



## パブリッククラウド向け**VMware** NetApp public and hybrid cloud solutions

NetApp  
February 04, 2026

# 目次

|  |     |
|--|-----|
| パブリッククラウド向けVMware  | 1   |
| VMwareを使用したNetAppハイブリッドマルチクラウドの概要                                  | 1   |
| パブリッククラウドにおけるVMware Cloudのオプション                                    | 1   |
| 知っていましたか？  | 2   |
| ストレージ構成  | 2   |
| NetAppクラウドストレージのメリット   | 3   |
| 前提   | 4   |
| 詳細なアーキテクチャ   | 4   |
| ハイパースケーラー向けVMware向けNetAppソリューション                                   | 5   |
| ハイパースケーラー構成におけるVMware  | 6   |
| NetAppストレージオプション   | 7   |
| NetApp / VMwareクラウドソリューション   | 8   |
| NetAppハイブリッドマルチクラウドとVMwareのサポート対象構成                                | 9   |
| ハイパースケーラー構成におけるVMware  | 9   |
| クラウドプロバイダーでの仮想化環境の構成   | 9   |
| AWS上で仮想化環境を展開および構成する   | 10  |
| Azureに仮想化環境を展開して構成する   | 26  |
| Google Cloud Platform (GCP)に仮想化環境をデプロイして構成する                       | 34  |
| パブリッククラウドにおけるNetAppストレージ   | 37  |
| パブリッククラウドプロバイダー向けのNetAppストレージオプション                                 | 37  |
| Amazon Web Services: NetAppストレージを使用するためのオプション                      | 38  |
| TR-4938: VMware Cloud on AWSでAmazon FSx ONTAPをNFSデータストアとしてマウントする   | 40  |
| AWSで補足NFSデータストアを作成する   | 42  |
| AWS向けNetAppゲスト接続ストレージオプション   | 59  |
| Azure仮想化サービス: NetAppストレージを使用するためのオプション                             | 89  |
| ANFデータストアソリューションの概要  | 91  |
| Azureで追加のNFSデータストアを作成する  | 93  |
| Azure向けNetAppゲスト接続ストレージオプション                                       | 106 |
| Google Cloud VMware Engine: NetAppストレージを使用するためのオプション               | 122 |
| Google Cloud VMware Engineの補足NFSデータストアとGoogle Cloud NetApp Volumes | 123 |
| GCP向けNetAppストレージオプション  | 126 |
| 要約と結論: VMwareとNetAppのハイブリッドマルチクラウドを組み合わせる理由                        | 152 |
| ユースケース1:ストレージの最適化  | 152 |
| ユースケース2:クラウド移行   | 153 |
| ユースケース3:データセンターの拡張   | 153 |
| ユースケース#4:クラウドへの災害復旧  | 153 |
| ユースケース#5:アプリケーションのモダナイゼーション  | 153 |
| まとめ  | 153 |

# パブリッククラウド向けVMware

## VMwareを使用したNetApp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のアプローチを採用しています。これらの組織は変革段階にあり、顧客は現在のIT環境を評価し、評価と検出の取り組みに基づいてワークロードをクラウドに移行しています。

顧客がクラウドに移行する要因としては、弾力性とバースト、データセンターの廃止、データセンターの統合、サポート終了のシナリオ、合併、買収などが挙げられます。この移行の理由は、各組織とそれぞれのビジネス優先順位によって異なります。ハイブリッドクラウドに移行する場合、クラウドの展開と弾力性の力を最大限に引き出すには、クラウド内で適切なストレージを選択することが非常に重要です。

### パブリッククラウドにおける VMware Cloud のオプション

このセクションでは、各クラウドプロバイダーが、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)および/またはVMware Cloud Foundation (VCF)スタックをどのようにサポートするかについて説明します。

#### Azure VMware ソリューション

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ことができるハイブリッドクラウドサービスです。Azure VMware Solutionは、Microsoftによって完全に管理およびサポートされ、Azureインフラストラクチャを活用してVMwareによって検証されたファーストパーティソリューションです。つまり、Azure VMware Solutionを導入すると、お客様は、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を利用できるようになると同時に、Microsoft Azureのグローバルなプレゼンス、クラス最高のデータセンター設備、ネイティブAzureサービスとソリューションの豊富なエコシステムへの近接性を活用できるようになります。

#### VMware Cloud on AWS

VMware Cloud on AWSは、ネイティブAWSサービスへの最適化されたアクセスを備えたVMwareのエンタープライズクラスのSDDCソフトウェアをAWSクラウドに提供します。VMware Cloud Foundationを搭載した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管理を統合し、専用の柔軟なベアメタル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 エンジン

Google Cloud VMware Engineは、Google Cloudの高性能でスケーラブルなインフラストラクチャとVMware Cloud Foundationスタック(VMware vSphere、vCenter、vSAN、NSX-T)を基盤とするIaaS(Infrastructure as a Service)サービスです。このサービスは、アプリケーションの再設計や運用の再構築に伴うコスト、労力、リスクを負うことなく、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することで、クラウドへの迅速な移行を実現します。これは、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 Volumes のコロケーションにより、最小限のネットワーク遅延で最高のパフォーマンスが実現します。

## 知っていましたか？

使用するクラウドに関係なく、VMware SDDC が展開されると、初期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仮想化用の 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
- ・仮想ネットワークとセキュリティのための VMware NSX と管理用の NSX Manager クラスタ

## ストレージ構成

ストレージ集約型のワークロードをホストし、クラウド ホストの VMware ソリューションでスケールアウトすることを計画しているお客様の場合、デフォルトのハイパーコンバージド インフラストラクチャでは、コンピューティング リソースとストレージ リソースの両方を拡張する必要があります。

Azure NetApp Files、Amazon FSx ONTAP、Cloud Volumes ONTAP（3 大ハイパースケーラーすべてで利用可能）、Google Cloud NetApp Volumes for Google Cloud などの NetApp Cloud Volumes と統合することで、お客様はストレージを個別に独立して拡張し、必要に応じて SDDC クラスターにコンピューティング ノードのみを追加できるようになりました。

注：

- ・VMware では、アンバランスなクラスタ構成は推奨されていません。そのため、ストレージを拡張すると、ホストが追加され、TCO が増加します。
- ・可能な vSAN 環境は 1 つだけです。したがって、すべてのストレージ トラフィックは実稼働ワークロードと直接競合することになります。
- ・アプリケーション要件、パフォーマンス、コストを調整するために複数のパフォーマンス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限界に達するのは非常に簡単です。NetApp Cloud Volumes を使用してストレージを拡張し、アクティブなデータセットをホストするか、使用頻度の低いデータを永続ストレージに階層化します。

Azure NetApp Files、Amazon FSx ONTAP、Cloud Volumes ONTAP（3 つの主要ハイパースケーラーすべてで利用可能）、および Google Cloud 向けの Google Cloud NetApp Volumes 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 イニシエーターまたは、それぞれ Amazon FSx ONTAP、Cloud Volume ONTAP、Azure NetApp Files、Google Cloud NetApp Volumes（Google Cloud 用）と直接通信する NFS/SMB マウントを介して VM に接続されます。この構成により、vSAN の場合と同様に、使用可能な空き領域は使用されるスラック領域とストレージ ポリシーによって決まるため、ストレージ容量に関する課題を簡単に克服できます。

VMware Cloud on AWS 上の 3 ノードの SDDC クラスターを考えてみましょう。

- ・3 ノード SDDC の合計生容量 = 31.1 TB（ノードごとに約 10 TB）。
- ・追加のホストを追加する前に維持する必要があるスラックススペース = 25% = (0.25 × 31.1 TB) = 7.7 TB。
- ・スラックススペースを差し引いた後の使用可能な生の容量 = 23.4TB

- ・使用可能な有効な空き容量は、適用されるストレージ ポリシーによって異なります。

例えば：

- RAID 0 = 有効空き容量 = 23.4TB (使用可能な生の容量/1)
- RAID 1 = 有効空き容量 = 11.7TB (使用可能な生の容量/2)
- RAID 5 = 有効空き容量 = 17.5TB (使用可能な生の容量/1.33)

したがって、NetApp Cloud Volumes 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、TCO を最適化するのに役立ちます。



このドキュメントが書かれた時点では、ゲスト内ストレージのみが利用可能なオプションでした。

### 覚えておくべきポイント

- ・ハイブリッド ストレージ モデルでは、Tier 1 または優先度の高いワークロードがホスト自体の一部であり、近接しているため、特定のレイテンシ要件に対応するには、これらのワークロードを vSAN データストアに配置します。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 ONTAPにワークロード データを複製し、ブロック レベルのメカニズムを使用して移行を容易にします。これは、Azure NetApp FilesおよびGoogle Cloud NetApp Volumesには適用されません。 Azure NetApp FilesまたはGoogle Cloud NetApp Volumesにデータを移行するには、使用的するファイルプロトコルに応じて、NetApp XCP、BlueXP Copy and Sync、rsync、またはrobocopyを使用します。
- ・テストでは、それぞれの SDDC からストレージにアクセスする際に 2 ~ 4 ミリ秒の追加遅延が発生することが示されています。ストレージをマッピングするときには、この追加のレイテンシをアプリケーション要件に考慮に入れてください。
- ・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中にゲスト接続ストレージをマウントするには、iSCSI イニシエーターが再構成され、SMB 共有の DNS が更新され、fstab で NFS マウント ポイントが更新されていることを確認します。
- ・ゲスト内の Microsoft マルチパス I/O (MPIO)、ファイアウォール、およびディスク タイムアウトのレジストリ設定が VM 内で適切に構成されていることを確認します。



これはゲスト接続ストレージにのみ適用されます。

### NetAppクラウドストレージのメリット

NetAppクラウドストレージには、次のような利点があります。

- ・コンピューティングとは独立してストレージを拡張することで、コンピューティングとストレージの密度を向上します。
- ・ホスト数を削減できるため、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影響を与えません。
- ・Azure NetApp Filesのボリュームの再形成と動的なサービス レベル機能を使用すると、安定した状態のワークロードに合わせてサイズを設定することでコストを最適化し、過剰なプロビジョニングを防ぐことが

できます。

- Cloud Volumes ONTAPのストレージ効率、クラウド階層化、インスタンス タイプ変更機能により、ストレージを最適な方法で追加および拡張できます。
- 過剰なプロビジョニングを防ぎ、必要な場合にのみストレージ リソースが追加されます。
- 効率的なスナップショット 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。
- スナップショット 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します。
- 効率的な増分ブロック転送ベースの地域災害復旧を提供し、地域全体のブロック レベルの統合バックアップにより、より優れた RPO と RTO を実現します。

## 前提

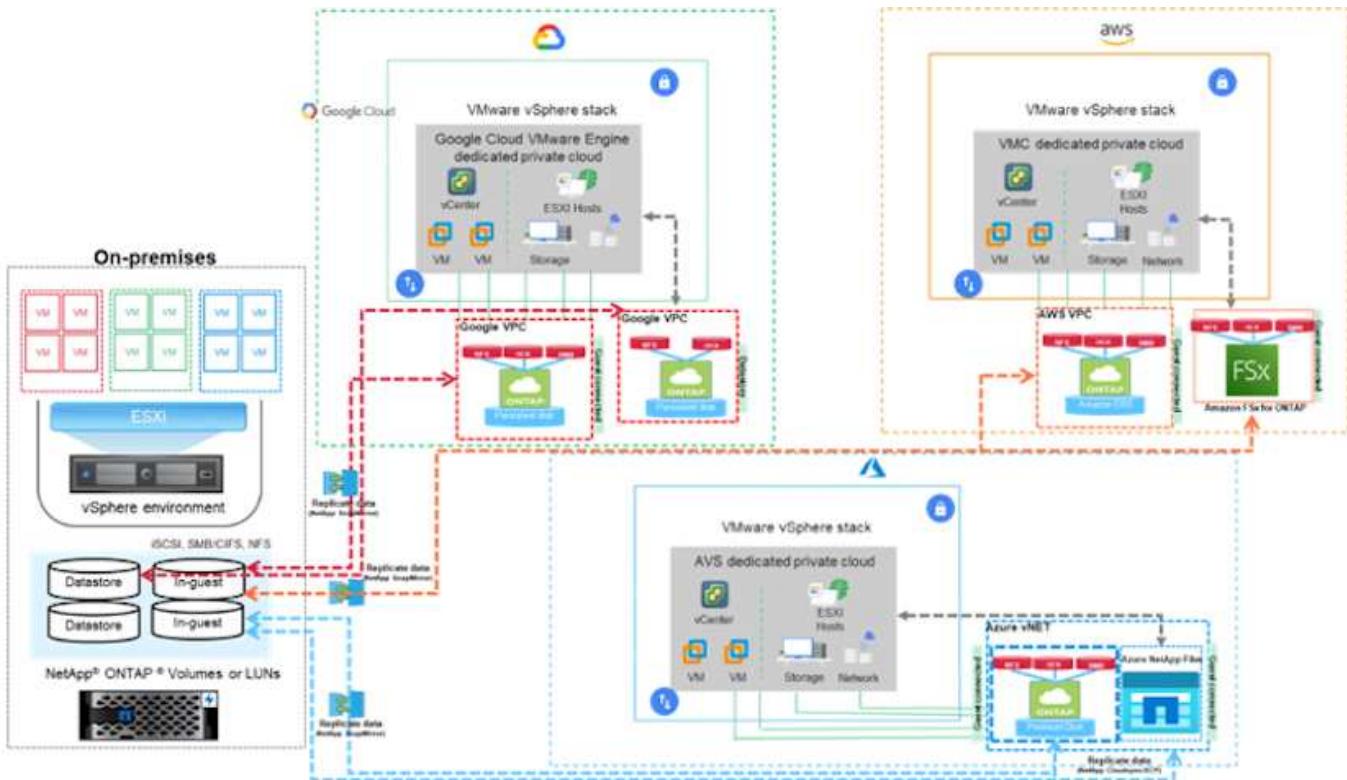
- SnapMirrorテクノロジーまたはその他の関連するデータ移行メカニズムが有効になっています。オンプレミスからハイペースケーラー クラウドまで、さまざまな接続オプションがあります。適切なパスを使用し、関連するネットワーク チームと連携します。
- このドキュメントが書かれた時点では、ゲスト内ストレージのみが利用可能なオプションでした。



ストレージと必要なホスト数の計画とサイズ設定については、NetAppソリューション アーキテクトと各ハイペースケーラー クラウド アーキテクトに依頼してください。NetApp、Cloud Volumes ONTAP Sizer を使用して適切なスループットでストレージ インスタンス タイプまたは適切なサービス レベルを決定する前に、ストレージ パフォーマンス要件を特定することをお勧めします。

## 詳細なアーキテクチャ

大まかに言えば、このアーキテクチャ(下の図を参照)は、NetApp Cloud Volumes ONTAP、Google Cloud NetApp Volumes for Google Cloud、および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 プロバイダー間でハイブリッド マルチクラウド接続とアプリの移植性を実現する方法をカバーしています。



## ハイパースケーラー向け VMware 向け NetApp ソリューション

ゲスト接続ストレージ デバイスまたは補助的な NFS データストアとしての NetApp から、ワークフローの移行、クラウドへの拡張/バースト、バックアップ/リストア、災害復旧まで、NetAppが 3 つの主要なハイパースケーラーに提供する機能について詳しく説明します。

クラウドを選択すると、あとはNetAppにお任せください。





特定のハイパースケーラーの機能を確認するには、そのハイパースケーラーの適切な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。

- ・ "ハイパースケーラー構成における VMware"
- ・ "NetAppストレージ オプション"
- ・ "NetApp / VMware クラウド ソリューション"

## ハイパースケーラー構成における **VMware**

オンプレミスの場合と同様に、VM の作成と移行のための本番環境を正常に構築するには、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、VMware Cloud on AWS SDDC を設定および管理し、NetAppストレージに接続するためには利用可能なオプションと組み合わせて使用する方法について説明します。



ゲスト内ストレージは、Cloud Volumes ONTAP をAWS VMC に接続するためにサポートされている唯一の方法です。

セットアッププロセスは次の手順に分けられます。

- VMware Cloud for AWS の導入と構成
- VMware Cloud を FSx ONTAPに接続する

詳細を表示 "[VMCの設定手順](#)"。

## Azure / AVS

このセクションでは、Azure VMware Solution をセットアップおよび管理し、NetAppストレージに接続するために使用可能なオプションと組み合わせて使用する方法について説明します。



ゲスト内ストレージは、Cloud Volumes ONTAP をAzure VMware Solution に接続するためにサポートされている唯一の方法です。

セットアッププロセスは次の手順に分けられます。

- リソースプロバイダーを登録してプライベートクラウドを作成する
- 新規または既存の ExpressRoute 仮想ネットワーク ゲートウェイに接続する
- 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する

詳細を表示 "[AVSの設定手順](#)"。

## GCP / GCVE

このセクションでは、GCVE を設定および管理する方法と、NetAppストレージに接続するために使用可能なオプションと組み合わせて使用する方法について説明します。



ゲスト内ストレージは、Cloud Volumes ONTAPおよびGoogle Cloud NetApp Volumes をGCVE に接続するためにサポートされている唯一の方法です。

セットアッププロセスは次の手順に分けられます。

- GCVE の導入と構成
- GCVEへのプライベートアクセスを有効にする

詳細を表示 "[GCVEの設定手順](#)"。

## NetAppストレージ オプション

NetAppストレージは、3つの主要なハイパースケーラーのそれぞれにおいて、ゲスト接続として、または補

助的な NFS データストアとしてなど、さまざまな方法で利用できます。

ぜひご覧ください"サポートされているNetAppストレージオプション"詳細についてはこちらをご覧ください。

### AWS / VMC

AWS は、次の構成でNetAppストレージ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
- ・ゲスト接続ストレージとしてのCloud Volumes ONTAP (CVO)
- ・補助的なNFSデータストアとしてのFSx ONTAP

詳細を表示"VMCのゲスト接続ストレージオプション"。 詳細を表示"VMC の補足 NFS データストア オプション"。

### Azure / AVS

Azure は、次の構成のNetAppストレージをサポートしています。

- ・ゲスト接続ストレージとしてのAzure NetApp Files (ANF)
- ・ゲスト接続ストレージとしてのCloud Volumes ONTAP (CVO)
- ・補助的な NFS データストアとしてのAzure NetApp Files (ANF)

詳細を表示"AVS のゲスト接続ストレージ オプション"。 詳細を表示"AVS の補足 NFS データストア オプション"。

### GCP / GCVE

Google Cloud は、次の構成のNetAppストレージをサポートしています。

- ・ゲスト接続ストレージとしてのCloud Volumes ONTAP (CVO)
- ・ゲスト接続ストレージとしてのGoogle Cloud NetApp Volumes (NetApp Volumes)
- ・補助的な NFS データストアとしてのGoogle Cloud NetApp Volumes (NetApp Volumes)

詳細を表示"GCVE のゲスト接続ストレージ オプション"。 詳細を表示"GCVE の補足 NFS データストア オプション"。

詳細はこちら"Google Cloud NetApp Volumesデータストアのサポート (NetAppブログ)"または"Google Cloud NetApp Volumes 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)"

## NetApp / VMware クラウド ソリューション

NetAppと VMware のクラウド ソリューションを使用すると、多くのユース ケースを任意のハイパースケーラーに簡単に導入できます。 VMware は、主要なクラウド 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（災害復旧とバックアップ/復元の両方を含む）
- ・移行

- ・拡張

#### AWS / VMC

["AWS / VMC向けNetAppソリューションを参照"](#)

#### Azure / AVS

["Azure / AVS向けNetAppソリューションを参照"](#)

#### GCP / GCVE

["Google Cloud Platform \(GCP\) /GCVE向けのNetAppソリューションをご覧ください"](#)

## NetAppハイブリッド マルチクラウドと VMware のサポート対象構成

主要なハイパースケーラーにおけるNetAppストレージ サポートの組み合わせを理解します。

|            |                                      |                                  |
|------------|--------------------------------------|----------------------------------|
|            | ゲスト接続                                | 補足 <b>NFS</b> データストア             |
| <b>AWS</b> | CVO FSx ONTAP <a href="#">"詳細"</a>   | FSx ONTAP <a href="#">"詳細"</a>   |
| アズール       | CVO ANF <a href="#">"詳細"</a>         | ANF <a href="#">"詳細"</a>         |
| <b>GCP</b> | CVO NetAppボリューム <a href="#">"詳細"</a> | NetAppボリューム <a href="#">"詳細"</a> |

## ハイパースケーラー構成におけるVMware

クラウドプロバイダーでの仮想化環境の構成

サポートされている各ハイパースケーラーで仮想化環境を構成する方法の詳細については、ここで説明します。

## AWS / VMC

このセクションでは、VMware Cloud on AWS SDDC を設定および管理し、NetAppストレージに接続するためには利用可能なオプションと組み合わせて使用する方法について説明します。



ゲスト内ストレージは、Cloud Volumes ONTAP をAWS VMC に接続するためにサポートされている唯一の方法です。

セットアッププロセスは次の手順に分けられます。

- VMware Cloud for AWS の導入と構成
- VMware Cloud を FSx ONTAPに接続する

詳細を表示 "[VMCの設定手順](#)"。

## Azure / AVS

このセクションでは、Azure VMware Solution をセットアップおよび管理し、NetAppストレージに接続するためには利用可能なオプションと組み合わせて使用する方法について説明します。



ゲスト内ストレージは、Cloud Volumes ONTAP をAzure VMware Solution に接続するためにサポートされている唯一の方法です。

セットアッププロセスは次の手順に分けられます。

- リソースプロバイダーを登録してプライベートクラウドを作成する
- 新規または既存の ExpressRoute 仮想ネットワーク ゲートウェイに接続する
- 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する

詳細を表示 "[AVSの設定手順](#)"。

## GCP / GCVE

このセクションでは、GCVE を設定および管理する方法と、NetAppストレージに接続するためには利用可能なオプションと組み合わせて使用する方法について説明します。



ゲスト内ストレージは、Cloud Volumes ONTAPおよびGoogle Cloud NetApp Volumes をGCVE に接続するためにサポートされている唯一の方法です。

セットアッププロセスは次の手順に分けられます。

- GCVE の導入と構成
- GCVEへのプライベートアクセスを有効にする

詳細を表示 "[GCVEの設定手順](#)"。

## AWS 上で仮想化環境を展開および構成する

オンプレミスの場合と同様に、VM の作成と移行のための本番環境を正常に構築するに

は、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、VMware Cloud on AWS SDDC を設定および管理し、NetAppストレージに接続するために利用可能なオプションと組み合わせて使用する方法について説明します。



現在、Cloud Volumes ONTAP (CVO) を AWS VMC に接続するためにサポートされている唯一の方法は、ゲスト内ストレージです。

セットアッププロセスは次の手順に分けられます。

## VMware Cloud for AWS の導入と構成

"VMware Cloud on AWS" 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 エクスペリエンスを提供します。各 VMware ソフトウェア定義データセンター (SDDC) は Amazon Virtual Private Cloud (VPC) で実行され、完全な VMware スタック (vCenter Server を含む)、NSX-T ソフトウェア定義ネットワーク、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、VMware Cloud on AWS をセットアップおよび管理し、ゲスト内ストレージを備えた Amazon FSx ONTAP や Cloud Volumes ONTAP on AWS と組み合わせて使用する方法について説明します。



現在、Cloud Volumes ONTAP (CVO) を AWS VMC に接続するためにサポートされている唯一の方法は、ゲスト内ストレージです。

セットアッププロセスは、次の 3 つの部分に分けられます。

### AWS アカウントを登録する

登録する "Amazon Web Services アカウント"。

開始するには AWS アカウントが必要です (まだ作成されていない場合)。新規または既存のアカウントに関わらず、この手順の多くのステップではアカウントの管理者権限が必要です。これを見て [リンク](#) AWS 認証情報に関する詳細については、こちらをご覧ください。

### My VMware アカウントを登録する

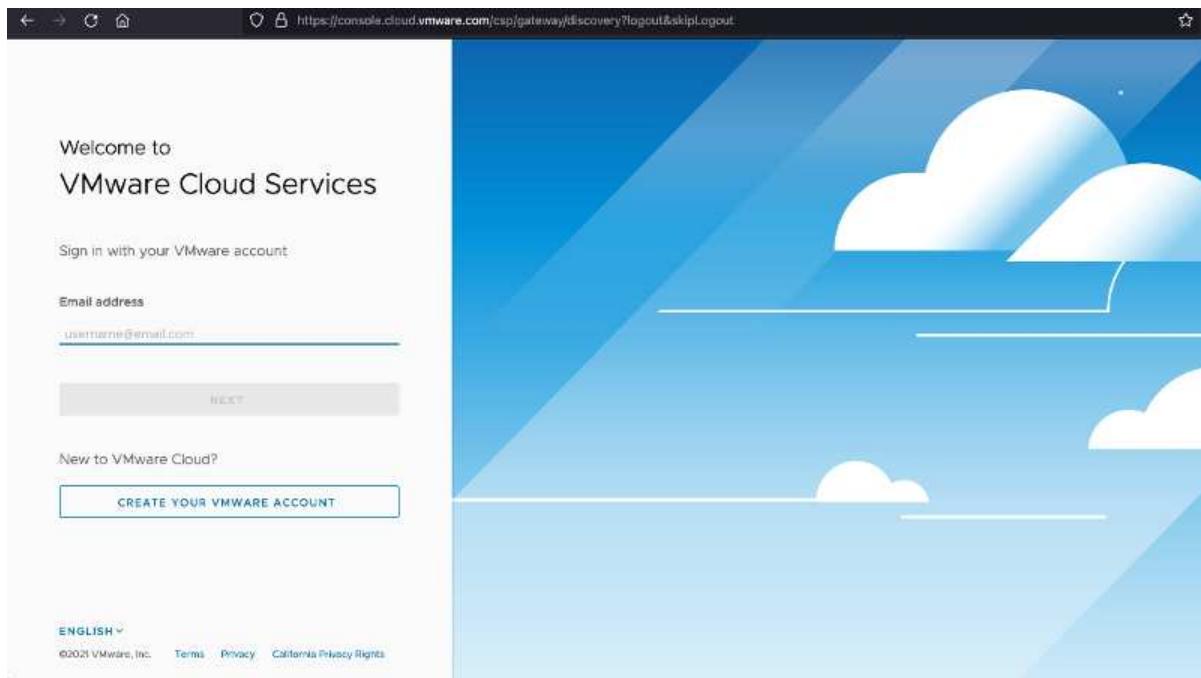
登録する "マイ VMware" アカウント。

VMware のクラウド ポートフォリオ (VMware Cloud on AWS を含む) にアクセスするには、VMware 顧客アカウントまたは My VMware アカウントが必要です。まだお持ちでない場合は、VMware アカウントを作成してください。["ここをクリックしてください。"](#)。

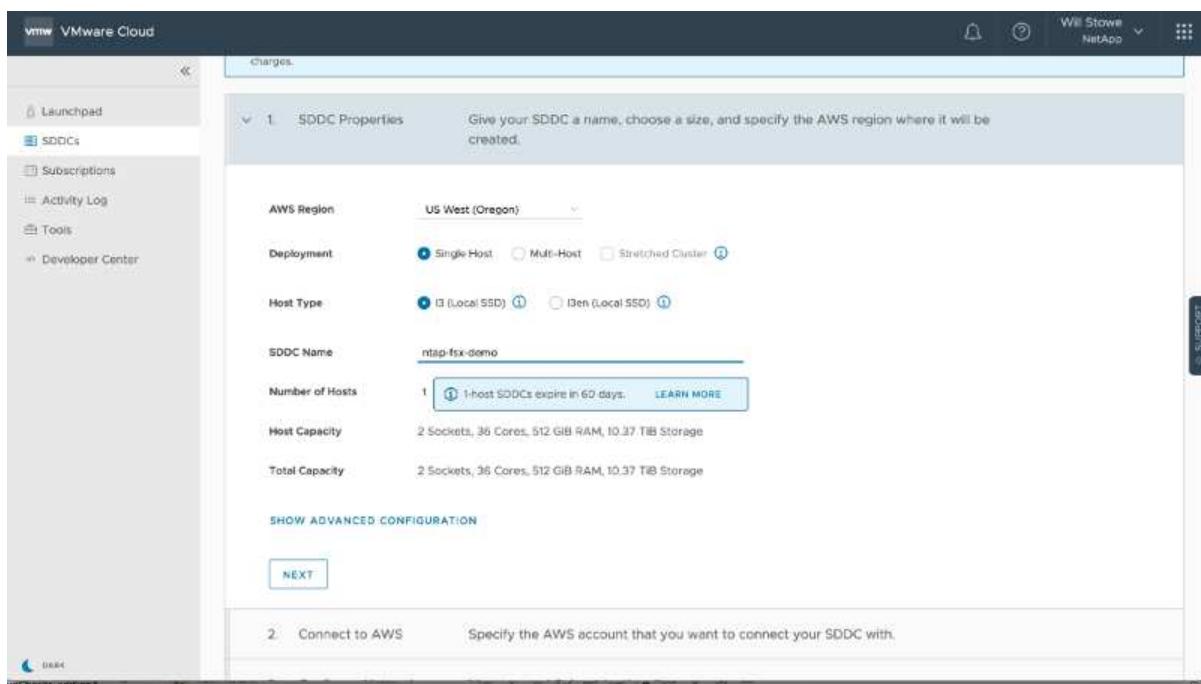
## VMware Cloud で SDDC をプロビジョニングする

VMware アカウントが構成され、適切なサイズ設定が実行されたら、VMware Cloud on AWS サービスを使用するための次のステップは、ソフトウェア定義データセンターの展開です。SDDC を作成するには、ホストする 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 アカウントをまだお持ちでない場合でも、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。

- 既存または新しく作成した VMware 認証情報を使用して、VMware Cloud Console にログインします。



- AWS リージョン、デプロイメント、ホストタイプ、および SDDC 名を構成します。



### 3. 目的の AWS アカウントに接続し、AWS Cloud Formation スタックを実行します。

The screenshot shows the AWS CloudFormation 'Quick create stack' wizard. It consists of three main sections:

- Template**: Shows the template URL: <https://vmware-sddc.s3.us-west-2.amazonaws.com/1eb9d184-a706-4488-abb8-692aad0a25d0/mq5ijohtclieoh815b75nteqq9ic4bddd7ifq07nv7v16fk36>. A note states: "This template is created by VMware Cloud on AWS for SDDC deployment and maintenance. Please do not remove."
- Stack name**: The stack name is set to "vmware-sddc-formation-a87f31c9-e5ac-4bb4-9d1e-9a3dabd197b7". A note says: "Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-)."
- Parameters**: A note says: "Parameters are defined in your template and allow you to input custom values when you create or update a stack." Below this, it says "No parameters" and "There are no parameters defined in your template".

At the bottom, there is a section titled "Capabilities" with a note: "The following resource(s) require capabilities: [AWS::IAM::Role]". It explains that the template contains IAM resources and asks the user to check if they want to create them. There is also a checkbox for acknowledging IAM creation.

At the very bottom, there are three buttons: "Cancel", "Create change set" (disabled), and "Create stack" (highlighted in orange).

VMware Cloud

SDDC Properties: ntap-fsx-demo - 1 Hosts - us-west-2

2. Connect to AWS: Specify the AWS account that you want to connect your SDDC with.

This step gives VMware permission to set up networking correctly for your SDDC on your AWS Infrastructure using cross-account rules.

Skip for now.  Connect to AWS now

Choose an AWS account:

When the CloudFormation stack has completed in your AWS account, the connection will show success below.

Establishing Connection

Estimated time remaining: 60 seconds

NEXT

Congratulations! Your connection is successfully established.

CF Stack: vmware-sddc-formation-af87f31c9-45ac-4bb4-9d1e-9a33ab897b7

AWS Account ID: [REDACTED]

NEXT

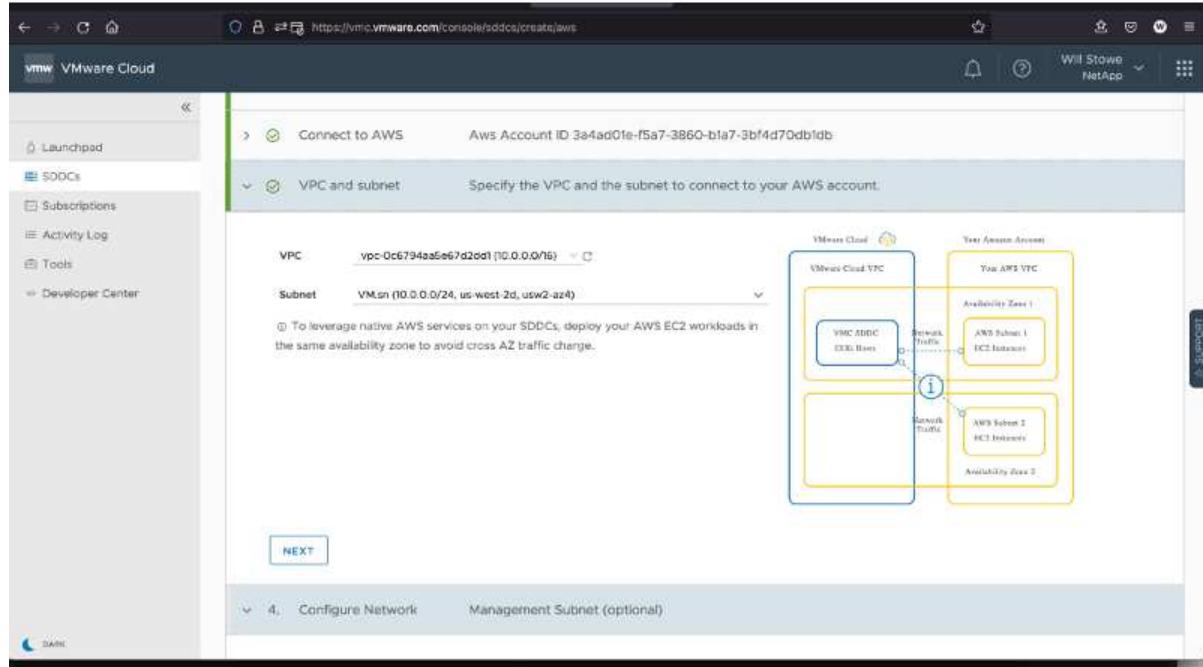
3. VPC and subnet: Specify the VPC and the subnet to connect to your AWS account.

4. Configure Network: Management Subnet (optional)

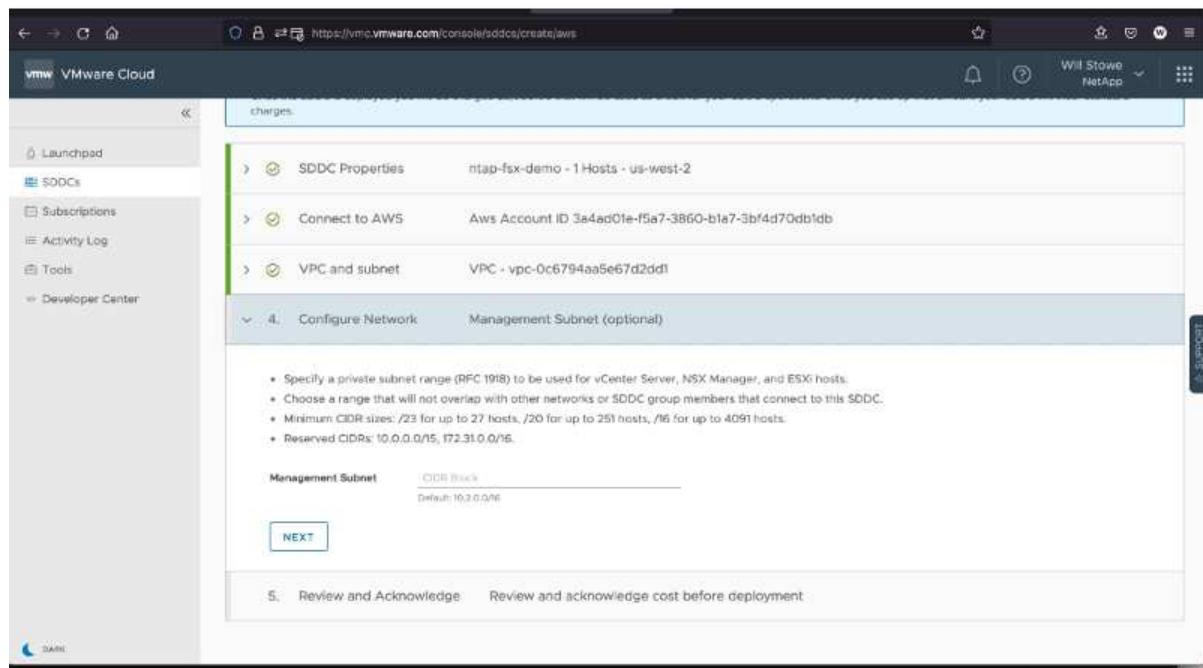


この検証では単一ホスト構成が使用されます。

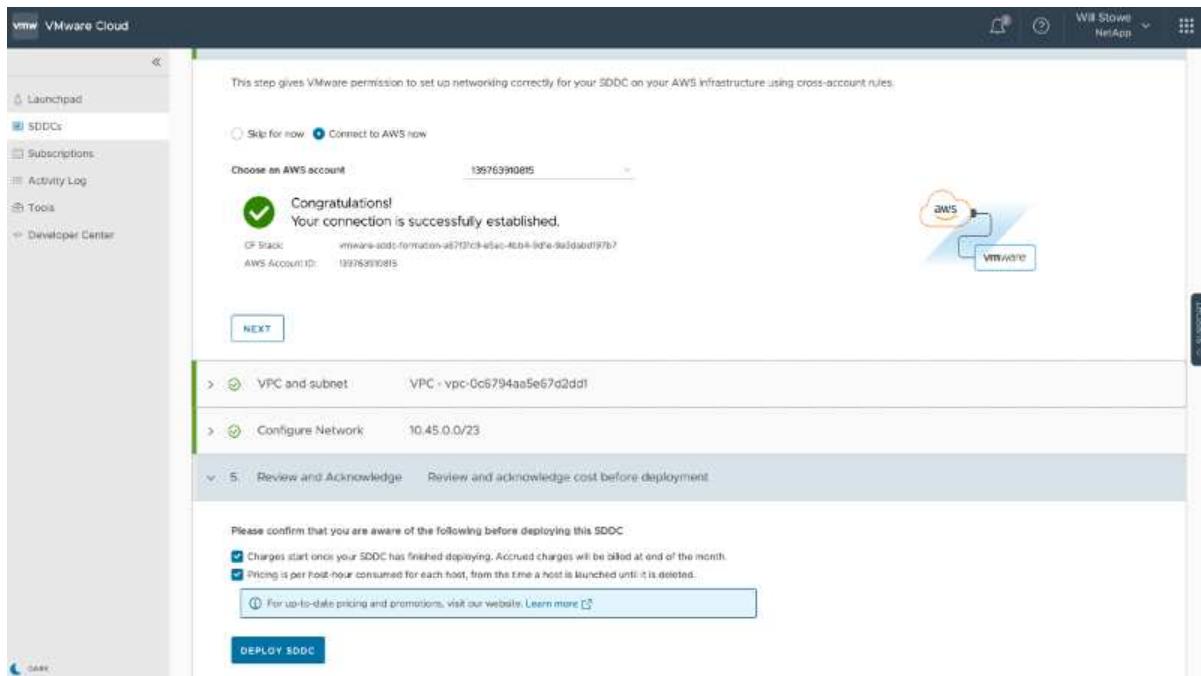
#### 4. VMC 環境を接続する目的の AWS VPC を選択します。



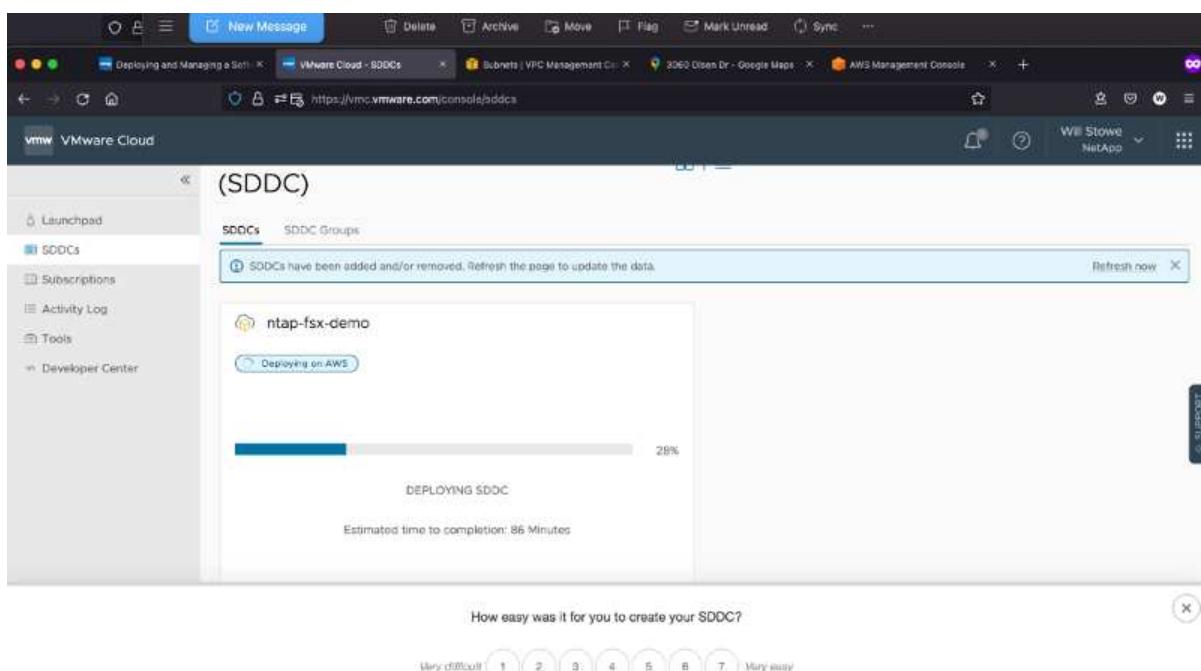
5. VMC 管理サブネットを構成します。このサブネットには、vCenter、NSX などの VMC 管理サービスが含まれます。SDDC 環境への接続を必要とする他のネットワークと重複するアドレス空間を選択しないでください。最後に、以下に示す CIDR サイズの推奨事項に従ってください。



6. SDDC 構成を確認して承認し、「SDDC の展開」をクリックします。



展開プロセスが完了するまでには通常約 2 時間かかります。



7. 完了すると、SDDC が使用できるようになります。

The screenshot shows the VMware Cloud interface for managing Software-Defined Data Centers (SDDCs). The main title is "Software-Defined Data Centers (SDDC)". On the left sidebar, there are links for "Launched", "Subscriptions", "Activity Log", "Tools", and "Developer Center". The "SDDCs" link is selected. In the center, there is a card for the SDDC "ntap-fsx-demo". The card displays the following details:

| Region             | US West (Oregon) | Clusters | 1  |
|--------------------|------------------|----------|----|
| Type               | VMC on AWS SDDC  | Hosts    | 1  |
| Availability Zones | us-west-2a       | Config   | 36 |
| VMC on AWS SDDC    |                  |          |    |

Below the card, resource statistics are shown:

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

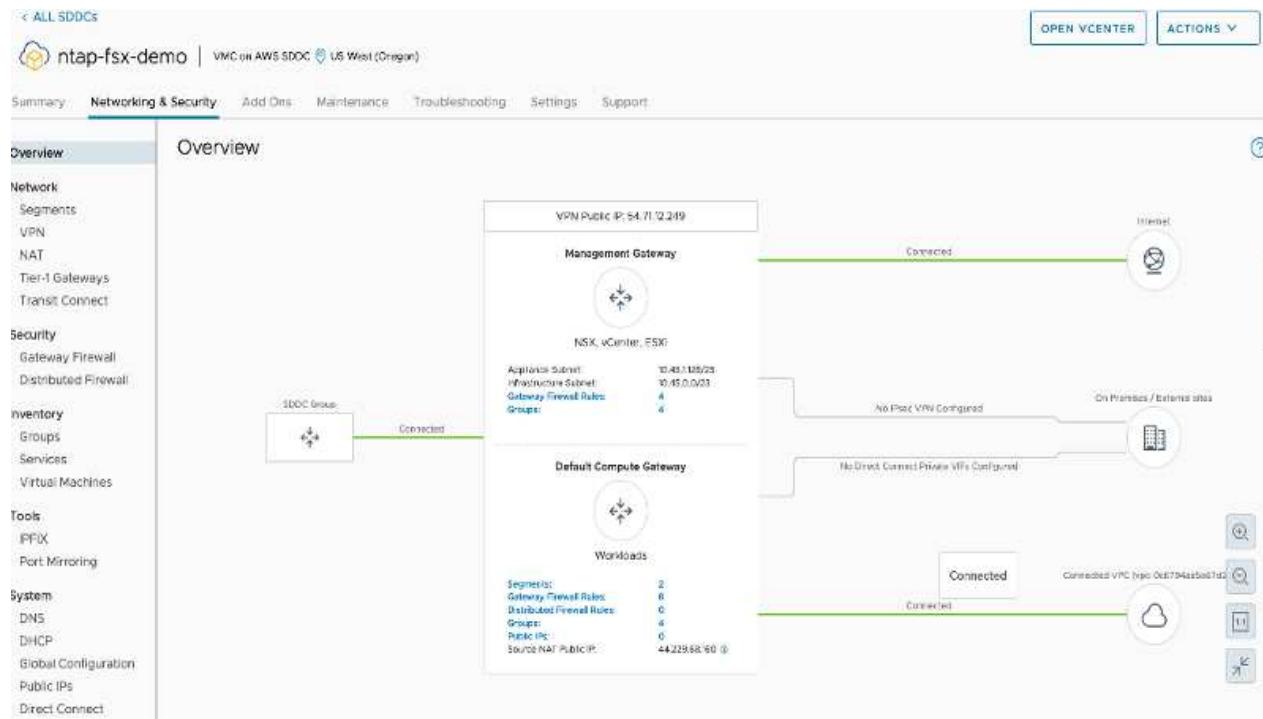
At the bottom of the card, there are three buttons: "VIEW DETAILS", "OPEN VCENTER", and "ACTIONS ▾". Below the card, there are two navigation links: "BACK TO TOP" and "GO TO GRID VIEW".

SDDC導入のステップバイステップガイドについては、"VMCコンソールからSDDCを展開する"。

## VMware Cloud を FSx ONTAPに接続する

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 のデプロイが完了し、AWS VPC に接続されたら、元の接続された VPC ではなく新しい VPC にAmazon FSx ONTAP をデプロイする必要があります(下のスクリーンショットを参照)。FSx (NFS および SMB フローティング IP) は、接続された VPC にデプロイされている場合はアクセスできません。Cloud Volumes ONTAPなどの iSCSI エンドポイントは、接続された VPC からは問題なく機能することに注意してください。



2. 同じリージョンに追加の VPC をデプロイし、新しい VPC にAmazon FSx ONTAP をデプロイします。

VMware Cloud コンソールで SDDC グループを構成すると、FSx がデプロイされている新しい VPC に接続するために必要なネットワーク構成オプションが有効になります。手順 3 で、「グループに VMware Transit Connect を構成すると、添付ファイルとデータ転送ごとに料金が発生します」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。このプロセスは完了するまでに数分かかる場合があります。

VMware Cloud

### Create SDDC Group

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

|             |             |
|-------------|-------------|
| Name        | sddcgroup01 |
| Description | sddcgroup01 |

**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

### Create SDDC Group

**1. Name and Description** Name: sddcgroup01

**2. Membership** Select SDDCs to be part of your group.

| Name          | Sddc ID                              | Location         | Version   | Management CIDR |
|---------------|--------------------------------------|------------------|-----------|-----------------|
| intap-lx-demo | 829a6e22-92d1-42db-ad3d-9e4eb7a90fb6 | US West (Oregon) | 1.14.0.14 | 10.45.0.0/23    |
| 1             |                                      |                  |           |                 |

**NEXT**

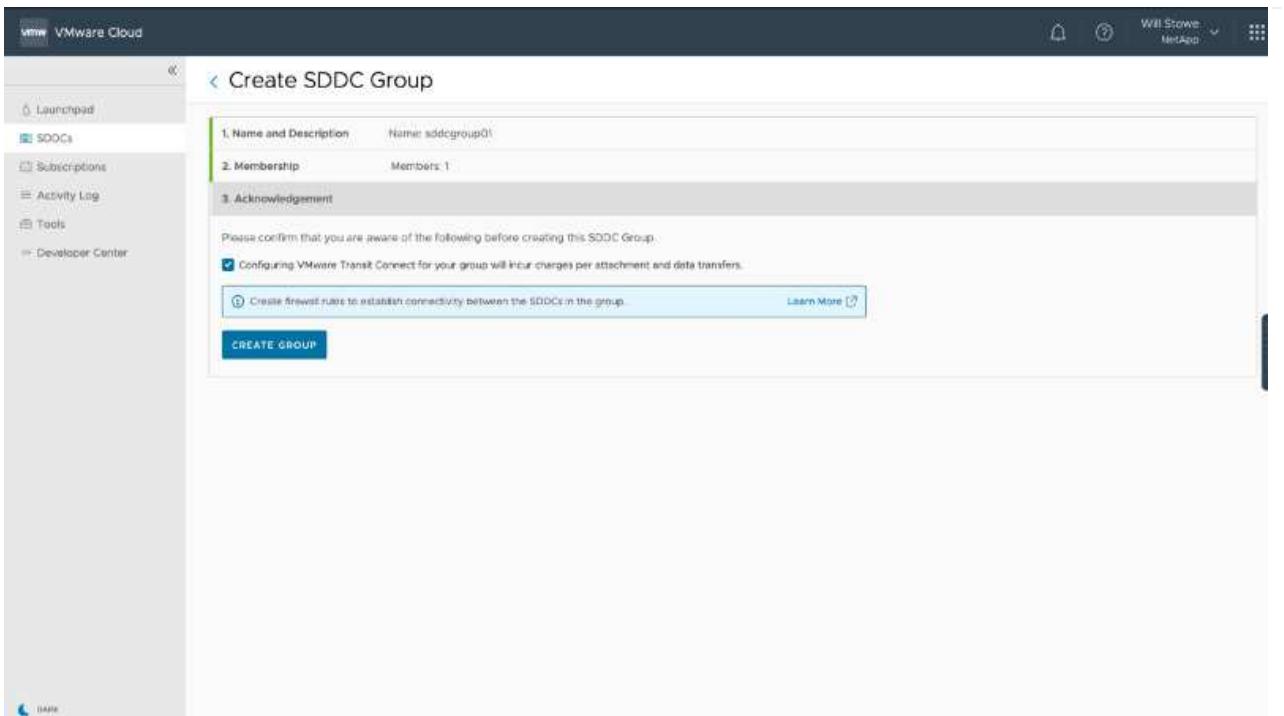
**3. Acknowledgement** Review and acknowledge requirements before creating the group.

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

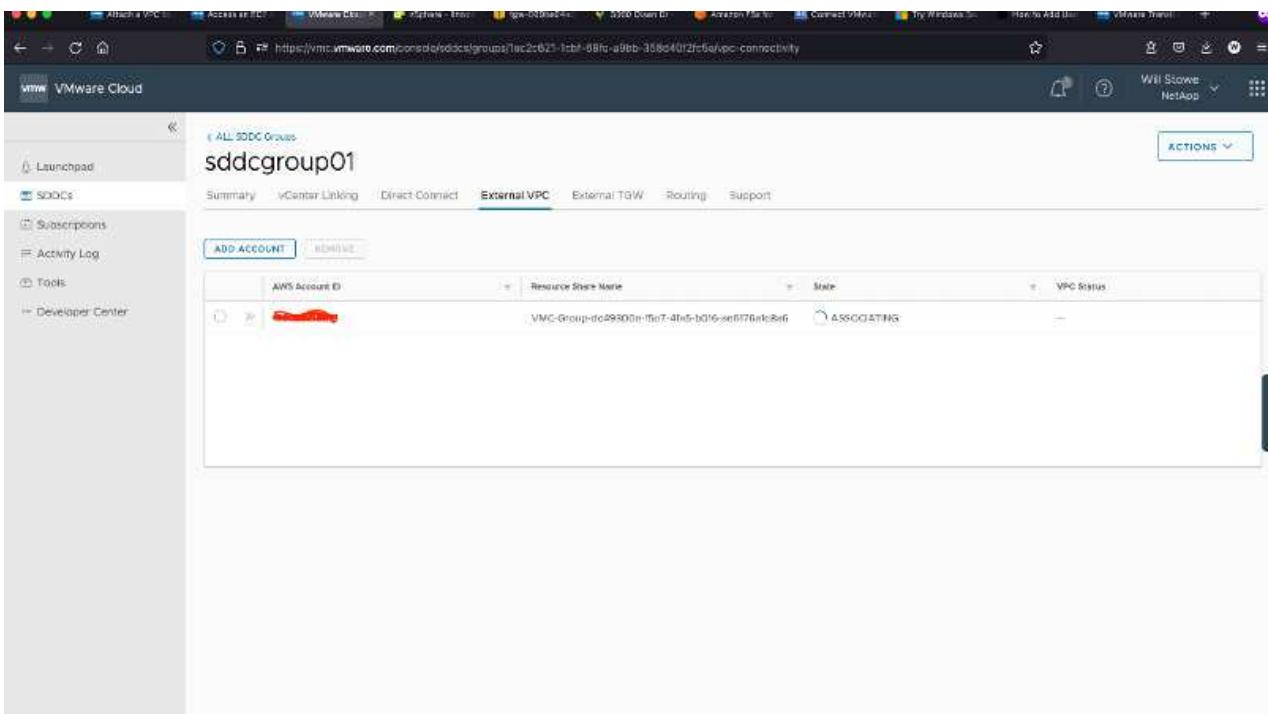
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.

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、先ほど作成した SDDC グループに接続します。外部VPCタブを選択し、"外部VPCを接続する手順"グループへ。このプロセスが完了するまでに 10 ~ 15 分かかる場合があります。



The screenshot shows the VMware Cloud interface with the 'External VPC' tab selected. The main area displays a table with one row, showing the following information:

| AWS Account ID                              | Resource Share Name                         | Status     | VPC Status |
|---|---|------------|------------|
| VMC-Group-dc09300e15e74fb5-b016-e80176e8e86 | VMC-Group-dc09300e15e74fb5-b016-e80176e8e86 | ASSOCIATED | ...        |

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 を介して新しい共有リソースへのプロンプトが表示されます。共有リソースは "AWS トランジットゲートウェイ" VMware Transit Connect によって管理されます。

The screenshot shows the AWS Resource Access Manager (RAM) console. The left sidebar shows navigation options like 'Resource shares' (selected), 'Shared resources', and 'Principals'. The main content area has the following sections:

- How it works:** A diagram illustrating the RAM workflow: RAM → Select Resources → Specify Principals → Share Resources.
- Use cases:**
  - Manage resources centrally in a multi-account environment.
  - Increase efficiency, decrease costs.
- Pricing:** RAM is offered at no additional charge; there are no setup fees or upfront commitments.
- More resources:** Links to 'What is AWS Resource Access Manager?', 'Getting started', and 'Documentation'.
- Your AZ ID:** A note about AZ IDs providing a consistent way of identifying resource locations across accounts.

The screenshot shows the AWS Resource Access Manager (RAM) interface. On the left, there's a sidebar with navigation options like 'Shared by me' and 'Shared with me'. Under 'Shared with me', 'Resource shares' is selected, showing one invitation. The main panel displays a 'Summary' table for a resource share named 'VMC-Group-dc49300e-f5e7-4fa5-b016-ae6176a1e8a6 (051a6fc5-0a1e-4560-853f-e2939d856b0c)'. The table includes columns for Name, Owner, Invitation date, and Status (Pending). Below the table, there are 'Reject resource share' and 'Accept resource share' buttons.

## 5. Transit Gateway アタッチメントを作成します。

The screenshot shows the 'Create transit gateway attachment' wizard. The first step, 'Details', is completed. It shows a 'Name tag - optional' field containing 'my-transit-gateway-attachment', a 'Transit gateway ID' dropdown set to 'tgw-001646b36ee07a2cb', and an 'Attachment type' dropdown set to 'VPC'. The second step, 'VPC attachment', is currently being configured. It includes sections for 'DNS support' (checked), 'IPv6 support' (unchecked), 'VPC ID' (selected 'vpc-0d1c764bcc495e805 (vmcfss2.vpc)'), and 'Subnet IDs' (unchecked).

## 6. VMC コンソールに戻り、VPC アタッチメントを承認します。このプロセスが完了するまでに約 10 分かかります。

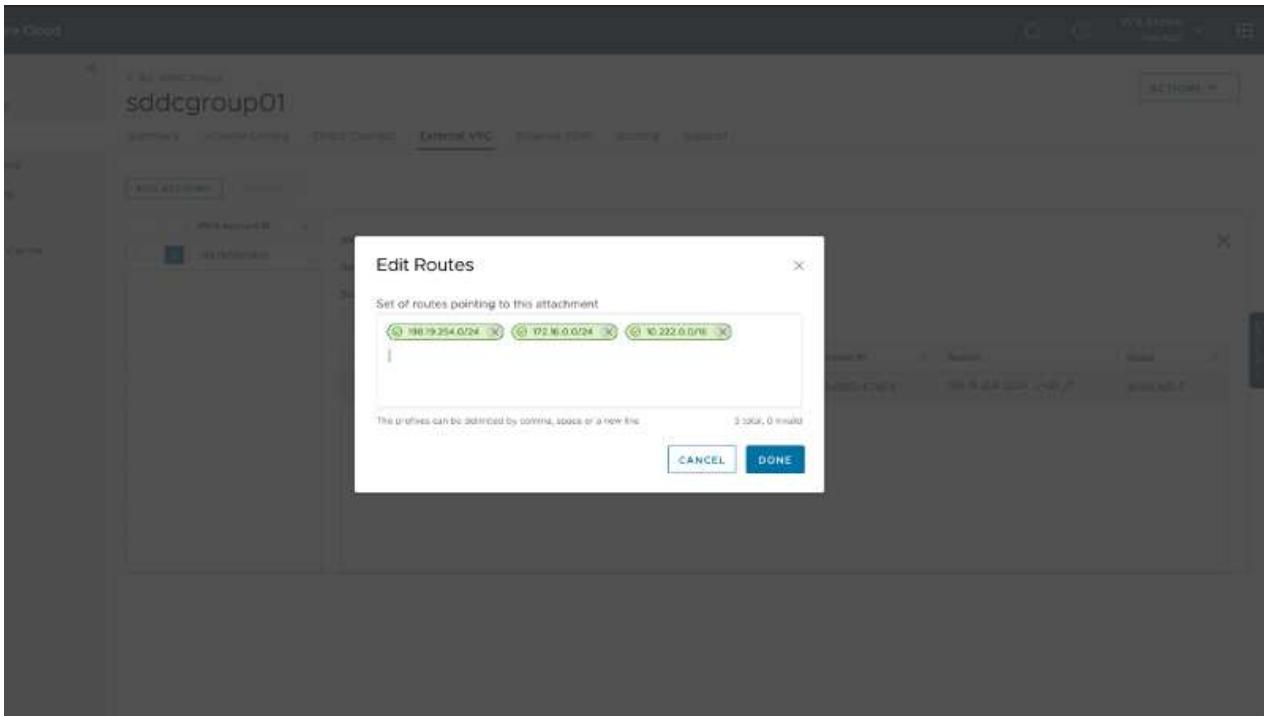
The screenshot shows the VMware Cloud SDDC Groups interface. On the left, there's a sidebar with options like Launchpad, SDDCs, Subscriptions, Activity Log, Tools, and Developer Center. The main area shows a group named "sddcgroup01". The "External VPC" tab is selected. A modal window is open, prompting for an AWS Account ID. It shows the VPC ID "vpc-0d1c764bcc495e805", the VMC on AWS Region "US West (Oregon)", and the Transit Gateway Attachment ID "tgw-attach-0a4883d6f82c67d64". The "Status" column shows "PENDING".

7. [外部 VPC] タブで、[ルート] 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。

- Amazon FSx ONTAPのフローディング IP 範囲のルート"フローディングIP"。
- Cloud Volumes ONTAPのフローディング IP 範囲のルート (該当する場合)。
- 新しく作成された外部 VPC アドレス空間へのルート。

The screenshot shows the same interface as before, but the modal window now displays the route status as "AVAILABLE". The rest of the interface remains the same, showing the SDDC group configuration.

8. 最後に、双方向トラフィックを許可する"ファイアウォール ルール"FSx/CVO にアクセスします。これらに従ってください"詳細な手順"SDDC ワークロード接続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 グループが設定されると、次のように vCenter にアクセスできるようになります。

| Name                  | ID   | Sources                | Destinations           | Services | Applied To       | Action |
|-----------------------|------|------------------------|------------------------|----------|------------------|--------|
| allow Internet fro... | 1019 | vmc-addc<br>vmc-addc-2 | Any                    | Any      | All Uplinks      | Allow  |
| allow VMC to VPC      | 1017 | vmc-addc<br>vmc-addc-2 | Connected...           | Any      | All Uplinks      | Allow  |
| allow VPC to VMC      | 1016 | Connected...           | vmc-addc               | Any      | All Uplinks      | Allow  |
| allow to vmcfsx2...   | 1022 | vmc-addc<br>vmc-addc-2 | vmcfsx2.v...           | Any      | All Uplinks      | Allow  |
| all from vmcfsx2...   | 1023 | vmcfsx2.v...           | vmc-addc-2<br>vmc-addc | Any      | All Uplinks      | Allow  |
| Default VTI Rule      | 1012 | Any                    | Any                    | Any      | VPN Tunnel In... | Allow  |
| Default Uplink Ru...  |      | Any                    | Any                    | Any      | All Uplinks      | Drop   |

次のステップでは、Amazon FSx ONTAPまたはCloud Volumes ONTAPが要件に応じて構成されていること、およびボリュームがプロビジョニングされて、vSAN からストレージ コンポーネントをオフロードし、展開が最適化されていることを確認します。

## Azure に仮想化環境を展開して構成する

オンプレミスと同様に、VM の作成と移行のための実稼働対応環境を正常に構築するには、Azure VMware Solution を計画することが重要です。

このセクションでは、Azure VMware Solution をセットアップおよび管理し、NetAppストレージに接続するために使用可能なオプションと組み合わせて使用する方法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られます。

## リソースプロバイダーを登録してプライベートクラウドを作成する

Azure VMware Solution を使用するには、まず、識別されたサブスクリプション内にリソース プロバイダーを登録します。

1. Azure ポータルにSign in。
2. Azure ポータル 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 プロバイダーを選択し、検索に「Microsoft.AVS」と入力します。
6. リソース プロバイダーが登録されていない場合は、[登録] を選択します。

The screenshot shows two overlapping Azure portal windows. The left window is titled 'Subscriptions' and displays a list of subscriptions. It includes filters for 'My role' (8 selected) and 'Status' (3 selected), and a search bar. The right window is titled 'Resource providers' and shows a list of providers. A search bar at the top of this window contains 'AVS'. A single provider entry, 'Microsoft.AVS', is listed in the table below, with its status shown as 'Registering'.

| Provider      | Status      |
|---------------|-------------|
| Microsoft.AVS | Registering |

| 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 プロバイダーを登録したら、Azure Portal を使用して Azure VMware Solution プライベート クラウドを作成します。
8. Azure ポータルにSign in。
9. [新しいリソースの作成]を選択します。
10. [Marketplace を検索] テキスト ボックスに「Azure VMware Solution」と入力し、結果から選択します。
11. Azure VMware Solution ページで、[作成] を選択します。
12. [基本] タブで、フィールドに値を入力し、[確認 + 作成] を選択します。

注：

- ・迅速に開始するには、計画段階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 リソースがデプロイおよび管理される論理コンテナーです。
- ・CIDR アドレスが一意であり、他の Azure 仮想ネットワークまたはオンプレミス ネットワークと重複していないことを確認します。CIDR はプライベート クラウド管理ネットワークを表し、vCenter Server や NSX-T Manager などのクラスタ管理サービスに使用されます。NetApp、/22 アドレス空間の使用を推奨しています。この例では、10.21.0.0/22 が使用されます。

## Create a private cloud

Prerequisites   \*Basics   Tags   Review and Create

**Project details**

Subscription \*  (New) NimoAVSDemo

Resource group \*

**Private cloud details**

Resource name \*

Location \*

Size of host \*

Number of hosts \*  Find out how many hosts you need

There is no metering for the selected subscription, region, and SKU. No cost data to display.

**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 vnets or on-premise networks.

Address block for private cloud \*

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、デプロイが成功したことを確認します。デプロイが完了すると、「成功」というステータスが表示されます。

Azure VMware Solution プライベート クラウドには、Azure Virtual Network が必要です。Azure VMware Solution 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 回線と仮想ネットワーク ゲートウェイの設定も必要です。クラスターのプロビジョニングが完了するまで待機中に、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 Solution に接続します。

Home >

 **nimoavsppriv**

**Essentials**

|   |  |
|---|--|
| Resource group (change)<br>NimoAVSDemo                  | Address block for private cloud<br>10.21.0.0/22  |
| Status<br>Succeeded                                     | Primary peering subnet<br>10.21.0.232/30         |
| Location<br>East US 2                                   | Secondary peering subnet<br>10.21.0.236/30       |
| Subscription (change)<br>SaaS Backup Production         | Private Cloud Management network<br>10.21.0.0/26 |
| Subscription ID<br>b58a041a-e464-4497-8be9-9048369ee8e1 | vMotion network<br>10.21.1.128/25                |
| Tags (change)<br>Click here to add tags                 | Number of hosts<br>3                             |

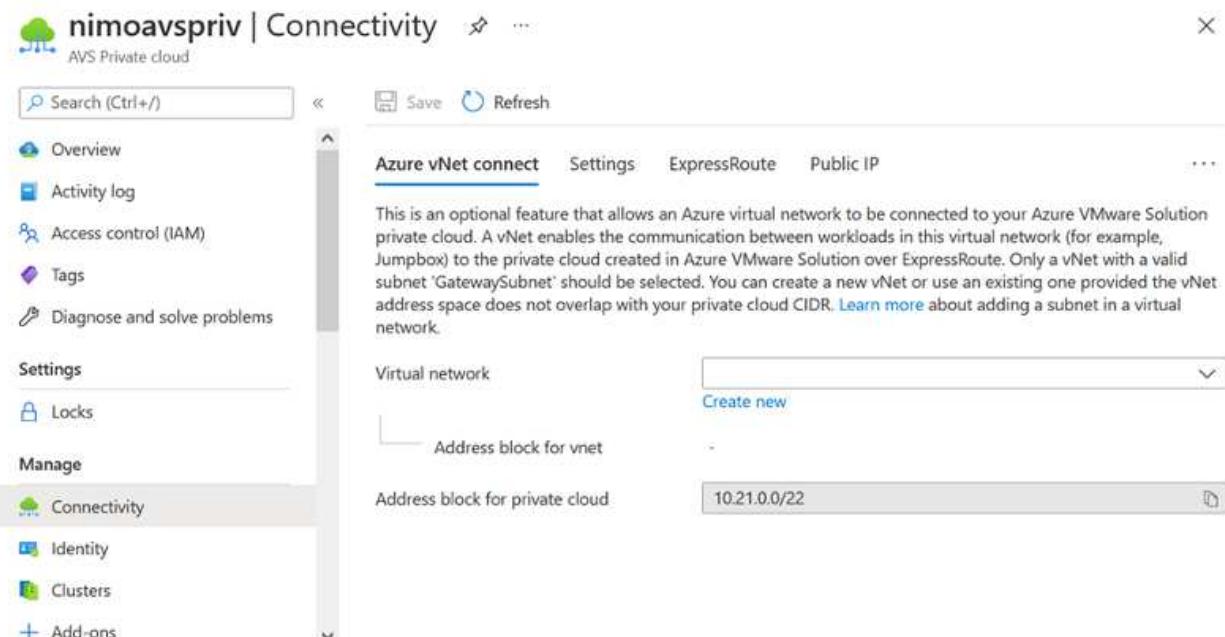
## 新規または既存の ExpressRoute 仮想ネットワーク ゲートウェイに接続する

新しい Azure 仮想ネットワーク (VNet) を作成するには、Azure VNet Connect タブを選択します。または、Azure ポータルから仮想ネットワークの作成ウィザードを使用して手動で作成することもできます。

1. Azure VMware Solution プライベート クラウドに移動し、[管理] オプションの [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、[新規作成] オプションを選択します。

この機能により、VNet を Azure VMware Solution プライベート クラウドに接続できるようになります。VNet は、ExpressRoute 経由で Azure VMware Solution に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、Cloud Volume ONTAPなど) を自動的に作成することにより、この仮想ネットワーク内のワークロード間の通信を可能にします。

注: VNet アドレス空間は、プライベート クラウド CIDR と重複しないでください。



4. 新しい VNet の情報を指定または更新し、[OK] を選択します。

## Create virtual network

X

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="checkbox"/>               | (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="checkbox"/>               | <input type="checkbox"/> | (0 Addresses)   |

指定されたアドレス範囲とゲートウェイ サブネットを持つ VNet が、指定され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 とゲートウェイの種類として ExpressRoute を使用して仮想ネットワーク ゲートウェイを作成します。デプロイが完了したら、承認キーを使用して、ExpressRoute 接続を Azure VMware Solution 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、以下を参照してください。 "[Azure で VMware プライベート クラウドのネットワークを構成する](#)"。

## Azure VMware Solution プライベート クラウドへのネットワーク接続とアクセスを検証します

Azure VMware Solution では、オンプレミスの VMware vCenter を使用してプライベート クラウドを管理することはできません。代わりに、Azure VMware Solution vCenter インスタンスに接続するにはジャンプ ホストが必要です。指定されたリソース グループにジャンプ ホストを作成し、Azure VMware Solution 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 である必要があります、vCenter と NSX Manager の両方へのアクセスを提供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](#)

仮想マシンがプロビジョニングされたら、[接続] オプションを使用して RDP にアクセスします。

The screenshot shows the Azure portal interface for a virtual machine named 'nimAVSJH'. On the left, there's a sidebar with navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, Connect (which is selected), Disks, and Size. The main content area has a search bar at the top. A warning message says: 'To improve security, enable just-in-time access on this VM.' Below it, there are tabs for RDP, SSH, and BASTION, with RDP selected. The 'Connect with RDP' section contains fields for 'IP address' (set to 'Public IP address (52.138.103.135)') and 'Port number' (set to '3389'). A blue 'Download RDP File' button is at the bottom.

クラウド管理者ユーザーを使用して、この新しく作成されたジャンプ ホスト仮想マシンから vCenter にSign in。資格情報にアクセスするには、Azure ポータルに移動し、(プライベート クラウド内の [管理] オプションの下の) [ID] に移動します。プライベート クラウド vCenter および NSX-T Manager の URL とユーザー資格情報はここからコピーできます。

The screenshot shows the Azure portal interface for an AVS Private cloud named 'nimoavsppriv'. On the left, there's a sidebar with navigation links: Access control (IAM), Tags, Diagnose and solve problems, Settings, Locks, Manage, Connectivity, Identity (which is selected), Clusters, Placement policies (preview), and Add-ons. The main content area shows 'Login credentials' and 'vCenter credentials' sections. Under 'vCenter credentials', the 'Web client URL' is set to 'https://10.21.0.2/' and the 'Admin username' is 'cloudadmin@vsphere.local'. Under 'NSX-T Manager credentials', the 'Web client URL' is set to 'https://10.21.0.3/' and the 'Admin username' is 'admin'.

Windows仮想マシンでブラウザを開き、vCenter WebクライアントのURLに移動します。  
("https://10.21.0.2/")にアクセスし、管理者ユーザー名として **cloudadmin@vsphere.local** を使用し、コピーしたパスワードを貼り付けます。同様に、NSX-TマネージャにもWebクライアントURLを使用してアクセスできます。("https://10.21.0.3/")にアクセスし、管理者ユーザー名とコピーしたパスワードを貼り付けて、新しいセグメントを作成したり、既存の層ゲートウェイを変更したりします。



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

The screenshot shows two windows side-by-side. The left window is the VMware vSphere web interface login screen, featuring a large blue and white geometric background graphic. It has fields for 'cloudadmin@vsphere.local' and a password, and a checkbox for 'Use Windows session authentication'. A blue 'LOGIN' button is at the bottom. The right window is the vSphere Client interface, showing a summary of resources for a host named 'vc.beeb9fd29eab4cbea81e62.eastus2.avs.azure.com'. It displays 0 virtual machines and 3 hosts. Resource usage statistics are shown for CPU, Memory, and Storage. Below this is a table of recent tasks, with one entry for 'Undeploy plug-in' which is completed.

Azure VMware Solution SDDC がデプロイされ、構成されました。ExpressRoute Global Reach を活用して、オンプレミス環境を Azure VMware Solution プライベート クラウドに接続します。詳細については、以下を参照してください。["オンプレミス環境を Azure VMware Solution にピアリングする"](#)。

## Google Cloud Platform (GCP) に仮想化環境をデプロイして構成する

オンプレミスの場合と同様に、VM の作成と移行のための本番環境対応環境を正常に構築するには、Google Cloud VMware Engine (GCVE) を計画することが重要です。

このセクションでは、GCVE を設定および管理する方法と、NetAppストレージに接続するために使用可能なオプションと組み合わせて使用する方法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られます。

## GCVE の展開と構成

GCP 上で GCVE 環境を構成するには、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。

「新しいプライベート クラウド」ボタンをクリックし、GCVE プライベート クラウドの希望する構成を入力します。「場所」では、最高のパフォーマンスと最低のレイテンシを確保するために、NetApp Volumes/CVO がデプロイされているのと同じリージョン/ゾーンにプライベート クラウドをデプロイするようしてください。

### 前提条件

- VMware Engine サービス管理者 IAM ロールを設定する
- "VMWare Engine API アクセスとノードクオータを有効にする"
- CIDR 範囲がオンプレミスまたはクラウドのサブネットと重複していないことを確認してください。CIDR 範囲は /27 以上である必要があります。

The screenshot shows the 'Create Private Cloud' interface. The 'Location' dropdown is highlighted with a red box, displaying 'us-east4 > v-zone-a > VE Placement Group 2'. Other visible fields include:

- Private Cloud name: NIMoGCVE
- Node type: vE1-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 時間ほどかかる場合があります。

## GCVEへのプライベートアクセスを有効にする

プライベート クラウドがプロビジョニングされたら、高スループットと低レイテンシのデータパス接続を実現するために、プライベート クラウドへのプライベート アクセスを構成します。

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。そのためには、"GCPのドキュメント"。Cloud Volume Service の場合、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 Engine と Google Cloud NetApp Volumes 間の接続を確立します。詳細な手順については、こちらを参照してください"リンク"。

| Tenant ID         | Service     | Region       | Routing Mode | Peered Project ID    | Peered VPC        | VPC Peering Status | Region Status |
|-------------------|-------------|--------------|--------------|----------------------|-------------------|--------------------|---------------|
| ke841388caa56b... | VPC Network | europe-west3 | Global       | cv-performance-te... | cloud-volumes-vpc | ● Active           | ● Connected   |
| jbd29510b3ebbf... | NetApp CVS  | europe-west3 | Global       | y2b6c17202af6dc...   | netapp-tenant-vpc | ● Active           | ● Connected   |

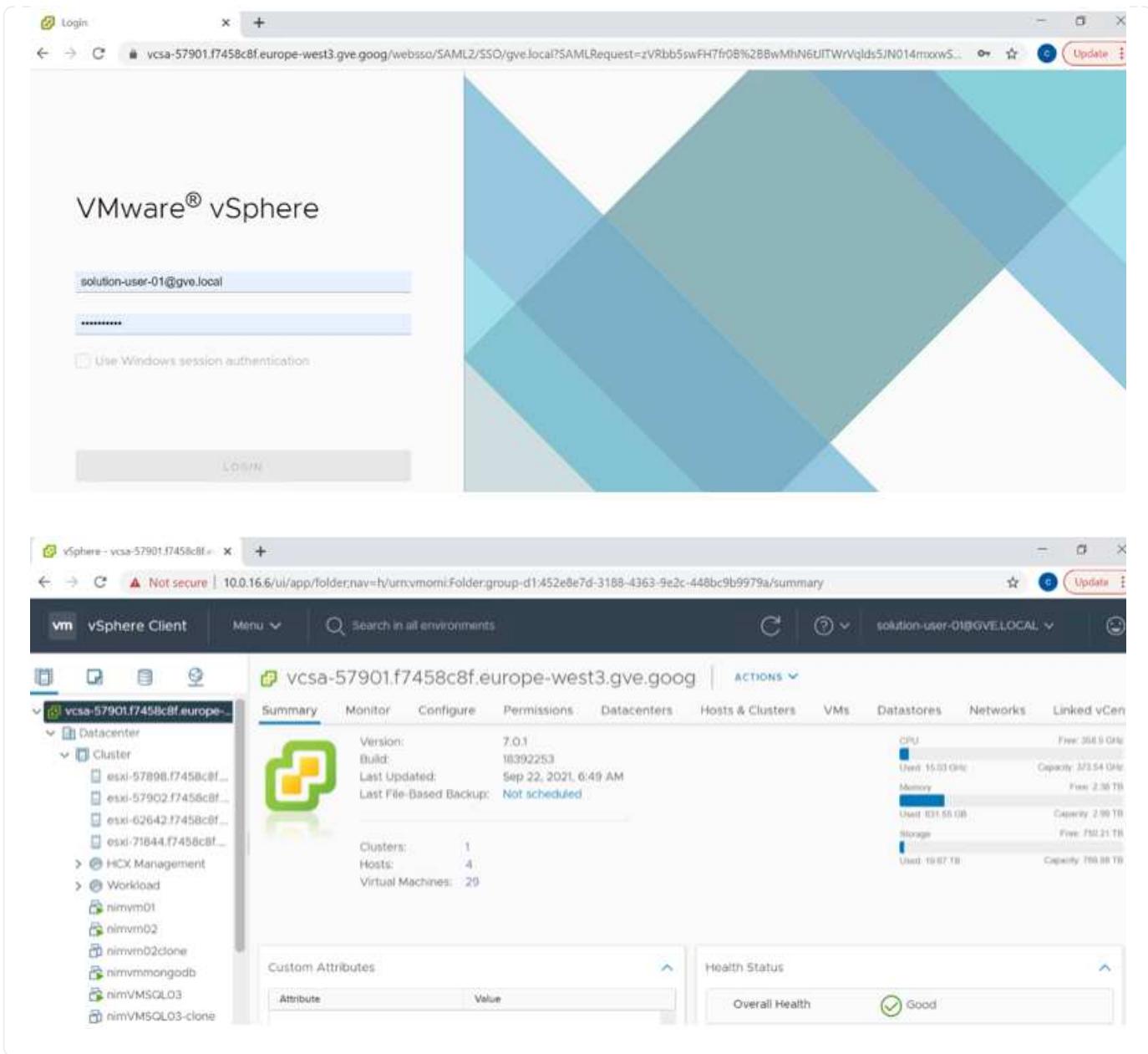
[CloudOwner@gve.local](#) ユーザーを使用して vCenter にSign in。認証情報にアクセスするには、VMware Engine ポータルにアクセスし、[リソース] に移動して、適切なプライベート クラウドを選択します。[基本情報] セクションで、vCenter ログイン情報 (vCenter Server、HDX Manager) または NSX-T ログイン情報 (NSX Manager) の [表示] リンクをクリックします。

The screenshot shows the Google Cloud VMware Engine interface. On the left, there's a sidebar with icons for Home, Resources, Network, Activity, and Account. The main area is titled 'gcve-cvs-hw-eu-west3' and has tabs for SUMMARY, CLUSTERS, SUBNETS, ACTIVITY, VS SPHERE MANAGEMENT NETWORK, ADVANCED VCENTER SETTINGS, and DNS CONFIGURATION. Under the SUMMARY tab, it shows basic info like Name (gcve-cvs-hw-eu-west3), Status (Operational), Location (europe-west3 > v-zone-a > VE Placement Group 1), and Cloud Monitoring. It also lists Clusters (1), vSphere/vSAN subnets CIDR range (10.0.16.0/24), and NSX-T login info. Under Capacity, it shows 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クライアントのURLに移動します。

("<https://10.0.16.6/>") にアクセスし、管理者ユーザー名として [CloudOwner@gve.local](#) を使用し、コピーしたパスワードを貼り付けます。同様に、NSX-TマネージャにもWebクライアントURLを使用してアクセスできます。("https://10.0.16.11/") にアクセスし、管理者ユーザー名とコピーしたパスワードを貼り付けて、新しいセグメントを作成したり、既存の層ゲートウェイを変更したりします。

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には、適切な接続のためにクラウド VPN または Cloud Interconnect を活用し、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、こちらを参照してください"リンク"。



Google Cloud NetApp Volumes補足データストアを GCVE にデプロイする

参考する["NetApp Volumes を使用した追加の NFS データストアを GCVE に展開する手順"](#)

## パブリッククラウドにおけるNetAppストレージ

パブリッククラウドプロバイダー向けのNetAppストレージオプション

3大ハイパースケーラーにおけるストレージとしてのNetAppのオプションを検討します。

## AWS / VMC

AWS は、次の構成でNetAppストレージ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
- ・ゲスト接続ストレージとしてのCloud Volumes ONTAP (CVO)
- ・補助的なNFSデータストアとしてのFSx ONTAP

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

## Azure / AVS

Azure は、次の構成のNetAppストレージをサポートしています。

- ・ゲスト接続ストレージとしてのAzure NetApp Files (ANF)
- ・ゲスト接続ストレージとしてのCloud Volumes ONTAP (CVO)
- ・補助的な NFS データストアとしてのAzure NetApp Files (ANF)

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

## GCP / GCVE

Google Cloud は、次の構成のNetAppストレージをサポートしています。

- ・ゲスト接続ストレージとしてのCloud Volumes ONTAP (CVO)
- ・ゲスト接続ストレージとしてのGoogle Cloud NetApp Volumes (NetApp Volumes)
- ・補助的な NFS データストアとしてのGoogle Cloud NetApp Volumes (NetApp Volumes)

詳細を表示["GCVE のゲスト接続ストレージ オプション"](#)。 詳細を表示["GCVE の補足 NFS データストア オプション"](#)。

詳細はこちら["Google Cloud NetApp Volumesデータストアのサポート \(NetAppブログ\)"](#)または["Google Cloud NetApp Volumes を Google Cloud VMware Engine のデータストアとして使用する方法 \(Google ブログ\)"](#)

## Amazon Web Services: NetAppストレージを使用するためのオプション

NetAppストレージは、ゲスト接続ストレージまたは補助ストレージとして Amazon Web Services に接続できます。

### 補助的な NFS データストアとしてのAmazon FSx for NetApp ONTAP (FSx ONTAP)

Amazon FSx ONTAP は、データ要件をアプリケーション層にシームレスに適用することで TCO を削減しながら、ファイルサービスとともにアプリケーションワークロードをデプロイおよび管理するための優れたオプションを提供します。ユースケースに関係なく、VMware Cloud on AWS と Amazon FSx ONTAPを併せて選択すると、クラウドのメリットの迅速な実現、オンプレミスから AWS への一貫したインフラストラクチャと運用、ワークロードの双向の移植性、エンタープライズ グレードの容量とパフォーマンスが得られます。

これは、ストレージを接続するために使用される、使い慣れたプロセスと手順と同じです。

詳細については、以下をご覧ください。

- ・ "補足的な NFS データストアとしての FSx ONTAP : 概要"
- ・ "Amazon FSx for ONTAPを補助データストアとして"

### ゲスト接続ストレージとしてのAmazon FSx for NetApp ONTAP

Amazon FSx ONTAP は、NetApp の人気のONTAPファイルシステム上に構築された、信頼性が高く、スケーラブルで、高性能かつ機能豊富なファイルストレージを提供するフルマネージドサービスです。 FSx ONTAP は、NetApp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操作と、完全に管理された AWS サービスの俊敏性、拡張性、シンプルさを兼ね備えています。

FSx ONTAP は、AWS またはオンプレミスで実行されている Linux、Windows、macOS コンピューティングインスタンスから広くアクセスできる、機能豊富で高速かつ柔軟な共有ファイルストレージを提供します。 FSx ONTAP は、1 ミリ秒未満のレイテンシを備えた高性能ソリッド ステート ドライブ (SSD) ストレージを提供します。 FSx ONTAPを使用すると、データのごく一部に対してのみ SSD ストレージ料金を支払いながら、ワークロードに対して SSD レベルのパフォーマンスを実現できます。

FSx ONTAPを使用すると、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、クローン、複製ができるため、データの管理が簡単になります。さらに、FSx ONTAP はデータを低成本で弾力性のあるストレージに自動的に階層化するため、容量のプロビジョニングや管理の必要性が軽減されます。

FSx ONTAP は、完全に管理されたバックアップとリージョン間の災害復旧のサポートを備えた、可用性と耐久性に優れたストレージも提供します。データの保護とセキュリティ確保を容易にするために、FSx ONTAP は一般的なデータ セキュリティおよびウイルス対策アプリケーションをサポートしています。

詳細については、"ゲスト接続ストレージとしての FSx ONTAP"

### ゲスト接続ストレージとしてのCloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP(CVO) は、NetApp のONTAPストレージ ソフトウェア上に構築された業界をリードするクラウド データ管理ソリューションであり、Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP) でネイティブに利用できます。

これはクラウドネイティブストレージを使用するONTAPのソフトウェア定義バージョンであり、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、データを管理するためのまったく新しい方法について IT スタッフを再トレーニングする必要性が軽減されます。

CVO により、エッジからデータセンター、クラウドへとシームレスにデータを移動し、ハイブリッド クラウドを統合することが可能になります。これらはすべて、単一ペインの管理コンソールであるNetApp Cloud Manager で管理されます。

CVO は設計上、クラウドで最も要求の厳しいアプリケーションにも対応できる極めて優れたパフォーマンスと高度なデータ管理機能を提供します。

詳細については、"ゲスト接続ストレージとしてのCVO"。

## TR-4938: VMware Cloud on AWS でAmazon FSx ONTAP をNFS データストアとしてマウントする

このドキュメントでは、VMware Cloud on AWS を使用してAmazon FSx 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。

はじめに

成功している組織はすべて、変革と近代化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 投資を活用してクラウドのメリットを活用し、プロセスを可能な限りシームレスに移行、バースト、拡張し、災害復旧を提供する方法を検討します。クラウドに移行する顧客は、弾力性とバースト、データセンターの廃止、データセンターの統合、サポート終了のシナリオ、合併、買収などのユースケースを評価する必要があります。

VMware Cloud on AWS は、顧客に独自のハイブリッド機能を提供するため、大多数の顧客が好むオプションですが、ネイティブストレージオプションが限られているため、ストレージを多用するワークロードを持つ組織にとってはそ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結び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あり、これによりストレージを集中的に使用するワークロードのコストが 35 ~ 40% 以上増加する可能性があります。これらのワークロードには、追加の処理能力ではなく、追加のストレージと分離されたパフォーマンスが必要ですが、追加のホストに対して料金を支払う必要があります。ここで、"最近の統合" FSx ONTAPは、VMware Cloud on AWS でのストレージとパフォーマンス集約型のワークロードに役立ちます。

次のシナリオを考えてみましょう。顧客は処理能力 (vCPU/vMem) のために 8 台のホストを必要としていますが、ストレージについてもかなりの要件があります。評価によると、ストレージ要件を満たすには 16 台のホストが必要です。これにより、実際に必要なのはストレージの増設だけなのに、追加の処理能力をすべて購入する必要があるため、全体的な TCO が増加します。これは、移行、災害復旧、バースト、開発/テストなど、あらゆるユースケースに適用できます。

このドキュメントでは、VMware Cloud on AWS の NFS データストアとして FSx ONTAP をプロビジョニングして接続するために必要な手順について説明します。



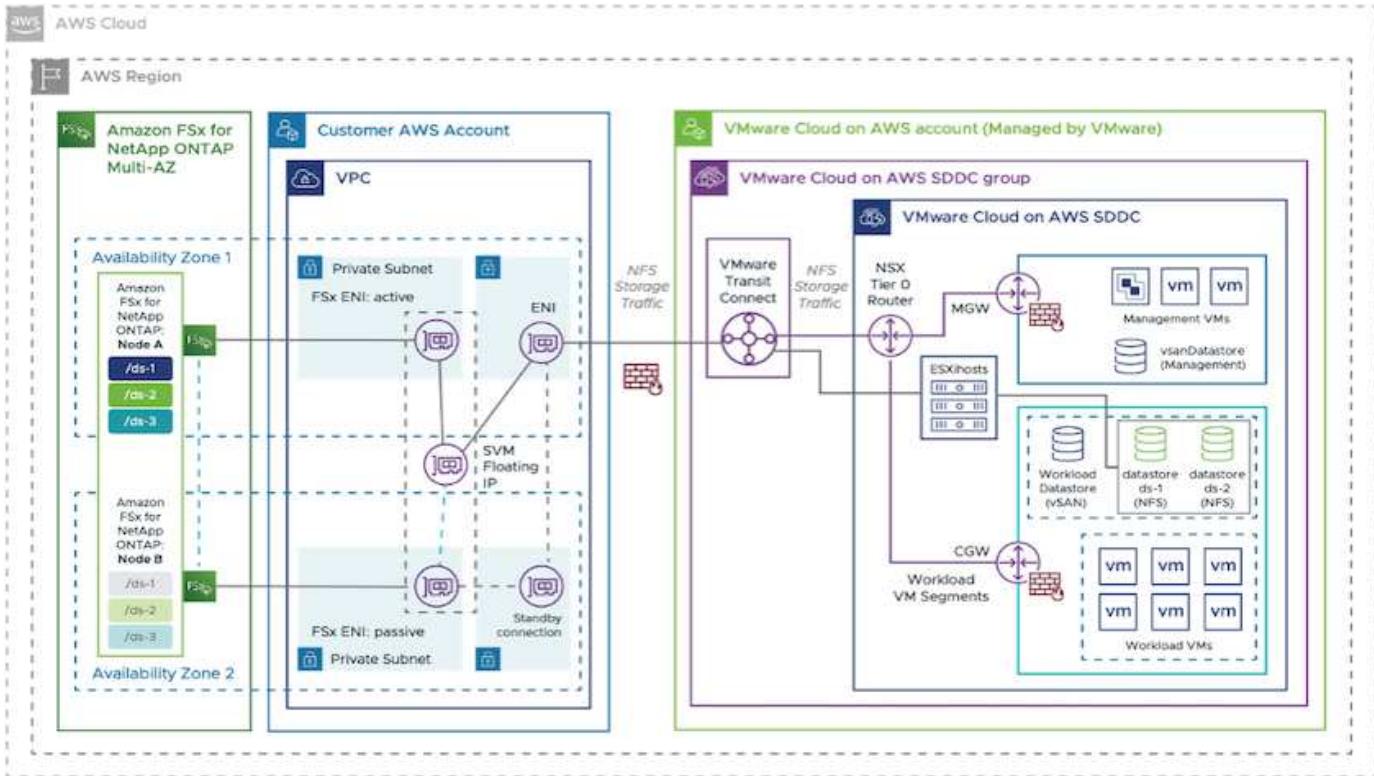
このソリューションは VMware からも入手できます。こちらをご覧ください"VMware Cloud on AWS ドキュメント"詳細についてはこちらをご覧ください。

接続オプション



VMware Cloud on AWS は、FSx ONTAP のマルチ AZ とシングル AZ の両方のデプロイメントをサポートしています。

このセクションでは、ホストを追加せずに SDDC クラスター内のストレージを拡張するソリューションを実装するために必要な手順とともに、高レベルの接続アーキテクチャについて説明します。



大まかな展開手順は次のとおりです。

1. 新しく指定された VPC にAmazon FSx 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 アタッチメントを作成します。
4. ルーティング (AWS VPC および SDDC) とセキュリティ グループを構成します。
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。

FSx ONTAP 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 VMware on Cloud SDDC 環境をセットアップするか、既存の SDDC を v1.20 以上にアップグレードする必要があります。詳細については、 "[VMware Cloud on AWS を使い始める](#)"。



FSx ONTAPは現在、ストレッチ クラスター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、VMware Cloud on AWS を使用してAmazon FSx ONTAPを構成するために必要な手順について説明します。Amazon FSx ONTAP は、データ要件をアプリケーション層にシームレスに適用することで TCO を削減しながら、ファイルサービスとともにアプリケーションワークロードをデプロイおよび管理するための優れたオプションを提供します。ユースケースに関係なく、VMware Cloud on AWS とAmazon FSx ONTAPを併せて選択すると、クラウドのメリットの迅速な実現、オンプレミスから AWS への一貫したインフラストラクチャと運用、ワークロードの双方向の移植性、エンタープライズ グレードの容量とパフォーマンスが実現します。これは、ストレージを接続するために使用される、使い慣れたプロセスと手順と同じです。覚えておいてください、新しい名前とともに変更されたのはデータの位置だけです。ツールとプロセスはすべて同じままで、Amazon FSx ONTAP は全体的なデプロイメントの最適化に役立ちます。

このプロセスについて詳しく知りたい場合は、詳細なウォークスルービデオをご覧ください。

## AWS で補足 NFS データストアを作成する

VMware Cloud の準備が整い、AWS VPC に接続されたら、元の接続済みまたは既存のデフォルト VPC ではなく、新しく指定した VPC にAmazon FSx ONTAPをデプロイする必要があります。

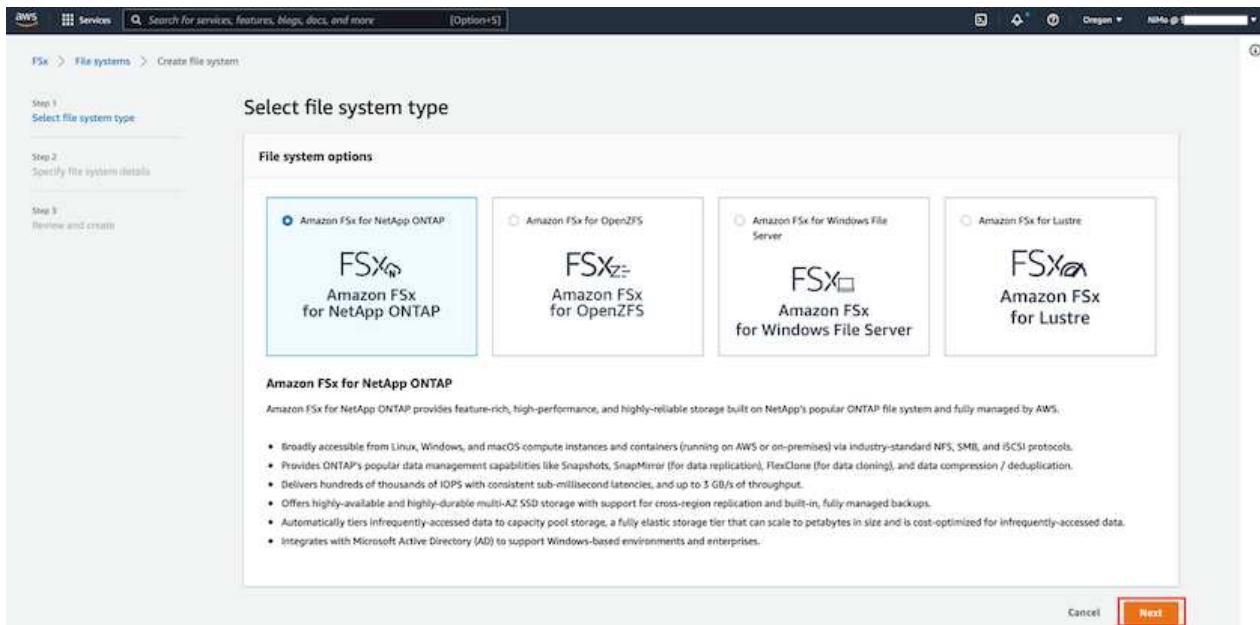
まず、SDDC が存在するのと同じリージョンとアベイラビリティーゾーンに追加の VPC をデプロイし、新しい VPC にAmazon FSx ONTAP をデプロイします。["VMware Cloud における SDDC グループの構成"](#)コンソールは、FSx ONTAPがデプロイされる新しく指定された VPC に接続するために必要なネットワーク構成オプションを有効にします。

- i FSx ONTAP をVMware Cloud on AWS SDDC と同じアベイラビリティーゾーンにデプロイします。
- i 接続された VPC に FSx ONTAPをデプロイすることはできません。代わりに、新しい指定された VPC にデプロイし、SDDC グループを介して VPC を VMware Managed Transit Gateway (vTGW) に接続する必要があります。

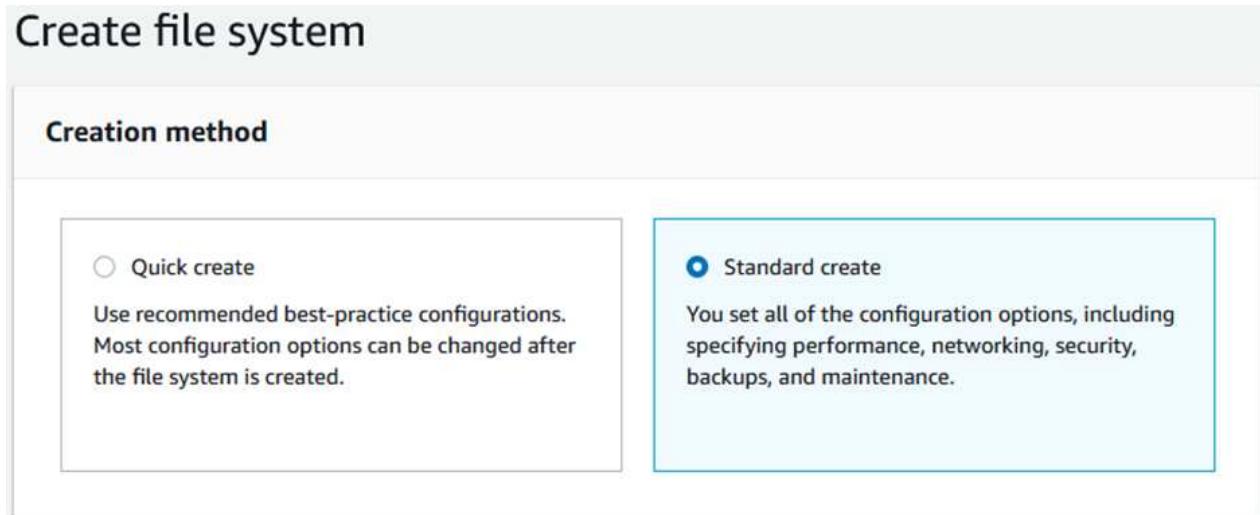
## ステップ 1: 新しい指定 VPC にAmazon FSx ONTAPを作成する

Amazon FSx ONTAPファイルシステ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. Amazon FSxコンソールを開きます [https://console.aws.amazon.com/fsx/\\*](https://console.aws.amazon.com/fsx/*) ファイルシステムの作成\*を選択して、\*ファイルシステムの作成\*ウィザードを開始します。
2. [ファイルシステム タイプの選択] ページで、\* Amazon FSx ONTAP\* を選択し、次へをクリックします。 ファイルシステムの作成 ページが表示されます。



3. 作成方法としては\*標準作成\*を選択します。



## File system details

File system name - optional [Info](#)

FSxONTAPDatastoreFS

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

Deployment type [Info](#)

- Multi-AZ
- Single-AZ

SSD storage capacity [Info](#)

2048

Minimum 1024 GiB; Maximum 192 TiB.

Provisioned SSD IOPS

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

- Automatic (3 IOPS per GiB of SSD storage)
- User-provisioned

40000

Maximum 80,000 IOPS

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.

- Recommended throughput capacity  
128 MB/s
- Specify throughput capacity

Throughput capacity

2048 MB/s



データストアのサイズは顧客ごとにかなり異なります。 NFS データストアあたりの仮想マシンの推奨数は主観的ですが、各データストアに配置できる仮想マシンの最適な数は多くの要因によって決まります。ほとんどの管理者は容量のみを考慮しますが、VMDK に送信される同時 I/O の量は、全体的なパフォーマンスにとって最も重要な要素の 1 つです。オンプレミスのパフォーマンス統計を使用して、それに応じてデータストアのボリュームのサイズを決定します。

4. 仮想プライベートクラウド (VPC) のネットワーク セクションで、適切な VPC と優先サブネット、およびルートテーブルを選択します。この場合、ドロップダウン メニューから Demo-FSxforONTAP-VPC が選択されます。



これが接続された VPC ではなく、指定された新しい VPC であることを確認してください。



デフォルトでは、FSx ONTAP はファイルシステムのデフォルトのエンドポイント IP アドレス範囲として 198.19.0.0/16 を使用します。エンドポイント IP アドレス範囲が、AWS SDDC、関連付けられた VPC サブネット、オンプレミスインフラストラクチャ上の VMC と競合しないことを確認します。不明な場合は、競合のない重複しない範囲を使用してください。

## Network & security

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

Specify the VPC from which your file system is accessible.

Demo-FsxforONTAP-VPC | vpc-

7

▼

### VPC Security Groups [Info](#)

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

Choose VPC security group(s)

▼

sg-0d

t) X

### Preferred subnet [Info](#)

Specify the preferred subnet for your file system.

DemoFSxONTAP-Sub02 | subnet-0

3 (us-west-2b)

▼

### Standby subnet

DemoFSxONTAP-Sub01 | subnet-1

(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

3.3.0.0/24

Enter a selected IP range

5. 暗号化キーのセキュリティと暗号化セクションで、保存中のファイルシステムのデータを保護する AWS Key Management Service (AWS KMS) 暗号化キーを選択します。ファイルシステム管理パスワードには、fsxadmin ユーザーの安全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 key that protects my FSx resources when no other key is defined | 402     | 6-         |

### 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

6. \*デフォルトのストレージ仮想マシン構成\*セクションで、SVM の名前を指定します。



GA 時点では、4 つの NFS データストアがサポートされています。

## Default storage virtual machine configuration

### Storage virtual machine name

FSxONTAPDatastoreSVM

### 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

### 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

7. デフォルトのボリューム構成\*セクションで、データストアに必要なボリューム名とサイズを指定し、\*次へ\*をクリックします。これは **NFSv3** ボリュームである必要があります。\*ストレージ効率では、有効を選択して、ONTAPストレージ効率機能(圧縮、重複排除、および圧縮)をオンにします。作成後、シェルを使用して、次のように **volume modify** を使用してボリューム パラメータを変更します。

| 設定               | 構成                        |
|------------------|---------------------------|
| ボリューム保証（スペース保証型） | なし（シンプロビジョンング） – デフォルトで設定 |
| 部分準備金（部分準備金）     | 0% – デフォルトで設定             |

| 設定                              | 構成                    |
|---------------------------------|-----------------------|
| snap_reserve (スナップショット領域のパーセント) | 0%                    |
| 自動サイズ調整 (autosize-mode)         | grow_shrink           |
| ストレージ効率                         | 有効 – デフォルトで設定されています   |
| 自動削除                            | 巻 / 古い順               |
| ボリューム階層化ポリシー                    | スナップショットのみ – デフォルトで設定 |
| try_first                       | 自動拡張                  |
| スナップショットポリシー                    | なし                    |

ボリュームを作成および変更するには、次の SSH コマンドを使用します。

シェルから新しいデータストアボリュームを作成するコマンド:

```
volume create -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-aggregate aggr1 -size 1024GB -state online -tiering-policy
snapshot-only -percent-snapshot-space 0 -autosize-mode grow
-snapshot-policy none -junction-path /DemoDS002
```

注意: シェル経由で作成されたボリュームが AWS コンソールに表示されるまでには数分かかります。

デフォルトで設定されていないボリュームパラメータを変更するコマンド:

```
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-fractional-reserve 0
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002 -space
-mgmt-try-first vol_grow
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-autosize-mode grow
```

## Default volume configuration

### Volume name

DemoDS01

Maximum of 203 alphanumeric characters, plus \_.

### Junction path

/DemoDS01

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

### Volume size

2048000



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.

Snapshot Only



## ▼ Backup and maintenance - optional

### Daily automatic backup [Info](#)

Amazon FSx can protect your data through daily backups

Enabled

Disabled

### Weekly maintenance window [Info](#)

When patching needs to be performed, Amazon FSx performs maintenance on your file system only during this window.

No preference

Select start time for 30-minute weekly maintenance window

## ► Tags - optional

Cancel

Back

Next



初期移行シナリオでは、デフォルトのスナップショット ポリシーにより、データストアの容量不足の問題が発生する可能性があります。これを克服するには、ニーズに合わせてスナップショット ポリシーを変更します。

8. ファイルシステムの作成 ページに表示されるファイル システム構成を確認します。

9. \*ファイルシステムの作成\*をクリックします。

The screenshot shows the AWS FSx console interface. In the top navigation bar, 'File systems' is selected under 'FSx'. A search bar at the top left contains the placeholder 'Filter file systems'. On the right side of the header, there are buttons for 'Create file system', 'Attach', and 'Actions'. Below the header is a table titled 'File systems (2)'. The table has columns: 'File system name', 'File system ID', 'File system type', 'Status', 'Deployment type', 'Storage type', 'Storage capacity', 'Throughput capacity', and 'Creation time'. The first row shows a file system named 'fs-0971...' with an ID of 'fs-0971...', type 'ONTAP', status 'Creating', deployment 'Multi-AZ', storage 'SSD', and creation time '2022-09-12T15:19:06+01:00'. The second row is partially visible. At the bottom of the main content area, a green banner displays the message 'fs-0971d5cad638c5cb93 is now available'. To the left of the main content area is a sidebar titled 'Amazon FSx' with a 'File systems' section containing links for 'Volumes', 'Backups', 'ONTAP', 'OpenZFS', 'Solutions', 'Windows File Server', 'Lustre', and 'Data repository tasks'. Below this is a link for 'FSx on Service Quotas'.



容量とパフォーマンスの要件に応じて、前の手順を繰り返して、さらにストレージ仮想マシンまたはファイルシステムとデータストアボリュームを作成します。

Amazon FSx ONTAPのパフォーマンスについては、以下を参照してください。 ["Amazon FSx ONTAP のパフォーマンス"](#)。

## ステップ2: SDDCグループを作成する

ファイルシステムと SVM が作成されたら、VMware コンソールを使用して SDDC グループを作成し、VMware Transit Connect を構成します。これを行うには、次の手順を実行します。VMware Cloud コンソールと AWS コンソール間を移動する必要があることに注意してください。

1. VMCコンソールにログインします <https://vmc.vmware.com>。
2. \*インベントリ\*ページで、\*SDDC グループ\*をクリックします。
3. **SDDC グループ**タブで、アクションをクリックし、**SDDC グループの作成**を選択します。デモ的目的で、SDDCグループは FSxONTAPDatastoreGrp。
4. [メンバーシップ] グリッドで、グループメンバーとして含める SDDC を選択します。

### < Add SDDCs

Select which SDDC(s) you want to add to the group.

| Name         | Sddc Id                              | Location         | Version   | Management CIDR |
|--------------|--------------------------------------|------------------|-----------|-----------------|
| FSxNDemoSDDC | c6baecd9-e01b-41d5-89e2-1f095d719a0d | US West (Oregon) | 1.18.0.14 | 172.30.160.0/23 |

Items per page: 100 1 - 1 of 1 items

**ADD SDDCS** CANCEL

5. 「グループに VMware Transit Connect を構成すると、添付ファイルとデータ転送ごとに料金が発生します」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。このプロセスは完了するまでに数分かかる場合があります。

VMware Cloud

FSxONTAPDatastoreGrp

Summary vCenter Linking Direct Connect External VPC External TGW Routing Support

Description: SDDC group for demo purposes

Transit Connect Status: CONNECTED

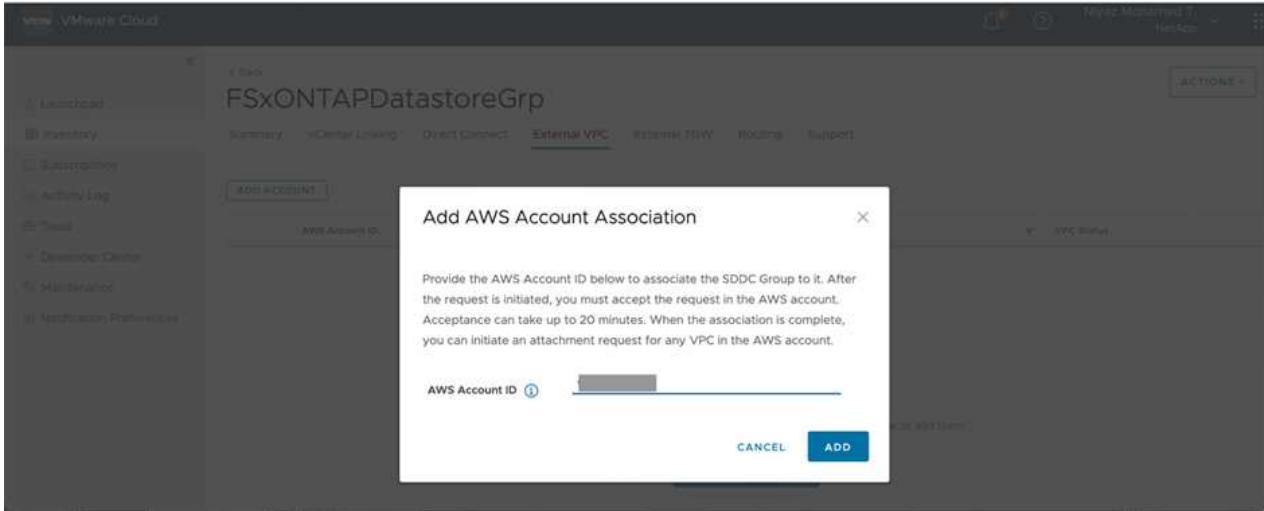
SDDCs

ADD SDDCS REMOVE SDDCS

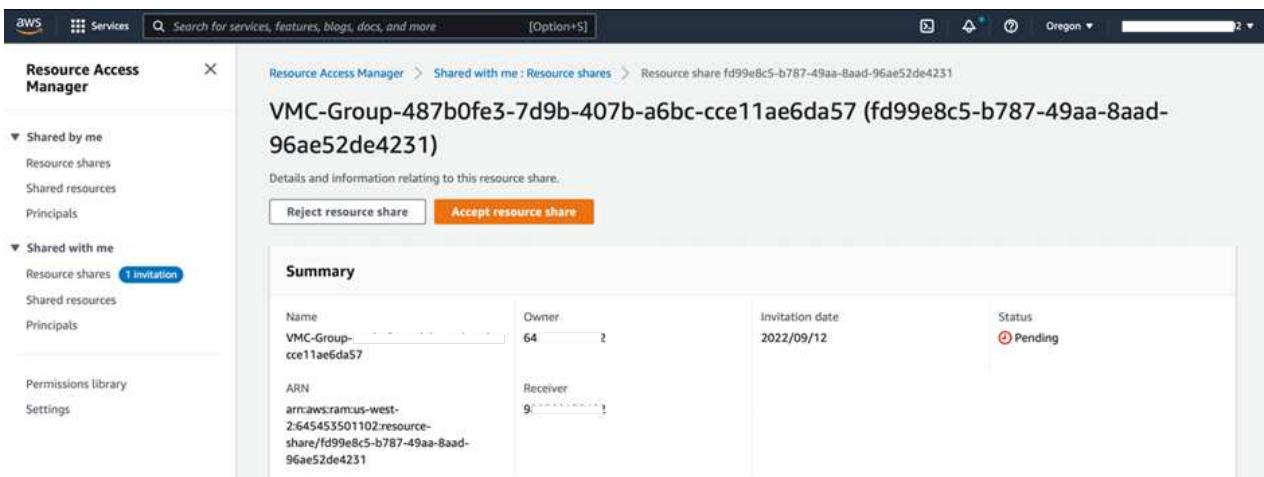
| Name         | SDDC ID                              | SDDC Version | Management CIDR | Location         | Connectivity Status |
|--------------|--------------------------------------|--------------|-----------------|------------------|---------------------|
| FSxNDemoSDDC | c6baecd9-e01b-41d5-89e2-1f095d719a0d | 1.18.0.14    | 172.30.160.0/23 | US West (Oregon) | CONNECTED           |

### ステップ3: VMware Transit Connectを構成する

- 新しく作成した指定 VPC を SDDC グループに接続します。 \*外部VPC\*タブを選択し、 "外部VPCをグループに接続する手順"。このプロセスは完了するまでに 10 ~ 15 分かかる場合があります。



- \*アカウントを追加\*をクリックします。
  - FSx ONTAPファイルシステムのプロビジョニングに使用された AWS アカウントを提供します。
  - \*[追加]\*をクリックします。
- AWS コンソールに戻り、同じ AWS アカウントにログインして、Resource Access Manager サービスページに移動します。リソース共有を受け入れるためのボタンがあります。



外部 VPC プロセスの一環として、AWS コンソールから Resource Access Manager を介して新しい共有リソースへのプロンプトが表示されます。共有リソースは、VMware Transit Connect によって管理される AWS Transit Gateway です。

- \*リソース共有を承認\*をクリックします。

The screenshot shows the VMware Cloud interface. On the left, there's a sidebar with options like Launchpad, Inventory, Subscriptions, Activity Log, Tools (Developer Center, Maintenance), and Notification Preferences. The main area has a title 'FSxONTAPDatastoreGrp' and tabs for Summary, vCenter Linking, Direct Connect, External VPC (which is selected), External TGW, Routing, and Support. Below the tabs is a table with columns: AWS Account ID, Resource Share Name, State, and VPC Status. One row is visible: AWS Account ID is '02...', Resource Share Name is 'VMC-Group-487', State is 'ASSOCIATED', and VPC Status is '...'. There are 'ADD ACCOUNT' and 'REMOVE' buttons above the table. A small 'SUBSCRIBED' badge is on the right.

5. VMC コンソールに戻ると、外部 VPC が関連付けられた状態になっていることがわかります。表示されるまで数分かかる場合があります。

#### ステップ4: トランジットゲートウェイアタッチメントを作成する

1. AWS コンソールで、VPC サービスページに移動し、FSx ファイルシステムのプロビジョニングに使用された VPC に移動します。ここでは、右側のナビゲーションペインで **Transit Gateway Attachment** をクリックして、トランジットゲートウェイアタッチメントを作成します。
2. **VPC アタッチメント** で、DNS サポートがチェックされていることを確認し、FSx ONTAP がデプロイされている VPC を選択します。

The screenshot shows the 'Create transit gateway attachment' wizard. In the 'Details' section, a name tag 'fsxontap-tgw-attach-01' is entered, and the transit gateway ID is set to 'tgw-0d'. The attachment type is selected as 'VPC'. In the 'VPC attachment' section, 'DNS support' is checked, while 'IPv6 support' is unchecked.

3. \*トランジットゲートウェイアタッチメントの作成\*をクリックします。

The screenshot shows the 'Create transit gateway attachment' wizard. It lists the VPC ID 'vpc-05596abe79cb653b7 (Demo-FsxforONTAP-VPC)' and the selected subnets 'us-west-2a' and 'us-west-2b'. Under the 'Tags' section, a tag 'Name' is added with the value 'fsxontap-tgw-attach-01'. At the bottom, there is a 'Create transit gateway attachment' button.

4. VMware Cloud コンソールに戻り、[SDDC グループ] > [外部 VPC] タブに戻ります。FSx に使用する AWS アカウント ID を選択し、VPC をクリックして [承認] をクリックします。

|                       | AWS Account ID | Resource Share Name | State      | VPC Status                         |
|-----------------------|----------------|---------------------|------------|------------------------------------|
| <input type="radio"/> | 96             | VMC-Group-4f        | ASSOCIATED | 0 Available (1 Pending Acceptance) |

| VPC ID | VMC on AWS Region | Transit Gateway Attachment ID | Routes | Status             |
|--------|-------------------|-------------------------------|--------|--------------------|
| vpc-0  | US West (Oregon)  | tgw-attach-0                  | 9      | PENDING ACCEPTANCE |

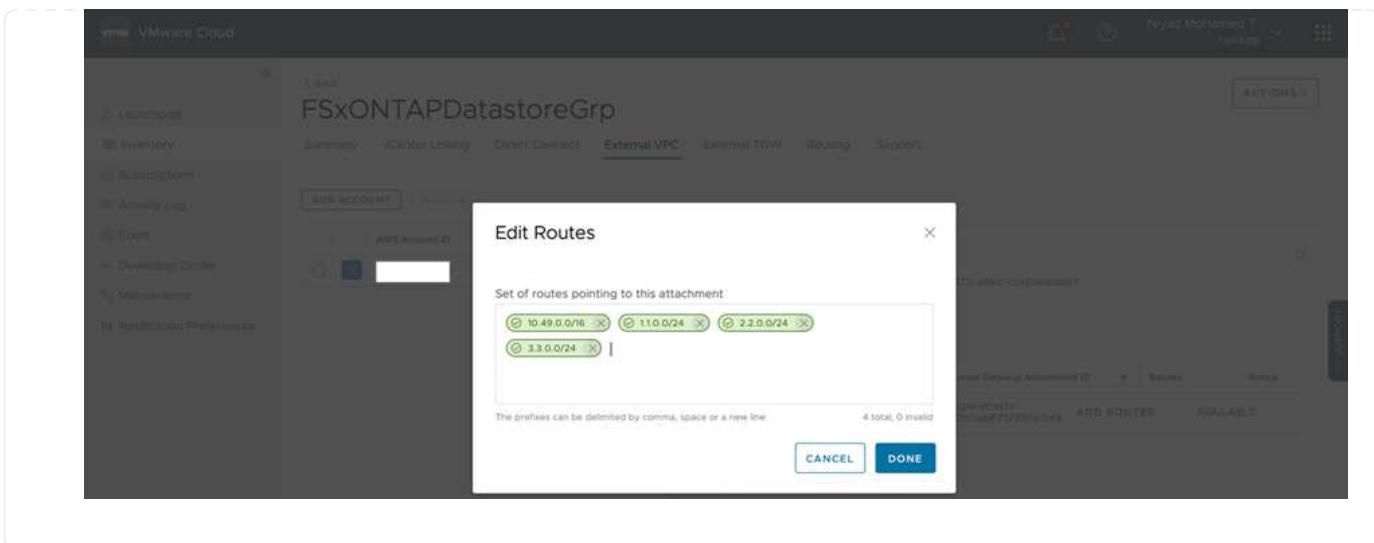


このオプションが表示されるまで数分かかる場合があります。

5. 次に、「外部 VPC」タブの「ルート」列で、「ルートの追加」オプションをクリックし、必要なルートを追加します。

- Amazon FSx ONTAPフローーティング IP のフローーティング IP 範囲のルート。
- 新しく作成された外部 VPC アドレス空間へのルート。

| VPC ID | VMC on AWS Region | Transit Gateway Attachment ID | Routes | Status    |
|--------|-------------------|-------------------------------|--------|-----------|
| vpc-0  | US West (Oregon)  | tgw-attach-0                  | 9      | AVAILABLE |



## ステップ5: ルーティング (AWS VPCとSDDC) とセキュリティグループを構成する

1. AWS コンソールで、VPC サービスページで VPC を見つけて、VPC のメインルートテーブルを選択し、SDDC に戻るルートを作成します。
2. 下部のパネルでルートテーブルを参照し、[ルートの編集] をクリックします。

The screenshot shows the AWS VPC Route Tables page. On the left sidebar, under 'Route tables', 'rtb-Oaaaae5dbc8b7c26cc' is selected. In the main content area, the 'Details' tab is active, showing route table information like 'Route table ID: rtb-Oaaaae5dbc8b7c26cc', 'Main: Yes', and 'Owner ID: 982589175402'. Below this, the 'Routes' tab is selected, showing a table of routes. A red box highlights the 'Edit routes' button at the top right of this table.

3. ルートの編集パネルで、ルートの追加をクリックし、トランジットゲートウェイと関連する TGW ID を選択して、SDDC インフラストラクチャの CIDR を入力します。\*変更を保存\*をクリックします。

The screenshot shows the AWS VPC Route Tables page after a successful update. A green banner at the top says 'Updated routes for rtb-Oaaaae5dbc8b7c26cc successfully'. The 'Routes' tab is selected, showing a table of routes. A red box highlights the last row, which has been updated with a new target 'tgw-0d4'. The status is 'Active' and 'Propagated' is 'No'.

4. 次のステップでは、関連付けられた VPC 内のセキュリティグループが、SDDC グループ CIDR の正しい受信ルールで更新されていることを確認します。
5. SDDC インフラストラクチャの CIDR ブロックを使用して受信ルールを更新します。

The screenshot shows the AWS VPC Security Groups page. The URL is [VPC > Security Groups > sg-0d26f822a764c1075 - default](#). The page displays the details of the default VPC security group, including its name, ID, description, owner, and rule counts. The Inbound rules section lists three rules, with the last one being the newly added NFS traffic rule, which is highlighted with a red border.

| Name | Security group rule... | Port range | Source                 | Description |
|------|------------------------|------------|------------------------|-------------|
| -    | sgr-0a95b39a62c20084c  | All        | 0.0.0.0/0              | -           |
| -    | sgr-03f4bc442a40baade  | All        | sg-0d26f822a764c107... | -           |
| -    | sgr-0011220bb8dfeb1... | All        | 172.30.160.0/23        | -           |

**接続の問題を回避するために、VPC (FSx ONTAP が存在する場所) のルート テーブルが更新されていることを確認します。**

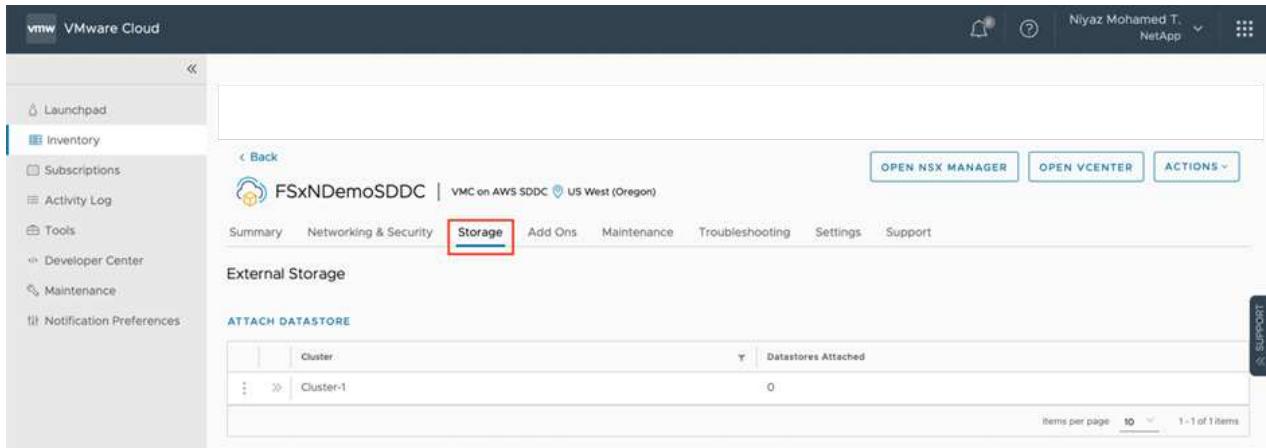
**NFS トラフィックを受け入れるようにセキュリティ グループを更新します。**

これは、適切な SDDC への接続を準備するための最後の手順です。ファイルシステムを構成し、ルートを追加し、セキュリティ グループを更新したら、データストアをマウントします。

## ステップ6: NFSボリュームをデータストアとしてSDDCクラスタに接続する

ファイルシステムがプロビジョニングされ、接続が確立されたら、VMware Cloud Console にアクセスして NFS データストアをマウントします。

1. VMC コンソールで、SDDC のストレージタブを開きます。

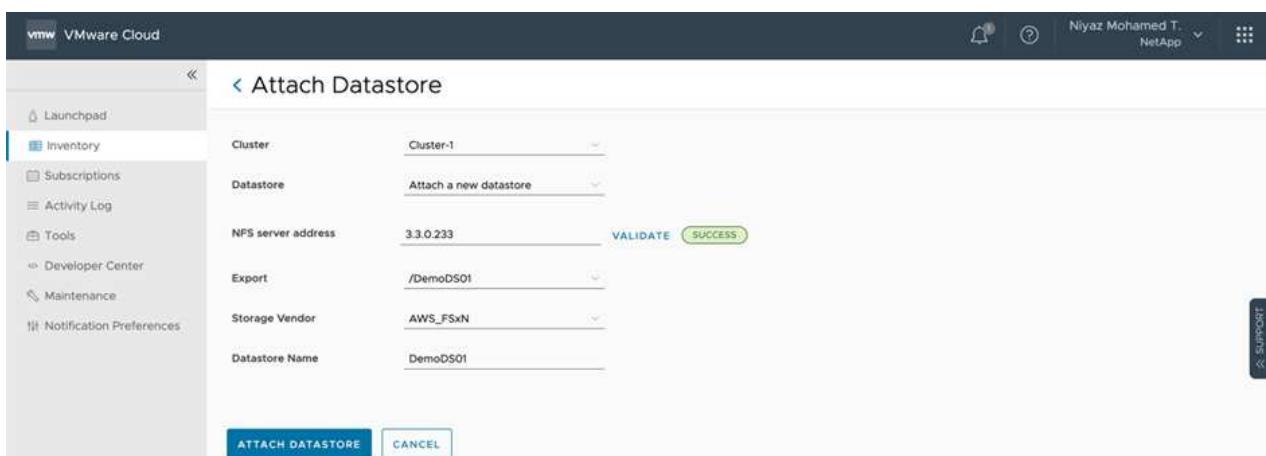


The screenshot shows the VMware Cloud console interface. On the left, the navigation bar includes 'Launchpad', 'Inventory' (which is selected), 'Subscriptions', 'Activity Log', 'Tools', 'Developer Center', 'Maintenance', and 'Notification Preferences'. The main content area displays the 'FSxNDemoSDDC | VMC on AWS SDDC | US West (Oregon)' cluster. The 'Storage' tab is highlighted with a red box. Below it, the 'External Storage' section shows a table titled 'ATTACH DATASTORE' with one entry: 'Cluster-1'. The table has columns for 'Cluster' and 'Datastores Attached'. At the bottom right of the table, there are buttons for 'Items per page' (set to 10) and '1 - 1 of 1 items'. Action buttons at the top right include 'OPEN NSX MANAGER', 'OPEN VCENTER', and 'ACTIONS'.

2. **ATTACH DATASTORE** をクリックし、必要な値を入力します。



NFS サーバー アドレスは、AWS コンソール内の FSx > ストレージ仮想マシンタブ > エンドポイントで確認できる NFS IP アドレスです。



The screenshot shows the 'Attach Datastore' dialog box. The left sidebar lists 'Launchpad', 'Inventory' (selected), 'Subscriptions', 'Activity Log', 'Tools', 'Developer Center', 'Maintenance', and 'Notification Preferences'. The main form fields are:

- Cluster: Cluster-1
- Datastore: Attach a new datastore
- NFS server address: 3.3.0.233 (VALIDATE SUCCESS)
- Export: /DemoDS01
- Storage Vendor: AWS\_FSxN
- Datastore Name: DemoDS01

At the bottom are 'ATTACH DATASTORE' and 'CANCEL' buttons.

3. データストアをクラスターに接続するには、「データストアの接続」をクリックします。

4. 以下に示すように vCenter にアクセスして NFS データストアを検証します。

## AWS 向けNetAppゲスト接続ストレージ オプション

AWS は、ネイティブ FSx サービス (FSx ONTAP) またはCloud Volumes ONTAP (CVO) を使用してゲスト接続されたNetAppストレージをサポートします。

### FSx ONTAP

Amazon FSx ONTAP は、NetApp の人気のONTAPファイルシステム上に構築された、信頼性が高く、スケーラブルで、高性能かつ機能豊富なファイルストレージを提供するフルマネージドサービスです。 FSx ONTAP は、NetApp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 操作と、完全に管理された AWS サービスの俊敏性、拡張性、シンプルさを兼ね備えています。

FSx ONTAP は、AWS またはオンプレミスで実行されている Linux、Windows、macOS コンピューティングインスタンスから広くアクセスできる、機能豊富で高速かつ柔軟な共有ファイルストレージを提供します。 FSx ONTAP は、1 ミリ秒未満のレイテンシを備えた高性能ソリッド ステート ドライブ (SSD) ストレージを提供します。 FSx ONTAPを使用すると、データのごく一部に対してのみ SSD ストレージ料金を支払いながら、ワークロードに対して SSD レベルのパフォーマンスを実現できます。

FSx ONTAPを使用すると、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、クローン、複製がで

きるため、データの管理が簡単になります。さらに、FSx ONTAP はデータを低成本で弾力性のあるストレージに自動的に階層化するため、容量のプロビジョニングや管理の必要性が軽減されます。

FSx ONTAP は、完全に管理されたバックアップとリージョン間の災害復旧のサポートを備えた、可用性と耐久性に優れたストレージも提供します。データの保護とセキュリティ確保を容易にするために、FSx ONTAP は一般的なデータ セキュリティおよび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

#### VMware Cloud on AWS で Amazon FSx ONTAP を構成する

Amazon FSx ONTAP ファイル共有と LUN は、VMware Cloud at AWS の VMware SDDC 環境内で作成された VM からマウントできます。ボリュームは Linux クライアントにマウントし、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プすることもできます。また、iSCSI 経由でマウントすると、LUN は Linux または Windows クライアント上でブロック 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、次の手順で簡単にセットアップできます。

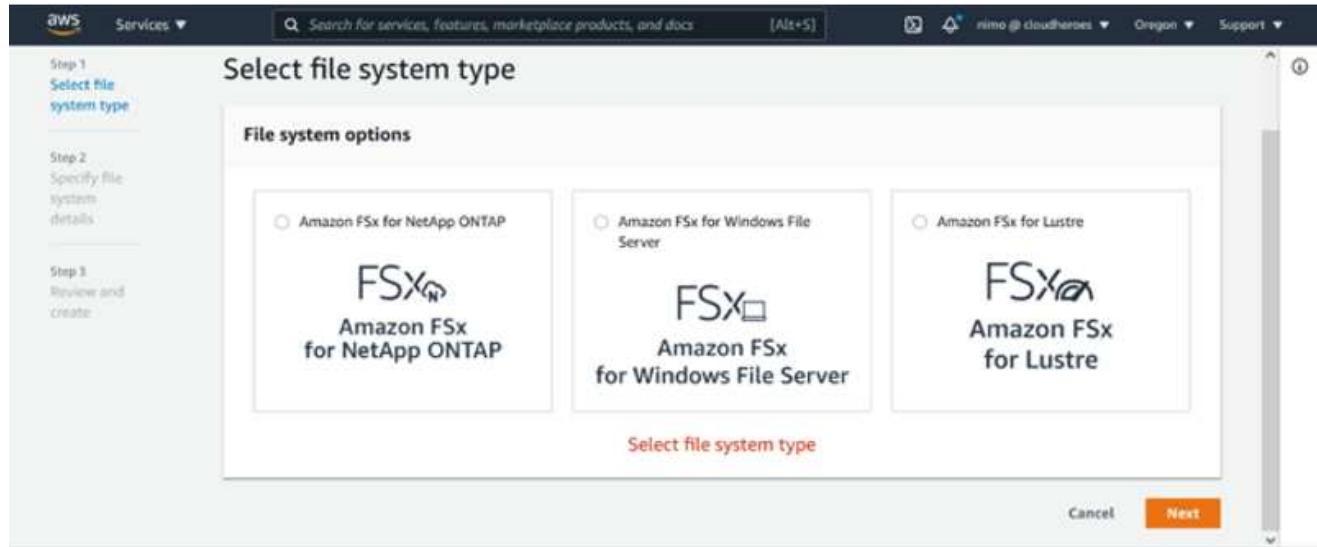


パフォーマンスを向上させ、アベイラビリティゾーン間のデータ転送料金を回避するには、Amazon FSx ONTAP と VMware Cloud on AWS が同じアベイラビリティゾーンに存在する必要があります。

## Amazon FSx ONTAPボリュームの作成とマウント

Amazon FSx ONTAPファイルシステ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. 開く "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起動します。
2. [ファイルシステムタイプの選択] ページで、[Amazon FSx ONTAP]を選択し、[次へ] を選択します。  
「ファイル システムの作成」ページが表示されます。



1. [ネットワーク] セクションの [仮想プライベート クラウド (VPC)] で、適切な VPC と優先サブネット、およびルート テーブルを選択します。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

### Creation method

#### Quick create

Use recommended best-practice configurations.  
Most configuration options can be changed after  
the file system is created.

#### Standard create

You set all of the configuration options, including  
specifying performance, networking, security,  
backups, and maintenance.

1. 作成方法として、「標準作成」を選択します。クリ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. [ネットワーク] セクションの [仮想プライベート クラウド (VPC)] で、適切な VPC と優先サブネット、およびルート テーブルを選択します。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)

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



[ネットワーク] セクションの [仮想プライベート クラウド (VPC)] で、適切な VPC と優先サブネット、およびルート テーブルを選択します。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、保存中のファイルシステムのデータを保護する AWS Key Management Service (AWS KMS) 暗号化キーを選択します。ファイルシステム管理パスワードには、fsxadmin ユーザーの安全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、REST API または CLI を使用してONTAP を管理するために vsadmin で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、fsxadmin ユーザーを使用して SVM を管理できます。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 に参加させていることを確認します。[既定のストレージ仮想マシン構成] セクションで、この検証のストレージの名前を指定します。SMB 共有は、自己管理型 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

vmcfsxval2svm

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. デフォルトのボリューム構成セクションで、ボリューム名とサイズを指定します。これは NFS ボリュームです。ストレージ効率では、ONTAPストレージ効率機能(圧縮、重複排除、および圧縮)をオンにするには [有効] を選択し、オフにするには [無効] を選択します。

## Default volume configuration

Volume name

vol1

Maximum of 203 alphanumeric characters, plus \_.

Junction path

/vol1

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



- 「ファイルシステムの作成」ページに表示されるファイルシステム構成を確認します。
- 「ファイルシステムの作成」をクリックします。

The screenshot shows the AWS FSx console interface. The top navigation bar includes the AWS logo, Services dropdown, search bar, and user information (nimo @ cloudheroes, Oregon, Support). The main navigation menu on the left has 'Amazon FSx' selected, with options like 'File systems', 'Backups', 'ONTAP', 'Windows File Server', 'Lustre', and 'FSx on Service Quotas'. The 'File systems' section shows three existing file systems: 'fsxtapcifs', 'vmcfsxval2', and 'fsxtapsql', each with details like ID, type, status, deployment type, storage type, and size.

The 'Storage virtual machines' tab is selected in the navigation bar. Below it, the 'Storage virtual machines (SVMs)' list shows two entries: 'fsxsmbtesting01' and 'vmcfsxval2svm', both created on 2021-10-19 at 15:17:08 UTC. The 'Create storage virtual machine' button is visible at the top right of this section.

The detailed view for 'fsxsmbtesting01' shows its summary information:

| SVM ID                               | Creation time             | Active Directory                       |
|--------------------------------------|---------------------------|--|
| svm-075dcfbe2cfa2ece9                | 2021-10-19T15:17:08+01:00 | FSXTESTING.LOCAL                       |
| SVM name                             | Lifecycle state           | Net BIOS name                          |
| fsxsmbtesting01                      | 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                           |

At the bottom, a note states: 詳しい情報については、"Amazon FSx ONTAPを使い始める"。

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. 開く "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. 「ボリューム」タブを選択します。
4. 「ボリュームの作成」タブを選択します。
5. ボリュームの作成ダイアログ ボックスが表示されます。

このセクションでは、デモ用に、VMware Cloud on AWS で実行されている VM に簡単にマウントできる NFS ボリュームを作成します。nfsdemovol01 は次のように作成されます。

**Create volume**

File system  
fs-040eacc5d0ac31017 | vmcfsxval2

Storage virtual machine  
svm-095db076341561212 | vmcfsxval2svm

Volume name  
nfsdemovol01

Maximum of 203 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

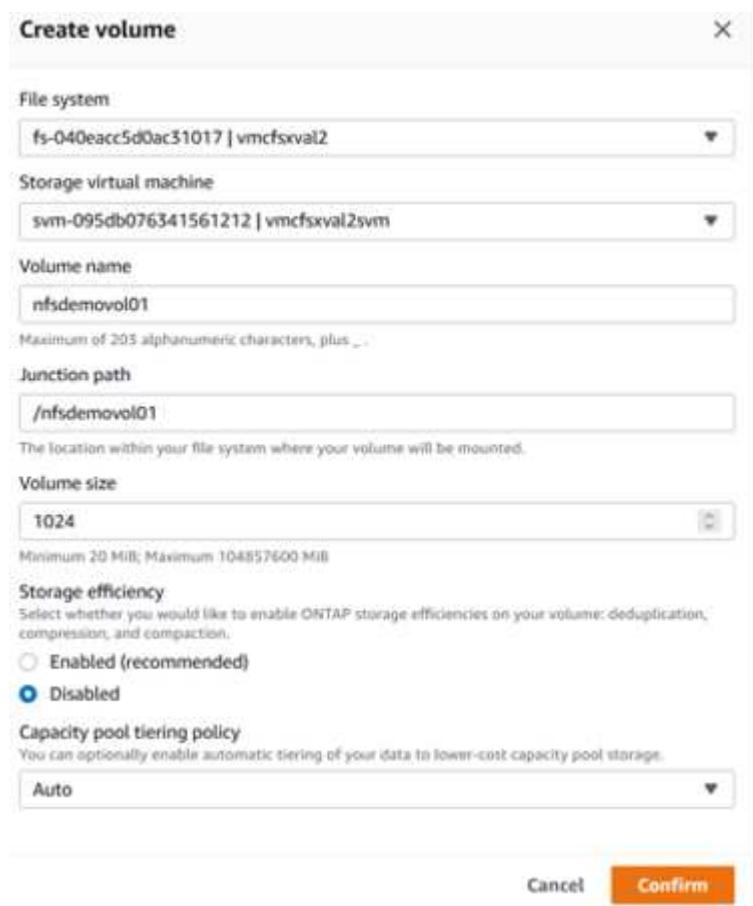
Storage efficiency  
Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

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



This screenshot shows the 'Create volume' dialog box from the Amazon FSx console. It's a step-by-step guide for creating a new volume. The first few steps are completed: selecting the file system (fs-040eacc5d0ac31017) and storage virtual machine (svm-095db076341561212). The next step, 'Volume name', has been filled with 'nfsdemovol01'. Below it, a note says 'Maximum of 203 alphanumeric characters, plus \_.' The 'Junction path' field contains '/nfsdemovol01', with a note below stating 'The location within your file system where your volume will be mounted.' The 'Volume size' is set to 1024 MiB. Under 'Storage efficiency', there are two options: 'Enabled (recommended)' and 'Disabled'; 'Disabled' is selected. At the bottom, there's a note about 'Capacity pool tiering policy' and a dropdown menu currently set to 'Auto'. At the very bottom are 'Cancel' and 'Confirm' buttons.

## LinuxクライアントにFSx ONTAPボリュームをマウントする

前の手順で作成した FSx ONTAPボリュームを VMC on AWS SDDC 内の Linux VM からマウントするには、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上でターミナルを開き、適切な資格情報でログインします。
3. 次のコマンドを使用して、ボリュームのマウント ポイントのディレクトリを作成します。

```
$ sudo mkdir /fsx/nfsdemovol01  
. 前の手順で作成したディレクトリにAmazon FSx ONTAP NFS  
ボリュームをマウントします。
```

```
sudo mount -t nfs nfsvers=4.1,198.19.254.239:/nfsdemovol01  
/fsx/nfsdemovol01
```

```
root@ubuntu01:/fsx/nfsdemovol01# mount -t nfs 198.19.254.239:/nfsdemovol01 /fsx/nfsdemovol01
```

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/nfsdemovol01# df  
Filesystem      1K-blocks    Used   Available Use% Mounted on  
tmpfs             814396     1176    813220  1% /run  
/dev/mapper/ubuntu--vg-ubuntu--lv 15412160 3666428 10943132 28% /  
tmpfs            4071560      0    4071560  0% /dev/shm  
tmpfs             5120      0    5120  0% /run/lock  
tmpfs             4096      0    4096  0% /sys/fs/cgroup  
/dev/sda2        999820  254996    675512  28% /boot  
tmpfs             814392      4    814388  1% /run/user/1000  
198.19.254.239:/nfsdemovol01  9961472 4041792 5719680 40% /fsx/nfsdemovol01  
root@ubuntu01:/fsx/nfsdemovol01# cd /fsx/nfsdemovol01/  
root@ubuntu01:/fsx/nfsdemovol01# ls  
nimewill.txt
```

## LinuxクライアントにFSx ONTAPボリュームをマウントする

## FSx ONTAPボリュームをMicrosoft Windowsクライアントに接続する

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プするには、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。これを行うと、共有フォルダー 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、[別のコンピューターに接続] を選択します。
3. 別のコンピュータの場合は、ストレージ仮想マシン (SVM) の DNS 名を入力します。たとえば、この例では FSXSMBTESTING01.FSXTESTING.LOCAL が使用されています。



Amazon FSxコンソールで SVM の DNS 名を見つけ、[Storage Virtual Machines] を選択し、[SVM] を選択してから、[エンドポイント] まで下にスクロールして SMB DNS 名を見つけます。[OK]をクリックします。Amazon FSxファイルシステムが共有フォルダのリストに表示されます。

## 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で、左側のペインの [共有] を選択して、Amazon FSxファイルシステムのアクティブな共有を表示します。

Computer Management

File Action View Help

Computer Management (FSXSMBTESTING01.FSXTESTING.LOCAL)

System Tools

- Task Scheduler
- Event Viewer
- Shared Folders
  - Shares
  - Sessions
  - Open Files
- Local Users and Groups
- Performance
- Device Manager

Storage

- Windows Server Backup
- Disk Management

Services and Applications

| Share Name | Folder Path     | Type    | # Client Connections | Description |
|------------|-----------------|---------|----------------------|-------------|
| c\$        | C:\             | Windows | 0                    |             |
| ipc\$      |                 | Windows | 1                    |             |
| smbdemo... | C:\smbdemovol01 | Windows | 1                    |             |
| testnimvol | C:\testnimvol   | Windows | 0                    |             |

1. 次に、新しい共有を選択し、共有フォルダーの作成ウィザードを完了します。

Create A Shared Folder Wizard

**Name, Description, and Settings**

Specify how people see and use this share over the network.

Type information about the share for users. To modify how people use the content while offline, click Change.

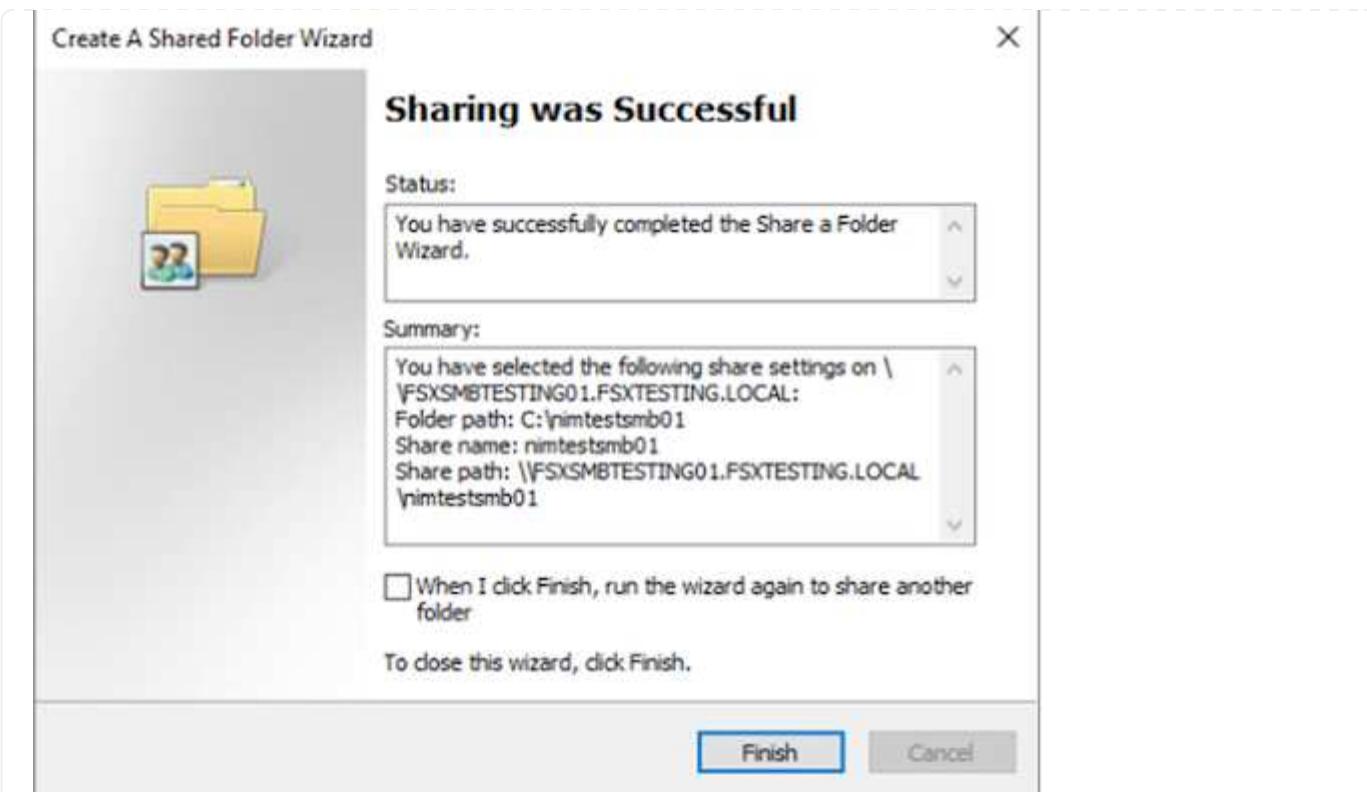
Share name:

Share path:

Description:

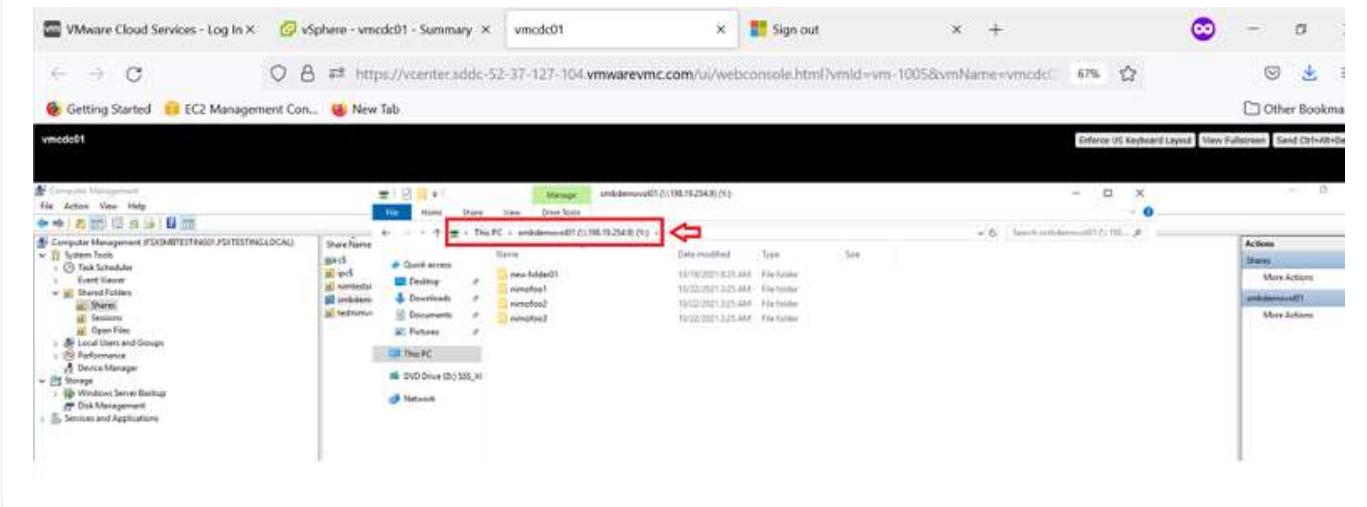
Offline setting:

< Back  Cancel



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、以下を参照してください。["SMB共有の作成"](#)。

- 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。これを実現するには、共有パスをコピーし、ネットワークドライブのマップオプションを使用して、AWS SDDC上のVMware Cloudで実行されている仮想マシンにボリュームをマウントします。



## iSCSI を使用して FSx ONTAP LUN をホストに接続する

### iSCSI を使用して FSx ONTAP LUN をホストに接続する

FSx の iSCSI トラフィックは、前のセクションで提供されたルートを介して VMware Transit Connect/AWS Transit Gateway を通過します。Amazon FSx ONTAPでLUNを設定するには、以下のドキュメントに従ってください。["ここをクリックしてください。"](#)。

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 がプロビジョニングされたら、Ubuntu での iSCSI 構成に関する詳細なガイダンスを参照してください (例として)["ここをクリックしてください。"](#)。

このホワイトペーパーでは、iSCSI LUN を Windows ホストに接続する方法について説明します。

## FSx ONTAPで LUN をプロビジョニングします。

1. ONTAPファイルシステム用の FSx の管理ポートを使用して、NetApp ONTAP CLI にアクセスします。
2. サイズ出力に示されている必要なサイズの LUN を作成します。

```
FsxId040eacc5d0ac31017::> lun create -vserver vmcfsxval2svm -volume nimfsxscsivol -lun nimofsxlun01 -size 5gb -ostype windows -space -reserve enabled
```

この例では、サイズ 5g (5368709120) の LUN を作成しました。

1. 特定の LUN にアクセス可能なホストを制御するために必要な igrup を作成します。

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

```
FsxId040eacc5d0ac31017::> igrup 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 igrup にマップします。

```

FsxId040eacc5d0ac31017::> lun map -vserver vmcfsxval2svm -path
/vol/nimfsxscsivol/nimofsxlun01 -igroup winIG

FsxId040eacc5d0ac31017::> lun show

Vserver      Path          State   Mapped   Type
Size

-----
-----
vmcfsxval2svm

/vol/blocktest01/lun01      online  mapped   linux
5GB

vmcfsxval2svm

/vol/nimfsxscsivol/nimofsxlun01 online  mapped   windows
5GB

```

2つのエントリが表示されました。

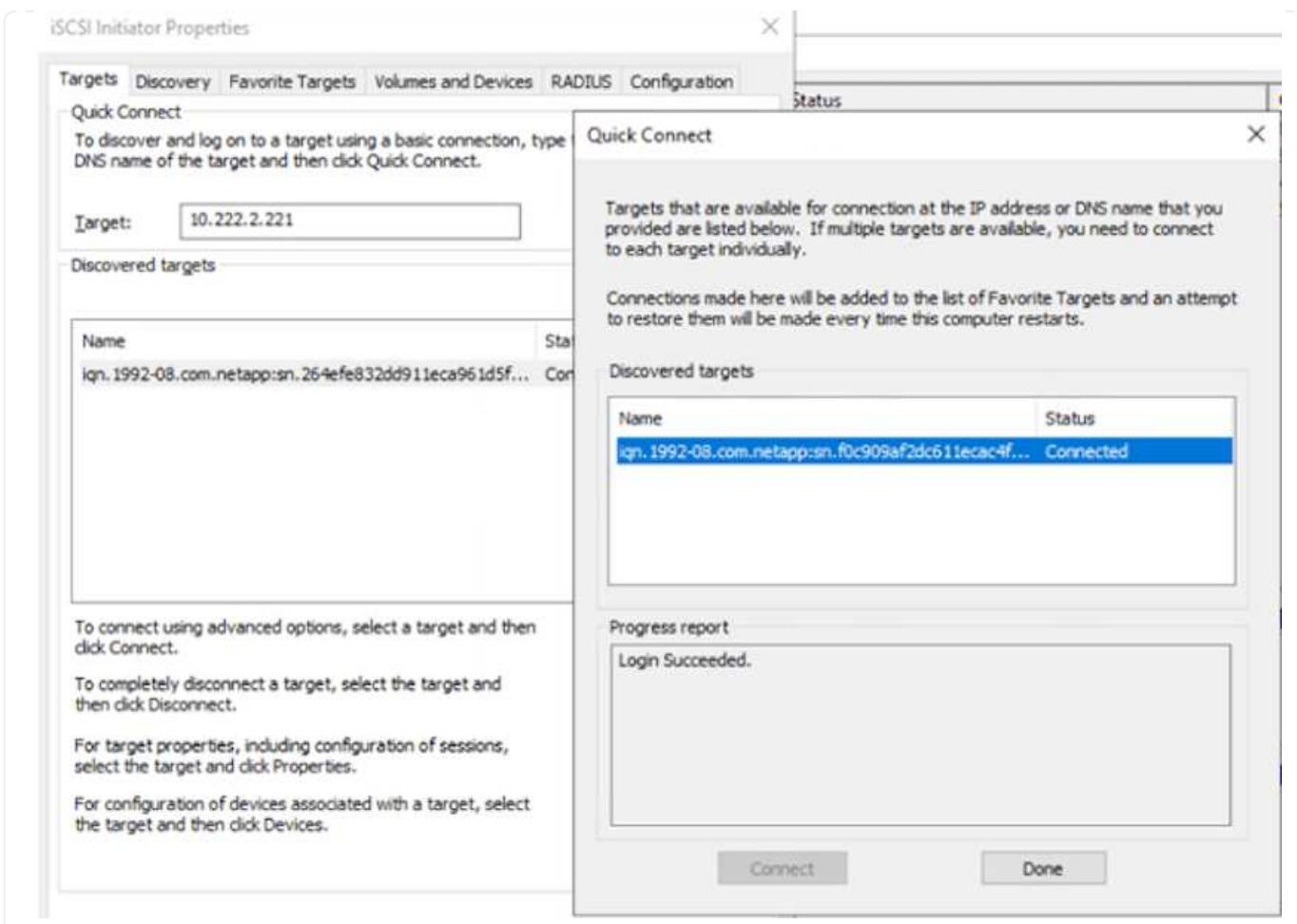
- 新しくプロビジョニングされた LUN を Windows VM に接続します。

新しい LUN を VMware Cloud on AWS SDDC 上にある Windows ホストに接続するには、次の手順を実行します。

- VMware Cloud on AWS SDDC でホストされている Windows VM に RDP 接続します。
- サーバー マネージャー > ダッシュボード > ツール > iSCSI イニシエーター に移動して、iSCSI イニシエーターのプロパティ ダイアログ ボックスを開きます。
- [検出] タブで、[ポータルの検出] または [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。
- [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。
- 「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のターゲットのリストに追加する」を選択します。[Advanced]をクリックします。

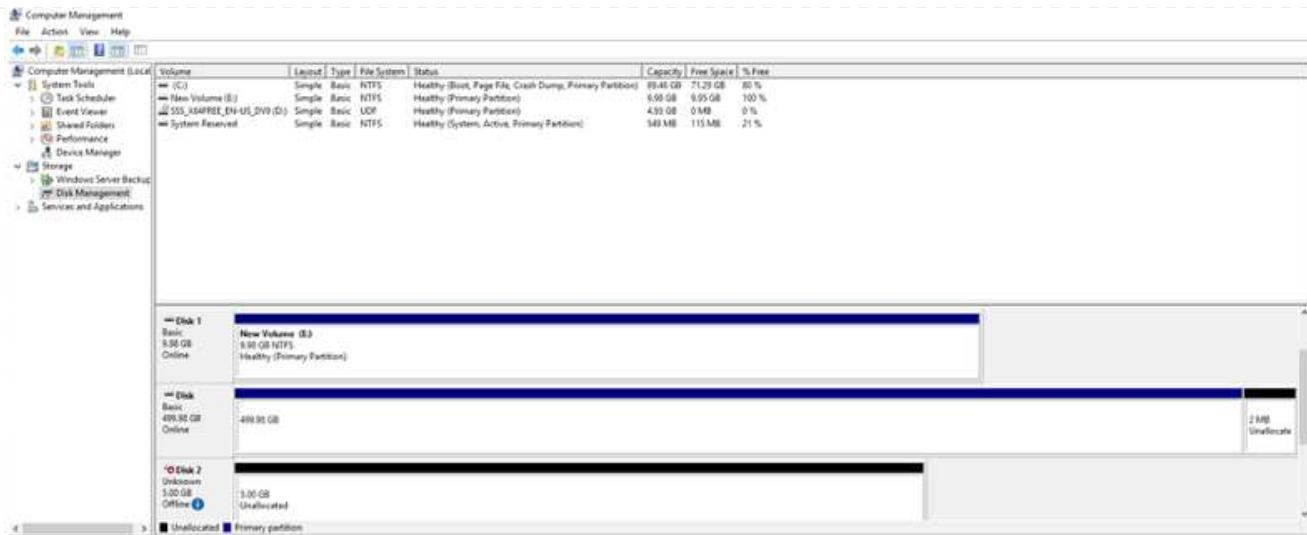


Windows ホストには、クラスタ内のそれぞれのノードへの iSCSI 接続が必要です。標準の DSM によって最適なパスが選択され、



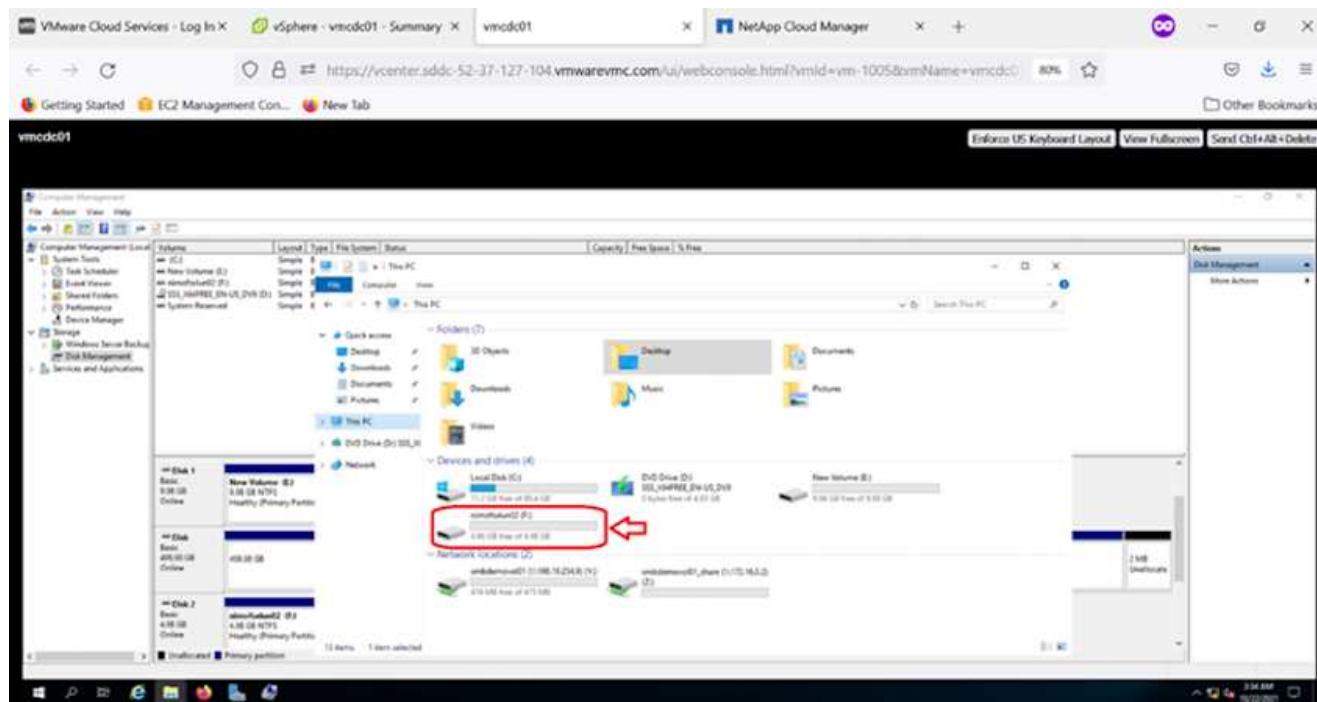
ストレージ仮想マシン (SVM) 上の LUN は、Windows ホストに対してディスクとして表示されます。追加された新しいディスクは、ホストによって自動的に検出されません。次の手順を実行して、手動での再スキャンをトリガーし、ディスクを検出します。

1. Windows のコンピューターの管理ユーティリティを開きます (スタート > 管理ツール > コンピューターの管理)。
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] をクリックします。



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。次の手順を実行して、LUNを初期化し、オプションでファイルシステムを使用してLUNをフォーマットします。

1. Windowsの[ディスクの管理]を起動します。
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種類を選択します。
3. ウィザードの指示に従います。この例では、ドライブ F: がマウントされます。



## Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP(CVO) は、NetApp のONTAPストレージ ソフトウェア上に構築された業界をリードするクラウド データ管理ソリューションであり、Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP) でネイティブに利用できます。

これはクラウドネイティブストレージを使用するONTAPのソフトウェア定義バージョンであり、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、データを管理するためのまったく新しい方法についてITスタッフを再トレーニングする必要性が軽減されます。

CVOにより、エッジからデータセンター、クラウドへと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することが可能になります。これらはすべて、単一ペインの管理コンソールであるNetApp Cloud Managerで管理されます。

CVOは設計上、クラウドで最も要求の厳しいアプリケーションにも対応できる優れたパフォーマンスと高度なデータ管理機能を提供します。

#### ゲスト接続ストレージとしての**Cloud Volumes ONTAP (CVO)**

## AWS に新しいCloud Volumes ONTAPインスタンスをデプロイする(自分で行う)

Cloud Volumes ONTAP共有と LUN は、VMware Cloud on AWS SDDC 環境で作成された VM からマウントできます。ボリュームはネイティブの AWS VM Linux Windows クライアントにマウントすることもできます。また、Cloud Volumes ONTAP はiSCSI、SMB、NFS プロトコルをサポートしているため、iSCSI 経由でマウントすると、Linux または Windows クライアントで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セットアップできます。

災害復旧または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複製するには、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へのデータの複製については、このドキュメントの範囲外です。オンプレミスとCloud Volumes ONTAPシステム間でデータを複製するには、["システム間のデータ複製の設定"](#)。



使用["Cloud Volumes ONTAPサイザー"](#)Cloud Volumes ONTAPインスタンスのサイズを正確に決定します。また、オンプレミスのパフォーマンスを監視して、Cloud Volumes ONTAPサイザーの入力として使用します。

1. NetApp Cloud Central にログインすると、Fabric View 画面が表示されます。Cloud Volumes ONTAPタブを見つけて、「Go to Cloud Manager」を選択します。ログインすると、Canvas 画面が表示されます。

1. Cloud Manager のホームページで、「作業環境の追加」をクリックし、クラウドとして AWS を選択し、システム構成のタイプを選択します。

1. 環境名や管理者の資格情報など、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<br>Credential Name | 139763910815<br>Account ID | netapp.com-cloud-volumes-...<br>Marketplace Subscription | <a href="#">Edit Credentials</a> |
|-----------------|-------------------------------------|----------------------------|--|----------------------------------|

Details

Working Environment Name (Cluster Name)  
fsxvotesting01

Credentials

User Name  
admin

Password  
\*\*\*\*\*

Confirm Password  
\*\*\*\*\*

Add Tags  
Optional Field | Up to four tags

[Continue](#)

1. BlueXP分類、BlueXP backup and recovery、Cloud Insightsなど、Cloud Volumes ONTAPデプロイメントのアドオンサービスを選択します。[Continue]をクリックします。

Create a New Working Environment

Services

|                         |                                     |                   |
|-------------------------|-------------------------------------|-------------------|
| Data Sense & Compliance | <input checked="" type="checkbox"/> | <a href="#">v</a> |
| Backup to Cloud         | <input checked="" type="checkbox"/> | <a href="#">v</a> |
| Monitoring              | <input checked="" type="checkbox"/> | <a href="#">v</a> |

[Continue](#)

1. HA デプロイメントモデルページで、複数のアベイラビリティゾーン構成を選択します。

Create a New Working Environment

HA Deployment Models

↑ Previous Step

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

- 「リージョンと VPC」ページでネットワーク情報を入力し、「続行」をクリックします。

Create a New Working Environment

### Region & VPC

↑ Previous Step

AWS Region: US West | Oregon

VPC: vpc-0d1c764bcc495e805 - 10.222.0.0/16

Security group: Use a generated security group

**Node 1:**  
Availability Zone: us-west-2a  
Subnet: 10.222.1.0/24

**Node 2:**  
Availability Zone: us-west-2b  
Subnet: 10.222.2.0/24

**Mediator:**  
Availability Zone: us-west-2c  
Subnet: 10.222.3.0/24

**Continue**

- [接続と SSH 認証] ページで、HA ペアとメディエーターの接続方法を選択します。

Create a New Working Environment

### Connectivity & SSH Authentication

↑ Previous Step

**Nodes**  
SSH Authentication Method: Password

**Mediator**  
Security Group: Use a generated security group  
Key Pair Name: nimokey  
Internet Connection Method: Public IP address

**Continue**

- フローティング IP アドレスを指定して、「続行」をクリックします。

## Floating IPs

[↑ 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ト テーブルを選択し、[続行] をクリックします。

## Route Tables

[↑ 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. 「データ暗号化」ページで、AWS 管理の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](#)

- 既存のライセンスを使用する場合は、ライセンス オプション (Pay-As-You-Go または BYOL) を選択します。この例では、Pay-As-You-Go オプションが使用されています。

## Create a New Working Environment Cloud Volumes ONTAP Charging Methods &amp; 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 it's created, use the Support Registration option to create an NSS account.

[Continue](#)

- AWS SDDC 上の VMware クラウドで実行されている VM に展開するワークロードのタイプに基づいて、利用可能ないくつかの事前構成済みパッケージから選択します。



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、[実行] をクリックします。

Create a New Working Environment      Review & Approve

↑ Previous Step **fsxvotesting** AWS | us-west-2 | HA Show API request

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

**①**  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がプロビジョニングされると、Canvas ページの作業環境にリストされます。

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

**Canvas** [Go to Tabular View](#)

**Add Working Environment**

**vmchadval2** FSA for ONTAP  
9 Volumes    26.49 GB Capacity    AWS

**fsxvotesting01** On

**DETAILS**  
Cloud Volumes ONTAP | AWS | HA

**SERVICES**

|                  |            |                         |
|------------------|------------|-------------------------|
| Replication      | Off        | <a href="#">Enable</a>  |
| Backup & Restore | Loading... | <a href="#">Details</a> |

## SMBボリュームの追加構成

1. 作業環境の準備ができたら、CIFS サーバーが適切な DNS および Active Directory 構成パラメータで構成されていることを確認します。SMB ボリュームを作成する前にこの手順を実行する必要があります。

The screenshot shows the 'Create a CIFS server' configuration page within the AWS CloudFormation console. It includes fields for 'DNS Primary IP Address' (192.168.1.3), 'Active Directory Domain to join' (fxtesting.local), 'DNS Secondary IP Address (Optional)', 'Credentials authorized to join the domain' (Username and Password), and a 'Save' button.

1. ボリュームを作成する CVO インスタンスを選択し、「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すると、クラウド マネージャーはそれを含む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 SMB が選択されています。

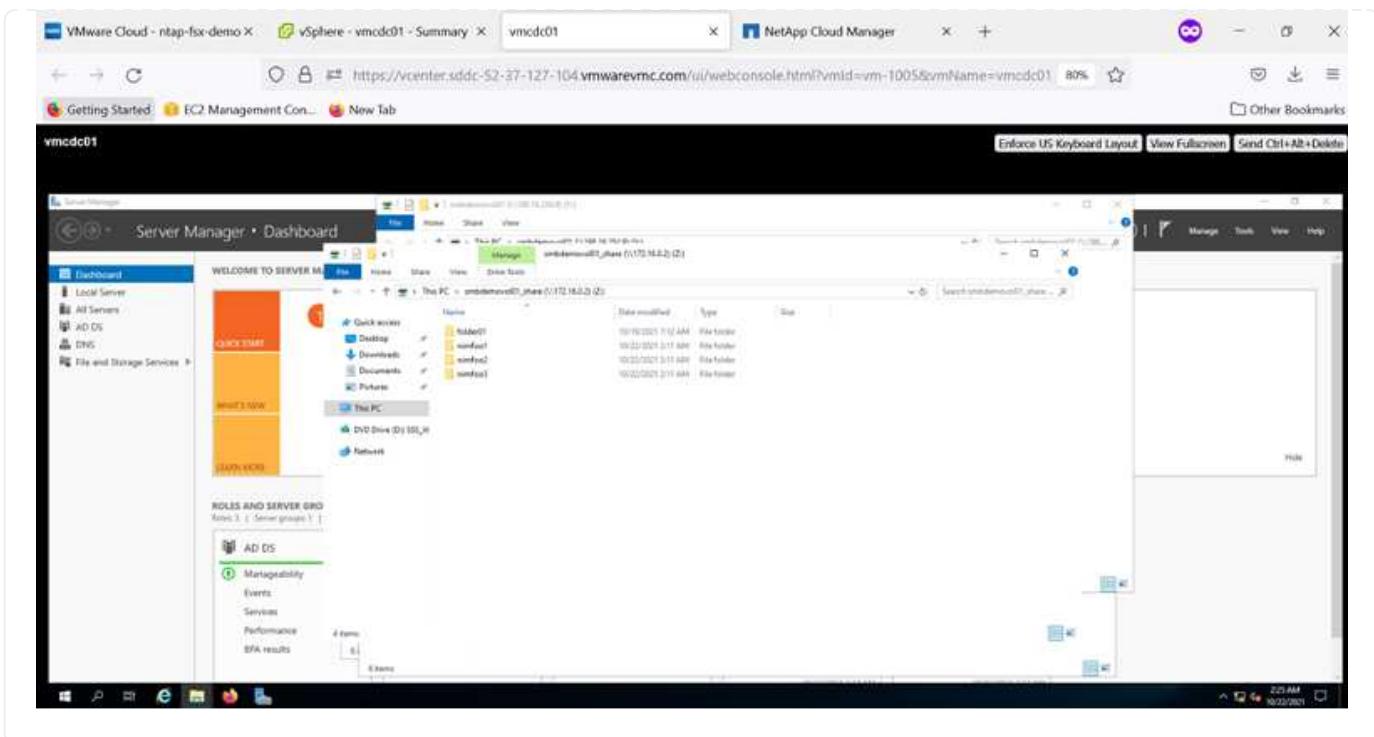
The screenshot shows the 'Volume Details, Protection & Protocol' configuration page for a new volume. It includes sections for 'Details & Protection' (Volume Name: smbdemovol01, Size (GB): 100, Snapshot Policy: default) and 'Protocol' (Protocol tab selected, Share name: smbdemovol01\_share, Permissions: Full Control, Users / Groups: Everyone). A 'Continue' button is at the bottom.

1. ボリュームがプロビジョニングされると、ボリュームペインで使用できるようになります。CIFS 共有がプロビジョニングされているため、ユーザーまたはグループにファイルとフォルダーへのアクセス許可を与え、それらのユーザー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。



- ボリュームが作成されたら、マウント 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。
- 次のパスをコピーし、ネットワーク ドライブのマップ 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。

The screenshot shows the AWS Storage service interface for an FSx volume named 'fsxcvotesting01'. At the top, it says '(Multiple AZs)'. Below the volume name, there are tabs for 'Volumes', 'HA Status', 'Cost', and 'Replications'. On the right, there are icons for 'Edit', 'Delete', and 'Copy'. The main area is titled 'Mount Volume' and shows 'smbdemovol01' selected. It provides two access methods: 'Access from inside the VPC using Floating IP' and 'Access from outside the VPC using AWS Private IP'. Under each method, there are two options: 'Auto failover between nodes' (IP address migrates between nodes if failures occur) and 'No auto failover between nodes' (IP address does not migrate between nodes if failures occur). Below these, there are 'Copy' buttons for the mount commands: '\\172.16.0.2\smbdemovol01\_share' and '\\10.222.1.100\smbdemovol01\_share'. A note at the bottom says 'If the primary node goes offline, mount the volume by using the HA partner's IP address:'.



## LUNをホストに接続する

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 Canvas 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. [ボリュームの追加] > [新しいボリューム] をクリックし、[iSCSI] を選択して、[イニシエーター グループの作成] をクリックします。[Continue]をクリックします。

Create new volume in fsxvcotesting01      Volume Details, Protection & Protocol

Details & Protection      Protocol

Volume Name: nimofsxiscsicvo01      Size (GB): 500

Snapshot Policy: default

Default Policy

NFS      CIFS      iSCSI      What about LUNs?

Initiator Group

Map Existing Initiator Groups       Create Initiator Group

Operating System Type: Windows

Select Initiator Groups: 1 (of 3) Groups

winiG | windows  
 iqn.1991-05.com.microsoft:vmcdc01.fsxtestin...

Continue

VMware Cloud - ntap-for-demo X vSphere - vmcdc01 - Summary X vmcdc01 X NetApp Cloud Manager X

https://vcenter.sddc-52-37-127-104.vmwarevmc.com/ui/webconsole.html?vmId=vm-1005&vmName=vmcdc01 80%

Getting Started EC2 Management Con... New Tab

vmcdc01

Server Manager - Dashboard

WELCOME TO SERVER M...

File and Storage Services >

Local Server All Servers AD DS DNS File and Storage Services >

QUICKING WHAT'S NEW LEARN MORE

File Tools

Manage umbdemo01\_share (172.16.0.2) (D)

Name Date modified Type Size

Desktop 19/11/2021 17:01 AM File folder

Downloads 19/11/2021 17:01 AM File folder

Documents 19/11/2021 17:01 AM File folder

Pictures 19/11/2021 17:01 AM File folder

This PC DVD Drive (D) 153.0K

Network

ROLES AND SERVER GRID Roles 7 / Server groups 1

AD DS Manageability Events Services Performance BKA results

Manage Task View Help

Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

1. ボリュームがプロビジョニングされたら、ボリュームを選択し、「ターゲット IQN」をクリックします。iSCSI 修飾名 (IQN) をコピーするには、[コピー] をクリックします。ホストから LUN への iSCSI 接続を設定します。

VMware Cloud on AWS SDDC 上にあるホストに対して同じことを実行するには、次の手順を実行します。

1. VMware Cloud on AWS でホストされている VM に RDP 接続します。
2. iSCSI イニシエーターのプロパティ ダイアログ ボックスを開きます: サーバー マネージャー > ダッシュボード > ツール > iSCSI イニシエーター。
3. [検出] タブで、[ポータルの検出] または [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、[コンピューター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のターゲットの一覧に追加する] を選択します。[Advanced]をクリックします。

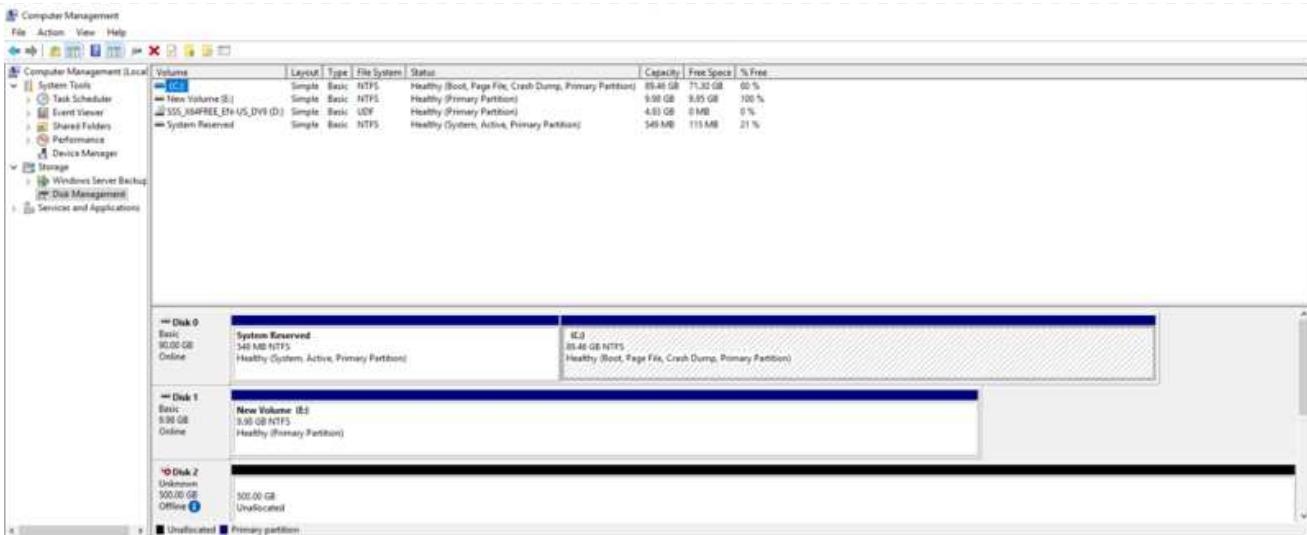


Windows ホストには、クラスタ内のそれぞれのノードへの iSCSI 接続が必要です。標準の DSM によって最適なパスが選択され、



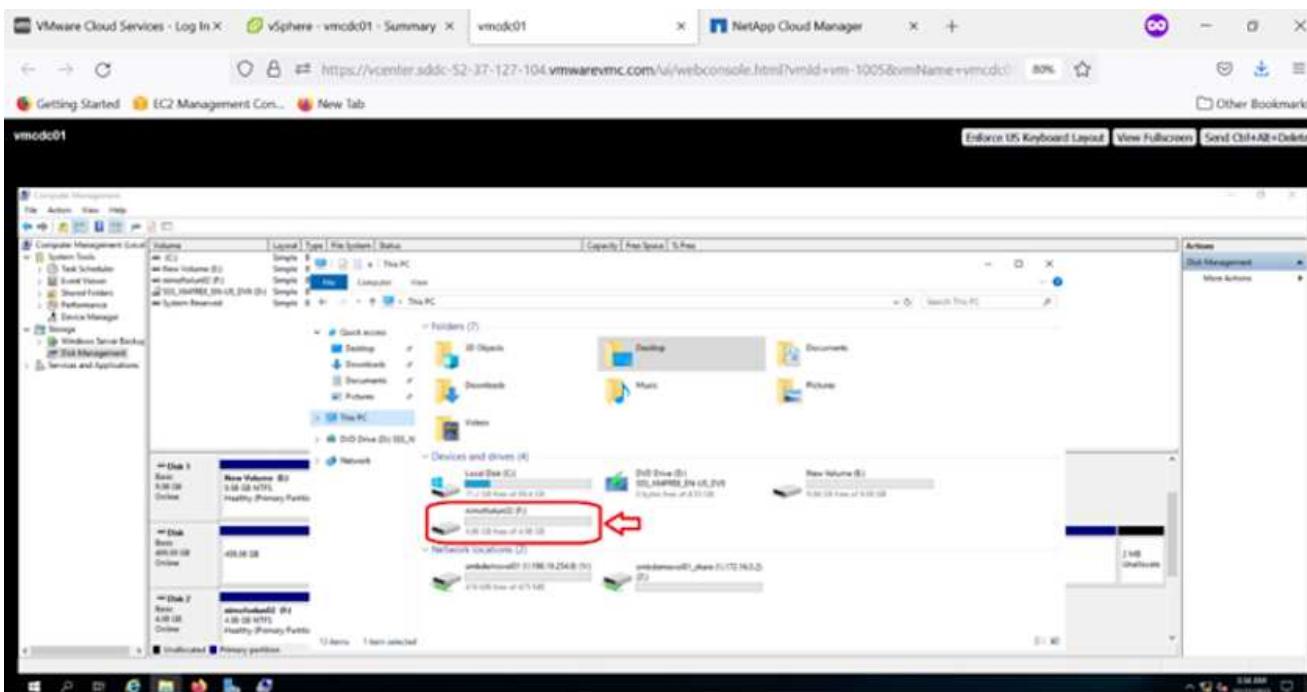
SVM からの LUN は、Windows ホストに対してディスクとして表示されます。追加された新しいディスクは、ホストによって自動的に検出されません。次の手順を実行して、手動での再スキャンをトリガーし、ディスクを検出します。

1. Windows のコンピューターの管理ユーティリティを開きます (スタート > 管理ツール > コンピューターの管理)。
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] をクリックします。



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、オプションで次の手順を実行して、LUNをファイルシステムでフォーマットします。

1. Windowsの[ディスクの管理]を起動します。
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種類を選択します。
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がプロビジョニングされたら、LinuxディストリビューションのiSCSI構成に関する詳細なガイドを参照してください。例えば、UbuntuのiSCSI設定は次のようにになります。["ここをクリックしてください。"](#)。確認するには、シェルからlsblk cmdを実行します。

## LinuxクライアントにCloud Volumes ONTAP NFSボリュームをマウントする

VMC on AWS SDDC 内の仮想マシンからCloud Volumes ONTAP (DIY) ファイル システムをマウントするには、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. セキュア シェル (SSH) を使用してインスタンス上でターミナルを開き、適切な資格情報でログインします。
3. 次のコマンドを使用して、ボリュームのマウント ポイントのディレクトリを作成します。

```
$ sudo mkdir /fsxvotesting01/nfsdemovol01  
. 前の手順で作成したディレクトリにAmazon FSx ONTAP NFS  
ボリュームをマウントします。
```

```
sudo mount -t nfs nfsvers=4.1,172.16.0.2:/nfsdemovol01  
/fsxvotesting01/nfsdemovol01
```



## Azure 仮想化サービス: NetAppストレージを使用するためのオプション

NetAppストレージは、ゲスト接続ストレージまたは補助ストレージとして Azure VMware サービスに接続できます。

### 補助的な NFS データストアとしてのAzure NetApp Files (ANF)

NFS データストアのサポートは、オンプレミス展開の ESXi バージョン 3 で導入され、vSphere のストレージ機能が大幅に拡張されました。

NFS 上で vSphere を実行することは、優れたパフォーマンスと安定性を提供するため、オンプレミスの仮想化展開で広く採用されているオプションです。オンプレミスのデータセンターに大規模なネットワーク接続ストレージ (NAS) がある場合は、容量とパフォーマンスの課題を克服するために、Azure NetAppファイルデータストアを使用して Azure VMware ソリューション SDDC を Azure にデプロイすることを検討する必要があ

ります。

Azure NetApp Files は、業界をリードする高可用性のNetApp ONTAPデータ管理ソフトウェア上に構築されています。 Microsoft Azure サービスは、基礎、メインストリーム、専門の 3 つのカテゴリに分類されます。 Azure NetApp Files は特殊なカテゴリに属しており、多くのリージョンにすでに導入されているハードウェアによってサポートされています。高可用性 (HA) が組み込まれたAzure NetApp Files は、ほとんどの停止からデータを保護し、業界をリードする 99.99%^ の稼働率の SLA を提供します。

補足的な NFS データストアとしての ANF の詳細については、次の Web サイトを参照してください。

- ・ "補助的な NFS データストアとしての ANF: 概要"
- ・ "Azure の補足 NFS データストア オプション"

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

Azure NetApp Files は、エンタープライズ グレードのデータ管理とストレージを Azure に提供するため、ワークフローとアプリケーションを簡単に管理できます。ワークフローをクラウドに移行し、パフォーマンスを犠牲にすることなく実行します。

Azure NetApp Files は障害を取り除き、すべてのファイルベースのアプリケーションを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がなくなり、複雑さなしでアプリケーション用の永続ストレージを利用できるようになります。

サービスは Microsoft Azure ポータルを通じて提供されるため、ユーザーは Microsoft エンタープライズ契約の一環として完全に管理されたサービスを体験できます。 Microsoft が管理する世界クラスのサポートにより、完全な安心感が得られます。この単一のソリューションにより、マルチプロトコルのワークフローを迅速かつ簡単に追加できます。レガシー環境でも、Windows と Linux の両方のファイルベースのアプリケーションを構築および展開できます。

詳細については、"ゲスト接続ストレージとしての ANF"。

#### ゲスト接続ストレージとしての**Cloud Volumes ONTAP (CVO)**

Cloud Volumes ONTAP (CVO) は、NetApp のONTAPストレージ ソフトウェア上に構築された業界をリードするクラウド データ管理ソリューションであり、Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP) でネイティブに利用できます。

これはクラウドネイティブ ストレージを使用するONTAPのソフトウェア定義バージョンであり、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、データを管理するためのまったく新しい方法について IT スタッフを再トレーニングする必要性が軽減されます。

CVO により、エッジからデータセンター、クラウドへとシームレスにデータを移動し、ハイブリッド クラウドを統合することが可能になります。これらはすべて、単一ペインの管理コンソールであるNetApp Cloud Manager で管理されます。

CVOは設計上、クラウドで最も要求の厳しいアプリケーションにも対応できる優れたパフォーマンスと高度なデータ管理機能を提供します。

詳細については、"ゲスト接続ストレージとしてのCVO"。

## ANFデータストアソリューションの概要

成功している組織はすべて、変革と近代化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 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、および災害復旧のプロセスを可能な限りシームレスにする方法を検討します。クラウドに移行する顧客は、弾力性とバースト、データセンターの撤退、データセンターの統合、サポート終了のシナリオ、合併、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上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備えた低コストの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ことに加え、クラウドの展開と弾力性の力を最大限に引き出すには、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です。

### ユースケース

Azure VMware ソリューションは顧客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オプションが限られているため、ストレージ負荷の高いワークロードを持つ組織にとってそ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結び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あり、これによりストレージを集中的に使用するワークロードのコストが 35 ~ 40% 以上増加する可能性があります。これらのワークロードには追加の処理能力ではなく追加のストレージが必要ですが、追加のホストに対して料金を支払う必要があります。

次のシナリオを考えてみましょう。顧客は処理能力 (vCPU/vMem) のために 6 台のホストを必要としていますが、ストレージについてもかなりの要件があります。評価によると、ストレージ要件を満たすには 12 台のホストが必要です。これにより、実際に必要なのはストレージの増設だけなのに、追加の処理能力をすべて購入する必要があるため、全体的な TCO が増加します。これは、移行、災害復旧、バースト、開発/テストなど、あらゆるユースケースに適用できます。

Azure VMware Solution のもう 1 つの一般的な使用例は、災害復旧 (DR) です。ほとんどの組織は、確実な DR 戦略を持っていません。あるいは、DR のためだけにゴースト データセンターを運用することを正当化するのに苦労するかもしれません。管理者は、パイロットライト クラスターまたはオンデマンド クラスターを使用して、ゼロ フットプリントの DR オプションを検討できます。そうすれば、ホストを追加せずにストレージを拡張することができ、魅力的な選択肢になる可能性があります。

まとめると、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
- ANF データストアを、オンプレミスまたはソフトウェア定義データセンター (SDDC) 間の Azure リージョン内からのコスト最適化された復旧ワークフローのディザスター リカバリー ターゲットとして使用します。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 (現在パブリック プレビュー) を提供するとともに、Azure VMware ソリューションのクラス最高のデータ保護と DR 機能について説明し、vSAN ストレージからストレージ容量をオフロードできるようにします。



ANF データストアの使用に関する追加情報については、お住まいの地域の NetApp または Microsoft ソリューション 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 ソリューション

Azure VMware Solution (AVS) は、Microsoft Azure パブリック クラウド内で完全に機能する VMware SDDC を提供するハイブリッド クラウド サービスです。AVS は、Microsoft によって完全に管理およびサポートされ、Azure インフラストラクチャを使用する VMware によって検証されたファーストパーティ ソリューションです。そのため、お客様は、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 を利用できると同時に、Microsoft Azure のグローバルな展開、クラス最高のデータセンター設備、ネイティブ Azure サービスとソリューションの豊富なエコシステムへの近接性を活用できます。Azure VMware Solution SDDC と Azure NetApp Files を組み合わせることで、最小限のネットワーク待機時間で最高のパフォーマンスが得られます。

使用するクラウドに関係なく、VMware SDDC が展開されると、初期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 サーバー 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。
- ・仮想ネットワークとセキュリティのための VMware NSX と、管理用の NSX Manager クラスタ。

## まとめ

オールクラウドまたはハイブリッド クラウドのどちらをターゲットにしているかに関係なく、Azure NetApp ファイルは、データ要件をアプリケーション レイヤーにシームレスにすることで TCO を削減しながら、ファイル サービスとともにアプリケーション ワークロードを展開および管理するための優れたオプションを提供します。ユース ケースがどのようなものであっても、Azure VMware Solution と Azure NetApp Files を併せて選択すると、クラウドのメリットの迅速な実現、オンプレミスと複数のクラウドにわたる一貫性のあるインフラストラクチャと運用、ワークロードの双方向の移植性、エンタープライズ レベルの容量とパフォーマンスが実現します。これは、ストレージを接続するために使用される、使い慣れたプロセスと手順と同じです。覚えておいてください。変更されたのはデータの位置と新しい名前だけです。ツールとプロセスはすべて同じままで、Azure NetApp Files は全体的な展開の最適化に役立ちます。

## まとめ

このドキュメントの主なポイントは次のとおりです。

- ・ Azure NetApp Files を AVS SDDC 上のデータストアとして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向上させ、より高い可用性を実現し、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。
- ・ シンプルで即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簡素化します。
- ・ 動的な再形成機能を使用して、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します。
- ・ Azure VMware Solution Cloud が宛先である場合、Azure NetApp Files は最適化された展開に適したストレージ ソリューションです。

## 詳細情報の入手方法

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 リンクを参照してください。

- ・ Azure VMware ソリューションのドキュメント

"<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 NetApp Files データストアを Azure VMware Solution ホストに接続する (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 で追加の NFS データストアを作成する

NFS データストアのサポートは、オンプレミス展開の ESXi バージョン 3 で導入され、vSphere のストレージ機能が大幅に拡張されました。

NFS 上で vSphere を実行することは、優れたパフォーマンスと安定性を提供するため、オンプレミスの仮想化展開で広く採用されているオプションです。オンプレミスのデータセンターに大規模なネットワーク接続ストレージ (NAS) がある場合は、容量とパフォーマンスの課題を克服するために、Azure NetApp ファイル データストアを使用して Azure VMware ソリューション SDDC を Azure にデプロイすることを検討する必要があります。

Azure NetApp Files は、業界をリードする高可用性の NetApp ONTAP データ管理ソフトウェア上に構築されています。Microsoft Azure サービスは、基礎、メインストリーム、専門の 3 つのカテゴリに分類されます。

Azure NetApp Files は特殊なカテゴリに属しており、多くのリージョンにすでに導入されているハードウェアによってサポートされています。Azure NetApp Files は、高可用性 (HA) を内蔵しており、ほとんどの障害からデータを保護し、業界をリードする SLA を提供します。"99.99%"稼働時間。

Azure NetApp Files データストア機能が導入される前は、パフォーマンスとストレージを集中的に使用するワークロードをホストすることを計画している顧客のスケールアウト操作には、コンピューティングとストレージの両方の拡張が必要でした。

次の点に留意してください。

- SDDC クラスタでは、不均衡なクラスタ構成は推奨されません。したがって、ストレージを拡張するということは、ホストを追加することを意味し、TCO が増加します。
- 可能な vSAN 環境は 1 つだけです。したがって、すべてのストレージ トラフィックは実稼働ワークロードと直接競合します。
- アプリケーション要件、パフォーマンス、コストを調整するために複数のパフォーマンス層を提供するオプションはありません。
- クラスター ホスト上に構築された vSAN のストレージ容量の限界に簡単に達してしまいます。Azure NetApp Files の Platform as a Service (PaaS) オファリングをデータストアとして統合することで、顧客はストレージを個別に独立して拡張し、必要に応じて SDDC クラスターにコンピューティング ノードのみを追加できるようになります。この機能により、前述の課題が克服されます。

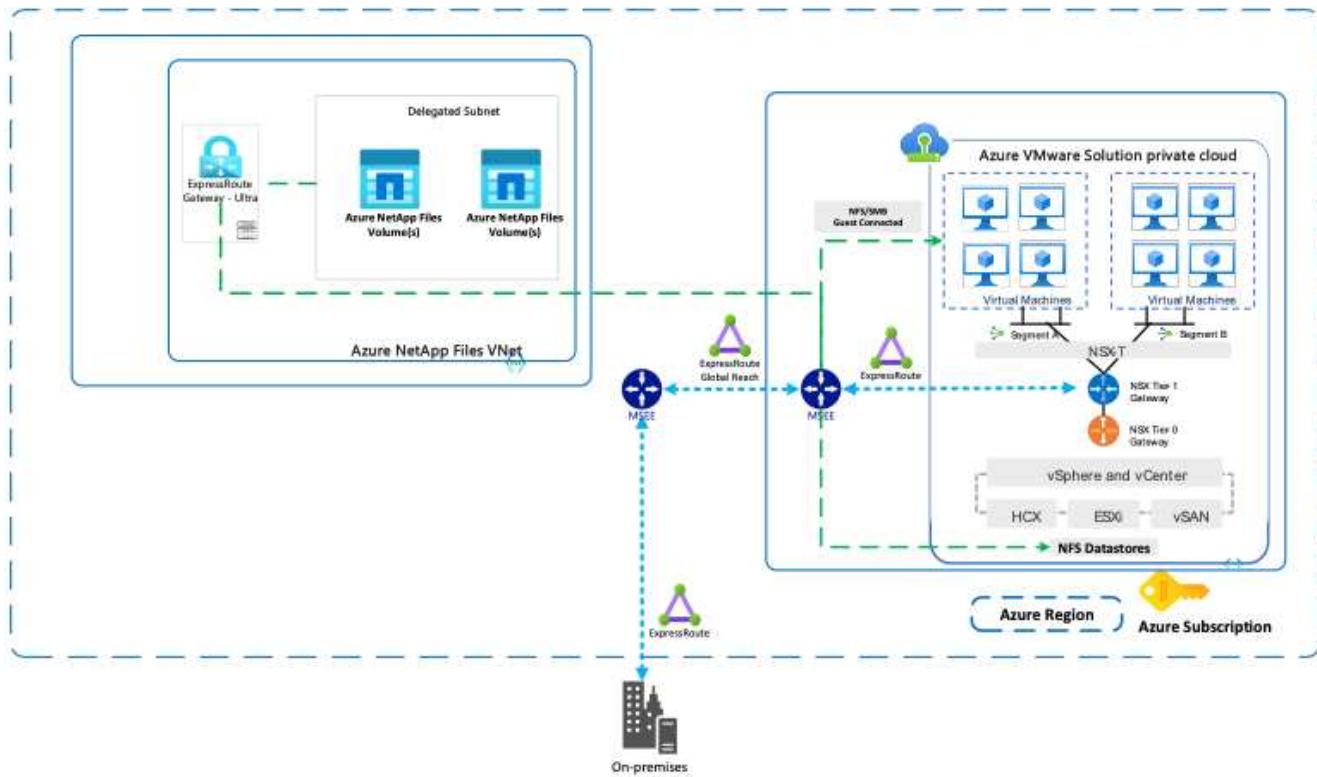
Azure NetApp Files を使用すると、複数のデータストアをデプロイすることもできます。これにより、適切なデータストアに仮想マシンを配置し、ワークロードのパフォーマンス要件を満たすために必要なサービス レベルを割り当てることで、オンプレミスのデプロイ モデルを模倣できます。マルチプロトコル サポートの独自の機能により、ゲストストレージは、SQL や Oracle などのデータベース ワークロードの追加オプションとなるとともに、追加の NFS データストア機能を使用して残りの VMDK を格納することもできます。これに加えて、ネイティブ スナップショット機能を使用すると、迅速なバックアップと詳細な復元を実行できます。



ストレージの計画とサイズ設定、および必要なホスト数の決定については、Azure および NetApp ソリューション アーキテクチャにお問い合わせください。NetApp、テスト、POC、および本番環境の展開のデータストアレイアウトを最終決定する前に、ストレージ パフォーマンス要件を特定することを推奨しています。

## 詳細なアーキテクチャ

このアーキテクチャでは、高レベルの観点から、オンプレミス環境と Azure 間でハイブリッド クラウドの接続性とアプリの移植性を実現する方法について説明します。また、Azure NetApp Files を補助的な NFS データストアとして使用する方法や、Azure VMware ソリューションでホストされているゲスト仮想マシンのゲスト内ストレージ オプションとして使用する方法についても説明します。



## サイジング

移行または災害復旧において最も重要なのは、ターゲット環境の適切なサイズを決定することです。オンプレミスから Azure VMware Solution へのリフト アンド シフトを実行するために必要なノードの数を理解することは非常に重要です。

サイズ設定には、RVTools (推奨) または Live Optics や Azure Migrate などの他のツールを使用して、オンプレミス環境からの履歴データを使用します。RVTools は、vCPU、vMem、vDisk、および電源オン/オフの VM を含む必要なすべての情報をキャプチャして、ターゲット環境の特性を把握するのに最適なツールです。

RVtools を実行するには、次の手順を実行します。

1. RVTools をダウンロードしてインストールします。
2. RVTools を実行し、オンプレミスの vCenter Server に接続するために必要な情報を入力して、「ログイン」を押します。
3. 在庫を Excel スプレッドシートにエクスポートします。

4. スプレッドシートを編集し、[vInfo] タブから理想的な候補ではない VM を削除します。このアプローチにより、必要な数のホストを使用して Azure VMware SDDC クラスターを適切なサイズにするために使用できるストレージ要件に関する明確な出力が得られます。



ゲスト内ストレージで使用されるゲスト VM は個別に計算する必要がありますが、Azure NetApp Files は追加のストレージ容量を簡単にカバーできるため、全体的な TCO を低く抑えることができます。

## Azure VMware Solution のデプロイと構成

オンプレミスと同様に、仮想マシンの作成と移行のための運用準備が整った環境を正常に構築するには、Azure VMware ソリューションを計画することが重要です。

このセクションでは、ゲスト内ストレージを備えたデータストアとして Azure NetApp Files と組み合わせて使用するために AVS を設定および管理する方法について説明します。

セットアッププロセスは、次の 3 つの部分に分けられます。

- リソース プロバイダーを登録し、プライベート クラウドを作成します。
- 新規または既存の 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します。こちらを参照してください["リンク" Azure VMware ソリューションの SDDC プロビジョニング プロセスのステップバイステップのチュートリアル。](#)

## Azure VMware Solution を使用して Azure NetApp Files を構成する

Azure NetApp Files 間の新しい統合により、Azure VMware Solution リソース プロバイダー API/CLI を介して Azure NetApp Files ボリュームを使用して NFS データストアを作成し、プライベート クラウド内の任意のクラスターにデータストアをマウントできるようになります。VM とアプリ VMDK を格納するだけでなく、Azure NetApp ファイル ボリュームは、Azure VMware Solution SDDC 環境で作成された VM からマウントすることもできます。Azure NetApp Files はサーバー メッセージ ブロック (SMB) プロトコルとネットワーク ファイル システム (NFS) プロトコルをサポートしているため、ボリュームを Linux クライアントにマウントし、Windows クライアントにマップすることができます。



最適なパフォーマンスを得るには、Azure NetApp Files をプライベート クラウドと同じ可用性ゾーンにデプロイします。Express ルート ファストパスとのコロケーションにより、ネットワーク遅延が最小限に抑えられ、最高のパフォーマンスが実現します。

Azure NetApp ファイル ボリュームを Azure VMware Solution プライベート クラウドの VMware データストアとして接続するには、次の前提条件が満たされていることを確認してください。

## 前提条件

- az login を使用して、サブスクリプションが Microsoft.AVS 名前空間の CloudSanExperience 機能に登録されていることを確認します。

```
az login -tenant xcvxcvxc- vxvc- xcvx- cvxc- vxcvxcvxcv  
az feature show --name "CloudSanExperience" --namespace "Microsoft.AVS"
```

- 登録されていない場合は登録してください。

```
az feature register --name "CloudSanExperience" --namespace  
"Microsoft.AVS"
```



登録が完了するまでに約 15 分かかります。

- 登録のステータスを確認するには、次のコマンドを実行します。

```
az feature show --name "CloudSanExperience" --namespace "Microsoft.AVS"  
--query properties.state
```

- 登録が中間状態で 15 分以上停止している場合は、フラグを登録解除してから再登録してください。

```
az feature unregister --name "CloudSanExperience" --namespace  
"Microsoft.AVS"  
az feature register --name "CloudSanExperience" --namespace  
"Microsoft.AVS"
```

- サブスクリプションが Microsoft.AVS 名前空間の AnfDatastoreExperience 機能に登録されていることを確認します。

```
az feature show --name "AnfDatastoreExperience" --namespace  
"Microsoft.AVS" --query properties.state
```

- VMware 拡張機能がインストールされていることを確認します。

```
az extension show --name vmware
```

- 拡張機能がすでにインストールされている場合は、バージョンが 3.0.0 であることを確認してください。古いバージョンがインストールされている場合は、拡張機能を更新してください。

```
az extension update --name vmware
```

1. 拡張機能がまだインストールされていない場合は、インストールしてください。

```
az extension add --name vmware
```

## Azure NetApp Filesボリュームを作成してマウントする

1. Azure Portal 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 プロバイダーを登録するには、`az provider register --namespace Microsoft.NetApp --wait` 指示。登録後、NetAppアカウントを作成します。こちらを参照してください ["リンク"](#) 詳細な手順については、こちらをご覧ください。

Home > Azure NetApp Files >

The screenshot shows the Azure NetApp Files portal. On the left, there's a sidebar with 'Create' and 'Manage view' buttons. Below that is a search bar labeled 'Filter for any field...'. A list of existing accounts is shown: 'ANFAVSAcct' and 'ANFDatstoreacct'. On the right, a large form titled 'New NetApp account' is displayed. It has fields for 'Name' (with placeholder 'Enter the name'), 'Subscription' (set to 'Hybrid Cloud TME Onprem'), 'Resource group' (set to 'ANFAVSAVal2'), 'Location' (set to 'West Europe'), and a 'Create new' button.

1. NetAppアカウントを作成したら、必要なサービス レベルとサイズで容量プールを設定します。詳細については、こちらを参照してください。 ["リンク"](#)。

The screenshot shows the Azure NetApp Files portal. On the left, the sidebar shows 'ANFDatstoreacct' selected. The main area displays 'Capacity pools' with two existing pools: 'ANFRec0DS' and 'ANFRec0DSU'. On the right, a modal window titled 'New capacity pool' is open. It contains fields for 'Name' (placeholder 'Enter the name'), 'Service level' (set to 'Premium'), 'Size (TiB)' (set to '4'), and 'QoS type' (radio button selected for 'Auto').

### 覚えておくべきポイント

- NFSv3 は、Azure NetApp Files上のデータストアでサポートされています。
- 容量制限のあるワークロードには Premium または Standard 層を使用し、必要に応じて、デフォルトの vSAN ストレージを補完しながら、パフォーマンス制限のあるワークロードには Ultra 層を使用します。

1. Azure NetApp Filesの委任されたサブネットを構成し、ボリュームを作成するとき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、こちらを参照してください。 ["リンク"](#)。
2. 容量プール ブレードのボリューム ブレードを使用して、データストアの NFS ボリュームを追加します。

**ANFDatastoreacct | Volumes**

NetApp account

Search (Ctrl+ /)  Add volume  Add data replication  Refresh

Overview  Activity log  Access control (IAM)  Tags  Settings

Search volumes

| Name          | Quota | Throughput    | Protocol type | Mount path             | Service level | Network features | Capacity   |
|---------------|-------|---------------|---------------|------------------------|---------------|------------------|------------|
| anfrecods001  | 4 TiB | 262.144 MiB/s | NFSv3         | 172.30.153.132:/ANFRc  | Premium       | Standard         | anfrecods  |
| anfrecodsu002 | 4 TiB | 524.288 MiB/s | NFSv3         | 172.30.153.132:/anfrec | Ultra         | Standard         | anfrecodsu |

Azure NetApp Filesボリュームのパフォーマンスをサイズまたはクオータ別に確認するには、以下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"。

## Azure NetApp ファイル データストアをプライベート クラウドに追加する



Azure NetApp Filesボリュームは、Azure Portal を使用してプライベート クラウドに接続できます。これに従ってください["Microsoftからのリンク"](#) Azure Portal を使用して Azure NetApp Files データストアをマウントする手順について説明します。

Azure NetApp ファイル データストアをプライベート クラウドに追加するには、次の手順を実行します。

- 必要な機能が登録されたら、適切なコマンドを実行して、NFS データストアを Azure VMware Solution プライベート クラウド クラスターに接続します。
- Azure VMware Solution プライベート クラウド クラスター内の既存の ANF ボリュームを使用してデータストアを作成します。

```
C:\Users\niyaz>az vmware datastore netapp-volume create --name
ANFRecoDSU002 --resource-group anfavsval2 --cluster Cluster-1 --private
--cloud ANFDataClus --volume-id /subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netAp
pAccounts/anfdastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU0
02
{
  "diskPoolVolume": null,
  "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateC
louds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDSU002",
  "name": "ANFRecoDSU002",
  "netAppVolume": {
    "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netAp
pAccounts/anfdastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU0
02",
    "resourceGroup": "anfavsval2"
  },
  "provisioningState": "Succeeded",
  "resourceGroup": "anfavsval2",
  "type": "Microsoft.AVS/privateClouds/clusters/datastores"
}

. List all the datastores in a private cloud cluster.
```

```
C:\Users\niyaz>az vmware データストアリスト --resource-group anfavsval2 --cluster Cluster-1
--private-cloud ANFDataClus [ { "diskPoolVolume": null, "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFDataClus/clusters/
Cluster-1/datastores/ANFRecoDS001", "name": "ANFRecoDS001", "netAppVolume": { "id": "
/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.
NetApp/netAppAccounts/anfdastoreacct/capacityPools/anfrecods/volumes/ANFRecoDS001",
"resourceGroup": "anfavsval2" }, "provisioningState": "Succeeded", "resourceGroup": "anfavsval2", "type": "
Microsoft.AVS/privateClouds/clusters/datastores" }, { "diskPoolVolume": null, "id": "
```

```

"/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsvl2/providers/Microsoft.AVS/privateClouds/ANFDataClus/clusters/
Cluster-1/datastores/ANFRecoDSU002", "name": "ANFRecoDSU002", "netAppVolume": { "id": 
"/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsvl2/providers/Microsoft.
NetApp/netAppAccounts/anfdatystoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002",
"resourceGroup": "anfavsvl2" }, "provisioningState": "Succeeded", "resourceGroup": "anfavsvl2", "type": 
"Microsoft.AVS/privateClouds/clusters/datastores" } ]

```

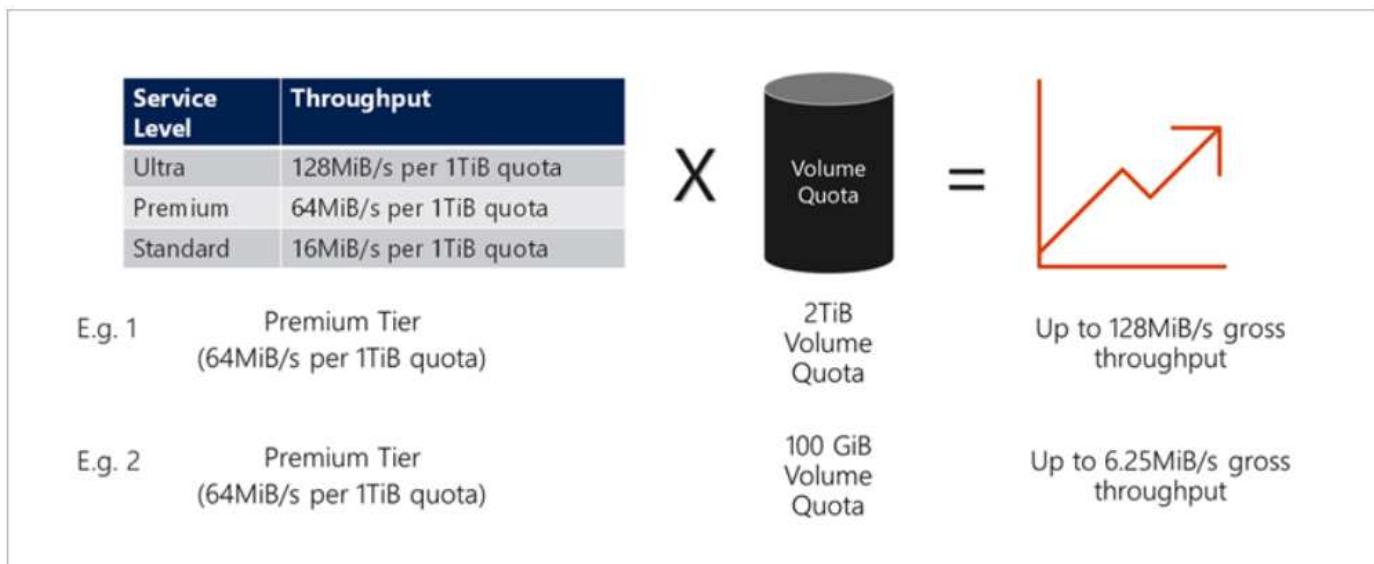
1. 必要な接続が確立されると、ボリュームはデータストアとしてマウントされます。

| Attribute        | Value                                |
|------------------|--------------------------------------|
| Location         | ds://vmfs/volumes/d2abb02d-2c53af49/ |
| Type             | NFS 3                                |
| Hosts            | 3                                    |
| Virtual machines | 2                                    |
| VM templates     | 0                                    |
| Server           | 172.30.136.70                        |
| Folder           | anf-z1-stds01                        |

## サイズとパフォーマンスの最適化

Azure NetApp Files は、Standard (1 テラバイトあたり 16 MBps)、Premium (1 テラバイトあたり 64 MBps)、Ultra (1 テラバイトあたり 128 MBps) の 3 つのサービス レベルをサポートしています。適切なボリューム サイズをプロビジョニングすることは、データベース ワークロードのパフォーマンスを最適化するために重要です。Azure NetApp Files では、ボリュームのパフォーマンスとスループットの制限は次の要因に基づいて決まります。

- ・ボリュームが属する容量プールのサービス レベル
- ・ボリュームに割り当てられたクオータ
- ・容量プールのサービス品質 (QoS) タイプ (自動または手動)



詳細については、以下を参照してください。 "Azure NetApp Filesのサービス レベル"。

こちらを参照してください["Microsoftからのリンク"](#)サイズ設定の演習中に使用できる詳細なパフォーマンス ベンチマーク。

#### 覚えておくべきポイント

- 最適な容量とパフォーマンスを得るには、データストア ボリュームに Premium または Standard 層を使用します。パフォーマンスが必要な場合は、Ultra 層を使用できます。
- ゲスト マウント要件の場合は Premium または Ultra レベルを使用し、ゲスト VM のファイル共有要件の場合は Standard または Premium レベルのボリュームを使用します。

#### パフォーマンスに関する考慮事項

NFS バージョン 3 では、ESXi ホストと単一のストレージ ターゲット間の接続にアクティブなパイプが 1 つしかないことを理解することが重要です。つまり、フェイルオーバーに使用できる代替接続が存在する場合でも、単一のデータストアと基盤となるストレージの帯域幅は、単一の接続で提供できるものに制限されます。

Azure NetApp Filesボリュームで利用可能な帯域幅をさらに活用するには、ESXi ホストにストレージ ターゲットへの複数の接続が必要です。この問題を解決するには、複数のデータストアを構成し、各データストアで ESXi ホストとストレージ間の個別の接続を使用します。

より高い帯域幅を得るには、ベストプラクティスとして、複数の ANF ボリュームを使用して複数のデータストアを作成し、VMDK を作成し、論理ボリュームを VMDK 全体にストライピング化します。

こちらを参照してください["Microsoftからのリンク"](#)サイズ設定の演習中に使用できる詳細なパフォーマンス ベンチマーク。

## 覚えておくべきポイント

- Azure VMware ソリューションでは、既定で 8 つの NFS データストアが許可されます。これはサポートリクエストを通じて増やすことができます。
- ER ファストパスと Ultra SKU を併用して、より高い帯域幅とより低いレイテンシを実現します。詳細情報
- Azure NetApp ファイルの「基本」ネットワーク機能では、Azure VMware Solution からの接続は、ExpressRoute 回線と ExpressRoute ゲートウェイの帯域幅によって制限されます。
- 「Standard」ネットワーク機能を備えた Azure NetApp Files ボリュームでは、ExpressRoute FastPath がサポートされます。有効にすると、FastPath はゲートウェイをバイパスしてネットワーク トラフィックを Azure NetApp Files ボリュームに直接送信し、より高い帯域幅とより低い待機時間を実現します。

## データストアのサイズを増やす

ボリュームの再形成と動的なサービス レベルの変更は、SDDC に対して完全に透過的です。Azure NetApp Files では、これらの機能により、継続的なパフォーマンス、容量、コストの最適化が実現します。Azure Portal または CLI を使用してボリュームのサイズを変更し、NFS データストアのサイズを増やします。完了したら、vCenter にアクセスし、データストア タブに移動して適切なデータストアを右クリックし、「容量情報の更新」を選択します。このアプローチを使用すると、ダウンタイムなしでデータストアの容量を増やし、データストアのパフォーマンスを動的に向上させることができます。このプロセスもアプリケーションに対して完全に透過的です。

## 覚えておくべきポイント

- ボリュームの再形成と動的サービス レベル機能により、安定した状態のワークロードに合わせてサイズを設定することでコストを最適化し、過剰プロビジョニングを回避できます。
- VAAI が無効になっています。

## ワークロード

### 移住

最も一般的なユースケースの 1 つは移行です。VMware HCX または vMotion を使用してオンプレミスの VM を移動します。あるいは、Rivermeadow を使用して VM を Azure NetApp Files データストアに移行することもできます。

## データ保護

VM のバックアップと迅速な回復は、ANF データストアの大きな強みの 1 つです。スナップショット コピーを使用すると、パフォーマンスに影響を与えることなく VM またはデータストアのクイック コピーを作成し、それを Azure ストレージに送信して長期的なデータ保護を行うか、クロス リージョン レプリケーションを使用してセカンダリ リージョンに送信して災害復旧を行うことができます。このアプローチでは、変更された情報のみを保存することで、ストレージスペースとネットワーク帯域幅を最小限に抑えます。

一般的な保護には Azure NetApp Files スナップショット コピーを使用し、ゲスト VM 上に存在する SQL Server や Oracle などのトランザクション データを保護するためにアプリケーション ツールを使用します。これらのスナップショット コピーは VMware (一貫性) スナップショットとは異なり、長期的な保護に適しています。



ANF データストアでは、「新しいボリュームに復元」オプションを使用してデータストア ボリューム全体のクローンを作成し、復元されたボリュームを AVS SDDC 内のホストに別のデータストアとしてマウントできます。データストアをマウントすると、その中の VM は、個別にクローン作成された VM であるかのように登録、再構成、カスタマイズできるようになります。

## 仮想マシンのBlueXP backup and recovery

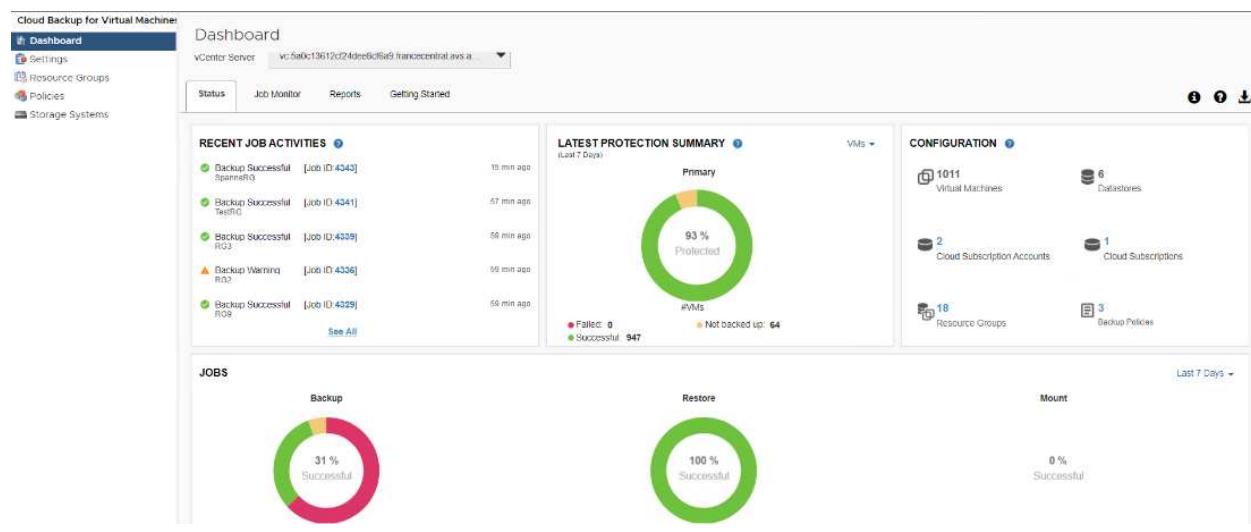
BlueXP backup and recoveryでは、vCenter 上の vSphere Web クライアント GUI が提供され、バックアップ ポリシーを通じて Azure VMware Solution 仮想マシンと Azure NetApp ファイル データストアを保護します。これらのポリシーでは、スケジュール、保持期間、その他の機能を定義できます。BlueXP backup and recovery機能は、実行コマンドを使用して展開できます。

セットアップと保護ポリシーは、次の手順を実行してインストールできます。

1. 実行コマンドを使用して、Azure VMware Solution プライベート クラウドの仮想マシン用のBlueXP backup and recoveryをインストールします。
2. クラウド サブスクリプションの資格情報(クライアントとシークレット値)を追加し、保護するリソースが含まれるクラウド サブスクリプション アカウント(NetAppアカウントと関連付けられたリソース グループ)を追加します。
3. リソース グループ バックアップの保持期間、頻度、その他の設定を管理する1つ以上のバックアップ ポリシーを作成します。
4. バックアップ ポリシーで保護する必要がある1つ以上のリソースを追加するためのコンテナーを作成します。
5. 障害が発生した場合は、VM 全体または特定の個別の VMDK を同じ場所に復元します。



Azure NetApp Filesスナップショット テクノロジーにより、バックアップと復元が非常に高速になります。



## Azure NetApp Files、JetStream DR、Azure VMware Solution を使用した災害復旧

クラウドへの災害復旧は、サイトの停止やデータ破損イベント（ランサムウェアなど）からワークコードを保護する、回復力がありコスト効率に優れた方法です。VMware VAIO フレームワークを使用すると、オンプレミスの VMware ワークロードを Azure Blob ストレージに複製して回復できるため、データ損失を最小限に抑えるか、ほぼゼロにすることができ、RTO はほぼゼロになります。JetStream DR を使用すると、オンプレミスから AVS、具体的には Azure NetApp Files に複製されたワークコードをシームレスに回復できます。DR サイトでの最小限のリソースとコスト効率の高いクラウドストレージを使用することで、コスト効率の高い災害復旧が可能になります。JetStream DR は、Azure Blob Storage を介して ANF データストアへのリカバリを自動化します。JetStream DR は、ネットワークマッピングに従って、独立した VM または関連する VM のグループをリカバリ サイトインフラストラクチャに復元し、ランサムウェア保護のためのポイントインタイムリカバリを提供します。

"ANF、JetStream、AVS を使用した DR ソリューション"。

## Azure 向け NetApp ゲスト接続ストレージ オプション

Azure は、ネイティブの Azure NetApp Files (ANF) サービスまたは Cloud Volumes ONTAP (CVO) を使用して、ゲスト接続された NetApp ストレージをサポートします。

### Azure NetApp Files(ANF)

Azure NetApp Files は、エンタープライズグレードのデータ管理とストレージを Azure に提供するため、ワークコードとアプリケーションを簡単に管理できます。ワークコードをクラウドに移行し、パフォーマンスを犠牲にすることなく実行します。

Azure NetApp Files は障害を取り除き、すべてのファイルベースのアプリケーションを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がなくなり、複雑さなしでアプリケーション用の永続ストレージを利用できるようになります。

サービスは Microsoft Azure ポータルを通じて提供されるため、ユーザーは Microsoft エンタープライズ契約の一環として完全に管理されたサービスを体験できます。Microsoft が管理する世界クラスのサポートにより、完全な安心感が得られます。この単一のソリューションにより、マルチプロトコルのワークコードを迅速かつ簡単に追加できます。レガシー環境でも、Windows と Linux の両方のファイルベースのアプリケーションを構築および展開できます。

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

### Azure VMware Solution (AVS) を使用して Azure NetApp Files を構成する

Azure NetApp Files 共有は、Azure VMware Solution SDDC 環境で作成された VM からマウントできます。Azure NetApp Files は SMB および NFS プロトコルをサポートしているため、ボリュームを Linux クライアントにマウントし、Windows クライアントにマップ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 Solution は同じ Azure リージョンに存在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する

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 Portal 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、`az provider register --namespace Microsoft.NetApp -wait` コマンドを使用してAzure NetApp Filesリソース プロバイダーを登録します。登録が完了したら、NetAppアカウントを作成します。

詳細な手順については、"Azure NetApp Files共有"。このページでは、手順を順に説明します。

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and various navigation icons. Below the header, the breadcrumb navigation shows 'Home > Azure NetApp Files >'. The main content area is titled 'New NetApp account'. The form fields are as follows:

- Name \*: nimoAVSANFDemo
- Subscription: SaaS Backup Production
- Resource group \*: NimoAVSDemo
- Location \*: East US 2

At the bottom of the form, there are two buttons: 'Create' and 'Download a template for automation'.

2. NetAppアカウントを作成したら、必要なサービス レベルとサイズで容量プールを設定します。

詳細については、以下を参照してください。"容量プールを設定する"。

The screenshot shows the Azure NetApp Files interface. On the left, there's a navigation pane with 'Create', 'Manage view', and a search bar. The main area is titled 'nimoAVSANFdemo | Capacity pools'. It has a search bar and a table with columns 'Name', 'Capacity', and 'Service level'. Below the table, it says 'You don't have any capacity pools. Click Add pool to get started.' On the right, a modal window titled 'New capacity pool' is open, showing fields for 'Name' (set to 'nimappool'), 'Service level' (set to 'Standard'), 'Size (TiB)' (set to '4'), and 'QoS type' (set to 'Auto'). At the bottom of the modal are 'Create' and 'Discard' buttons.

3. Azure NetApp Filesの委任されたサブネットを構成し、ボリュームの作成時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、"サブネットをAzure NetApp Filesに委任する"。

The screenshot shows the Azure portal's 'Virtual network' section. On the left, there's a navigation pane with 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Settings', 'Address space', 'Connected devices', 'Subnets' (which is selected), 'DDoS protection', 'Firewall', and 'Security'. The main area is titled 'nimoavspiv-vnet | Subnets'. It has a search bar and a table with columns 'Name' and 'GatewaySubnet'. A new subnet named 'anf.del' is being added. The configuration form includes fields for 'Name' (set to 'anf.del'), 'Subnet address range' (set to '172.24.3.0/28'), 'Add IPv6 address space' (unchecked), 'NAT gateway' (set to 'None'), 'Network security group' (set to 'None'), and 'Route table' (set to 'None'). At the bottom of the form are 'Save' and 'Cancel' buttons.

4. [容量プール] ブレードの下の [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 コネクタが構成されていることを確認してください。

The screenshot shows the 'nimoAVSANFdemo | Active Directory connections' page in the Azure NetApp Files portal. On the left, there's a sidebar with options like 'Create', 'Manage view', 'Filter for any field...', 'Name', and a search bar. The main area shows 'No currently joined Active Directories.' On the right, the 'Join Active Directory' form is displayed with fields for Primary DNS (172.24.1.5), Secondary DNS, AD DNS Domain Name (nimdemo.com), AD Site Name, SMB Server (Computer Account) Prefix (nimsmrb), and Organizational Unit Path. A 'Join' button is at the bottom.

5. [確認 + 作成] 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 の継続的な可用性を有効にします。

The screenshot shows the 'nimoAVSANFdemo | Volumes' page. The sidebar includes 'Active Directory connections', 'Storage service', 'Capacity pools', and 'Volumes'. The main area shows a message: 'You don't have any volumes. Click Add volume to get started.' On the right, the 'Create a volume' dialog is open, showing the 'Basics' tab. It has fields for 'Volume name' (nimvoltest1), 'Capacity pool' (nimcappool), 'Available quota (GiB)' (4096), and 'Quota (GiB)' (100). Buttons at the bottom include 'Review + create' (highlighted in blue), '< Previous', and 'Next : Protocol >'.

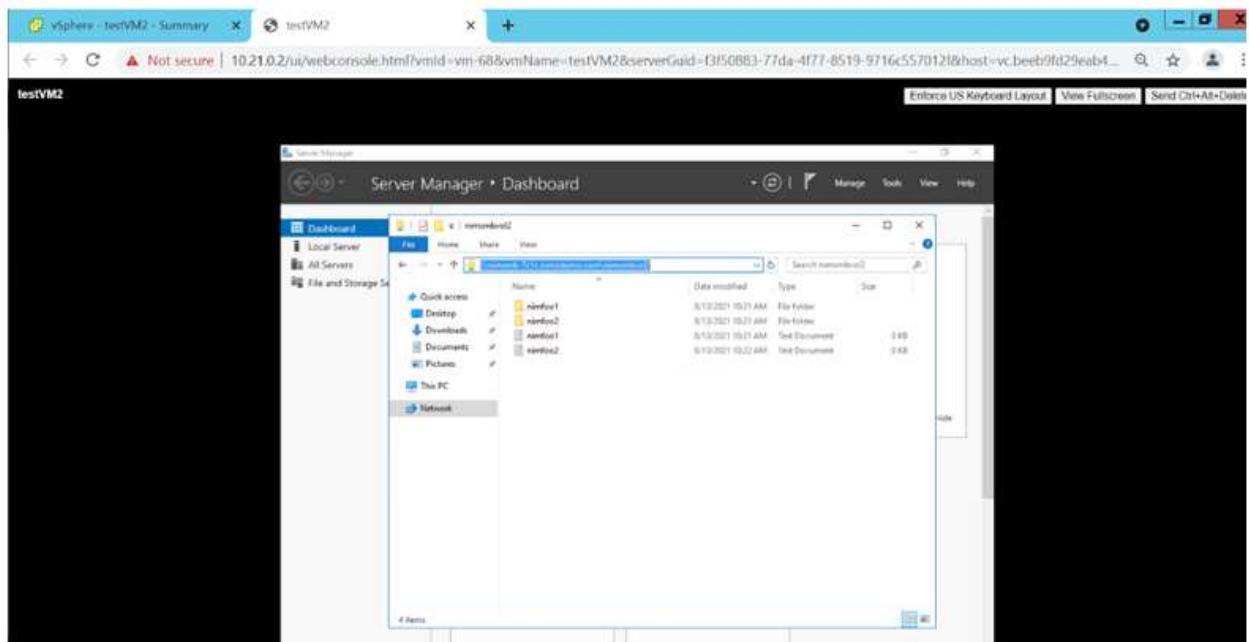
The screenshot shows the Azure NetApp Files portal interface. At the top, there's a navigation bar with 'Home > Azure NetApp Files > nimoAVSANFdemo'. Below it is a search bar and a 'Add volume' button. On the left, a sidebar has options like 'Quota', 'Properties', 'Locks', 'Azure NetApp Files', and 'Active Directory connections'. The main area is titled 'nimoAVSANFdemo | Volumes' and contains a table with columns: Name, Quota, Throughput, Protocol type, Mount path, Service level, and Capacity per. Two volumes are listed:

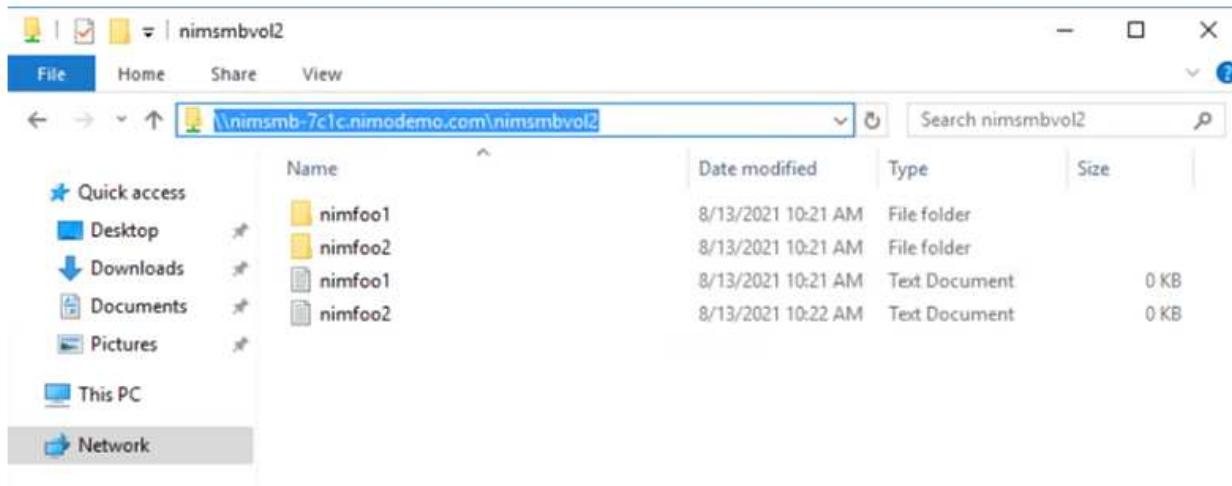
| Name        | Quota   | Throughput | Protocol type | Mount path             | Service level | Capacity per |
|-------------|---------|------------|---------------|------------------------|---------------|--------------|
| nimsmbvol2  | 100 GiB | 1.6 MiB/s  | SMB           | \\\nimsmb-7c1c.nimodr  | Standard      | nimcappoo    |
| nimvoltest1 | 100 GiB | 1.6 MiB/s  | NFSv3         | 172.24.3.4/nimvoltest1 | Standard      | nimcappoo    |

Azure NetApp Filesボリュームのサイズまたはクオータ別のパフォーマンスの詳細については、以下の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。

これを実行するには、Azure ポータルから [ボリューム] 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 ドライブのマップ] オプションを使用して、Azure VMware Solution SDDC で実行されている VM にボリュームをマウントします。





7. Azure VMware Solution 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には、同じプロセスを使用します。ボリュームの再形成または動的サービス レベル機能を使用して、ワークロードの要求を満たします。

```
nimoadmin@nimoadmin-virtual-machine:~$ sudo mount -t nfs -o rw,hard,tcp 172.24.3.4:/nimodemonfs1 /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 7982752  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
tmpfs            224256   224256     0 100% /snap/gnome-3-34-180
4/72
/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:/nimodemonfs1 104857600     0 104857600  0% /home/nimoadmin/nimodemo11
nimoadmin@nimoadmin-virtual-machine:~$
```

詳細については、以下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、NetApp のONTAPストレージ ソフトウェア上に構築された業界をリードするクラウド データ管理ソリューションであり、Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP) でネイティブに利用できます。

これはクラウドネイティブ ストレージを使用するONTAPのソフトウェア定義バージョンであり、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、データを管理するためのまったく新しい方法について IT スタッフを再トレーニングする必要性が軽減されます。

CVO により、エッジからデータセンター、クラウドへとシームレスにデータを移動し、ハイブリッド クラウドを統合することが可能になります。これらはすべて、単一ペインの管理コンソールであるNetApp Cloud Manager で管理されます。

CVOは設計上、クラウドで最も要求の厳しいアプリケーションにも対応できる優れたパフォーマンスと高度なデータ管理機能を提供します。

#### ゲスト接続ストレージとしての**Cloud Volumes ONTAP (CVO)**

## Azureに新しいCloud Volumes ONTAPを導入する

Cloud Volumes ONTAP共有と LUN は、Azure VMware Solution 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 プロトコルをサポートしているため、ボリュームは Linux クライアントと 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セットアップできます。

災害復旧または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へのデータの複製については、このドキュメントの範囲外です。オンプレミスとCloud Volumes ONTAPシステム間でデータを複製するには、["システム間のデータ複製の設定"](#)。



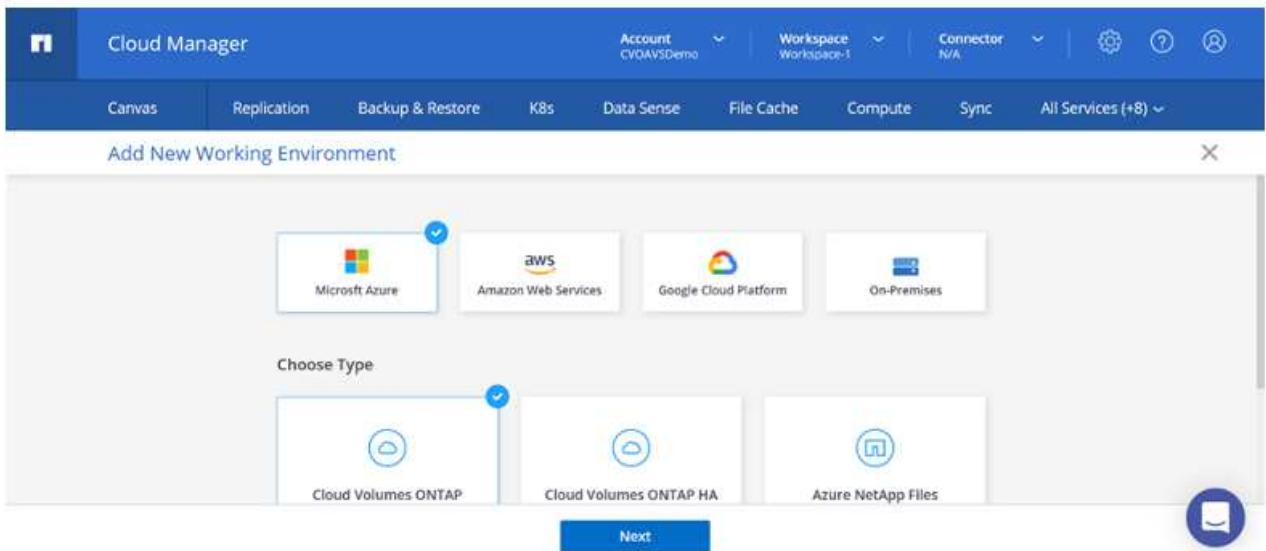
使用["Cloud Volumes ONTAPサイザー"](#)Cloud Volumes ONTAPインスタンスのサイズを正確に決定します。また、オンプレミスのパフォーマンスを監視して、Cloud Volumes ONTAPサイザーの入力として使用します。

1. NetApp Cloud Central にログインすると、Fabric View 画面が表示されます。Cloud Volumes ONTAPタブを見つけて、「Go to Cloud Manager」を選択します。ログインすると、Canvas 画面が表示されます。

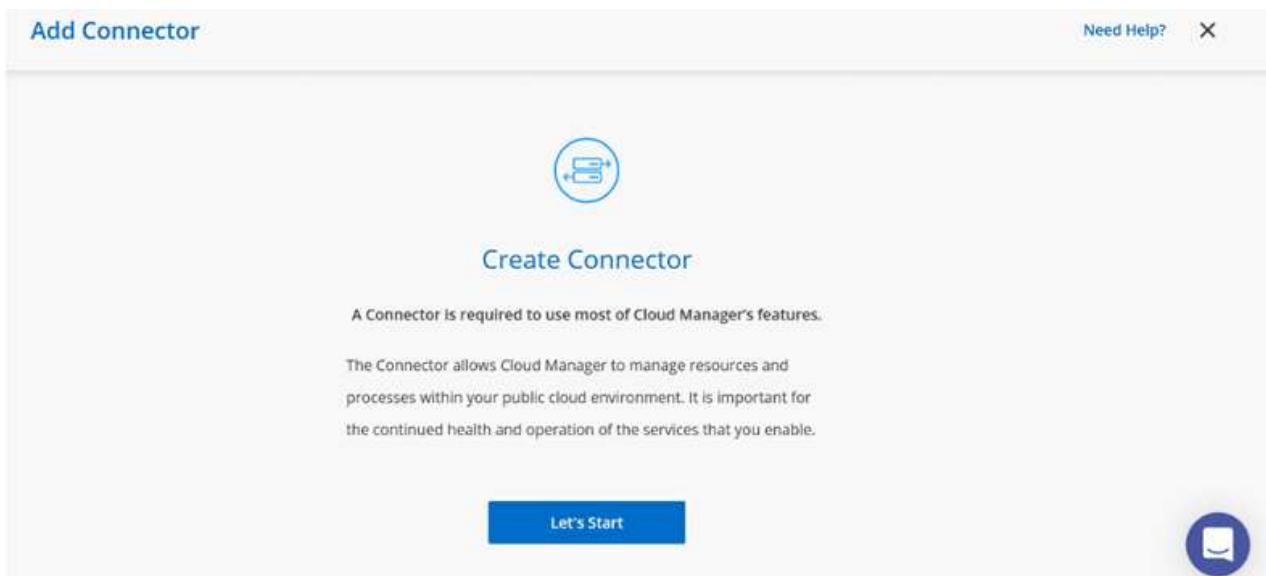
This is how you deploy, allocate or discover your cloud storage.  
(Cloud Volumes ONTAP, Cloud Volumes Service, on-prem ONTAP or S3 buckets.)

Add Working Environment

2. Cloud Manager のホームページで、「作業環境の追加」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。



- 最初のCloud Volumes ONTAP作業環境を作成するときに、Cloud Manager によってコネクタをデプロイするように求められます。



- コネクタが作成されたら、詳細および資格情報フィールドを更新します。

## Create a New Working Environment

## Details and Credentials

|                        |                     |                          |                                  |
|------------------------|---------------------|--------------------------|----------------------------------|
| Managed Service Ide... | SaaS Backup Prod... | CMCVOSub                 | <a href="#">Edit Credentials</a> |
| Credential Name        | Azure Subscription  | Marketplace Subscription |                                  |

Details

Working Environment Name (Cluster Name)  
nimavscVO

Credentials

User Name  
admin

Password

[Continue](#)

5. 環境名や管理者の資格情報など、作成する環境の詳細を指定します。オプション パラメーターとして、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。

## Create a New Working Environment

## Details and Credentials

|  |  |
|--|--|
| Details  | Credentials                                    |
| Working Environment Name (Cluster Name)<br>nimavscVO   | User Name<br>admin                             |
| <a href="#">Add Resource Group Tags</a> Optional Field | Password<br>*****<br>Confirm Password<br>***** |

[Continue](#)

6. BlueXP分類、BlueXP backup and recovery、Cloud Insightsなど、Cloud Volumes ONTAPデプロイメントのアドオン サービスを選択します。サービスを選択し、「続行」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](#)

7. Azure の場所と接続を構成します。使用する Azure リージョン、リソース グループ、VNet、サブネットを選択します。

Create a New Working Environment

### Location & Connectivity

|  |  |
|--|--|
| Azure Region<br>East US 2                        | Resource Group<br><input checked="" type="radio"/> Create a new group <input type="radio"/> Use an existing group.               |
| Availability Zone<br>Select an Availability Zone | Resource Group Name<br>nimavscv0-rg  |
| VNet<br>nimavspiv-vnet   NimioAVSDemo            | Security Group<br><input checked="" type="radio"/> Generated security group <input type="radio"/> Use existing security group    |
| Subnet<br>172.24.2.0/24                          | <input checked="" type="checkbox"/> I have verified network connectivity between the Cloud Manager server and the selected VNet. |
| <a href="#">Continue</a>                         |  |

- 既存のライセンスを使用する場合は、ライセンス オプション (Pay-As-You-Go または BYOL) を選択します。この例では、Pay-As-You-Go オプションが使用されています。

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

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

- さまざまな種類のワークロードに使用できる、事前構成された複数のパッケージから選択します。

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.

|  |   |  |   |
|--|---|--|---|
| <br>POC and small workloads<br>Up to 500GB of storage | <br>Database and application data production workloads | <br>Cost effective DR<br>Up to 500GB of storage | <br>Highest performance production workloads |
| <a href="#">Continue</a>   |   |  |   |

- 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。

The screenshot shows the 'Create a New Working Environment' interface. At the top, it displays 'nimavsCVO' under 'Azure | East US 2'. Below this are two checked checkboxes: 'I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp.' and 'I understand that Cloud Manager will allocate the appropriate Azure resources to comply with my above requirements.' The 'Overview' tab is selected. A prominent blue 'Go' button is located at the bottom right.

11. Cloud Volumes ONTAPがプロビジョニングされると、Canvas ページの作業環境にリストされます。

The screenshot shows the 'Canvas' page with various tabs like Replication, Backup & Restore, K8s, Data Sense, File Cache, Compute, Sync, and All Services (+8). The 'Canvas' tab is active. On the left, there's a 'Add Working Environment' section with a cloud icon labeled 'SINGLE nimavsCVO Cloud Volumes ONTAP Freemium'. On the right, the 'nimavsCVO' entry is listed under 'SERVICES' with options to edit, view details, or delete. The 'DETAILS' section shows 'Cloud Volumes ONTAP | Azure | Single'. A 'Replication' tab is also visible.

## SMBボリュームの追加構成

1. 作業環境の準備ができたら、CIFS サーバーが適切な DNS および Active Directory 構成パラメータで構成されていることを確認します。SMB ボリュームを作成する前にこの手順を実行する必要があります。

The screenshot shows the Nimav CVO interface with the following details:

- Volume Name:** nimavssmbvol1
- Size (GB):** 50
- Active Directory Domain to join:** nimodemo.com
- Credentials authorized to join the domain:** nimoadmin (password obscured)

2. SMB ボリュームの作成は簡単なプロセスです。ボリュームを作成する CVO インスタンスを選択し、「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すると、クラウドマネージャーはそれを含む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 SMB が選択されています。

The screenshot shows the 'Volume Details, Protection & Protocol' configuration page:

| Details & Protection |                     | Protocol        |
|----------------------|---------------------|-----------------|
| Volume Name:         | nimavssmbvol1       | Size (GB): 50   |
| Snapshot Policy:     | default             | NFS             |
|                      |                     | CIFS (selected) |
|                      |                     | iSCSI           |
| Share name:          | nimavssmbvol1_share |                 |
| Permissions:         | Full Control        |                 |
| Users / Groups:      | Everyone;           |                 |

**Protocol:** CIFS (selected)

**Share name:** nimavssmbvol1\_share

**Permissions:** Full Control

**Users / Groups:** Everyone;

**Continue**

3. ボリュームがプロビジョニングされると、ボリュームペインで使用できるようになります。CIFS 共有がプロビジョニングされているため、ユーザーまたはグループにファイルとフォルダーへの権限を与え、それらのユーザーが共有にアクセスしてファイルを作成できることを確認します。ボリュームがオンプレミス環境から複製される場合、ファイルとフォルダの権限はすべてSnapMirrorレプリケーションの一部として保持されるため、この手順は必要ありません。

Volumes      Replications

**Volumes**

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

| INFO           |             | CAPACITY  |           |
|----------------|-------------|-----------|-----------|
| Disk Type      | PREMIUM_LRS | 1.74 MB   | Disk Used |
| Tiering Policy | Auto        | 0 GB      | Blob Used |
| Backup         | OFF         | Allocated |           |

4. ボリュームが作成されたら、マウント コマンドを使用して、Azure VMware Solution 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 ドライブのマップ] オプションを使用して、Azure VMware Solution SDDC で実行されている VM にボリュームをマウントします。

---

Volumes      Replications

[Mount Volume nimavssmbvol1](#)

Go to your machine and enter this command

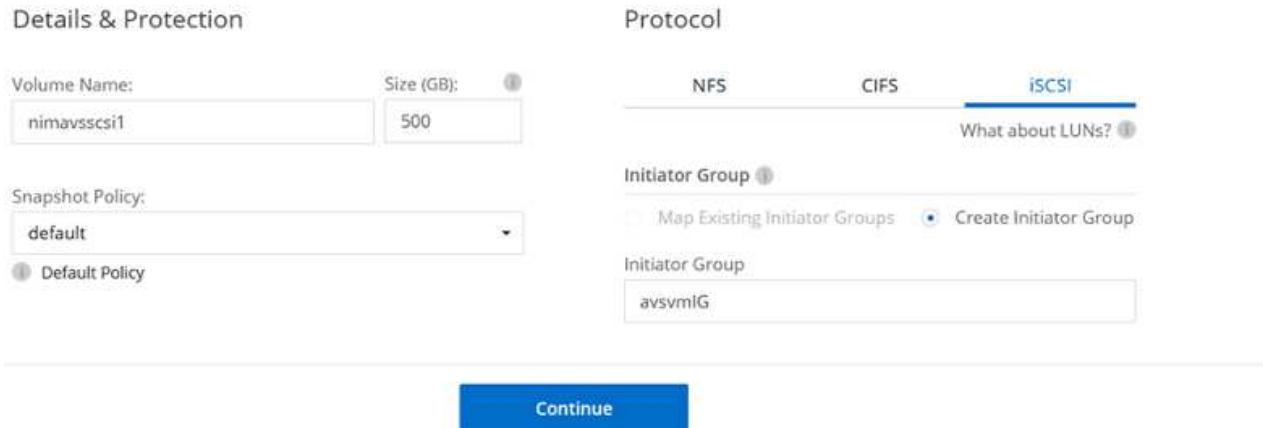
`\\"172.24.2.8\\nimavssmbvol1_share`

[Copy](#)

## LUNをホストに接続する

LUN をホストに接続するには、次の手順を実行します。

1. Canvas 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. [ボリュームの追加] > [新しいボリューム] をクリックし、[iSCSI] を選択して [イニシエーター グループの作成] をクリックします。[Continue]をクリックします。

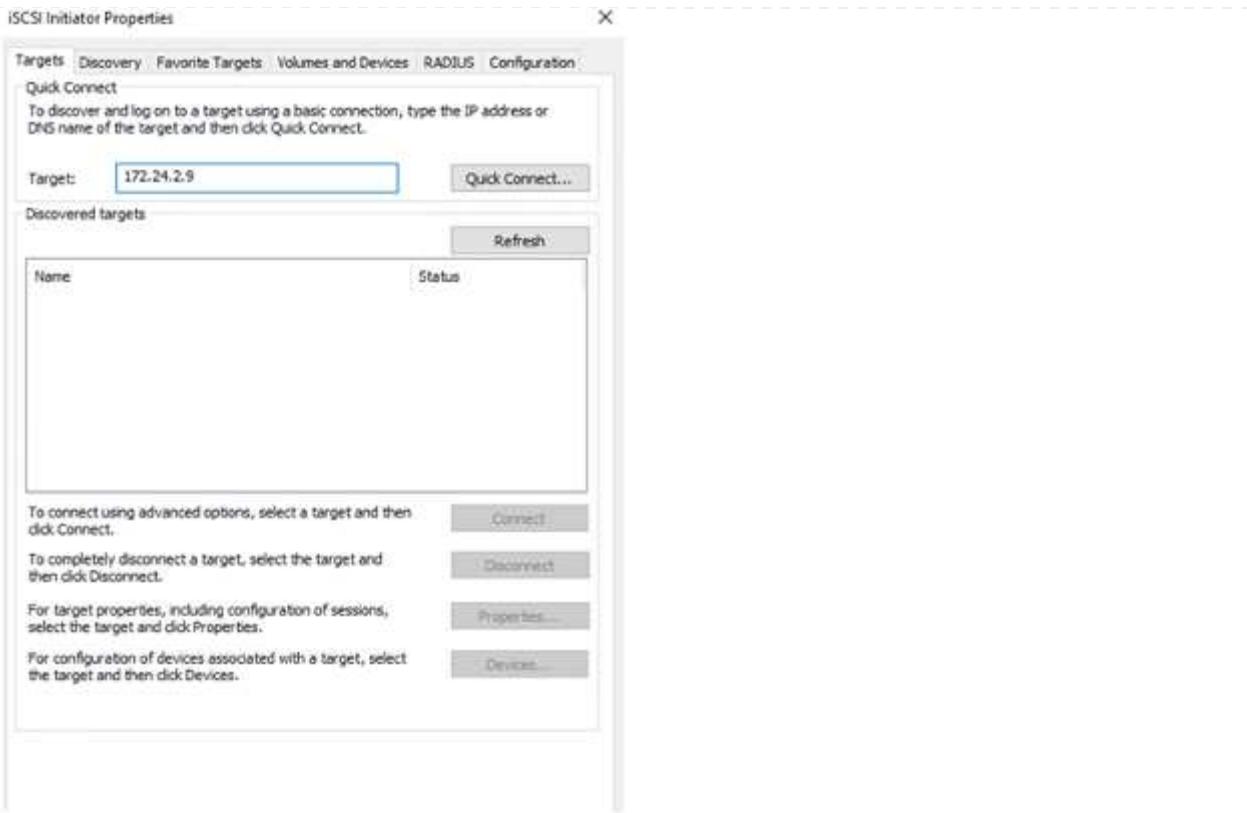


3. ボリュームがプロビジョニングされたら、ボリュームを選択し、「ターゲット IQN」をクリックします。iSCSI 修飾名 (IQN) をコピーするには、[コピー] をクリックします。ホストから LUN への iSCSI 接続を設定します。

Azure VMware Solution SDDC に存在するホストに対して同じことを実現するには、次の手順を実行します。

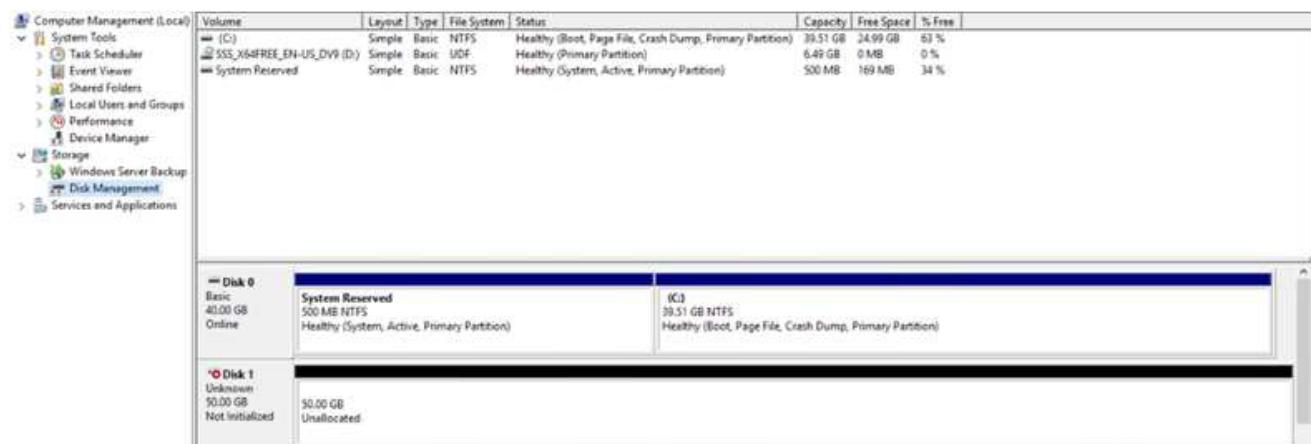
- a. Azure VMware Solution SDDC でホストされている VM に RDP 接続します。
- b. iSCSI イニシエーターのプロパティ ダイアログ ボックスを開きます: サーバー マネージャー > ダッシュボード > ツール > iSCSI イニシエーター。
- c. [検出] タブで、[ポータルの検出] または [ポータルの追加] をクリックし、iSCSI ターゲット ポートの IP アドレスを入力します。
- d. [ターゲット] タブで、検出されたターゲットを選択し、[ログオン] または [接続] をクリックします。
- e. [マルチパスを有効にする] を選択し、[コンピューター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のターゲットのリストに追加する] を選択します。[Advanced]をクリックします。

注: Windows ホストは、クラスター内の各ノードへの iSCSI 接続を持っている必要があります。標準のDSMによって最適なパスが選択され、



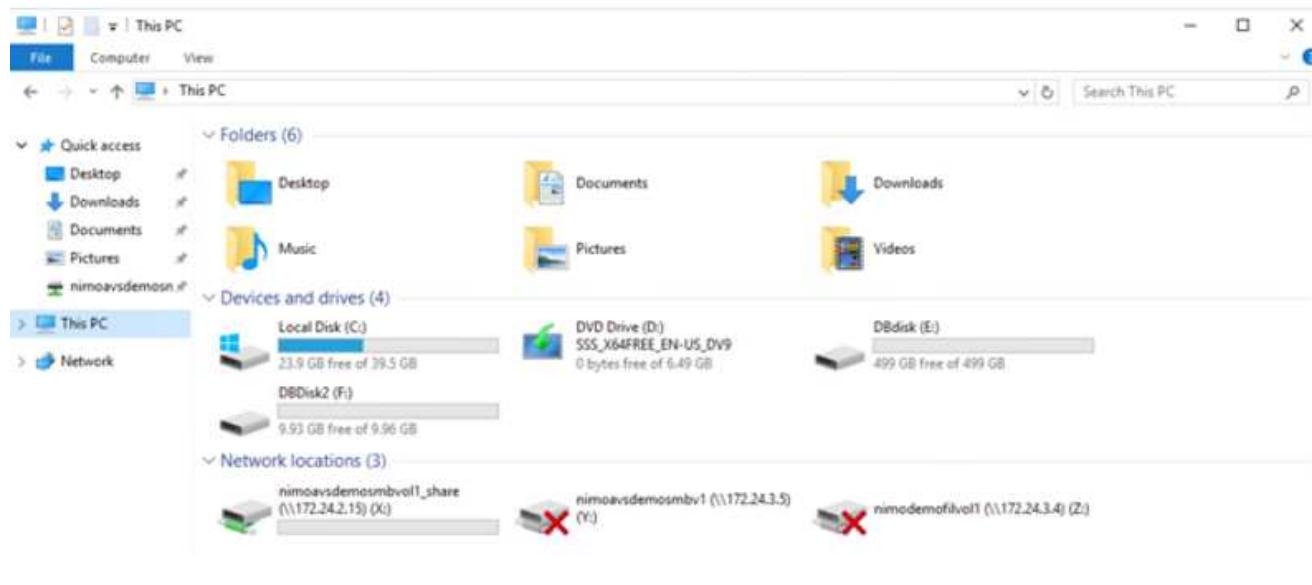
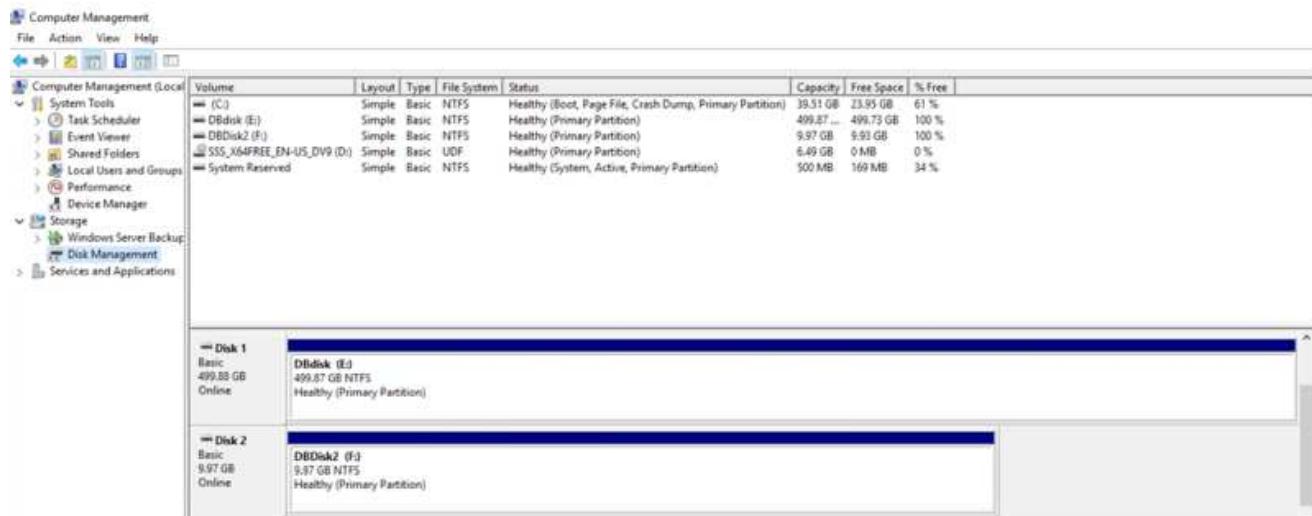
ストレージ仮想マシン (SVM) 上の LUN は、Windows ホストに対してディスクとして表示されます。追加された新しいディスクは、ホストによって自動的に検出されません。次の手順を実行して、手動での再スキャンをトリガーし、ディスクを検出します。

1. Windows のコンピューターの管理ユーティリティを開きます (スタート > 管理ツール > コンピューターの管理)。
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] をクリックします。



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、オプションで次の手順を実行して、LUN をファイルシステムでフォーマットします。

1. Windowsの[ディスクの管理]を起動します。
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種類を選択します。
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ストレージを使用するためのオプション

NetAppストレージは、ゲスト接続ストレージまたは補助ストレージとして Google Cloud Virtualization Engine に接続できます。

### 補助的な NFS データストアとしてのGoogle Cloud NetApp Volumes (NetApp Volumes)

Google Cloud VMware Engine (GCVE) 環境で追加のストレージ容量が必要なお客様は、Google Cloud NetApp Volumesを利用して、補足の NFS データストアとしてマウントできます。Google Cloud NetApp Volumesにデータを保存することで、リージョン間でデータを複製し、災害から保護することができます。

詳細については、"補助的な NFS データストアとしてのGoogle Cloud NetApp Volumes (NetApp Volumes)"

## ゲスト接続ストレージとしてのNetApp CVO

Cloud Volumes ONTAP(CVO) は、NetApp のONTAPストレージ ソフトウェア上に構築された業界をリードするクラウド データ管理ソリューションであり、Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP) でネイティブに利用できます。

これはクラウドネイティブ ストレージを使用するONTAPのソフトウェア定義バージョンであり、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、データを管理するためのまったく新しい方法について IT スタッフを再トレーニングする必要性が軽減されます。

CVO により、エッジからデータセンター、クラウドへとシームレスにデータを移動し、ハイブリッド クラウドを統合することが可能になります。これらはすべて、単一ペインの管理コンソールであるNetApp Cloud Manager で管理されます。

CVO は設計上、クラウドで最も要求の厳しいアプリケーションにも対応できる極めて優れたパフォーマンスと高度なデータ管理機能を提供します。

詳細については、["ゲスト接続ストレージとしてのNetApp CVO"](#)

## ゲスト接続ストレージとしてのGoogle Cloud NetApp Volumes (NetApp Volumes)

Google Cloud NetApp Volumes共有は、VMware Engine 環境で作成された VM からマウントできます。 Google Cloud NetApp Volumes はSMB および NFS プロトコルをサポートしているため、ボリュームを Linux クライアントにマウントし、Windows クライアントにマップすることもできます。 Google Cloud NetApp Volumesボリュームは簡単な手順で設定できます。

Google Cloud NetApp Volumesと Google Cloud VMware Engine プライベート クラウドは同じリージョンに存在する必要があります。

詳細については、["ゲスト接続ストレージとしてのGoogle Cloud NetApp Volumes \(NetApp Volumes\)"](#)

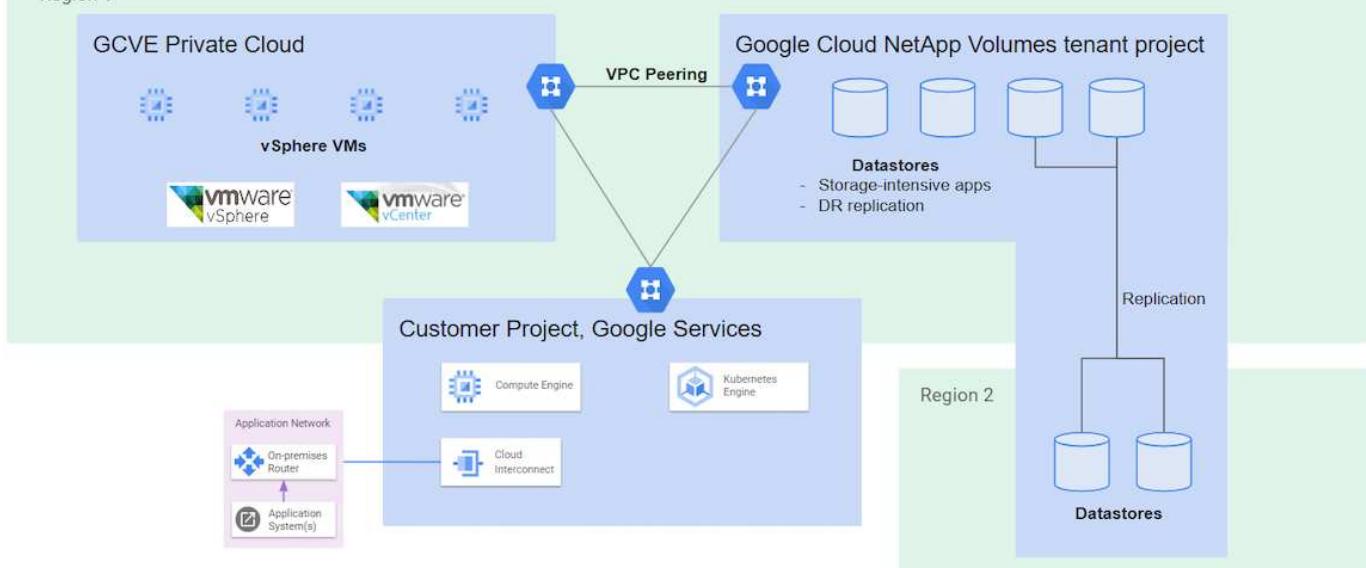
## Google Cloud VMware Engine の補足 NFS データストアとGoogle Cloud NetApp Volumes

お客様は、Google Cloud NetApp Volumesの NFS 補足データストアを使用して、Google Cloud VMware Engine 上のストレージ容量を拡張できます。

### 概要

Google Cloud VMware Engine (GCVE) 環境で追加のストレージ容量が必要なお客様は、Netapp Cloud Volume Service を利用して補足の NFS データストアとしてマウントできます。 Google Cloud NetApp Volumesにデータを保存することで、リージョン間でデータを複製し、災害から保護することができます。

Region 1



**GCVE 上の Google Cloud NetApp Volumes (NetApp Volumes) から NFS データストアをマウントするためのデプロイメント手順**

#### NetAppボリュームのプロビジョニング - パフォーマンスボリューム

Google Cloud NetApp Volumesボリュームは、["Google Cloud Console の使用"](#) ["NetApp BlueXPポータルまたはAPIを使用する"](#)

## NetApp Volumesボリュームを削除不可としてマークする

VMの実行中にボリュームが誤って削除されるのを防ぐには、以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してマークされていることを確認してください。

Cloud Volumes

← Edit File System

Storage Pools

Volumes

Backups

Snapshots

Active Directories

Volume Replication

Project Settings

Extreme

Up to 128 MiB/s per TiB

Volume Details

Allocated Capacity \* 1024 GiB

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

Managing your volumes for growth. [Learn more](#)

Protocol Type NFSv3

Active Directory must be setup to provision an SMB or dual-protocol volume. The Allow local NFS users with LDAP option in Active Directory connections enables local NFS client users not present on the Windows LDAP server to access a dual-protocol volume that has LDAP with extended groups enabled. [Learn more](#)

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 LDAP  
Enables user look up from AD LDAP server for your NFS volumes

Block volume from deletion when clients are connected  
Required for volumes used as GCVE datastores

Export Policy

詳細については、"NFSボリュームの作成"ドキュメント。

NetApp Volumes Tenant VPC に対して 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 Volumes プロジェクト間にプライベート接続が存在している必要があります。詳細については、"プライベートサービスアクセスの設定方法"

## NFSデータストアをマウントする

GCVEにNFSデータストアをマウントする方法については、以下を参照してください。["NetApp Volumes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 によって管理されているため、NFS vSphere API for Array Integration (VAAI) vSphere Installation Bundle (VIB) をインストールする権限はありません。仮想ボリューム (vVol) のサポートが必要な場合は、お知らせください。ジャンボフレームを使用する場合は、["GCP でサポートされる最大 MTU サイズ"](#)

## Google Cloud NetApp Volumesによる節約

GCVE のストレージ需要に対する Google Cloud NetApp Volumes の潜在的な節約の詳細については、以下をご覧ください。["NetApp ROI 計算ツール"](#)

## 参考リンク

- ["Google ブログ - Google Cloud VMware Engine のデータストアとしてNetApp Volumes を使用する方法"](#)
- ["NetApp ブログ - ストレージを多用するアプリを Google Cloud に移行するよりよい方法"](#)

## GCP 向けNetAppストレージ オプション

GCP は、Cloud Volumes ONTAP (CVO) または Google Cloud NetApp Volumes (NetApp Volumes) を使用してゲスト接続された NetAppストレージをサポートします。

### Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP(CVO) は、NetApp のONTAPストレージ ソフトウェア上に構築された業界をリードするクラウド データ管理ソリューションであり、Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP) でネイティブに利用できます。

これはクラウドネイティブストレージを使用するONTAPのソフトウェア定義バージョンであり、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、データを管理するためのまったく新しい方法について IT スタッフを再トレーニングする必要性が軽減されます。

CVO により、エッジからデータセンター、クラウドへとシームレスにデータを移動し、ハイブリッド クラウドを統合することが可能になります。これらはすべて、単一ペインの管理コンソールであるNetApp Cloud Manager で管理されます。

CVOは設計上、クラウドで最も要求の厳しいアプリケーションにも対応できる優れたパフォーマンスと高度なデータ管理機能を提供します。

### ゲスト接続ストレージとしてのCloud Volumes ONTAP (CVO)

## Google Cloud にCloud Volumes ONTAPをデプロイする（自分で行う）

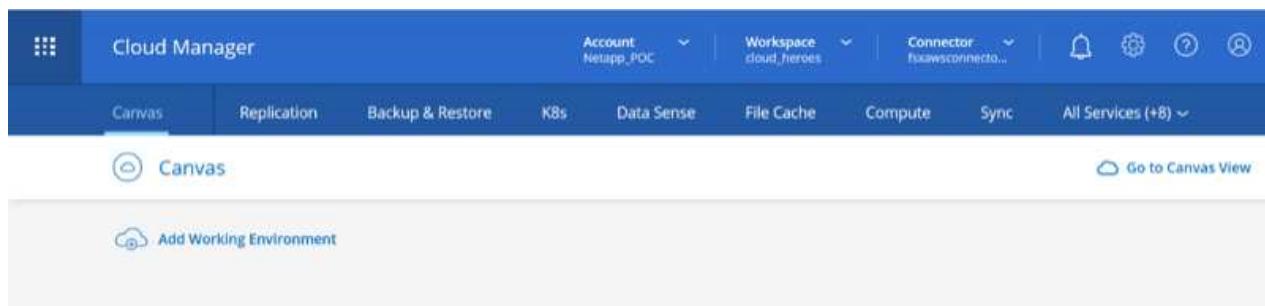
Cloud Volumes ONTAP共有と LUN は、GCVE プライベート クラウド環境で作成された VM からマウントできます。Cloud Volumes ONTAP はiSCSI、SMB、NFS プロトコルをサポートしているため、ボリュームは Linux クライアントと Windows クライアントにマウントすることもでき、iSCSI 経由でマウントすると、Linux または Windows クライアントでブロック デバイスとして LUN にアクセスできます。Cloud Volumes ONTAPボリュームは、いくつかの簡単な手順でセットアップできます。

障害復旧または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複製するには、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へのデータの複製については、このドキュメントの範囲外です。オンプレミスとCloud Volumes ONTAPシステム間でデータを複製するには、["システム間のデータ複製の設定"](#)。

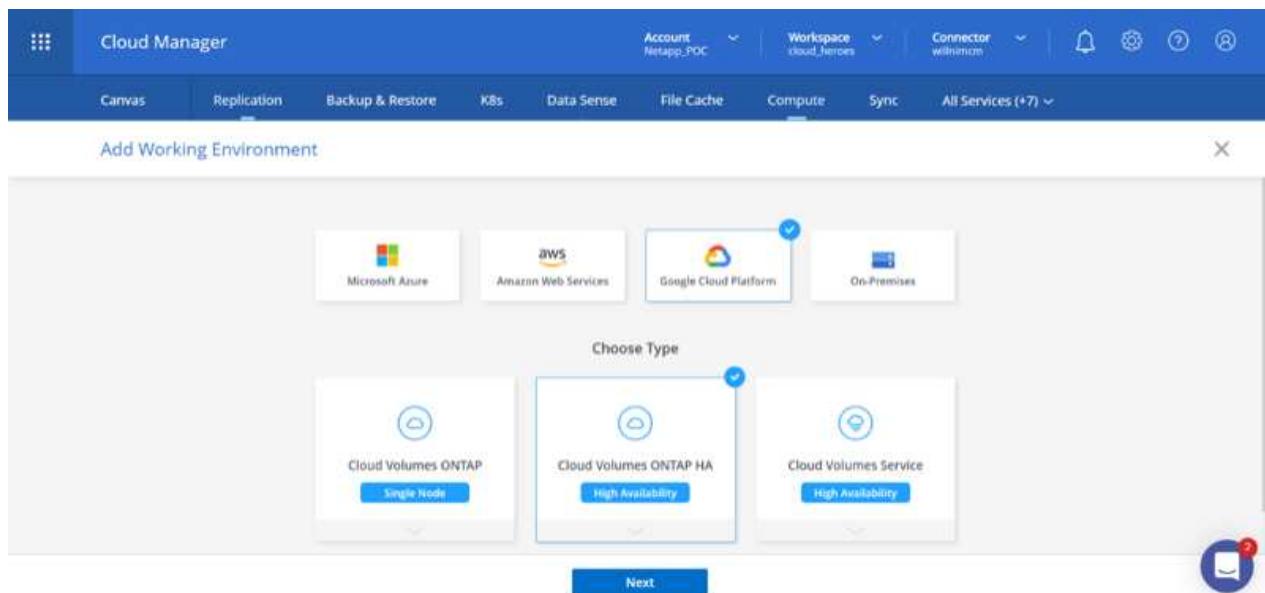


使用["Cloud Volumes ONTAPサイザー"](#)Cloud Volumes ONTAPインスタンスのサイズを正確に決定します。また、オンプレミスのパフォーマンスを監視して、Cloud Volumes ONTAPサイザーの入力として使用します。

1. NetApp Cloud Central にログインすると、Fabric View 画面が表示されます。Cloud Volumes ONTAPタブを見つけて、「Go to Cloud Manager」を選択します。ログインすると、Canvas 画面が表示されます。



2. Cloud Manager Canvas タブで、「作業環境の追加」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. 環境名や管理者の資格情報など、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。

Create a New Working Environment

Details and Credentials

↑ Previous Step CV-Performance-Testing HCLMainBillingAccountSubs...  
Google Cloud Project Marketplace Subscription Edit Project

Details

Working Environment Name (Cluster Name)  
cvogcveva

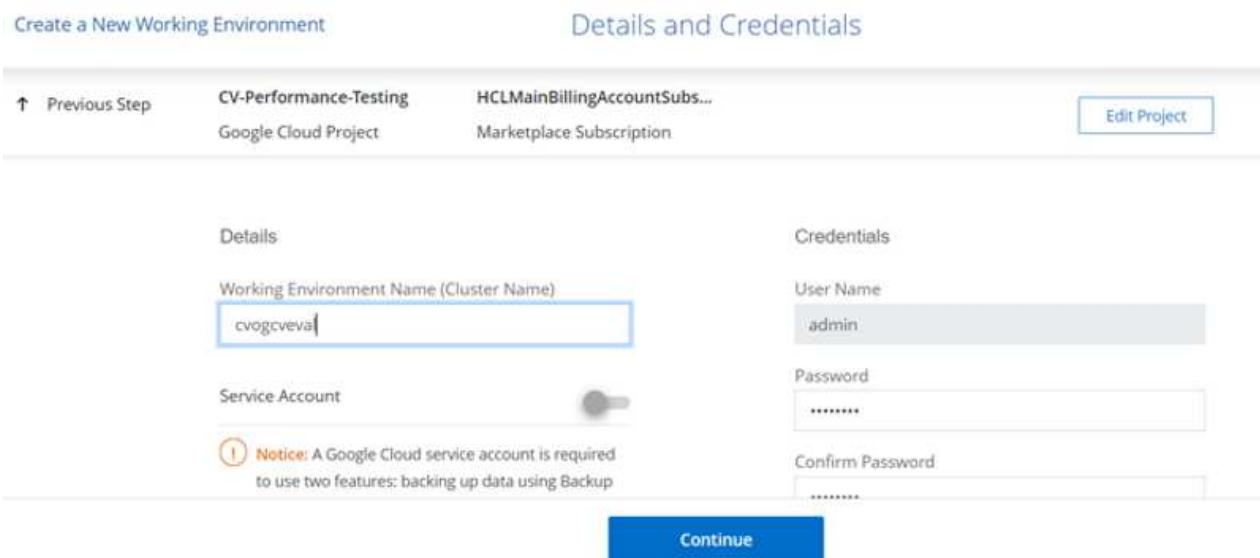
Service Account

**Notice:** A Google Cloud service account is required to use two features: backing up data using Backup

Credentials

User Name admin  
Password .....  
Confirm Password .....

Continue



4. Data Sense & Compliance や Backup to Cloud など、Cloud Volumes ONTAPデプロイメントのアドオン 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 サービスを非アクティブ化すると、確認のポップアップ メッセージが表示されます。アドオン サービスはCVO の導入後に追加/削除できますが、コストを避けるために最初から必要ない場合は選択解除することを検討してください。

Create a New Working Environment

Services

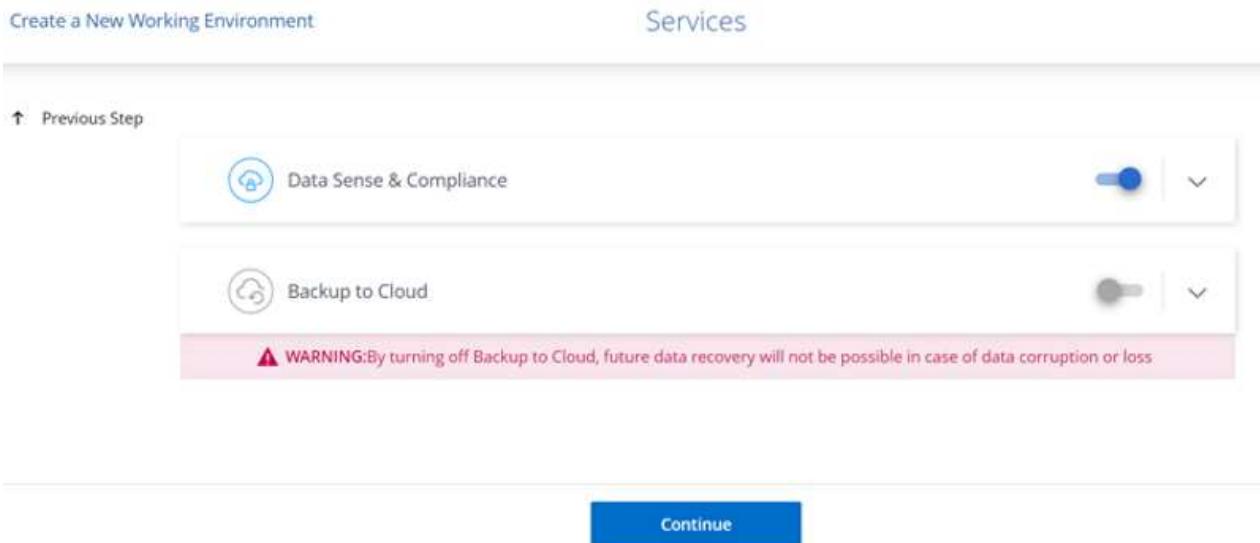
↑ Previous Step

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



5. 場所を選択し、ファイアウォール ポリシーを選択して、チェックボックスをオンにして、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

## Connectivity

## GCP Region

europe-west3

## VPC

cloud-volumes-vpc

## GCP Zone

europe-west3-c

## Subnet

10.0.6.0/24

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

## Firewall Policy

Generated firewall policy  Use existing firewall policy

[Continue](#)

6. 既存のライセンスを使用する場合は、ライセンス オプション (Pay-As-You-Go または BYOL) 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

## NetApp Support Site Account

[Learn more about our charging methods](#)[Learn more about NetApp Support Site \(NSS\) accounts](#) Pay-As-You-Go by the hour Bring your own license Freemium (Up to 500GB)

## NetApp Support Site Account

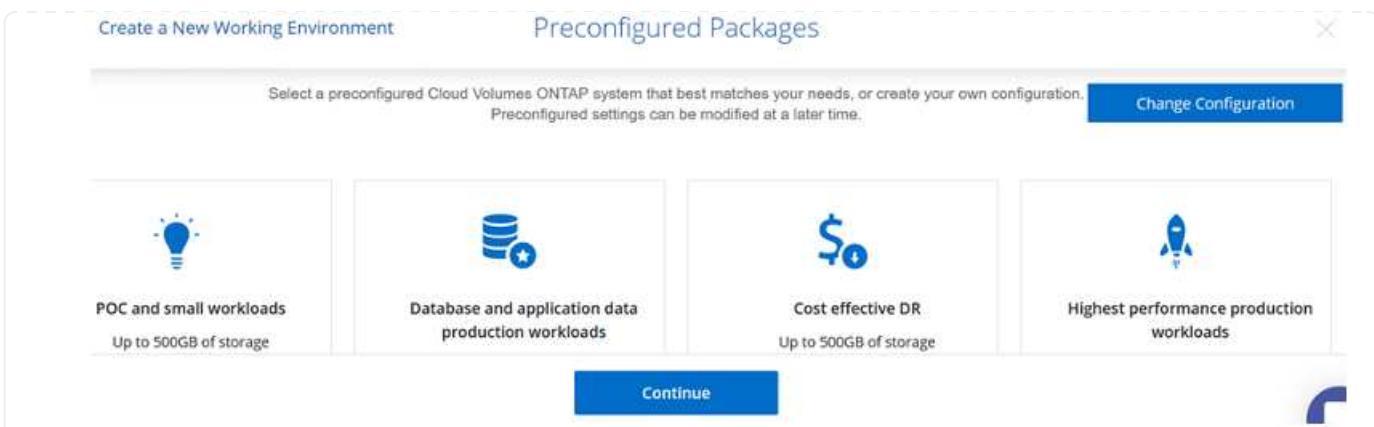
mchad

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

[Continue](#)

7. VMware Cloud on AWS SDDC で実行されている VM に展開されるワークフローのタイプに基づいて、利用可能ないくつかの事前構成済みパッケージから選択します。

ヒント: タイルの上にマウスを移動すると詳細が表示されます。また、[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することもできます。



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、[実行] をクリックします。

|                 |                              |                              |                      |
|-----------------|------------------------------|------------------------------|----------------------|
| 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               |

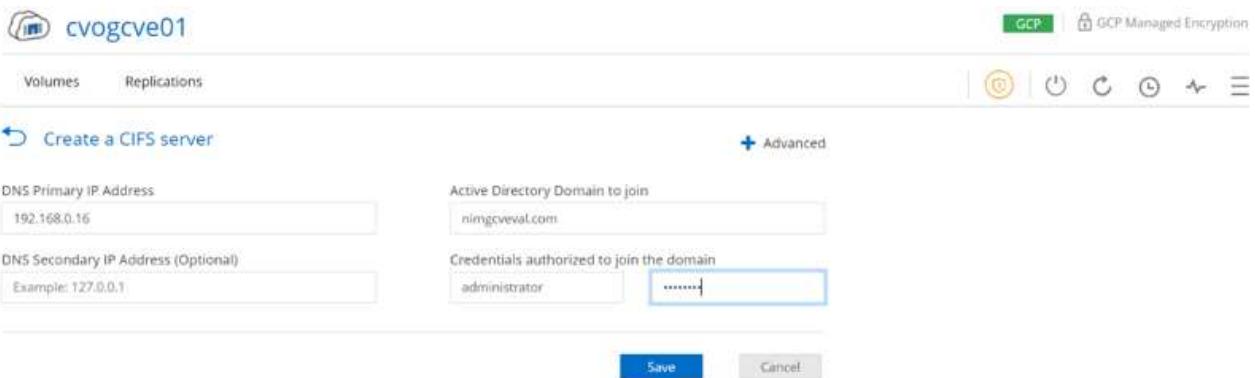
9. Cloud Volumes ONTAPがプロビジョニングされると、Canvas ページの作業環境にリストされます。

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

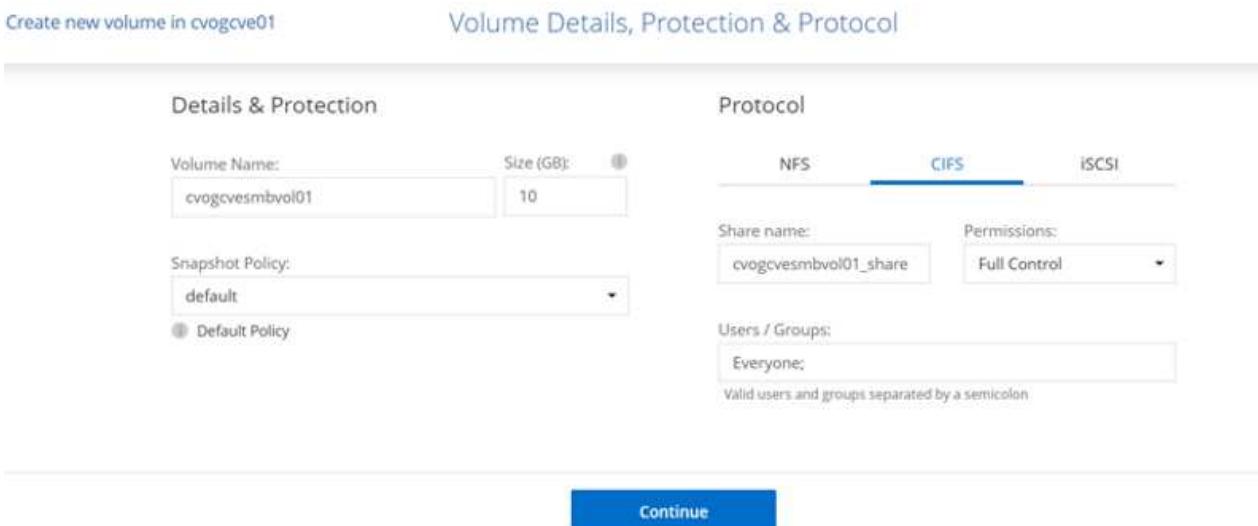
## SMBボリュームの追加構成

1. 作業環境の準備ができたら、CIFS サーバーが適切な DNS および Active Directory 構成パラメータで構成されていることを確認します。SMB ボリュームを作成する前にこの手順を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] を選択して他のオプションを表示し、[CIFS 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。Canvas 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すると、クラウド マネージャーはそれを含む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 が選択されています。



Create new volume in cvogcve01      Volume Details, Protection & Protocol

Details & Protection      Protocol

Volume Name: cvogcvesmbvol01      Size (GB): 10

Snapshot Policy: default

Share name: cvogcvesmbvol01\_share      Permissions: Full Control

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

Continue

3. ボリュームがプロビジョニングされると、ボリューム ペインで使用できるようになります。CIFS 共有がプロビジョニングされているため、ユーザーまたはグループにファイルとフォルダーへの権限を与え、それらのユーザーが共有にアクセスしてファイルを作成できることを確認します。ボリュームがオンプレミス環境から複製される場合、ファイルとフォルダの権限はすべて SnapMirror レプリケーションの一部として保持されるため、この手順は必要ありません。

ヒント: 音量メニュー (°) をクリックするとオプションが表示されます。



4. ボリュームが作成されたら、マウント 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、ネットワーク ドライブのマップ 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: Y:

Folder: \\10.0.6.251\cvogcvesmbvol01\_share

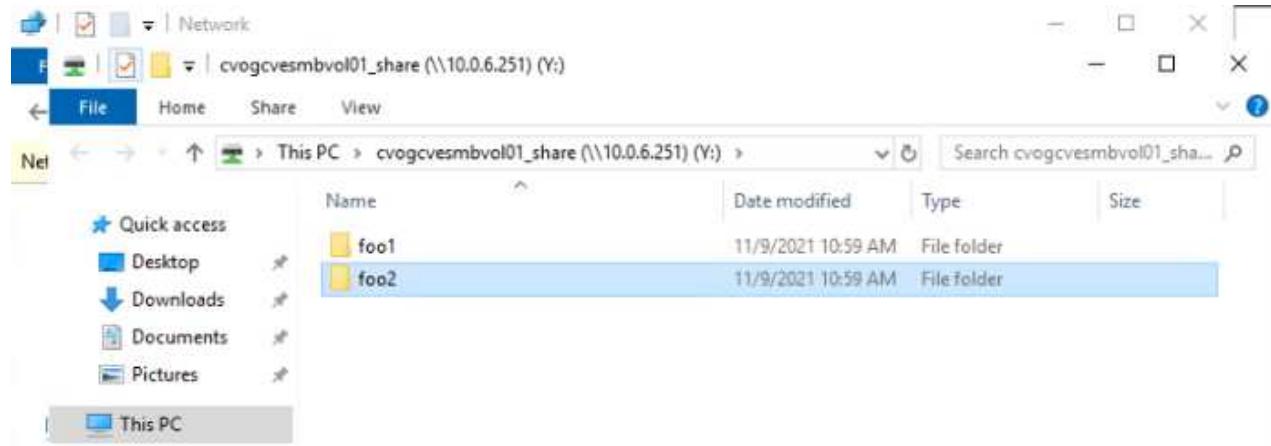
Example: \\server\share

Reconnect at sign-in

Connect using different credentials

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

一度マップすると、簡単にアクセスできるようになります、それに応じて NTFS アクセス許可を設定できます。



## Cloud Volumes ONTAP上のLUNをホストに接続する

クラウド ボリュームONTAP LUN をホストに接続するには、次の手順を実行します。

1. Canvas 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. [ボリュームの追加] > [新しいボリューム] をクリックし、[iSCSI] を選択して [イニシエーター グループの作成] をクリックします。[Continue]をクリックします。

The screenshot shows two windows side-by-side. The top window is titled 'Volume Details, Protection & Protocol' and is part of the 'Create new volume in cvogcve01' process. It has tabs for 'Details & Protection' and 'Protocol'. Under 'Protocol', the 'iSCSI' tab is selected. It shows fields for 'Volume Name' (cvogcvescsilun01), 'Size (GB)' (10), 'Snapshot Policy' (default), and 'Initiator Group' (WinG). The bottom window is titled 'vmcdc01' and shows the 'Server Manager - Dashboard'. It displays the 'File and Storage Services' role status, showing 'AD DS' as manageable. A file browser window is open, showing a folder structure under 'This PC > vmcdc01\_share (\\172.16.0.2) (D)'. The desktop taskbar includes icons for VMware Cloud, vSphere, and NetApp Cloud Manager.

3. ボリュームがプロビジョニングされたら、ボリューム メニュー (º) を選択し、[ターゲット iQN] をクリックします。iSCSI 修飾名 (iQN) をコピーするには、[コピー] をクリックします。ホストから LUN への iSCSI 接続を設定します。

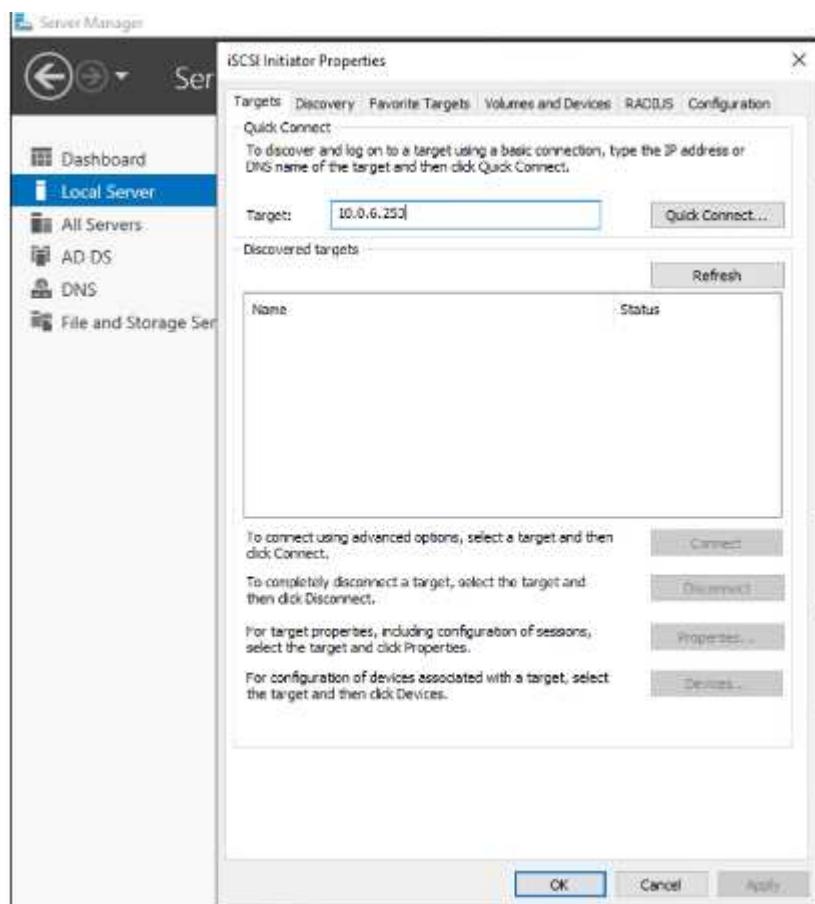
Google Cloud VMware Engine 上にあるホストで同じことを実現するには、次の手順を実行します。

1. Google Cloud VMware Engine でホストされている VM に RDP 接続します。

2. iSCSI イニシエーターのプロパティ ダイアログ ボックスを開きます: サーバー マネージャー > ダッシュボード > ツール > iSCSI イニシエーター。
3. [検出] タブで、[ポータルの検出] または [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、[コンピューター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のターゲットのリストに追加する] を選択します。[Advanced]をクリックします。

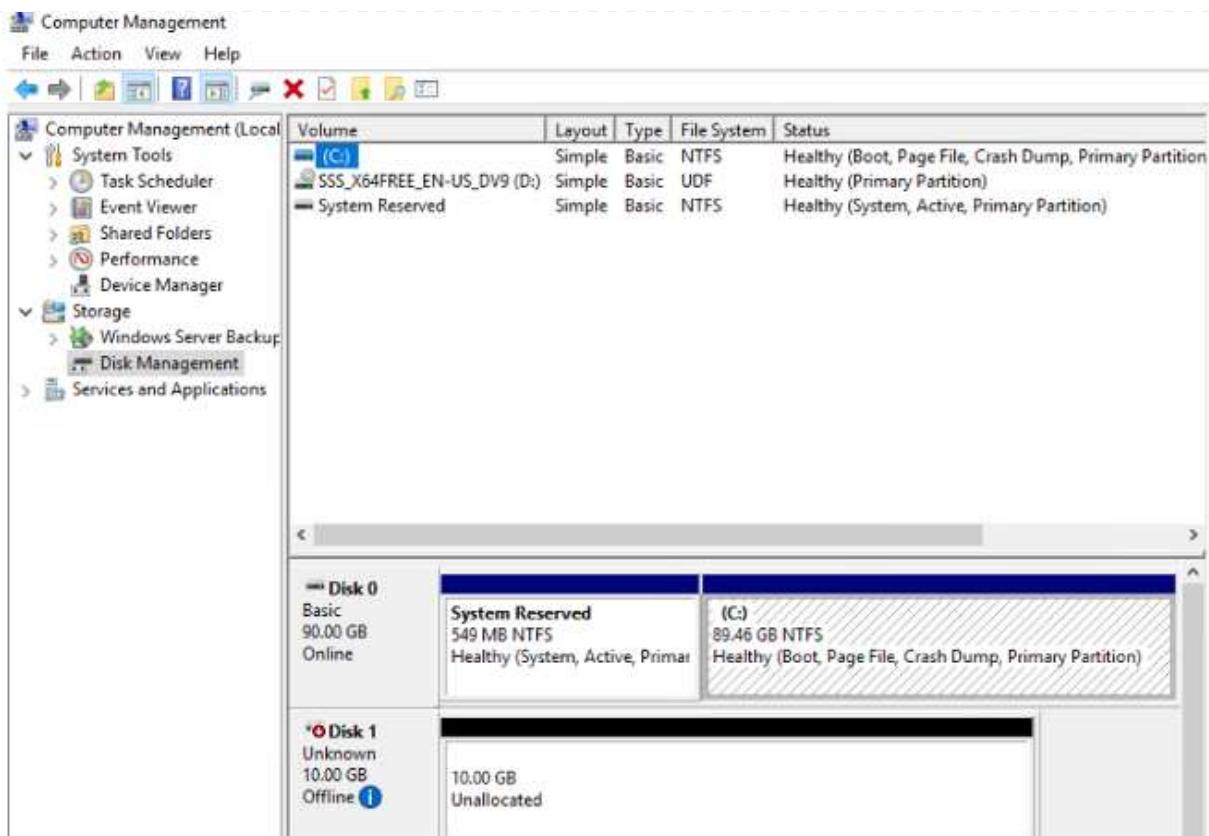


Windowsホストには、クラスタ内のそれぞれのノードへのiSCSI接続が必要です。標準のDSMによって最適なパスが選択され、



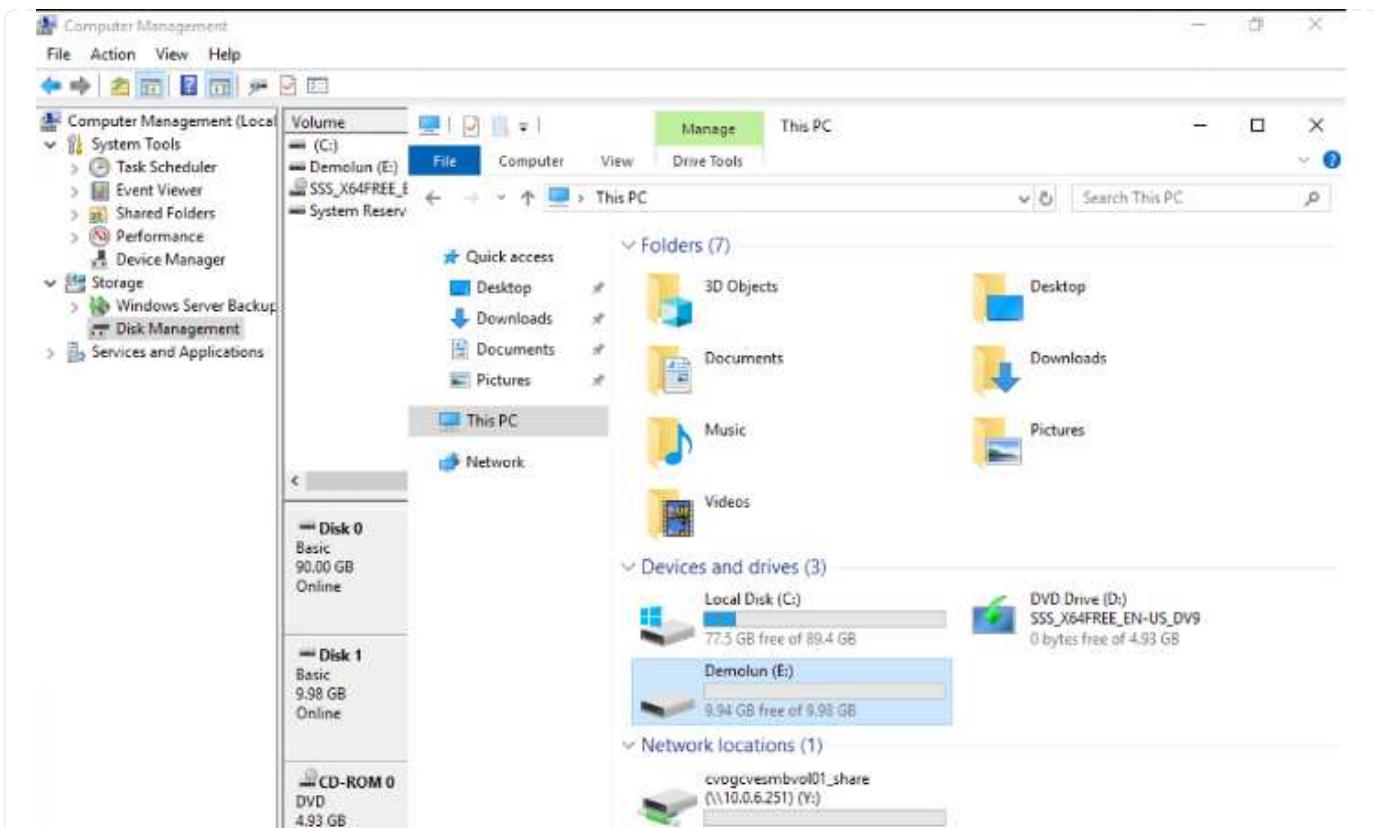
ストレージ仮想マシン (SVM) 上の LUN は、Windows ホストに対してディスクとして表示されます。追加された新しいディスクは、ホストによって自動的に検出されません。次の手順を実行して、手動での再スキャンをトリガーし、ディスクを検出します。

- a. Windows のコンピューターの管理ユーティリティを開きます (スタート > 管理ツール > コンピューターの管理)。
- 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] をクリックします。



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、オプションで次の手順を実行して、LUNをファイルシステムでフォーマットします。

- Windowsの[ディスクの管理]を起動します。
- 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種類を選択します。
- 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 がプロビジョニングされたら、Ubuntu を例として iSCSI 構成に関する詳細なガイダンスをここで参照してください。確認するには、シェルから `lsblk` cmd を実行します。

```
nlyaz@nimbubus:~$ 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/13648
loop6    7:6    0 55.5M  1 loop /snap/core18/2246
loop7    7:7    0   4K  1 loop /snap/barre/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/eft
└─sda2   8:2    0   1K  0 part
└─sda5   8:5    0 15.5G 0 part /
sdb      8:16   0   1G  0 disk
```

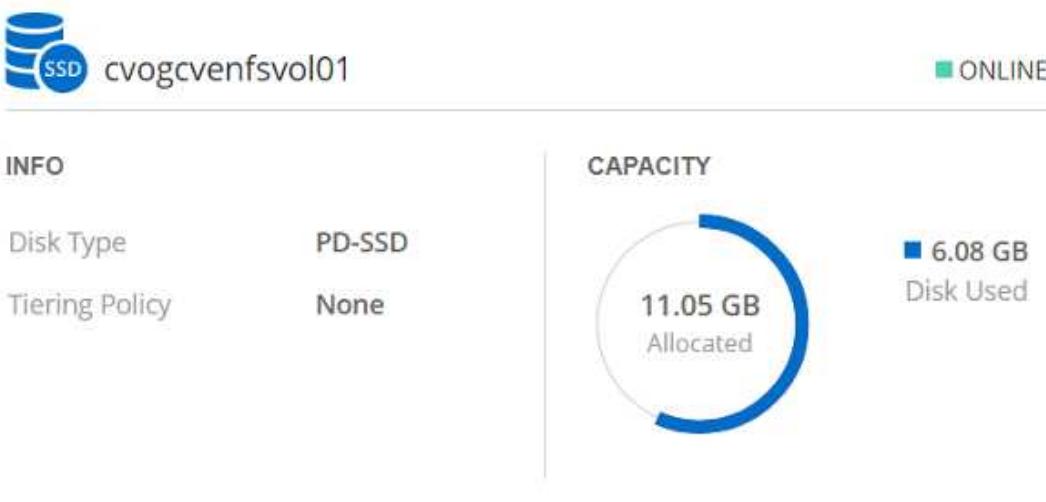
```
piyaz@nimubu01:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G   0    1.9G  0% /dev
tmpfs           394M  1.5M  392M  1% /run
/dev/sda5        16G   7.6G  6.9G  53% /
tmpfs           2.0G   0    2.0G  0% /dev/shm
tmpfs           5.0M   0    5.0M  0% /run/lock
tmpfs           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  967M  1% /mnt
```

## LinuxクライアントにCloud Volumes ONTAP NFSボリュームをマウントする

Google Cloud VMware Engine 内の VM からCloud Volumes ONTAP（DIY）ファイルシステムをマウントするには、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. [ボリューム] タブで、[新しいボリュームの作成] をクリックします。
2. [新しいボリュームの作成] ページで、ボリュームの種類を選択します。



3. [ボリューム] タブで、ボリュームの上にマウス カーソルを置き、メニュー アイコン (°) を選択して、[マウント コマンド] をクリックします。

Volumes      Replications

[Mount Volume cvogcvenfsvol01](#)

Go to your Linux machine and enter this mount command

```
mount 10.0.6.251:/cvogcvenfsvol01 <dest_dir>
```

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. セキュアシェル (SSH) を使用してインスタンス上でターミナルを開き、適切な資格情報でログインします。
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。

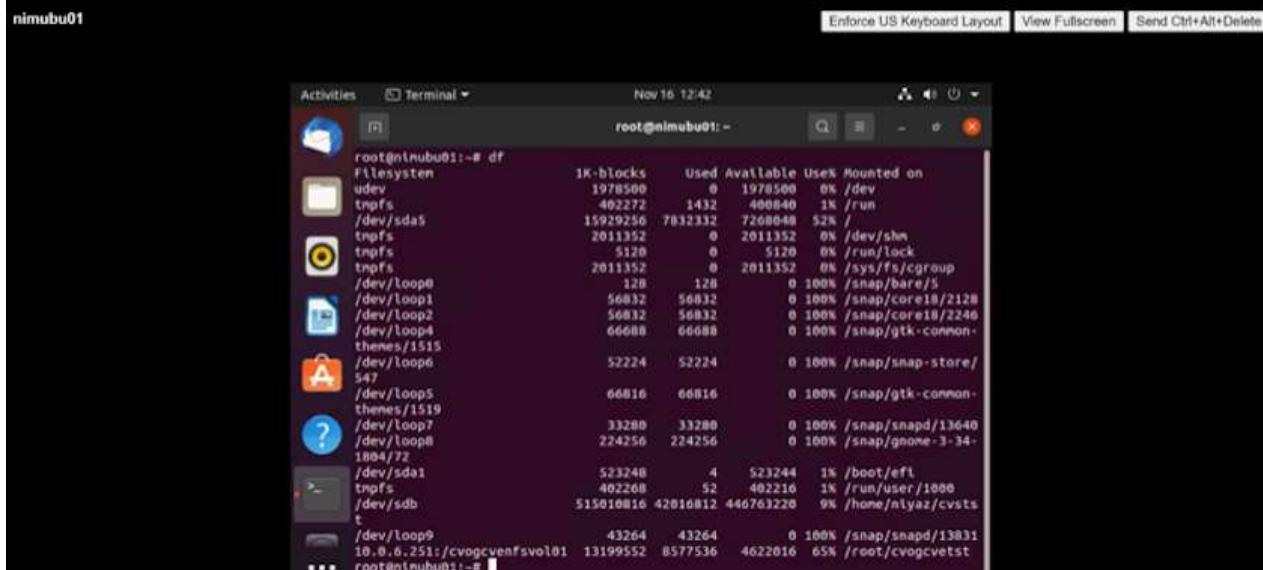
```
$ sudo mkdir /cvogcvetst
```

```
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
```



## Google Cloud NetApp Volumes(NetAppボリューム)

Google Cloud NetApp Volumes (NetApp Volumes) は、高度なクラウド ソリューションを提供するためのデータ サービスの完全なポートフォリオです。 NetApp Volumes は、主要なクラウド プロバイダーの複数のファイル アクセス プロトコル (NFS および SMB サポート) をサポートしています。

その他の利点と機能には、スナップショットによるデータ保護と復元、オンプレミスまたはクラウド内のデータの保存先を複製、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 レベルの一貫した高パフォーマンスなどがあります。

### ゲスト接続ストレージとしてのGoogle Cloud NetApp Volumes (NetApp Volumes)

## VMware Engine でNetApp Volumes を構成する

Google Cloud NetApp Volumes共有は、VMware Engine 環境で作成された VM からマウントできます。 Google Cloud NetApp Volumes はSMB および NFS プロトコルをサポートしているため、ボリュームを Linux クライアントにマウントし、Windows クライアントにマップすることもできます。 Google Cloud NetApp Volumesボリュームは簡単な手順で設定できます。

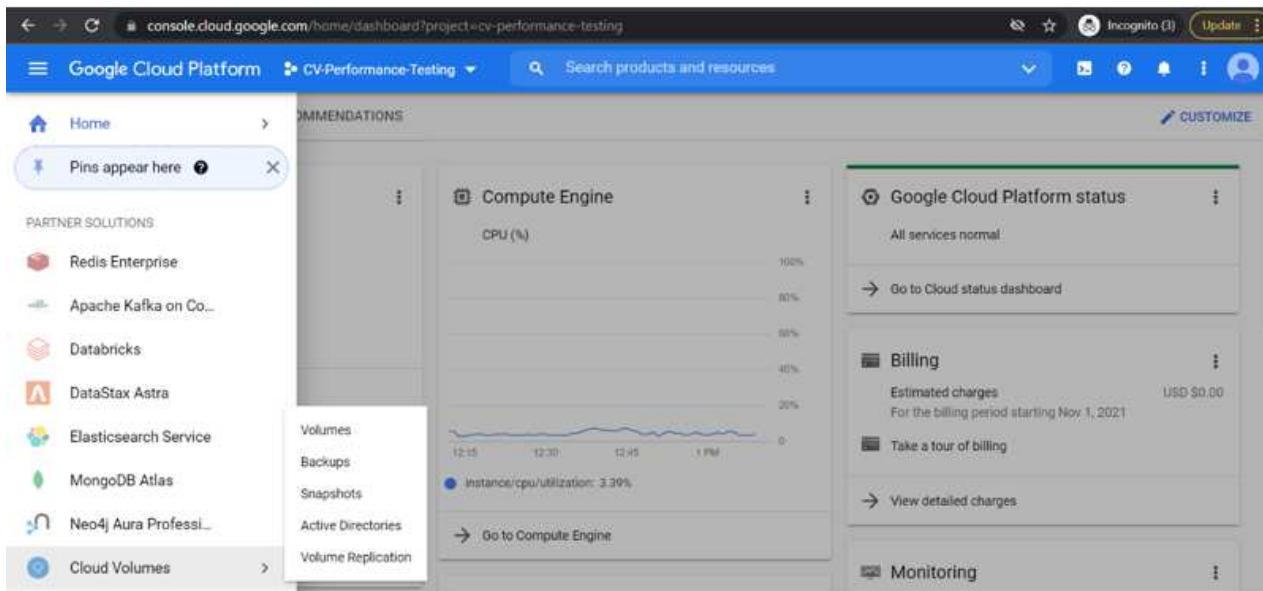
Google Cloud NetApp Volumesと Google Cloud VMware Engine プライベート クラウドは同じリージョンに存在する必要があります。

Google Cloud MarketplaceからGoogle Cloud NetApp Volumes for Google Cloudを購入、有効化、設定するには、以下の詳細な手順に従ってください。["ガイド"](#)。

## GCVEプライベートクラウドにNetApp Volumes NFSボリュームを作成する

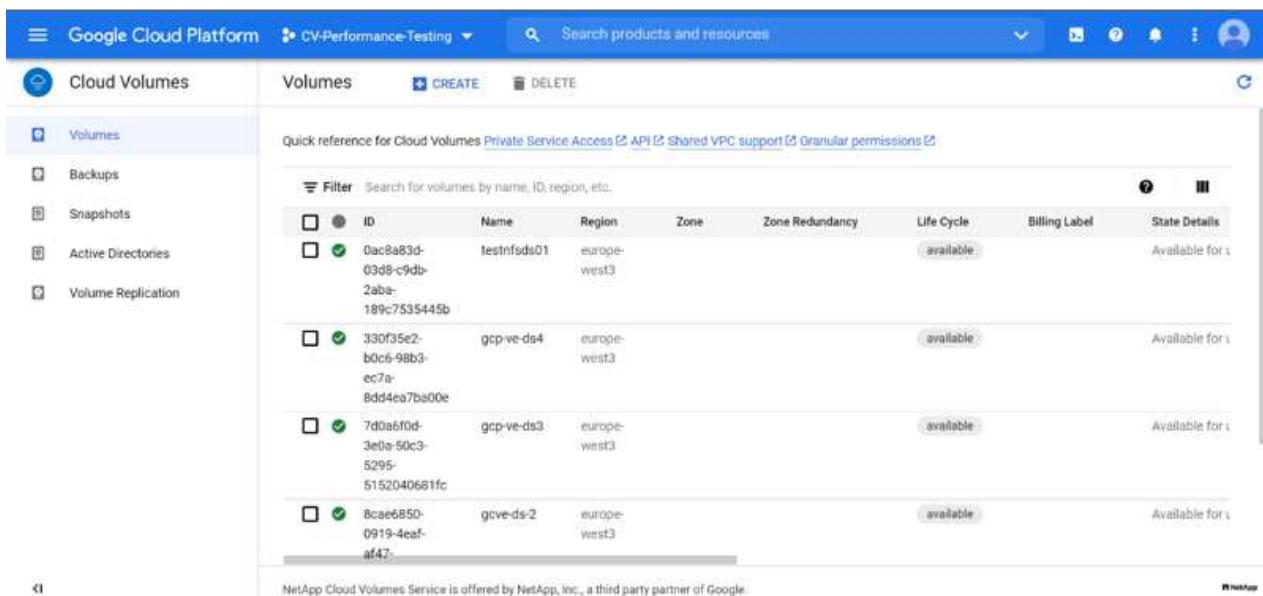
NFS ボリュームを作成してマウントするには、次の手順を実行します。

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 Volumes にアクセスします。



The screenshot shows the Google Cloud Platform dashboard for the project 'CV-Performance-Testing'. The left sidebar is expanded, showing various partner solutions like Redis Enterprise, Apache Kafka, Databricks, DataStax Astra, Elasticsearch Service, MongoDB Atlas, Neo4j Aura, and Cloud Volumes. The 'Cloud Volumes' option is highlighted. The main content area displays a 'Compute Engine' dashboard with a CPU utilization chart and a link to 'Go to Compute Engine'. To the right, there are sections for 'Google Cloud Platform status' (All services normal) and 'Billing' (Estimated charges USD \$0.00), with links to 'View detailed charges'.

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



The screenshot shows the 'Volumes' page within the Cloud Volumes section of the Google Cloud Platform interface. The left sidebar has options for 'Volumes', 'Backups', 'Snapshots', 'Active Directories', and 'Volume Replication', with 'Volumes' selected. The main area displays a table of existing volumes. The columns include ID, Name, Region, Zone, Zone Redundancy, Life Cycle, Billing Label, and State Details. Five volumes are listed:

| ID                                   | Name        | Region       | Zone | Zone Redundancy | Life Cycle | Billing Label | State Details   |
|--------------------------------------|-------------|--------------|------|-----------------|------------|---------------|-----------------|
| 0ac8a83d-03d8-c9db-2ab8-189c7535445b | testnfsds01 | europe-west3 |      |                 | available  |               | Available for v |
| 330f35e2-b0c6-98b3-ec7a-8dd4ea7ba00e | gcp-ve-ds4  | europe-west3 |      |                 | available  |               | Available for i |
| 7d0a6f0d-3e0a-50c3-5295-5152040681fc | gcp-ve-ds3  | europe-west3 |      |                 | available  |               | Available for i |
| bcae6850-0919-4eaf-a4f2-             | gcve-ds-2   | europe-west3 |      |                 | available  |               | Available for v |

3. 「ファイルシステムの作成」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。

|   |  |
|---|--|
|  Cloud Volumes <ul style="list-style-type: none"> <li> <a href="#">Volumes</a></li> <li> <a href="#">Backups</a></li> <li> <a href="#">Snapshots</a></li> <li> <a href="#">Active Directories</a></li> <li> <a href="#">Volume Replication</a></li> </ul> | <p style="text-align: center;"><a href="#"> Create File System</a></p> <p><b>Volume Name</b></p> <p>Name * <input type="text" value="nimCVNFSvol01"/></p> <p>A human readable name used for display purposes.</p> <p><b>Billing Labels</b></p> <p>Label your volumes for billing reports, queries.<br/>Supported with CVS-Performance service type; can be set with CVS service type but not available for billing at this time.</p> <p style="text-align: center;"><a href="#">+ ADD LABEL</a></p> |
|---|--|

- 適切なサービスを選択してください。 GCVE の場合、アプリケーションのワークロード要件に基づいて、レイテンシの改善とパフォーマンスの向上を実現するために、 NetApp Volumes-Performance と必要なサービス レベルを選択します。

|  |  |
|--|--|
|  Cloud Volumes <ul style="list-style-type: none"> <li> <a href="#">Volumes</a></li> <li> <a href="#">Backups</a></li> <li> <a href="#">Snapshots</a></li> <li> <a href="#">Active Directories</a></li> <li> <a href="#">Volume Replication</a></li> </ul> | <p style="text-align: center;"><a href="#"> Create File System</a></p> <p><b>Service Type</b></p> <p>Cloud Volumes Service is offered as two service types: CVS and CVS-Performance. Select the service type that matches your workload needs. <a href="#">Region availability</a> varies by service type. <a href="#">Learn more</a></p> <p><input type="radio"/> CVS<br/>Offers volumes created with zonal high availability.</p> <p><input checked="" type="radio"/> CVS-Performance<br/>Offers 3 performance levels and improved latency to address higher performance application requirements.</p> <p><b>Volume Replication</b></p> <p><input type="checkbox"/> Secondary<br/>Select to create volume as a destination target for volume replication. Applicable only to CVS-performance volumes.</p> |
|--|--|

- ボリュームとボリューム パスの Google Cloud リージョンを指定します (ボリューム パスは、プロジェクト内のすべてのクラウド ボリュームで一意である必要があります)

**Cloud Volumes**

**Create File System**

**Region**  
Region availability varies by service type.

**Region \*** europe-west3

Volume will be provisioned in the region you select.

**Volume Path \*** nimCVSNFS01

Must be unique to the project.

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**

**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.

7. ボリュームのサイズとプロトコルの種類を指定します。このテストでは、NFSv3 が使用されます。

**Cloud Volumes**

**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 \*** NFSv3

**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 LDAP**  
Enables user look up from AD LDAP server for your NFS volumes

8. このステップでは、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 ピアリングが確立されていることを確認します。

ヒント: VPC ピアリングが実行されていない場合は、ピアリング コマンドを案内する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、VPC を Google Cloud NetApp Volumes プロデューサーとピアリングします。事前に VPC ピアリングを準備する場合は、こちらの手順を参照してください。

**Create File System**

**Network Details**

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

VPC Network Name \*

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

Use Custom Address Range  
Reserved Address range

- 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。

注意: エクスポート ポリシーが追加されない限り、NFS ボリュームにアクセスすることはできません。

**Create File System**

**Export Policy**

**Rules**

Item 1

Allowed Clients 1 \*

Access

Read & Write  
 Read Only

Root Access

On  
 Off

Protocol Type (Select at least 1 of the below options)

Must select for Protocol type NFSv3. Optional for Protocol Type Both. Do not select for NFSv4.1

Allows Matching Clients for NFSv3

- 「保存」をクリックしてボリュームを作成します。

|                          | 4b8ed9d9-<br>bc6d-f3d5-<br>5a0f-<br>7da26aed3ed0 | nimnfsdemods02 | europe-<br>west3 | Available for use | CVS-<br>Performance | Primary | Extreme | NFSv3 : 10.53.0.4/nimnfsdemods02 |
|--------------------------|--|----------------|------------------|-------------------|---------------------|---------|---------|----------------------------------|
| <input type="checkbox"/> |  |                |                  |                   |                     |         |         |                                  |

## VMware Engine 上で実行されている VM への NFS エクスポートのマウント

NFS ボリュームをマウントする準備をする前に、プライベート接続のピアリング ステータスがアクティブとしてリストされていることを確認してください。ステータスがアクティブになったら、マウント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. Cloud Console で、[Cloud Volumes] > [ボリューム] に移動します。
2. ボリュームページへ
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」の下の「マウント手順」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、次の手順に従います。

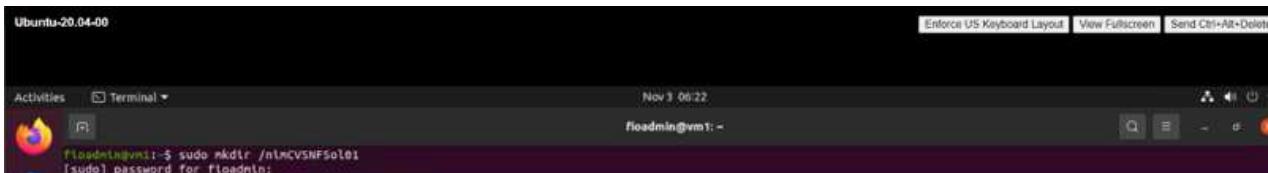
1. SSH クライアントを使用して仮想マシンに SSH 接続します。
2. インスタンスに NFS クライアントをインストールします。
  - a. Red Hat Enterprise Linux または SuSE Linux インスタンスの場合:

```
sudo yum install -y nfs-utils  
.. Ubuntu または Debian インスタンスの場合:
```

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

3. インスタンスに「/nimCVSNFS01」などの新しいディレクトリを作成します。

```
sudo mkdir /nimCVSNFS01
```



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。ラボからのコマンドの例は次のとおりです。

```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp  
10.53.0.4:/nimCVSNFS01 /nimCVSNFS01
```

```
root@vm1:~# sudo mkdir nimCVSNFS01  
root@vm1:~# sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp 10.53.0.4:/nimCVSNFS01 /nimCVSNFS01
```

```
root@vm1:~# df
Filesystem      1K-blocks   Used   Available Use% Mounted on
udev             16409952     0    16409952  0% /dev
tmpfs            3288328   1580    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/napperv/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:/nimCVSNFSol01 107374182400    256 107374182144  1% /nimCVSNFSol01
root@vm1:~#
```

## VMware Engine 上で実行されている VM への SMB 共有の作成とマウント

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

The screenshot shows the 'Active Directory connections' page with a table of existing connections. One connection is listed:

| Username      | Domain         | DNS Servers  | NetBIOS Prefix | OU Path      | AD Server Name | KDC IP | Region       | Status |
|---------------|----------------|--------------|----------------|--------------|----------------|--------|--------------|--------|
| administrator | nimgcveval.com | 192.168.0.16 | nimsmb         | CN=Computers |                |        | europe-west3 | In Use |

AD 接続が確立されたら、必要なサービス レベルでボリュームを作成します。適切なプロトコルを選択することを除いて、手順は NFS ボリュームを作成する場合と同様です。

1. Cloud Volumes コンソールで、「ボリューム」ページに移動し、「作成」をクリックします。
2. 「ファイルシステムの作成」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てください。GCVE の場合、NetApp Volumes-Performance と、ワークコード要件に基づいてレイテンシの改善とパフォーマンスの向上を図る必要なサービス レベルを選択します。

## 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. ボリュームとボリューム パスの Google Cloud リージョンを指定します (ボリューム パスは、プロジェクト内のすべてのクラウド ボリュームで一意である必要があります)

## Create File System

### Region

Region availability varies by service type.

Region \*   

Volume will be provisioned in the region you select.

Volume Path \*  

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.

- ボリュームのサイズとプロトコルの種類を指定します。このテストでは、SMB が使用されます。

## 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

- このステップでは、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 ピアリングが確立されていることを確認します。

ヒント: VPC ピアリングが実行されていない場合は、ピアリング コマンドを案内する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、VPC を Google Cloud NetApp Volumes プロデューサーとピアリングします。事前にVPCピアリングを準備

する場合は、以下を参照してください。["確認方法"](#)。

## 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。

|                          | 6a4552ed-7378-7302-be28-21a169374f28 | nimCVSMBvol01 | europe-west3 | Available for use | CVS-Performance | Primary | Standard | SMB : \\\nimsmb-3830.nimgcveval.com\vimCVSMBvol01 |
|--------------------------|--------------------------------------|---------------|--------------|-------------------|-----------------|---------|----------|---|
| <input type="checkbox"/> |                                      |               |              |                   |                 |         |          |   |

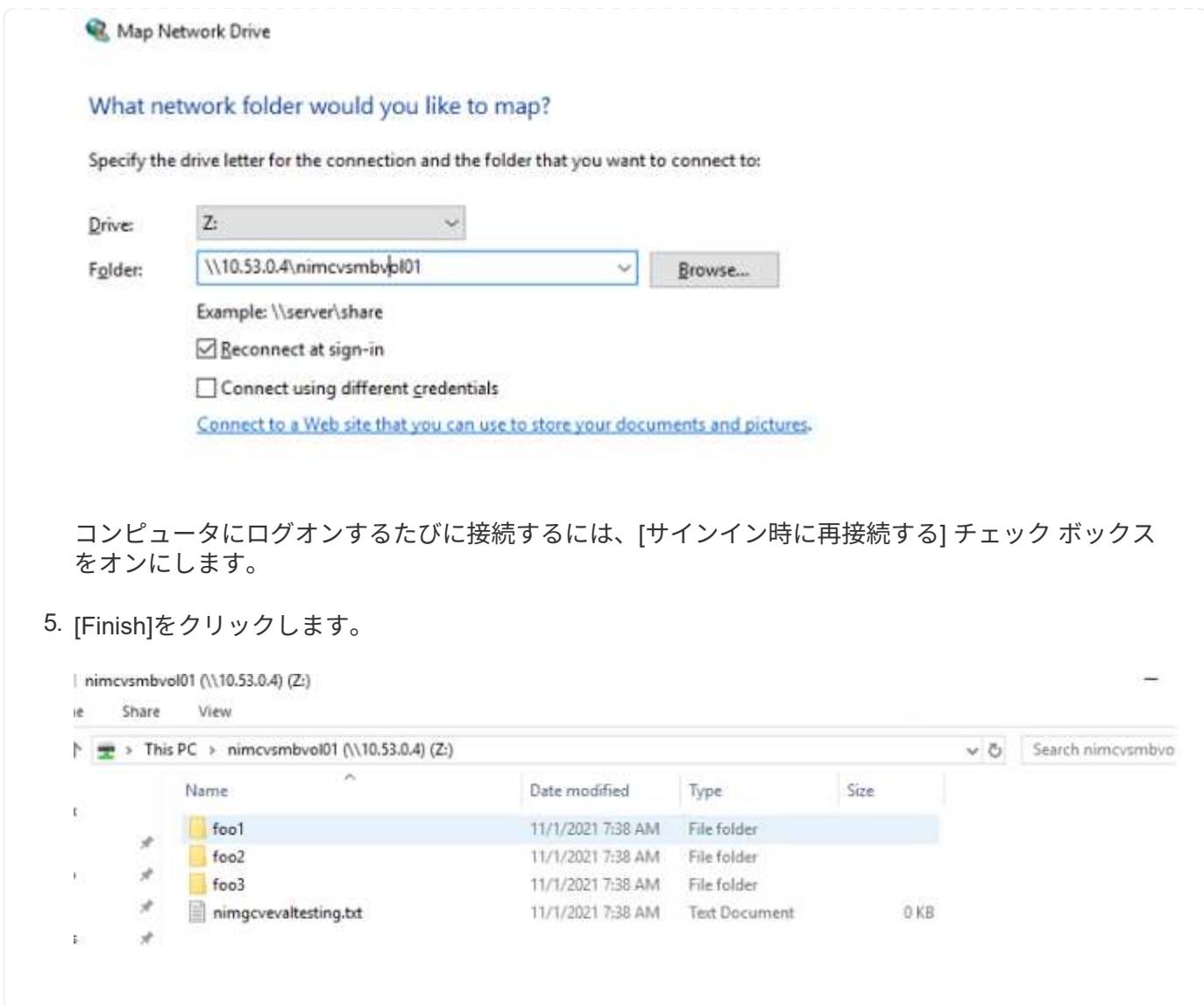
SMB ボリュームをマウントするには、次の手順を実行します。

1. Cloud Console で、[Cloud Volumes] > [ボリューム] に移動します。
2. ボリュームページへ
3. SMB 共有をマップする 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」の下の「マウント手順」をクリックします。

VMware VM の Windows ゲスト OS 内からマウント プロセスを実行するには、次の手順に従います。

1. [スタート] ボタンをクリックし、[コンピューター] 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、使用可能なドライブ文字をクリックします。
4. フォルダー ボックスに次のように入力します。

\\\nimsmb-3830.nimgcveval.com\vimCVSMBvol01



## 要約と結論: VMware と NetApp のハイブリッド マルチクラウドを組み合わせる理由

NetApp Cloud Volumes と大手ハイパースケーラー向けの VMware ソリューションを組み合わせることで、ハイブリッド クラウドを活用したい組織に大きな可能性がもたらされます。このセクションの残りの部分では、NetApp Cloud Volumes を統合することで真のハイブリッド マルチクラウド機能を実現できることを示すユースケースを紹介します。

### ユースケース1: ストレージの最適化

RVtools 出力を使用してサイズ設定を実行する場合、処理能力 (vCPU/vMem) のスケールがストレージと並行していることが常に明らかになります。多くの場合、組織は、ストレージ スペースが、処理能力に必要な量をはるかに超えるクラスターのサイズを要求する状況に陥ります。

NetApp Cloud Volumes を統合することで、組織はプラットフォームの再設定、IP の変更、アーキテクチャの変更を必要とせず、シンプルな移行アプローチで vSphere ベースのクラウド ソリューションを実現できま

す。さらに、この最適化により、vSphere で必要なホスト数を最小限に抑えながら、ストレージ フットプリントを拡張できますが、ストレージ階層、セキュリティ、または使用可能なファイルには変更が加えられません。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実稼働レベルのパフォーマンスまで、ストレージを数秒で拡張することもできます。

## ユースケース2: クラウド移行

組織は、近づいているリースの期限、資本支出 (capex) から運用支出 (opex) に移行するという財務上の指示、すべてをクラウドに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 クラウドにアプリケーションを移行するようプレッシャーを受けています。

スピードが重要な場合、クラウドの特定の IaaS プラットフォームに適応するためにアプリケーションを再プラットフォーム化およびリファクタリングするのは時間がかかり、コストも高く、数か月かかることもありますため、合理化された移行アプローチのみが実現可能です。NetApp Cloud Volumes と、ゲスト接続ストレージ用の帯域幅効率の高いSnapMirrorレプリケーション (アプリケーション整合性のあるスナップショット コピーと HCX を組み合わせた RDM、クラウド固有の移行 (Azure Migrate など)、または VM をレプリケートするためのサードパーティ製品を含む) を組み合わせることで、この移行は、時間のかかる I/O フィルター メカニズムに依存するよりもさらに簡単になります。

## ユースケース3: データセンターの拡張

季節的な需要の急増や、単に安定した有機的成长によりデータセンターの容量が限界に達した場合、クラウドでホストされる VMware と NetApp Cloud Volumes に移行するのが簡単な解決策です。NetApp Cloud Volumes を活用すると、可用性ゾーン全体にわたる高可用性と動的なスケーリング機能が提供され、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になります。NetApp Cloud Volumes を活用すると、ストレッチ クラスタの必要性を克服し、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: クラウドへの災害復旧

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 を復元するには、クラウド独自のハイパーバイザープラットフォームに変換する必要があります。これは危機時に処理すべきタスクではありません。

オンプレミスからのSnapCenterおよび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してゲスト接続ストレージにNetApp Cloud Volumes を使用することで、クラウド固有のリカバリツール (Azure Site Recovery など) または Veeam などの同等のサードパーティツールとともに、完全に一貫性のある VMware SDDC インフラストラクチャ上で VM レプリカをリカバリできる、より優れた災害復旧アプローチを考案できます。このアプローチにより、災害復旧訓練やランサムウェアからの復旧を迅速に実行することもできます。これにより、オンデマンドでホストを追加することで、テスト時や災害発生時に完全な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モダナイゼーション

アプリケーションがパブリック クラウドに移行した後、組織は数百もの強力なクラウド サービスを活用して、アプリケーションを最新化し、拡張したいと考えるようになります。NetApp Cloud Volumes 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 を含む幅広いユース ケースでのデータ モビリティが可能になるため、モダナイゼーションのプロセスが簡単になります。

## まとめ

オールクラウドまたはハイブリッド クラウドのどちらをターゲットにしているかに関係なく、NetApp Cloud Volumes は、データ要件をアプリケーション層にシームレスにすることで TCO を削減しながら、ファイルサ

ービスとブロック プロトコルとともにアプリケーション ワークロードを導入および管理するための優れたオプションを提供します。

ユースケースに関係なく、お気に入りのクラウド/ハイパースケーラーをNetApp Cloud Volumes と組み合わせて選択することで、クラウドのメリット、オンプレミスと複数のクラウドにわたる一貫したインフラストラクチャと運用、ワークロードの双方向の移植性、エンタープライズ グレードの容量とパフォーマンスを迅速に実現できます。

これは、ストレージを接続するために使用される、使い慣れたプロセスと手順と同じです。覚えておいてください。新しい名前で変更されたのはデータの位置だけです。ツールとプロセスはすべて同じままで、NetApp Cloud Volumes は全体的な導入の最適化に役立ちます。

## 著作権に関する情報

Copyright © 2026 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隨時、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 5225.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

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

## 商標に関する情報

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