Google Cloud で始めましょう

Cloud Volumes ONTAP

NetApp
May 28, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/bluexp-cloud-volumes-ontap/task-getting-started-gcp.html on May 28, 2024. Always check docs.netapp.com for the latest.

目次

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

1 コネクタを作成します

を持っていなければ "コネクタ" ただし、アカウント管理者がアカウントを作成する必要があります。 "Google Cloud でコネクタを作成する方法について説明します"

インターネットアクセスを使用できないサブネットにCloud Volumes ONTAP を導入する場合は、コネクタを手動でインストールし、そのコネクタで実行されているBlueXPユーザインターフェイスにアクセスする必要があります。 "インターネットにアクセスできない場所にコネクタを手動でインストールする方法について説明します"

2 構成を計画

BlueXPでは、ワークロード要件に合わせて事前設定されたパッケージを提供しています。また、独自の構成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"。

3 ネットワークをセットアップします

1. VPC とサブネットがコネクタと Cloud Volumes ONTAP 間の接続をサポートしていることを確認します。
2. 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のインターネットアクセスをNetApp AutoSupport で有効にします。

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

"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"。

4 サービスアカウントを設定します

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 "BlueXPのバックアップとリカバリ" 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"。

5 **Google Cloud API** を有効にします

"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

6 **BlueXP**を使用して**Cloud Volumes ONTAP** を起動します

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

関連リンク

- "BlueXPからコネクタを作成しています"
- "Linux ホストへの Connector ソフトウェアのインストール"
- "BlueXPがGoogle Cloud権限で実行する機能"

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 の Cloud Volumes ONTAP でのストレージの制限"

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。システムの容量をBlueXPで管理できるようになりますが、自分でアグリゲートを作成する場合は、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、BlueXP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	
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

BlueXPを使用すると、Google Cloudのハイアベイラビリティ（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、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。BlueXP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。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。

Google CloudでのCloud Volumes ONTAP 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ネットワークをセットアップします。

HA ペアを導入する場合は、を実行します "Google CloudでのHAペアの仕組みをご確認ください"。

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。

シングルノードシステムに固有の要件

シングル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

シングルノードシステムにはVirtual Private Cloud（VPC；仮想プライベートクラウド）が1つ必要です。

プライベート IP アドレス

BlueXPは、Google Cloudのシングルノードシステムに3つまたは4つのプライベートIPアドレスを割り当てます。

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ペアに固有の要件

HAペアを導入する場合は、ネットワークが次の要件を満たしていることを確認します。

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ペアを作成すると、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 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。

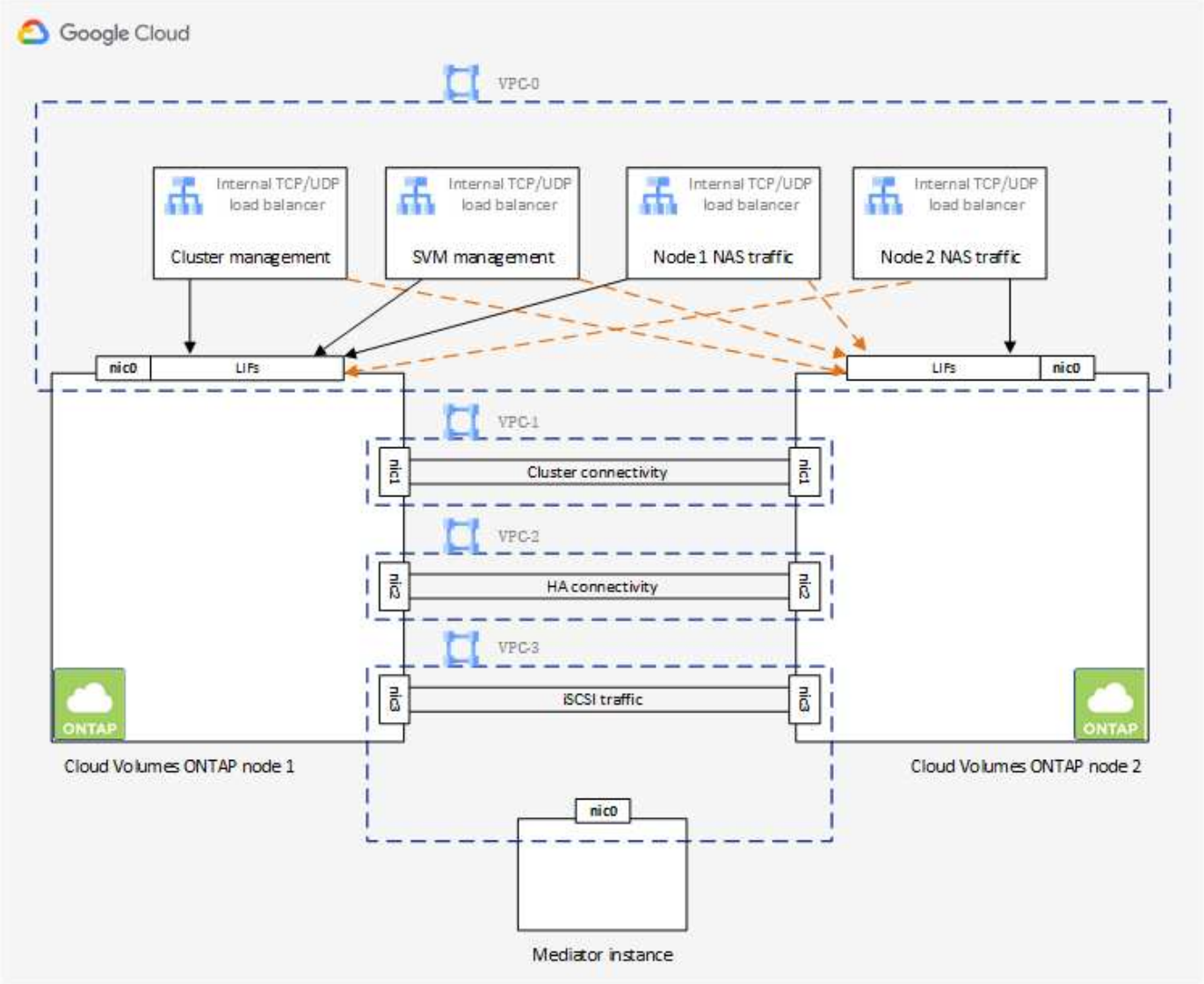
  この導入モデルでは、ゾーン間にデータ出力料金が発生しないため、コストが削減されます。

4つの仮想プライベートクラウド

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。Google Cloudでは各ネットワークインターフェイスを別 々 のVPCネットワークに配置する必要があるため、VPCは4つ必要です。

HAペアを作成するときに、4つのVPCを選択するように要求されます。

- 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



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。

プライベート **IP** アドレス

BlueXPは、必要な数のプライベートIPアドレスをGoogle Cloudの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アドレスがあることを確認する必要があります。

Cloud Volumes ONTAP 用に割り当てられるLIFの数は、シングルノードシステムとHAペアのどちらを導入するかによって異なります。LIF は、物理ポートに関連付けられた IP アドレスです。SnapCenter などの管理ツールには、 SVM 管理 LIF が必要です。

- シングルノード BlueXPでは、1つのノードシステムに4つのIPアドレスが割り当てられます。

- 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、システムがその他の重要なネットワークワークフローに使用します。これらのLIFは必須であり、削除しないでください。

- NAS LIF

  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

- * HAペア* BlueXPは、12~13個のIPアドレスをHAペアに割り当てます。
  - ノード管理LIF×2（e0a）
  - クラスタ管理LIF（e0a）×1
  - iSCSI LIF×2（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、システムがその他の重要なネットワークワークフローに使用します。これらのLIFは必須であり、削除しないでください。

  - NAS LIF（e0a）×1または2
  - クラスタLIF×2（e0b）
  - HAインターコネクトIPアドレス×2（e0c）
  - RSM iSCSI IPアドレス×2（e0d）

    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

内部ロードバランサ

BlueXPでは、Cloud Volumes ONTAP HAペアへの着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）が自動的に4つ作成されます。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されるポートは 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。

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サブネット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。

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 へのアウトバウンドのインターネットアクセスが必要です。ネットアップは、システムの健常性をプロアクティブに監視し、ネットアップテクニカルサポートにメッセージを送信します。

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 メッセージの送信にアウトバウンドのインターネット接続が使用できない場合、Cloud Volumes ONTAP システムは自動的にコネクタをプロキシサーバとして使用するように設定されます。唯一の要件は、コネクタのファイアウォールがポート3128上の_INBOUND接続を許可することです。コネクタを展開した後、このポートを開く必要があります。

Cloud Volumes ONTAP に厳密なアウトバウンドルールを定義した場合は、Cloud Volumes ONTAP ファイアウォールがポート3128で_OUTBOUND接続を許可することも必要です。

アウトバウンドのインターネットアクセスが使用可能であることを確認したら、 AutoSupport をテストしてメッセージを送信できることを確認します。手順については、を参照してください "ONTAP のドキュメント：「 AutoSupport のセットアップ"。

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。

AutoSupport メッセージを送信できないことがBlueXPから通知された場合は、 "AutoSupport 構成のトラブルシューティングを行います"。

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。BlueXPはファイアウォールルールを作成します。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。。

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"。

BlueXPでデータの階層化を設定するために必要な追加手順については'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

Google Cloud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"。

ファイアウォールルール

BlueXP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Google Cloudファイアウォールルールを作成します。テスト目的や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。

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。
- 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。。

コネクタに関する情報をお探しですか？ "コネクタのファイアウォールルールを表示します"

インバウンドルール

作業環境を作成する場合、展開時に定義済み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	コネクタへの接続と、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

プロトコル	ポート	目的
TCP	3260	iSCSI データ LIF を介した iSCSI アクセス
TCP	4045	NFS ロックデーモン
TCP	4046	NFS のネットワークステータスモニタ
TCP	10000	NDMP を使用したバックアップ
TCP	11104	SnapMirror のクラスタ間通信セッションの管理
TCP	11105	クラスタ間 LIF を使用した SnapMirror データ転送
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）
UDP	111	NFS のリモートプロシージャコール
UDP	161-162	簡易ネットワーク管理プロトコル
UDP	635	NFS マウント
UDP	2049	NFS サーバデーモン
UDP	4045	NFS ロックデーモン
UDP	4046	NFS のネットワークステータスモニタ
UDP	4049	NFS rquotad プロトコル

アウトバウンドルール

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

基本的なアウトバウンドルール

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

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

高度なアウトバウンドルール

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

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

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

サービス	プロトコル	ポート	ソース	宛先	目的
AutoSupport	HTTPS	443	ノード管理 LIF	support.netapp.com	AutoSupport （デフォルトは HTTPS ）
	HTTP	80	ノード管理 LIF	support.netapp.com	AutoSupport （転送プロトコルが HTTPS から HTTP に変更された場合のみ）
	TCP	3128	ノード管理 LIF	コネクタ	アウトバウンドのインターネット接続が使用できない場合に、コネクタのプロキシサーバを介してAutoSupport メッセージを送信する
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）
構成のバックアップ	HTTP	80	ノード管理 LIF	http://<connector-IP-address>/occm/offboxconfig	構成バックアップをコネクタに送信します。 "構成バックアップファイルについて説明します"。
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のルール

Google Cloudでは、4つのVPC間に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、BlueXP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定義済みのファイアウォールルールにより、_All_protocolsとポートでの入力通信が可能になります。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。

> Google Cloudの新しいHAペア環境で高速な書き込み速度を有効にするには、VPC-1、VPC-2、およびVPC-3のMaximum Transmission Unit（MTU；最大伝送ユニット）が8、896バイト以上必要です。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。

コネクタの要件

コネクタをまだ作成していない場合は、コネクタのネットワーク要件も確認してください。

- "コネクタのネットワーク要件を確認します"
- "Google Cloudのファイアウォールルール"

GCP での VPC サービスコントロールの計画

Google Cloud環境をVPC Service Controlsでロックダウンする場合は、BlueXPとCloud Volumes ONTAP がGoogle Cloud APIとどのように連携するか、またBlueXPとCloud Volumes ONTAP を展開するためのサービス境界を構成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

BlueXPは、Google Cloud APIと直接通信します。これは、Google Cloudの外部の外部IPアドレス（たとえば、api.services.cloud.netapp.comから）、またはBlueXPコネクタ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BlueXP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。組織内でホスティングされていない画像の使用をブロックするポリシーがある場合、これはBlueXP ConnectorおよびCloud Volumes ONTAP の展開に影響を与える可能性があります。

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

- BlueXPサービスアカウントは、projectId_NetApp-cloudmanager_and the project number_14190056516_ でホストされているイメージをサービスプロジェクトから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"。

BlueXP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

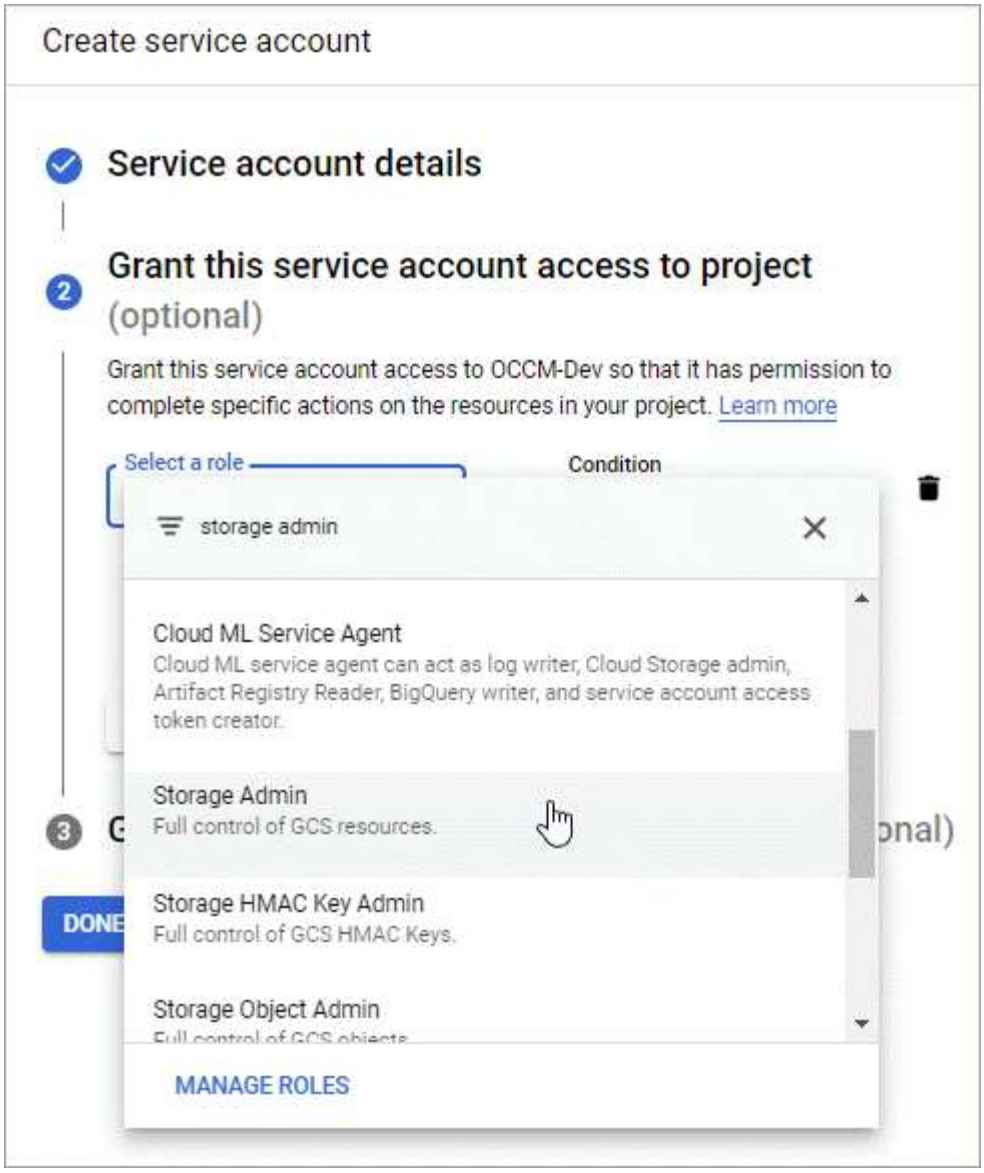
Cloud Volumes ONTAP には、 2 つの目的で Google Cloud サービスアカウントが必要です。1 つ目は、を有効にする場合です "データの階層化" Google Cloud でコールドデータを低コストのオブジェクトストレージに階層化すること。2 つ目は、を有効にした場合です "BlueXPのバックアップとリカバリ" ボリュームを低コストのオブジェクトストレージにバックアップできます。

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。

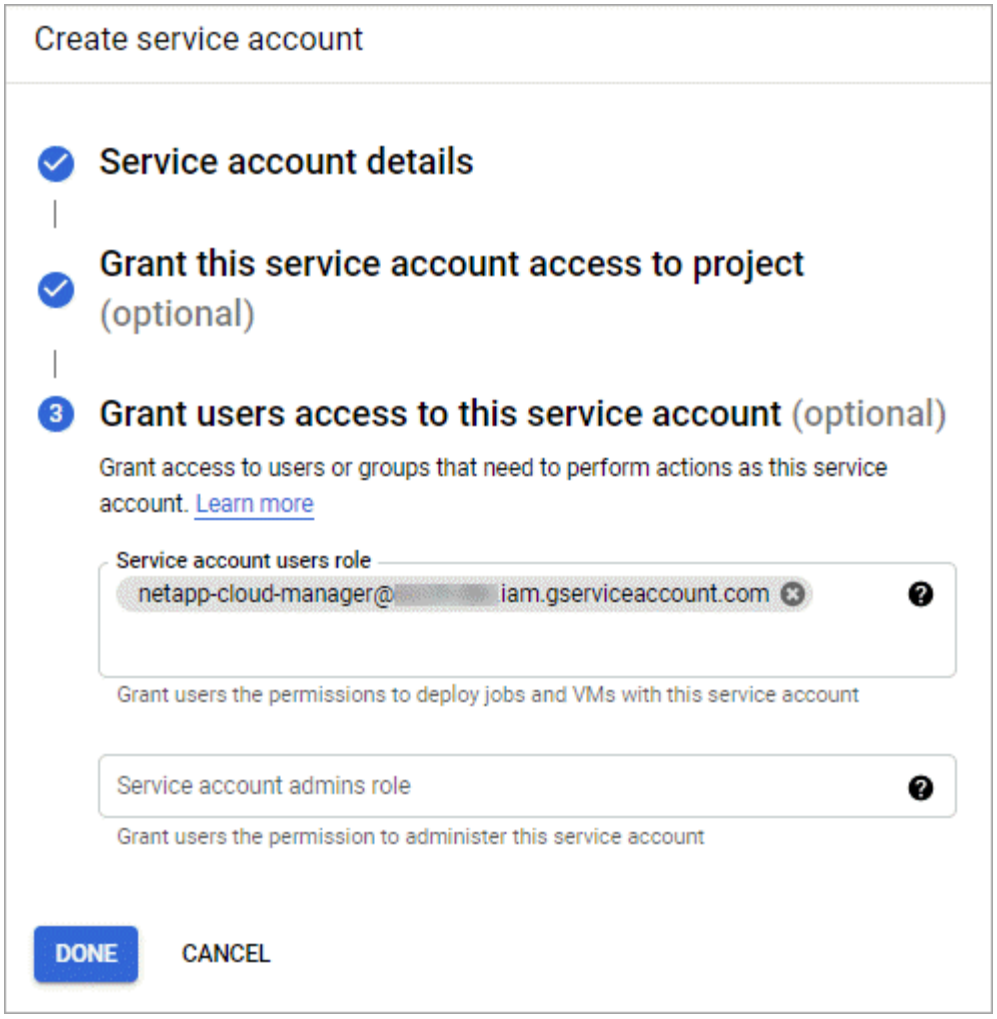
手順

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。



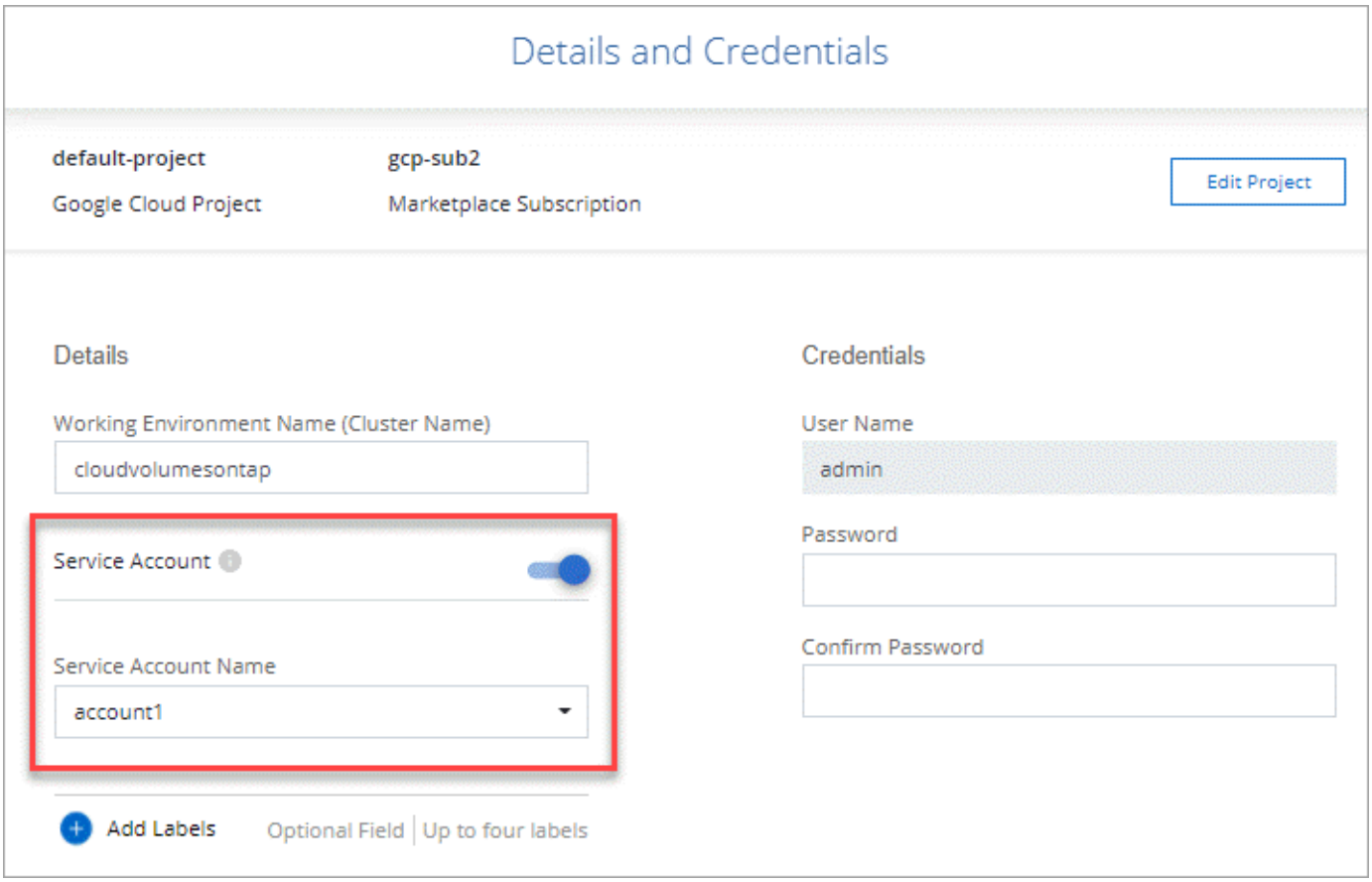
c. * このサービスアカウントへのアクセス権をユーザーに付与 *: Connector サービスアカウントを A_Service アカウント User_ としてこの新しいサービスアカウントに追加します。

この手順はデータ階層化にのみ必要です。BlueXPのバックアップとリカバリには必要ありません。



次の手順

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。



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、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、BlueXP APIを使用して、_お客様が管理する暗号化キー_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で、BlueXP Connectorサービスアカウントがプロジェクトレベルで正しいアクセス許可を持っていることを確認します。

   権限は、で提供されています "デフォルトでは、Connectorサービスアカウントの権限です"、ただし、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.useToEncrypt
- 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、データをオブジェクトストレージに階層化する場合、BlueXPは、永続ディスクの暗号化に使用されるのと同じキーを使用しようとします。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 "BlueXP自動化ドキュメント" "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

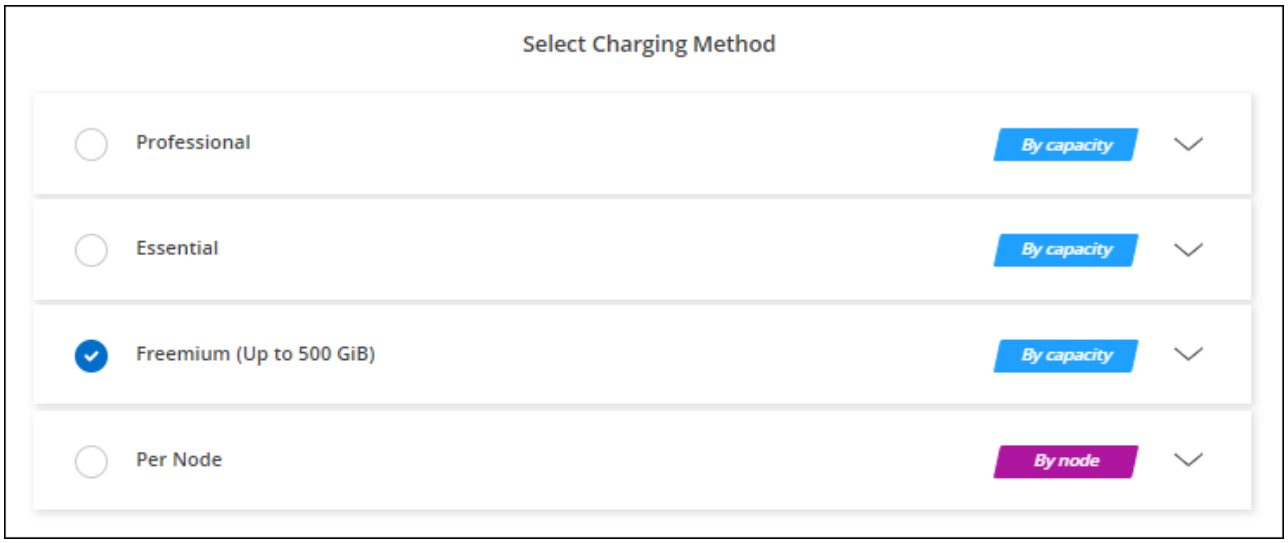
プロビジョニングされた容量が最大500GiBのCloud Volumes ONTAP を無料で使用するには、Freemium製品を選択してください。 "Freemium 製品の詳細をご覧ください"。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、*Add Working Environment*をクリックし、BlueXP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、システムはに自動的に変換されないかぎり、マーケットプレイスのサブスクリプションを通じて料金が請求されることはありません "Essentials パッケージ"。

   b. BlueXPに戻ったら、充電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. "NetApp Support Site アカウントをBlueXPに追加します"

   BlueXP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、NetApp Support Site 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、BlueXPは自動的にライセンスをデジタルウォレットに追加します。

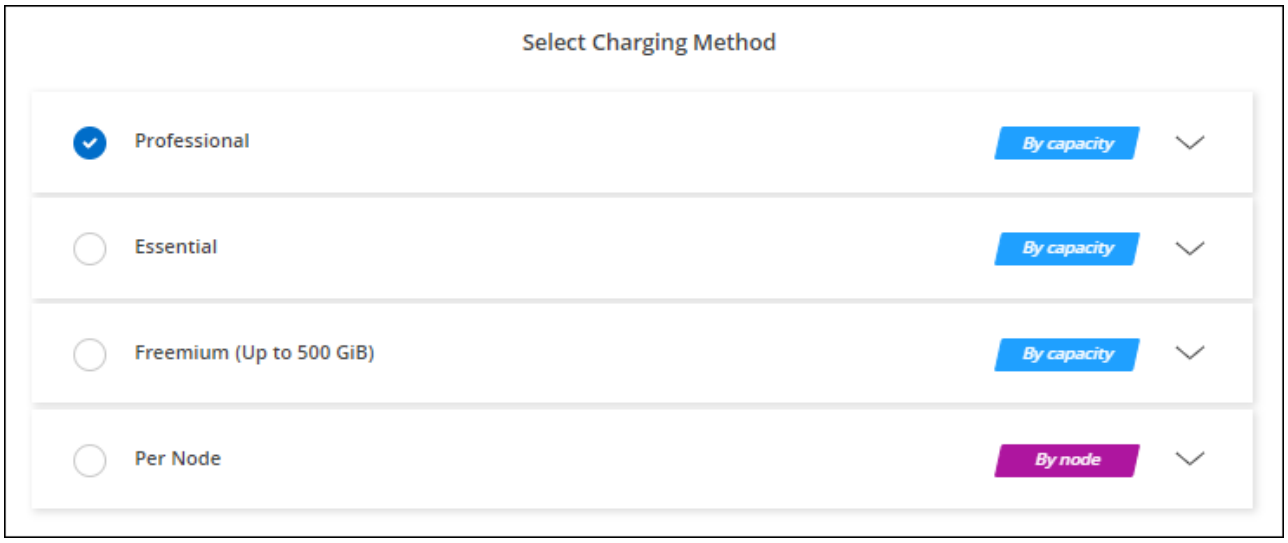
   Cloud Volumes ONTAP でライセンスを使用するには、事前にBlueXPデジタルウォレットからライセンスを入手しておく必要があります。必要に応じて、を実行できます "ライセンスをBlueXPデジタルウォレットに手動で追加します"。

3. キャンバスページで、*Add Working Environment*をクリックし、BlueXP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. BlueXP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

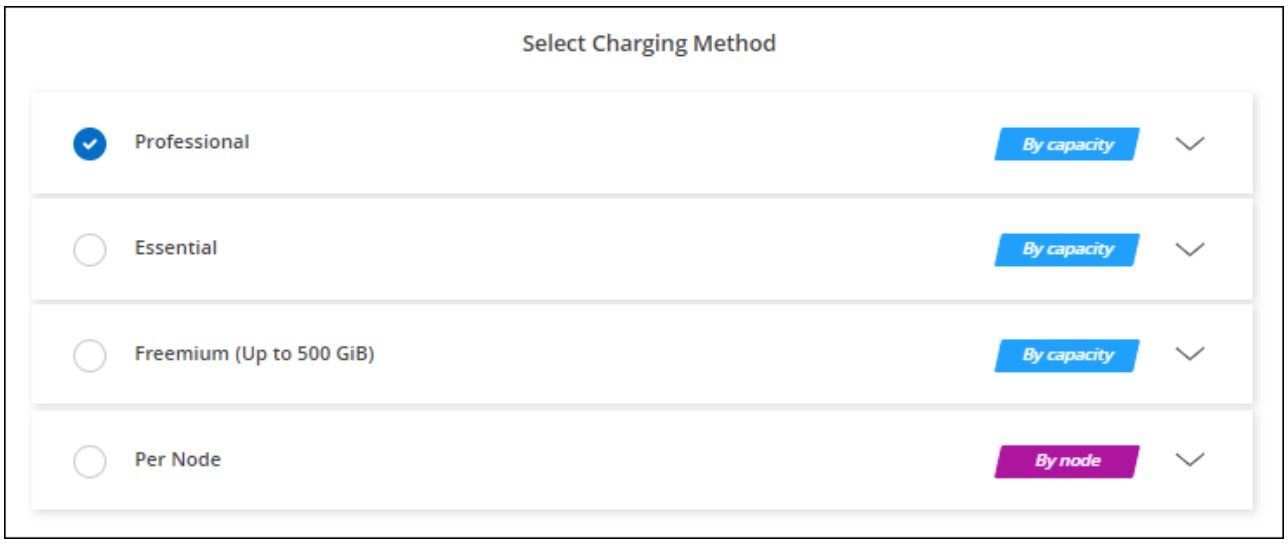
クラウドプロバイダのマーケットプレイスから提供されたサービスに登録すると、1時間ごとに料金が発生します。

Cloud Volumes ONTAP 作業環境を作成すると、Google Cloud Marketplaceで提供されている契約を購読するように求めるメッセージが表示されます。このサブスクリプションは、充電のための作業環境に関連付けられます。同じサブスクリプションを追加の作業環境に使用できます。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。

2. キャンバスページで、*Add Working Environment*をクリックし、BlueXP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. BlueXP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。

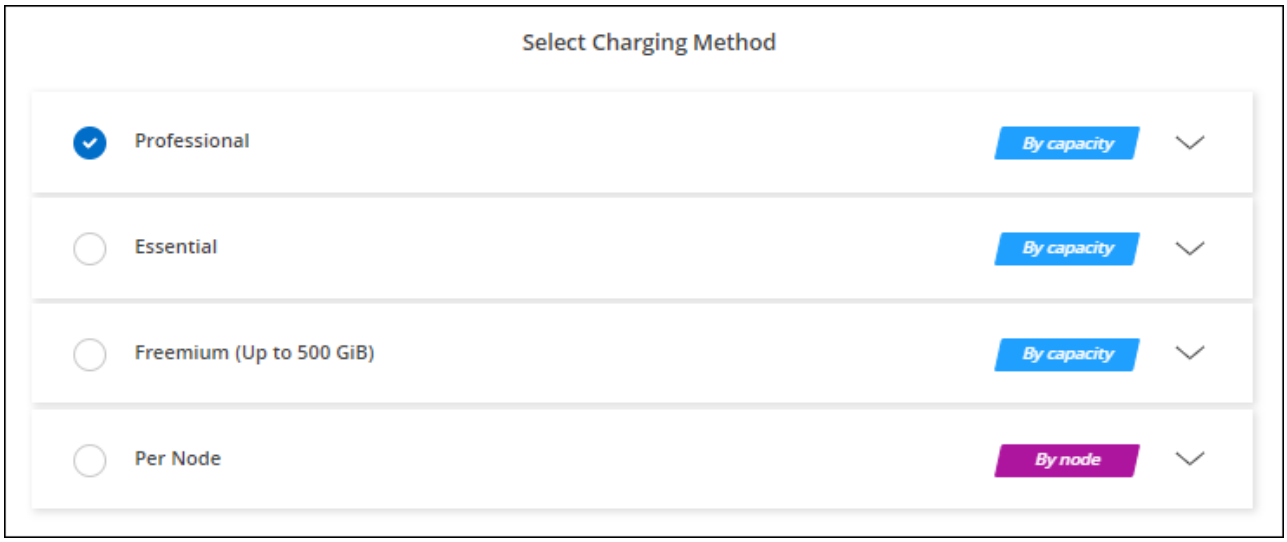
手順

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、*Add Working Environment*をクリックし、BlueXP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. BlueXP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。



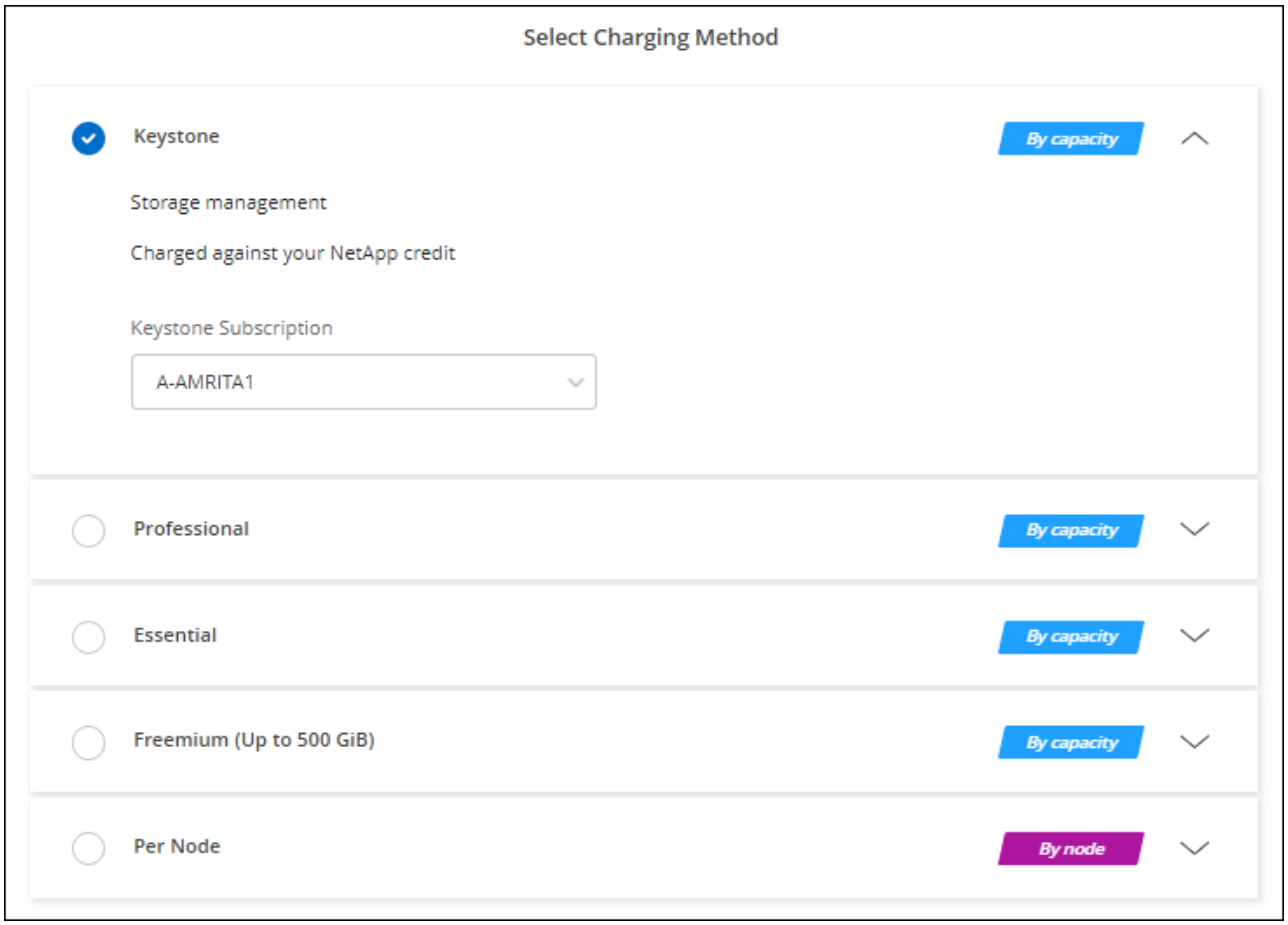
"Google CloudでCloud Volumes ONTAP を起動するための詳細な手順を表示します"。

Keystoneサブスクリプション

Keystoneサブスクリプションは、ビジネスの成長に応じた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については、こちらをご覧ください"。

手順

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



オプションのスクリーンショット。"]

"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"。

Google Cloud で Cloud Volumes ONTAP を起動しています

Cloud Volumes ONTAP は、シングルノード構成またはGoogle Cloud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 "必要な権限がある必要があります"
- 使用する構成についての理解。

  構成を選択し、管理者からGoogle Cloudネットワーク情報を入手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 はとする必要があります "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

Google Cloudでのシングルノードシステムの起動

BlueXPで作業環境を作成し、Cloud Volumes ONTAP をGoogle Cloudで起動します。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. [[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。
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、 "コネクタを作成します"。
5. 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	BlueXPは、作業環境名を使用して、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。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 "データの階層化" または "BlueXPのバックアップとリカバリ" 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。 "サービスアカウントの作成方法について説明します"。
ラベルを追加します	ラベルは、Google Cloudリソースのメタデータです。BlueXPは、システムに関連付けられているCloud Volumes ONTAP システムとGoogle Cloudリソースにラベルを追加します。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、を参照してください "Google Cloud のドキュメント：「 Labeling Resources"。
ユーザ名とパスワード	Cloud Volumes ONTAP クラスタ管理者アカウントのクレデンシャルです。このクレデンシャルを使用して、 System Manager またはその CLI から Cloud Volumes ONTAP に接続できます。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します

フィールド	説明
プロジェクトを編集します	Cloud Volumes ONTAP を配置するプロジェクトを選択します。既定のプロジェクトは、BlueXPが存在するプロジェクトです。 ドロップダウンリストに他のプロジェクトが表示されない場合は、まだBlueXP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。BlueXP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、BlueXP用に設定したサービスアカウントです。 "このページで説明されているように"。 [サブスクリプションの追加] をクリックして、選択した資格情報をサブスクリプションに関連付けます。 従量課金制のCloud Volumes ONTAP システムを作成するには、Google Cloud 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Google Cloudプロジェクトを選択する必要があります。

次のビデオでは、従量課金制のMarketplaceサブスクリプションをGoogle Cloudプロジェクトに関連付ける方法を紹介します。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Google Cloudクレデンシャルの関連付け" セクション。

Google Cloud MarketplaceからBlueXPにサブスクライブ

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。BlueXPのバックアップとリカバリを選択するか、BlueXPの階層化を使用するには、ステップ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。

   WORMとデータ階層化を活用する場合は、BlueXPの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 作業環境を導入する必要があります。

7. 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 "Google Cloud のドキュメント：「 Configuring Private Google Access"。

フィールド	説明
ファイアウォールポリシーが生成されました	BlueXPがファイアウォールポリシーを生成するようにした場合は、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。 • 「* 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。 • 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。
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。リンク：https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/reference-networking-gcp.html#firewall-rules[Learn Cloud Volumes ONTAPのファイアウォールルールについて^]。

8. * 充電方法と NSS アカウント * ：このシステムで使用する充電オプションを指定し、ネットアップサポートサイトのアカウントを指定します。
   - "Cloud Volumes ONTAP のライセンスオプションについて説明します"。
   - "ライセンスの設定方法について説明します"。
9. * 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。
10. 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、一般提供、またはパッチリリースが利用可能な場合、作業環境の作成時に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。
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、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。

    シンプルなプロビジョニングオプションを使用した場合、ディスクサイズは、初期アグリゲートのすべてのディスクと、BlueXPで作成される追加のアグリゲートのサイズです。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 "Google Cloudでシステムをサイジングする"。
12. * Flash Cache、書き込み速度、WORM * ：
    a. 必要に応じて、「Flash Cache」*を有効にします。

Cloud Volumes ONTAP 9.13.1以降では、n2-standard-16、n2-standard-32、n2-standard-48、およびn2-standard-64インスタンスタイプで_Flash Cache_が サポートされます。導入後にFlash Cacheを無効にすることはできません。

b. 必要に応じて、「標準」または「高速」の書き込み速度を選択します。

"書き込み速度の詳細については、こちらをご覧ください。"。

「* High * write speed」オプションを使用すると、高速な書き込み速度と最大伝送ユニット（MTU）8、896バイトを使用できます。また、MTUが8、896の場合は、導入環境でVPC-1、VPC-2、およびVPC-3を選択する必要があります。VPC-1、VPC-2、およびVPC-3の詳細については、を参照してください "VPC -1、VPC -2、およびVPC -3のルール"。

c. 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。

Cloud Volumes ONTAP 9.7以前のバージョンで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。Cloud Volumes ONTAP 9.8へのリバートまたはダウングレードは、WORMと階層化を有効にしたあとはブロックされます。

"WORM ストレージの詳細については、こちらをご覧ください。"。

a. WORMストレージをアクティブ化する場合は、保持期間を選択します。

13. * Google Cloud Platformでのデータ階層化*：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、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。

- Cloud Volumes ONTAP インスタンスで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を階層化サービスアカウントのユーザーとして追加してください。追加しないと、BlueXPから選択できません
- Google Cloudアカウントの追加については、を参照してください "9.6でのデータ階層化用にGoogle Cloudアカウントを設定および追加します"。
- 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。
- データの階層化を無効にすると、以降のアグリゲートで有効にすることができますが、システムの電源をオフにして、Google Cloud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。"。

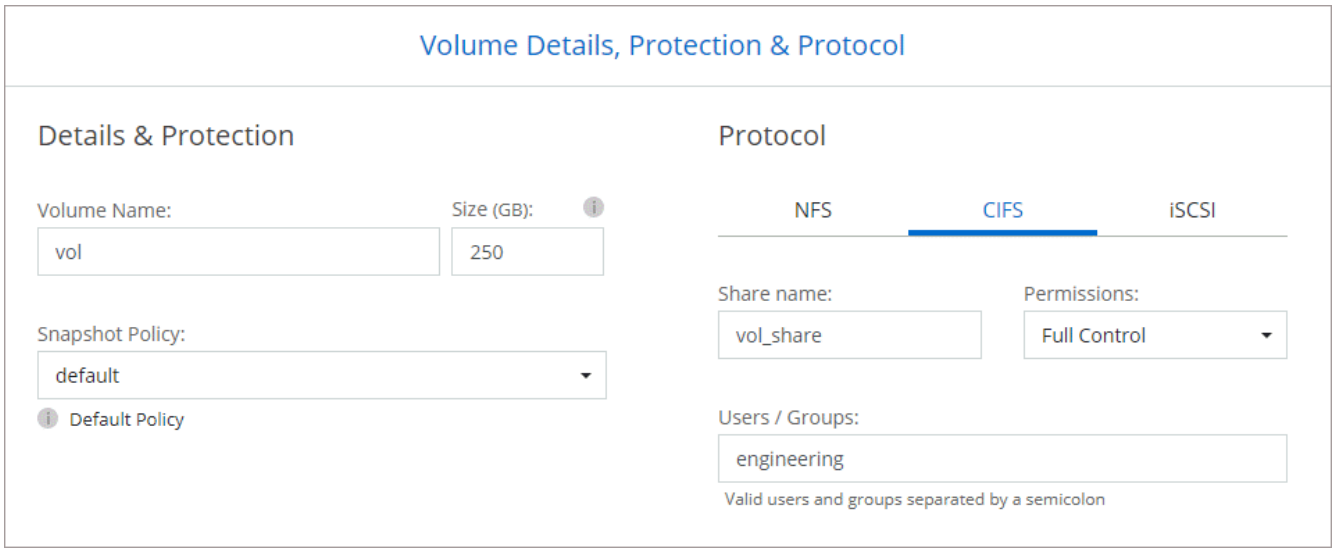
14. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

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

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



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 169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.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 サーバを参加させる Active Directory （ AD ）ドメインの FQDN 。
ドメインへの参加を許可されたクレデンシャル	AD ドメイン内の指定した組織単位（ OU ）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。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。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["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 "BlueXP自動化ドキュメント" を参照してください。 NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

16. * 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 "ボリュームの使用プロファイルを選択してください" および "データ階層化の概要"。

17. * レビューと承認 *: 選択内容を確認して確認します。
    a. 設定の詳細を確認します。
    b. サポートの詳細とBlueXPが購入するGoogle Cloudのリソースを確認するには、[詳細情報*]をクリックします。
    c. [* I understand … * （理解しています … * ）] チェックボックスを選択
    d. [Go*] をクリックします。

結果

BlueXPがCloud Volumes ONTAP システムを導入しました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。

Google CloudでのHAペアの起動

BlueXPで作業環境を作成し、Cloud Volumes ONTAP をGoogle Cloudで起動します。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. Canvas ページで、 * Add Working Environment * をクリックし、画面の指示に従います。
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	BlueXPは、作業環境名を使用して、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。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 "BlueXPの階層化" または "BlueXPのバックアップとリカバリ" 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、Google Cloudリソースのメタデータです。BlueXPは、システムに関連付けられているCloud Volumes ONTAP システムとGoogle Cloudリソースにラベルを追加します。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、を参照してください "Google Cloud のドキュメント：「 Labeling Resources"。

フィールド	説明
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
プロジェクトを編集します	Cloud Volumes ONTAP を配置するプロジェクトを選択します。既定のプロジェクトは、BlueXPが存在するプロジェクトです。 ドロップダウンリストに他のプロジェクトが表示されない場合は、まだBlueXP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。BlueXP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、BlueXP用に設定したサービスアカウントです。 "このページで説明されているように"。 [サブスクリプションの追加] をクリックして、選択した資格情報をサブスクリプションに関連付けます。 従量課金制のCloud Volumes ONTAP システムを作成するには、Google Cloud 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Google Cloudプロジェクトを選択する必要があります。

次のビデオでは、従量課金制のMarketplaceサブスクリプションをGoogle Cloudプロジェクトに関連付ける方法を紹介します。 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の関連付け" セクション。

Google Cloud MarketplaceからBlueXPにサブスクライブ

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。BlueXPのバックアップとリカバリを選択するか、BlueXP階層化を使用するには、ステップ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。

   WORMとデータ階層化を活用する場合は、BlueXPの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 作業環境を導入する必要があります。

6. *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"。

7. * 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"。

   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
ポリシーが生成されました	BlueXPがファイアウォールポリシーを生成するようにした場合は、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。 • 「* 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。 • 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。
既存のを使用します	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説明します"。

8. * 充電方法と NSS アカウント * ：このシステムで使用する充電オプションを指定し、ネットアップサポートサイトのアカウントを指定します。
   - "Cloud Volumes ONTAP のライセンスオプションについて説明します"。
   - "ライセンスの設定方法について説明します"。
9. * 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。
10. 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、一般提供、またはパッチリリースが利用可能な場合、作業環境の作成時に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。
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、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。

    シンプルなプロビジョニングオプションを使用した場合、ディスクサイズは、初期アグリゲートのすべてのディスクと、BlueXPで作成される追加のアグリゲートのサイズです。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 "Google Cloudでシステムをサイジングする"。
12. * Flash Cache、書き込み速度、WORM * ：

    a. 必要に応じて、「Flash Cache」*を有効にします。

Cloud Volumes ONTAP 9.13.1以降では、n2-standard-16、n2-standard-32、n2-standard-48、およびn2-standard-64インスタンスタイプで_Flash Cache_が サポートされます。導入後にFlash Cacheを無効にすることはできません。

b. 必要に応じて、「標準」または「高速」の書き込み速度を選択します。

"書き込み速度の詳細については、こちらをご覧ください。"。

インスタンスタイプn2-standard-16、n2-standard-32、n2-standard-48、およびn2-standard-64では、* High * write speedオプションを使用して、高速の書き込み速度とより高いMaximum Transmission Unit（MTU；最大伝送ユニット）8、896バイトを使用できます。また、MTUが8、896の場合は、導入環境でVPC-1、VPC-2、およびVPC-3を選択する必要があります。高速の書き込み速度とMTU 8、896は機能に依存し、設定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、およびVPC-3の詳細については、を参照してください "VPC -1、VPC -2、およびVPC -3のルール"。

c. 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。

Cloud Volumes ONTAP 9.7以前のバージョンで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。Cloud Volumes ONTAP 9.8へのリバートまたはダウングレードは、WORMと階層化を有効にしたあとはブロックされます。

"WORM ストレージの詳細については、こちらをご覧ください。"。

a. WORMストレージをアクティブ化する場合は、保持期間を選択します。

13. * Google Cloudでのデータ階層化*：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 Volumes ONTAP インスタンスで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を階層化サービスアカウントのユーザーとして追加してください。追加しないと、BlueXP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すると、以降のアグリゲートで有効にすることができますが、システムの電源をオフにして、Google Cloud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。"。

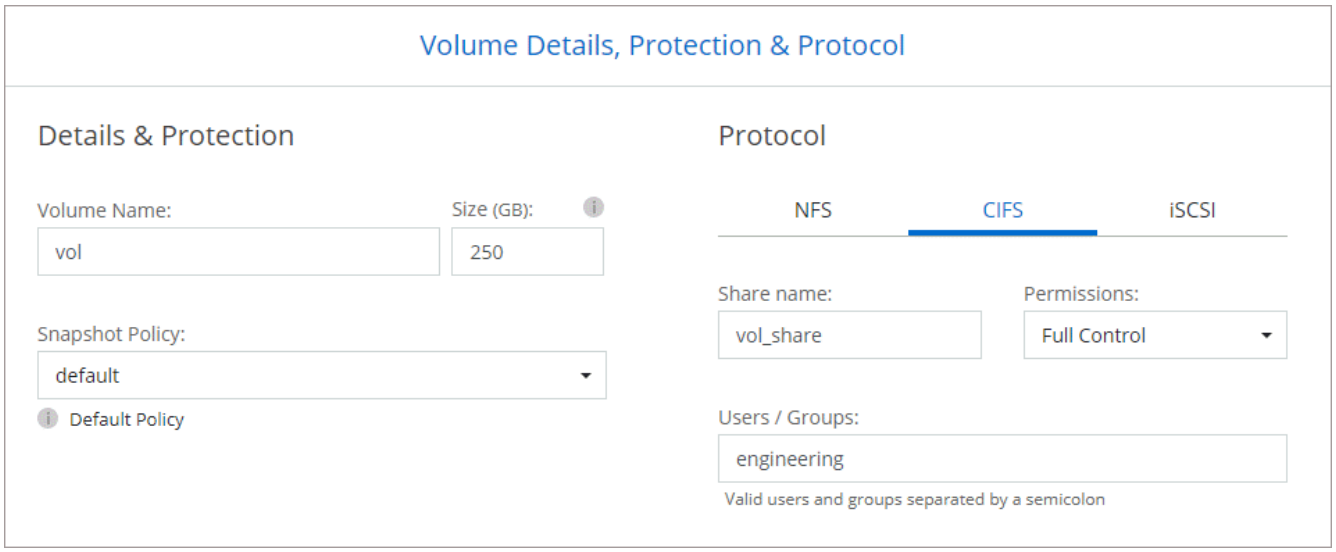
14. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

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

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



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 169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.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 サーバを参加させる Active Directory （ AD ）ドメインの FQDN 。
ドメインへの参加を許可されたクレデンシャル	AD ドメイン内の指定した組織単位（ OU ）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。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。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["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 "BlueXP自動化ドキュメント" を参照してください。 NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

16. * 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 "ボリュームの使用プロファイルを選択してください" および "データ階層化の概要"。

17. * レビューと承認 *: 選択内容を確認して確認します。
    a. 設定の詳細を確認します。
    b. サポートの詳細とBlueXPが購入するGoogle Cloudのリソースを確認するには、[詳細情報*]をクリックします。
    c. [* I understand … * （理解しています … * ）] チェックボックスを選択
    d. [Go*] をクリックします。

結果

BlueXPがCloud Volumes ONTAP システムを導入しました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。

Google Cloud Platformイメージの検証

Google Cloudの画像検証の概要

Google Cloudのイメージ検証機能は、ネットアップの高度なセキュリティ要件に準拠しています。このタスク用に特別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ためのイメージを生成するスクリプトに変更が加えられました。からダウンロードできるGoogle Cloud用の署名済みダイジェストとパブリック証明書を使用して、GCPイメージの整合性を検証できます "NSS" 特定のリリースの場合。

Google Cloudイメージの検証は、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で画像をRAW形式に変換します

新しいインスタンスの導入、アップグレード、または既存のイメージで使用されているイメージは、を通じてクライアントと共有されます "NetApp Support Site （NSS）"。署名済み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。ネットアップサポートが共有している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、9.13.0署名付きダイジェストとNSSで使用できる証明書があります。

この手順が必要なのはなぜですか？

Google Cloudからの画像は直接ダウンロードできません。署名済みダイジェストと証明書と照合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、画像を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。disk.rawファイルは、処理中にtarredおよびgzipされます。

ユーザ/サービスアカウントには、次の操作を実行するための権限が必要です。

- Googleストレージバケットへのアクセス
- Google Storageバケットに書き込みます
- クラウドビルドジョブの作成（エクスポートプロセスで使用）
- 目的の画像へのアクセス
- イメージのエクスポートタスクを作成します

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の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します

Cloud Storageにイメージをエクスポートする場合は、を使用することを推奨します "gcloud compute images exportコマンド"。このコマンドは、提供されたイメージを取得し、tarredおよびgzipされるdisk.rawファイルに変換します。生成されたファイルは保存先URLに保存され、ダウンロードして検証することができます。

この処理を実行するには、ユーザ/アカウントに目的のバケットへのアクセスと書き込み、イメージのエクスポート、およびクラウドビルド（Googleがイメージのエクスポートに使用）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します

をクリックしてスクリプトを表示します

```
$ 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
```

圧縮されたファイルを抽出します

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

を参照してください "画像のエクスポートに関するGoogle Cloudドキュメント" Google Cloudを使用して画像をエクスポートする方法の詳細については、を参照してください。

画像署名の検証

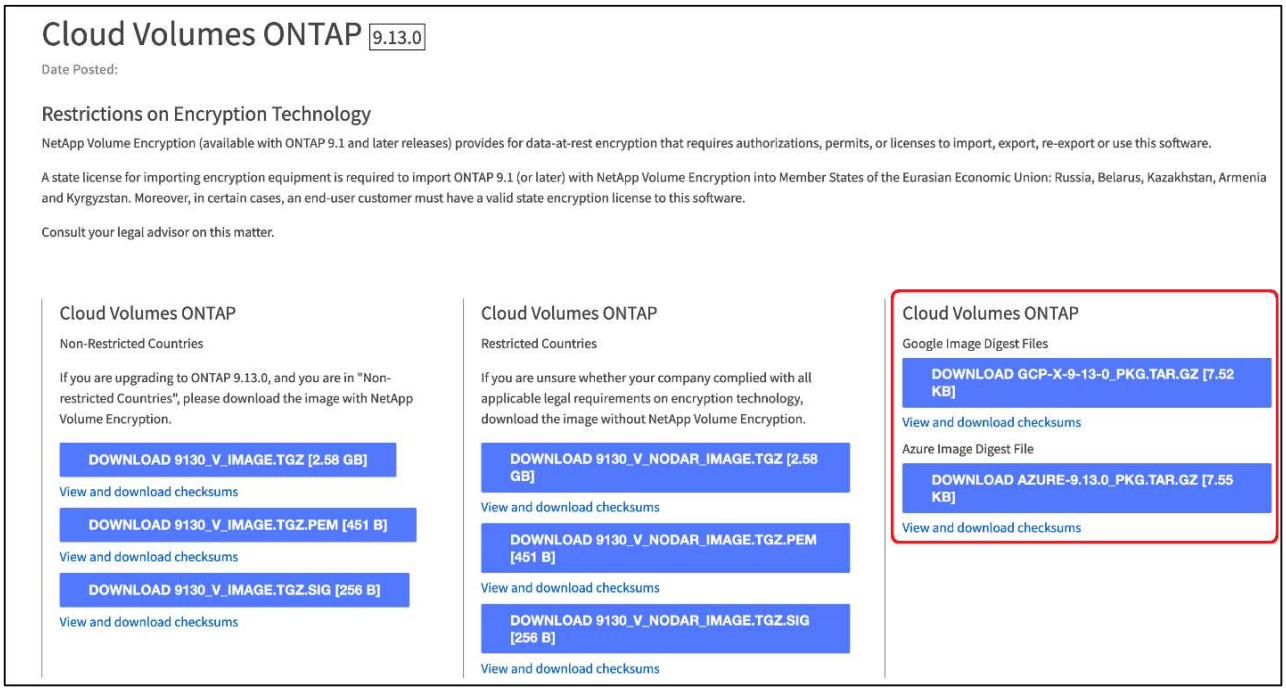
Google Cloudの署名済みイメージを検証します

エクスポートされたGoogle Cloud署名済みイメージを確認するには、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。

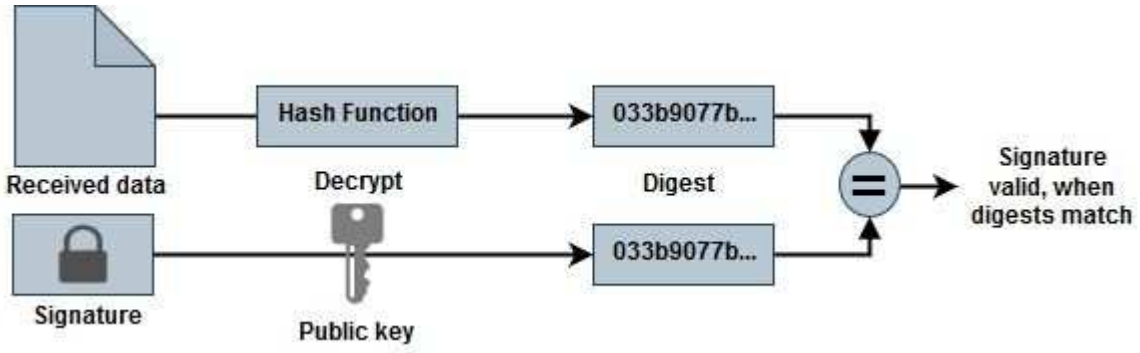
署名済み画像検証ワークフローの概要

以下は、Google Cloudの署名付き画像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（.pem）を含む証明書
  - 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します
- 証明書チェーンを使用して証明書を検証します
- 証明書に公開鍵が含まれていることを使用して、署名済みダイジェストを検証します
  - 公開鍵を使用して署名済みダイジェストを復号化し、イメージ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します
  - 2つのダイジェストファイルを比較して検証します



OpenSSLを使用した**disk.raw**ファイルおよびダイジェストファイルの内容の検証

Google Cloudでダウンロードしたdisk.rawファイルを、で使用できるダイジェストファイルの内容と照合して確認できます "NSS" OpenSSLを使用しています。

イメージがLinux、Mac OS、およびWindowsマシンと互換性があるかどうかを検証するOpenSSLコマンド。

手順

1. OpenSSLを使用して証明書を確認します。

をクリックしてスクリプトを表示します

```
# 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. 抽出した公開鍵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。

をクリックしてスクリプトを表示します

```
# 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
```

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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な保証、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、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

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って保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

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