶ" 。

このページのいくつかのフィールドは説明不要です。次の表では、ガイダンスが必要になる可能性のある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な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、コンソール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、ユーザーとグループの共有へのアクセス レベル (アクセス制御リストまたは ACL とも呼ばれます) を制御できます。ローカルまたはドメインの Windows ユーザーまたはグループ、あるいは UNIX ユーザーまたはグループを指定できます。ドメイン Windows ユーザー名を指定する場合は、domain\username の形式を使用してユーザーのドメインを含める必要があります。
スナップショットポリシー	スナップショット コピー ポリシーは、自動的に作成されるNetAppスナップショット コピーの頻度と数を指定します。NetAppスナップショット コピーは、パフォーマンスに影響を与えず、最小限のストレージしか必要としない、ポイントインタイム ファイル システム イメージです。デフォルトのポリシーを選択するか、ポリシーなしを選択できます。一時データの場合は none を選択できます (例: Microsoft SQL Server の場合は tempdb)。
詳細オプション（NFSのみ）	ボリュームの NFS バージョン (NFSv3 または NFSv4) を選択します。
イニシエーター 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供されます。イニシエーター グループは、iSCSI ホスト ノード名のテーブルであり、どのイニシエーターがどの 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 Ethernet ネットワーク アダプター (NIC)、ソフトウェア イニシエーターを備えた TCP オフロード エンジン (TOE) カード、統合ネットワーク アダプター (CNA)、または専用ホスト バス アダプター (HBA) を介してネットワークに接続し、iSCSI 修飾名 (IQN) によって識別されます。 iSCSI ボリュームを作成すると、コンソールによって LUN が自動的に作成されます。ボリュームごとに 1 つの LUN を作成するだけで簡単になるので、管理は不要です。ボリュームを作成したら、"IQNを使用してホストからLUNに接続します" 。

次の画像は、ボリューム作成ウィザードの最初のページを示しています。



16. **CIFS** セットアップ: CIFS プロトコルを選択した場合は、CIFS サーバー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 サーバーの名前解決を提供する DNS サーバーの IP アドレス。これらのDNSサーバには、Active DirectoryのLDAPサーバと、CIFSサーバが参加するドメインのドメイン コントローラを見つけるために必要なサービス 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 サーバーが参加する Active Directory (AD) ドメインの FQDN。
ドメインへの参加を許可された資格情報	AD ドメイン内の指定された組織単位 (OU) にコンピューターを追加するのに十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS server NetBIOS name	AD ドメイン内で一意の CIFS サーバー名。
組織単位	CIFS サーバーに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。 Azure AD Domain Services をCloud Volumes ONTAP の AD サーバーとして構成するには、このフィールドに **OU=AADDC Computers** または **OU=AADDC Users** を入力する必要があります。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure ドキュメント: Azure AD Domain Services マネージド ドメインに組織単位 (OU) を作成する"^]
DNSドメイン	Cloud Volumes ONTAPストレージ仮想マシン (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 サーバーを構成するには、「**Active Directory** ドメインを使用する」を選択します。別のアドレスを使用して NTP サーバーを構成する必要がある場合は、API を使用する必要があります。参照 "NetApp Console自動化ドキュメント"詳細については。 NTP サーバーを設定できるのは、CIFS サーバーを作成するときだけであることに注意してください。 CIFS サーバーを作成した後は構成できません。

17. 使用プロファイル、ディスク タイプ、階層化ポリシー: 必要に応じて、ストレージ効率機能を有効にするかどうか、およびボリューム階層化ポリシーを変更するかどうかを選択します。

詳細については、"ボリューム使用プロファイルを選択する" 、"データ階層化の概要" 、 そして "KB: CVO ではどのようなインライン ストレージ効率機能がサポートされていますか?"

18. 確認と承認: 選択内容を確認して確定します。
    a. 構成の詳細を確認します。
    b. 詳細情報 をクリックすると、サポートとコンソールが購入する Azure リソースの詳細を確認できます。
    c. 理解しました... チェックボックスを選択します。
    d. [Go] をクリックします。

結果

コンソールはCloud Volumes ONTAPシステムを展開します。監査ページで進捗状況を追跡できます。

Cloud Volumes ONTAPシステムのデプロイ中に問題が発生した場合は、失敗メッセージを確認してください。システムを選択して、「環境の再作成」をクリックすることもできます。

さらに詳しいヘルプについては、 "NetApp Cloud Volumes ONTAPサポート" 。

終了後の操作

- 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、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てください。
- ボリュームにクォータを適用する場合は、 ONTAP System Manager またはONTAP CLI を使用します。

  クォータを使用すると、ユーザー、グループ、または qtree が使用するディスク領域とファイル数を制限したり追跡したりできます。

デプロイ プロセスが完了したら、Azure ポータルでシステムによって生成されたCloud Volumes ONTAP構成、特にシステム タグを変更しないでください。これらの構成に変更を加えると、予期しない動作やデータ損失が発生する可能性があります。

関連リンク

*"Azure でのCloud Volumes ONTAP構成の計画" *"Azure MarketplaceからAzureにCloud Volumes ONTAPをデプロイする"

Azure プラットフォーム イメージの検証

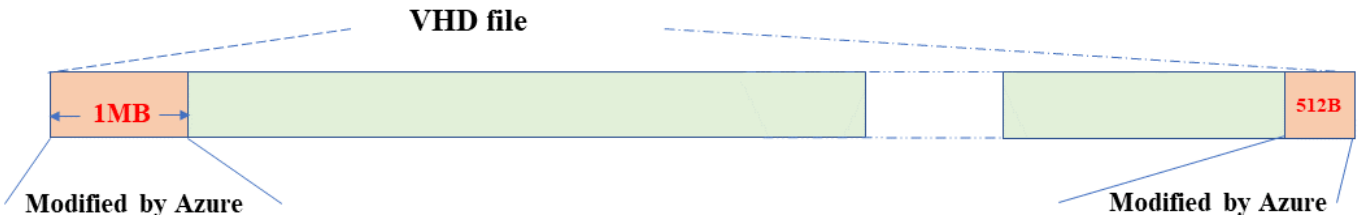
Cloud Volumes ONTAPの Azure Marketplace イメージ検証

Azure イメージ検証は、強化されたNetAppセキュリティ要件に準拠しています。画像ファイルの検証は簡単なプロセスです。ただし、Azure イメージ署名の検証では、Azure マーケットプレイスで変更されるため、Azure VHD イメージ ファイルに対して特定の考慮が必要になります。

Azure イメージ検証は、Cloud Volumes ONTAP 9.15.0 以降でサポートされています。

Azure による公開 **VHD** ファイルの変更

VHD ファイルの先頭の 1 MB (1048576 バイト) と末尾の 512 バイトは、Azure によって変更されます。 NetApp は残りの VHD ファイルに署名します。



この例では、VHD ファイルは 10 GB です。 NetAppが署名した部分は緑色でマークされています (10 GB - 1 MB - 512 バイト)。

関連リンク

- "ページフォールトブログ: OpenSSL を使った署名と検証の方法"
- "Azure Marketplace イメージを使用して、Azure Stack Edge Pro GPU 用の VM イメージを作成する | Microsoft Learn"
- "Azure CLI を使用してマネージド ディスクをストレージ アカウントにエクスポート/コピーする | Microsoft Learn"
- "Azure Cloud Shell クイックスタート - Bash | Microsoft Learn"
- "Azure CLI のインストール方法 | Microsoft Learn"
- "az storage blob コピー | Microsoft Learn"
- "Azure CLI でSign in- ログインと認証 | Microsoft Learn"

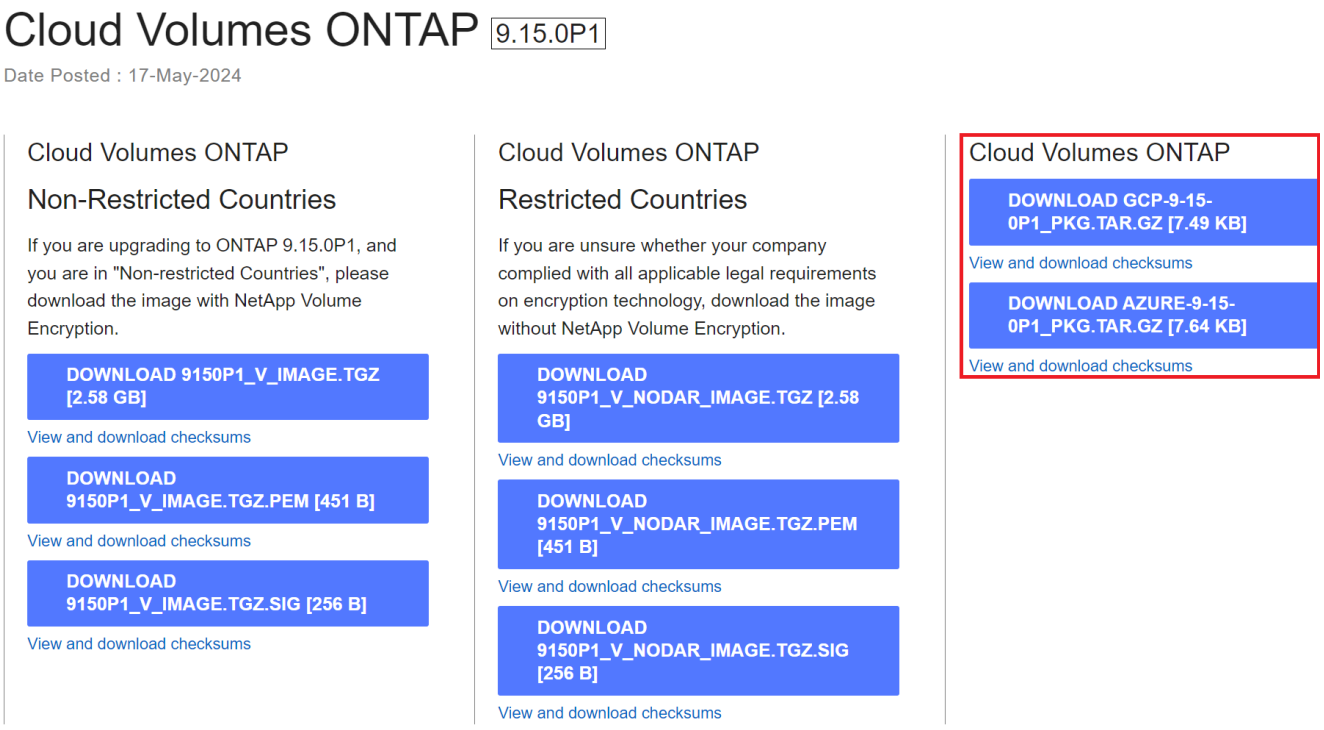
Cloud Volumes ONTAP用の **Azure** イメージ ファイルをダウンロードします。

Azureイメージファイルは、 "NetAppサポート サイト" 。

tar.gz ファイルには、イメージ署名の検証に必要なファイルが含まれています。 *tar.gz* ファイルと一緒に、イメージの *checksum* ファイルもダウンロードする必要があります。チェックサムファイルには、 `md5`そして `sha256`*tar.gz* ファイルのチェックサム。

手順

1. に行く "NetAppサポート サイトのCloud Volumes ONTAP製品ページ"*ダウンロード*セクションから必要なソフトウェア バージョンをダウンロードします。
2. Cloud Volumes ONTAP のダウンロード ページで、Azure イメージのダウンロード可能なファイルをクリックし、*tar.gz* ファイルをダウンロードします。



3. Linuxでは、 `md5sum AZURE-<version>_PKG.TAR.GZ` 。

   macOSでは、 `sha256sum AZURE-<version>_PKG.TAR.GZ` 。

4. 確認するには `md5sum`そして `sha256sum`値は、ダウンロードした Azure イメージの値と一致します。
5. LinuxおよびmacOSでは、 `tar -xzf`指示。

   抽出された *tar.gz* ファイルには、ダイジェスト (*.sig*) ファイル、公開鍵証明書 (*.pem*) ファイル、およびチェーン証明書 (*.pem*) ファイルが含まれています。

   tar.gz ファイルを抽出した後の出力例:

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

Azureマーケットプレイスから**Cloud Volumes ONTAP**の**VHD**イメージをエクスポートする

VHD イメージが Azure クラウドに公開されると、 NetAppによって管理されなくなります。代わりに、公開されたイメージは Azure マーケットプレイスに配置されます。イメージが Azure マーケットプレイスにステージングされ公開されると、Azure は VHD の先頭の 1 MB と末尾の 512 バイトを変更します。 VHD ファイルの署名を検証するには、Azure によって変更された VHD イメージを Azure マーケットプレイスからエクス

ポートする必要があります。

開始する前に

Azure CLI がシステムにインストールされていること、または Azure ポータルから Azure Cloud Shell が利用できることを確認してください。 Azure CLIのインストール方法の詳細については、 "Microsoft ドキュメント: Azure CLI のインストール方法" 。

手順

1. *version_readme* ファイルの内容を使用して、システム上のCloud Volumes ONTAPバージョンを Azure マーケットプレイスのイメージ バージョンにマッピングします。 Cloud Volumes ONTAPのバージョンは次のように表されます。 `buildname` Azureマーケットプレイスイメージバージョンは次のように表されます。 `version`バージョン マッピングで。

   次の例では、 Cloud Volumes ONTAPバージョン `9.15.0P1`Azureマーケットプレイスのイメージバージョンにマッピングされます `9150.01000024.05090105`。この Azure マーケットプレイスのイメージバージョンは、後でイメージ URN を設定するために使用されます。

   ```
   [
    "buildname": "9.15.0P1",
       "publisher": "netapp",
        "version": "9150.01000024.05090105"

   ]
   ```

2. VM を作成するリージョンを特定します。地域名は、 `locName`マーケットプレイスイメージの URN を設定するときに使用する変数。利用可能なリージョンを一覧表示するには、次のコマンドを実行します。

   ```
   az account list-locations -o table
   ```

   この表では、地域名は `Name`分野。

   ```
   $ az account list-locations -o table
   DisplayName               Name                 RegionalDisplayName
   ------------------------  -------------------
   -----------------------------------
   East US                   eastus               (US) East US
   East US 2                 eastus2              (US) East US 2
   South Central US          southcentralus       (US) South Central US
   ...
   ```

3. 以下の表で、対応するCloud Volumes ONTAPバージョンと VM 展開タイプの SKU 名を確認します。 SKU 名は、 `skuName`マーケットプレイスイメージの URN を設定するときに使用する変数。

   たとえば、 Cloud Volumes ONTAP 9.15.0を使用したすべてのシングルノード展開では、 `ontap_cloud_byol` SKU 名として。

* Cloud Volumes ONTAPバージョン*	**VM**の展開	**SKU**名
9.17.1以降	Azureマーケットプレイス	ontap_cloud_direct_gen2
9.17.1以降	NetApp Console	ontap_cloud_gen2
9.16.1	Azureマーケットプレイス	ontap_cloud_direct
9.16.1	コンソール	オンタップクラウド
9.15.1	コンソール	オンタップクラウド
9.15.0	コンソール、単一ノードの展開	ontap_cloud_byol
9.15.0	コンソール、高可用性（HA）展開	ontap_cloud_byol_ha

4. ONTAPバージョンと Azure マーケットプレイス イメージをマッピングした後、Azure Cloud Shell または Azure CLI を使用して Azure マーケットプレイスから VHD ファイルをエクスポートします。

Linux 上の **Azure Cloud Shell** を使用して **VHD** ファイルをエクスポートする

Azure Cloud Shell から、マーケットプレイス イメージを VHD ファイル (たとえば、*9150.01000024.05090105.vhd*) にエクスポートし、ローカル Linux システムにダウンロードします。Azure マーケットプレイスから VHD イメージを取得するには、次の手順を実行します。

手順

1. マーケットプレイス イメージの URN とその他のパラメータを設定します。 URN形式は `<publisher>:<offer>:<sku>:<version>`。必要に応じて、 NetAppマーケットプレイスのイメージを一覧表示して、正しいイメージ バージョンを確認できます。

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. 一致するイメージ バージョンを持つマーケットプレイス イメージから新しいマネージド ディスクを作成します。

```
PS /home/user1> $diskName = “9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = “fnf1”
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
```

3. マネージド ディスクから VHD ファイルを Azure Storage にエクスポートします。適切なアクセス レベルを持つコンテナーを作成します。この例では、 `vm-images`と `Container`アクセス レベル。 Azure ポータルからストレージ アカウントのアクセス キーを取得します: ストレージ アカウント **> *examplesaname*** **>** アクセス キー **> *key1*** **> *key*** **>** 表示 **> *<copy>***

```
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container $containerName
–Context $destContext -Blob $destBlobName
```

4. 生成されたイメージを Linux システムにダウンロードします。使用 `wget`VHD ファイルをダウンロードするコマンド:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

URL は標準形式に従います。自動化のために、以下のように URL 文字列を導出できます。あるいは、Azure CLIを使用することもできます。 `az` URL を取得するコマンド。 URLの例:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. 管理ディスクをクリーンアップする

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Linux 上の Azure CLI を使用して VHD ファイルをエクスポートする

ローカル Linux システムから Azure CLI を使用して、マーケットプレイス イメージを VHD ファイルにエクスポートします。

手順

1. Azure CLI にログインし、マーケットプレイスのイメージを一覧表示します。

```
% az login --use-device-code
```

2. サインインするには、ウェブブラウザを使用してページを開きます https://microsoft.com/devicelogin認証コードを入力します。

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...
```

3. 一致するイメージ バージョンを持つマーケットプレイス イメージから新しいマネージド ディスクを作成します。

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxx"
```

プロセスを自動化するには、標準出力から SAS を抽出する必要があります。ガイダンスについては適切なドキュメントを参照してください。

4. 管理ディスクから VHD ファイルをエクスポートします。

   a. 適切なアクセス レベルを持つコンテナーを作成します。この例では、 `vm-images`と `Container`アクセス レベルが使用されます。

   b. Azure ポータルからストレージ アカウントのアクセス キーを取得します: ストレージ アカウント **> *examplesaname* >** アクセス キー **> *key1* > *key* >** 表示 **> *<copy>***

      また、 `az`このステップのコマンド。

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
-container $containerName --account-name $storageAccountName --account
-key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. BLOB コピーのステータスを確認します。

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. 生成されたイメージを Linux サーバーにダウンロードします。

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

URL は標準形式に従います。自動化のために、以下のように URL 文字列を導出できます。あるいは、Azure CLIを使用することもできます。 `az` URL を取得するコマンド。 URLの例:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. 管理ディスクをクリーンアップする

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

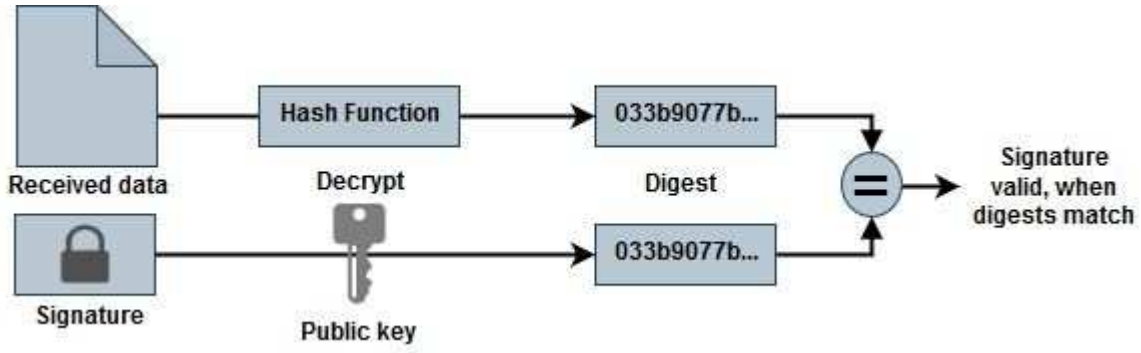
ファイルの署名を検証する

Cloud Volumes ONTAPの **Azure Marketplace** イメージ署名検証

Azure イメージ検証プロセスでは、先頭の 1 MB と末尾の 512 バイトを削除し、ハッシュ関数を適用して、VHD ファイルからダイジェスト ファイルを生成します。署名手順に合わせて、ハッシュには *sha256* が使用されます。

ファイル署名検証ワークフローの概要

以下は、ファイル署名検証ワークフロー プロセスの概要です。



- Azureイメージを "NetAppサポート サイト"ダイジェスト (.sig) ファイル、公開鍵証明書 (.pem) ファイル、チェーン証明書 (.pem) ファイルを抽出します。参照"Azure イメージ ダイジェスト ファイルをダウンロードする"詳細についてはこちらをご覧ください。
- 信頼チェーンの検証。
- 公開鍵証明書 (.pem) から公開鍵 (.pub) を抽出します。
- 抽出された公開鍵を使用してダイジェスト ファイルを復号化します。
- 先頭の 1 MB と末尾の 512 バイトを削除した後、イメージ ファイルから作成された一時ファイルの新しく生成されたダイジェストと結果を比較します。この手順は、OpenSSL コマンドライン ツールを使用して実行されます。 OpenSSL CLI ツールは、ファイルの一致が成功または失敗した場合に適切なメッセージを表示します。

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

Linux 上のCloud Volumes ONTAPの Azure Marketplace イメージ署名を確認する

Linux 上でエクスポートされた VHD ファイル署名の検証には、信頼チェーンの検証、ファイルの編集、署名の検証が含まれます。

手順

1. Azureイメージファイルを以下からダウンロードします。 "NetAppサポート サイト"ダイジェスト (.sig) ファイル、公開鍵証明書 (.pem) ファイル、チェーン証明書 (.pem) ファイルを抽出します。

   参照 "Azure イメージ ダイジェスト ファイルをダウンロードする"詳細についてはこちらをご覧ください。

2. 信頼チェーンを検証します。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. VHD ファイルの先頭の 1 MB (1,048,576 バイト) と末尾の 512 バイトを削除します。使用する場合 `tail、 -c +K`オプションは、ファイルの `K` 番目のバイトからバイトを生成します。したがって、`1048577`は `tail -c。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. OpenSSL を使用して証明書から公開キーを抽出し、署名ファイルと公開キーを使用してストリップされたファイル (sign.tmp) を検証します。

   コマンド プロンプトには、検証に基づいて成功または失敗を示すメッセージが表示されます。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. ワークスペースをクリーンアップします。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

macOS 上の**Cloud Volumes ONTAP**の **Azure Marketplace** イメージ署名を確認する

Linux 上でエクスポートされた VHD ファイル署名の検証には、信頼チェーンの検証、ファイルの編集、署名の検証が含まれます。

手順

1. Azureイメージファイルを以下からダウンロードします。 "NetAppサポート サイト"ダイジェスト (.sig) ファイル、公開鍵証明書 (.pem) ファイル、チェーン証明書 (.pem) ファイルを抽出します。

   参照 "Azure イメージ ダイジェスト ファイルをダウンロードする"詳細についてはこちらをご覧ください。

2. 信頼チェーンを検証します。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. VHD ファイルの先頭の 1 MB (1,048,576 バイト) と末尾の 512 バイトを削除します。使用する場合 `tail、 -c +K`オプションは、ファイルの `K` 番目のバイトからバイトを生成します。したがって、`1048577`は `tail -c`。 macOS では、tail コマンドが完了するまでに約 10 分かかる場合があることに注意してください。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. OpenSSL を使用して証明書から公開キーを抽出し、署名ファイルと公開キーを使用してストリップされたファイル (sign.tmp) を検証します。コマンド プロンプトには、検証に基づいて成功または失敗を示すメッセージが表示されます。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. ワークスペースをクリーンアップします。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Azureマーケットプレイスから**Cloud Volumes ONTAP**をデプロイする

Azure マーケットプレイスの直接展開を使用すると、 Cloud Volumes ONTAP を迅速かつ簡単に展開できます。 Azure マーケットプレイスでは、数回クリックするだけでCloud Volumes ONTAPを迅速に導入し、そのコア機能と機能を自分の環境で試すことができます。

このオファーの詳細については、以下を参照してください。"NetApp ConsoleとマーケットプレイスでCloud Volumes ONTAP のサービスについて学ぶ" 。

タスク概要

Azure マーケットプレイスの直接展開を使用して展開されたCloud Volumes ONTAPシステムには、次のプロパティがあります。 Azure マーケットプレイスを通じてデプロイされたスタンドアロン インスタンスの機能は、NetApp Consoleで検出された時点で変更されることに注意してください。

- 最新のCloud Volumes ONTAPバージョン (9.16.1 以降)。
- プロビジョニングされた容量が 500 GiB に制限されたCloud Volumes ONTAPの無料ライセンス。このライセンスにはNetAppサポートは含まれず、有効期限もありません。
- 単一の可用性ゾーン (AZ) に高可用性 (HA) モードで構成され、デフォルトのシリアル番号でプロビジョニングされた 2 つのノード。ストレージ仮想マシン（ストレージVM）は、"柔軟なオーケストレーションモード" 。
- デフォルトで作成されるインスタンスの集約。
- 500 GiB のプロビジョニング容量を持つ Premium SSD v2 マネージド ディスク、ルート ディスク、およびデータ ディスク。

- NFS、CIFS、iSCSI、NVMe/TCP データ サービスが備わった 1 つのデータ ストレージ VM がデプロイされています。追加のデータ ストレージ VM を追加することはできません。
- NFS、CIFS (SMB)、iSCSI、Autonomous Ransomware Protection (ARP)、 SnapLock、およびSnapMirror のライセンスがインストールされています。
- "ONTAP温度に敏感なストレージ効率 (TSSE)"、ボリューム暗号化、および外部キー管理がデフォルトで有効になっています。
- 以下の機能はサポートされていません:
  - FabricPool の階層化
  - ストレージVMタイプの変更
  - 高速書き込みモード

開始する前に

- 有効な Azure Marketplace サブスクリプションがあることを確認します。
- ネットワーク要件を満たしていることを確認してください"単一 AZ での HA 展開"Azure で。。 "Cloud Volumes ONTAP用の Azure ネットワークを設定する" 。
- Cloud Volumes ONTAPをデプロイするには、次のいずれかの Azure ロールが割り当てられている必要があります。
  - その `contributor`デフォルトの権限を持つロール。詳細については、 "Microsoft Azure ドキュメント: Azure 組み込みロール" 。
  - 次の権限を持つカスタム RBAC ロール。詳細については、 "Azure ドキュメント: Azure カスタム ロール" 。

```
"permissions": [ { "actions": [ "Microsoft.AAD/register/action",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Network/loadBalancers/write", "Microsoft.ClassicCompute/virtualMachines/write",
"Microsoft.Compute/capacityReservationGroups/deploy/action",
"Microsoft.ClassicCompute/virtualMachines/networkInterfaces/associatedNetworkSecurityGroups/
write", "Microsoft.Network/networkInterfaces/write", "Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Network/virtualNetworks/write", "Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Compute/disks/write",
"Microsoft.Compute/virtualMachineScaleSets/write", "Microsoft.Resources/deployments/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/subnets/write" ], "notActions": [], "dataActions": [],
"notDataActions": [] } ]
```

リソースプロバイダー「Microsoft.storage」をサブスクリプションに登録している場合は、 `Microsoft.AAD/register/action`許可。詳細については、 "Azure ドキュメント: ストレージの Azure アクセス許可" 。

手順

1. Azure Marketplace サイトから、 NetApp製品を検索します。
2. * NetApp Cloud Volumes ONTAP direct*を選択します。
3. 作成 をクリックして、デプロイメント ウィザードを起動します。
4. プランを選択してください。 プラン リストには通常、 Cloud Volumes ONTAPの最新リリースが表示されます。
5. *基本*タブで、次の詳細を入力します。
   - サブスクリプション: サブスクリプションを選択します。デプロイメントはサブスクリプション番号にリンクされます。
   - リソース グループ: 既存のリソース グループを使用するか、新しいリソース グループを作成します。リソース グループは、ディスクやストレージ VM などのすべてのリソースをCloud Volumes ONTAP システムの単一のグループ内に割り当てるのに役立ちます。
   - リージョン: 単一の AZ での Azure HA デプロイメントをサポートするリージョンを選択します。リストには利用可能なリージョンのみが表示されます。
   - サイズ: サポートされている Premium SSD v2 マネージド ディスクのストレージ VM サイズを選択します。
   - ゾーン: 選択した地域のゾーンを選択します。
   - 管理者パスワード: パスワードを設定します。デプロイメント後にシステムにログインするには、この管理者パスワードを使用します。
   - パスワードの確認: 確認のために同じパスワードをもう一度入力します。
     - ネットワーク タブで、仮想ネットワークとサブネットを追加するか、リストから選択します。

       Microsoft Azure の制限に準拠するには、新しい仮想ネットワークを設定するときに新しいサブネットを作成する必要があります。同様に、既存のネットワークを選択する場合は、既存のサブネットを選択する必要があります。

     - 定義済みのネットワーク セキュリティ グループを選択するには、[はい] を選択します。必要なトラフィック ルールが定義された Azure ネットワーク セキュリティ グループを割り当てるには、[いいえ] を選択します。詳細については、 "Azure のセキュリティ グループ ルール" 。
     - *詳細*タブで、このデプロイメントに必要な 2 つの Azure 機能が設定されているかどうかを確認します。参照"Cloud Volumes ONTAP の単一 AZ デプロイメントで Azure 機能を有効にする"そして"AzureでCloud Volumes ONTAPの高可用性モードを有効にする"。
     - タグ タブで、リソースまたはリソース グループの名前と値のペアを定義できます。
     - 確認 + 作成 タブで詳細を確認し、デプロイを開始します。

終了後の操作

通知アイコンを選択して、デプロイメントの進行状況を表示します。 Cloud Volumes ONTAPがデプロイされた後、操作用にリストされたストレージ VM を表示できます。

アクセスできるようになったら、 ONTAP System Manager またはONTAP CLI を使用して、設定した管理者認証情報でストレージ VM にログインします。その後、ボリューム、LUN、または共有を作成し、 Cloud Volumes ONTAPのストレージ機能を使い始めることができます。

デプロイメントの問題のトラブルシューティング

Azure マーケットプレイスを通じて直接導入されたCloud Volumes ONTAPシステムには、 NetAppからのサポートは含まれません。展開中に問題が発生した場合、独自にトラブルシューティングして解決できます。

手順

1. Azure Marketplace サイトで、ブート診断 > シリアル ログ に移動します。
2. シリアルログをダウンロードして調査します。
3. トラブルシューティングについては、製品ドキュメントとナレッジベース (KB) の記事を参照してください。
   - "Azure マーケットプレイスのドキュメント"
   - "NetAppのドキュメント"
   - "NetApp KB記事"

コンソールで展開されたシステムを検出する

Azure マーケットプレイスの直接展開を使用して展開したCloud Volumes ONTAPシステムを検出し、コンソールの システム ページで管理できます。コンソール エージェントはシステムを検出し、追加して必要なライセンスを適用し、これらのシステムに対してコンソールの全機能のロックを解除します。 PSSD v2 マネージド ディスクを使用した単一の AZ 内の元の HA 構成は保持され、システムは元のデプロイメントと同じ Azure サブスクリプションとリソース グループに登録されます。

タスク概要

Azure マーケットプレイスの直接展開を使用して展開されたCloud Volumes ONTAPシステムを検出すると、コンソール エージェントは次のタスクを実行します。

- 検出されたシステムの無料ライセンスを通常の容量ベースのライセンスに置き換えます"フリーミアムライセンス"。
- 展開されたシステムの既存の機能を保持し、データ保護、データ管理、セキュリティ機能などのコンソールの追加機能を追加します。
- ノードにインストールされているライセンスを、NFS、CIFS (SMB)、iSCSI、ARP、 SnapLock、およびSnapMirrorの新しいONTAPライセンスに置き換えます。
- 汎用ノードのシリアル番号を一意のシリアル番号に変換します。
- 必要に応じてリソースに新しいシステム タグを割り当てます。
- インスタンスの動的 IP アドレスを静的 IP アドレスに変換します。
- 以下の機能を有効にします"FabricPool の階層化"、"AutoSupport" 、 そして"一度書き込み、何度も読み取り"展開されたシステム上の (WORM) ストレージ。必要なときにコンソールからこれらの機能を有効にすることができます。
- インスタンスを検出するために使用される NSS アカウントにインスタンスを登録します。
- 容量管理機能を有効にする"自動モードと手動モード"発見されたシステムについて。

開始する前に

Azure マーケットプレイスでのデプロイが完了していることを確認します。コンソール エージェントは、展開が完了し、検出可能になった場合にのみシステムを検出できます。

手順

コンソールでは、既存のシステムを検出するための標準の手順に従います。。 "既存のCloud Volumes ONTAP システムをコンソールに追加する" 。

検出中に失敗メッセージが表示される場合がありますが、検出プロセスが完了するまで無視できます。検出中に、Azure Marketplace ポータルでシステムによって生成されたCloud Volumes ONTAP構成、特にシステム タグを変更しないでください。これらの構成に変更を加えると、予期しないシステム動作が発生する可能性があります。

終了後の操作

検出が完了すると、コンソールの システム ページにリストされているシステムを表示できます。次のようなさまざまな管理タスクを実行できます。"総計を拡大する" 、"ボリュームの追加" 、"追加のストレージVMのプロビジョニング" 、 そして"インスタンスタイプの変更"。

関連リンク

ストレージの作成の詳細については、 ONTAP のドキュメントを参照してください。

- "NFS用のボリュームを作成する"
- "iSCSI用のLUNを作成する"
- "CIFSの共有を作成する"

Google Cloud を使い始める

Google Cloud でのCloud Volumes ONTAPのクイック スタート

数ステップで Google Cloud のCloud Volumes ONTAPを使い始めましょう。

1 コンソールエージェントを作成する

もしあなたが "コンソールエージェント"まだ作成する必要があります。 "Google Cloud でコンソール エージェントを作成する方法を学びます"

インターネット アクセスが利用できないサブネットにCloud Volumes ONTAPを展開する場合は、コンソールエージェントを手動でインストールし、そのコンソール エージェントで実行されているNetApp Consoleにアクセスする必要があることに注意してください。 "インターネットにアクセスできない場所にコンソールエージェントを手動でインストールする方法を学びます"

2 構成を計画する

コンソールでは、ワークロード要件に一致する事前構成済みのパッケージが提供されており、独自の構成を作成することもできます。独自の構成を選択する場合は、利用可能なオプションを理解する必要があります。

"構成の計画について詳しくは" 。

3 ネットワークを設定する

1. VPC とサブネットがコンソール エージェントと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. データ階層化を有効にする場合は、 "プライベート Google アクセス用にCloud Volumes ONTAPサブネットを構成する" 。
3. HA ペアをデプロイする場合は、それぞれ独自のサブネットを持つ 4 つの VPC があることを確認してください。
4. 共有 VPC を使用している場合は、コンソール エージェント サービス アカウントに *Compute Network User* ロールを付与します。
5. NetApp AutoSupportのターゲット 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ます。

   インターネットにアクセスできない場所にCloud Volumes ONTAPを展開する場合、この手順は必要ありません。

"ネットワーク要件の詳細" 。


サービスアカウントを設定する

Cloud Volumes ONTAP、 2 つの目的で Google Cloud サービス アカウントが必要です。 1つ目は、"データ階層化"コールドデータを Google Cloud の低コストのオブジェクト ストレージに階層化します。 2つ目は、"NetApp Backup and Recovery"ボリュームを低コストのオブジェクト ストレージにバックアップします。

1 つのサービス アカウントを設定して、両方の目的に使用できます。サービス アカウントには **Storage Admin** ロールが必要です。

"ステップバイステップの説明を読む" 。


Google Cloud API を有効にする

"プロジェクトで Google Cloud API を有効にする"。 "これらのAPI"は、コンソールエージェントの作成時に既に有効になっている可能性がありますが、Google CloudにCloud Volumes ONTAPを導入するために必要です。


コンソールを使用して**Cloud Volumes ONTAP**を起動する

*システムの追加*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完了します。"ステップバイステップの説明を読む" 。

関連リンク

- "コンソールエージェントの作成"
- "Linuxホストにコンソールエージェントソフトウェアをインストールする"
- "コンソール エージェントの Google Cloud 権限"

Google Cloud でCloud Volumes ONTAP構成を計画する

Google Cloud にCloud Volumes ONTAP をデプロイする場合、ワークロード要件に一致する事前構成済みのシステムを選択するか、独自の構成を作成することができます。独

自の構成を選択する場合は、利用可能なオプションを理解する必要があります。

Cloud Volumes ONTAPライセンスを選択する

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。各オプションにより、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学ぶ"
- "ライセンスの設定方法を学ぶ"

サポートされている地域を選択してください

Cloud Volumes ONTAP は、ほとんどの Google Cloud 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地域の完全なリストを見る" 。

サポートされているマシンタイプを選択してください

Cloud Volumes ONTAP は、選択したライセンス タイプに応じて、いくつかのマシン タイプをサポートします。

"Google Cloudでサポートされ ているCloud Volumes ONTAPの構成"

ストレージ制限を理解する

Cloud Volumes ONTAPシステムの生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。構成を計画する際には、これらの制限に注意する必要があります。

"Google CloudのCloud Volumes ONTAPのストレージ制限"

Google Cloud でシステムのサイズを決定する

Cloud Volumes ONTAPシステムのサイズを設定すると、パフォーマンスと容量の要件を満たすことができます。マシン タイプ、ディスク タイプ、ディスク サイズを選択するときは、いくつかの重要なポイントに注意する必要があります。

機械の種類

サポートされているマシンタイプについては、 "Cloud Volumes ONTAPリリースノート"次に、サポートされている各マシンタイプに関する Google の詳細を確認します。ワークロード要件を、マシンタイプの vCPU とメモリの数に合わせてください。各 CPU コアによってネットワーク パフォーマンスが向上することに注意してください。

詳細については、以下を参照してください。

- "Google Cloud ドキュメント: N1 標準マシンタイプ"
- "Google Cloud ドキュメント: パフォーマンス"

ディスク タイプ

Cloud Volumes ONTAPのボリュームを作成するときは、 Cloud Volumes ONTAP がディスクに使用する基盤となるクラウド ストレージを選択する必要があります。ディスク タイプは次のいずれかになります。

- ゾーン *SSD* 永続ディスク: SSD 永続ディスクは、高レートのランダム IOPS を必要とするワークロードに最適です。
- ゾーンバランス永続ディスク: これらの SSD は、GB あたりの IOPS を低くすることで、パフォーマンスとコストのバランスをとります。
- ゾーン標準永続ディスク: 標準永続ディスクは経済的で、順次読み取り/書き込み操作を処理できます。

  詳細については、 "Google Cloud ドキュメント: ゾーン永続ディスク（標準および SSD）" 。

ディスク サイズ

Cloud Volumes ONTAPシステムをデプロイするときは、初期ディスク サイズを選択する必要があります。その後は、NetApp Consoleでシステムの容量を管理できるようになりますが、アグリゲートを自分で構築する場合は、次の点に注意してください。

- アグリゲート内のすべてのディスクは同じサイズである必要があります。
- パフォーマンスを考慮しながら、必要なスペースを決定します。
- 永続ディスクのパフォーマンスは、ディスク サイズとシステムで使用可能な vCPU の数に応じて自動的に調整されます。

  詳細については、以下を参照してください。

  - "Google Cloud ドキュメント: ゾーン永続ディスク（標準および SSD）"
  - "Google Cloud ドキュメント: 永続ディスクとローカル SSD のパフォーマンスの最適化"

デフォルトのシステムディスクを表示する

コンソールは、ユーザー データ用のストレージに加えて、 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。計画のために、Cloud Volumes ONTAP を展開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。

- "Google Cloud の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" 。
- "Google Cloud ドキュメント: Cloud Quota の概要"

  Google Cloud Compute Engine はリソース使用量に割り当て制限を適用するため、 Cloud Volumes ONTAP をデプロイする前に制限に達していないことを確認する必要があります。

コンソール エージェントにはシステム ディスクも必要です。 "コンソールエージェントのデフォルト構成の詳細を表示する" 。

ネットワーク情報を収集する

Google CloudにCloud Volumes ONTAPを導入する場合は、仮想ネットワークに関する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。

単一ノードシステムのネットワーク情報

Google Cloud 情報	あなたの価値
リージョン	

Google Cloud 情報	あなたの価値
ゾーン	
VPCネットワーク	
サブネット	
ファイアウォール ポリシー（独自のものを使用している場合）	

複数のゾーンにあるHAペアのネットワーク情報

Google Cloud 情報	あなたの価値
リージョン	
ノード1のゾーン	
ノード2のゾーン	
調停者のためのゾーン	
VPC-0とサブネット	
VPC-1とサブネット	
VPC-2とサブネット	
VPC-3とサブネット	
ファイアウォール ポリシー（独自のものを使用している場合）	

単一ゾーン内のHAペアのネットワーク情報

Google Cloud 情報	あなたの価値
リージョン	
ゾーン	
VPC-0とサブネット	
VPC-1とサブネット	
VPC-2とサブネット	
VPC-3とサブネット	
ファイアウォール ポリシー（独自のものを使用している場合）	

書き込み速度を選択する

コンソールを使用すると、Google Cloud の高可用性（HA）ペアを除き、 Cloud Volumes ONTAP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、標準設定と高速設定の違い、および高速書き込み速度を使用する場合のリスクと推奨事項を理解しておく必要があります。"書き込み速度について詳しくはこち

ら" 。

ボリューム使用プロファイルを選択する

ONTAPには、必要なストレージの総量を削減できるいくつかのストレージ効率機能が含まれています。コンソールでボリュームを作成するときに、これらの機能を有効にするプロファイルまたは無効にするプロファイルを選択できます。どのプロファイルを使用するかを決めるには、これらの機能について詳しく理解する必要があります。

NetAppストレージ効率機能には、次のような利点があります。

シンプロビジョニング

物理ストレージ プールに実際に存在するよりも多くの論理ストレージをホストまたはユーザーに提供します。ストレージ スペースを事前に割り当てるのではなく、データが書き込まれるときに各ボリュームにストレージ スペースが動的に割り当てられます。

重複排除

同一のデータ ブロックを見つけて、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。この手法は、同じボリューム内に存在する冗長なデータ ブロックを排除することで、ストレージ容量の要件を削減します。

圧縮

プライマリ、セカンダリ、アーカイブ ストレージのボリューム内のデータを圧縮することで、データの保存に必要な物理容量を削減します。

Cloud Volumes ONTAP用に Google Cloud ネットワークを設定する

NetApp Consoleは、IP アドレス、ネットマスク、ルートなどのCloud Volumes ONTAP 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 アクセスが利用可能であること、十分なプライベート IP アドレスが利用可能であること、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。

HAペアを導入する場合は、"Google Cloud での HA ペアの仕組みを学ぶ" 。

Cloud Volumes ONTAPの要件

Google Cloud では次の要件を満たす必要があります。

単一ノードシステムに固有の要件

単一ノード システムを導入する場合は、ネットワークが次の要件を満たしていることを確認してください。

1つの**VPC**

単一ノード システムには 1 つの仮想プライベート クラウド（VPC）が必要です。

プライベート**IP**アドレス

Google Cloud の単一ノード システムの場合、NetApp Console は次のものにプライベート IP アドレスを割り当てます。

- ノード
- クラスタ
- Storage VM
- データNAS LIF
- データ iSCSI LIF

API を使用してCloud Volumes ONTAPをデプロイし、次のフラグを指定すると、ストレージ VM (SVM) 管理 LIF の作成をスキップできます。

```
skipSvmManagementLif: true
```

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、ストレージ VM (SVM) 管理 LIF が必要です。

HAペア固有の要件

HA ペアを展開する場合は、ネットワークが次の要件を満たしていることを確認してください。

1つまたは複数のゾーン

複数のゾーンまたは単一のゾーンに HA 構成を展開することで、データの高可用性を確保できます。 HA ペアを作成するときに、コンソールで複数のゾーンまたは単一のゾーンを選択するように求められます。

- 複数のゾーン（推奨）

  3 つのゾーンにわたって HA 構成を展開すると、ゾーン内で障害が発生した場合でも継続的なデータ可用性が確保されます。書き込みパフォーマンスは単一ゾーンを使用する場合と比べてわずかに低下しますが、最小限であることに注意してください。

- 単一ゾーン

  単一のゾーンにデプロイされる場合、 Cloud Volumes ONTAP HA 構成では、スプレッド配置ポリシーが使用されます。このポリシーにより、障害の分離を実現するために個別のゾーンを使用する必要がなく、ゾーン内の単一障害点から HA 構成が保護されます。

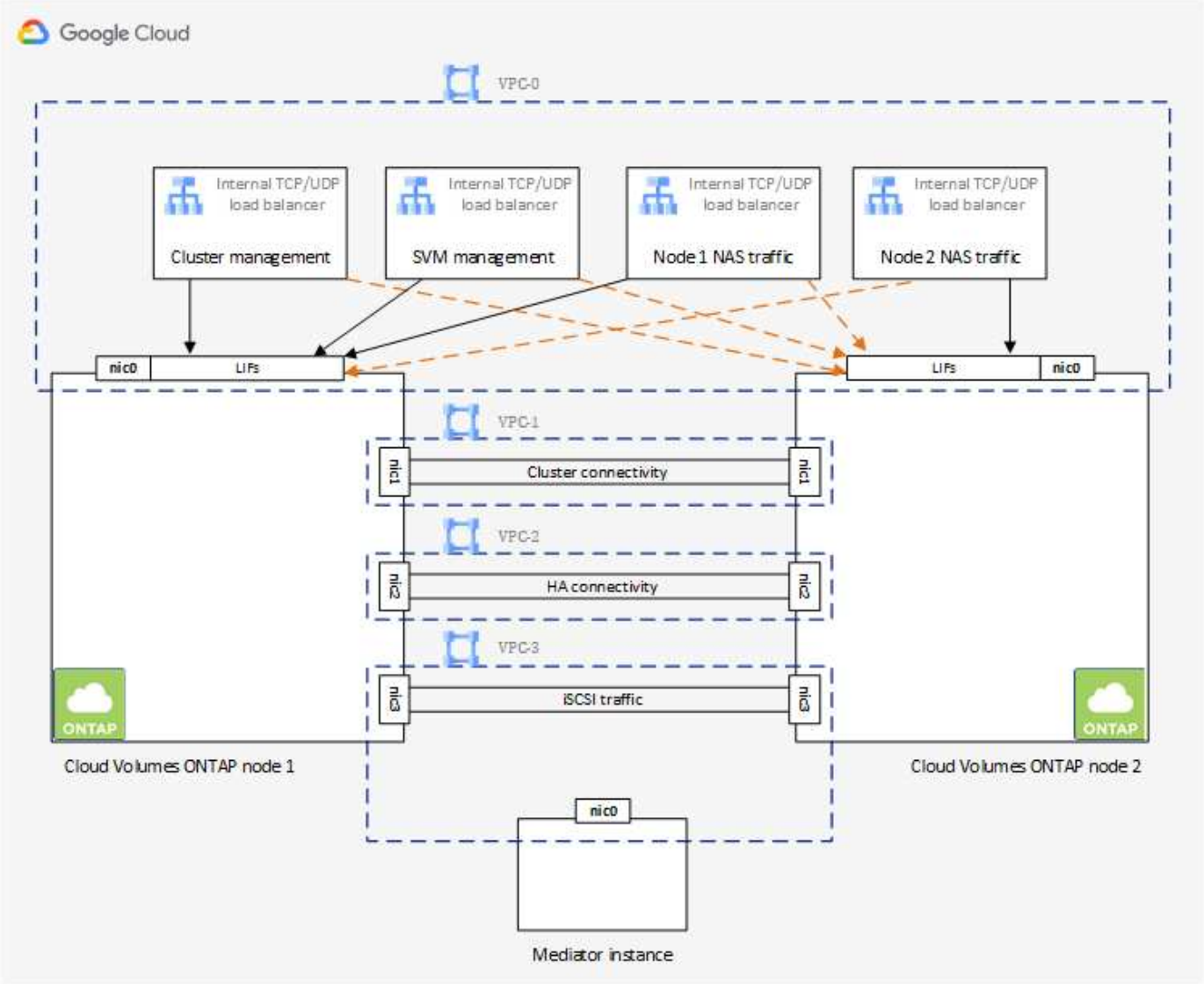
  このデプロイメント モデルでは、ゾーン間のデータ送信料金が発生しないため、コストが削減されます。

4つの仮想プライベートクラウド

HA 構成には 4 つの仮想プライベート クラウド (VPC) が必要です。 Google Cloud では各ネットワーク インターフェースが個別の VPC ネットワークに存在する必要があるため、4 つの VPC が必要です。

HA ペアを作成するときに、コンソールで 4 つの VPC を選択するように求められます。

- データとノードへのインバウンド接続用の VPC-0
- ノードと HA メディエーター間の内部通信用の VPC-1、VPC-2、および VPC-3



サブネット

各 VPC にはプライベート サブネットが必要です。

コンソール エージェントを VPC-0 に配置する場合は、API にアクセスしてデータ階層化を有効にするために、サブネットでプライベート Google アクセスを有効にする必要があります。

これらの VPC 内のサブネットには、異なる CIDR 範囲が必要です。重複する CIDR 範囲を持つことはできません。

プライベート**IP**アドレス

コンソールは、Google Cloud のCloud Volumes ONTAPに必要な数のプライベート IP アドレスを自動的に割り当てます。ネットワークに十分なプライベート アドレスが利用可能であることを確認する必要があります。

Cloud Volumes ONTAP に割り当てられる LIF の数は、単一ノード システムを導入するか HA ペア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。SVM 管理 LIF は、SnapCenter などの管理ツールに必要です。

- 単一ノード NetApp Consoleは単一ノード システムに 4 つの IP アドレスを割り当てます：
  - ノード管理LIF
  - クラスタ管理LIF
  - iSCSI データ LIF

    iSCSI LIF は、iSCSI プロトコルを介したクライアント アクセスを提供し、システムによって他の重要なネットワーク ワークフローに使用されます。これらの LIF は必須であり、削除しないでください。

  - NAS LIF

    API を使用してCloud Volumes ONTAPをデプロイし、次のフラグを指定すると、ストレージ VM (SVM) 管理 LIF の作成をスキップできます。

```
skipSvmManagementLif: true
```

- **HA** ペア コンソールは HA ペアに 12 ～ 13 個の IP アドレスを割り当てます。
  - 2つのノード管理LIF（e0a）
  - 1 クラスタ管理LIF（e0a）
  - 2 つの iSCSI LIF (e0a)

    iSCSI LIF は、iSCSI プロトコルを介したクライアント アクセスを提供し、システムによって他の重要なネットワーク ワークフローに使用されます。これらの LIF は必須であり、削除しないでください。

  - 1 個または 2 個の NAS LIF (e0a)
  - 2 つのクラスタ LIF (e0b)
  - 2 つの HA 相互接続 IP アドレス (e0c)
  - 2つのRSM iSCSI IPアドレス（e0d）

    API を使用してCloud Volumes ONTAPをデプロイし、次のフラグを指定すると、ストレージ VM (SVM) 管理 LIF の作成をスキップできます。

```
skipSvmManagementLif: true
```

内部ロードバランサ

コンソールは、Cloud Volumes ONTAP HA ペアへの受信トラフィックを管理する 4 つの Google Cloud 内部ロードバランサ（TCP/UDP）を作成します。お客様側での設定は必要ありません。これを要件としてリストしたのは、ネットワーク トラフィックを通知し、セキュリティ上の懸念を軽減するためだけです。

1 つのロード バランサはクラスタ管理用、1 つはストレージ VM (SVM) 管理用、1 つはノード 1 への NAS トラフィック用、最後の 1 つはノード 2 への NAS トラフィック用です。

各ロードバランサーの設定は次のとおりです。

- 1つの共有プライベートIPアドレス
- グローバルな健康診断

  デフォルトでは、ヘルスチェックで使用されるポートは 63001、63002、および 63003 です。

- 1つの地域TCPバックエンドサービス
- 1つの地域UDPバックエンドサービス
- 1つのTCP転送ルール
- 1つのUDP転送ルール
- グローバルアクセスが無効になっています

  グローバル アクセスはデフォルトで無効になっていますが、デプロイ後に有効にすることがサポートされています。リージョン間のトラフィックのレイテンシが大幅に増加するため、これを無効にしました。誤ってリージョンをまたいでマウントすることによって、ネガティブな体験をすることがないようにしたいと考えました。このオプションを有効にするかどうかは、ビジネス ニーズによって異なります。

共有**VPC**

Cloud Volumes ONTAPとコンソール エージェントは、Google Cloud 共有 VPC とスタンドアロン VPC でもサポートされています。

単一ノード システムの場合、VPC は共有 VPC またはスタンドアロン VPC のいずれかになります。

HA ペアの場合、4 つの VPC が必要です。これらの各 VPC は、共有またはスタンドアロンのいずれかになります。たとえば、VPC-0 は共有 VPC であり、VPC-1、VPC-2、VPC-3 はスタンドアロン VPC である可能性があります。

共有 VPC を使用すると、複数のプロジェクトにわたって仮想ネットワークを構成し、一元管理できます。 ホスト プロジェクト で共有 VPC ネットワークを設定し、サービス プロジェクト でコンソール エージェントとCloud Volumes ONTAP仮想マシン インスタンスをデプロイできます。

"Google Cloud ドキュメント: 共有 VPC の概要" 。

"コンソール エージェントのデプロイで説明されている必要な共有 VPC 権限を確認します。"

VPC でのパケットミラーリング

"パケットミラーリング"Cloud Volumes ONTAPをデプロイする Google Cloud サブネットで無効に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

Cloud Volumes ONTAPシステムでは、さまざまな機能の外部エンドポイントにアクセスするために、アウトバウンド インターネット アクセスが必要です。厳格なセキュリティ要件を持つ環境でこれらのエンドポイントがブロックされている場合、 Cloud Volumes ONTAP は正常に動作しません。

コンソール エージェントは、日常的な操作のために複数のエンドポイントにも接続します。エンドポイントの詳細については、以下を参照してください。 "コンソールエージェントから接続されたエンドポイントを表示する"そして "コンソールを使用するためのネットワークの準備"。

Cloud Volumes ONTAPエンドポイント

Cloud Volumes ONTAP はこれらのエンドポイントを使用してさまざまなサービスと通信します。

エンドポイント	適用対象	目的	展開モード	エンドポイントが利用できない場合の影響
https://netapp-cloud-account.auth0.com	認証	コンソールでの認証に使用されます。	標準モードと制限モード。	ユーザー認証が失敗し、次のサービスは利用できなくなります。 • Cloud Volumes ONTAPサービス • ONTAPサービス • プロトコルとプロキシサービス
https://api.bluexp.netapp.com/tenancy	賃貸借	コンソールからCloud Volumes ONTAPリソースを取得して、リソースとユーザーを承認するために使用されます。	標準モードと制限モード。	Cloud Volumes ONTAPリソースとユーザーは承認されていません。
https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	AutoSupportテレメトリ データをNetAppサポートに送信するために使用されます。	標準モードと制限モード。	AutoSupport情報は未配信のままです。

エンドポイント	適用対象	目的	展開モード	エンドポイントが利用できない場合の影響
https://cloudbuild.googleapis.com/v1（プライベートモードの展開のみ）\https://cloudkms.googleapis.com/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	Google Cloud（商用利用）。	Google Cloud サービスとの通信。	標準、制限、プライベートのモード。	Cloud Volumes ONTAP は、 Google Cloud サービスと通信して、Google Cloud のコンソールの特定の操作を実行できません。

他のネットワーク内の**ONTAP**システムへの接続

Google Cloud のCloud Volumes ONTAPシステムと他のネットワークのONTAPシステム間でデータを複製するには、VPC と他のネットワーク（企業ネットワークなど）の間に VPN 接続が必要です。

"Google Cloud ドキュメント: Cloud VPN の概要" 。

ファイアウォールルール

コンソールは、Cloud Volumes ONTAP が正常に動作するために必要な受信ルールと送信ルールを含む Google Cloud ファイアウォール ルールを作成します。テスト目的の場合、または独自のファイアウォール ルールを使用する場合は、ポートを参照することをお勧めします。

Cloud Volumes ONTAPのファイアウォール ルールには、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。 HA 構成を展開する場合、これらは VPC-0 のCloud Volumes ONTAPのファイアウォール ルールです。

HA 構成には 2 セットのファイアウォール ルールが必要であることに注意してください。

- VPC-0 の HA コンポーネントに対する 1 セットのルール。これらのルールにより、Cloud Volumes ONTAPへのデータ アクセスが可能になります。
- VPC-1、VPC-2、VPC-3 の HA コンポーネントに対する別のルール セット。これらのルールは、HA コンポーネント間の受信および送信通信に対して有効です。詳細情報 。

コンソール エージェントに関する情報をお探しですか? "コンソールエージェントのファイアウォールルールを表示する"

インバウンドルール

Cloud Volumes ONTAPシステムを追加する場合、展開時に事前定義されたファイアウォール ポリシーのソース フィルターを選択できます。

- 選択した **VPC** のみ: 受信トラフィックのソース フィルターは、Cloud Volumes ONTAPシステムの VPC のサブネット範囲と、コンソール エージェントが存在する VPC のサブネット範囲です。これは推奨されるオプションです。
- すべての **VPC**: 受信トラフィックのソース フィルターは 0.0.0.0/0 IP 範囲です。

独自のファイアウォール ポリシーを使用する場合は、 Cloud Volumes ONTAPと通信する必要があるすべてのネットワークを追加するだけでなく、内部 Google ロードバランサが正しく機能できるように両方のアドレス範囲も追加してください。これらのアドレスは 130.211.0.0/22 と 35.191.0.0/16 です。詳細については、"Google Cloud ドキュメント: ロードバランサのファイアウォール ルール" 。

プロトコル	ポート	目的
すべてのICMP	全て	インスタンスにpingを実行する
HTTP	80	クラスタ管理LIFのIPアドレスを使用してONTAP System Manager Webコンソールにアクセスする
HTTPS	443	コンソールエージェントとの接続と、クラスタ管理LIFのIPアドレスを使用したONTAP System Manager Webコンソールへのアクセス
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 フレームを使用した TCP 経由の Microsoft SMB/CIFS
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

プロトコル	ポート	目的
TCP	4046	NFS のネットワーク ステータス モニター
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
TCP	63001-63050	どのノードが正常であるかを判断するためにプローブ ポートをロード バランシングします (HA ペアの場合のみ必要)
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 モニター
UDP	4049	NFS rquotadプロトコル

アウトバウンドルール

Cloud Volumes ONTAPの定義済みセキュリティ グループは、すべての送信トラフィックを開きます。それが許容できる場合は、基本的な送信ルールに従ってください。より厳格なルールが必要な場合は、高度な送信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の定義済みセキュリティ グループには、次の送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ICMP	全て	すべての送信トラフィック
すべてTCP	全て	すべての送信トラフィック
すべてUDP	全て	すべての送信トラフィック

高度なアウトバウンドルール

送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による送信通信に必要なポートのみを開くことができます。 Cloud Volumes ONTAPクラスターは、ノード トラフィックを制御するために次のポートを使用します。

ソースは、Cloud Volumes ONTAPシステムのインターフェース (IP アドレス) です。

サービス	プロトコル	ポート	ソース	デスティネーション	目的
Active Directory	TCP	88	ノード管理LIF	アクティブディレクトリフォレスト	Kerberos V認証
	UDP	137	ノード管理LIF	アクティブディレクトリフォレスト	NetBIOSネーム サービス
	UDP	138	ノード管理LIF	アクティブディレクトリフォレスト	NetBIOSデータグラムサービス
	TCP	139	ノード管理LIF	アクティブディレクトリフォレスト	NetBIOSサービス セッション
	TCP とUDP	389	ノード管理LIF	アクティブディレクトリフォレスト	LDAP
	TCP	445	ノード管理LIF	アクティブディレクトリフォレスト	NetBIOS フレームを使用した TCP 経由の Microsoft SMB/CIFS
	TCP	464	ノード管理LIF	アクティブディレクトリフォレスト	Kerberos V パスワードの変更と設定 (SET_CHANGE)
	UDP	464	ノード管理LIF	アクティブディレクトリフォレスト	Kerberos鍵管理
	TCP	749	ノード管理LIF	アクティブディレクトリフォレスト	Kerberos V パスワードの変更と設定 (RPCSEC_GSS)
	TCP	88	データ LIF (NFS、CIFS、iSCSI)	アクティブディレクトリフォレスト	Kerberos V認証
	UDP	137	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	NetBIOSネーム サービス
	UDP	138	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	NetBIOSデータグラムサービス
	TCP	139	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	NetBIOSサービス セッション
	TCP とUDP	389	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	LDAP
	TCP	445	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	NetBIOS フレームを使用した TCP 経由の Microsoft SMB/CIFS
	TCP	464	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	Kerberos V パスワードの変更と設定 (SET_CHANGE)
	UDP	464	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	Kerberos鍵管理
	TCP	749	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	Kerberos V パスワードの変更と設定 (RPCSEC_GSS)

サービス	プロトコル	ポート	ソース	デスティネーション	目的
AutoSupport	HTTPS	443	ノード管理LIF	mysupport.netapp.com	AutoSupport （HTTPSがデフォルト）
	HTTP	80	ノード管理LIF	mysupport.netapp.com	AutoSupport （トランスポート プロトコルが HTTPS から HTTP に変更された場合のみ）
	TCP	3128	ノード管理LIF	コンソールエージェント	アウトバウンドインターネット接続が利用できない場合、コンソールエージェント上のプロキシサーバーを介してAutoSupportメッセージを送信する
構成のバックアップ	HTTP	80	ノード管理LIF	http://<コンソールエージェントのIPアドレス>/occm/offboxconfig	構成のバックアップをコンソールエージェントに送信します。"ONTAPのドキュメント"
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	宛先サーバー	NDMPコピー
SMTP	TCP	25	ノード管理LIF	メール サーバ	SMTPアラートはAutoSupportに使用できます
SNMP	TCP	161	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	UDP	161	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	TCP	162	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	UDP	162	ノード管理LIF	監視サーバー	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

VPC-1、**VPC-2**、**VPC-3**のルール

Google Cloud では、HA 構成が 4 つの VPC にデプロイされます。 VPC-0のHA構成に必要なファイアウォールルールはCloud Volumes ONTAPについては上記に記載されています。

一方、VPC-1、VPC-2、VPC-3 のインスタンスに作成された定義済みのファイアウォール ルールにより、すべてのプロトコルとポートを介した受信通信が可能になります。これらのルールにより、HA ノード間の通信が可能になります。

HA ノードから HA メディエーターへの通信は、ポート 3260 (iSCSI) を介して行われます。

> 新しい Google Cloud HA ペアのデプロイメントで高速書き込みを有効にするには、VPC-1、VPC-2、VPC-3 に少なくとも 8,896 バイトの最大転送単位 (MTU) が必要です。既存の VPC-1、VPC-2、および VPC-3 を 8,896 バイトの MTU にアップグレードすることを選択した場合は、設定プロセス中にこれらの VPC を使用している既存の HA システムをすべてシャットダウンする必要があります。

プライベートモード展開の**Infrastructure Manager**構成

プライベートモードでCloud Volumes ONTAP 9.16.1以降を導入する場合は、Googleが最終的に廃止する予定のDeployment Managerの代わりに、Cloud Volumes ONTAPがGoogle Cloud Infrastructure Managerを導入サービスとして使用できるように、いくつかの設定変更を行う必要があります。

開始する前に

- Cloud Volumes ONTAPシステムが9.16.1以降であることを確認してください。そうでない場合は、システムをアップグレードしてください。手順については "Cloud Volumes ONTAP のアップグレード"を参照してください。
- Google Cloud API が有効になっていることを確認します。 "Google Cloud API を有効にする"を参照してください。
- Cloud Build API が有効になっていることを確認します。参照 "ここで Cloud Build API を有効にします"。
- Console エージェントのサービスアカウントにすべての標準権限があることを確認します。さらに、サービスアカウントに `cloudbuild.workerpools.get`および `cloudbuild.workerpools.list`権限があることを確認します。 "コンソール エージェントの Google Cloud 権限"を参照してください。

手順

1. Cloud Volumes ONTAPデプロイメントと同じリージョンにこの構成でプライベートワーカープールを作成します。プライベートワーカープールの作成については、 "Google Cloud ドキュメント：プライベート プールの作成と管理"および "Google Cloud Build の料金"を参照してください。

   ワーカー プールには次の構成が必要です：

   - マシンタイプ：e2-medium
   - ディスクサイズ：100 GB
   - 外部IPの割り当て：False
   - ネットワーク：デフォルトまたはプライベート。
   - "Google API"にアクセスするように設定されたサブネット。サブネットが Google API にアクセスできることを確認するには、次の手順を実行します：
     i. サブネットに対して「プライベート Google アクセス」がオンになっていることを確認します。
     ii. *VPC ネットワークレベル > プライベートサービスアクセスタブ > サービスに割り当てられた IP 範囲*に移動します。
     iii. **IP** 範囲の割り当て を選択し、Google Compute Service へのプライベート接続用の内部 IP 範囲を割り当てます。

iv. *サービスへのプライベート接続*で、*接続の作成*を選択します。

v. **Connected service producer = Google Cloud Platform** を選択します。

vi. 前の手順で作成したプライベート接続 IP 範囲の割り当てを指定します。

2. このワーカープールを展開し、Cloud Volumes ONTAP管理のために実行し続けます。Google Cloudは、このワーカープールを使用して、すべてのTerraform操作を分離された環境で実行します。

3. Cloud Volumes ONTAPをプライベートモードで導入する場合は、*GCPワーカープール*フィールドでこのワーカープールの名前を選択します。手順については、"Google Cloud でCloud Volumes ONTAPを起動する"を参照してください。

コンソールエージェントの要件

コンソール エージェントをまだ作成していない場合は、ネットワーク要件を確認する必要があります。

- "コンソールエージェントのネットワーク要件を表示する"
- "Google Cloud のファイアウォール ルール"

コンソールエージェントプロキシをサポートするためのネットワーク構成

コンソール エージェント用に設定されたプロキシ サーバーを使用して、 Cloud Volumes ONTAPからのアウトバウンド インターネット アクセスを有効にすることができます。コンソールは次の 2 種類のプロキシをサポートしています。

- 明示的なプロキシ: Cloud Volumes ONTAPからの送信トラフィックは、コンソール エージェントのプロキシ構成時に指定されたプロキシ サーバーの HTTP アドレスを使用します。コンソール エージェント管理者は、追加の認証のためにユーザー資格情報とルート CA 証明書を構成している場合もあります。明示的なプロキシにルートCA証明書が利用可能な場合は、必ず同じ証明書を取得して、 Cloud Volumes ONTAP システムにアップロードしてください。 "ONTAP CLI: セキュリティ証明書のインストール"指示。
- 透過プロキシ: ネットワークは、 Cloud Volumes ONTAPからの送信トラフィックをコンソール エージェント プロキシ経由で自動的にルーティングするように構成されています。透過プロキシを設定する場合、コンソール エージェント管理者は、プロキシ サーバーの HTTP アドレスではなく、 Cloud Volumes ONTAPからの接続用のルート CA 証明書のみを提供する必要があります。同じルートCA証明書を取得し、 Cloud Volumes ONTAPシステムにアップロードしてください。 "ONTAP CLI: セキュリティ証明書のインストール"指示。

コンソールエージェントのプロキシサーバーの構成については、 "プロキシサーバーを使用するようにコンソールエージェントを構成する" 。

Google Cloud で**Cloud Volumes ONTAP**のネットワーク タグを構成する

コンソール エージェントの透過プロキシ構成中に、管理者は Google Cloud のネットワーク タグを追加します。 Cloud Volumes ONTAP構成に同じネットワーク タグを取得して手動で追加する必要があります。このタグは、プロキシ サーバーが正しく機能するために必要です。

1. Google Cloud ConsoleでCloud Volumes ONTAPシステムを見つけます。
2. 詳細 **>** ネットワーク **>** ネットワーク タグ に移動します。
3. コンソール エージェントに使用するタグを追加し、構成を保存します。

関連トピック

- "Cloud Volumes ONTAPのAutoSupport設定を確認する"

- "ONTAPの内部ポートについて学ぶ" 。

VPC Service Controls を設定して、Google Cloud にCloud Volumes ONTAP をデプロイする

VPC Service Controls を使用して Google Cloud 環境をロックダウンする場合は、NetApp ConsoleとCloud Volumes ONTAP がGoogle Cloud API とどのようにやり取りするか、また Console とCloud Volumes ONTAP をデプロイするためにサービス境界をどのように構成するかを理解する必要があります。

VPC Service Controls を使用すると、信頼できる境界外にある Google マネージド サービスへのアクセスを制御し、信頼できない場所からのデータアクセスをブロックし、不正なデータ転送のリスクを軽減できます。"Google Cloud VPC Service Controls の詳細" 。

NetAppサービスが VPC Service Controls と通信する方法

コンソールは Google Cloud API と直接通信します。これは、Google Cloud 外部の外部 IP アドレス（api.services.cloud.netapp.com など）からトリガーされるか、Google Cloud 内でコンソール エージェントに割り当てられた内部アドレスからトリガーされます。

コンソール エージェントの展開スタイルによっては、サービス境界に特定の例外を設ける必要がある場合があります。

イメージ

Cloud Volumes ONTAP と Console はどちらも、NetApp が管理する Google Cloud 内のプロジェクトのイメージを使用します。組織内でホストされていないイメージの使用をブロックするポリシーが組織にある場合、これは Console エージェントと Cloud Volumes ONTAP の導入に影響する可能性があります。

手動インストール方法を使用してコンソール エージェントを手動で展開できますが、 Cloud Volumes ONTAPNetAppプロジェクトからイメージをプルする必要もあります。コンソール エージェントとCloud Volumes ONTAPをデプロイするには、許可リストを提供する必要があります。

コンソールエージェントの展開

コンソール エージェントを展開するユーザーは、プロジェクト ID *netapp-cloudmanager* およびプロジェクト番号 *14190056516* でホストされているイメージを参照できる必要があります。

Cloud Volumes ONTAPの導入

- コンソール サービス アカウントは、サービス プロジェクトのプロジェクト ID *netapp-cloudmanager* とプロジェクト番号 *14190056516* でホストされているイメージを参照する必要があります。
- デフォルトの Google API サービス エージェントのサービス アカウントは、サービス プロジェクトのプロジェクト ID *netapp-cloudmanager* とプロジェクト番号 *14190056516* でホストされているイメージを参照する必要があります。

VPC Service Controls を使用してこれらのイメージをプルするために必要なルールの例を以下に定義します。

VPC Service Controls 境界ポリシー

ポリシーにより、VPC Service Controls ルールセットの例外が許可されます。ポリシーの詳細については、"Google Cloud VPC Service Controls Policy ドキュメント"を参照してください。

コンソールに必要なポリシーを設定するには、組織内の VPC Service Controls 境界に移動し、次のポリシーを追加します。フィールドは、VPC Service Controls ポリシー ページで指定されたオプションと一致する必要があります。また、すべての*ルールが必須であり、ルール セットでは ***OR*** パラメータを使用する必要があることにも注意してください。

イングレスルール

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

または

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

または

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

出口ルール

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

上記のプロジェクト番号は、 NetAppがコンソール エージェントおよびCloud Volumes ONTAP のイメージを保存するために使用するプロジェクト *netapp-cloudmanager* です。

Cloud Volumes ONTAP用の Google Cloud サービス アカウントを作成する

Cloud Volumes ONTAP、 2 つの目的で Google Cloud サービス アカウントが必要です。1つ目は、"データ階層化"コールドデータを Google Cloud の低コストのオブジェクト ストレージに階層化します。 2つ目は、 "NetApp Backup and Recovery"ボリュームを低コストのオブジェクト ストレージにバックアップします。

Cloud Volumes ONTAP は、サービス アカウントを使用して、階層化データ用の 1 つのバケットとバックアップ用の別のバケットにアクセスし、管理します。

1 つのサービス アカウントを設定して、両方の目的に使用できます。サービス アカウントには **Storage Admin** ロールが必要です。

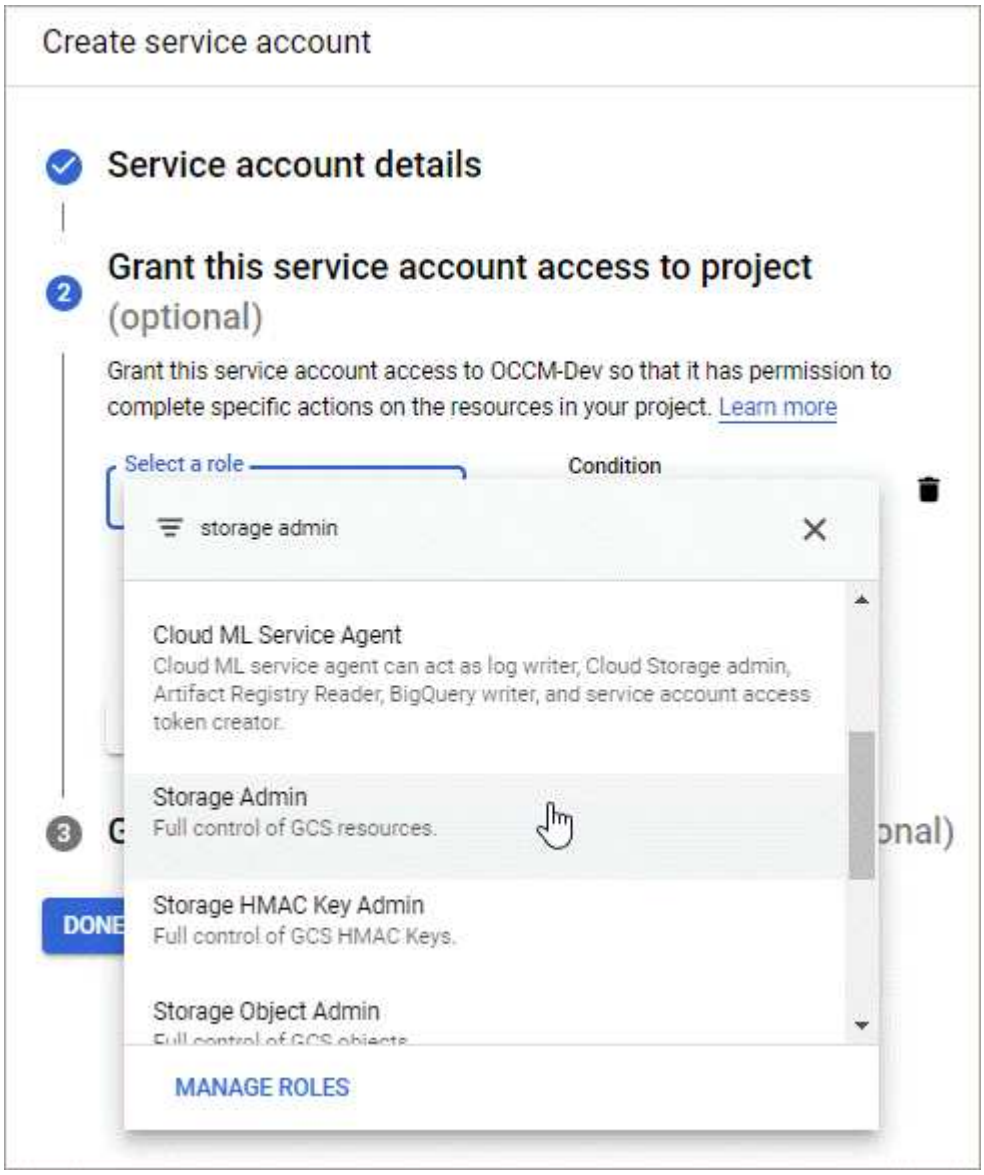
手順

1. Google Cloud Consoleで、 "サービスアカウントページに移動します"。
2. プロジェクトを選択してください。

3. サービス アカウントの作成 をクリックし、必要な情報を入力します。

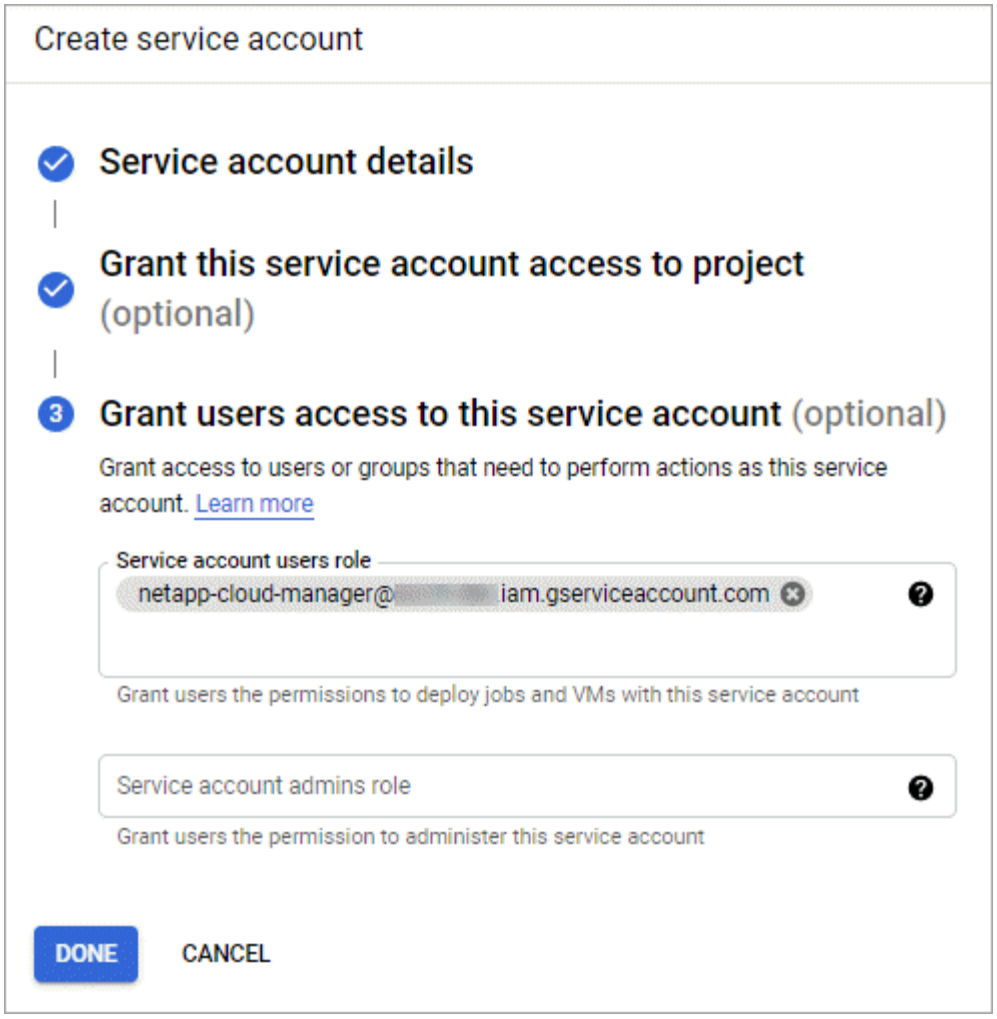
   a. サービス アカウントの詳細: 名前と説明を入力します。

   b. このサービス アカウントにプロジェクトへのアクセス権を付与します: ストレージ管理者 ロールを選択します。



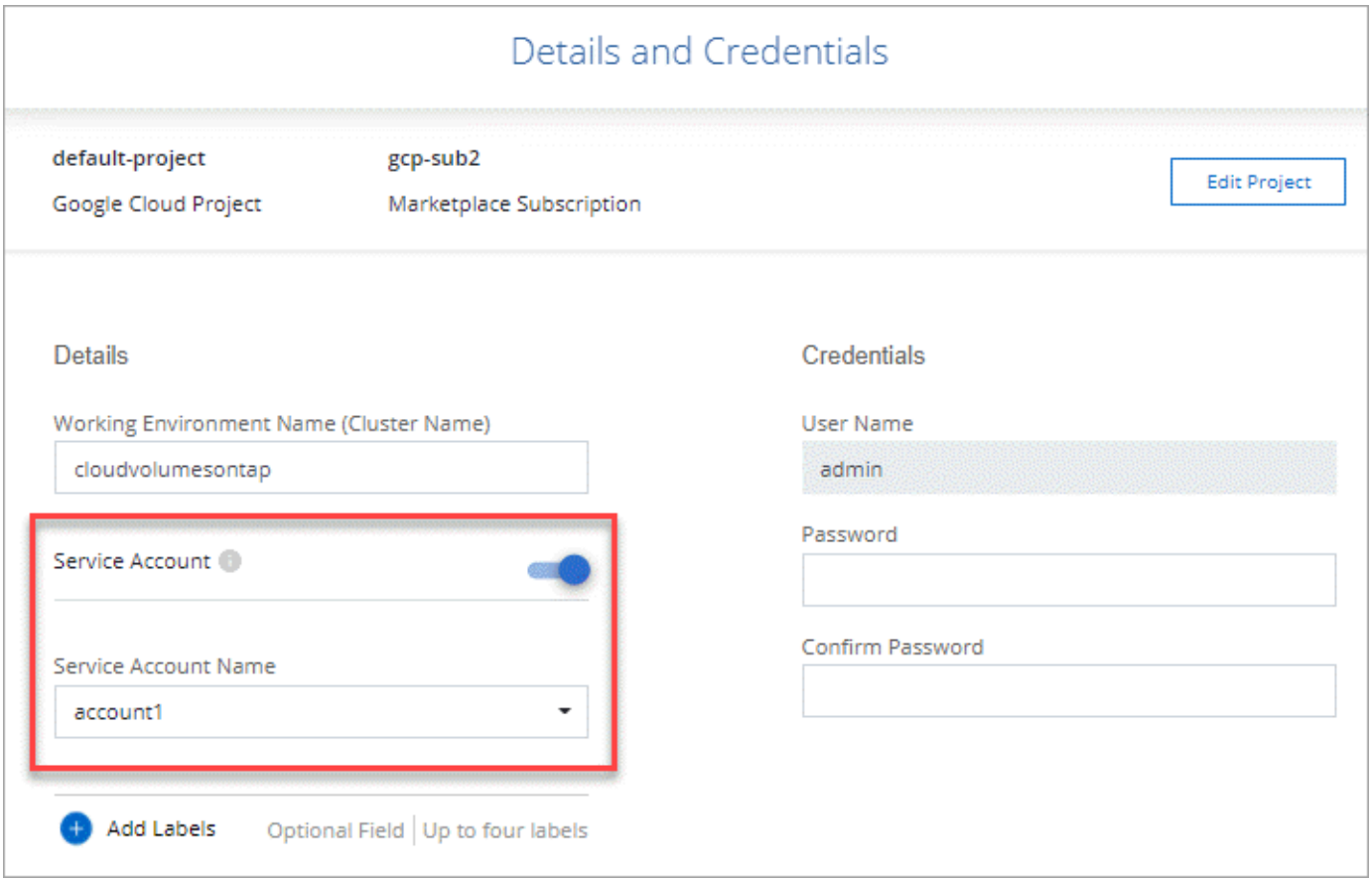
   c. ユーザーにこのサービス アカウントへのアクセスを許可: コンソール エージェント サービス アカウントを サービス アカウント ユーザー としてこの新しいサービス アカウントに追加します。

      この手順は、データ階層化の場合にのみ必要です。バックアップとリカバリには必要ありません。



次の手順

後でCloud Volumes ONTAPシステムを作成するときに、サービス アカウントを選択する必要があります。



Cloud Volumes ONTAPで顧客管理の暗号化キーを使用する

Google Cloud Storage では、データがディスクに書き込まれる前に常に暗号化されますが、API を使用して、顧客管理の暗号化キー を使用するCloud Volumes ONTAPシステムを作成できます。これらは、Cloud Key Management Service を使用して GCP で生成および管理するキーです。

手順

1. キーが保存されているプロジェクトにおいて、コンソール エージェント サービス アカウントにプロジェクト レベルでの適切な権限があることを確認します。

   権限は、 "デフォルトのサービスアカウント権限"ただし、Cloud Key Management Service に代替プロジェクトを使用する場合は適用されない可能性があります。

   権限は次のとおりです。

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. サービスアカウントが "Google Compute Engine サービス エージェント"キーに対する Cloud KMS 暗号化/復号化権限を持っています。

サービス アカウントの名前は、「service-[service_project_number]@compute-system.iam.gserviceaccount.com」という形式になります。

"Google Cloud ドキュメント: Cloud KMS での IAM の使用 - リソースに対するロールの付与"

3. getコマンドを呼び出してキーの「ID」を取得します。 `/gcp/vsa/metadata/gcp-encryption-keys` API 呼び出し、または GCP コンソールのキーで「リソース名のコピー」を選択します。
4. 顧客管理の暗号化キーを使用し、データをオブジェクト ストレージに階層化する場合、 NetApp Console は永続ディスクの暗号化に使用されるのと同じキーを利用しようとします。ただし、まず Google Cloud Storage バケットがキーを使用できるようにする必要があります。

   a. Google Cloud Storageサービスエージェントを見つけるには、 "Google Cloud ドキュメント: Cloud Storage サービス エージェントの取得" 。

   b. 暗号化キーに移動し、Google Cloud Storage サービス エージェントに Cloud KMS 暗号化/復号化権限を割り当てます。

   詳細については、 "Google Cloud ドキュメント: 顧客管理の暗号鍵の使用"

5. システムを作成するときに、API リクエストに「gcpEncryption」パラメータを使用します。

   例

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-1/cryptoKeys/generatedkey1"
  }
```

参照 "NetApp Console自動化ドキュメント"「GcpEncryption」パラメータの使用に関する詳細については、こちらをご覧ください。

Google Cloud でCloud Volumes ONTAPのライセンスを設定する

Cloud Volumes ONTAPで使用するライセンス オプションを決定したら、新しいシステムを作成するときにそのライセンス 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

最大 500 GiB のプロビジョニング容量でCloud Volumes ONTAP を無料で使用するには、Freemium オファリングを選択してください。"フリーミアムプランの詳細" 。

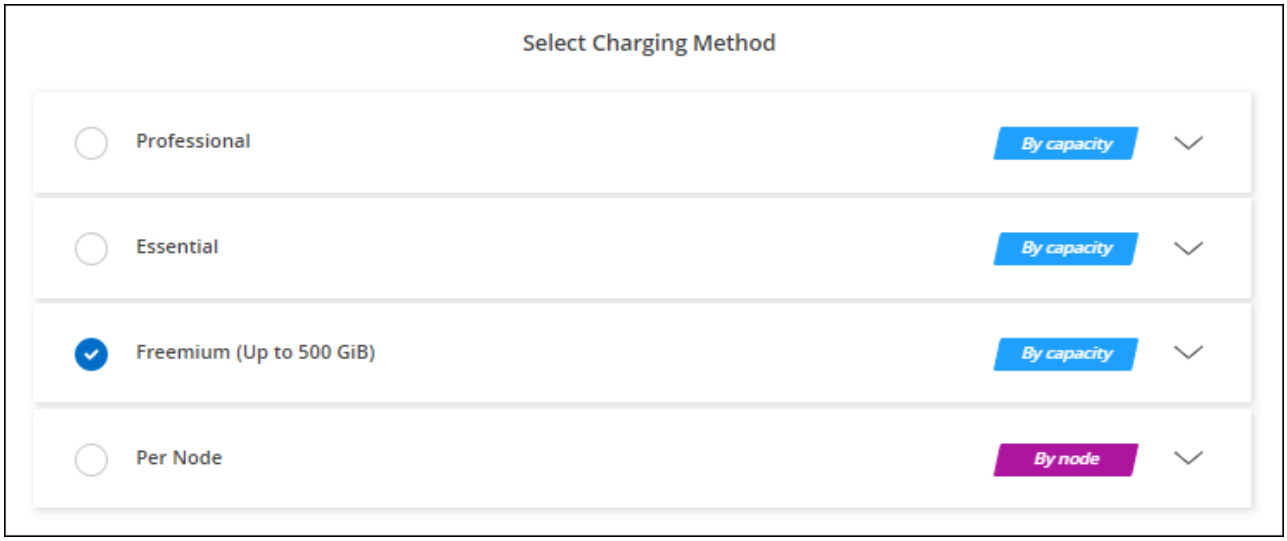
手順

1. 左側のナビゲーション メニューから、ストレージ > 管理 を選択します。
2. システム ページで、システムの追加 をクリックし、 NetApp Consoleの手順に従います。

   a. *詳細と認証情報*ページで、*認証情報の編集 > サブスクリプションの追加*をクリックし、指示に従ってGoogle Cloud Marketplaceの従量課金制オファーに登録します。

プロビジョニングされた容量が500GiBを超えない限り、マーケットプレイスのサブスクリプションを通じて課金されることはありません。その時点で、システムは自動的に"エッセンシャルパッケージ"。

b. コンソールに戻ったら、課金方法のページにアクセスして「**Freemium**」を選択します。



"Google Cloud でCloud Volumes ONTAP を起動するための手順をご覧ください"。

容量ベースのライセンス

容量ベースのライセンスでは、容量 1 TiB ごとにCloud Volumes ONTAPの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、Essentials パッケージまたは Professional パッケージというパッケージ形式で提供されます。

Essentials および Professional パッケージは、次の消費モデルまたは購入オプションで利用できます。

- NetAppから購入したライセンス（BYOL）
- Google Cloud Marketplace からの時間単位の従量課金制（PAYGO）サブスクリプション
- 年間契約

"容量ベースのライセンスについて詳しく見る"。

次のセクションでは、それぞれの消費モデルを開始する方法について説明します。

BYOL

NetAppからライセンス (BYOL) を購入して前払いすることで、任意のクラウド プロバイダーにCloud Volumes ONTAPシステムを導入できます。

はBYOLライセンスの購入、延長、および更新を制限しています。 "Cloud Volumes ONTAPのBYOL ライセンスの利用制限"。

手順

1. "ライセンスを取得するには、 NetApp の営業担当者にお問い合わせください。"

2. "NetAppサポートサイトのアカウントをNetApp Consoleに追加します"

   コンソールは NetApp のライセンス サービスに自動的にクエリを実行し、 NetAppサポート サイト アカウントに関連付けられているライセンスの詳細を取得します。エラーがなければ、コンソールはライセンスを追加します。

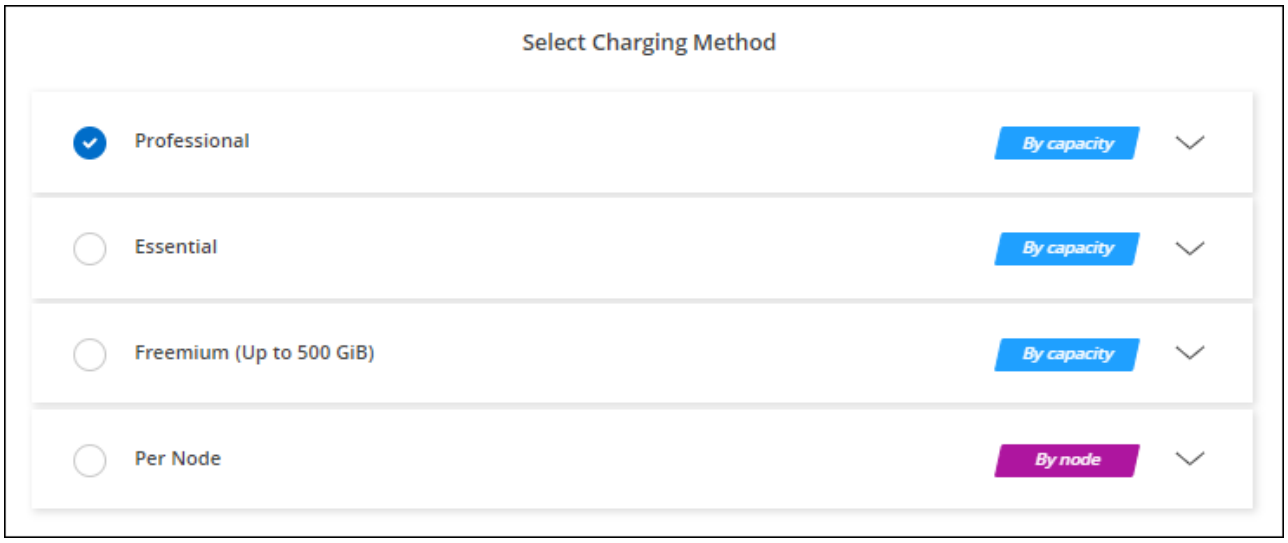
   Cloud Volumes ONTAPでライセンスを使用するには、コンソールからライセンスを利用できる必要があります。必要であれば、"コンソールにライセンスを手動で追加する" 。

3. *システム*ページで*システムの追加*をクリックし、手順に従います。

   a. *詳細と認証情報*ページで、*認証情報の編集 > サブスクリプションの追加*をクリックし、指示に従ってGoogle Cloud Marketplaceの従量課金制オファーに登録します。

      NetAppから購入したライセンスに対しては常に最初に課金されますが、ライセンス容量を超えた場合、またはライセンスの有効期限が切れた場合は、マーケットプレイスの時間単位料金で課金されます。

   b. コンソールに戻ったら、課金方法ページにアクセスして容量ベースのパッケージを選択します。



"Google Cloud でCloud Volumes ONTAP を起動するための手順をご覧ください" 。

PAYGOサブスクリプション

クラウド プロバイダーのマーケットプレイスからのオファーをサブスクライブして、時間単位で支払います。

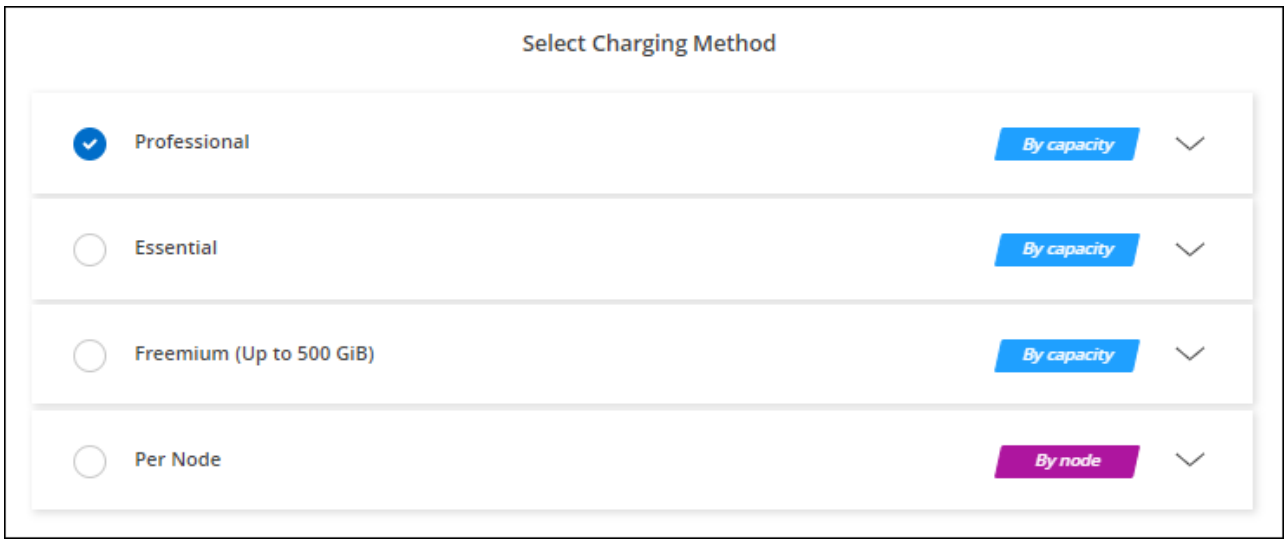
Cloud Volumes ONTAPシステムを作成すると、コンソールに、Google Cloud Marketplace で利用可能な契約に加入するように求めるメッセージが表示されます。そのサブスクリプションは課金システムに関連付けられます。同じサブスクリプションを追加のシステムにも使用できます。

手順

1. 左側のナビゲーション メニューから、ストレージ > 管理 を選択します。
2. *システム*ページで*システムの追加*をクリックし、手順に従います。

   a. *詳細と認証情報*ページで、*認証情報の編集 > サブスクリプションの追加*をクリックし、指示に従ってGoogle Cloud Marketplaceの従量課金制オファーに登録します。

b. コンソールに戻ったら、課金方法ページにアクセスして容量ベースのパッケージを選択します。



"Google Cloud でCloud Volumes ONTAP を起動するための手順をご覧ください" 。

アカウントに関連付けられている Google Cloud Marketplace サブスクリプションは、[設定] > [認証情報] ページから管理できます。 "Google Cloud の認証情報とサブスクリプションを管理する方法を学びます"

年間契約

年間契約を購入して、 Cloud Volumes ONTAP の料金を毎年支払います。

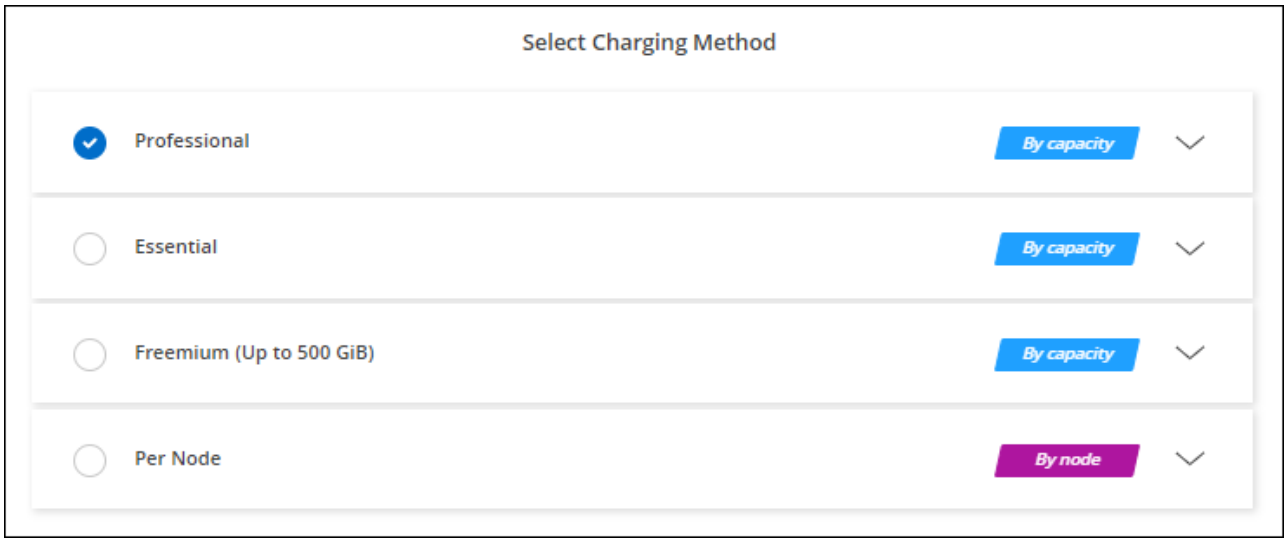
手順

1. 年間契約を購入するには、 NetApp の営業担当者にお問い合わせください。

   この契約は、Google Cloud Marketplace でプライベート オファーとして入手できます。

   NetApp がプライベート オファーを共有した後、システム作成中に Google Cloud Marketplace からサブスクライブするときに年間プランを選択できます。

2. *システム*ページで*システムの追加*をクリックし、手順に従います。
   a. *詳細と認証情報*ページで、*認証情報の編集 > サブスクリプションの追加*をクリックし、指示に従ってGoogle Cloud Marketplaceで年間プランを登録します。
   b. Google Cloud で、アカウントと共有された年間プランを選択し、[登録] をクリックします。
   c. コンソールに戻ったら、課金方法ページにアクセスして容量ベースのパッケージを選択します。



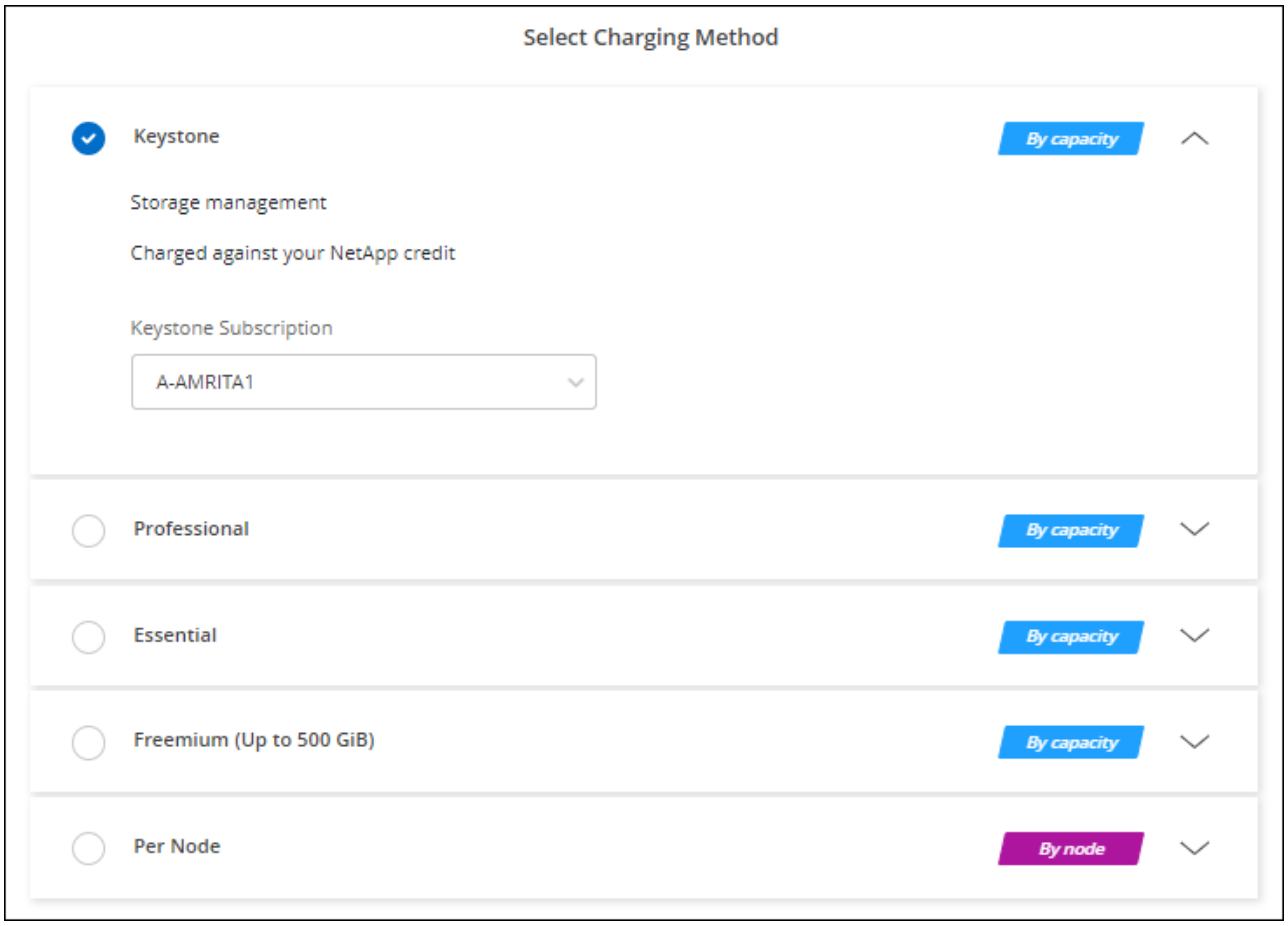
"Google Cloud でCloud Volumes ONTAP を起動するための手順をご覧ください" 。

Keystoneサブスクリプション

Keystoneサブスクリプションは、成長に応じて支払うサブスクリプション ベースのサービスです。"NetApp Keystoneサブスクリプションの詳細" 。

手順

1. まだ購読していない場合は、 "ネットアップに連絡"
2. NetAppに問い合わせ して、コンソール ユーザー アカウントに 1 つ以上のKeystoneサブスクリプションを承認します。
3. NetAppがアカウントを承認すると、"Cloud Volumes ONTAPで使用するためにサブスクリプションをリンクします" 。
4. *システム*ページで*システムの追加*をクリックし、手順に従います。
    a. 課金方法を選択するように求められたら、 Keystoneサブスクリプションの課金方法を選択します。



"Google Cloud でCloud Volumes ONTAP を起動するための手順をご覧ください" 。

ノードベースのライセンス

ノードベースライセンスは、Cloud Volumes ONTAPの旧世代ライセンスです。ノードベースライセンスはNetApp （BYOL）から取得でき、特定のケースに限りライセンス更新に利用できます。詳細については、以下を参照してください。

- "ノードベースライセンスの提供終了"
- "ノードベースライセンスの提供終了"
- "ノードベースのライセンスを容量ベースのライセンスに変換する"

Google Cloud でCloud Volumes ONTAPを起動する

Cloud Volumes ONTAPは、単一ノード構成または Google Cloud の HA ペアとして起動できます。

開始する前に

始める前に以下のものが必要です。

- 起動して実行中のNetApp Console エージェント。
  - あなたは "システムに関連付けられたコンソールエージェント"。

- "コンソールエージェントを常に実行しておく必要があります" 。
- コンソールエージェントに関連付けられたサービスアカウント "必要な権限を持っている必要があります"

- 使用する構成を理解すること。

  構成を選択し、管理者から Google Cloud ネットワーク情報を取得して準備しておく必要があります。詳細については、"Cloud Volumes ONTAP構成の計画" 。

- Cloud Volumes ONTAPのライセンスを設定するために必要なことを理解していること。

  "ライセンスの設定方法を学ぶ" 。

- Google Cloud APIは "プロジェクトで有効化":
  - クラウド デプロイメント マネージャー V2 API
  - クラウドロギングAPI
  - クラウド リソース マネージャー API
  - コンピューティングエンジン API
  - アイデンティティとアクセス管理 (IAM) API

Google Cloud でシングルノード システムを起動する

NetApp Consoleでシステムを作成し、Google Cloud でCloud Volumes ONTAP を起動します。

手順

1. 左側のナビゲーション メニューから、ストレージ **>** 管理 を選択します。
2. *システム*ページで、*システムの追加*をクリックし、指示に従います。
3. 場所を選択: **Google Cloud** と * Cloud Volumes ONTAP* を選択します。
4. プロンプトが表示されたら、 "コンソールエージェントを作成する" 。
5. 詳細と認証情報: プロジェクトを選択し、クラスター名を指定し、オプションでサービス アカウントを選択し、オプションでラベルを追加して、認証情報を指定します。

   次の表では、ガイダンスが必要になる可能性のあるフィールドについて説明します。

フィールド	説明
システム名	コンソールは、システム名を使用して、 Cloud Volumes ONTAPシステムとGoogle Cloud VM インスタンスの両方に名前を付けます。このオプションを選択した場合、定義済みのセキュリティ グループのプレフィックスとしても名前が使用されます。
サービスアカウント名	使用予定の場合"データ階層化"または "NetApp Backup and Recovery"Cloud Volumes ONTAPを使用する場合は、サービス アカウント を有効にし、事前定義されたストレージ管理者ロールを持つサービス アカウントを選択する必要があります。"サービスアカウントの作成方法を学ぶ" 。

フィールド	説明
ラベルを追加する	ラベルは、Google Cloud リソースのメタデータです。コンソールは、Cloud Volumes ONTAPシステムと、システムに関連付けられた Google Cloud リソースにラベルを追加します。システムを作成するときに、ユーザー インターフェイスから最大 4 つのラベルを追加でき、作成後にさらにラベルを追加できます。システムを作成するときに、API ではラベルが 4 つに制限されないことに注意してください。ラベルの詳細については、 "Google Cloud ドキュメント: ラベル付けリソース" 。
ユーザ名とパスワード	これらは、Cloud Volumes ONTAPクラスター管理者アカウントの資格情報です。これらの資格情報を使用して、 ONTAP System Manager またはONTAP CLI を介してCloud Volumes ONTAPに接続できます。デフォルトの *admin* ユーザー名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。
プロジェクトを編集	Cloud Volumes ONTAPを配置するプロジェクトを選択します。デフォルトのプロジェクトは、コンソールがあるプロジェクトです。 ドロップダウン リストに追加のプロジェクトが表示されない場合は、サービス アカウントが他のプロジェクトにまだ関連付けられていません。Google Cloud Console に移動し、IAM サービスを開いて、プロジェクトを選択します。NetApp Console に使用するロールを持つサービス アカウントをそのプロジェクトに追加します。プロジェクトごとにこの手順を繰り返す必要があります。 これはコンソール用に設定したサービスアカウントです。"このページに記載されている通り" 。 選択した資格情報をサブスクリプションに関連付けるには、「サブスクリプションの追加」をクリックします。 従量課金制のCloud Volumes ONTAPシステムを作成するには、Google Cloud マーケットプレイスからCloud Volumes ONTAPのサブスクリプションに関連付けられている Google Cloud プロジェクトを選択する必要があります。参照 "マーケットプレイスのサブスクリプションを Google Cloud 認証情報に関連付ける"。

6. サービス: このシステムで使用するサービスを選択します。バックアップとリカバリを選択するか、NetApp Cloud Tieringを使用するには、手順 3 でサービス アカウントを指定する必要があります。

   WORM とデータ階層化を利用する場合は、バックアップとリカバリを無効にし、バージョン 9.8 以降のCloud Volumes ONTAPシステムを展開する必要があります。

7. 場所と接続：システムの Google Cloud リージョンとゾーンを選択し、ファイアウォール ポリシーを選択して、データ階層化のための Google Cloud ストレージへのネットワーク接続を確認します。

   次の表では、ガイダンスが必要になる可能性のあるフィールドについて説明します。

フィールド	説明
接続検証	コールド データを Google Cloud Storage バケットに階層化するには、 Cloud Volumes ONTAP が存在するサブネットをプライベート Google アクセス用に構成する必要があります。手順については、 "Google Cloud ドキュメント: プライベート Google アクセスの設定" 。
生成されたファイアウォールポリシー	コンソールでファイアウォール ポリシーを生成させる場合は、トラフィックを許可する方法を選択する必要があります。 • 選択した **VPC** のみ を選択した場合、受信トラフィックのソース フィルターは、選択した VPC のサブネット範囲と、コンソール エージェントが存在する VPC のサブネット範囲になります。これは推奨されるオプションです。 • すべての **VPC** を選択した場合、受信トラフィックのソース フィルターは 0.0.0.0/0 IP 範囲になります。
既存のファイアウォールポリシーを使用する	既存のファイアウォール ポリシーを使用する場合は、必要なルールが含まれていることを確認してください。"Cloud Volumes ONTAPのファイアウォールルールについて学ぶ"

8. 課金方法と **NSS** アカウント: このシステムで使用する課金オプションを指定し、 NetApp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学ぶ"
   - "ライセンスの設定方法を学ぶ"
9. 事前構成済みパッケージ：パッケージの1つを選択してCloud Volumes ONTAPシステムを迅速に導入するか、*独自の構成を作成*をクリックします。事前構成済みパッケージは、選択したCloud Volumes ONTAPバージョンによって異なります。たとえば、Cloud Volumes ONTAP 9.18.1以降では、ConsoleにはHyperdisk Balancedディスクを含むC3 VMを含むパッケージが表示されます。ワークロードのニーズに応じて、IOPSやスループットパラメータなどの構成を変更できます。

   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構成を確認し、承認するだけです。
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、マシンタイプを選択します。

    選択したバージョンに対して新しいリリース候補、一般提供、またはパッチ リリースが利用可能な場合、コンソールは作成時にシステムをそのバージョンに更新します。たとえば、 Cloud Volumes ONTAP 9.13.1 を選択し、9.13.1 P4 が利用可能な場合は更新が行われます。更新は、あるリリースから別のリリース (たとえば、9.13 から 9.14) には行われません。
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 (ディスク タイプと各ディスクのサイズ) を選択します。

    ディスク タイプは初期ボリューム用です。後続のボリュームには異なるディスク タイプを選択できます。

    ディスク サイズは、初期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 オプションを使用するときにコンソールが作成する追加のアグリゲートのすべてのディスクに適用されます。高度な割り当てオプションを使用して、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、以下を参照してください。"Google Cloud でシステムのサイズを決定する" 。

12. フラッシュキャッシュ、書き込み速度、**WORM**:

    a. 必要に応じて、**Flash Cache** を有効にするか、標準 または 高 の書き込み速度を選択します。

    https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-gcp.html#flash-cache-support["Flash Cache"^]とlink:concept-write-speed.html["書き込み速度"]の詳細をご覧ください。

    「高」書き込み速度オプションを選択すると、高速書き込み速度と、8,896 バイトの最大転送単位 (MTU) をさらに高めることができます。さらに、MTU が 8,896 と高いため、デプロイメントには VPC-1、VPC-2、VPC-3 を選択する必要があります。 VPC-1、VPC-2、VPC-3の詳細については、以下を参照してください。 "VPC-1、VPC-2 、VPC-3のルール" 。

    b. 必要に応じて、一度書き込み、何度も読み取り可能な (WORM) ストレージをアクティブ化します。

    Cloud Volumes ONTAPバージョン 9.7 以下でデータ階層化が有効になっている場合、WORM を有効にすることはできません。 WORM と階層化を有効にした後、 Cloud Volumes ONTAP 9.8 への復元またはダウングレードはブロックされます。

    "WORMストレージについて詳しくはこちら" 。

    a. WORM ストレージを有効にする場合は、保持期間を選択します。

13. **Google Cloud Platform** でのデータ階層化: 初期アグリゲートでデータ階層化を有効にするかどうかを選択し、階層化データのストレージ クラスを選択してから、定義済みのストレージ管理者ロールを持つサービス アカウントを選択するか (Cloud Volumes ONTAP 9.7 以降に必要)、Google Cloud アカウントを選択します (Cloud Volumes ONTAP 9.6 に必要)。

    次の点に注意してください。

    - コンソールは、Cloud Volumes ONTAPインスタンスにサービス アカウントを設定します。このサービス アカウントは、Google Cloud Storage バケットへのデータ階層化の権限を付与します。コンソール エージェント サービス アカウントを階層化サービス アカウントのユーザーとして必ず追加してください。そうしないと、コンソールから選択できません。
    - Google Cloud アカウントの追加に関するヘルプについては、以下を参照してください。 "9.6 でデータ階層化を行うための Google Cloud アカウントの設定と追加" 。
    - 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。
    - データ階層化を無効にした場合、後続のアグリゲートで有効にすることはできますが、システムをオフにして、Google Cloud Console からサービス アカウントを追加する必要があります。

    "データ階層化の詳細" 。

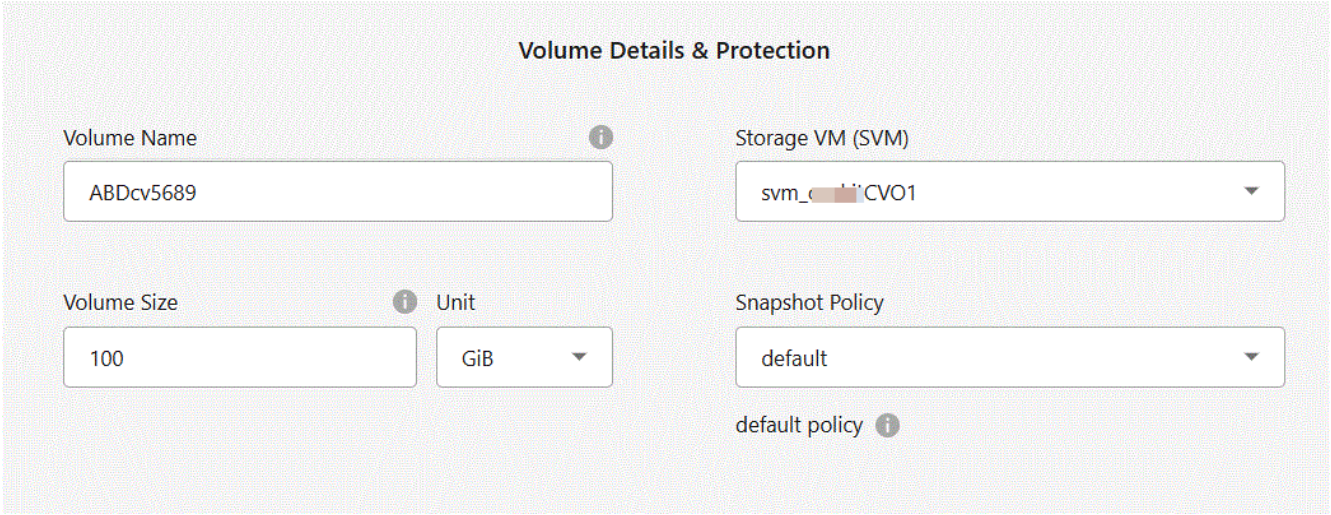
14. ボリュームの作成: 新しいボリュームの詳細を入力するか、[スキップ] をクリックします。

    "サポートされているクライアントプロトコルとバージョンについて学ぶ" 。

このページのいくつかのフィールドは説明不要です。次の表では、ガイダンスが必要になる可能性のある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な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、コンソール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、ユーザーとグループの共有へのアクセス レベル (アクセス制御リストまたは ACL とも呼ばれます) を制御できます。ローカルまたはドメインの Windows ユーザーまたはグループ、あるいは UNIX ユーザーまたはグループを指定できます。ドメイン Windows ユーザー名を指定する場合は、domain\username の形式を使用してユーザーのドメインを含める必要があります。
スナップショットポリシー	スナップショット コピー ポリシーは、自動的に作成されるNetAppスナップショット コピーの頻度と数を指定します。NetAppスナップショット コピーは、パフォーマンスに影響を与えず、最小限のストレージしか必要としない、ポイントインタイム ファイル システム イメージです。デフォルトのポリシーを選択するか、ポリシーなしを選択できます。一時データの場合は none を選択できます (例: Microsoft SQL Server の場合は tempdb)。
詳細オプション（NFSのみ）	ボリュームの NFS バージョン (NFSv3 または NFSv4) を選択します。
イニシエーター 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供されます。イニシエーター グループは、iSCSI ホスト ノード名のテーブルであり、どのイニシエーターがどの 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 Ethernet ネットワーク アダプター (NIC)、ソフトウェア イニシエーターを備えた TCP オフロード エンジン (TOE) カード、統合ネットワーク アダプター (CNA)、または専用ホスト バス アダプター (HBA) を介してネットワークに接続し、iSCSI 修飾名 (IQN) によって識別されます。 iSCSI ボリュームを作成すると、コンソールによって LUN が自動的に作成されます。ボリュームごとに 1 つの LUN を作成するだけで簡単になるので、管理は不要です。ボリュームを作成したら、"IQNを使用してホストからLUNに接続します" 。

次の画像は、ボリューム作成ウィザードの最初のページを示しています。



15. **CIFS** セットアップ: CIFS プロトコルを選択した場合は、CIFS サーバー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 サーバーの名前解決を提供する DNS サーバーの IP アドレス。これらのDNSサーバには、Active DirectoryのLDAPサーバと、CIFSサーバが参加するドメインのドメイン コントローラを見つけるために必要なサービス 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。 Google マネージド Active Directory を構成している場合、デフォルトでは 169.254.169.254 IP アドレスを使用して AD にアクセスできます。
参加するActive Directoryドメイン	CIFS サーバーが参加する Active Directory (AD) ドメインの FQDN。
ドメインへの参加を許可された資格情報	AD ドメイン内の指定された組織単位 (OU) にコンピューターを追加するのに十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS server NetBIOS name	AD ドメイン内で一意の CIFS サーバー名。
組織単位	CIFS サーバーに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。 Google Managed Microsoft AD をCloud Volumes ONTAPの AD サーバーとして構成するには、このフィールドに **OU=Computers,OU=Cloud** と入力します。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud ドキュメント: Google Managed Microsoft AD の組織単位"^]
DNSドメイン	Cloud Volumes ONTAPストレージ仮想マシン (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 サーバーを構成するには、「**Active Directory** ドメインを使用する」を選択します。別のアドレスを使用して NTP サーバーを構成する必要がある場合は、API を使用する必要があります。詳細については、 "NetApp Console自動化ドキュメント"詳細については。 NTP サーバーを設定できるのは、CIFS サーバーを作成するときだけであることに注意してください。 CIFS サーバーを作成した後は構成できません。

16. 使用プロファイル、ディスク タイプ、階層化ポリシー: 必要に応じて、ストレージ効率機能を有効にするかどうか、およびボリューム階層化ポリシーを変更するかどうかを選択します。

詳細については、"ボリューム使用プロファイルを選択する" 、"データ階層化の概要" 、 そして "KB: CVO ではどのようなインライン ストレージ効率機能がサポートされていますか?"

17. 確認と承認: 選択内容を確認して確定します。
    a. 構成の詳細を確認します。
    b. 詳細情報 をクリックすると、サポートと、コンソールで購入する Google Cloud リソースの詳細を確認できます。
    c. 理解しました... チェックボックスを選択します。
    d. [Go] をクリックします。

結果

コンソールはCloud Volumes ONTAPシステムを展開します。 *監査*ページで進捗状況を追跡できます。

Cloud Volumes ONTAPシステムのデプロイ中に問題が発生した場合は、失敗メッセージを確認してください。システムを選択して、「環境の再作成」をクリックすることもできます。

さらに詳しいヘルプについては、 "NetApp Cloud Volumes ONTAPサポート" 。

終了後の操作

- 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、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てください。
- ボリュームにクォータを適用する場合は、 ONTAP System Manager またはONTAP CLI を使用します。

  クォータを使用すると、ユーザー、グループ、または qtree が使用するディスク領域とファイル数を制限したり追跡したりできます。

> 展開プロセスが完了したら、Google Cloud ポータル内のシステム生成のCloud Volumes ONTAP構成（システムタグやGoogle Cloud リソースに設定されたラベルなど）を変更しないでください。これらの構成に変更を加えると、予期しない動作やデータ損失が発生する可能性があります。

Google Cloud で HA ペアを起動する

コンソールでシステムを作成し、Google Cloud でCloud Volumes ONTAP を起動します。

手順

1. 左側のナビゲーション メニューから、ストレージ > 管理 を選択します。
2. システム ページで、ストレージ > システム をクリックし、指示に従います。
3. 場所を選択: **Google Cloud** と * Cloud Volumes ONTAP HA* を選択します。
4. 詳細と認証情報: プロジェクトを選択し、クラスター名を指定し、オプションでサービス アカウントを選択し、オプションでラベルを追加して、認証情報を指定します。

   次の表では、ガイダンスが必要になる可能性のあるフィールドについて説明します。

フィールド	説明
システム名	コンソールは、システム名を使用して、 Cloud Volumes ONTAPシステムと Google Cloud VM インスタンスの両方に名前を付けます。このオプションを選択した場合、定義済みのセキュリティ グループのプレフィックスとしても名前が使用されます。
サービスアカウント名	ご利用予定の場合は"NetApp Cloud Tiering"または "バックアップとリカバリ" サービスでは、サービス アカウント スイッチを有効にして、定義済みのストレージ管理者ロールを持つサービス アカウントを選択する必要があります。
ラベルを追加する	ラベルは、Google Cloud リソースのメタデータです。コンソールは、Cloud Volumes ONTAPシステムと、システムに関連付けられた Google Cloud リソースにラベルを追加します。システムを作成するときに、ユーザー インターフェイスから最大 4 つのラベルを追加でき、作成後にさらにラベルを追加できます。システムを作成するときに、API ではラベルが 4 つに制限されないことに注意してください。ラベルの詳細については、 "Google Cloud ドキュメント: ラベル付けリソース" 。
ユーザ名とパスワード	これらは、Cloud Volumes ONTAPクラスター管理者アカウントの資格情報です。これらの資格情報を使用して、 ONTAP System Manager またはONTAP CLI を介してCloud Volumes ONTAPに接続できます。デフォルトの *admin* ユーザー名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。
プロジェクトを編集	Cloud Volumes ONTAPを配置するプロジェクトを選択してください。 ドロップダウン リストに追加のプロジェクトが表示されない場合は、サービス アカウントが他のプロジェクトにまだ関連付けられていません。Google Cloud Console に移動し、IAM サービスを開いて、プロジェクトを選択します。NetApp Console に使用するロールを持つサービス アカウントをそのプロジェクトに追加します。プロジェクトごとにこの手順を繰り返す必要があります。 これはコンソール用に設定したサービスアカウントです。"このページに記載されている通り" 。 選択した資格情報をサブスクリプションに関連付けるには、「サブスクリプションの追加」をクリックします。 従量課金制の Cloud Volumes ONTAPシステムを作成するには、Google Cloud Marketplace からCloud Volumes ONTAPのサブスクリプションに関連付けられている Google Cloud プロジェクトを選択する必要があります。参照 "マーケットプレイスのサブスクリプションを Google Cloud 認証情報に関連付ける"。

5. サービス: このシステムで使用するサービスを選択します。バックアップとリカバリを選択するか、NetApp Cloud Tieringを使用するには、手順 3 でサービス アカウントを指定する必要があります。

   WORM とデータ階層化を利用する場合は、バックアップとリカバリを無効にし、バージョン 9.8 以降のCloud Volumes ONTAPシステムを展開する必要があります。

6. **HA** 展開モデル：HA 構成に複数のゾーン（推奨）または単一のゾーンを選択します。次に、地域とゾーンを選択します。

"HA展開モデルの詳細" 。

7. 接続: HA 構成に 4 つの異なる VPC、各 VPC 内のサブネットを選択し、ファイアウォール ポリシーを選択します。

   "ネットワーク要件の詳細" 。

   次の表では、ガイダンスが必要になる可能性のあるフィールドについて説明します。

フィールド	説明
生成されたポリシー	コンソールでファイアウォール ポリシーを生成させる場合は、トラフィックを許可する方法を選択する必要があります。 • 選択した **VPC** のみ を選択した場合、受信トラフィックのソース フィルターは、選択した VPC のサブネット範囲と、コンソール エージェントが存在する VPC のサブネット範囲になります。これは推奨されるオプションです。 • すべての **VPC** を選択した場合、受信トラフィックのソース フィルターは 0.0.0.0/0 IP 範囲になります。
既存のものを使用する	既存のファイアウォール ポリシーを使用する場合は、必要なルールが含まれていることを確認してください。"Cloud Volumes ONTAPのファイアウォールルールについて学ぶ" 。

8. 課金方法と **NSS** アカウント: このシステムで使用する課金オプションを指定し、 NetAppサポート サイト 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学ぶ" 。
   - "ライセンスの設定方法を学ぶ" 。
9. 事前構成済みパッケージ: パッケージの 1 つを選択してCloud Volumes ONTAPシステムをすばやく展開するか、*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構成を確認し、承認するだけです。

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、マシンタイプを選択します。

    選択したバージョンに対して新しいリリース候補、一般提供、またはパッチ リリースが利用可能な場合、コンソールは作成時にシステムをそのバージョンに更新します。たとえば、 Cloud Volumes ONTAP 9.13.1 を選択し、9.13.1 P4 が利用可能な場合は更新が行われます。更新は、あるリリースから別のリリース (たとえば、9.13 から 9.14) には行われません。

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 (ディスク タイプと各ディスクのサイズ) を選択します。

    ディスク タイプは初期ボリューム用です。後続のボリュームには異なるディスク タイプを選択できます。

    ディスク サイズは、初期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 オプションを使用するときにコンソールが作成する追加のアグリゲートのすべてのディスクに適用されます。高度な

割り当てオプションを使用して、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、以下を参照してください。"Google Cloud でシステムのサイズを決定する" 。

12. フラッシュキャッシュ、書き込み速度、**WORM**:

    a. 必要に応じて、**Flash Cache** を有効にするか、標準 または 高 の書き込み速度を選択します。

    `https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-gcp.html#flash-cache-support["Flash Cache"^]とlink:concept-write-speed.html["書き込み速度"]の詳細をご覧ください。`

    n2-standard-16、n2-standard-32、n2-standard-48、n2-standard-64 インスタンス タイプの 高 書き込み速度オプションでは、高速書き込み速度と 8,896 バイトの最大転送単位 (MTU) のより高い速度を利用できます。さらに、MTU が 8,896 と高いため、デプロイメントには VPC-1、VPC-2、VPC-3 を選択する必要があります。高速書き込み速度と 8,896 の MTU は機能に依存しており、構成されたインスタンス内で個別に無効にすることはできません。 VPC-1、VPC-2、VPC-3の詳細については、以下を参照してください。 "VPC-1、VPC-2、VPC-3のルール" 。

    b. 必要に応じて、一度書き込み、何度も読み取り可能な (WORM) ストレージをアクティブ化します。

    Cloud Volumes ONTAPバージョン 9.7 以下でデータ階層化が有効になっている場合、WORM を有効にすることはできません。 WORM と階層化を有効にした後、 Cloud Volumes ONTAP 9.8 への復元またはダウングレードはブロックされます。

"WORMストレージについて詳しくはこちら" 。

    a. WORM ストレージを有効にする場合は、保持期間を選択します。

13. **Google Cloud** でのデータ階層化: 初期集約でデータ階層化を有効にするかどうかを選択し、階層化されたデータのストレージ クラスを選択してから、事前定義されたストレージ管理者のロールを持つサービス アカウントを選択します。

    次の点に注意してください。

    - コンソールは、Cloud Volumes ONTAPインスタンスにサービス アカウントを設定します。このサービス アカウントは、Google Cloud Storage バケットへのデータ階層化の権限を付与します。コンソール エージェント サービス アカウントを階層化サービス アカウントのユーザーとして必ず追加してください。そうしないと、コンソールから選択できません。
    - 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。
    - データ階層化を無効にした場合、後続のアグリゲートで有効にすることはできますが、システムをオフにして、Google Cloud Console からサービス アカウントを追加する必要があります。

    "データ階層化の詳細" 。

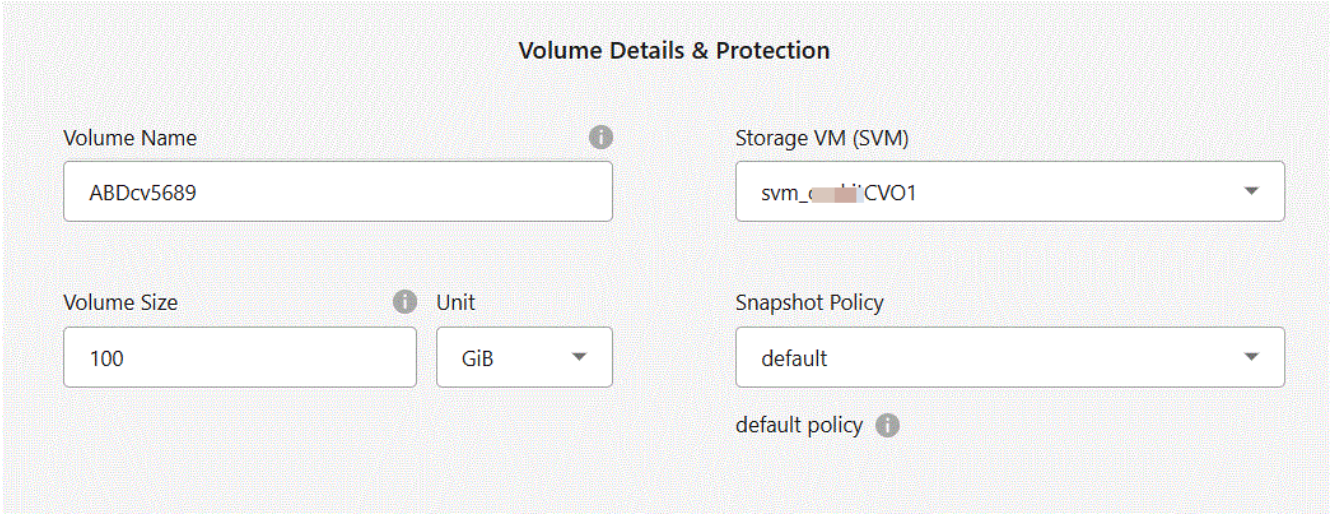
14. ボリュームの作成: 新しいボリュームの詳細を入力するか、[スキップ] をクリックします。

    "サポートされているクライアントプロトコルとバージョンについて学ぶ" 。

このページのいくつかのフィールドは説明不要です。次の表では、ガイダンスが必要になる可能性のある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な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、コンソール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、ユーザーとグループの共有へのアクセス レベル (アクセス制御リストまたは ACL とも呼ばれます) を制御できます。ローカルまたはドメインの Windows ユーザーまたはグループ、あるいは UNIX ユーザーまたはグループを指定できます。ドメイン Windows ユーザー名を指定する場合は、domain\username の形式を使用してユーザーのドメインを含める必要があります。
スナップショットポリシー	スナップショット コピー ポリシーは、自動的に作成されるNetAppスナップショット コピーの頻度と数を指定します。NetAppスナップショット コピーは、パフォーマンスに影響を与えず、最小限のストレージしか必要としない、ポイントインタイム ファイル システム イメージです。デフォルトのポリシーを選択するか、ポリシーなしを選択できます。一時データの場合は none を選択できます (例: Microsoft SQL Server の場合は tempdb)。
詳細オプション（NFSのみ）	ボリュームの NFS バージョン (NFSv3 または NFSv4) を選択します。
イニシエーター 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供されます。イニシエーター グループは、iSCSI ホスト ノード名のテーブルであり、どのイニシエーターがどの 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 Ethernet ネットワーク アダプター (NIC)、ソフトウェア イニシエーターを備えた TCP オフロード エンジン (TOE) カード、統合ネットワーク アダプター (CNA)、または専用ホスト バス アダプター (HBA) を介してネットワークに接続し、iSCSI 修飾名 (IQN) によって識別されます。 iSCSI ボリュームを作成すると、コンソールによって LUN が自動的に作成されます。ボリュームごとに 1 つの LUN を作成するだけで簡単になるので、管理は不要です。ボリュームを作成したら、"IQNを使用してホストからLUNに接続します" 。

次の画像は、ボリューム作成ウィザードの最初のページを示しています。



15. **CIFS** セットアップ: CIFS プロトコルを選択した場合は、CIFS サーバー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 サーバーの名前解決を提供する DNS サーバーの IP アドレス。これらのDNSサーバには、Active DirectoryのLDAPサーバと、CIFSサーバが参加するドメインのドメイン コントローラを見つけるために必要なサービス 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。 Google マネージド Active Directory を構成している場合、デフォルトでは 169.254.169.254 IP アドレスを使用して AD にアクセスできます。
参加するActive Directoryドメイン	CIFS サーバーが参加する Active Directory (AD) ドメインの FQDN。
ドメインへの参加を許可された資格情報	AD ドメイン内の指定された組織単位 (OU) にコンピューターを追加するのに十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS server NetBIOS name	AD ドメイン内で一意の CIFS サーバー名。
組織単位	CIFS サーバーに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。 Google Managed Microsoft AD をCloud Volumes ONTAPの AD サーバーとして構成するには、このフィールドに **OU=Computers,OU=Cloud** と入力します。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud ドキュメント: Google Managed Microsoft AD の組織単位"^]
DNSドメイン	Cloud Volumes ONTAPストレージ仮想マシン (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 サーバーを構成するには、「**Active Directory** ドメインを使用する」を選択します。別のアドレスを使用して NTP サーバーを構成する必要がある場合は、API を使用する必要があります。参照 "NetApp Console自動化ドキュメント"詳細については。 NTP サーバーを設定できるのは、CIFS サーバーを作成するときだけであることに注意してください。 CIFS サーバーを作成した後は構成できません。

16. 使用プロファイル、ディスク タイプ、階層化ポリシー: 必要に応じて、ストレージ効率機能を有効にするかどうか、およびボリューム階層化ポリシーを変更するかどうかを選択します。

詳細については、"ボリューム使用プロファイルを選択する" 、"データ階層化の概要" 、 そして "KB: CVO ではどのようなインライン ストレージ効率機能がサポートされていますか?"

17. 確認と承認: 選択内容を確認して確定します。
    a. 構成の詳細を確認します。
    b. 詳細情報 をクリックすると、サポートと、コンソールで購入する Google Cloud リソースの詳細を確認できます。
    c. 理解しました... チェックボックスを選択します。
    d. [Go] をクリックします。

結果

コンソールはCloud Volumes ONTAPシステムを展開します。 *監査*ページで進捗状況を追跡できます。

Cloud Volumes ONTAPシステムのデプロイ中に問題が発生した場合は、失敗メッセージを確認してください。システムを選択して、「環境の再作成」をクリックすることもできます。

さらに詳しいヘルプについては、 "NetApp Cloud Volumes ONTAPサポート" 。

終了後の操作

- 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、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てください。
- ボリュームにクォータを適用する場合は、 ONTAP System Manager またはONTAP CLI を使用します。

  クォータを使用すると、ユーザー、グループ、または qtree が使用するディスク領域とファイル数を制限したり追跡したりできます。

> 展開プロセスが完了したら、Google Cloud ポータル内のシステム生成のCloud Volumes ONTAP構成（システムタグやGoogle Cloud リソースに設定されたラベルなど）を変更しないでください。これらの構成に変更を加えると、予期しない動作やデータ損失が発生する可能性があります。

関連リンク

- "Google Cloud でのCloud Volumes ONTAP構成の計画"

Google Cloud Platform イメージ検証

Cloud Volumes ONTAPで **Google Cloud** イメージを検証する方法を学びます

Google Cloud イメージ検証は、強化されたNetAppセキュリティ要件に準拠しています。イメージを生成するスクリプトに変更が加えられ、このタスク専用に生成された秘密鍵を使用して、途中でイメージに署名するようになりました。 Google Cloud イメージの整合性は、Google Cloud の署名済みダイジェストと公開証明書を使用して検証できます。これらの証明書は、以下からダウンロードできます。 "NSS"特定のリリース用。

> Google Cloud イメージ検証は、Cloud Volumes ONTAPソフトウェア バージョン 9.13.0 以降でサポートされています。

Google Cloud イメージをCloud Volumes ONTAPの RAW 形式に変換する

新しいインスタンスやアップグレードを展開するために使用されているイメージ、または既存のイメージで使用されているイメージは、 "NetAppサポート サイト (NSS)" 。署名されたダイジェストと証明書は、NSS ポータルからダウンロードできます。 NetAppサポートによって共有されたイメージに対応する適切なリリースのダイジェストと証明書をダウンロードしていることを確認してください。たとえば、9.13.0 イメージには、NSS で利用可能な 9.13.0 署名ダイジェストと証明書が含まれます。

このステップはなぜ必要なのでしょうか?

Google Cloud からのイメージを直接ダウンロードすることはできません。署名されたダイジェストと証明書に対してイメージを検証するには、2 つのファイルを比較してイメージをダウンロードするメカニズムが必要です。これを行うには、イメージを disk.raw 形式にエクスポート/変換し、結果を Google Cloud のストレージ バケットに保存する必要があります。このプロセスでは、disk.raw ファイルが tar 圧縮され、gzip 圧縮されます。

ユーザー/サービス アカウントには、次の操作を実行する権限が必要です。

- Google ストレージ バケットへのアクセス
- Google Storage バケットに書き込む
- クラウド ビルド ジョブを作成する (エクスポート プロセス中に使用)
- 希望の画像へのアクセス
- 画像のエクスポートタスクを作成する

イメージを検証するには、disk.raw 形式に変換してからダウンロードする必要があります。

Google Cloud コマンドラインを使用して Google Cloud イメージをエクスポートする

画像をクラウドストレージにエクスポートする推奨方法は、 "gcloud compute images エクスポートコマンド" 。このコマンドは、提供されたイメージを取得し、それを tar および gzip で圧縮された disk.raw ファイルに変換します。生成されたファイルは宛先 URL に保存され、検証のためにダウンロードできます。

この操作を実行するには、ユーザー/アカウントに、目的のバケットにアクセスして書き込む権限、イメージをエクスポートする権限、クラウド ビルド (Google がイメージをエクスポートするために使用) の権限が必要です。

gcloud を使用して Google Cloud イメージをエクスポートする

クリックして表示

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

圧縮ファイルを解凍

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

Google Cloud経由で画像をエクスポートする方法の詳細については、 "画像のエクスポートに関する Google Cloud ドキュメント" 。

画像署名検証

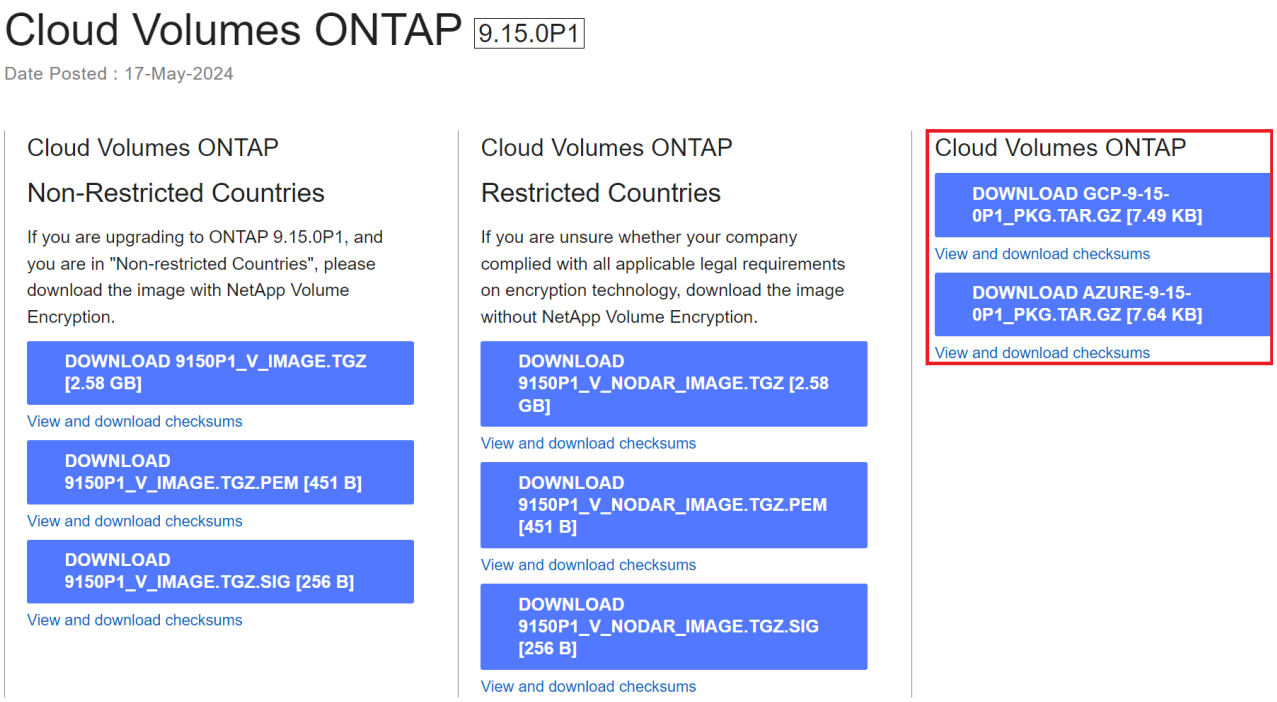
Cloud Volumes ONTAPの Google Cloud イメージ署名検証

エクスポートされた Google Cloud 署名付きイメージを検証するには、NSS からイメージ ダイジェスト ファイルをダウンロードして、disk.raw ファイルとダイジェスト ファイルの内容を検証する必要があります。

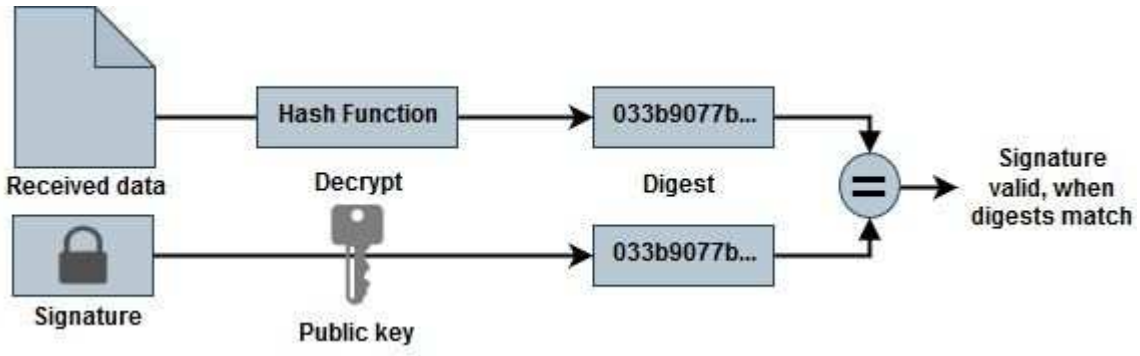
署名画像検証ワークフローの概要

以下は、Google Cloud 署名付きイメージ検証ワークフロー プロセスの概要です。

- から "NSS"次のファイルを含む Google Cloud アーカイブをダウンロードします。
  - 署名付きダイジェスト（.sig）
  - 公開鍵を含む証明書（.pem）
  - 証明書チェーン (.pem)



- 変換されたdisk.rawファイルをダウンロードする
- 証明書チェーンを使用して証明書を検証する
- 公開鍵を含む証明書を使用して署名されたダイジェストを検証する
  - 公開鍵を使用して署名されたダイジェストを復号化し、画像ファイルのダイジェストを抽出します。
  - ダウンロードしたdisk.rawファイルのダイジェストを作成する
  - 検証のために2つのダイジェストファイルを比較する



OpenSSL を使用して**Cloud Volumes ONTAP**の **Google Cloud** イメージの **disk.raw** ファイルを確認する

Google Cloudでダウンロードしたdisk.rawファイルを、以下のダイジェストファイルの内容と比較することができます。 "NSS" OpenSSL を使用します。

イメージを検証するための OpenSSL コマンドは、Linux、macOS、および Windows マシンと互換性があります。

手順

1. OpenSSL を使用して証明書を検証します。

クリックして表示

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
          e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
          22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
          38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
          fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
          bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. ダウンロードした disk.raw ファイル、署名、および証明書をディレクトリに配置します。
3. OpenSSL を使用して証明書から公開鍵を抽出します。
4. 抽出した公開キーを使用して署名を復号化し、ダウンロードした disk.raw ファイルの内容を確認します。

クリックして表示

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```