NetApp for GCP / GCVE

NetApp Solutions

NetApp
April 10, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/netapp-solutions/ehc/gcp-app-dr-sc-cvs-veeam.html on April 10, 2024. Always check docs.netapp.com for the latest.

目次

VMwareソリューションを使用したネットアップのハイブリッドマルチクラウド 1
GCP / GCVEでのワークロードの保護 1
GCP / GCVEでのワークロードの移行 8
リージョンの可用性–Google Cloud Platform（GCP）向けのNFSデータストア補足機能 29
セキュリティの概要- Google CloudでのNetApp Cloud Volumes Service （CVS 31

VMwareソリューションを使用したネットアップのハイブリッドマルチクラウド

GCP / GCVEでのワークロードの保護

NetApp SnapCenterとVeeamのレプリケーションにより、アプリケーションと整合性のあるディザスタリカバリを実現

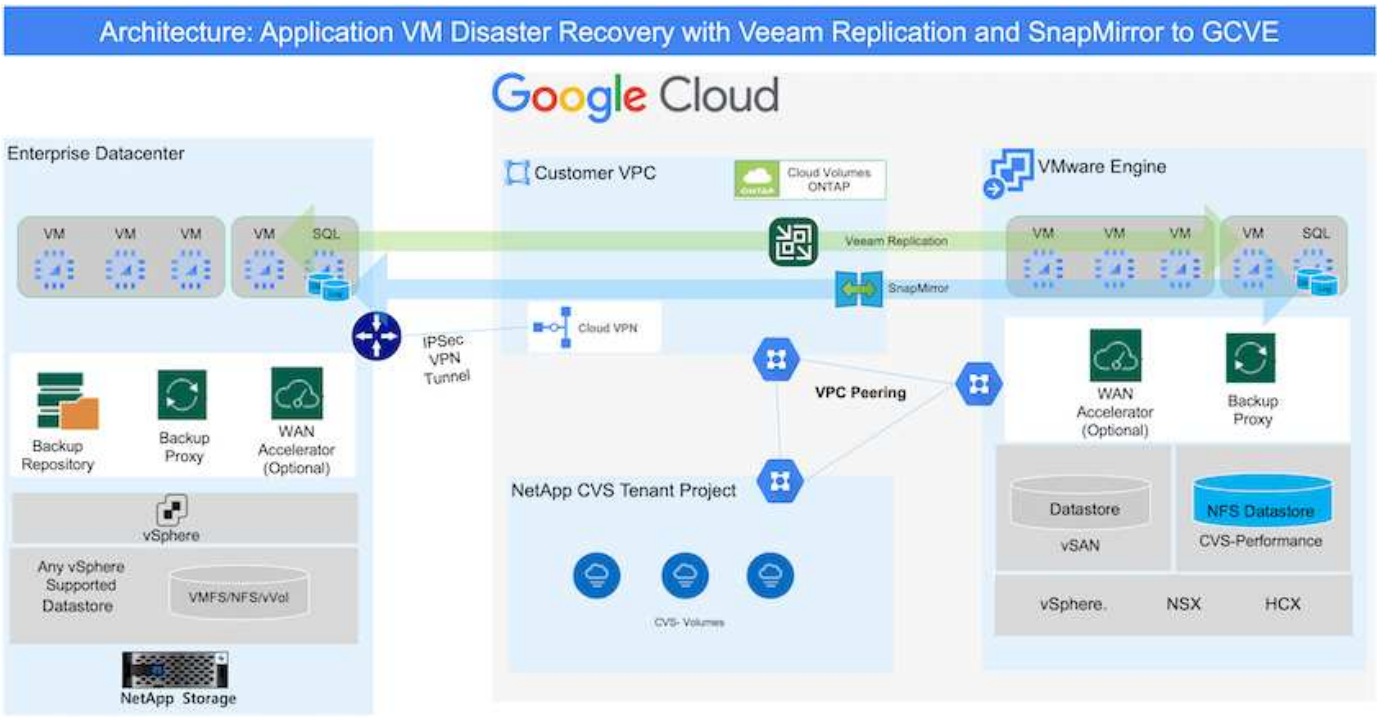
執筆者：ネットアップSuresh Thoppay

概要

多くのお客様は、VMware vSphereでホストされているアプリケーションVMに対して、効果的なディザスタリカバリ解決策を求めています。それらの多くは、既存のバックアップ解決策を使用して、ダイヤル中に回復を実行します。
多くの場合、解決策はRTOを高め、期待に応えられません。RPOとRTOを短縮するために、適切な権限を持つネットワーク接続と環境が利用可能であれば、オンプレミスからGCVEへのVeeam VMレプリケーションを利用できます。
注: Veeam VM Replicationでは、ゲストVM内のiSCSIマウントやNFSマウントなどのVMゲスト接続ストレージデバイスは保護されません。それらを別 々 に保護する必要があります。

SQL VMでアプリケーションと整合性のあるレプリケーションを実現し、RTOを短縮するために、SnapCenterを使用してSQLデータベースとログボリュームのSnapMirror処理をオーケストレーションしました。

このドキュメントでは、NetApp SnapMirror、Veeam、Google Cloud VMware Engine（GCVE）を使用してディザスタリカバリを設定および実行するためのステップバイステップ形式のアプローチについて説明します。



前提条件

本ドキュメントでは、アプリケーションデータ用のゲスト内ストレージ（ゲスト接続とも呼ばれます）を中心に説明します。オンプレミス環境では、アプリケーションと整合性のあるバックアップにSnapCenter を使用していると想定しています。

> 本ドキュメントは、環境 サードパーティ製バックアップまたはリカバリ用解決策 に関するものです。環境で使用されている解決策 に応じて、ベストプラクティスに従って、組織のSLAを満たすバックアップポリシーを作成してください。

オンプレミス環境とGoogle Cloudネットワーク間の接続には、専用のインターコネクトやCloud VPNなどの接続オプションを使用します。オンプレミスVLANの設計に基づいてセグメントを作成する必要があります。

> オンプレミスのデータセンターをGoogle Cloudに接続する方法は複数ありますが、この方法では、このドキュメントの特定のワークフローの概要を説明することはできません。オンプレミスからGoogleへの適切な接続方法については、Google Cloudのドキュメントを参照してください。

DR解決策 の導入

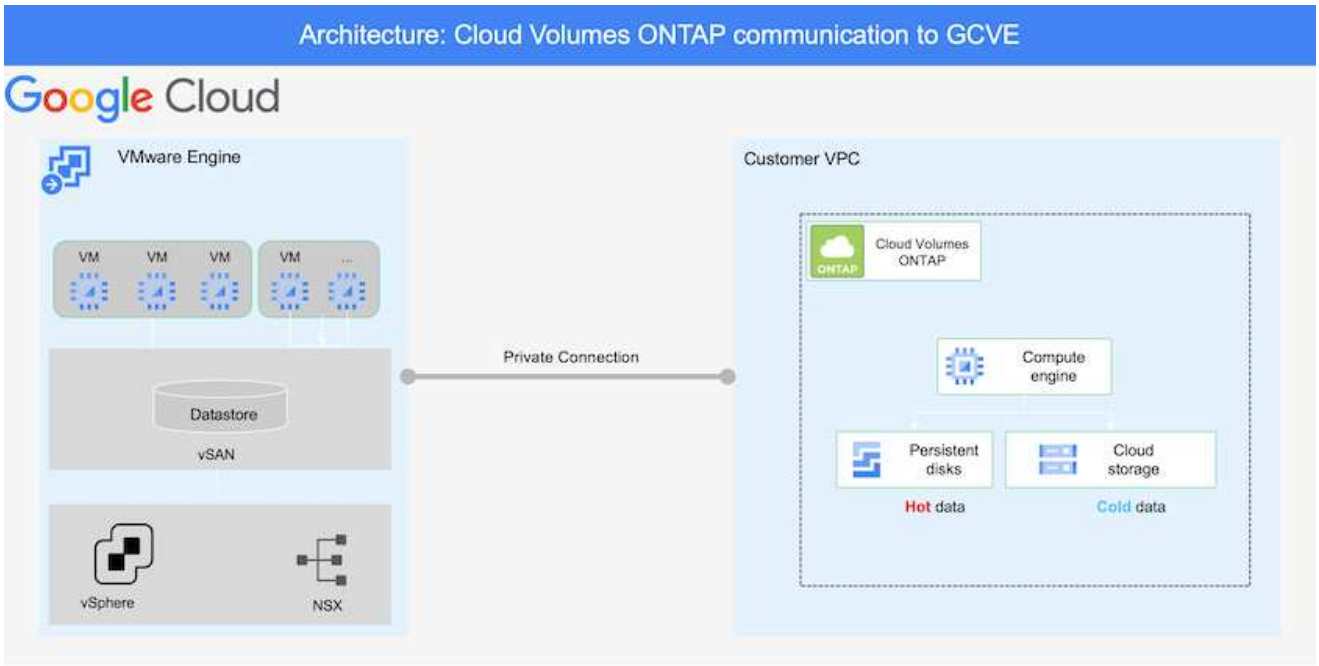
解決策 の導入の概要

1. SnapCenter を使用して、必要なRPO要件に従ってアプリケーションデータがバックアップされていることを確認してください。
2. 適切なサブスクリプションと仮想ネットワーク内でBlueXPを使用して、正しいインスタンスサイズでCloud Volumes ONTAPをプロビジョニングします。
   a. 該当するアプリケーションボリュームに対してSnapMirrorを設定します。
   b. スケジュールされたジョブの実行後にSnapMirror更新をトリガーするには、SnapCenter でバックアップポリシーを更新してください。
3. Veeamソフトウェアをインストールし、Google Cloud VMware Engineインスタンスへの仮想マシンのレプリケーションを開始します。
4. 災害発生時には、BlueXPを使用してSnapMirror関係を解除し、Veeamで仮想マシンのフェイルオーバーをトリガーします。
   a. アプリケーションVMのiSCSI LUNおよびNFSマウントを再接続します。
   b. アプリケーションをオンラインにします。
5. プライマリサイトのリカバリ後にSnapMirrorを逆再同期して、保護サイトへのフェイルバックを開始します。

展開の詳細

Google Cloudで**CVO**を構成し、ボリュームを**CVO**にレプリケート

最初の手順は、Google CloudでCloud Volumes ONTAP を設定することです ("CVOを確認して"）をクリックし、必要なボリュームを、必要な頻度とSnapshotの保持を使用してCloud Volumes ONTAP にレプリケートします。



SnapCenter の設定およびデータのレプリケートの手順の例については、を参照してください "SnapCenter を使用してレプリケーションを設定する"

SnapCenterを使用したSQL VMの保護の確認

GCVEホストと**CVO**データアクセスを設定する

SDDCを導入する際に考慮すべき2つの重要な要素は、GCVE解決策 のSDDCクラスタのサイズと、SDDCの稼働時間です。ディザスタリカバリ解決策 に関する以下の2つの重要な考慮事項は、全体的な運用コストの削減に役立ちます。SDDCは、3台のホストの規模に対応し、フルスケールの導入ではマルチホストクラスタにまで対応できます。

NetApp Cloud Volume Service for NFS DatastoreおよびCloud Volumes ONTAP for SQLデータベースとログを任意のVPCに導入できます。GCVEは、NFSデータストアをマウントしてVMをiSCSI LUNに接続するために、そのVPCにプライベート接続を確立する必要があります。

GCVE SDDCを設定するには、を参照してください "Google Cloud Platform （ GCP ）への仮想化環境の導入と構成"。前提条件として、接続が確立された後で、GCVEホストに存在するゲストVMがCloud Volumes ONTAP からデータを使用できることを確認します。

Cloud Volumes ONTAP とGCVEを適切に設定したら、Veeamのレプリケーション機能を使用して、Cloud Volumes ONTAP へのアプリケーションボリュームコピーにSnapMirrorを利用することで、オンプレミスのワークロードのGCVE（アプリケーションVMDKおよびゲストストレージを搭載したVM）へのリカバリを自動化するようにVeeamを設定します。

Veeamコンポーネントをインストールします

導入シナリオに基づいて、Veeamバックアップサーバ、バックアップリポジトリ、およびバックアッププロキシを導入する必要があります。このユースケースでは、Veeam用のオブジェクトストアとスケールアウトリポジトリも必要ありません。
"インストール手順 については、Veeamの製品ドキュメントを参照してください"
追加情報については、を参照してください "Veeam Replicationによる移行"

VMレプリケーションを**Veeam**とセットアップする

オンプレミスのvCenterとGCVEのvCenterをVeeamに登録する必要があります。 "vSphere VMレプリケーションジョブをセットアップします" ウィザードの[ゲスト処理]ステップで、[アプリケーション対応のバックアップとリカバリにSnapCenter を使用するので、アプリケーション処理を無効にする]を選択します。

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

Microsoft SQL Server VMのフェイルオーバー

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

この解決策 の利点

- 効率性と耐障害性に優れたSnapMirrorレプリケーションを使用します。
- ONTAP スナップショットの保持により、利用可能な任意の時点までリカバリします。
- ストレージ、コンピューティング、ネットワーク、アプリケーションの検証から、数百~数千のVMのリカバリに必要なすべての手順を完全に自動化できます。
- SnapCenter では、レプリケートされたボリュームを変更しないクローニングメカニズムが使用されます。
  - これにより、ボリュームとSnapshotのデータが破損するリスクを回避できます。
  - DRテストのワークフロー中にレプリケーションが中断されるのを回避します
  - 開発とテスト、セキュリティテスト、パッチとアップグレードのテスト、修正テストなど、DR以外のワークフローにDRデータを活用します。
- Veeam Replicationでは、DRサイトのVMのIPアドレスを変更できます。

SnapCenter 、**Cloud Volumes ONTAP** 、**Veeam**レプリケーションを使用したアプリケーションディザスタリカバリ

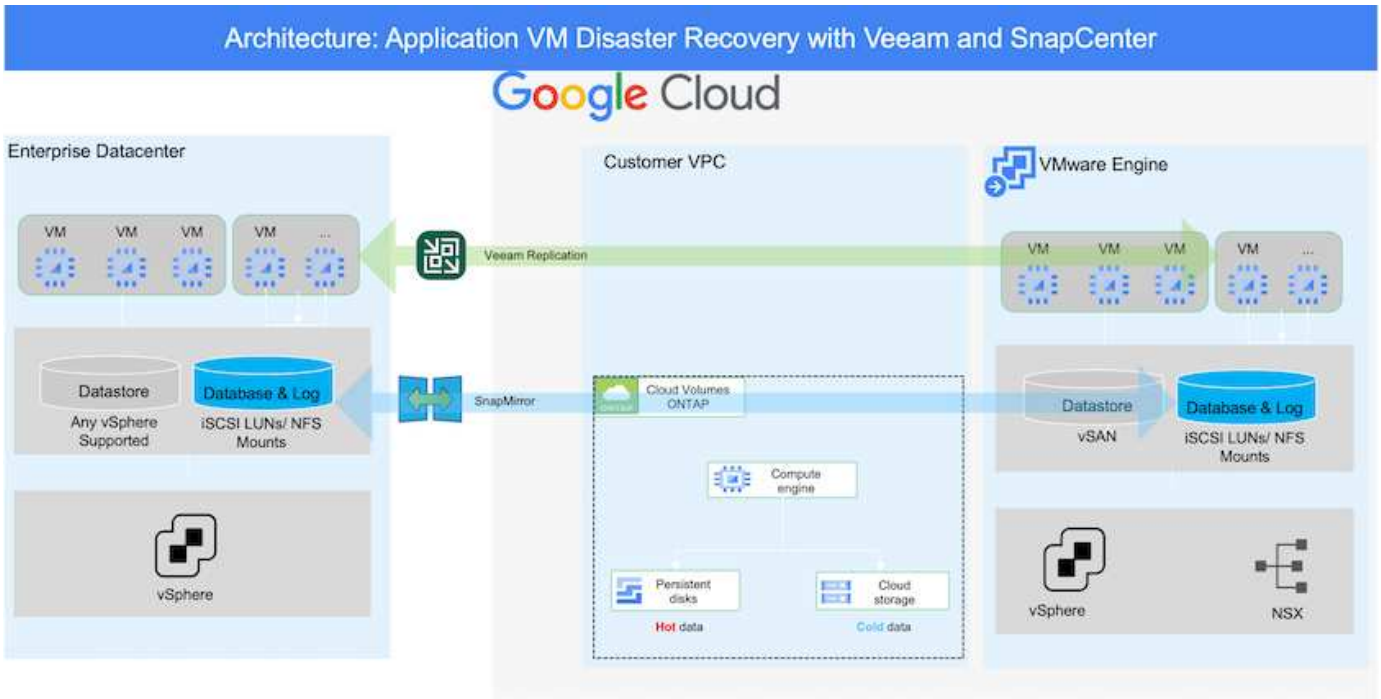
執筆者：ネットアップSuresh Thoppay

概要

クラウドへのディザスタリカバリは、耐障害性と対費用効果に優れた方法で、サイトの停止やランサムウェア

などのデータ破損からワークロードを保護します。NetApp SnapMirrorを使用すると、ゲスト接続ストレージを使用するオンプレミスのVMwareワークロードを、Google Cloudで実行されているNetApp Cloud Volumes ONTAP にレプリケートできます。これはアプリケーションデータに適用されますが、実際のVM自体についてはどうでしょうか。ディザスタリカバリは、仮想マシン、VMDK、アプリケーションデータなど、依存するすべてのコンポーネントを対象にする必要があります。これを実現するために、SnapMirrorとVeeamを併用すれば、オンプレミスからCloud Volumes ONTAP にレプリケートしたワークロードをシームレスにリカバリしながら、VM VMDKにvSANストレージを使用することができます。

このドキュメントでは、NetApp SnapMirror、Veeam、Google Cloud VMware Engine（GCVE）を使用してディザスタリカバリを設定および実行するためのステップバイステップ形式のアプローチについて説明します。



前提条件

本ドキュメントでは、アプリケーションデータ用のゲスト内ストレージ（ゲスト接続とも呼ばれます）を中心に説明します。オンプレミス環境では、アプリケーションと整合性のあるバックアップにSnapCenter を使用していると想定しています。

> ⓘ 本ドキュメントは、環境 サードパーティ製バックアップまたはリカバリ用解決策 に関するものです。環境で使用されている解決策 に応じて、ベストプラクティスに従って、組織のSLAを満たすバックアップポリシーを作成してください。

オンプレミス環境とGoogle Cloudネットワーク間の接続には、専用のインターコネクトやCloud VPNなどの接続オプションを使用します。オンプレミスVLANの設計に基づいてセグメントを作成する必要があります。

> ⓘ オンプレミスのデータセンターをGoogle Cloudに接続する方法は複数ありますが、この方法では、このドキュメントの特定のワークフローの概要を説明することはできません。オンプレミスからGoogleへの適切な接続方法については、Google Cloudのドキュメントを参照してください。

DR解決策 の導入

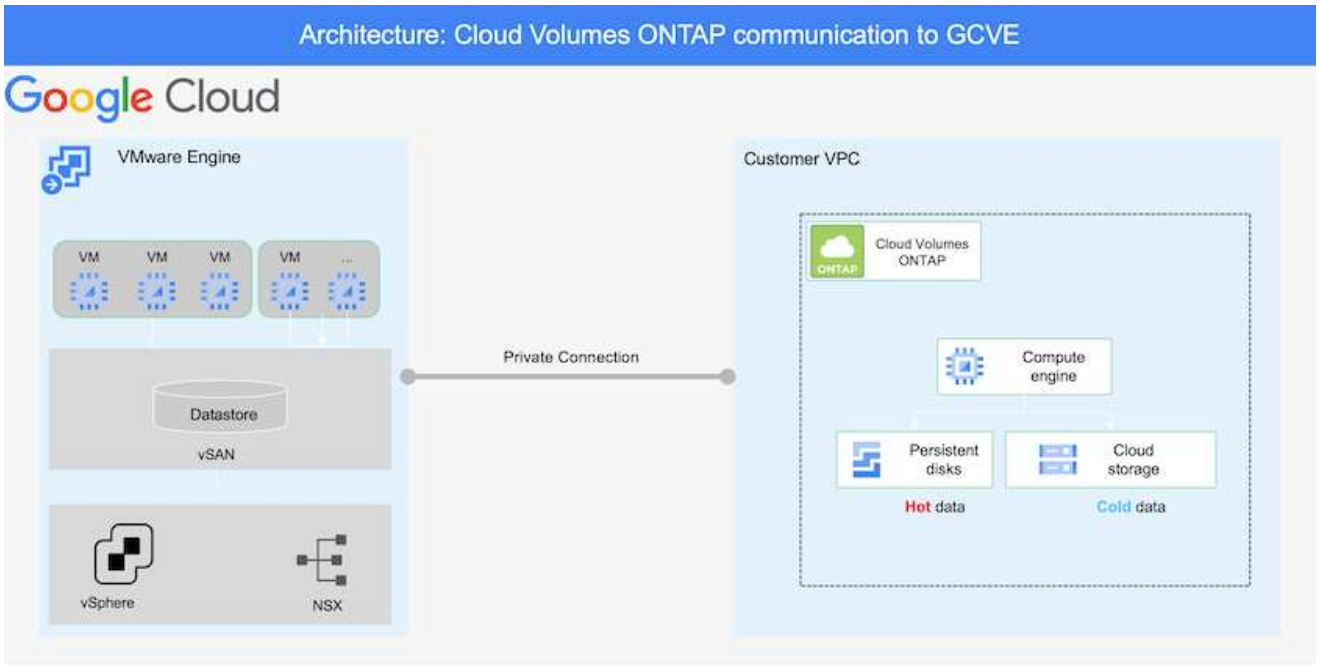
解決策 の導入の概要

1. SnapCenter を使用して、必要なRPO要件に従ってアプリケーションデータがバックアップされていることを確認してください。
2. 適切なサブスクリプションと仮想ネットワーク内で、Cloud Managerを使用して、適切なインスタンスサイズでCloud Volumes ONTAP をプロビジョニングします。
   a. 該当するアプリケーションボリュームに対してSnapMirrorを設定します。
   b. スケジュールされたジョブの実行後にSnapMirror更新をトリガーするには、SnapCenter でバックアップポリシーを更新してください。
3. Veeamソフトウェアをインストールし、Google Cloud VMware Engineインスタンスへの仮想マシンのレプリケーションを開始します。
4. 災害発生時は、Cloud Managerを使用してSnapMirror関係を解除し、仮想マシンとVeeamのフェイルオーバーをトリガーします。
   a. アプリケーションVMのiSCSI LUNおよびNFSマウントを再接続します。
   b. アプリケーションをオンラインにします。
5. プライマリサイトのリカバリ後にSnapMirrorを逆再同期して、保護サイトへのフェイルバックを開始します。

展開の詳細

Google Cloudで**CVO**を構成し、ボリュームを**CVO**にレプリケート

最初の手順は、Google CloudでCloud Volumes ONTAP を設定することです ("CVOを確認して"）をクリックし、必要なボリュームを、必要な頻度とSnapshotの保持を使用してCloud Volumes ONTAP にレプリケートします。



SnapCenter を設定してデータを複製する手順の例については、を参照してください "SnapCenter を使用してレプリケーションを設定する"

SnapCenter を使用してレプリケーションを設定する

GCVEホストと**CVO**データアクセスを設定する

SDDCを導入する際に考慮すべき2つの重要な要素は、GCVE解決策 のSDDCクラスタのサイズと、SDDCの稼働時間です。ディザスタリカバリ解決策 に関する以下の2つの重要な考慮事項は、全体的な運用コストの削減に役立ちます。SDDCは、3台のホストの規模に対応し、フルスケールの導入ではマルチホストクラスタにまで対応できます。

Cloud Volumes ONTAP は任意のVPCに導入でき、GCVEはそのVPCへのプライベート接続でiSCSI LUNに接続する必要があります。

GCVE SDDCを設定するには、を参照してください "Google Cloud Platform （ GCP ）への仮想化環境の導入と構成"。前提条件として、接続が確立された後で、GCVEホストに存在するゲストVMがCloud Volumes ONTAP からデータを使用できることを確認します。

Cloud Volumes ONTAP とGCVEを適切に設定したら、Veeamのレプリケーション機能を使用して、Cloud Volumes ONTAP へのアプリケーションボリュームコピーにSnapMirrorを利用することで、オンプレミスのワークロードのGCVE（アプリケーションVMDKおよびゲストストレージを搭載したVM）へのリカバリを自動化するようにVeeamを設定します。

Veeamコンポーネントをインストールします

導入シナリオに基づいて、Veeamバックアップサーバ、バックアップリポジトリ、およびバックアッププロキシを導入する必要があります。このユースケースでは、Veeam用のオブジェクトストアとスケールアウトリポジトリも必要ありません。https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["インストール手順 については、Veeamの製品ドキュメントを参照してください"]

VMレプリケーションを**Veeam**とセットアップする

オンプレミスのvCenterとGCVEのvCenterをVeeamに登録する必要があります。 "vSphere VMレプリケーションジョブをセットアップします" ウィザードの[ゲスト処理]ステップで、[アプリケーション対応のバックアップとリカバリにSnapCenter を使用するので、アプリケーション処理を無効にする]を選択します。

vSphere VMレプリケーションジョブをセットアップします

Microsoft SQL Server VMのフェイルオーバー

Microsoft SQL Server VMのフェイルオーバー

この解決策 の利点

- 効率性と耐障害性に優れたSnapMirrorレプリケーションを使用します。
- ONTAP スナップショットの保持により、利用可能な任意の時点までリカバリします。
- ストレージ、コンピューティング、ネットワーク、アプリケーションの検証から、数百~数千のVMのリカバリに必要なすべての手順を完全に自動化できます。
- SnapCenter では、レプリケートされたボリュームを変更しないクローニングメカニズムが使用されます。
  - これにより、ボリュームとSnapshotのデータが破損するリスクを回避できます。
  - DRテストのワークフロー中にレプリケーションが中断されるのを回避します
  - 開発とテスト、セキュリティテスト、パッチとアップグレードのテスト、修正テストなど、DR以外のワークフローにDRデータを活用します。
- Veeam Replicationでは、DRサイトのVMのIPアドレスを変更できます。

GCP / GCVEでのワークロードの移行

VMware HCX-Quickstartガイドを使用して、Google Cloud VMware Engine上のNetApp Cloud Volume Serviceデータストアにワークロードを移行します

執筆者：NetApp Solutions Engineering

概要：**VMware HCX**、**NetApp Cloud Volume Service**データストア、**Google Cloud VMware Engine**（**GCVE**）を使用した仮想マシンの移行

Google Cloud VMware EngineおよびCloud Volume Serviceデータストアの最も一般的なユースケースの1つは、VMwareワークロードの移行です。VMware HCXは推奨されるオプションであり、オンプレミスの仮想マシン（VM）とそのデータをCloud Volume Service NFSデータストアに移動するためのさまざまな移行メカニズムを提供します。

VMware HCXは、主に移行プラットフォームであり、クラウド間でのアプリケーションの移行、ワークロードの再バランシング、ビジネス継続性の簡素化を目的として設計されています。Google Cloud VMware Engine Private Cloudの一部として提供されており、ワークロードを移行し、ディザスタリカバリ（DR）処理に使用するためのさまざまな方法を提供します。

このドキュメントでは、Cloud Volume Serviceデータストアのプロビジョニングの手順ごとのガイダンスを示し、その後、さまざまなVM移行メカニズムを有効にするためのInterconnect、Network Extension、WAN最適化など、オンプレミスおよびGoogle Cloud VMware Engine側のすべての主要コンポーネントを含むVMware HCXのダウンロード、導入、設定を行います。

> VMware HCXはVMレベルで移行されるため、どのデータストアタイプでも動作します。このドキュメントは、対費用効果の高いVMwareクラウド導入のためにGoogle Cloud VMware Engineを使用したCloud Volume Serviceの導入を計画している既存のネットアップのお客様およびネットアップ以外のお客様を対象としています。

手順の概要

次のリストは、オンプレミスのHCX ConnectorからGoogle Cloud VMware Engine側のHCX Cloud ManagerにVMをペアリングして移行するために必要な手順の概要を示しています。

1. Google VMware Engineポータルを使用してHCXを準備します。
2. HCX Connector Open Virtualization Appliance（OVA）インストーラをオンプレミスのVMware vCenter Serverにダウンロードして導入します。
3. ライセンスキーを使用してHCXをアクティブにします。
4. オンプレミスのVMware HCXコネクタをGoogle Cloud VMware Engine HCX Cloud Managerとペアリングします。
5. ネットワークプロファイル、コンピューティングプロファイル、およびサービスメッシュを設定します。
6. （オプション）移行中に再IPが発生しないように、ネットワーク拡張を実行します。
7. アプライアンスのステータスを検証し、移行が可能であることを確認します。
8. VMワークロードを移行する。

前提条件

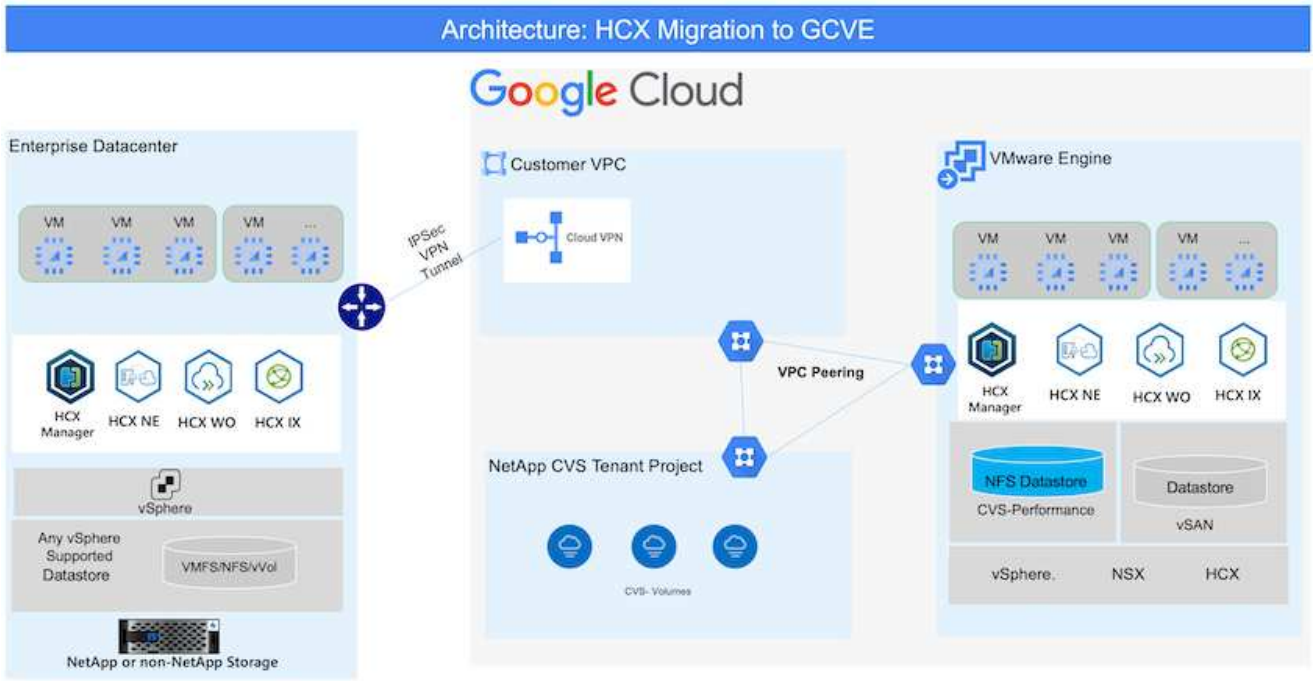
作業を開始する前に、次の前提条件が満たされていることを確認してください。詳細については、を参照してください "リンク"。接続などの前提条件が整ったら、Google Cloud VMware EngineポータルからHCXライセンスキーをダウンロードします。OVAインストーラをダウンロードしたら、次の手順に従ってインストールプロセスを実行します。

> HCx advancedはデフォルトオプションであり、VMware HCX Enterprise Editionはサポートチケットを通じても利用でき、追加料金なしでサポートされます。を参照してください "リンクをクリックしてください"

- 既存のGoogle Cloud VMware Engine Software-Defined Data Center（SDDC）を使用するか、このツールを使用してプライベートクラウドを作成します "ネットアップのリンク" またはこれ "Googleリンク"。
- オンプレミスのVMware vSphere対応データセンターからVMと関連データを移行するには、データセンターからSDDC環境へのネットワーク接続が必要です。ワークロードを移行する前に、 "Cloud VPN接続またはCloud Interconnect接続をセットアップします" オンプレミス環境とそれぞれのプライベートクラウドの間。
- オンプレミスのVMware vCenter Server環境からGoogle Cloud VMware Engineプライベートクラウドへのネットワークパスで、vMotionを使用したVMの移行がサポートされている必要があります。
- 必要なを確認します "ファイアウォールルールとポート" オンプレミスのvCenter ServerとSDDC vCenter間のvMotionトラフィックに許可されます。
- Cloud Volume Service NFSボリュームは、Google Cloud VMware Engineでデータストアとしてマウントする必要があります。詳細な手順を実行します "リンク" をクリックして、Cloud Volume ServiceデータストアをGoogle Cloud VMware Engineホストに接続します。

アーキテクチャの概要

テスト目的で、この検証に使用したオンプレミスのラボ環境は、Cloud VPNを介して接続されています。これにより、オンプレミスからGoogle Cloud VPCへの接続が可能になります。



HCXの詳細な図については、を参照してください "VMwareへのリンク"

解決策 の導入

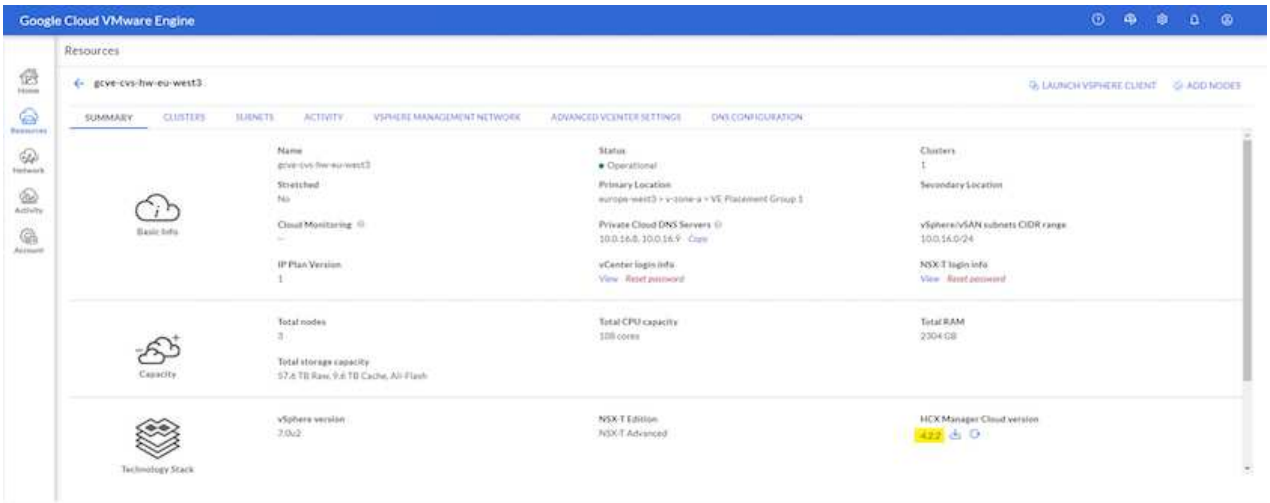
一連の手順に従って、この解決策 の導入を完了します。

ステップ**1**：**Google VMware Engine Portal**を使用して**HCX**を準備する

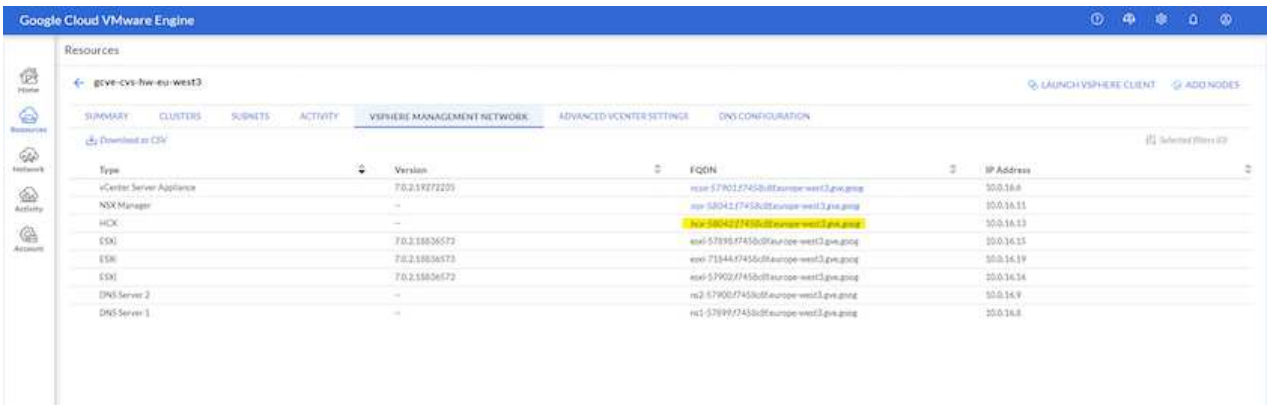
VMware Engineでプライベートクラウドをプロビジョニングすると、HCx Cloud Managerコンポーネントが自動的にインストールされます。サイトペアリングを準備するには、次の手順を実行します。

1. Google VMware Engine Portalにログインし、HCX Cloud Managerにサインインします。

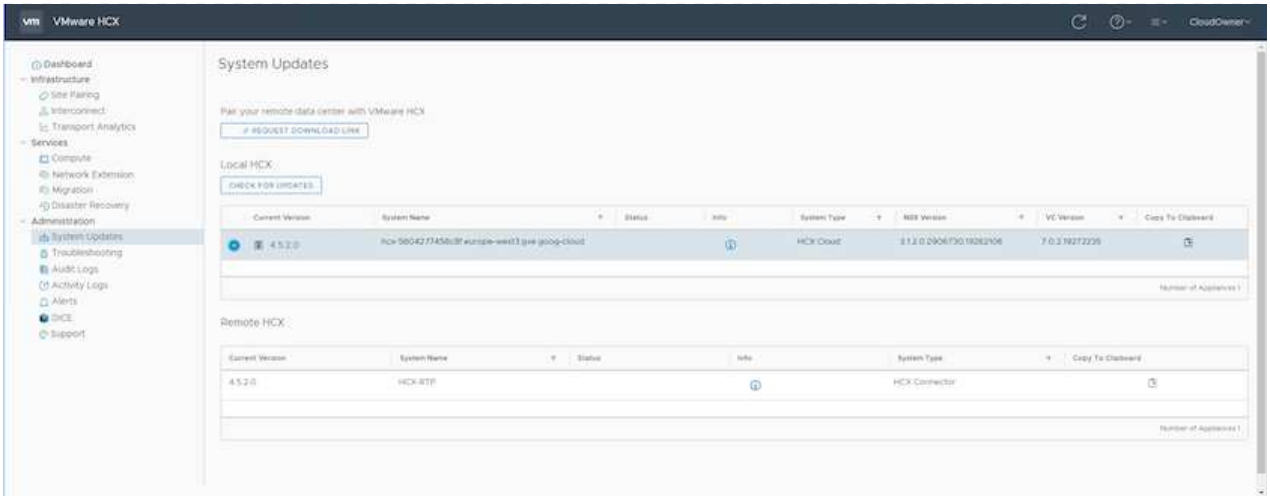
   HCXバージョンのリンクをクリックすると'HCXコンソールにログインできます



   または、vSphere Management NetworkタブのHCX FQDNをクリックします。



2. HCX Cloud Managerで、[**Administration]>[System Updates**（システムアップデート*）]の順に選択します。
3. [ダウンロードリンクのリクエスト]をクリックして、OVAファイルをダウンロードします。



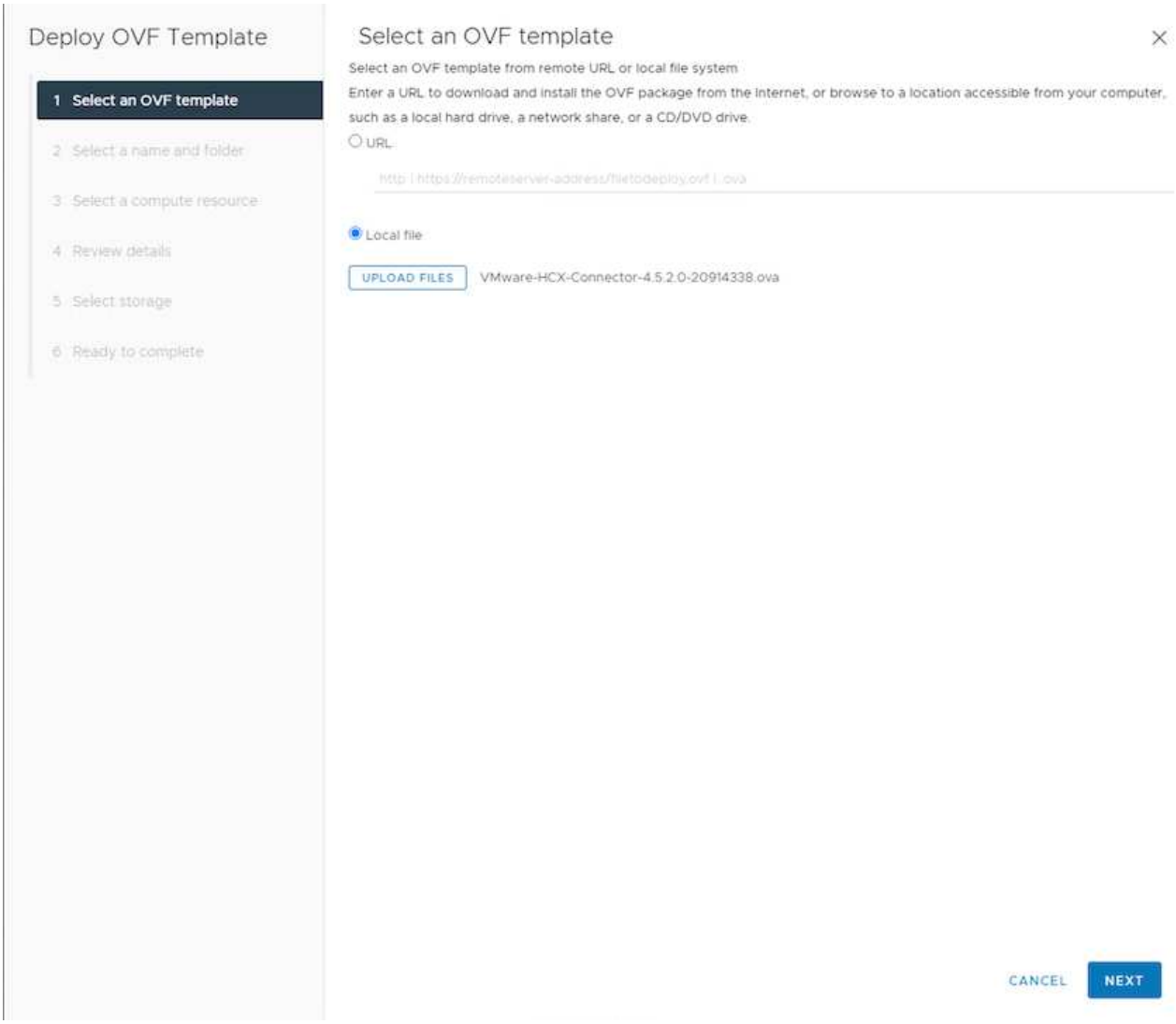
4. HCX Cloud ManagerをHCX Cloud Manager UIから入手可能な最新バージョンに更新します。

手順**2**：オンプレミスの**vCenter Server**にインストーラ**OVA**を導入する

Google Cloud VMware EngineのHCX Managerにオンプレミスコネクタを接続するには、オンプレミス環境で適切なファイアウォールポートが開いていることを確認します。

HCX ConnectorをオンプレミスのvCenter Serverにダウンロードしてインストールするには、次の手順を実行します。

1. 前の手順で説明したように、Google Cloud VMware Engine上のHCXコンソールからOVAをダウンロードしてもらいます。
2. OVAをダウンロードしたら、* Deploy OVF Template *オプションを使用して、OVAをオンプレミスのVMware vSphere環境に導入します。



3. OVA導入に必要なすべての情報を入力し、「次へ」をクリックしてから、「*完了」をクリックしてVMware HCX Connector OVAを導入します。

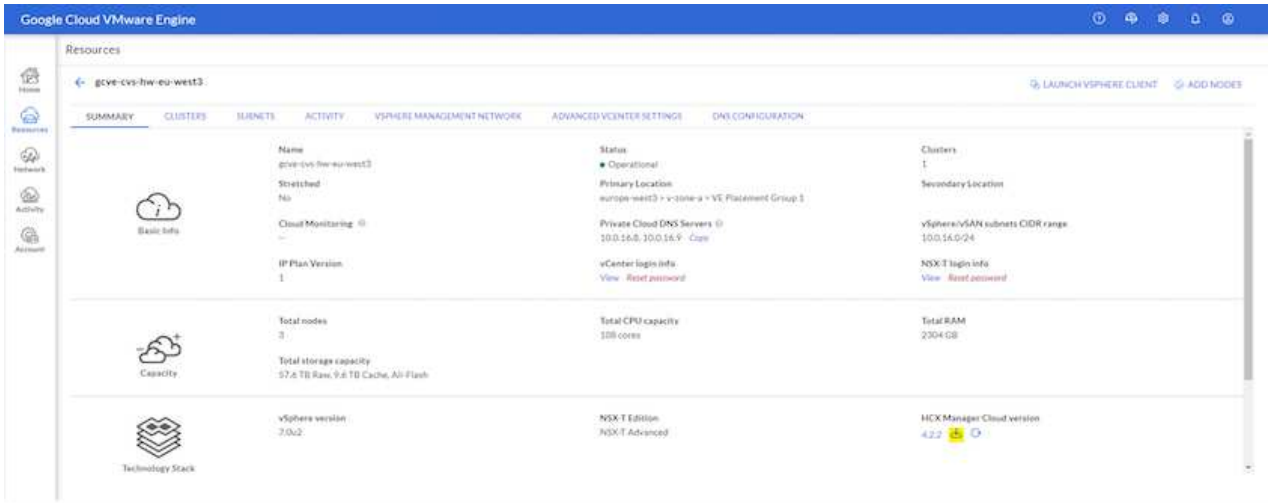
仮想アプライアンスの電源を手動でオンにします。

手順については、を参照してください "VMware HCXユーザーガイド"。

手順**3**：ライセンスキーを使用して**HCX**コネクタをアクティブにします

VMware HCX Connector OVAをオンプレミスに導入してアプライアンスを起動したら、次の手順を実行してHCX Connectorをアクティブにします。Google Cloud VMware Engineポータルからライセンスキーを生成し、VMware HCX Managerでアクティブ化します。

1. VMware Engineポータルで、Resources（リソース）をクリックし、プライベートクラウドを選択して、* HCX Manager Cloud Version（HCXマネージャクラウドバージョン）の下にあるdownload（ダウンロード）アイコンをクリックします。
*



ダウンロードしたファイルを開き、ライセンスキー文字列をコピーします。

2. オンプレミスのVMware HCX Managerにログインします "https://hcxmanagerIP:9443" 管理者のクレデンシャルを使用

> OVAの導入時に定義したhcxmanagerIPとパスワードを使用します。

3. ライセンスで、手順3からコピーしたキーを入力し、[* Activate*（有効化*）]をクリックします。

> オンプレミスのHCXコネクタにはインターネットアクセスが必要です。

4. **[Datacenter Location]**には、**VMware HCX Manager**をオンプレミスにインストールするために最も近い場所を指定します。**[** Continue （続行）] をクリックします
5. システム名*で名前を更新し、*続行*をクリックします。
6. [はい、続行]をクリックします。
7. [* vCenterの接続*]で、vCenter Serverの完全修飾ドメイン名（FQDN）またはIPアドレスと適切なクレデンシャルを入力し、[*続行]をクリックします。

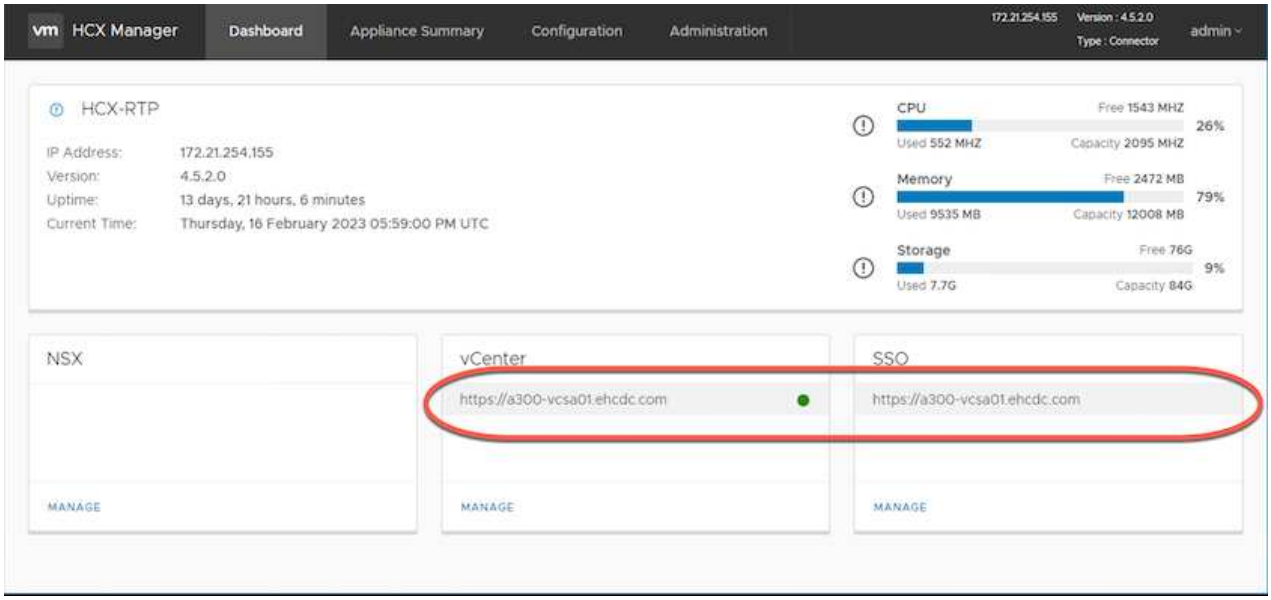
> あとで接続の問題が発生しないようにFQDNを使用してください。

8. Configure SSO/PSC で、**Platform Services Controller**（**PSC**）の**FQDN**または**IP**アドレスを入力し、 Continue *をクリックします。

> Embedded PSCの場合、VMware vCenter ServerのFQDNまたはIPアドレスを入力します。

9. 入力された情報が正しいことを確認し、[* Restart]をクリックします。
10. サービスが再起動すると、表示されるページに緑で表示されます。vCenter ServerとSSOの両方に適切な設定パラメータが必要です。これは前のページと同じである必要があります。

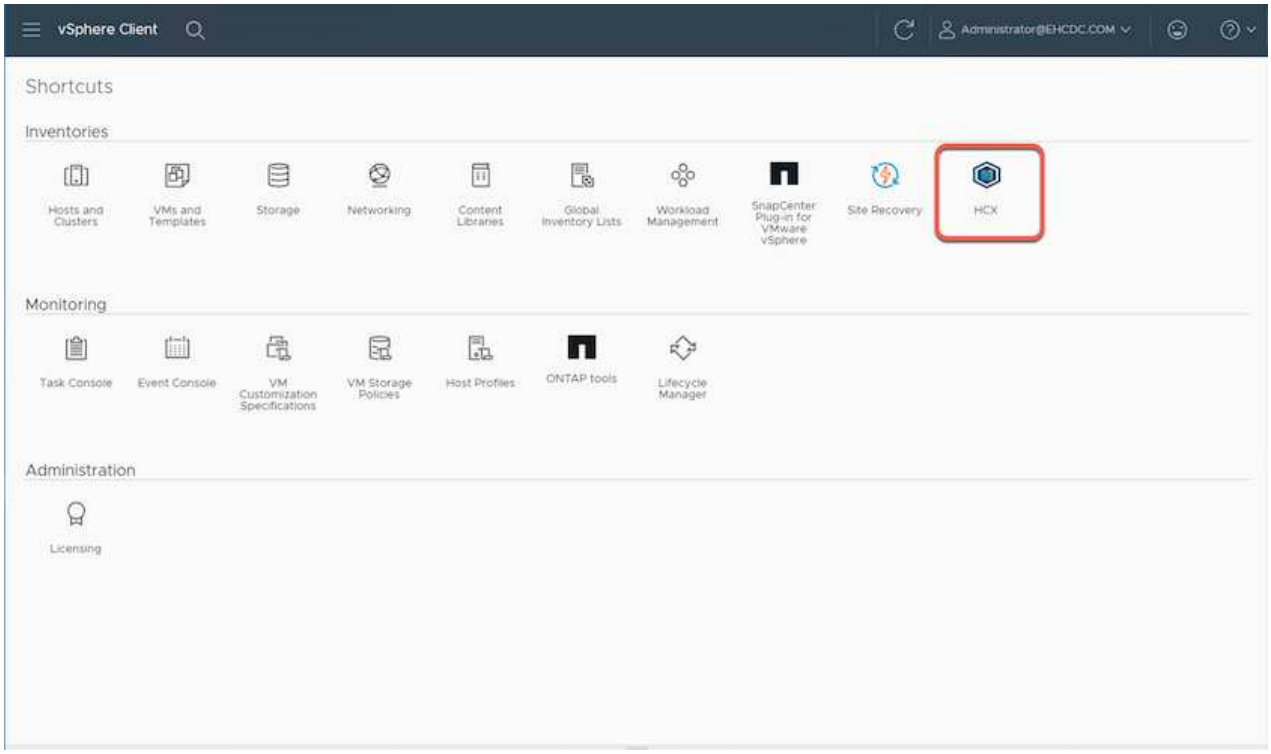
> この処理には10~20分かかります。また、プラグインをvCenter Serverに追加する必要があります。



手順**4**：オンプレミスの**VMware HCX Connector**と**Google Cloud VMware Engine HCX Cloud Manager**をペアリングします

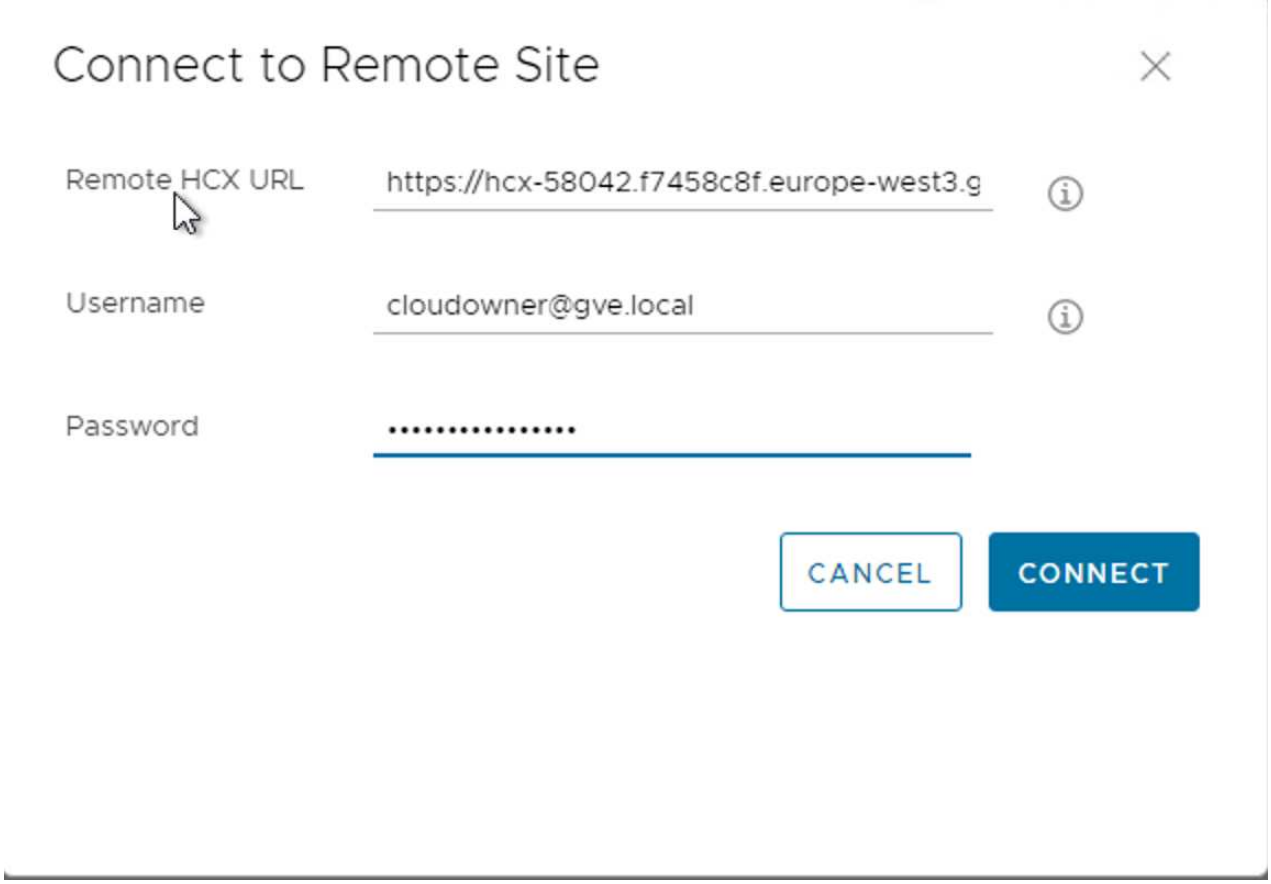
オンプレミスのvCenterにHCX Connectorを導入して設定したら、このペアリングを追加してCloud Managerへの接続を確立します。サイトペアリングを設定するには、次の手順を実行します。

1. オンプレミスのvCenter環境とGoogle Cloud VMware Engine SDDCの間にサイトペアを作成するには、オンプレミスのvCenter Serverにログインし、新しいHCX vSphere Web Clientプラグインにアクセスします。



2. [インフラストラクチャ]で、[サイトペアリングの追加*]をクリックします。

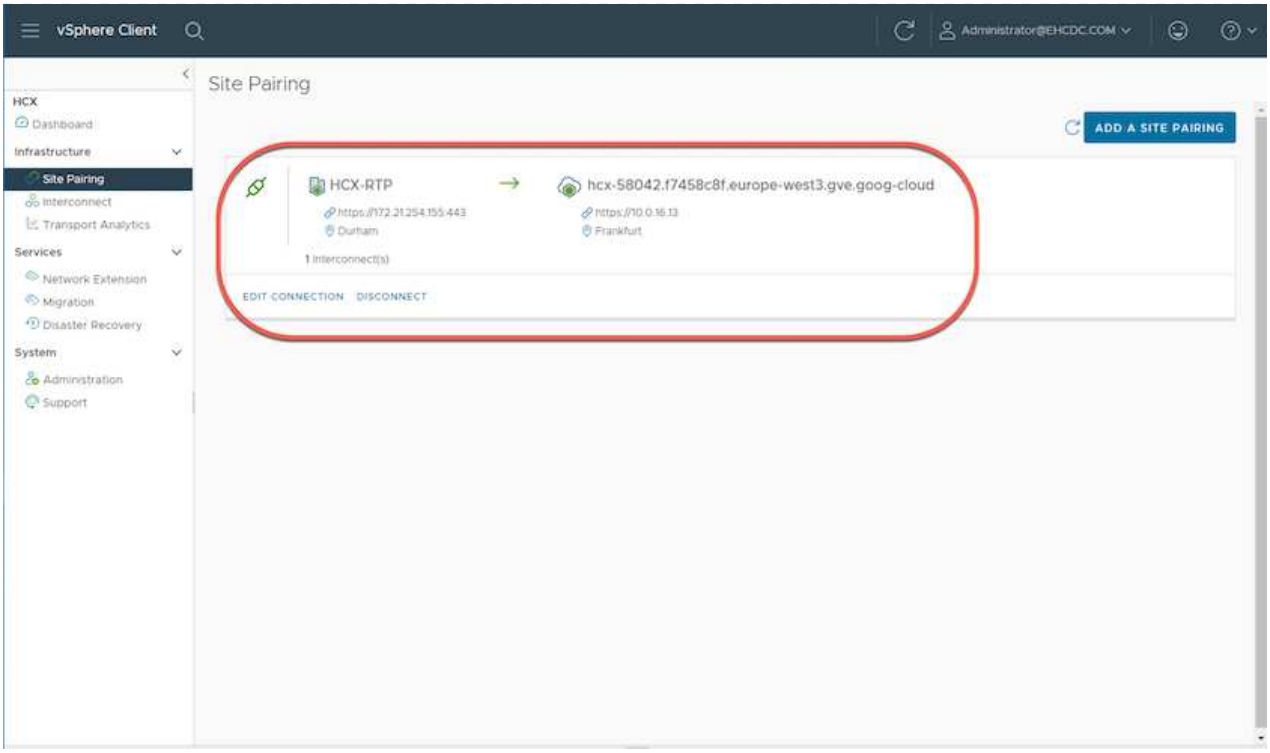
> プライベートクラウドにアクセスするためのCloud-Owner-Role権限を持つユーザのために、Google Cloud VMware Engine HCX Cloud ManagerのURLまたはIPアドレスとクレデンシャルを入力します。



3. [接続] をクリックします。

> VMware HCX Connectorは、ポート443経由でHCX Cloud Manager IPにルーティングできる必要があります。

4. ペアリングが作成されると、新しく構成されたサイトペアリングがHCXダッシュボードで使用できるようになります。

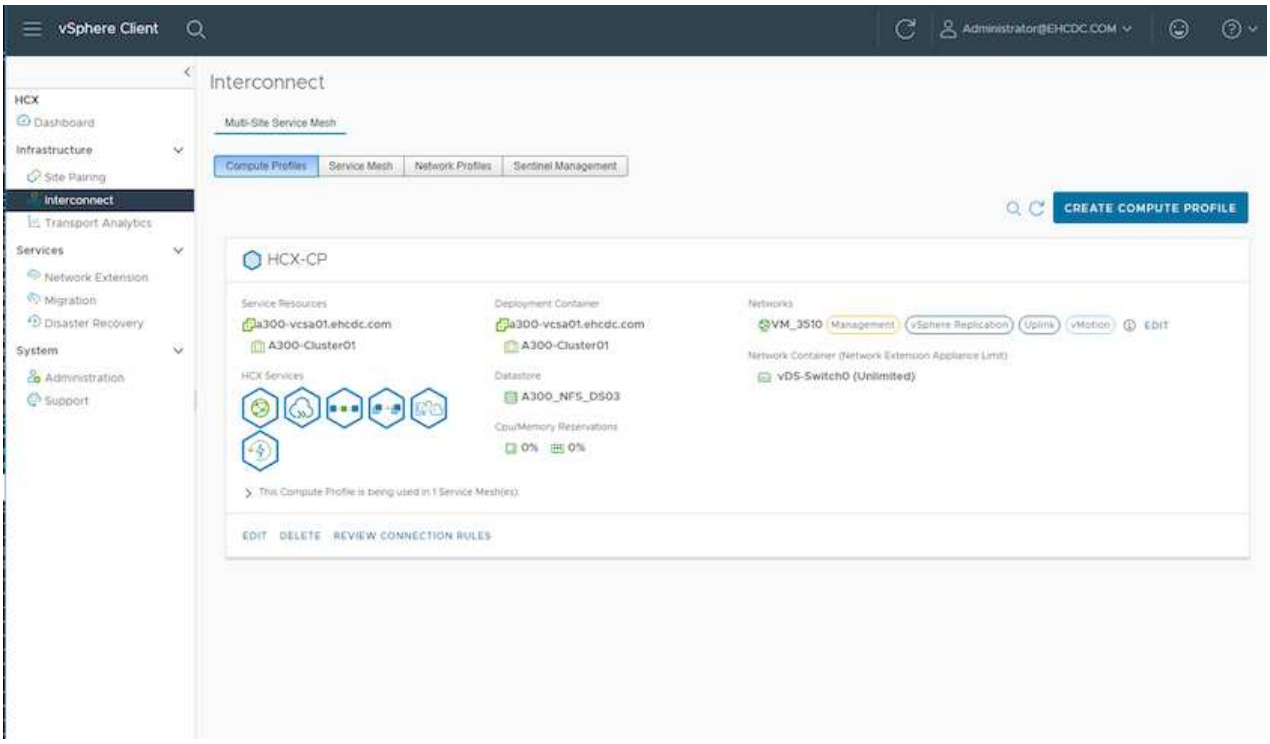

vSphere Client
Administrator@EHCDC.COM
HCX
Dashboard
Infrastructure
Site Pairing
Interconnect
Transport Analytics
Services
Network Extension
Migration
Disaster Recovery
System
Administration
Support
Site Pairing
ADD A SITE PAIRING
HCX-RTP
https://172.21.254.155:443
Durham
1 Interconnect(s)
hcx-58042.f7458c8f.europe-west3.gve.goog-cloud
https://10.0.16.13
Frankfurt
EDIT CONNECTION
DISCONNECT

手順**5**：ネットワークプロファイル、コンピューティングプロファイル、およびサービスメッシュを設定します

VMware HCX Interconnectサービスアプライアンスは、インターネットを介したレプリケーションおよびvMotionベースの移行機能を提供し、ターゲットサイトへのプライベート接続を提供します。インターコネクトは、暗号化、トラフィックエンジニアリング、VMモビリティを提供します。インターコネクトサービスアプライアンスを作成するには、次の手順を実行します。

1. インフラストラクチャー（Infrastructure）で、*インターコネクト（Interconnect）>マルチサイトサービスメッシュ（Multi-Site Service Mesh）>プロファイル計算（Compute Profiles）>コンピュートプロファイル作成（Create Compute Profile）*を選択

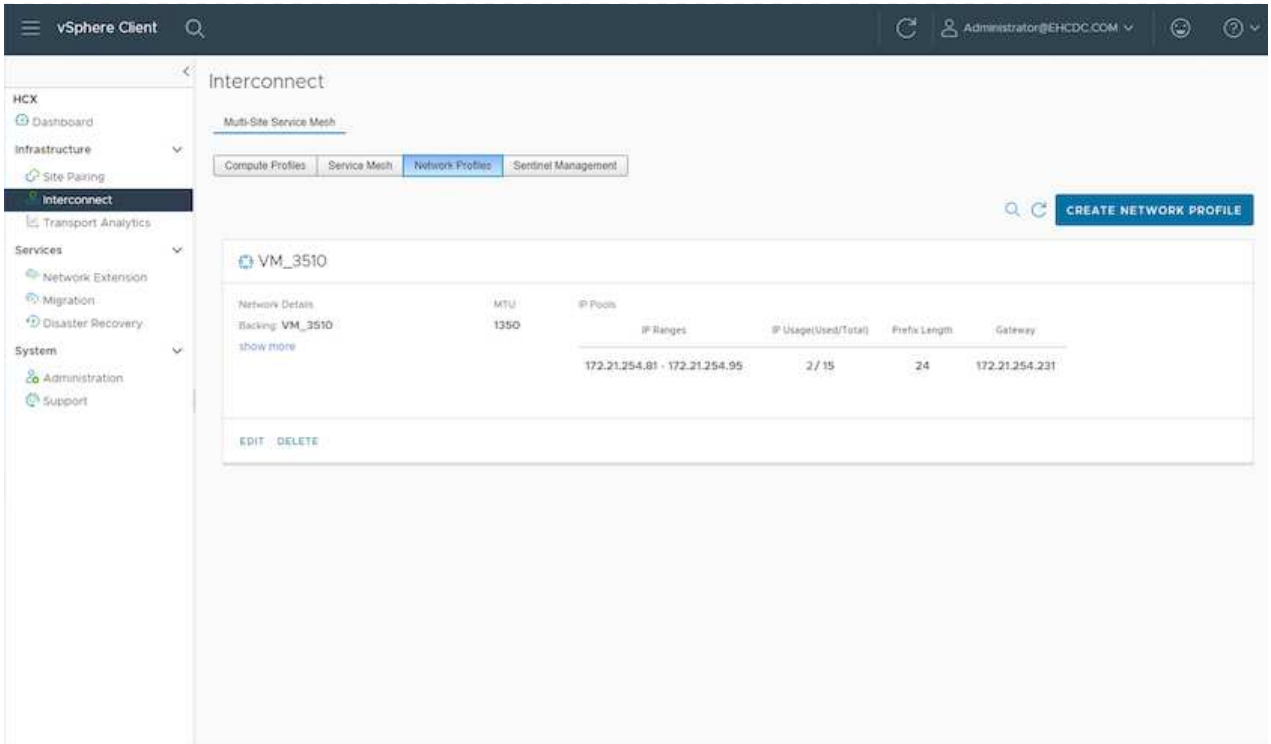
   コンピューティングプロファイルでは、導入されるアプライアンスや、HCXサービスからアクセスできるVMwareデータセンターの部分などの導入パラメータを定義します。



2. コンピューティングプロファイルを作成したら、*マルチサイトサービスメッシュ>ネットワークプロファイル>ネットワークプロファイルの作成*を選択して、ネットワークプロファイルを作成します。

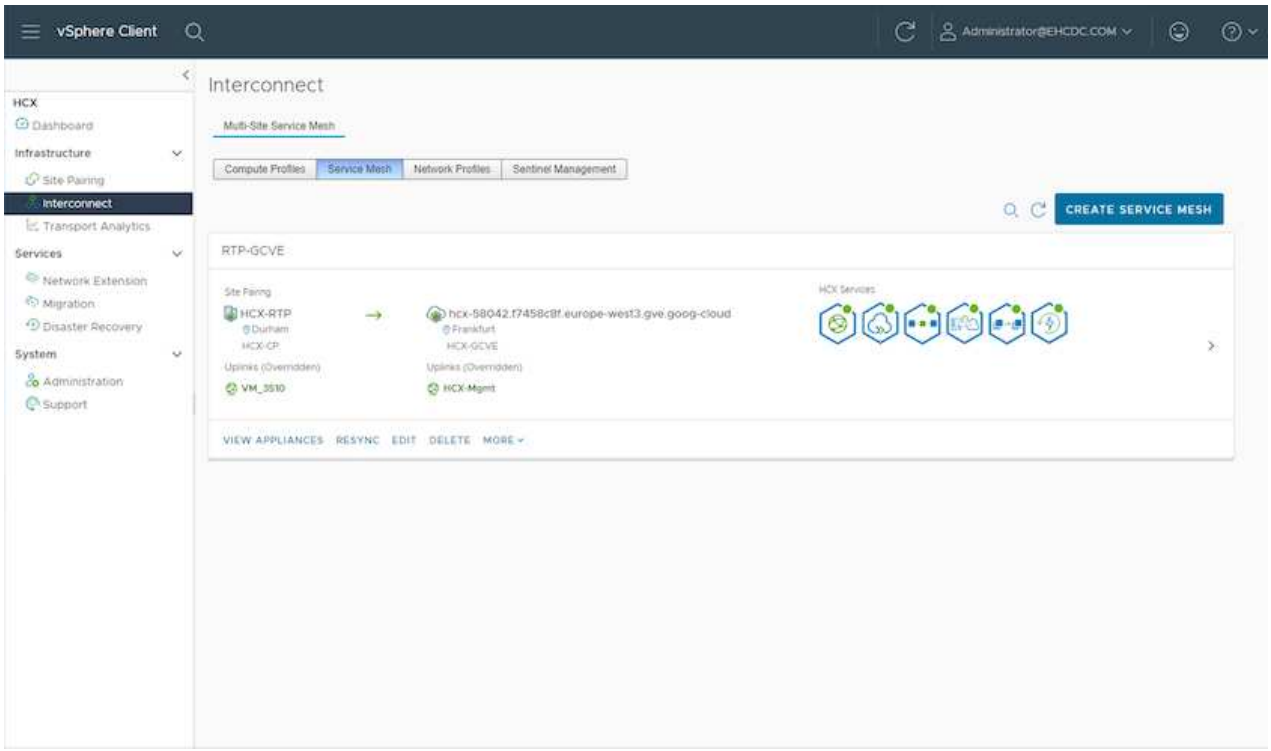
   ネットワークプロファイルは、HCXが仮想アプライアンスに使用するIPアドレスとネットワークの範囲を定義します。

   この手順には複数のIPアドレスが必要です。これらのIPアドレスは、管理ネットワークからインターコネクトアプライアンスに割り当てられます。

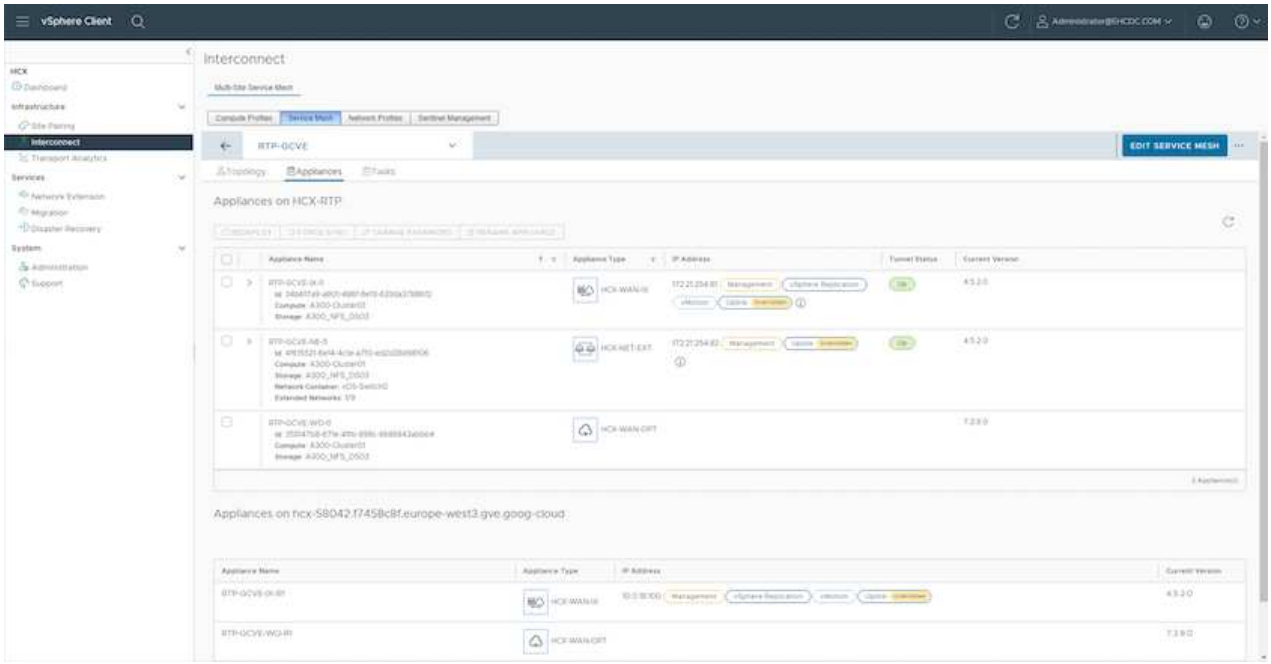


3. 現時点では、コンピューティングプロファイルとネットワークプロファイルは正常に作成されています。
4. [Interconnect（相互接続）]オプションの[* Service Mesh*（サービスメッシュ*）]タブを選択してサービスメッシュを作成し、オンプレミスサイトとGCVE SDDCサイトを選択します。
5. サービスメッシュは、ローカルとリモートのコンピューティングプロファイルとネットワークプロファイルのペアを指定します。

> このプロセスの一部として、セキュアなトランスポートファブリックを作成するために、ソースサイトとターゲットサイトの両方にHCXアプライアンスが展開され、自動的に設定されます。



6. これが設定の最後の手順です。導入が完了するまでに約30分かかります。サービスメッシュを設定すると、ワークロードVMを移行するためのIPsecトンネルが正常に作成され、環境の準備が整います。



手順**6**：ワークロードを移行する

さまざまなVMware HCX移行テクノロジを使用して、オンプレミスとGCVEのSDDC間でワークロードを双方向に移行できます。VMは、HCXバルク移行、HCX vMotion、HCXコールド移行、HCX Replication Assisted vMotion（HCX Enterprise Editionで利用可能）、HCX OS Assisted Migration（HCX Enterprise Editionで利用可能）などの複数の移行テクノロジーを使用して、VMware HCXでアクティブ化されたエンティティとの間で移動できます。

さまざまなHCX移行メカニズムの詳細については、を参照してください "VMware HCXの移行タイプ"。

HCX-IXアプライアンスは、Mobility Agentサービスを使用して、vMotion、コールド、およびReplication Assisted vMotion（RAV）の移行を実行します。

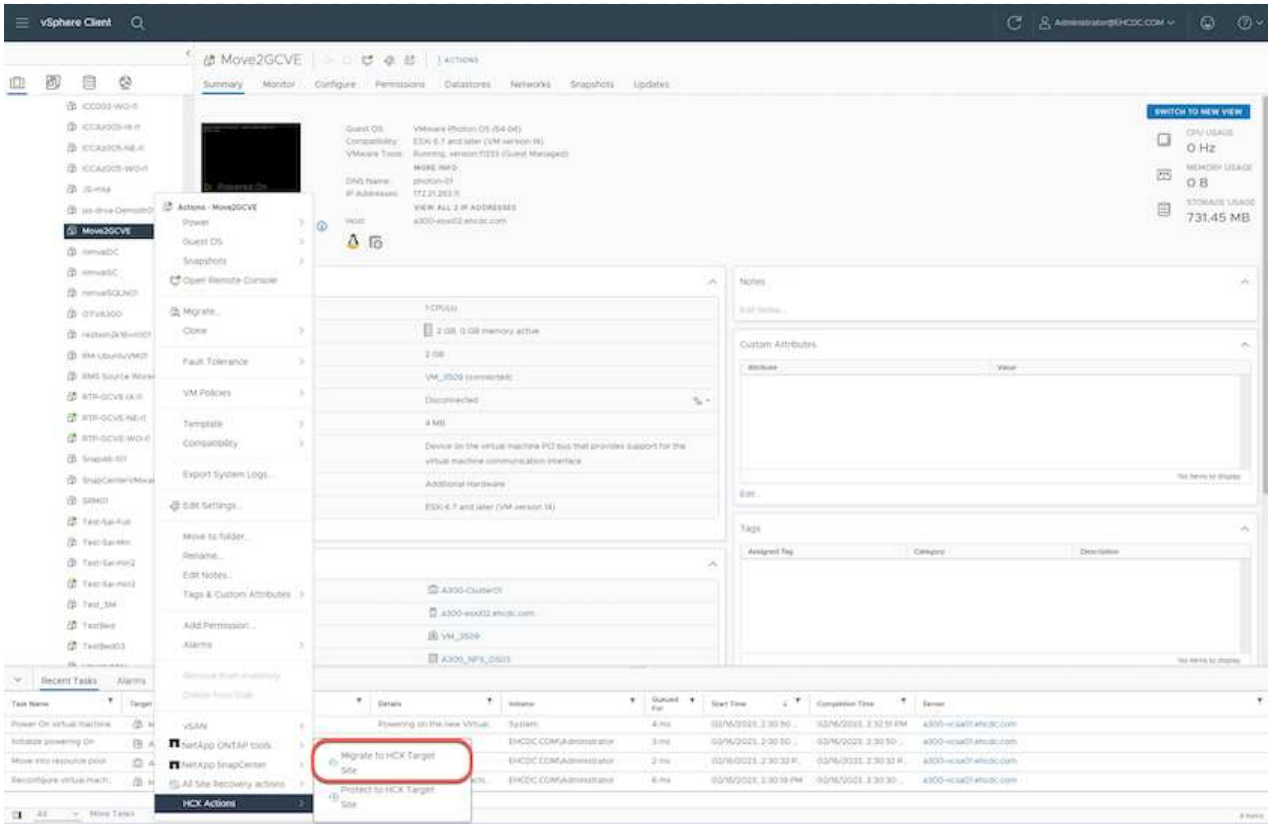
> HCX-IXアプライアンスは、Mobility AgentサービスをvCenter Serverのホストオブジェクトとして追加します。このオブジェクトに表示されるプロセッサ、メモリ、ストレージ、およびネットワークのリソースは、IXアプライアンスをホストする物理ハイパーバイザーでの実際の消費量を表していません。

- HCX vMotion *

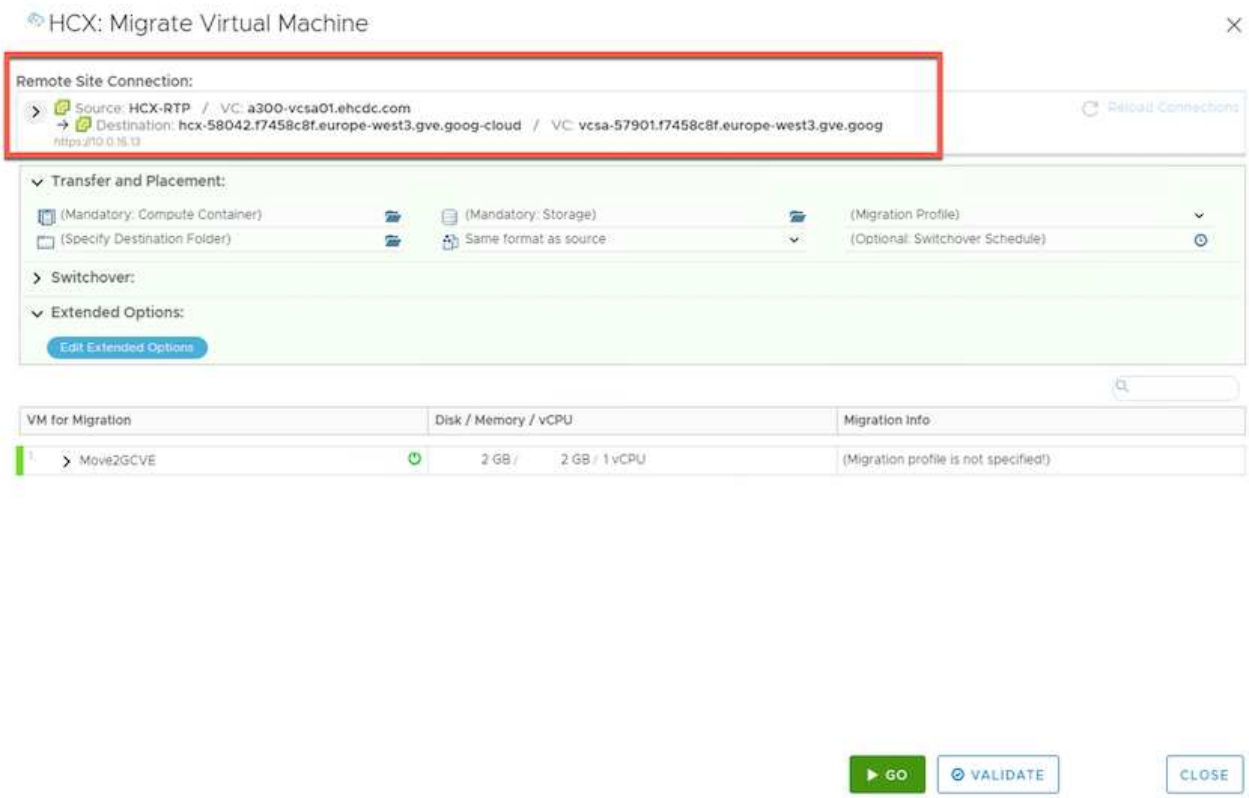
このセクションでは、HCX vMotionメカニズムについて説明します。この移行テクノロジは、VMware vMotionプロトコルを使用してVMをGCVEに移行します。vMotion移行オプションは、一度に1つのVMのVM状態を移行するために使用します。このマイグレーション方式では、サービスは中断されません。

> IPアドレスを変更せずにVMを移行するには、ネットワーク拡張を設定する必要があります（VMが接続されているポートグループの場合）。

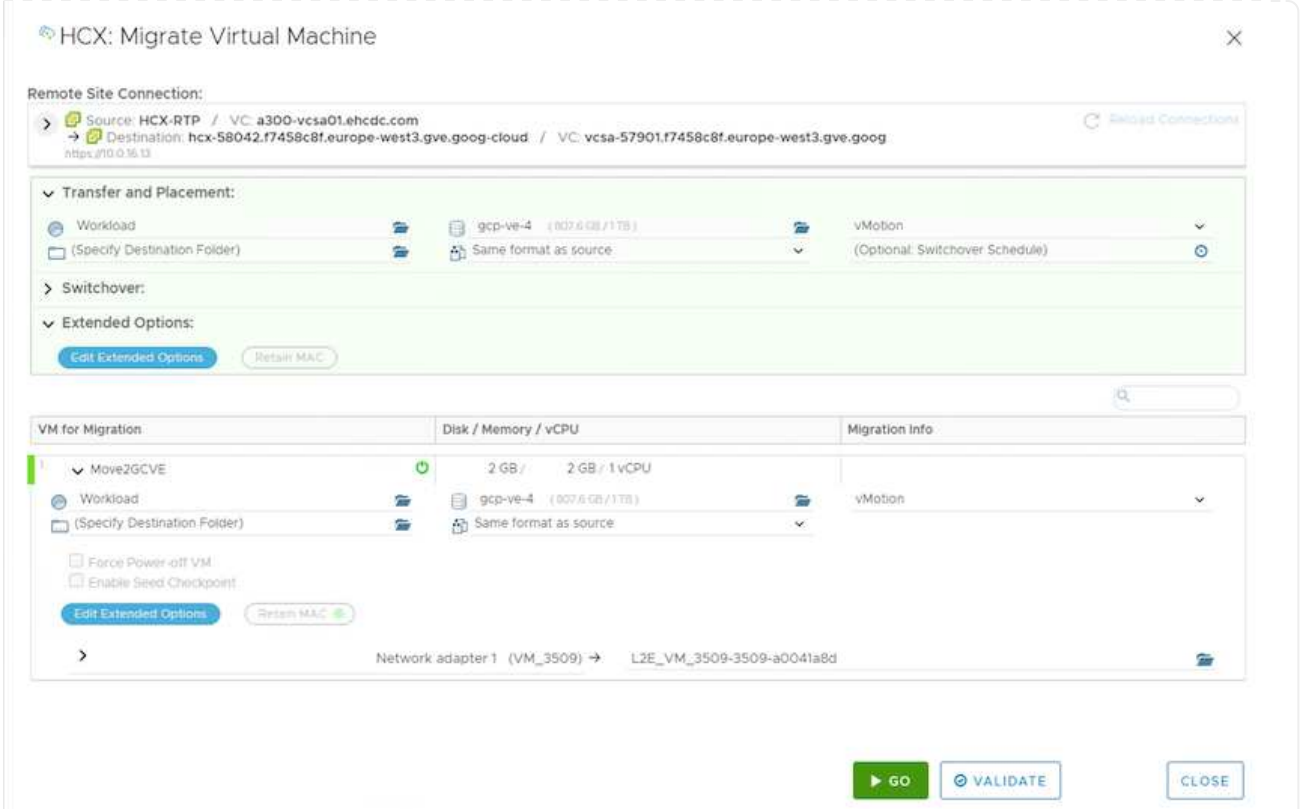
1. オンプレミスのvSphereクライアントから、Inventoryに移動し、移行するVMを右クリックして、HCX Actions > Migrate to HCX Target Siteを選択します。



2. 仮想マシンの移行ウィザードで、リモートサイト接続（ターゲットGCVE）を選択します。



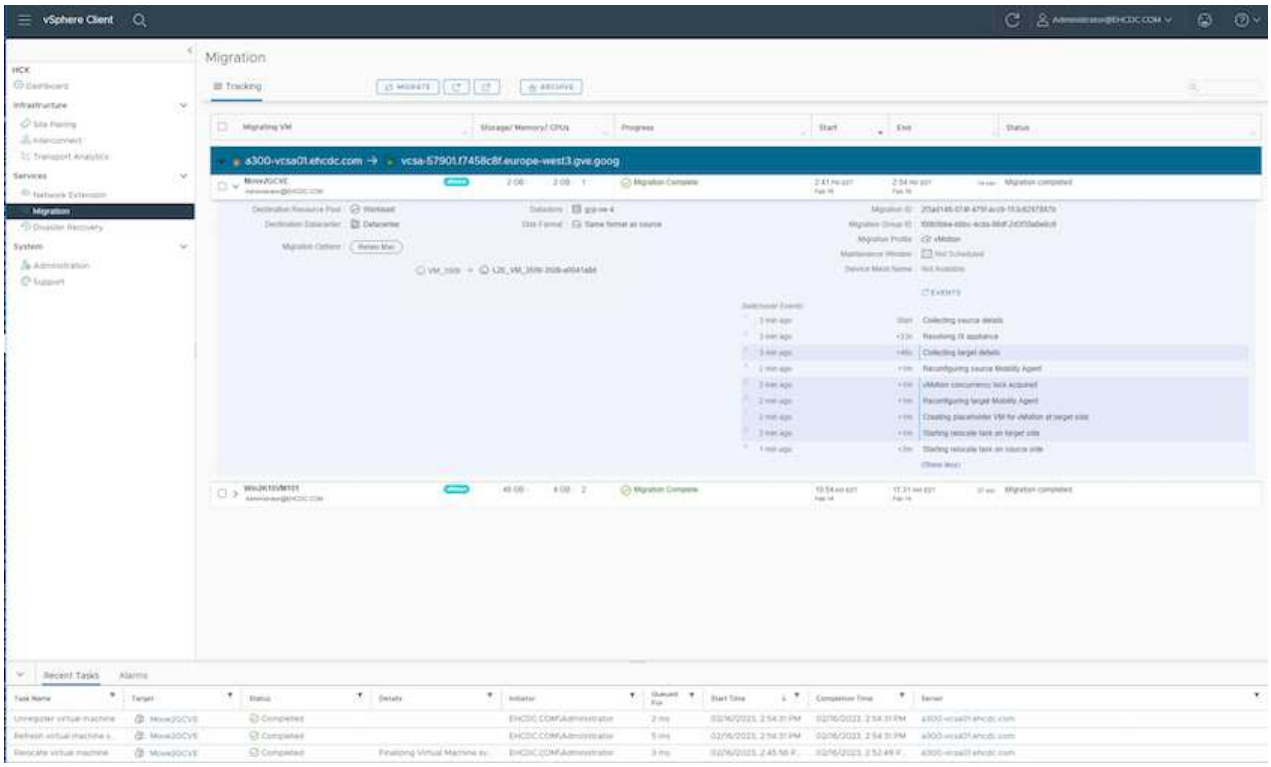
3. 必須フィールド（クラスタ、ストレージ、デスティネーションネットワーク）を更新し、検証をクリックします。



4. 検証チェックが完了したら、Goをクリックして移行を開始します。

> vMotionによる転送では、VMのアクティブメモリ、実行状態、IPアドレス、およびMACアドレスがキャプチャされます。HCX vMotionの要件と制限の詳細については、を参照してください "VMware HCX vMotionとコールドマイグレーションについて理解する"。

5. VMotionの進捗状況と完了は'HCX＞Migrationダッシュボードから監視できます



ターゲットのCVS NFSデータストアには、移行を処理するための十分なスペースが必要です。

まとめ

すべてのクラウドまたはハイブリッドクラウドをターゲットとしている場合でも、オンプレミスのあらゆるタイプ/ベンダーストレージに存在するデータを対象としている場合でも、Cloud Volume ServiceとHCXは、アプリケーションワークロードを展開および移行する優れたオプションを提供し、データ要件をアプリケーションレイヤにシームレスにすることでTCOを削減します。どのようなユースケースでも、クラウドのメリット、一貫したインフラ、オンプレミスと複数のクラウドにわたる運用、ワークロードの双方向の移動、エンタープライズクラスの容量とパフォーマンスを迅速に実現するには、Google Cloud VMware EngineとCloud Volume Serviceを選択してください。VMware vSphere Replication、VMware vMotion、Network File Copy（NFC；ネットワークファイルコピー）を使用してストレージの接続やVMの移行を行う場合と同じ手順を実行します。

重要なポイント

本ドキュメントの主な内容は次のとおりです。

- Google Cloud VMware Engine SDDCでクラウドボリュームサービスをデータストアとして使用できるようになりました。
- オンプレミスのデータストアからCloud Volume Serviceデータストアへのデータの移行は簡単です。
- 移行アクティビティ中の容量とパフォーマンスの要件に合わせて、Cloud Volume Serviceデータストアの拡張と縮小を簡単に行うことができます。

参考として、**Google**と**VMware**のビデオをご用意しています

Googleから

- "GCVEを使用してHCXコネクタを展開します"
- "GCVEを使用してHCX ServiceMeshを設定します"
- "HCXを使用するVMをGCVEに移行します"

VMwareを使用

- "GCVEのHCxコネクタ配置"
- "GCVEのHCx ServiceMesh設定"
- "HCxワークロードのGCVEへの移行"

追加情報の参照先

このドキュメントに記載されている情報の詳細については、次の Web サイトのリンクを参照してください。

- Google Cloud VMware Engineのドキュメント

  "https://cloud.google.com/vmware-engine/docs/overview"

- Cloud Volume Serviceのドキュメント

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes"

- VMware HCXユーザーガイド

  "https://docs.vmware.com/en/VMware-HCX/index.html"

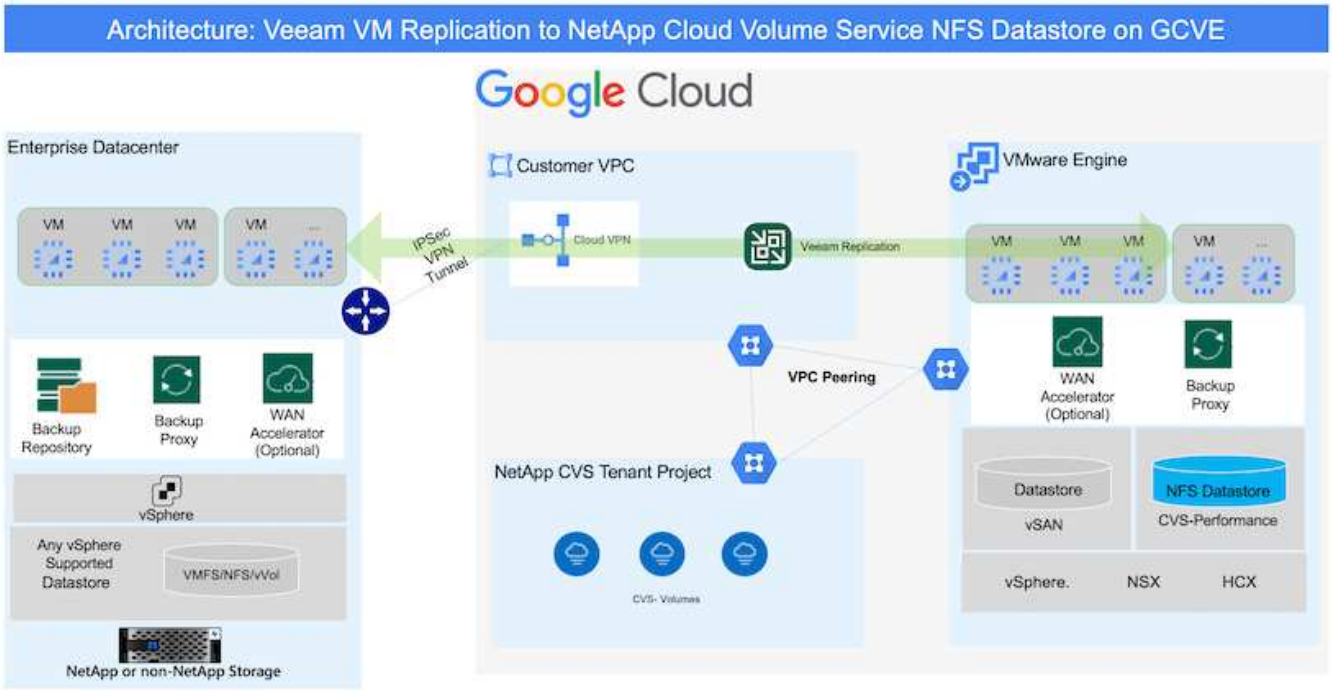
Veeamレプリケーション機能を使用した**Google Cloud VMware Engine**上の**NetApp**クラウドボリュームサービス**NFS**データストアへの**VM**の移行

概要

執筆者：ネットアップSuresh Thoppay

VMware vSphereで実行されているVMワークロードは、Veeam Replication機能を使用してGoogle Cloud VMware Engine（GCVE）に移行できます。

このドキュメントでは、NetApp Cloud Volume Service、Veeam、Google Cloud VMware Engine（GCVE）を使用してVM移行をセットアップして実行するための、ステップバイステップ形式のアプローチを紹介します。



前提条件

このドキュメントでは、既存のvSphereサーバからGoogle Cloud VMware Engineへのネットワーク接続を確立するために、Google Cloud VPN、Cloud Interconnect、またはその他のネットワークオプションが用意されていることを前提としています。

> オンプレミスのデータセンターをGoogle Cloudに接続する方法は複数ありますが、この方法では、このドキュメントの特定のワークフローの概要を説明することはできません。
> を参照してください "Google Cloudのドキュメント" オンプレミスからGoogleへの適切な接続方法

移行解決策の導入

解決策 の導入の概要

1. NetAppクラウドボリュームサービスのNFSデータストアがGCVE vCenterにマウントされていることを確認します。
2. Veeam Backup Recoveryが既存のVMware vSphere環境に導入されていることを確認します
3. レプリケーションジョブを作成して、Google Cloud VMware Engineインスタンスへの仮想マシンのレプリケーションを開始します。
4. Veeamレプリケーションジョブのフェイルオーバーを実行します。
5. Veeamで永続的フェイルオーバーを実行

展開の詳細

NetAppクラウドボリュームサービスの**NFS**データストアが**GCVE vCenter**にマウントされていることを確認します

GCVE vCenterにログインし、十分なスペースがあるNFSデータストアが使用可能であることを確認します。

そうでない場合は、を参照してください "NetApp CVSをNFSデータストアとしてGCVEにマウント"

Veeam Backup Recoveryが既存の**VMware vSphere**環境に導入されていることを確認します

を参照してください "Veeamレプリケーションのコンポーネント" 必要なコンポーネントをインストールするためのドキュメント。

レプリケーションジョブを作成して、**Google Cloud VMware Engine**インスタンスへの仮想マシンのレプリケーションを開始します。

オンプレミスのvCenterとGCVEのvCenterをVeeamに登録する必要があります。 "vSphere VMレプリケーションジョブをセットアップします"
ここでは、その方法を説明するビデオを紹介します
"レプリケーションジョブを設定します"。

> レプリカVMは、ソースVMとは異なるIPを持つことができ、異なるポートグループに接続することもできます。詳細については、上記のビデオを確認してください。

Veeamレプリケーションジョブのフェイルオーバーを実行します

VMを移行するには、を実行します "フェールオーバーを実行します"

Veeamで永続的フェイルオーバーを実行

GCVEを新しいソース環境として扱うには、を実行します "永続的フェイルオーバー"

この解決策 の利点

- 既存のVeeamバックアップインフラを移行に利用できます。
- Veeam Replicationを使用すると、ターゲットサイトのVM IPアドレスを変更できます。
- Veeam以外でレプリケートされた既存データを再マッピングする機能（BlueXPでレプリケートされたデータと同様）
- ターゲットサイトで異なるネットワークポートグループを指定できます。
- 電源をオンにするVMの順序を指定できます。
- VMware Change Block Trackingを使用して、WAN経由で送信するデータ量を最小限に抑えます。
- レプリケーションのプリスクリプトとポストスクリプトを実行する機能。
- スナップショットのプリスクリプトとポストスクリプトを実行する機能。

リージョンの可用性–Google Cloud Platform（GCP）向けのNFSデータストア補足機能

NetApp Cloud Volume Serviceでは、GCVE用の補完的NFSデータストアがサポートされます。

> GCVE NFSデータストアに使用できるのはCVS-Performanceボリュームのみです。
> 使用可能な場所については、を参照してください "グローバルリージョンマップ"

Google Cloud VMware Engineは次の場所で利用できます

asia-northeast1 > v-zone-a > VE Placement Group 1
asia-northeast1 > v-zone-a > VE Placement Group 2
asia-south1 > v-zone-a > VE Placement Group 2
asia-south1 > v-zone-a > VE Placement Group 1
asia-southeast1 > v-zone-a > VE Placement Group 1
asia-southeast1 > v-zone-a > VE Placement Group 2
australia-southeast1 > v-zone-b > VE Placement Group 1
australia-southeast1 > v-zone-a > VE Placement Group 1
australia-southeast1 > v-zone-b > VE Placement Group 2
australia-southeast1 > v-zone-a > VE Placement Group 2
europe-west2 > v-zone-a > VE Placement Group 2
europe-west2 > v-zone-a > VE Placement Group 1
europe-west3 > v-zone-b > VE Placement Group 2
europe-west3 > v-zone-a > VE Placement Group 3
europe-west3 > v-zone-a > VE Placement Group 4
europe-west3 > v-zone-b > VE Placement Group 1
europe-west3 > v-zone-a > VE Placement Group 2
europe-west3 > v-zone-a > VE Placement Group 1
europe-west4 > v-zone-a > VE Placement Group 2
europe-west4 > v-zone-a > VE Placement Group 1
europe-west6 > v-zone-a > VE Placement Group 1
europe-west8 > v-zone-a > VE Placement Group 1
northamerica-northeast1 > v-zone-a > VE Placement Group 1
northamerica-northeast1 > v-zone-a > VE Placement Group 2
northamerica-northeast2 > v-zone-a > VE Placement Group 2
northamerica-northeast2 > v-zone-a > VE Placement Group 1
southamerica-east1 > v-zone-a > VE Placement Group 1
southamerica-east1 > v-zone-a > VE Placement Group 2
us-central1 > v-zone-a > VE Placement Group 2
us-central1 > v-zone-a > VE Placement Group 5
us-central1 > v-zone-a > VE Placement Group 1
us-central1 > v-zone-a > VE Placement Group 3
us-east4 > v-zone-a > VE Placement Group 5
us-east4 > v-zone-a > VE Placement Group 10
us-east4 > v-zone-a > VE Placement Group 6
us-east4 > v-zone-a > VE Placement Group 3
us-east4 > v-zone-b > VE Placement Group 5
us-east4 > v-zone-a > VE Placement Group 1
us-east4 > v-zone-b > VE Placement Group 1
us-east4 > v-zone-a > VE Placement Group 4
us-east4 > v-zone-b > VE Placement Group 6
us-east4 > v-zone-a > VE Placement Group 2
us-west2 > v-zone-a > VE Placement Group 3
us-west2 > v-zone-a > VE Placement Group 4
us-west2 > v-zone-a > VE Placement Group 5
us-west2 > v-zone-a > VE Placement Group 2
us-west2 > v-zone-a > VE Placement Group 1
us-west2 > v-zone-a > VE Placement Group 6

レイテンシを最小限に抑えるには、ボリュームをマウントするNetApp CVSボリュームとGCVEを同じアベイラビリティゾーンに配置する必要があります。
GoogleおよびNetApp 解決策 アーキテクトと連携して、可用性とTCOを最適化します。

セキュリティの概要- Google CloudでのNetApp Cloud Volumes Service （CVS

TR-4918：『Security Overview - NetApp Cloud Volumes Service in Google Cloud』

ネットアップ、Oliver Krause、Justin Parisi

文書の範囲

特にストレージ管理者の管理権限がないクラウドでは、クラウドプロバイダが提供するサービスにデータを信頼することが何よりも重要です。本ドキュメントでは、ネットアップが提供するセキュリティソリューションの概要について説明します "Cloud Volumes Service はGoogle Cloudで提供されます"。

対象読者

このドキュメントの対象読者には、次の役割が含まれますが、これらに限定されません。

- クラウドプロバイダ
- ストレージ管理者
- ストレージアーキテクト
- フィールド用リソース
- ビジネス上の意思決定者

このテクニカルレポートの内容について不明な点がある場合は、を参照してください "「お問い合わせください。」"

略語	定義（ **Definition** ）
CVS -ソフトウェア	Cloud Volumes Service 、サービスタイプCVS
CVS - パフォーマンス	Cloud Volume Service、サービスタイプCVS -パフォーマンス
PSA	

Google CloudのCloud Volumes Service でデータを保護する方法

Google CloudのCloud Volumes Service は、さまざまな方法でデータをネイティブに保護します。

セキュアなアーキテクチャとテナンシーモデル

Cloud Volumes Service は、異なるエンドポイント間でサービス管理（コントロールプレーン）とデータアクセス（データプレーン）をセグメント化することで、Google Cloudのセキュアなアーキテクチャを提供します。これにより、どちらも他方に影響を与えることはありません（を参照） "「Cloud Volumes Service アー

キテクチャ」"）。Googleを使用している "プライベートサービスへのアクセス" （PSA）サービスを提供するためのフレームワーク。このフレームワークでは、ネットアップが提供、運用するサービスプロデューサーと、Cloud Volumes Service ファイル共有にアクセスするクライアントをホストする顧客プロジェクトのVirtual Private Cloud（VPC；仮想プライベートクラウド）であるサービスコンシューマが区別されます。

このアーキテクチャでは、テナント（セクションを参照） "「テナンシーモデル」"）は、ユーザーが明示的に接続していない限り、互いに完全に分離されたGoogle Cloudプロジェクトとして定義されます。テナントを使用すると、Cloud Volumes Service ボリュームプラットフォームを使用して、データボリューム、外部ネームサービス、その他の重要な解決策 を他のテナントから完全に分離できます。Cloud Volumes Service プラットフォームはVPCピアリングを通じて接続されるため、その分離環境 も接続されます。共有VPCを使用して、複数のプロジェクト間でのCloud Volumes Service ボリュームの共有を有効にすることができます（を参照） "「共有VPC」"）。SMB共有およびNFSエクスポートにアクセス制御を適用することで、データセットを表示または変更できるユーザまたはユーザを制限できます。

コントロールプレーンの強力なアイデンティティ管理

Cloud Volumes Service 構成が行われるコントロールプレーンでは、を使用してアイデンティティ管理を管理します "IDアクセス管理（IAM）"。IAMは、Google Cloudプロジェクトインスタンスに対する認証（ログイン）と許可（権限）を制御できる標準サービスです。すべての設定は、TLS 1.2暗号化を使用したセキュアなHTTPS転送を介してCloud Volumes Service APIで実行され、セキュリティを強化するためにJWTトークンを使用して認証が実行されます。Cloud Volumes Service 用のGoogleコンソールUIは、ユーザ入力をCloud Volumes Service API呼び出しに変換します。

セキュリティ強化-攻撃面の制限

効果的なセキュリティの一部は、サービスで使用できる攻撃対象の数を制限することです。攻撃対象には、保管データ、転送中転送、ログイン、データセット自体など、さまざまなものが含まれます。

マネージドサービスを使用すると、本質的に設計上の攻撃対象の一部が削除されます。の説明に従って、インフラストラクチャ管理を行います ""サービスオペレーション"" は専用チームによって処理され、人間が実際に構成に触れる回数を減らすために自動化されます。これにより、意図的なエラーや意図しないエラーの数を減らすことができます。必要なサービスだけが互いにアクセスできるように、ネットワークは遮断されます。暗号化はデータストレージに組み込まれており、Cloud Volumes Service 管理者はデータプレーンだけにセキュリティ上の注意を払う必要があります。APIインターフェイスの背後にあるほとんどの管理を隠すことで、攻撃対象を制限することでセキュリティを実現します。

ゼロトラストモデル

ITセキュリティの考え方は、これまでは信頼されていましたが、その信頼性は確認されており、脅威を軽減するために外部メカニズム（ファイアウォールや侵入検知システムなど）のみに依存していることが明示されてきました。しかし、攻撃や侵害は、フィッシング、ソーシャルエンジニアリング、内部の脅威など、ネットワークに侵入したり破壊的になったりするための検証を提供する方法によって、環境内での検証をバイパスするように進化しています。

ゼロ・トラストは、セキュリティの新しい方法論になりました。現在のテーマは「すべてを検証しながらは何も信頼しない」です。 したがって、デフォルトではアクセスは許可されません。この問題は、標準ファイアウォールや侵入検知システム（IDS）など、さまざまな方法で実施されています。また、次の方法も適用されています。

- 強力な認証方法（AESで暗号化されたKerberosトークンやJWTトークンなど）
- 単一の強力なアイデンティティソース（Windows Active Directory、Lightweight Directory Access Protocol（LDAP）、Google IAMなど）

- ネットワークのセグメント化とセキュアマルチテナンシー（デフォルトではテナントのみにアクセス可能）
- 最小限の権限付きアクセスポリシーで詳細なアクセス制御を実現します
- デジタル監査と紙の記録を使用した、信頼できる専任管理者の限定リスト

Google Cloudで実行されているCloud Volumes Service は、「何も信用しない、すべてを検証する」というスタンスを実装することで、ゼロトラストモデルに準拠しています。

暗号化

保存データを暗号化する（を参照） "「保存データの暗号化」"）転送には、NetApp Volume Encryption（NVE）および転送中のXTS-AES-256暗号を使用します "「SMB暗号化」" またはNFS Kerberos 5pをサポート。リージョン間レプリケーションの転送はTLS 1.2暗号化で保護されているので、安心して実行できます（を参照） "「リージョン間レプリケーション」"）。さらに、Googleネットワークは暗号化された通信も提供します（を参照） "「転送中のデータ暗号化」"）を使用してください。転送暗号化の詳細については、を参照してください "「Google Cloudネットワーク」"。

データ保護とバックアップ

セキュリティとは、攻撃の防御だけではありません。また、攻撃が発生した場合や発生した場合にどのように復旧するかについても説明します。この戦略には、データ保護とバックアップが含まれます。Cloud Volumes Service には、システム停止時に他のリージョンにレプリケートする方法が用意されています（を参照） "「リージョン間レプリケーション」"）またはデータセットがランサムウェア攻撃の影響を受ける場合。を使用して、Cloud Volumes Service インスタンス以外の場所へのデータの非同期バックアップを実行することもできます "Cloud Volumes Service バックアップ"。定期的なバックアップにより、セキュリティイベントの緩和にかかる時間を短縮し、管理者にとってコストと不安を軽減できます。

業界をリードする**Snapshot**コピーでランサムウェアを迅速に軽減

Cloud Volumes Service では、データ保護とバックアップに加えて、書き換え不可のSnapshotコピーもサポートしています（を参照） "「不変のSnapshotコピー」"）ランサムウェア攻撃からのリカバリを可能にするボリューム（を参照） "「サービスオペレーション」"）問題 を検出してから数秒以内に、システム停止を最小限に抑えることができます。リカバリ時間と影響はSnapshotスケジュールによって異なりますが、ランサムウェア攻撃ではわずか1時間の差分しか提供しないSnapshotコピーを作成できます。Snapshotコピーは、パフォーマンスや容量使用率にほとんど影響を与えず、データセットを保護するリスクが低く、効果も高くなります。

セキュリティに関する考慮事項と攻撃対象

データのセキュリティを確保する方法を理解する最初のステップは、リスクと潜在的な攻撃対象を特定することです。

これには、次のものが含まれます（ただし、これらに限定されません）。

- 管理とログイン
- 保存データ
- 転送中のデータ
- ネットワークとファイアウォール
- ランサムウェア、マルウェア、ウイルス

攻撃の対象となる面を理解することで、環境のセキュリティを強化できます。Google CloudのCloud Volumes Service は、これらのトピックの多くをすでに考慮しており、管理者の介入なしにデフォルトでセキュリティ機能を実装しています。

セキュアなログインの確保

重要なインフラコンポーネントを保護するには、承認されたユーザのみがログインして環境を管理できるようにすることが不可欠です。不良なアクターが管理資格情報に違反した場合、そのアクターは城へのキーを持ち、必要な操作（構成の変更、ボリュームとバックアップの削除、バックドアの作成、スナップショットスケジュールの無効化）を実行できます。

Cloud Volumes Service for Google Cloudを使用すると、ストレージサービス（StaaS）の難読化により、不正な管理ログインを防止できます。Cloud Volumes Service はクラウドプロバイダによって完全に管理されており、外部からのログインはできません。セットアップと設定の処理はすべて完全に自動化されているため、ごくまれな状況を除いて、人間の管理者がシステムを操作する必要はありません。

ログインが必要な場合、Google CloudのCloud Volumes Service は、システムにログインするためのアクセス権を持つ信頼できる管理者のごく短いリストを保持することで、ログインを保護します。このゲートキーピングは、アクセス権を持つ潜在的な不正アクターの数を減らすのに役立ちます。さらに、Google Cloudネットワークは、ネットワークセキュリティの層の背後にあるシステムを隠し、外部に必要なものだけを公開します。Google CloudのCloud Volumes Service アーキテクチャについては、を参照してください "「Cloud Volumes Service アーキテクチャ」"

クラスタの管理とアップグレード

潜在的なセキュリティリスクを持つ2つの領域には、クラスタ管理（不正なアクターに管理者アクセス権がある場合に発生する動作）とアップグレード（ソフトウェアイメージが侵害された場合に発生する動作）があります。

ストレージ管理の保護

ストレージサービスとして提供されるため、クラウドデータセンターの外部にあるエンドユーザがアクセスするリスクが軽減され、管理者のリスクを高めることができます。代わりに、顧客がデータアクセスプレーンを対象とした唯一の設定が行われます。各テナントは固有のボリュームを管理し、テナントが他のCloud Volumes Service インスタンスにアクセスすることはできません。このサービスは自動化によって管理され、セクションで説明するプロセスを通じて、信頼できる管理者のごく一部にシステムへのアクセス権が付与されます "「サービスオペレーション」"

CVS -パフォーマンスサービスタイプでは、リージョンに障害が発生した場合に別のリージョンにデータを保護するオプションとして、リージョン間のレプリケーションを提供できます。このような場合は、Cloud Volumes Service を影響を受けない領域にフェイルオーバーしてデータアクセスを維持できます。

サービスのアップグレード

更新プログラムは、脆弱なシステムの保護に役立ちます。各アップデートには、セキュリティの強化機能とバグ修正が含まれており、攻撃対象となる面を最小限に抑えるソフトウェアの更新は、中央リポジトリからダウンロードされ、更新が許可される前に検証されて、公式イメージが使用されていること、およびアップグレードが不正なアクターによって侵害されていないことを確認します。

Cloud Volumes Service を使用すると、クラウドプロバイダチームが更新を処理できるため、管理者チームは、プロセスの自動化と完全なテストに精通したエキスパートが設定とアップグレードに精通することで、リスクの危険性を回避できます。アップグレードは無停止で実行され、Cloud Volumes Service は全体的な最善の結果を得るために最新の更新を維持します。

これらのサービスのアップグレードを実行する管理者チームの詳細については、を参照してください "「サービスオペレーション」"

保存データを保護

保管データの暗号化は、ディスクが盗難、返却、転用された場合に機密データを保護するために重要です。Cloud Volumes Service のデータは、ソフトウェアベースの暗号化を使用して保存データを保護します。

- Googleで生成されたキーは、CVS-SWに使用されます。
- CVSパフォーマンスの場合、ボリューム単位のキーはCloud Volumes Service に組み込まれたキー管理ツールに格納されます。このキー管理ツールでは、NetApp ONTAP CryptoModを使用してAES-256暗号化キーが生成されます。CryptoModは、CMVP FIPS 140-2の検証済みモジュールのリストに表示されています。を参照してください "FIPS 140-2認定番号4144"。

2021年11月より、CVSパフォーマンス向けにプレビューによる顧客管理暗号化（CMEK）機能が提供されました。この機能を使用すると、ボリュームごとのキーを、Google Key Management Service（KMS）でホストされているプロジェクトごとのリージョンごとのマスターキーで暗号化できます。KMSを使用すると、外部キー管理ツールを接続できます。

CVS -パフォーマンス用のKMSの設定方法については、 "Cloud Volumes Service のドキュメントを参照してください"。

アーキテクチャの詳細については、を参照してください "「Cloud Volumes Service アーキテクチャ」"

転送中のデータを保護

保存データを保護するだけでなく、Cloud Volumes Service インスタンスとクライアントまたはレプリケーションターゲットの間で転送中のデータも保護する必要があります。Cloud Volumes Service では、Kerberosを使用したSMB暗号化、パケットの署名と封印、データ転送のエンドツーエンド暗号化に使用するNFS Kerberos 5pなどの暗号化方式を使用して、NASプロトコルで転送中のデータを暗号化できます。

Cloud Volumes Service ボリュームのレプリケーションにはTLS 1.2が使用され、AES-GCM暗号化方式を利用できます。

TelnetやNDMPなどのセキュアでないインフライトプロトコルのほとんどは、デフォルトで無効になっています。ただし、DNSはCloud Volumes Service によって暗号化されないため（DNSセキュリティはサポートされません）、可能な場合は外部ネットワーク暗号化を使用して暗号化する必要があります。を参照してください "「転送中のデータ暗号化」" 転送中のデータの保護に関する詳細については、を参照してください。

NASプロトコルの暗号化については、を参照してください "「NASプロトコル」。"

NAS権限のユーザとグループ

クラウドでデータを保護するには、適切なユーザ認証とグループ認証が必要になります。この場合、データにアクセスするユーザは環境内の実ユーザとして検証され、グループには有効なユーザが含まれます。これらのユーザとグループは、初回の共有アクセスとエクスポートアクセスに加え、ストレージシステム内のファイルとフォルダの権限検証も提供します。

Cloud Volumes Service では、SMB共有およびWindows形式の権限に対して、Active Directoryベースの標準のWindowsユーザ認証およびグループ認証を使用します。このサービスでは、NFSエクスポート、NFSv4 ID検証、Kerberos認証、NFSv4 ACL用のLDAPなど、UNIXユーザおよびグループのUNIX IDプロバイダも利用できます。

現在のところ、Cloud Volumes Service for LDAP機能ではActive Directory LDAPのみがサポートされています。

ランサムウェア、マルウェア、ウィルスの検出、防止、および軽減

ランサムウェア、マルウェア、ウィルスは管理者にとって常に脅威であり、これらの脅威の検出、防止、および軽減は、エンタープライズ組織にとって常に最重要課題です。重要なデータセットでランサムウェアが1回発生すると、数百万ドルのコストがかかる可能性があるため、リスクを最小限に抑えるために何ができるかを実行することが有益です。

Cloud Volumes Service には、現在、アンチウイルス保護やなどのネイティブの検出や防止対策は含まれていませんが "ランサムウェアの自動検出"では、定期的なSnapshotスケジュールを有効にすることで、ランサムウェアのイベントから迅速にリカバリする方法がいくつかあります。Snapshotコピーは変更不可で、ファイルシステム内の変更されたブロックへの読み取り専用ポインタであり、ほぼ瞬時に作成されます。パフォーマンスへの影響は最小限で、データが変更または削除された場合にのみスペースを消費します。Snapshotコピーのスケジュールは、許容されるRecovery Point Objective（RPO；目標復旧時点）やRecovery Time Objective（RTO；目標復旧時間）に合わせて設定できます。また、ボリュームあたり最大1、024個のSnapshotコピーを保持できます。

Cloud Volumes Service では、Snapshotのサポートは追加料金なしで利用でき（Snapshotコピーによって保持される変更されたブロックやデータのストレージ料金を除く）、ランサムウェア攻撃が発生した場合には、攻撃が発生する前にSnapshotコピーにロールバックするために使用できます。Snapshotのリストアは完了までに数秒しかかかりませんが、リストア完了後は通常どおりデータを提供できます。詳細については、を参照してください "『NetApp解決策 for Ransomware』"。

ランサムウェアによるビジネスへの影響を回避するには、次のようなマルチレイヤアプローチが必要です。

- エンドポイント保護
- ネットワークファイアウォールによる外部の脅威からの保護
- データの異常を検出します
- 重要なデータセットの複数のバックアップ（オンサイトおよびオフサイト）
- バックアップの定期的なリストアテスト
- 変更不可の読み取り専用NetApp Snapshotコピー
- 重要なインフラに対する多要素認証
- システムログインのセキュリティ監査

このリストは、完全なものではありませんが、ランサムウェア攻撃の可能性を扱う際の青写真としては適しています。Google CloudのCloud Volumes Service では、ランサムウェアのイベントを保護してその影響を軽減する方法を複数提供しています。

変更不可の**Snapshot**コピー

Cloud Volumes Service は、データを削除した場合や、ランサムウェア攻撃によってボリューム全体が影響を受けた場合に、カスタマイズ可能なスケジュールで作成された書き換え不可の読み取り専用Snapshotコピーを標準で提供します。以前の正常なSnapshotコピーへのSnapshotのリストアは高速で、Snapshotスケジュールの保持期間とRTO/RPOに基づいてデータ損失を最小限に抑えます。Snapshotテクノロジによるパフォーマンスへの影響はごくわずかです。

Cloud Volumes Service のSnapshotコピーは読み取り専用であるため、ランサムウェアが大量に発生してデー

タセットにデータが拡散し、Snapshotコピーがランサムウェアによって感染した場合を除き、ランサムウェアに感染することはできません。そのため、ランサムウェアによるデータの異常を検出することも検討する必要があります。Cloud Volumes Service は、現在ネイティブでは検出機能を提供していませんが、外部監視ソフトウェアを使用することもできます。

バックアップとリストア

Cloud Volumes Service は、標準のNASクライアントバックアップ機能（NFSまたはSMB経由のバックアップなど）を提供します。

- CVS -パフォーマンスを利用すると、他のCVSパフォーマンスボリュームにリージョン間でボリュームをレプリケーションすることができます。詳細については、を参照してください "ボリュームのレプリケーション" Cloud Volumes Service のドキュメントを参照してください。
- CVS-SWは、サービスネイティブのボリュームバックアップ/リストア機能を提供します。詳細については、を参照してください "クラウドバックアップ" Cloud Volumes Service のドキュメントを参照してください。

ボリュームレプリケーションを実行すると、ソースボリュームの正確なコピーが作成されるため、ランサムウェアのイベントなどの災害が発生した場合に迅速にフェイルオーバーできます。

クロスリージョンレプリケーション

CVS - Performanceを使用すると、Googleのネットワークで実行されているレプリケーションに使用される特定のインターフェイスを使用して、ネットアップが制御するバックエンドサービスネットワーク上でTLS1.2 AES 256 GCM暗号化を使用して、データ保護およびアーカイブのユースケース用にGoogle Cloudリージョン間でボリュームを安全に複製できます。プライマリ（ソース）ボリュームにはアクティブな本番データが格納され、セカンダリ（デスティネーション）ボリュームにレプリケートされてプライマリデータセットの正確なレプリカが提供されます。

最初のレプリケーションではすべてのブロックが転送されますが、更新ではプライマリボリューム内の変更されたブロックのみが転送されます。たとえば、プライマリボリュームにある1TBのデータベースがセカンダリボリュームにレプリケートされている場合、最初のレプリケーションでは1TBのスペースが転送されます。このデータベースの初期化と次の更新の間に数百行（仮定としては数MB）のデータがある場合、変更された行を持つブロックだけがセカンダリに複製されます（数MB）。これにより、転送時間を短縮し、レプリケーションの料金を抑えることができます。

ファイルとフォルダに対する権限はすべてセカンダリボリュームにレプリケートされますが、共有のアクセス権限（エクスポートポリシーとルール、SMB共有と共有ACLなど）は別々に処理する必要があります。サイトフェイルオーバーの場合、デスティネーションサイトは同じネームサービスとActive Directoryドメイン接続を利用して、ユーザ、グループのIDおよび権限を一貫して処理する必要があります。災害が発生したときにセカンダリボリュームをフェイルオーバーターゲットとして使用するには、レプリケーション関係を解除します。これにより、セカンダリボリュームが読み書き可能に変換されます。

ボリュームのレプリカは読み取り専用で、書き換え不可のデータのコピーをオフサイトに保管します。このため、ウィルスに感染したデータやランサムウェアによってプライマリデータセットが暗号化された場合に、データを迅速にリカバリできます。読み取り専用データは暗号化されませんが、プライマリボリュームに影響があり、レプリケーションが実行された場合は、感染したブロックもレプリケートされます。影響を受けない古いSnapshotコピーをリカバリに使用できますが、SLAは、攻撃が検出されるまでの時間に応じて、約束されたRTO/RPOの範囲外になる可能性があります。

また、Google Cloudのクロスリージョンレプリケーション（CRR）管理により、ボリュームの削除、Snapshotの削除、Snapshotスケジュールの変更など、悪意のある管理操作を防止できます。そのためには、ボリューム管理者を分離したカスタムロールを作成します。カスタムロールでは、ソースボリュームは削

除できますが、ミラーを解除できないため、ボリューム操作を実行できないCRR管理者からデスティネーションボリュームを削除できません。を参照してください "セキュリティに関する考慮事項" 各管理者グループが許可する権限については、Cloud Volumes Service のマニュアルを参照してください。

Cloud Volumes Service バックアップ

Cloud Volumes Service はデータの保持性は高くなりますが、外部イベントによって原因 のデータが失われる可能性があります。ウィルスやランサムウェアなどのセキュリティイベントが発生した場合、バックアップとリストアは、データアクセスを迅速に再開するために不可欠なものになります。管理者が誤ってCloud Volumes Service ボリュームを削除した場合があります。また、ユーザは、データのバックアップバージョンを数カ月間保持し、Snapshotコピー用にボリューム内に余分なスペースを残しておくことがコストの課題となります。過去数週間にバックアップ・バージョンを維持して失われたデータをリストアする方法としてはSnapshotコピーを推奨しますが、Snapshotコピーはボリューム内に置かれており、ボリュームが失われると失われます。

これらの理由から、NetApp Cloud Volumes Service は、を使用してバックアップサービスを提供します "Cloud Volumes Service バックアップ"。

Cloud Volumes Service バックアップを使用すると、Google Cloud Storage（GCS）にボリュームのコピーが生成されます。バックアップされるのはボリュームに格納されている実際のデータのみで、空きスペースはバックアップされません。増分データとして永久に機能するため、ボリュームの内容は1回転送され、以降も変更されたデータのみのバックアップが続行されます。従来のバックアップの概念と比較して、複数のフルバックアップを使用する場合に比べて、大量のバックアップストレージを節約し、コストを削減できます。バックアップスペースは、ボリュームと比べて月単位で少なくて済むため、バックアップバージョンの間隔を長くしておくのが理想的です。

ユーザはCloud Volumes Service バックアップを使用して、同じリージョン内の同じボリュームまたは別のボリュームに任意のバックアップバージョンをリストアできます。ソースボリュームを削除した場合は、バックアップデータが保持され、個別に管理する必要があります（削除した場合など）。

Cloud Volumes Service バックアップは、Cloud Volumes Service Asオプションに組み込まれています。ユーザは、Cloud Volumes Service バックアップをボリューム単位でアクティブ化して保護するボリュームを決定できます。を参照してください "Cloud Volumes Service バックアップのドキュメント" バックアップの詳細については、を参照してください "サポートされる最大バックアップバージョン数"、スケジュール、および "価格設定"。

プロジェクトのすべてのバックアップデータはGCSバケットに格納されます。GCSバケットはサービスによって管理され、ユーザには表示されません。各プロジェクトで異なるバケットを使用します。現在、バケットはCloud Volumes Service ボリュームと同じリージョンにありますが、その他のオプションについては現在説明しています。最新のステータスについては、のドキュメントを参照してください。

Cloud Volumes Service バケットからGCSへのデータ転送では、HTTPSとTLS1.2を使用したサービス内部のGoogleネットワークが使用されます。データはGoogleが管理するキーで保管中に暗号化されます。

Cloud Volumes Service バックアップの管理（バックアップの作成、削除、リストア）を行うには、が必要です "役割/ netappcloudvolumes .admin" ロール。

アーキテクチャ

概要

クラウド解決策 を信頼する一部は、アーキテクチャとその保護方法を理解していることです。このセクションでは、GoogleのCloud Volumes Service アーキテクチャのさまざ

まな側面を紹介し、データのセキュリティ保護に関する潜在的な懸念を軽減するとともに、最も安全な導入を実現するために追加の設定手順が必要な領域について説明します。

Cloud Volumes Service の一般的なアーキテクチャは、コントロールプレーンとデータプレーンの2つの主要コンポーネントに分類できます。

コントロールプレーン

Cloud Volumes Service のコントロールプレーンは、Cloud Volumes Service 管理者とネットアップの標準の自動化ソフトウェアが管理するバックエンドインフラです。このプレーンはエンドユーザに対して完全に透過的であり、ネットワーキング、ストレージハードウェア、ソフトウェアアップデートなどが含まれており、Cloud Volumes Service などのクラウド常駐解決策 に価値を提供します。

データプレーン

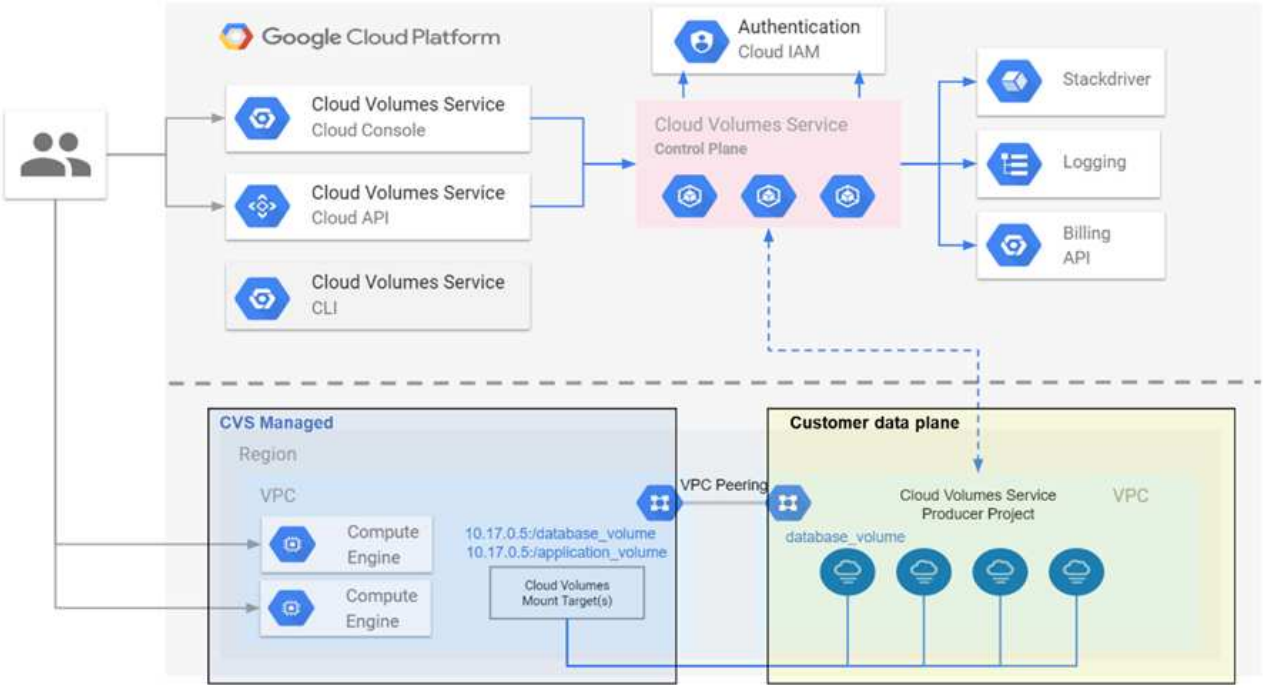
Cloud Volumes Service のデータプレーンには、実際のデータボリュームとCloud Volumes Service の全体的な設定（アクセス制御、Kerberos認証など）が含まれています。データプレーンは、エンドユーザとCloud Volumes Service プラットフォームの消費者の制御下に完全にあります。

各平面の保護および管理方法には、異なる違いがあります。以降のセクションでは、Cloud Volumes Service アーキテクチャの概要から始めて、これらの違いについて説明します。

Cloud Volumes Service アーキテクチャ

CloudSQL、Google Cloud VMware Engine（GCVE）、ファイルストアなど、他のGoogle Cloudネイティブサービスと同様の方法で、Cloud Volumes Service はを使用します "Google PSA" サービスを提供します。PSAでは、サービスは、を使用するサービスプロデューサプロジェクト内に構築されます "vPCネットワークピアリング" サービスコンシューマに接続するには、次の手順に従います。サービスプロデューサーはネットアップが提供して運用します。サービスコンシューマは、Cloud Volumes Service ファイル共有にアクセスするクライアントをホストする、お客様のプロジェクトのVPCです。

から参照される次の図 "アーキテクチャセクション" Cloud Volumes Service のドキュメントの概要をに示します。



点線の上の部分は、ボリュームのライフサイクルを制御するサービスのコントロールプレーンを示しています。点線の下の部分は、データプレーンを示しています。左側の青いボックスはユーザVPC（サービスコンシューマ）を示し、右側の青いボックスはネットアップが提供するサービスプロデューサーです。どちらもVPCピアリングを介して接続されます。

テナンシーモデル

Cloud Volumes Service では、個々のプロジェクトが固有のテナントとみなされます。つまり、ボリュームやSnapshotコピーの操作はプロジェクト単位で実行されます。つまり、すべてのボリュームは、で作成されたプロジェクトによって所有され、そのプロジェクトだけが、デフォルトでボリューム内のデータを管理およびアクセスできます。これは、サービスのコントロールプレーンビューと見なされます。

共有 **VPC**

データプレーンビューでは、Cloud Volumes Service を共有VPCに接続できます。ボリュームは、ホスティングプロジェクトまたは共有VPCに接続されたサービスプロジェクトのいずれかで作成できます。その共有VPCに接続されたすべてのプロジェクト（ホストまたはサービス）が、ネットワークレイヤのボリュームにアクセスできます（TCP / IP）。共有VPCでネットワーク接続を確立しているすべてのクライアントはNASプロトコルを使用してデータにアクセスできる可能性があるため、個々のボリュームでのアクセス制御（ユーザ/グループのアクセス制御リスト（ACL）やNFSエクスポートのホスト名/ IPアドレスなど）を使用して、データにアクセスできるユーザを制御する必要があります。

Cloud Volumes Service は、顧客プロジェクトごとに最大5つのVPCに接続できます。コントロールプレーンでは、どのVPCに接続されているかに関係なく、作成されたすべてのボリュームをプロジェクトで管理できます。データプレーンではVPCが相互に分離され、各ボリュームは1つのVPCにのみ接続できます。

個々のボリュームへのアクセスは、プロトコル固有の（NFS / SMB）アクセス制御メカニズムによって制御されます。

つまり、ネットワークレイヤでは、共有VPCに接続されているすべてのプロジェクトがボリュームを表示できますが、管理側では、コントロールプレーンでしか所有者プロジェクトにボリュームを表示できません。

vPCサービスコントロール

vPCサービスコントロールは、インターネットに接続され、世界中でアクセス可能なGoogleクラウド サービス の周辺にアクセス制御境界を確立します。これらのサービスは、ユーザIDを使用してアクセス制御を提供しますが、どのネットワークロケーション要求の送信元を制限することはできません。vPCサービスコントロールは、定義されたネットワークへのアクセスを制限する機能を導入することで、このギャップを解消します。

Cloud Volumes Service データプレーンは外部インターネットには接続されず、明確に定義されたネットワーク境界（境界）を持つプライベートVPCに接続されます。ネットワーク内では、各ボリュームはプロトコル固有のアクセス制御を使用します。外部ネットワーク接続は、Google Cloudプロジェクト管理者によって明示的に作成されます。ただし、コントロールプレーンはデータプレーンと同じ保護機能を提供しません。また、有効なクレデンシャル（）を持つ任意の場所から誰でもアクセスできます "JWTトークン"）。

つまり、Cloud Volumes Service データプレーンは、VPCサービスコントロールをサポートする必要なく、ネットワークアクセス制御機能を提供します。VPCサービスコントロールは明示的に使用しません。

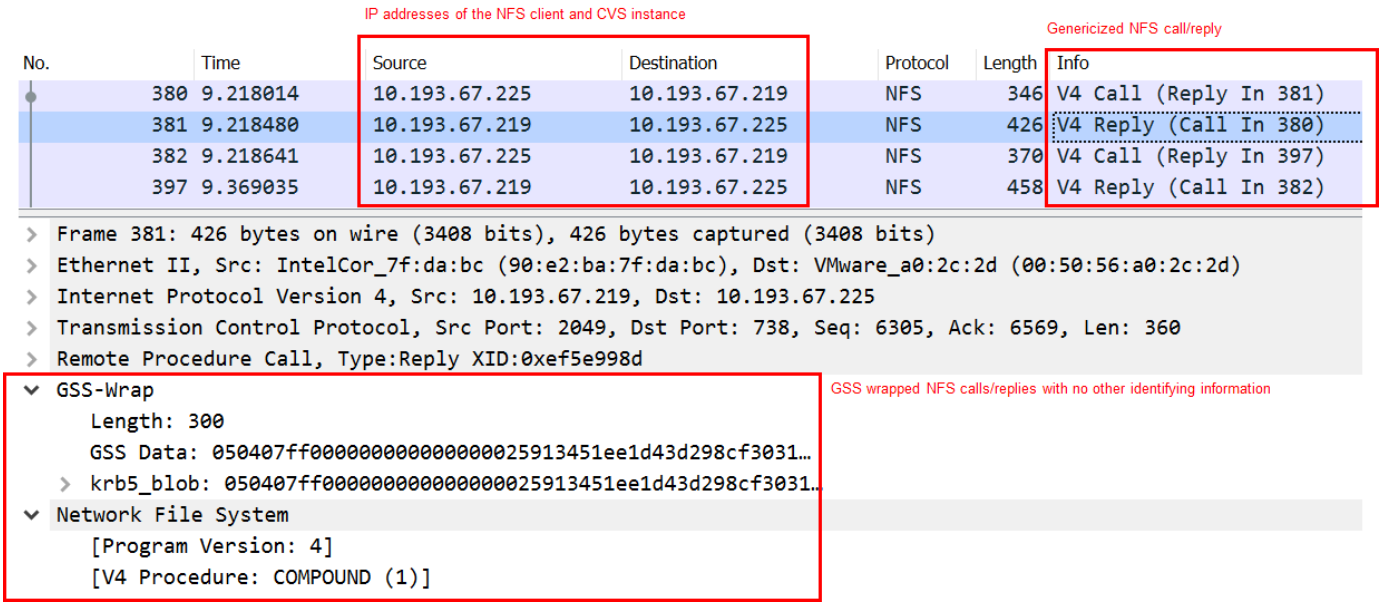
パケットのスニッフィング/トレースに関する考慮事項

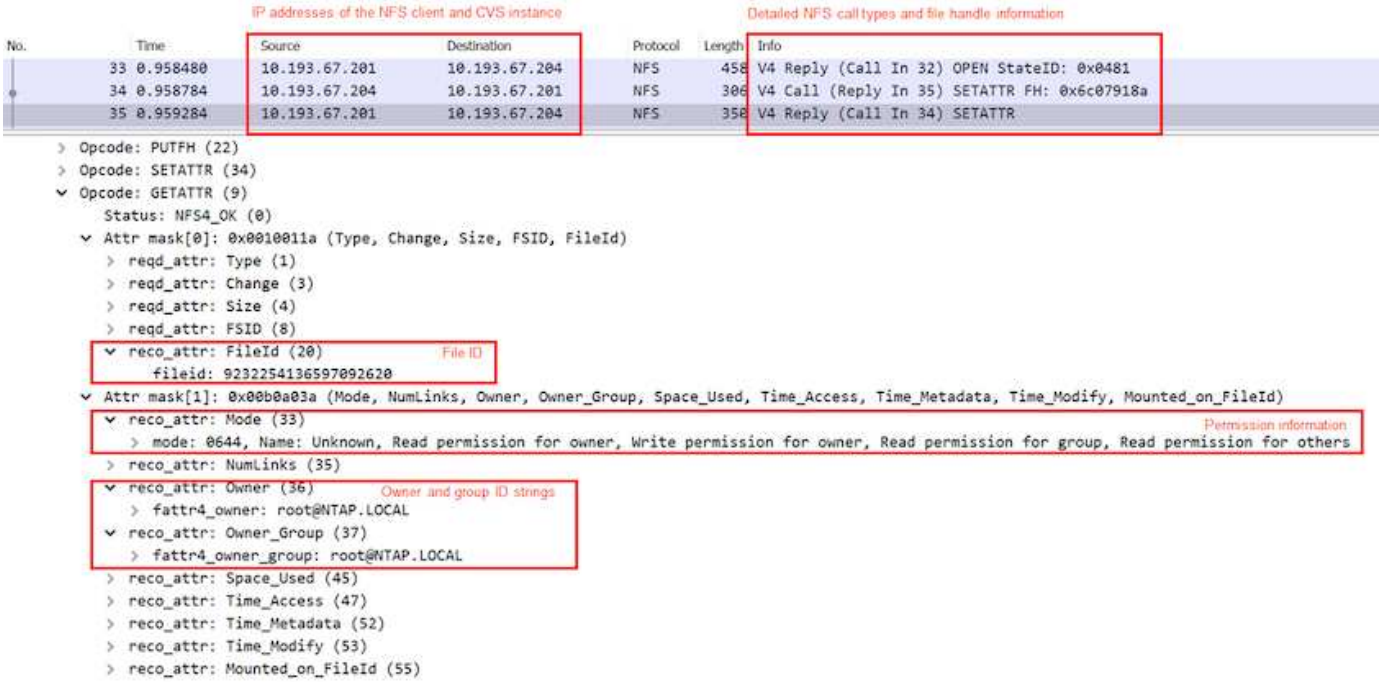
パケットキャプチャは、ネットワークの問題やその他の問題（NAS権限、LDAP接続など）のトラブルシューティングに役立ちますが、悪意を持ってネットワークIPアドレス、MACアドレス、ユーザ名およびグループ名、エンドポイントで使用されているセキュリティレベルなどの情報を取得することもできます。Google Cloudネットワーク、VPC、およびファイアウォールルールの設定方法が原因で、ユーザのログインクレデンシャルやを使用しないとネットワークパケットへの不要なアクセスを取得できなくなります "JWTトークン" クラウドインスタンスへ。パケットキャプチャはエンドポイント（仮想マシン（VM）など）でのみ可能であり、VPC内部のエンドポイントでのみ可能です。ただし、共有VPCまたは外部ネットワークトンネル/ IP転送を使用してエンドポイントへの外部トラフィックを明示的に許可している場合は除きます。クライアントの外部でトラフィックをスニファする方法はありません。

共有VPCを使用する場合は、NFS Kerberosまたは/またはを使用した転送中の暗号化が可能です "SMB暗号化" トレースから収集された情報の多くを隠すことができます。ただし、一部のトラフィックは、などのプレーンテキストで送信されます "DNS" および "LDAPクエリ"。次の図に、Cloud Volumes Service から発信されたプレーンテキストLDAPクエリからのパケットキャプチャと、公開されている可能性のある識別情報を示します。Cloud Volumes Service のLDAPクエリでは、現在、暗号化またはLDAP over SSLがサポートされていません。CVS - Active Directoryから要求された場合に、パフォーマンスがLDAP署名をサポートします。CVS-SWではLDAP署名はサポートされません。

unixUserPasswordはLDAPによって照会され、プレーンテキストではなくソルトハッシュで送信されます。デフォルトでは、Windows LDAPではunixUserPasswordフィールドは読み込まれません。このフィールドは、LDAPを使用してクライアントへの対話型ログインを行う必要がある場合にのみ必要になります。Cloud Volumes Service では、インスタンスへの対話型LDAPログインはサポートされていません。

次の図は、AUTH_SYSでNFSをキャプチャしたあとの、NFS Kerberos通信からのパケットキャプチャを示しています。トレースで使用できる情報が2つの違いと、転送中の暗号化を有効にすることでNASトラフィックの全体的なセキュリティが向上することに注意してください。





VMネットワークインターフェイス

攻撃者のトリックの1つとして、のVMに新しいNIC（ネットワークインターフェイスカード）を追加する方法があります "プロミスキャスモードです" （ポートミラーリング）を使用するか、既存のNICでプロミスキャスモードを有効にして、すべてのトラフィックをスニファします。Google Cloudで新しいNICを追加するには、VMを完全にシャットダウンする必要があります。これによりアラートが生成されるため、攻撃者はこのことに気づかれません。

また、NICをプロミスキャスモードに設定することはできず、Google Cloudでアラートをトリガーします。

コントロールプレーンのアーキテクチャ

Cloud Volumes Service に対する管理操作は、すべてAPIを通じて実行されます。GCPクラウドコンソールに統合されたCloud Volumes Service 管理でも、Cloud Volumes Service APIを使用します。

IDおよびアクセス管理

IDおよびアクセス管理 ("IAM"）は、Google Cloudプロジェクトインスタンスへの認証（ログイン）と許可（権限）を制御できる標準サービスです。Google IAMには、許可の承認と削除に関する完全な監査証跡が用意されています。現在、Cloud Volumes Service ではコントロールプレーンの監査を提供していません。

承認/権限の概要

IAMには、Cloud Volumes Service に対する詳細な権限があらかじめ組み込まれています。を見つけることができる "詳細な権限の一覧をここに入力します"。

IAMには、「netappcloudvolumes」と「netappcloudvolumes」という2つの事前定義された役割も用意されています。これらのロールは、特定のユーザまたはサービスアカウントに割り当てることができます。

IAMユーザにCloud Volumes Service の管理を許可する適切なロールと権限を割り当てます。

きめ細かい権限の使用例を次に示します。

- ボリュームを削除できないように、権限の取得/リスト/作成/更新だけを指定してカスタムロールを作成します。
- 「snapshot.*」権限のみを持つカスタム・ロールを使用して、アプリケーションと整合性のあるSnapshot統合を構築するために使用するサービス・アカウントを作成します。
- 特定のユーザーに'volumeereplication.*'を委任するカスタムロールを作成します

サービスアカウント

スクリプトまたはを使用してCloud Volumes Service API呼び出しを実行する "テラフォーム "'roles/netappcloudvolumes .admin'ロールを持つサービスアカウントを作成する必要がありますこのサービスアカウントを使用して、Cloud Volumes Service API要求の認証に必要なJWTトークンを生成できます。これには、次の2つの方法があります。

- JSONキーを生成し、Google APIを使用してJWTトークンを取得します。これは最もシンプルなアプローチですが、手動のシークレット（JSONキー）管理が必要になります。
- 使用 "サービスアカウントのなりすまし" 「roles/iam.serviceAccountTokenCreator`」を指定します。コード（スクリプト、Terraformなど）はで実行されます "アプリケーションのデフォルトクレデンシャル" また、サービスアカウントを偽装して権限を取得します。このアプローチは、Googleのセキュリティのベストプラクティスを反映しています。

を参照してください "サービスアカウントと秘密鍵を作成しています" 詳細については、Google Cloudのドキュメントを参照してください。

Cloud Volumes Service APIの略

Cloud Volumes Service APIでは、基盤となるネットワーク転送としてHTTPS（TLSv1.2）を使用してRESTベースのAPIを使用します。最新のAPI定義を確認できます "こちらをご覧ください" およびでのAPIの使用方法に関する情報 "Google CloudドキュメントのCloud Volume API"。

APIエンドポイントは、標準のHTTPS（TLSv1.2）機能を使用してネットアップによって処理および保護されます。

JWTトークン

APIへの認証は、JWTベアラートークンを使用して実行されます ("RFC-7519"）。有効なJWTトークンは、Google Cloud IAM認証を使用して取得する必要があります。そのためには、サービスアカウントのJSONキーを指定してIAMからトークンを取得する必要があります。

監査ロギング

現在、ユーザがアクセスできるコントロールプレーン監査ログはありません。

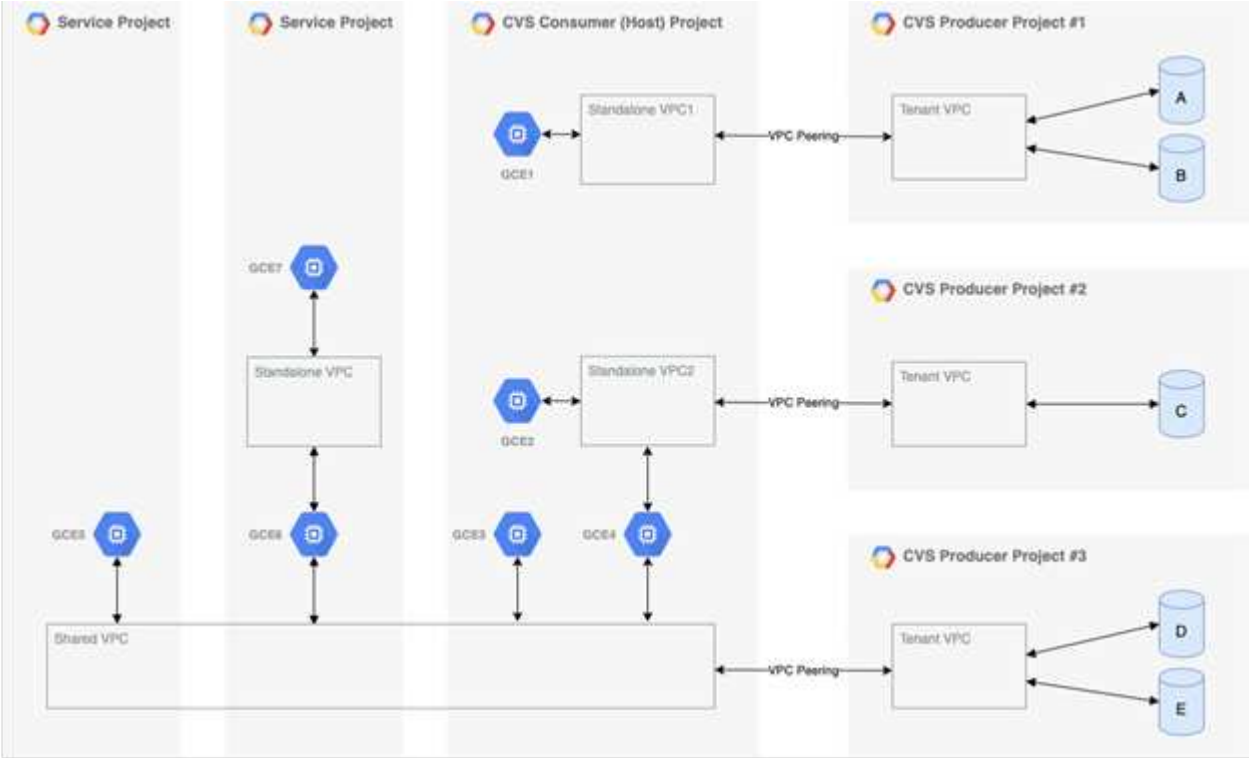
データプレーンアーキテクチャ

Cloud Volumes Service for Google CloudはGoogle Cloudを活用しています "プライベートサービスへのアクセス" フレームワーク：このフレームワークでは、ユーザーはCloud Volumes Service に接続できます。このフレームワークでは、他のGoogleクラウド サービス のようなサービスネットワーキングとVPCピアリングの構成要素を使用して、テナ

ント間の完全な分離を実現します。

Cloud Volumes Service for Google Cloudのアーキテクチャの概要については、を参照してください "Cloud Volumes Service のアーキテクチャ"。

ユーザVPC（スタンドアロンまたは共有）は、Cloud Volumes Service で管理されるテナントプロジェクト内のVPCとピア関係にあり、VPC間でボリュームをホストします。



上の図は、3つのVPCネットワークがCloud Volumes Service に接続され、複数のCompute Engine VM（GCE1-7）がボリュームを共有しているプロジェクト（中央のCVSコンシューマプロジェクト）を示しています。

- VPC1では、GCE1がボリュームAおよびBにアクセスできます
- VPC2は、GCE2とGCE4がボリュームCにアクセスできるようにします
- 3つ目のVPCネットワークは共有VPCで、2つのサービスプロジェクトで共有されます。これにより、GCE3、GCE4、GCE5、およびGCE6がボリュームDおよびEにアクセスできるようになります共有VPCネットワークは、CVS -パフォーマンスサービスタイプのボリュームでのみサポートされます。

GCE7はどのボリュームにもアクセスできません。

データは転送中（Kerberos暗号化やSMB暗号化を使用）と保管中（Cloud Volumes Service ）の両方で暗号化できます。

転送中のデータ暗号化

転送中のデータはNASプロトコルレイヤで暗号化でき、Google Cloudネットワーク自体は暗号化されます。これについては、次の項で説明します。

Google Cloudネットワーク

Google Cloudは、に記載されているように、ネットワークレベルでトラフィックを暗号化します "転送中の暗号化" Googleのドキュメントを参照してください。「Cloud Volume サービスアーキテクチャ」セクションで説明したように、Cloud Volumes Service は、ネットアップが管理するPSAプロデューサープロジェクトから提供されます。

CVSソフトウェアの場合、プロデューサーテナントはGoogle VMを実行してサービスを提供します。ユーザーVMとCloud Volumes Service VM間のトラフィックは、Googleによって自動的に暗号化されます。

CVSパフォーマンスのデータパスはネットワークレイヤでは完全に暗号化されていませんが、ネットアップとGoogleでは組み合わせて使用しています "IEEE 802.1AE暗号化（MACSec）"、 "カプセル化" （データ暗号化）、および物理的に制限されたネットワークを使用して、Cloud Volumes Service CVS -パフォーマンスサービスタイプとGoogle Cloudの間で転送されるデータを保護します。

NASプロトコル

NFSおよびSMB NASプロトコルは、プロトコルレイヤでオプションのトランスポート暗号化を提供します。

SMB暗号化

"SMB暗号化" SMBデータをエンドツーエンドで暗号化し、信頼されていないネットワーク上での盗聴からデータを保護します。クライアント/サーバのデータ接続（smb3.x対応クライアントでのみ使用可能）とサーバ/ドメインコントローラの認証の両方に対して暗号化を有効にできます。

SMB暗号化が有効な場合、暗号化をサポートしていないクライアントは共有にアクセスできません。

Cloud Volumes Service は、SMB暗号化でRC4-HMAC、AES-128 - CTS-HMAC-SHA1、およびAES-256 - HMAC-SHA1セキュリティ暗号をサポートしています。SMBは、サーバによってサポートされている最も高い暗号化タイプとネゴシエートします。

NFSv4.1 Kerberos

NFSv4.1のCVSパフォーマンスでは、Kerberos認証を使用できます。を参照してください "RFC7530" 。Kerberosはボリューム単位で有効にすることができます。

Kerberosで現在使用可能な最も強力な暗号化タイプは、AES-256、HMAC-SHA1です。NetApp Cloud Volumes Service は、NFS用にAES-256 - HMAC-SHA1、AES-128 - HMAC-SHA1、DES3、およびDESをサポートしています。CIFS / SMBトラフィックではARCFOUR-MHMAC（RC4）もサポートされますが、NFSではサポートされません。

Kerberosでは、NFSマウントに対する3つの異なるセキュリティレベルが提供され、Kerberosセキュリティの強固な設定を選択できます。

RedHatの場合と同様です "Common Mount Options（共通マウントオプション）" マニュアル：

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

一般的に、Kerberosセキュリティレベルを高くするほど、クライアントとサーバが送信する各パケットのNFS操作の暗号化と復号化に時間を費やすので、パフォーマンスが低下します。多くのクライアントとNFSサーバは、CPUにAES-NIオフロードをサポートして全体的なエクスペリエンスを向上していますが、Kerberos 5p（完全なエンドツーエンドの暗号化）のパフォーマンスへの影響はKerberos 5（ユーザ認証）の影響よりも大幅に大きくなります。

次の表に、セキュリティとパフォーマンスの各レベルの違いを示します。

セキュリティレベル	セキュリティ	パフォーマンス
NFSv3：sys	• 最小のセキュリティ。数値のユーザIDまたはグループIDを含むプレーンテキスト • UID、GID、クライアントIPアドレス、エクスポートパス、ファイル名を表示できる パケットキャプチャの権限	• ほとんどの場合に最適です
NFSv4.x - sys	• NFSv3（クライアントID、名前文字列/ドメイン文字列の照合）よりも安全ですが、それでもテキストは表示されません • UID、GID、クライアントIPアドレス、名前文字列、ドメインIDを表示できる パケットキャプチャでのエクスポートパス、ファイル名、権限	• シーケンシャルワークロード（VM、データベース、大容量ファイルなど）に適している • ファイル数が多い/メタデータが多い（30~50%悪化）

セキュリティレベル	セキュリティ	パフォーマンス
NFS—krb5	• すべてのNFSパケットのクレデンシャルのKerberos暗号化●GSSラッパー内のRPCコールでユーザ/グループのUID/GIDをラップします • マウントを要求しているユーザは、有効なKerberosチケット（ユーザ名とパスワード、または手動のキータブ交換）を必要とします。チケットは指定した期間が経過すると有効期限が切れ、ユーザはアクセスを再認証する必要があります • NFS処理またはmount / portmapper / NLMなどの補助プロトコル（エクスポートパス、IPアドレス、ファイルハンドル、権限、ファイル名を参照可能）の暗号化なし パケットキャプチャのatime / mtime）	• ほとんどの場合Kerberosに適しており、AUTH_SYSよりも深刻です
NFS—krb5i	• すべてのNFSパケットのクレデンシャルのKerberos暗号化●GSSラッパー内のRPCコールでユーザ/グループのUID/GIDをラップします • マウントを要求しているユーザは、有効なKerberosチケット（ユーザ名/パスワードまたは手動のキータブ交換を使用）を必要とします。チケットは指定した期間が経過すると失効し、ユーザはアクセスを再認証する必要があります • NFS処理またはmount / portmapper / NLMなどの補助プロトコル（エクスポートパス、IPアドレス、ファイルハンドル、権限、ファイル名を参照可能）の暗号化なし パケットキャプチャのatime / mtime） • Kerberos GSSチェックサムが各パケットに追加されるため、パケットを傍受することはありません。チェックサムが一致する場合は、会話が許可されます。	• NFSペイロードは暗号化されないため、krb5pよりも優れています。krb5よりも追加されたオーバーヘッドのみが整合性のチェックサムです。krb5iのパフォーマンスはkrb5よりもそれほど悪くはないが、多少の低下が見られる。

セキュリティレベル	セキュリティ	パフォーマンス
NFS–krb5p	• すべてのNFSパケットのクレデンシャルのKerberos暗号化●GSSラッパー内のRPCコールでユーザ/グループのUID/GIDをラップします • マウントを要求しているユーザは、有効なKerberosチケット（ユーザ名とパスワード、または手動のkeytab交換を使用）を必要とします。チケットは指定した期間が経過すると有効期限が切れ、ユーザはアクセスを再認証する必要があります • すべてのNFSパケットペイロードは、GSSラッパーで暗号化されます（パケットキャプチャではファイルハンドル、権限、ファイル名、atime/mtimeを確認できません）。 • 整合性チェックが含まれます。 • NFSの処理タイプは表示されます（fsinfo、access、GETATTRなど）。 • 補助プロトコル（マウント、portmap、NLMなど）は暗号化されません-（エクスポートパス、IPアドレスを参照可能）	• セキュリティレベルで最悪のパフォーマンス。krb5pは、暗号化や復号化がさらに必要です。 • NFSv4.xに加えてkrb5pを使用した方がパフォーマンスが向上し、ファイル数の多いワークロードに対応できます。

Cloud Volumes Service では、設定されたActive DirectoryサーバがKerberosサーバおよびLDAPサーバとして使用されます（RFC2307互換スキーマからユーザIDを検索する場合）。それ以外のKerberosサーバまたはLDAPサーバはサポートされません。Cloud Volumes Service では、アイデンティティ管理にLDAPを使用することを強く推奨します。NFS Kerberosがパケットキャプチャにどのように表示されるかについては、を参照してください "「パケットのスニッフィング/トレースに関する考慮事項」"

保存データの暗号化

Cloud Volumes Service 内のすべてのボリュームはAES-256暗号化を使用して暗号化されます。つまり、メディアに書き込まれたすべてのユーザデータが暗号化され、ボリューム単位のキーでのみ復号化できます。

- CVS - SWの場合は、Googleで生成されたキーが使用されます。
- CVS -パフォーマンスの場合は、ボリューム単位のキーが、Cloud Volumes Service に組み込まれているキー管理ツールに格納されます。

2021年11月より、顧客管理の暗号化キー（CMEK）機能のプレビューが提供されました。これにより、でホストされているプロジェクトごとのリージョンごとのマスターキーを使用して、ボリュームごとのキーを暗号

化できます "Google Key Management Service（KMS）：" KMSを使用すると、外部キー管理ツールを接続できます。

CVS -パフォーマンス用のKMSの設定については、を参照してください "お客様が管理する暗号化キーを設定する"。

ファイアウォール：

Cloud Volumes Service は、複数のTCPポートを公開してNFS共有とSMB共有に対応します。

- "NFSアクセスに必要なポート"
- "SMBアクセスに必要なポート"

さらに、Kerberosを含むLDAPを使用するSMB、NFS、およびデュアルプロトコル構成では、Windows Active Directoryドメインへのアクセスが必要になります。Active Directory接続はである必要があります "を設定します" 地域単位で指定します。Active Directoryドメインコントローラ（DC）は、で識別できます "DNSベースのDC検出" 指定したDNSサーバを使用しています。返されるDCはすべて使用されます。対象となるDCのリストは、Active Directoryサイトを指定することによって制限できます。

Cloud Volumes Service は、に割り当てられているCIDR範囲のIPアドレスを使用して到達します `gcloud compute address` コマンドを実行中です "Cloud Volumes Service への参加"。このCIDRをソースアドレスとして使用して、Active Directoryドメインコントローラへのインバウンドファイアウォールを設定できます。

Active Directoryドメインコントローラは必須です "ここで説明したCloud Volumes Service CIDRsにポートを公開します"。

NASプロトコル

NASプロトコルの概要

NASプロトコルには、NFS（v3およびv4.1）とSMB / CIFS（2.xおよび3.x）があります。CVSでは、これらのプロトコルを使用して、複数のNASクライアント間でデータへの共有アクセスが許可されます。また、Cloud Volumes Service は、NAS共有内のファイルやフォルダのIDおよび権限の設定をすべて満たしながら、NFSクライアントとSMB / CIFSクライアントへのアクセスを同時に提供（デュアルプロトコル）できます。最高レベルのデータ転送セキュリティを維持するため、Cloud Volumes Service は、SMB暗号化とNFS Kerberos 5pを使用して転送中のプロトコル暗号化をサポートしています。

> デュアルプロトコルはCVSパフォーマンスでのみ使用できます。

NASプロトコルの基本

NASプロトコルは、ネットワーク上の複数のクライアントが、GCP上のCloud Volumes Service などのストレージシステム上の同じデータにアクセスするための方法です。NFSとSMBは定義済みのNASプロトコルであり、Cloud Volumes Service がサーバとして機能するクライアント/サーバベースで動作します。クライアントは、アクセス要求、読み取り要求、および書き込み要求をサーバに送信します。サーバは、ファイルのロックメ

カニズムを調整し、権限を格納し、IDおよび認証要求を処理します。

たとえば、NASクライアントがフォルダに新しいファイルを作成する場合は、次の一般的なプロセスが実行されます。

1. クライアントは、ディレクトリに関する情報（権限、所有者、グループ、ファイルID、使用可能なスペース、 など）。要求元のクライアントとユーザが親フォルダに対して必要な権限を持っている場合、サーバは情報を返します。
2. ディレクトリ上のアクセス許可がアクセスを許可されている場合、クライアントは、作成されるファイル名がファイルシステムにすでに存在するかどうかをサーバに確認します。ファイル名がすでに使用されている場合は、の作成に失敗します。ファイル名が存在しない場合、サーバーはクライアントに処理を続行できることを通知します。
3. クライアントがサーバを呼び出して、ディレクトリハンドルとファイル名を指定してファイルを作成し、アクセス日時と変更日時を設定します。サーバは、一意のファイルIDをファイルに発行して、同じファイルIDで他のファイルが作成されないようにします。
4. クライアントは、書き込み処理の前に、ファイル属性をチェックする呼び出しを送信します。権限で許可されている場合、クライアントは新しいファイルを書き込みます。プロトコル/アプリケーションでロックが使用されている場合、クライアントは、データ破損を防ぐために、ロック中に他のクライアントがファイルにアクセスできないようにするために、サーバにロックを要求します。

NFS

NFSは、Request for Comments（RFC）で定義されたオープンIETF標準である分散ファイルシステムプロトコルで、誰でもこのプロトコルを実装できます。

Cloud Volumes Service 内のボリュームは、クライアントまたはクライアントのセットからアクセスできるパスをエクスポートすることによって、NFSクライアントに共有されます。これらのエクスポートをマウントするための権限は、Cloud Volumes Service 管理者が設定可能なエクスポートポリシーとルールによって定義されます。

ネットアップのNFS実装はプロトコルのゴールドスタンダードとみなされ、無数のエンタープライズNAS環境で使用されています。以降のセクションでは、NFSと、Cloud Volumes Service で使用できる特定のセキュリティ機能、およびそれらの実装方法について説明します。

デフォルトのローカル**UNIX**ユーザおよびグループ

Cloud Volumes Service には、基本的な機能のさまざまなデフォルトUNIXユーザおよびグループが含まれています。このようなユーザおよびグループは、現在変更または削除できません。現在、新しいローカルユーザとローカルグループをCloud Volumes Service に追加することはできません。デフォルトのユーザとグループ以外のUNIXユーザおよびグループは、外部LDAPネームサービスによって提供する必要があります。

次の表に、デフォルトのユーザとグループ、および対応する数値IDを示します。LDAPまたはローカルクライアントでこれらの数値IDを再使用する新しいユーザまたはグループを作成しないことを推奨します。

デフォルトユーザ：数値ID	デフォルトグループ：数値ID
• ルート：0 • pcuser：65534 • nobody：65535	• ルート：0 • デーモン：1. • pcuser：65534 • nobody：65535

NFSv4.1を使用している場合、NFSクライアントでディレクトリリストコマンドを実行すると、rootユーザがnobodyと表示されることがあります。これは、クライアントのIDドメインマッピング設定が原因です。を参照してください NFSv4.1およびnobodyユーザ/グループ この問題 の詳細および解決方法については、を参照してください。

rootユーザ

Linuxの場合、rootアカウントはLinuxベースのファイルシステムのすべてのコマンド、ファイル、フォルダにアクセスできます。このアカウントの権限のため、セキュリティのベストプラクティスでは、rootユーザを何らかの方法で無効にしたり制限したりする必要があります。NFSエクスポートでは、エクスポートポリシーとルール、およびroot squashと呼ばれる概念を使用して、rootユーザがファイルやフォルダを経由する際の電力をCloud Volumes Service で制御できます。

rootの引き下げにより、NFSマウントにアクセスしているrootユーザーは、匿名の数値ユーザー65534に引き下げられます（「」を参照）[匿名ユーザ]」）に設定されており、現在、CVSパフォーマンスを使用する場合にのみ利用できます。この場合は、エクスポートポリシールールの作成時にrootアクセスにOffを選択します。rootユーザを匿名ユーザに引き下げた場合、chownまたはを実行できなくなります "setuid / setgidコマンド（スティッキービット）" NFSマウント内のファイルまたはフォルダ、およびrootユーザが作成したファイルまたはフォルダについては、anon UIDが所有者/グループとして表示されます。また、NFSv4 ACLをrootユーザが変更することはできません。ただし、rootユーザは引き続きchmodにアクセスでき、削除されたファイルは明示的な権限を持っていません。rootユーザーのファイルおよびフォルダのアクセス権へのアクセスを制限する場合は、NTFS ACLを持つボリュームを使用し、「root」という名前のWindowsユーザーを作成し、必要なアクセス権をファイルまたはフォルダに適用することを検討してください。

匿名ユーザ

匿名（anon）ユーザIDは、有効なNFSクレデンシャルのないクライアント要求に割り当てられるUNIXユーザIDまたはユーザ名です。これには、rootの引き下げが使用されている場合のrootユーザが含まれます。Cloud Volumes Service のanonユーザは65534です。

このUIDは、Linux環境では通常、ユーザ名「nobody」または「nfsnobody」に関連付けられます。Cloud Volumes Service はまた'ローカルUNIXユーザpcuserとして65534を使用します（を参照してくださいデフォルトのローカルUNIXユーザおよびグループ「）」と入力します。これは、有効な一致するUNIXユーザがLDAPで見つからない場合に、WindowsからUNIXへのネームマッピングのデフォルトフォールバックユーザでもあります。

LinuxとCloud Volumes Service のUID 65534ではユーザ名が異なるため、NFSv4.1を使用する場合に65534にマッピングされたユーザの名前文字列が一致しないことがあります。その結果、一部のファイルやフォルダでは「nobody」がユーザーとして表示されることがあります。「」を参照してくださいNFSv4.1およびnobodyユーザ/グループ「この問題 の詳細と解決方法については、こちらをご覧ください。

アクセス制御/エクスポート

NFSマウントに対する最初のエクスポート/共有アクセスは、エクスポートポリシーに含まれるホストベースのエクスポートポリシールールによって制御されます。ホストIP、ホスト名、サブネット、ネットグループ、またはドメインが定義され、NFS共有へのアクセス、およびホストに許可されるアクセスレベルが許可されます。エクスポートポリシールールの設定オプションは、Cloud Volumes Service レベルによって異なります。

CVS - SWの場合は、エクスポートポリシー設定に次のオプションを使用できます。

- クライアント一致。 IPアドレスをカンマで区切ったリスト、ホスト名、サブネット、ネットグループ、ドメイン名をカンマで区切って指定します。
- * RO/RWアクセスルール。*エクスポートへのアクセスレベルを制御するには、読み取り/書き込みまたは読み取り専用を選択します。CVS -パフォーマンスには、次のオプションがあります。
- クライアント一致。 IPアドレスをカンマで区切ったリスト、ホスト名、サブネット、ネットグループ、ドメイン名をカンマで区切って指定します。
- * RO/RWアクセスルール。*エクスポートへのアクセスレベルを制御するには、読み取り/書き込みまたは読み取り専用を選択します。
- *ルートアクセス（オン/オフ）。*ルートスカッシュを設定します（「」を参照）[rootユーザ]"詳細については、を参照してください。
- プロトコル・タイプ。 NFSマウントへのアクセスを特定のプロトコル・バージョンに制限します。ボリュームに対してNFSv3とNFSv4.1の両方を指定する場合は、両方を空白にするか、両方のチェックボックスをオンにします。
- * Kerberosセキュリティレベル（「Kerberosを有効にする」を選択した場合）。*読み取り専用アクセスまたは読み取り/書き込みアクセス用のkrb5、krb5i、およびkrb5pのオプションを提供します。

所有権の変更（**chown**）とグループの変更（**chgrp**）

Cloud Volumes Service でNFSを使用すると、rootユーザに対してファイルとフォルダに対してchown / chgrpの実行のみを許可します。他のユーザーには「操作は許可されていません」というエラーが表示されます。これは、自分が所有しているファイルでもroot squashを使用する場合は、「」の項で説明されているようにしてください[rootユーザ]」）、ルートはrootユーザに引き下げられ、chownおよびchgrpへのアクセスは許可されません。現時点では、Cloud Volumes Service でroot以外のユーザに対してchownとchgrpの両方を実行できるようにするための回避策はありません。所有権の変更が必要な場合は、デュアルプロトコルのボリュームを使用し、Windows側からアクセス権を制御するためにセキュリティ形式をNTFSに設定することを検討してください。

権限の管理

Cloud Volumes Service では、UNIXセキュリティ形式を使用するボリュームのNFSクライアントに対する権限を制御するために、モードビット（rwxの場合に644、777など）とNFSv4.1 ACLの両方がサポートされます。標準の権限管理は、これら（chmod、chown、nfs4_setfaclなど）に対して使用し、これらをサポートするすべてのLinuxクライアントで機能します。

また、NTFSに設定されたデュアルプロトコルボリュームを使用する場合、NFSクライアントはWindowsユーザへのCloud Volumes Service ネームマッピングを利用でき、NTFSアクセス権の解決に使用されます。これには、Cloud Volumes Service へのLDAP接続で数値IDからユーザ名への変換が必要です。Cloud Volumes Service では、Windowsユーザ名に正しくマッピングするために有効なUNIXユーザ名が必要です。

NFSv3にきめ細かな**ACL**を提供

モードビットのアクセス権はセマンティクス上の所有者、グループ、その他すべてのユーザにのみ適用され、基本的なNFSv3については、細かいユーザアクセス制御は行われません。Cloud Volumes Service は、POSIX ACLおよび拡張属性（chattrなど）をサポートしていないため、次のシナリオでのみ詳細なACLを使用できます。

- 有効なUNIXからWindowsへのユーザマッピングを使用するNTFSセキュリティ形式のボリューム（CIFSサーバが必要）。
- 管理クライアントを使用してACLを適用したNFSv4.1 ACL。

どちらの方法でも、UNIX IDを管理するためにLDAP接続が必要です。また、有効なUNIXユーザおよびグループの情報が入力されている必要があります（を参照） "「LDAP」"）とは、CVSパフォーマンスインスタンスでのみ使用できます。NFSでNTFSセキュリティ形式のボリュームを使用するには、SMB接続を確立していない場合でも、デュアルプロトコル（SMBおよびNFSv3）またはデュアルプロトコル（SMBおよびNFSv4.1）を使用する必要があります。NFSv3マウントでNFSv4.1 ACLを使用するには、プロトコルタイプとして「both（nfsv3 / NFSv4.1）」を選択する必要があります。

通常のUNIXモードビットでは、NTFSまたはNFSv4.x ACLが提供する権限レベルは異なります。次の表に、NFSv3モードビットとNFSv4.1 ACLの権限の単位を比較します。NFSv4.1 ACLの詳細については、を参照してください "nfs4_acl - NFSv4アクセス制御リスト"。

NFSv3 モードビット	**NFSv4.1 ACL**
• 実行時にユーザーIDを設定します • 実行時にグループIDを設定します • スワップしたテキストを保存する(POSIXでは定義されていません • 所有者の読み取り権限 • 所有者の書き込み権限 • ファイルの所有者の実行権限、またはディレクトリ内の所有者の検索（検索）権限 • グループの読み取り権限 • グループの書き込み権限 • ファイル上のグループの実行権限、またはディレクトリ内のグループの検索（検索）権限 • 他のユーザーの読み取り許可 • 他のユーザーの書き込み許可 • ファイルに対する他のユーザーのアクセス許可を実行するか、ディレクトリ内の他のユーザーの検索(検索)アクセス許可を設定します	Access Control Entry（ACE;アクセス制御エントリ）タイプ（Allow/Deny/Audit）継承フラグ directory-inherit * file-inherit * no-propage-inherit * inherit-only Permissions * read-data（ファイル）/list-directories* write-data（ディレクトリ）* write-data（ファイル）/create-file（ディレクトリ）* append-data/create-subdirectory（ディレクトリ）* execute（ファイル）/change-directory（ディレクトリ）* delete * delete -child * read-write attributes * read-write -named-acl属性* read-write -acl属性* write-owner-acl属性*

最後に、NFSグループメンバーシップ（NFSv3とNFSv4.xの両方）は、RPCパケットの制限に従い、AUTH_SYSでのデフォルトの最大数である16に制限されています。NFS Kerberosでは、最大32のグループとNFSv4 ACLが提供され、ユーザおよびグループのACLをより細かく設定できるため（ACEごとに最大1024エントリ）、この制限は解消されます。

さらに、Cloud Volumes Service では、サポートされる最大グループ数を最大32まで拡張する拡張グループサポートが提供されています。そのためには、有効なUNIXユーザおよびグループのIDを含むLDAPサーバへのLDAP接続が必要です。この設定の詳細については、を参照してください "NFSボリュームの作成と管理" Googleのドキュメントを参照してください。

NFSv3のユーザIDとグループID

NFSv3のユーザIDとグループIDは、名前ではなく数値IDでネットワークに送信される。NFSv3では、UNIXセキュリティ形式のボリュームでモードビットのみを使用する場合、これらの数値IDに対するCloud Volumes Service でのユーザ名の解決は行われません。NFSv4.1 ACLが存在する場合は、NFSv3を使用している場合でも、ACLを適切に解決するために数値ID検索と名前文字列検索が必要です。NTFSセキュリティ形式のボリュームでは、Cloud Volumes Service が数値IDを有効なUNIXユーザに解決してから、有効なWindowsユーザにマッピングして、アクセス権をネゴシエートする必要があります。

NFSv3のユーザIDとグループIDのセキュリティ制限

NFSv3では、クライアントとサーバは、ユーザが数値IDで読み取りまたは書き込みを実行しようとしても、有効であることを確認する必要はありません。これは暗黙的に信頼されます。これにより、任意の数値IDをスプーフィングするだけで、ファイルシステムが侵害される可能性があります。このようなセキュリティホールを回避するために、Cloud Volumes Service にはいくつかのオプションがあります。

- NFSにKerberosを実装すると、ユーザはユーザ名とパスワードまたはkeytabファイルを使用して認証を受け、Kerberosチケットを取得してマウントにアクセスできるようになります。KerberosはCVS -パフォーマンスインスタンスで使用でき、NFSv4.1でのみ使用できます。
- エクスポートポリシールールでホストのリストを制限することで、Cloud Volumes Service ボリュームにアクセスできるNFSv3クライアントを制限できます。
- デュアルプロトコルボリュームを使用し、NTFS ACLをボリュームに適用すると、NFSv3クライアントは数値IDを有効なUNIXユーザ名に解決して、マウントへのアクセスが正しく認証されるようになります。そのためには、LDAPを有効にし、UNIXのユーザおよびグループのIDを設定する必要があります
- rootユーザをスクワッシャすると、rootユーザがNFSマウントで実行できる損傷が制限されますが、リスクを完全に排除することはできません。詳細については、「」を参照してください[rootユーザ]」

最終的に、NFSセキュリティは、使用しているプロトコルのバージョンによって制限されます。NFSv3は、NFSv4.1よりもパフォーマンスが高いのに対し、セキュリティレベルは異なります。

NFSv4.1

NFSv4.1は、次の理由から、NFSv3に比べてセキュリティと信頼性に優れています。

- リースベースのメカニズムによる統合ロック
- ステートフルセッション
- 1つのポートですべてのNFS機能（2049）
- TCPのみ
- IDドメインマッピング
- Kerberos統合（NFSv3ではKerberosを使用できますが、NFSのみを使用でき、NLMなどの補助プロトコルは使用できません）

NFSv4.1の依存関係

NFSv4.1のセキュリティ機能に加えて、NFSv3を使用するために必要とされなかった外部の依存関係もいくつかあります（SMBでActive Directoryなどの依存関係が必要とされる方法と似ています）。

NFSv4.1 ACL

Cloud Volumes Service では、NFSv4.x ACLがサポートされています。NFSv4.x ACLは、次のような通常のPOSIX形式の権限とは異なる利点があります。

- ファイルやディレクトリへのユーザアクセスの詳細な制御
- NFS セキュリティが向上します
- CIFS / SMBとの相互運用性が向上しました
- AUTH_SYSのセキュリティが設定された、ユーザあたり16個のグループに関するNFSの制限を削除
- ACLはグループID（GID）の解決の必要性をバイパスします。これにより、実質的にGIDの制限を解除することができ、Cloud Volumes Service からではなくNFSクライアントからNFSv4.1 ACLが制御されます。NFSv4.1 ACLを使用するには、クライアントのソフトウェアバージョンでサポートされていること、および適切なNFSユーティリティがインストールされていることを確認してください。

NFSv4.1 ACLとSMBクライアントの互換性

NFSv4 ACLはWindowsのファイルレベルのACL（NTFS ACL）とは異なりますが、同様の機能を備えています。ただし、マルチプロトコルNAS環境でNFSv4.1 ACLが存在し、デュアルプロトコルアクセス（同じデータセットでNFSおよびSMB）を使用している場合、SMB2.0以降を使用するクライアントは、WindowsのセキュリティタブでACLを表示または管理できません。

NFSv4.1 ACLの仕組み

参考のために、次の用語が定義されています。

- *アクセス制御リスト(ACL)。*アクセス権エントリのリスト。
- *アクセス制御エントリ(ACE)。*リスト内のアクセス許可エントリ。

クライアントがSETATTR操作でファイルにNFSv4.1 ACLを設定すると、Cloud Volumes Service は既存のACLに替わってそのACLをオブジェクトに設定します。ファイルにACLが設定されていない場合、ファイルのモード権限はOWNER@、GROUP@、およびEVERYONE@から計算されます。ファイルにSUID / SGID / STICKYのいずれかのビットが設定されている場合、それらのビットは影響を受けません。

クライアントがGETATTR操作でファイルのNFSv4.1 ACLを取得すると、Cloud Volumes Service はオブジェクトに関連付けられたNFSv4.1 ACLを読み取り、ACEのリストを作成してクライアントに返します。ファイルにNT ACLまたはモードビットが設定されている場合は、モードビットからACLが構築されてクライアントに返されます。

ACLにDENY ACEが存在する場合はアクセスが拒否され、ALLOW ACEが存在する場合はアクセスが許可されます。ただし、ACLにどちらのACEも存在しない場合も、アクセスが拒否されます。

セキュリティ記述子は、セキュリティACL（SACL）と随意ACL（DACL）で構成されます。NFSv4.1がCIFS / SMBと連動する場合は、DACLはNFSv4とCIFSに1対1でマッピングされます。DACLは、ALLOW ACEとDENY ACEで構成されます。

NFSv4.1 ACLが設定されたファイルまたはフォルダに対して基本的なchmodを実行すると、既存のユーザおよびグループのACLは維持されますが、デフォルトのOWNER@、GROUP@、およびEVERYONE@ ACLが変更されます。

NFSv4.1 ACLを使用するクライアントは、システム上のファイルとディレクトリにACLを設定し、そのACLを表示することができます。ACLが設定されているディレクトリ内にファイルやサブディレクトリを新しく作成すると、そのオブジェクトは、該当するACLでタグ付けされているACEをすべて継承します "継承フラグ"。

ファイルまたはディレクトリにNFSv4.1 ACLが設定されている場合、そのACLを使用して、ファイルまたはディレクトリへのアクセスにどのプロトコルが使用されるかに関係なく、アクセスが制御されます。

親ディレクトリのNFSv4 ACLのACEに正しい継承フラグが設定されていれば、ファイルやディレクトリは該当するACEを継承します（必要な変更が加えられる可能性があります）。

ファイルやディレクトリがNFSv4要求によって作成される場合、作成されるファイルやディレクトリのACLは、ファイル作成要求にACLが含まれているか、または標準のUNIXファイルアクセス権限のみが含まれているかによって異なります。また、親ディレクトリにACLが設定されているかどうかによっても異なります。

- 要求に ACL が含まれる場合は、その ACL が使用されます。
- 要求に標準の UNIX ファイルアクセス権限のみが含まれ、親ディレクトリに ACL がない場合は、クライアントのファイルモードを使用して標準の UNIX ファイルアクセス権限が設定されます。
- 要求に標準UNIXファイルアクセス権限のみが含まれ、親ディレクトリに継承できないACLがある場合は、要求で渡されたモードビットに基づいてデフォルトのACLが設定されます。
- 要求に標準 UNIX ファイルアクセス権限のみが含まれ、親ディレクトリに ACL がある場合、親ディレクトリの ACL の ACE に適切な継承フラグのタグが付けられていれば、それらの ACE が新しいファイルやディレクトリに継承されます。

ACE権限

NFSv4.1 ACLの権限では、大文字と小文字のアルファベットの一連の値（「rxtncy」など）を使用してアクセスが制御されます。これらの文字の値の詳細については、を参照してください "方法: NFSv4 ACLを使用します"。

umaskおよび**ACL**の継承が設定された**NFSv4.1 ACL**の動作

"NFSv4 ACLでは、ACLを継承することができます"。ACLの継承では、NFSv4.1 ACLが設定されているオブジェクトの下に作成されるファイルやフォルダに、の設定に基づいてACLを継承することができます "ACL継承フラグ"。

"umask" は、管理者とのやり取りなしでディレクトリ内にファイルやフォルダを作成する権限レベルを制御するために使用します。デフォルトでは、Cloud Volumes Service は継承されたACLをumaskによって上書きします。これは、の想定される動作です "RFC 5661"。

ACLのフォーマット

NFSv4.1 ACLには特定の形式があります。次の例は、ファイルに設定されたACEを示しています。

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

上記の例では、のACL形式のガイドラインに従います。

```
type:flags:principal:permissions
```

「A」のタイプは「許可」を意味します。 継承フラグはこの場合は設定されません。これは、プリンシパルがグループではなく、継承も含まれないためです。また、ACEは監査エントリではないため、監査フラグを設定する必要もありません。NFSv4.1 ACLの詳細については、を参照してください "http://linux.die.net/man/5/nfs4_acl"。

NFSv4.1 ACLが適切に設定されていない場合（またはクライアントとサーバが名前文字列を解決できない場合）、ACLが想定どおりに動作しないか、ACLの変更を適用できずにエラーがスローされる可能性があります。

エラーの例は次のとおりです。

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

明示的な**DENY**

NFSv4.1の権限では、OWNER、GROUP、およびEVERYONEに対する明示的なDENY属性を含めることができます。これは、NFSv4.1 ACLがdefault-denyであるためです。つまり、ACEによってACLが明示的に許可されなければ、ACLは拒否されます。明示的なDENY属性は、明示的なアクセスACEを上書きします。

拒否ACEは'D'の属性タグで設定されます

次の例では、group@はすべての読み取りおよび実行権限を許可していますが、すべての書き込みアクセスは拒否されています。

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

DENY ACEは複雑で混乱を招く可能性があるため、できるかぎり使用しないでください。明示的に定義されていないACLは暗黙的に拒否されます。DENY ACEを設定すると、アクセスを許可されるはずのユーザがアクセスを拒否される場合があります。

上記の一連のACEは、モードビットの755に相当します。つまり、次のようになります。

- 所有者にはフルアクセス権があります。
- グループは読み取り専用です。
- 読み取り専用のものもあります。

ただし、775と等しくなるように権限が調整されていても、EVERYONEに明示的なDENYが設定されているとアクセスが拒否される可能性があります。

NFSv4.1 IDドメインのマッピングの依存関係

NFSv4.1では、セキュリティレイヤとしてIDドメインのマッピングロジックを利用して、NFSv4.1マウントへのアクセスを試みるユーザが、そのユーザの要求を実際に把握できるかどうかを検証します。このような場合は、NFSv4.1クライアントからのユーザ名とグループ名に名前文字列が付加されて、Cloud Volumes Service インスタンスに送信されます。ユーザ名/グループ名とID文字列の組み合わせが一致しない場合は’クライアントの/etc/idmapd.confファイルに指定されているデフォルトのnobodyユーザにユーザまたはグループが引き下げられます

このID文字列は、特にNFSv4.1 ACLやKerberosを使用している場合に、適切な権限を順守するための要件です。そのため、ユーザやグループの名前IDが正しく解決されるように、クライアントとCloud Volumes Service 間で一貫性を確保するためには、LDAPサーバなどのネームサービスサーバに依存する必要があります。

Cloud Volumes Service は’静的なデフォルトIDドメイン名値defaultv4iddomain.comを使用しますNFSクライアントはデフォルトで’IDドメイン名設定のDNSドメイン名になりますが'/etc/idmapd.confでIDドメイン名を手動で調整できます

Cloud Volumes Service でLDAPが有効になっている場合、Cloud Volumes Service はNFS IDドメインを自動化して、DNSの検索ドメインに設定されている内容に変更します。クライアントは、別のDNSドメイン検索名を使用しない限り、変更する必要はありません。

Cloud Volumes Service がローカルファイルまたはLDAPでユーザ名またはグループ名を解決できる場合は、ドメイン文字列が使用され、一致しないドメインIDが引き下げられてnobodyになります。ローカルファイルまたはLDAPでユーザ名またはグループ名が見つからない場合Cloud Volumes Service は、数値のID値が使用され、NFSクライアントが名前を適切に解決します（NFSv3の動作と似ています）。

クライアントのNFSv4.1 IDドメインを、Cloud Volumes Service ボリュームで使用されているものと一致するように変更しないと、次のような動作が発生します。

- Cloud Volumes Service 内にローカルエントリがあるUNIXユーザおよびグループ（ローカルのUNIXユーザとグループで定義されているrootなど）は、nobody値に引き下げられます。
- LDAP内にエントリがあるUNIXユーザおよびグループ（Cloud Volumes Service でLDAPを使用するように設定されている場合）は、NFSクライアントとCloud Volumes Service でDNSドメインが異なる場合、そのハッシュがnobodyに引き下げられます。
- ローカルエントリやLDAPエントリがないUNIXユーザおよびグループは、数値ID値を使用して、NFSクライアントで指定された名前に解決されます。クライアントに名前が存在しない場合は、数値IDのみが表示されます。

上記のシナリオの結果を次に示します。

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

クライアントとサーバIDのドメインが一致した場合、同じファイルリストが表示されます。

```
# ls -la
total 8
drwxr-xr-x 2 root   root         4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root         4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835         9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

この問題 とその解決方法の詳細については、「」を参照してくださいNFSv4.1およびnobodyユーザ/グループ」

Kerberosの依存関係

NFSでKerberosを使用する場合は、Cloud Volumes Service で次の要件を満たす必要があります。

- Kerberosキー配布センターサービス（KDC）用のActive Directoryドメイン
- LDAP機能のUNIX情報を入力したユーザおよびグループの属性を持つActive Directoryドメイン（Cloud Volumes Service のNFS Kerberosでは、正常に機能するためにユーザのSPNからUNIXユーザのマッピングが必要です）。
- Cloud Volumes Service インスタンスでLDAPが有効になっている
- DNSサービスのActive Directoryドメインを指定します

NFSv4.1および**nobody**ユーザ/グループ

NFSv4.1設定でよく見られる問題の1つは、「user:group」の「nobody：nobody」の組み合わせによって所有されている「ls」を使用して一覧にファイルまたはフォルダが表示される場合です。

例：

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

数値IDは「99」です。

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

場合によっては、ファイルに正しい所有者が表示されることもありますが、グループとして「nobody」が表示されることもあります。

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

誰もいないのですか？

NFSv4.1のnobodyユーザはnfsnobodyユーザとは異なりますNFSクライアントが各ユーザーをどのように認識するかを表示するには'id'コマンドを実行します

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

NFSv4.1では'idmapd.confファイルによって定義されたデフォルトのユーザである'nobod'ユーザを使用する任意のユーザとして定義できます

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

なぜそうなるのでしょうか？

NFSv4.1の処理では、ネーム文字列マッピングによるセキュリティが重要な条件となるため、名前文字列が適切に一致しない場合のデフォルトの動作は、ユーザとグループが所有するファイルやフォルダに通常アクセスできないユーザの引き下げです。

ファイルの一覧にユーザまたはグループの「nobody」が表示される場合は、通常、NFSv4.1の設定が誤っています。ここでは、大文字と小文字の区別が使用されます。

たとえば、user1@CVSDEMO.LOCA L（uid 1234、gid 1234）がエクスポートにアクセスしている場合、Cloud Volumes Service はuser1@CVSDEMO.LOCA L（uid 1234、gid 1234）を検索できる必要があります。Cloud Volumes Service のユーザがUSER1@CVSDEMO.LOCA Lの場合、ユーザは一致しません（大文字のUSER1と小文字のuser1）。多くの場合、クライアント上のメッセージファイルに次の情報が表示されます。

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

クライアントとサーバーは、ユーザーが実際に誰を要求しているかに同意する必要があります。そのため、Cloud Volumes Service が表示するユーザーと同じ情報がクライアントに表示されることを確認するには、次の項目を確認する必要があります。

- **NFSv4.x ID domain.** Client:idmapd.confファイル。Cloud Volumes Service は「defaultv4iddomain.com」を使用しており、手動で変更することはできません。Cloud Volumes Service でNFSv4.1を使用する場合、DNS検索ドメインのIDドメインが、ADドメインと同じになるように変更されます。
- *ユーザー名と数値ID。*これは、クライアントがユーザー名を検索し、ネームサービススイッチ構成を利用する場所を決定します。client:nsswitch.conf'ローカルpasswdファイルとgroupファイルのいずれかまたは両方を使用します。Cloud Volumes Service では、この変更は許可されませんが、有効になっている場合は自動的にLDAPが構成に追加されます。
- *グループ名と数値ID。*これは、クライアントがグループ名を検索し、ネームサービススイッチ構成を利用する場所を決定します。client:nsswitch.conf'ローカルpasswdおよびgroupファイルのいずれかまたは両方を使用します。Cloud Volumes Service では、この変更は許可されていませんが、有効になっている場合は自動的にLDAPが構成に追加されます。

ほとんどの場合、クライアントからのユーザおよびグループの一覧に「nobody」が表示された場合、問題はCloud Volumes Service とNFSクライアント間でのユーザまたはグループの名前ドメインIDの変換です。この状況を回避するには、LDAPを使用して、クライアントとCloud Volumes Service 間でユーザおよびグループの情報を解決します。

クライアントでの**NFSv4.1**の名前**ID**文字列の表示

NFSv4.1を使用している場合、前述のように、NFS処理で実行される名前文字列のマッピングが存在します。

/var/log/messagesを使用してNFSv4 IDを持つ問題 を検索することに加え、を使用することもできます "nfsidmap -l" NFSクライアント上でコマンドを実行すると、NFSv4ドメインに適切にマッピングされているユーザ名が表示されます。

たとえば、クライアントで検出されたユーザとCloud Volumes Service がNFSv4.xマウントにアクセスすると、次のようなコマンドが出力されます。

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

NFSv4.1 IDドメインに適切にマッピングされていないユーザ（この場合「netapp -user」）が同じマウントにアクセスしてファイルにアクセスしようとすると、「nobody：nobody」が割り当てられます（想定どおり）。

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

「nfsidmap -l」の出力には、ユーザ「pcuser」が表示されますが、「NetApp-user」は表示されません。これは、エクスポートポリシールールの匿名ユーザ（「65534」）です。

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

SMB

"SMB" は、Microsoftが開発したネットワークファイル共有プロトコルです。ユーザ/グループの認証、権限、ロック、およびファイル共有を、イーサネットネットワークを介して複数のSMBクライアントに一元的に提供します。ファイルとフォルダは共有を通じてクライアントに提供されます。共有は、さまざまな共有プロパティを設定したり、共有レベルの権限を通じてアクセスを制御したりすることができます。SMBは、Windows、Apple、Linuxクライアントなど、このプロトコルをサポートする任意のクライアントに提供できます。

Cloud Volumes Service では、SMB 2.1および3.xバージョンのプロトコルがサポートされます。

アクセス制御/ SMB共有

- Windowsユーザ名がCloud Volumes Service ボリュームへのアクセスを要求すると、Cloud Volumes Service はCloud Volumes Service 管理者が設定した方法を使用してUNIXユーザ名を検索します。
- 外部UNIXアイデンティティ・プロバイダ（LDAP）が設定されていて、Windows/UNIXユーザ名が同一の場合、Windowsユーザ名は、追加の設定を必要とせずに1:1でUNIXユーザ名にマッピングされます。LDAPを有効にすると、Active Directoryを使用してユーザオブジェクトとグループオブジェクト

のUNIX属性がホストされます。

- Windows名とUNIX名が同じ設定にならない場合は、Cloud Volumes Service がLDAPネームマッピングの設定を使用できるようにLDAPを設定する必要があります（を参照）"「LDAPを使用した非対称ネームマッピング」"）。
- LDAPが使用されていない場合、Windows SMBユーザは、Cloud Volumes Service で「pcuser」という名前のデフォルトのローカルUNIXユーザにマッピングされます。つまり'マルチプロトコルのNAS環境では'pcuserにマップされているユーザーによってWindowsに書き込まれたファイルは'UNIXの所有権をpcuserとして表示しますここでは'pcuserがLinux環境では'nobodyユーザー（UID 65534）となっています

SMBのみの導入では、「pcuser」のマッピングは引き続き有効ですが、Windowsのユーザとグループの所有権が正しく表示され、SMBのみのボリュームへのNFSアクセスは許可されないため、問題ありません。また、SMBのみのボリュームでは、NFSまたはデュアルプロトコルのボリューム作成後のボリュームへの変換はサポートされません。

Windowsは、Active Directoryドメインコントローラでのユーザ名認証にKerberosを使用します。これには、Cloud Volumes Service インスタンスの外部にあるAD DCとのユーザ名/パスワードの交換が必要です。Kerberos認証は'\\servername'UNCパスがSMBクライアントによって使用され'次の場合に使用されます

- servernameにはDNS A/AAAAエントリがあります
- servernameに対するSMB / CIFSアクセス用の有効なSPNが存在します

Cloud Volumes Service SMBボリュームを作成すると、セクションの定義に従ってマシンアカウント名が作成されます"「Cloud Volumes Service がActive Directoryにどのように表示されるか」" Cloud Volumes Service は動的DNS（DDNS）を利用してDNSに必要なA/AAAAエントリとPTRエントリ、マシンアカウントプリンシパルの必要なSPNエントリを作成するため、そのマシンアカウント名もSMB共有アクセスパスになります。

> PTRエントリを作成するには、Cloud Volumes Service インスタンスIPアドレスの逆引き参照ゾーンがDNSサーバ上に存在している必要があります。

たとえば、このCloud Volumes Service ボリュームはUNC共有パス「\\cvs-east-433d.cvsdemo.local」を使用します。

Active Directoryでは、次のエントリがCloud Volume サービスによって生成されたSPNエントリです。

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

DNS前方/後方参照の結果は次のとおりです。

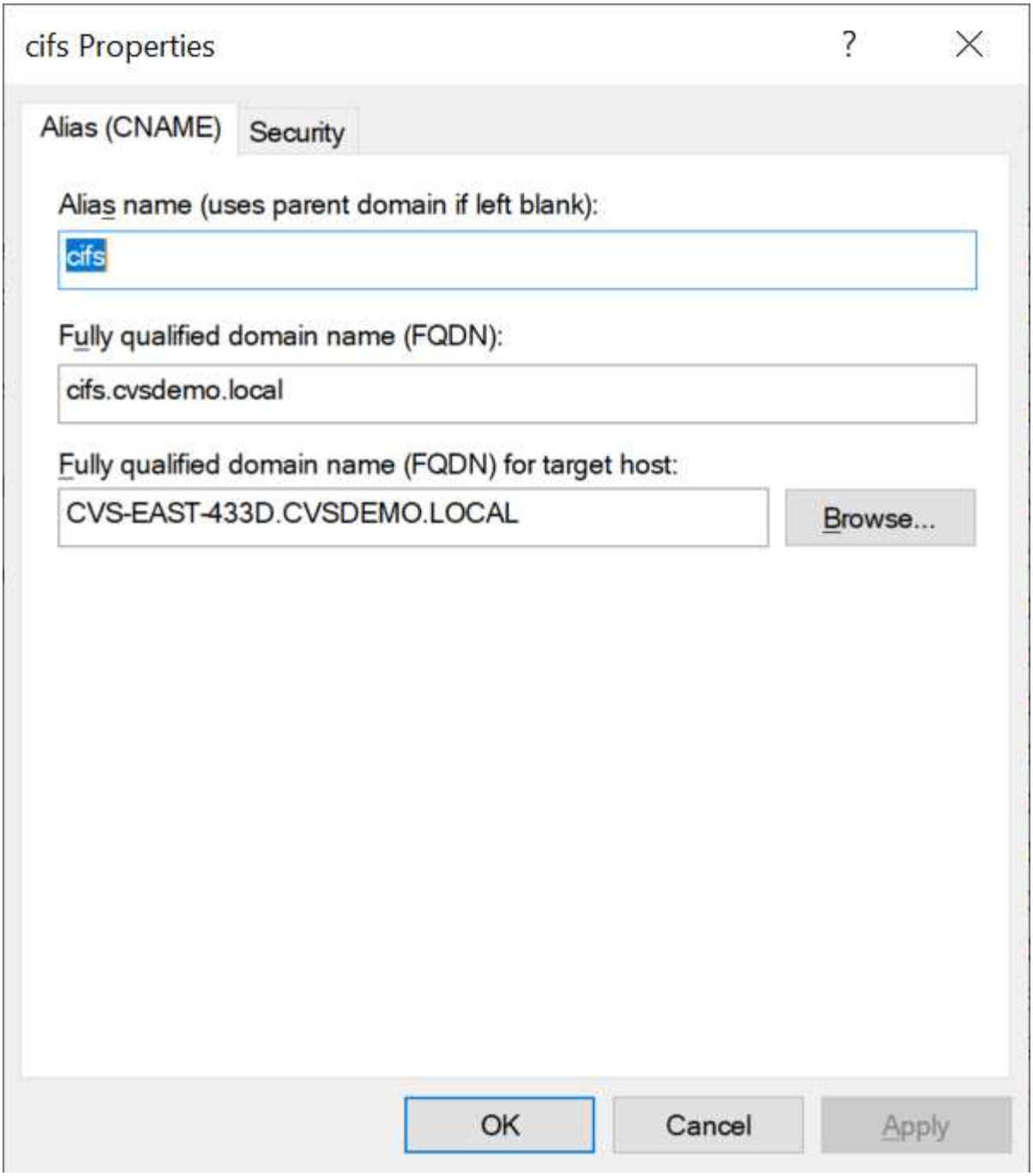
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

必要に応じて、Cloud Volumes Service 内のSMB共有に対してSMB暗号化を有効または要求することで、より多くのアクセス制御を適用できます。いずれかのエンドポイントでSMB暗号化がサポートされていない場合、アクセスは許可されません。

SMB名エイリアスを使用する

場合によっては、エンドユーザがCloud Volumes Service で使用するマシンアカウント名を把握することがセキュリティ上の懸念事項になることがあります。また、単にエンドユーザへのアクセスパスを単純化することもできます。このような場合は、SMBエイリアスを作成できます。

SMB共有パスのエイリアスを作成する場合は、DNSでCNAMEレコードと呼ばれるものを利用できます。たとえば'\\cvs-east-433d.cvsdemo.local'ではなく''\\CIFS'という名前を使用して共有にアクセスするが'Kerberos認証を使用する場合は'A/AAAAレコードを指すDNSのCNAMEと'既存のマシンアカウントに追加されたSPNがKerberosアクセスを提供します



CNAMEを追加したあとのDNS前方参照の結果を次に示します。

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

新しいSPNを追加したあとのSPNクエリの結果を次に示します。

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

パケットキャプチャでは、CNAMEに関連付けられたSPNを使用してセッション設定要求を確認できます。

```
431 4.156722                                    SMB2    308 Negotiate Protocol Response
432 4.156785                                    SMB2    232 Negotiate Protocol Request
434 4.158108                                    SMB2    374 Negotiate Protocol Response
435 4.160977                                    SMB2   1978 Session Setup Request
437 4.166224                                    SMB2    322 Session Setup Response
438 4.166891                                    SMB2    152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063                                    SMB2    138 Tree Connect Response
```

```
    realm: CVSDEMO.LOCAL
  ⌄ sname
      name-type: kRB5-NT-SRV-INST (2)
    ⌄ sname-string: 2 items
        SNameString: cifs
        SNameString: cifs
  ⌄ enc-part
      etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

SMB認証ダイアレクト

Cloud Volumes Service では、次の機能がサポートされ "方言" SMB認証の場合：

- LM
- NTLM
- NTLMv2
- Kerberos

SMB共有アクセスのKerberos認証は、使用できる最も安全な認証レベルです。AESおよびSMB暗号化が有効になっていると、セキュリティレベルがさらに向上します。

Cloud Volumes Service では、LMおよびNTLM認証の下位互換性もサポートされています。Kerberosの設定が正しくない場合（SMBエイリアスの作成時など）、共有アクセスはより脆弱な認証方法（NTLMv2など）にフォールバックされます。これらのメカニズムは安全性が低いため、一部のActive Directory環境では無効になっています。より脆弱な認証方法が無効になっていて、Kerberosが適切に設定されていない場合、フォールバックする有効な認証方法がないため、共有アクセスは失敗します。

Active Directoryでサポートされている認証レベルの設定/表示については、を参照してください "ネットワークセキュリティ：LAN Manager認証レベル"。

アクセス許可モデル

NTFS /ファイル権限

NTFS権限とは、NTFSロジックに準拠したファイルシステム内のファイルおよびフォルダに適用される権限です。NTFSアクセス権は'Basic'または'Advanced'で適用でき'アクセス制御の場合は'allow'または[Deny]に設定できます

基本的な権限は次のとおりです。

- フルコントロール
- 変更
- 読み取りと実行
- 読み取り
- 書き込み

ACEと呼ばれるユーザまたはグループに権限を設定すると、ACLに含まれます。NTFS権限では、UNIXモードビットと同じ読み取り/書き込み/実行の基本が使用されますが、所有権の取得、フォルダの作成/追加、データの書き込み、属性の書き込みなど、より詳細で拡張されたアクセス制御（特別な権限）にも拡張できます。

標準UNIXモードビットは、NTFSアクセス権と同じレベルの粒度を提供しません（ACL内の個々のユーザおよびグループオブジェクトにアクセス権を設定したり、拡張属性を設定したりすることなど）。ただし、NFSv4.1 ACLは、NTFS ACLと同じ機能を提供します。

NTFS権限は共有権限よりも限定的であり、共有権限と組み合わせて使用できます。NTFSの権限構造では、最も制限があります。このため、アクセス権を定義するときに、ユーザまたはグループに対する明示的な拒否もフルコントロールよりも優先されます。

NTFSアクセス権はWindows SMBクライアントから制御されます。

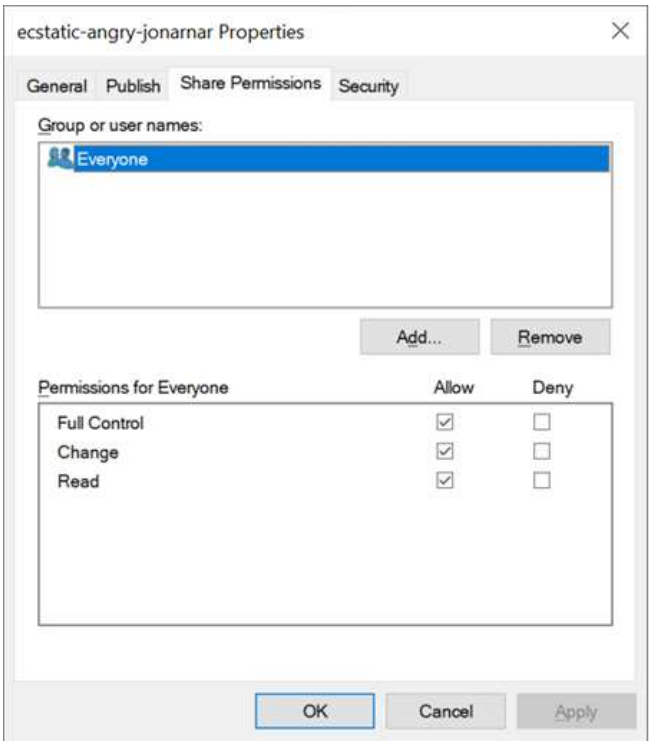
共有権限

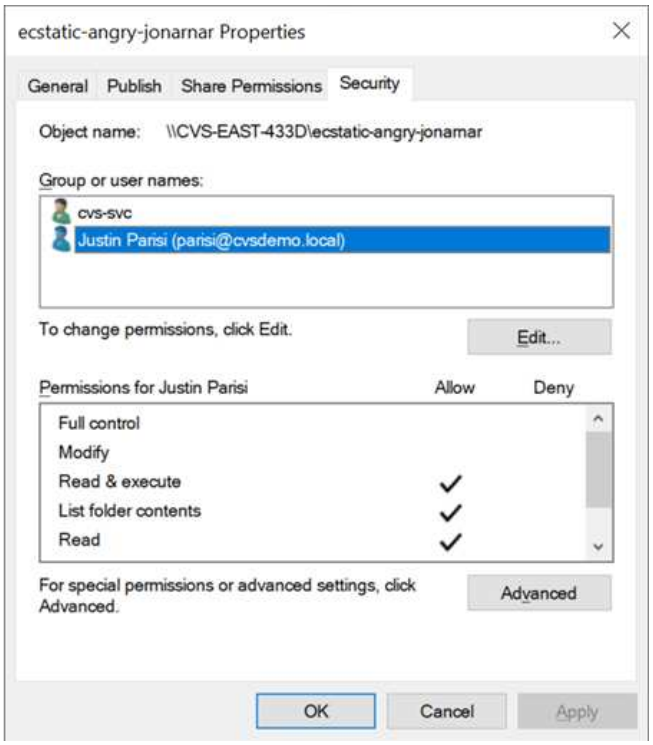
共有権限は、NTFS権限（読み取り/変更/フルコントロールのみ）よりも一般的で、NFSエクスポートポリシールールの仕組みと同様に、SMB共有への最初のエントリを制御します。

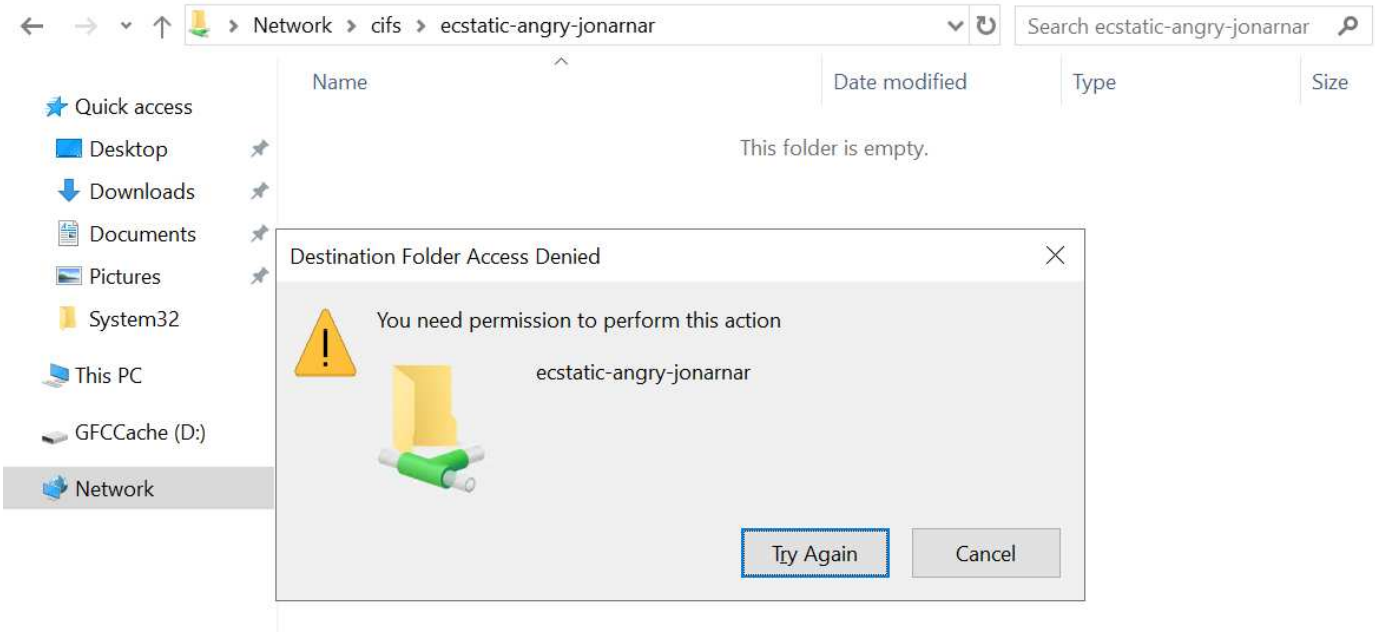
NFSエクスポートポリシールールは、IPアドレスやホスト名などのホストベースの情報を介したアクセスを制御しますが、SMB共有権限は共有ACLでユーザおよびグループACEを使用してアクセスを制御できます。共有ACLは、WindowsクライアントまたはCloud Volumes Service 管理UIから設定できます。

デフォルトでは、共有ACLと初期ボリュームACLにはフルコントロールを使用したすべてのメンバーが含まれます。ファイルACLを変更する必要がありますが、共有内のオブジェクトのファイル権限によって共有権限が上書きされます。

たとえば、ユーザにCloud Volumes Service ボリュームファイルACLへの読み取りアクセスのみが許可されている場合、次の図に示すように、共有ACLがフルコントロールを使用するEveryoneに設定されていても、ファイルおよびフォルダの作成アクセスは拒否されます。







セキュリティ上の最善の結果を得るには、次の手順を実行します。

- 共有およびファイルのACLからすべてのユーザを削除し、代わりにユーザまたはグループの共有アクセスを設定します。
- 個々のユーザではなくグループを使用してアクセス制御を行うと、管理が容易になり、グループ管理を通じてユーザの削除や追加を迅速に行うことができます。
- 共有権限のACEに対する制限が厳しくなく、一般的な共有アクセスを許可し、ファイル権限を持つユーザとグループにロックダウンされて、より詳細なアクセス制御が可能になります。
- 明示的なDENY ACLは、ALLOW ACLより優先されるため、一般的に使用しないでください。ファイルシステムへのアクセスを迅速に制限する必要があるユーザまたはグループに対する明示的なDENY ACLの使

用を制限してください。

- に注意を払ってください "ACLの継承" 権限を変更する際の設定。ファイル数の多いディレクトリまたはボリュームの最上位で継承フラグを設定すると、そのディレクトリまたはボリュームの下の各ファイルに継承された権限が追加されます。 これにより、各ファイルの調整時に意図しないアクセス/拒否や権限の大幅な変更など、不要な動作が発生する可能性があります。

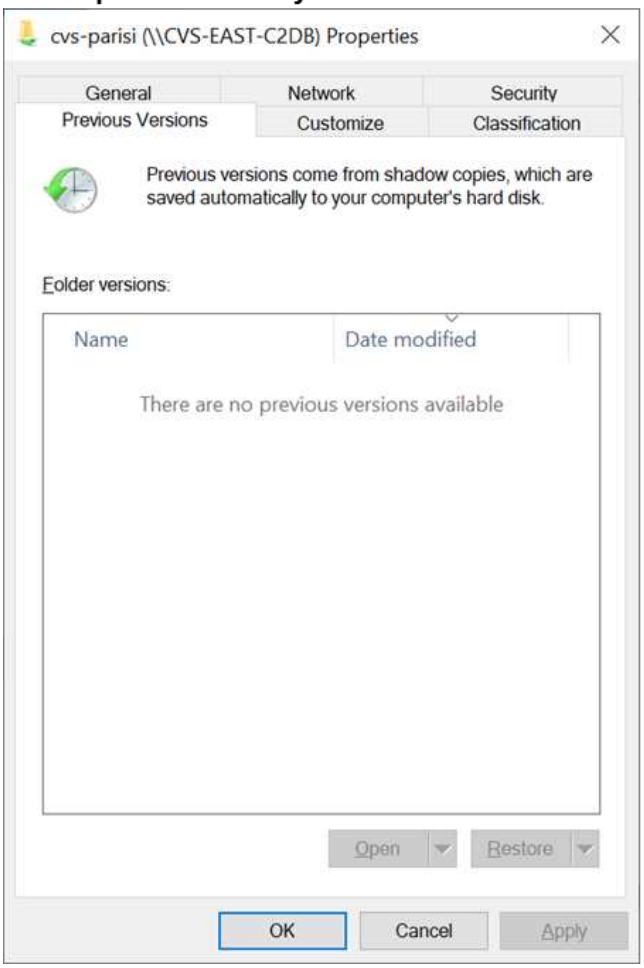
SMB共有のセキュリティ機能

Cloud Volumes Service でSMBアクセスを使用するボリュームを最初に作成するときに、そのボリュームを保護するための一連の選択肢が表示されます。

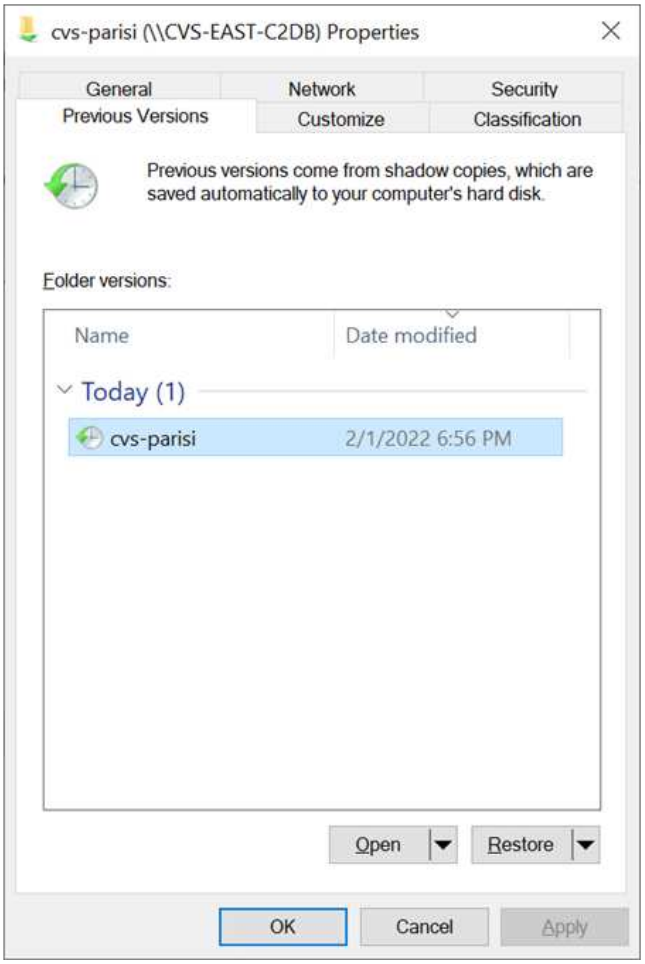
Cloud Volumes Service レベル（パフォーマンスまたはソフトウェア）に応じて、次の選択肢があります。

- *スナップショット・ディレクトリを表示する（CVS -パフォーマンスとCVS - SWの両方で利用可能）*このオプションはSMBクライアントがSMB共有内のスナップショット・ディレクトリにアクセスできるかどうかを制御します（\\server\share\~snapshotタブまたはPrevious Versionsタブ）。デフォルトの設定はチェックされませんボリュームのデフォルトは'~snapshot'ディレクトリへのアクセスを非表示にして拒否し'ボリュームの[以前のバージョン]タブにスナップショット・コピーは表示されません

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



セキュリティ上の理由、パフォーマンス上の理由（これらのフォルダをAVスキャンから非表示にする）、または設定上の理由から、エンドユーザに対してSnapshotコピーを非表示にすることが望ましい場合があります。Cloud Volumes Service スナップショットは読み取り専用であるため、これらのスナップショットが表示されていても、エンドユーザーはスナップショットディレクトリ内のファイルを削除または変更することはで

きません。Snapshotコピーが作成された時点のファイルまたはフォルダのファイル権限Snapshotコピー間でファイルまたはフォルダの権限が変更された場合、変更内容はSnapshotディレクトリ内のファイルまたはフォルダにも適用されます。ユーザとグループは、権限に基づいてこれらのファイルやフォルダにアクセスできます。Snapshotディレクトリ内のファイルの削除または変更はできませんが、ファイルまたはフォルダをSnapshotディレクトリからコピーすることは可能です。

- * SMB暗号化を有効にします（CVS -パフォーマンスとCVS - SWの両方で利用可能）。* SMB暗号化は、SMB共有ではデフォルトで無効になっています（オフ）。このチェックボックスをオンにすると、SMB暗号化が有効になります。つまり、SMBクライアントとサーバ間のトラフィックが、ネゴシエートされたサポート対象の最大暗号化レベルで転送中に暗号化されます。Cloud Volumes Service は、SMBで最大AES-256暗号化をサポートしています。SMB暗号化を有効にした場合、SMBクライアントが気づくことがあるパフォーマンス低下はありません。約10~20%の範囲になります。ネットアップでは、パフォーマンスへの影響が許容されるかどうかをテストで確認することを強く推奨してい
- * SMB共有を非表示にします（CVS -パフォーマンスとCVS - SWの両方に利用できます）。*このオプションを設定すると、SMB共有パスが通常の閲覧から見えなくなります。つまり、共有パスがわからないクライアントは、デフォルトのUNCパス（例：\\cvs-smb）にアクセスすると共有を参照できません。このチェックボックスをオンにすると、SMB共有パスを明示的に知っているクライアント、またはグループポリシーオブジェクトによって定義された共有パスを持つクライアントだけが、このパスにアクセスできます（難読化によるセキュリティ）。
- アクセスベースの列挙（**ABE**）を有効にします（**CVS - SW**のみ）。 SMB共有を非表示にするのと似ています。ただし、共有やファイルは、オブジェクトへのアクセス権限がないユーザまたはグループに対してのみ表示されます。たとえば、Windowsユーザ「joe」に許可されているアクセス許可で少なくとも読み取りアクセスが許可されていない場合、Windowsユーザ「joe」はSMB共有またはファイルをまったく表示できません。このオプションはデフォルトでは無効になっており、チェックボックスを選択することで有効にできます。ABEの詳細については、ネットアップの技術情報アーティクルを参照してください "アクセスベースの列挙（ABE）の仕組み"
- 継続的可用性（**CA**）共有のサポートを有効にします（**CVS -**パフォーマンスのみ）。 "継続的可用性を備えたSMB共有" Cloud Volumes Service バックエンドシステム内のノード間でロック状態をレプリケートすることで、フェイルオーバーイベント中のアプリケーションの停止を最小限に抑えることができます。これはセキュリティ機能ではありませんが、全体的な耐障害性は向上します。現在、この機能では、SQL ServerとFSLogixアプリケーションのみがサポートされています。

デフォルトの非表示共有

Cloud Volumes Service でSMBサーバを作成すると、その場所に配置されます "非表示の管理共有" データボリュームのSMB共有に加えて作成される（$命名規則を使用）。これには、C$（名前空間アクセス）とIPC$（Microsoft管理コンソール（MMC）へのアクセスに使用されるリモート手順 呼び出し（RPC）などのプログラム間の通信用の名前付きパイプの共有）が含まれます。

IPC$共有には共有ACLは含まれておらず、変更することはできません。これはRPC呼び出しおよびにのみ使用されます "Windowsは、これらの共有への匿名アクセスをデフォルトで禁止します"。

C$共有ではデフォルトでBUILTIN\Administratorsアクセスが許可されますが、Cloud Volumes Service 自動化によって共有ACLが削除され、C$共有へのアクセスによってCloud Volumes Service ファイルシステム内のマウントされたすべてのボリュームが可視化されるため、すべてのユーザにアクセスすることはできません。その結果'\\server\C$'への移動は失敗します

ローカル/ **BUILTIN**管理者/バックアップ権限を持つアカウント

Cloud Volumes Service SMBサーバは、選択したドメインユーザおよびグループにアクセス権を適用するローカルグループ（BUILTIN\Administratorsなど）があることに、通常のWindows SMBサーバと同様の機能を維持します。

バックアップユーザに追加するユーザを指定すると、そのActive Directory接続を使用するCloud Volumes Service インスタンスのBUILTIN\Backup Operatorsグループにユーザが追加され、が取得されます "SeBackupPrivilegeおよびSeRestorePrivilege"。

Security Privilegeユーザにユーザを追加すると、そのユーザにはSeSecurityPrivilegeが付与されます。これは、などの一部のアプリケーションユースケースで役立ちます "SMB共有上のSQL Server"。

Backup Users

Provide a comma separated list of domain users or a domain group name that require elevated privileges to access volumes created by Cloud Volumes Service.

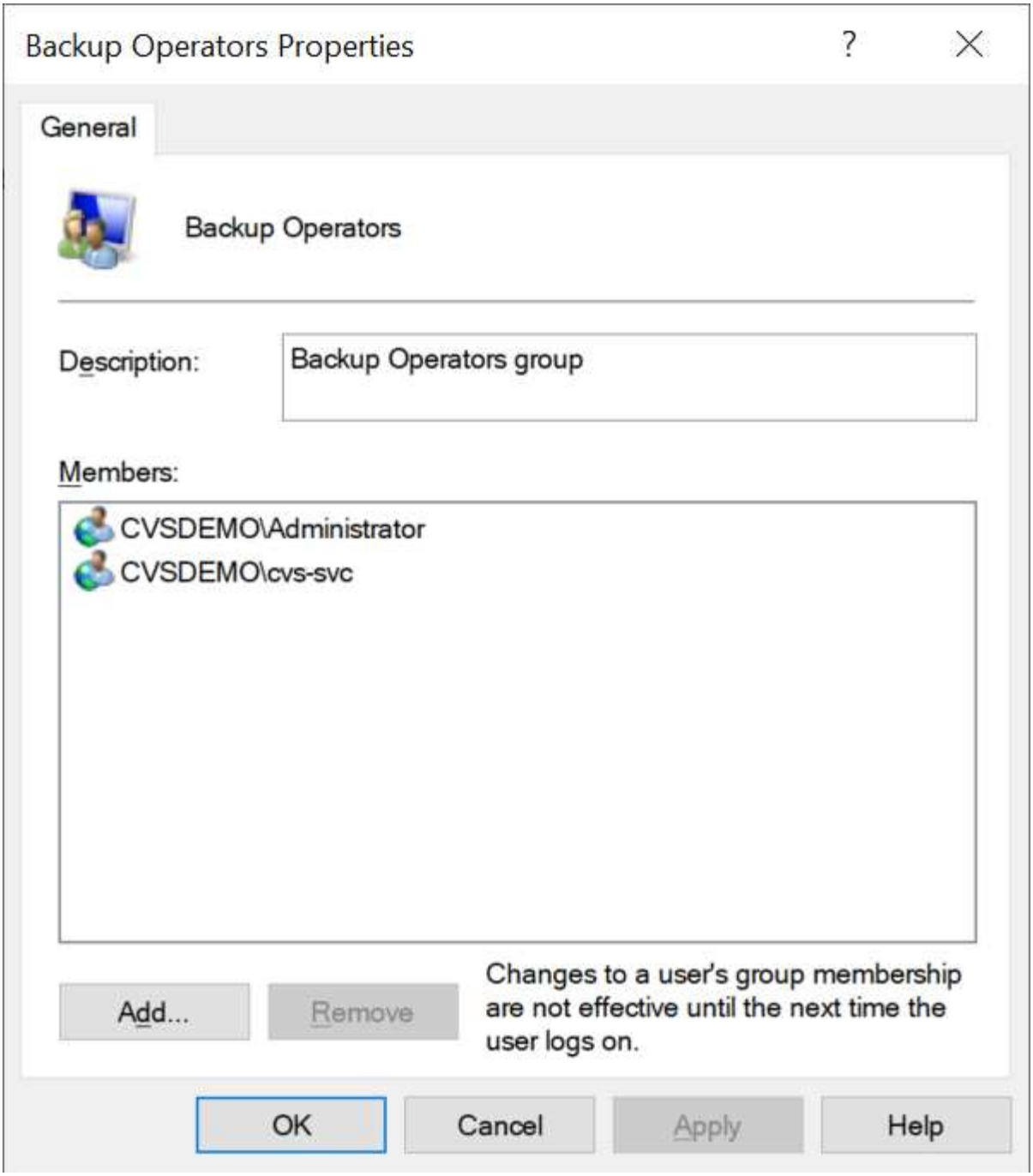
Accountnames
administrator,cvs-svc

Security Privilege Users

Provide a list of comma separated domain user accounts that require elevated privileges to manage security log for the Active Directory associated with Cloud Volumes Service.

Accountnames
administrator,cvs-svc

Cloud Volumes Service ローカルグループメンバーシップは、適切な権限を持つMMCを使用して表示できます。次の図に、Cloud Volumes Service コンソールを使用して追加されたユーザを示します。

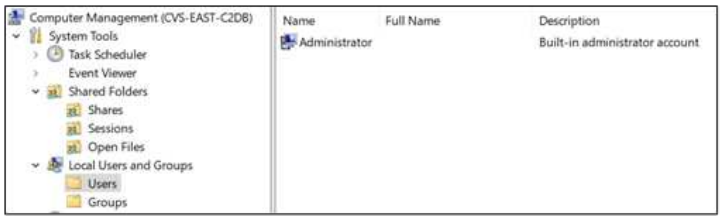


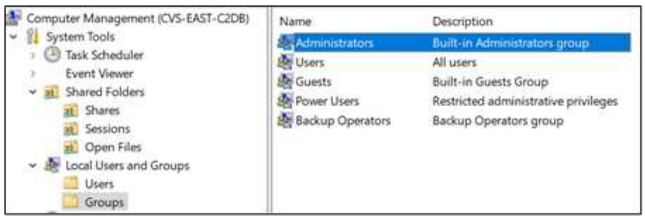
次の表に、デフォルトのBUILTINグループのリストと、デフォルトで追加されるユーザ/グループを示します。

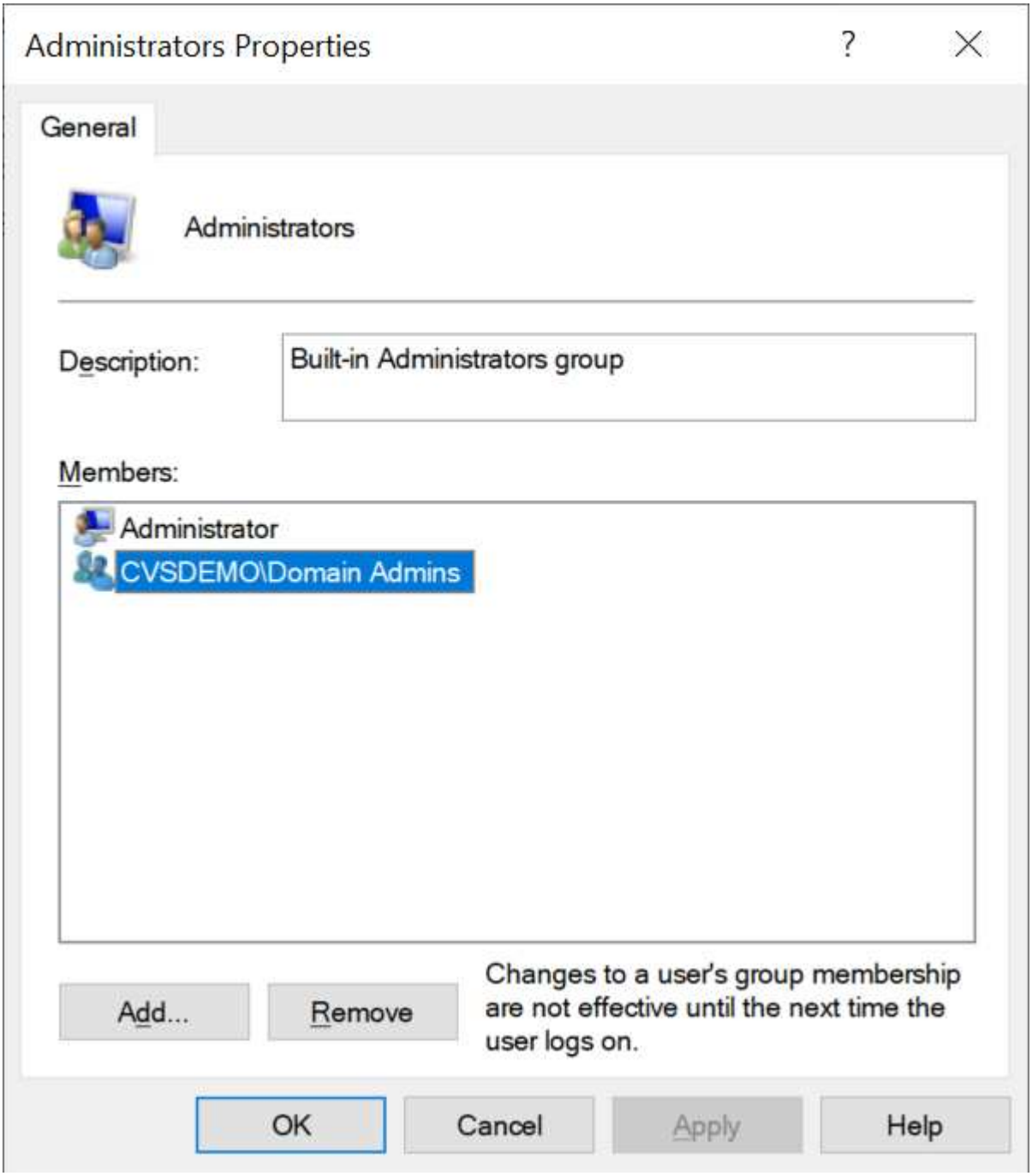
ローカル/ **BUILTIN**グループ	デフォルトのメンバー
builtin\Administrators*	Domain\Domain Adminsの略
Builtin\Backup Operators*	なし
組み込みのゲスト	Domain\Domainゲスト
Builtin\Power Usersの場合	なし
組み込みのドメインユーザ	Domain\Domain Usersの略

*グループメンバーシップはCloud Volumes Service Active Directory接続設定で制御されます。

MMCウィンドウにはローカルユーザとローカルグループ（およびグループメンバー）を表示できますが、このコンソールからオブジェクトの追加や削除、グループメンバーシップの変更はできません。デフォルトでは、Cloud Volumes Service のBUILTIN\AdministratorsグループとAdministratorのみが追加されます。現時点では、これを変更することはできません。







MMC /コンピュータ管理アクセス

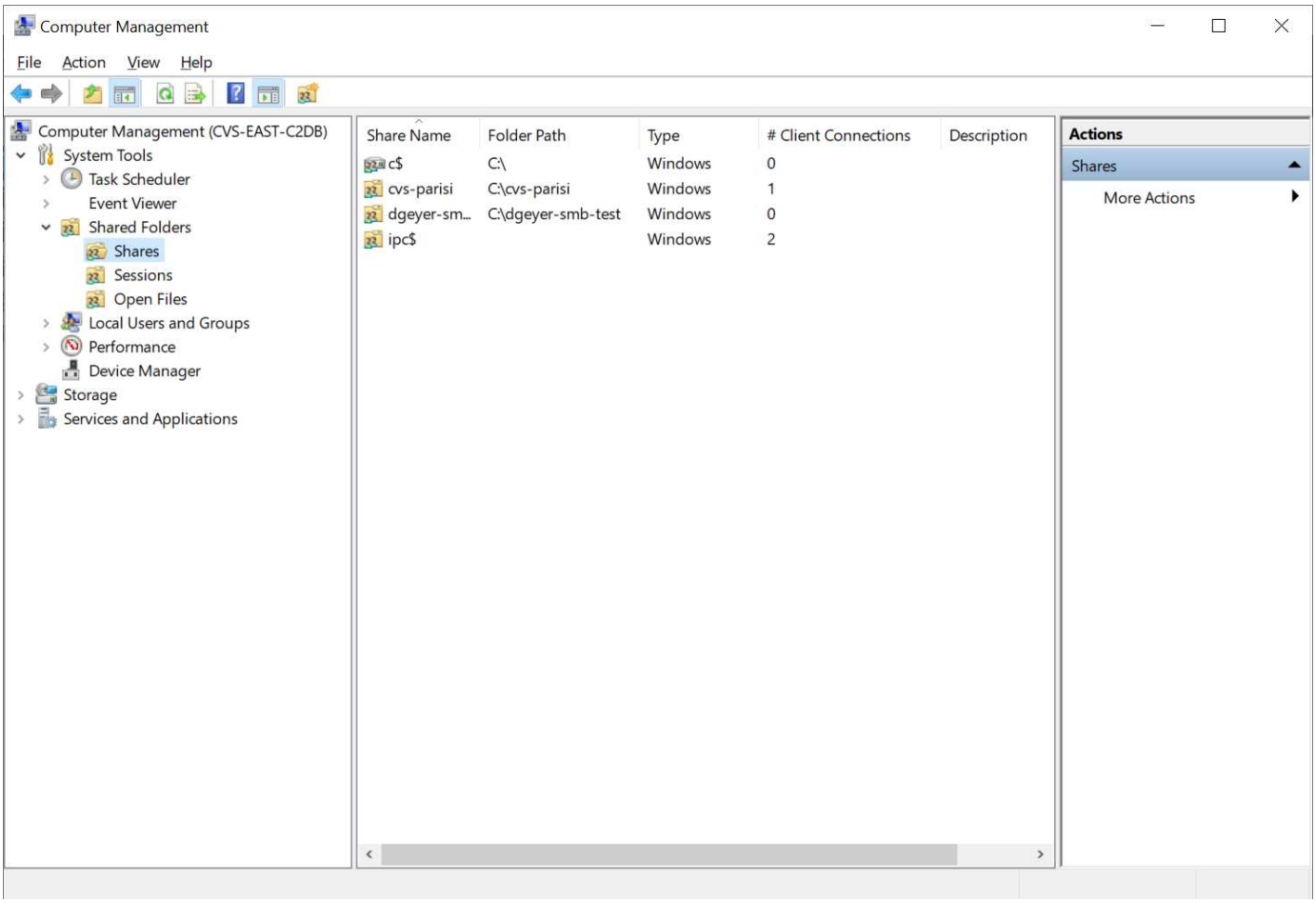
Cloud Volumes Service のSMBアクセスはコンピュータの管理MMCへの接続を提供します。MMCを使用すると、共有の表示、共有ACLの管理、SMBセッションの表示と管理、および開いているファイルの表示を行うことができます。

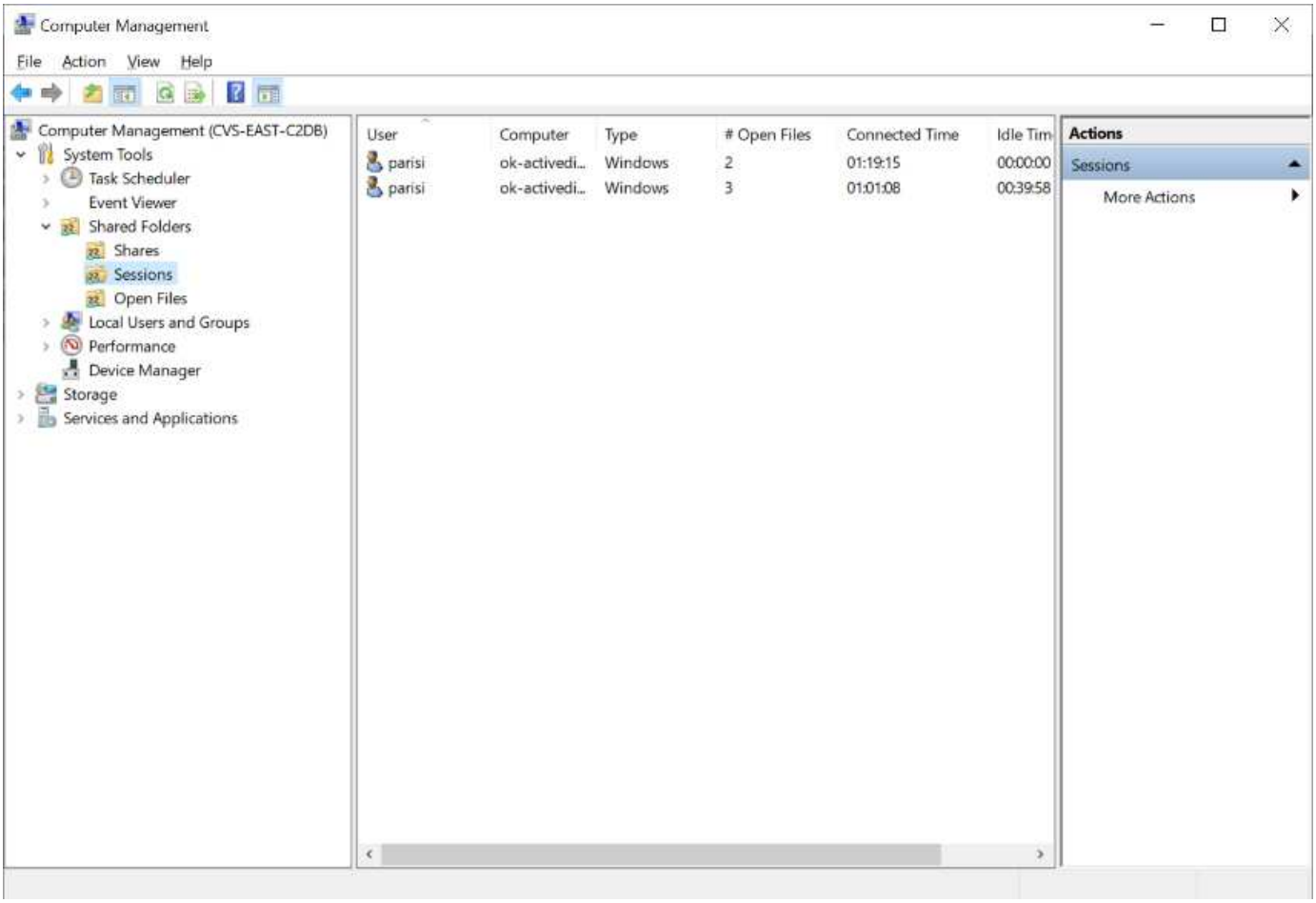
MMCを使用してCloud Volumes Service のSMB共有およびセッションを表示するには、現在ログインしているユーザがドメイン管理者である必要があります。他のユーザには、MMCを使用したSMBサーバの表示または管理へのアクセスを許可されているほか、Cloud Volumes Service SMBインスタンスで共有やセッションを表示しようとすると、[You do not have Permissions]ダイアログボックスが表示されます。

SMBサーバーに接続するには、[コンピューターの管理]を開き、[コンピューターの管理]を右クリックして、[別のコンピューターに接続]を選択します。コンピュータの選択ダイアログボックスが開き、SMBサーバ名（Cloud Volumes Service ボリューム情報に含まれています）を入力できます。

適切な権限を持つSMB共有を表示すると、Active Directory接続を共有するCloud Volumes Service インスタンス内の使用可能なすべての共有が表示されます。この動作を制御するには、Cloud Volumes Service ボリュームインスタンスでSMB共有を非表示オプションを設定します。

リージョンごとに許可されるActive Directory接続は1つだけです。





次の表に、MMCでサポートされる機能とサポートされない機能を示します。

サポートされている機能	サポートされていない機能
• 共有を表示します • アクティブなSMBセッションを表示します • 開いているファイルを表示します • ローカルユーザとローカルグループを表示します • ローカルグループメンバーシップを表示します • システムのセッション、ファイル、およびツリー接続のリストを列挙します • 開いているファイルを閉じます • 開いているセッションを閉じます • 共有を作成 / 管理します	• 新しいローカルユーザ / グループを作成しています • 既存のローカルユーザ/グループの管理/表示 • イベントまたはパフォーマンスログを表示します • ストレージの管理 • サービスとアプリケーションの管理

SMBサーバのセキュリティ情報

Cloud Volumes Service のSMBサーバでは、Kerberosのクロックスキュー、チケットの有効期間、暗号化など、SMB接続のセキュリティポリシーを定義する一連のオプションを使用します。

次の表に、これらのオプションとその機能、デフォルト設定、およびCloud Volumes Service で変更できるかどうかを示します。一部のオプションはCloud Volumes Service には適用されません。

セキュリティオプション	機能	デフォルト値	変更は可能ですか？
Kerberosの最大クロックスキュー（分）	Cloud Volumes Service とドメインコントローラ間の最大時間スキューを指定します。時刻のずれが5分を超えるとKerberos認証は失敗します。これはActive Directoryのデフォルト値に設定されています。	5.	いいえ
Kerberosチケットの有効期間（時間）	Kerberosチケットの有効期間が終了しないと更新が必要になります。10時間以内に更新が行われない場合は、新しいチケットを取得する必要があります。Cloud Volumes Service は、これらの更新を自動的に実行します。Active Directoryのデフォルト値は10時間です。	10.	いいえ
Kerberosチケットの最大更新日数	新しい許可要求が必要になるまでKerberosチケットを更新できる最大日数。Cloud Volumes Service はSMB接続のチケットを自動的に更新します。Active Directoryのデフォルト値は7日です。	7.	いいえ
Kerberos KDC接続タイムアウト（秒）	KDC接続がタイムアウトするまでの秒数。	3.	いいえ
受信SMBトラフィックに署名を要求します	SMBトラフィックに署名を要求するかどうかを設定します。trueに設定すると、署名をサポートしていないクライアントは接続に失敗します。	いいえ	
ローカルユーザアカウントに複雑なパスワードを要求します	ローカルSMBユーザのパスワードに使用します。Cloud Volumes Service ではローカルユーザの作成はサポートされないため、このオプションはCloud Volumes Service には適用されません。	正しいです	いいえ

セキュリティオプション	機能	デフォルト値	変更は可能ですか？
Active Directory LDAP接続にはstart_tlsを使用します	Active Directory LDAPのStart TLS接続を有効にするために使用します。現在、Cloud Volumes Service ではこの機能の有効化がサポートされていませ	いいえ	いいえ
は、KerberosのAES-128およびAES-256暗号化を有効にします	Active Directory接続にAES暗号化を使用するかどうかを制御し、Active Directory接続の作成/変更時にActive Directory認証用のAES暗号化を有効にするオプションで制御します。	いいえ	はい。
LM互換性レベル	Active Directory接続でサポートされている認証ダイアレクトのレベル。「」を参照してくださいSMB認証ダイアレクト」を参照してください。	NTLMv2 - krb	いいえ
受信CIFSトラフィックにSMB暗号化を要求します	すべての共有でSMB暗号化が必要です。これはCloud Volumes Serviceでは使用されません。代わりに、ボリューム単位で暗号化を設定します（「」を参照）SMB共有のセキュリティ機能」）をクリックします。	いいえ	いいえ
クライアントセッションセキュリティ	LDAP通信の署名と封印を設定します。この機能は現在Cloud Volumes Service には設定されていませんが、今後のリリースでサポートする必要が生じる可能性があります。WindowsパッチによるLDAP認証の問題に対する修正については、セクションで説明しています "「LDAPチャネルバインディング」"。	なし	いいえ
DC接続のSMB2有効化	DC接続にSMB2を使用します。デフォルトは有効です。	システム-デフォルト	いいえ

セキュリティオプション	機能	デフォルト値	変更は可能ですか？
LDAPリファーラル追跡	複数のLDAPサーバを使用している場合、リファーラル追跡を使用すると、クライアントが最初のサーバでエントリが見つからなかったときに、リスト内の他のLDAPサーバを参照することができます。これは現在、Cloud Volumes Service ではサポートされていません。	いいえ	いいえ
セキュアなActive Directory接続にLDAPSを使用します	LDAP over SSLを有効にします。現在、Cloud Volumes Service ではサポートされていません。	いいえ	いいえ
DC接続には暗号化が必要です	DC接続を成功させるには暗号化が必要です。Cloud Volumes Service ではデフォルトで無効になっています。	いいえ	いいえ

デュアルプロトコル/マルチプロトコル

Cloud Volumes Service では、適切なアクセス権限を維持しながら、SMBクライアントとNFSクライアントの両方で同じデータセットを共有できます ("デュアルプロトコル" ）。これを行うには、プロトコル間でIDマッピングを調整し、中央のバックエンドLDAPサーバを使用してUNIX IDをCloud Volumes Service に提供します。Windows Active Directoryを使用すると、WindowsとUNIXの両方のユーザに使いやすさを提供できます。

Access Control の略

- 共有アクセス制御。 NAS共有にアクセスできるクライアントまたはユーザーおよびグループを決定します。NFSの場合は、エクスポートへのクライアントアクセスを制御するエクスポートポリシーとルールがあります。NFSエクスポートはCloud Volumes Service インスタンスから管理されます。SMBは、CIFS / SMB共有と共有ACLを利用して、ユーザレベルおよびグループレベルでより細かく制御します。を使用して設定できるのは、SMBクライアントからのみ共有レベルのACLです "MMC /コンピュータの管理" Cloud Volumes Service インスタンスに対する管理者権限を持つアカウントを使用する場合（を参照） ""ローカル/ BUILTIN管理者/バックアップ権限を持つアカウント""）。
- *ファイルアクセス制御。*ファイルまたはフォルダレベルで権限を制御し、常にNASクライアントから管理します。NFSクライアントは、従来のモードビット（rwx）またはNFSv4 ACLを使用できます。SMBクライアントはNTFS権限を利用します。

NFSとSMBの両方にデータを提供するボリュームのアクセス制御は、使用しているプロトコルによって異なります。デュアルプロトコルの権限については、「」を参照してください[アクセス許可モデル]」

ユーザマッピング

クライアントがボリュームにアクセスすると、Cloud Volumes Service は受信ユーザを反対方向の有効なユーザにマッピングしようとします。これは、プロトコルを使用して適切なアクセスを決定し、アクセスを要求し

ているユーザが実際に誰であるかを確認するために必要です。

たとえば、「joe」という名前のWindowsユーザがSMB経由でUNIXアクセス権を持つボリュームにアクセスしようとすると、Cloud Volumes Service は「joe」という名前の対応するUNIXユーザを検索します。存在する場合、Windowsユーザ「joe」としてSMB共有に書き込まれるファイルは、NFSクライアントからはUNIXユーザ「joe」と表示されます。

また、「joe」という名前のUNIXユーザがWindows権限を持つCloud Volumes Service ボリュームへのアクセスを試みる場合、そのUNIXユーザは有効なWindowsユーザにマッピングできる必要があります。そうしないと、ボリュームへのアクセスが拒否されます。

現時点では、LDAPを使用した外部UNIX IDの管理でサポートされているのはActive Directoryのみです。このサービスへのアクセスの設定の詳細については、を参照してください "AD接続の作成"。

アクセス許可モデル

デュアルプロトコルのセットアップを使用する場合、Cloud Volumes Service では、ボリュームのセキュリティ形式を使用してACLのタイプを決定します。これらのセキュリティ形式は、Cloud Volumes Service ボリュームの作成時に選択したNASプロトコル、またはデュアルプロトコルの場合に選択したセキュリティ形式に基づいて設定されます。

- NFSのみを使用している場合は、Cloud Volumes Service ボリュームでUNIX権限が使用されます。
- SMBのみを使用する場合、Cloud Volumes Service ボリュームはNTFS権限を使用します。

デュアルプロトコルボリュームを作成する場合は、ボリュームの作成時にACL形式を選択できます。この決定は、必要な権限管理に基づいて行う必要があります。ユーザがWindows / SMBクライアントから権限を管理している場合は、NTFSを選択します。ユーザがNFSクライアントおよびchmod / chownを使用することを希望する場合は、UNIXセキュリティ形式を使用します。

Active Directory接続の作成に関する考慮事項

Cloud Volumes Service を使用すると、SMBユーザとUNIXユーザのIDを管理するために、Cloud Volumes Service インスタンスを外部のActive Directoryサーバに接続できます。Cloud Volumes Service でSMBを使用するには、Active Directory接続を作成する必要があります。

この構成には、セキュリティについて考慮する必要があるいくつかのオプションがあります。外部Active Directoryサーバは、オンプレミスインスタンスでもクラウドネイティブでもかまいません。オンプレミスのActive Directoryサーバを使用している場合は、ドメインを外部ネットワーク（DMZや外部IPアドレスなど）に公開しないでください。代わりに、を使用して、セキュアなプライベートトンネルまたはVPN、一方向フォレストトラスト、またはオンプレミスネットワークへの専用ネットワーク接続を使用します "プライベートGoogle アクセス"。詳細については、Google Cloudのドキュメントを参照してください "Google CloudでActive Directoryを使用する際のベストプラクティス"。

> CVS-SWを使用するには、Active Directoryサーバを同じリージョンに配置する必要があります。CVS-SWで別の地域へのDC接続を試みた場合、試行は失敗します。CV-SWを使用する場合は、Active Directory DCを含むActive Directoryサイトを作成し、Cloud Volumes Service でサイトを指定して、リージョン間のDC接続の試行を回避してください。

Active Directoryのクレデンシャル

NFS用のSMBまたはLDAPが有効な場合、Cloud Volumes Service はActive Directoryコントローラと通信して、認証に使用するマシンアカウントオブジェクトを作成します。これは、Windows SMBクライアントがドメインに参加する方法とまったく異なり、Active Directoryの組織単位（OU）への同じアクセス権を必要とします。

多くの場合、セキュリティグループでは、Cloud Volumes Service などの外部サーバでWindows管理者アカウントを使用できません。場合によっては、セキュリティのベストプラクティスとして、Windows Administratorユーザが完全に無効になっていることもあります。

SMBマシンアカウントの作成に必要な権限

Cloud Volumes Service マシンオブジェクトをActive Directoryに追加するには、ドメインに対する管理者権限を持つアカウント、またはが必要です "マシンアカウントオブジェクトを作成および変更する権限を委譲しました" 指定したOUに移動する必要があります。Active Directoryの制御の委任ウィザードでこれを行うには、次のアクセス権限を持つコンピュータオブジェクトの作成/削除へのユーザーアクセスを提供するカスタムタスクを作成します。

- 読み取り / 書き込み
- すべての子オブジェクトを作成/削除します
- すべてのプロパティの読み取り/書き込み
- パスワードの変更/リセット

これにより、定義済みのユーザのセキュリティACLがActive DirectoryのOUに自動的に追加され、Active Directory環境へのアクセスが最小限に抑えられます。ユーザを委任した後、そのユーザ名とパスワードをActive Directoryクレデンシャルとしてこのウィンドウに入力できます。

> Active Directoryドメインに渡されるユーザ名とパスワードは、マシンアカウントオブジェクトのクエリおよび作成時にKerberos暗号化を利用してセキュリティを強化します。

Active Directory接続の詳細

。 "Active Directory接続の詳細" 管理者がマシンアカウントの配置に関する特定のActive Directoryスキーマ情報を指定するためのフィールドを指定します。次に例を示します。

- * Active Directory接続タイプ。リージョン内のActive Directory接続を、Cloud Volumes Service またはCVS -パフォーマンスサービスタイプのボリュームに使用するかどうかを指定するために使用します。既存の接続で正しく設定しないと、使用または編集時に正しく機能しないことがあります。
- ドメイン。 Active Directoryドメイン名。
- サイト。 Active Directoryサーバを特定のサイトに制限して、セキュリティとパフォーマンスを確保します "考慮事項"。Cloud Volumes Service では現在、Cloud Volumes Service インスタンスとは別のリージョンにあるActive Directoryサーバへの認証要求の許可がサポートされていないため、複数のActive Directoryサーバがリージョンにまたがっている場合は、この設定が必要です。（たとえば、Active Directoryドメインコントローラは CVS -パフォーマンスのみがサポートするリージョンにありますが、CVS - SWインスタンスにSMB共有が必要です）。
- * DNSサーバ。*名前検索で使用するDNSサーバ。
- * NetBIOS名（オプション）。*必要に応じて、サーバのNetBIOS名。これは、Active Directory接続を使用して新しいマシンアカウントを作成するときに使用されます。たとえば、NetBIOS名がCVS - Eastに設定

されている場合、マシンアカウント名はCVS - East - ｛1234｝になります。を参照してください "Active DirectoryでのCloud Volumes Service の表示" を参照してください。

- *組織単位(OU)。*コンピュータアカウントを作成するための特定のOU。この機能は、マシンアカウントの制御を特定のOUに委任する場合に便利です。
- *AES暗号化。*AD認証用AES暗号化を有効にするチェックボックスをオンまたはオフにすることもできます。Active Directory認証用のAES暗号化を有効にすると、ユーザとグループの検索時にCloud Volumes Service からActive Directoryへの通信がセキュリティで保護されます。このオプションを有効にする前に、ドメイン管理者に問い合わせて、Active Directoryドメインコントローラが AES認証をサポートしていることを確認してください。

> デフォルトでは、ほとんどのWindowsサーバで弱い暗号（DESやRC4-HMACなど）は無効になりませんが、弱い暗号を無効にするように選択した場合は、Cloud Volumes Service Active Directory接続がAESを有効にするように設定されていることを確認してください。そうしないと、認証エラーが発生します。AES暗号化を有効にしても弱い暗号は無効になりませんが、Cloud Volumes Service SMBマシンアカウントにAES暗号のサポートが追加されます。

Kerberos Realmの詳細

このオプションはSMBサーバには適用されません。Cloud Volumes Service システムでNFS Kerberosを設定するときに使用されます。これらの詳細を入力すると、NFS Kerberos Realmが設定され（Linuxではkrb5.conf ファイルと同様）、Cloud Volumes Service ボリュームの作成時にNFS Kerberosが指定されている場合にActive Directory接続がNFS Kerberos Distribution Center（KDC；Kerberos配布センター）として機能するために使用されます。

> 現在、Windows以外のKDCはCloud Volumes Service との使用でサポートされていません。

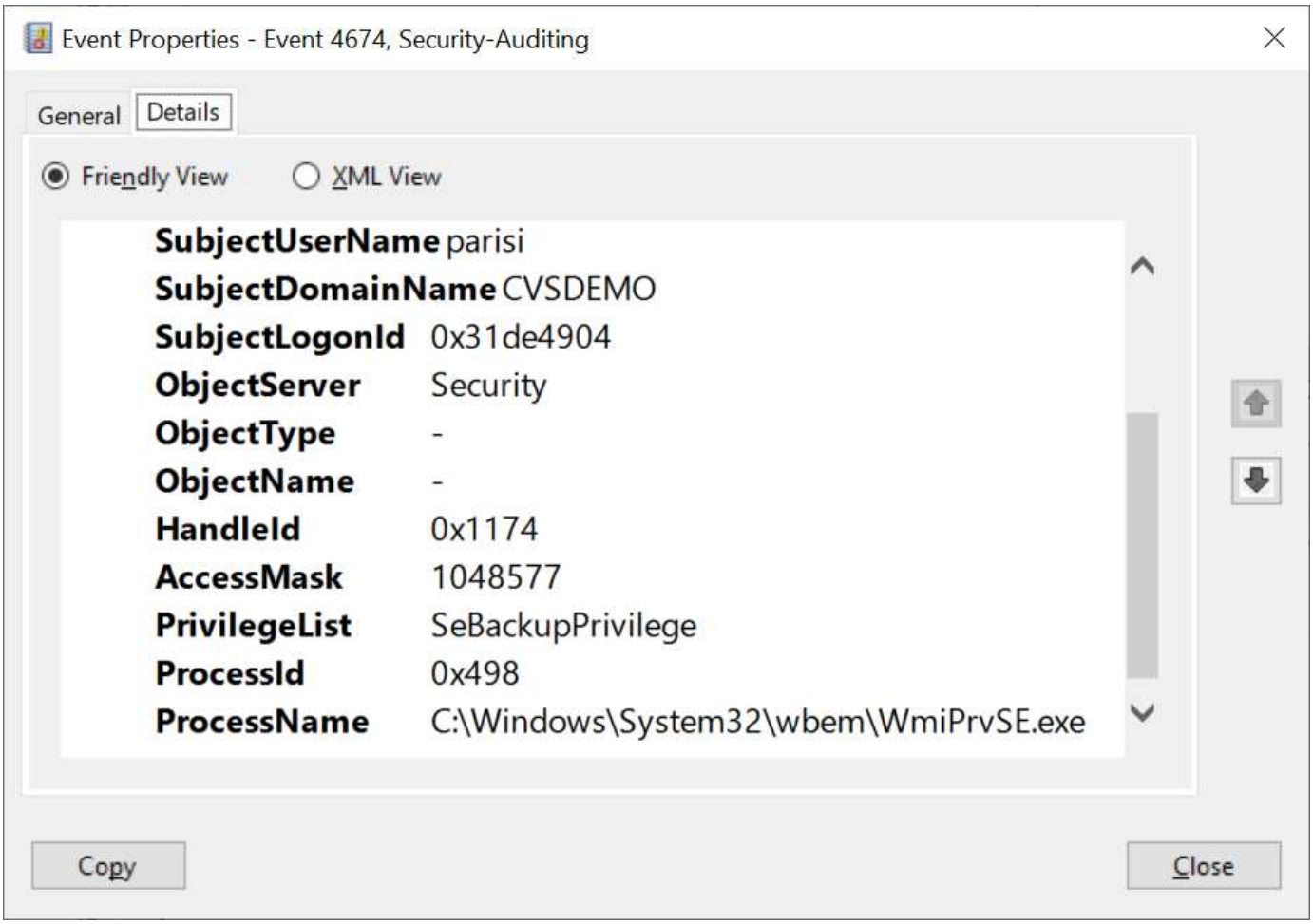
地域

リージョンを使用すると、Active Directory接続が存在する場所を指定できます。このリージョンはCloud Volumes Service ボリュームと同じである必要があります。

- *このセクションでは、LDAPを使用するローカルNFSユーザを許可するオプションもあります。*このセクションでは、LDAPを使用するローカルNFSユーザを許可するオプションもあります。NFS（拡張グループ）の16グループの制限を超えてUNIXユーザグループメンバーシップのサポートを拡張する場合は、このオプションを選択しないでください。ただし、拡張グループを使用するには、UNIX ID用のLDAPサーバを設定する必要があります。LDAPサーバがない場合は、このオプションを選択しないでください。LDAPサーバがあり、ローカルUNIXユーザ（rootなど）も使用する場合は、このオプションを選択します。

バックアップユーザ

このオプションを使用すると、Cloud Volumes Service ボリュームに対するバックアップ権限を持つWindowsユーザを指定できます。一部のアプリケーションでNASボリュームのデータを正しくバックアップおよびリストアするには、バックアップ権限（SeBackupPrivilege）が必要です。このユーザにはボリューム内のデータへのアクセスレベルが高いため、考慮する必要があります "そのユーザアクセスの監査を有効にします"。有効にすると、Event Viewer > Windows Logs > Securityに監査イベントが表示されます。



セキュリティ権限ユーザ

このオプションを使用すると、Cloud Volumes Service ボリュームに対するセキュリティの変更権限を持つWindowsユーザを指定できます。一部のアプリケーションにはセキュリティ権限（SeSecurityPrivilege）が必要です ("たとえば、SQL Serverなどです")を使用して、インストール時に権限を適切に設定します。この権限は、セキュリティログを管理するために必要です。この権限はSeBackupPrivilegeほど強力ではありませんが、ネットアップでは推奨しています "ユーザのユーザアクセスを監査する" 必要に応じて、この権限レベルで設定します。

詳細については、を参照してください "新しいログオンに割り当てられた特別な権限"。

Active DirectoryでのCloud Volumes Service の表示

Active Directoryでは、通常のマシンアカウントオブジェクトとしてCloud Volumes Service が表示されます。命名規則は次のとおりです。

- CIFS/SMBおよびNFS Kerberosでは、個別のマシンアカウントオブジェクトが作成されます。
- NFSでLDAPが有効になっている場合、Kerberos LDAPバインド用にActive Directoryにマシンアカウントが作成されます。
- LDAPを使用したデュアルプロトコルボリュームでは、LDAPとSMBのCIFS / SMBマシンアカウントが共有されます。
- CIFS / SMBマシンアカウントでは、マシンアカウントの名前付け規則として、name-1234（ランダムな4桁のIDに10文字未満の名前をハイフンで付加）を使用します。Active Directory接続では、NetBIOS名の設

定で名前を定義できます（「」を参照）Active Directory接続の詳細」）をクリックします。

- NFS Kerberosでは、命名規則としてnfs-name-1234を使用します（最大15文字）。15文字を超える文字が使用されている場合、名前はnfs-truncated-name-1234になります。
- NFSのみのCVS - LDAPが有効なパフォーマンスインスタンスは、CIFS / SMBインスタンスと同じ命名規則を使用してLDAPサーバにバインドするためのSMBマシンアカウントを作成します。
- SMBマシンアカウントを作成すると、デフォルトの非表示の管理共有が表示されます（を参照） "「デフォルトの非表示共有」"）も作成されます（c$、admin$、ipc$）が、ACLが割り当てられておらず、アクセスできない共有です。
- マシンアカウントオブジェクトはデフォルトではCN=Computersに配置されますが、必要に応じて別のOUを指定できます。「」を参照してくださいSMBマシンアカウントの作成に必要な権限「Cloud Volumes Service のマシンアカウントオブジェクトを追加または削除するために必要なアクセス権については、を参照してください。

Cloud Volumes Service によってSMBマシンアカウントがActive Directoryに追加されると、次のフィールドが設定されます。

- CN（指定したSMBサーバ名を使用）
- dNSHostName（SMBserver.domain.comを使用）
- msDs-SupportedEncryptionTypes（AES暗号化が有効でない場合は、DES-CBC_MD5、RC4_HMAC_MD5を許可します。AES暗号化が有効の場合は、DES-CBC_MD5、RC4_HMAC_MD5、AES128_CTS_HMAC_SHA1、AES256_CTC_HMAC_SHA1 96を許可します）
- 名前（SMBサーバ名を使用）
- sAMAccountName（SMBserver$を使用）
- servicePrincipalName（Kerberosのホスト/ smbserver.domain.comおよびホスト/ smbserver SPNを使用）

マシンアカウントで弱いKerberos暗号化タイプ(enctype)を無効にする場合は、マシンアカウントのmsDS-SupportedEncryptionTypes値を次の表のいずれかの値に変更してAESのみを許可することができます。

msDs-SupportedEncryptionTypesの値	暗号化タイプが有効です
2.	des_cbc_md5
4.	RC4_HMAC
8.	AES128_CTS_HMAC_SHA1 96のみ
16	AES256_CTS_HMAC_SHA1_96のみ
24	AES128_CTS_HMAC_SHA1_96およびAES256_CTS_HMAC_SHA1_96です
30	DES_CBC_MD5、RC4_HMAC、AES128_CTS_HMAC_SHA1 96およびAES256_CTS_HMAC_SHA1 96

SMBマシンアカウントのAES暗号化を有効にするには、Active Directory接続の作成時にAD認証のAES暗号化を有効にするをクリックします。

NFS KerberosのAES暗号化を有効にするには、 "Cloud Volumes Service のドキュメントを参照してください"。

その他の**NAS**インフラストラクチャサービスの依存関係（**KDC**、**LDAP**、および**DNS**）

NAS共有にCloud Volumes Service を使用する場合は、正常に機能するために外部との依存関係が必要になることがあります。これらの依存関係は、特定の状況下で有効になっています。次の表に、さまざまな設定オプションと、必要な依存関係を示します。

設定	必須の依存関係です
NFSv3のみ	なし
NFSv3 Kerberosのみ	Windows Active Directory：* KDC * DNS * LDAP
NFSv4.1のみ	クライアントIDマッピング設定（/etc/idmap.conf）
NFSv4.1 Kerberosのみ	• クライアントIDマッピング設定（/etc/idmap.conf） • Windows Active Directory：KDC DNS LDAP
SMBのみ	Active Directory：* KDC * DNS
マルチプロトコルのNAS（NFSおよびSMB）	• クライアントIDマッピングの設定（NFSv4.1のみ、/etc/idmap.conf） • Windows Active Directory：KDC DNS LDAP

マシンアカウントオブジェクトの**Kerberos keytab**のローテーション/パスワードがリセットされます

SMBマシンアカウントの場合、Cloud Volumes Service はSMBマシンアカウントのパスワードリセットを定期的にスケジュールします。これらのパスワードはKerberos暗号化を使用してリセットされ、毎週日曜日の午後11時から午前1時までのランダムな時刻にスケジュールされます。これらのパスワードは、Kerberosキーのバージョンをリセットし、Cloud Volumes Service システムに格納されているキータブをローテーションし、Cloud Volumes Service で実行されるSMBサーバのセキュリティを強化するのに役立ちます。マシンアカウントのパスワードはランダム化され、管理者には知られていません。

NFS Kerberosマシンアカウントの場合、パスワードのリセットは、新しいkeytabが作成され、KDCと交換されたときにのみ行われます。現在、Cloud Volumes Service では実行できません。

LDAPおよび**Kerberos**で使用するネットワークポート

LDAPおよびKerberosを使用する場合は、これらのサービスで使用されているネットワークポートを確認する必要があります。Cloud Volumes Service で使用されているすべてのポートの一覧については、を参照してください "セキュリティに関する考慮事項についてのCloud Volumes Service のドキュメント"。

LDAP

Cloud Volumes Service はLDAPクライアントとして機能し、UNIX IDのユーザおよびグループ検索に標準のLDAP検索クエリを使用します。Cloud Volumes Service が提供する標準のデフォルトユーザ以外のユーザとグループを使用する場合は、LDAPが必要です。また、ユーザプリンシパル（user1@domain.comなど）でNFS Kerberosを使用する場合も、LDAPが必要です。現在、Microsoft Active Directoryを使用するLDAPのみがサポートされています。

Active DirectoryをUNIX LDAPサーバとして使用するには、UNIX IDに使用するユーザおよびグループに、必要なUNIX属性を設定する必要があります。Cloud Volumes Service では、に基づいて属性を照会するデフォルト

のLDAPスキーマテンプレートが使用されます "RFC-2307 -bis"。このため、次の表に、ユーザとグループにデータを入力するために最低限必要なActive Directory属性と、それぞれの属性がどのような目的で使用されているかを示します。

Active DirectoryでのLDAP属性の設定の詳細については、を参照してください "デュアルプロトコルアクセスの管理"

属性	機能
UID *	UNIXユーザ名を指定します
uidNumber *	UNIXユーザの数値IDを指定します
gidNumber *	UNIXユーザのプライマリグループの数値IDを指定します
objectclass *	使用するオブジェクトのタイプを指定します。Cloud Volumes Service では、オブジェクトクラスのリストに「user」を含める必要があります（デフォルトではほとんどのActive Directory展開に含まれています）。
名前	アカウントに関する一般的な情報（実際の名前、電話番号など、「gecos」とも呼ばれる）
unixUserPassword	これを設定する必要はありません。NAS認証のUNIX ID検索では使用されません。設定すると、設定されたunixUserPasswordの値がプレーンテキストになります。
unixHomeDirectory	ユーザがLinuxクライアントからLDAPに照らして認証する場合のUNIXホームディレクトリへのパスを定義します。UNIXホームディレクトリの機能にLDAPを使用する場合は、このオプションを設定します。
loginShellの略	ユーザがLDAPに対して認証を行うときに、Linuxクライアントのbash/profileシェルへのパスを定義します。

*は、Cloud Volumes Service で適切に機能するために属性が必要であることを示します。残りの属性はクライアント側でのみ使用します。

属性	機能
CN *	UNIXグループ名を指定します。LDAPでActive Directoryを使用する場合は、オブジェクトの作成時に設定されますが、あとで変更することもできます。この名前を他のオブジェクトと同じにすることはできません。たとえば、user1という名前のUNIXユーザがLinuxクライアント上のuser1という名前のグループに属している場合、Windowsでは、同じcn属性を持つ2つのオブジェクトは許可されません。これを回避するには、Windowsユーザの名前を一意の名前（user1やunixなど）に変更します。Cloud Volumes Service のLDAPでは、UNIXユーザ名にuid属性を使用します。
gidNumber *	UNIXグループの数値IDを指定します。

属性	機能
objectclass *	使用するオブジェクトのタイプを指定します。Cloud Volumes Service では、オブジェクトクラスのリストにグループを含める必要があります（この属性はデフォルトでほとんどのActive Directory展開に含まれています）。
memberUid	UNIXグループのメンバーであるUNIXユーザを指定します。Cloud Volumes Service のActive Directory LDAPでは、このフィールドは必要ありません。Cloud Volumes Service LDAPスキーマでは、グループメンバーシップにMemberフィールドを使用します。
メンバー*	グループメンバーシップ/セカンダリUNIXグループに必要です。このフィールドには、WindowsユーザをWindowsグループに追加します。ただし、WindowsグループにUNIX属性が入力されていない場合、UNIXユーザのグループメンバーシップリストには含まれません。NFSで使用できる必要があるグループは、次の表に示す必要なUNIXグループ属性を設定する必要があります。

*は、Cloud Volumes Service で適切に機能するために属性が必要であることを示します。残りの属性はクライアント側でのみ使用します。

LDAPバインド情報

LDAPでユーザを照会するには、Cloud Volumes Service がLDAPサービスにバインド（ログイン）する必要があります。このログインには読み取り専用権限があり、LDAP UNIX属性を照会してディレクトリを検索するために使用されます。現在のところ、LDAPバインドはSMBマシンアカウントを使用した場合にのみ可能です。

LDAPを有効にできるのは「CVS -パフォーマンス」インスタンスのみで、NFSv3、NFSv4.1、またはデュアルプロトコルボリュームでのみです。LDAP対応ボリュームを導入するには、Cloud Volumes Service ボリュームと同じリージョンにActive Directory接続を確立する必要があります。

LDAPを有効にすると、特定の状況で次のような状況が発生します。

- Cloud Volumes Service プロジェクトにNFSv3またはNFSv4.1のみを使用する場合は、Active Directoryドメインコントローラに新しいマシンアカウントが作成され、Cloud Volumes Service 内のLDAPクライアントはマシンアカウントのクレデンシャルを使用してActive Directoryにバインドします。NFSボリュームおよびデフォルトの非表示の管理共有用にSMB共有は作成されません（を参照）"「デフォルトの非表示共有」"）共有ACLを削除しておきます。
- Cloud Volumes Service プロジェクトにデュアルプロトコルボリュームを使用する場合は、SMBアクセス用に作成された1つのマシンアカウントのみを使用して、Cloud Volumes Service のLDAPクライアントがActive Directoryにバインドされます。追加のマシンアカウントは作成されません。
- 専用のSMBボリュームを個別に作成する場合（LDAPを使用するNFSボリュームの有効化前と無効化後）、LDAPバインド用マシンアカウントはSMBマシンアカウントと共有されます。
- NFS Kerberosも有効になっている場合は、2つのマシンアカウントが作成されます。1つはSMB共有またはLDAPバインド用、もう1つはNFS Kerberos認証用です。

LDAPクエリ

LDAPバインドは暗号化されますが、LDAPクエリは共通のLDAPポート389を使用してプレーンテキストでワイヤ経由で渡されます。この既知のポートは、現在Cloud Volumes Service では変更できません。その結果、ネットワーク内のパケットスニファにアクセスできるユーザは、ユーザ名、グループ名、数値ID、およびグループメンバーシップを確認できます。

ただし、Google Cloud VMは他のVMのユニキャストトラフィックをスニファできません。LDAPトラフィックにアクティブに参加している（バインド可能な）VMのみが、LDAPサーバからのトラフィックを表示できます。Cloud Volumes Service でのパケットスニファの詳細については、を参照してください "「パケットのスニッフィング/トレースに関する考慮事項」"

LDAPクライアント設定のデフォルト

Cloud Volumes Service インスタンスでLDAPを有効にすると、デフォルトで特定の設定の詳細を使用してLDAPクライアント設定が作成されます。場合によっては、オプションがCloud Volumes Service に適用されない（サポートされない）か、設定できないことがあります。

LDAPクライアントオプション	機能	デフォルト値	変更は可能ですか？
LDAPサーバリスト	クエリに使用するLDAPサーバ名またはIPアドレスを設定します。これはCloud Volumes Service では使用されません。代わりに、Active Directory ドメインを使用してLDAPサーバを定義します。	未設定	いいえ
Active Directoryドメイン	LDAPクエリに使用するActive Directoryドメインを設定します。Cloud Volumes Service は、DNSのLDAPのSRVレコードを利用して、ドメイン内のLDAPサーバを検索します。	Active Directory接続で指定されているActive Directoryドメインに設定します。	いいえ
優先されるActive Directoryサーバ	LDAPで使用する優先Active Directoryサーバを設定します。Cloud Volumes Service ではサポートされていません。代わりに、Active Directory サイトを使用してLDAPサーバの選択を制御します。	未設定。	いいえ
SMBサーバクレデンシャルを使用してバインド	SMBマシンアカウントを使用してLDAPにバインドします。現在、Cloud Volumes Service でサポートされているLDAPバインド方式はのみです。	正しいです	いいえ

LDAPクライアントオプション	機能	デフォルト値	変更は可能ですか？
スキーマテンプレート	LDAPクエリに使用するスキーマテンプレート。	MS-AD-BIS を参照してください	いいえ
LDAPサーバポート	LDAPクエリに使用するポート番号。Cloud Volumes Service では現在、標準のLDAPポート389のみが使用されています。LDAPS /ポート636は、現在サポートされていません。	389	いいえ
LDAPSが有効になっています	LDAP over Secure Sockets Layer（SSL）をクエリおよびバインドに使用するかどうかを制御します。現在、Cloud Volumes Service ではサポートされていません。	いいえ	いいえ
クエリタイムアウト（秒）	クエリがタイムアウトしました。クエリに指定した値よりも長い時間がかかると、クエリが失敗します。	3.	いいえ
最小バインド認証レベル	サポートされる最小バインドレベルを指定します。Cloud Volumes Service はLDAPバインドにマシンアカウントを使用し、デフォルトではActive Directoryは匿名バインドをサポートしないため、このオプションはセキュリティ上の理由から有効になりません。	匿名	いいえ
バインド DN	シンプルバインドが使用されている場合にバインドに使用されるユーザ/識別名（DN）。Cloud Volumes Service は、LDAPバインドにマシンアカウントを使用しますが、現在のところ単純なバインド認証はサポートしていません。	未設定	いいえ
ベースDN	LDAP検索に使用するベースDN。	Active Directory接続に使用するWindowsドメイン（DN形式）（DC=domain、DC=local）	いいえ

LDAPクライアントオプション	機能	デフォルト値	変更は可能ですか？
ベースの検索範囲	ベースDN検索の検索範囲。値には、base、onelevel、subtreeのいずれかを指定できます。Cloud Volumes Service ではサブツリー検索のみがサポートされます。	サブツリー	いいえ
ユーザDN	ユーザがLDAPクエリの検索を開始するDNを定義します。現在Cloud Volumes Service ではサポートされていないため、すべてのユーザ検索はベースDNから開始されます。	未設定	いいえ
ユーザの検索範囲	ユーザDN検索の検索範囲。値には、base、onelevel、subtreeのいずれかを指定できます。Cloud Volumes Service では、ユーザ検索範囲の設定はサポートされていません。	サブツリー	いいえ
グループDN	グループ検索でLDAPクエリが開始されるDNを定義します。現在Cloud Volumes Service ではサポートされていないため、すべてのグループ検索はベースDNから開始されます。	未設定	いいえ
グループの検索範囲	グループDN検索の検索範囲。値には、base、onelevel、subtreeのいずれかを指定できます。Cloud Volumes Service では、グループ検索範囲の設定はサポートされていません。	サブツリー	いいえ
ネットグループDN	ネットグループ検索でLDAPクエリの開始に使用するDNを定義します。現在Cloud Volumes Service ではサポートされていないため、ネットグループ検索はすべてベースDNから開始されます。	未設定	いいえ

LDAPクライアントオプション	機能	デフォルト値	変更は可能ですか？
ネットグループ検索範囲	ネットグループDN検索の検索範囲。値には、base、onelevel、subtreeのいずれかを指定できます。Cloud Volumes Service では、ネットグループ検索範囲の設定はサポートされていません。	サブツリー	いいえ
LDAPでstart_tlsを使用します	Start TLSを使用して、証明書ベースのLDAP接続をポート389経由で行います。現在、Cloud Volumes Service ではサポートされていません。	いいえ	いいえ
ホスト単位のネットグループ検索を有効にします	ネットグループをすべてのメンバーの一覧に展開するのではなく、ホスト名によるネットグループ検索を有効にします。現在、Cloud Volumes Service ではサポートされていません。	いいえ	いいえ
ホスト単位のネットグループDN	ホスト単位のネットグループ検索がLDAPクエリを開始するDNを定義します。ホスト単位のネットグループは、現在Cloud Volumes Service ではサポートされていません。	未設定	いいえ
ホスト単位のネットグループ検索範囲	ホスト単位のネットグループDN検索の検索範囲。値には、base、onelevel、subtreeのいずれかを指定できます。ホスト単位のネットグループは、現在Cloud Volumes Service ではサポートされていません。	サブツリー	いいえ

LDAPクライアントオプション	機能	デフォルト値	変更は可能ですか？
クライアントセッションのセキュリティ	LDAPで使用されるセッションセキュリティのレベルを定義します（sign、seal、none）。LDAP署名は、Active Directoryから要求された場合にCVSパフォーマンスでサポートされます。CVS-SWではLDAP署名はサポートされません。どちらのタイプのサービスでも、現時点ではシーリングはサポートされていません。	なし	いいえ
LDAPリファーラルキャッシュ	複数のLDAPサーバを使用している場合、リファーラル追跡を使用すると、クライアントが最初のサーバでエントリが見つからなかったときに、リスト内の他のLDAPサーバを参照することができます。これは現在、Cloud Volumes Service ではサポートされていません。	いいえ	いいえ
グループメンバーシップフィルタ	LDAPサーバからグループメンバーシップを検索するときに使用するカスタムのLDAP検索フィルタを提供します。Cloud Volumes Service では現在サポートされていません。	未設定	いいえ

LDAPを使用した非対称ネームマッピング

デフォルトでは、Cloud Volumes Service は、WindowsユーザとUNIXユーザを、特別な設定なしで双方向に同一のユーザ名でマッピングします。有効なUNIXユーザ（LDAPを使用）がCloud Volumes Service で検出されると、1：1のネームマッピングが発生します。たとえば、Windowsユーザjohnsmithが使用されている場合、Cloud Volumes Service がLDAPで「johnsmith」という名前のUNIXユーザを検索できた場合、そのユーザのネームマッピングは成功し、「johnsmith」によって作成されたすべてのファイルおよびフォルダに正しいユーザ所有権が表示されます。 また'johnsmithに影響を与えるすべてのACLは'NASプロトコルの使用に関係なく使用されますこれは対称ネームマッピングと呼ばれます。

非対称ネームマッピングは、WindowsのユーザIDとUNIXのユーザIDが一致しない場合に使用します。たとえば'WindowsユーザjohnsmithがUNIX IDがjsmithの場合'UNIXのバリエーションをCloud Volumes Service に通知する必要がありますCloud Volumes Service は現在、静的なネームマッピングルールの作成をサポートしていないため、ファイルとフォルダの適切な所有権と予期される権限を確保するために、LDAPを使用してWindows IDとUNIX IDの両方のユーザのIDを検索する必要があります。

デフォルトでは、Cloud Volumes Service のネームマップデータベースのインスタンスのns-switchに「ldap」

が含まれているため、非対称名にLDAPを使用してネームマッピング機能を提供するために必要なのは、Cloud Volumes Service の検索内容を反映するためにユーザ/グループの属性の一部のみです。

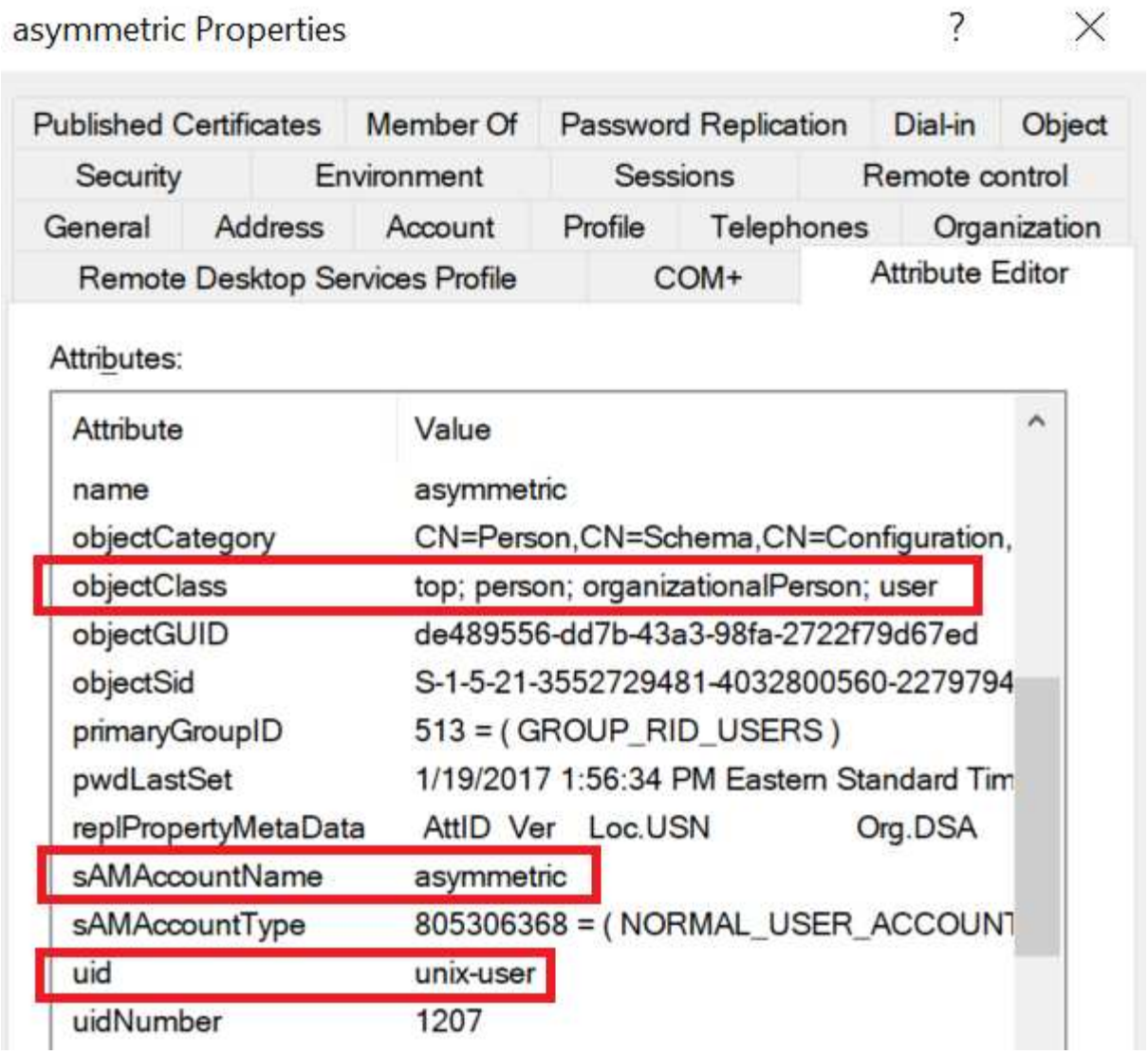
次の表に、非対称ネームマッピング機能のためにLDAPに入力する必要がある属性を示します。ほとんどの場合、Active Directoryはすでに設定されています。

Cloud Volumes Service 属性	機能	**Cloud Volumes Service** がネームマッピングに使用する値
WindowsからUNIX objectClass	使用するオブジェクトのタイプを指定します。（ユーザ、グループ、posixAccountなど）	userを含める必要があります（必要に応じて、他の値を複数含めることもできます）。
WindowsからUNIXへの属性	作成時にWindowsユーザ名を定義します。Cloud Volumes Service では、これをWindowsからUNIXへのルックアップに使用します。	ここでは変更は必要ありません。sAMAccountNameはWindowsログイン名と同じです。
UID	UNIXユーザ名を定義します。	必要なUNIXユーザ名。

Cloud Volumes Service では現在、LDAP検索でドメインプレフィックスが使用されないため、LDAPネームマップ検索で複数のドメインLDAP環境が正常に機能しません。

次の例は、Windows名が「asymmetric」で、UNIX名が「unix-user」で、SMBとNFSの両方からファイルを書き込む際の動作を示しています。

次の図に、LDAP属性がWindowsサーバからどのように見えているかを示します。



NFSクライアントからは、UNIX名を照会できますが、Windows名は照会できません。

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

ファイルがNFSから「unix-user」として書き込まれると、NFSクライアントから次のような結果になります。

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

Windowsクライアントでは、ファイルの所有者が適切なWindowsユーザに設定されていることを確認できます。

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

逆に、WindowsユーザがSMBクライアントから「asymmetric」で作成したファイルの場合、次のテキストに示すように、適切なUNIX所有者が表示されます。

SMB：

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS ：

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

LDAPチャネルバインド

Windows Active Directoryドメインコントローラの脆弱性により、 "マイクロソフトセキュリティアドバイザリADV190023" DCによるLDAPバインドの許可方法を変更します。

Cloud Volumes Service による影響は、どのLDAPクライアントでも同じです。Cloud Volumes Service では現在、チャネルバインドはサポートされていません。Cloud Volumes Service はネゴシエーションを通じてデフォルトでLDAP署名をサポートしているため、LDAPチャネルバインドを問題 にすることはできません。チャネルバインドが有効な状態でLDAPにバインドする問題がある場合は、「ADV190023」の修正手順に従って、Cloud Volumes Service からのLDAPバインドを成功させるようにしてください。

DNS

Active DirectoryとKerberosはどちらも、ホスト名からIP / IPを経由したホスト名解決で、DNSに依存します。DNSでは、ポート53を開く必要があります。Cloud Volumes Service では、DNSレコードに変更を加えたり、現在のところの使用をサポートしていません "動的DNS" ネットワークインターフェイス。

Active Directory DNSを設定して、DNSレコードを更新できるサーバを制限できます。詳細については、を参照してください "Windows DNSを保護"。

Googleプロジェクト内のリソースは、既定ではGoogle Cloud DNSを使用しますが、Active Directory DNSには接続されていません。クラウドDNSを使用するクライアントは、Cloud Volumes Service から返されたUNCパスを解決できません。Active Directoryドメインに参加しているWindowsクライアントは、Active Directory DNSを使用するように設定され、このようなUNCパスを解決できます。

クライアントをActive Directoryに参加させるには、Active Directory DNSを使用するようにそのDNS設定を構成する必要があります。必要に応じて、Active Directory DNSに要求を転送するようにCloud DNSを設定することができます。を参照してください "クライアントでSMB NetBIOS名を解決できないのはなぜですか？"を参照してください。

> Cloud Volumes Service は現在DNSSECをサポートしておらず、DNSクエリはプレーンテキストで実行されます。

ファイルアクセスの監査

現在、Cloud Volumes Service ではサポートされていません。

アンチウイルスによる保護

Cloud Volumes Service で、クライアントからNAS共有へのウィルススキャンを実行する必要があります。現在のところ、Cloud Volumes Service とウィルス対策はネイティブで統合されていません。

サービスの処理

Cloud Volumes Service チームはGoogle Cloudでバックエンドサービスを管理し、複数の戦略を使用してプラットフォームを保護し、不要なアクセスを防止します。

お客様ごとに固有のサブネットが割り当てられ、デフォルトで他のお客様から遮断されたアクセス権が付与される。Cloud Volumes Service の各テナントは、データを完全に分離するために独自のネームスペースとVLANを取得する。ユーザが認証されると、Service Delivery Engine（SDE；サービス提供エンジン）はそのテナントに固有の設定データのみを読み取ることができます。

物理的セキュリティ

事前承認が必要な場合、ケージとラックにアクセスできるのは、オンサイトエンジニアとネットアップ認定のフィールドサポートエンジニア（FSE）のみです。ストレージとネットワークの管理は許可されていません。ハードウェアのメンテナンス作業を実行できるのは、これらのオンサイトリソースのみです。

オンサイトエンジニアの場合は、作業仕様書（SOW）のチケットが発行されます。この作業内容には、ラックIDとデバイスの場所（RU）、その他すべての詳細情報が含まれます。NetApp FSEの場合、サイト訪問チケットはColoで発行する必要があります。チケットには、監査を目的とした訪問者の詳細、日付、時刻が含まれています。FSEのSOWは、社内でネットアップに通知されます。

運用チーム

Cloud Volumes Service の運用チームは、クラウドボリュームサービス向けの生産エンジニアリングとサイト信頼性エンジニア（SRE）、およびハードウェア向けのネットアップフィールドサポートエンジニアとパートナーで構成されています。すべての運用チームメンバーは、Google Cloudでの作業が認定されており、発行されたチケットごとに詳細な作業記録が保持されています。また、各意思決定が適切に精査されるように、厳格な変更管理および承認プロセスが用意されています。

SREチームは、コントロールプレーンと、UI要求からCloud Volumes Service のバックエンドハードウェアおよびソフトウェアにデータをルーティングする方法を管理します。SREチームは、ボリュームやinodeの最大数などのシステムリソースも管理します。SREは、カスタマーデータとやり取りしたり、カスタマーデータにアクセスしたりすることはできません。SREは、バックエンドハードウェアに対する新しいディスク交換要求やメモリ交換要求などのReturn Material Authorizations（RMA）との調整も行います。

お客様の責任

Cloud Volumes Service のお客様は、組織のActive Directoryとユーザーの役割管理だけでなく、ボリュームとデータの操作も管理します。お客様は管理者ロールを割り当てられ、ネットアップとGoogle Cloudが提供する2つの事前定義されたロール（管理者とビューア）を使用して、同じGoogle Cloudプロジェクト内の他のエンドユーザに権限を委譲できます。

管理者は、お客様のプロジェクト内の任意のVPCを、お客様が適切と判断したCloud Volumes Service にピアリングできます。Google Cloud Marketplaceサブスクリプションへのアクセスの管理、およびデータプレーンへのアクセス権を持つVPCの管理は、お客様の責任において行ってください。

悪意のある**SRE**保護

Cloud Volumes Service は、悪意のあるSREが存在するシナリオやSRE資格情報が侵害された場合に、どのように保護するのかという懸念事項があります。

本番環境へのアクセスには、限られた数のSRE担当者のみが使用されます。管理者権限は、経験豊富な一部の管理者にも制限されています。Cloud Volumes Service の運用環境で実行されるすべてのアクションは記録され、ベースラインまたは疑わしいアクティビティへの異常は、セキュリティ情報およびイベント管理（SIEM）脅威インテリジェンスプラットフォームによって検出されます。その結果、悪意のあるアクションを追跡し、Cloud Volumes Service バックエンドに過剰な損害が発生する前に軽減することができます。

ボリュームのライフサイクル

Cloud Volumes Service は、サービス内のオブジェクトのみを管理し、ボリューム内のデータは管理しません。データ、ACL、ファイル所有者などを管理できるのは、ボリュームにアクセスしているクライアントだけです。これらのボリューム内のデータは保存中も暗号化され、Cloud Volumes Service インスタンスのテナントのみにアクセスできます。

Cloud Volumes Service のボリュームライフサイクルはcreate-update-deleteです。ボリュームは、ボリュームが削除されるまでボリュームのSnapshotコピーを保持します。Cloud Volumes Service 内のボリュームを削除できるのは、検証済みのCloud Volumes Service 管理者だけです。管理者がボリューム削除を要求した場合、削除の確認のためにボリューム名を入力する手順が追加で必要になります。ボリュームを削除すると、そのボリュームは削除され、リカバリできなくなります。

Cloud Volumes Service 契約を終了した場合、ネットアップは特定の期間が経過したボリュームに削除マークを付けます。この期間が終了する前に、お客様の要求に応じてボリュームをリカバリできます。

認定資格

Google Cloud向けCloud Volume サービスは、現在ISO/IEC 27001：2013およびISO/IEC 27018：2019規格に準拠しています。サービスは最近、SOC2 Type Iアテステーションレポートを受信しました。ネットアップのデータ セキュリティ への取り組みとプライバシーに関する詳細については、を参照してください "コンプライアンス：データ セキュリティ とデータプライバシー"。

GDPR

プライバシーに対する当社のコミットメントとGDPRへの準拠は、当社のさまざまな方法で提供されています "お客様との契約"などです "カスタマーデータ処理補遺"が含まれます "標準契約条項" 欧州委員会が提供します。また、当社のプライバシーポリシーには、当社の企業行動規範に規定されている中核的な価値観に裏付けられたこれらのコミットメントを定めています。

追加情報と連絡先情報

このドキュメントに記載されている情報の詳細については、以下のドキュメントや Web サイトを参照してください。

- Cloud Volumes Service 向けGoogle Cloudドキュメント

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes/"

- Googleプライベートサービスへのアクセス

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- ネットアップの製品マニュアル

  "https://www.netapp.com/support-and-training/documentation/"

- 暗号化検証モジュールプログラム—NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- 『NetApp解決策 for Ransomware』

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- TR-4616 ：『 NFS Kerberos in ONTAP 』

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

お問い合わせください

本テクニカルレポートの品質向上について、ご意見をお寄せください。

mailto：doccomments@netapp.com [doccomments@netapp.com ^]までお問い合わせください。件名にはテクニカルレポート4918を含めてください。

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。