



# Google Cloud で始めましょう

## Cloud Volumes ONTAP

NetApp  
June 21, 2022

# 目次

|   |    |
|---|----|
| Google Cloud で始めましょう .....                          | 1  |
| Google Cloud の Cloud Volumes ONTAP のクイックスタート .....  | 1  |
| Google CloudでCloud Volumes ONTAP 構成を計画する .....      | 2  |
| Cloud Volumes ONTAP in GCP のネットワーク要件 .....          | 6  |
| GCP での VPC サービスコントロールの計画 .....                      | 16 |
| データ階層化とバックアップ用のサービスアカウントを作成します .....                | 18 |
| お客様が管理する暗号化キーを Cloud Volumes ONTAP で使用する .....      | 21 |
| Google CloudでCloud Volumes ONTAP のライセンスを設定します ..... | 22 |
| GCP での Cloud Volumes ONTAP の起動 .....                | 27 |

# Google Cloud で始めましょう

## Google Cloud の Cloud Volumes ONTAP のクイックスタート

Cloud Volumes ONTAP for GCP の使用を開始するには、いくつかの手順を実行します。

を持っていないければ ["コネクタ"](#) ただし、アカウント管理者がアカウントを作成する必要があります。 ["GCP でコネクタを作成する方法を説明します"](#)。

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

Cloud Manager には、ワークロードの要件に応じた事前設定パッケージが用意されています。または、独自の設定を作成することもできます。独自の設定を選択する場合は、使用可能なオプションを理解しておく必要があります。

["構成の計画の詳細については、こちらをご覧ください"](#)。

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

1. VPC とサブネットがコネクタと Cloud Volumes ONTAP 間の接続をサポートしていることを確認します。
2. データの階層化を有効にする場合は、["プライベート Google アクセス用の Cloud Volumes ONTAP サブネットを設定します"](#)。
3. HA ペアを導入する場合は、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ます。
4. 共有 VPC を使用する場合は、コネクタサービスアカウントに `_Compute Network User_role` を指定します。
5. ターゲット VPC からのアウトバウンドインターネットアクセスを有効にして、コネクタと Cloud Volumes ONTAP が複数のエンドポイントに接続できるようにします。

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

["ネットワーク要件の詳細については、こちらをご覧ください"](#)。

Cloud Volumes ONTAP には、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、を有効にする場合です ["データの階層化"](#) Google Cloud でコールドデータを低コストのオブジェクトストレージに階層化すること。2 つ目は、を有効にした場合です ["Cloud Backup サービスの略"](#) 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できます。

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。

["詳細な手順を参照してください"](#)。

["プロジェクトで次の Google Cloud API を有効にします"](#)。これらの API は、コネクタと Cloud Volumes ONTAP を導入するために必要です。

- Cloud Deployment Manager V2 API
- クラウドロギング API
- Cloud Resource Manager API の略
- Compute Engine API
- ID およびアクセス管理（IAM）API

[ 作業環境の追加 ] をクリックし、展開するシステムのタイプを選択して、ウィザードの手順を実行します。 "[詳細な手順を参照してください](#)"。

#### 関連リンク

- "[Cloud Manager からコネクタを作成します](#)"
- "[Linux ホストへの Connector ソフトウェアのインストール](#)"
- "[Cloud Manager が GCP 権限を使用して実行する処理](#)"

## Google CloudでCloud Volumes ONTAP 構成を計画する

Google Cloud に Cloud Volumes ONTAP を導入する場合は、ワークロードの要件に合わせて事前設定されたシステムを選択するか、または独自の設定を作成できます。独自の設定を選択する場合は、使用可能なオプションを理解しておく必要があります。

### Cloud Volumes ONTAP ライセンスを選択します

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

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

### サポートされているリージョンを選択します

Cloud Volumes ONTAP は、ほとんどの 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リージョンの完全なリストを表示します](#)"。

### 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 では、選択したライセンスタイプに応じて、複数のマシンタイプがサポートされます。

"[GCP の Cloud Volumes ONTAP でサポートされている構成](#)"

### ストレージの制限を確認

Cloud Volumes ONTAP システムの未フォーマット時の容量制限は、ライセンスに関連付けられています。追加の制限は、アグリゲートとボリュームのサイズに影響します。設定を計画する際には、これらの制限に注意する必要があります。

## GCPでシステムのサイズを設定します

Cloud Volumes ONTAP システムのサイジングを行うことで、パフォーマンスと容量の要件を満たすのに役立ちます。マシンタイプ、ディスクタイプ、およびディスクサイズを選択する際には、次の点に注意してください。

### マシンのタイプ

でサポートされているマシンタイプを確認します ["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ついて Google の詳細を確認します。ワークロードの要件を、マシンタイプの vCPU とメモリの数と一致させます。各 CPU コアは、ネットワークパフォーマンスを向上させ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 のドキュメント：「Performance」"](#)

### GCP ディスクタイプ

Cloud Volumes ONTAP 用のボリュームを作成する際には、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です。

- [\\_ゾーン SSD 永続ディスク\\_](#)： SSD 永続ディスクは、ランダム IOPS が高いワークロードに最適です。
- [\\_ゾーン バランシング永続ディスク\\_](#)：これらの SSD は、GB あたりの IOPS を下げて、パフォーマンスとコストのバランスを取ります。
- [\\_Zonal 標準パーシステントディスク\\_](#)：標準パーシステントディスクは経済的で、シーケンシャルな読み取り / 書き込み処理に対応できます。

詳細については、を参照してください ["Google Cloud のドキュメント：「ゾーン永続ディスク（標準および SSD）」](#)。

### GCP ディスクサイズ

Cloud Volumes ONTAP システムを導入する際には、初期ディスクサイズを選択する必要があります。そのあと、システムの容量を Cloud Manager で管理できるようになりますが、アグリゲートを手動で作成する場合は、次の点に注意してください。

- アグリゲート内のディスクはすべて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、必要なスペースを判断します。
- パーシステントディスクのパフォーマンスは、システムで使用可能なディスクサイズと vCPU の数に応じて自動的に拡張されます。

詳細については、以下を参照してください。

- ["Google Cloud のドキュメント：「ゾーン永続ディスク（標準および SSD）」](#)
- ["Google Cloud のドキュメント：「Optimizing Persistent Disk and Local SSD Performance」"](#)

## デフォルトのシステムディスクを表示します

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

- ["Cloud Volumes ONTAP システムデータ用のデフォルトディスクを Google Cloud で表示します"](#)。
- ["Google Cloud のドキュメント：リソースクォータ"](#)

Google Cloud Compute Engine では、リソース使用量にクォータが適用されるため、Cloud Volumes ONTAP を導入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。



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

## ネットワーク情報を収集

GCP で Cloud Volumes ONTAP を導入する場合は、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。

- シングルノードシステム \* のネットワーク情報

| GCP 情報                         | あなたの価値 |
|--------------------------------|--------|
| 地域                             |        |
| 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（独自のポリシーを使用している場合） |        |

- 複数ゾーン内の HA ペアのネットワーク情報 \*

| GCP 情報         | あなたの価値 |
|----------------|--------|
| 地域             |        |
| ノード 1 のゾーン     |        |
| ノード 2 のゾーン     |        |
| メディエーターのゾーン    |        |
| vPC-0 およびサブネット |        |
| vPC-1 とサブネット   |        |
| vPC-2 およびサブネット |        |
| vPC-3 とサブネット   |        |

| GCP 情報                         | あなたの価値 |
|--------------------------------|--------|
| ファイアウォールポリシー（独自のポリシー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 \*

| GCP 情報                         | あなたの価値 |
|--------------------------------|--------|
| 地域                             |        |
| ゾーン                            |        |
| vPC-0 およびサブネット                 |        |
| vPC-1 とサブネット                   |        |
| vPC-2 およびサブネット                 |        |
| vPC-3 とサブネット                   |        |
| ファイアウォールポリシー（独自のポリシーを使用している場合） |        |

## 書き込み速度を選択します

Cloud Manager では、Google Cloud のハイアベイラビリティ（HA）ペアを除く 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、高速書き込みを使用する場合の標準設定と高設定の違い、およびリスクと推奨事項を理解しておく必要があります。["書き込み速度の詳細については、こちらをご覧ください。"](#)

## ボリュームの使用プロファイルを選択してください

ONTAP には、必要なストレージの合計容量を削減できるストレージ効率化機能がいくつか搭載されています。Cloud Manager でボリュームを作成する場合は、これらの機能を有効にするプロファイルを選択するか、無効にするプロファイルを選択できます。これらの機能の詳細については、使用するプロファイルを決定する際に役立ちます。

NetApp Storage Efficiency 機能には、次のようなメリットがあります。

### シンプロビジョニング

物理ストレージプールよりも多くの論理ストレージをホストまたはユーザに提供します。ストレージスペースは、事前にストレージスペースを割り当てる代わりに、データの書き込み時に各ボリュームに動的に割り当てられます。

### 重複排除

同一のデータブロックを検索し、単一の共有ブロックへの参照に置き換えることで、効率を向上します。この手法では、同じボリュームに存在するデータの冗長ブロックを排除することで、ストレージ容量の要件を軽減します。

### 圧縮

プライマリ、セカンダリ、アーカイブストレージ上のボリューム内のデータを圧縮することで、データの

格納に必要な物理容量を削減します。

## Cloud Volumes ONTAP in GCP のネットワーク要件

Cloud Volumes ONTAP システムが正常に動作するように、Google Cloud Platform ネットワークをセットアップします。これには、コネクタと Cloud Volumes ONTAP のネットワークも含まれます。

HA ペアを導入する場合は、を実行します ["GCP での HA ペアの仕組みをご確認ください"](#)。

### Cloud Volumes ONTAP の要件

GCP では、次の要件を満たす必要があります。

#### 内部ロードバランサ

Cloud Manager は、Cloud Volumes ONTAP HA ペアへの受信トラフィックを管理する Google Cloud 内部ロードバランサ（TCP / UDP）を 4 つ自動作成します。セットアップは必要ありませんネットワークトラフィックを通知し、セキュリティ上の問題を緩和するだけで、この要件が満たされることがわかりました。

クラスタ管理用のロードバランサで、1 つは Storage VM（SVM）管理用、もう 1 つはノード 1 への NAS トラフィック用、もう 1 つはノード 2 への NAS トラフィック用です。

各ロードバランサの設定は次のとおりです。

- 共有プライベート IP アドレス × 1
- グローバル健全性チェック 1 回

デフォルトでは、ヘルスチェックで使用するポートは 63001、63002、および 63003 です。

- 地域 TCP バックエンドサービス × 1
- 地域 UDP バックエンドサービス × 1
- 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は無効です

グローバルアクセスはデフォルトでは無効になっていますが、展開後に有効にすることができます。クロスリージョントラフィックのレイテンシが大幅に高くなるため、この機能は無効にしました。誤ってリージョン間にマウントすることが原因でマイナスの体験が得られないようにしたいと考えていました。このオプションを有効にすることは、ビジネスニーズに固有のものです。

#### HA ペア用のゾーン

複数のゾーンまたは単一のゾーンに HA 構成を導入することで、データの高可用性を確保できます。HA ペアの作成時には、Cloud Manager から複数のゾーンまたは単一のゾーンの選択を求められます。

- 複数のゾーン（推奨）

3 つのゾーンに HA 構成を導入することで、ゾーン内で障害が発生した場合の継続的なデータ可用性を



確保できます。書き込みパフォーマンスは、単一のゾーンを使用する場合に比べてわずかに低くなりますが、最小のパフォーマンスです。

- シングルゾーン

Cloud Volumes ONTAP HA 構成では、単一のゾーンに導入する場合は分散配置ポリシーを使用します。このポリシーにより、HA 構成がゾーン内の単一点障害から保護されます。障害の切り分けに別々のゾーンを使用する必要はありません。

この導入モデルでは、ゾーン間にデータ出力料金が発生しないため、コストが削減されます。

## HA ペア用の仮想プライベートクラウド × 4

HA 構成には、4 つの Virtual Private Cloud (VPC ; 仮想プライベートクラウド) が必要です。GCP では各ネットワークインターフェイスが別々の 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 ペアの作成時に、Cloud Manager から 4 つの VPC を選択するよう求められます。

- vPC-0 : データおよびノードへのインバウンド接続
- vPC-1、VPC -2、および VPC -3 : ノードと HA メディエーター間の内部通信



## HA ペアのサブネット

VPC ごとにプライベートサブネットが必要です。

コネクタを VPC 0 に配置する場合は、サブネットで Private Google Access を有効にして API にアクセスし、データの階層化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、個別の CIDR 範囲が必要です。CIDR 範囲を重複させることはできません。

## シングルノードシステムに対応した 1 つの仮想プライベートクラウド

シングルノードシステムには 1 つの VPC が必要です。

## 共有 VPC

Cloud Volumes ONTAP とコネクタは、Google Cloud の共有 VPC とスタンドアロンの VPC でサポートされます。

シングルノードシステムの場合は、VPC は共有 VPC またはスタンドアロン VPC のどちらかになります。

HA ペアの場合は、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どちらかにすることができます。たとえば、VPC は VPC を共有化し、VPC は VPC 1、VPC は 2、VPC は 3 で構成されることになります。

共有 VPC を使用すると、複数のプロジェクトの仮想ネットワークを設定し、一元管理できます。ホストプロジェクト \_ で共有 VPC ネットワークをセットアップし、Connector および Cloud Volumes ONTAP 仮想マシンインスタンスをサービスプロジェクト \_ で導入できます。"[Google Cloud のドキュメント：「Shared VPC Overview」](#)"。

"[Connector の導入でカバーされている必要な共有 VPC の権限を確認します](#)"。

## 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 を導入する Google Cloud VPC で無効にする必要があります。パケットミラーリングがイネーブルの場合、Cloud Volumes ONTAP は正常に動作しません。

## Cloud Volumes ONTAP 用のアウトバウンドインターネットアクセス

Cloud Volumes ONTAP では、ネットアップ AutoSupport にメッセージを送信するためにアウトバウンドインターネットアクセスが必要です。ネットアップ AutoSupport は、ストレージの健全性をプロアクティブに監視します。

Cloud Volumes ONTAP が AutoSupport メッセージを送信できるように、ルーティングポリシーとファイアウォールポリシーで次のエンドポイントへの HTTP / HTTPS トラフィックを許可する必要があります。

- \ <https://support.netapp.com/aods/asupmessage>
- \ <https://support.netapp.com/asupprod/post/1.0/postAsup>

"[AutoSupport の検証方法について説明します](#)"。



HA ペアを使用している場合、HA メディエーターではアウトバウンドのインターネットアクセスは必要ありません。

## プライベート IP アドレス

Cloud Manager は、次の数のプライベート IP アドレスを GCP の Cloud Volumes ONTAP に割り当てます。

- **\* シングルノード \*** : 3 または 4 つのプライベート IP アドレス

Cloud Volumes ONTAP を API を使用して導入する場合、Storage VM (SVM) 管理 LIF の作成をスキップし、次のフラグを指定できます。

'kipsvmManagementLIF : 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、Storage VM (SVM) 管理 LIF が必要です。

- **\* HA ペア \*** : 14 または 15 個のプライベート IP アドレス

- VPC -0 の 7 つまたは 8 つのプライベート IP アドレス

Cloud Volumes ONTAP を API を使用して導入する場合、Storage VM (SVM) 管理 LIF の作成をスキップし、次のフラグを指定できます。

'kipsvmManagementLIF : true

- VPC 1 用のプライベート IP アドレスが 2 つあります
- VPC 2 のプライベート IP アドレス × 2
- VPC 3 つのプライベート IP アドレス

## ファイアウォールルール

ファイアウォールルールを作成する必要はありません。ファイアウォールルールは Cloud Manager で自動的に作成されます。独自のファイアウォールを使用する必要がある場合は、以下のファイアウォールルールを参照してください。

HA 構成には、次の 2 組のファイアウォールルールが必要です。

- VPC -0 の HA コンポーネントのルールセット。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。 [詳細はこちら](#)。
- VPC -1、VPC -2、および VPC -3 の HA コンポーネントに関するもう 1 つのルールセット。これらのルールは、HA コンポーネント間のインバウンド通信とアウトバウンド通信に対してオープンです。 [詳細はこちら](#)。

## の Cloud Volumes ONTAP から Google Cloud Storage への接続 データ階層化

コールドデータを Google Cloud Storage バケットに階層化する場合は、Cloud Volumes ONTAP が配置されているサブネットをプライベート Google Access 用に設定する必要があります (HA ペアを使用している場合、これは VPC 0 のサブネットです)。手順については、を参照してください ["Google Cloud のドキュメント: 「Configuring Private Google Access」](#)。

Cloud Manager でデータの階層化を設定するための追加の手順については、を参照してください ["コールドデータを低コストのオブジェクトストレージに階層化する"](#)。

## 他のネットワーク内の ONTAP システムへの接続

GCP 内の Cloud Volumes ONTAP システムと他のネットワーク内の ONTAP システムの間でデータをレプリケートするには、VPC と他のネットワーク（たとえば社内ネットワーク）の間に VPN 接続が必要です。

手順については、を参照してください ["Google Cloud のドキュメント：「Cloud VPN Overview」](#)。

## コネクタの要件

コネクタがパブリッククラウド環境内のリソースやプロセスを管理できるように、ネットワークを設定します。最も重要なステップは、さまざまなエンドポイントへのアウトバウンドインターネットアクセスを確保することです。



ネットワークでインターネットへのすべての通信にプロキシサーバを使用している場合は、[設定] ページでプロキシサーバを指定できます。を参照してください ["プロキシサーバを使用するようにコネクタを設定します"](#)。

## ターゲットネットワークへの接続

コネクタには、Cloud Volumes ONTAP を導入する VPC へのネットワーク接続が必要です。HA ペアを導入する場合は、コネクタから VPC -0 への接続のみが必要です。

コネクタとは別のVPCにCloud Volumes ONTAP を導入する場合は、VPCネットワークピアリングを設定する必要があります。 ["VPCネットワークピアリングの詳細を確認できます"](#)

## アウトバウンドインターネットアクセス

Connector では、パブリッククラウド環境内のリソースとプロセスを管理するためにアウトバウンドインターネットアクセスが必要です。

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

## Cloud Volumes ONTAP のファイアウォールルール

Cloud Manager は、Cloud Volumes ONTAP が正常に動作するために必要なインバウンドとアウトバウンドのルールを含む GCP ファイアウォールルールを作成します。テスト目的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、ポートを参照してください。

Cloud Volumes ONTAP のファイアウォールルールには、インバウンドとアウトバウンドの両方のルールが必要です。

HA 構成を導入する場合は、VPC 0 の Cloud Volumes ONTAP のファイアウォールルールを以下に示します。

## インバウンドルール

HAペアの場合、事前定義されたファイアウォールポリシーのインバウンドトラフィックのソースフィルタは0.0.0.0/0です。

シングルノードシステムの場合は、導入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を選択できます。

- 選択した**VPC**のみ：インバウンドトラフィックのソースフィルタは、Cloud Volumes ONTAP システムのVPCのサブネット範囲、およびコネクタが存在するVPCのサブネット範囲です。これが推奨されるオプションです。
- \*すべてのVPC\*：インバウンドトラフィックのソースフィルタは0.0.0.0/0の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 と通信する必要のあるすべてのネットワークを追加し、内部のGoogleロードバランサが正常に機能するように両方のアドレス範囲を追加してください。これらのアドレスは 130.211.0.0/22 および 35.191.0.0/16 です。詳細については、を参照してください ["Google Cloud ドキュメント：ロードバランサ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 | すべて         | インスタンスの ping を実行します   |
| HTTP      | 80          | クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTP アクセス  |
| HTTPS     | 443         | クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTPS アクセス |
| SSH       | 22          | クラスタ管理 LIF またはノード管理 LIF の IP アドレスへの SSH アクセス                    |
| TCP       | 111         | NFS のリモートプロシージャコール  |
| TCP       | 139         | CIFS の NetBIOS サービスセッション  |
| TCP       | 161-162     | 簡易ネットワーク管理プロトコル   |
| TCP       | 445         | NetBIOS フレーム同期を使用した Microsoft SMB over TCP                      |
| TCP       | 635         | NFS マウント  |
| TCP       | 749         | Kerberos  |
| TCP       | 2049        | NFS サーバデーモン   |
| TCP       | 3260        | iSCSI データ LIF を介した iSCSI アクセス                                   |
| TCP       | 4045        | NFS ロックデーモン   |
| TCP       | 4046        | NFS のネットワークステータスマニタ   |
| TCP       | 10000       | NDMP を使用したバックアップ  |
| TCP       | 11104       | SnapMirror のクラスタ間通信セッションの管理                                     |
| TCP       | 11105       | クラスタ間 LIF を使用した SnapMirror データ転送                                |
| TCP       | 63001-63050 | プローブポートをロードバランシングして、どのノードが正常であるかを判断します（ HA ペアの場合のみ必要）           |

| プロトコル | ポート     | 目的                  |
|-------|---------|---------------------|
| UDP   | 111     | NFS のリモートプロシージャコール  |
| UDP   | 161-162 | 簡易ネットワーク管理プロトコル     |
| UDP   | 635     | NFS マウント            |
| UDP   | 2049    | NFS サーバデーモン         |
| UDP   | 4045    | NFS ロックデーモン         |
| UDP   | 4046    | NFS のネットワークステータスマニタ |
| UDP   | 4049    | NFS rquotad プロトコル   |

## アウトバウンドルール

Cloud Volumes 用の事前定義済みセキュリティグループ ONTAP は、すべての発信トラフィックをオープンします。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

### 基本的なアウトバウンドルール

Cloud Volumes ONTAP 用の定義済みセキュリティグループには、次のアウトバウンドルールが含まれています。

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

### 高度なアウトバウンドルール

発信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、Cloud Volumes ONTAP による発信通信に必要なポートのみを開くことができます。



source は、Cloud Volumes ONTAP システムのインターフェイス（IP アドレス）です。

| サービス             | プロトコル       | ポート | ソース                        | 宛先                     | 目的  |
|------------------|-------------|-----|----------------------------|------------------------|---|
| Active Directory | TCP         | 88  | ノード管理 LIF                  | Active Directory フォレスト | Kerberos V 認証                                   |
|                  | UDP         | 137 | ノード管理 LIF                  | Active Directory フォレスト | NetBIOS ネームサービス                                 |
|                  | UDP         | 138 | ノード管理 LIF                  | Active Directory フォレスト | NetBIOS データグラムサービス                              |
|                  | TCP         | 139 | ノード管理 LIF                  | Active Directory フォレスト | NetBIOS サービスセッション                               |
|                  | TCP および UDP | 389 | ノード管理 LIF                  | Active Directory フォレスト | LDAP  |
|                  | TCP         | 445 | ノード管理 LIF                  | Active Directory フォレスト | NetBIOS フレーム同期を使用した Microsoft SMB over TCP      |
|                  | TCP         | 464 | ノード管理 LIF                  | Active Directory フォレスト | Kerberos V パスワードの変更と設定 ( SET_CHANGE )           |
|                  | UDP         | 464 | ノード管理 LIF                  | Active Directory フォレスト | Kerberos キー管理                                   |
|                  | TCP         | 749 | ノード管理 LIF                  | Active Directory フォレスト | Kerberos V Change & Set Password ( RPCSEC_GSS ) |
|                  | TCP         | 88  | データ LIF ( NFS、CIFS、iSCSI ) | Active Directory フォレスト | Kerberos V 認証                                   |
|                  | UDP         | 137 | データ LIF ( NFS、CIFS )       | Active Directory フォレスト | NetBIOS ネームサービス                                 |
|                  | UDP         | 138 | データ LIF ( NFS、CIFS )       | Active Directory フォレスト | NetBIOS データグラムサービス                              |
|                  | TCP         | 139 | データ LIF ( NFS、CIFS )       | Active Directory フォレスト | NetBIOS サービスセッション                               |
|                  | TCP および UDP | 389 | データ LIF ( NFS、CIFS )       | Active Directory フォレスト | LDAP  |
|                  | TCP         | 445 | データ LIF ( NFS、CIFS )       | Active Directory フォレスト | NetBIOS フレーム同期を使用した Microsoft SMB over TCP      |
|                  | TCP         | 464 | データ LIF ( NFS、CIFS )       | Active Directory フォレスト | Kerberos V パスワードの変更と設定 ( SET_CHANGE )           |
|                  | UDP         | 464 | データ LIF ( NFS、CIFS )       | Active Directory フォレスト | Kerberos キー管理                                   |
|                  | TCP         | 749 | データ LIF ( NFS、CIFS )       | Active Directory フォレスト | Kerberos V Change & Set Password ( RPCSEC_GSS ) |



| サービス        | プロトコル      | ポート           | ソース                          | 宛先                 | 目的   |
|-------------|------------|---------------|------------------------------|--------------------|--|
| AutoSupport | HTTPS      | 443           | ノード管理 LIF                    | support.netapp.com | AutoSupport（デフォルトは HTTPS）                      |
|             | HTTP       | 80            | ノード管理 LIF                    | support.netapp.com | AutoSupport（転送プロトコルが HTTPS から HTTP に変更された場合のみ） |
| クラスタ        | すべてのトラフィック | すべてのトラフィック    | 1つのノード上のすべての LIF             | もう一方のノードのすべての LIF  | クラスタ間通信（Cloud Volumes ONTAP HA のみ）             |
| DHCP        | UDP        | 68            | ノード管理 LIF                    | DHCP               | 初回セットアップ用の DHCP クライアント                         |
| DHCP        | UDP        | 67            | ノード管理 LIF                    | DHCP               | DHCP サーバ                                       |
| DNS         | UDP        | 53            | ノード管理 LIF とデータ LIF（NFS、CIFS） | DNS                | DNS  |
| NDMP        | TCP        | 18600 ~ 18699 | ノード管理 LIF                    | 宛先サーバ              | NDMP コピー                                       |
| SMTP        | TCP        | 25            | ノード管理 LIF                    | メールサーバ             | SMTP アラート。AutoSupport に使用できます                  |
| SNMP        | TCP        | 161           | ノード管理 LIF                    | サーバを監視します          | SNMP トラップによる監視                                 |
|             | UDP        | 161           | ノード管理 LIF                    | サーバを監視します          | SNMP トラップによる監視                                 |
|             | TCP        | 162           | ノード管理 LIF                    | サーバを監視します          | SNMP トラップによる監視                                 |
|             | UDP        | 162           | ノード管理 LIF                    | サーバを監視します          | SNMP トラップによる監視                                 |
| SnapMirror  | TCP        | 11104         | クラスタ間 LIF                    | ONTAP クラスタ間 LIF    | SnapMirror のクラスタ間通信セッションの管理                    |
|             | TCP        | 11105         | クラスタ間 LIF                    | ONTAP クラスタ間 LIF    | SnapMirror によるデータ転送                            |
| syslog      | UDP        | 514           | ノード管理 LIF                    | syslog サーバ         | syslog 転送メッセージ                                 |

## VPC -1、VPC -2、および VPC -3 のファイアウォールルール

GCP では、4 つの VPC 間で HA 構成が導入されます。VPC -0 の HA 構成に必要なファイアウォールルールはです [Cloud Volumes ONTAP については上記のリストを参照してください](#)。

一方、Cloud Manager で VPC -1、VPC -2、および VPC -3 のインスタンスに対して作成される事前定義されたファイアウォールルールによって、\_All\_protocols とポートを介した入力通信が有効になります。これらのルールに従って、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。



## コネクタのファイアウォールルール

コネクタのファイアウォールルールには、インバウンドとアウトバウンドの両方のルールが必要です。

### インバウンドルール

| プロトコル | ポート | 目的   |
|-------|-----|--|
| SSH   | 22  | コネクタホストへの SSH アクセスを提供します                             |
| HTTP  | 80  | クライアント Web ブラウザからローカルへの HTTP アクセスを提供します ユーザインターフェイス  |
| HTTPS | 443 | クライアント Web ブラウザからローカルへの HTTPS アクセスを提供します ユーザインターフェイス |

### アウトバウンドルール

コネクタの定義済みファイアウォールルールによって、すべてのアウトバウンドトラフィックが開かれます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

#### 基本的なアウトバウンドルール

コネクタの定義済みファイアウォールルールには、次のアウトバウンドルールが含まれています。

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

#### 高度なアウトバウンドルール

発信トラフィックに固定ルールが必要な場合は、次の情報を使用して、コネクタによる発信通信に必要なポートだけを開くことができます。



送信元 IP アドレスは、コネクタホストです。

| サービス                 | プロトコル | ポート | 宛先                                 | 目的   |
|----------------------|-------|-----|------------------------------------|--|
| API コールと AutoSupport | HTTPS | 443 | アウトバウンドインターネットおよび ONTAP クラスタ管理 LIF | API が GCP と ONTAP にコールし、クラウドデータを検知してランサムウェア対策サービスに送信し、AutoSupport メッセージをネットアップに送信します |

| サービス | プロトコル | ポート | 宛先  | 目的                              |
|------|-------|-----|-----|---------------------------------|
| DNS  | UDP   | 53  | DNS | Cloud Manager による DNS 解決に使用されます |

## GCP での VPC サービスコントロールの計画

VPC Service Controls を使用して Google Cloud 環境をロックダウンすることを選択する際には、Cloud Manager と Cloud Volumes ONTAP が Google Cloud API とどのように連携するか、また Cloud Manager と Cloud Volumes ONTAP を導入するためのサービス境界を設定する方法について理解しておく必要があります。

vPC サービスコントロールを使用すると、信頼できる境界外の Google 管理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 の詳細をご覧ください](#)"。

### ネットアップサービスと VPC サービスコントロールの通信方法

Cloud Central や Cloud Manager などのネットアップサービスは、Google Cloud API と直接通信します。これは、Google Cloud 以外の外部 IP アドレス（`api.services.cloud.netapp.com` など）または Cloud Manager Connector に割り当てられた内部アドレスから Google Cloud 内でトリガーされます。

コネクタの配置スタイルによっては、サービスの境界に対して特定の例外を設定する必要があります。

### イメージ

Cloud Volumes ONTAP と Cloud Manager はどちらも、ネットアップが管理する GCP 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ある場合、Cloud Manager Connector および Cloud Volumes ONTAP の導入に影響することがあります。

手動インストールでもコネクタを手動で導入できますが、Cloud Volumes ONTAP プロジェクトからイメージを取得する必要があります。Connector と Cloud Volumes ONTAP を導入するには、許可されたリストを指定する必要があります。

### コネクタの配置

コネクタを導入するユーザーは、`projectId_NetApp-cloudmanager_and the project Number_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

- Cloud Manager サービスアカウントは、サービスプロジェクトから `projectId_NetApp-cloudmanager_and the project number_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、`projectId_NetApp-cloudmanager_and the project number_14190056516_` サービスプロジェクトから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 サービスコントロール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次に示します。

## vPC サービスは境界ポリシーを制御します

ポリシーでは、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、を参照してください ["GCP VPC Service Controls Policy Documentation を参照してください"](#)。

Cloud Manager で必要なポリシーを設定するには、組織内の VPC Service Controls Perimeter に移動し、次のポリシーを追加します。各フィールドは、VPC の [Service Controls Policy] 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 \* ルールが必要であり、\* または \* パラメーターをルールセットで使用する必要があります。

### 入力規則

```
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
```

## 出力ルール

```
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、コネクタと Cloud Volumes ONTAP のイメージを格納するために  
ネットアップが使用する project\_name cloudmanager\_used です。

## データ階層化とバックアップ用のサービスアカウントを作成します

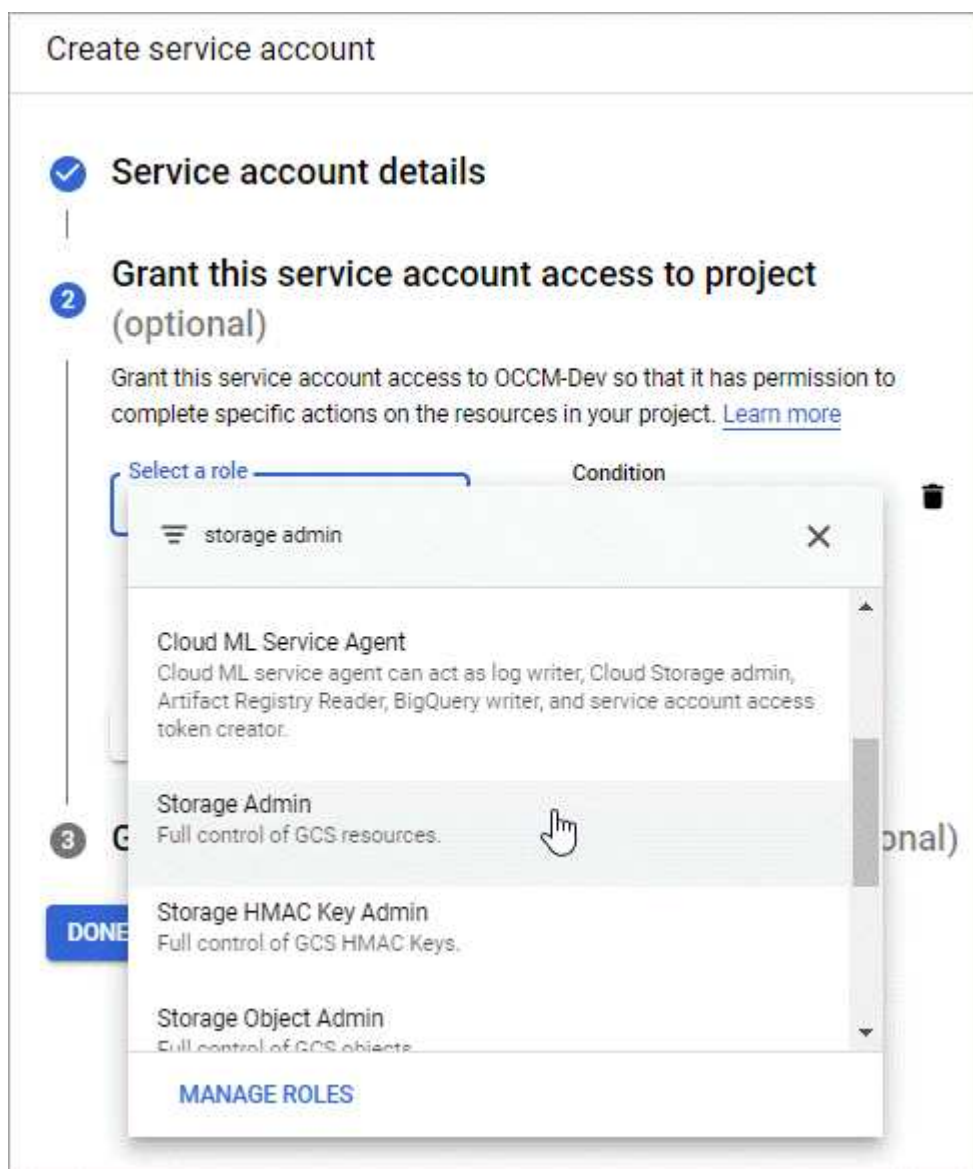
Cloud Volumes ONTAP には、2 つの目的で Google Cloud サービスアカウントが必要です。1 つ目は、を有効にする場合です ["データの階層化"](#) Google Cloud でコールドデータを低コストのオブジェクトストレージに階層化すること。2 つ目は、を有効にした場合です ["Cloud Backup サービスの略"](#) ボリュームを低コストのオブジェクトストレージにバックアップできます。

Cloud Volumes ONTAP では、このサービスアカウントを使用して、階層化データ用のバケットとバックアップ用のバケットにアクセスして管理します。

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 コンソールで、 "[ 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ます。
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を許可 \* : \* ストレージ管理者 \* の役割を選択します。



- c. \* このサービスアカウントへのアクセス権をユーザーに付与 \*: Connector サービスアカウントを A\_Service アカウント User\_ 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にのみ必要です。Cloud Backup Service では必要ありません。

Create service account

✓ Service account details

✓ Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role

netapp-cloud-manager@iam.gserviceaccount.com

?

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role

?

Grant users the permission to administer this service account

DONE

CANCEL

サービスアカウントは、Cloud Volumes ONTAP 作業環境の作成後に選択する必要があります。

Details and Credentials

default-project

Google Cloud Project

gcp-sub2

Marketplace Subscription

Edit Project

Details

Working Environment Name (Cluster Name)

cloudvolumesontap

Service Account ⓘ

Service Account Name

account1

+ Add Labels

Optional Field | Up to four labels

Credentials

User Name

admin

Password

Confirm Password

ページのスクリーンショット。"]

## お客様が管理する暗号化キーを **Cloud Volumes ONTAP** で使用する

Google Cloud Storage では常にデータが暗号化されてからディスクに書き込まれますが、Cloud Manager API を使用して、`_cuser-managed` 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. キーが格納されているプロジェクトのプロジェクトレベルで、Cloud Manager Connector サービスアカウントの権限が正しいことを確認します。

権限はから提供されます "[Cloud Manager YAML ファイル](#)" デフォルトでは、Cloud Key Management Service に別のプロジェクトを使用する場合は適用できません。

権限は次のとおりです。

```
- cloudkms.cryptoKeyVersions.list
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

2. のサービスアカウントを確認します ["Google Compute Engine Service Agent"](#) キーに対する Cloud KMS の暗号化 / 復号化権限があることを確認します。

サービスアカウントの名前は、「service-[[SERVICE\\_PROJECT\\_NUMBER](#)\_[@compute-system.iam.gserviceaccount.com](#) ]」という形式で指定します。

["Google Cloud のドキュメント：「Using IAM with Cloud KMS - Granting roles on a resource"](#)

3. 「/GCP/VSA/meta/META/GCP-encryption-keys」API 呼び出しの get コマンドを呼び出すか、GCP コンソールのキーで「Copy Resource Name」を選択して、キーの「id」を取得します。
4. お客様が管理する暗号化キーを使用してオブジェクトストレージにデータを階層化する場合、Cloud Manager は永続ディスクの暗号化に使用されるキーと同じキーを使用します。キーを使用するには、まず Google Cloud Storage バケットを有効にする必要があります。
  - a. 次の手順に従って、Google Cloud Storage サービスエージェントを検索します ["Google Cloud ドキュメント：「Getting the Cloud Storage service agent"](#)。
  - b. 暗号化キーに移動し、Cloud KMS 暗号化 / 復号化権限を持つ Google Cloud Storage サービスエージェントを割り当てます。

詳細については、を参照してください ["Google Cloud のドキュメント：「Using customer-managed encryption keys"](#)

5. 作業環境を作成するときは、API 要求で "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"  
}
```

を参照してください ["Cloud Manager 自動化に関するドキュメント"](#) "GcpEncryption" パラメータの使用方法の詳細については、を参照してください。

## Google CloudでCloud Volumes ONTAP のライセンスを設定します

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

### フリーミアム

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

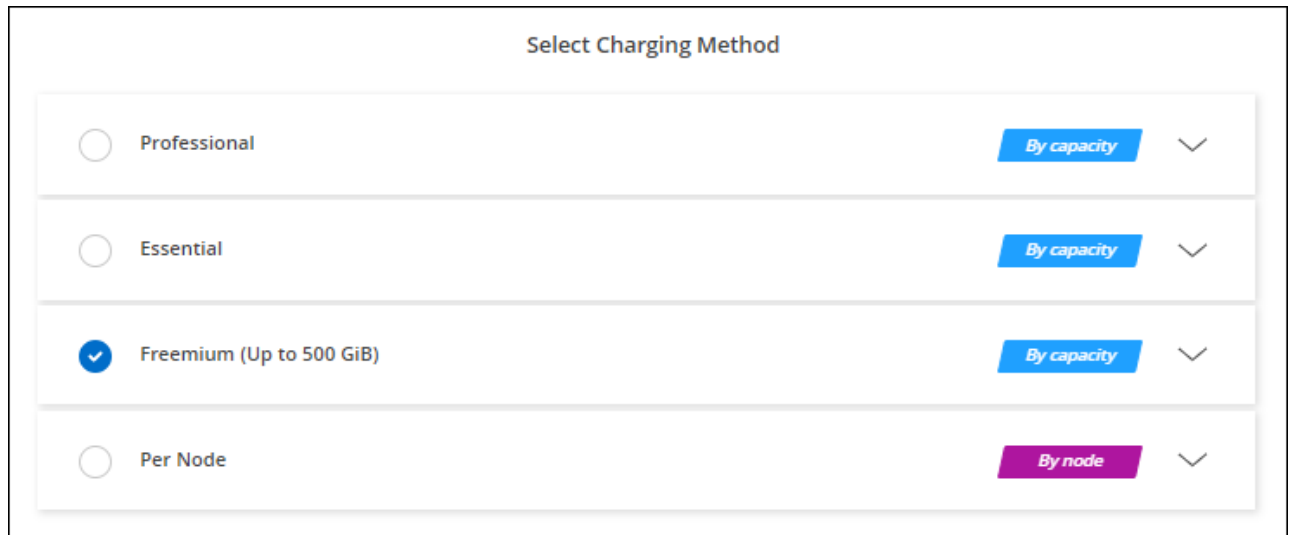
手順



1. キャンバスページで、\*作業環境の追加\*をクリックし、Cloud Managerの手順に従います。
  - a. [詳細と資格情報]ページで、[資格情報の編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってGoogle Cloud Marketplaceでの従量課金制サービスに登録します。

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

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



| Select Charging Method                                    |             |   |
|---|-------------|---|
| <input type="radio"/> Professional                        | By capacity | ▼ |
| <input type="radio"/> Essential                           | By capacity | ▼ |
| <input checked="" type="radio"/> Freemium (Up to 500 GiB) | By capacity | ▼ |
| <input type="radio"/> Per Node                            | By node     | ▼ |

["Google CloudでCloud Volumes ONTAP を起動するための詳細な手順を表示します"](#)。

## 容量単位のライセンスです

容量単位のライセンスでは、TiB 単位の Cloud Volumes ONTAP に対して料金を支払うことができます。容量ベースのライセンスは、パッケージ：Essentialsパッケージまたはプロフェッショナルパッケージの形式で提供されます。

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

- ネットアップから購入したライセンス（BYOL）
- Google Cloud Marketplaceから1時間単位の従量課金制（PAYGO）サブスクリプション
- 年間契約

["容量単位のライセンスに関する詳細は、こちらをご覧ください"](#)。

以降のセクションでは、これらの各消費モデルの使用方法について説明します。

## BYOL

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

手順

1. "ライセンスの取得については、ネットアップの営業部門にお問い合わせください"

2. "Cloud Managerにネットアップサポートサイトのアカウントを追加します"

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

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

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

a. [詳細と資格情報]ページで、[資格情報の編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってGoogle Cloud Marketplaceでの従量課金制サービスに登録します。

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

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

The screenshot shows a 'Select Charging Method' dialog box with four radio button options. The 'Professional' option is selected, indicated by a blue checkmark. To the right of each option is a button labeled 'By capacity' (for the first three) or 'By node' (for the last one), followed by a downward arrow. The buttons for 'By capacity' are blue, while the button for 'By node' is purple.

| Charging Method          | Button Label |
|--------------------------|--------------|
| Professional             | By capacity  |
| Essential                | By capacity  |
| Freemium (Up to 500 GiB) | By capacity  |
| Per Node                 | By node      |

"Google CloudでCloud Volumes ONTAP を起動するための詳細な手順を表示します"。

## PAYGOサブスクリプション

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

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

### 手順

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

a. [詳細と資格情報]ページで、[資格情報の編集]、[サブスクリプションの追加]の順にクリックし、プロン

プトに従ってGoogle Cloud Marketplaceでの従量課金制サービスに登録します。

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

The screenshot shows a 'Select Charging Method' dialog with four radio button options. The 'Professional' option is selected, indicated by a blue checkmark in its radio button. To the right of each option is a button labeled 'By capacity' (for Professional, Essential, and Freemium) or 'By node' (for Per Node), followed by a downward arrow. The 'Per Node' button is highlighted in purple.

| Charging Method                                | Button Label |
|--|--------------|
| <input checked="" type="radio"/> Professional  | By capacity  |
| <input type="radio"/> Essential                | By capacity  |
| <input type="radio"/> Freemium (Up to 500 GiB) | By capacity  |
| <input type="radio"/> Per Node                 | By node      |

"Google CloudでCloud Volumes ONTAP を起動するための詳細な手順を表示します"。



アカウントに関連付けられたGoogle Cloud Marketplaceのサブスクリプションは、[設定]>[クレデンシャル]ページで管理できます。"Google Cloudのクレデンシャルとサブスクリプションを管理する方法について説明します"

## 年間契約

年間契約を購入することで、Cloud Volumes ONTAP の年間料金をお支払いいただけます。

### 手順

1. 年間契約を購入するには、ネットアップ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\_private\_offerとして提供されます。

ネットアップがプライベートオファーを共有した後は、作業環境の作成中にGoogle Cloud Marketplaceから登録するときに、年間プランを選択できます。

2. キャンバスページで、\*作業環境の追加\*をクリックし、Cloud Managerの手順に従います。
  - a. [詳細と資格情報]ページで、[資格情報の編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってGoogle Cloud Marketplaceで年間プランを購読します。
  - b. Google Cloudで、アカウントと共有されている年間プランを選択し、[Subscribe]をクリックします。
  - c. Cloud Managerに戻ったら、課金方法のページで容量ベースのパッケージを選択します。

Select Charging Method

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

"Google CloudでCloud Volumes ONTAP を起動するための詳細な手順を表示します"。

## Keystone Flex サブスクリプション

Keystone Flexサブスクリプションは、ビジネスの成長に合わせて拡張できるサブスクリプションベースのサービスです。 "[Keystone Flex Subscriptions の詳細をご覧ください](#)"。

### 手順

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

Select Charging Method

Keystone

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1

By capacity

Professional

By capacity

Essential

By capacity

Freemium (Up to 500 GiB)

By capacity

Per Node

By node

["Google CloudでCloud Volumes ONTAP を起動するための詳細な手順を表示します"。](#)

# GCP での Cloud Volumes ONTAP の起動

Cloud Volumes ONTAP は、シングルノード構成または Google Cloud Platform の HA ペアとして起動できます。

## 始める前に

作業環境を作成するには、次の作業が必要です。

- 稼働中のコネクタ。
  - を用意しておく必要があります "ワークスペースに関連付けられているコネクタ"。
  - "コネクタをで実行したままにする準備をしておく必要があります 常時"。
  - コネクタに関連付けられているサービスアカウント "最新の権限が必要です"。
- 使用する構成についての理解。

設定を選択し、管理者から GCP ネットワーク情報を取得して準備を完了しておく必要があります。詳細については、[を参照してください "Cloud Volumes ONTAP 構成を計画"](#)。

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

"ライセンスの設定方法について説明します"。

- Google Cloud API はとすることがあります ["プロジェクトで有効にします"](#) :
  - Cloud Deployment Manager V2 API
  - クラウドロギング API
  - Cloud Resource Manager API の略
  - Compute Engine API
  - ID およびアクセス管理（IAM）API

## GCP でシングルノードシステムを起動する


Cloud Manager で作業環境を作成して、GCP で Cloud Volumes ONTAP を起動します。

### 手順

1. [\[\[subscribe\]](#) キャンバスページで、\* 作業環境の追加 \* をクリックし、プロンプトに従います。
2. \* 場所を選択 \* : 「\* Google Cloud \* 」と「\* Cloud Volumes ONTAP \* 」を選択します。
3. プロンプトが表示されたら、["コネクタを作成します"](#)。
4. 詳細と認証情報：プロジェクトを選択し、クラスタ名を指定します。必要に応じてサービスアカウントを選択し、ラベルを追加し、クレデンシャルを指定することもできます。

次の表では、ガイダンスが必要なフィールドについて説明します。

| フィールド      | 説明   |
|------------|--|
| 作業環境名      | Cloud Manager は、作業環境名を使用して、Cloud Volumes ONTAP システムと GCP VM インスタンスの両方に名前を付けます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。  |
| サービスアカウント名 | を使用する場合は <a href="#">"データの階層化"</a> または <a href="#">"クラウドバックアップ"</a> Cloud Volumes ONTAP では、* サービスアカウント * を有効にして、事前定義されたストレージ管理者ロールが割り当てられたサービスアカウントを選択する必要があります。 <a href="#">"サービスアカウントの作成方法について説明します"</a> 。   |
| ラベルを追加します  | ラベルは GCP リソースのメタデータです。Cloud Manager によって、システムに関連付けられた Cloud Volumes ONTAP システムと GCP リソースにラベルが追加されます。作業環境の作成時にユーザインターフェイスからラベルを 4 つまで追加し、その後追加することができます。API では、作業環境の作成時にラベルを 4 つに制限することはありません。ラベルの詳細については、 <a href="#">を参照してください "Google Cloud のドキュメント：「Labeling Resources"</a> 。 |
| ユーザ名とパスワード | Cloud Volumes ONTAP クラスタ管理者アカウントのクレデンシャルです。このクレデンシャルを使用して、System Manager またはその CLI から Cloud Volumes ONTAP に接続できます。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します  |

| フィールド        | 説明  |
|--------------|---|
| プロジェクトを編集します | <p>Cloud Volumes ONTAP を配置するプロジェクトを選択します。デフォルトプロジェクトは、Cloud Manager が配置されているプロジェクトです。</p> <p>ド롭ダウンリストにプロジェクトが表示されない場合は、Cloud Manager サービスアカウントを他のプロジェクトに関連付けていません。Google Cloud コンソールに移動し、IAM サービスを開き、プロジェクトを選択します。Cloud Manager ロールが割り当てられた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。</p> <div>  <p>これは Cloud Manager 用に設定するサービスアカウントです。<br/>"このページで説明されているように"。</p> </div> <p>[サブスクリプションの追加] をクリックして、選択した資格情報をサブスクリプションに関連付けます。</p> <p>従量課金制の Cloud Volumes ONTAP システムを作成するには、GCP Marketplace から Cloud Volumes ONTAP へのサブスクリプションに関連付けられている GCP プロジェクトを選択する必要があります。</p> |

次のビデオでは、従量課金制の Marketplace サブスクリプションを GCP プロジェクトに関連付ける方法を説明します。または、の手順に従って、に登録します "[Marketplace サブスクリプションと GCP クレデンシャルの関連付け](#)" セクション。

▶ [https://docs.netapp.com/ja-jp/cloud-manager-cloud-volumes-ontap//media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/ja-jp/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4)

(video)

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。クラウドバックアップまたは階層化を選択するには、手順 3 でサービスアカウントを指定しておく必要があります。
6. 場所と接続性: 場所を選択し、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、ガイダンスが必要なフィールドについて説明します。

| フィールド                | 説明  |
|----------------------|---|
| 接続の検証                | 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 が配置されてい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、を参照してください <a href="#">"Google Cloud のドキュメント: 「Configuring Private Google Access」</a> 。   |
| ファイアウォールポリシーが生成されました | Cloud Managerでファイアウォールポリシーを生成するように設定した場合は、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。 <ul style="list-style-type: none"><li>• 「* Selected VPC Only *」を選択した場合、インバウンドトラフィックのソースフィルタは、選択したVPCのサブネット範囲とコネクタが存在するVPCのサブネット範囲になります。これが推奨されるオプションです。</li><li>• どのVPC *も選択した場合、インバウンドトラフィックのソースフィルタは0.0.0.0/0のIP範囲になります。</li></ul> |
| 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。 <a href="#">"Cloud Volumes ONTAP のファイアウォールルールについて説明します"</a> 。   |

7. \* 充電方法と NSS アカウント \* : このシステムで使用する充電オプションを指定し、ネットアップサポートサイトのアカウントを指定します。
  - ["Cloud Volumes ONTAP のライセンスオプションについて説明します"](#)。
  - ["ライセンスの設定方法について説明します"](#)。
8. \* 構成済みパッケージ \* : Cloud Volumes ONTAP システムを迅速に導入するパッケージを 1 つ選択するか、\* 独自の構成を作成 \* をクリックします。

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

9. ライセンス: 必要に応じてCloud Volumes ONTAP 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で新しいリリース候補、一般的な可用性、またはパッチリリースが利用可能な場合は、作業環境の作成時に Cloud Manager によってシステムがそのバージョンに更新されます。たとえば、Cloud Volumes ONTAP 9.10.1と9.10.1 P4が利用可能になれば、更新が実行されます。たとえば、9.6 から 9.7 への更新など、あるリリースから別のリリースへの更新は行われません。

10. \* 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、つまり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。以降のボリュームでは、別のディスクタイプを選択できます。

ディスクサイズは、最初のアグリゲート内のすべてのディスクと、シンプルプロビジョニングオプションを使用したときに Cloud Manager によって作成される追加のアグリゲートに適用されます。Advanced Allocation オプションを使用すると、異なるディスクサイズを使用するアグリゲートを作成できます。

ディスクの種類とサイズの選択については、を参照してください ["GCP でシステムのサイジングを行う"](#)。

11. \* Write Speed & WORM \* : 「 \* Normal \* 」または「 \* High \* write speed 」を選択し、必要に応じて Write Once 、 Read Many （ WORM ）ストレージをアクティブにします。

書き込み速度の選択はシングルノードシステムでのみサポートされます。

["書き込み速度の詳細については、こちらをご覧ください。"](#)。

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

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

12. \* Google Cloud Platform でのデータ階層化 \* : 最初のアグリゲートでデータの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、事前に定義されたストレージ管理者ロール（ Cloud Volumes ONTAP 9.7 以降で必要）を持つサービスアカウントを選択します。または GCP アカウントを選択します（ Cloud Volumes ONTAP 9.6 では必須）。

次の点に注意してください。

- Cloud Manager 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提供します。Connector サービスアカウントは、階層化サービスアカウントのユーザとして追加してください。追加していないと、 Cloud Manager から選択できません。
- GCP アカウントの追加については、を参照してください ["でのデータ階層化のための GCP アカウントの設定と追加 9.6."](#)。
- ボリュームを作成または編集するときに、特定のボリューム階層化ポリシーを選択できます。
- データの階層化を無効にした場合は、後続のアグリゲートで有効にできますが、システムをオフにして GCP コンソール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については、こちらをご覧ください。"](#)。

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

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

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

| フィールド | 説明   |
|-------|--|
| サイズ   | 入力できる最大サイズは、シンプル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。シンプルプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。 |

| フィールド                     | 説明   |
|---------------------------|--|
| アクセス制御（NFS のみ）            | エクスポートポリシーは、ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、Cloud Manager はサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。   |
| 権限とユーザー / グループ（CIFS のみ）   | これらのフィールドを使用すると、ユーザおよびグループ（アクセスコントロールリストまたはACL と呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、domain\username 形式でユーザのドメインを指定する必要があります。  |
| スナップショットポリシー              | Snapshot コピーポリシーは、自動的に作成される NetApp Snapshot コピーの頻度と数を指定します。NetApp Snapshot コピーは、パフォーマンスに影響を与えず、ストレージを最小限に抑えるポイントインタイムファイルシステムイメージです。デフォルトポリシーを選択することも、なしを選択することもできます。一時データには、Microsoft SQL Server の tempdb など、none を選択することもできます。   |
| アドバンスドオプション（NFS のみ）       | ボリュームの NFS バージョンを NFSv3 または NFSv4 のいずれかで選択してください。  |
| イニシエータグループと IQN（iSCSI のみ） | iSCSI ストレージターゲットは LUN（論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。イニシエータグループは、iSCSI ホストのノード名のテーブルであり、どのイニシエータがどの LUN にアクセスできるかを制御します。iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（NIC）、ソフトウェアイニシエータを搭載した TOE カード、CNA、または専用の HBA を使用してネットワークに接続され、iSCSI Qualified Name（IQN）で識別されます。iSCSI ボリュームを作成すると、Cloud Manager によって自動的に LUN が作成されます。ボリュームごとに 1 つの LUN だけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、 <b>"IQN を使用して、から LUN に接続します ホスト"</b> 。 |

次の図は、CIFS プロトコルの [Volume] ページの設定を示しています。

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy:

*Default Policy*

#### Protocol

NFS **CIFS** iSCSI

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

14. \* CIFS セットアップ\* : CIFS プロトコルを選択した場合は、CIFS サーバをセットアップします。

| フィールド                      | 説明   |
|----------------------------|--|
| DNS プライマリおよびセカンダリ IP アドレス  | CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスレコード（SRV）が含まれている必要があります。Google Managed Active Directory を設定している場合は、デフォルトで 169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.x.x の 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 サーバに参加させる Active Directory （AD）ドメインの FQDN。  |
| ドメインへの参加を許可されたクレデンシャル      | AD ドメイン内の指定した組織単位（OU）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。   |
| CIFS サーバの NetBIOS 名        | AD ドメイン内で一意の CIFS サーバ名。  |
| 組織単位                       | CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。Google Managed Microsoft AD を Cloud Volumes ONTAP の AD サーバとして設定するには、このフィールドに「* OU=computers、OU=Cloud」と入力します。 <a href="https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units">https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units</a> ["Google Cloud ドキュメント：「Organizational Units in Google Managed Microsoft AD」"] |
| DNS ドメイン                   | Cloud Volumes ONTAP Storage Virtual Machine （SVM）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。  |
| NTP サーバ                    | Active Directory DNS を使用して NTP サーバを設定するには、「Active Directory ドメインを使用」を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、API を使用してください。を参照してください <a href="#">"Cloud Manager 自動化に関するドキュメント"</a> を参照してください。NTP サーバは、CIFS サーバを作成するときのみ設定できます。CIFS サーバを作成したあとで設定することはできません。   |

15. \* 使用状況プロファイル、ディスクタイプ、階層化ポリシー \*：Storage Efficiency 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変更します。

詳細については、を参照してください ["ボリューム使用率プロファイルについて"](#) および ["データ階層化の概要"](#)。

16. \* レビューと承認 \*: 選択内容を確認して確認します。
- 設定の詳細を確認します。
  - [ 詳細情報 \*（More information \*） ] をクリックして、Cloud Manager が購入するサポートと GCP リソースの詳細を確認します。
  - [ \* I understand ... \*（理解しています ... \*） ] チェックボックスを選択
  - [ Go\* ] をクリックします。

Cloud Manager は Cloud Volumes ONTAP システムを導入します。タイムラインで進行状況を追跡できます。

Cloud Volumes ONTAP システムの導入で問題が発生した場合は、障害メッセージを確認してください。作業

環境を選択し、\* 環境の再作成 \* をクリックすることもできます。

詳細については、を参照してください ["NetApp Cloud Volumes ONTAP のサポート"](#)。

完了後

- CIFS 共有をプロビジョニングした場合は、ファイルとフォルダに対する権限をユーザまたはグループに付与し、それらのユーザが共有にアクセスしてファイルを作成できることを確認します。
- ボリュームにクォータを適用する場合は、System Manager または CLI を使用します。

クォータを使用すると、ユーザ、グループ、または qtree が使用するディスク・スペースとファイル数を制限または追跡できます。

## GCP で HA ペアを起動する

Cloud Manager で作業環境を作成して、GCP で Cloud Volumes ONTAP を起動します。

手順

1. Canvas ページで、\* Add Working Environment \* をクリックし、画面の指示に従います。
2. \* 場所を選択 \* : 「\* Google Cloud \*」と「\* Cloud Volumes ONTAP HA \*」を選択します。
3. \* 詳細と認証情報 \* : プロジェクトを選択し、クラスタ名を指定します。必要に応じてサービスアカウントを選択し、ラベルを追加し、クレデンシャルを指定することもできます。

次の表では、ガイダンスが必要なフィールドについて説明します。

| フィールド      | 説明  |
|------------|---|
| 作業環境名      | Cloud Manager は、作業環境名を使用して、Cloud Volumes ONTAP システムと GCP VM インスタンスの両方に名前を付けます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。   |
| サービスアカウント名 | を使用する場合は <a href="#">"階層化"</a> または <a href="#">"クラウドバックアップ"</a> サービスを利用するには、* Service Account * スイッチを有効にし、事前定義された Storage Admin ロールが割り当てられたサービスアカウントを選択する必要があります。   |
| ラベルを追加します  | ラベルは GCP リソースのメタデータです。Cloud Manager によって、システムに関連付けられた Cloud Volumes ONTAP システムと GCP リソースにラベルが追加されます。作業環境の作成時にユーザインターフェイスからラベルを 4 つまで追加し、その後追加することができます。API では、作業環境の作成時にラベルを 4 つに制限することはありません。ラベルの詳細については、 <a href="#">を参照してください "Google Cloud のドキュメント：「Labeling Resources"。</a> |
| ユーザ名とパスワード | Cloud Volumes ONTAP クラスタ管理者アカウントのクレデンシャルです。このクレデンシャルを使用して、System Manager またはその CLI から Cloud Volumes ONTAP に接続できます。default_admin_user の名前をそのまま使用するか 'カスタム・ユーザー名' に変更します  |

| フィールド        | 説明  |
|--------------|---|
| プロジェクトを編集します | <p>Cloud Volumes ONTAP を配置するプロジェクトを選択します。デフォルトプロジェクトは、Cloud Manager が配置されているプロジェクトです。</p> <p>ド롭ダウンリストにプロジェクトが表示されない場合は、Cloud Manager サービスアカウントを他のプロジェクトに関連付けていません。Google Cloud コンソールに移動し、IAM サービスを開き、プロジェクトを選択します。Cloud Manager ロールが割り当てられた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。</p> <div>  <p>これは Cloud Manager 用に設定するサービスアカウントです。<br/>"このページで説明されているように"。</p> </div> <p>[サブスクリプションの追加] をクリックして、選択した資格情報をサブスクリプションに関連付けます。</p> <p>従量課金制の Cloud Volumes ONTAP システムを作成するには、GCP Marketplace から Cloud Volumes ONTAP へのサブスクリプションに関連付けられている GCP プロジェクトを選択する必要があります。</p> |

次のビデオでは、従量課金制の Marketplace サブスクリプションを GCP プロジェクトに関連付ける方法を説明します。または、の手順に従って、に登録します "[Marketplace サブスクリプションと GCP クレデンシャルの関連付け](#)" セクション。

▶ [https://docs.netapp.com/ja-jp/cloud-manager-cloud-volumes-ontap//media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/ja-jp/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4)

(video)

4. \* 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。クラウドバックアップまたは階層化を選択するには、手順 3 でサービスアカウントを指定しておく必要があります。
5. \* HA 配置モデル \* : HA 構成用に複数のゾーン (推奨) または単一ゾーンを選択します。次に、リージョンとゾーンを選択します。

["HA 導入モデルの詳細については、こちらをご覧ください"](#)。

6. \* 接続 \* : HA 構成の場合は 4 つの VPC、各 VPC 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については、こちらをご覧ください"](#)。

7. \* 充電方法と NSS アカウント \* : このシステムで使用する充電オプションを指定し、ネットアップサポートサイトのアカウントを指定します。

◦ ["Cloud Volumes ONTAP のライセンスオプションについて説明します"](#)。

◦ ["ライセンスの設定方法について説明します"](#)。

8. \* 構成済みパッケージ \* : Cloud Volumes ONTAP システムを迅速に導入するパッケージを 1 つ選択するか、\* 独自の構成を作成 \* をクリックします。

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

9. ライセンス : 必要に応じて Cloud Volumes ONTAP 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で新しいリリース候補、一般的な可用性、またはパッチリリースが利用可能な場合は、作業環境の作成時に Cloud Manager によってシステムがそのバージョンに更新されます。たとえば、Cloud Volumes ONTAP 9.10.1 と 9.10.1 P4 が利用可能になっていれば、更新が実行されます。たとえば、9.6 から 9.7 への更新など、あるリリースから別のリリースへの更新は行われません。

10. \* 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、つまり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。以降のボリュームでは、別のディスクタイプを選択できます。

ディスクサイズは、最初のアグリゲート内のすべてのディスクと、シンプルプロビジョニングオプションを使用したときに Cloud Manager によって作成される追加のアグリゲートに適用されます。Advanced Allocation オプションを使用すると、異なるディスクサイズを使用するアグリゲートを作成できます。

ディスクの種類とサイズの選択については、を参照してください ["GCP でシステムのサイジングを行う"](#)。

11. \* WORM \* : 必要に応じて、Write Once Read Many (WORM) ストレージをアクティブにします。

データの階層化が有効になっていると、WORM を有効にできません。 ["WORM ストレージの詳細については、こちらをご覧ください"](#)。

12. \* Google Cloud Platform でのデータ階層化 \* : 最初のアグリゲートでデータの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 Storage Admin 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。

- Cloud Manager 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提供します。Connector サービスアカウントは、階層化サービスアカウントのユーザとして追加してください。追加していないと、Cloud Manager 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。
- データの階層化を無効にした場合は、後続のアグリゲートで有効にできますが、システムをオフにして GCP コンソール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については、こちらをご覧ください。"](#)

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

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

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

| フィールド                   | 説明   |
|-------------------------|--|
| サイズ                     | 入力できる最大サイズは、シンプロビジョニングを有効にするかどうかによって大きく異なります。シンプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。   |
| アクセス制御（NFS のみ）          | エクスポートポリシーは、ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、Cloud Manager はサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。   |
| 権限とユーザー / グループ（CIFS のみ） | これらのフィールドを使用すると、ユーザおよびグループ（アクセスコントロールリストまたは ACL と呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、domain\username 形式でユーザのドメインを指定する必要があります。                             |
| スナップショットポリシー            | Snapshot コピーポリシーは、自動的に作成される NetApp Snapshot コピーの頻度と数を指定します。NetApp Snapshot コピーは、パフォーマンスに影響を与えず、ストレージを最小限に抑えるポイントインタイムファイルシステムイメージです。デフォルトポリシーを選択することも、なしを選択することもできます。一時データには、Microsoft SQL Server の tempdb など、none を選択することもできます。 |
| アドバンスドオプション（NFS のみ）     | ボリュームの NFS バージョンを NFSv3 または NFSv4 のいずれかで選択してください。  |

| フィールド                     | 説明  |
|---------------------------|---|
| イニシエータグループと IQN（iSCSI のみ） | iSCSI ストレージターゲットは LUN（論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。イニシエータグループは、iSCSI ホストのノード名のテーブルであり、どのイニシエータがどの LUN にアクセスできるかを制御します。iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（NIC）、ソフトウェアイニシエータを搭載した TOE カード、CNA、または専用の HBA を使用してネットワークに接続され、iSCSI Qualified Name（IQN）で識別されます。iSCSI ボリュームを作成すると、Cloud Manager によって自動的に LUN が作成されます。ボリュームごとに 1 つの LUN だけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、 <a href="#">"IQN を使用して、から LUN に接続します ホスト"</a> 。 |

次の図は、CIFS プロトコルの [Volume] ページの設定を示しています。

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:

Size (GB): i

Snapshot Policy:  

default v

  
i Default Policy

#### Protocol

NFS
CIFS
iSCSI

Share name:

Permissions:  

Full Control v

Users / Groups:  
  
Valid users and groups separated by a semicolon

14. \* CIFS セットアップ\*：CIFS プロトコルを選択した場合は、CIFS サーバをセットアップします。

| フィールド                      | 説明  |
|----------------------------|---|
| DNS プライマリおよびセカンダリ IP アドレス  | CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスロケーションレコード（SRV）が含まれている必要があります。Google Managed Active Directory を設定している場合は、デフォルトで 169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.x.x の 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 サーバに参加させる Active Directory（AD）ドメインの FQDN。  |
| ドメインへの参加を許可されたクレデンシャル      | AD ドメイン内の指定した組織単位（OU）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。  |
| CIFS サーバの NetBIOS 名        | AD ドメイン内で一意の CIFS サーバ名。   |



| フィールド    | 説明   |
|----------|--|
| 組織単位     | CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。Google Managed Microsoft AD を Cloud Volumes ONTAP の AD サーバとして設定するには、このフィールドに「* OU=computers、OU=Cloud」と入力します。 <a href="https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units">https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units</a> ["Google Cloud ドキュメント：「Organizational Units in Google Managed Microsoft AD」"] |
| DNS ドメイン | Cloud Volumes ONTAP Storage Virtual Machine（SVM）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。   |
| NTP サーバ  | Active Directory DNS を使用して NTP サーバを設定するには、「Active Directory ドメインを使用」を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、API を使用してください。を参照してください <a href="#">"Cloud Manager 自動化に関するドキュメント"</a> を参照してください。NTP サーバは、CIFS サーバを作成するときのみ設定できます。CIFS サーバを作成したあとで設定することはできません。   |

15. \* 使用状況プロファイル、ディスクタイプ、階層化ポリシー \*：Storage Efficiency 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変更します。

詳細については、を参照してください ["ボリューム使用率プロファイルについて"](#) および ["データ階層化の概要"](#)。

16. \* レビューと承認 \*：選択内容を確認して確認します。
- 設定の詳細を確認します。
  - [ 詳細情報 \*（More information\*） ] をクリックして、Cloud Manager が購入するサポートと GCP リソースの詳細を確認します。
  - [ \* I understand ... \*（理解しています ... \*） ] チェックボックスを選択
  - [ Go\* ] をクリックします。

Cloud Manager は Cloud Volumes ONTAP システムを導入します。タイムラインで進行状況を追跡できます。

Cloud Volumes ONTAP システムの導入で問題が発生した場合は、障害メッセージを確認してください。作業環境を選択し、\* 環境の再作成 \* をクリックすることもできます。

詳細については、を参照してください ["NetApp Cloud Volumes ONTAP のサポート"](#)。

完了後

- CIFS 共有をプロビジョニングした場合は、ファイルとフォルダに対する権限をユーザまたはグループに付与し、それらのユーザが共有にアクセスしてファイルを作成できることを確認します。
- ボリュームにクォータを適用する場合は、System Manager または CLI を使用します。

クォータを使用すると、ユーザ、グループ、または qtree が使用するディスク・スペースとファイル数を制限または追跡できます。

## 著作権情報

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

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、いかなる場合でも、間接的、偶発的、特別、懲罰的、またはまたは結果的損害（代替品または代替サービスの調達、使用の損失、データ、利益、またはこれらに限定されないものを含みますが、これらに限定されません。）ただし、契約、厳格責任、または本ソフトウェアの使用に起因する不法行為（過失やその他を含む）のいずれであっても、かかる損害の可能性について知らされていた場合でも、責任の理論に基づいて発生します。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、またはその他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1 つ以上の米国特許、その他の国の特許、および出願中の特許により特許、その他の国の特許、および出願中の特許。

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

## 商標情報

NetApp、NetAppのロゴ、に記載されているマーク <http://www.netapp.com/TM> は、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。