



パブリッククラウド向け **VMware** NetApp Solutions

NetApp
September 26, 2024

目次

パブリッククラウド向け VMware	1
VMware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の概要	1
ハイパースケーラにおける VMware 向けネットアップソリューション	5
VMwareでサポートされるネットアップハイブリッドマルチクラウドの構成	9
ハイパースケーラ構成における VMware	9
ハイパースケーラクラウドにおけるネットアップストレージ	37
まとめ：VMware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が選ばれる理由とは	122

パブリッククラウド向け VMware

VMware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の概要

ほとんどの IT 組織は、ハイブリッドクラウドファーストアプローチに準拠しています。このような組織は変革の段階にあり、お客様は現在の IT 環境を評価してから、評価と調査の演習に基づいてワークロードをクラウドに移行しています。

クラウドに移行するお客様の要因には、柔軟性とバースト性、データセンターの終了、データセンターの統合、サポート終了シナリオ、合併、買収など。この移行の理由は、各組織とそれぞれのビジネス上の優先事項によって異なります。ハイブリッドクラウドに移行する際は、クラウドの導入と柔軟性を最大限に活用するために、クラウドに最適なストレージを選択することがきわめて重要です。

パブリッククラウドの VMware Cloud オプション

ここでは、各クラウドプロバイダが、それぞれのパブリッククラウドサービス内でVMware Software Defined Data Center (SDDC) やVMware Cloud Foundation (VCF) スタックをサポートする方法について説明します。

Azure VMware 解決策の略



Azure VMware Solutionは、Microsoft Azureパブリッククラウド内でVMware SDDCを完全に機能させるためのハイブリッドクラウドサービスです。Azure VMware 解決策は、Microsoft がフルマネージドでサポートし、VMware が Azure インフラを活用して検証した、ファーストパーティ製解決策です。つまり、Azure VMware 解決策を導入すると、お客様のコンピューティング仮想化向けにVMware のESXiを、ハイパーコンバージドストレージ用にvSANを、さらにNSXは、ネットワークとセキュリティを実現するだけでなく、Microsoft Azure のグローバルプレゼンス、クラスをリードするデータセンター施設を活用し、ネイティブのAzure サービスとソリューションの豊富なエコシステムに近接しています。

AWS 上の VMware Cloud



VMware Cloud on AWSは、VMwareのエンタープライズクラスのSDDC ソフトウェアをAWSクラウドに移行し、AWSのネイティブサービスへのアクセスを最適化します。VMware Cloud Foundation を基盤とする VMware Cloud on AWS は、VMware のコンピューティング、ストレージ、ネットワーク仮想化製品（VMware vSphere、VMware vSAN、VMware NSX）と VMware vCenter Server の管理を統合し、専用の柔軟性の高いベアメタル AWS インフラストラクチャ上で実行できるように最適化されています。

Google Cloud VMware Engine



Google Cloud VMware Engineは、Google Cloudのハイパフォーマンスな拡張性に優れたインフラとVMware Cloud Foundationスタック（VMware vSphere、vCenter、vSAN、NSX-T）上に構築されたインフラサービス（IaaS）です。このサービスにより、クラウドへの迅速な移行が可能になり、既存のVMwareワークロードをオンプレミス環境からGoogle Cloud Platformにシームレスに移行または拡張できます。VMware と緊密に連携して Google が販売およびサポートするサービスです。



SDDC プライベートクラウドと NetApp Cloud Volume コロケーション施設は、最小限のネットワークレイテンシで最高のパフォーマンスを提供します。

ご存知ですか？

VMware SDDC を導入する際、使用するクラウドに関係なく、最初のクラスタには次の製品が含まれます。

- コンピューティングの仮想化に使用する VMware ESXi ホストと、管理用の vCenter Server アプライアンス
- 各 ESXi ホストの物理ストレージ資産を組み込んだ VMware vSAN ハイパーコンバージドストレージ
- 管理のために NSX Manager クラスタを使用した仮想ネットワークとセキュリティのための VMware NSX

ストレージ構成

ストレージを大量に消費するワークロードをホストし、クラウドホスト型の VMware 解決策でスケールアウトする場合、デフォルトのハイパーコンバージドインフラでは、コンピューティングリソースとストレージリソースの両方で拡張を行う必要があります。

Azure NetApp Files、NetApp ONTAP 向け Amazon FSX、Cloud Volumes ONTAP（3つの主要ハイパースケアラすべてに対応）、Cloud Volumes Service for Google Cloud などの NetApp Cloud Volume と統合することで、お客様はストレージを個別に拡張できるオプションを利用できるようになりました。また、必要に応じてコンピューティングノードを SDDC クラスタに追加します。

注：

- VMware では、アンバランスなクラスタ構成を推奨していません。そのため、ストレージを拡張するとホストが増え、TCO が増加します。
- 1つの VSAN 環境のみが可能です。そのため、すべてのストレージトラフィックが本番環境のワークロードと直接競合します。
- アプリケーションの要件、パフォーマンス、コストに合わせて複数のパフォーマンス階層を提供するオプションはありません。
- クラスタホスト上に構築された VSAN のストレージ容量の制限に非常に簡単に到達できます。NetApp Cloud Volume を使用して、アクティブなデータセットをホストするか、またはティアクーラデータを永続的ストレージにホストするかに応じてストレージを拡張できます。

Azure NetApp Files、NetApp ONTAP 向け Amazon FSX、Cloud Volumes ONTAP（3つの主要なハイパースケアラすべてで利用可能）、および Cloud Volumes Service for Google Cloud は、ゲスト VM と組み合わせて使用できます。このハイブリッドストレージアーキテクチャは、ゲストオペレーティングシステムとアプリケーションバイナリデータを保持する VSAN データストアで構成されます。アプリケーションデータは、ゲストベースの iSCSI イニシエータを介して VM に接続されます。または、Amazon FSX for NetApp ONTAP、Cloud Volume ONTAP、Azure NetApp Files、Cloud Volumes Service for Google Cloud と直接通信する NFS/SMB マウントを使用して VM に接続されます。この構成では、VSAN と同様にストレージ容量の問題を簡単に解決できます。使用可能な空きスペースは、使用する余裕容量およびストレージポリシーによって異なります。

次に、AWS 上の VMware Cloud 上の 3 ノード SDDC クラスタについて考えてみましょう。

- 3 ノード SDDC の合計物理容量は 31.1TB（各ノードのおおよその 10TB）です。
- 追加のホストが追加される前に保持されるスラックスペース = 25% = $(.25 \times 31.1\text{TB}) = 7.7\text{TB}$ 。
- 余裕期間を計算した後の使用可能な物理容量 = 23.4TB
- 使用可能な有効な空きスペースは、適用するストレージポリシーによって異なります。

例：

- RAID 0 = 有効な空きスペース = 23.4TB（使用可能な物理容量 / 1）
- RAID 1 = 有効な空きスペース = 11.7TB（使用可能な物理容量 / 2）
- RAID 5 = 有効な空きスペース = 17.5TB（使用可能な物理容量 / 1.33）

そのため、NetApp Cloud Volume をゲスト接続ストレージとして使用すると、パフォーマンスとデータ保護の要件を満たしながら、ストレージを拡張して TCO を最適化できます。



本ドキュメントの作成時点で使用可能な唯一のオプションは、ゲスト内ストレージでした。NFSデータストアの補足サポートが提供されるようになりましたが、それ以外のドキュメントも提供されます "[こちらをご覧ください](#)".

覚えておいてください

- ハイブリッドストレージモデルでは、ホスト自体にも近接しているため、特定のレイテンシ要件に対処するために、VSAN データストアにティア 1 または高優先度のワークロードを配置します。トランザクションのレイテンシが許容されるワークロード VM には、ゲスト内メカニズムを使用します。
- NetApp SnapMirror® テクノロジーを使用して、オンプレミスの ONTAP システムから Cloud Volumes ONTAP または Amazon FSx for NetApp ONTAP にワークロードデータをレプリケートすることで、ブロックレベルのメカニズムによって移行を簡易化できます。これは、Azure NetApp Files および Cloud Volume サービスには適用されません。Azure NetApp Files または Cloud Volumes Services へのデータ移行には、使用するファイルプロトコルに応じて、NetApp XCP、BlueXP のコピーと同期、rsync、または Robocopy を使用します。
- テストでは、該当する SDDC からストレージにアクセスする際のレイテンシが 2 ~ 4 ミリ秒増加しました。ストレージをマッピングする際には、このレイテンシをアプリケーション要件に考慮してください。
- テストフェイルオーバーおよび実際のフェイルオーバー時にゲスト接続ストレージをマウントする場合は、iSCSI イニシエータが再設定されていること、SMB 共有の DNS が更新されていること、および NFS マウントポイントが fstab で更新されていることを確認してください。
- ゲスト内の Microsoft Multipath I/O (MPIO ; マルチパス I/O)、ファイアウォール、ディスクタイムアウトのレジストリ設定が VM 内で適切に設定されていることを確認します。



この環境ゲスト接続ストレージのみ。

ネットアップのクラウドストレージのメリット

ネットアップのクラウドストレージには次のようなメリットがあります。

- コンピューティングとストレージの別々にストレージを拡張できるため、コンピューティングとストレージの密度が向上します。
- ホスト数を削減し、全体的な TCO を削減できます。
- コンピューティングノードの障害は、ストレージのパフォーマンスには影響しません。
- Azure NetApp Files のボリュームの形状変更と動的なサービスレベル機能を使用すると、安定状態のワークロードのサイジングによってコストを最適化し、オーバープロビジョニングを防止できます。
- Cloud Volumes ONTAP の Storage Efficiency、クラウド階層化、インスタンスタイプの変更機能を使用すると、ストレージの追加や拡張を最適な方法で行うことができます。
- ストレージリソースのオーバープロビジョニングは、必要な場合にのみ発生します。
- 効率的な Snapshot コピーとクローンにより、パフォーマンスに影響を与えることなく迅速にコピーを作成できます。
- Snapshot コピーからの迅速なリカバリを使用して、ランサムウェア攻撃に対処できます。
- 複数のリージョン間で効率的なブロック転送ベースのリージョナルディザスタリカバリと統合されたバックアップブロックレベルを提供することで、RPO と RTO が向上します。

前提条件

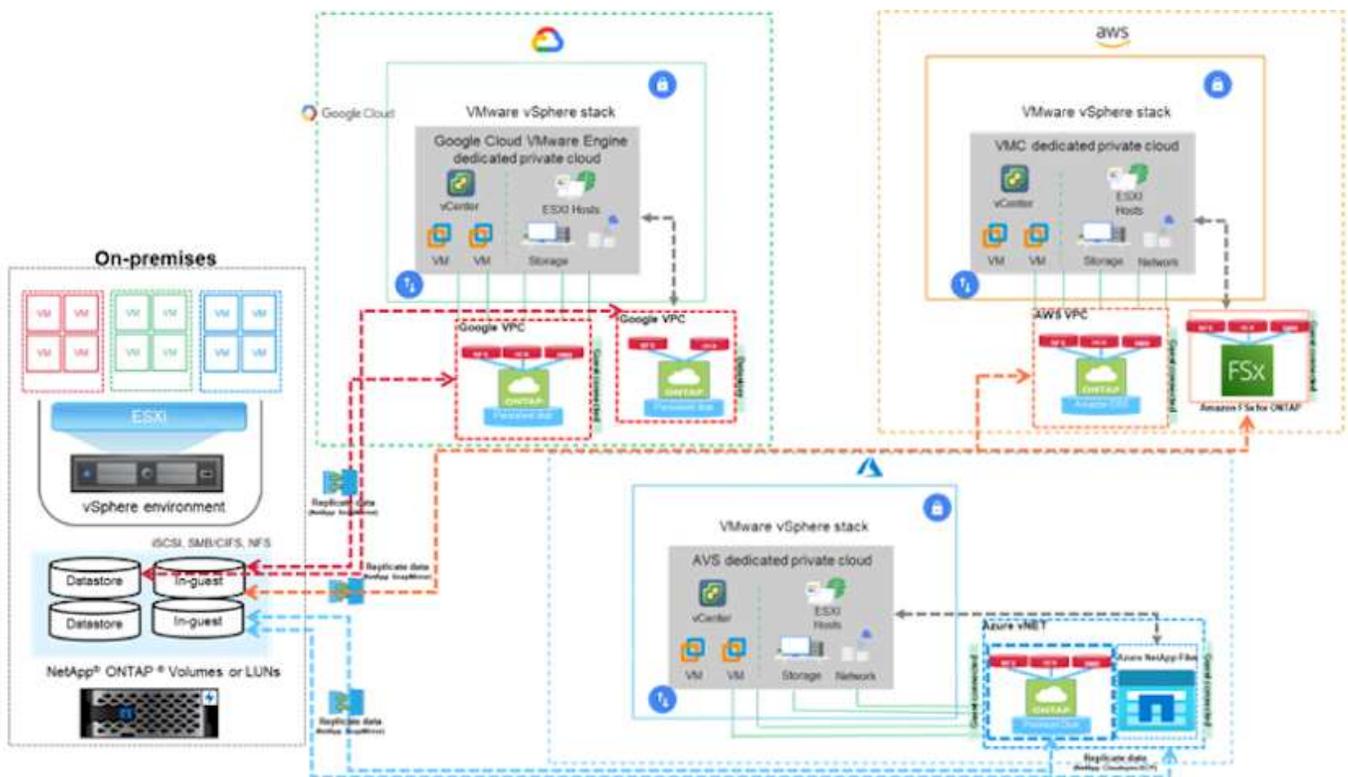
- SnapMirror テクノロジーやその他の関連するデータ移行メカニズムが有効になっている。オンプレミスから任意のハイパースケラクラウドまで、さまざまな接続オプションがあります。適切なパスを使用し、関連するネットワークチームと連携します。
- 本ドキュメントの作成時点で使用可能な唯一のオプションは、ゲスト内ストレージでした。 NFSデータストアの補足サポートが提供されるようになりましたが、それ以外のドキュメントも提供されます "[こちらをご覧ください](#)"。



ストレージの計画とサイジング、および必要なホスト数については、ネットアップの解決策アーキテクトと対応するハイパースケラクラウドアーキテクトに相談してください。 Cloud Volumes ONTAP サイジングツールを使用してストレージインスタンスのタイプや適切なサービスレベルを最終決定する前に、ストレージのパフォーマンス要件を特定することを推奨します。

詳細なアーキテクチャ

このアーキテクチャ（下の図を参照）では、NetApp Cloud Volumes ONTAP、Cloud Volumes Service for Google Cloud、Azure NetApp Files を追加のゲスト内ストレージオプションとして使用して、複数のクラウドプロバイダ間でハイブリッドマルチクラウド接続とアプリケーションのモビリティを実現する方法を大まかに説明します。



ハイパースケラにおける VMware 向けネットアップソリューション

ネットアップが提供する3つの主要ハイパースケラ（ゲスト接続ストレージデバイスまたはNFSデータストアとしてのネットアップ提供）の機能について、詳しくはこちらを

ご覧ください。また、ワークフローの移行、クラウドへの拡張/バースト対応、バックアップ/リストア、ディザスタリカバリも行っています。

クラウドを選択して、ネットアップに任せてください。



特定のハイパースケアラの機能を確認するには、そのハイパースケアラに適したタブをクリックします。

次のオプションから選択して、目的のコンテンツのセクションに移動します。

- ["ハイパースケアラ構成における VMware"](#)
- ["ネットアップストレージオプション"](#)
- ["ネットアップとVMwareのクラウドソリューション"](#)

ハイパースケアラ構成における **VMware**

オンプレミスと同様に、VM と移行を作成する本番環境に適したクラウドベースの仮想化環境を計画することが重要です。

AWS / VMC

このセクションでは、AWS SDDC で VMware Cloud をセットアップおよび管理する方法と、ネットアップストレージの接続に使用できるオプションについて説明します。



Cloud Volumes ONTAP をAWS VMCに接続する方法としてサポートされているのは、ゲスト内ストレージだけです。

セットアッププロセスは、次の手順に分けることができます。

- VMware Cloud for AWSを導入して設定
- VMware Cloud を FSX ONTAP に接続します

詳細を表示します ["VMCの設定手順"](#)。

Azure / AVS

このセクションでは、Azure VMware 解決策をセットアップおよび管理する方法と、ネットアップストレージの接続に使用できるオプションについて説明します。



Cloud Volumes ONTAP をAzure VMware解決策 に接続する方法としてサポートされているのは、ゲスト内ストレージだけです。

セットアッププロセスは、次の手順に分けることができます。

- リソースプロバイダを登録し、プライベートクラウドを作成
- 新しい ExpressRoute 仮想ネットワークゲートウェイまたは既存の ExpressRoute 仮想ネットワークゲートウェイに接続します
- ネットワーク接続を検証し、プライベートクラウドにアクセス

詳細を表示します ["AVSの設定手順"](#)。

GCP/GCVE

このセクションでは、GCVE のセットアップと管理方法、およびネットアップストレージの接続に使用できるオプションとの組み合わせについて説明します。



Cloud Volume と Cloud Volumes ONTAP サービスを GCVE に接続する方法としてサポートされているのは、ゲスト内ストレージだけです。

セットアッププロセスは、次の手順に分けることができます。

- GCVE を導入および設定します
- GCVE へのプライベートアクセスを有効にします

詳細を表示します ["GCVEの設定手順"](#)。

ネットアップストレージオプション

ネットアップストレージは、3大ハイパースケーラのそれぞれで、ゲスト接続として、または補完的なNFSデータストアとして、いくつかの方法で利用できます。

にアクセスしてください ["サポートされているネットアップストレージオプション"](#) を参照してください。

AWS / VMC

AWS は、次の構成でネットアップストレージをサポートします。

- ゲスト接続ストレージとしての FSX ONTAP
- Cloud Volumes ONTAP (CVO) をゲスト接続ストレージとして活用
- 補完的なNFSデータストアとしてのFSX ONTAP

詳細を表示します ["VMCのゲスト接続ストレージオプション"](#)。詳細を表示します ["VMCの追加のNFSデータストアオプション"](#)。

Azure / AVS

Azure は、以下の構成でネットアップストレージをサポートします。

- ゲスト接続ストレージとしての Azure NetApp Files (ANF)
- Cloud Volumes ONTAP (CVO) をゲスト接続ストレージとして活用
- Azure NetApp Files (ANF) を追加のNFSデータストアとして使用できます

詳細を表示します ["AVSのゲスト接続ストレージオプション"](#)。詳細を表示します ["AVSの補完的なNFSデータストアオプション"](#)。

GCP/GCVE

Google Cloud は、次の構成でネットアップストレージをサポートします。

- Cloud Volumes ONTAP (CVO) をゲスト接続ストレージとして活用
- Cloud Volumes Service (CVS) をゲスト接続ストレージとして使用できるようになりました
- Cloud Volumes Service (CVS) をNFSデータストアとして追加

詳細を表示します ["GCVEのゲスト接続ストレージオプション"](#)。

詳細については、をご覧ください ["NetApp Cloud Volumes Service データストアでのGoogle Cloud VMware Engineのサポート \(ネットアップブログ\)"](#) または ["ネットアップCVSをGoogle Cloud VMware Engineのデータストアとして使用する方法 \(Googleブログ\)"](#)

ネットアップとVMwareのクラウドソリューション

ネットアップとVMwareのクラウドソリューションを使用すれば、さまざまなユースケースをハイパースケーラに簡単に導入できます。VMwareは、主なクラウドワークロードのユースケースを次のように定義しています。

- 保護 (ディザスタリカバリとバックアップ/リストアの両方を含む)

- 移動
- 拡張

AWS / VMC

"ネットアップのAWS / VMC向けソリューションをご確認ください"

Azure / AVS

"ネットアップのAzure / AVS向けソリューションをご覧ください"

GCP/GCVE

"Google Cloud Platform (GCP) / GCVE向けのネットアップソリューションをご覧ください"

VMwareでサポートされるネットアップハイブリッドマルチクラウドの構成

主要なハイパースケアラにおけるネットアップストレージサポートの組み合わせを理解している。

	ゲスト接続	* NFSデータストアの追加*
* AWS *	CVO FSX ONTAP "詳細"	FSX ONTAP の略 "詳細"
* Azure *	CVOのANF "詳細"	ANF "詳細"
* GCP *	CVO CVS "詳細"	CVS "詳細"

ハイパースケアラ構成における VMware

クラウドプロバイダでの仮想化環境の設定

サポートされている各ハイパースケアラで仮想化環境を設定する方法については、こちらで詳しく説明しています。

AWS / VMC

このセクションでは、AWS SDDC で VMware Cloud をセットアップおよび管理する方法と、ネットアップストレージの接続に使用できるオプションについて説明します。



Cloud Volumes ONTAP をAWS VMCに接続する方法としてサポートされているのは、ゲスト内ストレージだけです。

セットアッププロセスは、次の手順に分けることができます。

- VMware Cloud for AWSを導入して設定
- VMware Cloud を FSX ONTAP に接続します

詳細を表示します ["VMCの設定手順"](#)。

Azure / AVS

このセクションでは、Azure VMware 解決策をセットアップおよび管理する方法と、ネットアップストレージの接続に使用できるオプションについて説明します。



Cloud Volumes ONTAP をAzure VMware解決策 に接続する方法としてサポートされているのは、ゲスト内ストレージだけです。

セットアッププロセスは、次の手順に分けることができます。

- リソースプロバイダを登録し、プライベートクラウドを作成
- 新しい ExpressRoute 仮想ネットワークゲートウェイまたは既存の ExpressRoute 仮想ネットワークゲートウェイに接続します
- ネットワーク接続を検証し、プライベートクラウドにアクセス

詳細を表示します ["AVSの設定手順"](#)。

GCP/GCVE

このセクションでは、GCVE のセットアップと管理方法、およびネットアップストレージの接続に使用できるオプションとの組み合わせについて説明します。



Cloud Volume と Cloud Volumes ONTAP サービスを GCVE に接続する方法としてサポートされているのは、ゲスト内ストレージだけです。

セットアッププロセスは、次の手順に分けることができます。

- GCVE を導入および設定します
- GCVE へのプライベートアクセスを有効にします

詳細を表示します ["GCVEの設定手順"](#)。

AWS に仮想化環境を導入して設定

オンプレミスと同様に、VM と移行を作成する本番環境に適した VMware Cloud on AWS を計画することが重要です。

このセクションでは、AWS SDDC で VMware Cloud をセットアップおよび管理する方法と、ネットアップストレージの接続に使用できるオプションについて説明します。



現在、Cloud Volumes ONTAP (CVO) をAWS VMCに接続する方法としてサポートされているのは、ゲスト内ストレージだけです。

セットアッププロセスは、次の手順に分けることができます。

VMware Cloud for AWS を導入して設定

"AWS 上の VMware Cloud" AWS エコシステム内の VMware ベースのワークロードにクラウドネイティブのエクスペリエンスを提供します。各 VMware Software-Defined Data Center (SDDC) は Amazon Virtual Private Cloud (VPC) 内で動作し、フル VMware スタック (vCenter Server を含む)、NSX ベースの Software-Defined Networking、VSAN ソフトウェア定義ストレージ、およびワークロードにコンピューティングリソースとストレージリソースを提供する 1 つ以上の ESXi ホストを提供します。

このセクションでは、AWS で VMware Cloud をセットアップおよび管理する方法について説明します。また、AWS で NetApp ONTAP を使用する場合は Amazon FSX、ゲスト内ストレージを使用する場合は Cloud Volumes ONTAP と組み合わせて使用する方法についても説明します。



現在、Cloud Volumes ONTAP (CVO) を AWS VMC に接続する方法としてサポートされているのは、ゲスト内ストレージだけです。

セットアッププロセスは、次の 3 つの部分に分けることができます。

AWS アカウントを登録

に登録します ["Amazon Web Services アカウント"](#)。

まだ作成していない場合は、AWS アカウントが必要です。新規または既存の手順では、多くの手順を実行するためにアカウント内で管理者権限が必要です。を参照してください ["リンク"](#) をクリックしてください。

My VMware アカウントに登録します

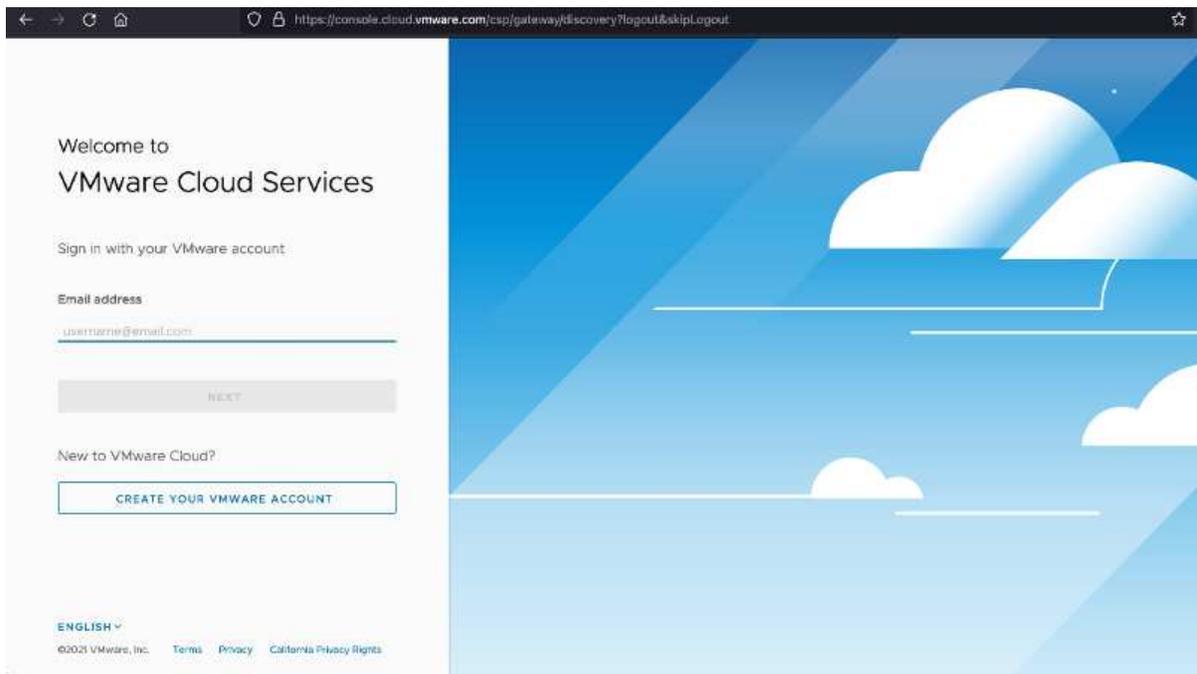
に登録します ["マイ VMware"](#) アカウント：

VMware のクラウドポートフォリオ (AWS 上の VMware Cloud を含む) にアクセスするには、VMware の顧客アカウントまたは My VMware アカウントが必要です。VMware アカウントをまだ作成していない場合は作成します ["こちらをご覧ください"](#)。

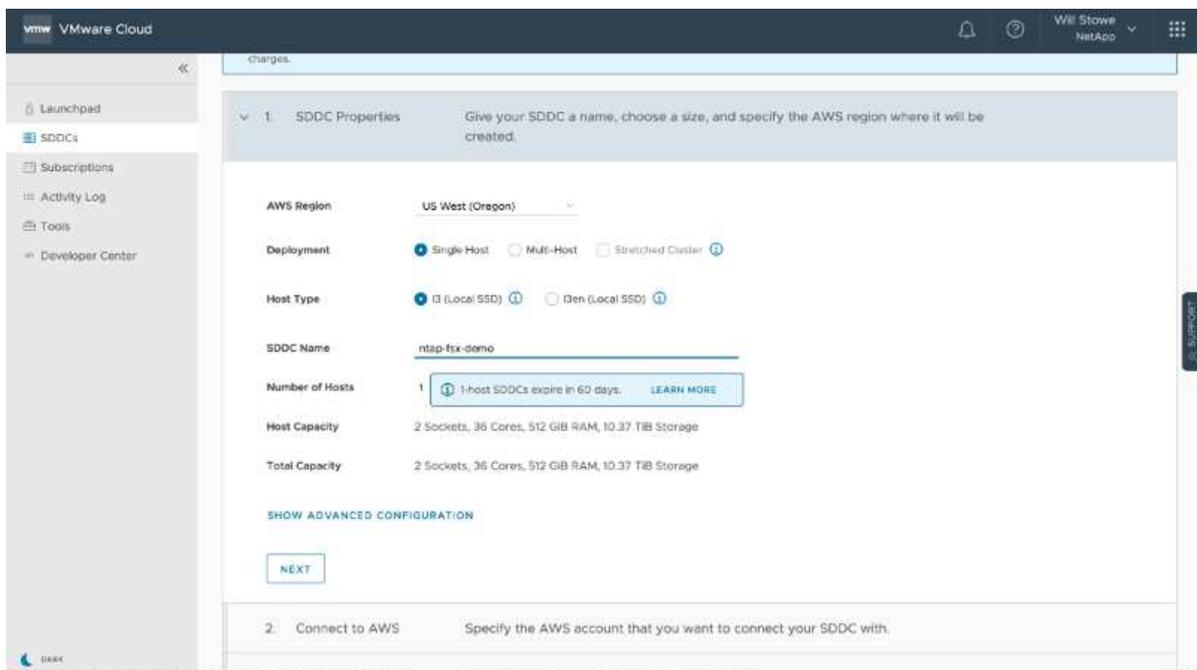
VMware Cloud で SDDC をプロビジョニングします

VMware アカウントを設定して適切なサイジングを実行したら、AWS サービスで VMware Cloud を使用するための次の一步として Software-Defined Data Center を導入します。SDDC を作成するには、そのホストとして AWS リージョンを選択し、SDDC に名前を付け、SDDC に含める ESXi ホストの数を指定します。AWS アカウントがない場合でも、単一の ESXi ホストを含むスターター構成の SDDC を作成できます。

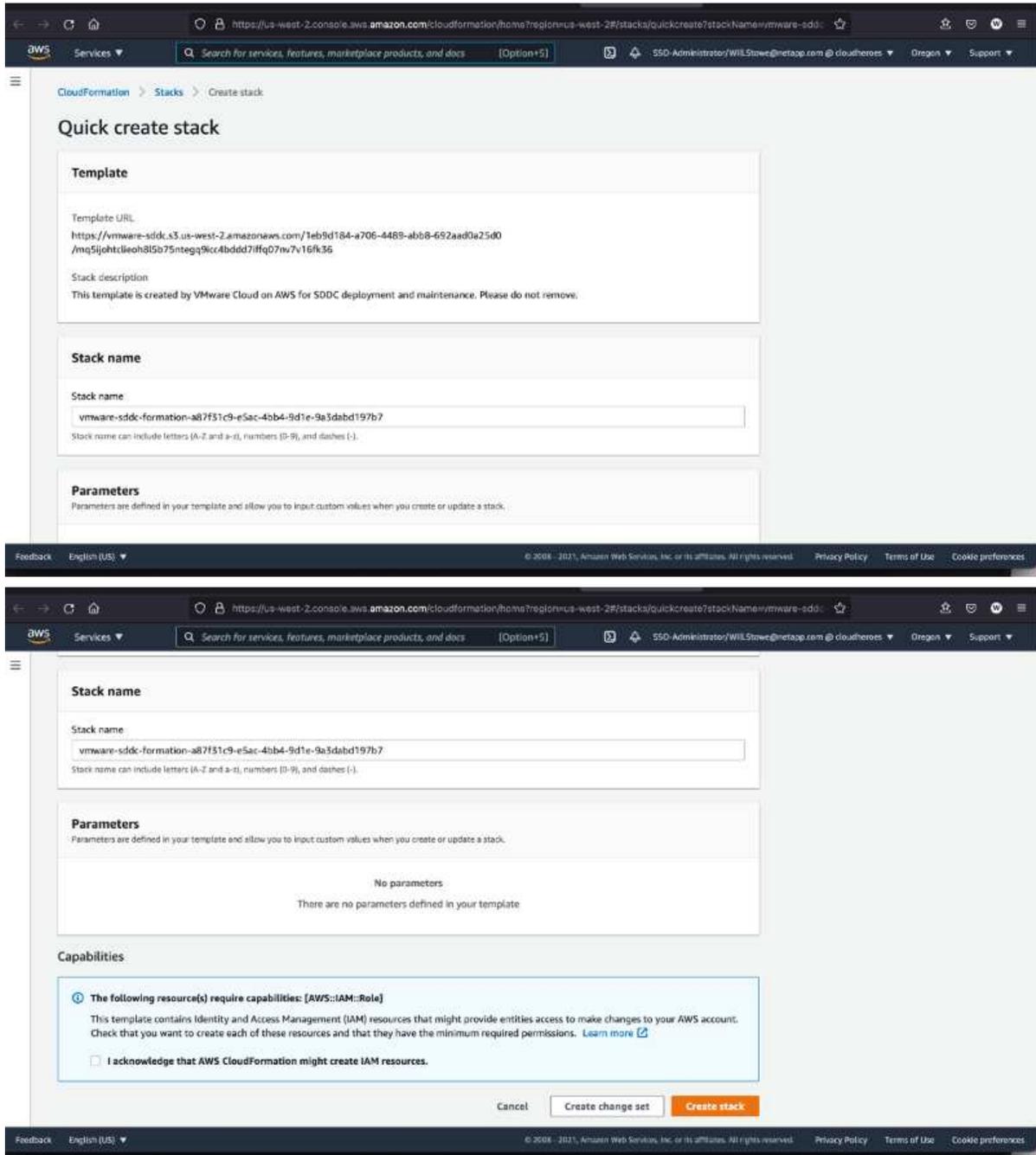
1. 既存または新規に作成した VMware クレデンシャルを使用して、VMware Cloud Console にログインします。

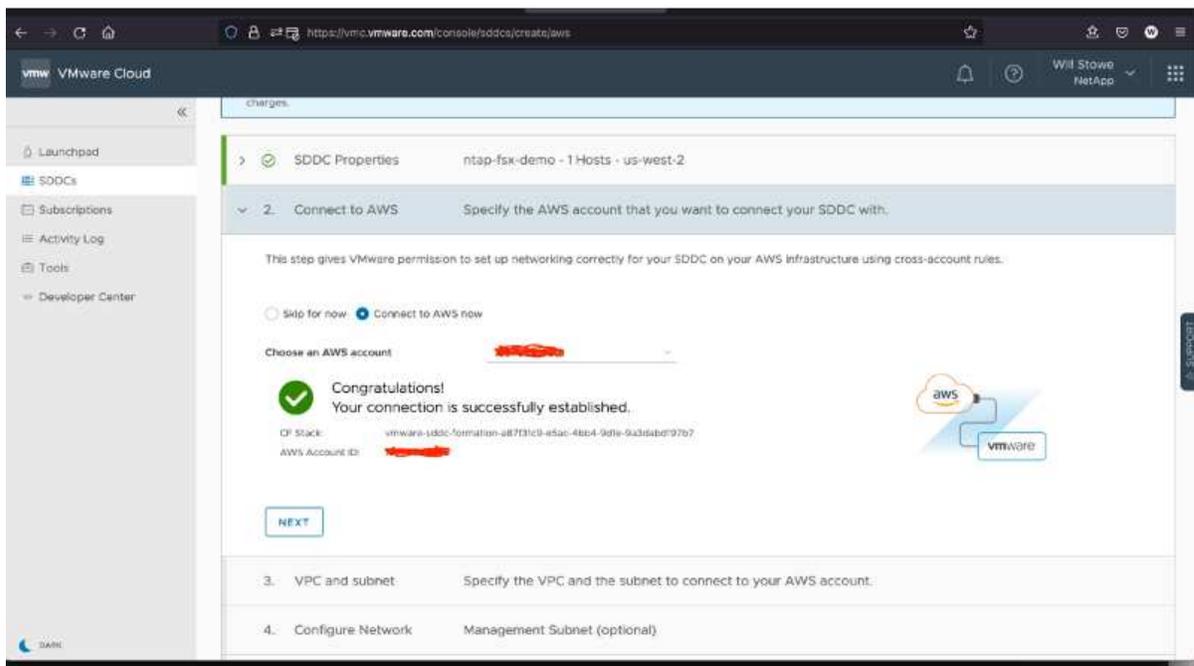
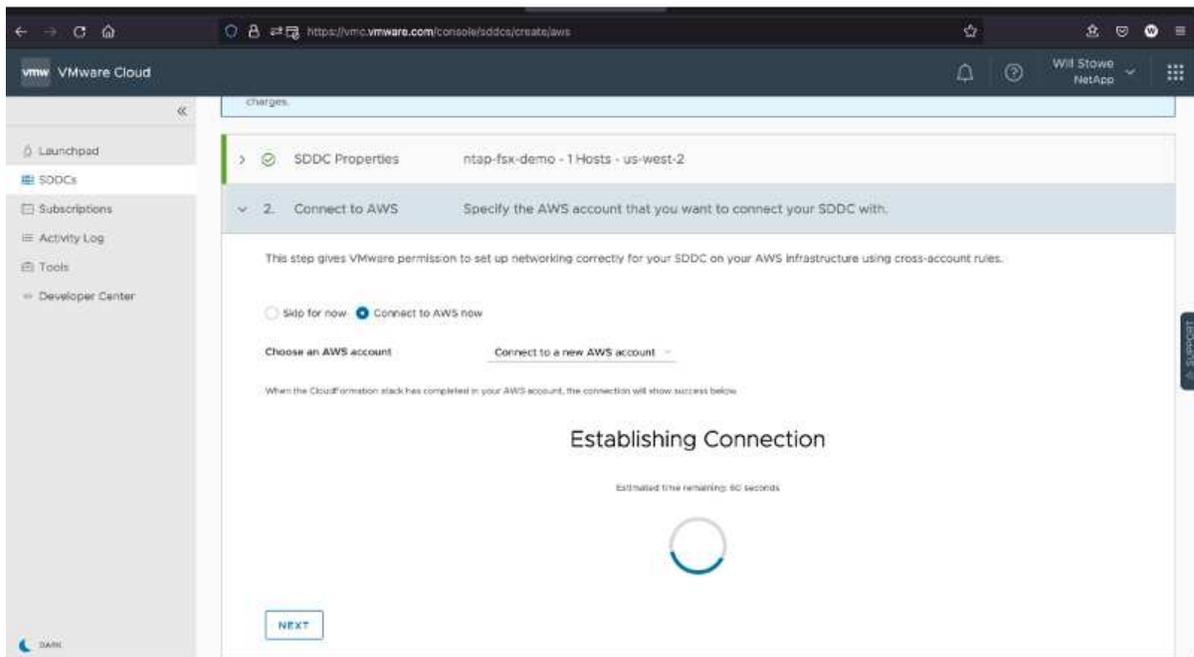


2. AWS のリージョン、導入環境、およびホストタイプと SDDC 名を設定します。



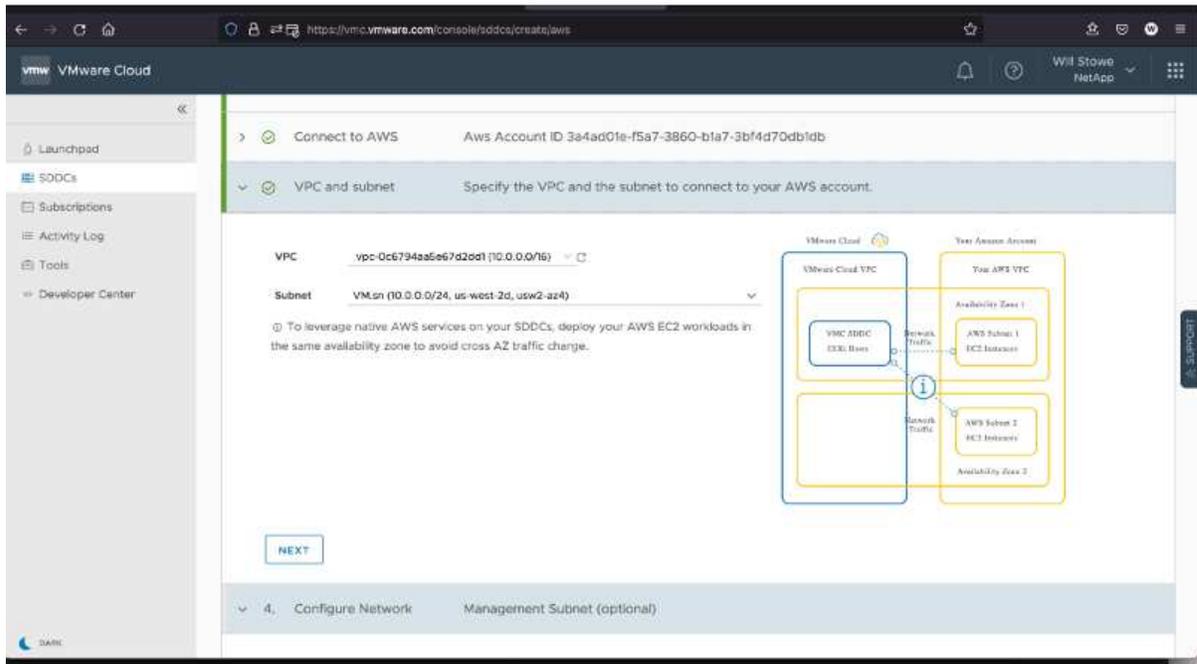
3. 目的の AWS アカウントに接続し、AWS クラウド形成スタックを実行します。



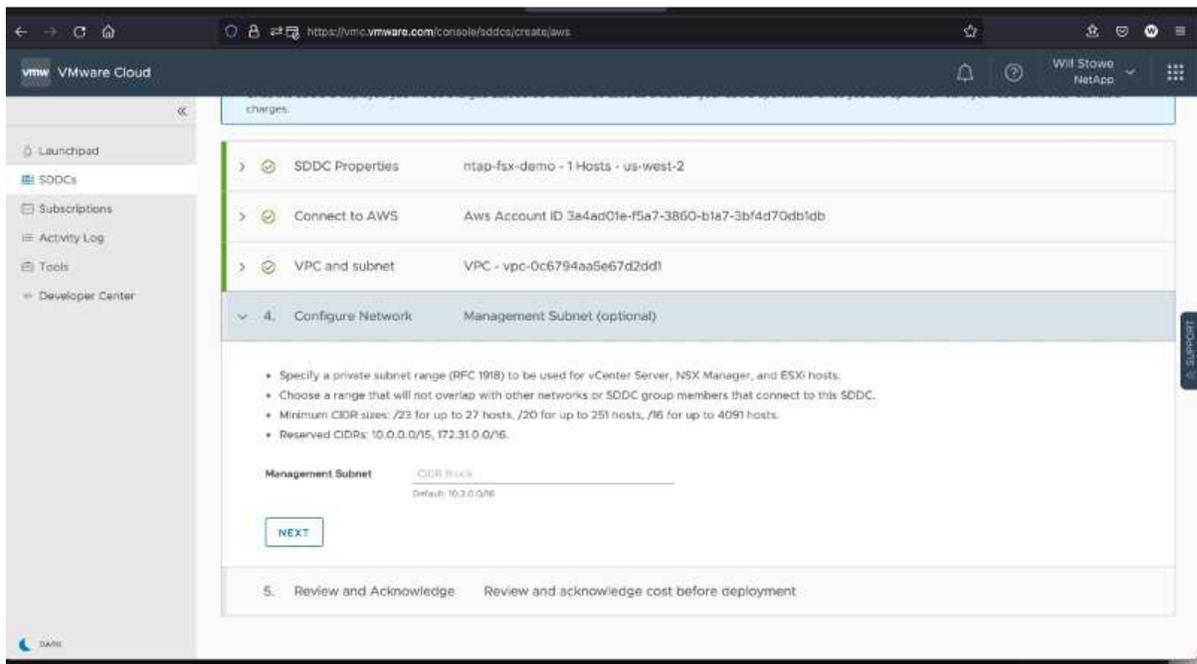


この検証ではシングルホスト構成を使用します。

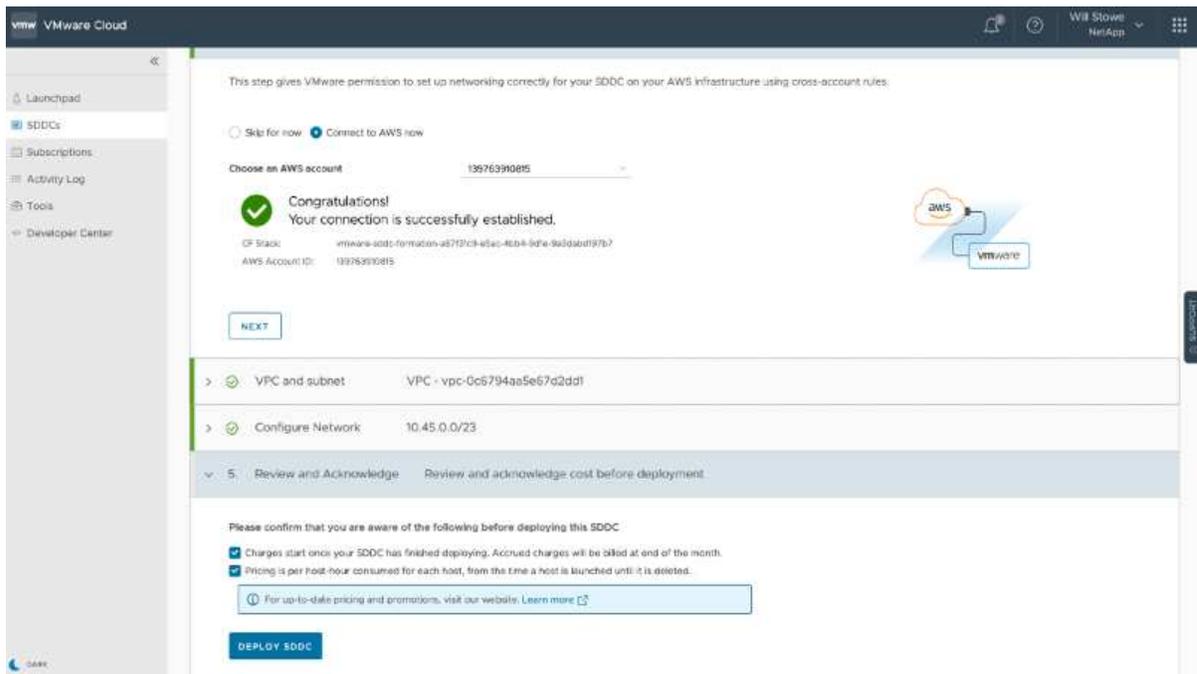
4. VMC 環境を接続する AWS VPC を選択します。



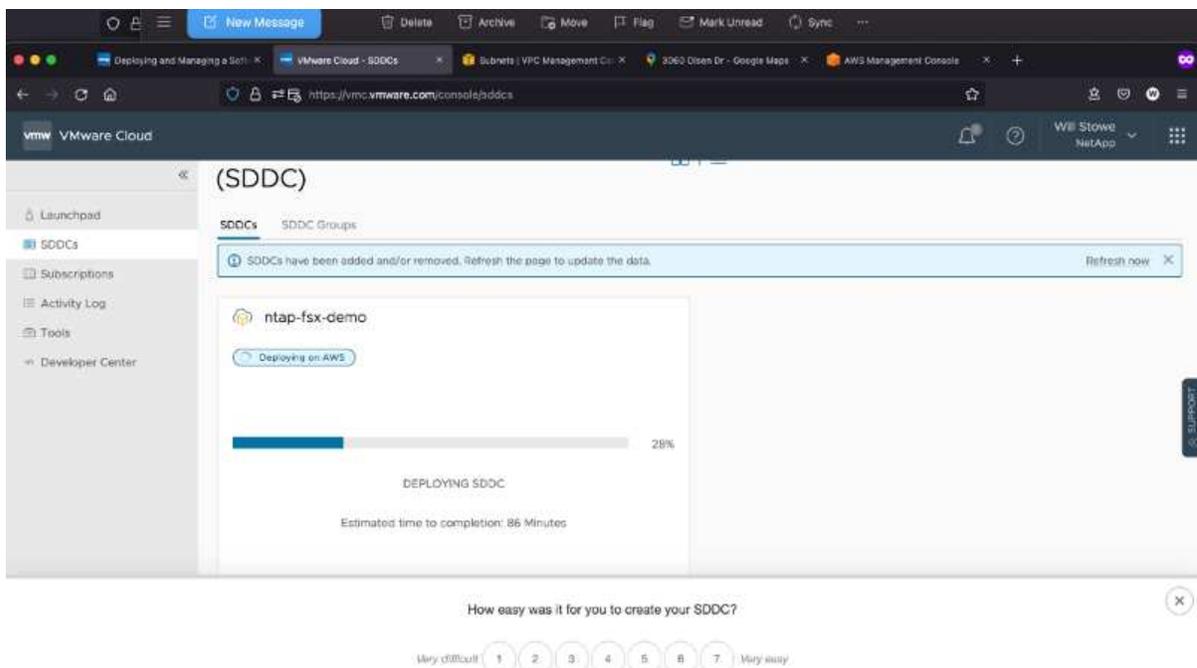
5. VMC 管理サブネットを構成します。このサブネットには、vCenter や NSX などの VMC 管理サービスが含まれます。SDDC 環境への接続が必要な他のネットワークと重複するアドレス空間を選択しないでください。最後に、以下に示す CIDR サイズの推奨事項に従います。



6. SDDC 構成を確認して承認し、[Deploy the SDDC] をクリックします。



導入プロセスの完了には、通常約 2 時間かかります。



7. 完了すると、SDDC を使用できるようになります。

The screenshot displays the VMware Cloud interface for Software-Defined Data Centers (SDDC). The main heading is "Software-Defined Data Centers (SDDC)". On the left, a navigation sidebar includes "Launchpad", "SDDCs", "Subscriptions", "Activity Log", "Tools", and "Developer Center". The top right corner shows "VMware Store NetApp" and a user profile icon. Below the heading, there are buttons for "CREATE SDDC" and "ACTIONS". The main content area shows details for an SDDC named "ntap-fsx-demo", which is in a "Ready" state. A table lists the following details:

Property	Value	Count
Region	US West (Oregon)	1
Type	VMC on AWS SDDC	1
Availability Zones	US-WEST-2a	36
	VMC on AWS SDDC	

Below the table, resource usage is summarized:

- CPU: 82.8 GHz
- Memory: 512 GiB
- Storage: 10.37 TiB

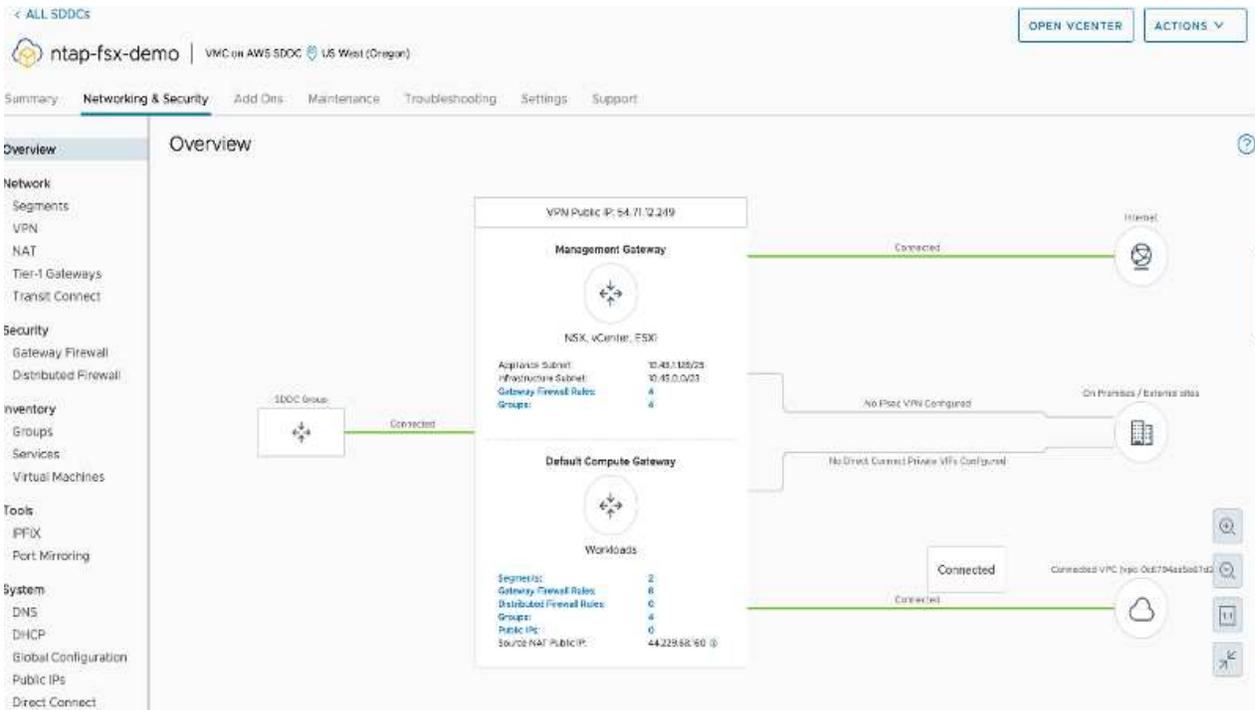
At the bottom of the details panel, there are links for "VIEW DETAILS", "OPEN VCENTER", and "ACTIONS". At the very bottom of the interface, there are links for "BACK TO TOP" and "GO TO GRID VIEW".

SDDC の導入の詳細な手順については、を参照してください "[VMC コンソールから SDDC を展開します](#)".

VMware Cloud を FSX ONTAP に接続します

VMware Cloud を FSX ONTAP に接続するには、次の手順を実行します。

1. VMware Cloud の導入が完了して AWS VPC に接続されているため、Amazon FSX for NetApp ONTAP を、元の接続済み VPC ではなく新しい VPC に導入する必要があります（以下のスクリーンショットを参照）。接続された VPC に FSX（NFS および SMB のフローティング IP）が導入されている場合、これらの IP にはアクセスできません。Cloud Volumes ONTAP のような iSCSI エンドポイントは、接続された VPC からは正常に機能します。



2. 同じリージョンに別の VPC を導入し、その新しい VPC に Amazon FSX for NetApp ONTAP を導入します。

VMware Cloud コンソールで SDDC グループを構成すると、FSX が導入された新しい VPC に接続するために必要なネットワーク設定オプションが有効になります。手順 3 で、「グループ用の VMware トランジット接続の構成に添付ファイルおよびデータ転送ごとの料金が発生する」がチェックされていることを確認し、「グループの作成」を選択します。このプロセスが完了するまでに数分かかることがあります。

VMware Cloud

WBI Stowe NetApp

< Create SDDC Group

1. Name and Description Create a name and description for your group

Name

Description

NEXT

2. Membership Members: 1

3. Acknowledgement

Please confirm that you are aware of the following before creating this SDDC Group.

Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.

Create firewall rules to establish connectivity between the SDDCs in the group. [Learn More](#)

CREATE GROUP

VMware Cloud

WBI Stowe NetApp

< Create SDDC Group

1. Name and Description Name: sddcgroup01

2. Membership Select SDDCs to be part of your group

<input checked="" type="checkbox"/>	Name	Site ID	Location	Version	Management OSB
<input checked="" type="checkbox"/>	ntap-5xx-demo	829b6e22-92af-42db-acd3-9e4e07a908b5	US West (Oregon)	1.14.0.14	10.45.0.0/23

Items per page: 100 1-1 of 1 items

NEXT

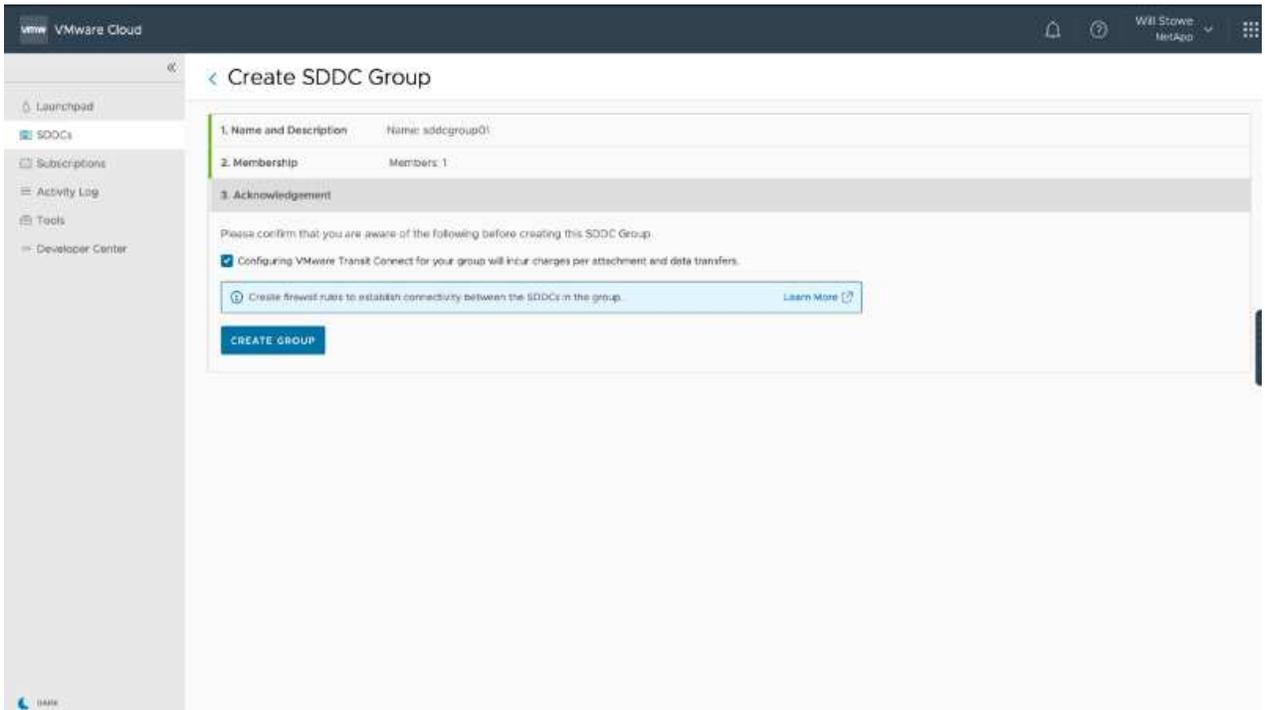
3. Acknowledgement Review and acknowledge requirements before creating the group.

Please confirm that you are aware of the following before creating this SDDC Group.

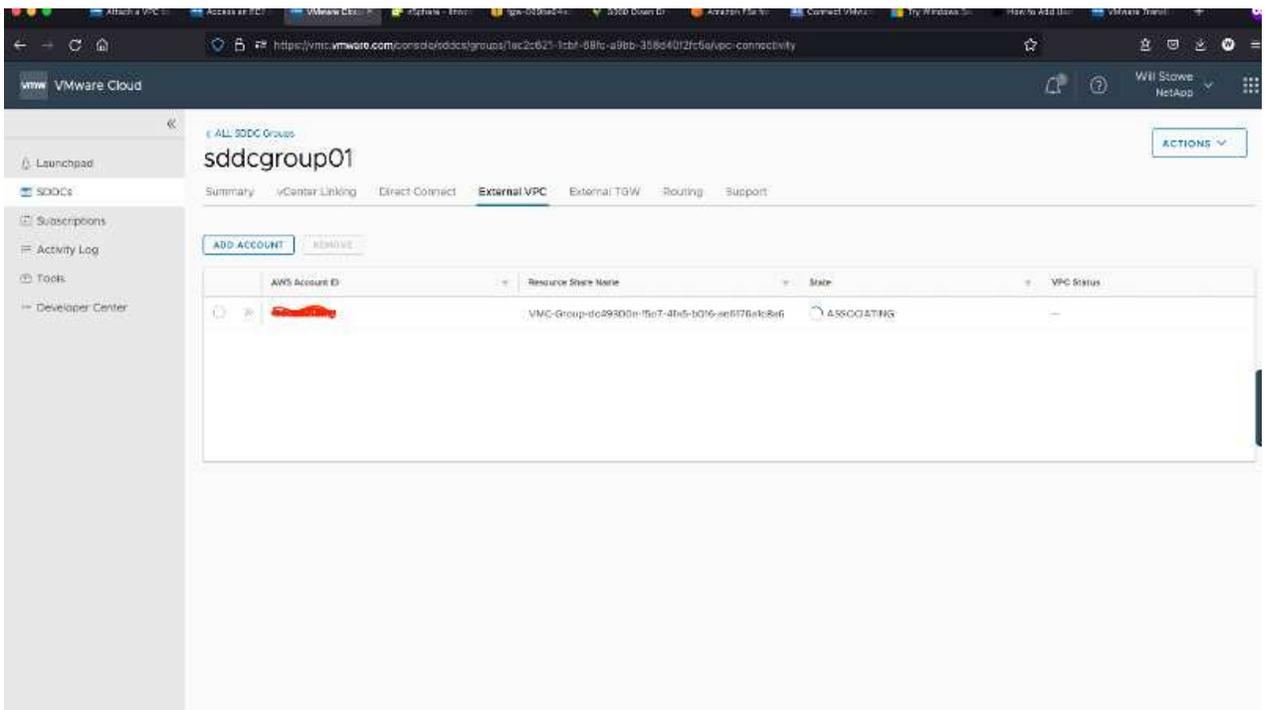
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.

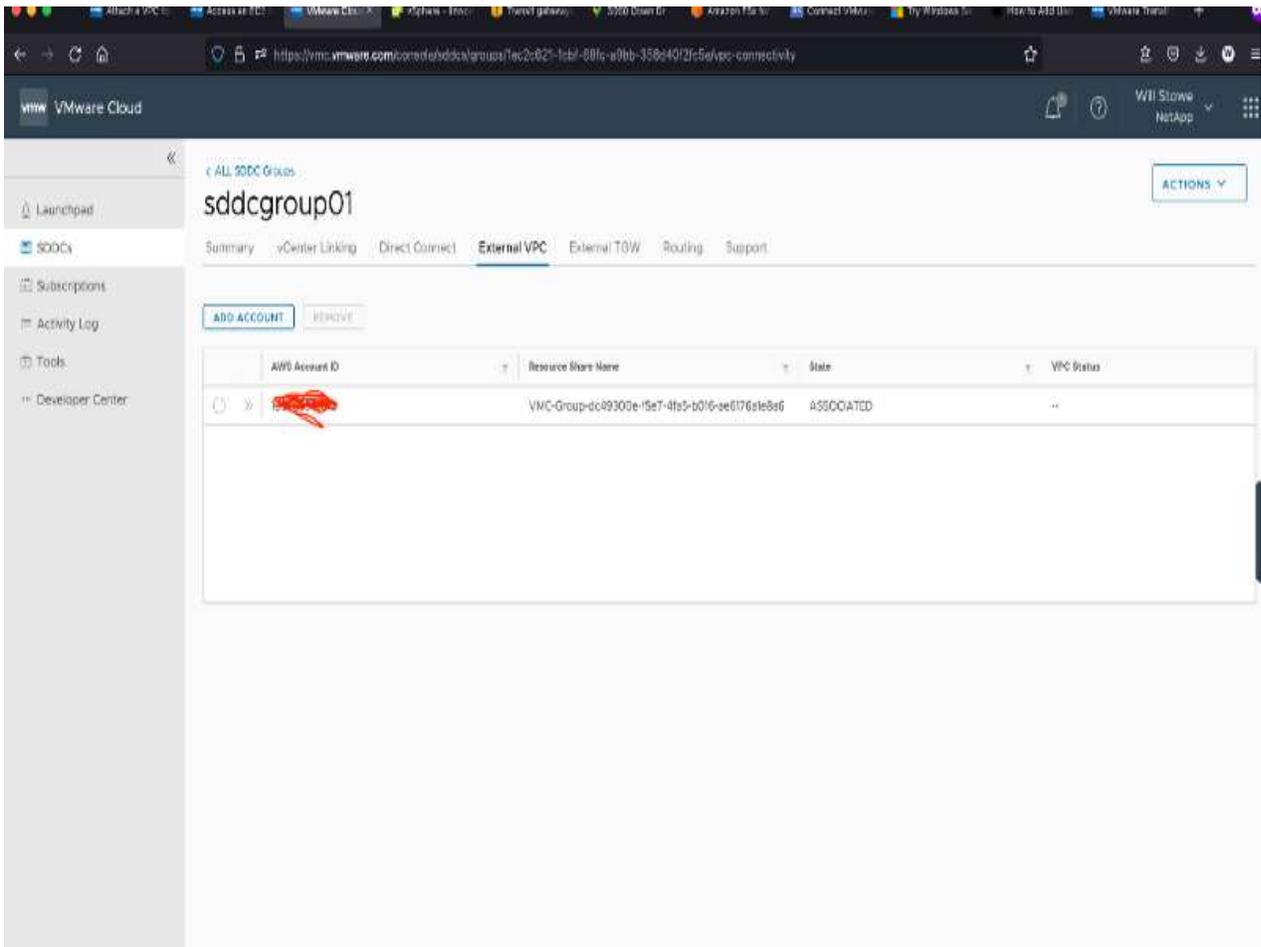
Create firewall rules to establish connectivity between the SDDCs in the group. [Learn More](#)

CREATE GROUP

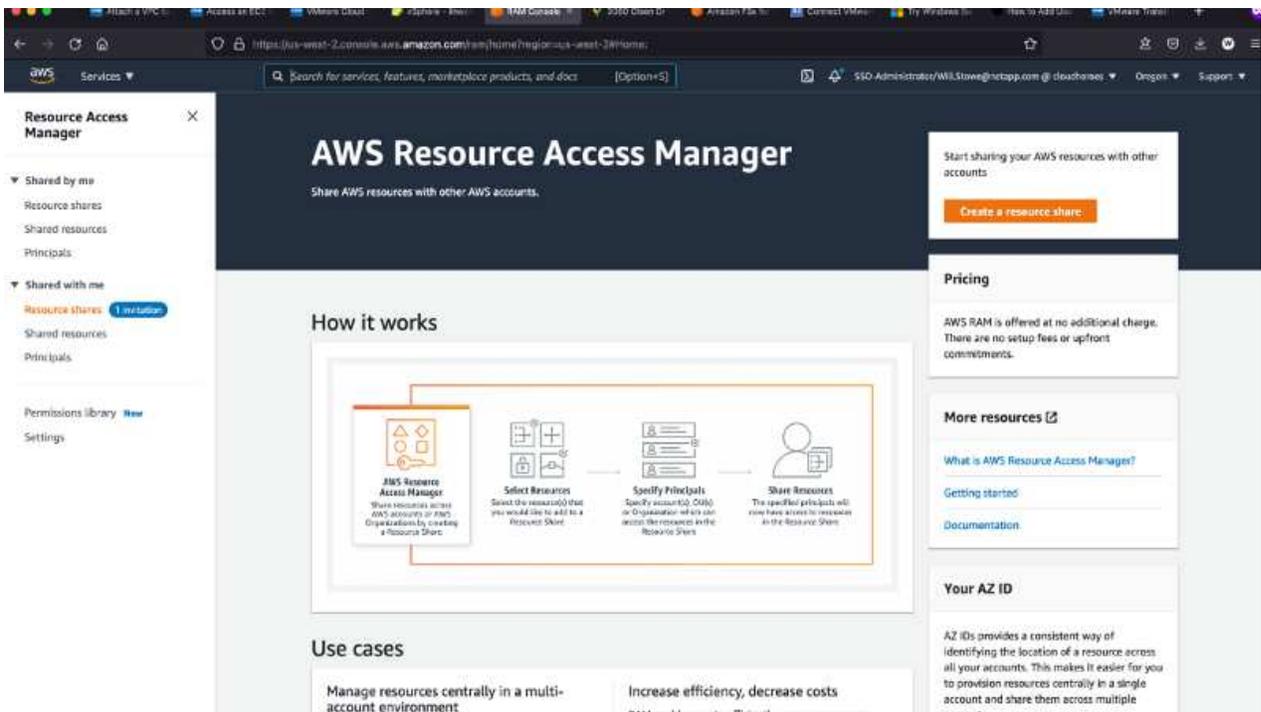


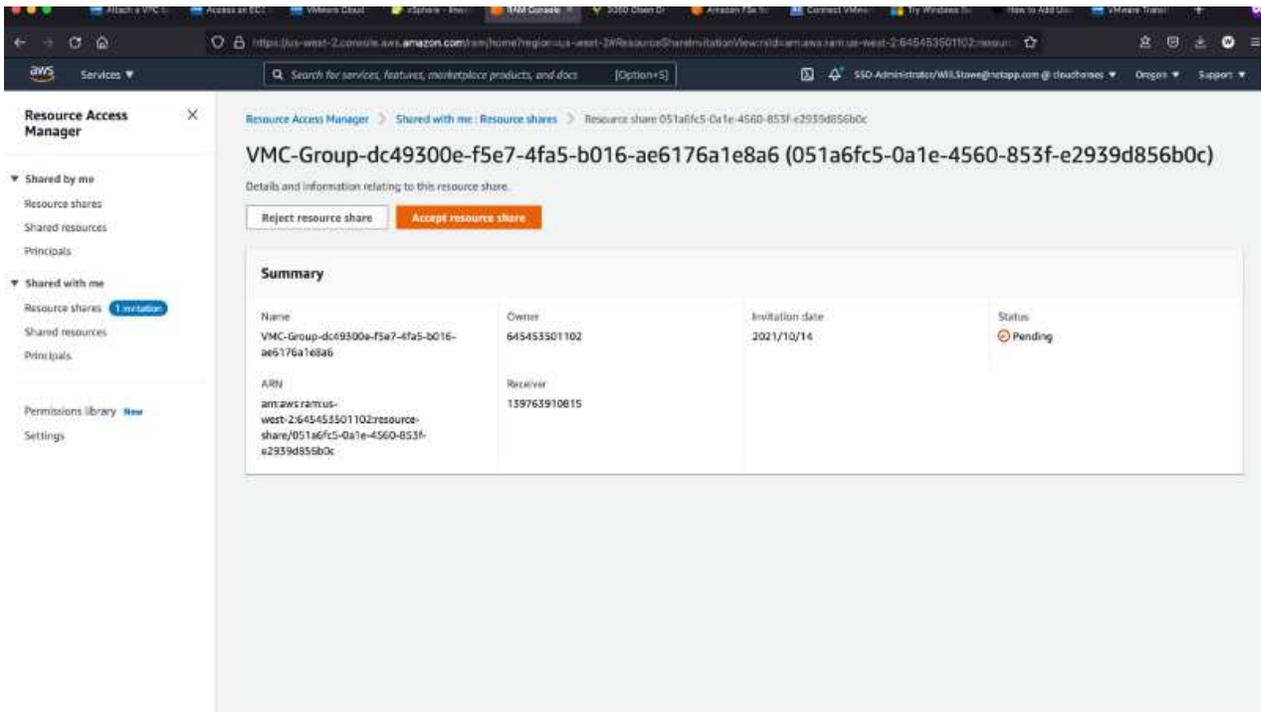
3. 新しく作成した VPC を作成した SDDC グループに接続します。[External VPC (外部 VPC)] タブを選択し、に従います "外部 VPC を接続する手順" をグループに追加します。このプロセスが完了するまでに 10~15 分かかることがあります。



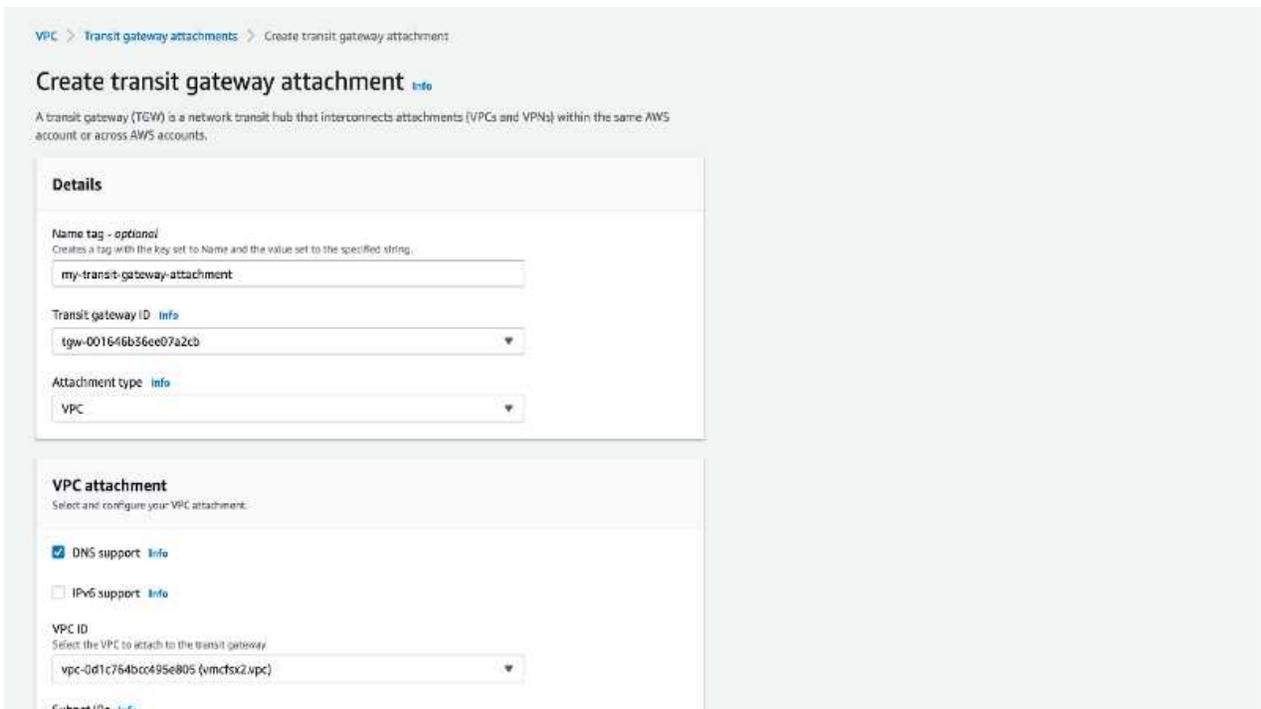


4. 外部 VPC プロセスの一環として、AWS コンソールから Resource Access Manager を使用して新しい共有リソースにアクセスするように求められます。共有リソースはです "AWS 転送ゲートウェイ" VMware Transit Connect によって管理されます。

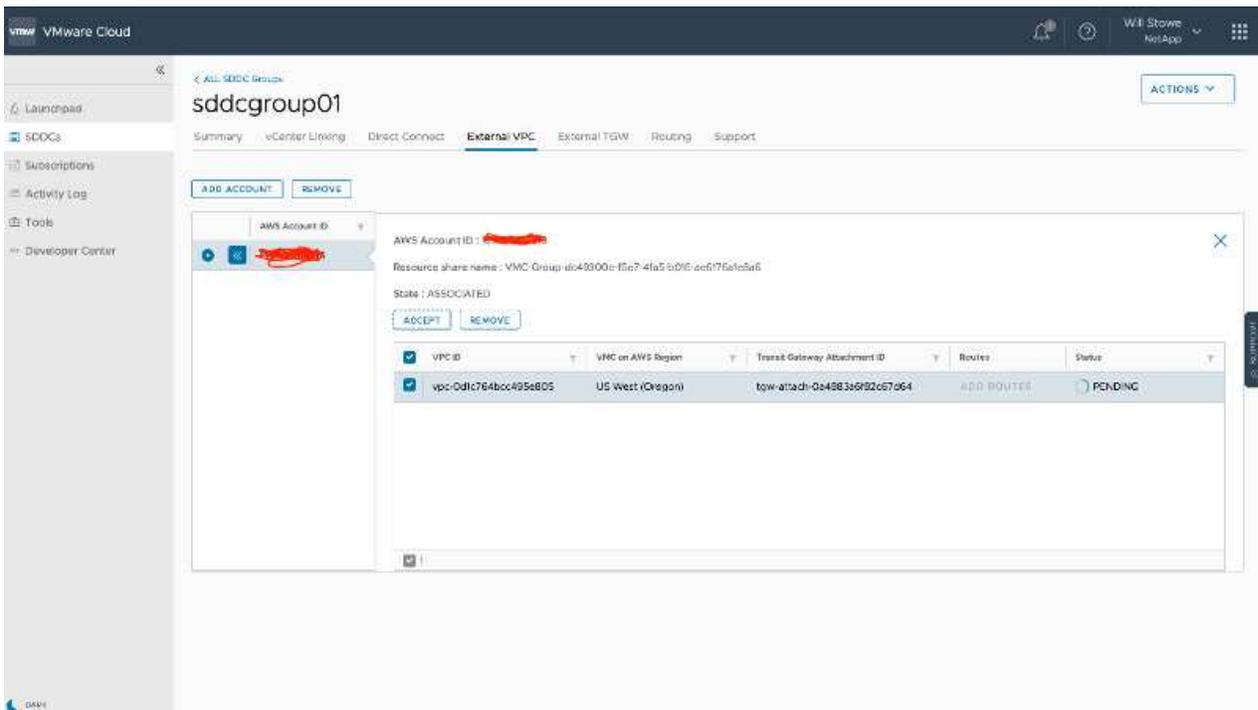




5. トランジットゲートウェイ添付ファイルを作成します。

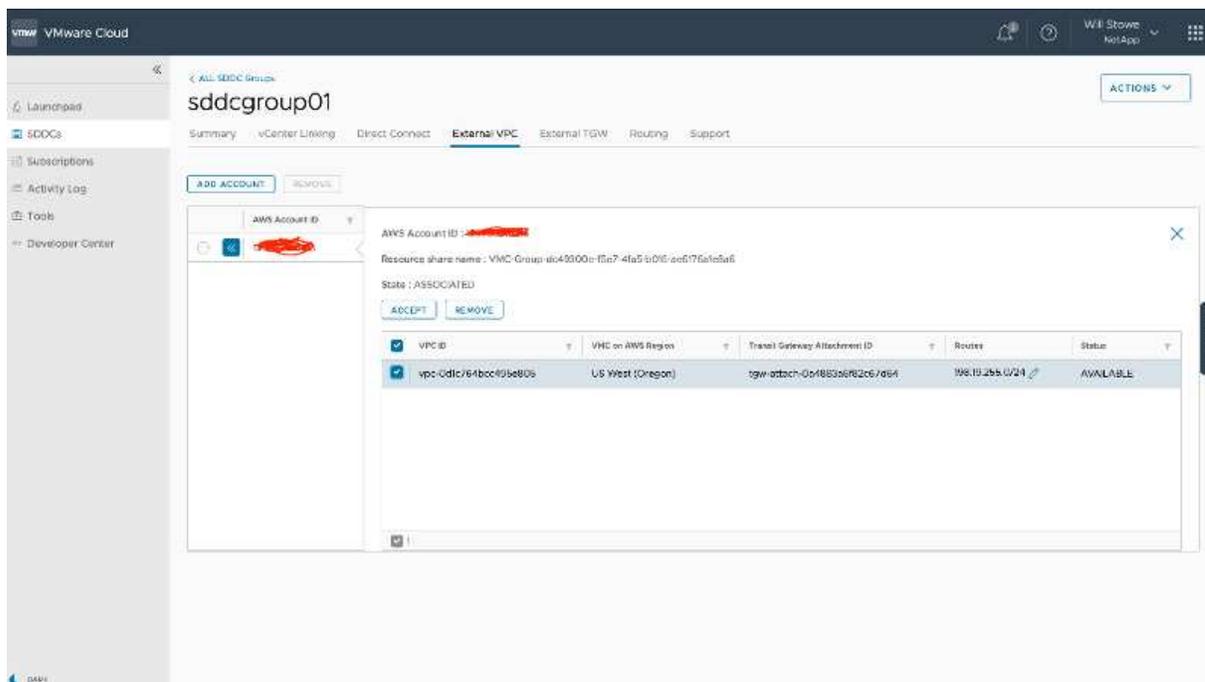


6. VMC コンソールに戻り、VPC 接続を受け入れます。この処理が完了するまでに約 10 分かかります。

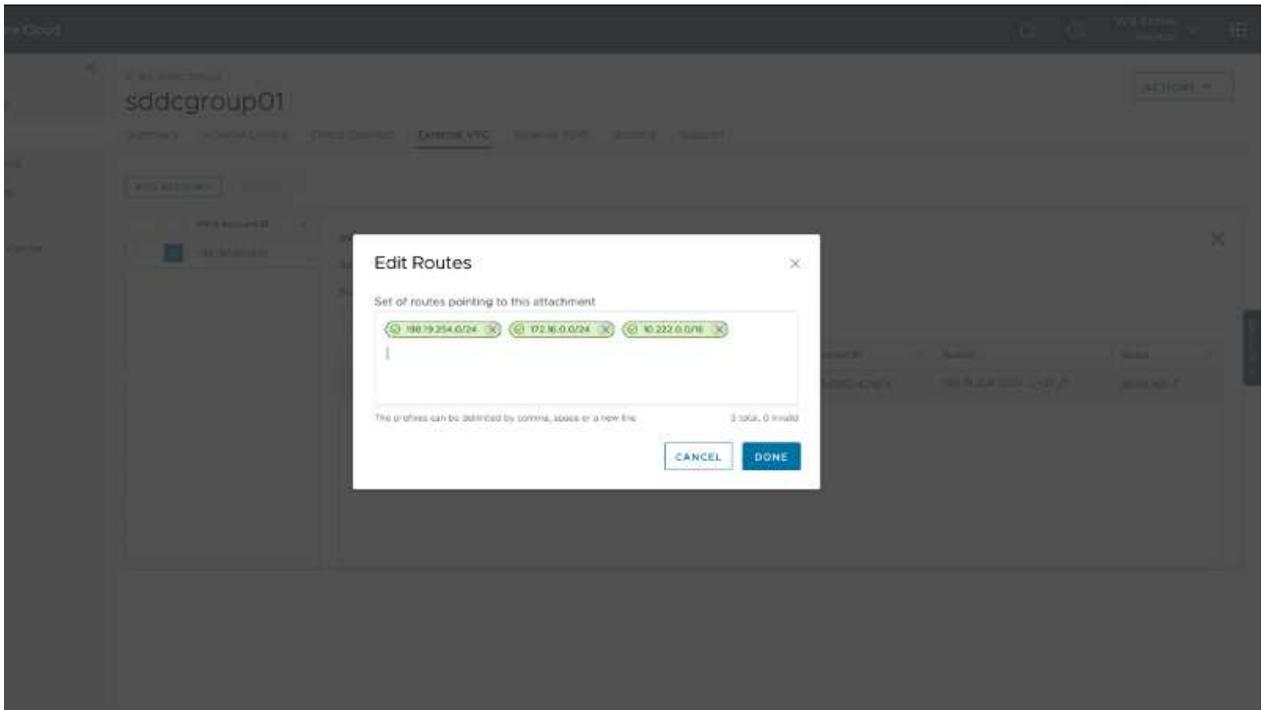


7. [External VPC (外部 VPC)] タブで、[Routes] 列の編集アイコンをクリックし、次の必要なルートを追加します。

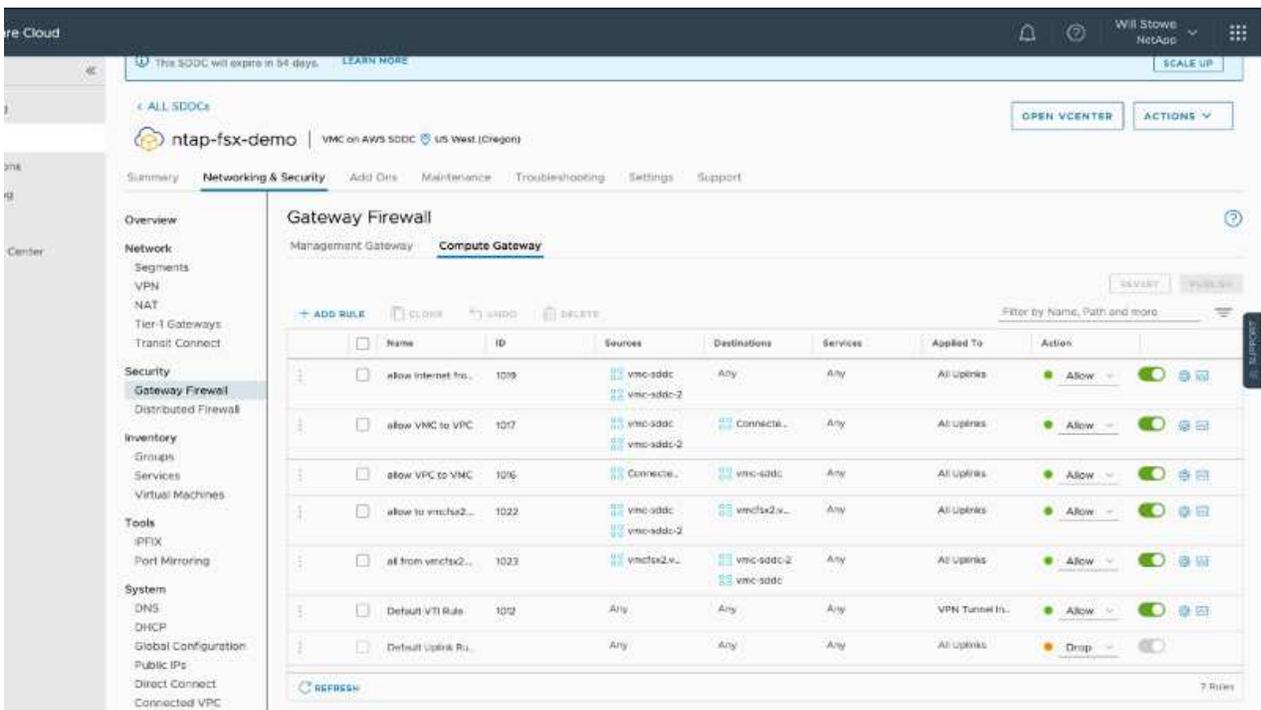
- NetApp ONTAP の Amazon FSX のフローティング IP 範囲のルート **"フローティング IP"**。
- Cloud Volumes ONTAP のフローティング IP 範囲のルート (該当する場合)。
- 新しく作成される外部 VPC アドレススペースのルート。



8. 最後に、双方向トラフィックを許可します **"ファイアウォールルール"** FSX/CVO へのアクセスに必要です。以下の手順に従ってください **"詳細な手順"** SDDC ワークロード接続用のコンピューティングゲートウェイファイアウォールルール用。



9. 管理ゲートウェイとコンピューティングゲートウェイの両方にファイアウォールグループを設定したら、次の手順で vCenter にアクセスできます。



次の手順では、Amazon FSX ONTAP または Cloud Volumes ONTAP が要件に応じて設定されていること、およびストレージコンポーネントを VSAN からオフロードして導入を最適化するようにボリュームがプロビジョニングされていることを確認します。

Azure に仮想化環境を導入して設定

オンプレミスと同様に、Azure VMware 解決策を計画することは、VM と移行を作成する本番環境に欠かせません。

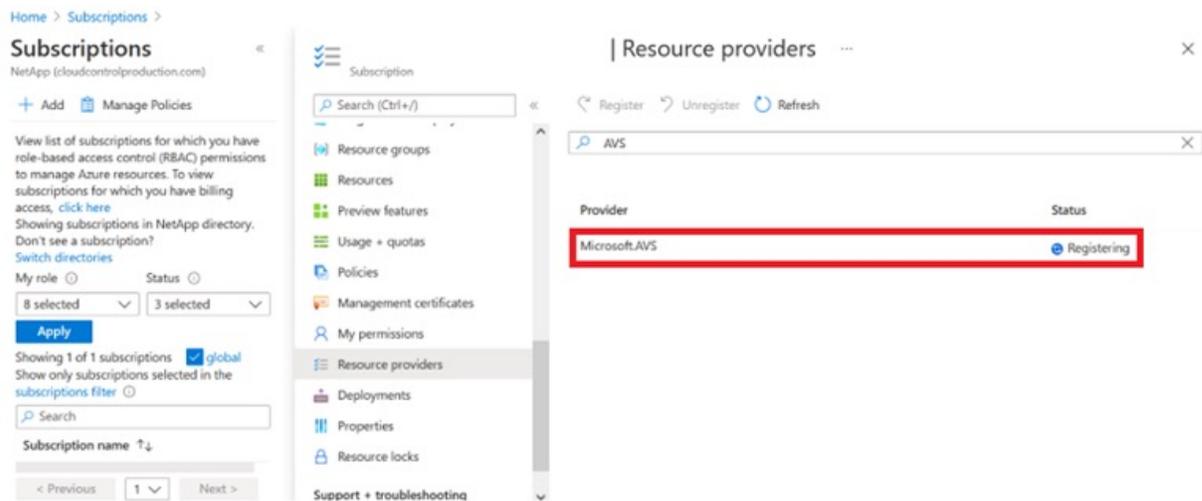
このセクションでは、Azure VMware 解決策をセットアップおよび管理する方法と、ネットアップストレージの接続に使用できるオプションについて説明します。

セットアッププロセスは、次の手順に分けることができます。

リソースプロバイダを登録し、プライベートクラウドを作成

Azure VMware 解決策を使用するには、まず、特定されたサブスクリプションにリソースプロバイダを登録します。

1. Azure ポータルにサインインします。
2. Azure ポータルのメニューで、すべてのサービスを選択します。
3. [すべてのサービス] ダイアログボックスで、サブスクリプションを入力し、[サブスクリプション] を選択します。
4. 表示するには、サブスクリプションリストからサブスクリプションを選択します。
5. [リソースプロバイダ] を選択し、検索結果に「Microsoft.AVS」と入力します。
6. リソースプロバイダが登録されていない場合は、[登録] を選択します。



Provider	Status
Microsoft.OperationsManagement	Registered
Microsoft.Compute	Registered
Microsoft.ContainerService	Registered
Microsoft.ManagedIdentity	Registered
Microsoft.AVS	Registered
Microsoft.OperationalInsights	Registered
Microsoft.GuestConfiguration	Registered

7. リソースプロバイダの登録が完了したら、Azure ポータルを使用して Azure VMware 解決策プライベートクラウドを作成します。
8. Azure ポータルにサインインします。
9. 新規リソースを作成を選択する。
10. [Search the Marketplace] テキストボックスに Azure VMware 解決策と入力し、検索結果から選択します。
11. Azure VMware 解決策ページで、Create を選択します。
12. [基本設定] タブのフィールドに値を入力し、[レビュー]、[作成] の順に選択します。

注：

- クイックスタートのために、計画フェーズで必要な情報を収集します。
- 既存のリソースグループを選択するか、プライベートクラウド用の新しいリソースグループを作成します。リソースグループは、Azure リソースを導入および管理する論理コンテナです。
- CIDR アドレスが一意で、他の Azure Virtual Network やオンプレミスネットワークと重複しないことを確認してください。CIDR はプライベートクラウド管理ネットワークであり、vCenter Server や NSX Manager などのクラスタ管理サービスに使用されます。ネットアップでは、/22 アドレススペースを使用することを推奨します。この例では、10.21.0.0/22 が使用されています。

Create a private cloud ...

Prerequisites * Basics Tags Review and Create

Project details

Subscription *

Resource group * [Create new](#)

Private cloud details

Resource name *

Location *

Size of host *

Number of hosts * [Find out how many hosts you need](#)

CIDR address block

Provide IP address for private cloud for cluster management. Make sure these are unique and do not overlap with any other Azure mets or on-premise networks.

Address block for private cloud *

[Review and Create](#) [Previous](#) [Next: Tags >](#)

プロビジョニングプロセスには約 4~5 時間かかります。プロセスが完了したら、Azure ポータルからプライベートクラウドにアクセスして、導入が成功したことを確認します。導入が完了すると、「成功しました」のステータスが表示されます。

Azure VMware 解決策プライベートクラウドには Azure Virtual Network が必要です。Azure VMware 解決策はオンプレミスの vCenter をサポートしていないため、既存のオンプレミス環境と統合するには追加の手順が必要です。ExpressRoute 回線および仮想ネットワークゲートウェイのセットアップも行う必要があります。クラスタのプロビジョニングが完了するのを待っている間に、新しい仮想ネットワークを作成するか、既存の仮想ネットワークを使用して Azure VMware 解決策に接続します。

[Home >](#)

 **nimoavpriv** [✕](#) [...](#)
AVS Private cloud

[Delete](#)

[Overview](#)

[Activity log](#)

[Access control \(IAM\)](#)

[Tags](#)

[Diagnose and solve problems](#)

Settings

[Locks](#)

Manage

[Connectivity](#)

[Identity](#)

[Clusters](#)

Essentials

Resource group [\(change\)](#)
NimoAVSDemo

Status
Succeeded

Location
East US 2

Subscription [\(change\)](#)
SaaS Backup Production

Subscription ID
b58a041a-e464-4497-8be9-9048369ee8e1

[Tags \(change\)](#)
[Click here to add tags](#)

Address block for private cloud
10.21.0.0/22

Primary peering subnet
10.21.0.232/30

Secondary peering subnet
10.21.0.236/30

Private Cloud Management network
10.21.0.0/26

vMotion network
10.21.1.128/25

Number of hosts
3

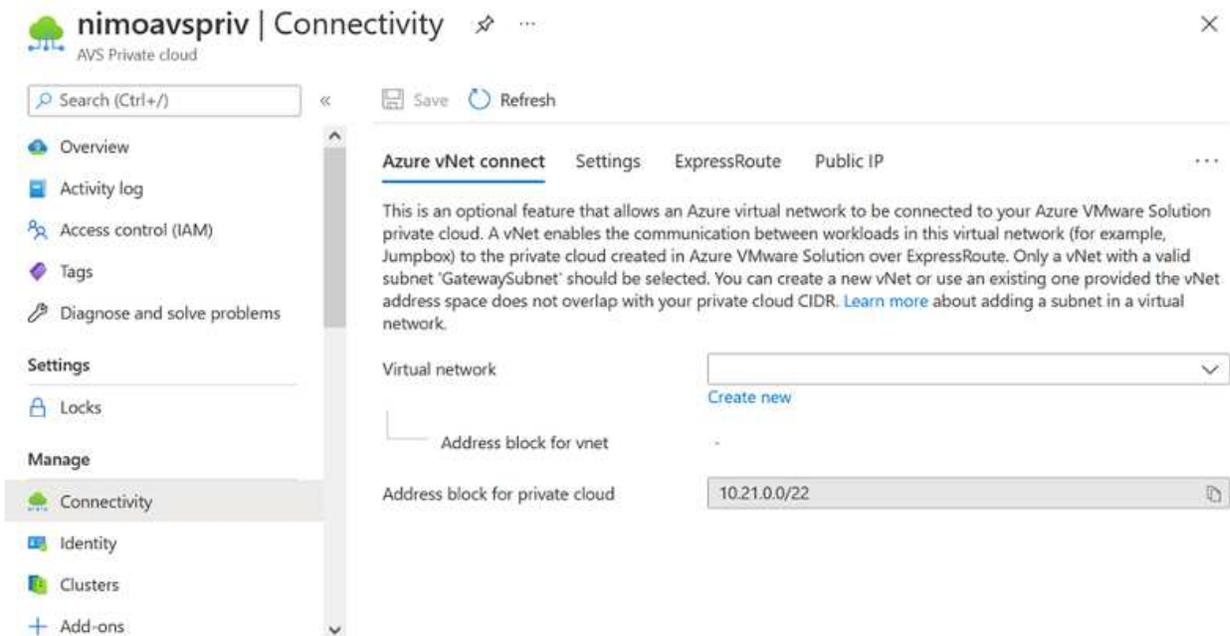
新しい **ExpressRoute** 仮想ネットワークゲートウェイまたは既存の **ExpressRoute** 仮想ネットワークゲートウェイに接続します

新しい Azure Virtual Network (VNet) を作成するには、Azure VNet Connect (Azure VNet 接続) タブを選択します。または、Create Virtual Network ウィザードを使用して、Azure ポータルから手動で作成することもできます。

1. Azure VMware 解決策プライベートクラウドに移動し、管理オプションで接続にアクセスします。
2. Azure VNet Connect を選択します。
3. 新しい VNet を作成するには、Create New オプションを選択します。

この機能により、VNet を Azure VMware 解決策プライベートクラウドに接続できます。VNet は、ExpressRoute 経由で Azure VMware 解決策で作成されたプライベートクラウドに必要なコンポーネント (ジャンプボックス、Azure NetApp Files などの共有サービス、クラウドボリューム ONTAP など) を自動的に作成することで、この仮想ネットワークのワークロード間の通信を有効にします。

◦ 注：* VNet アドレス空間はプライベートクラウド CIDR と重複しないようにしてください。



The screenshot shows the 'Connectivity' page in the Azure portal for an 'AVS Private cloud'. The page title is 'nimoavspriv | Connectivity'. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks), and Manage (Connectivity, Identity, Clusters, Add-ons). The main content area is titled 'Azure vNet connect' and includes a 'Settings' tab. Below the title, there is a descriptive paragraph: 'This is an optional feature that allows an Azure virtual network to be connected to your Azure VMware Solution private cloud. A vNet enables the communication between workloads in this virtual network (for example, Jumpbox) to the private cloud created in Azure VMware Solution over ExpressRoute. Only a vNet with a valid subnet 'GatewaySubnet' should be selected. You can create a new vNet or use an existing one provided the vNet address space does not overlap with your private cloud CIDR. Learn more about adding a subnet in a virtual network.' Below this text are three input fields: 'Virtual network' (a dropdown menu), 'Address block for vnet' (a text input field), and 'Address block for private cloud' (a text input field containing '10.21.0.0/22').

4. 新しい VNet の情報を入力または更新し、OK を選択します。

Create virtual network



This virtual network enables the communication between workloads in this virtual network (e.g. a JumpHost) to the private cloud created in Azure VMware Solution over an Express route. A default address range and a subnet is selected for this virtual network. For changing the default address range and subnet of this virtual network, follow these steps: Step 1: Change the "Address Range" to desired range (e.g. 172.16.0.0/16). Step 2: Add a subnet under "Subnets" with the name as "GatewaySubnet" and provide subnet's address range in CIDR notation (e.g. 172.16.1.0/24). [Learn more about virtual networks](#)

Name *

Address space

The virtual network's address space specified as one or more address prefixes in CIDR notation (e.g. 10.0.0.0/16).

<input type="checkbox"/> Address range	Addresses	Overlap
<input type="checkbox"/> 172.24.0.0/16	172.24.0.4 - 172.24.255.254 (65531 addresses)	None
<input type="text"/>	(0 Addresses)	None

Subnets

The subnet's address range in CIDR notation (e.g. 10.0.0.0/24). It must be contained by the address space of the virtual network.

<input type="checkbox"/> Subnet name	Address range	Addresses
<input type="checkbox"/> GatewaySubnet	172.24.0.0/24	172.24.0.4 - 172.24.0.254 (251 addresses)
<input type="text"/>	<input type="text"/>	(0 Addresses)

指定したアドレス範囲とゲートウェイサブネットを使用した VNet は、指定したサブスクリプションとリソースグループに作成されます。



VNet を手動で作成する場合は、適切な SKU と ExpressRoute をゲートウェイタイプとして使用して仮想ネットワークゲートウェイを作成します。導入が完了したら、認証キーを使用して、ExpressRoute 接続を、Azure VMware 解決策プライベートクラウドを含む仮想ネットワークゲートウェイに接続します。詳細については、[を参照してください "Azure で VMware プライベートクラウド用のネットワークを設定します"](#)。

ネットワーク接続を検証し、**Azure VMware** 解決策プライベートクラウドにアクセスします

Azure VMware 解決策では、オンプレミスの VMware vCenter でプライベートクラウドを管理することはできません。代わりに、ジャンプホストが Azure VMware 解決策 vCenter インスタンスに接続する必要があります。指定したリソースグループにジャンプホストを作成し、Azure VMware 解決策 vCenter にサインインします。このジャンプホストは、接続用に作成された同じ仮想ネットワーク上の Windows VM であり、vCenter と NSX Manager の両方にアクセスする必要があります。

Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Virtual machine name *

Region *

Availability options

Image * [See all images](#)

Azure Spot instance

Size * [See all sizes](#)

仮想マシンをプロビジョニングしたら、Connect オプションを使用して RDP にアクセスします。

nimAVSJH | Connect

Virtual machine

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Disks
- Size

⚠ To improve security, enable just-in-time access on this VM. →

RDP SSH BASTION

Connect with RDP

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.

IP address *

Public IP address (52.138.103.135)

Port number *

3389

Download RDP File

新しく作成したジャンプホスト仮想マシンから、クラウド管理者ユーザを使用して vCenter にサインインします。クレデンシャルにアクセスするには、Azure ポータルにアクセスし、（プライベートクラウド内の管理オプションで）Identity に移動します。プライベートクラウド vCenter と NSX Manager の URL とユーザー資格情報は、ここからコピーできます。

nimoavspriv | Identity

AWS Private cloud

Search (Ctrl+/)

- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Locks

Manage

- Connectivity
- Identity
- Clusters
- Placement policies (preview)
- Add-ons

Login credentials

vCenter credentials

Web client URL

https://10.21.0.2/

Admin username

cloudadmin@vsphere.local

Admin password

Certificate thumbprint

AE26B15A5CE38DC069D35F045F088CA6343475EC

NSX-T Manager credentials

Web client URL

https://10.21.0.3/

Admin username

admin

Admin password

Certificate thumbprint

B2B722EA683958283EE159007246D5166D0509D3

Windows 仮想マシンでブラウザを開き、vCenter Web Client の URL にアクセスします ("https://10.21.0.2/") にアクセスし、admin ユーザ名に「* cloudadmin@vsphere.local」と入力して、コピーしたパスワードを貼り付けます。同様に、Web クライアントの URL を使用して NSX Manager にアクセスすることもできます ("https://10.21.0.3/") をクリックし、admin ユーザ名を使用してコピーしたパスワードを貼り付け、新しいセグメントを作成するか、既存の階層ゲートウェイを変更します。



Web クライアントの URL は、プロビジョニングされる SDDC ごとに異なります。

The image shows two screenshots. The top screenshot is the VMware vSphere login page, displaying the VMware logo and a login form with fields for 'cloudadmin@vsphere.local' and a password. A 'LOGIN' button is at the bottom. The bottom screenshot is the vSphere Client interface, showing a summary of a vCenter instance with 0 Virtual Machines and 3 Hosts. It includes resource usage charts for CPU, Memory, and Storage, and a 'Recent Tasks' table at the bottom.

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Undeploy plug-in	vc.beeb9fd29...	Completed	VMware vRops Client Plugin	VSPHERE.LOCAL...	8 ms	08/12/2021, 11:38:11 AM	08/12/2021, 11:38:11 AM	vc.beeb9fd29eab...

これで、Azure VMware 解決策 SDDC の導入と設定が完了しました。ExpressRoute グローバルリーチを活用して、オンプレミス環境を Azure VMware 解決策プライベートクラウドに接続します。詳細については、を参照してください "[オンプレミス環境から Azure VMware 解決策へのピアリング](#)".

Google Cloud Platform (GCP) への仮想化環境の導入と構成

オンプレミスと同様に、VM と移行を作成する本番環境に成功するには、Google Cloud VMware Engine (GCVE) の計画が不可欠です。

このセクションでは、GCVE のセットアップと管理方法、およびネットアップストレージの接続に使用できるオプションとの組み合わせについて説明します。

セットアッププロセスは、次の手順に分けることができます。

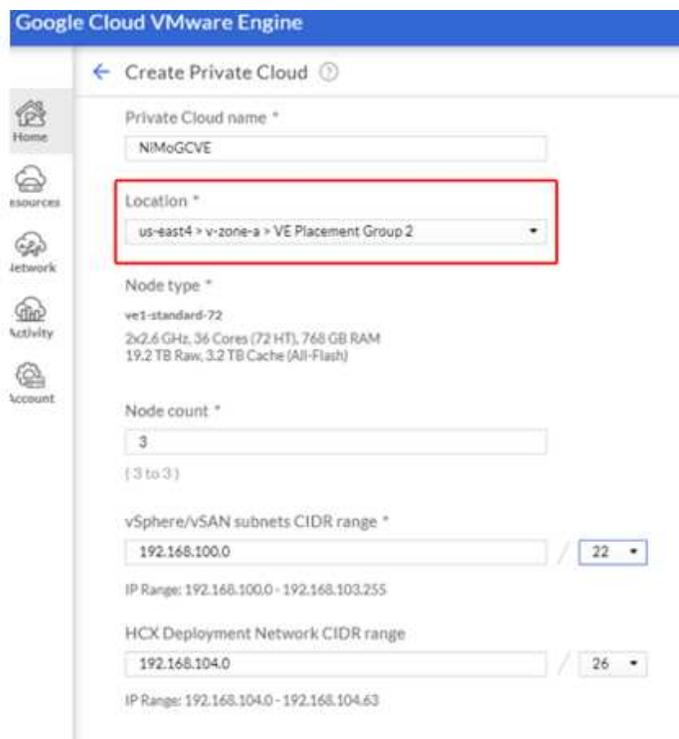
GCVE を導入して設定します

GCP で GCVE 環境を設定するには、GCP コンソールにログインし、VMware Engine ポータルにアクセスします。

[New Private Cloud] ボタンをクリックして、GCVE プライベートクラウドに必要な設定を入力します。「場所」で、CV/CVO を導入するリージョン/ゾーンにプライベートクラウドを導入して、最高のパフォーマンスと最小のレイテンシを確保してください。

前提条件

- VMware Engine Service Admin IAM ロールを設定します
- "VMware Engine API アクセスおよびノードクォータを有効にします"
- CIDR 範囲がオンプレミスサブネットやクラウドサブネットと重複しないようにしてください。CIDR 範囲は /27 以上である必要があります。



Google Cloud VMware Engine

← Create Private Cloud ⓘ

Private Cloud name *
NIMoGCVE

Location *
us-east4 > v-zone-a > VE Placement Group 2

Node type *
vet1-standard-72
2x2.6 GHz, 36 Cores (72 HT), 768 GB RAM
19.2 TB Raw, 3.2 TB Cache (All-Flash)

Node count *
3
(3 to 3)

vSphere/vSAN subnets CIDR range *
192.168.100.0 / 22
IP Range: 192.168.100.0 - 192.168.103.255

HCX Deployment Network CIDR range
192.168.104.0 / 26
IP Range: 192.168.104.0 - 192.168.104.63

注：プライベートクラウドの作成には、30分から2時間かかります。

GCVE へのプライベートアクセスを有効にします

プライベートクラウドのプロビジョニングが完了したら、プライベートクラウドへのプライベートアクセスを設定して、高スループットで低レイテンシのデータパス接続を実現します。

これにより、Cloud Volumes ONTAP インスタンスが実行されている VPC ネットワークが、GCVE プライベートクラウドと通信できるようになります。これを行うには、に従ってください "[GCP ドキュメント](#)"。クラウドボリュームサービスの場合は、テナントホストプロジェクト間で 1 回限りのピアリングを実行して、VMware エンジンと Cloud Volumes Service 間の接続を確立します。詳細な手順については、次の手順を実行してください "[リンク](#)"。

Tenant P...	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Sta...	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	Active	Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	Active	Connected

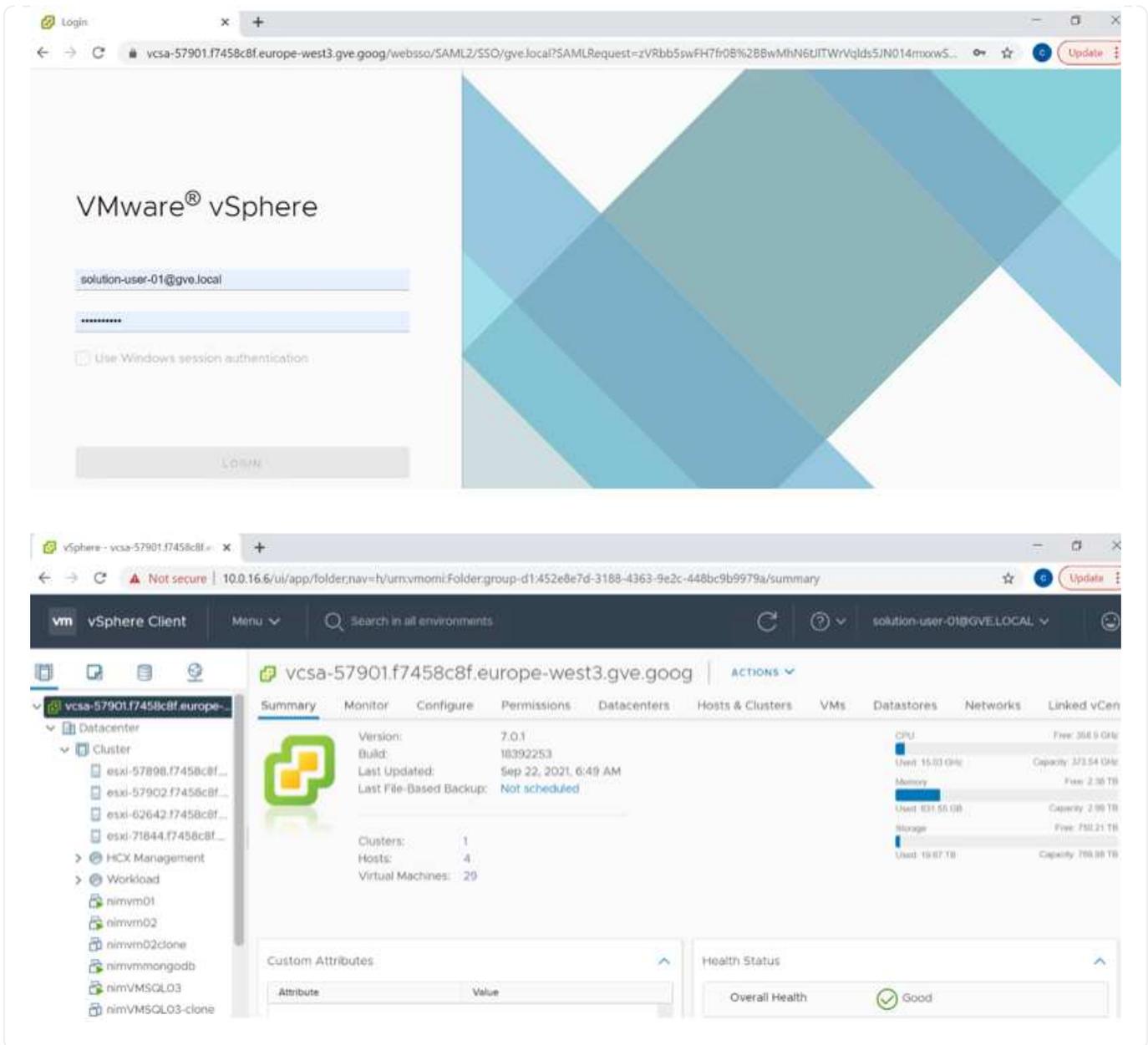
[CloudOwner@gve.loc](#) ユーザを使用して vCenter にサインインします。クレデンシャルにアクセスするには、VMware Engine ポータルにアクセスし、Resources にアクセスして、適切なプライベートクラウドを選択します。[Basic info] セクションで、vCenter ログイン情報（vCenter Server、HCX Manager）または NSX ログイン情報（NSX Manager）の [View] リンクをクリックします。

The screenshot shows the Google Cloud VMware Engine console interface. The main content area displays the 'Resources' page for a private cloud instance named 'gcve-cvs-hw-eu-west3'. The page is divided into several sections:

- Summary:** Shows the instance name, status (Operational), location (europe-west3 > v-zone-a > VE Placement Group 1), and Cloud Monitoring status.
- Basic Info:** Includes details about Clusters (1), vSphere/vSAN subnets CIDR range (10.0.16.0/24), vCenter login info, and NSX-T login info.
- Capacity:** Displays Total nodes (4), Total CPU capacity (144 cores), Total RAM (3072 GB), and Total storage capacity (76.8 TB Raw, 12.8 TB Cache, All-Flash).

Windows 仮想マシンでブラウザを開き、vCenter Web Client の URL にアクセスします ("https://10.0.16.6/") にアクセスし、adminユーザ名としてCloudOwner@gve.locを使用して、コピーしたパスワードを貼り付けます。同様に、Web クライアントの URL を使用して NSX Manager にアクセスすることもできます ("https://10.0.16.11/") をクリックし、adminユーザ名を使用してコピーしたパスワードを貼り付け、新しいセグメントを作成するか、既存の階層ゲートウェイを変更します。

オンプレミスネットワークから VMware Engine プライベートクラウドに接続する場合は、クラウド VPN または Cloud Interconnect を利用して適切な接続を行い、必要なポートが開いていることを確認します。詳細な手順については、次の手順を実行してください "[リンク](#)"。



NetApp Cloud Volume Serviceの補完的データストアをGCVEに導入

を参照してください "手順を使用して、NetApp CVSを使用した補完的NFSデータストアをGCVEに導入します"

ハイパースケーラクラウドにおけるネットアップストレージ

パブリッククラウドプロバイダ向けのネットアップストレージオプション

主要な 3 種類のハイパースケーラにおけるストレージとしてのネットアップのオプションをご確認ください。

AWS / VMC

AWS は、次の構成でネットアップストレージをサポートします。

- ゲスト接続ストレージとしての FSX ONTAP
- Cloud Volumes ONTAP (CVO) をゲスト接続ストレージとして活用
- 補足的なNFSデータストアとしてのFSX ONTAP

詳細を表示します ["VMCのゲスト接続ストレージオプション"](#)。詳細を表示します ["VMCの追加のNFSデータストアオプション"](#)。

Azure / AVS

Azure は、以下の構成でネットアップストレージをサポートします。

- ゲスト接続ストレージとしての Azure NetApp Files (ANF)
- Cloud Volumes ONTAP (CVO) をゲスト接続ストレージとして活用
- Azure NetApp Files (ANF) を追加のNFSデータストアとして使用できます

詳細を表示します ["AVSのゲスト接続ストレージオプション"](#)。詳細を表示します ["AVSの補足的なNFSデータストアオプション"](#)。

GCP/GCVE

Google Cloud は、次の構成でネットアップストレージをサポートします。

- Cloud Volumes ONTAP (CVO) をゲスト接続ストレージとして活用
- Cloud Volumes Service (CVS) をゲスト接続ストレージとして使用できるようになりました
- Cloud Volumes Service (CVS) をNFSデータストアとして追加

詳細を表示します ["GCVEのゲスト接続ストレージオプション"](#)。

詳細については、をご覧ください ["NetApp Cloud Volumes Service データストアでのGoogle Cloud VMware Engineのサポート \(ネットアップブログ\)"](#) または ["ネットアップCVSをGoogle Cloud VMware Engineのデータストアとして使用する方法 \(Googleブログ\)"](#)

TR-4938 : AWSにVMware CloudでNFSデータストアとしてAmazon FSX for ONTAPをマウント

本ドキュメントでは、VMware Cloud on AWSを使用してAmazon FSx for ONTAPをNFSデータストアとしてマウントする方法について説明します。

ネットアップ、 Niyaz Mohamed

はじめに

成功を収めている組織は、変革と刷新の道を歩んでいます。このプロセスの一環として、企業は通常、既存のVMwareへの投資を使用して、クラウドのメリットを活用し、プロセスの移行、バースト、拡張、ディザスタリカバリを可能なかぎりシームレスに実行する方法を模索しています。クラウドに移行するお客様は、柔軟

性とバースト性、データセンターの終了、データセンターの統合、ライフサイクルの終了、合併、合併などのユースケースを評価する必要があります。買収など。

VMware Cloud on AWSはお客様に独自のハイブリッド機能を提供するため、大多数のお客様に適していますが、ネイティブストレージの選択肢が限られているため、ストレージの負荷が高い組織での有用性が制限されています。ストレージはホストに直接関連付けられているため、ストレージを拡張する唯一の方法は、ホストを追加することです。これにより、ストレージを大量に消費するワークロードのコストを35~40%以上増加させることができます。このようなワークロードには、追加の処理能力ではなく、ストレージと分離されたパフォーマンスが必要ですが、追加のホストに料金を支払うことになります。ここでは、を行います ["最近の統合"](#) ONTAP 向けFSXは、VMware Cloud on AWSを使用して、大量のストレージとパフォーマンスを必要とするワークロードに最適です。

次のシナリオを考えてみましょう。お客様は8台のホストで馬力を求めています (vCPU / vMem) が必要ですが、ストレージにも大きな要件があります。評価に基づいて、ストレージ要件を満たすために16台のホストが必要です。これにより、必要な容量をすべて追加購入するだけで、より多くのストレージが必要になるため、全体的なTCOが増加します。これは、移行、ディザスタリカバリ、バースト、開発/テストなど、あらゆるユースケースに当てはまります。 など。

このドキュメントでは、AWS上のVMware Cloud用のNFSデータストアとしてONTAP 用のFSXをプロビジョニングして接続するために必要な手順を説明します。



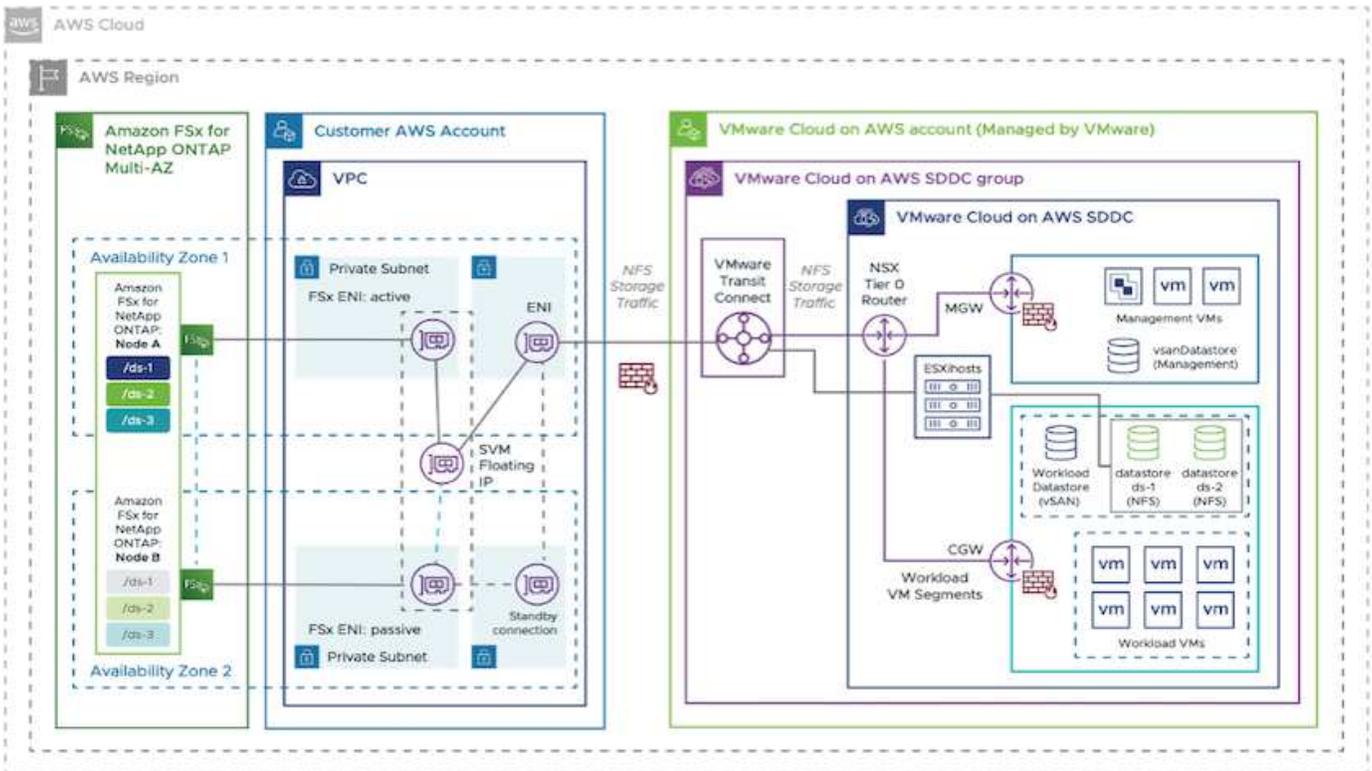
この解決策 は、VMwareからも入手できます。にアクセスしてください ["VMware Cloud Tech Zone"](#) を参照してください。

接続オプション



AWS上のVMware Cloudでは、複数AZおよび単一AZ環境のFSX for ONTAP をサポートしません。

ここでは、ハイレベルな接続アーキテクチャと、ホストを追加することなくSDDCクラスタ内のストレージを拡張するために解決策 を実装するために必要な手順について説明します。



導入手順の概要は次のとおりです。

1. 新しい指定VPCでAmazon FSX for ONTAP を作成します。
2. SDDCグループを作成します。
3. VMware Transit ConnectとTGWの添付ファイルを作成します。
4. ルーティング（AWS VPCとSDDC）とセキュリティグループを設定する。
5. NFSボリュームをデータストアとしてSDDCクラスタに接続します。

ONTAP 用のFSXをNFSデータストアとしてプロビジョニングして接続する前に、まずCloud SDDC環境でVMwareをセットアップするか、またはv1.20以上にアップグレードした既存のSDDCを取得する必要があります。詳細については、を参照してください ["AWSでのVMware Cloudの導入"](#)。



ONTAP のFSXは、現在、ストレッチクラスタではサポートされていません。

まとめ

このドキュメントでは、AWSでVMwareクラウドを使用してAmazon FSX for ONTAP を設定するために必要な手順について説明します。Amazon FSX for ONTAP は、アプリケーションワークロードとファイルサービスを導入および管理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とシームレスにすることでTCOを削減します。どのようONTAP なユースケースでも、オンプレミスからAWSにクラウドのメリット、一貫したインフラ、運用を迅速に実現するためには、AWS対応のVMwareクラウドとAmazon FSXを選択し、ワークロードの双方向の移動性、エンタープライズクラスの容量とパフォーマンスを実現できます。ストレージの接続に使用する一般的なプロセスと手順は同じです。新しい名前と同様に変更されたデータの位置にすぎないことを忘れないでください。ツールとプロセスはすべて変わらないので、Amazon FSX for ONTAP を使用すると、全体的な導入を最適化できます。

このプロセスの詳細については、詳細なウォークスルービデオをご覧ください。

AWS 用のネットアップゲスト接続ストレージオプション

AWSでは、ゲスト接続のネットアップストレージをネイティブのFSXサービス（FSX ONTAP）またはCloud Volumes ONTAP（CVO）でサポートしています。

FSX ONTAP の略

Amazon FSX for NetApp ONTAP はフルマネージドサービスで、ネットアップの広く普及したONTAP ファイルシステムを基盤に、信頼性、拡張性、パフォーマンス、機能豊富なファイルストレージを提供します。FSX for ONTAP は、ネットアップファイルシステムの使い慣れた機能、パフォーマンス、機能、API操作に、AWS のフルマネージドサービスならではの即応性、拡張性、シンプルさを兼ね備えています。

FSX for ONTAP は、機能豊富で高速で柔軟性に優れた共有ファイルストレージを提供します。このストレージは、AWSまたはオンプレミスで動作するLinux、Windows、macOSコンピューティングインスタンスから幅広くアクセスできます。FSX for ONTAP は、1ミリ秒未満のレイテンシでハイパフォーマンスのソリッドステートドライブ（SSD）ストレージを提供します。FSX for ONTAP を使用すると、SSDストレージに支払うデータの量がごくわずかであるのに、ワークロードでSSDレベルのパフォーマンスを実現できます。

ボタンをクリックするだけでファイルのスナップショット作成、複製、複製ができるため、FSX for ONTAP でのデータ管理が簡単になります。さらに、FSX for ONTAP は、データを低コストで柔軟なストレージに自動的に階層化し、容量のプロビジョニングや管理の必要性を軽減します。

また、FSX for ONTAP は、フルマネージドのバックアップとクロスリージョンディザスタリカバリのサポートにより、可用性と耐久性に優れたストレージを提供します。データの保護とセキュリティを容易にするため、ONTAP 対応FSXは、一般的な データ セキュリティ アプリケーションとウイルス対策アプリケーションをサポートしています。

ゲスト接続ストレージとしての FSX ONTAP

AWS で VMware Cloud を使用して、NetApp ONTAP 用に Amazon FSX を設定します

Amazon FSX for NetApp ONTAP ファイル共有および LUN は、AWS の VMware Cloud にある VMware SDDC 環境内で作成された VM からマウントできます。また、このボリュームは、Linux クライアントにマウントして NFS または SMB プロトコルを使用して Windows クライアントにマッピングすることもできます。また、iSCSI 経由でマウントした場合、Linux クライアントまたは Windows クライアントから LUN にブロックデバイスとしてアクセスできます。NetApp ONTAP ファイルシステム用の Amazon FSX は、次の手順ですばやく設定できます。

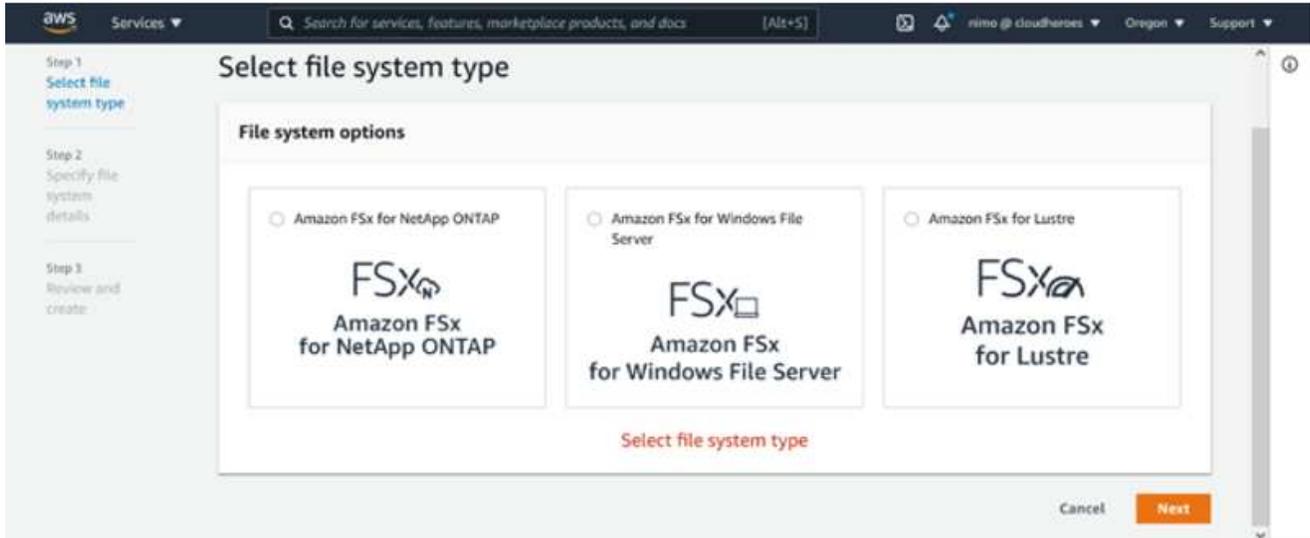


パフォーマンスを向上させ、アベイラビリティゾーン間でのデータ転送料金を回避するには、NetApp ONTAP 向け Amazon FSX と AWS 上の VMware Cloud を同じアベイラビリティゾーンに配置する必要があります。

ONTAP ボリューム用に Amazon FSX を作成してマウントします

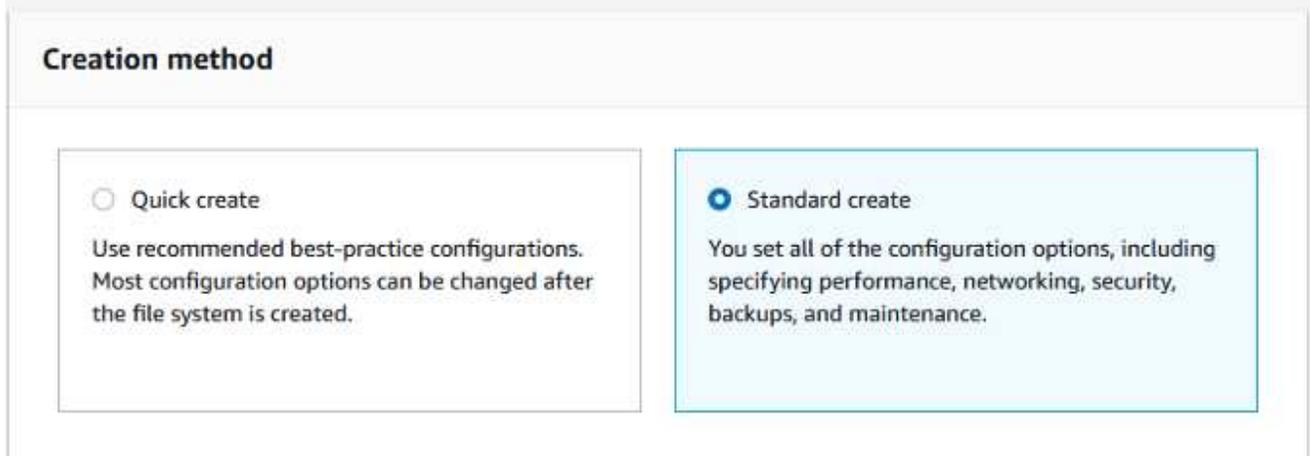
NetApp ONTAP ファイルシステム用に Amazon FSX を作成してマウントするには、次の手順を実行します。

1. を開きます **"Amazon FSX コンソール"** ファイルシステムの作成を選択して 'ファイルシステム作成ウィザードを開始します
2. [Select File System Type] ページで、 [Amazon FSX for NetApp ONTAP] を選択し、 [Next] をクリックします。Create File System ページが表示されます。



1. Virtual Private Cloud (VPC ; 仮想プライベートクラウド) のネットワークセクションで、ルーティングテーブルとともに適切な VPC と優先サブネットを選択します。この場合、ドロップダウンから vmcfsx2.vpc が選択されます。

Create file system



1. 作成方法として、標準作成を選択します。 [クイック作成] を選択することもできますが、このドキュメントでは [標準作成] オプションを使用します。

File system details

File system name - optional [Info](#)

vmcfsxval2

Maximum of 256 Unicode letters, whitespace, and numbers, plus + - = _ : /

SSD storage capacity [Info](#)

1024

Minimum 1024 GB; Maximum 192 TB.

Provisioned SSD IOPS

Amazon FSx provides 3 IOPS per GB of storage capacity. You can also provision additional SSD IOPS as needed.

Automatic (3 IOPS per GB of SSD storage)

User-provisioned

Throughput capacity [Info](#)

The sustained speed at which the file server hosting your file system can serve data. The file server can also burst to higher speeds for periods of time.

512 MB/s (Recommended)

1. Virtual Private Cloud (VPC ; 仮想プライベートクラウド) のネットワークセクションで、ルーティングテーブルとともに適切な VPC と優先サブネットを選択します。この場合、ドロップダウンから vmcfsx2.vpc が選択されます。

Network & security

Virtual Private Cloud (VPC) [Info](#)

Specify the VPC from which your file system is accessible.

vmcfsx2.vpc | vpc-0d1c764bcc495e805

VPC Security Groups [Info](#)

Specify VPC Security Groups to associate with your file system's network interface.

Choose VPC security group(s)

sg-018896ea218164ccb (default) X

Preferred subnet [Info](#)

Specify the preferred subnet for your file system.

subnet02.sn | subnet-013675849a5b99b3c (us-west-2b)

Standby subnet

subnet01.sn | subnet-0ef956cebf539f970 (us-west-2a)

VPC route tables

Specify the VPC route tables associated with your file system.

VPC's default route table

Select one or more VPC route tables

Endpoint IP address range

Specify the IP address range in which the endpoints to access your file system will be created.

No preference

Select an IP address range



Virtual Private Cloud (VPC ; 仮想プライベートクラウド) のネットワークセクションで、ルーティングテーブルとともに適切な VPC と優先サブネットを選択します。この場合、ドロップダウンから vmcfsx2.vPC が選択されます。

1. 「セキュリティと暗号化」セクションの「暗号化キー」で、ファイルシステムの保存データを保護する AWS Key Management Service (AWS KMS) 暗号化キーを選択します。File System Administrative Password に、 fsxadmin ユーザのセキュアなパスワードを入力します。

Security & encryption

Encryption key [Info](#)

AWS Key Management Service (KMS) encryption key that protects your file system data at rest.

aws/fsx (default) ▼

Description	Account	KMS key ID
Default master key that protects my FSx resources when no other key is defined	139763910815	72745367-7bb0-499c-acc0-4f2c0a80e7c5

File system administrative password

Password for this file system's "fsxadmin" user, which you can use to access the ONTAP CLI or REST API.

Don't specify a password

Specify a password

Password

••••••••

Confirm password

••••••••

1. 仮想マシンで、vsadmin で REST API または CLI を使用して ONTAP を管理するために使用するパスワードを指定します。パスワードを指定しない場合は、SVM の管理に fsxadmin ユーザを使用できません。Active Directory セクションで、SMB 共有をプロビジョニングするために Active Directory を SVM に追加してください。Default Storage Virtual Machine Configuration セクションで、この検証でストレージの名前を指定します。SMB 共有は自己管理 Active Directory ドメインを使用してプロビジョニングされます。

Default storage virtual machine configuration

Storage virtual machine name

SVM administrative password

Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.

- Don't specify a password
 Specify a password

Password

Confirm password

Active Directory

Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.

- Do not join an Active Directory
 Join an Active Directory

1. Default Volume Configuration セクションで、ボリュームの名前とサイズを指定します。これは NFS ボリュームです。Storage Efficiency の場合、ONTAP の Storage Efficiency 機能（圧縮、重複排除、コンパクション）をオンにするには Enabled を、オフにするには Disabled を選択します。

Default volume configuration

Volume name

Maximum of 203 alphanumeric characters, plus _ , -

Junction path

The location within your file system where your volume will be mounted.

Volume size

Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

- Enabled (recommended)
 Disabled

Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

1. Create File System ページに表示されるファイルシステム設定を確認します。
2. ファイルシステムの作成をクリックします。

The screenshot shows the AWS Management Console interface for Amazon FSx. The top navigation bar includes the AWS logo, 'Services', a search bar, and user information. The left sidebar shows the 'Amazon FSx' navigation menu with options like 'File systems', 'Backups', 'ONTAP', 'Storage virtual machines', 'Volumes', 'Windows File Server', and 'Lustre'. The main content area is divided into two sections: 'File systems (3)' and 'Storage virtual machines (SVMs) (2)'. The 'File systems' section contains a table with columns for File system name, File system ID, File system type, Status, Deployment type, and Storage type. The 'Storage virtual machines' section contains a table with columns for SVM name, SVM ID, Status, Creation time, and Active Directory. The 'fsxmbtesting01' SVM is selected, and its details are shown in the 'Summary' section, including SVM ID, SVM name, UUID, File system ID, Creation time, Lifecycle state, Subtype, Active Directory, Net BIOS name, Fully qualified domain name, Service account username, and Organizational unit distinguished name.

File system name	File system ID	File system type	Status	Deployment type	Storage type	St ca
fsxntapcifs	fs-014c28399be9c1f9f	ONTAP	Available	Multi-AZ	SSD	1,4
vmcfsxval2	fs-040eacc5d0ac31017	ONTAP	Available	Multi-AZ	SSD	1,4
fsxntapsql	fs-0ab4b447ebd6082aa	ONTAP	Available	Multi-AZ	SSD	2,4

SVM name	SVM ID	Status	Creation time	Active Directory
fsxmbtesting01	svm-075dcfbe2cfa2ece9	Created	2021-10-19 15:17:08 UTC +01:00	FSXTESTING.LOCAL
vmcfsxval2svm	svm-095db076341561212	Created	2021-10-15 15:16:54 UTC +01:00	-

fsxmbtesting01 (svm-075dcfbe2cfa2ece9) [Delete] [Update]

Summary

SVM ID	Creation time	Active Directory
svm-075dcfbe2cfa2ece9	2021-10-19T15:17:08+01:00	FSXTESTING.LOCAL
SVM name	Lifecycle state	Net BIOS name
fsxmbtesting01	Created	FSXSMBTESTING01
UUID	Subtype	Fully qualified domain name
4a50e659-30e7-11ec-ac4f-f3ad92a6a735	DEFAULT	FSXTESTING.LOCAL
File system ID		Service account username
fs-040eacc5d0ac31017		administrator
		Organizational unit distinguished name
		CN=Computers

詳細については、を参照してください ["Amazon FSx for NetApp ONTAP の利用を開始する"](#)。

上記のようにファイルシステムを作成したら、必要なサイズとプロトコルでボリュームを作成します。

1. を開きます "Amazon FSX コンソール"。
2. 左側のナビゲーションペインで、[ファイルシステム] を選択し、ボリュームを作成する ONTAP ファイルシステムを選択します。
3. Volumes (ボリューム) タブを選択します。
4. Create Volume (ボリュームの作成) タブを選択します。
5. Create Volume (ボリュームの作成) ダイアログボックスが表示されます。

デモ用として、このセクションで NFS ボリュームを作成します。このボリュームは、AWS 上の VMware クラウドで実行されている VM に簡単にマウントできます。nfsdemovol01 は次のように作成されます。



Create volume [X]

File system
fs-040eacc5d0ac31017 | vmcfsxval2

Storage virtual machine
svm-095db076341561212 | vmcfsxval2svm

Volume name
nfsdemovol01
Maximum of 205 alphanumeric characters, plus _.

Junction path
/nfsdemovol01
The location within your file system where your volume will be mounted.

Volume size
1024
Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency
Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.
 Enabled (recommended)
 Disabled

Capacity pool tiering policy
You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.
Auto

Cancel **Confirm**

FSX ONTAP ボリュームを Linux クライアントにマウントします

前の手順で作成した FSX ONTAP ボリュームをマウントします。AWS SDDC 上の VMC 内の Linux VM から、次の手順を実行します。

1. 指定された Linux インスタンスに接続します。
2. Secure Shell (SSH) を使用してインスタンスの端末を開き、適切なクレデンシャルを使用してログインします。
3. 次のコマンドを使用して、ボリュームのマウントポイント用のディレクトリを作成します。

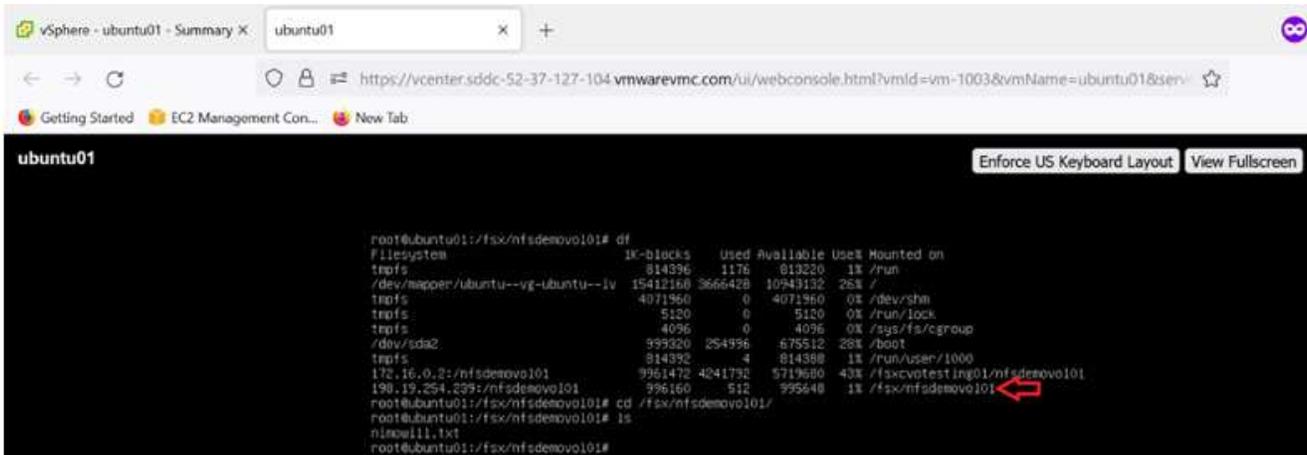
```
$ sudo mkdir /fsx/nfsdemov0101
```

・ 前の手順で作成したディレクトリに、 NetApp ONTAP NFS ボリュームの Amazon FSX をマウントします。

```
sudo mount -t nfs nfsvers=4.1,198.19.254.239:/nfsdemov0101 /fsx/nfsdemov0101
```

```
root@ubuntu01:/fsx/nfsdemov0101# mount -t nfs 198.19.254.239:/nfsdemov0101 /fsx/nfsdemov0101
```

1. 実行したら、df コマンドを実行してマウントを検証します。



```
root@ubuntu01:/fsx/nfsdemov0101# df
Filesystem            1K-blocks    Used Available Use% Mounted on
tmpfs                  814396      1176    813220   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv 19412168 3666428 10943132 26% /
tmpfs                  4071960     0    4071960   0% /dev/shm
tmpfs                   5120        0     5120    0% /run/lock
tmpfs                   4096        0     4096    0% /sys/fs/cgroup
/dev/sda2              999320 254996 675512 28% /boot
tmpfs                  814392        4    814388   1% /run/user/1000
172.16.0.2:/nfsdemov0101 9961472 4241792 5719680 43% /fsxcvtestling01/nfsdemov0101
198.19.254.239:/nfsdemov0101 996160    512    995648   1% /fsx/nfsdemov0101
root@ubuntu01:/fsx/nfsdemov0101# cd /fsx/nfsdemov0101/
root@ubuntu01:/fsx/nfsdemov0101# ls
nfsxwill.txt
root@ubuntu01:/fsx/nfsdemov0101#
```

FSX ONTAP ボリュームを Linux クライアントにマウントします

FSX ONTAP ボリュームを Microsoft Windows クライアントに接続します

Amazon FSX ファイルシステム上のファイル共有を管理およびマッピングするには、共有フォルダ GUI を使用する必要があります。

1. [スタート]メニューを開き、[管理者として実行]を使用して fsmgmt.msc を実行します。これにより、共有フォルダ GUI ツールが開きます。
2. アクション > すべてのタスクをクリックし、別のコンピュータに接続を選択します。
3. 別のコンピュータの場合は、Storage Virtual Machine (SVM) の DNS 名を入力します。たとえば、FSXSMBTESTING01.FSXTESTING.LOCAL はこの例で使用されています。



TP が Amazon FSX コンソールで SVM の DNS 名を検索し、Storage Virtual Machines を選択してから、endpoints までスクロールして SMB DNS 名を検索します。[OK] をクリックします。共有フォルダのリストに Amazon FSX ファイルシステムが表示されます。

Endpoints

Management DNS name

svm-075dcfbe2cfa2ece9.fs-040eacc5d0ac31017.fsx.us-west-2.amazonaws.com

NFS DNS name

svm-075dcfbe2cfa2ece9.fs-040eacc5d0ac31017.fsx.us-west-2.amazonaws.com

SMB DNS name

FSXSMBTESTING01.FSXTESTING.LOCAL

iSCSI DNS name

iscsi.svm-075dcfbe2cfa2ece9.fs-040eacc5d0ac31017.fsx.us-west-2.amazonaws.com

Management IP address

198.19.254.9

NFS IP address

198.19.254.9

SMB IP address

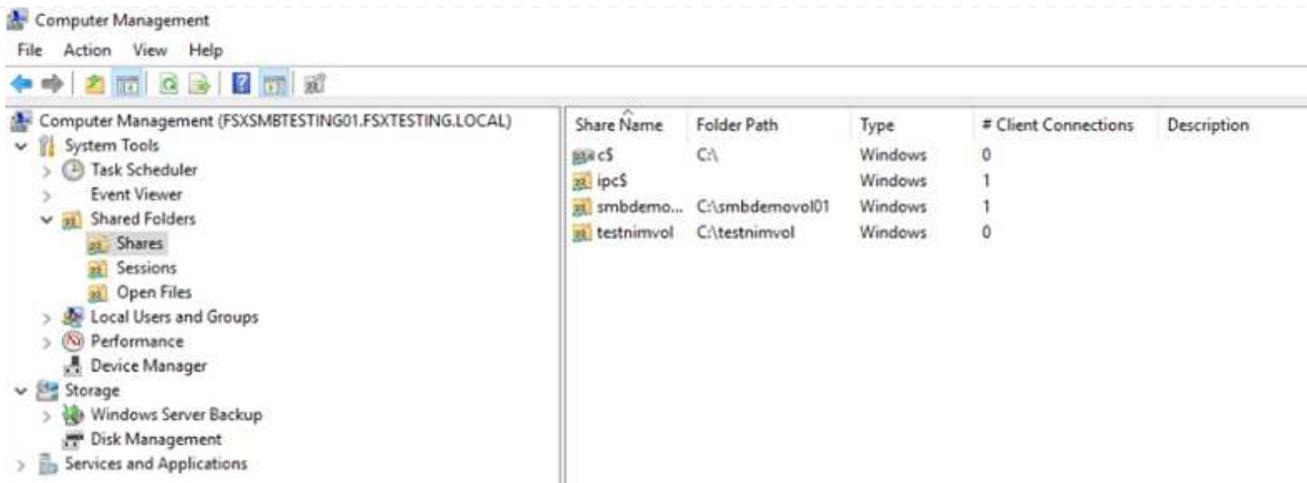
198.19.254.9

iSCSI IP addresses

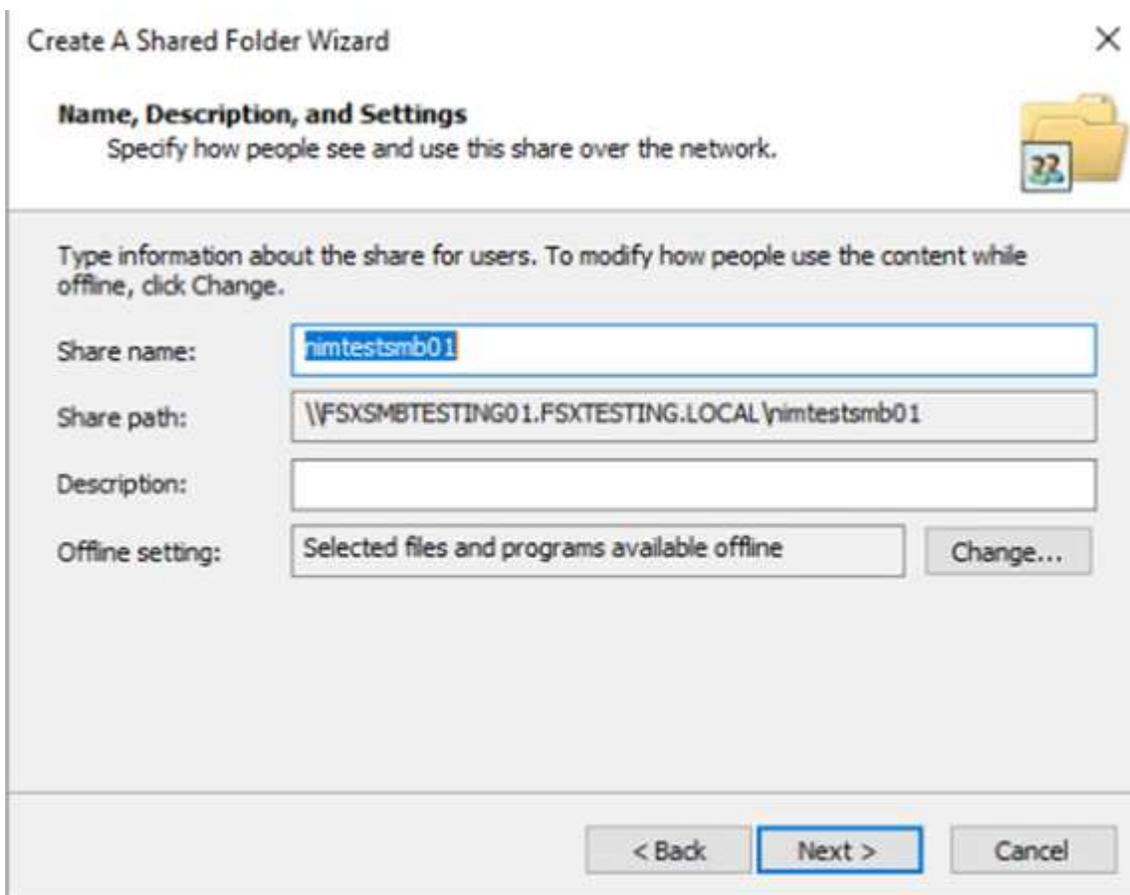
10.222.2.224, 10.222.1.94



1. 共有フォルダツールの左ペインで [共有] を選択すると、Amazon FSX ファイルシステムのアクティブな共有が表示されます。



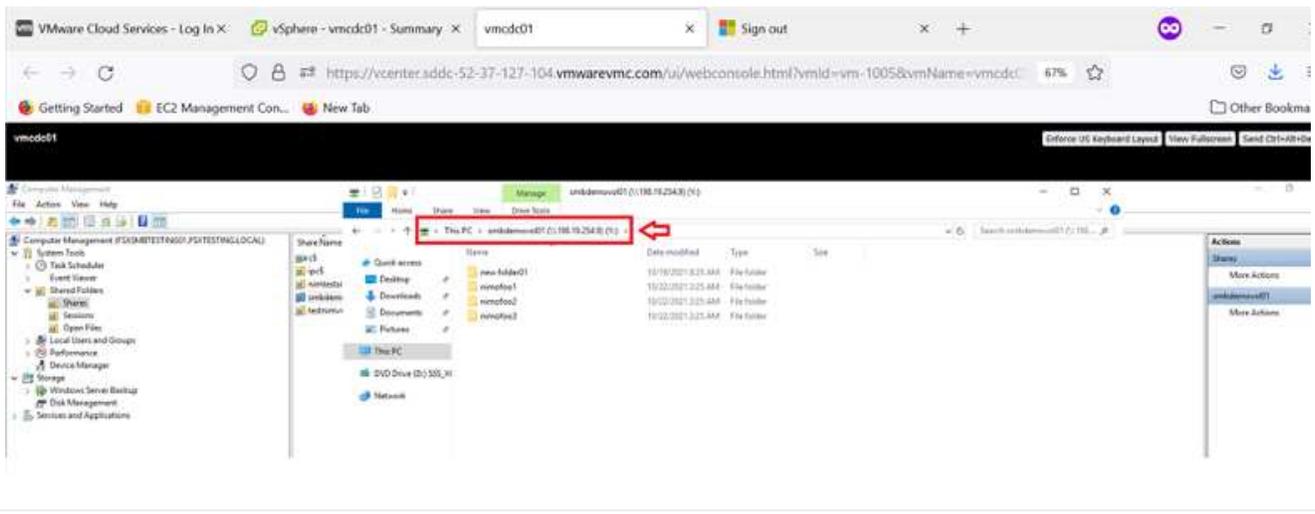
1. 新しい共有を選択し、共有フォルダの作成ウィザードを完了します。





Amazon FSX ファイルシステムでの SMB 共有の作成と管理の詳細については、[を参照してください](#) "SMB 共有の作成".

1. 接続が確立されると、SMB 共有を接続してアプリケーションデータに使用できるようになります。これを行うには、共有パスをコピーし、Map Network Drive オプションを使用して、AWS SDDC 上の VMware Cloud で実行されている VM にボリュームをマウントします。



iSCSI を使用して、NetApp ONTAP LUN の FSX をホストに接続します

iSCSI を使用して、NetApp ONTAP LUN の FSX をホストに接続します

FSX の iSCSI トラフィックは、前のセクションで説明したルートを通じて、VMware Transit Connect/AWS Transit Gateway を経由します。NetApp ONTAP 用に Amazon FSX 内の LUN を設定するには、該当するマニュアルを参照してください ["こちらをご覧ください"](#)。

Linux クライアントでは、iSCSI デーモンが実行されていることを確認します。LUN のプロビジョニングが完了したら、（例として）Ubuntu を使用した iSCSI 構成に関する詳細なガイダンスを参照してください。 ["こちらをご覧ください"](#)。

このドキュメントでは、iSCSI LUN を Windows ホストに接続する方法を示します。

NetApp ONTAP の FSX で LUN をプロビジョニングします。

1. ONTAP ファイルシステムの FSX の管理ポートを使用して、NetApp ONTAP CLI にアクセスします。
2. サイジング結果から得られるように、必要なサイズの LUN を作成します。

```
FsxId040eacc5d0ac31017::> lun create -vserver vmcfsxval2svm -volume
nimfsxscsivol -lun nimofsx1un01 -size 5gb -ostype windows -space
-reserve enabled
```

この例では、5g（5368709120）の LUN を作成しました。

1. 必要な igroup を作成して、どのホストが特定の LUN にアクセスできるかを制御します。

```
FsxId040eacc5d0ac31017::> igroup create -vserver vmcfsxval2svm -igroup
winIG -protocol iscsi -ostype windows -initiator iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local
```

```
FsxId040eacc5d0ac31017::> igroup show
```

```
Vserver    Igroup      Protocol OS Type  Initiators
-----
-----
```

```
vmcfsxval2svm
```

```
          ubuntu01      iscsi   linux   iqn.2021-
10.com.ubuntu:01:initiator01
```

```
vmcfsxval2svm
```

```
          winIG        iscsi   windows iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local
```

2つのエントリが表示されました。

1. 次のコマンドを使用して、LUN を igroup にマッピングします。

```
FsxId040eacc5d0ac31017::> lun map -vserver vmcfsxval2svm -path
/vol/nimfsxscsivol/nimofsxln01 -igroup winIG

FsxId040eacc5d0ac31017::> lun show
```

Vserver	Path	State	Mapped	Type
Size				

vmcfsxval2svm				
	/vol/blocktest01/lun01	online	mapped	linux
5GB				
vmcfsxval2svm				
	/vol/nimfsxscsivol/nimofsxln01	online	mapped	windows
5GB				

2つのエントリが表示されました。

1. 新しくプロビジョニングした LUN を Windows VM に接続します。

AWS SDDC 上の VMware クラウド上にある Windows ホストに新しい LUN の接続を行うには、次の手順を実行します。

1. AWS SDDC 上の VMware Cloud でホストされる Windows VM への RDP
2. サーバーマネージャ > ダッシュボード > ツール > iSCSI イニシエータと進み、iSCSI イニシエータのプロパティダイアログボックスを開きます。
3. Discovery (検出) タブで、Discover Portal (ポータルを検出) または Add Portal (ポータルの追加) をクリックし、iSCSI ターゲットポートの IP アドレスを入力します。
4. ターゲットタブで検出されたターゲットを選択し、ログオンまたは接続をクリックします。
5. [マルチパスを有効にする] を選択し、[コンピュータの起動時にこの接続を自動的に復元する] または [この接続をお気に入りターゲットのリストに追加する] を選択します。Advanced (詳細設定) をクリック



Windows ホストには、クラスタ内の各ノードへの iSCSI 接続が必要です。ネイティブ DSM では、使用する最適なパスが選択されます。

Quick Connect

To discover and log on to a target using a basic connection, type DNS name of the target and then click Quick Connect.

Target:

Discovered targets

Name	Status
iqn.1992-08.com.netapp:sn.264ef832dd911eca961d5f...	Con

To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

Quick Connect

Targets that are available for connection at the IP address or DNS name that you provided are listed below. If multiple targets are available, you need to connect to each target individually.

Connections made here will be added to the list of Favorite Targets and an attempt to restore them will be made every time this computer restarts.

Discovered targets

Name	Status
iqn.1992-08.com.netapp:sn.f0c909af2dc611ecac4f...	Connected

Progress report

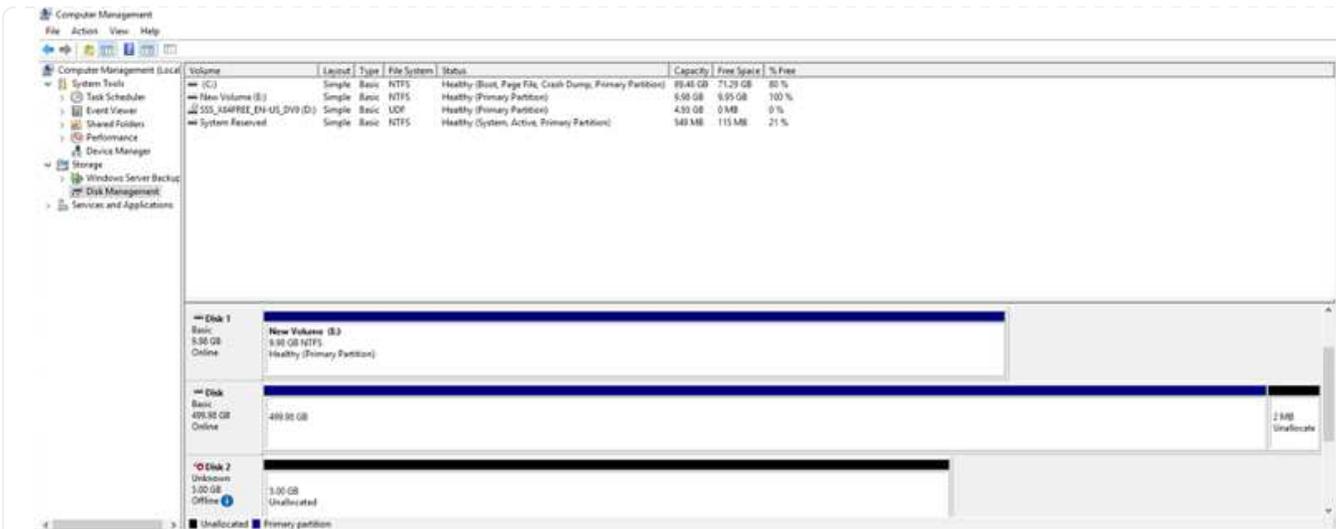
Login Succeeded.

Connect

Done

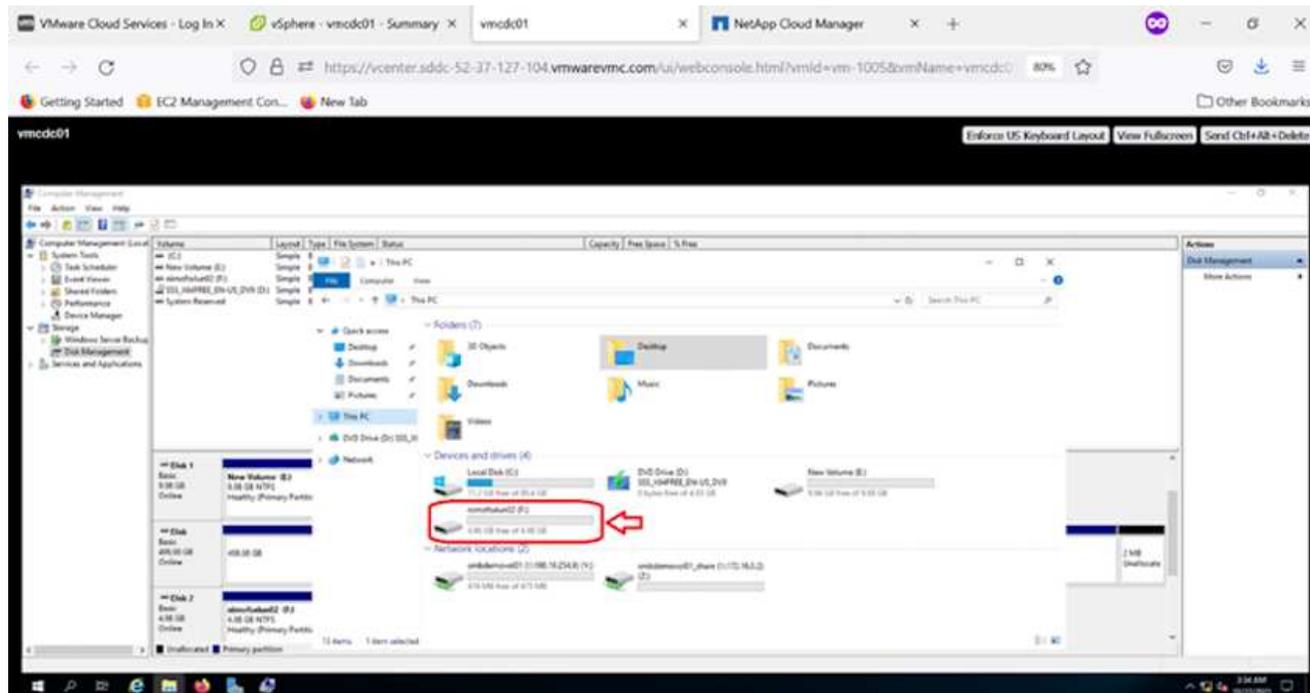
Storage Virtual Machine (SVM) の LUN は、Windows ホストではディスクとして表示されます。追加した新しいディスクは、ホストでは自動的に検出されません。手動の再スキャンをトリガーしてディスクを検出するには、次の手順を実行します。

1. Windows コンピュータの管理ユーティリティを開きます。[スタート]>[管理ツール]>[コンピュータの管理]を選択します。
2. ナビゲーションツリーでストレージノードを展開します。
3. [ディスクの管理]をクリックします
4. [アクション] > [ディスクの再スキャン] の順にクリック



Windows ホストから初めてアクセスした時点では、新しい LUN にはパーティションやファイルシステムは設定されていません。LUN を初期化し、必要に応じて、次の手順を実行してファイルシステムで LUN をフォーマットします。

1. Windows ディスク管理を開始します。
2. LUN を右クリックし、必要なディスクまたはパーティションのタイプを選択します。
3. ウィザードの指示に従います。この例では、ドライブ F : がマウントされています。



Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP (CVO) は、ネットアップのONTAP ストレージソフトウェアを基盤に構築された、業界をリードするクラウドデータ管理解決策です。Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP) でネイティブに利用できます。

ソフトウェアで定義されるONTAPバージョンで、クラウドネイティブなストレージを消費し、クラウドとオンプレミスで同じストレージソフトウェアを使用できるため、まったく新しい方法でIT担当者のデータ管理を再トレーニングする必要がありません。

CVOを使用すれば、エッジ、データセンター、クラウド間でシームレスにデータを移動し、ハイブリッドクラウドを統合できます。すべてを1画面の管理コンソールであるNetApp Cloud Managerで管理できます。

設計上、CVOは卓越したパフォーマンスと高度なデータ管理機能を備えており、クラウドで最も要件の厳しいアプリケーションにも対応できます

Cloud Volumes ONTAP (CVO) をゲスト接続ストレージとして活用

AWS に新しい Cloud Volumes ONTAP インスタンスを導入（自分で実行）

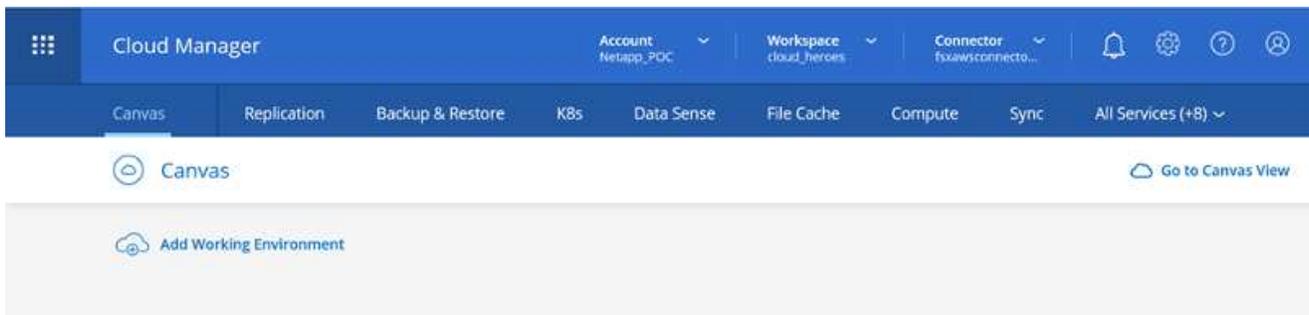
Cloud Volumes ONTAP 共有および LUN は、AWS SDDC 環境の VMware クラウドで作成された VM からマウントできます。Cloud Volumes ONTAP では iSCSI、SMB、NFS の各プロトコルがサポートされているため、このボリュームをネイティブの AWS VM Linux Windows クライアントにマウントすることもでき、iSCSI 経由でマウントする場合は、Linux クライアントまたは Windows クライアントからブロックデバイスとして LUN にアクセスできます。Cloud Volumes ONTAP ボリュームは、いくつかの簡単な手順で設定できます。

ディザスタリカバリや移行の目的でオンプレミス環境からクラウドにボリュームをレプリケートするには、サイト間 VPN または DirectConnect を使用して、AWS へのネットワーク接続を確立します。オンプレミスから Cloud Volumes ONTAP へのデータのレプリケートについては、本ドキュメントでは扱いません。オンプレミスシステムと Cloud Volumes ONTAP システム間でデータをレプリケートする方法については、を参照してください ["システム間のデータレプリケーションの設定"](#)。

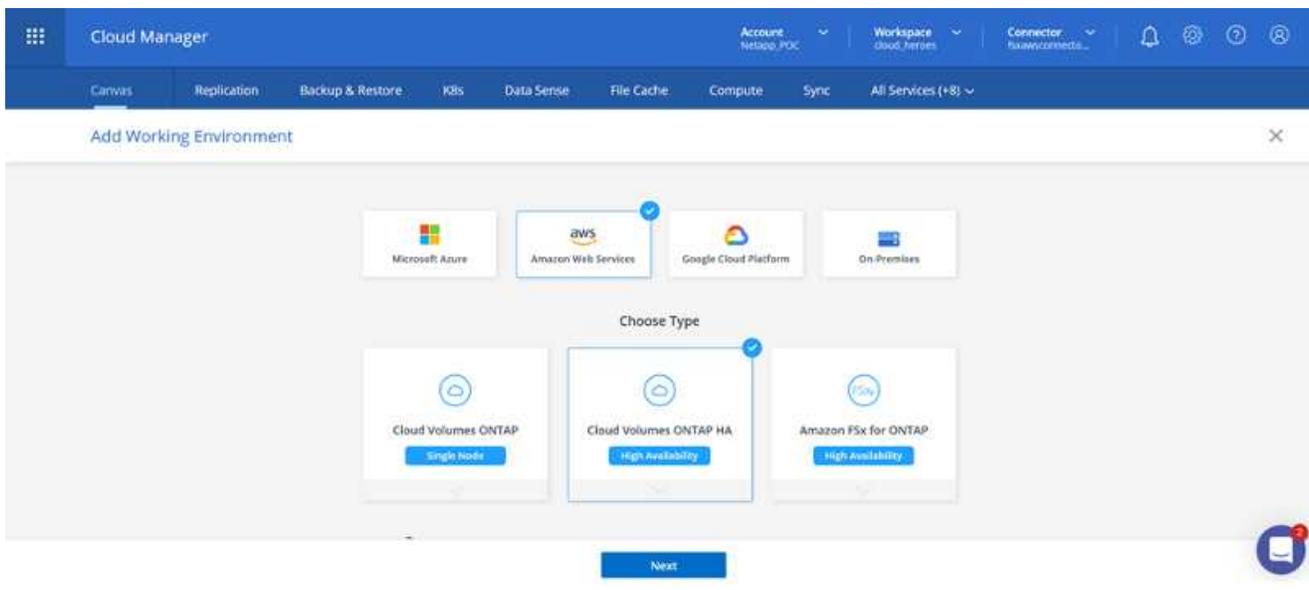


を使用します ["Cloud Volumes ONTAP サイジングツール"](#) Cloud Volumes ONTAP インスタンスのサイズを正確に設定します。また、オンプレミスのパフォーマンスを監視して、Cloud Volumes ONTAP サイジングツールの入力として使用することもできます。

1. NetApp Cloud Central にログインします。Fabric View 画面が表示されます。Cloud Volumes ONTAP タブを探し、Go to Cloud Manager を選択します。ログインすると、キャンバス画面が表示されます。



1. Cloud Manager のホームページで、Add a Working Environment をクリックし、AWS をクラウドとして選択し、システム構成のタイプを選択します。



1. 環境名と admin クレデンシャルなど、作成する環境の詳細を指定します。Continue をクリックします。

Create a New Working Environment Details and Credentials

↑ Previous Step Instance Profile: 139763910815 netapp.com-cloud-volumes-...
Credential Name Account ID Marketplace Subscription [Edit Credentials](#)

<p>Details</p> <p>Working Environment Name (Cluster Name)</p> <input type="text" value="fsxcvotesting01"/> <p>+ Add Tags Optional Field Up to four tags</p>	<p>Credentials</p> <p>User Name</p> <input type="text" value="admin"/> <p>Password</p> <input type="password" value="*****"/> <p>Confirm Password</p> <input type="password" value="*****"/>
--	--

[Continue](#)

1. Cloud Volumes ONTAPの導入に使用するアドオンサービス（BlueXPの分類、BlueXPのバックアップとリカバリ、Cloud Insightsなど）を選択します。Continue をクリックします。

Create a New Working Environment Services

 Data Sense & Compliance	<input checked="" type="checkbox"/> 
 Backup to Cloud	<input checked="" type="checkbox"/> 
 Monitoring	<input checked="" type="checkbox"/> 

[Continue](#)

1. HA Deployment Models ページで、Multiple Availability Zones 設定を選択します。

Create a New Working Environment HA Deployment Models

↑ Previous Step

<p>Multiple Availability Zones</p> <ul style="list-style-type: none"> Provides maximum protection against AZ failures. Enables selection of 3 availability zones. An HA node serves data if its partner goes offline. <p><small>Extended Info</small></p>	<p>Single Availability Zone</p> <ul style="list-style-type: none"> Protects against failures within a single AZ. Single availability zone. HA nodes are in a placement group, spread across distinct underlying hardware. An HA node serves data if its partner goes offline. <p><small>Extended Info</small></p>
---	---

1. Region & VPC ページで、ネットワーク情報を入力し、Continue をクリックします。

Create a New Working Environment Region & VPC

↑ Previous Step

AWS Region:

VPC:

Security group:

Node 1:	Node 2:	Mediator:
Availability Zone: <input type="text" value="us-west-2a"/>	Availability Zone: <input type="text" value="us-west-2b"/>	Availability Zone: <input type="text" value="us-west-2c"/>
Subnet: <input type="text" value="10.222.1.0/24"/>	Subnet: <input type="text" value="10.222.2.0/24"/>	Subnet: <input type="text" value="10.222.3.0/24"/>

1. [Connectivity and SSH Authentication] ページで、HA ペアとメディエータの接続方法を選択します。

Create a New Working Environment Connectivity & SSH Authentication

↑ Previous Step

Nodes	Mediator
SSH Authentication Method: <input type="text" value="Password"/>	Security Group: <input type="text" value="Use a generated security group"/>
	Key Pair Name: <input type="text" value="nimokey"/>
	Internet Connection Method: <input type="text" value="Public IP address"/>

1. フローティング IP アドレスを指定し、Continue（続行）をクリックします。

↑ Previous Step

Floating IP addresses are required for cluster and SVM access and for NFS and CIFS data access. These floating IPs can migrate between HA nodes if failures occur. To access the data from outside the VPC, [you can set up an AWS transit gateway](#).

You must specify IP addresses that are outside of the CIDR blocks for all VPCs in the selected AWS region.

Floating IP address for cluster management

172.16.0.1

Floating IP address 1 for NFS and CIFS data

172.16.0.2

Floating IP address 2 for NFS and CIFS data

172.16.0.3

Floating IP address for SVM management (Optional)

172.16.0.4

Continue

1. フローティング IP アドレスへのルートを含める適切なルーティングテーブルを選択し、Continue（続行）をクリックします。

↑ Previous Step

Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volumes ONTAP HA pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair.

Additional information ⓘ

Name	Main	ID	Associate with Subnet	Tags
<input checked="" type="checkbox"/>	Yes	rtb-00b2d30c3f68fdbdd	0 Subnets	1 Tags

1 Route Tables | The main route table is the default for the VPC

Continue

1. Data Encryption ページで、AWS で管理する暗号化を選択します。

↑ Previous Step

AWS Managed Encryption

AWS is responsible for data encryption and decryption operations. Key management is handled by AWS key management services.

Default Master Key: `aws/ebs`

[Change Key](#)

Continue

1. ライセンスオプションとして、「従量課金制」または「BYOL for using an existing license」を選択します。この例では、[従量課金制] オプションを使用します。

Create a New Working Environment Cloud Volumes ONTAP Charging Methods & NSS Account

Cloud Volumes ONTAP Charging Methods

[Learn more about our charging methods](#)



Pay-As-You-Go by the hour



Bring your own license

NetApp Support Site Account *(Optional)*

[Learn more about NetApp Support Site \(NSS\) accounts](#)

To register this Cloud Volumes ONTAP to support, you should add NetApp Support Site Account.

Don't have a NetApp Support Site account? Select go to finish deploying this system. After its created, use the Support Registration option to create an NSS account.

Continue

1. AWS SDDC 上の VMware クラウドで実行されている VM に導入するワークロードのタイプに基づいて、複数の事前設定パッケージから選択できます。



Select a preconfigured Cloud Volumes ONTAP system that best matches your needs, or create your own configuration. Preconfigured settings can be modified at a later time.

[Change Configuration](#)



POC and small workloads

Up to 500GB of storage



Database and application data
production workloads



Cost effective DR
Up to 500GB of storage



Highest performance production
workloads

Continue

1. [確認と承認] ページで、選択内容を確認して確定します。 Cloud Volumes ONTAP インスタンスを作成するには、[移動] をクリックします。

Create a New Working Environment Review & Approve

↑ Previous Step **fsxcvotesting** Show API request

AWS | us-west-2 | HA

This Cloud Volumes ONTAP instance will be registered with NetApp support under the NSS Account **mchad**.

I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. [More information >](#)

Overview | Networking | Storage

Storage System:	Cloud Volumes ONTAP HA	HA Deployment Model:	Multiple Availability Zones
License Type:	Cloud Volumes ONTAP Explore	Encryption:	AWS Managed
Capacity Limit:	2TB	Customer Master Key:	aws/ebs

[Go](#)

1. Cloud Volumes ONTAP のプロビジョニングが完了すると、[Canvas] ページの作業環境に表示されます。

Canvas | Replication | Backup & Restore | KBS | Data Sense | File Cache | Compute | Sync | All Services (+8) v

Canvas Go to Tabular View

Add Working Environment

fsxcvotesting01
Cloud Volumes ONTAP
46 GB Capacity

wndsva12
FSa for ONTAP
9 Volumes | 26.49 GB Capacity

Amazon S3
4 Buckets | 2 Regions

fsxcvotesting01 ⓘ ⓘ ⌵

On

DETAILS

Cloud Volumes ONTAP | AWS | HA

SERVICES

- Replication Enable ⓘ
- Backup & Restore Loading... ⓘ

SMB ボリューム用の追加の設定

1. 作業環境の準備ができたなら、CIFS サーバに適切な DNS および Active Directory 設定パラメータが設定されていることを確認します。この手順は、SMB ボリュームを作成する前に実行する必要があります。

The screenshot shows the 'Create a CIFS server' form in the AWS console for the instance 'fsxcvotesting01'. The form includes the following fields:

- DNS Primary IP Address: 192.168.1.3
- DNS Secondary IP Address (Optional): Example: 127.0.0.1
- Active Directory Domain to join: fsxtesting.local
- Credentials authorized to join the domain: Username and Password fields.

Buttons for 'Save' and 'Cancel' are visible at the bottom.

1. CVO インスタンスを選択してボリュームを作成し、Create Volume（ボリュームの作成）オプションをクリックします。適切なサイズを選択し、包含アグリゲートを選択するか、高度な割り当てメカニズムを使用して特定のアグリゲートに配置します。このデモでは、SMB がプロトコルとして選択されます。

The screenshot shows the 'Volume Details, Protection & Protocol' configuration page. It is divided into two main sections:

- Details & Protection:**
 - Volume Name: smbdemov01
 - Size (GB): 100
 - Snapshot Policy: default
 - Default Policy: selected
- Protocol:**
 - Selected Protocol: CIFS
 - Share name: smbdemov01_share
 - Permissions: Full Control
 - Users / Groups: Everyone;

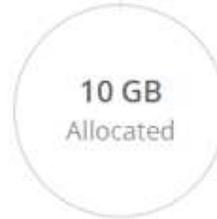
A 'Continue' button is located at the bottom of the form.

1. ボリュームのプロビジョニングが完了すると、Volumes（ボリューム）ペインにボリュームが表示されます。CIFS 共有はプロビジョニングされるため、ユーザまたはグループにファイルおよびフォルダに対する権限を付与し、ユーザが共有にアクセスしてファイルを作成できることを確認する必要があります。

INFO

Disk Type	GP2
Tiering Policy	None
Backup	OFF

CAPACITY



1.67 MB
EBS Used

1. ボリュームが作成されたら、 mount コマンドを使用して、 AWS SDDC ホストの VMware Cloud で実行されている VM から共有に接続します。
2. 次のパスをコピーし、 Map Network Drive オプションを使用して、 AWS SDDC の VMware Cloud で実行されている VM にボリュームをマウントします。

Volumes HA Status Cost Replications



Mount Volume smbdemov01

Access from inside the VPC using Floating IP

Auto failover between nodes
The IP address automatically migrates between nodes if failures occur

Go to your machine and enter this command

\\172.16.0.2\smbdemov01_share



Access from outside the VPC using AWS Private IP

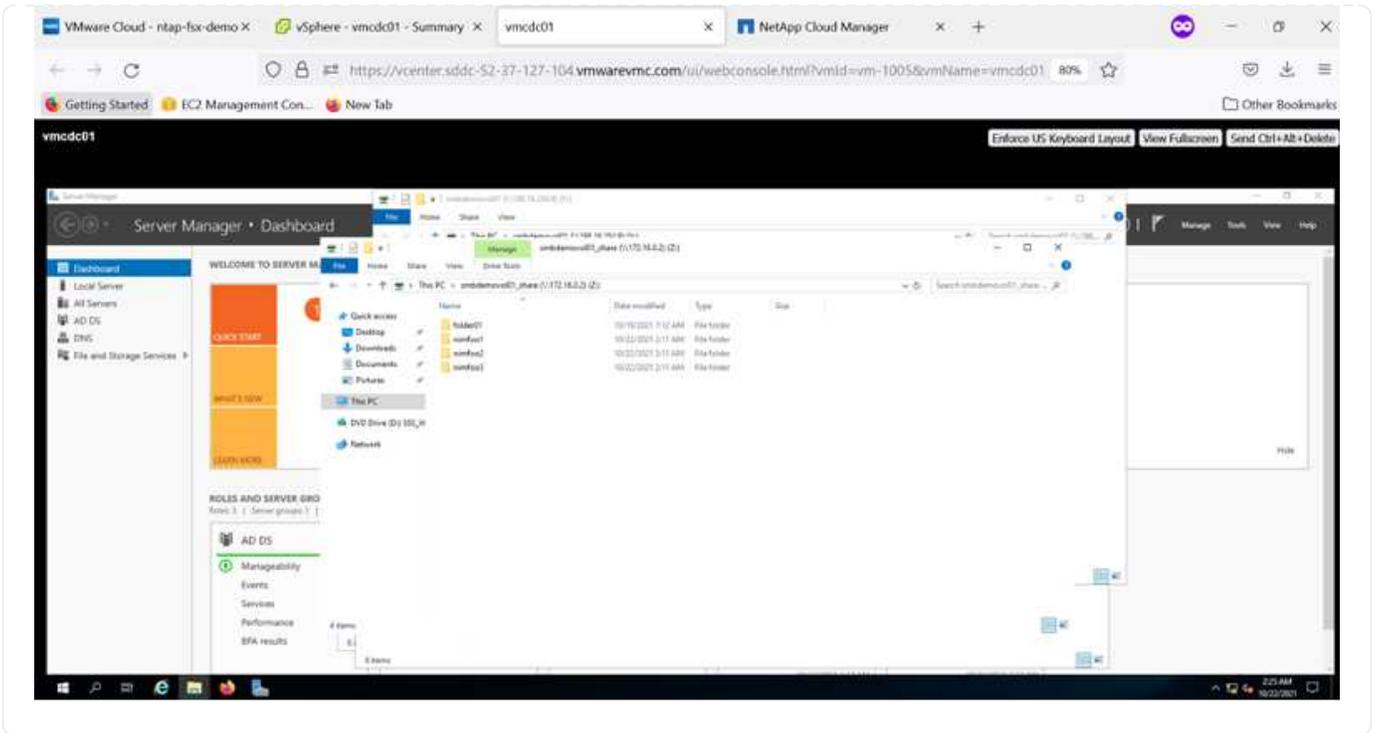
No auto failover between nodes
The IP address does not migrate between nodes if failures occur

To avoid traffic between nodes, mount the volume by using the primary node's IP address:

\\10.222.1.100\smbdemov01_share



If the primary node goes offline, mount the volume by using the HA partner's IP address:



LUN をホストに接続します

Cloud Volumes ONTAP LUN をホストに接続するには、次の手順を実行します。

1. Cloud Manager のキャンバスページで、Cloud Volumes ONTAP 作業環境をダブルクリックしてポリシーームを作成および管理します。
2. Add Volume (ボリュームの追加) > New Volume (新規ボリューム) をクリックし、iSCSI を選択して Create Initiator Group (イニシエータグループのContinue をクリックします)。

Create new volume in fsxcvotesting01 Volume Details, Protection & Protocol

Details & Protection

Volume Name: Size (GB):

Snapshot Policy:
 Default Policy

Protocol

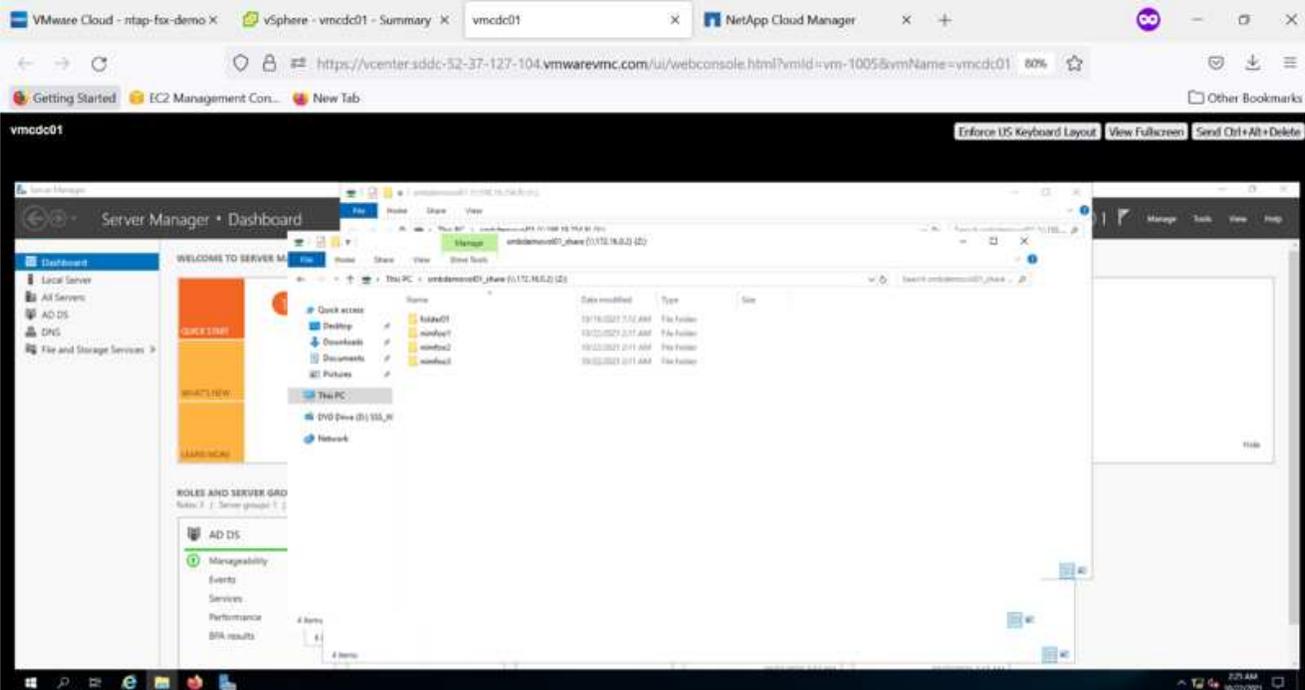
NFS CIFS **iSCSI**
 What about LUNs?

Initiator Group
 Map Existing Initiator Groups Create Initiator Group

Operating System Type

Select Initiator Groups: 1 (of 3) Groups
 winIG | windows
 iqn.1991-05.com.microsoft:vmcdc01.fsxtestin...

Continue



1. ボリュームのプロビジョニングが完了したら、ボリュームを選択し、ターゲット IQN をクリックします。iSCSI Qualified Name (IQN) をコピーするには、Copy (コピー) をクリックします。ホストから LUN への iSCSI 接続をセットアップします。

AWS SDDC 上の VMware Cloud にあるホストでも同じ処理を実行するには、次の手順を実行します。

1. AWS の VMware クラウドでホストされる VM への RDP
2. [iSCSI イニシエータのプロパティ] ダイアログ・ボックスを開きます [サーバーマネージャ] > [ダッシュボード] > [ツール] > [iSCSI イニシエータ]
3. Discovery (検出) タブで、Discover Portal (ポータルを検出) または Add Portal (ポータルの追加) をクリックし、iSCSI ターゲットポートの IP アドレスを入力します。
4. ターゲットタブで検出されたターゲットを選択し、ログオンまたは接続をクリックします。
5. [マルチパスを有効にする] を選択し、コンピュータの起動時に [この接続を自動的に復元する] または [この接続をお気に入りターゲットのリストに追加する] を選択します。Advanced (詳細設定) をクリック

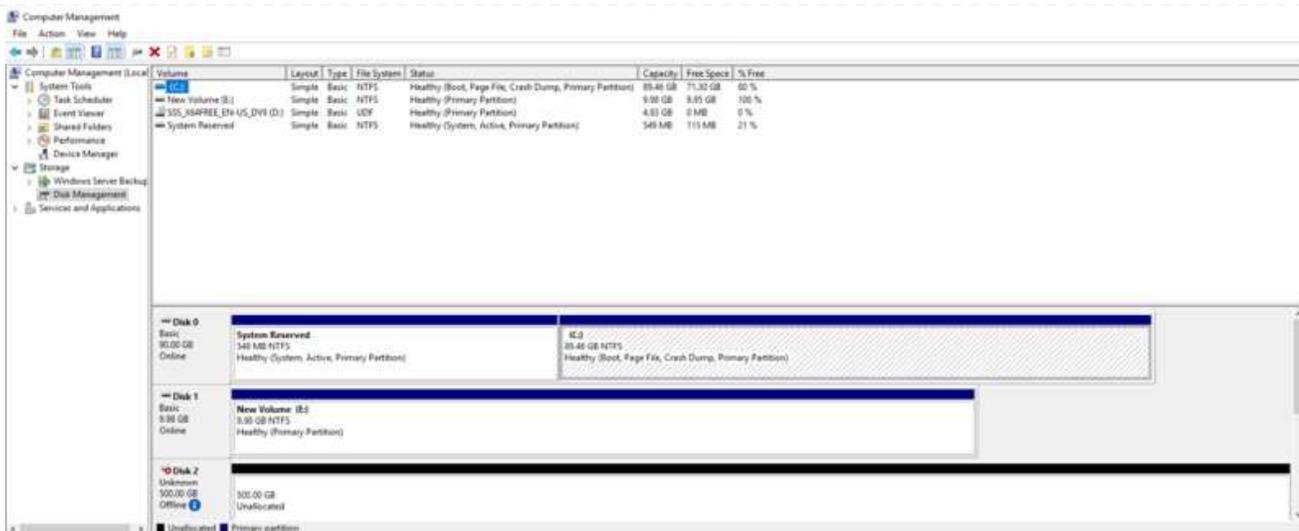


Windows ホストには、クラスタ内の各ノードへの iSCSI 接続が必要です。ネイティブ DSM では、使用する最適なパスが選択されます。



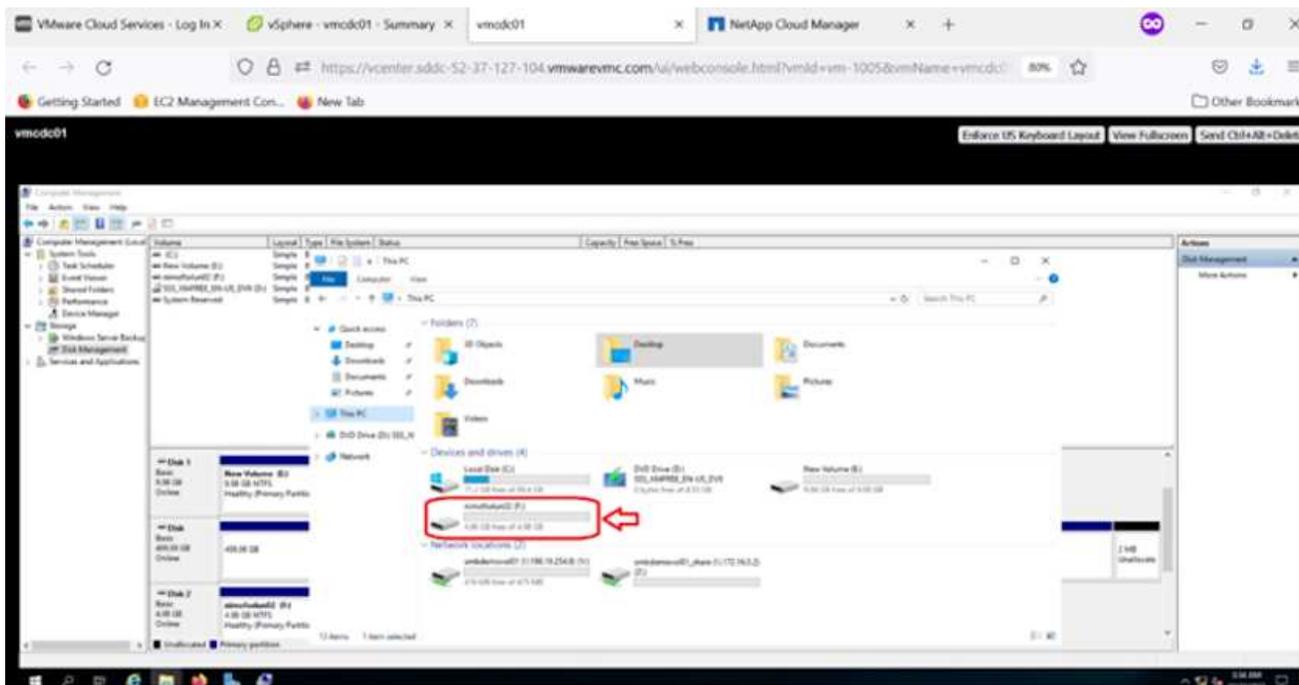
SVM の LUN は、Windows ホストではディスクとして表示されます。追加した新しいディスクは、ホストでは自動的に検出されません。手動の再スキャンをトリガーしてディスクを検出するには、次の手順を実行します。

1. Windows コンピュータの管理ユーティリティを開きます。[スタート]>[管理ツール]>[コンピュータの管理] を選択します。
2. ナビゲーションツリーでストレージノードを展開します。
3. [ディスクの管理] をクリックします
4. [アクション] > [ディスクの再スキャン] の順にクリック



Windows ホストから初めてアクセスした時点では、新しい LUN にはパーティションやファイルシステムは設定されていません。LUN を初期化します。必要に応じて、次の手順を実行してファイルシステムで LUN をフォーマットします。

1. Windows ディスク管理を開始します。
2. LUN を右クリックし、必要なディスクまたはパーティションのタイプを選択します。
3. ウィザードの指示に従います。この例では、ドライブ F : がマウントされています。



Linux クライアントで、iSCSI デーモンが実行されていることを確認します。LUN のプロビジョニングが完了したら、Linux ディストリビューション向けの iSCSI 構成に関する詳しいガイダンスを参照してください。たとえば、Ubuntu の iSCSI 構成が見つかります "[こちらをご覧ください](#)". これを確認するには、シェルから `lsblk` cmd を実行します。

Cloud Volumes ONTAP NFS ボリュームを Linux クライアントにマウント

Cloud Volumes ONTAP（DIY）ファイルシステムを VMC 内の VM から AWS SDDC にマウントするには、次の手順を実行します。

1. 指定された Linux インスタンスに接続します。
2. Secure Shell（SSH）を使用してインスタンスの端末を開き、適切なクレデンシャルでログインします。
3. 次のコマンドを使用して、ボリュームのマウントポイント用のディレクトリを作成します。

```
$ sudo mkdir /fsxcvotesting01/nfsdemov0101
. 前の手順で作成したディレクトリに、NetApp ONTAP NFS ボリュームの Amazon FSX をマウントします。
```

```
sudo mount -t nfs nfsvers=4.1,172.16.0.2:/nfsdemov0101
/fsxcvotesting01/nfsdemov0101
```



```
root@ubuntu01:/fsx# mount -t nfs 172.16.0.2:/nfsdemov0101 /fsxcvotesting01/nfsdemov0101_
root@ubuntu01:/fsx/nfsdemov0101# df
Filesystem            1k-blocks    Used Available Use% Mounted on
tmpfs                  814396      1176    813220   1% /run
/dev/mapper/ubuntuvg-ubuntu--iv 19412168 3666428 10943132  2% /
tmpfs                  4071960      0    4071960   0% /dev/shm
tmpfs                   5120         0     5120   0% /run/lock
tmpfs                   4096         0     4096   0% /sys/fs/cgroup
/dev/sda2              999320 254996  675512  2% /boot
tmpfs                   814392         4     814388   1% /run/user/1000
172.16.0.2:/nfsdemov0101 9961472 4241792 5719680 43% /fsxcvotesting01/nfsdemov0101
190.19.254.239:/nfsdemov0101 996160     512   995648   1% /fsx/nfsdemov0101
root@ubuntu01:/fsx/nfsdemov0101# cd /fsx/nfsdemov0101/
root@ubuntu01:/fsx/nfsdemov0101# ls
nfsvol11.txt
root@ubuntu01:/fsx/nfsdemov0101#
```

ANFデータストアソリューションの概要

成功を収めている組織は、変革と刷新の道を歩んでいます。このプロセスの一環として、企業は通常、既存のVMwareへの投資を活用しながら、クラウドのメリットを活用し、移行、バースト、拡張、ディザスタリカバリのプロセスを可能な限りシームレスに実行する方法を模索しています。クラウドに移行するお客様は、柔軟性とバースト性、データセンターの終了、データセンターの統合、サポート終了シナリオ、合併や買収などの問題を評価する必要があります。各組織が採用するアプローチは、それぞれのビジネスの優先順位に応じて異なります。クラウドベースの運用を選択する場合、適切なパフォーマンスと最小限の障害を持つ低コストモデルを選択することが重要な目標です。適切なプラットフォームを選択するとともに、クラウドの導入と柔軟性を最大限に活用するために、ストレージとワークフローのオーケストレーションが特に重要になり

ます。

ユースケース

Azure VMware解決策 はお客様に独自のハイブリッド機能を提供しますが、ネイティブストレージのオプションが限られているため、ストレージの負荷が高い組織での有用性が制限されています。ストレージはホストに直接関連付けられているため、ストレージを拡張する唯一の方法は、ホストを追加することです。これにより、ストレージを大量に消費するワークロードのコストを35~40%以上増加させることができます。このようなワークロードに必要なストレージ容量は追加ではなく、追加のホストに料金が発生します。

次のシナリオを考えてみましょう。お客様は6台のホストで馬力（vCPUとvMem）を求めています、ストレージの要件も大きくなっています。評価に基づいて、12台のホストがストレージ要件を満たしている必要があります。これにより、必要な容量をすべて追加購入するだけで、より多くのストレージが必要になるため、全体的なTCOが増加します。これは、移行、ディザスタリカバリ、バースト、開発/テストなど、あらゆるユースケースに当てはまります。 など。

Azure VMware解決策 のもう1つの一般的なユースケースは、ディザスタリカバリ（DR）です。ほとんどの組織には、裏付けのないDR戦略がないため、DR目的だけでゴーストデータセンターを運用する正当性を証明するのに苦労することがあります。管理者は、パイロットライトクラスタやオンデマンドクラスタを使用して、フットプリントゼロのDRオプションを検討できます。ホストを追加せずにストレージを拡張できるため、魅力的な選択肢となる可能性があります。

つまり、ユースケースは次の2つの方法で分類できます。

- ANFデータストアを使用したストレージ容量の拡張
- オンプレミスまたはAzureリージョン内のSoftware-Defined Storage（SDDC）間で、ANFデータストアをディザスタリカバリターゲットとして使用することで、コストを最適化したリカバリワークフローを実現できます。このガイドでは、Azure NetApp Files を使用してデータストアに最適化されたストレージを提供する方法を説明します（現時点ではパブリックプレビュー版です）。 Azure VMware解決策 の業界最高のデータ保護機能とDR機能を組み合わせることで、VSANストレージからストレージ容量をオフロードできます。



ANFデータストアの使用については、地域の追加情報 ネットアップアーキテクトまたはMicrosoft解決策 アーキテクトにお問い合わせください。

AzureのVMware Cloudオプション

Azure VMware 解決策の略

Azure VMware解決策（AVS）は、Microsoft Azureパブリッククラウド内でVMware SDSを完全に機能させるハイブリッドクラウドサービスです。AVSはMicrosoftが完全に管理およびサポートするファーストパーティの解決策で、Azureインフラストラクチャを使用するVMwareにより検証されています。そのため、コンピューティング仮想化用のVMware ESXi、ハイパーコンバージドストレージ用のVSAN、ネットワークとセキュリティ用のNSXを、Microsoft Azureのグローバルプレゼンス、クラス最高レベルのデータセンター施設、ネイティブのAzureサービスとソリューションの豊富なエコシステムの近くで利用できます。Azure VMware解決策 SDDCとAzure NetApp Files を組み合わせることで、ネットワークレイテンシを最小限に抑えながら最高のパフォーマンスを実現できます。

VMware SDDCを導入する際、使用するクラウドに関係なく、最初のクラスタには次のコンポーネントが含まれます。

- コンピューティング仮想化用のVMware ESXiホストと、管理用のvCenterサーバプライアンス

- 各ESXiホストの物理ストレージ資産を組み込んだVMware vSANハイパーコンバージドストレージ。
- 管理のためにNSX Managerクラスタを使用した仮想ネットワークとセキュリティのためのVMware NSX

まとめ

Azure NetApp Files は、オールクラウドとハイブリッドクラウドのどちらをターゲットとしている場合でも、アプリケーションワークロードとファイルサービスを導入して管理するための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と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性、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、Azure VMware解決策とAzure NetApp Files を選択してください。ストレージの接続に使用される一般的なプロセスと手順は同じです。新しい名前とともに変更されたデータの位置にすぎません。ツールやプロセスはすべて変わらないので、Azure NetApp Files を使用すると導入全体を最適化できます。

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。

- AVS SDDCのデータストアとしてAzure NetApp Files を使用できるようになりました。
- アプリケーションの応答時間を短縮し、可用性を高めて、必要なときに必要な場所でワークロードデータにアクセスできるようにします。
- シンプルで瞬時のサイズ変更機能により、VSANストレージの全体的な複雑さを緩和
- 動的な再構築機能でミッションクリティカルなワークロードのパフォーマンスを保証
- Azure VMware解決策 クラウドが移行先である場合、Azure NetApp Files は最適化された導入に最適なストレージ解決策 です。

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。

- Azure VMware解決策 のドキュメント

["https://docs.microsoft.com/en-us/azure/azure-vmware/"](https://docs.microsoft.com/en-us/azure/azure-vmware/)

- Azure NetApp Files のドキュメント

["https://docs.microsoft.com/en-us/azure/azure-netapp-files/"](https://docs.microsoft.com/en-us/azure/azure-netapp-files/)

- Azure VMware解決策 ホストへのAzure NetApp Files データストアの接続（プレビュー）

<https://docs.microsoft.com/en-us/azure/azure-vmware/attach-azure-netapp-files-to-azure-vmware-solution-hosts?tabs=azure-portal/>

Azure 向けネットアップゲスト接続ストレージオプション

Azureでは、ネイティブのAzure NetApp Files（ANF）サービスまたはCloud Volumes ONTAP（CVO）でゲスト接続ネットアップストレージをサポートしています。

Azure NetApp ファイル (ANF)

Azure NetApp Files は、エンタープライズクラスの詳細なデータ管理とストレージを Azure に提供するため、ワークロードとアプリケーションを簡単に管理できます。パフォーマンスを低下させることなく、ワークロードをクラウドに移行して実行できます。

Azure NetApp Files は障害を取り除き、ファイルベースのアプリケーションをすべてクラウドに移行できるようにします。初めてアプリケーションを再設計する必要はなく、アプリケーションの永続的ストレージを複雑化することはありません。

このサービスは Microsoft Azure Portal を通じて提供されるため、ユーザは Microsoft Enterprise Agreement の一部としてフルマネージドサービスを利用できます。マイクロソフトが管理するワールドクラスのサポートにより、安心してご利用いただけます。この1つの解決策で、マルチプロトコルワークロードをすばやく簡単に追加できます。従来の環境でも、Windows と Linux の両方のファイルベースアプリケーションを構築して導入できます。

ゲスト接続ストレージとしての **Azure NetApp Files (ANF)**

Azure VMware 解決策 (AVS) を使用した Azure NetApp Files の設定

解決策共有は、Azure VMware Azure NetApp Files SDDC 環境で作成された VM からマウントできます。Azure NetApp Files では SMB プロトコルと NFS プロトコルがサポートされているため、ボリュームを Linux クライアントにマウントして Windows クライアントにマッピングすることもできます。Azure NetApp Files ボリュームは、5 つの簡単な手順で設定できます。

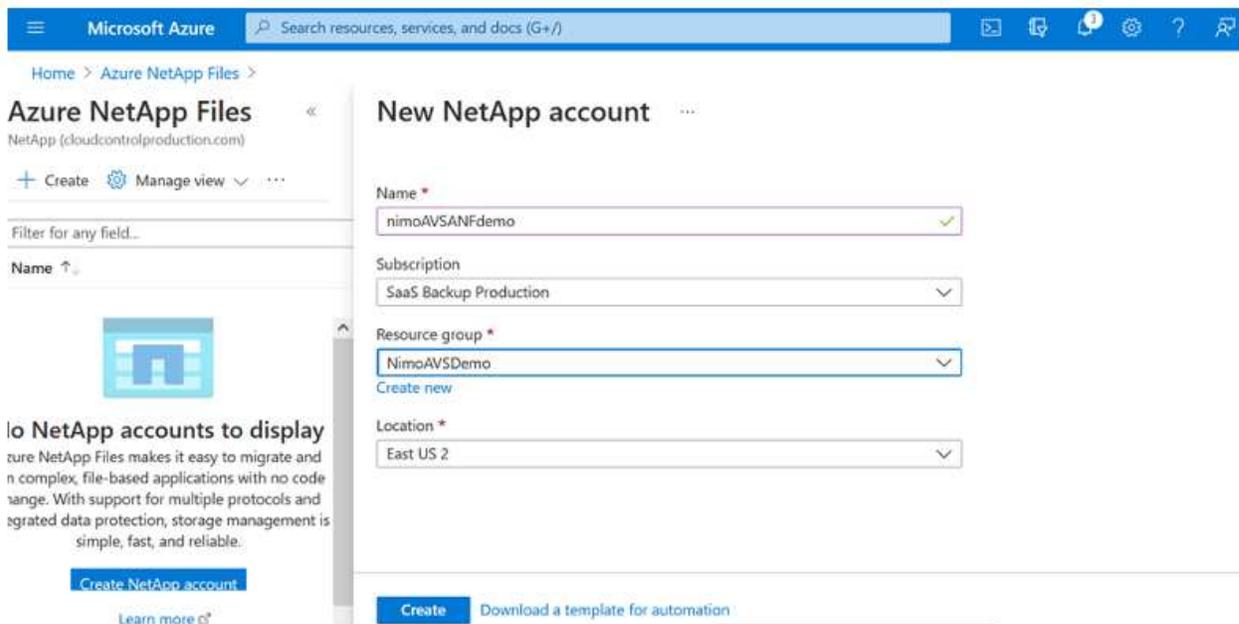
Azure NetApp Files と Azure VMware 解決策は、同じ Azure リージョンに配置する必要があります。

Azure NetApp Files ボリュームを作成してマウント

Azure NetApp Files ボリュームを作成してマウントするには、次の手順を実行します。

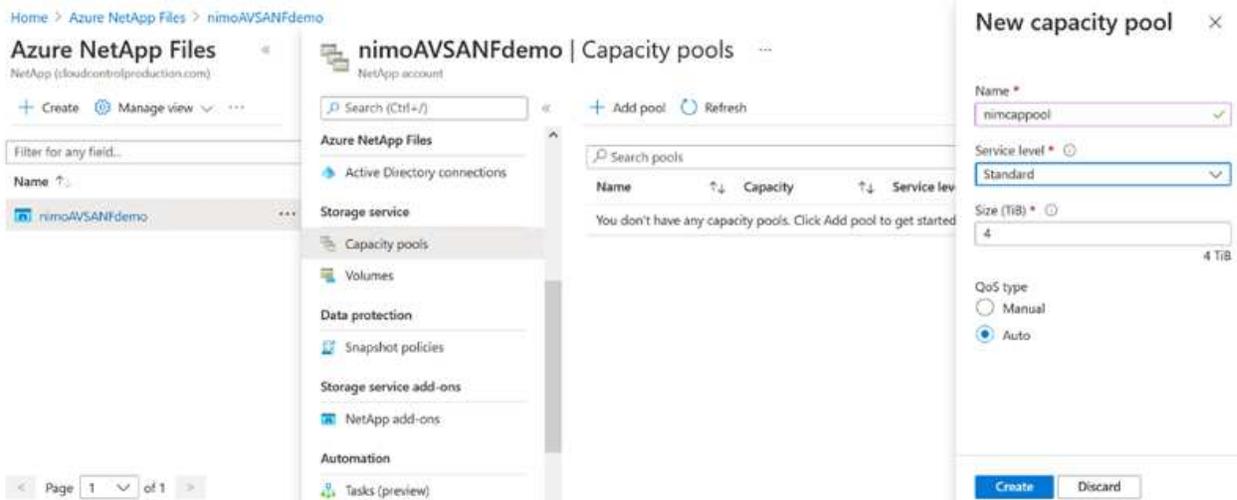
1. Azure ポータルにログインし、Azure NetApp Files にアクセスします。Azure NetApp Files サービスへのアクセスを確認し、Azure NetApp Files リソースプロバイダを登録するには、_az プロバイダ登録 — namespace Microsoft.NetApp – wait_command を使用します。登録が完了したら、ネットアップアカウントを作成します。

詳細な手順については、を参照してください ["Azure NetApp Files 共有"](#)。このページでは、ステップバイステップのプロセスについて説明します。

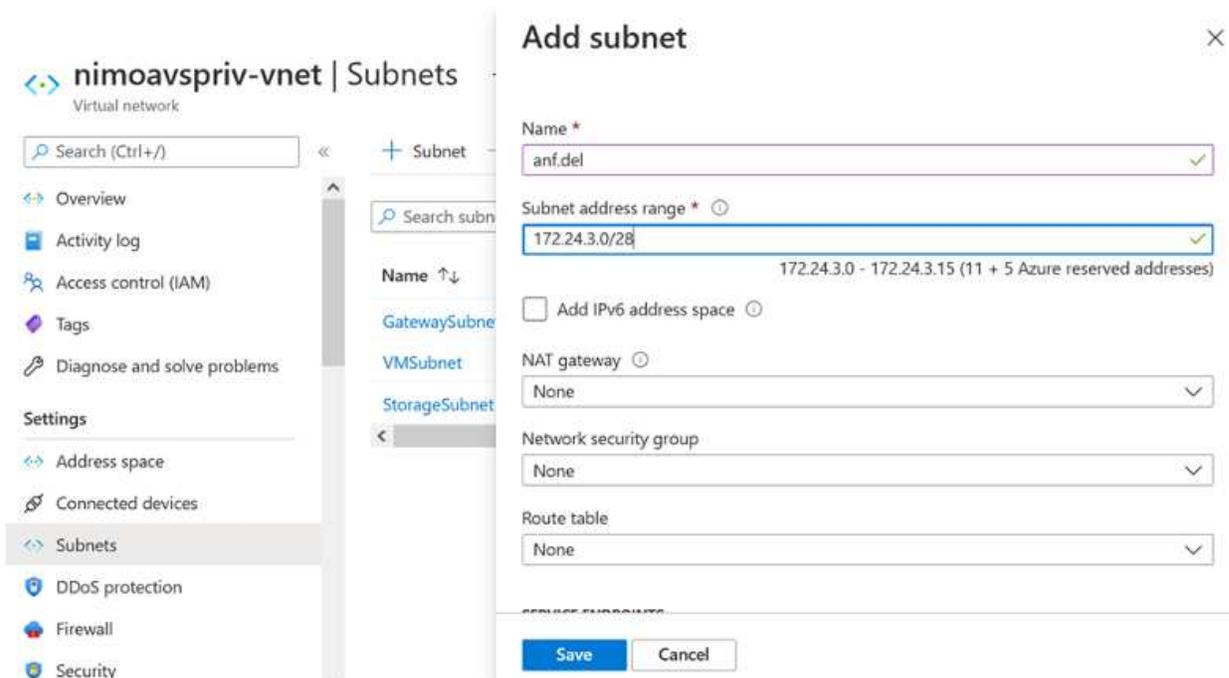


2. ネットアップアカウントが作成されたら、必要なサービスレベルとサイズの容量プールを設定します。

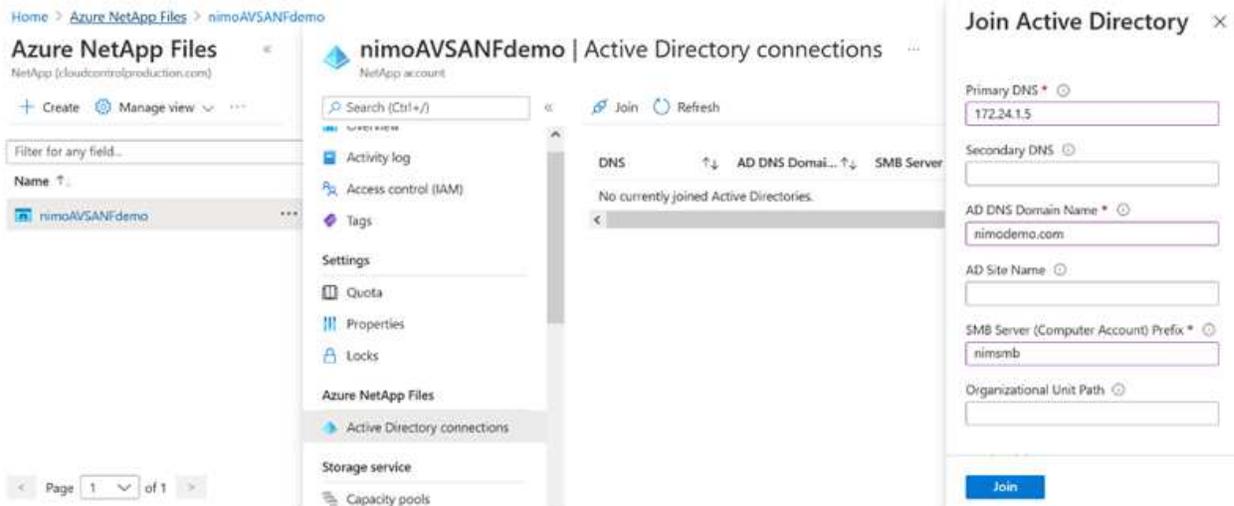
詳細については、を参照してください ["容量プールをセットアップする"](#)。



3. Azure NetApp Files の委任されたサブネットを設定し、ボリュームを作成する際にこのサブネットを指定します。委任されたサブネットを作成する詳細な手順については、[を参照してください "サブネットを Azure NetApp Files に委譲します"](#)。

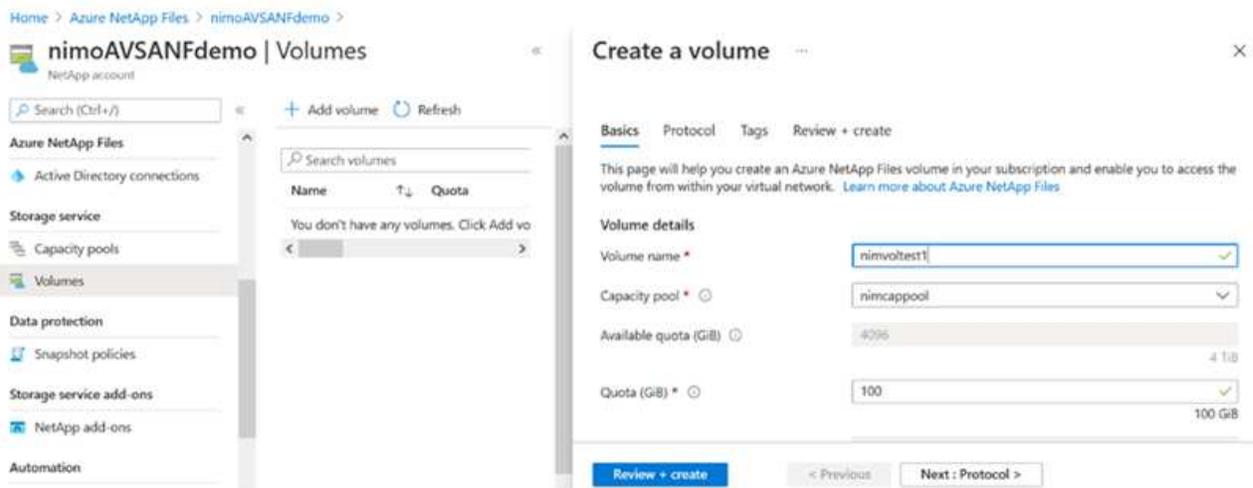


4. 容量プールブレードの下ボリュームブレードを使用して、SMB ボリュームを追加します。SMB ボリュームを作成する前に、Active Directory Connector が設定されていることを確認してください。



5. [Review + Create] をクリックして、SMB ボリュームを作成します。

アプリケーションが SQL Server の場合は、SMB 継続的可用性を有効にします。

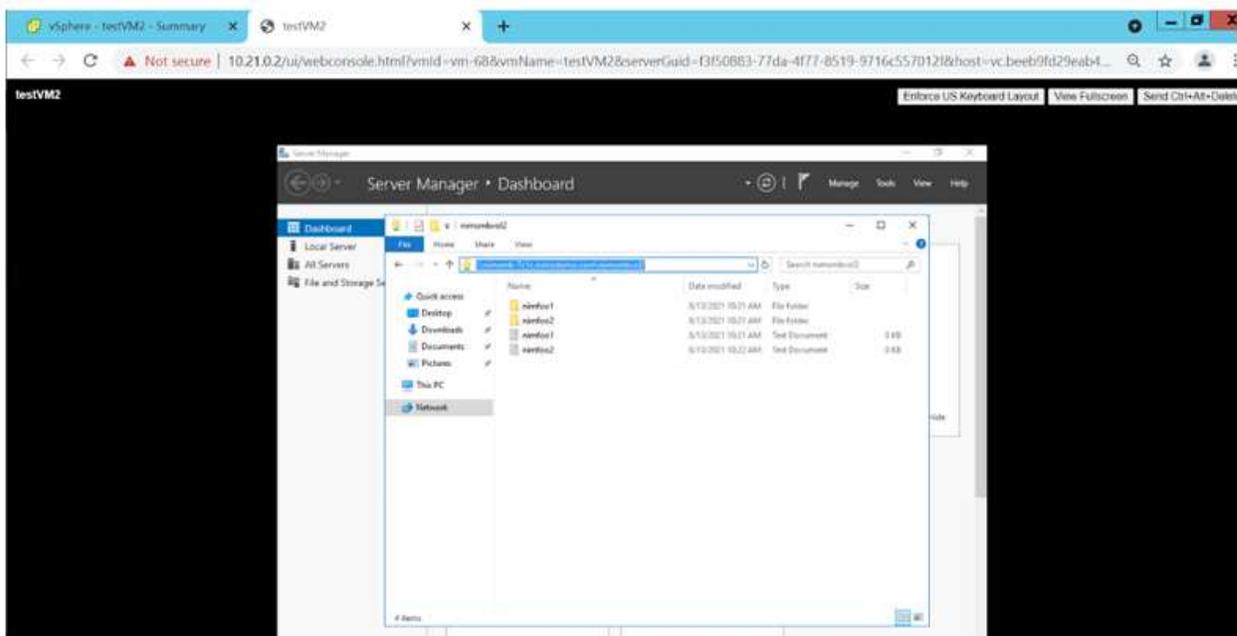


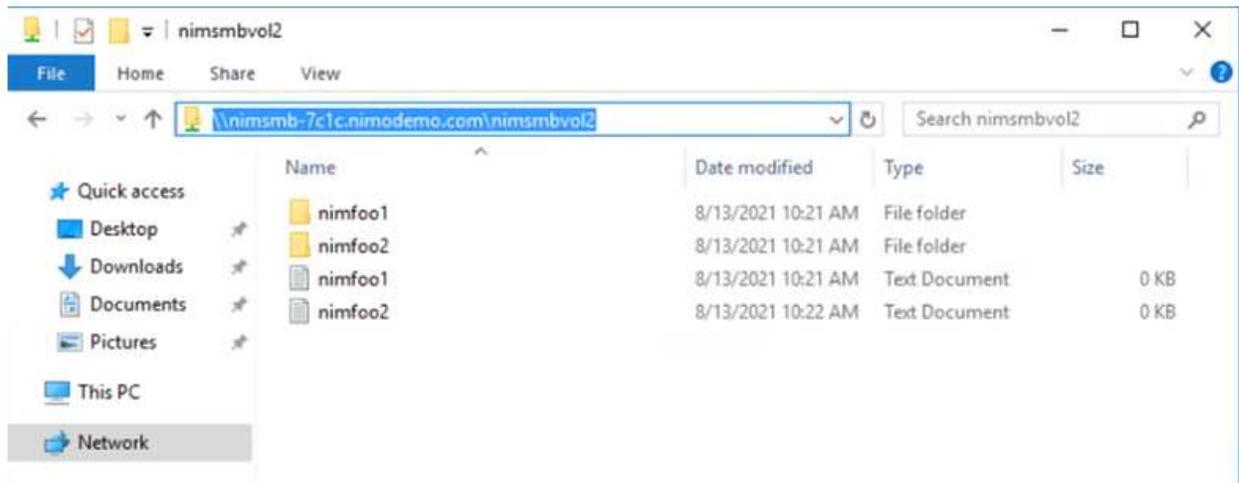


サイズまたはクォータ別の Azure NetApp Files ボリュームのパフォーマンスの詳細については、を参照してください ["Azure NetApp Files のパフォーマンスに関する考慮事項"](#)。

- 接続が確立されると、ボリュームをマウントしてアプリケーションデータに使用できるようになります。

これを行うには、Azure ポータルで Volumes ブレードをクリックし、マウントするボリュームを選択して、マウント手順にアクセスします。パスをコピーし、ネットワークドライブのマッピングオプションを使用して、Azure VMware 解決策 SDDC で実行されている VM にボリュームをマウントします。





- Azure VMware 解決策 SDDC で実行されている Linux VM に NFS ボリュームをマウントする場合も、同じ手順を使用します。ボリュームの形状変更機能または動的なサービスレベル機能を使用して、ワークロードの要件を満たします。

```
nimoadmin@nimoadmin-virtual-machine:~$ sudo mount -t nfs -o rw,hard,tcp 172.24.3.4:/niodemonfsv1 /home/nimoadmin/nimodemo11
nimoadmin@nimoadmin-virtual-machine:~$ df
Filesystem                1K-blocks    Used Available Use% Mounted on
udev                      8168112         0  8168112   0% /dev
tmpfs                     1639548         1488  1638060   1% /run
/dev/sda5                 50824704 7902752  40310496  17% /
tmpfs                     8197728         0  8197728   0% /dev/shm
tmpfs                     5120           0    5120     0% /run/lock
tmpfs                     8197728         0  8197728   0% /sys/fs/cgroup
/dev/loop0                56832          56832     0 100% /snap/core18/2128
/dev/loop2                66688          66688     0 100% /snap/gtk-common-themes/1515
/dev/loop1                224256         224256     0 100% /snap/gnome-3-34-1804/72
/dev/loop3                52224          52224     0 100% /snap/snap-store/547
/dev/loop4                33152          33152     0 100% /snap/snapd/12704
/dev/sda1                 523248         4    523244   1% /boot/efi
tmpfs                     1639544         52  1639492   1% /run/user/1000
/dev/sr0                  54738          54738     0 100% /media/nimoadmin/VMware Tools
172.24.3.4:/niodemonfsv1 104857600         0 104857600  0% /home/nimoadmin/nimodemo11
nimoadmin@nimoadmin-virtual-machine:~$
```

詳細については、[こちら](#)を参照してください "ボリュームのサービスレベルを動的に変更する"。

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP (CVO) は、ネットアップのONTAP ストレージソフトウェアを基盤に構築された、業界をリードするクラウドデータ管理解決策です。Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP) でネイティブに利用できます。

ソフトウェアで定義されるONTAP バージョンで、クラウドネイティブなストレージを消費し、クラウドとオ

ンプレミスで同じストレージソフトウェアを使用できるため、まったく新しい方法でIT担当者のデータ管理を再トレーニングする必要がありません。

CVOを使用すれば、エッジ、データセンター、クラウド間でシームレスにデータを移動し、ハイブリッドクラウドを統合できます。すべてを1画面の管理コンソールであるNetApp Cloud Managerで管理できます。

設計上、CVOは卓越したパフォーマンスと高度なデータ管理機能を備えており、クラウドで最も要件の厳しいアプリケーションにも対応できます

Cloud Volumes ONTAP (CVO) をゲスト接続ストレージとして活用

Azure に新しい Cloud Volumes ONTAP を導入

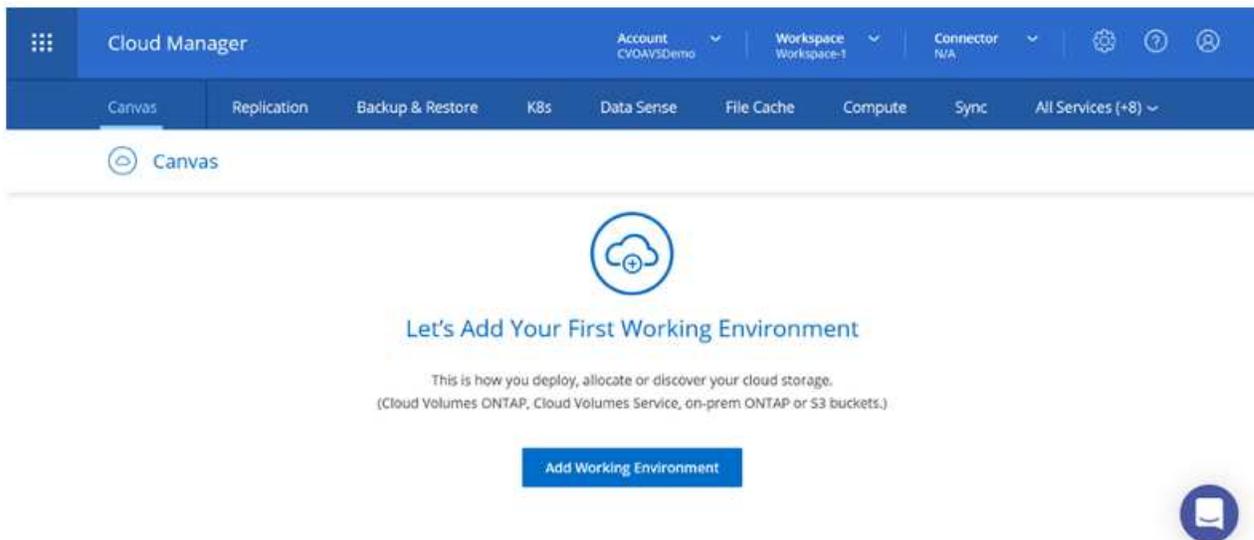
解決策共有および LUN は、Azure VMware Cloud Volumes ONTAP SDDC 環境で作成された VM からマウントできます。Cloud Volumes ONTAP は iSCSI、SMB、NFS の各プロトコルをサポートしているため、このボリュームは Linux クライアントおよび Windows クライアントにもマウントできます。Cloud Volumes ONTAP ボリュームは、いくつかの簡単な手順で設定できます。

ディザスタリカバリや移行の目的でオンプレミス環境からクラウドにボリュームをレプリケートするには、サイト間 VPN または ExpressRoute を使用して、Azure へのネットワーク接続を確立します。オンプレミスから Cloud Volumes ONTAP へのデータのレプリケートについては、本ドキュメントでは扱いません。オンプレミスシステムと Cloud Volumes ONTAP システム間でデータをレプリケートする方法については、を参照してください ["システム間のデータレプリケーションの設定"](#)。

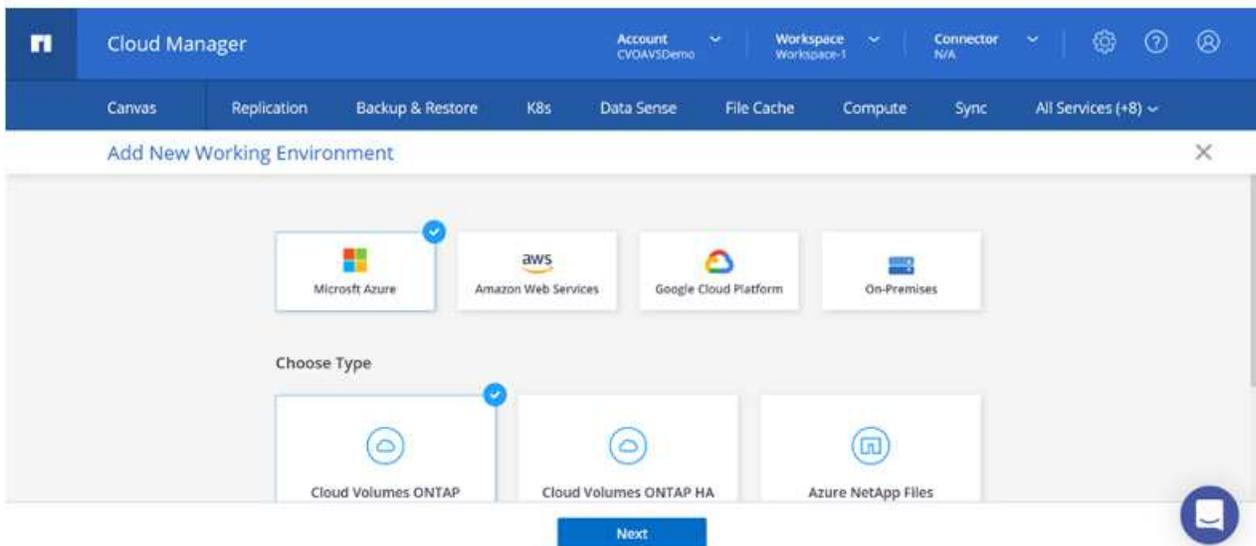


使用 ["Cloud Volumes ONTAP サイジングツール"](#) Cloud Volumes ONTAP インスタンスのサイズを正確に設定します。また、オンプレミスのパフォーマンスを監視し、Cloud Volumes ONTAP のサイジングツールの情報として使用できます。

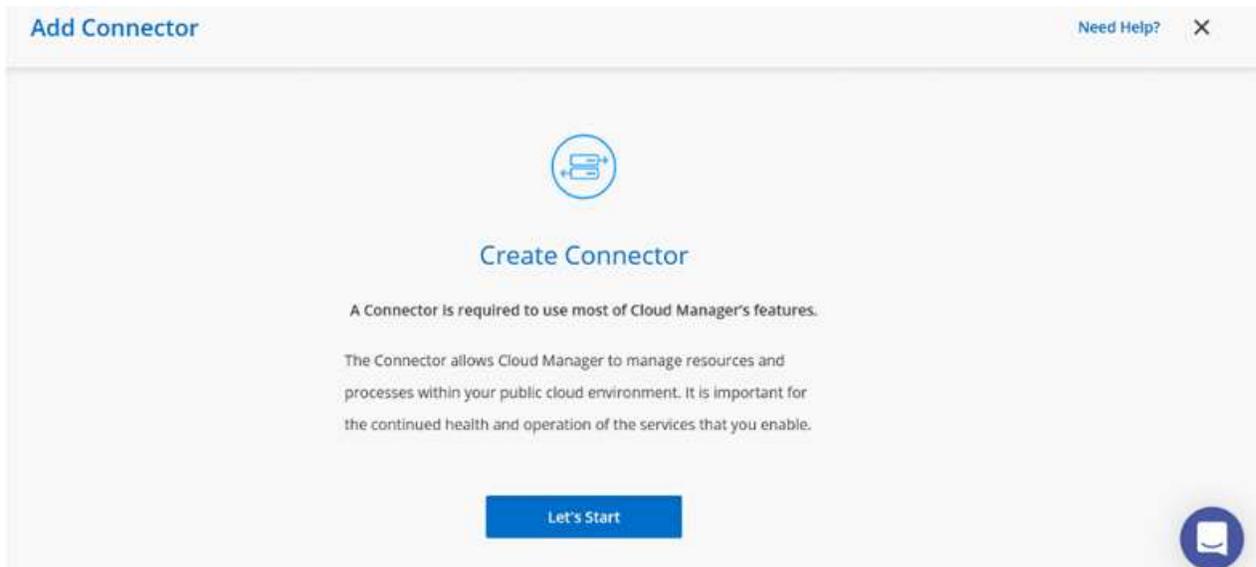
1. NetApp Cloud Central にログイン— Fabric View (ファブリックビュー) 画面が表示されます。Cloud Volumes ONTAP タブを探し、Go to Cloud Manager を選択します。ログインすると、キャンバス画面が表示されます。



2. Cloud Manager のホームページで、Add a Working Environment をクリックし、クラウドとして Microsoft Azure を選択し、システム構成のタイプを選択します。



3. Cloud Volumes ONTAP の最初の作業環境を作成する際、Cloud Manager はコネクタの導入を求めます。



4. コネクタが作成されたら、[詳細 (Details)] および [資格情報 (Credentials)] フィールドを更新します。

Managed Service Ide...	SaaS Backup Prod...	CMCVOSub	Edit Credentials
Credential Name	Azure Subscription	Marketplace Subscription	

Details	Credentials
Working Environment Name (Cluster Name)	User Name
<input type="text" value="nimavsCVO"/>	<input type="text" value="admin"/>
	Password

[Continue](#)

5. 環境名と admin クレデンシャルなど、作成する環境の詳細を指定します。オプションのパラメータとして、Azure 環境のリソースグループタグを追加します。完了したら、[続行] をクリックします。

Details	Credentials
Working Environment Name (Cluster Name)	User Name
<input type="text" value="nimavsCVO"/>	<input type="text" value="admin"/>
+ Add Resource Group Tags <small>Optional Field</small>	Password
	<input type="password" value="....."/>
	Confirm Password
	<input type="password" value="....."/>

[Continue](#)

6. Cloud Volumes ONTAPの導入に使用するアドオンサービス（BlueXPの分類、BlueXPのバックアップとリカバリ、Cloud Insightsなど）を選択します。サービスを選択し、Continue（続行）をクリックします。

 Data Sense & Compliance	<input checked="" type="checkbox"/> ▼
 Backup to Cloud	<input checked="" type="checkbox"/> ▼
 Monitoring	<input checked="" type="checkbox"/> ▼

[Continue](#)

7. Azure の場所と接続を設定します。使用する Azure のリージョン、リソースグループ、VNet、およびサブネットを選択します。

Azure Region East US 2	Resource Group <input checked="" type="radio"/> Create a new group <input type="radio"/> Use an existing group
Availability Zone (Optional) Select an Availability Zone	Resource Group Name nimassCVO-rg
VNet nimoavspriv-vnet NimoAVSDemo	Security Group <input checked="" type="radio"/> Generated security group <input type="radio"/> Use existing security group
Subnet 172.24.2.0/24	<input checked="" type="checkbox"/> I have verified network connectivity between the Cloud Manager server and the selected VNet.

[Continue](#)

8. ライセンスオプションとして、「従量課金制」または「BYOL for using existing license」を選択します。この例では、[従量課金制] オプションを使用します。

Create a New Working Environment Cloud Volumes ONTAP Charging Methods & NSS Account

<p>Cloud Volumes ONTAP Charging Methods</p> <p>Learn more about our charging methods</p> <p><input checked="" type="radio"/> Pay-As-You-Go by the hour</p> <p><input type="radio"/> Bring your own license</p>	<p>NetApp Support Site Account (Optional)</p> <p>Learn more about NetApp Support Site (NSS) accounts</p> <p>To register this Cloud Volumes ONTAP to support, you should add NetApp Support Site Account.</p> <p>Don't have a NetApp Support Site account? Select go to finish deploying this system. After its created, use the Support Registration option to create an NSS account.</p>
--	---

[Continue](#)

9. さまざまなタイプのワークロードに使用できる事前設定されたパッケージをいくつか選択できます。

Select a preconfigured Cloud Volumes ONTAP system that best matches your needs, or create your own configuration. Preconfigured settings can be modified at a later time. [Change Configuration](#)

<p></p> <p>POC and small workloads Up to 500GB of storage</p>	<p></p> <p>Database and application data production workloads</p>	<p></p> <p>Cost effective DR Up to 500GB of storage</p>	<p></p> <p>Highest performance production workloads</p>
---	---	---	---

[Continue](#)

10. サポートのアクティブ化と Azure リソースの割り当てに関する 2 つの契約に同意します。 Cloud Volumes ONTAP インスタンスを作成するには、Go をクリックします。

nimavsCVO

Azure | East US 2

- I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp. [More information >](#)
- I understand that Cloud Manager will allocate the appropriate Azure resources to comply with my above requirements. [More information >](#)

Overview

Networking

Storage

Go

11. Cloud Volumes ONTAP のプロビジョニングが完了すると、[Canvas] ページの作業環境に表示されます。

The screenshot shows the 'Canvas' page in NetApp Cloud Manager. The top navigation bar includes 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. The main content area is titled 'Canvas' and features an 'Add Working Environment' section with a cloud icon and the text 'nimavsCVO Cloud Volumes ONTAP' and 'Freemium'. To the right, a sidebar displays the details for the 'nimavsCVO' environment, which is 'On'. The 'DETAILS' section shows 'Cloud Volumes ONTAP | Azure | Single'. The 'SERVICES' section shows 'Replication' and an 'Enter Working Environment' button.

SMB ボリューム用の追加の設定

1. 作業環境の準備ができたなら、CIFS サーバに適切な DNS および Active Directory 設定パラメータが設定されていることを確認します。この手順は、SMB ボリュームを作成する前に実行する必要があります。

The screenshot shows the 'Create a CIFS server' configuration page in the Azure portal for the instance 'nimavsCVO'. The page includes the following fields:

- DNS Primary IP Address:** 172.24.1.5
- Active Directory Domain to join:** nimodemo.com
- DNS Secondary IP Address (Optional):** Example: 127.0.0.1
- Credentials authorized to join the domain:** nimoadmin and a masked password field.

2. SMB ボリュームの作成は簡単なプロセスです。CVO インスタンスを選択してボリュームを作成し、Create Volume（ボリュームの作成）オプションをクリックします。適切なサイズを選択し、包含アグリゲートを選択するか、高度な割り当てメカニズムを使用して特定のアグリゲートに配置します。このデモでは、SMB がプロトコルとして選択されます。

The screenshot shows the 'Volume Details, Protection & Protocol' configuration page for a new volume. The page is divided into two main sections:

- Details & Protection:**
 - Volume Name:** nimavssmbvol1
 - Size (GB):** 50
 - Snapshot Policy:** default
 - Default Policy:** Default Policy
- Protocol:**
 - NFS:** Unselected
 - CIFS:** Selected (indicated by a blue underline)
 - iSCSI:** Unselected
 - Share name:** nimavssmbvol1_share
 - Permissions:** Full Control
 - Users / Groups:** Everyone;

A blue 'Continue' button is located at the bottom of the configuration area.

3. ボリュームのプロビジョニングが完了すると、Volumes（ボリューム）ペインにボリュームが表示されます。CIFS 共有はプロビジョニングされるため、ユーザまたはグループにファイルとフォルダに対する権限を付与し、ユーザが共有にアクセスしてファイルを作成できることを確認してください。ファイル権限とフォルダ権限はすべて SnapMirror レプリケーションの一部として保持されるため、オンプレミス環境からボリュームをレプリケートする場合はこの手順は必要ありません。

Volumes

1 Volume | 50 GB Allocated | 1.74 MB Total Used (1.74 MB in Disk, 0 KB in Blob)


nimavssmbvol1
■ ONLINE

INFO

Disk Type	PREMIUM_LRS
Tiering Policy	Auto
Backup	OFF

CAPACITY

50 GB
 Allocated

■ 1.74 MB
 Disk Used

■ 0 GB
 Blob Used

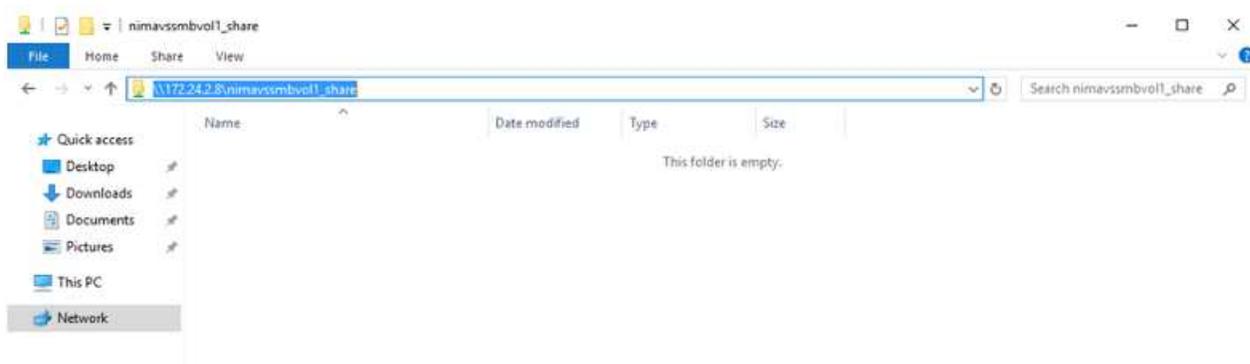
4. ボリュームが作成されたら、 mount コマンドを使用して、 Azure VMware 解決策 SDDC ホストで実行されている VM から共有に接続します。
5. 次のパスをコピーし、 ネットワークドライブのマッピングオプションを使用して、 Azure VMware 解決策 SDDC で実行されている VM にボリュームをマウントします。

Mount Volume nimavssmbvol1

Go to your machine and enter this command

```
\\172.24.2.8\nimavssmbvol1_share
```

 Copy



LUN をホストに接続します

LUN をホストに接続するには、次の手順を実行します。

1. キャンバスページで、Cloud Volumes ONTAP 作業環境をダブルクリックしてボリュームを作成および管理します。
2. Add Volume (ボリュームの追加) > New Volume (新しいボリューム) をクリックし、iSCSI を選択して Create Initiator Group (イニシエータContinue をクリックします)。

The screenshot shows two configuration panels. The 'Details & Protection' panel on the left includes a 'Volume Name' field with 'nimavsscsi1', a 'Size (GB)' field with '500', a 'Snapshot Policy' dropdown set to 'default', and a 'Default Policy' link. The 'Protocol' panel on the right has tabs for 'NFS', 'CIFS', and 'iSCSI' (which is selected). Below the tabs is a 'What about LUNs?' link. Underneath is an 'Initiator Group' section with radio buttons for 'Map Existing Initiator Groups' and 'Create Initiator Group' (which is selected). Below that is an 'Initiator Group' text input field containing 'avsvmlG'. A blue 'Continue' button is centered below the panels.

3. ボリュームのプロビジョニングが完了したら、ボリュームを選択し、ターゲット IQN をクリックします。iSCSI Qualified Name (IQN) をコピーするには、Copy (コピー) をクリックします。ホストから LUN への iSCSI 接続をセットアップします。

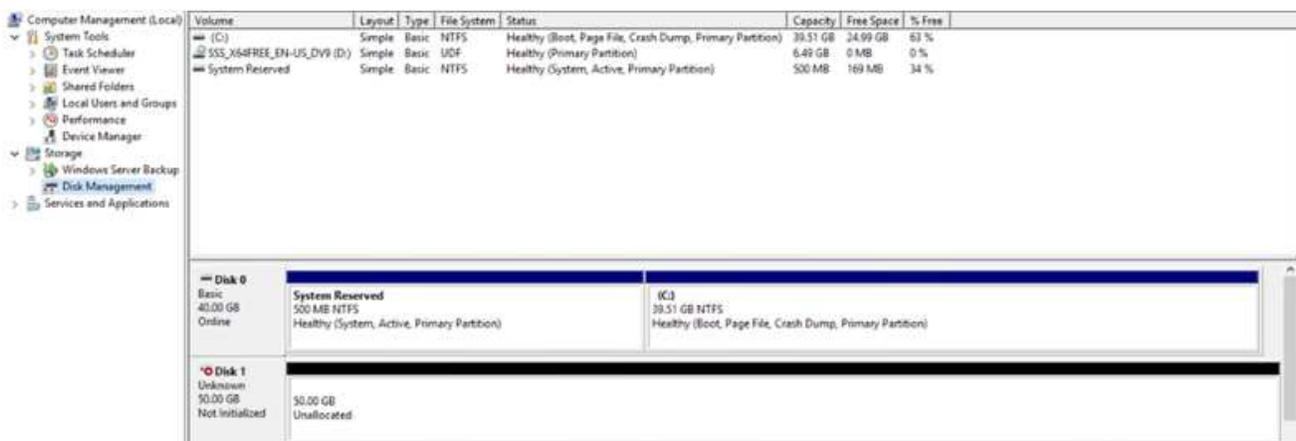
Azure VMware 解決策 SDDC にあるホストでも同じ処理を実行するには、次の手順を実行します。

- a. Azure VMware 解決策 SDDC にホストされている VM への RDP
- b. [iSCSI イニシエータのプロパティ] ダイアログ・ボックスを開きます [サーバーマネージャ] > [ダッシュボード] > [ツール] > [iSCSI イニシエータ]
- c. Discovery (検出) タブで、Discover Portal (ポータルを検出) または Add Portal (ポータルの追加) をクリックし、iSCSI ターゲットポートの IP アドレスを入力します。
- d. ターゲットタブで検出されたターゲットを選択し、ログオンまたは接続をクリックします。
- e. [マルチパスを有効にする] を選択し、コンピュータの起動時に [この接続を自動的に復元する] または [この接続をお気に入りターゲットのリストに追加する] を選択します。Advanced (詳細設定) をクリック
 - 注： * Windows ホストからクラスタ内の各ノードへの iSCSI 接続が確立されている必要があります。ネイティブ DSM では、使用する最適なパスが選択されます。



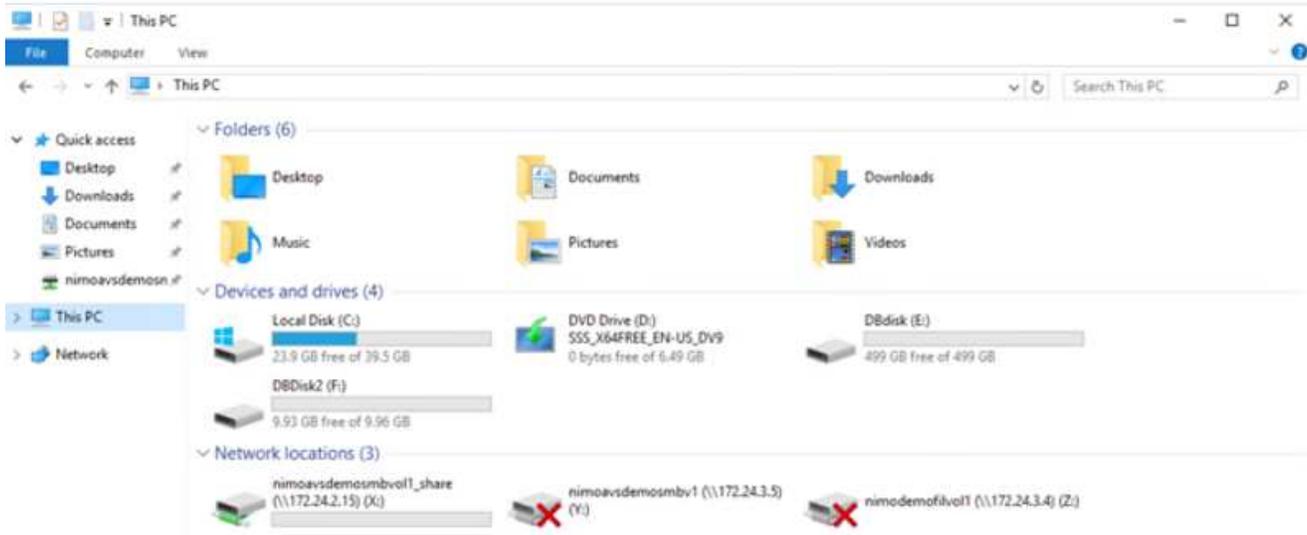
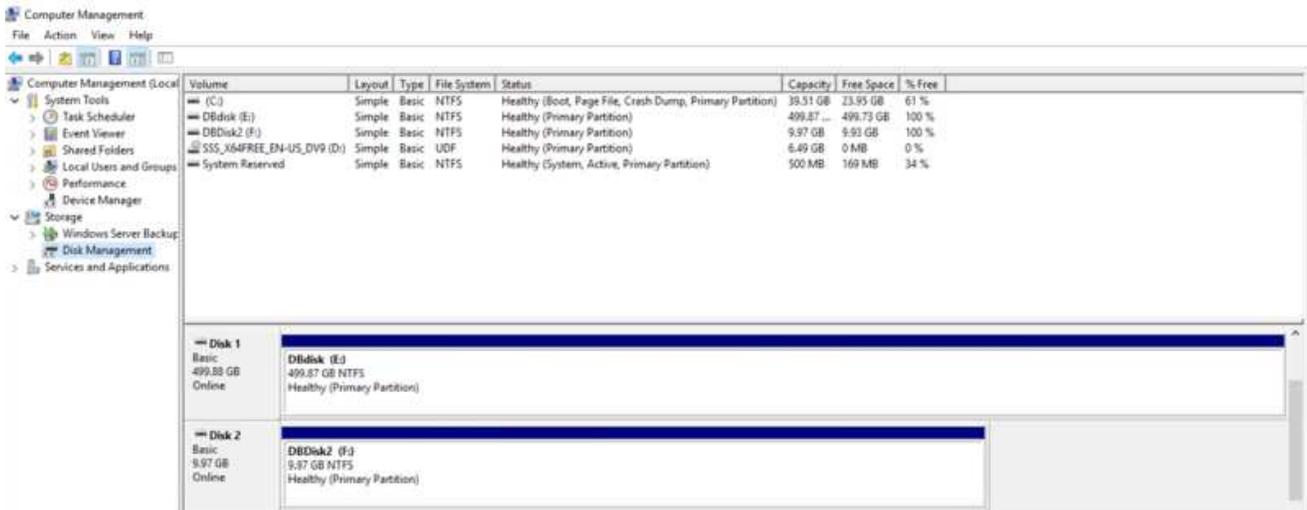
Storage Virtual Machine（SVM）の LUN は、Windows ホストではディスクとして表示されます。追加した新しいディスクは、ホストでは自動的に検出されません。手動の再スキャンをトリガーしてディスクを検出するには、次の手順を実行します。

1. Windows コンピュータの管理ユーティリティを開きます。[スタート]>[管理ツール]>[コンピュータの管理]を選択します。
2. ナビゲーションツリーでストレージノードを展開します。
3. [ディスクの管理]をクリックします
4. [アクション] > [ディスクの再スキャン] の順にクリック



Windows ホストから初めてアクセスした時点では、新しい LUN にはパーティションやファイルシステムは設定されていません。LUN を初期化します。必要に応じて、次の手順を実行してファイルシステムで LUN をフォーマットします。

1. Windows ディスク管理を開始します。
2. LUN を右クリックし、必要なディスクまたはパーティションのタイプを選択します。
3. ウィザードの指示に従います。この例では、ドライブ E : がマウントされています



Google Cloud VMware Engine NetApp Cloud Volume Serviceを使用したNFSデータストアの補完

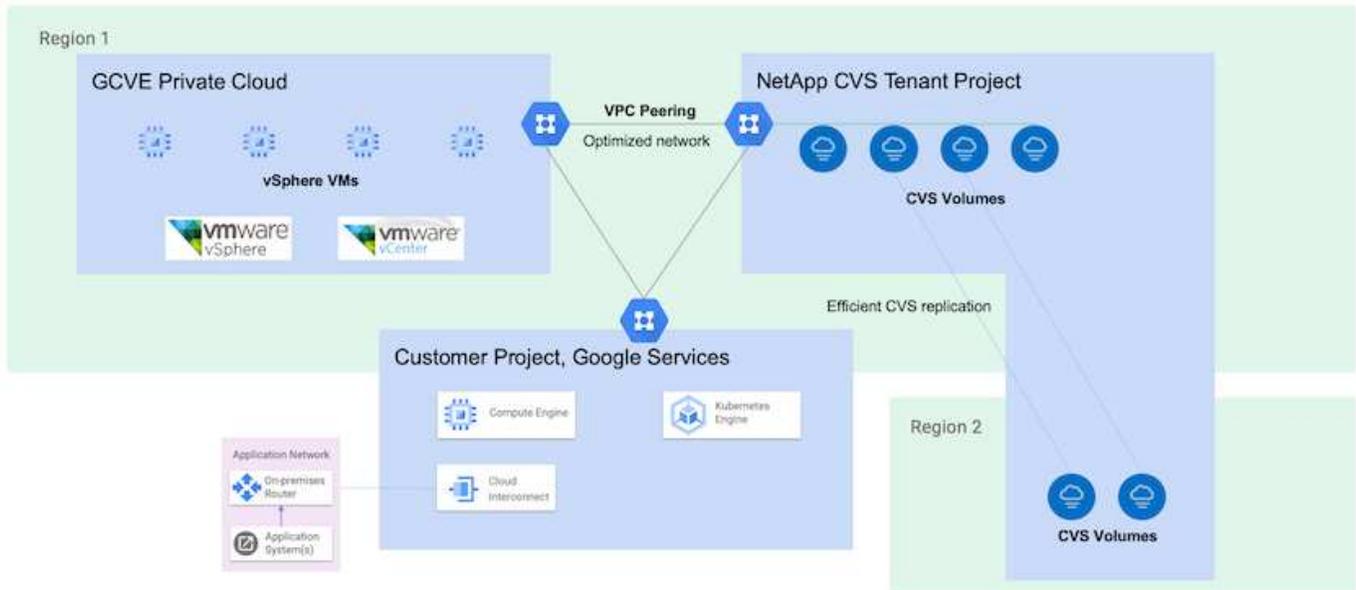
お客様は、NetApp Cloud Volume ServiceでNFSの補完的なデータストアを使用し、Google Cloud VMware Engineのストレージ容量を拡張できます。

概要

執筆者：ネットアップSuresh Thoppay

Google Cloud VMware Engine (GCVE) 環境で追加のストレージ容量が必要な場合は、NetApp Cloud Volume Serviceを使用して補完的なNFSデータストアとしてマウントできます。NetAppクラウドボリュームサービスにデータを格納することで、リージョン間でレプリケートして災害から

データを保護できます。



NetApp CVSからGCVEにNFSデータストアをマウントする導入手順

CVS-Performanceボリュームをプロビジョニングします

NetAppクラウドボリュームサービスボリュームは、からプロビジョニングできます
"Google Cloud Consoleを使用"
"NetApp BlueXPポータルまたはAPIを使用"

そのCVSボリュームを削除不可としてマークします

VMの実行中に誤ってボリュームが削除されないように、下のスクリーンショットに示すように、ボリュームが削除不可とマークされていることを確認してください。

The screenshot shows the 'Edit File System' configuration page. On the left is a navigation menu with 'Volumes' selected. The main content area shows 'Extreme' performance tier and 'Volume Details'. The 'Allocated Capacity' is set to 1024 GiB. The 'Protocol Type' is set to NFSv3. A red box highlights the checkbox 'Block volume from deletion when clients are connected', which is checked. Below this is the 'Export Policy' section.

詳細については、"[NFSボリュームを作成しています](#)"ドキュメントを参照してください。

NetApp CVSテナントVPC用のGCVE上のプライベート接続が存在することを確認します。

NFSデータストアをマウントするには、GCVEとNetApp CVSプロジェクトの間にプライベート接続が確立されている必要があります。

詳細については、[を参照してください "プライベートサービスアクセスのセットアップ方法"](#)

NFSデータストアをマウント

GCVEにNFSデータストアをマウントする方法については、を参照してください "[NetApp CVSを使用してNFSデータストアを作成する方法](#)"



vSphereホストはGoogleで管理されるため、NFS vSphere API for Array Integration (VAAI) vSphere Installation Bundle (VIB) をインストールすることはできません。仮想ボリューム (VVol) のサポートが必要な場合は、ぜひお知らせください。ジャンボフレームを使用する場合は、を参照してください "[GCPでサポートされる最大MTUサイズ](#)"

NetAppクラウドボリュームサービスによるコスト削減

NetAppクラウドボリュームサービスでGCVEへのストレージ需要を削減できる可能性の詳細については、を参照してください "[NetApp ROI計算ツール](#)"

参照リンク

- "[Googleブログ- Google Cloud VMware EngineのデータストアとしてNetApp CVSを使用する方法](#)"
- "[NetAppブログ-ストレージを大量に消費するアプリケーションをGoogle Cloudに移行するためのより良い方法](#)"

GCP のネットアップストレージオプション

GCPは、Cloud Volumes ONTAP (CVO) またはCloud Volumes Service (CVS) でゲスト接続のネットアップストレージをサポートします。

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP (CVO) は、ネットアップのONTAP ストレージソフトウェアを基盤に構築された、業界をリードするクラウドデータ管理解決策です。Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP) でネイティブに利用できます。

ソフトウェアで定義されるONTAP バージョンで、クラウドネイティブなストレージを消費し、クラウドとオンプレミスで同じストレージソフトウェアを使用できるため、まったく新しい方法でIT担当者のデータ管理を再トレーニングする必要がありません。

CVOを使用すれば、エッジ、データセンター、クラウド間でシームレスにデータを移動し、ハイブリッドクラウドを統合できます。すべてを1画面の管理コンソールであるNetApp Cloud Managerで管理できます。

設計上、CVOは卓越したパフォーマンスと高度なデータ管理機能を備えており、クラウドで最も要件の厳しいアプリケーションにも対応できます

Cloud Volumes ONTAP (CVO) をゲスト接続ストレージとして活用

Cloud Volumes ONTAP を Google Cloud に導入（自分で導入）

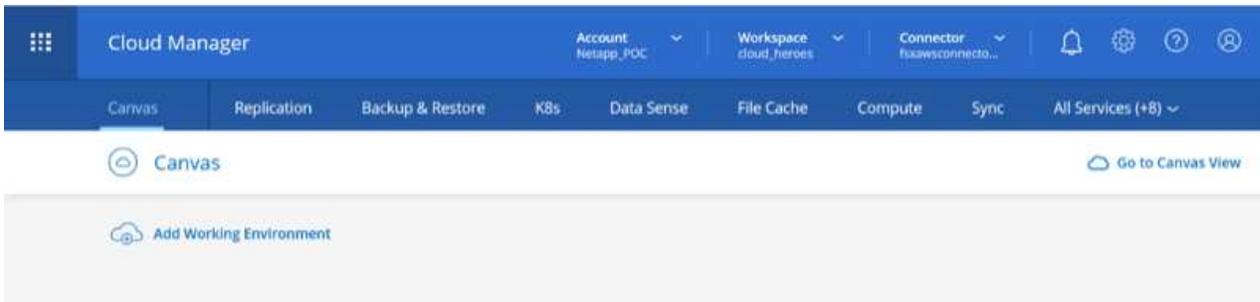
Cloud Volumes ONTAP 共有と LUN は、GCVE プライベートクラウド環境で作成された VM からマウントできます。Cloud Volumes ONTAP は iSCSI、SMB、NFS の各プロトコルをサポートしているため、iSCSI 経由でマウントしたボリュームを Linux クライアントや Windows クライアントにマウントし、LUN に Linux クライアントや Windows クライアントからブロックデバイスとしてアクセスすることもできます。Cloud Volumes ONTAP ボリュームは、いくつかの簡単な手順で設定できます。

ディザスタリカバリや移行の目的でオンプレミス環境からクラウドにボリュームをレプリケートするには、サイト間 VPN または Cloud Interconnect を使用して Google Cloud へのネットワーク接続を確立します。オンプレミスから Cloud Volumes ONTAP へのデータのレプリケートについては、本ドキュメントでは扱いません。オンプレミスシステムと Cloud Volumes ONTAP システム間でデータをレプリケートする方法については、を参照してください [xref:./ehc/"システム間のデータレプリケーションの設定"](#)。

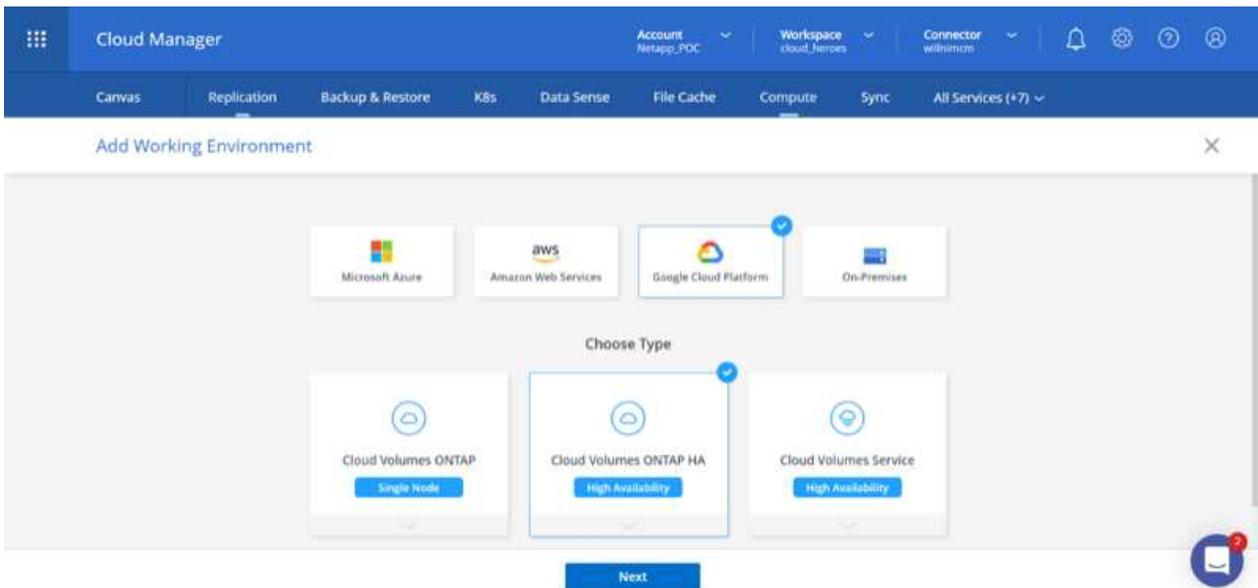


使用 "[Cloud Volumes ONTAP サイジングツール](#)" Cloud Volumes ONTAP インスタンスのサイズを正確に設定します。また、オンプレミスのパフォーマンスを監視し、Cloud Volumes ONTAP のサイジングツールの情報として使用できます。

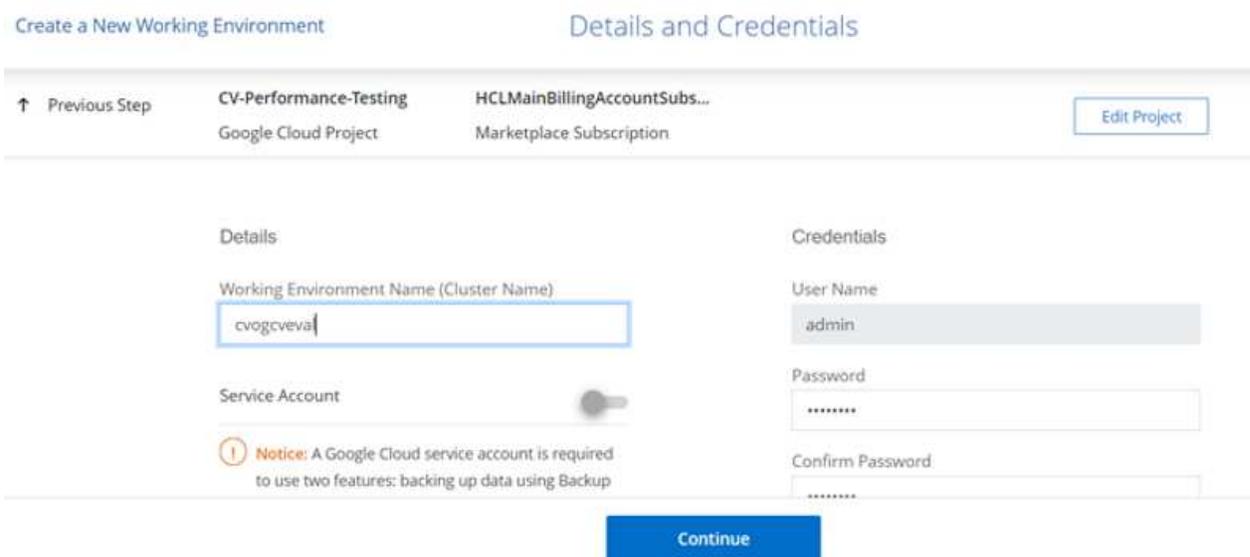
1. NetApp Cloud Central にログイン—Fabric View（ファブリックビュー）画面が表示されます。Cloud Volumes ONTAP タブを探し、Go to Cloud Manager を選択します。ログインすると、キャンバス画面が表示されます。



2. Cloud Manager Canvas タブで、Add a Working Environment をクリックし、クラウドとして Google Cloud Platform を選択し、システム構成のタイプを選択します。次に、[次へ] をクリックします。



3. 環境名と admin クレデンシャルなど、作成する環境の詳細を指定します。完了したら、[続行] をクリックします。



4. データセンスとコンプライアンス、クラウドへのバックアップなど、Cloud Volumes ONTAP 導入用のアドオンサービスを選択または選択解除します。次に、[続行] をクリックします。

ヒント：アドオンサービスを無効にすると、確認のポップアップメッセージが表示されます。CVO の導入後にアドオンサービスを追加 / 削除できます。コストを回避するために、不要なサービスは最初から選択解除することを検討してください。

↑ Previous Step



Data Sense & Compliance



Backup to Cloud



WARNING:By turning off Backup to Cloud, future data recovery will not be possible in case of data corruption or loss

[Continue](#)

- 場所を選択し、ファイアウォールポリシーを選択し、チェックボックスを選択して Google Cloud ストレージへのネットワーク接続を確認します。

↑ Previous Step

Location

GCP Region

europe-west3



GCP Zone

europe-west3-c



I have verified connectivity between the target VPC and Google Cloud storage.

Connectivity

VPC

cloud-volumes-vpc



Subnet

10.0.6.0/24



Firewall Policy

 Generated firewall policy Use existing firewall policy[Continue](#)

- ライセンスオプションとして、「従量課金制」または「BYOL for using existing license」を選択します。この例では、Freemium オプションが使用されています。次に、[続行] をクリックします。

↑ Previous Step Cloud Volumes ONTAP Charging Methods

[Learn more about our charging methods](#)

- Pay-As-You-Go by the hour
- Bring your own license
- Freemium (Up to 500GB)

NetApp Support Site Account

[Learn more about NetApp Support Site \(NSS\) accounts](#)

NetApp Support Site Account

mchad

To add a new NetApp Support Site account, go to the Support - NSS Management tab.

Continue

7. AWS SDDC 上の VMware クラウドで実行されている VM に導入されるワークロードのタイプに基づいて、複数の事前設定パッケージから選択できます。

ヒント：タイルの上にマウスを移動して詳細を表示したり、[構成の変更]をクリックして CVO コンポーネントと ONTAP バージョンをカスタマイズしたりできます。

Create a New Working Environment Preconfigured Packages

Select a preconfigured Cloud Volumes ONTAP system that best matches your needs, or create your own configuration. Preconfigured settings can be modified at a later time. [Change Configuration](#)

- POC and small workloads**
Up to 500GB of storage
- Database and application data production workloads**
- Cost effective DR**
Up to 500GB of storage
- Highest performance production workloads**

Continue

8. [確認と承認] ページで、選択内容を確認して確定します。Cloud Volumes ONTAP インスタンスを作成するには、[移動]をクリックします。

Create a New Working Environment Review & Approve

↑ Previous Step cvogcveval [Show API request](#)

GCP | europe-west3

This Cloud Volumes ONTAP instance will be registered with NetApp support under the NSS Account mchad.

I understand that Cloud Manager will allocate the appropriate GCP resources to comply with my above requirements. [More information >](#)

Overview Networking Storage

Storage System:	Cloud Volumes ONTAP	Cloud Volumes ONTAP runs on:	n2-standard-4
License Type:	Cloud Volumes ONTAP Freemium	Encryption:	Google Cloud Managed
Capacity Limit:	500GB	Write Speed:	Normal

Go

9. Cloud Volumes ONTAP のプロビジョニングが完了すると、[Canvas] ページの作業環境に表示されます。

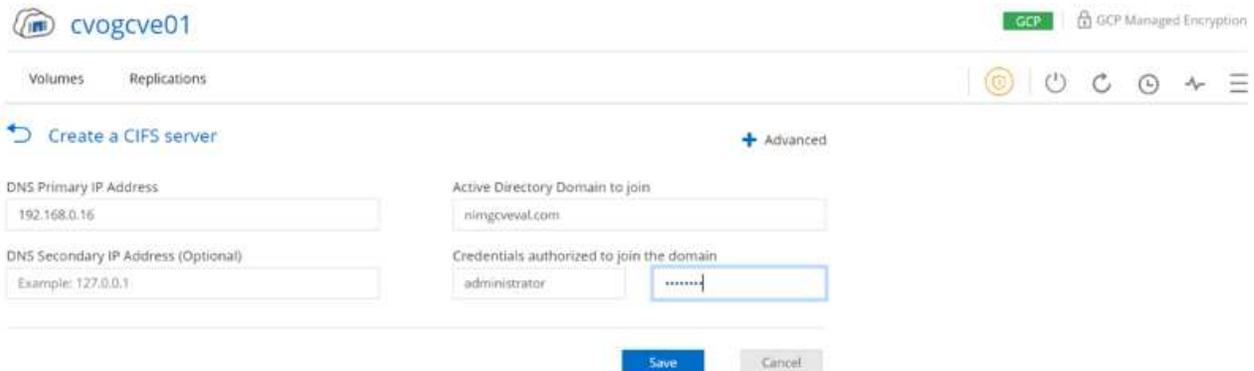
The screenshot displays the NetApp Cloud Manager interface. At the top, the navigation bar includes 'Cloud Manager' and various service tabs: Canvas, Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+7). The 'Canvas' tab is active, showing an 'Add Working Environment' button and two environment cards. The first card, 'cvogve01 Cloud Volumes ONTAP', is labeled 'Freeium'. The second card, 'DatacenterDude Azure NetApp Files', shows '31 Volumes' and '9.71 TiB Capacity'. On the right, a 'Working Environments' list shows three items: '1 Cloud Volumes ONTAP' with '43.05 GiB Provisioned Capacity', '1 FSx for ONTAP (High-Availability)' with '0B Provisioned Capacity', and '1 Azure NetApp Files' with '9.71 TiB Provisioned Capacity'.

Environment Name	Provisioned Capacity
1 Cloud Volumes ONTAP	43.05 GiB
1 FSx for ONTAP (High-Availability)	0B
1 Azure NetApp Files	9.71 TiB

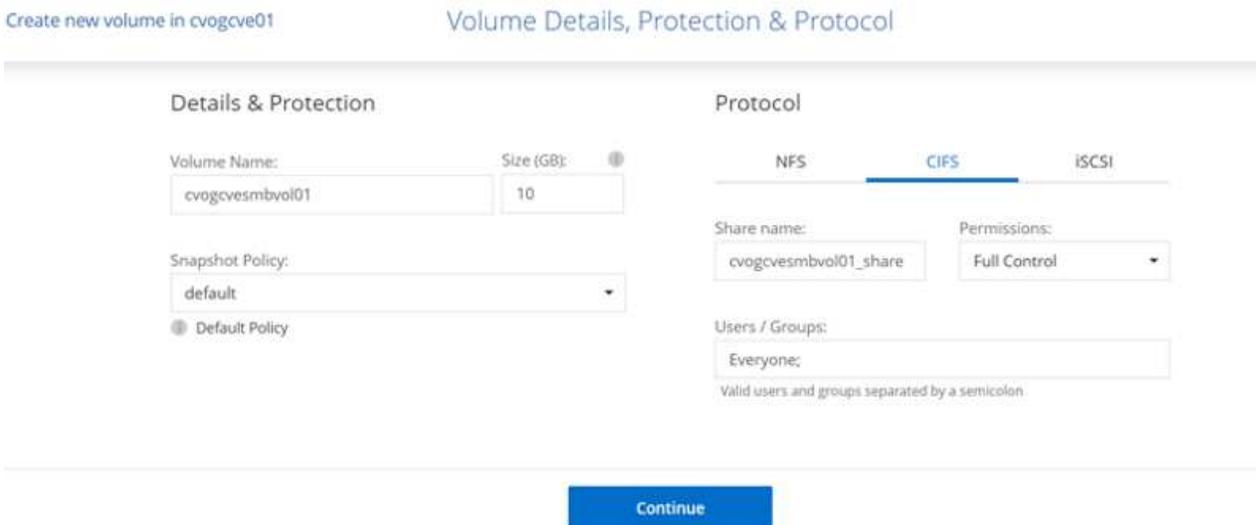
SMB ボリューム用の追加の設定

1. 作業環境の準備ができれば、CIFS サーバに適切な DNS および Active Directory 設定パラメータが設定されていることを確認します。この手順は、SMB ボリュームを作成する前に実行する必要があります。

ヒント：メニューアイコン（°）をクリックし、詳細設定を選択してオプションを表示し、CIFS のセットアップを選択します。



2. SMB ボリュームの作成は簡単なプロセスです。キャンバスで、Cloud Volumes ONTAP 作業環境をダブルクリックしてボリュームを作成および管理し、ボリュームの作成オプションをクリックします。適切なサイズを選択し、包含アグリゲートを選択するか、高度な割り当てメカニズムを使用して特定のアグリゲートに配置します。このデモでは、プロトコルとして CIFS/SMB が選択されます。



3. ボリュームのプロビジョニングが完了すると、Volumes（ボリューム）ペインにボリュームが表示されます。CIFS 共有はプロビジョニングされるため、ユーザまたはグループにファイルとフォルダに対する権限を付与し、ユーザが共有にアクセスしてファイルを作成できることを確認してください。ファイル権限とフォルダ権限はすべて SnapMirror レプリケーションの一部として保持されるため、オンプレミス環境からボリュームをレプリケートする場合はこの手順は必要ありません。

ヒント：ボリュームメニュー（°）をクリックすると、そのオプションが表示されます。

cvogcvesmbvol01 ONLINE

INFO

Disk Type	PD-SSD
Tiering Policy	None

CAPACITY

10 GB Allocated

1.84 MB Disk Used

4. ボリュームが作成されたら、mount コマンドを使用してボリュームの接続手順を表示し、Google Cloud VMware Engine 上の VM から共有に接続します。

cvogcve01

Volumes Replications

Mount Volume cvogcvesmbvol01

Go to your machine and enter this command

```
\\10.0.6.251\cvogcvesmbvol01_share
```

Copy

5. 次のパスをコピーし、Map Network Drive オプションを使用して、Google Cloud VMware Engine で実行されている VM にボリュームをマウントします。

Specify the drive letter for the connection and the folder that you want to connect to:

Drive:

Folder:

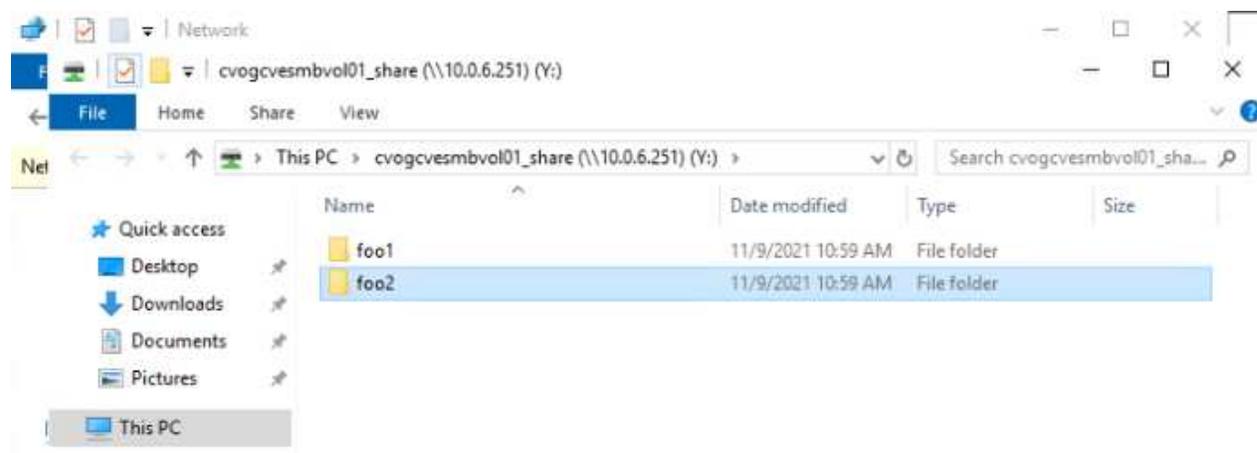
Example: \\server\share

Reconnect at sign-in

Connect using different credentials

[Connect to a Web site that you can use to store your documents and pictures.](#)

マッピングが完了すると、このマッピングに簡単にアクセスでき、NTFS アクセス権を適切に設定できます。



Cloud Volumes ONTAP 上の LUN をホストに接続します

Cloud Volumes ONTAP LUN をホストに接続するには、次の手順を実行します。

1. キャンバスページで、Cloud Volumes ONTAP 作業環境をダブルクリックしてボリュームを作成および管理します。
2. Add Volume (ボリュームの追加) > New Volume (新しいボリューム) をクリックし、iSCSI を選択して Create Initiator Group (イニシエータContinue をクリックします)。

Create new volume in cvogcve01

Volume Details, Protection & Protocol

Details & Protection

Volume Name: cvogcvescilun01

Size (GB): 10

Snapshot Policy: default

Default Policy

Protocol

NFS CIFS **iSCSI**

What about LUNs?

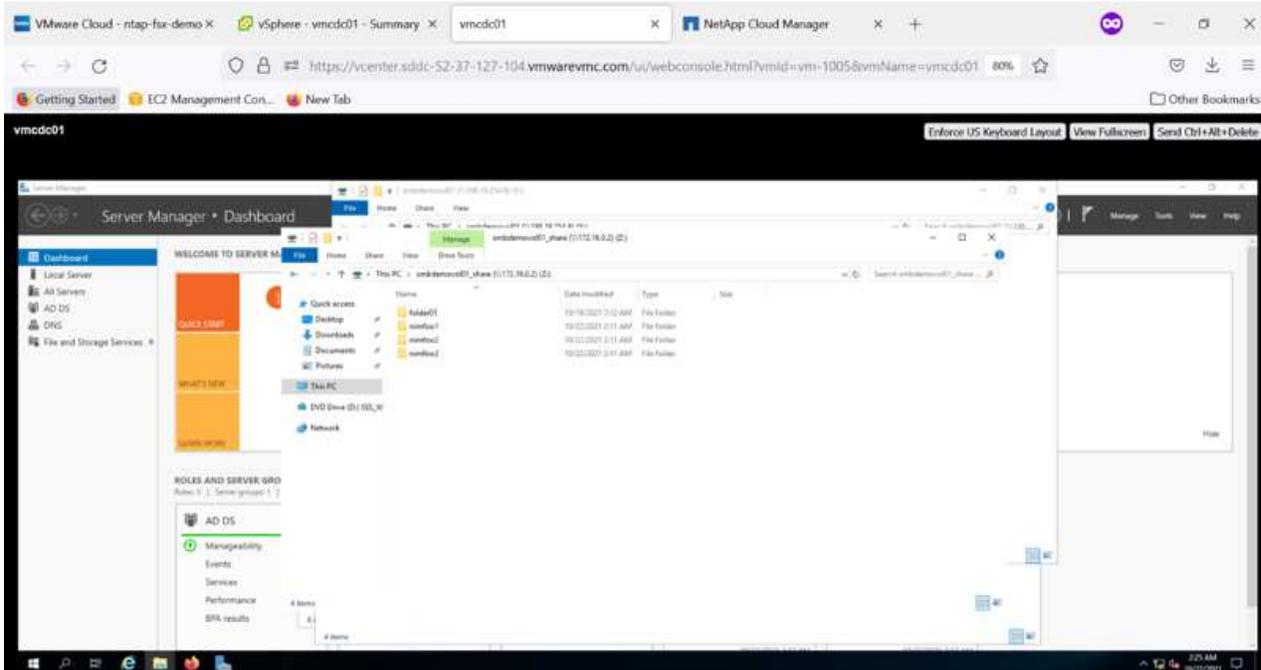
Initiator Group

Map Existing Initiator Groups Create Initiator Group

Initiator Group: WiniG

Operating System Type: Windows

Continue



3. ボリュームのプロビジョニングが完了したら、ボリュームメニュー (°) を選択し、ターゲット IQN をクリックします。iSCSI Qualified Name (IQN) をコピーするには、Copy (コピー) をクリックします。ホストから LUN への iSCSI 接続をセットアップします。

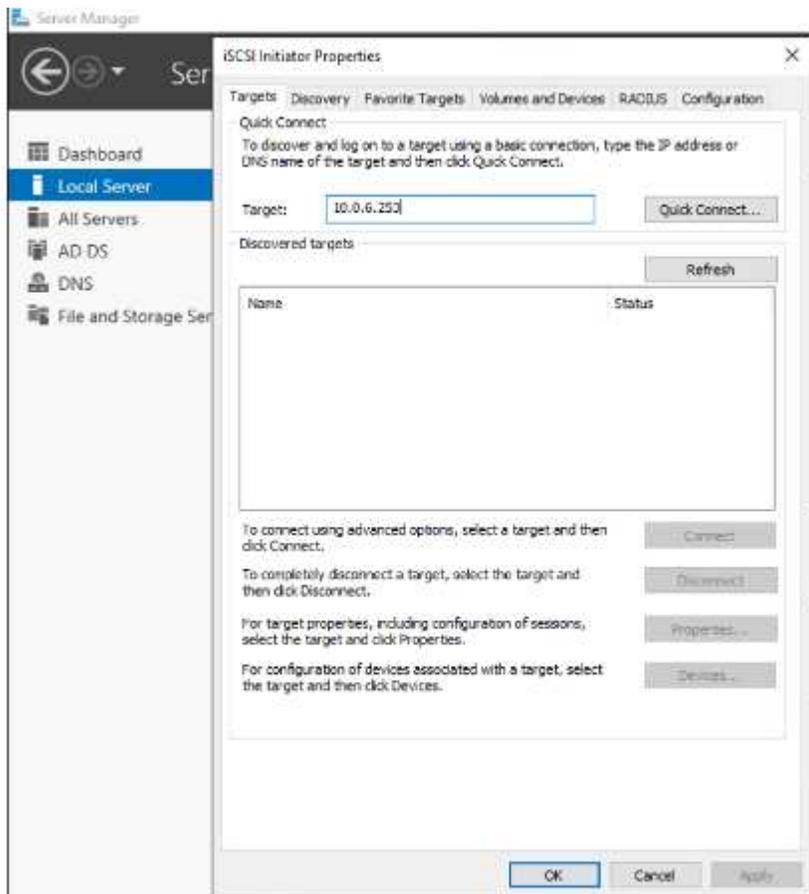
Google Cloud VMware Engine 上のホストで同じ処理を実行するには、次の手順を実行します。

1. Google Cloud VMware Engine でホストされている VM への RDP

2. [iSCSI イニシエータのプロパティ] ダイアログ・ボックスを開きます [サーバーマネージャ] > [ダッシュボード] > [ツール] > [iSCSI イニシエータ]
3. Discovery (検出) タブで、Discover Portal (ポータルを検出) または Add Portal (ポータルの追加) をクリックし、iSCSI ターゲットポートの IP アドレスを入力します。
4. ターゲットタブで検出されたターゲットを選択し、ログオンまたは接続をクリックします。
5. [マルチパスを有効にする] を選択し、コンピュータの起動時に [この接続を自動的に復元する] または [この接続をお気に入りターゲットのリストに追加する] を選択します。Advanced (詳細設定) をクリック

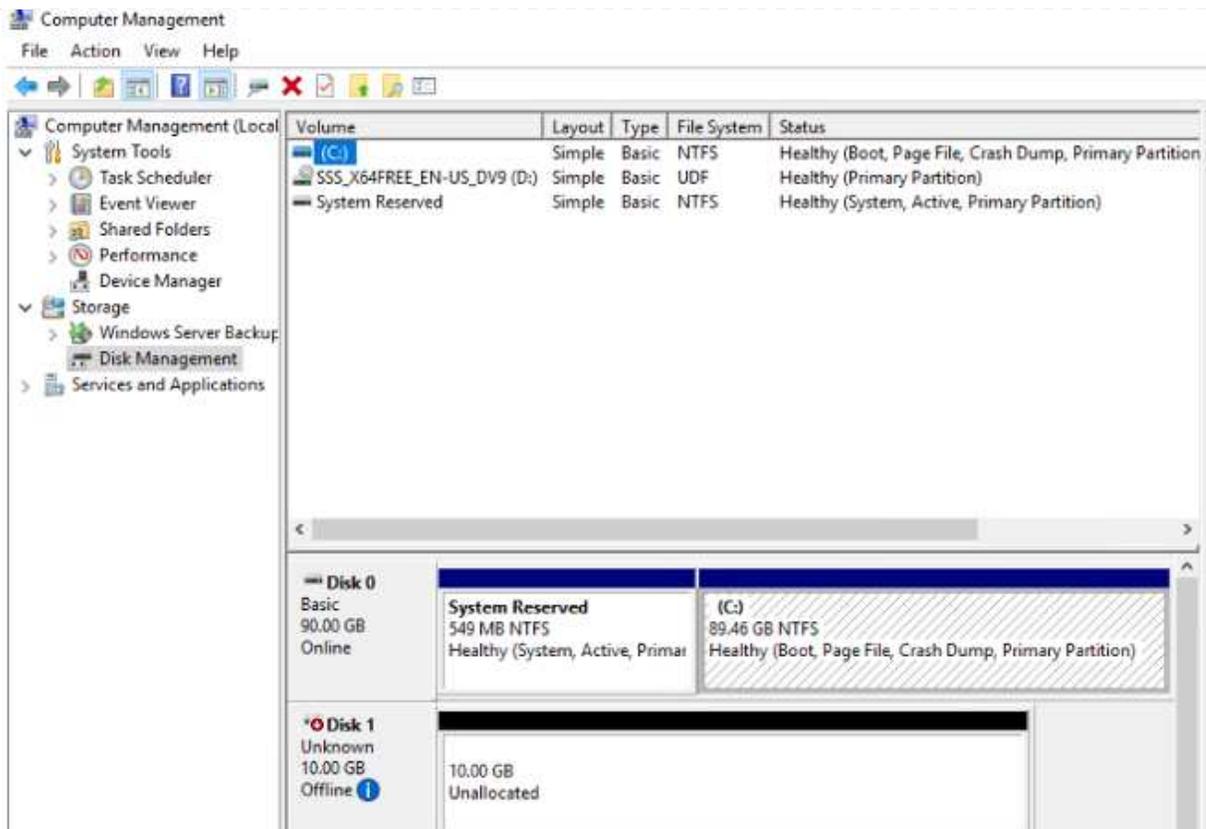


Windows ホストには、クラスタ内の各ノードへの iSCSI 接続が必要です。ネイティブ DSM では、使用する最適なパスが選択されます。



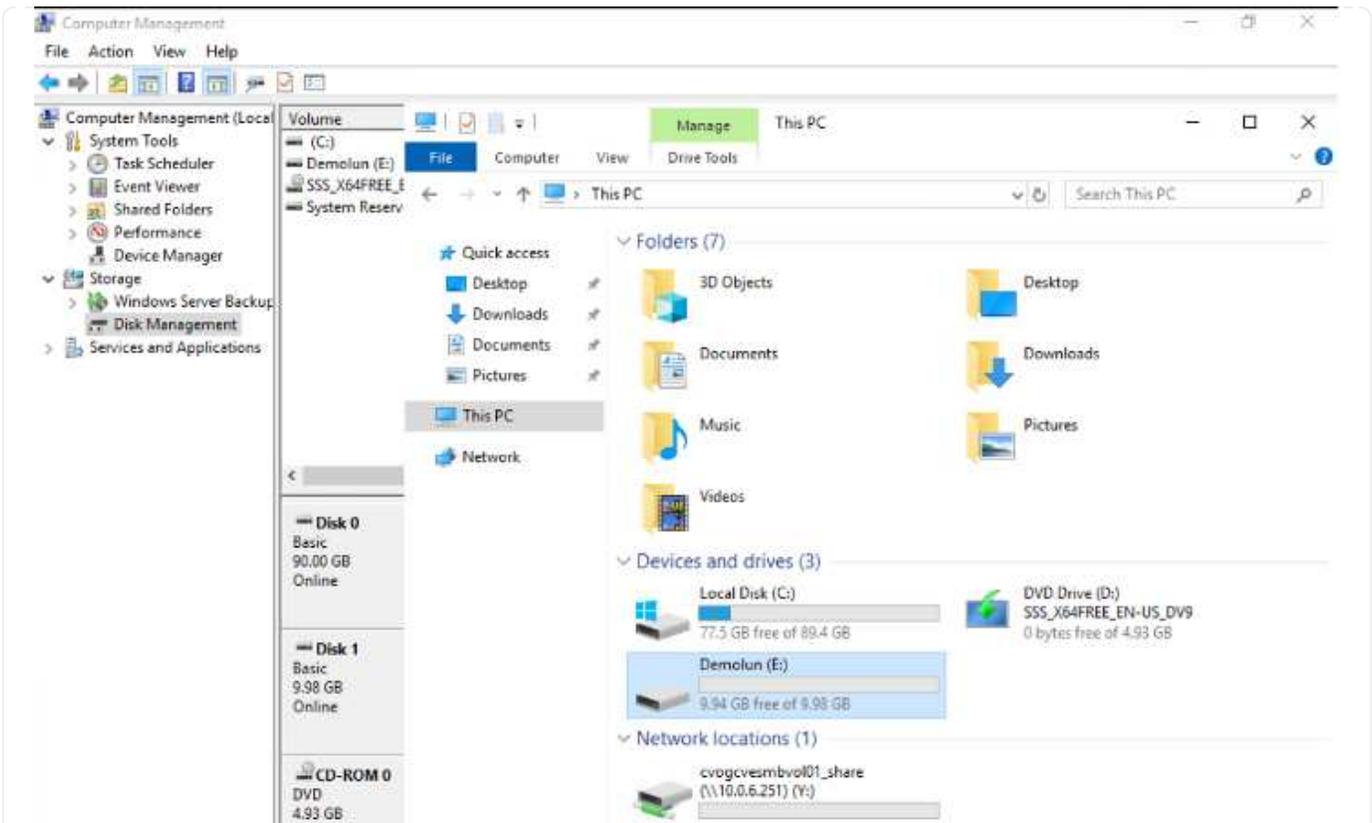
Storage Virtual Machine (SVM) の LUN は、Windows ホストではディスクとして表示されます。追加した新しいディスクは、ホストでは自動的に検出されません。手動の再スキャンをトリガーしてディスクを検出するには、次の手順を実行します。

- a. Windows コンピュータの管理ユーティリティを開きます。[スタート]>[管理ツール]>[コンピュータの管理] を選択します。
- b. ナビゲーションツリーでストレージノードを展開します。
- c. [ディスクの管理] をクリックします
- d. [アクション] > [ディスクの再スキャン] の順にクリック



Windows ホストから初めてアクセスした時点では、新しい LUN にはパーティションやファイルシステムは設定されていません。LUN を初期化します。必要に応じて、次の手順を実行してファイルシステムで LUN をフォーマットします。

- a. Windows ディスク管理を開始します。
- b. LUN を右クリックし、必要なディスクまたはパーティションのタイプを選択します。
- c. ウィザードの指示に従います。この例では、ドライブ F : がマウントされています。



Linux クライアントで、iSCSI デーモンが実行されていることを確認します。LUN のプロビジョニングが完了したら、以下の例として Ubuntu を使用した iSCSI 構成に関する詳細なガイダンスを参照してください。これを確認するには、シェルから `lsblk` cmd を実行します。

```
nlyaz@nlnubuds:~$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
loop0 7:0 0 55.4M 1 loop /snap/core18/2128
loop1 7:1 0 219M 1 loop /snap/gnome-3-34-1804/72
loop2 7:2 0 65.1M 1 loop /snap/gtk-common-themes/1515
loop3 7:3 0 51M 1 loop /snap/snap-store/547
loop4 7:4 0 32.3M 1 loop /snap/snapd/12704
loop5 7:5 0 32.5M 1 loop /snap/snapd/13640
loop6 7:6 0 55.5M 1 loop /snap/core18/2246
loop7 7:7 0 4K 1 loop /snap/bare/5
loop8 7:8 0 65.2M 1 loop /snap/gtk-common-themes/1519
sda 8:0 0 16G 0 disk
├─sda1 8:1 0 512M 0 part /boot/efl
├─sda2 8:2 0 1K 0 part
├─sda5 8:5 0 15.5G 0 part /
└─sdb 8:16 0 1G 0 disk
```

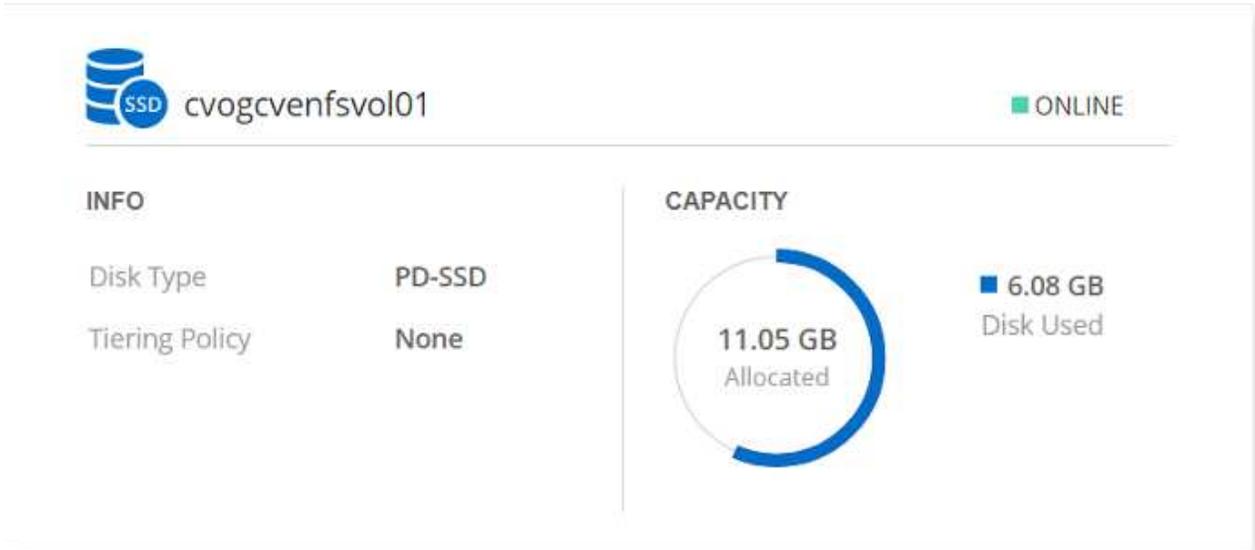
```
niyaz@nimubu01:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G   0 1.9G   0% /dev
tmpfs           394M  1.5M 392M   1% /run
/dev/sda5       16G   7.6G 6.9G  53% /
tmpfs           2.0G   0 2.0G   0% /dev/shm
tmpfs           5.0M   0 5.0M   0% /run/lock
tmpfs           2.0G   0 2.0G   0% /sys/fs/cgroup
/dev/loop1      219M  219M   0 100% /snap/gnome-3-34-1804/72
/dev/loop2       66M   66M   0 100% /snap/gtk-common-themes/1515
/dev/loop3       51M   51M   0 100% /snap/snap-store/547
/dev/loop0       56M   56M   0 100% /snap/core18/2128
/dev/loop4       33M   33M   0 100% /snap/snapd/12704
/dev/sda1       511M  4.0K 511M   1% /boot/efi
tmpfs           394M   64K 394M   1% /run/user/1000
/dev/loop5       33M   33M   0 100% /snap/snapd/13640
/dev/loop6       56M   56M   0 100% /snap/core18/2246
/dev/loop7      128K  128K   0 100% /snap/bare/5
/dev/loop8       66M   66M   0 100% /snap/gtk-common-themes/1519
/dev/sdb        976M  2.6M 907M   1% /mnt
```

Cloud Volumes ONTAP NFS ボリュームを Linux クライアントにマウント

Cloud Volumes ONTAP (DIY) ファイルシステムを Google Cloud VMware Engine 内の VM からマウントするには、次の手順に従います。

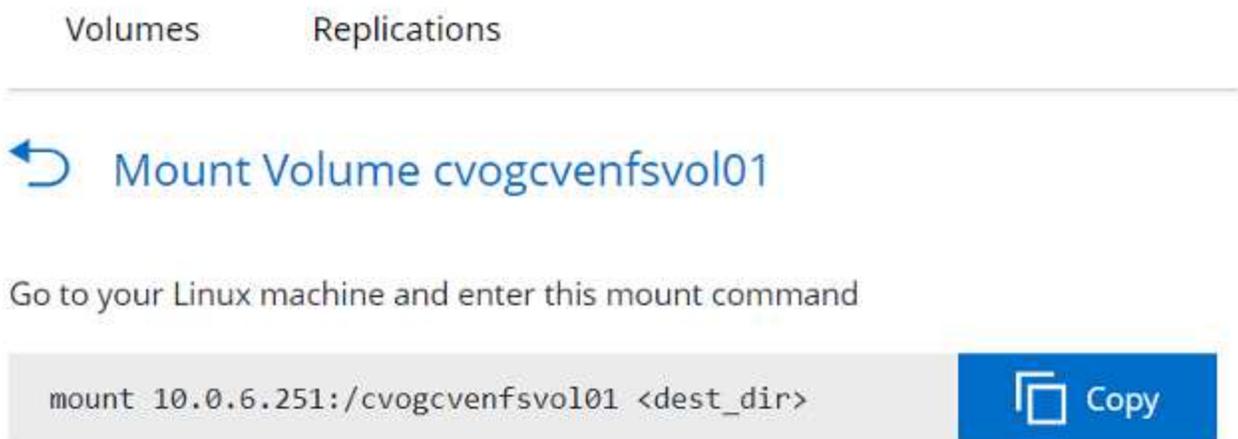
以下の手順に従ってボリュームをプロビジョニングします

1. Volumes (ボリューム) タブで、Create New Volume (新規ボリュームの作成) をクリックします。
2. [Create New Volume] ページで、ボリュームタイプを選択します。



The screenshot displays the details for a volume named 'cvogcvenfsvol01'. It features a blue 'SSD' icon and a green 'ONLINE' status indicator. The 'INFO' section lists 'Disk Type' as 'PD-SSD' and 'Tiering Policy' as 'None'. The 'CAPACITY' section shows a donut chart with '11.05 GB Allocated' and '6.08 GB Disk Used'.

3. ボリュームタブで、ボリューム上にマウスカーソルを置き、メニューアイコン (°) を選択してから、マウントコマンドをクリックします。



The screenshot shows the 'Mount Volume cvogcvenfsvol01' dialog box. It has tabs for 'Volumes' and 'Replications'. Below the title, it says 'Go to your Linux machine and enter this mount command'. A code block contains the command: `mount 10.0.6.251:/cvogcvenfsvol01 <dest_dir>`. To the right of the code block is a blue button with a copy icon and the text 'Copy'.

4. [コピー] をクリックします。
5. 指定された Linux インスタンスに接続します。
6. Secure Shell (SSH) を使用してインスタンスの端末を開き、適切なクレデンシャルでログインします。

7. 次のコマンドを使用して、ボリュームのマウントポイント用のディレクトリを作成します。

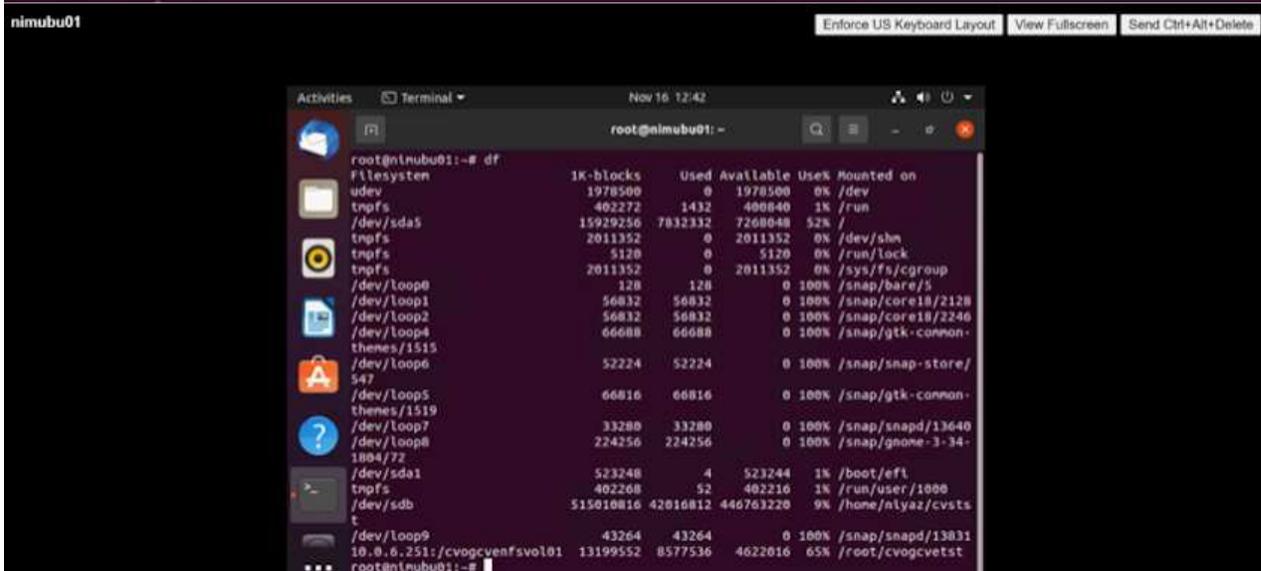
```
$ sudo mkdir /cvogcvetst
```

```
root@nimubu01:~# sudo mkdir cvogcvetst
```

8. 前の手順で作成したディレクトリに Cloud Volumes ONTAP NFS ボリュームをマウントします。

```
sudo mount 10.0.6.251:/cvogcvenfsvol01 /cvogcvetst
```

```
root@nimubu01:~# sudo mount -t nfs 10.0.6.251:/cvogcvenfsvol01 cvogcvetst
```



Filesystem	1K-blocks	Used	Available	Use%	Mounted on
filessystem	1978500	0	1978500	0%	/dev
tmpfs	402272	1432	400840	1%	/run
/dev/sda5	15929256	7832332	7200488	52%	/
tmpfs	2011352	0	2011352	0%	/dev/shm
tmpfs	5120	0	5120	0%	/run/lock
tmpfs	2011352	0	2011352	0%	/sys/fs/cgroup
/dev/loop0	128	128	0	100%	/snap/bare/5
/dev/loop1	56832	56832	0	100%	/snap/core18/2128
/dev/loop2	56832	56832	0	100%	/snap/core18/2246
/dev/loop4	66688	66688	0	100%	/snap/gtk-common-
themes/1515					
/dev/loop6	52224	52224	0	100%	/snap/snap-store/
547					
/dev/loop5	66816	66816	0	100%	/snap/gtk-common-
themes/1519					
/dev/loop7	33280	33280	0	100%	/snap/snapd/13640
/dev/loop8	224256	224256	0	100%	/snap/gnome-3-34-
1804/72					
/dev/sda1	523248	4	523244	1%	/boot/efi
tmpfs	402268	52	402216	1%	/run/user/1000
/dev/sdb	515010816	42016812	446763220	9%	/home/nlyaz/cvsts
t					
/dev/loop9	43264	43264	0	100%	/snap/snapd/13831
10.0.6.251:/cvogcvenfsvol01	13199552	8577536	4622016	65%	/root/cvogcvetst

Cloud Volumes Service (CVS)

Cloud Volume サービス (CVS) は、高度なクラウドソリューションを提供するための包括的なデータサービスポートフォリオです。Cloud Volume サービスは、主要なクラウドプロバイダ向けに複数のファイルアクセスプロトコルをサポートしています (NFSとSMBのサポート)。

その他のメリットと機能としては、Snapshotによるデータ保護とリストア、オンプレミスとクラウドの間でデータをレプリケート、同期、移行するための特別な機能、専用フラッシュストレージシステムのレベルで一貫した高パフォーマンスが挙げられます。

Cloud Volumes Service (CVS) をゲスト接続ストレージとして使用できるようになりました

VMware Engine を使用して Cloud Volumes Service を設定します

Cloud Volumes Service 共有は、VMware エンジン環境で作成された VM からマウントできます。Cloud Volumes Service では SMB プロトコルと NFS プロトコルがサポートされているため、ボリュームを Linux クライアントにマウントして Windows クライアントにマッピングすることもできます。Cloud Volumes Service ボリュームは簡単な手順で設定できます。

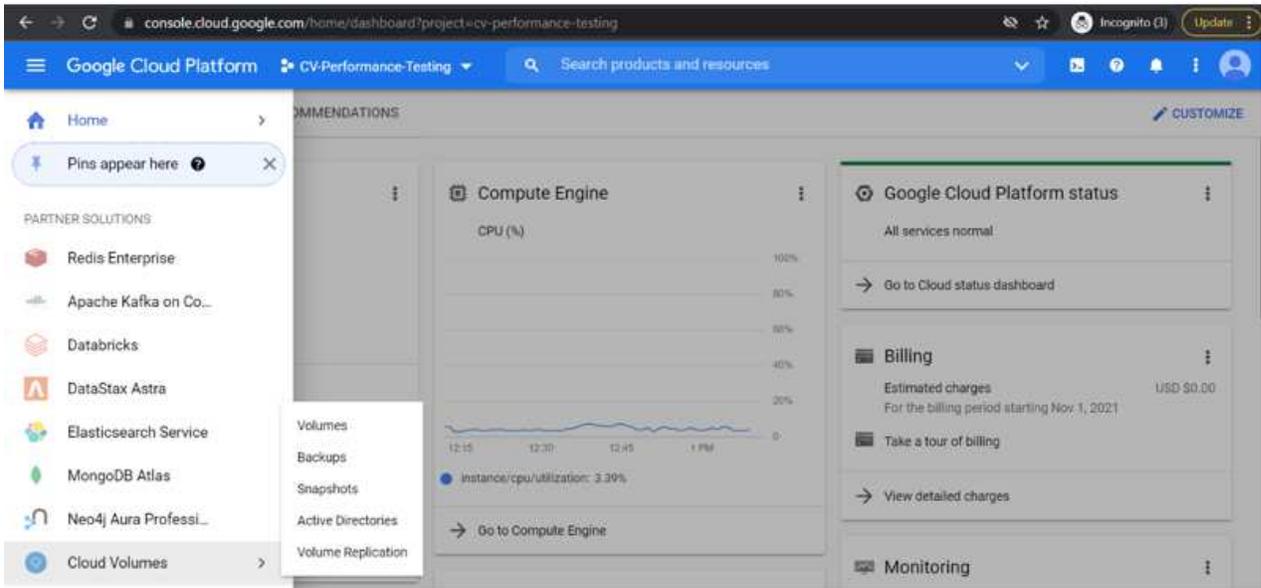
Cloud Volume Service と Google Cloud VMware Engine のプライベートクラウドは同じリージョンに配置する必要があります。

Google Cloud Marketplace で NetApp Cloud Volumes Service for Google Cloud を購入、有効化、設定するには、次の手順を実行します ["ガイド"](#)。

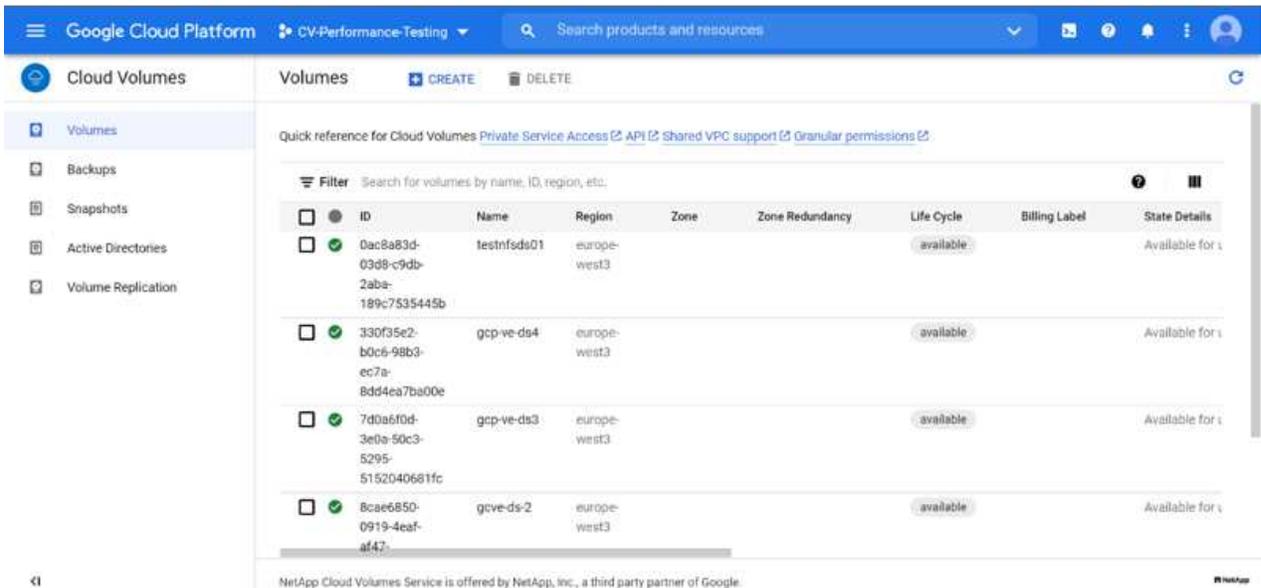
CVS NFS ボリュームを GCVE プライベートクラウドに作成する

NFS ボリュームを作成してマウントするには、次の手順を実行します。

1. Google クラウドコンソール内のパートナーソリューションから Cloud Volume にアクセスします。



2. Cloud Volume コンソールで、Volumes（ボリューム）ページに移動し、Create（作成）をクリックします。



3. [Create File System] ページで、チャージバックメカニズムに必要なボリューム名と課金ラベルを指定します。

4. 適切なサービスを選択します。GCVE は、CVS パフォーマンスと希望するサービスレベルを選択して、アプリケーションワークロードの要件に基づいてレイテンシの向上とパフォーマンスの向上を実現します。

Region availability varies by service type. [Learn more](#)'. There are two radio button options: 'CVS' (unselected) with the description 'Offers volumes created with zonal high availability.' and 'CVS-Performance' (selected) with the description 'Offers 3 performance levels and improved latency to address higher performance application requirements.' Below this is a 'Volume Replication' section with a checkbox for 'Secondary' and the description 'Select to create volume as a destination target for volume replication. Applicable only to CVS-performance volumes.'"/>

5. ボリュームおよびボリュームパスに Google Cloud のリージョンを指定（プロジェクト内のすべての Cloud Volume でボリュームパスが一意である必要があります）

Cloud Volumes	← Create File System
<ul style="list-style-type: none"> Volumes Backups Snapshots Active Directories Volume Replication 	<p>Region</p> <p>Region availability varies by service type.</p> <p>Region * <input type="text" value="europe-west3"/></p> <p>Volume will be provisioned in the region you select.</p> <p>Volume Path * <input type="text" value="nimCVSNFSol01"/></p> <p>Must be unique to the project.</p>

6. ボリュームのパフォーマンスレベルを選択します。

Cloud Volumes	← Create File System
<ul style="list-style-type: none"> Volumes Backups Snapshots Active Directories Volume Replication 	<p>Service Level</p> <p>Select the performance level required for your workload.</p> <p><input checked="" type="radio"/> Standard Up to 16 MiB/s per TiB</p> <p><input type="radio"/> Premium Up to 64 MiB/s per TiB</p> <p><input type="radio"/> Extreme Up to 128 MiB/s per TiB</p> <p>Snapshot <input type="text" value=""/></p> <p>The snapshot to create the volume from.</p>

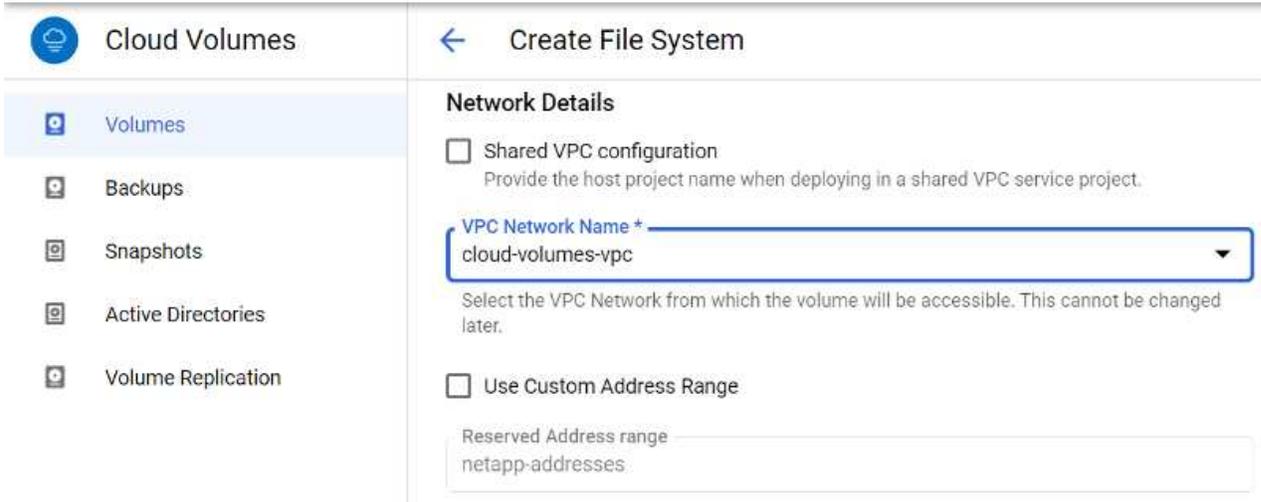
7. ボリュームのサイズとプロトコルのタイプを指定します。このテストでは、NFSv3 が使用されています。

Cloud Volumes	← Create File System
<ul style="list-style-type: none"> Volumes Backups Snapshots Active Directories Volume Replication 	<p>Volume Details</p> <p>Allocated Capacity * <input type="text" value="1024"/> GiB</p> <p>Allocated size must be between 1 TiB (1024 GiB) and 100 TiB (102400 GiB)</p> <p>Protocol Type * <input type="text" value="NFSv3"/></p> <p><input type="checkbox"/> Make snapshot directory (.snapshot) visible Makes .snapshot directory visible to clients. For NFSv4.1 volumes (CVS-Performance only), the directory itself will not be listed but can be accessed to list contents, etc.</p> <p><input type="checkbox"/> Enable LDAP Enables user look up from AD LDAP server for your NFS volumes</p>

8. この手順では、ボリュームにアクセスできる VPC ネットワークを選択します。VPC ピアリングが実

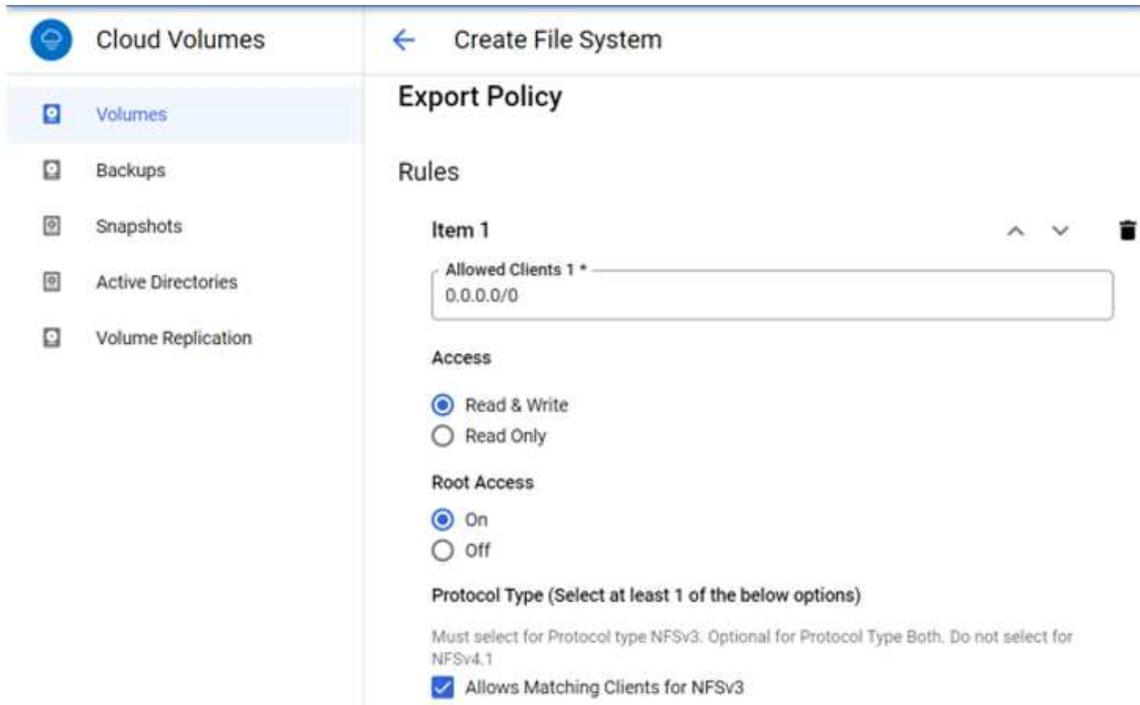
行されていることを確認します。

ヒント：VPC ピアリングが行われていない場合は、ピアリングコマンドの説明を示すポップアップボタンが表示されます。Cloud Shell セッションを開き、適切なコマンドを実行して、Cloud Volumes Service プロデューサーと VPC をピアリングします。事前に VPC ピアリングを準備する場合は、以下の手順を参照してください。



9. 適切なルールを追加してエクスポートポリシールールを管理し、対応する NFS バージョンのチェックボックスを選択します。

注：エクスポートポリシーを追加しないと、NFS ボリュームへのアクセスは許可されません。



10. [保存] をクリックしてボリュームを作成します。



VMware Engine で実行されている VM に NFS エクスポートをマウントする

NFS ボリュームのマウントを準備する前に、プライベート接続のピアステータスが Active と表示されていることを確認してください。ステータスが Active になったら、mount コマンドを使用します。

NFS ボリュームをマウントするには、次の手順を実行します。

1. クラウドコンソールで、Cloud Volume > Volumes に移動します。
2. Volumes (ボリューム) ページに移動します
3. NFS エクスポートをマウントする NFS ボリュームをクリックします。
4. 右にスクロールし、[詳細を表示] の下にある [指示のマウント] をクリックします。

VMware VM のゲスト OS 内からマウントプロセスを実行するには、次の手順を実行します。

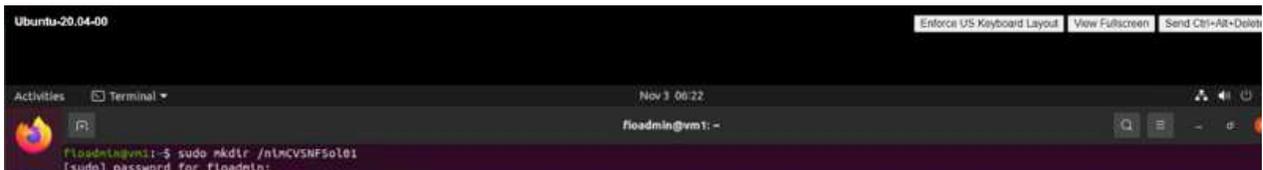
1. SSH クライアントと SSH を使用して仮想マシンに接続します。
2. インスタンスに NFS クライアントをインストールします。
 - a. Red Hat Enterprise Linux または SUSE Linux インスタンスの場合：

```
sudo yum install -y nfs-utils
.. Ubuntu または Debian のインスタンスで次の手順を実行します。
```

```
sudo apt-get install nfs-common
```

3. 「/nimCVSNFSol01」などの新しいディレクトリをインスタンスに作成します。

```
sudo mkdir /nimCVSNFSol01
```



4. 適切なコマンドを使用してボリュームをマウントします。ラボで使用するコマンドの例を次に示します。

```
sudo mount -t nfs -o rw,hard,rsize=65536,wsiz=65536,vers=3,tcp
10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```

```
root@vm1:~# sudo mkdir /nimCVSNFSol01
root@vm1:~# sudo mount -t nfs -o rw,hard,rsize=65536,wsiz=65536,vers=3,tcp 10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```

```

root@vni:~# df
Filesystem            1K-blocks      Used    Available  Use% Mounted on
udev                  16409952         0    16409952   0% /dev
tmpfs                  3288328         1500     3286748   1% /run
/dev/sdb5              61145932    19231356    38778832  34% /
tmpfs                  16441628         0     16441628   0% /dev/shm
tmpfs                   5120           0         5120   0% /run/lock
tmpfs                  16441628         0     16441628   0% /sys/fs/cgroup
/dev/loop0              128            128           0 100% /snap/bare/5
/dev/loop1              56832          56832           0 100% /snap/core18/2128
/dev/loop2              66688          66688           0 100% /snap/gtk-common-themes/1515
/dev/loop4              66816          66816           0 100% /snap/gtk-common-themes/1519
/dev/loop3              52224          52224           0 100% /snap/snap-store/547
/dev/loop5              224256         224256           0 100% /snap/gnome-3-34-1804/72
/dev/sdb1              523248         4         523244   1% /boot/efi
tmpfs                  3288324         28     3288296   1% /run/user/1000
10.53.0.4:/gcve-ds-1  107374182400 1136086016 106238096384 2% /base
/dev/napper/nfsprdvgl-prod01 419155968 55384972 363770996 14% /datastore1
/dev/loop8              33280          33280           0 100% /snap/snapd/13270
/dev/loop6              33280          33280           0 100% /snap/snapd/13640
/dev/loop7              56832          56832           0 100% /snap/core18/2246
10.53.0.4:/nlmCVSNFSol01 107374182400 256 107374182144 1% /nlmCVSNFSol01
root@vni:~#

```

VMware Engine で実行されている VM に SMB 共有を作成してマウントします

SMB ボリュームの場合は、SMB ボリュームを作成する前に、Active Directory 接続が設定されていることを確認してください。

Active Directory connections CREATE DELETE

Create a Windows Active Directory connection to your existing AD server. This is a prerequisite step before creating volumes with the SMB protocol type. [Learn more](#)

Filter Search for Active Directory connections by ID, username, DNS, netBIOS, region, etc.

<input type="checkbox"/>	Username	Domain	DNS Servers	NetBIOS Prefix	OU Path	AD Server Name	KDC IP	Region	Status
<input type="checkbox"/>	administrator	nimgcveval.com	192.168.0.16	nimsmb	CN=Computers			europa-west3	In Use

AD 接続が確立されたら、必要なサービスレベルを指定してボリュームを作成します。適切なプロトコルを選択する以外に、NFS ボリュームを作成する手順は同じです。

1. Cloud Volume コンソールで、Volumes（ボリューム）ページに移動し、Create（作成）をクリックします。
2. [Create File System] ページで、チャージバックメカニズムに必要なボリューム名と課金ラベルを指定します。

← Create File System

Volume Name

Name *

nimCVSMBvol01

A human readable name used for display purposes.

Billing Label

Label your volumes for billing reports, queries.

Supported with CVS-Performance service type; can be set with CVS service type but not available for billing at this time.

+ ADD LABEL

3. 適切なサービスを選択します。GCVE として、CVS パフォーマンスと希望するサービスレベルを選択し、ワークロード要件に基づいてレイテンシの向上とパフォーマンスの向上を実現します。

← Create File System

Service Type

Cloud Volumes Service is offered as two service types: CVS and CVS-Performance. Select the service type that matches your workload needs. [Region availability](#) varies by service type. [Learn more](#)

CVS

Offers volumes created with zonal high availability.

CVS-Performance

Offers 3 performance levels and improved latency to address higher performance application requirements.

Volume Replication

Secondary

Select to create volume as a destination target for volume replication. Applicable only to CVS-performance volumes.

4. ボリュームおよびボリュームパスに Google Cloud のリージョンを指定（プロジェクト内のすべての Cloud Volume でボリュームパスが一意である必要があります）

← Create File System

Region

Region availability varies by service type.

Region *

europa-west3

Volume will be provisioned in the region you select.

Volume Path *

nimCVSMBvol01

Must be unique to the project.

5. ボリュームのパフォーマンスレベルを選択します。

← Create File System

Service Level

Select the performance level required for your workload.

- Standard
Up to 16 MiB/s per TiB
- Premium
Up to 64 MiB/s per TiB
- Extreme
Up to 128 MiB/s per TiB

Snapshot

The snapshot to create the volume from.

6. ボリュームのサイズとプロトコルのタイプを指定します。このテストでは、SMB を使用します。

← Create File System

Volume Details

Allocated Capacity *

1024

GiB

Allocated size must be between 1 TiB (1024 GiB) and 100 TiB (102400 GiB)

Protocol Type *

SMB

- Make snapshot directory (.snapshot) visible
Makes .snapshot directory visible to clients. For NFSv4.1 volumes (CVS-Performance only), the directory itself will not be listed but can be accessed to list contents, etc.
- Enable SMB Encryption
Enable this option only if you require encryption of your SMB data traffic.
- Enable CA share support for SQL Server, FSLogix
Enable this option only for SQL Server and FSLogix workloads that require continuous availability.
- Hide SMB Share
Enable this option to make SMB shares non-browsable

7. この手順では、ボリュームにアクセスできる VPC ネットワークを選択します。VPC ピアリングが実行されていることを確認します。

ヒント： VPC ピアリングが行われていない場合は、ピアリングコマンドの説明を示すポップアップボタンが表示されます。Cloud Shell セッションを開き、適切なコマンドを実行して、Cloud Volumes Service プロデューサーと VPC をピアリングします。事前に VPC ピアリングを準備する場

合は、こちらを参照してください "手順"。

Network Details

Shared VPC configuration

Provide the host project name when deploying in a shared VPC service project.

VPC Network Name +

cloud-volumes-vpc

Select the VPC Network from which the volume will be accessible. This cannot be changed later.

Use Custom Address Range

Reserved Address range

netapp-addresses

SHOW SNAPSHOT POLICY

SAVE

CANCEL

8. [保存] をクリックしてボリュームを作成します。

<input type="checkbox"/>	<input checked="" type="checkbox"/>	6e4552ed-7378-7302-be28-21a169374f28	nimCVSMBvol01	europa-west3	Available for use	CVS-Performance	Primary	Standard	SMB: \\nimsmb-3830.nimgcveval.com\nimCVSMBvol01
--------------------------	-------------------------------------	--------------------------------------	---------------	--------------	-------------------	-----------------	---------	----------	---

SMB ボリュームをマウントするには、次の手順を実行します。

1. クラウドコンソールで、Cloud Volume > Volumes に移動します。
2. Volumes (ボリューム) ページに移動します
3. SMB 共有をマッピングする SMB ボリュームをクリックします。
4. 右にスクロールし、[詳細を表示] の下にある [指示のマウント] をクリックします。

VMware VM の Windows ゲスト OS からマウントプロセスを実行するには、次の手順を実行します。

1. [スタート] ボタンをクリックし、[コンピュータ] をクリックします。
2. [ネットワークドライブの割り当て] をクリックします。
3. [ドライブ] リストで、使用可能な任意のドライブ文字をクリックします。
4. フォルダボックスに、次のように入力します。

```
\\nimsmb-3830.nimgcveval.com\nimCVSMBvol01
```

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive:

Folder:

Example: \\server\share

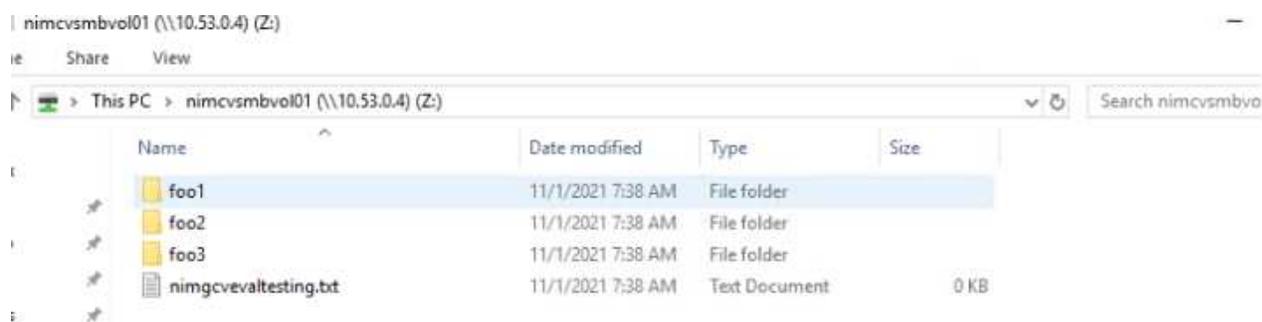
Reconnect at sign-in

Connect using different credentials

[Connect to a Web site that you can use to store your documents and pictures.](#)

コンピュータにログオンするたびに接続するには、[サインイン時に再接続]チェックボックスをオンにします。

5. 完了をクリックします。



Region Availability : AWS、Azure、GCPのNFS補足データストア

AWS、Azure、Google Cloud Platform (GCP) でのNFSデータストアの補足サポートについては、Global Regionを参照してください。

AWSリージョンの可用性

AWS / VMCで追加のNFSデータストアを使用できるかどうかは、Amazonによって定義されています。まず、VMCとFSxNの両方が指定されたリージョンで利用可能かどうかを確認する必要があります。次に、FSxNの補足的なNFSデータストアがそのリージョンでサポートされているかどうかを確認する必要があります。

- VMCの可用性を確認します "[こちらをご覧ください](#)".
- Amazonの価格設定ガイドには、FSxN (FSX ONTAP) が提供されている場所に関する情報が記載されています。この情報は次のページで確認できます "[こちらをご覧ください](#)".
- VMCのFSxN補足的なNFSデータストアがまもなく利用可能になります。

次の表に、情報がまだリリースされている間に、VMC、FSxN、およびFSxNの現在のサポート状況をNFSデ

一タストアとして示します。

南北アメリカ

* AWSリージョン*	* VMCの可用性*	* FSX ONTAP 可用性*	* NFSデータストアの可用性*
米国東部（北バージニア州）	はい。	はい。	はい。
米国東部（オハイオ州）	はい。	はい。	はい。
米国西部（北カリフォルニア）	はい。	いいえ	いいえ
US West（オレゴン州）	はい。	はい。	はい。
GovCloud（米国西部）	はい。	はい。	はい。
カナダ（中央）	はい。	はい。	はい。
南米（サンパウロ）	はい。	はい。	はい。

最終更新日：2022年6月2日

EMEAの場合

* AWSリージョン*	* VMCの可用性*	* FSX ONTAP 可用性*	* NFSデータストアの可用性*
ヨーロッパ（アイルランド）	はい。	はい。	はい。
ヨーロッパ（ロンドン）	はい。	はい。	はい。
ヨーロッパ（フランクフルト）	はい。	はい。	はい。
ヨーロッパ（パリ）	はい。	はい。	はい。
ヨーロッパ（ミラノ）	はい。	はい。	はい。
ヨーロッパ（ストックホルム）	はい。	はい。	はい。

最終更新日：2022年6月2日

アジア太平洋地域

* AWSリージョン*	* VMCの可用性*	* FSX ONTAP 可用性*	* NFSデータストアの可用性*
アジア太平洋地域（シドニー）	はい。	はい。	はい。
アジア太平洋地域（東京）	はい。	はい。	はい。
アジア太平洋地域（大阪）	はい。	いいえ	いいえ
アジア太平洋地域（シンガポール）	はい。	はい。	はい。

アジア太平洋地域（ソウル）	はい。	はい。	はい。
アジア太平洋地域（ムンバイ）	はい。	はい。	はい。
アジア太平洋地域（ジャカルタ）	いいえ	いいえ	いいえ
アジア太平洋地域（香港）	はい。	はい。	はい。

最終更新日：2022年9月28日

Azureリージョンの可用性

Microsoftは、AzureとAVS上でNFSデータストアの補足情報を提供します。まず、AVSとANFの両方が特定の地域で利用可能かどうかを確認する必要があります。次に、ANF補助NFSデータストアがそのリージョンでサポートされているかどうかを確認する必要があります。

- AVSとANFの対応状況を確認します ["こちらをご覧ください"](#)。
- ANF補助NFSデータストアが使用可能かどうかを確認します ["こちらをご覧ください"](#)。

GCPリージョンの可用性

GCPリージョンの可用性は、GCPがパブリック可用性に移行するとリリースされません。

まとめ：VMware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が選ばれる理由とは

ネットアップの Cloud Volume と主要ハイパースケール向け VMware ソリューションは、ハイブリッドクラウドの活用を検討している組織に大きな可能性をもたらします。このセクションの残りの部分では、NetApp Cloud Volume の統合によって真のハイブリッドマルチクラウド機能が実現されることを示すユースケースについて説明します。

ユースケース 1：ストレージの最適化

RVtools の出力を使用したサイジングの演習では、馬力（vCPU / vMem）のスケールがストレージと平行になっていることが常に明らかです。多くの場合、組織は、ストレージスペースを必要とするだけでなく、クラスタのサイズを十分に拡張して処理能力を必要とする状況に遭遇します。

NetApp Cloud Volume を統合することで、組織は vSphere ベースのクラウド解決策を簡単な移行アプローチで実現できます。再プラットフォーム化や IP の変更は不要で、アーキテクチャの変更も必要ありません。また、この最適化により、ホストの数を vSphere で必要な量以上に抑えながらストレージの設置面積を拡張できます。ただし、ストレージ階層、セキュリティ、ファイルは変更されません。これにより、導入を最適化し、全体的な TCO を 35 ~ 45% 削減できます。この統合により、ウォームストレージから本番環境レベルのパフォーマンスまで、ストレージを数秒で拡張できます。

ユースケース 2：クラウドへの移行

企業は、次のような理由から、オンプレミスのデータセンターからパブリッククラウドへのアプリケーション移行を迫られています。設備投資（CAPEX）から運用コスト（OPEX）に移行するための資金調達ディレクティブや、すべてをクラウドへ移行するというトップダウンの指示など、さまざまな理由があります。

スピードが重要な場合は、合理化された移行アプローチのみが可能で、これは、クラウド固有の IaaS プラットフォームに適応するためのアプリケーションの再プラットフォーム化とリファクタリングが低速でコストがかかるためですが、多くの場合、数か月かかることがあります。ネットアップの Cloud Volume とゲスト接続ストレージ用の帯域幅効率に優れた SnapMirror レプリケーションを組み合わせることで、アプリケーションと整合性のある Snapshot コピーと HCX、クラウド固有の移行（例 Azure Migrate）、または VM のレプリケーションに使用するサードパーティ製品）。この移行は、時間のかかる I/O フィルタメカニズムを使用する場合よりも簡単です。

ユースケース 3：データセンターの拡張

季節によって変動する需要の急増や、わずかに変動する有機的な成長によってデータセンターの容量が上限に達し解決策た場合、NetApp Cloud Volume と一緒にクラウドホスト型の VMware 環境に移行するのは簡単です。NetApp Cloud Volume を利用すると、アベイラビリティゾーン全体の高可用性と動的な拡張機能を提供することで、ストレージの作成、レプリケーション、拡張が非常に簡単に行えます。NetApp Cloud Volume を活用すると、ストレッチクラスタが不要になるため、ホストクラスタの容量を最小限に抑えることができます。

ユースケース 4：クラウドへのディザスタリカバリ

従来のアプローチでは、災害が発生した場合、クラウドに複製された VM は、クラウドに復元する前にクラウド独自のハイパーバイザプラットフォームに変換する必要があります。これは、危機的な状況では対処できません。

SnapCenter を使用してゲスト接続ストレージに NetApp Cloud Volume を使用し、オンプレミスからの SnapMirror レプリケーションとパブリッククラウド仮想化ソリューションを使用することで、ディザスタリカバリに対する優れたアプローチを考案できます。これにより、完全に一貫性のある VMware SDDC インフラ上で VM レプリカをリカバリできるようになり、クラウド固有のリカバリツールも利用できます（Azure Site Recovery を参照）、または Veeam などの同等のサードパーティツールが必要です。また、このアプローチにより、ランサムウェアからのディザスタリカバリ訓練やリカバリも迅速に実行できます。また、テスト用や災害時に、ホストをオンデマンドで追加することで、フル本番環境に拡張することもできます。

ユースケース 5：アプリケーションの最新化

アプリケーションがパブリッククラウドに配置されたら、組織は数百もの強力なクラウドサービスを活用して最新化と拡張を実現したいと考えています。NetApp Cloud Volume を使用すると、アプリケーションデータが vSAN にロックされず、Kubernetes などの幅広いユースケースでデータを移動できるため、最新化は簡単なプロセスです。

まとめ

オールクラウドとハイブリッドクラウドのどちらをターゲットとしている場合でも、NetApp Cloud Volume は、アプリケーションワークロードを導入、管理するための優れたオプションを提供し、ファイルサービスとブロックプロトコルに加えて、データ要件をアプリケーションレイヤと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、任意のクラウドやハイパースケーラを NetApp Cloud Volume と組み合わせる

ことで、オンプレミスと複数のクラウドにわたるクラウドのメリット、一貫したインフラ、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できます。

ストレージの接続に使用する一般的なプロセスや手順は同じです。新しい名前に変更されたデータの位置にすぎません。ツールやプロセスはすべて変わらないので、NetApp Cloud Volume を使用すれば導入全体を最適化できます。

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权を有し、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权については、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。