パブリッククラウドとハイブリッドクラウド

NetApp Solutions

NetApp
May 10, 2024

目次

パブリッククラウドとハイブリッドクラウド

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

パブリッククラウド向け VMware

VMwareを使用したネットアップのハイブリッドマルチクラウドの概要

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

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

パブリッククラウドの VMware Cloud オプション

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

Azure VMware 解決策の略

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

AWS 上の VMware Cloud

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

Google Cloud VMware Engine

Google Cloud VMware Engine は、 Google Cloud の高性能で拡張性の高いインフラストラクチャと VMware Cloud Foundation スタック（ VMware vSphere 、 vCenter 、 VSAN 、 NSX ）を基盤とした IaaS （ Infrastructure-as-a-Service ）ですこのサービスにより、アプリケーションの再構築やツールの再構築にかかるコスト、労力、リスクを伴わずに、クラウドへの迅速な移行を実現し、既存の VMware ワークロードをオンプレミス環境から Google Cloud Platform にシームレスに移行または拡張できます。VMware と緊密に連携して Google が販売およびサポートするサービスです。

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

ご存知ですか？

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

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

ストレージ構成

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

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

注：

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

Azure NetApp Files 、 NetApp ONTAP 向け Amazon FSX 、 Cloud Volumes ONTAP （ 3 つの主要なハイパースケーラすべてで利用可能）、および Cloud Volumes Service for Google Cloud は、ゲスト VM と組み合わせ

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

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

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

  例：

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

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

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

覚えておいてください

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

この環境ゲスト接続ストレージのみ。

ネットアップのクラウドストレージのメリット

ネットアップのクラウドストレージには次のようなメリットがあります。

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

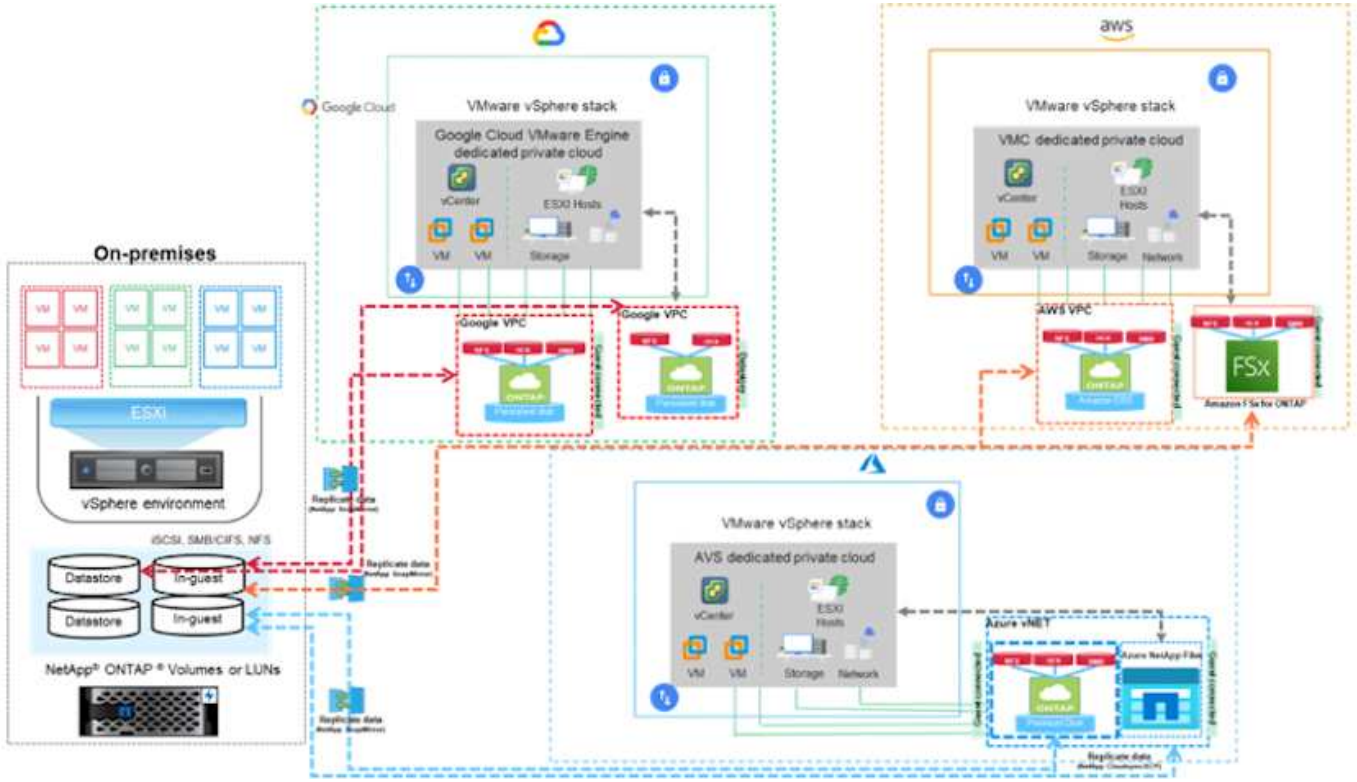
前提条件

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

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

詳細なアーキテクチャ

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



ハイパースケーラにおける **VMware** 向けネットアップソリューション

ネットアップが提供する3つの主要ハイパースケーラ（ゲスト接続ストレージデバイスまたはNFSデータストアとしてのネットアップ提供）の機能について、詳しくはこちらをご覧ください。また、ワークフローの移行、クラウドへの拡張/バースト対応、バックアップ/リストア、ディザスタリカバリも行っています。

クラウドを選択して、ネットアップに任せてください。

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

次のオプションから選択して、目的のコンテンツのセクションに移動します。

- "ハイパースケーラ構成における VMware"

- "ネットアップストレージオプション"
- "ネットアップとVMwareのクラウドソリューション"

ハイパースケーラ構成における **VMware**

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

AWS / VMC

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

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

セットアッププロセスは、次の手順に分けることができます。

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

詳細を表示します "VMCの設定手順"。

Azure / AVS

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

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

セットアッププロセスは、次の手順に分けることができます。

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

詳細を表示します "AVSの設定手順"。

GCP/GCVE

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

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

セットアッププロセスは、次の手順に分けることができます。

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

詳細を表示します "GCVEの設定手順"。

ネットアップストレージオプション

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

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

AWS / VMC

AWS は、次の構成でネットアップストレージをサポートします。

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

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

Azure / AVS

Azure は、以下の構成でネットアップストレージをサポートします。

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

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

GCP/GCVE

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

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

詳細を表示します "GCVEのゲスト接続ストレージオプション"。

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

ネットアップと**VMware**のクラウドソリューション

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

- 保護（ディザスタリカバリとバックアップ/リストアの両方を含む）

- 移動
- 拡張

AWS / VMC

"ネットアップのAWS / VMC向けソリューションをご確認ください"

Azure / AVS

"ネットアップのAzure / AVS向けソリューションをご覧ください"

GCP/GCVE

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

VMwareでサポートされるネットアップハイブリッドマルチクラウドの構成

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

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

クラウドプロバイダでの仮想化環境の設定

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

AWS / VMC

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

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

セットアッププロセスは、次の手順に分けることができます。

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

詳細を表示します "VMCの設定手順"。

Azure / AVS

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

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

セットアッププロセスは、次の手順に分けることができます。

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

詳細を表示します "AVSの設定手順"。

GCP/GCVE

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

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

セットアッププロセスは、次の手順に分けることができます。

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

詳細を表示します "GCVEの設定手順"。

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

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

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

セットアッププロセスは、次の手順に分けることができます。

VMware Cloud for AWS を導入して設定

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

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

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

セットアッププロセスは、次の 3 つの部分に分けることができます。

AWSアカウントを登録

に登録します "Amazon Web Services アカウント"。

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

My VMwareアカウントに登録します

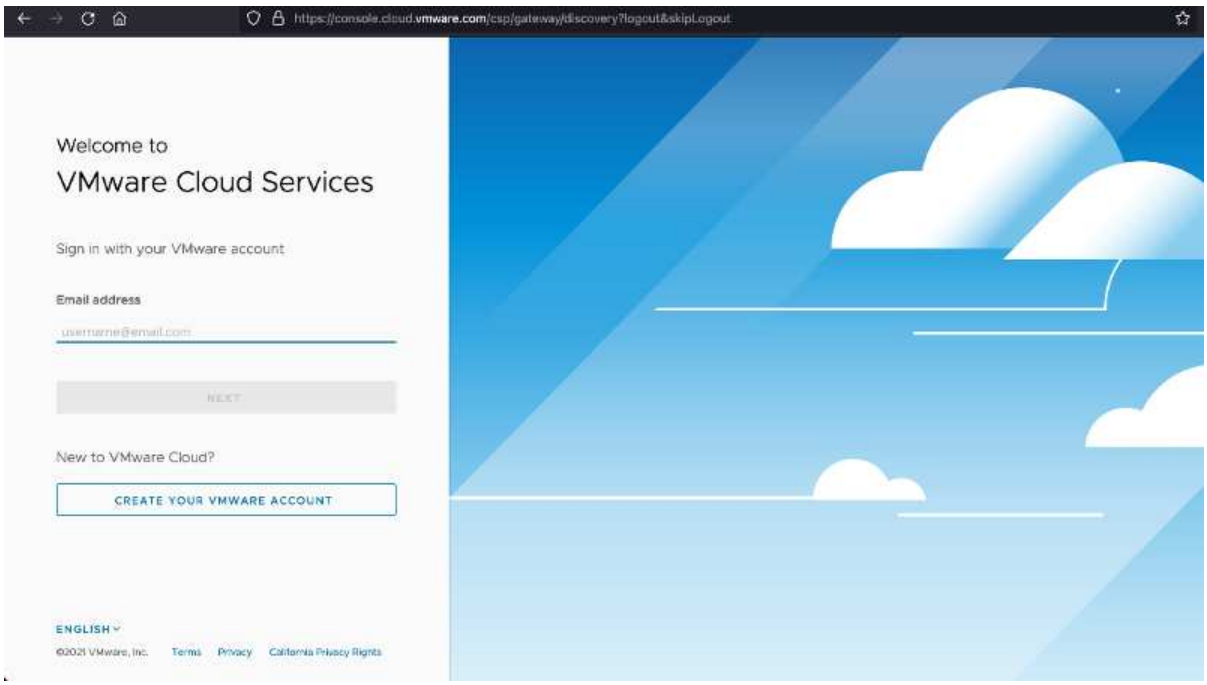
に登録します "マイ VMware" アカウント：

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

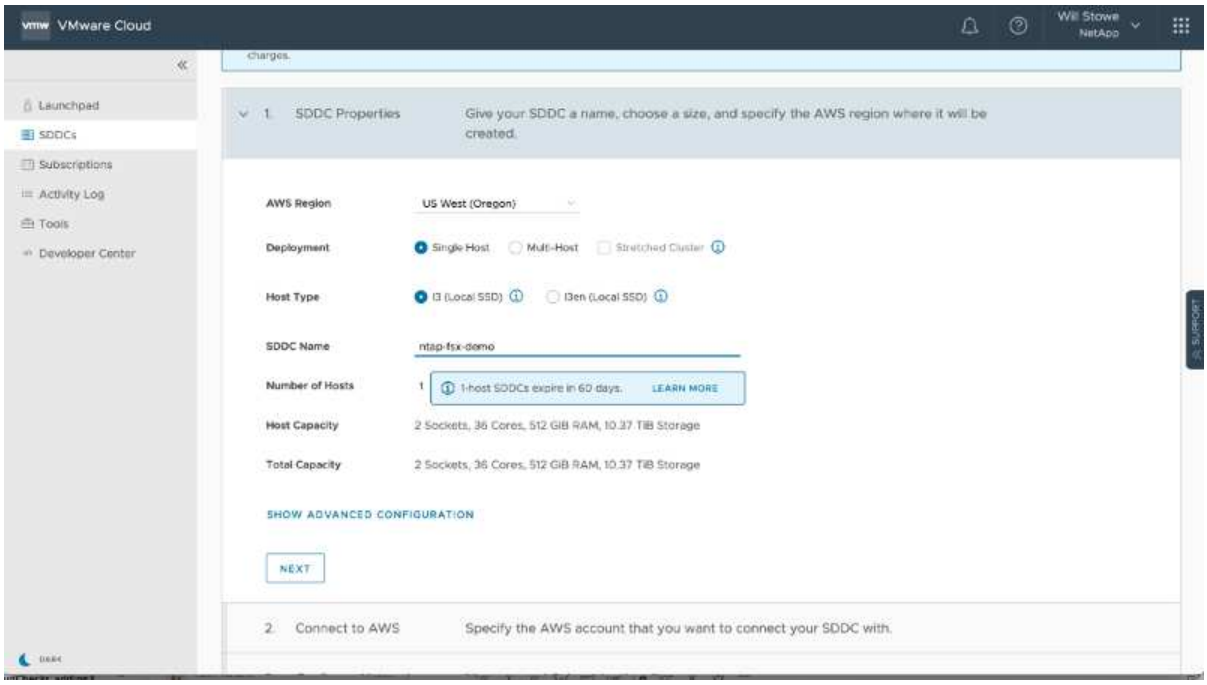
VMware Cloud で **SDDC** をプロビジョニングします

VMware アカウントを設定して適切なサイジングを実行したら、 AWS サービスで VMware Cloud を使用するための次の一歩として Software-Defined Data Center を導入します。SDDC を作成するには、そのホストとして AWS リージョンを選択し、 SDDC に名前を付け、 SDDC に含める ESXi ホストの数を指定します。AWS アカウントがない場合でも、単一の ESXi ホストを含むスターター構成の SDDC を作成できます。

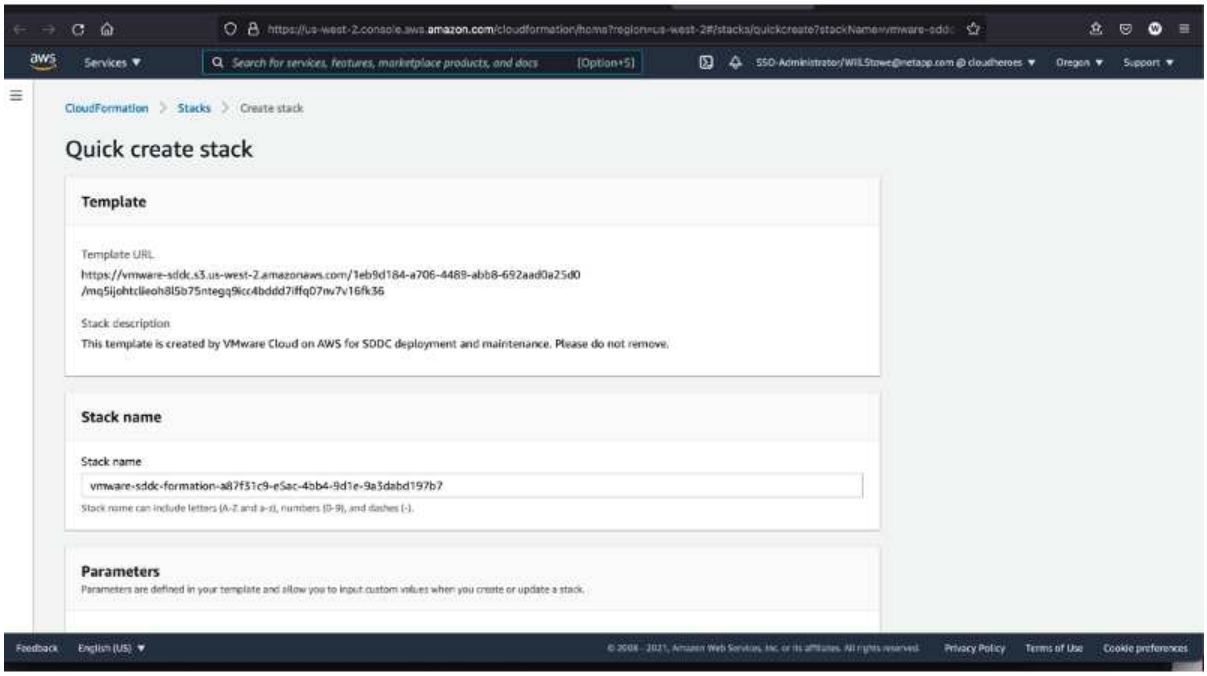
1. 既存または新規に作成した VMware クレデンシャルを使用して、 VMware Cloud Console にログインします。

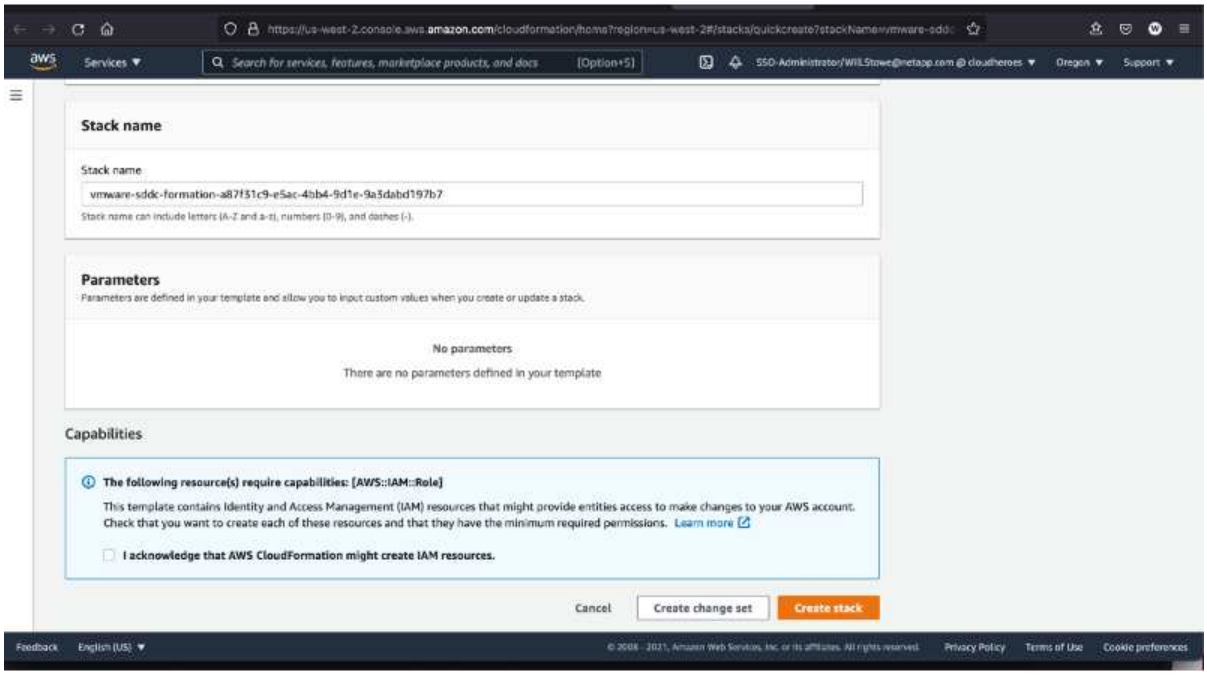


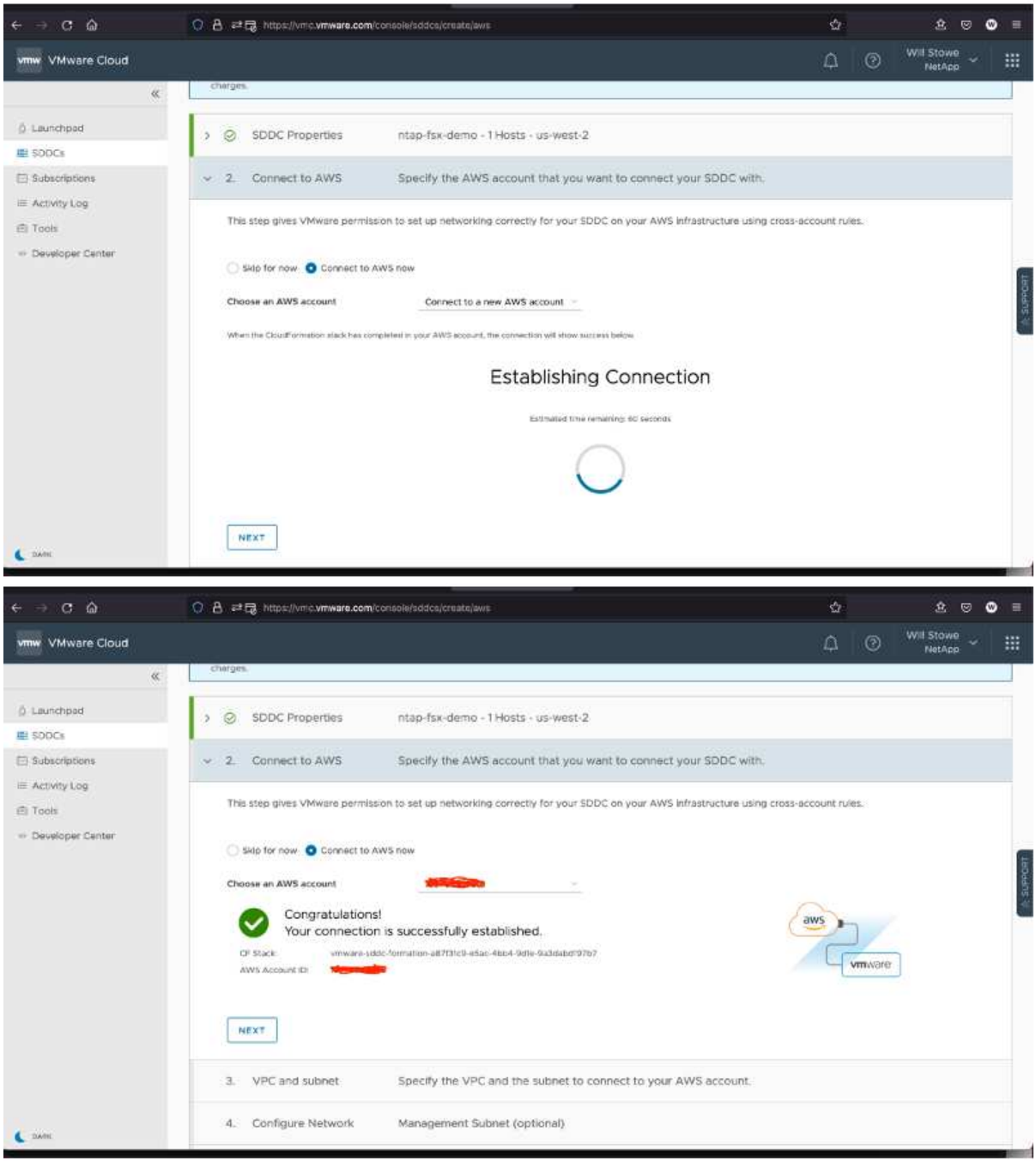
2. AWS のリージョン、導入環境、およびホストタイプと SDDC 名を設定します。



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

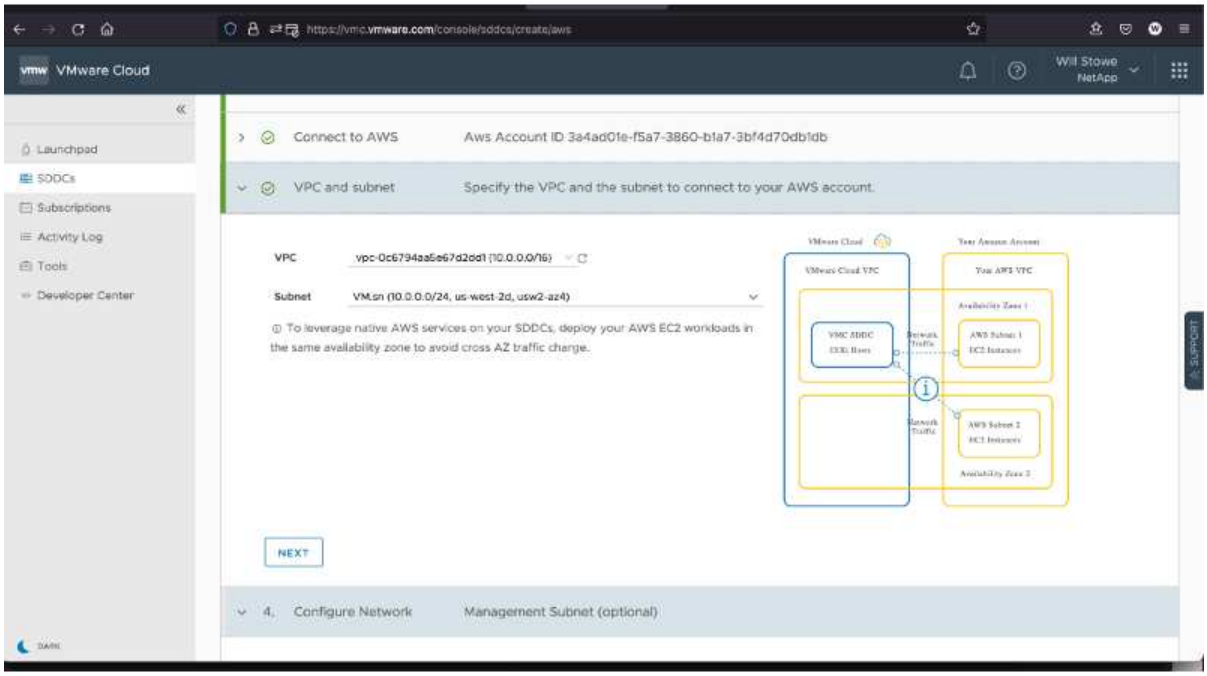




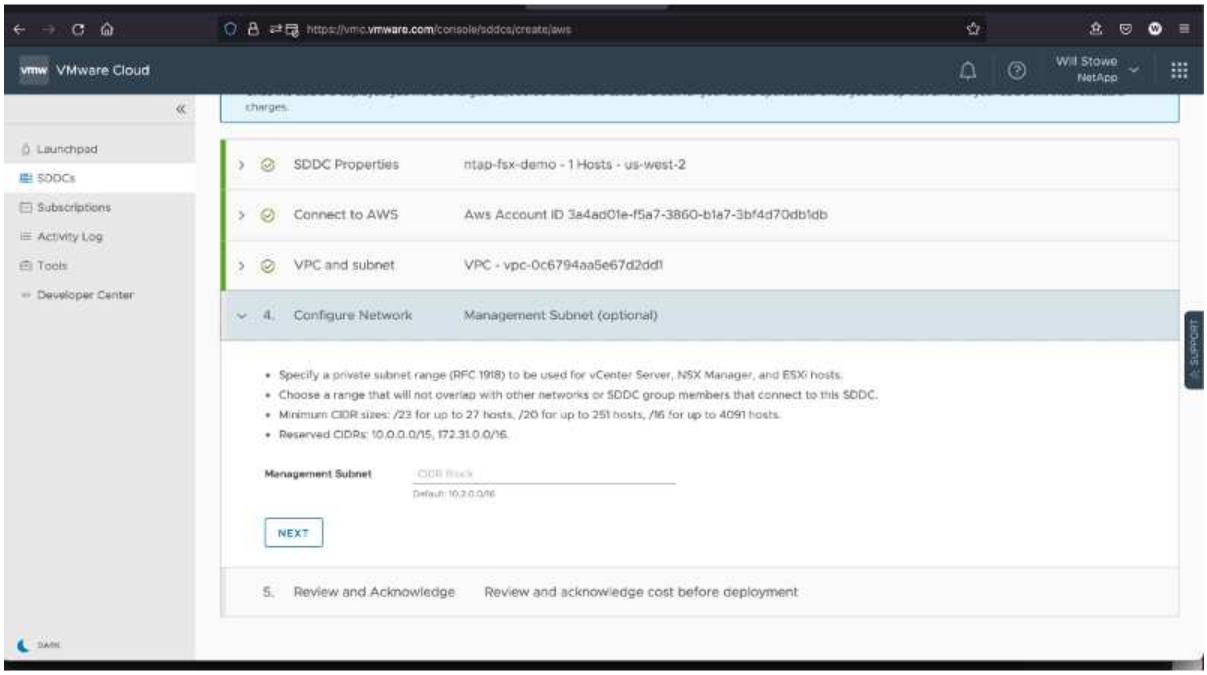


この検証ではシングルホスト構成を使用します。

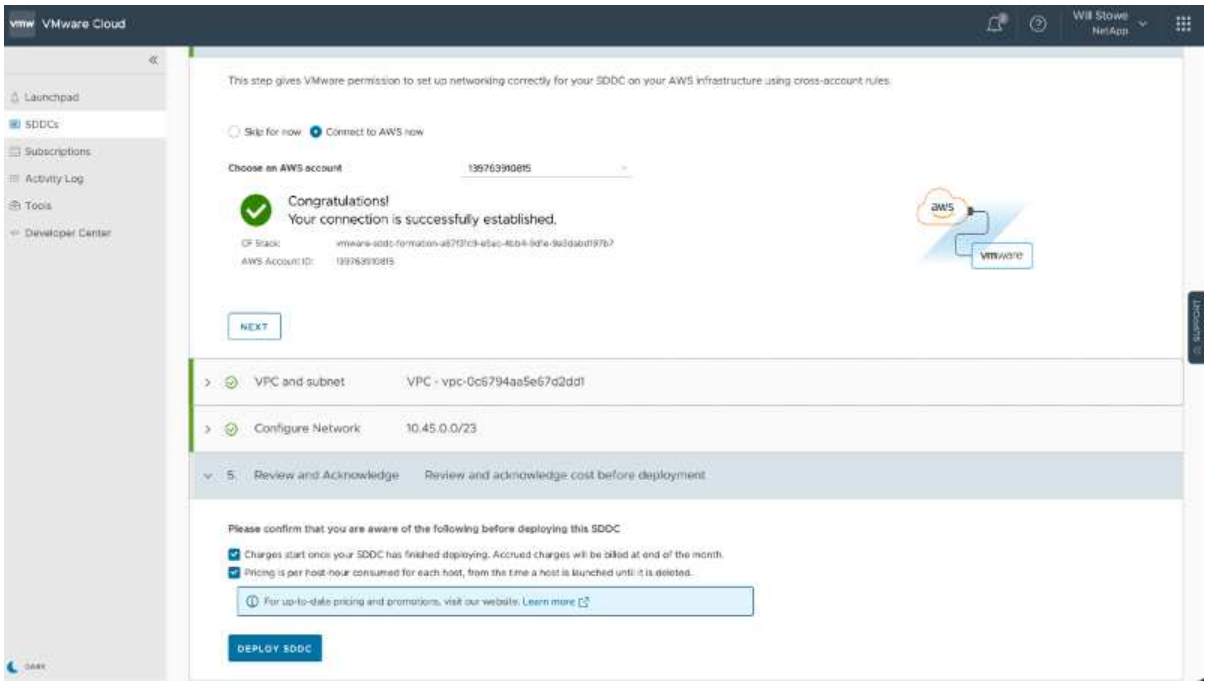
4. VMC 環境を接続する AWS VPC を選択します。



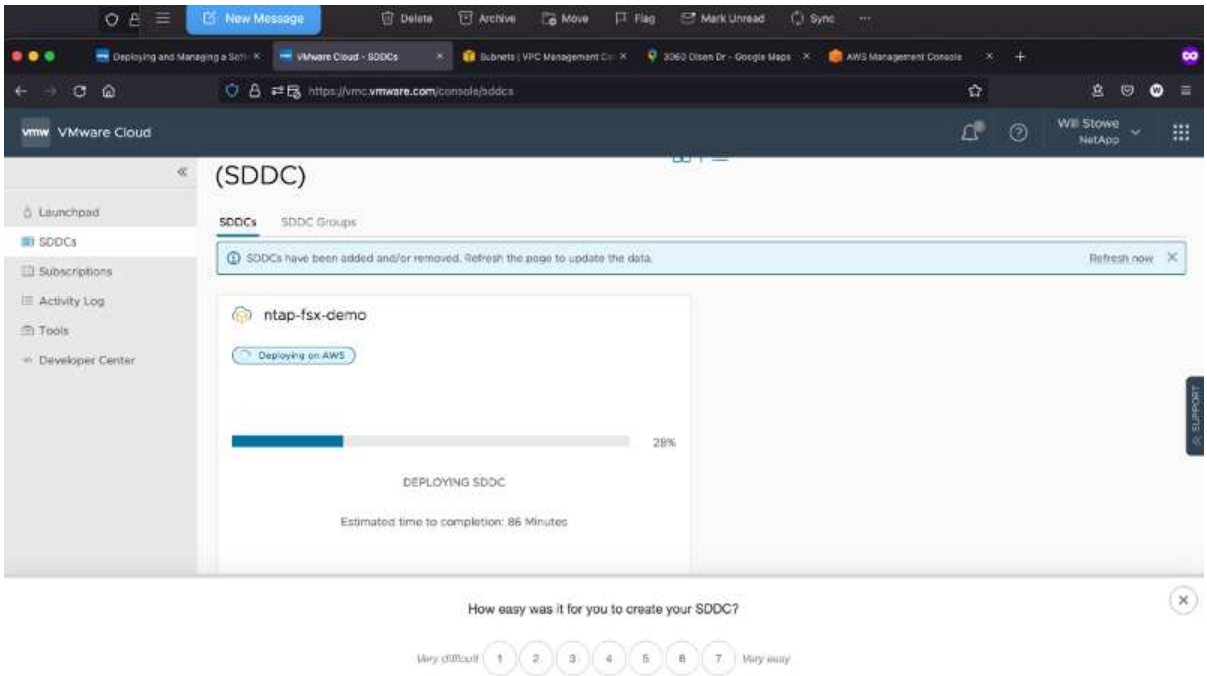
5. VMC 管理サブネットを構成します。このサブネットには、 vCenter や NSX などの VMC 管理サービスが含まれます。SDDC 環境への接続が必要な他のネットワークと重複するアドレス空間を選択しないでください。最後に、以下に示す CIDR サイズの推奨事項に従います。



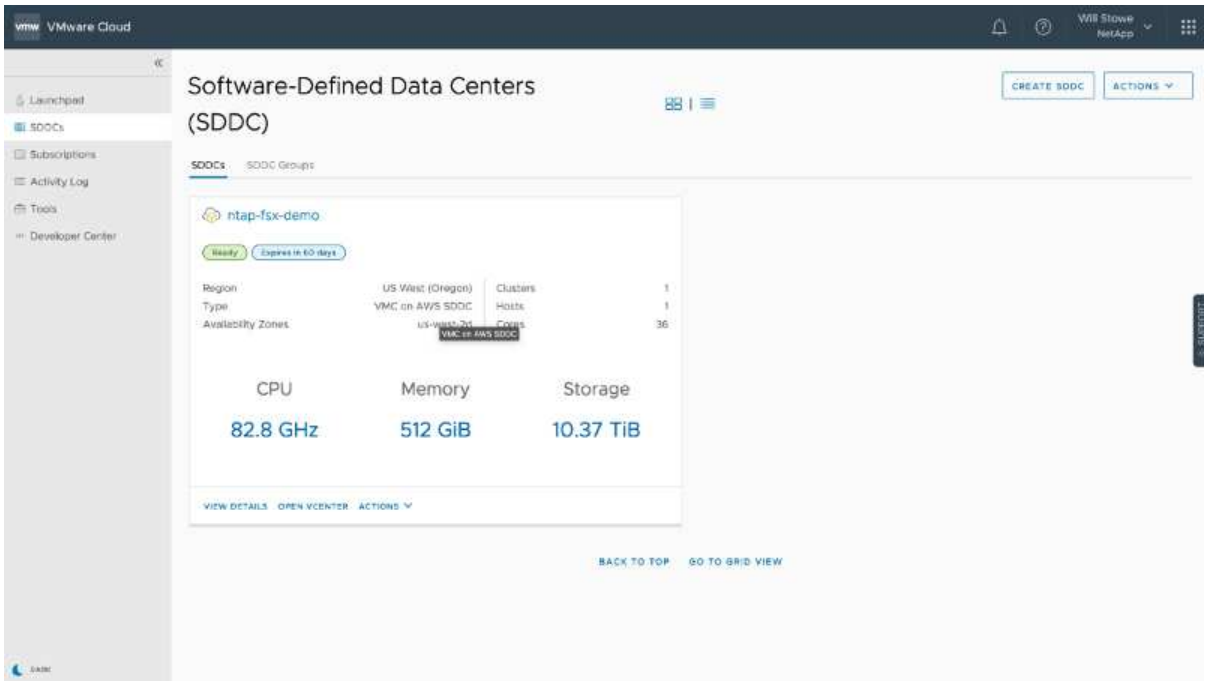
6. SDDC 構成を確認して承認し、 [Deploy the SDDC] をクリックします。



導入プロセスの完了には、通常約 2 時間かかります。



7. 完了すると、 SDDC を使用できるようになります。

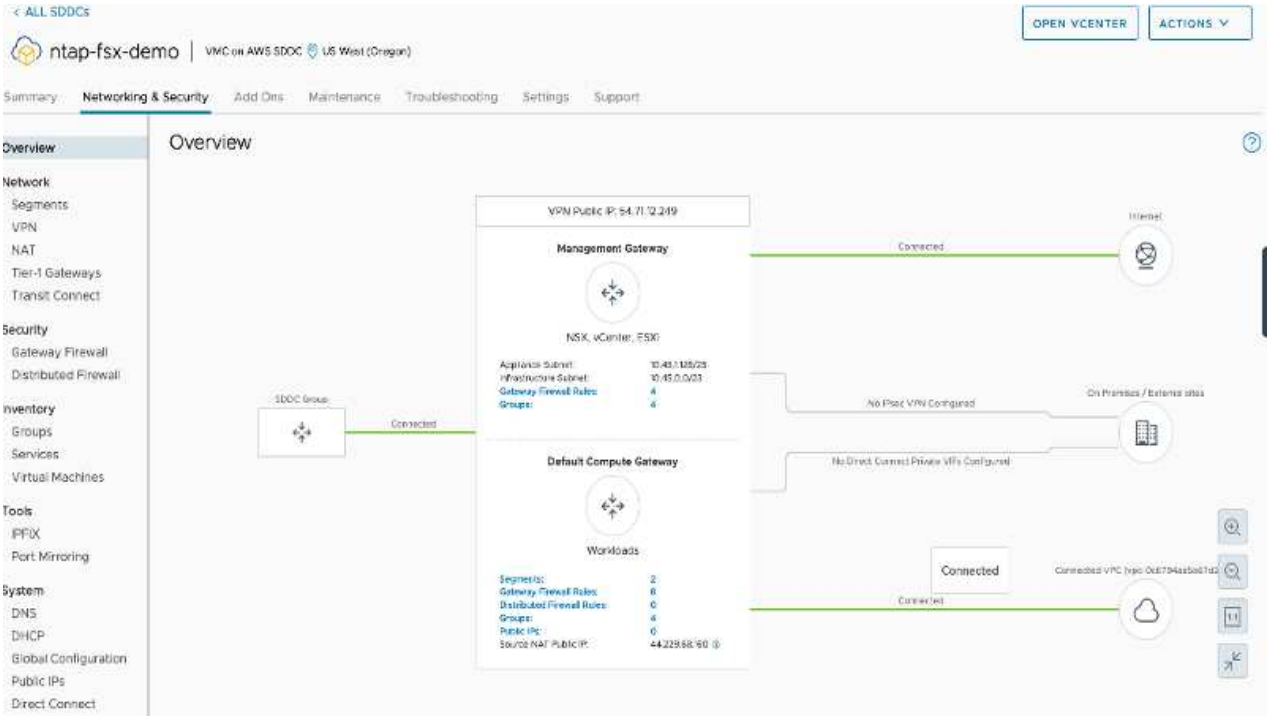


SDDC の導入の詳細な手順については、を参照してください "VMC コンソールから SDDC を展開します"。

VMware Cloud を **FSX ONTAP** に接続します

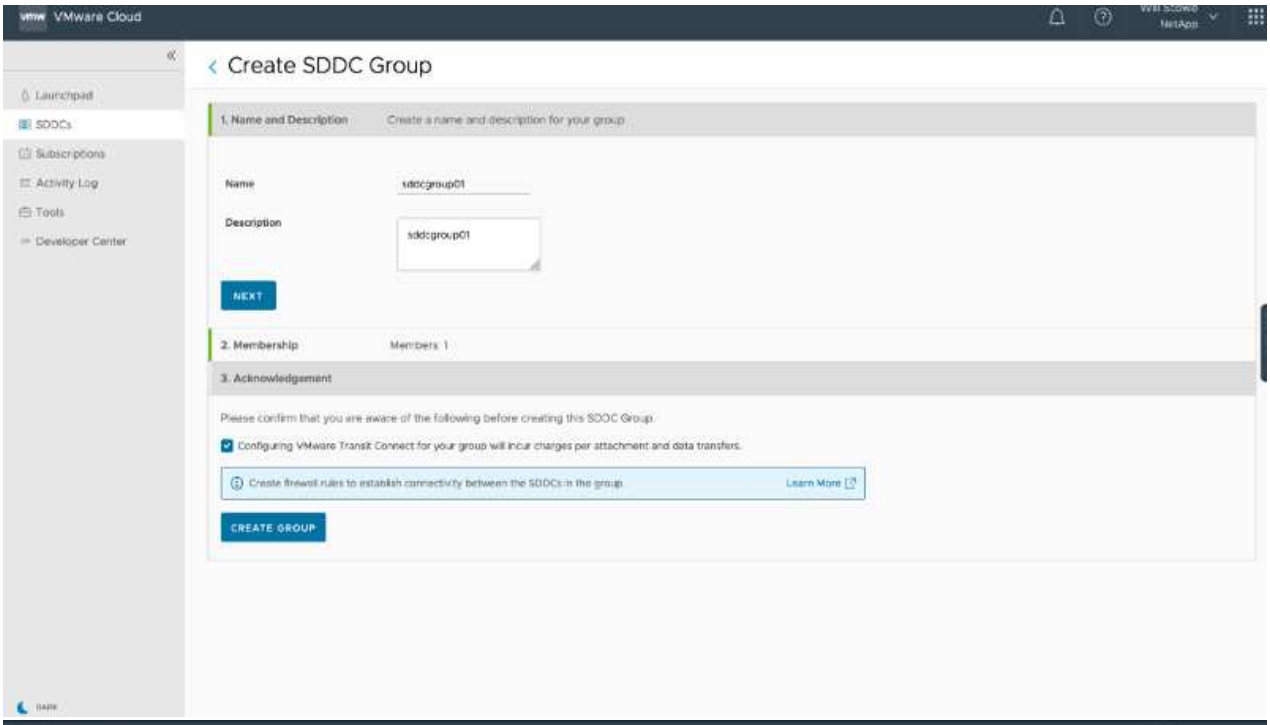
VMware Cloud を FSX ONTAP に接続するには、次の手順を実行します。

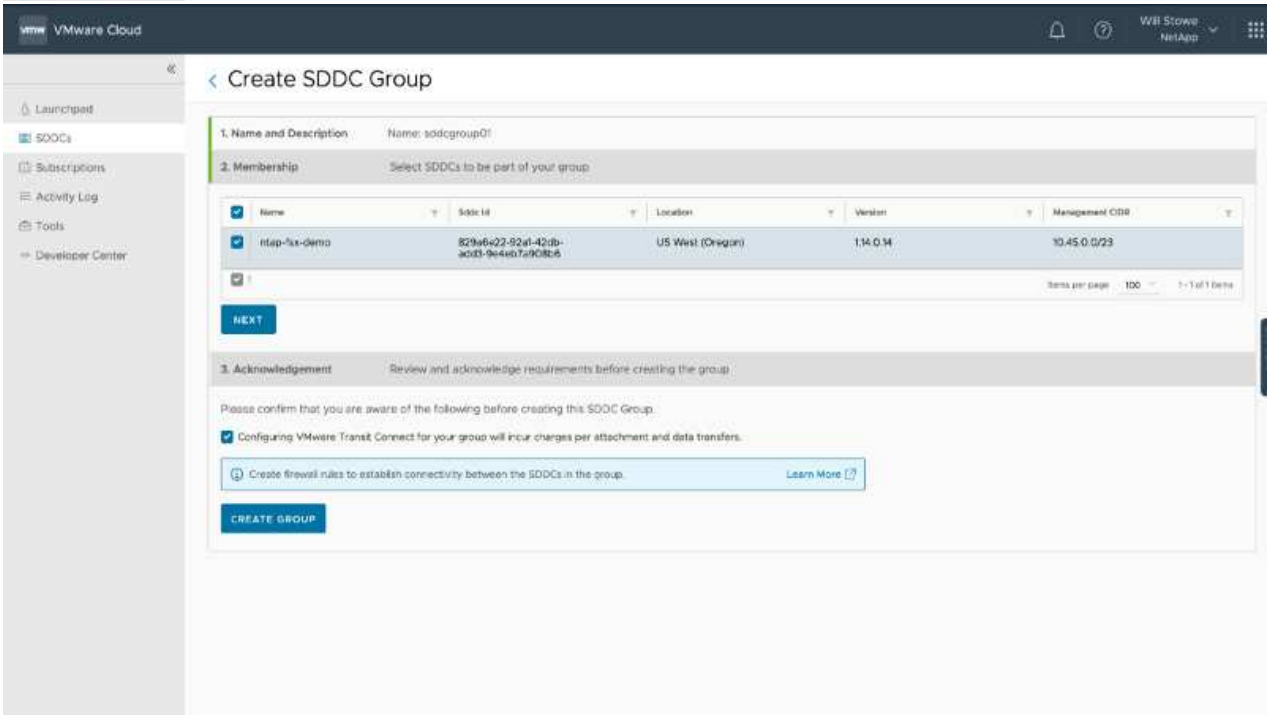
1. VMware Cloud の導入が完了して AWS VPC に接続されているため、 Amazon FSX for NetApp ONTAP を、元の接続済み VPC ではなく新しい VPC に導入する必要があります（以下のスクリーンショットを参照）。接続された VPC に FSX （ NFS および SMB のフローティング IP ）が導入されている場合、これらの IP にはアクセスできません。Cloud Volumes ONTAP のような iSCSI エンドポイントは、接続された VPC からは正常に機能します。

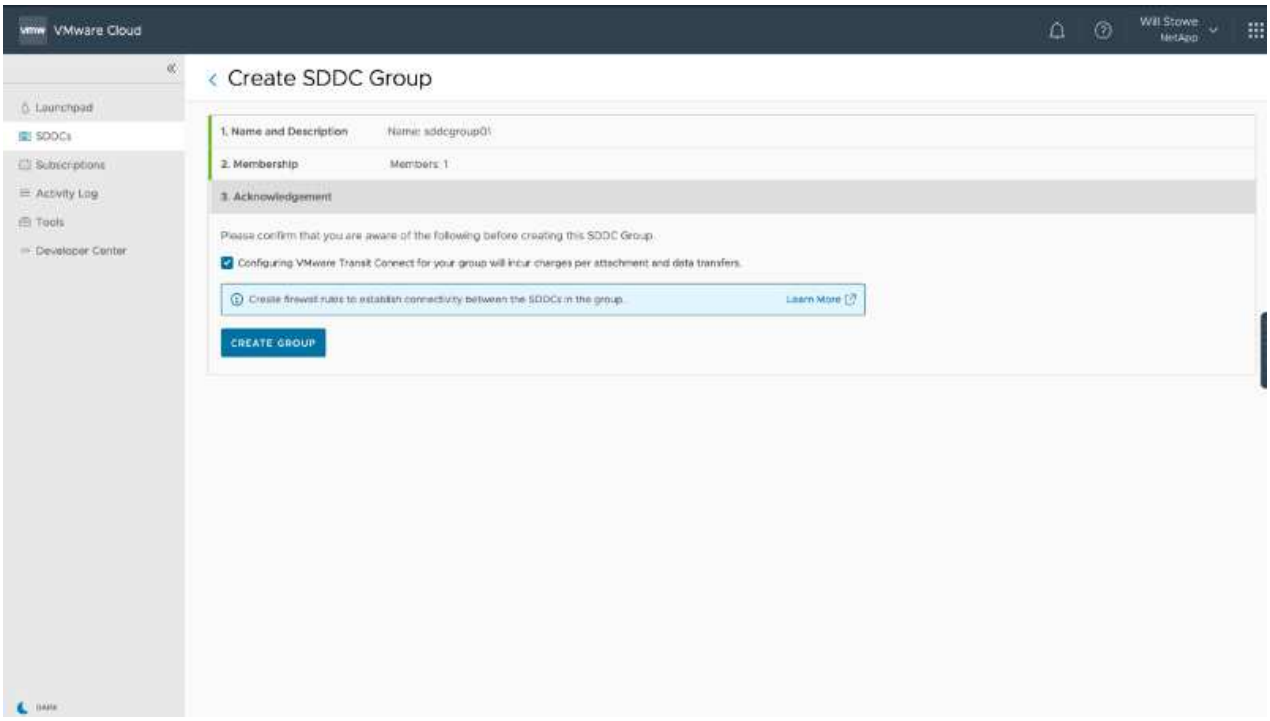


2. 同じリージョンに別の VPC を導入し、その新しい VPC に Amazon FSX for NetApp ONTAP を導入します。

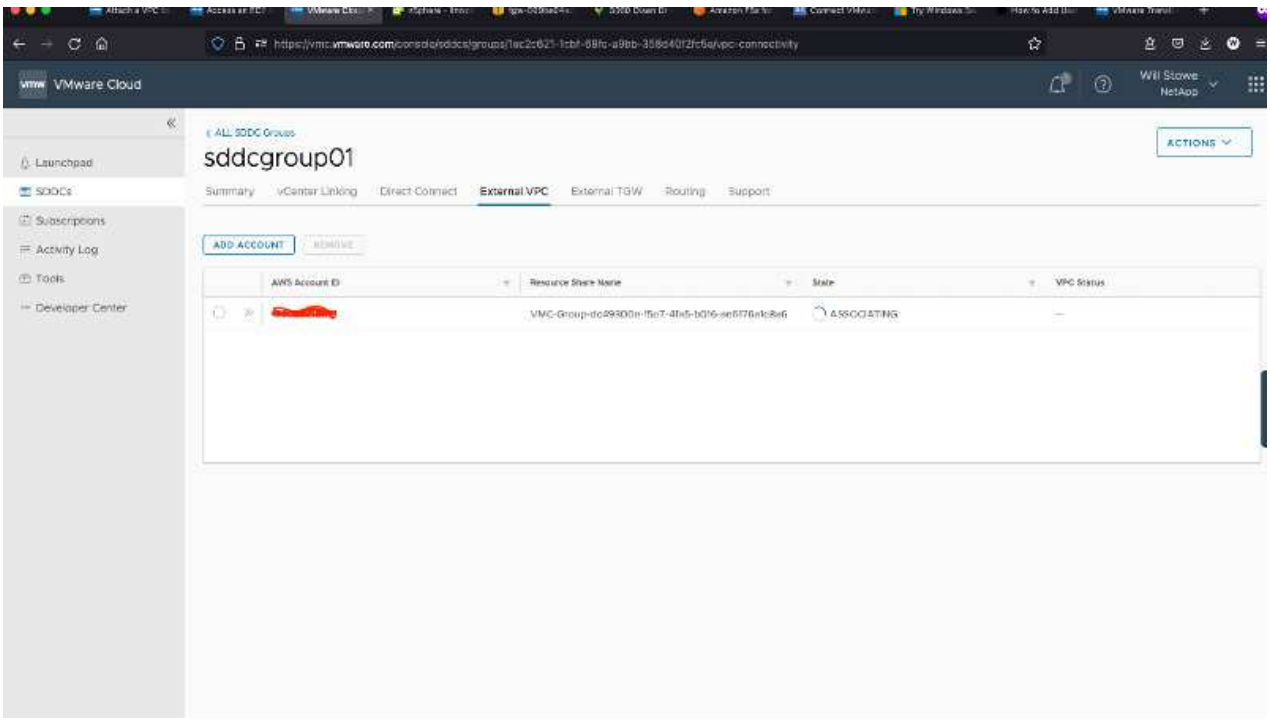
   VMware Cloud コンソールで SDDC グループを構成すると、 FSX が導入された新しい VPC に接続するために必要なネットワーク設定オプションが有効になります。手順 3 で、「グループ用の VMware トランジット接続の構成に添付ファイルおよびデータ転送ごとの料金が発生する」がチェックされていることを確認し、「グループの作成」を選択します。このプロセスが完了するまでに数分かかることがあります。

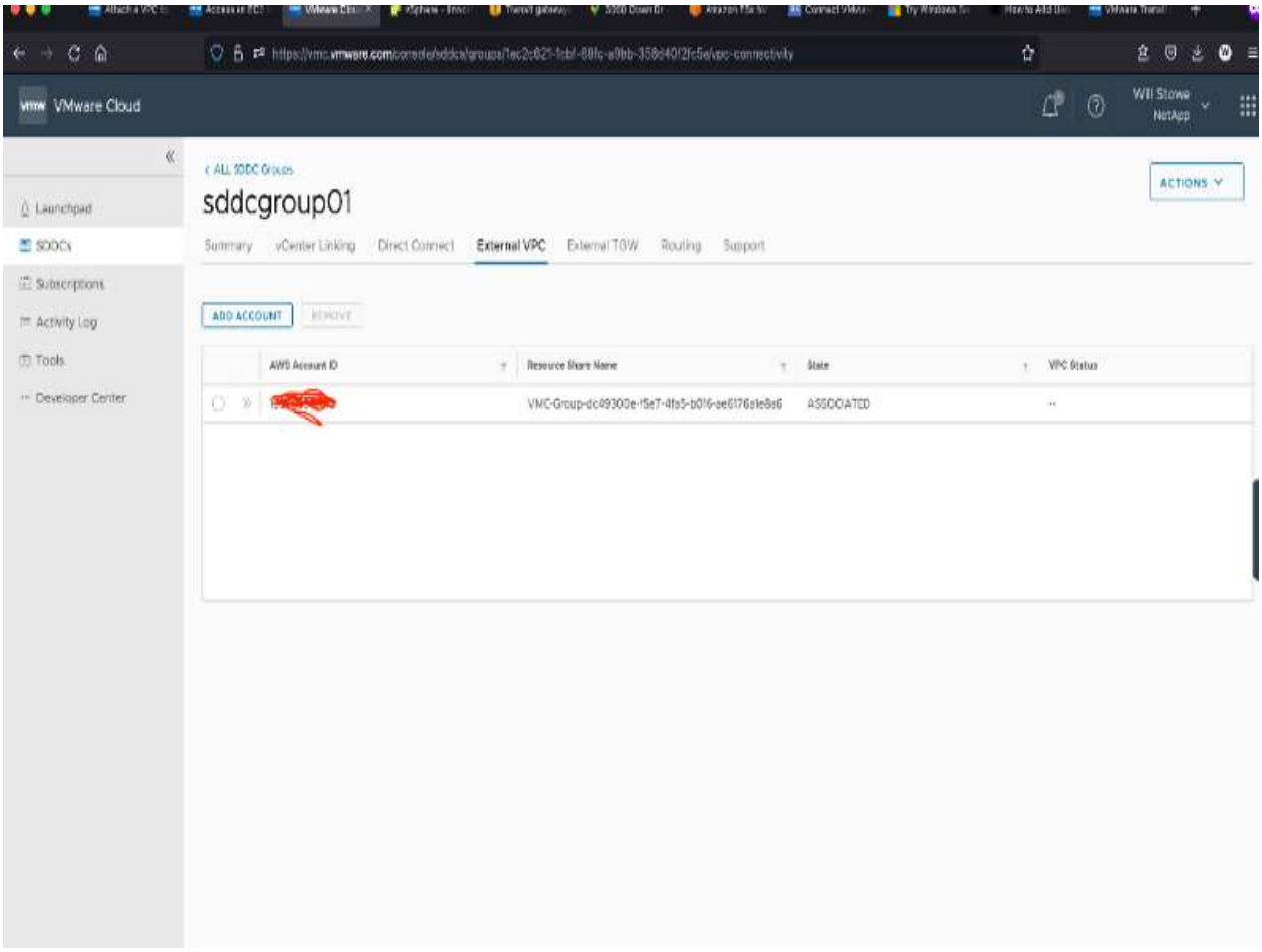

VMware Cloud
Create SDDC Group
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
1. Name and Description
Create a name and description for your group
Name
sddcgroup01
Description
sddcgroup01
NEXT
2. Membership
Members: 1
3. Acknowledgement
Please confirm that you are aware of the following 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
Will Stowe
NetApp
Create SDDC Group
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
1. Name and Description
Name: sddcgroup01
2. Membership
Select SDDCs to be part of your group
Name
Sddc Id
Location
Version
Management CIDR
ntap-fsx-demo
829a6e22-92a1-42db-acd3-9e4eb7a908b6
US West (Oregon)
1.14.0.14
10.45.0.0/23
Items per page
100
1 - 1 of 1 items
NEXT
3. Acknowledgement
Review and acknowledge requirements before creating the group
Please confirm that you are aware of the following before creating this SDDC Group.
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.
Create firewall rules to establish connectivity between the SDDCs in the group.
Learn More
CREATE GROUP

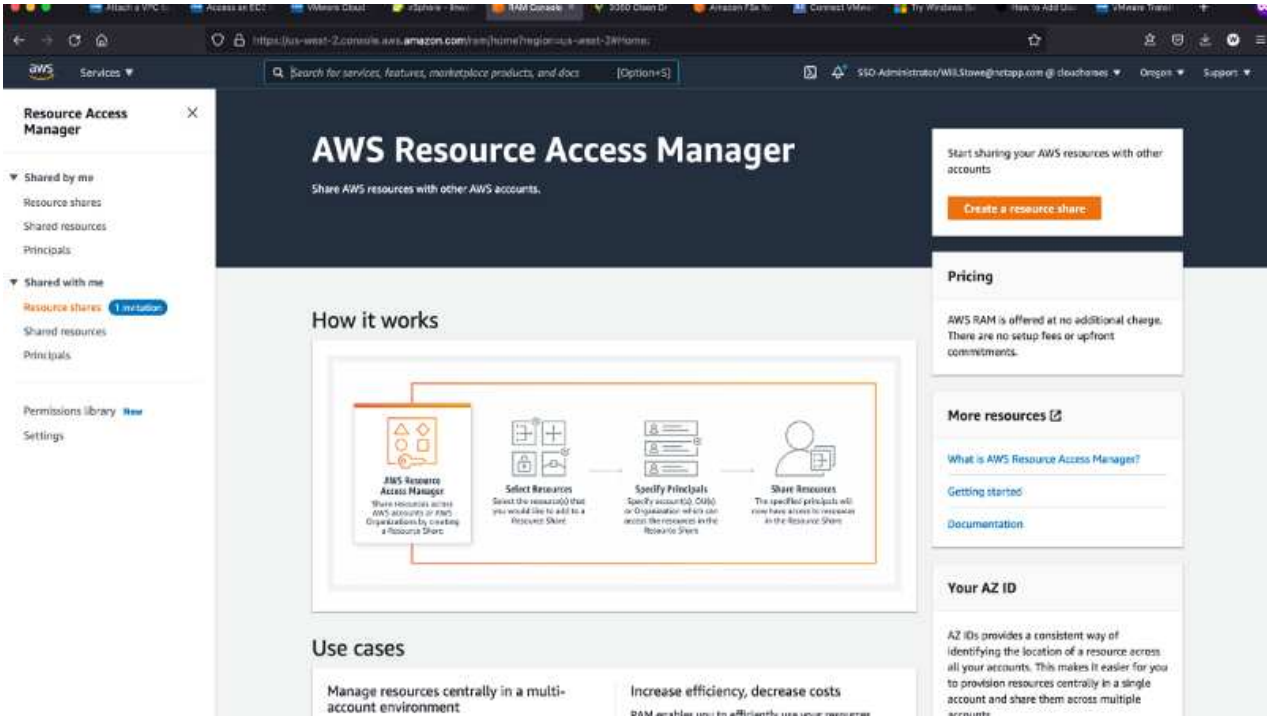


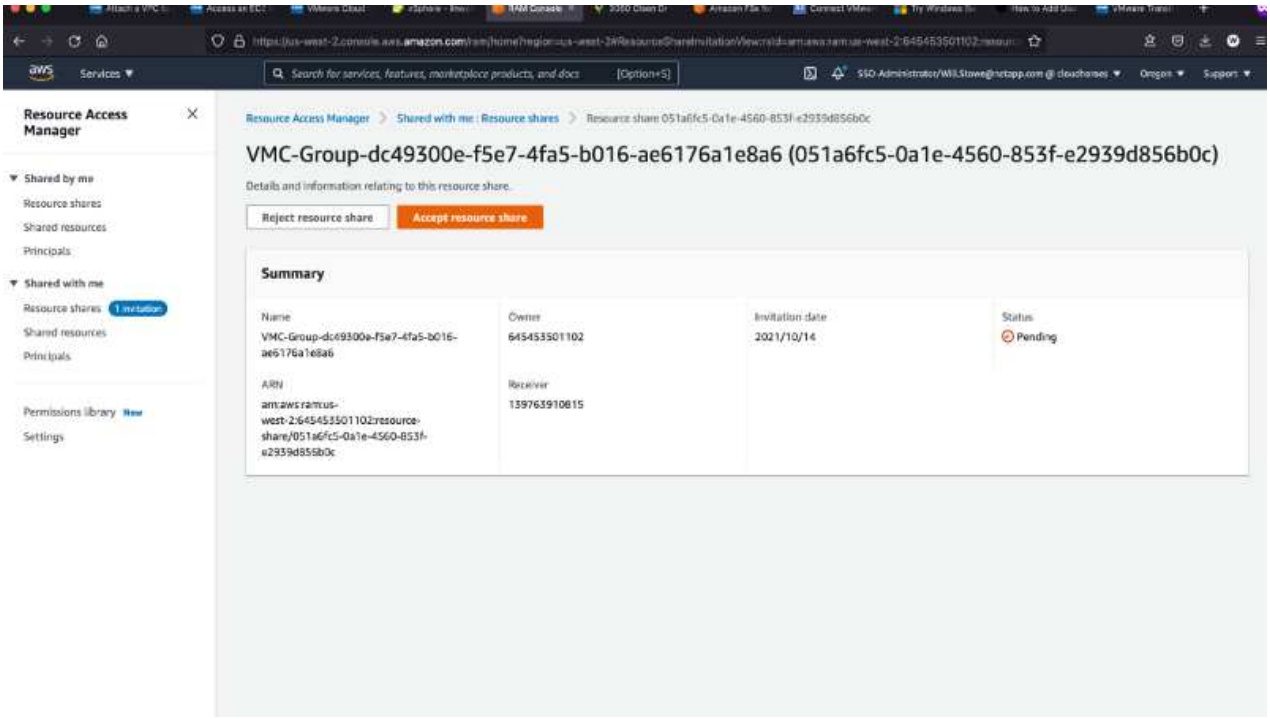
3. 新しく作成した VPC を作成した SDDC グループに接続します。[External VPC （外部 VPC ）] タブを選択し、に従います "外部 VPC を接続する手順" をグループに追加します。このプロセスが完了するまでに 10~15 分かかることがあります。



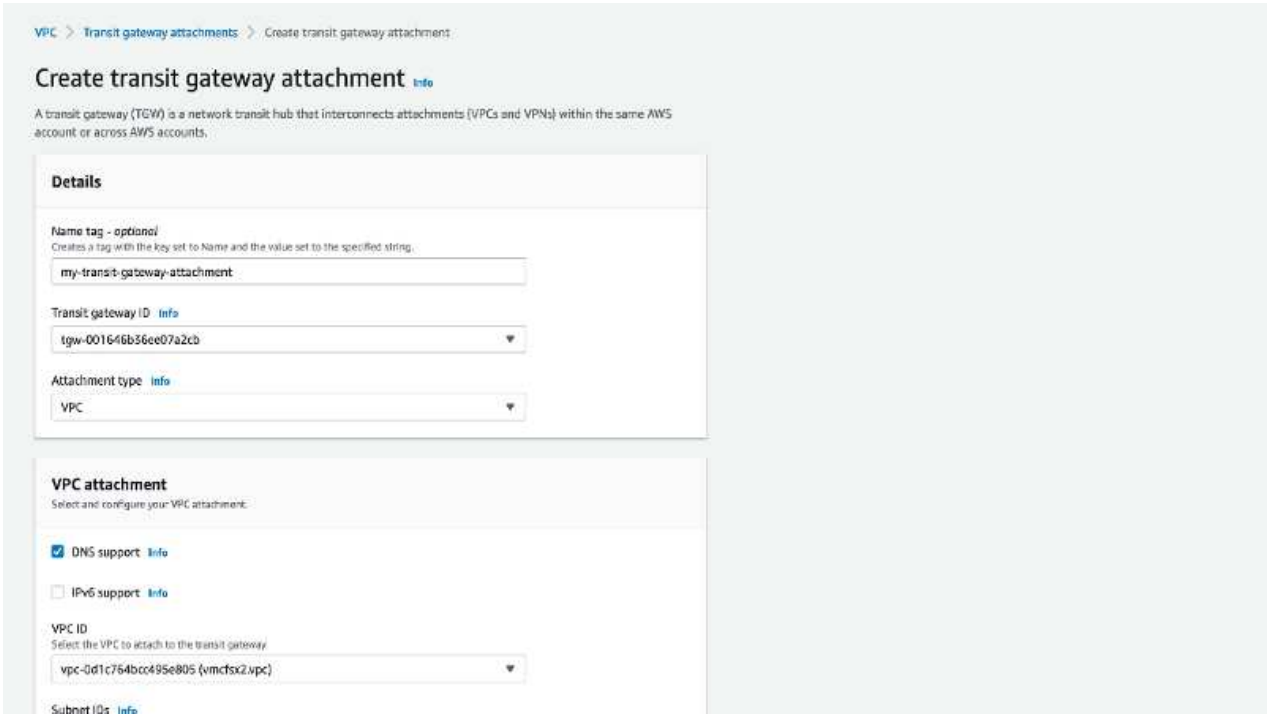


4. 外部 VPC プロセスの一環として、 AWS コンソールから Resource Access Manager を使用して新しい共有リソースにアクセスするように求められます。共有リソースはです "AWS 転送ゲートウェイ" VMware Transit Connect によって管理されます。

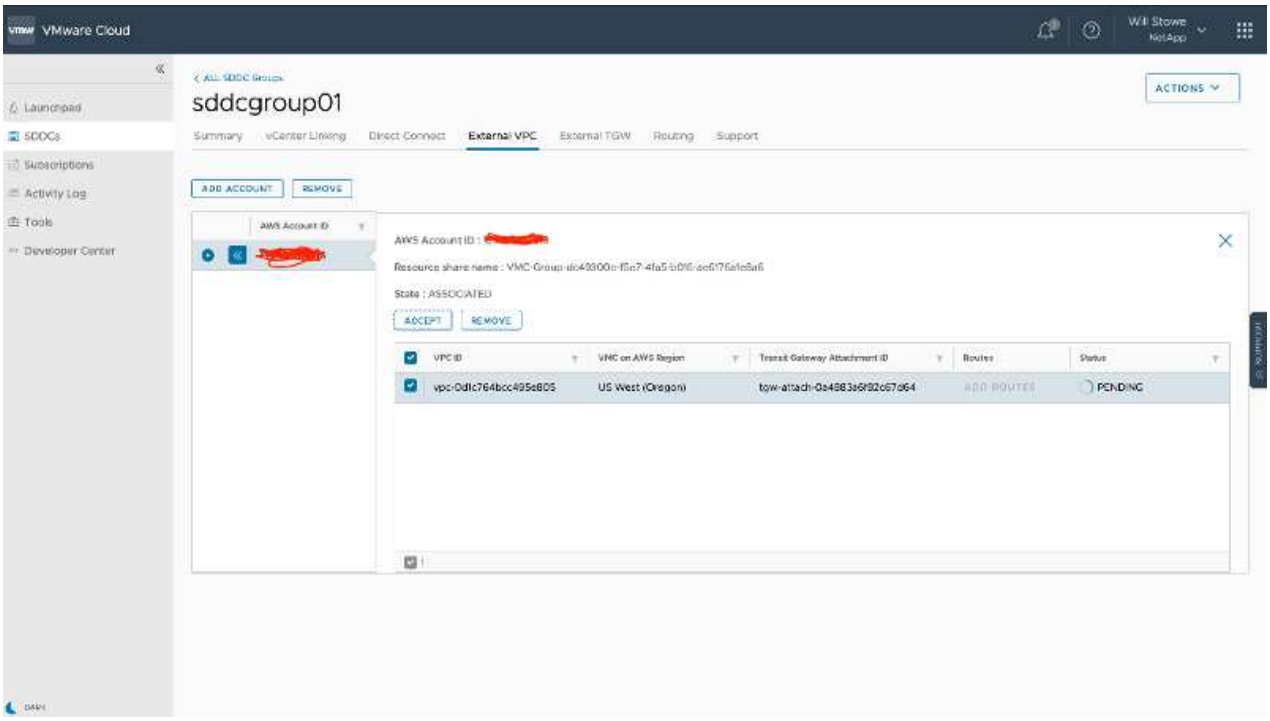




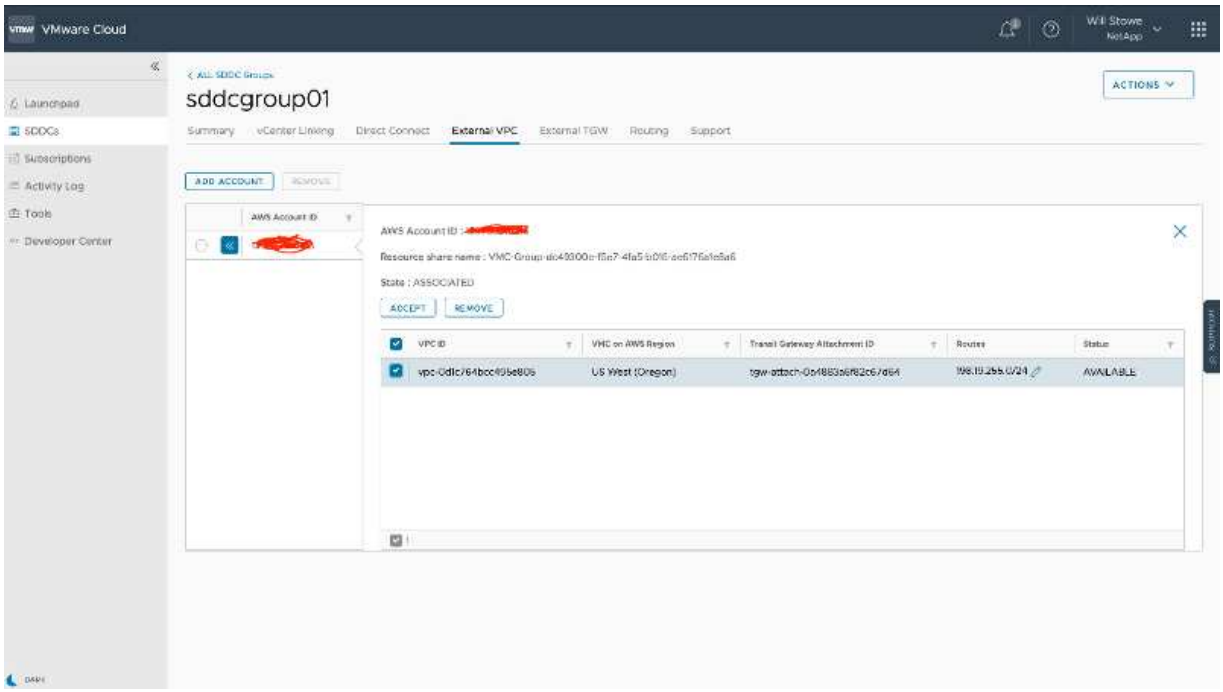
5. トランジットゲートウェイ添付ファイルを作成します。



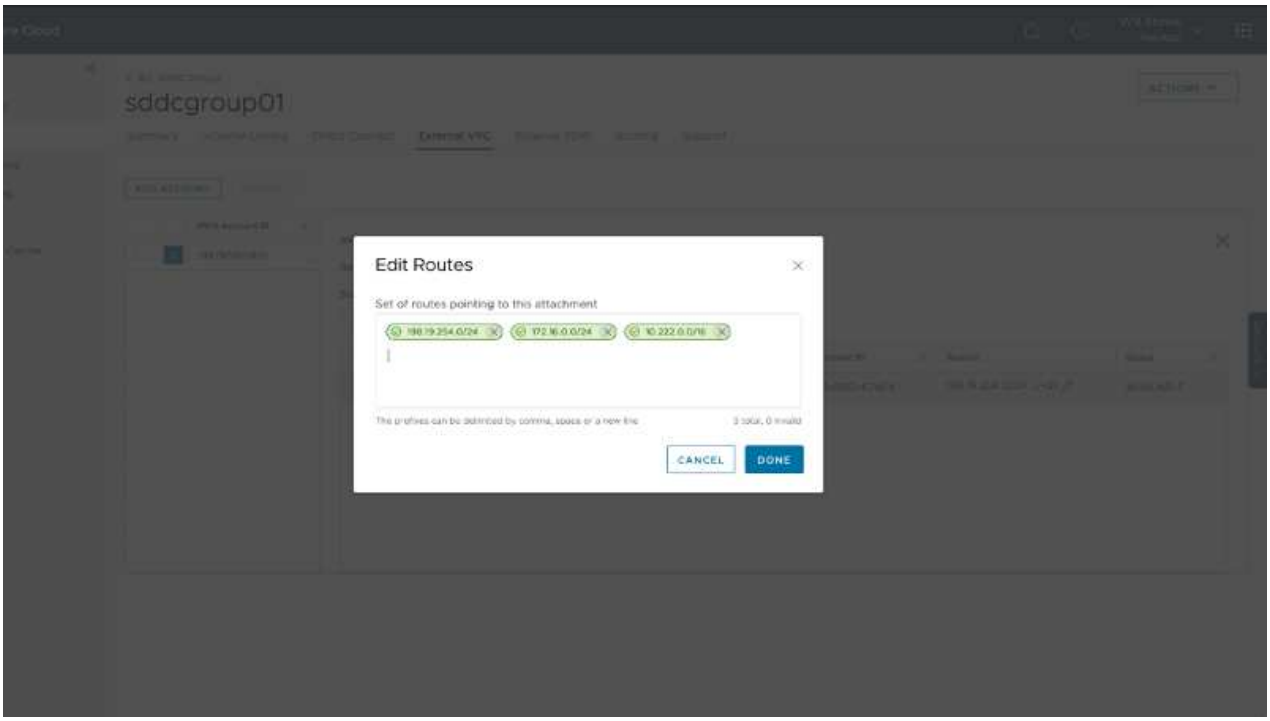
6. VMC コンソールに戻り、 VPC 接続を受け入れます。この処理が完了するまでに約 10 分かかることがあります。



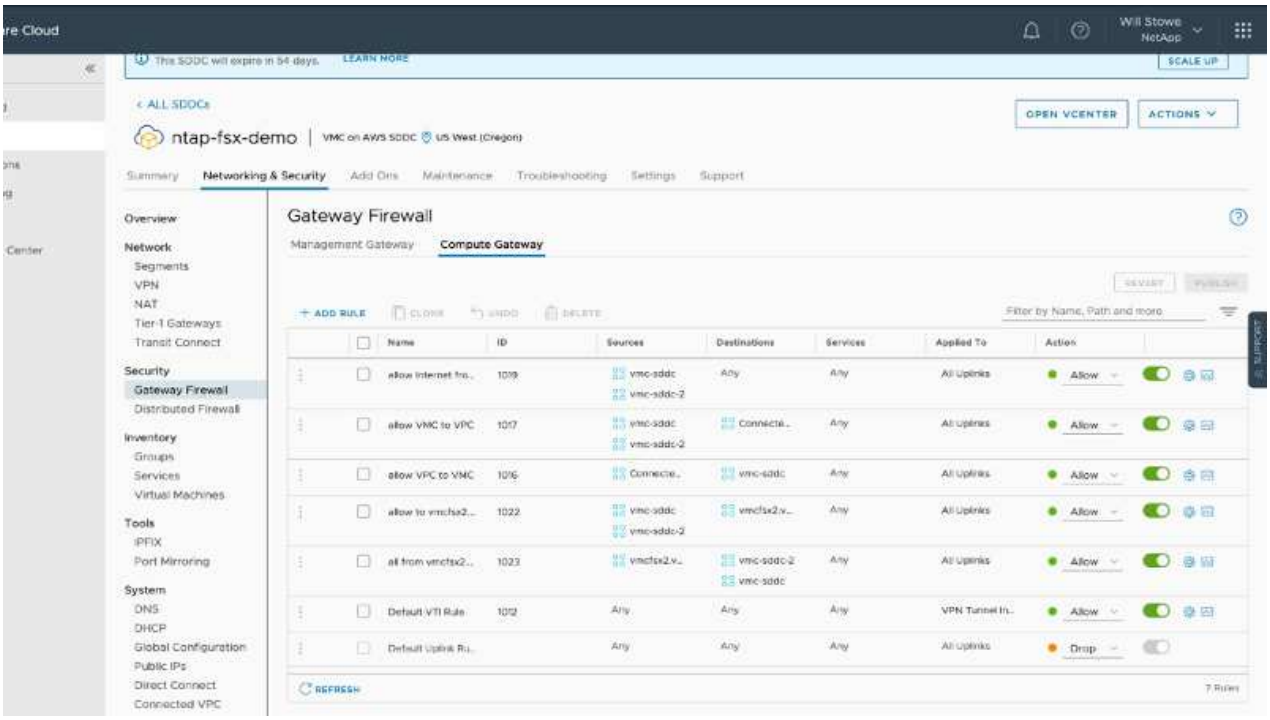
7. [External VPC （外部 VPC ）] タブで、 [Routes] 列の編集アイコンをクリックし、次の必要なルートを追加します。
   - NetApp ONTAP の Amazon FSX のフローティング IP 範囲のルート "フローティング IP"。
   - Cloud Volumes ONTAP のフローティング IP 範囲のルート（該当する場合）。
   - 新しく作成される外部 VPC アドレススペースのルート。



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



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



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

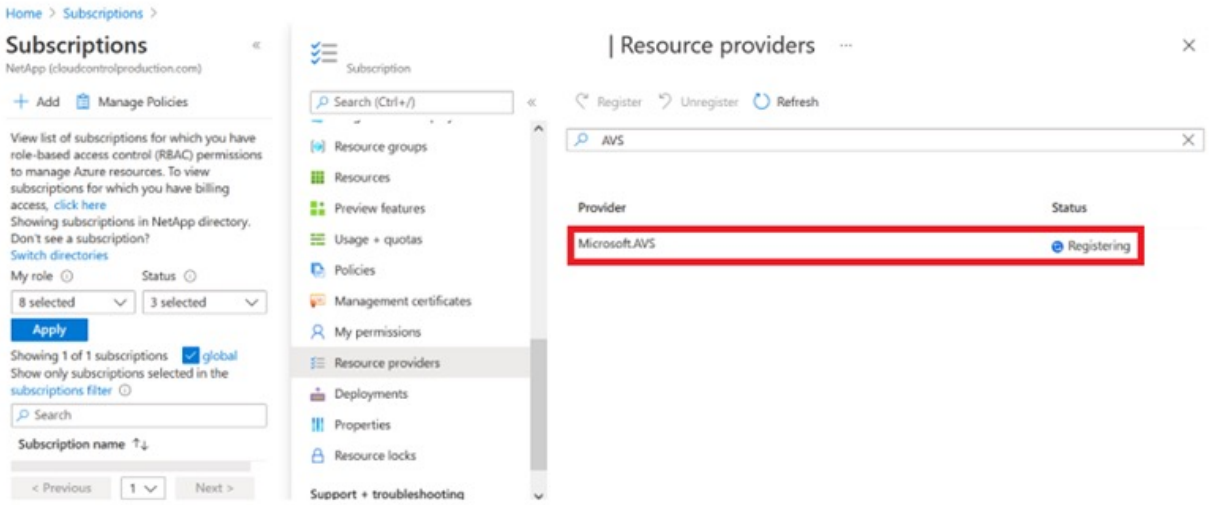
オンプレミスと同様に、 Azure VMware 解決策を計画することは、 VM と移行を作成する本番環境に欠かせません。

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

セットアッププロセスは、次の手順に分けることができます。

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

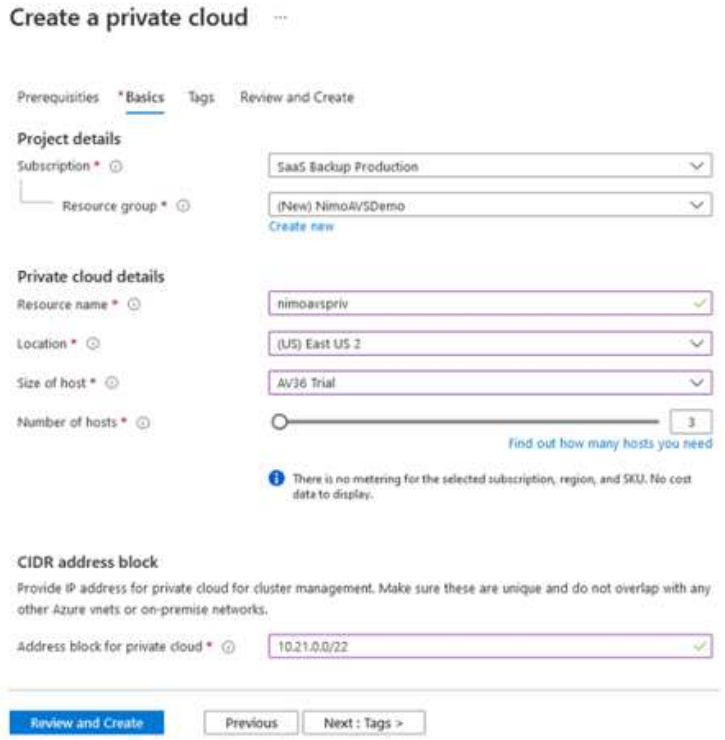
1. Azure ポータルにサインインします。
2. Azure ポータルのメニューで、すべてのサービスを選択します。
3. [すべてのサービス] ダイアログボックスで、サブスクリプションを入力し、 [サブスクリプション] を選択します。
4. 表示するには、サブスクリプションリストからサブスクリプションを選択します。
5. [リソースプロバイダ] を選択し、検索結果に「 Microsoft.AVS 」と入力します。
6. リソースプロバイダが登録されていない場合は、 [登録] を選択します。



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

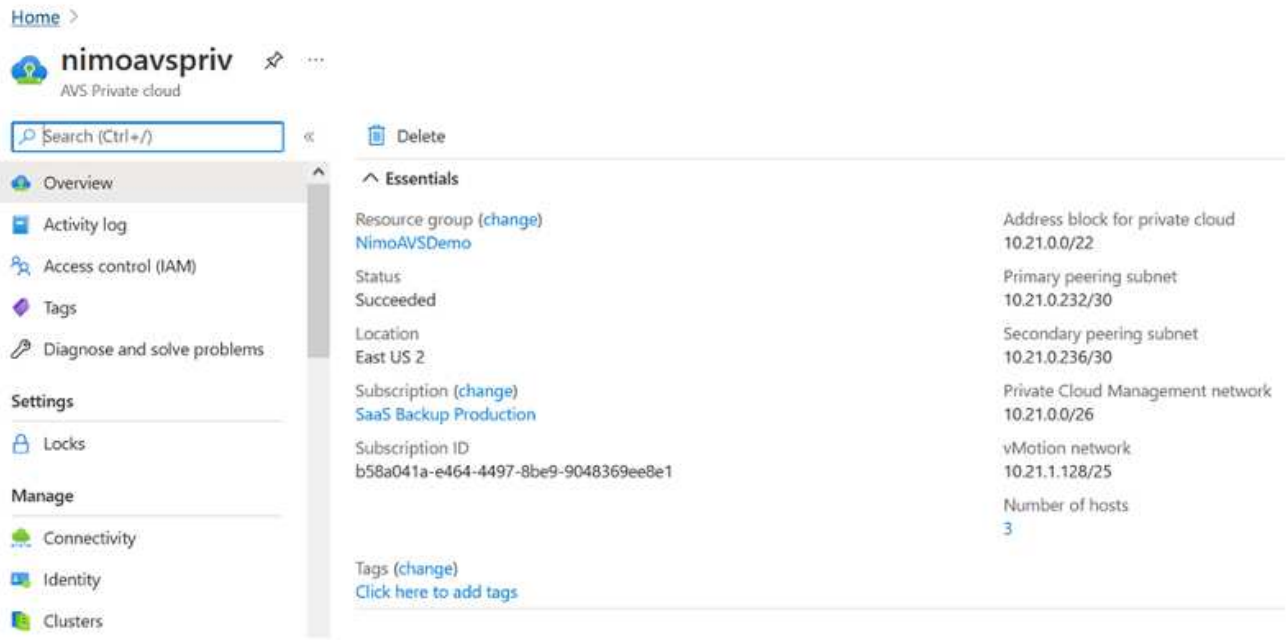
注：

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



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

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



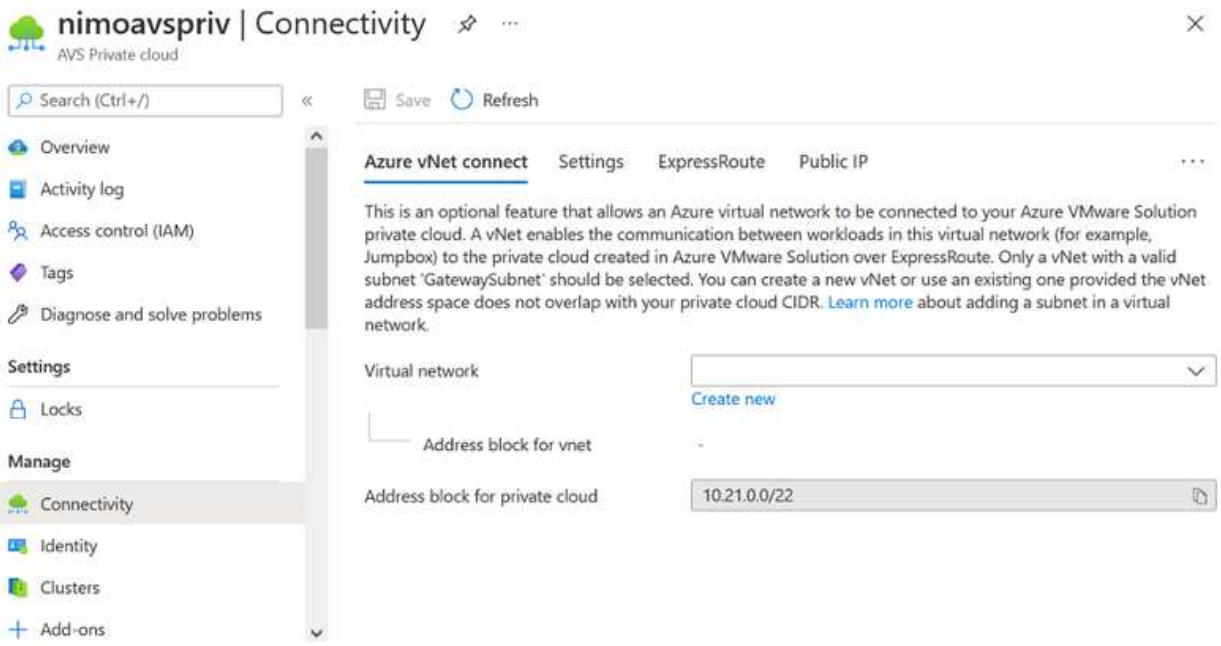
新しい **ExpressRoute** 仮想ネットワークゲートウェイまたは既存の **ExpressRoute** 仮想ネットワークゲートウェイに接続します

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

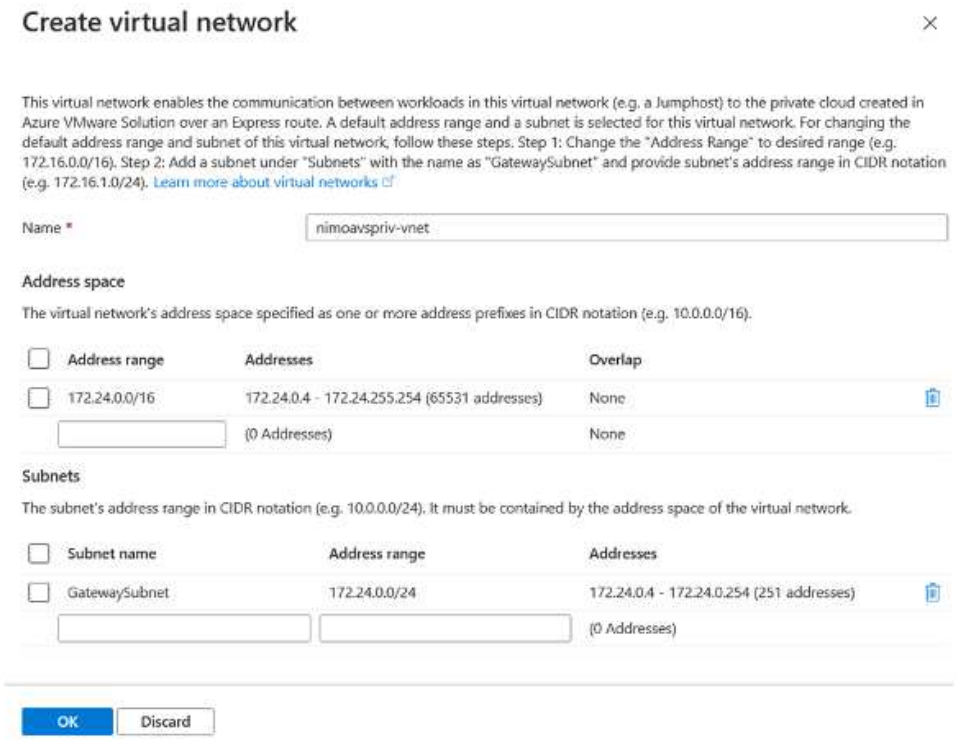
1. Azure VMware 解決策プライベートクラウドに移動し、管理オプションで接続にアクセスします。
2. Azure VNet Connect を選択します。
3. 新しい VNet を作成するには、 Create New オプションを選択します。

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

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



4. 新しい VNet の情報を入力または更新し、 OK を選択します。

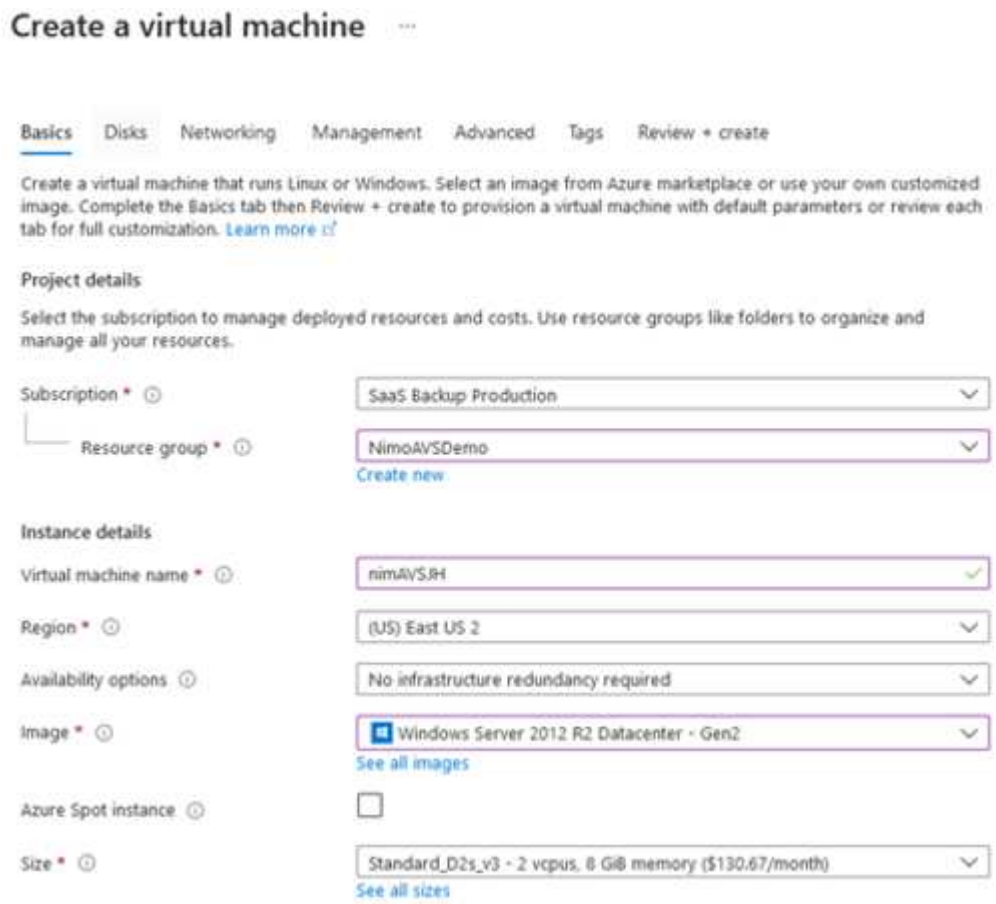


指定したアドレス範囲とゲートウェイサブネットを使用した VNet は、指定したサブスクリプションとリソースグループに作成されます。

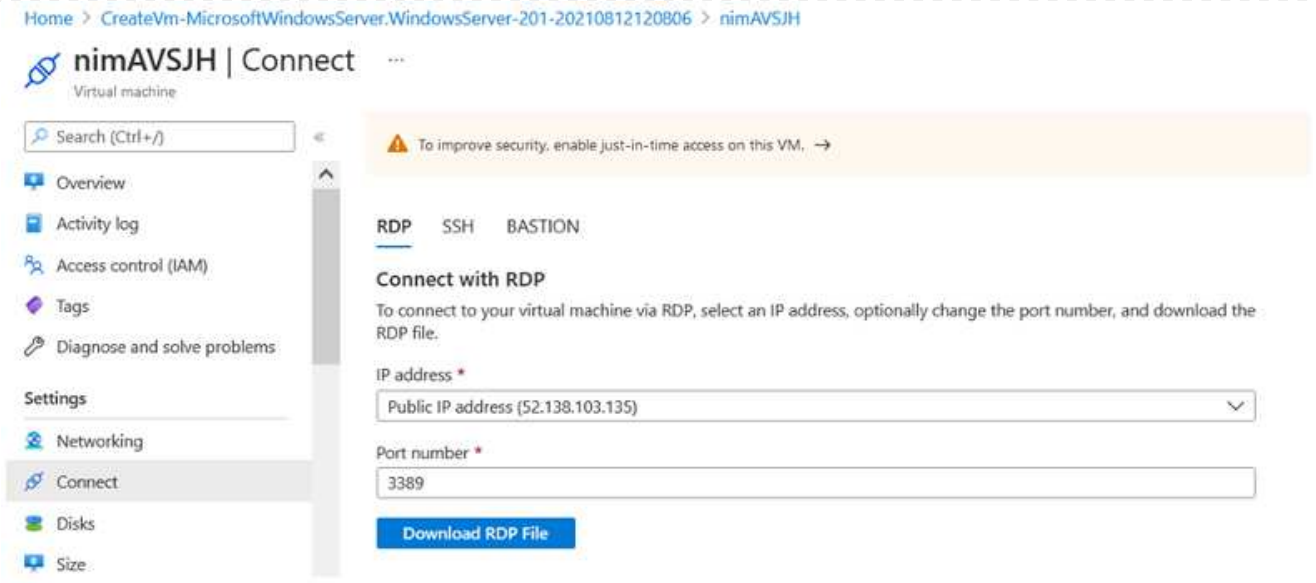
VNet を手動で作成する場合は、適切な SKU と ExpressRoute をゲートウェイタイプとして使用して仮想ネットワークゲートウェイを作成します。導入が完了したら、認証キーを使用して、 ExpressRoute 接続を、 Azure VMware 解決策プライベートクラウドを含む仮想ネットワークゲートウェイに接続します。詳細については、を参照してください "Azure で VMware プライベートクラウド用のネットワークを設定します"。

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

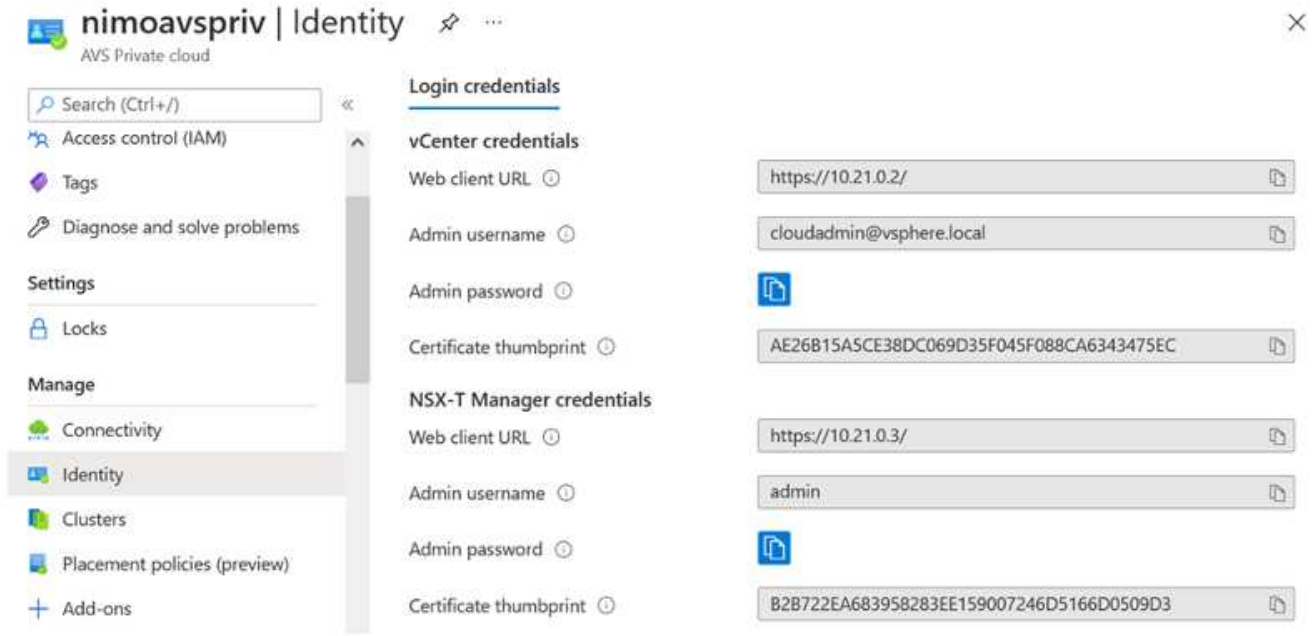
Azure VMware 解決策では、オンプレミスの VMware vCenter でプライベートクラウドを管理することはできません。代わりに、ジャンプホストが Azure VMware 解決策 vCenter インスタンスに接続する必要があります。指定したリソースグループにジャンプホストを作成し、 Azure VMware 解決策 vCenter にサインインします。このジャンプホストは、接続用に作成された同じ仮想ネットワーク上の Windows VM であり、 vCenter と NSX Manager の両方にアクセスできる必要があります。



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

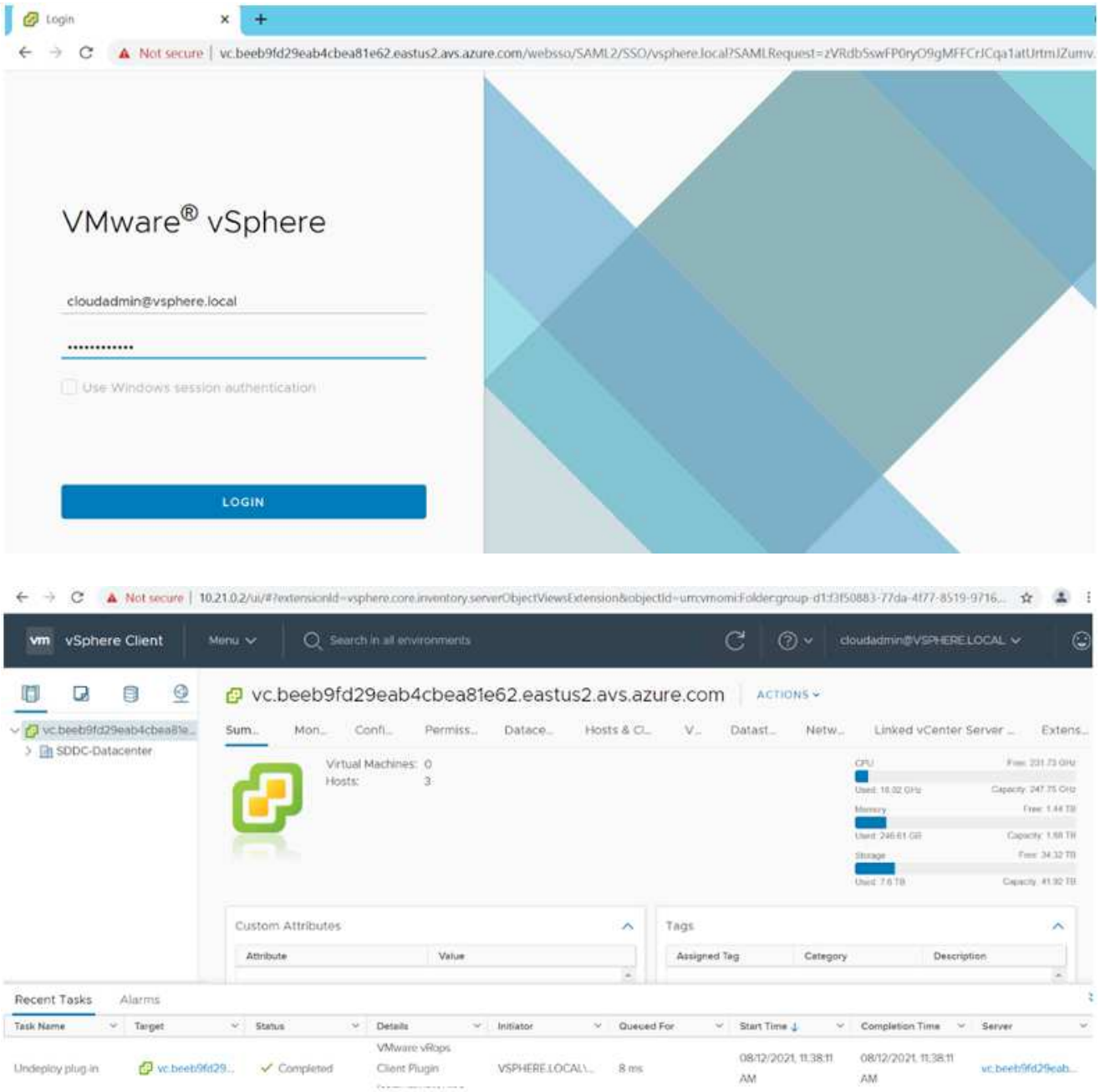


新しく作成したジャンプホスト仮想マシンから、クラウド管理者ユーザを使用して vCenter にサインインします。クレデンシャルにアクセスするには、 Azure ポータルにアクセスし、（プライベートクラウド内の管理オプションで） Identity に移動します。プライベートクラウド vCenter と NSX Manager の URL とユーザー資格情報は、ここからコピーできます。



Windows 仮想マシンでブラウザを開き、 vCenter Web Client の URL にアクセスします admin ユーザのユーザ名に「 * cloudadmin@vsphere.loca l * 」と入力し、コピーしたパスワードを貼り付けます。同様に、 Web クライアントの URL を使用して NSX Manager にアクセスすることもできます admin ユーザ名を使用し、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、既存の階層ゲートウェイを変更したりできます。

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



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

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

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

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

セットアッププロセスは、次の手順に分けることができます。

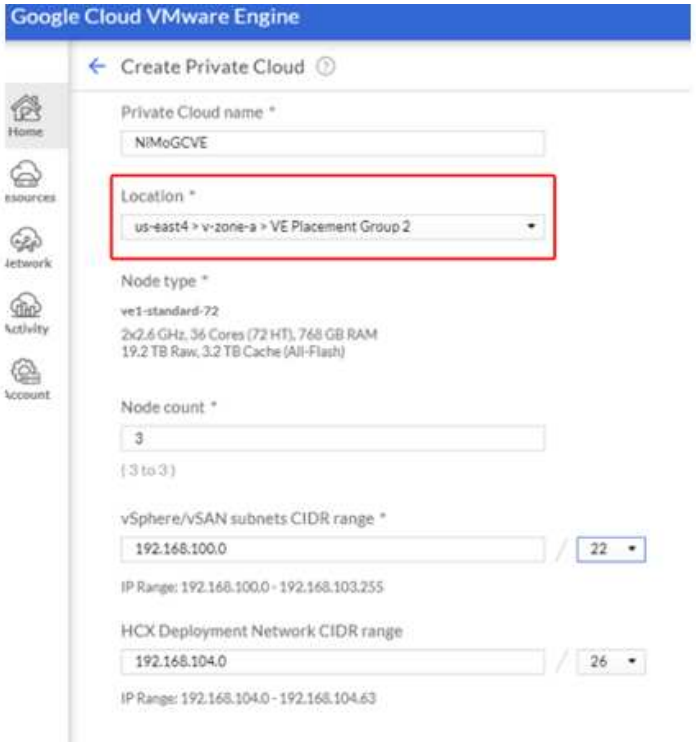
GCVE を導入して設定します

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

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

前提条件

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



注：プライベートクラウドの作成には、 30 分から 2 時間かかります。

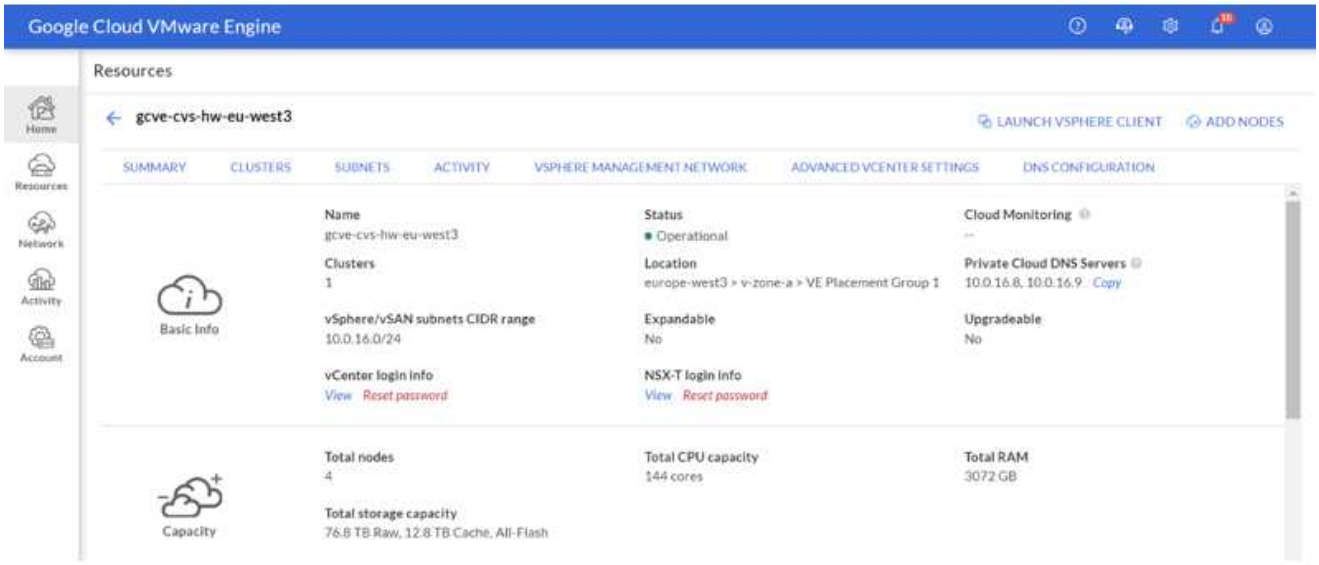
GCVE へのプライベートアクセスを有効にします

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

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

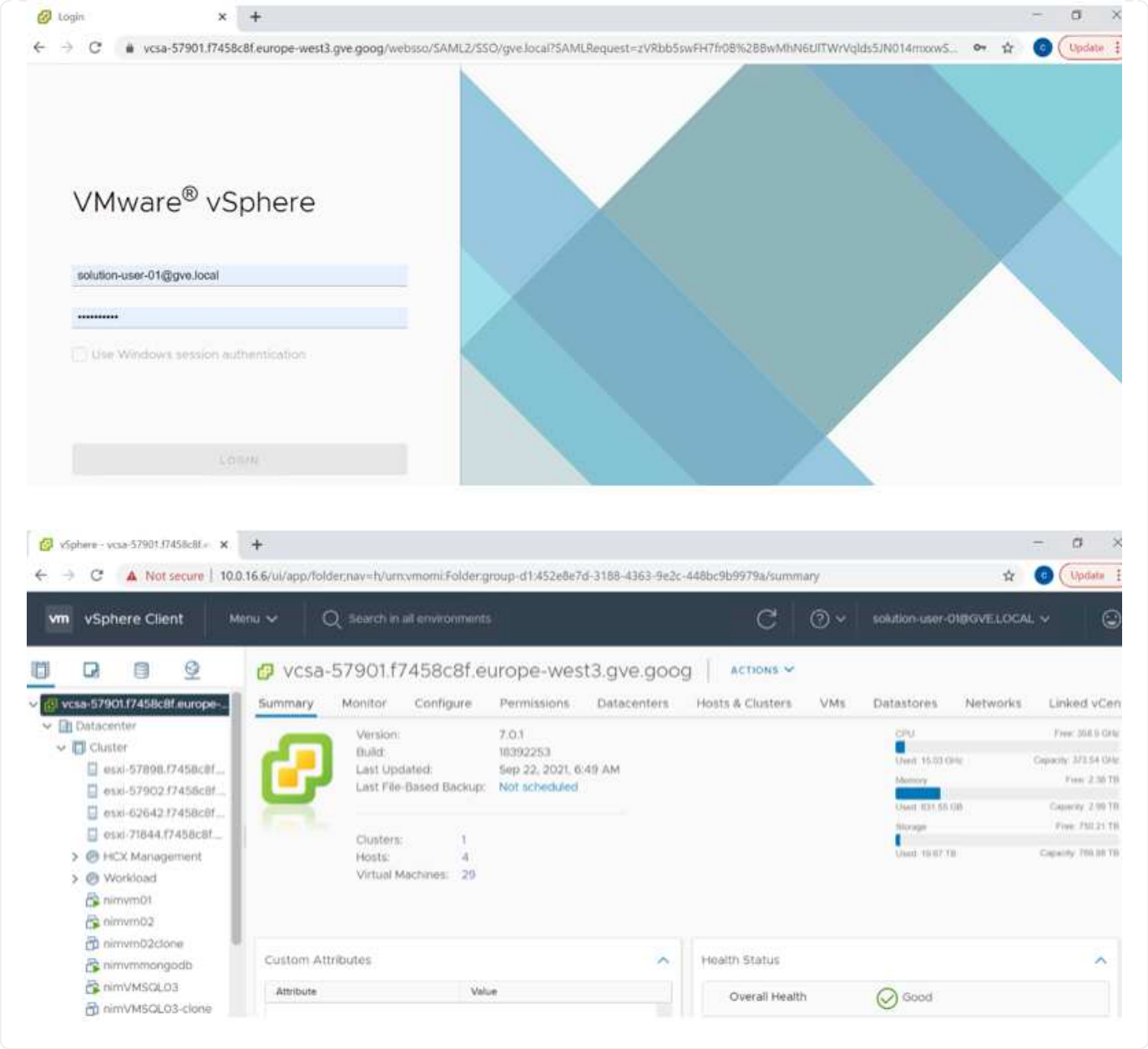
Tenant P	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Sta...	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	Active	Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	Active	Connected

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



Windows 仮想マシンでブラウザを開き、 vCenter Web Client の URL にアクセスします admin ユーザのユーザ名として CloudOwner@gve.loca を使用し、コピーしたパスワードを貼り付けます。同様に、 Web クライアントの URL を使用して NSX Manager にアクセスすることもできます admin ユーザ名を使用し、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、既存の階層ゲートウェイを変更したりできます。

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



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

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

パブリッククラウドプロバイダ向けのネットアップストレージオプション

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

AWS / VMC

AWS は、次の構成でネットアップストレージをサポートします。

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

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

Azure / AVS

Azure は、以下の構成でネットアップストレージをサポートします。

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

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

GCP/GCVE

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

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

詳細を表示します "GCVEのゲスト接続ストレージオプション"。

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

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

ネットアップ、 Niyaz Mohamed

はじめに

成功を収めている組織は、変革と刷新の道を歩んでいます。このプロセスの一環として、企業は通常、既存のVMwareへの投資を使用して、クラウドのメリットを活用し、プロセスの移行、バースト、拡張、ディザスタリカバリを可能なかぎりシームレスに実行する方法を模索しています。クラウドに移行するお客様は、柔軟性とバースト性、データセンターの終了、データセンターの統合、ライフサイクルの終了、合併、合併などのユースケースを評価する必要があります。 買収など。

VMware Cloud on AWSはお客様に独自のハイブリッド機能を提供するため、大多数のお客様に適していますが、ネイティブストレージの選択肢が限られているため、ストレージの負荷が高い組織での有用性が制限され

ています。ストレージはホストに直接関連付けられているため、ストレージを拡張する唯一の方法は、ホストを追加することです。これにより、ストレージを大量に消費するワークロードのコストを35～40%以上増加させることができます。このようなワークロードには、追加の処理能力ではなく、ストレージと分離されたパフォーマンスが必要ですが、追加のホストに料金を支払うことになります。ここでは、を行います "最近の統合" ONTAP 向けFSXは、VMware Cloud on AWSを使用して、大量のストレージとパフォーマンスを必要とするワークロードに最適です。

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

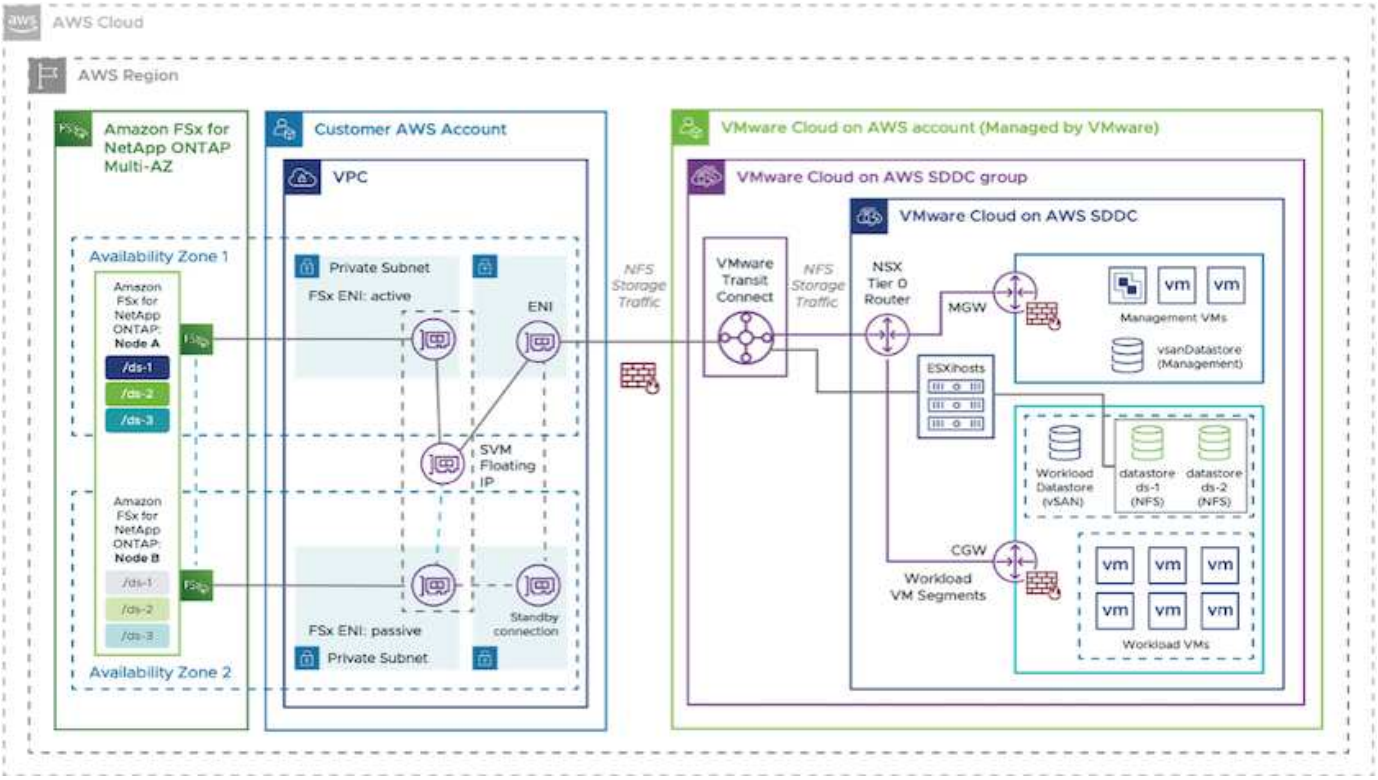
このドキュメントでは、AWS上のVMware Cloud用のNFSデータストアとしてONTAP 用のFSXをプロビジョニングして接続するために必要な手順を説明します。

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

接続オプション

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

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



導入手順の概要は次のとおりです。

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

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

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

まとめ

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

このプロセスの詳細については、詳細なウォークスルービデオをご覧ください。

Amazon FSx for ONTAP VMware Cloud

AWS 用のネットアップゲスト接続ストレージオプション

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

FSX ONTAP の略

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

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

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

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

ゲスト接続ストレージとしての **FSX ONTAP**

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

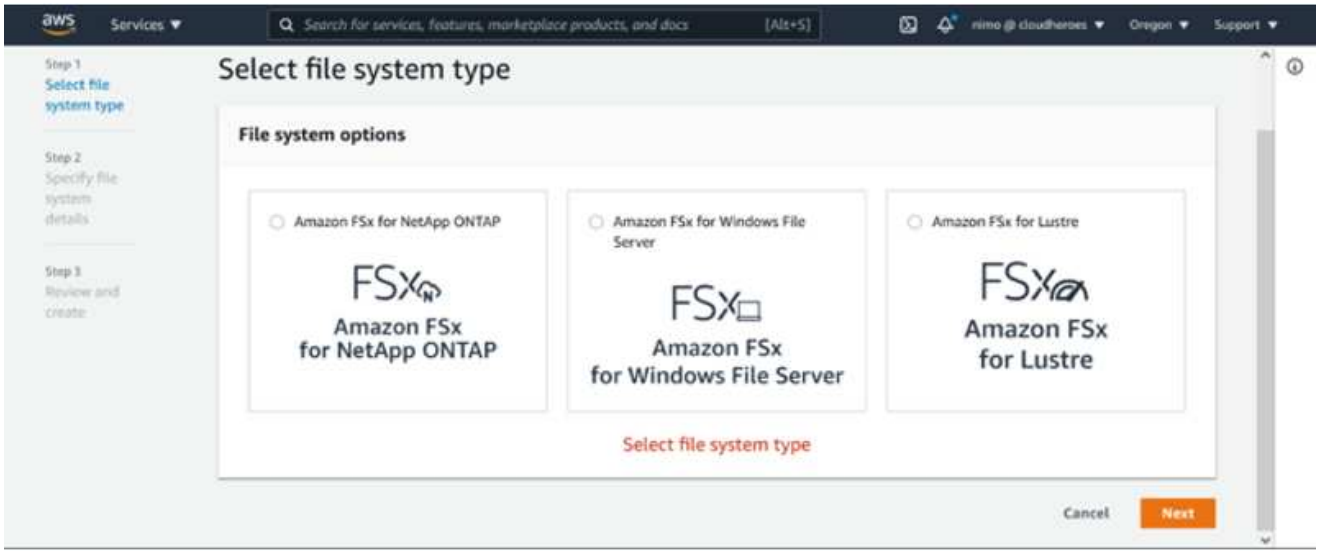
Amazon FSX for NetApp ONTAP ファイル共有および LUN は、 AWS の VMware クラウドにある VMware SDDC 環境内で作成された VM からマウントできます。また、このボリュームは、 Linux クライアントにマウントして NFS または SMB プロトコルを使用して Windows クライアントにマッピングすることもできます。また、 iSCSI 経由でマウントした場合、 Linux クライアントまたは Windows クライアントから LUN にブロックデバイスとしてアクセスできます。NetApp ONTAP ファイルシステム用の Amazon FSX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

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

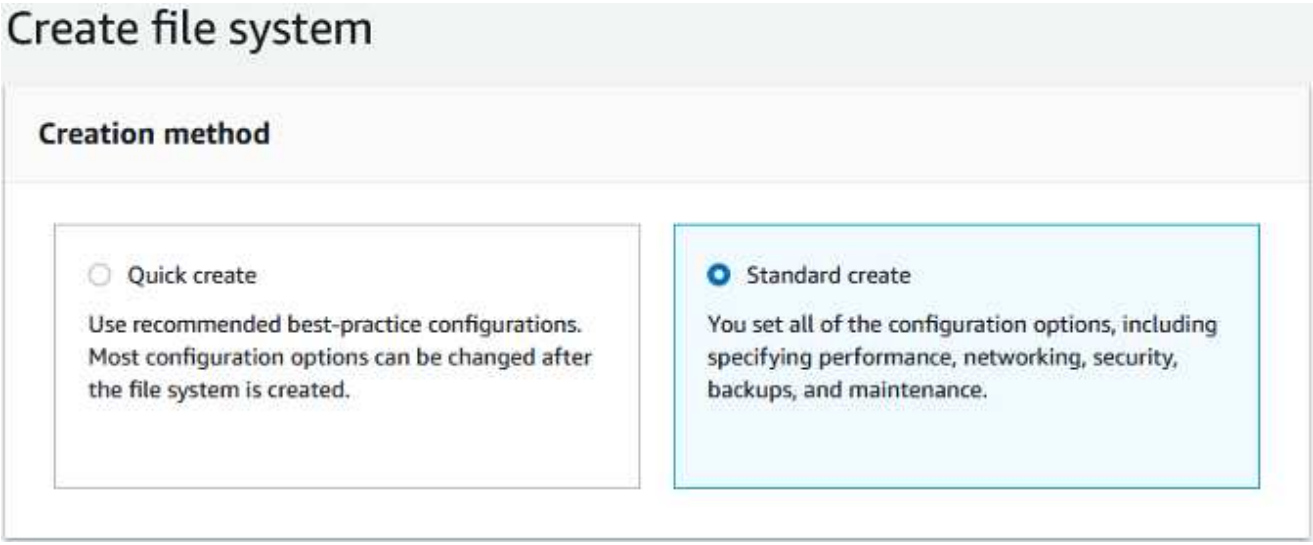
ONTAP ボリューム用に Amazon FSX を作成してマウントします

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

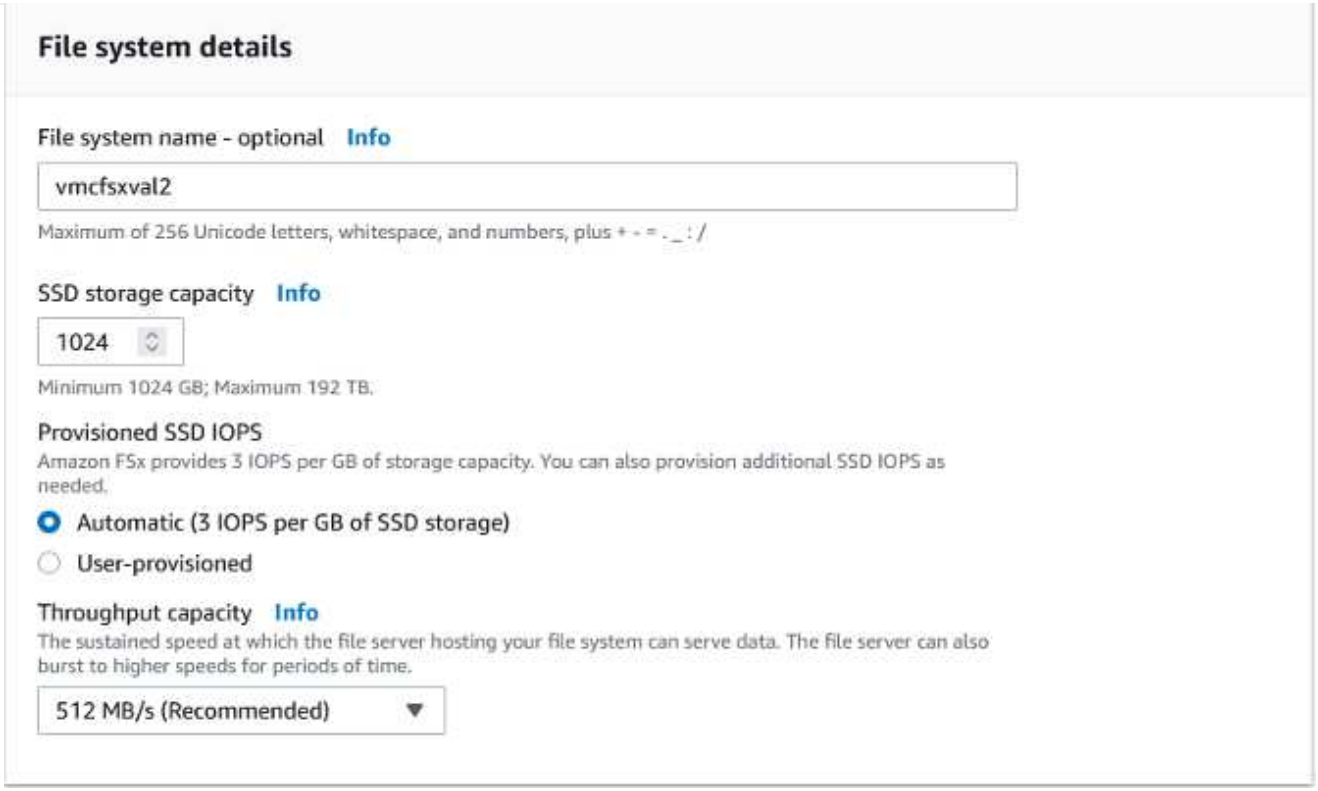
1. を開きます "Amazon FSX コンソール" ファイルシステムの作成を選択して ' ファイルシステム作成ウィザードを開始します
2. [Select File System Type] ページで、 [Amazon FSX for NetApp ONTAP] を選択し、 [Next] をクリックします。Create File System ページが表示されます。



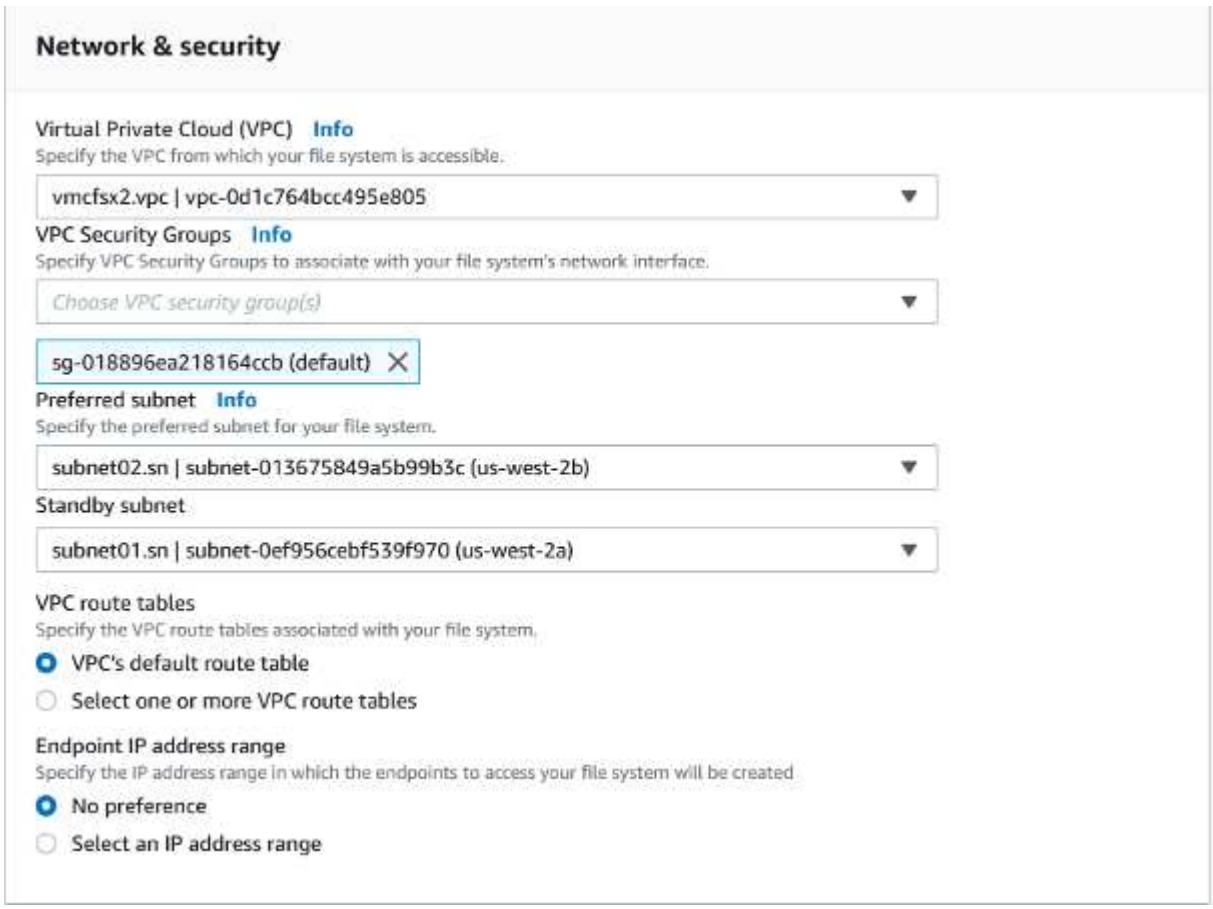
1. Virtual Private Cloud （ VPC ；仮想プライベートクラウド）のネットワークセクションで、ルーティングテーブルとともに適切な VPC と優先サブネットを選択します。この場合、ドロップダウンから vmcfsx2.vPC が選択されます。



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

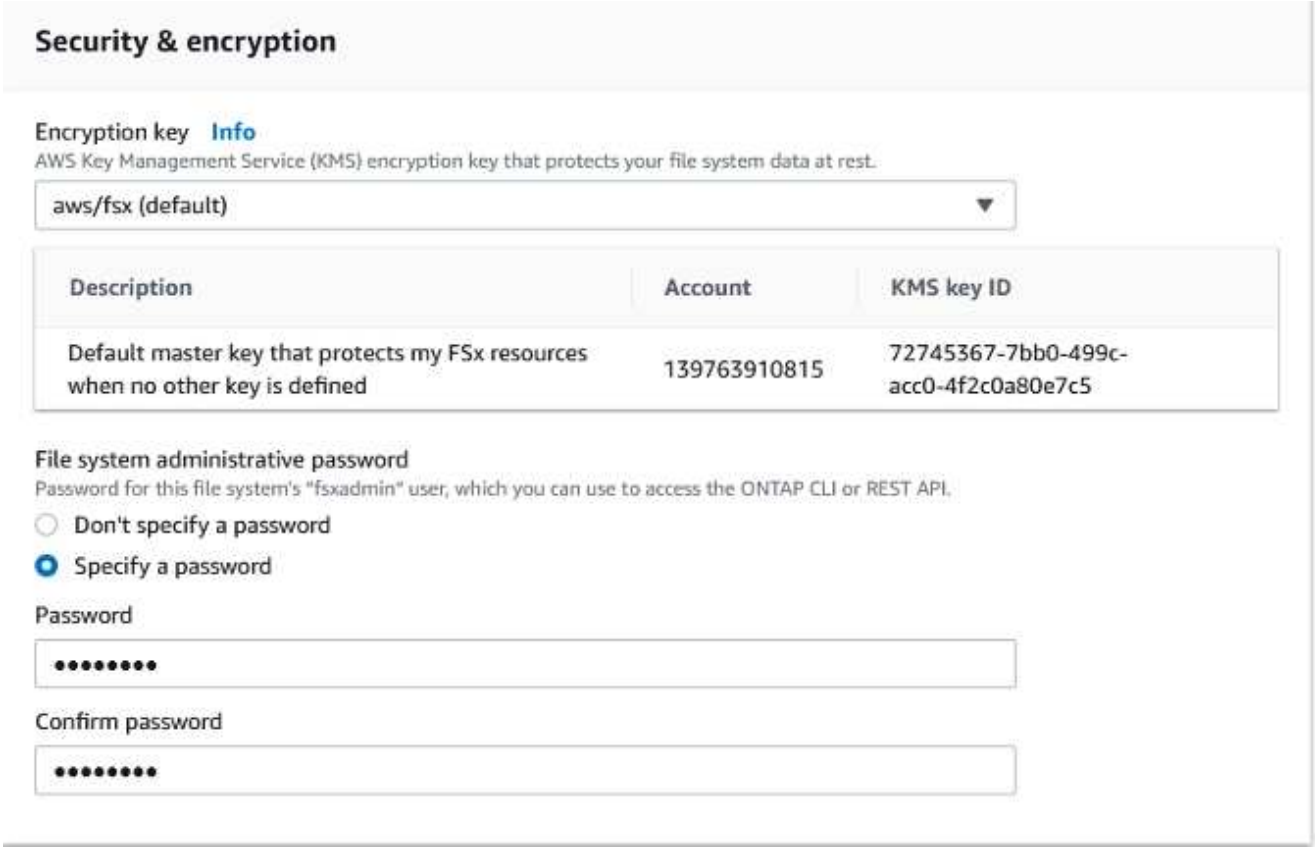


1. Virtual Private Cloud （ VPC ；仮想プライベートクラウド）のネットワークセクションで、ルーティングテーブルとともに適切な VPC と優先サブネットを選択します。この場合、ドロップダウンから vmcfsx2.vPC が選択されます。

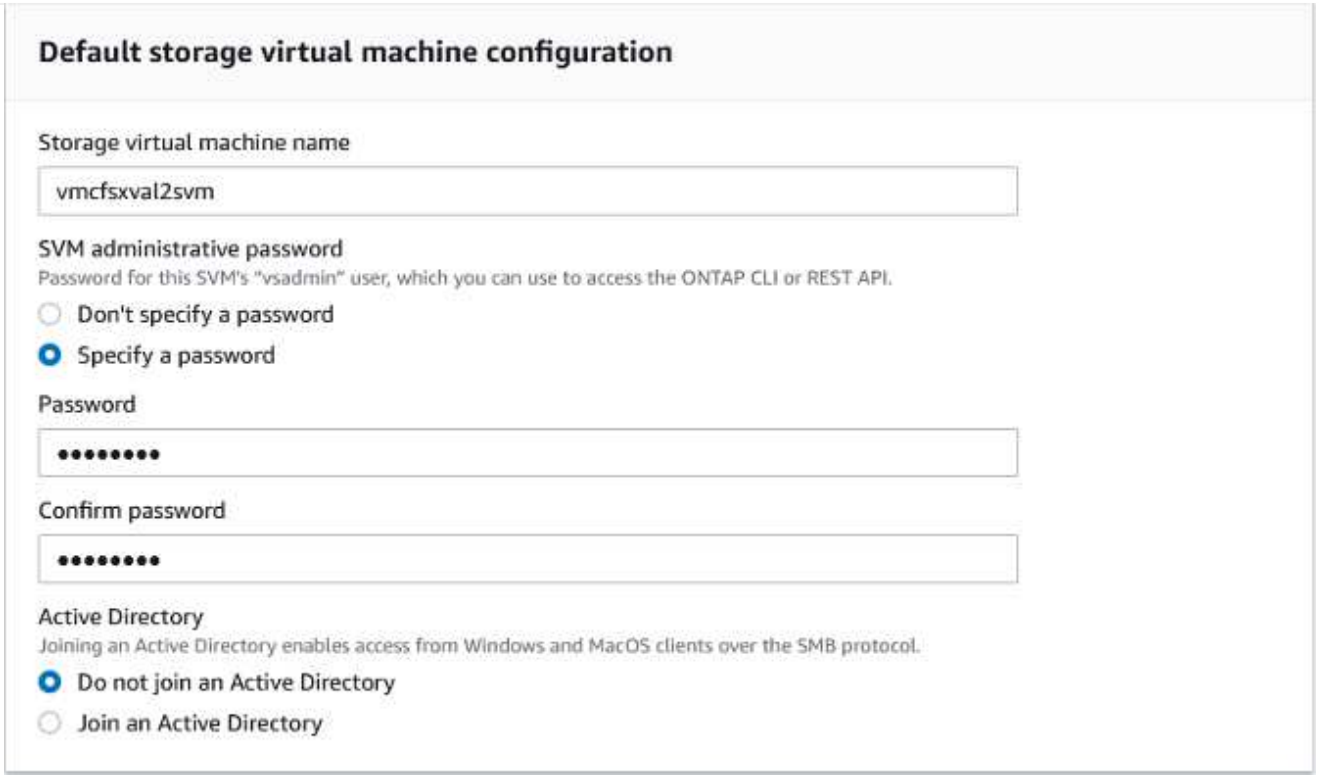


Virtual Private Cloud （ VPC ；仮想プライベートクラウド）のネットワークセクションで、ルーティングテーブルとともに適切な VPC と優先サブネットを選択します。この場合、ドロップダウンから vmcfsx2.vPC が選択されます。

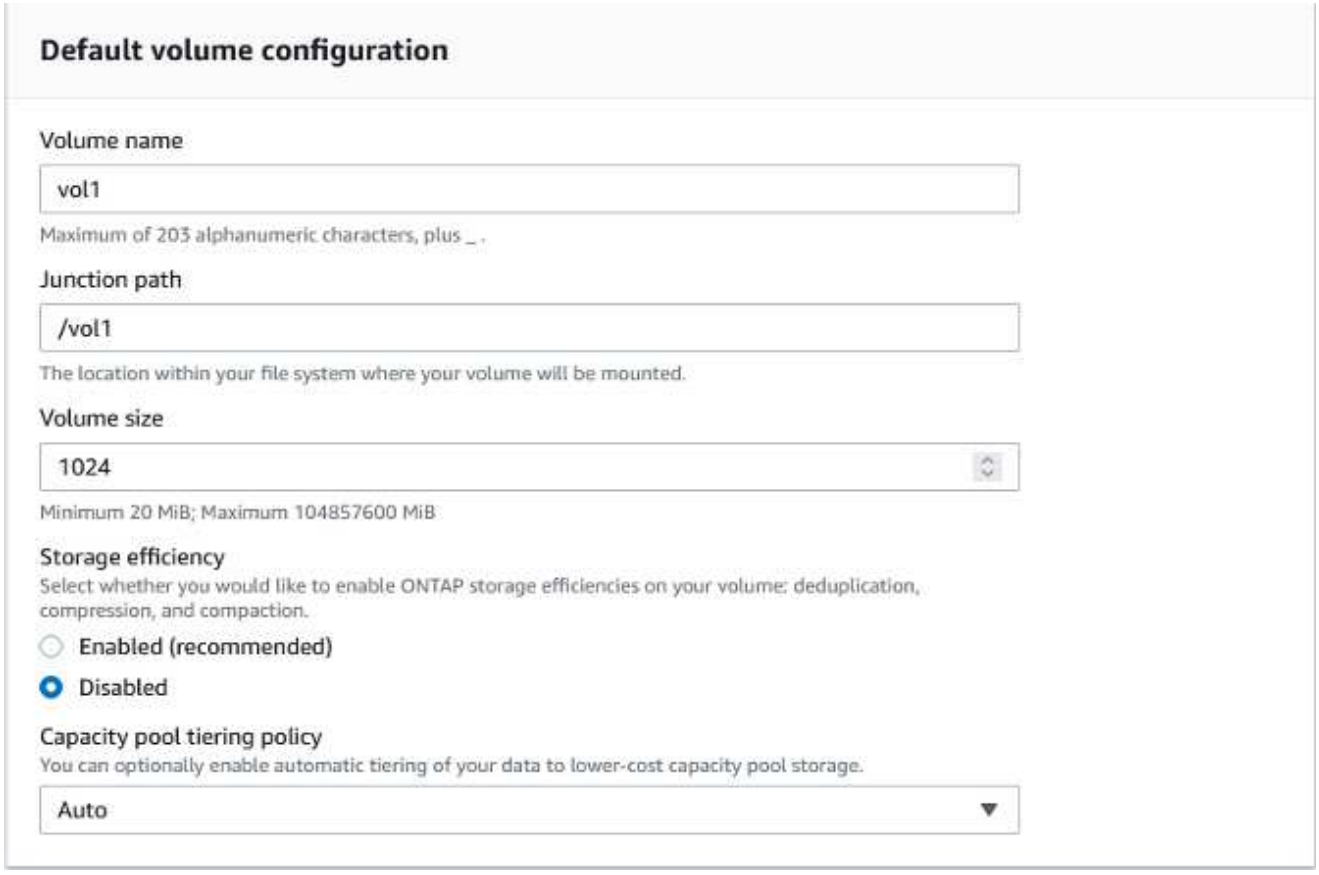
1. 「セキュリティと暗号化」セクションの「暗号化キー」で、ファイルシステムの保存データを保護する AWS Key Management Service （ AWS KMS ）暗号化キーを選択します。File System Administrative Password に、 fsxadmin ユーザのセキュアなパスワードを入力します。



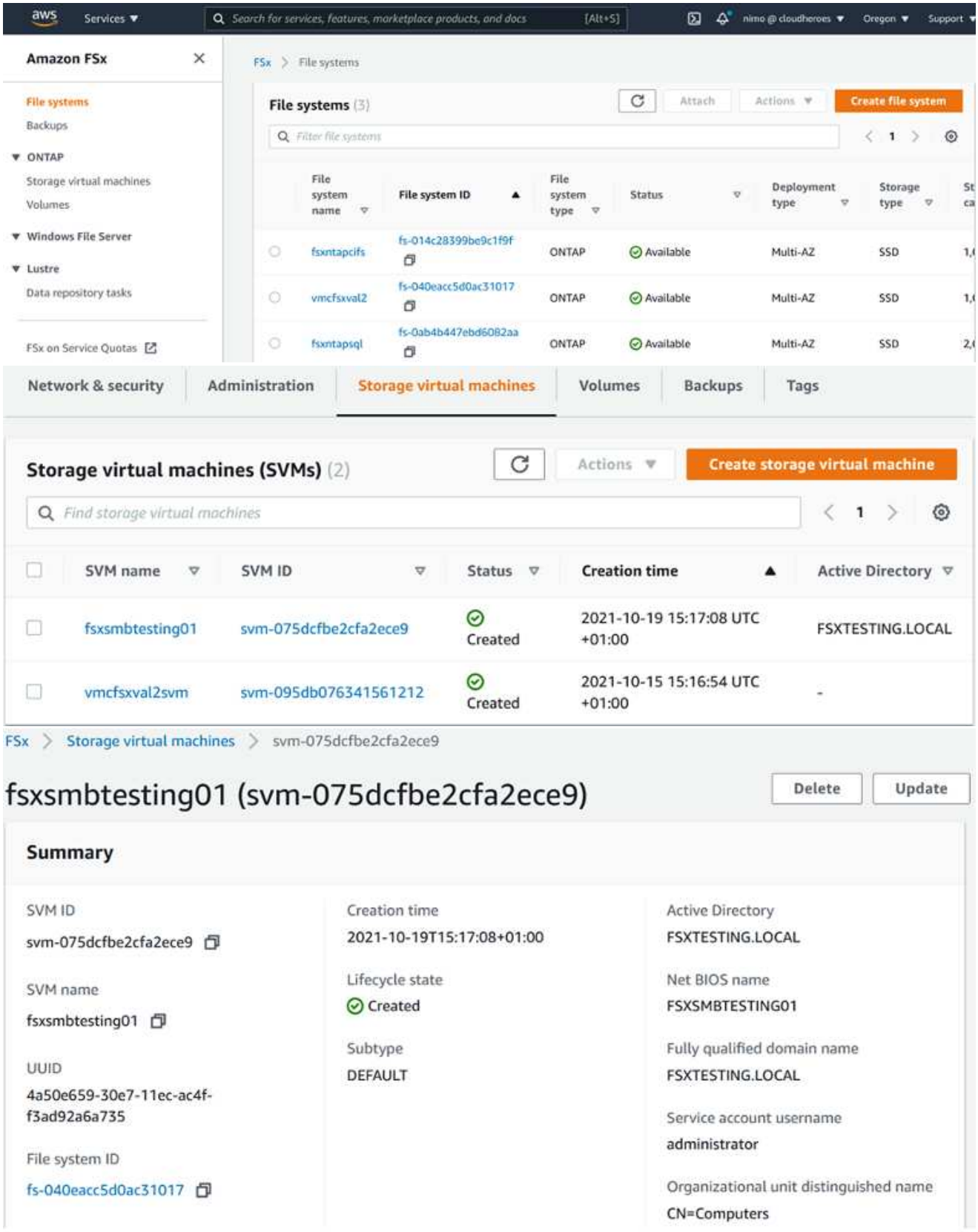
1. 仮想マシンで、 vsadmin で REST API または CLI を使用して ONTAP を管理するために使用するパスワードを指定します。パスワードを指定しない場合は、 SVM の管理に fsxadmin ユーザを使用できます。Active Directory セクションで、 SMB 共有をプロビジョニングするために Active Directory を SVM に追加してください。Default Storage Virtual Machine Configuration セクションで、この検証でストレージの名前を指定します。 SMB 共有は自己管理 Active Directory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



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



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

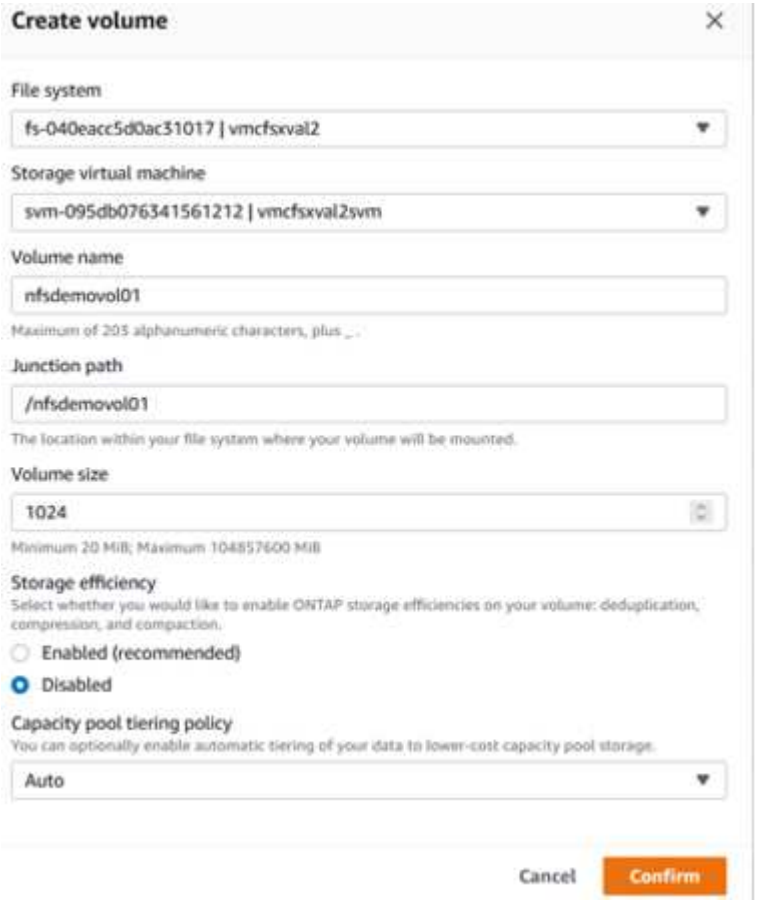


詳細については、を参照してください "Amazon FSX for NetApp ONTAP の利用を開始する"。

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

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

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



FSX ONTAP ボリュームを **Linux** クライアントにマウントします

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

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

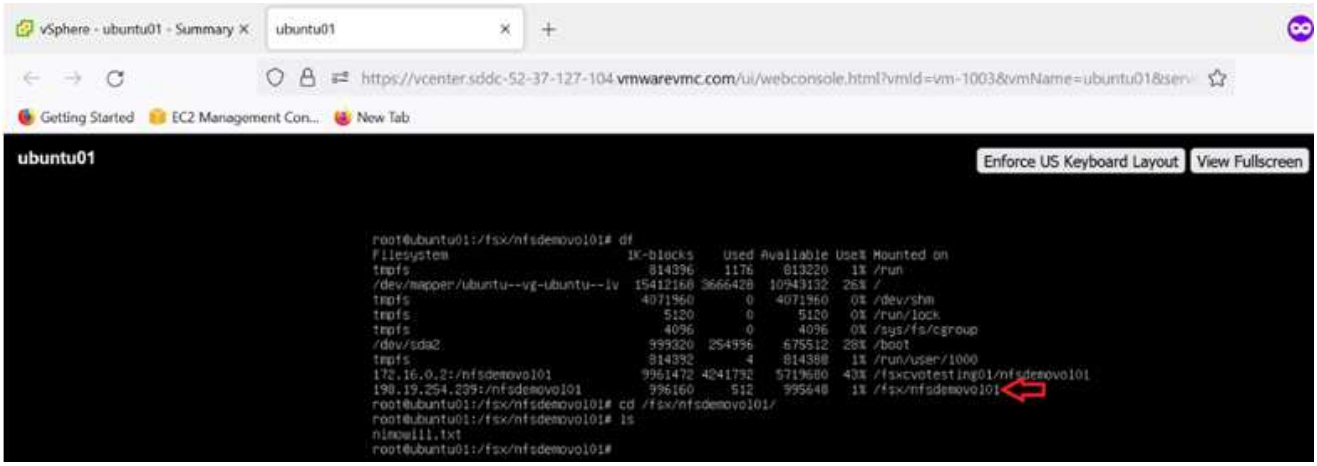
```
 $ sudo mkdir /fsx/nfsdemovol01
```

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

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

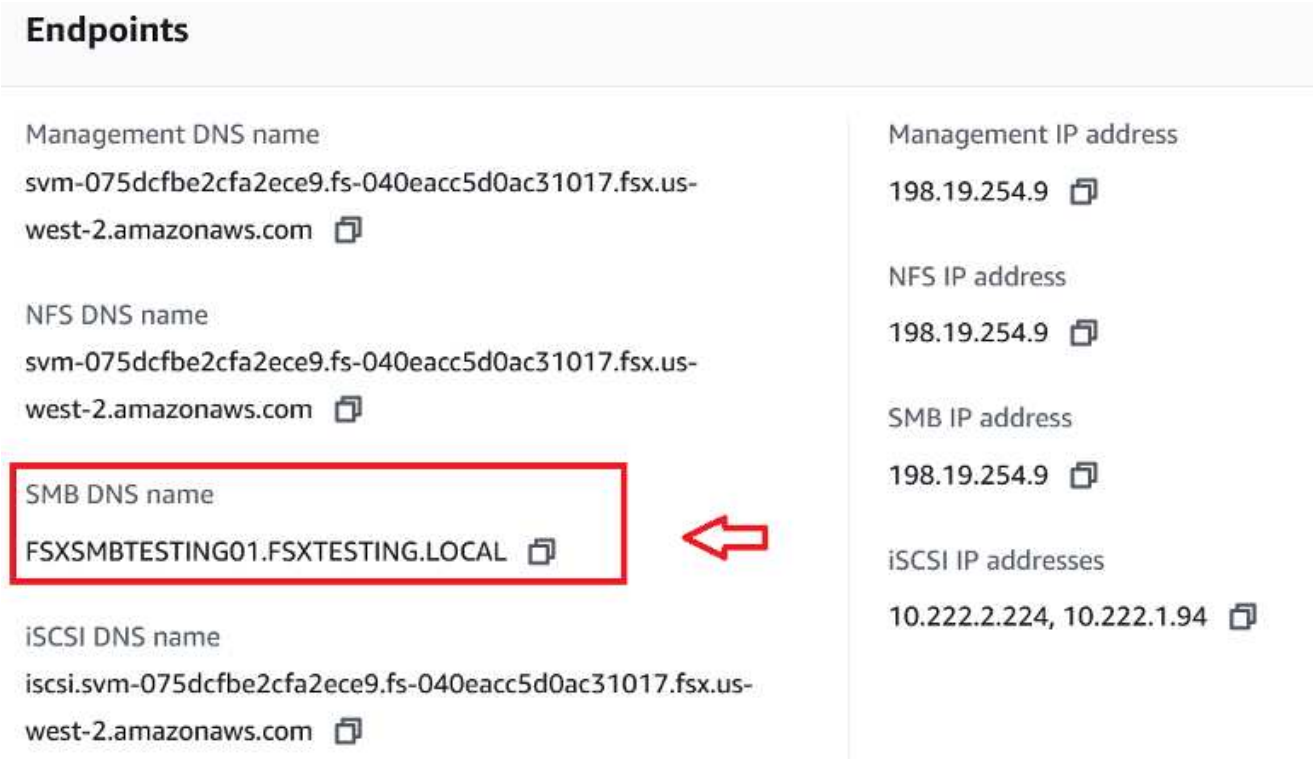


FSX ONTAP ボリュームを Linux クライアントにマウントします

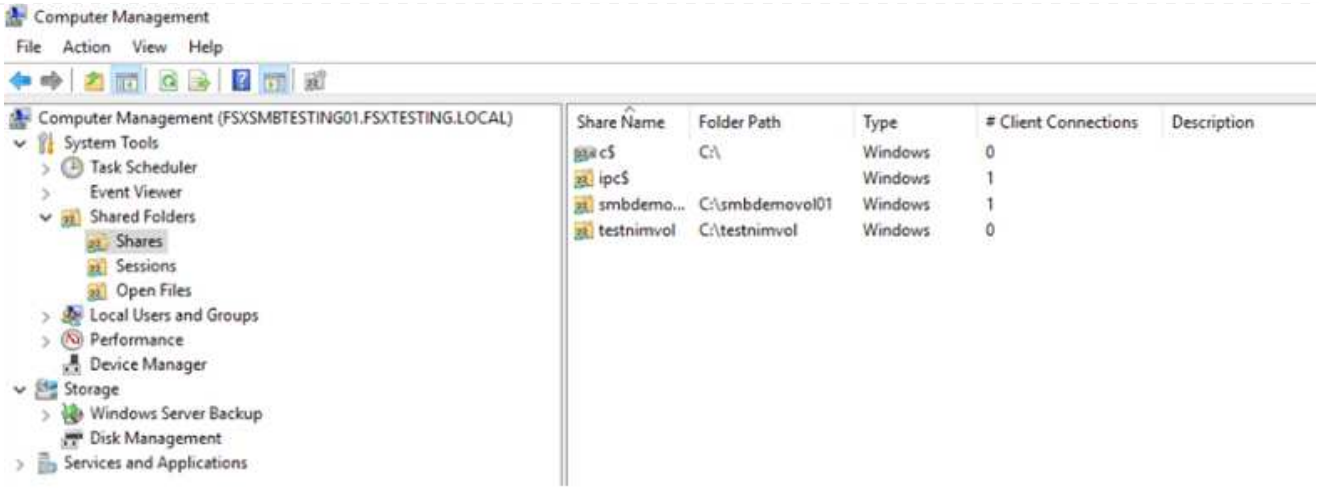
Amazon FSX ファイルシステム上のファイル共有を管理およびマッピングするには、共有フォルダ GUI を使用する必要があります。

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

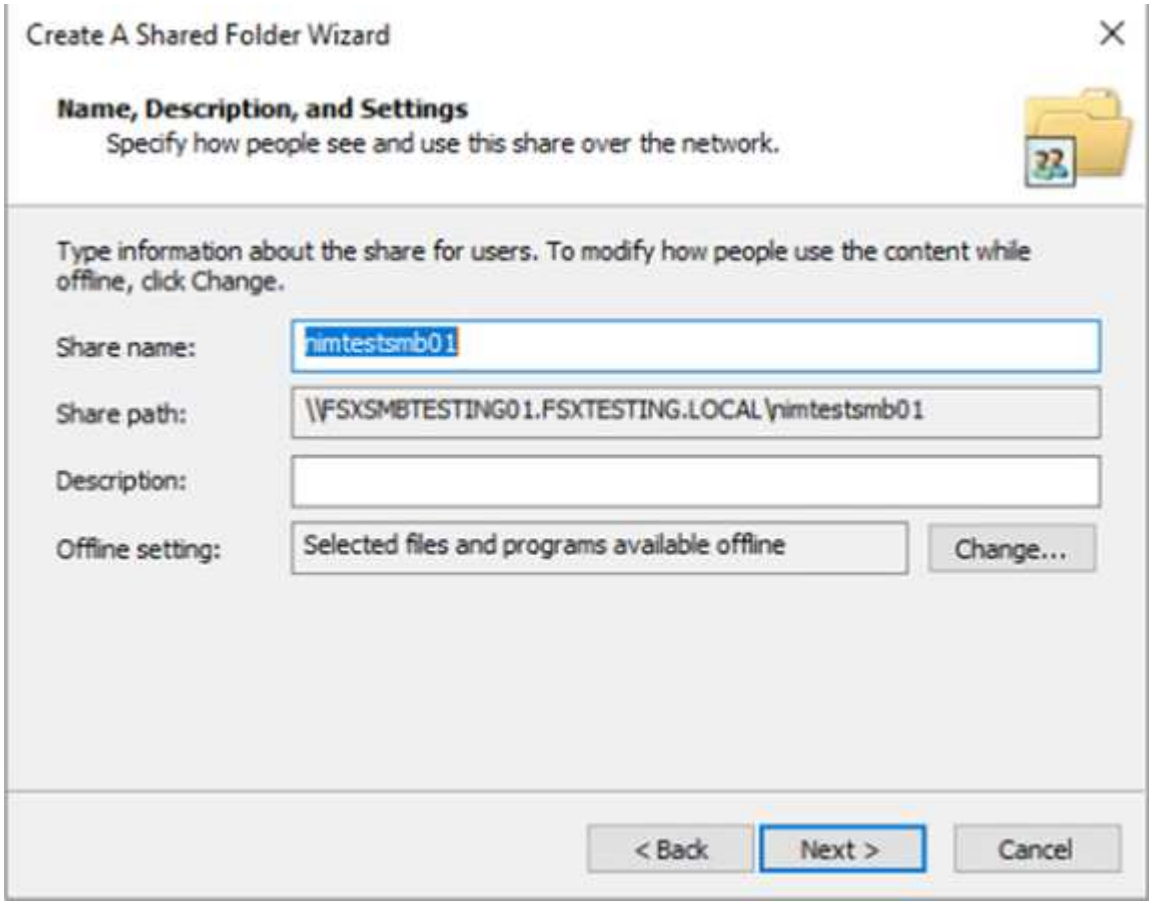
TP が Amazon FSX コンソールで SVM の DNS 名を検索し、 Storage Virtual Machines を選択してから、 endpoints までスクロールして SMB DNS 名を検索します。[OK] をクリックします。共有フォルダのリストに Amazon FSX ファイルシステムが表示されます。



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

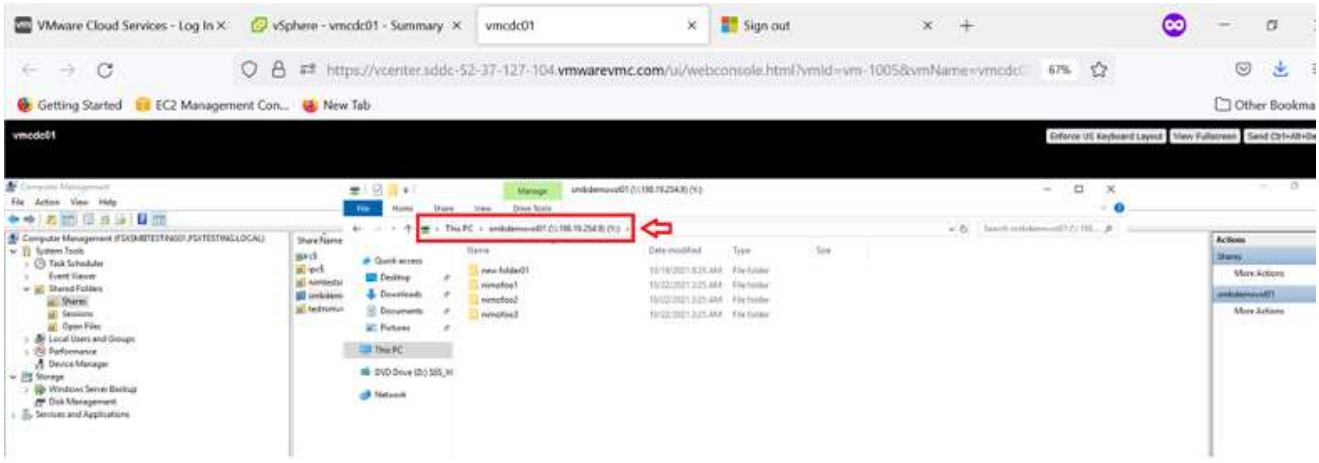


1. 新しい共有を選択し、共有フォルダの作成ウィザードを完了します。



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

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



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

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

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

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

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

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

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

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

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

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

FsxId040eacc5d0ac31017::> igroup show

Vserver   Igroup       Protocol OS Type  Initiators

--------- ------------ -------- --------
------------------------------------

vmcfsxval2svm

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

vmcfsxval2svm

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

2 つのエントリが表示されました。

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

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

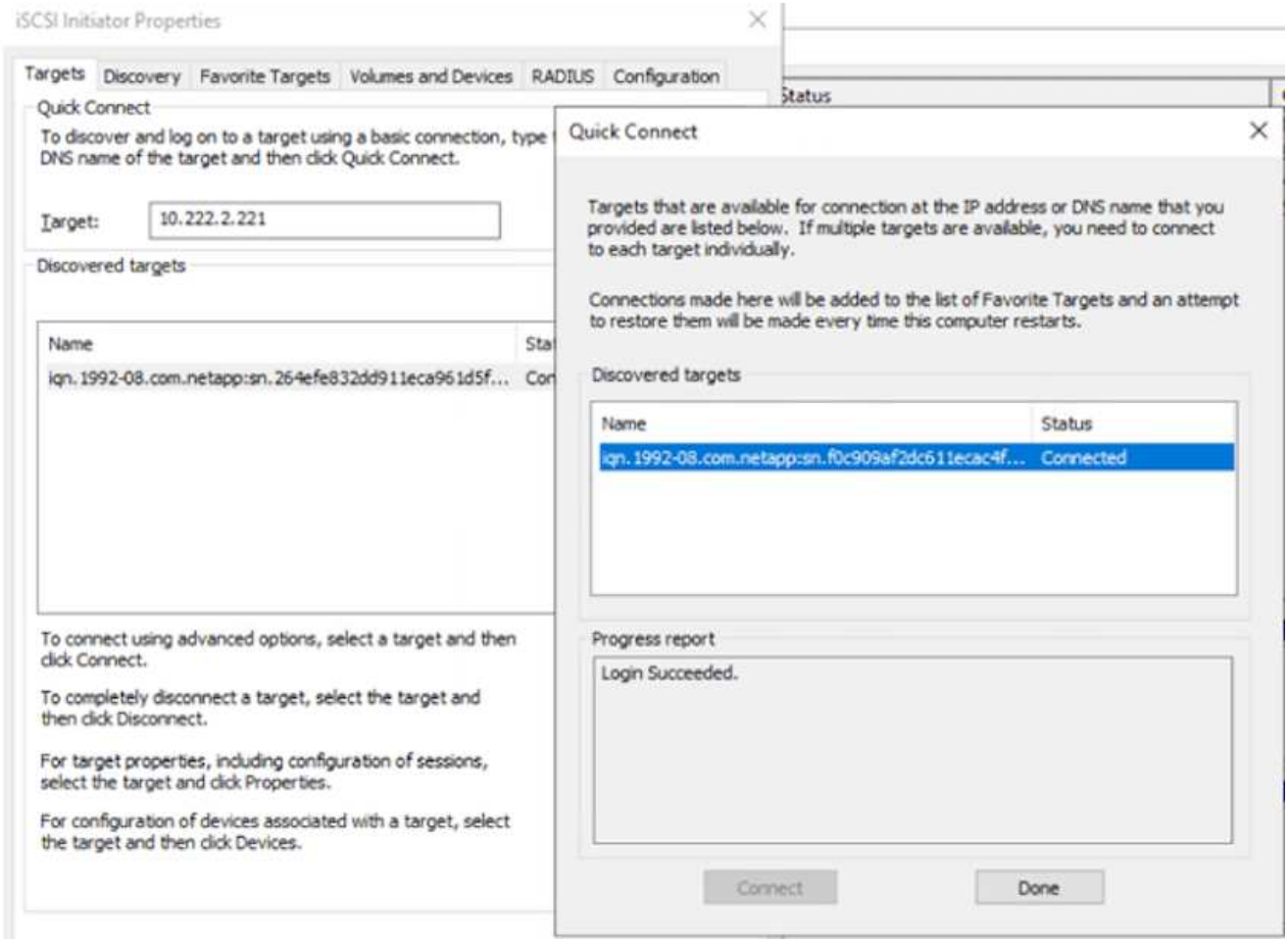
2 つのエントリが表示されました。

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

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

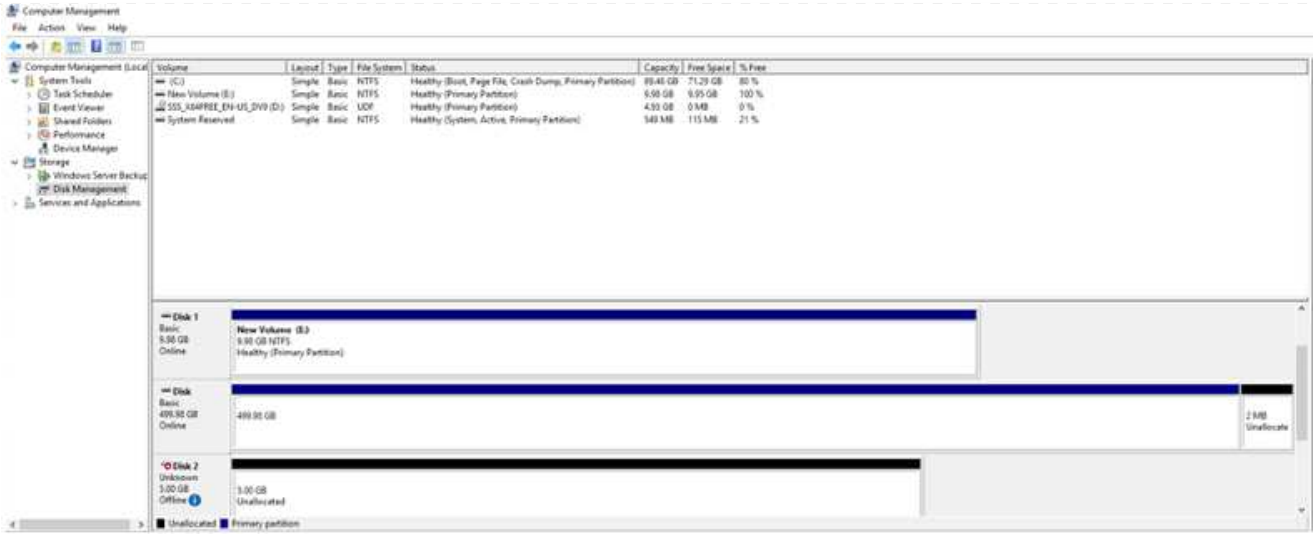
1. AWS SDDC 上の VMware Cloud でホストされる Windows VM への RDP
2. サーバーマネージャ > ダッシュボード > ツール > iSCSI イニシエータと進み、 iSCSI イニシエータのプロパティダイアログボックスを開きます。
3. Discovery （検出）タブで、 Discover Portal （ポータルの検出）または Add Portal （ポータルの追加）をクリックし、 iSCSI ターゲットポートの IP アドレスを入力します。
4. ターゲットタブで検出されたターゲットを選択し、ログオンまたは接続をクリックします。
5. [マルチパス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

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



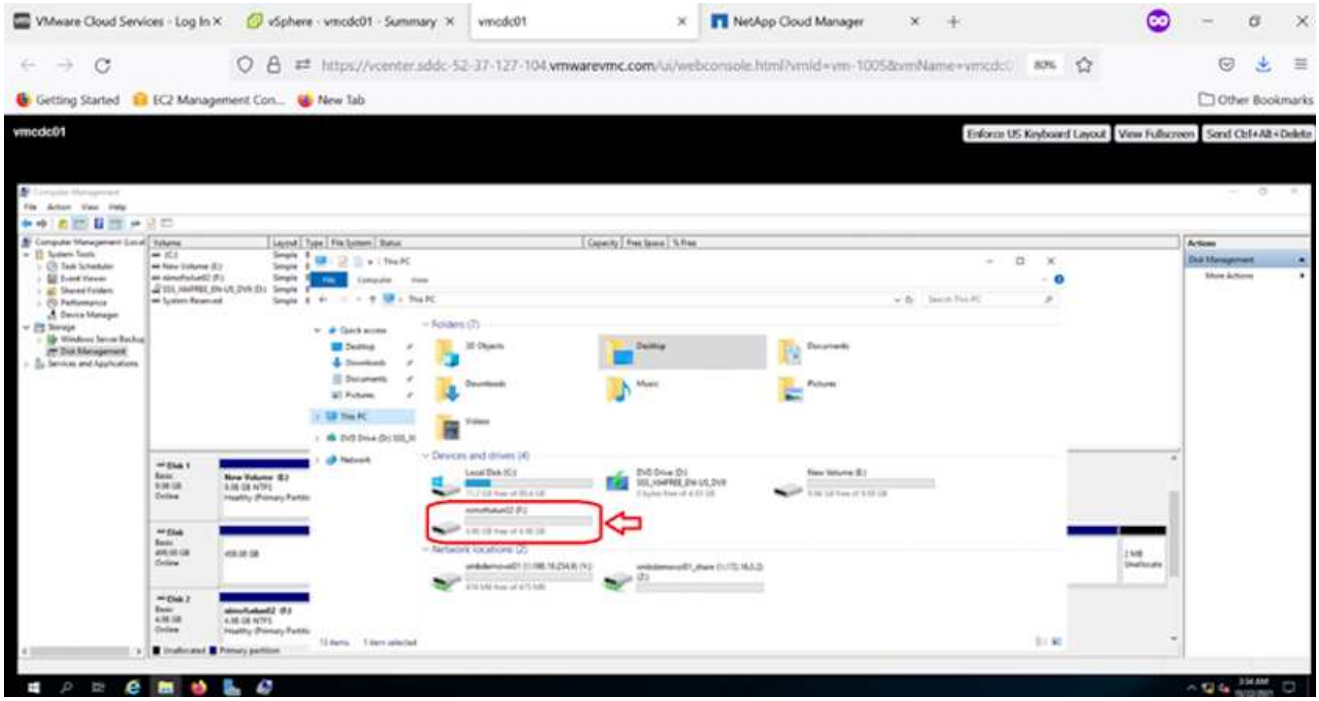
Storage Virtual Machine （ SVM ）の LUN は、 Windows ホストではディスクとして表示されます。追加した新しいディスクは、ホストでは自動的に検出されません。手動の再スキャンをトリガーしてディスクを検出するには、次の手順を実行します。

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



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

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



Cloud Volumes ONTAP （CVO）

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

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

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

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

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

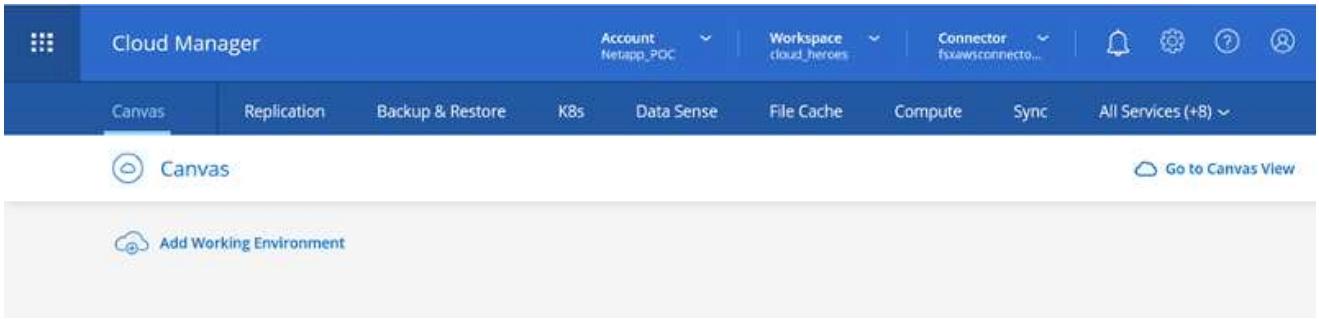
AWS に新しい Cloud Volumes ONTAP インスタンスを導入（自分で実行）

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

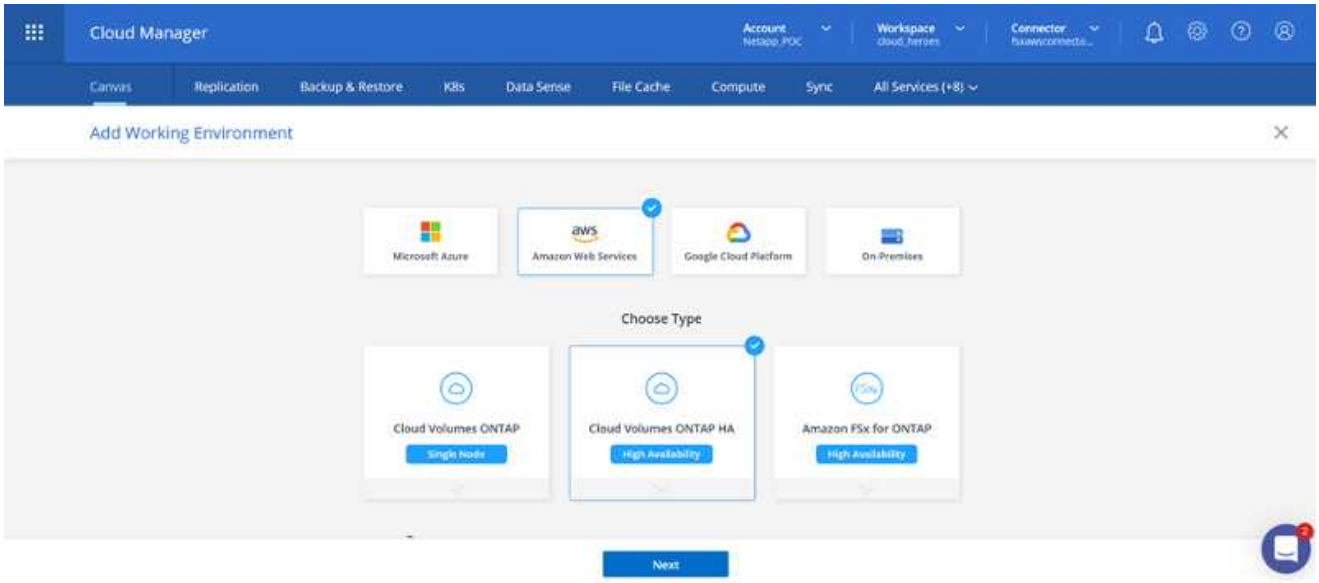
ディザスタリカバリや移行の目的でオンプレミス環境からクラウドにボリュームをレプリケートするには、サイト間 VPN または DirectConnect を使用して、 AWS へのネットワーク接続を確立します。オンプレミスから Cloud Volumes ONTAP へのデータのレプリケートについては、本ドキュメントでは扱いません。オンプレミスシステムと Cloud Volumes ONTAP システム間でデータをレプリケートする方法については、を参照してください "システム間のデータレプリケーションの設定"。

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

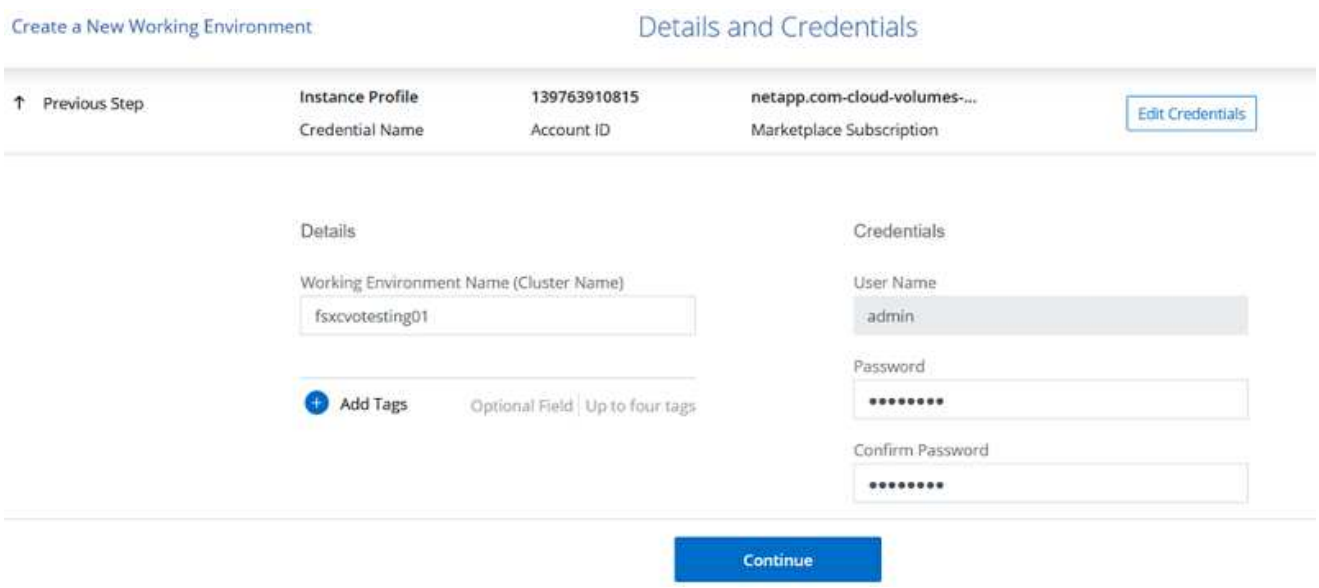
1. NetApp Cloud Central にログインします。 Fabric View 画面が表示されます。Cloud Volumes ONTAP タブを探し、 Go to Cloud Manager を選択します。ログインすると、キャンバス画面が表示されます。



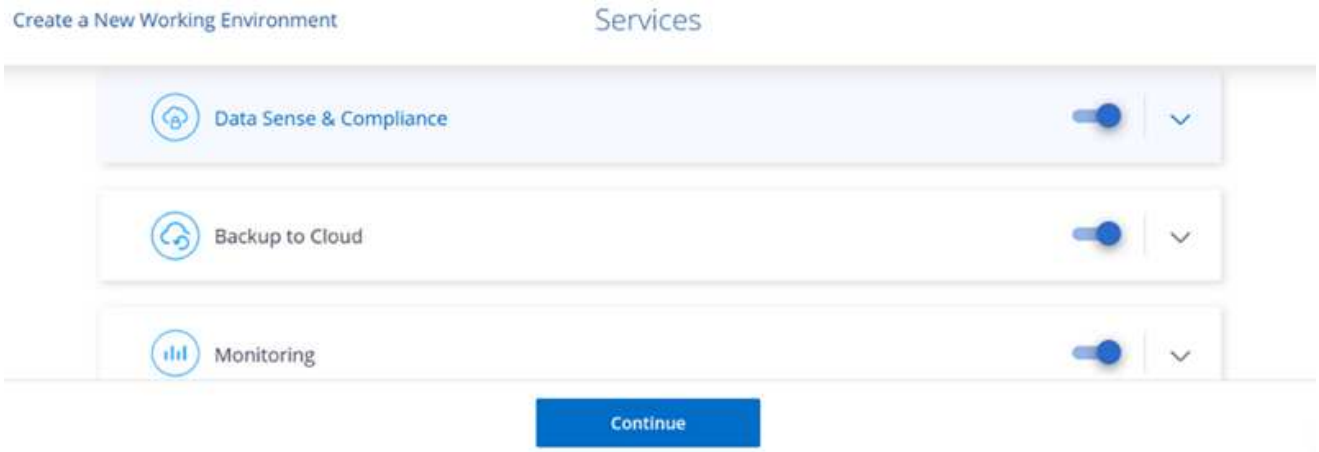
1. Cloud Manager のホームページで、 Add a Working Environment をクリックし、 AWS をクラウドとして選択し、システム構成のタイプを選択します。



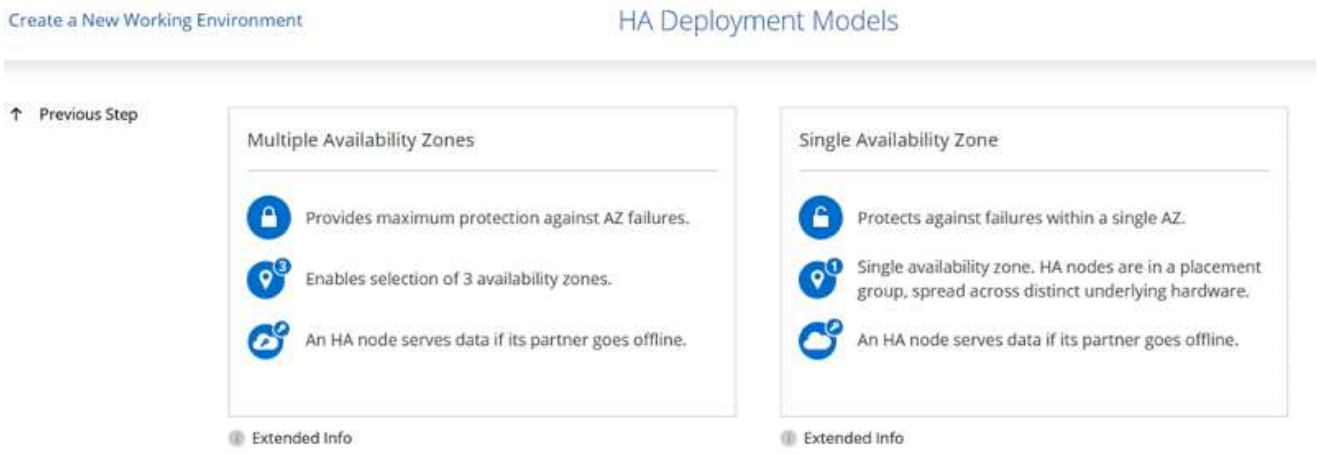
1. 環境名と admin クレデンシャルなど、作成する環境の詳細を指定します。Continue をクリックします。 .



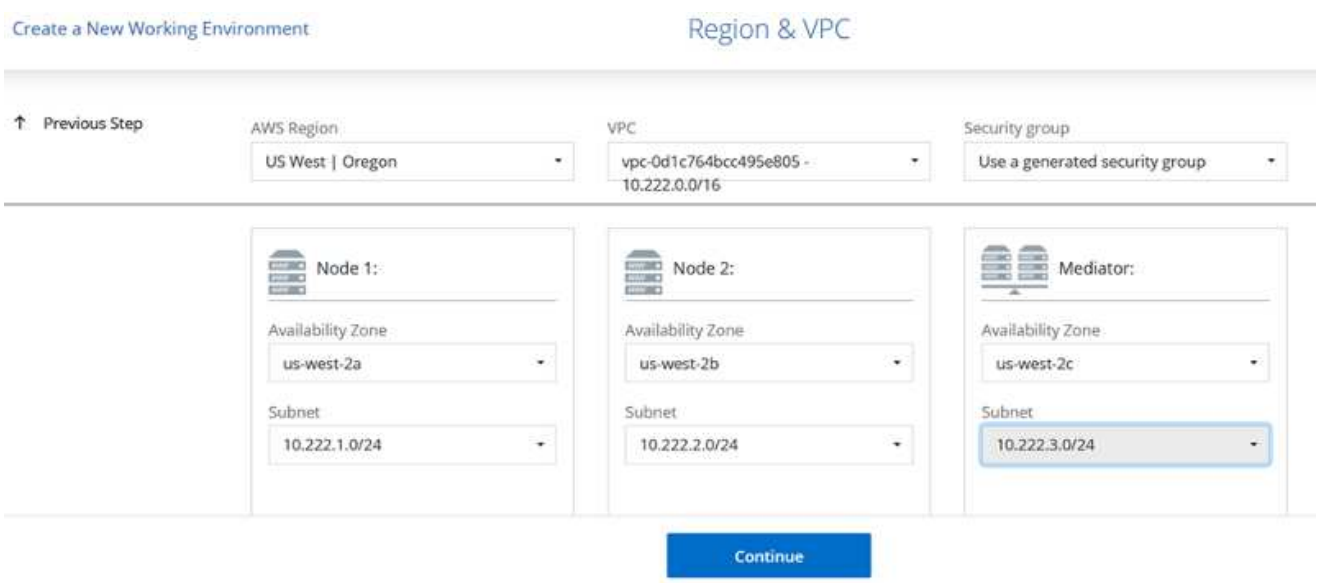
1. Cloud Volumes ONTAPの導入に使用するアドオンサービス（BlueXPの分類、BlueXPのバックアップとリカバリ、Cloud Insightsなど）を選択します。Continue をクリックします。 .



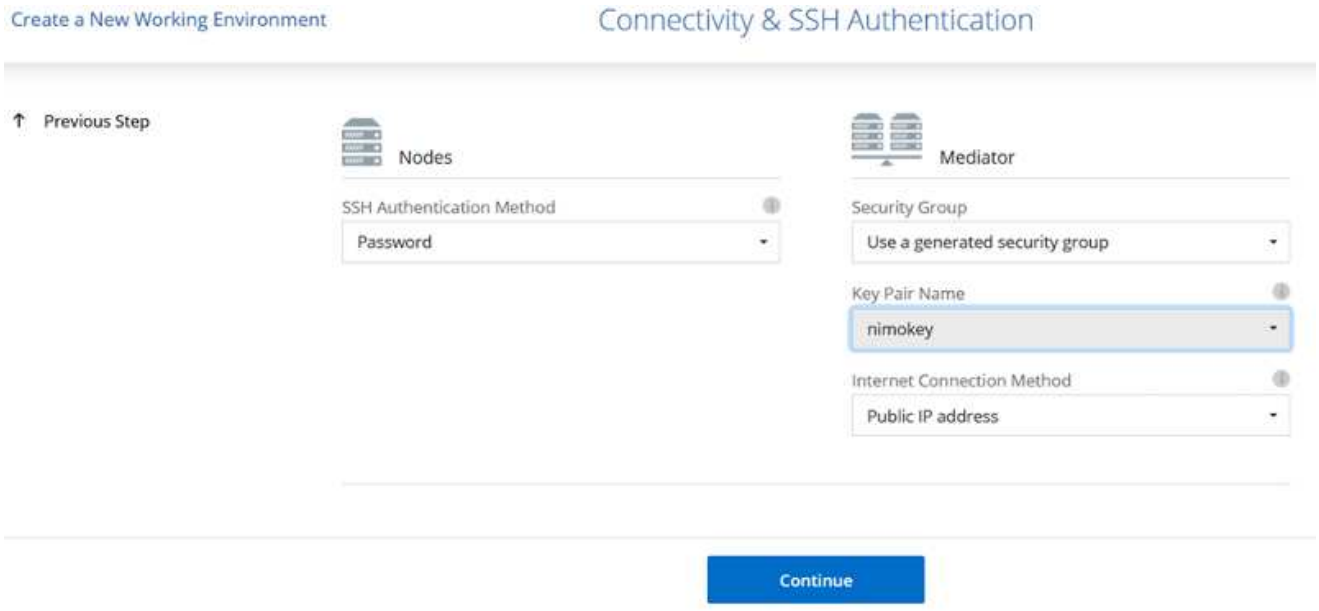
1. HA Deployment Models ページで、 Multiple Availability Zones 設定を選択します。



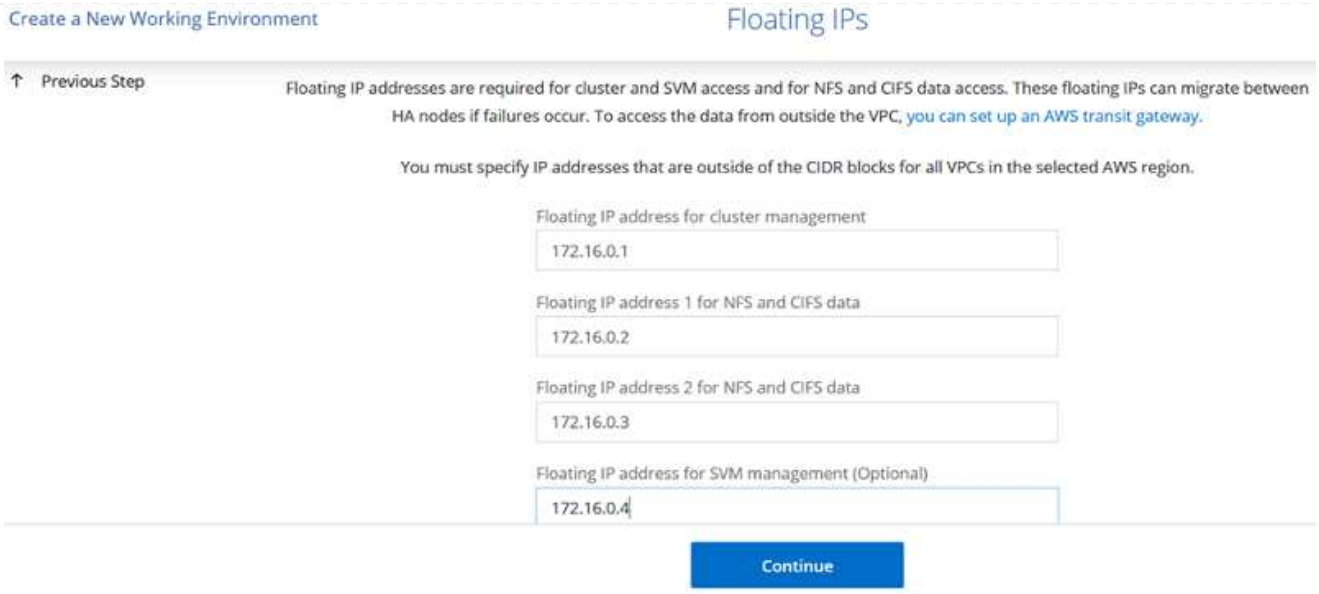
1. Region & VPC ページで、ネットワーク情報を入力し、 Continue をクリックします。



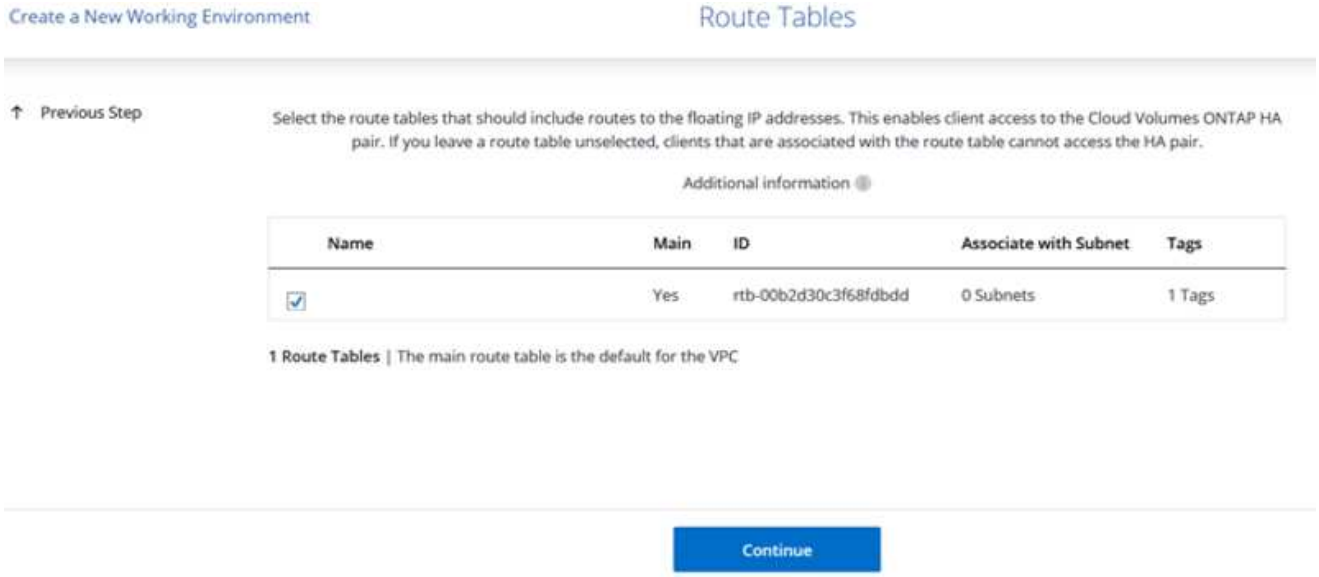
1. [Connectivity and SSH Authentication] ページで、 HA ペアとメディエータの接続方法を選択します。



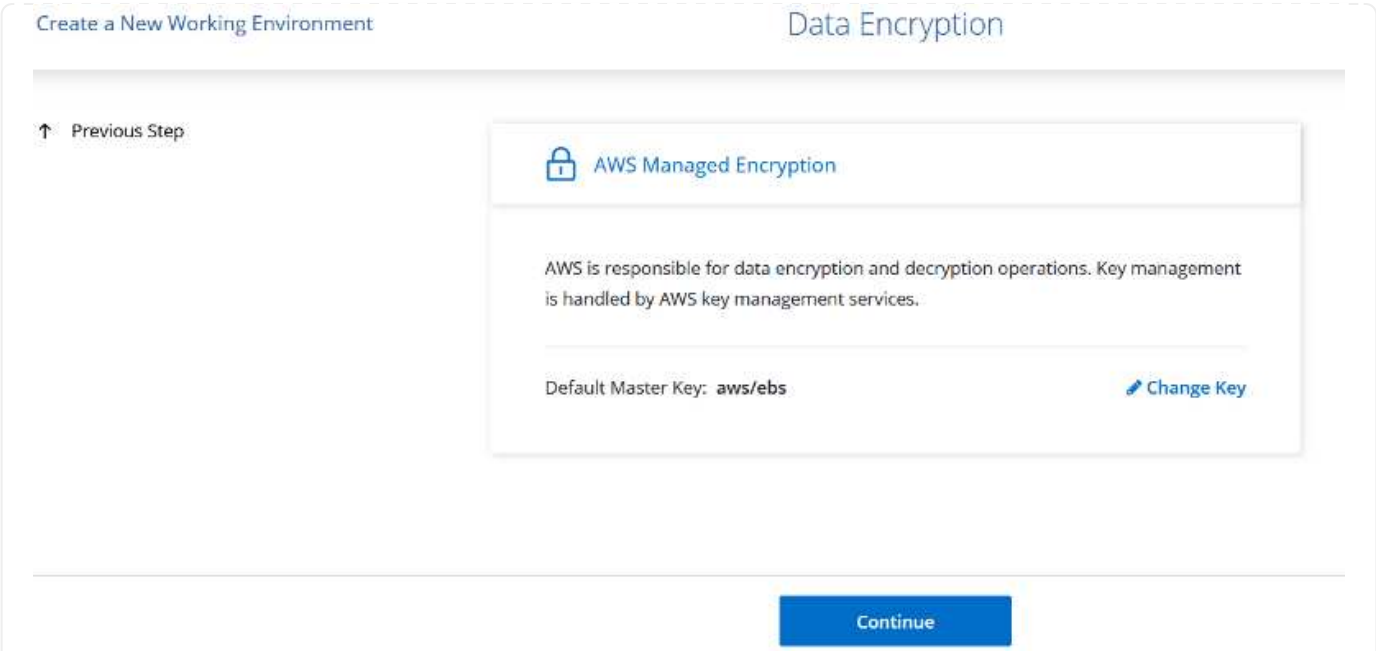
1. フローティング IP アドレスを指定し、 Continue （続行）をクリックします。



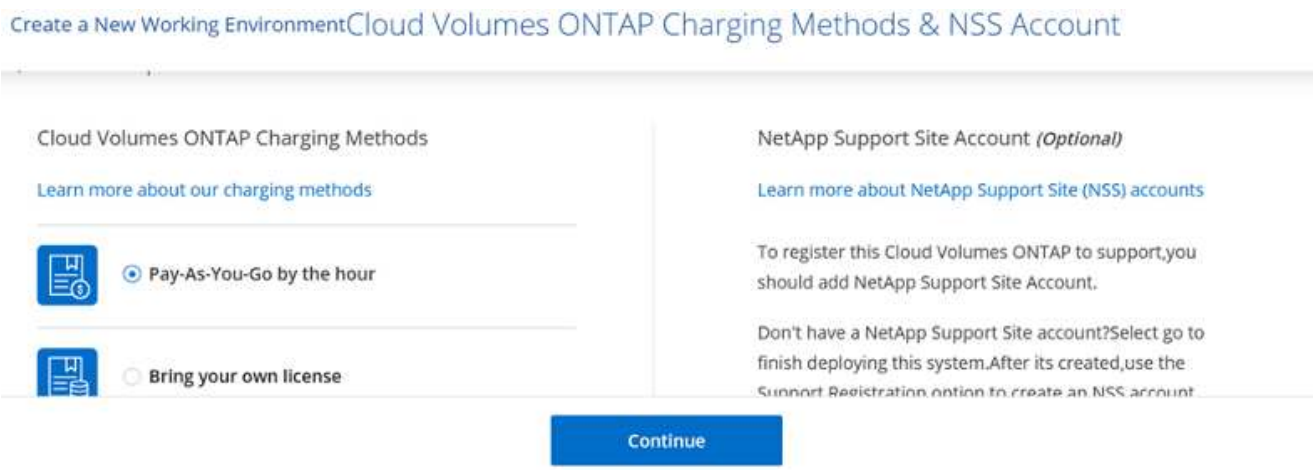
1. フローティング IP アドレスへのルートを含める適切なルーティングテーブルを選択し、 Continue （続行）をクリックします。



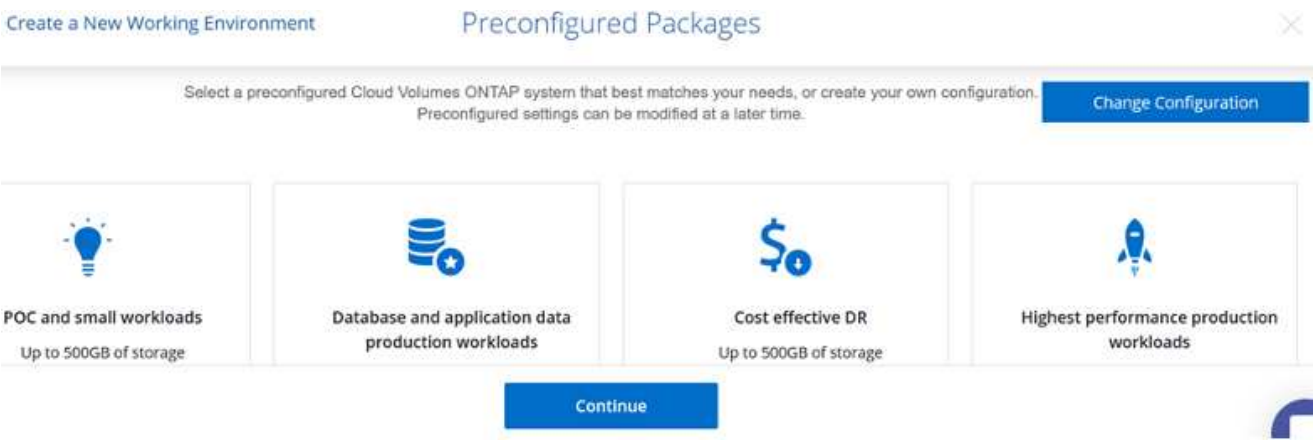
1. Data Encryption ページで、 AWS で管理する暗号化を選択します。



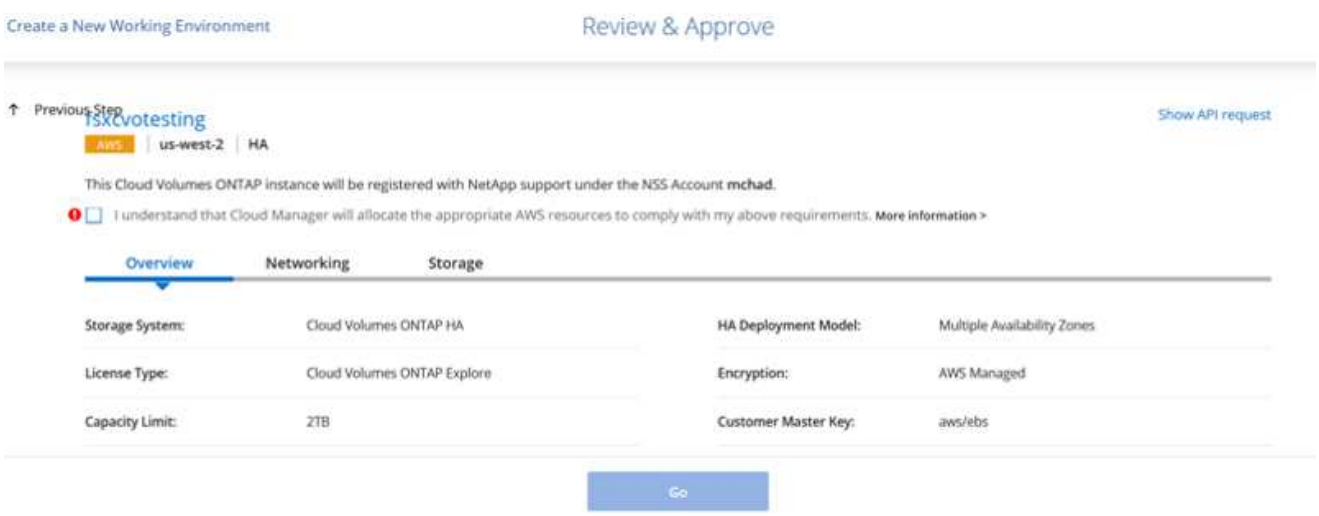
1. ライセンスオプションとして、「従量課金制」または「 BYOL for using an existing license 」を選択します。この例では、 ［ 従量課金制 ］ オプションを使用します。



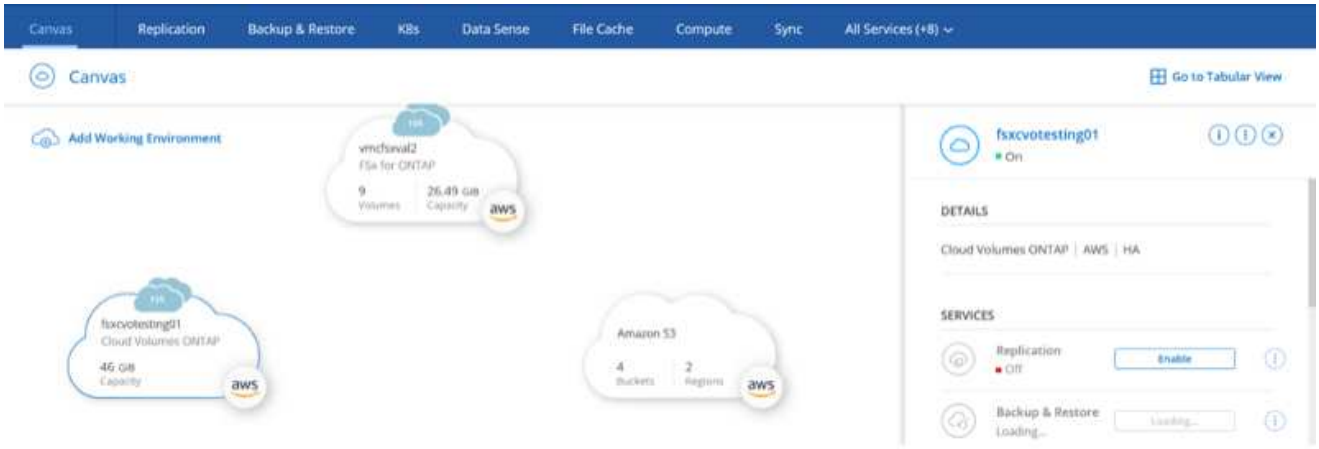
1. AWS SDDC 上の VMware クラウドで実行されている VM に導入するワークロードのタイプに基づいて、複数の事前設定パッケージから選択できます。



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

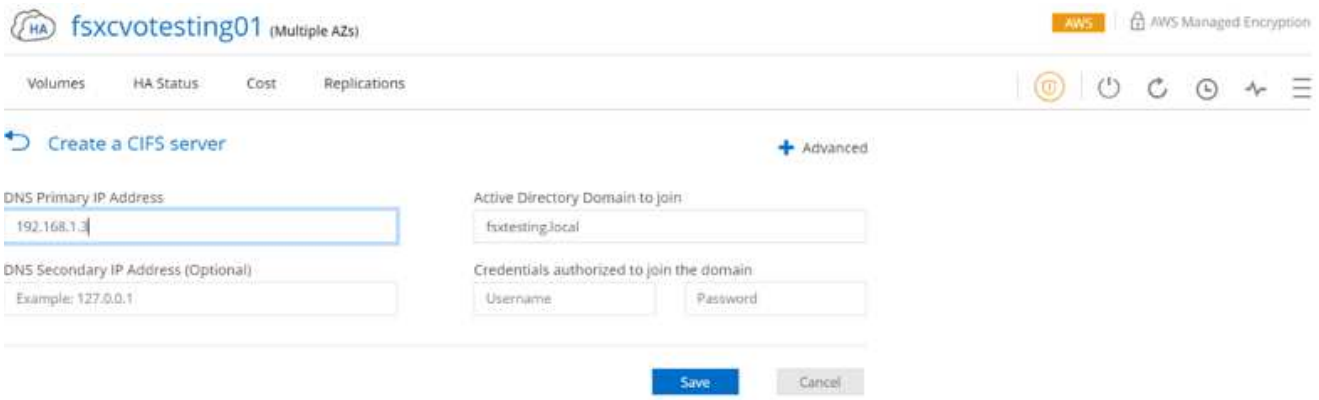


1. Cloud Volumes ONTAP のプロビジョニングが完了すると、 [Canvas] ページの作業環境に表示されます。

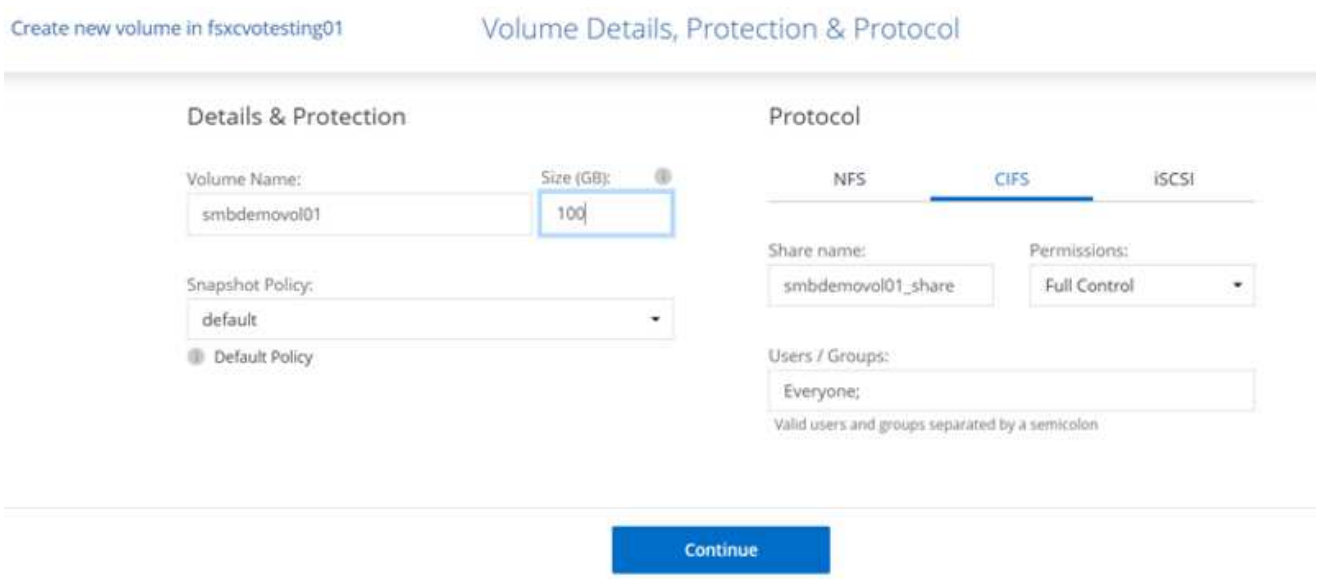


SMB ボリューム用の追加の設定

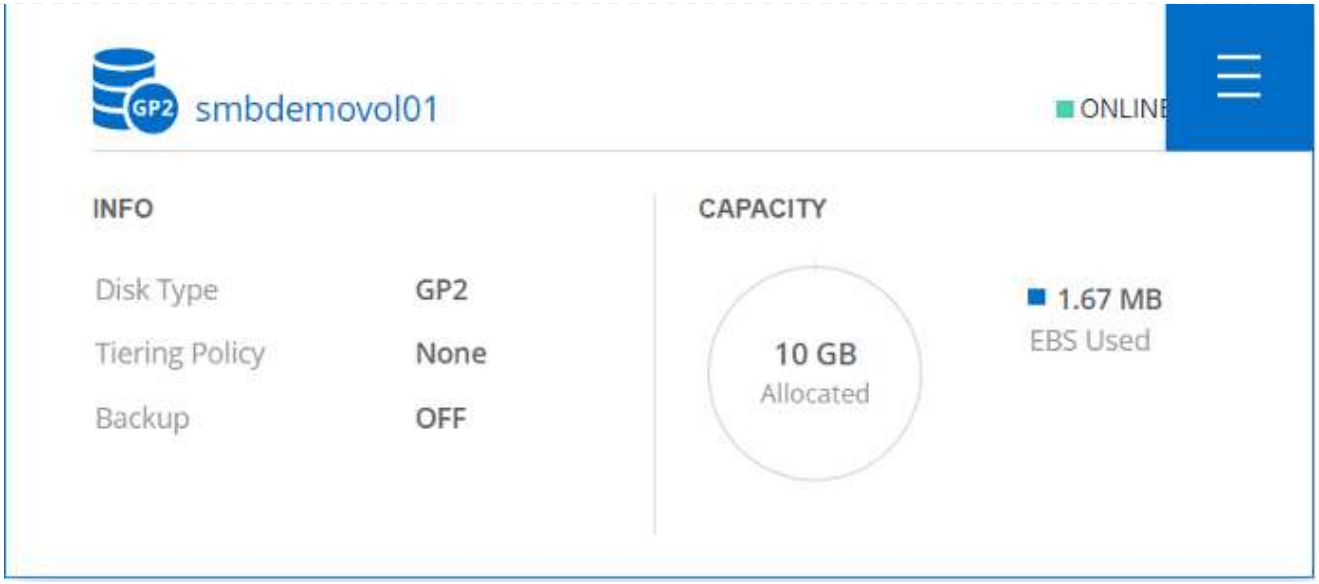
1. 作業環境の準備ができたら、 CIFS サーバに適切な DNS および Active Directory 設定パラメータが設定されていることを確認します。この手順は、 SMB ボリュームを作成する前に実行する必要があります。



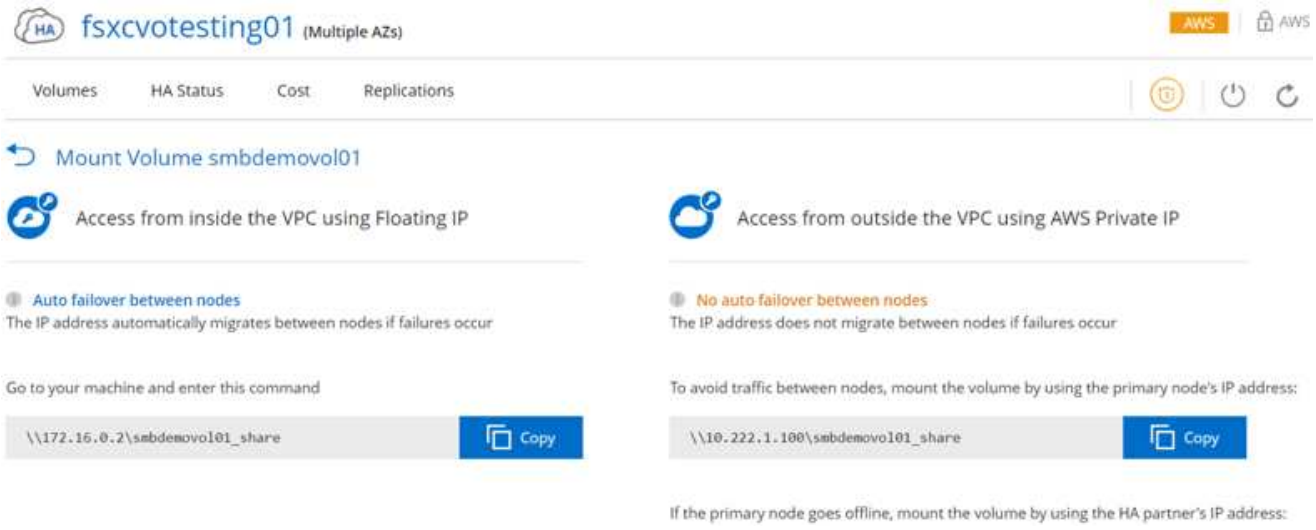
1. CVO インスタンスを選択してボリュームを作成し、 Create Volume （ボリュームの作成）オプションをクリックします。適切なサイズを選択し、包含アグリゲートを選択するか、高度な割り当てメカニズムを使用して特定のアグリゲートに配置します。このデモでは、 SMB がプロトコルとして選択されます。

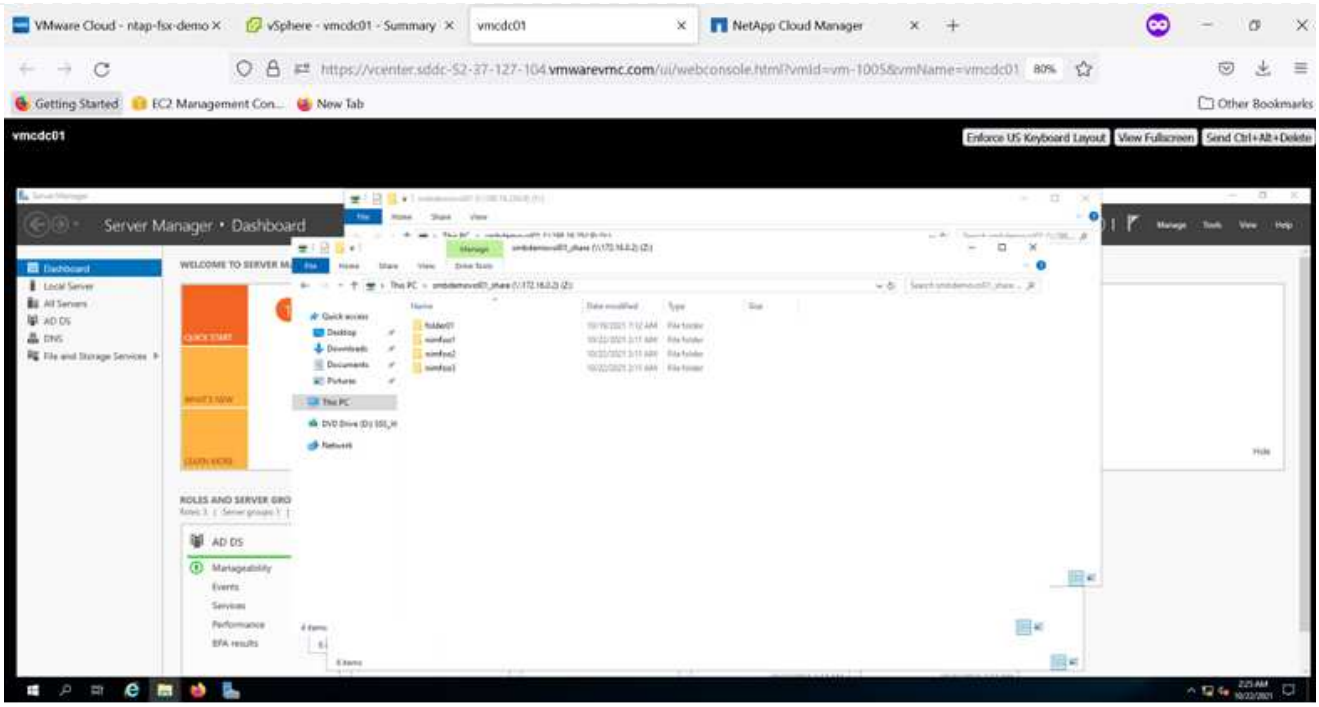


1. ボリュームのプロビジョニングが完了すると、 Volumes （ボリューム）ペインにボリュームが表示されます。CIFS 共有はプロビジョニングされるため、ユーザまたはグループにファイルおよびフォルダに対する権限を付与し、ユーザが共有にアクセスしてファイルを作成できることを確認する必要があります。



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

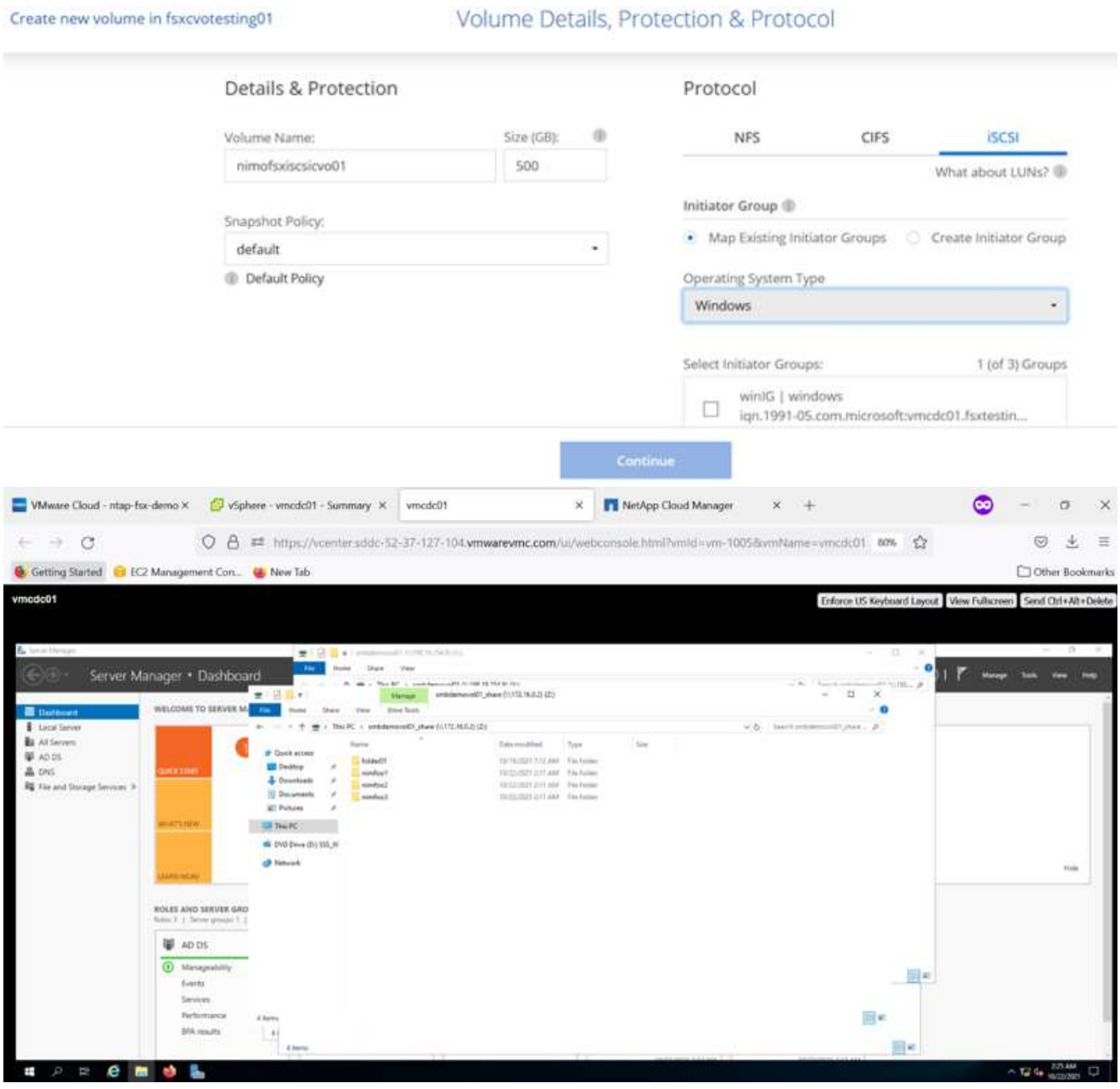



VMware Cloud - ntap-fsx-demo
vSphere - vmcdc01 - Summary
vmcdc01
NetApp Cloud Manager
https://vcenter.sddc-52-37-127-104.vmwarevmc.com/ui/webconsole.html?vmId=vm-1005&vmName=vmcdc01
Getting Started
EC2 Management Con...
New Tab
Other Bookmarks
vmcdc01
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Server Manager • Dashboard

LUN をホストに接続します

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

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



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

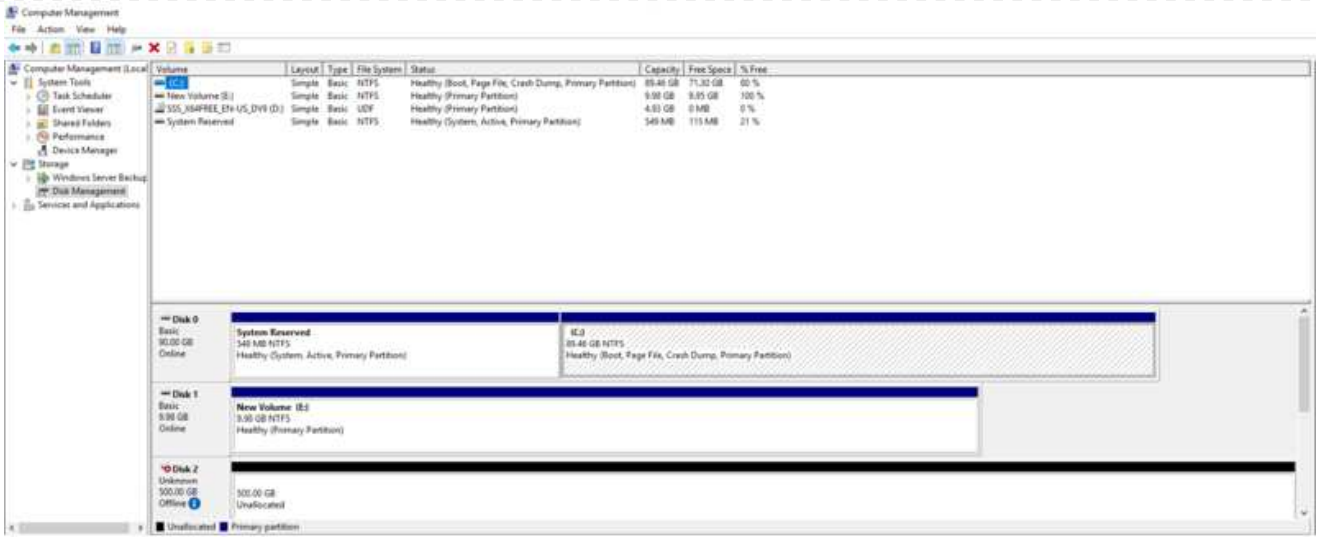
AWS SDDC 上の VMware Cloud にあるホストでも同じ処理を実行するには、次の手順を実行します。

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

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

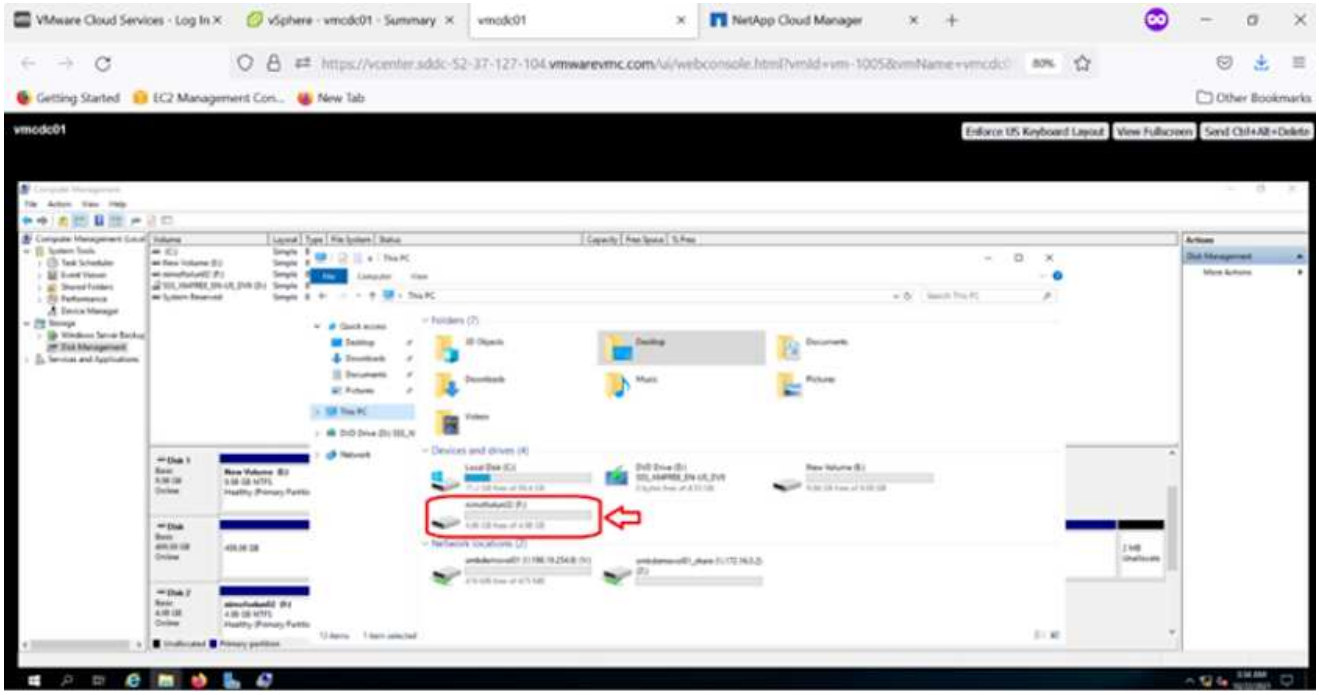
SVM の LUN は、 Windows ホストではディスクとして表示されます。追加した新しいディスクは、ホストでは自動的に検出されません。手動の再スキャンをトリガーしてディスクを検出するには、次の手順を実行します。

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



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

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



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

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

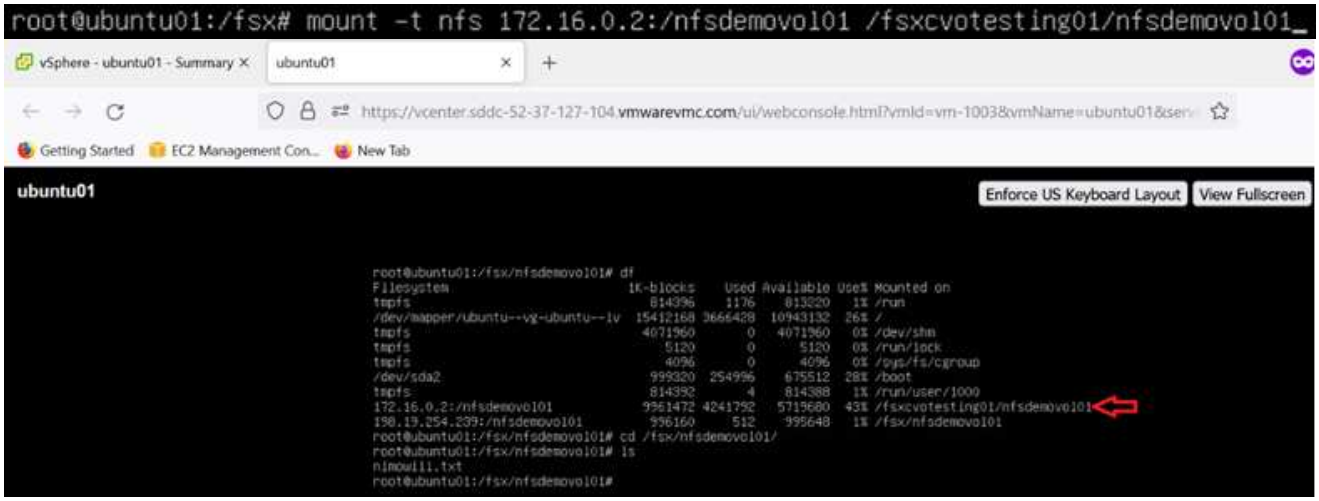
Cloud Volumes ONTAP （ DIY ）ファイルシステムを VMC 内の VM から AWS SDDC にマウントするには、次の手順を実行します。

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

```
 $ sudo mkdir /fsxcvotesting01/nfsdemovol01
```

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

```
sudo mount -t nfs nfsvers=4.1,172.16.0.2:/nfsdemovol01
/fsxcvotesting01/nfsdemovol01
```



ANFデータストアソリューションの概要

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

ます。

ユースケース

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

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

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

つまり、ユースケースは次の2つの方法で分類できます。

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

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

Azureの**VMware Cloud**オプション

Azure VMware 解決策の略

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

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

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

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

まとめ

Azure NetApp Files は、オールクラウドとハイブリッドクラウドのどちらをターゲットとしている場合でも、アプリケーションワークロードとファイルサービスを導入して管理するための優れたオプションを提供し、データ要件をアプリケーションレイヤとシームレスにすることでTCOを削減します。どのようなユースケースでも、クラウドのメリット、一貫したインフラ、オンプレミスと複数のクラウドにわたる運用、ワークロードの双方向性、エンタープライズクラスの容量とパフォーマンスを迅速に実現するには、Azure VMware解決策とAzure NetApp Files を選択してください。ストレージの接続に使用される一般的なプロセスと手順は同じです。新しい名前とともに変更されたデータの位置にすぎません。ツールやプロセスはすべて変わらないので、Azure NetApp Files を使用すると導入全体を最適化できます。

重要なポイント

本ドキュメントの主な内容は次のとおりです。

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

追加情報の参照先

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

- Azure VMware解決策 のドキュメント

  "https://docs.microsoft.com/en-us/azure/azure-vmware/"

- Azure NetApp Files のドキュメント

  "https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

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

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

Azure 向けネットアップゲスト接続ストレージオプション

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

Azure NetApp ファイル（ ANF ）

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

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

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

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

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

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

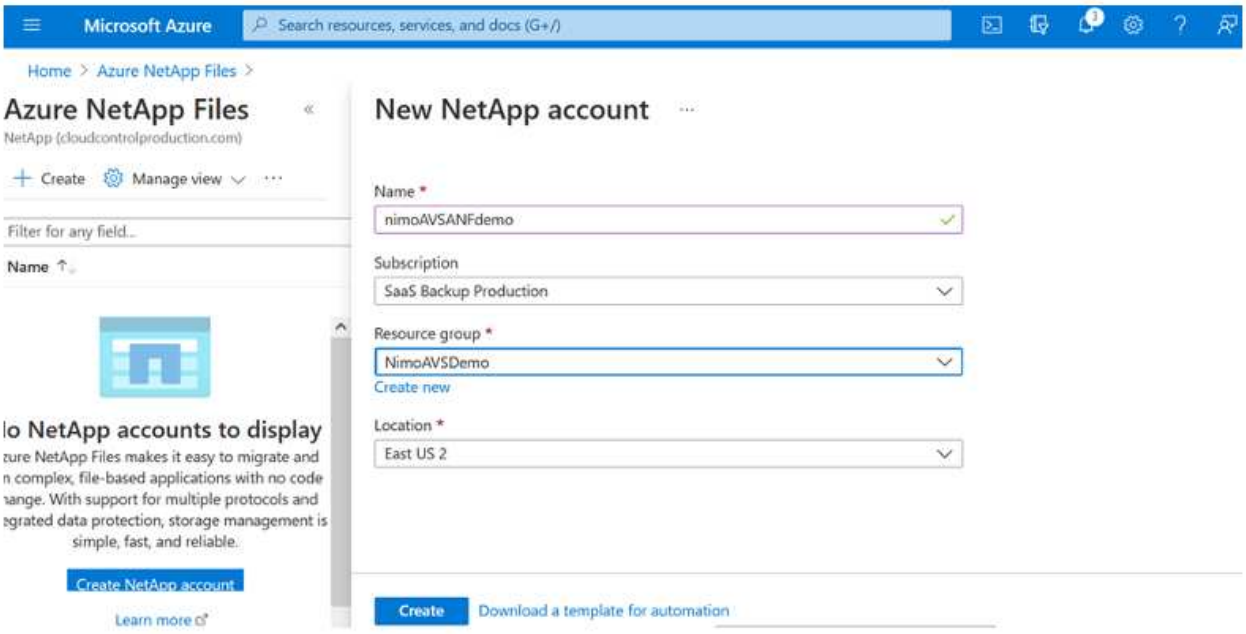
Azure NetApp Files と Azure VMware 解決策は、同じ Azure リージョンに配置する必要があります。

Azure NetApp Files ボリュームを作成してマウント

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

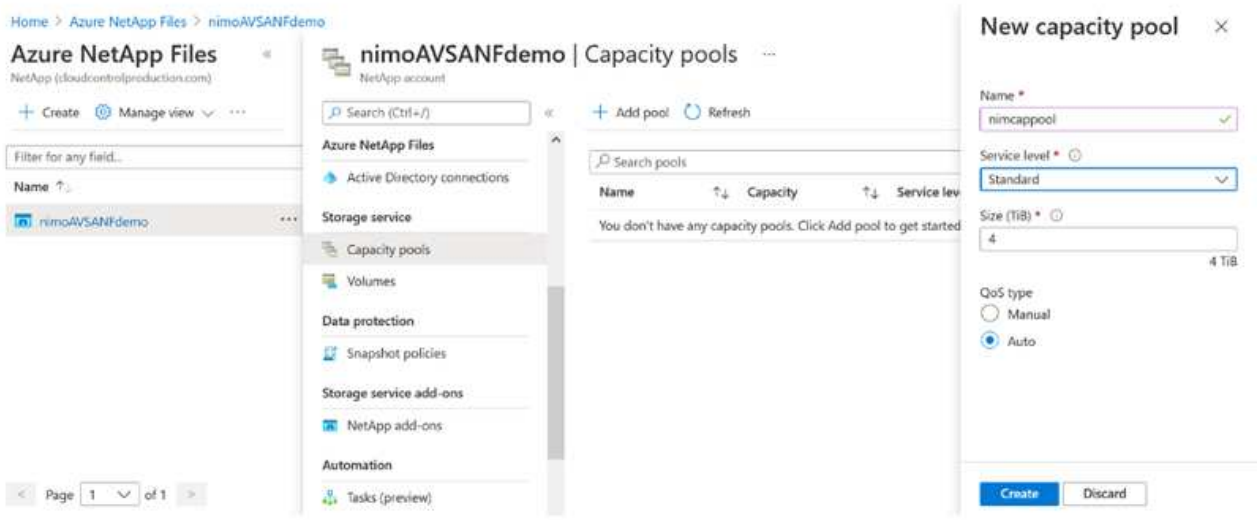
1. Azure ポータルにログインし、 Azure NetApp Files にアクセスします。Azure NetApp Files サービスへのアクセスを確認し、 Azure NetApp Files リソースプロバイダを登録するには、 _az プロバイダ登録 — namespace Microsoft.NetApp – wait_command を使用します。登録が完了したら、ネットアップアカウントを作成します。

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

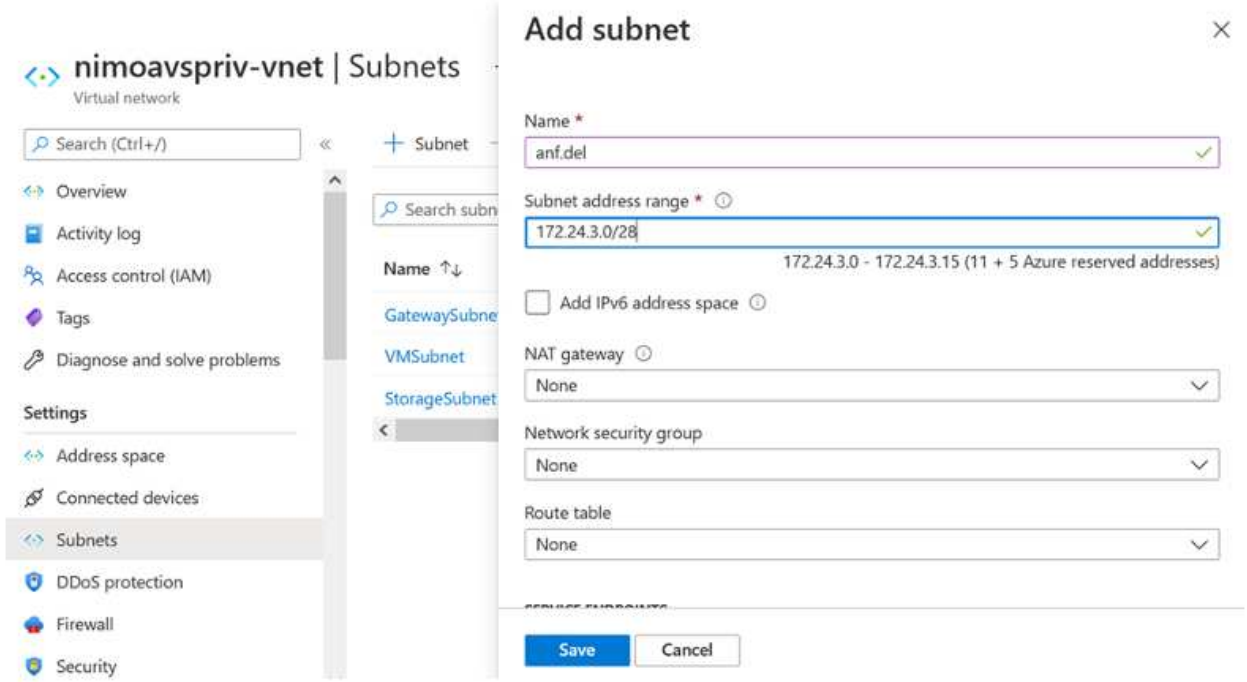


2. ネットアップアカウントが作成されたら、必要なサービスレベルとサイズの容量プールを設定します。

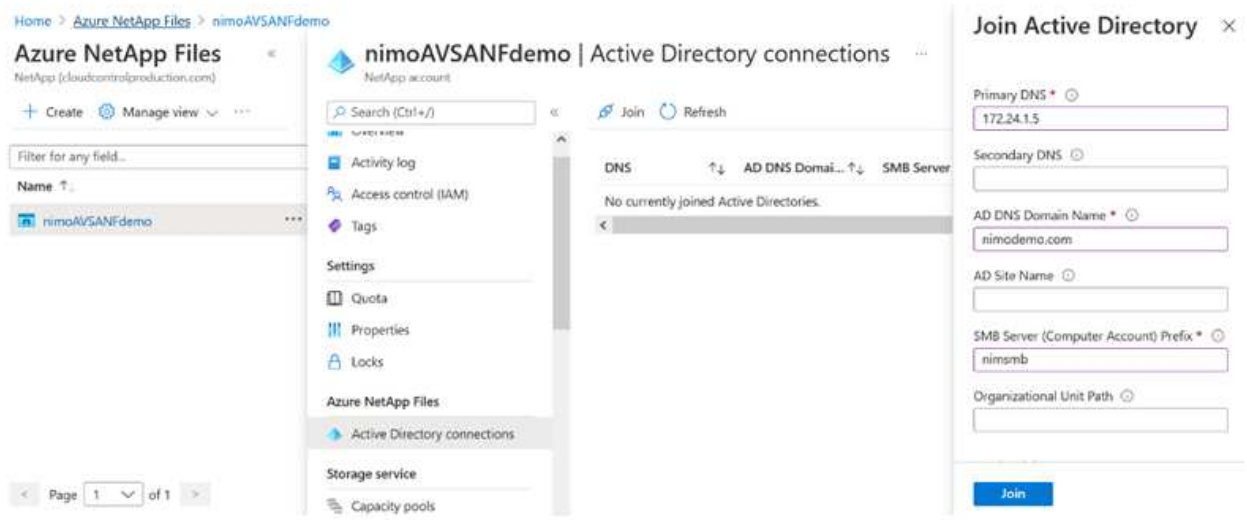
   詳細については、を参照してください "容量プールをセットアップする"。



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

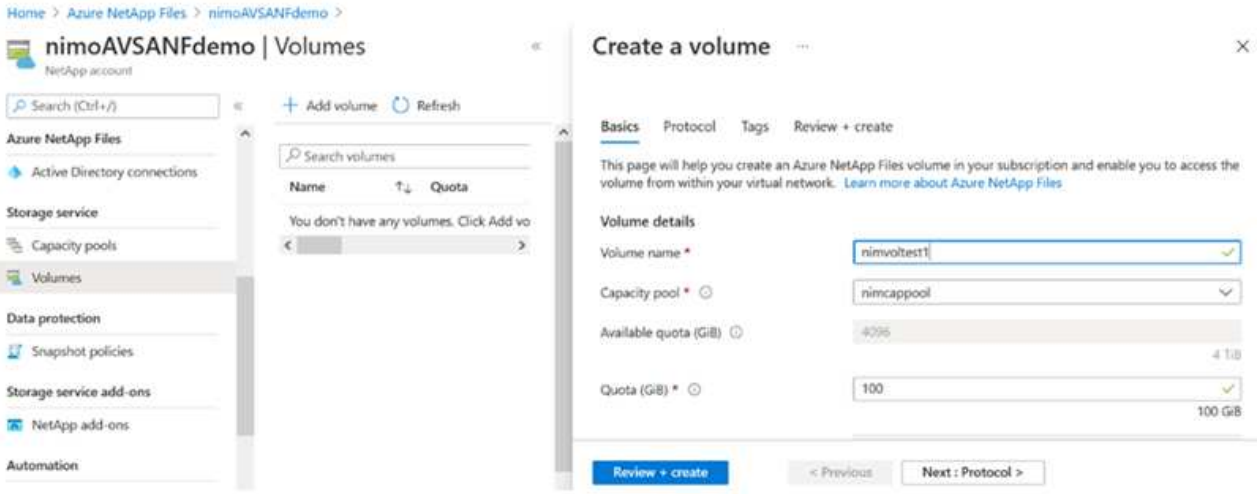


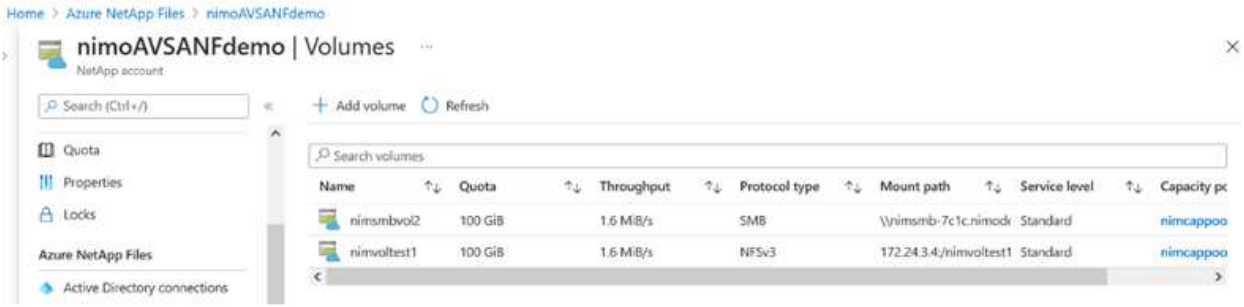
4. 容量プールブレードの下のボリュームブレードを使用して、 SMB ボリュームを追加します。SMB ボリュームを作成する前に、 Active Directory Connector が設定されていることを確認してください。



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

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

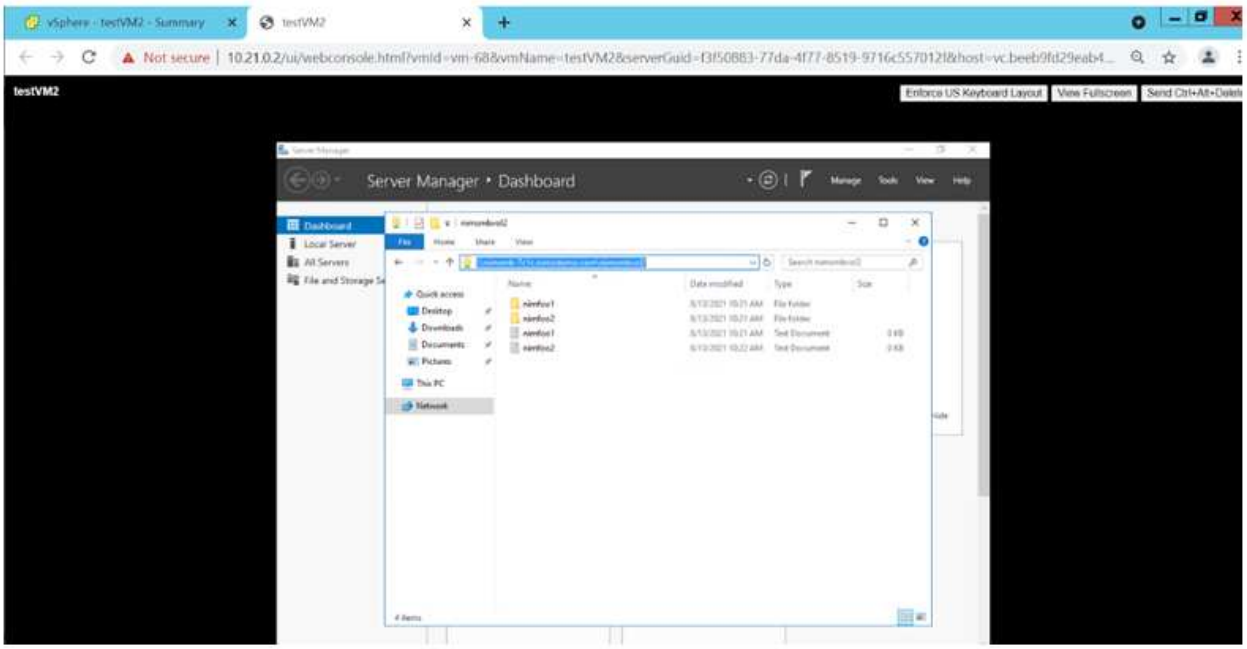


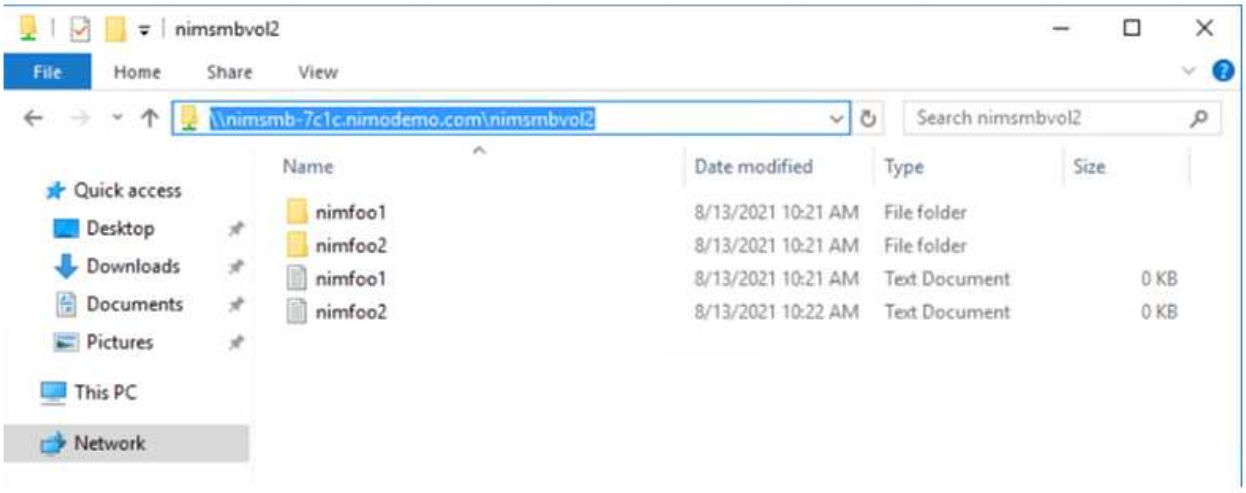


サイズまたはクォータ別の Azure NetApp Files ボリュームのパフォーマンスの詳細については、を参照してください "Azure NetApp Files のパフォーマンスに関する考慮事項"。

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

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





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

```
nimoadmin@nimoadmin-virtual-machine:~$ sudo mount -t nfs -o rw,hard,tcp 172.24.
3.4:/nimodemonfsv1 /home/nimoadmin/nimodemo11
nimoadmin@nimoadmin-virtual-machine:~$ df
Filesystem                  1K-blocks     Used Available Use% Mounted on
udev                          8168112        0   8168112   0% /dev
tmpfs                         1639548     1488   1638060   1% /run
/dev/sda5                    50824704  7902752  40310496  17% /
tmpfs                         8197728        0   8197728   0% /dev/shm
tmpfs                            5120        0      5120   0% /run/lock
tmpfs                         8197728        0   8197728   0% /sys/fs/cgroup
/dev/loop0                      56832    56832         0 100% /snap/core18/2128
/dev/loop2                      66688    66688         0 100% /snap/gtk-common-the
mes/1515
/dev/loop1                     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/VMw
are Tools
172.24.3.4:/nimodemonfsv1 104857600        0 104857600   0% /home/nimoadmin/nimo
demo11
nimoadmin@nimoadmin-virtual-machine:~$
```

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

Cloud Volumes ONTAP （CVO）

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

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

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

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

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

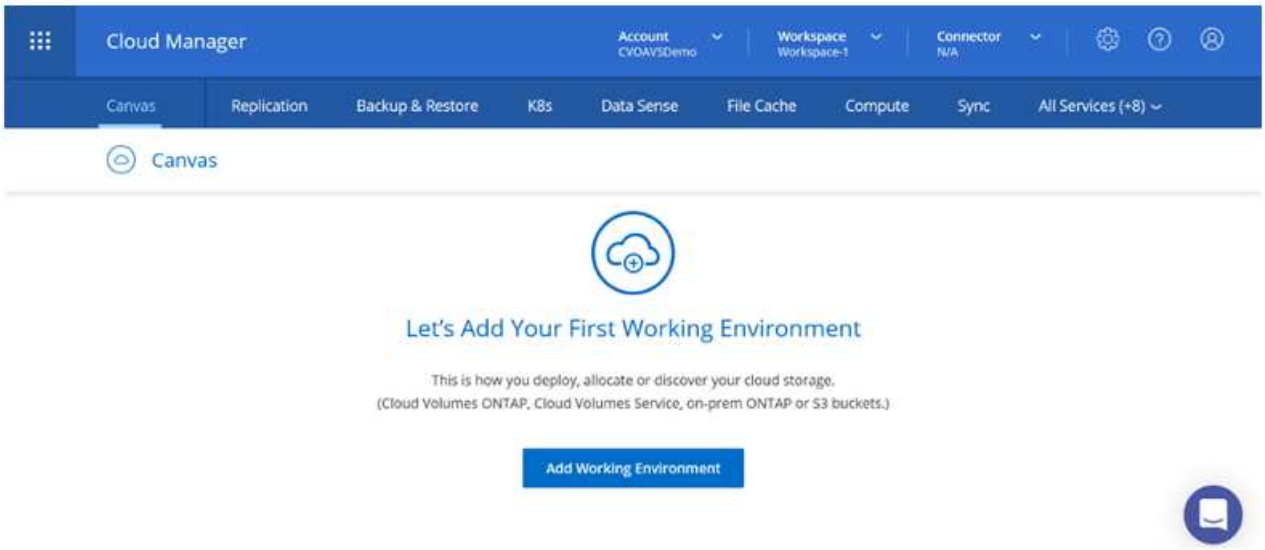
Cloud Volumes ONTAP （ CVO ）をゲスト接続ストレージとして活用

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

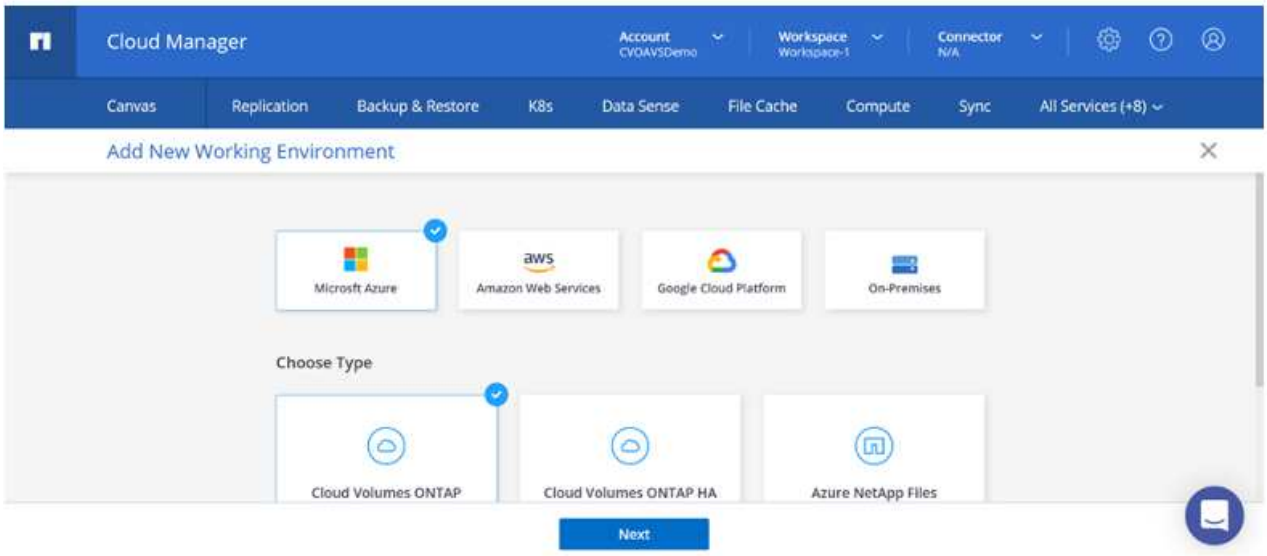
ディザスタリカバリや移行の目的でオンプレミス環境からクラウドにボリュームをレプリケートするには、サイト間 VPN または ExpressRoute を使用して、 Azure へのネットワーク接続を確立します。オンプレミスから Cloud Volumes ONTAP へのデータのレプリケートについては、本ドキュメントでは扱いません。オンプレミスシステムと Cloud Volumes ONTAP システム間でデータをレプリケートする方法については、を参照してください "システム間のデータレプリケーションの設定"。

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

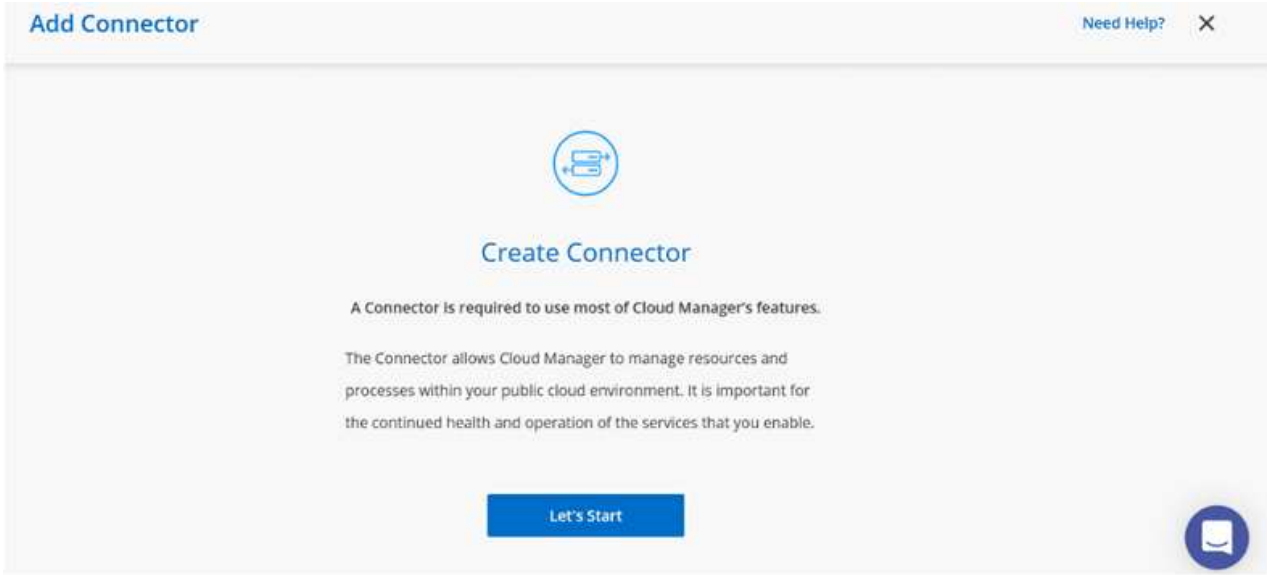
1. NetApp Cloud Central にログイン— Fabric View （ファブリックビュー）画面が表示されます。Cloud Volumes ONTAP タブを探し、 Go to Cloud Manager を選択します。ログインすると、キャンバス画面が表示されます。



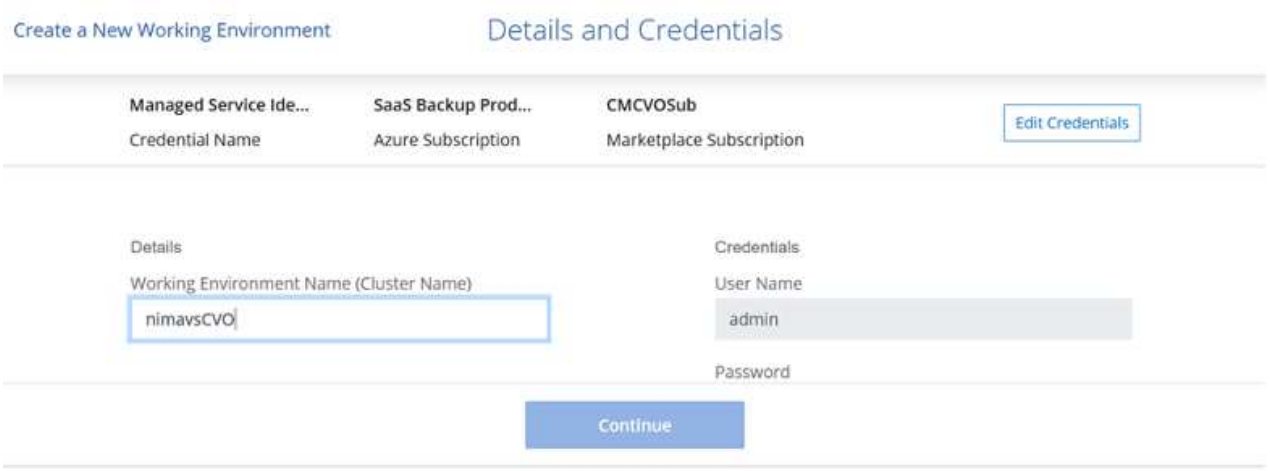
2. Cloud Manager のホームページで、 Add a Working Environment をクリックし、クラウドとして Microsoft Azure を選択し、システム構成のタイプを選択します。



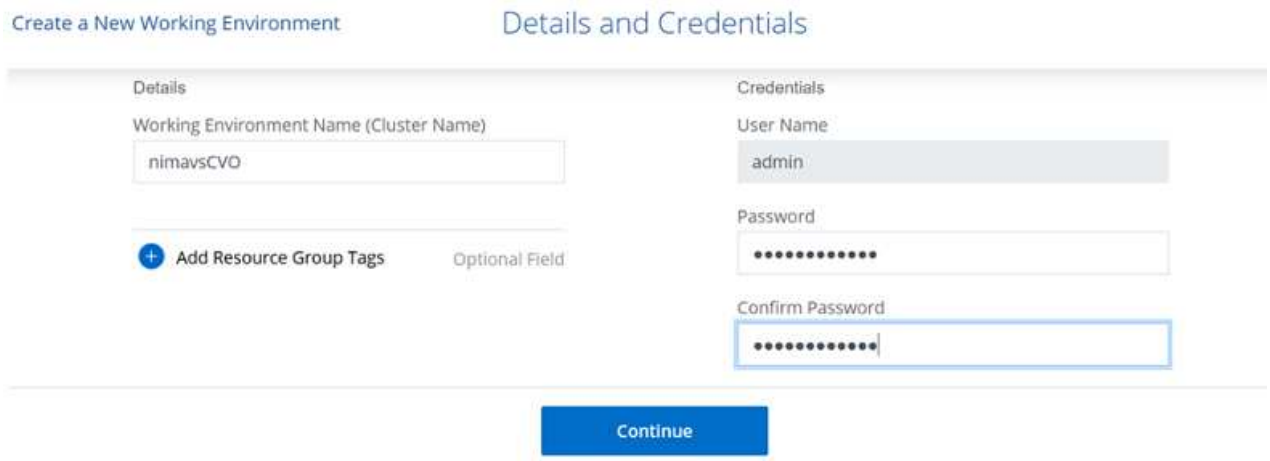
3. Cloud Volumes ONTAP の最初の作業環境を作成する際、 Cloud Manager はコネクタの導入を求めます。



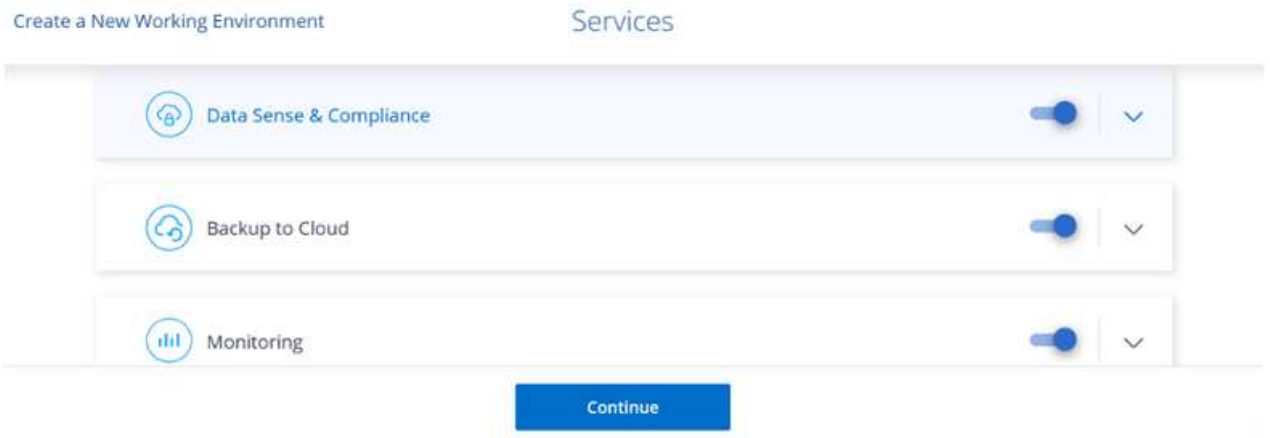
4. コネクタが作成されたら、 [詳細（ Details ）] および [資格情報（ Credentials ）] フィールドを更新します。



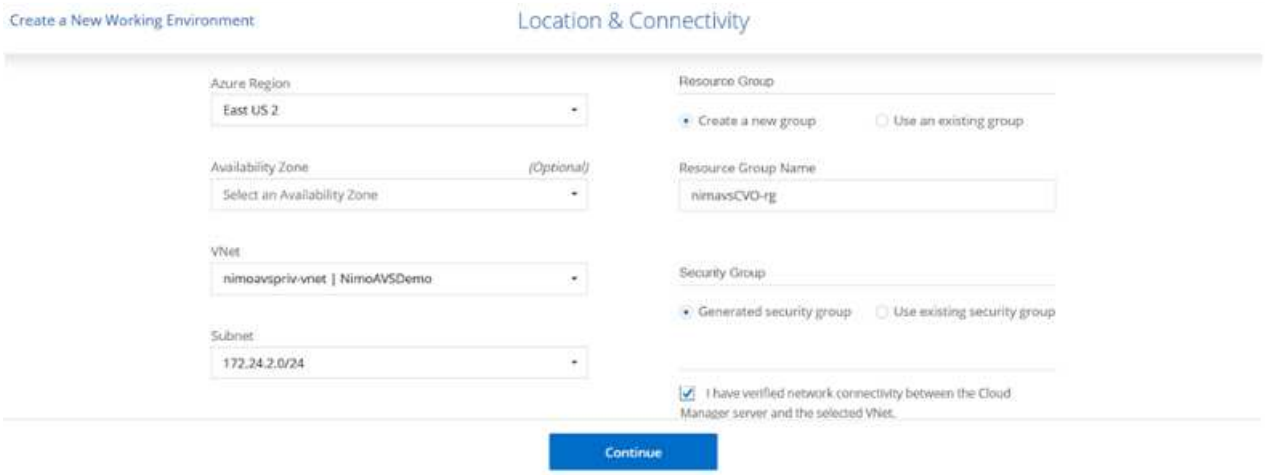
5. 環境名と admin クレデンシャルなど、作成する環境の詳細を指定します。オプションのパラメータとして、 Azure 環境のリソースグループタグを追加します。完了したら、 [続行] をクリックします。



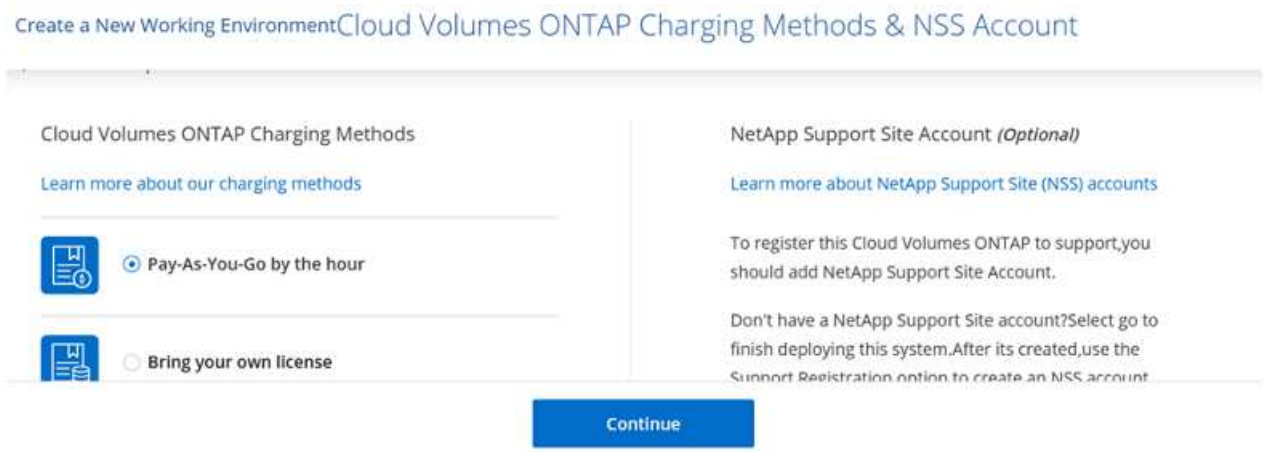
6. Cloud Volumes ONTAPの導入に使用するアドオンサービス（BlueXPの分類、BlueXPのバックアップとリカバリ、Cloud Insightsなど）を選択します。サービスを選択し、 Continue （続行）をクリックします。



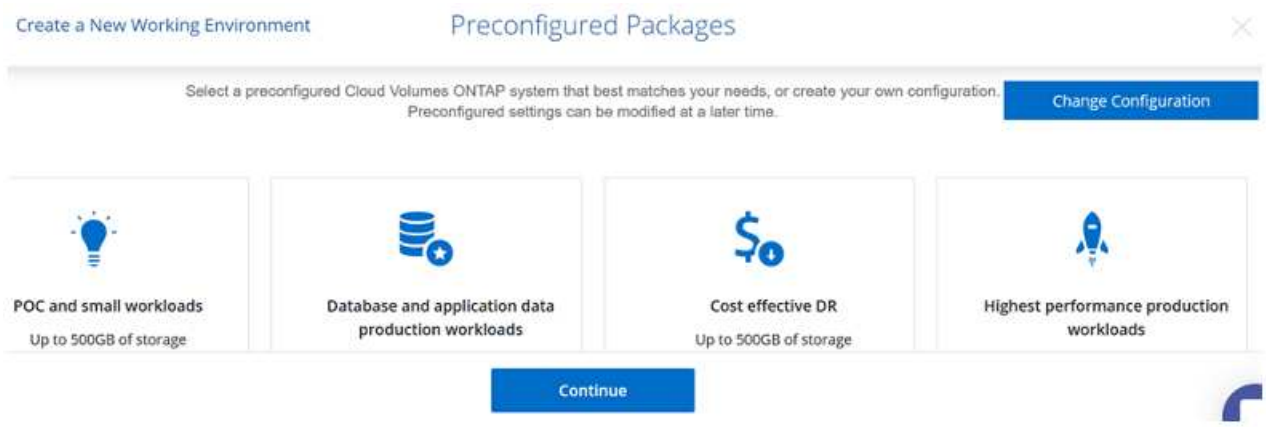
7. Azure の場所と接続を設定します。使用する Azure のリージョン、リソースグループ、 VNet 、およびサブネットを選択します。



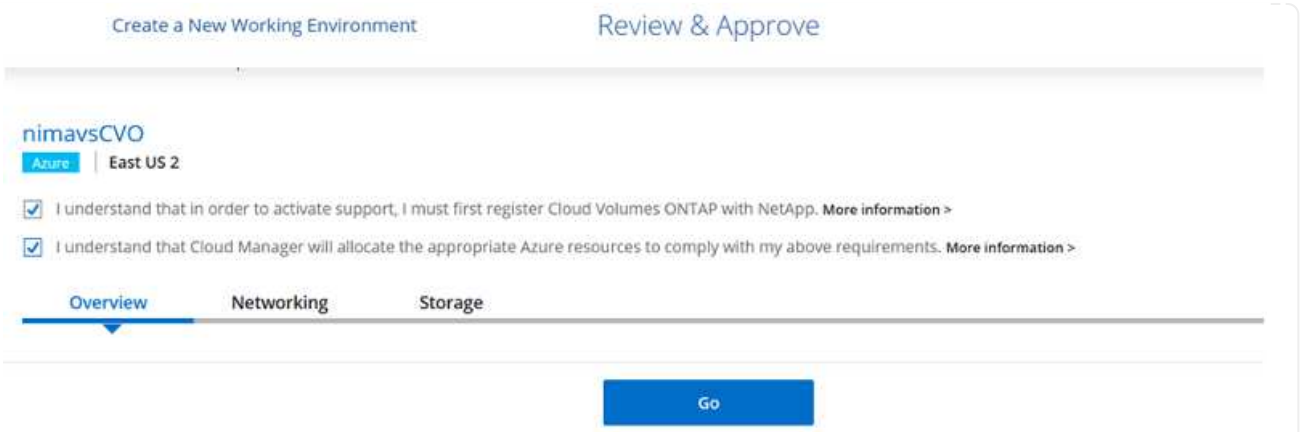
8. ライセンスオプションとして、「従量課金制」または「 BYOL for using existing license 」を選択します。この例では、 ［従量課金制］ オプションを使用します。



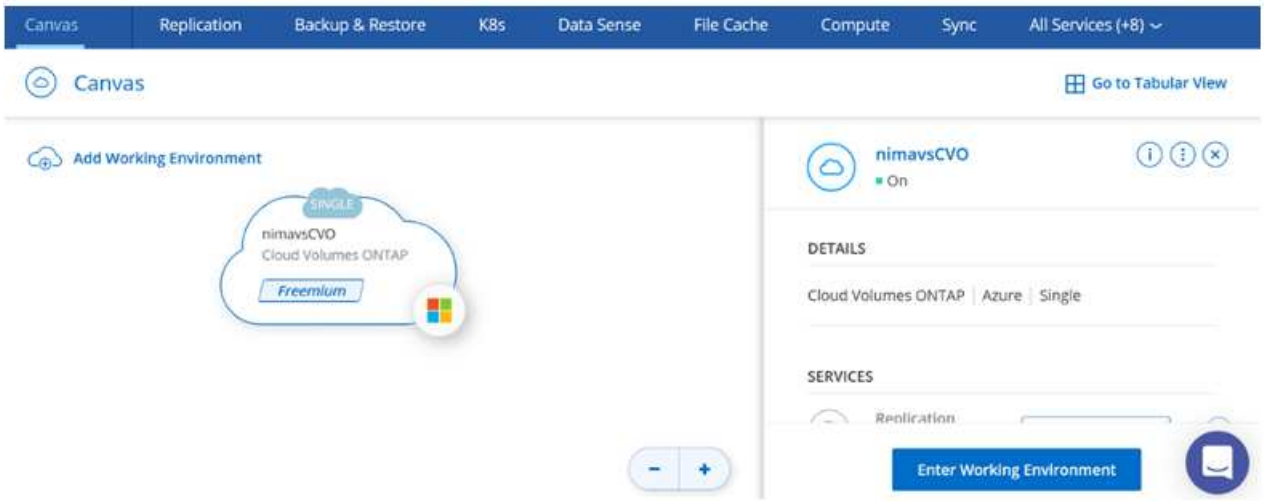
9. さまざまなタイプのワークロードに使用できる事前設定されたパッケージをいくつか選択できます。



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

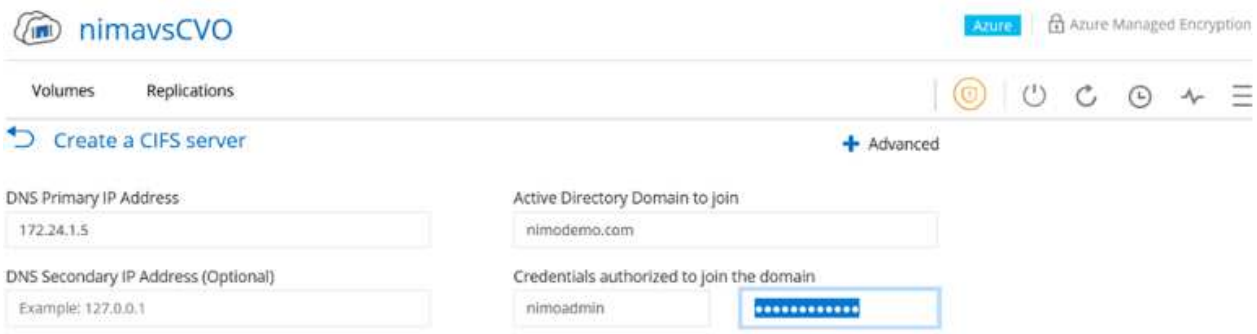


11. Cloud Volumes ONTAP のプロビジョニングが完了すると、 [Canvas] ページの作業環境に表示されます。

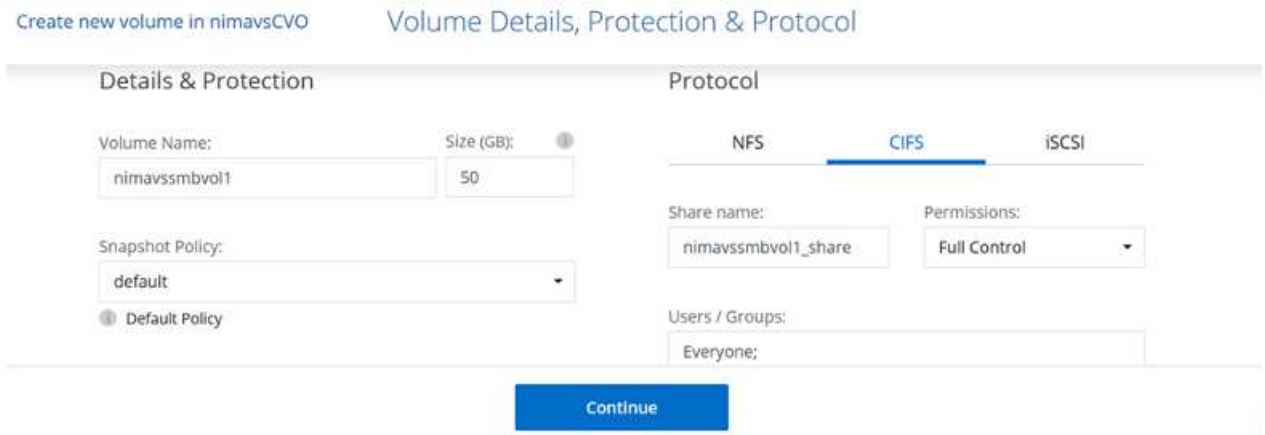


SMB ボリューム用の追加の設定

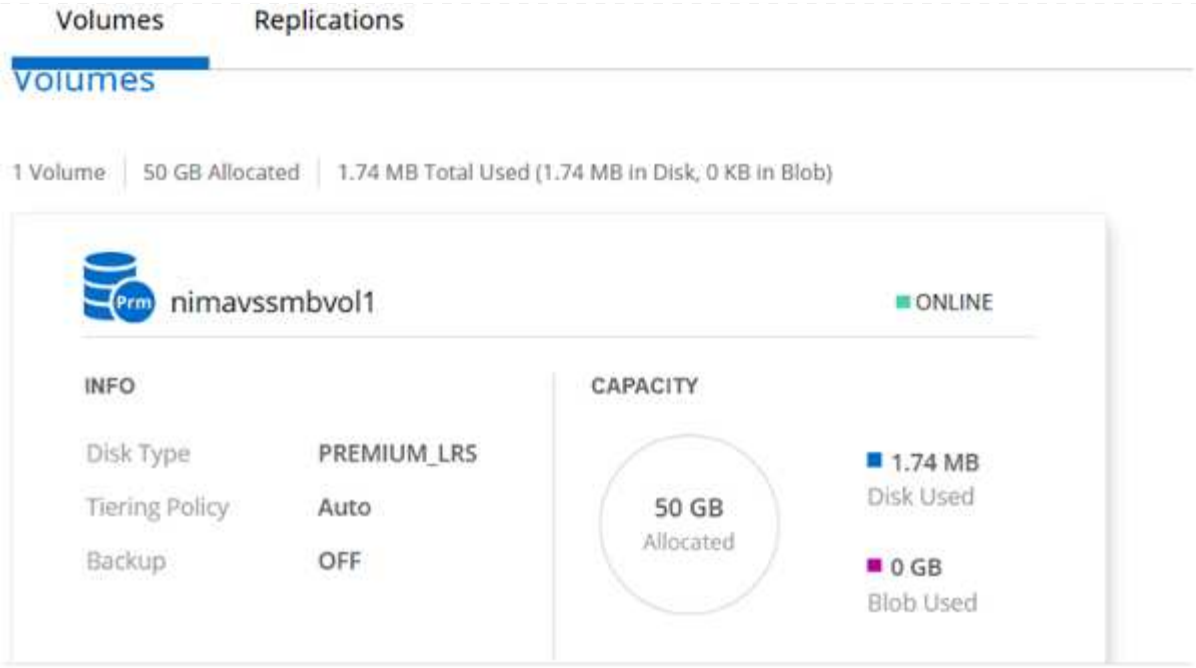
1. 作業環境の準備ができたら、 CIFS サーバに適切な DNS および Active Directory 設定パラメータが設定されていることを確認します。この手順は、 SMB ボリュームを作成する前に実行する必要があります。



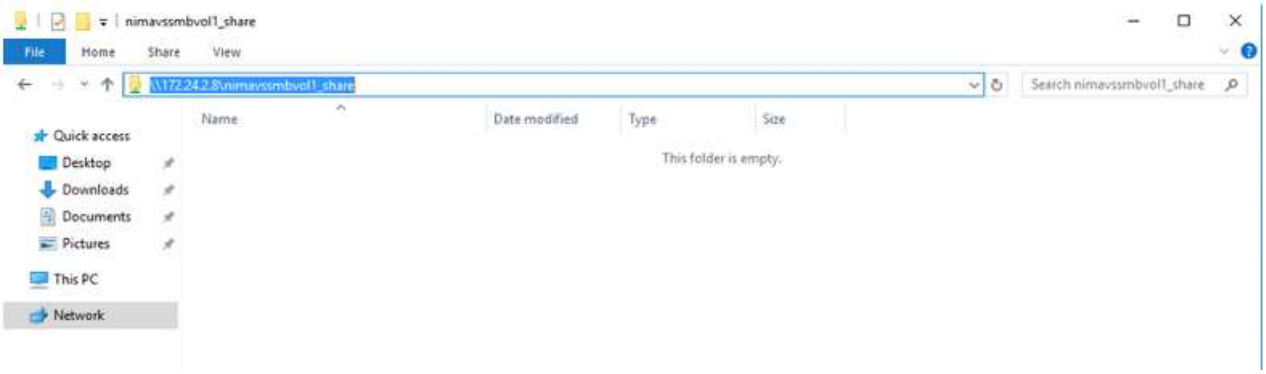
2. SMB ボリュームの作成は簡単なプロセスです。CVO インスタンスを選択してボリュームを作成し、 Create Volume （ボリュームの作成）オプションをクリックします。適切なサイズを選択し、包含アグリゲートを選択するか、高度な割り当てメカニズムを使用して特定のアグリゲートに配置します。このデモでは、 SMB がプロトコルとして選択されます。



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



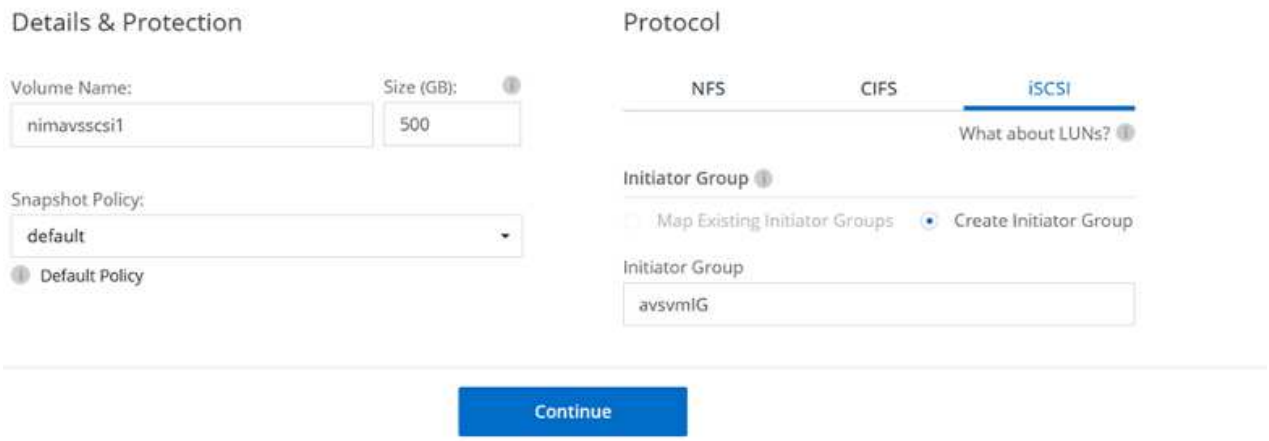
4. ボリュームが作成されたら、 mount コマンドを使用して、 Azure VMware 解決策 SDDC ホストで実行されている VM から共有に接続します。
5. 次のパスをコピーし、ネットワークドライブのマッピングオプションを使用して、 Azure VMware 解決策 SDDC で実行されている VM にボリュームをマウントします。



LUN をホストに接続します

LUN をホストに接続するには、次の手順を実行します。

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



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

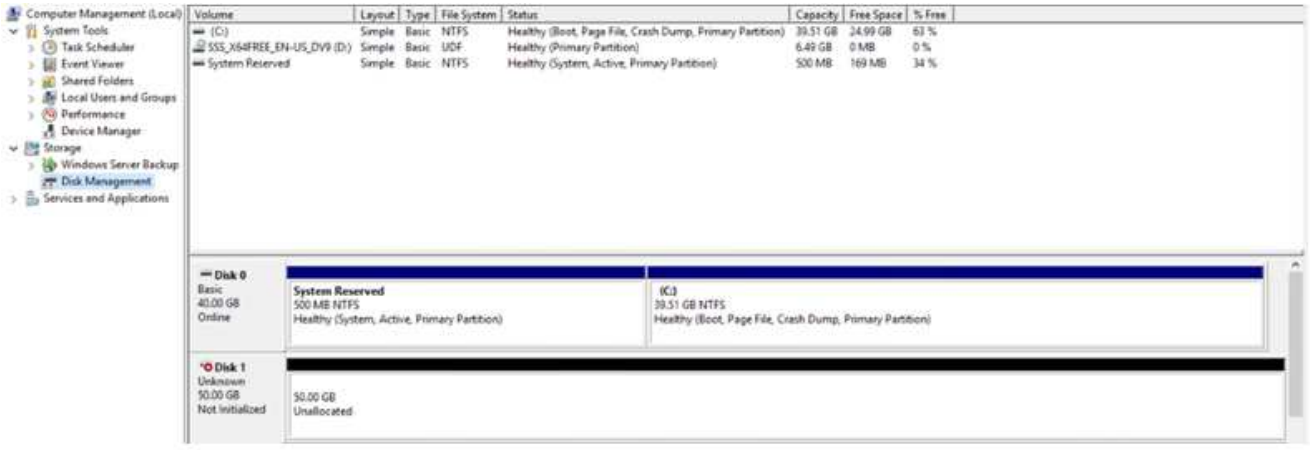
   Azure VMware 解決策 SDDC にあるホストでも同じ処理を実行するには、次の手順を実行します。

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

      - 注： * Windows ホストからクラスタ内の各ノードへの iSCSI 接続が確立されている必要があります。ネイティブ DSM では、使用する最適なパスが選択されます。

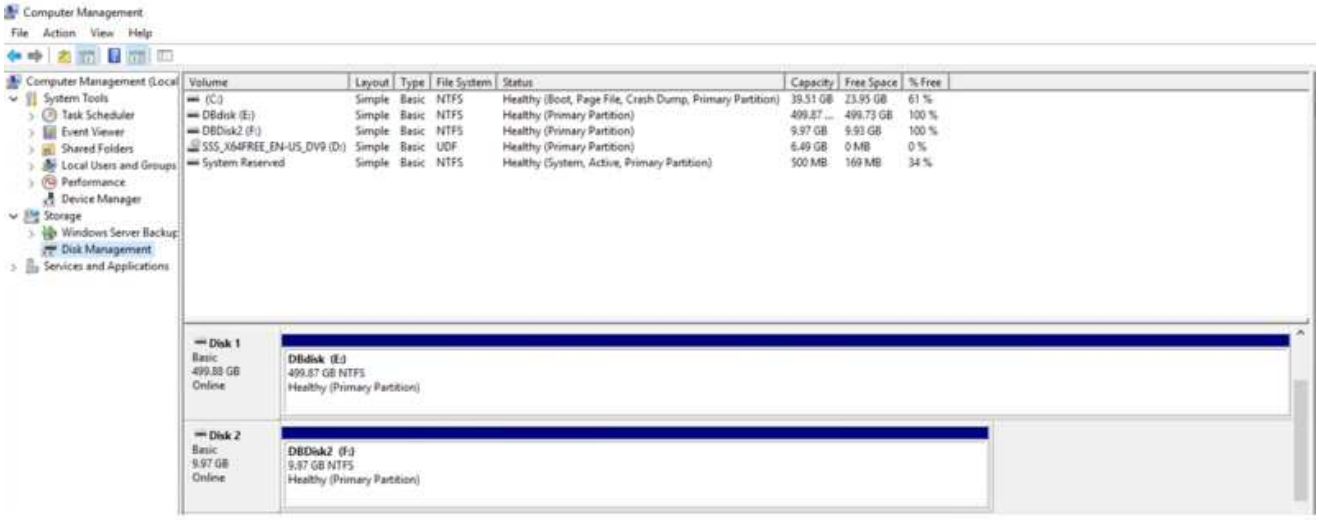
Storage Virtual Machine （ SVM ）の LUN は、 Windows ホストではディスクとして表示されます。追加した新しいディスクは、ホストでは自動的に検出されません。手動の再スキャンをトリガーしてディスクを検出するには、次の手順を実行します。

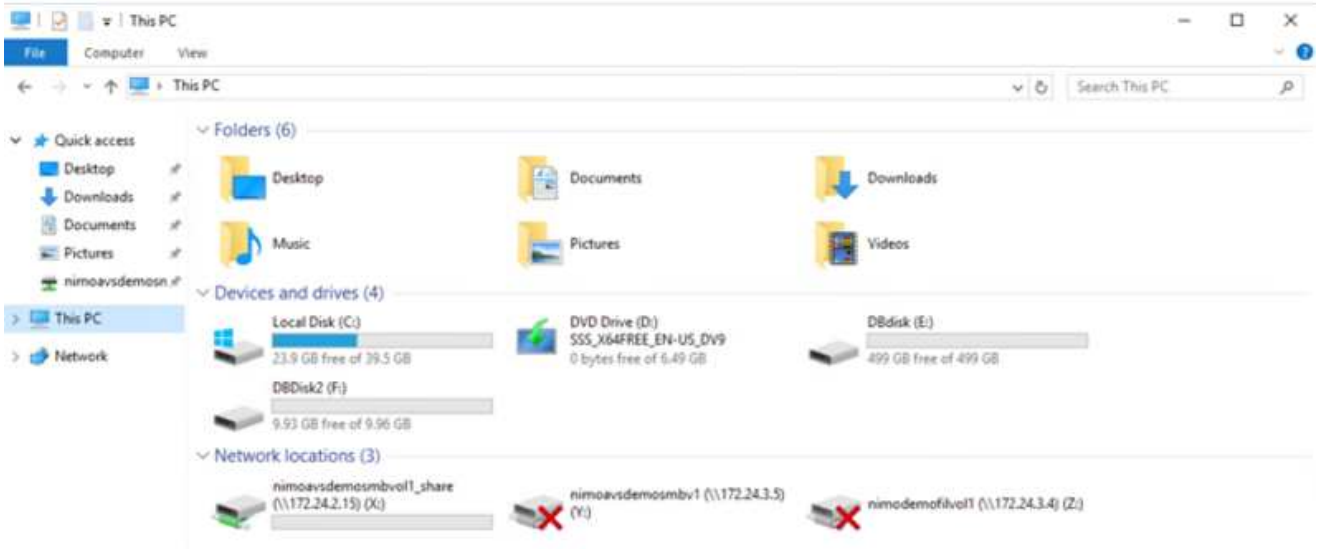
1. Windows コンピュータの管理ユーティリティを開きます。 [スタート]>[管理ツール]>[コンピュータの管理] を選択します。
2. ナビゲーションツリーでストレージノードを展開します。
3. [ディスクの管理] をクリックします
4. ［ アクション ］ > ［ ディスクの再スキャン ］ の順にクリック



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

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



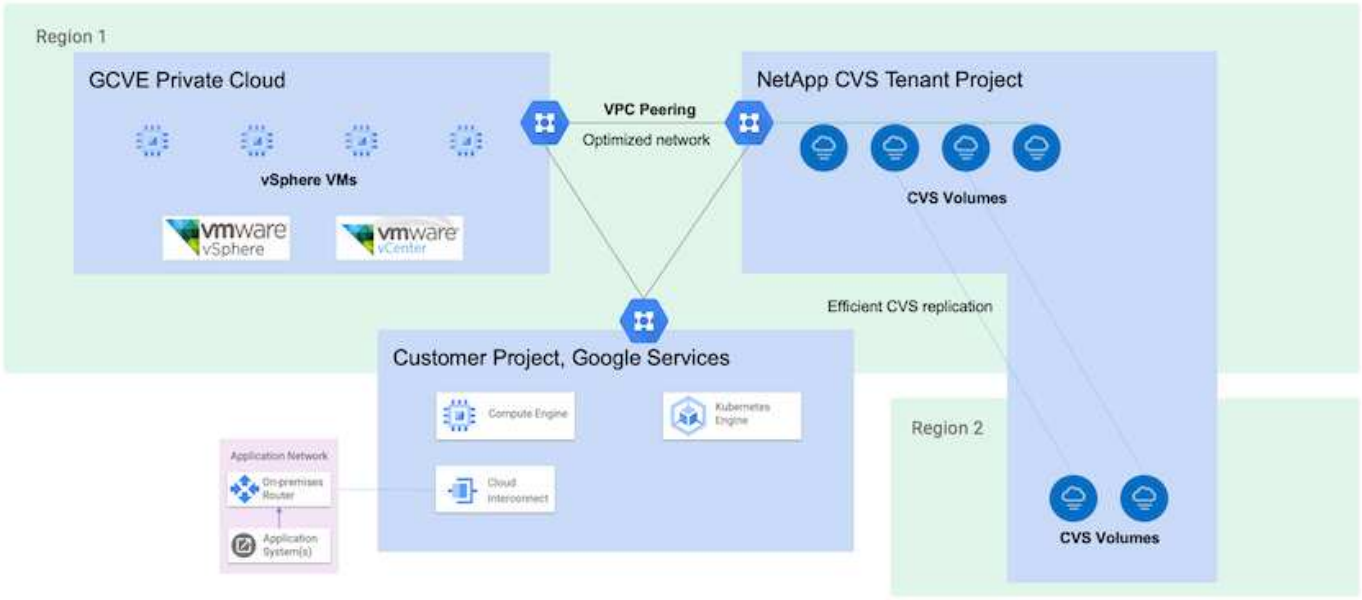


Google Cloud VMware Engine NetApp Cloud Volume Serviceを使用した**NFS**データストアの補完

概要

執筆者：ネットアップSuresh Thoppay

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



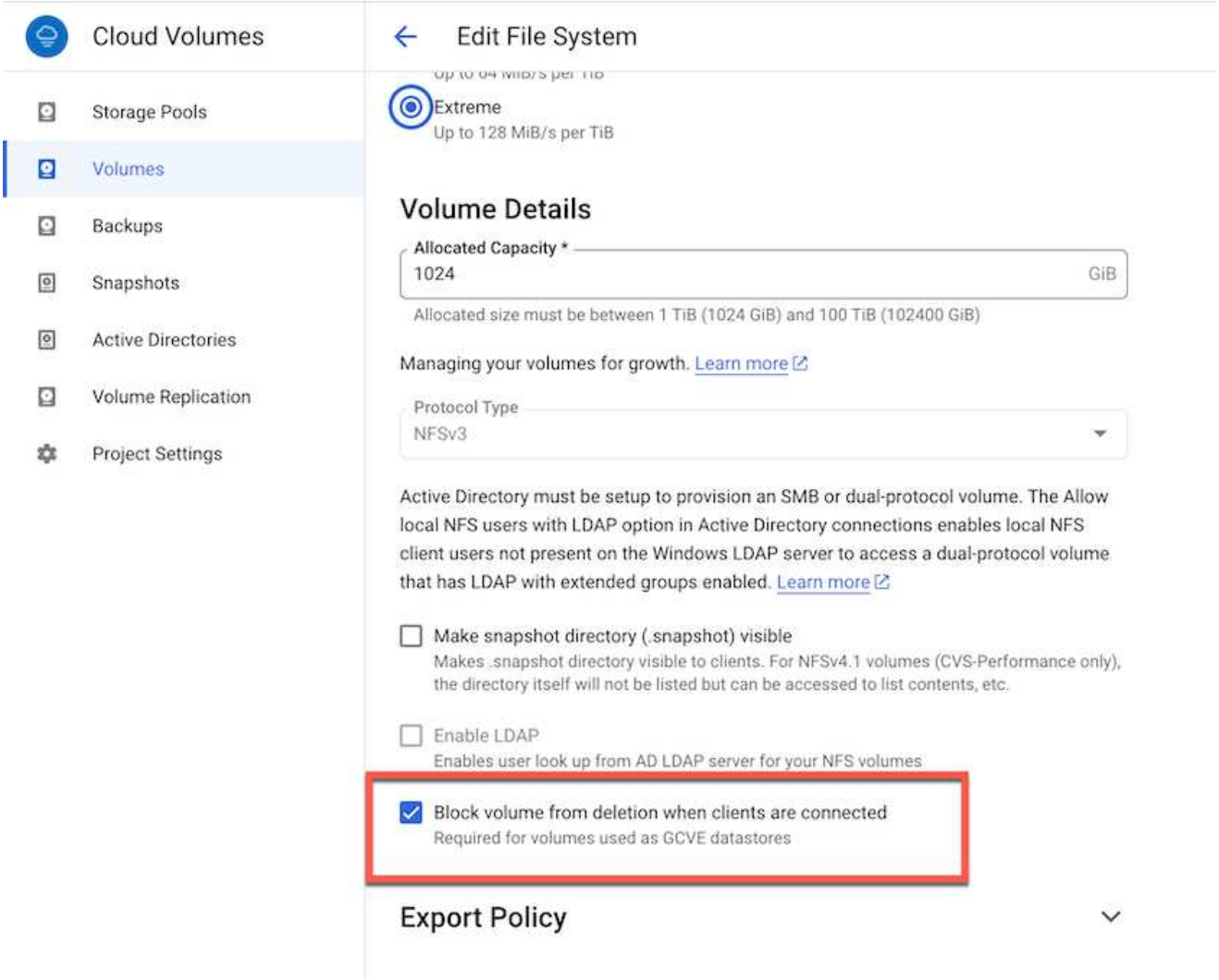
NetApp CVSから**GCVE**に**NFS**データストアをマウントする導入手順

CVS-Performanceボリュームをプロビジョニングします

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

そのCVSボリュームを削除不可としてマークします

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



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

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

NFSデータストアをマウントするには、GCVEとNetApp CVSプロジェクトの間にプライベート接続が確立されている必要があります。
詳細については、を参照してください "プライベートサービスアクセスのセットアップ方法"

NFSデータストアをマウント

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

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

NetAppクラウドボリュームサービスによるコスト削減

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

参照リンク

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

GCP のネットアップストレージオプション

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

Cloud Volumes ONTAP （CVO）

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

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

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

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

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

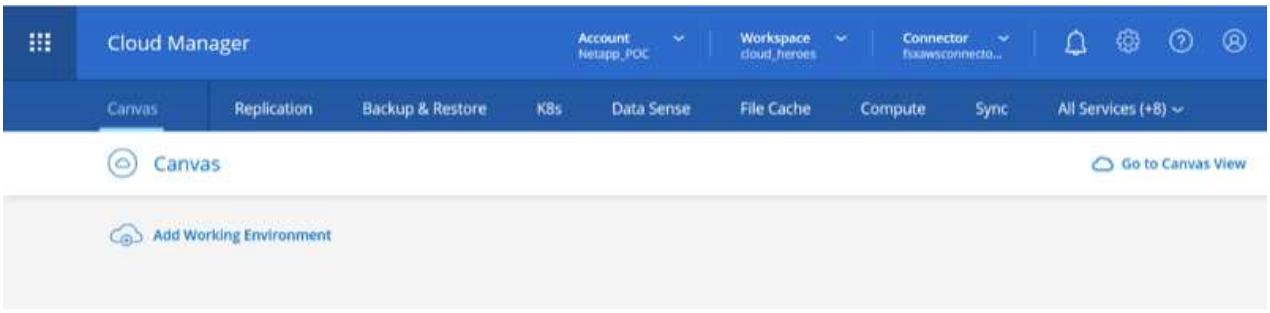
Cloud Volumes ONTAP を Google Cloud に導入（自分で導入）

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

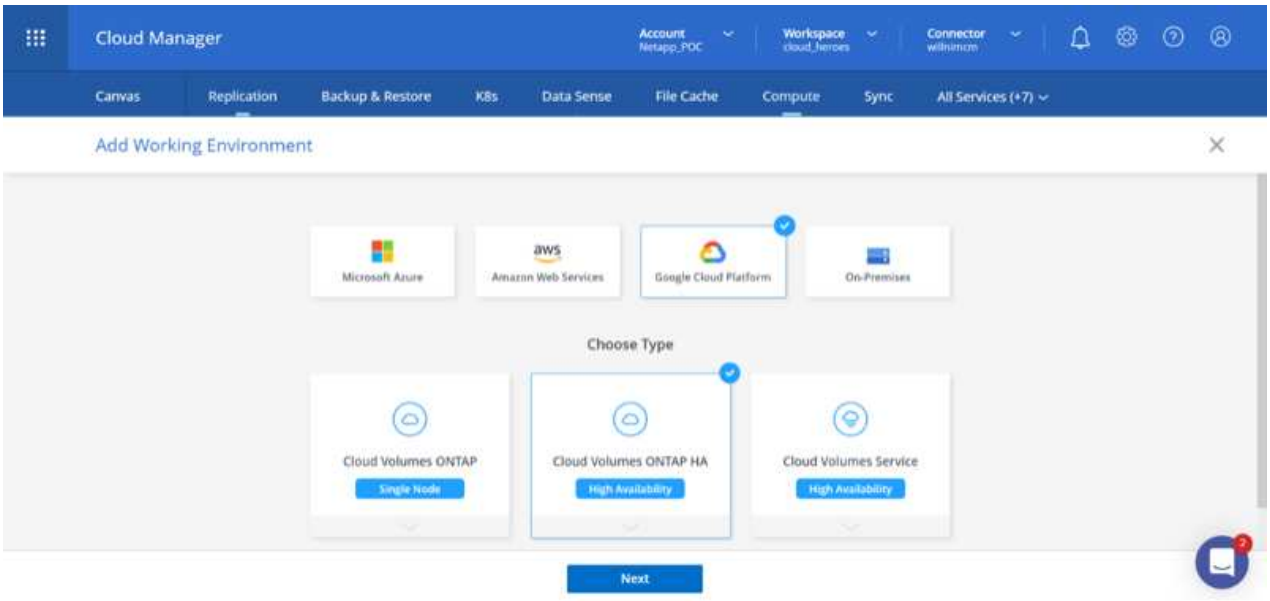
ディザスタリカバリや移行の目的でオンプレミス環境からクラウドにボリュームをレプリケートするには、サイト間 VPN または Cloud Interconnect を使用して Google Cloud へのネットワーク接続を確立します。オンプレミスから Cloud Volumes ONTAP へのデータのレプリケートについては、本ドキュメントでは扱いません。オンプレミスシステムと Cloud Volumes ONTAP システム間でデータをレプリケートする方法については、を参照してください xref:./ehc/"システム間のデータレプリケーションの設定"。

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

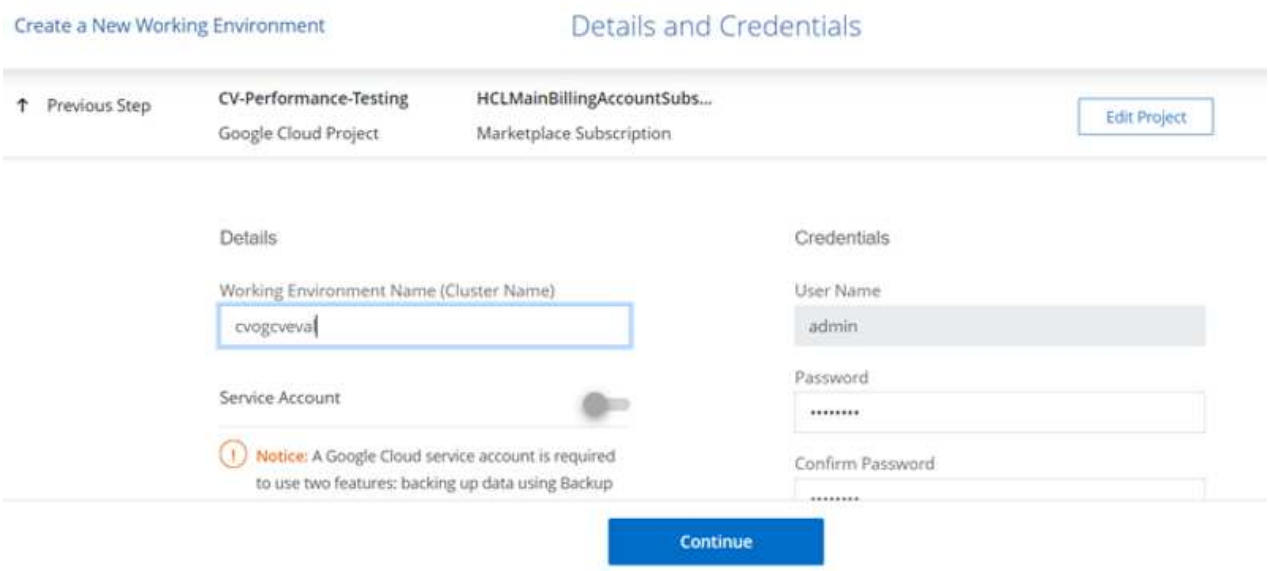
1. NetApp Cloud Central にログイン— Fabric View （ファブリックビュー）画面が表示されます。Cloud Volumes ONTAP タブを探し、 Go to Cloud Manager を選択します。ログインすると、キャンバス画面が表示されます。



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

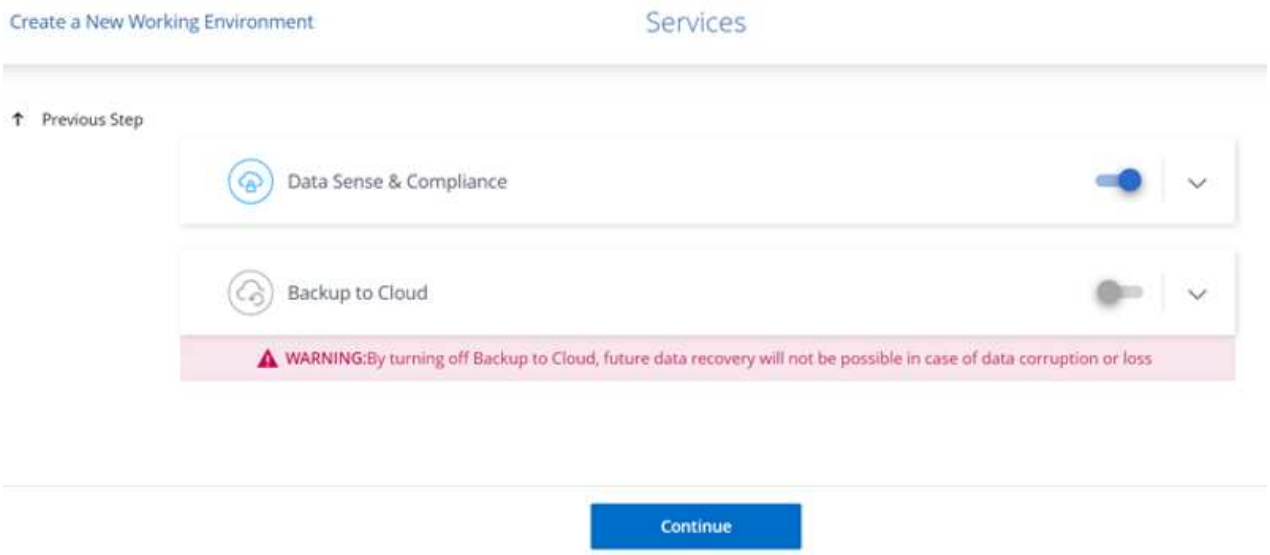


3. 環境名と admin クレデンシャルなど、作成する環境の詳細を指定します。完了したら、 [続行] をクリックします。

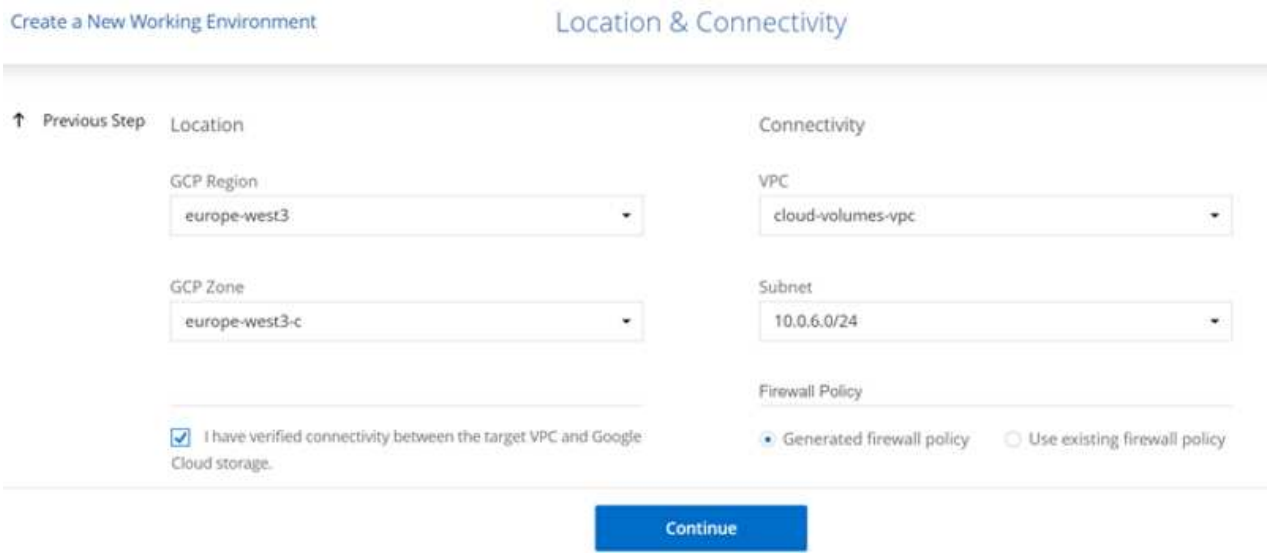


4. データセンスとコンプライアンス、クラウドへのバックアップなど、 Cloud Volumes ONTAP 導入用のアドオンサービスを選択または選択解除します。次に、 [続行] をクリックします。

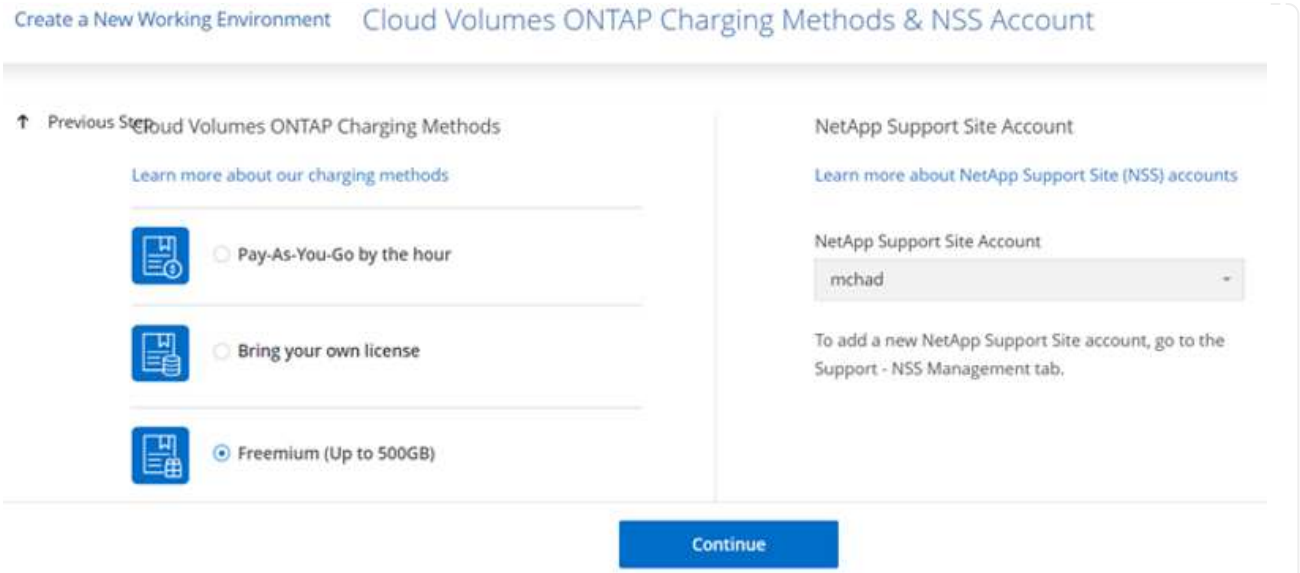
   ヒント：アドオンサービスを無効にすると、確認のポップアップメッセージが表示されます。CVO の導入後にアドオンサービスを追加 / 削除できます。コストを回避するために、不要なサービスは最初から選択解除することを検討してください。



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



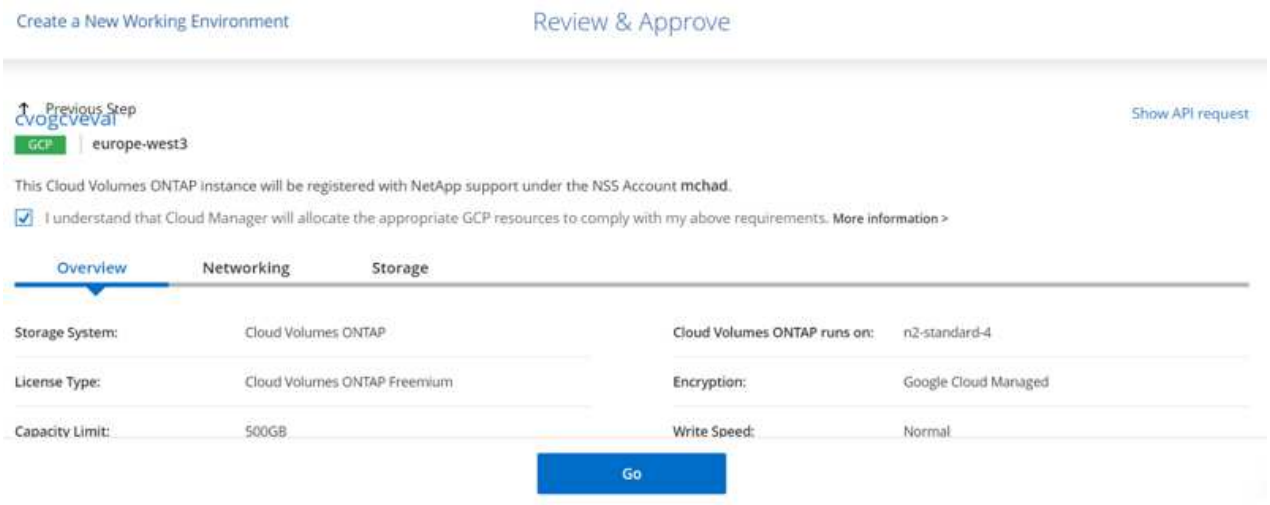
6. ライセンスオプションとして、「従量課金制」または「 BYOL for using existing license 」を選択します。この例では、 Freemium オプションが使用されています。次に、 [続行] をクリックします。



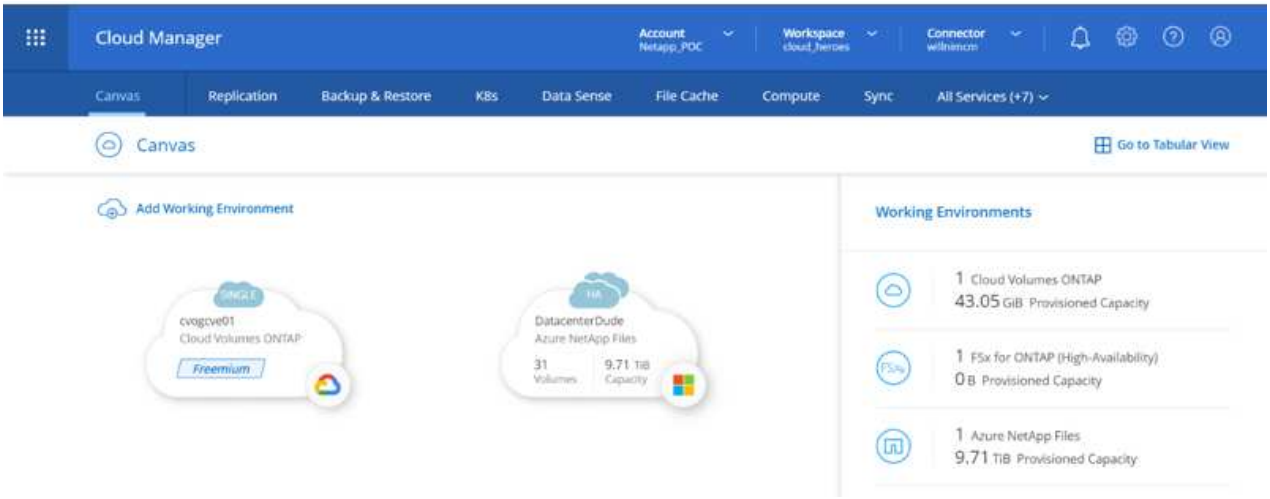
7. AWS SDDC 上の VMware クラウドで実行されている VM に導入されるワークロードのタイプに基づいて、複数の事前設定パッケージから選択できます。

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

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



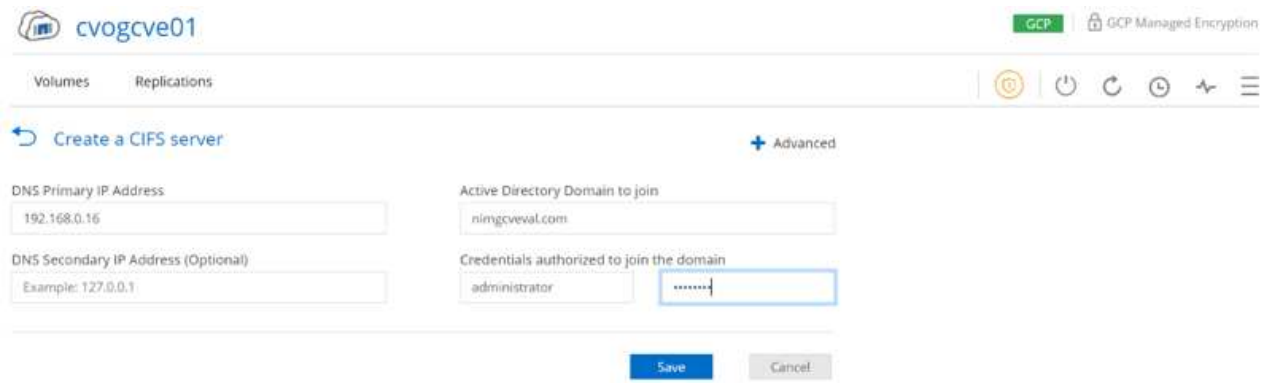
9. Cloud Volumes ONTAP のプロビジョニングが完了すると、 [Canvas] ページの作業環境に表示されます。



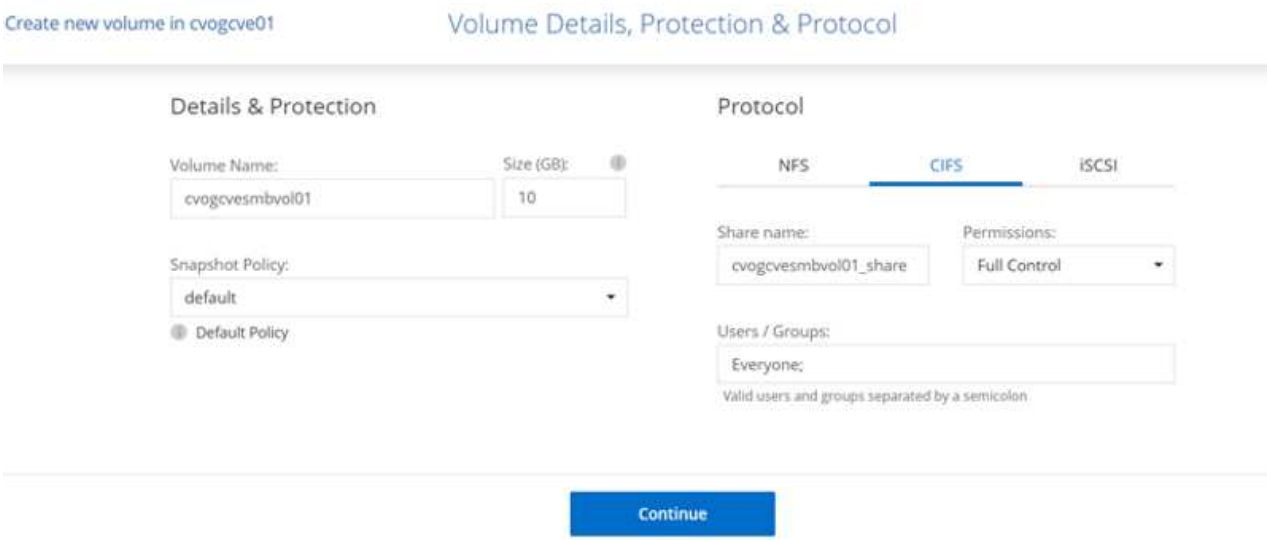
SMB ボリューム用の追加の設定

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

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



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

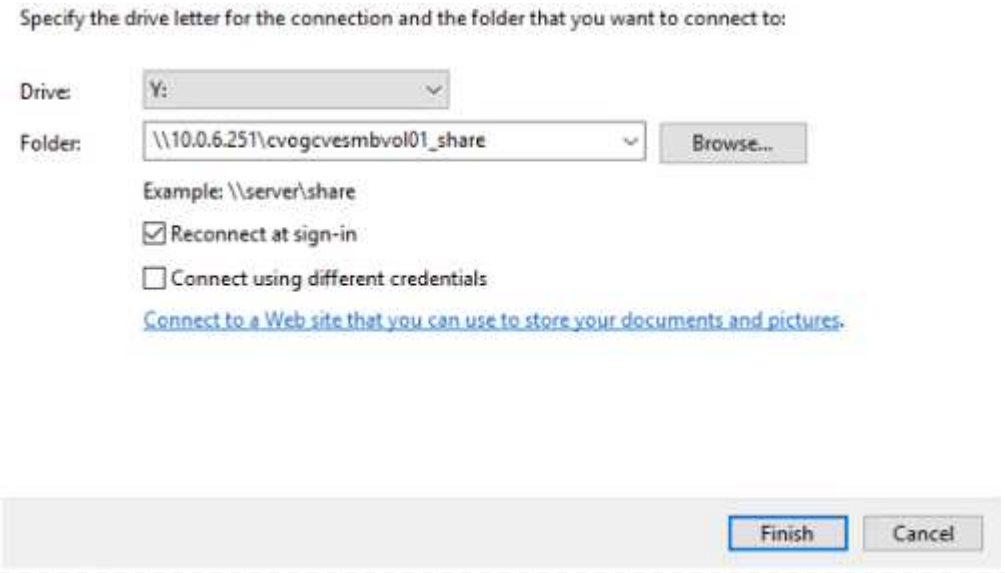


3. ボリュームのプロビジョニングが完了すると、 Volumes （ボリューム）ペインにボリュームが表示されます。CIFS 共有はプロビジョニングされるため、ユーザまたはグループにファイルとフォルダに対する権限を付与し、ユーザが共有にアクセスしてファイルを作成できることを確認してください。ファイル権限とフォルダ権限はすべて SnapMirror レプリケーションの一部として保持されるため、オンプレミス環境からボリュームをレプリケートする場合はこの手順は必要ありません。

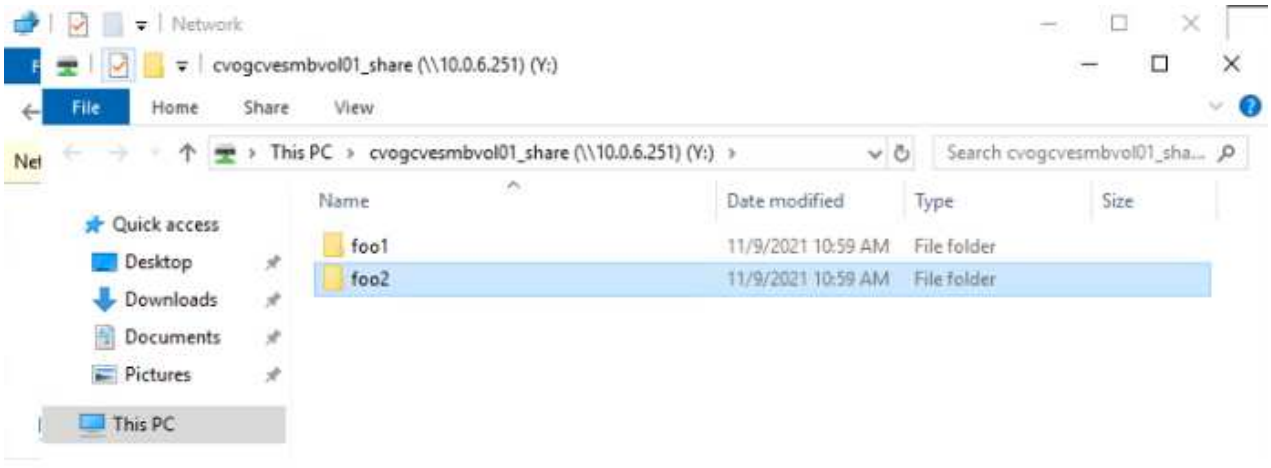
   ヒント：ボリュームメニュー（ ° ）をクリックすると、そのオプションが表示されます。

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

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



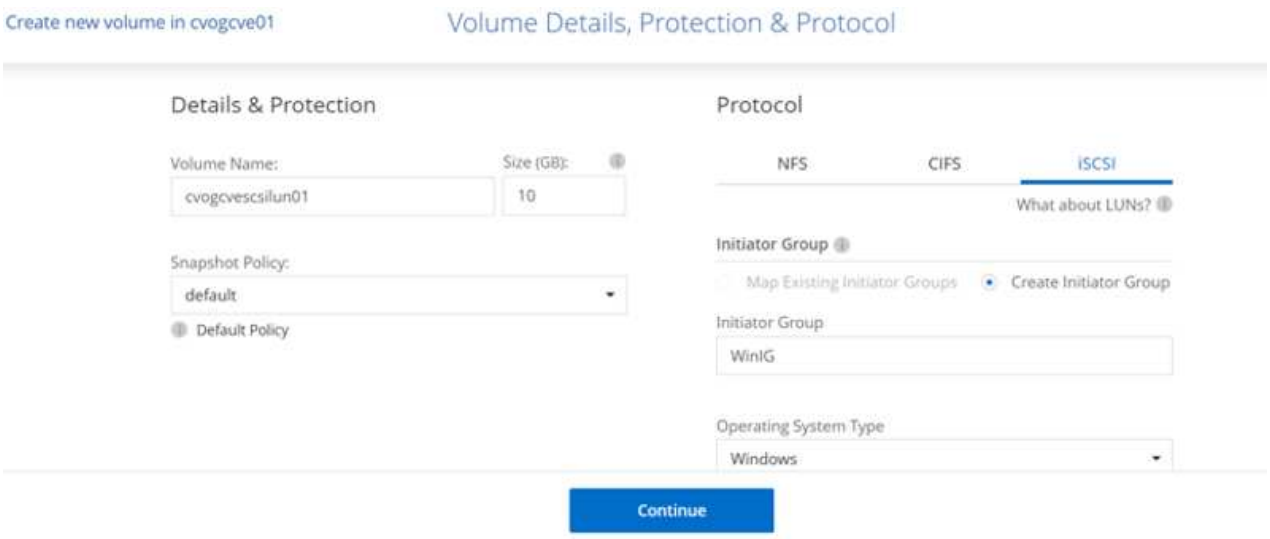
マッピングが完了すると、このマッピングに簡単にアクセスでき、 NTFS アクセス権を適切に設定できます。

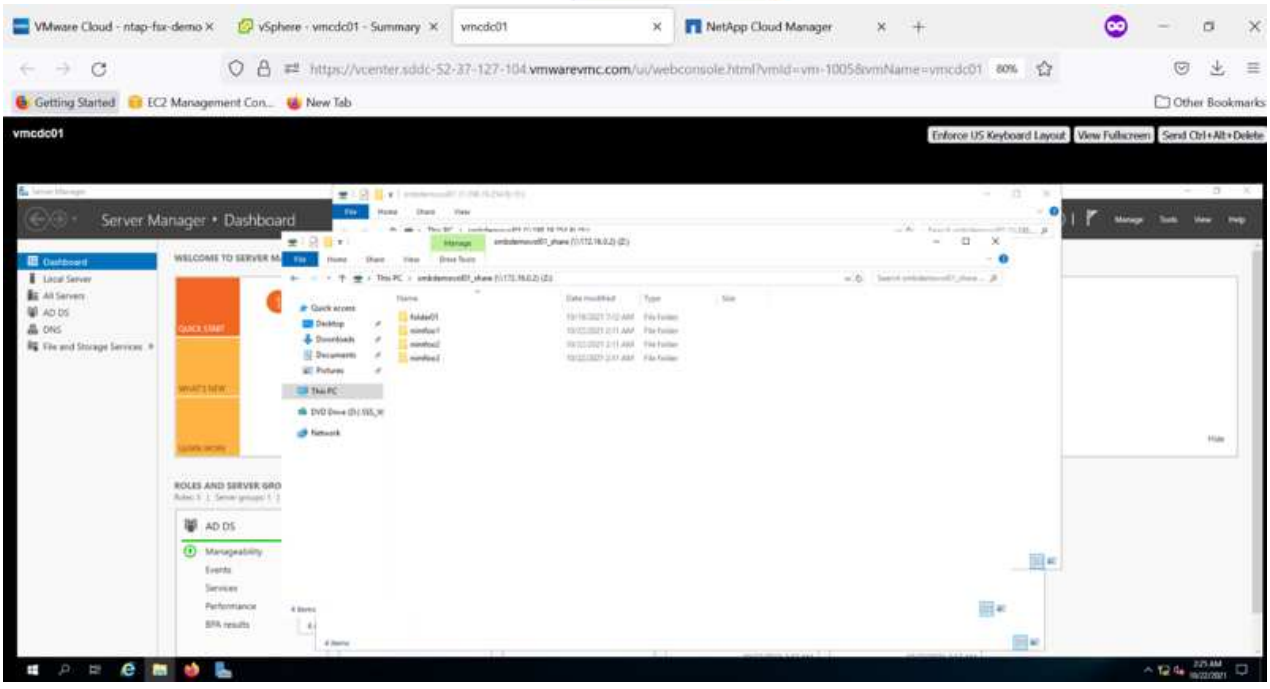


Cloud Volumes ONTAP 上の LUN をホストに接続します

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

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





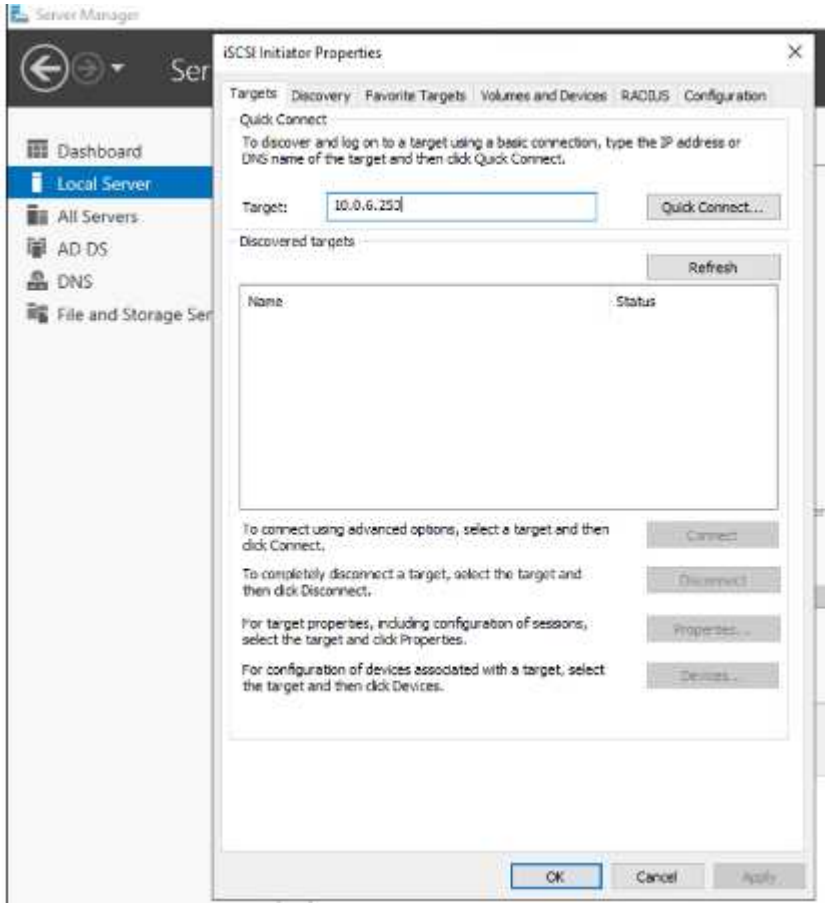
3. ボリュームのプロビジョニングが完了したら、ボリュームメニュー（ ° ）を選択し、ターゲット IQN をクリックします。iSCSI Qualified Name （ IQN ）をコピーするには、 Copy （コピー）をクリックします。ホストから LUN への iSCSI 接続をセットアップします。

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

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

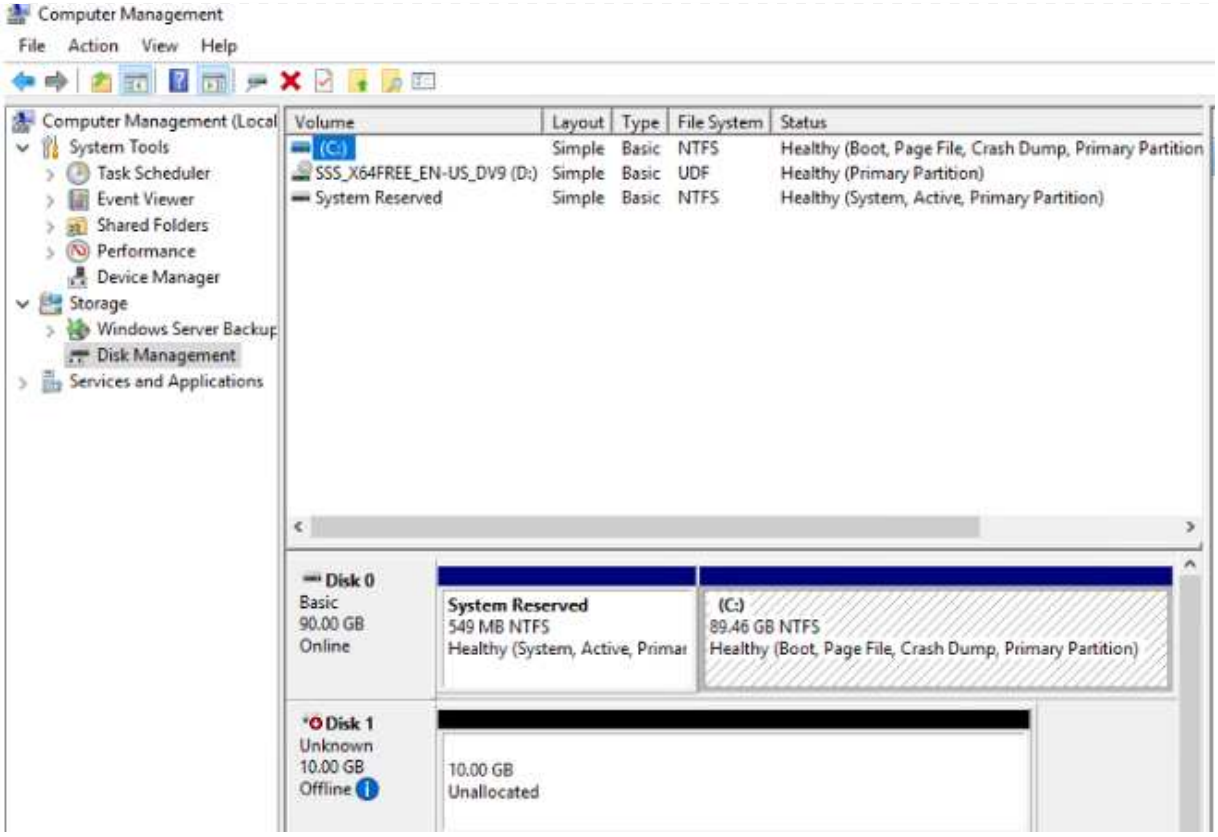
2. ［ iSCSI イニシエータのプロパティ ］ ダイアログ・ボックスを開きます ［ サーバーマネージャ ］ ＞ ［ ダッシュボード ］ ＞ ［ ツール ］ ＞ ［ iSCSI イニシエータ ］
3. Discovery （検出）タブで、 Discover Portal （ポータルの検出）または Add Portal （ポータルの追加）をクリックし、 iSCSI ターゲットポートの IP アドレスを入力します。
4. ターゲットタブで検出されたターゲットを選択し、ログオンまたは接続をクリックします。
5. [マルチパスを有効にする] を選択し、コンピュータの起動時に [この接続を自動的に復元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

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



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

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

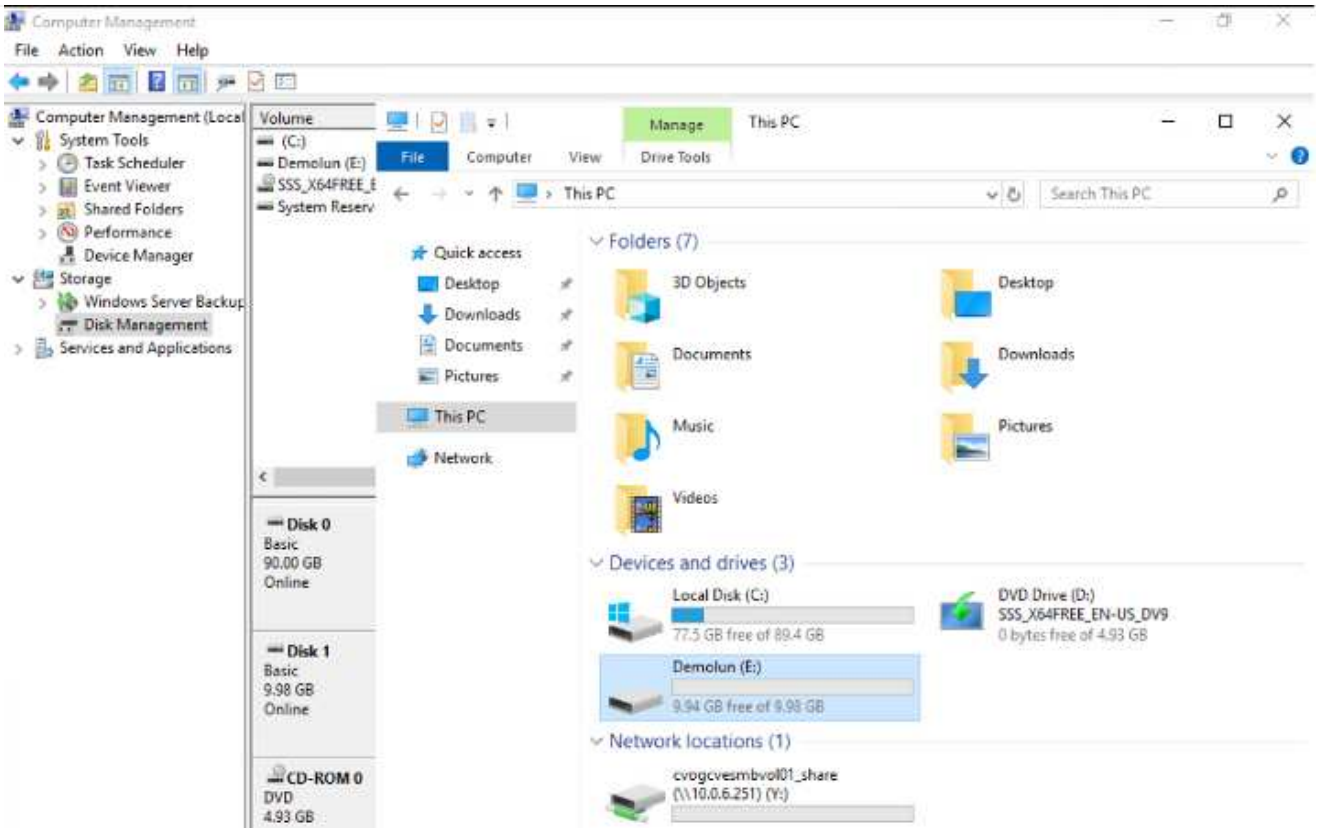


Windows ホストから初めてアクセスした時点では、新しい LUN にはパーティションやファイルシステムは設定されていません。LUN を初期化します。必要に応じて、次の手順を実行してファイルシステムで LUN をフォーマットします。

a. Windows ディスク管理を開始します。

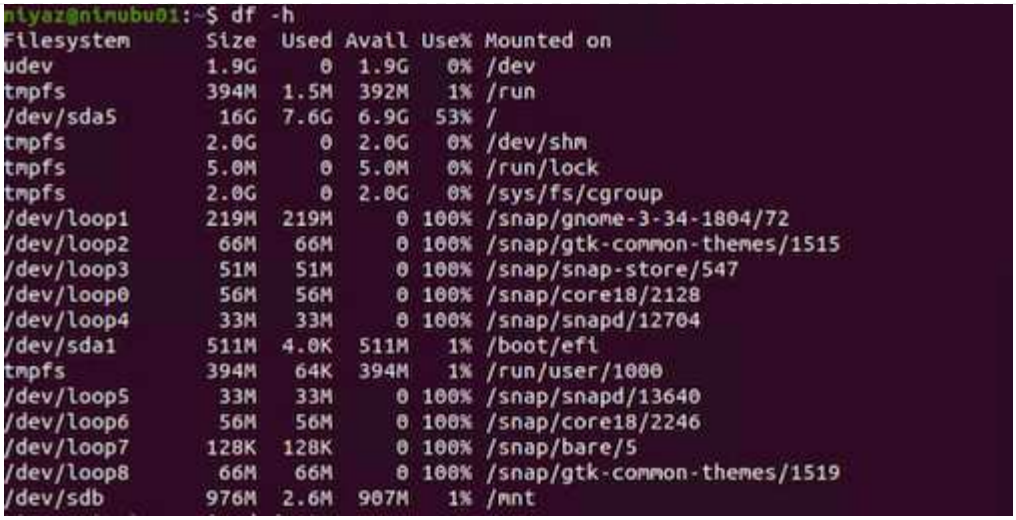
b. LUN を右クリックし、必要なディスクまたはパーティションのタイプを選択します。

c. ウィザードの指示に従います。この例では、ドライブ F ：がマウントされています。



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

```
niyaz@nimubu01: ~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0    7:0    0 55.4M  1 loop /snap/core18/2128
loop1    7:1    0  219M  1 loop /snap/gnome-3-34-1804/72
loop2    7:2    0 65.1M  1 loop /snap/gtk-common-themes/1515
loop3    7:3    0   51M  1 loop /snap/snap-store/547
loop4    7:4    0 32.3M  1 loop /snap/snapd/12704
loop5    7:5    0 32.5M  1 loop /snap/snapd/13640
loop6    7:6    0 55.5M  1 loop /snap/core18/2246
loop7    7:7    0    4K  1 loop /snap/bare/5
loop8    7:8    0 65.2M  1 loop /snap/gtk-common-themes/1519
sda      8:0    0   16G  0 disk
├─sda1   8:1    0  512M  0 part /boot/efi
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0 15.5G  0 part /
sdb      8:16   0    1G  0 disk
```

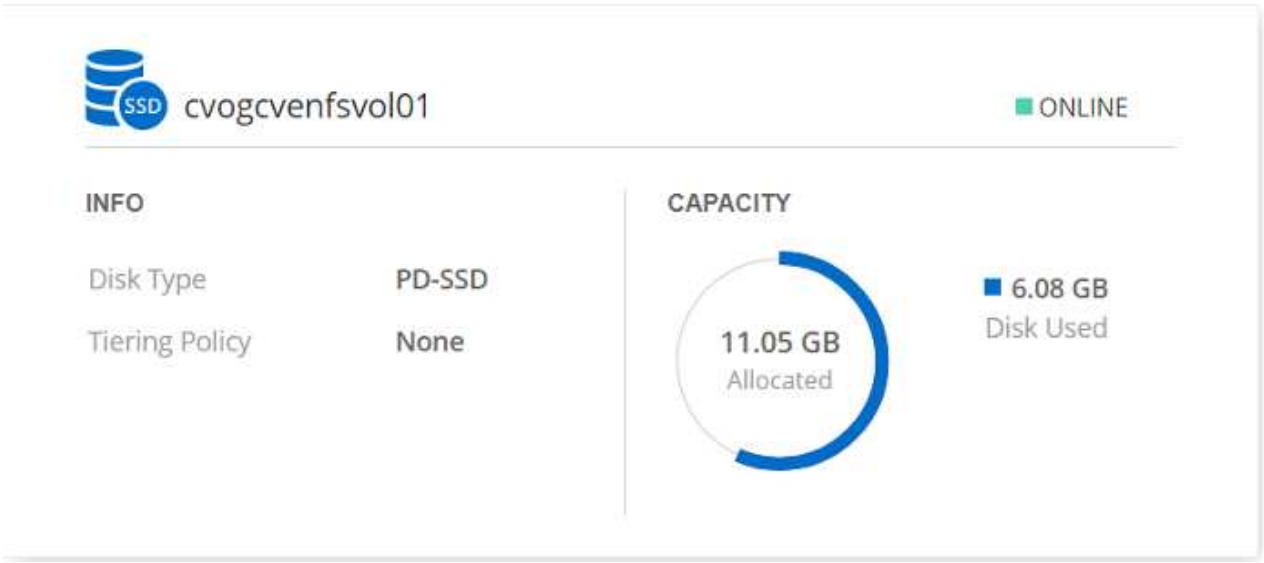

niyaz@ninubu01:~$ df -h
Filesystem Size Used Avail Use% Mounted on
udev 1.9G 0 1.9G 0% /dev
tmpfs 394M 1.5M 392M 1% /run
/dev/sda5 16G 7.6G 6.9G 53% /
tmpfs 2.0G 0 2.0G 0% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 2.0G 0 2.0G 0% /sys/fs/cgroup
/dev/loop1 219M 219M 0 100% /snap/gnome-3-34-1804/72
/dev/loop2 66M 66M 0 100% /snap/gtk-common-themes/1515
/dev/loop3 51M 51M 0 100% /snap/snap-store/547
/dev/loop0 56M 56M 0 100% /snap/core18/2128
/dev/loop4 33M 33M 0 100% /snap/snapd/12704
/dev/sda1 511M 4.0K 511M 1% /boot/efi
tmpfs 394M 64K 394M 1% /run/user/1000
/dev/loop5 33M 33M 0 100% /snap/snapd/13640
/dev/loop6 56M 56M 0 100% /snap/core18/2246
/dev/loop7 128K 128K 0 100% /snap/bare/5
/dev/loop8 66M 66M 0 100% /snap/gtk-common-themes/1519
/dev/sdb 976M 2.6M 907M 1% /mnt

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

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

以下の手順に従ってボリュームをプロビジョニングします

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



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

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

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

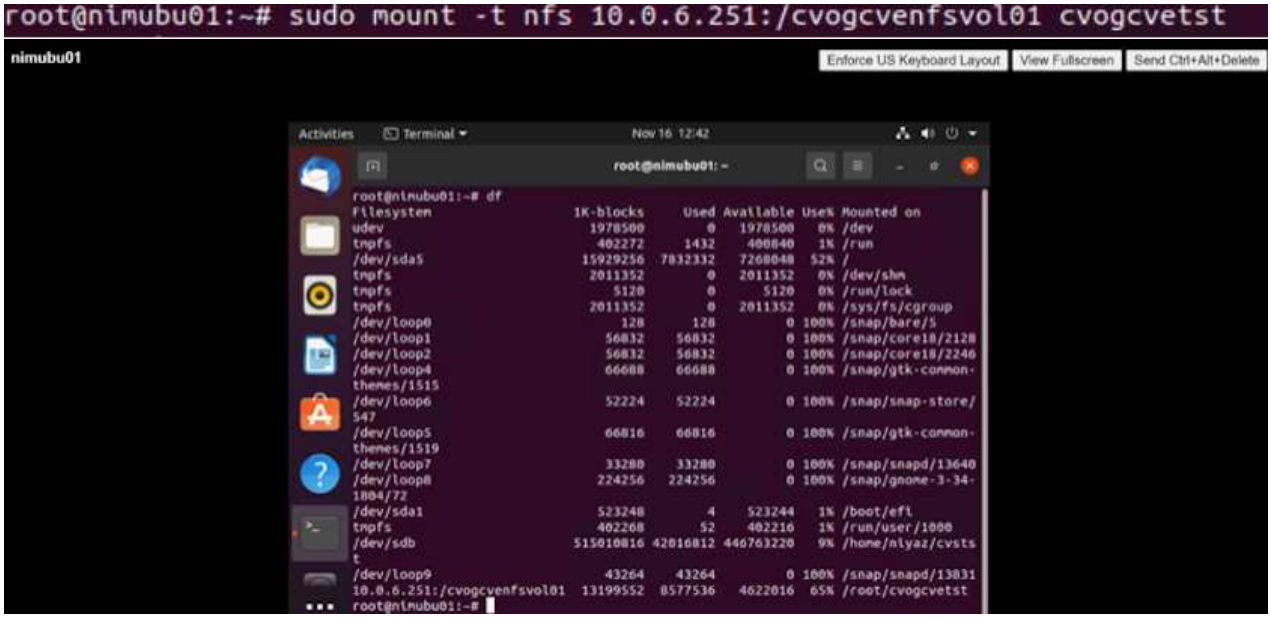
```
$ sudo mkdir /cvogcvetst
```

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

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

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

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



Cloud Volumes Service （CVS）

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

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

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

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

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

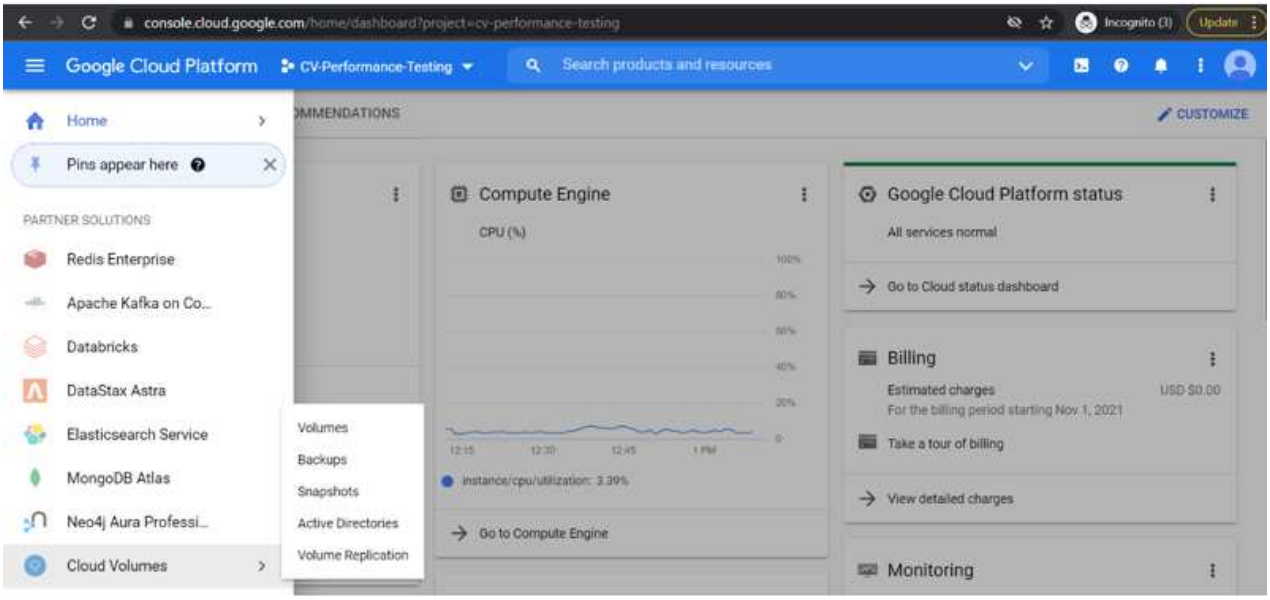
Cloud Volume Service と Google Cloud VMware Engine のプライベートクラウドは同じリージョンに配置する必要があります。

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

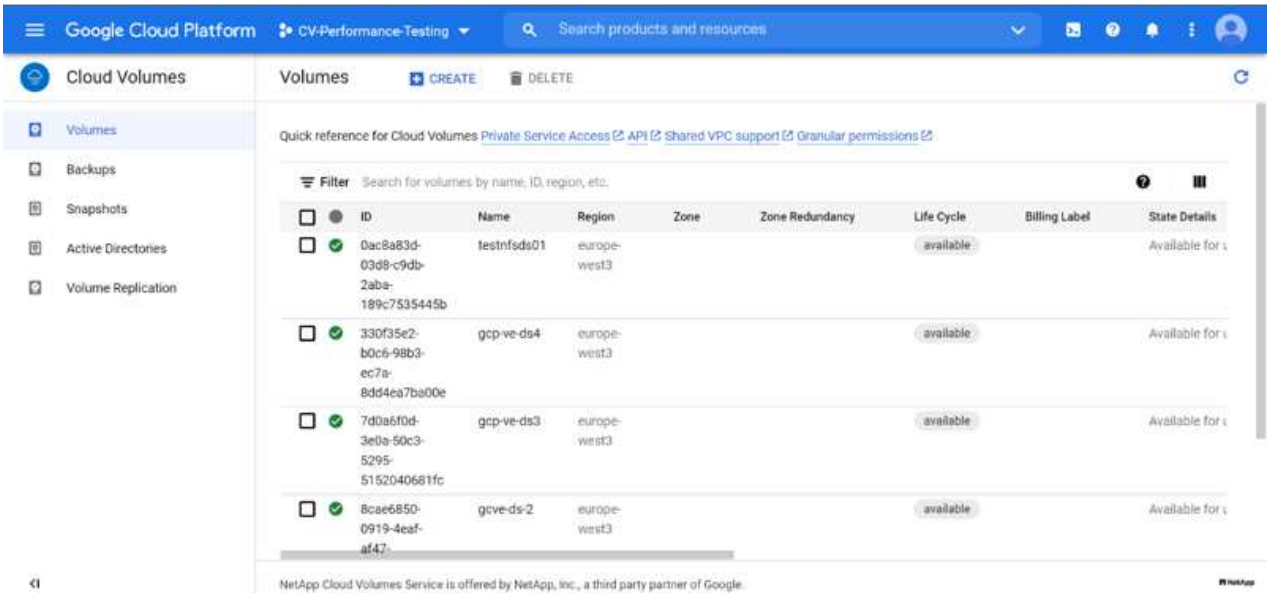
CVS NFS ボリュームを GCVE プライベートクラウドに作成する

NFS ボリュームを作成してマウントするには、次の手順を実行します。

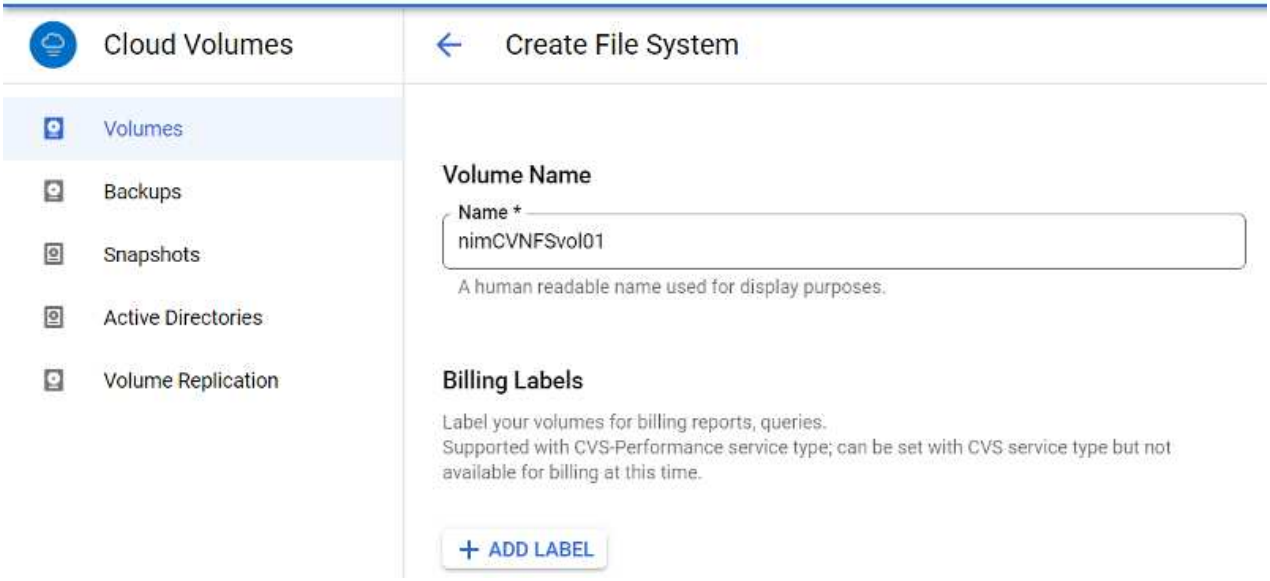
1. Google クラウドコンソール内のパートナーソリューションから Cloud Volume にアクセスします。



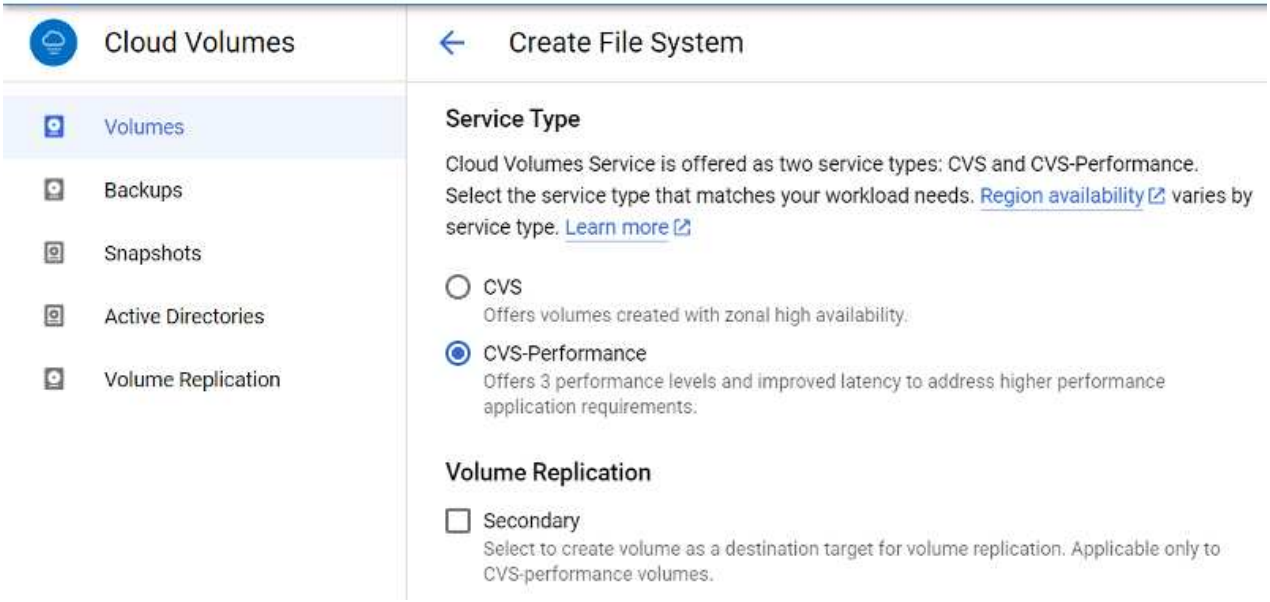
2. Cloud Volume コンソールで、 Volumes （ボリューム）ページに移動し、 Create （作成）をクリックします。



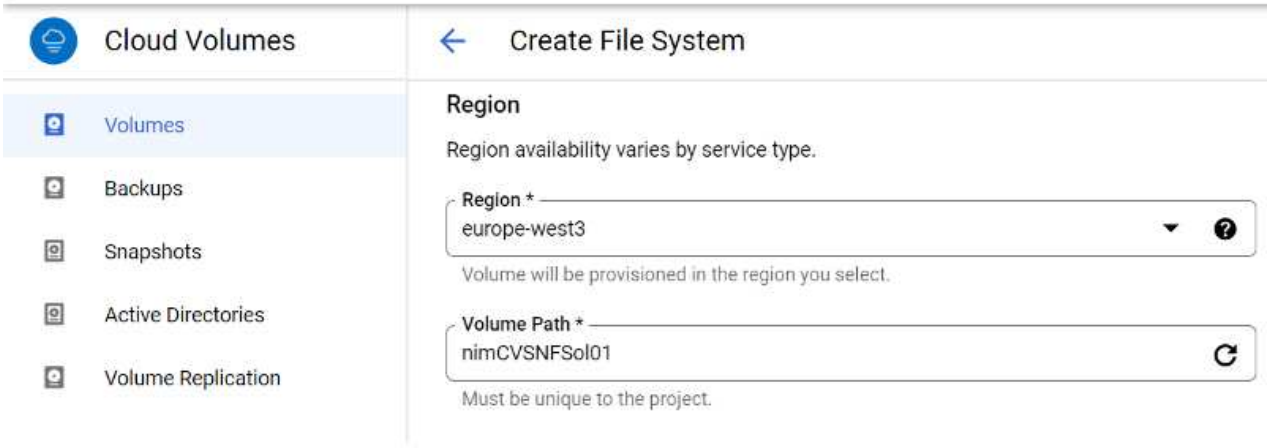
3. [Create File System] ページで、チャージバックメカニズムに必要なボリューム名と課金ラベルを指定します。



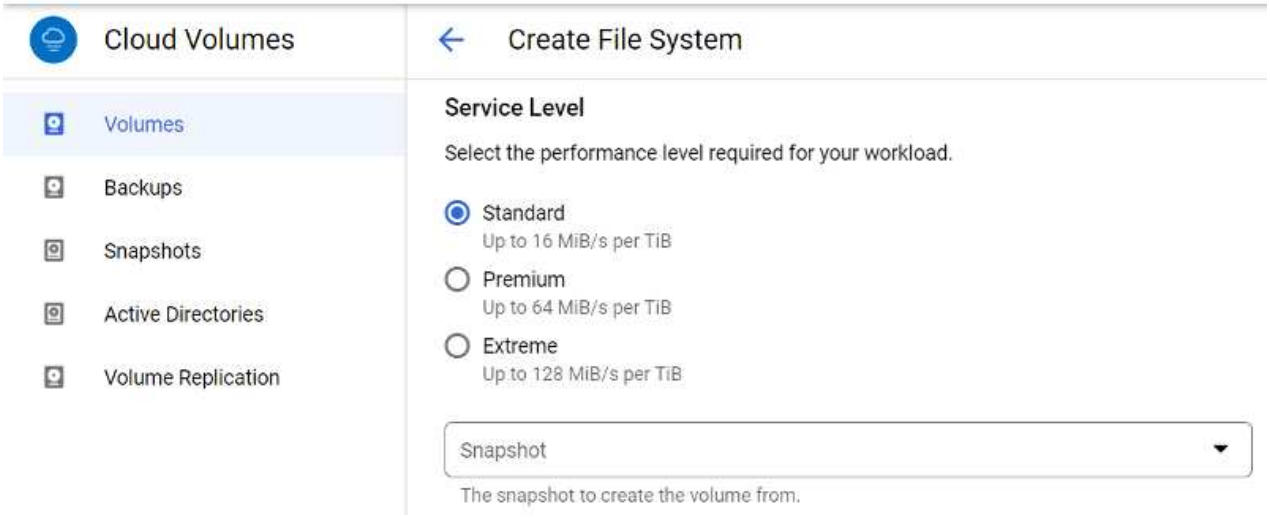
4. 適切なサービスを選択します。GCVE は、 CVS パフォーマンスと希望するサービスレベルを選択して、アプリケーションワークロードの要件に基づいてレイテンシの向上とパフォーマンスの向上を実現します。



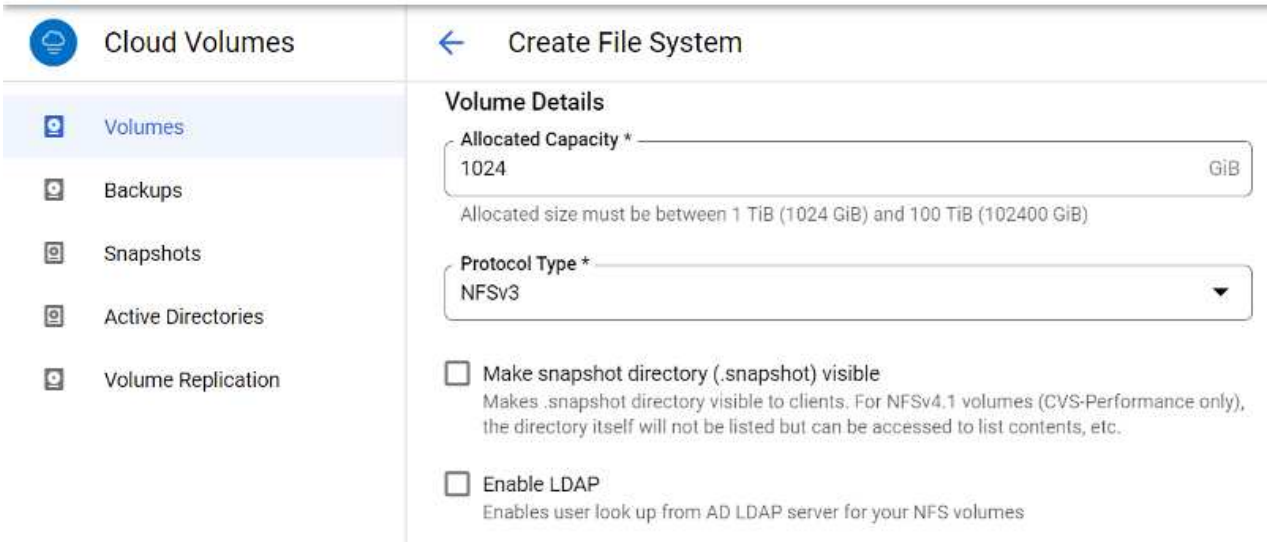
5. ボリュームおよびボリュームパスに Google Cloud のリージョンを指定（プロジェクト内のすべての Cloud Volume でボリュームパスが一意である必要があります）



6. ボリュームのパフォーマンスレベルを選択します。



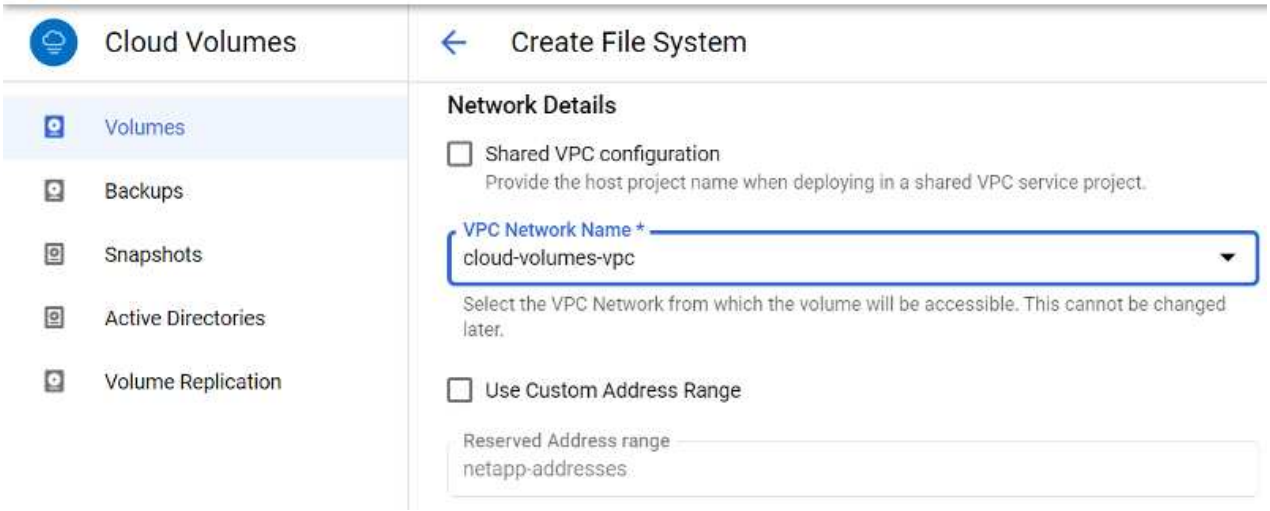
7. ボリュームのサイズとプロトコルのタイプを指定します。このテストでは、 NFSv3 が使用されています。



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

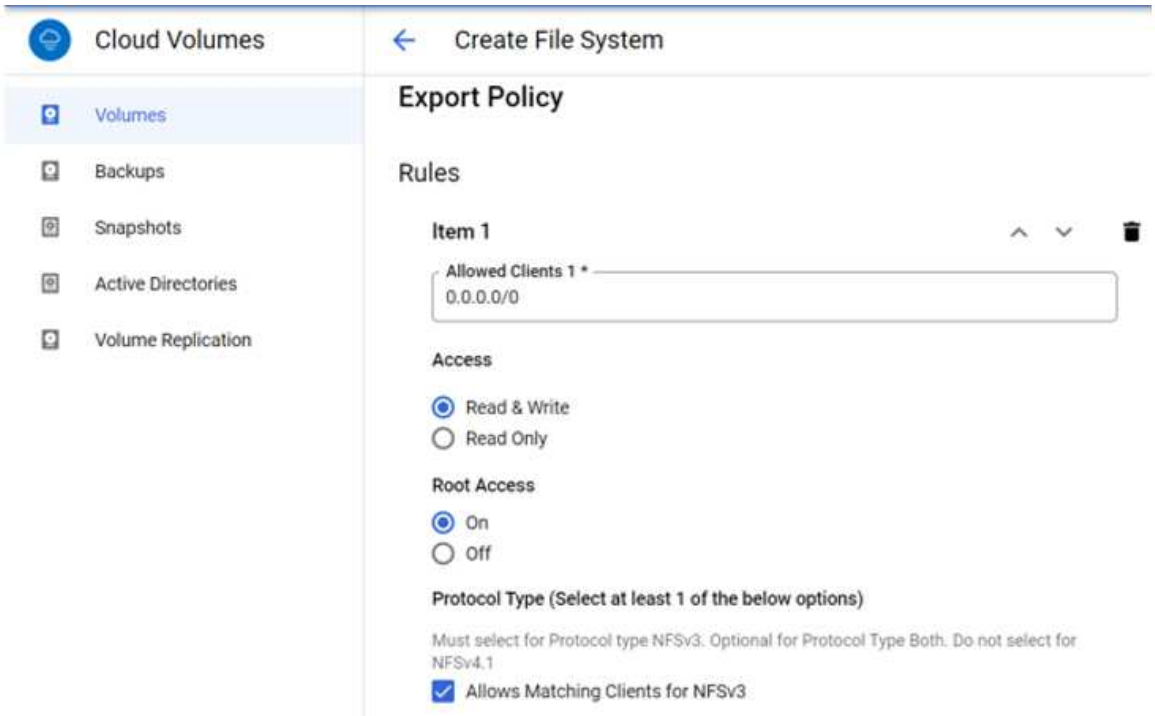
行されていることを確認します。

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



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

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



10. [保存] をクリックしてボリュームを作成します。

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

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

NFS ボリュームをマウントするには、次の手順を実行します。

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

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

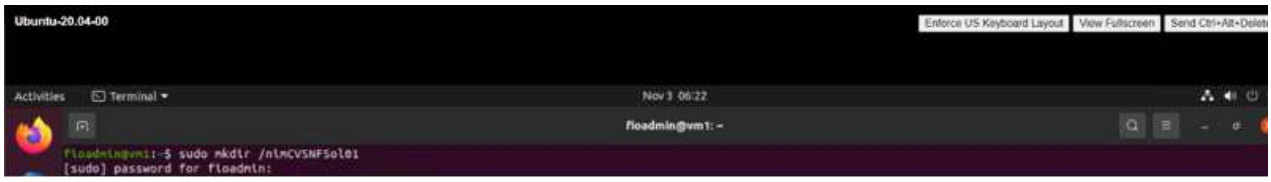
1. SSH クライアントと SSH を使用して仮想マシンに接続します。
2. インスタンスに NFS クライアントをインストールします。
   a. Red Hat Enterprise Linux または SUSE Linux インスタンスの場合：

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

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

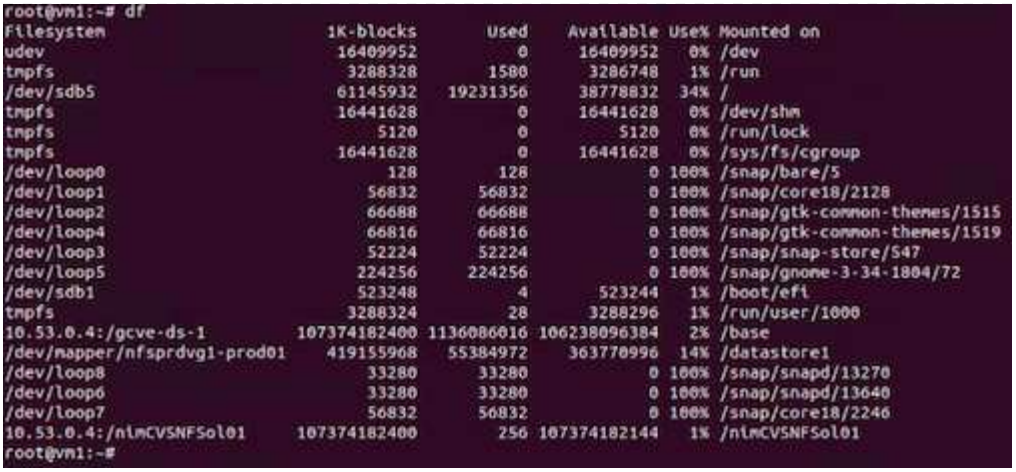
3. 「 /nimCVSNFSol01 」などの新しいディレクトリをインスタンスに作成します。

```
sudo mkdir /nimCVSNFSol01
```



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

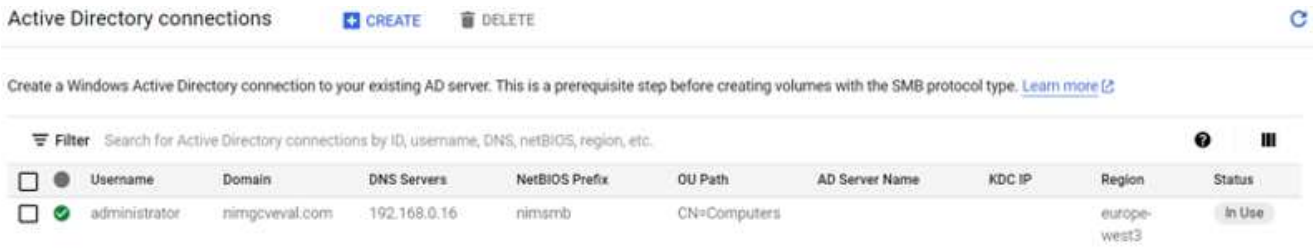
```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp
10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```



```
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/mapper/nfsprdvg1-prod01    419155968    55384972    363770996  14% /datastore1
/dev/loop8                          33280       33280            0 100% /snap/snapd/13270
/dev/loop6                          33280       33280            0 100% /snap/snapd/13640
/dev/loop7                          56832       56832            0 100% /snap/core18/2246
10.53.0.4:/nlmCVSNFSol01      107374182400         256 107374182144   1% /nlmCVSNFSol01
root@vm1:~#
```

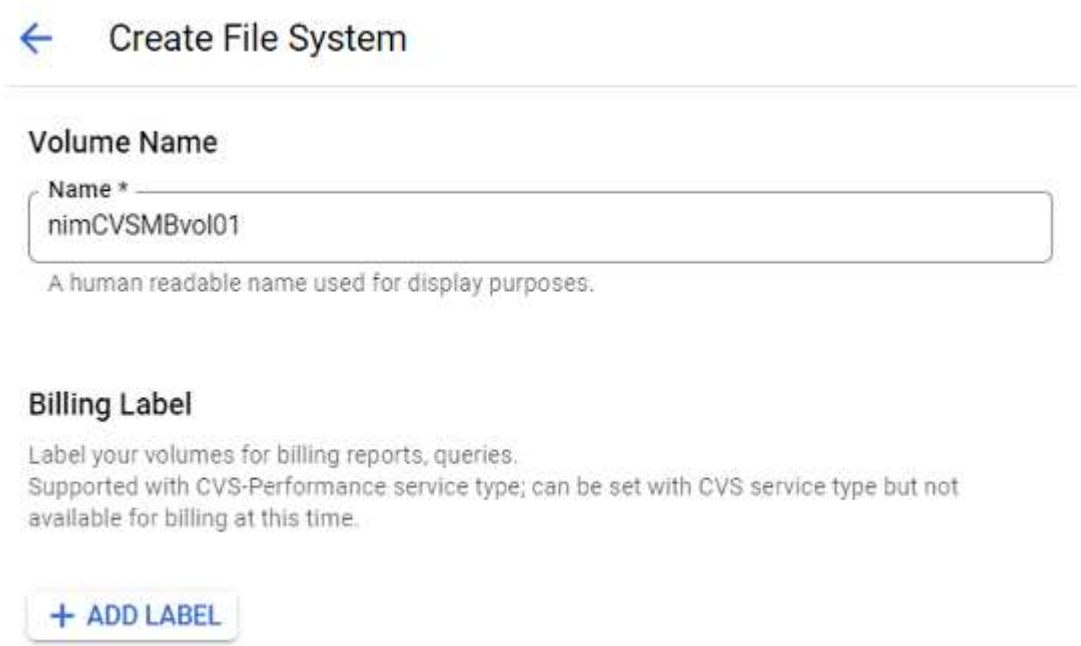
VMware Engine で実行されている **VM** に **SMB** 共有を作成してマウントします

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

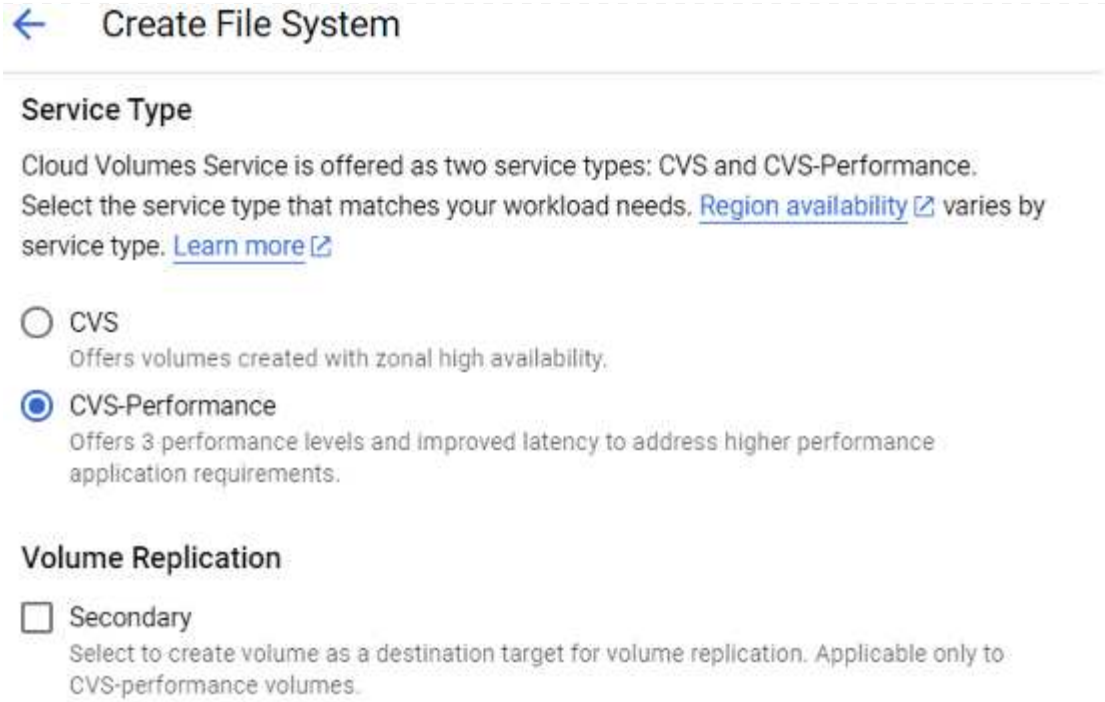


AD 接続が確立されたら、必要なサービスレベルを指定してボリュームを作成します。適切なプロトコルを選択する以外に、 NFS ボリュームを作成する手順は同じです。

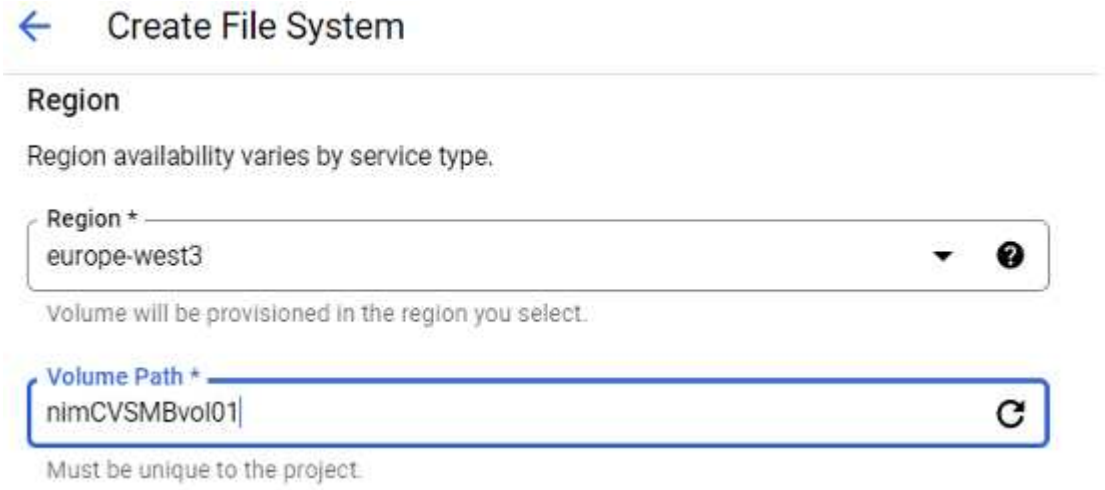
1. Cloud Volume コンソールで、 Volumes （ボリューム）ページに移動し、 Create （作成）をクリックします。
2. [Create File System] ページで、チャージバックメカニズムに必要なボリューム名と課金ラベルを指定します。



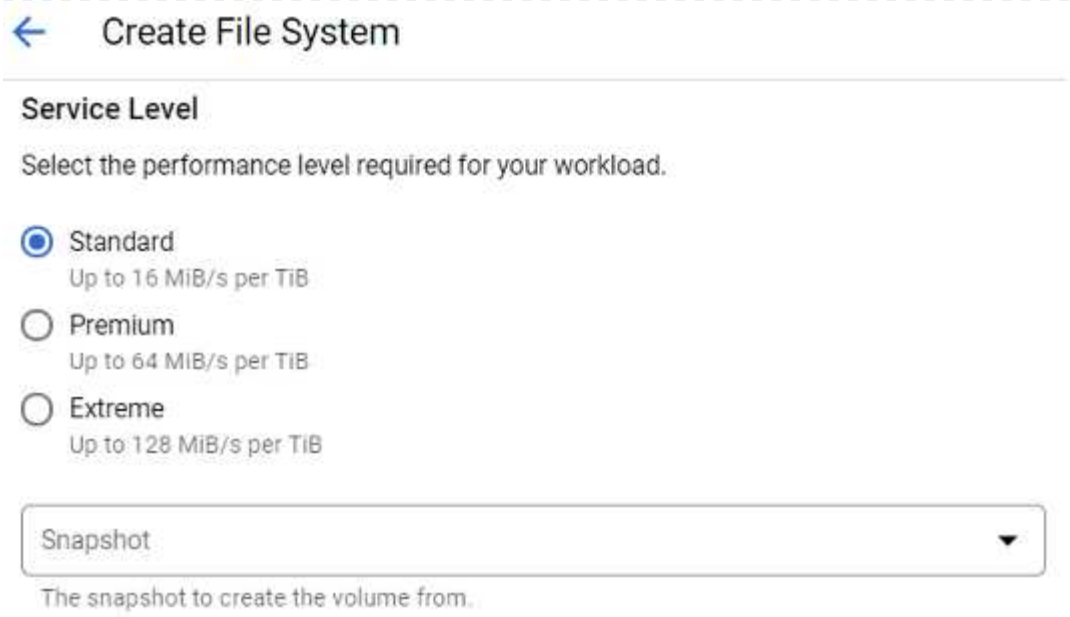
3. 適切なサービスを選択します。GCVE として、 CVS パフォーマンスと希望するサービスレベルを選択し、ワークロード要件に基づいてレイテンシの向上とパフォーマンスの向上を実現します。



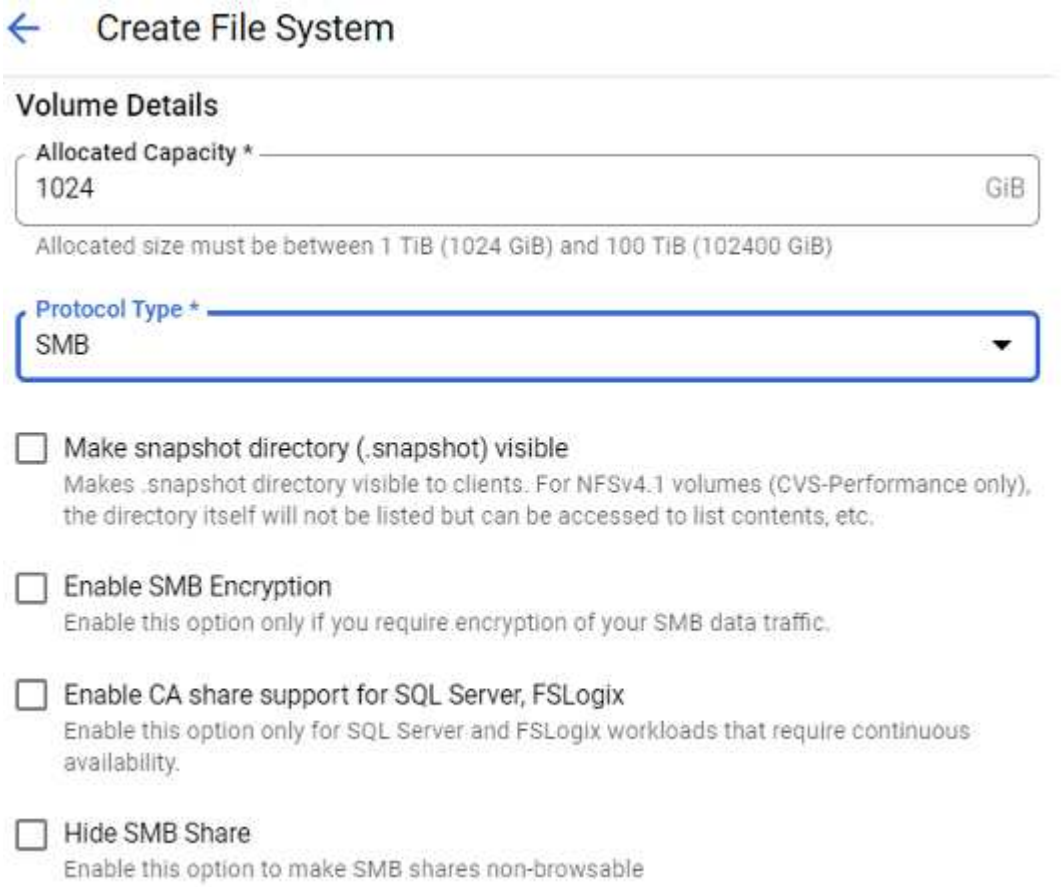
4. ボリュームおよびボリュームパスに Google Cloud のリージョンを指定（プロジェクト内のすべての Cloud Volume でボリュームパスが一意である必要があります）



5. ボリュームのパフォーマンスレベルを選択します。



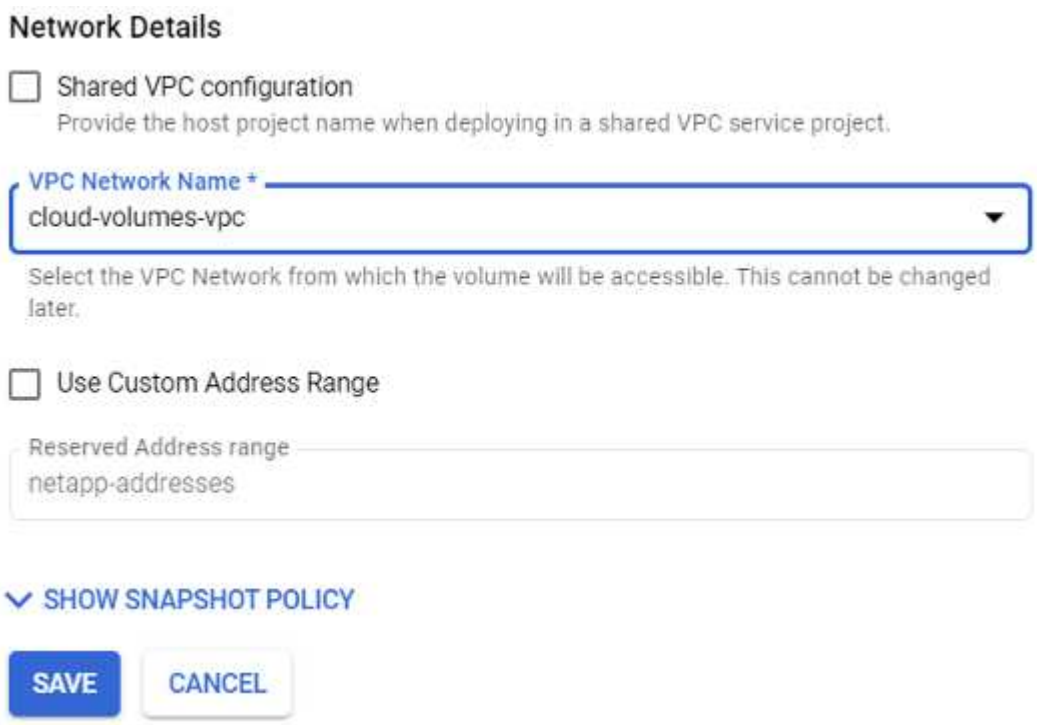
6. ボリュームのサイズとプロトコルのタイプを指定します。このテストでは、 SMB を使用します。



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

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

合は、こちらを参照してください "手順"。



8. [保存] をクリックしてボリュームを作成します。

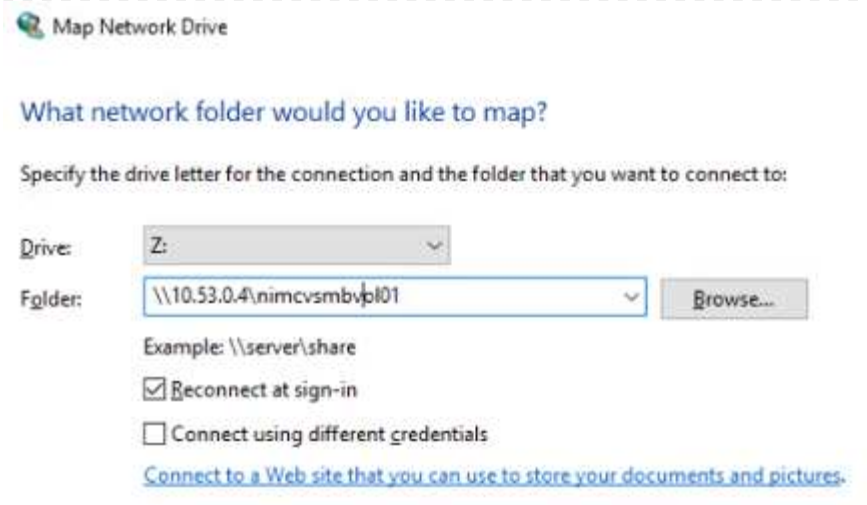
SMB ボリュームをマウントするには、次の手順を実行します。

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

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

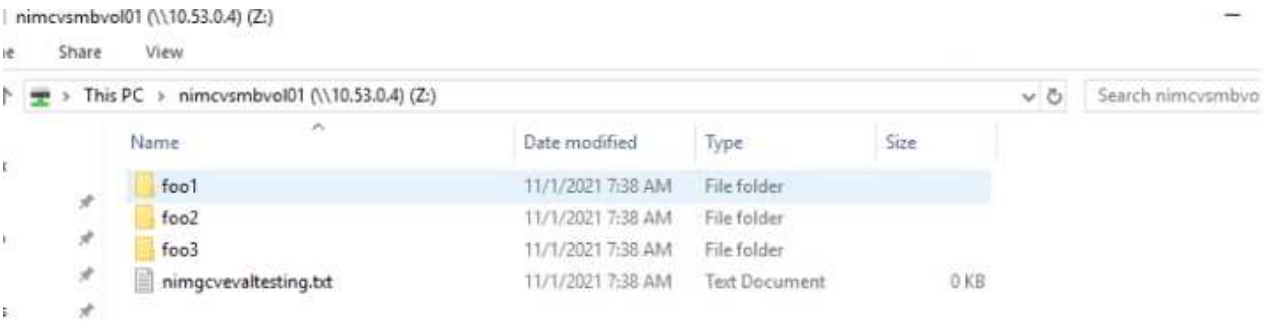
1. [スタート] ボタンをクリックし、 [コンピュータ] をクリックします。
2. [ネットワークドライブの割り当て] をクリックします。
3. [ドライブ] リストで、使用可能な任意のドライブ文字をクリックします。
4. フォルダボックスに、次のように入力します。

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



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

5. 完了をクリックします。



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

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

AWSリージョンの可用性

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

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

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

ータストアとして示します。

南北アメリカ

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

最終更新日：2022年6月2日

EMEAの場合

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

最終更新日：2022年6月2日

アジア太平洋地域

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

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

最終更新日：2022年9月28日

Azureリージョンの可用性

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

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

GCPリージョンのアベイラビリティ

GCPリージョンのアベイラビリティは、GCPがパブリックアベイラビリティに移行するとリリースされます。

まとめ：**VMware**を使用したネットアップのハイブリッドマルチクラウドが選ばれる理由とは

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

ユースケース **1** ：ストレージの最適化

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

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

ユースケース **2** ：クラウドへの移行

企業は、次のような理由から、オンプレミスのデータセンターからパブリッククラウドへのアプリケーション移行を迫られています。設備投資（ CAPEX ）から運用コスト（ OPEX ）に移行するための資金調達ディレ

クティブや、すべてをクラウドへ移行するというトップダウンの指示など、さまざまな理由があります。

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

ユースケース **3** ：データセンターの拡張

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

ユースケース **4** ：クラウドへのディザスタリカバリ

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

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

ユースケース **5** ：アプリケーションの最新化

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

まとめ

オールクラウドとハイブリッドクラウドのどちらをターゲットとしている場合でも、 NetApp Cloud Volume は、アプリケーションワークロードを導入、管理するための優れたオプションを提供し、ファイルサービスとブロックプロトコルに加えて、データ要件をアプリケーションレイヤとシームレスにすることで TCO を削減します。

どのようなユースケースでも、任意のクラウドやハイパースケーラを NetApp Cloud Volume と組み合わせることで、オンプレミスと複数のクラウドにわたるクラウドのメリット、一貫したインフラ、運用、ワークロードの双方向の移動、エンタープライズクラスの容量とパフォーマンスを迅速に実現できます。

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

VMware ハイブリッドクラウドのユースケース

VMwareを使用したネットアップハイブリッドマルチクラウドのユースケース

ハイブリッドクラウドまたはクラウドファーストの導入を計画する際に IT 組織にとって重要なユースケースの概要。

一般的なユースケース

ユースケースには次のものがあり

- ディザスタリカバリ、 SVM
- データセンターのメンテナンス時にワークロードをホストする。 * ローカルのデータセンターでプロビジョニングされたリソース以外に追加のリソースが必要になる、迅速なバースト。
- VMware サイトの拡張
- クラウドへの迅速な移行
- 開発 / テスト、および
- クラウドの補助的なテクノロジーを活用したアプリケーションの最新化。

このドキュメントでは、VMwareのユースケースを使用してクラウドワークロードの参考資料について詳しく説明します。ユースケースは次のとおりです。

- 保護（ディザスタリカバリとバックアップ/リストアの両方を含む）
- 移動
- 拡張

IT の旅の中で

ほとんどの組織は、変革と最新化への移行を進めています。このプロセスの一環として、企業は既存の VMware への投資を活用しながら、クラウドのメリットを活用し、移行プロセスをできるだけシームレスに実行する方法を模索しています。このアプローチでは、データがすでにクラウドにあるため、最新化への取り組みが非常に簡単になります。

このシナリオに最も簡単に使用できる回答は、各ハイパースケーラにおける VMware ソリューションです。ネットアップの Cloud Volume と同様に、 VMware はオンプレミスの VMware 環境を任意のクラウドに移行または拡張できるため、既存のオンプレミスの資産、スキル、ツールを保持しながら、ワークロードをクラウド内でネイティブに実行できます。これにより、サービスの中断や IP 変更の必要性がなくなり、 IT チームは既存のスキルやツールを使用してオンプレミスで行う方法を運用できるようになるため、リスクが軽減されます。これにより、クラウドへの移行が高速化され、ハイブリッドマルチクラウドアーキテクチャへの移行が大幅にスムーズになります。

NFS追加ストレージオプションの重要性を理解する

あらゆるクラウドでVMwareが提供する独自のハイブリッド機能に加えて、NFSストレージオプションの追加によってストレージ負荷の高い組織での有用性が制限されています。ストレージはホストに直接関連付けられているため、ストレージを拡張する唯一の方法は、ホストを追加することです。これにより、ストレージを大量に消費するワークロードの場合、 35 ～ 40% 以上のコストがかかる可能性があります。このようなワークロードに必要なストレージ容量は増えても容量は増えません。つまり、追加のホストに料金を支払うことにな

ります。

次のシナリオを考えてみましょう。

CPU とメモリ用にわずか 5 台のホストが必要ですが、ストレージには多くのニーズがあり、ストレージ要件を満たすために 12 台のホストが必要です。この要件は、ストレージを増設するだけで追加の処理能力を購入する必要があるため、財務面での拡張性に大きな転換を実現できます。

クラウドの導入と移行を計画する場合は、最適なアプローチを評価し、投資の総削減に最も簡単な方法をとることが常に重要です。あらゆるアプリケーション移行で最も一般的かつ簡単なアプローチは、仮想マシン（ VM ）やデータ変換がない場所でリホスト（リフトアンドシフト）を行うことです。NetApp Cloud Volume と VMware の Software-Defined Data Center （ SDDC ）を併用し、 vSAN を補完することで、移行と切り替えが容易になります。

Amazon VMware マネージドクラウド（ **VMC** ）向けネットアップソリューション

ネットアップがAWSに提供するソリューションの詳細をご確認ください。

VMwareは、クラウドワークロードを次の3つのカテゴリのいずれかに分類します。

- 保護（ディザスタリカバリとバックアップ/リストアの両方を含む）
- 移動
- 拡張

次のセクションで使用可能なソリューションを参照してください。

保護

- "AWS上のVMCを使用したディザスタリカバリ（ゲスト接続）"
- "FSx for ONTAP を使用したVMCでのVeeamバックアップとリストア"
- "FSXを使用したONTAP およびVMC向けディザスタリカバリ（DRO）"
- "Veeam ReplicationとFSx for ONTAPを使用したVMware Cloud on AWSへのディザスタリカバリ"

移動

- "VMware HCXを使用して、ワークロードをFSxNデータストアに移行します"

拡張

近日公開！

Azure VMware 解決策（ **AVS** ）向けネットアップソリューション

ネットアップがAzureにもたらすソリューションの詳細をご確認ください。

VMwareは、クラウドワークロードを次の3つのカテゴリのいずれかに分類します。

- 保護（ディザスタリカバリとバックアップ/リストアの両方を含む）
- 移動

- 拡張

次のセクションで使用可能なソリューションを参照してください。

保護

- "ANFおよびJetStreamを使用したディザスタリカバリ（補足的なNFSデータストア）"
- "ANFおよびCVOを使用したディザスタリカバリ（ゲスト接続ストレージ）"
- "ANFとAVSを使用したディザスタリカバリ（DRO）"
- "Veeam ReplicationとAzure NetApp Filesデータストアを使用したAzure VMware解決策へのディザスタリカバリ"

移動

- "VMware HCXを使用して、ワークロードをAzure NetApp Files データストアに移行します"

拡張

近日公開！

Google Cloud VMware Engine（GCVE）向けNetAppソリューション

ネットアップがGCPに提供するソリューションの詳細をご確認ください。

VMwareは、クラウドワークロードを次の3つのカテゴリのいずれかに分類します。

- 保護（ディザスタリカバリとバックアップ/リストアの両方を含む）
- 移動
- 拡張

次のセクションで使用可能なソリューションを参照してください。

保護

- "SnapCenter 、Cloud Volumes ONTAP 、Veeamレプリケーションを使用したアプリケーションディザスタリカバリ"
- "NetApp SnapCenterとVeeamによるGCVE上のNetApp CVSへのレプリケーションを使用した、アプリケーションと整合性のあるディザスタリカバリ"

移動

- "VMware HCXを使用したNetApp Cloud Volume Service NFSデータストアへのワークロードの移行"
- "Veeamを使用したNetAppクラウドボリュームサービスNFSデータストアへのVMレプリケーション"

拡張

近日公開！

ネットアップの **AWS VMC** 向け機能

ネットアップがAWS VMware Cloud（VMC）にもたらす機能の詳細をご確認ください。ネットアップのゲスト接続ストレージデバイスやNFSデータストアを追加で提供し、ワークフローの移行、クラウドへの拡張/バースト対応、バックアップ/リストア、ディザスタリカバリを実現します。

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。

- "AWS で VMC を設定しています"
- "VMC のネットアップストレージオプション"
- "ネットアップとVMwareのクラウドソリューション"

AWS で **VMC** を設定しています

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

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

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

セットアッププロセスは、次の手順に分けることができます。

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

詳細を表示します "VMCの設定手順"。

VMC のネットアップストレージオプション

ネットアップストレージは、AWS VMC内で、接続されている推測データストアまたはNFSデータストア補助的なデータストアとして、いくつかの方法で利用できます。

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

AWS は、次の構成でネットアップストレージをサポートします。

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

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

解決策のユースケース

ネットアップと VMware のクラウドソリューションを使用すれば、多くのユースケースを AWS VMC に簡単に導入できます。ユースケースは、VMwareが定義したクラウド領域ごとに定義されます。

- 保護（ディザスタリカバリとバックアップ/リストアの両方を含む）
- 拡張
- 移動

"ネットアップの AWS VMC 向けソリューションをご覧ください"

AWS / VMCのワークロードを保護

TR-4931：『Disaster Recovery with VMware Cloud on Amazon Web Services and Guest Connect』

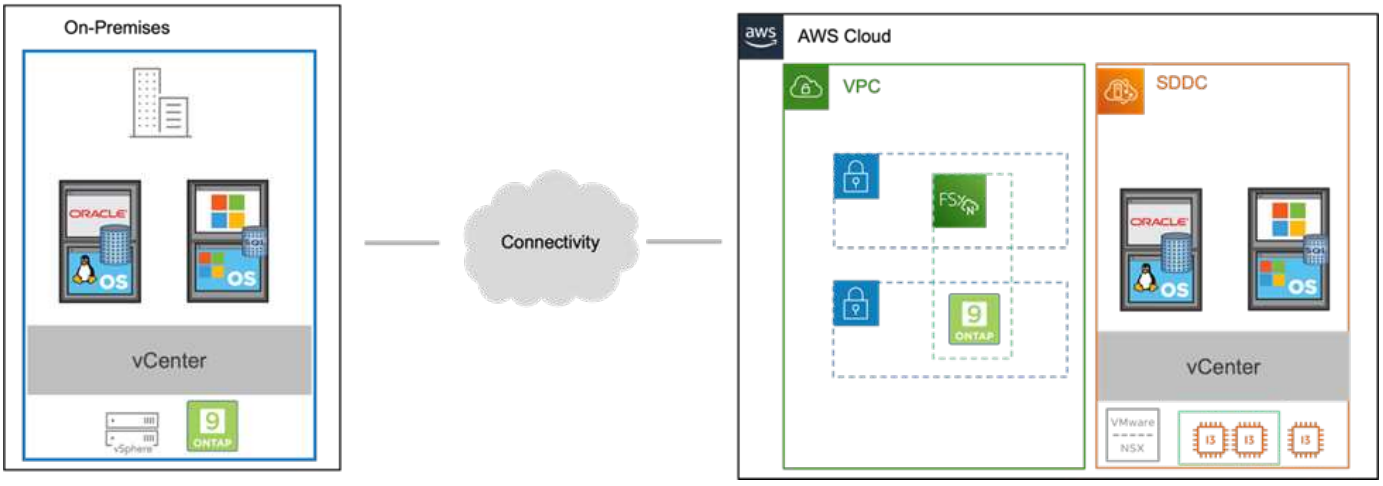
執筆者：Chris Reno、Josh Powell、Suresh Thoppay - NetApp Solutions Engineering

概要

大規模な障害が発生した場合にビジネスクリティカルなアプリケーションを迅速にリストアできるようにするには、実績のあるディザスタリカバリ（DR）環境と計画が不可欠です。この解決策 では、オンプレミスとVMware Cloud on AWSの両方で、VMwareとネットアップのテクノロジを中心にDRのユースケースを紹介します。

ネットアップはVMwareとの長年の統合を実現してきました。これは、仮想環境のストレージパートナーとしてネットアップを選んだ何万ものお客様から証明されています。この統合は、クラウドのゲスト接続オプションのほか、NFSデータストアとの最近の統合とも連動します。この解決策 では、一般にゲスト接続ストレージと呼ばれるユースケースを取り上げます。

ゲスト接続ストレージでは、ゲストVMDKはVMwareでプロビジョニングされたデータストアに導入され、アプリケーションデータはiSCSIまたはNFSに格納されてVMに直接マッピングされます。次の図に示すように、OracleおよびMS SQLアプリケーションを使用してDRシナリオを検証します。



前提条件、前提条件、コンポーネントの概要

この解決策 を導入する前に、コンポーネントの概要、解決策 を導入するための前提条件、およびこの解決策のドキュメント化に記載した前提条件を確認してください。

"DR解決策 の要件、事前要件、計画"

SnapCenter を使用してDRを実行する

この解決策 では、SnapCenter は、SQL ServerおよびOracleアプリケーションデータ用に、アプリケーションと整合性のあるSnapshotを提供します。この構成とSnapMirrorテクノロジを組み合わせることで、オンプレミスのAFF とFSX ONTAP クラスタ間で高速なデータレプリケーションを実現できます。また、Veeam Backup & Replicationは、仮想マシンのバックアップとリストア機能も提供します。

ここでは、バックアップとリストアの両方について、SnapCenter 、SnapMirror、およびVeeamの構成について説明します。

次のセクションでは、セカンダリサイトでフェイルオーバーを完了するために必要な設定と手順について説明します。

SnapMirror関係と保持スケジュールを設定

SnapCenter では、長期のアーカイブと保持を目的として、プライマリストレージシステム（primary > mirror ）およびセカンダリストレージシステム（primary > vault）内のSnapMirror関係を更新できます。そのためには、SnapMirrorを使用して、デスティネーションボリュームとソースボリューム間のデータレプリケーション関係を確立して初期化する必要があります。

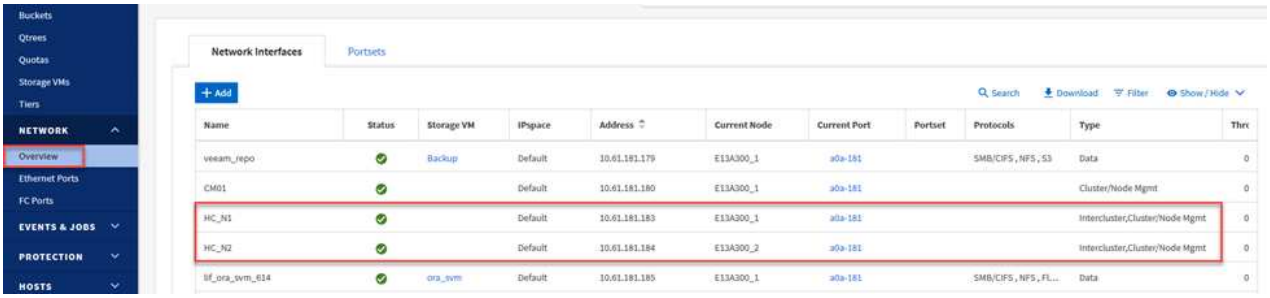
ソースとデスティネーションのONTAP システムが、Amazon VPCピアリング、トランジットゲートウェイ、AWS Direct Connect、またはAWS VPNを使用してピア関係にあるネットワークに配置されている必要があります。

オンプレミスのONTAP システムとFSX ONTAP 間にSnapMirror関係を設定するには、次の手順を実行する必要があります。

を参照してください "FSX for ONTAP –ONTAP ユーザーガイド" FSXを使用したSnapMirror関係の作成の詳細については、を参照してください。

オンプレミスにあるソースONTAP システムの場合、クラスタ間LIFの情報をSystem ManagerまたはCLIから取得できます。

1. ONTAP System Managerで、ネットワークの概要ページに移動し、タイプ：クラスタ間のIPアドレスを取得します。このIPアドレスは、FSXがインストールされているAWS VPCと通信するように設定されています。



2. FSXのクラスタ間IPアドレスを取得するには、CLIにログインして次のコマンドを実行します。

```
FSx-Dest::> network interface show -role intercluster
```

```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
FsxId0ae40e08acc0dea67
            inter_1      up/up    172.30.15.42/25    FsxId0ae40e08acc0dea67-01
                                                                   e0e     true
            inter_2      up/up    172.30.14.28/26    FsxId0ae40e08acc0dea67-02
                                                                   e0e     true
2 entries were displayed.
```

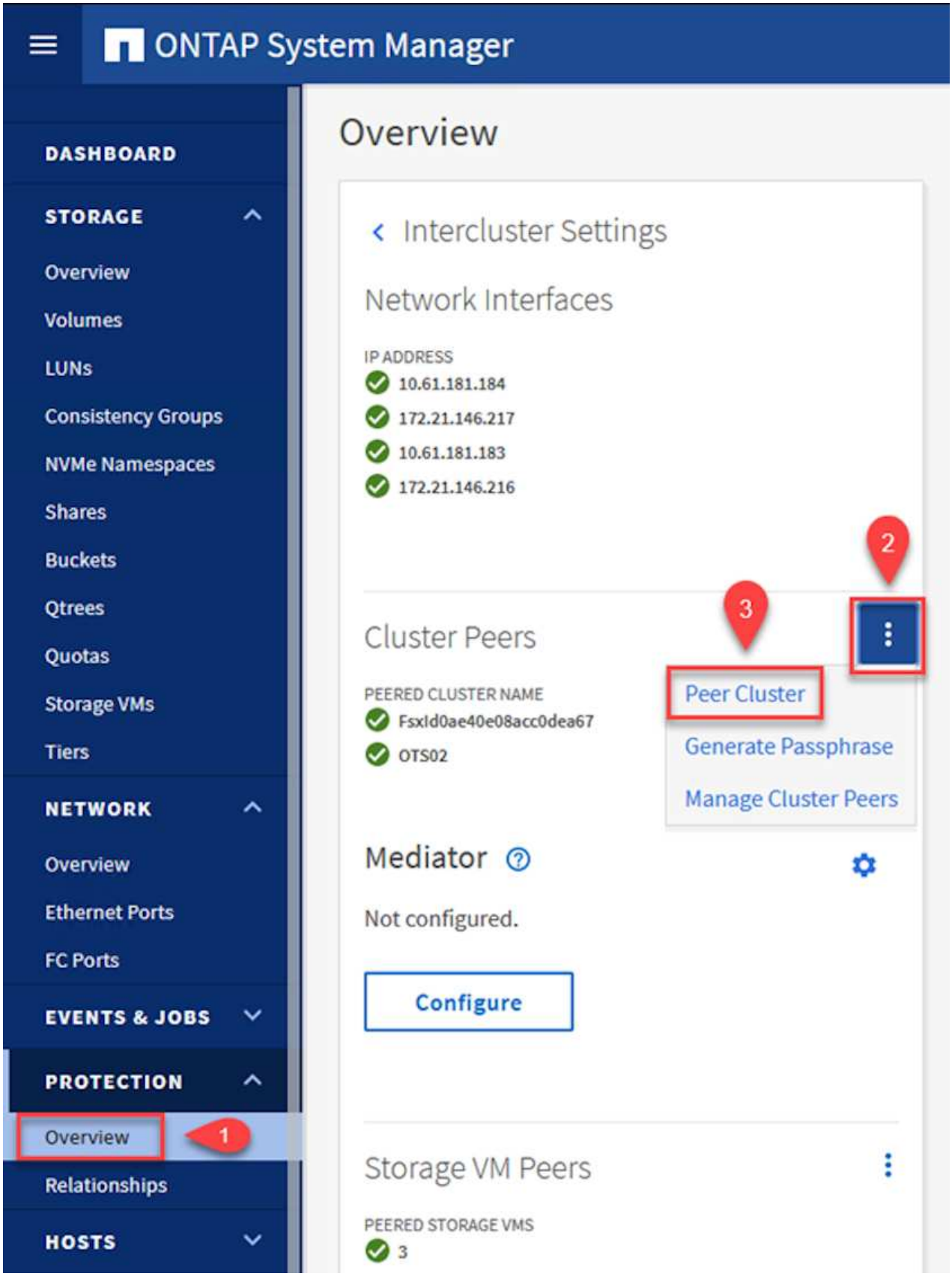
ONTAP とFSXの間にクラスタピアリングを確立します

ONTAP クラスタ間のクラスタピアリングを確立するには、開始側のONTAP クラスタで入力した一意のパスフレーズを、もう一方のピアクラスタで確認する必要があります。

1. デスティネーションFSXクラスタ上で' cluster peer createコマンドを使用してピアリングを設定しますプロンプトが表示されたら、あとでソースクラスタで使用する一意のパスフレーズを入力して作成プロセスを完了します。

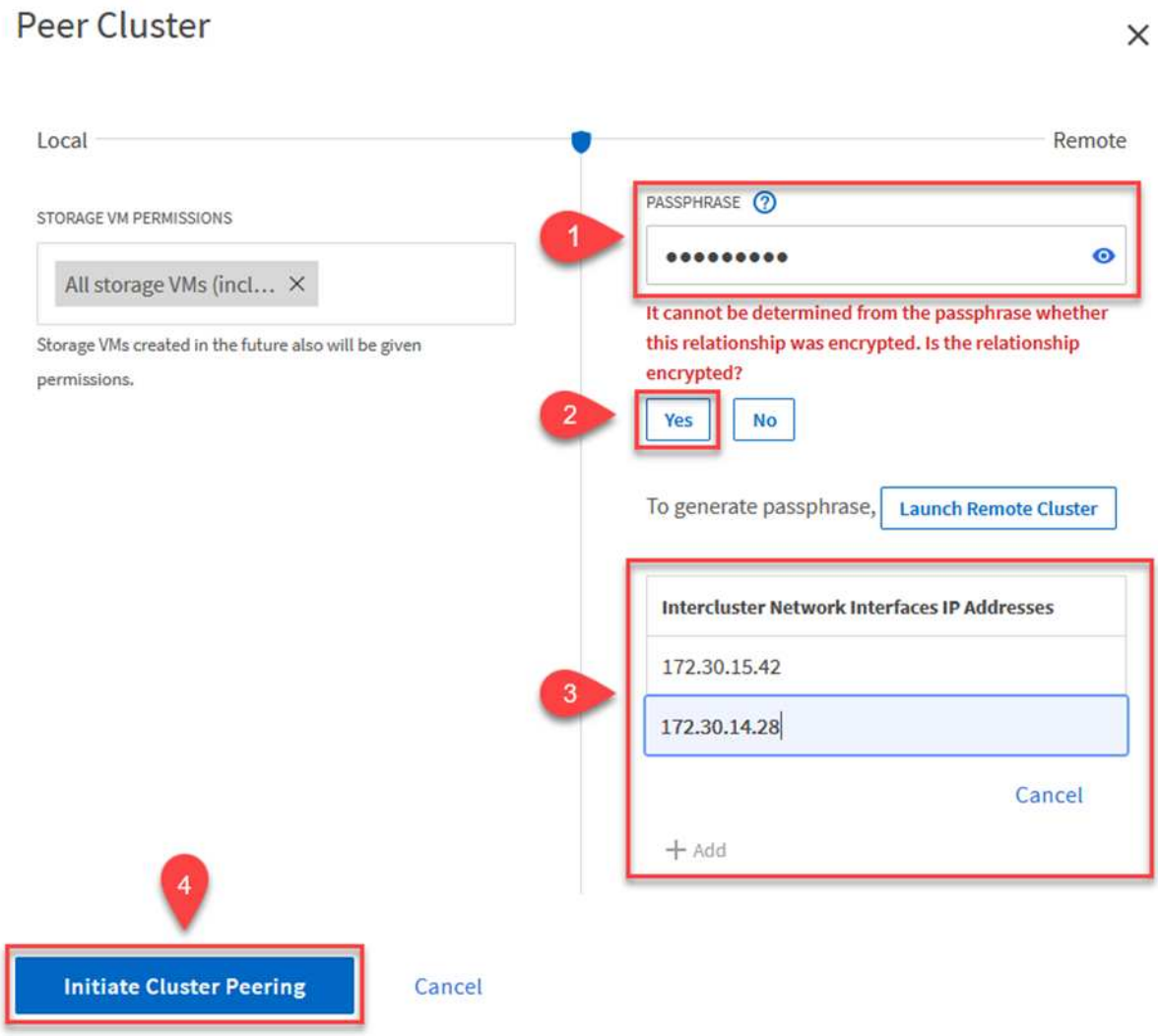
```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. ソースクラスタでは、ONTAP System ManagerまたはCLIを使用してクラスタピア関係を確立できます。ONTAP System Managerで、Protection > Overviewの順に選択し、Peer Clusterを選択します。



3. Peer Cluster（ピアクラスタ）ダイアログボックスで、必要な情報を入力します。
   a. デスティネーションFSXクラスタでピアクラスタ関係を確立するために使用したパスフレーズを入力します。

b. [はい]を選択して'暗号化された関係を確立します
c. デスティネーションFSXクラスタのクラスタ間LIFのIPアドレスを入力します。
d. クラスタピアリングの開始をクリックしてプロセスを完了します。



4. 次のコマンドを使用して、FSXクラスタからクラスタピア関係のステータスを確認します。

```
FSx-Dest::> cluster peer show
```

```
FsxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability   Authentication
------------------------- --------------------- -------------- --------------
E13A300                   1-80-000011           Available      ok
```

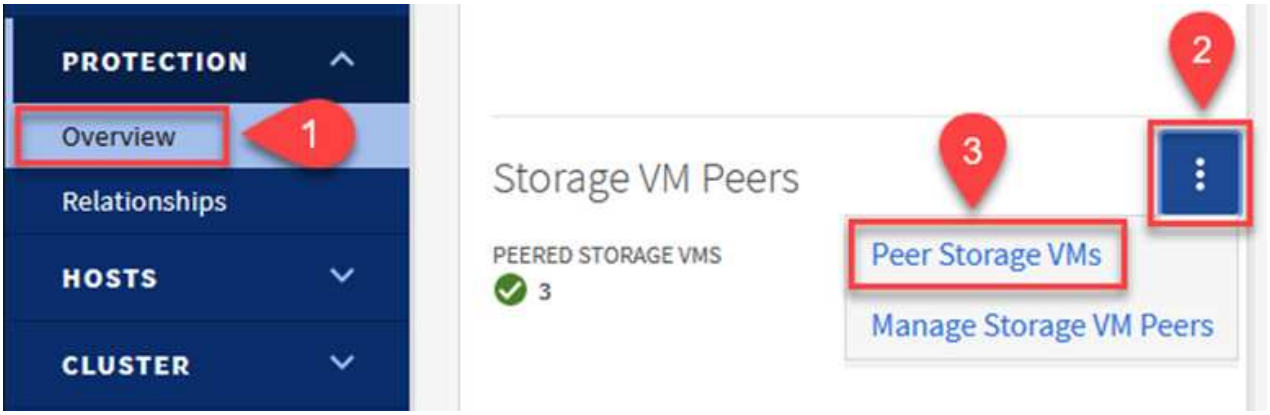
SVMピア関係を確立する

次の手順では、SnapMirror関係にあるボリュームを含むデスティネーションとソースのStorage Virtual Machineの間にSVM関係をセットアップします。

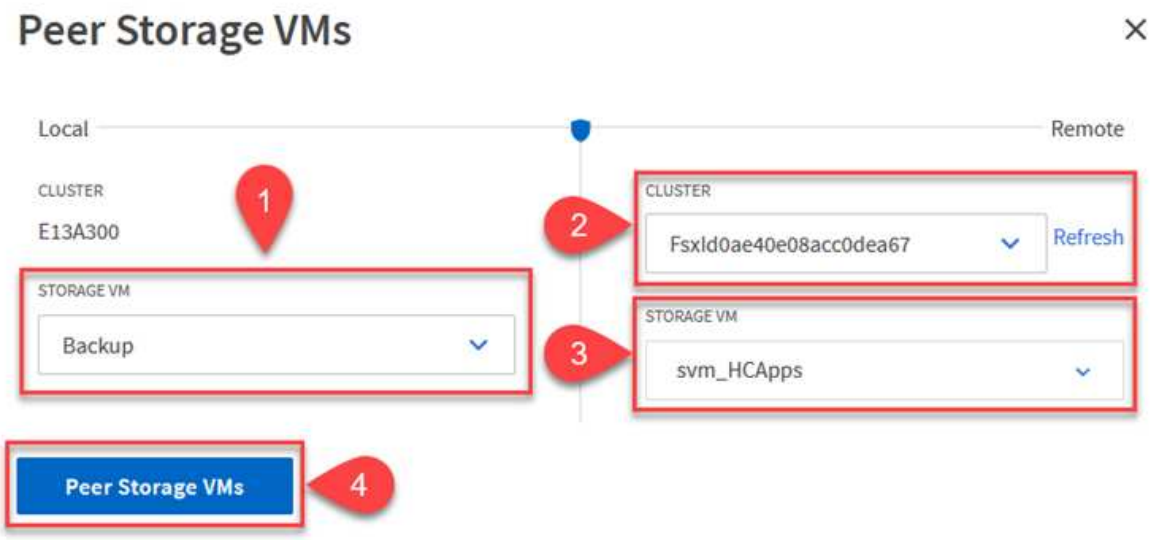
1. ソースFSXクラスタから、CLIから次のコマンドを使用して、SVMピア関係を作成します。

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. ソースONTAP クラスタで、ONTAP System ManagerまたはCLIのいずれかを使用してピアリング関係を承認します。
3. ONTAP System Managerで、保護>概要に移動し、Storage VMピアの下にあるピアStorage VMを選択します。



4. Peer Storage VMダイアログボックスで、次のフィールドに入力します。
   - ソースStorage VM
   - デスティネーションクラスタ
   - デスティネーションStorage VM



5. [Peer Storage VMs]をクリックして、SVMピアリングプロセスを完了します。

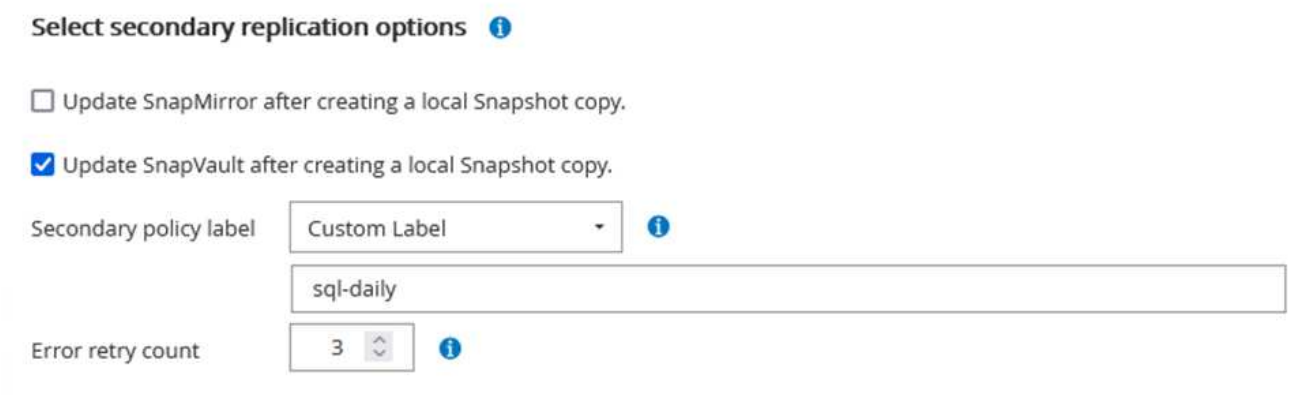
Snapshot保持ポリシーを作成します

SnapCenter は、プライマリストレージシステムにSnapshotコピーとして存在するバックアップの保持スケジュールを管理します。これは、SnapCenter でポリシーを作成するときに確立されます。SnapCenter では、セカンダリストレージシステムに保持されるバックアップの保持ポリシーは管理されません。これらのポリシーは、セカンダリFSXクラスタで作成されたSnapMirrorポリシーを使用して個別に管理され、ソースボリュームとSnapMirror関係にあるデスティネーションボリュームに関連付けられます。

SnapCenter ポリシーを作成するときに、SnapCenter バックアップの作成時に生成される各SnapshotのSnapMirrorラベルに追加するセカンダリポリシーラベルを指定できます。

セカンダリストレージでは、Snapshotを保持するために、これらのラベルがデスティネーションボリュームに関連付けられたポリシールールと照合されます。

次の例は、SQL Serverデータベースおよびログボリュームの日次バックアップに使用するポリシーの一部として生成されたすべてのSnapshotに適用されるSnapMirrorラベルを示しています。



SQL ServerデータベースのSnapCenter ポリシーの作成の詳細については、を参照してください "SnapCenter のドキュメント"。

まず、保持するSnapshotコピーの数にルールを指定してSnapMirrorポリシーを作成する必要があります。

1. FSXクラスタ上にSnapMirrorポリシーを作成します。

```
FSx-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. SnapCenter ポリシーで指定されたセカンダリポリシーラベルと一致するSnapMirrorラベルを持つルールをポリシーに追加します。

```
FSx-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

次のスクリプトは、ポリシーに追加できるルールの例を示しています。

```
FSx-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy
Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

SnapMirrorラベルごとに追加のルールを作成し、保持するSnapshotの数（保持期間）を指定します。

デスティネーションボリュームを作成

ソースボリュームからSnapshotコピーの受信者となるデスティネーションボリュームをFSX上に作成するには、FSX ONTAP 上で次のコマンドを実行します。

```
FSx-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

ソースボリュームとデスティネーションボリューム間に**SnapMirror**関係を作成します

ソースボリュームとデスティネーションボリューム間のSnapMirror関係を作成するには、FSX ONTAP で次のコマンドを実行します。

```
FSx-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

SnapMirror関係を初期化

SnapMirror関係を初期化このプロセスにより、ソースボリュームから生成された新しいSnapshotが開始され、デスティネーションボリュームにコピーされます。

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

Windows SnapCenter サーバをオンプレミスに導入して設定

Windows SnapCenter Serverをオンプレミスに導入

この解決策 では、NetApp SnapCenter を使用して、アプリケーションと整合性のあるSQL Serverデータベースのバックアップを作成します。仮想マシンのVMDKをバックアップするVeeam Backup & Replicationと併用することで、オンプレミスのデータセンターとクラウドベースのデータセンター向けに包括的なディザスタリカバリ解決策 を実現できます。

SnapCenter ソフトウェアはネットアップサポートサイトから入手でき、ドメインまたはワークグループ内にあるMicrosoft Windowsシステムにインストールできます。詳細な計画ガイドとインストール手順については、を参照してください "ネットアップドキュメントセンター"。

SnapCenter ソフトウェアは、から入手できます "リンクをクリックしてください"。

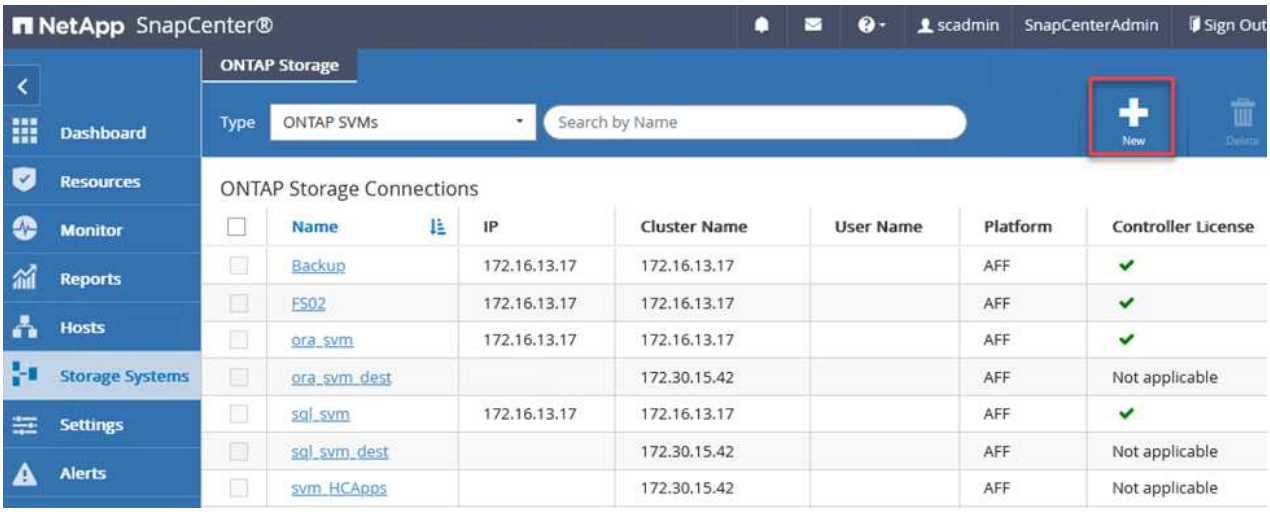
インストール後、\\ https://Virtual_Cluster_IP_or_FQDN:8146_を使用してWebブラウザからSnapCenterコンソールにアクセスできます。

コンソールにログインしたら、バックアップSQL ServerおよびOracleデータベース用にSnapCenter を設定する必要があります。

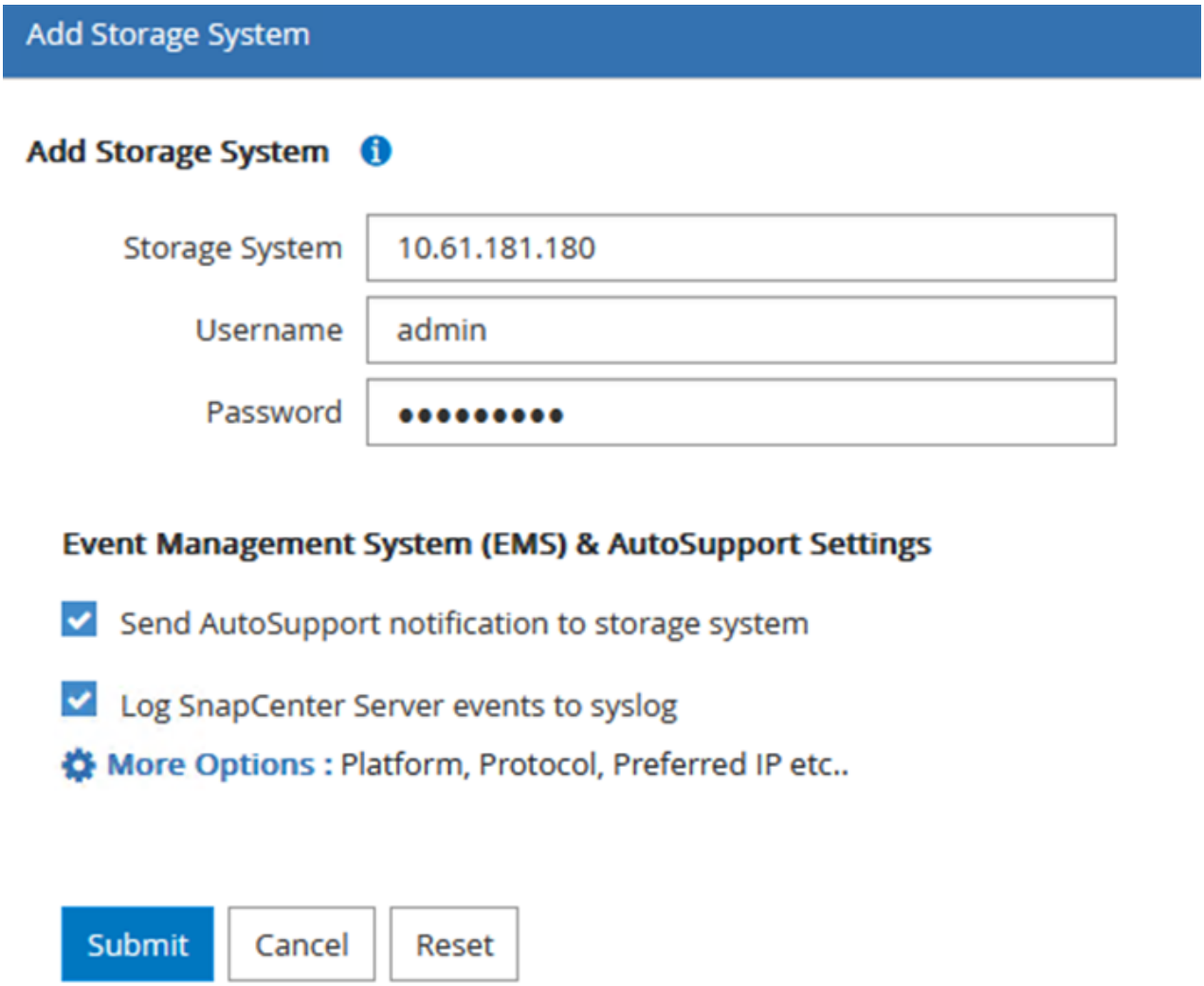
SnapCenter にストレージコントローラを追加

SnapCenter にストレージコントローラを追加するには、次の手順を実行します。

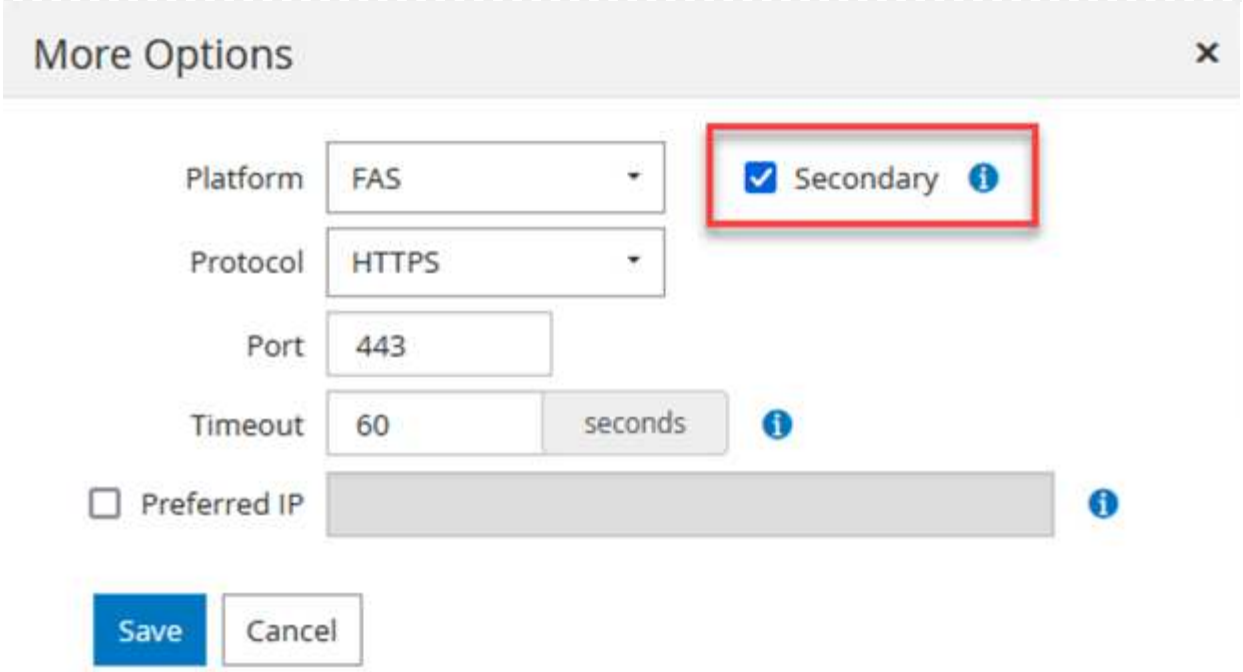
1. 左側のメニューから、ストレージシステムを選択し、新規をクリックして、ストレージコントローラをSnapCenter に追加するプロセスを開始します。



2. Add Storage System（ストレージシステムの追加）ダイアログボックスで、ローカルのオンプレミスONTAP クラスタの管理IPアドレス、およびユーザ名とパスワードを追加します。Submitをクリックして、ストレージ・システムの検出を開始します。



3. FSX ONTAP システムをSnapCenter に追加するには、この手順を繰り返します。この場合、Add Storage Systemウィンドウの下部にあるMore Optionsを選択し、Secondaryチェックボックスをオンにして、SnapMirrorコピーまたはプライマリバックアップスナップショットで更新されたセカンダリストレージシステムとしてFSXシステムを指定します。

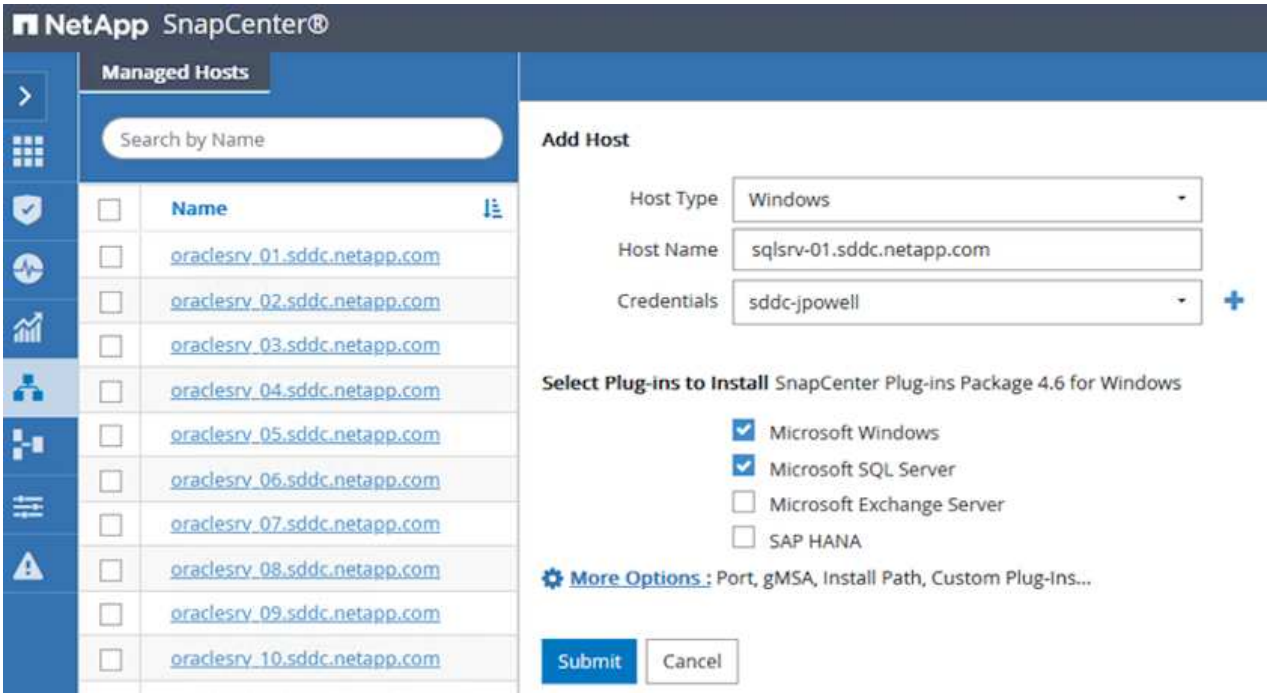


SnapCenter へのストレージシステムの追加に関する詳細については、のドキュメントを参照してください "リンクをクリックしてください"。

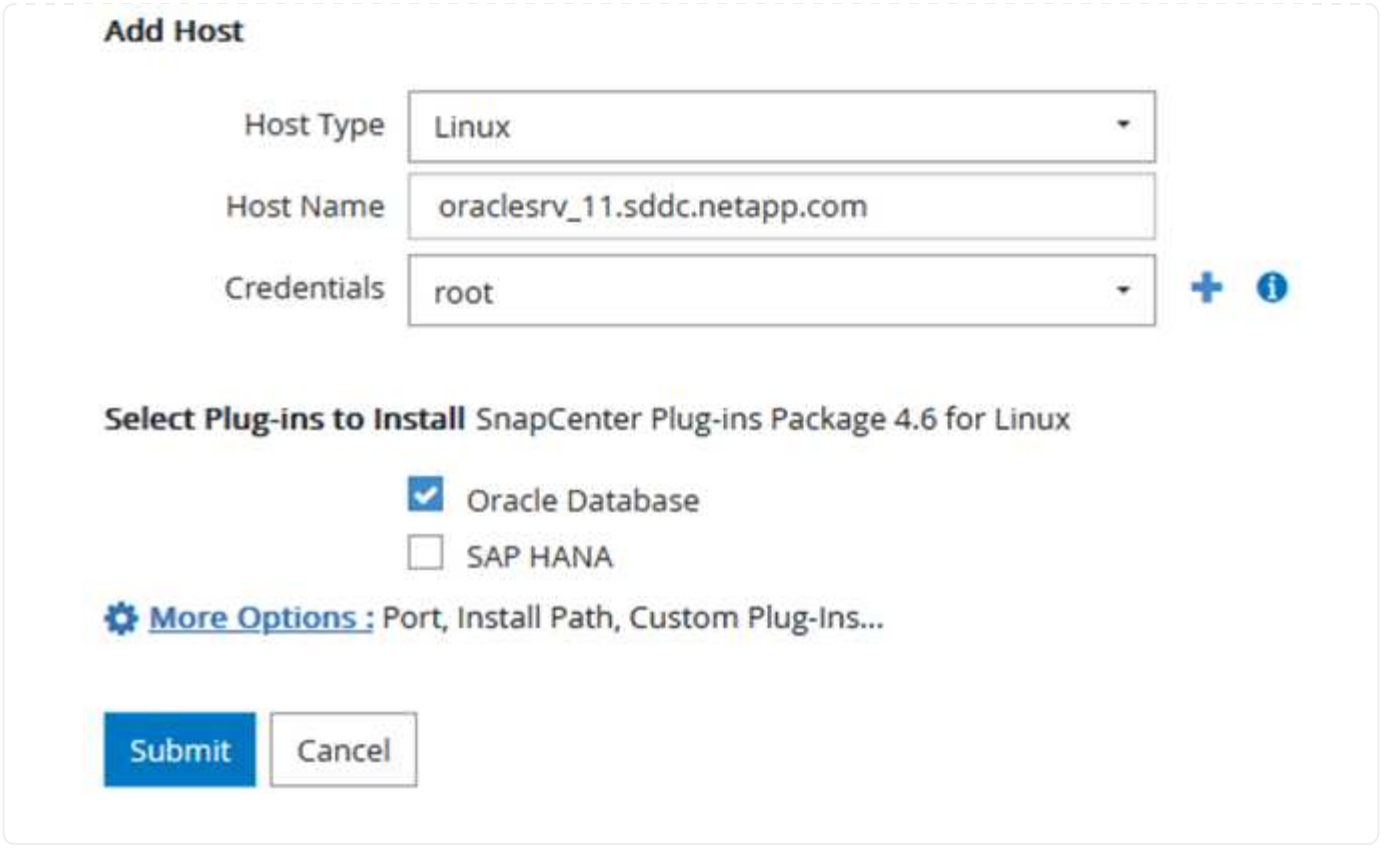
SnapCenter にホストを追加します

次の手順では、ホストアプリケーションサーバをSnapCenter に追加します。このプロセスは、SQL ServerとOracleのどちらでもほぼ同じです。

1. 左側のメニューから、Hostsを選択し、Addをクリックして、SnapCenter にストレージコントローラを追加する処理を開始します。
2. [Add Hosts]ウィンドウで、ホストタイプ、ホスト名、およびホストシステムの認証情報を追加します。プラグインタイプを選択します。SQL Serverの場合は、Microsoft WindowsとMicrosoft SQL Serverプラグインを選択します。



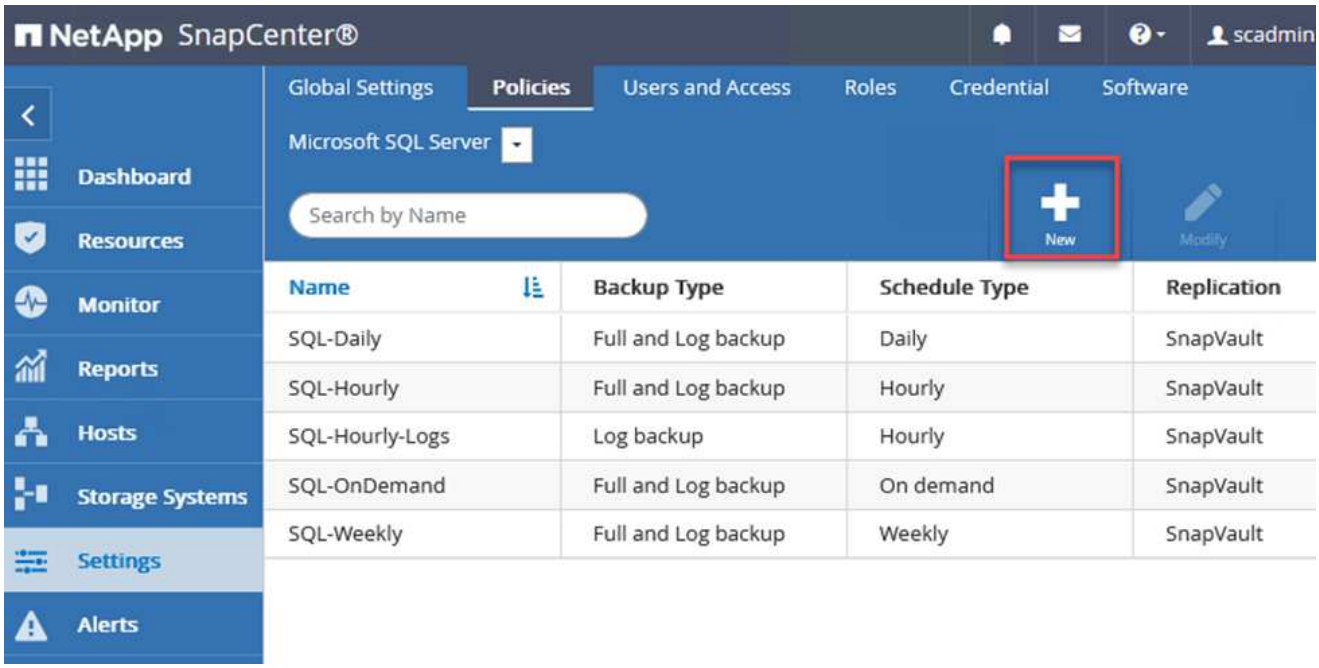
3. Oracleの場合は、[Add Host]ダイアログボックスの必須フィールドに入力し、Oracle Databaseプラグインのチェックボックスをオンにします。次に、Submitをクリックして検出プロセスを開始し、ホストをSnapCenter に追加します。


Add Host
Host Type
Linux
Host Name
oraclesrv_11.sddc.netapp.com
Credentials
root
Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Linux
Oracle Database
SAP HANA
More Options : Port, Install Path, Custom Plug-Ins...
Submit
Cancel

SnapCenter ポリシーを作成する

ポリシーを使用すると、バックアップジョブで使用する特定のルールを設定できます。バックアップスケジュール、レプリケーションタイプ、SnapCenter によるトランザクションログのバックアップと切り捨ての処理方法などが含まれますが、これらに限定されません。

ポリシーには、SnapCenter Webクライアントの設定セクションからアクセスできます。

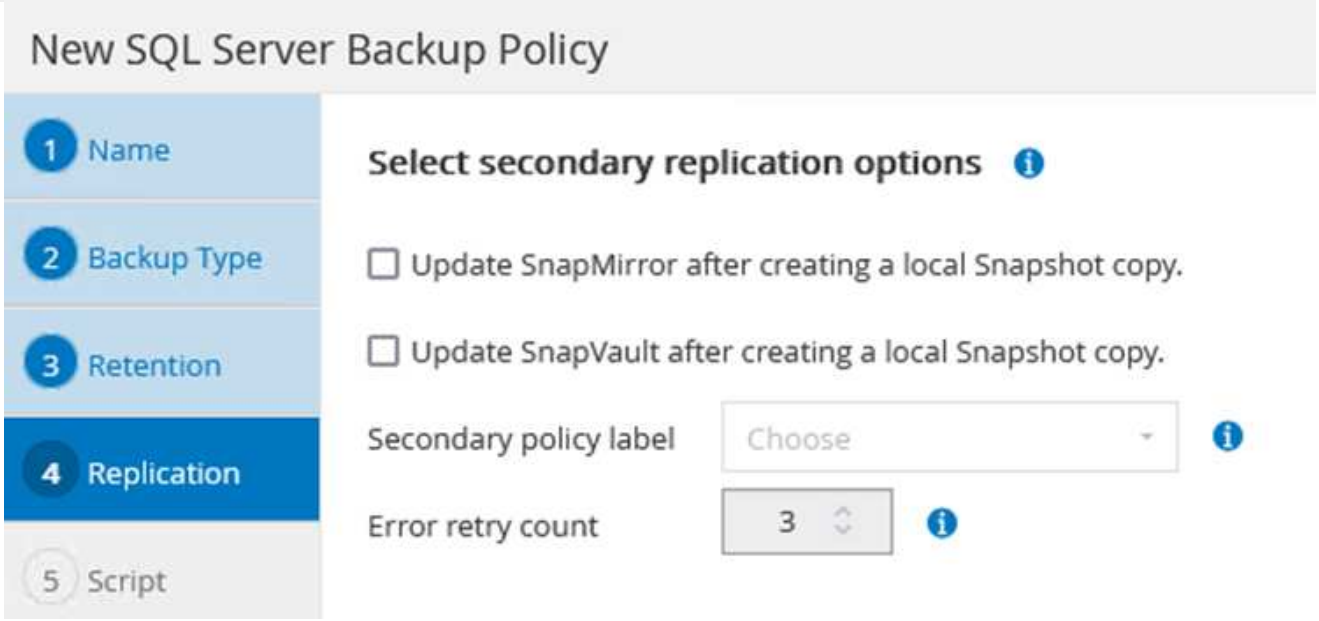


SQL Serverバックアップのポリシー作成の詳細については、を参照してください "SnapCenter のドキュメント"。

Oracleバックアップのポリシー作成の詳細については、を参照してください "SnapCenter のドキュメント"。

- 注：*
- ポリシー作成ウィザードの進行中は、Replicationセクションに特別な注意をしてください。このセクションでは、バックアッププロセスで作成するセカンダリSnapMirrorコピーのタイプを指定します。
- 「ローカルSnapshotコピー作成後にSnapMirrorを更新」設定とは、同じクラスタ上にある2台のSVM間にSnapMirror関係が存在する場合に、この関係を更新することを指します。
- 「ローカルSnapshotコピーの作成後にSnapVault を更新」設定は、2つの別々のクラスタ間、およびオンプレミスのONTAP システムとCloud Volumes ONTAP またはFSxNとの間に存在するSnapMirror関係を更新する場合に使用します。

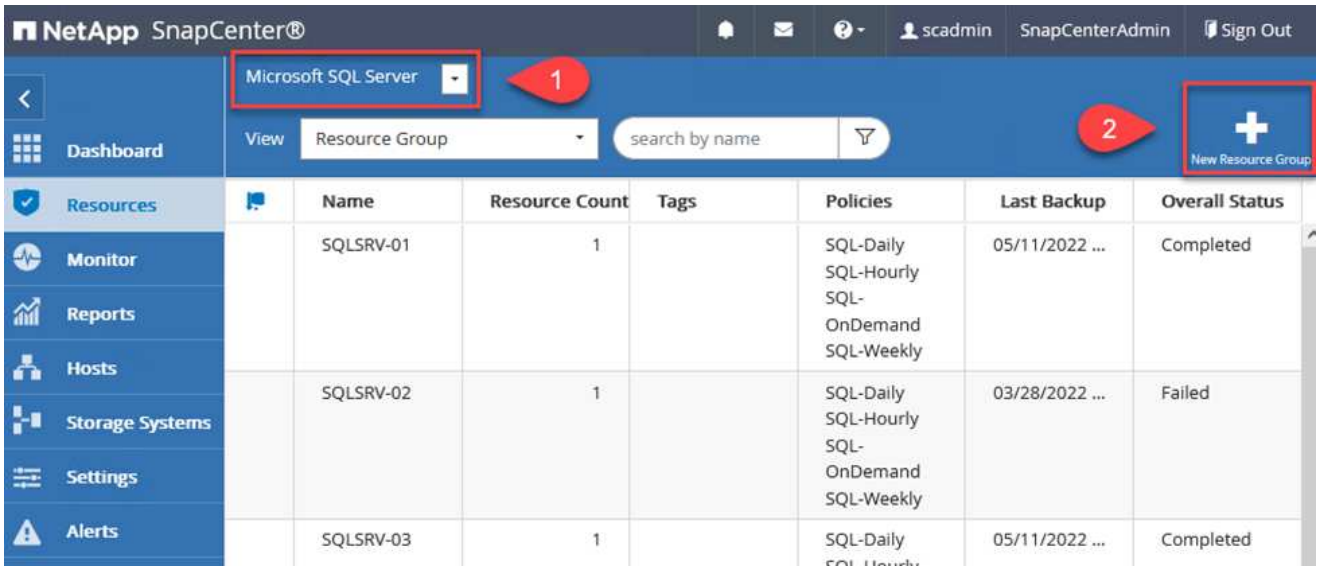
次の図は、この手順を示しており、バックアップポリシーウィザードでどのように表示されるかを示しています。



SnapCenter リソースグループを作成します

リソースグループを使用すると、バックアップに含めるデータベースリソースを選択できます。ポリシーは各リソースに適用されます。

1. 左側のメニューの[Resources]セクションに移動します。
2. ウィンドウの上部で、使用するリソースタイプ（この場合はMicrosoft SQL Server）を選択し、[新しいリソースグループ]をクリックします。



SnapCenter のドキュメントでは、SQL ServerデータベースとOracleデータベースの両方について、リソースグループを作成する手順を詳しく説明しています。

SQLリソースのバックアップについては、を参照してください "リンクをクリックしてください"。

Oracleリソースのバックアップについては、を参照してください "リンクをクリックしてください"。

Veeam Backup Serverを導入して設定します

Veeam Backup & Replicationソフトウェアは、解決策 で、アプリケーション仮想マシンのバックアップと、Veeamスケールアウトバックアップリポジトリ（SOBR）を使用したAmazon S3バケットへのバックアップのコピーのアーカイブを行うために使用します。Veeamは、この解決策 内のWindowsサーバに導入されます。Veeamの導入に関する具体的なガイダンスについては、を参照してください "Veeamヘルプセンターのテクニカルドキュメント"。

Veeamスケールアウトバックアップリポジトリを設定

ソフトウェアを導入してライセンスを設定したら、バックアップジョブのターゲットストレージとしてスケールアウトバックアップリポジトリ（SOBR）を作成できます。また、ディザスタリカバリ用にVMデータのバックアップ用にS3バケットをオフサイトに配置することも必要です。

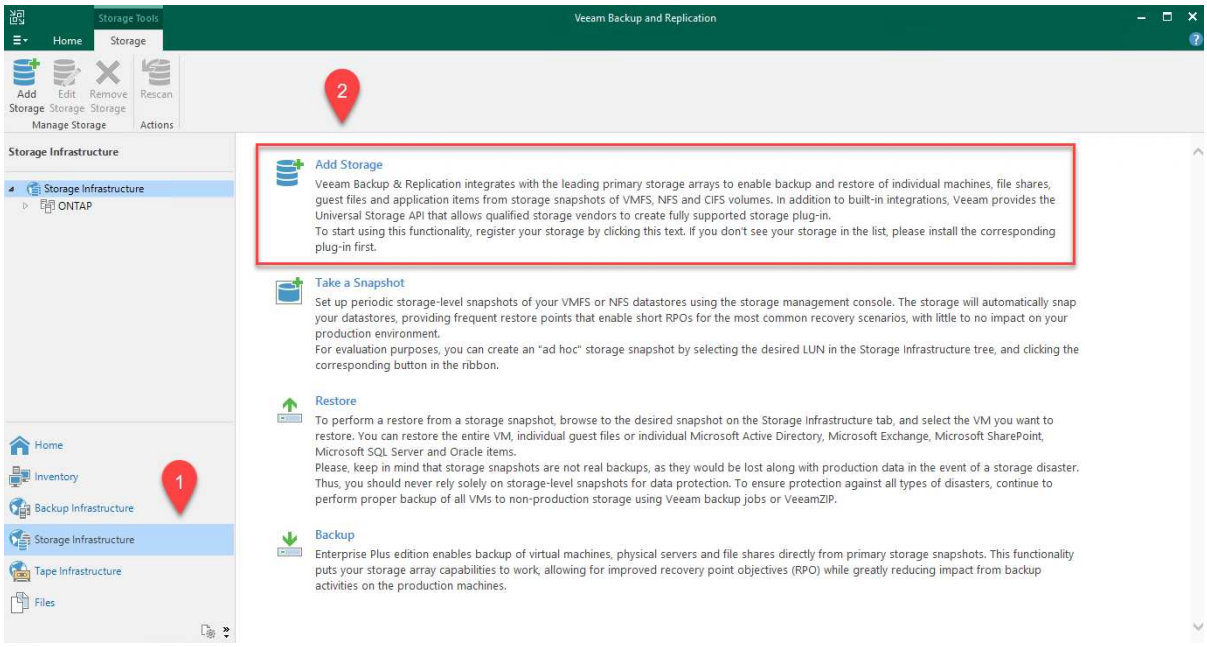
作業を開始する前に、次の前提条件を確認してください。

1. バックアップのターゲットストレージとして、オンプレミスのONTAP システム上にSMBファイル共有を作成します。
2. SOBRに含めるAmazon S3バケットを作成します。これは、オフサイトバックアップ用のリポジトリです。

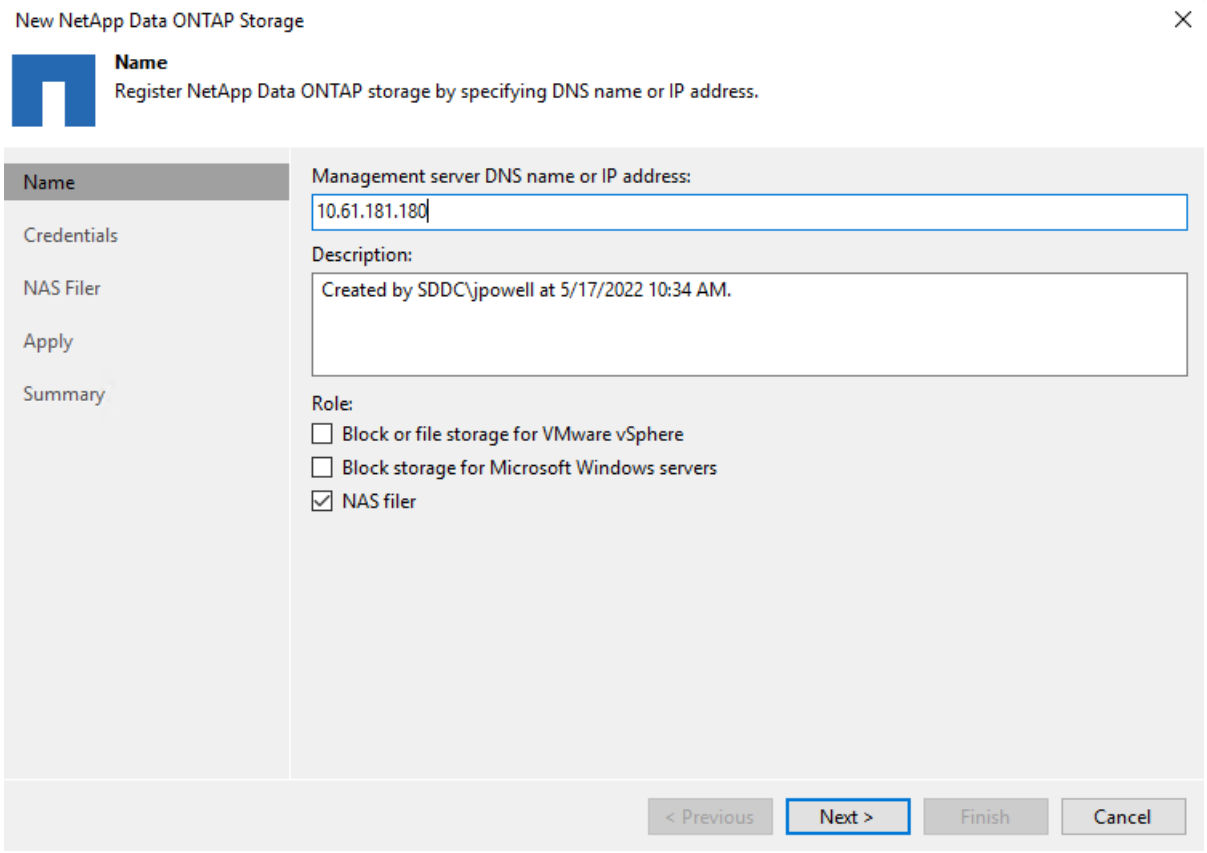
VeeamにONTAP ストレージを追加します

まず、ONTAP ストレージクラスタと関連するSMB / NFSファイルシステムをストレージインフラとしてVeeamに追加します。

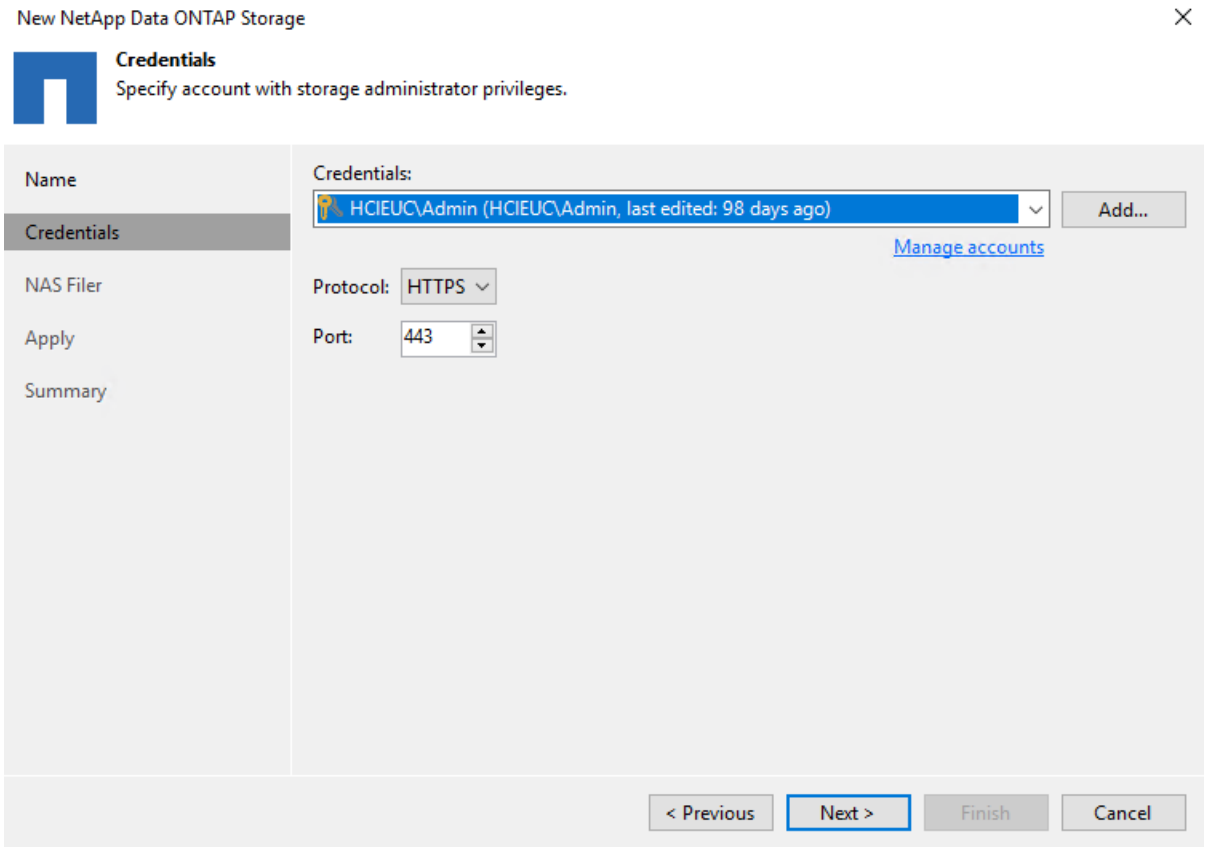
1. Veeamコンソールを開き、ログインします。ストレージインフラに移動し、ストレージの追加を選択します。



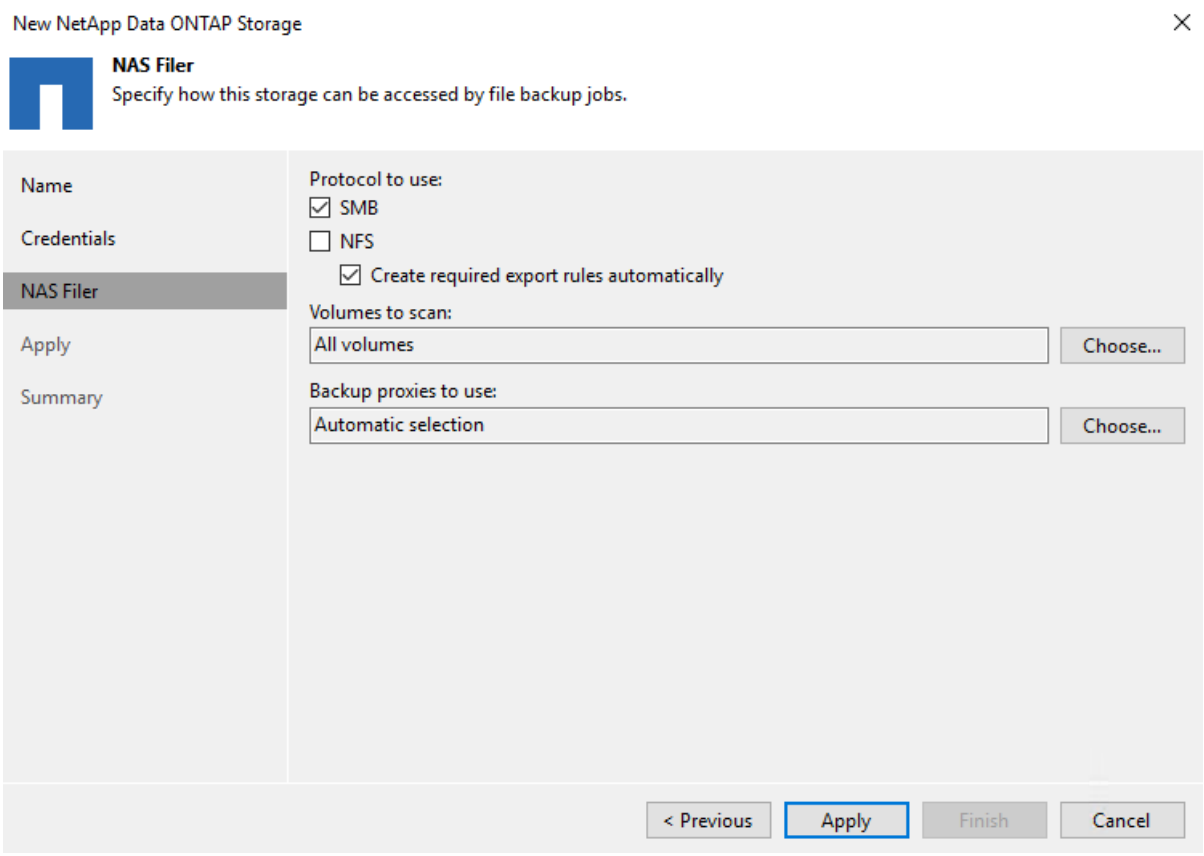
2. ストレージの追加ウィザードで、ストレージベンダーとしてネットアップを選択し、Data ONTAP を選択します。
3. 管理IPアドレスを入力し、NASファイラーボックスをオンにします。次へをクリックします。



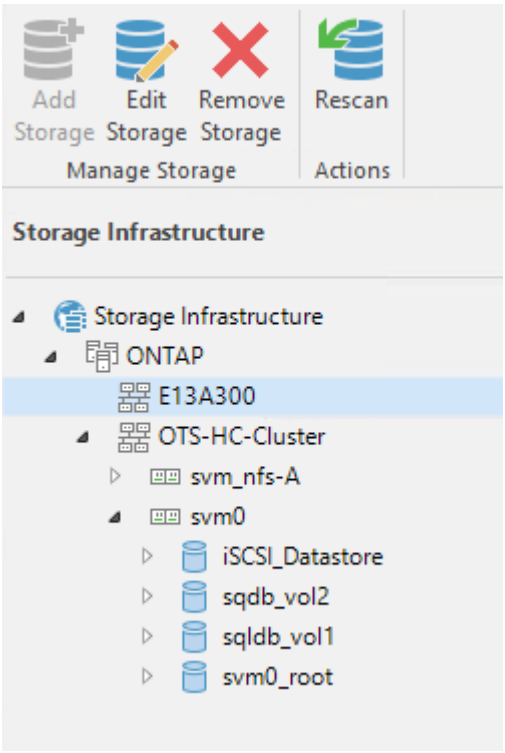
4. ONTAP クラスタにアクセスするためのクレデンシャルを追加してください。



5. NASファイラーページで、スキャンするプロトコルを選択し、次へを選択します。

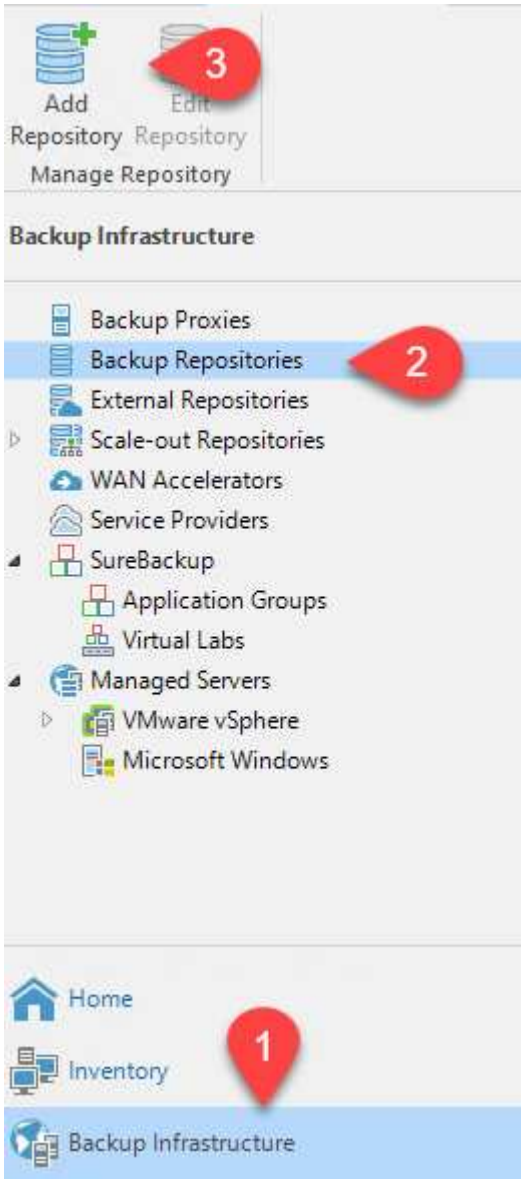


6. ウィザードのApplyページとSummaryページを設定し、Finishをクリックしてストレージ検出プロセスを開始します。スキャンが完了すると、ONTAP クラスタがNASファイラーとともに使用可能なリソースとして追加されます。

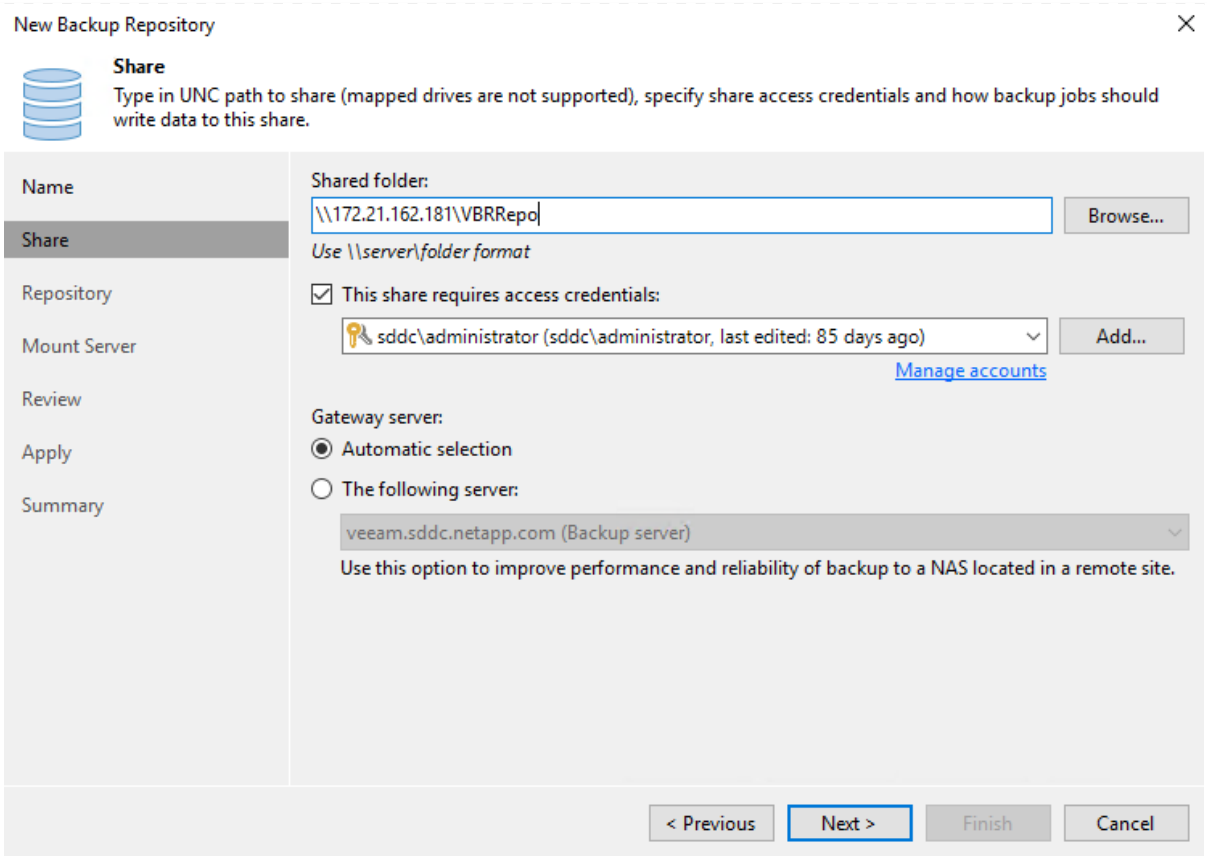


7. 新たに検出されたNAS共有を使用して、バックアップリポジトリを作成します。[バックアップインフラストラクチャ]で、[バックアップリポジトリ]を選択し、[リポジトリの追加]メニューア

イテムをクリックします。



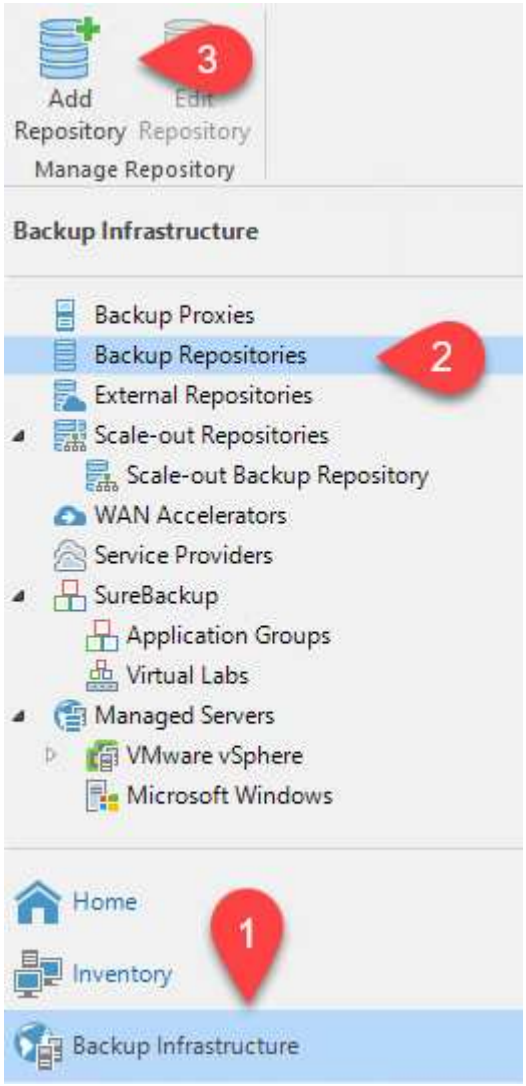
8. リポジトリを作成するには、[新規バックアップリポジトリ]ウィザードのすべての手順に従います。Veeamバックアップリポジトリの作成の詳細については、を参照してください "Veeamの製品ドキュメント"。


New Backup Repository
Share
Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.
Name
Share
Repository
Mount Server
Review
Apply
Summary
Shared folder:
\\172.21.162.181\VBRRepo
Browse...
Use \\server\folder format
This share requires access credentials:
sddc\administrator (sddc\administrator, last edited: 85 days ago)
Add...
Manage accounts
Gateway server:
Automatic selection
The following server:
veeam.sddc.netapp.com (Backup server)
Use this option to improve performance and reliability of backup to a NAS located in a remote site.
< Previous
Next >
Finish
Cancel

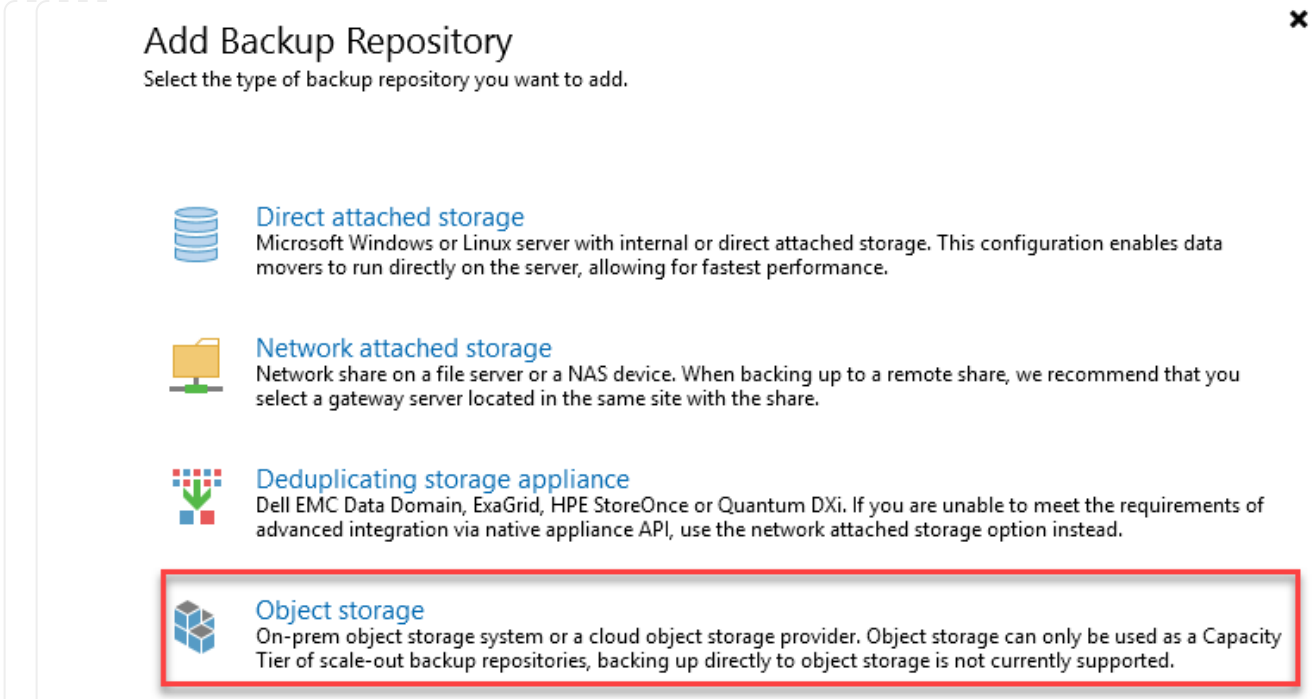
Amazon S3バケットをバックアップリポジトリとして追加します

次の手順では、Amazon S3ストレージをバックアップリポジトリとして追加します。

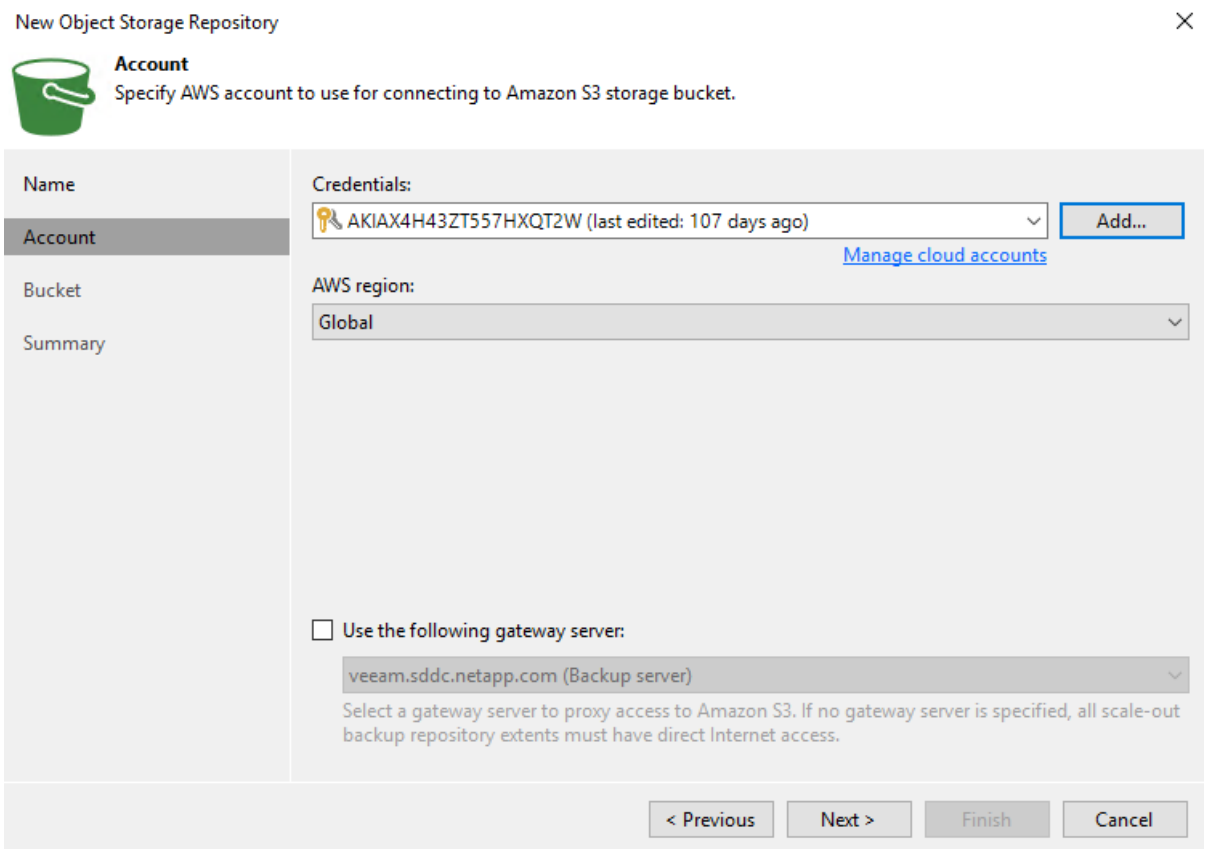
1. [バックアップインフラストラクチャ]>[バックアップリポジトリ]に移動します。[リポジトリの追加]をクリックします



2. バックアップリポジトリの追加ウィザードで、オブジェクトストレージ、Amazon S3の順に選択します。これにより、新規オブジェクトストレージリポジトリウィザードが起動します。



3. オブジェクトストレージリポジトリの名前を入力し、次へをクリックします。
4. 次のセクションで、クレデンシャルを入力します。AWSのアクセスキーとシークレットキーが必要です。

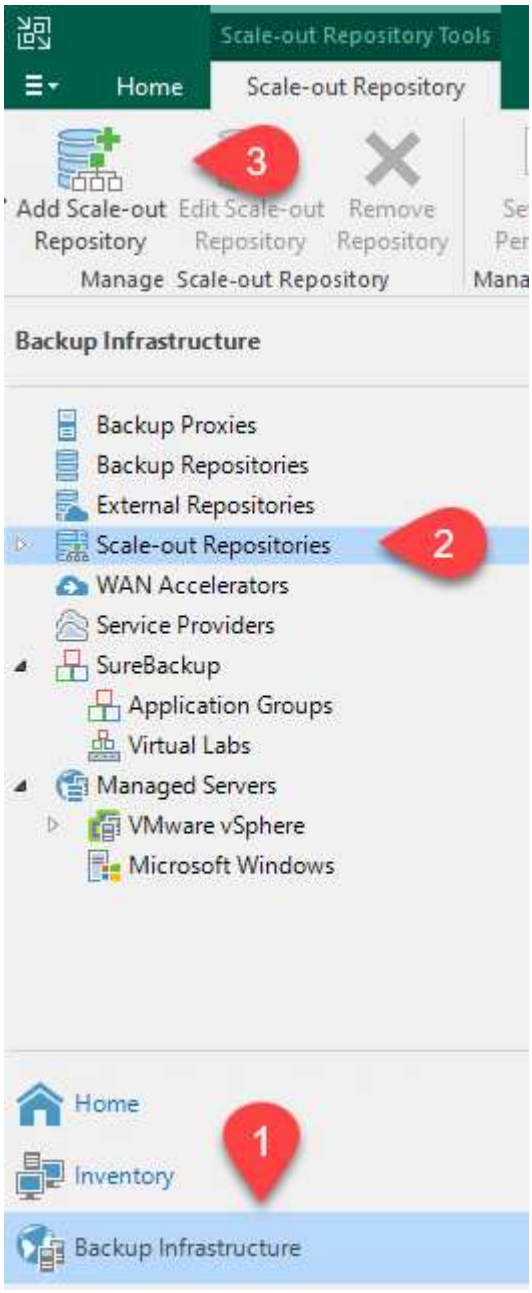


5. Amazon設定がロードされたら、データセンター、バケット、およびフォルダを選択し、適用をクリックします。最後に、[完了]をクリックしてウィザードを終了します。

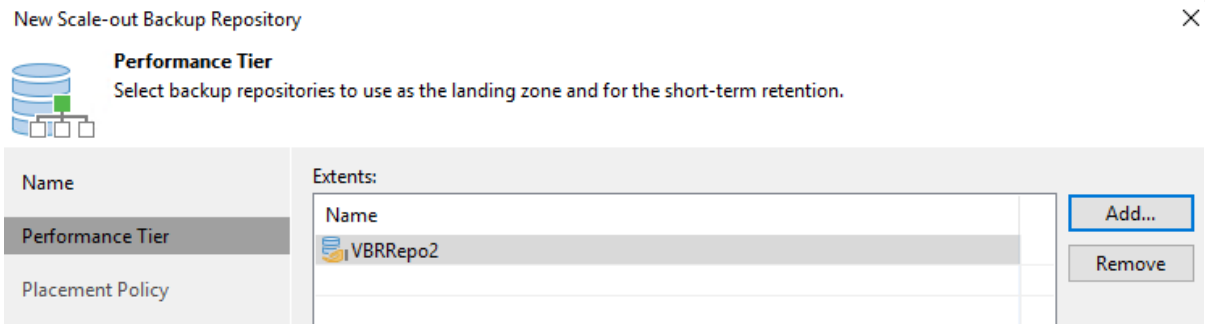
スケールアウトバックアップリポジトリの作成

これでVeeamにストレージリポジトリを追加したので、SOBRを作成して、ディザスタリカバリ用にオフサイトのAmazon S3オブジェクトストレージにバックアップコピーを自動的に階層化できます。

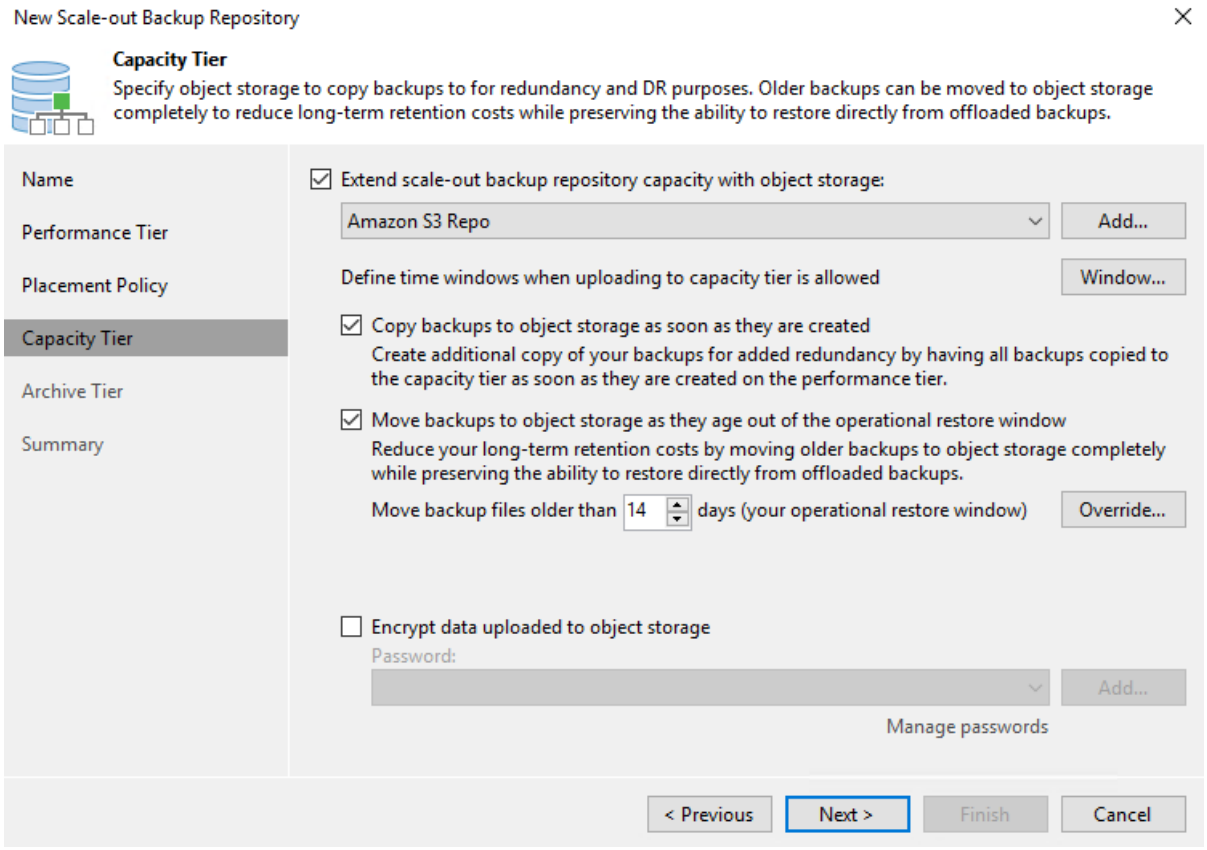
1. [バックアップインフラストラクチャ]で、[スケールアウトリポジトリ]を選択し、[スケールアウトリポジトリの追加]メニューアイテムをクリックします。



2. [新しいスケールアウトバックアップリポジトリ]で’SOBRの名前を指定し'[次へ]をクリックします
3. 階層のパフォーマンスについて、ローカルのONTAP クラスタにあるSMB共有を含むバックアップリポジトリを選択します。



4. 配置ポリシーで、要件に基づいて[データの局所性]または[パフォーマンス]を選択します。[次へ]を選択し
5. 大容量階層の場合は、SOBRとAmazon S3オブジェクトストレージを拡張します。ディザスタリカバリのために、セカンダリバックアップをタイムリーに提供できるように、バックアップを作成したらすぐにオブジェクトストレージにコピーするを選択します。



6. 最後に、[適用（Apply）]と[完了（Finish）]を選択してSOBRの作成を確定する。

スケールアウトバックアップリポジトリジョブを作成

Veeamを設定する最後の手順は、新しく作成したバックアップ先のSOBRを使用してバックアップジョブを作成することです。バックアップジョブの作成は、ストレージ管理者の作業内容に含まれる通常の作業であり、ここでは詳細な手順については説明しません。Veeamでのバックアップジョブの作成の詳細については、を参照してください "Veeam Help Centerテクニカルドキュメント"。

BlueXPのバックアップとリカバリのツールと構成

アプリケーションVMおよびデータベースボリュームをAWSで実行されているVMware Cloud Volumeサービスにフェイルオーバーするには、SnapCenter サーバとVeeam Backup and Replication Serverの両方の実行中のインスタンスをインストールして設定する必要があります。フェイルオーバーが完了したら、オンプレミスのデータセンターへのフェイルバックが計画されて実行されるまで、通常のバックアップ処理を再開するようにこれらのツールも設定する必要があります。

セカンダリ**Windows SnapCenter** サーバを導入します

SnapCenter サーバは、VMware Cloud SDDCに導入するか、VPC内のEC2インスタンスにインストールし、VMware Cloud環境にネットワーク接続します。

SnapCenter ソフトウェアはネットアップサポートサイトから入手でき、ドメインまたはワークグループ内にあるMicrosoft Windowsシステムにインストールできます。詳細な計画ガイドとインストール手順については、を参照してください "ネットアップドキュメントセンター"。

SnapCenter ソフトウェアは、から入手できます "リンクをクリックしてください"。

セカンダリ**Windows SnapCenter** サーバを設定します

FSX ONTAP にミラーリングされたアプリケーション・データのリストアを実行するには'まずオンプレミスのSnapCenter データベースのフル・リストアを実行する必要がありますこのプロセスが完了すると、VMとの通信が再確立され、プライマリストレージとしてFSX ONTAP を使用してアプリケーションのバックアップを再開できるようになります。

これを行うには、SnapCenter サーバで次の項目を完了する必要があります。

1. コンピュータ名を、元のオンプレミスSnapCenter サーバと同じ名前に設定します。
2. VMware CloudおよびFSX ONTAP インスタンスと通信するためのネットワークを設定します。
3. 手順 を完了してSnapCenter データベースをリストアします。
4. SnapCenter がディザスタリカバリモードになっていることを確認し、FSXがバックアップ用のプライマリストレージになったことを確認します。
5. リストアした仮想マシンとの通信が再確立されたことを確認します。

セカンダリ**Veeam Backup & Replication**サーバを導入します

Veeam Backup & Replicationサーバは、AWS上のVMware CloudまたはEC2インスタンス上のWindowsサーバにインストールできます。実装の詳細なガイダンスについては、を参照してください "Veeam Help Centerテクニカルドキュメント"。

セカンダリ**Veeam Backup & Replication**サーバを設定します

Amazon S3ストレージにバックアップされた仮想マシンをリストアするには、WindowsサーバにVeeamサーバをインストールし、VMware Cloud、FSX ONTAP 、および元のバックアップリポジトリが格納されたS3バケットと通信するように設定する必要があります。また、リストア後にVMの新しいバックアップを実行するために、FSX ONTAP に新しいバックアップリポジトリが設定されている必要があります。

このプロセスを実行するには、次の項目を完了する必要があります。

1. VMware Cloud、FSX ONTAP 、および元のバックアップリポジトリを含むS3バケットと通信するためのネットワークを設定します。
2. FSX ONTAP 上のSMB共有を新しいバックアップリポジトリとして設定します。
3. スケールアウトバックアップリポジトリの一部として使用されていた元のS3バケットをオンプレミスにマウントします。
4. VMをリストアしたら、SQL VMとOracle VMを保護するための新しいバックアップジョブを確立します。

Veeamを使用したVMのリストアの詳細については、を参照してください "アプリケーションVMをVeeam Full Restoreでリストアします"。

ディザスタリカバリに備えた**SnapCenter** データベースバックアップ

SnapCenter を使用すると、災害発生時にSnapCenter サーバをリカバリできるように、基盤となるMySQLデータベースおよび設定データのバックアップとリカバリを行うことができます。解決策 では、VPC内のAWS EC2インスタンスでSnapCenter データベースと設定をリカバリしました。この手順の詳細については、を参照してください "リンクをクリックしてください"。

SnapCenter バックアップの前提条件

SnapCenter バックアップを実行するには、次の前提条件が必要です。

- オンプレミスのONTAP システムに作成されたボリュームとSMB共有。バックアップされたデータベースと構成ファイルを検索します。
- オンプレミスのONTAP システムと、AWSアカウントのFSXまたはCVOとの間のSnapMirror関係。この関係は、バックアップされたSnapCenter データベースおよび構成ファイルを含むSnapshotの転送に使用されます。
- EC2インスタンスまたはVMware Cloud SDDC内のVMに、クラウドアカウントにWindows Serverをインストールします。
- SnapCenter は、VMware CloudのWindows EC2インスタンスまたはVMにインストールします。

SnapCenter のバックアップとリストアのプロセスの概要

- バックアップのdbファイルと構成ファイルをホストするボリュームをオンプレミスのONTAP システムに作成します。
- オンプレミスとFSX/CVOの間にSnapMirror関係を設定
- SMB共有をマウント
- APIタスクを実行するためのSwagger承認トークンを取得します。
- dbのリストア・プロセスを開始します。
- xcopyユーティリティを使用して、dbおよびconfigファイルのローカルディレクトリをSMB共有にコピーします。
- FSXで、ONTAP ボリュームのクローンを作成する（オンプレミスからSnapMirror経由でコピーする）。
- FSXからEC2/VMware CloudにSMB共有をマウントします。
- SMB共有からローカルディレクトリにリストアディレクトリをコピーします。
- SwaggerからSQL Serverのリストアプロセスを実行します。

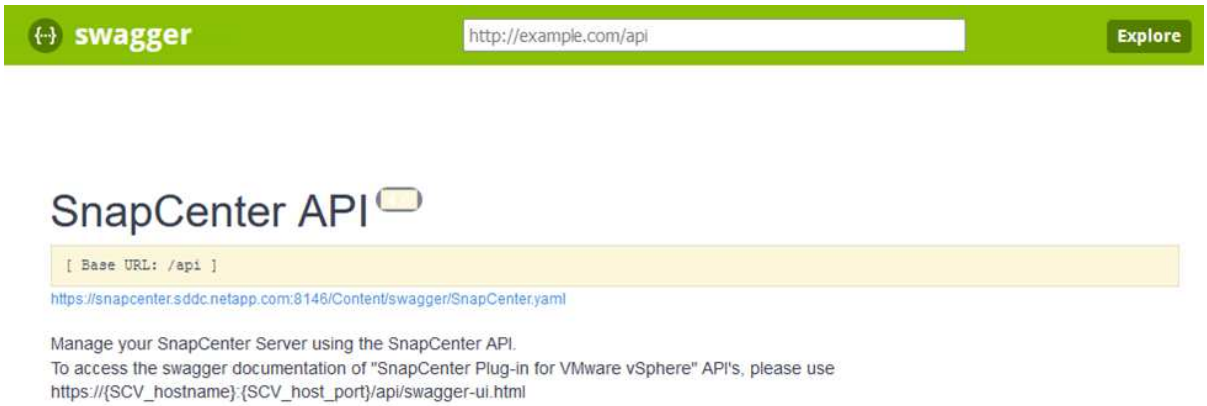
SnapCenter データベースと設定をバックアップします

SnapCenter は、REST APIコマンドを実行するためのWebクライアントインターフェイスを提供します。Swagger経由でのREST APIへのアクセスについては、SnapCenter のドキュメントを参照してください "リンクをクリックしてください"。

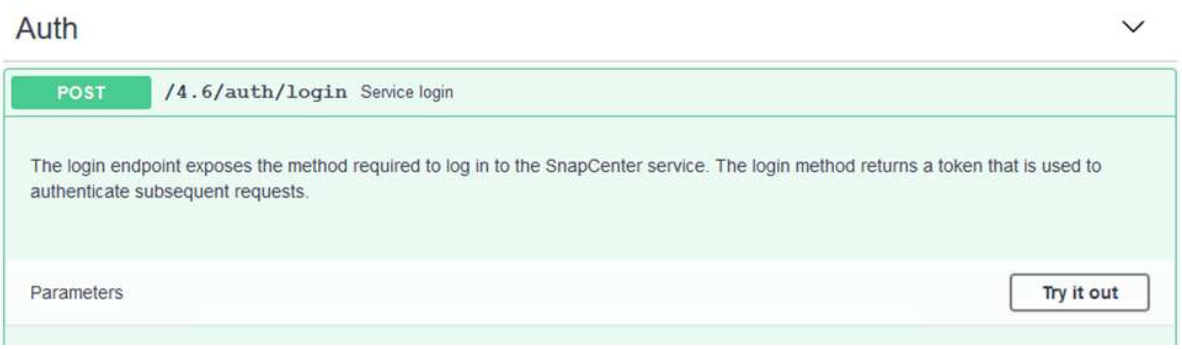
Swaggerにログインし、認証トークンを取得します

Swaggerページに移動したら、認証トークンを取得してデータベースリストアプロセスを開始する必要があります。

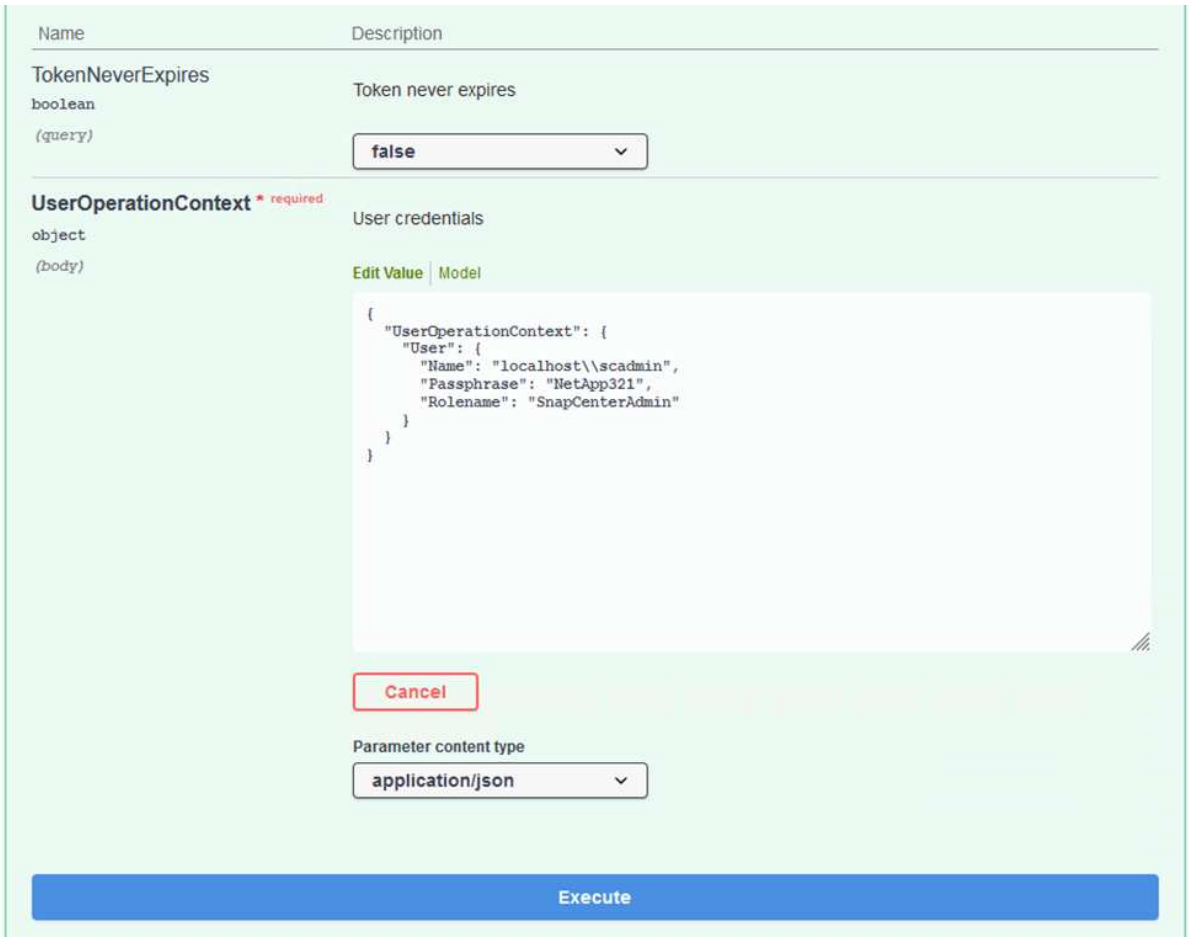
1. SnapCenter Swagger API Webページ（\\ https://<SnapCenterサーバIP >：8146 /スワッガ/_）にアクセスします。



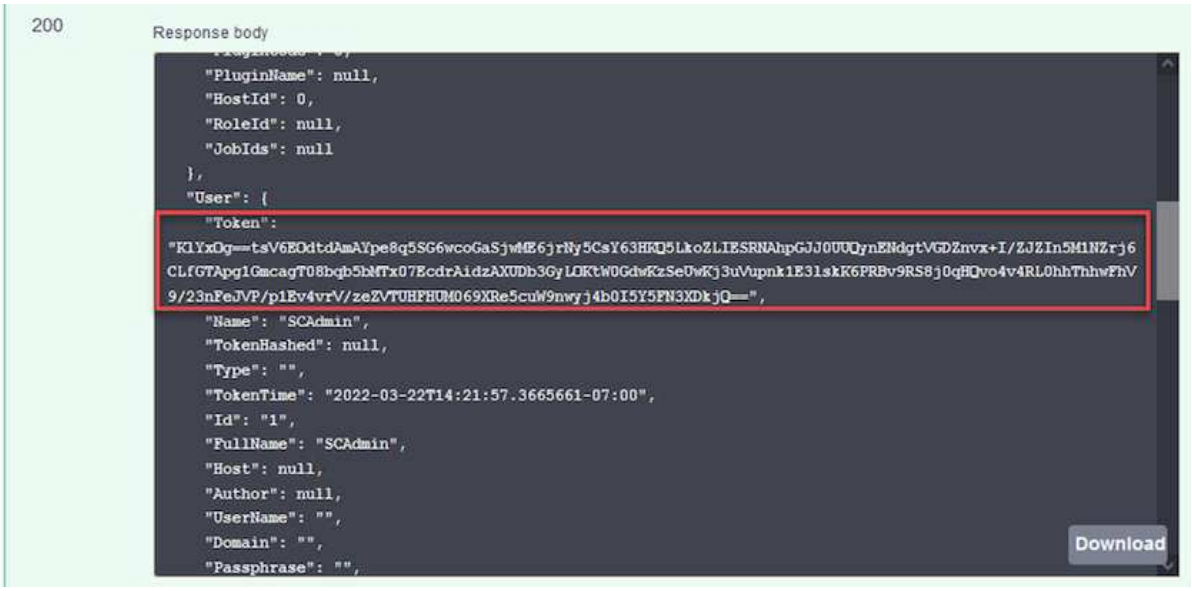
2. [Auth]セクションを展開し、[Try it Out]をクリックします。



3. UserOperationContext領域で、SnapCenter の資格情報と役割を入力し、Executeをクリックします。



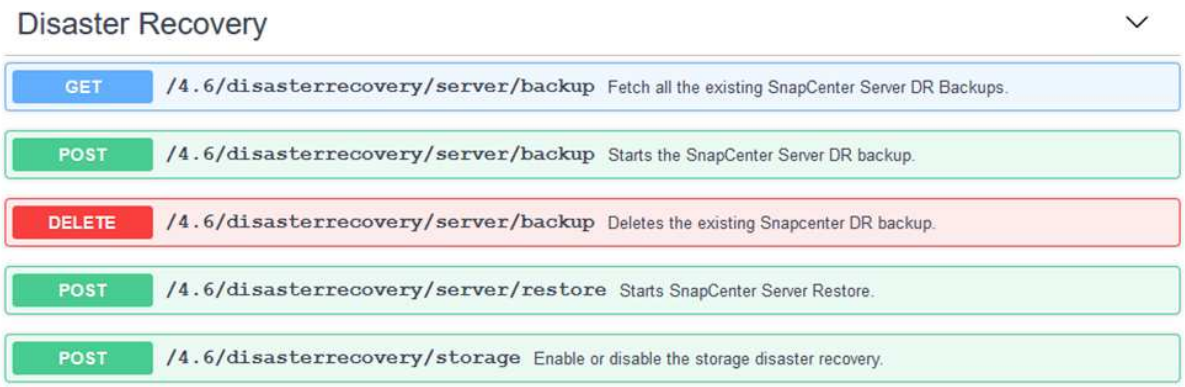
4. 以下の応答本文では、トークンを確認できます。バックアッププロセス実行時に、認証用のトークンテキストをコピーします。



SnapCenter データベースのバックアップを実行する

次に、Swaggerページのディザスタリカバリ領域に移動して、SnapCenter バックアッププロセスを開始します。

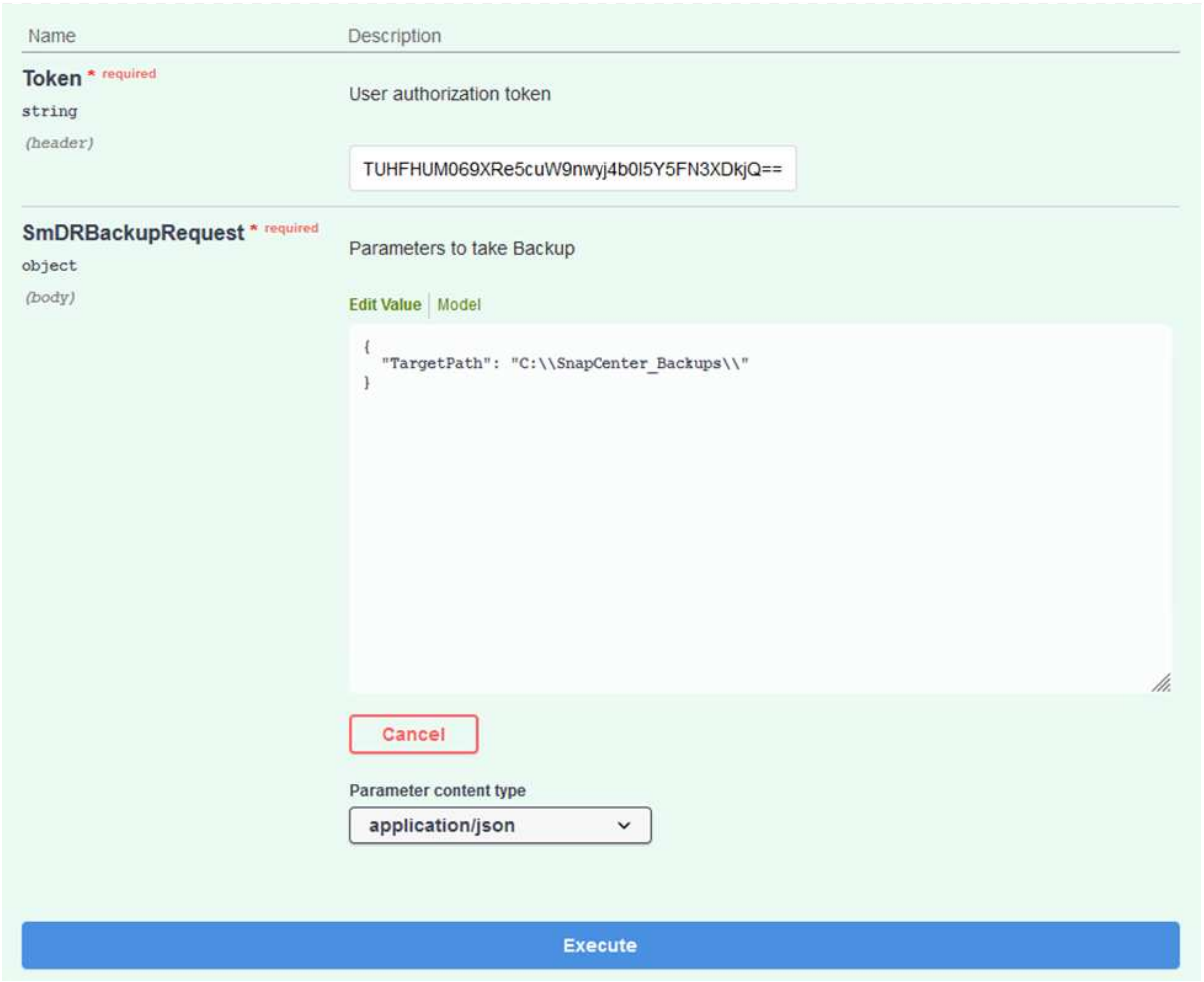
1. [Disaster Recovery]領域をクリックして展開します。



2. 「/4.6/disasterrecovery/sa/backup」セクションを展開し、「試してみてください」をクリックします。

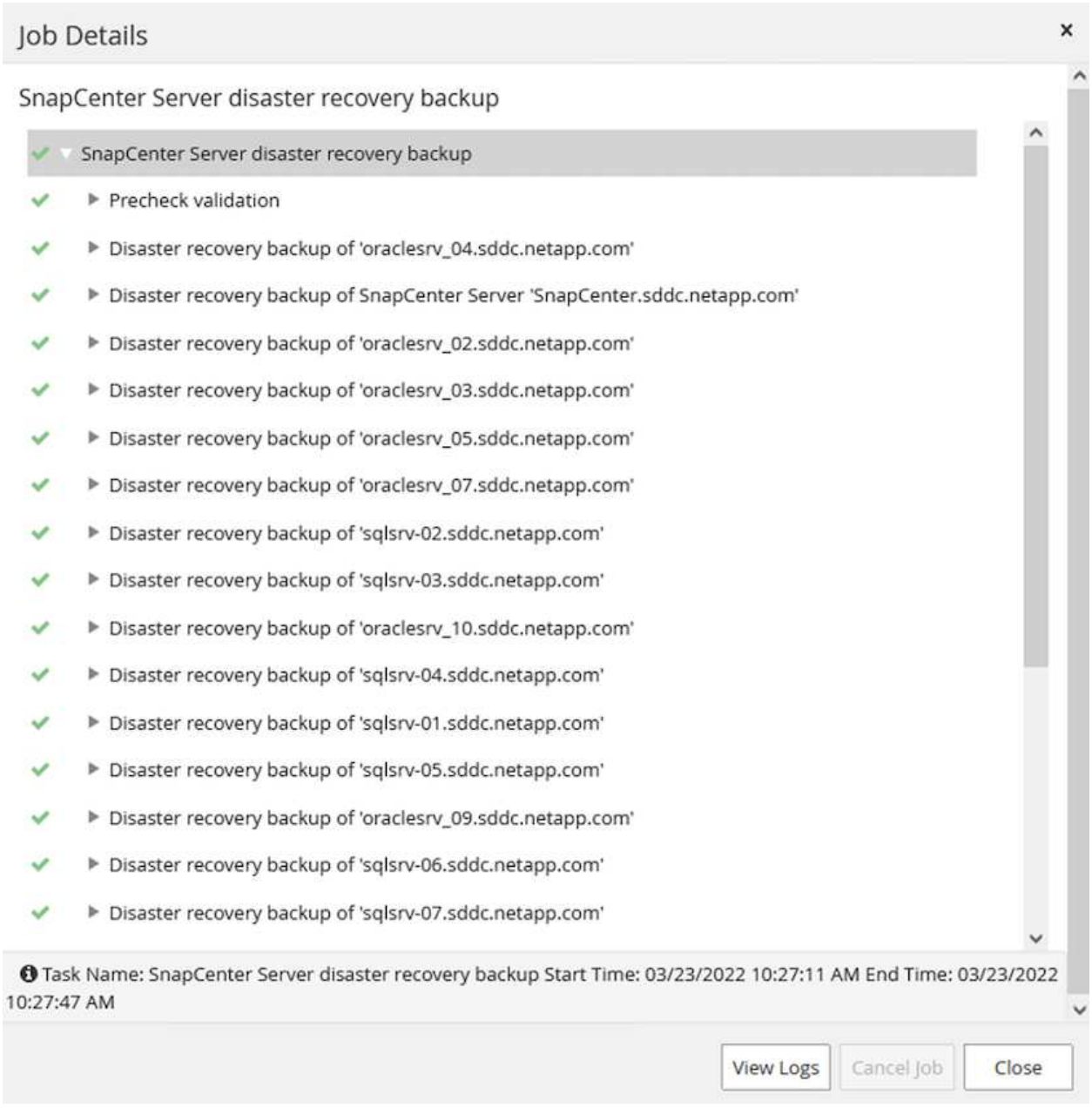
3. SmDRBackupRequestセクションで、正しいローカルターゲットパスを追加し、Executeを選択してSnapCenter データベースと設定のバックアップを開始します。

> バックアッププロセスでは、NFSまたはCIFSのファイル共有に直接バックアップすることはできません。


Name
Description
Token * required
string
(header)
User authorization token
TUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ==
SmDRBackupRequest * required
object
(body)
Parameters to take Backup
Edit Value
Model
{
"TargetPath": "C:\\SnapCenter_Backups\\"
}
Cancel
Parameter content type
application/json
Execute

SnapCenter からバックアップジョブを監視

データベースリストアプロセスを開始するときに、SnapCenter にログインしてログファイルを確認します。Monitorセクションでは、SnapCenter サーバのディザスタリカバリバックアップの詳細を表示できます。



XCOPYユーティリティを使用してデータベースバックアップファイルを**SMB**共有にコピーします

次に、SnapCenter サーバ上のローカルドライブから、SnapMirrorによってデータがAWSのFSXインスタンス上のセカンダリサイトにコピーされるCIFS共有にバックアップを移動する必要があります。ファイルのアクセス権を保持する特定のオプションを指定してxcopyを使用します

管理者としてコマンドプロンプトを開きます。コマンドプロンプトで、次のコマンドを入力します。

```
xcopy  <Source_Path>  \\<Destination_Server_IP>\<Folder_Path> /O /X
/E /H /K
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O
/X /E /H /K
```

フェイルオーバー

災害はプライマリサイトで発生します

プライマリオンプレミスのデータセンターで災害が発生した場合のシナリオとして、AWSでVMware Cloudを使用して、Amazon Web Servicesインフラにあるセカンダリサイトへのフェイルオーバーがあります。仮想マシンとオンプレミスのONTAP クラスタにはアクセスできなくなると仮定しています。また、SnapCenter とVeeamの仮想マシンはどちらもアクセスできなくなり、2次サイトで再構築する必要があります。

このセクションでは、インフラからクラウドへのフェイルオーバーについて説明します。ここでは、次のトピックについて説明します。

- SnapCenter データベースのリストア：新しいSnapCenter サーバが確立されたら、MySQLデータベースと構成ファイルをリストアし、データベースをディザスタリカバリモードに切り替えて、セカンダリFSXストレージをプライマリストレージデバイスにします。
- Veeam Backup & Replicationを使用してアプリケーション仮想マシンをリストアします。VMバックアップを含むS3ストレージを接続し、バックアップをインポートして、AWS上のVMware Cloudにリストアします。
- SnapCenter を使用してSQL Serverアプリケーションデータをリストアします。
- SnapCenter を使用してOracleアプリケーションのデータをリストアします。

SnapCenter データベースのリストアプロセス

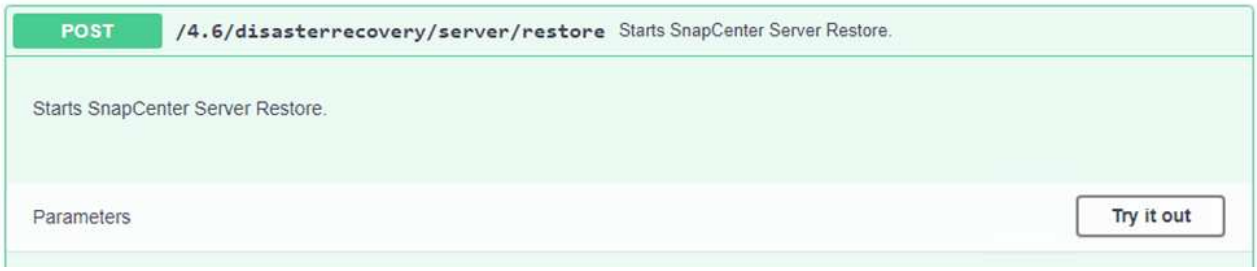
SnapCenter では、MySQLデータベースおよび構成ファイルのバックアップとリストアが可能なため、ディザスタリカバリのシナリオがサポートされます。これにより、管理者はSnapCenter データベースの定期的なバックアップをオンプレミスのデータセンターで保持し、そのデータベースをセカンダリSnapCenter データベースにリストアすることができます。

リモートSnapCenter サーバ上のSnapCenter バックアップファイルにアクセスするには、次の手順を実行します。

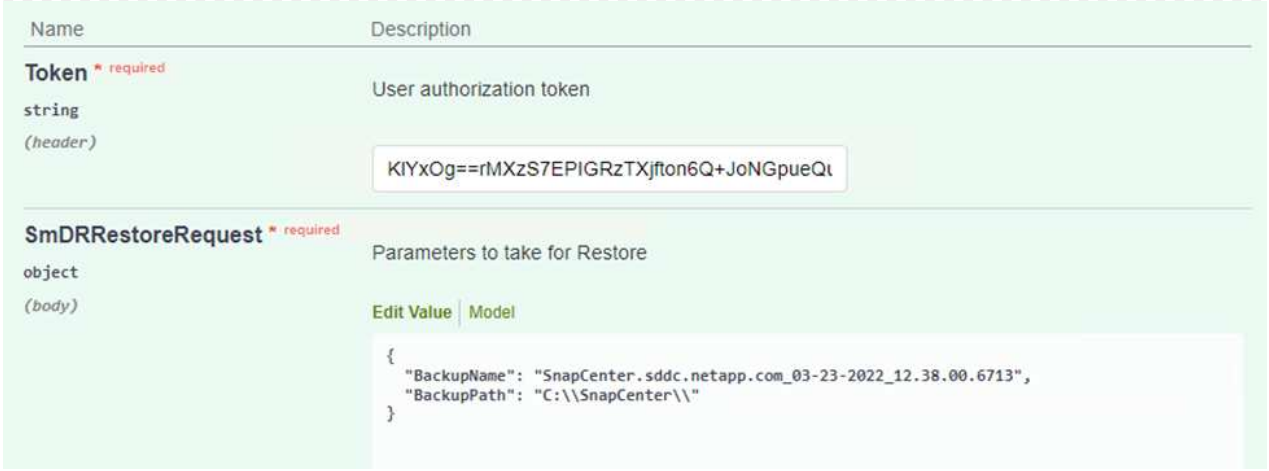
1. ボリュームを読み取り/書き込み可能にするFSXクラスタからSnapMirror関係を解除します。
2. 必要に応じてCIFSサーバを作成し、クローニングされたボリュームのジャンクションパスを参照するCIFS共有を作成します。
3. xcopyを使用して、セカンダリSnapCenter システムのローカルディレクトリにバックアップファイルをコピーします。
4. SnapCenter v4.6をインストールします。
5. SnapCenter サーバのFQDNが元のサーバと同じであることを確認します。これは、データベースのリストアを正常に実行するために必要です。

リストア・プロセスを開始するには、次の手順を実行します。

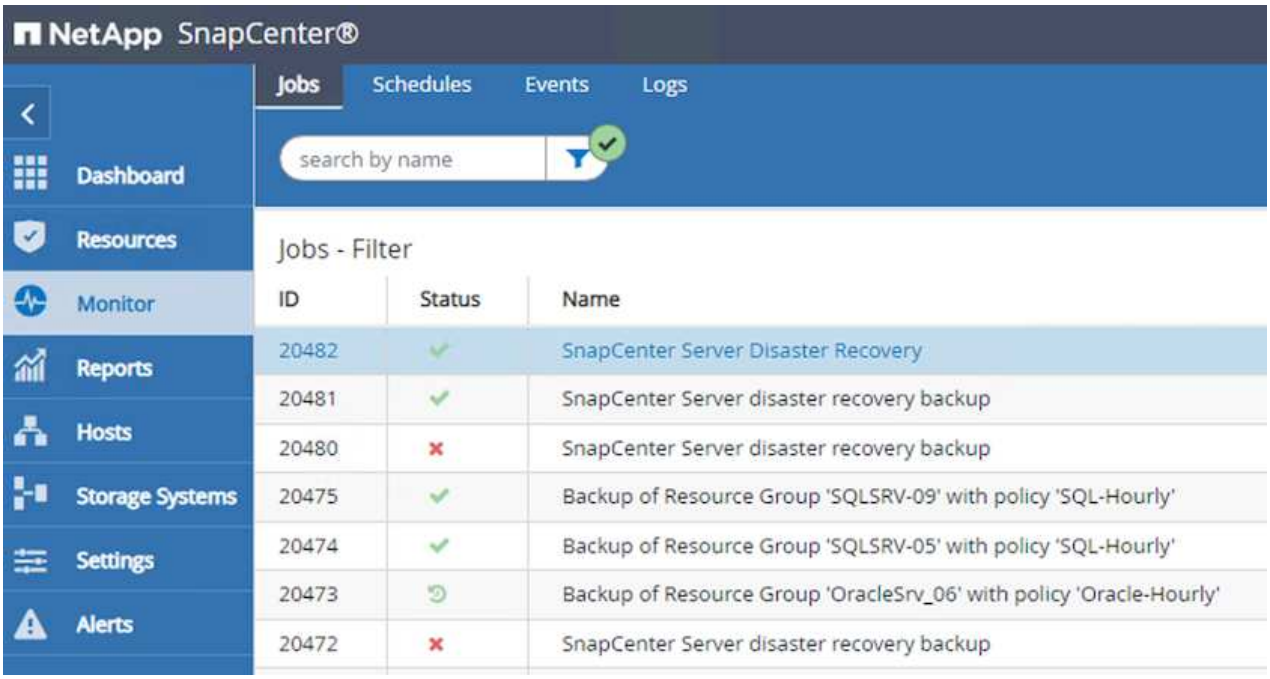
1. セカンダリSnapCenter サーバのSwagger API Webページに移動し、前述の手順に従って認証トークンを取得します。
2. Swaggerページの[Disaster Recovery]セクションに移動し、[0/4.6/disasterrecovery/sa/restore]を選択して、[Try it out]をクリックします。

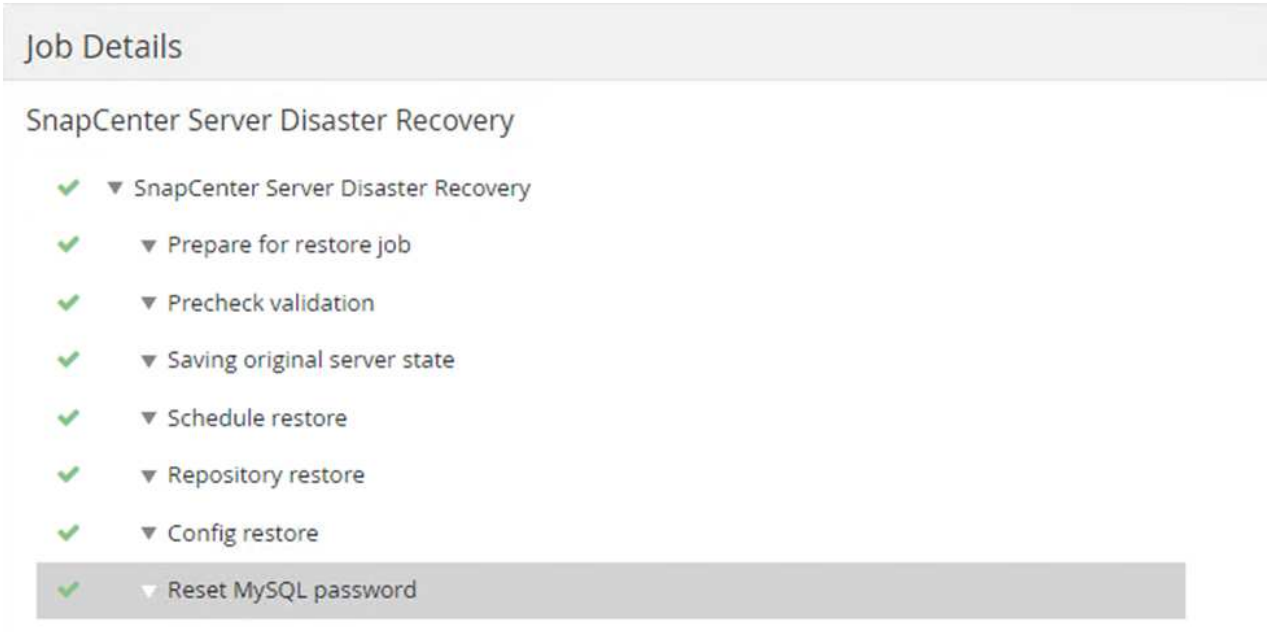


3. 認証トークンに貼り付けて、SmDRRestarterRequestセクションで、バックアップ名とセカンダリSnapCenter サーバのローカルディレクトリに貼り付けます。



4. Executeボタンを選択して'リストア・プロセスを開始します
5. SnapCenter で、監視セクションに移動してリストアジョブの進捗状況を確認します。





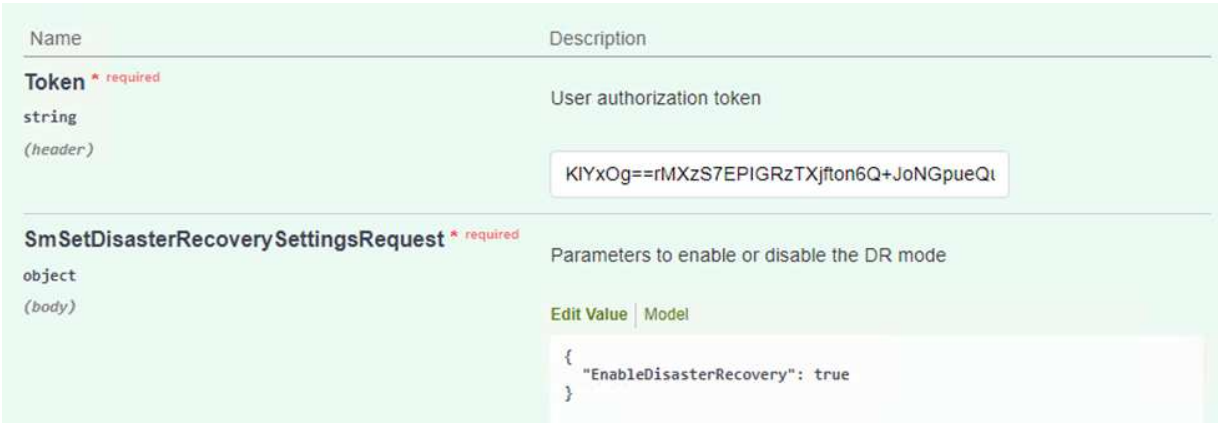
6. セカンダリストレージからのSQL Serverのリストアを有効にするには、SnapCenter データベースをディザスタリカバリモードに切り替える必要があります。この処理は、Swagger API Webページで個別の処理として開始されます。

   a. [Disaster Recovery]セクションに移動し'[/4.6/disasterrecovery/storage]をクリックします

   b. ユーザー認証トークンに貼り付けます。

   c. SmSetDisasterRecoverySettingsRequestセクションで'EnableDisasterRecoverを'true'に変更します

   d. Executeをクリックして'SQL Serverの災害復旧モードを有効にします



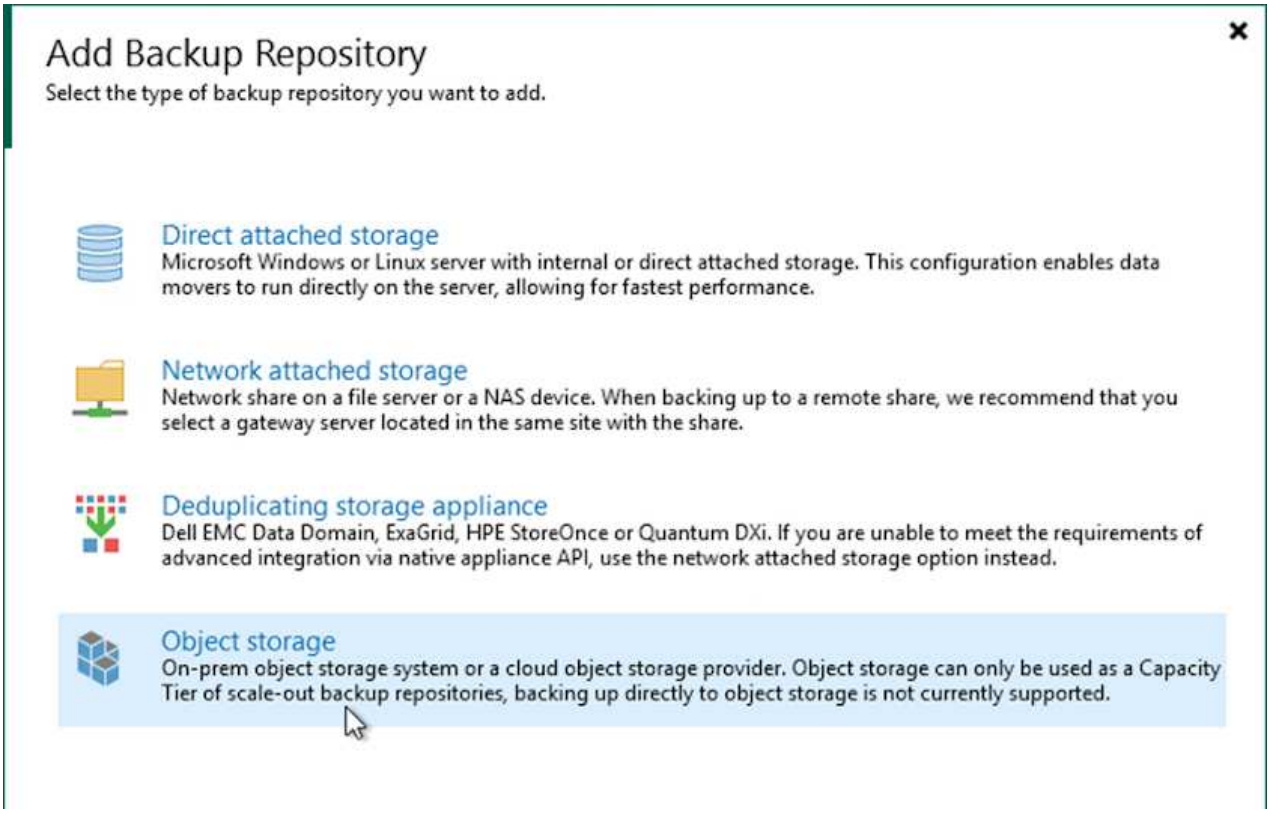
追加手順に関するコメントを参照してください。

Veeamフルリストアを使用してアプリケーション**VM**をリストアする

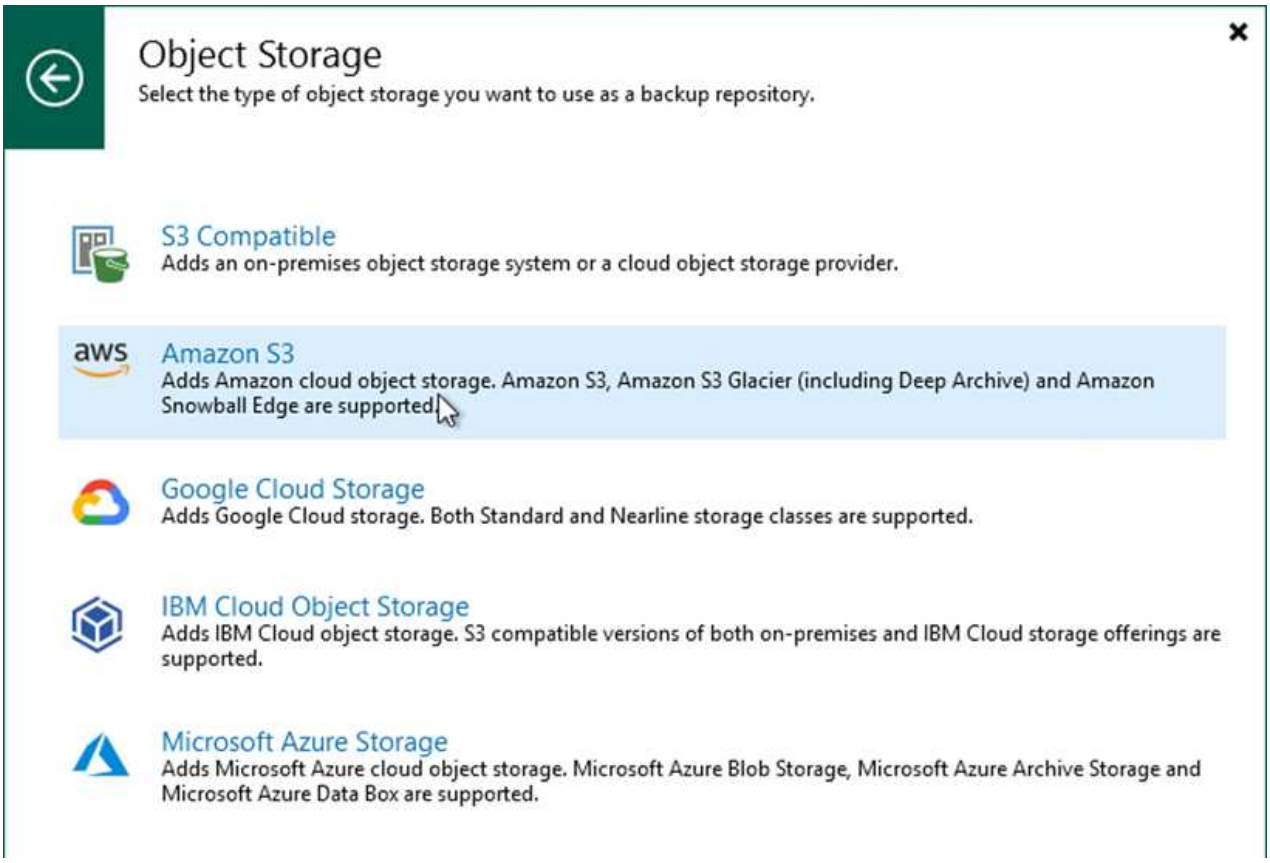
セカンダリVeeamサーバから、S3ストレージからバックアップをインポートし、SQL Server VMとOracle VMをVMware Cloudクラスタにリストアします。

オンプレミスのスケールアウトバックアップリポジトリに含まれていたS3オブジェクトからバックアップをインポートするには、次の手順を実行します。

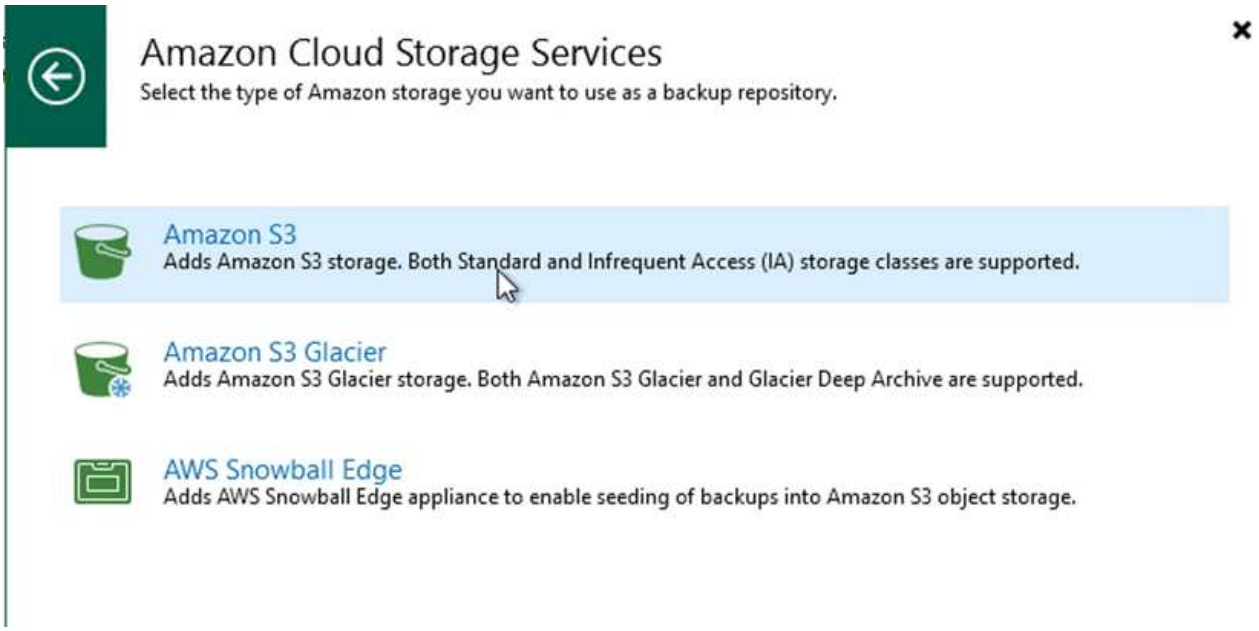
1. [バックアップリポジトリ]に移動し、上部のメニューで[リポジトリの追加]をクリックして、[バックアップリポジトリの追加]ウィザードを起動します。ウィザードの最初のページで、バックアップリポジトリタイプとしてObject Storageを選択します。



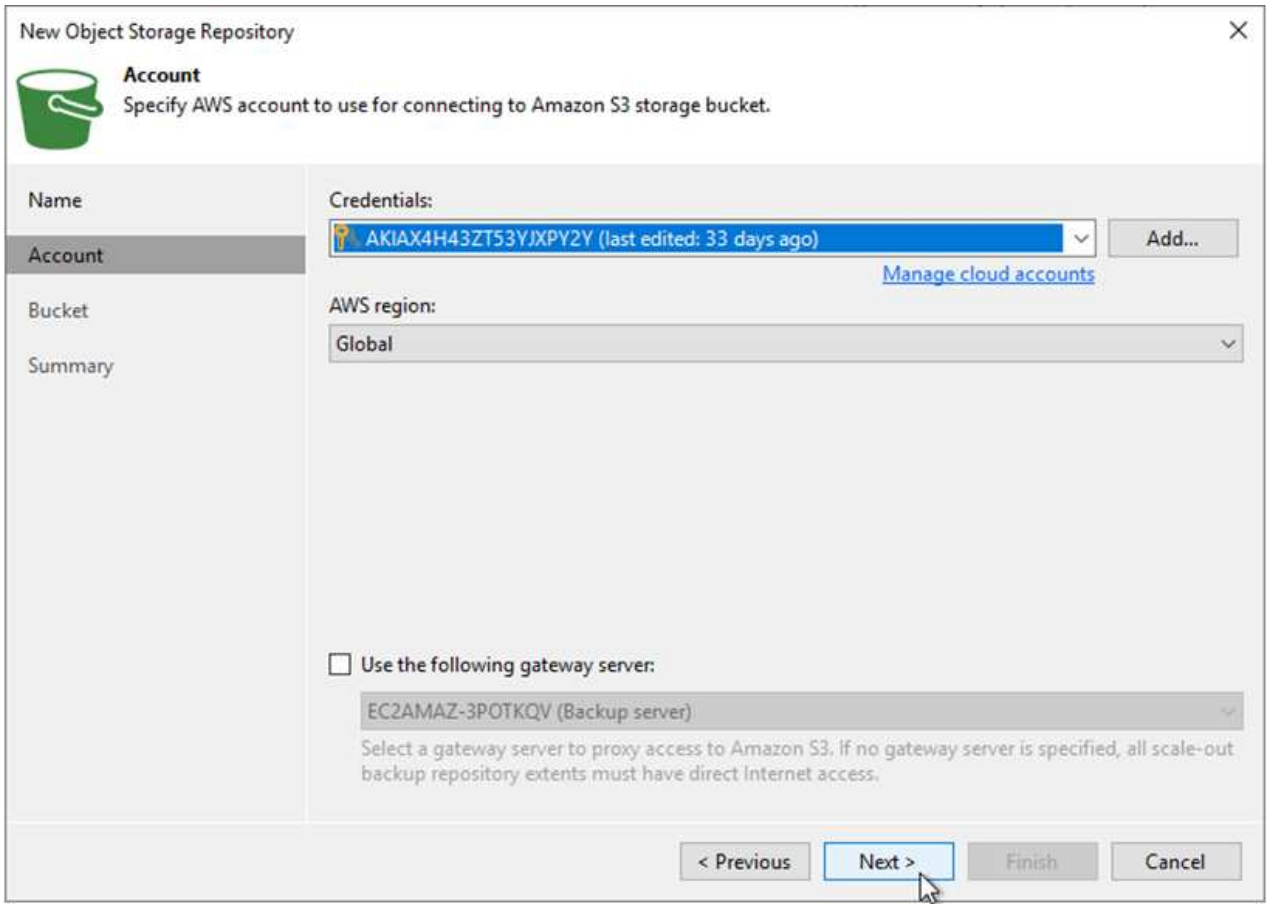
2. オブジェクトストレージタイプとしてAmazon S3を選択します。



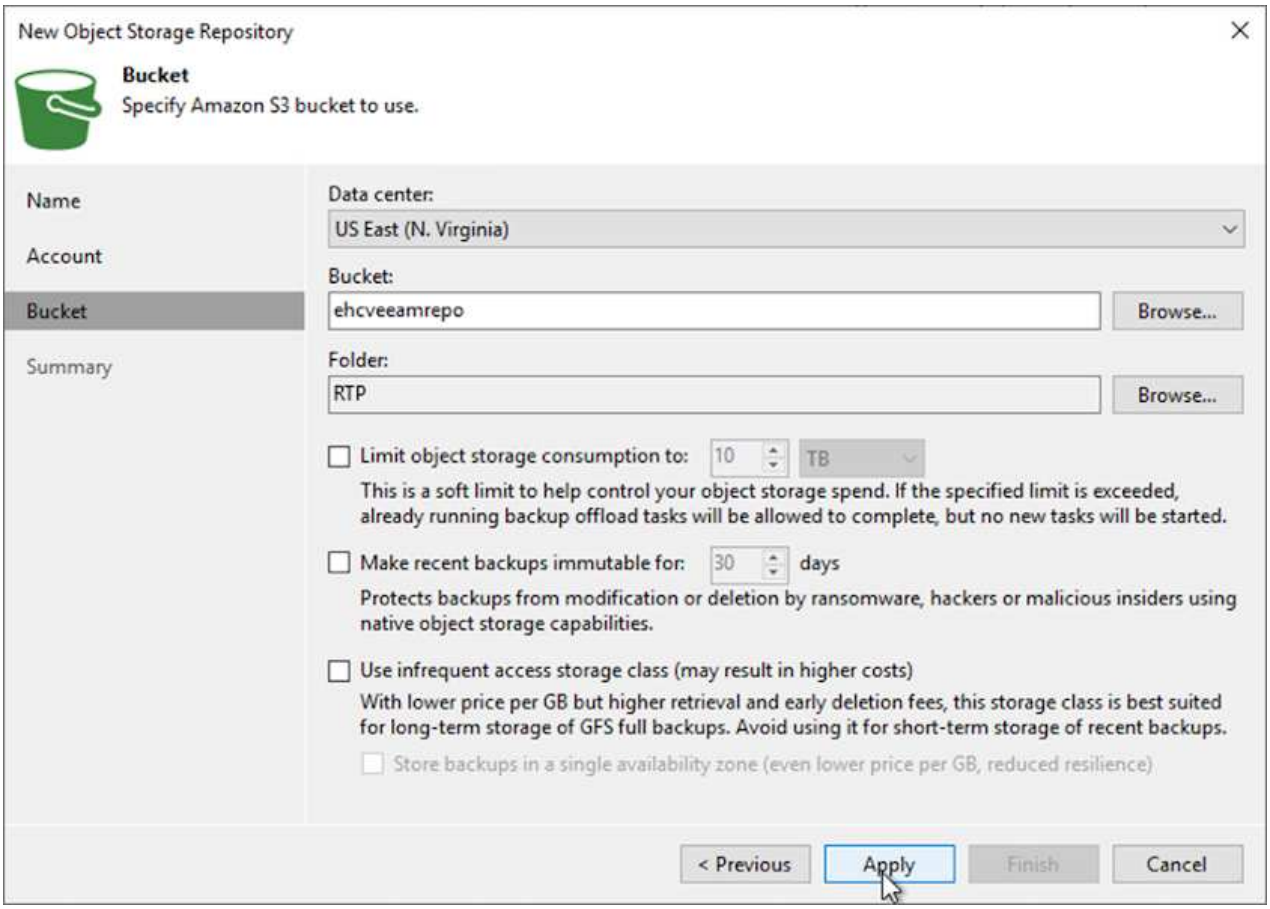
3. Amazon Cloud Storage ServicesのリストからAmazon S3を選択します。



4. ドロップダウンリストから事前に入力したクレデンシャルを選択するか、クラウドストレージリソースにアクセスするための新しいクレデンシャルを追加します。次へをクリックして続行します。



5. Bucketページで、データセンター、バケット、フォルダ、および必要なオプションを入力します。適用をクリックします。

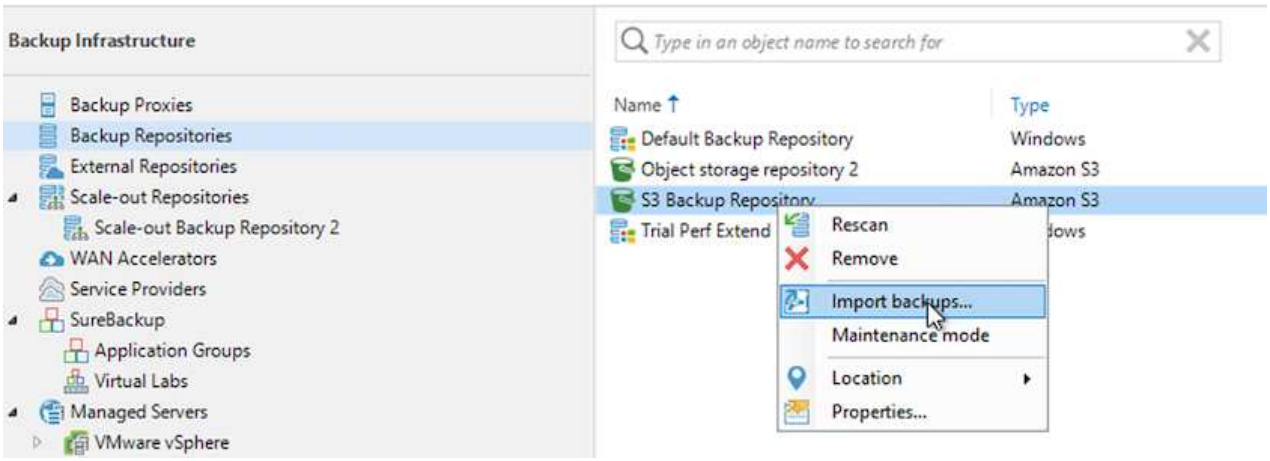


6. 最後に'完了を選択してプロセスを完了し'リポジトリを追加します

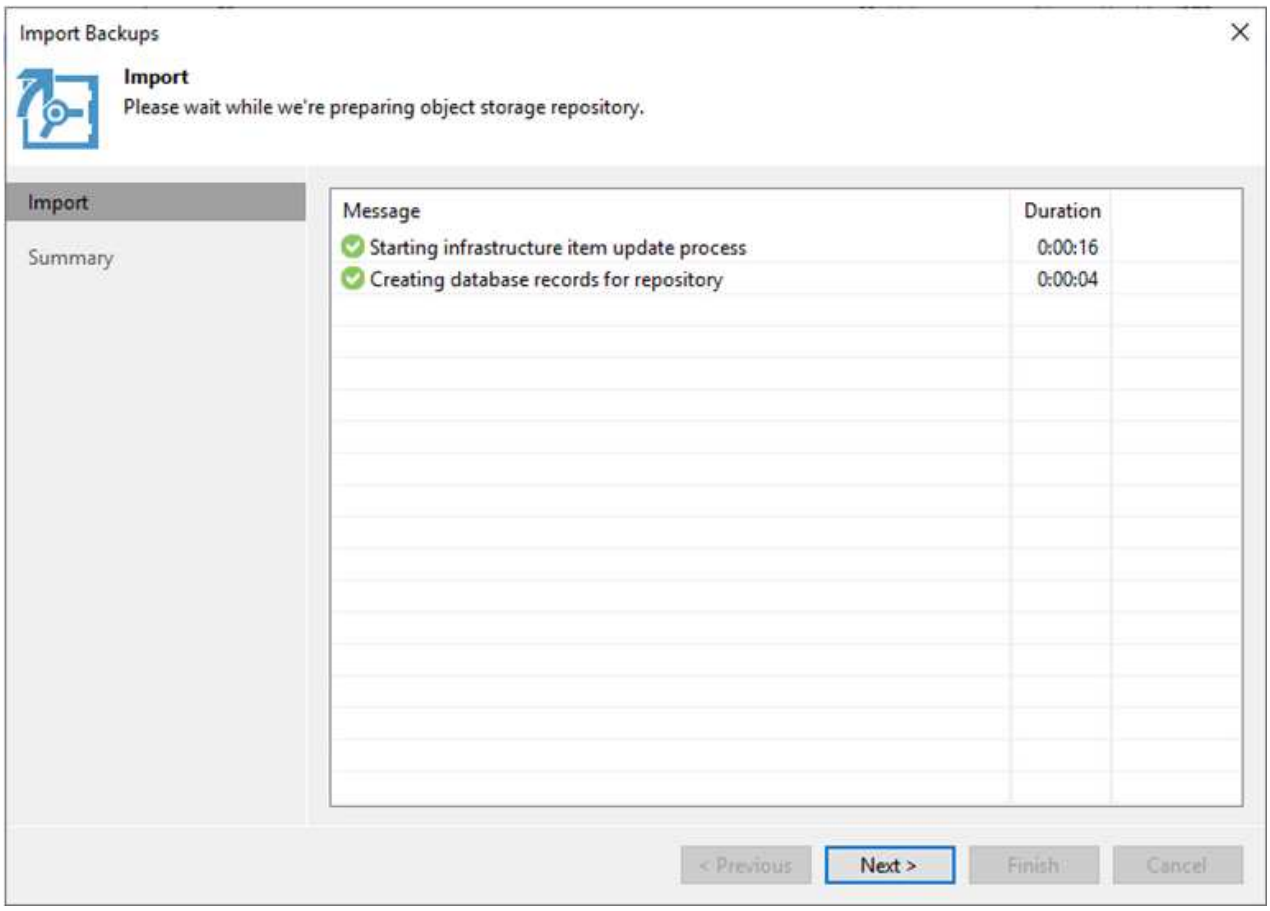
S3オブジェクトストレージからバックアップをインポートする

前のセクションで追加したS3リポジトリからバックアップをインポートするには、次の手順を実行します。

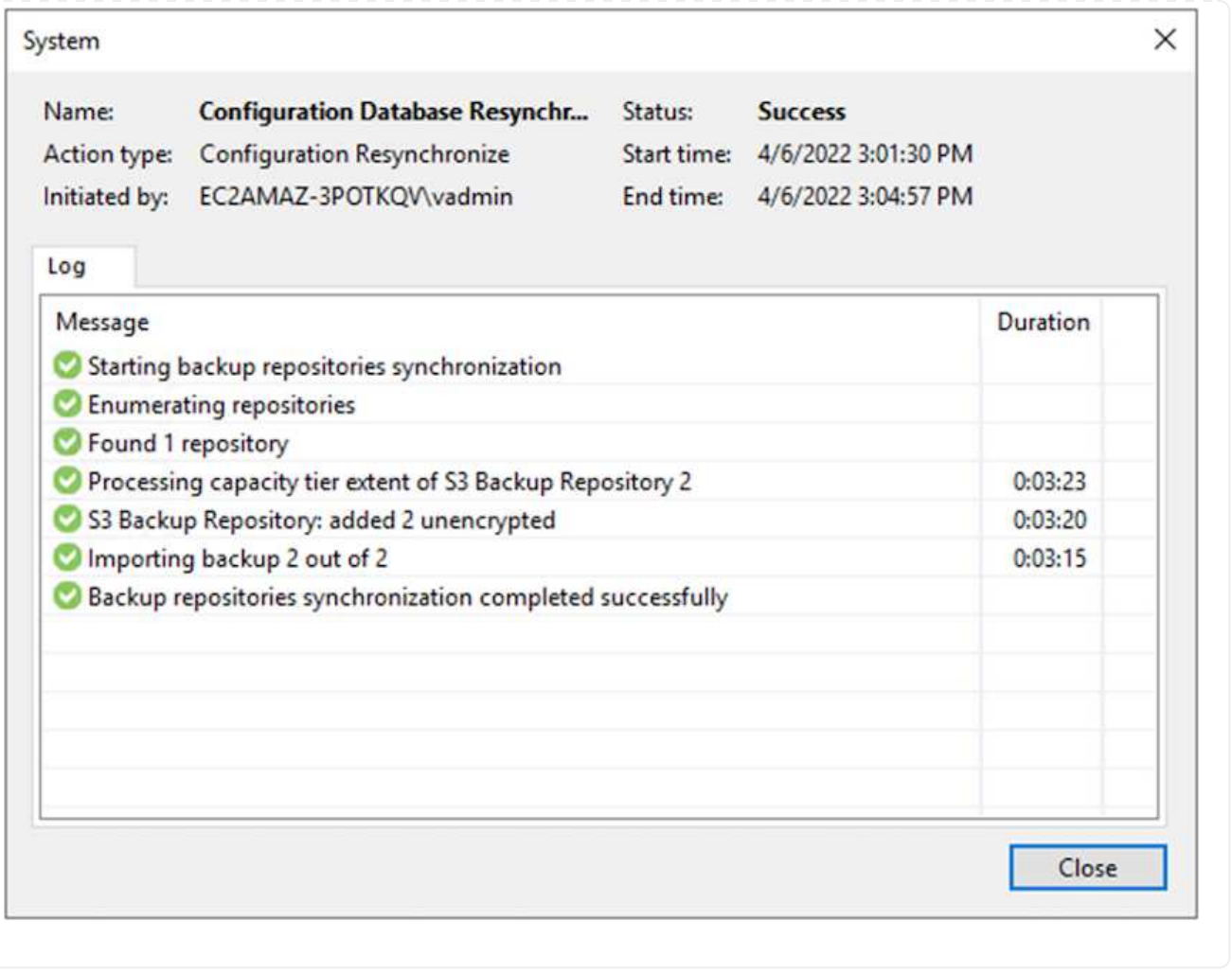
1. S3バックアップリポジトリで、バックアップのインポートを選択してバックアップのインポートウィザードを起動します。



2. インポート用のデータベースレコードが作成されたら、[次へ]を選択し、サマリー画面で[完了]を選択してインポートプロセスを開始します。

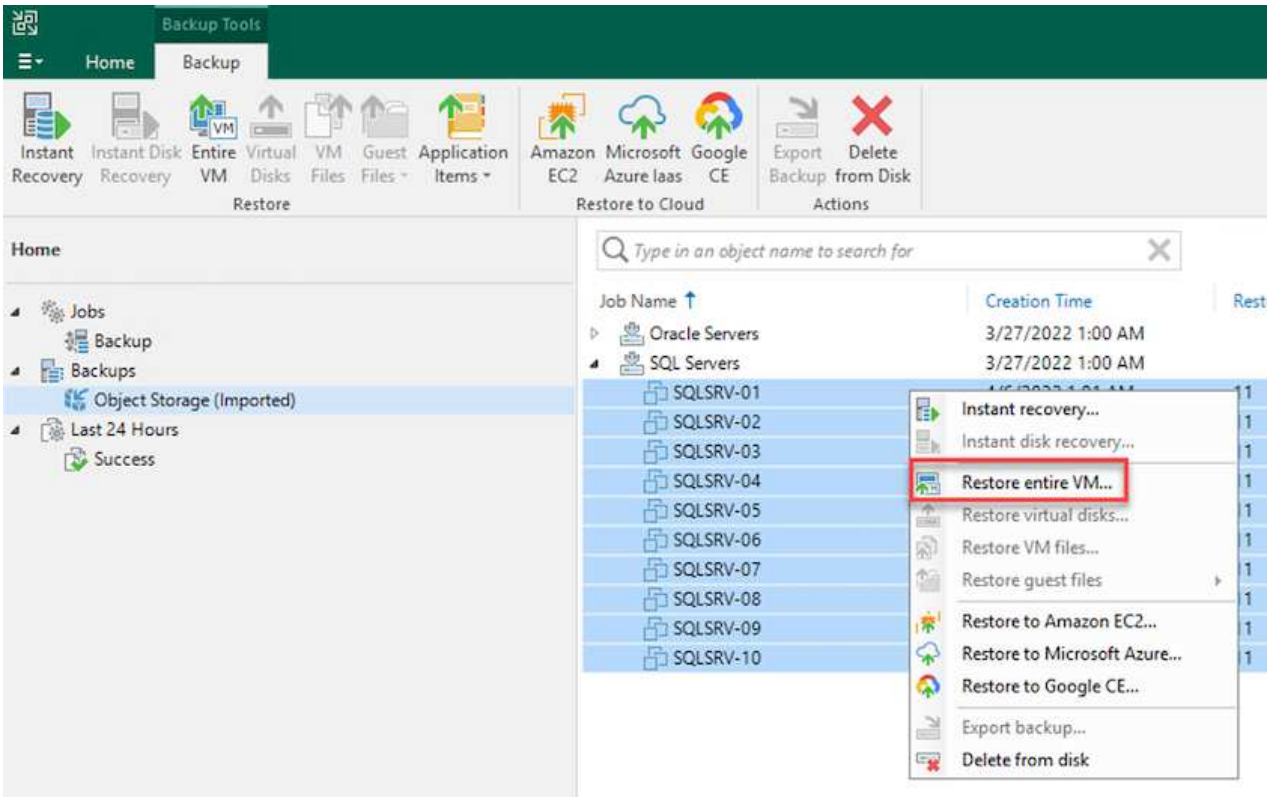


3. インポートが完了したら、VMware CloudクラスタにVMをリストアできます。

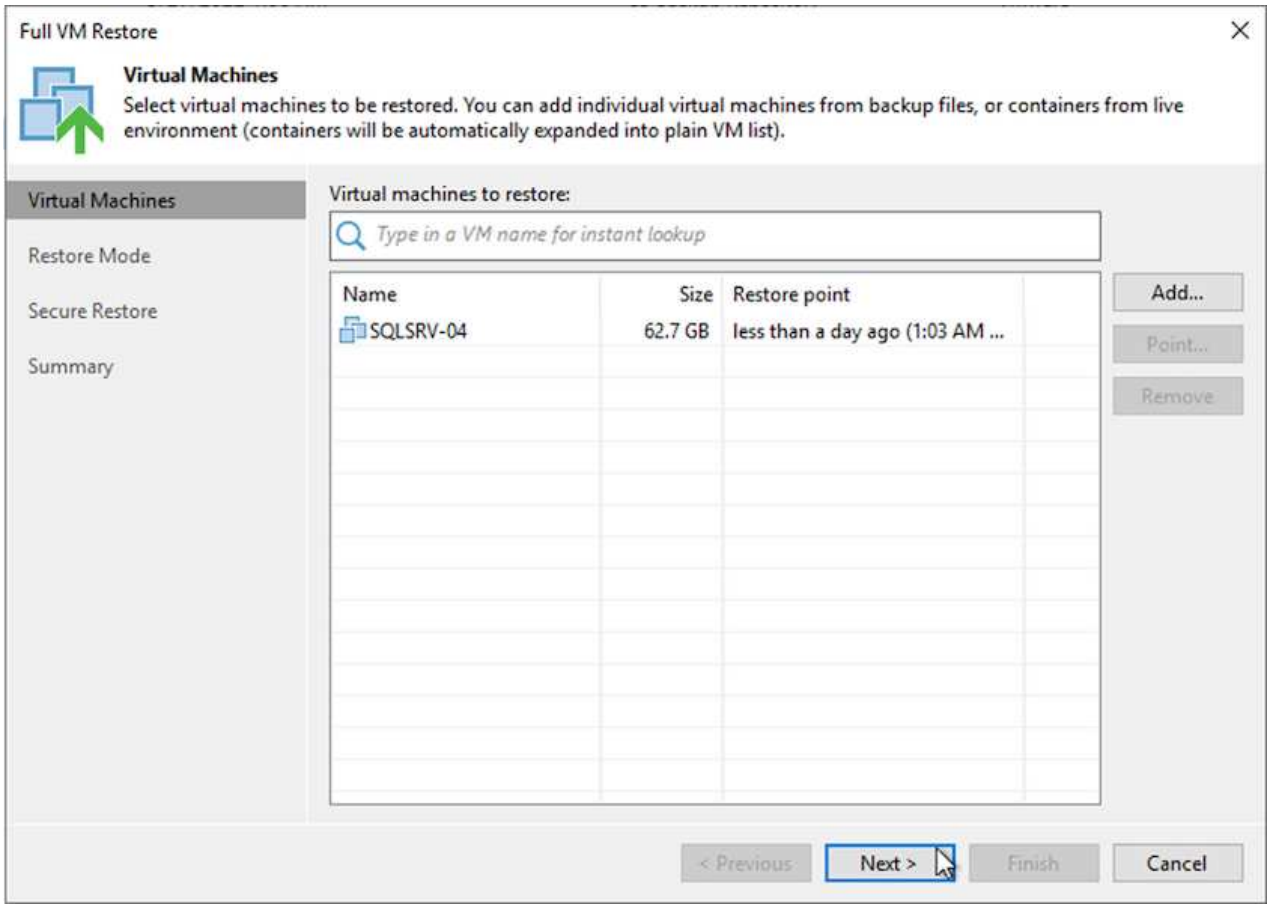

System
Name: Configuration Database Resynchr...
Status: Success
Action type: Configuration Resynchronize
Start time: 4/6/2022 3:01:30 PM
Initiated by: EC2AMAZ-3POTKQV\vadmin
End time: 4/6/2022 3:04:57 PM
Log
Message
Duration
Starting backup repositories synchronization
Enumerating repositories
Found 1 repository
Processing capacity tier extent of S3 Backup Repository 2
0:03:23
S3 Backup Repository: added 2 unencrypted
0:03:20
Importing backup 2 out of 2
0:03:15
Backup repositories synchronization completed successfully
Close

SQLおよびOracle仮想マシンをAWSワークロードドメイン/クラスタ上のVMware Cloudにリストアするには、次の手順を実行します。

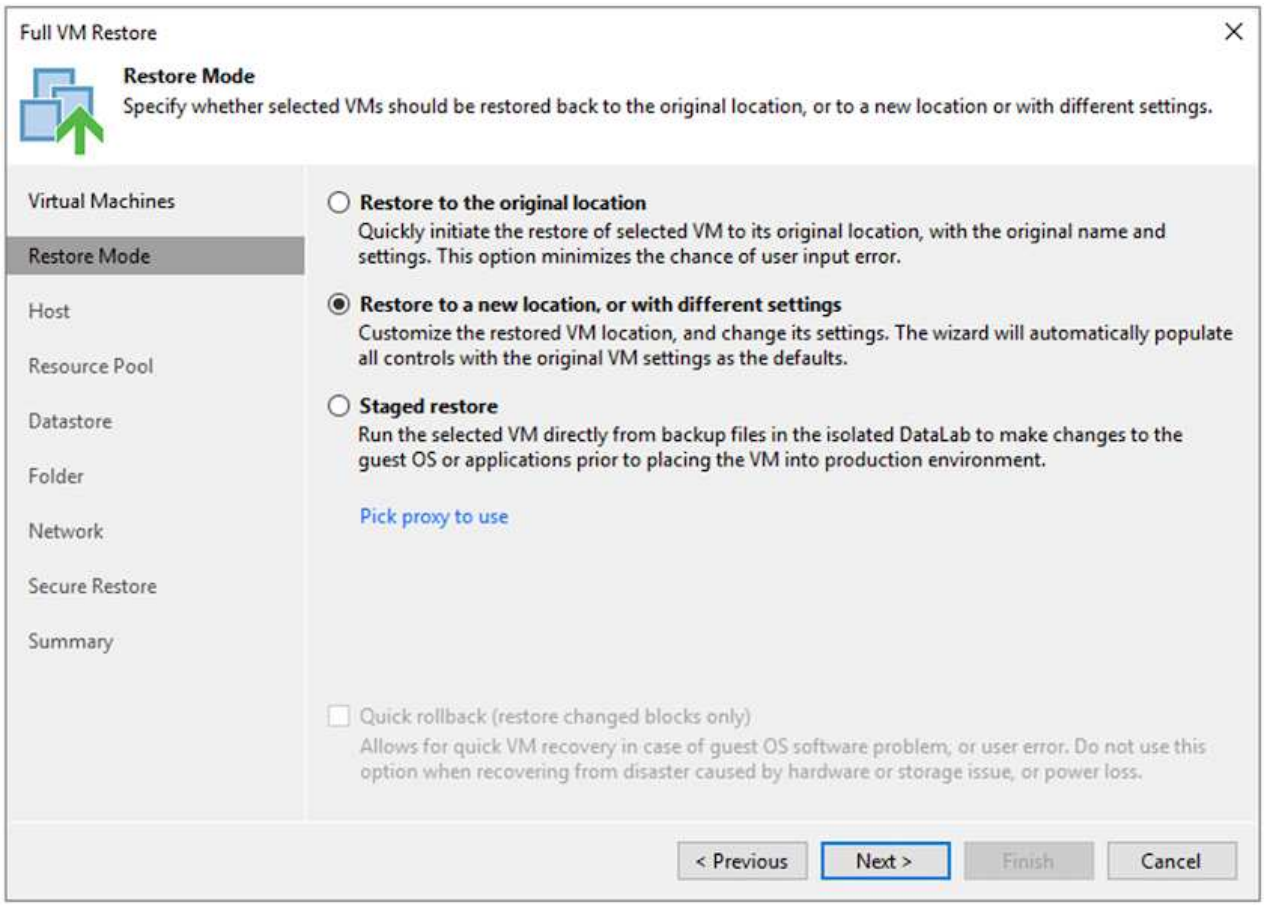
1. Veeamのホームページで、インポートしたバックアップを含むオブジェクトストレージを選択し、リストアするVMを選択して右クリックし、Restore Entire VM（VM全体のリストア）を選択します。



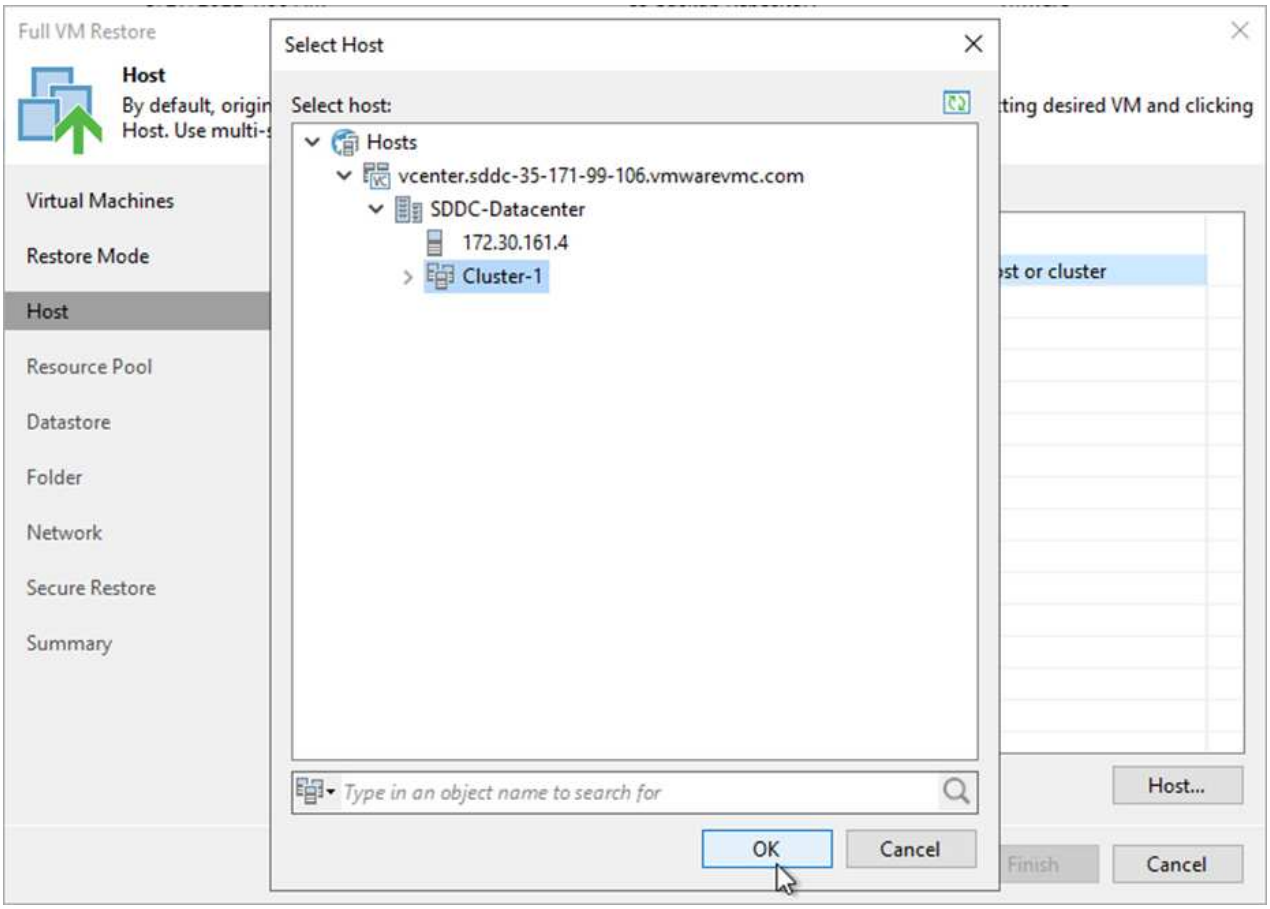
2. [Full VM Restore]ウィザードの最初のページで、必要に応じてVMをバックアップに変更し、[Next]を選択します。



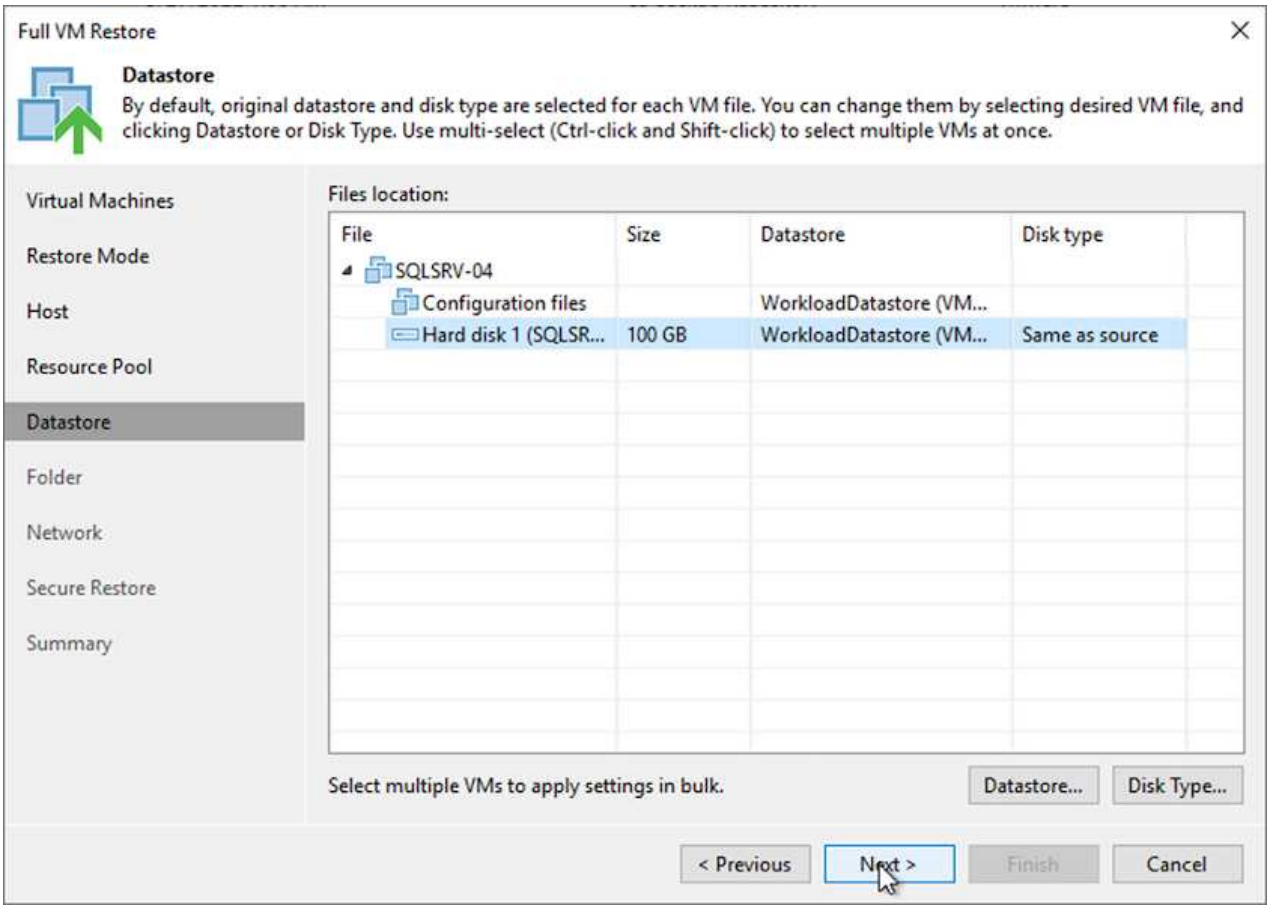
3. [復元モード]ページで、[新しい場所に復元]または[別の設定]を選択します。



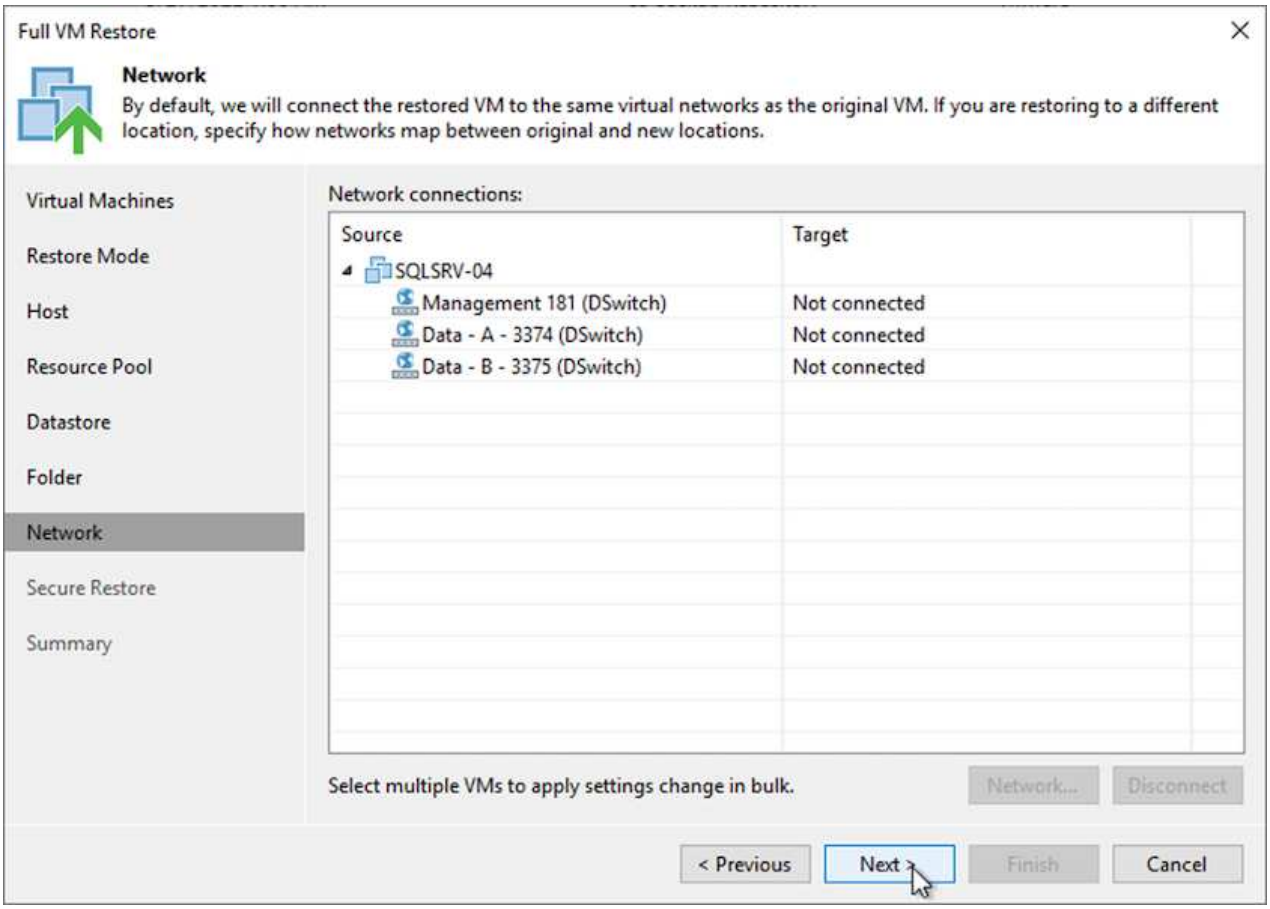
4. ホストページで、VMのリストア先となるターゲットESXiホストまたはクラスタを選択します。

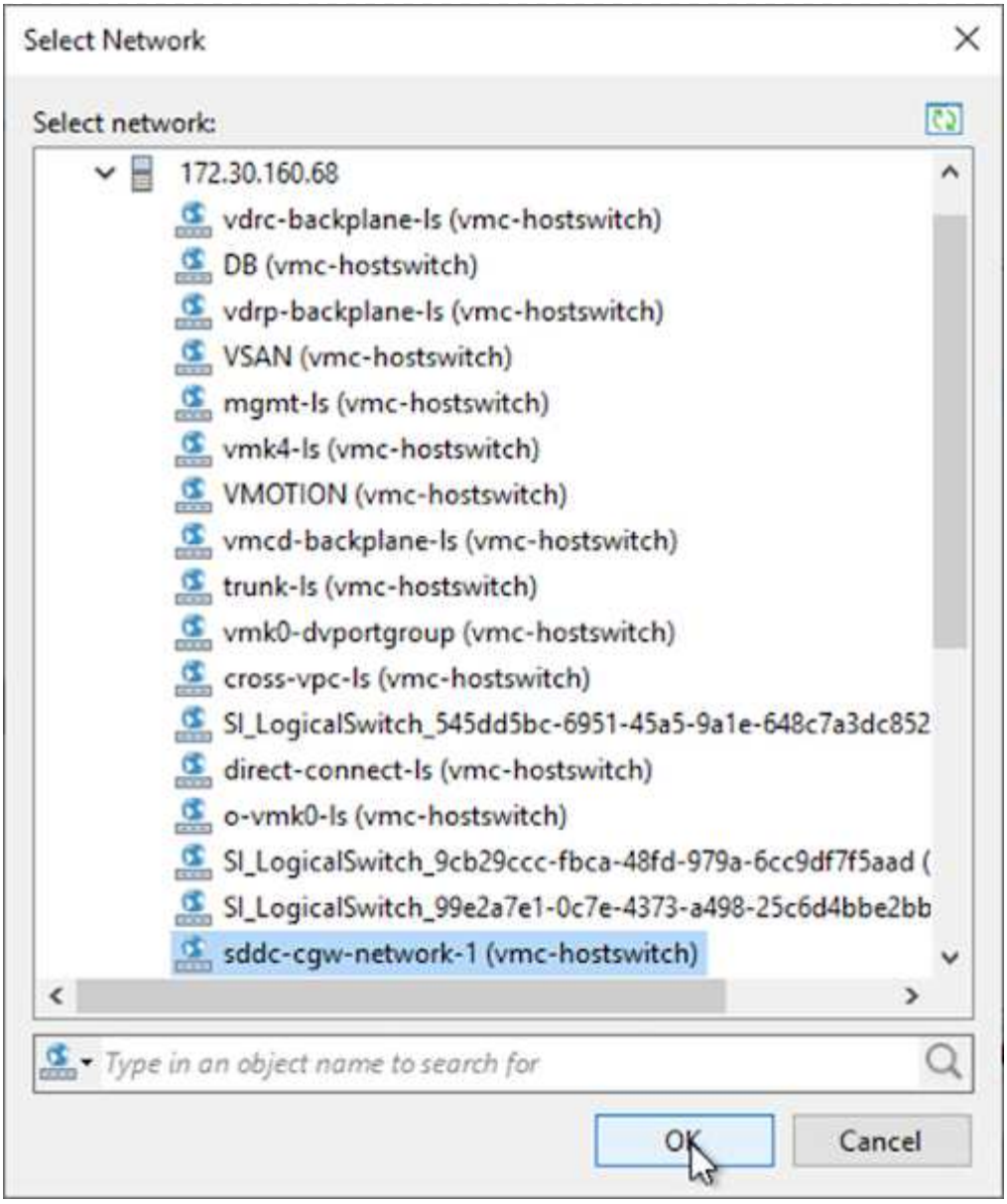


5. Datastores（データストア）ページで、構成ファイルとハードディスクの両方のターゲットデータストアの場所を選択します。



6. [ネットワーク]ページで、VM上の元のネットワークを新しいターゲットの場所にあるネットワークにマッピングします。


Full VM Restore
Network
By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.
Virtual Machines
Restore Mode
Host
Resource Pool
Datastore
Folder
Network
Secure Restore
Summary
Network connections:
Source
Target
SQLSRV-04
Management 181 (DSwitch)
Not connected
Data - A - 3374 (DSwitch)
Not connected
Data - B - 3375 (DSwitch)
Not connected
Select multiple VMs to apply settings change in bulk.
Network...
Disconnect
< Previous
Next >
Finish
Cancel



7. 復元されたVMをスキャンしてマルウェアを検出するかどうかを選択し、概要ページを確認してから、完了をクリックして復元を開始します。

SQL Serverアプリケーションデータをリストアする

次のプロセスでは、オンプレミスサイトが動作不能になった場合に、VMwareクラウド サービス でAWS内のSQL Serverをリカバリする方法について説明します。

リカバリ手順を続行するには、次の前提条件を満たしている必要があります。

1. Windows Server VMがVeeam Full Restoreを使用してVMware Cloud SDDCにリストアされている。
2. セカンダリSnapCenter サーバが確立され、セクションで説明する手順に従ってSnapCenter データベースのリストアと設定が完了している "SnapCenter のバックアップとリストアのプロセスの概要"

VM：SQL Server VMのリストア後の設定

VMのリストアが完了したら、SnapCenter でホストVMを再検出するための準備として、ネットワークやその他の項目を設定する必要があります。

1. 管理およびiSCSIまたはNFS用に新しいIPアドレスを割り当てます。
2. ホストをWindowsドメインに追加します。
3. DNSにホスト名を追加するか、SnapCenter サーバのhostsファイルにホスト名を追加します。

SnapCenter プラグインが現在のドメインとは異なるドメインクレデンシャルを使用して導入されている場合は、SQL Server VMでPlug-in for Windowsサービスのログオンアカウントを変更する必要があります。ログオンアカウントを変更したら、SnapCenter SMCore、Plug-in for Windows、およびPlug-in for SQL Serverの各サービスを再起動します。

リストアされたVMをSnapCenter で自動的に再検出するには、FQDNをオンプレミスのSnapCenter に最初に追加されたVMと同じにする必要があります。

SQL Serverリストア用にFSXストレージを構成します

SQL Server VMのディザスタリカバリリストアプロセスを実行するには、既存のSnapMirror関係をFSXクラスタから解除し、ボリュームへのアクセスを許可する必要があります。これには、次の手順を実行します。

1. SQL Serverデータベースボリュームとログボリュームの既存のSnapMirror関係を解除するには、FSX CLIから次のコマンドを実行します。

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

2. SQL Server Windows VMのiSCSI IQNを含むイニシエータグループを作成して、LUNへのアクセスを許可します。

```
FSx-Dest::> igroup create -vserver DestSVM -igroup igroupName
-protocol iSCSI -ostype windows -initiator IQN
```

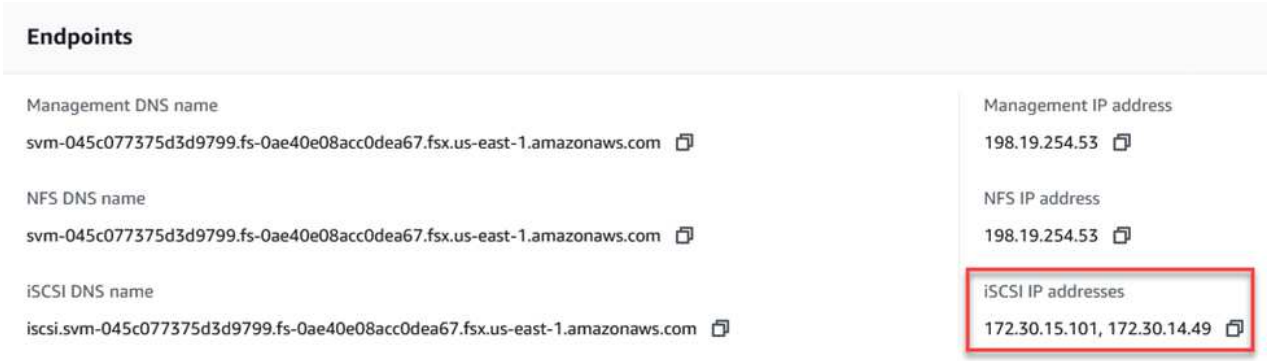
3. 最後に、作成したigroupにLUNをマッピングします。

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup
igroupName
```

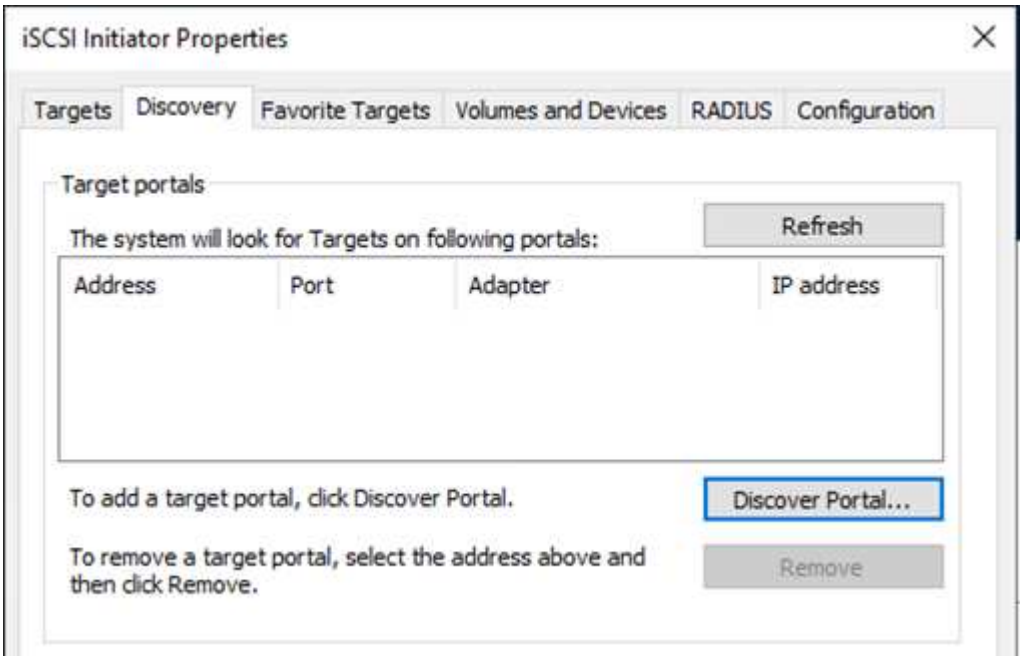
4. パス名を検索するには'lun showコマンドを実行します

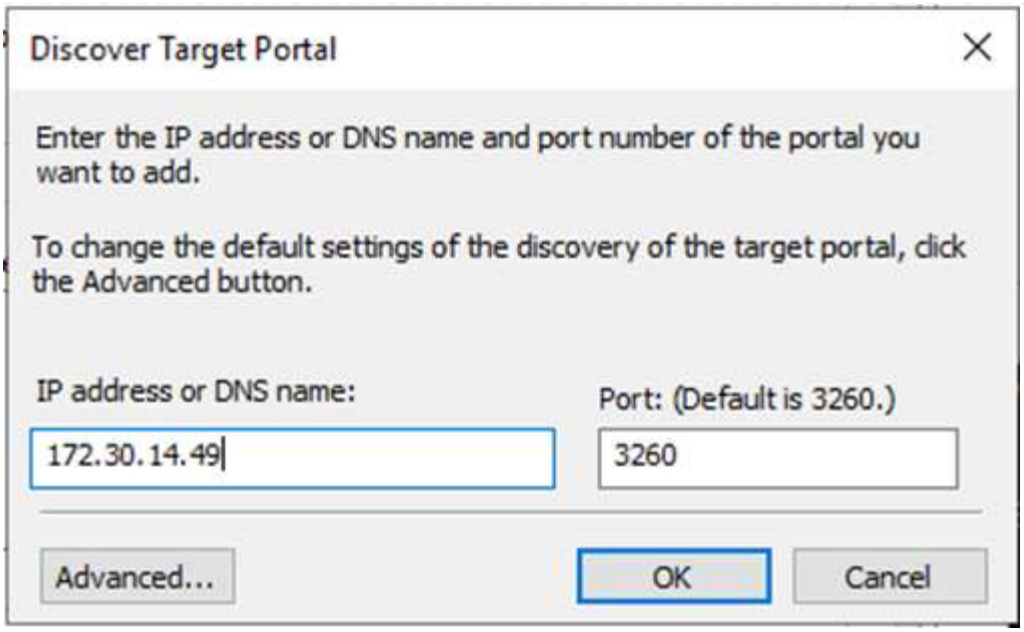
Windows VMでiSCSIアクセスを設定し、ファイルシステムを検出します

1. SQL Server VMからiSCSIネットワークアダプタをセットアップし、FSXインスタンス上のiSCSIターゲットインターフェイスへの接続が確立されたVMwareポートグループ上で通信します。
2. iSCSI Initiator Propertiesユーティリティを開き、Discovery、Favorite Targets、およびTargetsタブの古い接続設定を消去します。
3. FSXインスタンス/クラスタ上のiSCSI論理インターフェイスにアクセスするためのIPアドレスを特定します。これは、AWSコンソールのAmazon FSX > ONTAP > Storage Virtual Machinesの下にあります。

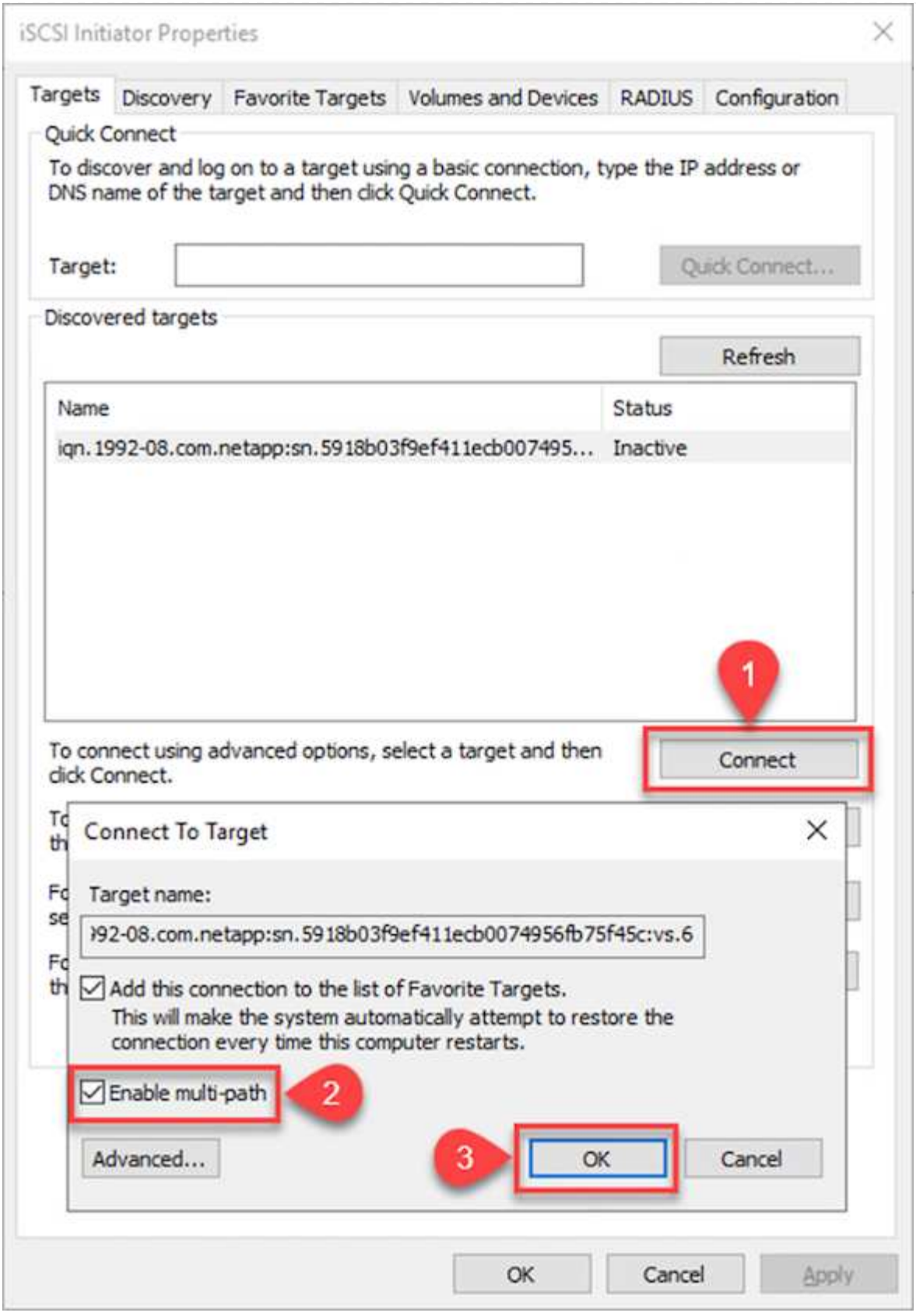


4. [Discovery]タブで[Discover Portal]をクリックし、FSX iSCSIターゲットのIPアドレスを入力します。

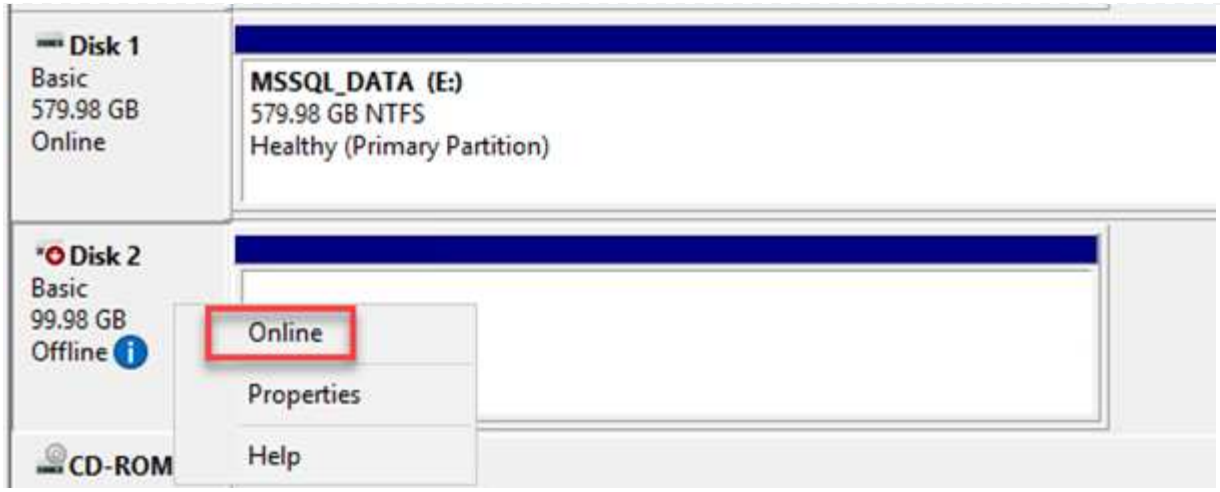




5. [ターゲット]タブで[接続]をクリックし、構成に応じて[マルチパスを有効にする]を選択し、[OK]をクリックしてターゲットに接続します。

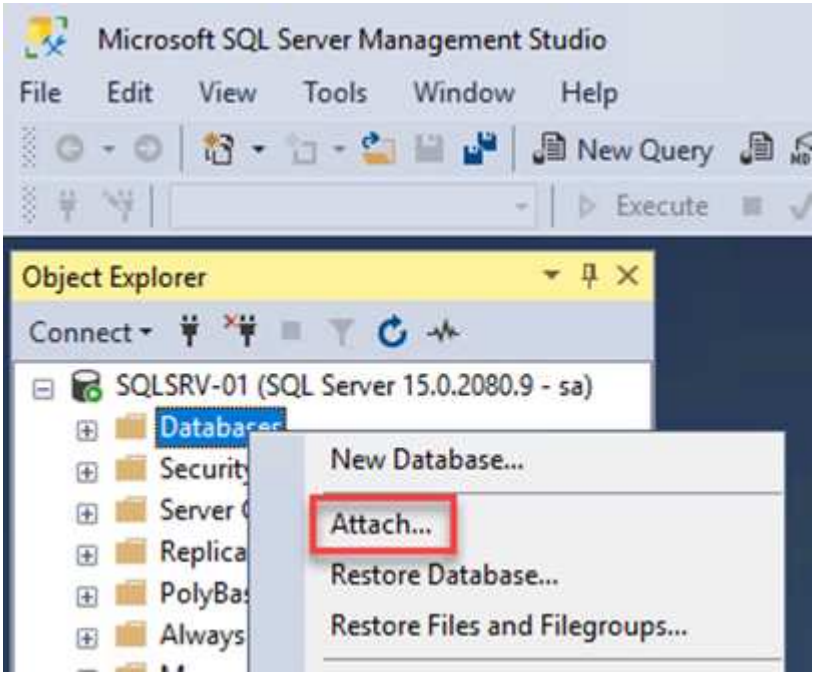


6. コンピュータの管理ユーティリティを開き、ディスクをオンラインにします。以前と同じドライブレターを保持していることを確認します。

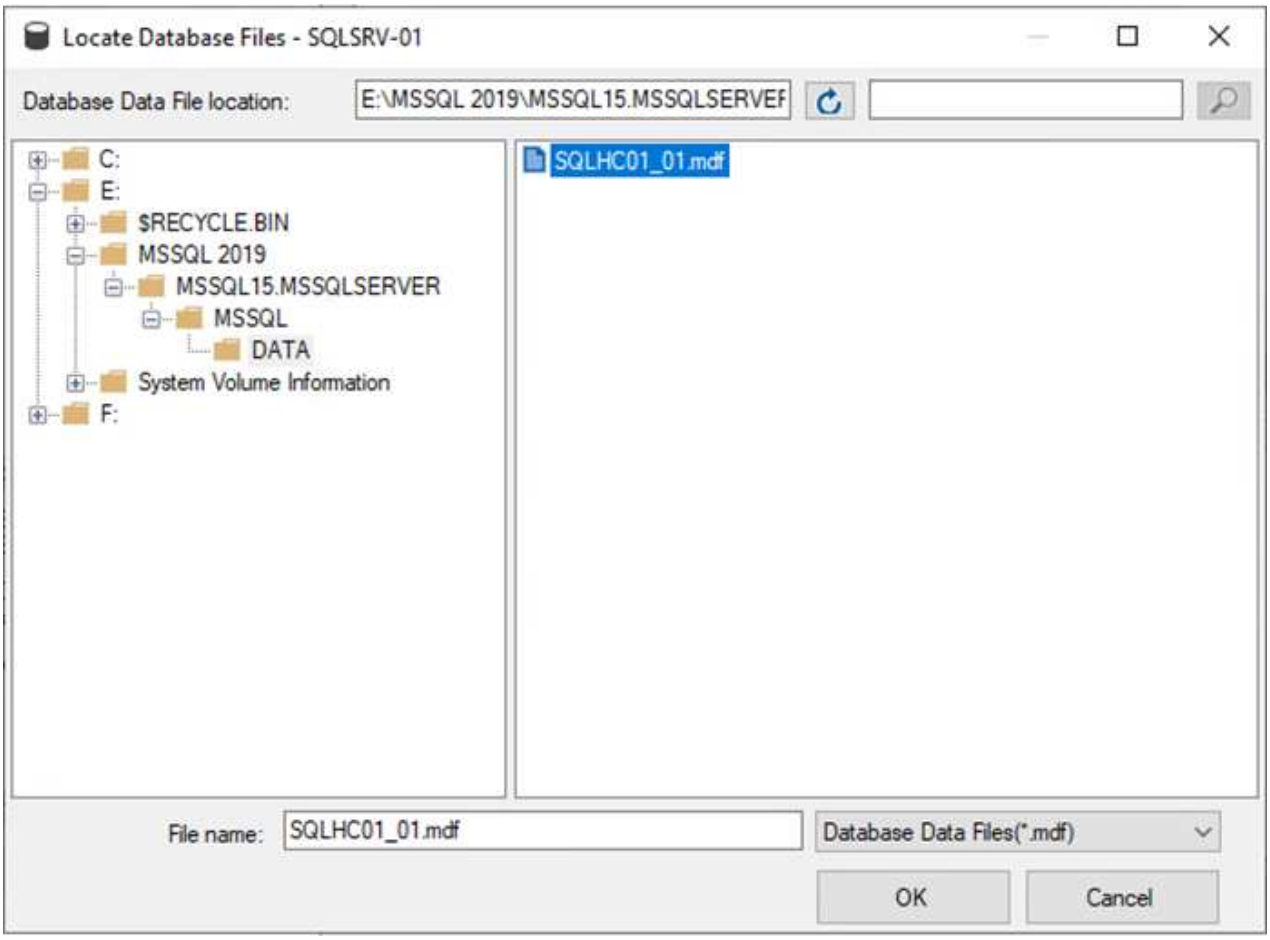

Disk 1
Basic
579.98 GB
Online
MSSQL_DATA (E:)
579.98 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
99.98 GB
Offline
Online
Properties
Help
CD-ROM

SQL Serverデータベースを接続します

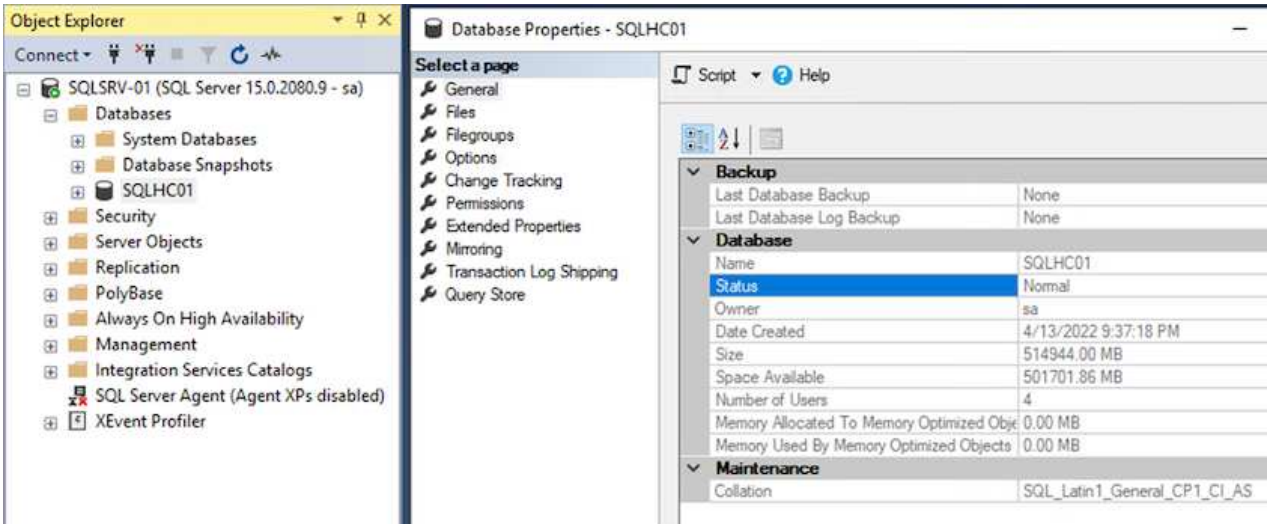
1. SQL Server VMで、Microsoft SQL Server Management Studioを開き、接続を選択してデータベースへの接続プロセスを開始します。



2. [追加]をクリックし、SQL Serverプライマリデータベースファイルが格納されているフォルダに移動して選択し、[OK]をクリックします。



3. トランザクションログが別のドライブにある場合は、トランザクションログが格納されているフォルダを選択します。
4. 終了したら、[OK]をクリックしてデータベースに接続します。

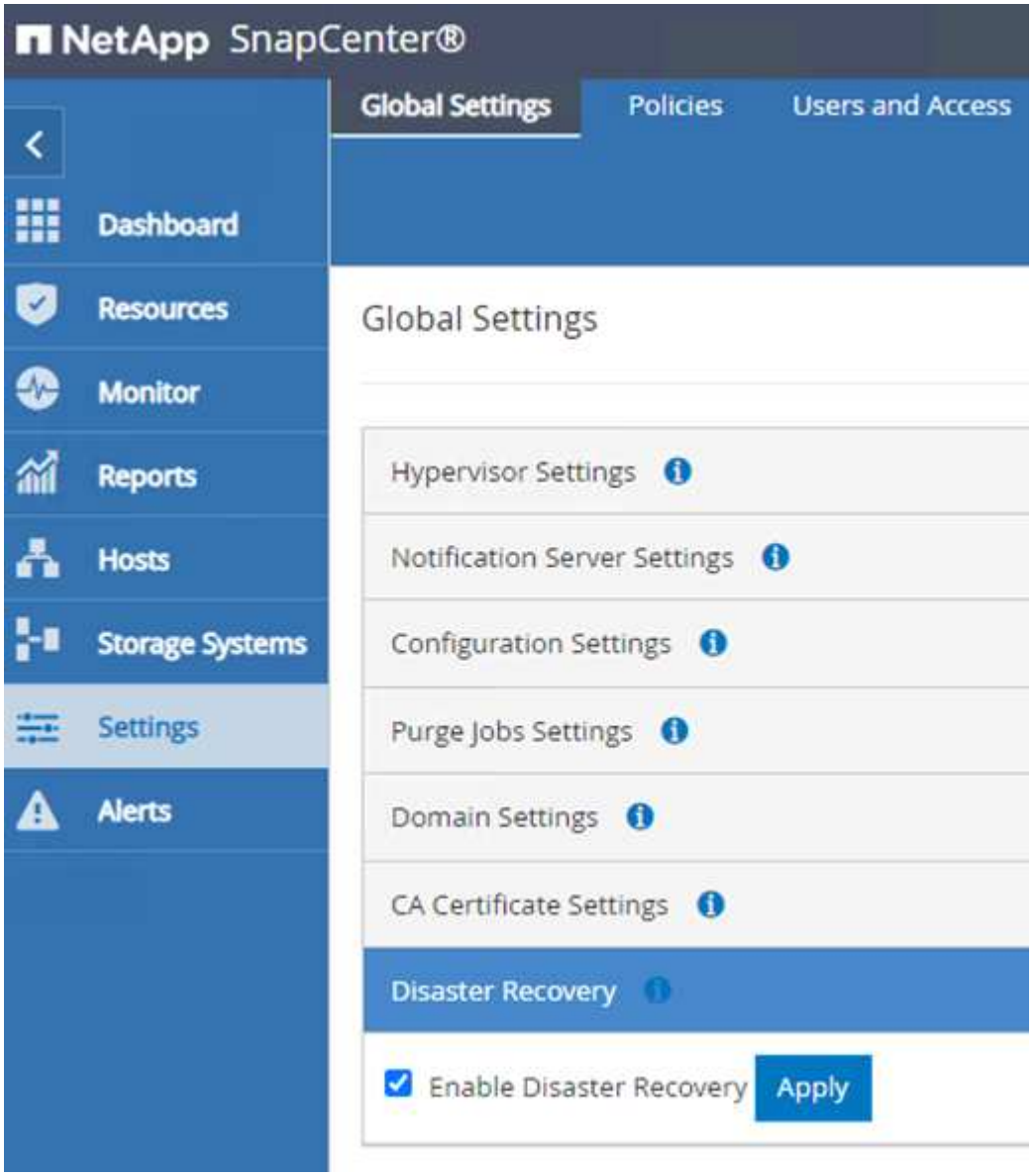


SQL Server Plug-inとのSnapCenter 通信を確認します

SnapCenter データベースを以前の状態にリストアすると、SQL Serverホストが自動的に再検出されます。これを正しく機能させるには、次の前提条件に注意してください。

- SnapCenter はディザスタリカバリモードにする必要があります。これは、Swagger APIまたはディザスタリカバリのグローバル設定で実行できます。
- SQL ServerのFQDNは、オンプレミスのデータセンターで実行されていたインスタンスと同じである必要があります。
- 元のSnapMirror関係が解除されている必要があります。
- データベースを含むLUNをSQL Serverインスタンスにマウントし、データベースを接続しておく必要があります。

SnapCenter がディザスタリカバリモードになっていることを確認するには、SnapCenter Webクライアントで設定に移動します。[グローバル設定]タブに移動し、[災害復旧]をクリックします。ディザスタリカバリを有効にするチェックボックスがオンになっていることを確認します。



Oracleアプリケーションデータをリストアします

次のプロセスでは、オンプレミスサイトが動作不能になった場合に、VMwareクラウド サービス でAWS でOracleアプリケーションデータをリカバリする方法について説明します。

リカバリ手順を続行するには、次の前提条件を満たしている必要があります。

1. Veeam Full Restoreを使用して、Oracle LinuxサーバVMがVMware Cloud SDDCにリストアされている。
2. セカンダリSnapCenter サーバが確立され、このセクションで説明する手順でSnapCenter データベースおよび構成ファイルがリストアされている "SnapCenter のバックアップとリストアのプロセスの概要"

FSxNインスタンスでホストされているセカンダリストレージボリュームにOracleサーバからアクセスできるようにするには、まず既存のSnapMirror関係を解除する必要があります。

1. FSX CLIにログインした後、次のコマンドを実行して、正しい名前でフィルタリングされたボリュームを表示します。

```
FSx-Dest::> volume show -volume VolumeName*
```

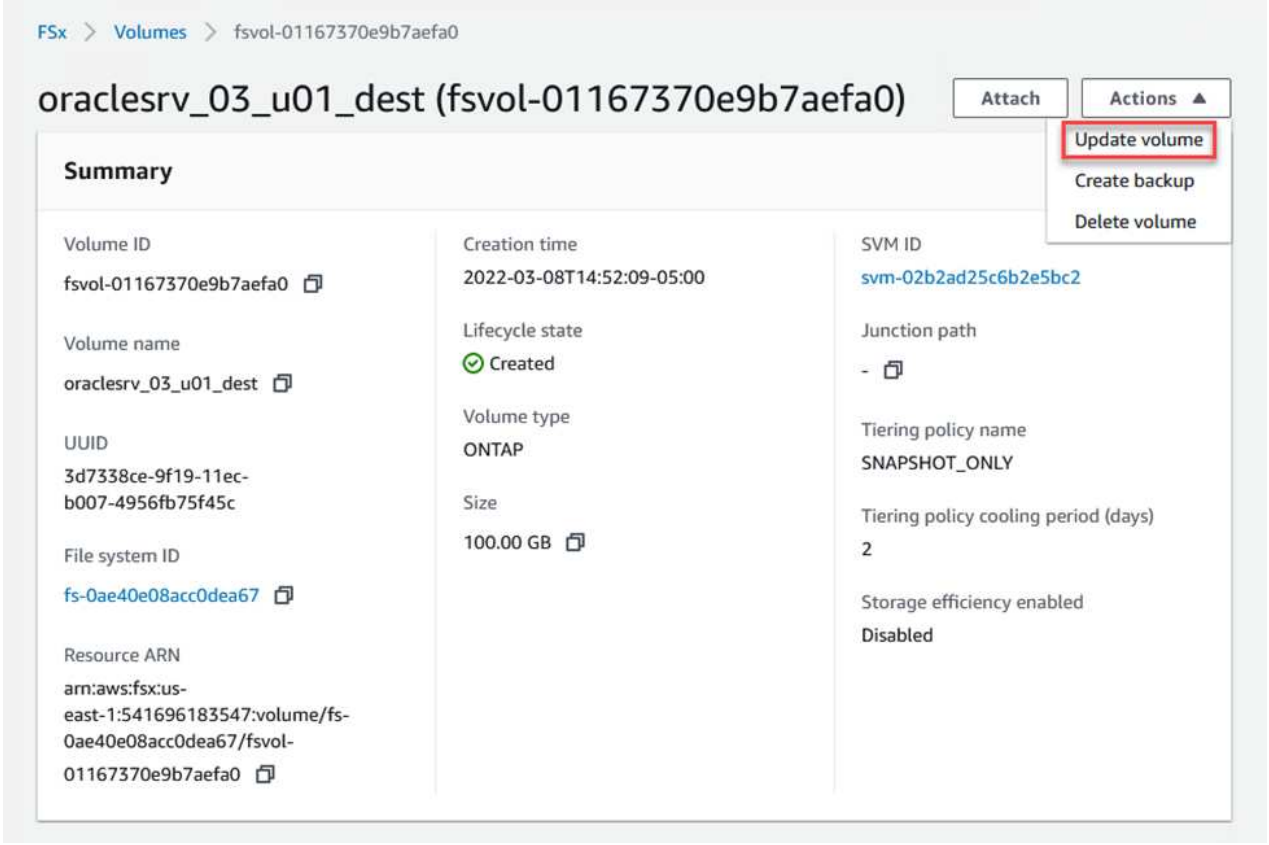
```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
ora_svm_dest
          oraclesrv_03_u01_dest
                       aggr1        online     DP        100GB    93.12GB    6%
ora_svm_dest
          oraclesrv_03_u02_dest
                       aggr1        online     DP        200GB    34.98GB   82%
ora_svm_dest
          oraclesrv_03_u03_dest
                       aggr1        online     DP        150GB    33.37GB   77%
3 entries were displayed.

FsxId0ae40e08acc0dea67::>
```

2. 次のコマンドを実行して、既存のSnapMirror関係を解除します。

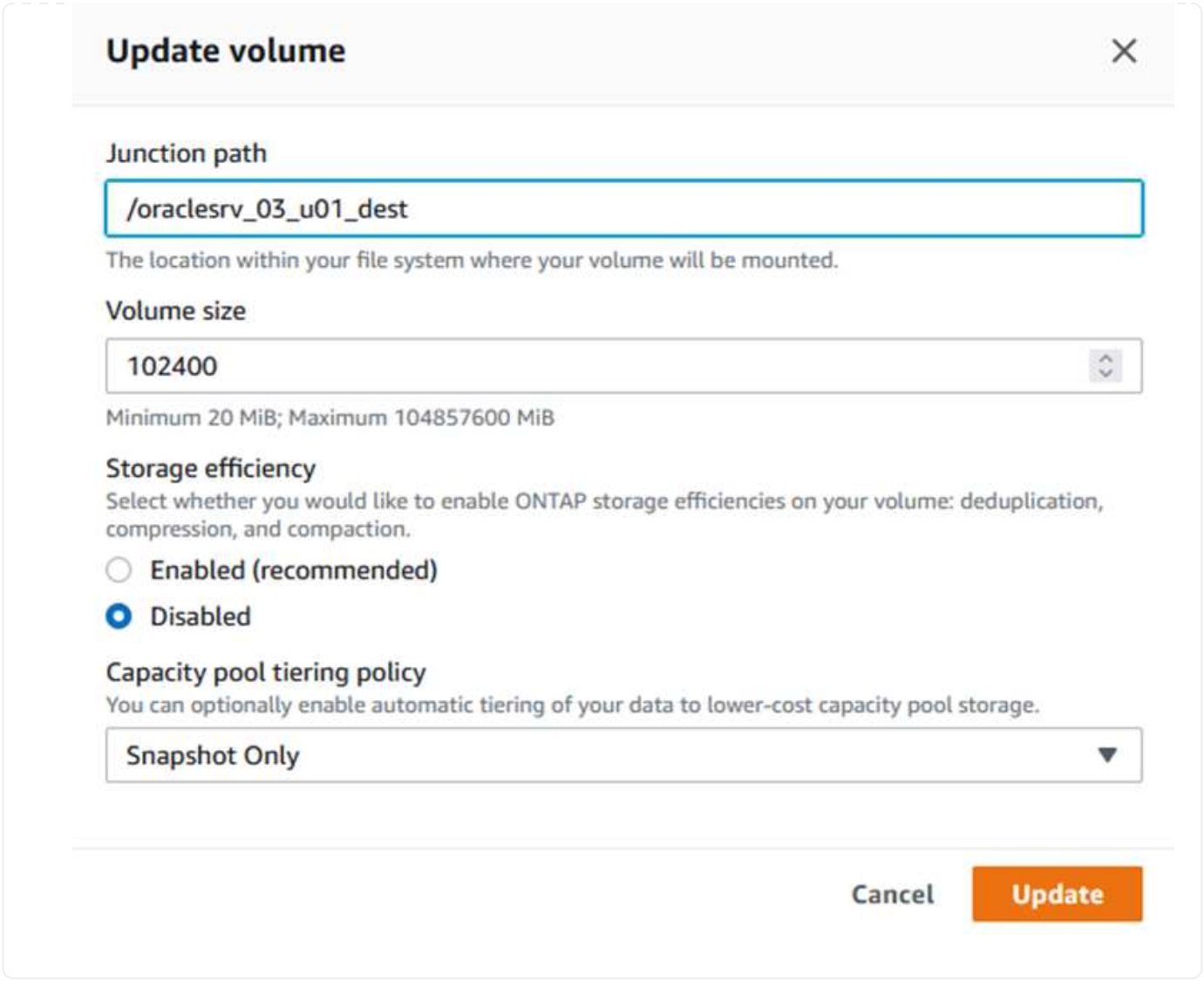
```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".
```

3. Amazon FSX Web Clientでjunction-pathを更新します。



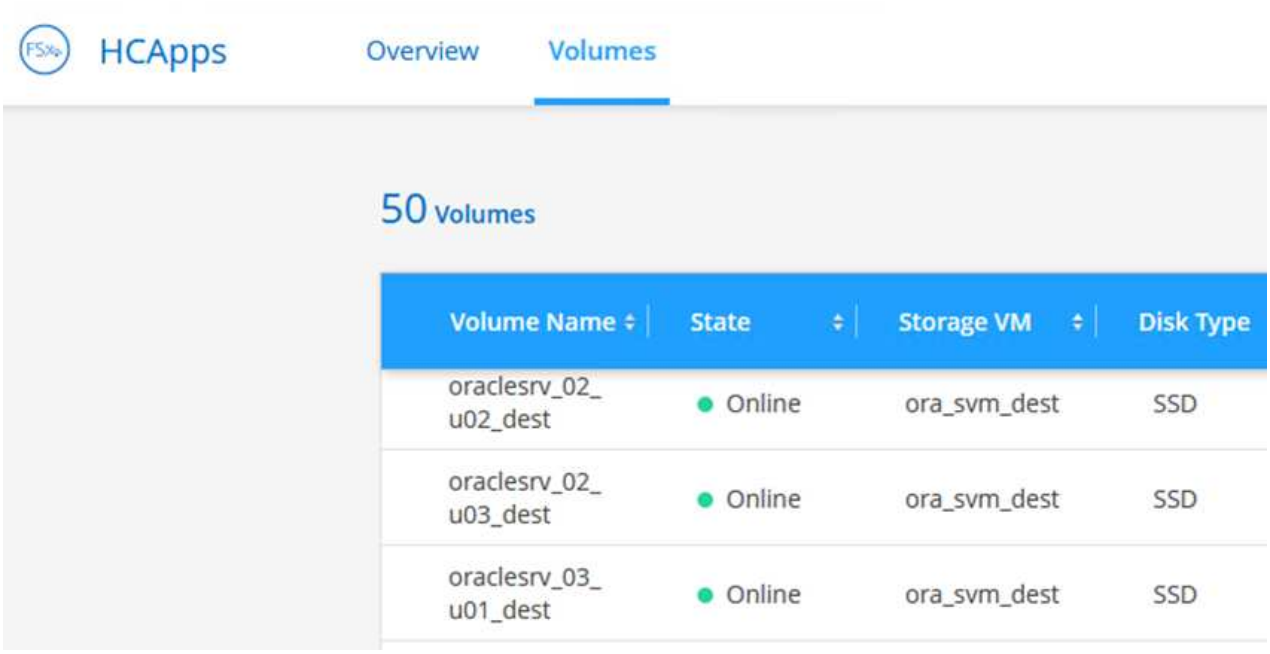
4. ジャンクションパス名を追加し、更新（Update）をクリックする。OracleサーバからNFSボリュームをマウントする際に、このジャンクションパスを指定します。


Update volume
Junction path
/oraclesrv_03_u01_dest
The location within your file system where your volume will be mounted.
Volume size
102400
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
Cancel
Update

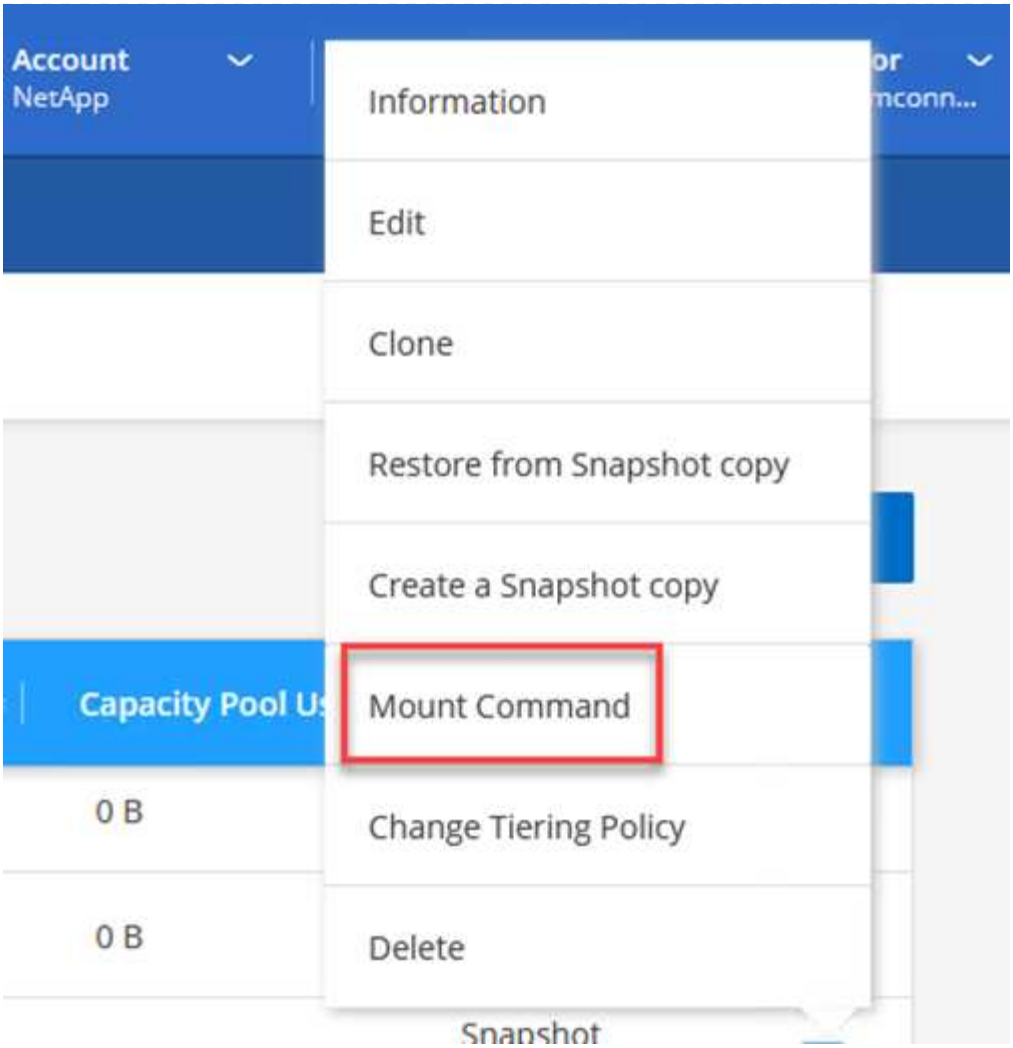
Oracle Serverに**NFS**ボリュームをマウントします

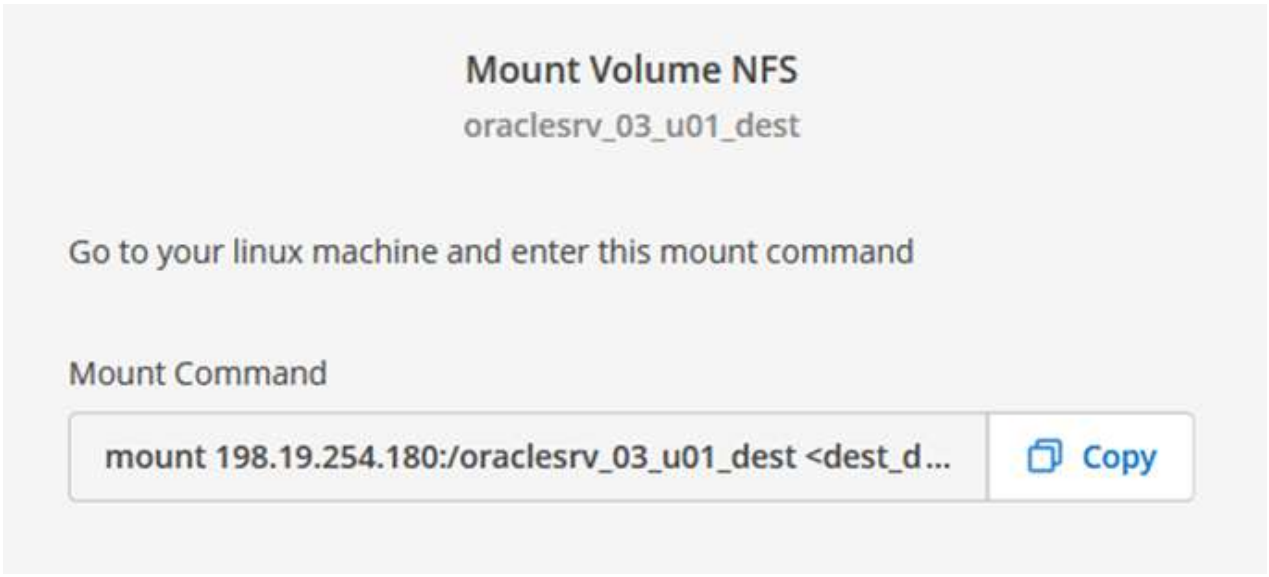
Cloud Managerでは、Oracleデータベースファイルとログを格納するNFSボリュームをマウントするための、正しいNFS LIFのIPアドレスを指定してmountコマンドを取得できます。

1. Cloud Managerで、FSXクラスタのボリュームのリストにアクセスします。



2. アクションメニューからマウントコマンドを選択し、Oracle Linuxサーバで使用するマウントコマンドを表示してコピーします。





3. NFSファイルシステムをOracle Linux Serverにマウントします。NFS共有をマウントするためのディレクトリがOracle Linuxホスト上にすでに存在している。
4. Oracle Linuxサーバから、mountコマンドを使用してNFSボリュームをマウントします。

```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

Oracleデータベースに関連付けられたボリュームごとに、この手順を繰り返します。

再起動時にNFSマウントを維持するには'/etc/fstabファイルを編集してマウント・コマンドを追加します

5. Oracleサーバをリブートします。Oracleデータベースは正常に起動し、使用できるようになっている必要があります。

フェイルバック

この解決策 で概説しているフェイルオーバープロセスが正常に完了すると、SnapCenter とVeeamがAWSで実行されるバックアップ機能を再開します。FSX for ONTAP は、元のオンプレミスデータセンターとの間にSnapMirror関係が確立されていないプライマリストレージとして指定されます。オンプレミスで通常の機能が再開されたら、本ドキュメントに記載されているプロセスと同じ方法で、オンプレミスのONTAP ストレージシステムにデータをミラーリングできます。

また、このドキュメントで説明しているように、アプリケーションデータボリュームをFSX for ONTAP からオンプレミスのONTAP ストレージシステムにミラーリングするようにSnapCenter を設定することもできます。同様に、スケールアウトバックアップリポジトリを使用してAmazon S3にバックアップコピーをレプリケートするようにVeeamを設定し、オンプレミスのデータセンターにあるVeeamバックアップサーバからこれらのバックアップにアクセスできるようにします。

フェイルバックについてはこのドキュメントでは説明していませんが、フェイルバックについてはここで説明する詳細なプロセスとはほとんど異なります。

まとめ

このドキュメントで紹介するユースケースでは、ネットアップとVMwareの統合に特化した、実績のあるディザスタリカバリテクノロジに焦点を当てています。ネットアップのONTAP ストレージシステムは、実績あるデータミラーリングテクノロジを提供します。このテクノロジを使用すると、業界をリードするクラウドプロバイダのオンプレミステクノロジとONTAP テクノロジにまたがるディザスタリカバリソリューションを設計できます。

ONTAP on AWSは、アプリケーションデータをクラウドにレプリケートするためにSnapCenter やSyncMirrorとシームレスに統合できる解決策 の1つです。Veeam Backup & Replicationも、ネットアップのONTAP ストレージシステムと緊密に統合され、vSphereネイティブストレージへのフェイルオーバーを可能にする、よく知られたテクノロジです。

この解決策 では、SQL ServerとOracleアプリケーションデータをホストしているONTAP システムから、ゲスト接続ストレージを使用してディザスタリカバリ解決策 を提供しています。SnapCenter とSnapMirrorを使用すると、ONTAP システム上のアプリケーションボリュームを保護し、それらをクラウド上のFSXまたはCVOにレプリケートするための管理しやすい解決策 が提供されます。SnapCenter は、DR対応の解決策 で、すべてのアプリケーションデータをAWS上のVMware Cloudにフェイルオーバーします。

追加情報の参照先

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

- 解決策 のドキュメントへのリンク

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

  "ネットアップのソリューション"

Veeam Backup & Restore in VMware Cloud with Amazon FSx for ONTAP

作成者：Josh Powell -ネットアップソリューションエンジニアリングチーム

概要

Veeam Backup & Replicationは、VMware Cloud内のデータを保護するための効果的で信頼性の高い解決策 です。この解決策 では、Veeam Backup and Replicationを使用して、FSx for ONTAP NFSデータストアにあるアプリケーションVMをVMware Cloudでバックアップおよびリストアするための適切なセットアップと構成について説明します。

VMware Cloud（AWS）は、補完的ストレージとしてNFSデータストアの使用をサポートしています。FSx for NetApp ONTAP は、SDDCクラスタ内のESXiホストの数に関係なく拡張できる、クラウドアプリケーション用の大量のデータを保存する必要があるお客様向けのセキュアな解決策 です。このAWS統合ストレージサービスは、従来のNetApp ONTAP の機能をすべて備えた、効率性に優れたストレージを提供します。

ユースケース

この解決策 は、次のユースケースに対応します。

- バックアップリポジトリとしてFSx for NetApp ONTAP を使用して、VMCでホストされているWindowsおよびLinux仮想マシンのバックアップとリストアを実行できます。
- FSx for NetApp ONTAP をバックアップリポジトリとして使用して、Microsoft SQL Serverアプリケーションデータをバックアップおよびリストアします。
- バックアップリポジトリとしてFSx for NetApp ONTAP を使用した、Oracleアプリケーションデータのバックアップとリストア

Amazon FSx for ONTAP を使用したNFSデータストア

この解決策 内のすべての仮想マシンは、FSx for ONTAP の補完的NFSデータストア上に配置されます。FSx for ONTAP を補完的NFSデータストアとして使用することには、いくつかのメリットがあります。たとえば、次のことが可能です。

- 複雑なセットアップと管理を必要とせずに、拡張性と可用性に優れたクラウドファイルシステムを構築できます。
- 既存のVMware環境との統合により、使い慣れたツールやプロセスを使用してクラウドリソースを管理できます。
- Snapshotやレプリケーションなど、ONTAP が提供する高度なデータ管理機能を活用して、データを保護し、データの可用性を確保できます。

解決策 の導入の概要

以下のリストには、Veeam Backup & Replicationの設定、バックアップリポジトリとしてFSx for ONTAPを使用したバックアップジョブとリストアジョブの実行、SQL ServerとOracleのVMとデータベースのリストアに必要な手順の概要が記載されています。

1. Veeam Backup & ReplicationのiSCSIバックアップリポジトリとして使用するFSx for ONTAP ファイルシステムを作成します。
2. Veeamプロキシを導入して、バックアップワークロードを分散し、FSx for ONTAP でホストされたiSCSIバックアップリポジトリをマウントします。
3. SQL Server、Oracle、Linux、Windowsの仮想マシンをバックアップするようにVeeam Backup Jobsを設定します。
4. SQL Server仮想マシンおよび個 々 のデータベースをリストアします。
5. Oracle仮想マシンおよび個 々 のデータベースをリストアします。

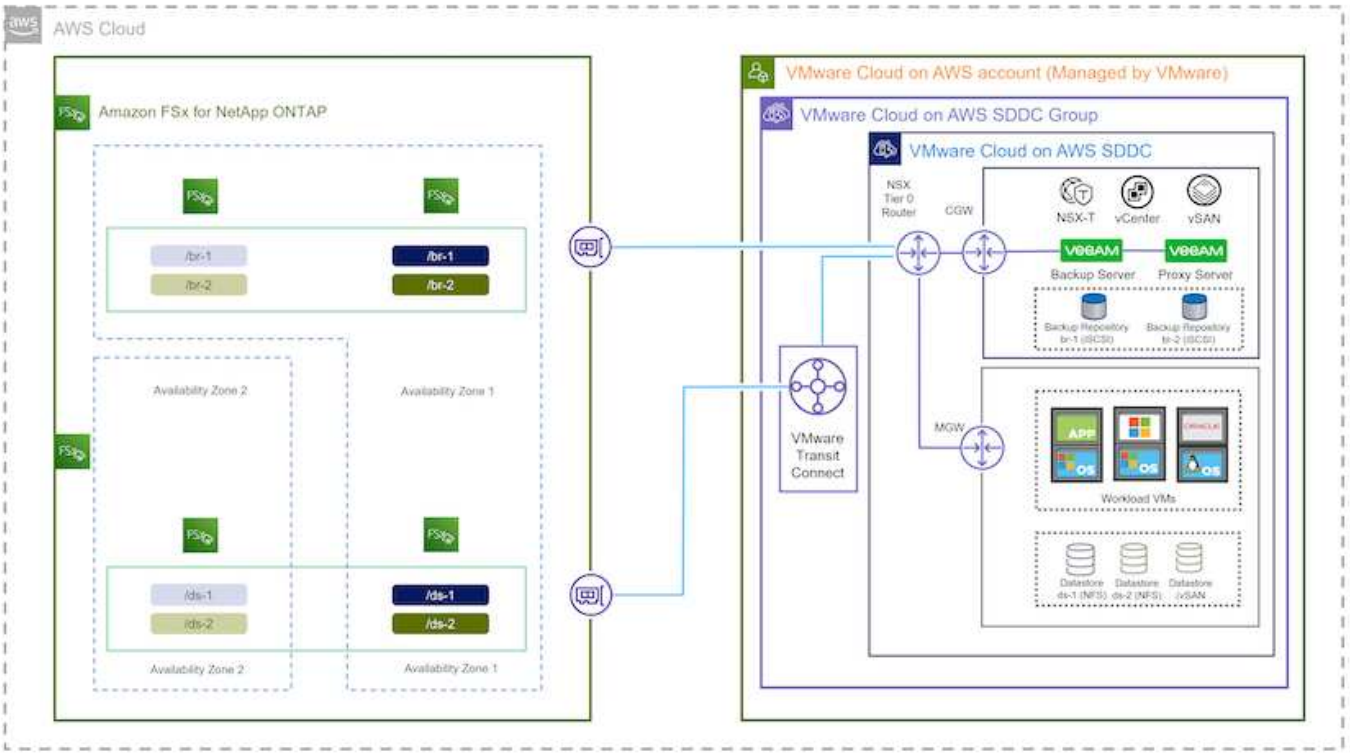
前提条件

この解決策 の目的は、VMware Cloudで実行され、FSx for NetApp ONTAP でホストされるNFSデータストア上に配置された仮想マシンのデータ保護について説明することです。この解決策 は、次のコンポーネントが構成され、使用可能な状態にあることを前提としています。

1. FSx for ONTAP ファイルシステムで、VMware Cloudに接続された1つ以上のNFSデータストアを使用します。
2. Veeam Backup & Replicationソフトウェアがインストールされ
Microsoft Windows Server VM。
    - vCenter Serverが、IPアドレスまたは完全修飾ドメイン名を使用してVeeam Backup & Replicationサーバによって検出されている。
3. 解決策 の導入時にVeeamバックアッププロキシコンポーネントとともにインストールするMicrosoft Windows Server VM。
4. Microsoft SQL Server VMとVMDKおよびアプリケーションデータがFSx for ONTAP NFSデータストアに格納されている。この解決策 では、2つのSQLデータベースを2つの独立したVMDKに格納しました。
    - 注：ベストプラクティスとして、データベースとトランザクションログファイルは別 々 のドライブに配置します。これにより、パフォーマンスと信頼性が向上します。これは、トランザクションログがシーケンシャルに書き込まれるのに対し、データベースファイルはランダムに書き込まれるためです。
5. OracleデータベースVMとVMDKおよびアプリケーションデータがFSx for ONTAP NFSデータストアに格納されている。
6. FSx for ONTAP NFSデータストア上に配置されたVMDKを使用したLinuxおよびWindowsのファイルサーバVM。
7. Veeamには、バックアップ環境のサーバとコンポーネント間の通信に特定のTCPポートが必要です。Veeamバックアップインフラコンポーネントでは、必要なファイアウォールルールが自動的に作成されます。ネットワークポート要件の詳細なリストについては、の「ポート」のセクションを参照してください "Veeam Backup and Replication User Guide for VMware vSphereを参照してください"。

アーキテクチャの概要

この解決策 のテストと検証は、最終的な導入環境と異なる場合があるラボで実施しました。詳細については、次のセクションを参照してください。



ハードウェア/ソフトウェアコンポーネント

この解決策 の目的は、VMware Cloudで実行され、FSx for NetApp ONTAP でホストされるNFSデータストア上に配置された仮想マシンのデータ保護について説明することです。この解決策 では、次のコンポーネントが設定済みで、使用可能な状態であることを前提としています。

- Microsoft Windows VMはFSx for ONTAP NFSデータストアに配置されます
- FSx for ONTAP NFSデータストアにあるLinux（CentOS）VM
- FSx for ONTAP NFSデータストアに配置されたMicrosoft SQL Server VM
  - 2つのデータベースが別 々 のVMDKにホストされている
- Oracle VMはFSx for ONTAP NFSデータストアに配置されます

解決策 の導入

この解決策 では、Veeam Backup & Replicationソフトウェアを使用して、AWS上のVMwareクラウドSDDC内のSQL Server、Oracle、WindowsおよびLinuxファイルサーバ仮想マシンのバックアップとリカバリを実行する解決策 の導入と検証の詳細な手順を説明します。この解決策 の仮想マシンは、FSx for ONTAP でホストされる補完的なNFSデータストアに配置されます。また、Veeamバックアップリポジトリに使用するiSCSIボリュームのホストには、独立したFSx for ONTAP ファイルシステムが使用されます。

FSx for ONTAP ファイルシステムの作成、バックアップリポジトリとして使用するiSCSIボリュームのマウント、バックアップジョブの作成と実行、VMとデータベースのリストアについて説明します。

FSx for NetApp ONTAP の詳細については、を参照してください "FSx for ONTAP ユーザガイド"。

Veeam Backup and Replicationの詳細については、を参照してください "Veeam Help Centerテクニカルドキュメント" サイト

Veeam Backup and ReplicationをVMware Cloud on AWSで使用する場合の考慮事項と制限事項については、を参照してください "VMware Cloud on AWSおよびVMware Cloud on Dell EMCサポート考慮事項および制限事項"。

Veeam Proxyサーバを導入します

VeeamプロキシサーバはVeeam Backup & Replicationソフトウェアのコンポーネントで、ソースとバックアップまたはレプリケーションのターゲットを仲介します。プロキシサーバは、データをローカルで処理することで、バックアップジョブ中のデータ転送の最適化と高速化に役立ちます。また、さまざまな転送モードを使用して、VMware vStorage APIs for Data Protectionまたはダイレクトストレージアクセスを使用してデータにアクセスできます。

Veeamプロキシサーバの設計を選択する際には、同時に実行するタスクの数、転送モード、または必要なストレージアクセスの種類を考慮することが重要です。

プロキシサーバの数およびシステム要件については、を参照してください "Veeam VMware vSphere Best Practice Guideを参照してください"。

Veeam Data MoverはVeeam Proxy Serverのコンポーネントであり、ソースからVMデータを取得してターゲットに転送する方法としてトランスポートモードを使用します。転送モードは、バックアップジョブの設定時に指定します。ストレージへの直接アクセスを使用することで、NFSデータストアからのバックアップ効率を高めることができます。

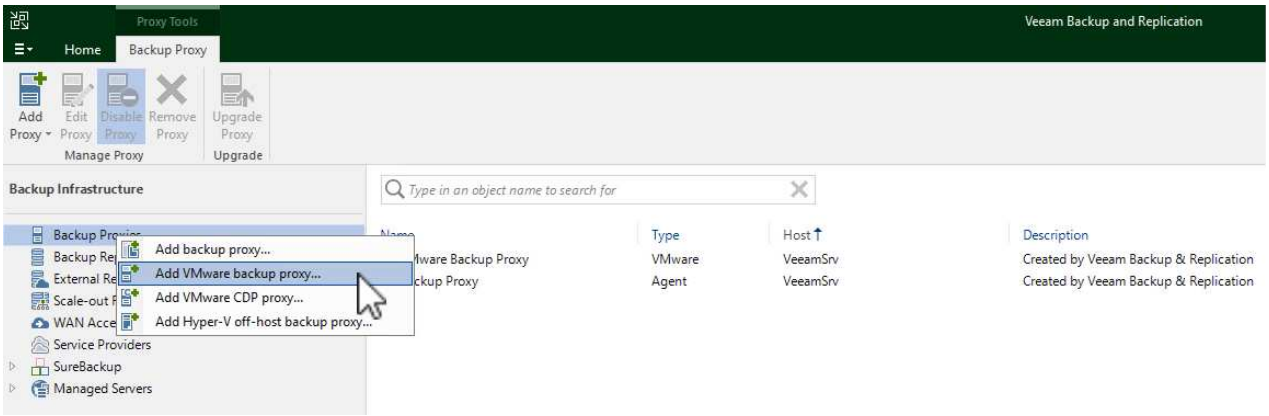
トランスポートモードの詳細については、を参照してください "Veeam Backup and Replication User Guide for VMware vSphereを参照してください"。

次の手順では、VMware Cloud SDDC内のWindows VMにVeeam Proxy Serverを導入します。

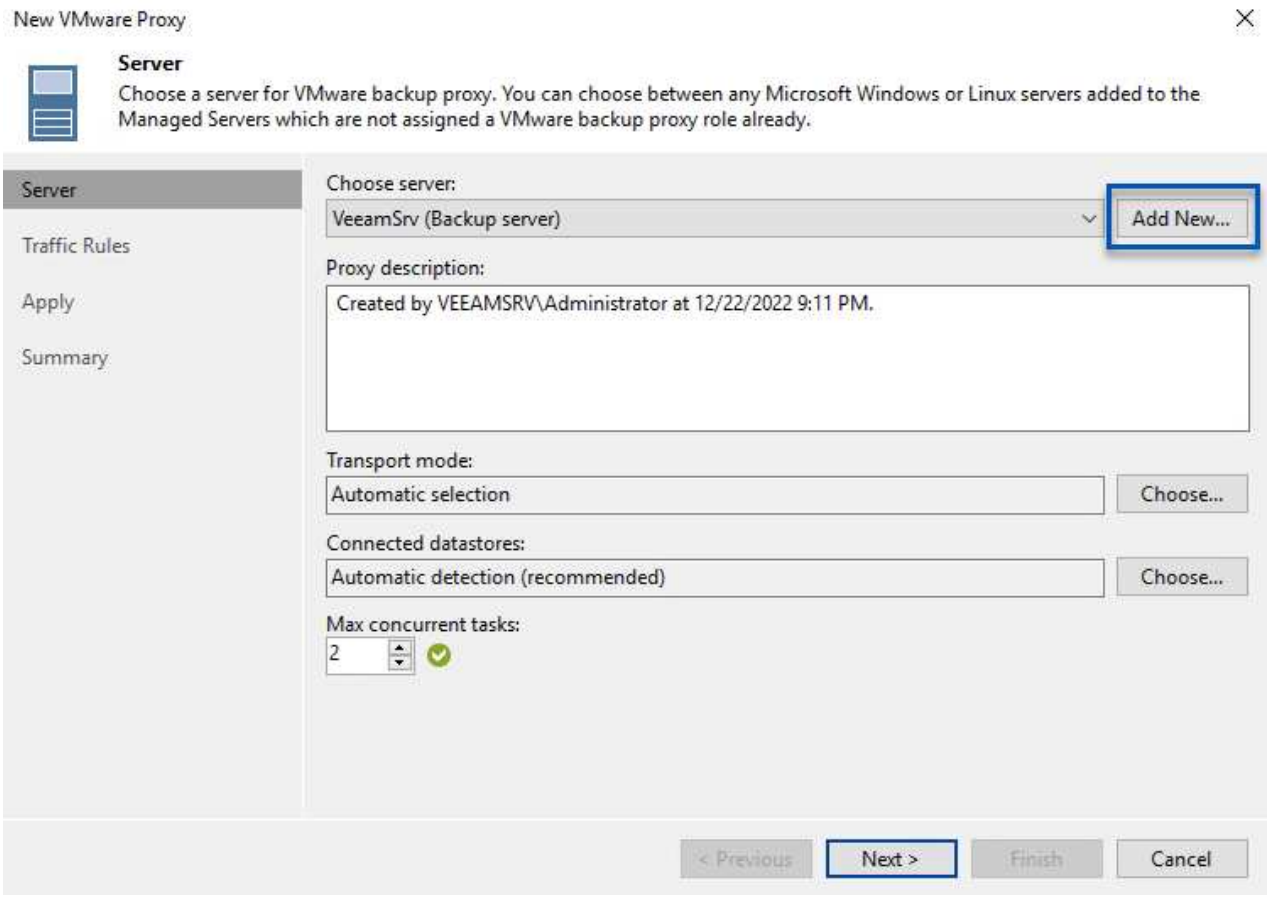
Veeam Proxyを導入してバックアップワークロードを分散

この手順では、Veeamプロキシを既存のWindows VMに導入します。これにより、プライマリVeeam Backup ServerとVeeam Proxyの間でバックアップジョブを分散させることができます。

1. Veeam Backup and Replicationサーバで、管理コンソールを開き、左下のメニューから*[バックアップインフラストラクチャ]*を選択します。
2. を右クリックし、[VMwareバックアッププロキシの追加…]*をクリックしてウィザードを開きます。

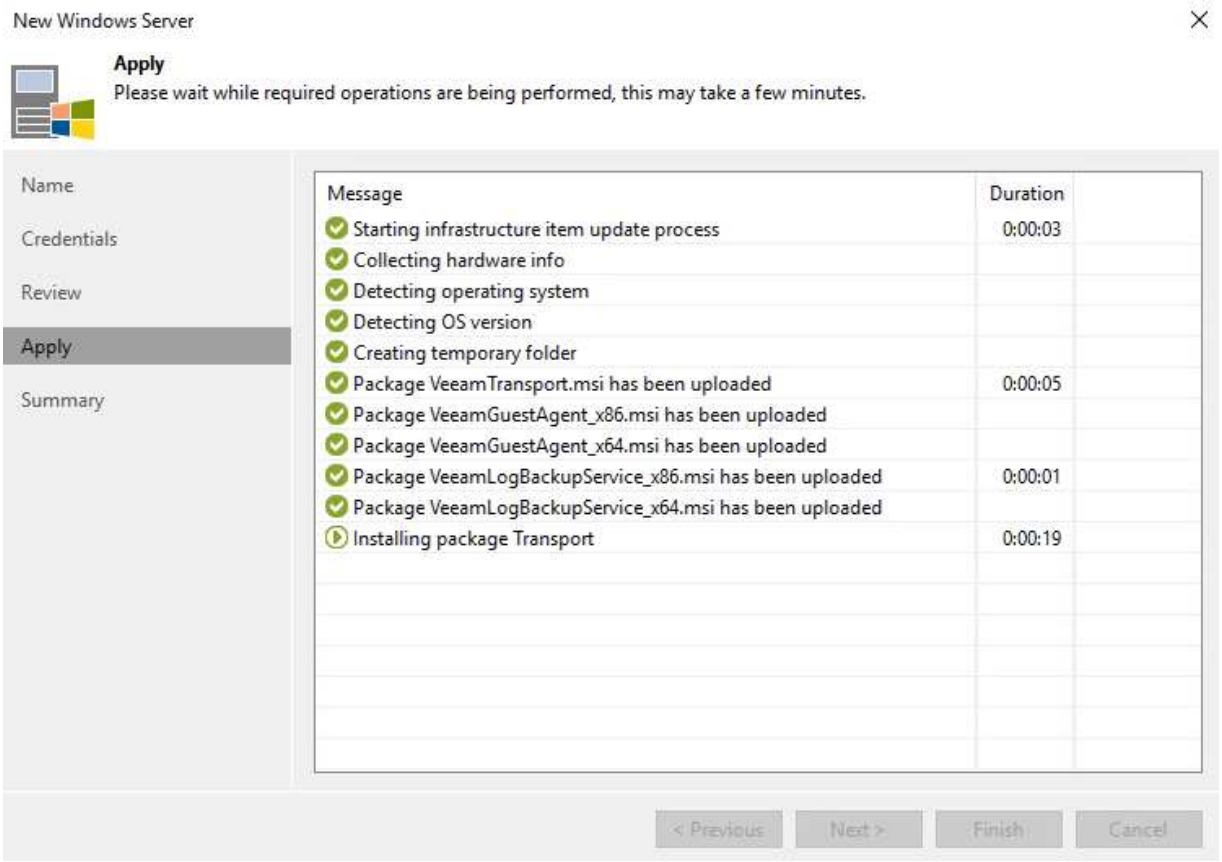


3. VMware Proxyの追加*ウィザードで*新規追加…*ボタンをクリックして、新しいプロキシサーバーを追加します。

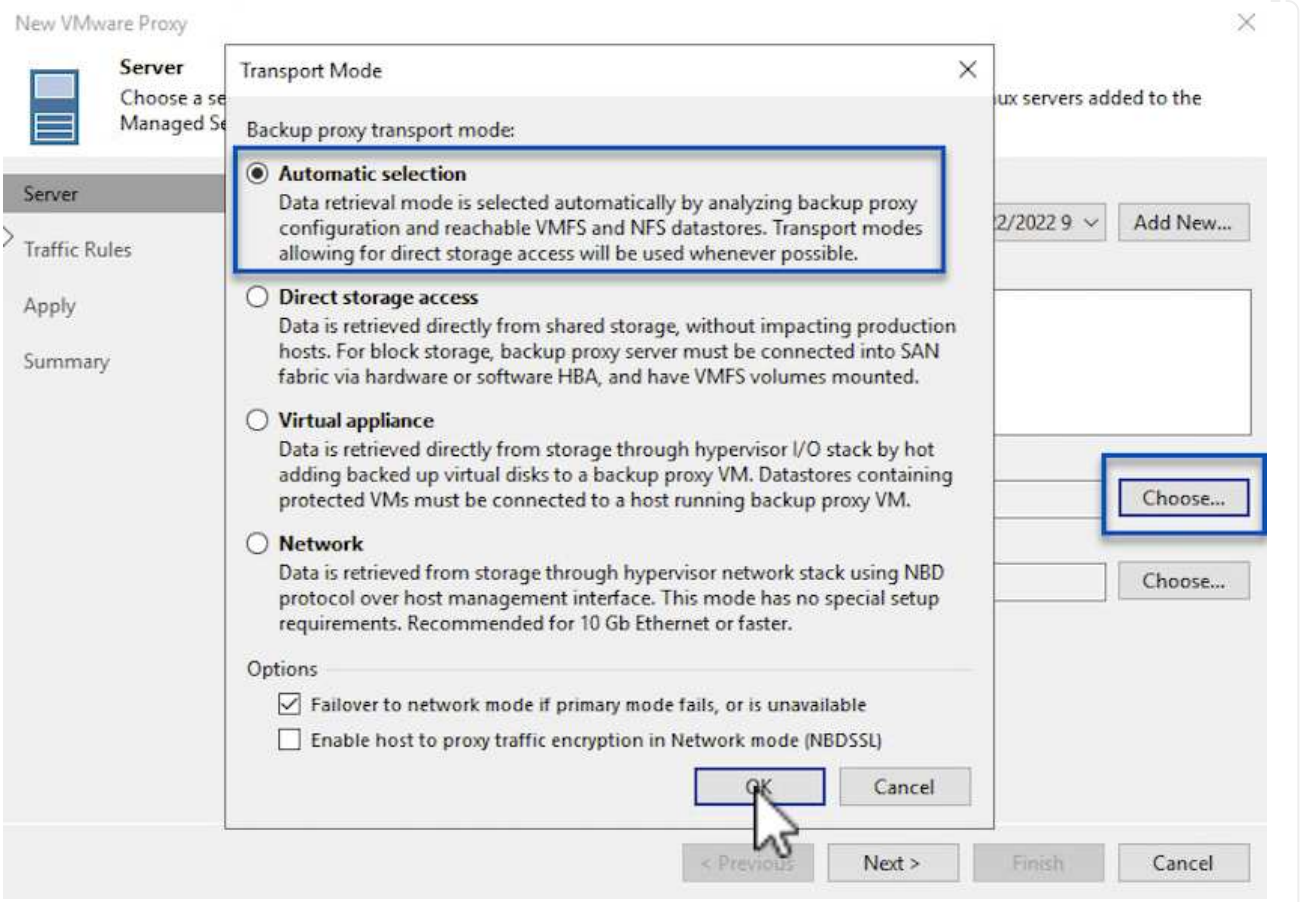


4. Microsoft Windowsを追加する場合に選択し、プロンプトに従ってサーバを追加します。

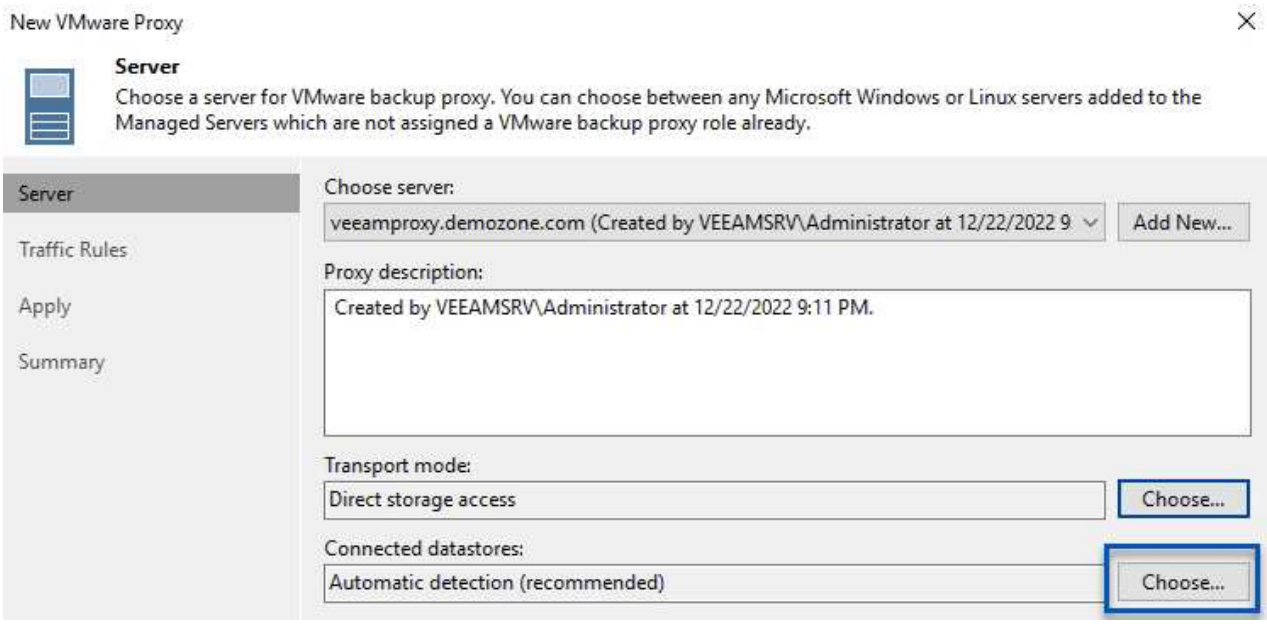
- DNS名またはIPアドレスを入力します
- 新しいシステムのクレデンシャルに使用するアカウントを選択するか、新しいクレデンシャルを追加します
- インストールするコンポーネントを確認し、*適用*をクリックして導入を開始します

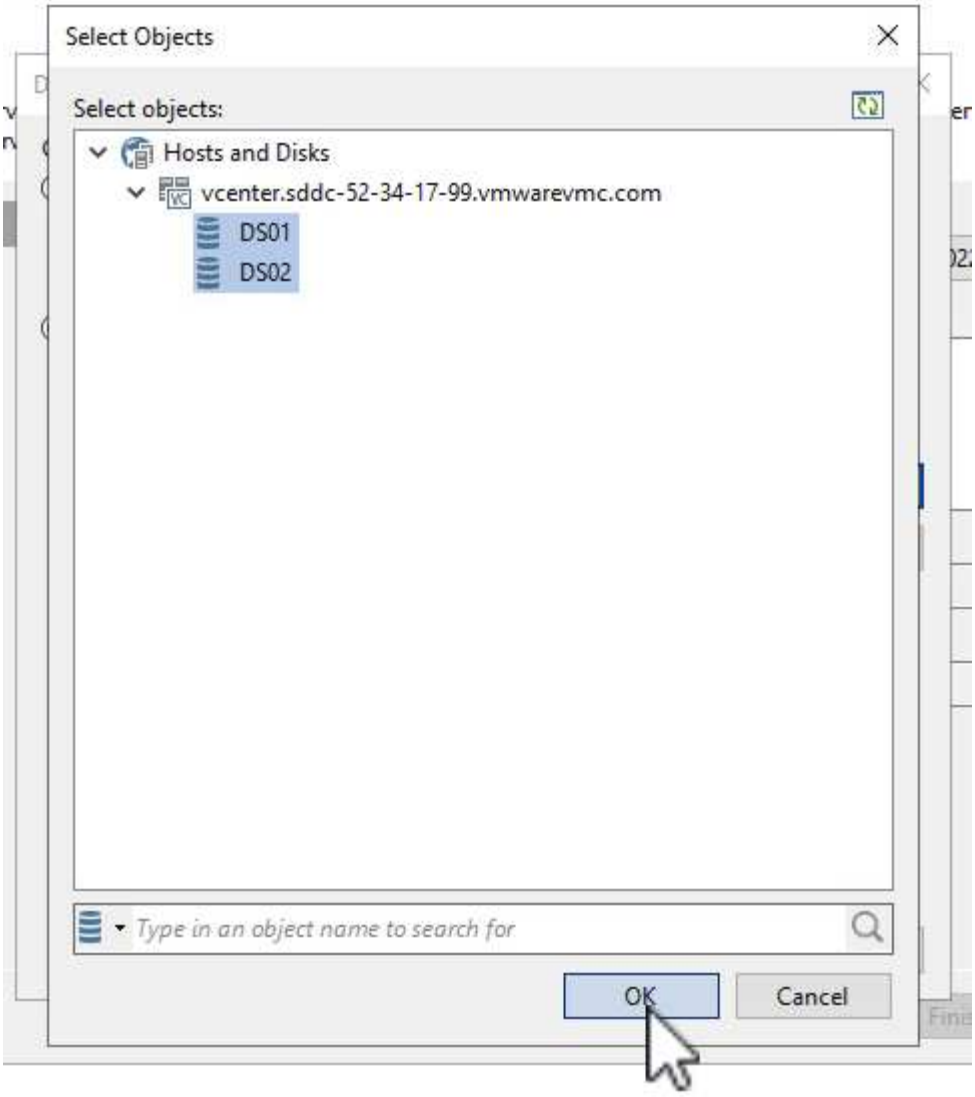


5. [New VMware Proxy]ウィザードに戻り、[Transport Mode]を選択します。ここでは、*自動選択*を選択しました。

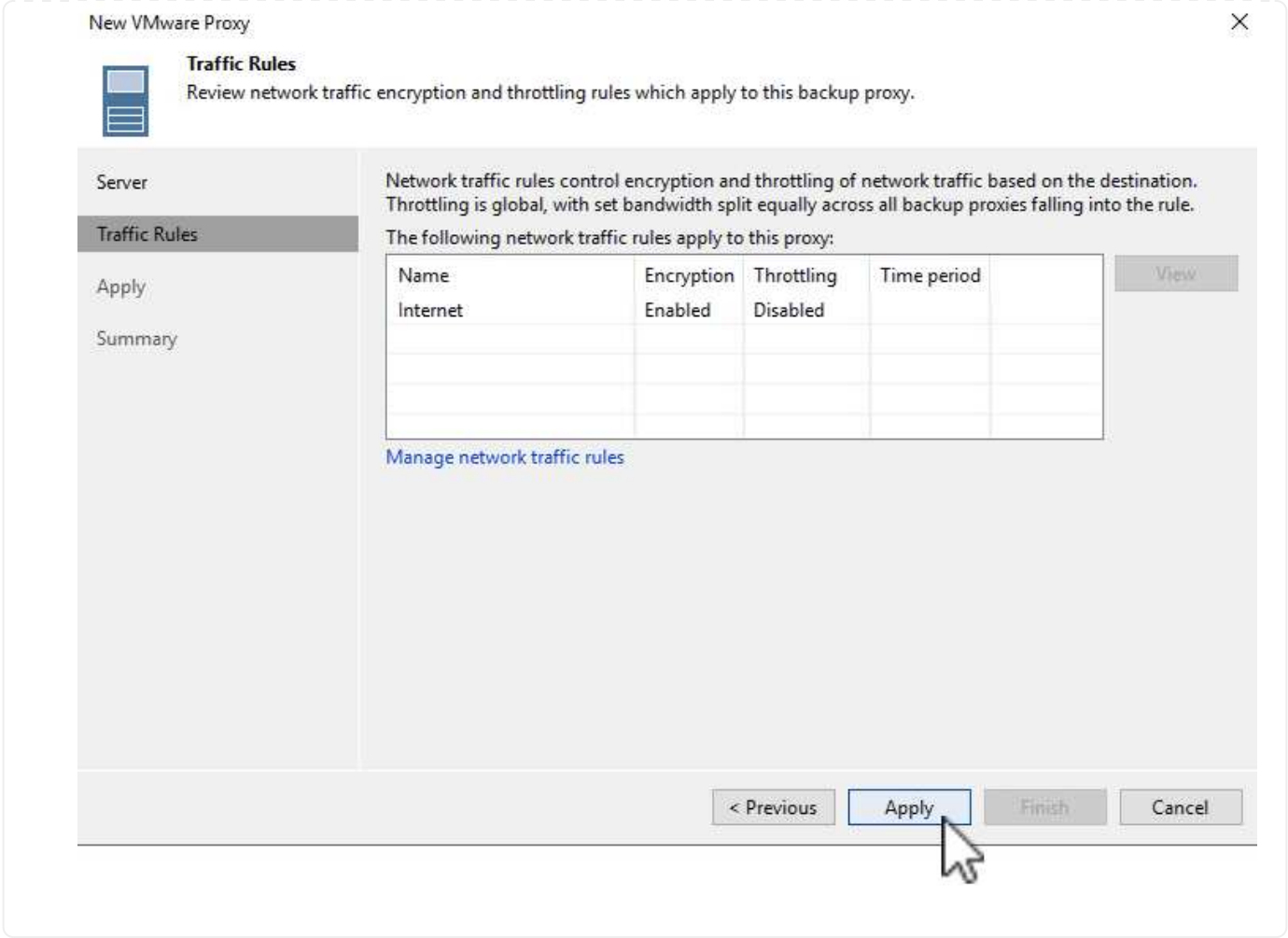


6. VMware Proxyから直接アクセスできるようにする、接続されているデータストアを選択します。





7. 暗号化やスロットリングなど、必要な特定のネットワークトラフィックルールを設定して適用します。完了したら、*[適用]*ボタンをクリックして導入を完了します。



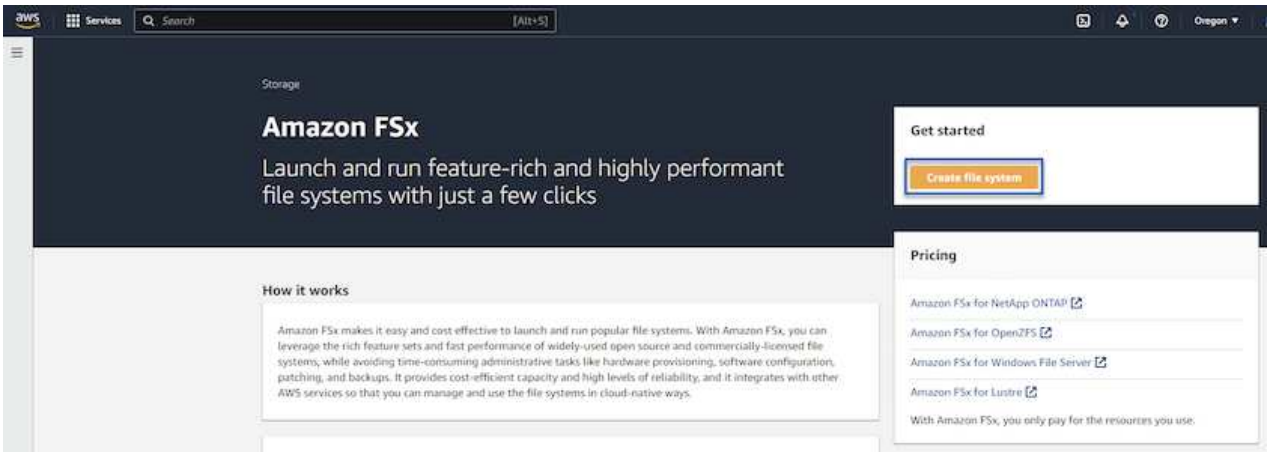
ストレージとバックアップリポジトリを設定します

プライマリVeeam BackupサーバとVeeam Proxyサーバは、直接接続されたストレージ形式のバックアップリポジトリにアクセスできます。このセクションでは、FSx for ONTAP ファイルシステムの作成、VeeamサーバへのiSCSI LUNのマウント、バックアップリポジトリの作成について説明します。

FSx for ONTAP ファイルシステムを作成

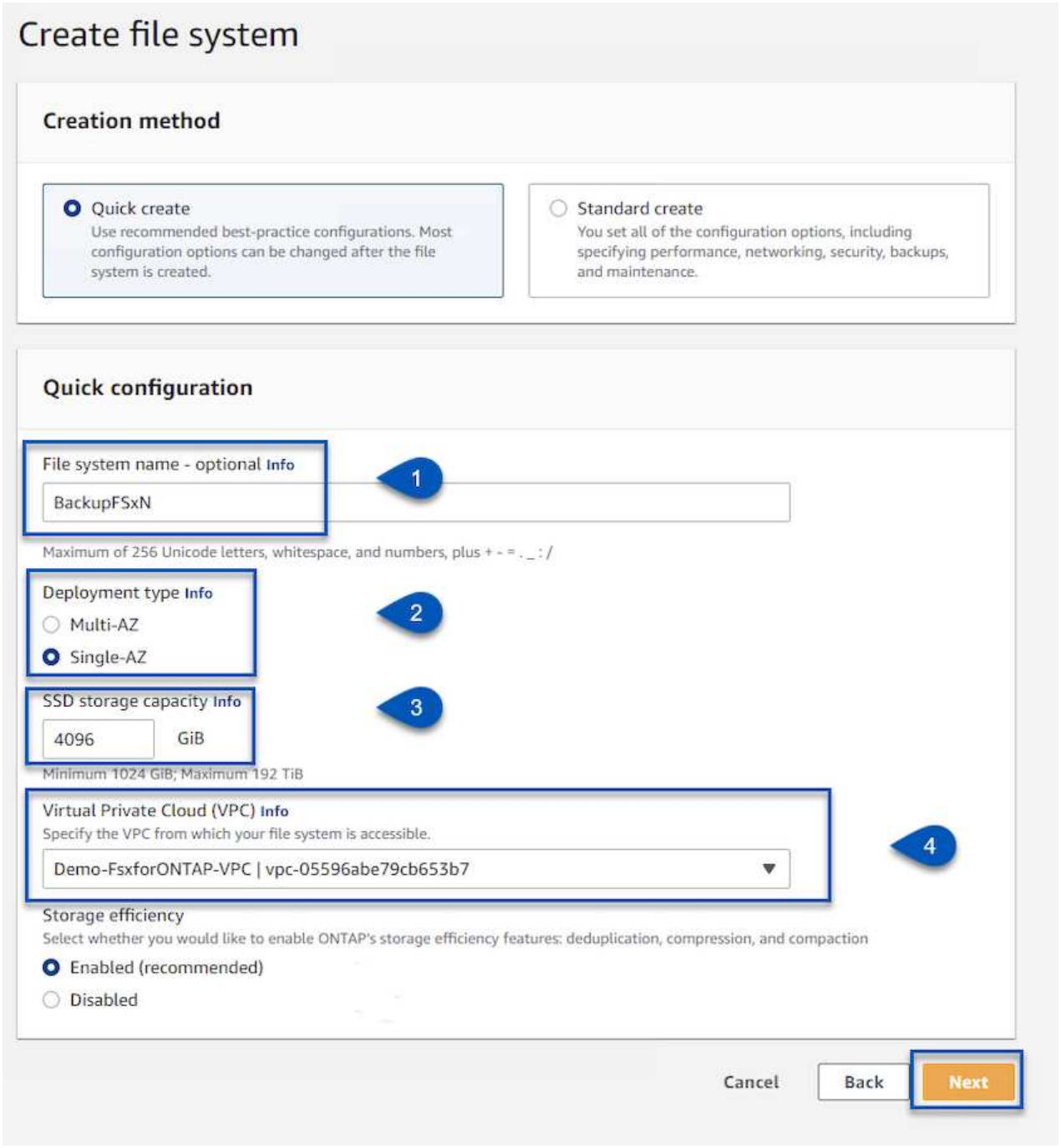
Veeamバックアップリポジトリ用のiSCSIボリュームのホストに使用するFSx for ONTAP ファイルシステムを作成します。

1. AWSコンソールで、FSxに移動し、*ファイルシステムの作成*をクリックします



2. Amazon FSx for NetApp ONTAP を選択し、 Next *を選択して続行します。

3. ファイルシステム名、導入タイプ、SSDストレージ容量、FSx for ONTAP クラスタを配置するVPCを入力します。これは、VMware Cloud内の仮想マシンネットワークと通信するように設定されたVPCである必要があります。[次へ]*をクリックします。



4. 導入手順を確認し、* Create File System *をクリックしてファイルシステムの作成プロセスを開始します。

iSCSI LUNを設定してマウントします

FSx for ONTAP でiSCSI LUNを作成して設定し、Veeamバックアップサーバとプロキシサーバにマウントします。これらのLUNは、あとでVeeamバックアップリポジトリの作成に使用されます。

FSx for ONTAP でiSCSI LUNを作成するプロセスは複数の手順で構成されます。ボリューム作成の最初のステップは、Amazon FSxコンソールまたはNetApp ONTAP CLIで実行できます。

FSx for ONTAP の使用方法の詳細については、を参照してください "FSx for ONTAP ユーザガイド"。

1. NetApp ONTAP CLIから次のコマンドを使用して初期ボリュームを作成します。

```
FSx-Backup::> volume create -vserver svm_name -volume vol_name
-aggregate aggregate_name -size vol_size -type RW
```

2. 前の手順で作成したボリュームを使用してLUNを作成します。

```
FSx-Backup::> lun create -vserver svm_name -path
/vol/vol_name/lun_name -size size -ostype windows -space-allocation
enabled
```

3. VeeamバックアップサーバとプロキシサーバのiSCSI IQNを含むイニシエータグループを作成して、LUNへのアクセスを許可します。

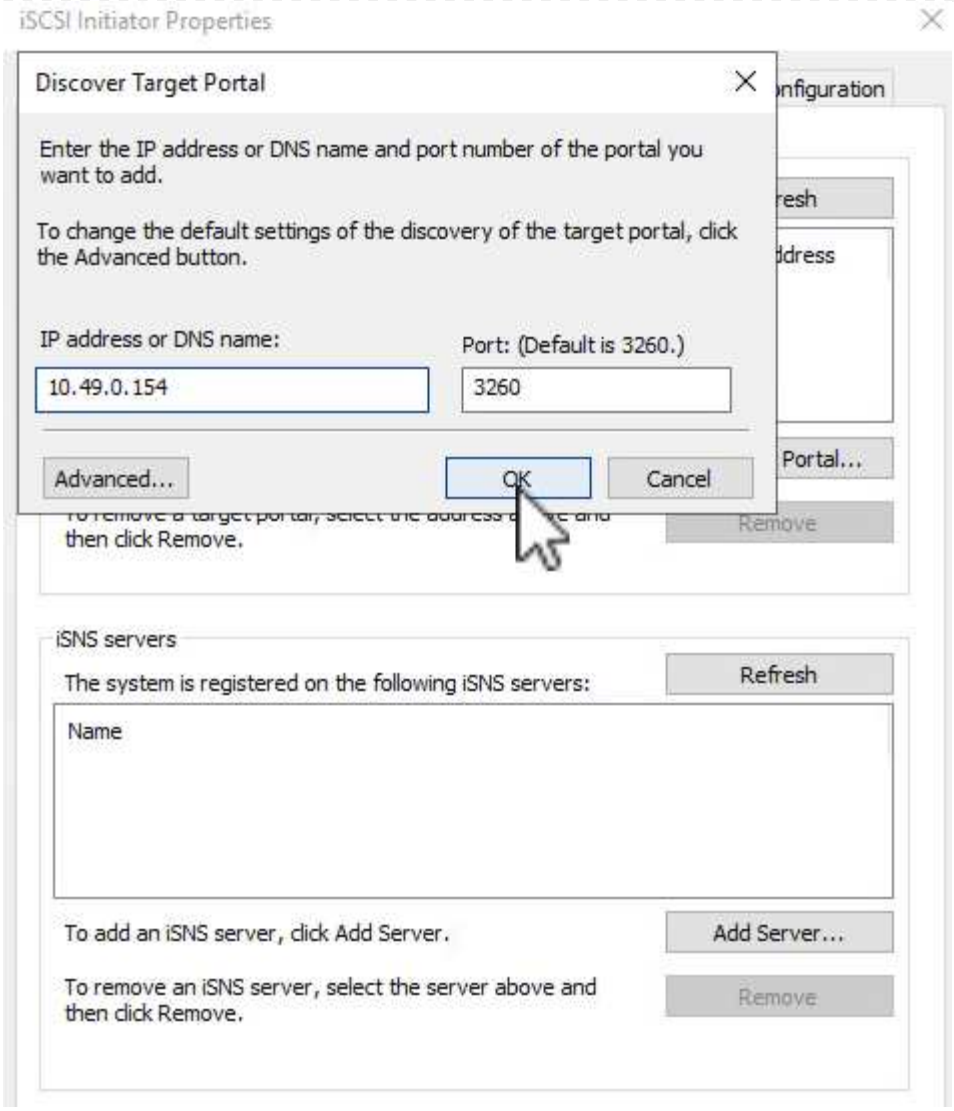
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

前の手順を完了するには、まずWindowsサーバのiSCSIイニシエータプロパティからIQNを取得する必要があります。

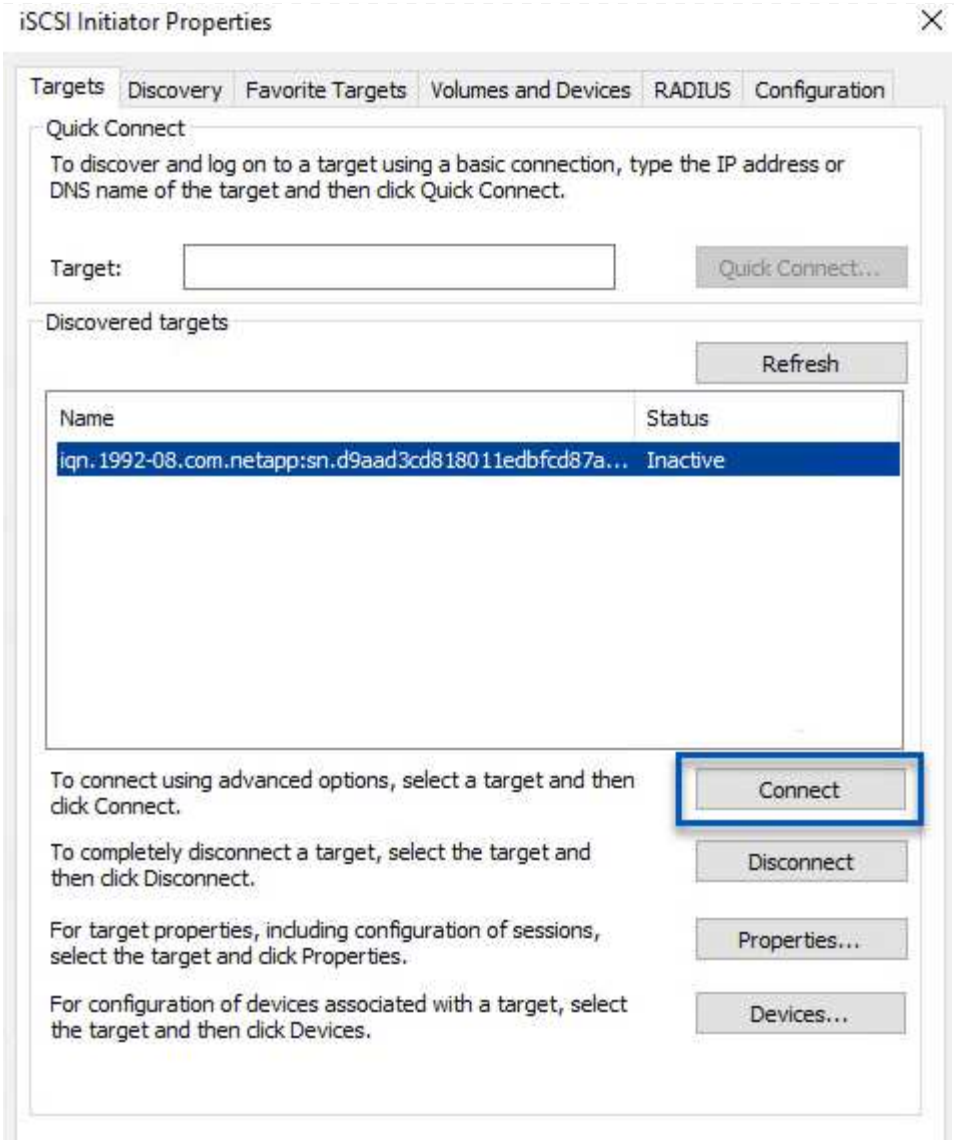
4. 最後に、作成したigroupにLUNをマッピングします。

```
FSx-Backup::> lun mapping create -vserver svm_name -path
/vol/vol_name/lun_name igroup igroup_name
```

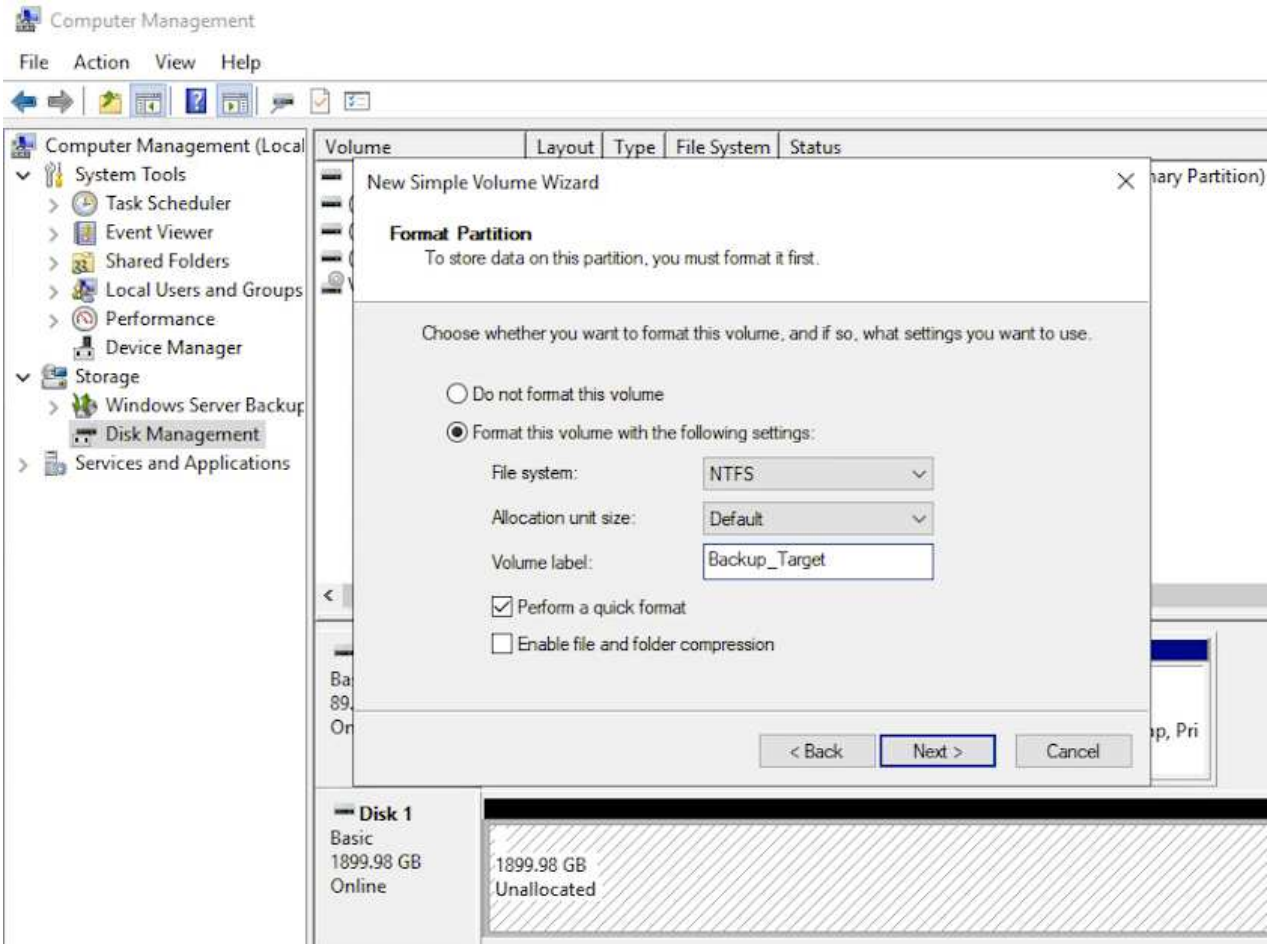
5. iSCSI LUNをマウントするには、Veeam Backup & Replication Serverにログインし、[iSCSI Initiator Properties]を開きます。[検出]タブに移動し、iSCSIターゲットのIPアドレスを入力します。



6. [ターゲット]タブで、非アクティブなLUNをハイライト表示し、**[接続]***をクリックします。**[Enable multi-path]***ボックスをオンにし、[OK]*をクリックしてLUNに接続します。



7. ディスクの管理ユーティリティで、新しいLUNを初期化し、必要な名前とドライブレターでボリュームを作成します。ボックスをオンにし、[OK]*をクリックしてLUNに接続します。

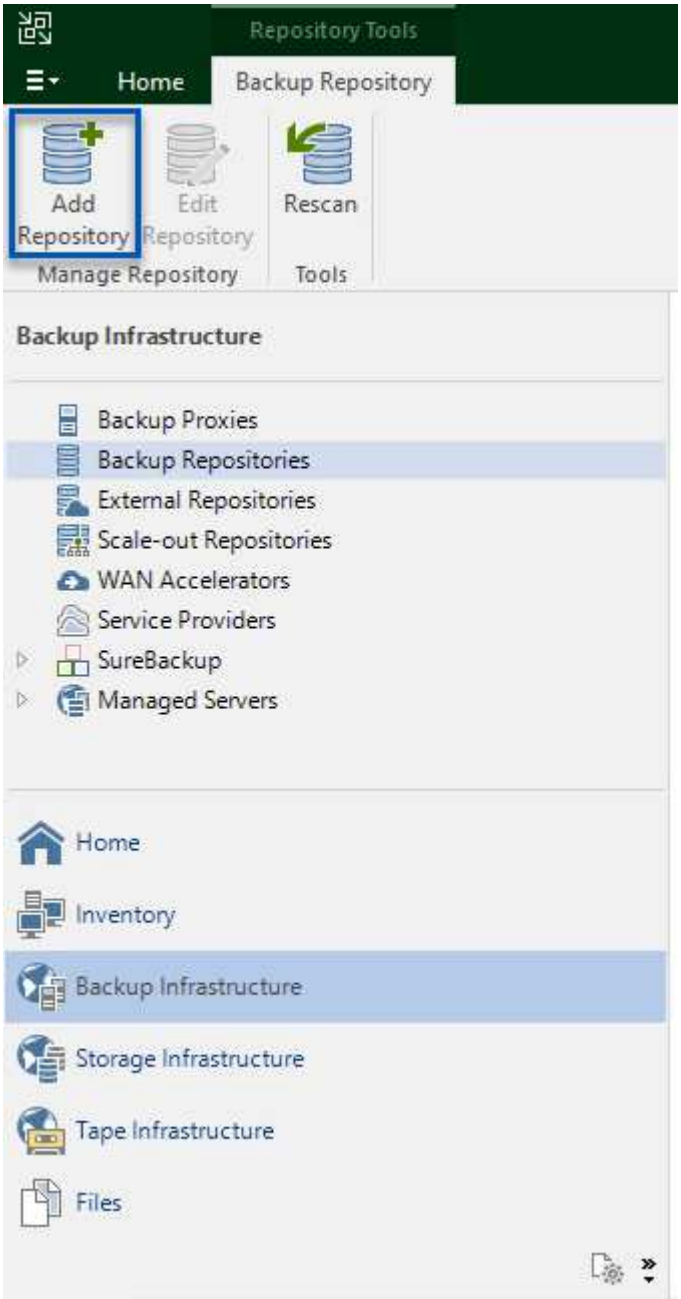


8. 同じ手順を繰り返して、iSCSIボリュームをVeeam Proxyサーバにマウントします。

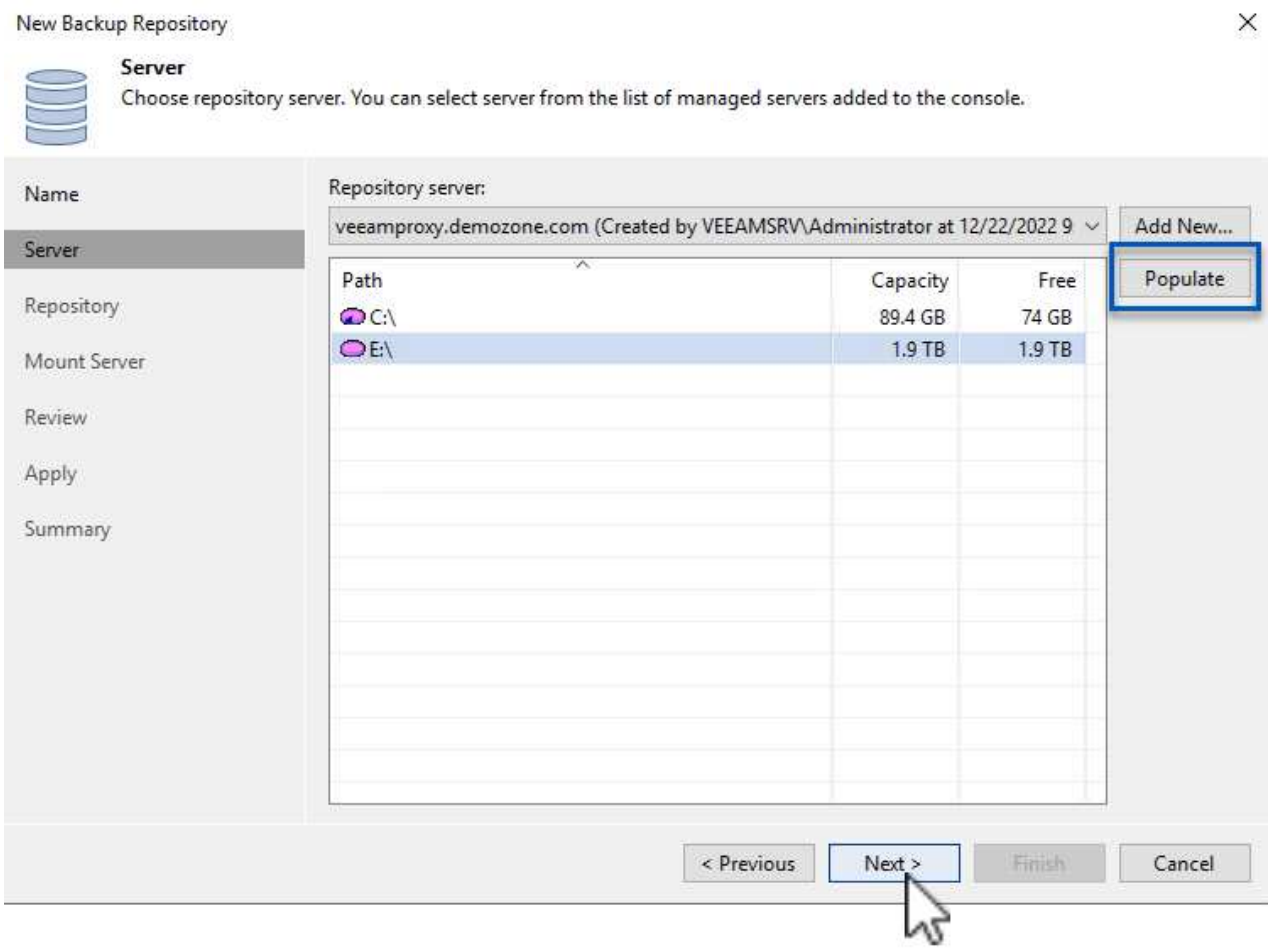
Veeamバックアップリポジトリを作成します

Veeam Backup and Replicationコンソールで、Veeam BackupサーバとVeeam Proxyサーバのバックアップリポジトリを作成します。これらのリポジトリは、仮想マシンのバックアップのバックアップターゲットとして使用されます。

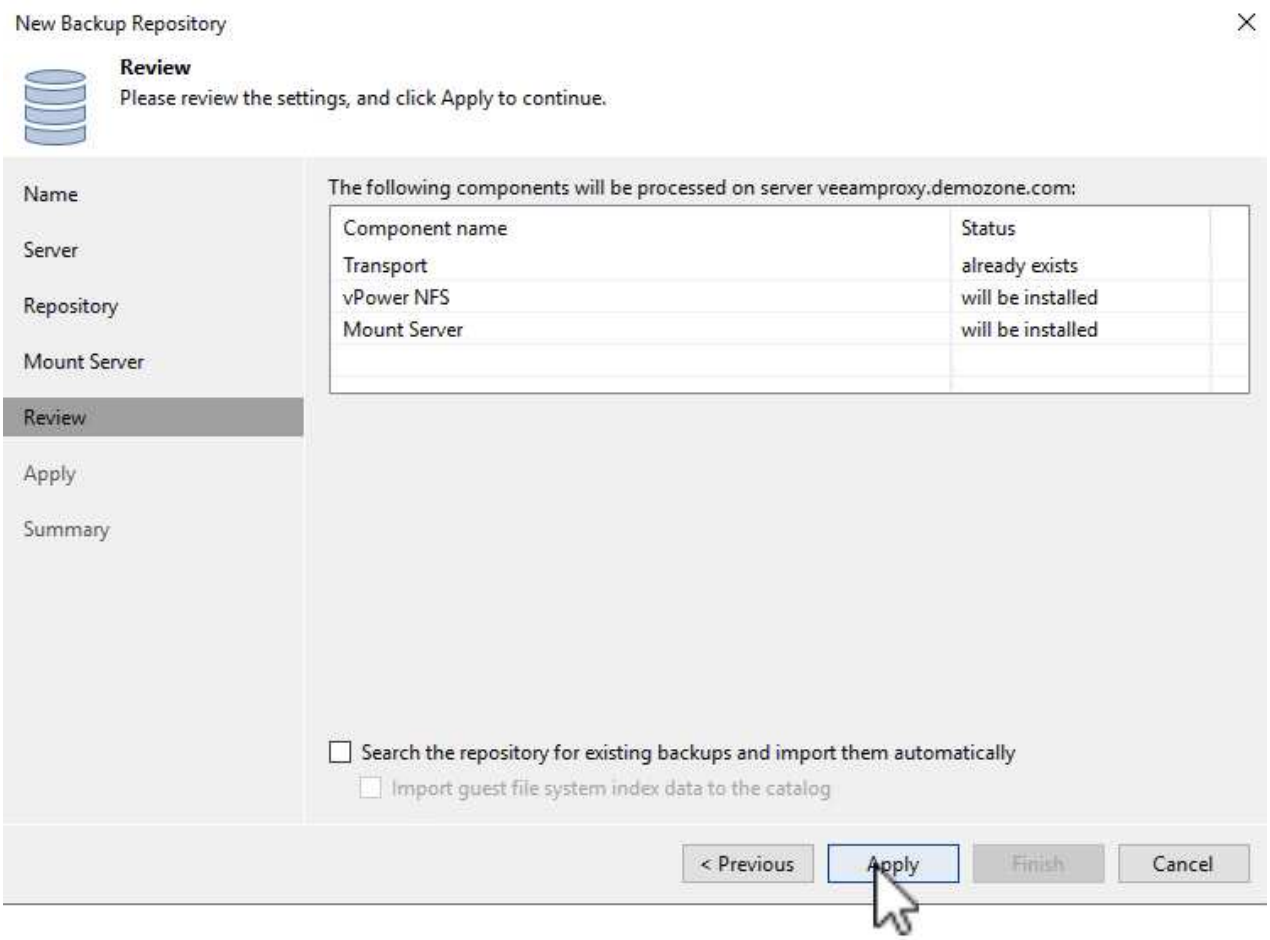
1. Veeam Backup and Replicationコンソールで、左下の*をクリックし、[リポジトリの追加]*を選択します



2. [New Backup Repository]ウィザードで、リポジトリの名前を入力し、ドロップダウンリストからサーバを選択して*[Populate]*ボタンをクリックし、使用するNTFSボリュームを選択します。



3. 次のページで'高度なリストアを実行するときにバックアップのマウント先となるマウント・サーバを選択しますデフォルトでは、リポジトリストレージが接続されているサーバと同じです。
4. 選択内容を確認し、*[適用]*をクリックしてバックアップリポジトリの作成を開始します。



5. 追加のプロキシサーバについて、上記の手順を繰り返します。

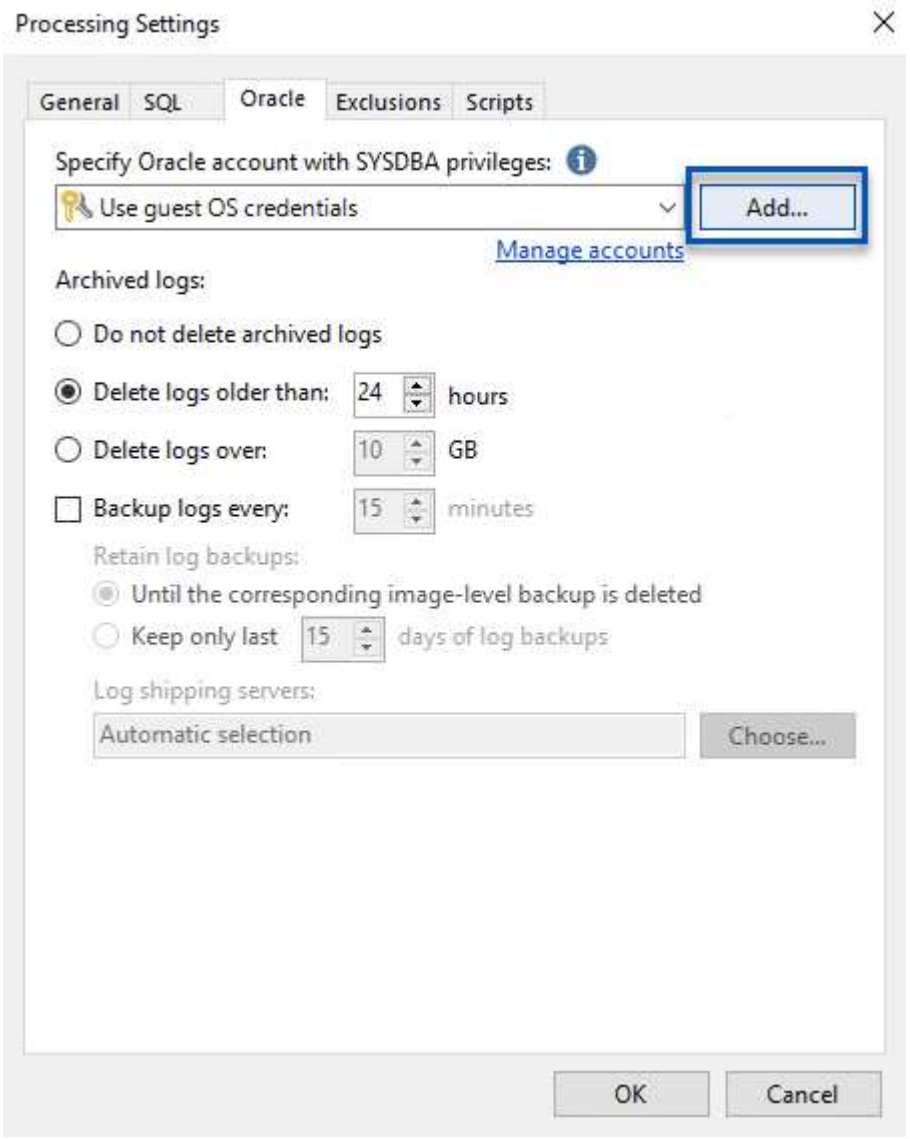
Veeamバックアップジョブを設定します

バックアップジョブは、前のセクションのバックアップリポジトリを使用して作成します。バックアップジョブの作成は、ストレージ管理者の業務の通常の一部であり、ここで紹介するすべての手順を網羅しているわけではありません。Veeamでのバックアップジョブの作成の詳細については、を参照してください "Veeam Help Centerテクニカルドキュメント"。

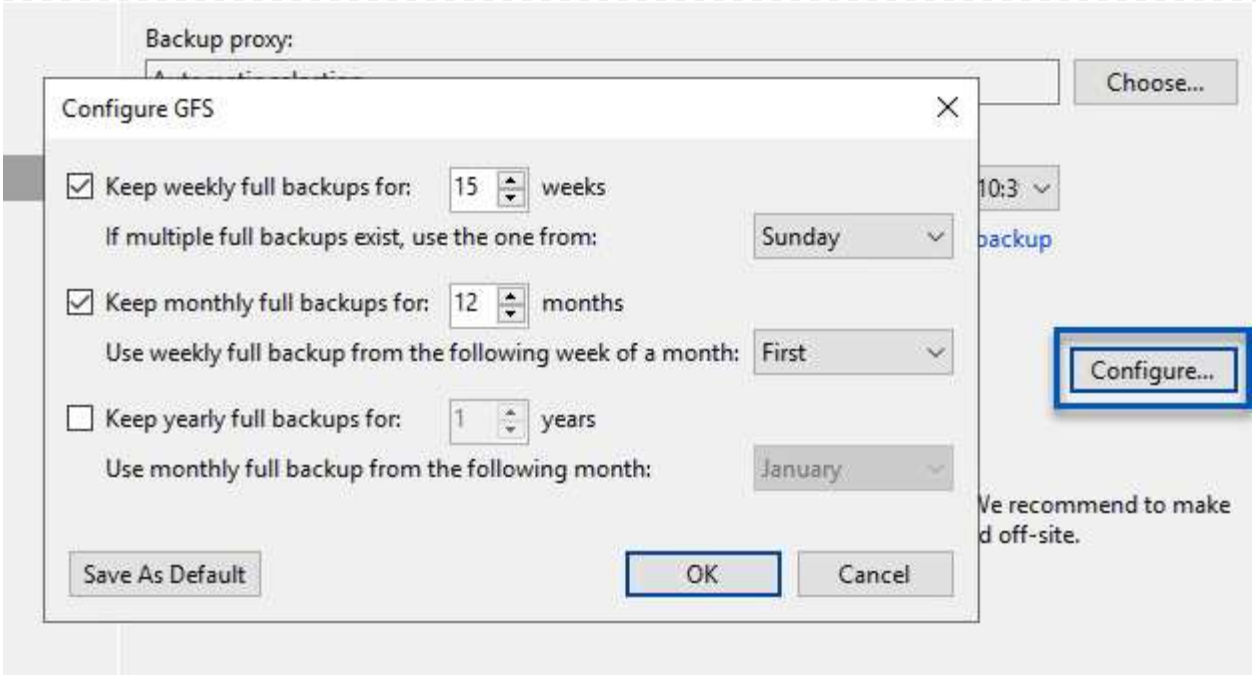
この解決策 では、次の項目に対して個別のバックアップジョブが作成されました。

- Microsoft Windows SQL Serverの略
- Oracleデータベースサーバ
- Windowsファイルサーバ
- Linuxファイルサーバ

1. アプリケーション対応の処理で整合性のあるバックアップを作成し、トランザクションログ処理を実行できます。
2. アプリケーション対応の処理を有効にした後、ゲストOSのクレデンシャルとは異なる可能性があるため、管理者権限を持つ正しいクレデンシャルをアプリケーションに追加します。



3. バックアップの保持ポリシーを管理するには、**[**アーカイブ用に特定のフルバックアップを長く保持する**]***をオンにし、[設定…]*ボタンをクリックしてポリシーを設定します。



Veeamのフルリストアによるアプリケーション**VM**のリストア

アプリケーションのリストアを実行する最初のステップは、Veeamを使用したフルリストアの実行です。VMのフルリストアの電源がオンになっており、すべてのサービスが正常に実行されていることを確認しました。

サーバのリストアは、ストレージ管理者の業務の通常の一部であり、ここで説明するすべての手順を説明するわけではありません。Veeamでのフルリストアの実行の詳細については、を参照してください "Veeam Help Centerテクニカルドキュメント"。

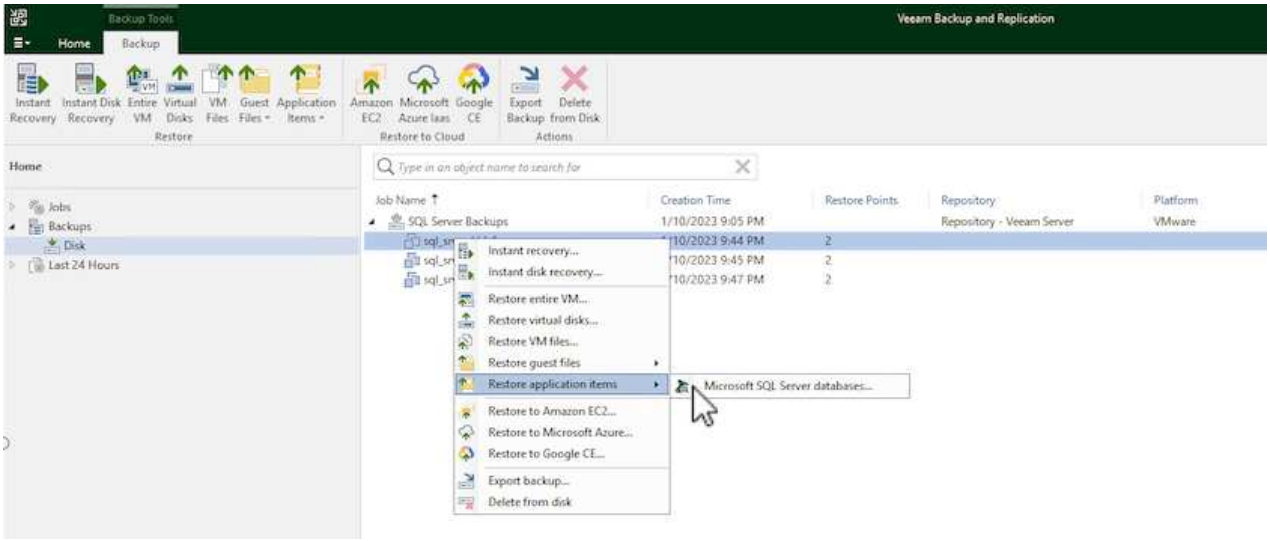
SQL Serverデータベースをリストアします

Veeam Backup & Replicationには、SQL Serverデータベースをリストアするためのオプションがいくつか用意されています。この検証では、Veeam Explorer for SQL ServerとInstant Recoveryを使用して、SQL Serverデータベースのリストアを実行しました。SQL Server Instant Recoveryは、データベースのフルリストアを待たずに、SQL Serverデータベースを迅速にリストアできる機能です。この迅速なリカバリプロセスにより、ダウンタイムが最小限に抑えられ、ビジネス継続性が確保されます。仕組みは次のとおりです。

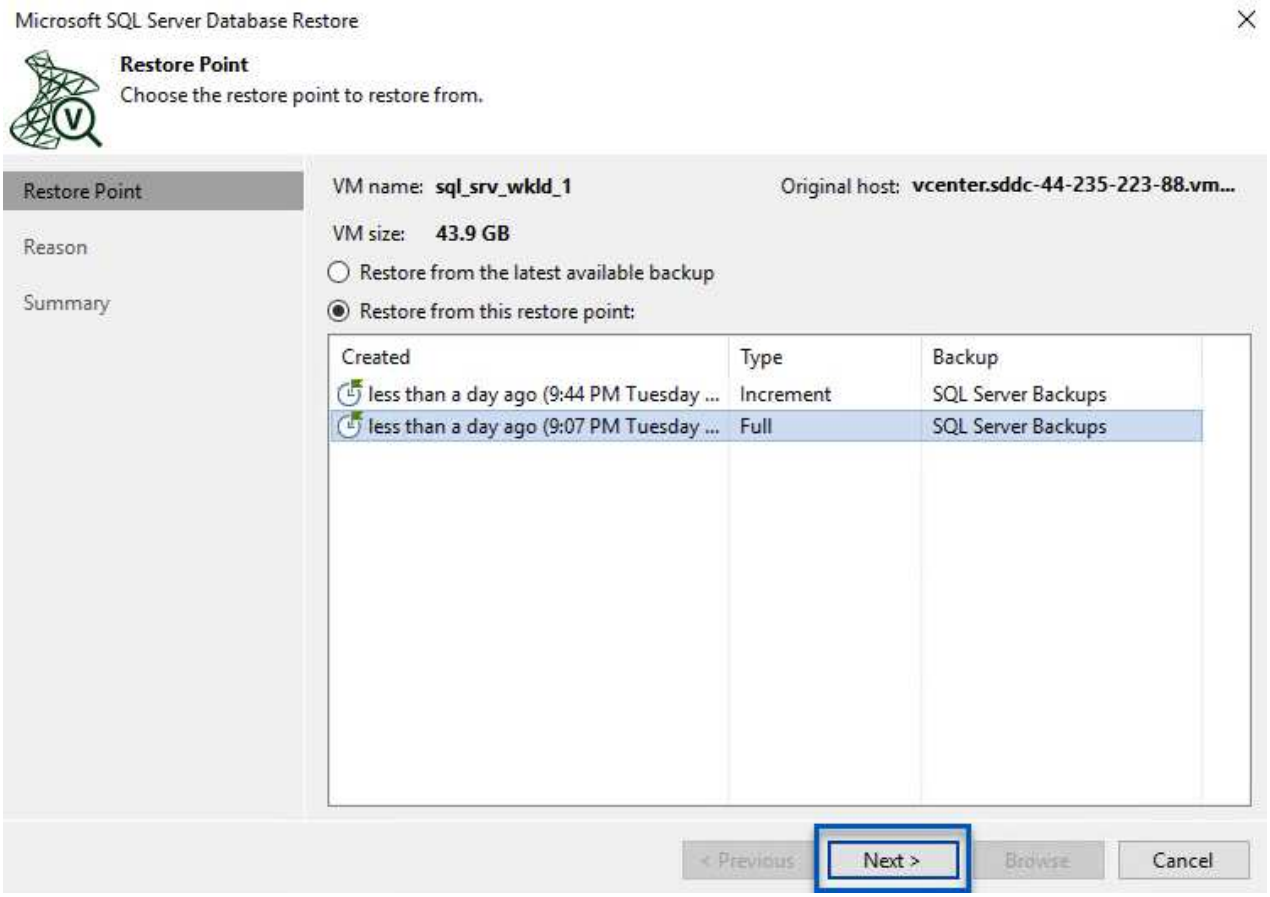
- Veeam Explorer *で、リストア対象のSQL Serverデータベースを含むバックアップ*をマウントします。
- ソフトウェア*は、マウントされたファイルからデータベース*を直接パブリッシュし、ターゲットSQL Serverインスタンス上の一時データベースとしてアクセスできるようにします。
- 一時データベースの使用中、Veeam Explorer *はユーザークエリ*をこのデータベースにリダイレクトし、ユーザーが引き続きデータにアクセスして作業できるようにします。
- Veeam *はバックグラウンドでフルデータベースリストア*を実行し、一時データベースから元のデータベースの場所にデータを転送します。
- フルデータベースのリストアが完了すると、Veeam Explorer *はユーザークエリを元の*データベースに戻し、一時データベースを削除します。

Veeam Explorer Instant Recoveryを使用して**SQL Server**データベースをリストアします

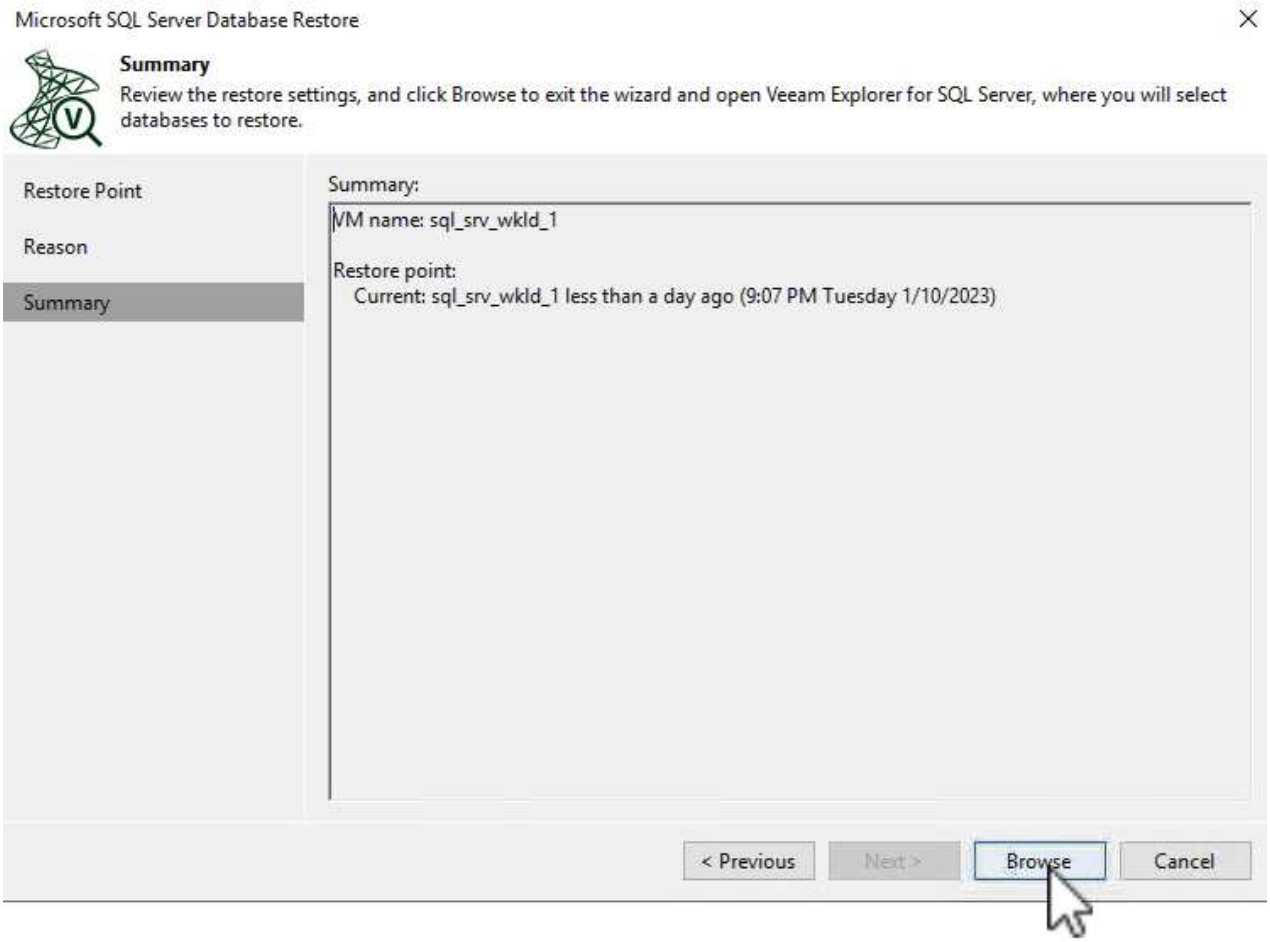
1. Veeam Backup & Replicationコンソールで、SQL Serverバックアップのリストに移動し、サーバを右クリックして*を選択し、[Microsoft SQL Serverデータベース…]*を選択します。



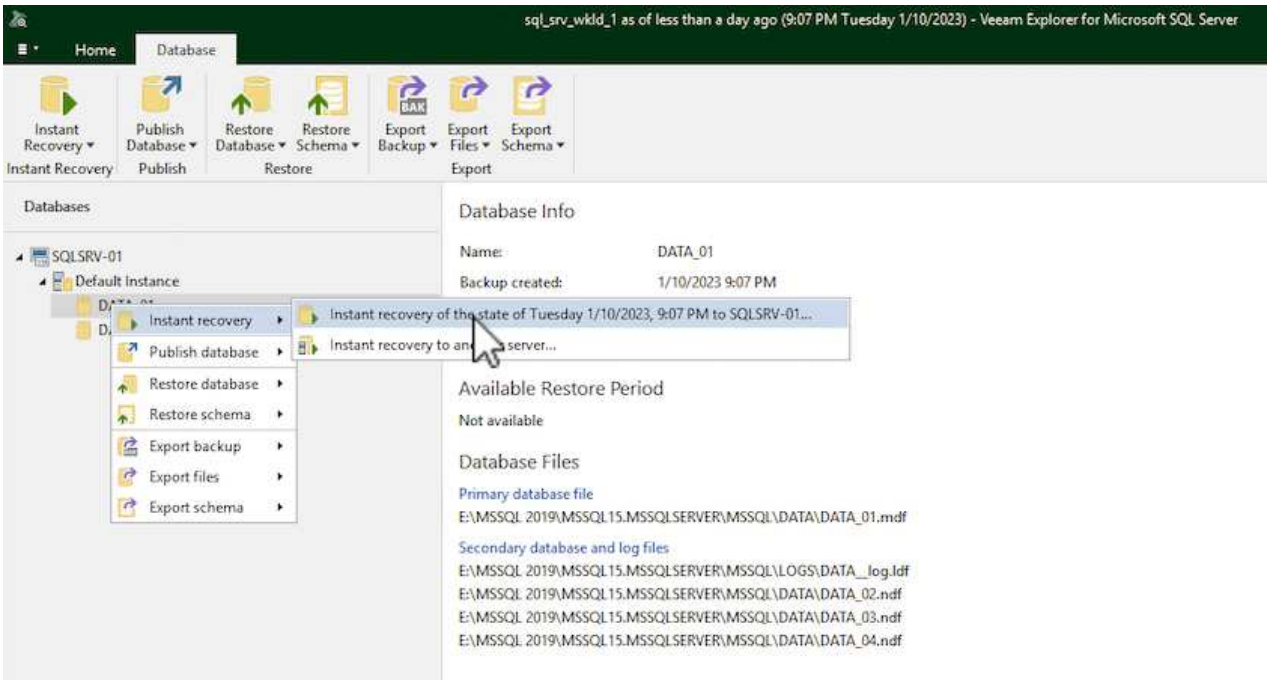
2. Microsoft SQL Serverデータベースのリストアウィザードで、リストからリストアポイントを選択し、*[次へ]*をクリックします。



3. 必要に応じて*を入力し、**[**概要**]**ページで[参照]*ボタンをクリックしてVeeam Explorer for Microsoft SQL Serverを起動します。

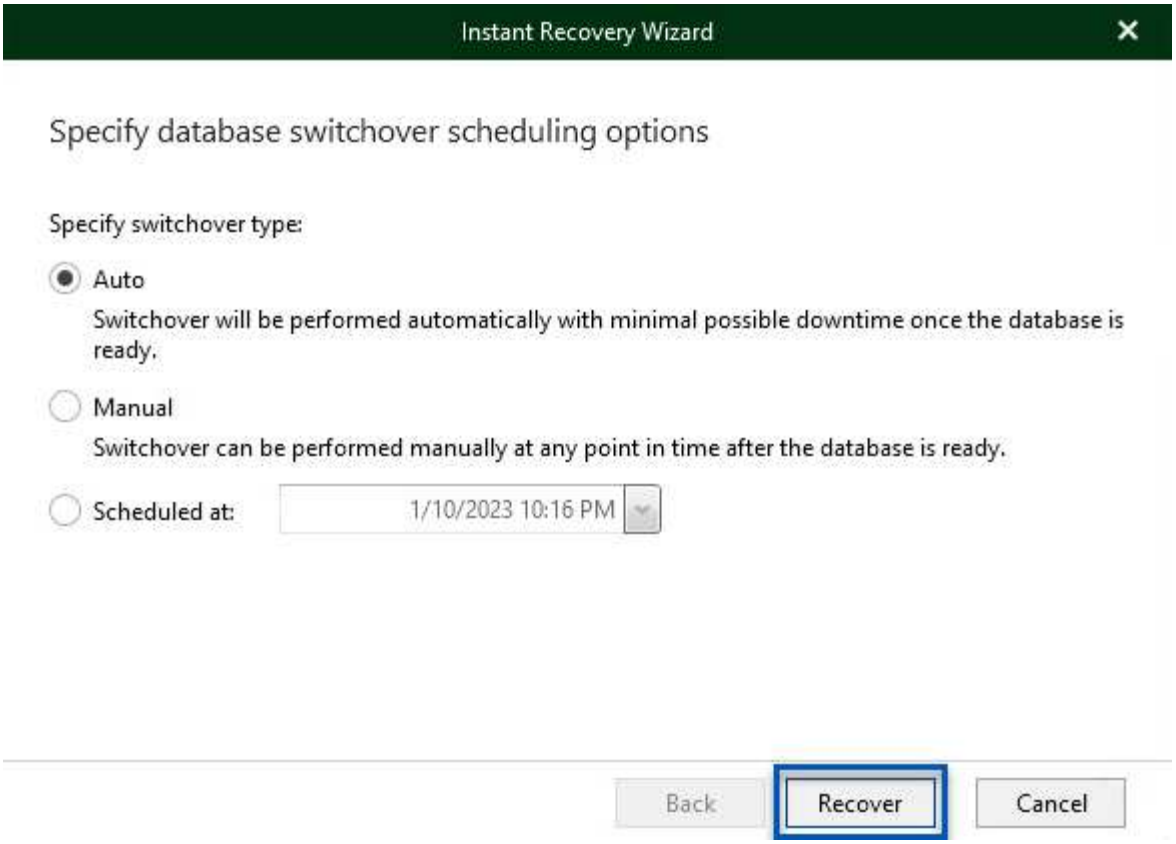


4. Veeam Explorerでデータベースインスタンスのリストを展開し、右クリックして*[Instant recovery]*を選択し、リカバリ先のリストアポイントを指定します。

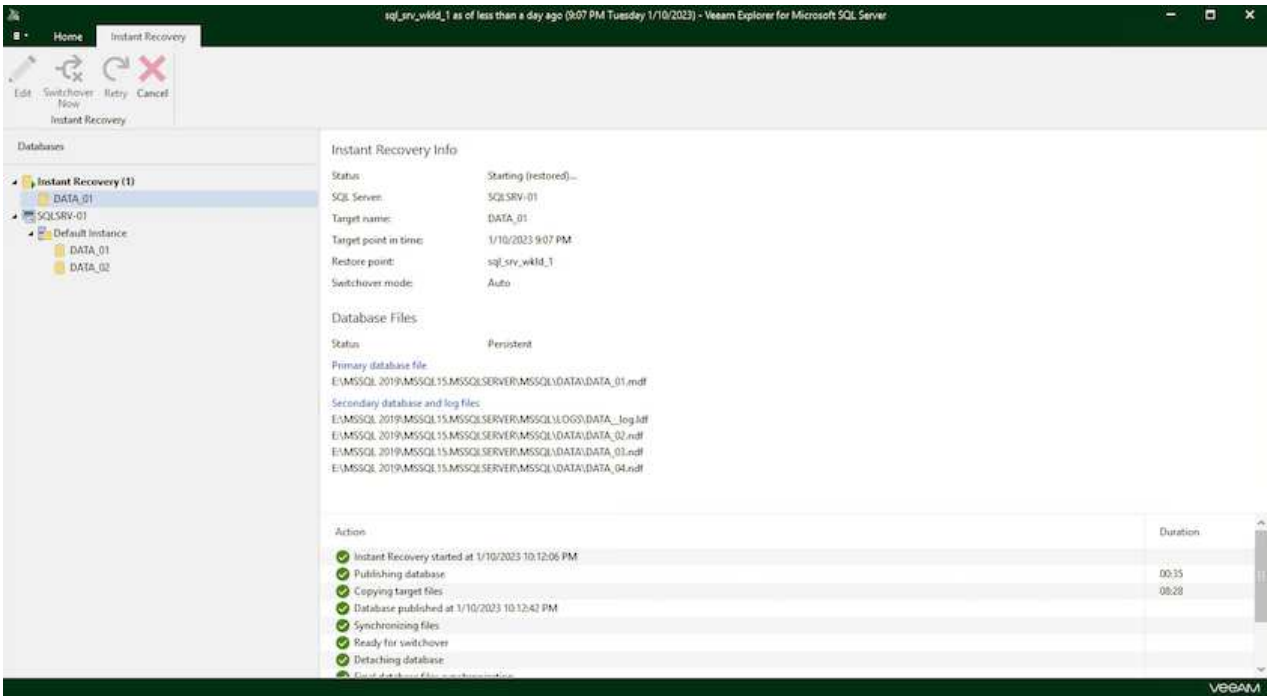


5. Instant Recovery Wizardで、スイッチオーバータイプを指定します。これは、最小限のダウンタイムで自動的に行うことも、手動で行うことも、指定した時間に行うこともできます。次に、*回復*ボタ

ンをクリックして、復元プロセスを開始します。



6. リカバリプロセスはVeeam Explorerから監視できます。



Veeam Explorerを使用してSQL Serverのリストア処理を実行する方法の詳細については、のMicrosoft SQL Serverの項を参照してください "Veeam Explorers User Guideを参照してください"。

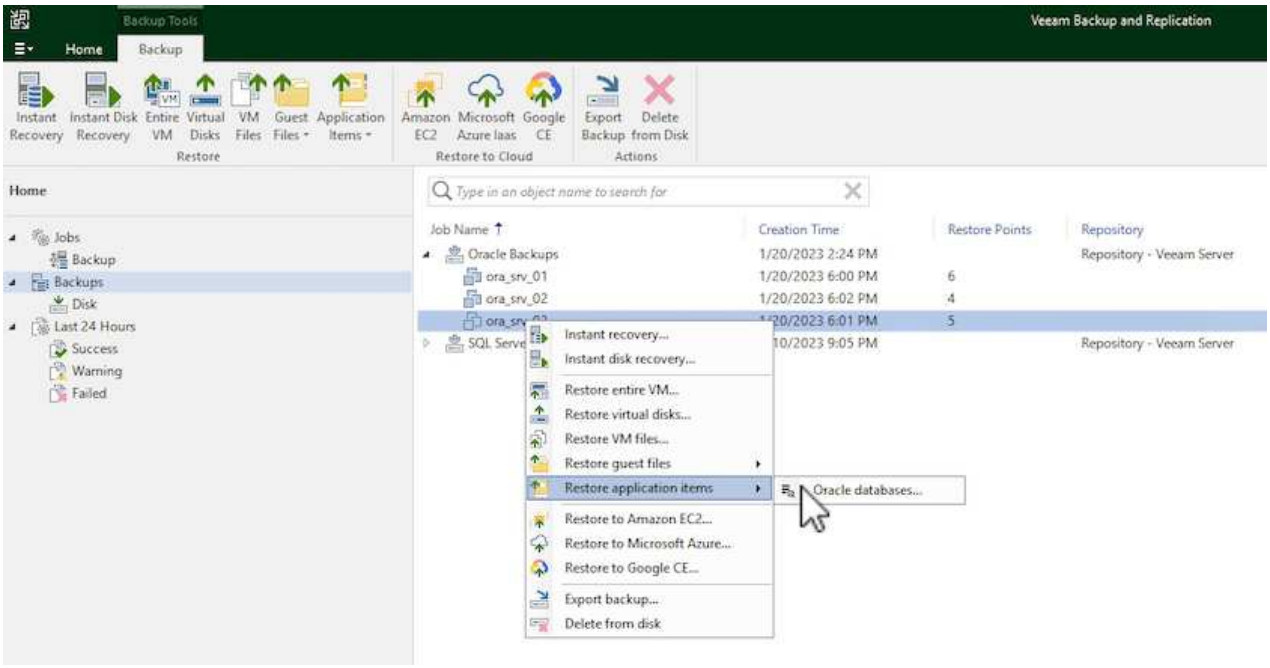
Veeam Explorerを使用してOracleデータベースをリストアします

Veeam Explorer for Oracle databaseでは、Instant Recoveryを使用して、Oracleデータベースの標準リストアまたは中断のないリストアを実行できます。また、データベースのパブリッシュをサポートしているため、高速アクセス、Data Guardデータベースのリカバリ、RMANバックアップからのリストアが可能です。

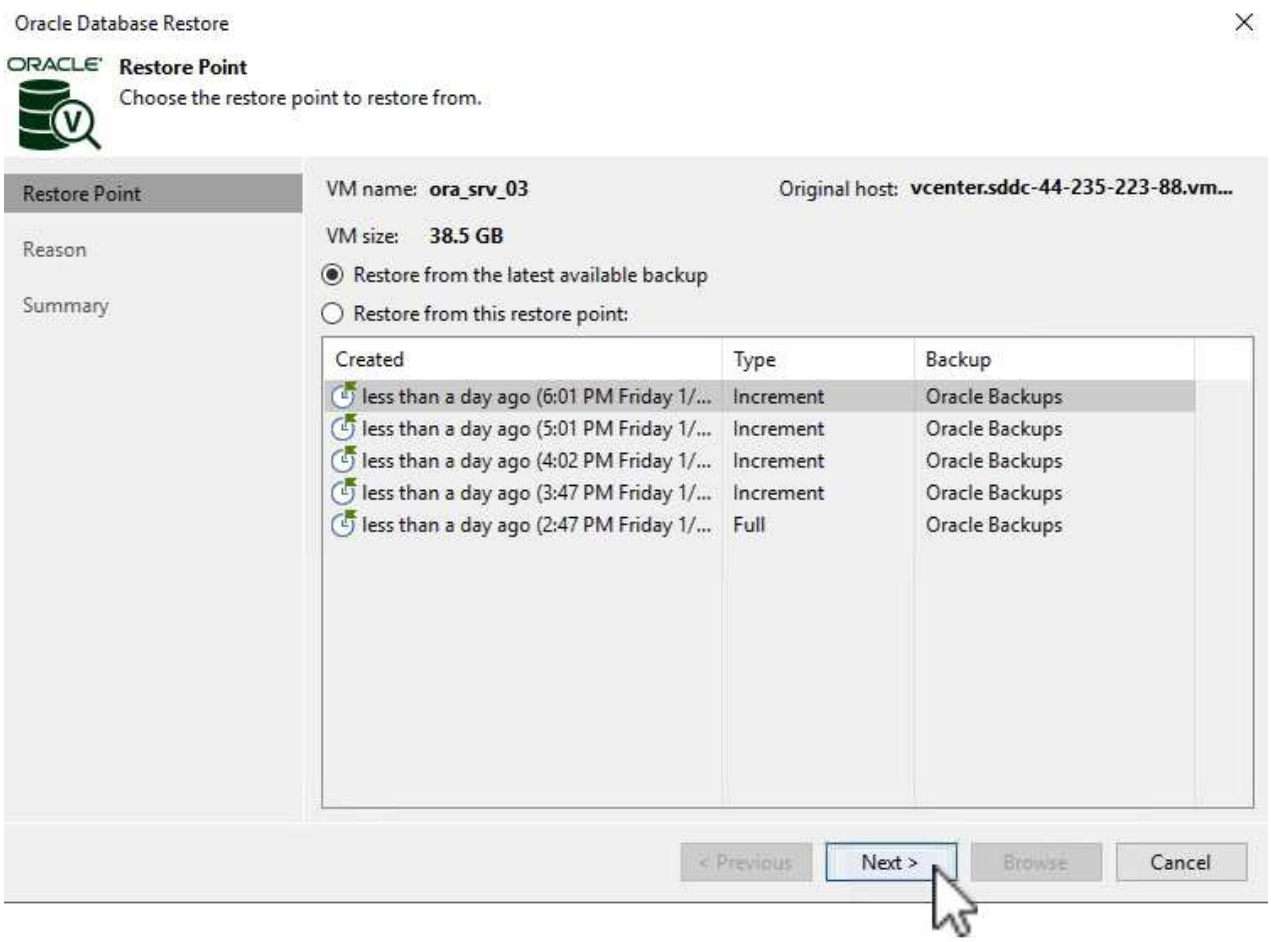
Veeam Explorerを使用してOracleデータベースのリストア処理を実行する方法の詳細については、のOracleのセクションを参照してください "Veeam Explorers User Guideを参照してください"。

このセクションでは、Veeam Explorerを使用して、別のサーバへのOracleデータベースのリストアについて説明します。

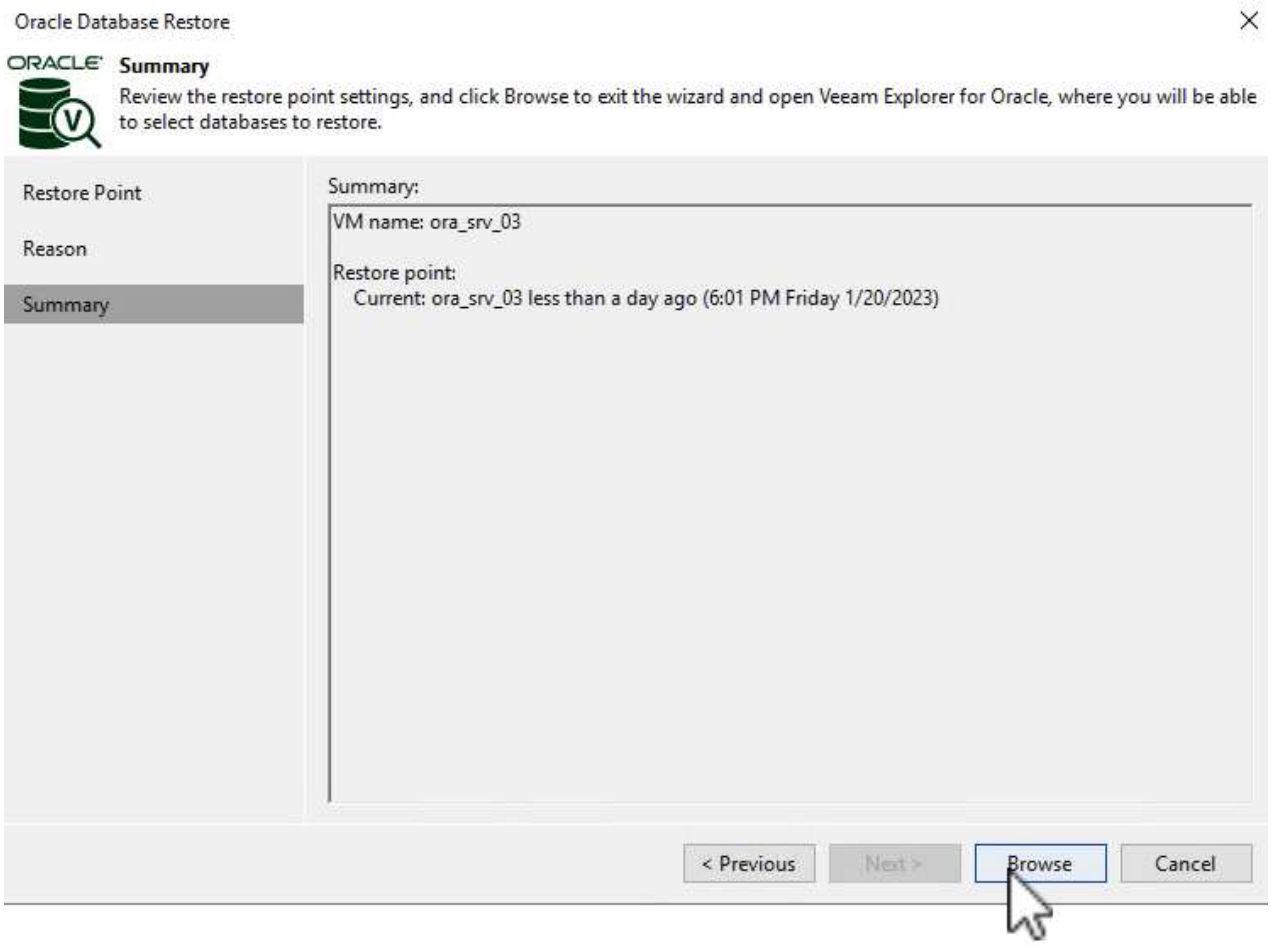
1. Veeam Backup & Replicationコンソールで、Oracleバックアップのリストに移動し、サーバを右クリックして*を選択し、[Oracleデータベース…]*を選択します。



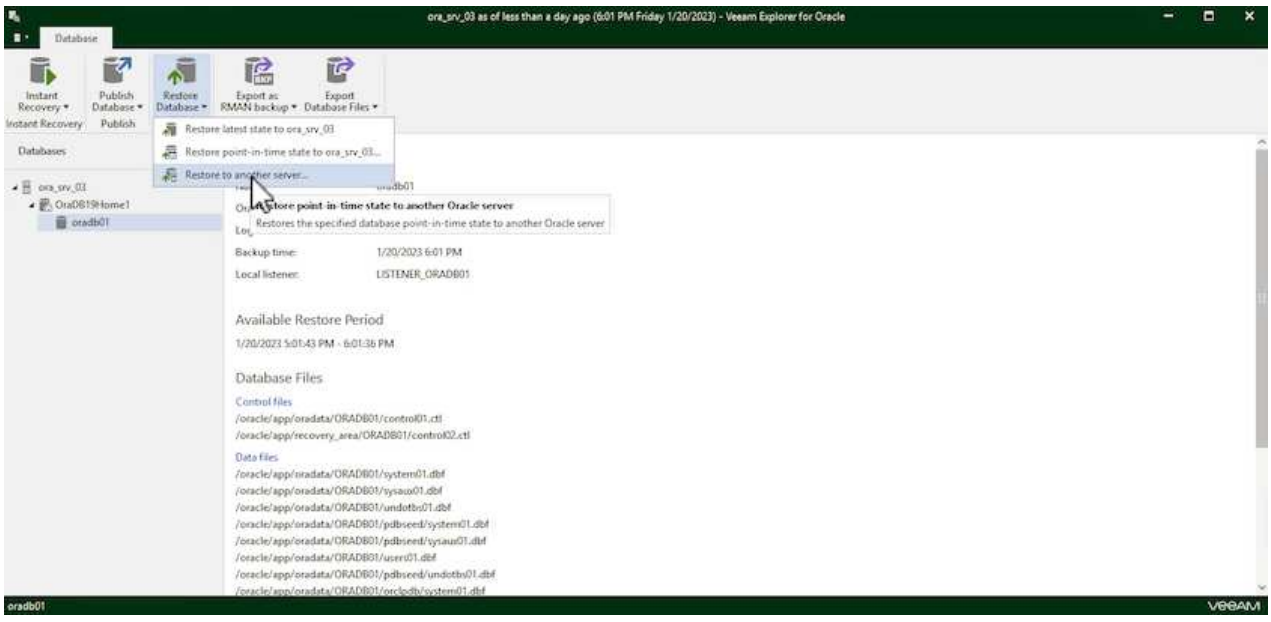
2. Oracle Databaseリストア・ウィザードで、リストからリストア・ポイントを選択し、*[Next]*をクリックします。



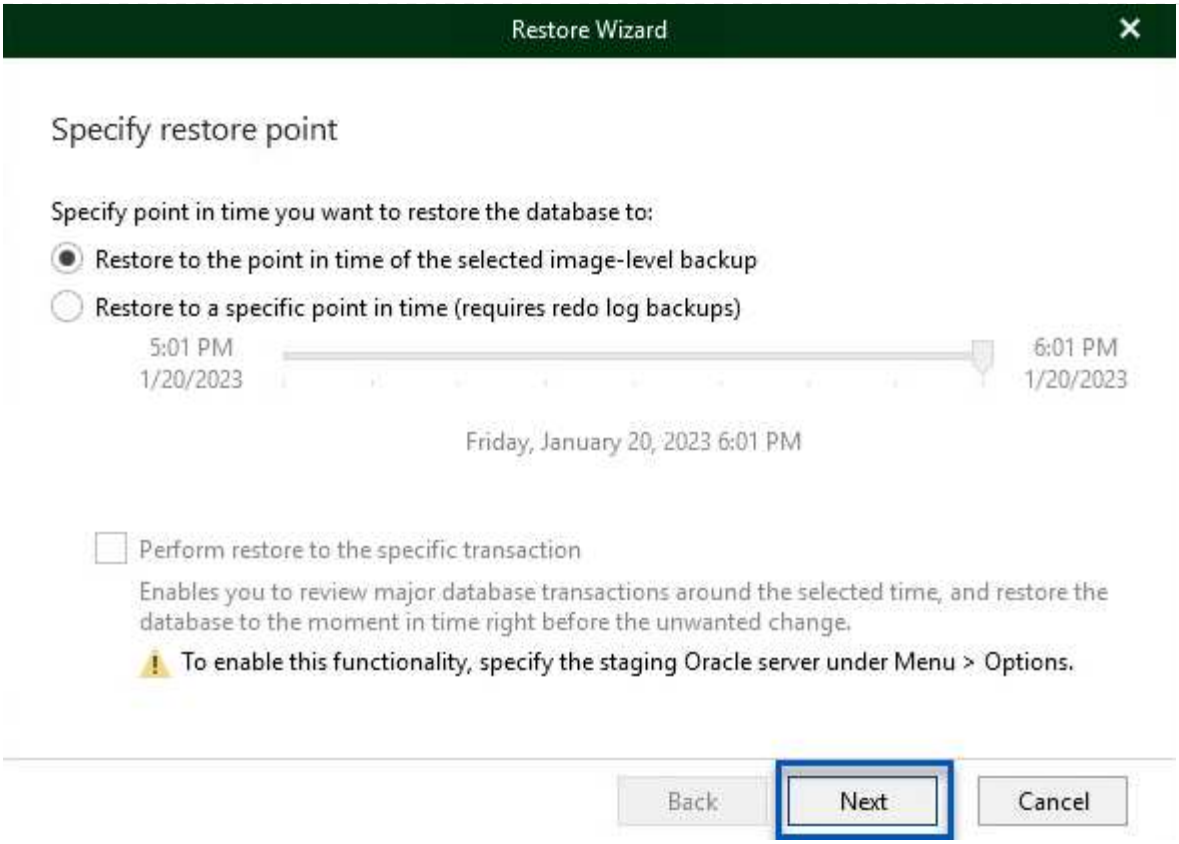
3. 必要に応じて*を入力し、**[**概要**]**ページで[参照]*ボタンをクリックしてVeeam Explorer for Oracleを起動します。



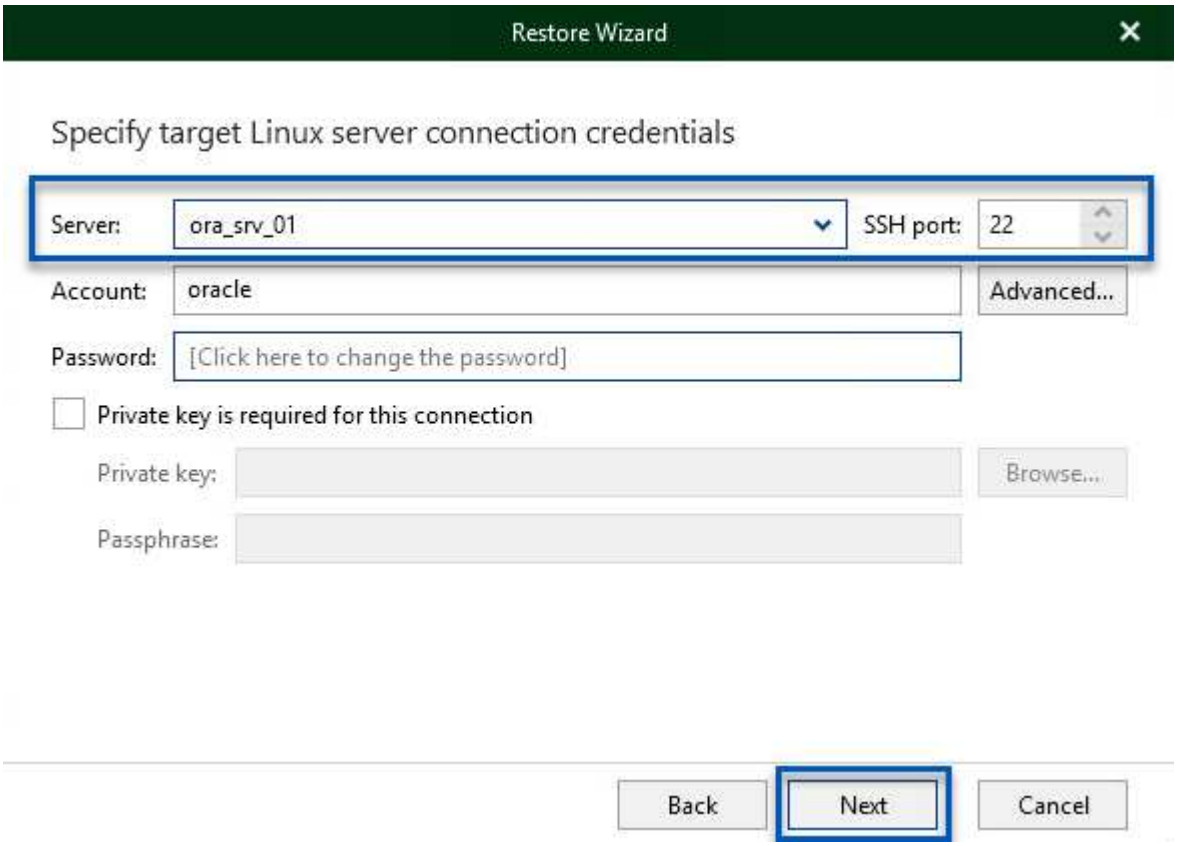
4. Veeam Explorerでデータベースインスタンスのリストを展開表示し、リストアするデータベースをクリックしてから、上部の*ドロップダウンメニューから[別のサーバにリストア...]*を選択します。



5. リストアウィザードで、リストア元のリストアポイントを指定し、*[次へ]*をクリックします。

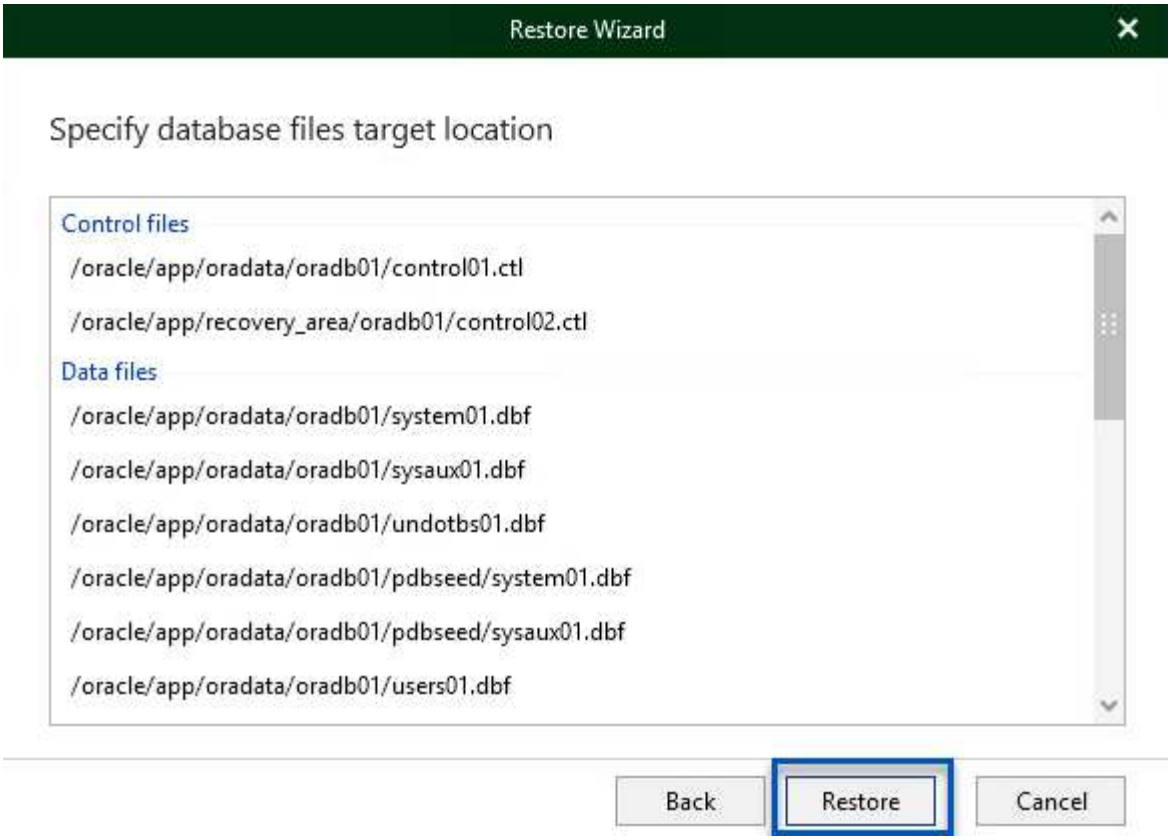


6. データベースのリストア先となるターゲットサーバとアカウントのクレデンシャルを指定し、*[次へ]*をクリックします。



7. 最後に、データベースファイルのターゲットの場所を指定し、*[リストア]*ボタンをクリックしてリ

ストアプロセスを開始します。

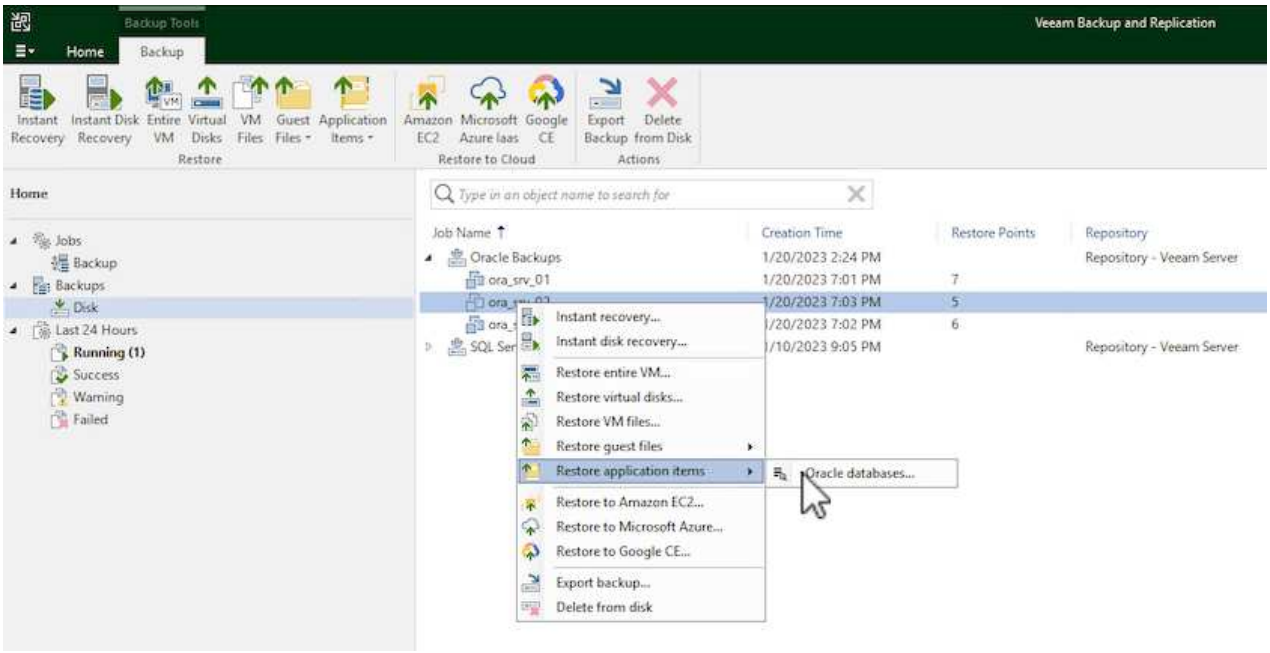


8. データベースのリカバリが完了したら、サーバ上でOracleデータベースが正常に起動していることを確認します。

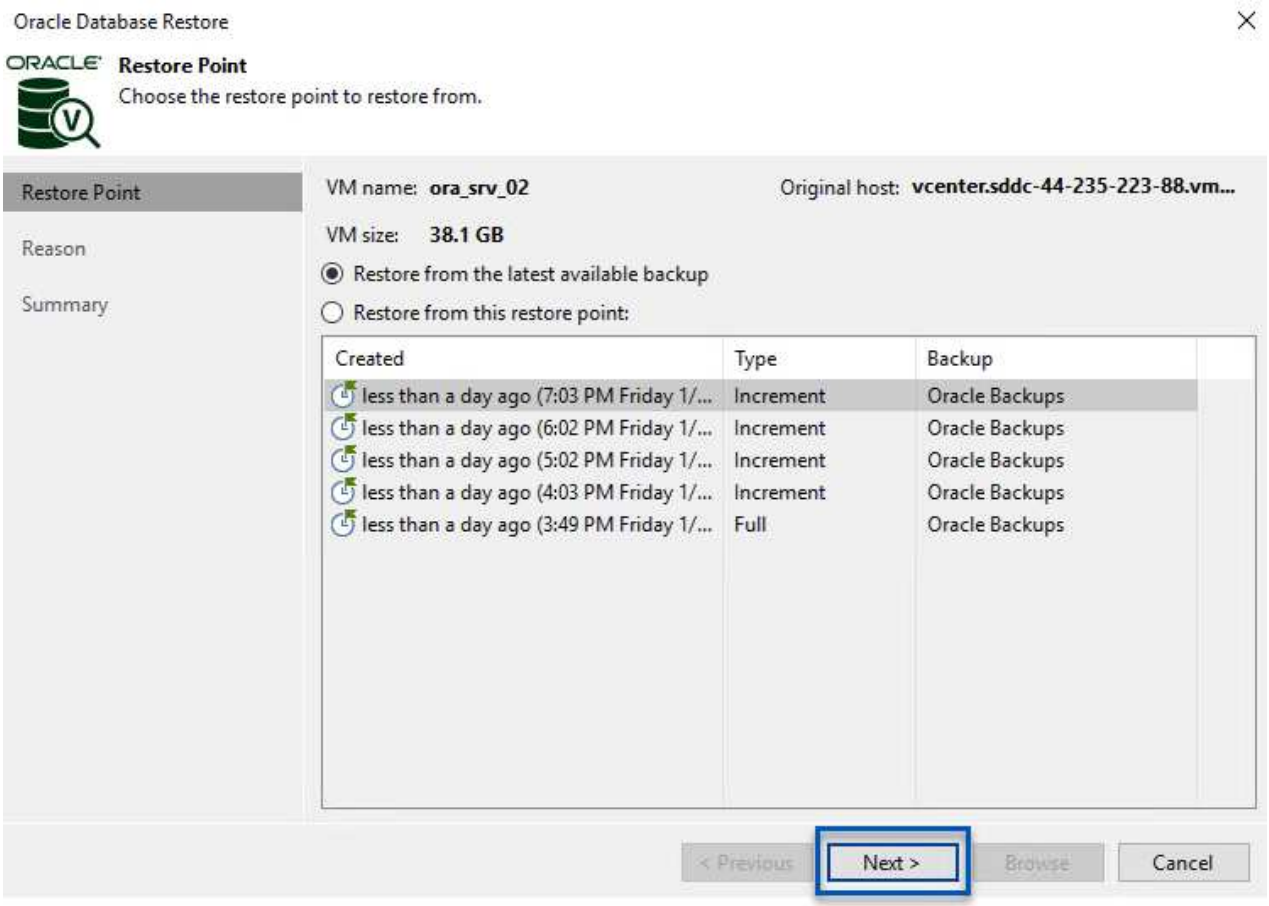
Oracleデータベースを代替サーバにパブリッシュします

このセクションでは、フルリストアを起動せずに高速アクセスできるように、データベースを代替サーバにパブリッシュします。

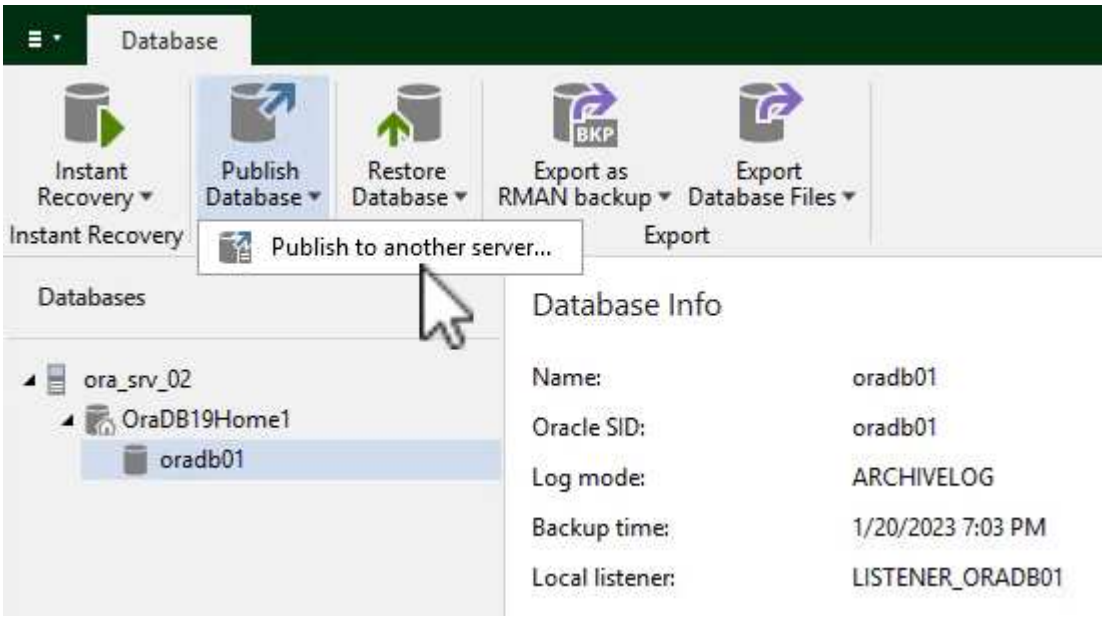
1. Veeam Backup & Replicationコンソールで、Oracleバックアップのリストに移動し、サーバを右クリックして*を選択し、[Oracleデータベース…]*を選択します。



2. Oracle Databaseリストア・ウィザードで、リストからリストア・ポイントを選択し、*[Next]*をクリックします。

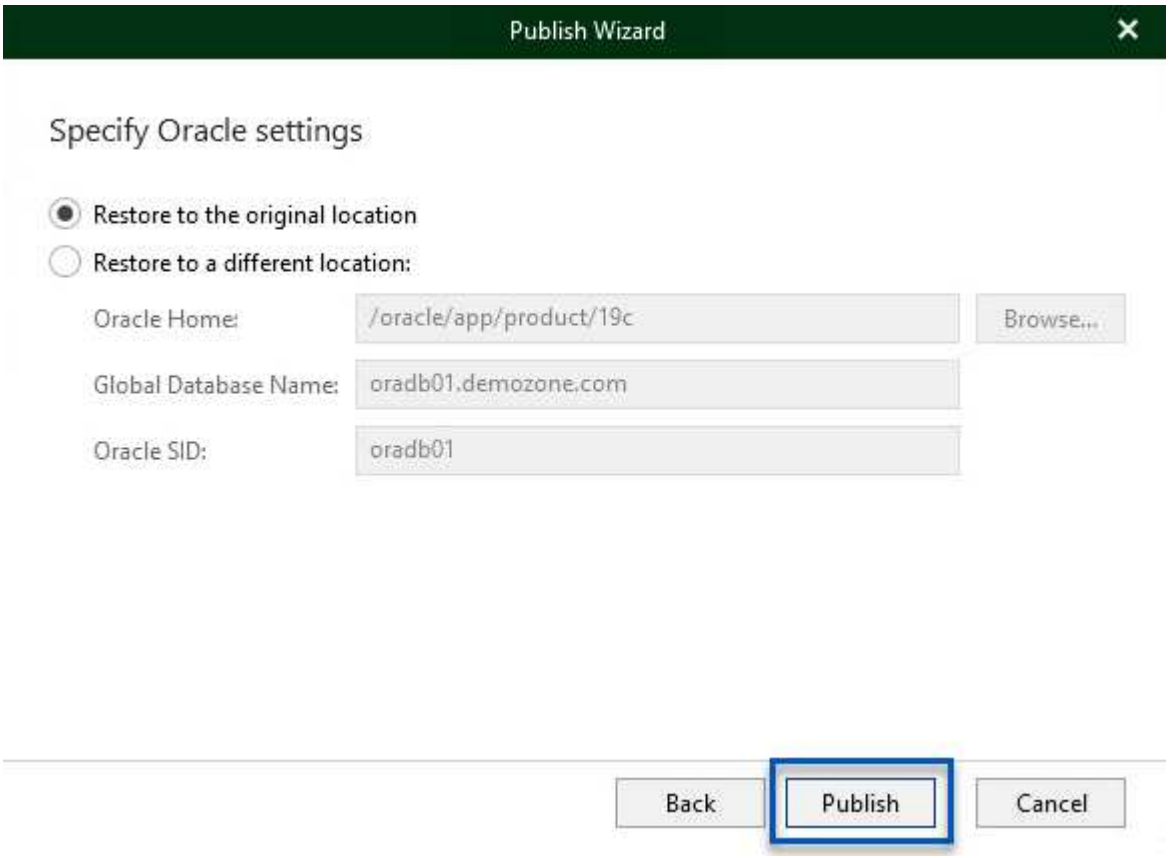


3. 必要に応じて*を入力し、[概要]ページで[参照]*ボタンをクリックしてVeeam Explorer for Oracleを起動します。
4. Veeam Explorerでデータベースインスタンスのリストを展開し、リストアするデータベースをクリックしてから、上部の*ドロップダウン・メニューから[Publish to another server…]*を選択します。



5. パブリッシュウィザードで、データベースのパブリッシュ元の復元ポイントを指定し、*次へ*をクリックします。

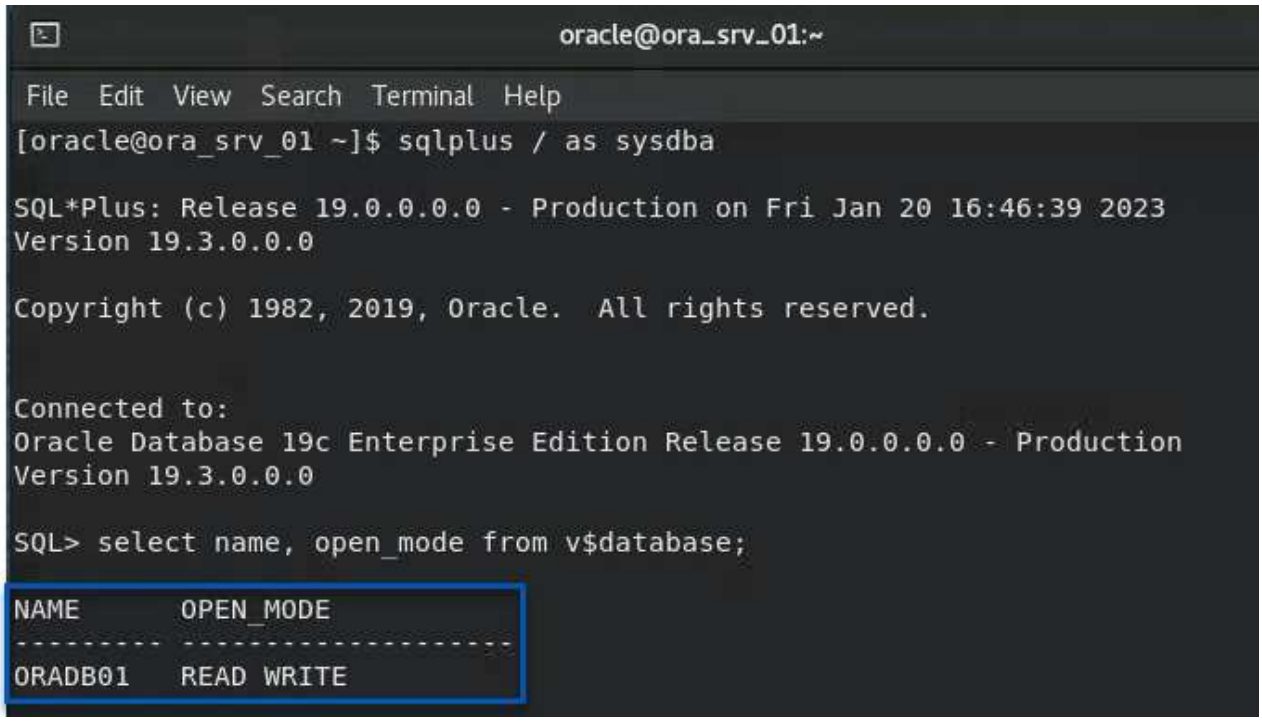
6. 最後に、ターゲットLinuxファイルシステムの場所を指定し、* Publish *をクリックしてリストアプロセスを開始します。



7. パブリッシュが完了したら、ターゲットサーバーにログインし、次のコマンドを実行してデータベースが実行されていることを確認します。

```
oracle@ora_srv_01> sqlplus / as sysdba
```

```
SQL> select name, open_mode from v$database;
```



まとめ

VMware Cloudは、ビジネスクリティカルなアプリケーションを実行し、機密データを保存するための強力なプラットフォームです。セキュアなデータ保護解決策 は、ビジネス継続性を確保し、サイバー脅威やデータ損失から保護するためにVMware Cloudを利用する企業にとって不可欠です。信頼性と堅牢性に優れたデータ保護解決策 を選択することで、企業は、重要なデータが何であっても安全であることを確信できます。

本ドキュメントで紹介するユースケースは、ネットアップ、VMware、Veeamの統合に焦点を当てた実績のあるデータ保護テクノロジに焦点を当てています。FSx for ONTAP は、AWSのVMware Cloud向けの補完的NFSデータストアとしてサポートされており、すべての仮想マシンとアプリケーションデータに使用されます。Veeam Backup & Replicationは、バックアップ/リカバリプロセスの改善、自動化、合理化を支援するために設計された包括的なデータ保護解決策 です。VeeamをiSCSIバックアップターゲットボリューム（FSx for ONTAP でホスト）と組み合わせて使用すると、VMware Cloudに存在するアプリケーションデータに対して、安全で管理しやすいデータ保護解決策 を提供できます。

追加情報

この解決策 に記載されているテクノロジの詳細については、次の追加情報 を参照してください。

- "FSx for ONTAP ユーザガイド"
- "Veeam Help Centerテクニカルドキュメント"
- "VMware Cloud on AWSのサポート：考慮事項および制限事項"

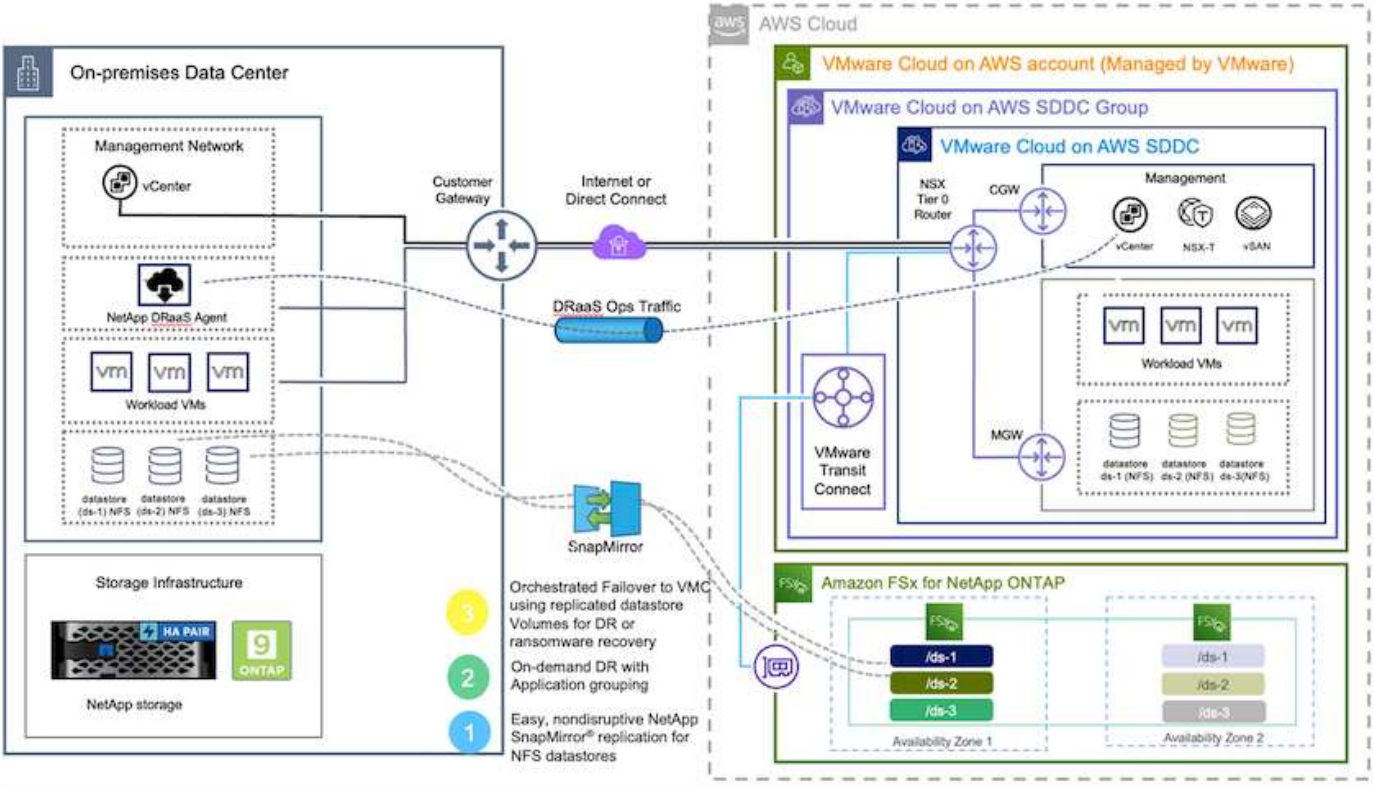
TR-4955：『Disaster Recovery with FSX for ONTAP and VMC（AWS VMware Cloud）』

ネットアップ、 Niyaz Mohamed

概要

クラウドへのディザスタリカバリは、耐障害性に優れた対費用効果の高い方法で、サイトの停止やデータ破損からワークロードを保護します（ランサムウェアなど）。NetApp SnapMirrorテクノロジを使用すると、オンプレミスのVMwareワークロードをAWSで実行されるFSX for ONTAP にレプリケートできます。

ディザスタリカバリオーケストレーションツール（DRO：UIを備えたスクリプト化された解決策 ）を使用すると、オンプレミスからFSX for ONTAP にレプリケートされたワークロードをシームレスにリカバリできます。DROは'VMの登録からVMCへのSnapMirrorレベルからNSXで直接ネットワーク・マッピングへのリカバリを自動化しますこの機能はすべてのVMC環境に含まれています。



はじめに

AWSに**VMware Cloud**を導入して設定

"AWS 上の VMware Cloud" AWSエコシステム内のVMwareベースのワークロードにクラウドネイティブなエクスペリエンスを提供します。各VMware Software-Defined Data Center（SDDC）はAmazon Virtual Private Cloud（VPC）内で動作し、フルVMwareスタック（vCenter Serverを含む）、NSXベースのSoftware-Defined Networking、VSANソフトウェア定義ストレージ、およびワークロードにコンピューティングリソースとストレージリソースを提供する1つ以上のESXiホストを提供します。AWSでVMC環境を設定するには、次の手順を実行します "リンク"。パイロットライトクラスタはDRにも使用できます。

初期リリースでは、DROは既存のパイロットライトクラスタをサポートします。オンデマンドのSDDC作成は、今後のリリースで提供される予定です。

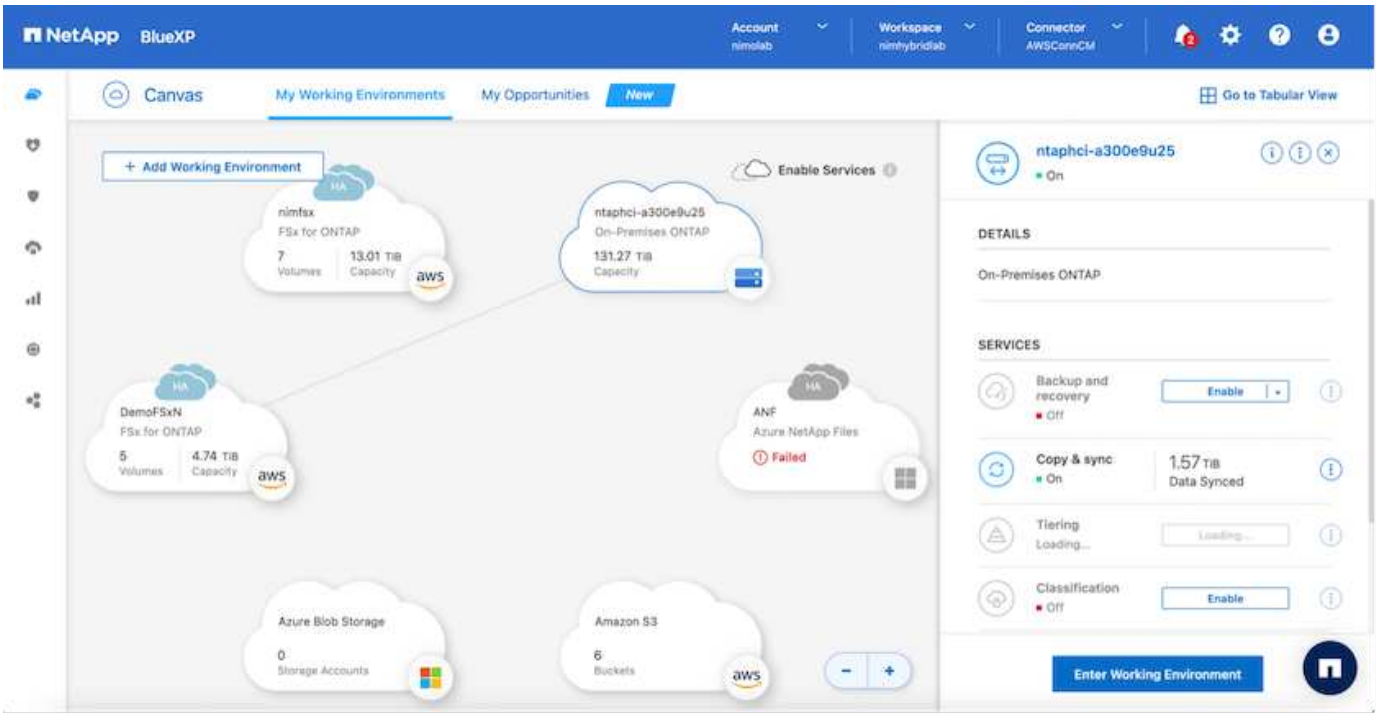
ONTAP の**FSX**をプロビジョニングして構成します

Amazon FSX for NetApp ONTAP はフルマネージドサービスで、広く普及しているNetApp ONTAP ファイルシステムを基盤に、信頼性、拡張性、パフォーマンス、機能豊富なファイルストレージを提供します。この手

順を実行します "リンク" ONTAP のFSXをプロビジョニングおよび構成するには、次の手順を実行します

SnapMirrorを**ONTAP** 用に**FSX**に導入して設定する

次の手順では、NetApp BlueXPを使用して、AWSインスタンス上のONTAP 用にプロビジョニングされたFSXを検出し、必要なデータストアボリュームをオンプレミス環境から適切な頻度でFSX for ONTAP にレプリケートし、ネットアップのSnapshotコピーを保持します。



BlueXPを設定するには、このリンクの手順に従います。NetApp ONTAP CLIを使用して、このリンクに続くレプリケーションをスケジュールすることもできます。

SnapMirror関係は前提条件であり、事前に作成しておく必要があります。

DROのインストール

DROを開始するには、指定されたEC2インスタンスまたは仮想マシン上のUbuntuオペレーティングシステムを使用して、前提条件を満たしていることを確認します。次に、パッケージをインストールします。

前提条件

- ソースおよびデスティネーションのvCenterおよびストレージシステムへの接続が存在することを確認してください。
- DNS名を使用する場合は、DNS解決を実施する必要があります。それ以外の場合は、vCenterとストレージシステムのIPアドレスを使用してください。
- root権限を持つユーザを作成します。EC2インスタンスではsudoも使用できます。

OSの要件

- Ubuntu 20.04（LTS）：2GB以上、vCPU×4

- 指定されたエージェントVMに次のパッケージがインストールされている必要があります。
  - Docker です
  - docker -構成
  - Jq

の権限を変更します `docker.sock`： `sudo chmod 666 /var/run/docker.sock`。

。 `deploy.sh` スクリプトは必要な前提条件をすべて実行します。

パッケージをインストールします

1. 指定した仮想マシンにインストールパッケージをダウンロードします。

```
git clone https://github.com/NetApp/DRO-AWS.git
```

このエージェントは、オンプレミスまたはAWS VPC内にインストールできます。

2. パッケージを解凍して導入スクリプトを実行し、ホストIP（10.10.10.10など）を入力します。

```
tar xvf DRO-prereq.tar
```

3. ディレクトリに移動し、次のように配置スクリプトを実行します。

```
sudo sh deploy.sh
```

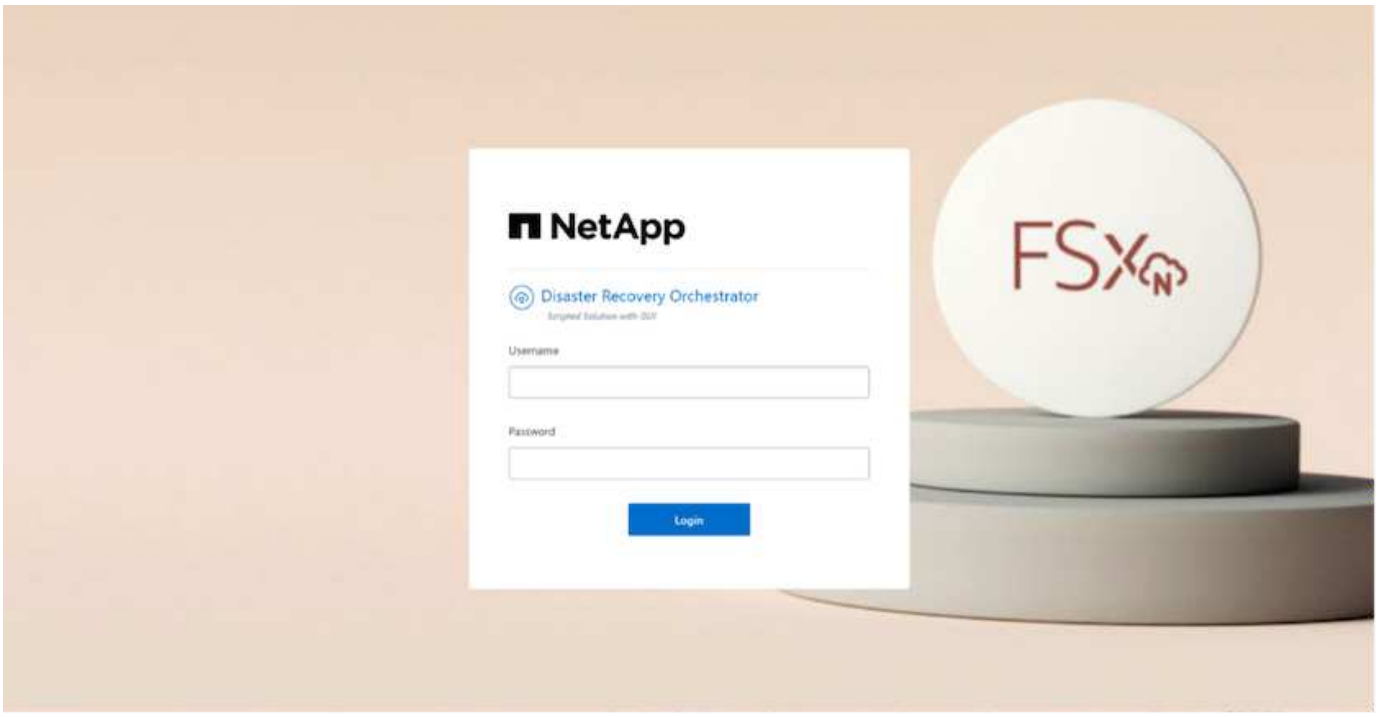
4. UIには次の方法でアクセスします。

```
https://<host-ip-address>
```

次のデフォルトクレデンシャルを使用：

```
Username: admin
Password: admin
```

パスワードは、Change Passwordオプションを使用して変更できます。



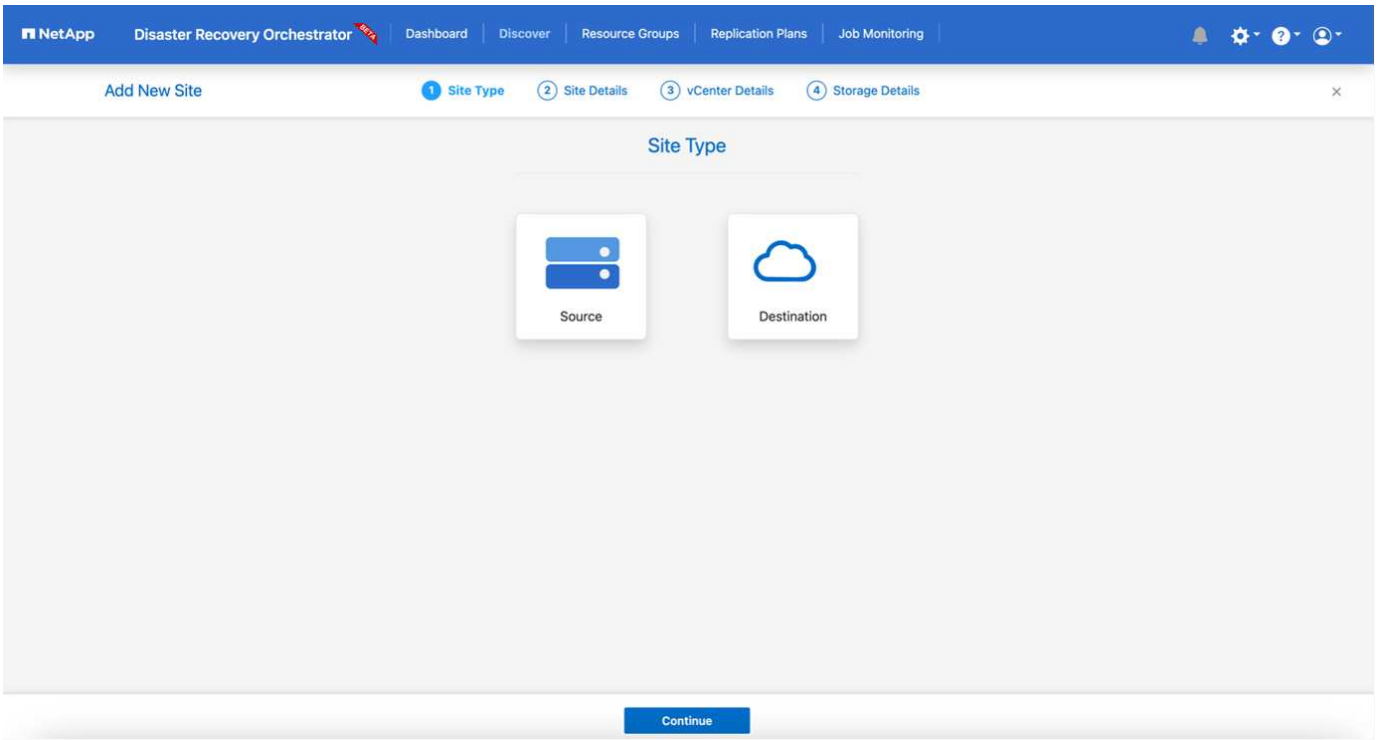
DRO構成

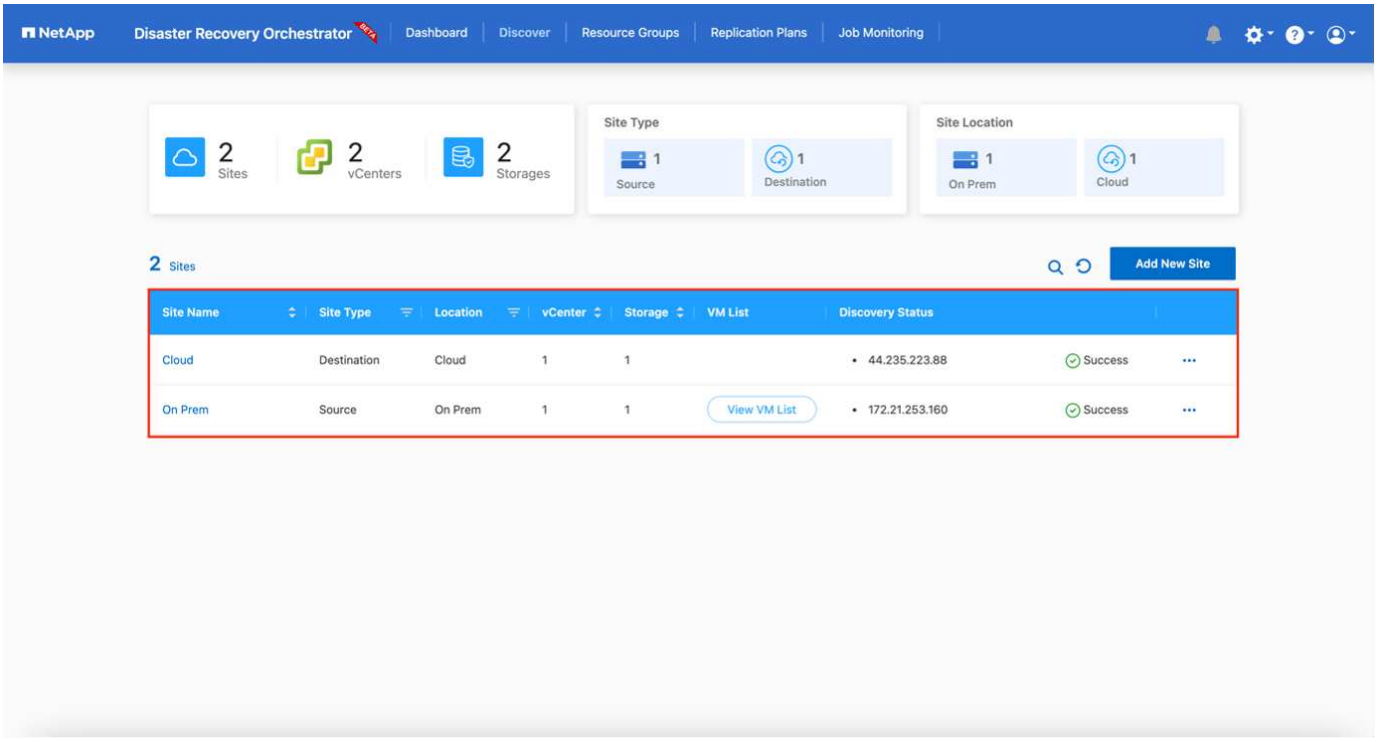
FSX for ONTAP およびVMCが適切に構成されると、FSX for ONTAP 上の読み取り専用SnapMirrorコピーを使用して、オンプレミスのワークロードをVMCに自動でリカバリするためのDROの設定を開始できます。

AWSでDROエージェントを導入し、FSX for ONTAP が導入されているVPCにも導入することを推奨します（ピア接続も可能です）。DROエージェントがネットワーク経由でオンプレミスコンポーネントおよびFSX for ONTAP およびVMCリソースと通信できるようにします。

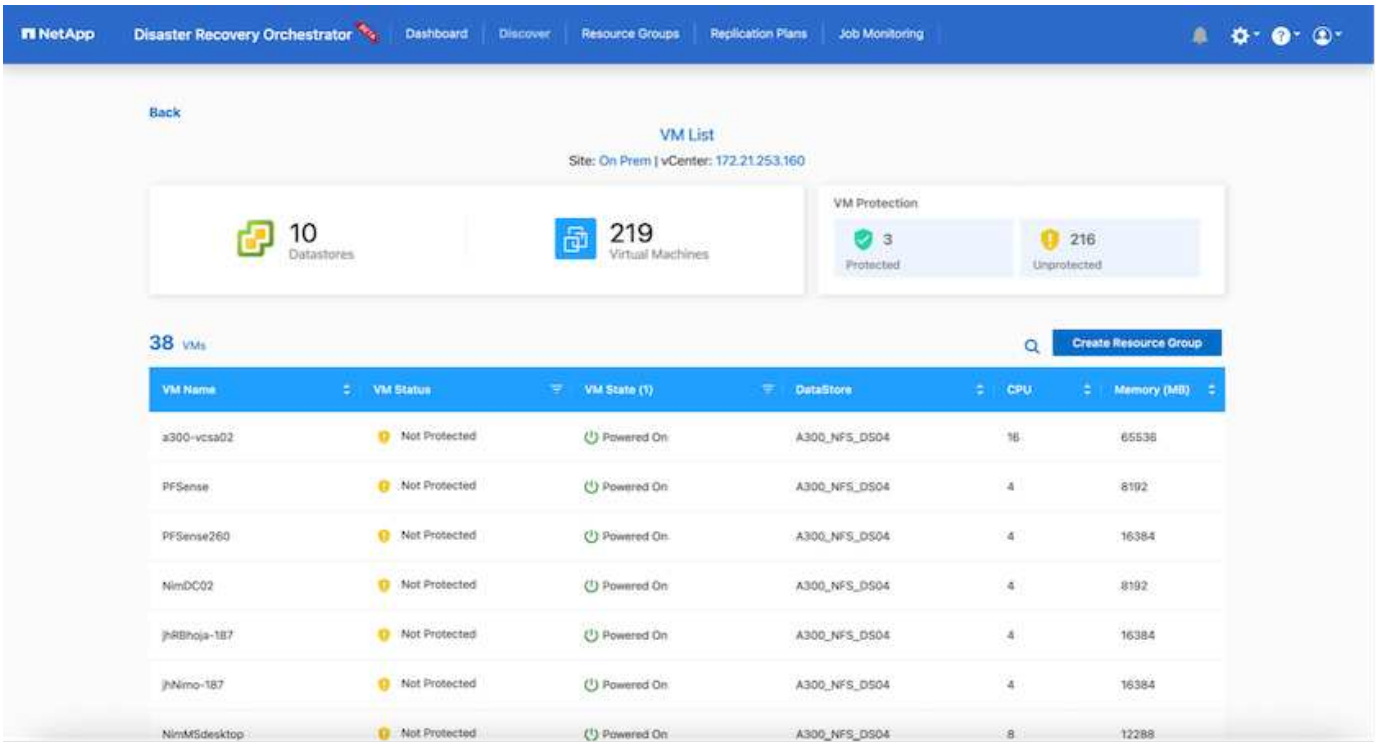
まず、オンプレミスリソースとクラウドリソース（vCenterとストレージの両方）を検出してDROに追加します。サポートされているブラウザでDROを開き、デフォルトのユーザー名とパスワード（admin/admin）およびサイトの追加を使用します。サイトは、Discoverオプションを使用して追加することもできます。次のプラットフォームを追加します。

- オンプレミス
  - オンプレミスのvCenter
  - ONTAP ストレージシステム
- クラウド
  - VMC vCenter
  - FSX for ONTAP の略





追加されると、DROは自動検出を実行し、対応するSnapMirrorレプリカがソーストレージからFSX for ONTAP にあるVMを表示します。DROは、VMが使用するネットワークとポートグループを自動的に検出して、それらにデータを入力します。



次の手順では、必要なVMを、リソースグループとして機能するように機能グループにグループ化します。

リソースのグループ化

プラットフォームを追加したら、リカバリするVMをリソースグループにまとめることができます。DROリソースグループを使用すると、依存する一連のVMを論理グループにグループ化して、それらの起動順序、ブート遅延、およびリカバリ時に実行可能なオプションのアプリケーション検証を含めることができます。

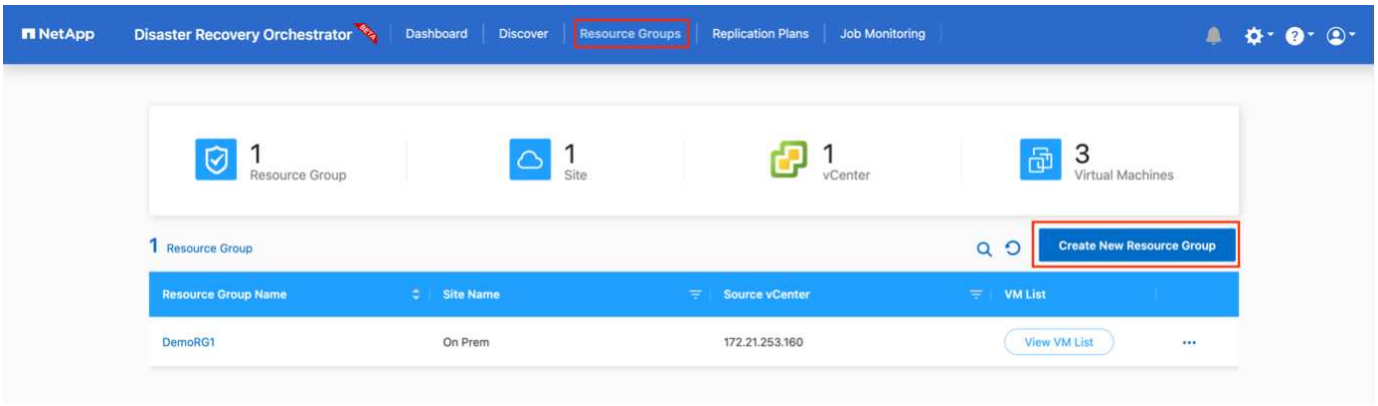
リソースグループの作成を開始するには、次の手順を実行します。

1. *リソースグループ*にアクセスし、*新しいリソースグループの作成*をクリックします。
2. [新しいリソースグループ*]で、ドロップダウンからソースサイトを選択し、[*Create]をクリックします。
3. リソースグループの詳細を入力し、*続行*をクリックします。
4. 検索オプションを使用して、適切なVMを選択します。
5. 選択したVMのブート順序とブート遅延（秒）を選択します。各VMを選択して優先順位を設定し、電源投入シーケンスの順序を設定します。3つはすべてのVMのデフォルト値です。

   オプションは次のとおりです。

   1–最初にパワーオンする仮想マシン3 -デフォルト5 -最後にパワーオンする仮想マシン

6. [リソースグループの作成]をクリックします。

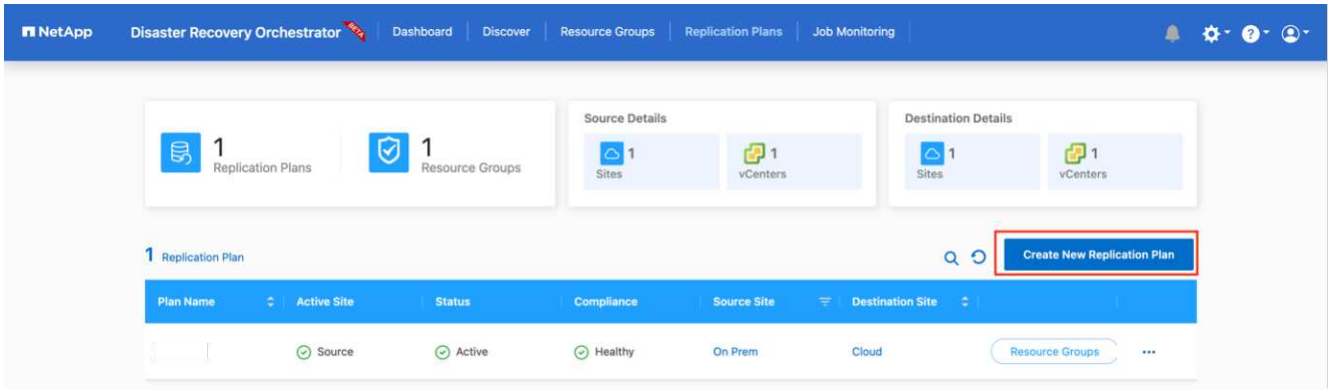


レプリケーションプラン

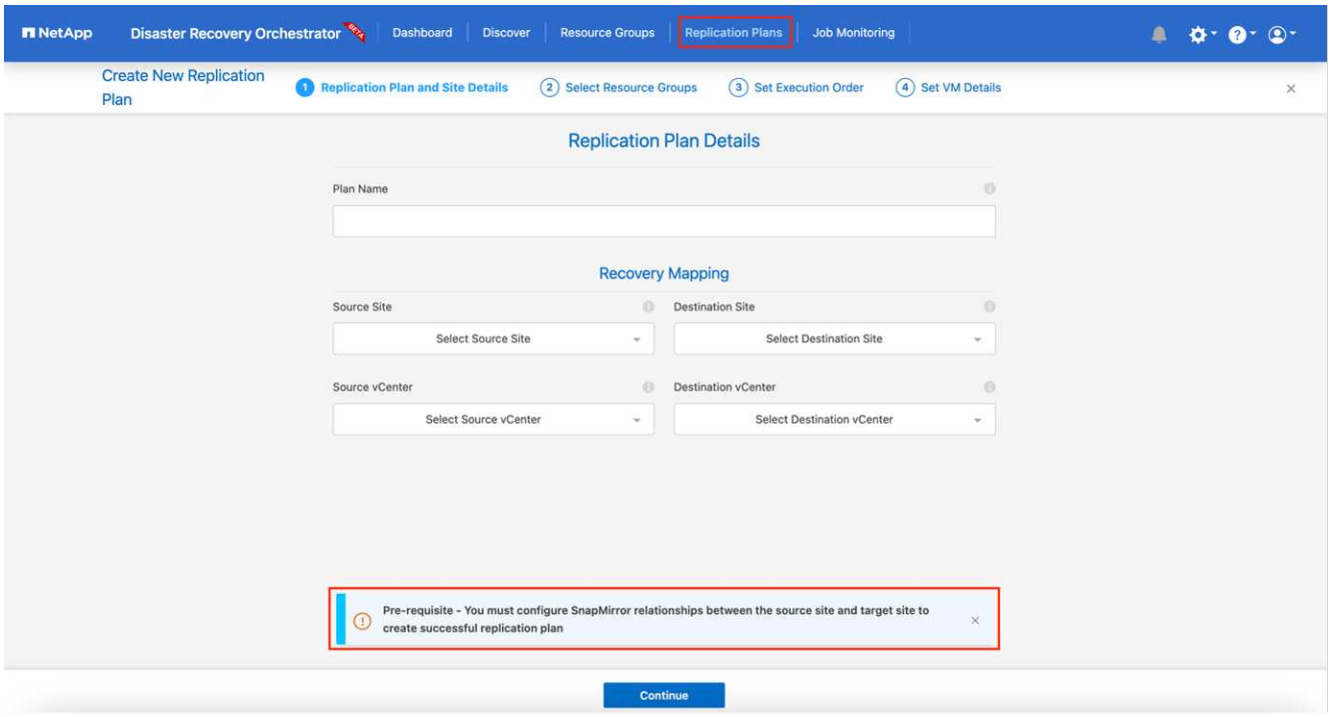
災害発生時にアプリケーションをリカバリするための計画が必要です。ドロップダウンからvCenterのソースプラットフォームとデスティネーションプラットフォームを選択し、このプランに含めるリソースグループと、アプリケーションのリストア方法と電源オン方法のグループを選択します（ドメインコントローラ、ティア1、ティア2など）。このような計画は、ブループリントとも呼ばれます。リカバリ・プランを定義するには'[レプリケーション・プラン]タブに移動し'[新しいレプリケーション・プラン]をクリックします

レプリケーションプランの作成を開始するには、次の手順を実行します。

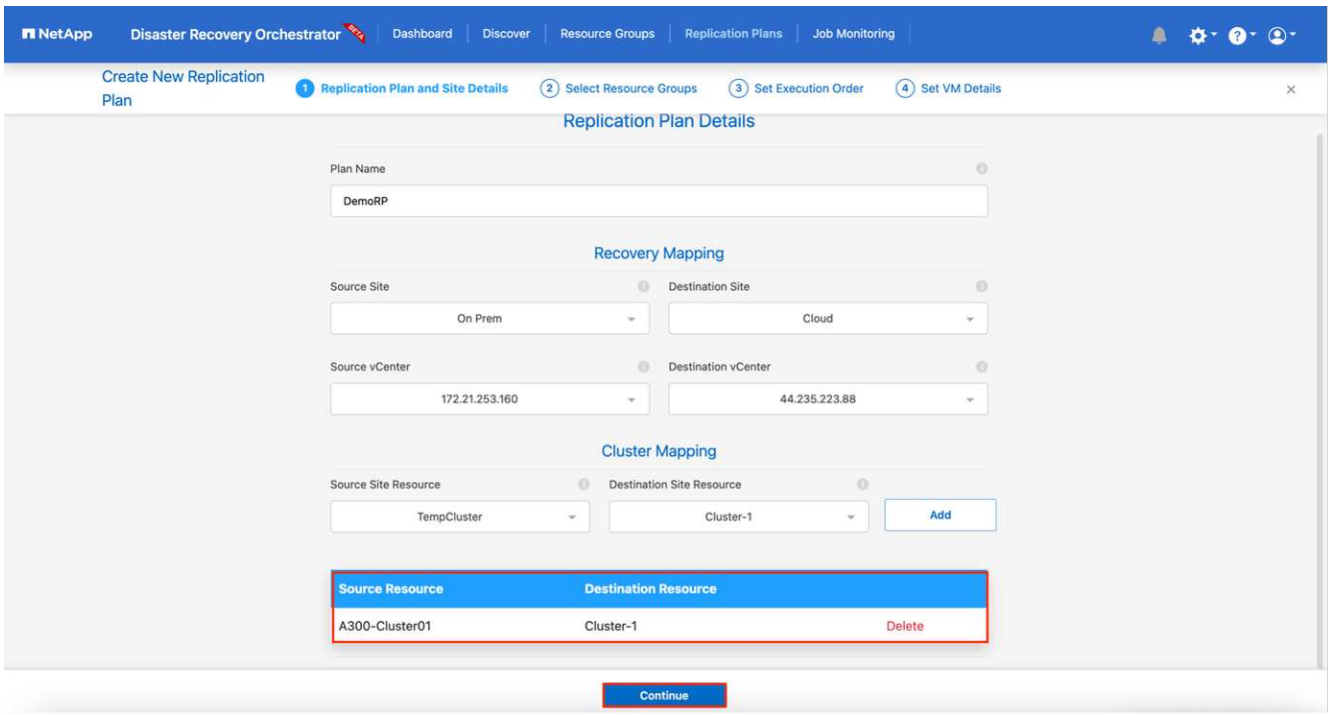
1. *レプリケーションプラン*にアクセスし、*新しいレプリケーションプランの作成*をクリックします。



2. [New Replication Plan]で、ソースサイト、関連するvCenter、デスティネーションサイト、および関連するvCenterを選択して、プランの名前を指定し、リカバリマッピングを追加します。

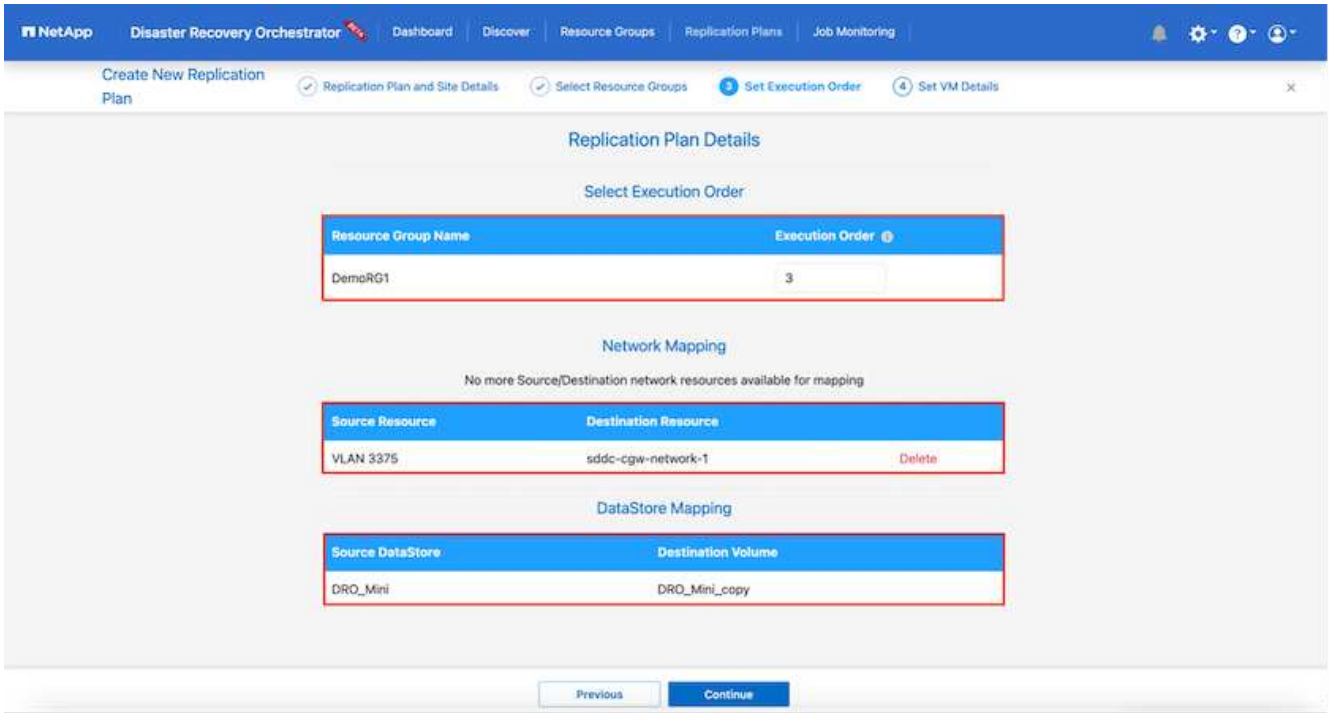


3. リカバリマッピングが完了したら、クラスタマッピングを選択します。

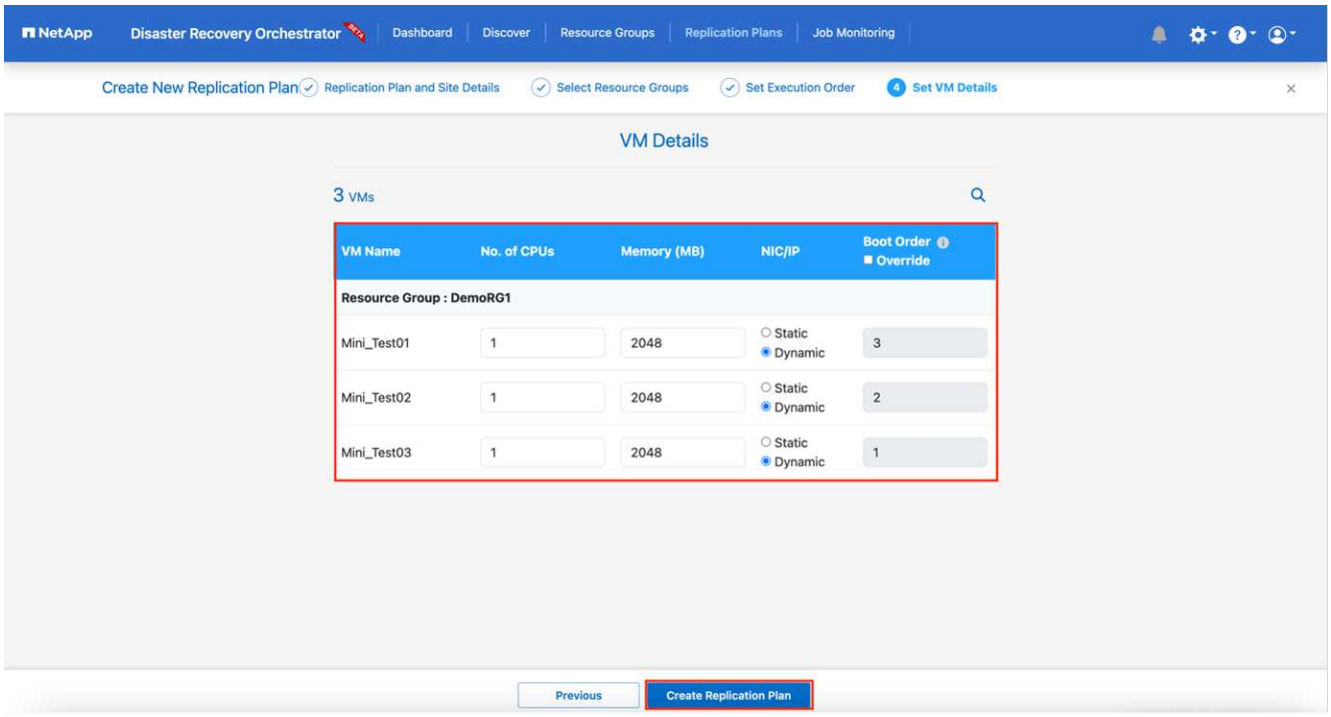


4. [リソースグループの詳細]を選択し、[*続行]をクリックします。
5. リソースグループの実行順序を設定します。このオプションを使用すると、複数のリソースグループが存在する場合の処理の順序を選択できます。
6. 完了したら、該当するセグメントへのネットワークマッピングを選択します。セグメントはVMC内でプロビジョニング済みである必要があるため、VMをマッピングする適切なセグメントを選択してください。
7. VMを選択すると、データストアマッピングが自動的に選択されます。

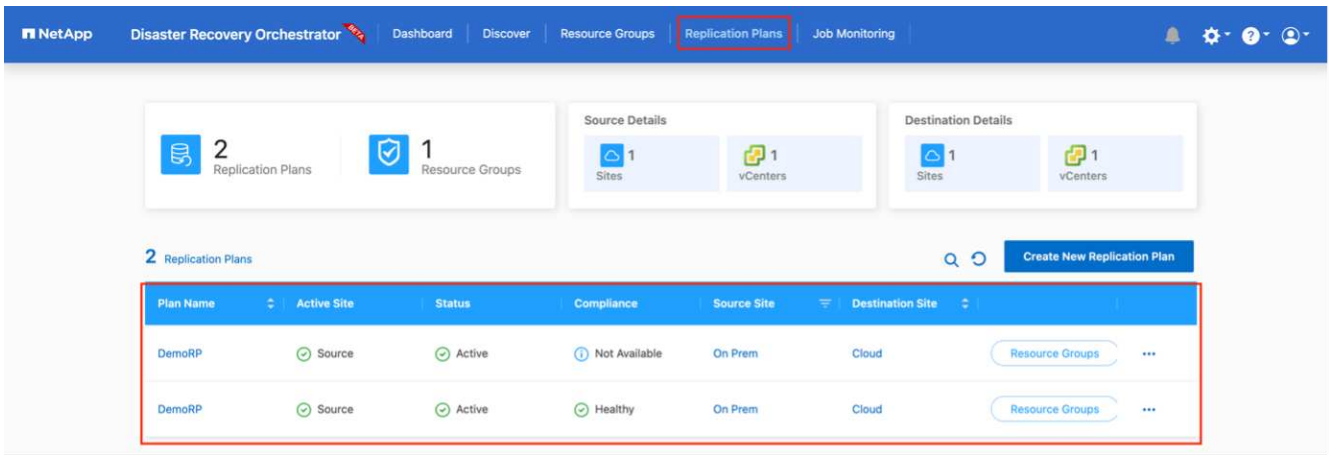
SnapMirrorはボリュームレベルです。したがって、すべてのVMがレプリケーションデスティネーションにレプリケートされます。必ずデータストアに含まれるすべてのVMを選択してください。選択しない場合は、レプリケーションプランの一部であるVMのみが処理されます。



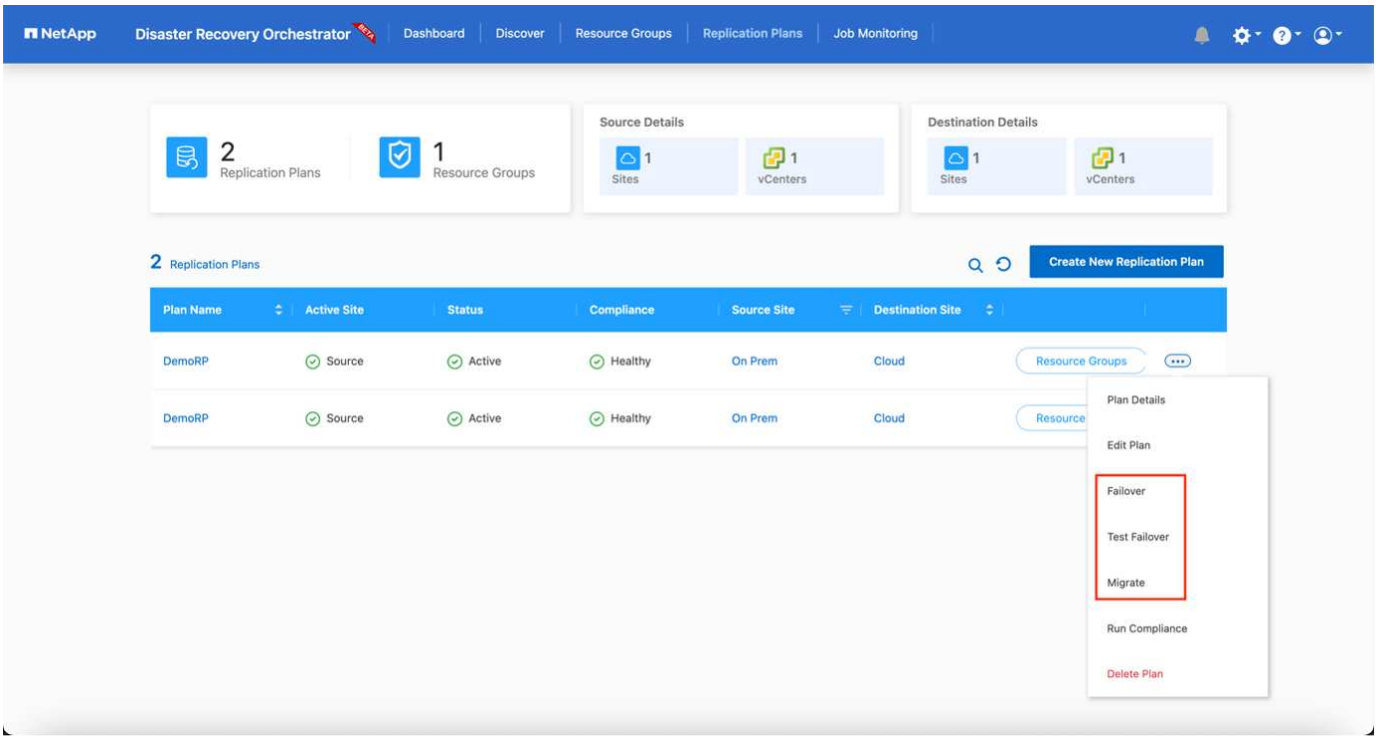
8. VMの詳細の下では、オプションでVMのCPUパラメータとRAMパラメータのサイズを変更できます。これは、大規模な環境を小規模なターゲットクラスタにリカバリする場合や、1対1の物理VMwareインフラをプロビジョニングしなくてもDRテストを実行する場合に非常に役立ちます。また、リソースグループ内の選択したすべてのVMのブート順序とブート遅延（秒）を変更することもできます。リソースグループのブート順序の選択時に選択したブート順序に変更が必要な場合は、追加のオプションを使用してブート順序を変更できます。デフォルトでは、リソースグループの選択時に選択したブート順序が使用されますが、この段階で変更を行うことができます。

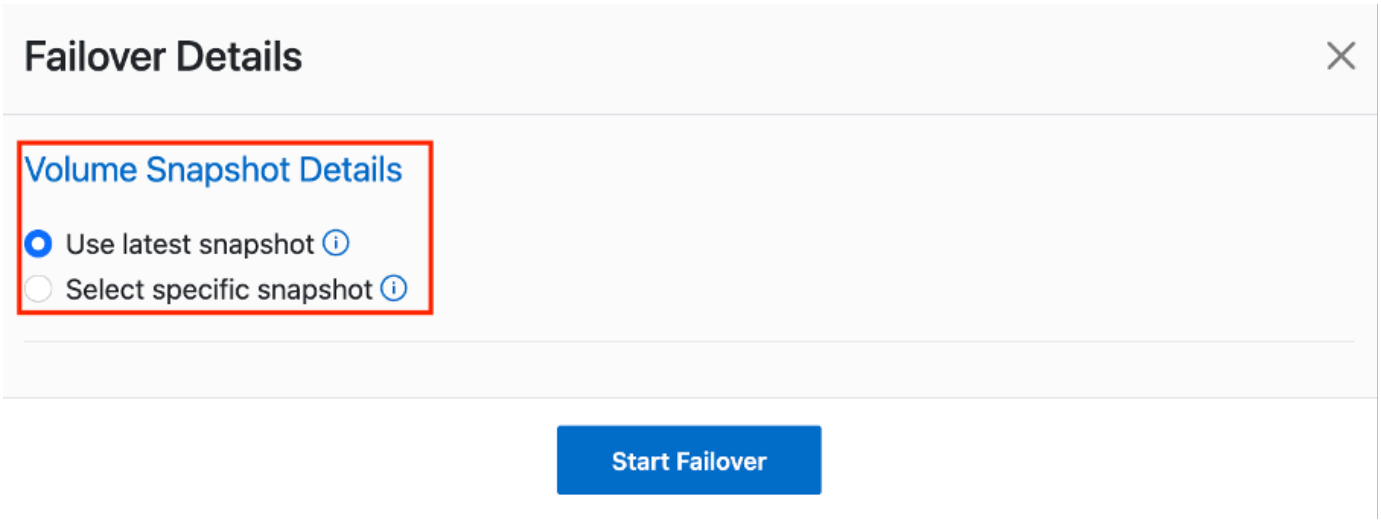


9. レプリケーションプランの作成*をクリックします。

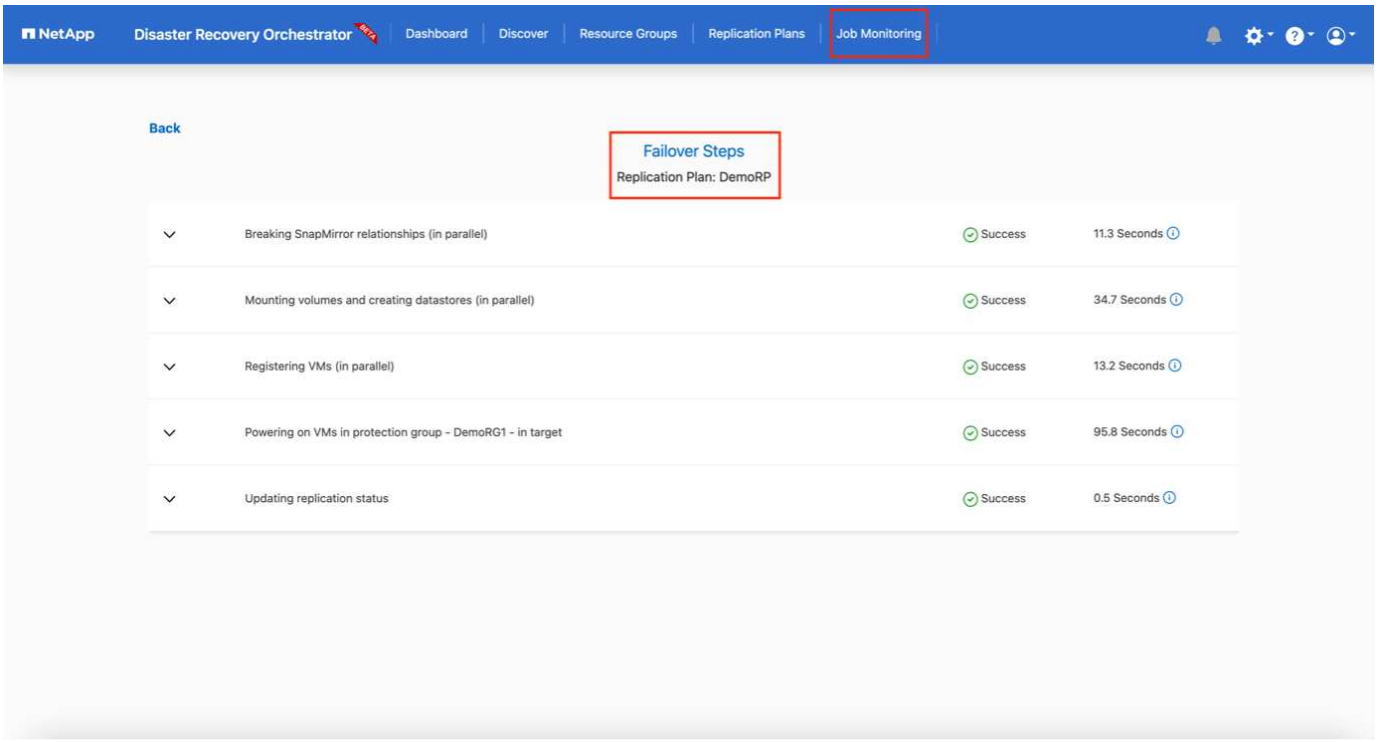


レプリケーションプランの作成後は、要件に応じて、フェイルオーバーオプション、テストフェイルオーバーオプション、または移行オプションを実行できます。フェイルオーバーおよびテストフェイルオーバーのオプションでは、最新のSnapMirror Snapshotコピーが使用されるほか、（SnapMirrorの保持ポリシーに基づいて）ポイントインタイムのSnapshotコピーから特定のSnapshotコピーを選択できます。ポイントインタイムオプションは、ランサムウェアなどの破損イベントに直面している場合に、最新のレプリカがすでに侵害されているか暗号化されていると非常に役立ちます。DROは、使用可能なすべてのポイントを時間単位で表示します。レプリケーションプランで指定された構成でフェイルオーバーまたはテストフェイルオーバーをトリガーするには、*フェイルオーバー*または*テストフェイルオーバー*をクリックします。

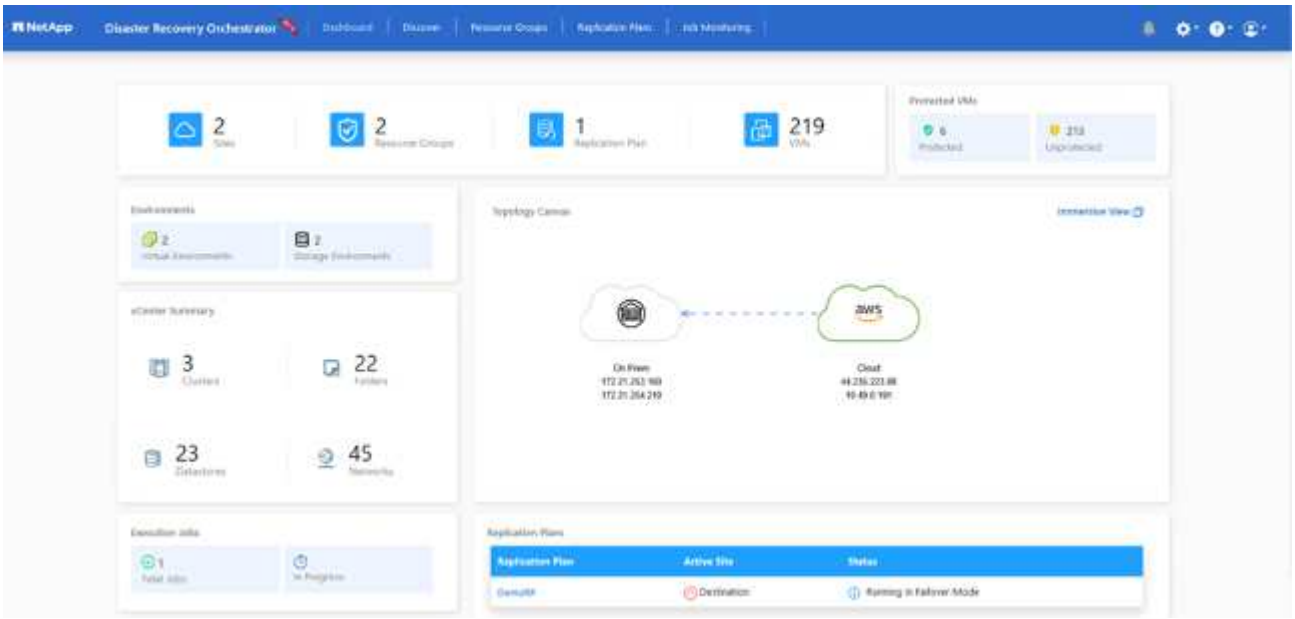




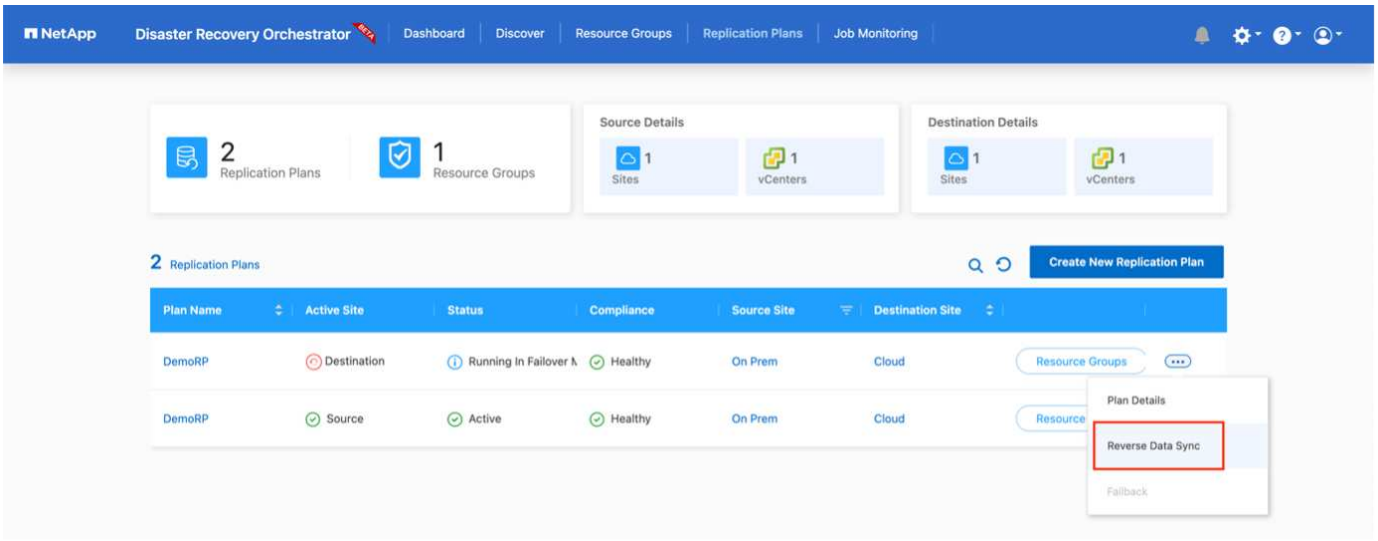
レプリケーションプランは、次のタスクメニューで監視できます。

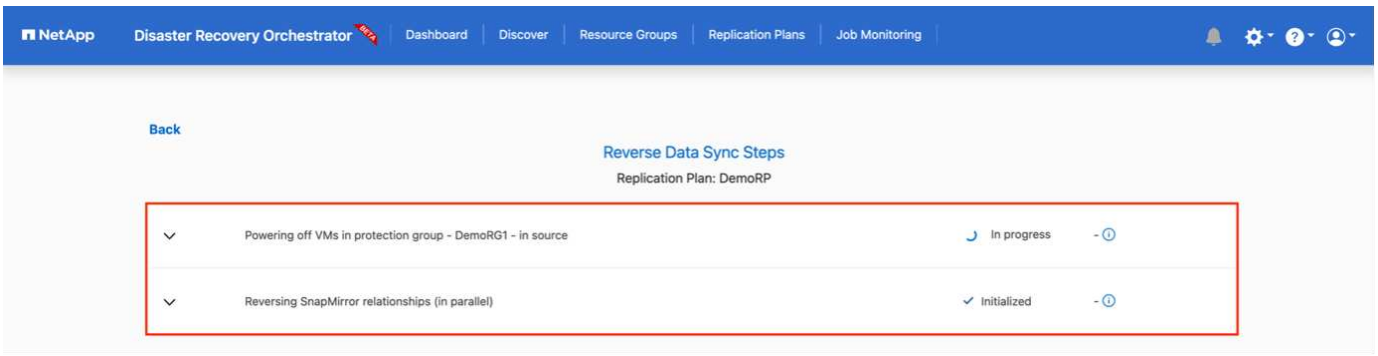


フェイルオーバーがトリガーされると、リカバリされた項目をVMC vCenter（VM、ネットワーク、データストア）で確認できます。デフォルトでは、VMはWorkloadフォルダにリカバリされます。

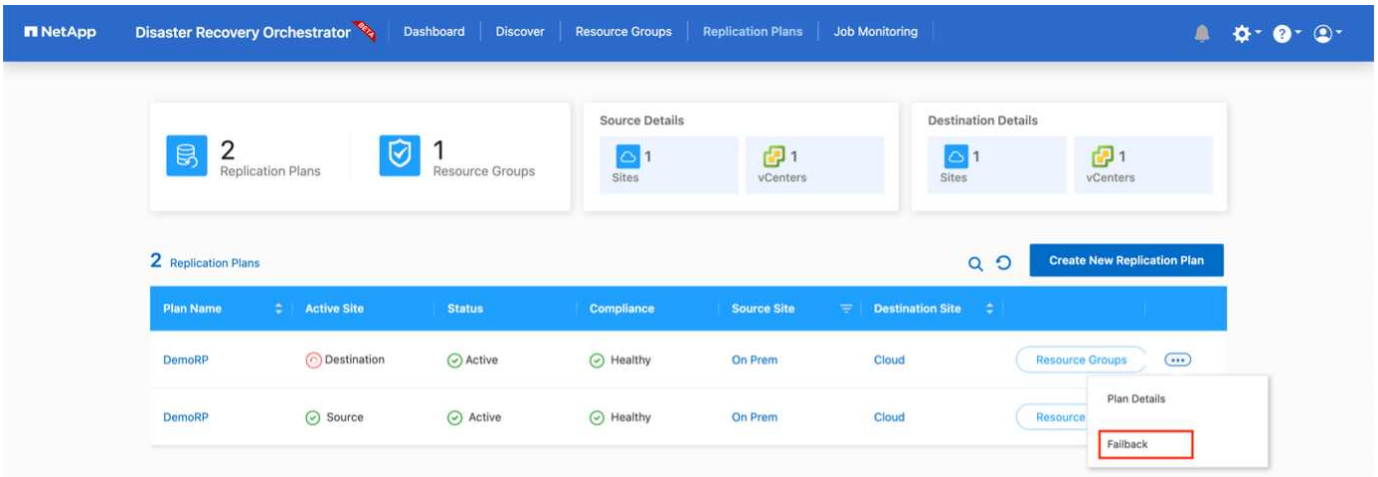


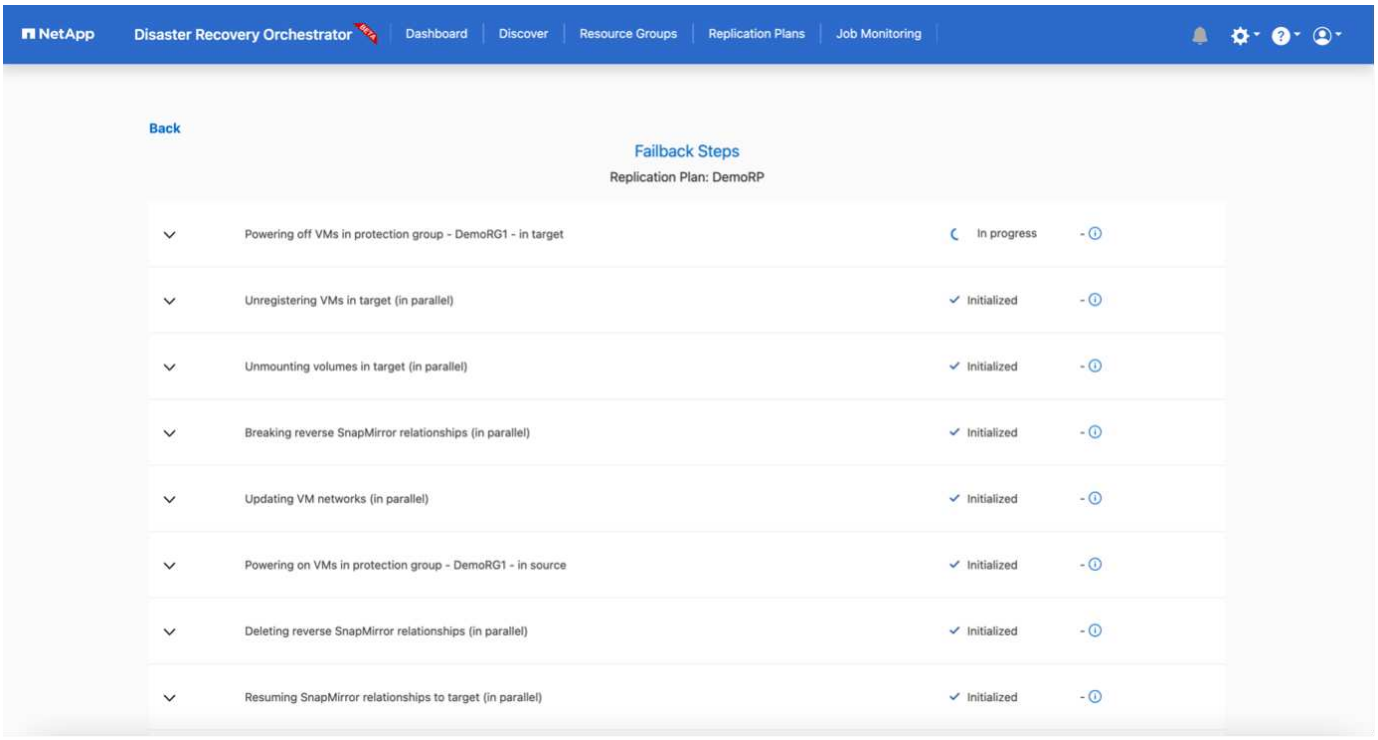
フェイルバックは、レプリケーションプランレベルで実行できます。テストフェイルオーバーでは、ティアダウンオプションを使用して変更をロールバックし、FlexClone関係を削除できます。フェイルオーバーに関連したフェイルバックは、2つのステップで行います。レプリケーションプランを選択し、*リバースデータ同期*を選択します。



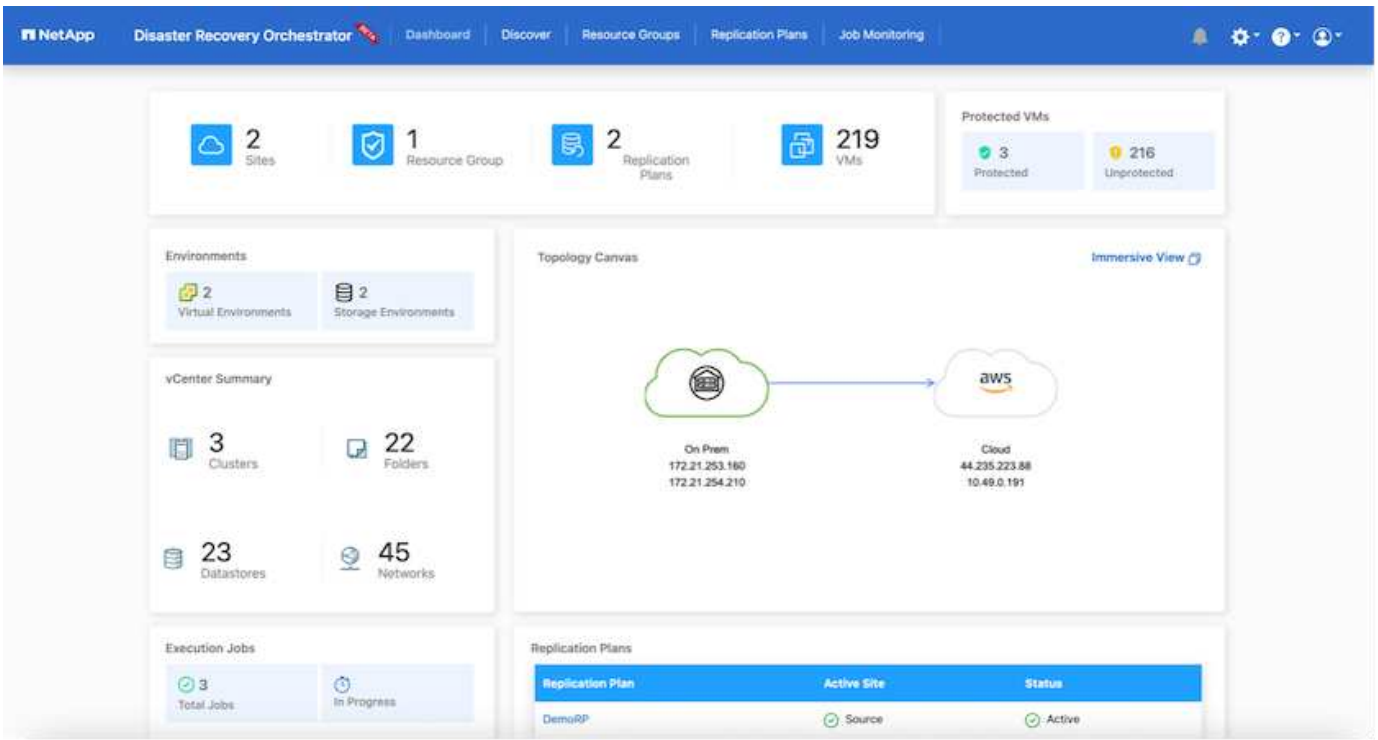


完了したら、フェイルバックを開始して元の本番サイトに戻すことができます。





NetApp BlueXPでは、該当するボリューム（読み書き可能ボリュームとしてVMCにマッピングされているボリューム）のレプリケーションの健常性が遮断されていることがわかります。テストフェイルオーバー中、DROはデスティネーションボリュームまたはレプリカボリュームをマッピングしません。代わりに、必要なSnapMirror（またはSnapshot）インスタンスのFlexCloneコピーを作成し、FlexCloneインスタンスを公開します。FlexCloneインスタンスは、ONTAP のFSX用に追加の物理容量を消費することはありません。このプロセスにより、DRのテストや優先度の異なるワークフローの実行中も、ボリュームが変更されず、レプリカジョブを続行できます。また'このプロセスにより'エラーが発生した場合や破損したデータがリカバリされた場合には'レプリカが破壊されるリスクを伴わずにリカバリをクリーンアップできます



ランサムウェアからのリカバリ

ランサムウェアからのリカバリは困難な作業です。具体的には、IT組織にとっては、安全な返品ポイントが特定され、復元されたワークロードを、睡眠中のマルウェアや脆弱なアプリケーションなどから再発生する攻撃から保護するために、ピンポイントを確立することは困難です。

DROは、利用可能な任意の時点からシステムを回復できるようにすることで、このような問題に対処します。また、機能的で分離されたネットワークにワークロードをリカバリして、南北トラフィックにさらされない場所でアプリケーションが機能し、相互に通信できるようにすることもできます。これにより、セキュリティチームはフォレンジックを実行する安全な場所を手に入れ、隠れているマルウェアや睡眠中のマルウェアが存在しないことを確認できます。

利点

- 効率性と耐障害性に優れたSnapMirrorレプリケーションの使用：
- Snapshotコピーの保持により、任意の時点までのリカバリが可能
- ストレージ、コンピューティング、ネットワーク、アプリケーションの検証から、数百から数千のVMをリカバリするのに必要なすべての手順を完全に自動化します。
- ONTAP FlexCloneテクノロジを使用したワークロードのリカバリ：レプリケートされたボリュームを変更しない方法を使用します。
  - ボリュームやSnapshotコピーのデータが破損するリスクを回避します。
  - DRテストのワークフロー中にレプリケーションが中断されるのを回避します
  - DRデータとクラウドコンピューティングリソースを組み合わせたDRデータの使用は、DR以外のワークフロー（DevTest、セキュリティテスト、パッチテスト、アップグレードテスト、修復テストなど）にも適しています。
- CPUとRAMの最適化により、小規模なコンピューティングクラスタへのリカバリが可能になり、クラウドコストを削減

Veeam Replicationと**FSx for ONTAP**を使用した**VMware Cloud on AWS**へのディザスタリカバリ

作成者：Niyaz Mohamed - NetAppソリューションエンジニアリング

概要

Amazon FSx for NetApp ONTAPとVMware Cloud on AWSの統合は、ネットアップのONTAPファイルシステム上に構築されたAWS管理の外部NFSデータストアで、SDDCのクラスタに接続できます。コンピューティングリソースとは別に拡張できる、柔軟性に優れたハイパフォーマンスな仮想ストレージインフラをお客様に提供します。

VMware Cloud on AWS SDDCをディザスタリカバリのターゲットとして使用することを検討しているお客様の場合、FSx for ONTAPデータストアを使用して、VMレプリケーション機能を提供する検証済みのサードパーティ製解決策を使用してオンプレミスからデータをレプリケートできます。FSx for ONTAPデータストアを追加することで、ストレージに対応するためだけに大量のESXiホストを使用してAWS SDDC上にVMwareクラウドを構築するよりも、コストを最適化できます。

また、このアプローチは、VMCのパイロットライトクラスタとFSx for ONTAPデータストアを使用してVMレプリカをホストするのにも役立ちます。レプリケーション計画を正常にフェイルオーバーすることで、VMware Cloud on AWSへの移行オプションとして同じプロセスを拡張することもできます。

問題点

本ドキュメントでは、FSx for ONTAPデータストアとVeeam Backup and Replicationを使用して、VMレプリケーション機能を使用してオンプレミスのVMware VMからVMware Cloud on AWSへのディザスタリカバリを設定する方法について説明します。

Veeam Backup & Replicationを使用すると、オンサイトとリモートのレプリケーションでディザスタリカバリ（DR）を実現できます。仮想マシンがレプリケートされると、Veeam Backup & Replicationは、ネイティブのVMware vSphere形式でターゲットのVMware Cloud on AWS SDDCクラスタにVMの正確なコピーを作成し、元のVMとの同期を維持します。

VMのコピーがすぐに開始できる状態にあるため、レプリケーションによって最適なRecovery Time Objective（RTO；目標復旧時間）値が得られます。 このレプリケーションメカニズムにより、災害発生時にVMware Cloud on AWS SDDCでワークロードを迅速に開始できます。Veeam Backup & Replicationソフトウェアは、WAN経由のレプリケーションや低速接続のトラフィック転送も最適化します。さらに、重複データブロック、ゼロデータブロック、スワップファイル、除外VMゲストOSファイルを除外し、レプリカトラフィックを圧縮します。

レプリケーションジョブがネットワーク帯域幅全体を消費しないようにするには、WANアクセラレータとネットワークスロットリングルールを設定します。Veeam Backup & Replicationのレプリケーションプロセスはジョブベースです。つまり、レプリケーションはレプリケーションジョブを設定して実行されます。災害が発生した場合は、レプリカコピーにフェイルオーバーすることで、フェイルオーバーをトリガーしてVMをリカバリできます。

フェイルオーバーが実行されると、レプリケートされたVMが元のVMの役割を引き継ぎます。フェイルオーバーは、レプリカの最新の状態、または既知の任意のリストアポイントに対して実行できます。これにより、必要に応じてランサムウェアからのリカバリや個別のテストが可能Veeam Backup & Replicationでは、フェイルオーバーとフェイルバックは一時的な中間ステップであり、あとで完了する必要があります。Veeam Backup & Replicationには、さまざまなディザスタリカバリシナリオに対応するためのオプションが複数用意されています。

[Veeam ReplicationとFSx ONTAP for VMCを使用したDRシナリオの図]

解決策 の導入

手順の概要

1. Veeam Backup & Replicationソフトウェアは、適切なネットワーク接続を備えたオンプレミス環境で実行されています。
2. VMware Cloud on AWSの設定：VMware Cloud Tech Zoneに関する記事を参照 "VMware Cloud on AWS integration with Amazon FSx for NetApp ONTAP導入ガイド" 導入するには、VMware Cloud on AWS SDDCとFSx for ONTAPをNFSデータストアとして設定します。（最小限の構成でセットアップされたパイロットライト環境は、DR目的で使用できます。インシデントが発生した場合、VMはこのクラスタにフェイルオーバーし、ノードを追加できます）。
3. Veeam Backup and Replicationを使用してVMレプリカを作成するためのレプリケーションジョブを設定します。
4. フェイルオーバープランを作成し、フェイルオーバーを実行
5. 災害が完了し、プライマリサイトが稼働したら、本番環境のVMにスイッチバックします。

VMCおよび**FSx for ONTAP**データストアへの**Veeam VM**レプリケーションの前提条件

1. Veeam Backup & ReplicationのバックアップVMがソースvCenterと、AWS SDDCクラスタ上のターゲットVMwareクラウドに接続されていることを確認します。
2. バックアップサーバは、短縮名を解決し、ソースvCenterとターゲットvCenterに接続できる必要があります。
3. ターゲットのFSx for ONTAPデータストアには、レプリケートされたVMのVMDKを格納できるだけの十分な空きスペースが必要

追加情報については、「考慮事項と制限事項」を参照してください。 "こちらをご覧ください"。

展開の詳細

ステップ**1**：**VM**のレプリケート

Veeam Backup & ReplicationはVMware vSphereスナップショット機能を活用し、レプリケーション中にVeeam Backup & ReplicationはVMware vSphereにVMスナップショットの作成を要求します。VMスナップショットは、仮想ディスク、システムの状態、構成などを含むVMのポイントインタイムコピーです。Veeam Backup & Replicationでは、Snapshotをレプリケーションのデータソースとして使用します。

VMをレプリケートするには、次の手順を実行します。

1. Veeam Backup & Replicationコンソールを開きます。
2. [Home]ビューで、[Replication Job]>[Virtual machine]>[VMware vSphere]を選択します。
3. ジョブ名を指定し、適切な詳細制御チェックボックスを選択します。次へをクリックします。
   - オンプレミスとAWS間の接続で帯域幅が制限されている場合は、[Replica seeding]チェックボックスをオンにします。
   - VMware Cloud on AWS SDDC上のセグメントがオンプレミスサイトネットワークのセグメントと一致しない場合は、[Network remapping（for AWS VMC sites with different networks）]チェックボックスをオンにします。
   - オンプレミスの本番用サイトのIPアドレス指定方式がAWS VMCサイトのIPアドレス指定方式と異なる場合は、Replica Re-IP（for DR sites with different IP addressing scheme）チェックボックスを選択します。

     [DR Veeam FSxイメージ2] | *dr-veeam-fsx-image2.png*
4. [仮想マシン]ステップで、VMware Cloud on AWS SDDCに接続されたFSx for ONTAPデータストアにレプリケートする必要のあるVMを選択します。仮想マシンをVSANに配置して、使用可能なVSANデータストアの容量をいっぱいにすることができます。パイロットライトクラスタでは、3ノードクラスタの使用可能容量が制限されます。残りのデータはFSx for ONTAPデータストアにレプリケートできます。をクリックし、[オブジェクトの追加]ウィンドウで必要な**VM**または**VM**コンテナを選択して[追加]*をクリックします。「 * 次へ * 」をクリックします。

   [DR Veeam FSxイメージ3] | *dr-veeam-fsx-image3.png*
5. その後、デスティネーションをVMware Cloud on AWS SDDCクラスター/ホストとして選択し、VMレプリカ用の適切なリソースプール、VMフォルダ、FSx for ONTAPデータストアを選択します。次に*[次へ]*をクリックします。

   [DR Veeam FSxイメージ4] | *dr-veeam-fsx-image4.png*
6. 次の手順では、必要に応じてソースとデスティネーションの仮想ネットワーク間のマッピングを作成します。

   [DR Veeam FSxイメージ5] | *dr-veeam-fsx-image5.png*
7. [ジョブ設定]ステップで、VMレプリカのメタデータや保持ポリシーなどを格納するバックアップリポジトリを指定します。
8. Data Transfer（データ転送）ステップで* Source（ソース）および Target（ターゲット）プロキシサーバーを更新し、 Automatic（自動）選択（デフォルト）のままにして Direct オプションを選択したままにして Next（次へ）*をクリックします。

9. [Guest Processing]ステップで、必要に応じて[Enable application-aware processing]オプションを選択します。「 * 次へ * 」をクリックします。

   [DR Veeam FSxイメージ6] | *dr-veeam-fsx-image6.png*

10. レプリケーションジョブを定期的に実行するレプリケーションスケジュールを選択します。
11. ウィザードの* Summary ステップで、レプリケーションジョブの詳細を確認します。ウィザードを終了した直後にジョブを開始するには、[完了]をクリックしたときにジョブを実行する*チェックボックスをオンにします。オンにしない場合は、チェックボックスをオフのままにします。次に、*[完了]*をクリックしてウィザードを閉じます。

    [DR Veeam FSxイメージ7] | *dr-veeam-fsx-image7.png*

レプリケーションジョブが開始されると、指定されたサフィックスのVMがデスティネーションVMC SDDCクラスタ/ホストに取り込まれます。

[DR Veeam FSxイメージ8] | *dr-veeam-fsx-image8.png*

追加情報によるVeeamレプリケーションについては、を参照してください。 "レプリケーションの仕組み"。

手順**2**：フェイルオーバープランを作成する

最初のレプリケーションまたはシードが完了したら、フェイルオーバープランを作成します。フェイルオーバープランは、依存するVMのフェイルオーバーを1つずつ、またはグループとして自動的に実行するのに役立ちます。フェイルオーバープランは、ブート遅延を含むVMの処理順序の青写真です。フェイルオーバープランは、重要な依存VMがすでに実行されていることを確認するのにも役立ちます。

プランを作成するには、レプリカという新しいサブセクションに移動し、フェイルオーバープランを選択します。適切なVMを選択します。Veeam Backup & Replicationは、この時点に最も近いリストアポイントを検索し、それらを使用してVMレプリカを開始します。

フェイルオーバープランを追加できるのは、初期レプリケーションが完了し、VMレプリカがReady状態になってからです。

フェイルオーバープランの実行時に同時に起動できるVMの最大数は10です。

フェイルオーバープロセス中は、ソースVMの電源はオフになりません。

フェイルオーバープラン*を作成するには、次の手順を実行します。

1. [ホーム]ビューで、*[フェイルオーバープラン]>[VMware vSphere]*を選択します。
2. 次に、プランの名前と概要を入力します。必要に応じて、フェイルオーバー前およびフェイルオーバー後のスクリプトを追加できます。たとえば、スクリプトを実行して、レプリケートされたVMを起動する前にVMをシャットダウンします。

   [DR Veeam FSxイメージ9] | *dr-veeam-fsx-image9.png*

3. VMを計画に追加し、VMのブート順序とブート遅延を変更して、アプリケーションの依存関係を満たすようにします。

   [DR Veeam FSxイメージ10] | *dr-veeam-fsx-image10.png*

レプリケーションジョブを作成するための追加情報については、を参照してください。 "レプリケーションジョブの作成"。

手順**3**：フェイルオーバープランを実行する

フェイルオーバー時には、本番サイトのソースVMがディザスタリカバリサイトのレプリカにスイッチオーバーされます。フェイルオーバープロセスの一環として、Veeam Backup & ReplicationはVMレプリカを必要なリストアポイントにリストアし、すべてのI/Oアクティビティをソース VMからそのレプリカに移動します。レプリカは、災害発生時だけでなく、DRドリルのシミュレーションにも使用できます。フェイルオーバーのシミュレーション中は、ソースVMは引き続き実行されます。必要なテストがすべて完了したら、フェイルオーバーを元に戻して通常の運用に戻すことができます。

DRドリル中にIPの競合を回避するために、ネットワークのセグメント化が行われていることを確認します。

フェイルオーバープランを開始するには、* Failover Plans タブをクリックし、フェイルオーバープランを右クリックします。「 *** Start** （開始）」を選択しますこれにより、**VM**レプリカの最新のリストアポイントを使用してフェイルオーバーが実行されます。**VM**レプリカの特定のリストアポイントにフェイルオーバーするには、 Start to *を選択します。

[DR Veeam FSxイメージ11] | *dr-veeam-fsx-image11.png*

[DR Veeam FSxイメージ12] | *dr-veeam-fsx-image12.png*

VMレプリカの状態がReadyからFailoverに変わり、VMはデスティネーションのVMware Cloud on AWS SDDCクラスタ/ホストで開始されます。

[DR Veeam FSxイメージ13] | *dr-veeam-fsx-image13.png*

フェイルオーバーが完了すると、VMのステータスが「Failover」に変わります。

[DR Veeam FSxイメージ14] | *dr-veeam-fsx-image14.png*

Veeam Backup & Replicationは、レプリカがReady状態に戻るまで、ソースVMのすべてのレプリケーションアクティビティを停止します。

フェイルオーバープランの詳細については、を参照してください。 "フェイルオーバープラン"。

手順4：本番サイトへのフェイルバック

フェイルオーバープランの実行中は中間ステップとみなされ、要件に基づいて確定する必要があります。オプションには次のものがあります。

- 本番環境へのフェイルバック：元のVMに切り替えて、VMレプリカの実行中に発生したすべての変更を元のVMに転送します。

> フェイルバックを実行すると、変更は転送されますが、パブリッシュされません。[Commit failback]*（元のVMが期待どおりに動作することが確認されたら）または[Undo failback]*を選択して、元のVMが期待どおりに動作しない場合はVMレプリカに戻ります。

- フェイルオーバーを元に戻す-元のVMに切り替えて、VMレプリカの実行中に行った変更をすべて破棄します。
- 永続的フェイルオーバー-元のVMからVMレプリカに永続的に切り替え、このレプリカを元のVMとして使用します。

このデモでは、本番環境へのフェイルバックを選択しました。ウィザードの[Destination]ステップで[Failback to the original VM]が選択され、[Power on VM after restoring]チェックボックスが有効になっている。

[DR Veeam FSxイメージ15] | *dr-veeam-fsx-image15.png*

[DR Veeam FSxイメージ16] | *dr-veeam-fsx-image16.png*

フェイルバックコミットは、フェイルバック操作を完了する方法の1つです。フェイルバックがコミットされると、フェイルバックされたVM（本番VM）に送信された変更が想定どおりに機能していることが確認されます。コミット処理が完了すると、Veeam Backup & Replicationは本番用VMのレプリケーションアクティビティを再開します。

フェイルバックプロセスの詳細については、次のVeeamのドキュメントを参照してください：["レプリケーションのフェイルオーバーとフェイルバック"]。

[DR Veeam FSxイメージ17] | *dr-veeam-fsx-image17.png*

[DR Veeam FSxイメージ18] | *dr-veeam-fsx-image18.png*

本番環境へのフェイルバックが成功すると、VMはすべて元の本番サイトにリストアされます。

[DR Veeam FSxイメージ19] | *dr-veeam-fsx-image19.png*

まとめ

FSx for ONTAPデータストア機能を使用すると、Veeamやその他の検証済みサードパーティ製ツールを使用して、VMのレプリカコピーに対応するためだけにクラスタ内の多数のホストを立ち上げることなく、パイロットライトクラスタを使用して低コストのDR解決策を提供できます。これにより、カスタマイズされたディザスタリカバリ計画を処理する強力な解決策が提供されます。また、既存のバックアップ製品を社内で再利用してDRのニーズを満たすことができるため、オンプレミスのDRデータセンターを終了することで、クラウドベースのディザスタリカバリを実現できます。フェイルオーバーは、計画的フェイルオーバーまたはフェイルオーバーとして実行でき、災害発生時にボタンをクリックするだけでDRサイトをアクティブ化できます。

このプロセスの詳細については、詳細なウォークスルービデオをご覧ください。

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a

AWS / VMCでのワークロードの移行

TR-4942：『Migrate workloads to FSX ONTAP datastore using VMware HCX』

執筆者：NetApp Solutions Engineering

概要：**VMware HCX、FSX ONTAP** 補足データストア、および**VMware Cloud**を使用した仮想マシンの移行

Amazon Web Services（AWS）上のVMware Cloud（VMC）の一般的なユースケースであり、Amazon FSX for NetApp ONTAP 上の追加のNFSデータストアは、VMwareワークロードの移行です。VMware HCXは、オンプレミスの仮想マシン（VM）とそのデータを、VMwareがサポートする任意のデータストア上で実行して、FSX for ONTAP の補足的なNFSデータストアを含むVMCデータストアに移動するための、さまざまな移行方法を推奨します。

VMware HCXは、主に、クラウド間でのワークロードの移行、ワークロードの再バランシング、ビジネス継続性を簡素化するように設計されたモビリティプラットフォームです。VMware Cloud on AWSに含まれており、ワークロードを移行して、ディザスタリカバリ（DR）処理に使用するためのさまざまな方法が用意されています。

このドキュメントでは、VMware HCXの導入と構成に関するステップバイステップ形式のガイダンスを提供します。これには、VMware HCXのすべての主要コンポーネント、オンプレミス、クラウドデータセンター側などが含まれ、さまざまなVM移行メカニズムが可能になります。

詳細については、を参照してください "HCXの導入の概要" および "チェックリストB-HCXとVMware CloudをAWS SDDCデスティネーション環境にインストールします"。

手順の概要

VMware HCXのインストールと構成の手順の概要を次に示します。

1. VMwareクラウド サービス コンソールを使用して、VMC Software-Defined Data Center（SDDC）のHCXをアクティブにします。
2. HCX Connector OVAインストーラをオンプレミスのvCenter Serverにダウンロードして導入します。
3. ライセンスキーを使用してHCXをアクティブにします。
4. オンプレミスのVMware HCX ConnectorとVMC HCX Cloud Managerをペアリングします。
5. ネットワークプロファイル、コンピューティングプロファイル、およびサービスメッシュを設定します。
6. （任意）ネットワーク拡張を実行してネットワークを拡張し、再IP化を回避します。
7. アプライアンスのステータスを検証し、移行が可能であることを確認します。
8. VMワークロードを移行する。

前提条件

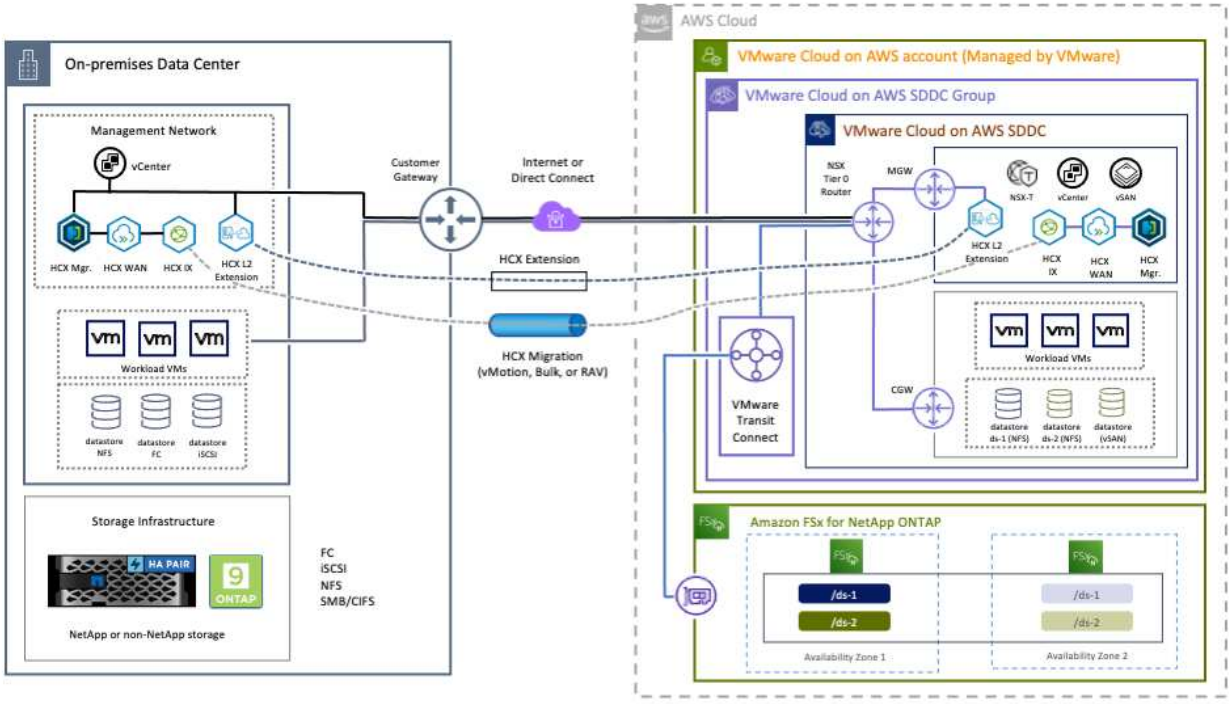
作業を開始する前に、次の前提条件が満たされていることを確認してください。詳細については、を参照してください "HCXインストールの準備中"。接続性を含む前提条件を満たした後、VMCのVMware HCXコンソールからライセンスキーを生成して、HCXを構成してアクティブ化します。HCXがアクティブ化されると、vCenter Plug-inが展開され、管理にvCenterコンソールを使用してアクセスできるようになります。

HCXのアクティベーションと展開を行う前に、次のインストール手順を完了する必要があります。

1. 既存のVMC SDDCを使用するか、次の手順で新しいSDDCを作成します "ネットアップのリンク" またはこれ "VMwareへのリンク"。
2. オンプレミスのvCenter環境からVMC SDDCへのネットワークパスで、vMotionを使用したVMの移行がサポートされている必要があります。
3. 必要なを確認します "ファイアウォールルールとポート" オンプレミスのvCenter ServerとSDDC vCenter間のvMotionトラフィックに許可されます。
4. ONTAP NFSボリュームのFSXは、VMC SDDCに補助的なデータストアとしてマウントする必要があります。 NFSデータストアを適切なクラスタに接続するには、以下の手順を実行します "ネットアップのリンク" またはこれ "VMwareへのリンク"。

テスト目的では、この検証に使用したオンプレミスのラボ環境をサイト間VPNを介してAWS VPCに接続しました。これにより、オンプレミスでAWSに接続し、さらに外部の中継ゲートウェイ経由でVMware クラウドSDDCに接続できるようになりました。HCx移行およびネットワーク拡張トラフィックは、オンプレミスとVMwareクラウドのデスティネーションSDDC間でインターネットを介して送信されます。このアーキテクチャは、Direct Connectプライベート仮想インターフェイスを使用するように変更できます。

次の図は、アーキテクチャの概要を示しています。



解決策 の導入

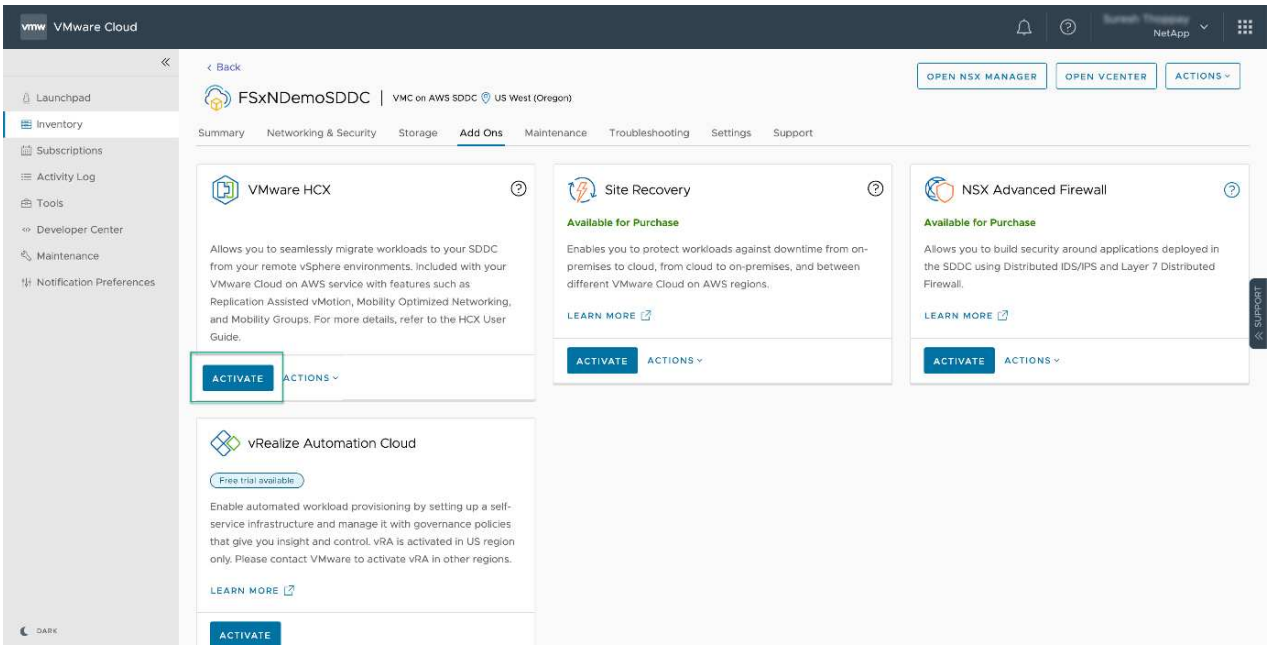
一連の手順に従って、この解決策 の導入を完了します。

手順**1**：アドオンオプションを使用して**VMC SDDC**経由で**HCX**をアクティブにします

インストールを実行するには、次の手順を実行します。

1. でVMCコンソールにログインします "vmc.vmware.com" Inventoryにアクセスします。
2. 適切なSDDCを選択し、アドオンにアクセスするには、[SDDCで詳細を表示]をクリックして、[Add ONS]タブを選択します。
3. Activate for VMware HCXをクリックします。

   この手順の完了には最大25分かかります。

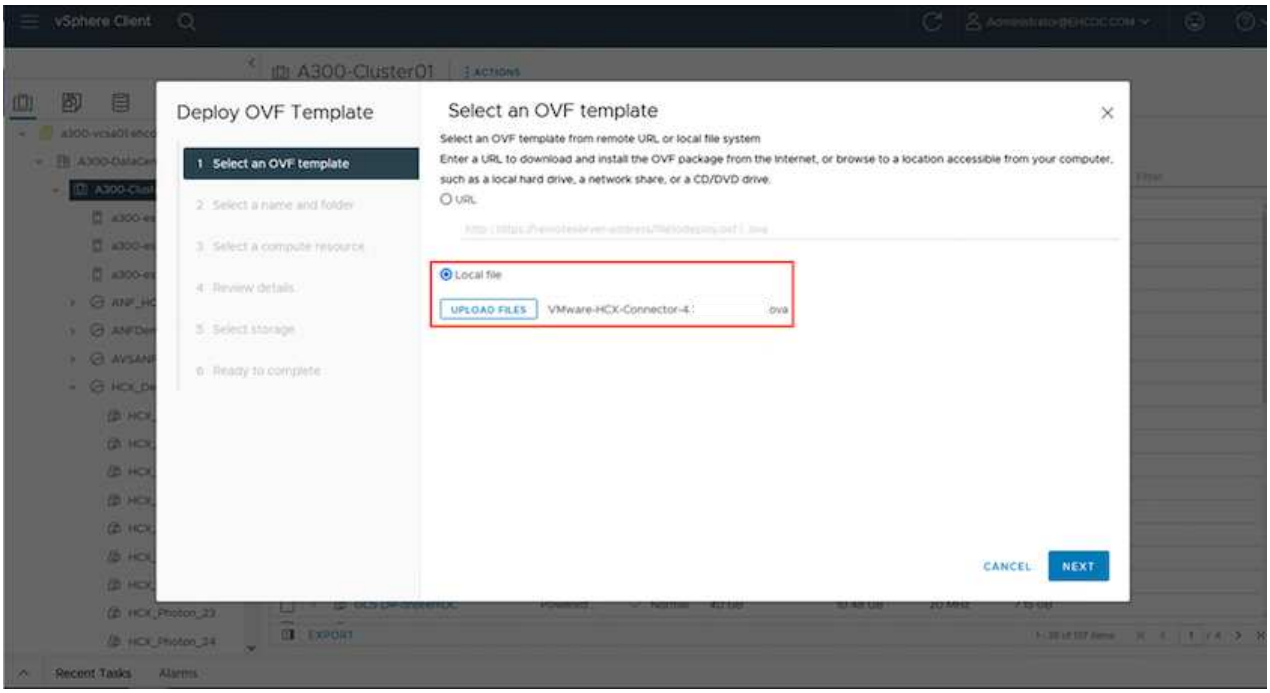


4. 導入が完了したら、HCX Managerとそれに関連するプラグインがvCenterコンソールで使用可能であることを確認して、導入を検証します。
5. 適切な管理ゲートウェイファイアウォールを作成して、HCX Cloud Managerへのアクセスに必要なポートを開きます。HCX Cloud ManagerはHCX操作に対応しています。

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

オンプレミスコネクタがVMCのHCXマネージャと通信するためには、適切なファイアウォールポートがオンプレミス環境で開いていることを確認します。

1. VMCコンソールからHCXダッシュボードに移動し、管理に移動して、システム更新タブを選択します。HCX Connector OVAイメージのRequest a Download Linkをクリックします。
2. HCXコネクタをダウンロードした状態で、OVAをオンプレミスのvCenter Serverに導入します。vSphere Clusterを右クリックし、Deploy OVF Templateオプションを選択します。

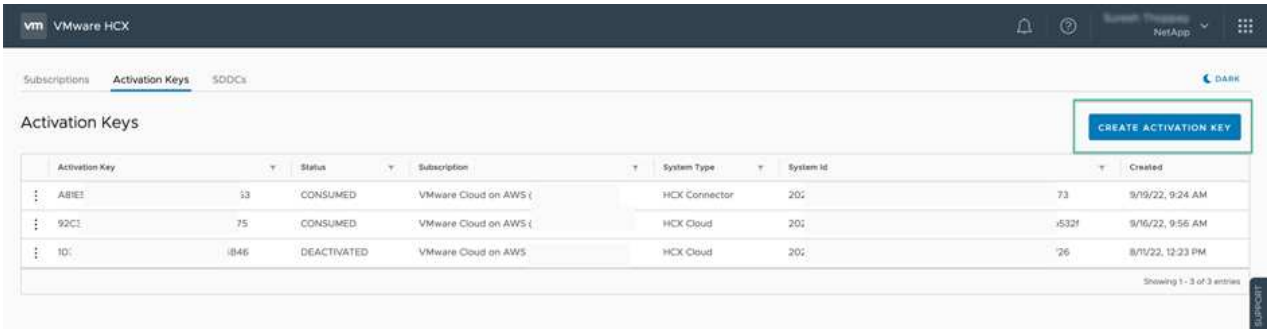


3. Deploy OVF Templateウィザードで必要な情報を入力し、Nextをクリックしてから Finishをクリックして、VMware HCX Connector OVAを導入します。
4. 仮想アプライアンスの電源を手動でオンにします。詳しい手順については、を参照してください "VMware HCXユーザーガイド"。

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

VMware HCX Connector OVAをオンプレミスに導入してアプライアンスを起動したら、次の手順を実行してHCX Connectorをアクティブにします。VMCのVMware HCXコンソールからライセンスキーを生成し、VMware HCX Connectorのセットアップ中にライセンスを入力します。

1. VMware Cloud Consoleで、Inventory（インベントリ）に移動し、SDDCを選択してView Details（詳細の表示）をクリックします。アドオンタブのVMware HCXタイルで、HCXを開くをクリックします。
2. Activation Keysタブで、Create Activation Keyをクリックします。システムタイプをHCXコネクタとして選択し、確認をクリックしてキーを生成します。アクティベーションキーをコピーします。



オンプレミスに配置されたHCXコネクタごとに、個別のキーが必要です。

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

OVAの導入時に定義されたパスワードを使用します。

4. [ライセンス交付（Licensing）]セクションで、手順2からコピーしたアクティベーションキーを入力し、[有効化（Activate）]をクリックします。

有効化を正常に完了するには、オンプレミスHCXコネクタにインターネットアクセスが必要です。

5. データセンターの場所で、VMware HCX Managerをオンプレミスにインストールする場所を指定します。Continue をクリックします。 .
6. [システム名]で名前を更新し、[続行]をクリックします。
7. [はい]を選択してから、[続行]
8. [vCenterの接続]で、IPアドレスまたは完全修飾ドメイン名（FQDN）とvCenter Serverの資格情報を入力し、[続行]をクリックします。

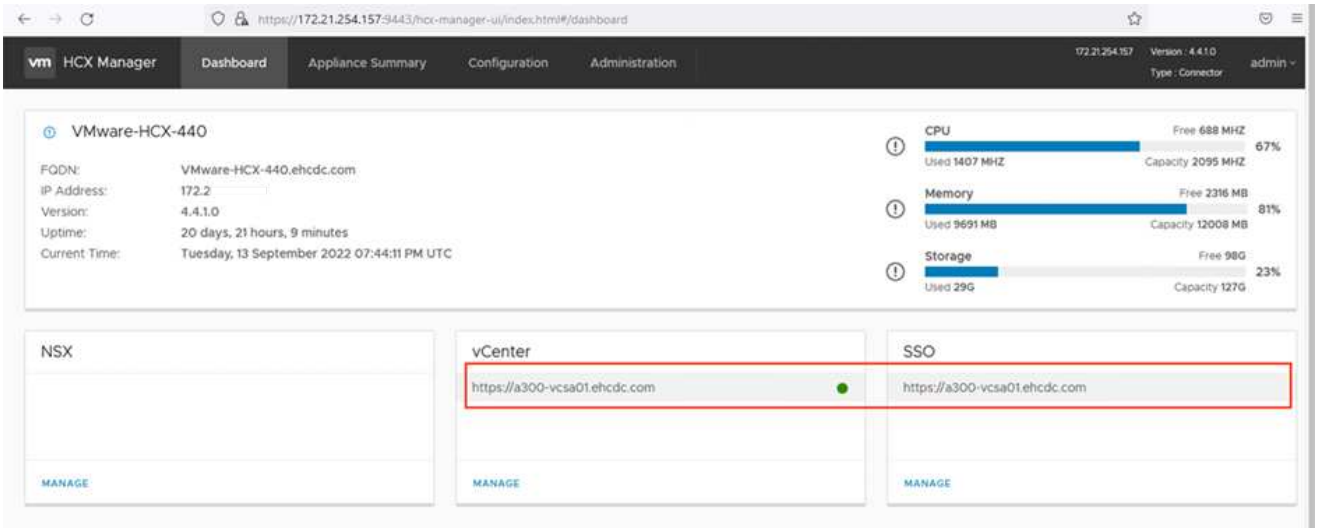
あとで通信の問題が発生しないようにFQDNを使用してください。

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

vCenter ServerのIPアドレスまたはFQDNを入力します。

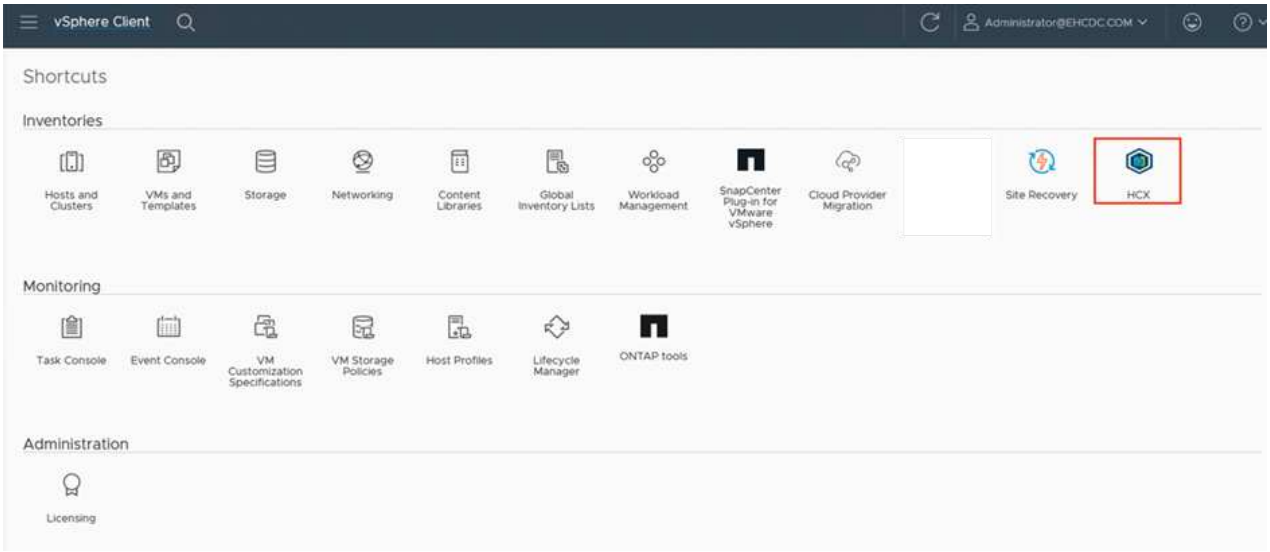
10. 情報が正しく入力されていることを確認し、[再起動]をクリックします。
11. 完了すると、vCenter Serverは緑で表示されます。vCenter ServerとSSOの両方で、前のページと同じ設定パラメータを指定する必要があります。

この処理には10~20分かかります。また、プラグインをvCenter Serverに追加することもできます。

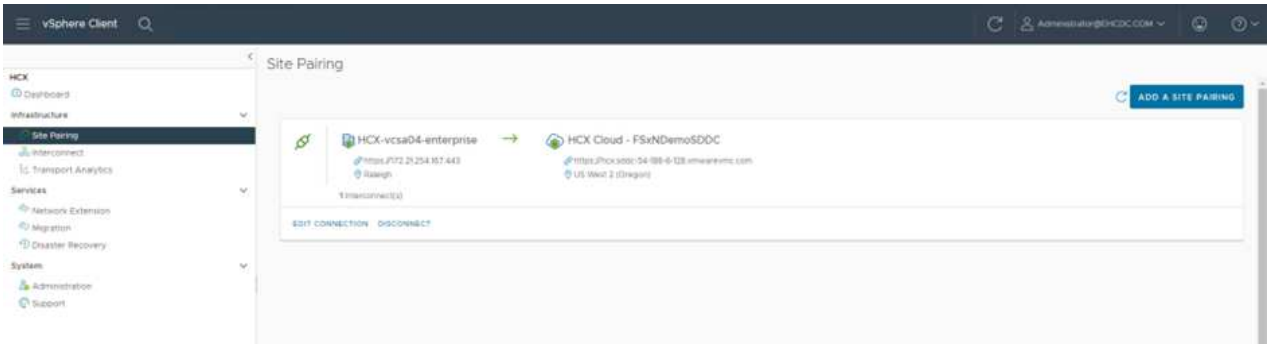


手順4：オンプレミスのVMware HCXコネクタをVMC HCX Cloud Managerとペアリングします

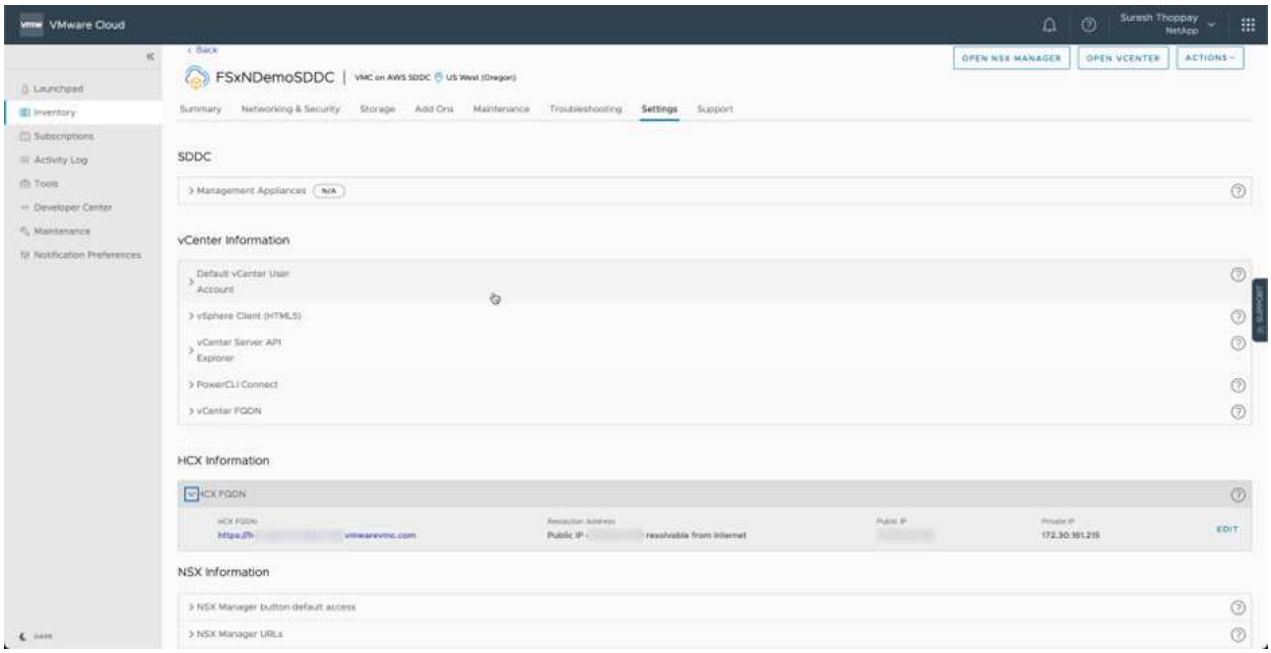
1. オンプレミスのvCenter ServerとVMC SDDCの間にサイトペアを作成するには、オンプレミスのvCenter Serverにログインして、HCX vSphere Web Clientプラグインにアクセスします。

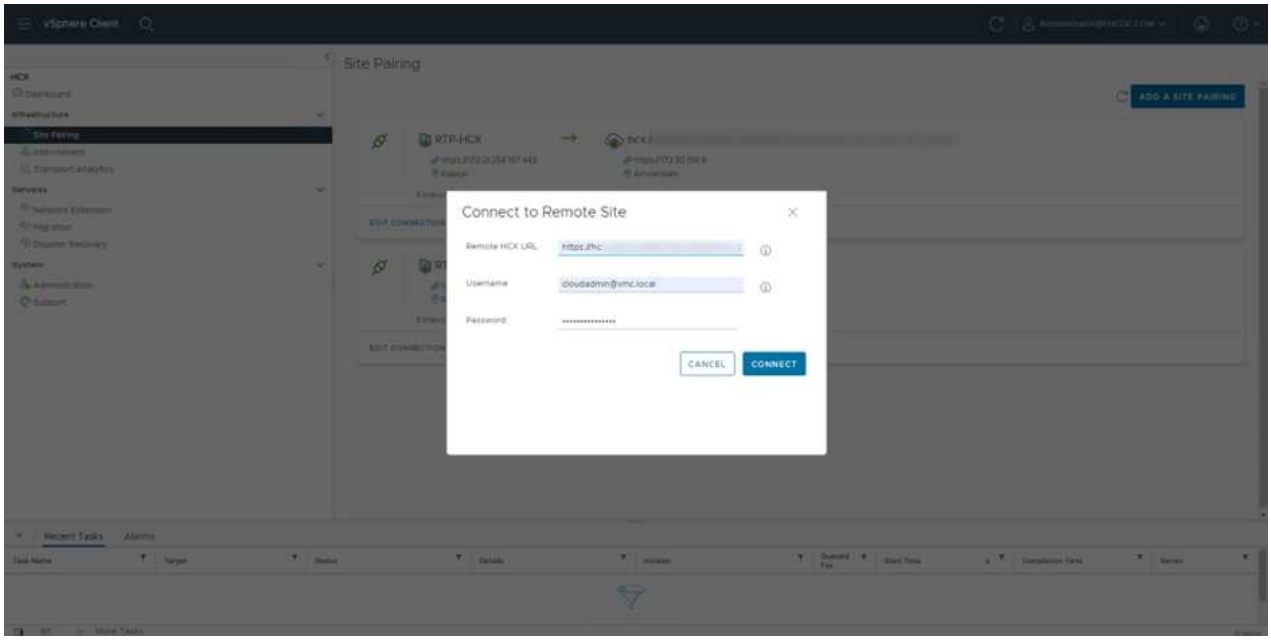


2. [インフラストラクチャ]で、[サイトペアリングの追加]をクリックします。リモートサイトを認証するには、VMC HCX Cloud ManagerのURLまたはIPアドレス、およびCloudAdminロールのクレデンシャルを入力します。



HCx情報は、SDDC Settingsページから取得できます。





3. サイトのペアリングを開始するには、[接続]をクリックします。

> VMware HCX Connectorは、ポート443経由でHCX Cloud Manager IPと通信できる必要があります。

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

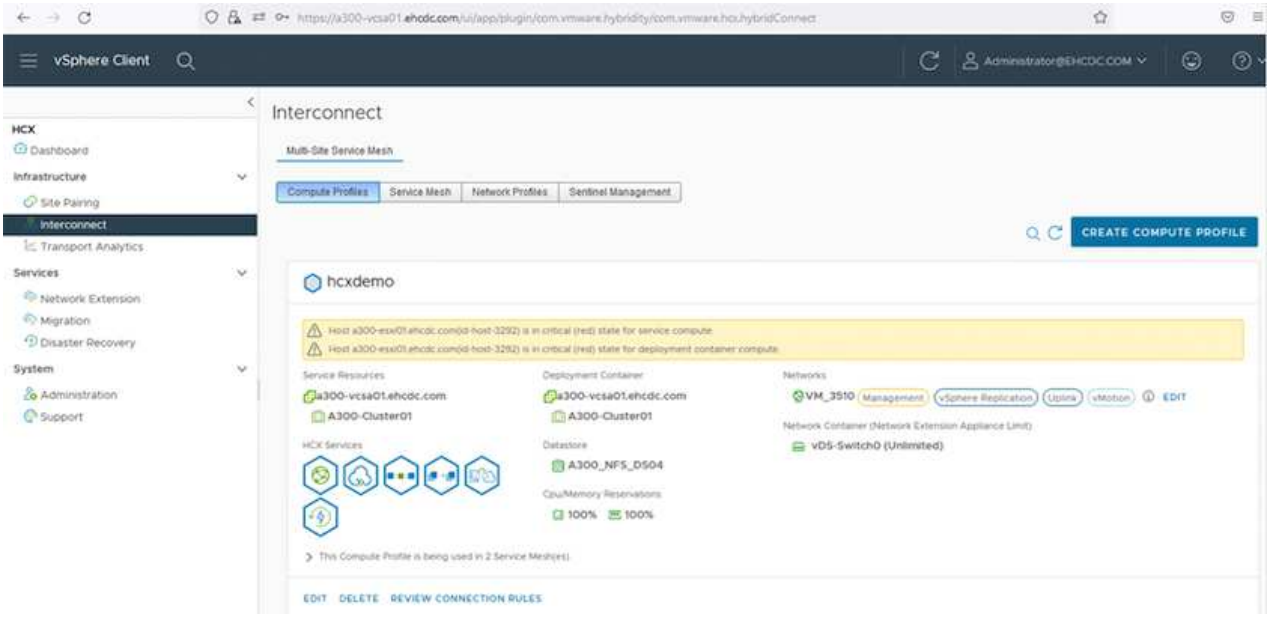
手順**5**：ネットワークプロファイル、コンピューティングプロファイル、およびサービスメッシュを設定します

VMware HCX Interconnect（HCX-IX）アプライアンスは、インターネットを介したセキュアなトンネル機能と、レプリケーションおよびvMotionベースの機能を実現するターゲットサイトへのプライベート接続を提供します。インターコネクトは、暗号化、トラフィックエンジニアリング、SD-WANを提供します。HCI IX Interconnect Applianceを作成するには、次の手順を実行します。

1. インフラストラクチャー（Infrastructure）で、相互接続（Interconnect）>マルチサイトサービスメッシュ（Multi-Site Service Mesh）>プロファイル計算（Compute Profiles）>コンピュートプロファイルの作成（Create Compute Profile

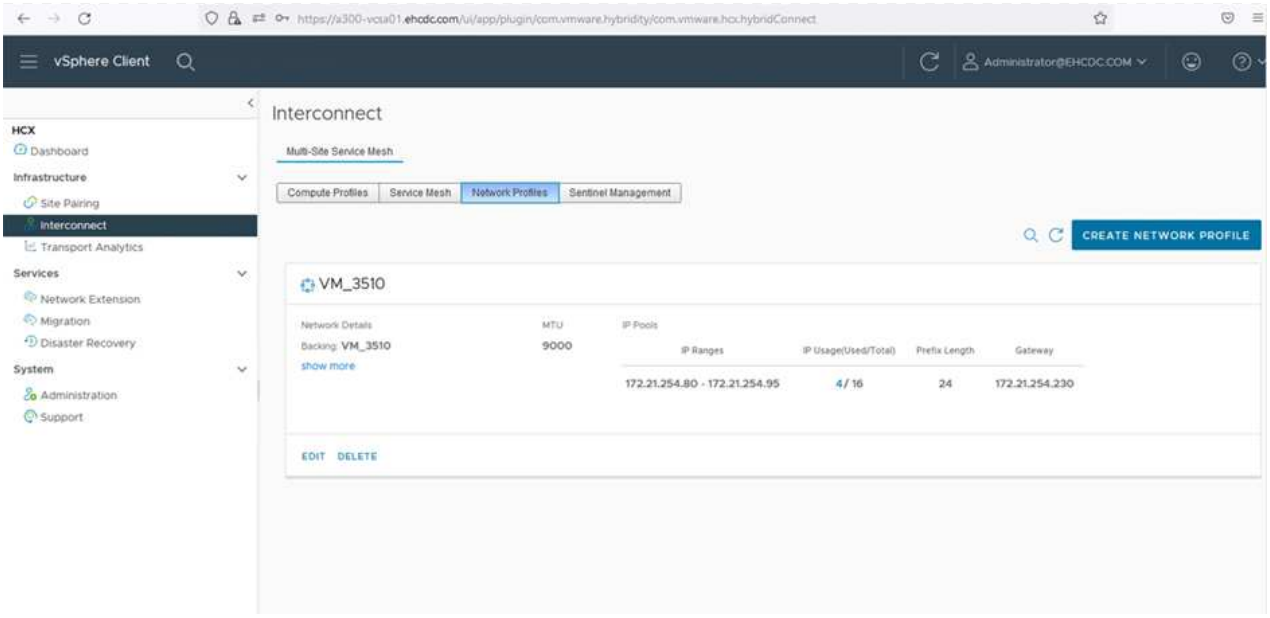
   コンピューティングプロファイルには、インターコネクト仮想アプライアンスの導入に必要なコンピューティング、ストレージ、およびネットワーク導入のパラメータが含まれています。また、VMwareデータセンターのどの部分にHCXサービスからアクセスできるかを指定します。

   手順の詳細については、を参照してください "計算プロファイルの作成"。



2. コンピューティングプロファイルを作成したら、Multi-Site Service Mesh > Network Profiles > Create Network Profileを選択して、ネットワークプロファイルを作成します。
3. ネットワークプロファイルは、HCXが仮想アプライアンスに使用するIPアドレスとネットワークの範囲を定義します。

   これには2つ以上のIPアドレスが必要です。これらのIPアドレスは、管理ネットワークから仮想アプライアンスに割り当てられます。

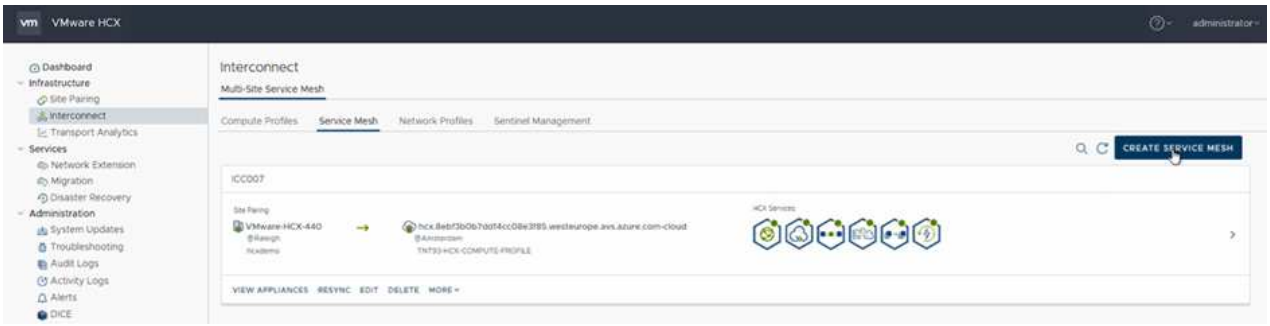


手順の詳細については、を参照してください "ネットワークプロファイルの作成"。

インターネット経由でSD-WANに接続する場合は、[ネットワークとセキュリティ]セクションでパブリックIPを予約する必要があります。

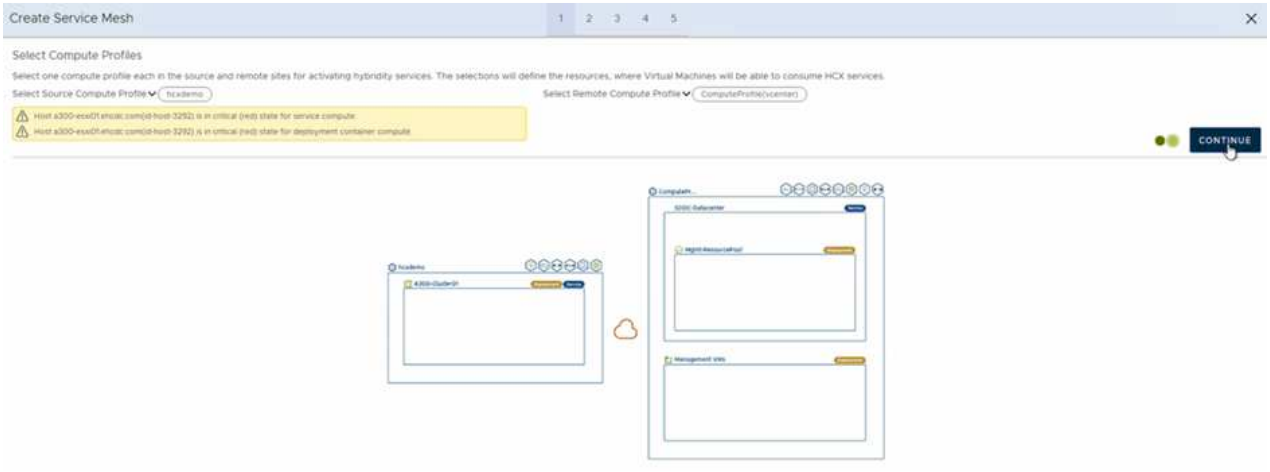
4. サービスメッシュを作成するには、InterconnectオプションのService Meshタブを選択し、オンプレミスサイトとVMC SDDCサイトを選択します。

   サービスメッシュによって、ローカルとリモートのコンピューティングプロファイルとネットワークプロファイルのペアが確立されます。

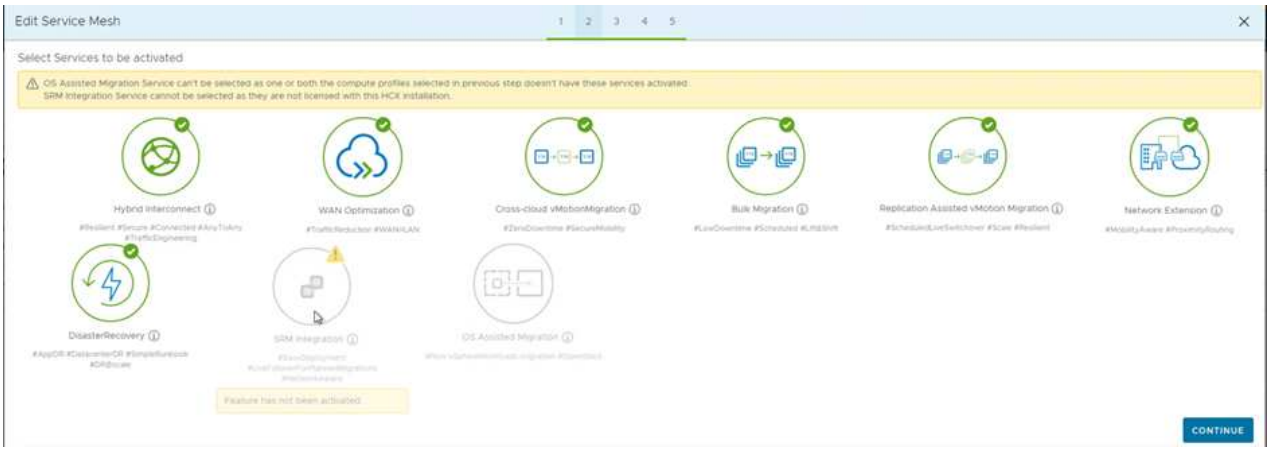


このプロセスの一部では、ソースサイトとターゲットサイトの両方で自動的に構成されるHCXアプライアンスを展開し、セキュアなトランスポートファブリックを作成します。

5. ソースとリモートのコンピューティングプロファイルを選択し、Continue（続行）をクリックします。

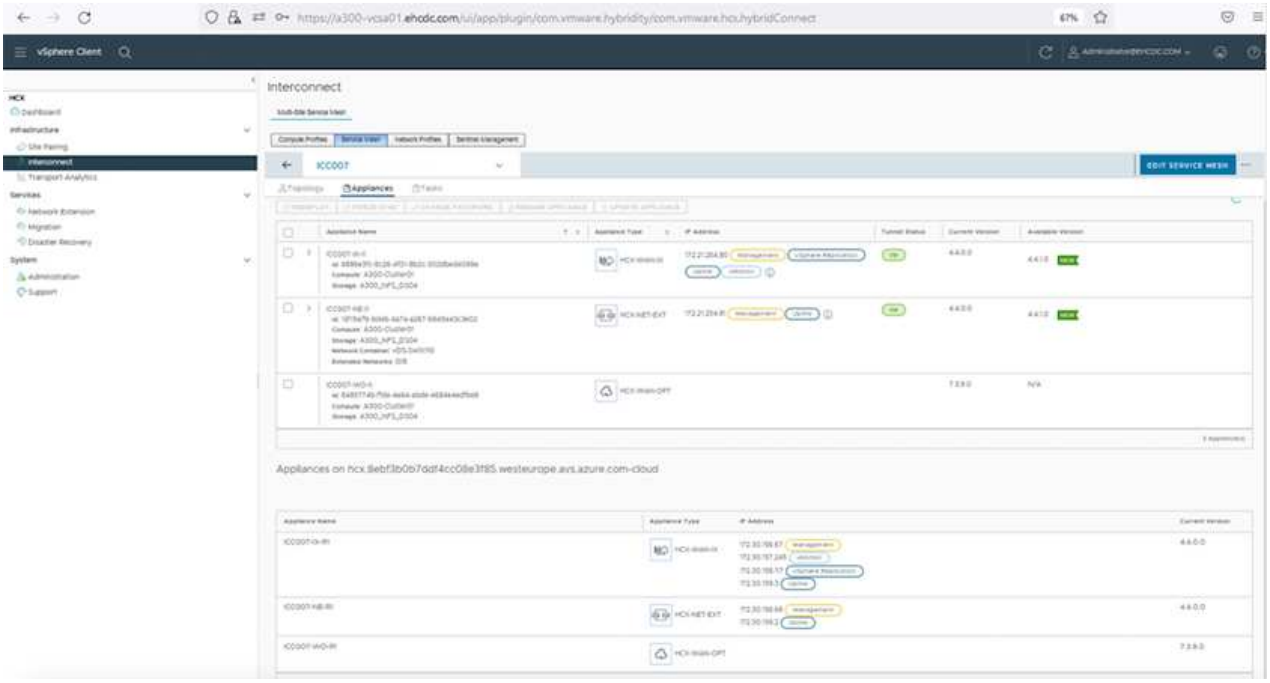


6. アクティブにするサービスを選択し、[続行]をクリックします。



Replication Assisted vMotion Migration、SRM Integration、およびOS Assisted Migrationには、HCX Enterpriseライセンスが必要です。

7. サービスメッシュの名前を作成し、完了をクリックして作成プロセスを開始します。導入が完了するまでに約30分かかります。サービスメッシュを設定したら、ワークロードVMの移行に必要な仮想インフラとネットワークを作成します。


vSphere Client
Interconnect
ICC007
EDIT SERVICE MESH
Appliances
Appliances on hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud

手順**6**：ワークロードを移行する

HCxは、オンプレミスやVMC SDDCなど、2つ以上の異なる環境間で双方向の移行サービスを提供します。HCXバルク移行、HCX vMotion、HCXコールド移行、HCX Replication Assisted vMotion（HCX Enterprise Editionで利用可能）、HCX OS Assisted Migration（HCX Enterprise Editionで利用可能）などのさまざまな移行テクノロジーを使用して、HCXでアクティブ化されたサイトとの間でアプリケーションワークロードを移行できます。

使用可能なHCX移行テクノロジの詳細については、を参照してください "VMware HCXの移行タイプ"

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

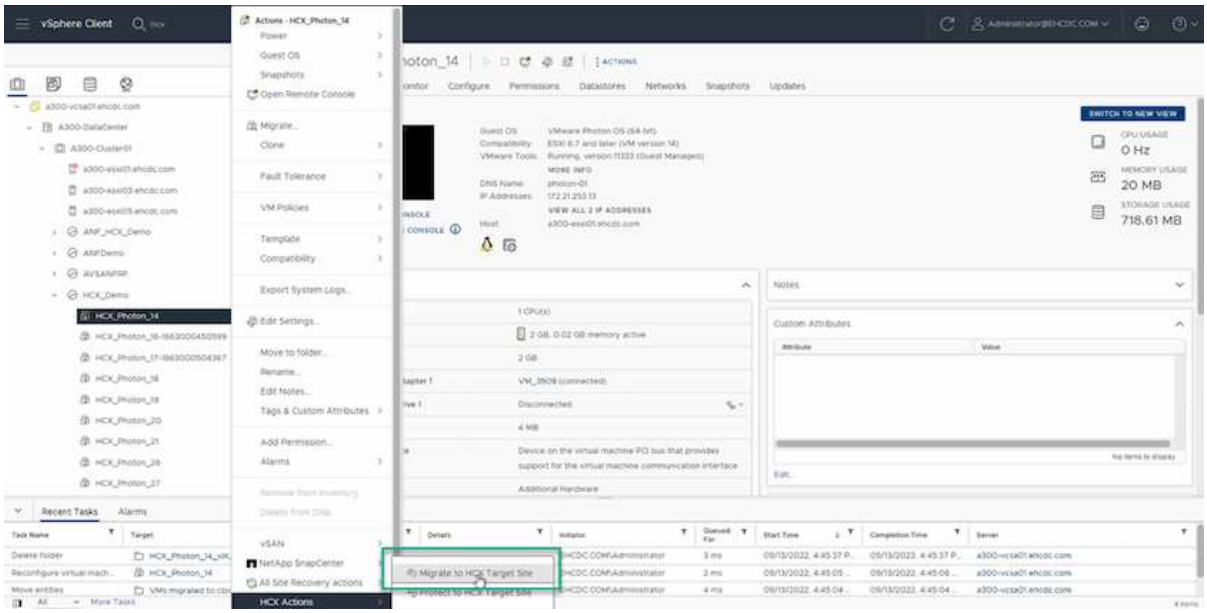
HCX-IXアプライアンスは、Mobility AgentサービスをvCenter Serverのホストオブジェクトとして追加します。このオブジェクトに表示されるプロセッサ、メモリ、ストレージ、およびネットワークのリソースは、IXアプライアンスをホストする物理ハイパーバイザーでの実際の消費量を表していません。

VMware HCX vMotion

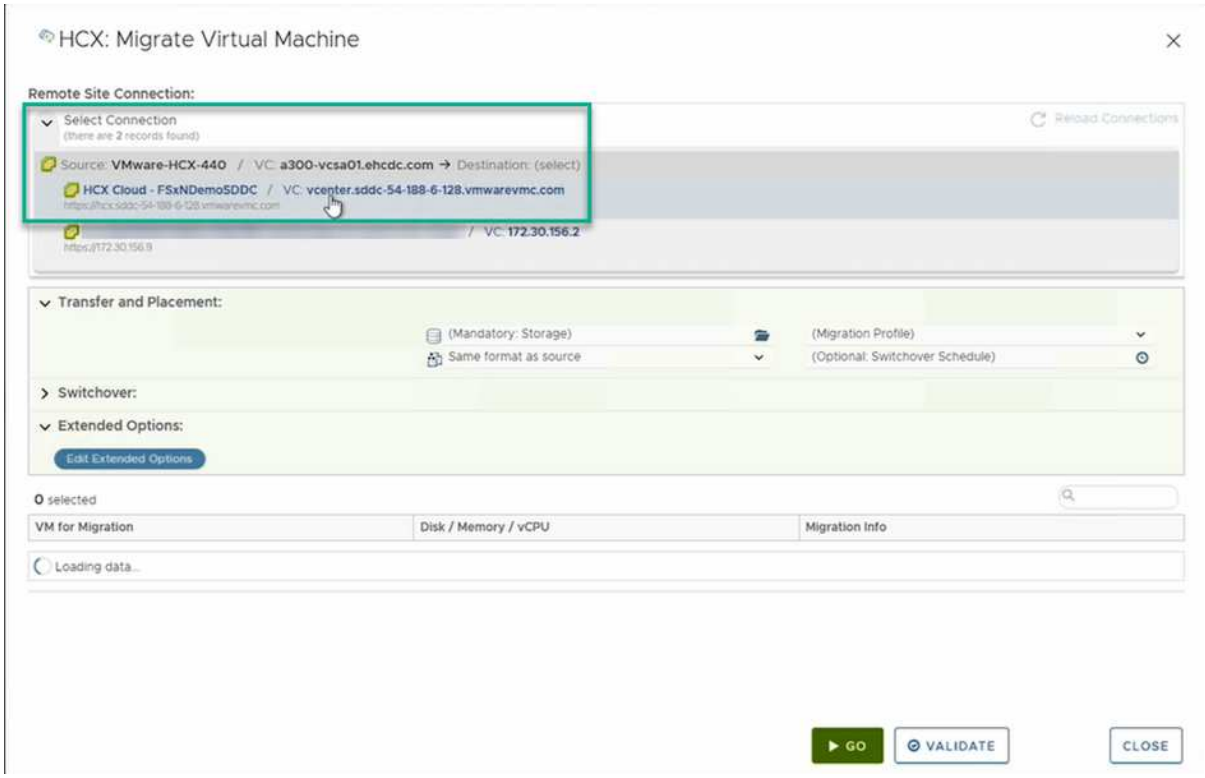
このセクションでは、HCX vMotionメカニズムについて説明します。この移行テクノロジは、VMware vMotionプロトコルを使用してVMをVMC SDDCに移行します。vMotion移行オプションは、一度に1つのVMのVM状態を移行するために使用します。このマイグレーション方式では、サービスは中断されません。

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

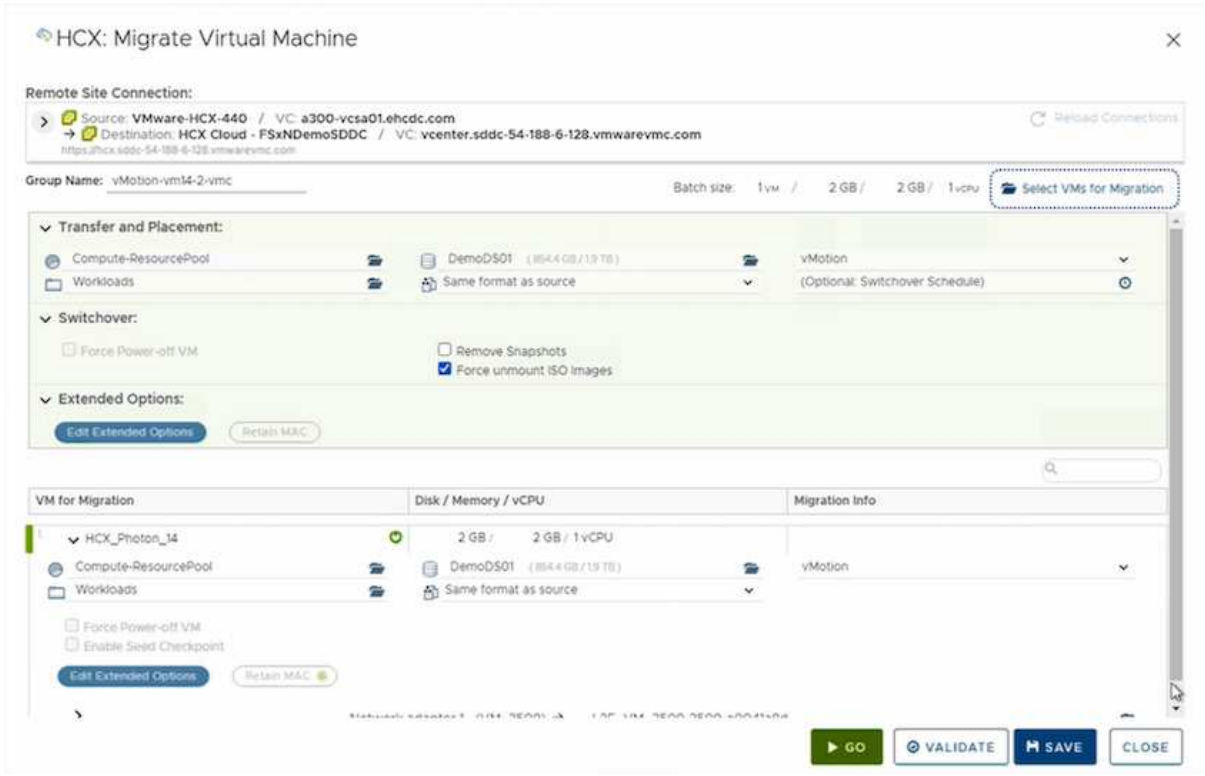
1. オンプレミスのvSphereクライアントから、Inventoryに移動し、移行するVMを右クリックして、HCX Actions > Migrate to HCX Target Siteを選択します。



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



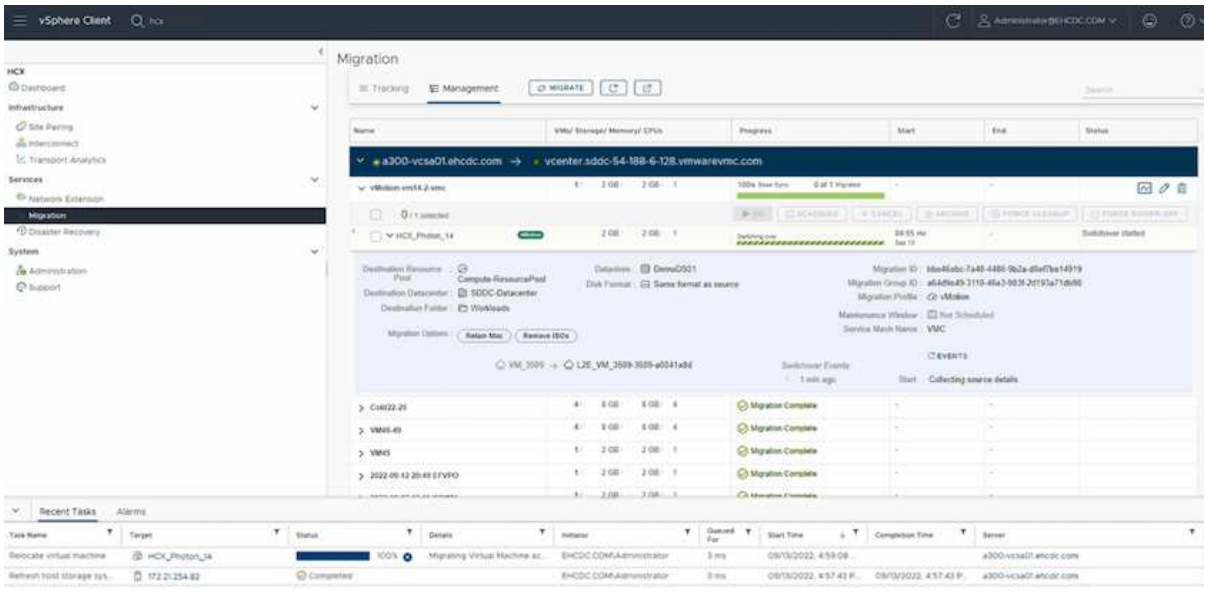
3. グループ名を追加し、[転送と配置]の下で必須フィールド(クラスタ、ストレージ、および宛先ネットワーク)を更新し、[検証]をクリックします。



4. 検証チェックが完了したら、Goをクリックして移行を開始します。

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

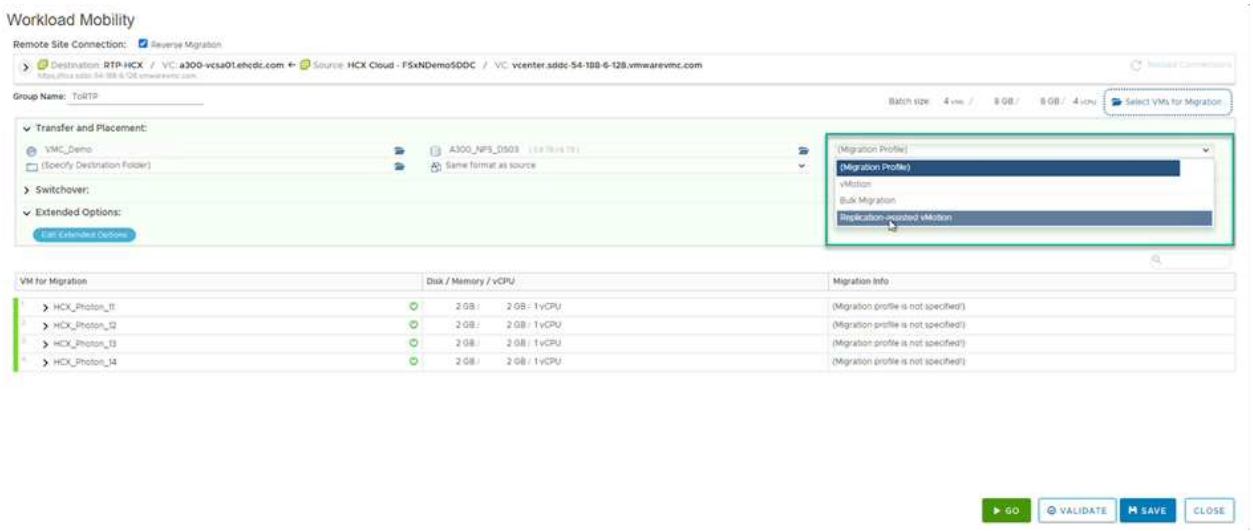
5. VMotionの進捗状況と完了は'HCX＞Migrationダッシュボードから監視できます



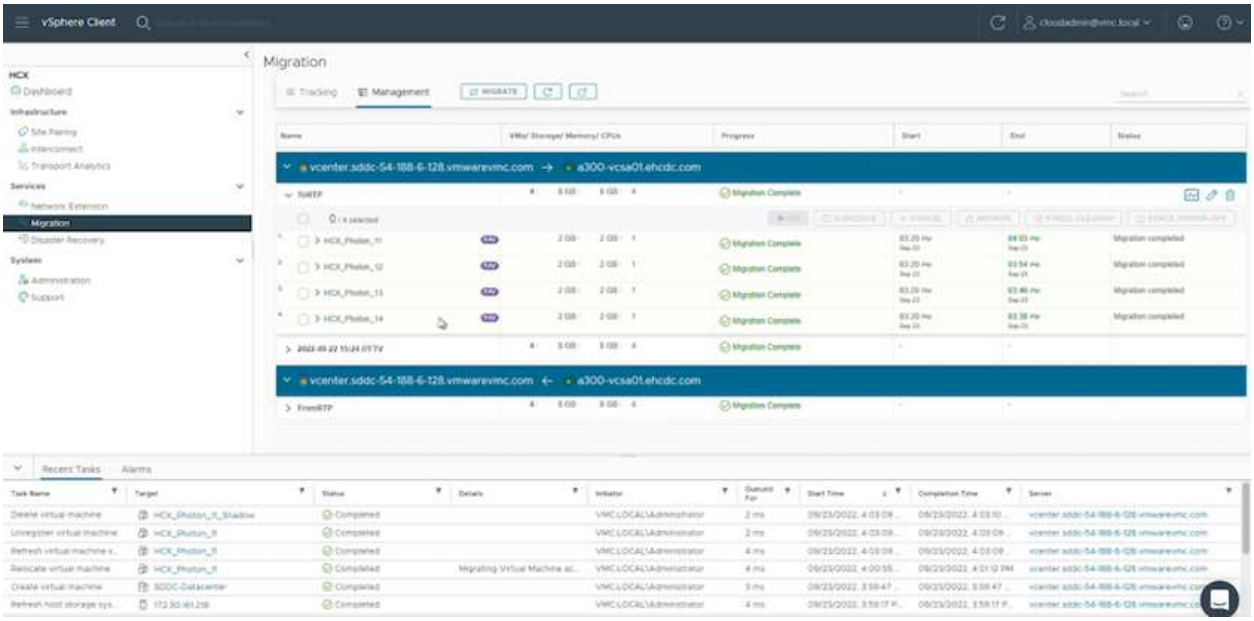
VMware Replication Assisted vMotionの場合

VMwareのドキュメントに気づいたように、VMware HCX Replication Assisted vMotion（RAV）は、バルク移行とvMotionのメリットを組み合わせています。一括移行では、vSphere Replicationを使用して複数のVMが同時に移行されます。これは、スイッチオーバー中にVMがリブートされるためです。HCx vMotionはダウンタイムなしで移行を行いますが、レプリケーショングループで一度に1つのVMが順次実行されます。RAVは、VMを並行して複製し、スイッチオーバーウィンドウまで同期させます。スイッチオーバープロセスでは、VMを停止することなく一度に1つずつ移行します。

次のスクリーンショットは、マイグレーションプロファイルをReplication Assisted vMotionとして示しています。



レプリケーションの所要時間は、少数のVMのvMotionよりも長くなる可能性があります。RAVでは、差分のみを同期し、メモリの内容を含めます。以下はマイグレーションステータスのスクリーンショットです。マイグレーションの開始時刻がVMごとに異なり、終了時刻も表示されます。



HCXマイグレーションオプションと、HCXを使用してオンプレミスからAWS上のVMware Cloudにワー

クロードを移行する方法については、を参照してください追加情報 "VMware HCXユーザーガイド"。

VMware HCX vMotionには、100 Mbps以上のスループット機能が必要です。

ONTAP データストア用のターゲットVMC FSXには、移行に対応できる十分なスペースが必要です。

まとめ

オールクラウドとハイブリッドクラウドのどちらをターゲットとしていても、オンプレミスのあらゆるタイプ/ベンダーストレージに保存されているデータを対象としている場合でも、NetApp ONTAP 対応のAmazon FSXとHCXは、データ要件をアプリケーションレイヤにシームレスにすることで、ワークロードの導入と移行を実現する優れたオプションを提供します。どのようなユースケースでも、VMCとFSX for ONTAP データストアを選択すれば、オンプレミスと複数のクラウドにわたるクラウドのメリット、一貫したインフラ、運用、ワークロードの双方向の移動、エンタープライズクラスの容量とパフォーマンスを迅速に実現できます。VMware vSphereレプリケーション、VMware vMotion、さらにはNFCコピーを使用してストレージを接続し、VMを移行するための一般的なプロセスと手順は同じです。

重要なポイント

本ドキュメントの主な内容は次のとおりです。

- Amazon FSX ONTAP をVMC SDDCを使用するデータストアとして使用できるようになりました。
- ONTAP データストア用のFSXを使用して、任意のオンプレミスデータセンターからVMCに簡単にデータを移行できます
- 移行アクティビティ中に容量とパフォーマンスの要件を満たすために、FSX ONTAP データストアを簡単に拡張および縮小できます。

追加情報の参照先

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

- VMware Cloudのドキュメント

  "https://docs.vmware.com/en/VMware-Cloud-on-AWS/"

- Amazon FSX for NetApp ONTAP のドキュメント

  "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"

  VMware HCXユーザーガイド

- "https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"

Region Availability - VMCの補助的な**NFS**データストア

AWS / VMCで追加のNFSデータストアを使用できるかどうかは、Amazonによって定義されています。まず、VMCとFSxNの両方が指定されたリージョンで利用可能かどうか

を確認する必要があります。次に、FSxNの補足的なNFSデータストアがそのリージョンでサポートされているかどうかを確認する必要があります。

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

次の表に、情報がまだリリースされている間に、VMC、FSxN、およびFSxNの現在のサポート状況をNFSデータストアとして示します。

南北アメリカ

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

最終更新日：2022年6月2日

EMEAの場合

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

最終更新日：2022年6月2日

アジア太平洋地域

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

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

最終更新日：2022年9月28日

Azure AVS 向けのネットアップの機能

ネットアップがAzure VMware解決策 （AVS）に提供する機能の詳細をご確認ください。ゲスト接続ストレージデバイスとしてネットアップが提供する機能と、NFSデータストアの追加機能を利用して、ワークフローを移行し、クラウドへの拡張/バースト対応、バックアップ/リストア、ディザスタリカバリを実施できます。

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。

- "Azure で AVS を設定する"
- "AVS 向けのネットアップストレージオプション"
- "ネットアップとVMwareのクラウドソリューション"

Azure で AVS を設定する

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

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

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

セットアッププロセスは、次の手順に分けることができます。

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

詳細を表示します "AVSの設定手順"。

AVS 向けのネットアップストレージオプション

ネットアップのストレージは、Azure AVS内で接続されたか、NFSデータストアとして追加で利用するかのいずれかの方法で利用できます。

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

Azure は、以下の構成でネットアップストレージをサポートします。

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

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

解決策のユースケース

ネットアップと VMware のクラウドソリューションを使用すれば、多くのユースケースを Azure AVS で簡単に導入できます。SEケースは、VMwareが定義したクラウド領域ごとに定義されます。

- 保護（ディザスタリカバリとバックアップ/リストアの両方を含む）
- 拡張
- 移動

"Azure AVS 向けネットアップソリューションをご覧ください"

Azure / AVS上のワークロードを保護

ANFとJetStreamを使用したディザスタリカバリ

クラウドへのディザスタリカバリは、耐障害性に優れた対費用効果の高い方法で、サイトの停止やデータ破損からワークロードを保護します（ランサムウェアなど）。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ストレージにレプリケートしてリカバリできるため、データ損失を最小限に抑えたり、ほぼゼロのRTOを実現できます。

Jetstream DRを使用すると、オンプレミスからAVS、特にAzure NetApp Files に複製されたワークロードをシームレスにリカバリできます。ディザスタリカバリサイトにある最小限のリソースと対費用効果の高いクラウドストレージを使用して、対費用効果の高いディザスタリカバリを実現します。Jetstream DRは、Azure Blob Storageを介したANFデータストアへのリカバリを自動化します。Jetstream DRは、独立したVMまたは関連するVMのグループを、ネットワークマッピングに従ってリカバリサイトインフラストラクチャにリカバリし、ランサムウェアからの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。

このドキュメントでは、JetStream DRの動作原理とその主なコンポーネントについて説明します。

1. JetStream DRソフトウェアをオンプレミスのデータセンターにインストールします。
   a. JetStream DRソフトウェアバンドルをAzure Marketplace（ZIP）からダウンロードし、JetStream DR MSA（OVA）を指定のクラスタに導入します。
   b. I/Oフィルタパッケージを使用してクラスタを設定します(JetStream VIBをインストールします)。
   c. DR AVSクラスタと同じリージョンでAzure Blob（Azureストレージアカウント）をプロビジョニング
   d. DRVAアプライアンスを導入し、レプリケーションログボリューム（既存のデータストアまたは共有iSCSIストレージからVMDK）を割り当てます。
   e. 保護されたドメイン（関連するVMのグループ）を作成し、DRVAとAzure Blob Storage / ANFを割り当てます。
   f. 保護を開始します。
2. JetStream DRソフトウェアをAzure VMware解決策 プライベートクラウドにインストールします。
   a. Runコマンドを使用して、JetStream DRをインストールおよび設定します。
   b. [Scan Domains]オプションを使用して、同じAzure BLOBコンテナを追加し、ドメインを検出します。
   c. 必要なDRVAアプライアンスを導入します。
   d. 使用可能なvSANまたはANFデータストアを使用してレプリケーションログボリュームを作成します。
   e. 保護されたドメインをインポートし、VMの配置にANFデータストアを使用するようにRocVA（リカバリVA）を設定します。
   f. 適切なフェイルオーバーオプションを選択し、ほぼゼロのRTOドメインまたはVMに対して継続的なリハイドレートを開始します。
3. 災害発生時に、指定したAVS DRサイトでAzure NetApp Files データストアへのフェイルオーバーをトリガーします。
4. 保護対象サイトのリカバリ後、保護対象サイトへのフェイルバックを起動します。開始する前に、前提条件が満たされていることを確認してください "リンク" また、JetStream Softwareが提供するBandwidth Testing Tool（BWT）を実行して、JetStream DRソフトウェアで使用した場合にAzure BLOBストレージとそのレプリケーション帯域幅のパフォーマンスを評価します。接続を含む前提条件が整ったら、からJetStream DR for AVSをセットアップして登録します "Azure Marketplace で入手できます"。ソフトウェアバンドルをダウンロードしたら、上記のインストールプロセスに進みます。

多数のVM（100+など）の保護を計画して開始する場合は、JetStream DR Automation ToolkitからCapacity Planning Tool（CPT）を使用します。RTOとリカバリ・グループの設定とともに保護対象のVMのリストを指定し、CPTを実行します。

CPTは次の機能を実行します。

- RTOに応じたVMを保護ドメインに統合する。
- DRVAとそのリソースの最適な数を定義する。

- 必要なレプリケーション帯域幅の見積もり
- レプリケーションログボリュームの特性（容量、帯域幅など）を特定します。
- 必要なオブジェクトストレージ容量などを見積もります。

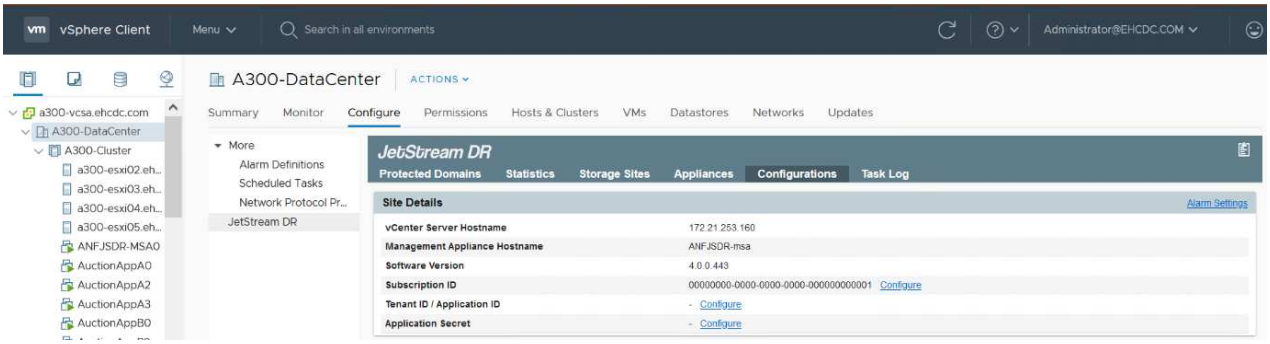
ドメインの数と内容は、平均IOPS、合計容量、優先度（フェイルオーバー順序を定義）、RTOなど、VMのさまざまな特性によって異なります。

JetStream DRをオンプレミスのデータセンターにインストールします

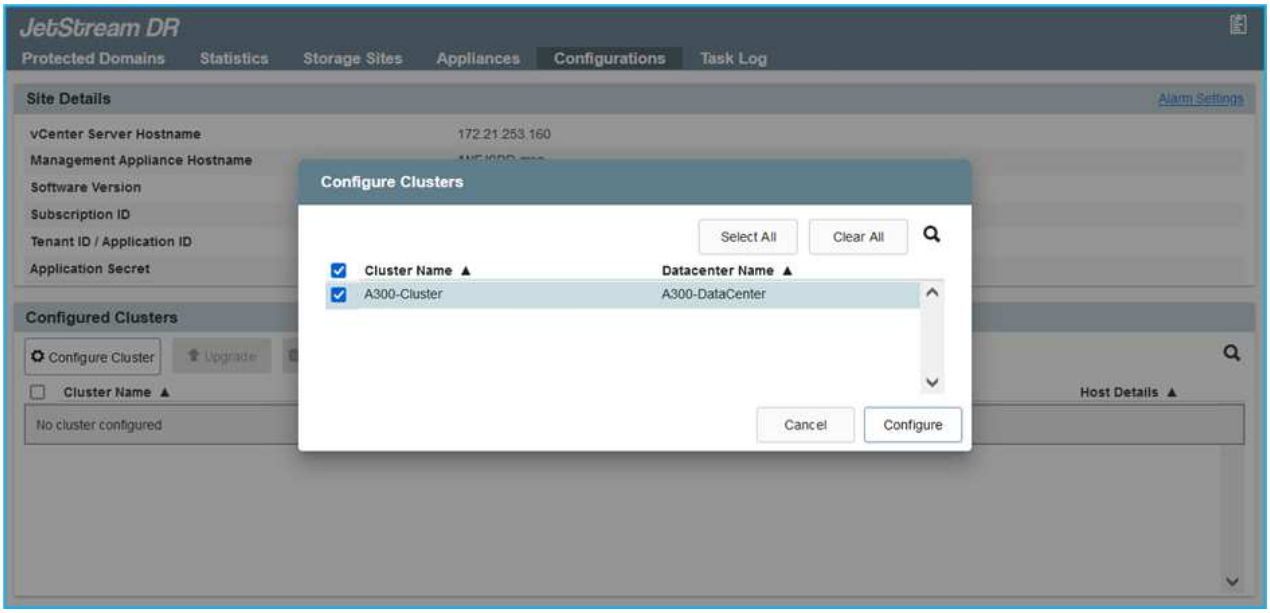
Jetstream DRソフトウェアは、JetStream DR Management Server Virtual Appliance（MSA）、DR Virtual Appliance（DRVA）、およびホストコンポーネント（I/O Filterパッケージ）の3つの主要コンポーネントで構成されています。MSAは、コンピューティングクラスタにホストコンポーネントをインストールして構成し、JetStream DRソフトウェアを管理するために使用されます。次に、インストールプロセスの概要 の概要を示します。

JetStream DRをオンプレミスにインストールする方法

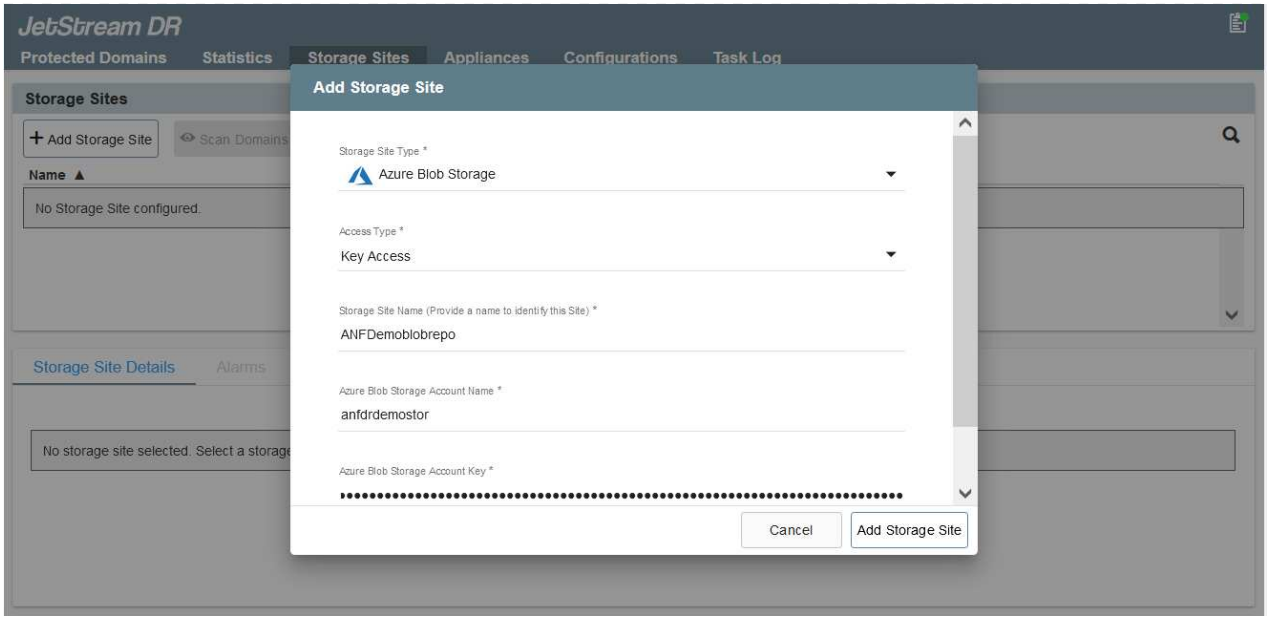
1. 前提条件を確認する。
2. キャパシティプランニングツールを実行して、リソースと構成に関する推奨事項を確認します（オプションですが、コンセプトの実証の試用には推奨されます）。
3. JetStream DR MSAを指定されたクラスタ内のvSphereホストに展開します。
4. ブラウザでDNS名を使用してMSAを起動します。
5. vCenterサーバをMSAに登録します。インストールを実行するには、次の手順を実行します。
6. JetStream DR MSAが導入され、vCenter Serverが登録されたら、vSphere Web Clientを使用してJetStream DRプラグインにアクセスします。これを行うには、[データセンター]>[設定]>[JetStream DR]に移動します。



7. JetStream DRインタフェースから、適切なクラスタを選択します。



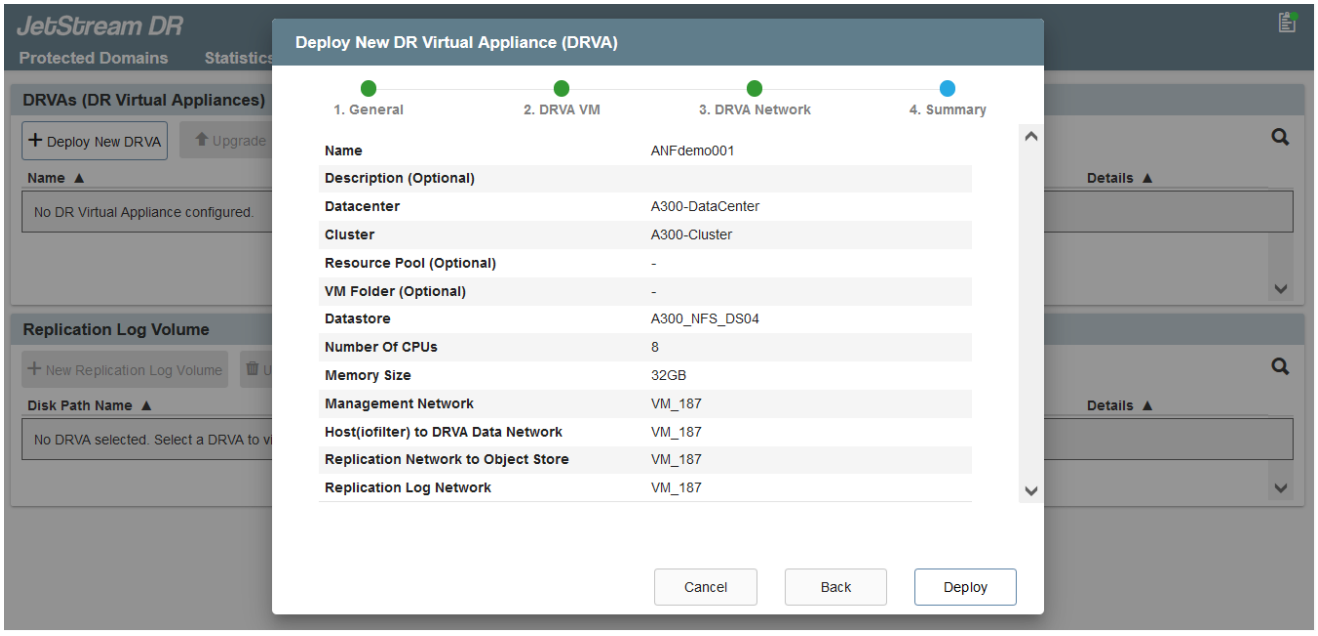
8. I/Oフィルタパッケージを使用してクラスタを設定します。



9. リカバリサイトにAzure Blob Storageを追加します。
10. アプライアンスタブからDR仮想アプライアンス（DRVA）を導入します。

DRFAはCPTによって自動的に作成できますが、POCトライアルの場合は、DRサイクルを手動で設定して実行することをお勧めします（Start protection > failover > failback）。

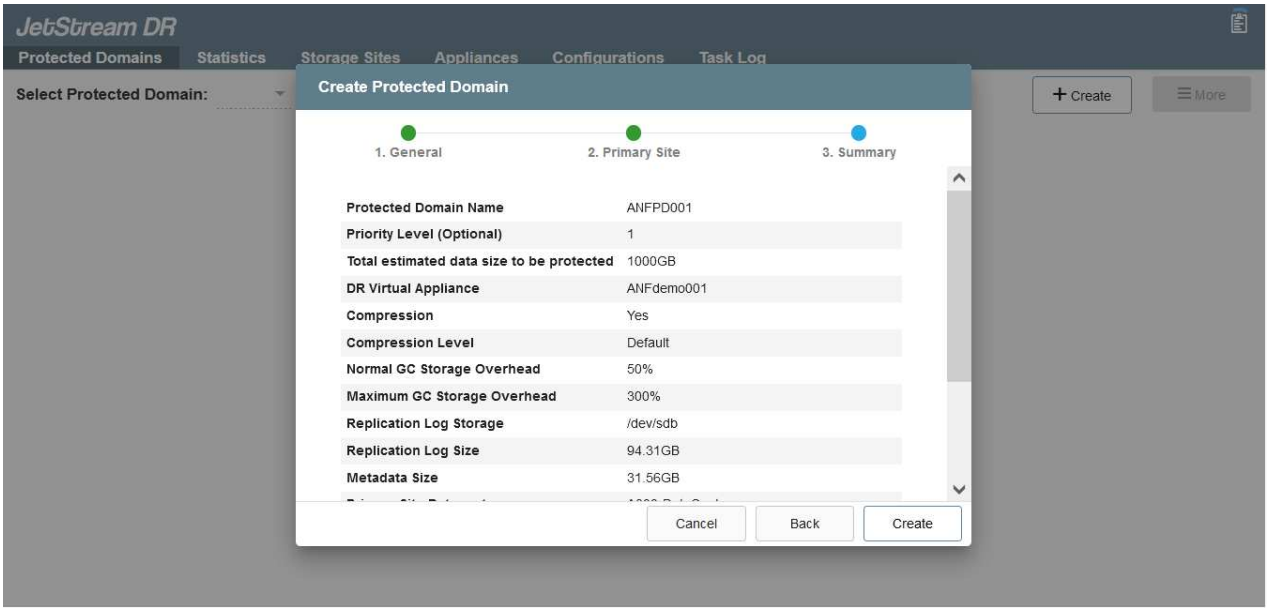
JetStream DRVAは、データ複製プロセスの主要な機能を容易にする仮想アプライアンスです。保護されたクラスタには少なくとも1つのDRVAが含まれている必要があります。通常は、ホストごとに1つのDRVAが構成されます。各DRVAは、複数の保護ドメインを管理できます。



この例では、4台のDRVAが80台の仮想マシン用に作成されています。

1. 使用可能なデータストアまたは独立した共有iSCSIストレージプールからVMDKを使用して、各DRVAのレプリケーションログボリュームを作成します。

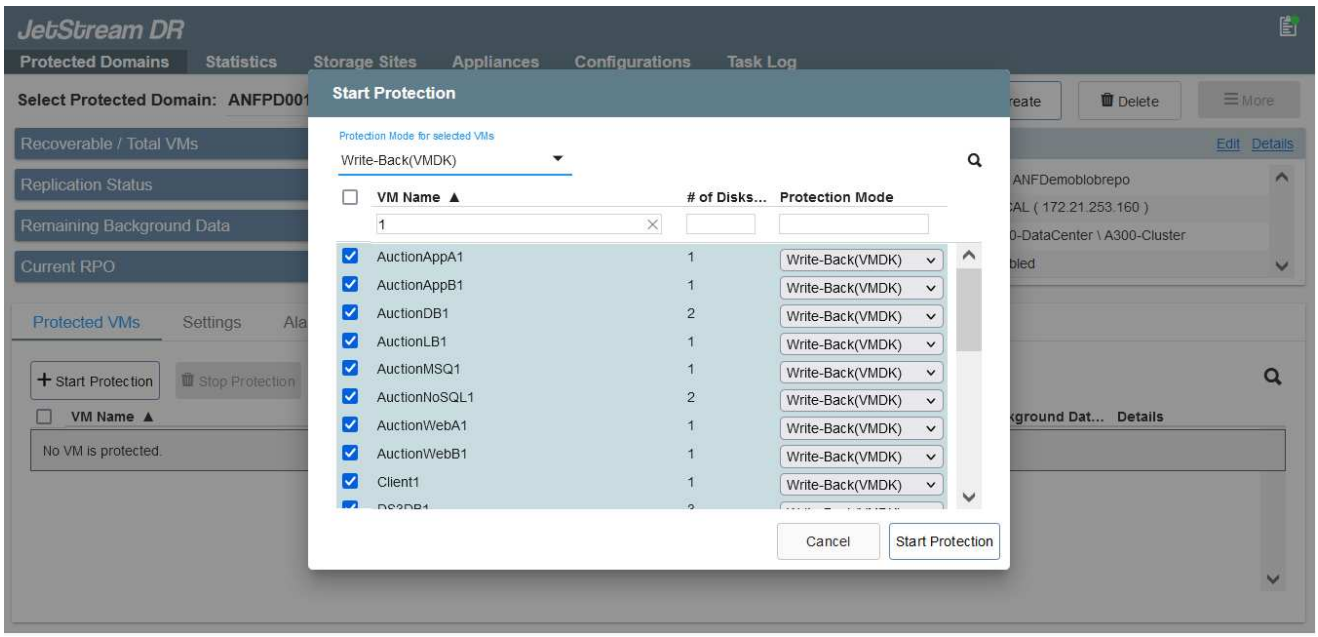
2. Protected Domainsタブで、Azure Blob Storageサイト、DRVAインスタンス、およびレプリケーションログに関する情報を使用して、必要な数の保護ドメインを作成します。保護ドメインは、クラスタ内の特定のVMまたはVMのセットを定義します。これらのVMは一緒に保護され、フェイルオーバー/フェイルバック処理の優先順位が割り当てられます。



3. 保護するVMを選択し、保護ドメインのVM保護を開始します。これにより、指定したBlob Storeへのデータレプリケーションが開始されます。

保護ドメイン内のすべてのVMに同じ保護モードが使用されていることを確認します。

ライトバック（VMDK）モードを使用すると、パフォーマンスが向上します。



レプリケーションログボリュームがハイパフォーマンスストレージに配置されていることを確認します。

フェイルオーバー実行ブックは、VM（回復グループ）のグループ化、起動順序の設定、およびCPU /メモリの設定とIP設定の変更を行うように構成できます。

Runコマンドを使用して、**Azure VMware**解決策 プライベートクラウドに**JetStream DR for AVS**をインストールします

リカバリサイト（AVS）では、3ノードのパイロットライトクラスタを事前に作成することを推奨します。これにより、次の項目を含むリカバリサイトのインフラを事前に設定できます。

- 宛先ネットワークセグメント、ファイアウォール、DHCPやDNSなどのサービスなど。
- AVS対応のJetStream DRのインストール
- ANFボリュームをデータストアとして構成し、moreJetStream DRではミッションクリティカルなドメインのRTOモードをほぼゼロに設定できます。これらのドメインには、デスティネーションストレージが事前にインストールされている必要があります。この場合、ANFは推奨ストレージタイプです。

セグメント作成を含むネットワーク構成は、オンプレミスの要件に合わせてAVSクラスタ上で設定する必要があります。

SLAやRTOの要件に応じて、継続的なフェイルオーバーモードや通常の（標準）フェイルオーバーモードを使用できます。RTOがほぼゼロの場合は、リカバリサイトで継続的なリハイドレートを開始する必要があります。

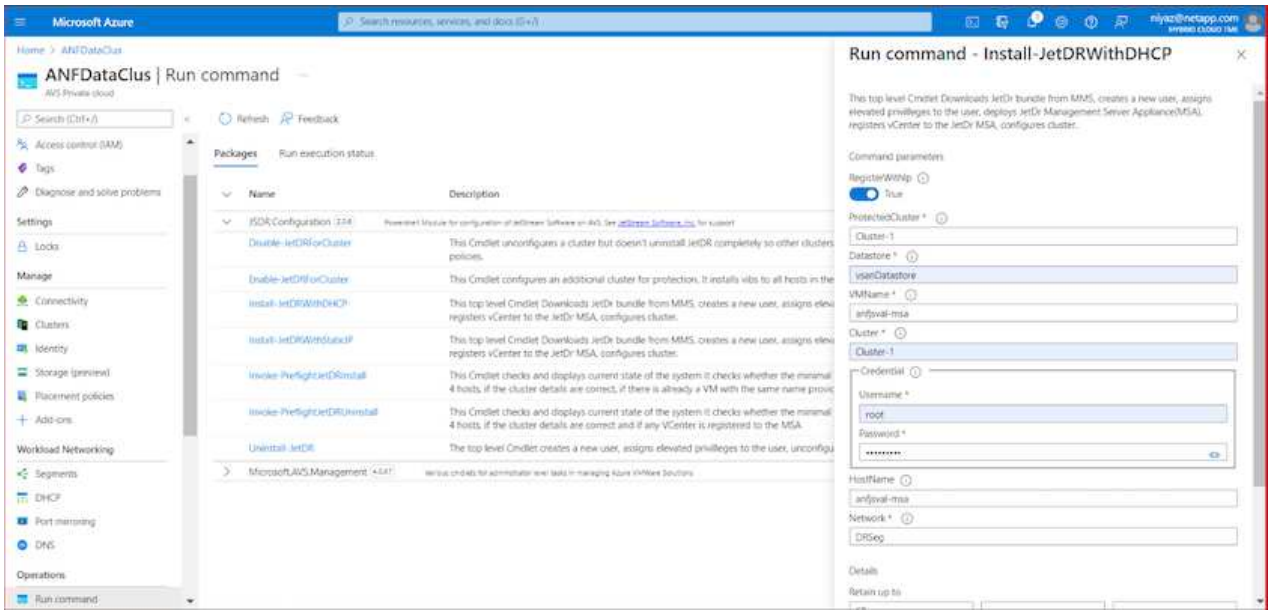
プライベートクラウドに**JetStream DR for AVS**をインストールする方法

Azure VMware解決策 プライベートクラウドにJetStream DR for AVSをインストールするには、次の手順を実行します。

1. AzureポータルからAzure VMware解決策 に移動し、プライベートクラウドを選択して、実行コマンド>パッケージ> JSDR.Configurationを選択します。

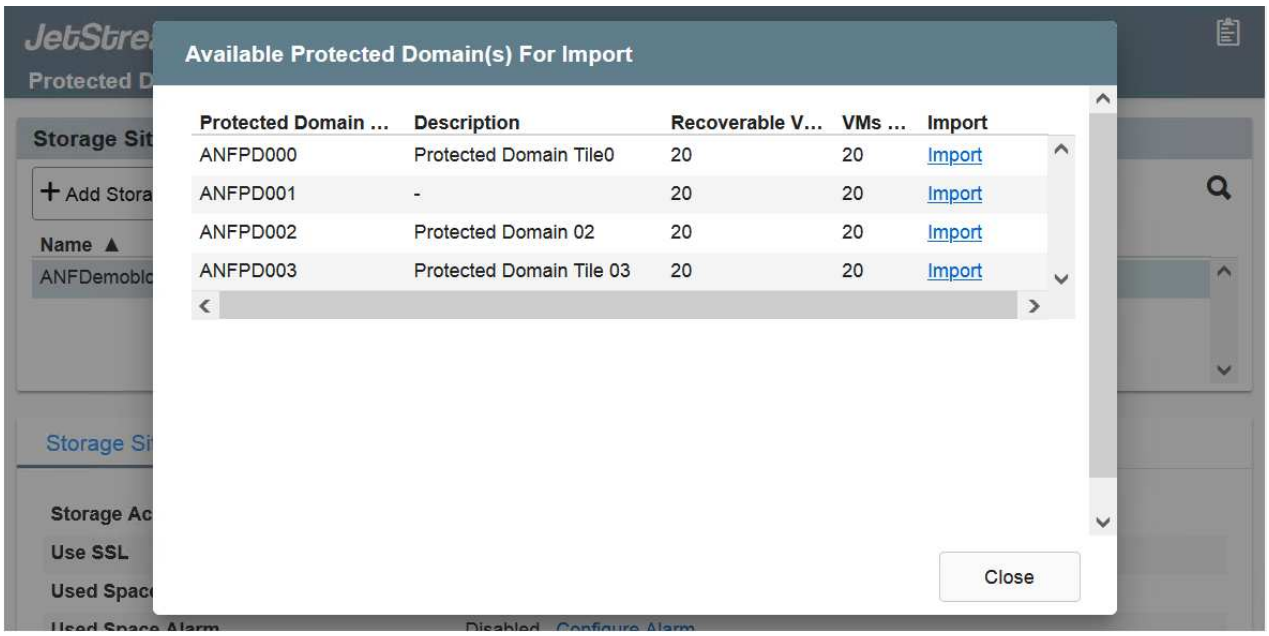
> Azure VMware解決策 のデフォルトCloudAdminユーザには、AVS対応のJetStream DRをインストールするための十分な権限がありません。Azure VMware解決策 では、JetStream DR用のAzure VMware解決策 実行コマンドを呼び出すことで、JetStream DRを簡単かつ自動でインストールできます。

次のスクリーンショットは、DHCPベースのIPアドレスを使用したインストール方法を示しています。



2. JetStream DR for AVSのインストールが完了したら、ブラウザをリフレッシュします。JetStream DR UIにアクセスするには、SDDC Datacenter > Configure > JetStream DRに移動します。

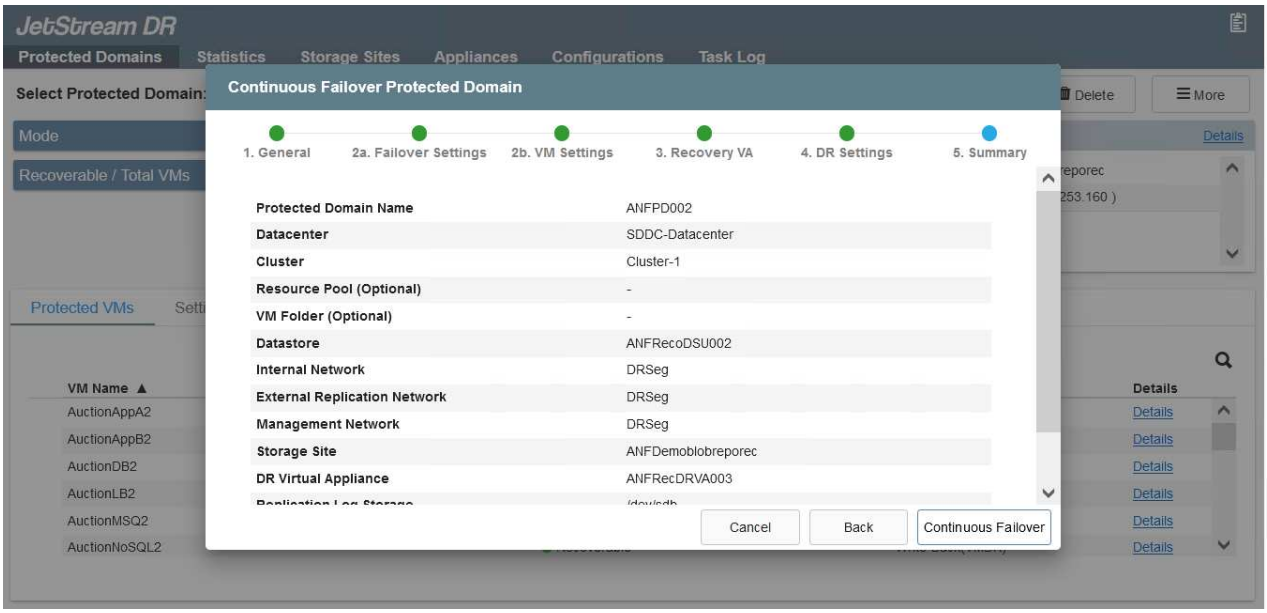
3. JetStream DRインターフェイスから、オンプレミスクラスタをストレージサイトとして保護するために使用したAzure Blob Storageアカウントを追加し、Scan Domainsオプションを実行します。



4. 保護ドメインをインポートしたら、DRVAアプライアンスを展開します。この例では、JetStream DR UIを使用して、リカバリサイトから継続的なリハイドレートを手動で開始します。

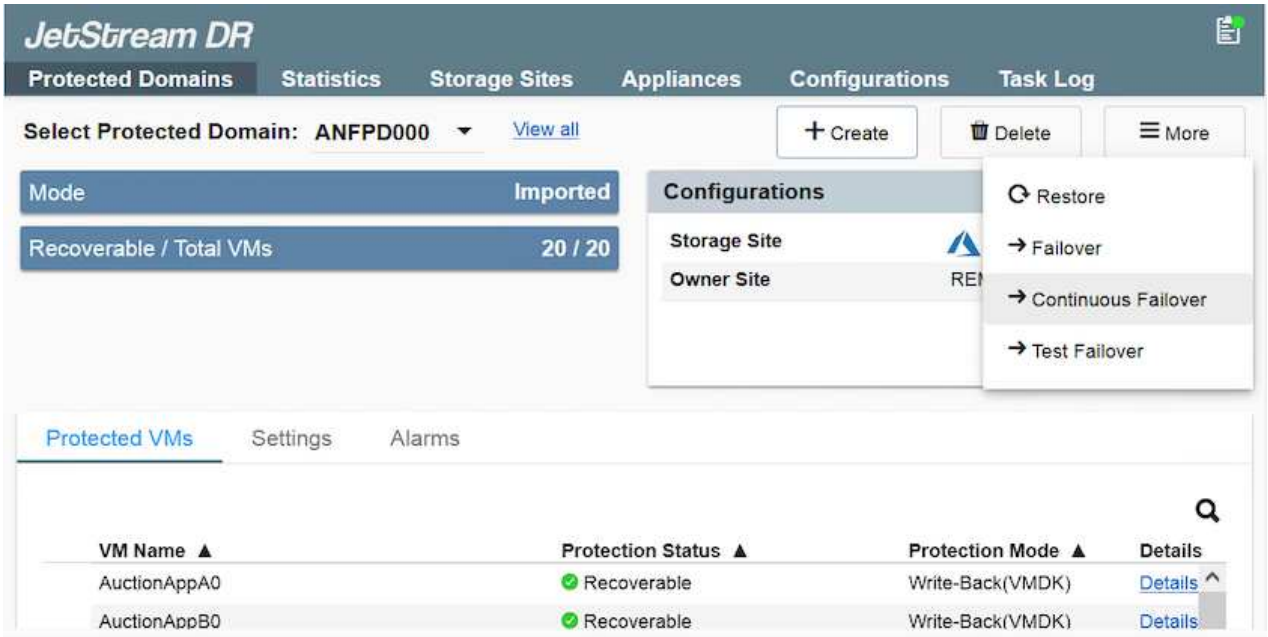
> これらの手順は、CPT作成計画を使用して自動化することもできます。

5. 使用可能なvSANまたはANFデータストアを使用してレプリケーションログボリュームを作成します。
6. 保護ドメインをインポートし、VMの配置にANFデータストアを使用するようにリカバリVAを設定します。



選択したセグメントでDHCPが有効になっていて、十分なIPが使用可能であることを確認します。ダイナミックIPは、ドメインのリカバリ中に一時的に使用されます。リカバリVM（連続リハイドレートを含む）ごとに、個別のダイナミックIPが必要です。リカバリの完了後、IPは解放され、再利用できます。

7. 適切なフェイルオーバーオプション（継続的フェイルオーバーまたはフェイルオーバー）を選択します。この例では、連続リハイドレート（連続フェールオーバー）が選択されています。



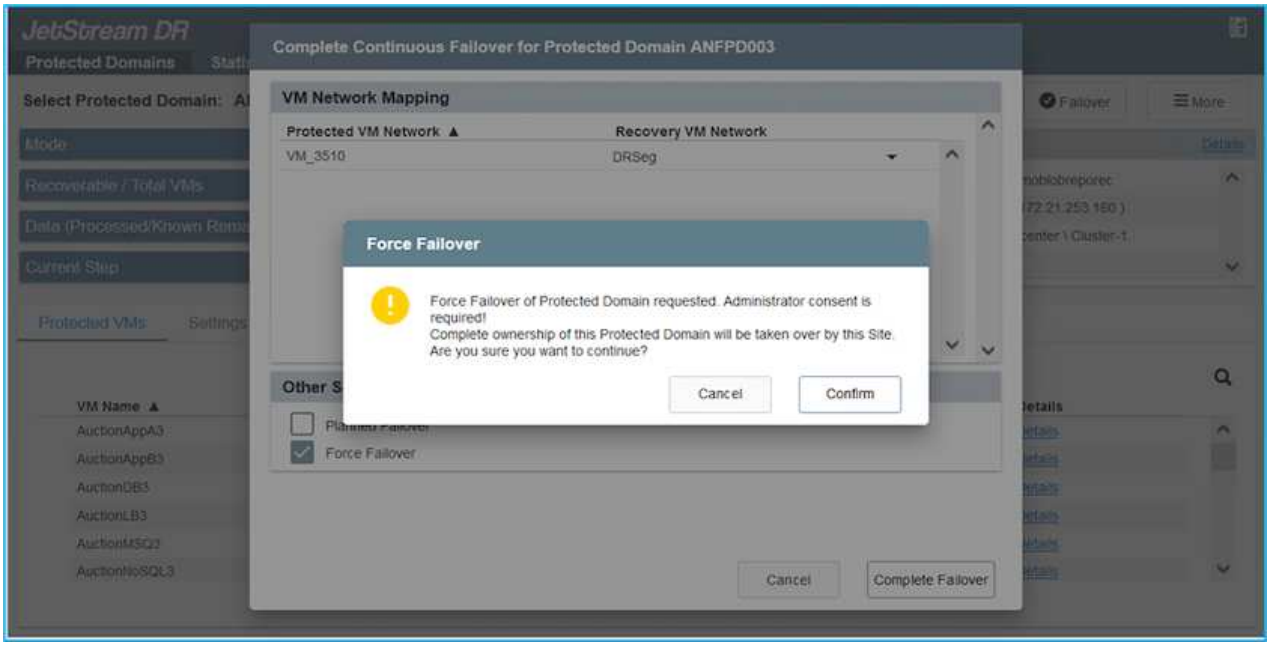
フェイルオーバー/フェイルバックを実行しています

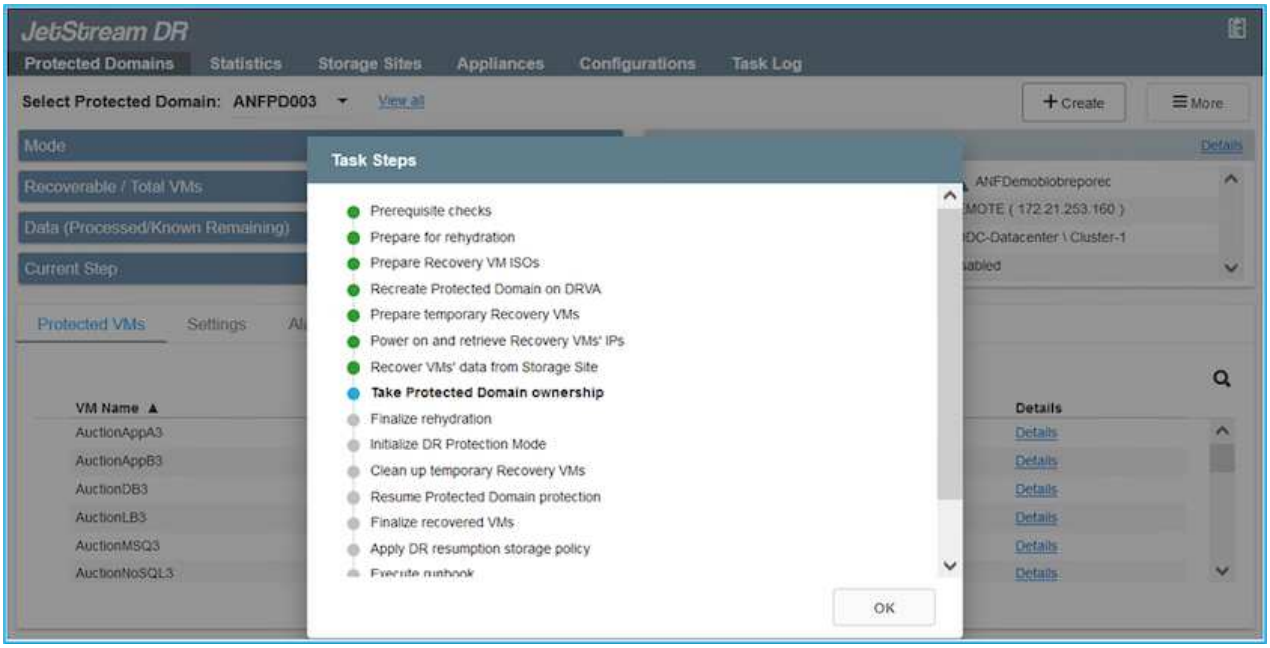
フェールオーバー/フェールバックの実行方法

1. オンプレミス環境の保護対象クラスタで障害が発生した場合（部分的または完全な障害）、フェイルオーバーをトリガーします。

   CPTを使用すると、フェイルオーバープランを実行して、Azure Blob StorageからAVSクラスタリカバリサイトにVMをリカバリできます。

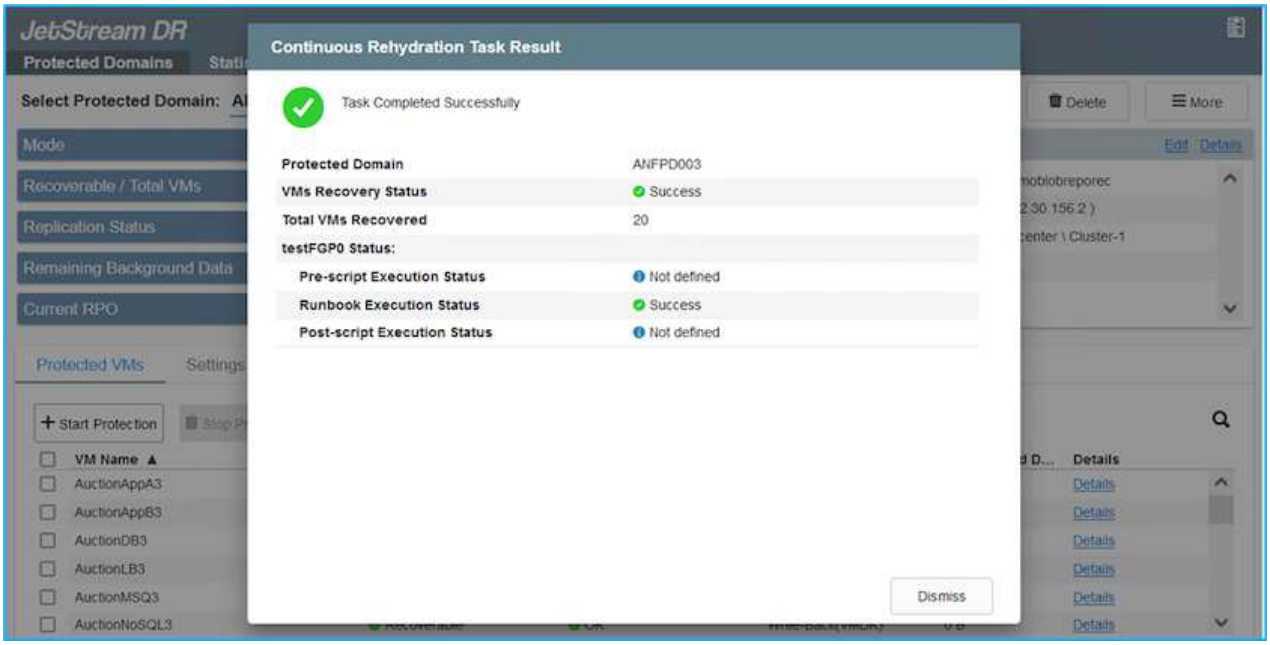
   保護対象のVMがAVSで起動されると、フェイルオーバー後（継続的または標準的なリハイドレート）、保護は自動的に再開され、JetStream DRは、Azure Blob Storage内の適切なコンテナまたは元のコンテナにデータをレプリケートし続けます。





タスクバーにフェイルオーバーアクティビティの進行状況が表示されます。

2. タスクが完了すると、リカバリされたVMとビジネスに通常どおりアクセスできます。

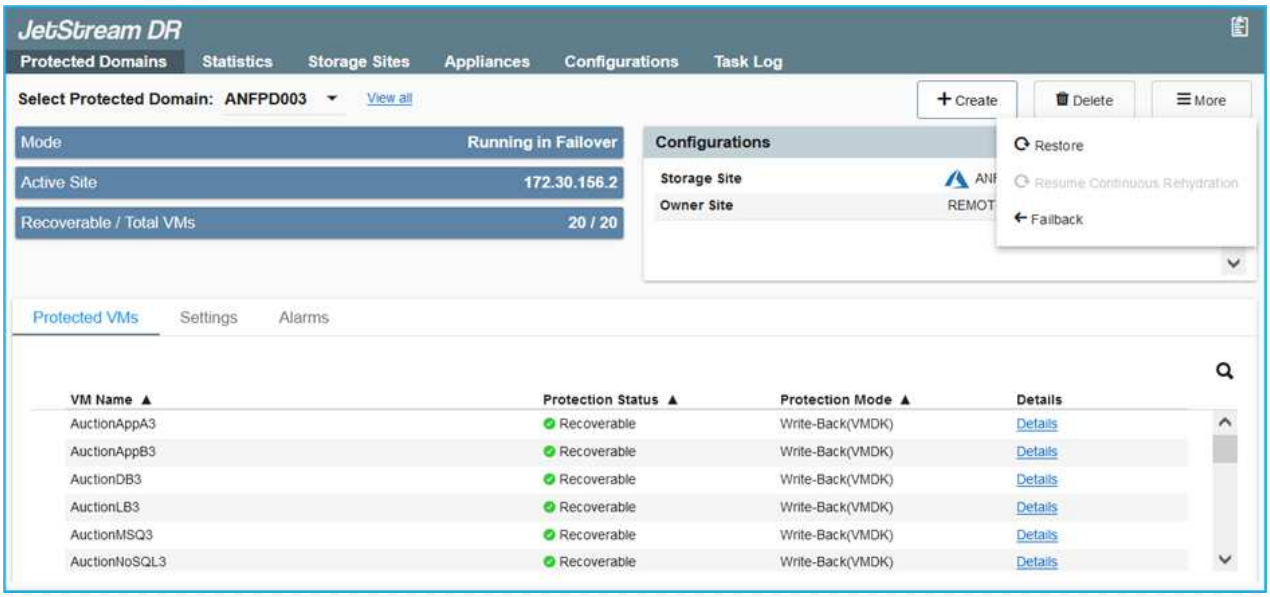


プライマリサイトが起動して再び実行されるようになったら、フェイルバックを実行できます。VM保護が再開され、データの整合性を確認する必要があります。

3. オンプレミス環境をリストア災害のタイプによっては、保護対象クラスタの構成をリストアまたは検証しなければならない場合があります。必要に応じて、JetStream DRソフトウェアを再インストールする必要があります。

> 注：Automation Toolkitで提供されている「recovery_utility_prepare_failback」スクリプトを使用すると、古いVMやドメイン情報などの元の保護サイトをクリーンアップできます。

4. リストアされたオンプレミス環境にアクセスし、Jetstream DR UIに移動して、適切な保護ドメインを選択します。保護サイトがフェイルバックできる状態になったら、UIで[Failback]オプションを選択します。



CPTで生成されたフェイルバックプランを使用して、VMとそのデータをオブジェクトストアから元のVMware環境に戻すこともできます。

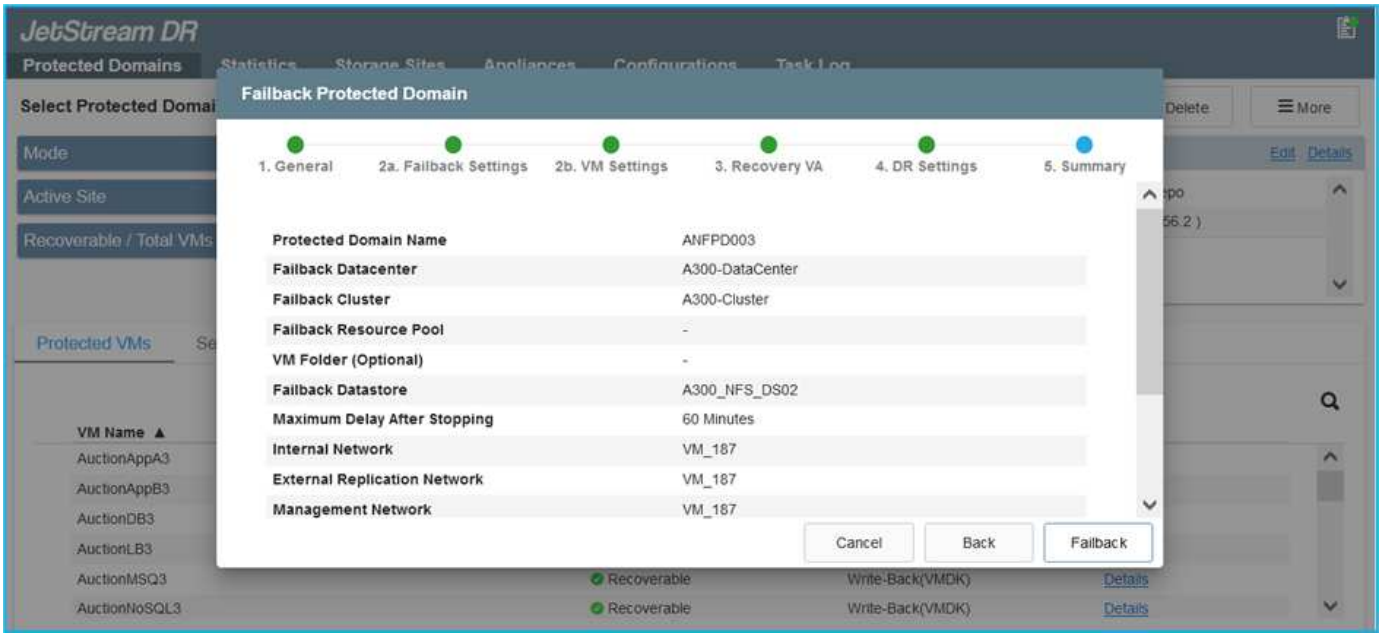
リカバリサイトのVMを一時停止して保護対象サイトで再起動したあとの最大遅延時間を指定します。この時間には、フェイルオーバーVMを停止したあとのレプリケーションの完了、リカバリサイトのクリーンアップにかかる時間、保護サイトでVMを再作成する時間などが含まれます。ネットアップの推奨値は10分です。

フェイルバックプロセスを完了し、VM保護およびデータの整合性が再開されたことを確認する。

Ransomware回復

ランサムウェアからのリカバリは困難な作業です。具体的には、IT組織にとって、返品の安全ポイントを特定することは困難です。また、復旧したワークロードを、（睡眠中のマルウェアや脆弱なアプリケーションによって）再発する攻撃から確実に保護する方法が決定された場合もあります。

Jetstream DR for AVSとAzure NetApp Files データストアを併用すると、組織が使用可能なポイントインタイムからリカバリできるため、ワークロードが機能的な分離されたネットワークに必要に応じてリカバリされるため、これらの問題に対処できます。リカバリを使用すると、アプリケーションが相互に機能して通信できるようになり、南北のトラフィックにさらされることがなくなります。その結果、セキュリティチームはフォレンジックなどの必要な修復を安全に実行できます。



CVOと**AVS**（ゲスト接続ストレージ）によるディザスタリカバリ

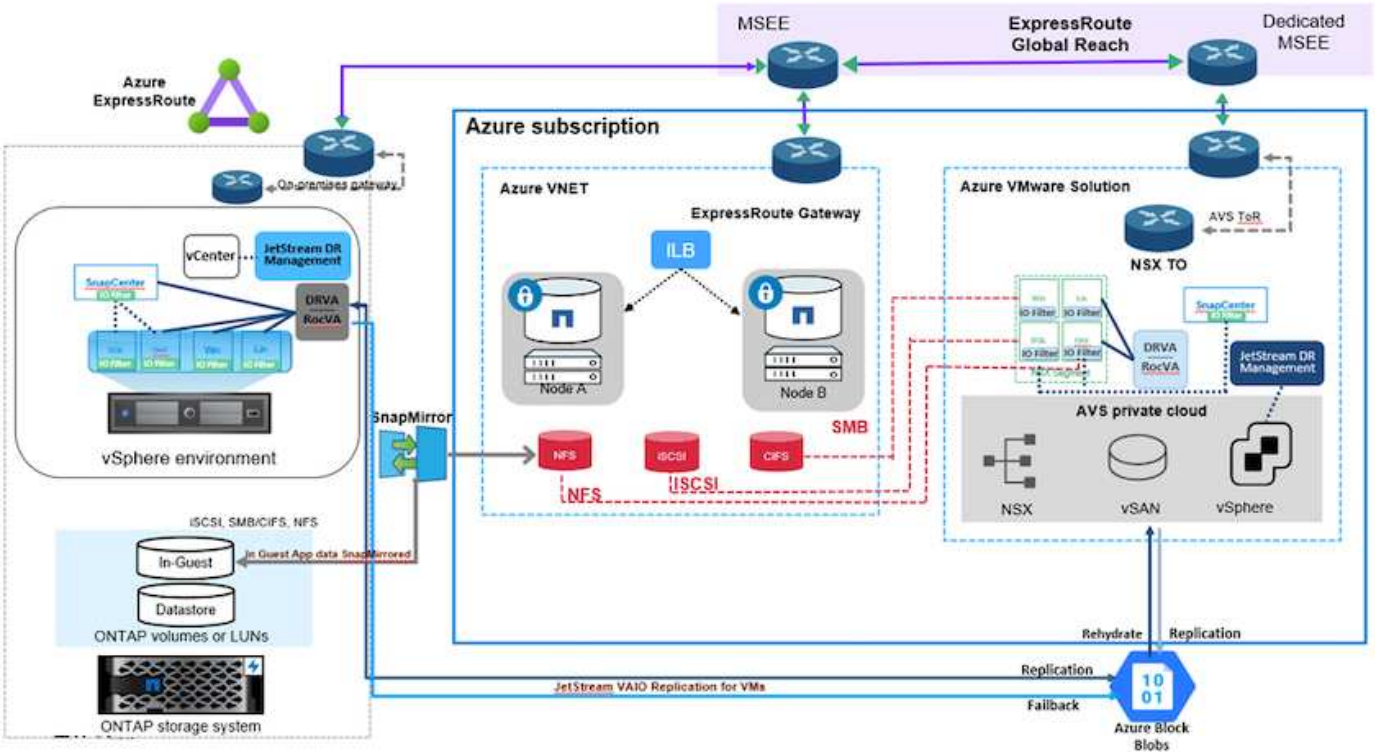
概要

著者：Ravi BCBとNiyaz Mohamedネットアップ

クラウドへのディザスタリカバリは、耐障害性と対費用効果に優れた方法で、サイトの停止やランサムウェアなどのデータ破損からワークロードを保護します。NetApp SnapMirrorを使用すると、ゲスト接続ストレージを使用するオンプレミスのVMwareワークロードを、Azure内で実行されているNetApp Cloud Volumes ONTAP にレプリケートできます。これはアプリケーションデータに適用されますが、実際のVM自体につい

てはどうでしょうか。ディザスタリカバリは、仮想マシン、VMDK、アプリケーションデータなど、依存するすべてのコンポーネントを対象にする必要があります。これを実現するために、JetstreamとSnapMirrorを併用すると、VM VMDK用のVSANストレージを使用しながら、オンプレミスからCloud Volumes ONTAP にレプリケートされたワークロードをシームレスにリカバリできます。

本ドキュメントでは、NetApp SnapMirror、JetStream、およびAzure VMware解決策 （AVS）を使用してディザスタリカバリを設定および実行するためのステップバイステップ形式のアプローチを紹介します。



前提条件

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

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

オンプレミス環境とAzure Virtual Network間の接続には、エクスプレスルートグローバルリーチまたはVPNゲートウェイを使用した仮想WANを使用します。オンプレミスVLANの設計に基づいてセグメントを作成する必要があります。

オンプレミスのデータセンターをAzureに接続する方法は複数ありますが、これにより、本ドキュメントの特定のワークフローの概要がわかりません。適切なオンプレミスからAzureへの接続方法については、Azureのドキュメントを参照してください。

DR解決策 の導入

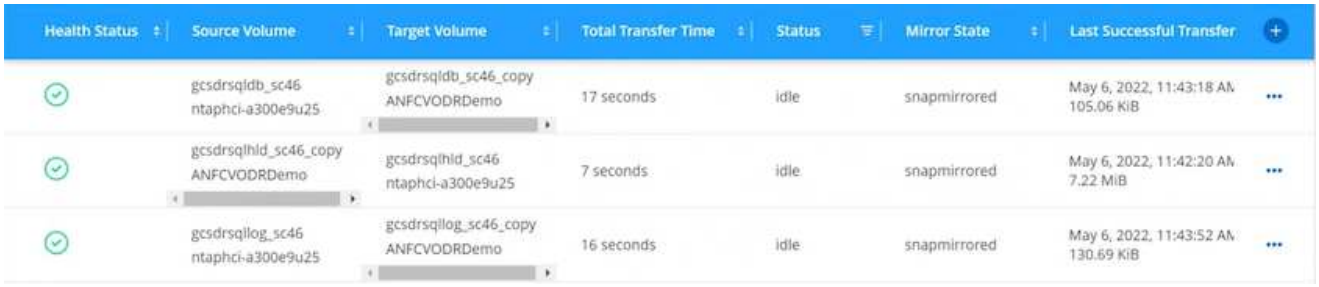
解決策 の導入の概要

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

展開の詳細

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

まず、AzureでCloud Volumes ONTAPを設定します（"リンク"）をクリックし、必要なボリュームを、必要な頻度とSnapshotの保持を使用してCloud Volumes ONTAP にレプリケートします。



AVSホストと**CVO**データアクセスを設定

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

AVSクラスタを導入するかどうかは、主にRPOとRTOの要件に基づきます。Azure VMware解決策 では、テストや実際の災害に備えて、SDDCを随時プロビジョニングできます。SDDCを時間内に導入することで、災害に対処しない場合のESXiホストのコストを削減できます。ただし、このような導入形態では、SDDCのプロビジョニングに数時間かかるRTOが影響を受けます。

最も一般的な導入オプションは、SDDCを常時稼働のパイロットライトモードで実行することです。このオプションを使用すると、常に使用可能なホストを3台分のスペースに縮小できます。また、シミュレーションアクティビティとコンプライアンスチェックのベースラインを実行できるため、本番サイトとDRサイト間の運用のずれを回避できるため、リカバリ処理の時間を短縮できます。パイロットライトクラスタは、実際のDRイベントを処理する必要がある場合に、必要なレベルまで迅速に拡張できます。

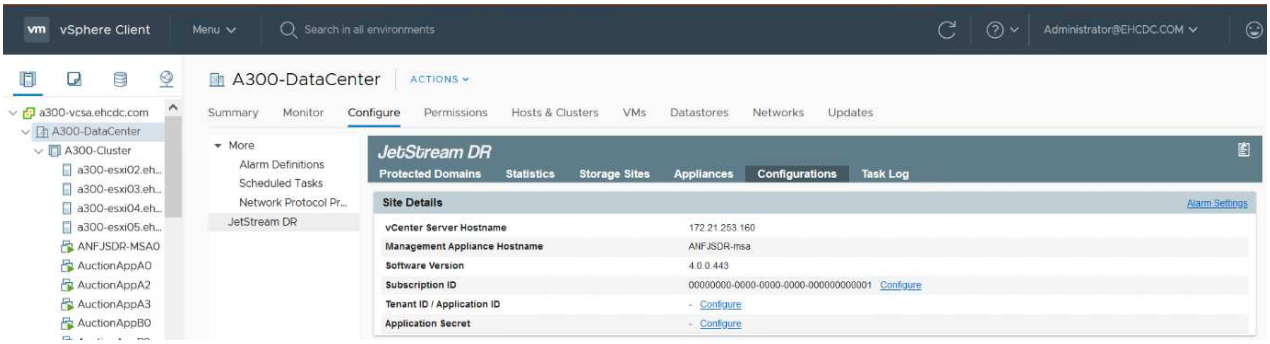
AVS SDDCを設定するには（オンデマンドモードまたはパイロットライトモード）、を参照してください "Azure に仮想化環境を導入して設定"。事前に、接続の確立後、AVSホストに常駐するゲストVMがCloud Volumes ONTAP からデータを消費できることを確認してください。

Cloud Volumes ONTAP とAVSを適切に設定したら、VAIOメカニズムを使用し、Cloud Volumes ONTAPへのアプリケーションボリュームのコピーにSnapMirrorを利用することにより、オンプレミスワークロードからAVSへのリカバリ（アプリケーションVMDKとゲストストレージを搭載したVM）を自動化するようにJetstreamを設定します。

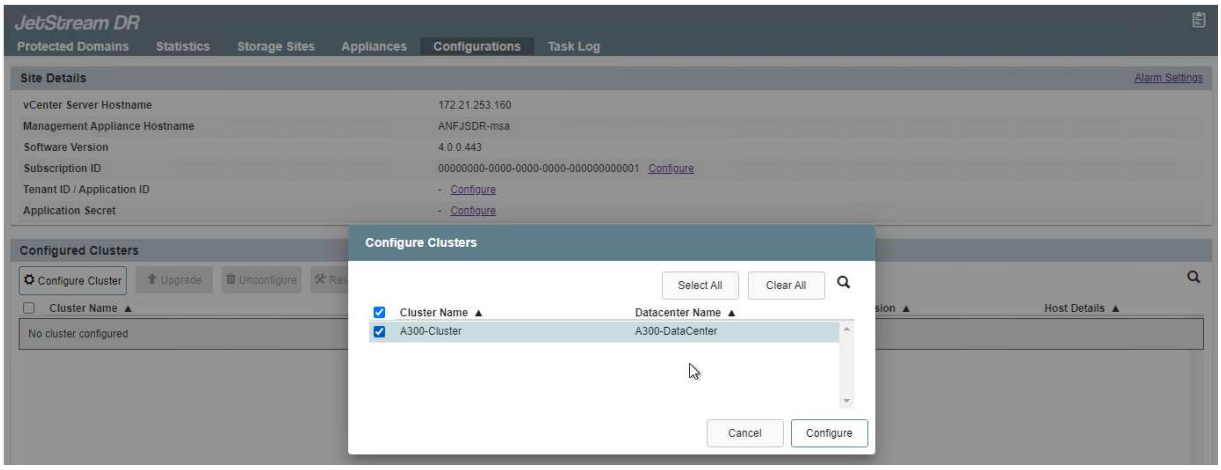
JetStream DRをオンプレミスデータセンターにインストールします

Jetstream DRソフトウェアは、JetStream DR Management Server Virtual Appliance（MSA）、DR Virtual Appliance（DRVA）、およびホストコンポーネント（I/Oフィルタパッケージ）の3つの主要コンポーネントで構成されています。MSAは、コンピューティングクラスタにホストコンポーネントをインストールおよび構成し、JetStream DRソフトウェアを管理するために使用されます。インストールプロセスは次のとおりです。

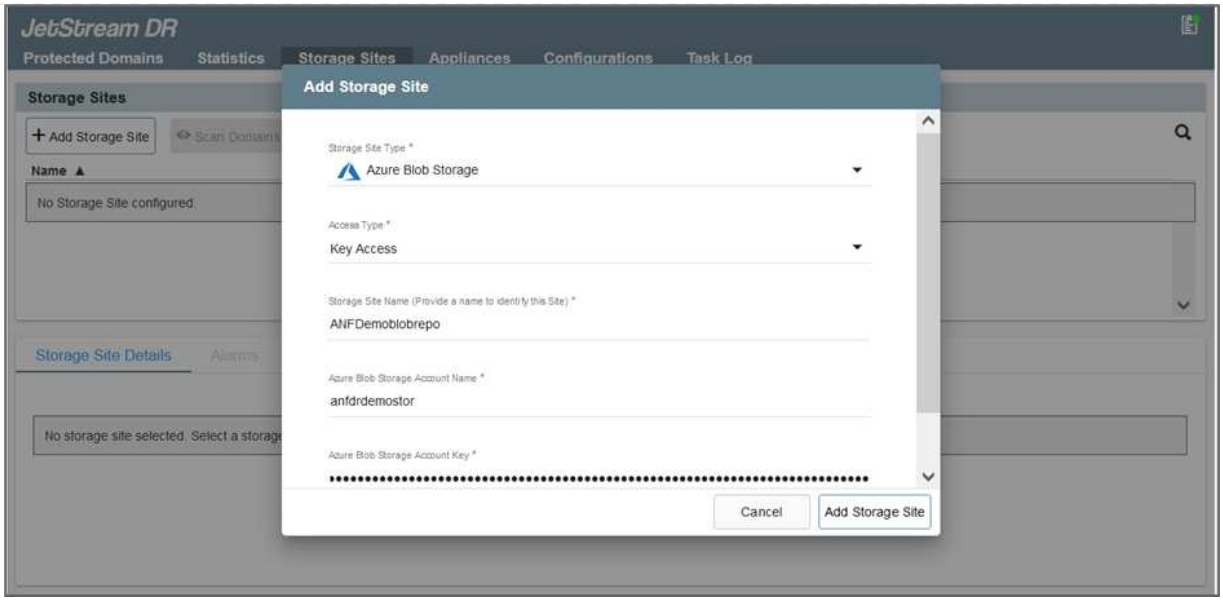
1. 前提条件を確認します。
2. リソースと構成に関する推奨事項については、Capacity Planning Toolを実行してください。
3. JetStream DR MSAを、指定されたクラスタ内の各vSphereホストに導入します。
4. ブラウザでDNS名を使用してMSAを起動します。
5. vCenterサーバをMSAに登録します。
6. JetStream DR MSAが導入され、vCenter Serverが登録されたら、vSphere Web ClientでJetStream DRプラグインに移動します。これを行うには、[データセンター]>[設定]>[JetStream DR]に移動します。



7. JetStream DRインターフェイスから、次の作業を行います。
   a. I/Oフィルタパッケージを使用してクラスタを設定します。

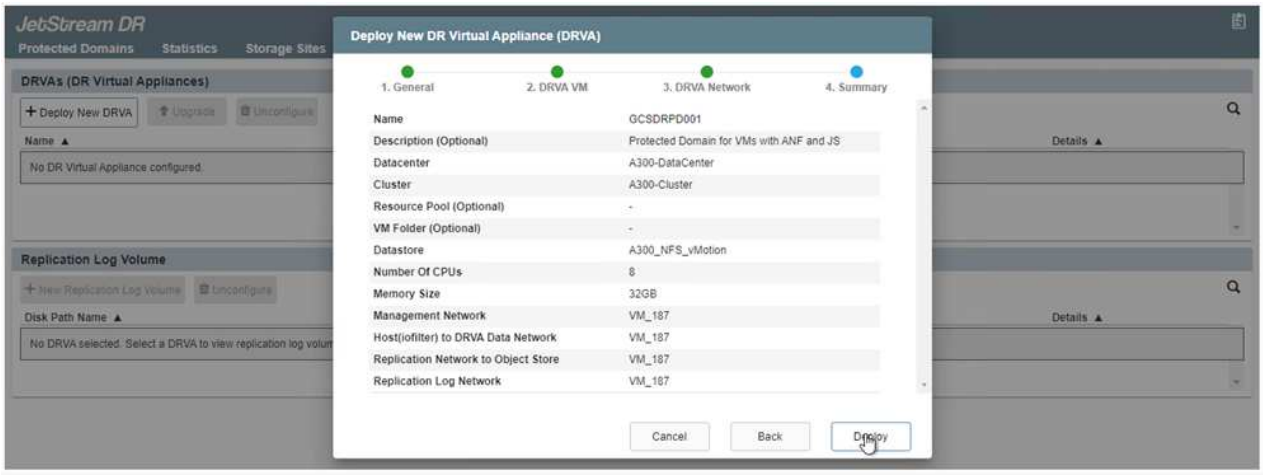


   b. リカバリサイトにあるAzure BLOBストレージを追加します。

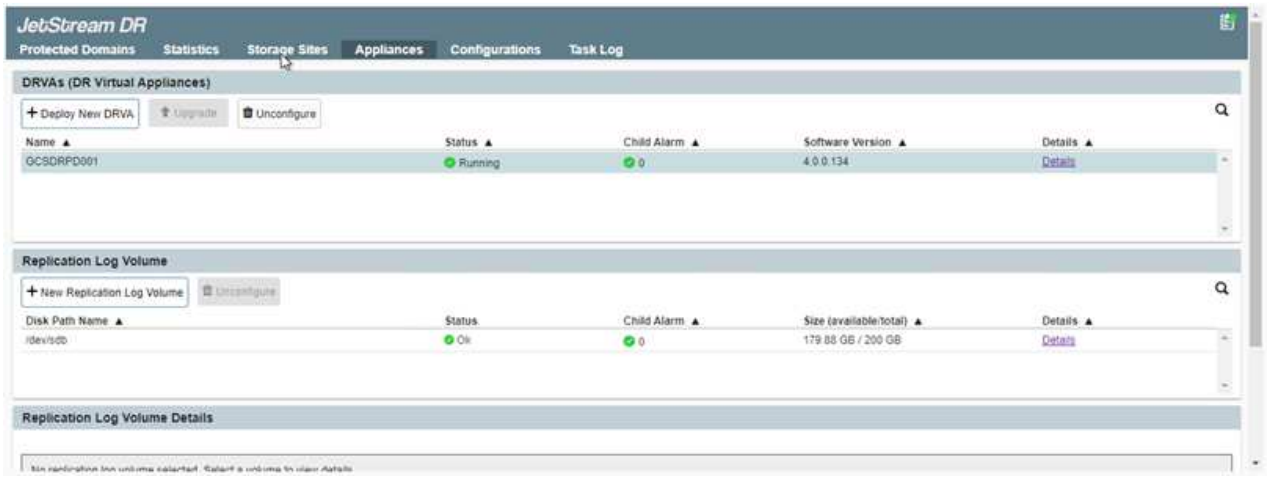


8. アプライアンスタブから必要な数のDR仮想アプライアンス（DRVA）を導入します。

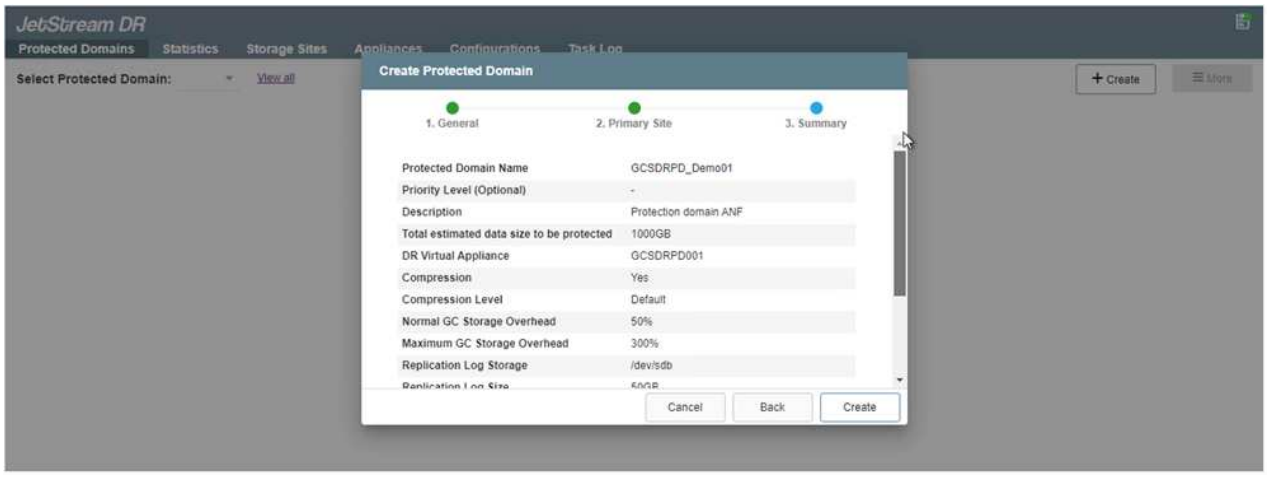
   キャパシティプランニングツールを使用して、必要なDRVAの数を見積もります。

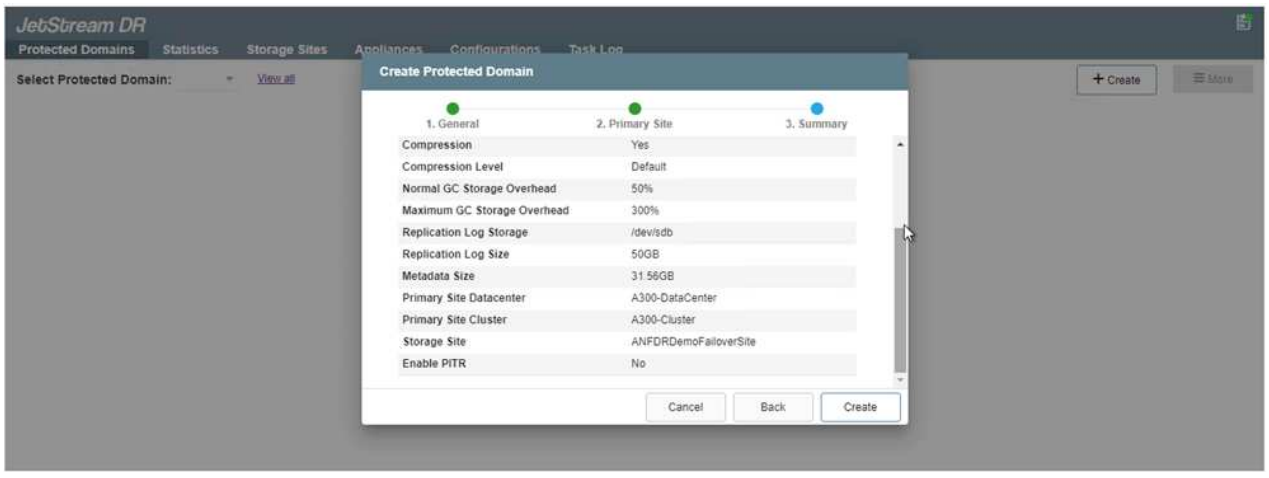


9. 使用可能なデータストアまたは独立した共有iSCSIストレージプールからVMDKを使用して、各DRVAのレプリケーションログボリュームを作成します。



10. Protected Domainsタブで、Azure Blob Storageサイト、DRVAインスタンス、およびレプリケーションログに関する情報を使用して、必要な数の保護ドメインを作成します。保護ドメインは、クラスタ内の特定のVMまたはアプリケーションVMのセットを定義します。これらのVMは一緒に保護され、フェイルオーバー/フェイルバック処理の優先順位が割り当てられます。

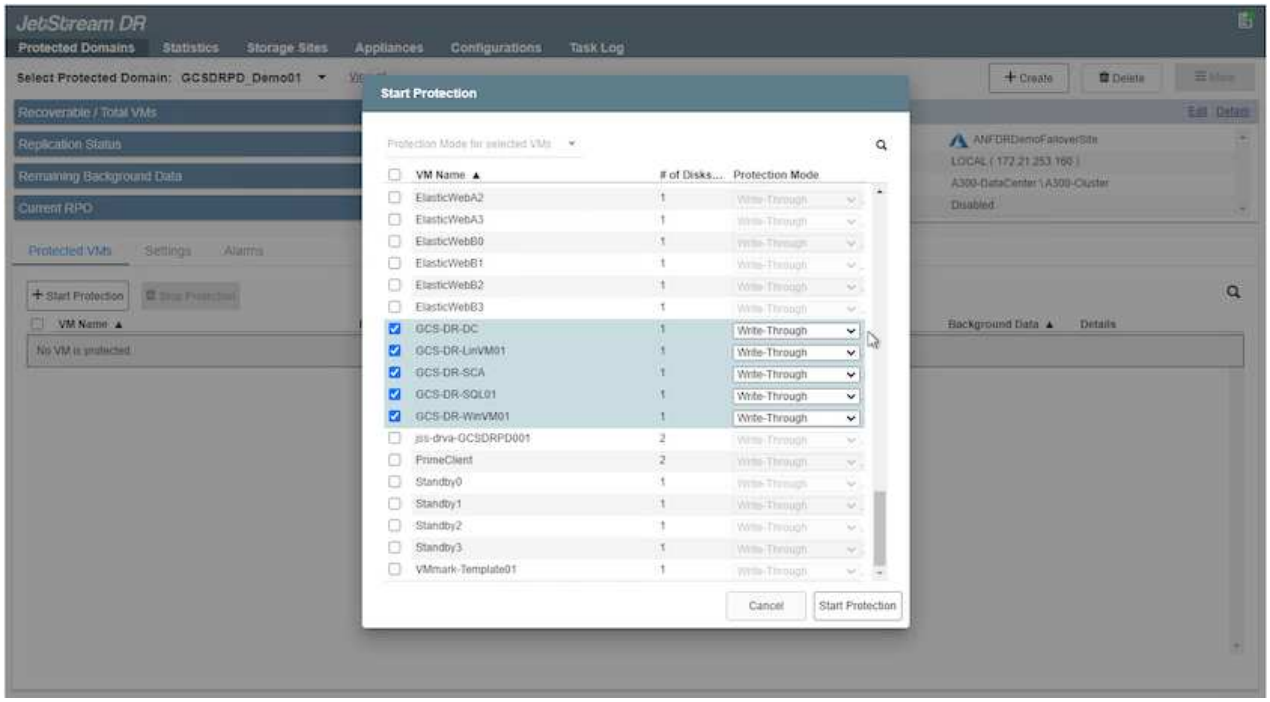




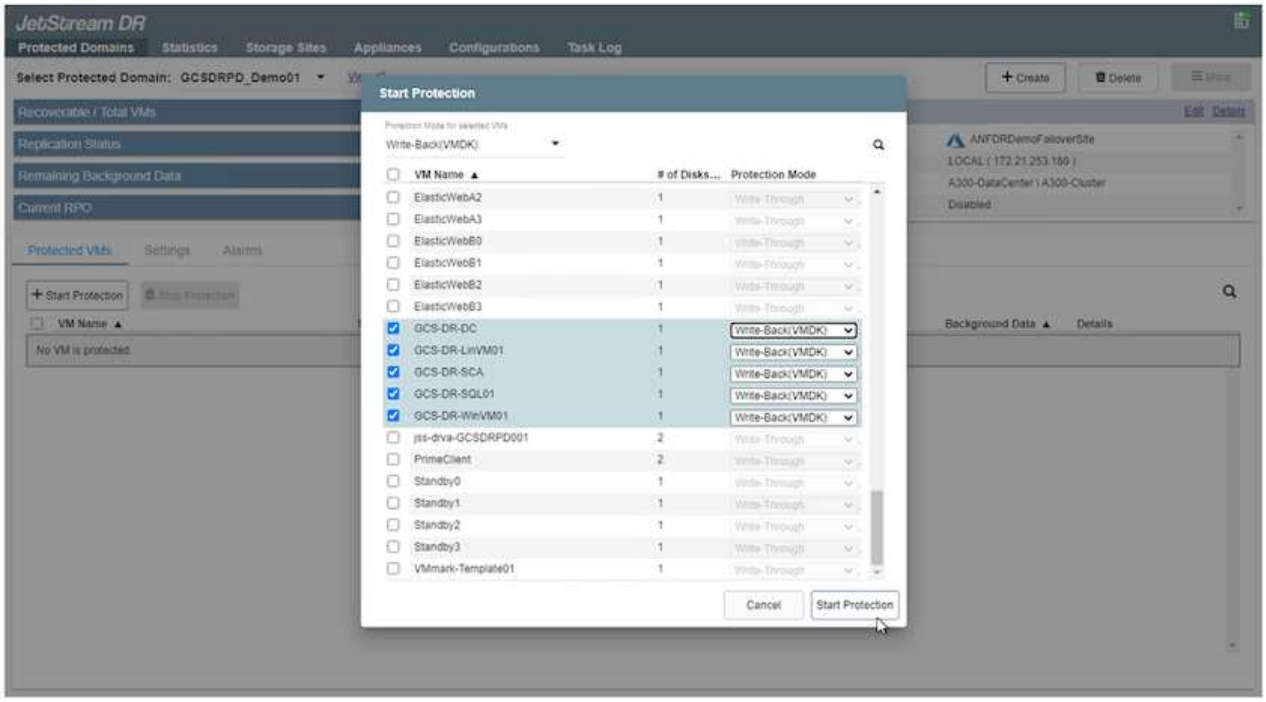
11. 保護するVMを選択し、依存関係に基づいてVMをアプリケーショングループにグループ化します。アプリケーション定義を使用すると、VMのセットを、ブート順序、ブート遅延、およびリカバリ時に実行可能なオプションのアプリケーション検証を含む論理グループにグループ化できます。

保護ドメイン内のすべてのVMに同じ保護モードを使用していることを確認します。

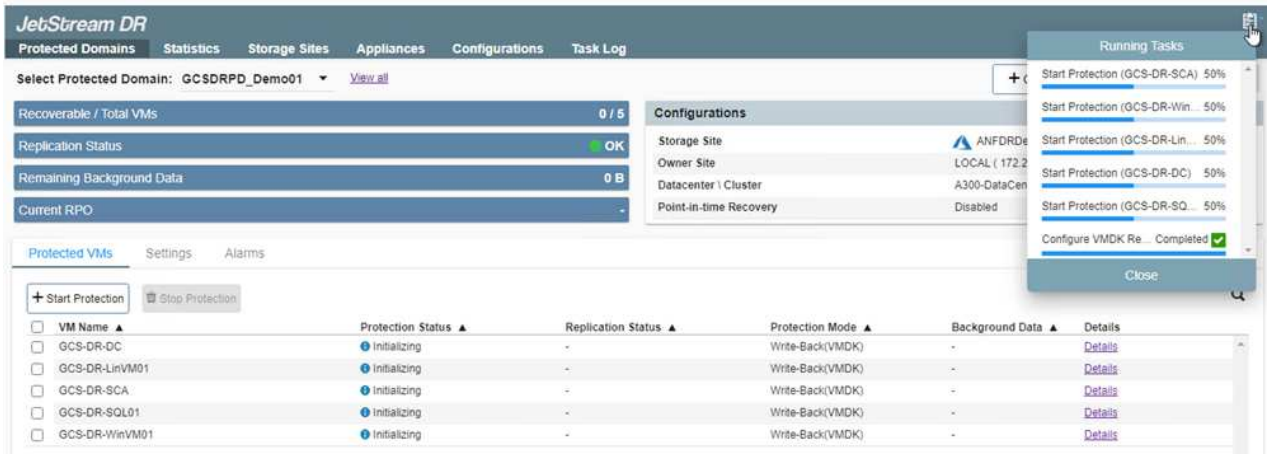
ライトバック（VMDK）モードを使用すると、パフォーマンスが向上します。



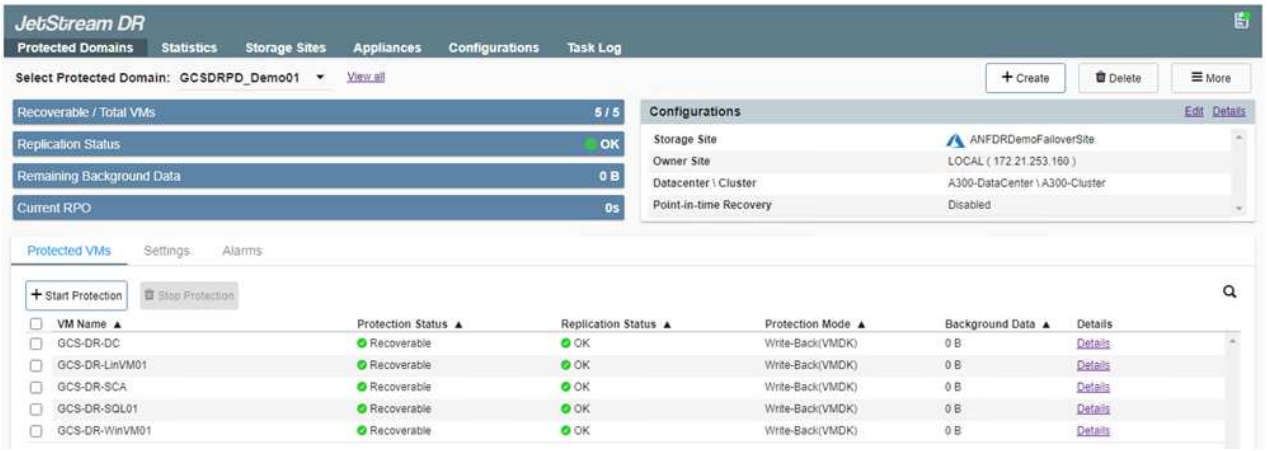
12. レプリケーションログボリュームがハイパフォーマンスストレージに配置されていることを確認します。



13. 完了したら、保護ドメインの保護の開始をクリックします。選択したVMのデータレプリケーションが開始され、指定したBLOBストアに送信されます。



14. レプリケーションが完了すると、VMの保護ステータスは「回復可能」とマークされます。

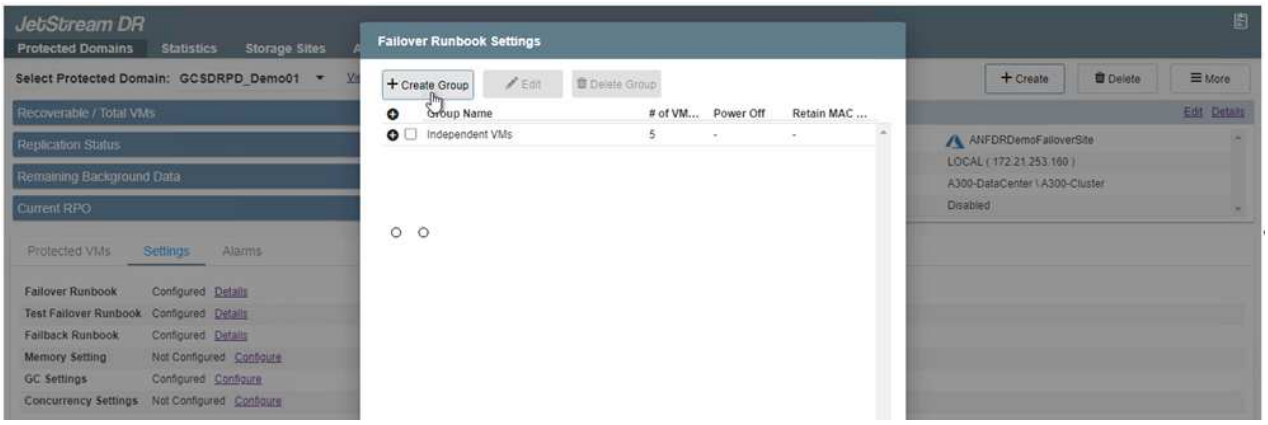


フェールオーバーランブックは、VM（回復グループと呼ばれる）をグループ化し、起動順序シーケンスを設定して、CPU /メモリ設定とIP設定を変更するように構成できます。

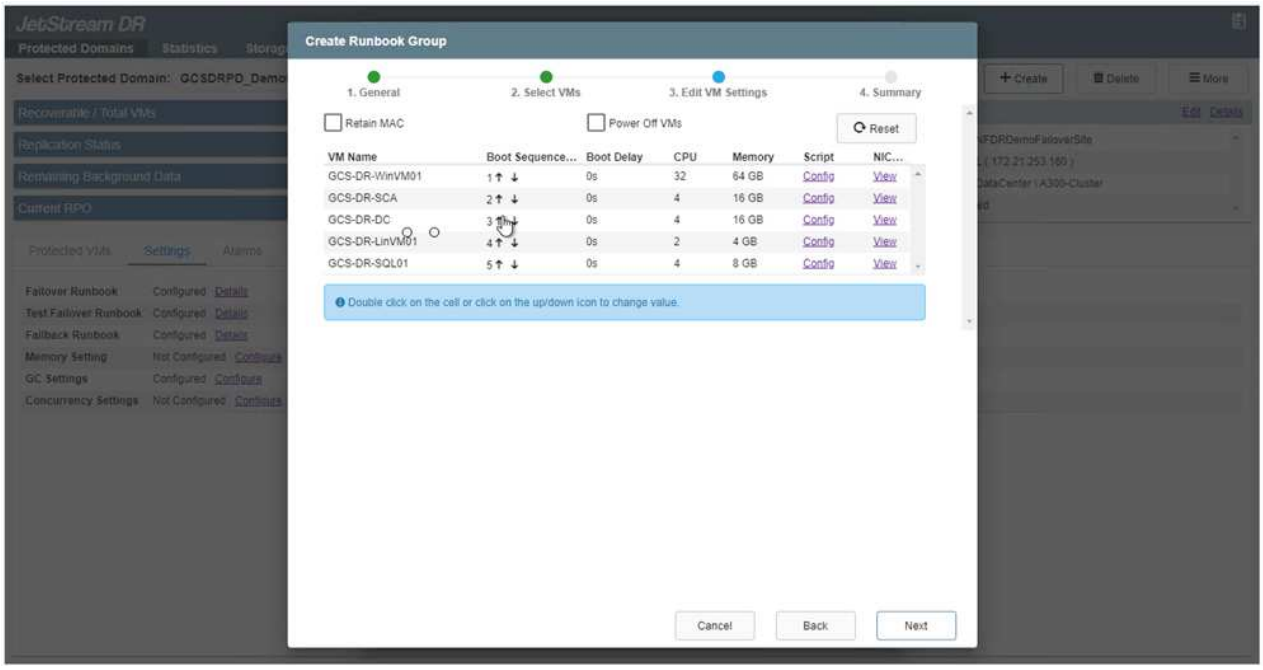
15. 「設定」をクリックし、「Runbook設定」リンクをクリックして、Runbookグループを設定します。

16. [グループの作成]ボタンをクリックして、新しいランブックグループの作成を開始します。

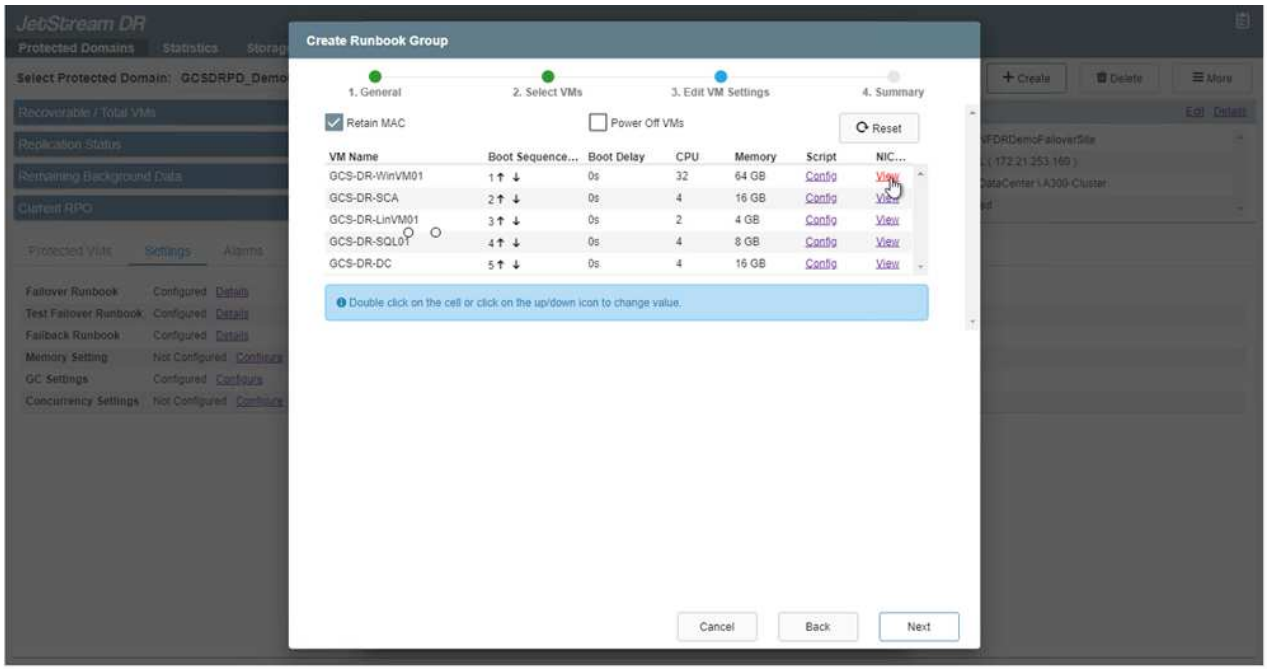
必要に応じて、画面の下部で、カスタムのプレスクリプトとポストスクリプトを適用して、ランブックグループの操作前および操作後に自動的に実行します。Runbookスクリプトが管理サーバ上に存在することを確認します。



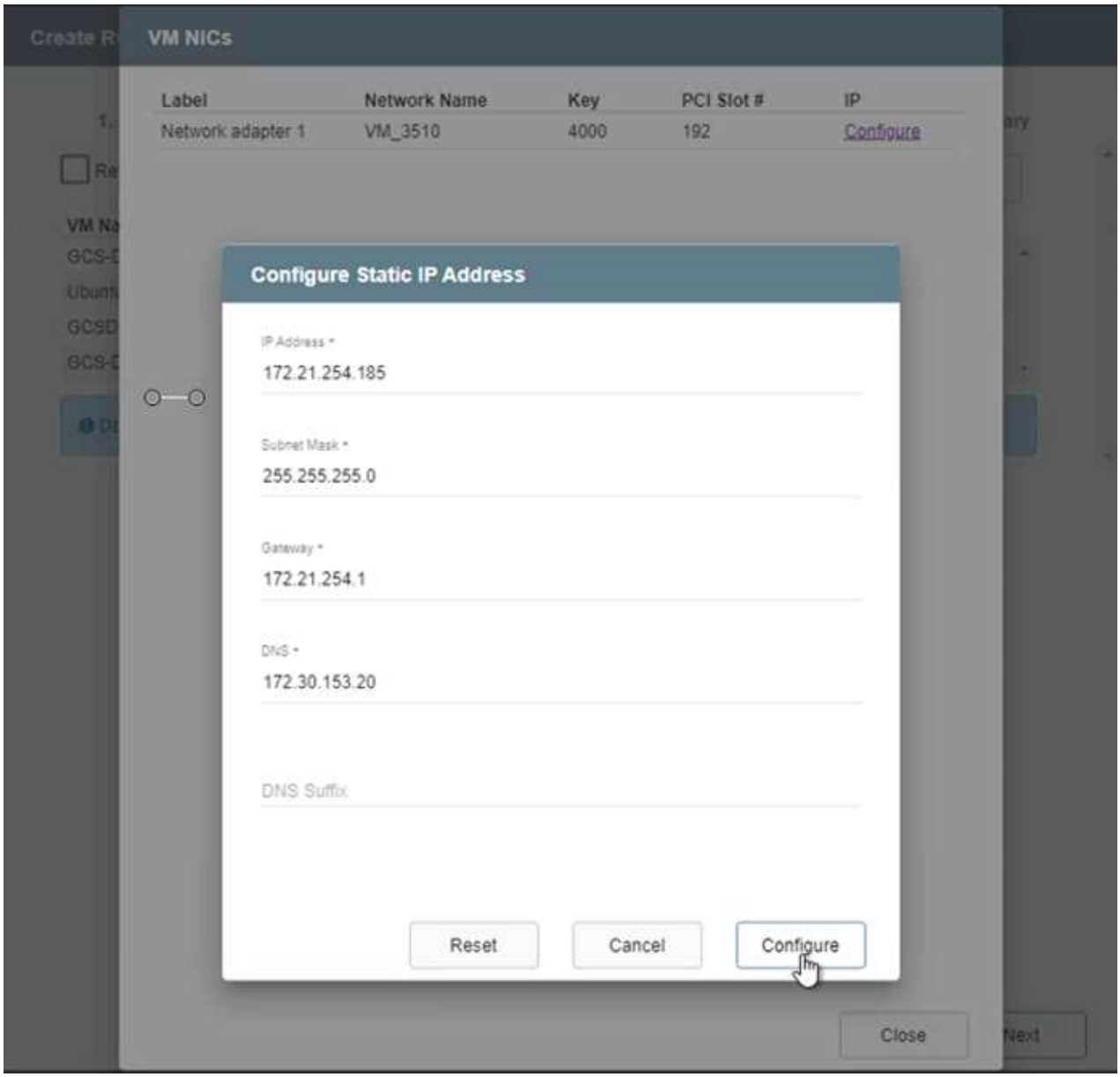
17. 必要に応じてVMの設定を編集します。VMをリカバリするためのパラメータを指定します。これには、ブートシーケンス、ブート遅延（秒単位）、CPUの数、割り当てるメモリの量などが含まれます。上下の矢印をクリックして、VMのブートシーケンスを変更します。MACを保持するためのオプションも用意されています。

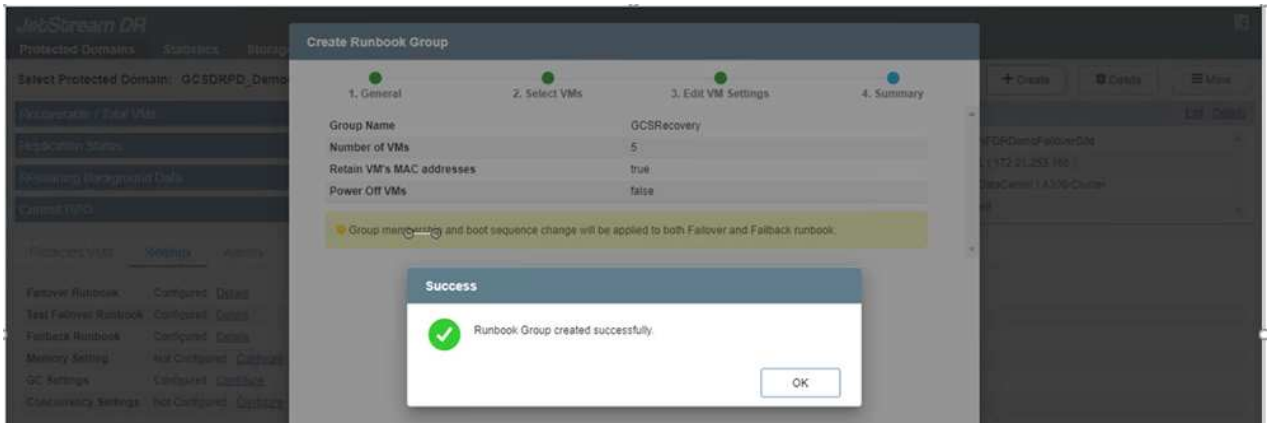


18. 静的IPアドレスは、グループの個々のVMに手動で設定できます。VMのNICビューリンクをクリックして、IPアドレスを手動で設定します。



19. Configureボタンをクリックして、それぞれのVMのNIC設定を保存します。





フェイルオーバーとフェイルバックの両方のランブックのステータスが構成済みとして表示されるようになりました。フェイルオーバーとフェイルバックのRunbookグループは、同じVMと設定の初期グループを使用してペアで作成されます。必要に応じて、それぞれの[詳細]リンクをクリックして変更を行うことで、ランブックグループの設定を個別にカスタマイズできます。

リカバリサイト（AVS）では、3ノードのパイロットライトクラスタを事前に作成することを推奨します。これにより、以下を含むリカバリサイトのインフラを事前に設定できます。

- 宛先ネットワークセグメント、ファイアウォール、DHCPやDNSなどのサービスなど
- AVS対応のJetStream DRのインストール
- ANFボリュームをデータストアなどとして設定

Jetstream DRは、ミッションクリティカルなドメインでほぼゼロのRTOモードをサポートします。これらのドメインには、デスティネーションストレージが事前にインストールされている必要があります。この場合、ANFは推奨ストレージタイプです。

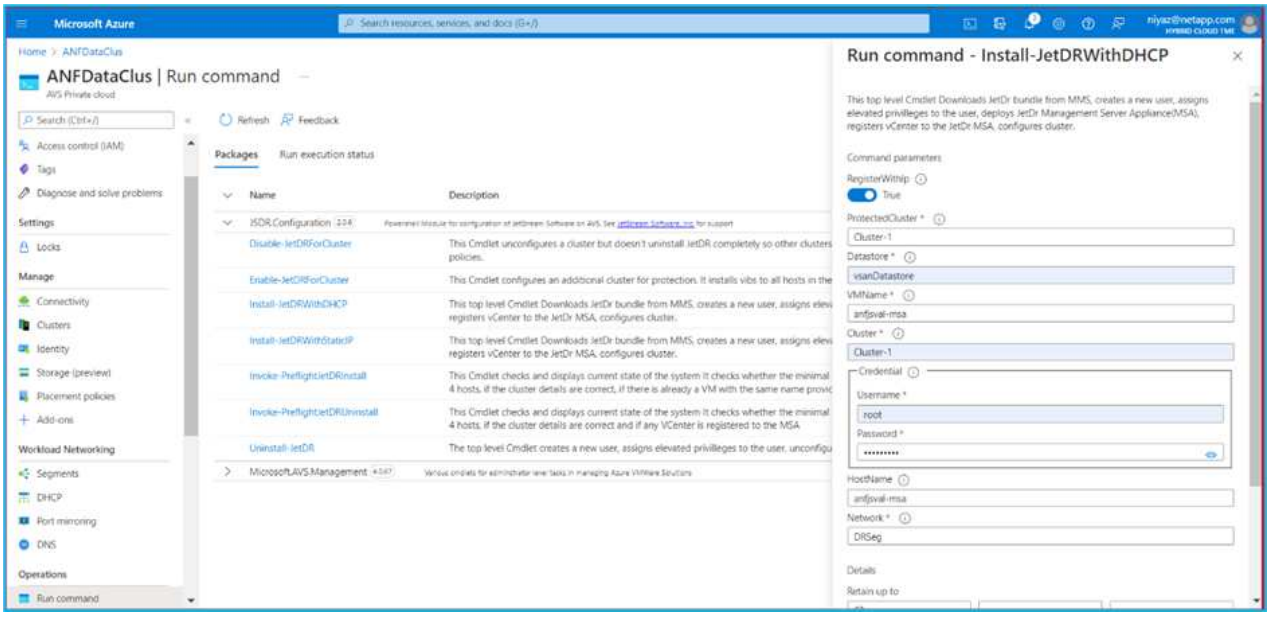
セグメント作成を含むネットワーク構成は、オンプレミスの要件に合わせてAVSクラスタ上で設定する必要があります。

SLAやRTOの要件に応じて、継続的フェイルオーバーモードまたは通常の（標準）フェイルオーバーモードを使用できます。RTOがほぼゼロになるように、リカバリサイトで継続的なリハイドレートを開始する必要があります。

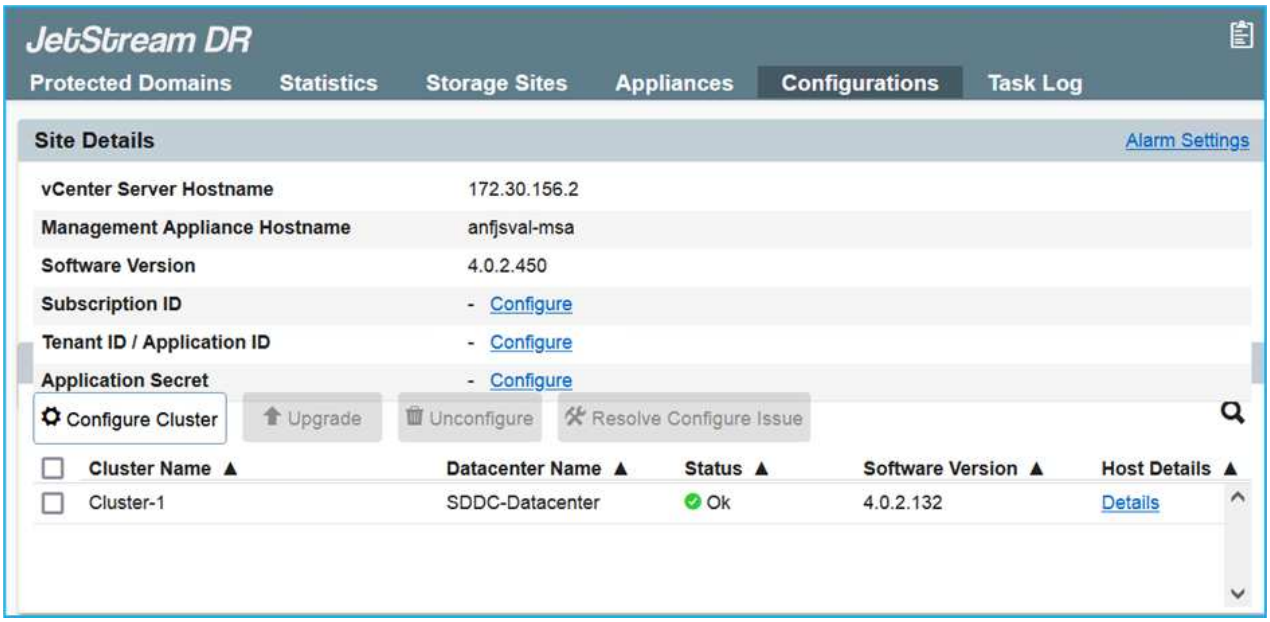
1. Azure VMware解決策 プライベートクラウドにJetStream DR for AVSをインストールするには、実行コマンドを使用します。Azureポータルで、Azure VMware解決策 に移動し、プライベートクラウドを選択して、実行コマンド>パッケージ> JSDR.Configurationを選択します。

   Azure VMware解決策 のデフォルトCloudAdminユーザには、AVS対応のJetStream DRをインストールするための十分な権限がありません。Azure VMware解決策 では、JetStream DR用のAzure VMware解決策 実行コマンドを呼び出すことで、JetStream DRのインストールを簡単かつ自動化できます。

   次のスクリーンショットは、DHCPベースのIPアドレスを使用したインストール方法を示しています。



2. JetStream DR for AVSのインストールが完了したら、ブラウザをリフレッシュします。JetStream DR UIにアクセスするには、SDDC Datacenter > Configure > JetStream DRに移動します。



3. JetStream DRインターフェイスから、次の作業を行います。

   a. オンプレミスクラスタをストレージサイトとして保護するために使用したAzure Blob Storageアカウントを追加し、Scan Domainsオプションを実行します。

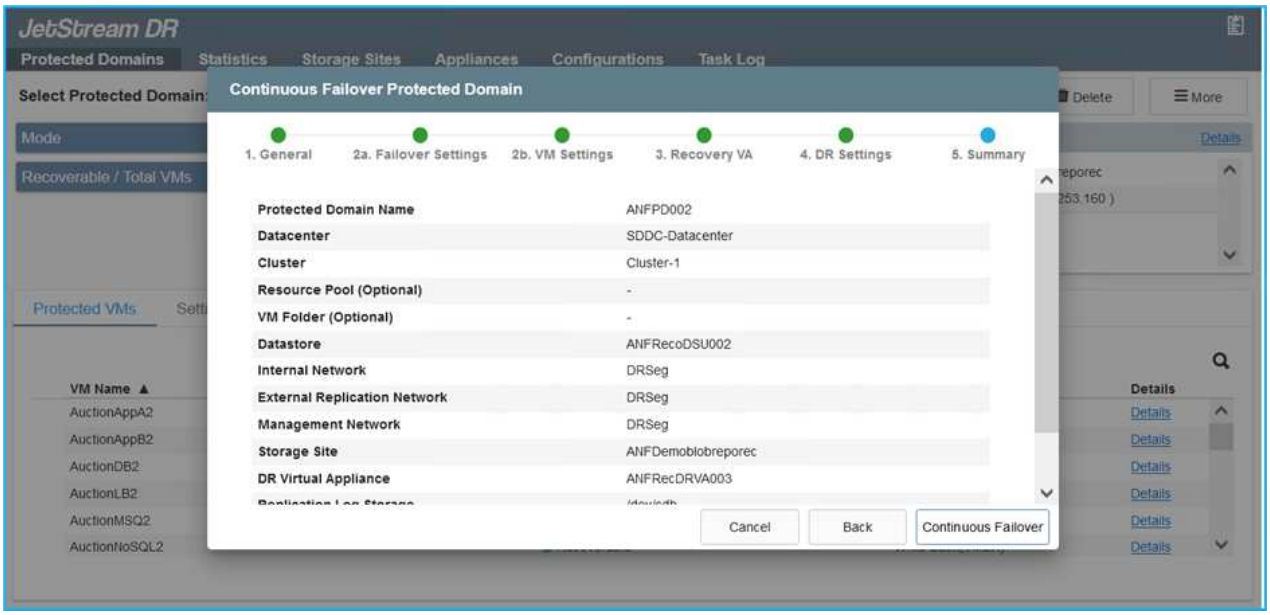
   b. 表示されるポップアップダイアログで、インポートする保護ドメインを選択し、そのインポートリンクをクリックします。

4. ドメインがリカバリ用にインポートされます。[保護ドメイン]タブに移動して、目的のドメインが選択されていることを確認するか、[保護ドメインの選択]メニューから目的のドメインを選択します。保護ドメイン内のリカバリ可能なVMのリストが表示されます。

5. 保護ドメインをインポートしたら、DRVAアプライアンスを展開します。

これらの手順は、CPT作成プランを使用して自動化することもできます。

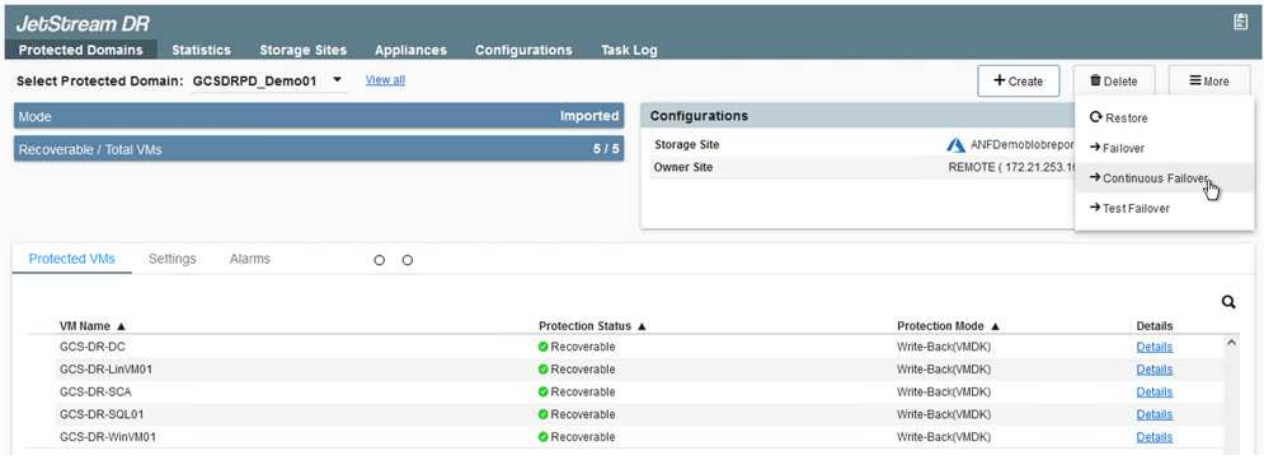
6. 使用可能なvSANまたはANFデータストアを使用してレプリケーションログボリュームを作成します。
7. 保護ドメインをインポートし、VMの配置にANFデータストアを使用するようにリカバリVAを設定します。



選択したセグメントでDHCPが有効になっていて、十分なIPが使用可能であることを確認します。ダイナミックIPは、ドメインのリカバリ中に一時的に使用されます。リカバリVM（連続リハイドレートを含む）ごとに、個別のダイナミックIPが必要です。リカバリの完了後、IPは解放され、再利用できます。

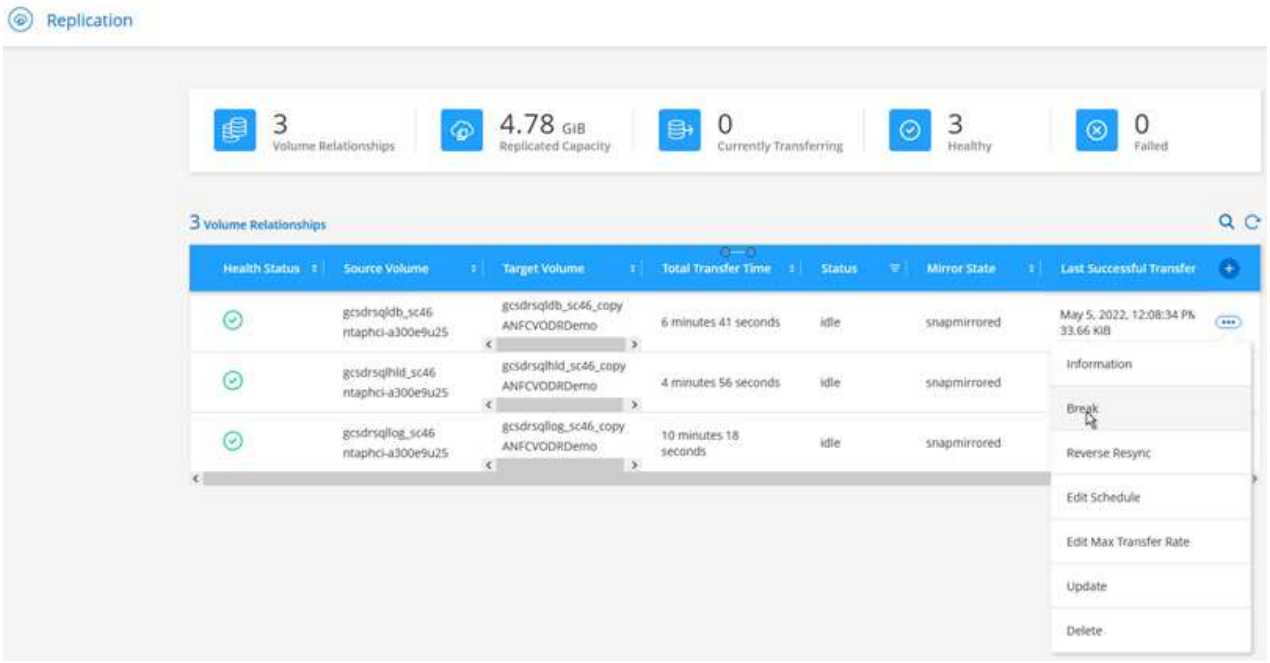
8. 適切なフェイルオーバーオプション（継続的フェイルオーバーまたはフェイルオーバー）を選択します。この例では、連続リハイドレート（連続フェールオーバー）が選択されています。

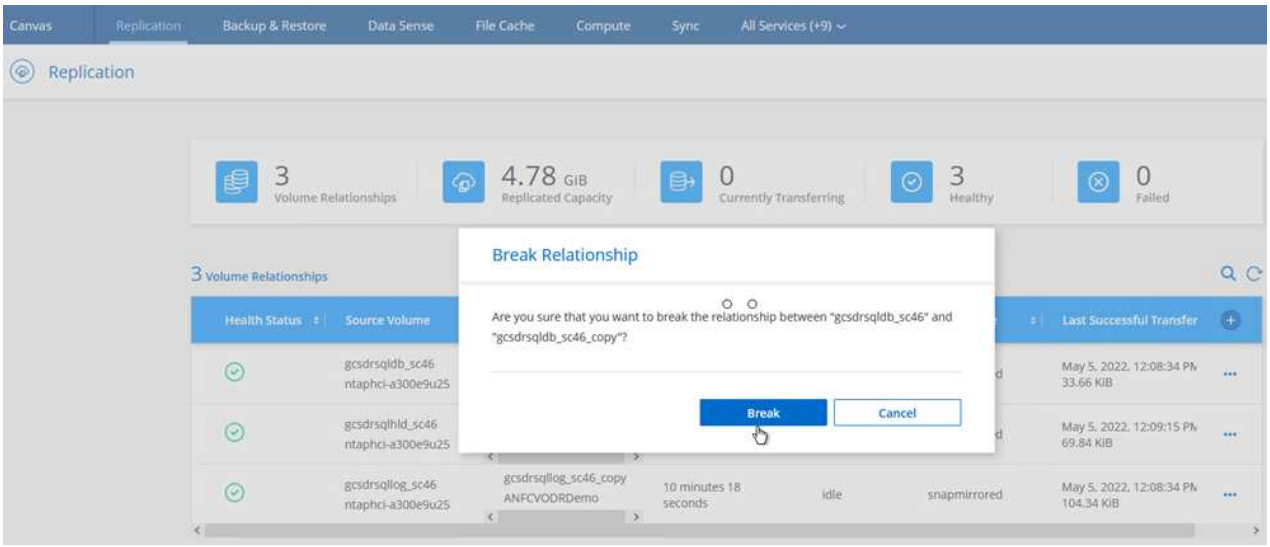
設定の実行時には、継続的フェイルオーバーモードとフェイルオーバーモードが異なりますが、両方のフェイルオーバーモードを同じ手順で設定します。フェイルオーバー手順は、災害発生時の対応として一緒に設定および実行されます。継続的フェイルオーバーはいつでも設定でき、通常のシステム運用中はバックグラウンドで実行できます。災害が発生すると、継続的なフェイルオーバーが完了し、保護対象のVMの所有権がリカバリサイトにただちに移行されます（RTOはほぼゼロ）。



継続的なフェイルオーバープロセスが開始され、UIから進行状況を監視できます。[現在のステップ]セクションの青いアイコンをクリックすると、ポップアップウィンドウが開き、フェイルオーバープロセスの現在のステップの詳細が表示されます。

1. オンプレミス環境の保護対象クラスタで障害が発生した場合（部分的または完全な障害）、該当するアプリケーションボリュームのSnapMirror関係を解除したあと、Jetstreamを使用してVMのフェイルオーバーをトリガーできます。

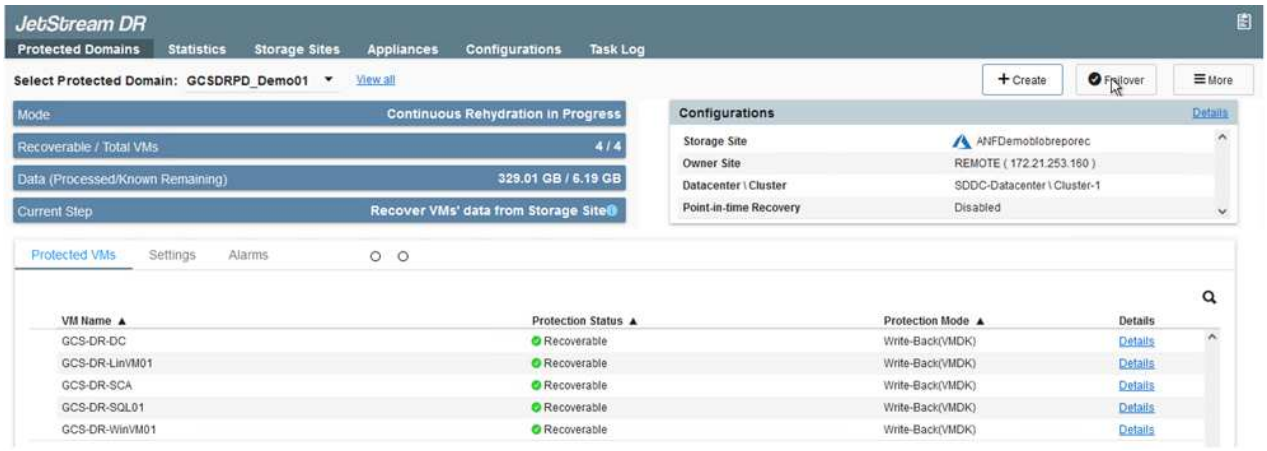


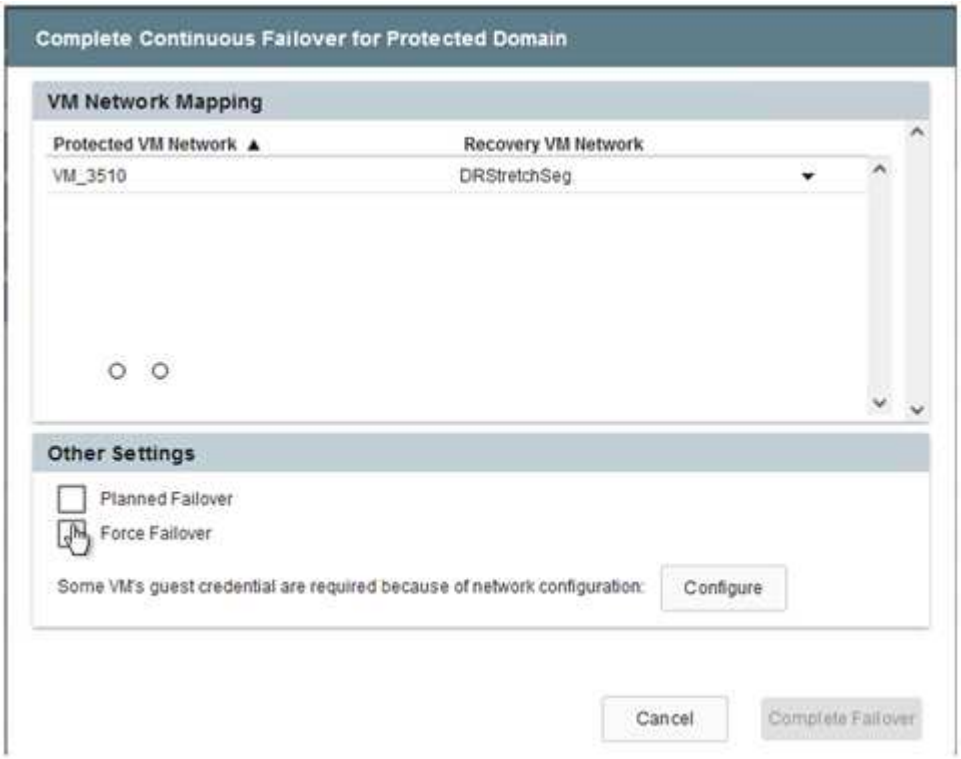


この手順は簡単に自動化できるため、リカバリプロセスが容易になります。

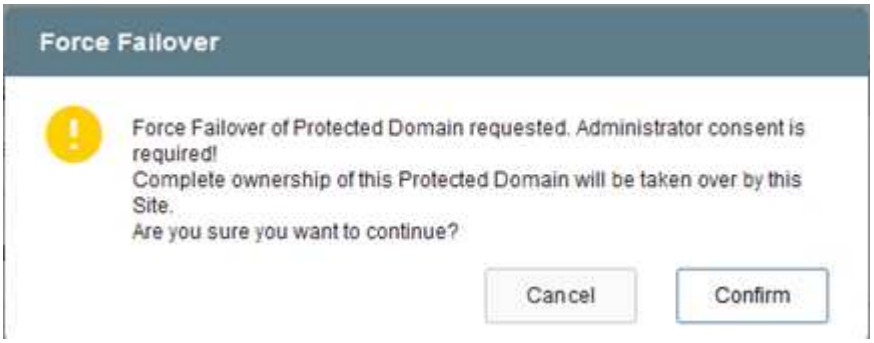
2. AVS SDDC（宛先側）上のJetstream UIにアクセスし、フェールオーバーオプションをトリガしてフェールオーバーを完了します。タスクバーにフェイルオーバーアクティビティの進行状況が表示されます。

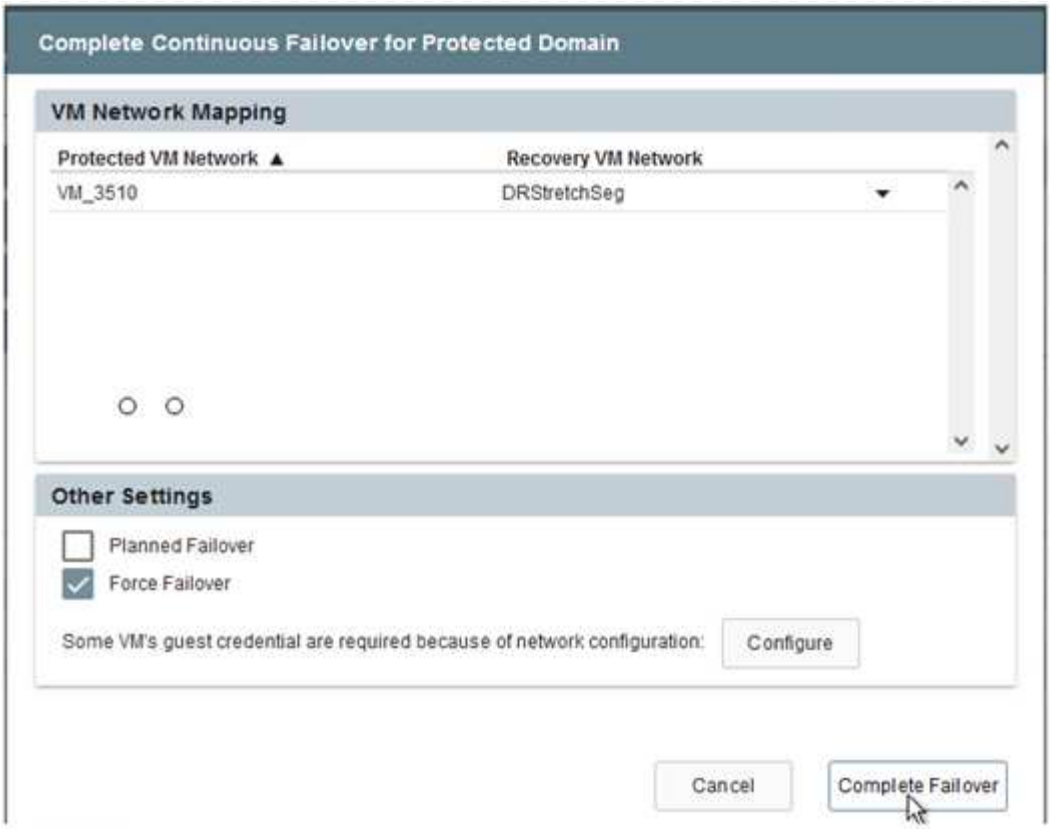
   フェイルオーバーが完了したときに表示されるダイアログウィンドウで、フェイルオーバータスクを計画どおりに指定することも、強制的に実行することもできます。





強制フェイルオーバーでは、プライマリサイトがアクセス不能になり、保護ドメインの所有権がリカバリサイトによって直接引き継がれる必要があります。



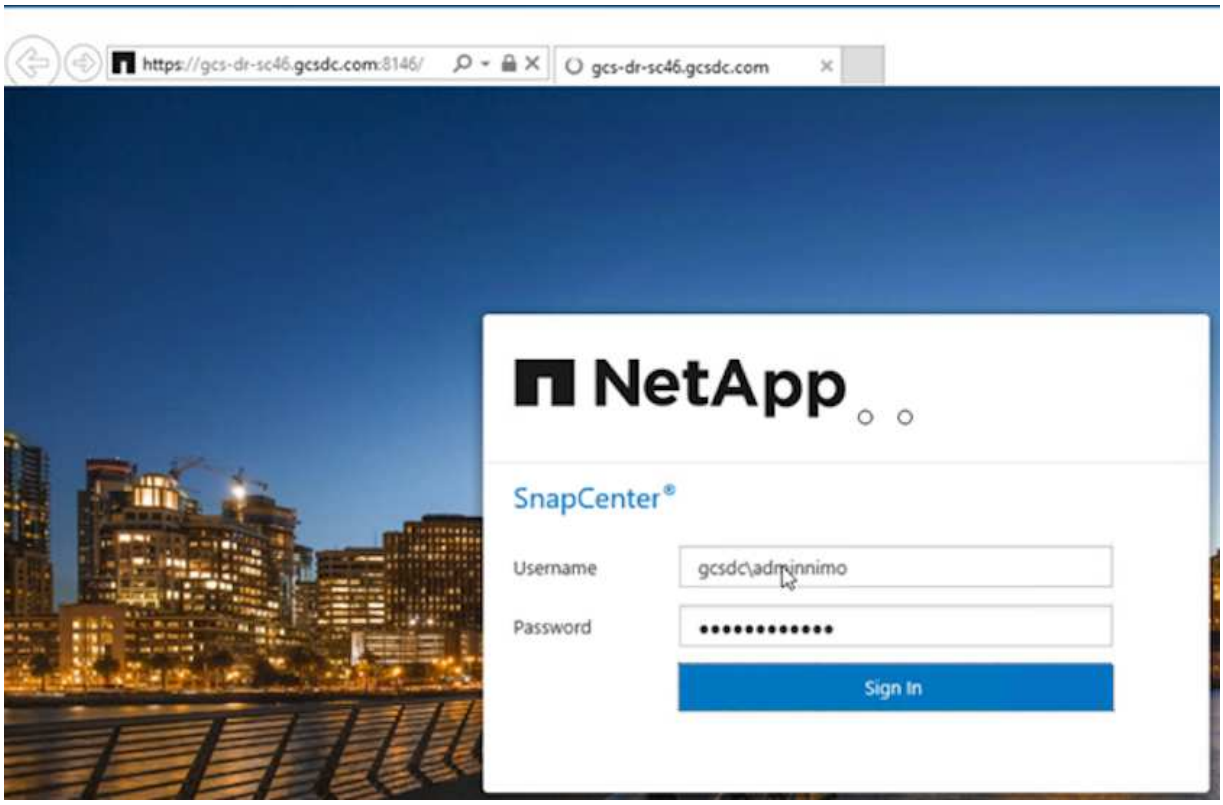


3. 継続的なフェイルオーバーが完了すると、タスクの完了を確認するメッセージが表示されます。タスクが完了したら、リカバリしたVMにアクセスしてiSCSIセッションまたはNFSセッションを設定します。

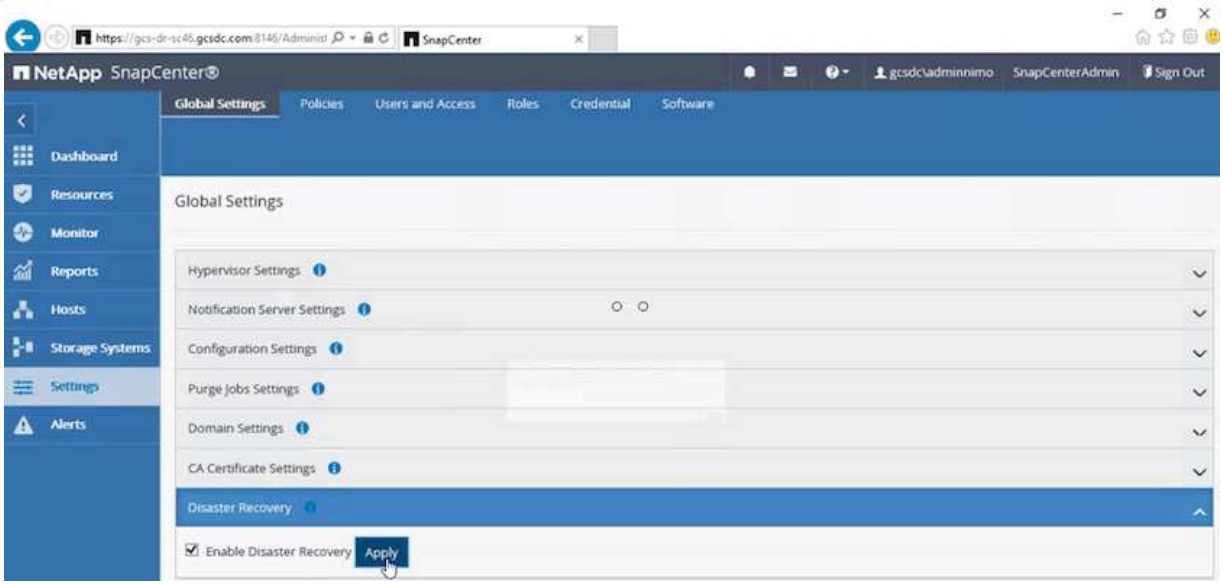
フェイルオーバーモードが「Running in Failover」に変わり、VMのステータスが「Recoverable」になります。保護ドメインのすべてのVMが、フェールオーバーランブック設定で指定された状態でリカバリサイトで実行されるようになりました。

フェールオーバー構成とインフラストラクチャを検証するために、JetStream DRをテストモード（テストフェールオーバーオプション）で実行して、仮想マシンとそのデータをオブジェクトストアからテストリカバリ環境にリカバリすることができます。フェールオーバー手順 がテストモードで実行されると、その動作は実際のフェールオーバープロセスに似ています。

4. 仮想マシンのリカバリが完了したら、ゲスト内ストレージにストレージディザスタリカバリを使用します。このプロセスを実証するために、この例ではSQL Serverを使用しています。
5. AVS SDDCでリカバリしたSnapCenter VMにログインし、DRモードを有効にします。
   a. browserNを使用してSnapCenter UIにアクセスします。



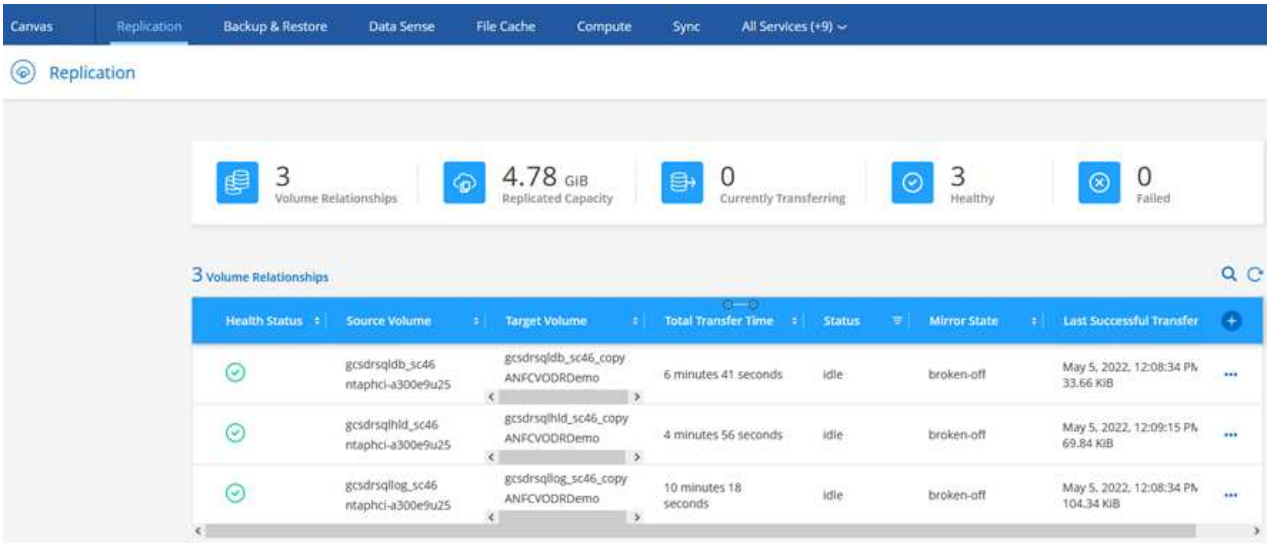
   b. [設定]ページで、[設定]>[グローバル設定]>[ディザスタリカバリ]の順に選択します。
   c. Enable Disaster Recoveryを選択します。
   d. 適用をクリックします。



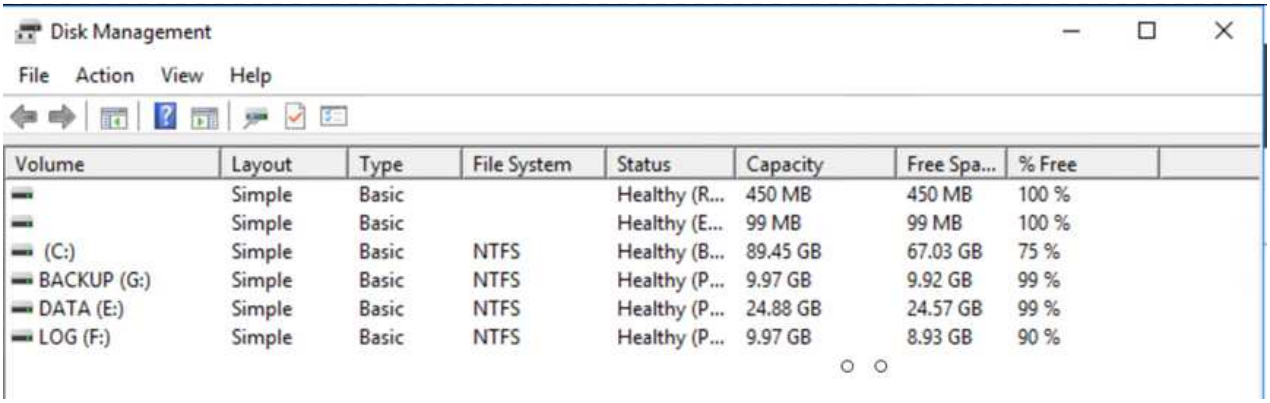
e. [Monitor]>[Jobs]をクリックして、DRジョブが有効になっているかどうかを確認します。

ストレージのディザスタリカバリには、NetApp SnapCenter 4.6以降を使用してください。以前のバージョンでは、アプリケーションと整合性のあるSnapshot（SnapMirrorを使用してレプリケート）を使用し、ディザスタリカバリサイトで以前のバックアップをリカバリする必要がある場合に手動でリカバリする必要があります。

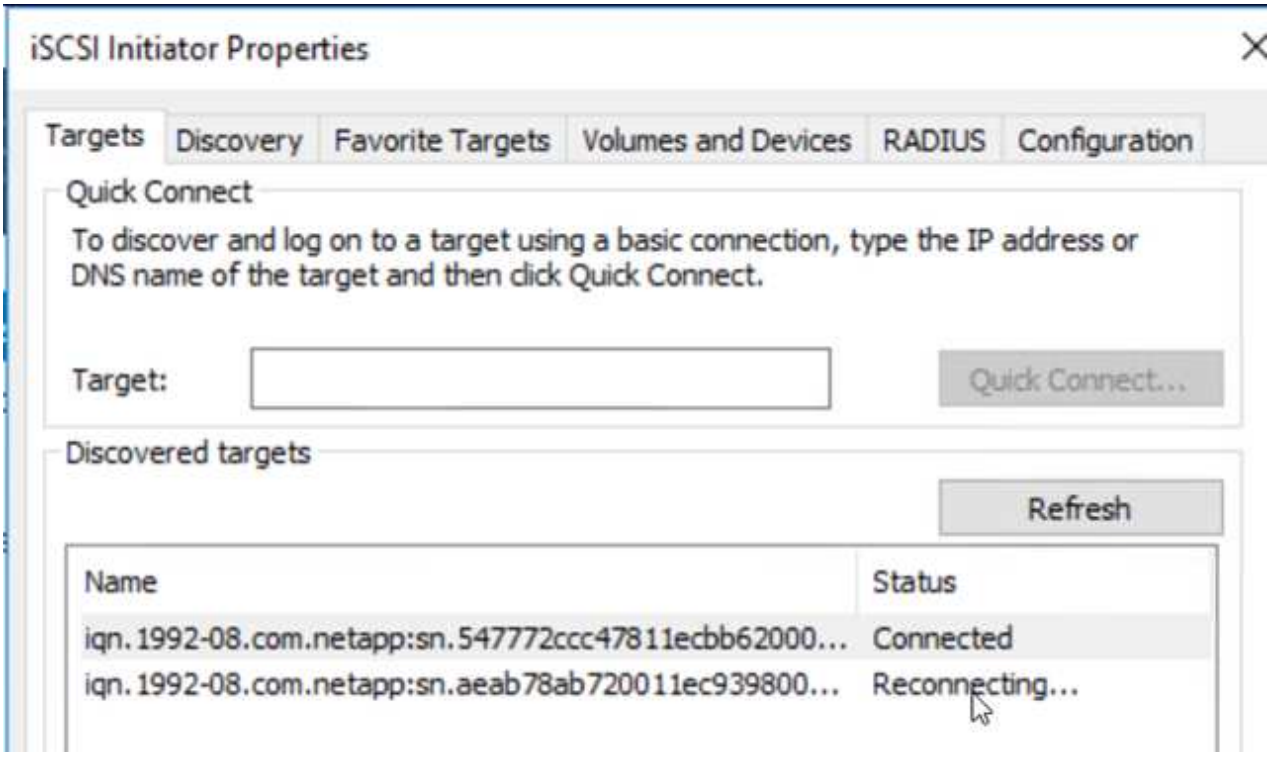
6. SnapMirror関係が解除されていることを確認します。



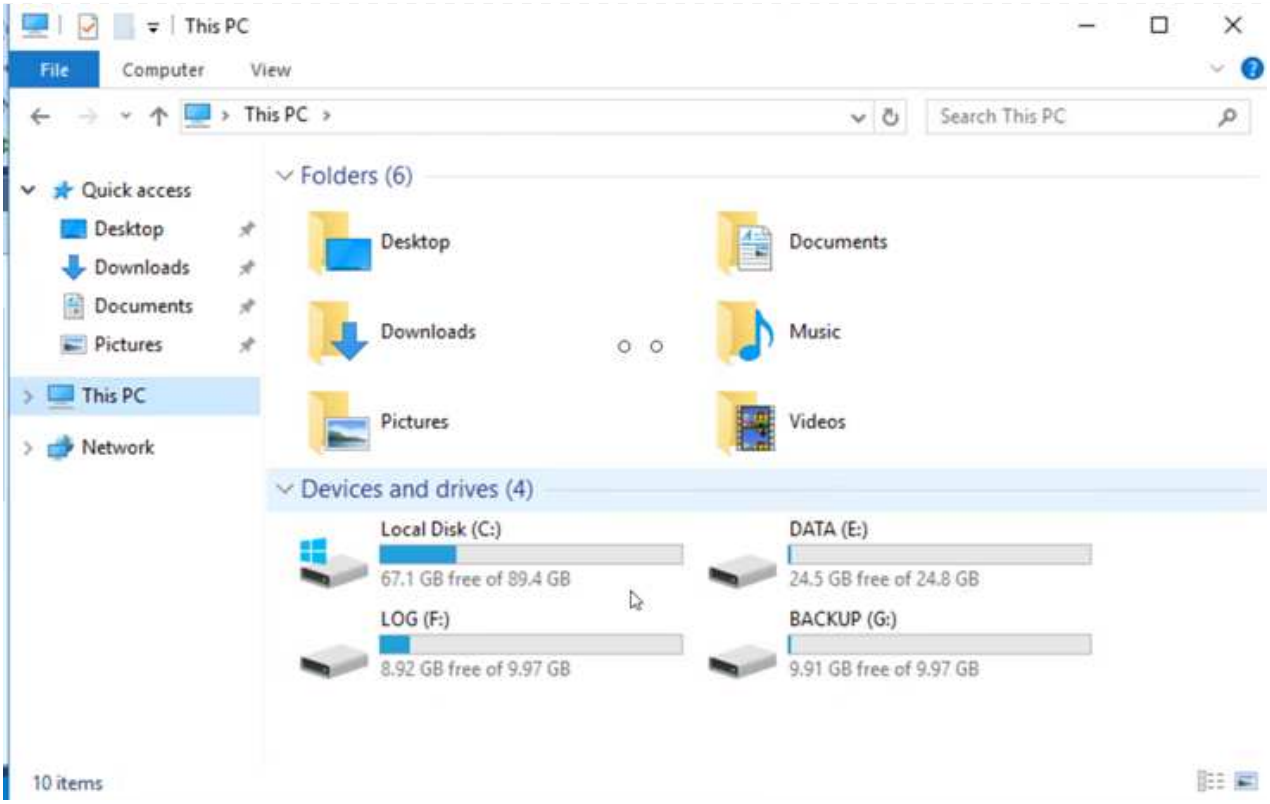
7. Cloud Volumes ONTAP からリカバリしたSQLゲストVMに、同じドライブレターを使用してLUNを接続します。



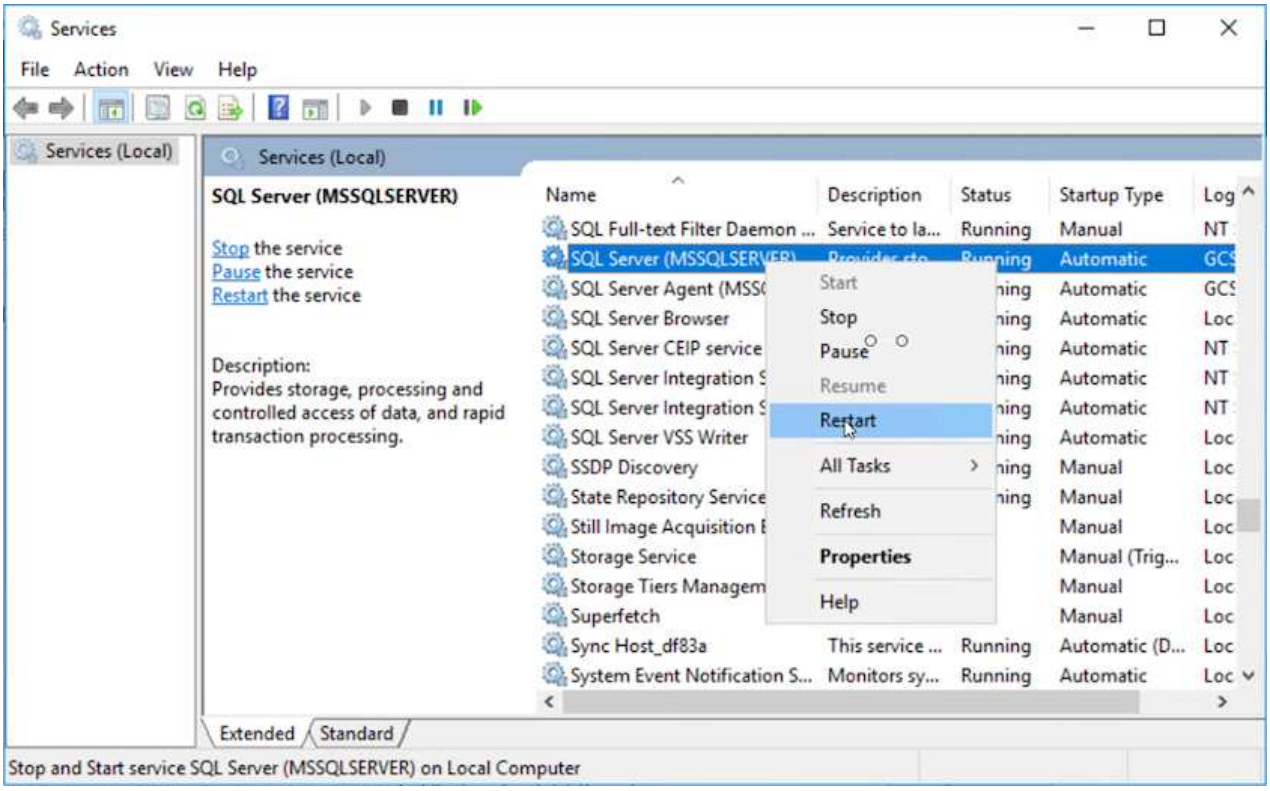
8. iSCSIイニシエータを開き、以前切断したセッションを消去して、レプリケートされたCloud Volumes ONTAP ボリュームのマルチパスとともに新しいターゲットを追加します。



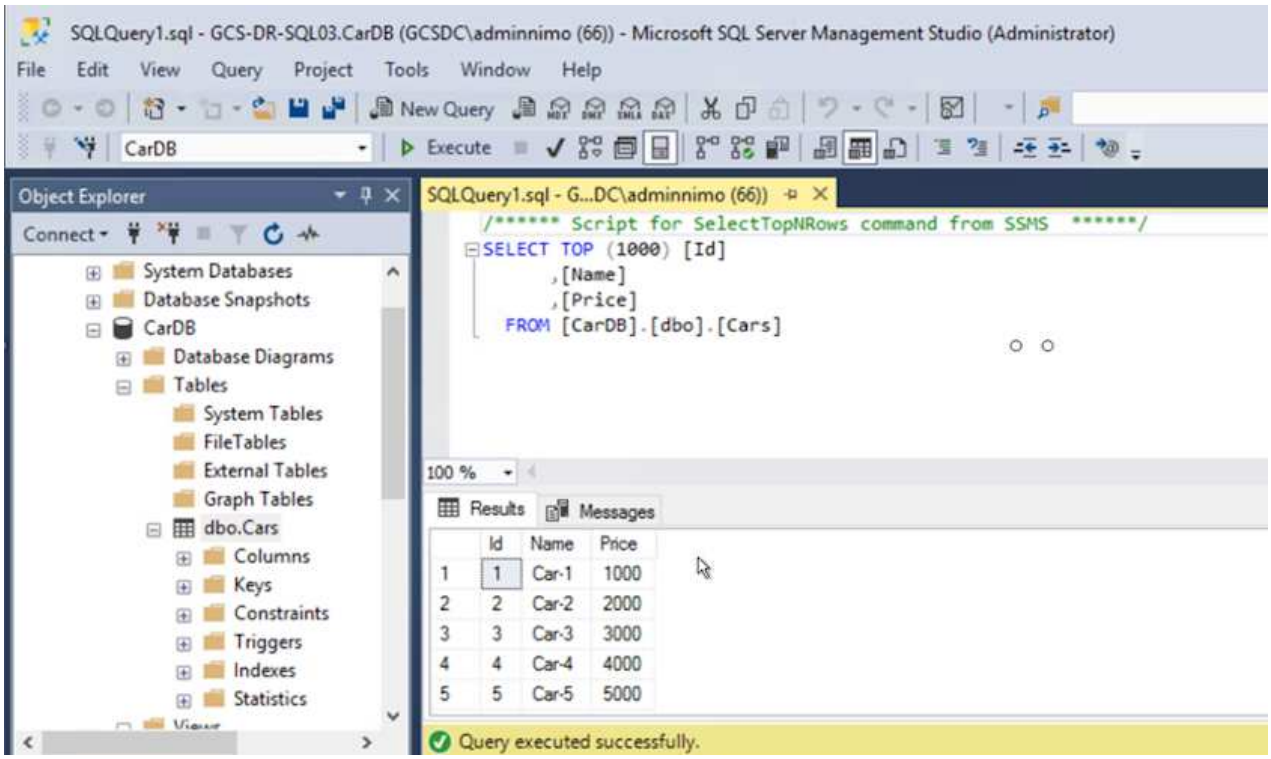
9. DR実行前に使用したのと同じドライブレターを使用して、すべてのディスクが接続されていることを確認してください。



10. MSSQLサーバサービスを再起動します。



11. SQLリソースがオンラインに戻っていることを確認します。



NFSの場合は'mountコマンドを使用してボリュームを接続し'/etc/fstabエントリーを更新します

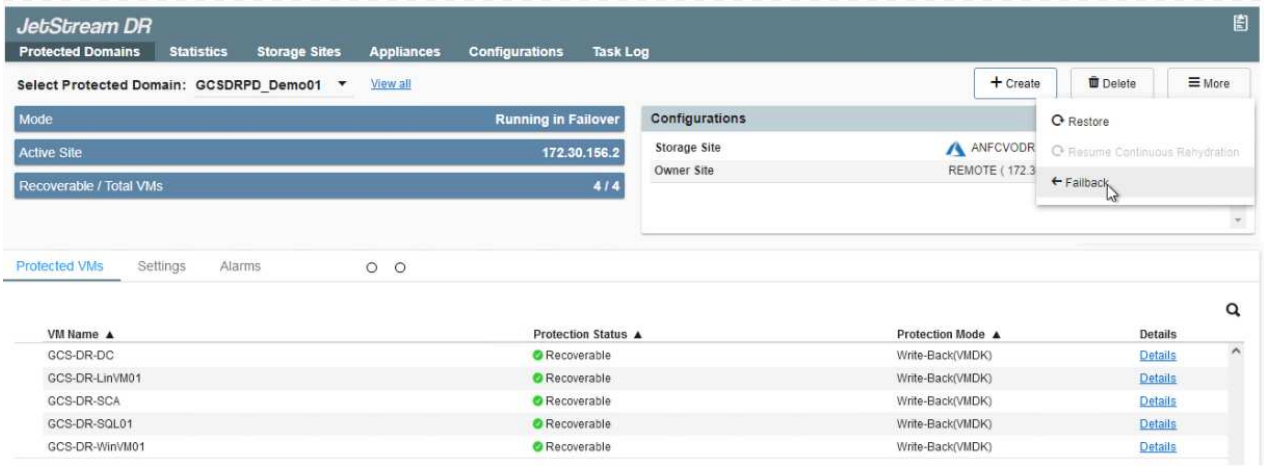
この時点で運用を開始し、通常どおり業務を継続できます。

NSX Tエンドでは'フェイルオーバー・シナリオをシミュレートするために'個別の専用ティア1ゲートウェイを作成できますこれにより、すべてのワークロードが相互に通信できるようになりますが、環境内や環境外にトラフィックをルーティングできないため、トリアージ、封じ込め、セキュリティ強化のタスクをクロスコンタミネーションのリスクなしに実行できます。この操作はこのドキュメントでは扱いませんが、分離をシミュレートするために簡単に行うことができます。

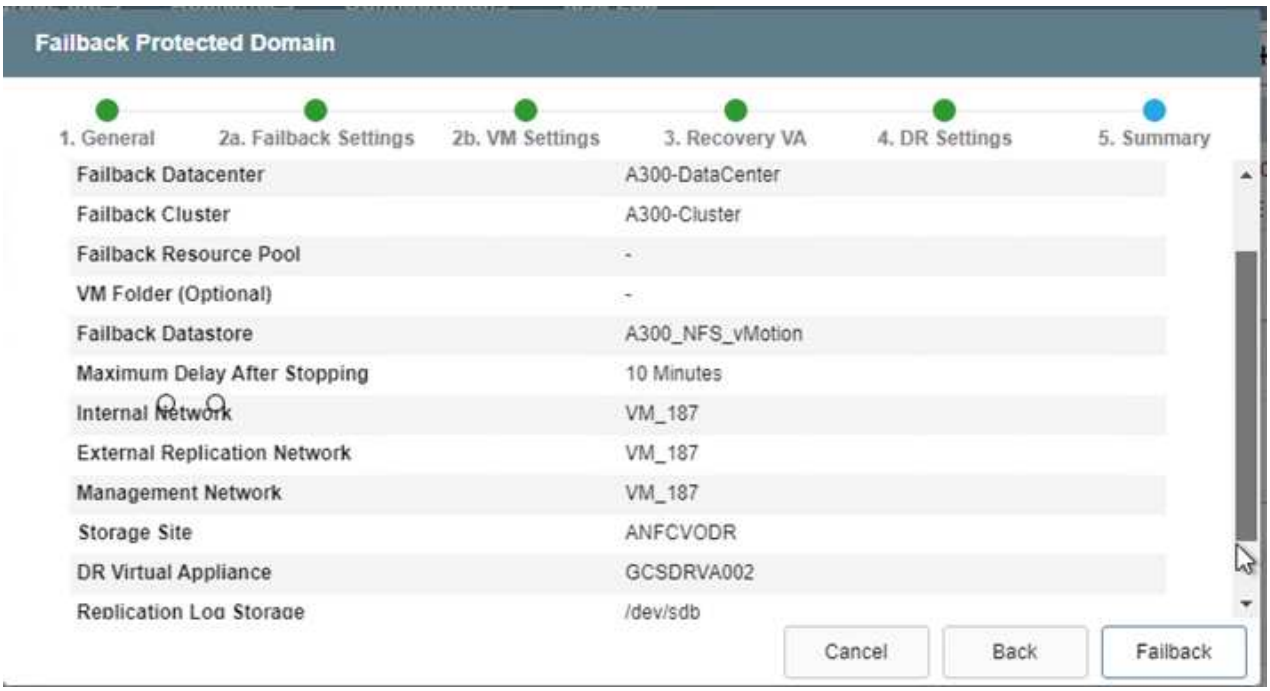
プライマリサイトが起動し、再び実行されるようになったら、フェイルバックを実行できます。VM保護はJetstreamで再開され、SnapMirror関係を反転する必要があります。

1. オンプレミス環境をリストア災害のタイプによっては、保護対象クラスタの構成をリストアまたは検証しなければならない場合があります。必要に応じて、JetStream DRソフトウェアを再インストールする必要があります。
2. リストアされたオンプレミス環境にアクセスし、Jetstream DR UIに移動して、適切な保護ドメインを選択します。保護サイトがフェイルバックできる状態になったら、UIで[Failback]オプションを選択します。

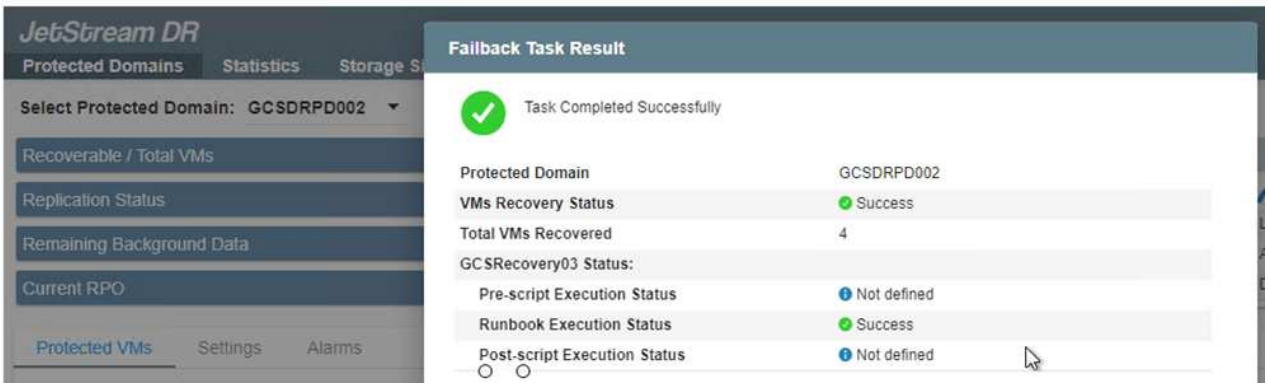
CPTによって生成されたフェイルバック計画を使用して、VMとそのデータをオブジェクトストアから元のVMware環境に戻すこともできます。



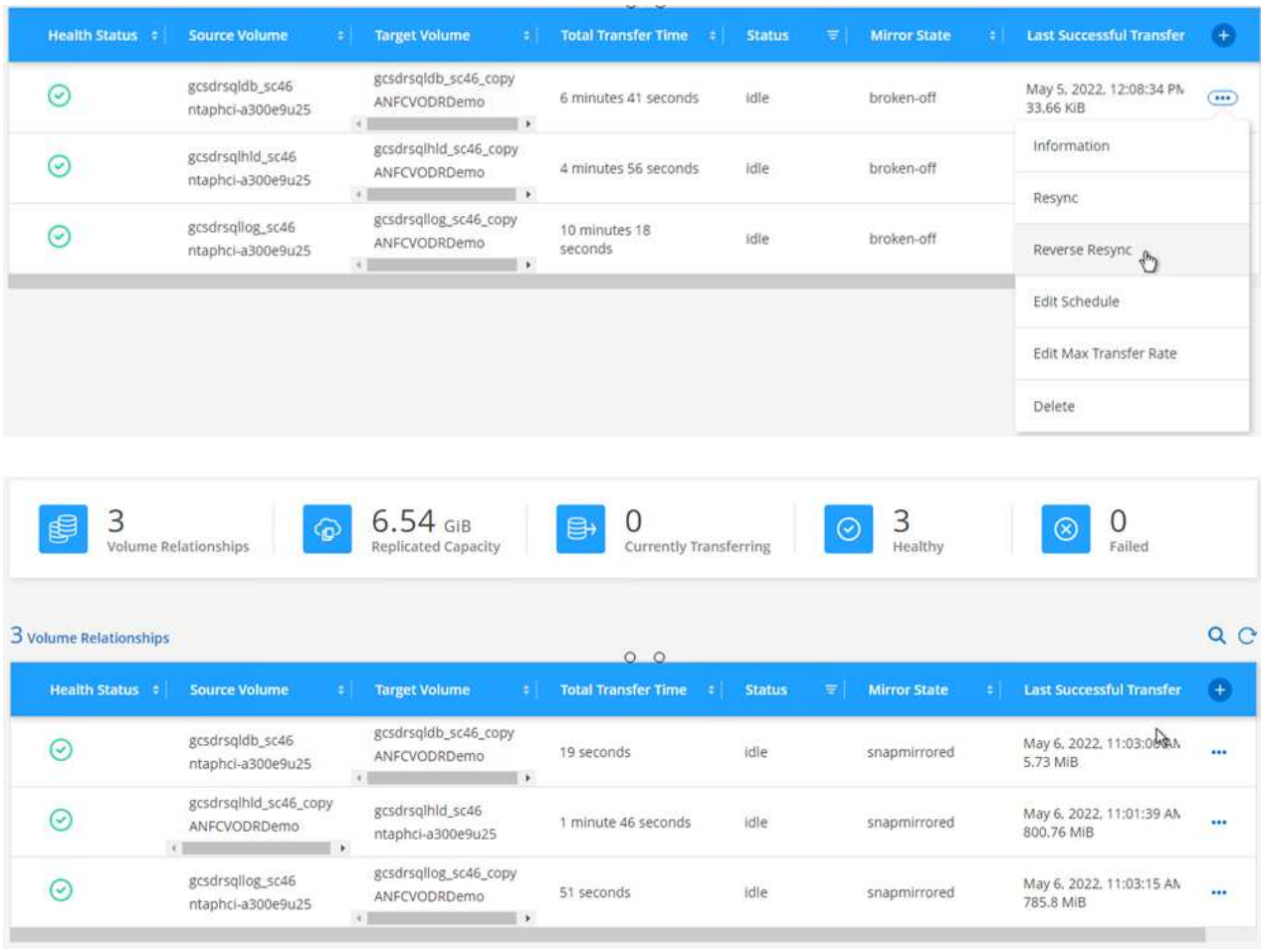
リカバリサイトでVMを一時停止して保護対象サイトで再起動したあとの最大遅延時間を指定します。このプロセスには、フェイルオーバーVMを停止したあとのレプリケーションの完了、リカバリサイトのクリーンアップに必要な時間、保護サイトでVMを再作成するのに必要な時間などが含まれます。10分を推奨します。



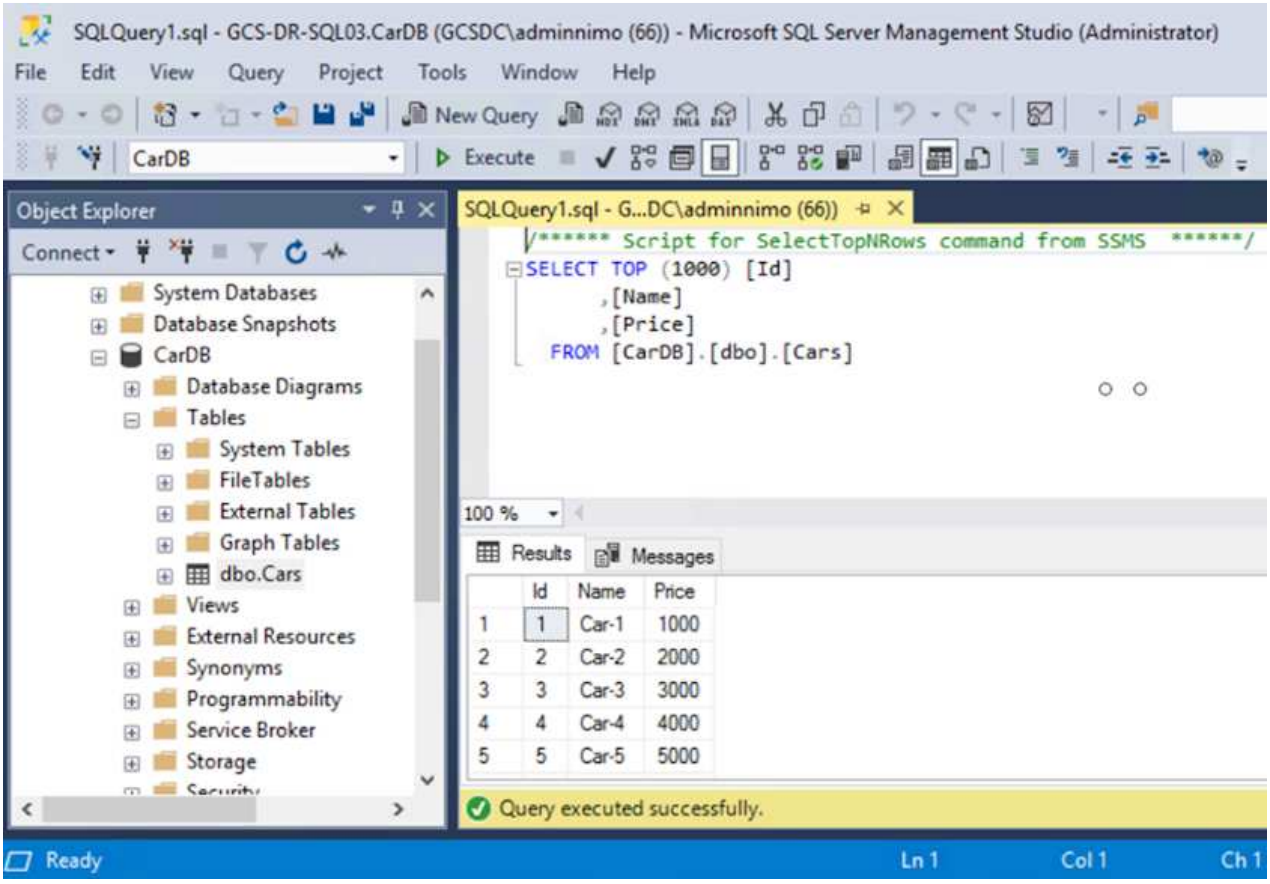
3. フェイルバックプロセスを完了し、VM保護およびデータの整合性が再開されたことを確認する。



4. VMのリカバリが完了したら、セカンダリストレージをホストから切断してプライマリストレージに接続します。



5. MSSQLサーバサービスを再起動します。
6. SQLリソースがオンラインに戻っていることを確認します。



プライマリストレージにフェイルバックするには、逆再同期処理を実行して、フェイルオーバーの前と同じ関係の方向が維持されていることを確認します。

逆再同期処理の実行後もプライマリストレージとセカンダリストレージのロールを保持するには、逆再同期処理をもう一度実行します。

このプロセスは、Oracleなどの他のアプリケーション、類似したデータベースの種類、ゲスト接続ストレージを使用するその他のアプリケーションに適用されます。

常に同様に、重要なワークロードを本番環境に移植する前に、リカバリに必要な手順をテストしてください。

この解決策 の利点

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

◦ 開発とテスト、セキュリティテスト、パッチとアップグレードのテスト、修正テストなど、DR以外のワークフローにDRデータを活用します。

- CPUとRAMの最適化は、小規模なコンピューティングクラスタへのリカバリを可能にすることで、クラウドコストの削減に役立ちます。

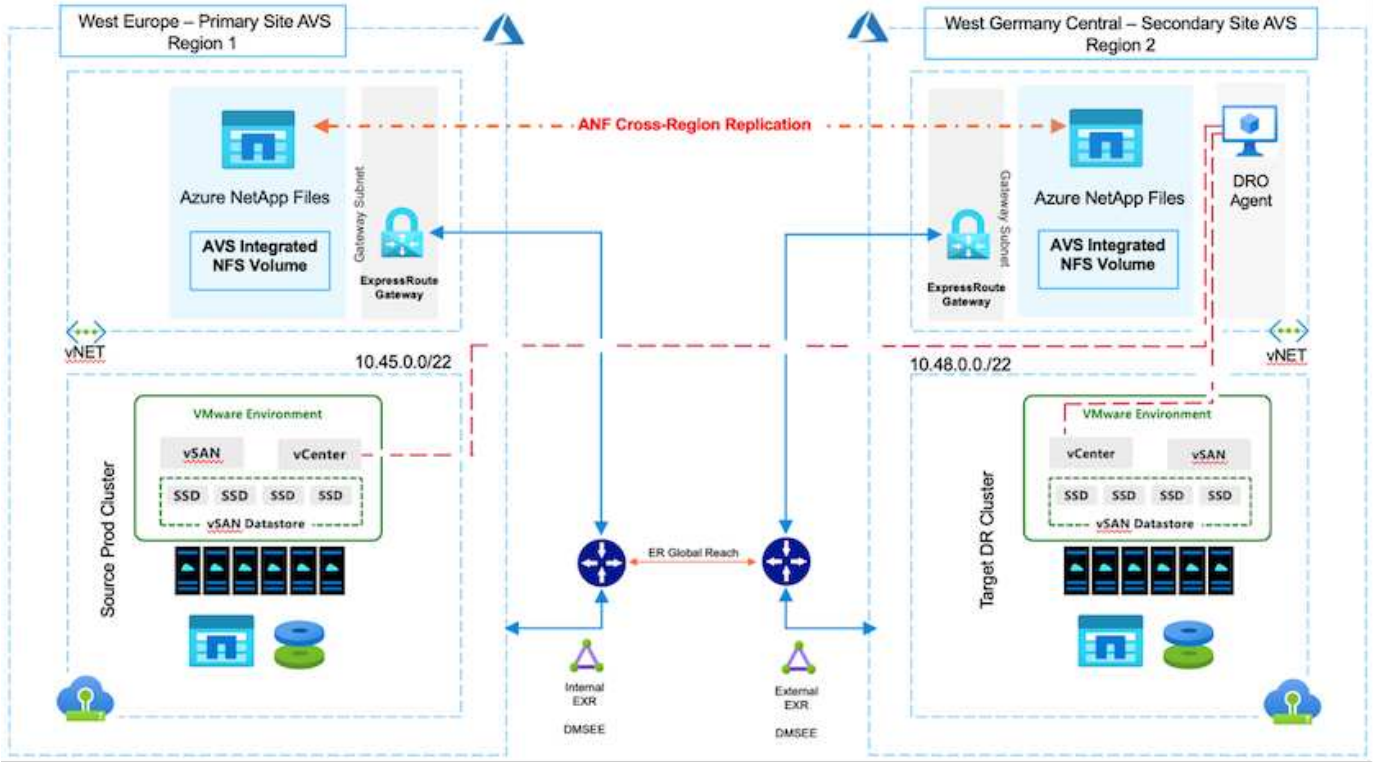
TR-4955：『Disaster Recovery with Azure NetApp Files （ANF）and Azure VMware解決策 （AVS）』

作成者：ネットアップソリューションエンジニアリング担当Niyaz Mohamed

概要

クラウド内のリージョン間でブロックレベルのレプリケーションを使用したディザスタリカバリは、耐障害性に優れた対費用効果の高い方法で、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）からワークロードを保護します。Azure NetApp Files （ANF）のリージョン間ボリュームレプリケーションを使用するとAzure NetApp Files 、Azure VMware解決策 （AVS）SDDCサイトで実行されているVMwareワークロードを、プライマリAVSサイトのNFSデータストアとして使用し、ターゲットリカバリリージョンの指定されたセカンダリAVSサイトにレプリケートできます。

ディザスタリカバリオーケストレーションツール（DRO）（UI付きのスクリプト化された解決策 ）を使用すると、AVS SDDC間でレプリケートされたワークロードをシームレスにリカバリできます。DROは、レプリケーションピアリングを解除してから、AVSへのVM登録を通じて、NSX-T（すべてのAVSプライベートクラウドに含まれる）上のネットワークマッピングに、デスティネーションボリュームをデータストアとしてマウントすることで、リカバリを自動化します。



前提条件と一般的な推奨事項

- レプリケーションピアリングを作成して、リージョン間レプリケーションが有効になっていることを確認します。を参照してください "Azure NetApp Files のボリュームレプリケーションを作成します"。
- ソースとターゲットのAzure VMware解決策 プライベートクラウド間でExpressRouteグローバルリーチを

設定する必要があります。

- リソースにアクセスできるサービスプリンシパルが必要です。
- サポートされるトポロジは、プライマリAVSサイトからセカンダリAVSサイトです。
- を設定します "レプリケーション" ビジネスニーズとデータ変更率に基づいて、ボリュームごとに適切なスケジュールを設定します。

> カスケードトポロジ、ファンイントポロジ、ファンアウトトポロジはサポートされていません。

はじめに

Azure VMware解決策 を導入します

。 "Azure VMware 解決策の略" （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が完全に管理およびサポートするファーストパーティの解決策 で、Azureインフラストラクチャを使用するVMwareにより検証されています。そのため、お客様は、コンピューティングの仮想化にVMware ESXi、ハイパーコンバージドストレージにvSAN、ネットワークとセキュリティにNSXを利用できます。また、Microsoft Azureのグローバルなプレゼンス、クラスをリードするデータセンター施設、Azureネイティブのサービスとソリューションで構成される豊富なエコシステムへの近接性を活用できます。Azure VMware解決策 SDDCとAzure NetApp Files を組み合わせることで、ネットワークレイテンシを最小限に抑えながら最高のパフォーマンスを実現できます。

AzureでAVSプライベートクラウドを構成するには、以下の手順に従います "リンク" を参照してください "リンク" （Microsoftのマニュアル）。 最小限の構成でセットアップされたパイロットライト環境は、DR目的で使用できます。 このセットアップには、重要なアプリケーションをサポートするためのコアコンポーネントのみが含まれており、フェイルオーバーが発生した場合に、より多くのホストをスケールアウトして生成し、負荷の大部分を処理することができます。

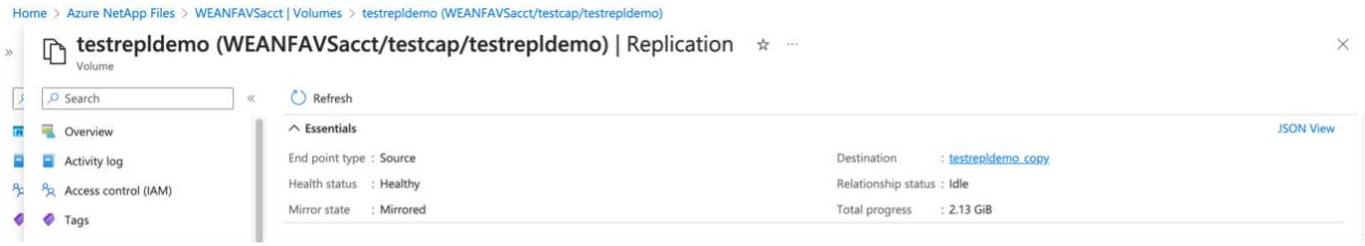
> 初期リリースでは、DROは既存のAVS SDDCクラスタをサポートしています。オンデマンドのSDDC作成は、今後のリリースで提供される予定です。

Azure NetApp Files をプロビジョニングして設定

"Azure NetApp Files の特長" エンタープライズクラスのハイパフォーマンスな従量課金制ファイルストレージサービスです。以下の手順に従ってください "リンク" AVSプライベートクラウド環境を最適化するために、Azure NetApp Files をNFSデータストアとしてプロビジョニングおよび設定します。

Azure NetApp Filesに対応したデータストアボリュームのボリュームレプリケーションを作成します

最初の手順では、AVSプライマリサイトからAVSセカンダリサイトへ、適切な頻度と保持期間を使用して、目的のデータストアボリュームのリージョン間レプリケーションを設定します。



以下の手順に従ってください "リンク" レプリケーションピアリングを作成してリージョン間レプリケーションを設定するには、次の手順を実行します。デスティネーションの容量プールのサービスレベルは、ソースの容量プールのサービスレベルと同じにすることができます。ただし、このユースケースでは、標準のサービスレベルを選択してから選択できます "サービスレベルを変更する" 実際に災害が発生した場合やDRシミュレーションが発生した場合。

リージョン間レプリケーション関係は前提条件であり、事前に作成しておく必要があります。

DROのインストール

DROの使用を開始するには、指定されたAzure仮想マシンでUbuntuオペレーティングシステムを使用し、前提条件を満たしていることを確認します。次に、パッケージをインストールします。

前提条件：

- リソースにアクセスできるサービスプリンシパル。
- ソースとデスティネーションのSDDCおよびAzure NetApp Files インスタンスへの適切な接続が存在することを確認します。
- DNS名を使用する場合は、DNS解決を実施する必要があります。それ以外の場合は、vCenterのIPアドレスを使用します。
- OS要件：*
- Ubuntu Focal 20.04 (LTS)指定されたエージェント仮想マシンに次のパッケージをインストールする必要があります。
- Docker です
- docker-composeの略
- JqChange `docker.sock` 次の新しい権限を追加します。 `sudo chmod 666 /var/run/docker.sock`。

。 `deploy.sh` スクリプトは、必要なすべての前提条件を実行します。

手順は次のとおりです。

1. 指定した仮想マシンにインストールパッケージをダウンロードします。

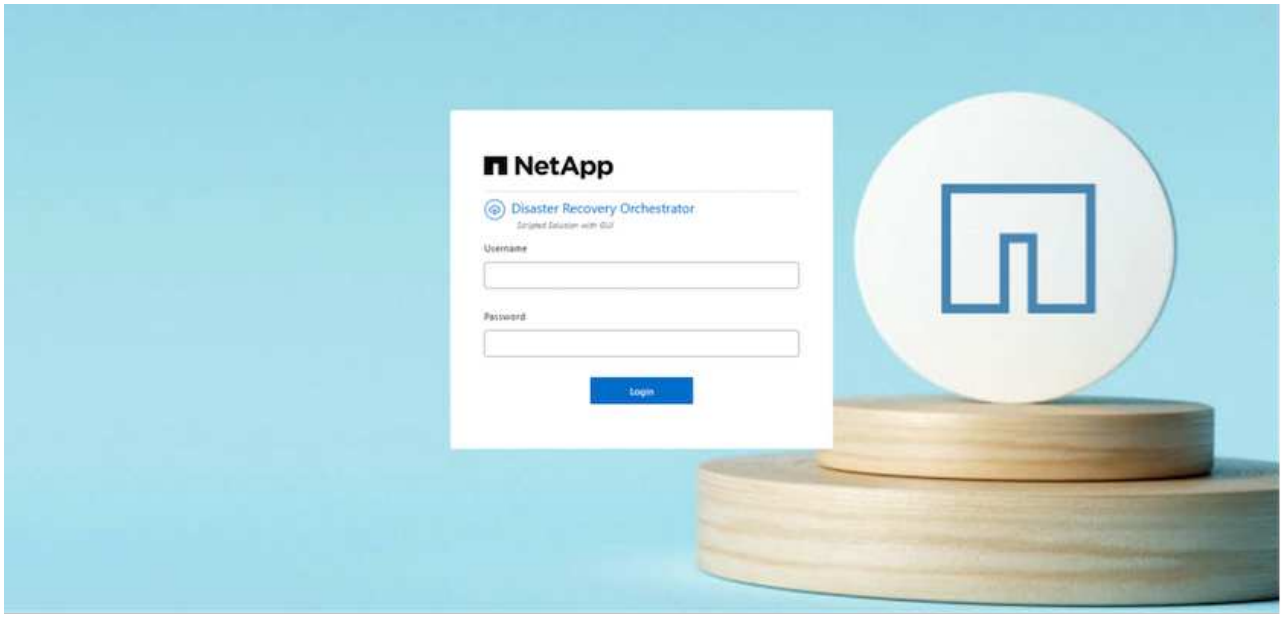
```
git clone https://github.com/NetApp/DRO-Azure.git
```

エージェントは、セカンダリAVSサイトリージョンまたはプライマリAVSサイトリージョンのSDDCとは別のAZにインストールする必要があります。

2. パッケージを解凍し、導入スクリプトを実行して、ホストIP（例： `10.10.10.10`）。

```
tar xvf draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

3. 次のクレデンシャルを使用してUIにアクセスします。
   - ユーザ名： `admin`
   - パスワード： `admin`



DRO構成

Azure NetApp Files とAVSが正しく設定されたら、プライマリAVSサイトからセカンダリAVSサイトへのワークロードのリカバリを自動化するDROの設定を開始できます。セカンダリAVSサイトにDROエージェントを導入し、ExpressRouteゲートウェイ接続を設定して、DROエージェントが適切なAVSおよびAzure NetApp Files コンポーネントとネットワーク経由で通信できるようにすることを推奨します。

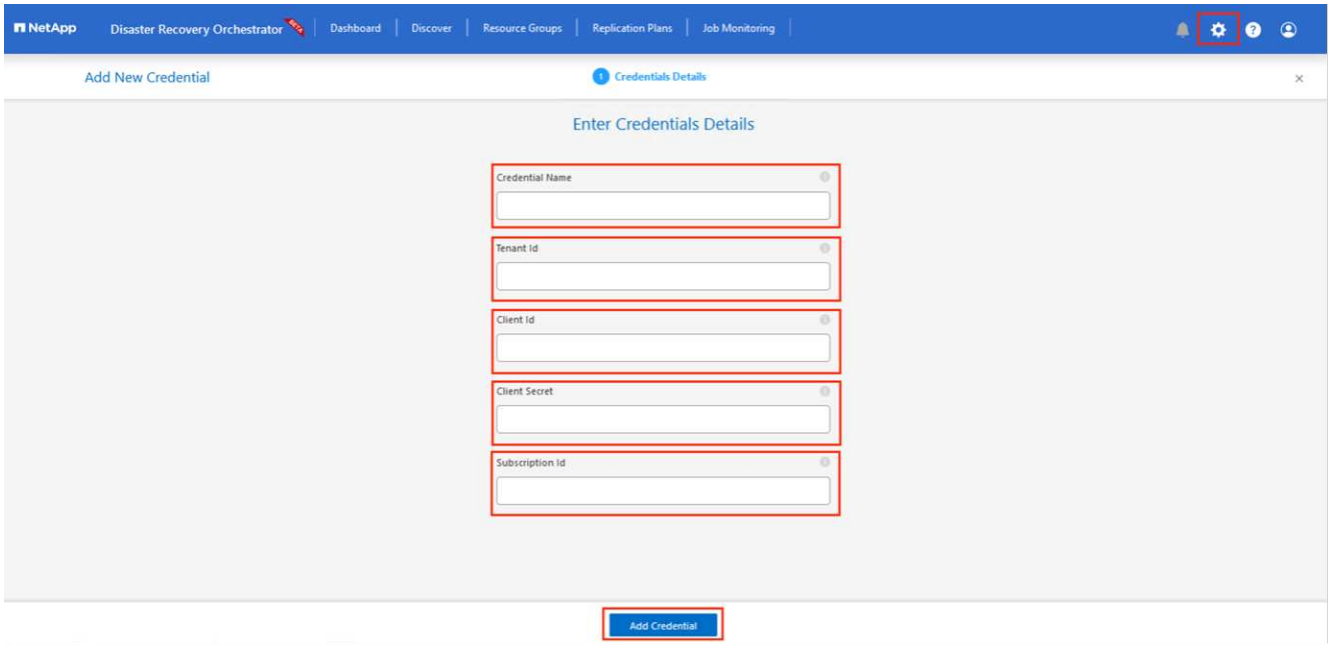
まず、クレデンシャルを追加します。DROには、Azure NetApp Files とAzure VMware解決策 を検出する権限が必要です。Azure Active Directory（AD）アプリケーションを作成してセットアップし、DROに必要なAzureクレデンシャルを取得することで、Azureアカウントに必要な権限を付与できます。サービスプリンシパルをAzureサブスクリプションにバインドし、関連する必要な権限を持つカスタムロールを割り当てる必要があります。ソース環境とデスティネーション環境を追加すると、サービスプリンシパルに関連付けられているクレデンシャルを選択するように求められます。[Add New Site]をクリックする前に、これらのクレデンシャルをDROに追加する必要があります。

この処理を実行するには、次の手順を実行します。

1. サポートされているブラウザでDROを開き、デフォルトのユーザ名とパスワードを使用します `/admin /admin`）。パスワードは、[Change Password]オプションを使用して初回ログイン後にリセットできます。
2. DROコンソールの右上にある*設定*アイコンをクリックし、*資格情報*を選択します。
3. [Add New Credential]をクリックし、ウィザードの手順に従います。

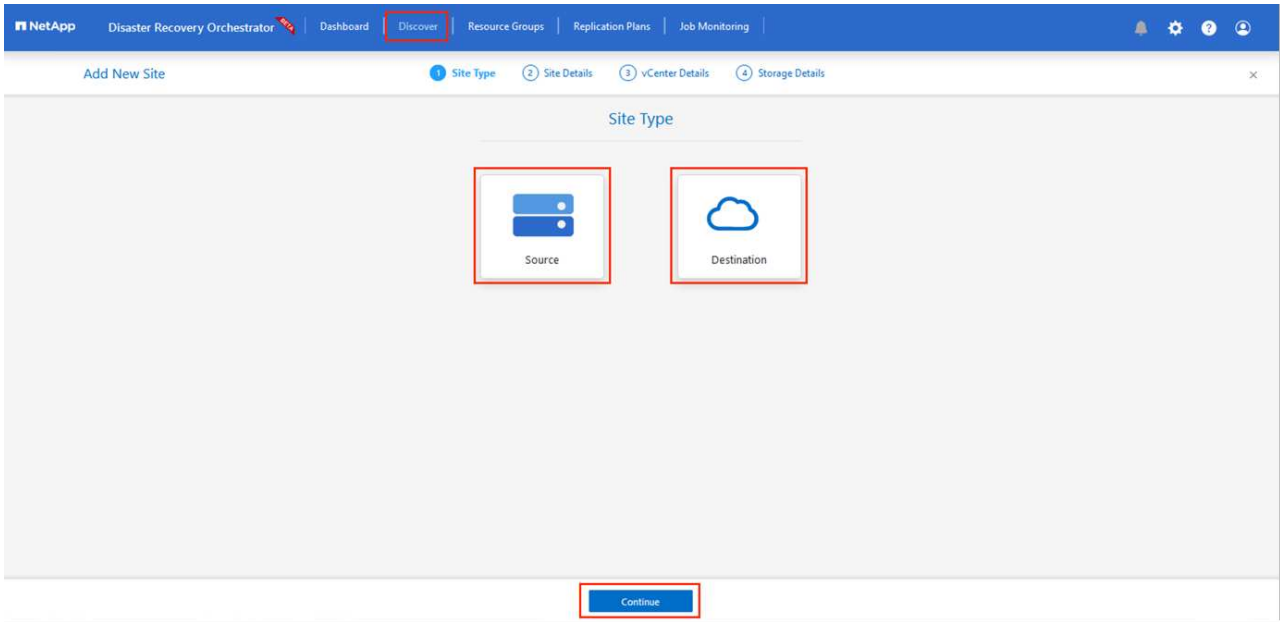
4. クレデンシャルを定義するには、必要な権限を付与するAzure Active Directoryサービスプリンシパルに関する情報を入力します。
   - クレデンシャル名
   - テナントID
   - クライアント ID
   - クライアントシークレット
   - サブスクリプションID

     この情報は、ADアプリケーションの作成時に取得しておく必要があります。
5. 新しいクレデンシャルの詳細を確認し、[Add Credential]をクリックします。



クレデンシャルを追加したら、プライマリとセカンダリのAVSサイト（vCenterとAzure NetApp Files ストレージアカウントの両方）を検出してDROに追加します。ソースサイトとデスティネーションサイトを追加するには、次の手順を実行します。

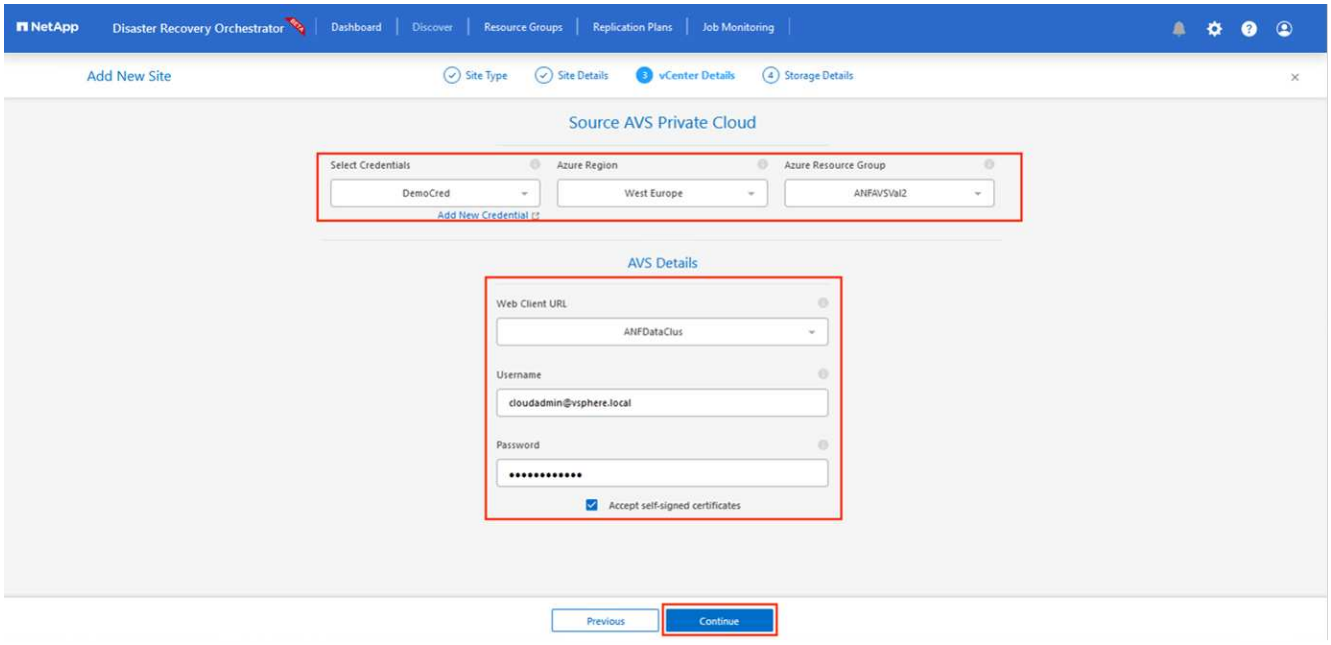
6. [検出]タブに移動します。
7. [新しいサイトの追加]*をクリックします。
8. 次のプライマリAVSサイトを追加します(コンソールで*ソース*として指定)。
   - SDDC vCenter
   - Azure NetApp Files ストレージアカウント
9. 次のセカンダリAVSサイト（コンソールで* Destination *として指定）を追加します。
   - SDDC vCenter
   - Azure NetApp Files ストレージアカウント



10. [ソース]をクリックしてサイト名を入力し、コネクタを選択してサイトの詳細を追加します。[* Continue（続行）] をクリックします。

   このドキュメントでは、デモ用にソースサイトを追加する方法について説明します。

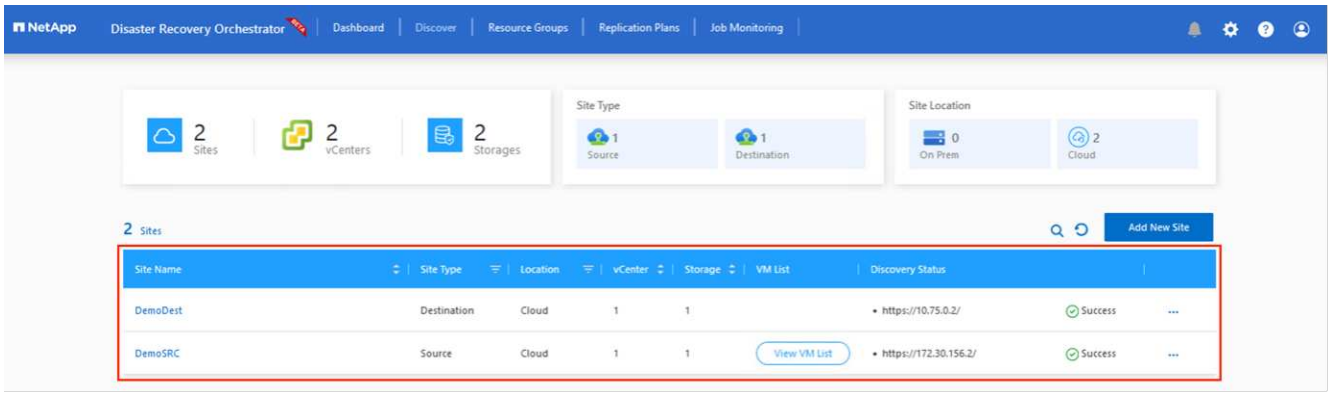
11. vCenterの詳細を更新します。これを行うには、プライマリAVS SDDCのドロップダウンからクレデンシャル、Azureリージョン、およびリソースグループを選択します。
12. DROには、リージョン内で使用可能なすべてのSDDCが一覧表示されます。ドロップダウンから、指定したプライベートクラウドのURLを選択します。
13. を入力します `cloudadmin@vsphere.local` ユーザクレデンシャル。これにはAzure Portalからアクセスできます。ここに記載されている手順に従ってください "リンク"。完了したら、*[続行]*をクリックします。



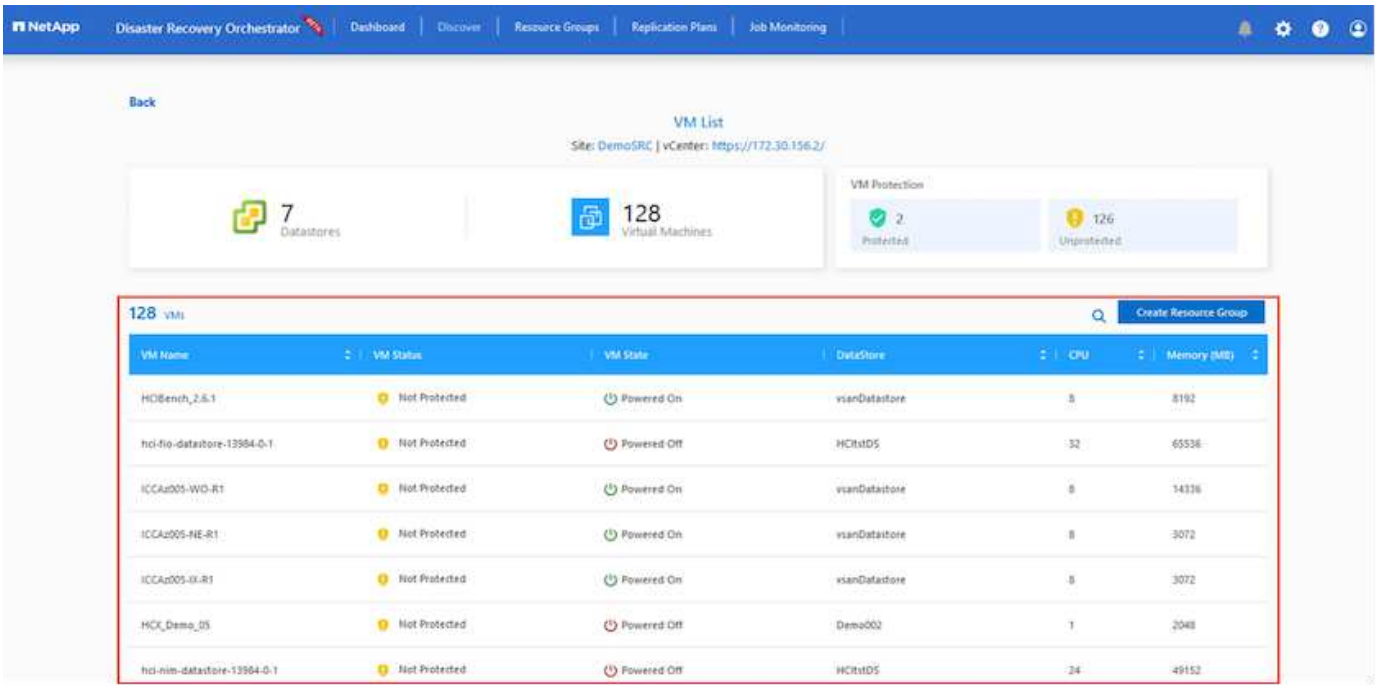
14. Azureリソースグループとネットアップアカウントを選択して、ソーススストレージの詳細（ANF）を選択

します。

15. [サイトの作成]*をクリックします。



追加されると、DROは自動検出を実行し、ソースサイトからデスティネーションサイトへの対応するリージョン間レプリカを持つVMを表示します。DROは、VMで使用されているネットワークとセグメントを自動的に検出して入力します。



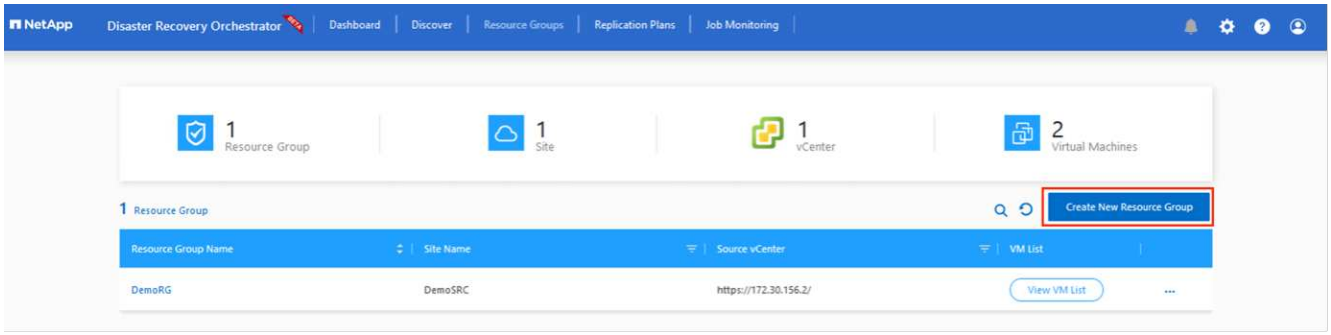
次の手順では、必要なVMをリソースグループとして機能グループにグループ化します。

リソースのグループ化

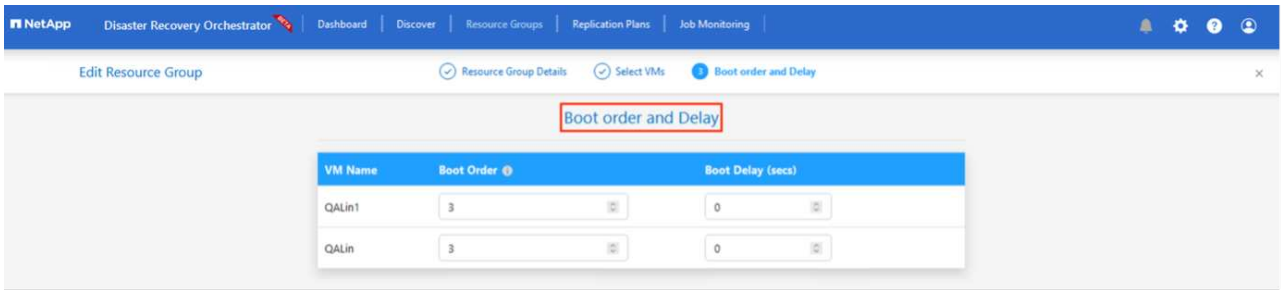
プラットフォームを追加したら、リカバリするVMをリソースグループにグループ化します。DROリソースグループを使用すると、依存する一連のVMを論理グループにグループ化して、それらの起動順序、ブート遅延、およびリカバリ時に実行可能なオプションのアプリケーション検証を含めることができます。

リソースグループの作成を開始するには、*[新しいリソースグループの作成]*メニュー項目をクリックします。

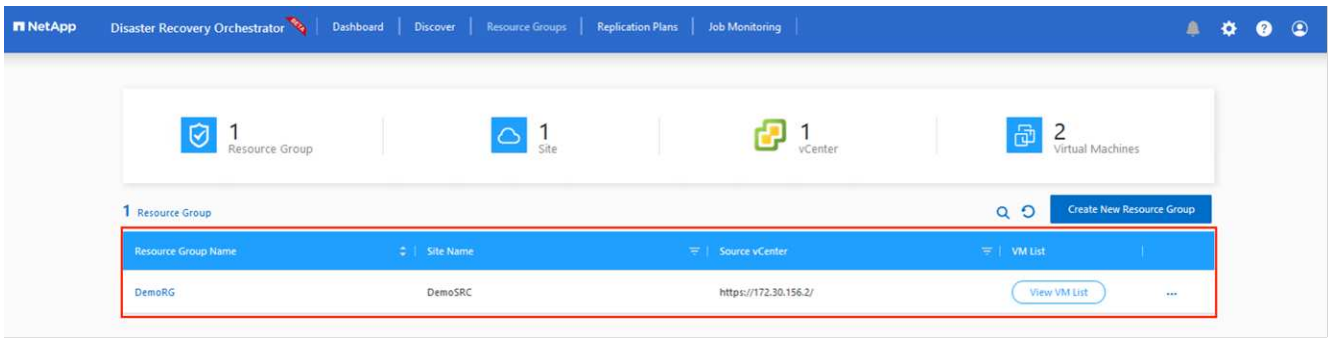
1. **[PS]**にアクセスし、[Create New Resource Group]*をクリックします。



2. [New Resource Group]で、ドロップダウンからソースサイトを選択し、*[Create]*をクリックします。
3. リソースグループの詳細を指定し、*[続行]*をクリックします。
4. 検索オプションを使用して適切なVMを選択します。
5. 選択したすべてのVMについて、と**[Boot Delay]**（秒）を選択します。各仮想マシンを選択して優先度を設定し、パワーオンシーケンスの順序を設定します。すべての仮想マシンのデフォルト値は3です。オプションは次のとおりです。
   - パワーオンする最初の仮想マシン
   - デフォルト
   - 最後にパワーオンした仮想マシン



6. [リソースグループの作成]をクリックします。

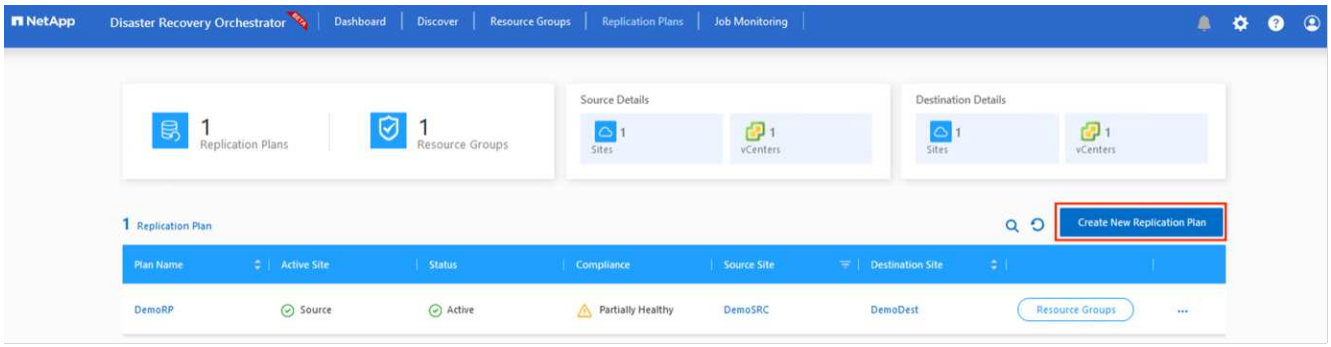


レプリケーションプラン

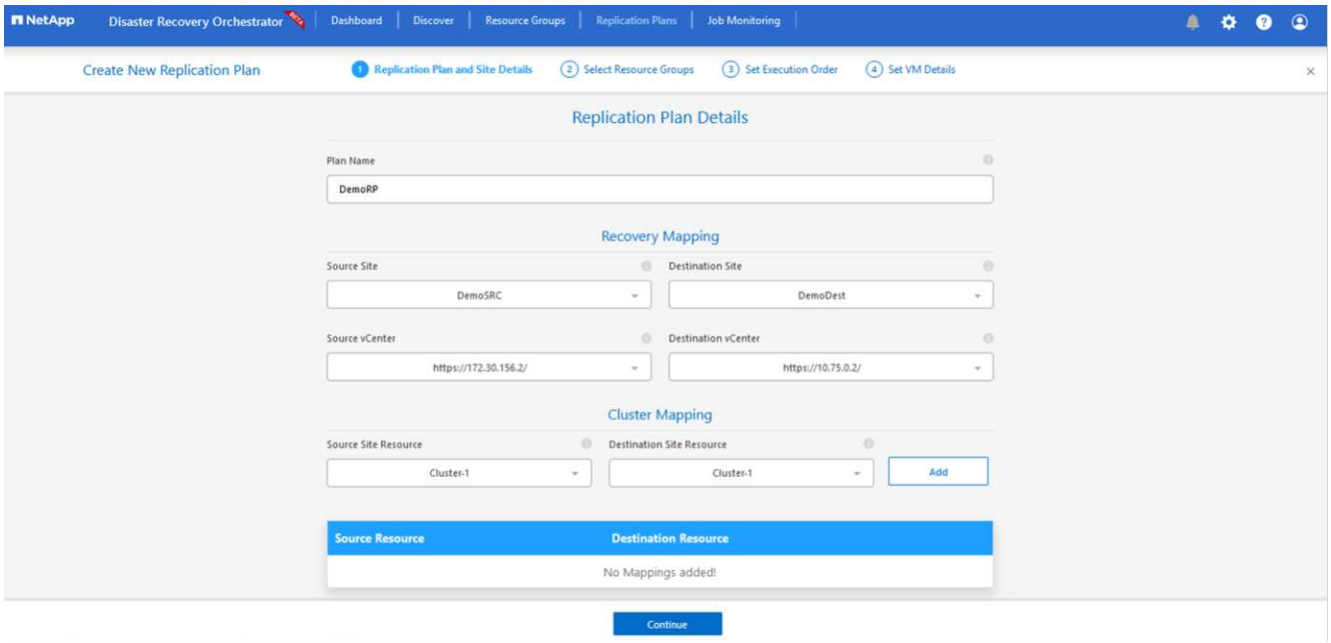
災害発生時にアプリケーションをリカバリするための計画を立てておく必要があります。ドロップダウンからソースとデスティネーションのvCenterプラットフォームを選択し、このプランに含めるリソースグループを選択します。また、アプリケーションをリストアおよびパワーオンする方法（ドメインコントローラ、ティア1、ティア2など）もグループ化します。計画は設計図とも呼ばれます。リカバリプランを定義するには、[Replication Plan]タブに移動し、*[New Replication Plan]*をクリックします。

レプリケーションプランの作成を開始するには、次の手順を実行します。

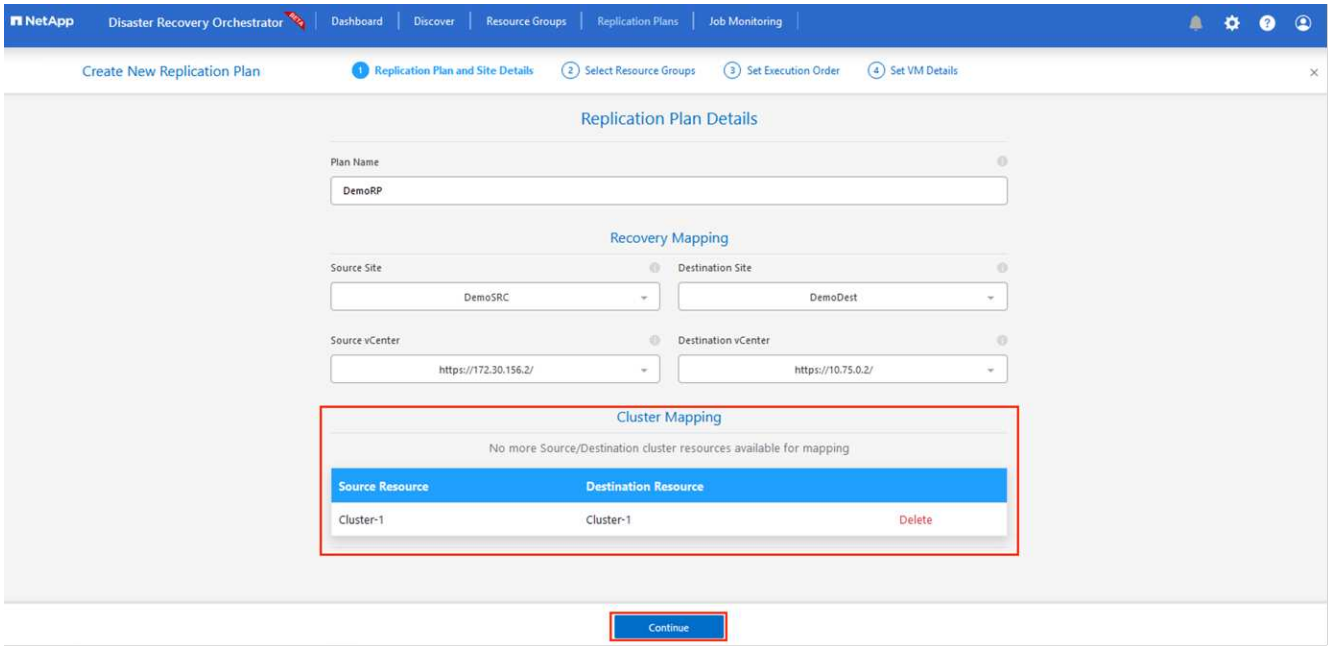
1. に移動し、[Create New Replication Plan]*をクリックします。



2. [New Replication Plan]*で、プランの名前を指定し、ソースサイト、関連付けられているvCenter、デスティネーションサイト、および関連付けられているvCenterを選択してリカバリマッピングを追加します。

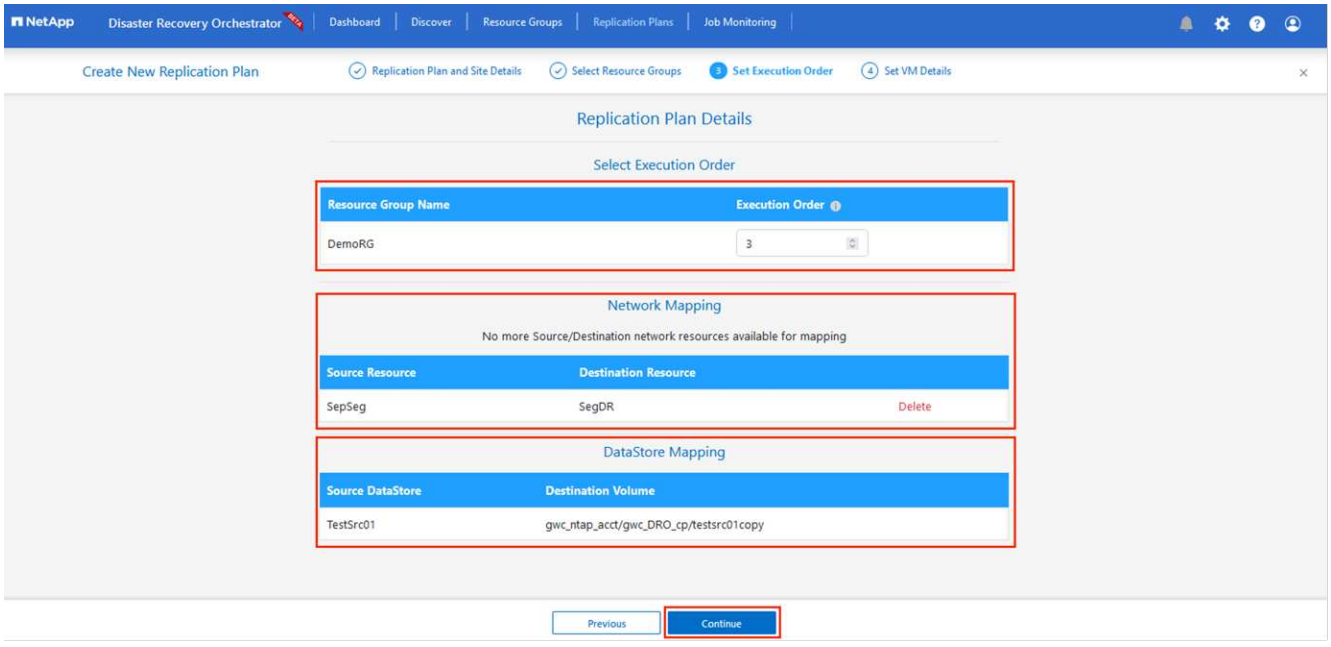


3. リカバリマッピングが完了したら、*[クラスタマッピング]*を選択します。

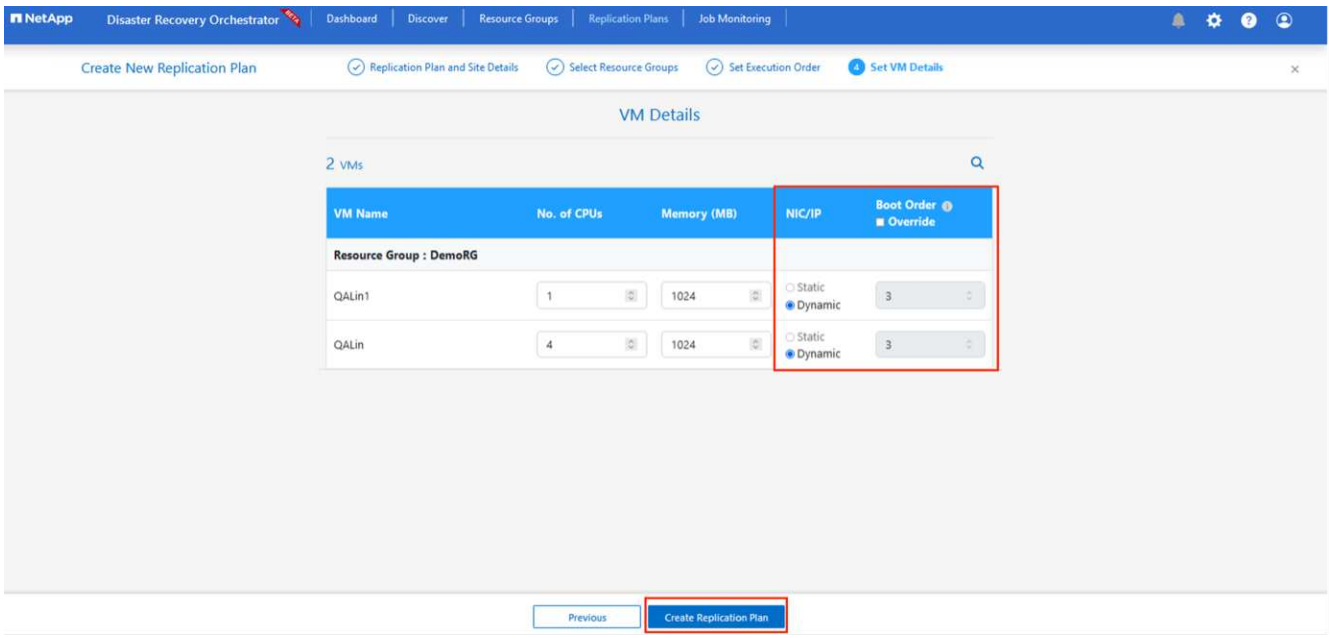


4. [リソースグループの詳細]を選択し、[*続行]をクリックします。
5. リソースグループの実行順序を設定します。このオプションを使用すると、複数のリソースグループが存在する場合の処理の順序を選択できます。
6. 完了したら、適切なセグメントにネットワークマッピングを設定します。セグメントはセカンダリAVSクラスタですでにプロビジョニングされている必要があります。それらにVMをマッピングするには、適切なセグメントを選択します。
7. データストアのマッピングは、VMの選択に基づいて自動的に選択されます。

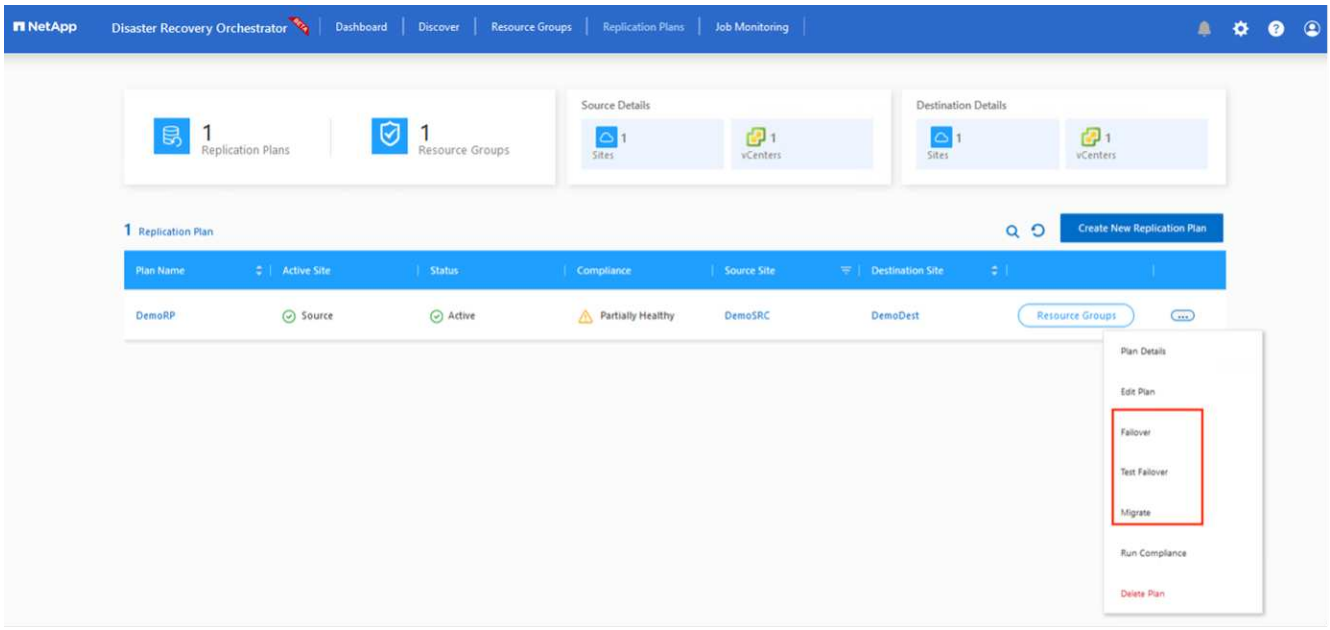
リージョン間レプリケーション（CRR）はボリュームレベルで実行されます。そのため、該当するボリューム上のすべてのVMがCRRデスティネーションにレプリケートされます。レプリケーションプランに含まれる仮想マシンのみが処理されるため、データストアに含まれるすべてのVMを選択してください。



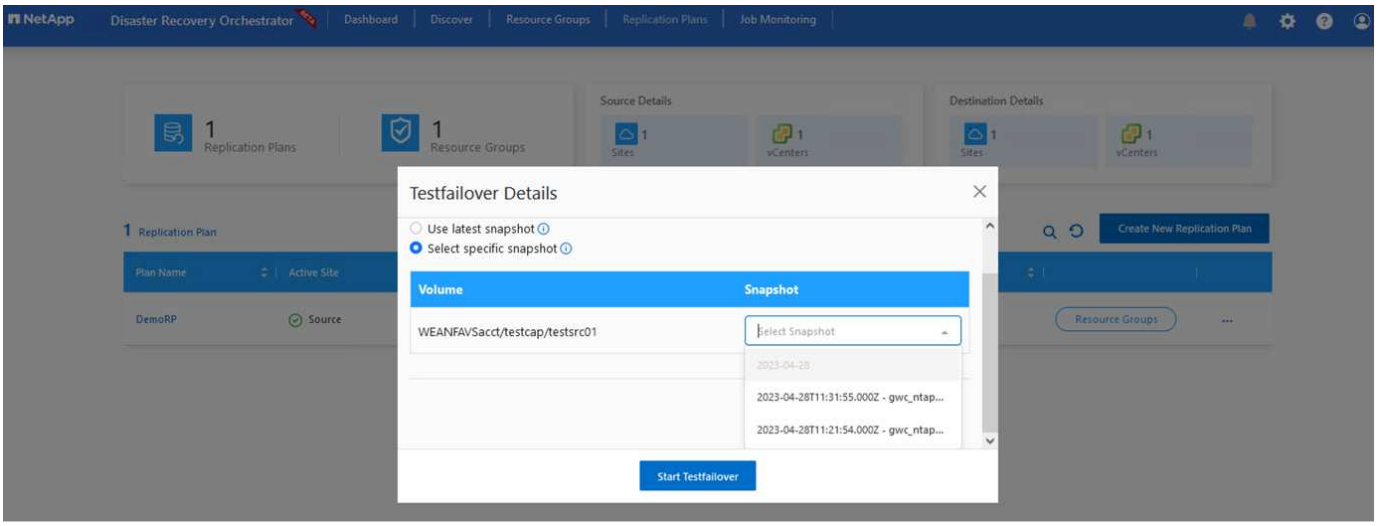
8. [VM details]で、必要に応じてVMのCPUパラメータとRAMパラメータのサイズを変更できます。これは、大規模な環境を小規模なターゲットクラスタにリカバリする場合や、1対1の物理VMwareインフラストラクチャをプロビジョニングせずにDRテストを実行する場合に非常に役立ちます。また、リソースグループ全体で選択したすべてのVMのブート順序とブート遅延（秒）を変更します。リソースグループのブート順序の選択時に選択したものから変更が必要な場合は'ブート順序を変更する追加オプションがありますデフォルトでは、リソースグループの選択時に選択された起動順序が使用されますが、この段階で変更を実行できます。



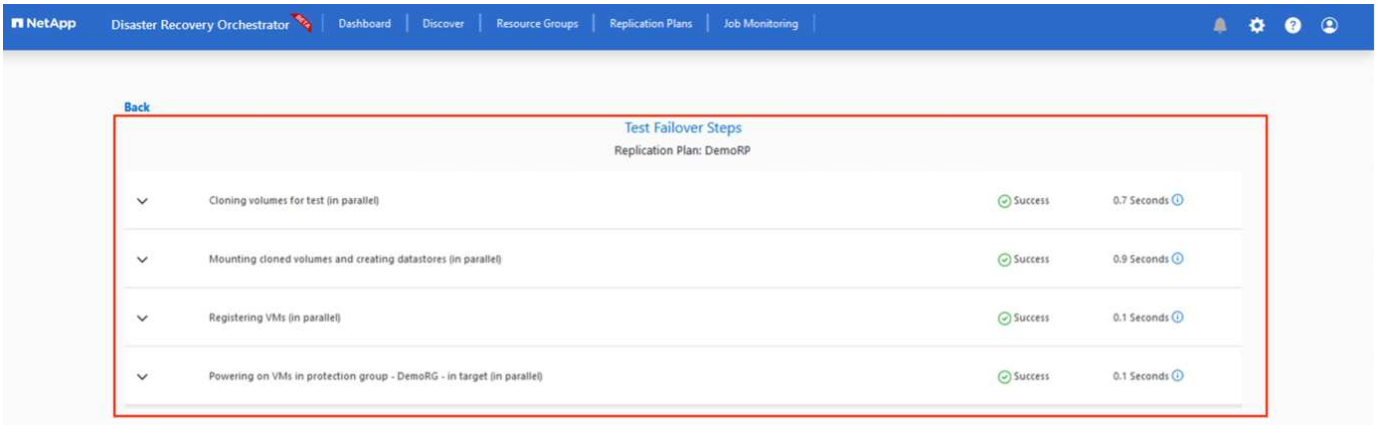
9. レプリケーションプランの作成*をクリックします。レプリケーションプランの作成後、要件に応じてフェイルオーバー、テストフェイルオーバー、移行オプションを実行できます。



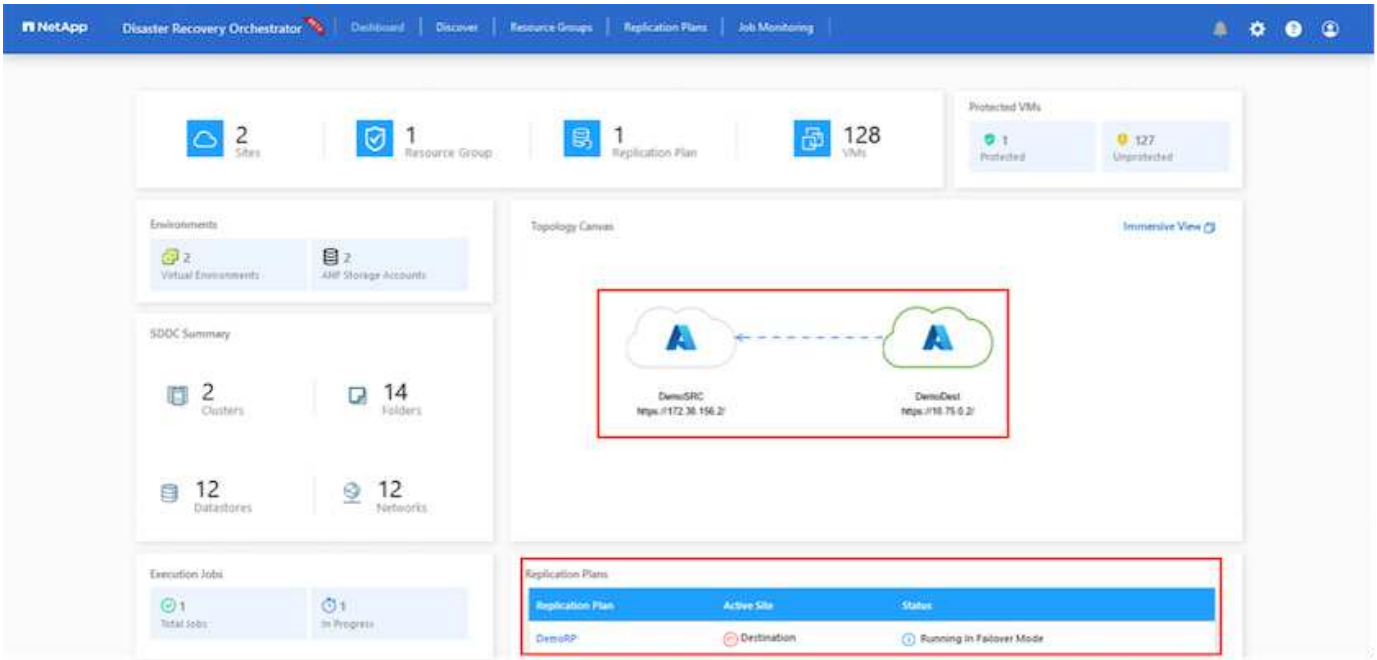
フェイルオーバーオプションとテストフェイルオーバーオプションでは、最新のSnapshotが使用されるか、ポイントインタイムSnapshotから特定のSnapshotを選択できます。ポイントインタイムオプションは、最新のレプリカがすでに侵害または暗号化されているランサムウェアなどの破損イベントに直面している場合に非常に役立ちます。DROには使用可能なすべてのタイムポイントが表示されます。



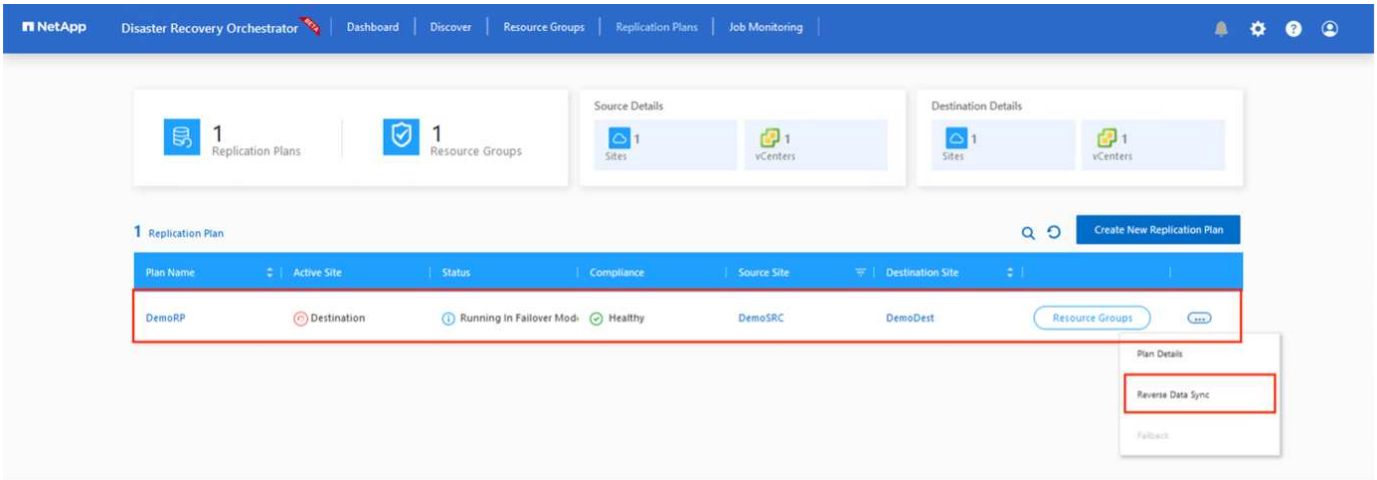
レプリケーションプランで指定した構成でフェイルオーバーまたはテストフェイルオーバーをトリガーするには、* Failover または Test Failover *をクリックします。タスクメニューでレプリケーション計画を監視できます。



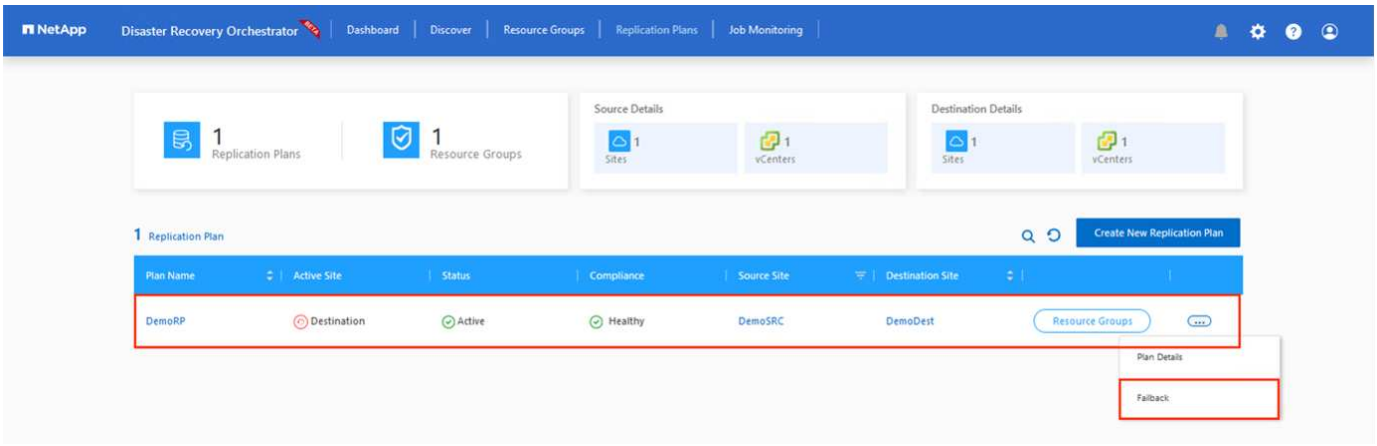
フェイルオーバーがトリガーされると、リカバリされた項目がセカンダリサイトのAVS SDDC vCenter（VM、ネットワーク、およびデータストア）に表示されます。デフォルトでは、VMはWorkloadフォルダにリカバリされます。

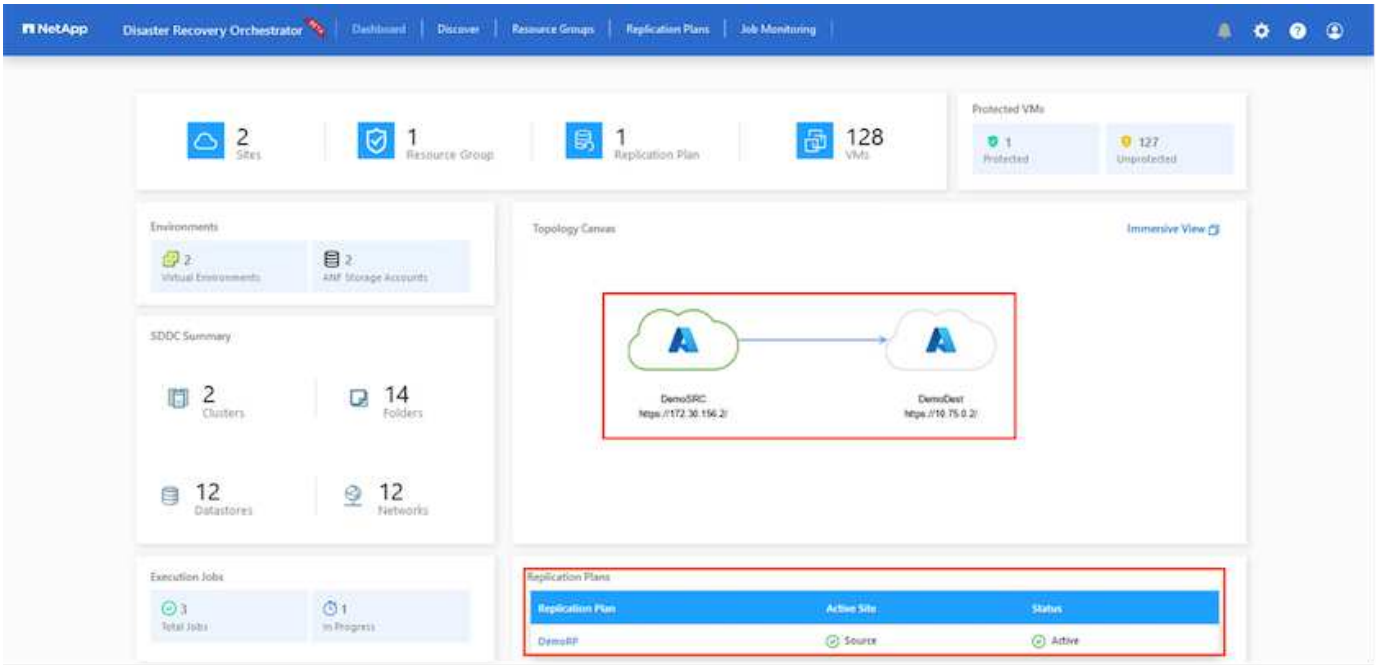


フェイルバックは、レプリケーションプランレベルでトリガーできます。テストフェイルオーバーの場合は、ティアダウンオプションを使用して変更をロールバックし、新しく作成したボリュームを削除できます。フェイルオーバーに関連するフェイルバックは、2つの手順で構成されます。レプリケーション計画を選択し、*[Reverse Data sync]*を選択します。



この手順が完了したら、フェイルバックをトリガーしてプライマリAVSサイトに戻ります。





Azureポータルから、セカンダリサイトのAVS SDDCに読み取り/書き込みボリュームとしてマッピングされた適切なボリュームについて、レプリケーションの健常性が切断されていることを確認できます。テストフェイルオーバー中、DROはデスティネーションボリュームまたはレプリカボリュームをマッピングしません。代わりに、必要なクロスリージョンレプリケーションSnapshotの新しいボリュームを作成し、そのボリュームをデータストアとして公開します。データストアは容量プールから追加の物理容量を消費し、ソースボリュームが変更されないようにします。特に、DRテスト中やトリアージワークフロー中もレプリケーションジョブを継続できます。さらに、このプロセスにより、エラーが発生した場合や破損したデータがリカバリされた場合にレプリカが破棄されるリスクなしに、リカバリをクリーンアップできます。

ランサムウェアからのリカバリ

ランサムウェアからのリカバリは困難な作業です。具体的には、IT部門が安全な回収ポイントを特定し、それが決定されたら、再発生する攻撃（スリープ状態のマルウェアや脆弱なアプリケーションなど）から回復したワークロードを確実に保護する方法を特定することは困難です。

DROは、組織が利用可能な任意の時点からリカバリできるようにすることで、これらの懸念に対処します。その後、ワークロードは機能していても分離されたネットワークにリカバリされるため、アプリケーションは相互に機能して通信できますが、南北方向のトラフィックにはさらされません。このプロセスにより、セキュリティチームはフォレンジックを実行し、隠れたマルウェアや眠っているマルウェアを特定するための安全な場所を提供します。

まとめ

Azure NetApp Files とAzure VMwareディザスタリカバリ解決策 には、次のようなメリットがあります。

- 効率的で耐障害性に優れたAzure NetApp Files のリージョン間レプリケーションを活用できます。
- Snapshotの保持機能により、任意の時点までリカバリできます。
- ストレージ、コンピューティング、ネットワーク、アプリケーションの検証に必要なすべての手順を完全に自動化して、数百から数千のVMをリカバリします。
- ワークロードのリカバリでは、「最新のSnapshotから新しいボリュームを作成する」プロセスが利用されます。このプロセスでは、レプリケートされたボリュームは操作されません。
- ボリュームまたはSnapshotのデータ破損のリスクを回避します。
- DRテストワークフロー中のレプリケーションの中断を回避します。
- 開発とテスト、セキュリティテスト、パッチとアップグレードのテスト、修正テストなど、DR以外のワークフローにもDRデータとクラウドコンピューティングリソースを活用できます。
- CPUとRAMを最適化すると、小規模なコンピューティングクラスタへのリカバリが可能になるため、クラウドコストを削減できます。

追加情報の参照先

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

- Azure NetApp Files のボリュームレプリケーションを作成します

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Azure NetApp Files のリージョン間レプリケーション

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"

- "Azure VMware 解決策の略"

  "https://learn.microsoft.com/en-us/azure/azure-vmware/introduction"

- Azure に仮想化環境を導入して設定

  "AzureでAVSをセットアップ"

- Azure VMware解決策 を導入して設定

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

Veeam Replicationと**Azure NetApp Files**データストアを使用した**Azure VMware**解決策へのディザスタリカバリ

作成者：Niyaz Mohamed - NetAppソリューションエンジニアリング

概要

Azure NetApp Files（ANF）データストアは、コンピューティングからストレージを切り離し、あらゆる組織がワークロードをクラウドに移行するために必要な柔軟性を実現します。お客様は、コンピューティングリソースとは別に拡張できる、柔軟性に優れたハイパフォーマンスなストレージインフラを利用できます。Azure NetApp Filesデータストアのは、オンプレミスのVMware環境のディザスタリカバリサイトとしてAzure VMware解決策（AVS）とともに導入を簡易化、最適化します。

Azure NetApp Files（ANF）ボリュームベースのNFSデータストアを使用すると、VMレプリケーション機能を提供する検証済みのサードパーティ製解決策を使用して、オンプレミスからデータをレプリケートできます。Azure NetApp Filesデータストアを追加することで、ストレージに対応する膨大な量のESXiホストでAzure VMware解決策SDDCを構築するよりも、コストを最適化できます。このアプローチは「パイロットライトクラスタ」と呼ばれます。パイロットライトクラスタは、Azure NetApp Filesデータストアの容量に加えて、最小限のAVSホスト構成（AVSノード×3）です。

その目的は、フェイルオーバーを処理するためのすべてのコアコンポーネントを備えた低コストのインフラストラクチャを維持することです。パイロットライトクラスタは、フェイルオーバーが発生した場合に、スケールアウトしてより多くのAVSホストをプロビジョニングできます。また、フェールオーバーが完了し、通常の動作が復元されると、パイロットライトクラスタは低コストの動作モードにスケールダウンできます。

本書の目的

この記事では、Azure NetApp FilesデータストアとVeeam Backup and Replicationを使用して、Veeam VMレプリケーションソフトウェア機能を使用してオンプレミスのVMware VMから（AVS）へのディザスタリカバリを設定する方法について説明します。

Veeam Backup & Replicationは、仮想環境向けのバックアップおよびレプリケーションアプリケーションです。仮想マシンがレプリケートされると、Veeam Backup & ReplicationがAVS上からレプリケートされます。ソフトウェアは、ターゲットAVS SDDCクラスタに、ネイティブのVMware vSphere形式でVMの正確なコピーを作成します。 Veeam Backup & Replicationは、コピーと元のVMの同期を維持します。DRサイトにはVMのコピーがすぐにマウントされているため、レプリケーションによって最適なRecovery Time Objective（RTO；目標復旧時間）が実現します。

このレプリケーションメカニズムにより、災害発生時にAVS SDDCでワークロードを迅速に開始できます。Veeam Backup & Replicationソフトウェアは、WAN経由のレプリケーションや低速接続のトラフィック転送も最適化します。また、重複データブロック、ゼロデータブロック、スワップファイル、「除外VMゲストOSファイル」も除外されます。ソフトウェアはレプリカトラフィックも圧縮します。レプリケーションジョブがネットワーク帯域幅全体を消費しないようにするには、WANアクセラレータとネットワークスロットリングルールを使用します。

Veeam Backup & Replicationのレプリケーションプロセスはジョブベースです。つまり、レプリケーションはレプリケーションジョブを設定して実行されます。災害が発生した場合は、レプリカコピーにフェイルオーバーすることで、フェイルオーバーをトリガーしてVMをリカバリできます。フェイルオーバーが実行されると、レプリケートされたVMが元のVMの役割を引き継ぎます。フェイルオーバーは'レプリカの最新の状態'または既知の任意のリストア・ポイントに対して実行できますこれにより、必要に応じてランサムウェアからのリカバリや個別のテストが可能Veeam Backup & Replicationには、さまざまなディザスタリカバリシナリオに対応するためのオプションが複数用意されています。

[]

解決策 の導入

手順の概要

1. Veeam Backup & Replicationソフトウェアは、適切なネットワーク接続を備えたオンプレミス環境で実行されます。
2. "Azure VMware解決策（AVS）の導入" プライベートクラウドと "Azure NetApp Filesデータストアの接続" Azure VMware解決策ホストに接続します。

   最小限の構成でセットアップされたパイロットライト環境は、DR目的で使用できます。インシデントが発生した場合、VMはこのクラスタにフェイルオーバーし、ノードを追加できます）。
3. Veeam Backup and Replicationを使用してVMレプリカを作成するためのレプリケーションジョブを設定します。
4. フェイルオーバープランを作成し、フェイルオーバーを実行
5. 災害が完了し、プライマリサイトが稼働したら、本番環境のVMにスイッチバックします。

AVSおよび**ANF**データストアへの**Veeam VM**レプリケーションの前提条件

1. Veeam Backup & ReplicationバックアップVMがソースとターゲットのAVS SDDCクラスタに接続されていることを確認します。
2. バックアップサーバは、短縮名を解決し、ソースvCenterとターゲットvCenterに接続できる必要があります。
3. ターゲットのAzure NetApp Filesデータストアに、レプリケートされたVMのVMDKを格納できるだけの十分な空きスペースが必要です。

追加情報については、「考慮事項と制限事項」を参照してください。 "こちらをご覧ください"。

展開の詳細

ステップ**1**：**VM**のレプリケート

Veeam Backup & ReplicationはVMware vSphereスナップショット機能を活用します。レプリケーション時に、Veeam Backup & ReplicationはVMware vSphereにVMスナップショットの作成を要求します。VMスナップショットは、仮想ディスク、システムの状態、設定、メタデータを含むVMのポイントインタイムコピーです。Veeam Backup & Replicationでは、Snapshotをレプリケーションのデータソースとして使用します。

VMをレプリケートするには、次の手順を実行します。

1. Veeam Backup & Replicationコンソールを開きます。
2. をクリックします。ジョブノードを右クリックし、[Replication Job]>[Virtual machine]を選択します。
3. ジョブ名を指定し、適切な詳細制御チェックボックスを選択します。次へをクリックします。
   - オンプレミスとAzure間の接続で帯域幅が制限されている場合は、[Replica seeding]チェックボックスをオンにします。
     - Azure VMware解決策SDDCのセグメントがオンプレミスサイトネットワークのセグメントと一致しない場合は、[ネットワークの再マッピング(AVS SDDCサイトと異なるネットワークの場合)]チェックボックスをオンにします。
   - オンプレミスの本番サイトのIPアドレス指定方式がターゲットAVSサイトのIPアドレス指定方式と異なる場合は、Replica Re-IP（異なるIPアドレス指定方式を使用するDRサイトの場合）チェックボックスを選択します。

     []
4. [Virtual * Machines]手順で、Azure VMware解決策SDDCに接続されたAzure NetApp Filesデータストアにレプリケートするを選択します。仮想マシンをVSANに配置して、使用可能なVSANデータストアの容量をいっぱいにすることができます。パイロットライトクラスタでは、3ノードクラスタの使用可能容量が制限されます。残りのデータはAzure NetApp Filesデータストアに簡単に配置してVMをリカバリしたり、CPU /メモリの要件に合わせてクラスタを拡張したりできます。をクリックし、[オブジェクトの追加]ウィンドウで必要な**VM**または**VM**コンテナを選択して[追加]*をクリックします。「 * 次へ * 」をクリックします。

   []
5. その後、デスティネーションをAzure VMware解決策SDDCクラスター/ホストとして選択し、VMレプリカ用の適切なリソースプール、VMフォルダ、FSx for ONTAPデータストアを選択します。次に、 [* 次へ *] をクリックします。

   []
6. 次の手順では、必要に応じてソースとデスティネーションの仮想ネットワーク間のマッピングを作成します。

   []
7. [ジョブ設定]ステップで、VMレプリカのメタデータや保持ポリシーなどを格納するバックアップリポジトリを指定します。
8. Data Transfer（データ転送）ステップで* Source（ソース）および Target（ターゲット）プロキシサーバーを更新し、 Automatic（自動）選択（デフォルト）のままにして Direct オプションを選択したままにして Next（次へ）*をクリックします。

9. [Guest Processing]ステップで、必要に応じて[Enable application-aware processing]オプションを選択します。「 * 次へ * 」をクリックします。

   []

10. レプリケーションジョブを定期的に実行するレプリケーションスケジュールを選択します。

    []

11. ウィザードの* Summary ステップで、レプリケーションジョブの詳細を確認します。ウィザードを終了した直後にジョブを開始するには、[完了]をクリックしたときにジョブを実行する*チェックボックスをオンにします。オンにしない場合は、チェックボックスをオフのままにします。次に、*[完了]*をクリックしてウィザードを閉じます。

    []

レプリケーションジョブが開始されると、指定されたサフィックスのVMがデスティネーションAVS SDDCクラスタ/ホストに取り込まれます。

[]

追加情報によるVeeamレプリケーションについては、 "レプリケーションの仕組み"

手順**2**：フェイルオーバープランを作成する

最初のレプリケーションまたはシードが完了したら、フェイルオーバープランを作成します。フェイルオーバープランは、依存するVMのフェイルオーバーを1つずつ、またはグループとして自動的に実行するのに役立ちます。フェイルオーバープランは、ブート遅延を含むVMの処理順序の青写真です。フェイルオーバープランは、重要な依存VMがすでに実行されていることを確認するのにも役立ちます。

プランを作成するには、*レプリカ*という新しいサブセクションに移動し、*フェイルオーバープラン*を選択します。適切なVMを選択します。Veeam Backup & Replicationは、この時点に最も近いリストアポイントを検索し、それらを使用してVMレプリカを開始します。

フェイルオーバープランを追加できるのは、初期レプリケーションが完了し、VMレプリカがReady状態になってからです。

フェイルオーバープランの実行時に同時に起動できるVMの最大数は10です。

フェイルオーバープロセス中は、ソースVMの電源はオフになりません。

フェイルオーバープラン*を作成するには、次の手順を実行します。

1. をクリックします。レプリカノードを右クリックし、[Failover Plans]>[Failover Plan]>[VMware vSphere]を選択します。

   []

2. 次に、計画の名前と概要を入力します。必要に応じて、フェイルオーバー前およびフェイルオーバー後のスクリプトを追加できます。たとえば、スクリプトを実行して、レプリケートされたVMを起動する前にVMをシャットダウンします。

   []

3. VMを計画に追加し、VMのブート順序とブート遅延を変更して、アプリケーションの依存関係を満たすようにします。

   []

レプリケーションジョブを作成するための追加情報については、を参照してください。 "レプリケーションジョブの作成"。

手順**3**：フェイルオーバープランを実行する

フェイルオーバー時には、本番サイトのソースVMがディザスタリカバリサイトのレプリカにスイッチオーバーされます。フェイルオーバープロセスの一環として、Veeam Backup & ReplicationはVMレプリカを必要なリストアポイントにリストアし、すべてのI/Oアクティビティをソース VMからそのレプリカに移動します。レプリカは、災害発生時だけでなく、DRドリルのシミュレーションにも使用できます。フェイルオーバーのシミュレーション中は、ソースVMは引き続き実行されます。必要なテストがすべて完了したら、フェイルオーバーを元に戻して通常の運用に戻すことができます。

フェイルオーバー中のIP競合を回避するために、ネットワークセグメンテーションが設定されていることを確認します。

フェイルオーバープランを開始するには、* Failover Plans タブをクリックし、フェイルオーバープランを右クリックします。**[***Start]を選択します。これにより、VMレプリカの最新のリストアポイントを使用してフェイルオーバーが実行されます。VMレプリカの特定のリストアポイントにフェイルオーバーするには、* Start to *を選択します。

[]

[]

VMレプリカの状態がReadyからFailoverに変わり、デスティネーションAzure VMware解決策（AVS）SDDCクラスタ/ホストでVMが起動します。

[]

フェイルオーバーが完了すると、VMのステータスが「Failover」に変わります。

[]

Veeam Backup & Replicationは、レプリカがReady状態に戻るまで、ソースVMのすべてのレプリケーションアクティビティを停止します。

フェイルオーバープランの詳細については、を参照してください。 "フェイルオーバープラン"。

手順4：本番サイトへのフェイルバック

フェイルオーバープランの実行中は中間ステップとみなされ、要件に基づいて確定する必要があります。オプションには次のものがあります。

- 本番環境へのフェイルバック：元のVMに切り替えて、VMレプリカの実行中に発生したすべての変更を元のVMに転送します。

> フェイルバックを実行すると、変更は転送されますが、パブリッシュされません。[Commit failback]*（元のVMが期待どおりに動作することが確認されたら）または[Undo failback]を選択して、元のVMが期待どおりに動作していない場合はVMレプリカに戻ります。

- フェイルオーバーを元に戻す-元のVMに切り替えて、VMレプリカの実行中に行った変更をすべて破棄します。
- 永続的フェイルオーバー-元のVMからVMレプリカに永続的に切り替え、このレプリカを元のVMとして使用します。

このデモでは、本番環境へのフェイルバックを選択しました。ウィザードの[Destination]ステップで[Failback to the original VM]が選択され、[Power on VM after restoring]チェックボックスが有効になっている。

[]

[]

[]

[]

フェイルバックコミットは、フェイルバック操作を完了する方法の1つです。フェイルバックがコミットされると、フェイルバックされたVM（本番VM）に送信された変更が想定どおりに機能していることが確認されます。コミット処理が完了すると、Veeam Backup & Replicationは本番用VMのレプリケーションアクティビティを再開します。

フェイルバックプロセスの詳細については、次のVeeamのドキュメントを参照してください：["レプリケーションのフェイルオーバーとフェイルバック"]。

[]

本番環境へのフェイルバックが成功すると、VMはすべて元の本番サイトにリストアされます。

[]

まとめ

Azure NetApp Filesデータストア機能を使用すると、Veeamまたは検証済みのサードパーティ製ツールを使用して、VMレプリカに対応するためだけに大規模なクラスタをセットアップするのではなく、パイロットライトクラスタを活用して低コストのDR解決策を提供できます。これにより、カスタマイズされたディザスタリカバリ計画を効率的に処理し、社内の既存のバックアップ製品をDR用に再利用できるようになり、オンプレミスのDRデータセンターを終了してクラウドベースのディザスタリカバリを実現できます。災害の場合はボタンをクリックしてフェイルオーバーしたり、災害が発生した場合は自動的にフェイルオーバーすることがで

きます。

このプロセスの詳細については、詳細なウォークスルービデオをご覧ください。

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278

Azure / AVSでのワークロードの移行

TR-4640：『**VMware HCX-Quickstart guide**』を使用してワークロードを**Azure NetApp Files** データストアに移行する

執筆者：NetApp Solutions Engineering

概要：**VMware HCX**、**Azure NetApp Files** データストア、**Azure VMware**解決策 を使用した仮想マシンの移行

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

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

このドキュメントでは、Azure NetApp Files データストアのプロビジョニングの手順を追ったガイダンスを示し、その後、さまざまなVM移行メカニズムを有効にするためのインターコネクト、ネットワーク拡張、WAN最適化を含む、オンプレミスおよびAzure VMware解決策 サイドのすべての主要コンポーネントを含む、VMware HCXのダウンロード、導入、設定を行います。

> VMware HCXはVMレベルで移行されるため、どのデータストアタイプでも動作します。このドキュメントAzure NetApp Files は、解決策 コスト効率に優れたVMwareクラウドの導入を計画している、ネットアップの既存のお客様と、ネットアップ以外のお客様を対象としています。

手順の概要

次のリストは、Azureクラウド側でHCX Cloud Managerをインストールおよび設定し、オンプレミスでHCX Connectorをインストールするために必要な手順の概要を示しています。

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

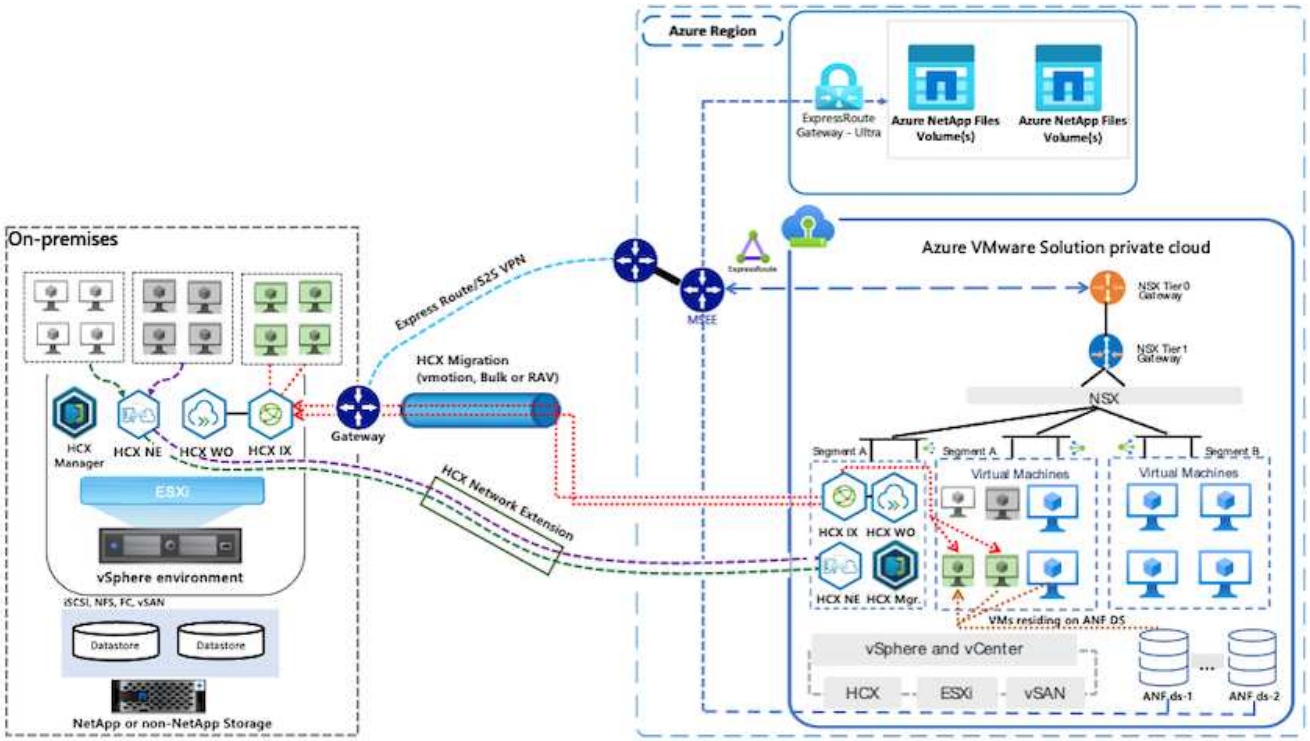
前提条件

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

HCx advancedはデフォルトオプションであり、VMware HCX Enterprise Editionはサポートチケットを通じても利用でき、追加料金なしでサポートされます。

- 既存のAzure VMware解決策 Software-Defined Data Center（SDDC）を使用するか、またはこれを使用してプライベートクラウドを作成します "ネットアップのリンク" またはこれ "Microsoftのリンク"。
- オンプレミスのVMware vSphere対応データセンターからVMと関連データを移行するには、データセンターからSDDC環境へのネットワーク接続が必要です。ワークロードを移行する前に、 "サイト間VPNまたはエクスプレスルートグローバルリーチ接続をセットアップします" オンプレミス環境とそれぞれのプライベートクラウドの間。
- オンプレミスのVMware vCenter Server環境からAzure VMware解決策 プライベートクラウドへのネットワークパスで、vMotionを使用したVMの移行がサポートされている必要があります。
- 必要なを確認します "ファイアウォールルールとポート" オンプレミスのvCenter ServerとSDDC vCenter間のvMotionトラフィックに許可されます。プライベートクラウドでは、vMotionネットワーク上のルーティングはデフォルトで設定されます。
- Azure NetApp Files NFSボリュームは、Azure VMware解決策 でデータストアとしてマウントする必要があります。詳細な手順を実行します "リンク" を使用して、Azure NetApp Files データストアをAzure VMwareソリューションホストに接続します。

テスト目的で、この検証に使用したオンプレミスのラボ環境はサイト間VPNを介して接続されており、オンプレミスでAzure VMware解決策 に接続できます。



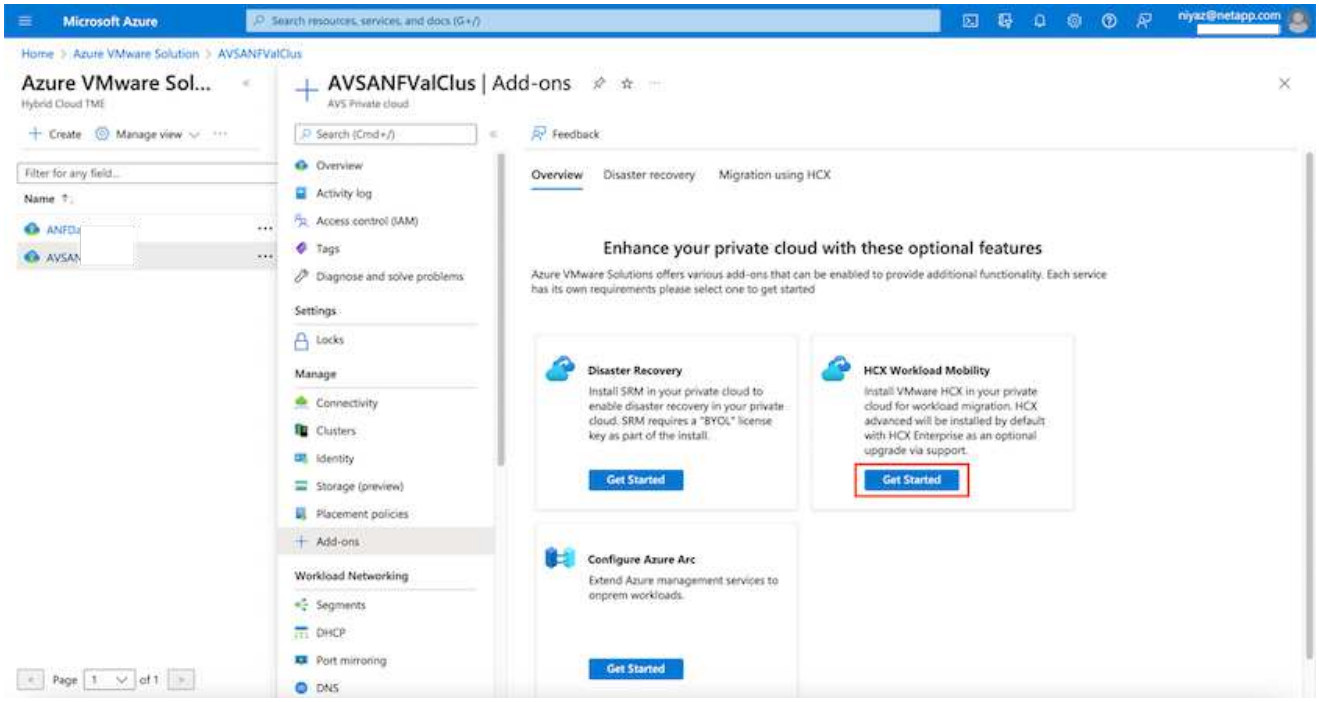
解決策 の導入

一連の手順に従って、この解決策 の導入を完了します。

手順1：アドオンオプションを使用して、**Azure Portal**から**HCX**をインストールする

インストールを実行するには、次の手順を実行します。

1. Azureポータルにログインし、Azure VMware解決策 プライベートクラウドにアクセスします。
2. 適切なプライベートクラウドを選択し、アドオンにアクセスします。これを行うには、* Manage > Add-ons *に移動します。
3. [HCX Workload Mobility]セクションで、[* Get Started*]をクリックします。

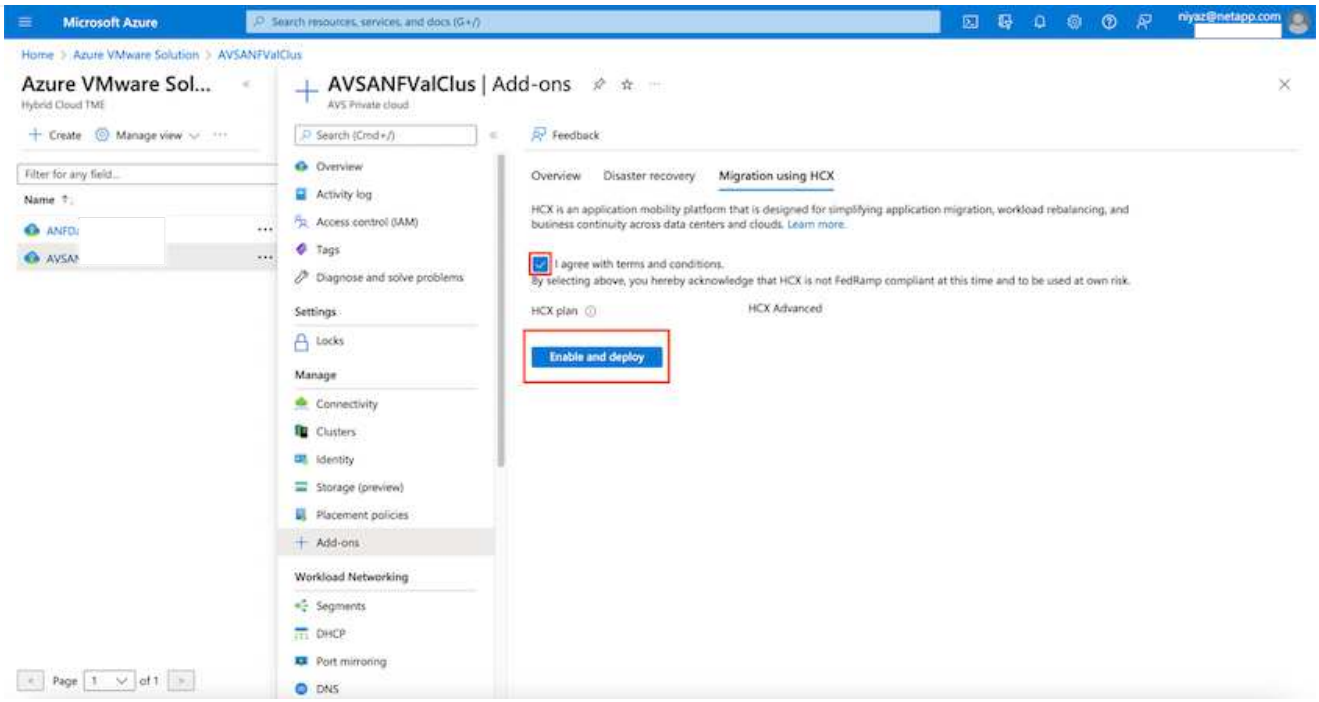


セクションのスクリーンショット。"]

1. [契約条件に同意します]オプションを選択し、[有効化して展開]をクリックします。

デフォルトの展開はHCX Advancedです。エンタープライズエディションを有効にするには、サポートリクエストを開きます。

導入には約25～30分かかります。



セクションの完了のスクリーンショット。"]

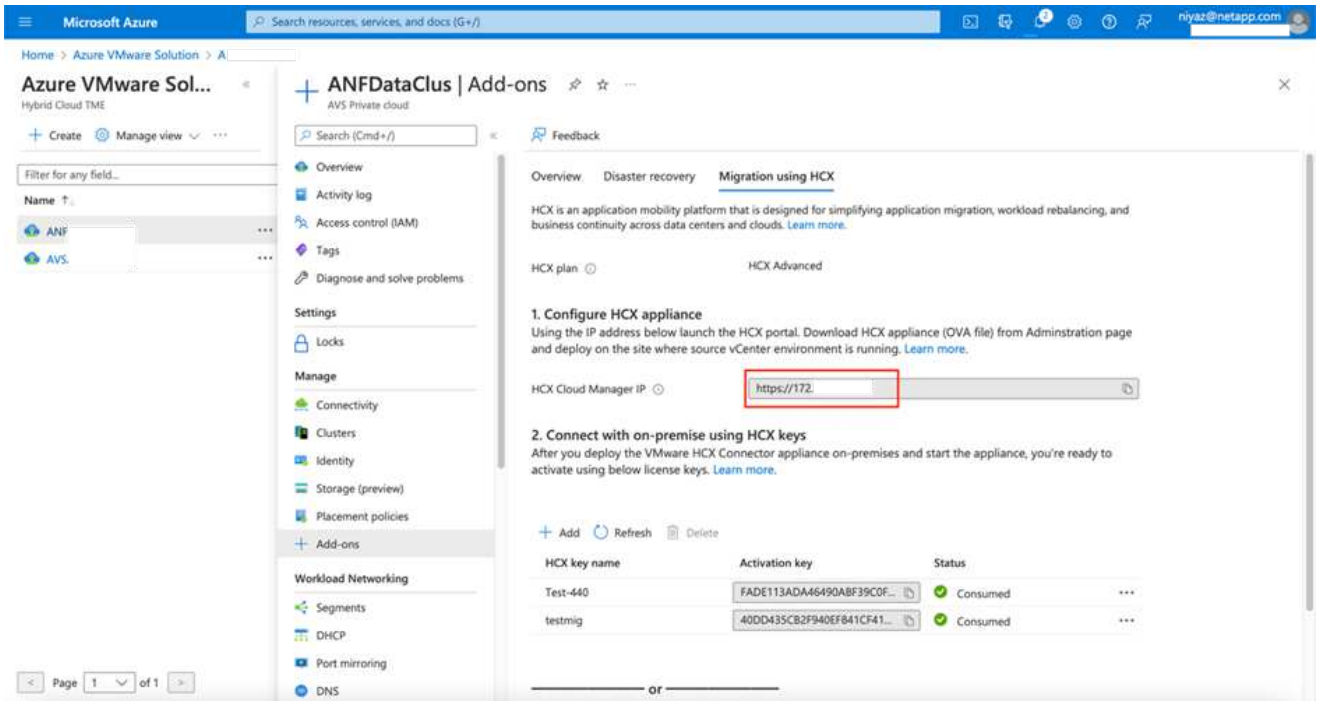
手順2：オンプレミスのvCenter ServerにインストーラOVAを導入する

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

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

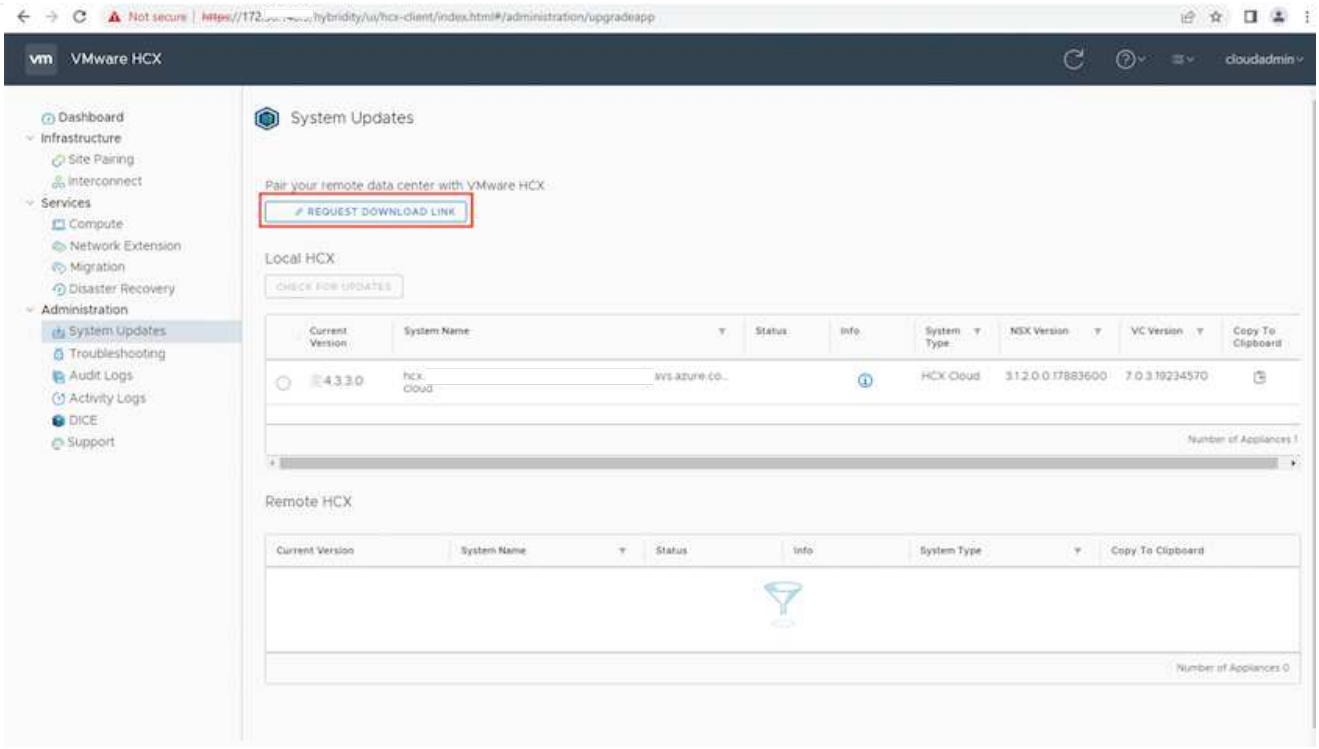
1. AzureポータルからAzure VMware解決策 にアクセスし、プライベートクラウドを選択して、* Manage > Add-ons > Migration * using HCXを選択し、HCX Cloud ManagerポータルをコピーしてOVAファイルをダウンロードします。

HCXポータルにアクセスするには、デフォルトのCloudAdminユーザー資格情報を使用します。

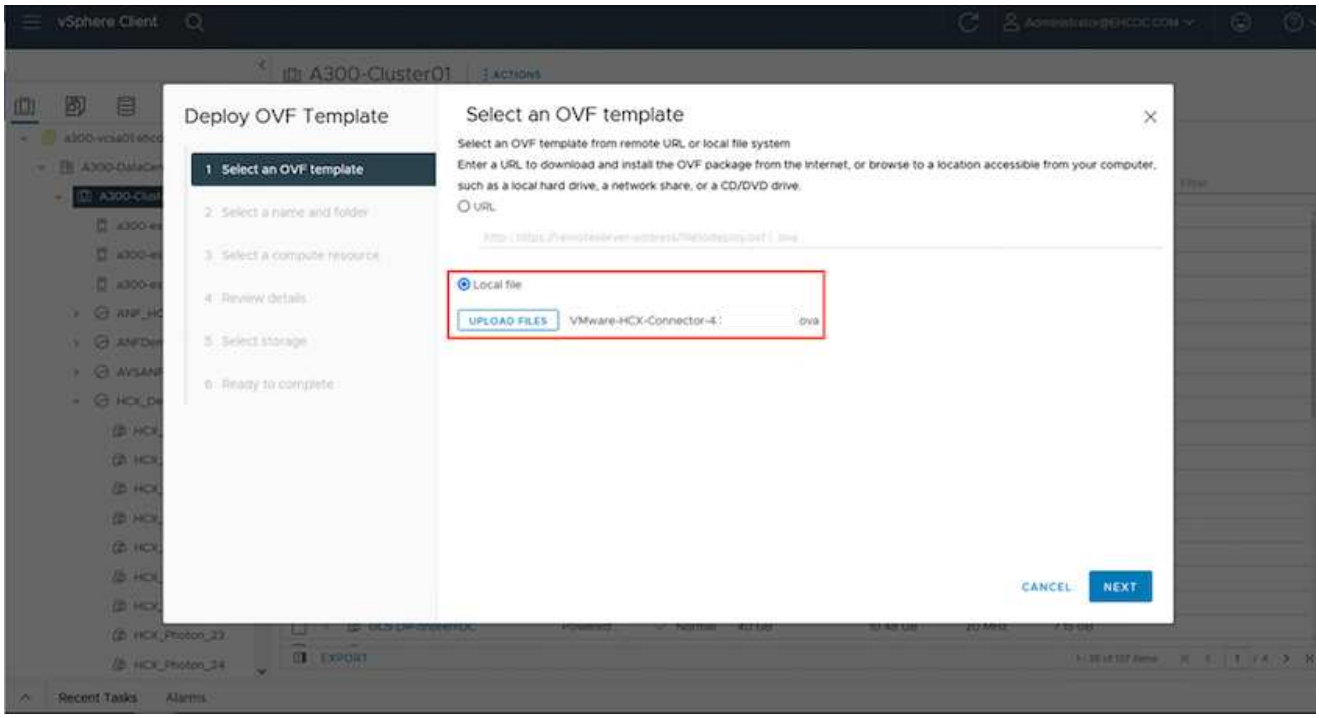


1. jumphostを使用してmailto：cloudadmin@vsphere.loca l [cloudadmin@vsphere.loca l^]でHCXポータルにアクセスしたら、* Administration > System Updates に移動し、 Request Download Link *をクリックします。

OVAをダウンロードするか、OVAにコピーしてブラウザに貼り付け、オンプレミスのvCenter Serverに導入するVMware HCX Connector OVAファイルのダウンロードプロセスを開始します。



1. OVAをダウンロードしたら、* Deploy OVF Template *オプションを使用して、OVAをオンプレミスのVMware vSphere環境に導入します。



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

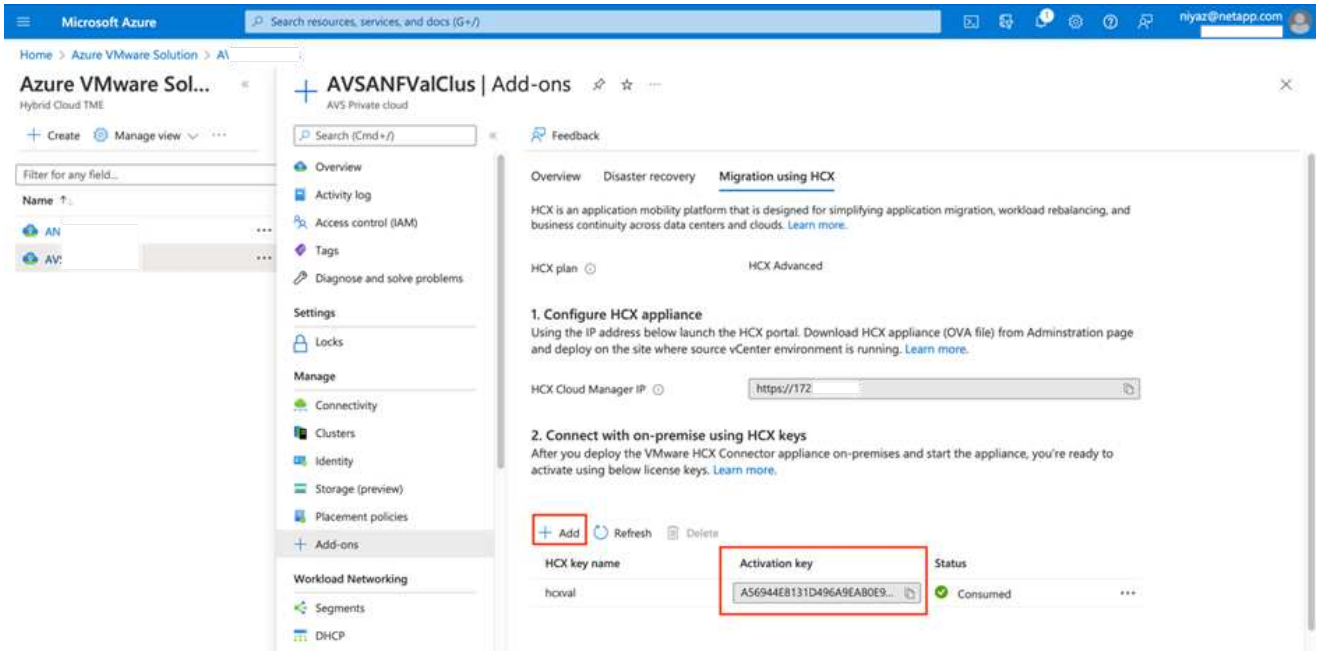
仮想アプライアンスの電源を手動でオンにします。

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

手順3：ライセンスキーを使用して**HCX**コネクタをアクティブにします

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

1. AzureポータルからAzure VMware解決策 にアクセスし、プライベートクラウドを選択して、* Manage > Add-ons > Migration Using HCX*を選択します。
2. [* HCXキーを使用してオンプレミスと接続する*]で、[*追加]をクリックしてアクティベーションキーをコピーします。



導入されているオンプレミスのHCXコネクタごとに別々のキーが必要です。

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

OVAの導入時に定義されたパスワードを使用します。

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

オンプレミスのHCXコネクタにはインターネットアクセスが必要です。

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

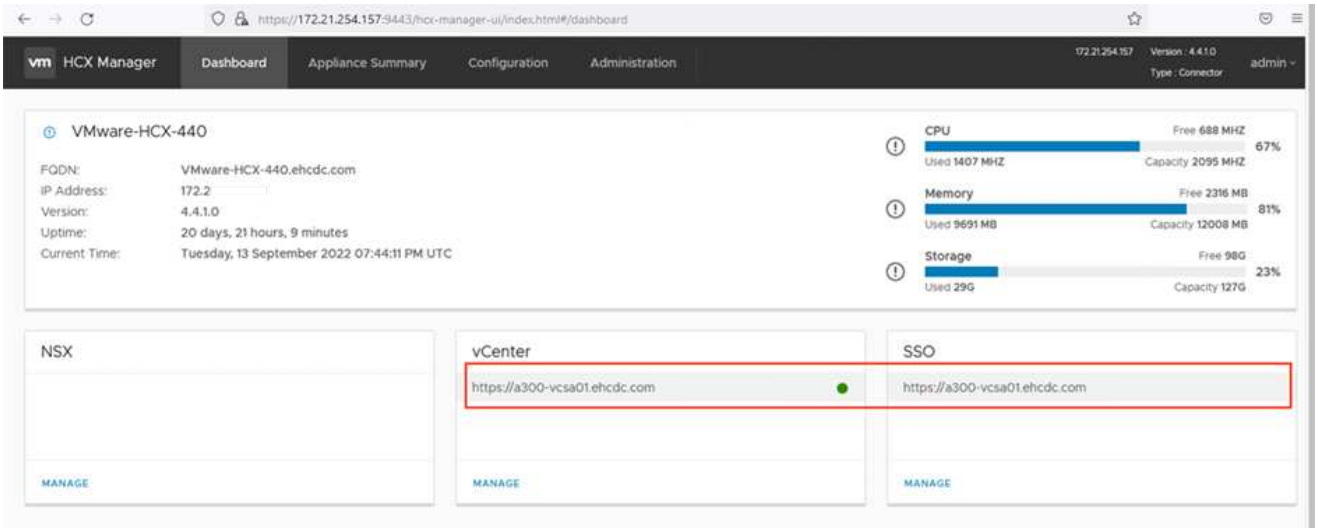
あとで接続の問題が発生しないようにFQDNを使用してください。

1. Configure SSO/PSC で、プラットフォームサービスコントローラの**FQDN**または**IP**アドレスを入力し、 Continue *をクリックします。

VMware vCenter ServerのFQDNまたはIPアドレスを入力します。

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

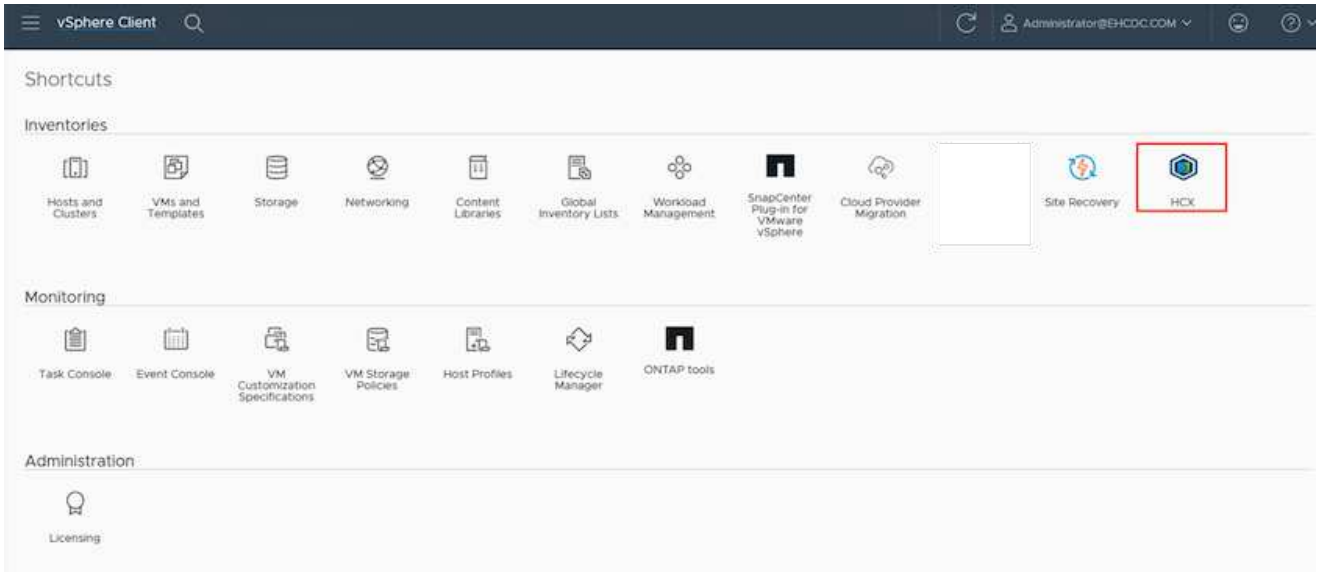
この処理には10~20分かかります。また、プラグインをvCenter Serverに追加する必要があります。



手順4：オンプレミスのVMware HCXコネクタをAzure VMware解決策 HCX Cloud Managerとペアリングします

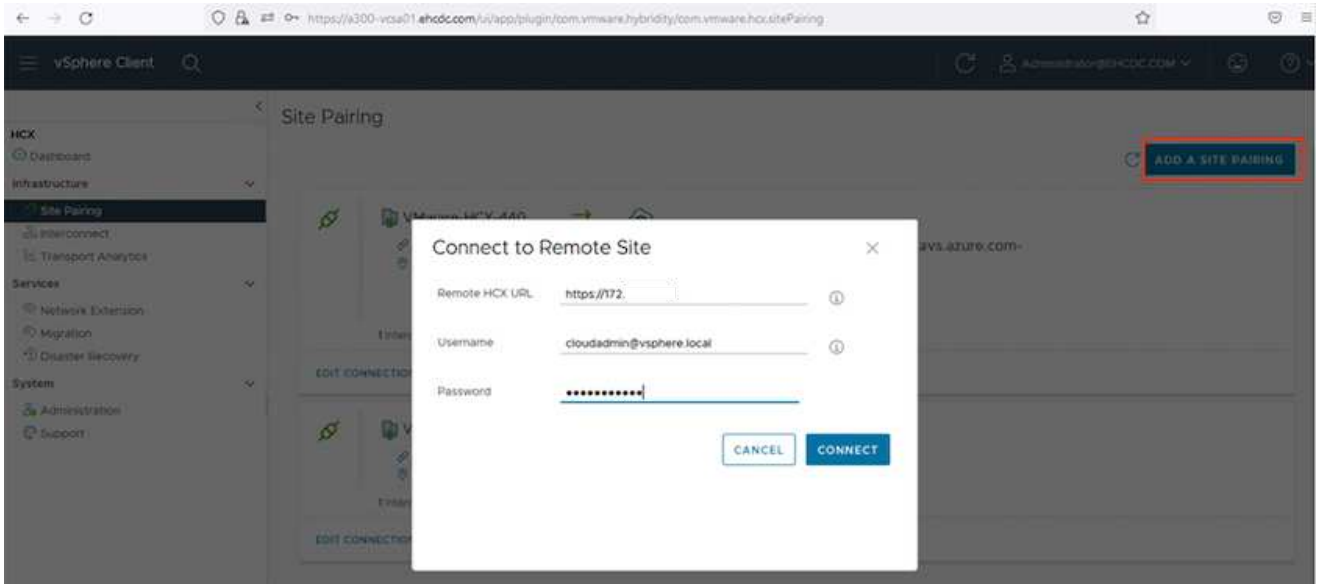
オンプレミスとAzure VMware解決策 の両方にHCX Connectorをインストールした後、このペアリングを追加して、オンプレミスのVMware HCX Connector for Azure VMware解決策 プライベートクラウドを構成します。サイトペアリングを設定するには、次の手順を実行します。

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



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

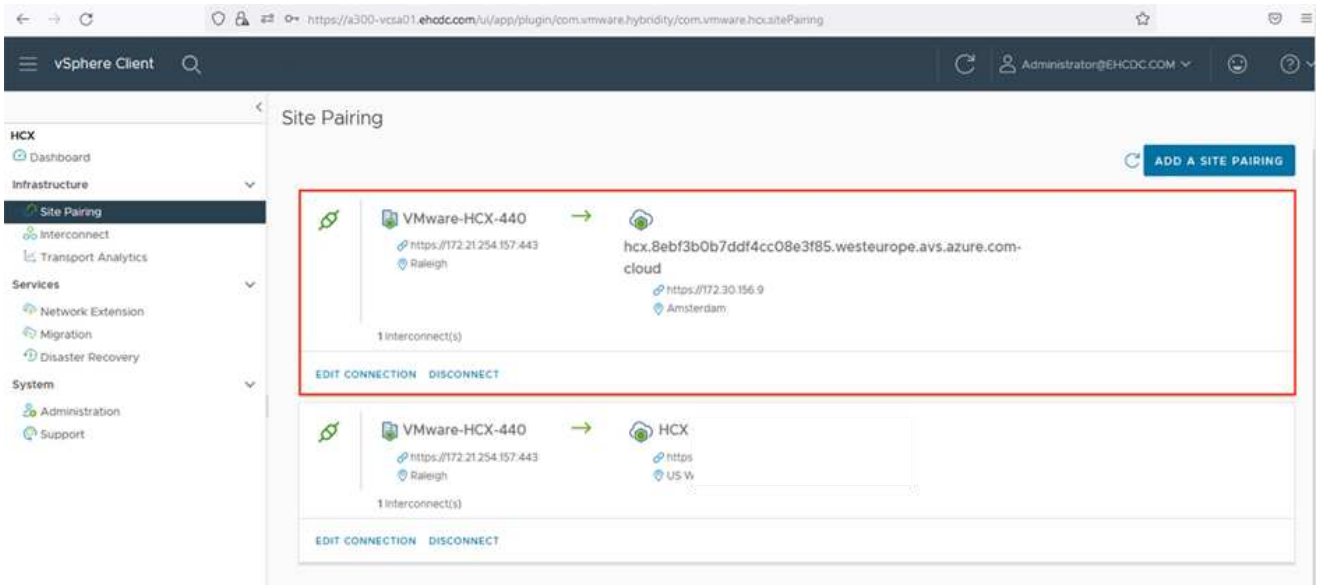
プライベートクラウドにアクセスするための、Azure VMware解決策 HCXのURLまたはIPアドレス、およびCloudAdminロールのクレデンシャルを入力します。



1. [接続] をクリックします。

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

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

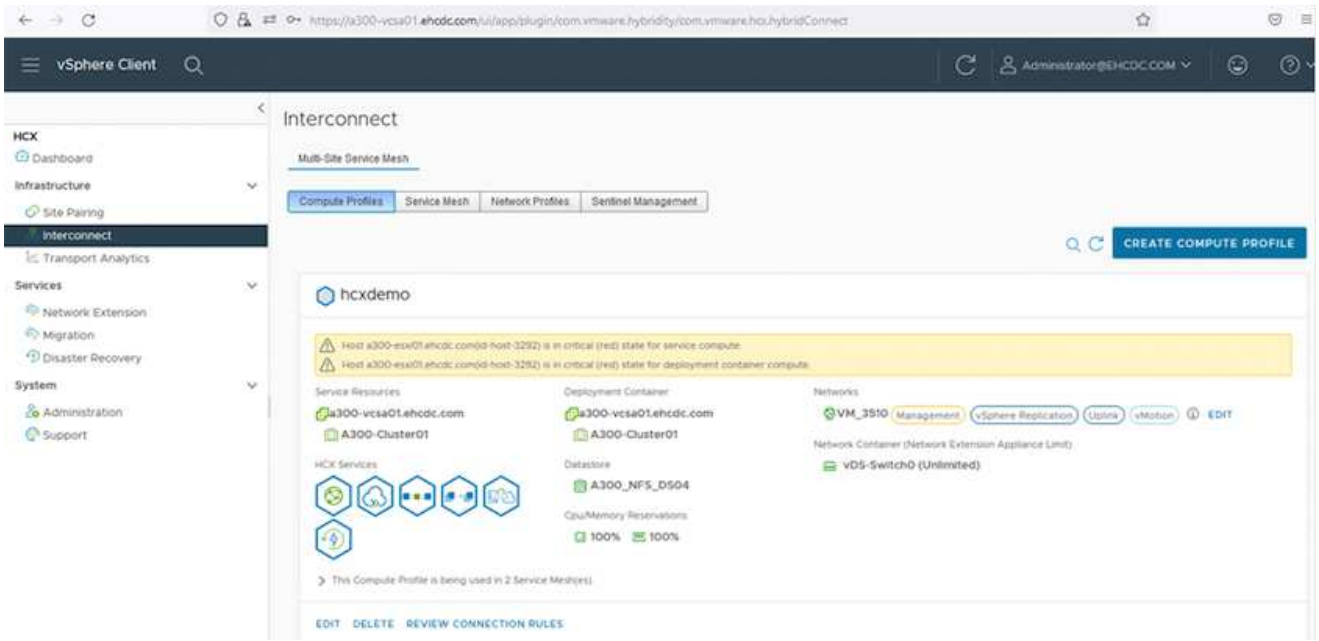


手順**5**：ネットワークプロファイル、コンピューティングプロファイル、およびサービスメッシュを設定します

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

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

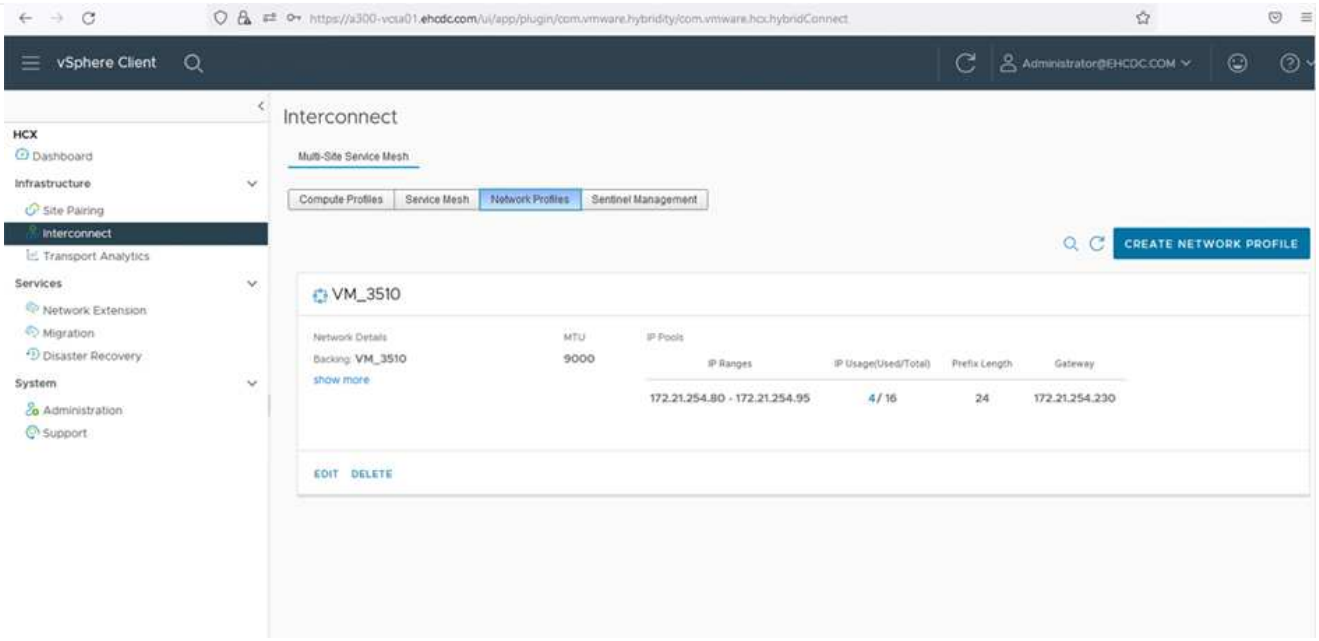
コンピューティングプロファイルでは、導入されるアプライアンスや、HCXサービスからアクセスできるVMwareデータセンターの部分などの導入パラメータを定義します。



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

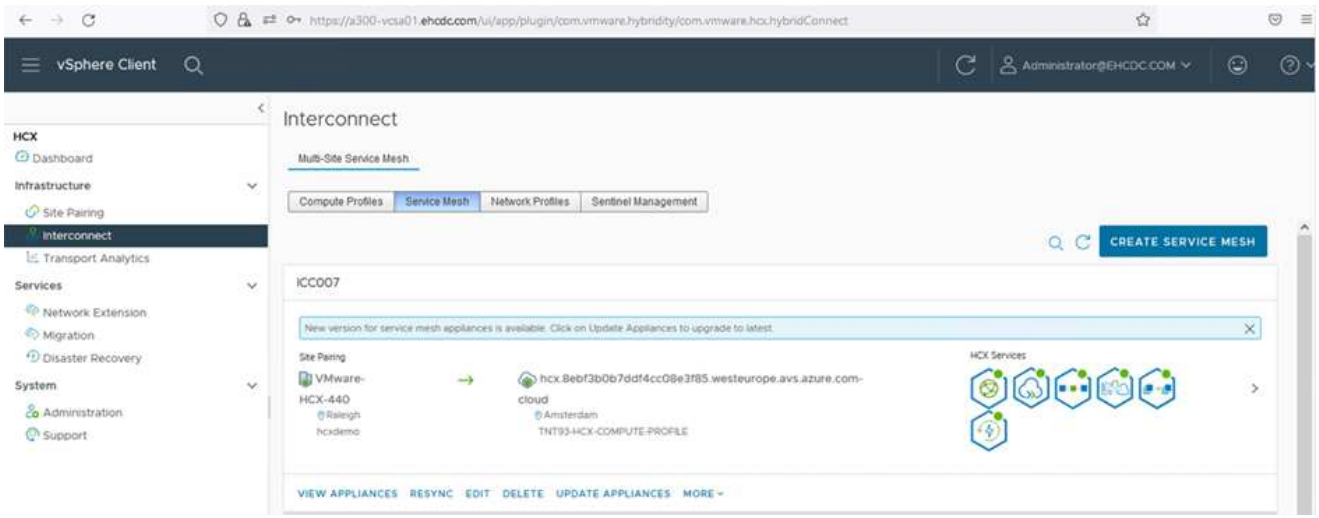
ネットワークプロファイルは、HCXが仮想アプライアンスに使用するIPアドレスとネットワークの範囲を定義します。

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

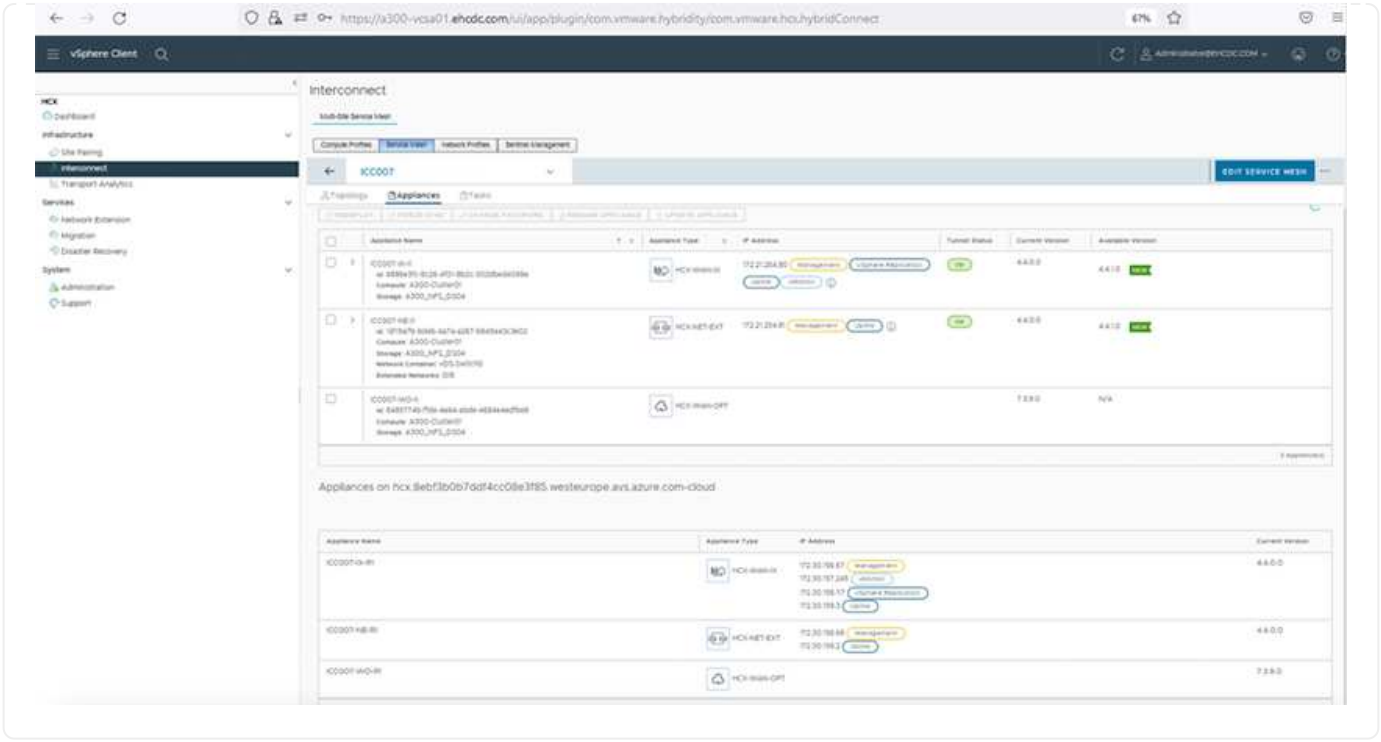


1. 現時点では、コンピューティングプロファイルとネットワークプロファイルは正常に作成されています。
2. [Interconnect（相互接続）]オプションの[* Service Mesh（サービスメッシュ*）]タブを選択してサービスメッシュを作成し、オンプレミスサイトとAzure SDDCサイトを選択します。
3. サービスメッシュは、ローカルとリモートのコンピューティングプロファイルとネットワークプロファイルのペアを指定します。

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



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


vSphere Client
Interconnect
ICC007
EDIT SERVICE MESH
Appliances
Appliances on hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud

手順**6**：ワークロードを移行する

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

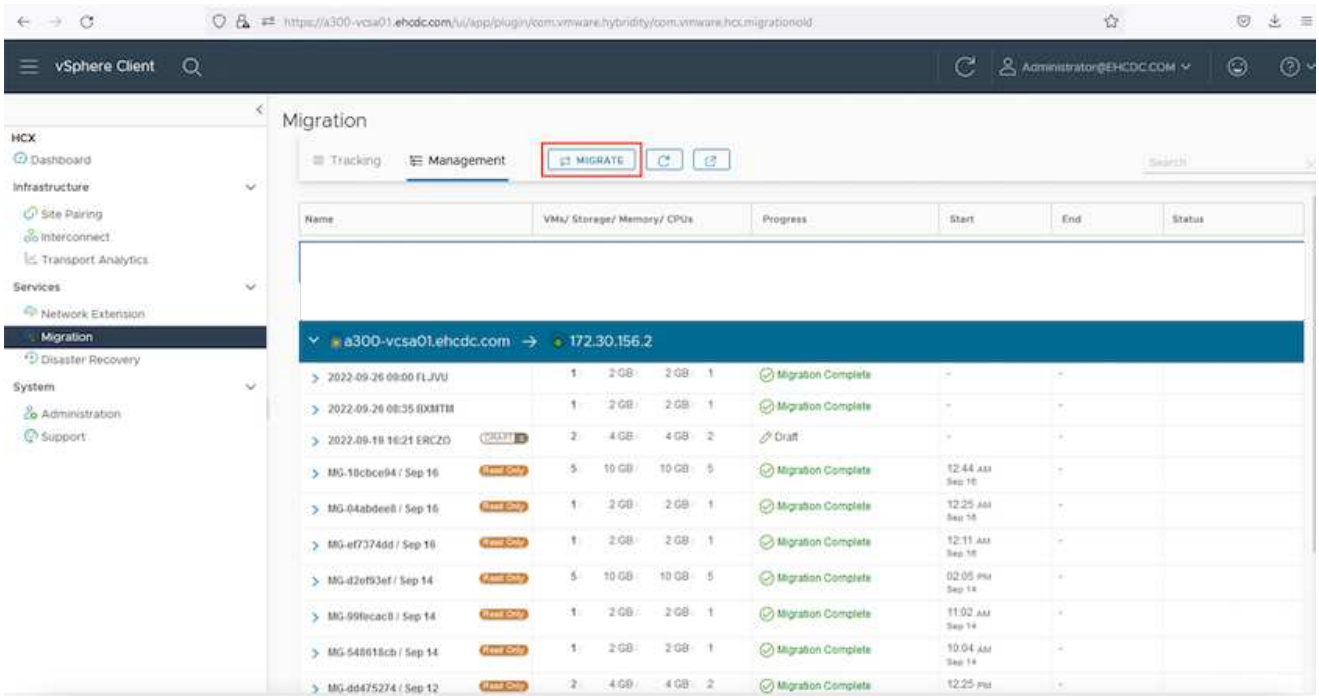
さまざまなHCX移行メカニズムの詳細については、を参照してください "VMware HCXの移行タイプ"。

一括移行

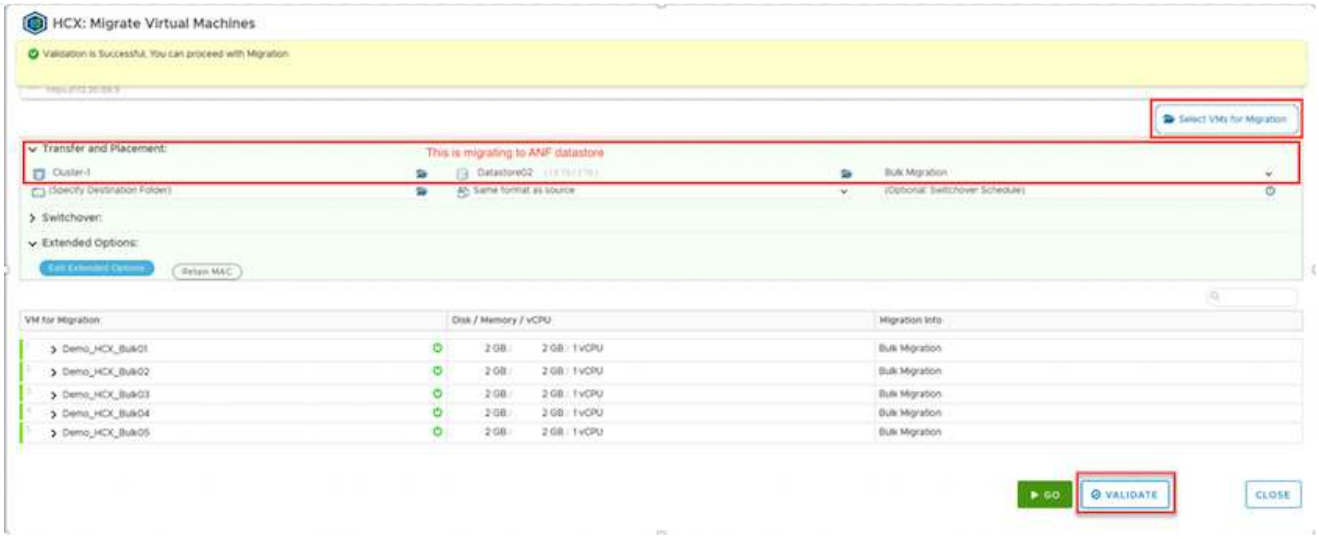
このセクションでは、一括移行のメカニズムについて詳しく説明します。HCXの一括移行機能では、移行先のvSphere HCXインスタンスでVMを再作成する際に、vSphere Replicationを使用してディスクファイルを移行します。

VMの一括移行を開始するには、次の手順を実行します。

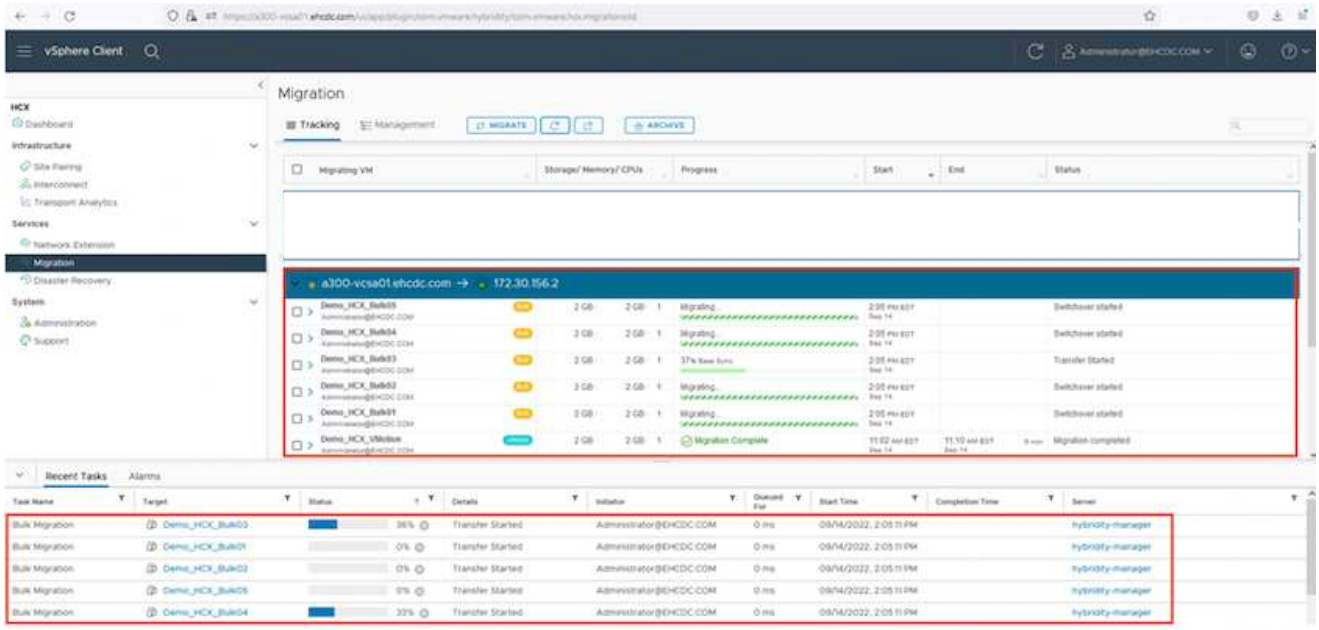
1. [**Services**]>[**Migration**]の下の[**Migrate**]タブにアクセスします。



1. [リモートサイト接続*]で、リモートサイト接続を選択し、ソースとデスティネーションを選択します。この例では、デスティネーションはAzure VMware解決策 SDDC HCXエンドポイントです。
2. [移行するVMの選択]をクリックします。これにより、すべてのオンプレミスVMが一覧表示されます。match:value式に基づいてVMを選択し、* Add *をクリックします。
3. [転送と配置]セクションで、移行プロファイルを含む必須フィールド（クラスタ、ストレージ、デスティネーション、ネットワーク）を更新し、[検証]をクリックします。

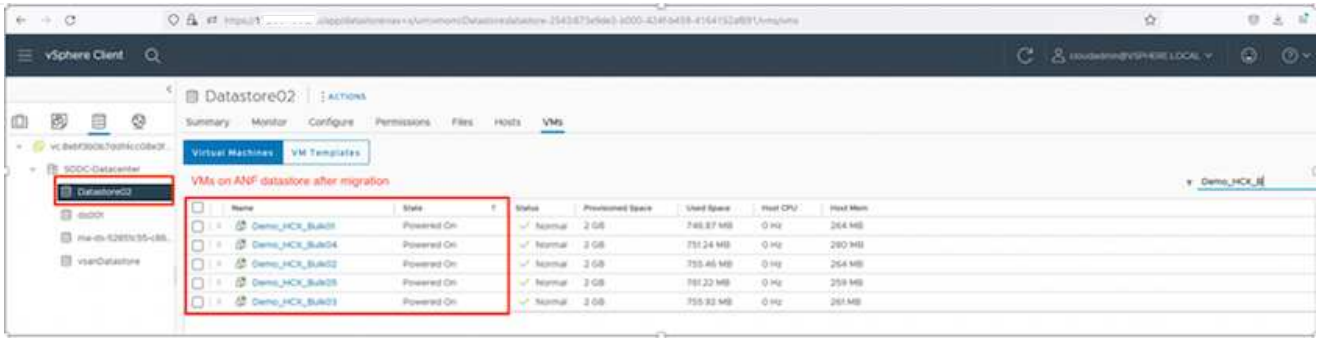


1. 検証チェックが完了したら、*移動*をクリックして移行を開始します。



この移行では、移行元VMディスクのデータをプレースホルダディスクにレプリケートできるように、移行先vCenter内の指定したAzure NetApp Files データストアにプレースホルダディスクが作成されます。HBRはターゲットへの完全な同期に対してトリガーされ、ベースラインが完了すると、RPO（目標復旧時点）サイクルに基づいて増分同期が実行されます。フル/増分同期が完了すると、特定のスケジュールが設定されていないかぎり、スイッチオーバーが自動的にトリガーされます。

1. 移行が完了したら、移行先のSDDC vCenterにアクセスして同じことを検証します。

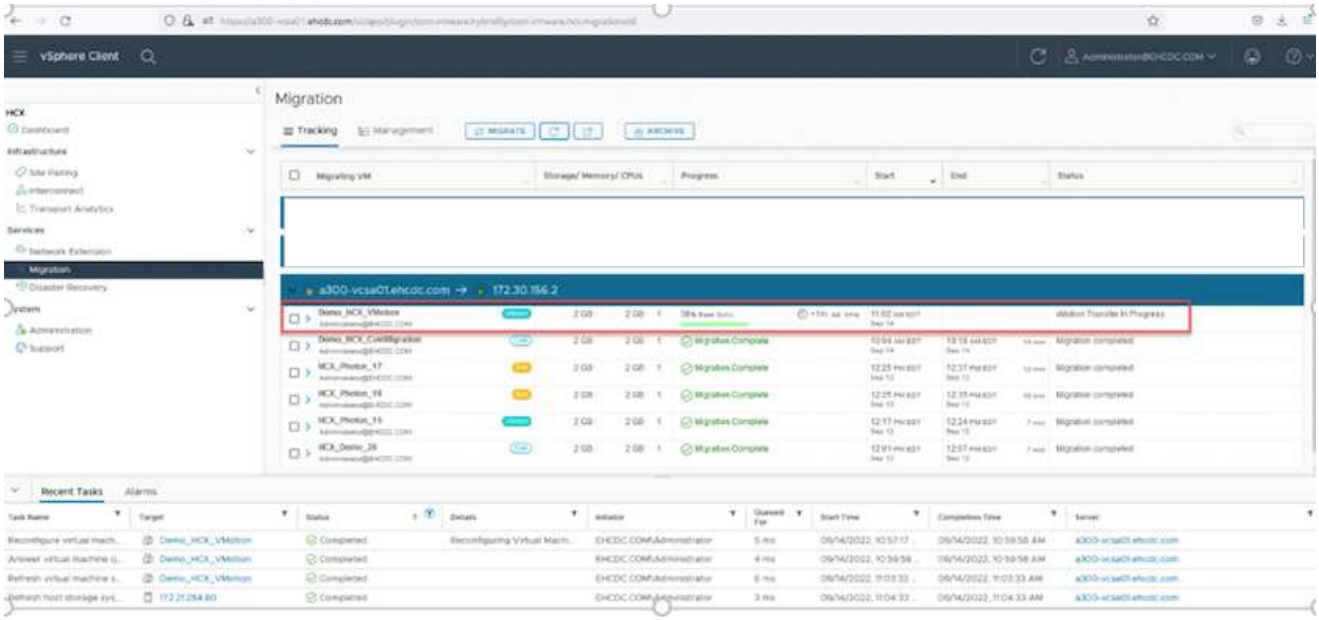


さまざまな移行オプションの詳細と、HCXを使用してオンプレミスからAzure VMware解決策 にワークロードを移行する方法については、を参照してください "VMware HCXユーザーガイド"。

このプロセスの詳細については、次のビデオをご覧ください。

HCXを使用したワークロードの移行

HCX vMotionオプションのスクリーンショットを次に示します。



このプロセスの詳細については、次のビデオをご覧ください。

HCx vMotion

移行に十分な帯域幅を使用できることを確認します。

移行先のANFデータストアには、移行を処理するための十分なスペースが必要です。

まとめ

オンプレミスのあらゆるタイプ/ベンダーストレージに存在するオールクラウドやハイブリッドクラウド、データのいずれをターゲットとしている場合でも、Azure NetApp Files とHCXは、アプリケーションワークロー

ドを展開して移行するための優れたオプションを提供し、データ要件をアプリケーションレイヤとシームレスにすることでTCOを削減します。どのようなユースケースでも、クラウドのメリット、一貫したインフラ、オンプレミスと複数のクラウドにわたる運用、ワークロードの双方向の移動、エンタープライズクラスの容量とパフォーマンスを迅速に実現するには、Azure VMware解決策 とAzure NetApp Files を選択してください。VMware vSphere Replication、VMware vMotion、Network File Copy（NFC；ネットワークファイルコピー）を使用してストレージの接続やVMの移行を行う場合と同じ手順を実行します。

重要なポイント

本ドキュメントの主な内容は次のとおりです。

- Azure NetApp Files をAzure VMware解決策 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。
- オンプレミスからAzure NetApp Files データストアへのデータの移行は簡単です。
- Azure NetApp Files データストアは、移行アクティビティ中に必要な容量やパフォーマンスに合わせて簡単に拡張および縮小することができます。

追加情報の参照先

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

- Azure VMware解決策 のドキュメント

"https://docs.microsoft.com/en-us/azure/azure-vmware/"

- Azure NetApp Files のドキュメント

"https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

- VMware HCXユーザーガイド

"https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"

Region Availability - ANFの補助的な**NFS**データストア

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

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

Google Cloud Platform GCVE のネットアップ機能

NetAppがGoogle Cloud Platform（GCP）にもたらす機能の詳細については、ゲスト接続ストレージデバイスとしてのNetAppや補完的なNFSデータストアから、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、ディザスタリカバリま

で、Google Cloud VMware Engine（GCVE）をご覧ください。

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。

- "GCP での GCVE の設定"
- "GCVE のネットアップストレージオプション"
- "ネットアップとVMwareのクラウドソリューション"

GCP での GCVE の設定

オンプレミスと同様に、 VM と移行を作成する本番環境に適した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。

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

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

セットアッププロセスは、次の手順に分けることができます。

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

詳細を表示します "GCVEの設定手順"。

GCVE のネットアップストレージオプション

ネットアップストレージは、接続されている推測データストアまたはNFSデータストア補助的なGCP GCVE内のいくつかの方法で利用できます。

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

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

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

詳細を表示します "GCVEのゲスト接続ストレージオプション"。

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

解決策のユースケース

ネットアップと VMware のクラウドソリューションを使用すれば、多くのユースケースを Azure AVS で簡単に導入できます。SEケースは、VMwareが定義したクラウド領域ごとに定義されます。

- 保護（ディザスタリカバリとバックアップ/リストアの両方を含む）
- 拡張
- 移動

"ネットアップの Google Cloud GCVE ソリューションをご覧ください"

GCP / GCVEでのワークロードの保護

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

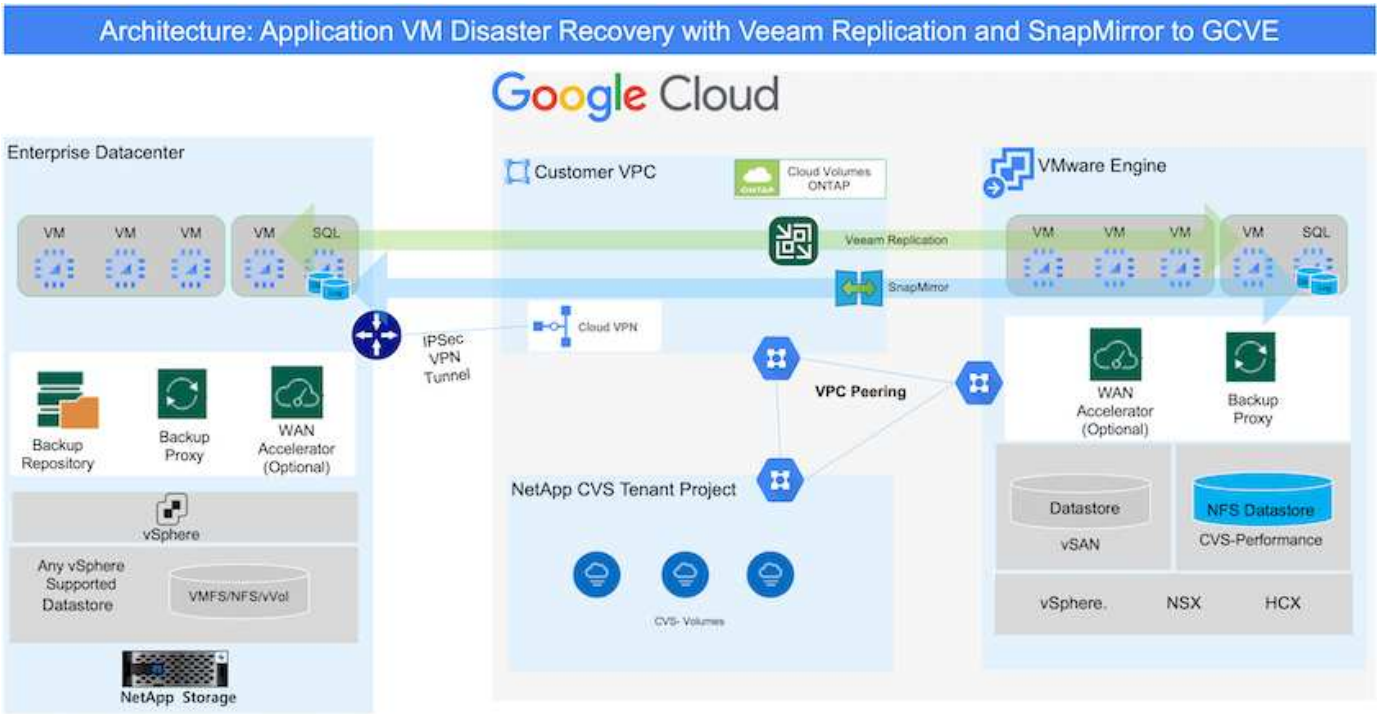
執筆者：ネットアップSuresh Thoppay

概要

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

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

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



前提条件

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

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

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

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

DR解決策 の導入

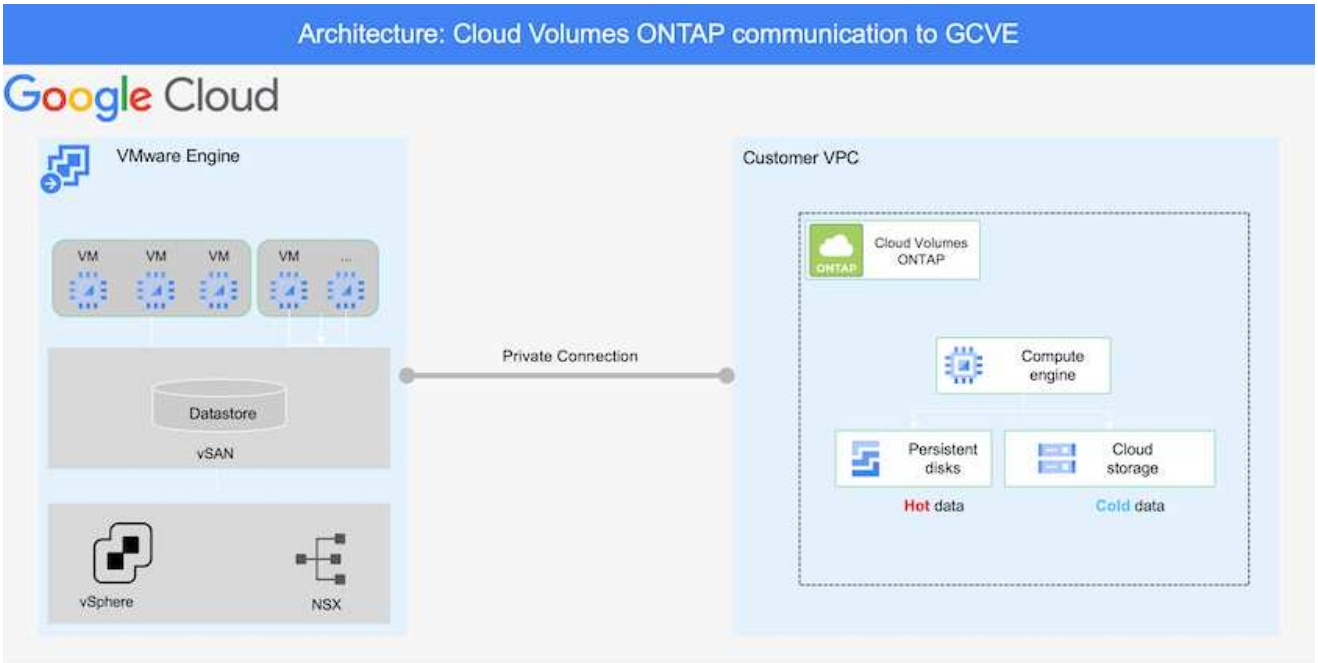
解決策 の導入の概要

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

展開の詳細

Google CloudでCVOを構成し、ボリュームをCVOにレプリケート

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



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

SnapCenterを使用したSQL VMの保護の確認

GCVEホストとCVOデータアクセスを設定する

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

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

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

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

Veeamコンポーネントをインストールします

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

VMレプリケーションを**Veeam**とセットアップする

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

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

Microsoft SQL Server VMのフェイルオーバー

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

この解決策 の利点

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

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

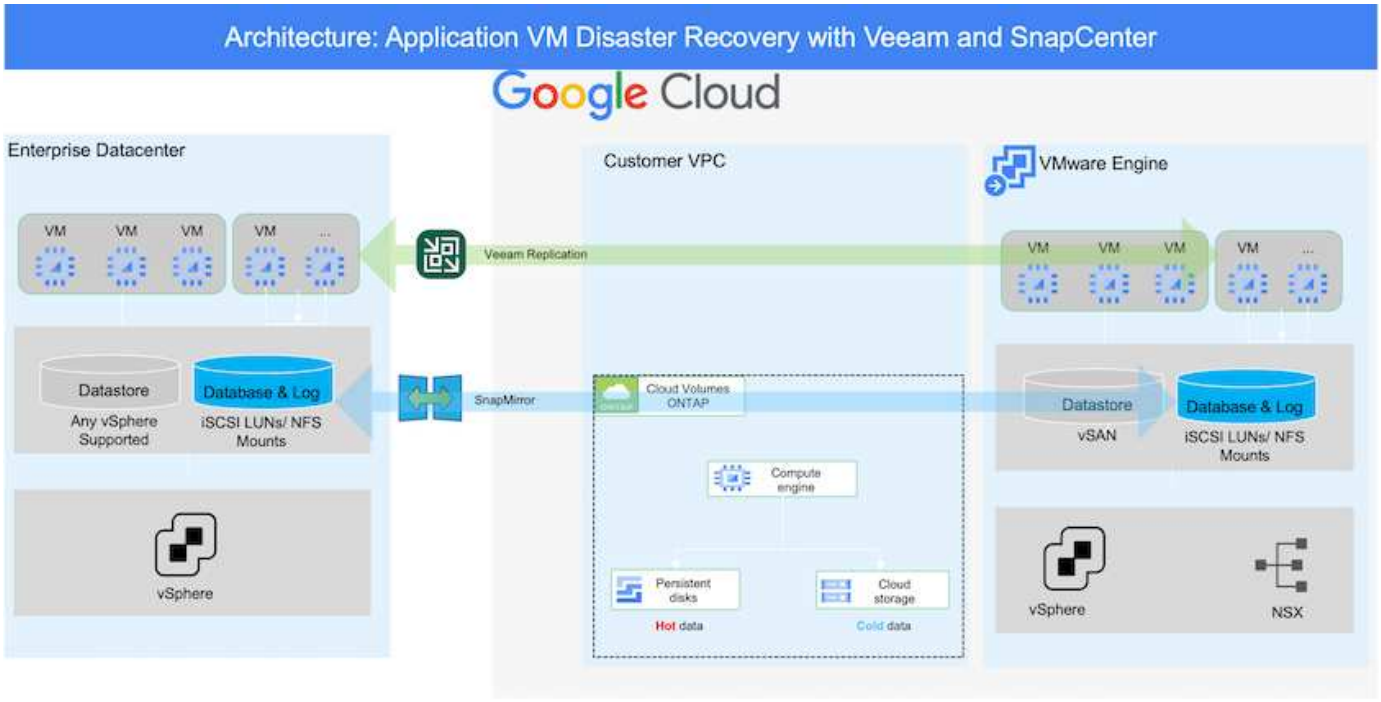
執筆者：ネットアップSuresh Thoppay

概要

クラウドへのディザスタリカバリは、耐障害性と対費用効果に優れた方法で、サイトの停止やランサムウェアなどのデータ破損からワークロードを保護します。NetApp SnapMirrorを使用すると、ゲスト接続ストレージを使用するオンプレミスのVMwareワークロードを、Google Cloudで実行されているNetApp Cloud Volumes

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

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



前提条件

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

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

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

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

DR解決策 の導入

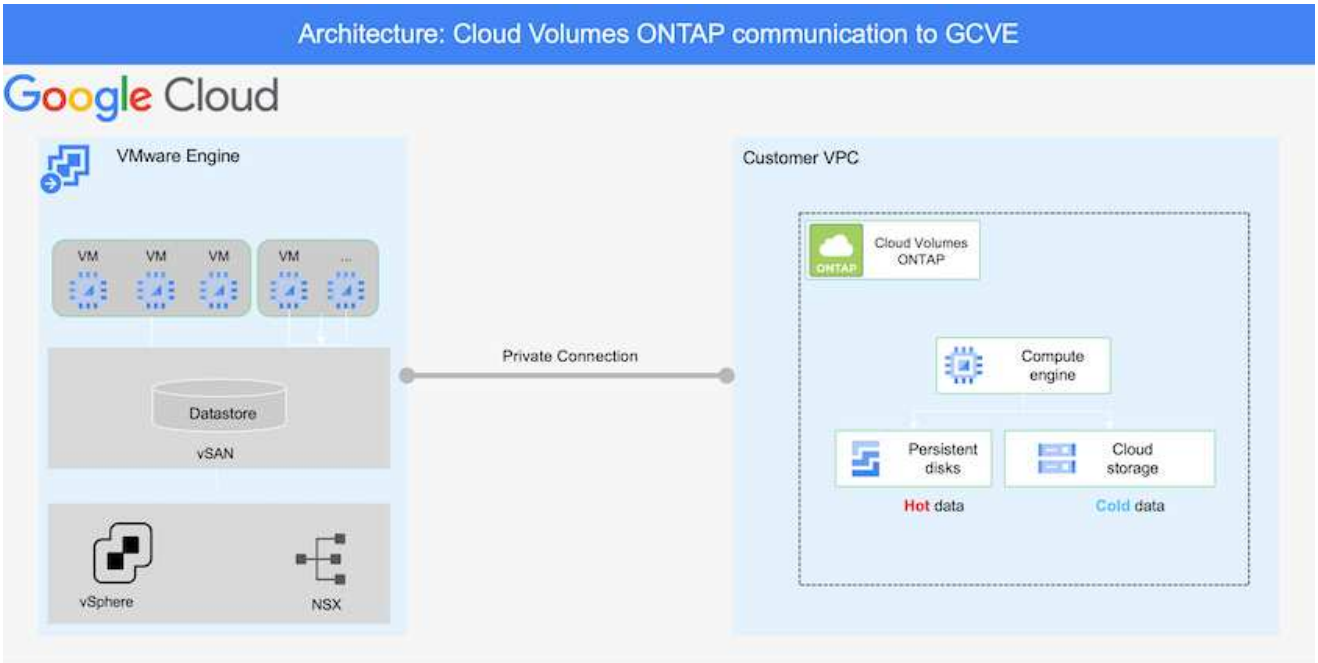
解決策 の導入の概要

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

展開の詳細

Google CloudでCVOを構成し、ボリュームをCVOにレプリケート

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



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

SnapCenter を使用してレプリケーションを設定する

GCVEホストとCVOデータアクセスを設定する

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

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

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

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

Veeamコンポーネントをインストールします

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

VMレプリケーションを**Veeam**とセットアップする

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

vSphere VMレプリケーションジョブをセットアップします

Microsoft SQL Server VMのフェイルオーバー

Microsoft SQL Server VMのフェイルオーバー

この解決策 の利点

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

GCP / GCVEでのワークロードの移行

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

執筆者：NetApp Solutions Engineering

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

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

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

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

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

手順の概要

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

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

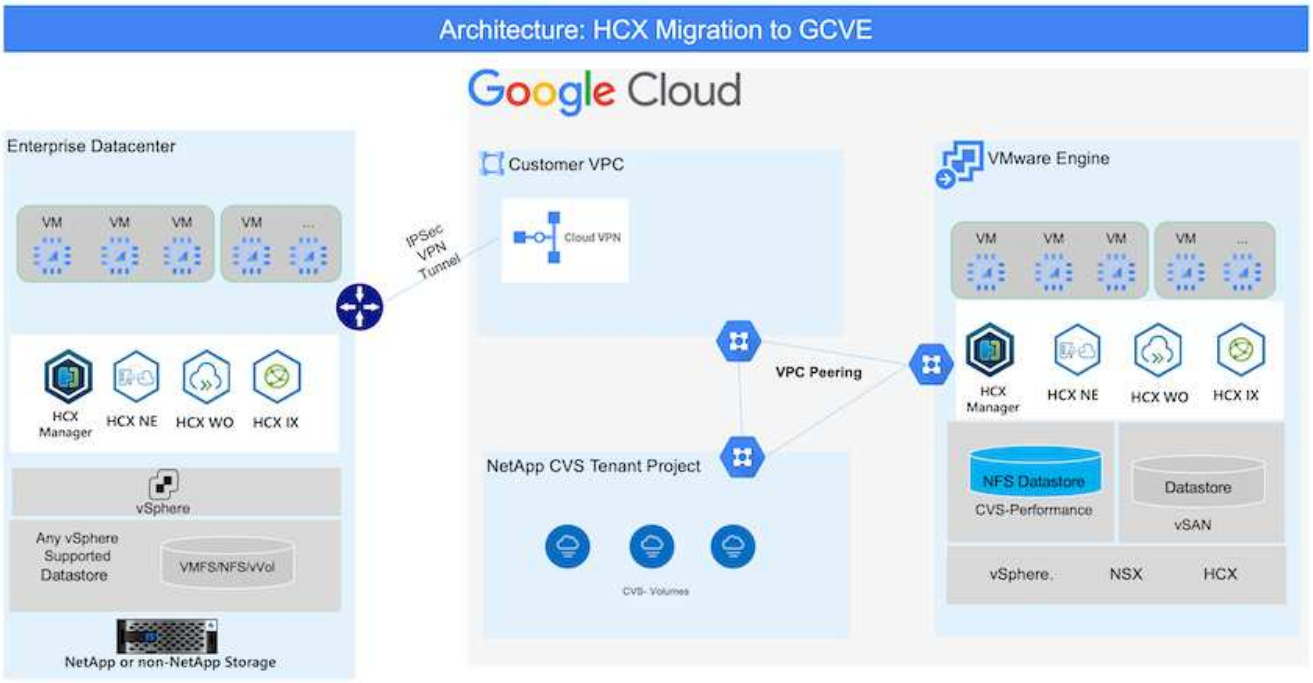
前提条件

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

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

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

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



HCXの詳細な図については、を参照してください "VMwareへのリンク"

解決策 の導入

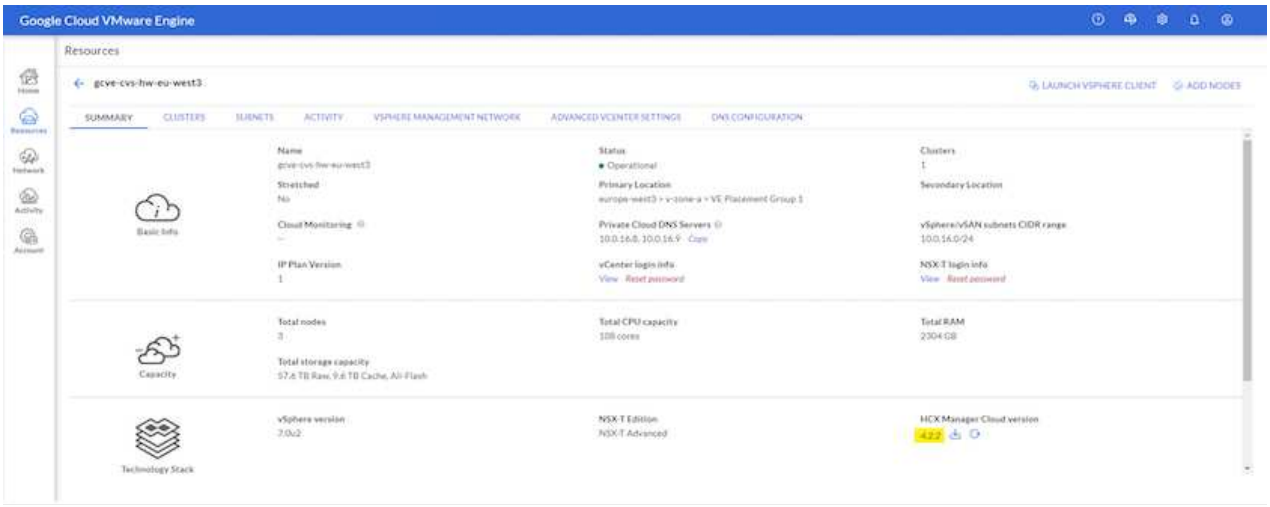
一連の手順に従って、この解決策 の導入を完了します。

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

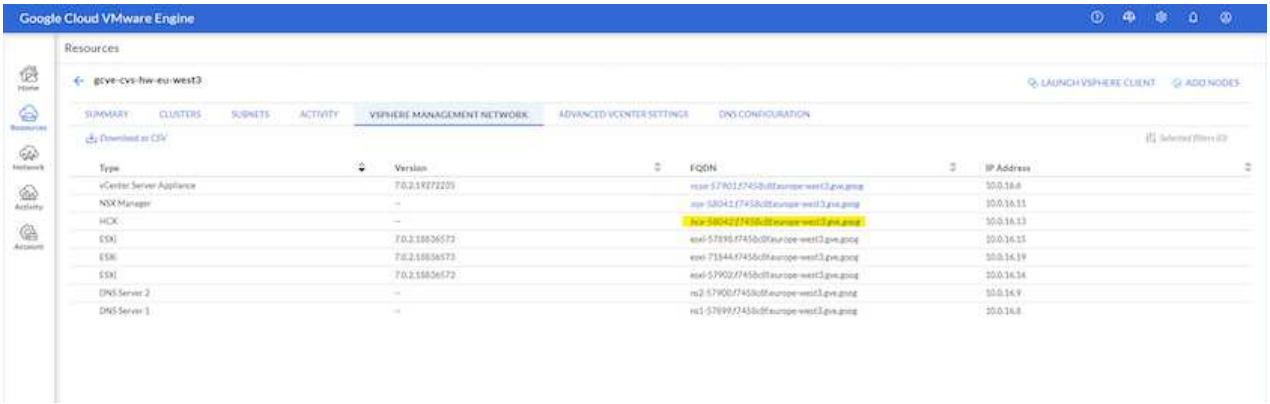
VMware Engineでプライベートクラウドをプロビジョニングすると、HCx Cloud Managerコンポーネントが自動的にインストールされます。サイトペアリングを準備するには、次の手順を実行します。

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

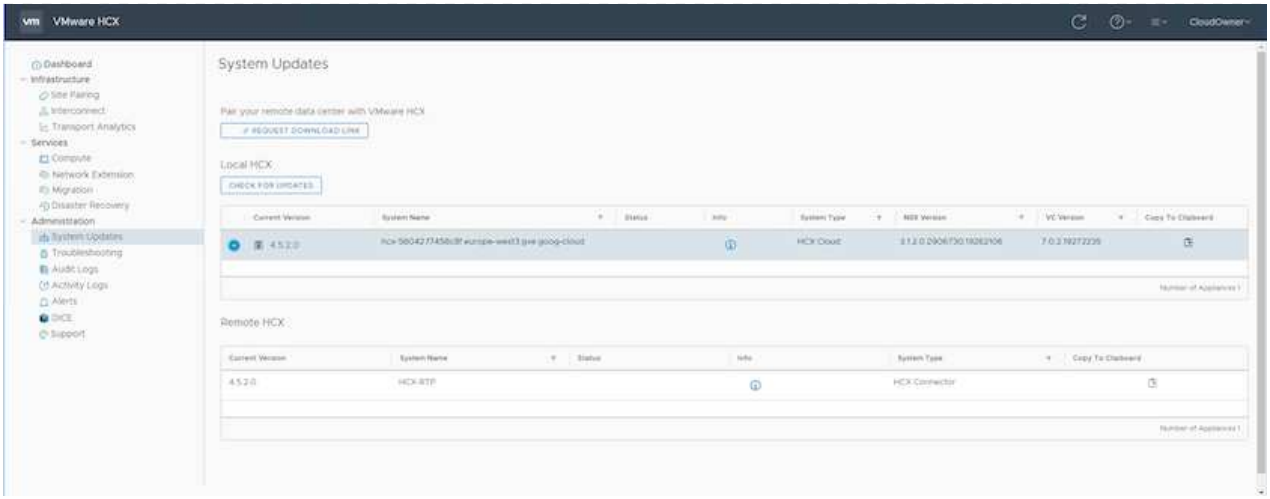
   HCXバージョンのリンクをクリックすると'HCXコンソールにログインできます



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



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



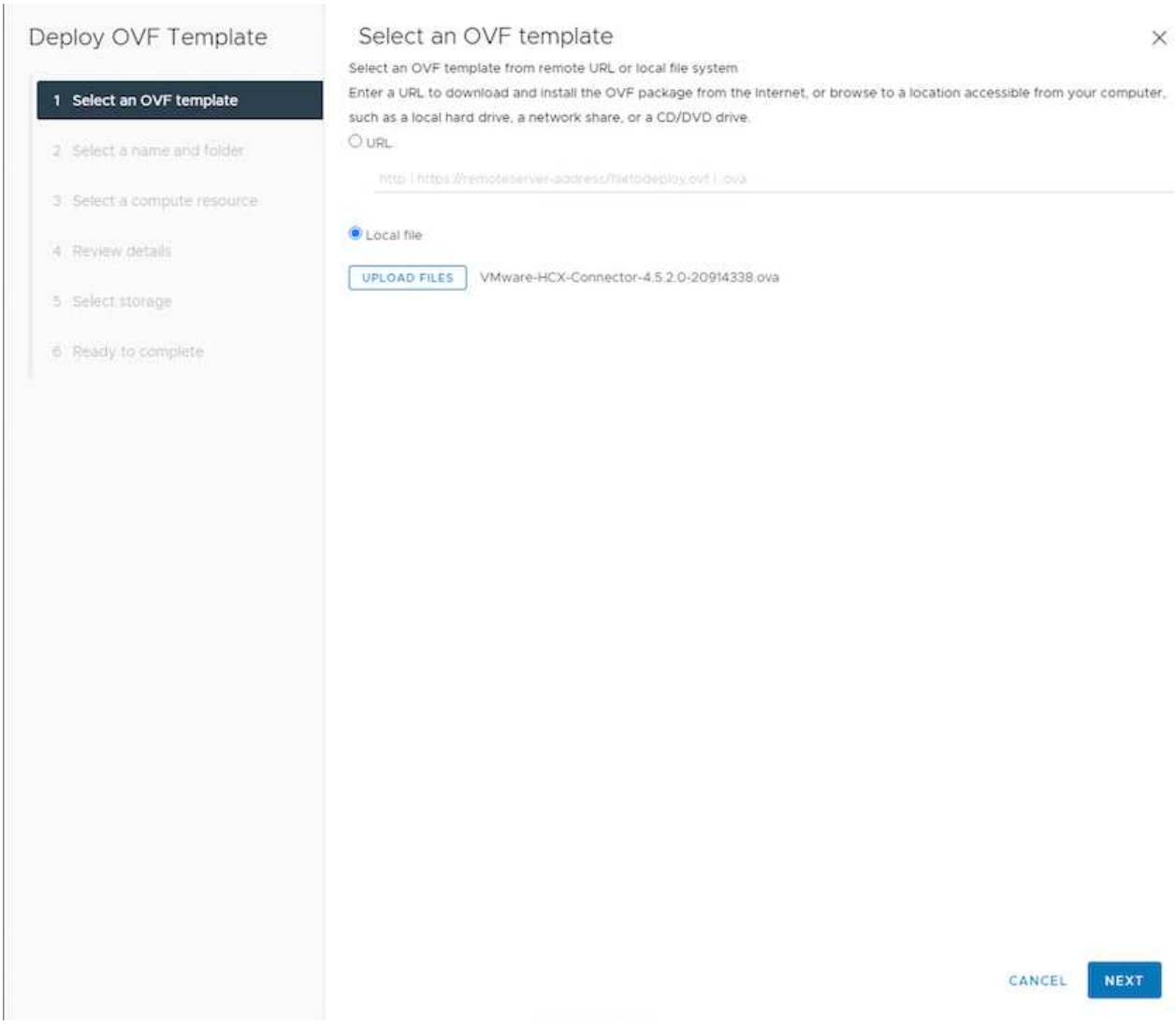
4. HCX Cloud ManagerをHCX Cloud Manager UIから入手可能な最新バージョンに更新します。

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

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

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

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



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

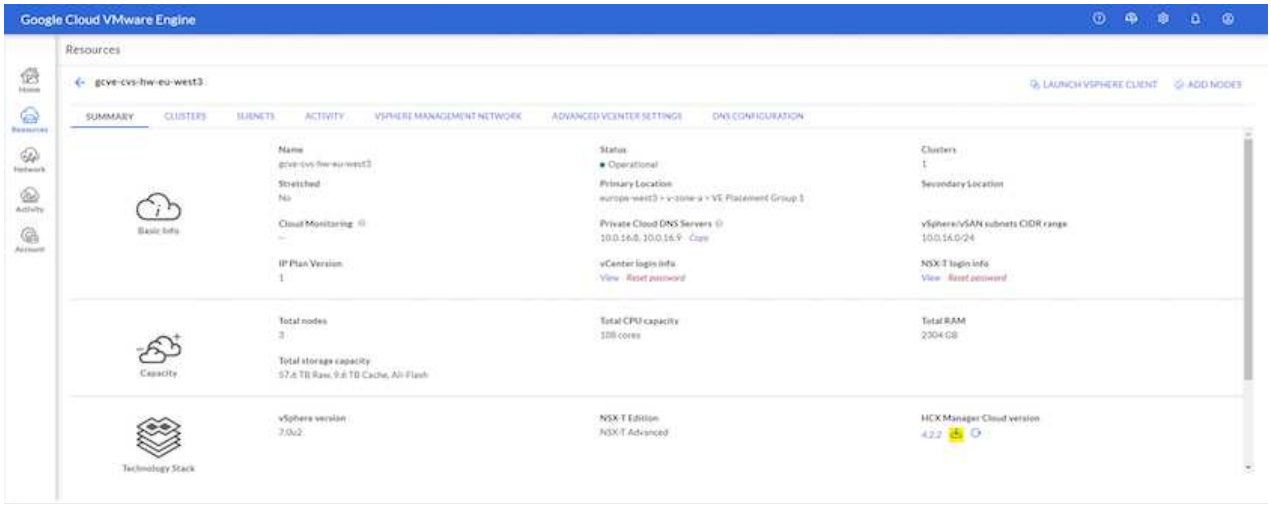
仮想アプライアンスの電源を手動でオンにします。

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

手順3：ライセンスキーを使用して**HCX**コネクタをアクティブにします

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

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



ダウンロードしたファイルを開き、ライセンスキー文字列をコピーします。

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

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

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

   オンプレミスのHCXコネクタにはインターネットアクセスが必要です。

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

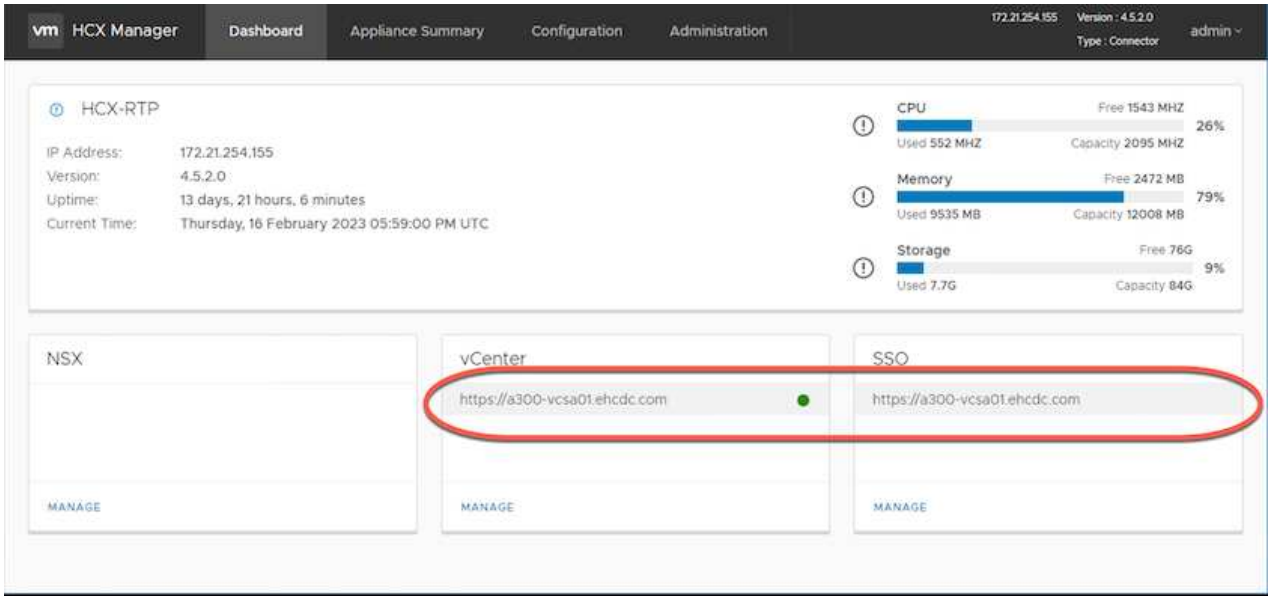
   あとで接続の問題が発生しないようにFQDNを使用してください。

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

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

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

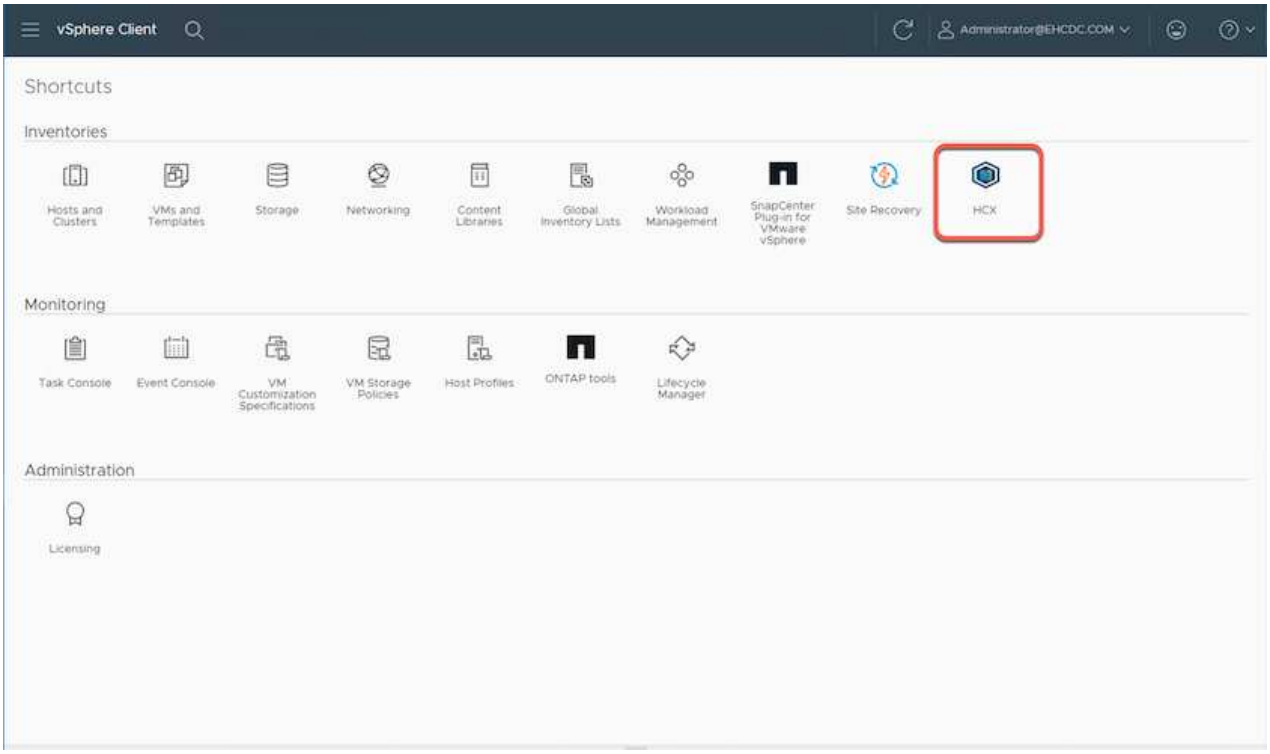
> この処理には10~20分かかります。また、プラグインをvCenter Serverに追加する必要があります。



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

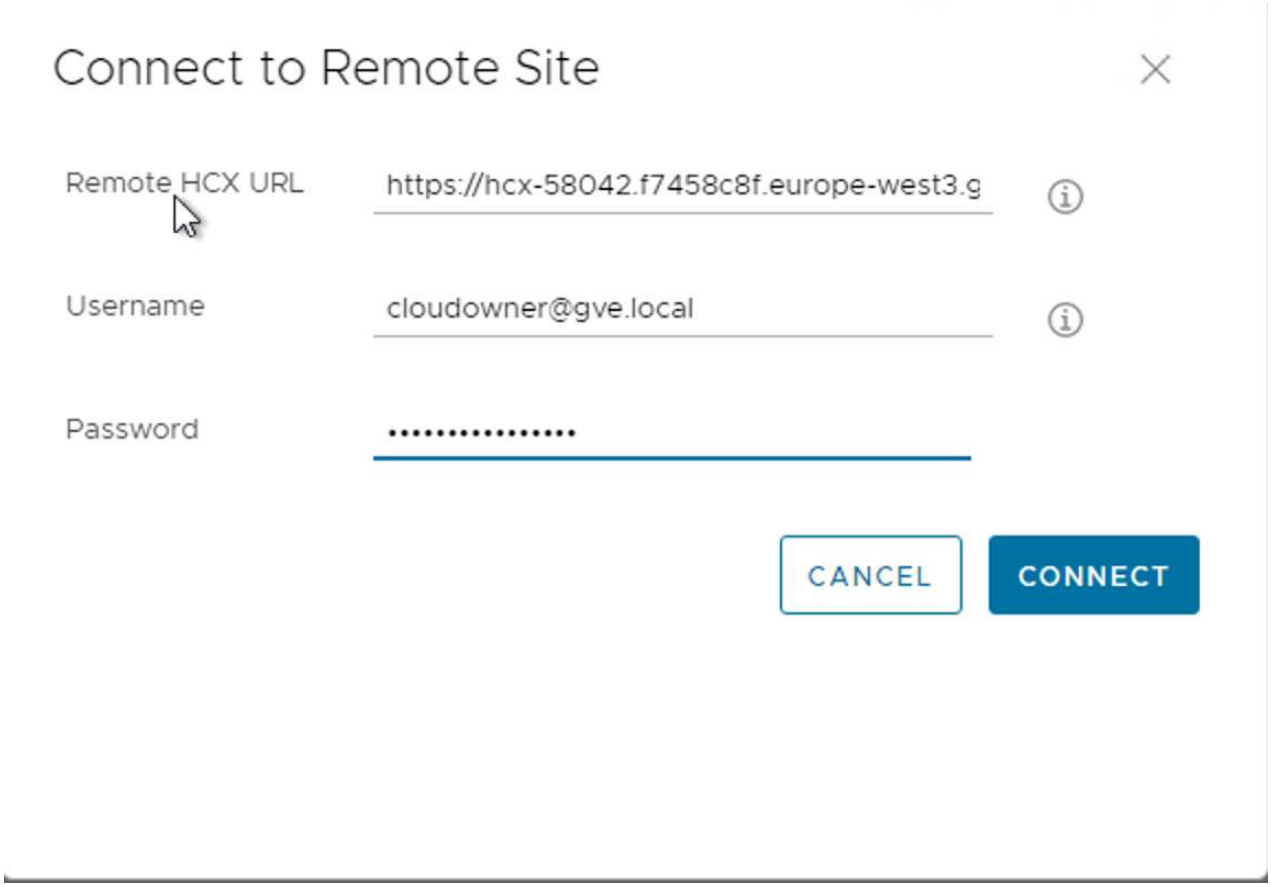
オンプレミスのvCenterにHCX Connectorを導入して設定したら、このペアリングを追加してCloud Managerへの接続を確立します。サイトペアリングを設定するには、次の手順を実行します。

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



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

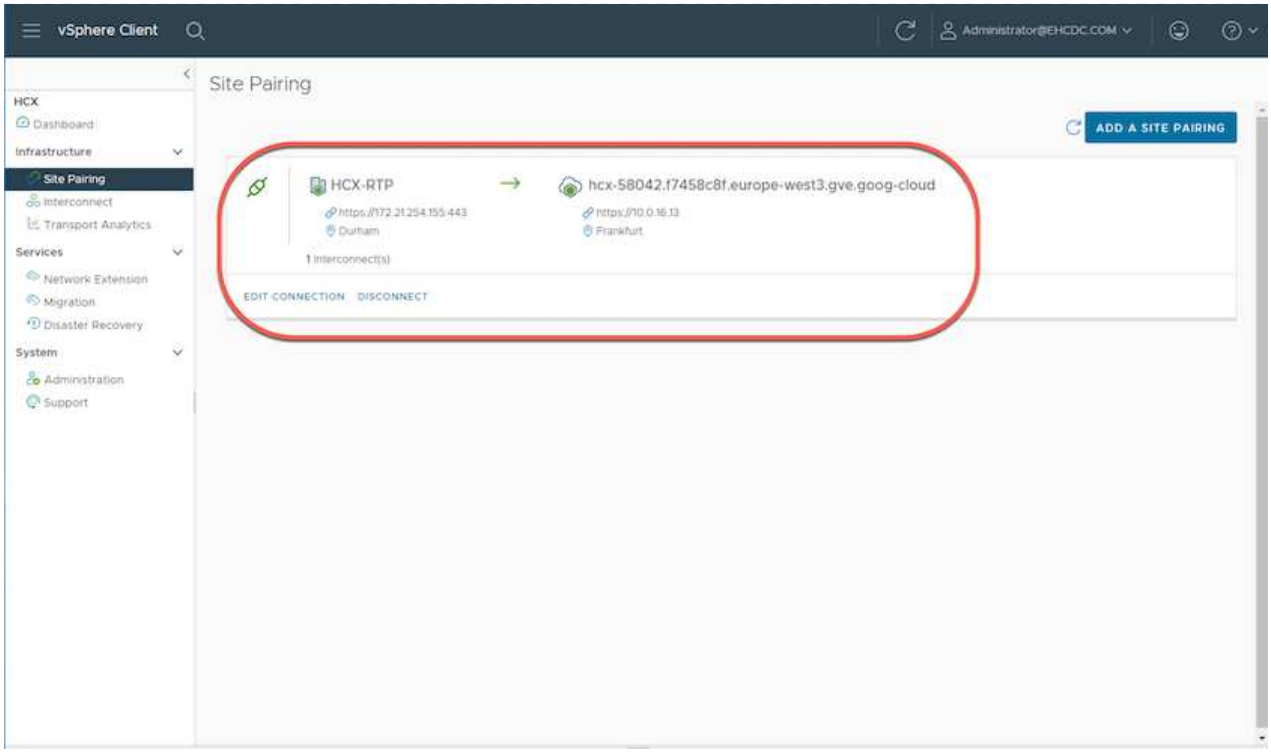
> プライベートクラウドにアクセスするためのCloud-Owner-Role権限を持つユーザのために、Google Cloud VMware Engine HCX Cloud ManagerのURLまたはIPアドレスとクレデンシャルを入力します。



3. [接続] をクリックします。

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

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

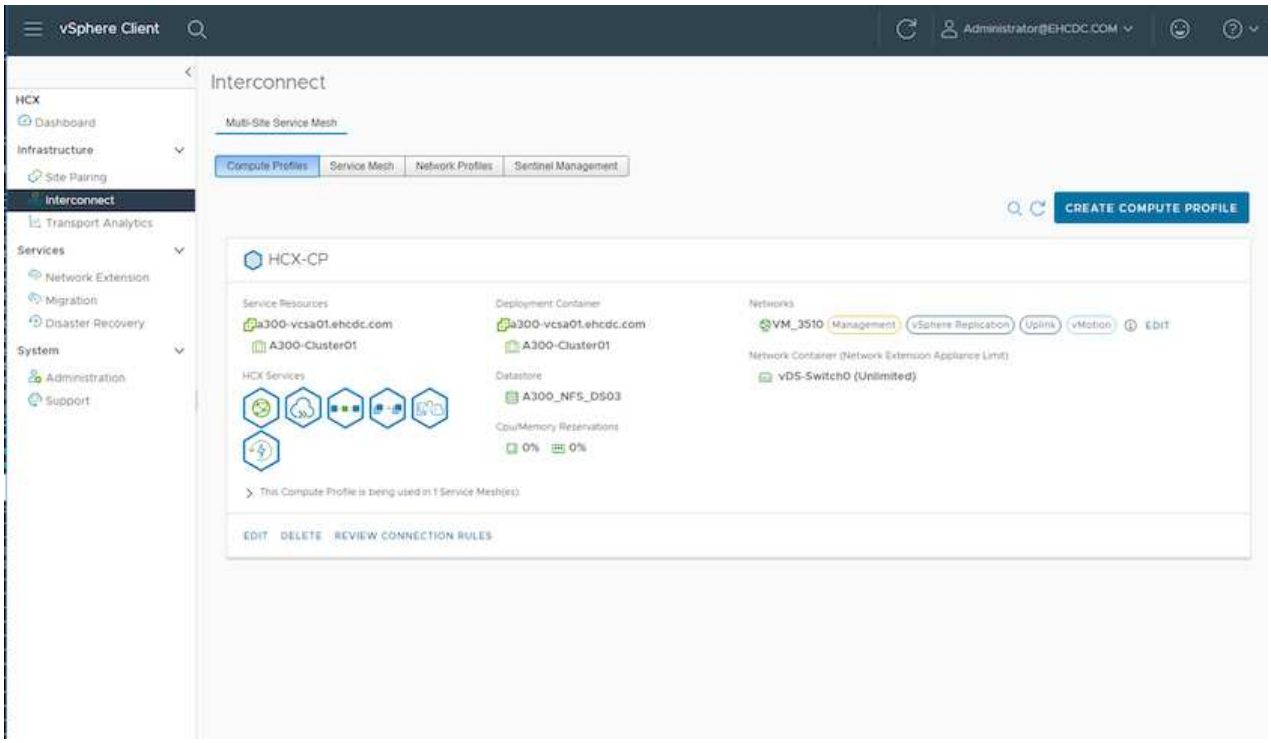

vSphere Client
Administrator@EHCDC.COM
HCX
Dashboard
Infrastructure
Site Pairing
Interconnect
Transport Analytics
Services
Network Extension
Migration
Disaster Recovery
System
Administration
Support
Site Pairing
ADD A SITE PAIRING
HCX-RTP
https://172.21.254.155:443
Durham
hcx-58042.f7458c8f.europe-west3.gve.goog-cloud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

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

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

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

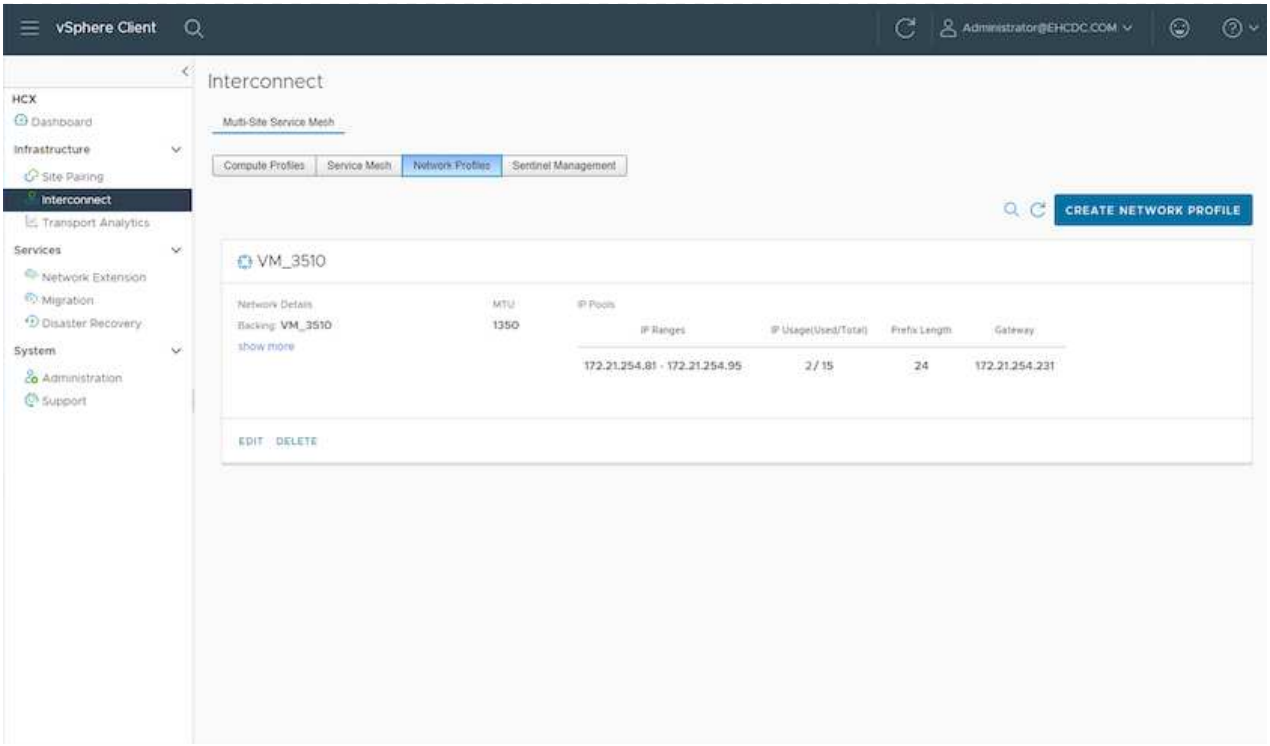
   コンピューティングプロファイルでは、導入されるアプライアンスや、HCXサービスからアクセスできるVMwareデータセンターの部分などの導入パラメータを定義します。



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

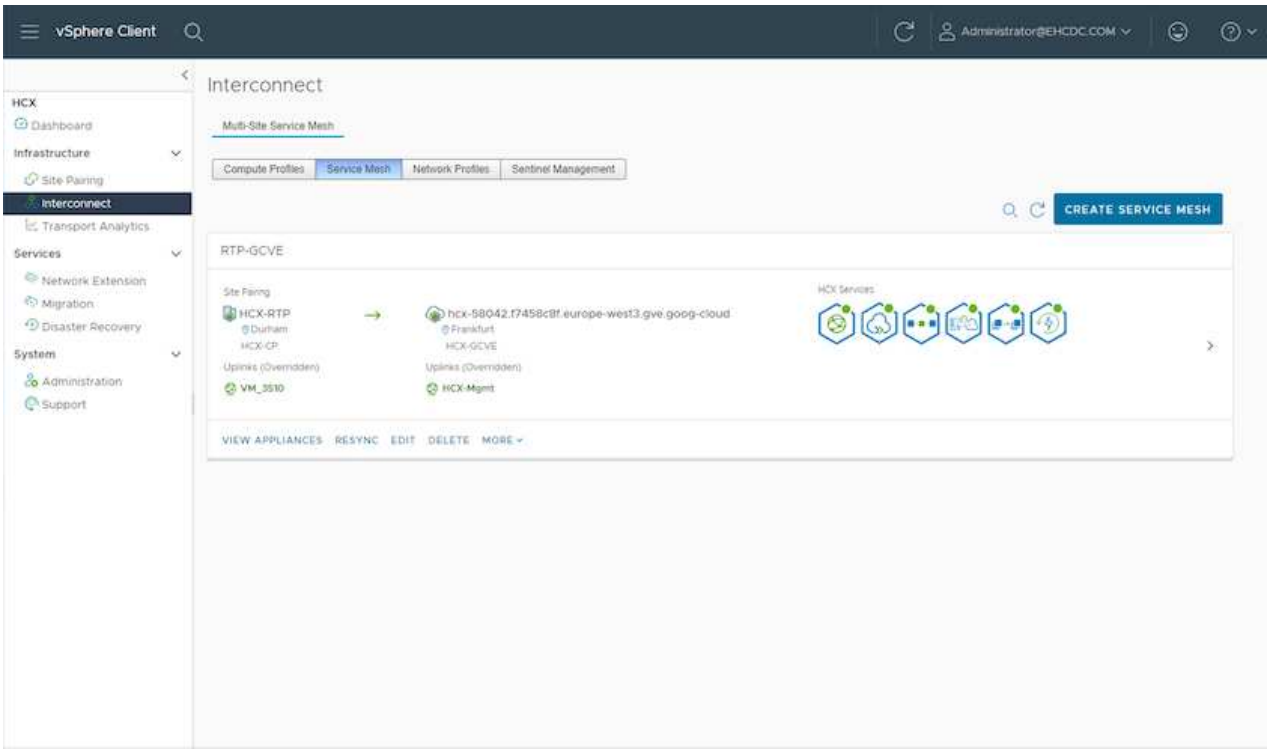
   ネットワークプロファイルは、HCXが仮想アプライアンスに使用するIPアドレスとネットワークの範囲を定義します。

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

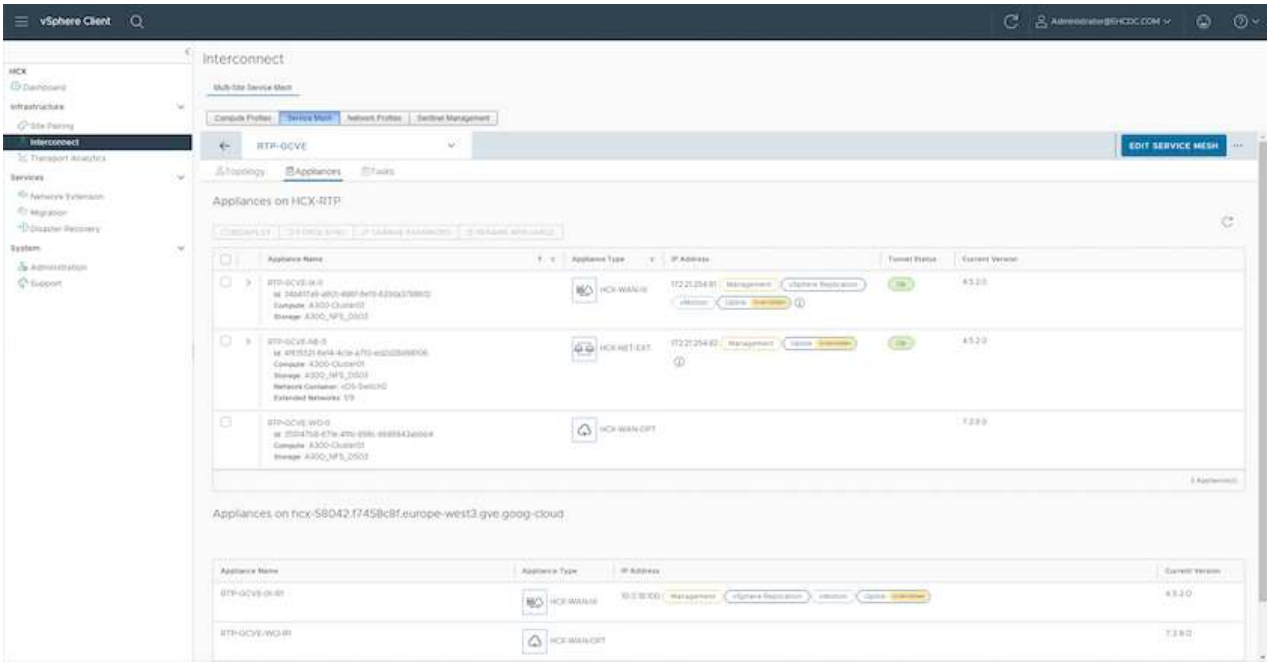


3. 現時点では、コンピューティングプロファイルとネットワークプロファイルは正常に作成されています。
4. [Interconnect（相互接続）]オプションの[* Service Mesh*（サービスメッシュ*）]タブを選択してサービスメッシュを作成し、オンプレミスサイトとGCVE SDDCサイトを選択します。
5. サービスメッシュは、ローカルとリモートのコンピューティングプロファイルとネットワークプロファイルのペアを指定します。

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



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



手順**6**：ワークロードを移行する

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

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

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

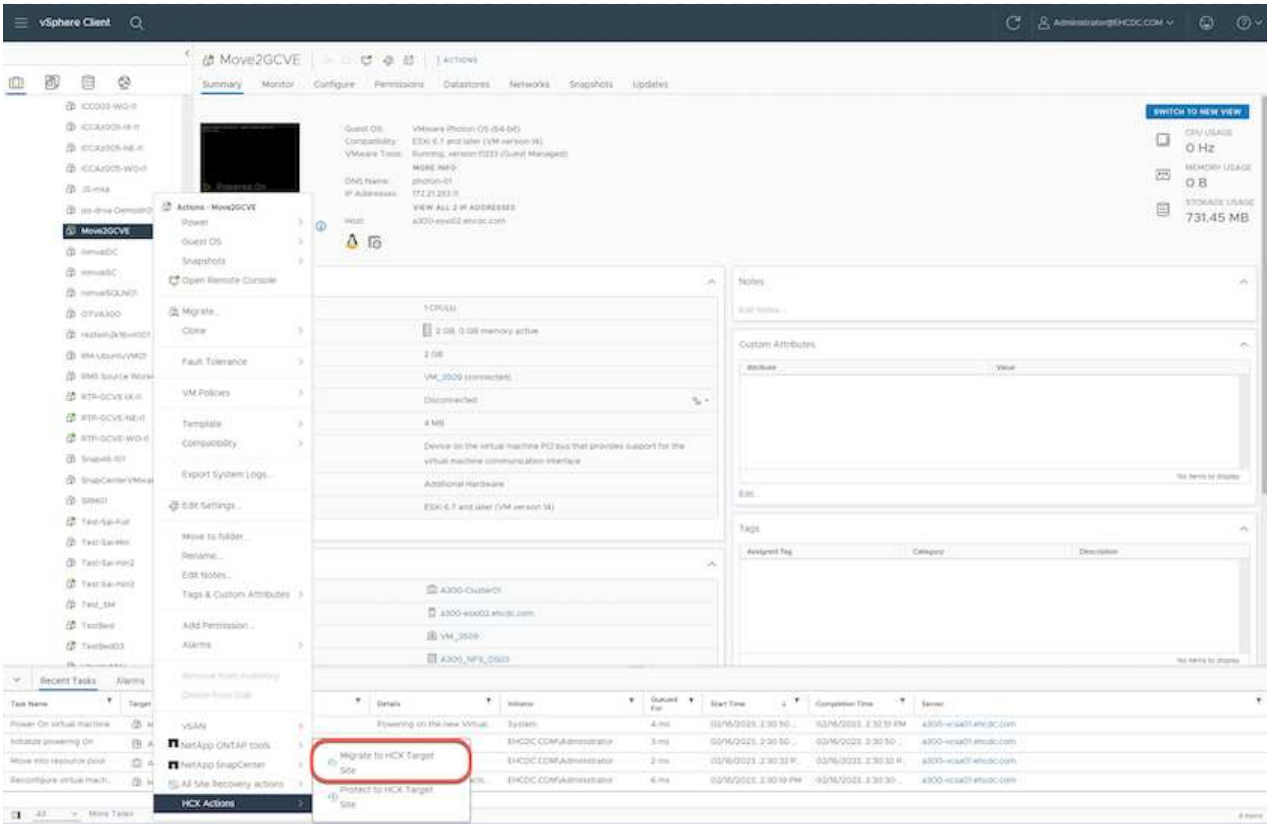
> HCX-IXアプライアンスは、Mobility AgentサービスをvCenter Serverのホストオブジェクトとして追加します。このオブジェクトに表示されるプロセッサ、メモリ、ストレージ、およびネットワークのリソースは、IXアプライアンスをホストする物理ハイパーバイザーでの実際の消費量を表していません。

- HCX vMotion *

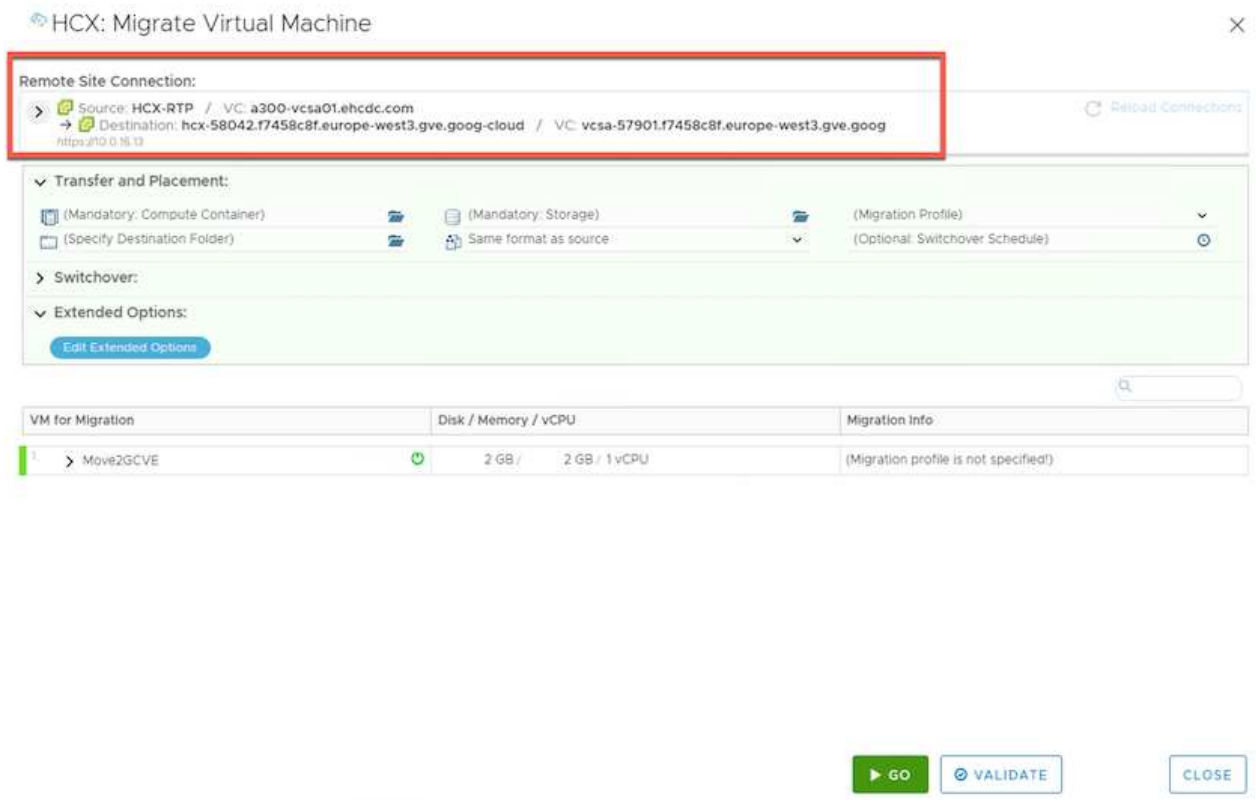
このセクションでは、HCX vMotionメカニズムについて説明します。この移行テクノロジは、VMware vMotionプロトコルを使用してVMをGCVEに移行します。vMotion移行オプションは、一度に1つのVMのVM状態を移行するために使用します。このマイグレーション方式では、サービスは中断されません。

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

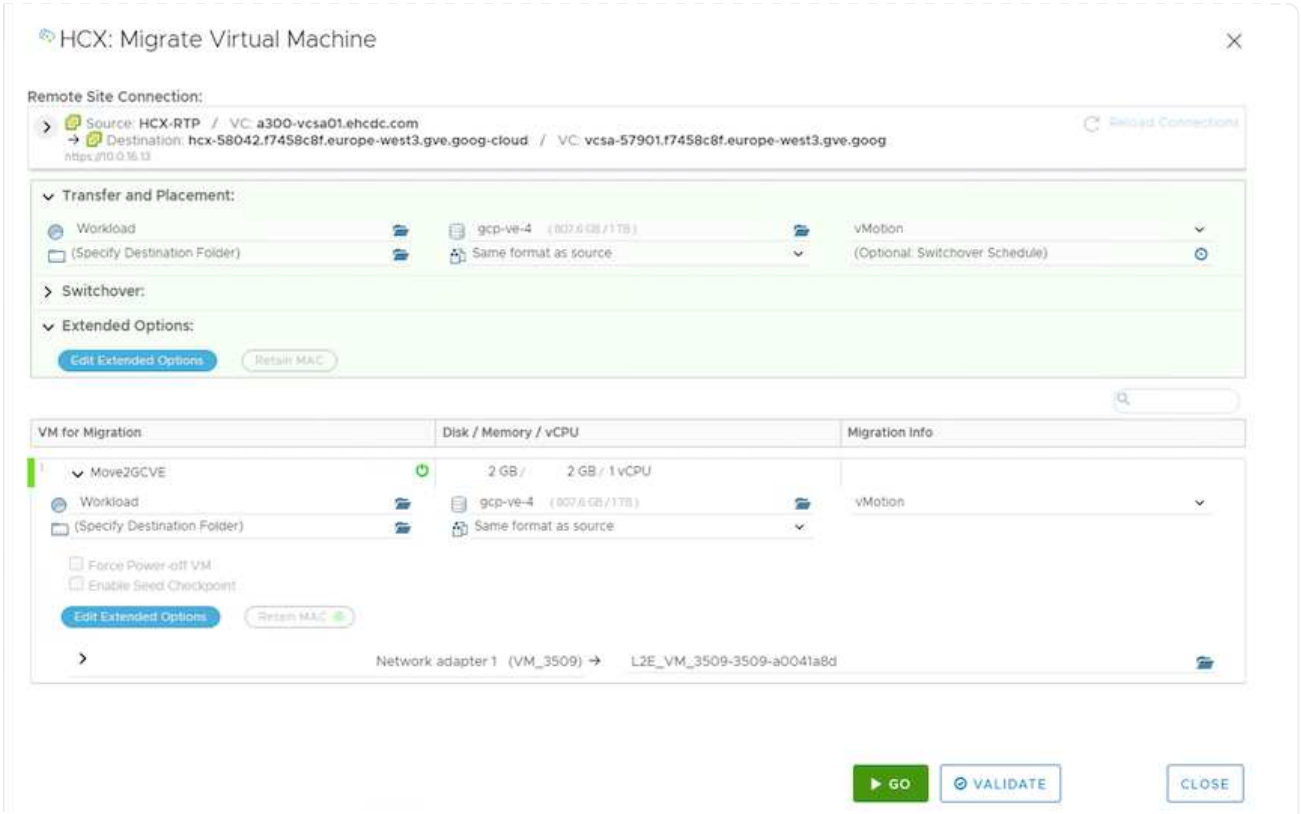
1. オンプレミスのvSphereクライアントから、Inventoryに移動し、移行するVMを右クリックして、HCX Actions > Migrate to HCX Target Siteを選択します。



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



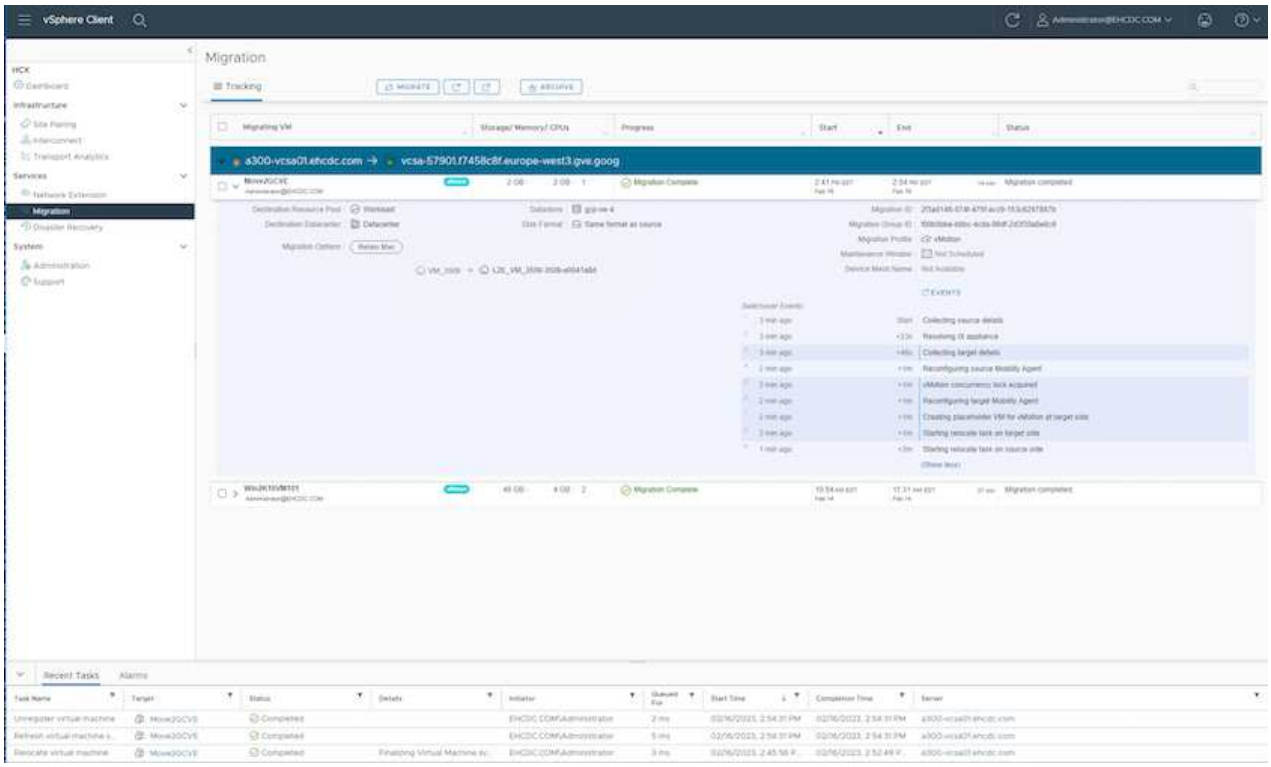
3. 必須フィールド（クラスタ、ストレージ、デスティネーションネットワーク）を更新し、検証をクリックします。



4. 検証チェックが完了したら、Goをクリックして移行を開始します。

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

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



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

まとめ

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

重要なポイント

本ドキュメントの主な内容は次のとおりです。

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

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

Googleから

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

VMwareを使用

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

追加情報の参照先

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

- Google Cloud VMware Engineのドキュメント

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

- Cloud Volume Serviceのドキュメント

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

- VMware HCXユーザーガイド

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

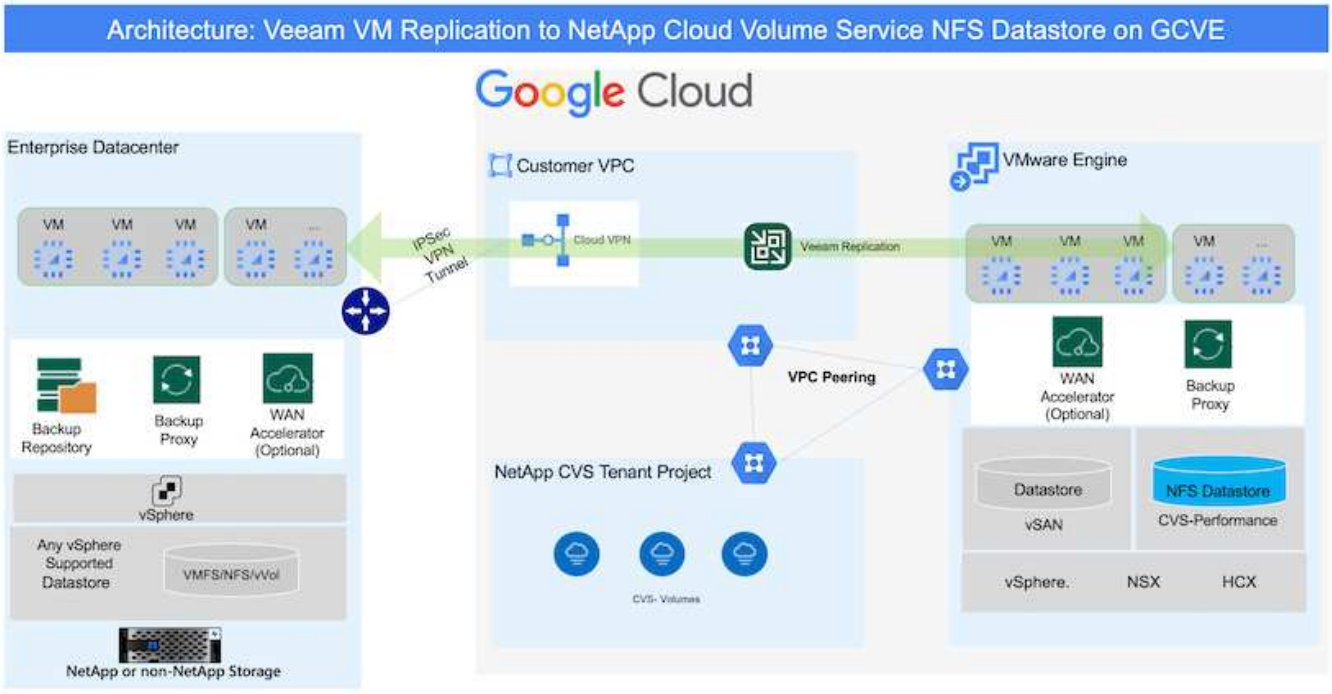
Veeamレプリケーション機能を使用した**Google Cloud VMware Engine**上の**NetApp**クラウドボリュームサービス**NFS**データストアへの**VM**の移行

概要

執筆者：ネットアップSuresh Thoppay

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

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



前提条件

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

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

移行解決策の導入

解決策 の導入の概要

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

展開の詳細

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

GCVE vCenterにログインし、十分なスペースがあるNFSデータストアが使用可能であることを確認します。そうでない場合は、を参照してください "NetApp CVSをNFSデータストアとしてGCVEにマウント"

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

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

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

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

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

Veeamレプリケーションジョブのフェイルオーバーを実行します

VMを移行するには、を実行します "フェールオーバーを実行します"

Veeamで永続的フェイルオーバーを実行

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

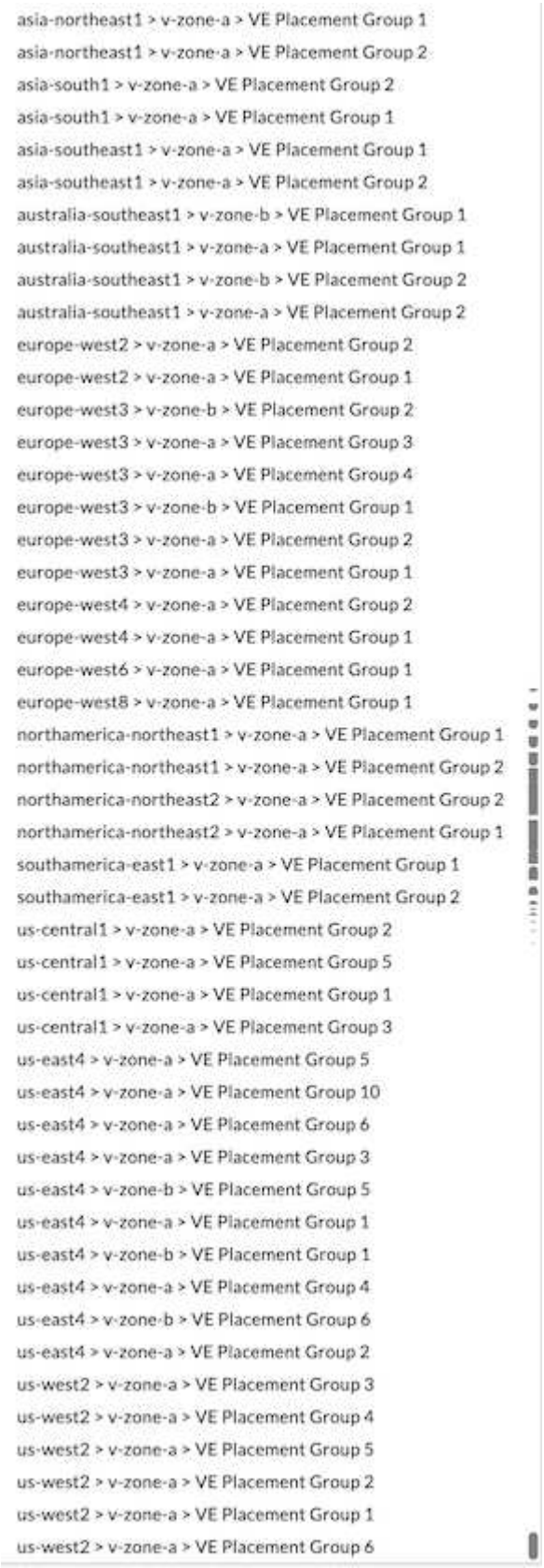
この解決策 の利点

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

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

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

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



Google Cloud VMware Engineは次の場所で利用できます
レイテンシを最小限に抑えるには、ボリュームをマウントするNetApp CVSボリュームとGCVEを同じアベイラビリティゾーンに配置する必要があります。

GoogleおよびNetApp 解決策 アーキテクトと連携して、可用性とTCOを最適化します。

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

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

ネットアップ、Oliver Krause、Justin Parisi

文書の範囲

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

対象読者

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

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

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

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

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

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

セキュアなアーキテクチャとテナンシーモデル

Cloud Volumes Service は、異なるエンドポイント間でサービス管理（コントロールプレーン）とデータアクセス（データプレーン）をセグメント化することで、Google Cloudのセキュアなアーキテクチャを提供します。これにより、どちらも他方に影響を与えることはありません（を参照） "「Cloud Volumes Service アーキテクチャ」"）。Googleを使用している "プライベートサービスへのアクセス" （PSA）サービスを提供するためのフレームワーク。このフレームワークでは、ネットアップが提供、運用するサービスプロデューサーと、Cloud Volumes Service ファイル共有にアクセスするクライアントをホストする顧客プロジェクトのVirtual Private Cloud（VPC；仮想プライベートクラウド）であるサービスコンシューマが区別されます。

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

コントロールプレーンの強力なアイデンティティ管理

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

セキュリティ強化-攻撃面の制限

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

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

ゼロトラストモデル

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

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

- 強力な認証方法（AESで暗号化されたKerberosトークンやJWTトークンなど）
- 単一の強力なアイデンティティソース（Windows Active Directory、Lightweight Directory Access Protocol（LDAP）、Google IAMなど）
- ネットワークのセグメント化とセキュアマルチテナンシー（デフォルトではテナントのみにアクセス可能）
- 最小限の権限付きアクセスポリシーで詳細なアクセス制御を実現します
- デジタル監査と紙の記録を使用した、信頼できる専任管理者の限定リスト

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

暗号化

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

データ保護とバックアップ

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

業界をリードする**Snapshot**コピーでランサムウェアを迅速に軽減

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

セキュリティに関する考慮事項と攻撃対象

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

これには、次のものが含まれます（ただし、これらに限定されません）。

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

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

セキュアなログインの確保

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

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

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

クラスタの管理とアップグレード

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

ストレージ管理の保護

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

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

サービスのアップグレード

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

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

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

保存データを保護

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

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

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

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

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

転送中のデータを保護

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

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

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

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

NAS権限のユーザとグループ

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

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

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

ランサムウェア、マルウェア、ウィルスの検出、防止、および軽減

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

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

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

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

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

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

変更不可の**Snapshot**コピー

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

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

バックアップとリストア

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

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

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

クロスリージョンレプリケーション

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

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

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

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

また、Google Cloudのクロスリージョンレプリケーション（CRR）管理により、ボリュームの削除、Snapshotの削除、Snapshotスケジュールの変更など、悪意のある管理操作を防止できます。そのためには、ボリューム管理者を分離したカスタムロールを作成します。カスタムロールでは、ソースボリュームは削除できますが、ミラーを解除できないため、ボリューム操作を実行できないCRR管理者からデスティネーションボリュームを削除できません。を参照してください "セキュリティに関する考慮事項" 各管理者グループが許可する権限については、Cloud Volumes Service のマニュアルを参照してください。

Cloud Volumes Service バックアップ

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

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

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

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

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

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

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

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

アーキテクチャ

概要

クラウド解決策 を信頼する一部は、アーキテクチャとその保護方法を理解していることです。このセクションでは、GoogleのCloud Volumes Service アーキテクチャのさまざまな側面を紹介し、データのセキュリティ保護に関する潜在的な懸念を軽減するとともに、最も安全な導入を実現するために追加の設定手順が必要な領域について説明します。

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

コントロールプレーン

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

データプレーン

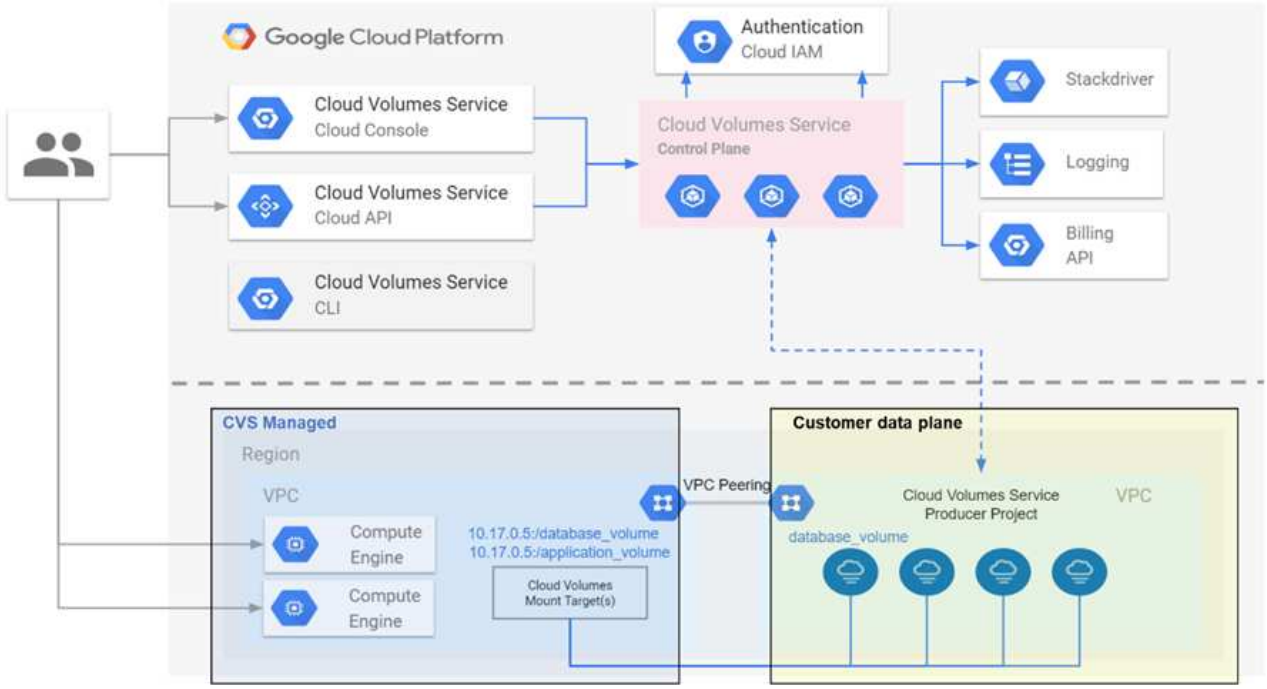
Cloud Volumes Service のデータプレーンには、実際のデータボリュームとCloud Volumes Service の全体的な設定（アクセス制御、Kerberos認証など）が含まれています。データプレーンは、エンドユーザとCloud Volumes Service プラットフォームの消費者の制御下に完全にあります。

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

Cloud Volumes Service アーキテクチャ

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

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



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

テナンシーモデル

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

共有 **VPC**

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

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

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

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

vPCサービスコントロール

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

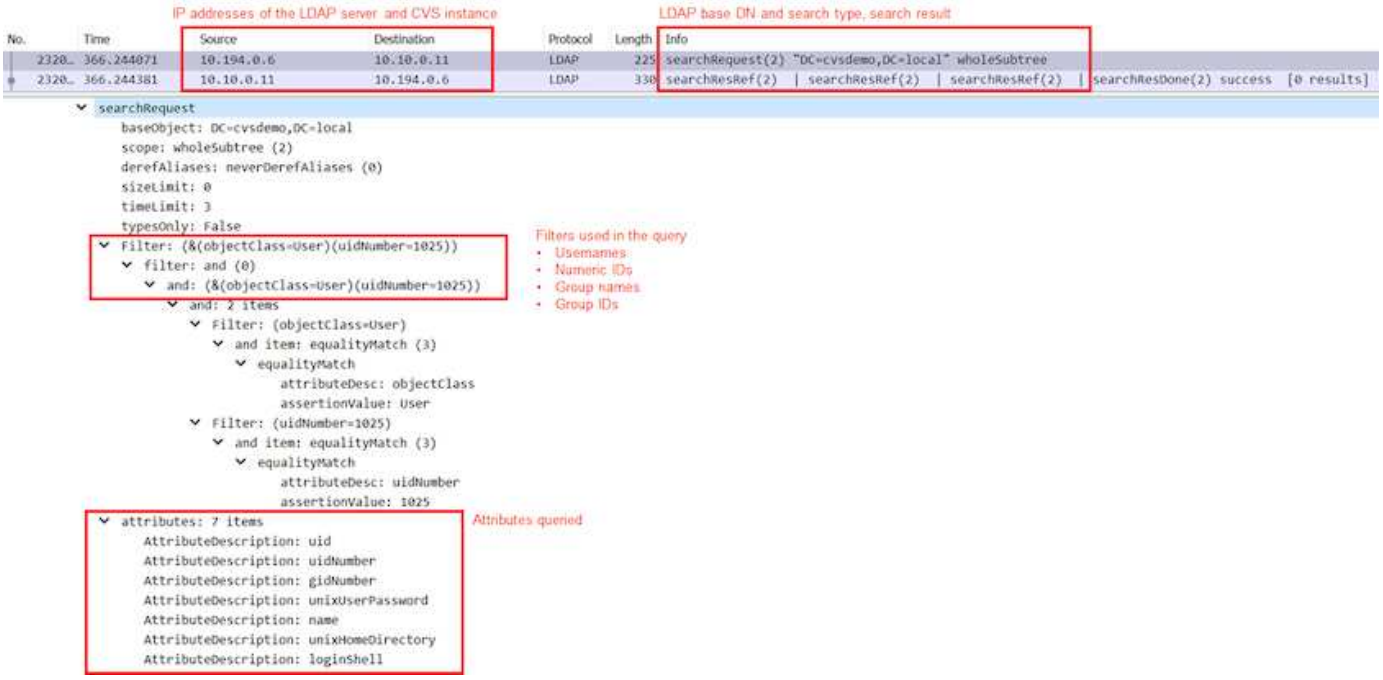
Cloud Volumes Service データプレーンは外部インターネットには接続されず、明確に定義されたネットワーク境界（境界）を持つプライベートVPCに接続されます。ネットワーク内では、各ボリュームはプロトコル固有のアクセス制御を使用します。外部ネットワーク接続は、Google Cloudプロジェクト管理者によって明示的に作成されます。ただし、コントロールプレーンはデータプレーンと同じ保護機能を提供しません。また、有効なクレデンシャル（）を持つ任意の場所から誰でもアクセスできます "JWTトークン"）。

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

パケットのスニッフィング/トレースに関する考慮事項

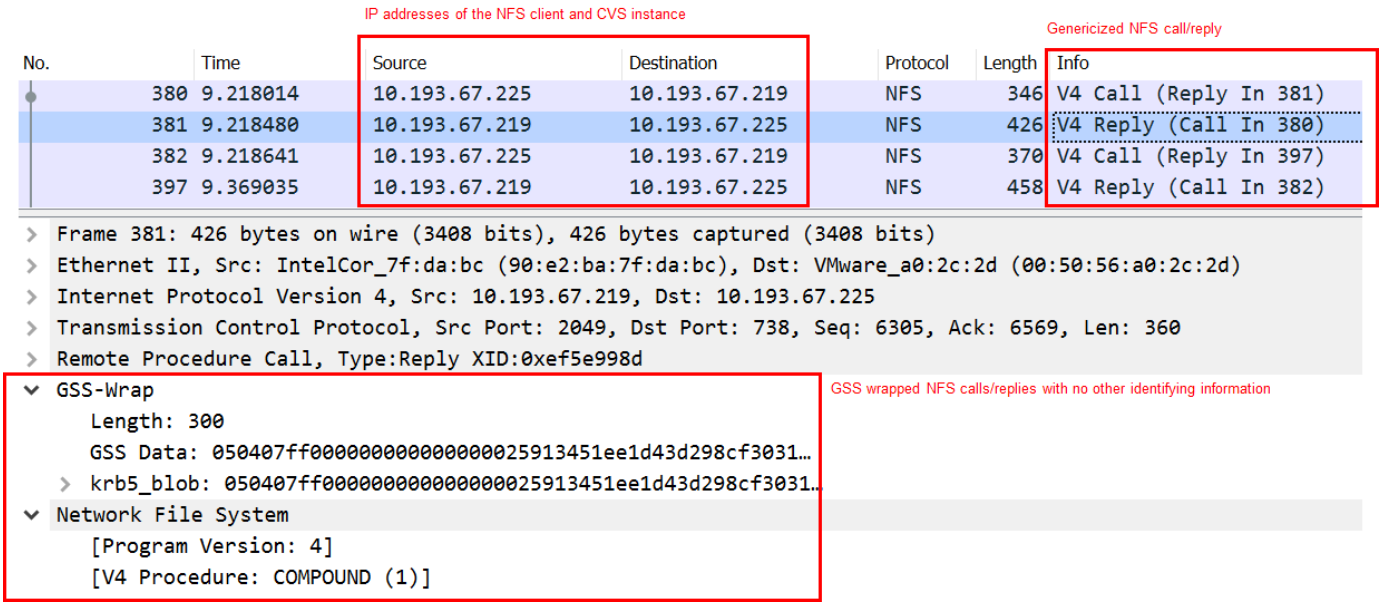
パケットキャプチャは、ネットワークの問題やその他の問題（NAS権限、LDAP接続など）のトラブルシューティングに役立ちますが、悪意を持ってネットワークIPアドレス、MACアドレス、ユーザ名およびグループ名、エンドポイントで使用されているセキュリティレベルなどの情報を取得することもできます。Google Cloudネットワーク、VPC、およびファイアウォールルールの設定方法が原因で、ユーザのログインクレデンシャルやを使用しないとネットワークパケットへの不要なアクセスを取得できなくなります "JWTトークン" クラウドインスタンスへ。パケットキャプチャはエンドポイント（仮想マシン（VM）など）での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

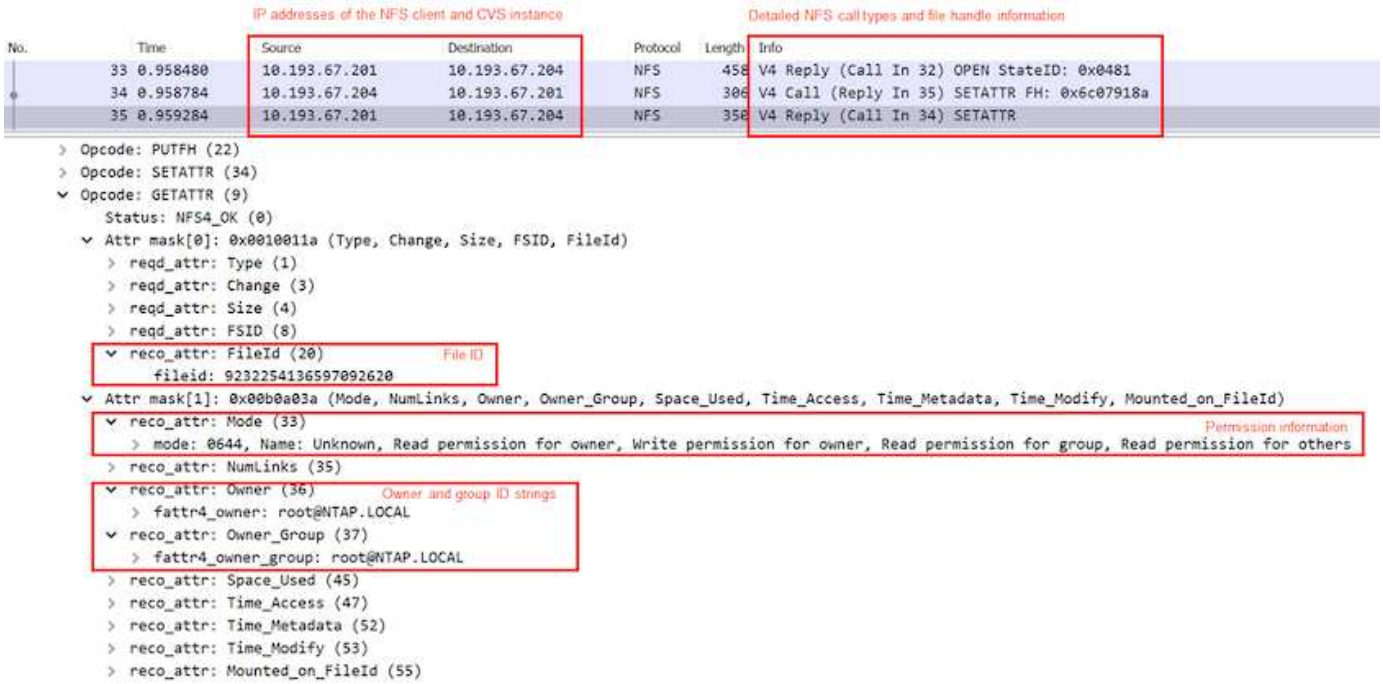
共有VPCを使用する場合は、NFS Kerberosまたは/またはを使用した転送中の暗号化が可能です "SMB暗号化" トレースから収集された情報の多くを隠すことができます。ただし、一部のトラフィックは、などのプレーンテキストで送信されます "DNS" および "LDAPクエリ"。次の図に、Cloud Volumes Service から発信されたプレーンテキストLDAPクエリからのパケットキャプチャと、公開されている可能性のある識別情報を示します。Cloud Volumes Service のLDAPクエリでは、現在、暗号化またはLDAP over SSLがサポートされていません。CVS -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



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

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





VMネットワークインターフェイス

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

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

コントロールプレーンのアーキテクチャ

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

IDおよびアクセス管理

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

承認/権限の概要

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

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

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

きめ細かい権限の使用例を次に示します。

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

サービスアカウント

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

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

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

Cloud Volumes Service APIの略

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

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

JWTトークン

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

監査ロギング

現在、ユーザがアクセスできるコントロールプレーン監査ログはありません。

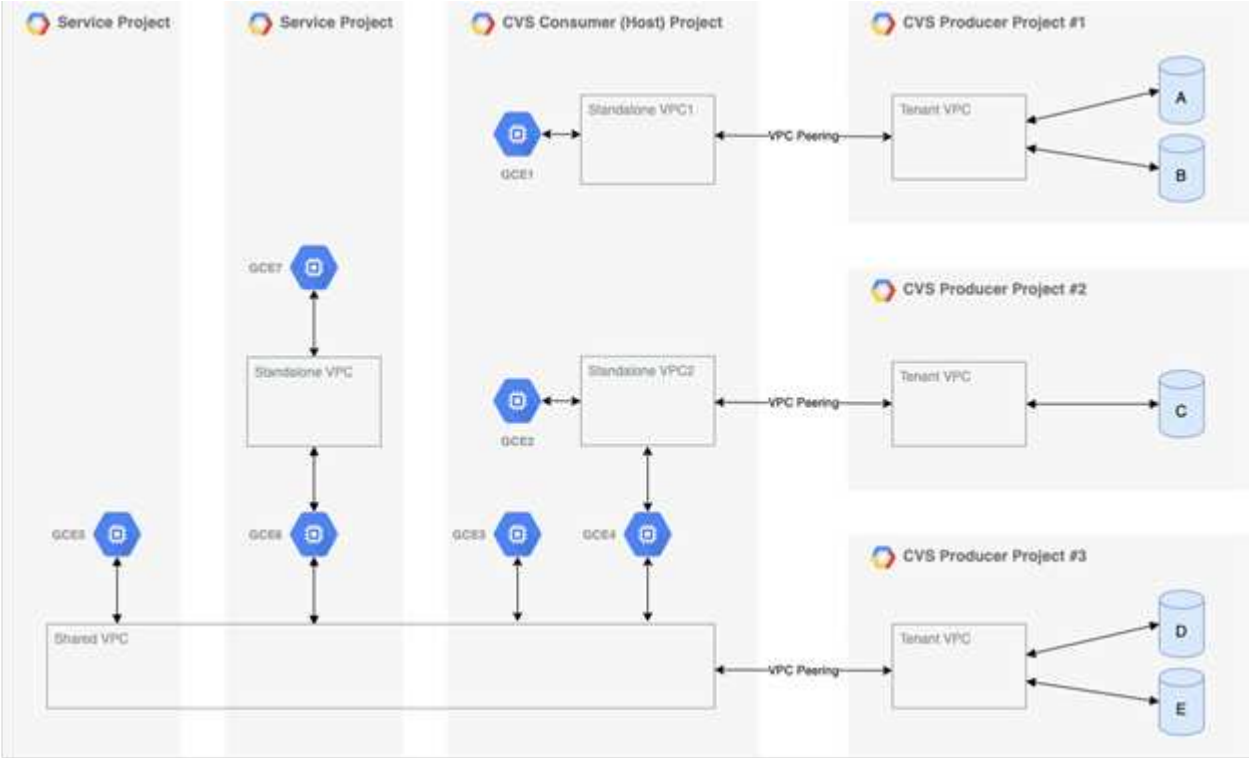
データプレーンアーキテクチャ

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

ント間の完全な分離を実現します。

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

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



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

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

GCE7はどのボリュームにもアクセスできません。

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

転送中のデータ暗号化

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

Google Cloudネットワーク

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

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

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

NASプロトコル

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

SMB暗号化

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

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

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

NFSv4.1 Kerberos

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

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

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

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

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

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

次の表に、セキュリティとパフォーマンスの各レベルの違いを示します。

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

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

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

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

保存データの暗号化

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

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

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

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

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

ファイアウォール：

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

- "NFSアクセスに必要なポート"
- "SMBアクセスに必要なポート"

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

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

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

NASプロトコル

NASプロトコルの概要

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

デュアルプロトコルはCVSパフォーマンスでのみ使用できます。

NASプロトコルの基本

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

カニズムを調整し、権限を格納し、IDおよび認証要求を処理します。

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

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

NFS

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

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

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

デフォルトのローカル**UNIX**ユーザおよびグループ

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

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

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

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

rootユーザ

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

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

匿名ユーザ

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

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

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

アクセス制御/エクスポート

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

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

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

所有権の変更（**chown**）とグループの変更（**chgrp**）

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

権限の管理

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

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

NFSv3にきめ細かな**ACL**を提供

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

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

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

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

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

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

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

NFSv3のユーザ**ID**とグループ**ID**

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

NFSv3のユーザ**ID**とグループ**ID**のセキュリティ制限

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

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

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

NFSv4.1

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

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

NFSv4.1の依存関係

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

NFSv4.1 ACL

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

- ファイルやディレクトリへのユーザアクセスの詳細な制御
- NFS セキュリティが向上します
- CIFS / SMBとの相互運用性が向上しました
- AUTH_SYSのセキュリティが設定された、ユーザあたり16個のグループに関するNFSの制限を削除
- ACLはグループID（GID）の解決の必要性をバイパスします。これにより、実質的にGIDの制限を解除することができ、Cloud Volumes Service からではなくNFSクライアントからNFSv4.1 ACLが制御されます。NFSv4.1 ACLを使用するには、クライアントのソフトウェアバージョンでサポートされていること、および適切なNFSユーティリティがインストールされていることを確認してください。

NFSv4.1 ACLとSMBクライアントの互換性

NFSv4 ACLはWindowsのファイルレベルのACL（NTFS ACL）とは異なりますが、同様の機能を備えています。ただし、マルチプロトコルNAS環境でNFSv4.1 ACLが存在し、デュアルプロトコルアクセス（同じデータセットでNFSおよびSMB）を使用している場合、SMB2.0以降を使用するクライアントは、Windowsのセキュリティタブでを表示または管理できません。

NFSv4.1 ACLの仕組み

参考のために、次の用語が定義されています。

- *アクセス制御リスト(ACL)。*アクセス権エントリのリスト。
- *アクセス制御エントリ(ACE)。*リスト内のアクセス許可エントリ。

クライアントがSETATTR操作でファイルにNFSv4.1 ACLを設定すると、Cloud Volumes Service は既存のACLに替わってそのACLをオブジェクトに設定します。ファイルにACLが設定されていない場合、ファイルのモード権限はOWNER@、GROUP@、およびEVERYONE@から計算されます。ファイルにSUID / SGID / STICKYのいずれかのビットが設定されている場合、それらのビットは影響を受けません。

クライアントがGETATTR操作でファイルのNFSv4.1 ACLを取得すると、Cloud Volumes Service はオブジェクトに関連付けられたNFSv4.1 ACLを読み取り、ACEのリストを作成してクライアントに返します。ファイルにNT ACLまたはモードビットが設定されている場合は、モードビットからACLが構築されてクライアントに返されます。

ACLにDENY ACEが存在する場合はアクセスが拒否され、ALLOW ACEが存在する場合はアクセスが許可されます。ただし、ACLにどちらのACEも存在しない場合も、アクセスが拒否されます。

セキュリティ記述子は、セキュリティACL（SACL）と随意ACL（DACL）で構成されます。NFSv4.1がCIFS / SMBと連動する場合は、DACLはNFSv4とCIFSに1対1でマッピングされます。DACLは、ALLOW ACEとDENY ACEで構成されます。

NFSv4.1 ACLが設定されたファイルまたはフォルダに対して基本的なchmodを実行すると、既存のユーザおよびグループのACLは維持されますが、デフォルトのOWNER@、GROUP@、およびEVERYONE@ ACLが変更されます。

NFSv4.1 ACLを使用するクライアントは、システム上のファイルとディレクトリにACLを設定し、そのACLを表示することができます。ACLが設定されているディレクトリ内にファイルやサブディレクトリを新しく作成すると、そのオブジェクトは、該当するACLでタグ付けされているACEをすべて継承します "継承フラグ"。

ファイルまたはディレクトリにNFSv4.1 ACLが設定されている場合、そのACLを使用して、ファイルまたはディレクトリへのアクセスにどのプロトコルが使用されるかに関係なく、アクセスが制御されます。

親ディレクトリのNFSv4 ACLのACEに正しい継承フラグが設定されていれば、ファイルやディレクトリは該当するACEを継承します（必要な変更が加えられる可能性があります）。

ファイルやディレクトリがNFSv4要求によって作成される場合、作成されるファイルやディレクトリのACLは、ファイル作成要求にACLが含まれているか、または標準のUNIXファイルアクセス権限のみが含まれているかによって異なります。また、親ディレクトリにACLが設定されているかどうかによっても異なります。

- 要求に ACL が含まれる場合は、その ACL が使用されます。
- 要求に標準の UNIX ファイルアクセス権限のみが含まれ、親ディレクトリに ACL がない場合は、クライアントのファイルモードを使用して標準の UNIX ファイルアクセス権限が設定されます。
- 要求に標準UNIXファイルアクセス権限のみが含まれ、親ディレクトリに継承できないACLがある場合は、要求で渡されたモードビットに基づいてデフォルトのACLが設定されます。
- 要求に標準 UNIX ファイルアクセス権限のみが含まれ、親ディレクトリに ACL がある場合、親ディレクトリの ACL の ACE に適切な継承フラグのタグが付けられていれば、それらの ACE が新しいファイルやディレクトリに継承されます。

ACE権限

NFSv4.1 ACLの権限では、大文字と小文字のアルファベットの一連の値（「rxtncy」など）を使用してアクセスが制御されます。これらの文字の値の詳細については、を参照してください "方法: NFSv4 ACLを使用します"。

umaskおよびACLの継承が設定されたNFSv4.1 ACLの動作

"NFSv4 ACLでは、ACLを継承することができます"。ACLの継承では、NFSv4.1 ACLが設定されているオブジェクトの下に作成されるファイルやフォルダに、の設定に基づいてACLを継承することができます "ACL継承フラグ"。

"umask" は、管理者とのやり取りなしでディレクトリ内にファイルやフォルダを作成する権限レベルを制御するために使用します。デフォルトでは、Cloud Volumes Service は継承されたACLをumaskによって上書きします。これは、の想定される動作です "RFC 5661"。

ACLのフォーマット

NFSv4.1 ACLには特定の形式があります。次の例は、ファイルに設定されたACEを示しています。

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

上記の例では、のACL形式のガイドラインに従います。

```
type:flags:principal:permissions
```

「A」のタイプは「許可」を意味します。 継承フラグはこの場合は設定されません。これは、プリンシパルがグループではなく、継承も含まれないためです。また、ACEは監査エントリではないため、監査フラグを設定する必要もありません。NFSv4.1 ACLの詳細については、を参照してください "http://linux.die.net/man/5/nfs4_acl"。

NFSv4.1 ACLが適切に設定されていない場合（またはクライアントとサーバが名前文字列を解決できない場合）、ACLが想定どおりに動作しないか、ACLの変更を適用できずにエラーがスローされる可能性があります。

エラーの例は次のとおりです。

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

明示的な**DENY**

NFSv4.1の権限では、OWNER、GROUP、およびEVERYONEに対する明示的なDENY属性を含めることができます。これは、NFSv4.1 ACLがdefault-denyであるためです。つまり、ACEによってACLが明示的に許可されなければ、ACLは拒否されます。明示的なDENY属性は、明示的なアクセスACEを上書きします。

拒否ACEは'D'の属性タグで設定されます

次の例では、group@はすべての読み取りおよび実行権限を許可していますが、すべての書き込みアクセスは拒否されています。

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

DENY ACEは複雑で混乱を招く可能性があるため、できるかぎり使用しないでください。明示的に定義されていないACLは暗黙的に拒否されます。DENY ACEを設定すると、アクセスを許可されるはずのユーザがアクセスを拒否される場合があります。

上記の一連のACEは、モードビットの755に相当します。つまり、次のようになります。

- 所有者にはフルアクセス権があります。
- グループは読み取り専用です。
- 読み取り専用のものもあります。

ただし、775と等しくなるように権限が調整されていても、EVERYONEに明示的なDENYが設定されているとアクセスが拒否される可能性があります。

NFSv4.1 IDドメインのマッピングの依存関係

NFSv4.1では、セキュリティレイヤとしてIDドメインのマッピングロジックを利用して、NFSv4.1マウントへのアクセスを試みるユーザが、そのユーザの要求を実際に把握できるかどうかを検証します。このような場合は、NFSv4.1クライアントからのユーザ名とグループ名に名前文字列が付加されて、Cloud Volumes Service インスタンスに送信されます。ユーザ名/グループ名とID文字列の組み合わせが一致しない場合は'クライアントの/etc/idmapd.confファイルに指定されているデフォルトのnobodyユーザにユーザまたはグループが引き下げられます

このID文字列は、特にNFSv4.1 ACLやKerberosを使用している場合に、適切な権限を順守するための要件です。そのため、ユーザやグループの名前IDが正しく解決されるように、クライアントとCloud Volumes Service 間で一貫性を確保するためには、LDAPサーバなどのネームサービスサーバに依存する必要があります。

Cloud Volumes Service は'静的なデフォルトIDドメイン名値defaultv4iddomain.comを使用しますNFSクライアントはデフォルトで'IDドメイン名設定のDNSドメイン名になりますが'/etc/idmapd.confでIDドメイン名を手動で調整できます

Cloud Volumes Service でLDAPが有効になっている場合、Cloud Volumes Service はNFS IDドメインを自動化して、DNSの検索ドメインに設定されている内容に変更します。クライアントは、別のDNSドメイン検索名を使用しない限り、変更する必要はありません。

Cloud Volumes Service がローカルファイルまたはLDAPでユーザ名またはグループ名を解決できる場合は、ドメイン文字列が使用され、一致しないドメインIDが引き下げられてnobodyになります。ローカルファイルまたはLDAPでユーザ名またはグループ名が見つからない場合Cloud Volumes Service は、数値のID値が使用され、NFSクライアントが名前を適切に解決します（NFSv3の動作と似ています）。

クライアントのNFSv4.1 IDドメインを、Cloud Volumes Service ボリュームで使用されているものと一致するように変更しないと、次のような動作が発生します。

- Cloud Volumes Service 内にローカルエントリがあるUNIXユーザおよびグループ（ローカルのUNIXユーザとグループで定義されているrootなど）は、nobody値に引き下げられます。
- LDAP内にエントリがあるUNIXユーザおよびグループ（Cloud Volumes Service でLDAPを使用するように設定されている場合）は、NFSクライアントとCloud Volumes Service でDNSドメインが異なる場合、そのハッシュがnobodyに引き下げられます。
- ローカルエントリやLDAPエントリがないUNIXユーザおよびグループは、数値ID値を使用して、NFSクライアントで指定された名前に解決されます。クライアントに名前が存在しない場合は、数値IDのみが表示されます。

上記のシナリオの結果を次に示します。

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

クライアントとサーバIDのドメインが一致した場合、同じファイルリストが表示されます。

```
# ls -la
total 8
drwxr-xr-x 2 root   root         4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root         4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835         9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

この問題 とその解決方法の詳細については、「」を参照してくださいNFSv4.1およびnobodyユーザ/グループ」

Kerberosの依存関係

NFSでKerberosを使用する場合は、Cloud Volumes Service で次の要件を満たす必要があります。

- Kerberosキー配布センターサービス（KDC）用のActive Directoryドメイン
- LDAP機能のUNIX情報を入力したユーザおよびグループの属性を持つActive Directoryドメイン（Cloud Volumes Service のNFS Kerberosでは、正常に機能するためにユーザのSPNからUNIXユーザのマッピングが必要です）。
- Cloud Volumes Service インスタンスでLDAPが有効になっている
- DNSサービスのActive Directoryドメインを指定します

NFSv4.1および**nobody**ユーザ/グループ

NFSv4.1設定でよく見られる問題の1つは、「user:group」の「nobody：nobody」の組み合わせによって所有されている「ls」を使用して一覧にファイルまたはフォルダが表示される場合です。

例：

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

数値IDは「99」です。

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

場合によっては、ファイルに正しい所有者が表示されることもありますが、グループとして「nobody」が表示されることもあります。

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

誰もいないのですか？

NFSv4.1のnobodyユーザはnfsnobodyユーザとは異なりますNFSクライアントが各ユーザーをどのように認識するかを表示するには'id'コマンドを実行します

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

NFSv4.1では'idmapd.confファイルによって定義されたデフォルトのユーザである'nobod'ユーザを使用する任意のユーザとして定義できます

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

なぜそうなるのでしょうか？

NFSv4.1の処理では、ネーム文字列マッピングによるセキュリティが重要な条件となるため、名前文字列が適切に一致しない場合のデフォルトの動作は、ユーザとグループが所有するファイルやフォルダに通常アクセスできないユーザの引き下げです。

ファイルの一覧にユーザまたはグループの「nobody」が表示される場合は、通常、NFSv4.1の設定が誤っています。ここでは、大文字と小文字の区別が使用されます。

たとえば、user1@CVSDEMO.LOCA L（uid 1234、gid 1234）がエクスポートにアクセスしている場合、Cloud Volumes Service はuser1@CVSDEMO.LOCA L（uid 1234、gid 1234）を検索できる必要があります。Cloud Volumes Service のユーザがUSER1@CVSDEMO.LOCA Lの場合、ユーザは一致しません（大文字のUSER1と小文字のuser1）。多くの場合、クライアント上のメッセージファイルに次の情報が表示されます。

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

クライアントとサーバーは、ユーザーが実際に誰を要求しているかに同意する必要があります。そのため、Cloud Volumes Service が表示するユーザーと同じ情報がクライアントに表示されることを確認するには、次の項目を確認する必要があります。

- **NFSv4.x ID domain.** Client:idmapd.confファイル。Cloud Volumes Service は「defaultv4iddomain.com」を使用しており、手動で変更することはできません。Cloud Volumes Service でNFSv4.1を使用する場合、DNS検索ドメインのIDドメインが、ADドメインと同じになるように変更されます。
- *ユーザー名と数値ID。*これは、クライアントがユーザー名を検索し、ネームサービススイッチ構成を利用する場所を決定します。client:nsswitch.conf'ローカルpasswdファイルとgroupファイルのいずれかまたは両方を使用します。Cloud Volumes Service では、この変更は許可されませんが、有効になっている場合は自動的にLDAPが構成に追加されます。
- *グループ名と数値ID。*これは、クライアントがグループ名を検索し、ネームサービススイッチ構成を利用する場所を決定します。client:nsswitch.conf'ローカルpasswdおよびgroupファイルのいずれかまたは両方を使用します。Cloud Volumes Service では、この変更は許可されていませんが、有効になっている場合は自動的にLDAPが構成に追加されます。

ほとんどの場合、クライアントからのユーザおよびグループの一覧に「nobody」が表示された場合、問題はCloud Volumes Service とNFSクライアント間でのユーザまたはグループの名前ドメインIDの変換です。この状況を回避するには、LDAPを使用して、クライアントとCloud Volumes Service 間でユーザおよびグループの情報を解決します。

クライアントでの**NFSv4.1**の名前**ID**文字列の表示

NFSv4.1を使用している場合、前述のように、NFS処理で実行される名前文字列のマッピングが存在します。

/var/log/messagesを使用してNFSv4 IDを持つ問題 を検索することに加え、を使用することもできます "nfsidmap -l" NFSクライアント上でコマンドを実行すると、NFSv4ドメインに適切にマッピングされているユーザ名が表示されます。

たとえば、クライアントで検出されたユーザとCloud Volumes Service がNFSv4.xマウントにアクセスすると、次のようなコマンドが出力されます。

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

NFSv4.1 IDドメインに適切にマッピングされていないユーザ（この場合「netapp -user」）が同じマウントにアクセスしてファイルにアクセスしようとすると、「nobody：nobody」が割り当てられます（想定どおり）。

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

「nfsidmap -l」の出力には、ユーザ「pcuser」が表示されますが、「NetApp-user」は表示されません。これは、エクスポートポリシールールの匿名ユーザ（「65534」）です。

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

SMB

"SMB" は、Microsoftが開発したネットワークファイル共有プロトコルです。ユーザ/グループの認証、権限、ロック、およびファイル共有を、イーサネットネットワークを介して複数のSMBクライアントに一元的に提供します。ファイルとフォルダは共有を通じてクライアントに提供されます。共有は、さまざまな共有プロパティを設定したり、共有レベルの権限を通じてアクセスを制御したりすることができます。SMBは、Windows、Apple、Linuxクライアントなど、このプロトコルをサポートする任意のクライアントに提供できます。

Cloud Volumes Service では、SMB 2.1および3.xバージョンのプロトコルがサポートされます。

アクセス制御/ **SMB**共有

- Windowsユーザ名がCloud Volumes Service ボリュームへのアクセスを要求すると、Cloud Volumes Service はCloud Volumes Service 管理者が設定した方法を使用してUNIXユーザ名を検索します。
- 外部UNIXアイデンティティ・プロバイダ（LDAP）が設定されていて、Windows/UNIXユーザ名が同一の場合、Windowsユーザ名は、追加の設定を必要とせずに1:1でUNIXユーザ名にマッピングされま

す。LDAPを有効にすると、Active Directoryを使用してユーザオブジェクトとグループオブジェクトのUNIX属性がホストされます。

- Windows名とUNIX名が同じ設定にならない場合は、Cloud Volumes Service がLDAPネームマッピングの設定を使用できるようにLDAPを設定する必要があります（を参照）"「LDAPを使用した非対称ネームマッピング」"）。
- LDAPが使用されていない場合、Windows SMBユーザは、Cloud Volumes Service で「pcuser」という名前のデフォルトのローカルUNIXユーザにマッピングされます。つまり'マルチプロトコルのNAS環境では'pcuserにマップされているユーザーによってWindowsに書き込まれたファイルは'UNIXの所有権をpcuserとして表示しますここでは'pcuserがLinux環境では'nobodyユーザー（UID 65534）となっています

SMBのみの導入では、「pcuser」のマッピングは引き続き有効ですが、Windowsのユーザとグループの所有権が正しく表示され、SMBのみのボリュームへのNFSアクセスは許可されないため、問題ありません。また、SMBのみのボリュームでは、NFSまたはデュアルプロトコルのボリューム作成後のボリュームへの変換はサポートされません。

Windowsは、Active Directoryドメインコントローラでのユーザ名認証にKerberosを使用します。これには、Cloud Volumes Service インスタンスの外部にあるAD DCとのユーザ名/パスワードの交換が必要です。Kerberos認証は'\\servername'UNCパスがSMBクライアントによって使用され'次の場合に使用されます

- servernameにはDNS A/AAAAエントリがあります
- servernameに対するSMB / CIFSアクセス用の有効なSPNが存在します

Cloud Volumes Service SMBボリュームを作成すると、セクションの定義に従ってマシンアカウント名が作成されます"「Cloud Volumes Service がActive Directoryにどのように表示されるか」" Cloud Volumes Service は動的DNS（DDNS）を利用してDNSに必要なA/AAAAエントリとPTRエントリ、マシンアカウントプリンシパルの必要なSPNエントリを作成するため、そのマシンアカウント名もSMB共有アクセスパスになります。

PTRエントリを作成するには、Cloud Volumes Service インスタンスIPアドレスの逆引き参照ゾーンがDNSサーバ上に存在している必要があります。

たとえば、このCloud Volumes Service ボリュームはUNC共有パス「\\cvs-east-433d.cvsdemo.local」を使用します。

Active Directoryでは、次のエントリがCloud Volume サービスによって生成されたSPNエントリです。

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

DNS前方/後方参照の結果は次のとおりです。

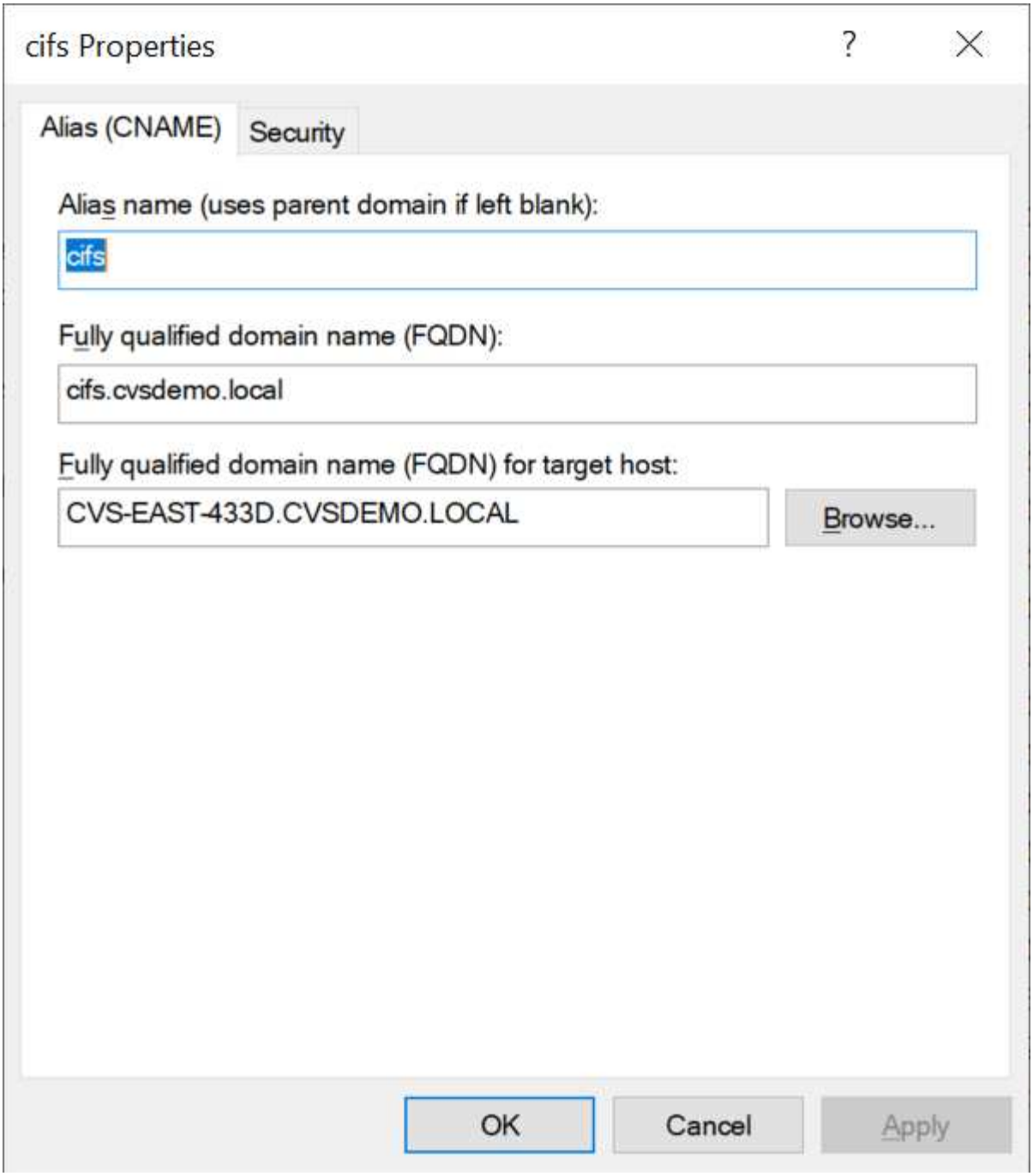
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

必要に応じて、Cloud Volumes Service 内のSMB共有に対してSMB暗号化を有効または要求することで、より多くのアクセス制御を適用できます。いずれかのエンドポイントでSMB暗号化がサポートされていない場合、アクセスは許可されません。

SMB名エイリアスを使用する

場合によっては、エンドユーザがCloud Volumes Service で使用するマシンアカウント名を把握することがセキュリティ上の懸念事項になることがあります。また、単にエンドユーザへのアクセスパスを単純化することもできます。このような場合は、SMBエイリアスを作成できます。

SMB共有パスのエイリアスを作成する場合は、DNSでCNAMEレコードと呼ばれるものを利用できます。たとえば'\\cvs-east-433d.cvsdemo.local'ではなく'\\CIFS'という名前を使用して共有にアクセスするが'Kerberos認証を使用する場合は'A/AAAAレコードを指すDNSのCNAMEと'既存のマシンアカウントに追加されたSPNがKerberosアクセスを提供します



CNAMEを追加したあとのDNS前方参照の結果を次に示します。

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

新しいSPNを追加したあとのSPNクエリの結果を次に示します。

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

パケットキャプチャでは、CNAMEに関連付けられたSPNを使用してセッション設定要求を確認できます。

```
431 4.156722                                    SMB2     308 Negotiate Protocol Response
432 4.156785                                    SMB2     232 Negotiate Protocol Request
434 4.158108                                    SMB2     374 Negotiate Protocol Response
435 4.160977                                    SMB2    1978 Session Setup Request
437 4.166224                                    SMB2     322 Session Setup Response
438 4.166891                                    SMB2     152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063                                    SMB2     138 Tree Connect Response
```

```
realm: CVSDEMO.LOCAL
sname
   name-type: kRB5-NT-SRV-INST (2)
   sname-string: 2 items
      SNameString: cifs
      SNameString: cifs
enc-part
   etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

SMB認証ダイアレクト

Cloud Volumes Service では、次の機能がサポートされ "方言" SMB認証の場合：

- LM
- NTLM
- NTLMv2
- Kerberos

SMB共有アクセスのKerberos認証は、使用できる最も安全な認証レベルです。AESおよびSMB暗号化が有効になっていると、セキュリティレベルがさらに向上します。

Cloud Volumes Service では、LMおよびNTLM認証の下位互換性もサポートされています。Kerberosの設定が正しくない場合（SMBエイリアスの作成時など）、共有アクセスはより脆弱な認証方法（NTLMv2など）にフォールバックされます。これらのメカニズムは安全性が低いため、一部のActive Directory環境では無効になっています。より脆弱な認証方法が無効になっていて、Kerberosが適切に設定されていない場合、フォールバックする有効な認証方法がないため、共有アクセスは失敗します。

Active Directoryでサポートされている認証レベルの設定/表示については、を参照してください "ネットワークセキュリティ：LAN Manager認証レベル"。

アクセス許可モデル

NTFS /ファイル権限

NTFS権限とは、NTFSロジックに準拠したファイルシステム内のファイルおよびフォルダに適用される権限です。NTFSアクセス権は'Basic'または'Advanced'で適用でき'アクセス制御の場合は'allow'または[Deny]に設定できます

基本的な権限は次のとおりです。

- フルコントロール
- 変更
- 読み取りと実行
- 読み取り
- 書き込み

ACEと呼ばれるユーザまたはグループに権限を設定すると、ACLに含まれます。NTFS権限では、UNIXモードビットと同じ読み取り/書き込み/実行の基本が使用されますが、所有権の取得、フォルダの作成/追加、データの書き込み、属性の書き込みなど、より詳細で拡張されたアクセス制御（特別な権限）にも拡張できます。

標準UNIXモードビットは、NTFSアクセス権と同じレベルの粒度を提供しません（ACL内の個々のユーザおよびグループオブジェクトにアクセス権を設定したり、拡張属性を設定したりすることなど）。ただし、NFSv4.1 ACLは、NTFS ACLと同じ機能を提供します。

NTFS権限は共有権限よりも限定的であり、共有権限と組み合わせて使用できます。NTFSの権限構造では、最も制限があります。このため、アクセス権を定義するときに、ユーザまたはグループに対する明示的な拒否もフルコントロールよりも優先されます。

NTFSアクセス権はWindows SMBクライアントから制御されます。

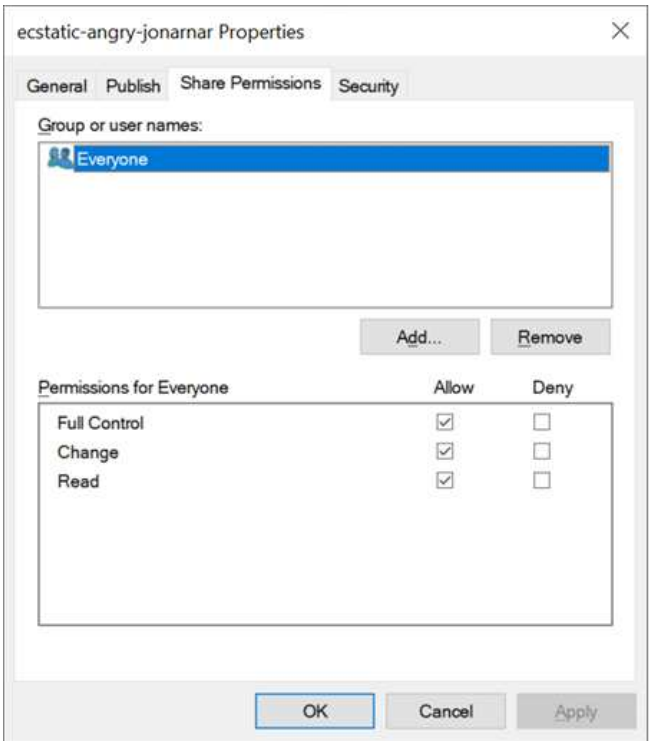
共有権限

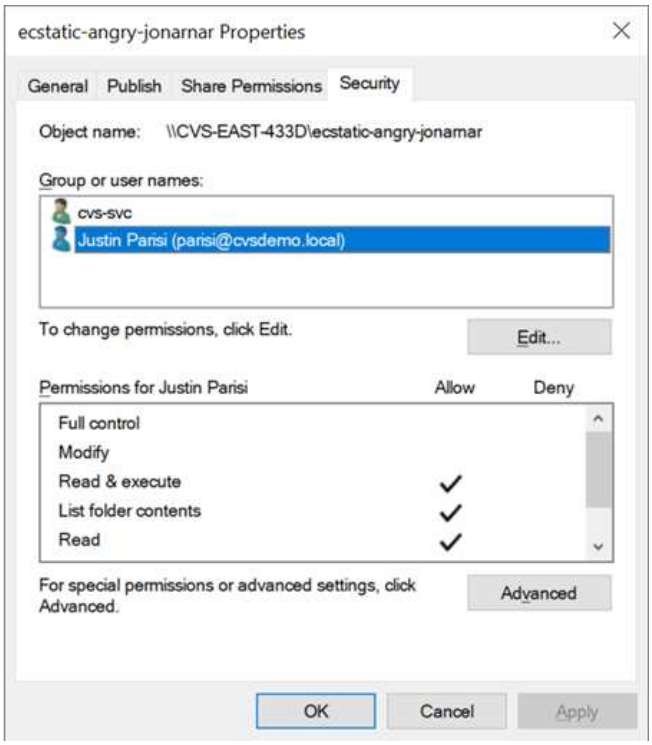
共有権限は、NTFS権限（読み取り/変更/フルコントロールのみ）よりも一般的で、NFSエクスポートポリシールールの仕組みと同様に、SMB共有への最初のエントリを制御します。

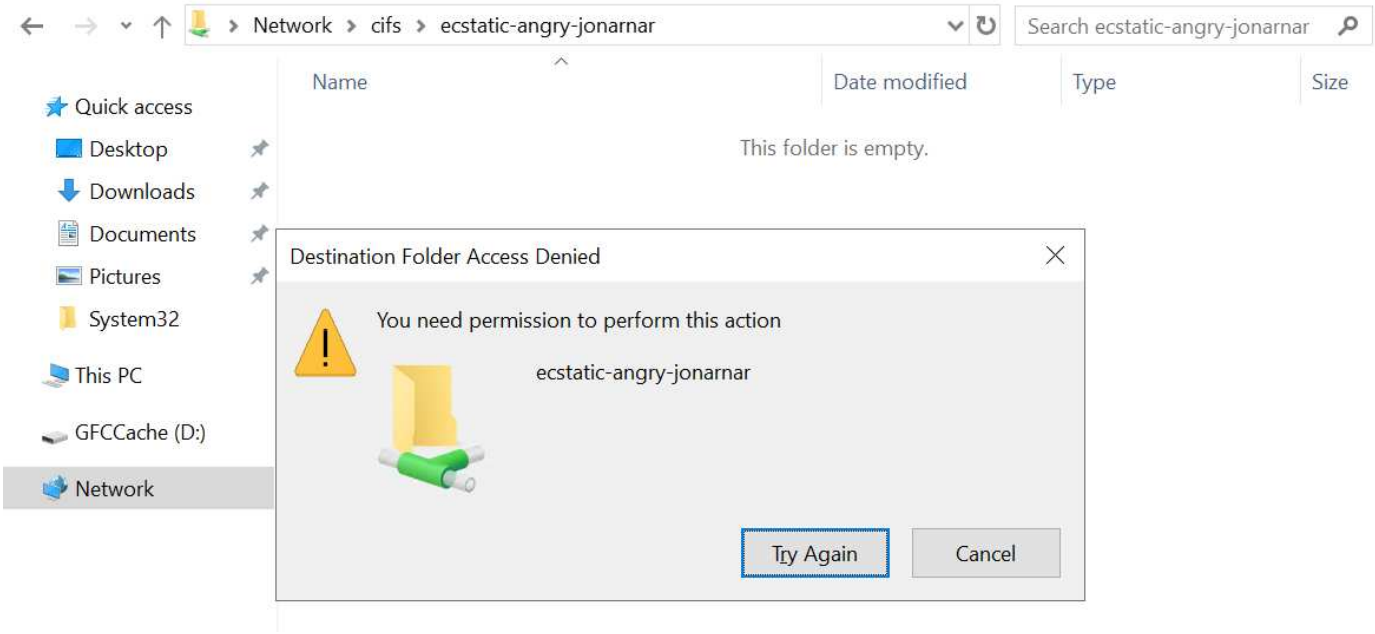
NFSエクスポートポリシールールは、IPアドレスやホスト名などのホストベースの情報を介したアクセスを制御しますが、SMB共有権限は共有ACLでユーザおよびグループACEを使用してアクセスを制御できます。共有ACLは、WindowsクライアントまたはCloud Volumes Service 管理UIから設定できます。

デフォルトでは、共有ACLと初期ボリュームACLにはフルコントロールを使用したすべてのメンバーが含まれます。ファイルACLを変更する必要がありますが、共有内のオブジェクトのファイル権限によって共有権限が上書きされます。

たとえば、ユーザにCloud Volumes Service ボリュームファイルACLへの読み取りアクセスのみが許可されている場合、次の図に示すように、共有ACLがフルコントロールを使用するEveryoneに設定されていても、ファイルおよびフォルダの作成アクセスは拒否されます。







セキュリティ上の最善の結果を得るには、次の手順を実行します。

- 共有およびファイルのACLからすべてのユーザを削除し、代わりにユーザまたはグループの共有アクセスを設定します。
- 個々のユーザではなくグループを使用してアクセス制御を行うと、管理が容易になり、グループ管理を通じてユーザの削除や追加を迅速に行うことができます。
- 共有権限のACEに対する制限が厳しくなく、一般的な共有アクセスを許可し、ファイル権限を持つユーザとグループにロックダウンされて、より詳細なアクセス制御が可能になります。
- 明示的なDENY ACLは、ALLOW ACLより優先されるため、一般的に使用しないでください。ファイルシステムへのアクセスを迅速に制限する必要があるユーザまたはグループに対する明示的なDENY ACLの使

用を制限してください。

- に注意を払ってください "ACLの継承" 権限を変更する際の設定。ファイル数の多いディレクトリまたはボリュームの最上位で継承フラグを設定すると、そのディレクトリまたはボリュームの下の各ファイルに継承された権限が追加されます。 これにより、各ファイルの調整時に意図しないアクセス/拒否や権限の大幅な変更など、不要な動作が発生する可能性があります。

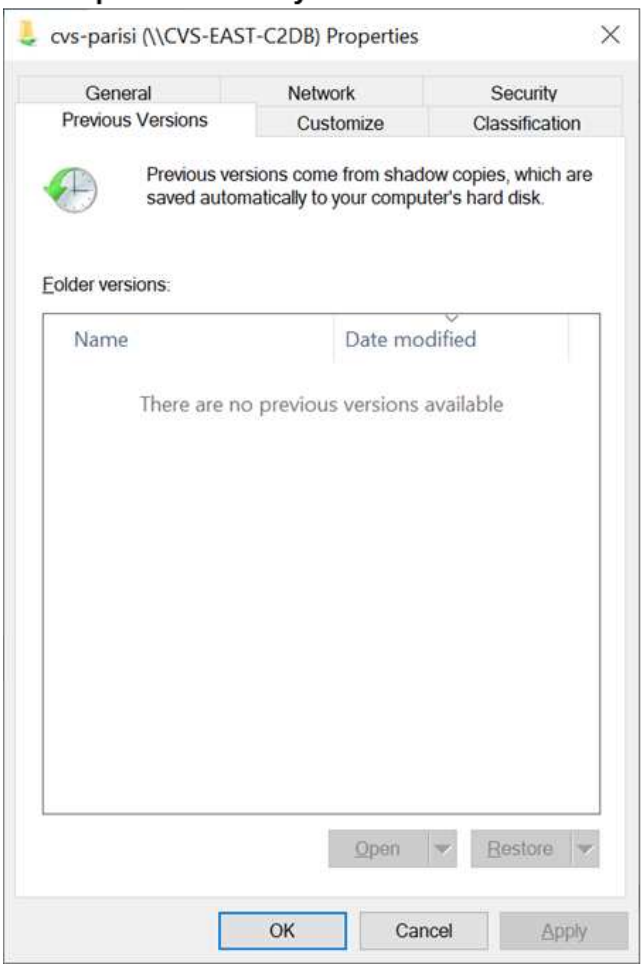
SMB共有のセキュリティ機能

Cloud Volumes Service でSMBアクセスを使用するボリュームを最初に作成するときに、そのボリュームを保護するための一連の選択肢が表示されます。

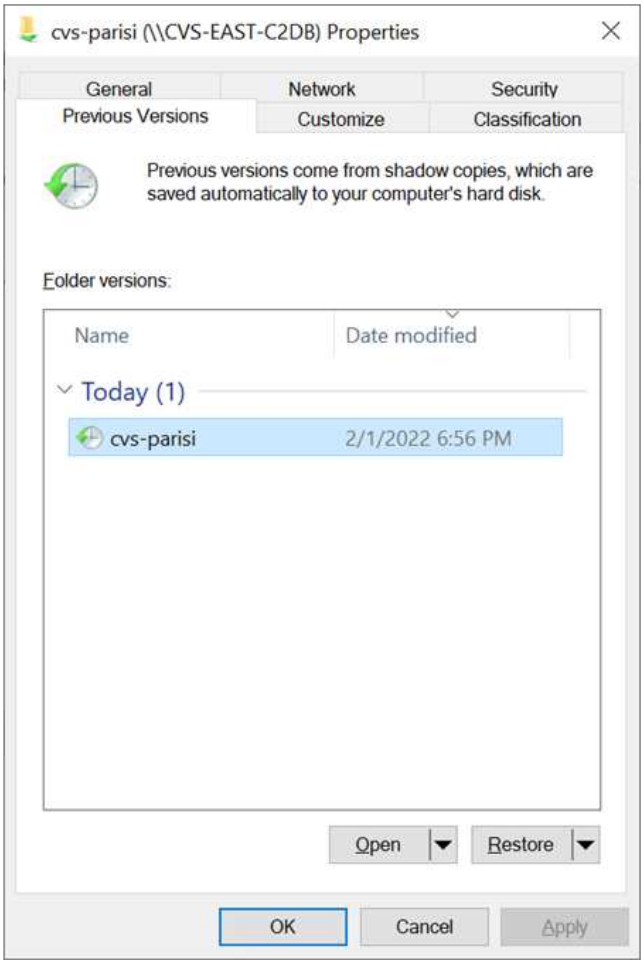
Cloud Volumes Service レベル（パフォーマンスまたはソフトウェア）に応じて、次の選択肢があります。

- *スナップショット・ディレクトリを表示する（CVS -パフォーマンスとCVS - SWの両方で利用可能）*このオプションはSMBクライアントがSMB共有内のスナップショット・ディレクトリにアクセスできるかどうかを制御します（\\server\share\~snapshotタブまたはPrevious Versionsタブ）。デフォルトの設定はチェックされませんボリュームのデフォルトは'~snapshot'ディレクトリへのアクセスを非表示にして拒否し'ボリュームの[以前のバージョン]タブにスナップショット・コピーは表示されません

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



セキュリティ上の理由、パフォーマンス上の理由（これらのフォルダをAVスキャンから非表示にする）、または設定上の理由から、エンドユーザに対してSnapshotコピーを非表示にすることが望ましい場合があります。Cloud Volumes Service スナップショットは読み取り専用であるため、これらのスナップショットが表示されていても、エンドユーザーはスナップショットディレクトリ内のファイルを削除または変更することはで

きません。Snapshotコピーが作成された時点のファイルまたはフォルダのファイル権限Snapshotコピー間でファイルまたはフォルダの権限が変更された場合、変更内容はSnapshotディレクトリ内のファイルまたはフォルダにも適用されます。ユーザとグループは、権限に基づいてこれらのファイルやフォルダにアクセスできます。Snapshotディレクトリ内のファイルの削除または変更はできませんが、ファイルまたはフォルダをSnapshotディレクトリからコピーすることは可能です。

- * SMB暗号化を有効にします（CVS -パフォーマンスとCVS - SWの両方で利用可能）。* SMB暗号化は、SMB共有ではデフォルトで無効になっています（オフ）。このチェックボックスをオンにすると、SMB暗号化が有効になります。つまり、SMBクライアントとサーバ間のトラフィックが、ネゴシエートされたサポート対象の最大暗号化レベルで転送中に暗号化されます。Cloud Volumes Service は、SMBで最大AES-256暗号化をサポートしています。SMB暗号化を有効にした場合、SMBクライアントが気づくことがあるパフォーマンス低下はありません。約10~20%の範囲になります。ネットアップでは、パフォーマンスへの影響が許容されるかどうかをテストで確認することを強く推奨してい
- * SMB共有を非表示にします（CVS -パフォーマンスとCVS - SWの両方に利用できます）。*このオプションを設定すると、SMB共有パスが通常の閲覧から見えなくなります。つまり、共有パスがわからないクライアントは、デフォルトのUNCパス（例：\\cvs-smb）にアクセスすると共有を参照できません。このチェックボックスをオンにすると、SMB共有パスを明示的に知っているクライアント、またはグループポリシーオブジェクトによって定義された共有パスを持つクライアントだけが、このパスにアクセスできます（難読化によるセキュリティ）。
- アクセスベースの列挙（**ABE**）を有効にします（**CVS - SW**のみ）。 SMB共有を非表示にするのと似ています。ただし、共有やファイルは、オブジェクトへのアクセス権限がないユーザまたはグループに対してのみ表示されます。たとえば、Windowsユーザ「joe」に許可されているアクセス許可で少なくとも読み取りアクセスが許可されていない場合、Windowsユーザ「joe」はSMB共有またはファイルをまったく表示できません。このオプションはデフォルトでは無効になっており、チェックボックスを選択することで有効にできます。ABEの詳細については、ネットアップの技術情報アーティクルを参照してください "アクセスベースの列挙（ABE）の仕組み"
- 継続的可用性（**CA**）共有のサポートを有効にします（**CVS -**パフォーマンスのみ）。 "継続的可用性を備えたSMB共有" Cloud Volumes Service バックエンドシステム内のノード間でロック状態をレプリケートすることで、フェイルオーバーイベント中のアプリケーションの停止を最小限に抑えることができます。これはセキュリティ機能ではありませんが、全体的な耐障害性は向上します。現在、この機能では、SQL ServerとFSLogixアプリケーションのみがサポートされています。

デフォルトの非表示共有

Cloud Volumes Service でSMBサーバを作成すると、その場所に配置されます "非表示の管理共有" データボリュームのSMB共有に加えて作成される（$命名規則を使用）。これには、C$（名前空間アクセス）とIPC$（Microsoft管理コンソール（MMC）へのアクセスに使用されるリモート手順 呼び出し（RPC）などのプログラム間の通信用の名前付きパイプの共有）が含まれます。

IPC$共有には共有ACLは含まれておらず、変更することはできません。これはRPC呼び出しおよびにのみ使用されます "Windowsは、これらの共有への匿名アクセスをデフォルトで禁止します"。

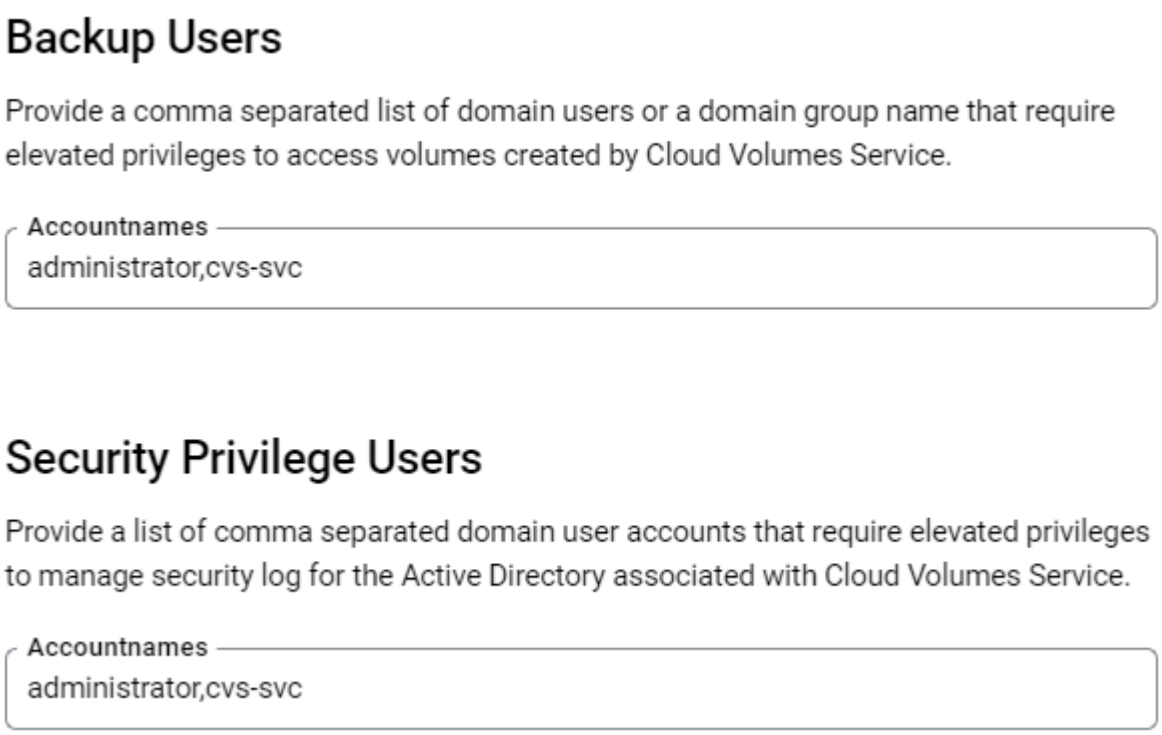
C$共有ではデフォルトでBUILTIN\Administratorsアクセスが許可されますが、Cloud Volumes Service 自動化によって共有ACLが削除され、C$共有へのアクセスによってCloud Volumes Service ファイルシステム内のマウントされたすべてのボリュームが可視化されるため、すべてのユーザにアクセスすることはできません。その結果'\\server\C$'への移動は失敗します

ローカル/ **BUILTIN**管理者/バックアップ権限を持つアカウント

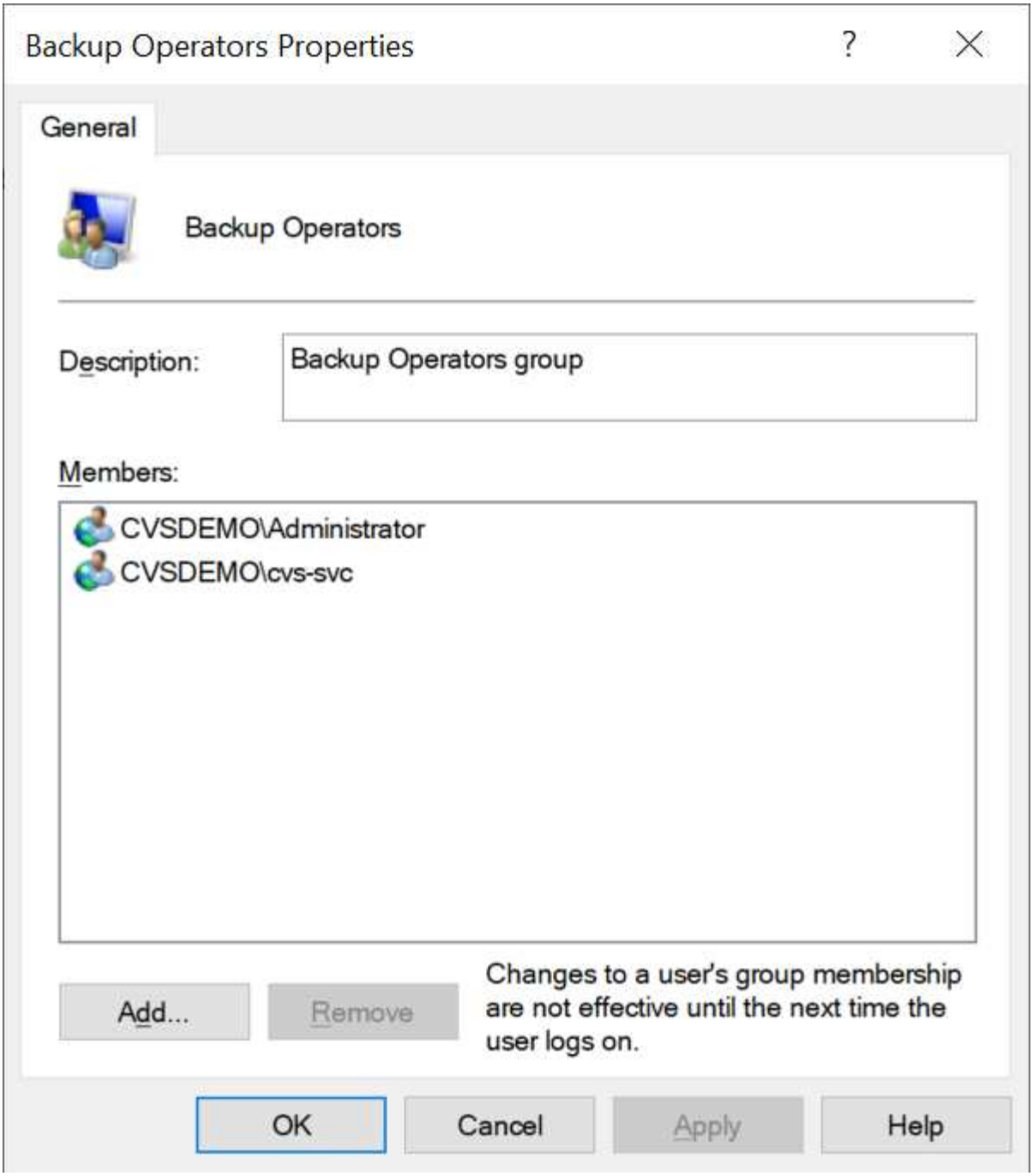
Cloud Volumes Service SMBサーバは、選択したドメインユーザおよびグループにアクセス権を適用するローカルグループ（BUILTIN\Administratorsなど）があることに、通常のWindows SMBサーバと同様の機能を維持します。

バックアップユーザに追加するユーザを指定すると、そのActive Directory接続を使用するCloud Volumes Service インスタンスのBUILTIN\Backup Operatorsグループにユーザが追加され、が取得されます "SeBackupPrivilegeおよびSeRestorePrivilege"。

Security Privilegeユーザにユーザを追加すると、そのユーザにはSeSecurityPrivilegeが付与されます。これは、などの一部のアプリケーションユースケースで役立ちます "SMB共有上のSQL Server"。



Cloud Volumes Service ローカルグループメンバーシップは、適切な権限を持つMMCを使用して表示できます。次の図に、Cloud Volumes Service コンソールを使用して追加されたユーザを示します。

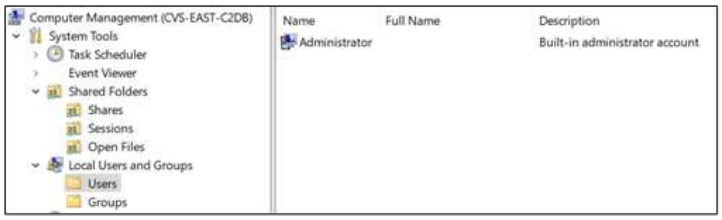


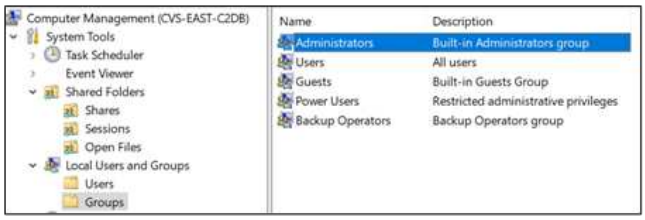
次の表に、デフォルトのBUILTINグループのリストと、デフォルトで追加されるユーザ/グループを示します。

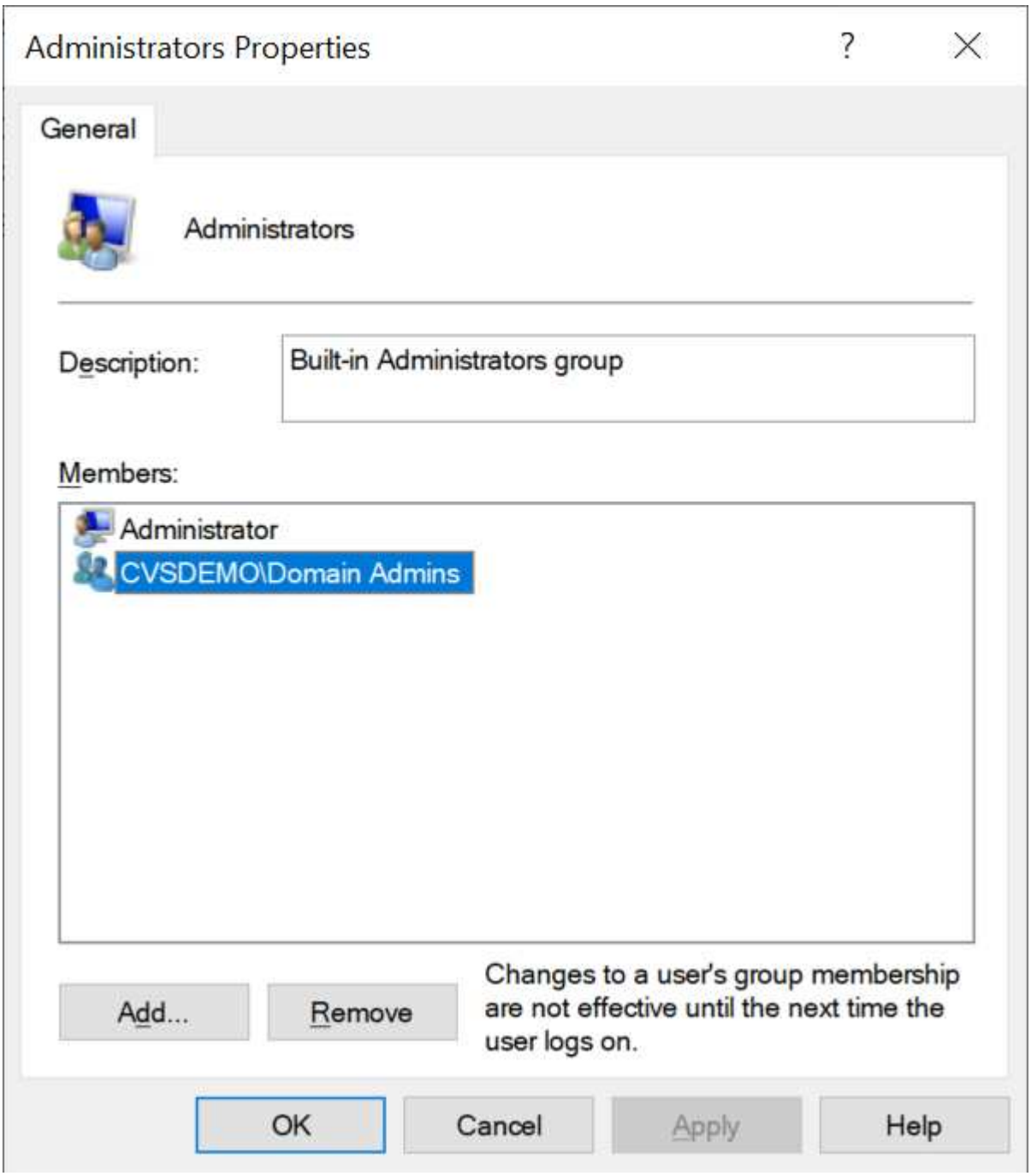
ローカル/ **BUILTIN**グループ	デフォルトのメンバー
builtin\Administrators*	Domain\Domain Adminsの略
Builtin\Backup Operators*	なし
組み込みのゲスト	Domain\Domainゲスト
Builtin\Power Usersの場合	なし
組み込みのドメインユーザ	Domain\Domain Usersの略

*グループメンバーシップはCloud Volumes Service Active Directory接続設定で制御されます。

MMCウィンドウにはローカルユーザとローカルグループ（およびグループメンバー）を表示できますが、このコンソールからオブジェクトの追加や削除、グループメンバーシップの変更はできません。デフォルトでは、Cloud Volumes Service のBUILTIN\AdministratorsグループとAdministratorのみが追加されます。現時点では、これを変更することはできません。







MMC /コンピュータ管理アクセス

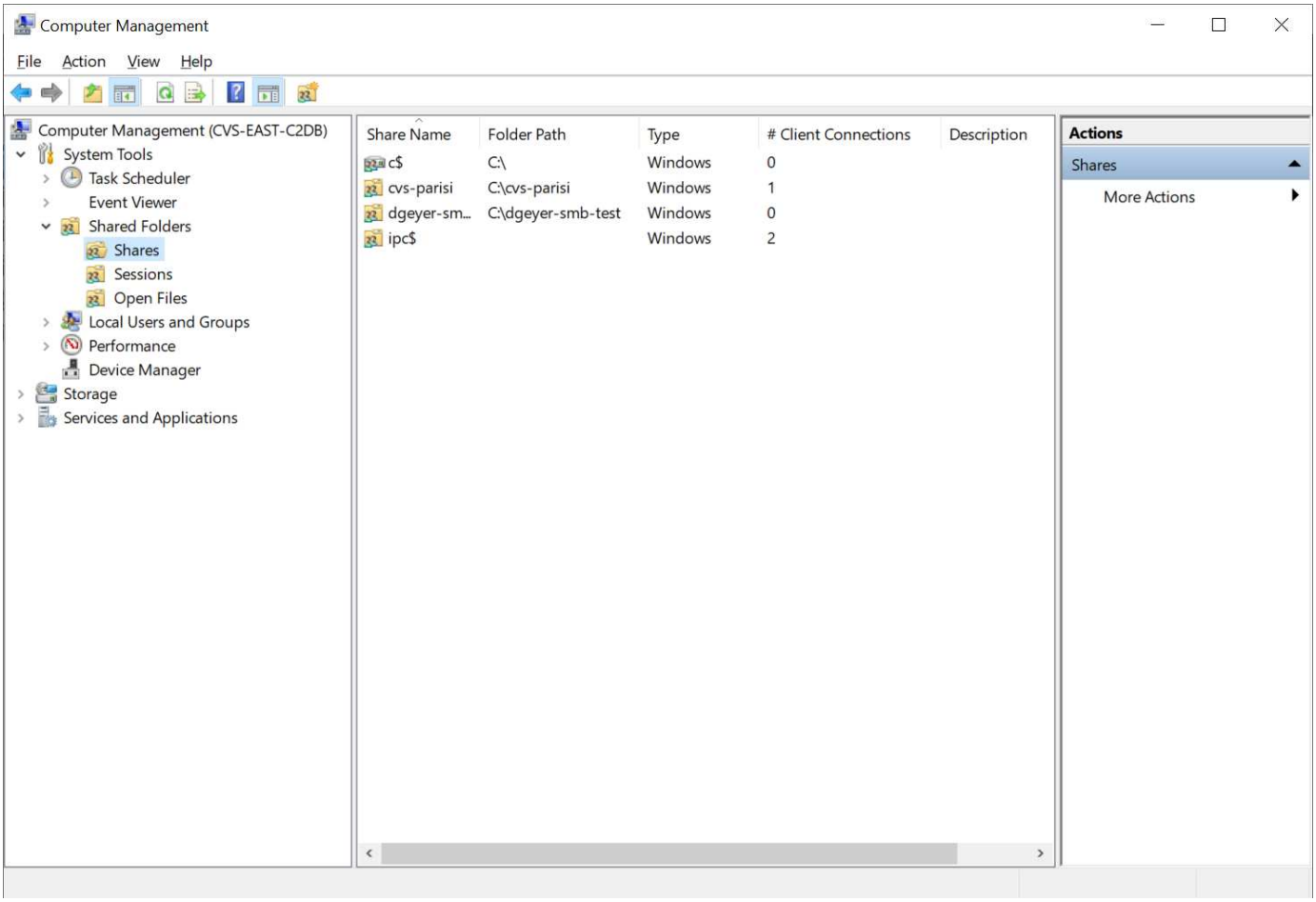
Cloud Volumes Service のSMBアクセスはコンピュータの管理MMCへの接続を提供します。MMCを使用すると、共有の表示、共有ACLの管理、SMBセッションの表示と管理、および開いているファイルの表示を行うことができます。

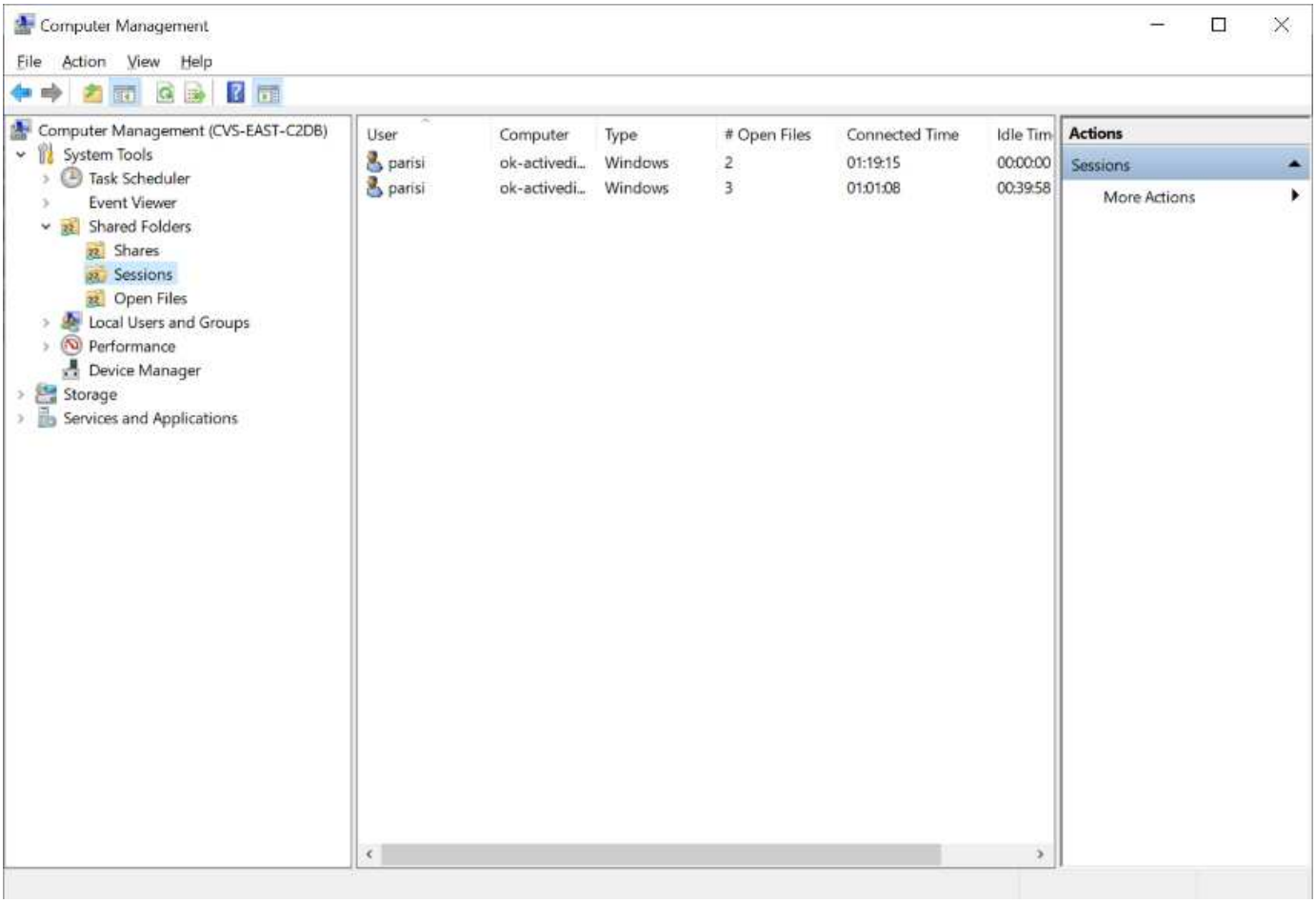
MMCを使用してCloud Volumes Service のSMB共有およびセッションを表示するには、現在ログインしているユーザがドメイン管理者である必要があります。他のユーザには、MMCを使用したSMBサーバの表示または管理へのアクセスを許可されているほか、Cloud Volumes Service SMBインスタンスで共有やセッションを表示しようとすると、[You do not have Permissions]ダイアログボックスが表示されます。

SMBサーバーに接続するには、[コンピューターの管理]を開き、[コンピューターの管理]を右クリックして、[別のコンピューターに接続]を選択します。コンピュータの選択ダイアログボックスが開き、SMBサーバ名（Cloud Volumes Service ボリューム情報に含まれています）を入力できます。

適切な権限を持つSMB共有を表示すると、Active Directory接続を共有するCloud Volumes Service インスタンス内の使用可能なすべての共有が表示されます。この動作を制御するには、Cloud Volumes Service ボリュームインスタンスでSMB共有を非表示オプションを設定します。

リージョンごとに許可されるActive Directory接続は1つだけです。





次の表に、MMCでサポートされる機能とサポートされない機能を示します。

サポートされている機能	サポートされていない機能
• 共有を表示します • アクティブなSMBセッションを表示します • 開いているファイルを表示します • ローカルユーザとローカルグループを表示します • ローカルグループメンバーシップを表示します • システムのセッション、ファイル、およびツリー接続のリストを列挙します • 開いているファイルを閉じます • 開いているセッションを閉じます • 共有を作成 / 管理します	• 新しいローカルユーザ / グループを作成しています • 既存のローカルユーザ/グループの管理/表示 • イベントまたはパフォーマンスログを表示します • ストレージの管理 • サービスとアプリケーションの管理

SMBサーバのセキュリティ情報

Cloud Volumes Service のSMBサーバでは、Kerberosのクロックスキュー、チケットの有効期間、暗号化など、SMB接続のセキュリティポリシーを定義する一連のオプションを使用します。

次の表に、これらのオプションとその機能、デフォルト設定、およびCloud Volumes Service で変更できるかどうかを示します。一部のオプションはCloud Volumes Service には適用されません。

セキュリティオプション	機能	デフォルト値	変更は可能ですか？
Kerberosの最大クロックスキュー（分）	Cloud Volumes Service とドメインコントローラ間の最大時間スキューを指定します。時刻のずれが5分を超えるとKerberos認証は失敗します。これはActive Directoryのデフォルト値に設定されています。	5.	いいえ
Kerberosチケットの有効期間（時間）	Kerberosチケットの有効期間が終了しないと更新が必要になります。10時間以内に更新が行われない場合は、新しいチケットを取得する必要があります。Cloud Volumes Service は、これらの更新を自動的に実行します。Active Directoryのデフォルト値は10時間です。	10.	いいえ
Kerberosチケットの最大更新日数	新しい許可要求が必要になるまでKerberosチケットを更新できる最大日数。Cloud Volumes Service はSMB接続のチケットを自動的に更新します。Active Directoryのデフォルト値は7日です。	7.	いいえ
Kerberos KDC接続タイムアウト（秒）	KDC接続がタイムアウトするまでの秒数。	3.	いいえ
受信SMBトラフィックに署名を要求します	SMBトラフィックに署名を要求するかどうかを設定します。trueに設定すると、署名をサポートしていないクライアントは接続に失敗します。	いいえ	
ローカルユーザアカウントに複雑なパスワードを要求します	ローカルSMBユーザのパスワードに使用します。Cloud Volumes Service ではローカルユーザの作成はサポートされないため、このオプションはCloud Volumes Service には適用されません。	正しいです	いいえ

セキュリティオプション	機能	デフォルト値	変更は可能ですか？
Active Directory LDAP接続にはstart_tlsを使用します	Active Directory LDAPのStart TLS接続を有効にするために使用します。現在、Cloud Volumes Service ではこの機能の有効化がサポートされていませ	いいえ	いいえ
は、KerberosのAES-128およびAES-256暗号化を有効にします	Active Directory接続にAES暗号化を使用するかどうかを制御し、Active Directory接続の作成/変更時にActive Directory認証用のAES暗号化を有効にするオプションで制御します。	いいえ	はい。
LM互換性レベル	Active Directory接続でサポートされている認証ダイアレクトのレベル。「」を参照してくださいSMB認証ダイアレクト」を参照してください。	NTLMv2 - krb	いいえ
受信CIFSトラフィックにSMB暗号化を要求します	すべての共有でSMB暗号化が必要です。これはCloud Volumes Serviceでは使用されません。代わりに、ボリューム単位で暗号化を設定します（「」を参照）SMB共有のセキュリティ機能」）をクリックします。	いいえ	いいえ
クライアントセッションセキュリティ	LDAP通信の署名と封印を設定します。この機能は現在Cloud Volumes Service には設定されていませんが、今後のリリースでサポートする必要が生じる可能性があります。WindowsパッチによるLDAP認証の問題に対する修正については、セクションで説明しています"「LDAPチャネルバインディング」"。	なし	いいえ
DC接続のSMB2有効化	DC接続にSMB2を使用します。デフォルトは有効です。	システム-デフォルト	いいえ

セキュリティオプション	機能	デフォルト値	変更は可能ですか？
LDAPリファーラル追跡	複数のLDAPサーバを使用している場合、リファーラル追跡を使用すると、クライアントが最初のサーバでエントリが見つからなかったときに、リスト内の他のLDAPサーバを参照することができます。これは現在、Cloud Volumes Service ではサポートされていません。	いいえ	いいえ
セキュアなActive Directory接続にLDAPSを使用します	LDAP over SSLを有効にします。現在、Cloud Volumes Service ではサポートされていません。	いいえ	いいえ
DC接続には暗号化が必要です	DC接続を成功させるには暗号化が必要です。Cloud Volumes Service ではデフォルトで無効になっています。	いいえ	いいえ

デュアルプロトコル/マルチプロトコル

Cloud Volumes Service では、適切なアクセス権限を維持しながら、SMBクライアントとNFSクライアントの両方で同じデータセットを共有できます ("デュアルプロトコル" ）。これを行うには、プロトコル間でIDマッピングを調整し、中央のバックエンドLDAPサーバを使用してUNIX IDをCloud Volumes Service に提供します。Windows Active Directoryを使用すると、WindowsとUNIXの両方のユーザに使いやすさを提供できます。

Access Control の略

- 共有アクセス制御。 NAS共有にアクセスできるクライアントまたはユーザーおよびグループを決定します。NFSの場合は、エクスポートへのクライアントアクセスを制御するエクスポートポリシーとルールがあります。NFSエクスポートはCloud Volumes Service インスタンスから管理されます。SMBは、CIFS / SMB共有と共有ACLを利用して、ユーザレベルおよびグループレベルでより細かく制御します。を使用して設定できるのは、SMBクライアントからのみ共有レベルのACLです "MMC /コンピュータの管理" Cloud Volumes Service インスタンスに対する管理者権限を持つアカウントを使用する場合（を参照） ""ローカル/ BUILTIN管理者/バックアップ権限を持つアカウント""）。
- *ファイルアクセス制御。*ファイルまたはフォルダレベルで権限を制御し、常にNASクライアントから管理します。NFSクライアントは、従来のモードビット（rwx）またはNFSv4 ACLを使用できます。SMBクライアントはNTFS権限を利用します。

NFSとSMBの両方にデータを提供するボリュームのアクセス制御は、使用しているプロトコルによって異なります。デュアルプロトコルの権限については、「」を参照してください[アクセス許可モデル]」

ユーザマッピング

クライアントがボリュームにアクセスすると、Cloud Volumes Service は受信ユーザを反対方向の有効なユー

ザにマッピングしようとします。これは、プロトコルを使用して適切なアクセスを決定し、アクセスを要求しているユーザが実際に誰であるかを確認するために必要です。

たとえば、「joe」という名前のWindowsユーザがSMB経由でUNIXアクセス権を持つボリュームにアクセスしようとすると、Cloud Volumes Service は「joe」という名前の対応するUNIXユーザを検索します。存在する場合、Windowsユーザ「joe」としてSMB共有に書き込まれるファイルは、NFSクライアントからはUNIXユーザ「joe」と表示されます。

また、「joe」という名前のUNIXユーザがWindows権限を持つCloud Volumes Service ボリュームへのアクセスを試みる場合、そのUNIXユーザは有効なWindowsユーザにマッピングできる必要があります。そうしないと、ボリュームへのアクセスが拒否されます。

現時点では、LDAPを使用した外部UNIX IDの管理でサポートされているのはActive Directoryのみです。このサービスへのアクセスの設定の詳細については、を参照してください "AD接続の作成"。

アクセス許可モデル

デュアルプロトコルのセットアップを使用する場合、Cloud Volumes Service では、ボリュームのセキュリティ形式を使用してACLのタイプを決定します。これらのセキュリティ形式は、Cloud Volumes Service ボリュームの作成時に選択したNASプロトコル、またはデュアルプロトコルの場合に選択したセキュリティ形式に基づいて設定されます。

- NFSのみを使用している場合は、Cloud Volumes Service ボリュームでUNIX権限が使用されます。
- SMBのみを使用する場合、Cloud Volumes Service ボリュームはNTFS権限を使用します。

デュアルプロトコルボリュームを作成する場合は、ボリュームの作成時にACL形式を選択できます。この決定は、必要な権限管理に基づいて行う必要があります。ユーザがWindows / SMBクライアントから権限を管理している場合は、NTFSを選択します。ユーザがNFSクライアントおよびchmod / chownを使用することを希望する場合は、UNIXセキュリティ形式を使用します。

Active Directory接続の作成に関する考慮事項

Cloud Volumes Service を使用すると、SMBユーザとUNIXユーザのIDを管理するために、Cloud Volumes Service インスタンスを外部のActive Directoryサーバに接続できます。Cloud Volumes Service でSMBを使用するには、Active Directory接続を作成する必要があります。

この構成には、セキュリティについて考慮する必要があるいくつかのオプションがあります。外部Active Directoryサーバは、オンプレミスインスタンスでもクラウドネイティブでもかまいません。オンプレミスのActive Directoryサーバを使用している場合は、ドメインを外部ネットワーク（DMZや外部IPアドレスなど）に公開しないでください。代わりに、を使用して、セキュアなプライベートトンネルまたはVPN、一方向フォレストトラスト、またはオンプレミスネットワークへの専用ネットワーク接続を使用します "プライベートGoogle アクセス"。詳細については、Google Cloudのドキュメントを参照してください "Google CloudでActive Directoryを使用する際のベストプラクティス"。

CVS-SWを使用するには、Active Directoryサーバを同じリージョンに配置する必要があります。CVS-SWで別の地域へのDC接続を試みた場合、試行は失敗します。CV-SWを使用する場合は、Active Directory DCを含むActive Directoryサイトを作成し、Cloud Volumes Service でサイトを指定して、リージョン間のDC接続の試行を回避してください。

Active Directoryのクレデンシャル

NFS用のSMBまたはLDAPが有効な場合、Cloud Volumes Service はActive Directoryコントローラと通信して、認証に使用するマシンアカウントオブジェクトを作成します。これは、Windows SMBクライアントがドメインに参加する方法とまったく異なり、Active Directoryの組織単位（OU）への同じアクセス権を必要とします。

多くの場合、セキュリティグループでは、Cloud Volumes Service などの外部サーバでWindows管理者アカウントを使用できません。場合によっては、セキュリティのベストプラクティスとして、Windows Administratorユーザが完全に無効になっていることもあります。

SMBマシンアカウントの作成に必要な権限

Cloud Volumes Service マシンオブジェクトをActive Directoryに追加するには、ドメインに対する管理者権限を持つアカウント、またはが必要です "マシンアカウントオブジェクトを作成および変更する権限を委譲しました" 指定したOUに移動する必要があります。Active Directoryの制御の委任ウィザードでこれを行うには、次のアクセス権限を持つコンピュータオブジェクトの作成/削除へのユーザーアクセスを提供するカスタムタスクを作成します。

- 読み取り / 書き込み
- すべての子オブジェクトを作成/削除します
- すべてのプロパティの読み取り/書き込み
- パスワードの変更/リセット

これにより、定義済みのユーザのセキュリティACLがActive DirectoryのOUに自動的に追加され、Active Directory環境へのアクセスが最小限に抑えられます。ユーザを委任した後、そのユーザ名とパスワードをActive Directoryクレデンシャルとしてこのウィンドウに入力できます。

Active Directoryドメインに渡されるユーザ名とパスワードは、マシンアカウントオブジェクトのクエリおよび作成時にKerberos暗号化を利用してセキュリティを強化します。

Active Directory接続の詳細

。 "Active Directory接続の詳細" 管理者がマシンアカウントの配置に関する特定のActive Directoryスキーマ情報を指定するためのフィールドを指定します。次に例を示します。

- * Active Directory接続タイプ。リージョン内のActive Directory接続を、Cloud Volumes Service またはCVS -パフォーマンスサービスタイプのボリュームに使用するかどうかを指定するために使用します。既存の接続で正しく設定しないと、使用または編集時に正しく機能しないことがあります。
- ドメイン。 Active Directoryドメイン名。
- サイト。 Active Directoryサーバを特定のサイトに制限して、セキュリティとパフォーマンスを確保します "考慮事項"。Cloud Volumes Service では現在、Cloud Volumes Service インスタンスとは別のリージョンにあるActive Directoryサーバへの認証要求の許可がサポートされていないため、複数のActive Directoryサーバがリージョンにまたがっている場合は、この設定が必要です。（たとえば、Active Directoryドメインコントローラは CVS -パフォーマンスのみがサポートするリージョンにありますが、CVS - SWインスタンスにSMB共有が必要です）。
- * DNSサーバ。*名前検索で使用するDNSサーバ。
- * NetBIOS名（オプション）。*必要に応じて、サーバのNetBIOS名。これは、Active Directory接続を使用して新しいマシンアカウントを作成するときに使用されます。たとえば、NetBIOS名がCVS - Eastに設定

されている場合、マシンアカウント名はCVS - East -｛1234｝になります。を参照してください "Active DirectoryでのCloud Volumes Service の表示" を参照してください。

- *組織単位(OU)。*コンピュータアカウントを作成するための特定のOU。この機能は、マシンアカウントの制御を特定のOUに委任する場合に便利です。
- *AES暗号化。*AD認証用AES暗号化を有効にするチェックボックスをオンまたはオフにすることもできます。Active Directory認証用のAES暗号化を有効にすると、ユーザとグループの検索時にCloud Volumes Service からActive Directoryへの通信がセキュリティで保護されます。このオプションを有効にする前に、ドメイン管理者に問い合わせて、Active Directoryドメインコントローラが AES認証をサポートしていることを確認してください。

デフォルトでは、ほとんどのWindowsサーバで弱い暗号（DESやRC4-HMACなど）は無効になりませんが、弱い暗号を無効にするように選択した場合は、Cloud Volumes Service Active Directory接続がAESを有効にするように設定されていることを確認してください。そうしないと、認証エラーが発生します。AES暗号化を有効にしても弱い暗号は無効になりませんが、Cloud Volumes Service SMBマシンアカウントにAES暗号のサポートが追加されます。

Kerberos Realmの詳細

このオプションはSMBサーバには適用されません。Cloud Volumes Service システムでNFS Kerberosを設定するときに使用されます。これらの詳細を入力すると、NFS Kerberos Realmが設定され（Linuxではkrb5.conf ファイルと同様）、Cloud Volumes Service ボリュームの作成時にNFS Kerberosが指定されている場合にActive Directory接続がNFS Kerberos Distribution Center（KDC；Kerberos配布センター）として機能するために使用されます。

現在、Windows以外のKDCはCloud Volumes Service との使用でサポートされていません。

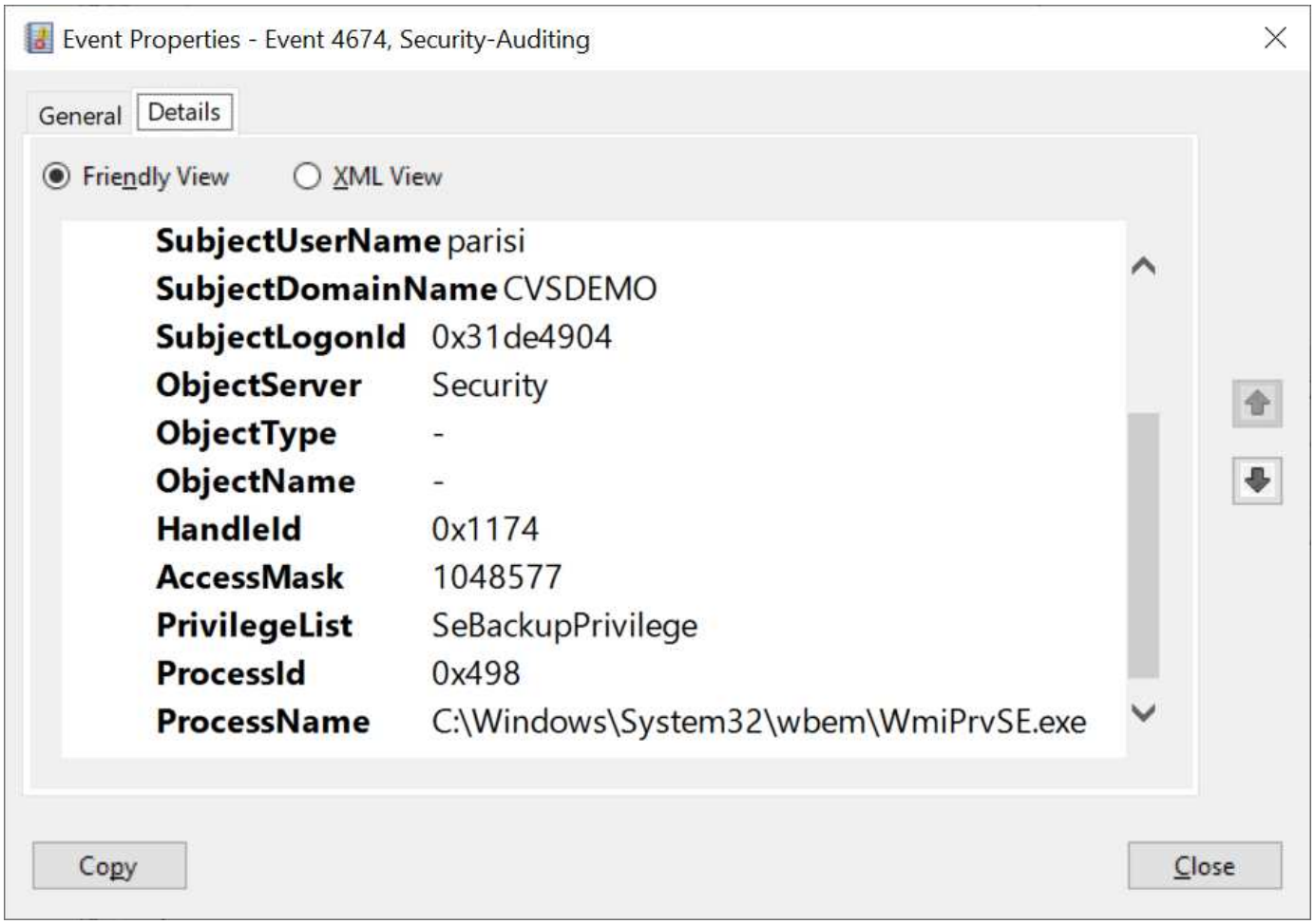
地域

リージョンを使用すると、Active Directory接続が存在する場所を指定できます。このリージョンはCloud Volumes Service ボリュームと同じである必要があります。

- *このセクションでは、LDAPを使用するローカルNFSユーザを許可するオプションもあります。*このセクションでは、LDAPを使用するローカルNFSユーザを許可するオプションもあります。NFS（拡張グループ）の16グループの制限を超えてUNIXユーザグループメンバーシップのサポートを拡張する場合は、このオプションを選択しないでください。ただし、拡張グループを使用するには、UNIX ID用のLDAPサーバを設定する必要があります。LDAPサーバがない場合は、このオプションを選択しないでください。LDAPサーバがあり、ローカルUNIXユーザ（rootなど）も使用する場合は、このオプションを選択します。

バックアップユーザ

このオプションを使用すると、Cloud Volumes Service ボリュームに対するバックアップ権限を持つWindowsユーザを指定できます。一部のアプリケーションでNASボリュームのデータを正しくバックアップおよびリストアするには、バックアップ権限（SeBackupPrivilege）が必要です。このユーザにはボリューム内のデータへのアクセスレベルが高いため、考慮する必要があります "そのユーザアクセスの監査を有効にします"。有効にすると、Event Viewer > Windows Logs > Securityに監査イベントが表示されます。



セキュリティ権限ユーザ

このオプションを使用すると、Cloud Volumes Service ボリュームに対するセキュリティの変更権限を持つWindowsユーザを指定できます。一部のアプリケーションにはセキュリティ権限（SeSecurityPrivilege）が必要です (*たとえば、SQL Serverなどです*)を使用して、インストール時に権限を適切に設定します。この権限は、セキュリティログを管理するために必要です。この権限はSeBackupPrivilegeほど強力ではありませんが、ネットアップでは推奨しています *ユーザのユーザアクセスを監査する* 必要に応じて、この権限レベルで設定します。

詳細については、を参照してください *新しいログオンに割り当てられた特別な権限*。

Active Directoryでの**Cloud Volumes Service** の表示

Active Directoryでは、通常のマシンアカウントオブジェクトとしてCloud Volumes Service が表示されます。命名規則は次のとおりです。

- CIFS/SMBおよびNFS Kerberosでは、個別のマシンアカウントオブジェクトが作成されます。
- NFSでLDAPが有効になっている場合、Kerberos LDAPバインド用にActive Directoryにマシンアカウントが作成されます。
- LDAPを使用したデュアルプロトコルボリュームでは、LDAPとSMBのCIFS / SMBマシンアカウントが共有されます。
- CIFS / SMBマシンアカウントでは、マシンアカウントの名前付け規則として、name-1234（ランダムな4桁のIDに10文字未満の名前をハイフンで付加）を使用します。Active Directory接続では、NetBIOS名の設

定で名前を定義できます（「」を参照）Active Directory接続の詳細」）をクリックします。

- NFS Kerberosでは、命名規則としてnfs-name-1234を使用します（最大15文字）。15文字を超える文字が使用されている場合、名前はnfs-truncated-name-1234になります。
- NFSのみのCVS - LDAPが有効なパフォーマンスインスタンスは、CIFS / SMBインスタンスと同じ命名規則を使用してLDAPサーバにバインドするためのSMBマシンアカウントを作成します。
- SMBマシンアカウントを作成すると、デフォルトの非表示の管理共有が表示されます（を参照） "「デフォルトの非表示共有」"）も作成されます（c$、admin$、ipc$）が、ACLが割り当てられておらず、アクセスできない共有です。
- マシンアカウントオブジェクトはデフォルトではCN=Computersに配置されますが、必要に応じて別のOUを指定できます。「」を参照してくださいSMBマシンアカウントの作成に必要な権限「Cloud Volumes Service のマシンアカウントオブジェクトを追加または削除するために必要なアクセス権については、を参照してください。

Cloud Volumes Service によってSMBマシンアカウントがActive Directoryに追加されると、次のフィールドが設定されます。

- CN（指定したSMBサーバ名を使用）
- dNSHostName（SMBserver.domain.comを使用）
- msDs-SupportedEncryptionTypes（AES暗号化が有効でない場合は、DES-CBC_MD5、RC4_HMAC_MD5を許可します。AES暗号化が有効の場合は、DES-CBC_MD5、RC4_HMAC_MD5、AES128_CTS_HMAC_SHA1、AES256_CTC_HMAC_SHA1 96を許可します）
- 名前（SMBサーバ名を使用）
- sAMAccountName（SMBserver$を使用）
- servicePrincipalName（Kerberosのホスト/ smbserver.domain.comおよびホスト/ smbserver SPNを使用）

マシンアカウントで弱いKerberos暗号化タイプ(enctype)を無効にする場合は、マシンアカウントのmsDS-SupportedEncryptionTypes値を次の表のいずれかの値に変更してAESのみを許可することができます。

msDs-SupportedEncryptionTypesの値	暗号化タイプが有効です
2.	des_cbc_md5
4.	RC4_HMAC
8.	AES128_CTS_HMAC_SHA1 96のみ
16	AES256_CTS_HMAC_SHA1_96のみ
24	AES128_CTS_HMAC_SHA1_96およびAES256_CTS_HMAC_SHA1_96です
30	DES_CBC_MD5、RC4_HMAC、AES128_CTS_HMAC_SHA1 96およびAES256_CTS_HMAC_SHA1 96

SMBマシンアカウントのAES暗号化を有効にするには、Active Directory接続の作成時にAD認証のAES暗号化を有効にするをクリックします。

NFS KerberosのAES暗号化を有効にするには、 "Cloud Volumes Service のドキュメントを参照してください"。

その他の**NAS**インフラストラクチャサービスの依存関係（**KDC**、**LDAP**、および**DNS**）

NAS共有にCloud Volumes Service を使用する場合は、正常に機能するために外部との依存関係が必要になることがあります。これらの依存関係は、特定の状況下で有効になっています。次の表に、さまざまな設定オプションと、必要な依存関係を示します。

設定	必須の依存関係です
NFSv3のみ	なし
NFSv3 Kerberosのみ	Windows Active Directory：* KDC * DNS * LDAP
NFSv4.1のみ	クライアントIDマッピング設定（/etc/idmap.conf）
NFSv4.1 Kerberosのみ	• クライアントIDマッピング設定（/etc/idmap.conf） • Windows Active Directory：KDC DNS LDAP
SMBのみ	Active Directory：* KDC * DNS
マルチプロトコルのNAS（NFSおよびSMB）	• クライアントIDマッピングの設定（NFSv4.1のみ、/etc/idmap.conf） • Windows Active Directory：KDC DNS LDAP

マシンアカウントオブジェクトの**Kerberos keytab**のローテーション/パスワードがリセットされます

SMBマシンアカウントの場合、Cloud Volumes Service はSMBマシンアカウントのパスワードリセットを定期的にスケジュールします。これらのパスワードはKerberos暗号化を使用してリセットされ、毎週日曜日の午後11時から午前1時までのランダムな時刻にスケジュールされます。これらのパスワードは、Kerberosキーのバージョンをリセットし、Cloud Volumes Service システムに格納されているキータブをローテーションし、Cloud Volumes Service で実行されるSMBサーバのセキュリティを強化するのに役立ちます。マシンアカウントのパスワードはランダム化され、管理者には知られていません。

NFS Kerberosマシンアカウントの場合、パスワードのリセットは、新しいkeytabが作成され、KDCと交換されたときにのみ行われます。現在、Cloud Volumes Service では実行できません。

LDAPおよび**Kerberos**で使用するネットワークポート

LDAPおよびKerberosを使用する場合は、これらのサービスで使用されているネットワークポートを確認する必要があります。Cloud Volumes Service で使用されているすべてのポートの一覧については、を参照してください "セキュリティに関する考慮事項についてのCloud Volumes Service のドキュメント"。

LDAP

Cloud Volumes Service はLDAPクライアントとして機能し、UNIX IDのユーザおよびグループ検索に標準のLDAP検索クエリを使用します。Cloud Volumes Service が提供する標準のデフォルトユーザ以外のユーザとグループを使用する場合は、LDAPが必要です。また、ユーザプリンシパル（user1@domain.comなど）でNFS Kerberosを使用する場合も、LDAPが必要です。現在、Microsoft Active Directoryを使用するLDAPのみがサポートされています。

Active DirectoryをUNIX LDAPサーバとして使用するには、UNIX IDに使用するユーザおよびグループに、必要なUNIX属性を設定する必要があります。Cloud Volumes Service では、に基づいて属性を照会するデフォルト

のLDAPスキーマテンプレートが使用されます "RFC-2307 -bis"。このため、次の表に、ユーザとグループにデータを入力するために最低限必要なActive Directory属性と、それぞれの属性がどのような目的で使用されているかを示します。

Active DirectoryでのLDAP属性の設定の詳細については、を参照してください "デュアルプロトコルアクセスの管理"

属性	機能
UID *	UNIXユーザ名を指定します
uidNumber *	UNIXユーザの数値IDを指定します
gidNumber *	UNIXユーザのプライマリグループの数値IDを指定します
objectclass *	使用するオブジェクトのタイプを指定します。Cloud Volumes Service では、オブジェクトクラスのリストに「user」を含める必要があります（デフォルトではほとんどのActive Directory展開に含まれています）。
名前	アカウントに関する一般的な情報（実際の名前、電話番号など、「gecos」とも呼ばれる）
unixUserPassword	これを設定する必要はありません。NAS認証のUNIX ID検索では使用されません。設定すると、設定されたunixUserPasswordの値がプレーンテキストになります。
unixHomeDirectory	ユーザがLinuxクライアントからLDAPに照らして認証する場合のUNIXホームディレクトリへのパスを定義します。UNIXホームディレクトリの機能にLDAPを使用する場合は、このオプションを設定します。
loginShellの略	ユーザがLDAPに対して認証を行うときに、Linuxクライアントのbash/profileシェルへのパスを定義します。

*は、Cloud Volumes Service で適切に機能するために属性が必要であることを示します。残りの属性はクライアント側でのみ使用します。

属性	機能
CN *	UNIXグループ名を指定します。LDAPでActive Directoryを使用する場合は、オブジェクトの作成時に設定されますが、あとで変更することもできます。この名前を他のオブジェクトと同じにすることはできません。たとえば、user1という名前のUNIXユーザがLinuxクライアント上のuser1という名前のグループに属している場合、Windowsでは、同じcn属性を持つ2つのオブジェクトは許可されません。これを回避するには、Windowsユーザの名前を一意の名前（user1やunixなど）に変更します。Cloud Volumes Service のLDAPでは、UNIXユーザ名にuid属性を使用します。
gidNumber *	UNIXグループの数値IDを指定します。

属性	機能
objectclass *	使用するオブジェクトのタイプを指定します。Cloud Volumes Service では、オブジェクトクラスのリストにグループを含める必要があります（この属性はデフォルトでほとんどのActive Directory展開に含まれています）。
memberUid	UNIXグループのメンバーであるUNIXユーザを指定します。Cloud Volumes Service のActive Directory LDAPでは、このフィールドは必要ありません。Cloud Volumes Service LDAPスキーマでは、グループメンバーシップにMemberフィールドを使用します。
メンバー*	グループメンバーシップ/セカンダリUNIXグループに必要です。このフィールドには、WindowsユーザをWindowsグループに追加します。ただし、WindowsグループにUNIX属性が入力されていない場合、UNIXユーザのグループメンバーシップリストには含まれません。NFSで使用できる必要があるグループは、次の表に示す必要なUNIXグループ属性を設定する必要があります。

*は、Cloud Volumes Service で適切に機能するために属性が必要であることを示します。残りの属性はクライアント側でのみ使用します。

LDAPバインド情報

LDAPでユーザを照会するには、Cloud Volumes Service がLDAPサービスにバインド（ログイン）する必要があります。このログインには読み取り専用権限があり、LDAP UNIX属性を照会してディレクトリを検索するために使用されます。現在のところ、LDAPバインドはSMBマシンアカウントを使用した場合にのみ可能です。

LDAPを有効にできるのは「CVS -パフォーマンス」インスタンスのみで、NFSv3、NFSv4.1、またはデュアルプロトコルボリュームでのみです。LDAP対応ボリュームを導入するには、Cloud Volumes Service ボリュームと同じリージョンにActive Directory接続を確立する必要があります。

LDAPを有効にすると、特定の状況で次のような状況が発生します。

- Cloud Volumes Service プロジェクトにNFSv3またはNFSv4.1のみを使用する場合は、Active Directoryドメインコントローラに新しいマシンアカウントが作成され、Cloud Volumes Service 内のLDAPクライアントはマシンアカウントのクレデンシャルを使用してActive Directoryにバインドします。NFSボリュームおよびデフォルトの非表示の管理共有用にSMB共有は作成されません（を参照） "「デフォルトの非表示共有」"）共有ACLを削除しておきます。
- Cloud Volumes Service プロジェクトにデュアルプロトコルボリュームを使用する場合は、SMBアクセス用に作成された1つのマシンアカウントのみを使用して、Cloud Volumes Service のLDAPクライアントがActive Directoryにバインドされます。追加のマシンアカウントは作成されません。
- 専用のSMBボリュームを個別に作成する場合（LDAPを使用するNFSボリュームの有効化前と無効化後）、LDAPバインド用マシンアカウントはSMBマシンアカウントと共有されます。
- NFS Kerberosも有効になっている場合は、2つのマシンアカウントが作成されます。1つはSMB共有またはLDAPバインド用、もう1つはNFS Kerberos認証用です。

LDAPクエリ

LDAPバインドは暗号化されますが、LDAPクエリは共通のLDAPポート389を使用してプレーンテキストでワイヤ経由で渡されます。この既知のポートは、現在Cloud Volumes Service では変更できません。その結果、ネットワーク内のパケットスニファにアクセスできるユーザは、ユーザ名、グループ名、数値ID、およびグループメンバーシップを確認できます。

ただし、Google Cloud VMは他のVMのユニキャストトラフィックをスニファできません。LDAPトラフィックにアクティブに参加している（バインド可能な）VMのみが、LDAPサーバからのトラフィックを表示できます。Cloud Volumes Service でのパケットスニファの詳細については、を参照してください "「パケットのスニッフィング/トレースに関する考慮事項」"

LDAPクライアント設定のデフォルト

Cloud Volumes Service インスタンスでLDAPを有効にすると、デフォルトで特定の設定の詳細を使用してLDAPクライアント設定が作成されます。場合によっては、オプションがCloud Volumes Service に適用されない（サポートされない）か、設定できないことがあります。

LDAPクライアントオプション	機能	デフォルト値	変更は可能ですか？
LDAPサーバリスト	クエリに使用するLDAPサーバ名またはIPアドレスを設定します。これはCloud Volumes Service では使用されません。代わりに、Active Directoryドメインを使用してLDAPサーバを定義します。	未設定	いいえ
Active Directoryドメイン	LDAPクエリに使用するActive Directoryドメインを設定します。Cloud Volumes Service は、DNSのLDAPのSRVレコードを利用して、ドメイン内のLDAPサーバを検索します。	Active Directory接続で指定されているActive Directoryドメインに設定します。	いいえ
優先されるActive Directoryサーバ	LDAPで使用する優先Active Directoryサーバを設定します。Cloud Volumes Service ではサポートされていません。代わりに、Active Directoryサイトを使用してLDAPサーバの選択を制御します。	未設定。	いいえ
SMBサーバクレデンシャルを使用してバインド	SMBマシンアカウントを使用してLDAPにバインドします。現在、Cloud Volumes Service でサポートされているLDAPバインド方式はのみです。	正しいです	いいえ

LDAPクライアントオプション	機能	デフォルト値	変更は可能ですか？
スキーマテンプレート	LDAPクエリに使用するスキーマテンプレート。	MS-AD-BIS を参照してください	いいえ
LDAPサーバポート	LDAPクエリに使用するポート番号。Cloud Volumes Service では現在、標準のLDAPポート389のみが使用されています。LDAPS /ポート636は、現在サポートされていません。	389	いいえ
LDAPSが有効になっています	LDAP over Secure Sockets Layer（SSL）をクエリおよびバインドに使用するかどうかを制御します。現在、Cloud Volumes Service ではサポートされていません。	いいえ	いいえ
クエリタイムアウト（秒）	クエリがタイムアウトしました。クエリに指定した値よりも長い時間がかかると、クエリが失敗します。	3.	いいえ
最小バインド認証レベル	サポートされる最小バインドレベルを指定します。Cloud Volumes Service はLDAPバインドにマシンアカウントを使用し、デフォルトではActive Directoryは匿名バインドをサポートしないため、このオプションはセキュリティ上の理由から有効になりません。	匿名	いいえ
バインド DN	シンプルバインドが使用されている場合にバインドに使用されるユーザ/識別名（DN）。Cloud Volumes Service は、LDAPバインドにマシンアカウントを使用しますが、現在のところ単純なバインド認証はサポートしていません。	未設定	いいえ
ベースDN	LDAP検索に使用するベースDN。	Active Directory接続に使用するWindowsドメイン（DN形式）（DC=domain、DC=local）	いいえ

LDAPクライアントオプション	機能	デフォルト値	変更は可能ですか？
ベースの検索範囲	ベースDN検索の検索範囲。値には、base、onelevel、subtreeのいずれかを指定できます。Cloud Volumes Service ではサブツリー検索のみがサポートされます。	サブツリー	いいえ
ユーザDN	ユーザがLDAPクエリの検索を開始するDNを定義します。現在Cloud Volumes Service ではサポートされていないため、すべてのユーザ検索はベースDNから開始されます。	未設定	いいえ
ユーザの検索範囲	ユーザDN検索の検索範囲。値には、base、onelevel、subtreeのいずれかを指定できます。Cloud Volumes Service では、ユーザ検索範囲の設定はサポートされていません。	サブツリー	いいえ
グループDN	グループ検索でLDAPクエリが開始されるDNを定義します。現在Cloud Volumes Service ではサポートされていないため、すべてのグループ検索はベースDNから開始されます。	未設定	いいえ
グループの検索範囲	グループDN検索の検索範囲。値には、base、onelevel、subtreeのいずれかを指定できます。Cloud Volumes Service では、グループ検索範囲の設定はサポートされていません。	サブツリー	いいえ
ネットグループDN	ネットグループ検索でLDAPクエリの開始に使用するDNを定義します。現在Cloud Volumes Service ではサポートされていないため、ネットグループ検索はすべてベースDNから開始されます。	未設定	いいえ

LDAPクライアントオプション	機能	デフォルト値	変更は可能ですか？
ネットグループ検索範囲	ネットグループDN検索の検索範囲。値には、base、onelevel、subtreeのいずれかを指定できます。Cloud Volumes Service では、ネットグループ検索範囲の設定はサポートされていません。	サブツリー	いいえ
LDAPでstart_tlsを使用します	Start TLSを使用して、証明書ベースのLDAP接続をポート389経由で行います。現在、Cloud Volumes Service ではサポートされていません。	いいえ	いいえ
ホスト単位のネットグループ検索を有効にします	ネットグループをすべてのメンバーの一覧に展開するのではなく、ホスト名によるネットグループ検索を有効にします。現在、Cloud Volumes Service ではサポートされていません。	いいえ	いいえ
ホスト単位のネットグループDN	ホスト単位のネットグループ検索がLDAPクエリを開始するDNを定義します。ホスト単位のネットグループは、現在Cloud Volumes Service ではサポートされていません。	未設定	いいえ
ホスト単位のネットグループ検索範囲	ホスト単位のネットグループDN検索の検索範囲。値には、base、onelevel、subtreeのいずれかを指定できます。ホスト単位のネットグループは、現在Cloud Volumes Service ではサポートされていません。	サブツリー	いいえ

LDAPクライアントオプション	機能	デフォルト値	変更は可能ですか？
クライアントセッションのセキュリティ	LDAPで使用されるセッションセキュリティのレベルを定義します（sign、seal、none）。LDAP署名は、Active Directoryから要求された場合にCVSパフォーマンスでサポートされます。CVS-SWではLDAP署名はサポートされません。どちらのタイプのサービスでも、現時点ではシーリングはサポートされていません。	なし	いいえ
LDAPリファーラルキャッシュ	複数のLDAPサーバを使用している場合、リファーラル追跡を使用すると、クライアントが最初のサーバでエントリが見つからなかったときに、リスト内の他のLDAPサーバを参照することができます。これは現在、Cloud Volumes Service ではサポートされていません。	いいえ	いいえ
グループメンバーシップフィルタ	LDAPサーバからグループメンバーシップを検索するときに使用するカスタムのLDAP検索フィルタを提供します。Cloud Volumes Service では現在サポートされていません。	未設定	いいえ

LDAPを使用した非対称ネームマッピング

デフォルトでは、Cloud Volumes Service は、WindowsユーザとUNIXユーザを、特別な設定なしで双方向に同一のユーザ名でマッピングします。有効なUNIXユーザ（LDAPを使用）がCloud Volumes Service で検出されると、1：1のネームマッピングが発生します。たとえば、Windowsユーザjohnsmithが使用されている場合、Cloud Volumes Service がLDAPで「johnsmith」という名前のUNIXユーザを検索できた場合、そのユーザのネームマッピングは成功し、「johnsmith」によって作成されたすべてのファイルおよびフォルダに正しいユーザ所有権が表示されます。 また'johnsmithに影響を与えるすべてのACLは'NASプロトコルの使用に関係なく使用されますこれは対称ネームマッピングと呼ばれます。

非対称ネームマッピングは、WindowsのユーザIDとUNIXのユーザIDが一致しない場合に使用します。たとえば'WindowsユーザjohnsmithがUNIX IDがjsmithの場合'UNIXのバリエーションをCloud Volumes Service に通知する必要がありますCloud Volumes Service は現在、静的なネームマッピングルールの作成をサポートしていないため、ファイルとフォルダの適切な所有権と予期される権限を確保するために、LDAPを使用してWindows IDとUNIX IDの両方のユーザのIDを検索する必要があります。

デフォルトでは、Cloud Volumes Service のネームマップデータベースのインスタンスのns-switchに「ldap」

が含まれているため、非対称名にLDAPを使用してネームマッピング機能を提供するために必要なのは、Cloud Volumes Service の検索内容を反映するためにユーザ/グループの属性の一部のみです。

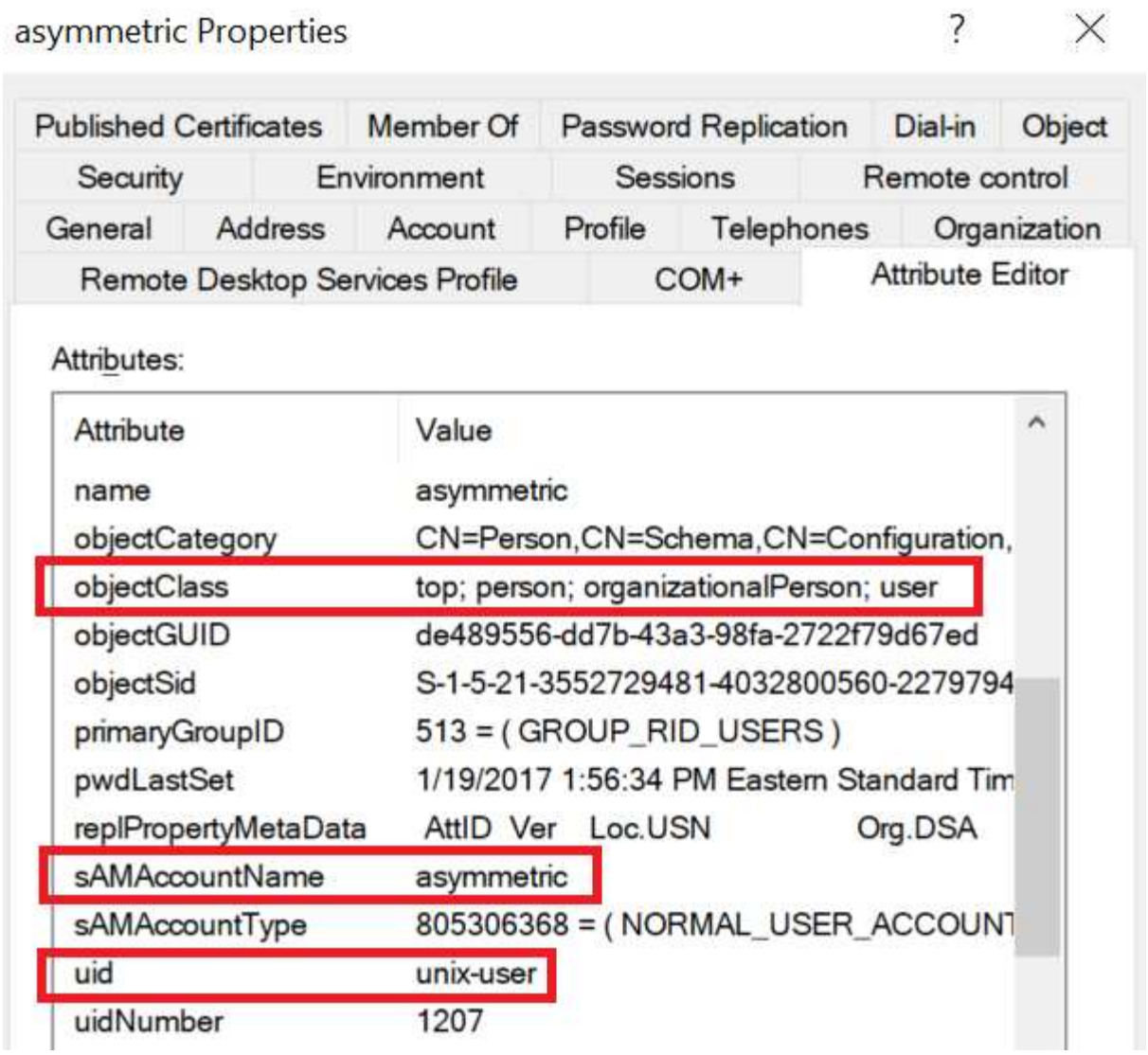
次の表に、非対称ネームマッピング機能のためにLDAPに入力する必要がある属性を示します。ほとんどの場合、Active Directoryはすでに設定されています。

Cloud Volumes Service 属性	機能	**Cloud Volumes Service** がネームマッピングに使用する値
WindowsからUNIX objectClass	使用するオブジェクトのタイプを指定します。（ユーザ、グループ、posixAccountなど）	userを含める必要があります（必要に応じて、他の値を複数含めることもできます）。
WindowsからUNIXへの属性	作成時にWindowsユーザ名を定義します。Cloud Volumes Service では、これをWindowsからUNIXへのルックアップに使用します。	ここでは変更は必要ありません。sAMAccountNameはWindowsログイン名と同じです。
UID	UNIXユーザ名を定義します。	必要なUNIXユーザ名。

Cloud Volumes Service では現在、LDAP検索でドメインプレフィックスが使用されないため、LDAPネームマップ検索で複数のドメインLDAP環境が正常に機能しません。

次の例は、Windows名が「asymmetric」で、UNIX名が「unix-user」で、SMBとNFSの両方からファイルを書き込む際の動作を示しています。

次の図に、LDAP属性がWindowsサーバからどのように見えているかを示します。



NFSクライアントからは、UNIX名を照会できますが、Windows名は照会できません。

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

ファイルがNFSから「unix-user」として書き込まれると、NFSクライアントから次のような結果になります。

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

Windowsクライアントでは、ファイルの所有者が適切なWindowsユーザに設定されていることを確認できます。

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

逆に、WindowsユーザがSMBクライアントから「asymmetric」で作成したファイルの場合、次のテキストに示すように、適切なUNIX所有者が表示されます。

SMB：

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS ：

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

LDAPチャネルバインド

Windows Active Directoryドメインコントローラの脆弱性により、 "マイクロソフトセキュリティアドバイザリADV190023" DCによるLDAPバインドの許可方法を変更します。

Cloud Volumes Service による影響は、どのLDAPクライアントでも同じです。Cloud Volumes Service では現在、チャネルバインドはサポートされていません。Cloud Volumes Service はネゴシエーションを通じてデフォルトでLDAP署名をサポートしているため、LDAPチャネルバインドを問題 にすることはできません。チャネルバインドが有効な状態でLDAPにバインドする問題がある場合は、「ADV190023」の修正手順に従って、Cloud Volumes Service からのLDAPバインドを成功させるようにしてください。

DNS

Active DirectoryとKerberosはどちらも、ホスト名からIP / IPを経由したホスト名解決で、DNSに依存します。DNSでは、ポート53を開く必要があります。Cloud Volumes Service では、DNSレコードに変更を加えたり、現在のところの使用をサポートしていません "動的DNS" ネットワークインターフェイス。

Active Directory DNSを設定して、DNSレコードを更新できるサーバを制限できます。詳細については、を参照してください "Windows DNSを保護"。

Googleプロジェクト内のリソースは、既定ではGoogle Cloud DNSを使用しますが、Active Directory DNSには接続されていません。クラウドDNSを使用するクライアントは、Cloud Volumes Service から返されたUNCパスを解決できません。Active Directoryドメインに参加しているWindowsクライアントは、Active Directory DNSを使用するように設定され、このようなUNCパスを解決できます。

クライアントをActive Directoryに参加させるには、Active Directory DNSを使用するようにそのDNS設定を構成する必要があります。必要に応じて、Active Directory DNSに要求を転送するようにCloud DNSを設定することができます。を参照してください "クライアントでSMB NetBIOS名を解決できないのはなぜですか？"を参照してください。

Cloud Volumes Service は現在DNSSECをサポートしておらず、DNSクエリはプレーンテキストで実行されます。

ファイルアクセスの監査

現在、Cloud Volumes Service ではサポートされていません。

アンチウイルスによる保護

Cloud Volumes Service で、クライアントからNAS共有へのウィルススキャンを実行する必要があります。現在のところ、Cloud Volumes Service とウィルス対策はネイティブで統合されていません。

サービスの処理

Cloud Volumes Service チームはGoogle Cloudでバックエンドサービスを管理し、複数の戦略を使用してプラットフォームを保護し、不要なアクセスを防止します。

お客様ごとに固有のサブネットが割り当てられ、デフォルトで他のお客様から遮断されたアクセス権が付与される。Cloud Volumes Service の各テナントは、データを完全に分離するために独自のネームスペースとVLANを取得する。ユーザが認証されると、Service Delivery Engine（SDE；サービス提供エンジン）はそのテナントに固有の設定データのみを読み取ることができます。

物理的セキュリティ

事前承認が必要な場合、ケージとラックにアクセスできるのは、オンサイトエンジニアとネットアップ認定のフィールドサポートエンジニア（FSE）のみです。ストレージとネットワークの管理は許可されていません。ハードウェアのメンテナンス作業を実行できるのは、これらのオンサイトリソースのみです。

オンサイトエンジニアの場合は、作業仕様書（SOW）のチケットが発行されます。この作業内容には、ラックIDとデバイスの場所（RU）、その他すべての詳細情報が含まれます。NetApp FSEの場合、サイト訪問チケットはColoで発行する必要があります。チケットには、監査を目的とした訪問者の詳細、日付、時刻が含まれています。FSEのSOWは、社内でネットアップに通知されます。

運用チーム

Cloud Volumes Service の運用チームは、クラウドボリュームサービス向けの生産エンジニアリングとサイト信頼性エンジニア（SRE）、およびハードウェア向けのネットアップフィールドサポートエンジニアとパートナーで構成されています。すべての運用チームメンバーは、Google Cloudでの作業が認定されており、発行されたチケットごとに詳細な作業記録が保持されています。また、各意思決定が適切に精査されるように、厳格な変更管理および承認プロセスが用意されています。

SREチームは、コントロールプレーンと、UI要求からCloud Volumes Service のバックエンドハードウェアおよびソフトウェアにデータをルーティングする方法を管理します。SREチームは、ボリュームやinodeの最大数などのシステムリソースも管理します。SREは、カスタマーデータとやり取りしたり、カスタマーデータにアクセスしたりすることはできません。SREは、バックエンドハードウェアに対する新しいディスク交換要求やメモリ交換要求などのReturn Material Authorizations（RMA）との調整も行います。

お客様の責任

Cloud Volumes Service のお客様は、組織のActive Directoryとユーザーの役割管理だけでなく、ボリュームとデータの操作も管理します。お客様は管理者ロールを割り当てられ、ネットアップとGoogle Cloudが提供する2つの事前定義されたロール（管理者とビューア）を使用して、同じGoogle Cloudプロジェクト内の他のエンドユーザに権限を委譲できます。

管理者は、お客様のプロジェクト内の任意のVPCを、お客様が適切と判断したCloud Volumes Service にピアリングできます。Google Cloud Marketplaceサブスクリプションへのアクセスの管理、およびデータプレーンへのアクセス権を持つVPCの管理は、お客様の責任において行ってください。

悪意のある**SRE**保護

Cloud Volumes Service は、悪意のあるSREが存在するシナリオやSRE資格情報が侵害された場合に、どのように保護するのかという懸念事項があります。

本番環境へのアクセスには、限られた数のSRE担当者のみが使用されます。管理者権限は、経験豊富な一部の管理者にも制限されています。Cloud Volumes Service の運用環境で実行されるすべてのアクションは記録され、ベースラインまたは疑わしいアクティビティへの異常は、セキュリティ情報およびイベント管理（SIEM）脅威インテリジェンスプラットフォームによって検出されます。その結果、悪意のあるアクションを追跡し、Cloud Volumes Service バックエンドに過剰な損害が発生する前に軽減することができます。

ボリュームのライフサイクル

Cloud Volumes Service は、サービス内のオブジェクトのみを管理し、ボリューム内のデータは管理しません。データ、ACL、ファイル所有者などを管理できるのは、ボリュームにアクセスしているクライアントだけです。これらのボリューム内のデータは保存中も暗号化され、Cloud Volumes Service インスタンスのテナントのみにアクセスできます。

Cloud Volumes Service のボリュームライフサイクルはcreate-update-deleteです。ボリュームは、ボリュームが削除されるまでボリュームのSnapshotコピーを保持します。Cloud Volumes Service 内のボリュームを削除できるのは、検証済みのCloud Volumes Service 管理者だけです。管理者がボリューム削除を要求した場合、削除の確認のためにボリューム名を入力する手順が追加で必要になります。ボリュームを削除すると、そのボリュームは削除され、リカバリできなくなります。

Cloud Volumes Service 契約を終了した場合、ネットアップは特定の期間が経過したボリュームに削除マークを付けます。この期間が終了する前に、お客様の要求に応じてボリュームをリカバリできます。

認定資格

Google Cloud向けCloud Volume サービスは、現在ISO/IEC 27001：2013およびISO/IEC 27018：2019規格に準拠しています。サービスは最近、SOC2 Type Iアテステーションレポートを受信しました。ネットアップのデータ セキュリティ への取り組みとプライバシーに関する詳細については、を参照してください "コンプライアンス：データ セキュリティ とデータプライバシー"。

GDPR

プライバシーに対する当社のコミットメントとGDPRへの準拠は、当社のさまざまな方法で提供されています "お客様との契約"などです "カスタマーデータ処理補遺"が含まれます "標準契約条項" 欧州委員会が提供します。また、当社のプライバシーポリシーには、当社の企業行動規範に規定されている中核的な価値観に裏付けられたこれらのコミットメントを定めています。

このドキュメントに記載されている情報の詳細については、以下のドキュメントや Web サイトを参照してください。

- Cloud Volumes Service 向けGoogle Cloudドキュメント

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes/"

- Googleプライベートサービスへのアクセス

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- ネットアップの製品マニュアル

  "https://www.netapp.com/support-and-training/documentation/"

- 暗号化検証モジュールプログラム—NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- 『NetApp解決策 for Ransomware』

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- TR-4616 ：『 NFS Kerberos in ONTAP 』

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

お問い合わせください

本テクニカルレポートの品質向上について、ご意見をお寄せください。

mailto：doccomments@netapp.com [doccomments@netapp.com ^]までお問い合わせください。件名にはテクニカルレポート4918を含めてください。

BlueXPのバックアップとリカバリ

BlueXPによるVMのバックアップとリカバリ

3-2-1 SnapCenterプラグインとBlueXPによるVMのバックアップとリカバリによるVMwareのデータ保護

作成者：Josh Powell -ネットアップソリューションエンジニアリングチーム

概要

3-2-1バックアップ戦略は、業界で受け入れられているデータ保護方法であり、重要なデータを保護するための包括的なアプローチを提供します。 この戦略は信頼性が高く、予期せぬ災害が発生した場合でも、データのコピーを確実に利用できるようにします。

この戦略は、次の3つの基本ルールで構成されています。

1. データのコピーを3つ以上保持します。これにより、1つのコピーが失われたり破損したりしても、フォールバックするコピーが少なくとも2つ残っています。
2. 2つのバックアップコピーを別 々 のストレージメディアまたはデバイスに保存します。ストレージメディアの多様化は、デバイス固有またはメディア固有の障害からの保護に役立ちます。一方のデバイスが破損したり、一方のタイプのメディアに障害が発生したりしても、もう一方のバックアップコピーは影響を受けません。
3. 最後に、少なくとも1つのバックアップコピーがオフサイトにあることを確認します。オフサイトストレージは、火災や洪水などの局地的な災害に対してフェイルセーフとして機能し、オンサイトのコピーを使用できなくなる可能性があります。

この解決策ドキュメントでは、SnapCenter Plug-in for VMware vSphere（SCV）を使用してオンプレミスの仮想マシンのプライマリとセカンダリのバックアップを作成する3-2-1バックアップ解決策と、データのコピーをクラウドストレージまたはStorageGRIDにバックアップするための仮想マシンのBlueXPバックアップとリカバリについて説明します。

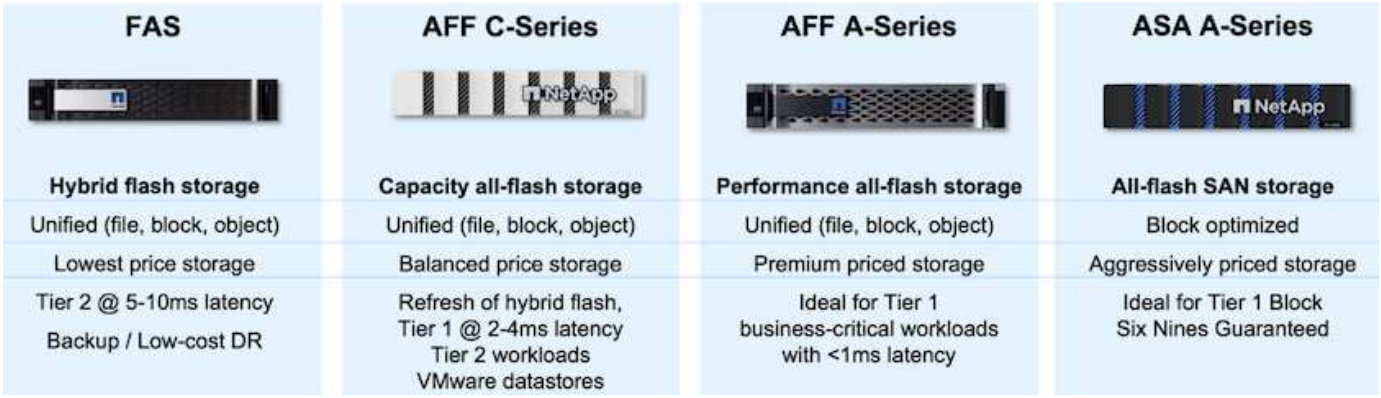
ユースケース

この解決策 は、次のユースケースに対応します。

- SnapCenter Plug-in for VMware vSphereを使用した、オンプレミスの仮想マシンおよびデータストアのバックアップとリストア
- ONTAPクラスタでホストされているオンプレミスの仮想マシンとデータストアのバックアップとリストア、および仮想マシンのBlueXPバックアップ/リカバリを使用したオブジェクトストレージへのバックアップ。

NetApp ONTAPデータストレージ

ONTAPは、業界をリードするネットアップのストレージ解決策で、SANプロトコルとNASプロトコルのどちらでアクセスしてもユニファイドストレージを提供します。3-2-1バックアップ戦略により、オンプレミスのデータが複数のメディアタイプで確実に保護されます。NetAppは、高速フラッシュから低コストのメディアまで、さまざまなプラットフォームを提供します。



ネットアップのすべてのハードウェアプラットフォームの詳細については、 "NetAppデータストレージ"。

SnapCenter Plug-in for VMware vSphere

SnapCenter Plug-in for VMware vSphereは、VMware vSphereと緊密に統合されたデータ保護ソリューションであり、仮想マシンのバックアップとリストアを簡単に管理できます。この解決策の一部として、SnapMirrorは、仮想マシンのデータの書き換え不可能な2つ目のバックアップコピーを、セカンダリONTAPストレージク

ラスタに高速かつ信頼性の高い方法で作成します。このアーキテクチャを導入すると、プライマリまたはセカンダリバックアップのどちらからでも、仮想マシンのリストア処理を簡単に開始できます。

SCVは、OVAファイルを使用してLinux仮想アプライアンスとして導入されます。プラグインでリモートプラグインが使用されるようになりました。
アーキテクチャ：リモートプラグインはvCenterサーバの外部で実行され、SCV仮想アプライアンスでホストされます。

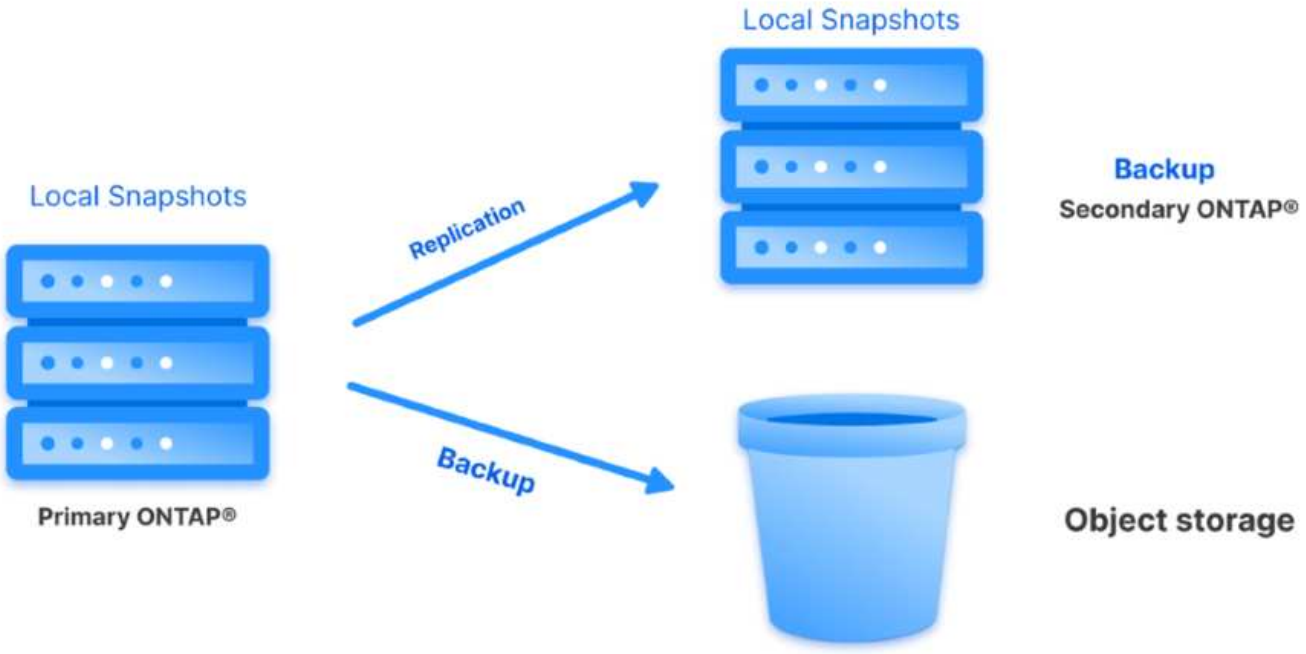
SCVの詳細については、を参照してください。 "SnapCenter Plug-in for VMware vSphere のドキュメント"。

BlueXPによる仮想マシンのバックアップとリカバリ

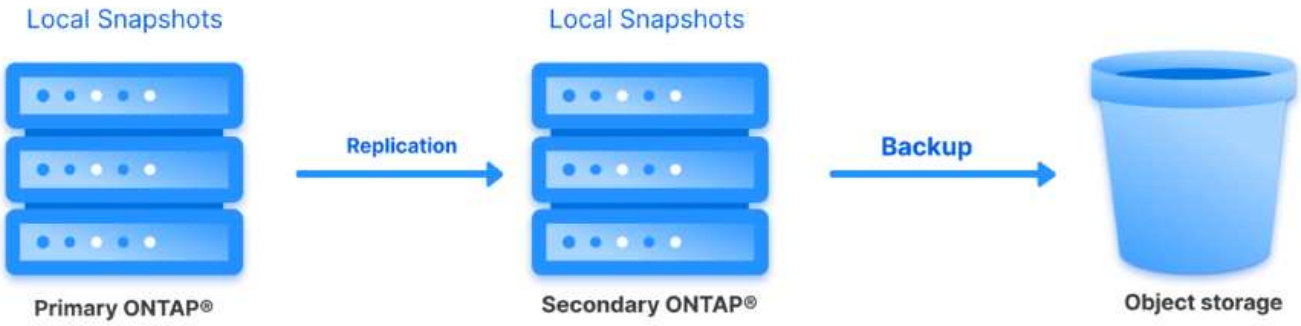
BlueXPのバックアップとリカバリは、クラウドベースのデータ管理ツールです。オンプレミス環境とクラウド環境の両方で、幅広いバックアップとリカバリの処理を単一のコントロールプレーンで実行できます。NetApp BlueXPのバックアップ/リカバリスイートに含まれる機能は、SnapCenter Plugin for VMware vSphere（オンプレミス）と統合して、データのコピーをクラウド上のオブジェクトストレージに拡張することができます。これにより、プライマリストレージまたはセカンダリストレージのバックアップからソースとなるデータの3つ目のコピーがオフサイトに作成されます。BlueXPのバックアップとリカバリでは、2つのオンプレミス環境のどちらかからデータのコピーを転送するストレージポリシーを簡単に設定できます。

BlueXPのバックアップとリカバリでソースとしてプライマリバックアップとセカンダリバックアップのどちらかを選択すると、次の2つのトポロジのいずれかが実装されます。

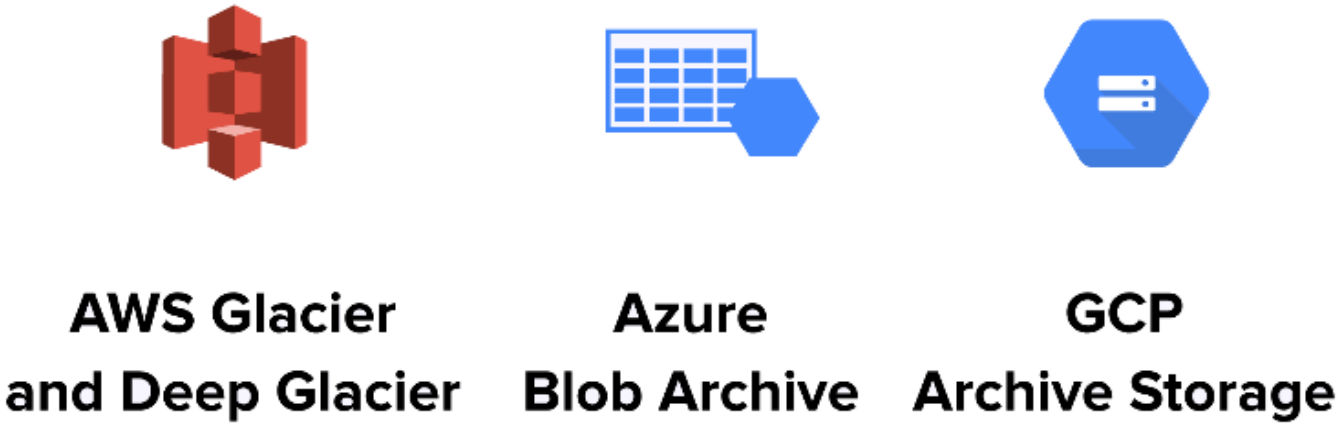
ファンアウトトポロジ–SnapCenter Plug-in for VMware vSphereによってバックアップが開始されると、ローカルスナップショットが即座に作成されます。次に、最新のSnapshotをセカンダリONTAPクラスタにレプリケートするSnapMirror処理を開始します。BlueXPのバックアップとリカバリでは、ポリシーによって、選択したクラウドプロバイダのオブジェクトストレージにデータのSnapshotコピーを転送するソースとしてプライマリONTAPクラスタが指定されます。



カスケードトポロジ–SCVを使用してプライマリとセカンダリのデータコピーを作成する手順は、前述のファンアウトトポロジと同じです。ただし、今回はBlueXPのバックアップとリカバリでポリシーを作成し、オブジェクトストレージへのバックアップをセカンダリONTAPクラスタから開始するように指定します。



BlueXPのバックアップとリカバリでは、オンプレミスのONTAP Snapshotのバックアップコピーを AWS Glacier、Azure Blob、GCPアーカイブストレージに作成できます。



また、オブジェクトストレージのバックアップターゲットとしてNetApp StorageGRIDを使用することもできます。StorageGRIDの詳細については、 "StorageGRIDランディングページ"。

以下に、この解決策を設定し、SCVおよびBlueXPのバックアップとリカバリからバックアップとリストアの処理を実行するために必要な手順の概要を示します。

1. プライマリとセカンダリのデータコピーに使用するONTAPクラスタ間のSnapMirror関係を設定します。
2. SnapCenter Plug-in for VMware vSphereを設定する
    a. ストレージシステムを追加
    b. バックアップポリシーを作成する
    c. リソースグループを作成する
    d. バックアップ先のバックアップジョブを実行
3. 仮想マシンのBlueXPバックアップ/リカバリの設定
    a. 作業環境の追加
    b. SCVおよびvCenterアプライアンスの検出
    c. バックアップポリシーを作成する
    d. バックアップのアクティブ化
4. SCVを使用して、プライマリストレージとセカンダリストレージから仮想マシンをリストアします。
5. BlueXPのバックアップとリストアを使用して、オブジェクトストレージから仮想マシンをリストアできます。

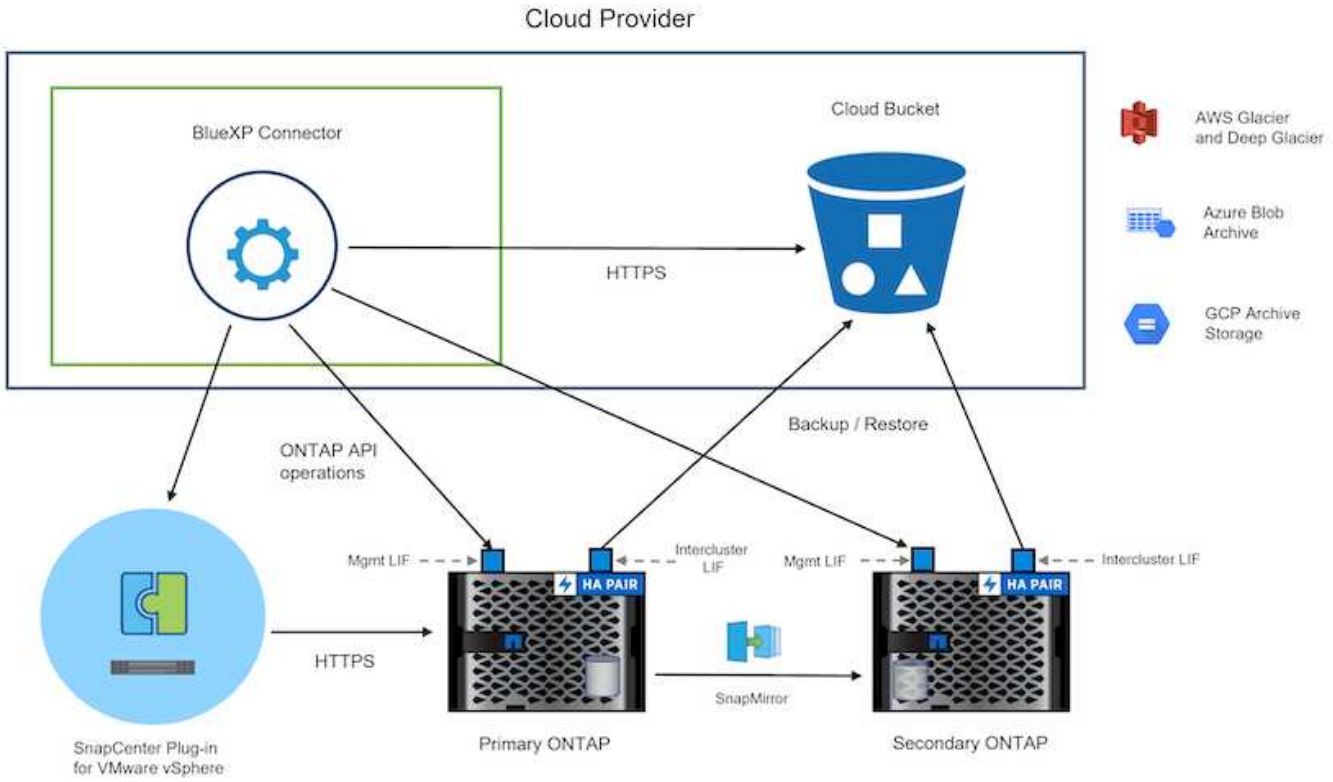
前提条件

この解決策の目的は、VMware vSphereで実行され、NetApp ONTAPでホストされるNFSデータストアに配置された仮想マシンのデータ保護を実証することです。この解決策 は、次のコンポーネントが構成され、使用可能な状態にあることを前提としています。

1. VMware vSphereに接続されたNFSまたはVMFSデータストアを使用するONTAPストレージクラスタ。NFSデータストアとVMFSデータストアの両方がサポートされます。この解決策にはNFSデータストアが使用されました。
2. NFSデータストア用に使用されるボリュームのSnapMirror関係が確立されたセカンダリONTAPストレージクラスタ。
3. オブジェクトストレージのバックアップに使用するクラウドプロバイダ用にBlueXP Connectorをインストール
4. バックアップ対象の仮想マシンが、プライマリONTAPストレージクラスタ上のNFSデータストア上にある。
5. BlueXP ConnectorとオンプレミスのONTAPストレージクラスタ管理インターフェイス間のネットワーク接続。
6. BlueXPコネクタとオンプレミスSCVアプライアンスVMの間、およびBlueXPコネクタとvCenterの間のネットワーク接続。
7. オンプレミスのONTAPクラスタ間LIFとオブジェクトストレージサービスの間のネットワーク接続。
8. プライマリとセカンダリのONTAPストレージクラスタで管理SVM用に設定されたDNS。詳細については、を参照してください。 "ホスト名解決に使用する DNS を設定します"。

アーキテクチャの概要

この解決策 のテストと検証は、最終的な導入環境と異なる場合があるラボで実施しました。



解決策 の導入

この解決策では、オンプレミスのデータセンターにあるVMware vSphereクラスタ内のWindowsおよびLinux仮想マシンのバックアップとリカバリを実行するために、SnapCenter Plug-in for VMware vSphereとBlueXPのバックアップおよびリカバリを使用する解決策を導入および検証するための詳細な手順を説明します。このセットアップの仮想マシンは、ONTAP A300ストレージクラスタでホストされるNFSデータストアに格納されます。さらに、独立したONTAP A300ストレージクラスタは、SnapMirrorを使用してレプリケートされるボリュームのセカンダリデスティネーションとして機能します。さらに、Amazon Web ServicesとAzure Blobでホストされているオブジェクトストレージを、データの3つ目のコピーのターゲットとして使用しました。

ここでは、SCVで管理されるバックアップのセカンダリコピー用のSnapMirror関係の作成と、SCVとBlueXPの両方のバックアップ/リカバリでのバックアップジョブの設定について説明します。

SnapCenter Plug-in for VMware vSphereの詳細については、 "SnapCenter Plug-in for VMware vSphere のドキュメント"。

BlueXPのバックアップとリカバリの詳細については、 "BlueXPのバックアップとリカバリに関するドキュメント"。

ONTAPクラスタ間に**SnapMirror**関係を確立

SnapCenter Plug-in for VMware vSphereは、ONTAP SnapMirrorテクノロジを使用して、セカンダリONTAPクラスタへのセカンダリSnapMirrorまたはSnapVaultコピーの転送を管理します。

SCVバックアップポリシーでは、SnapMirror関係とSnapVault関係のどちらを使用するかを選択できます。主な違いは、SnapMirrorオプションを使用する場合、ポリシーでバックアップの保持スケジュールがプライマリサイトとセカンダリサイトで同じになる点です。SnapVaultはアーカイブ用に設計されており、このオプションを使用する場合は、セカンダリONTAPストレージクラスタ上のSnapshotコピーのSnapMirror関係と別に保持スケジュールを設定できます。

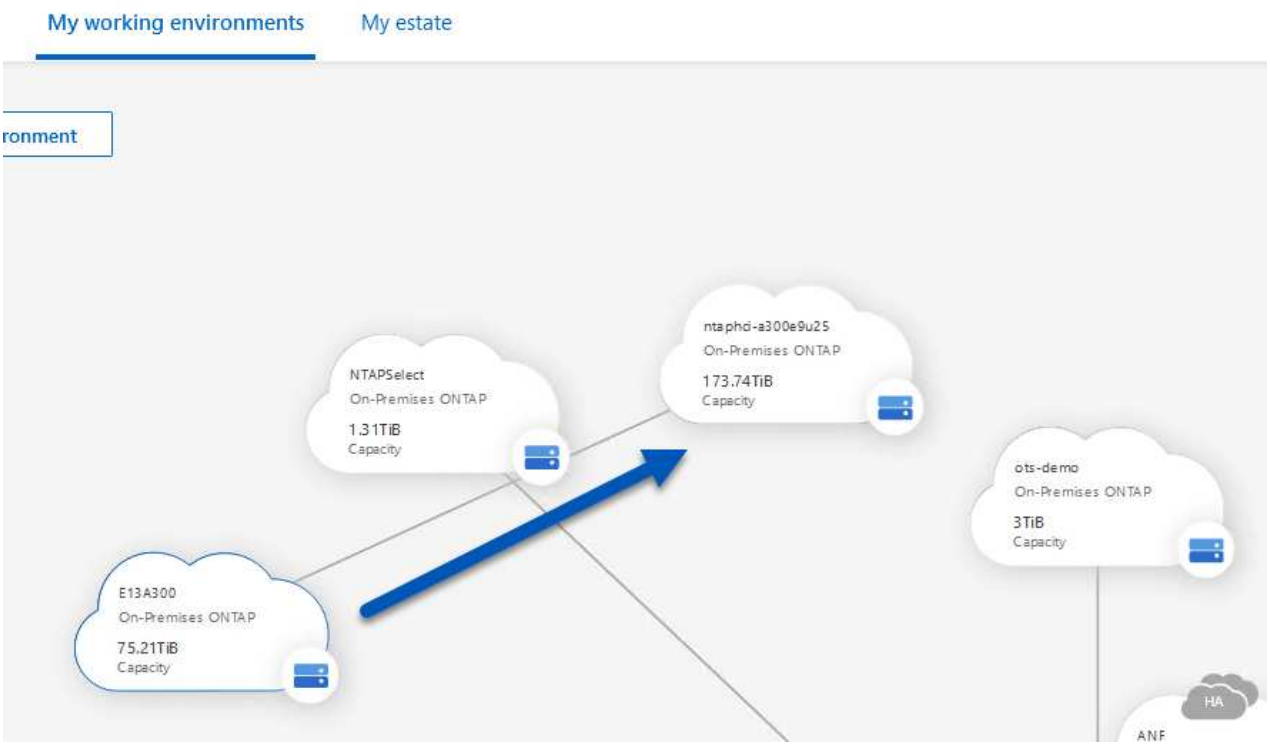
SnapMirror関係のセットアップは、多くの手順が自動化されたBlueXPまたはSystem ManagerとONTAP CLIを使用して実行できます。これらの方法については、以下で説明します。

BlueXPで**SnapMirror**関係を確立

BlueXPのWebコンソールで次の手順を実行する必要があります。

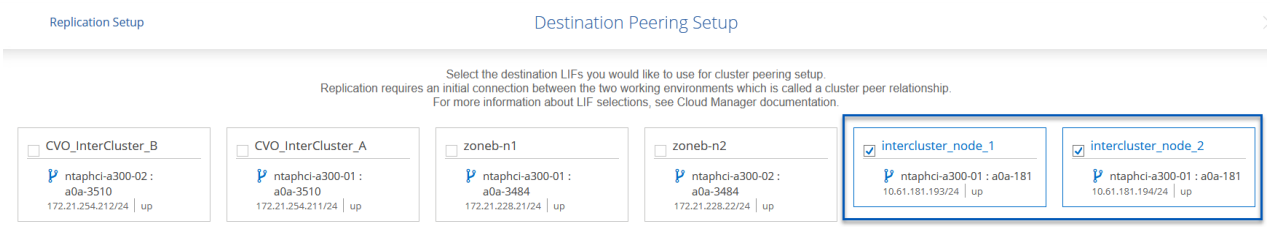
まず、BlueXP Webコンソールにログインし、Canvasに移動します。

1. ソース（プライマリ）ONTAPストレージシステムをデスティネーション（セカンダリ）ONTAPストレージシステムにドラッグアンドドロップします。

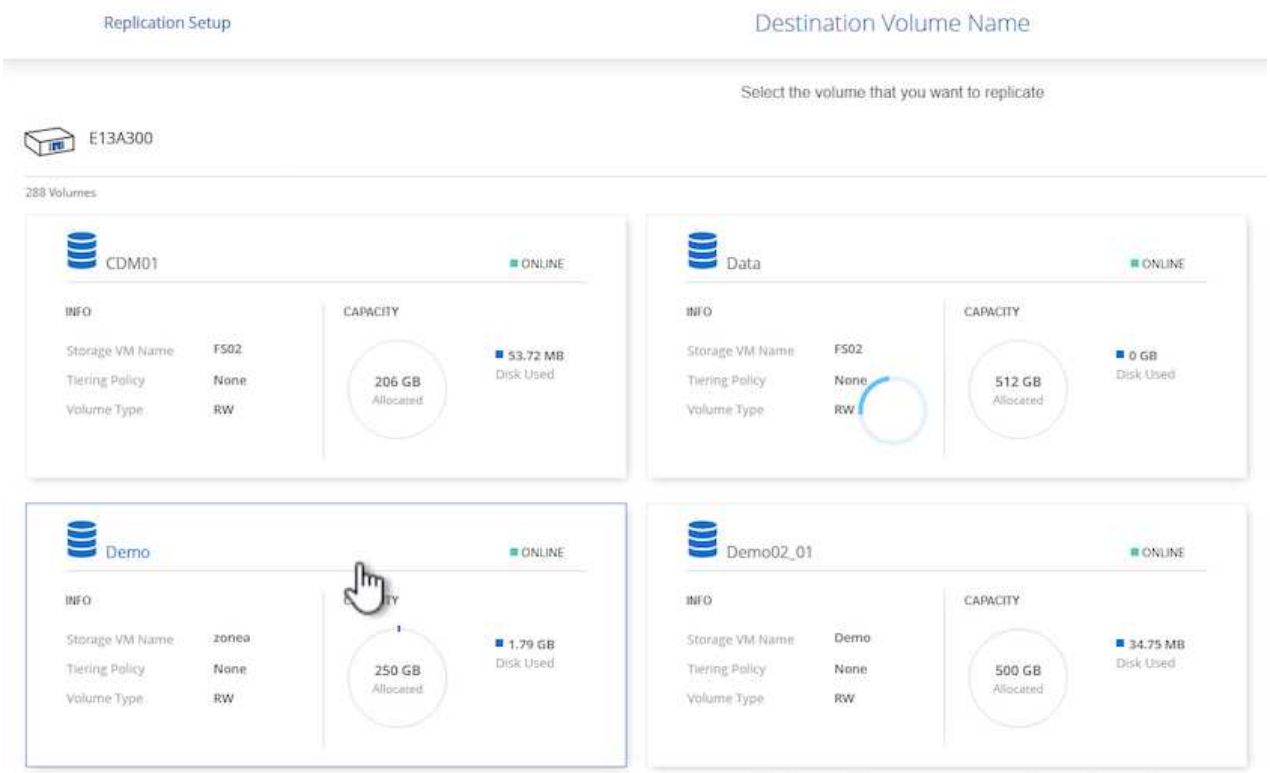


2. 表示されたメニューから* Replication（レプリケーション）*を選択します。

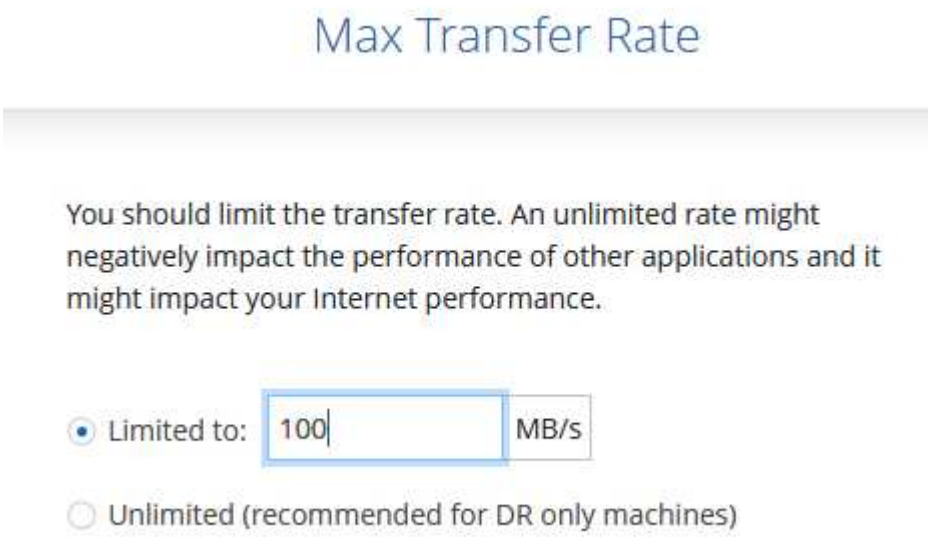
3. [デスティネーションピアリングのセットアップ]*ページで、ストレージシステム間の接続に使用するデスティネーションのクラスタ間LIFを選択します。



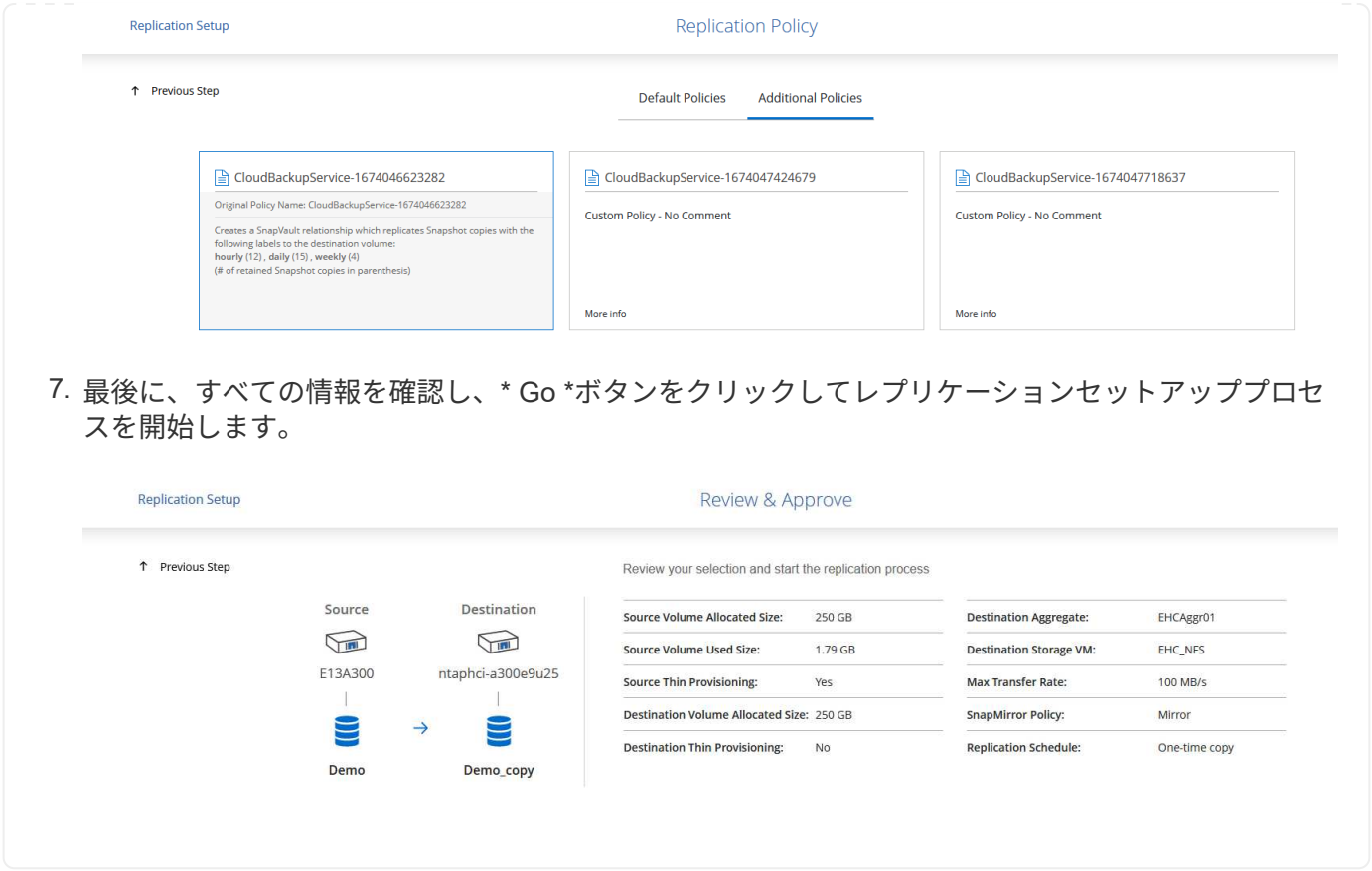
4. [デスティネーションボリューム名]*ページで、最初にソースボリュームを選択してからデスティネーションボリュームの名前を入力し、デスティネーションSVMとアグリゲートを選択します。[次へ]*をクリックして続行します。



5. レプリケーションの最大転送速度を選択します。



6. セカンダリバックアップの保持スケジュールを決定するポリシーを選択します。このポリシーは事前に作成することも（*スナップショット保持ポリシーの作成*手順の手動プロセスを参照）、後で必要に応じて変更することもできます。



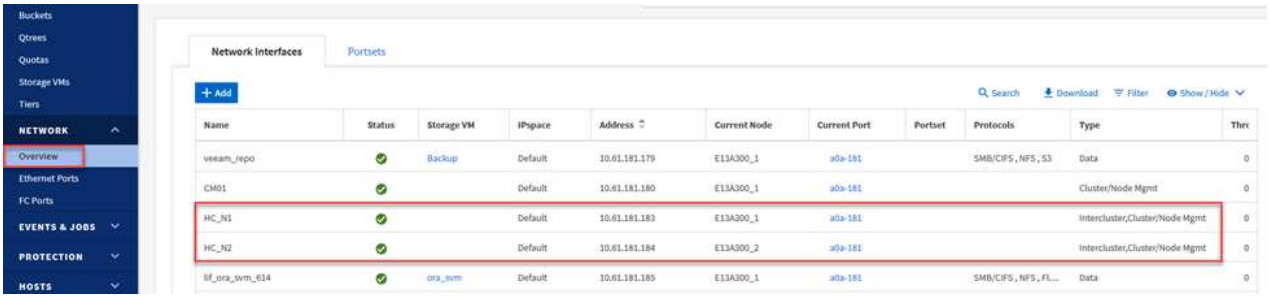
7. 最後に、すべての情報を確認し、* Go *ボタンをクリックしてレプリケーションセットアッププロセスを開始します。

System ManagerとONTAP CLIを使用してSnapMirror関係を確立

SnapMirror関係を確立するために必要なすべての手順は、System ManagerまたはONTAP CLIで実行できます。次のセクションでは、両方の方法の詳細について説明します。

ソースとデスティネーションのONTAPクラスタの場合、System ManagerまたはCLIからクラスタ間LIFの情報を取得できます。

1. ONTAP System Managerで、ネットワークの概要ページに移動し、タイプ：クラスタ間のIPアドレスを取得します。このIPアドレスは、FSXがインストールされているAWS VPCと通信するように設定されています。



2. CLIを使用してクラスタ間IPアドレスを取得するには、次のコマンドを実行します。

```
ONTAP-Dest::> network interface show -role intercluster
```

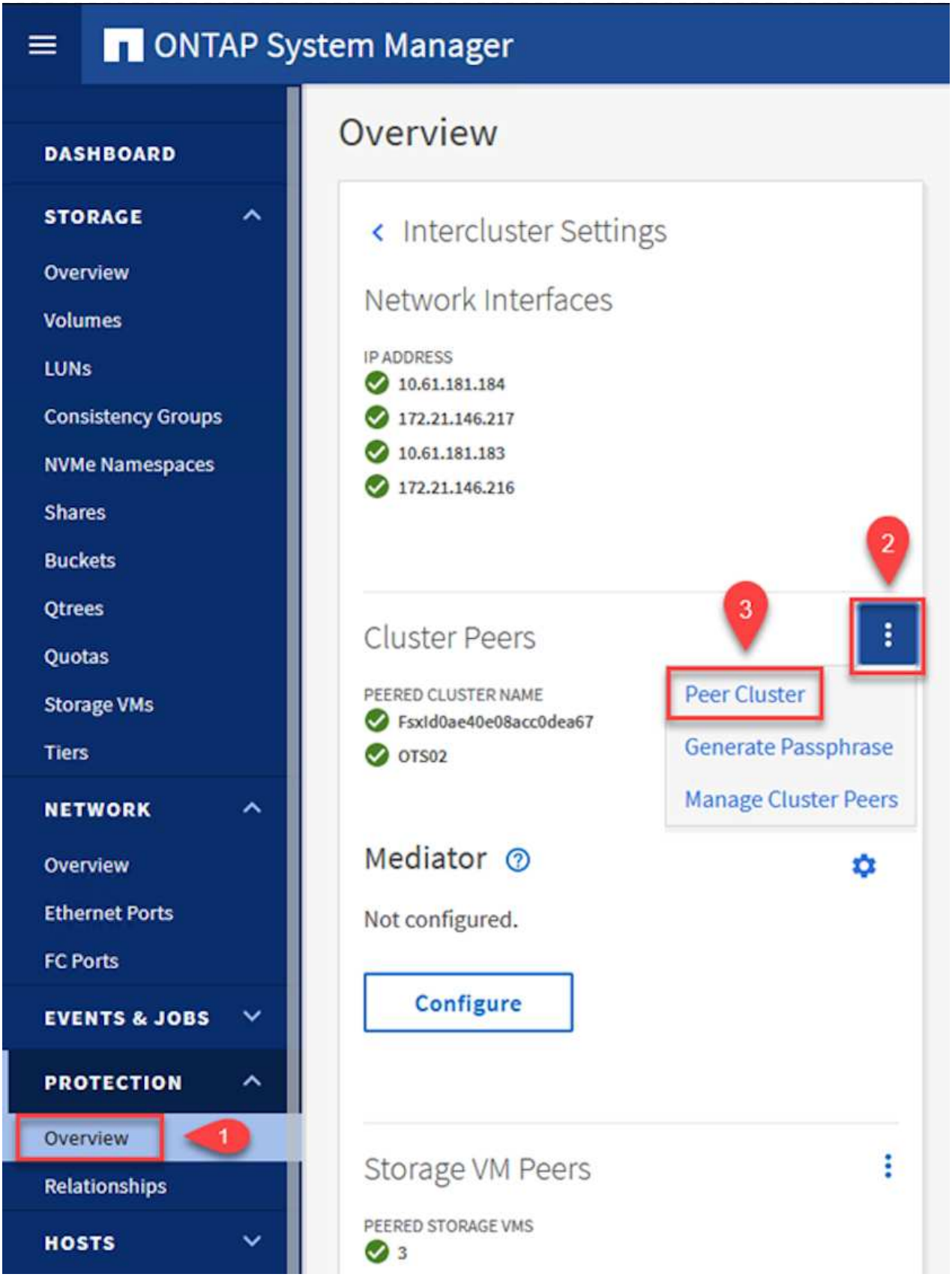
ONTAPクラスタ間にクラスタピアリングを確立

ONTAP クラスタ間のクラスタピアリングを確立するには、開始側のONTAP クラスタで入力した一意のパスフレーズを、もう一方のピアクラスタで確認する必要があります。

1. を使用して、デスティネーションONTAPクラスタでピアリングを設定します。 `cluster peer create` コマンドを実行しますプロンプトが表示されたら、あとでソースクラスタで使用する一意のパスフレーズを入力して作成プロセスを完了します。

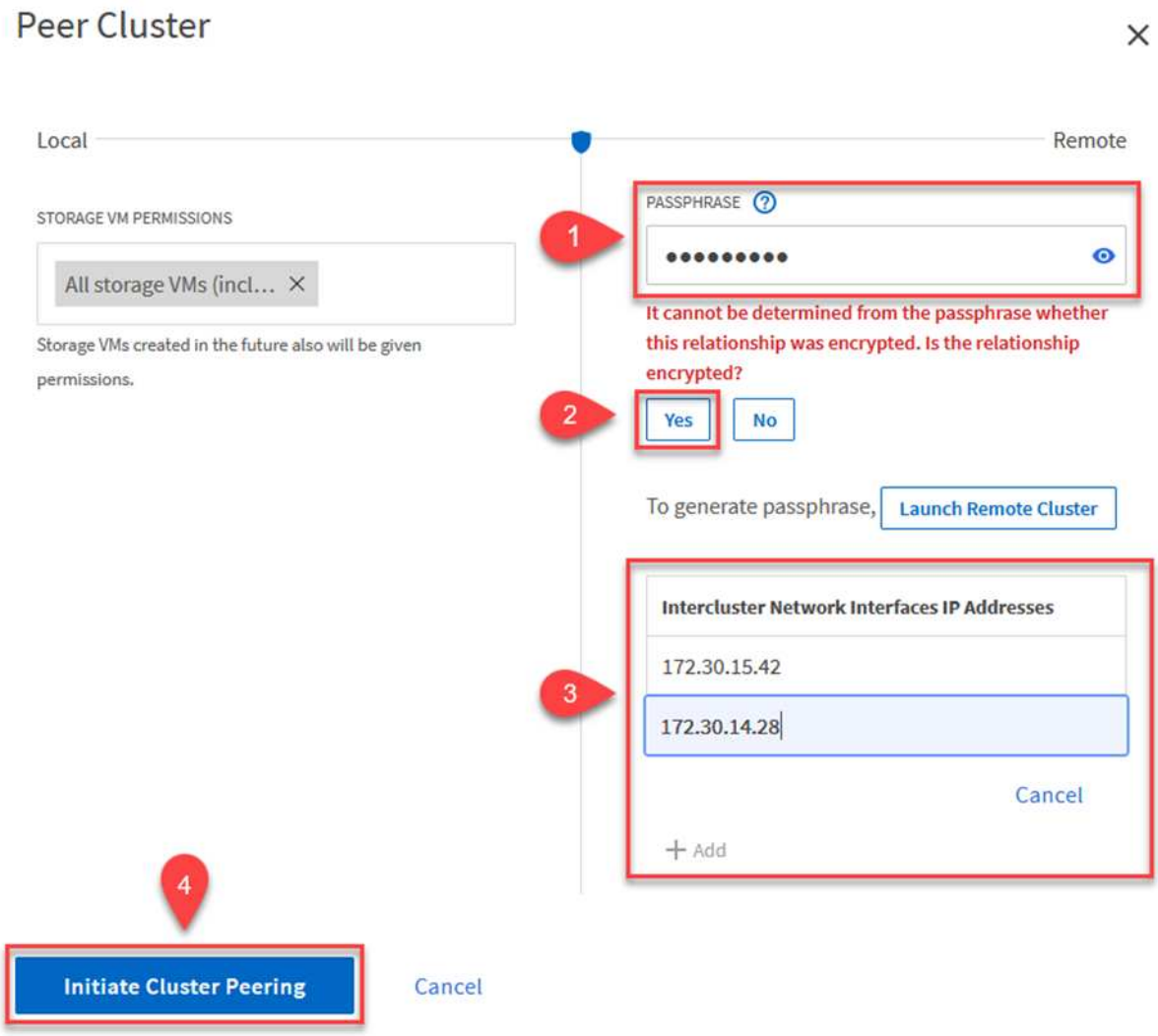
```
ONTAP-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. ソースクラスタでは、ONTAP System ManagerまたはCLIを使用してクラスタピア関係を確立できます。ONTAP System Managerで、Protection > Overviewの順に選択し、Peer Clusterを選択します。



3. Peer Cluster（ピアクラスタ）ダイアログボックスで、必要な情報を入力します。
   a. デスティネーションONTAPクラスタでピアクラスタ関係を確立するために使用したパスフレーズを入力します。

b. [はい]を選択して'暗号化された関係を確立します
c. デスティネーションONTAPクラスタのクラスタ間LIFのIPアドレスを入力します。
d. クラスタピアリングの開始をクリックしてプロセスを完了します。



4. 次のコマンドを使用して、デスティネーションONTAPクラスタからクラスタピア関係のステータスを確認します。

```
ONTAP-Dest::> cluster peer show
```

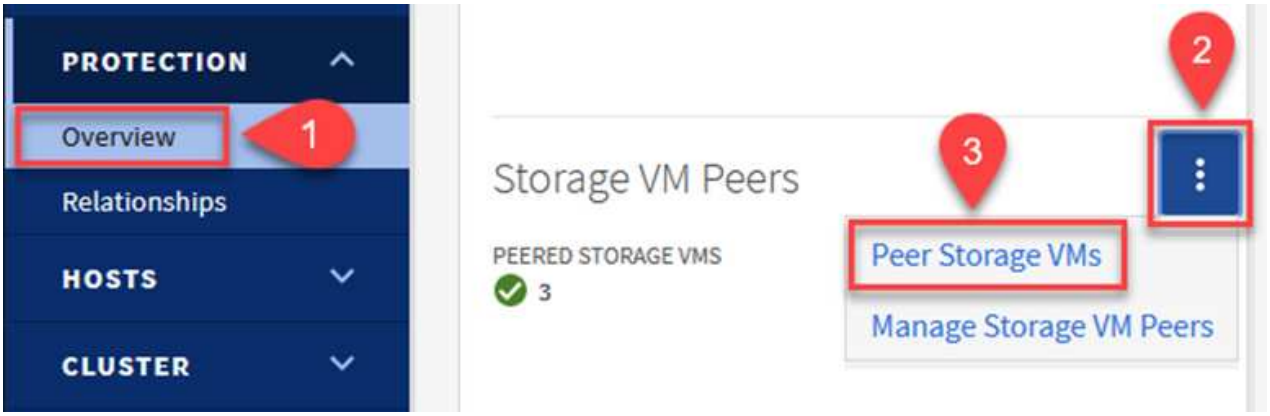
SVMピア関係を確立する

次の手順では、SnapMirror関係にあるボリュームを含むデスティネーションとソースのStorage Virtual Machineの間にSVM関係をセットアップします。

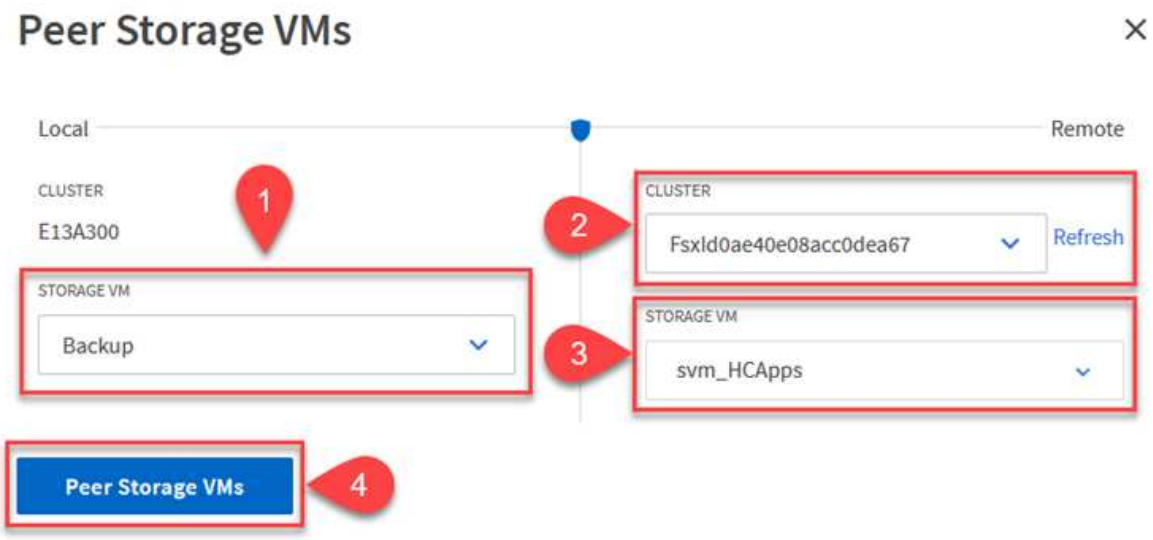
1. デスティネーションONTAPクラスタから、CLIから次のコマンドを使用して、SVMピア関係を作成します。

```
ONTAP-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. ソースONTAP クラスタで、ONTAP System ManagerまたはCLIのいずれかを使用してピアリング関係を承認します。
3. ONTAP System Managerで、保護>概要に移動し、Storage VMピアの下にあるピアStorage VMを選択します。



4. Peer Storage VMダイアログボックスで、次のフィールドに入力します。
   - ソースStorage VM
   - デスティネーションクラスタ
   - デスティネーションStorage VM



5. [Peer Storage VMs]をクリックして、SVMピアリングプロセスを完了します。

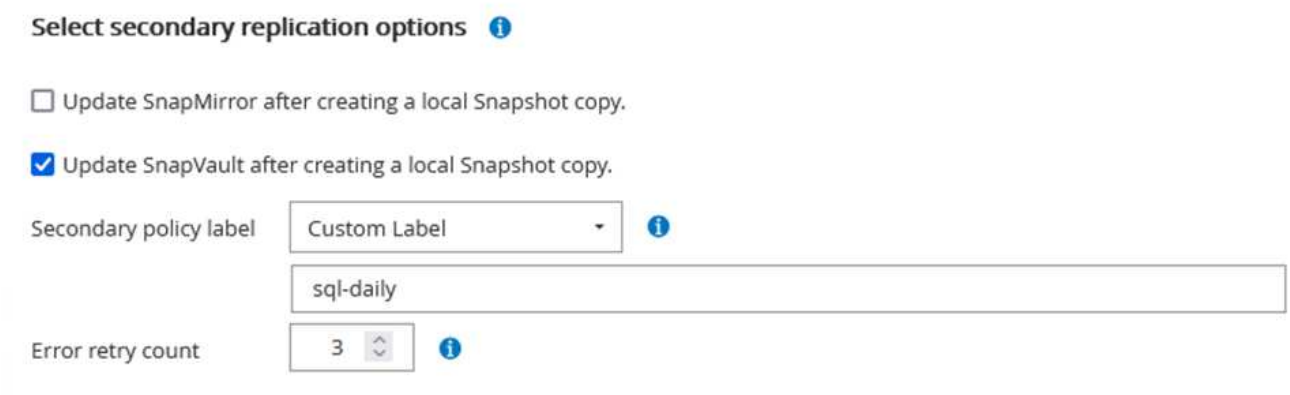
Snapshot保持ポリシーを作成します

SnapCenter は、プライマリストレージシステムにSnapshotコピーとして存在するバックアップの保持スケジュールを管理します。これは、SnapCenter でポリシーを作成するときに確立されます。SnapCenter では、セカンダリストレージシステムに保持されるバックアップの保持ポリシーは管理されません。これらのポリシーは、セカンダリFSXクラスタで作成されたSnapMirrorポリシーを使用して個別に管理され、ソースボリュームとSnapMirror関係にあるデスティネーションボリュームに関連付けられます。

SnapCenter ポリシーを作成するときに、SnapCenter バックアップの作成時に生成される各SnapshotのSnapMirrorラベルに追加するセカンダリポリシーラベルを指定できます。

> セカンダリストレージでは、Snapshotを保持するために、これらのラベルがデスティネーションボリュームに関連付けられたポリシールールと照合されます。

次の例は、SQL Serverデータベースおよびログボリュームの日次バックアップに使用するポリシーの一部として生成されたすべてのSnapshotに適用されるSnapMirrorラベルを示しています。



SQL ServerデータベースのSnapCenter ポリシーの作成の詳細については、を参照してください "SnapCenter のドキュメント"。

まず、保持するSnapshotコピーの数にルールを指定してSnapMirrorポリシーを作成する必要があります。

1. FSXクラスタ上にSnapMirrorポリシーを作成します。

```
ONTAP-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. SnapCenter ポリシーで指定されたセカンダリポリシーラベルと一致するSnapMirrorラベルを持つルールをポリシーに追加します。

```
ONTAP-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

次のスクリプトは、ポリシーに追加できるルールの例を示しています。

```
ONTAP-Dest::> snapmirror policy add-rule -vserver sql_svm_dest
-policy Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

SnapMirrorラベルごとに追加のルールを作成し、保持するSnapshotの数（保持期間）を指定します。

デスティネーションボリュームを作成

ソースボリュームのSnapshotコピーを受け取るデスティネーションボリュームをONTAPに作成するには、デスティネーションONTAPクラスタで次のコマンドを実行します。

```
ONTAP-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

ソースボリュームとデスティネーションボリューム間に**SnapMirror**関係を作成します

ソースボリュームとデスティネーションボリューム間にSnapMirror関係を作成するには、デスティネーションONTAPクラスタで次のコマンドを実行します。

```
ONTAP-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

SnapMirror関係を初期化

SnapMirror関係を初期化このプロセスにより、ソースボリュームから生成された新しいSnapshotが開始され、デスティネーションボリュームにコピーされます。

ボリュームを作成するには、デスティネーションONTAPクラスタで次のコマンドを実行します。

```
ONTAP-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

SnapCenter Plug-in for VMware vSphereの設定

インストールが完了すると、vCenter Server Appliance管理インターフェイスからSnapCenter Plug-in for VMware vSphereにアクセスできるようになります。SCVは、ESXiホストにマウントされた、Windows VMとLinux VMを含むNFSデータストアのバックアップを管理します。

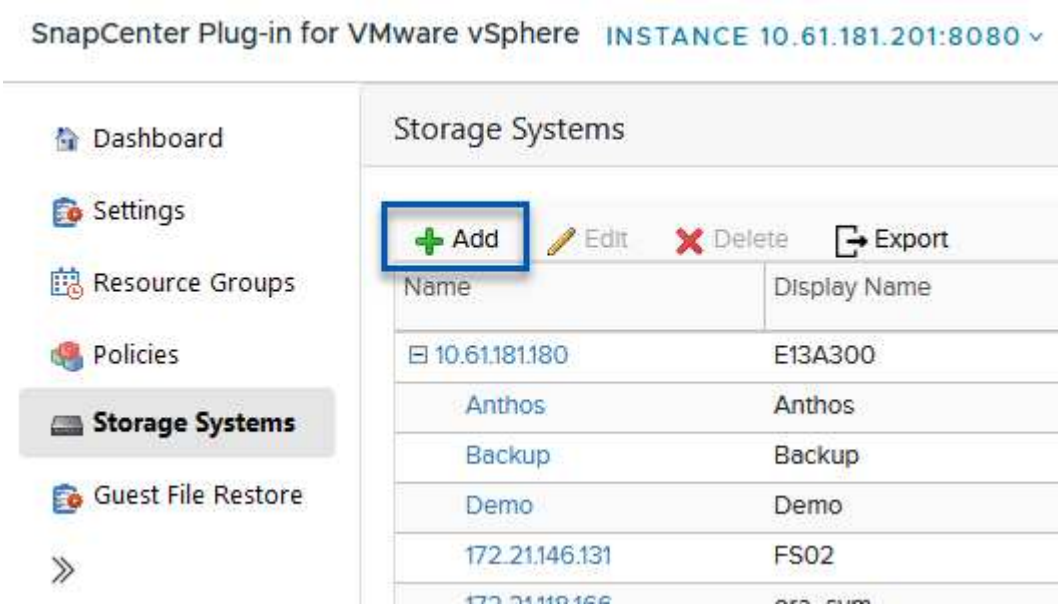
を確認します "データ保護のワークフロー" バックアップの設定手順の詳細については、SCVのマニュアルのセクションを参照してください。

仮想マシンとデータストアのバックアップを設定するには、プラグインインターフェイスから次の手順を実行する必要があります。

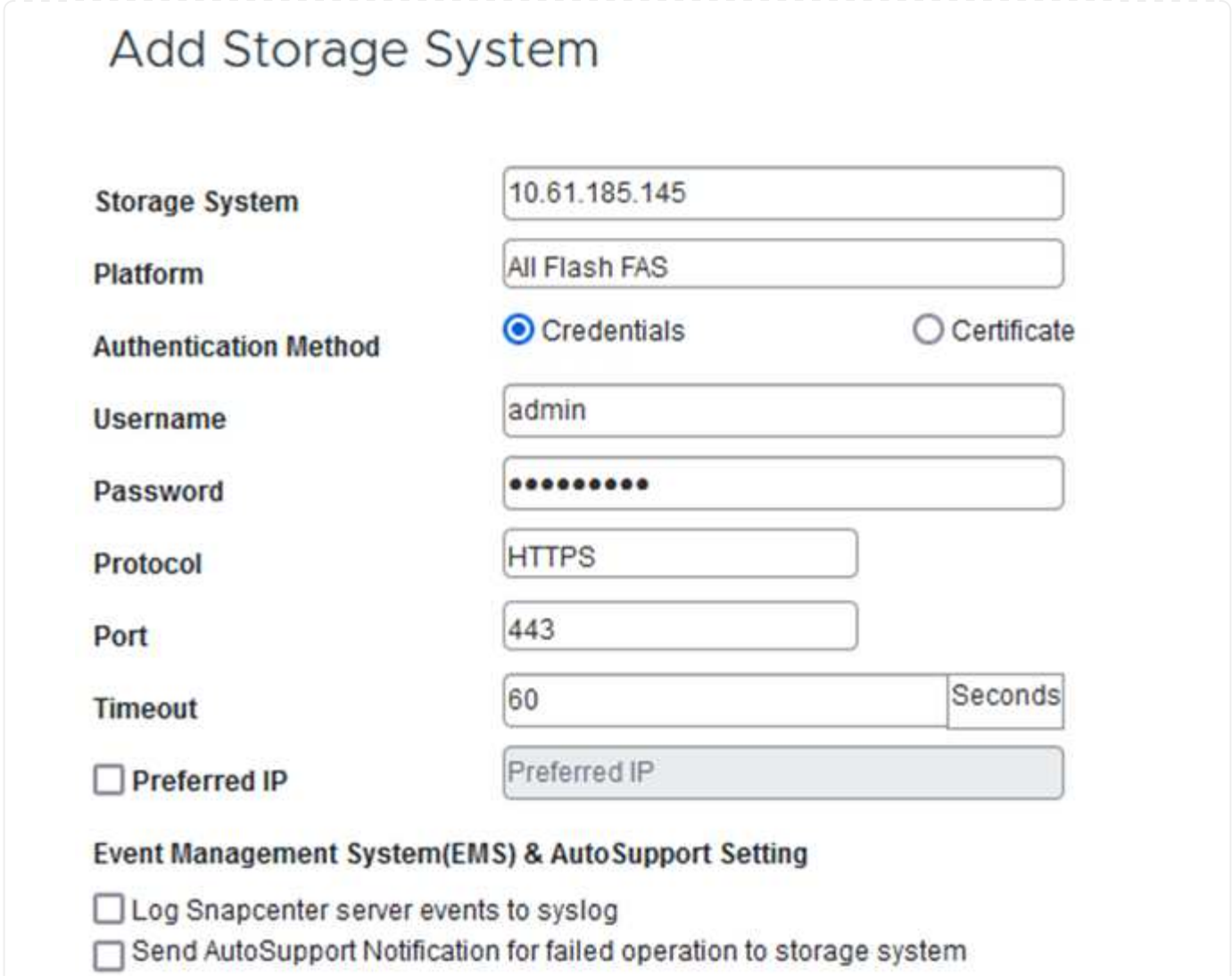
Discovery ONTAPストレージシステム

プライマリバックアップとセカンダリバックアップの両方に使用するONTAPストレージクラスタを検出します。

1. SnapCenter Plug-in for VMware vSphereで、左側のメニューの*に移動し、[追加]*ボタンをクリックします。



2. プライマリONTAPストレージシステムのクレデンシャルとプラットフォームタイプを入力し、*[追加]*をクリックします。



3. セカンダリONTAPストレージシステムに対してこの手順を繰り返します。

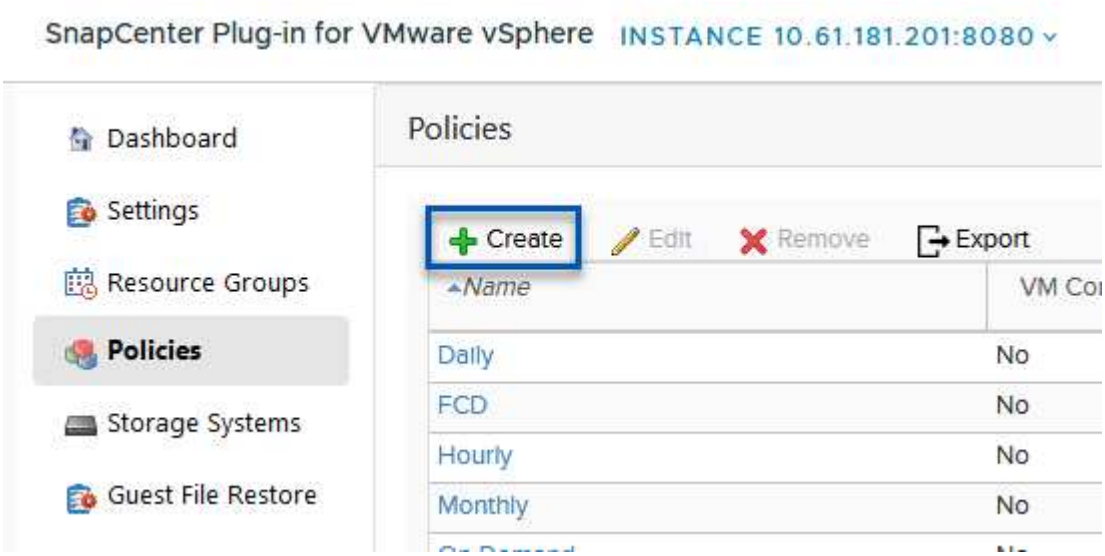
SCVバックアップポリシーの作成

ポリシーは、SCVで管理されるバックアップの保持期間、頻度、およびレプリケーションオプションを指定します。

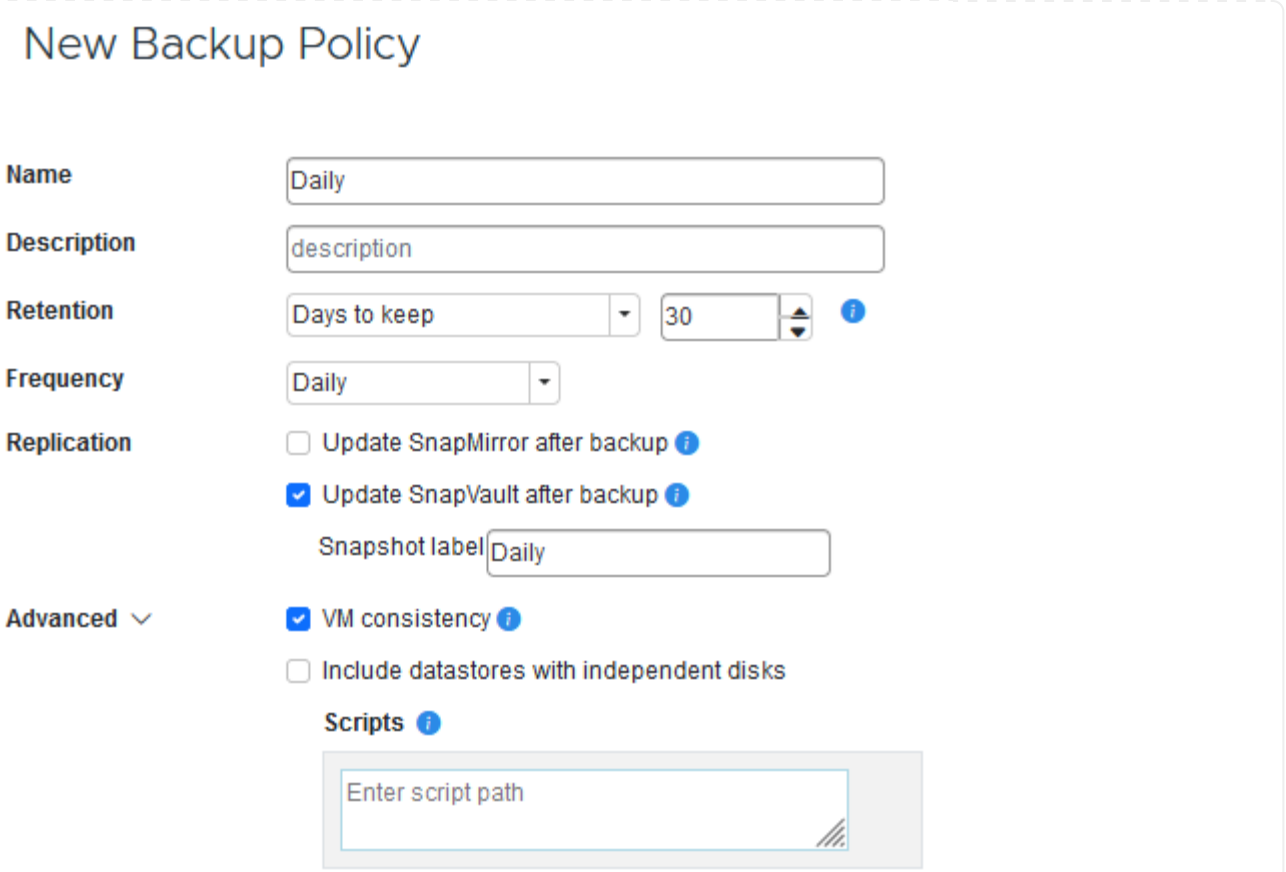
を確認します "VM とデータストアのバックアップポリシーの作成" 詳細については、を参照してください。

バックアップポリシーを作成するには、次の手順を実行します。

1. SnapCenter Plug-in for VMware vSphereで、左側のメニューの*に移動し、[Create]*ボタンをクリックします。



2. ポリシーの名前、保持期間、頻度とレプリケーションのオプション、およびSnapshotラベルを指定します。



SnapCenter Plug-inでポリシーを作成すると、[SnapMirror]と[SnapMirror]のオプションが表示されSnapVaultます。[SnapMirror]を選択した場合、ポリシーに指定された保持スケジュールは、プライマリSnapshotとセカンダリSnapshotの両方で同じになります。SnapVaultを選択した場合、セカンダリSnapshotの保持スケジュールは、SnapMirror関係で実装される個別のスケジュールに基づいて決まります。これは、セカンダリバックアップの保持期間を長くしたい場合に便利です。

SnapshotラベルはセカンダリONTAPクラスタにレプリケートされたSnapVaultコピーの保持期間を指定したポリシーを作成する場合に役立ちます。SCVをBlueXPのバックアップおよびリストアで使用する場合は、[Snapshot label]フィールドを空白にするか、match BlueXPバックアップポリシーで指定したラベルを指定する必要があります。

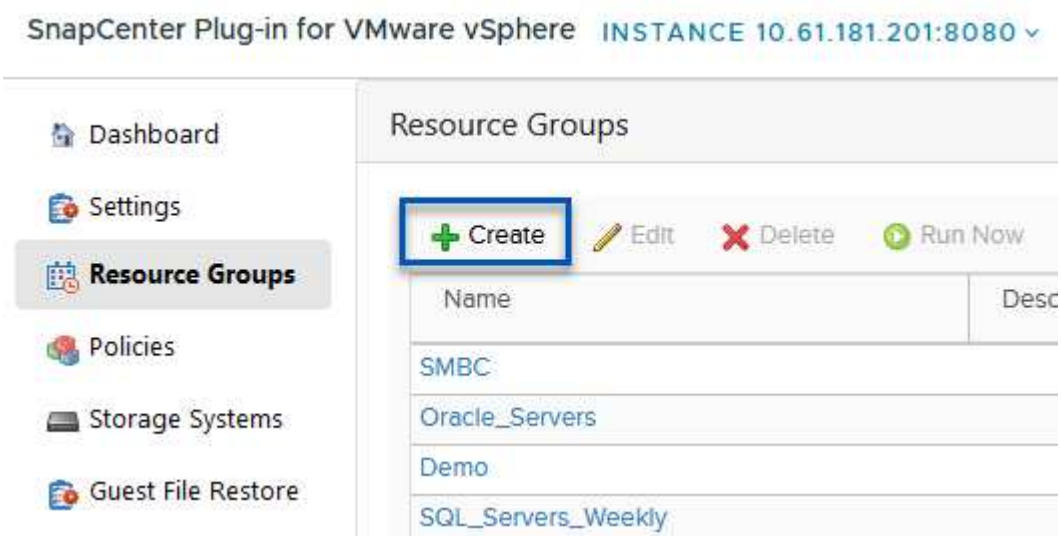
3. 必要なポリシーごとに手順を繰り返します。たとえば、日次、週次、月次のバックアップのポリシーを個別に指定します。

リソースグループには、バックアップジョブに含めるデータストアと仮想マシンのほか、関連付けられているポリシーとバックアップスケジュールが含まれます。

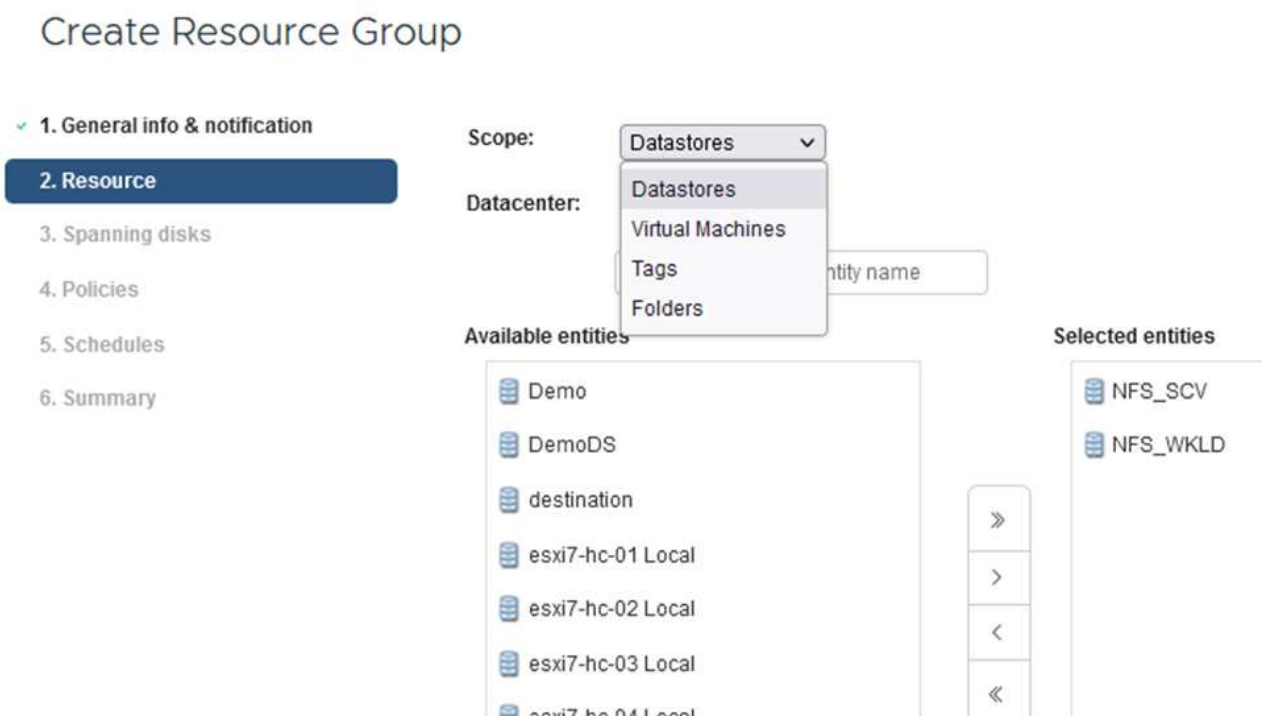
を確認します "リソースグループを作成する" 詳細については、を参照してください。

リソースグループを作成するには、次の手順を実行します。

1. SnapCenter Plug-in for VMware vSphereで、左側のメニューの*に移動し、[作成]*ボタンをクリックします。

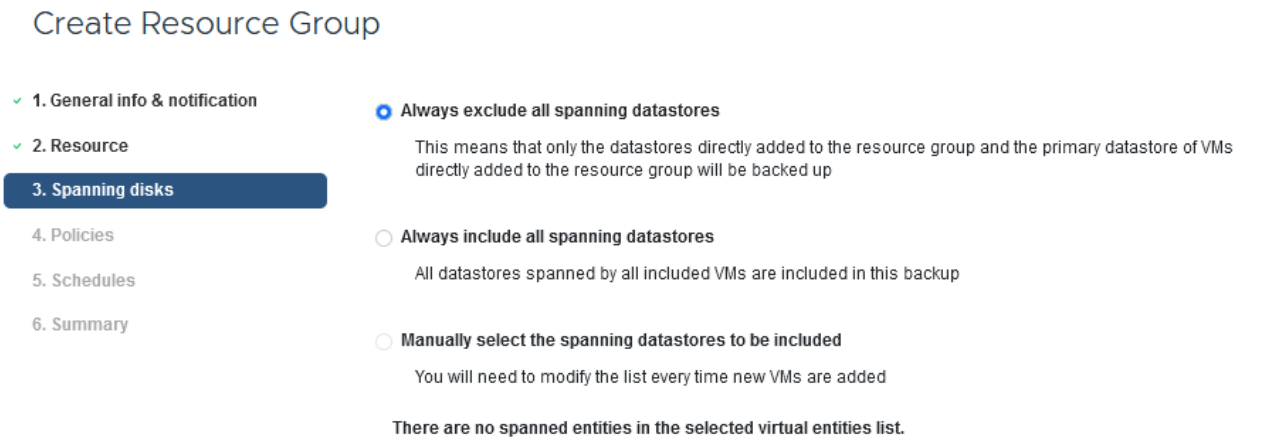


2. [Create Resource Group]ウィザードで、グループの名前と概要、および通知を受信するために必要な情報を入力します。[次へ]*をクリックします。
3. 次のページで、バックアップジョブに含めるデータストアと仮想マシンを選択し、*[Next]*をクリックします。



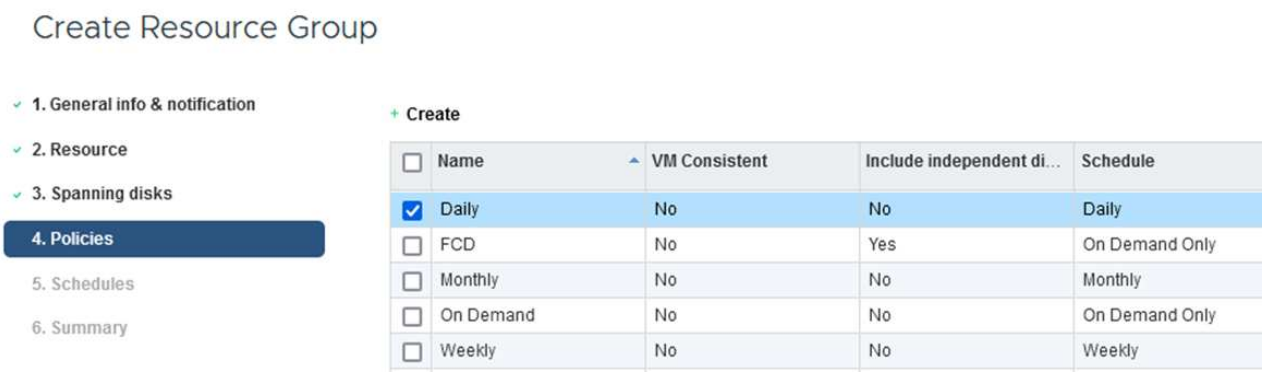
特定のVMまたはデータストア全体を選択できます。どちらを選択するかに関係なく、基盤となるボリュームのSnapshotが作成されるため、バックアップではボリューム全体（およびデータストア）がバックアップされます。ほとんどの場合、データストア全体を選択するのが最も簡単です。ただし、リストア時に使用可能なVMのリストを制限する場合は、バックアップするVMのサブセットのみを選択できます。

4. 複数のデータストアに配置されているVMDKを使用するVMのデータストアにスパニングするオプションを選択し、*[Next]*をクリックします。



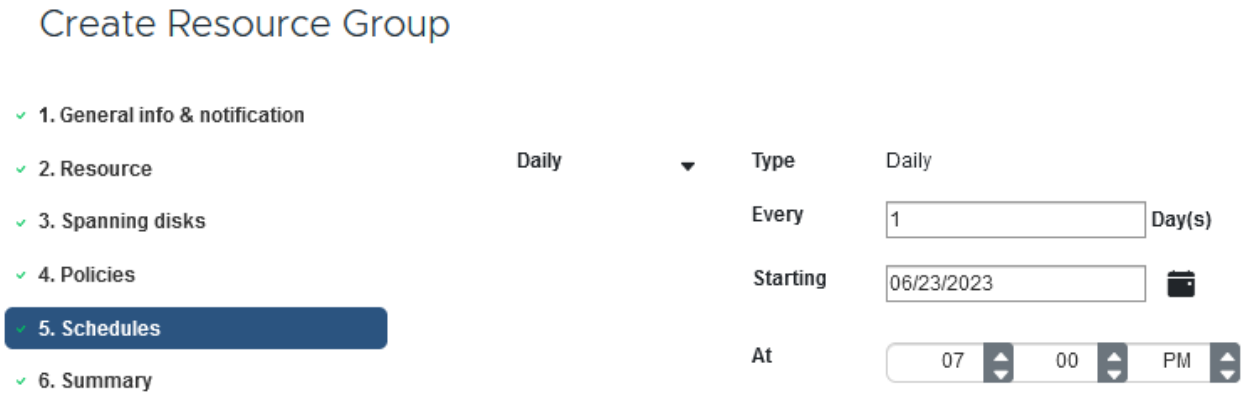
現在、BlueXPのバックアップ/リカバリでは、複数のデータストアにまたがるVMDKを使用したVMのバックアップはサポートされていません。

5. 次のページで、リソースグループに関連付けるポリシーを選択し、*[次へ]*をクリックします。



BlueXPのバックアップとリカバリを使用してSCV管理Snapshotをオブジェクトストレージにバックアップする場合は、各リソースグループに関連付けることができるポリシーは1つだけです。

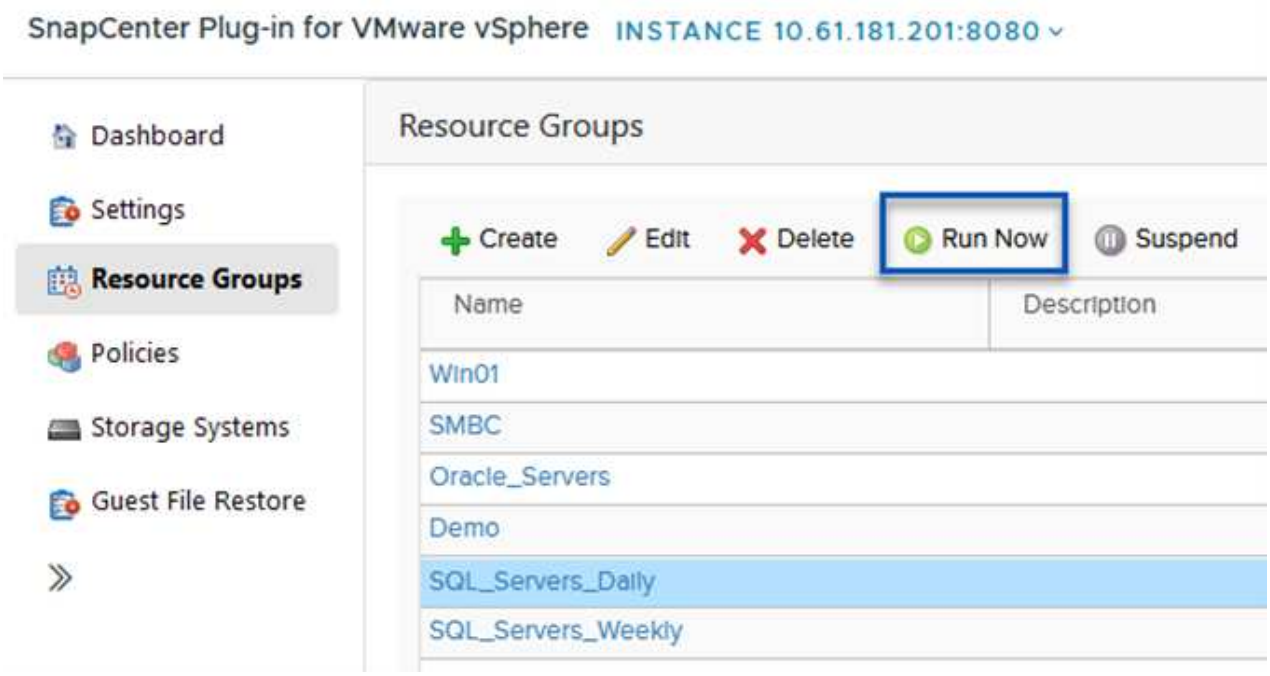
6. バックアップを実行する時刻を決定するスケジュールを選択します。[次へ]*をクリックします。



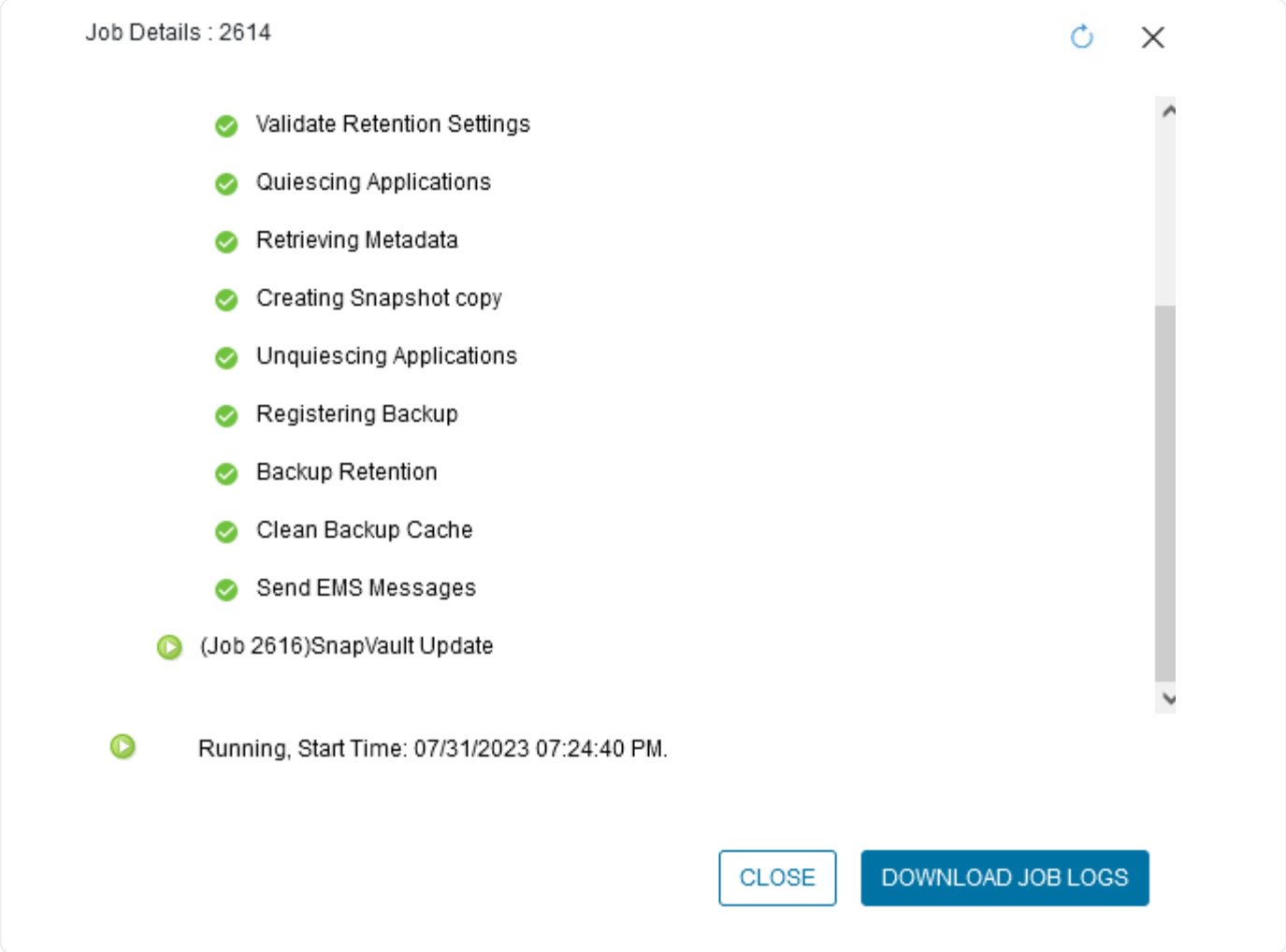
7. 最後に、概要ページを確認し、*[完了]*でリソースグループの作成を完了します。

この最後の手順では、バックアップジョブを実行して進捗状況を監視します。BlueXPのバックアップとリカバリからリソースを検出するには、SCVで少なくとも1つのバックアップジョブが完了している必要があります。

1. SnapCenter Plug-in for VMware vSphereで、左側のメニューの*[リソースグループ]*に移動します。
2. バックアップジョブを開始するには、目的のリソースグループを選択し、*[今すぐ実行]*ボタンをクリックします。



3. バックアップジョブを監視するには、左側のメニューの*[ダッシュボード]*に移動します。[Recent Job Activities]*で、ジョブID番号をクリックしてジョブの進捗状況を監視します。



BlueXPのバックアップとリカバリでオブジェクトストレージへのバックアップを設定

BlueXPでデータインフラを効果的に管理するには、コネクタを事前にインストールする必要があります。コネクタは、リソースの検出とデータ操作の管理に関連するアクションを実行します。

BlueXPコネクタの詳細については、 "コネクタについて説明します" を参照してください。

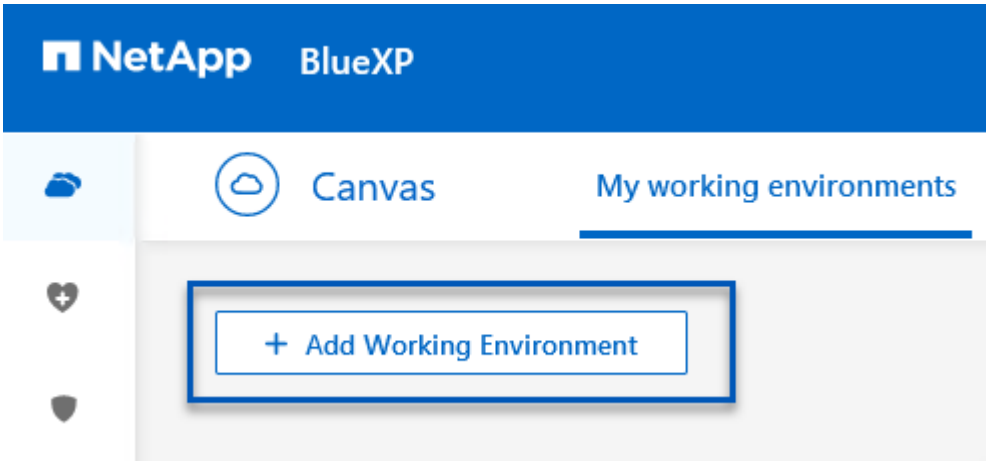
使用しているクラウドプロバイダ用のコネクタをインストールすると、オブジェクトストレージの図がキャンバスに表示されます。

オンプレミスのSCVで管理されるデータをバックアップするようにBlueXPのバックアップとリカバリを設定するには、次の手順を実行します。

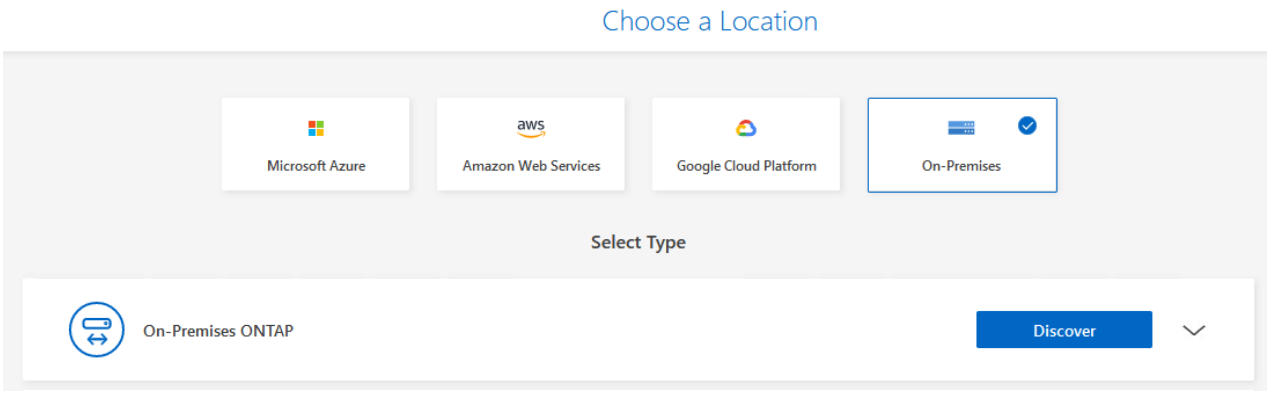
Canvasへの作業環境の追加

最初のステップは、オンプレミスのONTAPストレージシステムをBlueXPに追加することです。

1. キャンバスから*[Add Working Environment]*を選択して開始します。



2. 選択した場所から*オンプレミス*を選択し、*検出*ボタンをクリックします。



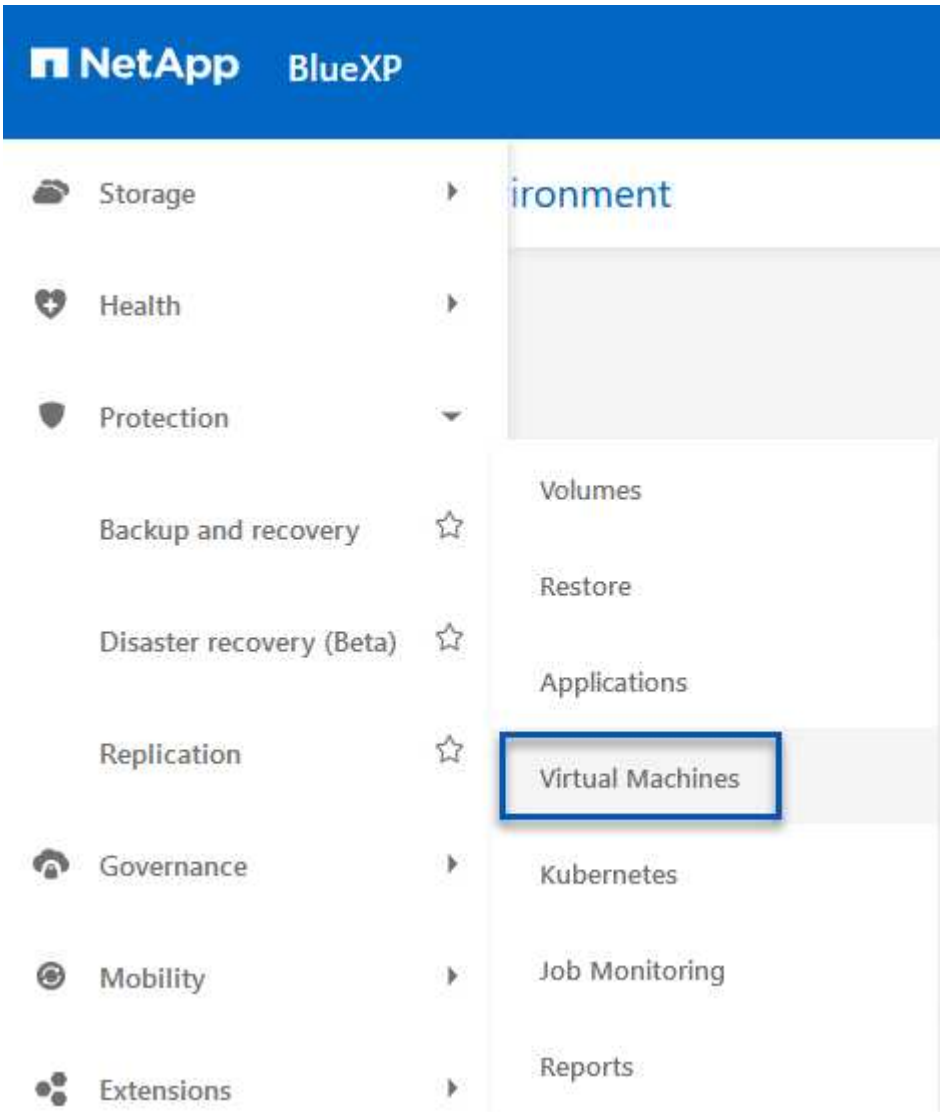
3. ONTAPストレージシステムのクレデンシャルを入力し、*[検出]*ボタンをクリックして作業環境を追加します。


ONTAP Cluster IP
10.61.181.180
User Name
admin
Password

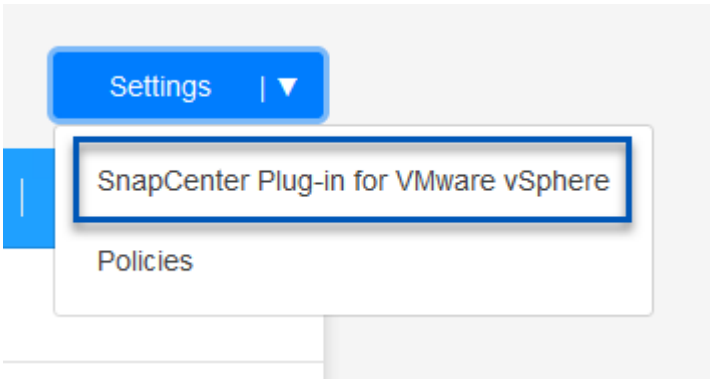
オンプレミスの**SCV**アプライアンスと**vCenter**を検出

オンプレミスのデータストアと仮想マシンのリソースを検出するには、SCVデータブローカーの情報とvCenter管理アプライアンスのクレデンシャルを追加します。

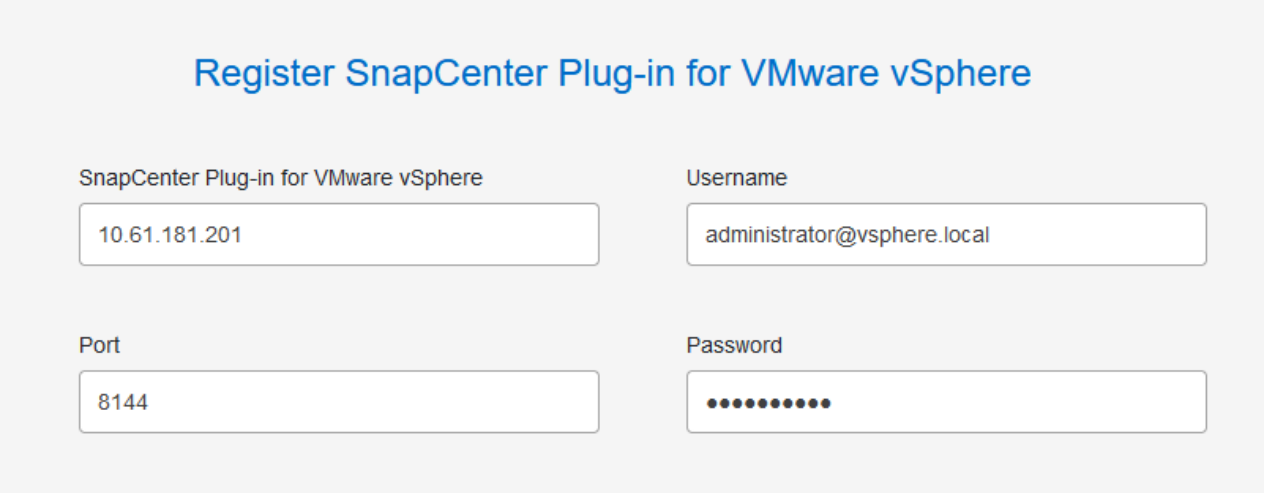
1. BlueXPの左側のメニューで*[保護]>[バックアップとリカバリ]>[仮想マシン]*を選択します。



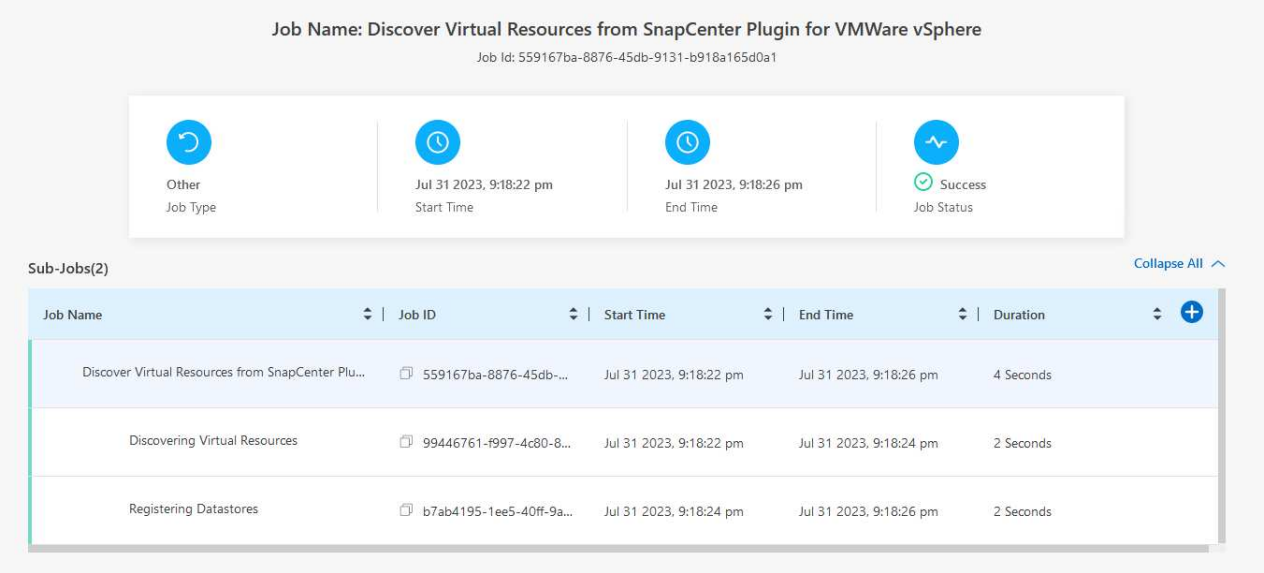
2. 仮想マシンのメイン画面から*ドロップダウンメニューにアクセスし、 SnapCenter Plug-in for VMware vSphere *を選択します。



3. [Register]ボタンをクリックし、SnapCenter Plug-inアプライアンスのIPアドレスとポート番号、およびvCenter管理アプライアンスのユーザ名とパスワードを入力します。[登録]ボタンをクリックして、検出プロセスを開始します。



4. ジョブの進捗状況は、[Job Monitoring]タブで監視できます。



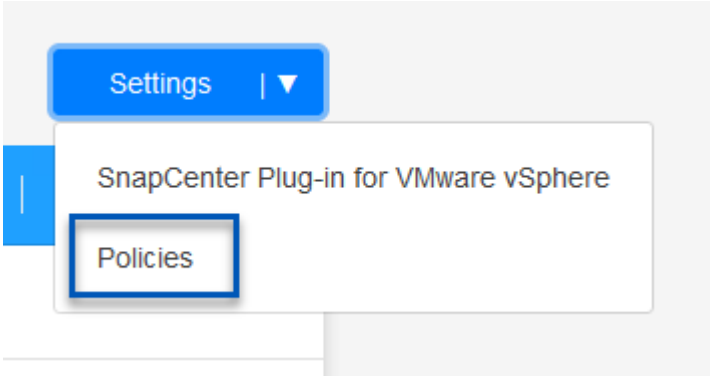
5. 検出が完了すると、検出されたすべてのSCVアプライアンスのデータストアと仮想マシンを表示できるようになります。
[+]
image：：bxp-scv-hybrid-23.png [利用可能なリソースを表示]

BlueXPバックアップポリシーの作成

仮想マシンのBlueXPバックアップ/リカバリで、保持期間、バックアップソース、アーカイブポリシーを指定するポリシーを作成します。

ポリシーの作成の詳細については、を参照してください。 "データストアをバックアップするポリシーを作成します"。

1. BlueXPの仮想マシンのバックアップとリカバリのメインページで、**[設定]***ドロップダウンメニューにアクセスし、[ポリシー]*を選択します。



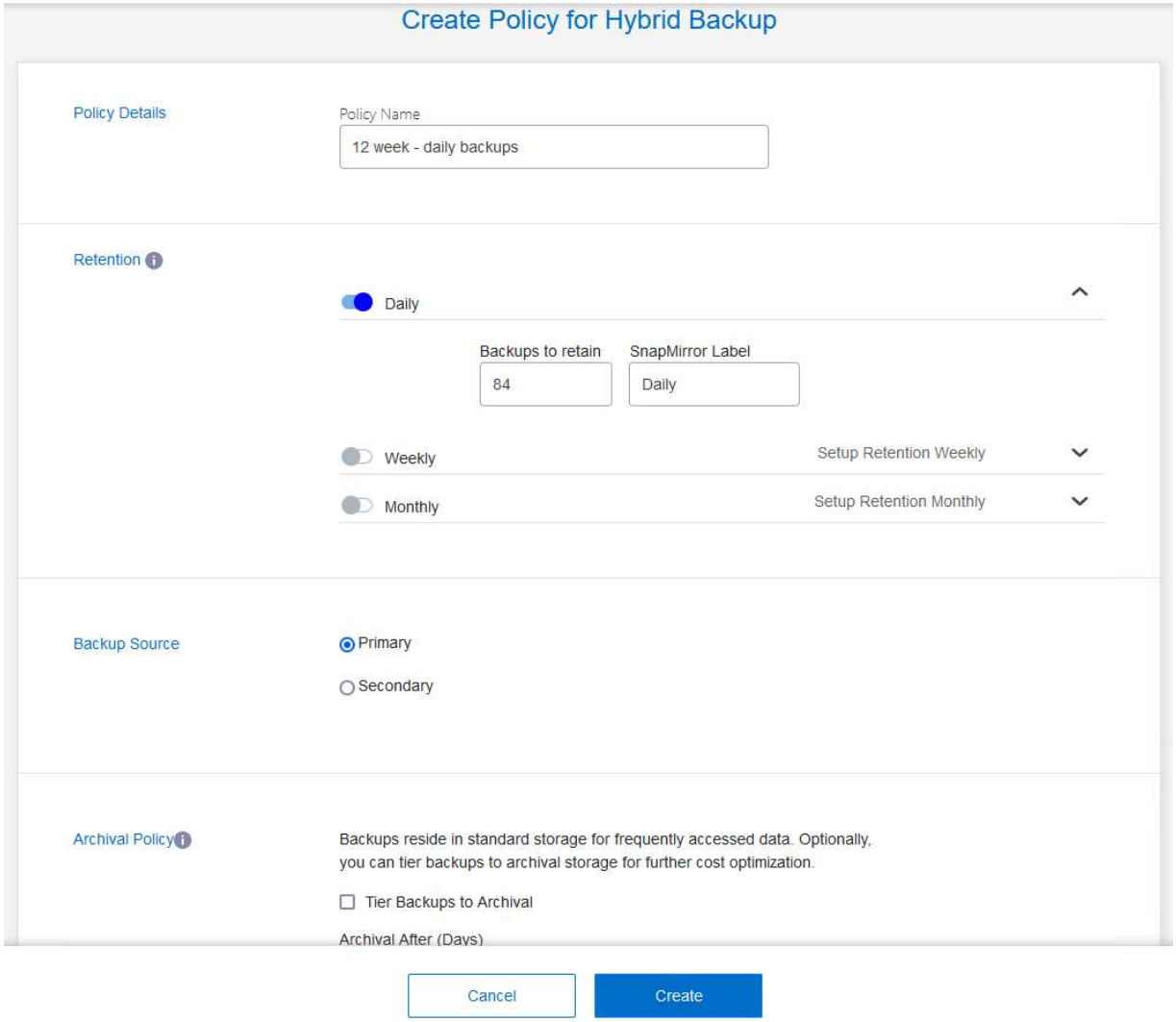
2. をクリックして、[Create Policy for Hybrid Backup]*ウィンドウにアクセスします。

   a. ポリシーの名前を追加します。

   b. 必要な保持期間を選択

   c. バックアップをオンプレミスのプライマリまたはセカンダリONTAPストレージシステムから実行するかどうかを選択します。

   d. 必要に応じて、バックアップをアーカイブストレージに階層化してコストをさらに削減する期間を指定します。



ここで入力したSnapMirrorラベルは、ポリシーを適用するバックアップを識別するために使用されます。ラベル名は、対応するオンプレミスSCVポリシー内のラベル名と一致する必要があります。

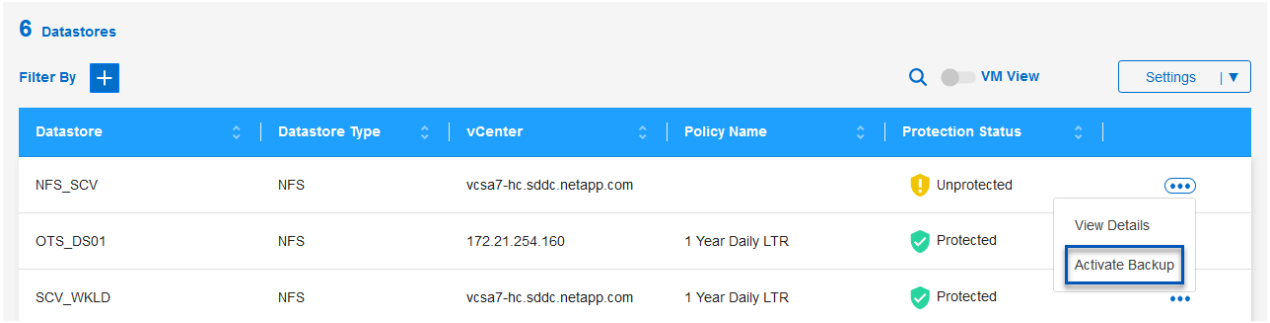
3. [作成]*をクリックしてポリシーの作成を完了します。

Amazon Web Servicesへのデータストアのバックアップ

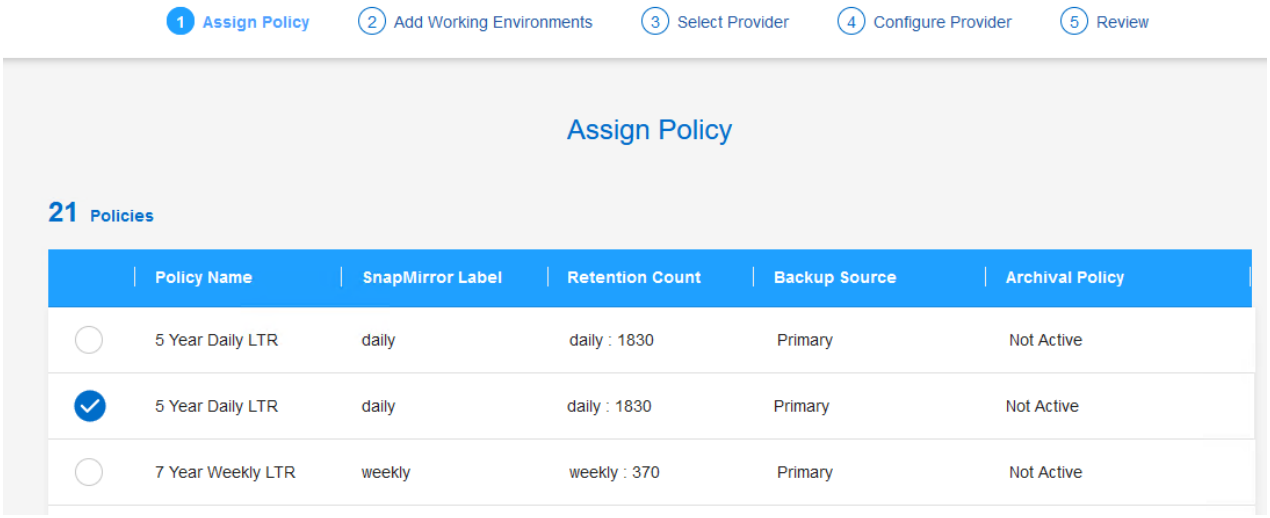
最後に、個 々 のデータストアおよび仮想マシンのデータ保護をアクティブ化します。次の手順は、AWSへのバックアップをアクティブ化する方法の概要です。

詳細については、を参照してください。 "データストアをAmazon Web Servicesにバックアップする"。

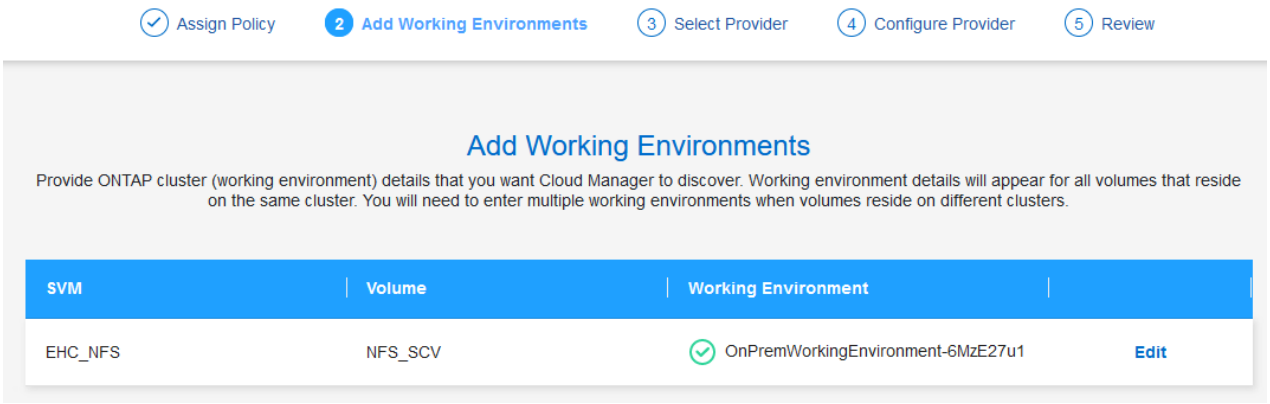
1. BlueXPの仮想マシンのバックアップとリカバリのメインページで、バックアップするデータストアの設定ドロップダウンにアクセスし、*[バックアップのアクティブ化]*を選択します。



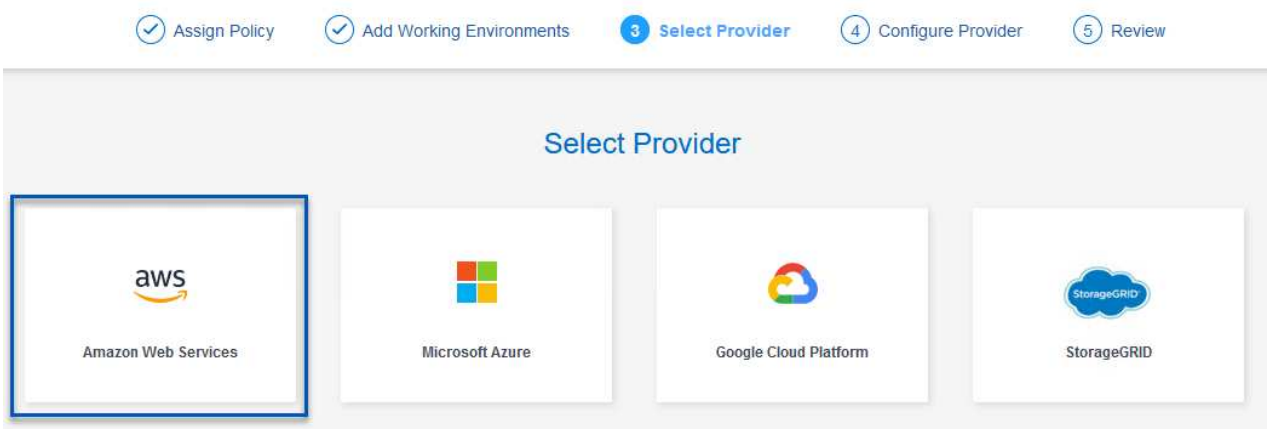
2. データ保護処理に使用するポリシーを割り当てて、*[次へ]*をクリックします。



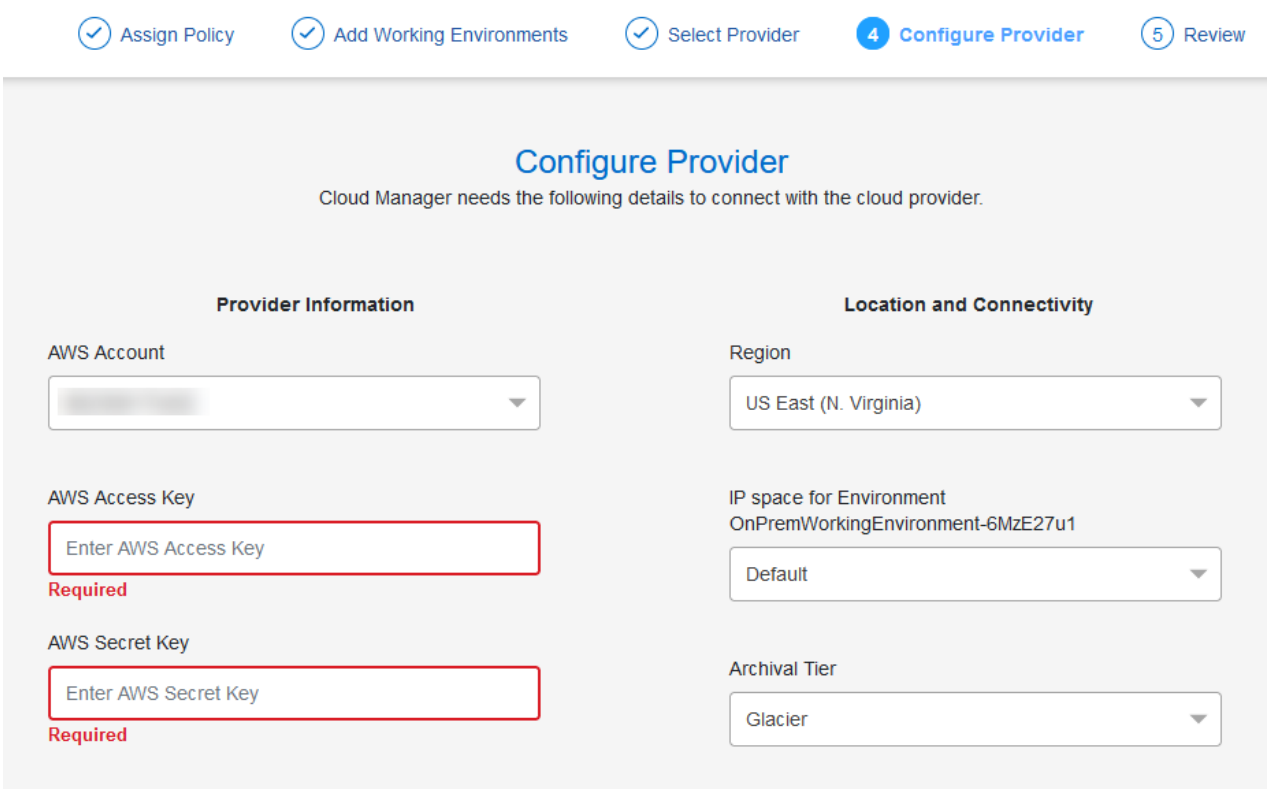
3. 以前に作業環境が検出された場合は、[作業環境の追加]*ページにチェックマークが付いたデータストアと作業環境が表示されます。作業環境がまだ検出されていない場合は、ここに追加できます。[次へ]*をクリックして続行します。



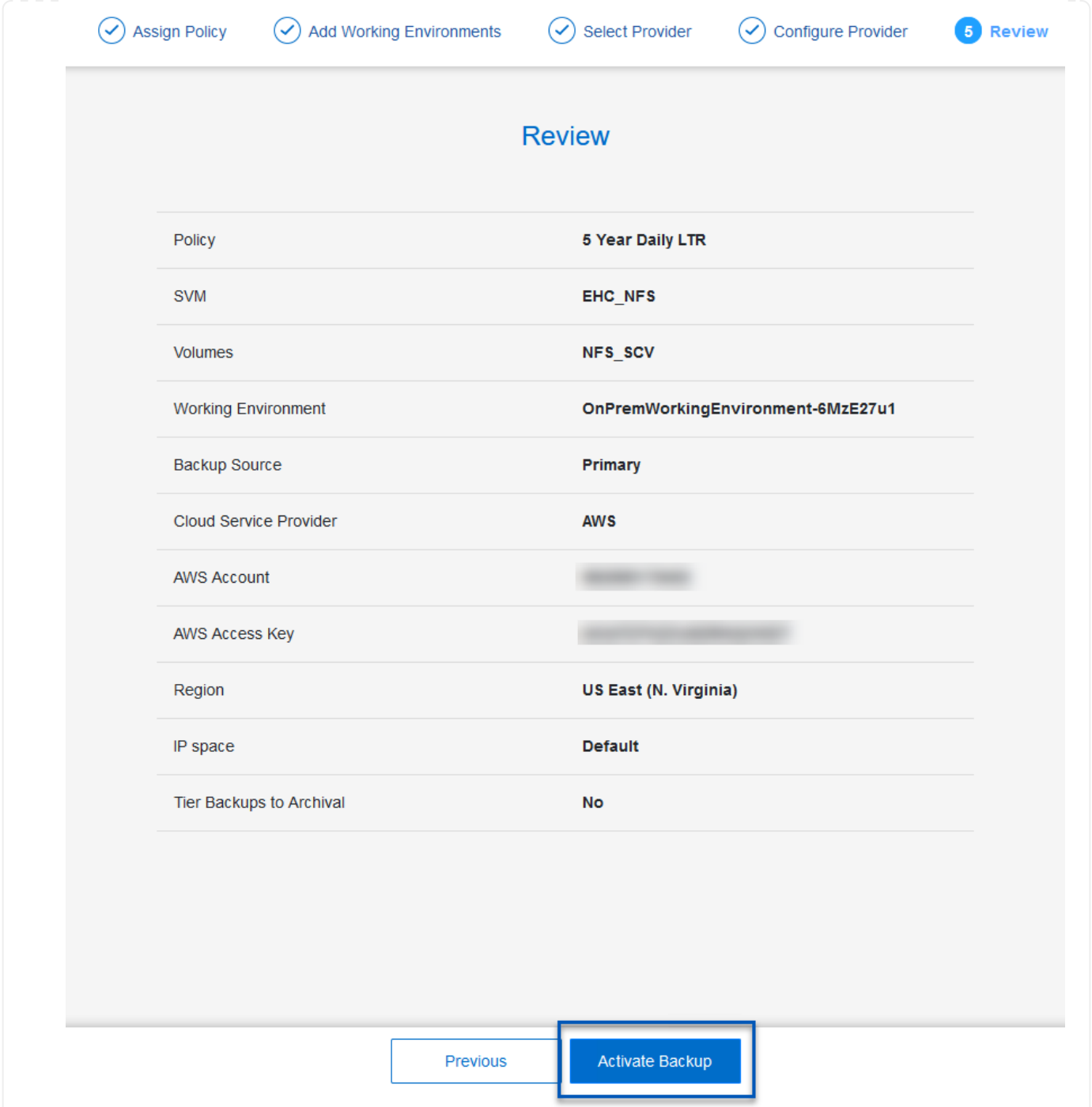
4. ページで、**AWS**をクリックし、[Next]*ボタンをクリックして次に進みます。



5. AWSのプロバイダ固有のクレデンシャル情報（AWSアクセスキーとシークレットキー、リージョン、アーカイブ層など）を入力します。また、オンプレミスのONTAPストレージシステムのONTAP IPスペースを選択します。[次へ]*をクリックします。



6. 最後に、バックアップジョブの詳細を確認し、*[バックアップをアクティブ化]*ボタンをクリックしてデータストアのデータ保護を開始します。



この時点では、データ転送がすぐに開始されない場合があります。BlueXPのバックアップ/リカバリは、未完了のSnapshotを1時間ごとにスキャンし、オブジェクトストレージに転送します。

データ損失時の仮想マシンのリストア

データの保護を確実にすることは、包括的なデータ保護の1つの側面にすぎません。同様に、データ損失やランサムウェア攻撃が発生した場合に、任意の場所からデータを迅速にリストアできることも重要です。この機能は、シームレスなビジネス運用を維持し、目標復旧時点（RPO）を達成するために不可欠です。

NetAppは、柔軟性に優れた3-2-1戦略を提供し、プライマリ、セカンダリ、オブジェクトの各ストレージの保持スケジュールをカスタマイズして管理します。この戦略により、データ保護アプローチを特定のニーズに合わせて柔軟に調整できます。

このセクションでは、仮想マシンのSnapCenter Plug-in for VMware vSphereとBlueXPの両方からのデータリストアプロセスの概要を説明します。

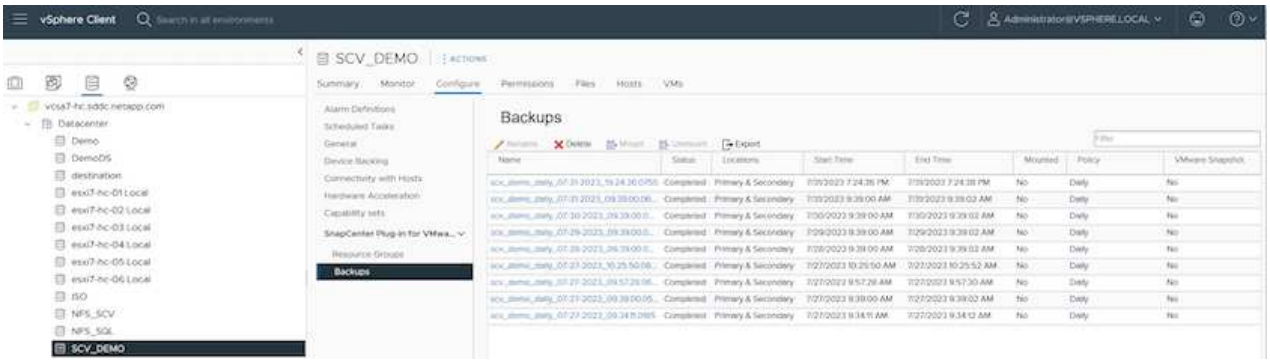
SnapCenter Plug-in for VMware vSphereからの仮想マシンのリストア

この解決策仮想マシンは、元の場所と別の場所にリストアされました。SCVのデータリストア機能のすべての側面がこの解決策でカバーされるわけではありません。SCVが提供しなければならないすべての詳細については、 "バックアップから VM をリストアする" を参照してください。

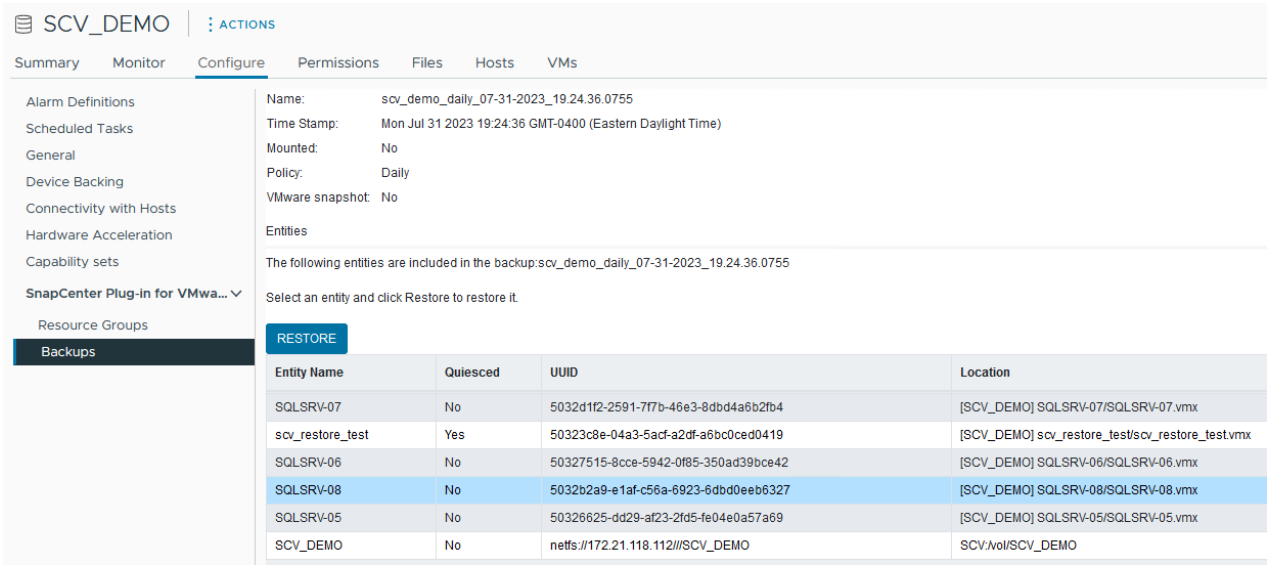
SCVからの仮想マシンのリストア

プライマリストレージまたはセカンダリストレージから仮想マシンをリストアするには、次の手順を実行します。

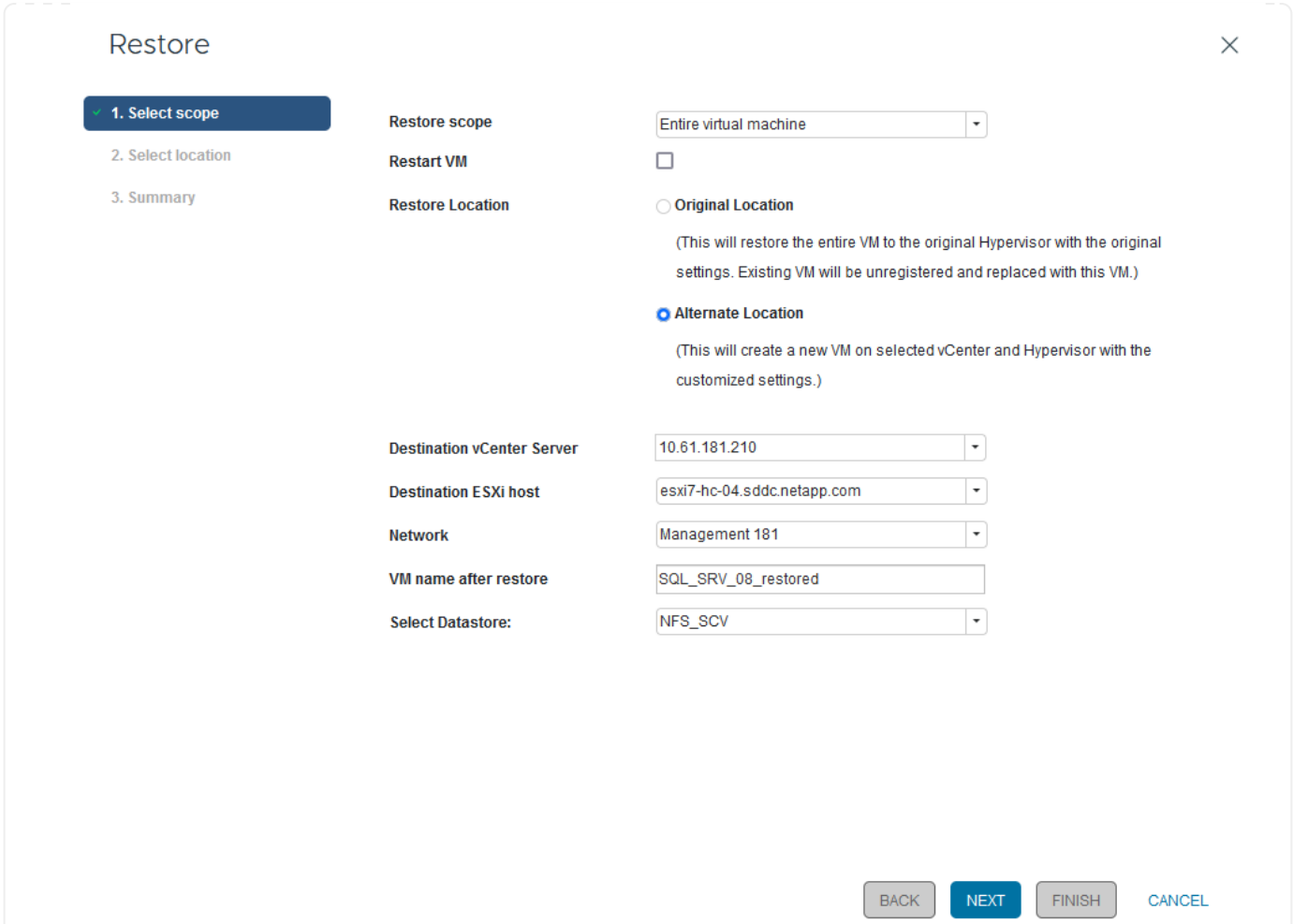
1. vCenter Clientで、*[インベントリ]>[ストレージ]*に移動し、リストアする仮想マシンが格納されているデータストアをクリックします。
2. [設定]タブで*[バックアップ]*をクリックして、使用可能なバックアップのリストにアクセスします。



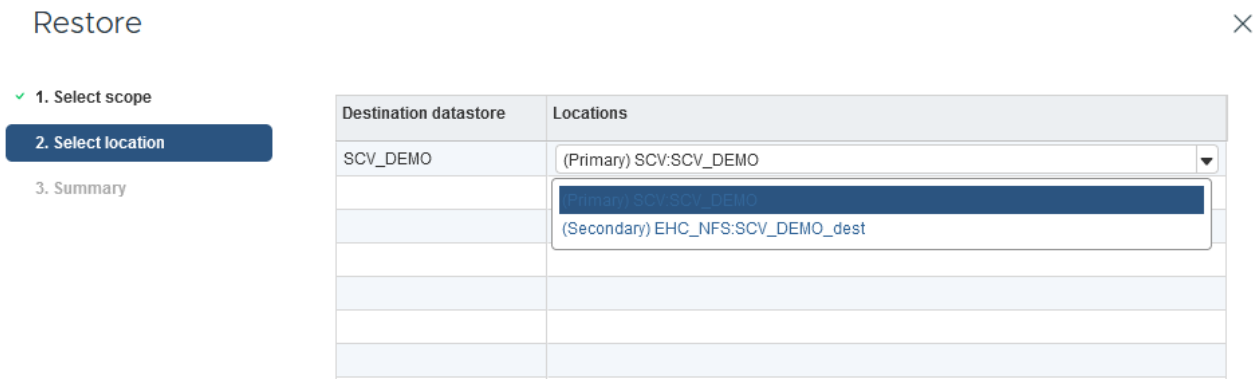
3. バックアップをクリックしてVMのリストにアクセスし、リストアするVMを選択します。[リストア]*をクリックします。



4. [Restore]ウィザードで、仮想マシン全体または特定のVMDKをリストアする場合に選択します。元の場所または別の場所にインストールする場合は、リストア後にVM名を指定し、デスティネーションデータストアを選択します。「 * 次へ * 」をクリックします。



5. プライマリストレージとセカンダリストレージのどちらからバックアップするかを選択します。



6. 最後に、バックアップジョブの概要を確認し、[Finish]をクリックしてリストアプロセスを開始します。

仮想マシンの**BlueXP**バックアップおよびリカバリからの仮想マシンのリストア

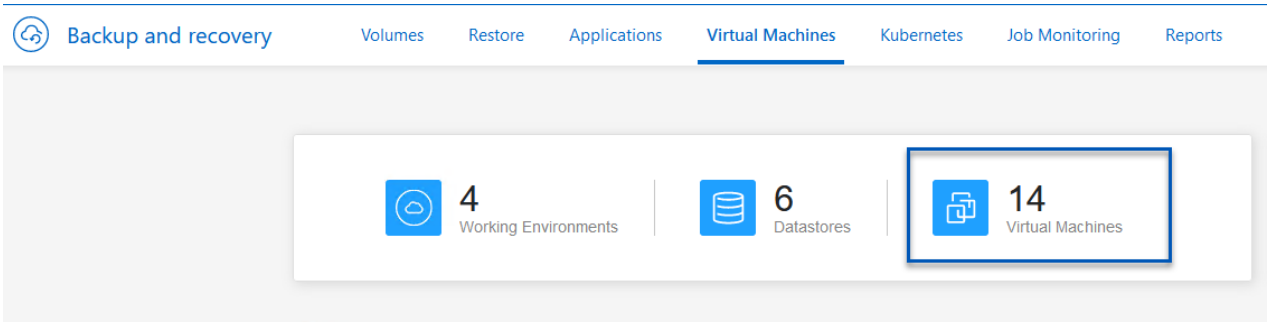
BlueXPでは、仮想マシンのバックアップとリカバリ機能を使用して、仮想マシンを元の場所にリストアできます。リストア機能には、BlueXPのWebコンソールからアクセスできます。

詳細については、を参照してください。 "仮想マシンのデータをクラウドからリストア"。

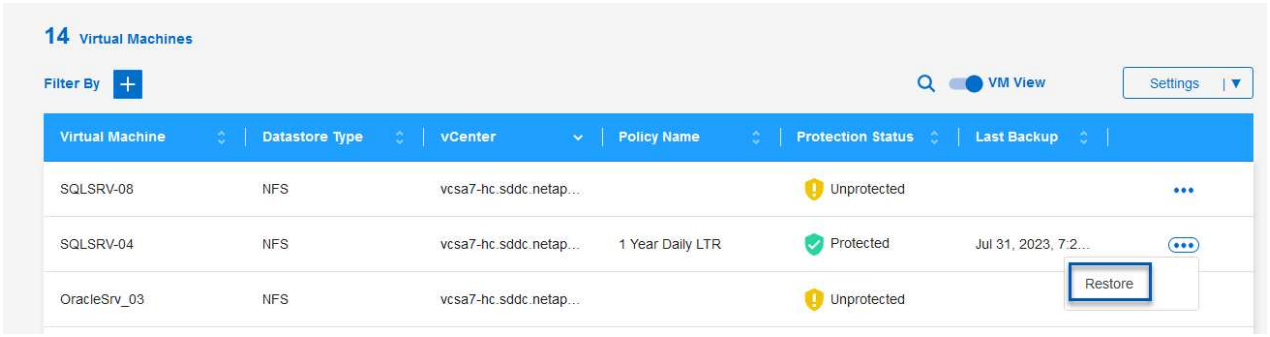
BlueXPのバックアップとリカバリから仮想マシンをリストア

BlueXPのバックアップとリカバリから仮想マシンをリストアするには、次の手順を実行します。

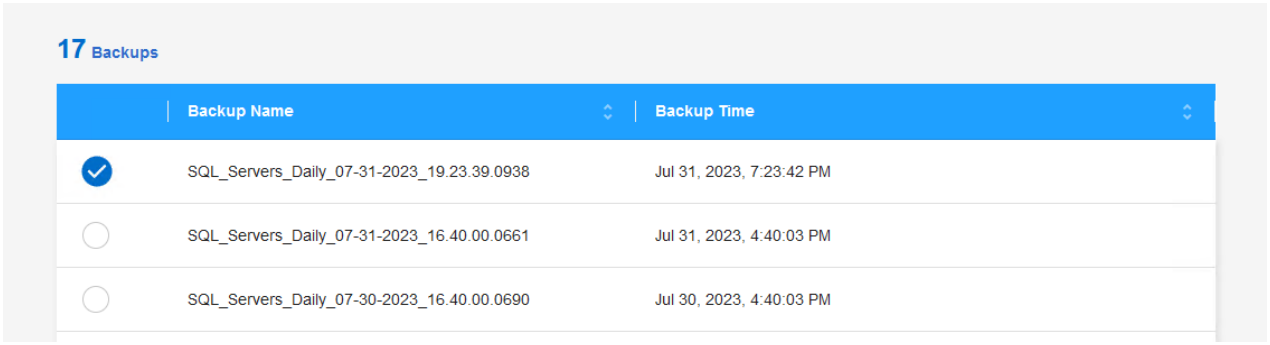
1. [保護]>[バックアップとリカバリ]>[仮想マシン]*に移動し、[仮想マシン]をクリックしてリストア可能な仮想マシンのリストを表示します。



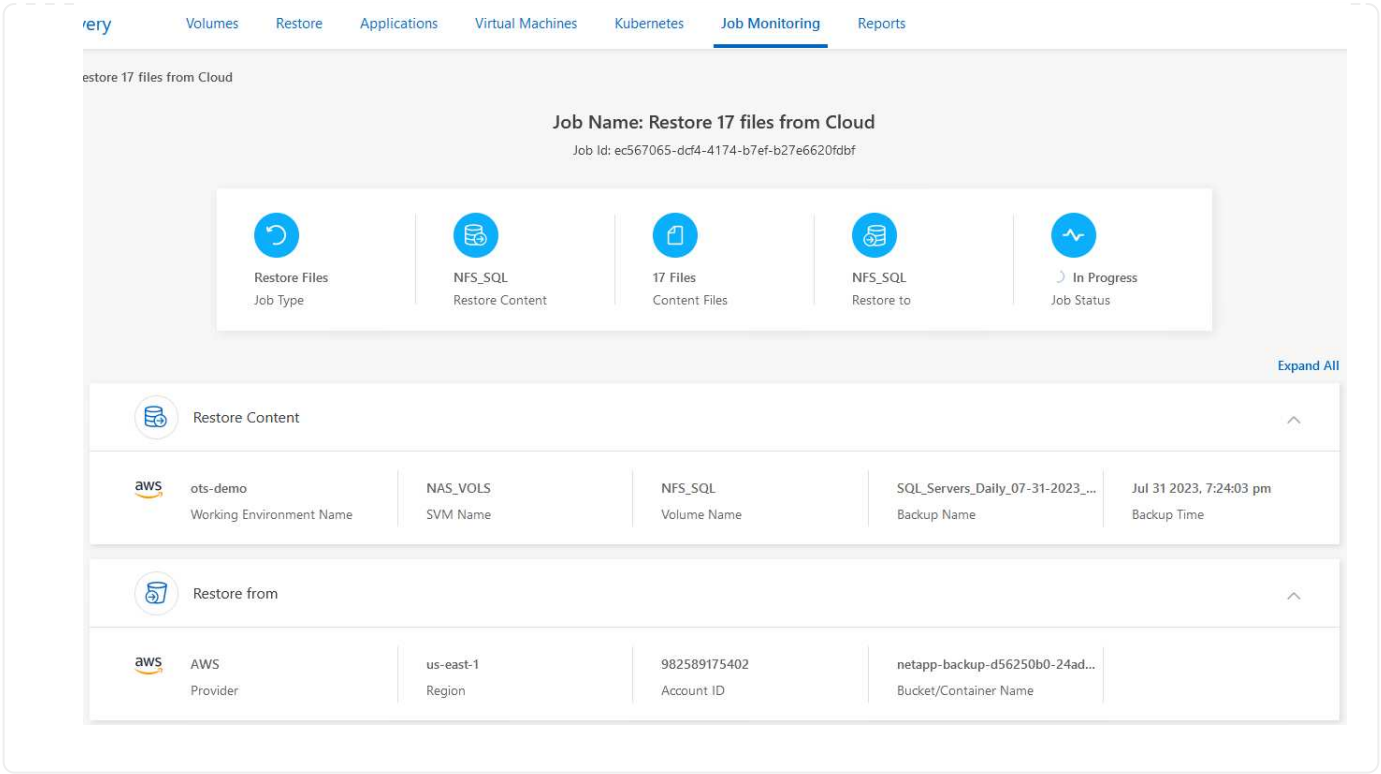
2. リストアするVMの設定ドロップダウンメニューにアクセスし、



3. リストア元のバックアップを選択し、*[Next]*をクリックします。



4. バックアップジョブの概要を確認し、*[リストア]*をクリックしてリストアプロセスを開始します。
5. [ジョブ監視]*タブでリストアジョブの進捗状況を監視します。



まとめ

3-2-1のバックアップ戦略をSnapCenter Plug-in for VMware vSphereとBlueXPで仮想マシンのバックアップとリカバリを実装すると、堅牢で信頼性に優れ、対費用効果の高い解決策でデータを保護できます。この戦略により、データの冗長性とアクセス性が確保されるだけでなく、場所を問わず、オンプレミスのONTAPストレージシステムとクラウドベースのオブジェクトストレージの両方からデータを柔軟にリストアできます。

本ドキュメントで紹介するユースケースは、NetApp、VMware、主要なクラウドプロバイダの統合に焦点を当てた、実績のあるデータ保護テクノロジに焦点を当てています。SnapCenter Plug-in for VMware vSphereは、VMware vSphereとシームレスに統合されるため、データ保護処理を効率的かつ一元的に管理できます。この統合により、仮想マシンのバックアップおよびリカバリプロセスが合理化され、VMwareエコシステム内でのスケジュール設定、監視、柔軟なリストア操作が容易になります。BlueXPの仮想マシン向けバックアップ/リカバリ機能は、仮想マシンのデータをエアギャップで保護してクラウドベースのオブジェクトストレージにバックアップすることで、3-2-1に1つの機能を提供します。直感的なインターフェイスと論理ワークフローにより、重要なデータを長期的にアーカイブするためのセキュアなプラットフォームが提供されます。

追加情報

この解決策 に記載されているテクノロジの詳細については、次の追加情報 を参照してください。

- "SnapCenter Plug-in for VMware vSphere のドキュメント"
- "BlueXPのマニュアル"

VMwareソブリンクラウド

ソブリンクラウド向け**VMware**リソース

NetAppとVMwareソブリンクラウド

VMware Sovereign Cloudの概要

国や州の政府、規制の厳しい業界（金融や医療など）など、機密性の高いデータを処理、維持する多くの企業にとって、クラウドコンピューティングに必要なコンポーネントとして主権の概念が登場しています。政府はまた、デジタル経済能力を拡大し、クラウドサービスに対する多国籍企業への依存を減らすことを目指しています。

VMwareソブリンクラウドイニシアチブ

VMwareは、ソブリンクラウドを次のようなメリットの1つとして定義

- 民間部門と公共部門の両方の組織にとって重要なデータ（国のデータ、企業データ、個人データなど）の価値を保護し、最大限に引き出す
- デジタル経済に国家的な能力を提供する
- 監査されたセキュリティ管理でデータを保護
- データプライバシー法へのコンプライアンスを確保
- データの常駐とデータ主権の両方を管轄区域全体で管理することで、データの制御性を向上

信頼できるVMwareソブリンクラウドサービスプロバイダとのパートナーシップ

成功を確実にするには、信頼できる、独立した信頼できるクラウドプラットフォームをホスティングできるパートナーと協力する必要があります。VMware Sovereign Cloudイニシアチブで認められたVMwareクラウドプロバイダは、VMware Sovereign Cloudフレームワークで概説されている主要な原則とベストプラクティスを具体化した、最新のソフトウェア定義アーキテクチャに基づいたクラウドソリューションの設計と運用に取り組んでいます。

- データ主権と管轄権–すべてのデータは居住者であり、そのデータが収集された国の排他的な管理と権限の対象となります。管轄区域内で運用を完全に管理
- データアクセスと整合性–クラウドインフラストラクチャは耐障害性に優れており、管轄区域内の少なくとも2つのデータセンターロケーションで利用でき、セキュアでプライベートな接続オプションを利用できます。
- データセキュリティとコンプライアンス–情報セキュリティ管理システムの制御は、業界で認められたグローバル（または地域）基準に照らして認定され、定期的に監査されます。
- データの独立性と移動性–最新のアプリケーションアーキテクチャをサポートし、ベンダーのクラウドロックインを防ぎ、アプリケーションのモビリティと独立性を実現

VMwareの詳細については、次のサイトを参照してください。

- "VMware Sovereign Cloudの概要"
- "VMware Sovereign Cloudとは"
- "新しいVMware Sovereign Cloud Initiativeのご紹介"
- "VMware Sovereign Cloudに関するテクニカルホワイトペーパー"

NetppとVMware Sovereign Cloud：ユースケース

NetAppは、複数のNetAppテクノロジを統合することで、VMwareソブリンクラウドの概念をサポートします。

VMwareソブリンクラウドとのNetAppテクノロジ統合の詳細については、次のリンクを参照してください。

- "オブジェクトストア拡張機能としてのNetApp StorageGRID"

オブジェクトストア拡張機能としての**NetApp StorageGRID**

NetAppは、VMwareと協力してNetApp StorageGRIDをVMware Cloud Directorに統合し、VMwareソブリンクラウドをサポートしています。このVMware Cloud Directorのプラグインを使用すると、サービスプロバイダは、ユースケースに関係なくStorageGRIDをオブジェクトストレージ製品として使用できます。また、サービスプロバイダが提供カタログの他の部分を管理するために使用するのと同じVMwareマルチテナント解決策（VMware Cloud Director）を使用してStorageGRIDを管理できます。

VMwareソブリンクラウドを提供するパートナーは、NetApp StorageGRIDを選択して、非構造化データを使用したクラウド環境の管理と保守を支援できます。Amazon S3 APIなどの業界標準のAPIをネイティブにサポートしているため、幅広いクラウド環境間でのスムーズな相互運用性が確保されます。また、自動化されたライフサイクル管理などの独自のイノベーションにより、非構造化データのより対費用効果の高い保護、ストレージ、長期保存が保証されます。

クラウドディレクタープロバイダのお客様とネットアップのソブリンクラウド統合により、次のようなメリットが得られます。

- メタデータを含む機密データを主権の下に保持しながら、データプライバシー法に違反する可能性のある外国当局によるアクセスを防止します。
- セキュリティとコンプライアンスの強化：急速に進化する攻撃ベクトルからアプリケーションとデータを保護しながら、信頼できるローカル企業との継続的なコンプライアンスを維持します。インフラストラクチャ、組み込みフレームワーク、地域の専門家。
- 将来を見据えたインフラ：変化するデータプライバシー規制、セキュリティ上の脅威、地政学に迅速に対応できます。
- 安全なデータ共有と分析によってデータの価値を最大限に引き出し、プライバシー法に違反することなくイノベーションを推進できます。データの整合性が保護され、正確な分析情報が得られます。

StorageGRIDとの統合の詳細については、以下を参照してください。

- "NetAppの発表"

ネットアップのハイブリッドマルチクラウドと**Red Hat OpenShift Container**ワークロード

Red Hat OpenShift Containerワークロード向けのネットアップハイブリッドマルチクラウドソリューション

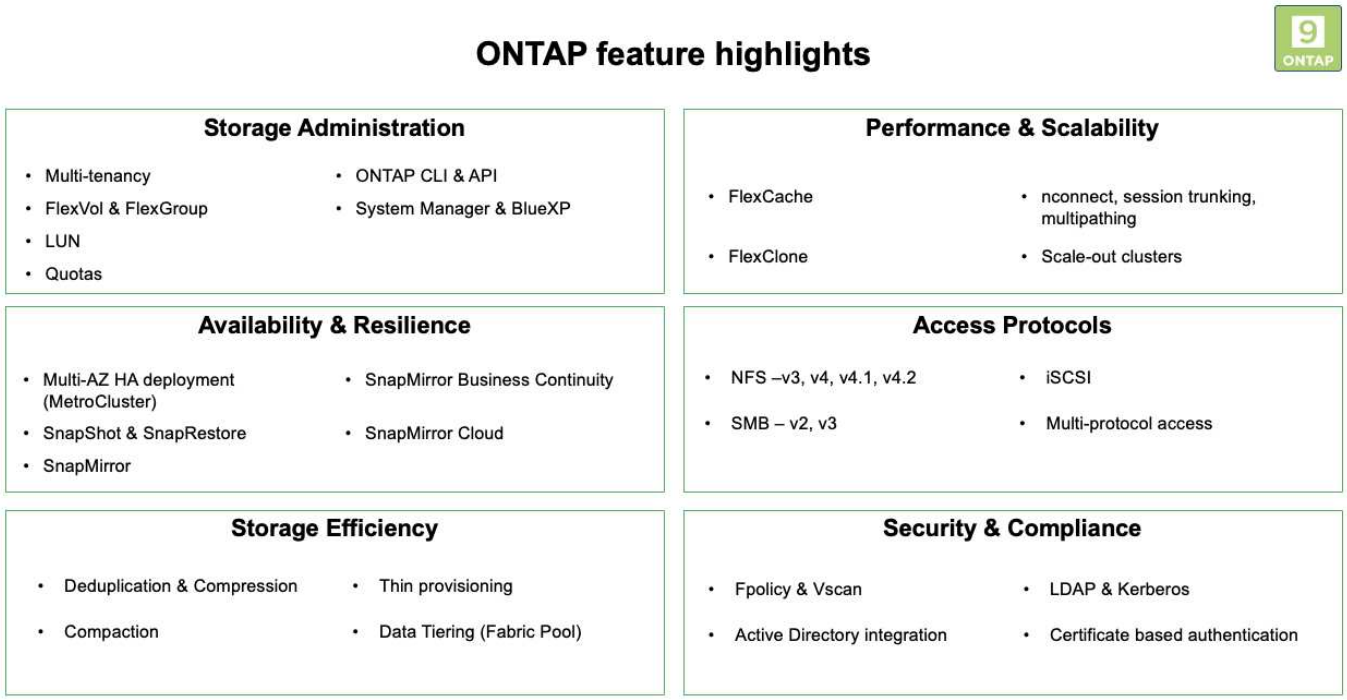
概要

ネットアップでは、従来型エンタープライズアプリケーションを最新化し、Kubernetesを中心に構築された

コンテナとオーケストレーションプラットフォームを使用して新しいアプリケーションを構築するお客様が大幅に増えています。Red Hat OpenShift Container Platformは、多くのお客様に採用されている例の1つです。

企業内でコンテナを採用するお客様がますます増えています。ネットアップは、ステートフルアプリケーションの永続的ストレージのニーズに加え、データ保護、データセキュリティ、データ移行などの従来のデータ管理のニーズにも応えることができます。しかし、これらのニーズは、さまざまな戦略、ツール、方法を使用して満たしています。

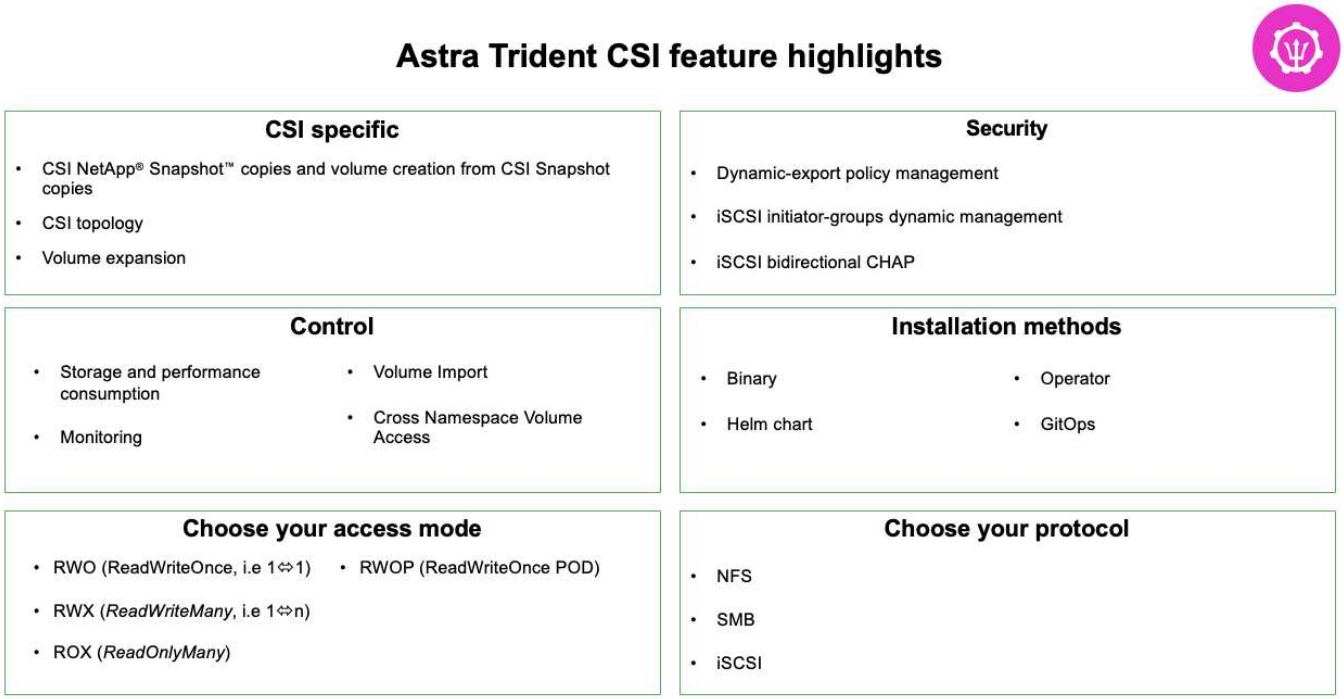
- NetApp ONTAP **ベースのストレージオプションを次に示します。コンテナとKubernetes環境にセキュリティ、データ保護、信頼性、柔軟性を提供します。
  - オンプレミスの自己管理型ストレージ：
- ネットアップファブリック接続ストレージ（FAS ）、ネットアップオールフラッシュFAS アレイ（AFF ）、ネットアップオールSANアレイ（ASA ）、ONTAP Select
  - オンプレミスのプロバイダ管理ストレージ：
- NetApp Keystone が提供するストレージサービス（STaaS）
  - クラウド内の自己管理型ストレージ：
- NetApp Cloud Volumes ONTAP（CVO）は、ハイパースケーラに自己管理型ストレージを提供します
  - クラウド上のプロバイダが管理するストレージ：
- Cloud Volumes Service for Google Cloud（CVS）、Azure NetApp Files （ANF）、Amazon FSx for NetApp ONTAP は、ハイパースケーラにフルマネージドストレージを提供します



- NetApp BlueXP **を使用すると、すべてのストレージ資産とデータ資産を単一のコントロールプレーン/インターフェイスから管理できます。

BlueXPを使用して、クラウドストレージ（Cloud Volumes ONTAP やAzure NetApp Files など）の作成と管理、データの移動、保護、分析、オンプレミスやエッジの多くのストレージデバイスの管理を行うことができます。

- NetApp Astra Trident **はCSI準拠のストレージオーケストレーションツールです。上記のさまざまなネットアップストレージオプションを利用して、永続的ストレージをすばやく簡単に利用できます。ネットアップが保守、サポートしているオープンソースのソフトウェアです。



ビジネスクリティカルなコンテナワークロードに必要なのは、永続的ボリュームだけではありません。同社のデータ管理要件では、アプリケーションのKubernetesオブジェクトの保護と移行も必要です。

アプリケーションデータには、ユーザデータに加えてKubernetesオブジェクトが含まれます。例を次に示します。 -ポッド仕様、PVC、デプロイ、サービスなどのKubernetesオブジェクト- 設定マップやシークレットなどのカスタム設定オブジェクト- Snapshotコピー、バックアップ、クローンなどの永続的データ- CRSやCRDなどのカスタムリソース

- NetApp Astra Control **は、フルマネージドと自己管理型の両方のソフトウェアとして提供され、堅牢なアプリケーションデータ管理のためのオーケストレーションを提供します。を参照してください "Astra のドキュメント" を参照してください。

このリファレンスドキュメントでは、NetApp Astra Control Centerを使用して、Red Hat OpenShiftコンテナプラットフォームに導入されたコンテナベースアプリケーションの移行と保護について検証します。また、解決策 では、コンテナプラットフォームを管理するためのRed Hat Advanced Cluster Management（ACM）の導入と使用に関する詳細についても説明しています。また、Astra Trident CSIプロビジョニングツールを使用して、ネットアップストレージとRed Hat OpenShiftコンテナプラットフォームを統合する方法についても詳しく説明します。Astra Control Centerはハブクラスタに導入され、コンテナアプリケーションとその永続的ストレージライフサイクルの管理に使用されます。最後に、Amazon FSx for NetApp ONTAP （FSxN）を永続的ストレージとして使用し、AWS（ROSA）のマネージドRed Hat OpenShiftクラスタ上のコンテナワークロードのレプリケーション、フェイルオーバー、フェイルバックのための解決策 を提供します。

Red Hat OpenShift Containerワークロード向けネットアップハイブリッドマルチクラウドソリューションの価値提案

ほとんどのお客様は、既存のインフラがない状態でKubernetesベースの環境を構築し始めたばかりではありません。おそらく、大規模なVMware環境などで、エンタープライ

ズアプリケーションのほとんどを仮想マシンで実行している従来型のIT環境です。その後、最新のアプリケーション開発チームのニーズを満たすために、小規模なコンテナベースの環境の構築を開始します。これらのイニシアチブは通常、小規模なものから始まり、チームがこれらの新しいテクノロジやスキルを学習し、それらを採用することの多くの利点を認識し始めるにつれて、より普及し始めます。ネットアップなら両方の環境のニーズに対応できるというのは、お客様にとって朗報です。Red Hat OpenShiftを使用したこのハイブリッドマルチクラウド向けソリューションセットは、ネットアップのお客様がインフラや組織全体を刷新することなく、最新のクラウドテクノロジとサービスを採用できるよう支援します。お客様のアプリケーションやデータがオンプレミスでホストされている場合でも、クラウドでホストされている場合でも、仮想マシンで実行されている場合でも、コンテナで実行される場合でも、ネットアップは一貫したデータ管理、保護、セキュリティ、モビリティを提供します。これらの新しいソリューションにより、ネットアップが数十年にわたってオンプレミスのデータセンター環境で提供してきたのと同じ価値を、企業全体のデータホライズン全体で利用できるようになります。ツールの再構築、新しいスキルの習得、新しいチームの構築に多額の投資を行う必要はありません。ネットアップは、お客様がクラウドへの移行のどの段階にいるかにかかわらず、これらのビジネス上の課題を解決できるよう、適切に位置付けられています。

Red Hat OpenShiftを使用したネットアップハイブリッドマルチクラウド：

- ネットアップベースのストレージソリューションでRed Hat OpenShiftを使用する場合に、お客様がデータとアプリケーションを管理、保護、保護、保護、移行するための最良の方法を実証する事前検証済みの設計と手法をお客様に提供します。
- VMware環境、ベアメタルインフラ、またはその両方でネットアップストレージを使用してRed Hat OpenShiftを実行しているお客様向けのベストプラクティスを紹介します。
- オンプレミス環境とクラウド環境、およびその両方を使用するハイブリッド環境の両方について、戦略とオプションを説明する。

Red Hat OpenShift Containerワークロード向けのネットアップハイブリッドマルチクラウドのサポート対象ソリューション

解決策 は、OpenShiftコンテナプラットフォーム（OCP）、OpenShift Advanced Cluster Manager（ACM）、NetApp ONTAP 、NetApp BlueXP、NetApp Astra Control Center（ACC）を使用した移行と一元的なデータ保護のテストと検証を行います。

この解決策 では、次のシナリオがネットアップによってテストおよび検証されます。解決策 は、次の特性に基づいて複数のシナリオに分けられます。

- オンプレミス
- クラウド
  - 自己管理型OpenShiftクラスタと自己管理型ネットアップストレージ
  - プロバイダが管理するOpenShiftクラスタとプロバイダが管理するネットアップストレージ

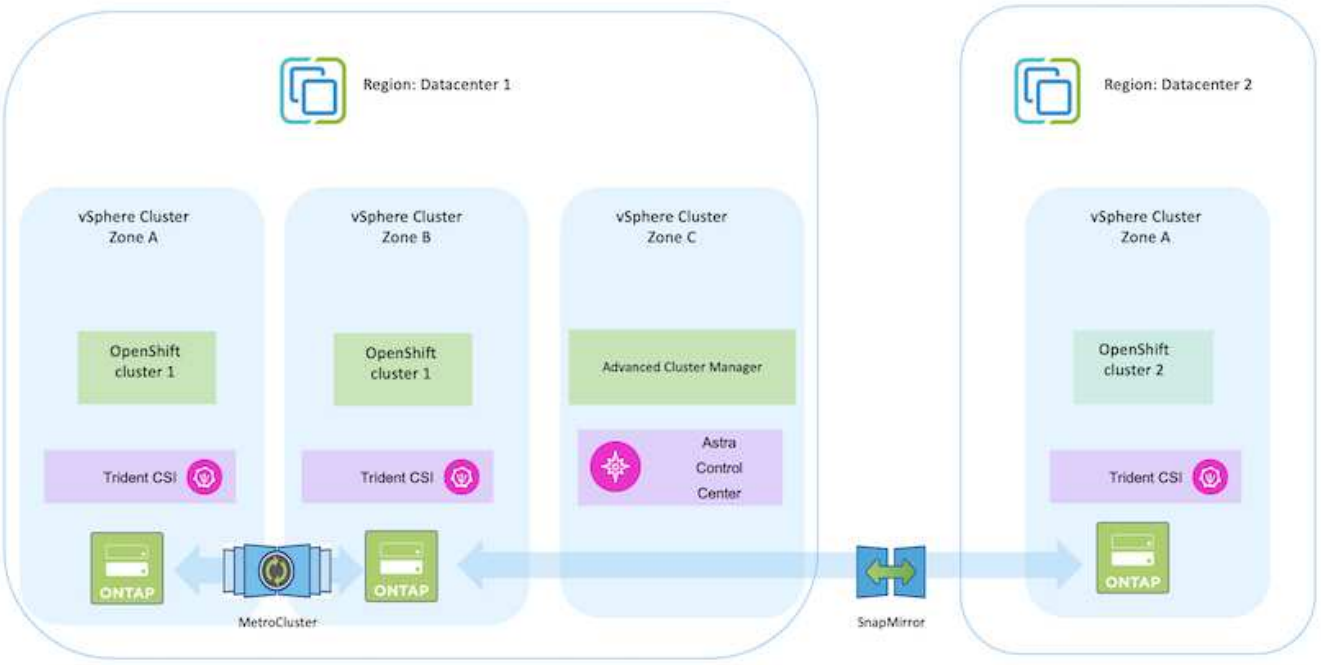
今後、追加のソリューションとユースケースを構築していきます。

シナリオ**1**：**ACC**を使用したオンプレミス環境内でのデータ保護と移行

オンプレミス：自己管理型**OpenShift**クラスタと自己管理型ネットアップストレージ

- ACCを使用して、データ保護のためにSnapshotコピー、バックアップ、リストアを作成します。
- ACCを使用して、コンテナアプリケーションのSnapMirrorレプリケーションを実行します。

シナリオ **1**

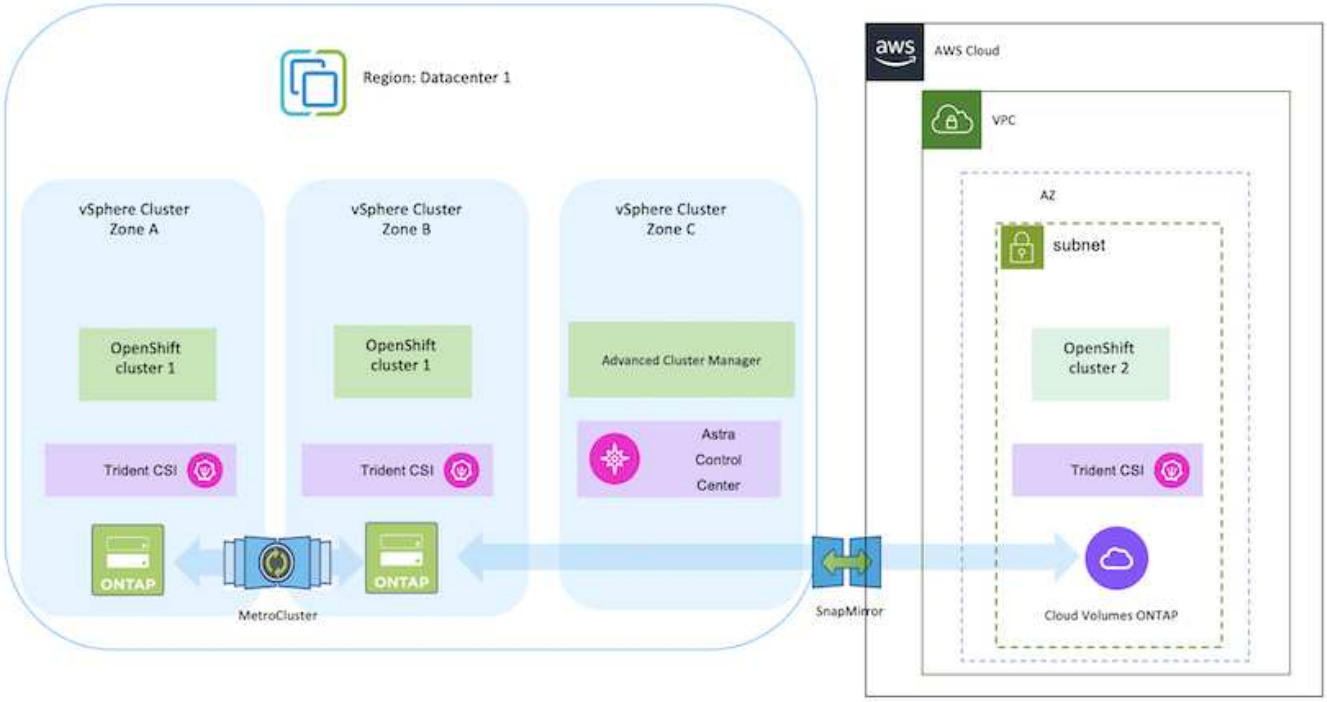


シナリオ**2**：**ACC**を使用したオンプレミス環境から**AWS**環境へのデータ保護と移行

オンプレミス：自己管理型**OpenShift**クラスタと自己管理型ストレージ AWSクラウド：自己管理型OpenShiftクラスタと自己管理型ストレージ**

- ACCを使用して、データ保護のためのバックアップとリストアを実行します。
- ACCを使用して、コンテナアプリケーションのSnapMirrorレプリケーションを実行します。

シナリオ **2**

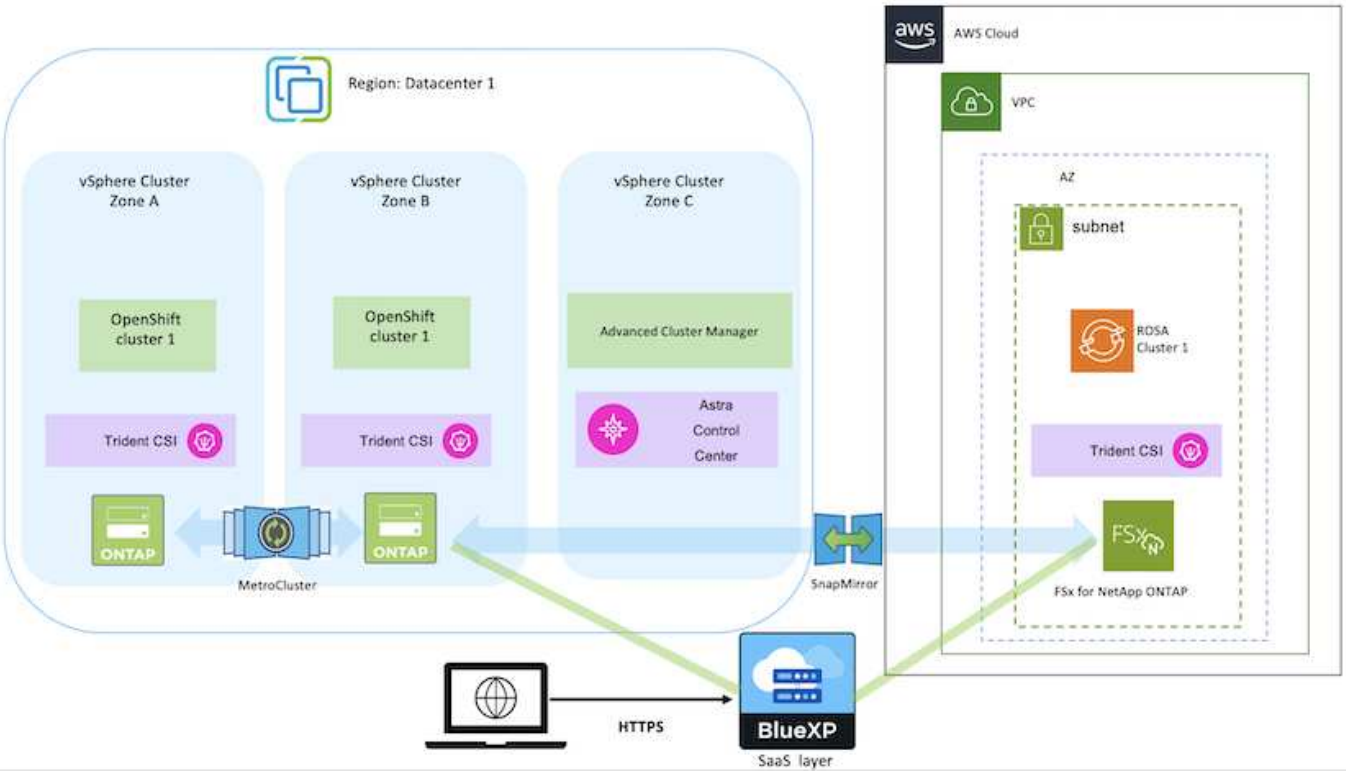


シナリオ**3**：オンプレミス環境から**AWS**環境へのデータ保護と移行

オンプレミス：自己管理型**OpenShift**クラスタと自己管理型ストレージ AWSクラウド：プロバイダ管理型OpenShiftクラスタ（ROSA）とプロバイダ管理型ストレージ（FSxN）**

- BlueXPを使用して永続ボリュームのレプリケーション（FSxN）を実行
- OpenShift GitOpsを使用して、アプリケーションメタデータを再作成します。

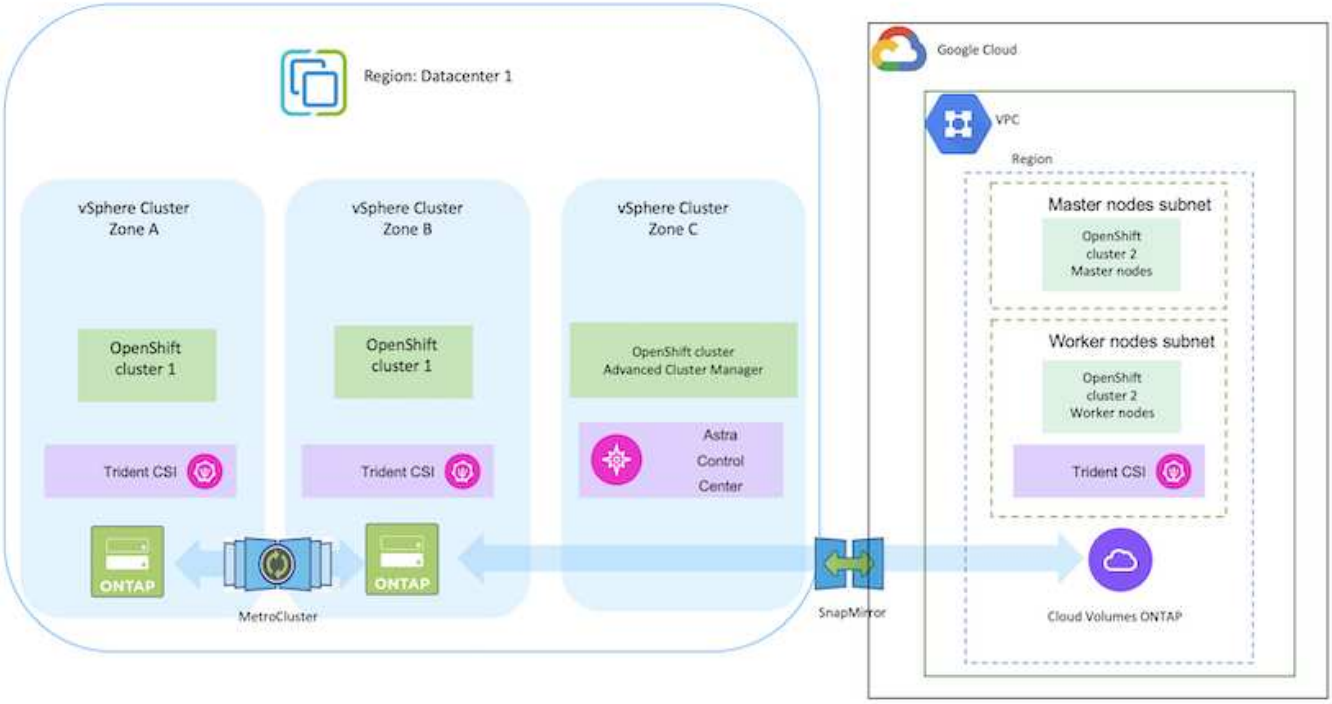
シナリオ**3**



シナリオ**4**：**ACC**を使用したオンプレミス環境から**GCP**環境へのデータ保護と移行

オンプレミス：自己管理型**OpenShift**クラスタと自己管理型ストレージ
Google Cloud：自己管理型**OpenShift**クラスタと自己管理型ストレージ

- ACCを使用して、データ保護のためのバックアップとリストアを実行します。
- ACCを使用して、コンテナアプリケーションのSnapMirrorレプリケーションを実行します。

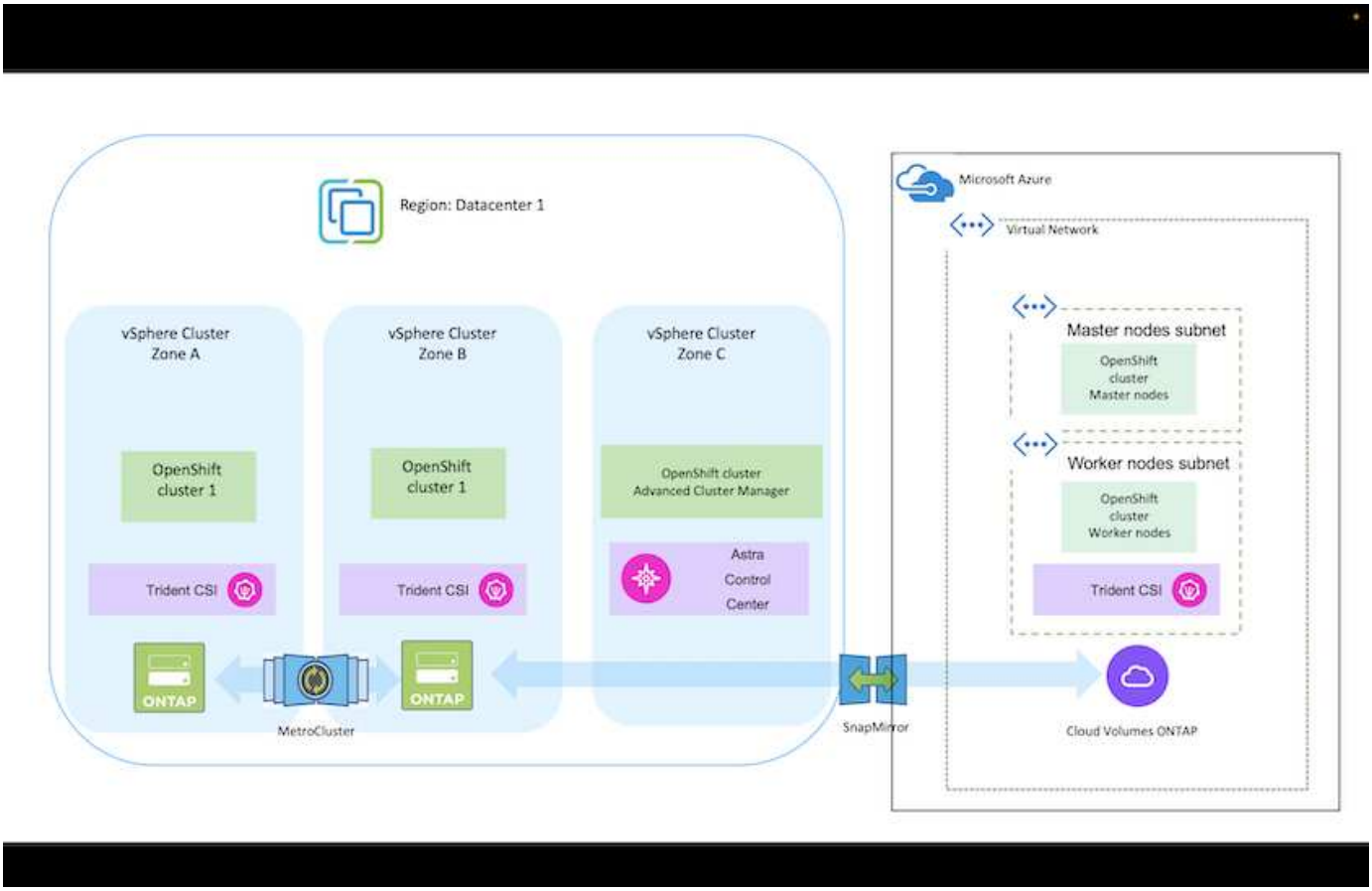


MetroCluster 構成でONTAP を使用する場合の考慮事項については、を参照してください "こちらをご覧ください"。

シナリオ**5**：**ACC**を使用したオンプレミス環境から**Azure**環境へのデータ保護と移行

オンプレミス：自己管理型**OpenShift**クラスタと自己管理型ストレージ
Azureクラウド：自己管理型**OpenShift**クラスタと自己管理型ストレージ

- ACCを使用して、データ保護のためのバックアップとリストアを実行します。
- ACCを使用して、コンテナアプリケーションのSnapMirrorレプリケーションを実行します。



MetroCluster 構成でONTAP を使用する場合の考慮事項については、を参照してください "こちらをご覧ください"。

解決策 検証で使用されるさまざまなコンポーネントのバージョン

解決策 は、OpenShiftコンテナプラットフォーム、OpenShift Advanced Cluster Manager、NetApp ONTAP 、NetApp Astra Control Centerを使用した移行と一元的なデータ保護のテストと検証を行います。

解決策のシナリオ1、2、3は、次の表に示すバージョンを使用して検証されました。

* コンポーネント *	* バージョン *
* VMware *	vSphere Clientバージョン8.0.0.10200 VMware ESXi、8.0.0、20842819
ハブクラスタ	OpenShift 4.11.34
ソースクラスタとデスティネーションクラスタ	オンプレミスとAWSでのOpenShift 4.12.9
* NetApp Astra Trident *	Tridentサーバとクライアント23.04.0
* NetApp Astra Control Center *	ACC 22.11.0-82
* NetApp ONTAP *	ONTAP 9.12.1
* AWS FSx for NetApp ONTAP *	シングルAZ

解決策のシナリオ4は、次の表に示すバージョンを使用して検証されました。

* コンポーネント *	* バージョン *
* VMware *	vSphere Clientバージョン8.0.2.00000 VMware ESXi、8.0.2、22380479
ハブクラスタ	OpenShift 4.13.13
ソースクラスタとデスティネーションクラスタ	OpenShift 4.13.12 オンプレミスとGoogle Cloud
* NetApp Astra Trident *	Tridentサーバおよびクライアント23.07.0
* NetApp Astra Control Center *	ACC 23.07.0-25
* NetApp ONTAP *	ONTAP 9.12.1
* Cloud Volumes ONTAP *	シングルAZ、シングルノード、9.14.0

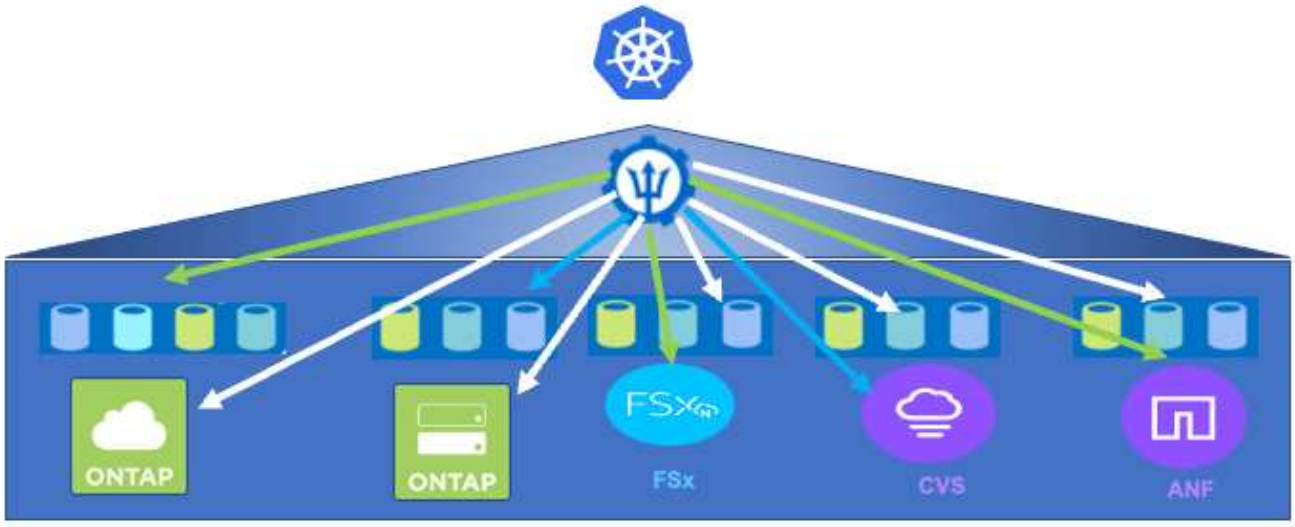
解決策のシナリオ5は、次の表に示すバージョンを使用して検証されました。

* コンポーネント *	* バージョン *
* VMware *	vSphere Clientバージョン8.0.2.00000 VMware ESXi、8.0.2、22380479
ソースクラスタとデスティネーションクラスタ	OpenShift 4.13.25 オンプレミスとAzure
* NetApp Astra Trident *	Tridentサーバとクライアント、Astra Controlプロビジョニングツール23.10.0
* NetApp Astra Control Center *	ACC 23.10
* NetApp ONTAP *	ONTAP 9.12.1
* Cloud Volumes ONTAP *	シングルAZ、シングルノード、9.14.0

Red Hat OpenShift Containersとのネットアップストレージ統合がサポートされています

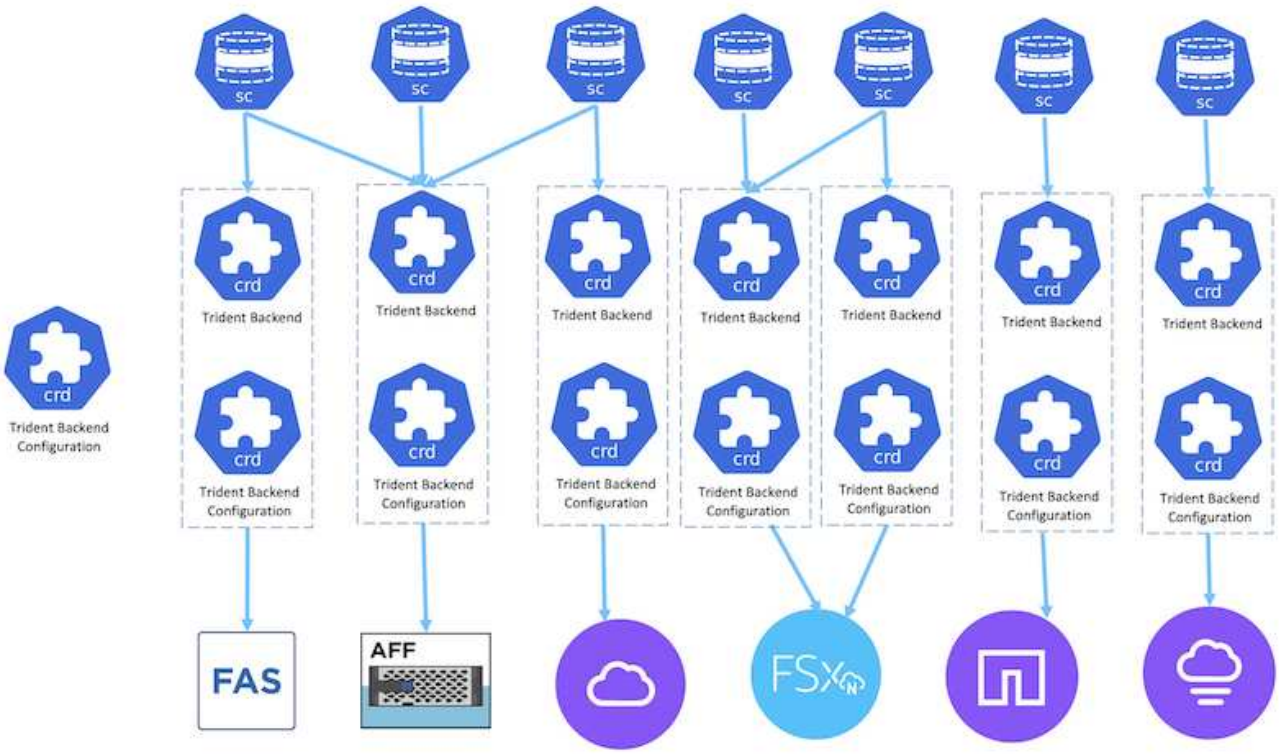
Red Hat Open Shiftコンテナを VMwareで実行する場合でも、ハイパースケーラで実行する場合でも、NetApp Astra Tridentは、サポートするさまざまなタイプのバックエンドネットアップストレージのCSIプロビジョニングツールとして使用できます。

次の図は、NetApp Astra Tridentを使用してOpenShiftクラスタと統合できるバックエンドのネットアップストレージを示しています。

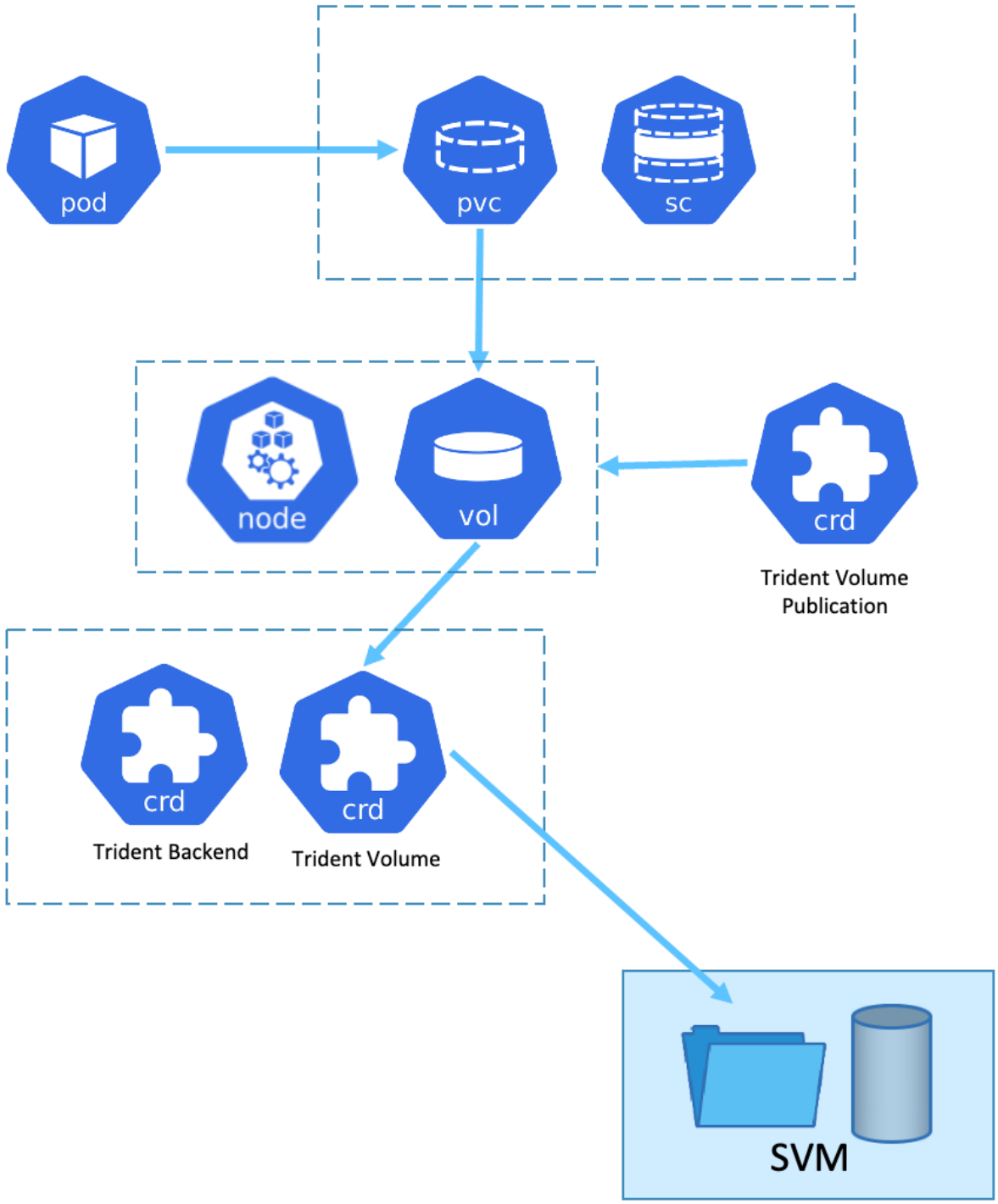


ONTAP Storage Virtual Machine（SVM）はセキュアマルチテナンシーを提供します。単一のOpenShiftクラスタは、単一のSVMまたは複数のSVMに接続することも、複数のONTAP クラスタに接続することもできます。ストレージクラスは、パラメータまたはラベルに基づいてバックエンドストレージをフィルタリングします。ストレージ管理者は、Tridentバックエンド構成を使用してストレージシステムに接続するためのパラメータを定義します。接続が正常に確立されると、Tridentバックエンドが作成され、ストレージクラスでフィルタできる情報が入力されます。

ストレージクラスとバックエンドの関係を次に示します。



アプリケーション所有者がストレージクラスを使用して永続ボリュームを要求します。バックエンドストレージはストレージクラスでフィルタリングされます。ポッドとバックエンドストレージの関係を以下に示します。



Container Storage Interface（CSI）オプション

vSphere環境では、VMware CSIドライバやAstra Trident CSIを選択してONTAP と統合できます。VMware CSIでは永続ボリュームがローカルSCSIディスクとして使用され、Tridentではネットワークが使用されます。VMware CSIはONTAP でのRWXアクセスモードをサポートしていないため、RWXモードが必要な場合は、アプリケーションでTrident CSIを使用する必要があります。FCベースの導入ではVMware CSIが推奨され、SnapMirror Business Continuity（SMBC）によってゾーンレベルの高可用性が実現されます。

VMware CSIがサポートします

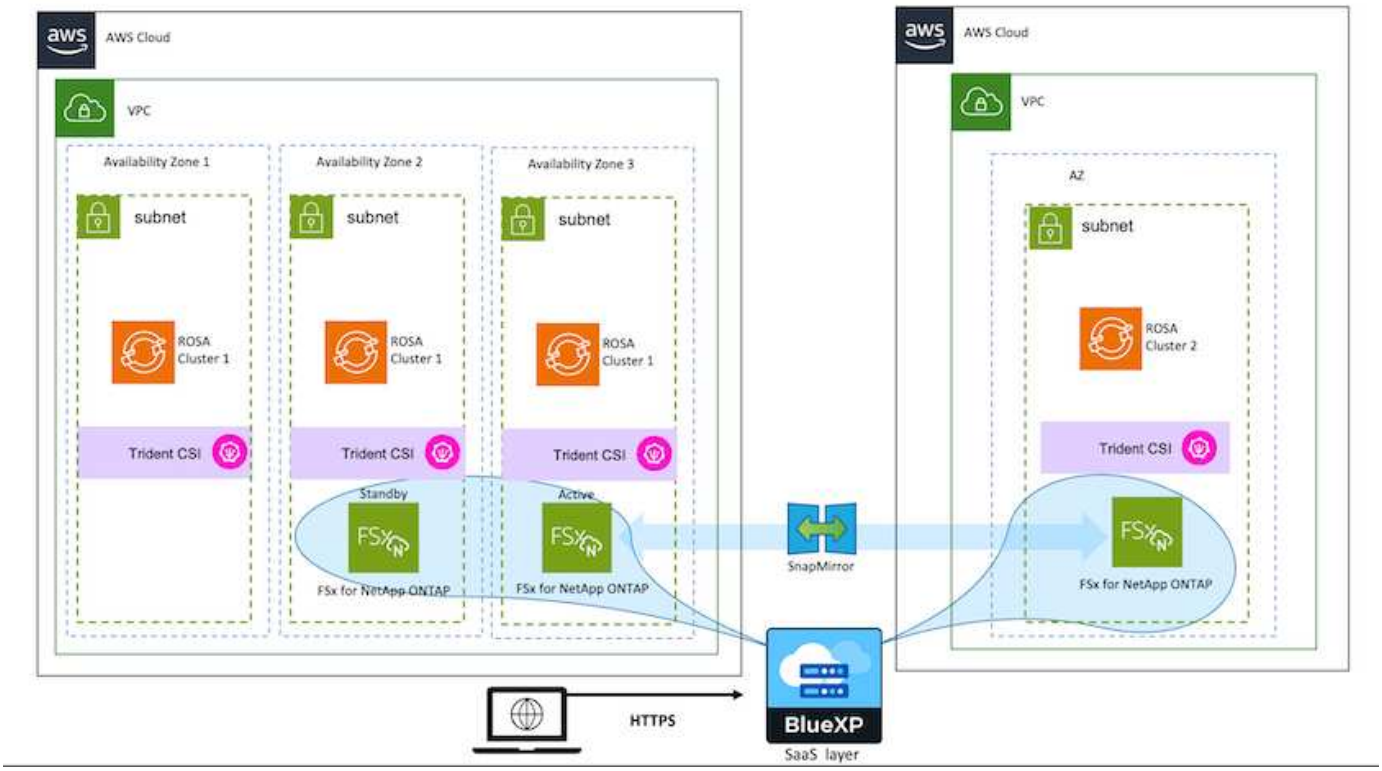
- ブロックベースのコアデータストア（FC、FCoE、iSCSI、NVMeoF）
- コアファイルベースのデータストア（NFS v3、v4）
- VVolデータストア（ブロックとファイル）

Tridentには、**ONTAP** をサポートするために次のドライバがあります

- ONTAP-SAN（専用ボリューム）
- ONTAP-SANの経済性（共有ボリューム）
- ONTAP-NAS（専用ボリューム）
- ONTAP-NASの経済性（共有ボリューム）
- ontap-nas-flexgroup（専用の大規模ボリューム）

ONTAP は、VMware CSIとAstra Trident CSIのどちらについても、NFSとマルチパスのnconnect、セッショントランキング、Kerberosなど、ブロックプロトコルのCHAP認証などをサポートします。

AWSでは、FSx for NetApp ONTAP （FSxN）を単一のアベイラビリティゾーン（AZ）または複数のAZに導入できます。高可用性を必要とする本番ワークロードに対しては、複数のAZを使用することでゾーンレベルのフォールトトレランスが実現し、NVMe読み取りキャッシュも単一のAZよりも優れています。詳細については、を参照してください "AWSパフォーマンスのガイドライン"。
ディザスタリカバリサイトのコストを削減するために、単一のAZ FSx ONTAP を利用できます。



FSx ONTAP でサポートされるSVMの数については、を参照してください "FSx ONTAP Storage Virtual Machineの管理"

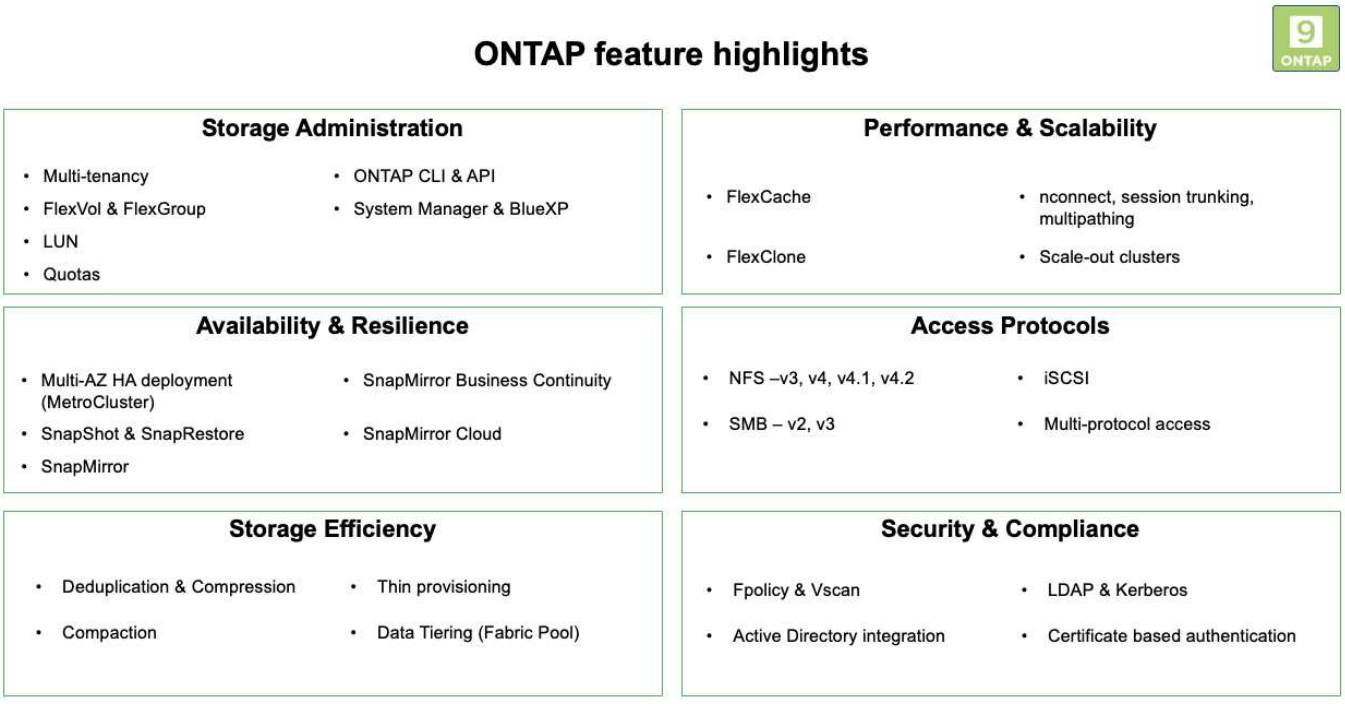
Red Hat OpenShift Containerワークロード向けのネットアップハイブリッドマルチクラウドソリューション

概要

ネットアップでは、従来型エンタープライズアプリケーションを最新化し、Kubernetesを中心に構築されたコンテナとオーケストレーションプラットフォームを使用して新しいアプリケーションを構築するお客様が大幅に増えています。Red Hat OpenShift Container Platformは、多くのお客様に採用されている例の1つです。

企業内でコンテナを採用するお客様がますます増えています。ネットアップは、ステートフルアプリケーションの永続的ストレージのニーズに加え、データ保護、データセキュリティ、データ移行などの従来のデータ管理のニーズにも応えることができます。しかし、これらのニーズは、さまざまな戦略、ツール、方法を使用して満たしています。

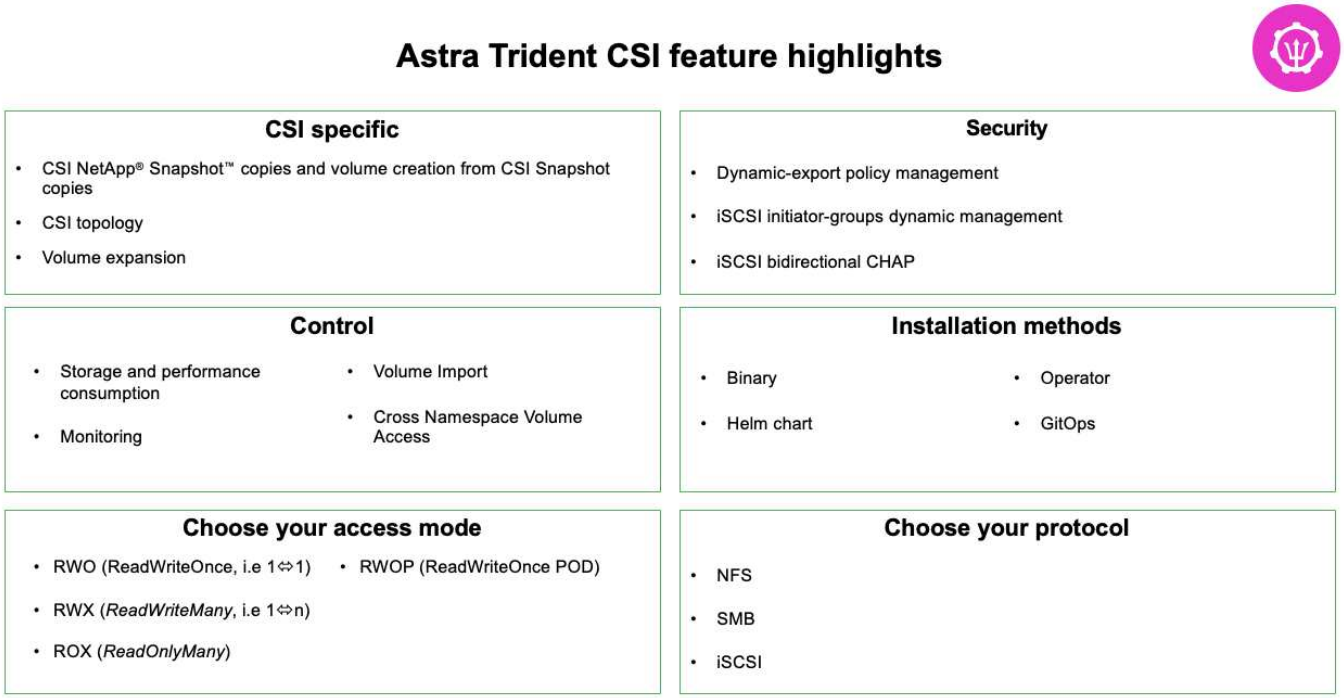
- NetApp ONTAP **ベースのストレージオプションを次に示します。コンテナとKubernetes環境にセキュリティ、データ保護、信頼性、柔軟性を提供します。
  - オンプレミスの自己管理型ストレージ：
- ネットアップファブリック接続ストレージ（FAS ）、ネットアップオールフラッシュFAS アレイ（AFF ）、ネットアップオールSANアレイ（ASA ）、ONTAP Select
  - オンプレミスのプロバイダ管理ストレージ：
- NetApp Keystone が提供するストレージサービス（STaaS）
  - クラウド内の自己管理型ストレージ：
- NetApp Cloud Volumes ONTAP（CVO）は、ハイパースケーラに自己管理型ストレージを提供します
  - クラウド上のプロバイダが管理するストレージ：
- Cloud Volumes Service for Google Cloud（CVS）、Azure NetApp Files （ANF）、Amazon FSx for NetApp ONTAP は、ハイパースケーラにフルマネージドストレージを提供します



- NetApp BlueXP **を使用すると、すべてのストレージ資産とデータ資産を単一のコントロールプレーン/インターフェイスから管理できます。

BlueXPを使用して、クラウドストレージ（Cloud Volumes ONTAP やAzure NetApp Files など）の作成と管理、データの移動、保護、分析、オンプレミスやエッジの多くのストレージデバイスの管理を行うことができます。

- NetApp Astra Trident **はCSI準拠のストレージオーケストレーションツールです。上記のさまざまなネットアップストレージオプションを利用して、永続的ストレージをすばやく簡単に利用できます。ネットアップが保守、サポートしているオープンソースのソフトウェアです。



ビジネスクリティカルなコンテナワークロードに必要なのは、永続的ボリュームだけではありません。同社のデータ管理要件では、アプリケーションのKubernetesオブジェクトの保護と移行も必要です。

アプリケーションデータには、ユーザデータに加えてKubernetesオブジェクトが含まれます。例を次に示します。 -ポッド仕様、PVC、デプロイ、サービスなどのKubernetesオブジェクト- 設定マップやシークレットなどのカスタム設定オブジェクト- Snapshotコピー、バックアップ、クローンなどの永続的データ- CRSやCRDなどのカスタムリソース

- NetApp Astra Control **は、フルマネージドと自己管理型の両方のソフトウェアとして提供され、堅牢なアプリケーションデータ管理のためのオーケストレーションを提供します。を参照してください "Astra のドキュメント" を参照してください。

このリファレンスドキュメントでは、NetApp Astra Control Centerを使用して、Red Hat OpenShiftコンテナプラットフォームに導入されたコンテナベースアプリケーションの移行と保護について検証します。また、解決策 では、コンテナプラットフォームを管理するためのRed Hat Advanced Cluster Management（ACM）の導入と使用に関する詳細についても説明しています。また、Astra Trident CSIプロビジョニングツールを使用して、ネットアップストレージとRed Hat OpenShiftコンテナプラットフォームを統合する方法についても詳しく説明します。Astra Control Centerはハブクラスタに導入され、コンテナアプリケーションとその永続的ストレージライフサイクルの管理に使用されます。最後に、Amazon FSx for NetApp ONTAP （FSxN）を永続的ストレージとして使用し、AWS（ROSA）のマネージドRed Hat OpenShiftクラスタ上のコンテナワーク

ロードのレプリケーション、フェイルオーバー、フェイルバックのための解決策 を提供します。

VMware上での**NetApp**解決策 と**Red Hat OpenShift Container**プラットフォームのワークロード

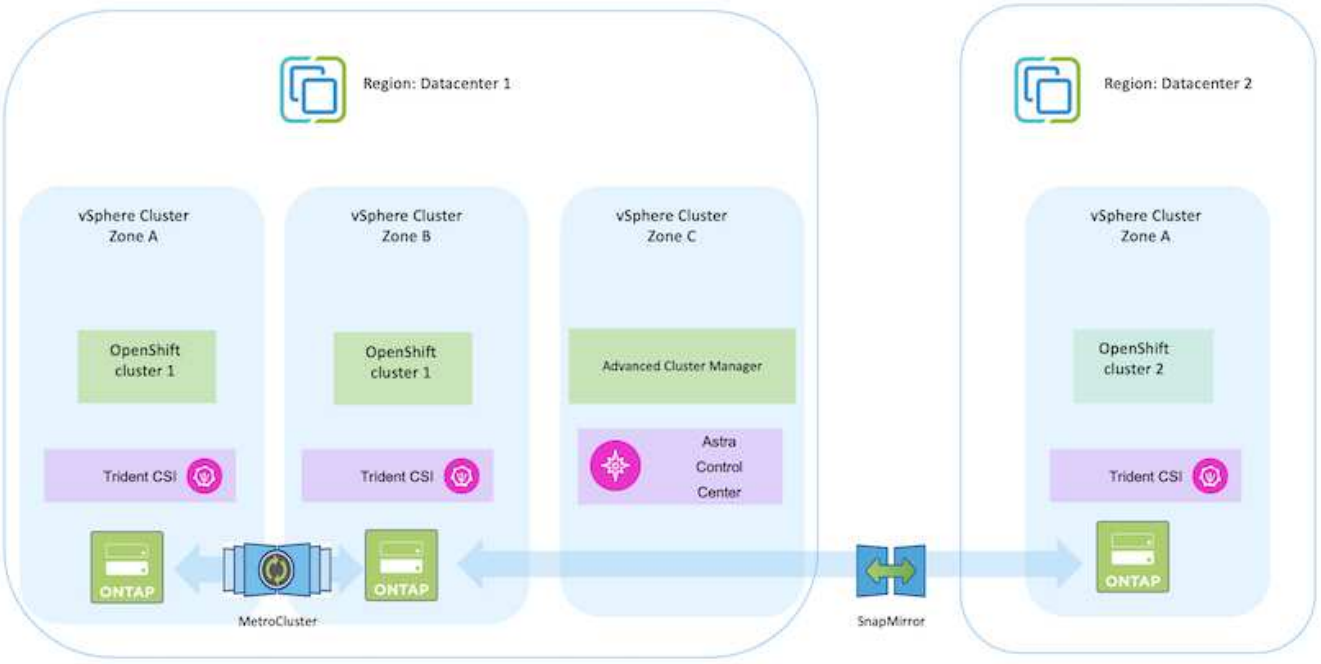
最新のコンテナ化されたアプリケーションをプライベートデータセンターのインフラで実行する必要がある場合は、実行できます。コンテナワークロードを導入するための本番環境向け環境を成功させるためには、Red Hat OpenShiftコンテナプラットフォーム（OCP）の計画と導入が必要です。OCPクラスタは、VMwareまたはベアメタルに導入できます。

NetApp ONTAP ストレージは、コンテナ導入にデータ保護、信頼性、柔軟性を提供します。Astra Tridentは、お客様のステートフルアプリケーション向けに永続的ONTAP ストレージを利用するための動的ストレージプロビジョニングツールとして機能します。Astra Control Centerを使用すると、データ保護、移行、ビジネス継続性など、ステートフルアプリケーションに求められる多くのデータ管理要件をオーケストレーションできます。

VMware vSphereでは、NetApp ONTAP toolsがvCenterプラグインを提供し、データストアのプロビジョニングに使用できます。タグを適用し、OpenShiftでノードの設定とデータを格納するために使用します。NVMeベースのストレージは、低レイテンシと高パフォーマンスを実現します。

この解決策 では、Astra Control Centerを使用したコンテナワークロードのデータ保護と移行について詳しく説明します。この解決策 では、オンプレミス環境内のvSphere上のRed Hat OpenShiftクラスタにコンテナワークロードが導入されます。注：今後、ベアメタル上のOpenShiftクラスタ上のコンテナワークロード向けに解決策 を提供する予定です。

Astra Control Centerを使用した**OpenShift**コンテナワークロード向けのデータ保護と移行の解決策

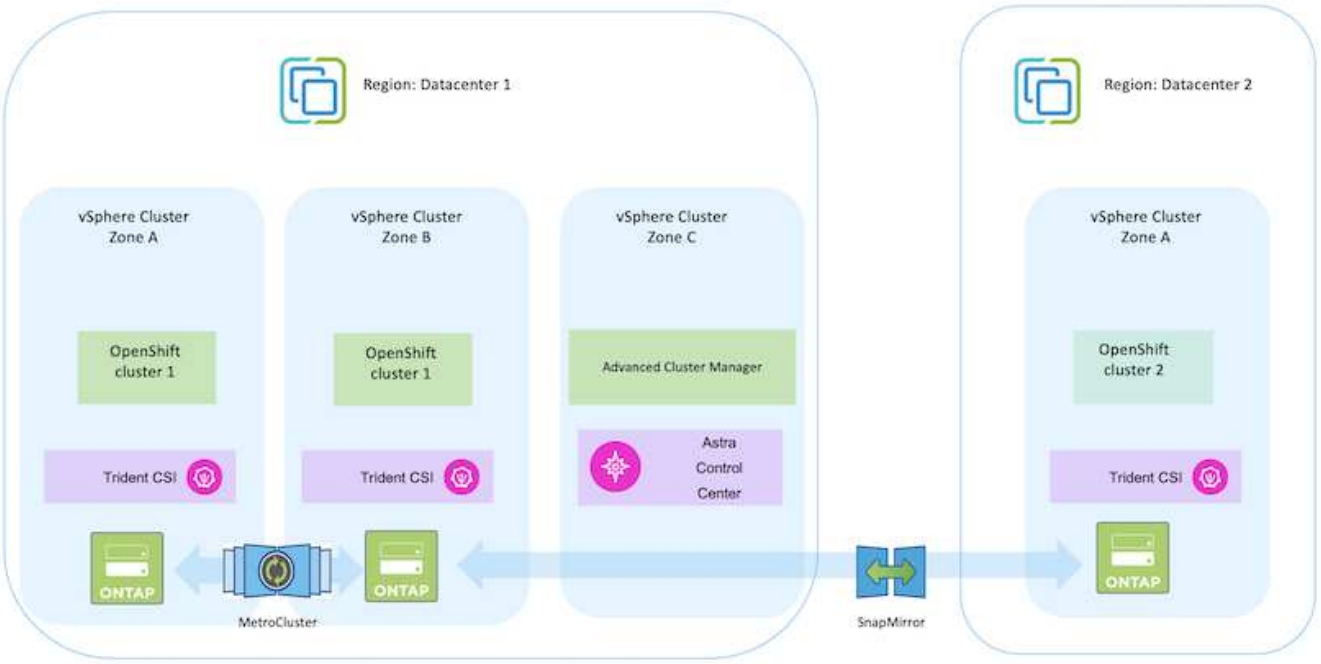


VMwareにRed Hat OpenShift Containerプラットフォームを導入して設定します

このセクションでは、OpenShiftクラスタをセットアップおよび管理し、クラスタ上でステートフルアプリケーションを管理する方法の大まかなワークフローについて説明します。このスライドでは、NetApp ONTAP ストレージアレイとAstra Tridentを使用して永続ボリュームを提供する方法を示しています。ステートフルアプリケーションに対してデータ保護と移行のアクティビティを実行するためのAstra Control Centerの使用方法について詳しく説明します。

Red Hat OpenShift Containerプラットフォームクラスタは、いくつかの方法で導入できます。このセットアップの概要概要 には、使用した具体的な方法のドキュメントへのリンクが記載されています。その他の方法については、に記載されている関連リンクを参照してください "リソースセクション"。

次の図は、データセンターのVMwareに導入されたクラスタを示しています。



セットアッププロセスは、次の手順に分けることができます。

CentOS VMを導入、設定

- VMware vSphere環境に導入されます。
- このVMは、NetApp Astra TridentやNetApp Astra Control Center for the解決策 など、一部のコンポーネントの導入に使用されます。
- このVMにはインストール時にrootユーザが設定されます。

VMware vSphere（ハブクラスタ）に**OpenShift Container Platform**クラスタを導入して設定

の手順を参照してください "支援された展開" OCPクラスタを導入する方法。

> 次の点に注意してください。-インストーラに提供するsshの公開鍵と秘密鍵を作成します。これらのキーは、必要に応じてマスターノードとワーカーノードにログインするために使用されます。-アシスタントインストーラからインストーラプログラムをダウンロードします。このプログラムを使用して、VMware vSphere環境でマスターノードとワーカーノード用に作成したVMをブートします。- VMには、CPU、メモリ、およびハードディスクの最小要件が必要です。（のvm createコマンドを参照してください "これ" この情報を提供するマスターノードとワーカーノードのページ）-すべてのVMでdiskUUIDを有効にする必要があります。-マスター用に最低3ノード、ワーカー用に3ノードを作成します。-インストーラによって検出されたら、VMware vSphere統合トグルボタンをオンにします。

ハブクラスタに**Advanced Cluster Management**をインストールします

これは、ハブクラスタのAdvanced Cluster Management Operatorを使用してインストールします。手順を参照してください "こちらをご覧ください"。

ハブクラスタに内部**Red Hat Quay**レジストリをインストールします。

- Astraイメージをプッシュするには内部レジストリが必要です。Quay内部レジストリは、HubクラスタのOperatorを使用してインストールされます。
- 手順を参照してください "こちらをご覧ください"

2つの**OCP**クラスタ（ソースとデスティネーション）を追加でインストール

- 追加のクラスタは、ハブクラスタのACMを使用して展開できます。
- 手順を参照してください "こちらをご覧ください"。

NetApp ONTAP ストレージの設定

- VMware環境のOCP VMに接続されたONTAP クラスタをインストールします。
- SVMを作成
- SVMのストレージにアクセスするようにNASデータLIFを設定します。

OCPクラスタに**NetApp Trident**をインストール

- ハブ、ソース、デスティネーションの3つのクラスタすべてにNetApp Tridentをインストール
- 手順を参照してください "こちらをご覧ください"。
- ONTAP-NAS用のストレージバックエンドを作成
- ONTAP-NAS用のストレージクラスを作成
- 手順を参照してください "こちらをご覧ください"。

NetApp Astra Control Centerをインストール

- NetApp Astra Control Centerは、ハブクラスタでAstra Operatorを使用してインストールします。
- 手順を参照してください "こちらをご覧ください"。

覚えておくべきポイント：*サポートサイトからNetApp Astra Control Centerのイメージをダウンロード* イメージを内部レジストリにプッシュします。*こちらの手順を参照してください。

ソースクラスタにアプリケーションを導入します

OpenShift GitOpsを使用してアプリケーションを導入します。（例：Postgres、Ghost）

ソースクラスタとデスティネーションクラスタを**Astra Control Center**に追加

Astra Controlの管理にクラスタを追加したら、（Astra Control以外の）クラスタにアプリケーションをインストールし、Astra Controlの[Applications]ページに移動してアプリケーションとそのリソースを定義できます。を参照してください "Astra Control Centerのアプリケーションの管理セクションを開始します"。

次の手順では、Astra Control Centerを使用して、ソースクラスタからデスティネーションクラスタへのデータ保護とデータ移行を行います。

Astraを使用したデータ保護

このページには、Astra Control Center（ACC）を使用してVMware vSphereで実行されるRed Hat OpenShift Containerベースのアプリケーションのデータ保護オプションが表示されます。

ユーザがRed Hat OpenShiftを使用してアプリケーションを最新化する過程で、偶発的な削除やその他の人的エラーからユーザを保護するためのデータ保護戦略を策定する必要があります。多くの場合、データを管理から保護するために、規制やコンプライアンスの目的で保護戦略が必要になります。

データ保護の要件は、ポイントインタイムコピーへのリバートから別の障害ドメインへの自動フェイルオーバーまで、人手を介さずにさまざまです。多くのお客様がONTAP をKubernetesアプリケーションに最適なストレージプラットフォームとして選択しています。その理由は、マルチテナンシー、マルチプロトコル、ハイパフォーマンスと容量のサービス、マルチサイト環境のレプリケーションとキャッシュ、セキュリティと柔軟性などの豊富な機能があるからです。

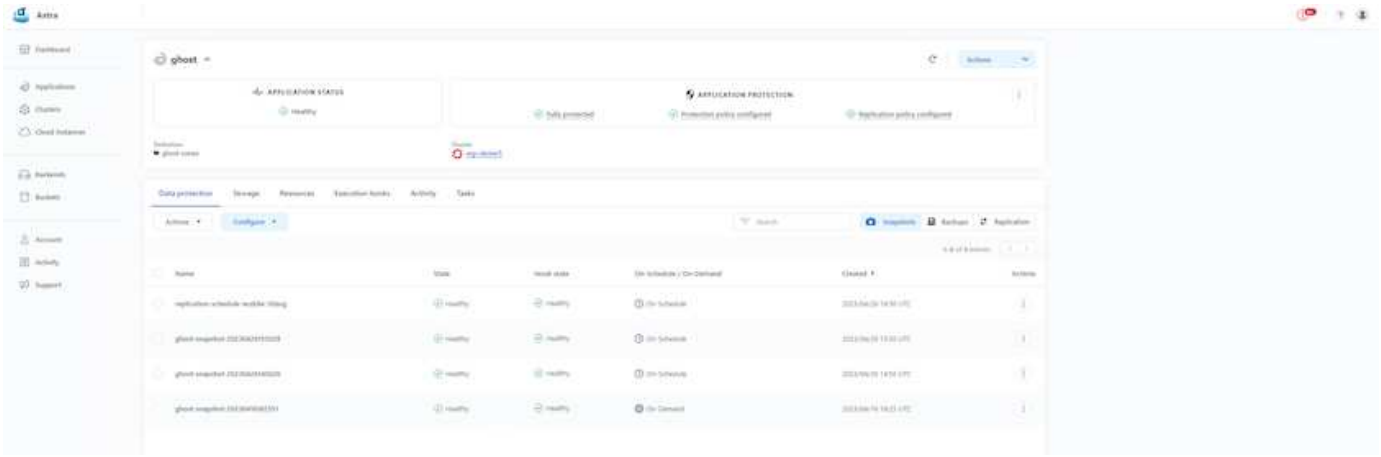
ONTAP のデータ保護は、アドホックまたはポリシー制御の-スナップショット*-バックアップおよびリストアを使用して実現できます

Snapshotコピーとバックアップのどちらも、次のタイプのデータを保護します。-アプリケーションの状態を表すアプリケーションメタデータ-アプリケーションに関連付けられた永続的データボリューム-アプリケーションに属するリソースアーティファクト

ACCを使用したスナップショット

SnapshotとACCを使用して、データのポイントインタイムコピーをキャプチャできます。保護ポリシーでは、保持するSnapshotコピーの数を定義します。最小スケジュールオプションは毎時です。オンデマンドで手動のSnapshotコピーをいつでも、スケジュールされたSnapshotコピーよりも短い間隔で作成できます。Snapshotコピーは、アプリケーションと同じプロビジョニングされたボリュームに格納されます。

ACCでスナップショットを設定しています

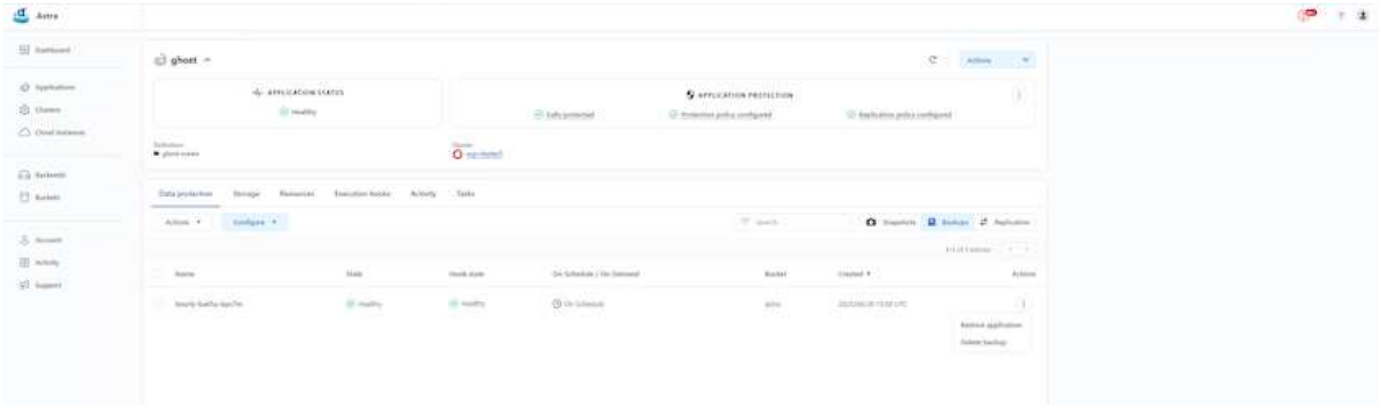


ACCを使用したバックアップと復元

バックアップはSnapshotに基づいています。ACCはCSIを使用してSnapshotコピーを作成し、ポイントインタイムSnapshotコピーを使用してバックアップを実行できます。バックアップは外部のオブジェクトストア（別の場所にあるONTAP S3を含むs3互換）に格納されます。スケジュールされたバックアップの保護ポリシーと保持するバックアップバージョンの数を設定できます。最小RPOは1時間です。

ACCを使用したバックアップからのアプリケーションのリストア

ACCは、バックアップが格納されているS3バケットからアプリケーションをリストアします。

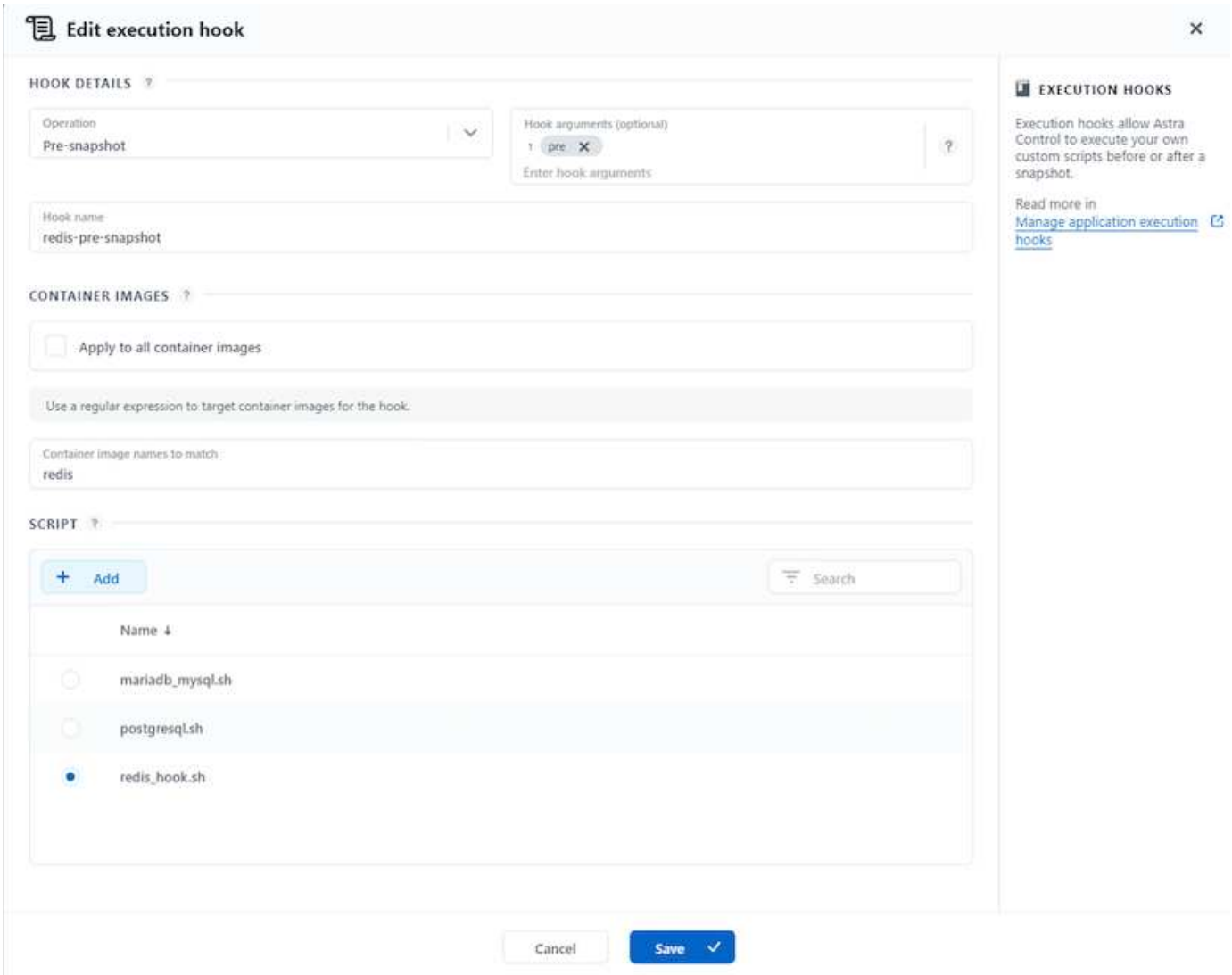


さらに、実行フックは、管理対象アプリのデータ保護操作と組み合わせて実行するように構成することができます。ストレージアレイレベルのデータ保護機能を使用できますが、バックアップとリストアでアプリケーションとの整合性を確保するために追加の手順が必要になることがよくあります。アプリケーション固有の追加手順は次のとおりです。- Snapshotコピーの作成前または作成後。-バックアップの作成前または作成後。- Snapshotコピーまたはバックアップからリストアしたあと。

Astra Controlでは、実行フックと呼ばれるカスタムスクリプトとしてコード化されたアプリケーション固有の手順を実行できます。

"NetApp Verda GitHubプロジェクト" 一般的なクラウドネイティブアプリケーションの実行フックを提供し、アプリケーションを簡単に保護し、堅牢で、オーケストレーションを容易にします。リポジトリにないアプリケーションに十分な情報がある場合は、そのプロジェクトに貢献してください。

redisアプリケーションの**pre-Snapshot**用のサンプル実行フック。



ACCを使用したレプリケーション

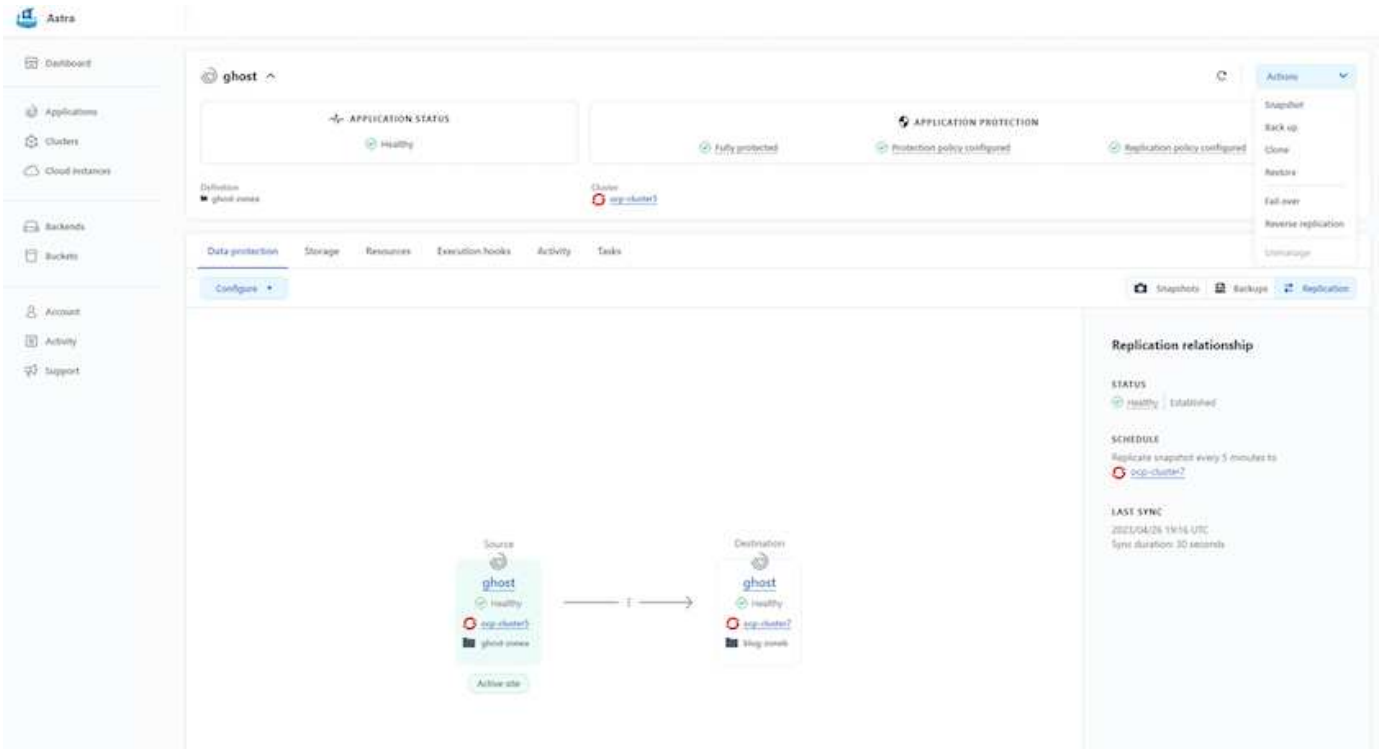
リージョンを保護する場合や、RPOとRTOの低い解決策 を実現する場合は、別のサイト（できれば別のリージョン）で実行されている別のKubernetesインスタンスにアプリケーションをレプリケートできます。ACCは、最短5分でRPOを実現するONTAP 非同期SnapMirrorを利用します。レプリケーションはONTAP にレプリ

ケートすることで実行され、フェイルオーバーによってデスティネーションクラスタにKubernetesリソースが作成されます。

> レプリケーションは、バックアップがS3に保存され、S3からリストアが実行されるバックアップとリストアとは異なります。2種類のデータ保護の違いの詳細については、https://docs.netapp.com/us-en/astra-control-center/concepts/data-protection.html#replication-to-a-remote-cluster[here]を参照してください。

を参照してください "こちらをご覧ください" SnapMirrorのセットアップ手順を参照してください。

ACCを使用した**SnapMirror**



> SANエコノミーおよびNASエコノミーのストレージドライバは、レプリケーション機能をサポートしていません。を参照してください "こちらをご覧ください" を参照してください。

デモビデオ：

"Astra Control Centerを使用したディザスタリカバリのデモビデオ"

Astra Control Centerによるデータ保護

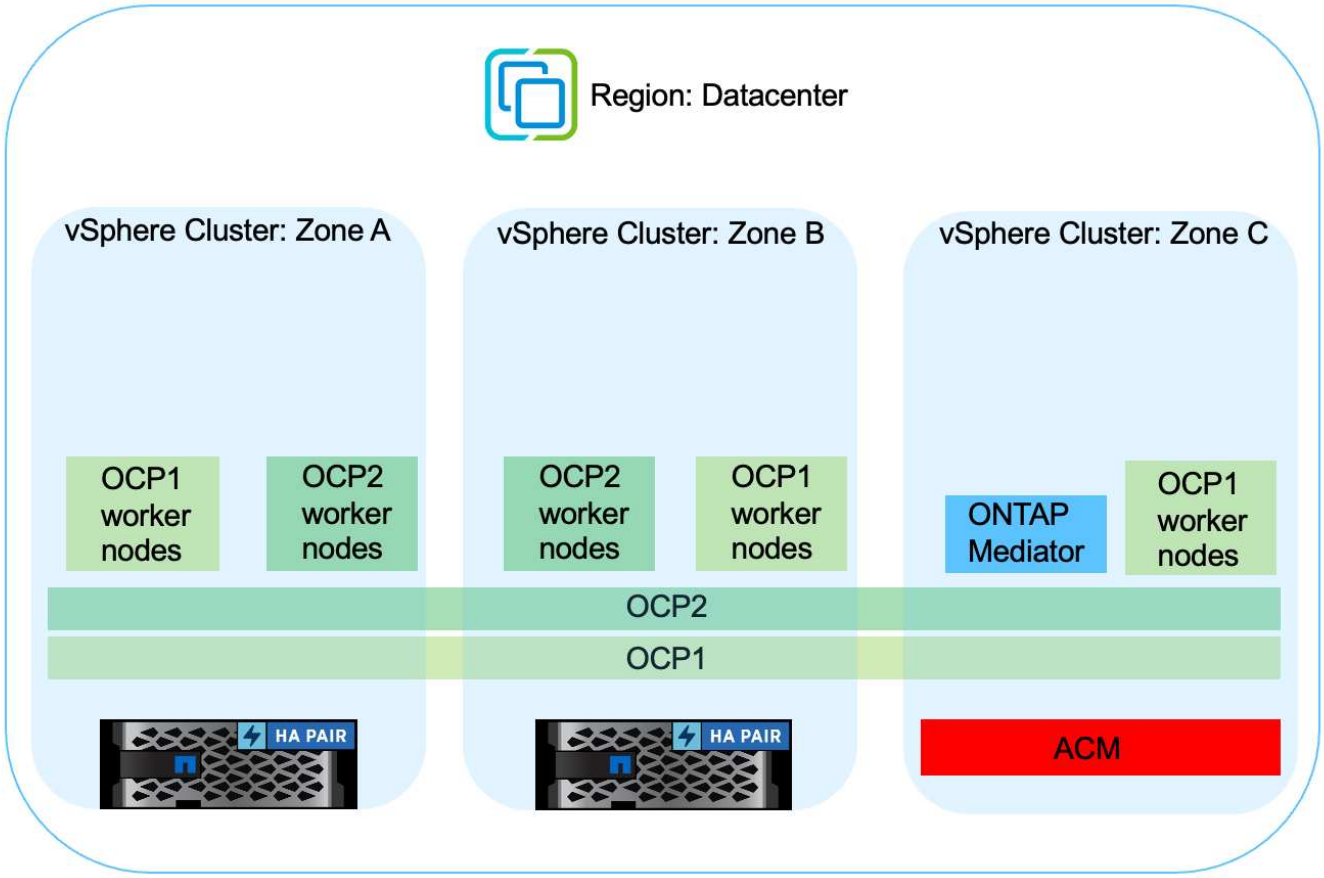
MetroCluster によるビジネス継続性

ONTAP 用のハードウェアプラットフォームのほとんどは、デバイス障害から保護するための高可用性機能を備えており、ダイヤスターリカバリを実行する必要はありません。しかし、火災やその他の災害からデータを保護し、RPOゼロとRTOを低く抑えてビジネスを継続するためには、多くの場合MetroCluster 解決策 が使用されます。

現在ONTAP システムをお持ちのお客様は、ゾーンレベルのディザスタリカバリを実現するために、距離の制限内にサポート対象のONTAP システムを追加することで、MetroCluster に拡張できます。CSI（コンテナス

トレージインターフェイス）であるAstra Tridentは、MetroCluster 構成のほか、Cloud Volumes ONTAP 、Azure NetApp Files 、AWS FSx for NetApp ONTAP などの他のオプションを含むNetApp ONTAP をサポートしています Astra Tridentには、ONTAP 向けに5つのストレージドライバオプションが用意されていますが、いずれもMetroCluster 構成でサポートされています。を参照してください "こちらをご覧ください" Astra TridentでサポートされるONTAP ストレージドライバの詳細については、を参照してください。

MetroCluster 解決策 には、両方のフォールトドメインから同じネットワークアドレスにアクセスするためのレイヤ2ネットワーク拡張または機能が必要です。MetroCluster を設定すると、MetroCluster SVM内のすべてのボリュームが保護され、SyncMirror （RPOゼロ）のメリットが得られるため、解決策 はアプリケーション所有者に対して透過的に実行されます。



Tridentバックエンド構成（TBC）の場合は、MetroCluster 構成を使用する際にデータLIFとSVMを指定しないでください。管理LIF用のSVM管理IPを指定し、vsadminロールのクレデンシャルを使用してください。

Astra Control Centerのデータ保護機能の詳細を確認できます "こちらをご覧ください"

Astra Control Centerを使用したデータ移行

このページには、Astra Control Center（ACC）を使用したRed Hat OpenShiftクラスタ上のコンテナワークロードのデータ移行オプションが表示されます。

Kubernetesアプリケーションは、多くの場合、ある環境から別の環境に移動する必要があります。アプリケーションを永続的データと一緒に移行する場合は、NetApp ACCを使用できます。

ACCは、Google Anthos、Red Hat OpenShift、Tanzu Kubernetes Grid、Rancher Kubernetes Engine 、Upstream Kubernetes、 など 詳細については、を参照してください "こちらをご覧ください"。

アプリケーションをあるクラスタから別のクラスタに移行するには、ACCの次の機能のいずれかを使用できます。

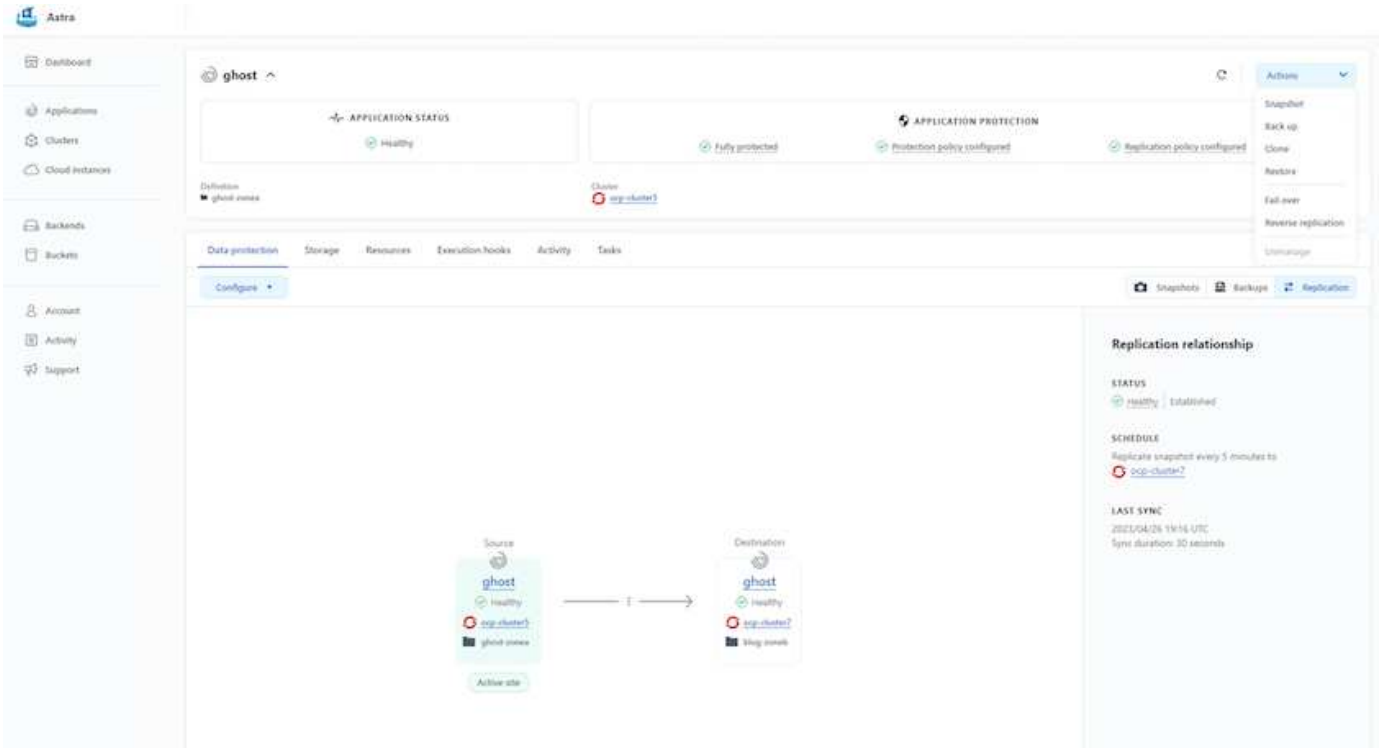
- レプリケーション
- バックアップとリストア
- クローン

を参照してください "データ保護セクション" レプリケーションおよびバックアップとリストアオプションの場合。

を参照してください "こちらをご覧ください" クローン作成の詳細については、を参照してください。

> Astraレプリケーション機能は、Trident Container Storage Interface（CSI）でのみサポートされます。ただし、NASエコノミードライバとSANエコノミードライバでは、レプリケーションはサポートされていません。

ACCを使用したデータ複製の実行



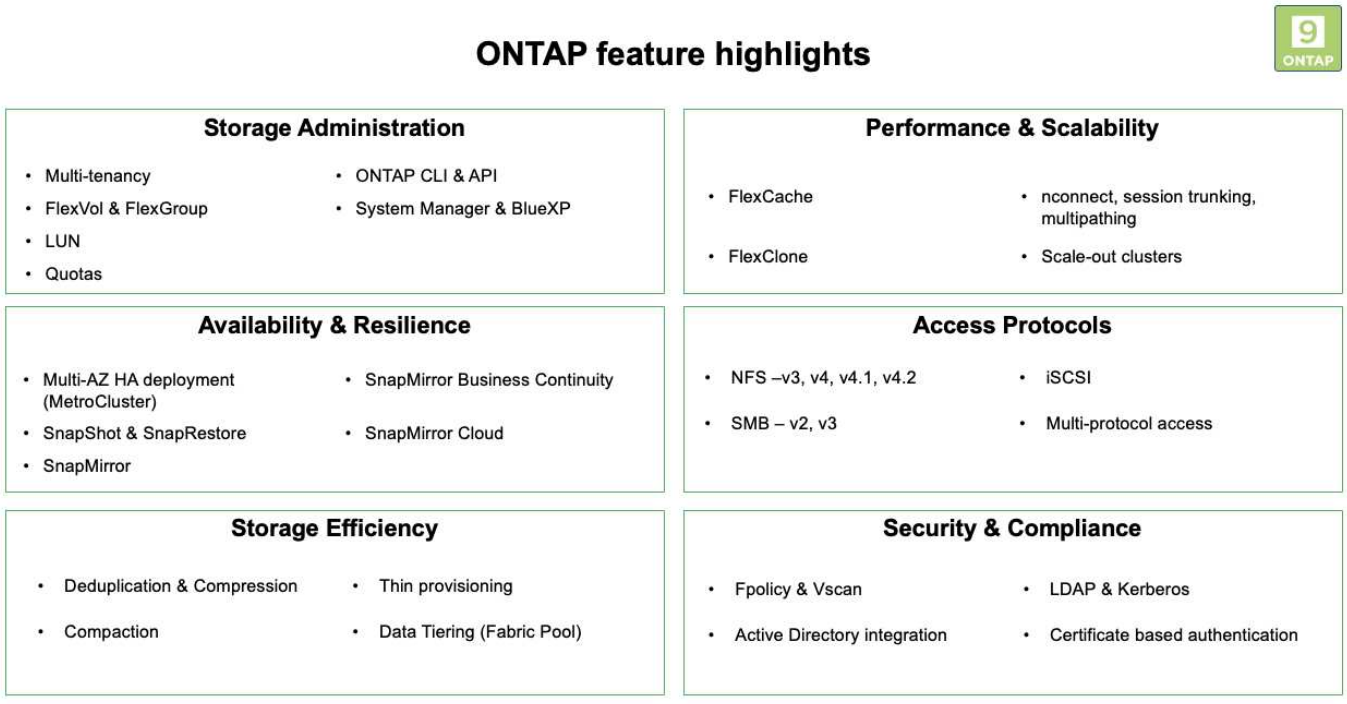
Red Hat OpenShift Containerワークロード向けのネットアップハイブリッドマルチクラウドソリューション

概要

ネットアップでは、従来型エンタープライズアプリケーションを最新化し、Kubernetesを中心に構築されたコンテナとオーケストレーションプラットフォームを使用して新しいアプリケーションを構築するお客様が大幅に増えています。Red Hat OpenShift Container Platformは、多くのお客様に採用されている例の1つです。

企業内でコンテナを採用するお客様がますます増えています。ネットアップは、ステートフルアプリケーションの永続的ストレージのニーズに加え、データ保護、データセキュリティ、データ移行などの従来のデータ管理のニーズにも応えることができます。しかし、これらのニーズは、さまざまな戦略、ツール、方法を使用して満たしています。

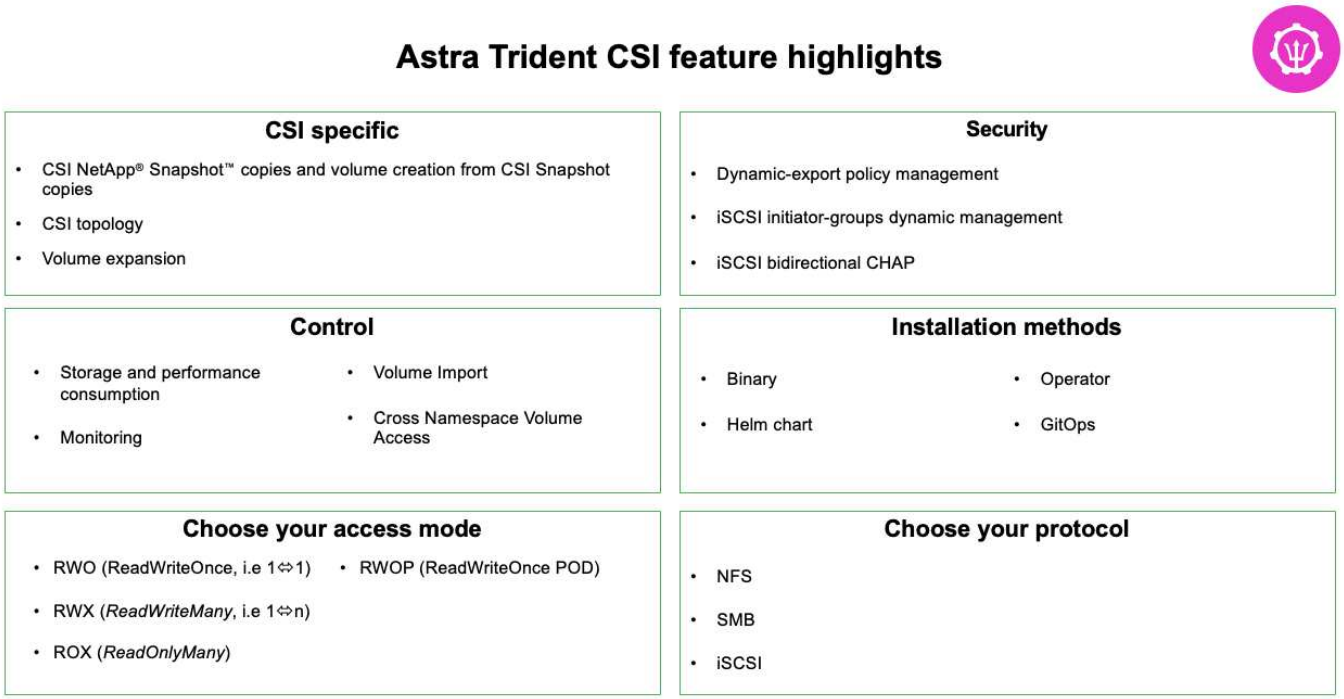
- NetApp ONTAP **ベースのストレージオプションを次に示します。コンテナとKubernetes環境にセキュリティ、データ保護、信頼性、柔軟性を提供します。
  - オンプレミスの自己管理型ストレージ：
- ネットアップファブリック接続ストレージ（FAS ）、ネットアップオールフラッシュFAS アレイ（AFF ）、ネットアップオールSANアレイ（ASA ）、ONTAP Select
  - オンプレミスのプロバイダ管理ストレージ：
- NetApp Keystone が提供するストレージサービス（STaaS）
  - クラウド内の自己管理型ストレージ：
- NetApp Cloud Volumes ONTAP（CVO）は、ハイパースケーラに自己管理型ストレージを提供します
  - クラウド上のプロバイダが管理するストレージ：
- Cloud Volumes Service for Google Cloud（CVS）、Azure NetApp Files （ANF）、Amazon FSx for NetApp ONTAP は、ハイパースケーラにフルマネージドストレージを提供します



- NetApp BlueXP **を使用すると、すべてのストレージ資産とデータ資産を単一のコントロールプレーン/インターフェイスから管理できます。

BlueXPを使用して、クラウドストレージ（Cloud Volumes ONTAP やAzure NetApp Files など）の作成と管理、データの移動、保護、分析、オンプレミスやエッジの多くのストレージデバイスの管理を行うことができます。

- NetApp Astra Trident **はCSI準拠のストレージオーケストレーションツールです。上記のさまざまなネットアップストレージオプションを利用して、永続的ストレージをすばやく簡単に利用できます。ネットアップが保守、サポートしているオープンソースのソフトウェアです。



ビジネスクリティカルなコンテナワークロードに必要なのは、永続的ボリュームだけではありません。同社のデータ管理要件では、アプリケーションのKubernetesオブジェクトの保護と移行も必要です。

アプリケーションデータには、ユーザデータに加えてKubernetesオブジェクトが含まれます。例を次に示します。 -ポッド仕様、PVC、デプロイ、サービスなどのKubernetesオブジェクト- 設定マップやシークレットなどのカスタム設定オブジェクト- Snapshotコピー、バックアップ、クローンなどの永続的データ- CRSやCRDなどのカスタムリソース

- NetApp Astra Control **は、フルマネージドと自己管理型の両方のソフトウェアとして提供され、堅牢なアプリケーションデータ管理のためのオーケストレーションを提供します。を参照してください "Astra のドキュメント" を参照してください。

このリファレンスドキュメントでは、NetApp Astra Control Centerを使用して、Red Hat OpenShiftコンテナプラットフォームに導入されたコンテナベースアプリケーションの移行と保護について検証します。また、解決策 では、コンテナプラットフォームを管理するためのRed Hat Advanced Cluster Management（ACM）の導入と使用に関する詳細についても説明しています。また、Astra Trident CSIプロビジョニングツールを使用して、ネットアップストレージとRed Hat OpenShiftコンテナプラットフォームを統合する方法についても詳しく説明します。Astra Control Centerはハブクラスタに導入され、コンテナアプリケーションとその永続的ストレージライフサイクルの管理に使用されます。最後に、Amazon FSx for NetApp ONTAP （FSxN）を永続的ストレージとして使用し、AWS（ROSA）のマネージドRed Hat OpenShiftクラスタ上のコンテナワークロードのレプリケーション、フェイルオーバー、フェイルバックのための解決策 を提供します。

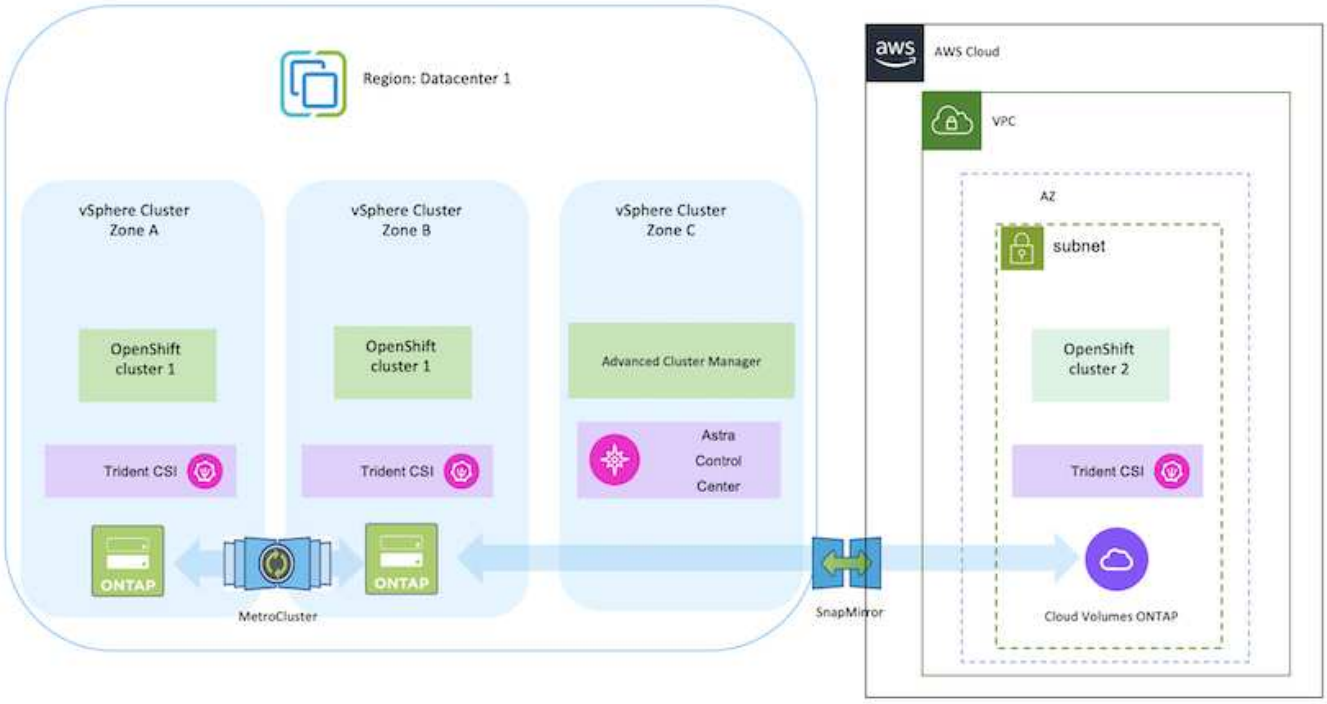
NetApp解決策 と**Red Hat OpenShift Container**プラットフォームのワークロードをハイブリッドクラウドで運用

お客様は、一部のワークロードまたはすべてのワークロードをデータセンターからクラウドに移行する準備が整った時点で、モダナイゼーションに移行する可能性があります。お客様は、さまざまな理由から、クラウドで自己管理型OpenShiftコンテナと自己管理型ネットアップストレージを使用することができます。データセンターからコンテナワークロードを移行するための本番環境向け環境を成功させるには、Red Hat OpenShiftコンテナプラットフォーム（OCP）をクラウドに計画して導入する必要があります。OCPクラスタは、データセンターのVMwareまたはベアメタルに導入し、クラウド環境のAWS、Azure、Google Cloudに導入できます。

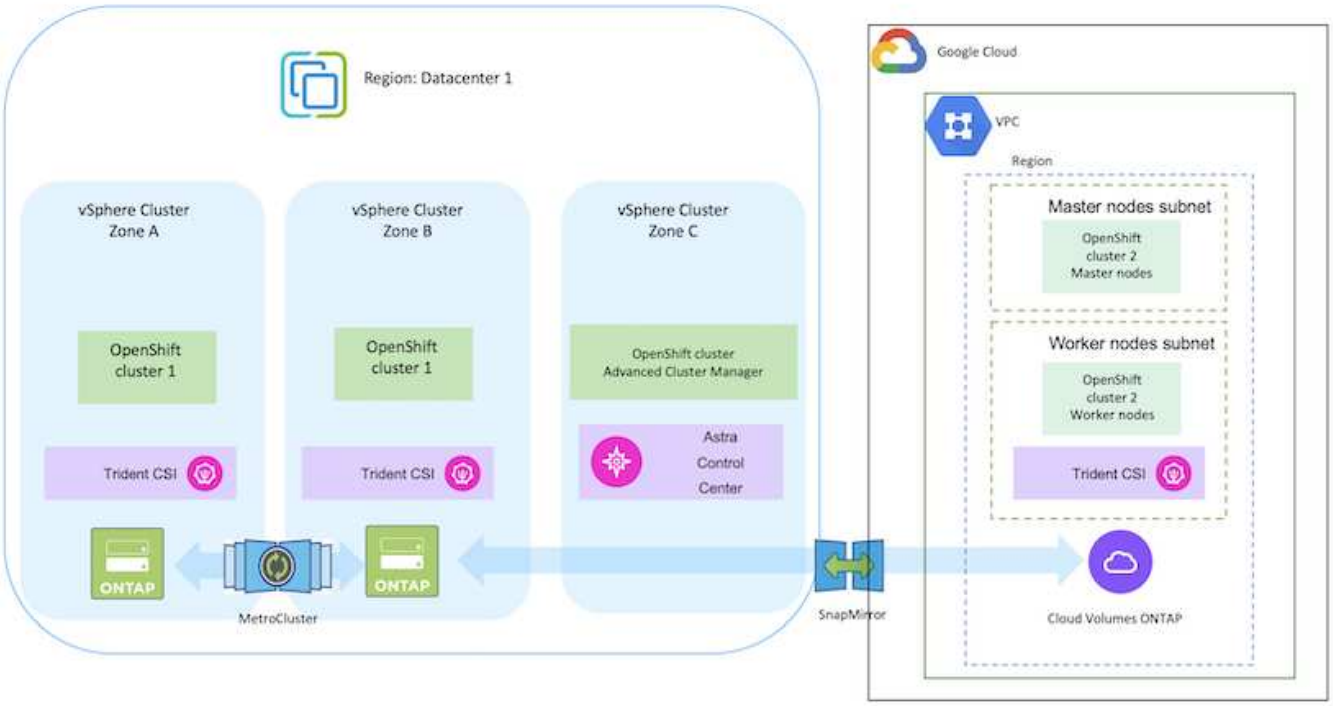
NetApp Cloud Volumes ONTAP ストレージは、AWS、Azure、Google Cloudでのコンテナ導入にデータ保護、信頼性、柔軟性を提供します。Astra Tridentは、お客様のステートフルアプリケーション向けに永続的Cloud Volumes ONTAP ストレージを利用するための動的ストレージプロビジョニングツールとして機能します。Astra Control Centerを使用すると、データ保護、移行、ビジネス継続性など、ステートフルアプリケーションに求められる多くのデータ管理要件をオーケストレーションできます。

Astra Control Centerを使用したハイブリッドクラウドでの**OpenShift**コンテナワークロード向けのデータ保護と移行解決策

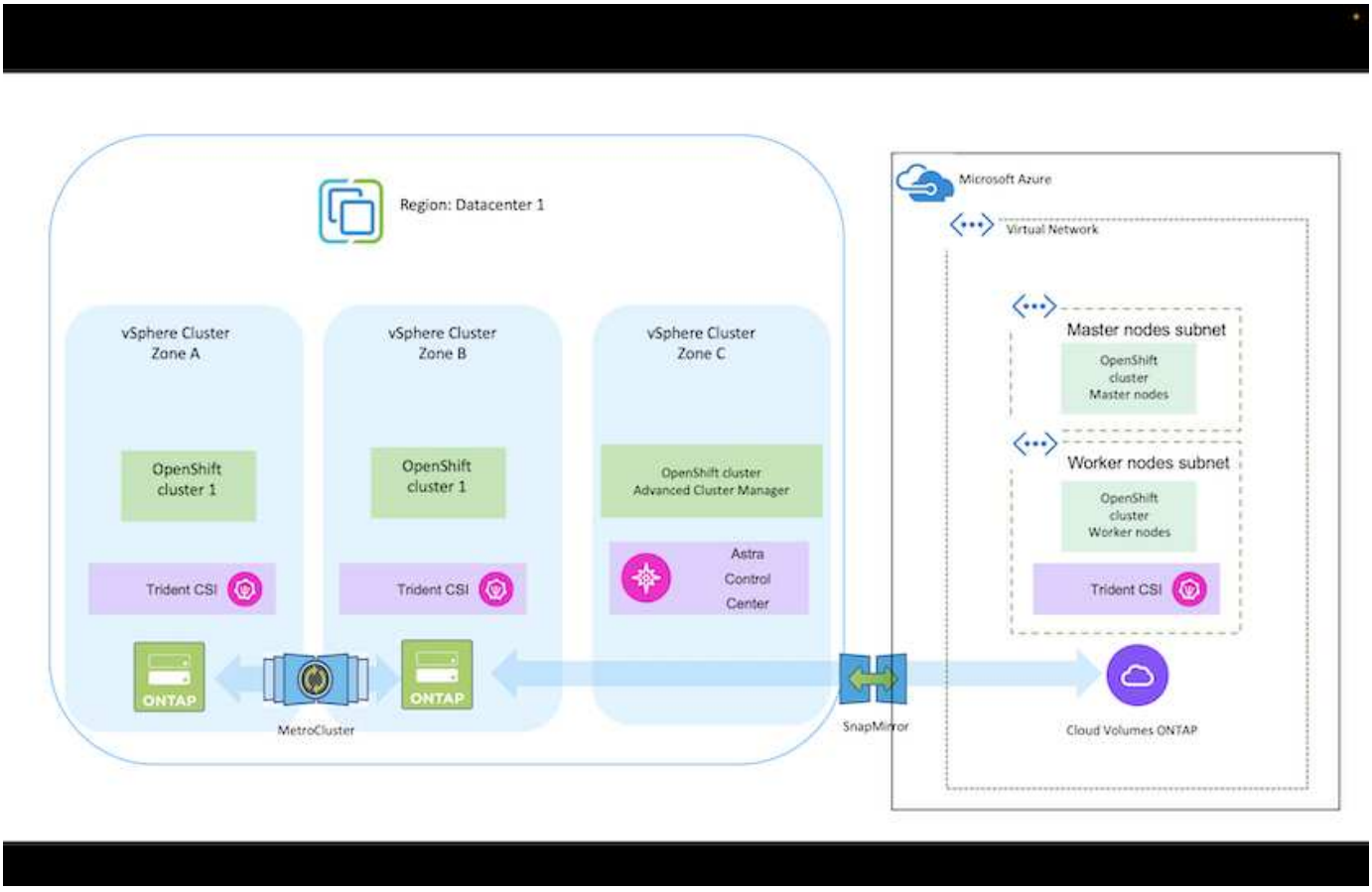
オンプレミスとAWS



オンプレミスとGoogle Cloud



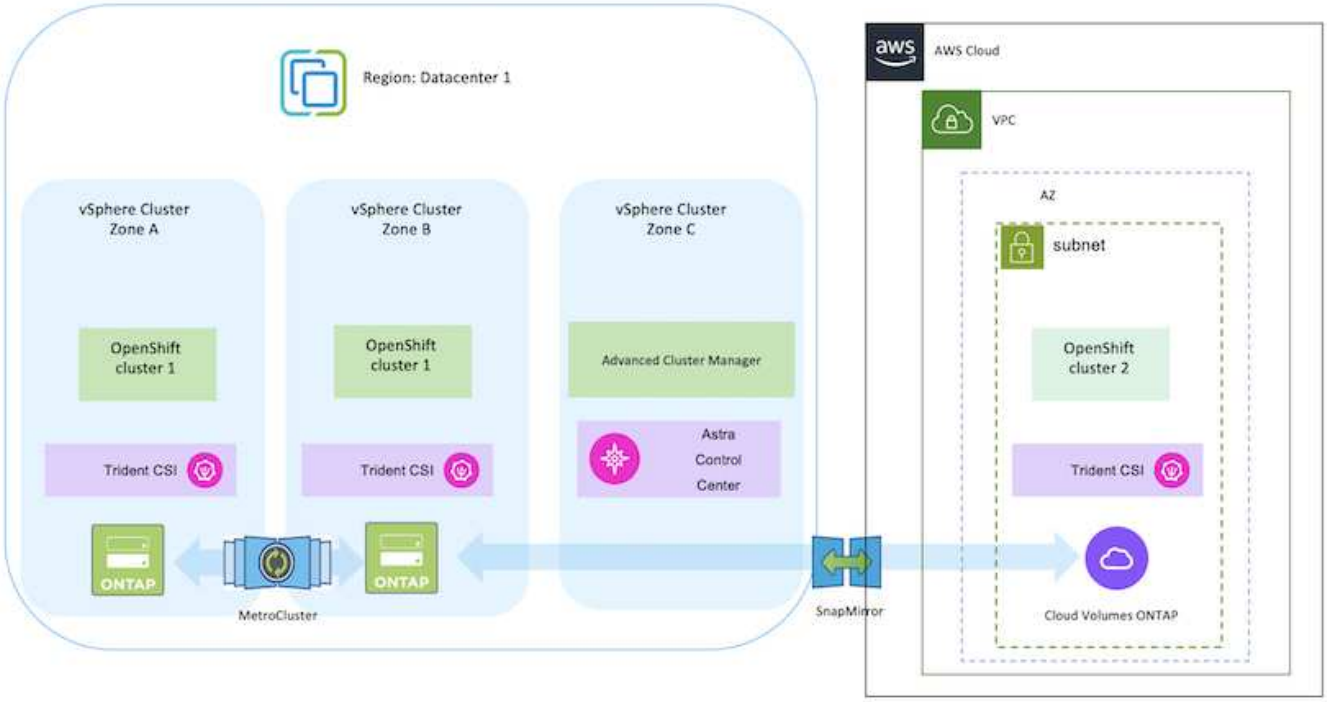
オンプレミスとAzureクラウド



このセクションでは、AWSでOpenShiftクラスタをセットアップおよび管理し、それらにステートフルアプリケーションを導入する方法の大まかなワークフローについて説明します。このスライドでは、Astra Tridentを使用してNetApp Cloud Volumes ONTAP ストレージを使用し、永続ボリュームを提供する方法を示しています。ステートフルアプリケーションに対してデータ保護と移行のアクティビティを実行するためのAstra Control Centerの使用方法について詳しく説明します。

Red Hat OpenShift Containerプラットフォームクラスタを AWSに導入する方法はいくつかあります。このセットアップの概要概要 には、使用した具体的な方法のドキュメントへのリンクが記載されています。その他の方法については、に記載されている関連リンクを参照してください "リソースセクション"。

次の図は、AWSに導入され、VPNを使用してデータセンターに接続されたクラスタを示しています。



セットアッププロセスは、次の手順に分けることができます。

Advanced Cluster Managementから**AWS**に**OCP**クラスタをインストールします。

- サイト間VPN接続（pfsenseを使用）を使用してVPCを作成し、オンプレミスネットワークに接続します。
- オンプレミスネットワークはインターネットに接続されています。
- 3つの異なるAZに3つのプライベートサブネットを作成します。
- VPC用にRoute 53プライベートホストゾーンとDNSリゾルバを作成します。

Advanced Cluster Management（ACM）ウィザードを使用して、AWSにOpenShiftクラスタを作成します。手順を参照してください "こちらをご覧ください"。

AWSでは、OpenShift Hybrid Cloudコンソールからクラスタを作成することもできます。を参照してください "こちらをご覧ください" 手順については、を参照し

ACMを使用してクラスタを作成する場合は、フォームビューで詳細を入力した後でYAMLファイルを編集してインストールをカスタマイズできます。クラスタが作成されたら、トラブルシューティングや追加の手動設定のために、クラスタのノードにSSHログインできます。インストール時に指定したsshキーとユーザ名coreを使用してログインします。

BlueXPを使用して**AWS**に**Cloud Volumes ONTAP** を導入

- オンプレミスのVMware環境にコネクタをインストールします。手順を参照してください "こちらをご覧ください"。
- コネクタを使用してAWSにCVOインスタンスを導入します。手順を参照してください "こちらをご覧ください"。

コネクタはクラウド環境にも設置できます。を参照してください "こちらをご覧ください" 追加情報 の場合。

OCPクラスタに**Astra Trident**をインストール

- Helmを使用してTrident Operatorを導入します。手順を参照してください "こちらをご覧ください"
- バックエンドとストレージクラスを作成手順を参照してください "こちらをご覧ください"。

AWSの**OCP**クラスタを**Astra Control Center**に追加します。

AWSのOCPクラスタをAstra Control Centerに追加します。

マルチゾーンアーキテクチャに**Trident**の**CSI**トポロジ機能を使用

今日のクラウドプロバイダは、Kubernetes / OpenShiftのクラスタ管理者がゾーンベースのクラスタのノードを生成できるようにしています。ノードは、リージョンによって異なるアベイラビリティゾーンに配置することも、リージョンによって配置することもできます。マルチゾーンアーキテクチャでワークロード用のボリュームをプロビジョニングするために、 Astra Trident は CSI トポロジを使用します。CSI トポロジ機能を使用すると、領域およびアベイラビリティゾーンに基づいて、ボリュームへのアクセスをノードのサブセットに制

限できます。を参照してください "こちらをご覧ください" を参照してください。

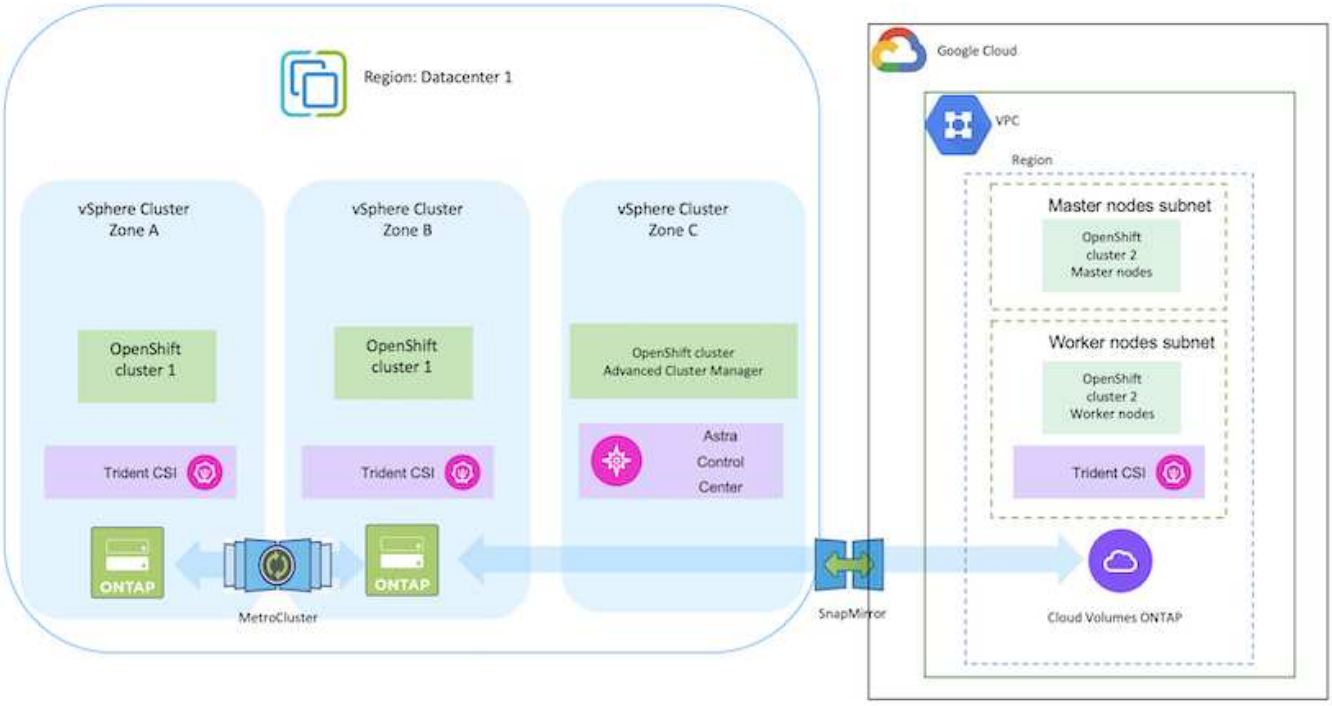
> Kubernetesでは2つのボリュームバインドモードがサポートされます。*-VolumeBindingMode_* が *_Immediate*（デフォルト）に設定されている場合、Astra Tridentはトポロジを認識せずにボリュームを作成します。永続ボリュームは、要求側ポッドのスケジュール要件に依存せずに作成されます。*-VolumeBindingMode_*が*_WaitForFirstConsumer*に設定されている場合、PVCの永続ボリュームの作成とバインドは、そのPVCを使用するポッドがスケジュールされて作成されるまで遅延します。これにより、トポロジの要件に応じたスケジュールの制約を満たすようにボリュームが作成されます。Astra Tridentのストレージバックエンドは、アベイラビリティゾーン（トポロジ対応バックエンド）に基づいて選択的にボリュームをプロビジョニングするように設計できます。ストレージクラスがそのようなバックエンドを使用する場合、ボリュームは、サポートされているリージョン / ゾーンでスケジュールされているアプリケーションから要求された場合にのみ作成されます。（Topology-Aware StorageClass）を参照してください "こちらをご覧ください" を参照してください。

GCPでのRed Hat OpenShift Containerプラットフォームの導入と設定

GCPでのRed Hat OpenShift Containerプラットフォームの導入と設定

このセクションでは、GCPでOpenShiftクラスタをセットアップおよび管理し、それらにステートフルアプリケーションを導入する方法の概要的なワークフローについて説明します。このスライドでは、Astra Tridentを使用してNetApp Cloud Volumes ONTAP ストレージを使用し、永続ボリュームを提供する方法を示しています。ステートフルアプリケーションに対してデータ保護と移行のアクティビティを実行するためのAstra Control Centerの使用方法について詳しく説明します。

次の図は、GCPに導入され、VPNを使用してデータセンターに接続されたクラスタを示しています。



GCPにRed Hat OpenShift Containerプラットフォームクラスタを導入する方法はいくつかあります。このセットアップの概要概要 には、使用した具体的な方法のドキュメントへのリンクが記載されています。その他の方法については、に記載されている関連リンクを参照してください "リソースセクション"。

セットアッププロセスは、次の手順に分けることができます。

CLIから**GCP**に**OCP**クラスタをインストールします。

- 記載されているすべての前提条件を満たしていることを確認します。 "こちらをご覧ください"。
- オンプレミスとGCP間のVPN接続については、pfsense VMを作成して設定しました。手順については、を参照してください "こちらをご覧ください"。
  - pfsenseのリモートゲートウェイアドレスは、Google Cloud PlatformでVPNゲートウェイを作成した後にのみ設定できます。
  - フェーズ2のリモートネットワークIPアドレスは、OpenShiftクラスタインストールプログラムが実行され、クラスタ用のインフラストラクチャコンポーネントが作成された後にのみ設定できます。
  - Google CloudのVPNは、インストールプログラムによってクラスタのインフラストラクチャコンポーネントが作成された後にのみ設定できます。
- 次に、GCPにOpenShiftクラスタをインストールします。
  - インストールプログラムとプルシークレットを入手し、ドキュメントに記載されている手順に従ってクラスタを導入する "こちらをご覧ください"。
  - インストールでGoogle Cloud PlatformにVPCネットワークが作成されます。また、Cloud DNSにプライベートゾーンを作成し、レコードを追加します。
    - VPCネットワークのCIDRブロックアドレスを使用してpfsenseを設定し、VPN接続を確立します。ファイアウォールが正しく設定されていることを確認します。
    - Google Cloud DNSのAレコードのIPアドレスを使用して、オンプレミス環境のDNSにAレコードを追加します。
  - クラスタのインストールが完了し、クラスタのコンソールにログインするためのkubeconfigファイルとユーザ名とパスワードが表示されます。

BlueXPを使用して**GCP**に**Cloud Volumes ONTAP**を導入

- Google Cloudにコネクタをインストールします。手順を参照してください "こちらをご覧ください"。
- コネクタを使用してGoogle CloudにCVOインスタンスを導入します。手順については、こちらを参照してください。 https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-gcp.html

GCPのOCPクラスタにAstra Tridentをインストール

- 図に示すように、Astra Tridentにはさまざまな導入方法がある "こちらをご覧ください"。
- このプロジェクトでは、Astra Tridentのオペレータを手順に従って手動で導入し、Astra Tridentをインストールしました。 "こちらをご覧ください"。
- バックエンドとストレージクラスを作成手順を参照してください "こちらをご覧ください"。

GCPのOCPクラスタをAstra Control Centerに追加します。

- クラスタの管理に必要な最小限の権限を含むクラスタロールを含むKubeConfigファイルを別途作成します。手順は次のとおりです。
  "こちらをご覧ください"。
- 手順に従ってクラスタをAstra Control Centerに追加
  "こちらをご覧ください"

マルチゾーンアーキテクチャに**Trident**の**CSI**トポロジ機能を使用

今日のクラウドプロバイダは、Kubernetes / OpenShiftのクラスタ管理者がゾーンベースのクラスタのノードを生成できるようにしています。ノードは、リージョンによって異なるアベイラビリティゾーンに配置することも、リージョンによって配置することもできます。マルチゾーンアーキテクチャでワークロード用のボリュームをプロビジョニングするために、 Astra Trident は CSI トポロジを使用します。CSI トポロジ機能を使用すると、領域およびアベイラビリティゾーンに基づいて、ボリュームへのアクセスをノードのサブセットに制限できます。を参照してください "こちらをご覧ください" を参照してください。

> Kubernetesでは2つのボリュームバインドモードがサポートされます。-***VolumeBindingMode***_が***_Immediate***（デフォルト）に設定されている場合、Astra Tridentはトポロジを認識せずにボリュームを作成します。永続ボリュームは、要求側ポッドのスケジュール要件に依存せずに作成されます。-***VolumeBindingMode***_が***_WaitForFirstConsumer***に設定されている場合、PVCの永続ボリュームの作成とバインドは、そのPVCを使用するポッドがスケジュールされて作成されるまで遅延します。これにより、トポロジの要件に応じたスケジュールの制約を満たすようにボリュームが作成されます。Astra Tridentのストレージバックエンドは、アベイラビリティゾーン（トポロジ対応バックエンド）に基づいて選択的にボリュームをプロビジョニングするように設計できます。ストレージクラスがそのようなバックエンドを使用する場合、ボリュームは、サポートされているリージョン / ゾーンでスケジュールされているアプリケーションから要求された場合にのみ作成されます。（Topology-Aware StorageClass）を参照してください "こちらをご覧ください" を参照してください。

デモビデオ

Google Cloud PlatformへのOpenShiftクラスタのインストール

Astra Control CenterへのOpenShiftクラスタのインポート

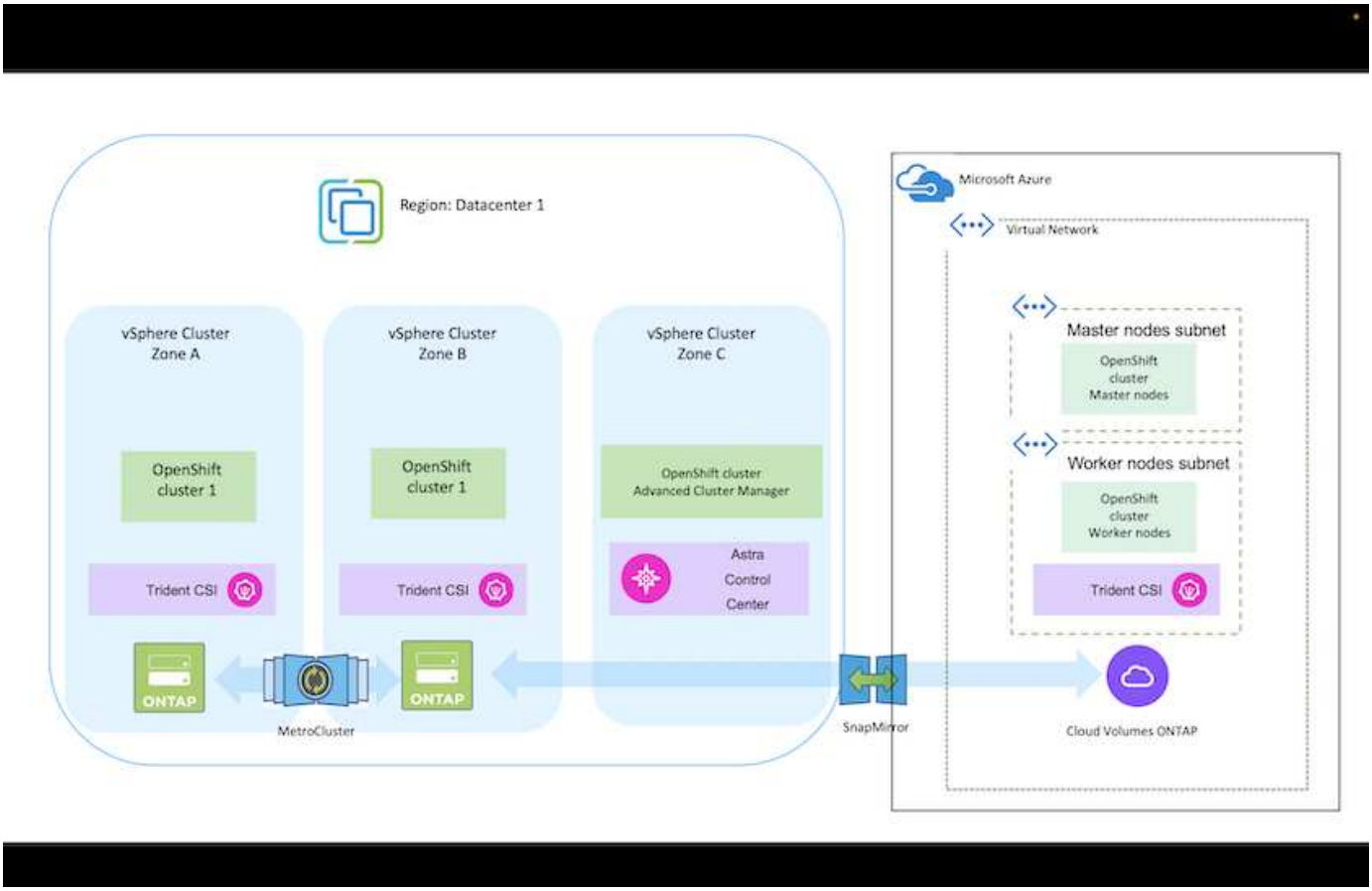
Azureでの**Red Hat OpenShift Container**プラットフォームの導入と設定

Azureでの**Red Hat OpenShift Container**プラットフォームの導入と設定

このセクションでは、AzureでOpenShiftクラスタをセットアップおよび管理し、それらにステートフルアプリケーションを導入する方法の概要的なワークフローについて説明

します。このスライドでは、Astra Trident / Astra Control Provisionerを使用して永続ボリュームを提供するNetApp Cloud Volumes ONTAPストレージを使用しています。ステートフルアプリケーションに対してデータ保護と移行のアクティビティを実行するためのAstra Control Centerの使用方法について詳しく説明します。

次の図は、Azureに導入され、VPNを使用してデータセンターに接続されたクラスタを示しています。



Red Hat OpenShift Containerプラットフォームクラスタを Azureに導入するには、いくつかの方法があります。このセットアップの概要概要 には、使用した具体的な方法のドキュメントへのリンクが記載されています。その他の方法については、に記載されている関連リンクを参照してください "リソースセクション"。

セットアッププロセスは、次の手順に分けることができます。

CLIを使用して**Azure**に**OCP**クラスタをインストールします。

- 記載されているすべての前提条件を満たしていることを確認します。 "こちらをご覧ください"。
- VPN、サブネット、ネットワークセキュリティグループ、およびプライベートDNSゾーンを作成します。VPNゲートウェイおよびサイト間VPN接続を作成します。
- オンプレミスとAzure間のVPN接続のために、pfsense VMを作成して設定しました。手順については、を参照してください "こちらをご覧ください"。
- インストールプログラムとプルシークレットを入手し、ドキュメントに記載されている手順に従ってクラスタを導入する "こちらをご覧ください"。
- クラスタのインストールが完了し、クラスタのコンソールにログインするためのkubeconfigファイルとユーザ名とパスワードが表示されます。

install-config.yamlファイルの例を以下に示します。

```
apiVersion: v1
baseDomain: sddc.netapp.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 512
        diskType: "StandardSSD_LRS"
      type: Standard_D2s_v3
      ultraSSDCapability: Disabled
      #zones:
      #- "1"
      #- "2"
      #- "3"
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 1024
        diskType: Premium_LRS
      type: Standard_D8s_v3
      ultraSSDCapability: Disabled
```

```
  replicas: 3
metadata:
  creationTimestamp: null
  name: azure-cluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    baseDomainResourceGroupName: ocp-base-domain-rg
    cloudName: AzurePublicCloud
    computeSubnet: ocp-subnet2
    controlPlaneSubnet: ocp-subnet1
    defaultMachinePlatform:
      osDisk:
        diskSizeGB: 1024
        diskType: "StandardSSD_LRS"
      ultraSSDCapability: Disabled
    networkResourceGroupName: ocp-nc-us-rg
    #outboundType: UserDefinedRouting
    region: northcentralus
    resourceGroupName: ocp-cluster-ncusrg
    virtualNetwork: ocp_vnet_ncus
publish: Internal
pullSecret:
```

BlueXPを使用して**Azure**に**Cloud Volumes ONTAP**を導入

- Azureにコネクタをインストールします。手順を参照してください "こちらをご覧ください"。
- コネクタを使用してAzureにCVOインスタンスを導入します。手順リンク：https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-azure.html [こちら]を参照してください。

AzureのOCPクラスタへの**Astra Control Provisioner**のインストール

- このプロジェクトでは、すべてのクラスタ（オンプレミスクラスタ、Astra Control Centerが導入されているオンプレミスクラスタ、およびAzureのクラスタ）にAstra Control Provisioner（ACP）をインストールしました。Astra Control Provisionerの詳細 "こちらをご覧ください"。
- バックエンドとストレージクラスを作成手順を参照してください "こちらをご覧ください"。

AzureのOCPクラスタを**Astra Control Center**に追加します。

- クラスタの管理に必要な最小限の権限を含むクラスタロールを含むKubeConfigファイルを別途作成します。手順は次のとおりです。
  "こちらをご覧ください"。
- 手順に従ってクラスタをAstra Control Centerに追加
  "こちらをご覧ください"

マルチゾーンアーキテクチャに**Trident**の**CSI**トポロジ機能を使用

今日のクラウドプロバイダは、Kubernetes / OpenShiftのクラスタ管理者がゾーンベースのクラスタのノードを生成できるようにしています。ノードは、リージョンによって異なるアベイラビリティゾーンに配置することも、リージョンによって配置することもできます。マルチゾーンアーキテクチャでワークロード用のボリュームをプロビジョニングするために、 Astra Trident は CSI トポロジを使用します。CSI トポロジ機能を使用すると、領域およびアベイラビリティゾーンに基づいて、ボリュームへのアクセスをノードのサブセットに制限できます。を参照してください "こちらをご覧ください" を参照してください。

> Kubernetesでは2つのボリュームバインドモードがサポートされます。-***VolumeBindingMode***_が***_Immediate***（デフォルト）に設定されている場合、Astra Tridentはトポロジを認識せずにボリュームを作成します。永続ボリュームは、要求側ポッドのスケジュール要件に依存せずに作成されます。-***VolumeBindingMode***_が***_WaitForFirstConsumer***に設定されている場合、PVCの永続ボリュームの作成とバインドは、そのPVCを使用するポッドがスケジュールされて作成されるまで遅延します。これにより、トポロジの要件に応じたスケジュールの制約を満たすようにボリュームが作成されます。Astra Tridentのストレージバックエンドは、アベイラビリティゾーン（トポロジ対応バックエンド）に基づいて選択的にボリュームをプロビジョニングするように設計できます。ストレージクラスがそのようなバックエンドを使用する場合、ボリュームは、サポートされているリージョン / ゾーンでスケジュールされているアプリケーションから要求された場合にのみ作成されます。（Topology-Aware StorageClass）を参照してください "こちらをご覧ください" を参照してください。

デモビデオ

Astra Controlを使用したアプリケーションのフェイルオーバーとフェイルバック

Astra Control Centerを使用したデータ保護

このページには、VMware vSphereまたはAstra Control Center（ACC）を使用してクラウドで実行されるRed Hat OpenShift Containerベースのアプリケーションのデータ保護オプションが表示されます。

ユーザがRed Hat OpenShiftを使用してアプリケーションを最新化する過程で、偶発的な削除やその他の人的エラーからユーザを保護するためのデータ保護戦略を策定する必要があります。多くの場合、データを管理か

ら保護するために、規制やコンプライアンスの目的で保護戦略が必要になります。

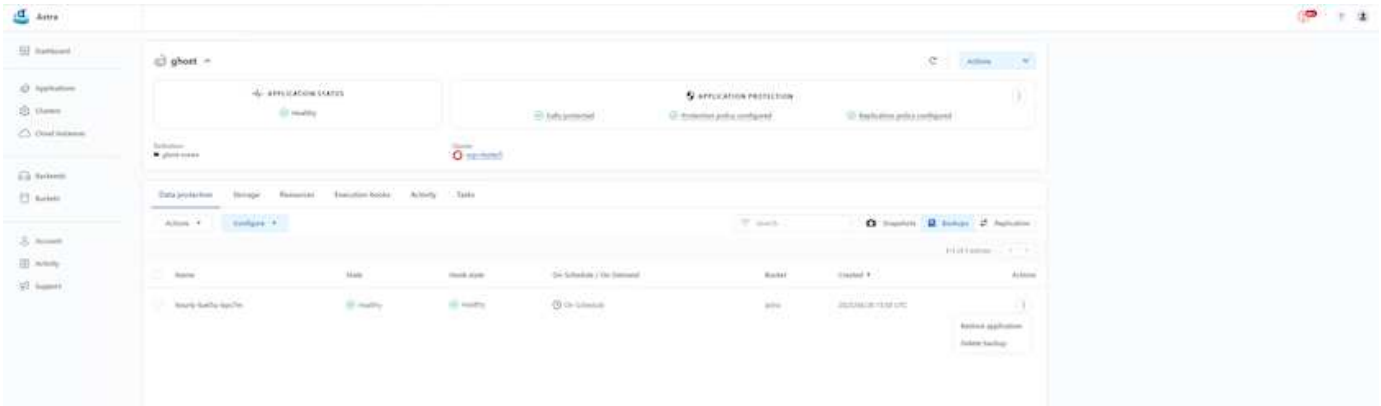
データ保護の要件は、ポイントインタイムコピーへのリバートから別の障害ドメインへの自動フェイルオーバーまで、人手を介さずにさまざまです。多くのお客様がONTAP をKubernetesアプリケーションに最適なストレージプラットフォームとして選択しています。その理由は、マルチテナンシー、マルチプロトコル、ハイパフォーマンスと容量のサービス、マルチサイト環境のレプリケーションとキャッシュ、セキュリティと柔軟性などの豊富な機能があるからです。

お客様は、データセンターの拡張機能としてクラウド環境を設定している場合があります。これにより、クラウドのメリットを活用できるだけでなく、将来的にワークロードを移行するための適切な位置付けを得ることができます。このようなお客様にとって、OpenShiftアプリケーションとデータをクラウド環境にバックアップすることは避けられません。その後、アプリケーションと関連データをクラウドまたはデータセンターのOpenShiftクラスタにリストアできます。

ACCを使用したバックアップと復元

アプリケーション所有者は、ACCによって検出されたアプリケーションを確認および更新できます。ACCはCSIを使用してSnapshotコピーを作成し、ポイントインタイムSnapshotコピーを使用してバックアップを実行できます。バックアップ先は、クラウド環境内のオブジェクトストアにすることができます。スケジュールされたバックアップの保護ポリシーと保持するバックアップバージョンの数を設定できます。最小RPOは1時間です。

ACCを使用したバックアップからのアプリケーションのリストア

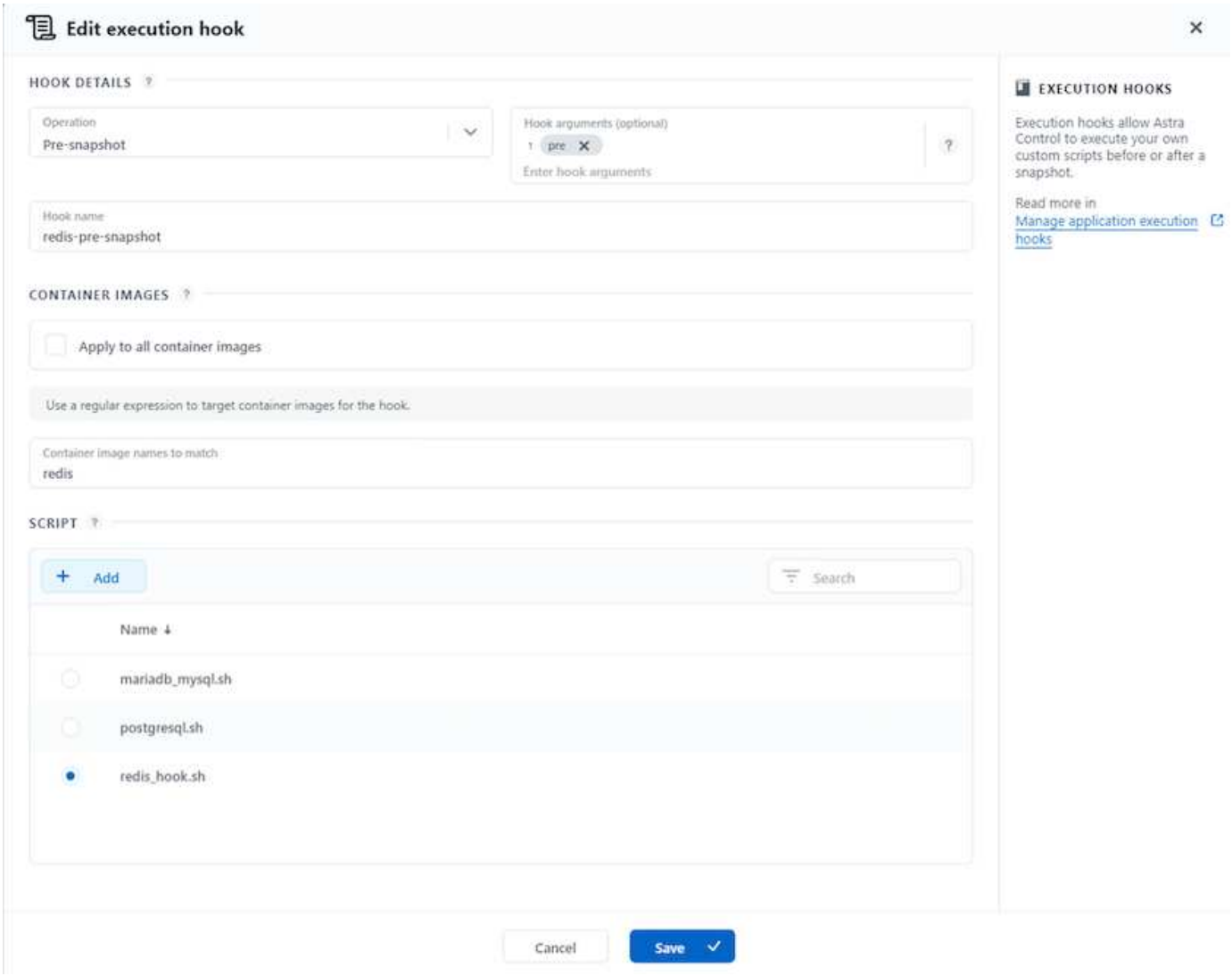


アプリケーション固有の実行フック

ストレージアレイレベルのデータ保護機能を使用できますが、アプリケーションのバックアップとリストアの整合性を確保するために追加の手順が必要になることがよくあります。アプリケーション固有の追加手順は次のとおりです。- Snapshotコピーの作成前または作成後。-バックアップの作成前または作成後。- Snapshotコピーまたはバックアップからリストアしたあと。Astra Controlでは、実行フックと呼ばれるカスタムスクリプトとしてコード化されたアプリケーション固有の手順を実行できます。

ネットアップの "オープンソースプロジェクトVerda" 一般的なクラウドネイティブアプリケーションの実行フックを提供し、アプリケーションを簡単に保護し、堅牢で、オーケストレーションを容易にします。リポジトリにないアプリケーションに十分な情報がある場合は、そのプロジェクトに貢献してください。

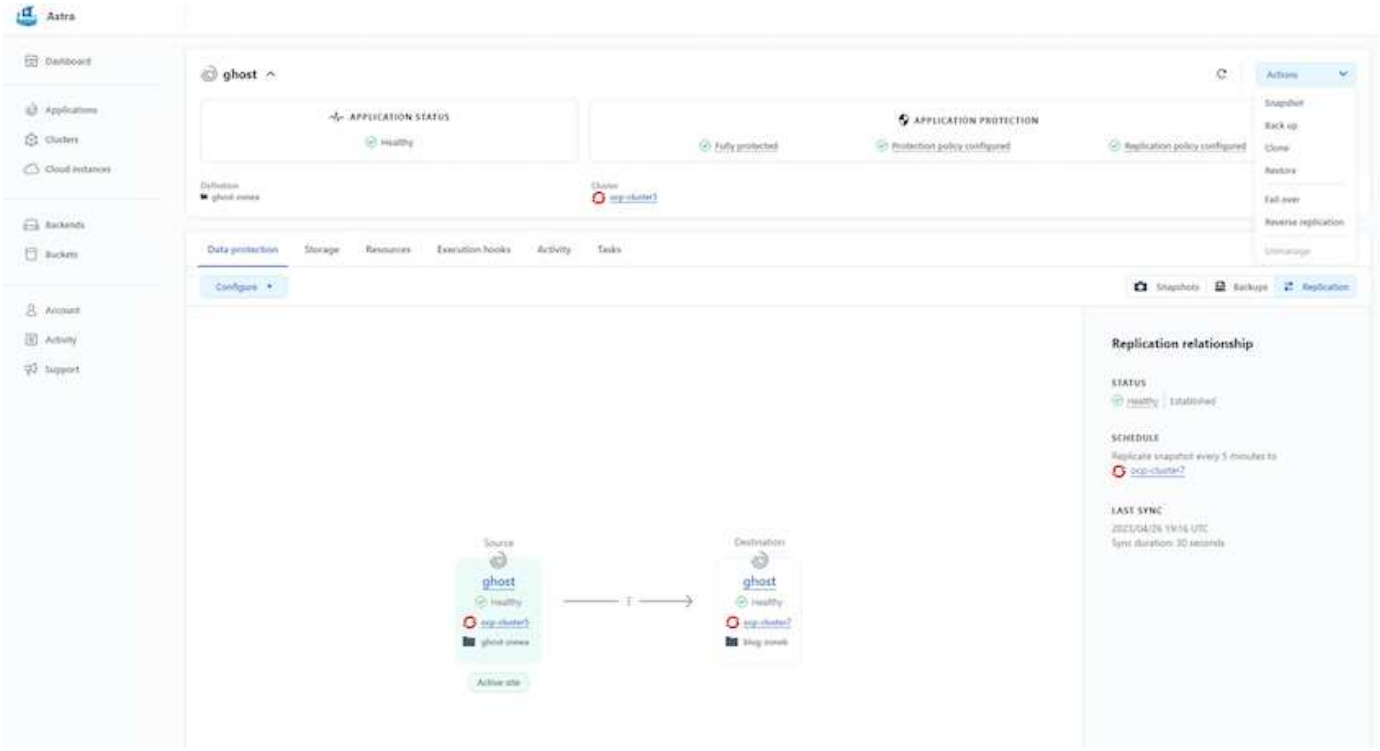
redisアプリケーションの**pre-Snapshot**用のサンプル実行フック。



ACCを使用したレプリケーション

リージョンを保護する場合や、RPOとRTOの低い解決策 を実現する場合は、別のサイト（できれば別のリージョン）で実行されている別のKubernetesインスタンスにアプリケーションをレプリケートできます。ACCは、最短5分でRPOを実現するONTAP 非同期SnapMirrorを利用します。を参照してください "こちらをご覧ください" SnapMirrorのセットアップ手順を参照してください。

ACCを使用した**SnapMirror**



SANエコノミーおよびNASエコノミーのストレージドライバは、レプリケーション機能をサポートしていません。を参照してください "こちらをご覧ください" を参照してください。

デモビデオ：

"Astra Control Centerを使用したディザスタリカバリのデモビデオ"

Astra Control Centerによるデータ保護

Astra Control Centerのデータ保護機能の詳細を確認できます "こちらをご覧ください"

ACCを使用したディザスタリカバリ（レプリケーションを使用したフェイルオーバーとフェイルバック）

Astra Controlを使用したアプリケーションのフェイルオーバーとフェイルバック

Astra Control Centerを使用したデータ移行

このページには、Astra Control Center（ACC）を使用したRed Hat OpenShiftクラスタ上のコンテナワークロードのデータ移行オプションが表示されます。具体的には、ACCを使用して、一部のワークロードまたはすべてのワークロードをオンプレミスのデータセンターからクラウドに移動したり、テスト目的でアプリケーションをクラウドにクローニングしたり、データセンターからクラウドに移行したりできます

データ移行

アプリケーションをある環境から別の環境に移行するには、ACCの次の機能のいずれかを使用できます。

- レプリケーション

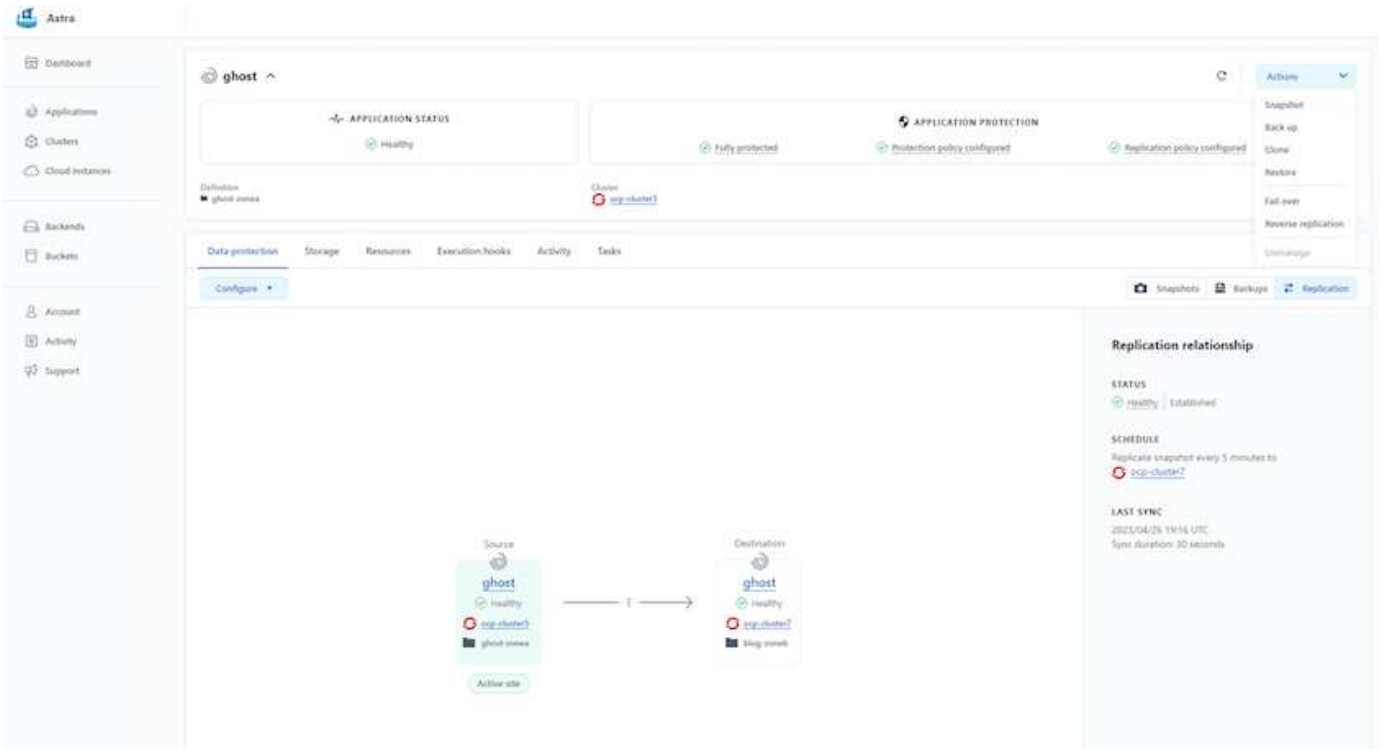
- バックアップとリストア
- クローン

を参照してください "データ保護セクション" レプリケーションおよびバックアップとリストアオプションの場合。

を参照してください "こちらをご覧ください" クローン作成の詳細については、を参照してください。

Astraレプリケーション機能は、Trident Container Storage Interface（CSI）でのみサポートされます。ただし、NASエコノミードライバとSANエコノミードライバでは、レプリケーションはサポートされていません。

ACCを使用したデータ複製の実行



Red Hat OpenShift Containerワークロード向けのネットアップハイブリッドマルチクラウドソリューション

概要

ネットアップでは、従来型エンタープライズアプリケーションを最新化し、Kubernetesを中心に構築されたコンテナとオーケストレーションプラットフォームを使用して新しいアプリケーションを構築するお客様が大幅に増えています。Red Hat OpenShift Container Platformは、多くのお客様に採用されている例の1つです。

企業内でコンテナを採用するお客様がますます増えています。ネットアップは、ステートフルアプリケーションの永続的ストレージのニーズに加え、データ保護、データセキュリティ、データ移行などの従来のデータ管理のニーズにも応えることができます。しかし、これらのニーズは、さまざまな戦略、ツール、方法を使用して満たしています。

- NetApp ONTAP **ベースのストレージオプションを次に示します。コンテナとKubernetes環境にセキュリ

ティ、データ保護、信頼性、柔軟性を提供します。

- オンプレミスの自己管理型ストレージ：

- ネットアップファブリック接続ストレージ（FAS ）、ネットアップオールフラッシュFAS アレイ（AFF ）、ネットアップオールSANアレイ（ASA ）、ONTAP Select

- オンプレミスのプロバイダ管理ストレージ：

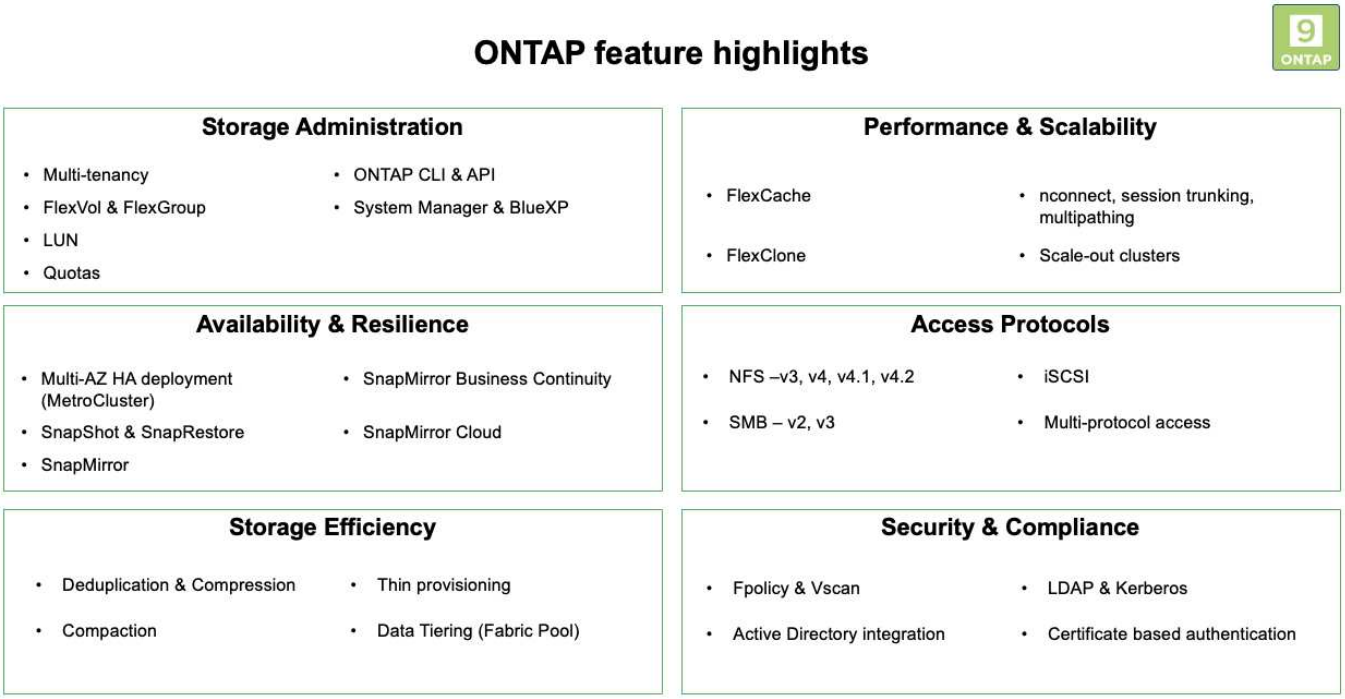
- NetApp Keystone が提供するストレージサービス（STaaS）

- クラウド内の自己管理型ストレージ：

- NetApp Cloud Volumes ONTAP（CVO）は、ハイパースケーラに自己管理型ストレージを提供します

- クラウド上のプロバイダが管理するストレージ：

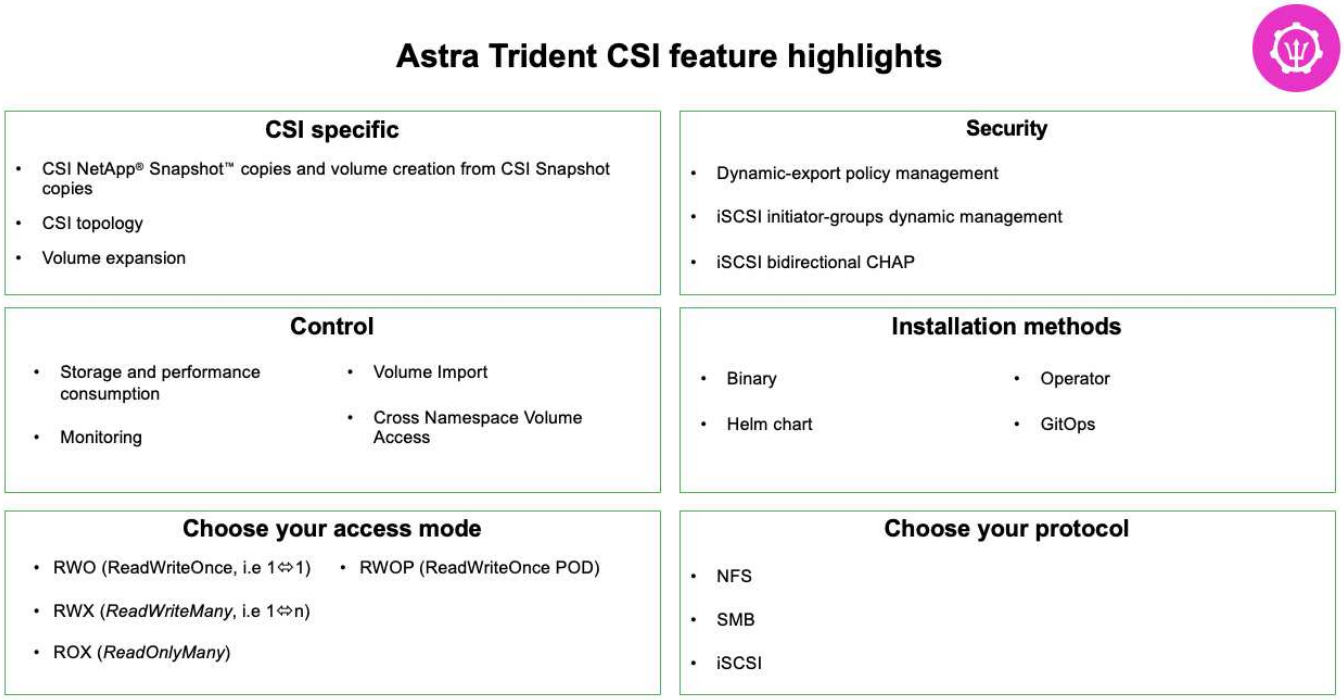
- Cloud Volumes Service for Google Cloud（CVS）、Azure NetApp Files （ANF）、Amazon FSx for NetApp ONTAP は、ハイパースケーラにフルマネージドストレージを提供します



- NetApp BlueXP **を使用すると、すべてのストレージ資産とデータ資産を単一のコントロールプレーン/インターフェイスから管理できます。

BlueXPを使用して、クラウドストレージ（Cloud Volumes ONTAP やAzure NetApp Files など）の作成と管理、データの移動、保護、分析、オンプレミスやエッジの多くのストレージデバイスの管理を行うことができます。

- NetApp Astra Trident **はCSI準拠のストレージオーケストレーションツールです。上記のさまざまなネットアップストレージオプションを利用して、永続的ストレージをすばやく簡単に利用できます。ネットアップが保守、サポートしているオープンソースのソフトウェアです。



ビジネスクリティカルなコンテナワークロードに必要なのは、永続的ボリュームだけではありません。同社のデータ管理要件では、アプリケーションのKubernetesオブジェクトの保護と移行も必要です。

アプリケーションデータには、ユーザデータに加えてKubernetesオブジェクトが含まれます。例を次に示します。 -ポッド仕様、PVC、デプロイ、サービスなどのKubernetesオブジェクト- 設定マップやシークレットなどのカスタム設定オブジェクト- Snapshotコピー、バックアップ、クローンなどの永続的データ- CRSやCRDなどのカスタムリソース

- NetApp Astra Control **は、フルマネージドと自己管理型の両方のソフトウェアとして提供され、堅牢なアプリケーションデータ管理のためのオーケストレーションを提供します。を参照してください "Astra のドキュメント" を参照してください。

このリファレンスドキュメントでは、NetApp Astra Control Centerを使用して、Red Hat OpenShiftコンテナプラットフォームに導入されたコンテナベースアプリケーションの移行と保護について検証します。また、解決策 では、コンテナプラットフォームを管理するためのRed Hat Advanced Cluster Management（ACM）の導入と使用に関する詳細についても説明しています。また、Astra Trident CSIプロビジョニングツールを使用して、ネットアップストレージとRed Hat OpenShiftコンテナプラットフォームを統合する方法についても詳しく説明します。Astra Control Centerはハブクラスタに導入され、コンテナアプリケーションとその永続的ストレージライフサイクルの管理に使用されます。最後に、Amazon FSx for NetApp ONTAP （FSxN）を永続的ストレージとして使用し、AWS（ROSA）のマネージドRed Hat OpenShiftクラスタ上のコンテナワークロードのレプリケーション、フェイルオーバー、フェイルバックのための解決策 を提供します。

NetApp解決策 とAWS上のマネージドRed Hat OpenShift Containerプラットフォームのワークロード

NetApp解決策 とAWS上のマネージドRed Hat OpenShift Containerプラットフォームのワークロード

お客様は、「クラウド生まれ」の場合もあれば、一部のワークロードやすべてのワークロードをデータセンターからクラウドに移行する準備ができた時点で、最新化に向けた取り組みを進めている場合もあります。ワークロードの実行に、プロバイダが管理するOpenShiftコンテナとプロバイダが管理するネットアップストレージをクラウドで使用

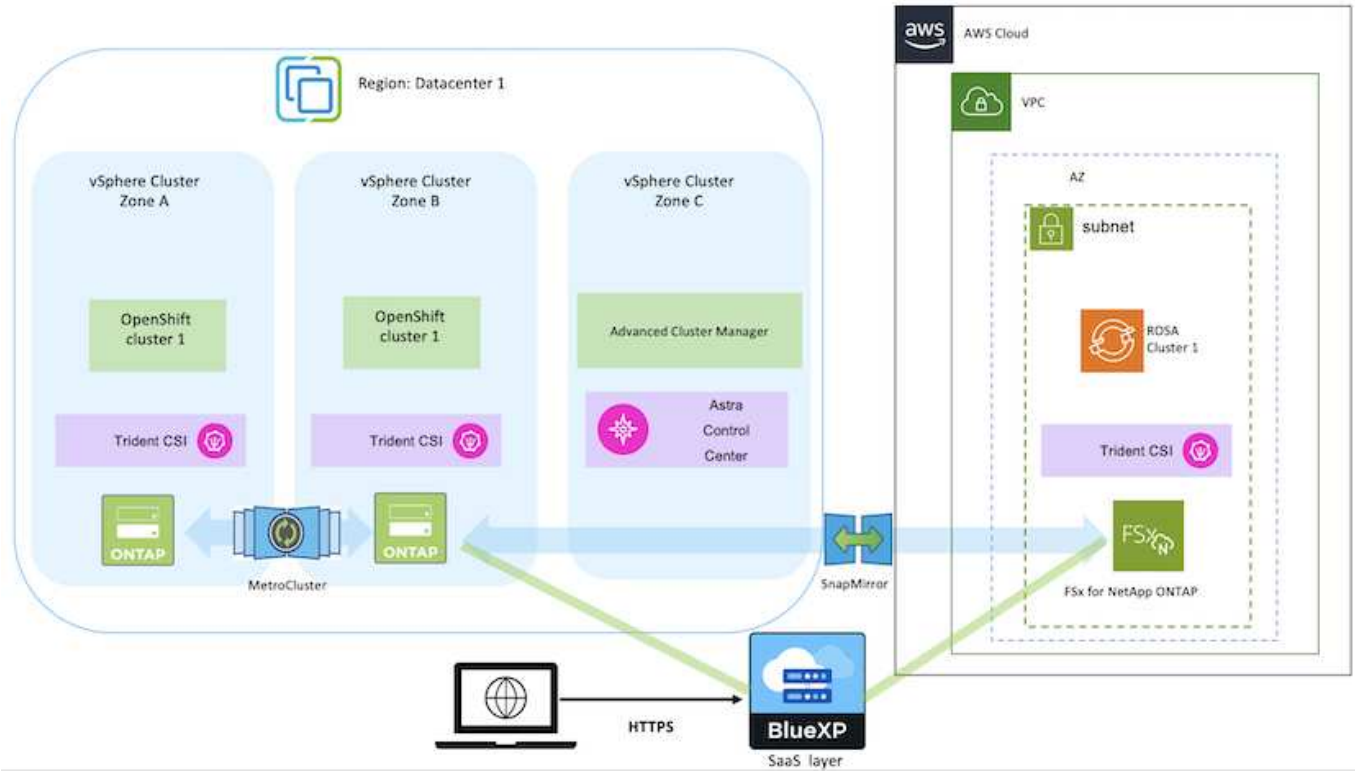
することもできます。コンテナワークロードに対応した本番環境を成功させるためには、マネージドRed Hat OpenShiftコンテナクラスタ（ROSA）をクラウドに計画して導入する必要があります。AWSクラウドにいる場合は、ストレージのニーズに合わせてFSx for NetApp ONTAP を導入することもできます。

FSx for NetApp ONTAP は、AWSのコンテナ導入にデータの保護、信頼性、柔軟性を提供します。Astra Tridentは、お客様のステートフルアプリケーション向けに永続的FSxNストレージを利用するための動的ストレージプロビジョニングツールとして機能します。

ROSAは、コントロールプレーンノードが複数のアベイラビリティゾーンに分散した状態でHAモードで導入できるため、FSx ONTAP は、高可用性を提供し、AZの障害から保護するマルチAZオプションを使用してプロビジョニングすることもできます。

ファイルシステムの優先アベイラビリティゾーン（AZ）からAmazon FSxファイルシステムにアクセスする場合、データ転送料金は発生しません。価格設定の詳細については、を参照してください "こちらをご覧ください"。

OpenShift Containerワークロード向けのデータ保護と移行用解決策

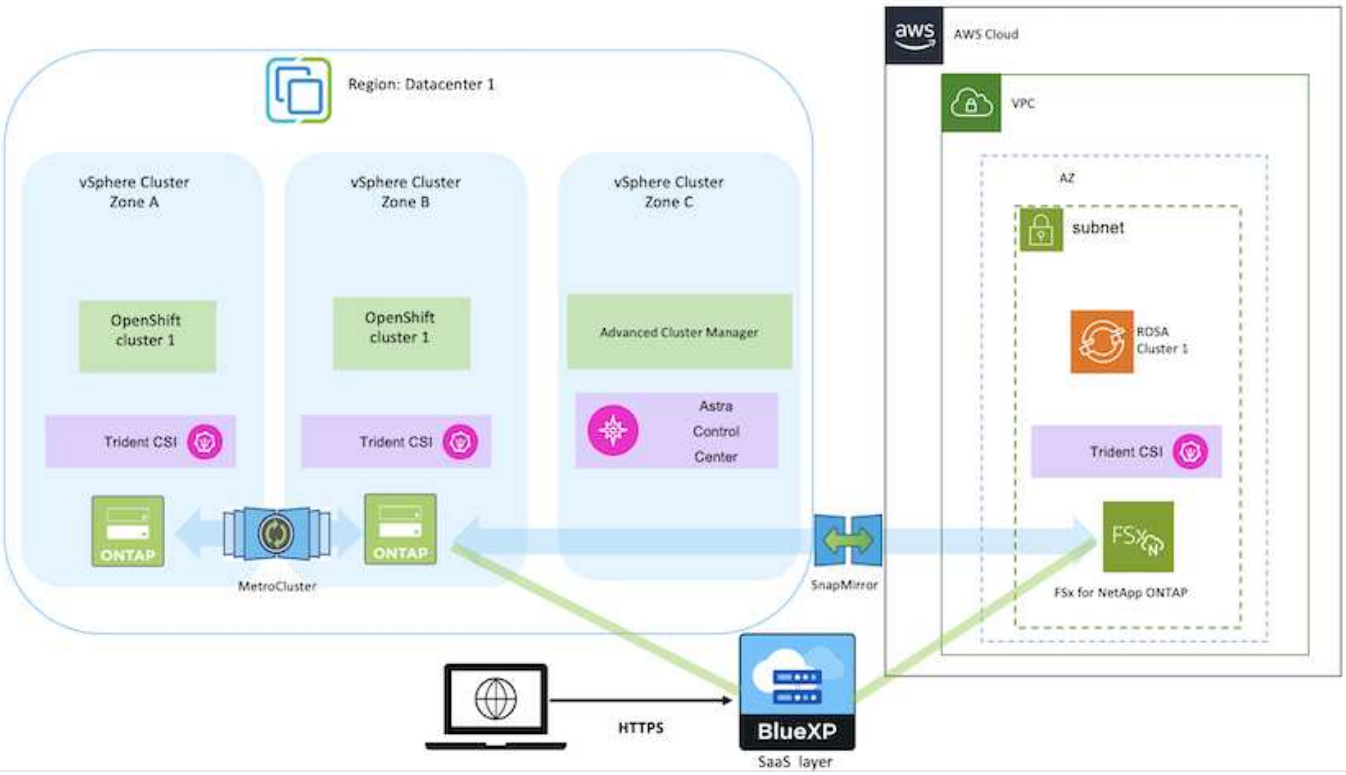


AWSにマネージド**Red Hat OpenShift Container**プラットフォームを導入して設定します

このセクションでは、AWS（ROSA）でマネージドRed Hat OpenShiftクラスタをセットアップする大まかなワークフローについて説明します。このスライドでは、Astra TridentによるストレージバックエンドとしてManaged FSx for NetApp ONTAP （FSxN）を使用して永続ボリュームを提供しています。BlueXPを使用したAWSへのFSxNの導入について詳しく説明します。また、ROSAクラスタ上のステートフルアプリケーションに対して、BlueXPとOpenShiftのGitOps（Argo CD）を使用してデータ保護と移行の

アクティビティを実行する方法についても詳しく説明します。

次の図は、AWSに導入され、FSxNをバックエンドストレージとして使用するROSAクラスタを示しています。



この解決策 は、AWSの2つのVPCで2つのROSAクラスタを使用して検証されました。各ROSAクラスタは、Astra Tridentを使用してFSxNに統合されています。ROSAクラスタとFSxNをAWSに導入するには、いくつかの方法があります。このセットアップの概要概要 には、使用した具体的な方法のドキュメントへのリンクが記載されています。その他の方法については、に記載されている関連リンクを参照してください "リソースセクション"。

セットアッププロセスは、次の手順に分けることができます。

ROSAクラスタをインストールします

- 2つのVPCを作成し、VPC間にVPCピアリング接続を設定します。
- を参照してください "こちらをご覧ください" ROSAクラスタのインストール手順については、を参照してください。

FSxNをインストールします

- BlueXPからVPCにFSxNをインストールします。を参照してください "こちらをご覧ください"（BlueXPアカウントの作成と使用を開始するため）を参照してください "こちらをご覧ください" FSxNのインストールに使用します。を参照してください "こちらをご覧ください" FSxNを管理するためにAWSでコネクタを作成します。
- AWSを使用してFSxNを導入する。を参照してください "こちらをご覧ください" AWSコンソールを使用した導入用。

ROSAクラスタへの**Trident**のインストール（**Helm**チャートを使用）

- Helmチャートを使用して、ROSAクラスタにTridentをインストールします。HelmチャートのURL：https://netapp.github.io/trident-helm-chart

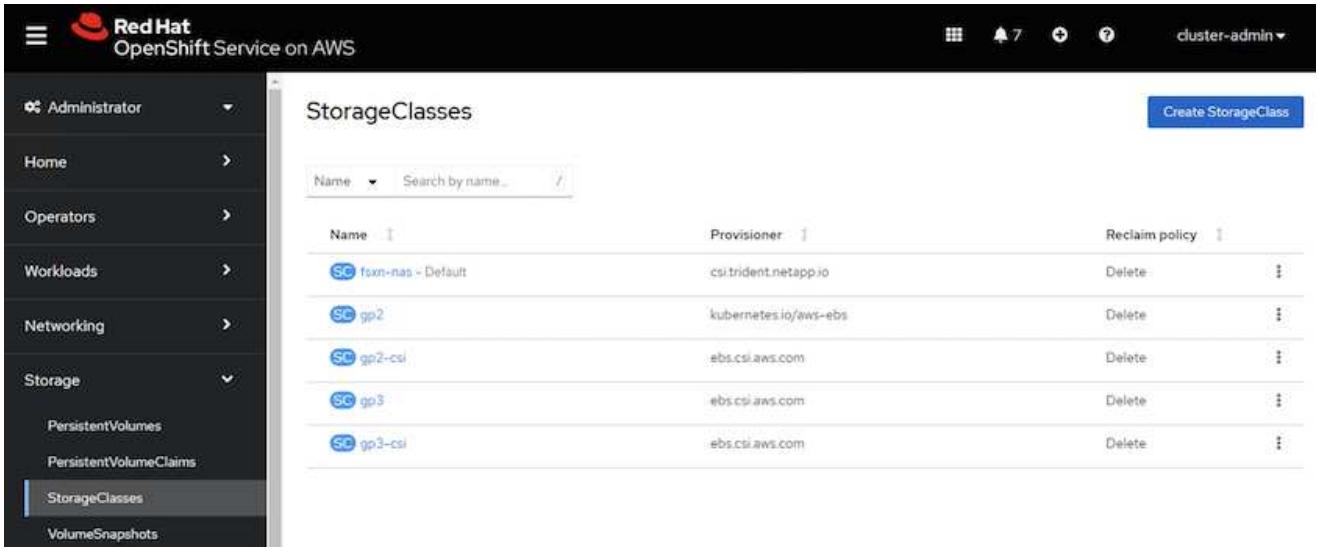
ROSAクラスタ向けのFSxNとAstra Tridentの統合

OpenShift GitOpsを使用すると、ApplicationSetを使用してArgoCDに登録されたすべての管理対象クラスタにAstra Trident CSIを導入できます。

```
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: trident-operator
spec:
  generators:
  - clusters: {}
    # selector:
    #   matchLabels:
    #     tridentversion: '23.04.0'
  template:
    metadata:
      name: '{{nameNormalized}}-trident'
    spec:
      destination:
        namespace: trident
        server: '{{server}}'
      source:
        repoURL: 'https://netapp.github.io/trident-helm-chart'
        targetRevision: 23.04.0
        chart: trident-operator
      project: default
      syncPolicy:
        syncOptions:
          - CreateNamespace=true
```

Tridentを使用したバックエンドとストレージクラスの作成（**FSxN**向け）

- を参照してください "こちらをご覧ください" バックエンドとストレージクラスの作成の詳細については、を参照してください。
- OpenShiftコンソールから、Trident CSIを使用してFsxN用に作成したストレージクラスをデフォルトで作成します。下のスクリーンショットを参照：



OpenShift GitOpsを使用したアプリケーションの導入（**Argo CD**）

- クラスタにOpenShift GitOpsオペレータをインストールします。手順を参照してください "こちらをご覧ください"。
- クラスタ用の新しいArgo CDインスタンスをセットアップします。手順を参照してください "こちらをご覧ください"。

Argo CDのコンソールを開き、アプリをデプロイします。たとえば、Argo CDとHelm Chartを使用してJenkins Appをデプロイできます。アプリケーションを作成するときに、次の詳細が提供されました。プロジェクト:デフォルトクラスタ: https://kubernetes.default.svc名前空間: Jenkins Helm ChartのURL : https://charts.bitnami.com/bitnami

Helmパラメータ：global.storageClass：fsxn -nas

データ保護

このページには、Astra Control Serviceを使用したAWS（ROSA）クラスタでのマネージドRed Hat OpenShiftのデータ保護オプションが表示されます。Astra Control Service（ACS）では、使いやすいグラフィカルユーザインターフェイスを使用して、クラスタの追加、クラスタ上で実行されるアプリケーションの定義、アプリケーション対応のデータ管理アクティビティの実行を行うことができます。ACS関数には、ワークフローの自動化を可能にするAPIを使用してアクセスすることもできます。

Astra Control（ACSまたはACC）に搭載されるのは、NetApp Astra Tridentです。Astra Tridentは、Red Hat OpenShift、EKS、AKS、SUSE Rancher、Anthosなど、いくつかのタイプのKubernetesクラスタを統合しま

す。 FAS / AFF、ONTAP Select、CVO、Google Cloud Volumes Service、Azure NetApp Files、Amazon FSx for NetApp ONTAPなど、さまざまな種類のNetApp ONTAPストレージを使用できます。

ここでは、ACSを使用した次のデータ保護オプションの詳細について説明します。

- ある地域で実行されているROSAアプリケーションのバックアップと復元と、別の地域への復元を示すビデオ。
- ROSAアプリケーションのスナップショットと復元を示すビデオ。
- ROSAクラスタ（Amazon FSx for NetApp ONTAP）のインストール、NetApp Astra Tridentを使用したストレージバックエンドとの統合、ROSAクラスタへのPostgreSQLアプリケーションのインストール、ACSを使用したアプリケーションのスナップショットの作成とそこからのアプリケーションのリストアの詳細を順を追って説明します。
- ACSを使用してFSx for ONTAPを使用してROSAクラスタ上のMySQLアプリケーションのスナップショットを作成し、そのスナップショットからリストアする手順の詳細を示すブログ。

バックアップ/バックアップからのリストア

次のビデオは、あるリージョンで実行されているROSAアプリケーションのバックアップと、別のリージョンへのリストアを示しています。

AWSでのRed Hat OpenShift向けFSx NetApp ONTAPサービス

Snapshot / Snapshotからのリストア

次のビデオでは、ROSAアプリケーションのスナップショットを作成してからスナップショットから復元する方法を示します。

Amazon FSx for NetApp ONTAPストレージを使用したRed Hat OpenShift Service on AWS（ROSA）クラスタでのアプリケーションのスナップショット/リストア

ブログ

- "Amazon FSxストレージを使用したROSAクラスタ上のアプリケーションのデータ管理にAstra Control Serviceを使用"

スナップショットを作成してそこからリストアするためのステップバイステップの詳細

セットアップの前提条件

- "AWS アカウント"
- "Red Hat OpenShiftアカウント"
- IAMユーザ "適切な権限" ROSAクラスタを作成してアクセスするには
- "AWS CLI"
- "ローザCLI"
- "OpenShift CLI"（OC）
- サブネットと適切なゲートウェイおよびルートを備えたvPC
- "Rosaクラスタインストール済み" VPCに挿入

- "NetApp ONTAP 対応の Amazon FSX" 同じVPCに作成
- ROSAクラスタへのアクセス "OpenShiftハイブリッドクラウドコンソール"

次のステップ

1. 管理者ユーザを作成し、クラスタにログインします。
2. クラスタ用のkubeconfigファイルを作成します。
3. クラスタにAstra Tridentをインストール
4. Trident CSIプロビジョニングツールを使用して、バックエンド、ストレージクラス、Snapshotクラスの構成を作成
5. クラスタにPostgreSQLアプリケーションを導入します。
6. データベースを作成し、レコードを追加します。
7. クラスタをACSに追加します。
8. ACSでアプリケーションを定義します。
9. ACSを使用してスナップショットを作成します。
10. PostgreSQLアプリケーションでデータベースを削除します。
11. ACSを使用してスナップショットから復元します。
12. アプリがスナップショットから復元されたことを確認します。

1：管理者ユーザを作成してクラスタにログイン

次のコマンドを使用してadminユーザを作成し、ROSAクラスタにアクセスします（adminユーザを作成する必要があるのは、インストール時にadminユーザを作成しなかった場合だけです）。

```
rosa create admin --cluster=<cluster-name>
```

次のような出力が表示されます。を使用してクラスタにログインします。 `oc login` コマンドは出力に表示されます。

```
W: It is recommended to add an identity provider to login to this cluster.
See 'rosa create idp --help' for more information.
I: Admin account has been added to cluster 'my-rosa-cluster'. It may take up
to a minute for the account to become active.
I: To login, run the following command:
oc login https://api.my-rosa-cluster.abcd.p1.openshiftapps.com:6443 \
--username cluster-admin \
--password FWGYL-2mkJI-00000-00000
```

トークンを使用してクラスタにログインすることもできます。クラスタの作成時にすでにadminユーザを作成している場合は、Red Hat OpenShift Hybrid Cloudコンソールからadminユーザのクレデンシャルを使用してクラスタにログインできます。右上隅にログインしているユーザの名前が表示されていることをクリックすると、 `oc login` コマンドラインのコマンド（トークンログイン）。

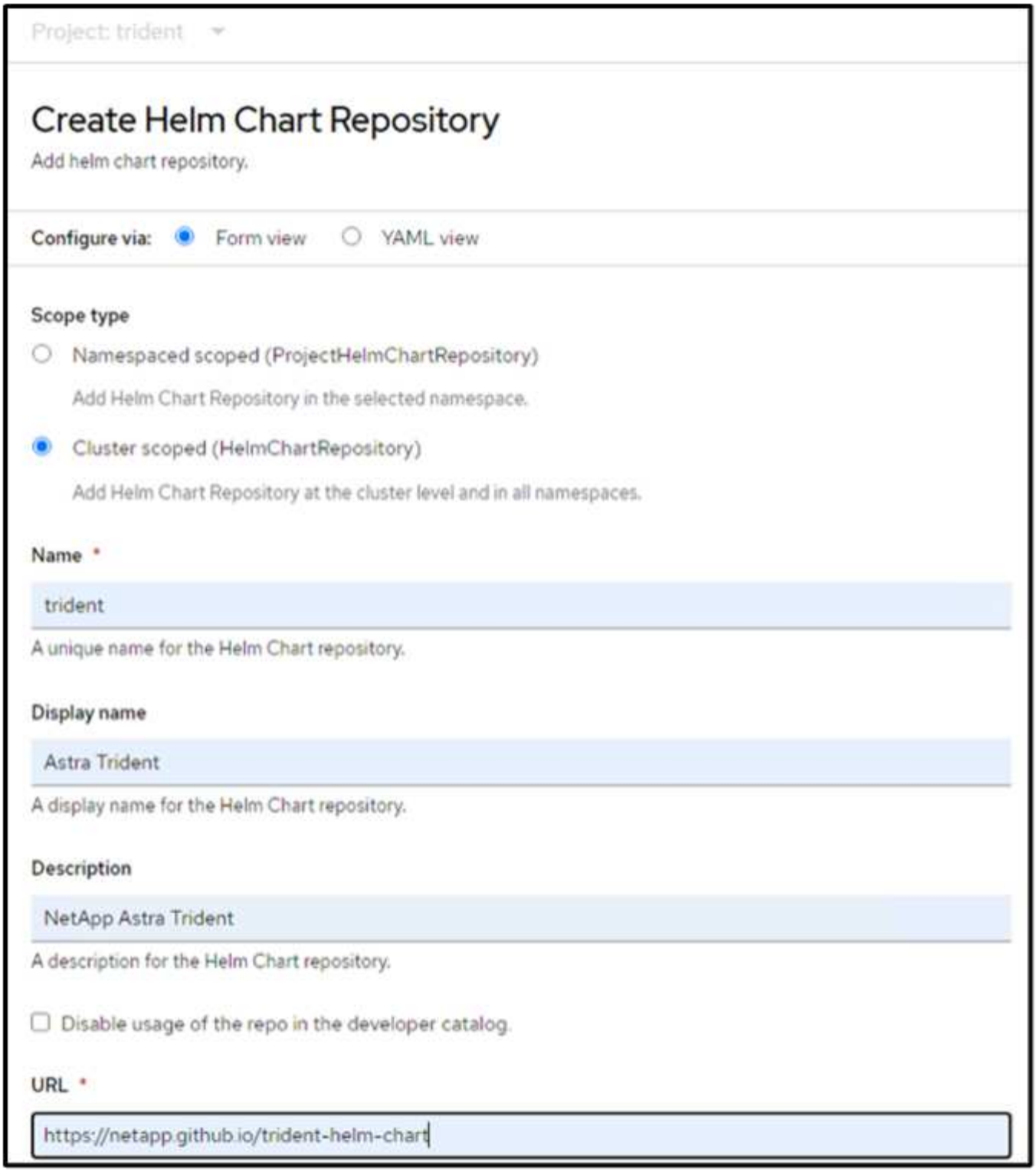
2.クラスタの**kubeconfig**ファイルを作成

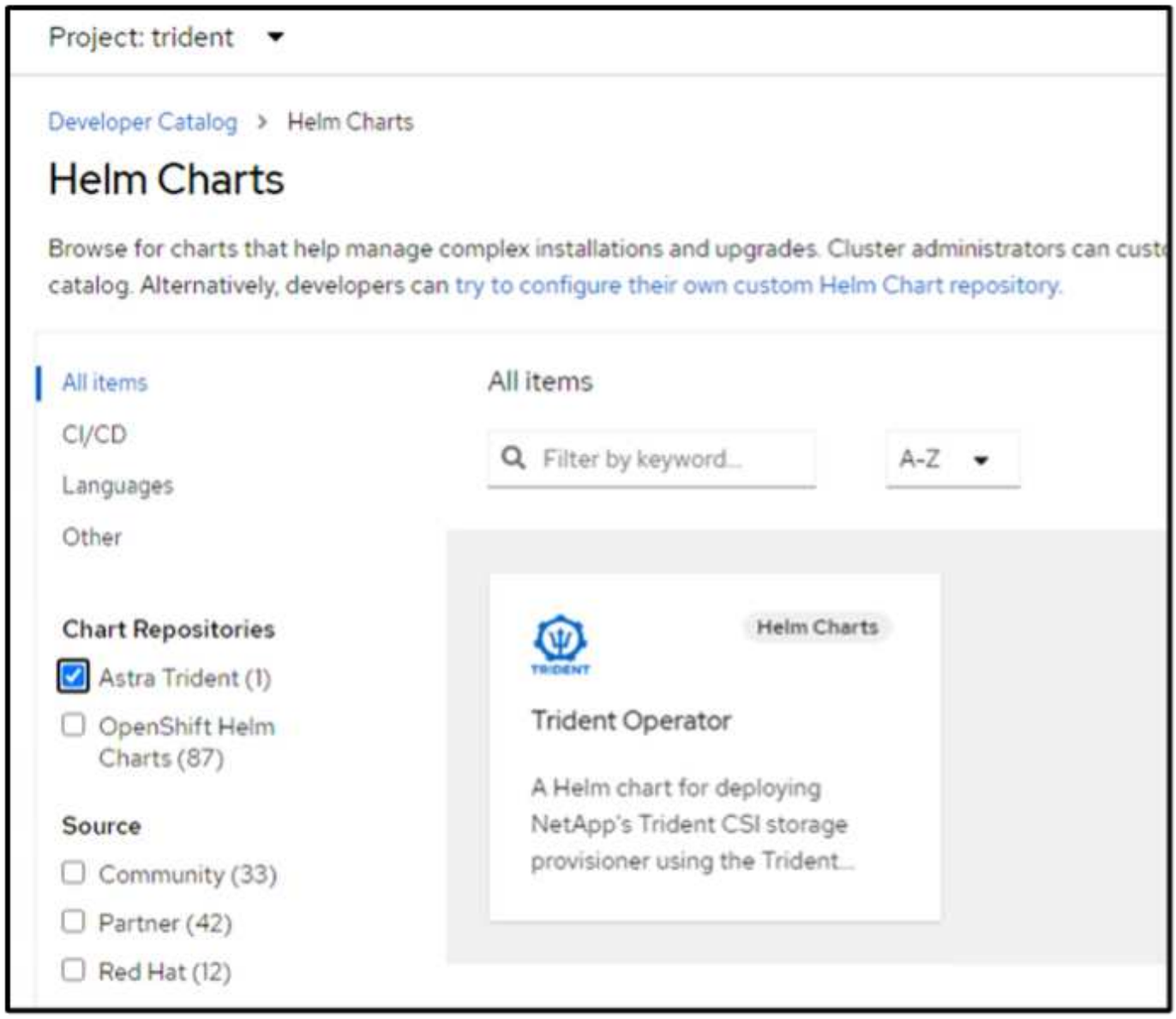
手順に従います "こちらをご覧ください" ROSAクラスタ用のkubeconfigファイルを作成します。このkubeconfigファイルは、あとでクラスタをACSに追加するときに使用されます。

3.クラスタへの**Astra Trident**のインストール

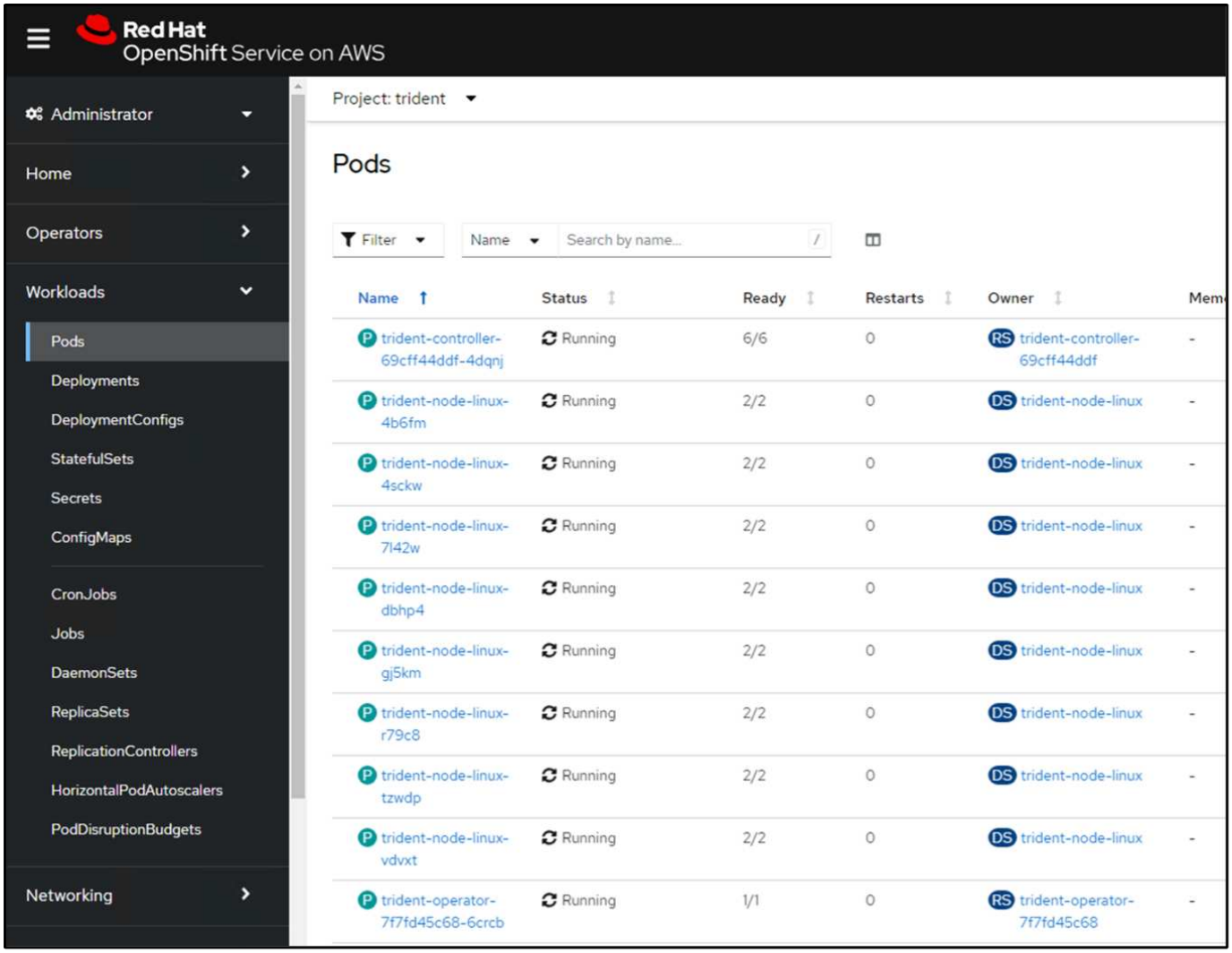
ROSAクラスタにAstra Trident（最新バージョン）をインストールこれを行うには、以下の手順のいずれかに従うことができます。 "こちらをご覧ください"。クラスタのコンソールからhelmを使用してTridentをインストールするには、まずTridentというプロジェクトを作成します。

次に、[開発者]ビューからHelmチャートリポジトリを作成します。URLフィールドの使用 `'https://netapp.github.io/trident-helm-chart'`。次に、Tridentオペレータ用のHelmリリースを作成します。


Project: trident
Create Helm Chart Repository
Add helm chart repository.
Configure via:
Form view
YAML view
Scope type
Namespaced scoped (ProjectHelmChartRepository)
Add Helm Chart Repository in the selected namespace.
Cluster scoped (HelmChartRepository)
Add Helm Chart Repository at the cluster level and in all namespaces.
Name *
trident
A unique name for the Helm Chart repository.
Display name
Astra Trident
A display name for the Helm Chart repository.
Description
NetApp Astra Trident
A description for the Helm Chart repository.
Disable usage of the repo in the developer catalog.
URL *
https://netapp.github.io/trident-helm-chart



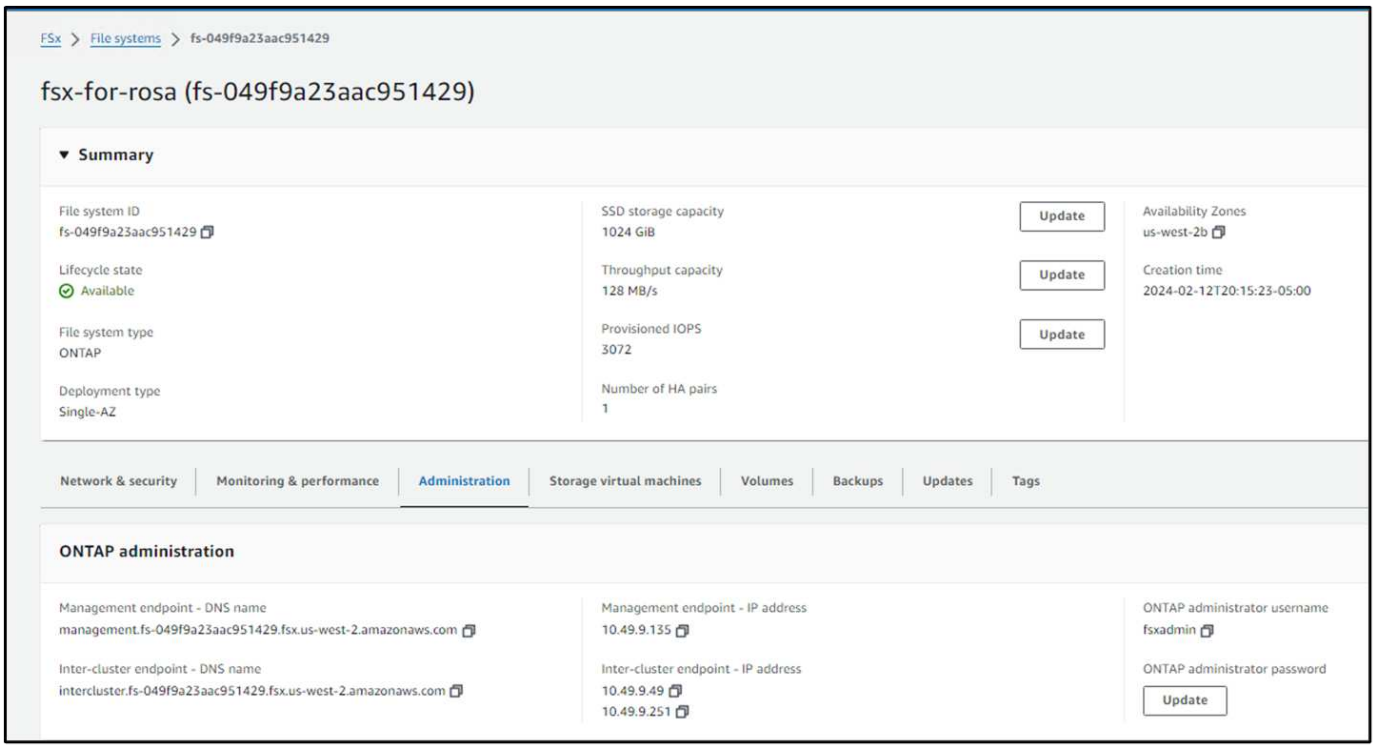
コンソールの管理者ビューに戻り、Tridentプロジェクトでポッドを選択して、すべてのTridentポッドが実行されていることを確認します。



4.Trident CSIプロビジョニングツールを使用して、バックエンド、ストレージクラス、スナップショットクラスの構成を作成

以下のYAMLファイルを使用して、Tridentバックエンドオブジェクト、ストレージクラスオブジェクト、およびVolumesnapshotオブジェクトを作成します。作成したAmazon FSx for NetApp ONTAPファイルシステム、管理LIF、およびファイルシステムのSVM名のクレデンシャルを、バックエンドの構成YAMLで指定してください。これらの詳細を確認するには、Amazon FSxのAWSコンソールに移動し、ファイルシステムを選択して、[管理]タブに移動します。また、[UPDATE]をクリックして、 `fsxadmin` ユーザ：

コマンドラインを使用して、ハイブリッドクラウドコンソールからオブジェクトを作成したり、YAMLファイルを使用してオブジェクトを作成したりできます。



- Tridentバックエンド構成**

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-nas-secret
type: Opaque
stringData:
  username: fsxadmin
  password: <password>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: <management lif>
  backendName: ontap-nas
  svm: fsx
  credentials:
    name: backend-tbc-ontap-nas-secret
```

ストレージクラス

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
allowVolumeExpansion: true
```

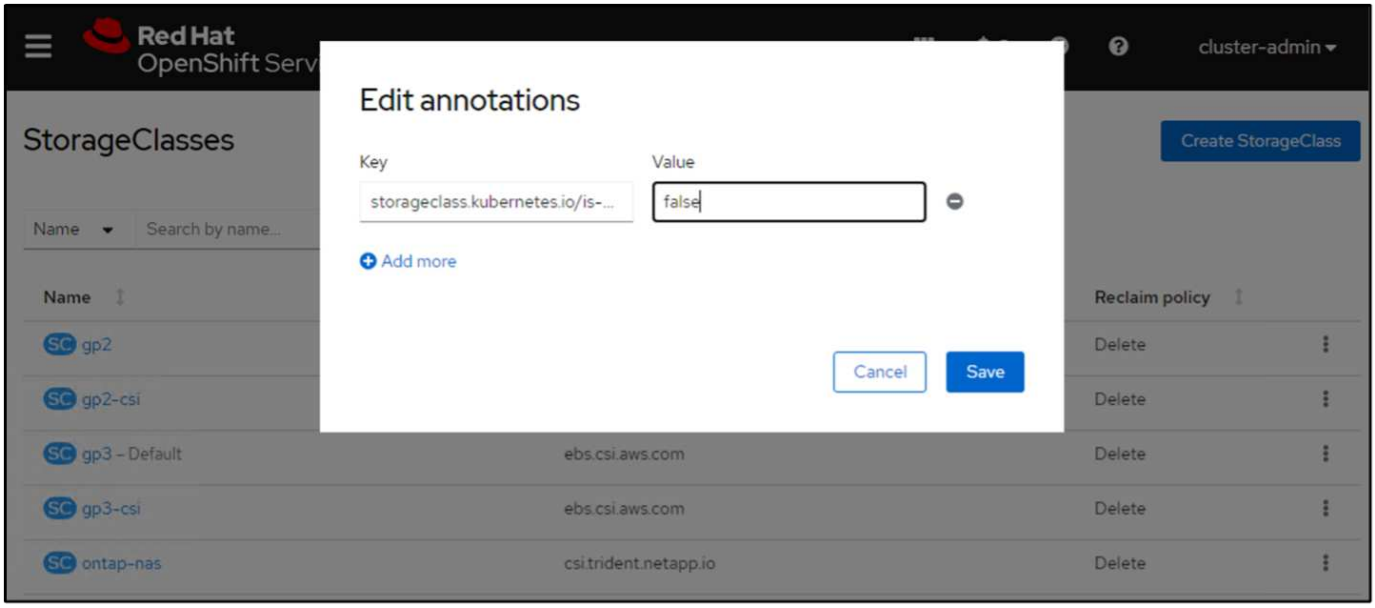
スナップショットクラス

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

以下のコマンドを実行して、バックエンド、ストレージクラス、およびtrident-snapshotclassオブジェクトが作成されたことを確認します。

```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get tbc -n trident
NAME        BACKEND NAME   BACKEND UUID                           PHASE   STATUS
ontap-nas   ontap-nas      8a5e4583-2dac-46bb-b01e-fa7c3816f121   Bound   Success
[ec2-user@ip-10-49-11-132 storage]$ kubectl get sc
NAME            PROVISIONER             RECLAIMPOLICY   VOLUMEBINDINGMODE      ALLOWVOLUMEEXPANSION   AGE
gp2             kubernetes.io/aws-ebs   Delete          WaitForFirstConsumer   true                   3h23m
gp2-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
gp3 (default)   ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h23m
gp3-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
ontap-nas       csi.trident.netapp.io   Delete          Immediate              true                   141m
[ec2-user@ip-10-49-11-132 storage]$ kubectl get Volumesnapshotclass
NAME                    DRIVER                  DELETIONPOLICY   AGE
csi-aws-vsc             ebs.csi.aws.com         Delete           3h19m
trident-snapshotclass   csi.trident.netapp.io   Delete           6m56s
[ec2-user@ip-10-49-11-132 storage]$
```

この時点で重要な変更点は、あとで導入するPostgreSQLアプリケーションでデフォルトのストレージクラスを使用できるように、ONTAP-NASをgp3ではなくデフォルトのストレージクラスに設定することです。クラスタのOpenShiftコンソールで、[Storage]で[StorageClasses]を選択します。現在のデフォルトクラスのアノテーションをfalseに編集し、ontap-nasストレージクラスに対してstorageclass.kubernetes.io/is-default-classをtrueに設定して追加します。



5.クラスタに**PostgreSQL**アプリケーションを導入する

次のように、コマンドラインからアプリケーションをデプロイできます。

```
helm install postgresql bitnami/postgresql -n postgresql --create-namespace
```

```
[ec2-user@ip-10-49-11-132 astra]$ helm install postgresql bitnami/postgresql -n postgresql --create-namespace
NAME: postgresql
LAST DEPLOYED: Tue Feb 13 14:46:16 2024
NAMESPACE: postgresql
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
CHART NAME: postgresql
CHART VERSION: 14.0.4
APP VERSION: 16.2.0

** Please be patient while the chart is being deployed **

PostgreSQL can be accessed via port 5432 on the following DNS names from within your cluster:

    postgresql.postgresql.svc.cluster.local - Read/Write connection

To get the password for "postgres" run:

    export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="{.data.postgres-password}" | base64 -d)

To connect to your database run the following command:

    kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PG
PASSWORD=$POSTGRES_PASSWORD" \
      --command -- psql --host postgresql -U postgres -d postgres -p 5432

    > NOTE: If you access the container using bash, make sure that you execute "/opt/bitnami/scripts/postgresql/entrypoint.sh /bin/bash" in order to avoid
the error "psql: local user with ID 1001} does not exist"

To connect to your database from outside the cluster execute the following commands:

    kubectl port-forward --namespace postgresql svc/postgresql 5432:5432 &
    PGPASSWORD="$POSTGRES_PASSWORD" psql --host 127.0.0.1 -U postgres -d postgres -p 5432

WARNING: The configured password will be ignored on new installation in case when previous PostgreSQL release was deleted through the helm command. In that
 case, old PVC will have an old password, and setting it through helm won't take effect. Deleting persistent volumes (PVs) will solve the issue.
[ec2-user@ip-10-49-11-132 astra]$
```

アプリケーションポッドが実行されていない場合は、セキュリティコンテキストの制約が原因でエラーが発生している可能性があります。

```
[ec2-user@ip-10-49-11-132 astra]$ kubectl get all -n postgresql
NAME                     TYPE        CLUSTER-IP     EXTERNAL-IP   PORT(S)    AGE
service/postgresql       ClusterIP   172.30.245.50  <none>        5432/TCP   12m
service/postgresql-hl    ClusterIP   None           <none>        5432/TCP   12m

NAME                          READY   AGE
statefulset.apps/postgresql   0/1     12m
[ec2-user@ip-10-49-11-132 astra]$ kubectl get events -n postgresql
LAST SEEN   TYPE      REASON                OBJECT                                  MESSAGE
2m39s       Normal    WaitForFirstConsumer  persistentvolumeclaim/data-postgresql-0  waiting for first consumer to be created before binding
12m         Normal    SuccessfulCreate      statefulset/postgresql                  create Claim data-postgresql-0 Pod postgresql-0 in StatefulSet postg
resql success
107s        Warning   FailedCreate          statefulset/postgresql                  create Pod postgresql-0 in StatefulSet postgresql failed error: pods
 "postgresql-0" is forbidden: unable to validate against any security context constraint: [provider "trident-controller": Forbidden: not usable by user or
serviceaccount, provider "anyuid": Forbidden: not usable by user or serviceaccount, provider restricted-v2: .spec.securityContext.fsGroup: Invalid value: [
]int64{1001}: 1001 is not an allowed group, provider restricted-v2: .containers[0].runAsUser: Invalid value: 1001: must be in the ranges: [1001010000, 1001
019999], provider "restricted": Forbidden: not usable by user or serviceaccount, provider "nonroot-v2": Forbidden: not usable by user or serviceaccount, pr
ovider "nonroot": Forbidden: not usable by user or serviceaccount, provider "pcap-dedicated-admins": Forbidden: not usable by user or serviceaccount, provi
der "hostmount-anyuid": Forbidden: not usable by user or serviceaccount, provider "machine-api-termination-handler": Forbidden: not usable by user or servi
ceaccount, provider "hostnetwork-v2": Forbidden: not usable by user or serviceaccount, provider "hostnetwork": Forbidden: not usable by user or serviceacco
unt, provider "hostaccess": Forbidden: not usable by user or serviceaccount, provider "splunkforwarder": Forbidden: not usable by user or serviceaccount, p
rovider "trident-node-linux": Forbidden: not usable by user or serviceaccount, provider "node-exporter": Forbidden: not usable by user or serviceaccount, p
rovider "privileged": Forbidden: not usable by user or serviceaccount]
[ec2-user@ip-10-49-11-132 astra]$
```

を編集してエラーを修正します。 `runAsUser` および `fsGroup` フィールド `statefuleset.apps/postgresql` の出力にあるuidを持つオブジェクト `oc get project` 次のようにコマンドを実行します。

```
[ec2-user@ip-10-49-11-132 astra]$ oc get project postgresql -o yaml | grep uid-range
    openshift.io/sa.scc.uid-range: 1001010000/10000
[ec2-user@ip-10-49-11-132 astra]$ oc edit -n postgresql statefulset.apps/postgresql
statefulset.apps/postgresql edited
[ec2-user@ip-10-49-11-132 astra]$
```

PostgreSQLアプリケーションを実行し、Amazon FSx for NetApp ONTAPストレージを基盤とする永続ボリュームを使用する必要があります。

```
[ec2-user@ip-10-49-11-132 astra]$ oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          2m46s
[ec2-user@ip-10-49-11-132 astra]$
```

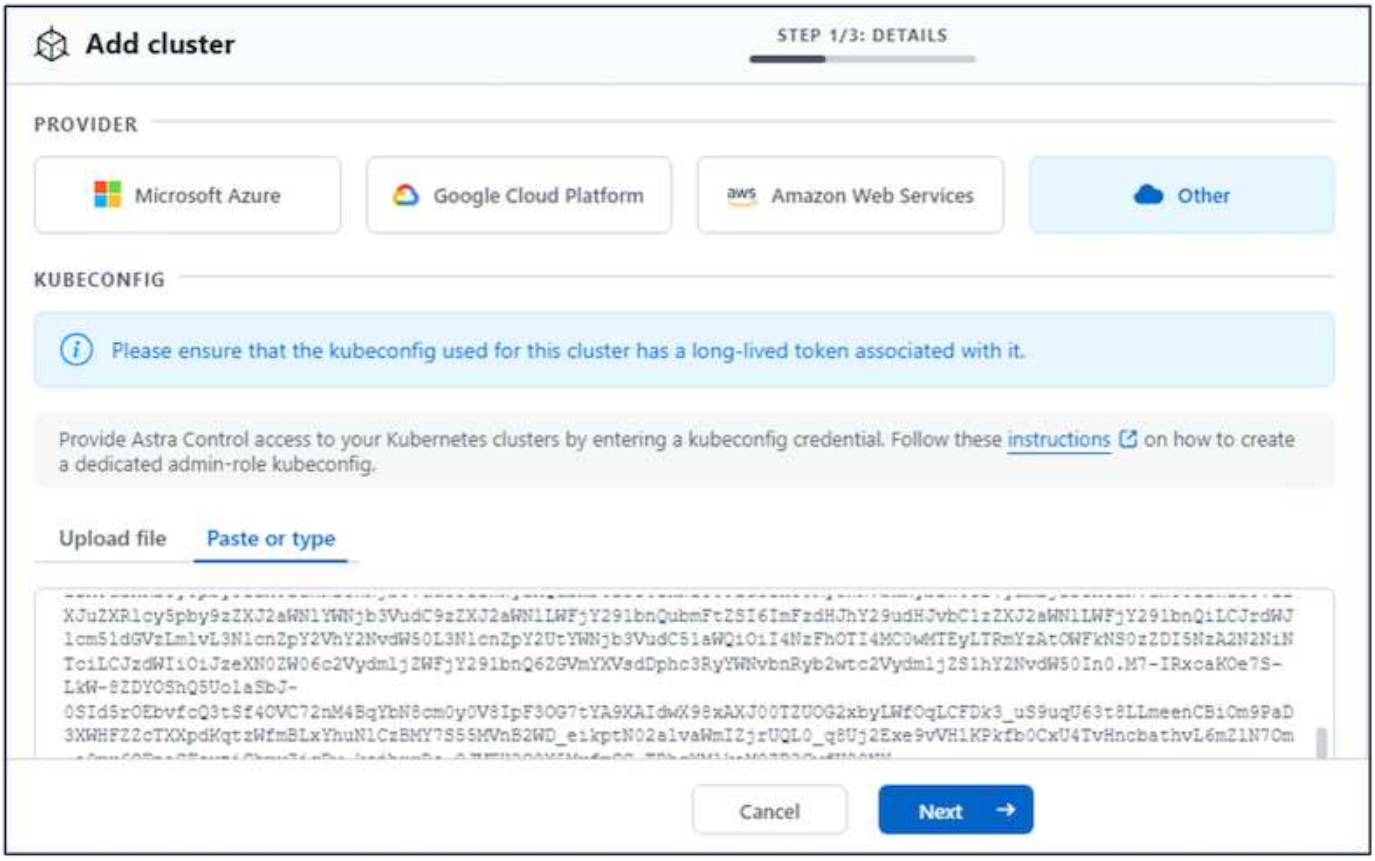
```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get pvc -n postgresql
NAME                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-dd09524a-de75-4825-9424-03a9b91195ca   8Gi        RWO            ontap-nas      4m2s
[ec2-user@ip-10-49-11-132 storage]$
```

6.データベースの作成とレコードの追加

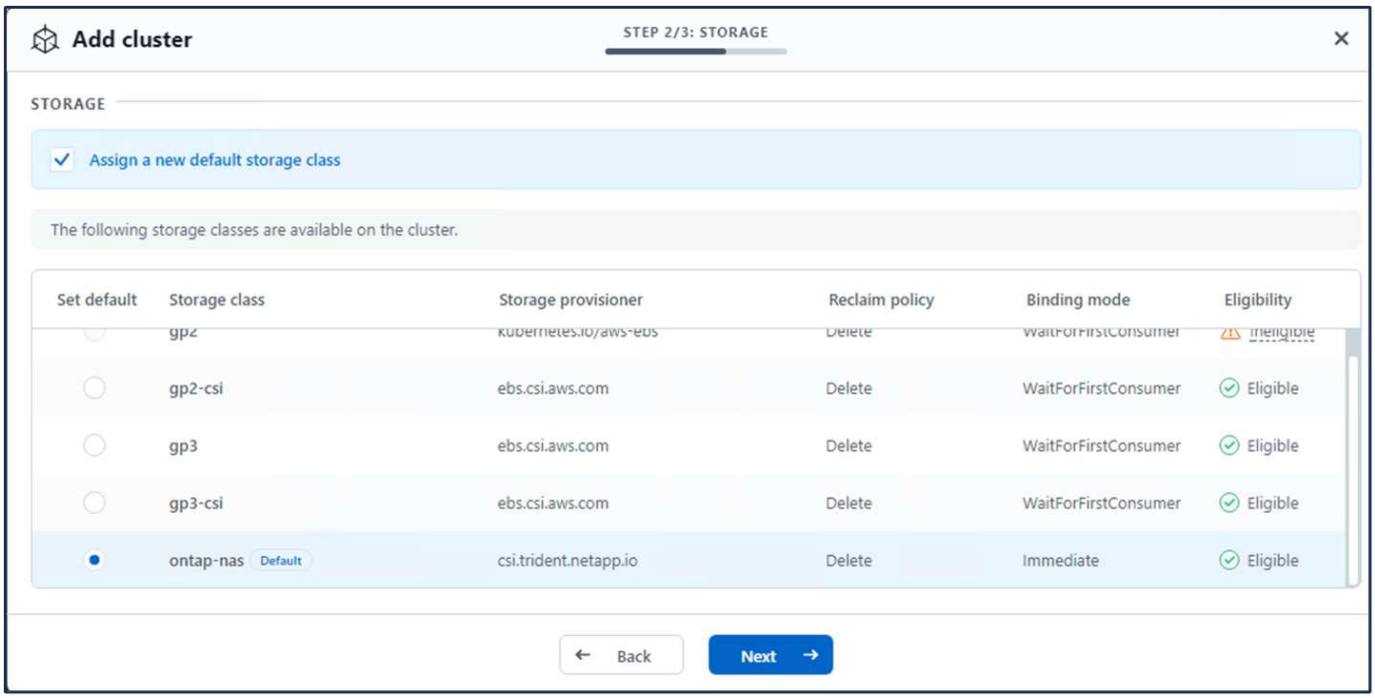
```
[ec2-user@ip-10-49-11-132 astra]$ export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="
{.data.postgres-password}" | base64 -d)
[ec2-user@ip-10-49-11-132 astra]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image
docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" \
> --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must se
t securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityCo
ntext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "postgresql-client" must set securityContext.runAsNonR
oot=true), seccompProfile (pod or container "postgresql-client" must set securityContext.seccompProfile.type to "RuntimeDefault
" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# CREATE DATABASE erp;
CREATE DATABASE
postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# CREATE TABLE PERSONS(ID INT PRIMARY KEY NOT NULL, FIRSTNAME TEXT NOT NULL, LASTNAME TEXT NOT NULL);
CREATE TABLE
erp=# INSERT INTO PERSONS VALUES(1,'John','Doe');
INSERT 0 1
erp=# \dt
         List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * FROM persons;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```

7.ACSへのクラスタの追加

ACSにログインします。クラスタを選択し、[Add]をクリックします。[Other]を選択し、kubeconfigファイルをアップロードまたは貼り付けます。



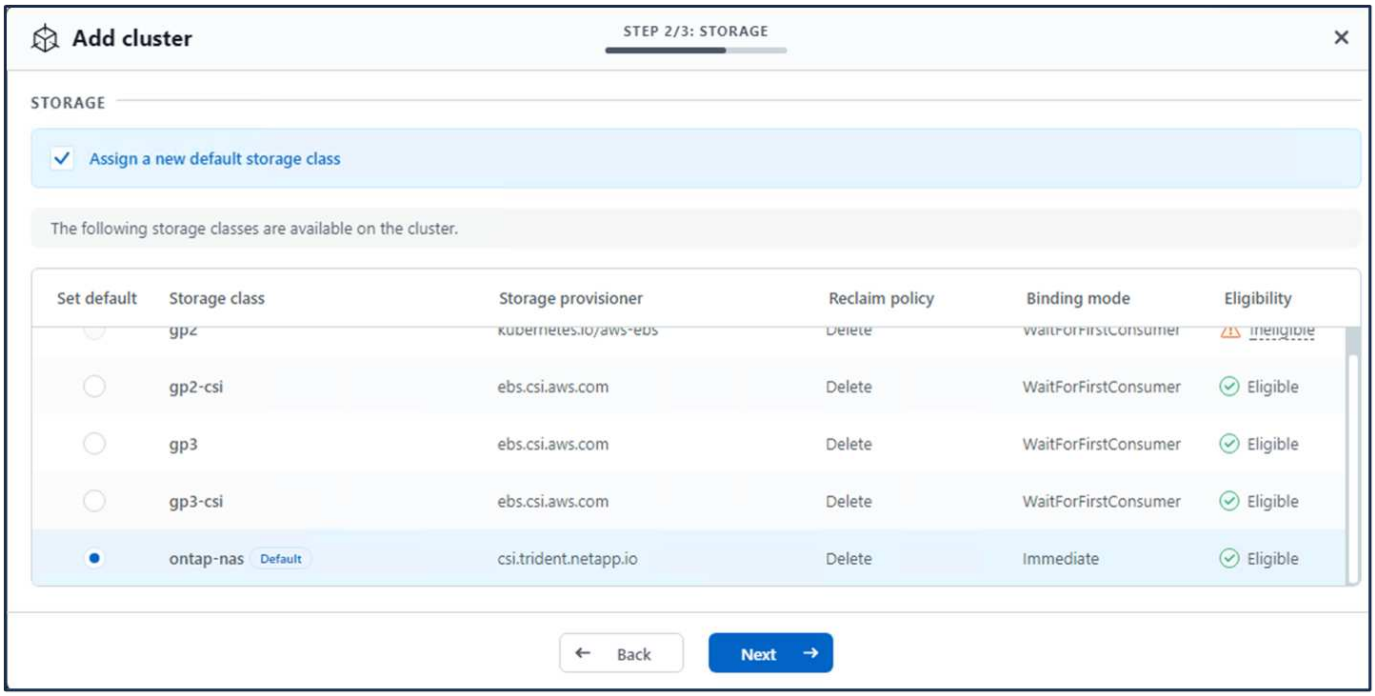
をクリックし、**ACS**のデフォルトのストレージクラスとして**[ONTAP-NAS]**を選択します。**[**次へ**]***をクリックし、詳細を確認して[クラスタを追加]*をクリックします。



8.ACSでのアプリケーションの定義

ACSでPostgreSQLアプリケーションを定義します。ランディングページで*、[定義]を選択し、適切な詳細を入力します。**[**次へ**]***を数回クリックし、詳細を確認して[定義]*をクリックします。アプリケーションがACSに

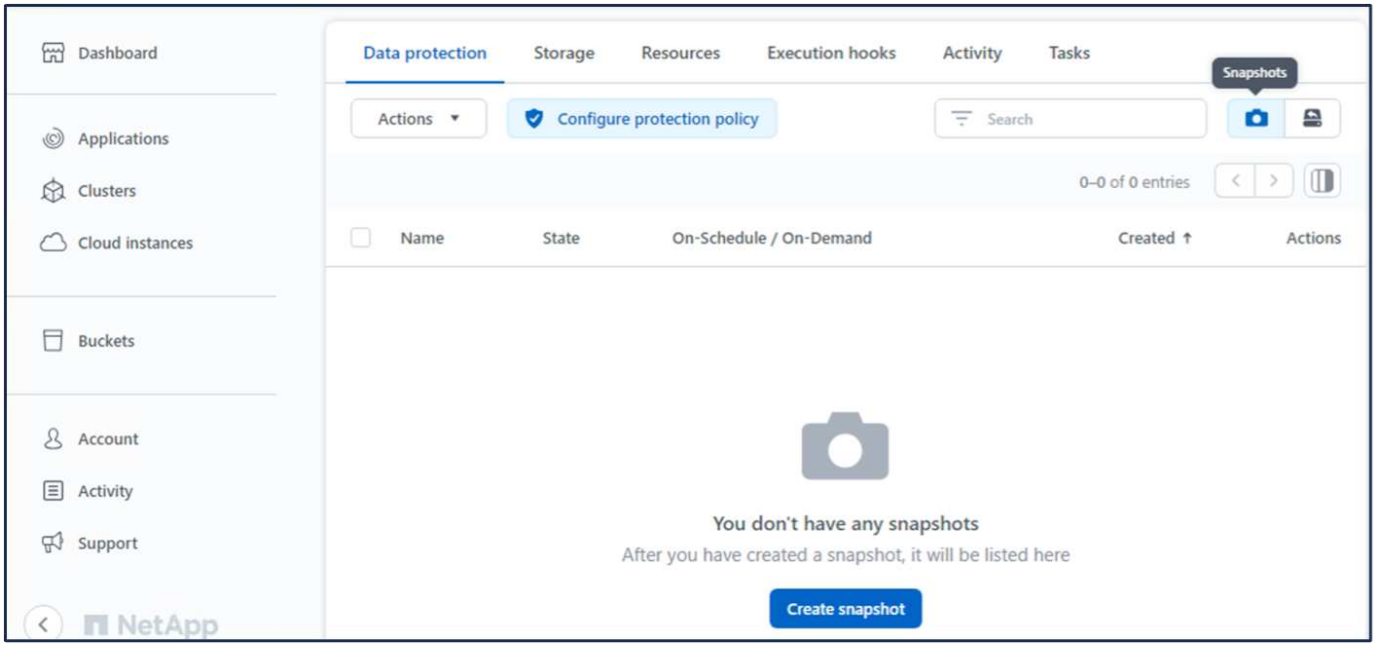
追加されます。

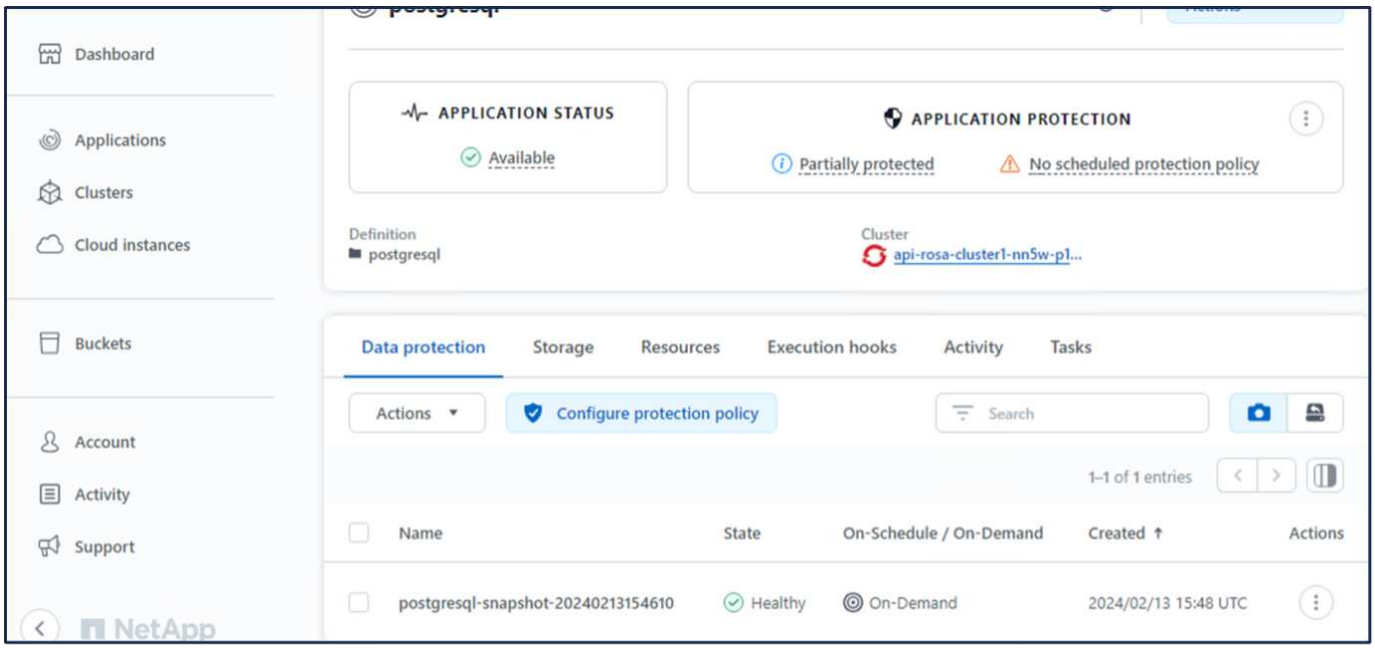


9.ACSを使用したスナップショットの作成

ACSでスナップショットを作成するには、さまざまな方法があります。アプリケーションを選択し、アプリケーションの詳細が表示されたページからスナップショットを作成できます。[Create snapshot]をクリックすると、オンデマンドSnapshotを作成したり、保護ポリシーを設定したりできます。

をクリックして名前を指定し、詳細を確認して[Snapshot]*をクリックするだけで、オンデマンドSnapshotを作成できます。処理が完了すると、Snapshotの状態が「Healthy」に変わります。





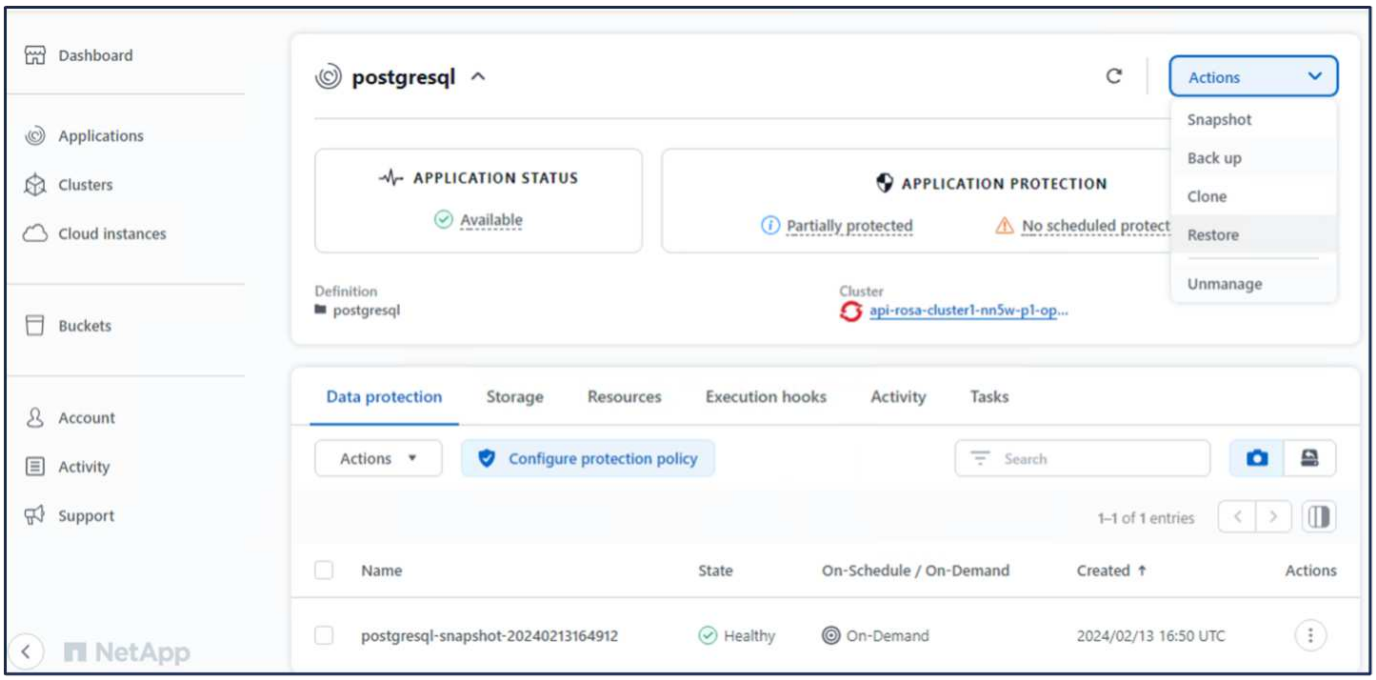
10。PostgreSQLアプリケーション内のデータベースの削除

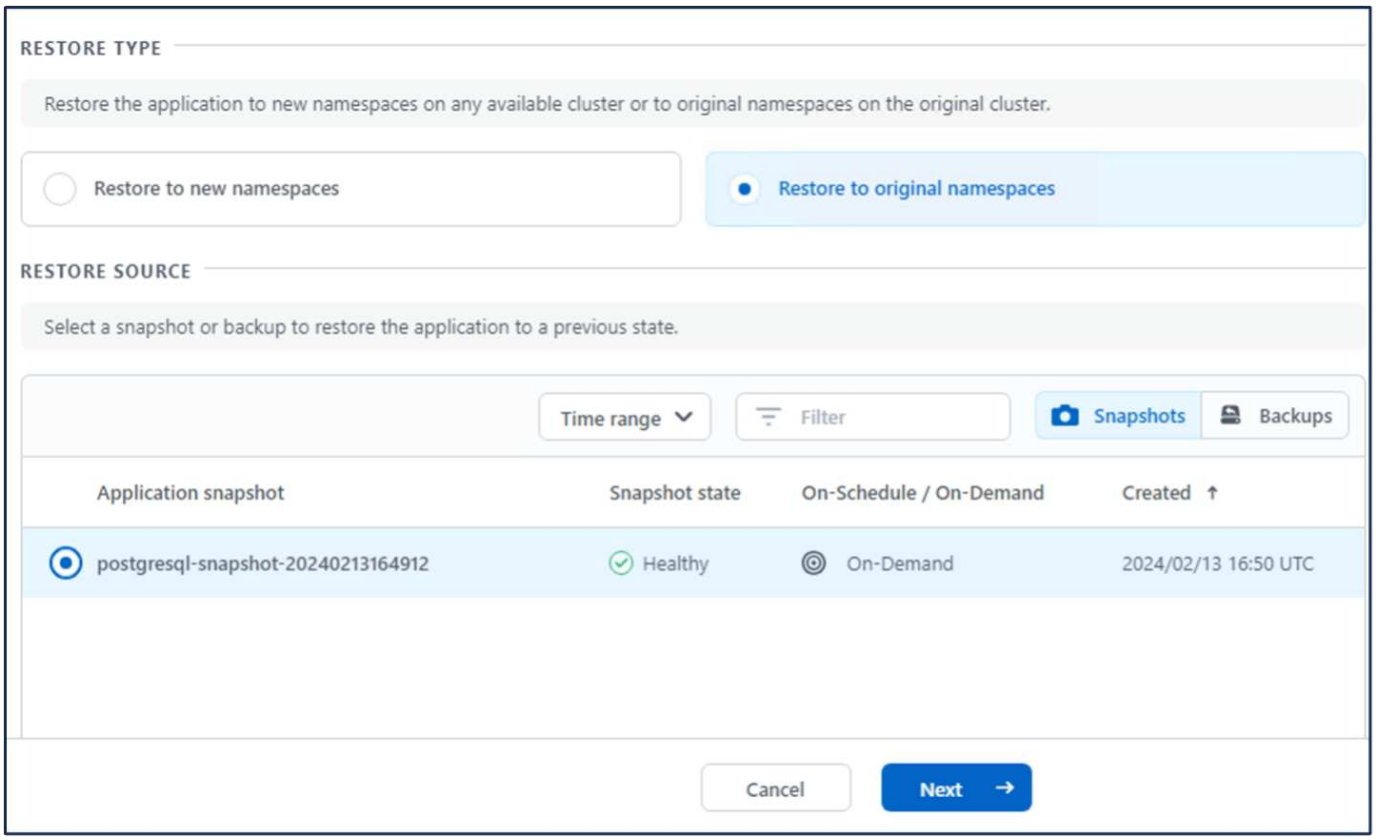
PostgreSQLに再度ログインし、利用可能なデータベースを一覧表示し、以前に作成したデータベースを削除して、データベースが削除されたことを確認します。

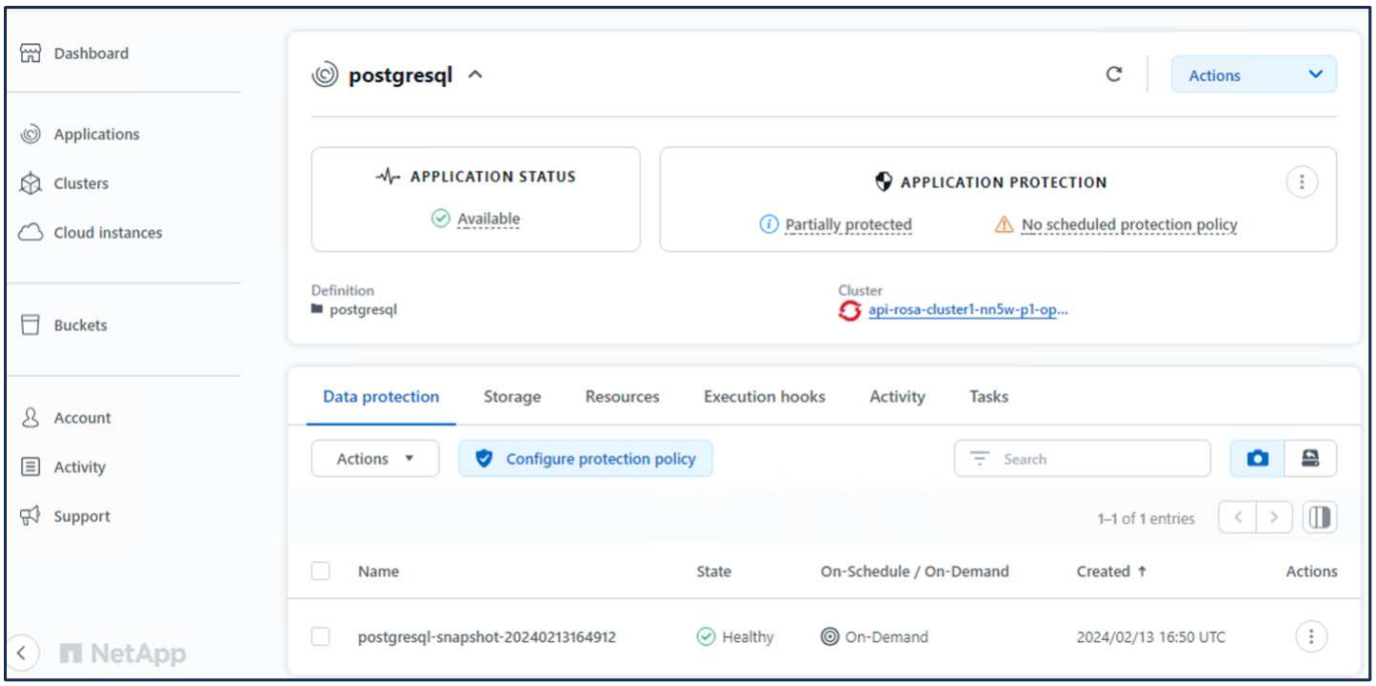
```
postgres=# \l
                                                List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-------------
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(4 rows)

postgres=# DROP DATABASE erp;
DROP DATABASE
postgres=# \l
                                                List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-------------
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(3 rows)
```

11.ACSを使用したスナップショットからのリストア

スナップショットからアプリケーションを復元するには、ACS UIランディングページに移動し、アプリケーションを選択して[Restore]を選択します。リストア元のスナップショットまたはバックアップを選択する必要があります。（通常は、設定したポリシーに基づいて複数のが作成されます）。次の2つの画面で適切な選択を行い、*[復元]*をクリックします。スナップショットからリストアされると、アプリケーションのステータスがRestoring（復元中）からAvailable（使用可能）に変わります。







12.アプリケーションがスナップショットから復元されたことを確認します

PostgreSQLクライアントにログインすると、以前に使用していたテーブルとレコードが表示されます。 これで終わりです。ボタンをクリックするだけで、アプリケーションは以前の状態に復元されます。Astra Controlを使用することで、お客様はそれを簡単に実現できます。

```
[ec2-user@ip-10-49-11-132 ~]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.
2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must set securityContext.allowPrivi
legeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (
pod or container "postgresql-client" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "postgresql-client" must set securityCon
text.seccompProfile.type to "RuntimeDefault" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# \l
                                                List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access privileges
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-----------------------
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
(4 rows)

postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# \dt
         List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * from PERSONS;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```


データ移行

このページでは、永続的ストレージにFSx for NetApp ONTAP を使用したマネージドRed Hat OpenShiftクラスタでのコンテナワークロードのデータ移行オプションを示します。

AWS上のRed Hat OpenShiftサービスと FSx for NetApp ONTAP （FSxN）は、AWSによるサービスポートフォリオに含まれています。FSxNは、単一のAZまたは複数のAZオプションで使用できます。複数のAZオプションを使用すると、アベイラビリティゾーンの障害からデータを保護できます。FSxNをAstra Tridentと統合することで、ROSAクラスタ上のアプリケーションに永続的ストレージを提供できます。

Helmチャートを使用した**FSxN**と**Trident**の統合

RosaクラスタとAmazon FSx for ONTAPの統合

コンテナアプリケーションの移行には、次の作業が含まれます。

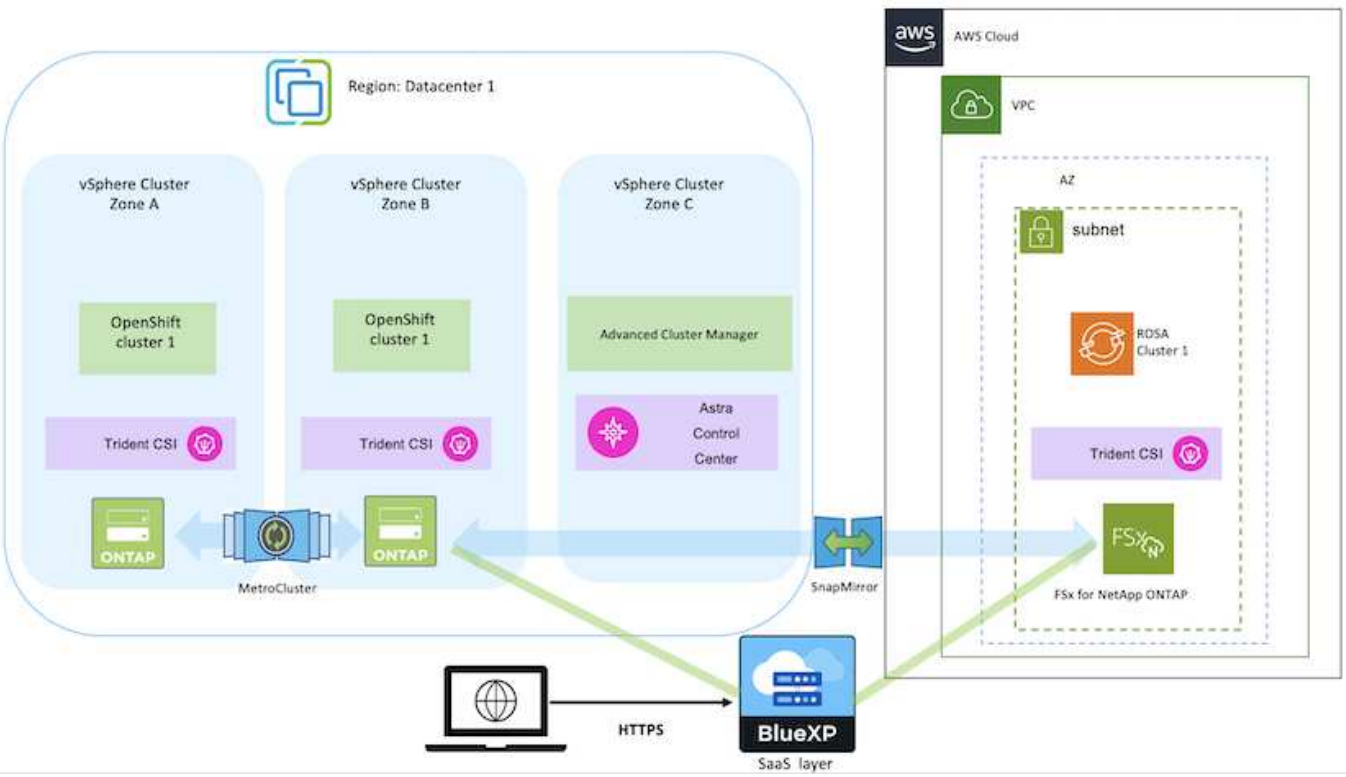
- 永続ボリューム：これはBlueXPを使用して実行できます。もう1つの方法は、Astra Control Centerを使用して、オンプレミスからクラウド環境へのコンテナアプリケーションの移行を処理する方法です。自動化も同じ目的で使用できます。
- アプリケーションメタデータ:これはOpenShift GitOps (Argo CD)を使用して実行できます。

永続的ストレージに**FSxN**を使用した**ROSA**クラスタ上のアプリケーションのフェイルオーバーとフェイルバック

次のビデオは、BlueXPとArgo CDを使用したアプリケーションのフェイルオーバーとフェイルバックのシナリオのデモです。

ROSAクラスタ上のアプリケーションのフェールオーバーとフェールバック

OpenShift Containerワークロード向けのデータ保護と移行用解決策



著作権に関する情報

商標に関する情報