NetAppパブリックおよびハイブリッドクラウド ソリューション

NetApp public and hybrid cloud solutions

NetApp
November 11, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/netapp-solutions-cloud/index.html on November 11, 2026. Always check docs.netapp.com for the latest.

目次

NetAppパブリックおよびハイブリッド クラウド ソリューション 1
NetAppのパブリッククラウドおよびハイブリッドクラウドソリューションの新機能 2
NetAppハイブリッド マルチクラウドと VMware ソリューション 3
パブリッククラウド向けVMware 3
VMware を使用したNetAppハイブリッド マルチクラウドの概要 3
ハイパースケーラー向け VMware 向けNetAppソリューション 7
NetAppハイブリッド マルチクラウドと VMware のサポート対象構成 10
ハイパースケーラー構成におけるVMware 10
パブリッククラウドにおけるNetAppストレージ 35
要約と結論: VMware とNetApp のハイブリッド マルチクラウドを組み合わせる理由 136
VMware ハイブリッド クラウドのユースケース 138
VMware を使用したNetAppハイブリッド マルチクラウドのユースケース 138
ハイパースケーラー向け VMware 向けNetAppソリューション 139
Amazon VMware Managed Cloud (VMC) 向けNetAppソリューション 140
Azure VMware Solution (AVS) 向けNetAppソリューション 140
Google Cloud VMware Engine (GCVE) 向けNetAppソリューション 141
AWS/VMC向けNetApp 141
AWS VMC 向けNetApp の機能 141
AWS/VMC 上のワークロードを保護する 143
AWS/VMC 上のワークロードを移行する 259
AWS / EVS 向けNetApp 274
FSx ONTAPをEVSの外部データストアとしてマウントする 274
EVS用FSx ONTAPデータストアの保護 298
Azure / AVS 向けNetApp 331
Azure AVS 向けNetApp の機能 332
Azure / AVS 上のワークロードを保護する 333
Azure/AVS 上のワークロードを移行する 402
GCP/GCVE 向けNetApp 417
Google Cloud Platform GCVE 向けNetApp の機能 417
GCP/GCVE 上のワークロードを保護する 418
GCP/GCVE 上のワークロードを移行する 450
Google Cloud のGoogle Cloud NetApp Volumesでデータを保護 467
NetApp Disaster Recovery 534
VMwareワークロードを保護するための、SnapCenterプラグインおよびNetApp Backup and Recoveryを使用したVMware向け3-2-1データ保護 534
NetApp Disaster Recovery 568
NetAppハイブリッド マルチクラウドと Red Hat OpenShift コンテナ ワークロード 610
始めましょう 610
Red Hat OpenShift Container ワークロード向けのNetAppハイブリッド マルチクラウド

ソリューション 610
Red Hat OpenShift Container ワークロード向けNetApp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 612
Red Hat OpenShift Container ワークロード向けNetApp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 613
ソリューション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 617
Red Hat OpenShift Containers とサポートされるNetAppストレージの統合 618
追加ドキュメント 622
オンプレミス向けOpenShift 622
VMware 上の Red Hat OpenShift Container プラットフォーム ワークロードを使用したNetAppソリューション 622
VMware 上で Red Hat OpenShift Container プラットフォームをデプロイおよび構成する 623
Trident Protectを使用したデータ保護 625
自己管理コンポーネントを備えたハイブリッドクラウド 626
ハイブリッドクラウドにおける Red Hat OpenShift Container プラットフォームのワークロードに対応したNetAppソリューション 626
AWS 上で Red Hat OpenShift Container プラットフォームをデプロイおよび構成する 628
Google Cloud に Red Hat OpenShift Container Platform をデプロイして構成する 630
Azure に Red Hat OpenShift Container プラットフォームをデプロイして構成する 632
Trident Protectを使用したデータ保護 636
プロバイダー管理コンポーネントを備えたハイブリッドクラウド 636
マネージド Red Hat OpenShift Container プラットフォーム ワークロードを備えたNetAppソリューション 636
AWS 上でマネージド Red Hat OpenShift Container プラットフォームをデプロイおよび構成する 636
Google Cloud NetApp Volumesを使用して Google Cloud に OpenShift Dedicated をデプロイおよび構成する 639
データ保護 641
Red Hat OpenShift ワークロード向けの追加のNetAppハイブリッド マルチクラウド ソリューション 642
Trident Protectを使用してデータを保護する 642
Trident Protectを使用したOpenShift Container Platformのコンテナアプリのデータ保護 642
Trident Protectを使用してRed Hat OpenShift VirtualizationのVMを保護 654
サードパーティのツールを使用してコンテナアプリを保護する 674
OpenShift API for Data Protection (OADP) を使用した OpenShift Container Platform のコンテナーアプリのデータ保護 674
OpenShift API for Data Protection (OADP) オペレーターのインストール 676
OpenShift Container Platform のアプリのオンデマンド バックアップの作成 685
あるクラスターから別のクラスターにアプリを移行する 688
バックアップからアプリを復元する 692
Velero を使用したバックアップと復元の削除 699
NetAppのハイブリッド マルチクラウド ソリューションに関するビデオとデモをご覧ください 701
NetAppを使用した Amazon Web Services 向けハイブリッド マルチクラウド

ソリューションに関するビデオを見る . . . 701
ゲスト接続ストレージ . . . 701
TCOと補足データストア . . . 701
移行ワークフロー (HCX) . . . 701
NetAppを使用した Azure VMware クラウド向けハイブリッド マルチクラウド
ソリューションに関するビデオを見る . . . 701
補足データストア . . . 701
ディザスタ リカバリ . . . 702
移行ワークフロー (HCX) . . . 702
NetAppを使用した Red Hat OpenShift 向けハイブリッド マルチクラウド
ソリューションに関するビデオを見る . . . 702
スナップショットと復元 . . . 702
ストレージ統合 . . . 702
フェイルオーバーとフェイルバック . . . 702
ソリューション自動化 . . . 702
NetApp の専門家によるクラウド ソリューションのブログを読む . . . 703
VMware と AWS およびAmazon FSx for ONTAP の統合 . . . 703
Azure VMware ソリューション . . . 703
Google Cloud VMware エンジン . . . 703
データ保護と管理 . . . 703
OpenShift コンテナ ワークロード向けNetApp . . . 703
VMware ソブリンクラウド . . . 703
法律上の表示 . . . 704
著作権 . . . 704
商標 . . . 704
特許 . . . 704
プライバシー ポリシー . . . 704

NetAppパブリックおよびハイブリッド クラウド ソリューション

NetAppのパブリッククラウドおよびハイブリッドクラウドソリューションの新機能

パブリック クラウド ソリューションとハイブリッド クラウド ソリューションの新機能について学習します。

[[18-august-2025]]
== 2025年8月18日

NetAppソリューションサイトは、"NetAppソリューションファミリー"これには次のサイトが含まれます。

- "NetAppの人工知能ソリューション"
- "NetAppコンテナソリューション"
- "NetAppデータ管理ソリューション"
- "NetAppデータベースソリューション"
- NetAppパブリックおよびハイブリッド クラウド ソリューション
- "SAP向けNetAppソリューション"
- "NetApp仮想化ソリューション"

NetAppハイブリッド マルチクラウドと VMware ソリューション

パブリッククラウド向けVMware

VMware を使用したNetAppハイブリッド マルチクラウドの概要

ほとんどの IT 組織はハイブリッド クラウド ファーストのアプローチを採用しています。これらの組織は変革段階にあり、顧客は現在の IT 環境を評価し、評価と検出の取り組みに基づいてワークロードをクラウドに移行しています。

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

パブリッククラウドにおける VMware Cloud のオプション

このセクションでは、各クラウド プロバイダーが、それぞれのパブリック クラウド サービス内で VMware Software Defined Data Center (SDDC) および/または VMware Cloud Foundation (VCF) スタックをどのようにサポートするかについて説明します。

Azure VMware ソリューション

Azure VMware Solution は、Microsoft Azure パブリック クラウド内で VMware SDDC を完全に機能させることができるハイブリッド クラウド サービスです。 Azure VMware Solution は、Microsoft によって完全に管理およびサポートされ、Azure インフラストラクチャを活用して VMware によって検証されたファーストパーティ ソリューションです。つまり、Azure VMware Solution を導入すると、お客様は、コンピューティング仮想化用の VMware ESXi、ハイパーコンバージド ストレージ用の vSAN、ネットワークとセキュリティ用の NSX を利用できるようになると同時に、Microsoft Azure のグローバルなプレゼンス、クラス最高のデータ センター設備、ネイティブ Azure サービスとソリューションの豊富なエコシステムへの近接性を活用できるようになります。

VMware Cloud on AWS

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

Google Cloud VMware エンジン

Google Cloud VMware Engine は、Google Cloud の高性能でスケーラブルなインフラストラクチャと VMware Cloud Foundation スタック（VMware vSphere、vCenter、vSAN、NSX-T）を基盤とする IaaS（Infrastructure as a Service）サービスです。このサービスは、アプリケーションの再設計や運用の再構築に伴うコスト、労力、リスクを負うことなく、既存の VMware ワークロードをオンプレミス環境から Google Cloud Platform にシームレスに移行または拡張することで、クラウドへの迅速な移行を実現します。これは、VMware と緊密に連携して Google が販売およびサポートするサービスです。

SDDC プライベート クラウドとNetApp Cloud Volumes のコロケーションにより、最小限のネットワーク遅延で最高のパフォーマンスが実現します。

知っていましたか？

使用するクラウドに関係なく、VMware SDDC が展開されると、初期クラスタには次の製品が含まれます。

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

ストレージ構成

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

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

注：

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

Azure NetApp Files、 Amazon FSx ONTAP、 Cloud Volumes ONTAP (3 つの主要ハイパースケーラーすべてで利用可能)、および Google Cloud 向けのGoogle Cloud NetApp Volumes は、ゲスト VM と組み合わせて使用できます。このハイブリッド ストレージ アーキテクチャは、ゲスト オペレーティング システムとアプリケーション バイナリ データを保持する vSAN データストアで構成されます。アプリケーション データは、ゲストベースの iSCSI イニシエーターまたは、それぞれAmazon FSx ONTAP、Cloud Volume ONTAP、 Azure NetApp Files 、 Google Cloud NetApp Volumes (Google Cloud 用) と直接通信する NFS/SMB マウントを介して VM に接続されます。この構成により、vSAN の場合と同様に、使用可能な空き領域は使用されるスラック領域とストレージ ポリシーによって決まるため、ストレージ容量に関する課題を簡単に克服できます。

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

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

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

  例えば：

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

したがって、 NetApp Cloud Volumes をゲスト接続ストレージとして使用すると、パフォーマンスとデータ保護の要件を満たしながら、ストレージを拡張し、TCO を最適化するのに役立ちます。

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

覚えておくべきポイント

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

> これはゲスト接続ストレージにのみ適用されます。

NetAppクラウドストレージのメリット

NetAppクラウド ストレージには、次のような利点があります。

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

できます。

- Cloud Volumes ONTAPのストレージ効率、クラウド階層化、インスタンス タイプ変更機能により、ストレージを最適な方法で追加および拡張できます。
- 過剰なプロビジョニングを防ぎ、必要な場合にのみストレージ リソースが追加されます。
- 効率的なスナップショット コピーとクローンにより、パフォーマンスに影響を与えることなく、迅速にコピーを作成できます。
- スナップショット コピーからの迅速なリカバリを使用して、ランサムウェア攻撃に対処します。
- 効率的な増分ブロック転送ベースの地域災害復旧を提供し、地域全体のブロック レベルの統合バックアップにより、より優れた RPO と RTO を実現します。

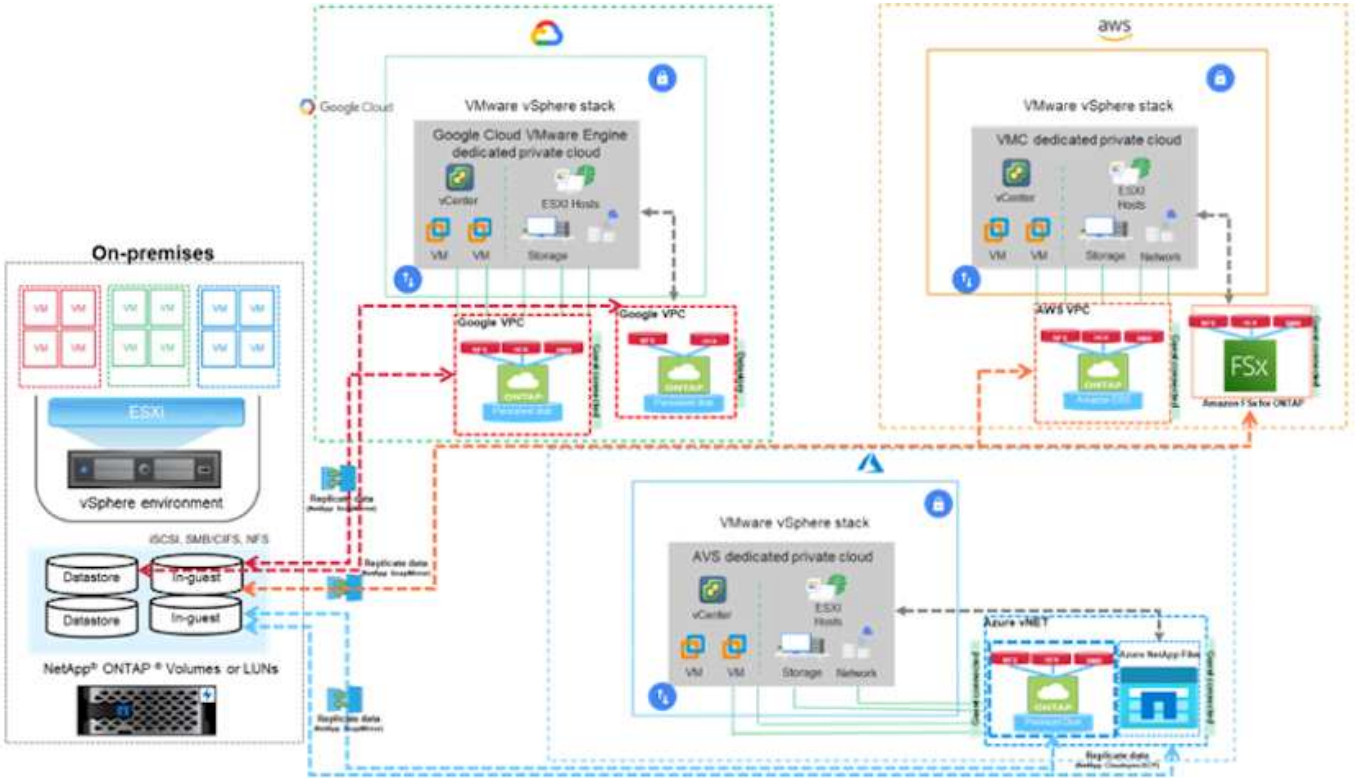
前提

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

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

詳細なアーキテクチャ

大まかに言えば、このアーキテクチャ (下の図を参照) は、 NetApp Cloud Volumes ONTAP、 Google Cloud NetApp Volumes for Google Cloud、およびAzure NetApp Files を追加のゲスト内ストレージ オプションとして使用して、複数のクラウド プロバイダー間でハイブリッド マルチクラウド接続とアプリの移植性を実現する方法をカバーしています。



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

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

クラウドを選択すると、あとはNetAppにお任せください。



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

リックします。

次のオプションから選択して、目的のコンテンツのセクションに移動します。

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

ハイパースケーラー構成における **VMware**

オンプレミスの場合と同様に、VM の作成と移行のための本番環境を正常に構築するには、クラウド ベースの仮想化環境を計画することが重要です。

AWS / VMC

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

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

セットアッププロセスは次の手順に分けられます。

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

詳細を表示"VMCの設定手順"。

Azure / AVS

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

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

セットアッププロセスは次の手順に分けられます。

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

詳細を表示"AVSの設定手順"。

GCP / GCVE

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

ゲスト内ストレージは、Cloud Volumes ONTAPおよびGoogle Cloud NetApp Volumes

をGCVE に接続するためにサポートされている唯一の方法です。

セットアッププロセスは次の手順に分けられます。

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

詳細を表示"GCVEの設定手順"。

NetAppストレージ オプション

NetAppストレージは、3 つの主要なハイパースケーラーのそれぞれにおいて、ゲスト接続として、または補助的な NFS データストアとしてなど、さまざまな方法で利用できます。

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

AWS / VMC

AWS は、次の構成でNetAppストレージをサポートしています。

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

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

Azure / AVS

Azure は、次の構成のNetAppストレージをサポートしています。

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

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

GCP / GCVE

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

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

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

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

NetApp / VMware クラウド ソリューション

NetAppと VMware のクラウド ソリューションを使用すると、多くのユース ケースを任意のハイパースケーラーに簡単に導入できます。 VMware は、主要なクラウド ワークロードのユースケースを次のように定義しています。

- 保護（災害復旧とバックアップ/復元の両方を含む）
- 移行
- 拡張

AWS / VMC

"AWS / VMC向けNetAppソリューションを参照"

Azure / AVS

"Azure / AVS向けNetAppソリューションを参照"

GCP / GCVE

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

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

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

	ゲスト接続	補足**NFS**データストア
AWS	CVO FSx ONTAP"詳細"	FSx ONTAP"詳細"
アズール	CVO ANF"詳細"	ANF"詳細"
GCP	CVO NetAppボリューム"詳細"	NetAppボリューム"詳細"

ハイパースケーラー構成における**VMware**

クラウドプロバイダーでの仮想化環境の構成

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

AWS / VMC

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

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

セットアッププロセスは次の手順に分けられます。

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

詳細を表示"VMCの設定手順"。

Azure / AVS

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

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

セットアッププロセスは次の手順に分けられます。

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

詳細を表示"AVSの設定手順"。

GCP / GCVE

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

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

セットアッププロセスは次の手順に分けられます。

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

詳細を表示"GCVEの設定手順"。

AWS 上で仮想化環境を展開および構成する

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

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

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

セットアッププロセスは次の手順に分けられます。

▼ **VMware Cloud for AWS** の導入と構成

"VMware Cloud on AWS"AWS エコシステム内の VMware ベースのワークロードにクラウド ネイティブ エクスペリエンスを提供します。各 VMware ソフトウェア定義データセンター (SDDC) は Amazon Virtual Private Cloud (VPC) で実行され、完全な VMware スタック (vCenter Server を含む)、NSX-T ソフトウェア定義ネットワーク、vSAN ソフトウェア定義ストレージ、およびワークロードにコンピューティング リソースとストレージ リソースを提供する 1 つ以上の ESXi ホストを提供します。

このセクションでは、VMware Cloud on AWS をセットアップおよび管理し、ゲスト内ストレージを備えたAmazon FSx ONTAPやCloud Volumes ONTAP on AWS と組み合わせて使用する方法について説明します。

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

セットアッププロセスは、次の 3 つの部分に分けられます。

▼ **AWS**アカウントを登録する

登録する"Amazon Web Servicesアカウント"。

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

▼ **My VMware** アカウントを登録する

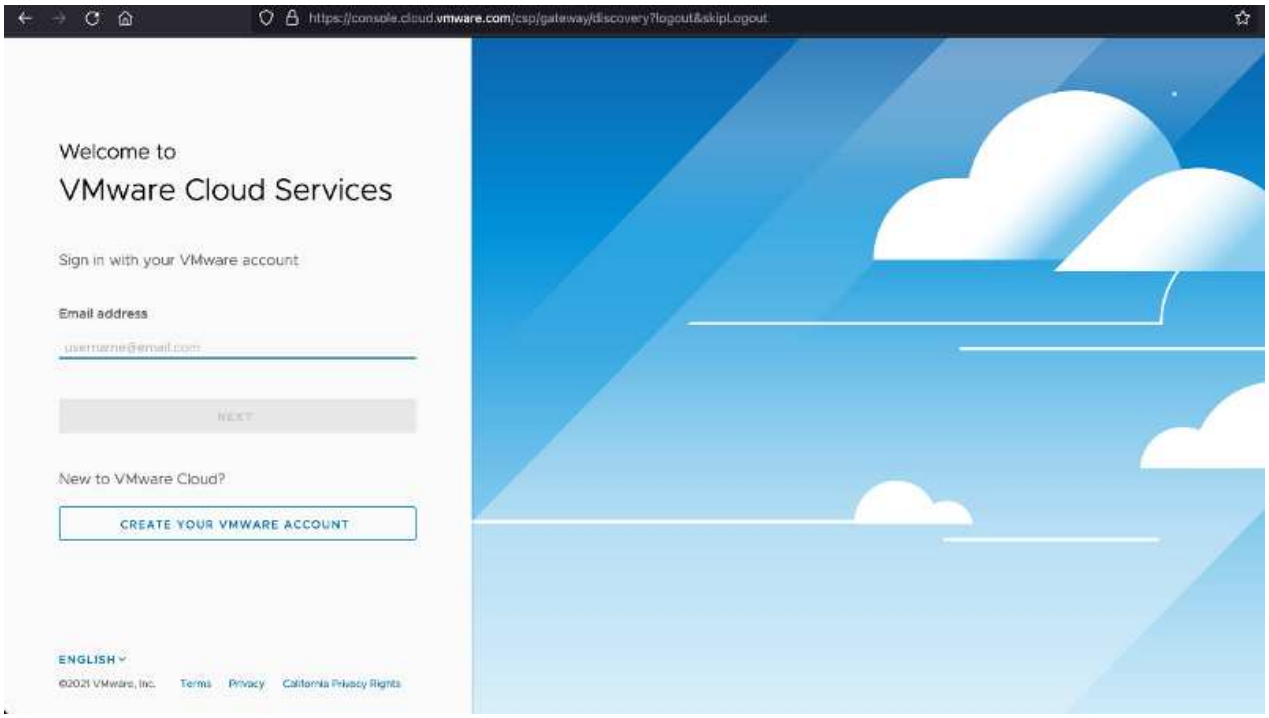
登録する"マイ VMware"アカウント。

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

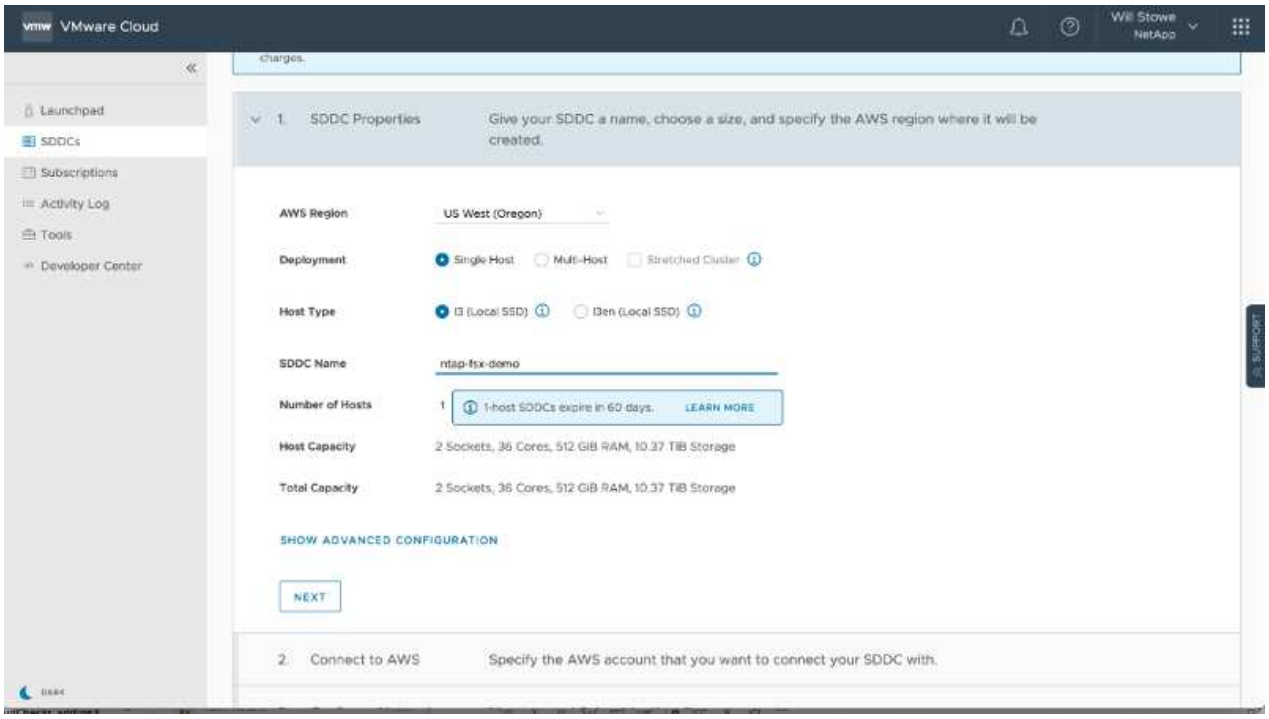
▼ **VMware Cloud** で **SDDC** をプロビジョニングする

VMware アカウントが構成され、適切なサイズ設定が実行されたら、VMware Cloud on AWS サービスを使用するための次のステップは、ソフトウェア定義データセンターの展開です。 SDDC を作成するには、ホストする AWS リージョンを選択し、SDDC に名前を付け、SDDC に含める ESXi ホストの数を指定します。 AWS アカウントをまだお持ちでない場合でも、単一の ESXi ホストを含むスターター構成の SDDC を作成できます。

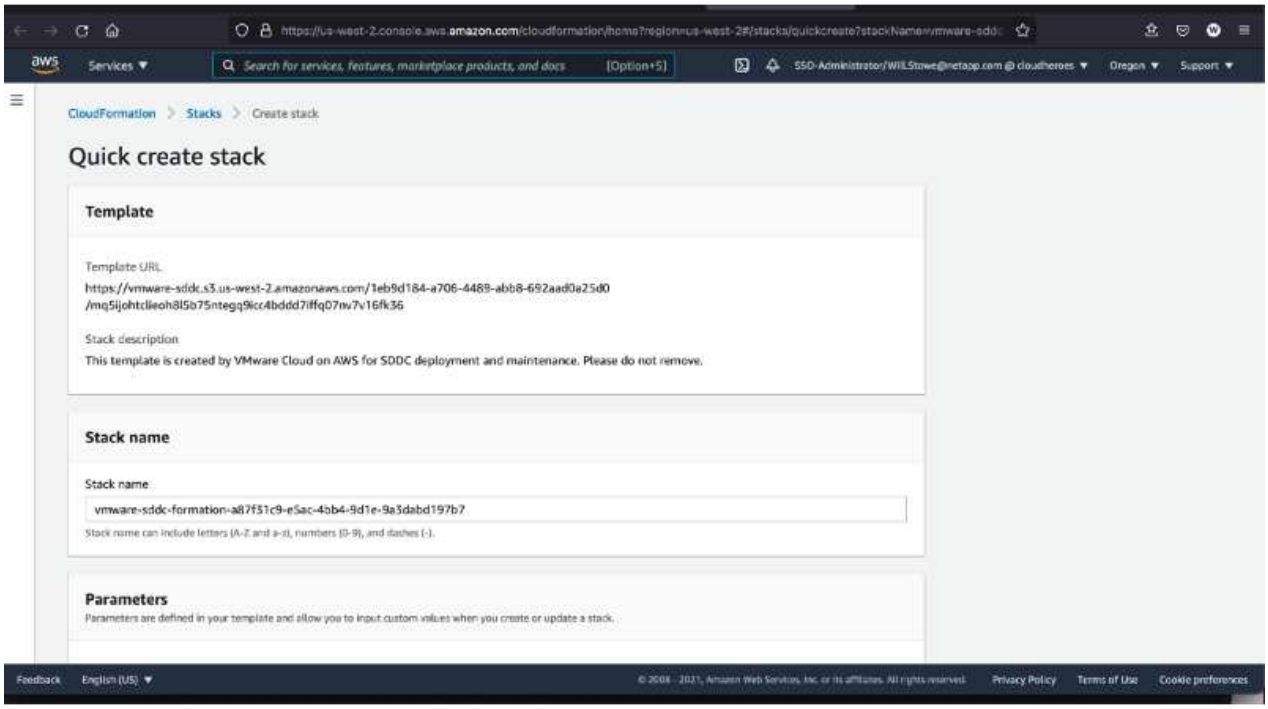
1. 既存または新しく作成した VMware 認証情報を使用して、VMware Cloud Console にログインします。

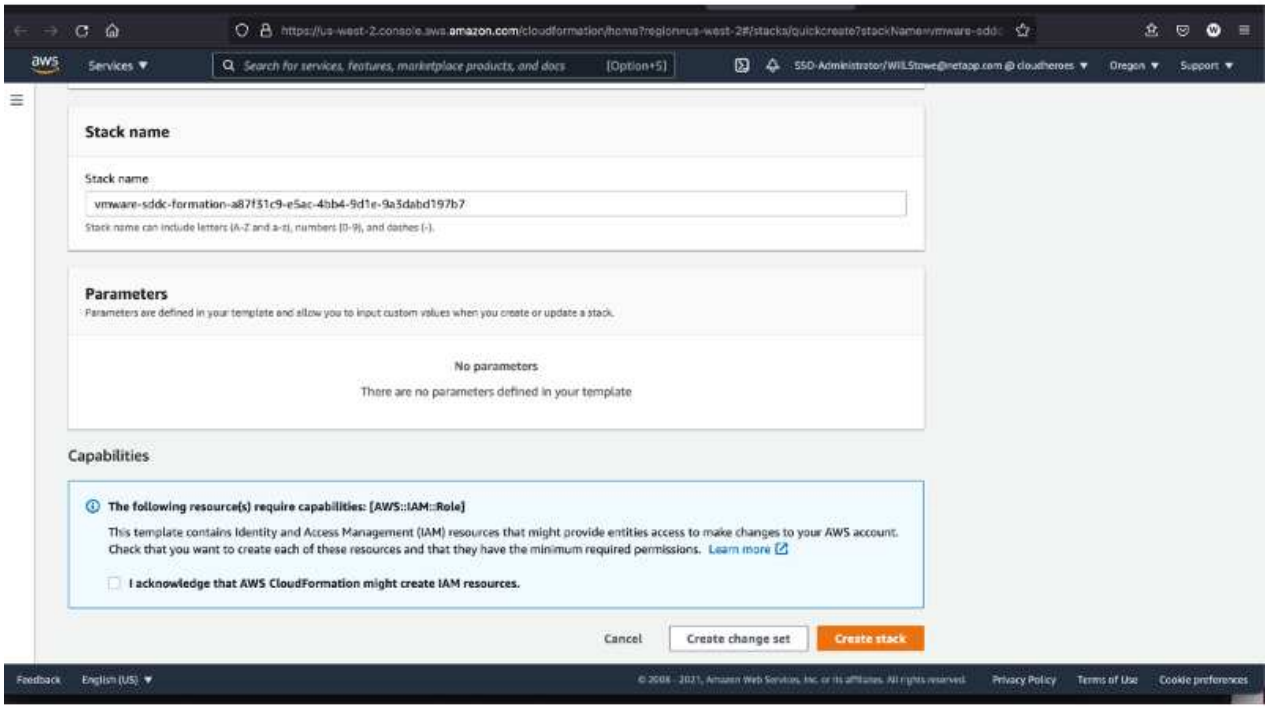


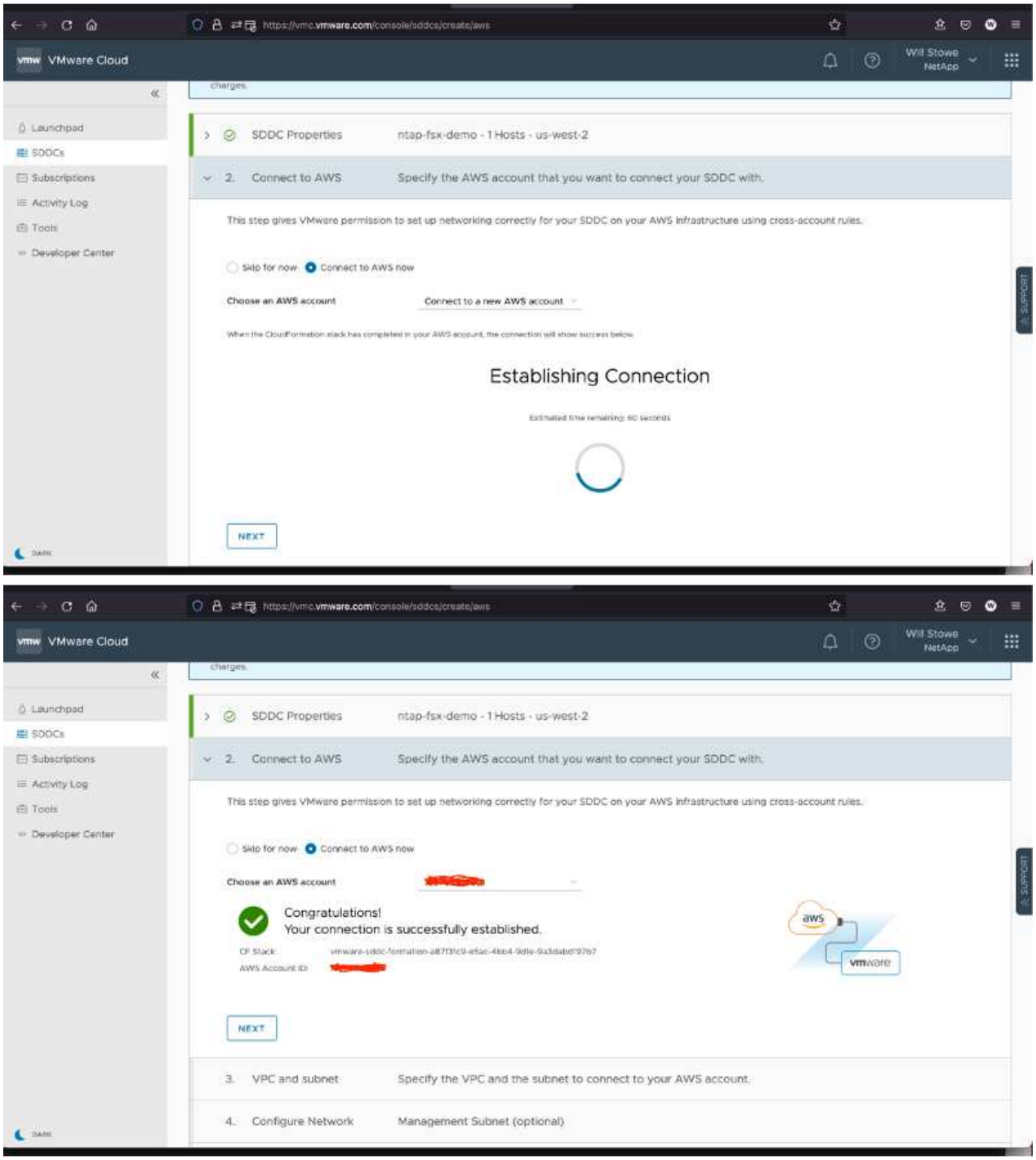
2. AWS リージョン、デプロイメント、ホスト タイプ、および SDDC 名を構成します。



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

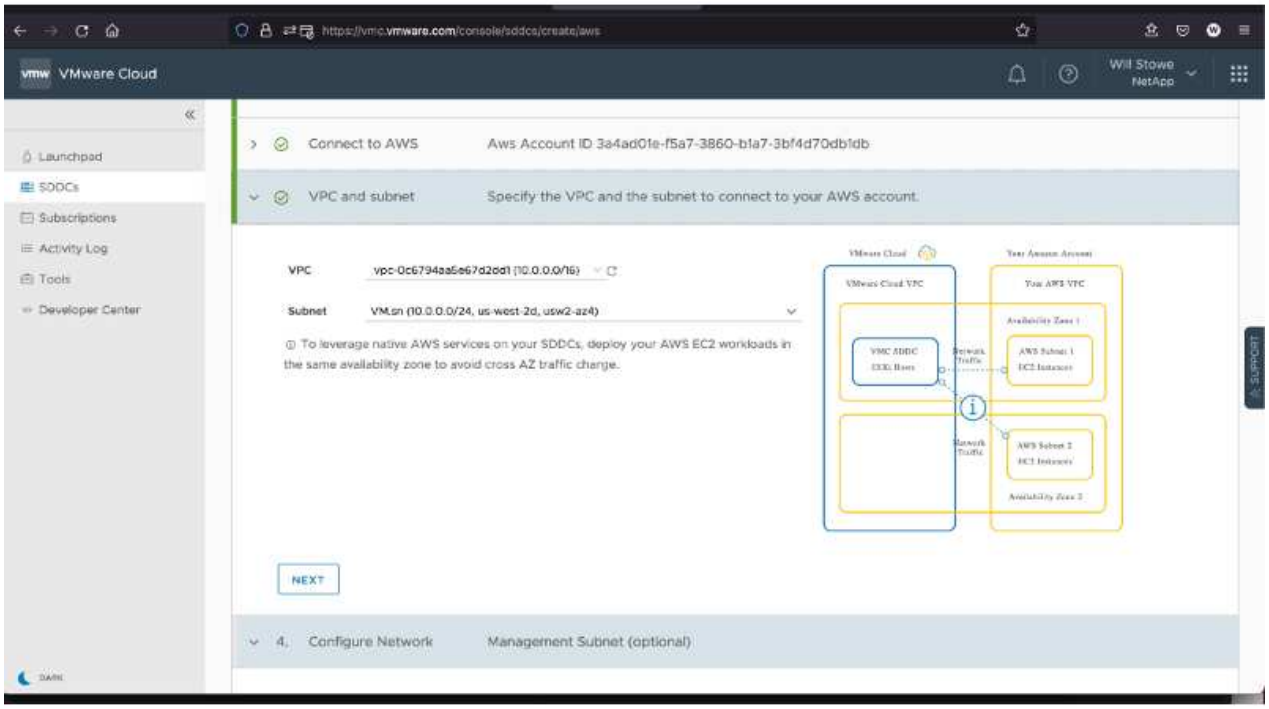

CloudFormation > Stacks > Create stack
Quick create stack
Template
Template URL
https://vmware-sddc.s3.us-west-2.amazonaws.com/1eb9d184-a706-4489-abb8-692aad0a25d0/mq5ljohtclieoh8l5b75ntegq9icc4bddd7iffq07nv7v16fk36
Stack description
This template is created by VMware Cloud on AWS for SDDC deployment and maintenance. Please do not remove.
Stack name
Stack name
vmware-sddc-formation-a87f31c9-e5ac-4bb4-9d1e-9a3dabd197b7
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.


Stack name
Stack name
vmware-sddc-formation-a87f31c9-e5ac-4bb4-9d1e-9a3dabd197b7
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
No parameters
There are no parameters defined in your template
Capabilities
The following resource(s) require capabilities: [AWS::IAM::Role]
This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. Learn more
I acknowledge that AWS CloudFormation might create IAM resources.
Cancel
Create change set
Create stack

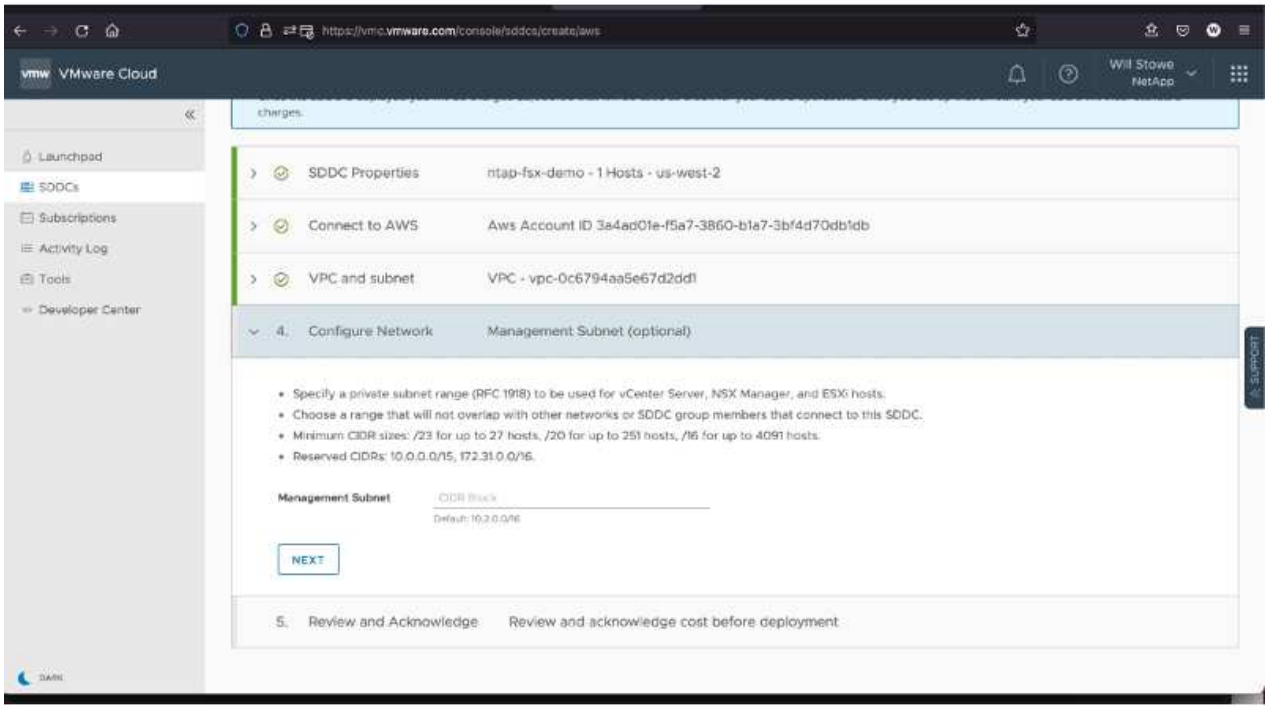


この検証では単一ホスト構成が使用されます。

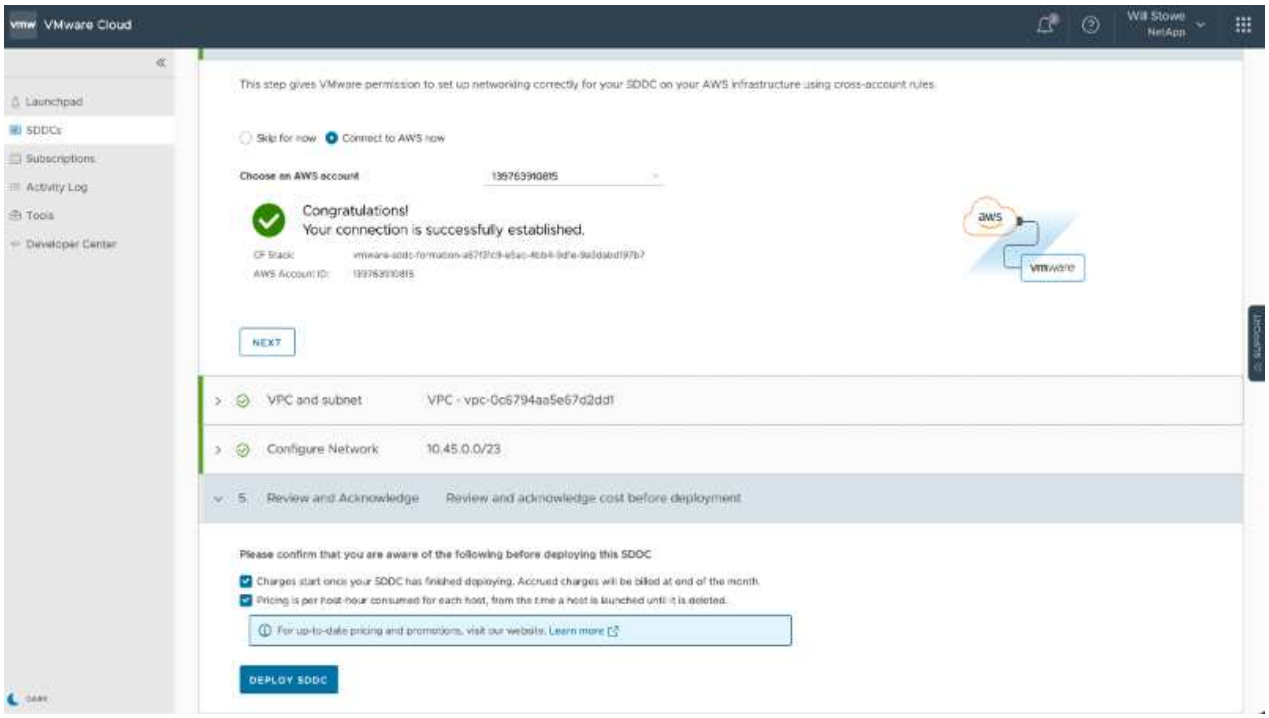
4. VMC 環境を接続する目的の AWS VPC を選択します。



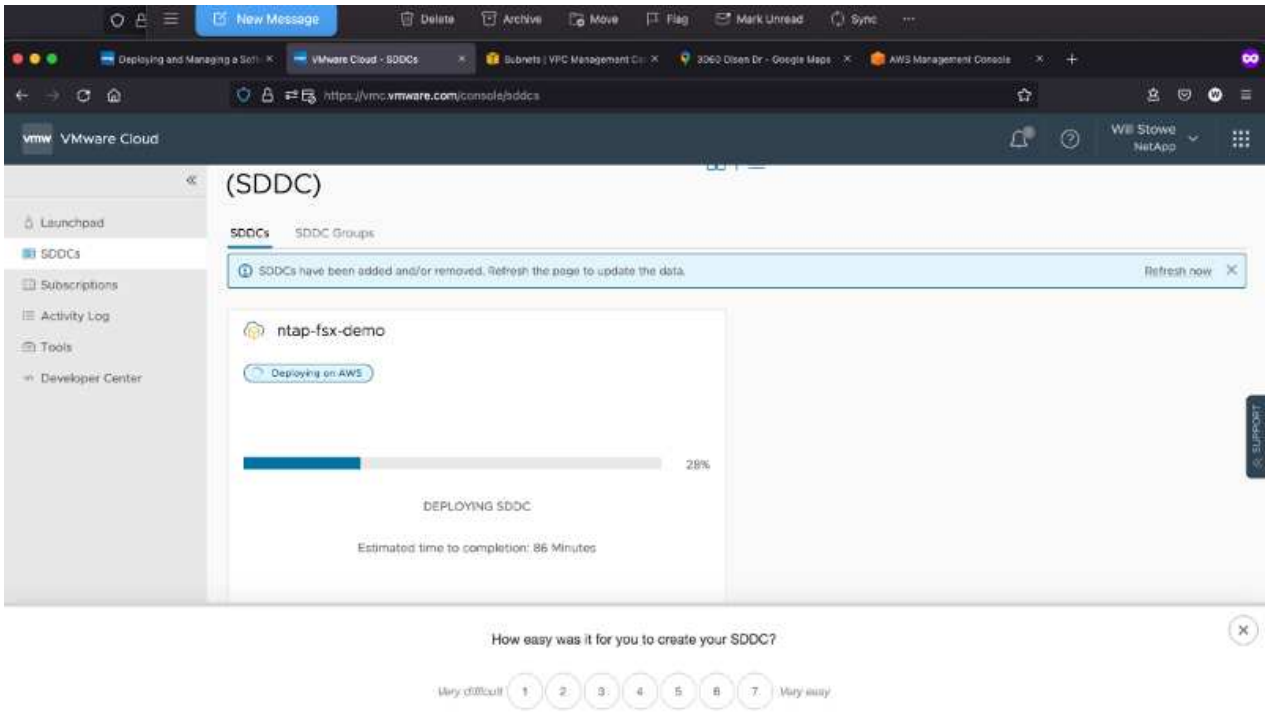
5. VMC 管理サブネットを構成します。このサブネットには、vCenter、NSX などの VMC 管理サービスが含まれます。 SDDC 環境への接続を必要とする他のネットワークと重複するアドレス空間を選択しないでください。最後に、以下に示す CIDR サイズの推奨事項に従ってください。



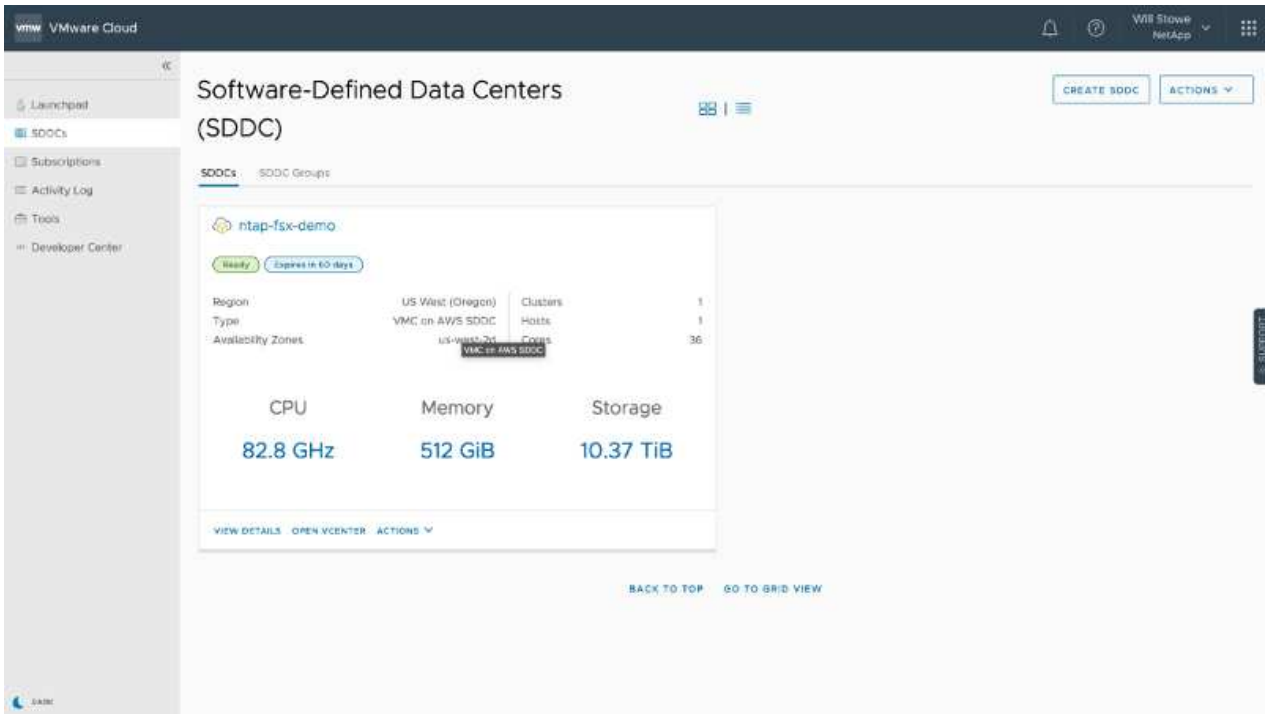
6. SDDC 構成を確認して承認し、「SDDC の展開」をクリックします。



展開プロセスが完了するまでには通常約 2 時間かかります。



7. 完了すると、SDDC が使用できるようになります。

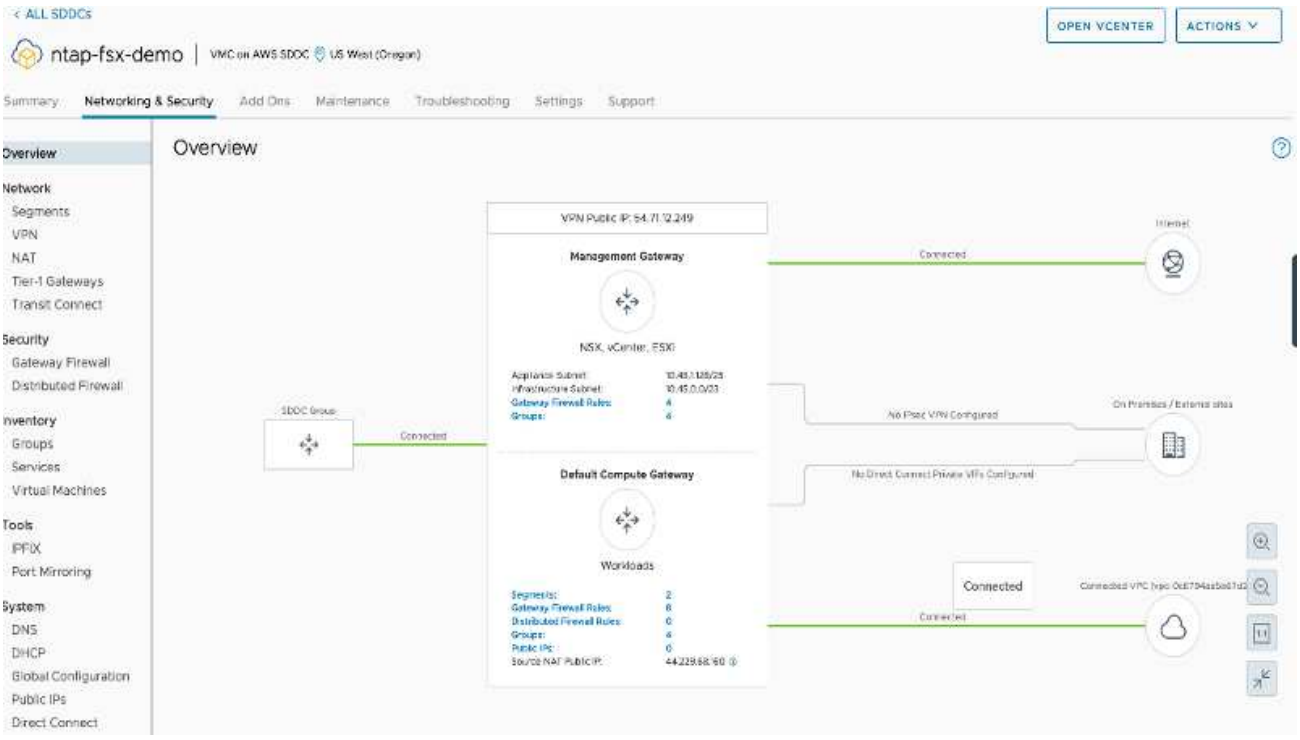


SDDC導入のステップバイステップガイドについては、"VMCコンソールからSDDCを展開する" 。

▼ **VMware Cloud** を **FSx ONTAP**に接続する

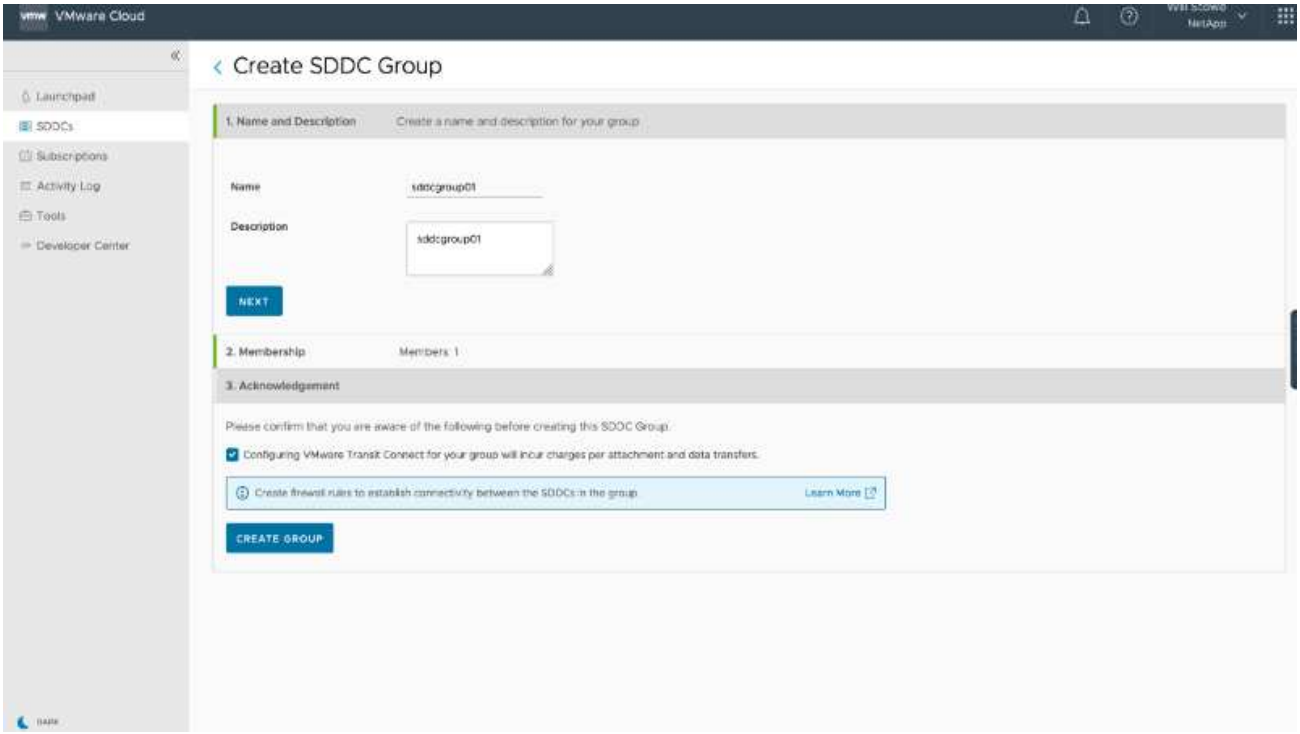
VMware Cloud を FSx ONTAPに接続するには、次の手順を実行します。

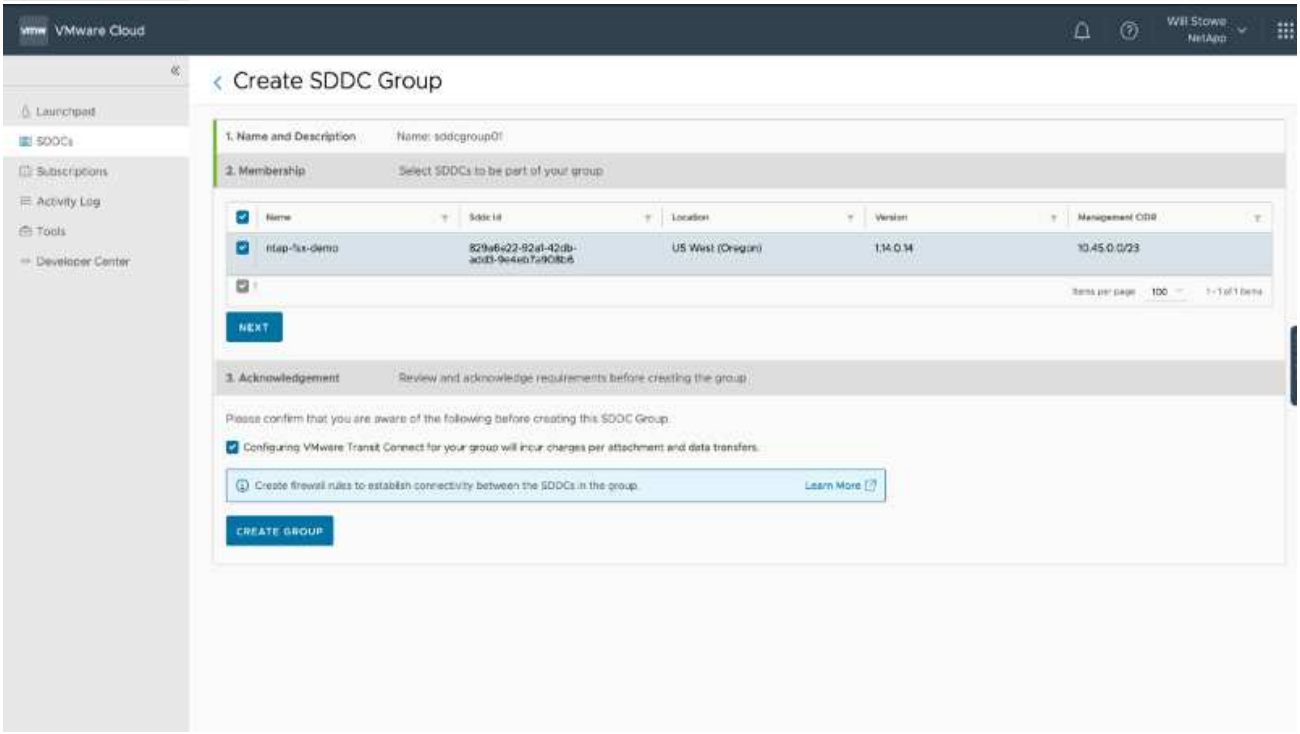
1. VMware Cloud のデプロイが完了し、AWS VPC に接続されたら、元の接続された VPC ではなく新しい VPC にAmazon FSx ONTAP をデプロイする必要があります (下のスクリーンショットを参照)。FSx (NFS および SMB フローティング IP) は、接続された VPC にデプロイされている場合はアクセスできません。 Cloud Volumes ONTAPなどの ISCSI エンドポイントは、接続された VPC からは問題なく機能することに注意してください。

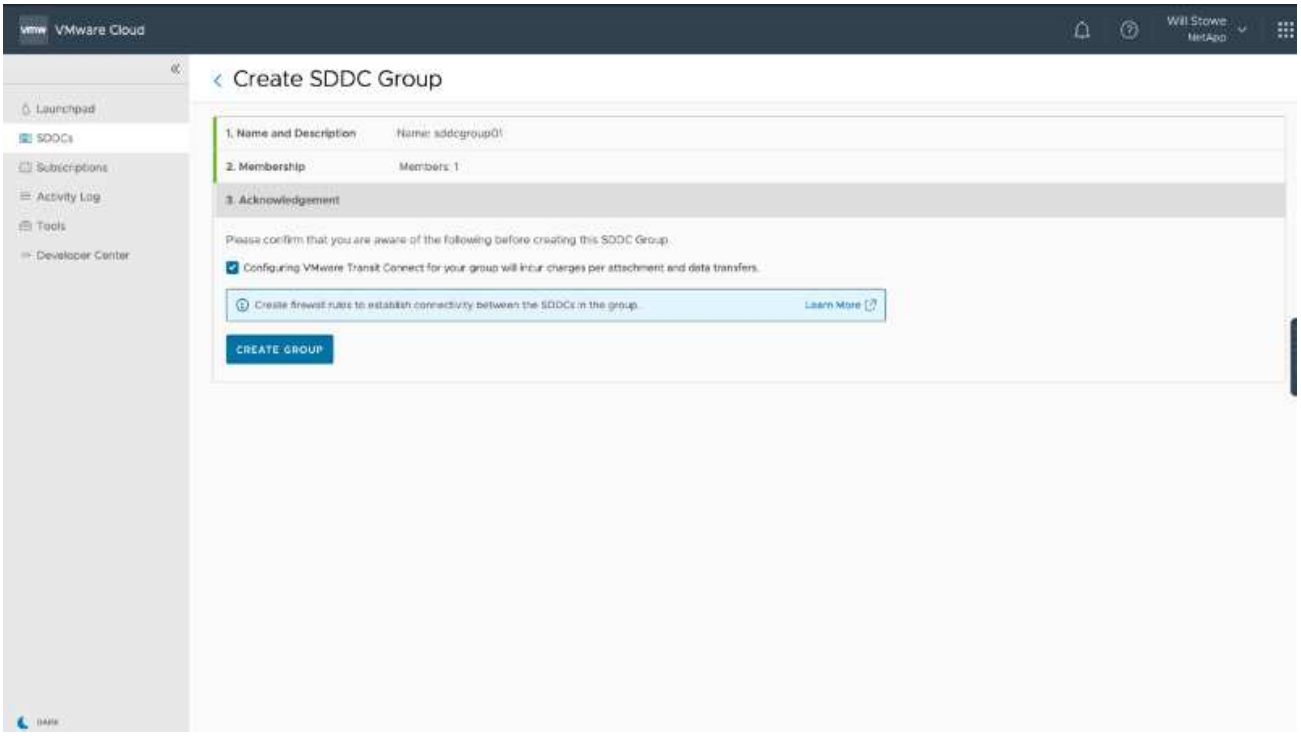


2. 同じリージョンに追加の VPC をデプロイし、新しい VPC にAmazon FSx ONTAP をデプロイします。

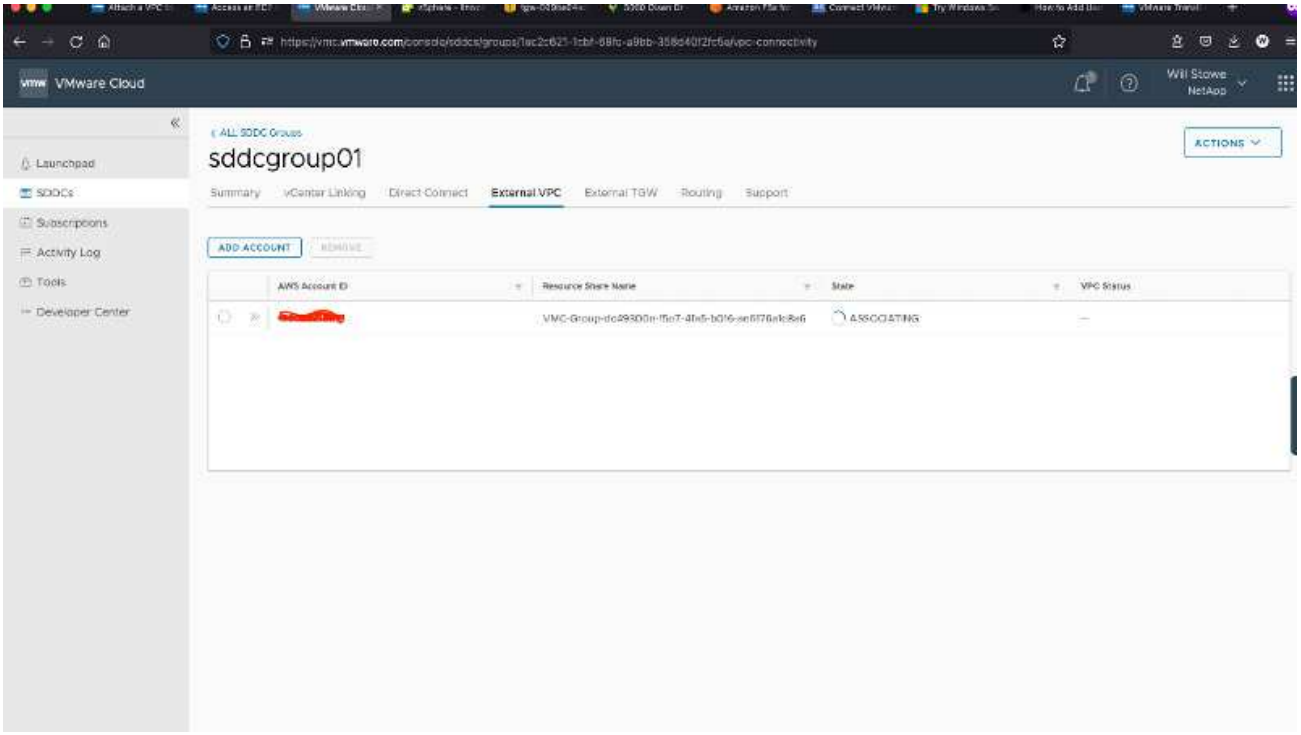
   VMware Cloud コンソールで SDDC グループを構成すると、FSx がデプロイされている新しい VPC に接続するために必要なネットワーク構成オプションが有効になります。手順 3 で、「グループに VMware Transit Connect を構成すると、添付ファイルとデータ転送ごとに料金が発生します」がチェックされていることを確認し、[グループの作成] を選択します。このプロセスは完了するまでに数分かかる場合があります。

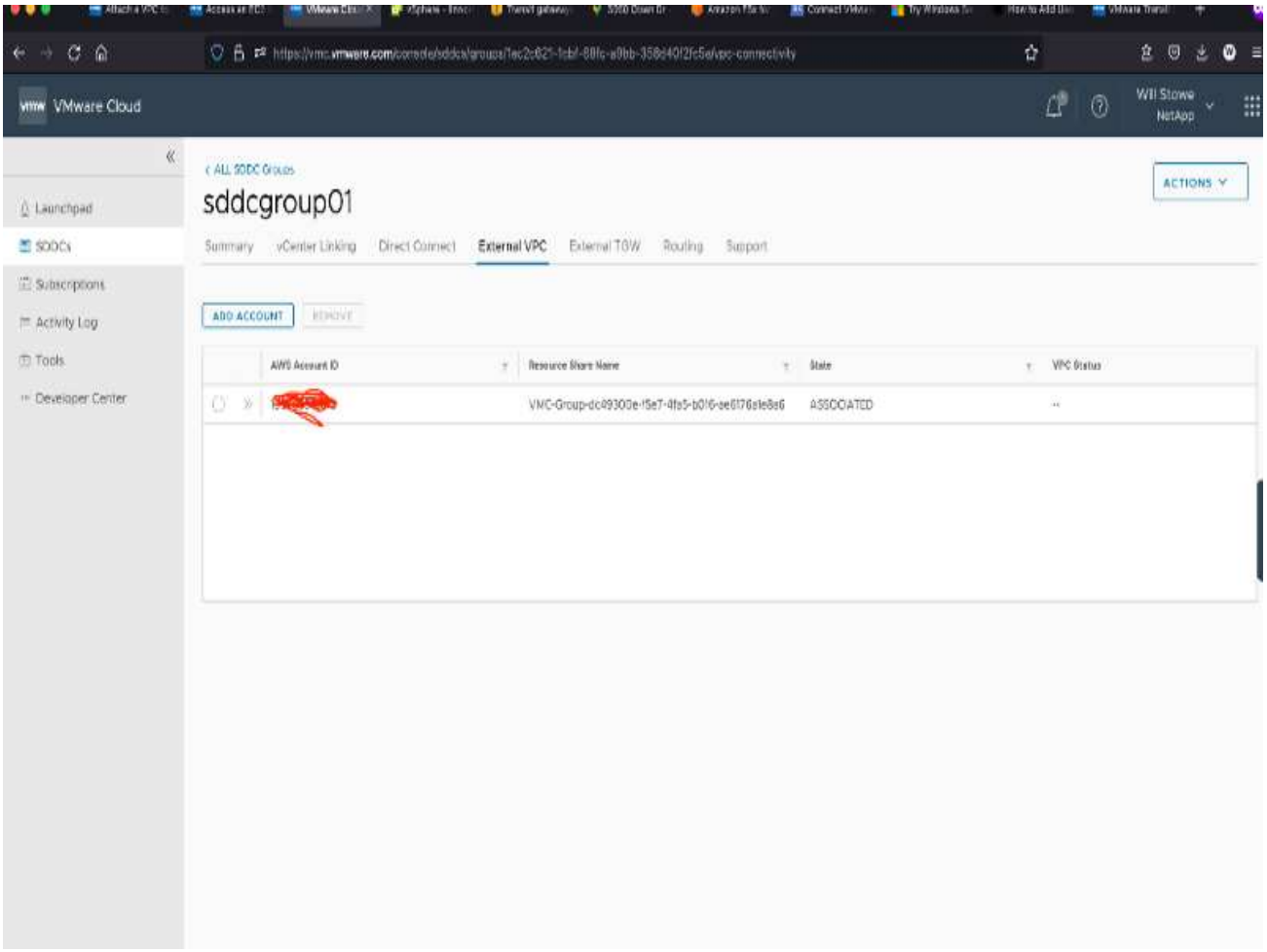




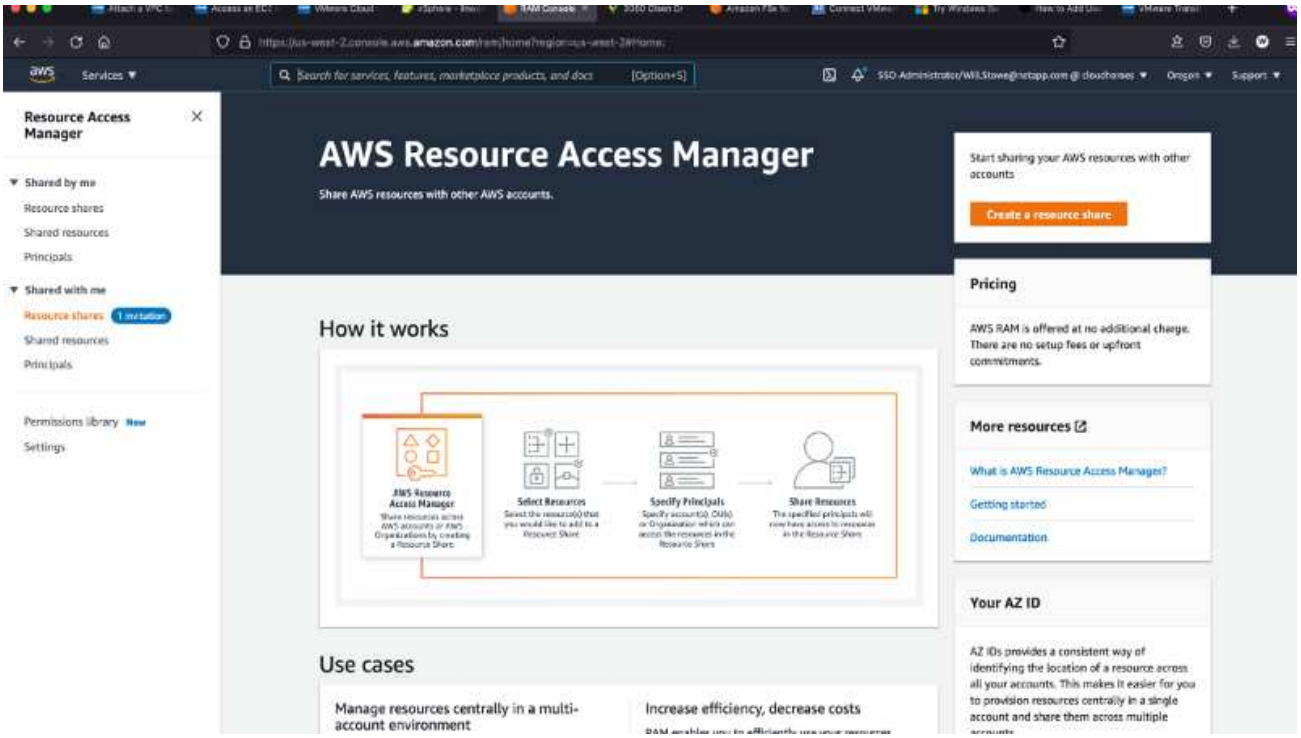


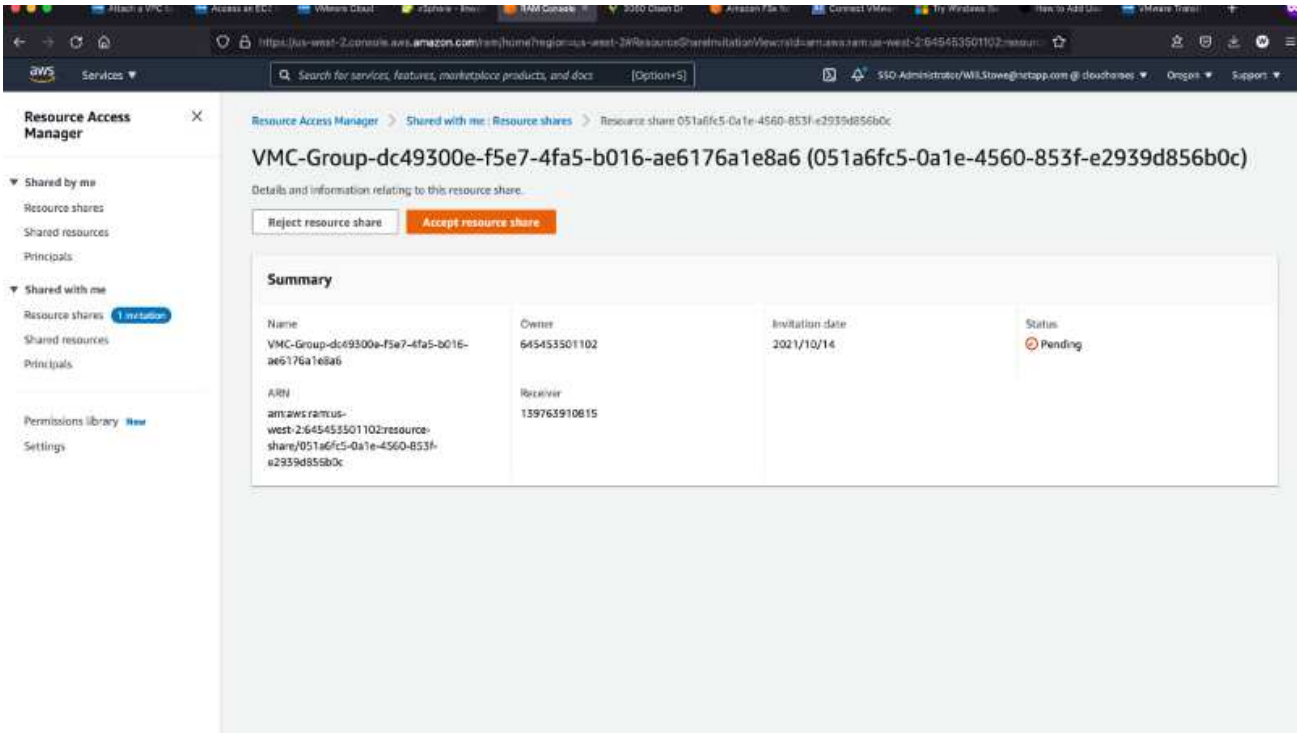
3. 新しく作成した VPC を、先ほど作成した SDDC グループに接続します。外部VPCタブを選択し、"外部VPCを接続する手順"グループへ。このプロセスが完了するまでに 10 ～ 15 分かかる場合があります。



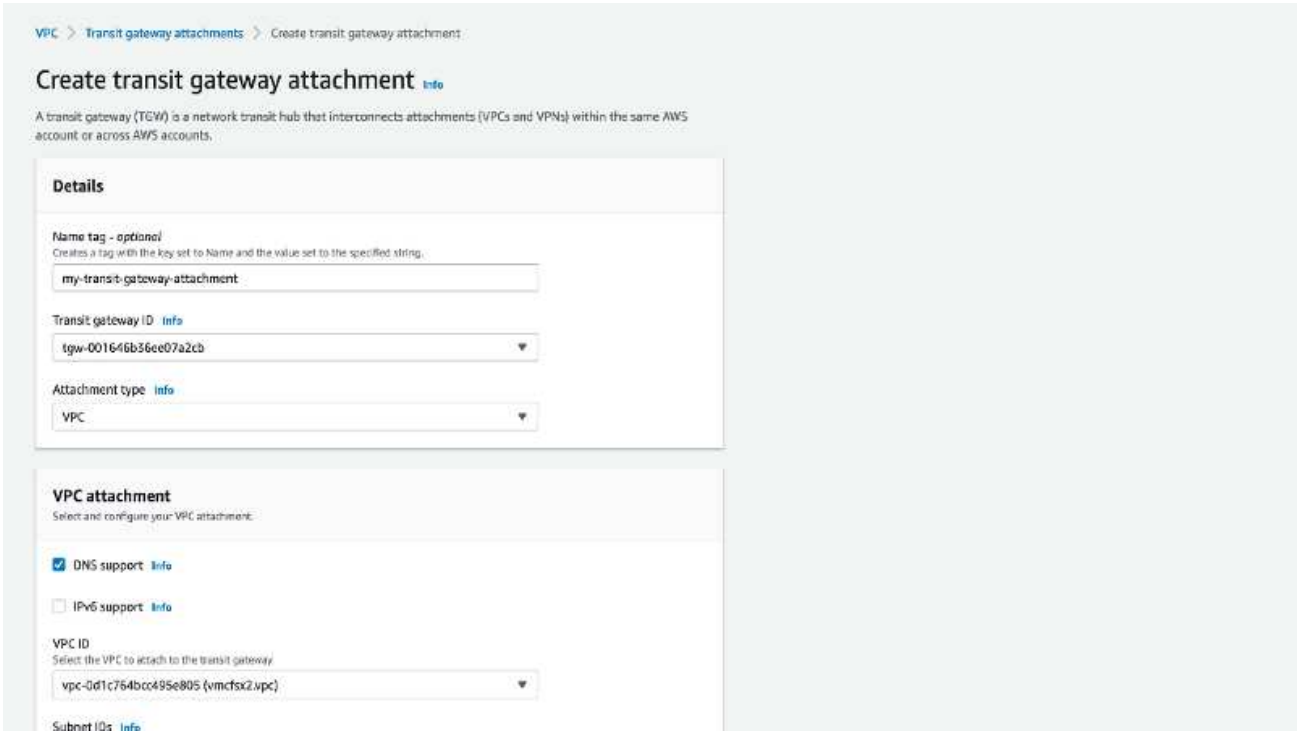


4. 外部 VPC プロセスの一環として、AWS コンソールから Resource Access Manager を介して新しい共有リソースへのプロンプトが表示されます。共有リソースは"AWS トランジットゲートウェイ"VMware Transit Connect によって管理されます。

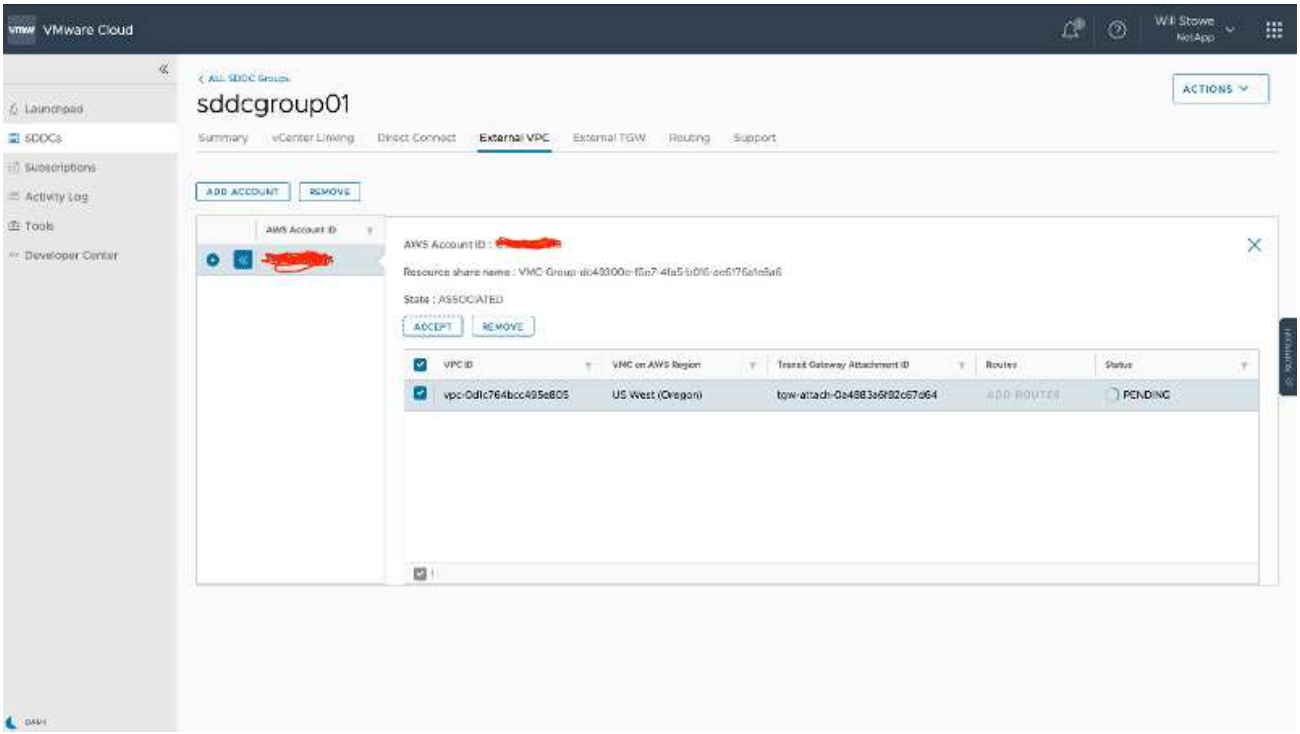




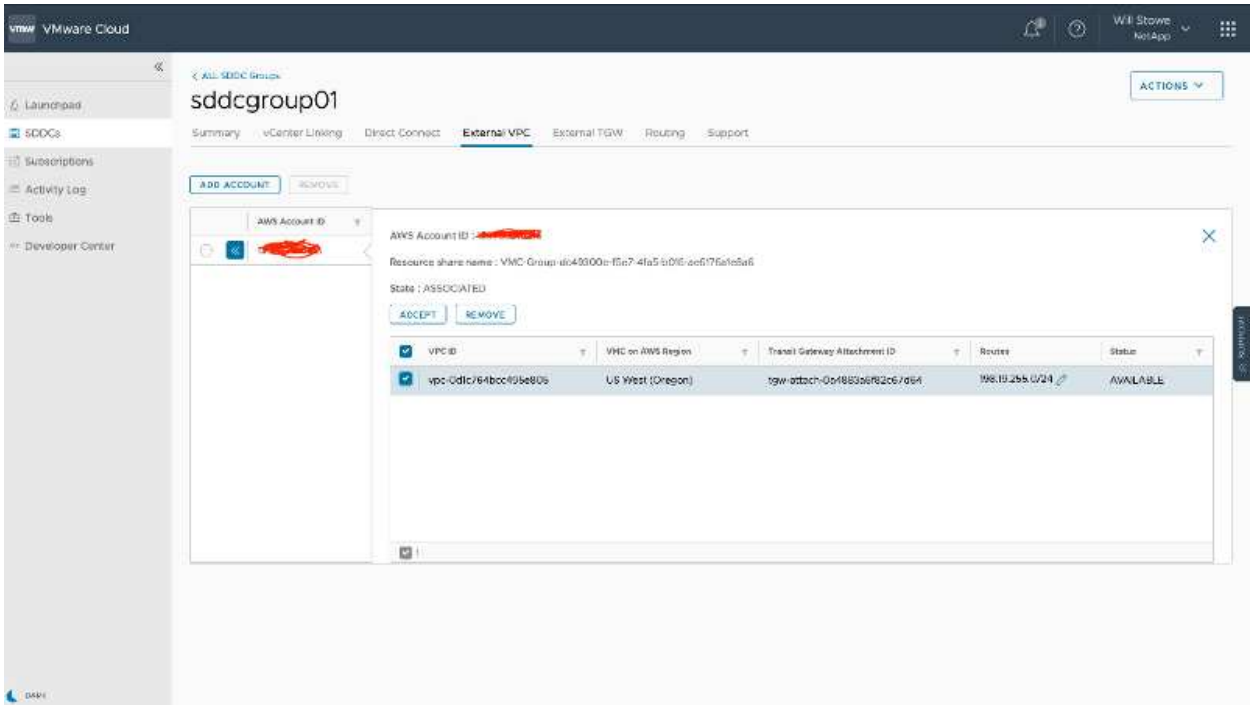
5. Transit Gateway アタッチメントを作成します。



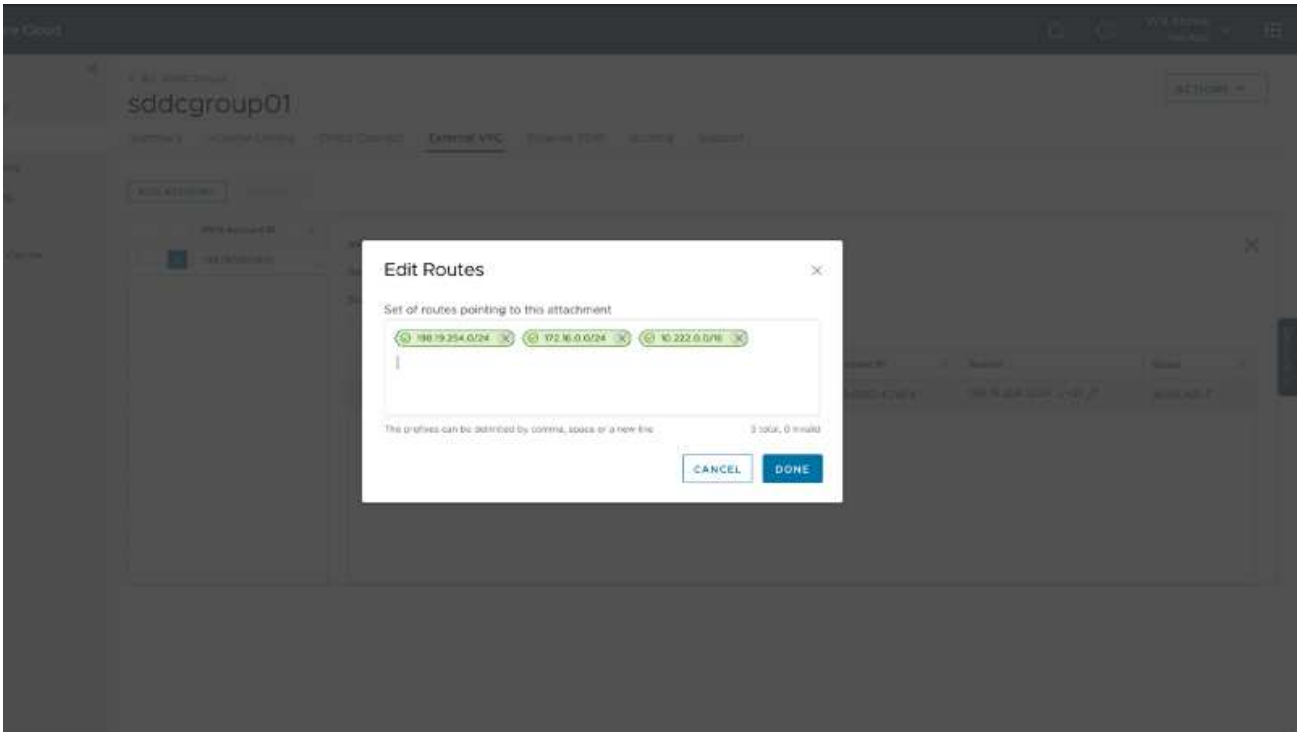
6. VMC コンソールに戻り、VPC アタッチメントを承認します。このプロセスが完了するまでに約 10 分かかります。



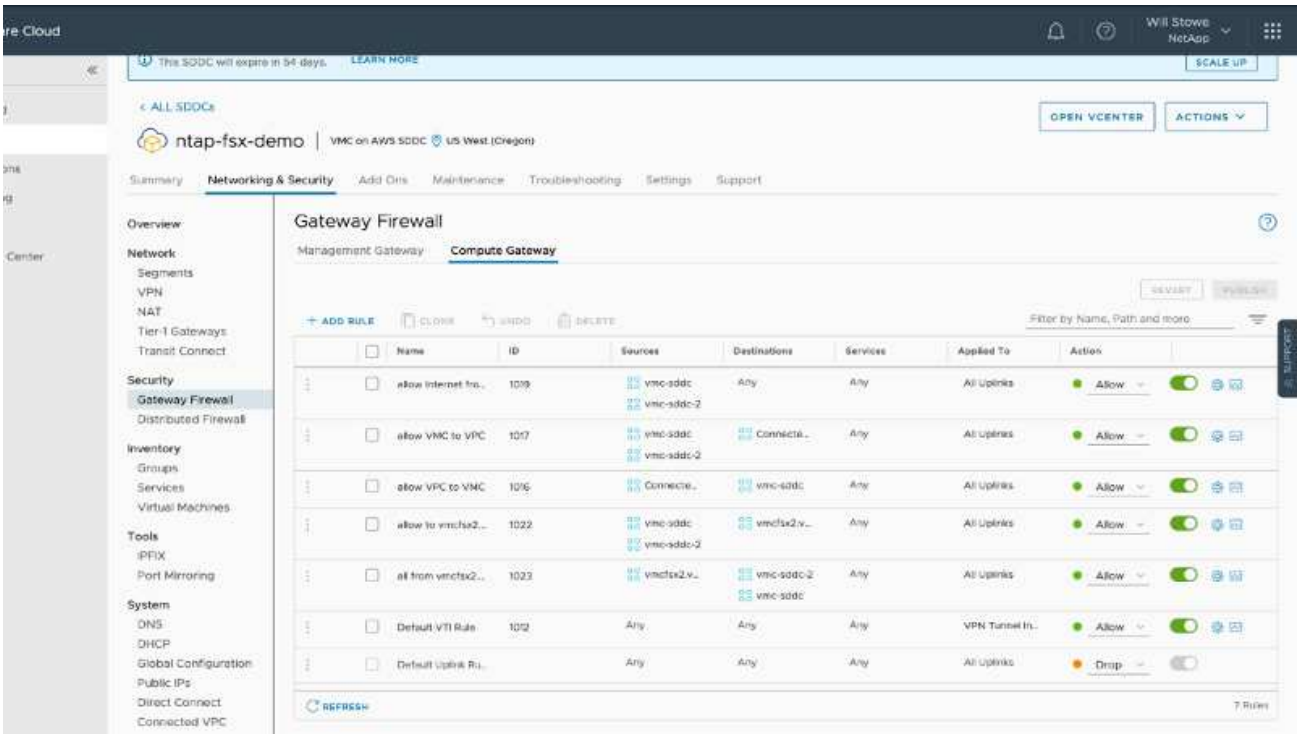
7. [外部 VPC] タブで、[ルート] 列の編集アイコンをクリックし、次の必要なルートを追加します。
   - Amazon FSx ONTAPのフローティング IP 範囲のルート"フローティングIP"。
   - Cloud Volumes ONTAPのフローティング IP 範囲のルート (該当する場合)。
   - 新しく作成された外部 VPC アドレス空間へのルート。



8. 最後に、双方向トラフィックを許可する"ファイアウォール ルール"FSx/CVO にアクセスします。これらに従ってください"詳細な手順"SDDC ワークロード接続のコンピューティング ゲートウェイ ファイアウォール ルール用。



9. 管理ゲートウェイとコンピューティングゲートウェイの両方にファイアウォール グループが設定されると、次のように vCenter にアクセスできるようになります。



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

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

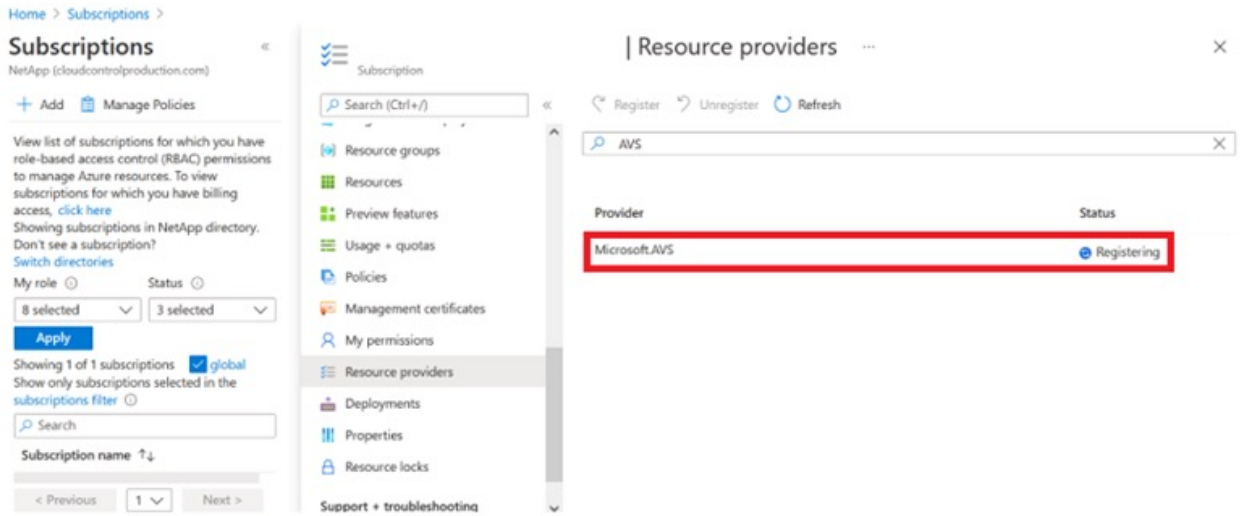
このセクションでは、Azure VMware Solution をセットアップおよび管理し、 NetAppストレージに接続するために使用可能なオプションと組み合わせて使用する方法について説明します。

セットアッププロセスは次の手順に分けられます。

▼ リソースプロバイダーを登録してプライベートクラウドを作成する

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

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

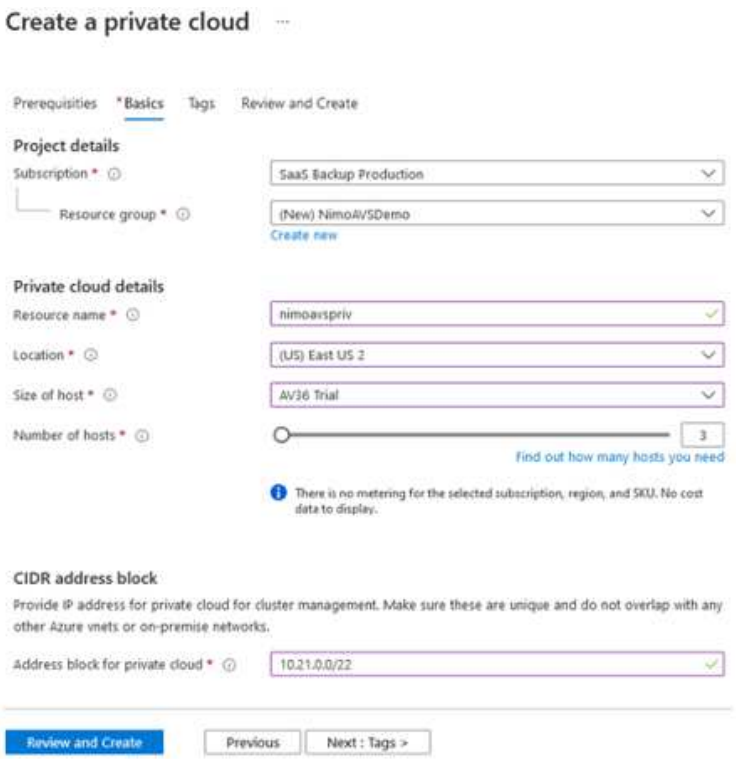




7. リソース プロバイダーを登録したら、Azure Portal を使用して Azure VMware Solution プライベート クラウドを作成します。
8. Azure ポータルにSign in。
9. [新しいリソースの作成]を選択します。
10. [Marketplace を検索] テキスト ボックスに「Azure VMware Solution」と入力し、結果から選択します。
11. Azure VMware Solution ページで、[作成] を選択します。
12. [基本] タブで、フィールドに値を入力し、[確認 + 作成] を選択します。

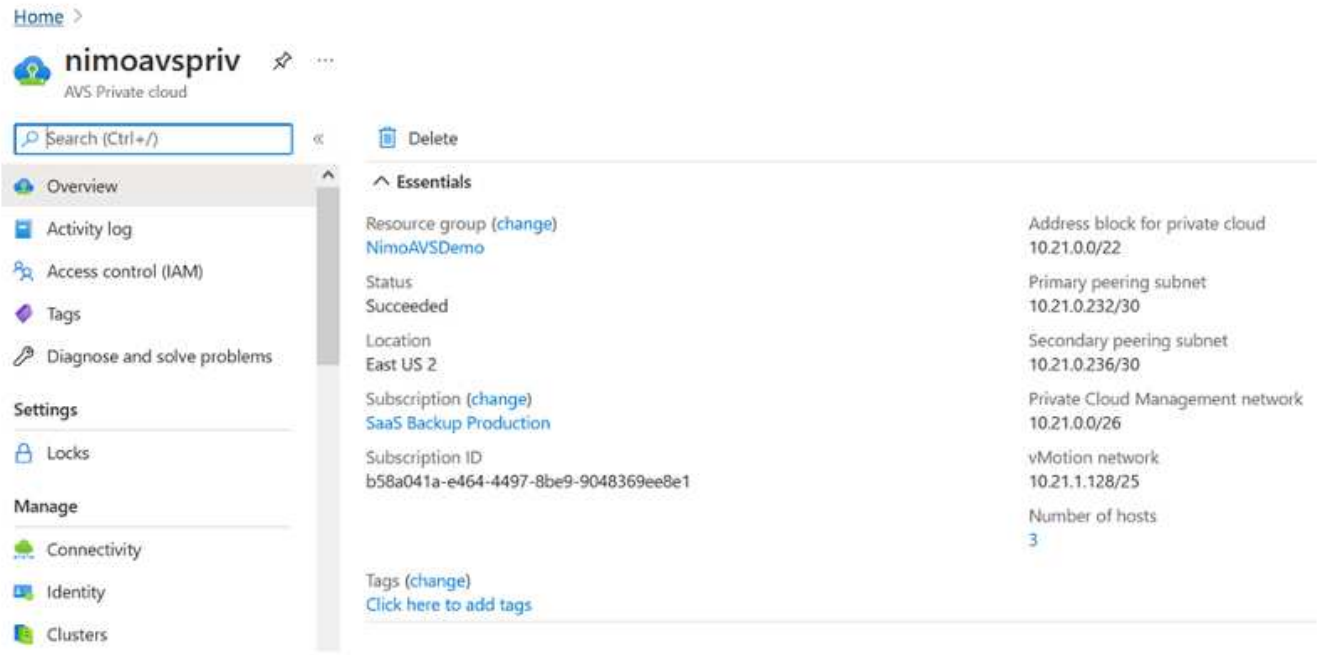
注：

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



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

Azure VMware Solution プライベート クラウドには、Azure Virtual Network が必要です。 Azure VMware Solution はオンプレミスの vCenter をサポートしていないため、既存のオンプレミス環境と統合するには追加の手順が必要です。 ExpressRoute 回線と仮想ネットワーク ゲートウェイの設定も必要です。クラスターのプロビジョニングが完了するまで待機中に、新しい仮想ネットワークを作成するか、既存の仮想ネットワークを使用して Azure VMware Solution に接続します。



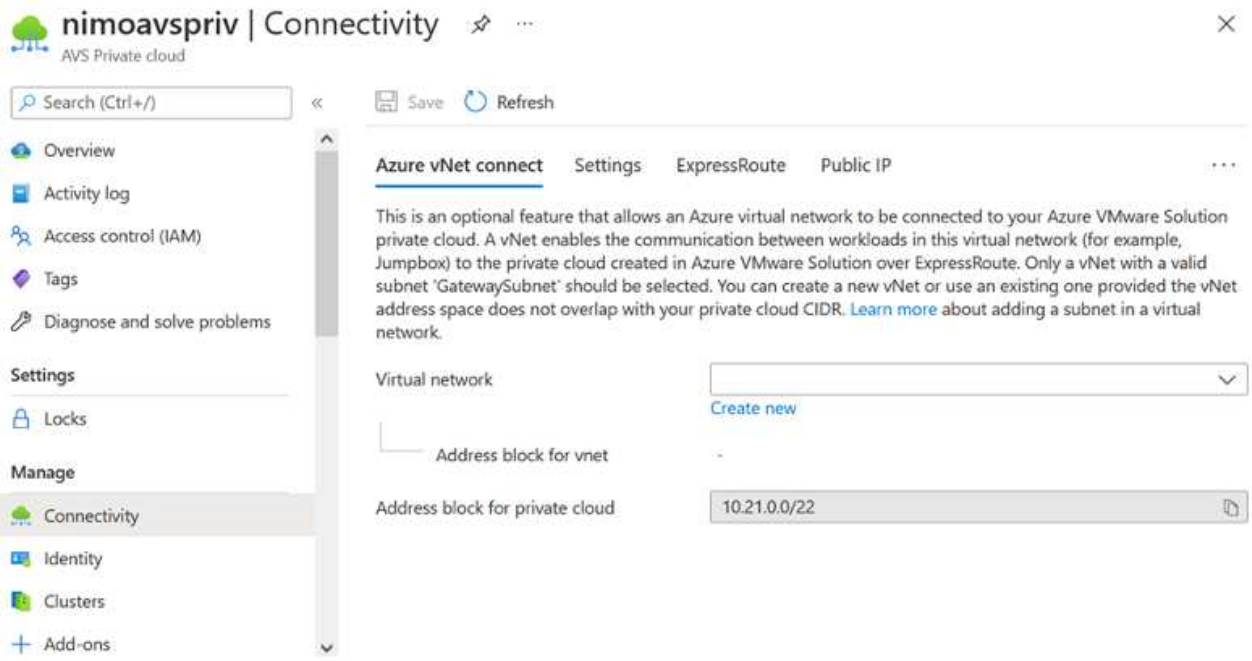
▼ 新規または既存の **ExpressRoute** 仮想ネットワーク ゲートウェイに接続する

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

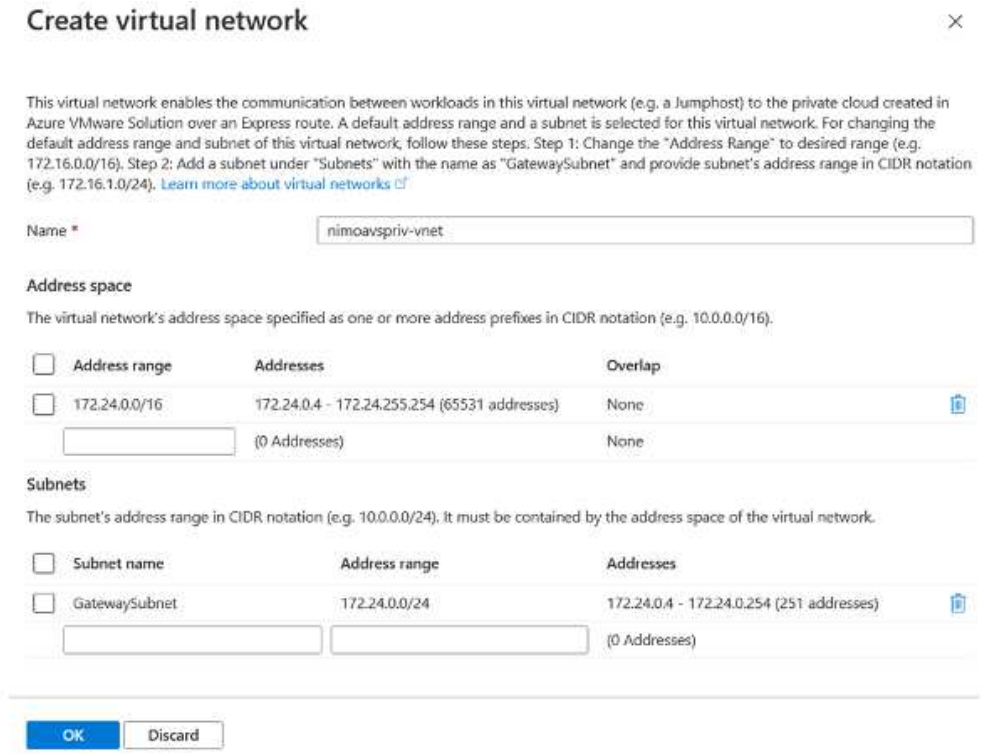
1. Azure VMware Solution プライベート クラウドに移動し、[管理] オプションの [接続] にアクセスします。
2. Azure VNet Connect を選択します。
3. 新しい VNet を作成するには、[新規作成] オプションを選択します。

   この機能により、VNet を Azure VMware Solution プライベート クラウドに接続できるようになります。 VNet は、ExpressRoute 経由で Azure VMware Solution に作成されたプライベート クラウドに必要なコンポーネント (ジャンプ ボックス、 Azure NetApp Filesなどの共有サービス、Cloud Volume ONTAPなど) を自動的に作成することにより、この仮想ネットワーク内のワークロード間の通信を可能にします。

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



4. 新しい VNet の情報を指定または更新し、[OK] を選択します。



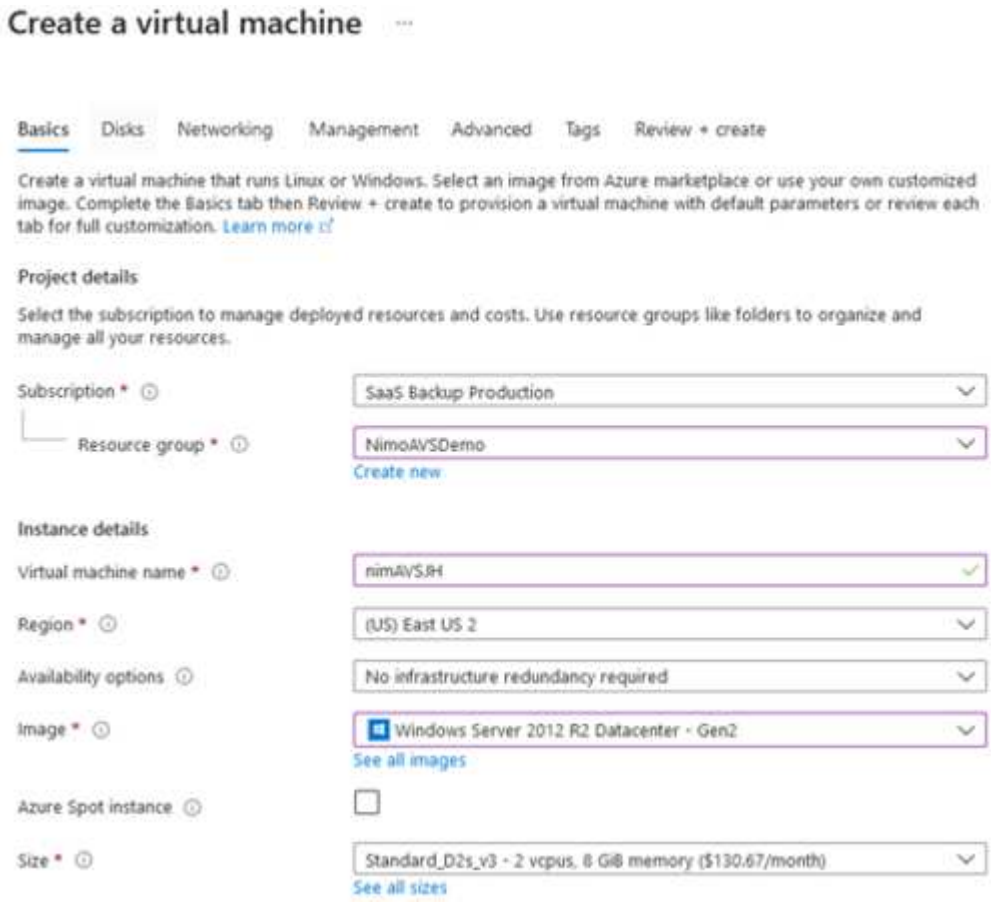
指定されたアドレス範囲とゲートウェイ サブネットを持つ VNet が、指定されたサブスクリプションとリソース グループに作成されます。

VNet を手動で作成する場合は、適切な SKU とゲートウェイの種類として ExpressRoute を使用して仮想ネットワーク ゲートウェイを作成します。デプロイが完了したら、承認キーを使用して、ExpressRoute 接続を Azure VMware Solution プライベート クラウドを含む仮想

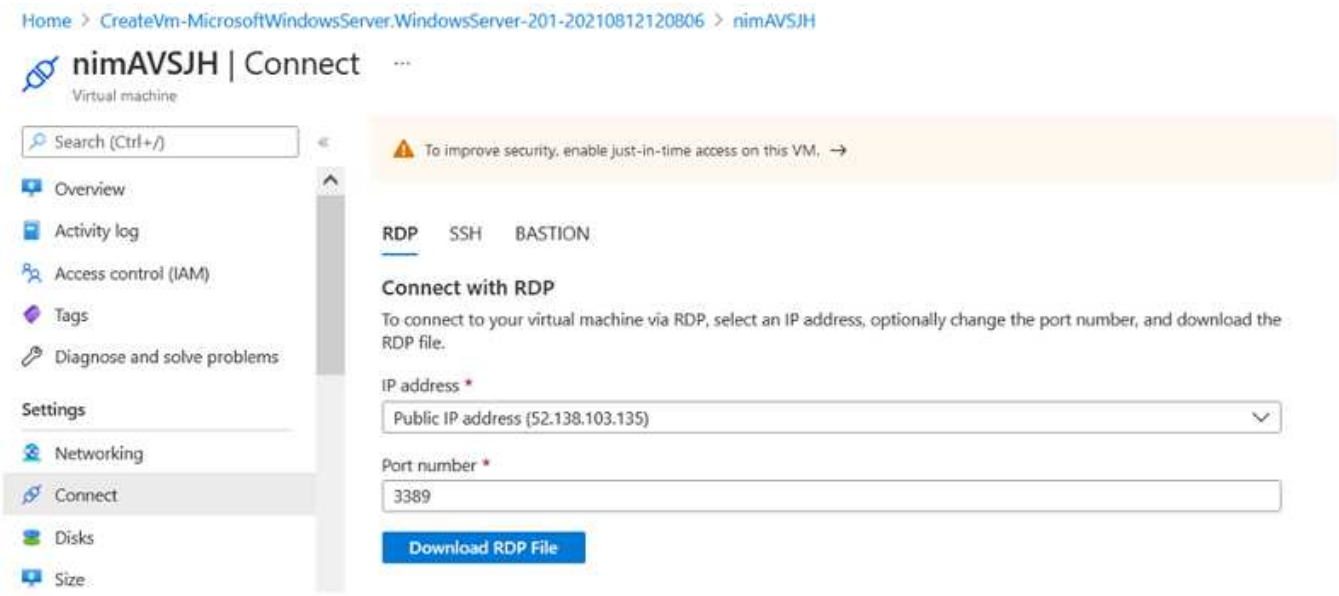
ネットワーク ゲートウェイに接続します。詳細については、以下を参照してください。"Azure で VMware プライベート クラウドのネットワークを構成する" 。

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

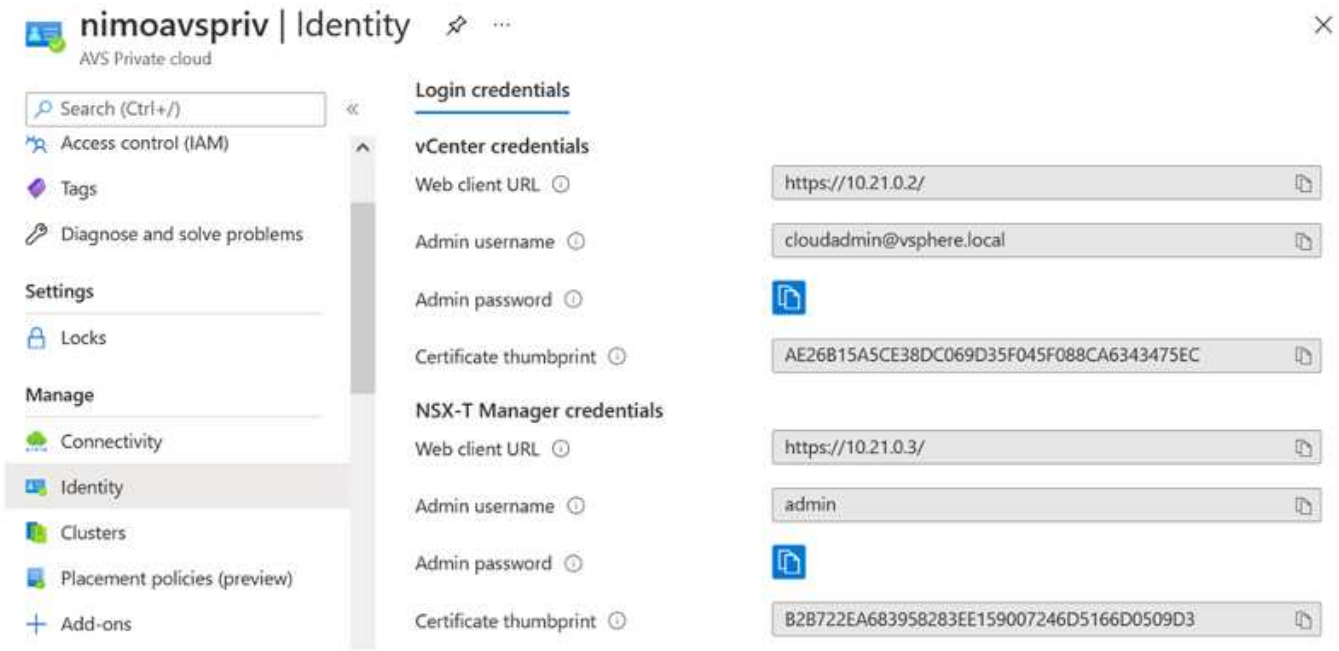
Azure VMware Solution では、オンプレミスの VMware vCenter を使用してプライベート クラウドを管理することはできません。代わりに、Azure VMware Solution vCenter インスタンスに接続するにはジャンプ ホストが必要です。指定されたリソース グループにジャンプ ホストを作成し、Azure VMware Solution vCenter にサインインします。このジャンプ ホストは、接続用に作成された同じ仮想ネットワーク上の Windows VM である必要があり、vCenter と NSX Manager の両方へのアクセスを提供する必要があります。



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



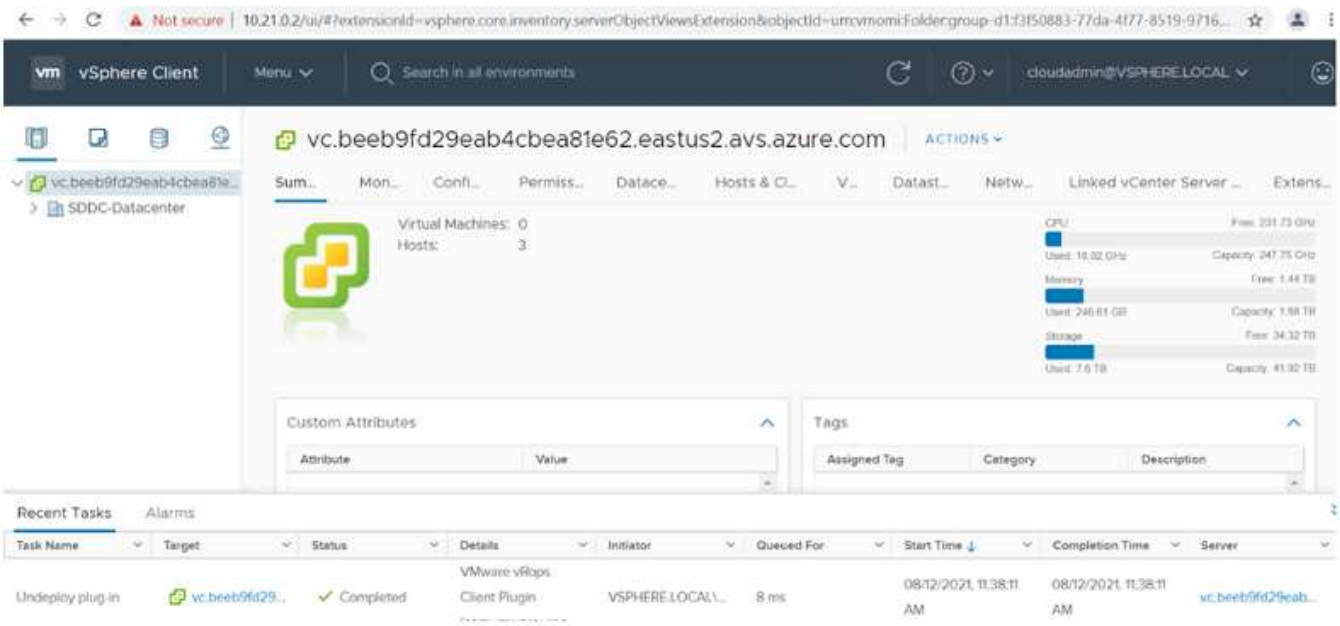
クラウド管理者ユーザーを使用して、この新しく作成されたジャンプ ホスト仮想マシンから vCenter にSign in。資格情報にアクセスするには、Azure ポータルに移動し、(プライベート クラウド内の [管理] オプションの下の) [ID] に移動します。プライベート クラウド vCenter および NSX-T Manager の URL とユーザー資格情報はここからコピーできます。



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

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





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

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

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

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

セットアッププロセスは次の手順に分けられます。

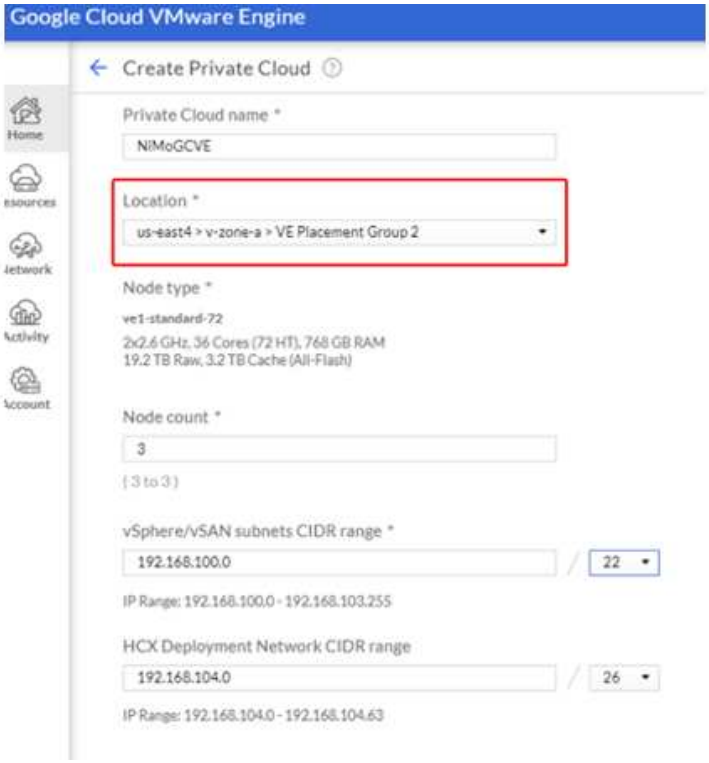
▼ **GCVE** の展開と構成

GCP 上で GCVE 環境を構成するには、GCP コンソールにログインし、VMware Engine ポータルにアクセスします。

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

前提条件

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



注: プライベート クラウドの作成には 30 分から 2 時間ほどかかる場合があります。

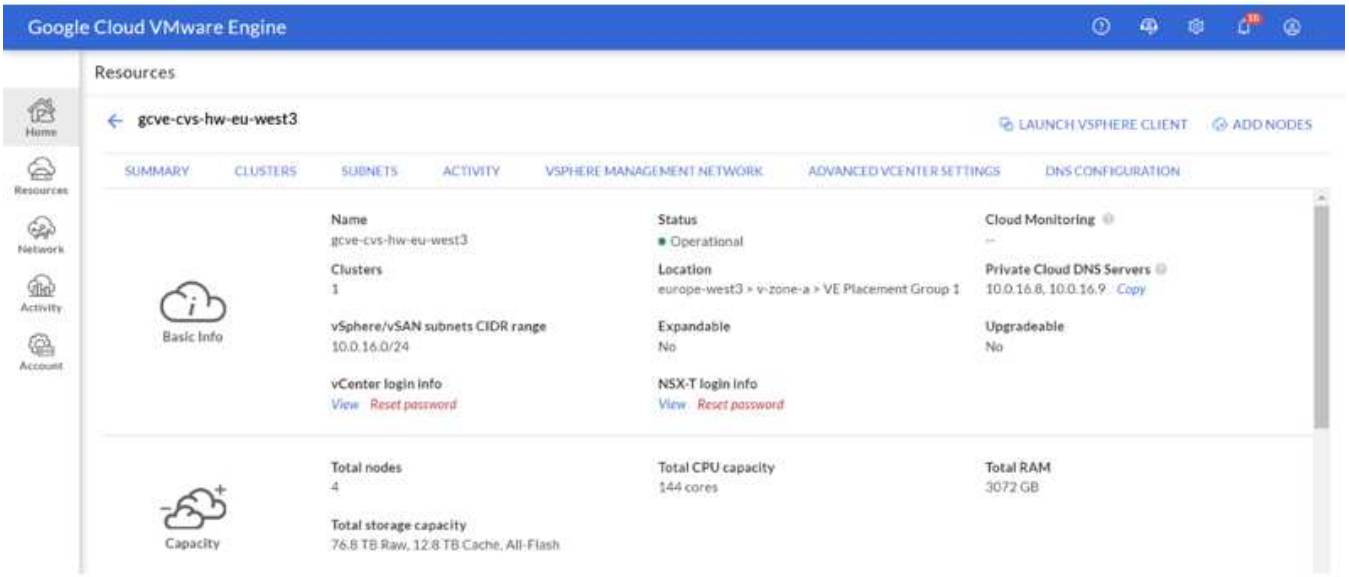
▼ **GCVE**へのプライベートアクセスを有効にする

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

これにより、Cloud Volumes ONTAPインスタンスが実行されているVPCネットワークが、GCVEプライベートクラウドと通信できるようになります。そのためには、"GCPのドキュメント"に従ってください。Cloud Volume Serviceの場合、テナントホストプロジェクト間で1回限りのピアリングを実行することにより、VMware EngineとGoogle Cloud NetApp Volumesの間の接続を確立します。詳細な手順については、この"リンク"に従ってください。

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

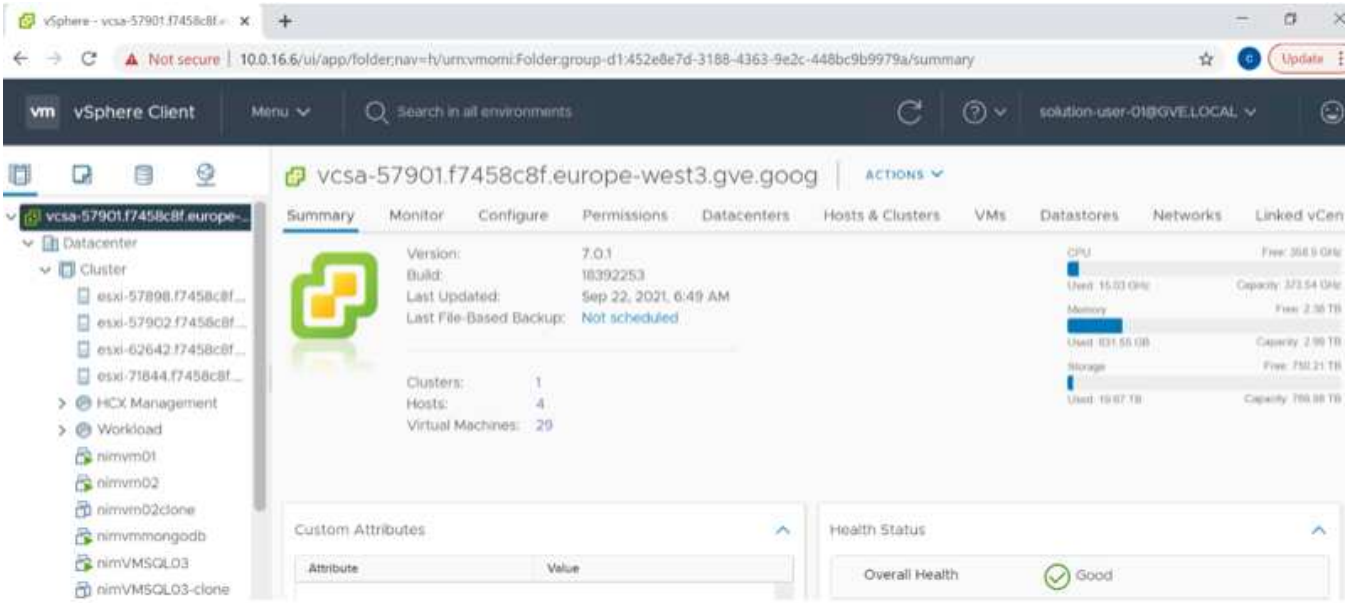
CloudOwner@gve.local ユーザーを使用して vCenter にSign in。認証情報にアクセスするには、VMware Engine ポータルにアクセスし、[リソース] に移動して、適切なプライベート クラウドを選択します。 [基本情報] セクションで、vCenter ログイン情報 (vCenter Server、HCX Manager) または NSX-T ログイン情報 (NSX Manager) の [表示] リンクをクリックします。



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

オンプレミス ネットワークから VMware Engine プライベート クラウドに接続するには、適切な接続のためにクラウド VPN または Cloud Interconnect を活用し、必要なポートが開いていることを確認します。詳細な手順については、こちらを参照してください"リンク"。





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

参照する"NetApp Volumes を使用した追加の NFS データストアを GCVE に展開する手順"

パブリッククラウドにおける**NetApp**ストレージ

パブリッククラウドプロバイダー向けの**NetApp**ストレージオプション

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

AWS / VMC

AWS は、次の構成でNetAppストレージをサポートしています。

- ゲスト接続ストレージとしての FSx ONTAP

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

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

Azure / AVS

Azure は、次の構成のNetAppストレージをサポートしています。

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

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

GCP / GCVE

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

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

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

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

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

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

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

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

詳細については、以下をご覧ください。

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

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

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

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

FSx ONTAPを使用すると、ボタンをクリックするだけでファイルのスナップショット、クローン、複製ができるため、データの管理が簡単になります。さらに、FSx ONTAP はデータを低コストで弾力性のあるストレージに自動的に階層化するため、容量のプロビジョニングや管理の必要性が軽減されます。

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

詳細については、"ゲスト接続ストレージとしての FSx ONTAP"

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

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

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

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

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

詳細については、"ゲスト接続ストレージとしてのCVO" 。

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

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

はじめに

成功している組織はすべて、変革と近代化の道を歩んでいます。このプロセスの一環として、企業は通常、既存の VMware 投資を活用してクラウドのメリットを活用し、プロセスを可能な限りシームレスに移行、バースト、拡張し、災害復旧を提供する方法を検討します。クラウドに移行する顧客は、弾力性とバースト、データセンターの廃止、データセンターの統合、サポート終了のシナリオ、合併、買収などのユースケースを評価

する必要があります。

VMware Cloud on AWS は、顧客に独自のハイブリッド機能を提供するため、大多数の顧客が好むオプションですが、ネイティブ ストレージ オプションが限られているため、ストレージを多用するワークロードを持つ組織にとってはその有用性が制限されています。ストレージはホストに直接結び付けられているため、ストレージを拡張する唯一の方法はホストを追加することであり、これによりストレージを集中的に使用するワークロードのコストが 35 ～ 40% 以上増加する可能性があります。これらのワークロードには、追加の処理能力ではなく、追加のストレージと分離されたパフォーマンスが必要ですが、追加のホストに対して料金を支払う必要があります。ここで、 "最近の統合" FSx ONTAPは、VMware Cloud on AWS でのストレージとパフォーマンス集約型のワークロードに役立ちます。

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

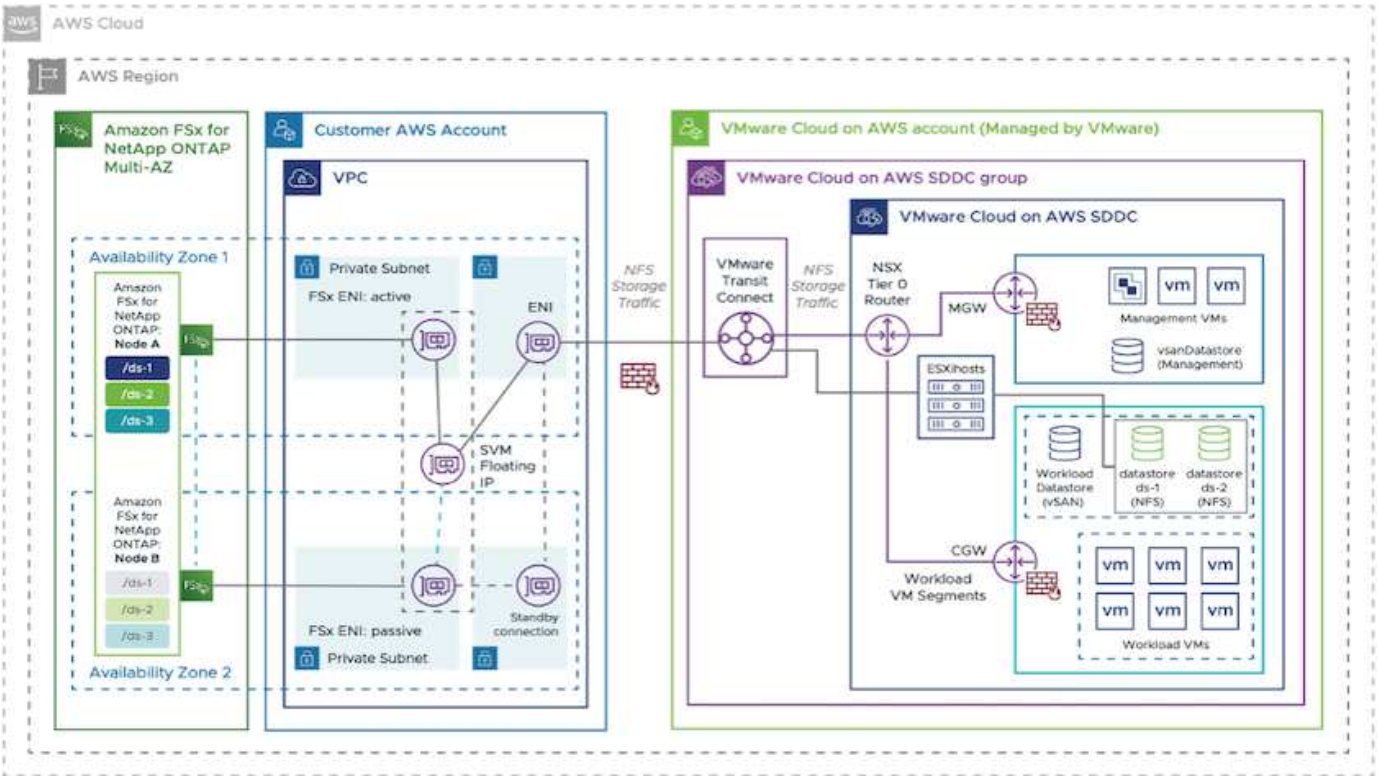
このドキュメントでは、VMware Cloud on AWS の NFS データストアとして FSx ONTAP をプロビジョニングして接続するために必要な手順について説明します。

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

接続オプション

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

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



大まかな展開手順は次のとおりです。

1. 新しく指定された VPC にAmazon FSx ONTAPを作成します。
2. SDDC グループを作成します。
3. VMware Transit Connect と TGW アタッチメントを作成します。
4. ルーティング (AWS VPC および SDDC) とセキュリティ グループを構成します。
5. NFS ボリュームをデータストアとして SDDC クラスタに接続します。

FSx ONTAP をNFS データストアとしてプロビジョニングして接続する前に、まず VMware on Cloud SDDC 環境をセットアップするか、既存の SDDC を v1.20 以上にアップグレードする必要があります。詳細については、 "VMware Cloud on AWS を使い始める" 。

FSx ONTAPは現在、ストレッチ クラスターではサポートされていません。

まとめ

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

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

AWS で補足 NFS データストアを作成する

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

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

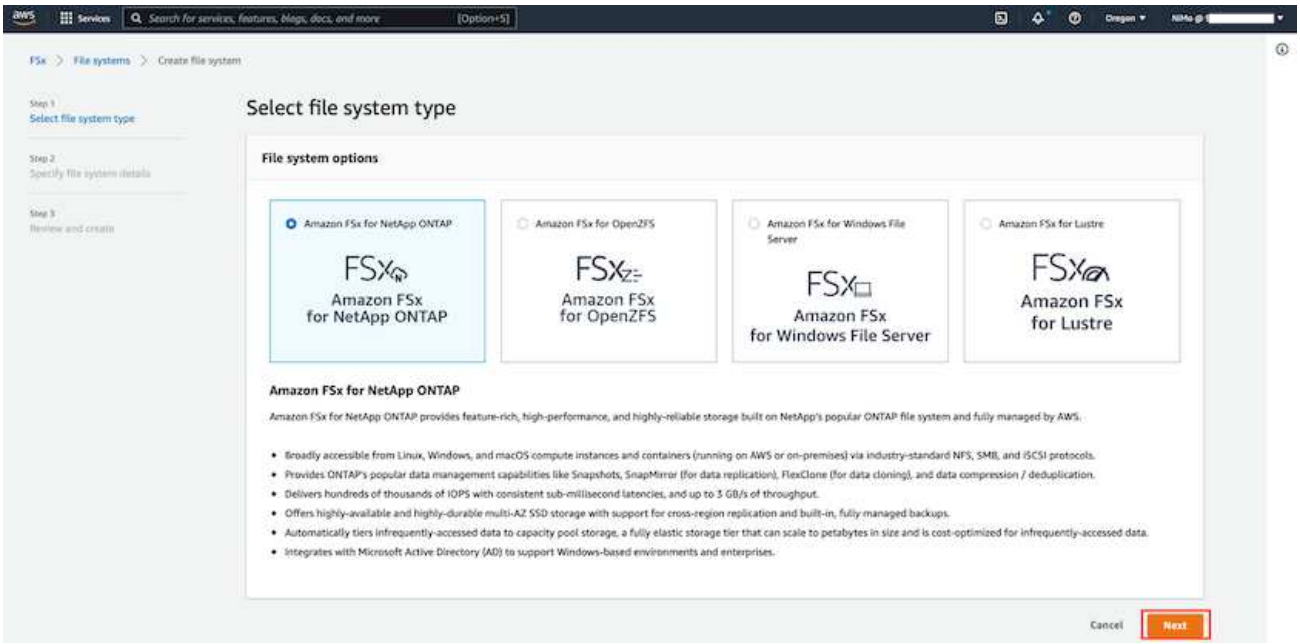
FSx ONTAP をVMware Cloud on AWS SDDC と同じアベイラビリティーゾーンにデプロイします。

接続された VPC に FSx ONTAPをデプロイすることはできません。代わりに、新しい指定された VPC にデプロイし、SDDC グループを介して VPC を VMware Managed Transit Gateway (vTGW) に接続する必要があります。

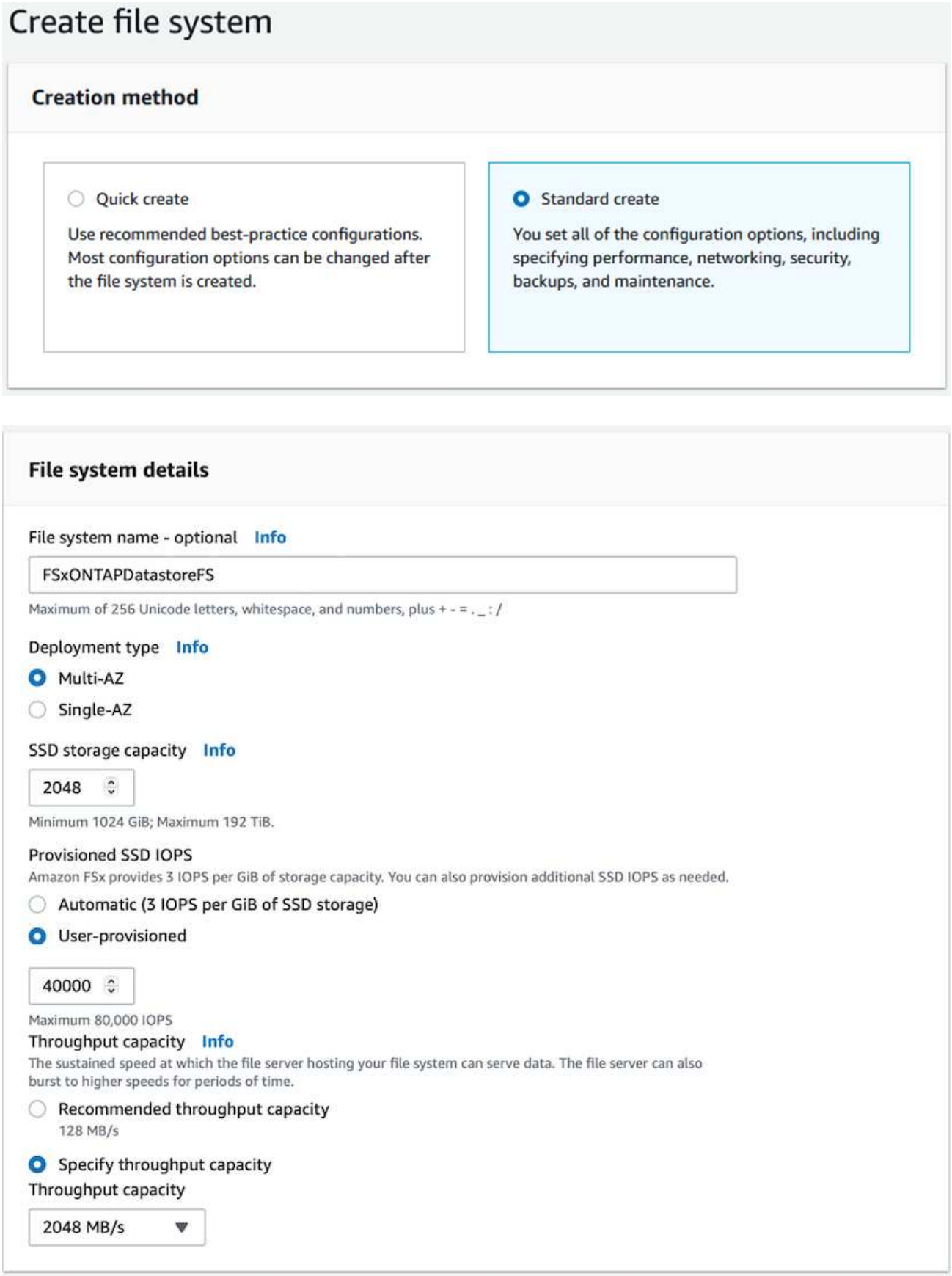
▼ ステップ 1: 新しい指定 VPC にAmazon FSx ONTAPを作成する

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

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



3. 作成方法としては*標準作成*を選択します。



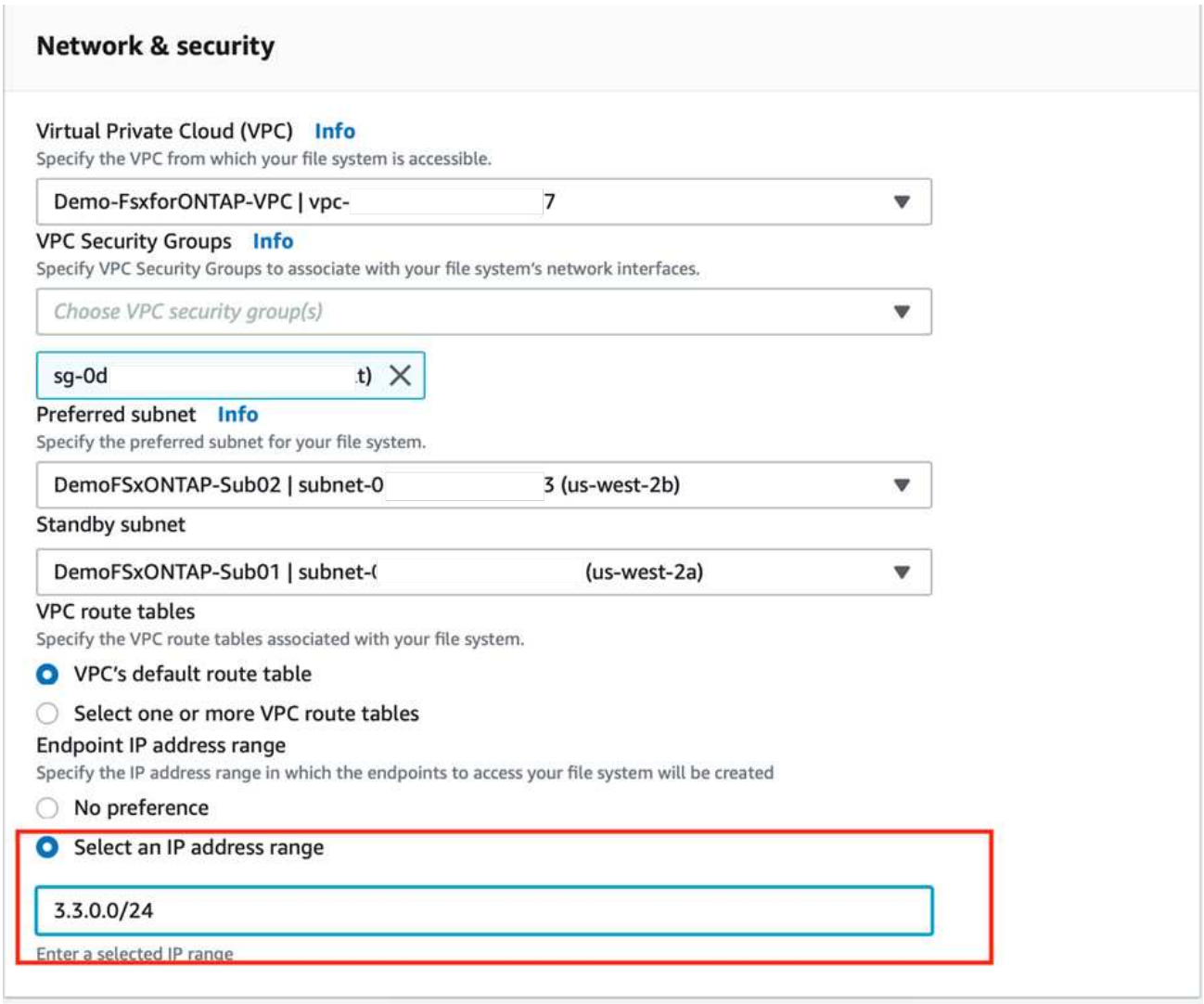
データストアのサイズは顧客ごとにかなり異なります。 NFS データストアあたりの仮想マシンの推奨数は主観的ですが、各データストアに配置できる仮想マシンの最適な数は

多くの要因によって決まります。ほとんどの管理者は容量のみを考慮しますが、VMDK に送信される同時 I/O の量は、全体的なパフォーマンスにとって最も重要な要素の 1 つです。オンプレミスのパフォーマンス統計を使用して、それに応じてデータストアのボリュームのサイズを決定します。

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

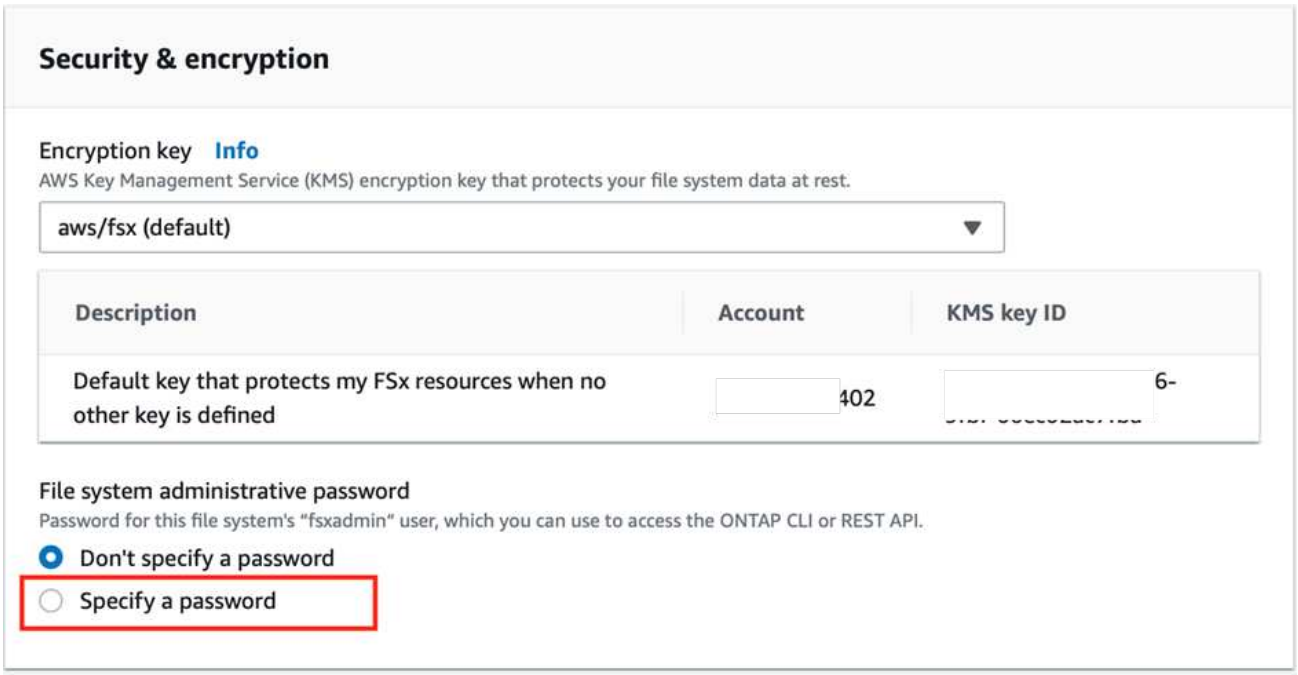
これが接続された VPC ではなく、指定された新しい VPC であることを確認してください。

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



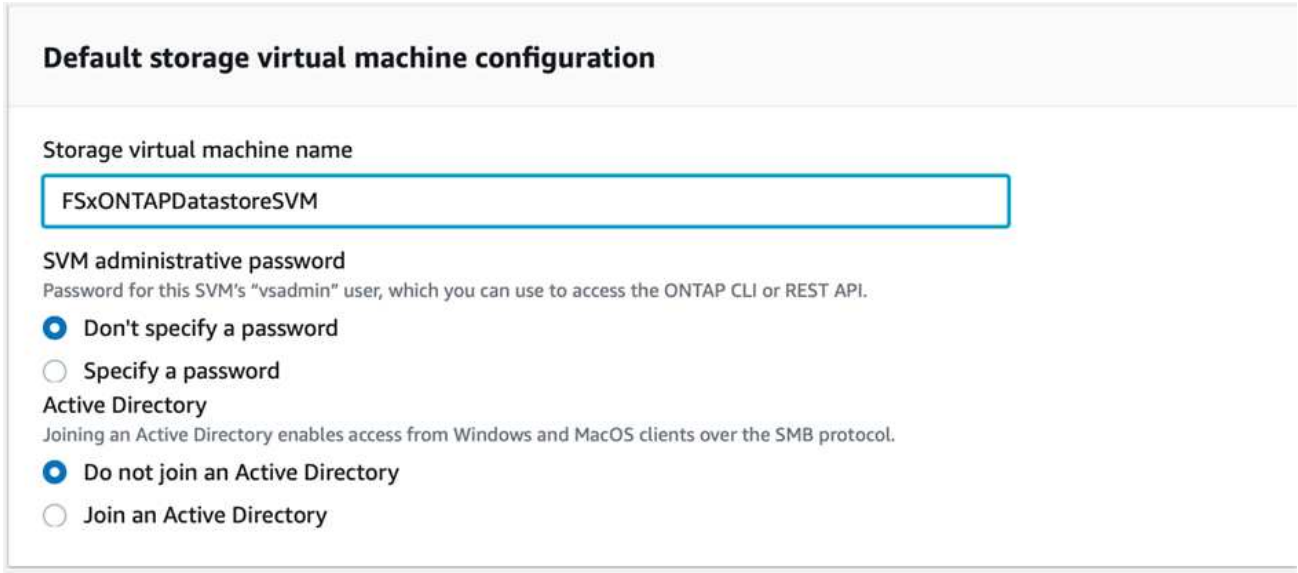
5. 暗号化キーの セキュリティと暗号化 セクションで、保存中のファイルシステムのデータを保護する AWS Key Management Service (AWS KMS) 暗号化キーを選択します。 ファイル システム管理パスワ

ード には、fsxadmin ユーザーの安全なパスワードを入力します。



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

GA 時点では、4 つの NFS データストアがサポートされています。



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

設定	構成
ボリューム保証（スペース保証型）	なし（シンプロビジョニング） – デフォルトで設定

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

ボリュームを作成および変更するには、次の SSH コマンドを使用します。

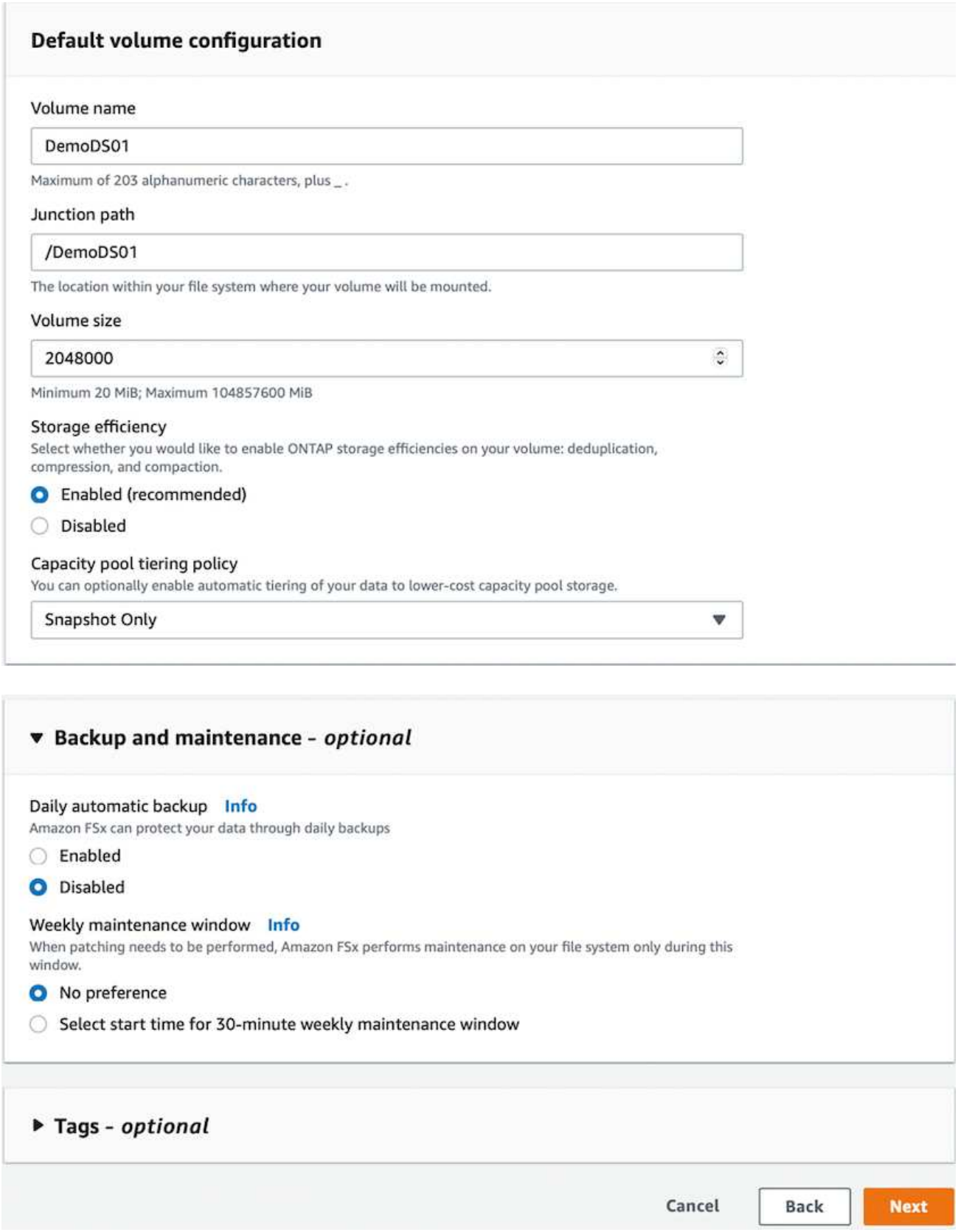
シェルから新しいデータストアボリュームを作成するコマンド:

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

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

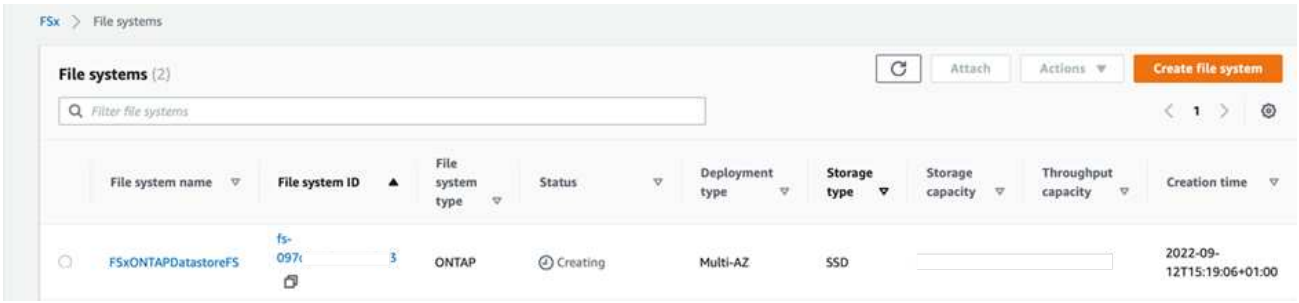
デフォルトで設定されていないボリュームパラメータを変更するコマンド:

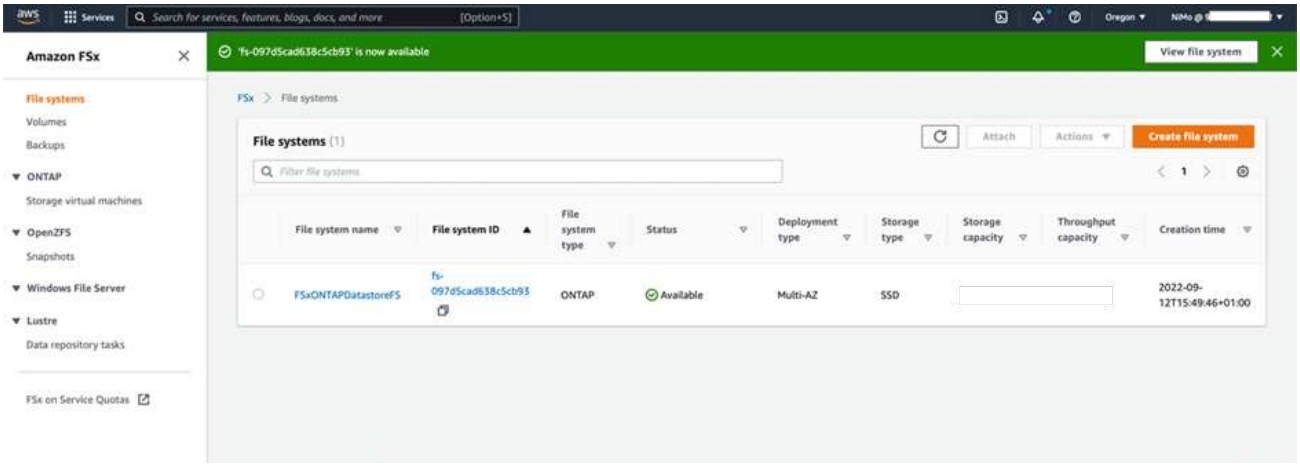
```
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-fractional-reserve 0
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002 -space
-mgmt-try-first vol_grow
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-autosize-mode grow
```



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

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





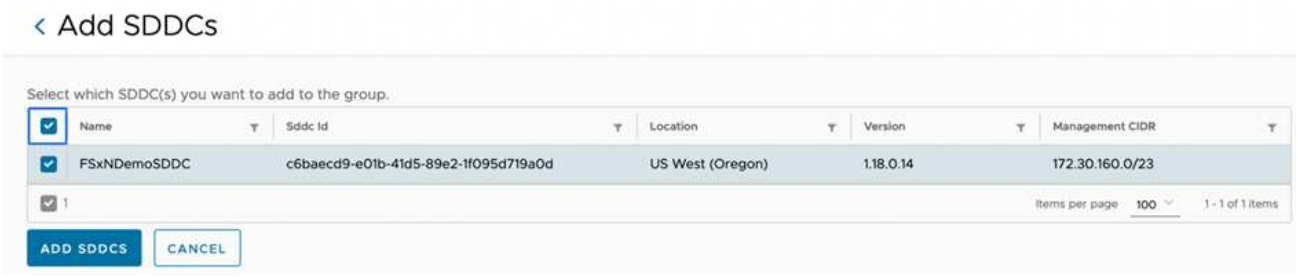
容量とパフォーマンスの要件に応じて、前の手順を繰り返して、さらにストレージ仮想マシンまたはファイル システムとデータストア ボリュームを作成します。

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

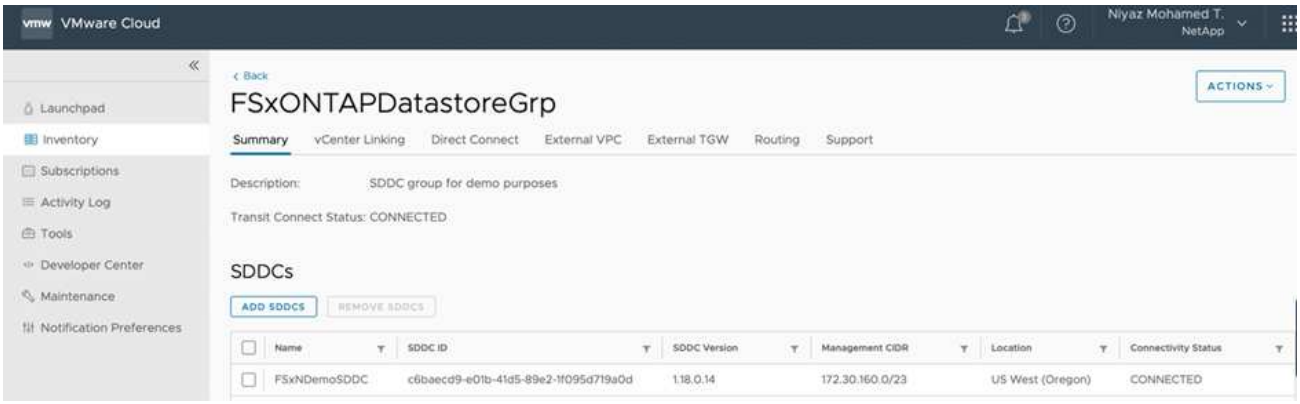
▼ ステップ**2: SDDC**グループを作成する

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

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

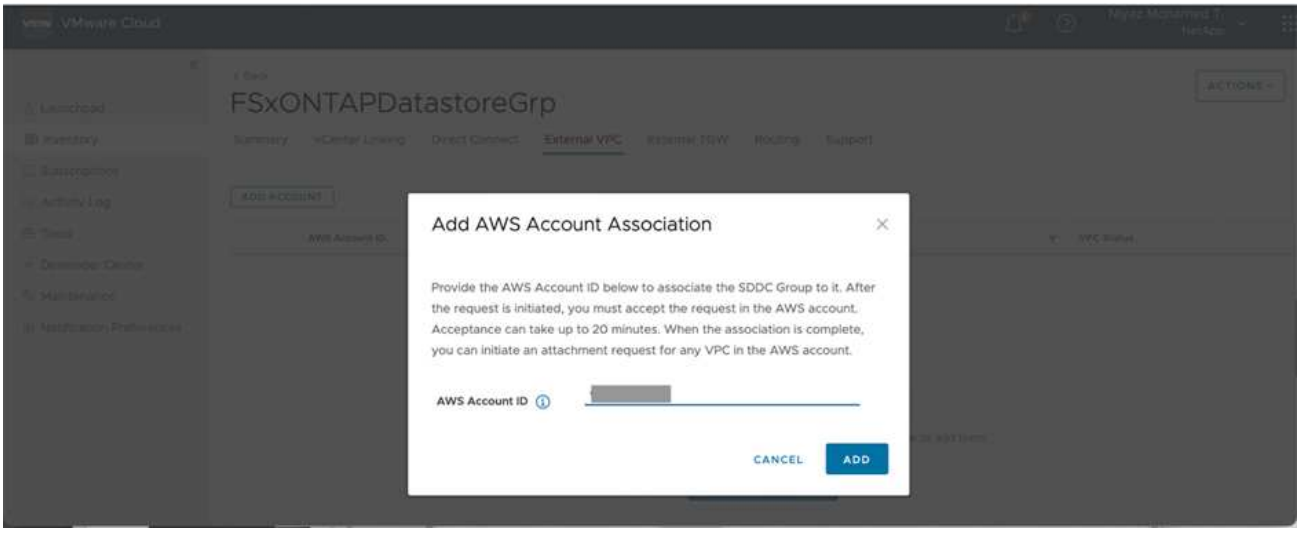


5. 「グループに VMware Transit Connect を構成すると、添付ファイルとデータ転送ごとに料金が発生します」がチェックされていることを確認し、[グループの作成] を選択します。このプロセスは完了するまでに数分かかる場合があります。

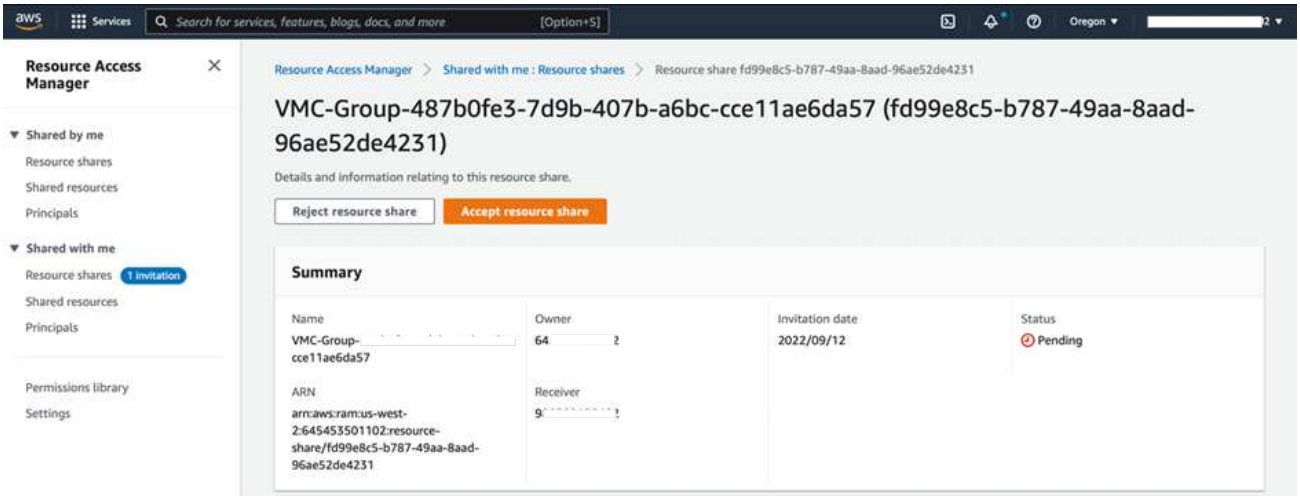


▼ ステップ**3: VMware Transit Connect**を構成する

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

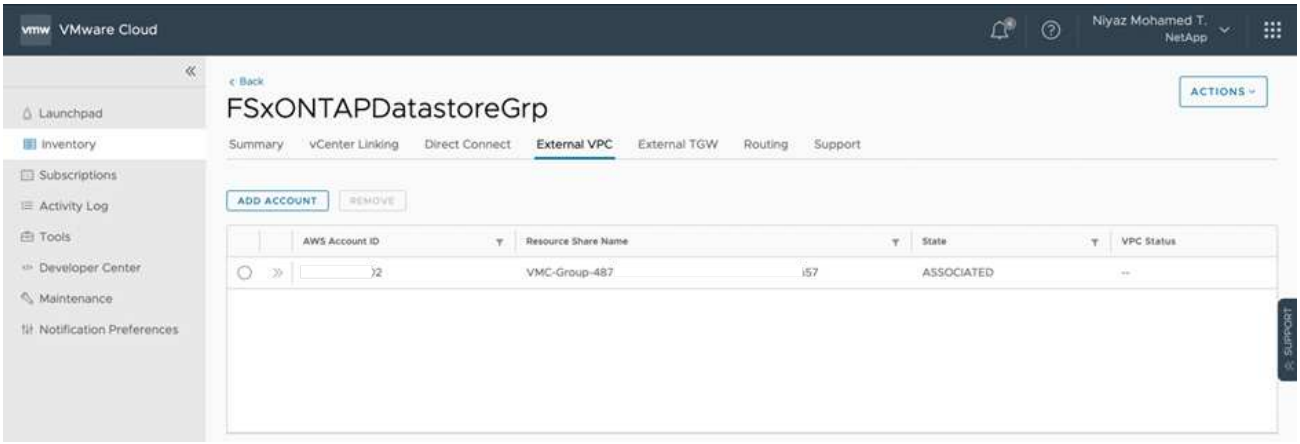


2. *アカウントを追加*をクリックします。
   a. FSx ONTAPファイルシステムのプロビジョニングに使用された AWS アカウントを提供します。
   b. *[追加]*をクリックします。
3. AWS コンソールに戻り、同じ AWS アカウントにログインして、**Resource Access Manager** サービス ページに移動します。リソース共有を受け入れるためのボタンがあります。



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

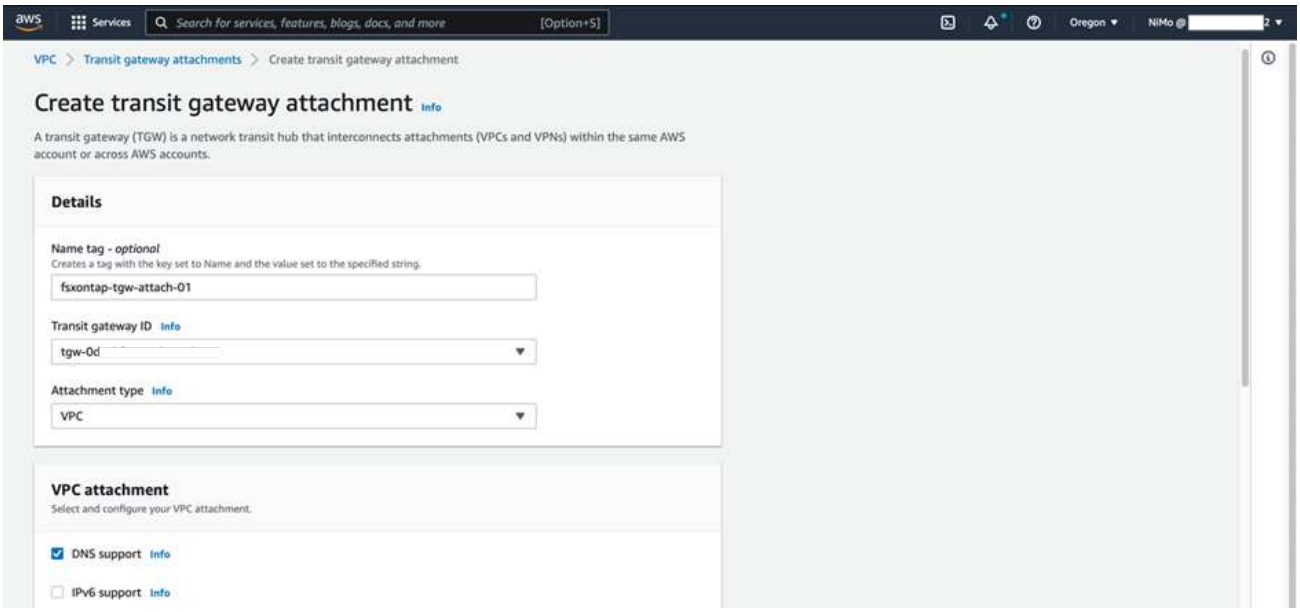
4. *リソース共有を承認*をクリックします。



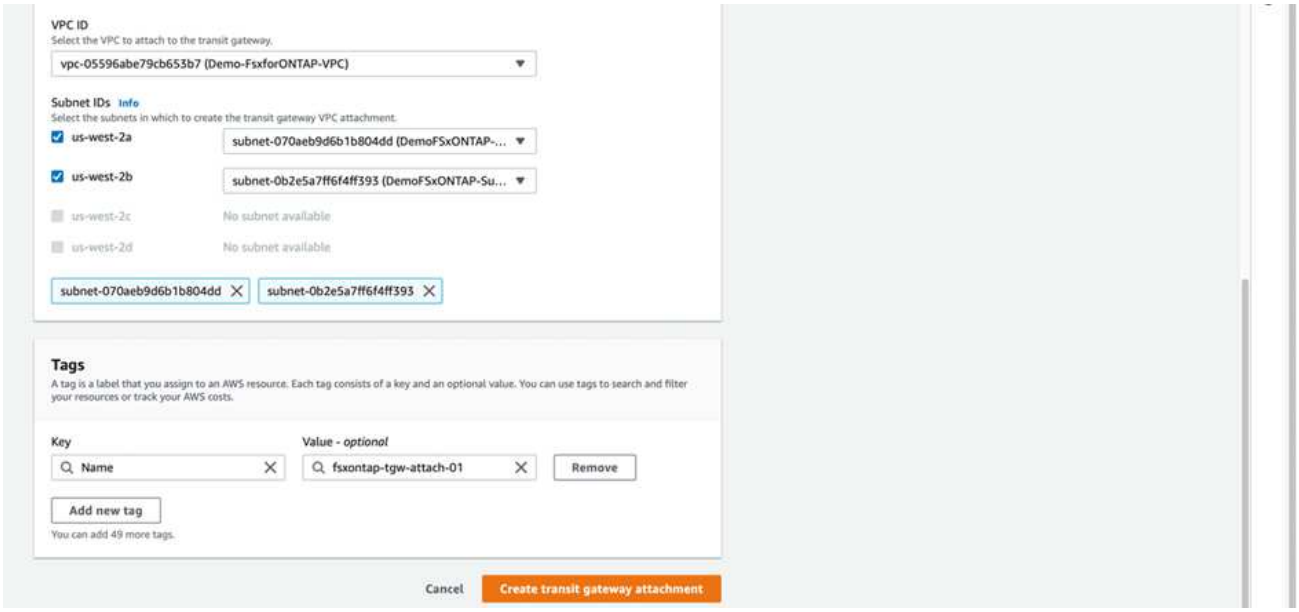
5. VMC コンソールに戻ると、外部 VPC が関連付けられた状態になっていることがわかります。表示されるまで数分かかる場合があります。

▼ ステップ**4:** トランジットゲートウェイアタッチメントを作成する

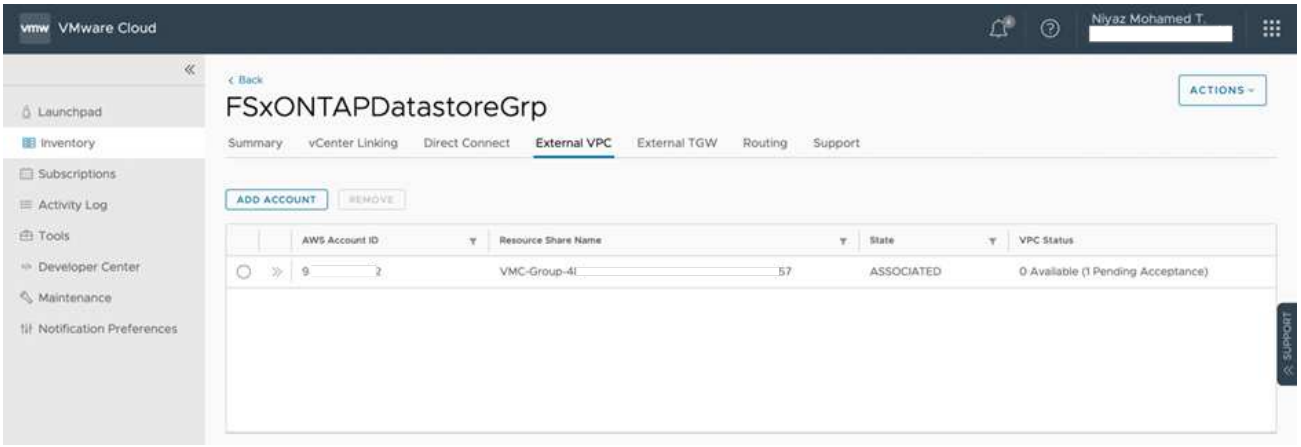
1. AWS コンソールで、VPC サービスページに移動し、FSx ファイルシステムのプロビジョニングに使用された VPC に移動します。ここでは、右側のナビゲーション ペインで **Transit Gateway Attachment** をクリックして、トランジット ゲートウェイ アタッチメントを作成します。
2. **VPC** アタッチメント で、DNS サポートがチェックされていることを確認し、FSx ONTAPがデプロイされている VPC を選択します。

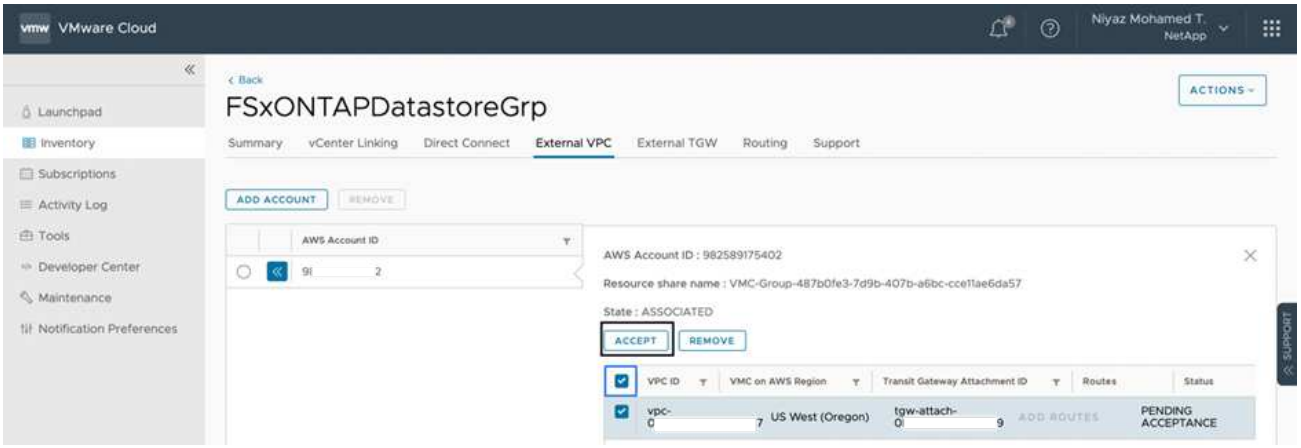


3. *トランジット ゲートウェイ アタッチメントの作成*をクリックします。



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

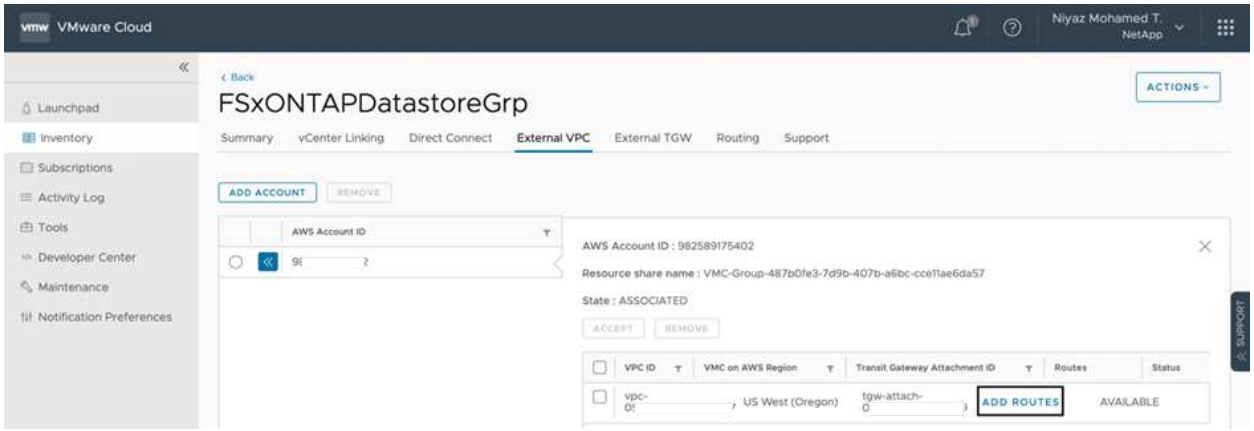


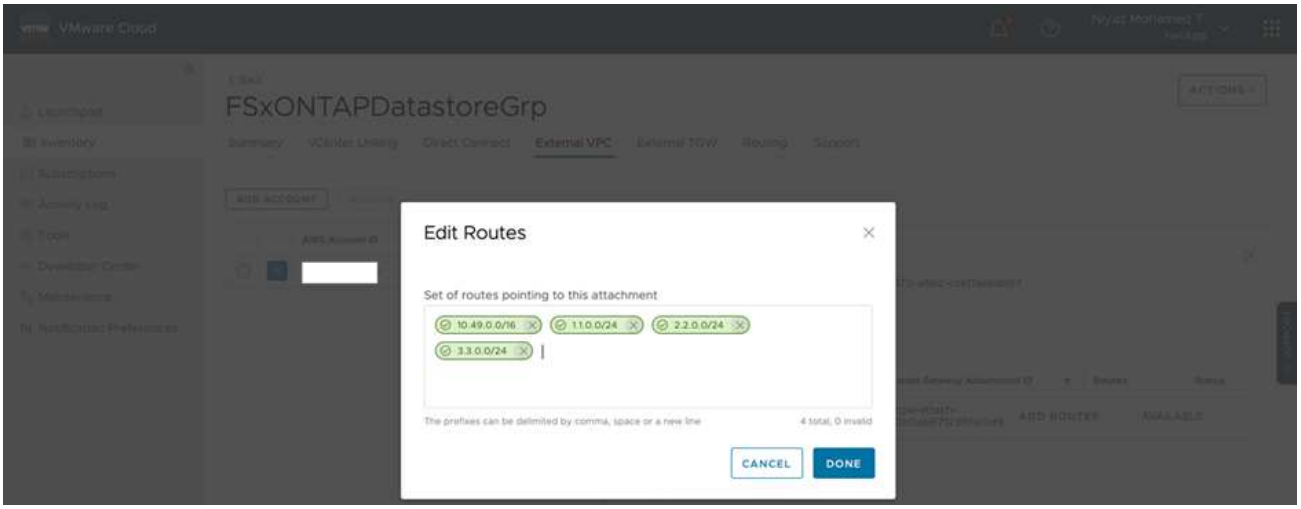


このオプションが表示されるまで数分かかる場合があります。

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

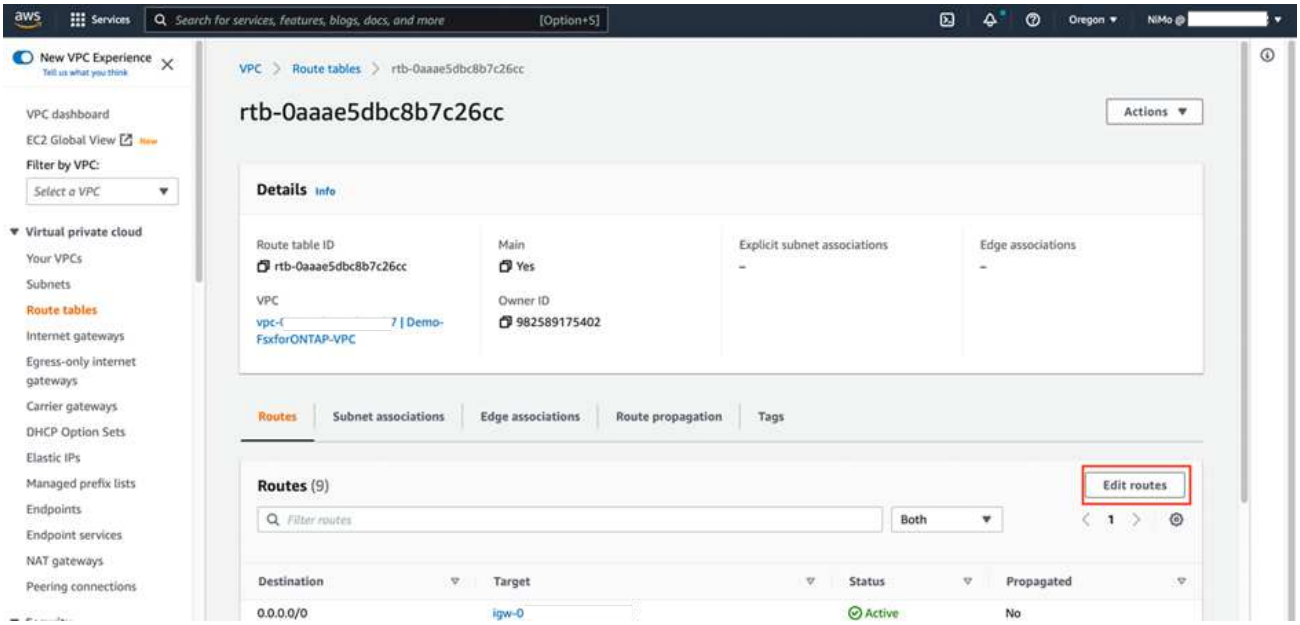
   - Amazon FSx ONTAPフローティング IP のフローティング IP 範囲のルート。
   - 新しく作成された外部 VPC アドレス空間へのルート。



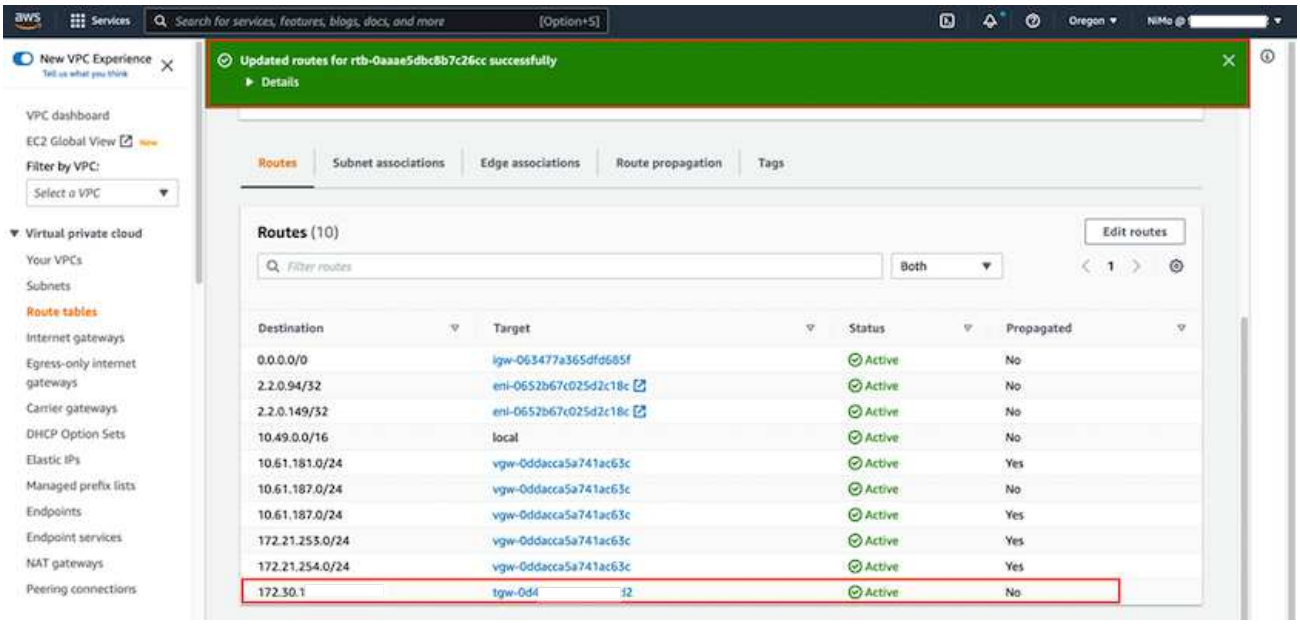


▼ ステップ**5:** ルーティング（**AWS VPC**と**SDDC**）とセキュリティグループを構成する

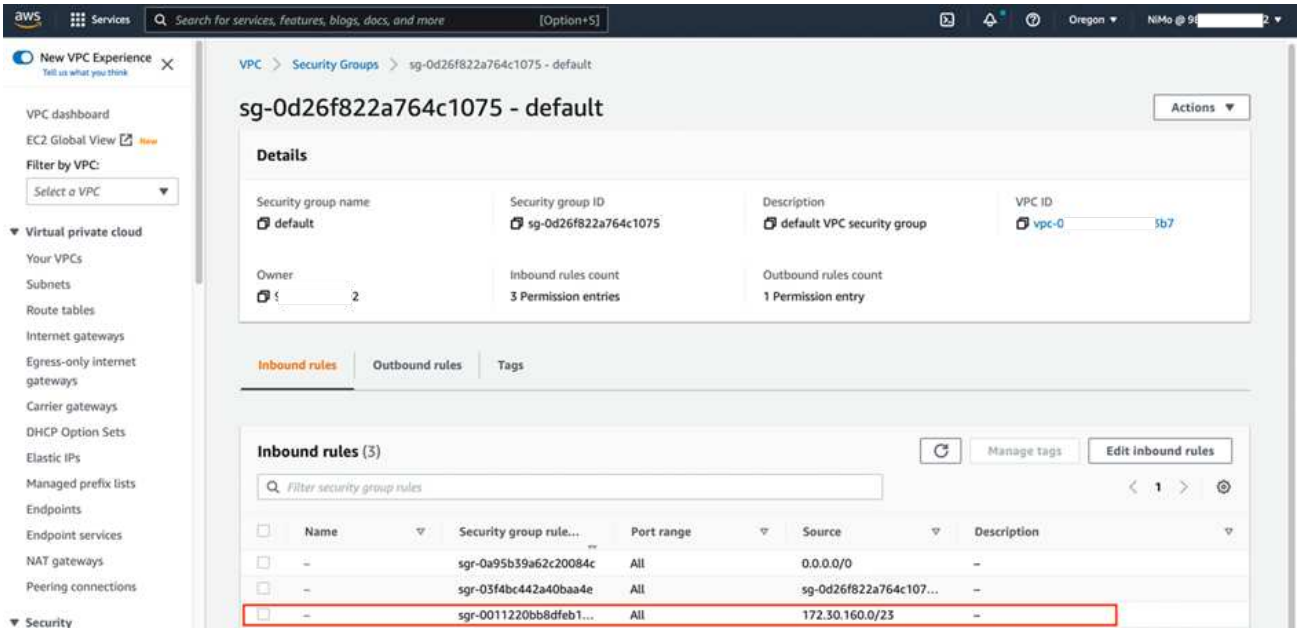
1. AWS コンソールで、VPC サービス ページで VPC を見つけて、VPC の メイン ルート テーブルを選択し、SDDC に戻るルートを作成します。
2. 下部のパネルでルート テーブルを参照し、[ルートの編集] をクリックします。



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



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



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

NFS トラフィックを受け入れるようにセキュリティ グループを更新します。

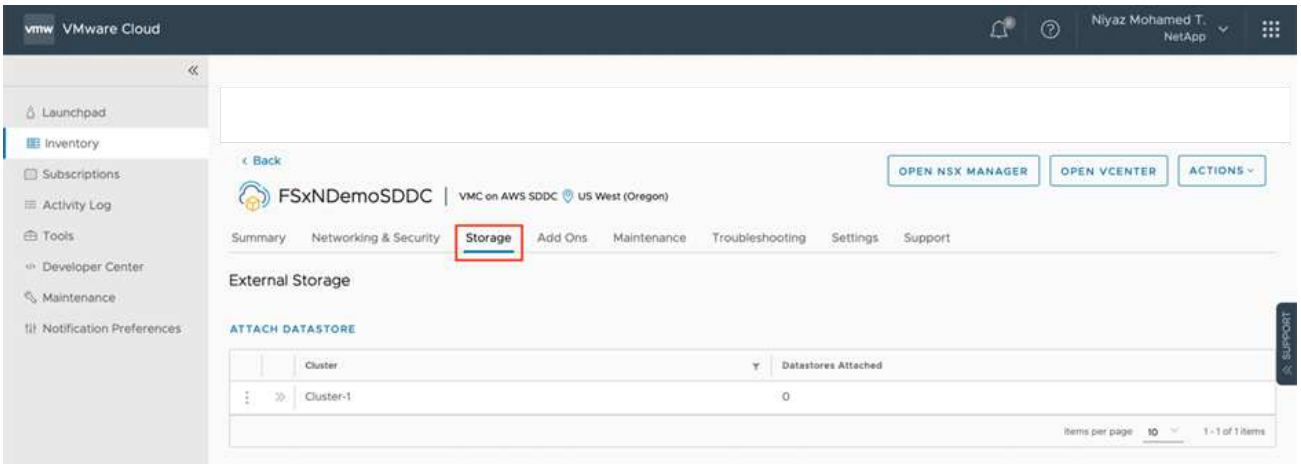
これは、適切な SDDC への接続を準備するための最後の手順です。ファイル システムを構成し、ルートを追加し、セキュリティ グループを更新したら、データストアをマウントします。

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

ファイル システムがプロビジョニングされ、接続が確立されたら、VMware Cloud Console にアクセスし

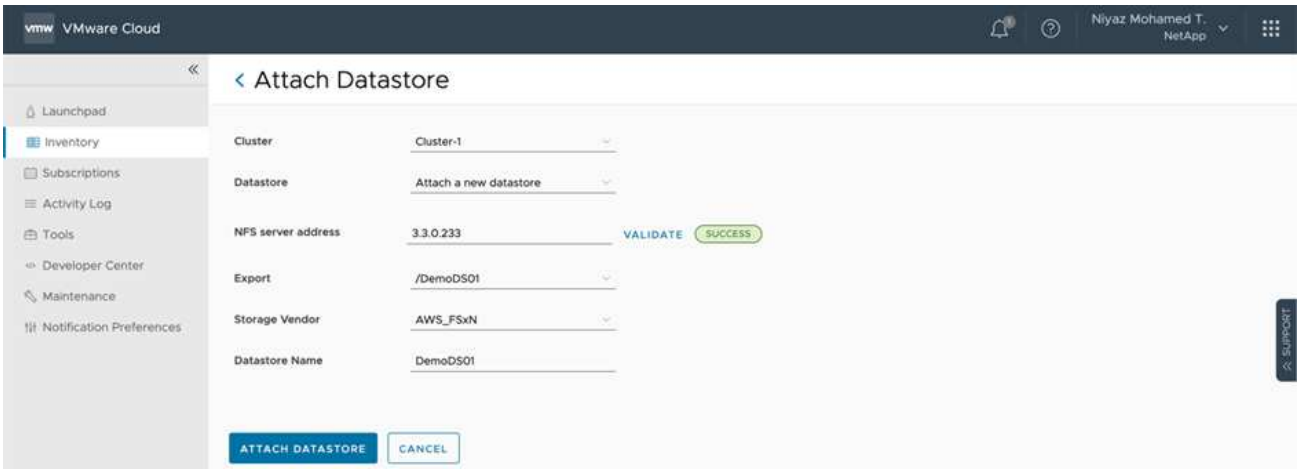
て NFS データストアをマウントします。

1. VMC コンソールで、SDDC の ストレージ タブを開きます。

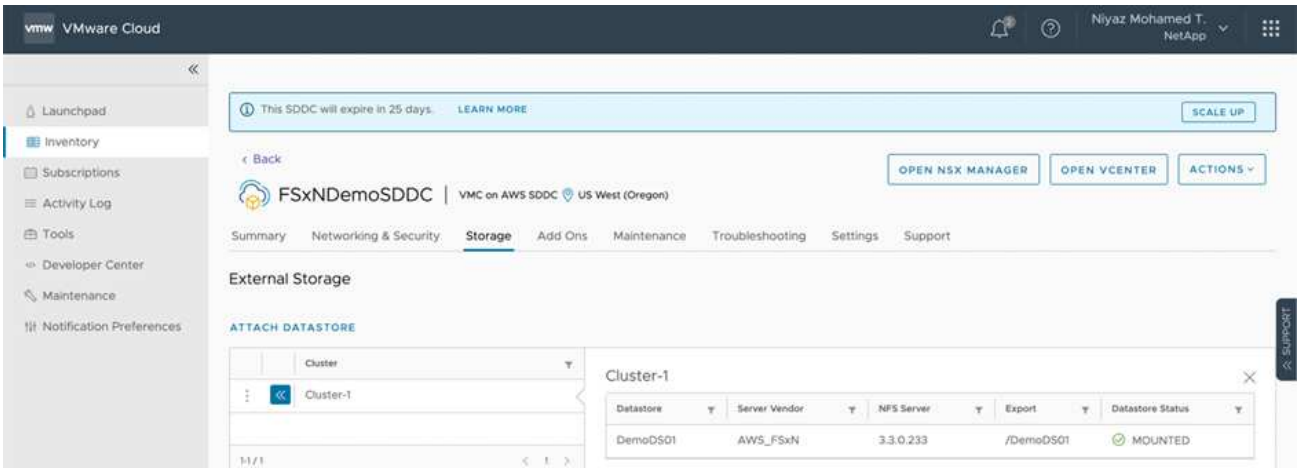


2. **ATTACH DATASTORE** をクリックし、必要な値を入力します。

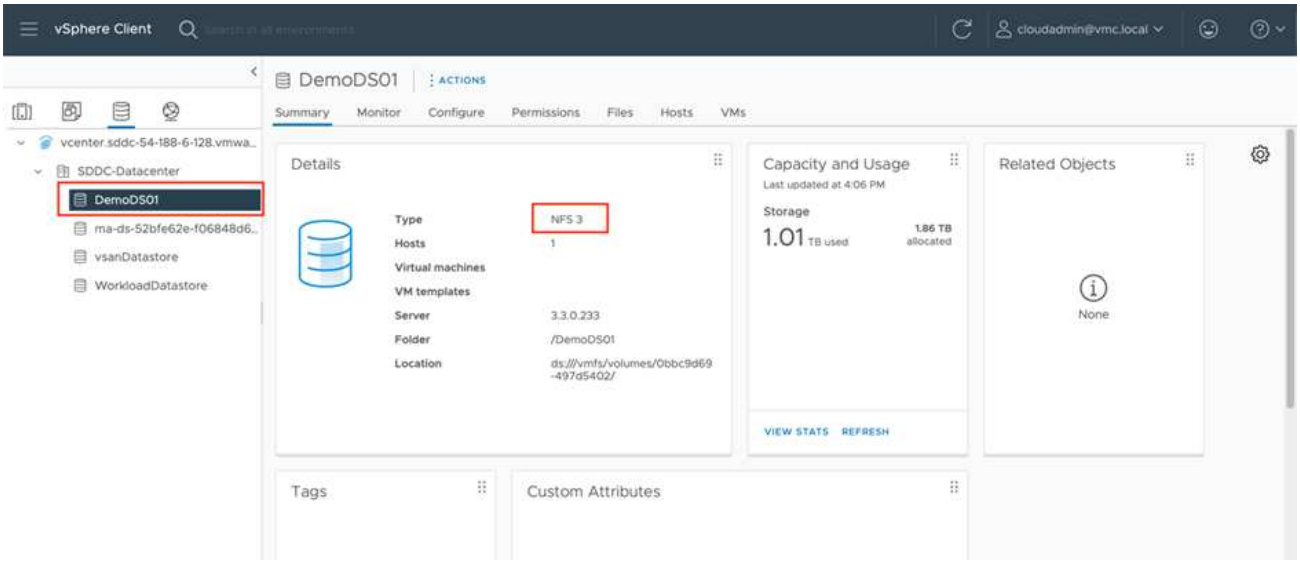
NFS サーバー アドレスは、AWS コンソール内の FSx > ストレージ仮想マシン タブ > エンドポイントで確認できる NFS IP アドレスです。



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



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



AWS 向け**NetApp**ゲスト接続ストレージ オプション

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

FSx ONTAP

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

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

FSx ONTAPを使用すると、ボタンをクリックするだけでファイルのスナップショット、クローン、複製ができるため、データの管理が簡単になります。さらに、FSx ONTAP はデータを低コストで弾力性のあるストレージに自動的に階層化するため、容量のプロビジョニングや管理の必要性が軽減されます。

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

ゲスト接続ストレージとしての **FSx ONTAP**

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

Amazon FSx ONTAPファイル共有と LUN は、VMware Cloud at AWS の VMware SDDC 環境内で作成された VM からマウントできます。ボリュームは Linux クライアントにマウントし、NFS または SMB プロトコルを使用して Windows クライアントにマップすることもできます。また、iSCSI 経由でマウントすると、LUN は Linux または Windows クライアント上でブロック デバイスとしてアクセスできます。 NetApp

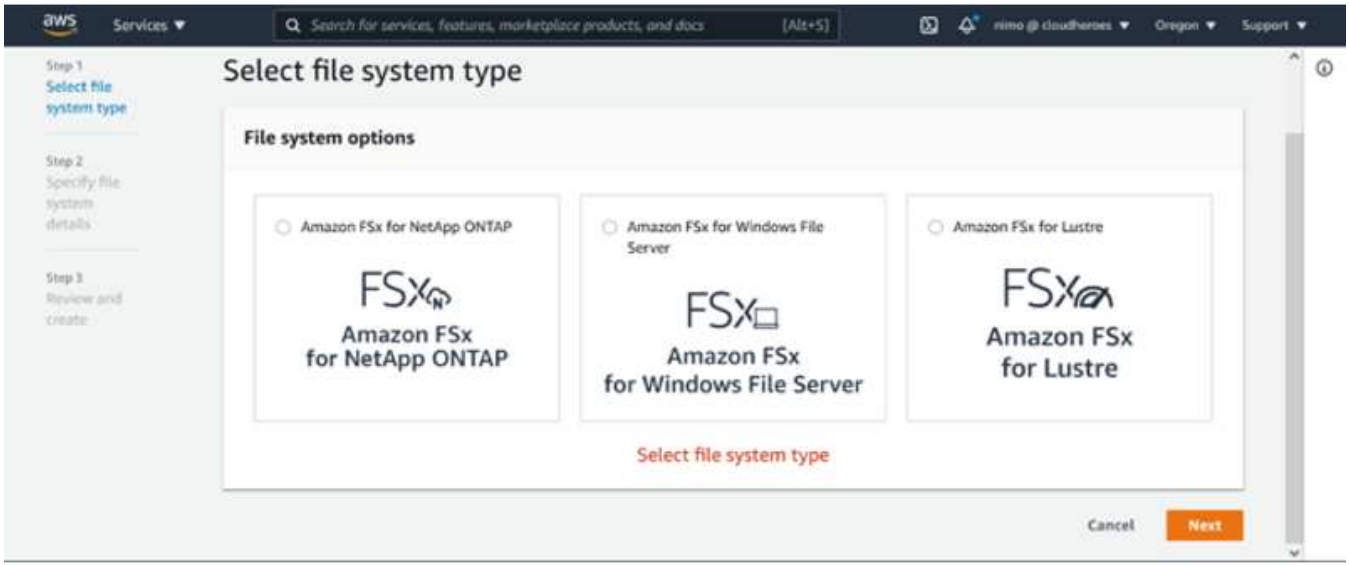
ONTAPファイルシステム用のAmazon FSx は、次の手順で簡単にセットアップできます。

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

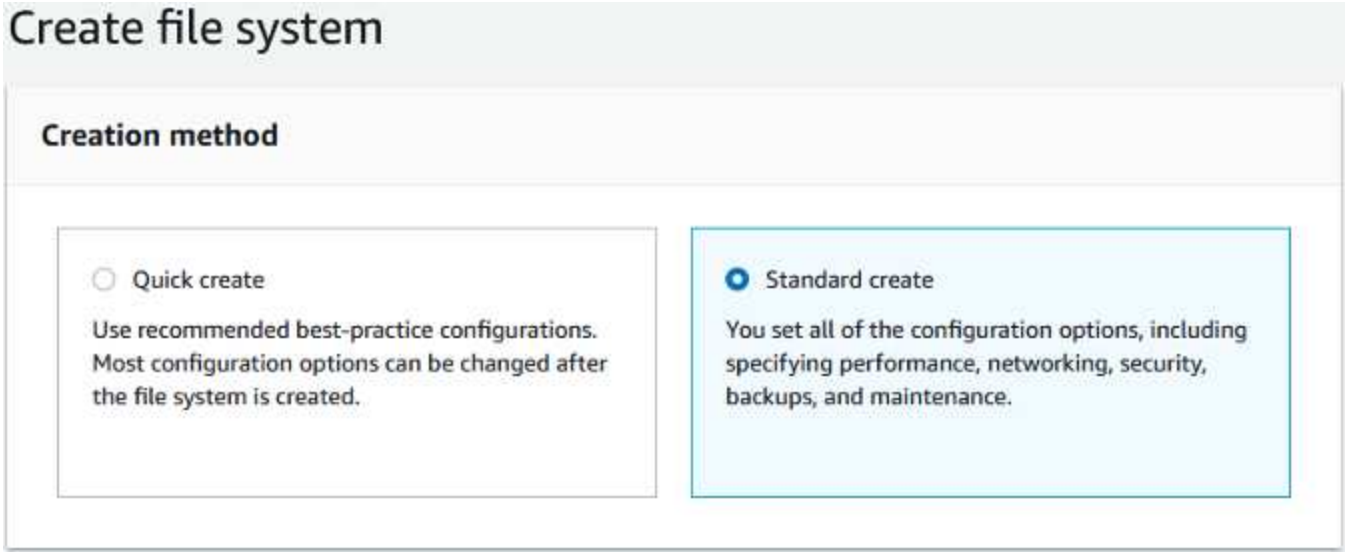
▼ **Amazon FSx ONTAP**ボリュームの作成とマウント

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

1. 開く"Amazon FSxコンソール"[ファイル システムの作成] を選択して、ファイル システム作成ウィザードを起動します。
2. [ファイルシステムタイプの選択] ページで、 [Amazon FSx ONTAP]を選択し、[次へ] を選択します。 「ファイル システムの作成」ページが表示されます。

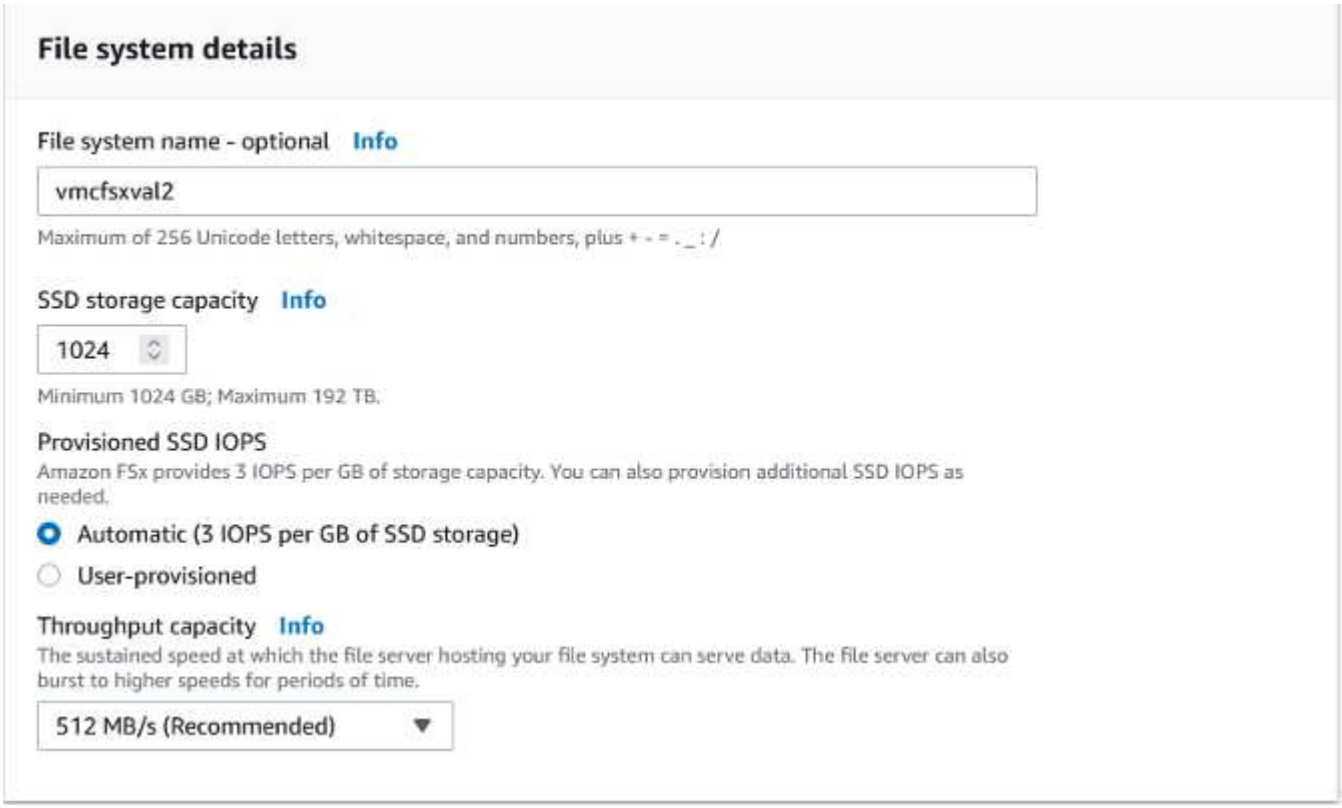


1. [ネットワーク] セクションの [仮想プライベート クラウド (VPC)] で、適切な VPC と優先サブネット、およびルート テーブルを選択します。この場合、ドロップダウンから vmcfsx2.vpc が選択されます。

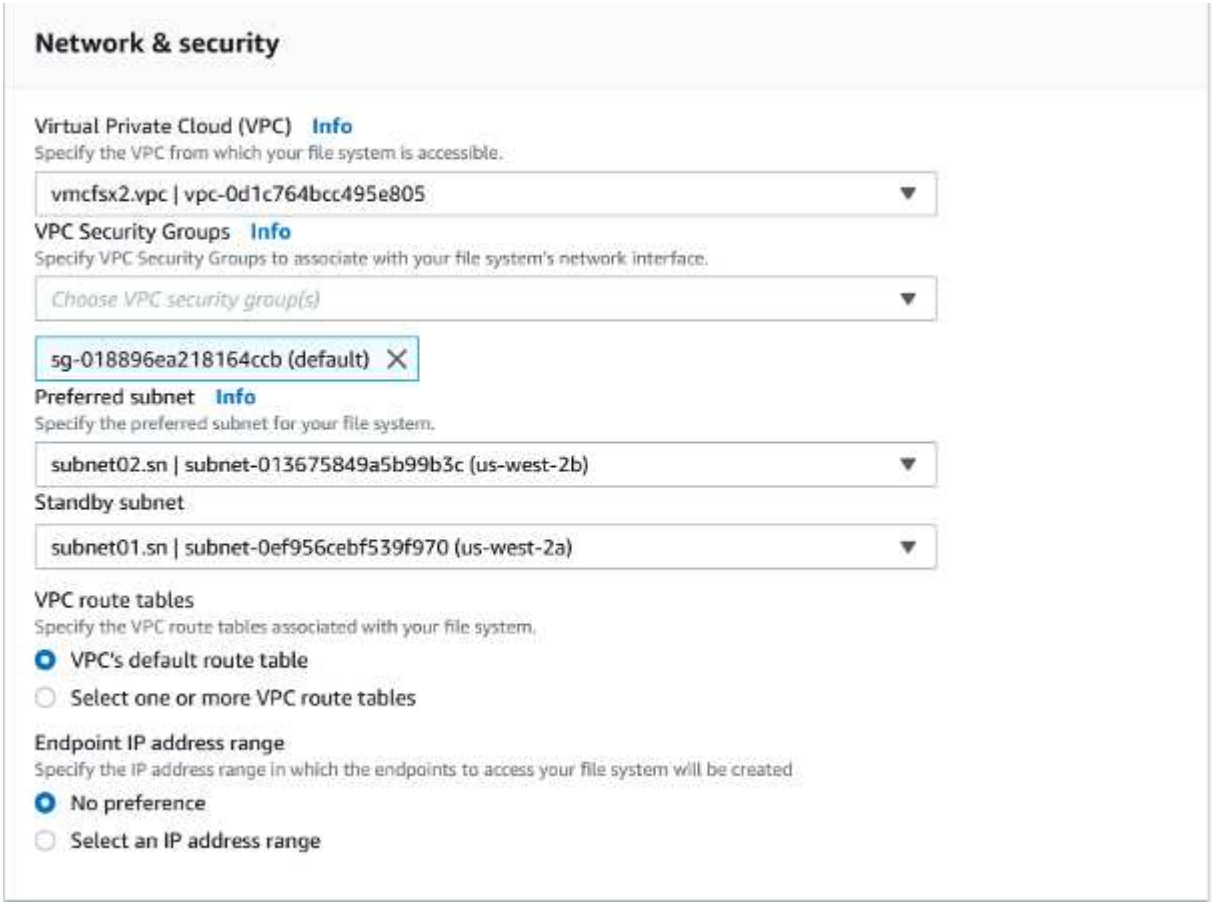


1. 作成方法として、「標準作成」を選択します。クイック作成を選択することもできますが、このドキュ

メントでは標準作成オプションを使用します。

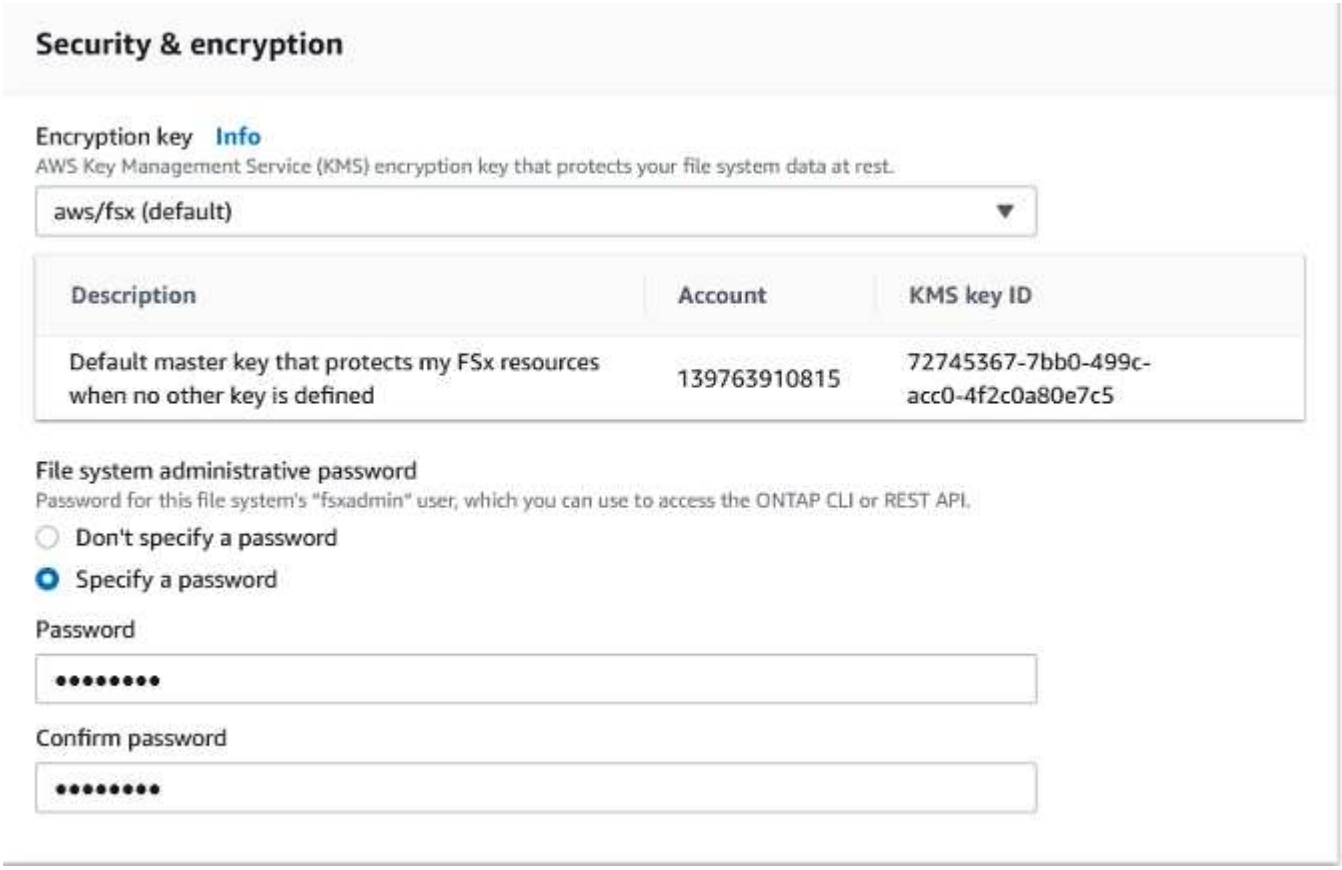


1. [ネットワーク] セクションの [仮想プライベート クラウド (VPC)] で、適切な VPC と優先サブネット、およびルート テーブルを選択します。この場合、ドロップダウンから vmcfsx2.vpc が選択されます。

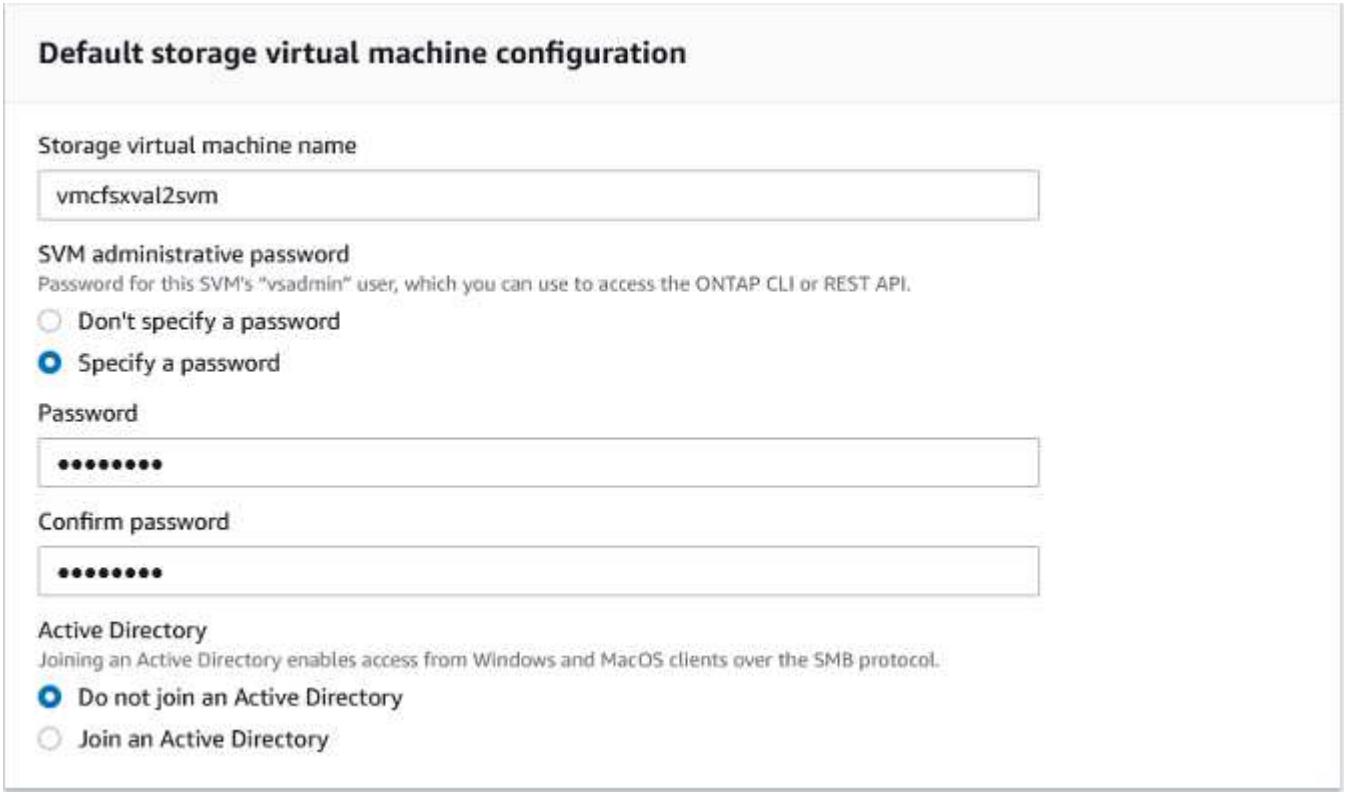


[ネットワーク] セクションの [仮想プライベート クラウド (VPC)] で、適切な VPC と優先サブネット、およびルート テーブルを選択します。この場合、ドロップダウンから vmcfsx2.vpc が選択されます。

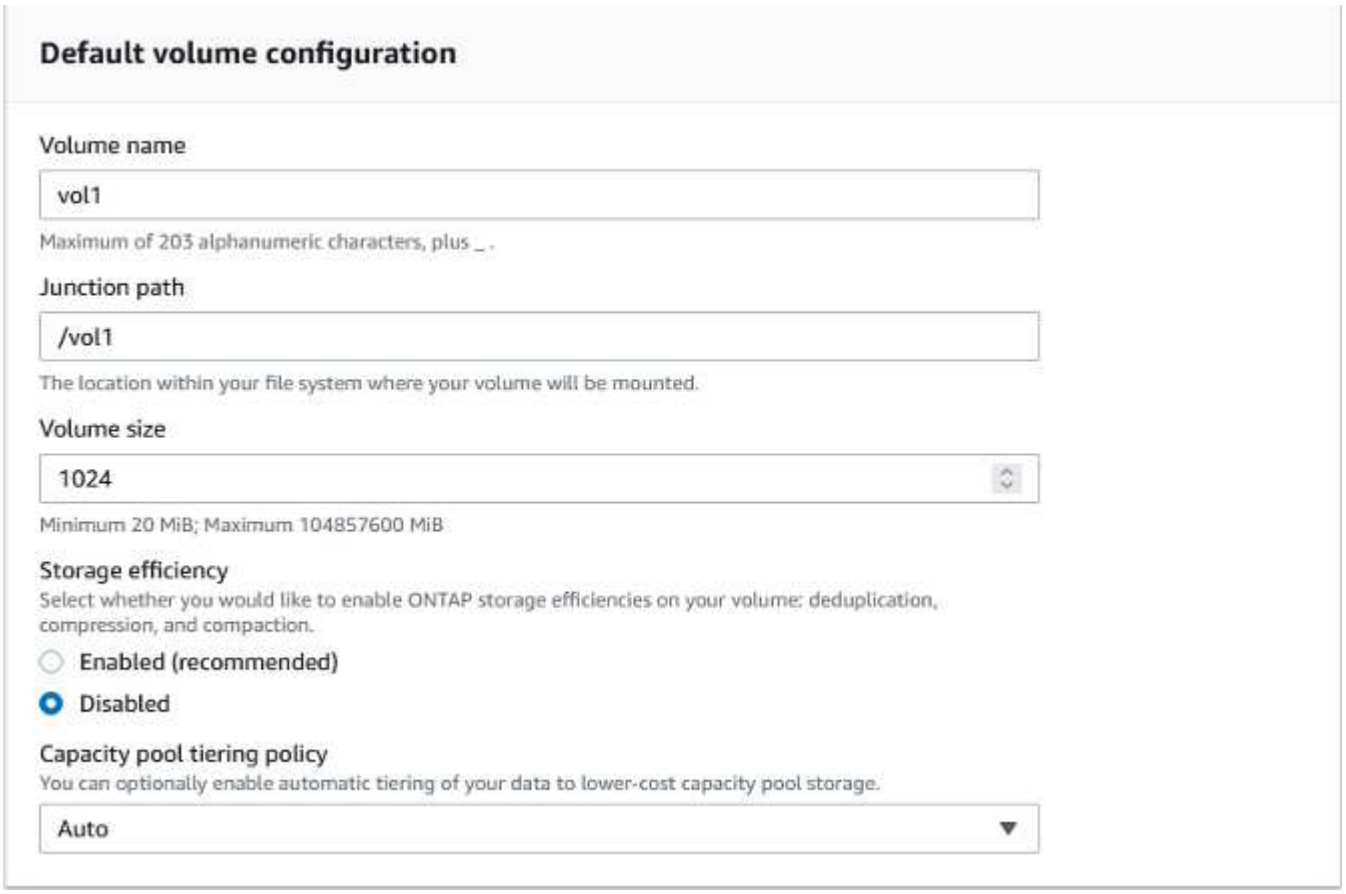
1. [セキュリティと暗号化] セクションの [暗号化キー] で、保存中のファイルシステムのデータを保護する AWS Key Management Service (AWS KMS) 暗号化キーを選択します。ファイル システム管理パスワードには、fsxadmin ユーザーの安全なパスワードを入力します。



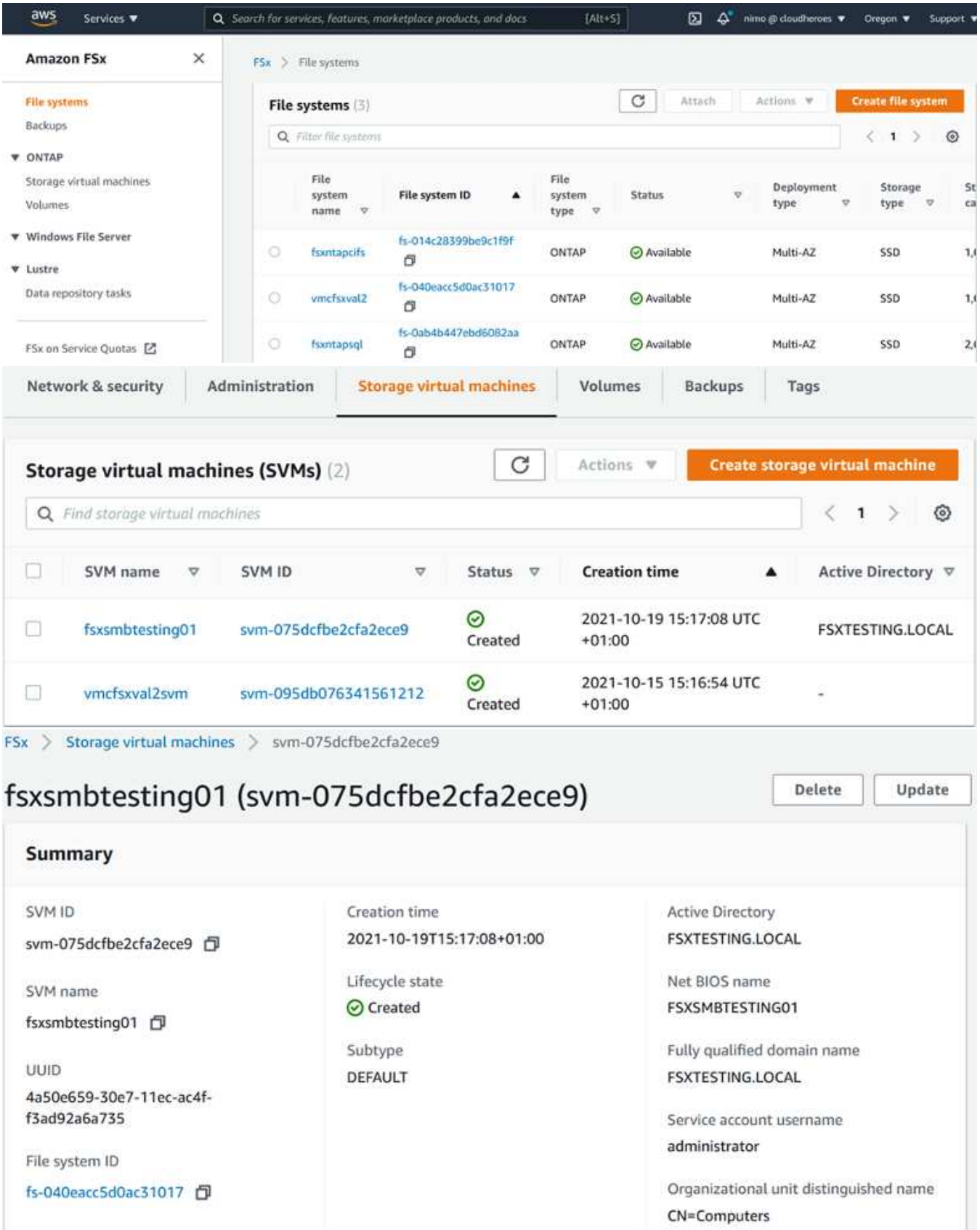
1. 仮想マシンで、REST API または CLI を使用してONTAP を管理するために vsadmin で使用するパスワードを指定します。パスワードを指定しない場合は、fsxadmin ユーザーを使用して SVM を管理できます。 Active Directory セクションで、SMB 共有をプロビジョニングするために Active Directory を SVM に参加させていることを確認します。 [既定のストレージ仮想マシン構成] セクションで、この検証のストレージの名前を指定します。SMB 共有は、自己管理型 Active Directory ドメインを使用してプロビジョニングされます。



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



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

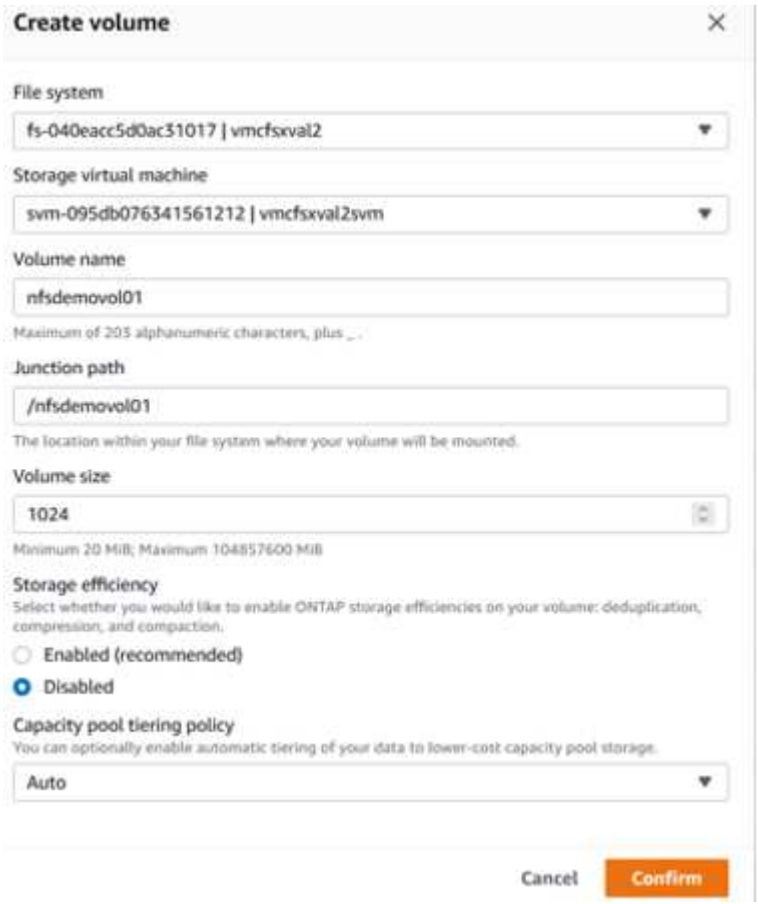


詳しい情報については、"Amazon FSx ONTAPを使い始める" 。

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

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

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



▼ **Linux**クライアントに**FSx ONTAP**ボリュームをマウントする

前の手順で作成した FSx ONTAPボリュームを VMC on AWS SDDC 内の Linux VM からマウントするには、次の手順を実行します。

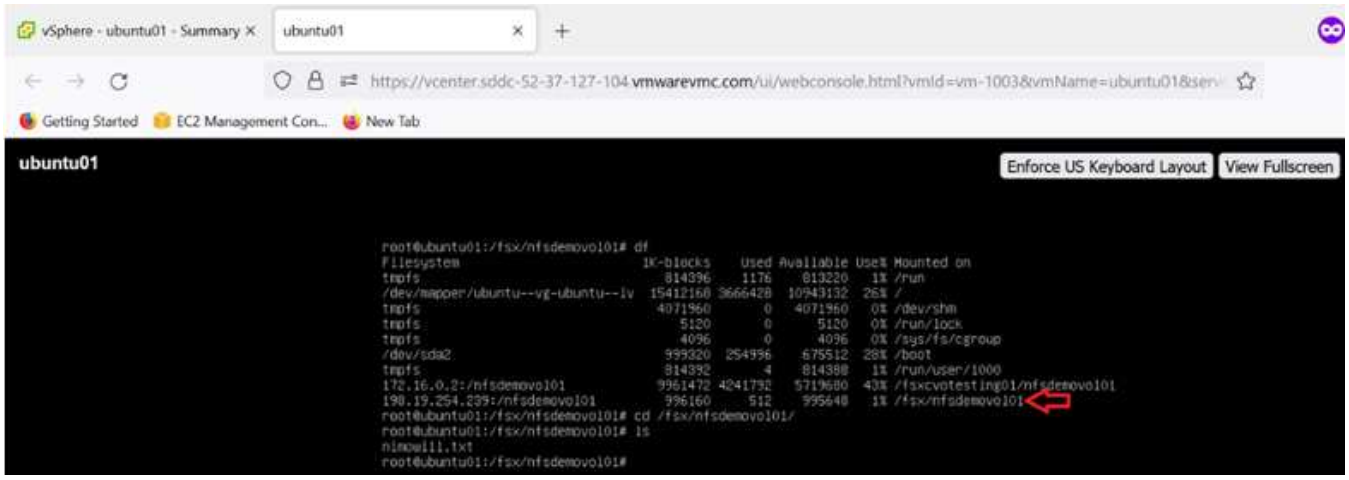
1. 指定された Linux インスタンスに接続します。
2. Secure Shell (SSH) を使用してインスタンス上でターミナルを開き、適切な資格情報でログインします。
3. 次のコマンドを使用して、ボリュームのマウント ポイントのディレクトリを作成します。

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

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

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

1. 実行したら、df コマンドを実行してマウントを検証します。



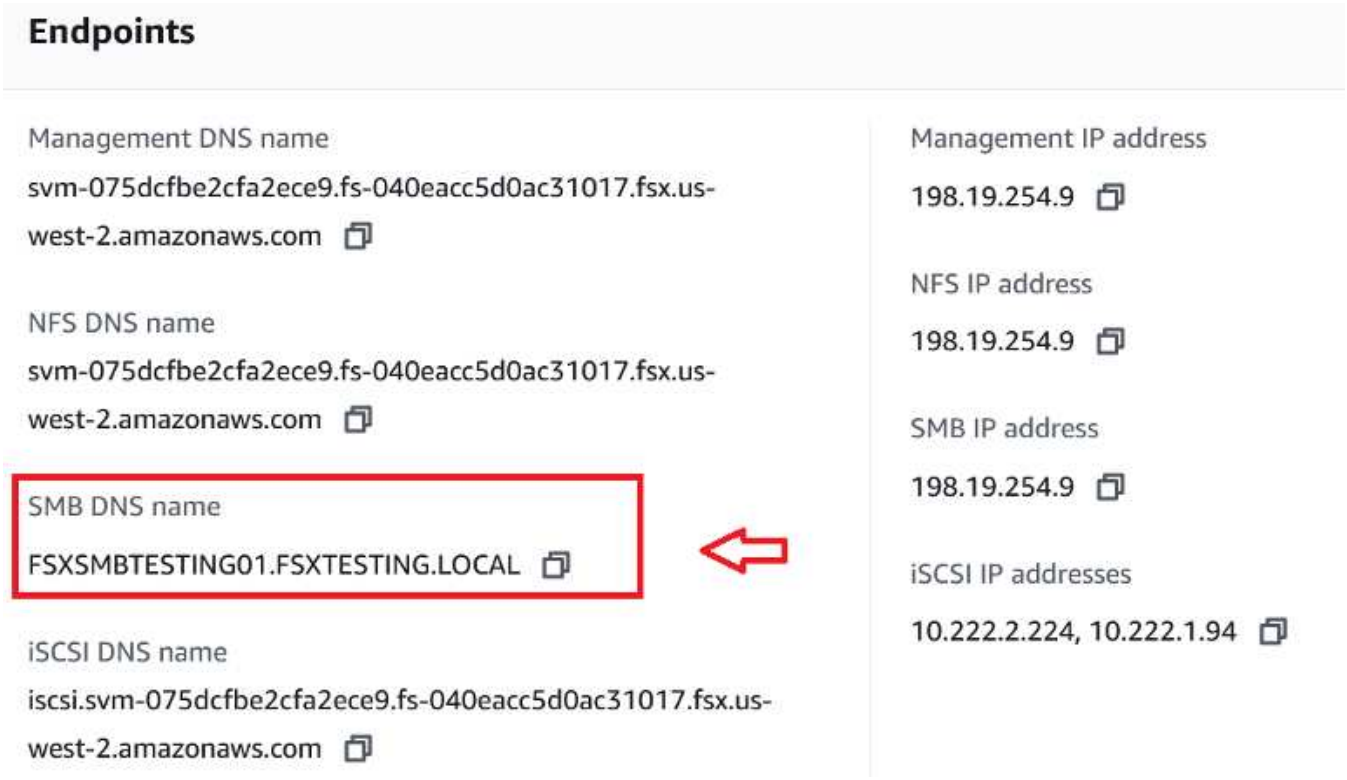
LinuxクライアントにFSx ONTAPボリュームをマウントする

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

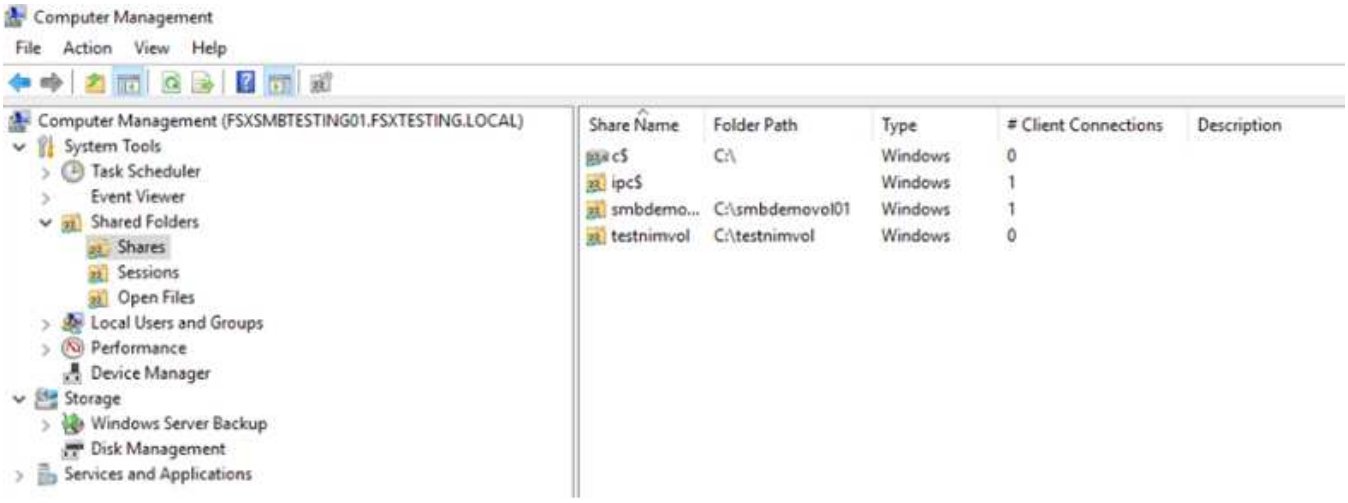
Amazon FSxファイルシステム上のファイル共有を管理およびマップするには、共有フォルダ GUI を使用する必要があります。

1. [スタート] メニューを開き、[管理者として実行] を使用して fsmgmt.msc を実行します。これを行うと、共有フォルダー GUI ツールが開きます。
2. [アクション] > [すべてのタスク] をクリックし、[別のコンピューターに接続] を選択します。
3. 別のコンピュータの場合は、ストレージ仮想マシン (SVM) の DNS 名を入力します。たとえば、この例では FSXSMBTESTING01.FSXTESTING.LOCAL が使用されています。

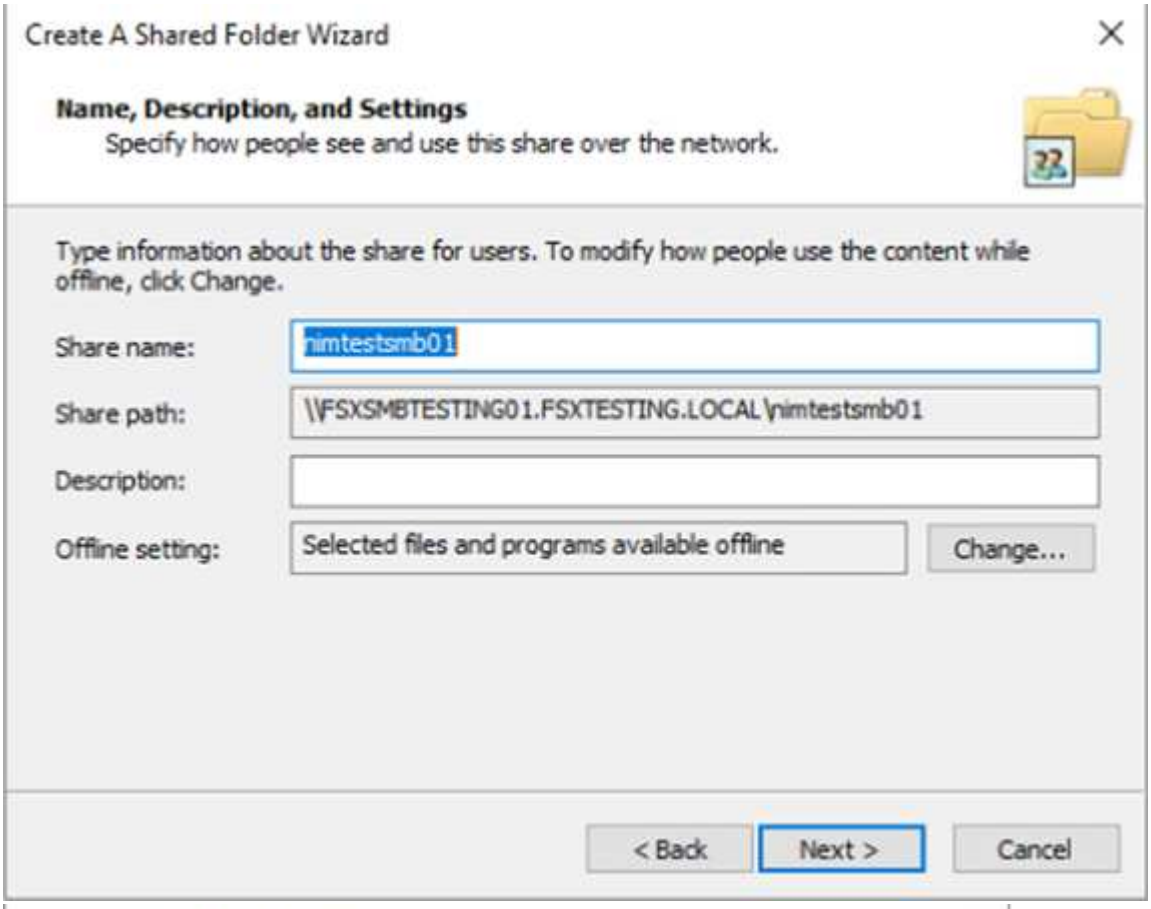
Amazon FSxコンソールで SVM の DNS 名を見つけ、[Storage Virtual Machines] を選択し、[SVM] を選択してから、[エンドポイント] まで下にスクロールして SMB DNS 名を見つけます。[OK]をクリックします。 Amazon FSxファイルシステムが共有フォルダのリストに表示されます。



1. 共有フォルダツールで、左側のペインの [共有] を選択して、 Amazon FSxファイルシステムのアクティブな共有を表示します。



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

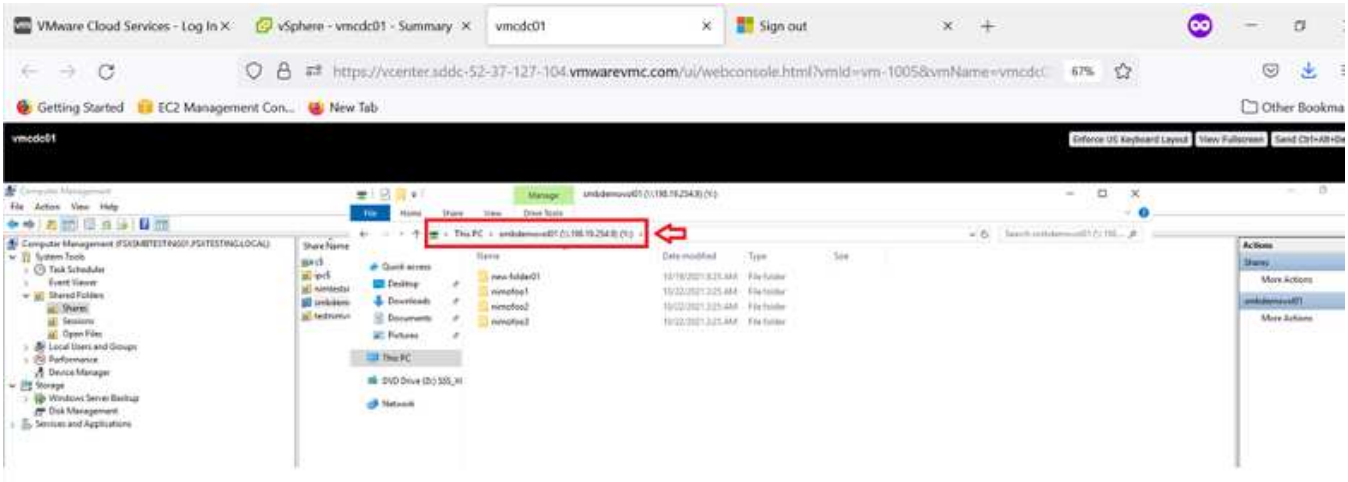




Amazon FSxファイルシステムでのSMB共有の作成と管理の詳細については、以下を参照してください。"SMB共有の作成" 。

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

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



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

iSCSI を使用して FSx ONTAP LUN をホストに接続する

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

Linux クライアントでは、iSCSI デーモンが実行されていることを確認します。 LUN がプロビジョニングされたら、Ubuntu での iSCSI 構成に関する詳細なガイダンスを参照してください (例として)"ここをクリックしてください。" 。

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

▼ **FSx ONTAP**で **LUN** をプロビジョニングします。

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

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

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

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

```
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 にマップします。

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

FsxId040eacc5d0ac31017::> lun show

Vserver   Path                            State   Mapped   Type
Size

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

vmcfsxval2svm

          /vol/blocktest01/lun01          online  mapped   linux
5GB

vmcfsxval2svm

          /vol/nimfsxscsivol/nimofsxlun01 online  mapped   windows
5GB
```

2つのエントリが表示されました。

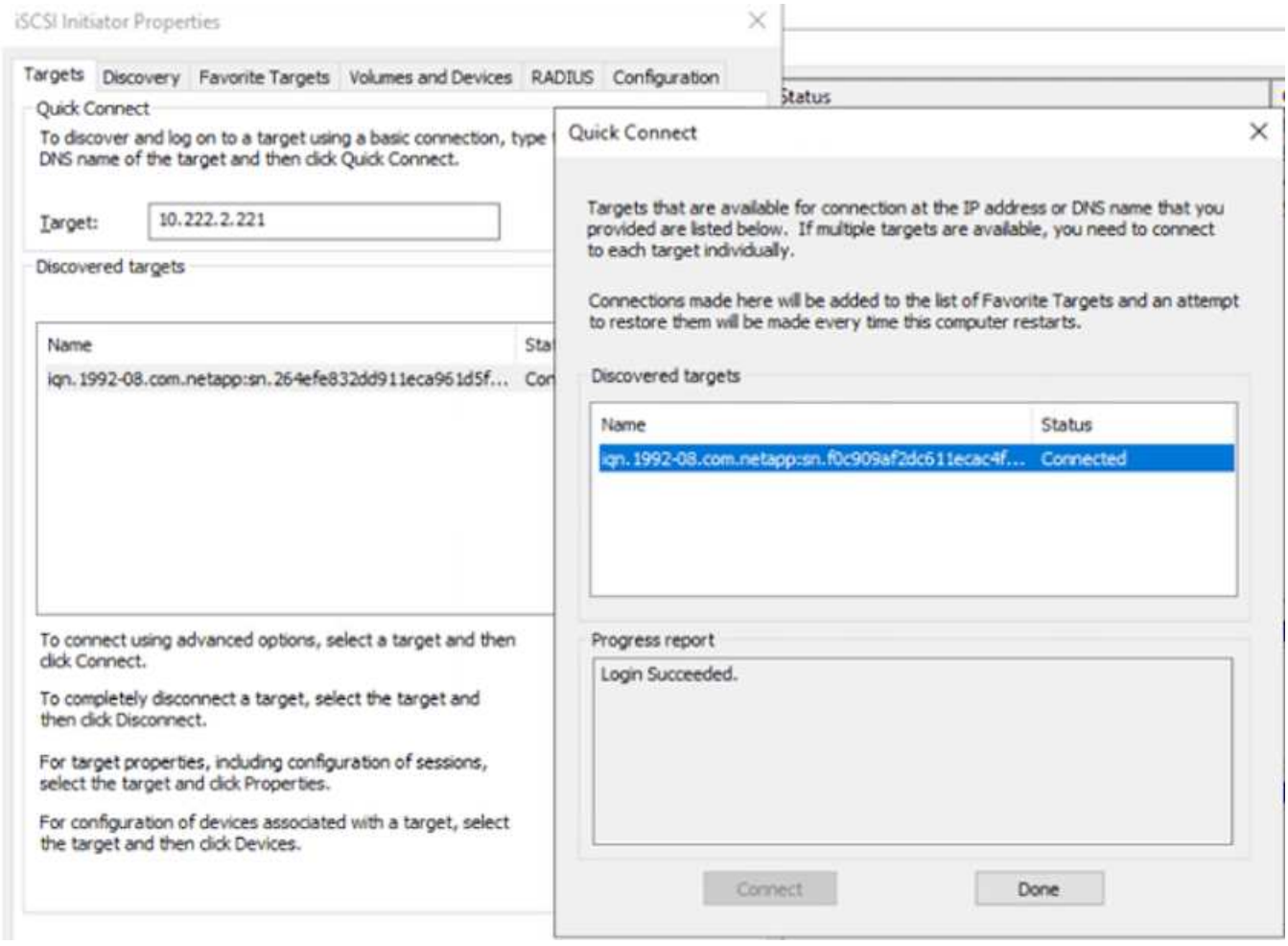
1. 新しくプロビジョニングされた LUN を Windows VM に接続します。

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

します。

1. VMware Cloud on AWS SDDC でホストされている Windows VM に RDP 接続します。
2. サーバー マネージャー > ダッシュボード > ツール > iSCSI イニシエーター に移動して、iSCSI イニシエーターのプロパティ ダイアログ ボックスを開きます。
3. [検出] タブで、[ポータルの検出] または [ポータルの追加] をクリックし、iSCSI ターゲット ポートの IP アドレスを入力します。
4. [ターゲット] タブで、検出されたターゲットを選択し、[ログオン] または [接続] をクリックします。
5. 「マルチパスを有効にする」を選択し、「コンピュータの起動時にこの接続を自動的に復元する」または「この接続をお気に入りのターゲットのリストに追加する」を選択します。[Advanced]をクリックします。

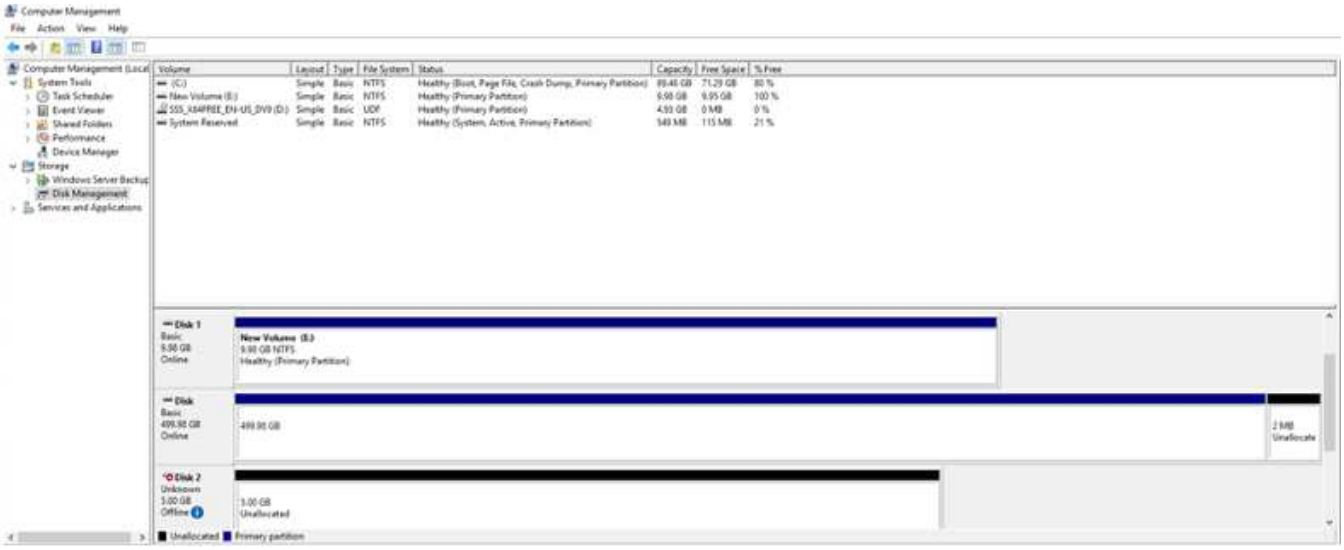
Windowsホストには、クラスタ内のそれぞれのノードへのiSCSI接続が必要です。標準のDSMによって最適なパスが選択され、



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

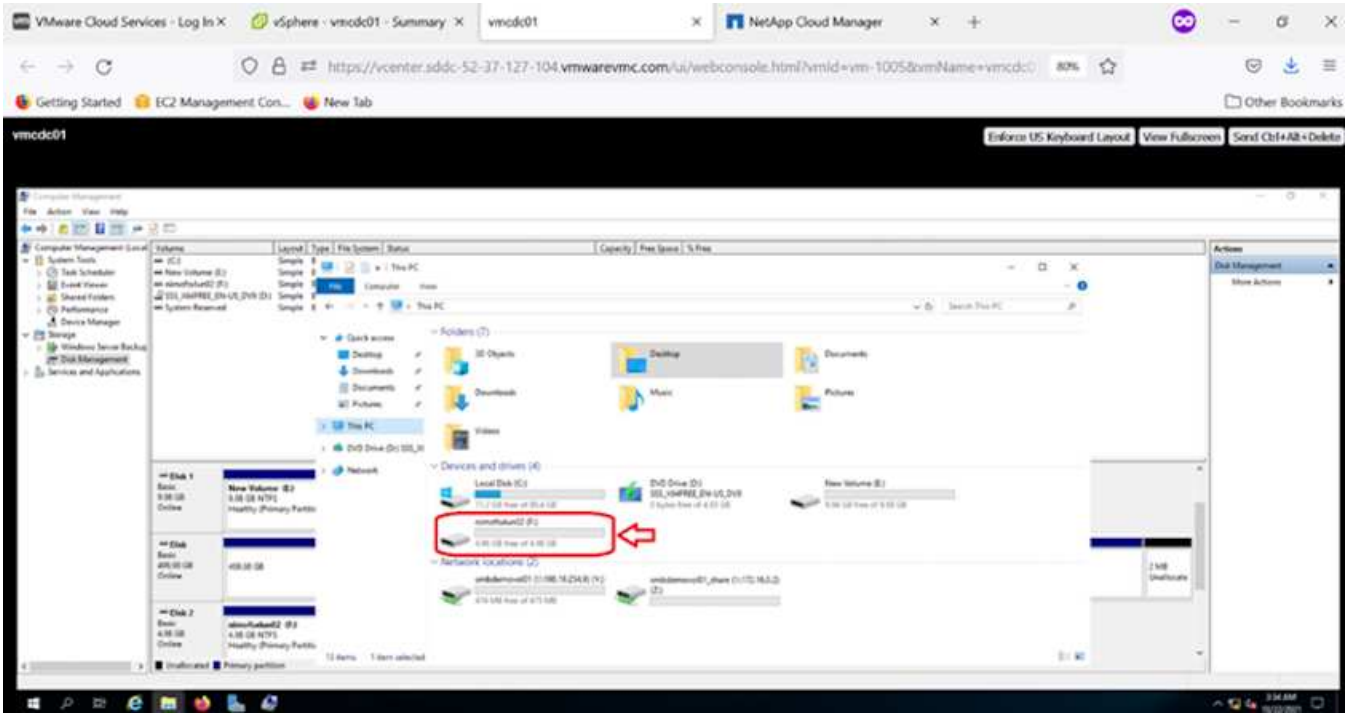
1. Windows のコンピューターの管理ユーティリティを開きます (スタート > 管理ツール > コンピューターの管理)。

2. ナビゲーション ツリーでストレージ ノードを展開します。
3. ディスクの管理をクリックします。
4. [アクション] > [ディスクの再スキャン] をクリックします。



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

1. Windowsの[ディスクの管理]を起動します。
2. LUNを右クリックし、必要なディスクまたはパーティションの種類を選択します。
3. ウィザードの指示に従います。この例では、ドライブ F: がマウントされます。



Cloud Volumes ONTAP（CVO）

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

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

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

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

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

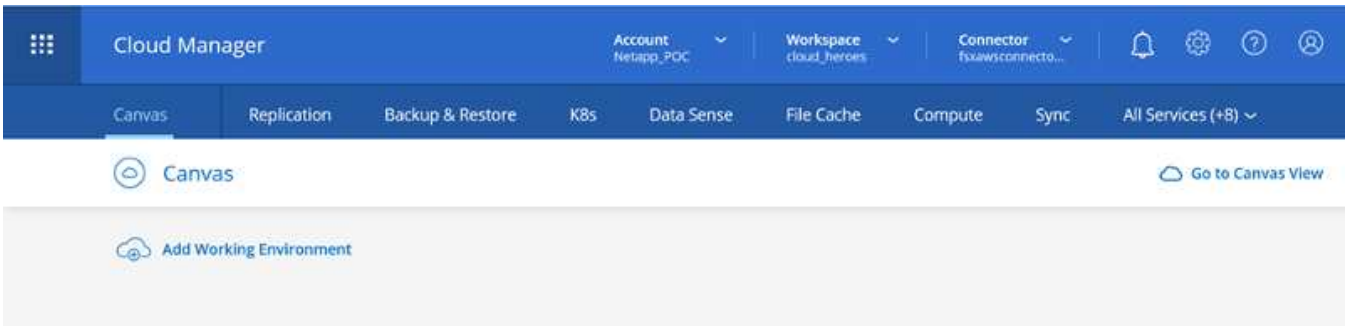
▼ **AWS** に新しい**Cloud Volumes ONTAP**インスタンスをデプロイする **(**自分で行う**)**

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

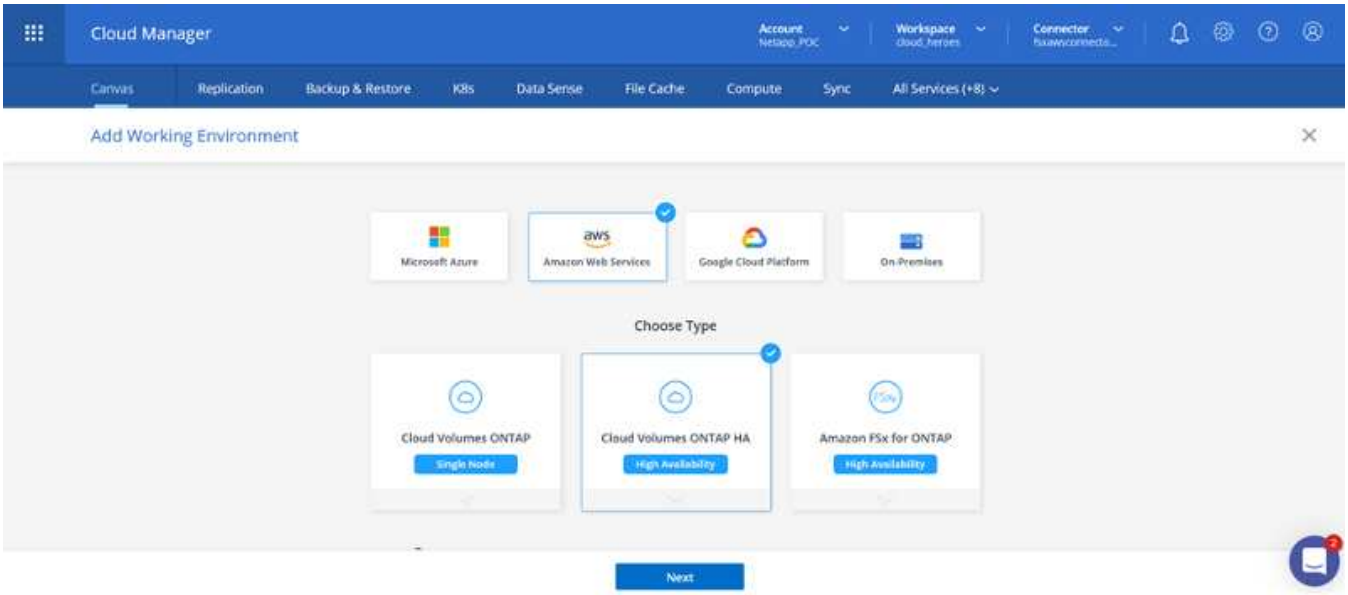
災害復旧または移行の目的でオンプレミス環境からクラウドにボリュームを複製するには、サイト間 VPN または DirectConnect を使用して AWS へのネットワーク接続を確立します。オンプレミスからCloud Volumes ONTAPへのデータの複製については、このドキュメントの範囲外です。オンプレミスとCloud Volumes ONTAPシステム間でデータを複製するには、"システム間のデータ複製の設定" 。

"Cloud Volumes ONTAPサイザー"を使用して、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サイザーの入力として使用します。

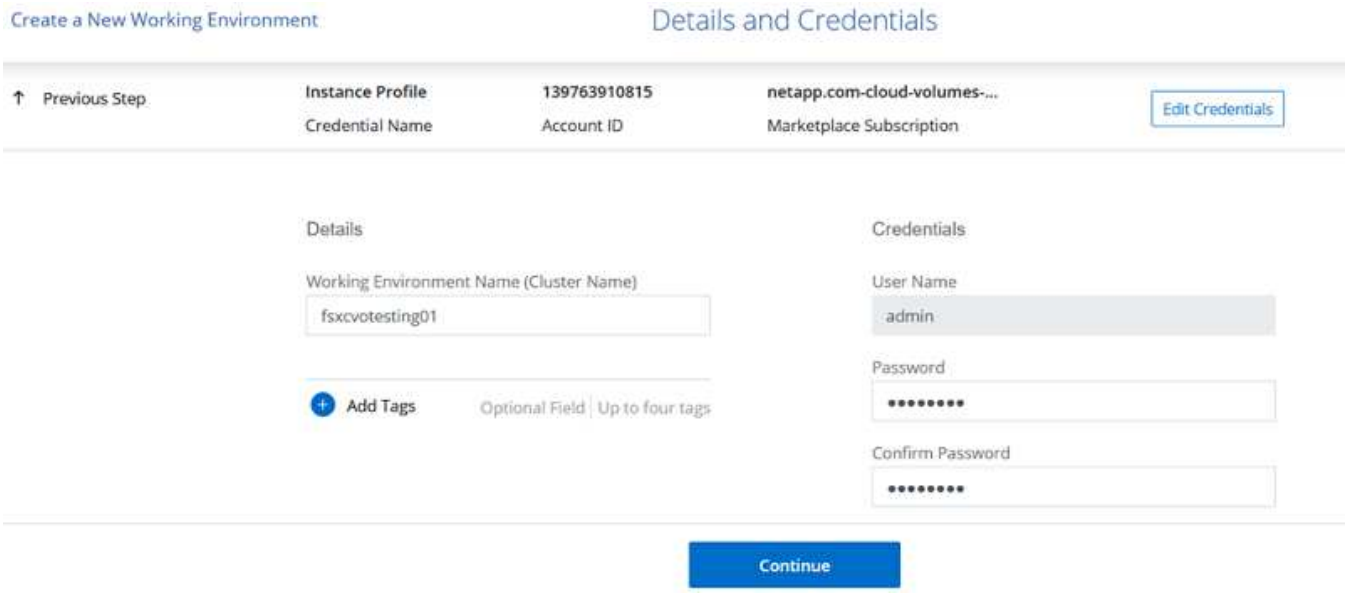
1. NetApp Cloud Central にログインすると、Fabric View 画面が表示されます。 Cloud Volumes ONTAPタブを見つけて、「Go to Cloud Manager」を選択します。ログインすると、Canvas 画面が表示されます。



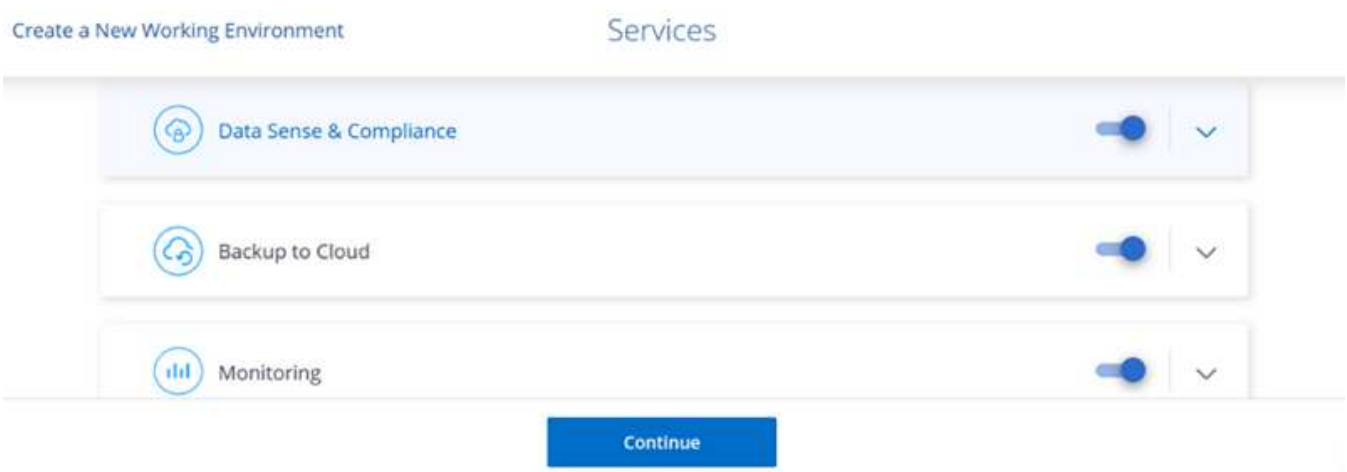
1. Cloud Manager のホームページで、「作業環境の追加」をクリックし、クラウドとして AWS を選択し、システム構成のタイプを選択します。



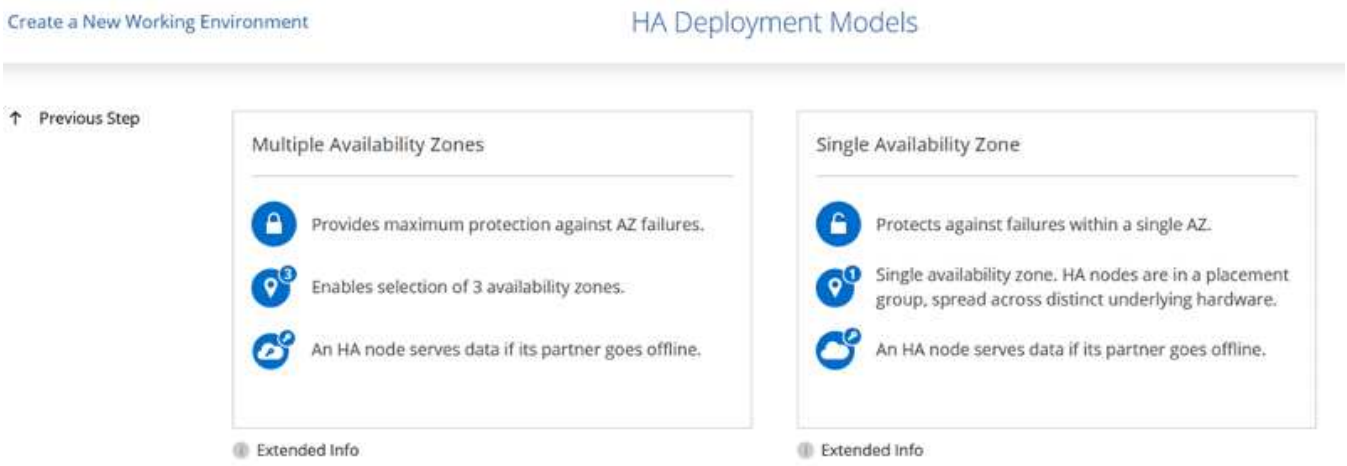
1. 環境名や管理者の資格情報など、作成する環境の詳細を指定します。[Continue]をクリックします。



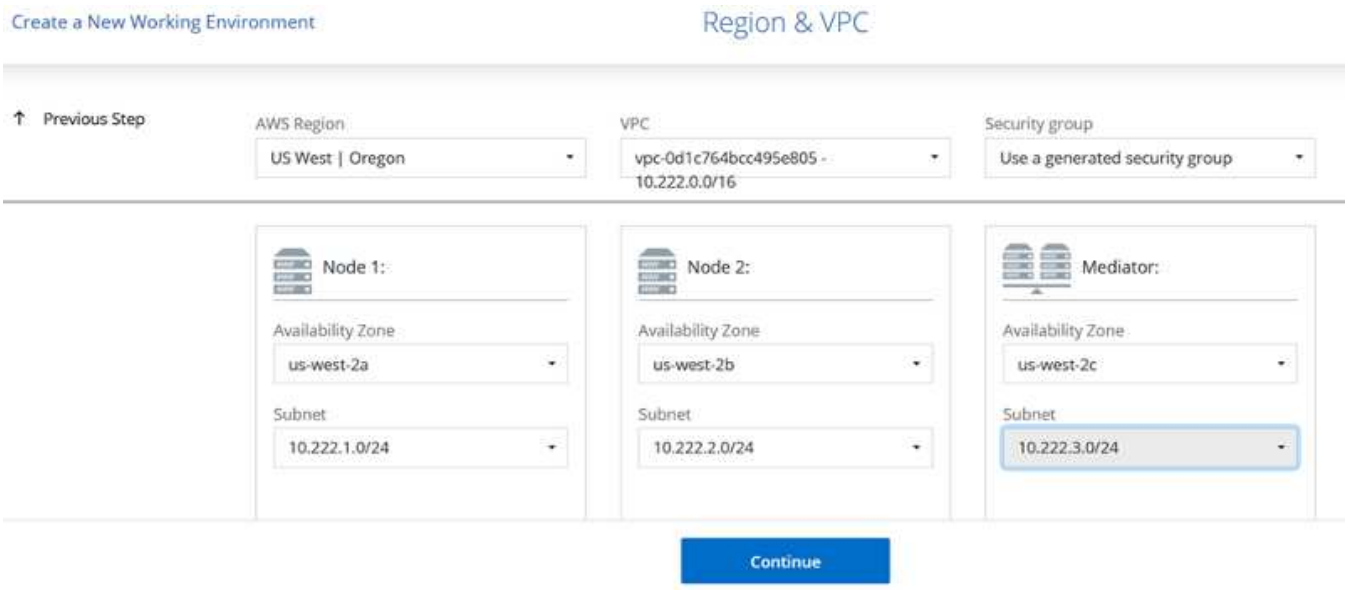
1. NetApp Data Classification、NetApp Backup and Recovery、Data Infrastructure Insightsなど、Cloud Volumes ONTAP展開用のアドオンサービスを選択します。続行をクリックします。



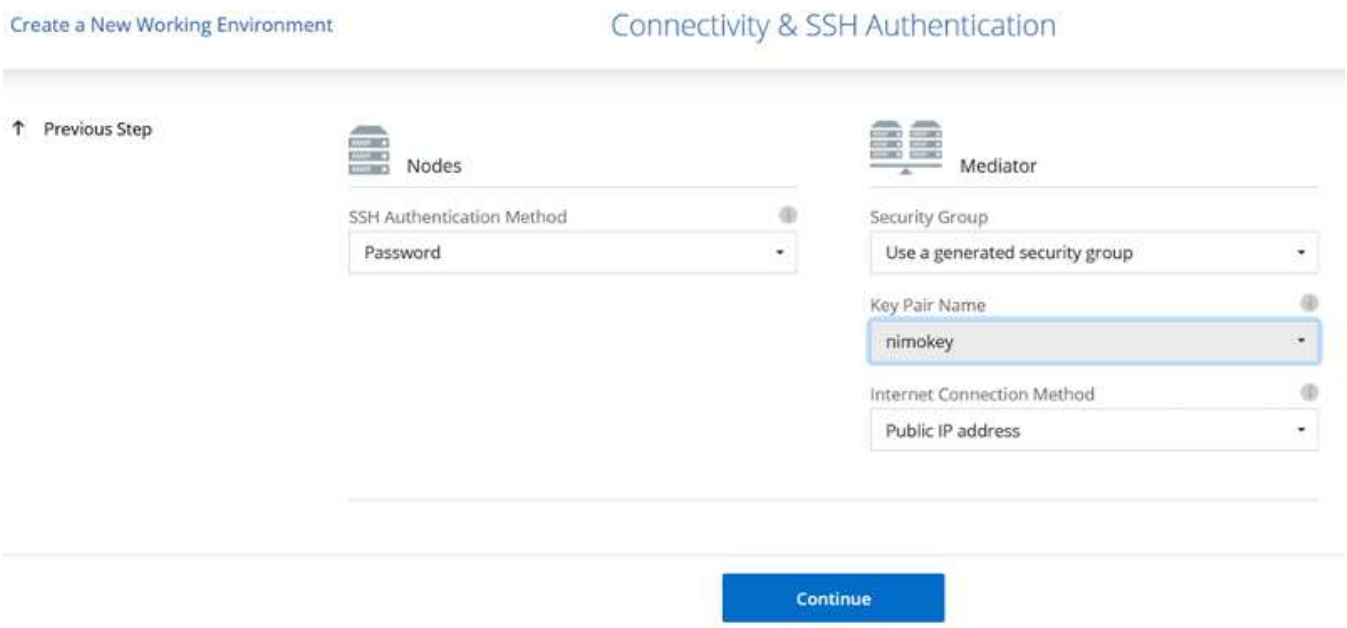
1. HA デプロイメント モデル ページで、複数のアベイラビリティー ゾーン構成を選択します。



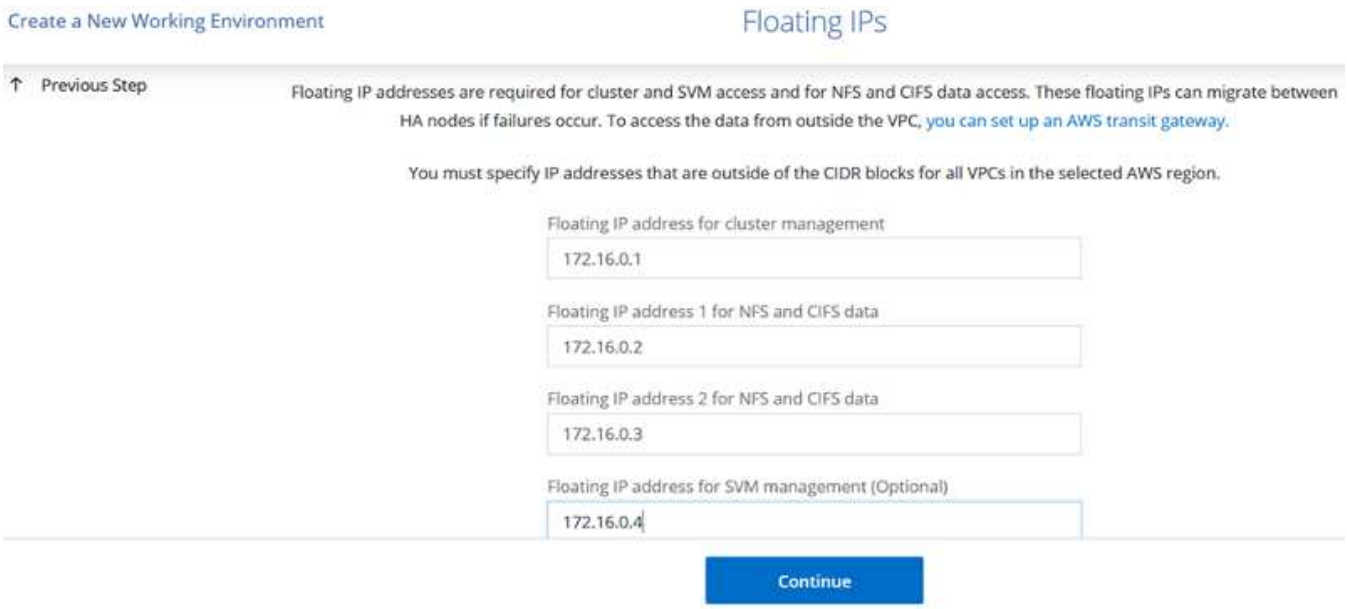
1. 「リージョンと VPC」ページでネットワーク情報を入力し、「続行」をクリックします。



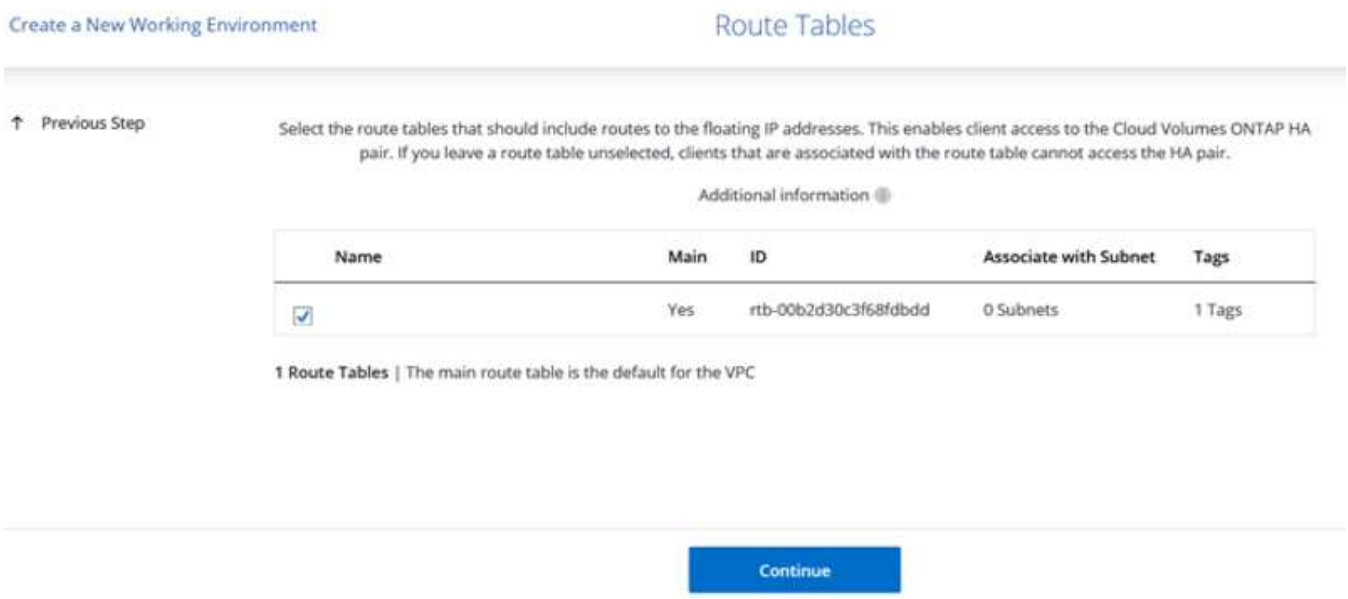
1. [接続と SSH 認証] ページで、HA ペアとメディエーターの接続方法を選択します。



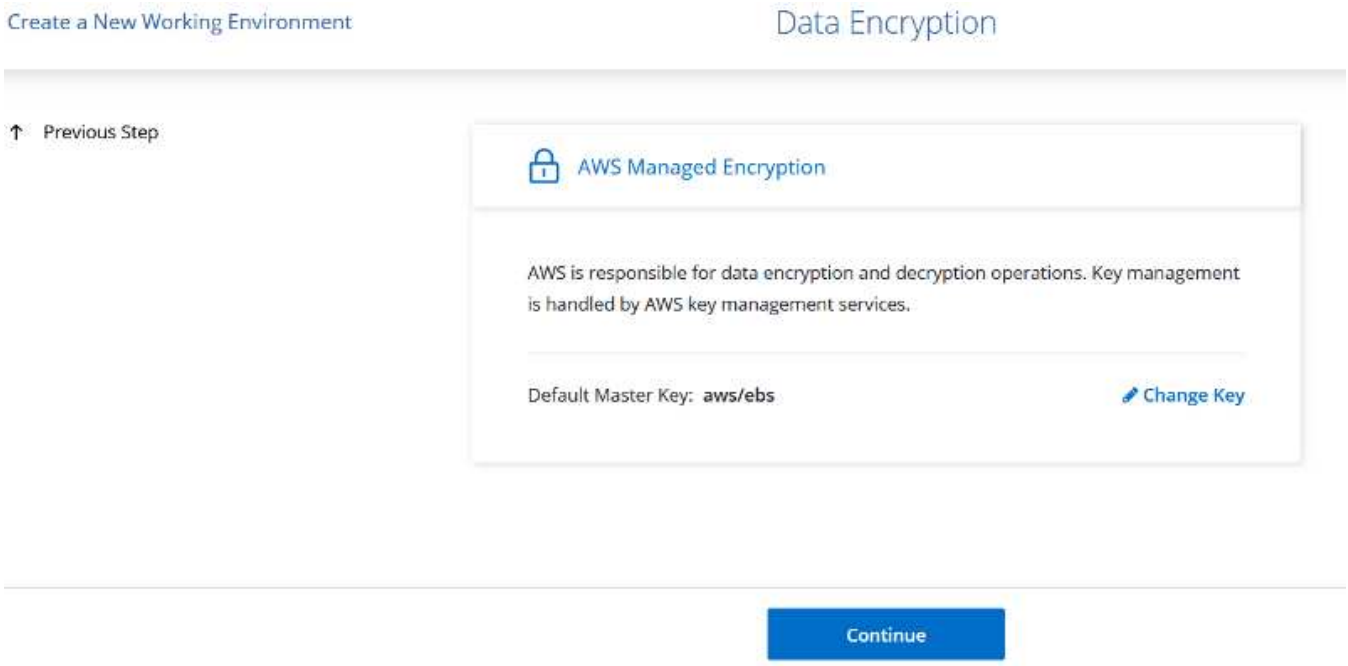
1. フローティング IP アドレスを指定して、「続行」をクリックします。



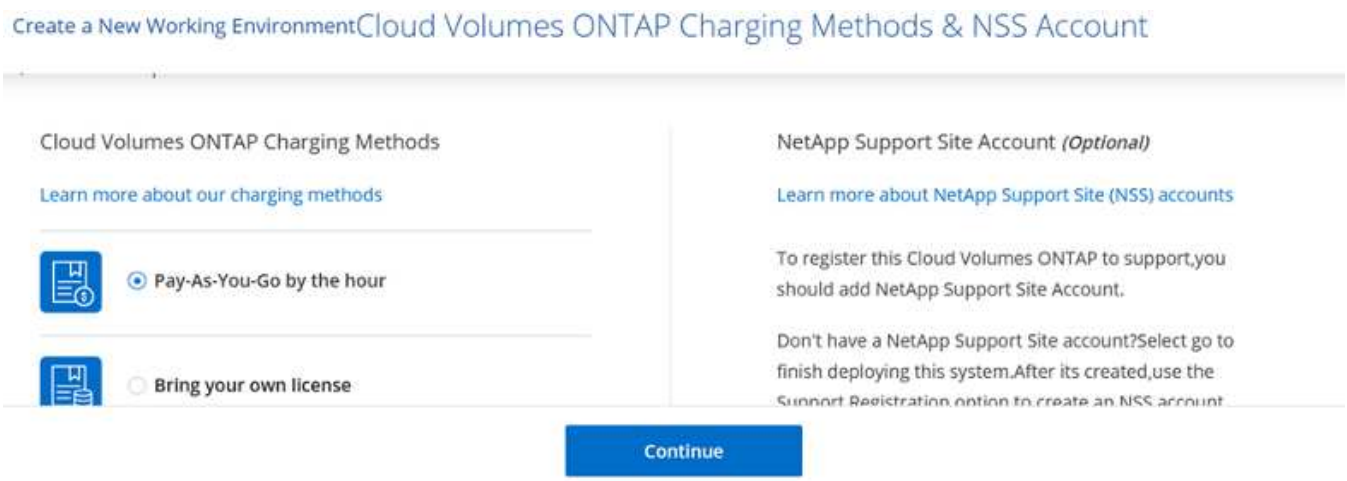
1. フローティング IP アドレスへのルートを含める適切なルート テーブルを選択し、[続行] をクリックします。



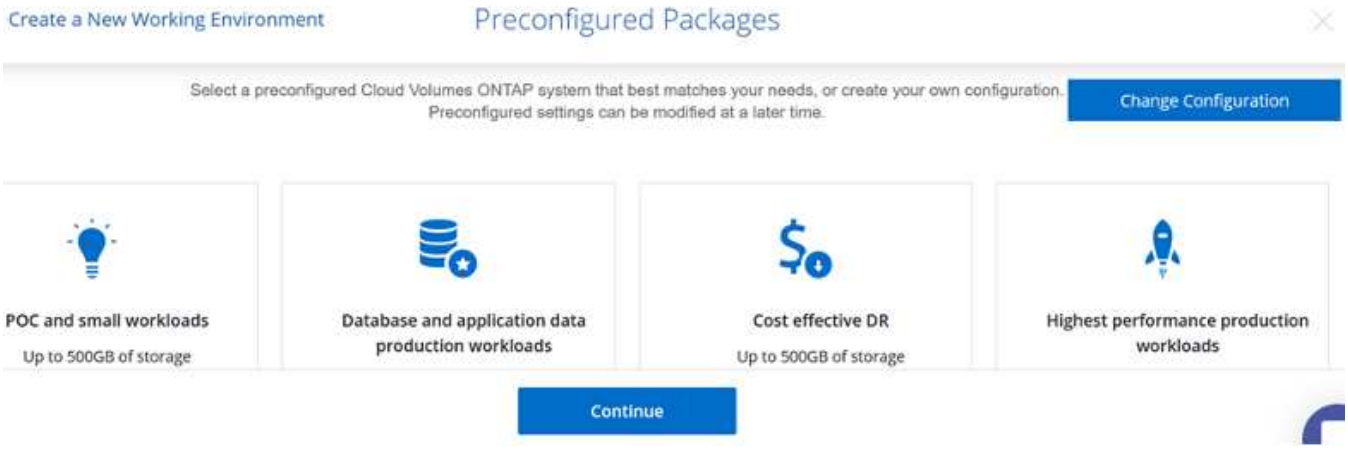
1. 「データ暗号化」ページで、AWS 管理の暗号化を選択します。



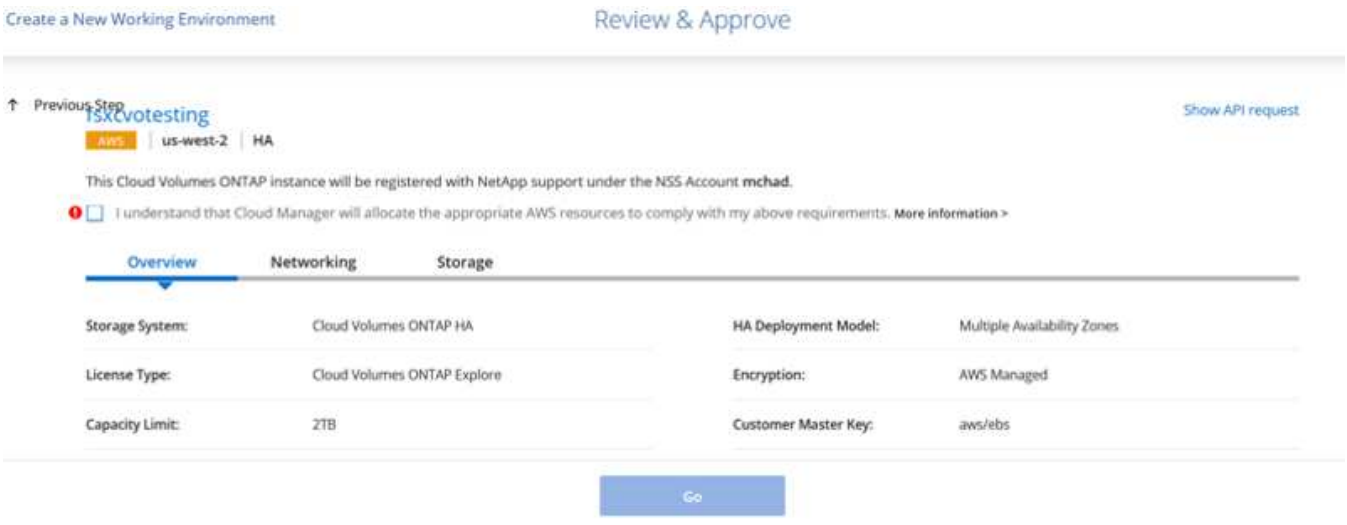
1. 既存のライセンスを使用する場合は、ライセンス オプション (Pay-As-You-Go または BYOL) を選択します。この例では、Pay-As-You-Go オプションが使用されています。



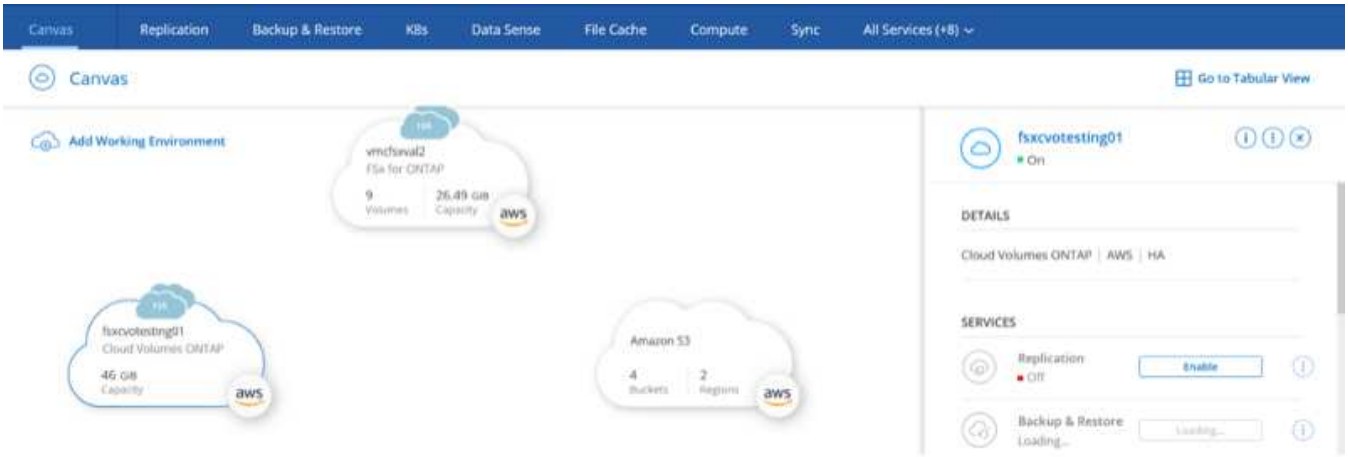
1. AWS SDDC 上の VMware クラウドで実行されている VM に展開するワークロードのタイプに基づいて、利用可能ないくつかの事前構成済みパッケージから選択します。



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

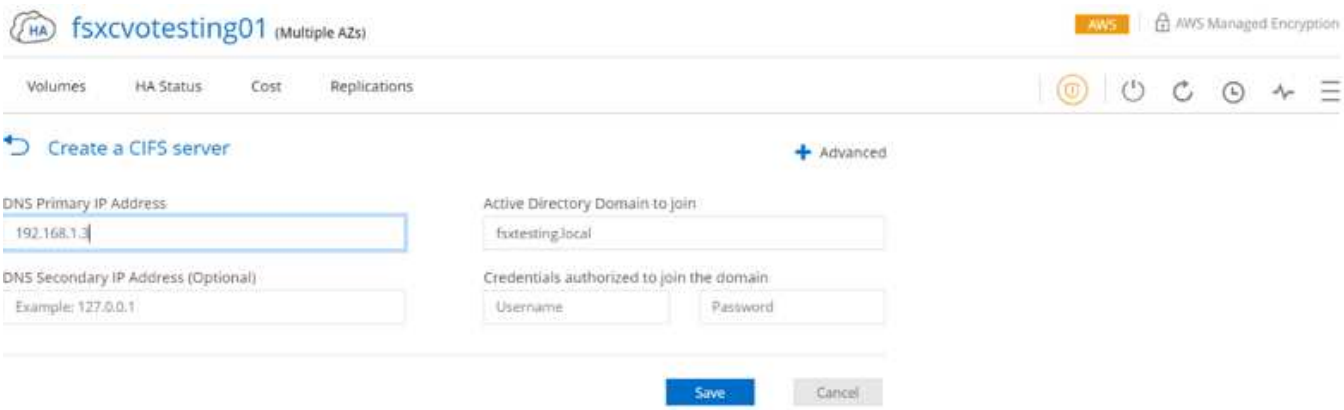


1. Cloud Volumes ONTAPがプロビジョニングされると、Canvas ページの作業環境にリストされます。

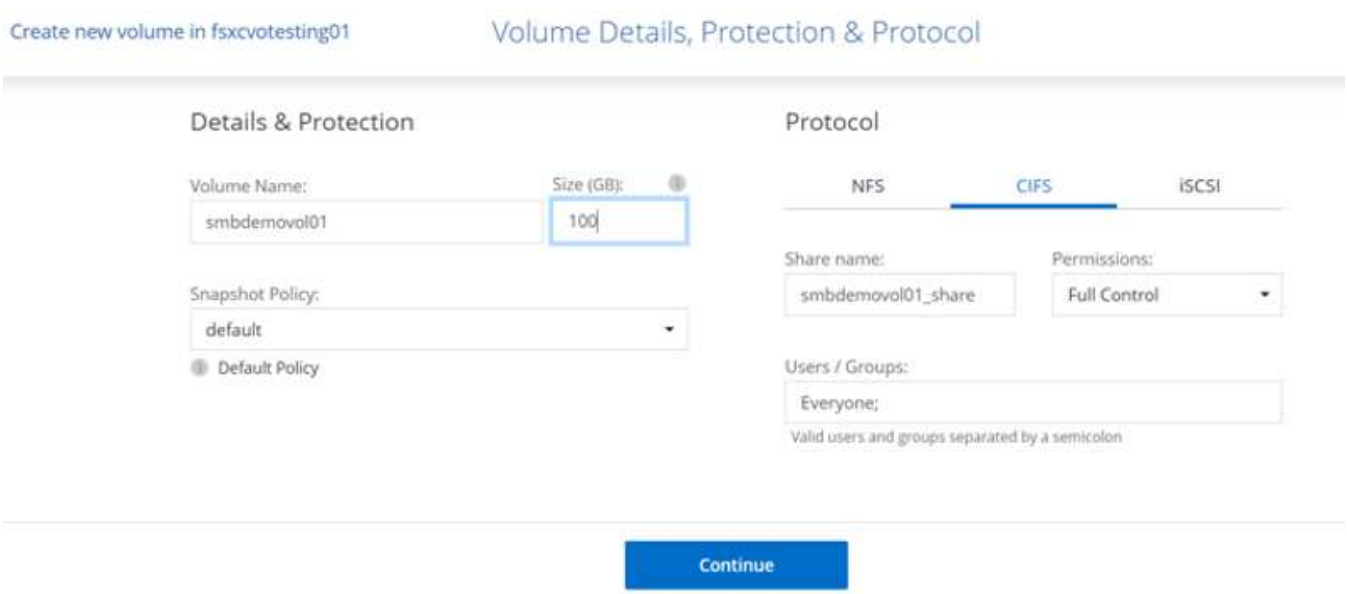


▼ **SMB**ボリュームの追加構成

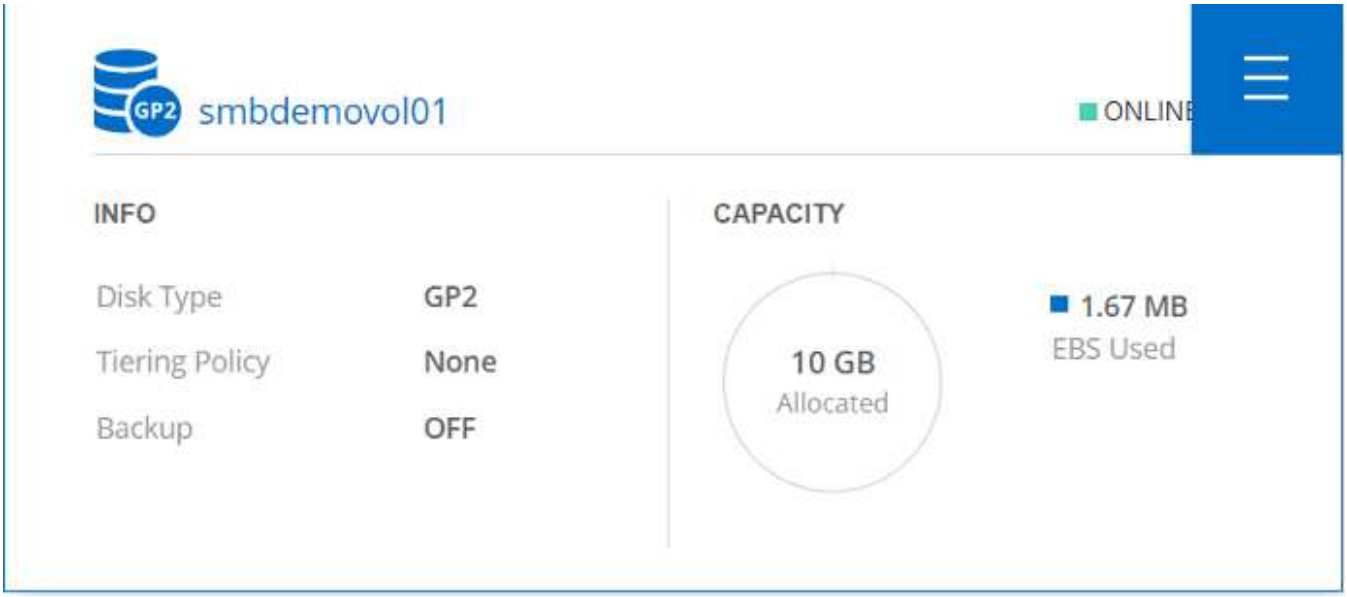
1. 作業環境の準備ができたら、CIFS サーバーが適切な DNS および Active Directory 構成パラメータで構成されていることを確認します。 SMB ボリュームを作成する前にこの手順を実行する必要があります。



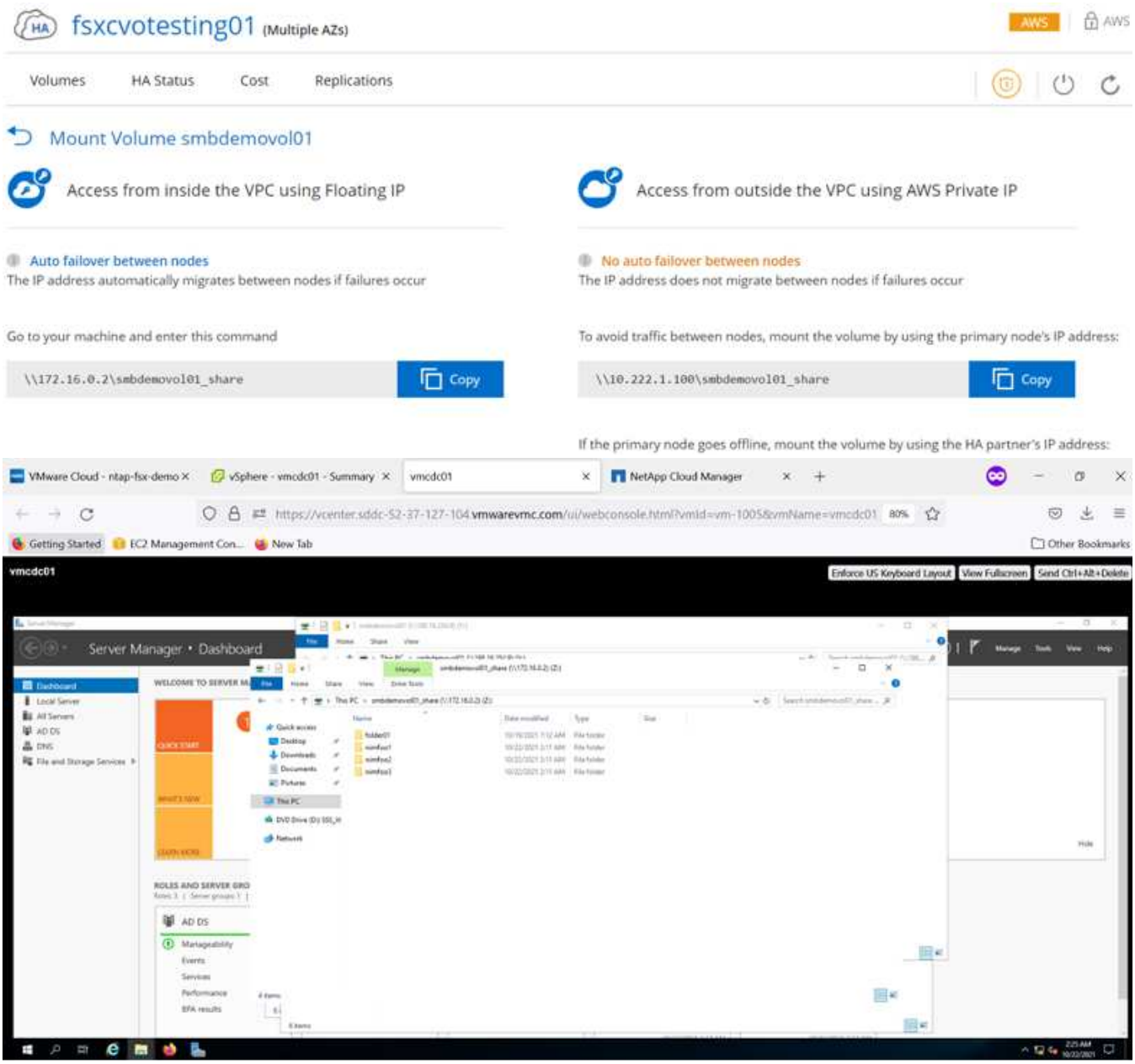
1. ボリュームを作成する CVO インスタンスを選択し、「ボリュームの作成」オプションをクリックします。適切なサイズを選択すると、クラウド マネージャーはそれを含むアグリゲートを選択するか、高度な割り当てメカニズムを使用して特定のアグリゲートに配置します。このデモでは、プロトコルとして SMB が選択されています。



1. ボリュームがプロビジョニングされると、ボリューム ペインで使用できるようになります。 CIFS 共有がプロビジョニングされているため、ユーザーまたはグループにファイルとフォルダーへのアクセス許可を与え、それらのユーザーが共有にアクセスしてファイルを作成できることを確認する必要があります。



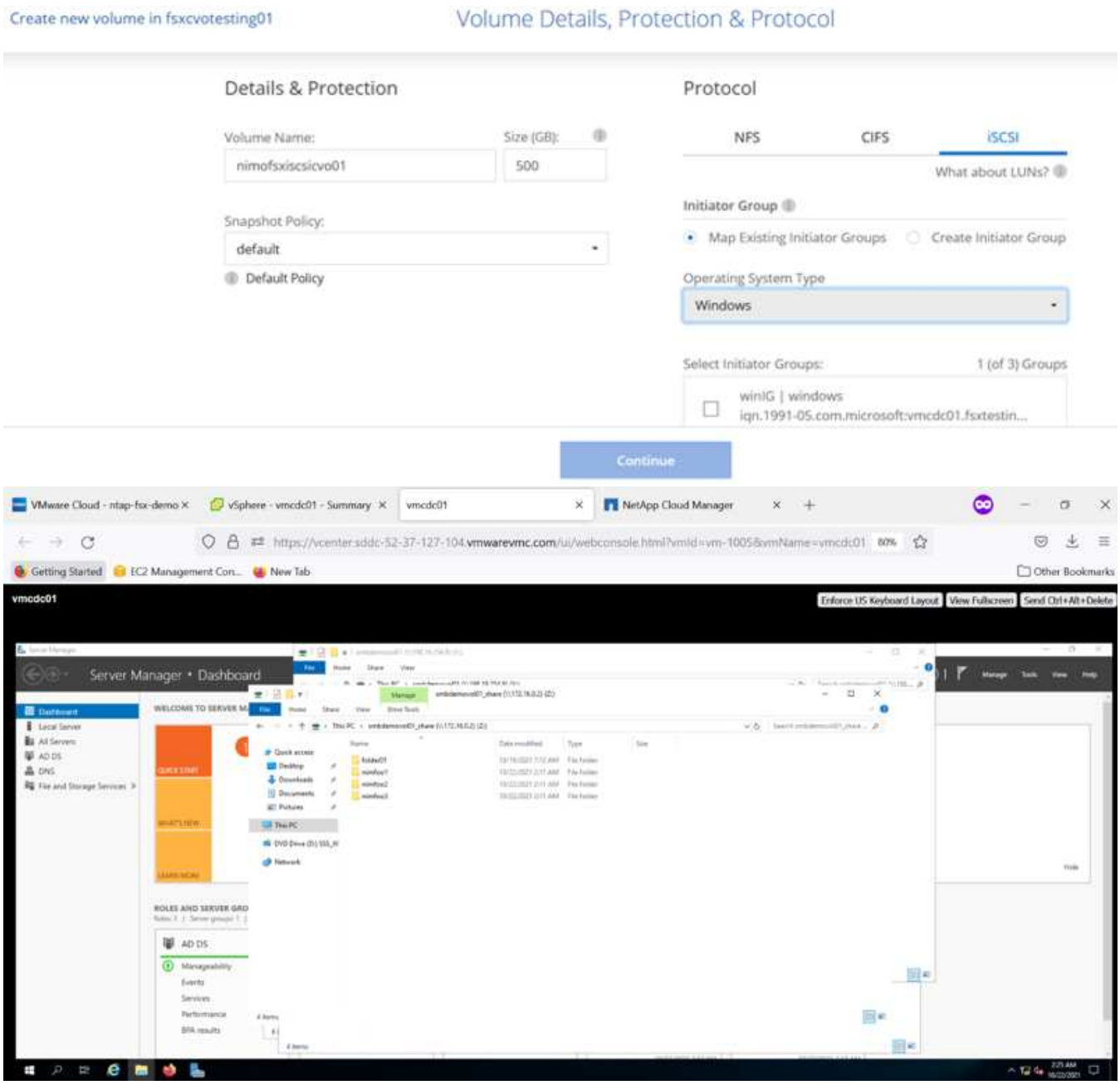
1. ボリュームが作成されたら、マウント コマンドを使用して、AWS SDDC ホストの VMware Cloud で実行されている VM から共有に接続します。
2. 次のパスをコピーし、ネットワーク ドライブのマップ オプションを使用して、AWS SDDC の VMware Cloud で実行されている VM にボリュームをマウントします。



▼ **LUN**をホストに接続する

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

1. Cloud Manager Canvas ページで、 Cloud Volumes ONTAP作業環境をダブルクリックして、ボリュームを作成および管理します。
2. [ボリュームの追加] > [新しいボリューム] をクリックし、[iSCSI] を選択して、[イニシエーター グループの作成] をクリックします。[Continue]をクリックします。



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

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

1. VMware Cloud on AWS でホストされている VM に RDP 接続します。
2. iSCSI イニシエーターのプロパティ ダイアログ ボックスを開きます: サーバー マネージャー > ダッシュボード > ツール > iSCSI イニシエーター。
3. [検出] タブで、[ポータルの検出] または [ポータルの追加] をクリックし、iSCSI ターゲット ポートの IP アドレスを入力します。
4. [ターゲット] タブで、検出されたターゲットを選択し、[ログオン] または [接続] をクリックします。
5. [マルチパスを有効にする] を選択し、[コンピューターの起動時にこの接続を自動的に復元する] または

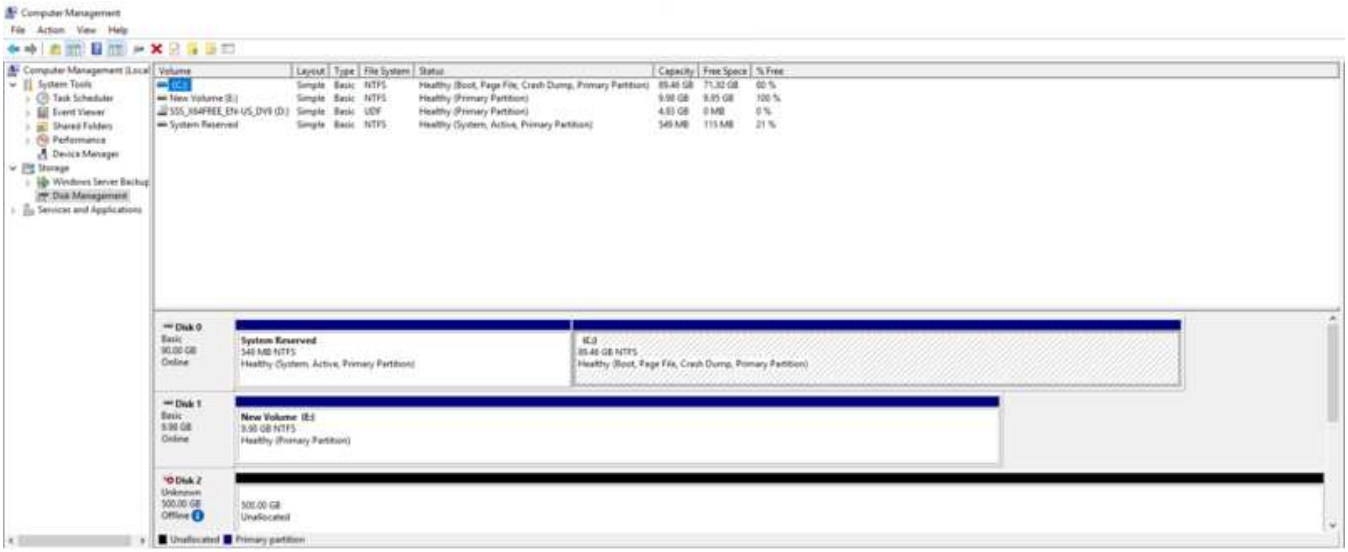
[この接続をお気に入りのターゲットの一覧に追加する] を選択します。[Advanced]をクリックします。

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



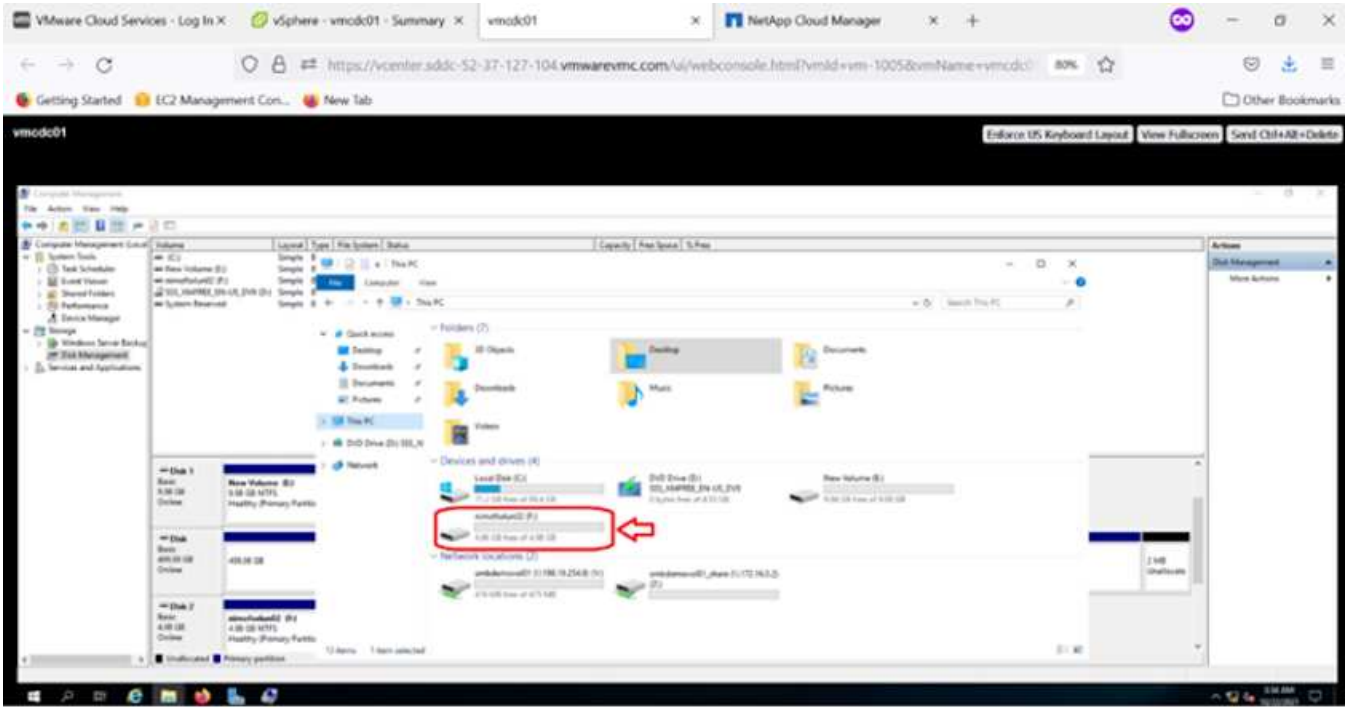
SVM からの LUN は、Windows ホストに対してディスクとして表示されます。追加された新しいディスクは、ホストによって自動的に検出されません。次の手順を実行して、手動での再スキャンをトリガーし、ディスクを検出します。

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



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

1. Windowsの[ディスクの管理]を起動します。
2. LUNを右クリックし、必要なディスクまたはパーティションの種類を選択します。
3. ウィザードの指示に従います。この例では、ドライブ F: がマウントされます。



Linux クライアントで、iSCSI デーモンが実行されていることを確認します。 LUN がプロビジョニングされたら、Linux ディストリビューションの iSCSI 構成に関する詳細なガイダンスを参照してください。例えば、UbuntuのiSCSI設定は次のようになります。"ここをクリックしてください。" 。確認するには、シェルから lsblk cmd を実行します。

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

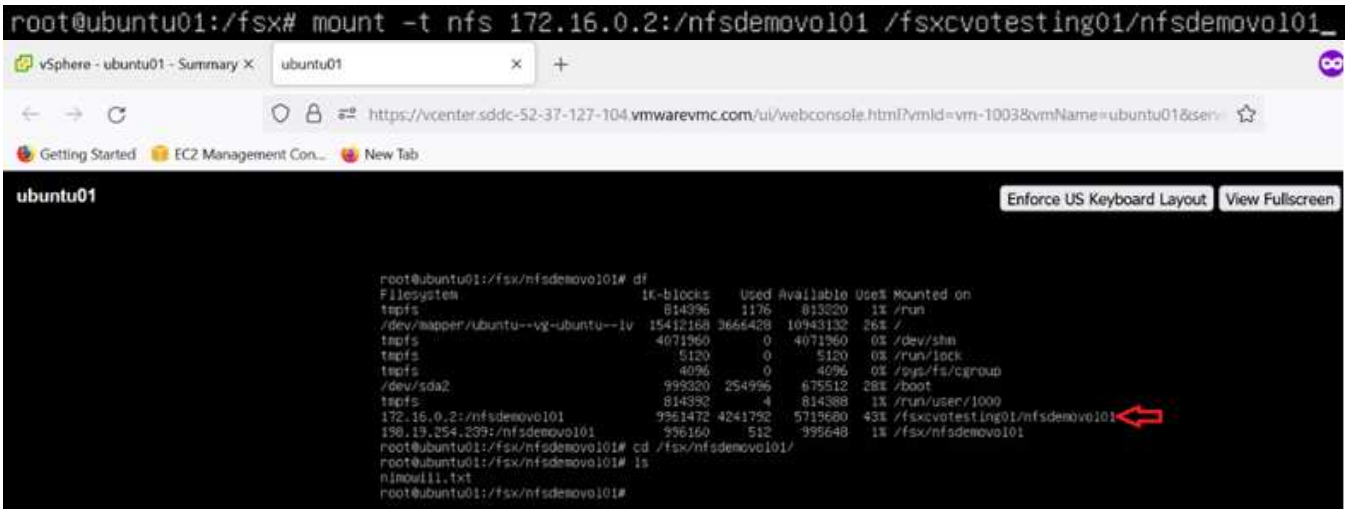
VMC on AWS SDDC 内の仮想マシンからCloud Volumes ONTAP (DIY) ファイル システムをマウントするには、次の手順を実行します。

1. 指定された Linux インスタンスに接続します。
2. セキュア シェル (SSH) を使用してインスタンス上でターミナルを開き、適切な資格情報でログインします。
3. 次のコマンドを使用して、ボリュームのマウント ポイントのディレクトリを作成します。

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

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

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



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

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

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

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

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

Azure NetApp Files は、業界をリードする高可用性のNetApp ONTAPデータ管理ソフトウェア上に構築されて

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

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

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

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

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

Azure NetApp Files は障害を取り除き、すべてのファイルベースのアプリケーションをクラウドに移行できるようにします。初めて、アプリケーションを再設計する必要がなくなり、複雑さなしでアプリケーション用の永続ストレージを利用できるようになります。

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

詳細については、"ゲスト接続ストレージとしての ANF" 。

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

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

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

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

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

詳細については、"ゲスト接続ストレージとしてのCVO" 。

ANFデータストアソリューションの概要

成功している組織はすべて、変革と近代化の道を歩んでいます。このプロセスの一環として、企業は通常、既存の VMware 投資を活用しながらクラウドのメリットを活用し、移行、バースト、拡張、および災害復旧のプロセスを可能な限りシームレスにする方法

を検討します。クラウドに移行する顧客は、弾力性とバースト、データセンターの撤退、データセンターの統合、サポート終了のシナリオ、合併、買収などの問題を評価する必要があります。各組織が採用するアプローチは、それぞれのビジネス上の優先順位に応じて異なります。クラウドベースの運用を選択する場合、適切なパフォーマンスと最小限の障害を備えた低コストのモデルを選択することが重要な目標です。適切なプラットフォームを選択することに加え、クラウドの展開と弾力性の力を最大限に引き出すには、ストレージとワークフローのオーケストレーションが特に重要です。

ユースケース

Azure VMware ソリューションは顧客に独自のハイブリッド機能を提供しますが、ネイティブ ストレージ オプションが限られているため、ストレージ負荷の高いワークロードを持つ組織にとってその有用性が制限されています。ストレージはホストに直接結び付けられているため、ストレージを拡張する唯一の方法はホストを追加することであり、これによりストレージを集中的に使用するワークロードのコストが 35 ～ 40% 以上増加する可能性があります。これらのワークロードには追加の処理能力ではなく追加のストレージが必要ですが、追加のホストに対して料金を支払う必要があります。

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

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

まとめると、ユースケースは次の 2 つの方法で分類できます。

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



ANF データストアの使用に関する追加情報については、お住まいの地域のNetAppまたは Microsoft ソリューション アーキテクトにお問い合わせください。

Azure の **VMware Cloud** オプション

Azure VMware ソリューション

Azure VMware Solution (AVS) は、Microsoft Azure パブリック クラウド内で完全に機能する VMware SDDC を提供するハイブリッド クラウド サービスです。 AVS は、Microsoft によって完全に管理およびサポートされ、Azure インフラストラクチャを使用する VMware によって検証されたファーストパーティ ソリューションです。そのため、お客様は、コンピューティング仮想化用の VMware ESXi、ハイパーコンバージド ストレージ用の vSAN、ネットワークとセキュリティ用の NSX を利用できると同時に、Microsoft Azure のグローバルな展開、クラス最高のデータ センター設備、ネイティブ Azure サービスとソリューションの豊富なエコシ

ステムへの近接性を活用できます。 Azure VMware Solution SDDC とAzure NetApp Files を組み合わせることで、最小限のネットワーク待機時間で最高のパフォーマンスが得られます。

使用するクラウドに関係なく、VMware SDDC が展開されると、初期クラスタには次のコンポーネントが含まれます。

- コンピューティング仮想化用の VMware ESXi ホストと管理用の vCenter サーバー アプライアンス。
- 各 ESXi ホストの物理ストレージ資産を組み込んだ VMware vSAN ハイパーコンバージド ストレージ。
- 仮想ネットワークとセキュリティのための VMware NSX と、管理用の NSX Manager クラスタ。

まとめ

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

まとめ

このドキュメントの主なポイントは次のとおりです。

- Azure NetApp Files をAVS SDDC 上のデータストアとして使用できるようになりました。
- アプリケーションの応答時間を向上させ、より高い可用性を実現し、必要なときに必要な場所でワークロード データにアクセスできるようにします。
- シンプルで即時のサイズ変更機能により、vSAN ストレージの全体的な複雑さを簡素化します。
- 動的な再形成機能を使用して、ミッションクリティカルなワークロードのパフォーマンスを保証します。
- Azure VMware Solution Cloud が宛先である場合、 Azure NetApp Files は最適化された展開に適したストレージ ソリューションです。

詳細情報の入手方法

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

- Azure VMware ソリューションのドキュメント

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

- Azure NetApp Files のドキュメント

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

- Azure NetApp Filesデータストアを Azure VMware Solution ホストに接続する (プレビュー)

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

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

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

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

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

次の点に留意してください。

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

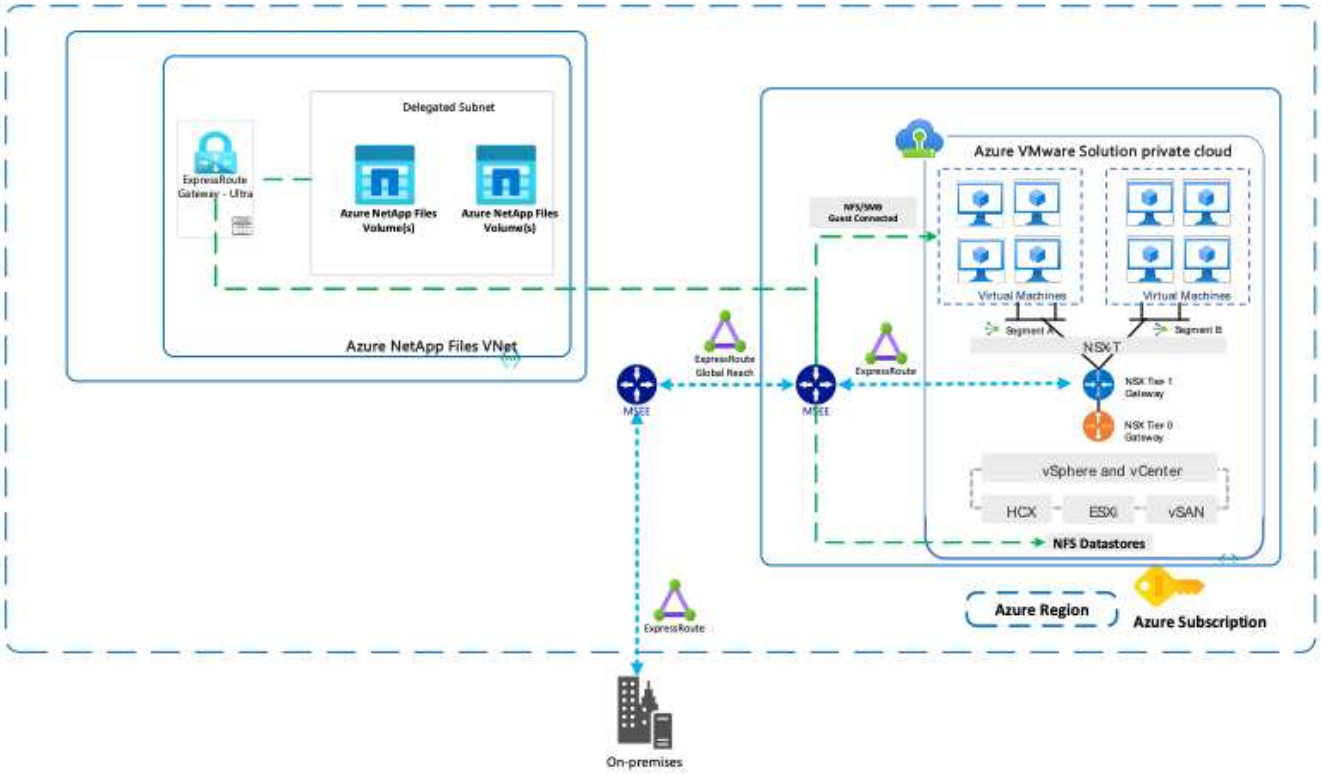
Azure NetApp Files を使用すると、複数のデータストアをデプロイすることもできます。これにより、適切なデータストアに仮想マシンを配置し、ワークロードのパフォーマンス要件を満たすために必要なサービス レベルを割り当てることで、オンプレミスのデプロイ モデルを模倣できます。マルチプロトコル サポートの独自の機能により、ゲスト ストレージは、SQL や Oracle などのデータベース ワークロードの追加オプションとなると同時に、追加の NFS データストア機能を使用して残りの VMDK を格納することもできます。これに加えて、ネイティブ スナップショット機能を使用すると、迅速なバッ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

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

詳細なアーキテクチャ

このアーキテクチャでは、高レベルの観点から、オンプレミス環境と Azure 間でハイブリッド クラウドの接続性とアプリの移植性を実現する方法について説明します。また、 Azure NetApp Files を補助的な NFS デー

タストアとして使用する方法や、Azure VMware ソリューションでホストされているゲスト仮想マシンのゲスト内ストレージ オプションとして使用する方法についても説明します。



サイジング

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

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

RVtools を実行するには、次の手順を実行します。

1. RVTools をダウンロードしてインストールします。
2. RVTools を実行し、オンプレミスの vCenter Server に接続するために必要な情報を入力して、「ログイン」を押します。
3. 在庫を Excel スプレッドシートにエクスポートします。
4. スプレッドシートを編集し、[vInfo] タブから理想的な候補ではない VM を削除します。このアプローチにより、必要な数のホストを使用して Azure VMware SDDC クラスターを適切なサイズにするために使用できるストレージ要件に関する明確な出力が得られます。

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

Azure VMware Solution のデプロイと構成

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

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

セットアッププロセスは、次の 3 つの部分に分けられます。

- リソース プロバイダーを登録し、プライベート クラウドを作成します。
- 新規または既存の ExpressRoute 仮想ネットワーク ゲートウェイに接続します。
- ネットワーク接続を検証し、プライベート クラウドにアクセスします。こちらを参照してください"リンク"Azure VMware ソリューションの SDDC プロビジョニング プロセスのステップバイステップのチュートリアル。

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

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

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

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

▼ 前提条件

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

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

1. 登録されていない場合は登録してください。

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

> 登録が完了するまでに約 15 分かかります。

1. 登録のステータスを確認するには、次のコマンドを実行します。

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

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

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

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

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

1. VMware 拡張機能がインストールされていることを確認します。

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

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

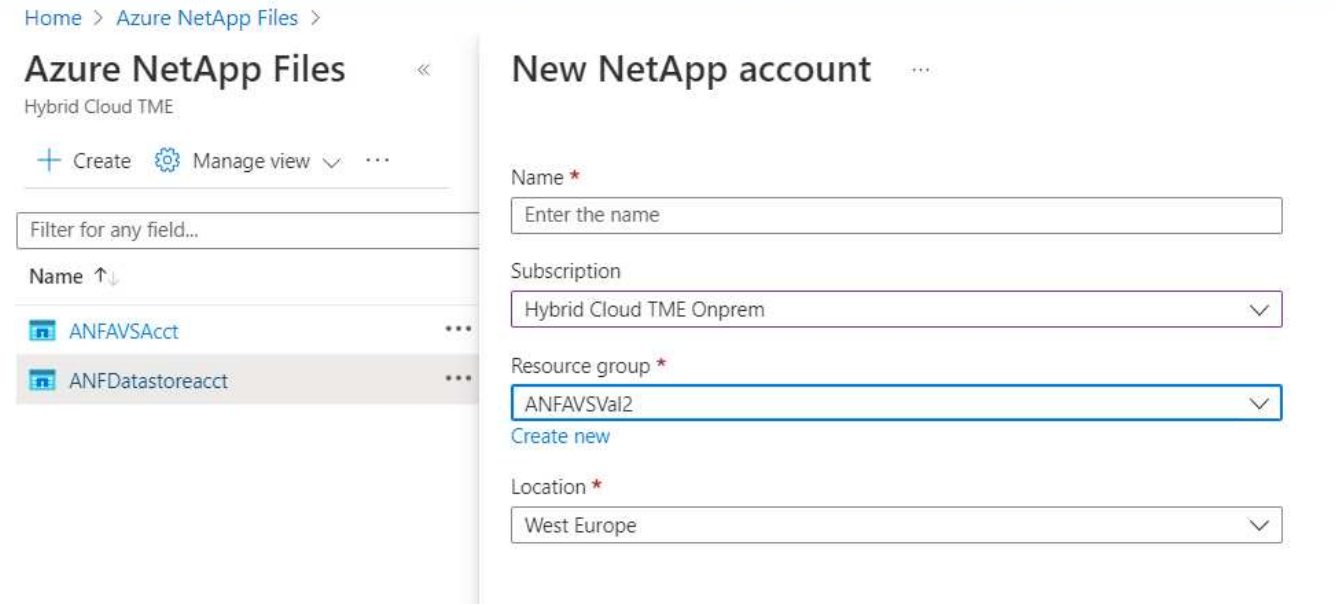
```
az extension update --name vmware
```

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

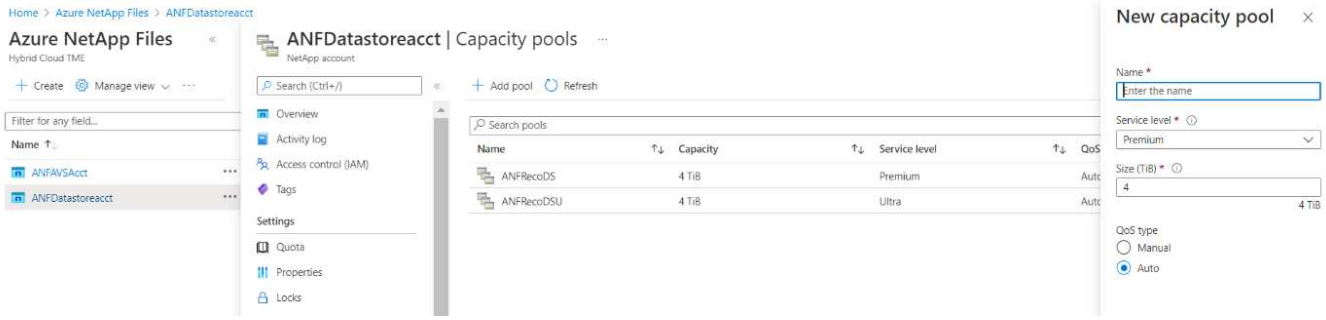
```
az extension add --name vmware
```

▼ **Azure NetApp Files**ボリュームを作成してマウントする

1. Azure Portal にログインし、 Azure NetApp Files にアクセスします。 Azure NetApp Filesサービスへのアクセスを確認し、 Azure NetApp Filesリソース プロバイダーを登録するには、 `az provider register `--namespace Microsoft.NetApp –wait`指示。登録後、 NetAppアカウントを作成します。こちらを参照してください "リンク"詳細な手順については、こちらをご覧ください。



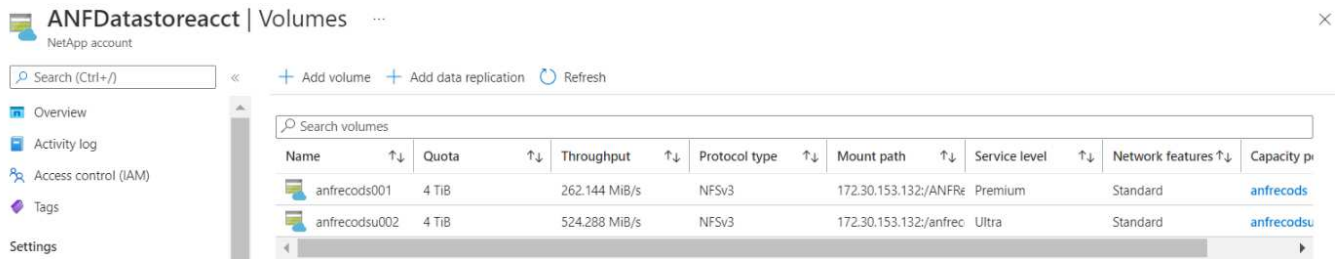
1. NetAppアカウントを作成したら、必要なサービス レベルとサイズで容量プールを設定します。詳細については、こちらを参照してください。 "リンク" 。



覚えておくべきポイント

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

1. Azure NetApp Filesの委任されたサブネットを構成し、ボリュームを作成するときにこのサブネットを指定します。委任されたサブネットを作成する詳細な手順については、こちらを参照してください。 "リンク" 。
2. 容量プール ブレードのボリューム ブレードを使用して、データストアの NFS ボリュームを追加します。



Azure NetApp Filesボリュームのパフォーマンスをサイズまたはクォータ別に確認するには、以下を参照してください。"Azure NetApp Files のパフォーマンスに関する考慮事項" 。

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

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

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

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

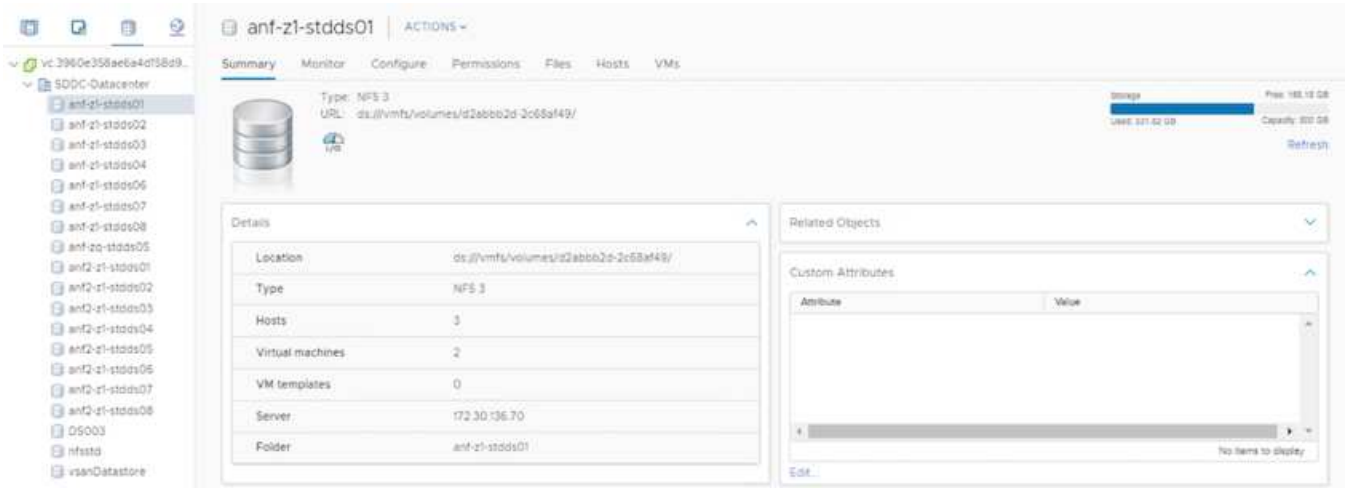
```
C:\Users\niyaz>az vmware datastore netapp-volume create --name
ANFRecoDSU002 --resource-group anfavsval2 --cluster Cluster-1 --private
-cloud ANFDataClus --volume-id /subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002
{
  "diskPoolVolume": null,
  "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateCl
ouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDSU002",
  "name": "ANFRecoDSU002",
  "netAppVolume": {
    "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002
",
    "resourceGroup": "anfavsval2"
  },
  "provisioningState": "Succeeded",
  "resourceGroup": "anfavsval2",
  "type": "Microsoft.AVS/privateClouds/clusters/datastores"
}

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

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

"Microsoft.AVS/privateClouds/clusters/datastores" }, { "diskPoolVolume": null, "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDSU002", "name": "ANFRecoDSU002", "netAppVolume": { "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netAppAccounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002", "resourceGroup": "anfavsval2" }, "provisioningState": "Succeeded", "resourceGroup": "anfavsval2", "type": "Microsoft.AVS/privateClouds/clusters/datastores" }]

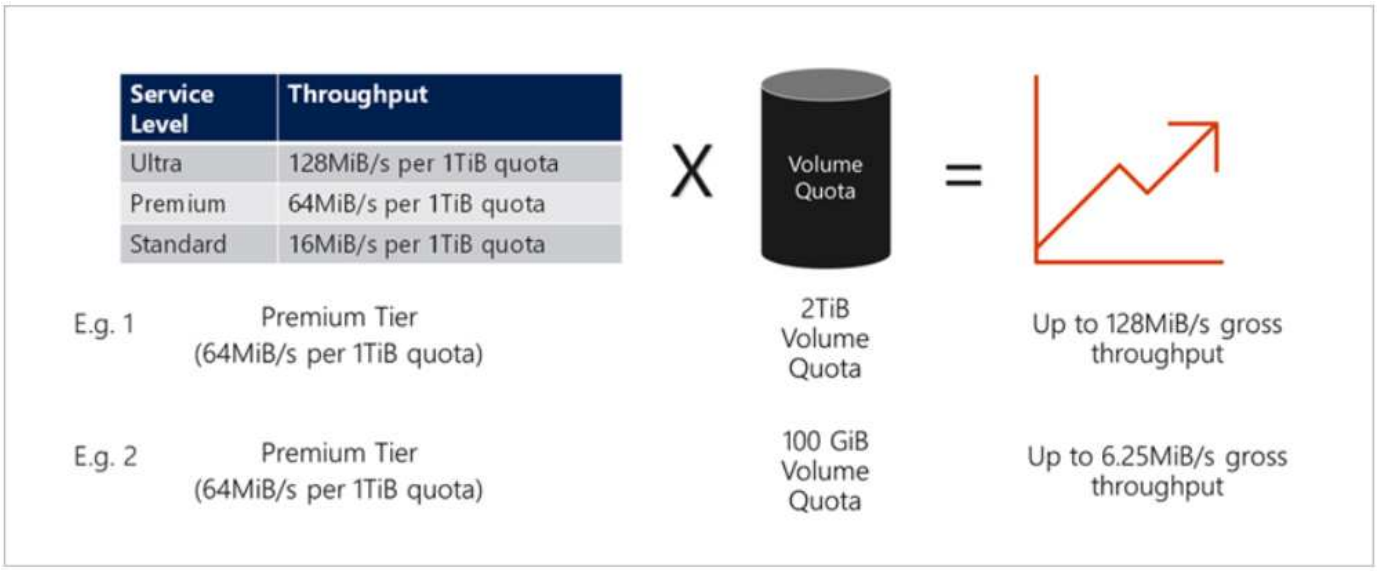
1. 必要な接続が確立されると、ボリュームはデータストアとしてマウントされます。



サイズとパフォーマンスの最適化

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

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



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

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

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

パフォーマンスに関する考慮事項

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

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

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

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

覚えておくべきポイント

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

データストアのサイズを増やす

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

覚えておくべきポイント

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

ワークロード

▼ 移住

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

▼ データ保護

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

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

ANF データストアでは、「新しいボリュームに復元」オプションを使用してデータストア ボリューム全体のクローンを作成し、復元されたボリュームを AVS SDDC 内のホストに別のデータストアとしてマウントできます。データストアをマウントすると、その中の VM

は、個別にクローン作成された VM であるかのように登録、再構成、カスタマイズできるようになります。

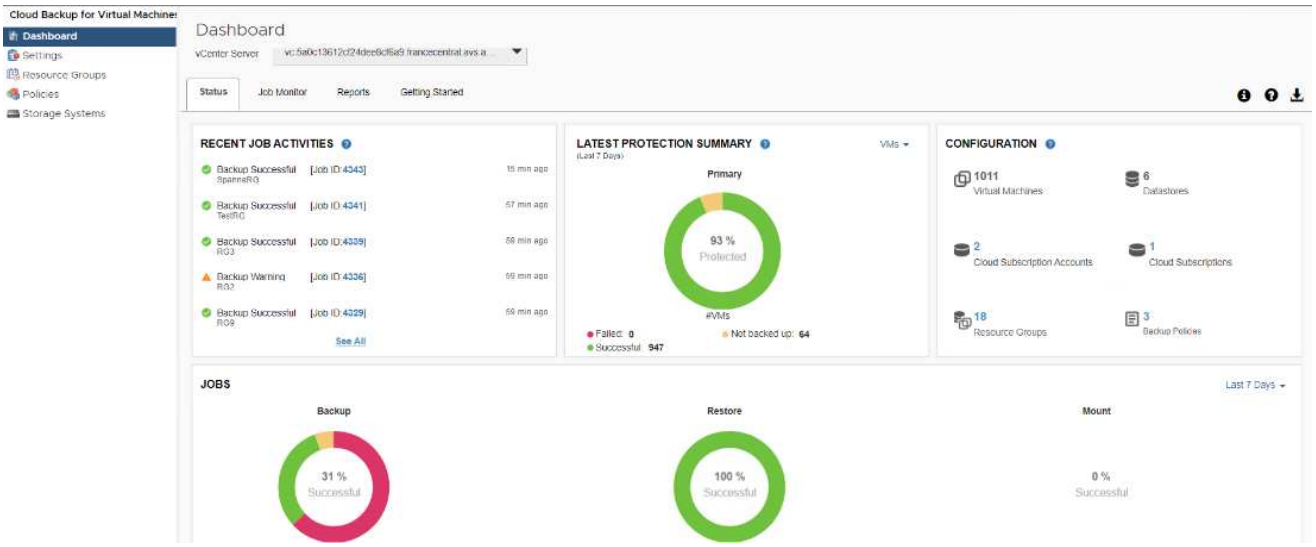
▼ 仮想マシン向け**NetApp Backup and Recovery**

NetApp Backup and Recovery for Virtual Machines は、vCenter 上に vSphere Web クライアント GUI を提供し、バックアップ ポリシーを使用して Azure VMware Solution 仮想マシンおよび Azure NetApp Files データストアを保護します。これらのポリシーでは、スケジュール、保持期間、その他の機能を定義できます。NetApp Backup and Recovery for Virtual Machines の機能は、Run コマンドを使用してデプロイできます。

セットアップと保護ポリシーは、次の手順を実行してインストールできます。

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

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



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

クラウドへの災害復旧は、サイトの停止やデータ破損イベント (ランサムウェアなど) からワークロードを保護する、回復力がありコスト効率に優れた方法です。 VMware VAIO フレームワークを使用すると、オンプレミスの VMware ワークロードを Azure Blob ストレージに複製して回復できるため、データ損失を最小限に抑えるか、ほぼゼロにすることができ、RTO はほぼゼロになります。 JetStream DR を使用すると、オンプレミスから AVS、具体的にはAzure NetApp Filesに複製されたワークロードをシームレスに回復できます。 DR サイトでの最小限のリソースとコスト効率の高いクラウド ストレージを使

用することで、コスト効率の高い災害復旧が可能になります。 JetStream DR は、Azure Blob Storage を介して ANF データストアへのリカバリを自動化します。 JetStream DR は、ネットワーク マッピングに従って、独立した VM または関連する VM のグループをリカバリ サイト インフラストラクチャに復元し、ランサムウェア保護のためのポイントインタイム リカバリを提供します。

"ANF、JetStream、AVS を使用した DR ソリューション" 。

Azure 向け**NetApp**ゲスト接続ストレージ オプション

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

Azure NetApp Files(ANF)

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

Azure netApp Files は障害を取り除き、すべてのファイルベースのアプリケーションをクラウドに移行できるようにします。初めて、アプリケーションを再設計する必要がなくなり、複雑さなしでアプリケーション用の永続ストレージを利用できるようになります。

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

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

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

Azure NetApp Files共有は、Azure VMware Solution SDDC 環境で作成された VM からマウントできます。Azure NetApp Files はSMB および NFS プロトコルをサポートしているため、ボリュームを Linux クライアントにマウントし、Windows クライアントにマップすることもできます。 Azure NetApp Filesボリュームは、5 つの簡単な手順で設定できます。

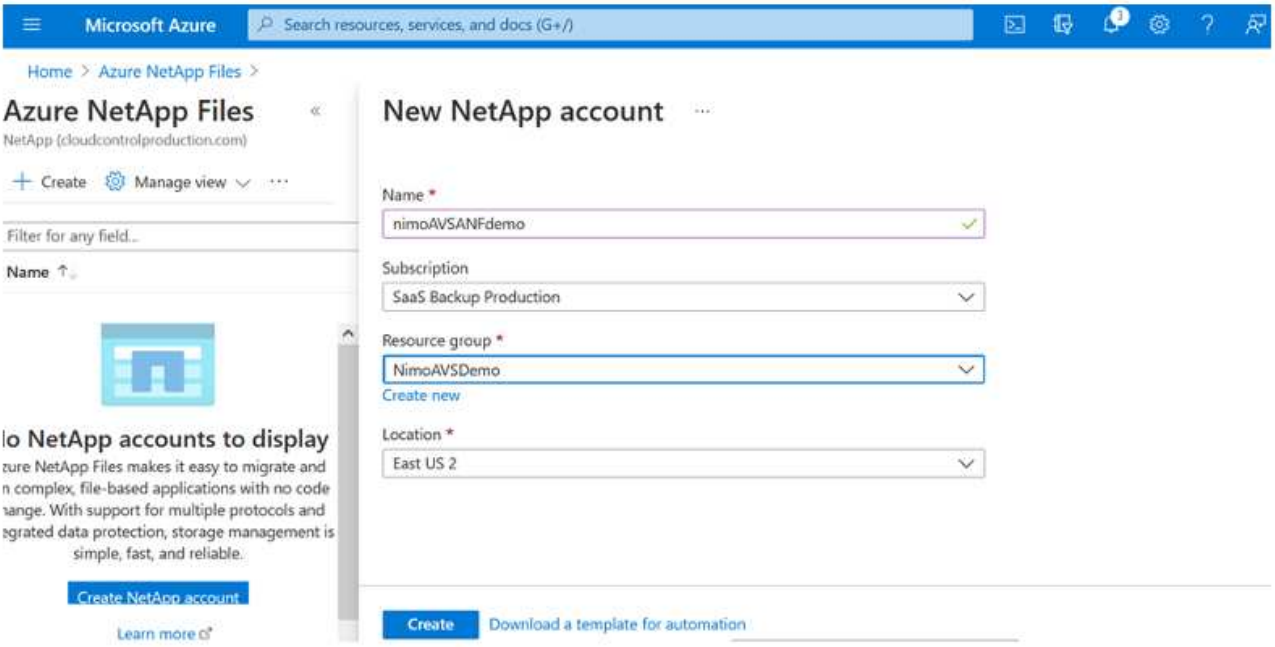
Azure NetApp Filesと Azure VMware Solution は同じ Azure リージョンに存在する必要があります。

▼ **Azure NetApp Files**ボリュームを作成してマウントする

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

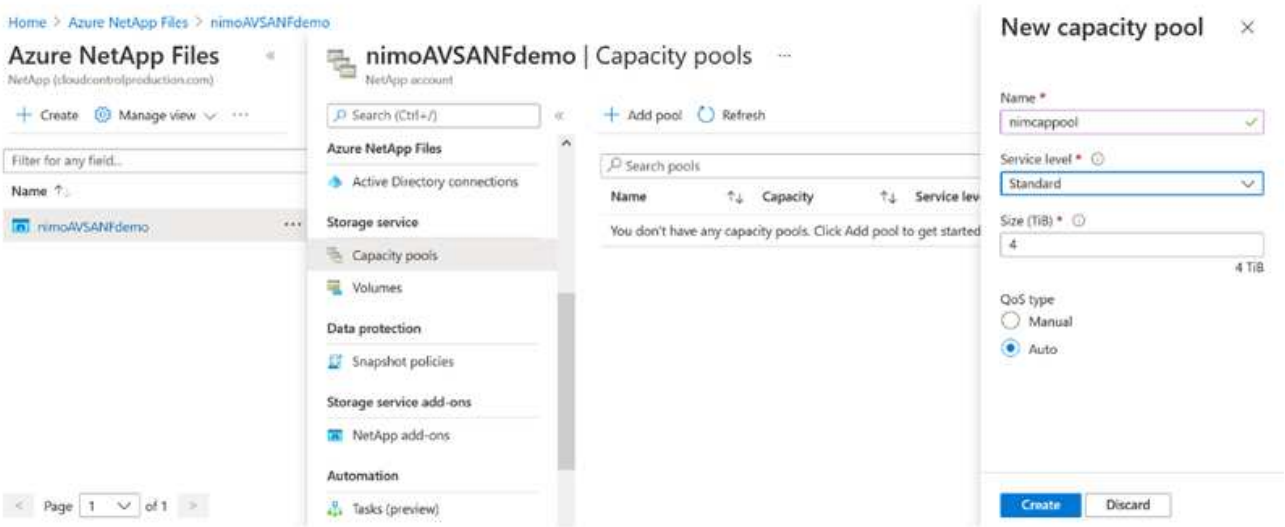
1. Azure Portal にログインし、 Azure NetApp Files にアクセスします。 Azure NetApp Filesサービスへのアクセスを確認し、*az provider register --namespace Microsoft. NetApp –wait* コマンドを使用してAzure NetApp Filesリソース プロバイダーを登録します。登録が完了したら、 NetAppアカウントを作成します。

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

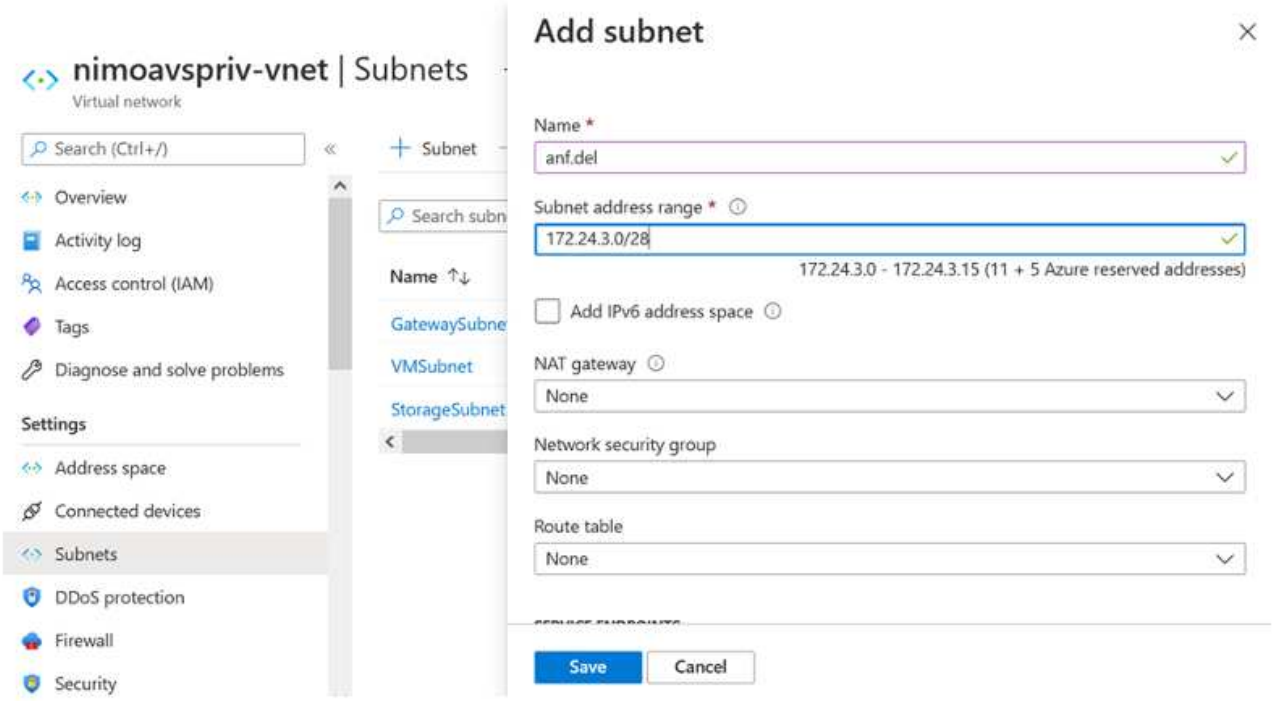


2. NetAppアカウントを作成したら、必要なサービス レベルとサイズで容量プールを設定します。

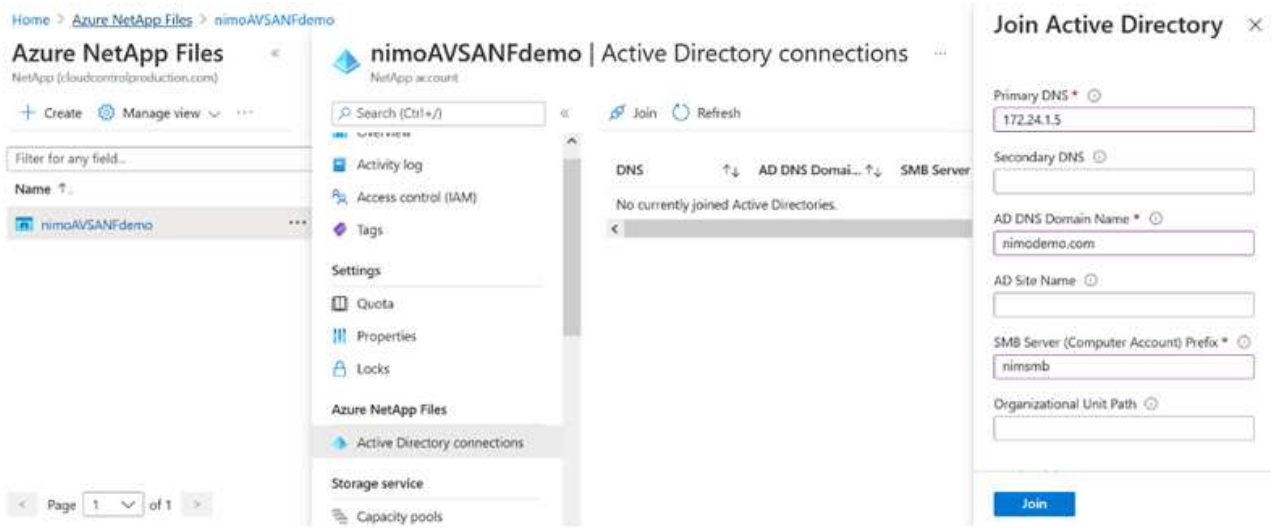
   詳細については、以下を参照してください。 "容量プールを設定する" 。



3. Azure NetApp Filesの委任されたサブネットを構成し、ボリュームの作成時にこのサブネットを指定します。委任されたサブネットを作成する詳細な手順については、"サブネットをAzure NetApp Filesに委任する" 。

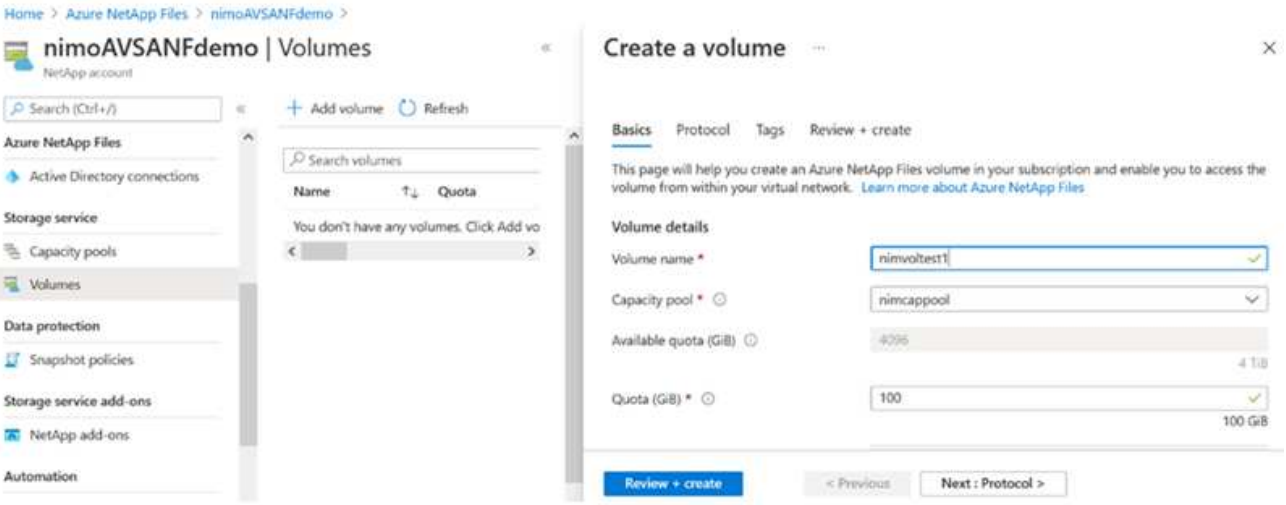


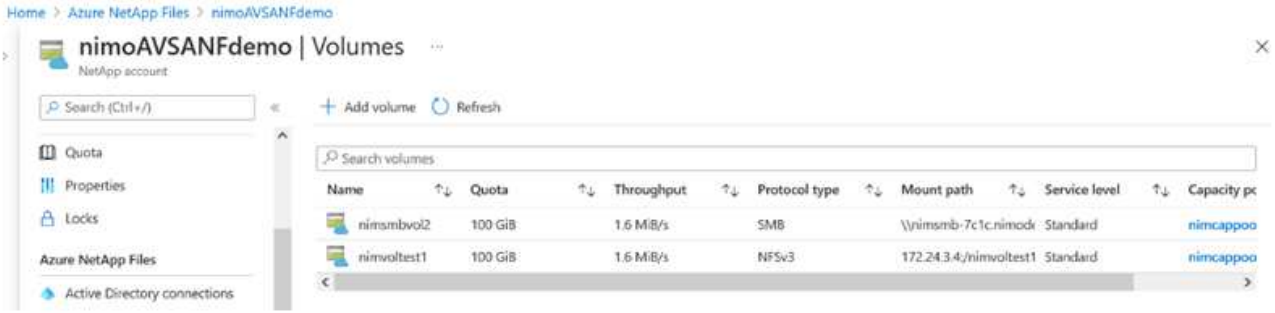
4. [容量プール] ブレードの下の [ボリューム] ブレードを使用して、SMB ボリュームを追加します。 SMB ボリュームを作成する前に、Active Directory コネクタが構成されていることを確認してください。



5. [確認 + 作成] をクリックして SMB ボリュームを作成します。

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

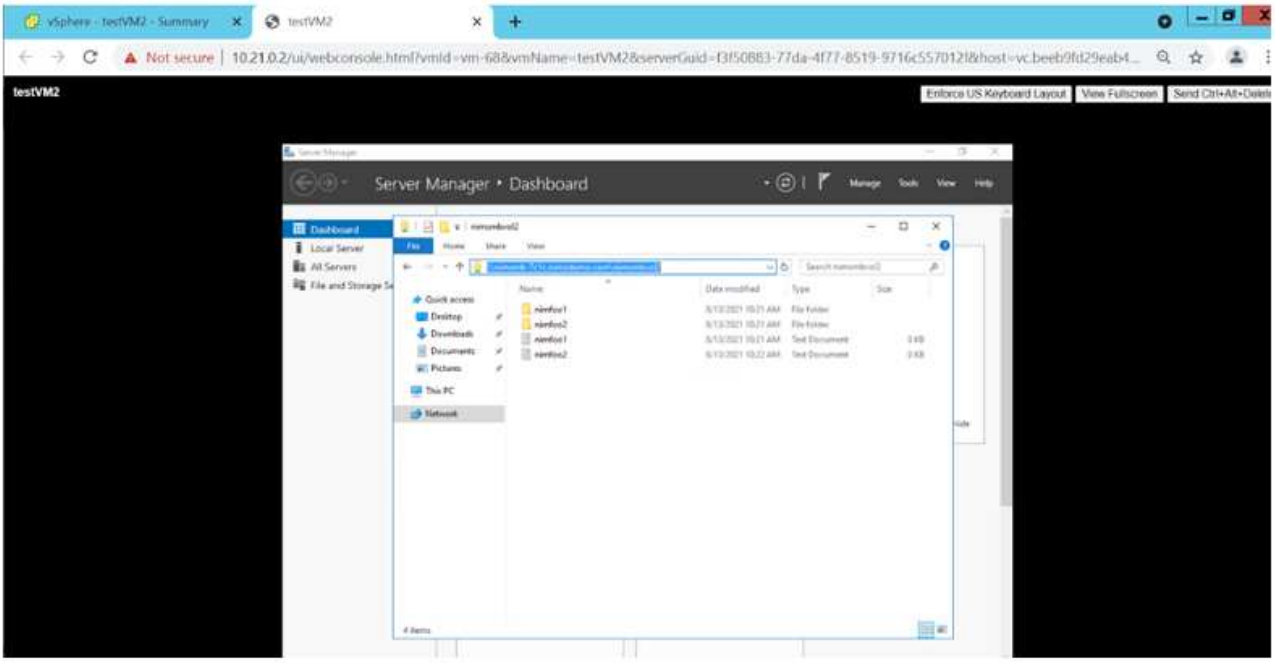


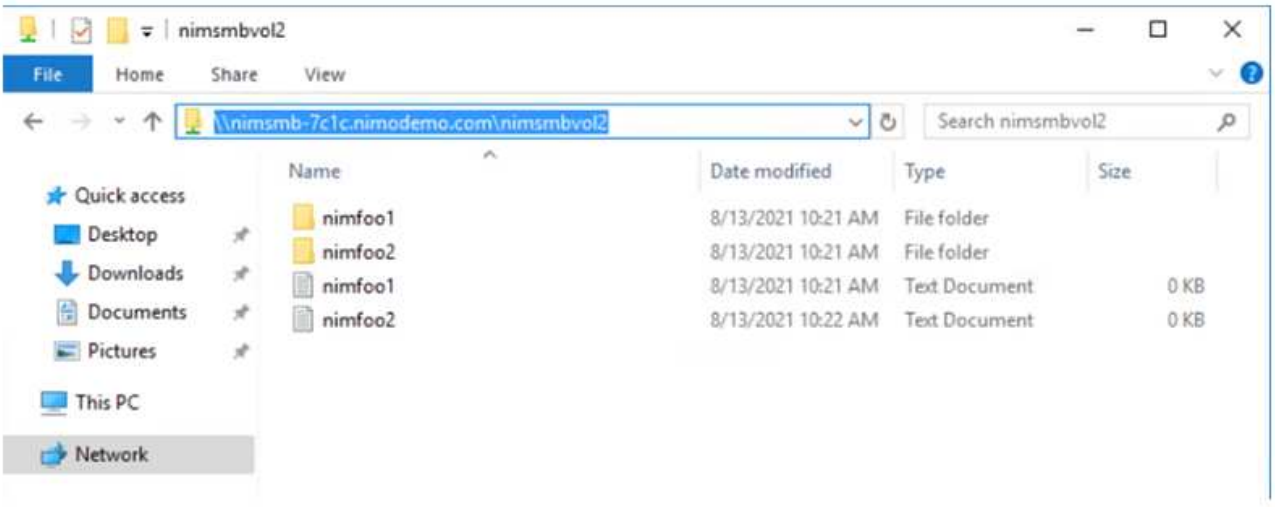


Azure NetApp Filesボリュームのサイズまたはクォータ別のパフォーマンスの詳細については、以下を参照してください。"Azure NetApp Files のパフォーマンスに関する考慮事項" 。

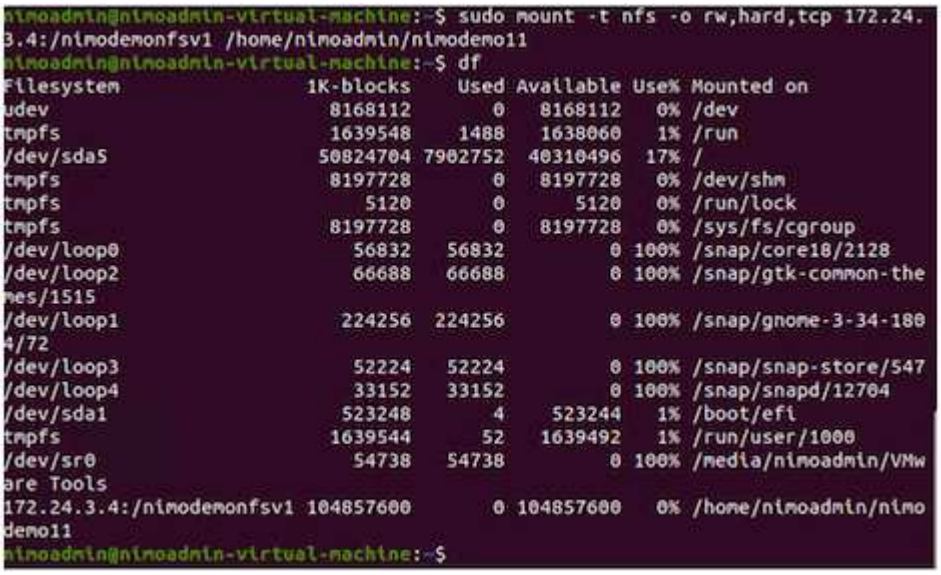
6. 接続が確立されると、ボリュームをマウントしてアプリケーション データに使用できるようになります。

これを実行するには、Azure ポータルから [ボリューム] ブレードをクリックし、マウントするボリュームを選択して、マウント手順にアクセスします。パスをコピーし、[ネットワーク ドライブのマップ] オプションを使用して、Azure VMware Solution SDDC で実行されている VM にボリュームをマウントします。





7. Azure VMware Solution SDDC で実行されている Linux VM に NFS ボリュームをマウントするには、同じプロセスを使用します。ボリュームの再形成または動的サービス レベル機能を使用して、ワークロードの要求を満たします。



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

Cloud Volumes ONTAP（CVO）

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

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

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

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

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

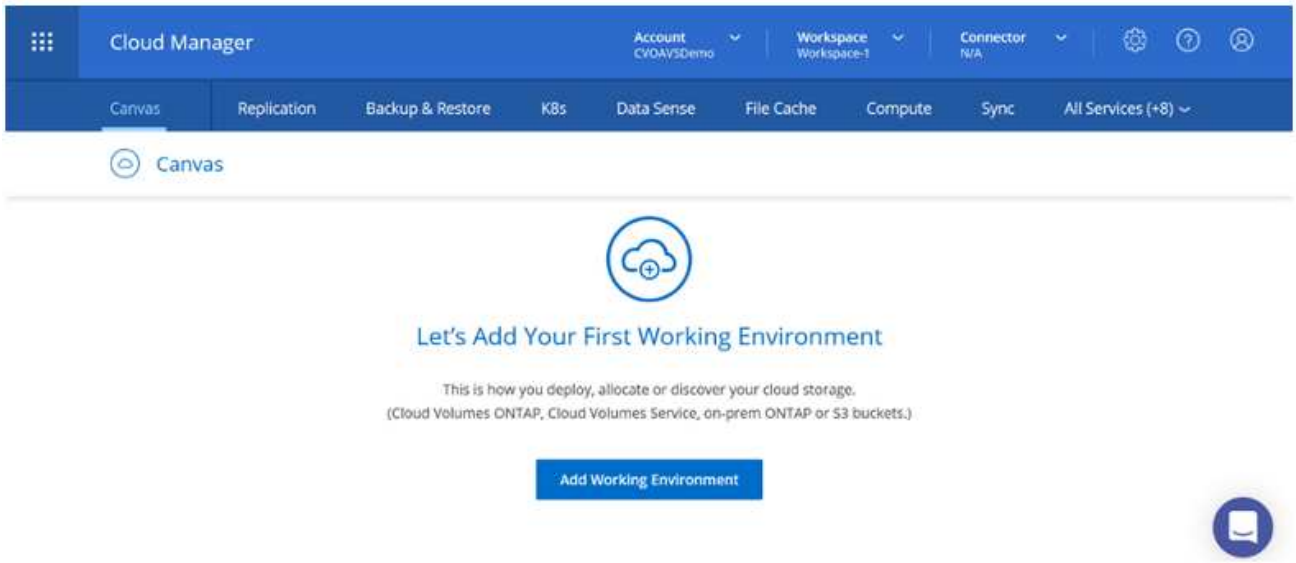
▼ **Azure**に新しい**Cloud Volumes ONTAP**を導入する

Cloud Volumes ONTAP共有と LUN は、Azure VMware Solution SDDC 環境で作成された VM からマウントできます。 Cloud Volumes ONTAP はiSCSI、SMB、NFS プロトコルをサポートしているため、ボリュームは Linux クライアントと Windows クライアントにもマウントできます。 Cloud Volumes ONTAPボリュームは、いくつかの簡単な手順でセットアップできます。

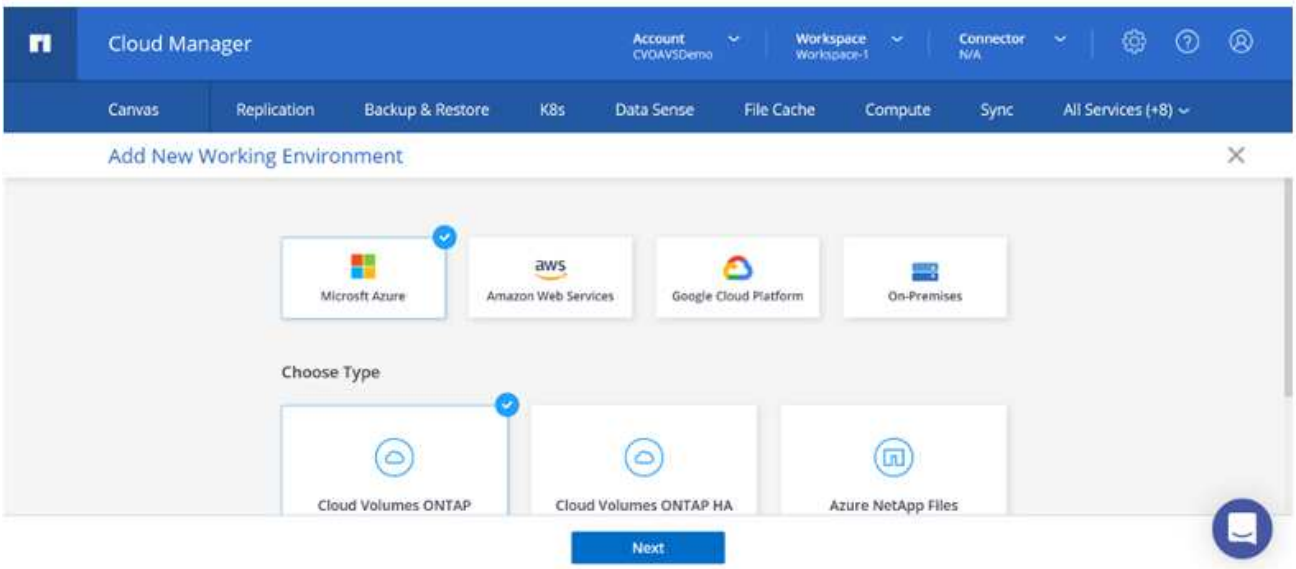
災害復旧または移行の目的でオンプレミス環境からクラウドにボリュームをレプリケートするには、サイト間 VPN または ExpressRoute を使用して Azure へのネットワーク接続を確立します。オンプレミスからCloud Volumes ONTAPへのデータの複製については、このドキュメントの範囲外です。オンプレミスとCloud Volumes ONTAPシステム間でデータを複製するには、"システム間のデータ複製の設定" 。

"Cloud Volumes ONTAPサイザー" を使用して、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サイザーの入力として使用します。

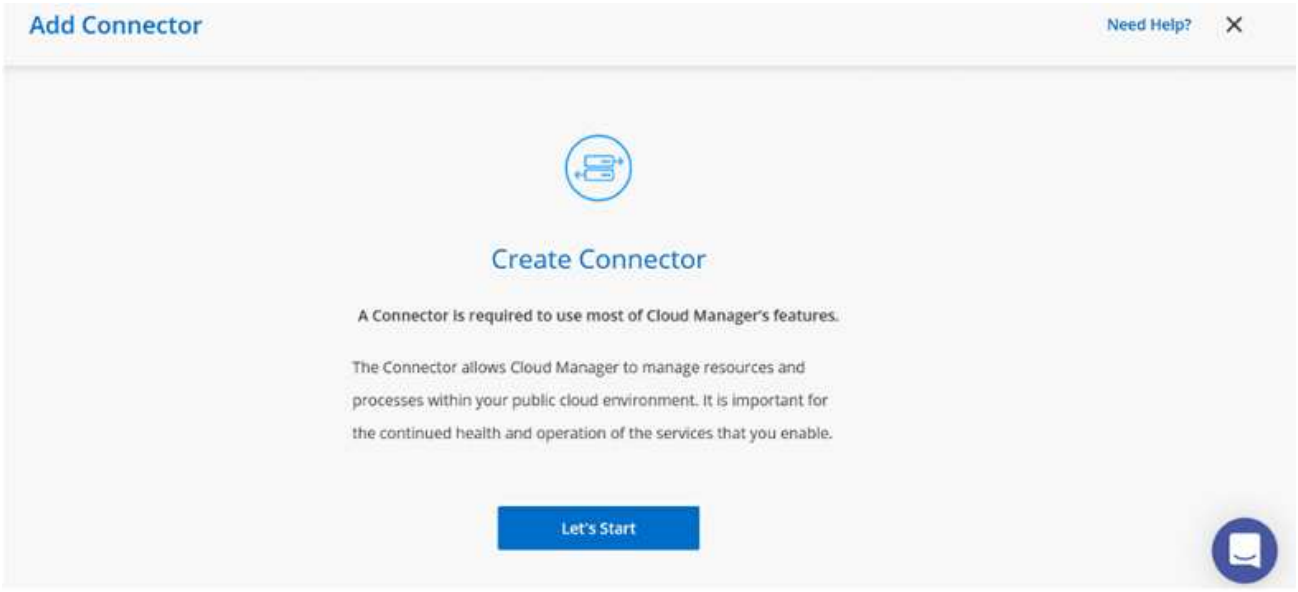
1. NetApp Cloud Central にログインすると、Fabric View 画面が表示されます。 Cloud Volumes ONTAPタブを見つけて、「Go to Cloud Manager」を選択します。ログインすると、Canvas 画面が表示されます。



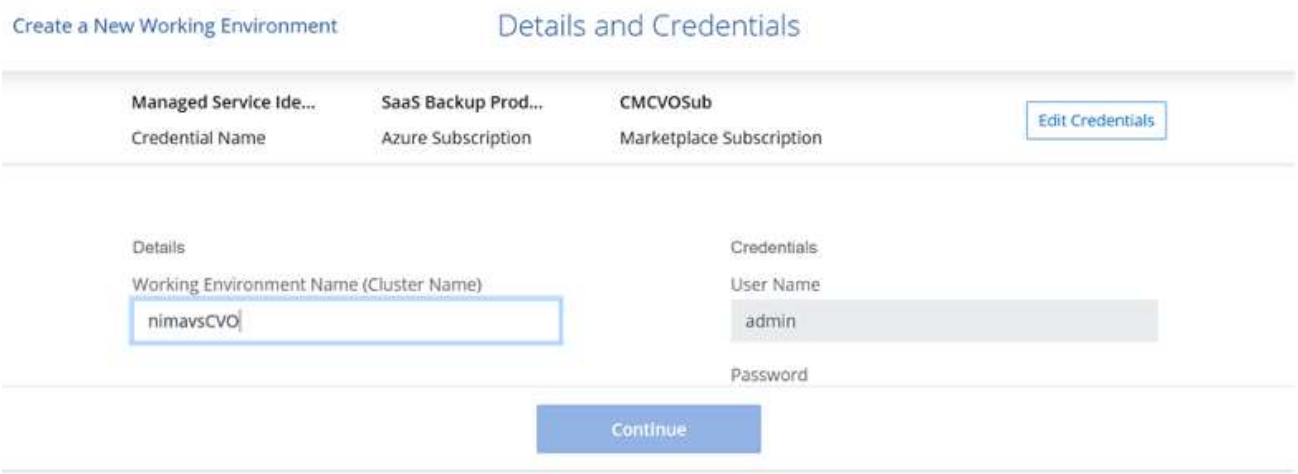
2. Cloud Manager のホームページで、「作業環境の追加」をクリックし、クラウドとして Microsoft Azure を選択し、システム構成のタイプを選択します。



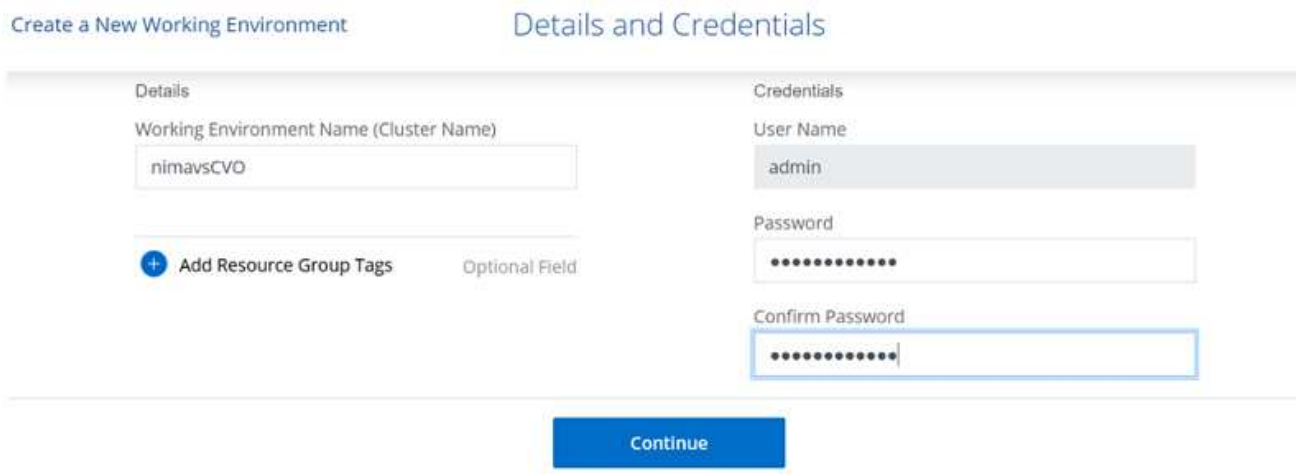
3. 最初のCloud Volumes ONTAP作業環境を作成するときに、Cloud Manager によってコネクタをデプロイするように求められます。



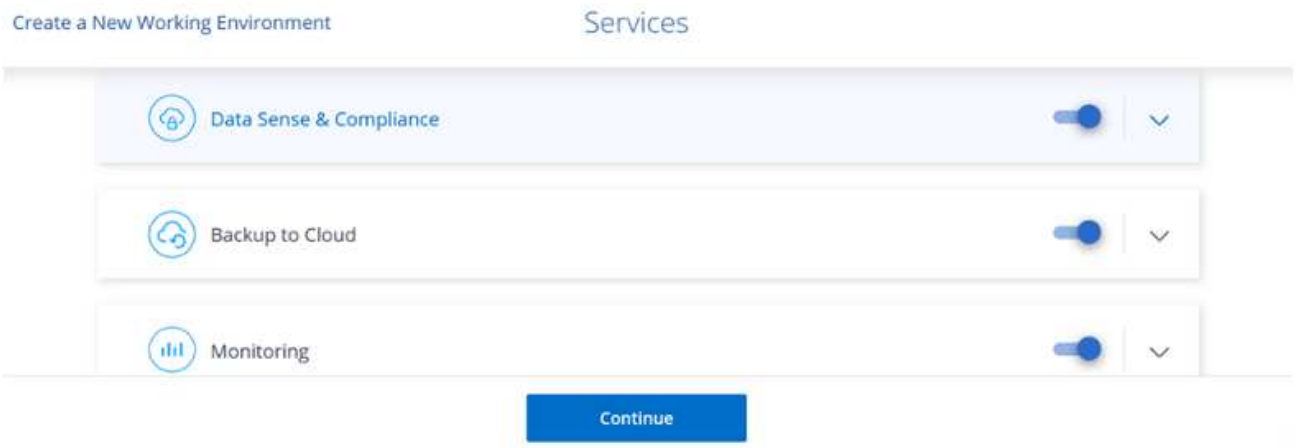
4. コネクタが作成されたら、詳細および資格情報フィールドを更新します。



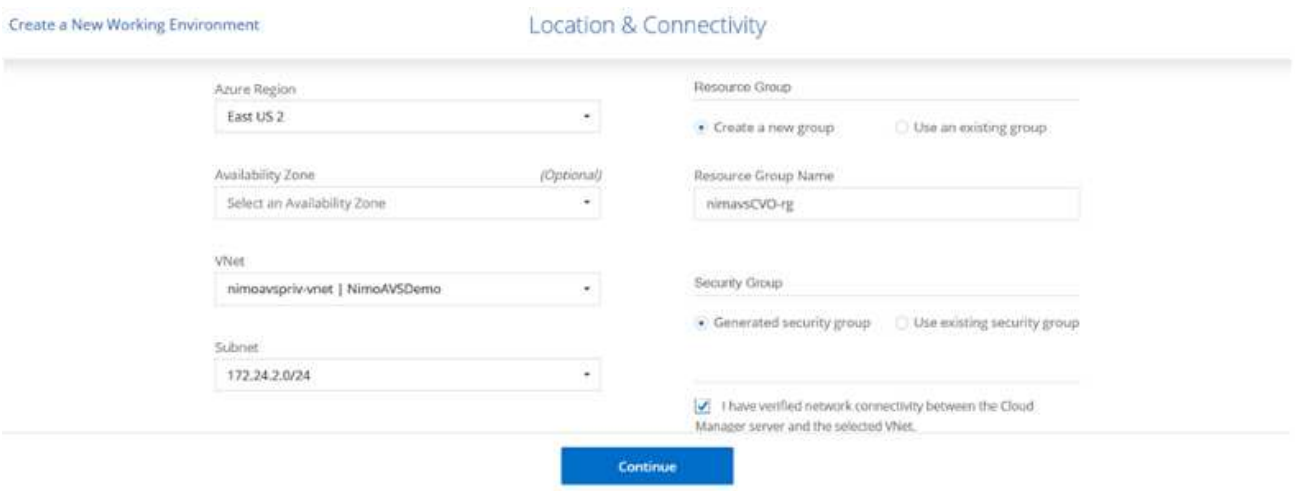
5. 環境名や管理者の資格情報など、作成する環境の詳細を指定します。オプション パラメーターとして、Azure 環境のリソース グループ タグを追加します。完了したら、「続行」をクリックします。



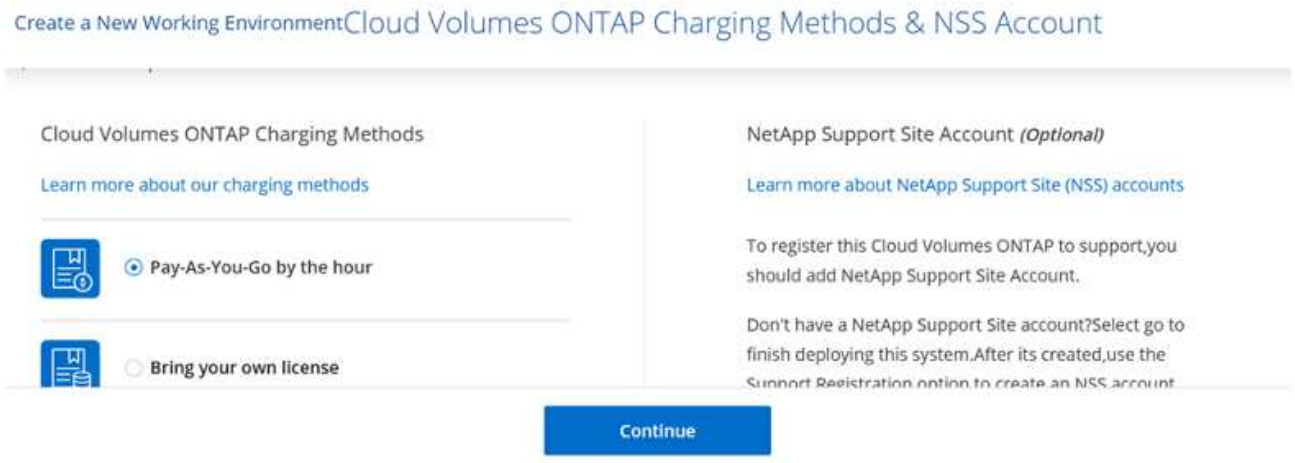
6. Cloud Volumes ONTAPの展開向けに、NetApp Data Classification、NetApp Backup and Recovery 、Data Infrastructure Insightsなどのアドオンサービスを選択します。サービスを選択し、「続行」をクリックします。



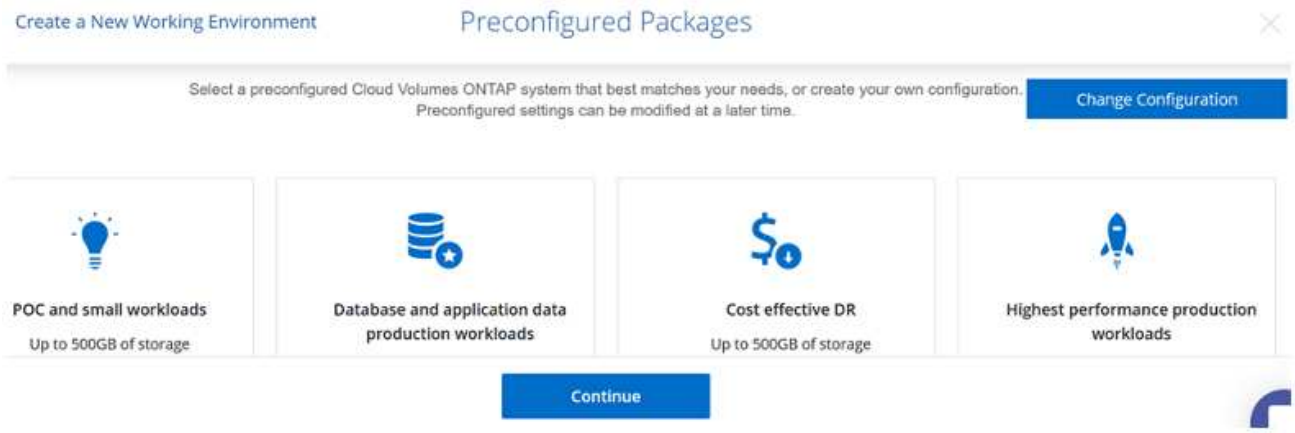
7. Azure の場所と接続を構成します。使用する Azure リージョン、リソース グループ、VNet、サブネットを選択します。



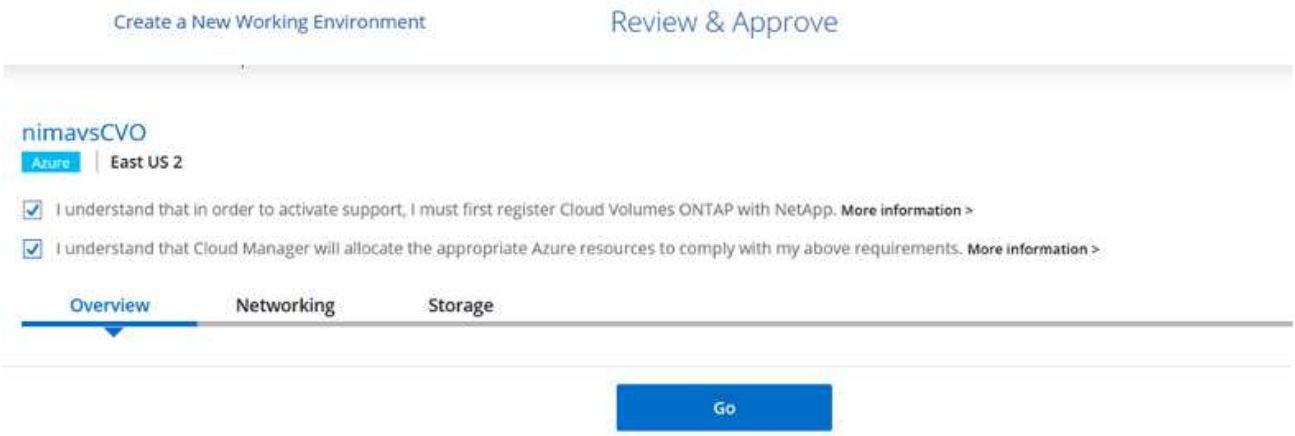
8. 既存のライセンスを使用する場合は、ライセンス オプション (Pay-As-You-Go または BYOL) を選択します。この例では、Pay-As-You-Go オプションが使用されています。



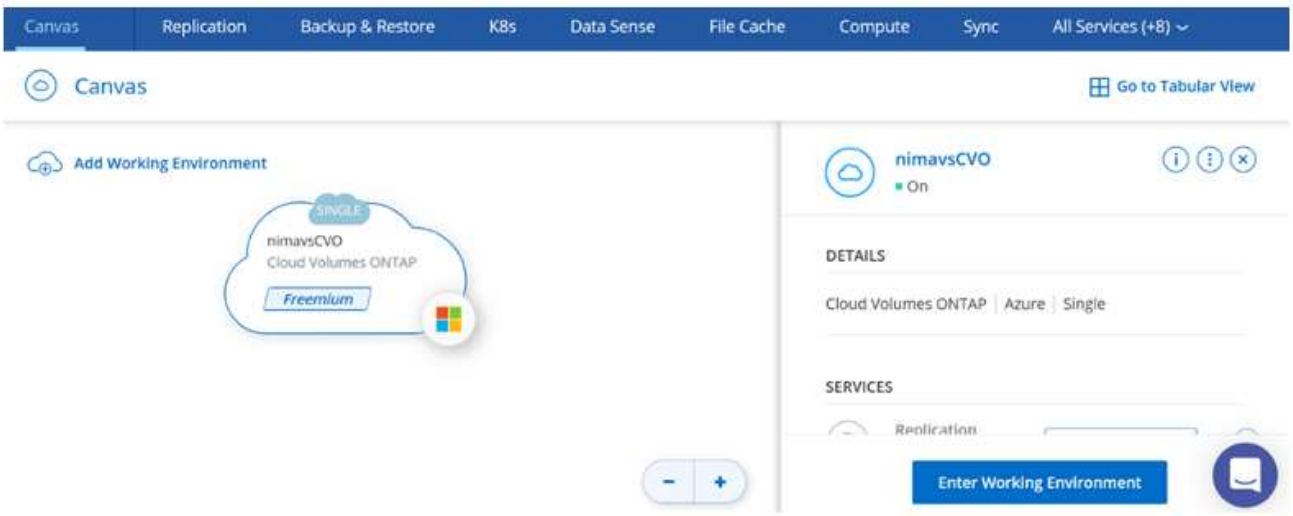
9. さまざまな種類のワークロードに使用できる、事前構成された複数のパッケージから選択します。



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。

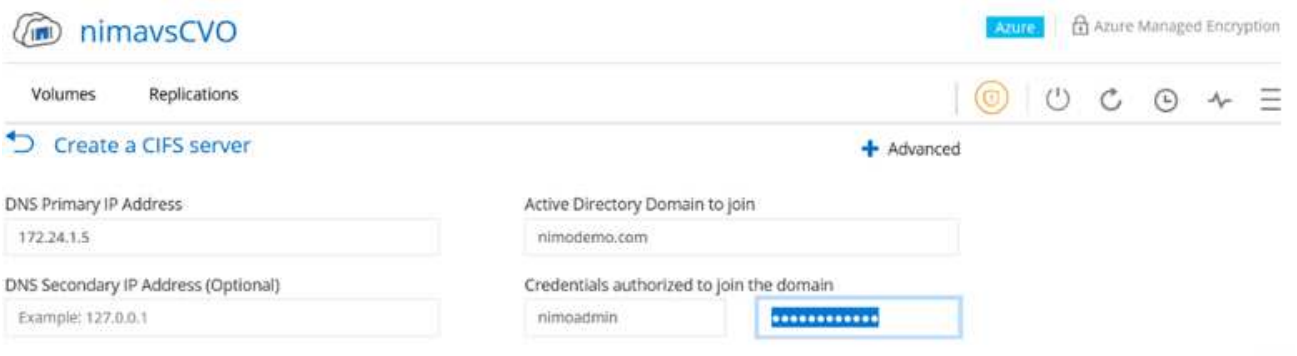


11. Cloud Volumes ONTAPがプロビジョニングされると、Canvas ページの作業環境にリストされます。

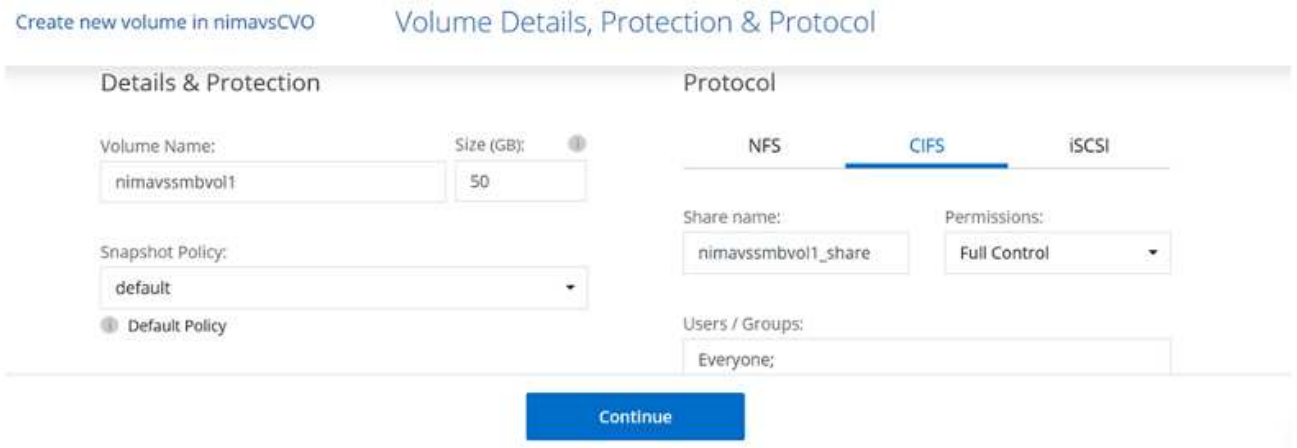


▼ **SMB**ボリュームの追加構成

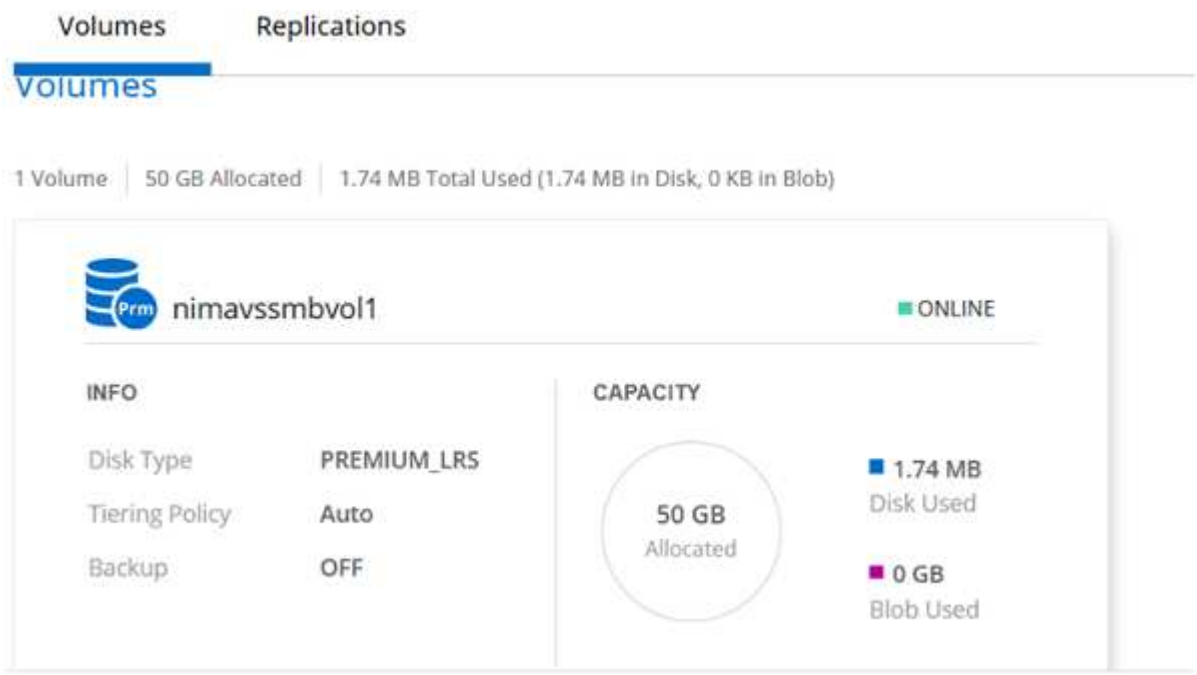
1. 作業環境の準備ができたら、CIFS サーバーが適切な DNS および Active Directory 構成パラメータで構成されていることを確認します。 SMB ボリュームを作成する前にこの手順を実行する必要があります。



2. SMB ボリュームの作成は簡単なプロセスです。ボリュームを作成する CVO インスタンスを選択し、「ボリュームの作成」オプションをクリックします。適切なサイズを選択すると、クラウド マネージャーはそれを含むアグリゲートを選択するか、高度な割り当てメカニズムを使用して特定のアグリゲートに配置します。このデモでは、プロトコルとして SMB が選択されています。

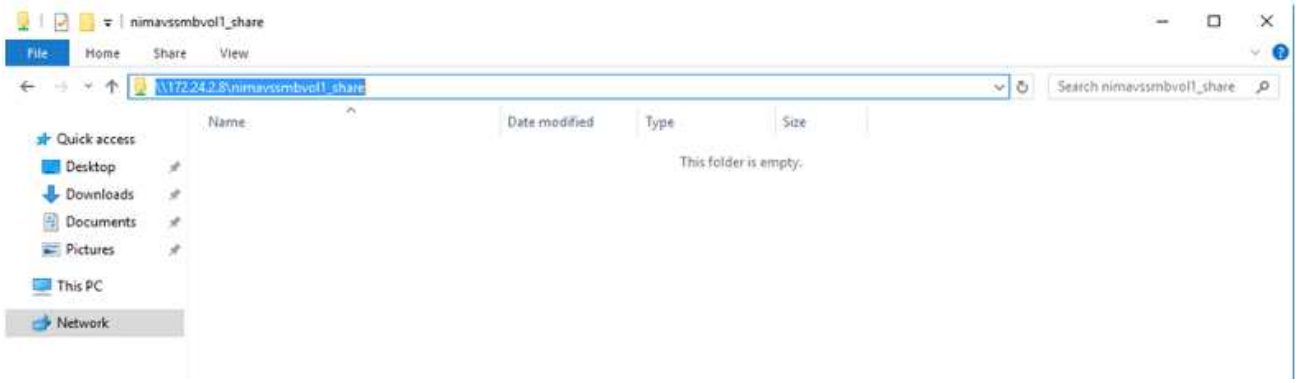


3. ボリュームがプロビジョニングされると、ボリューム ペインで使用できるようになります。 CIFS 共有がプロビジョニングされているため、ユーザーまたはグループにファイルとフォルダーへの権限を与え、それらのユーザーが共有にアクセスしてファイルを作成できることを確認します。ボリュームがオンプレミス環境から複製される場合、ファイルとフォルダの権限はすべてSnapMirrorレプリケーションの一部として保持されるため、この手順は必要ありません。



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

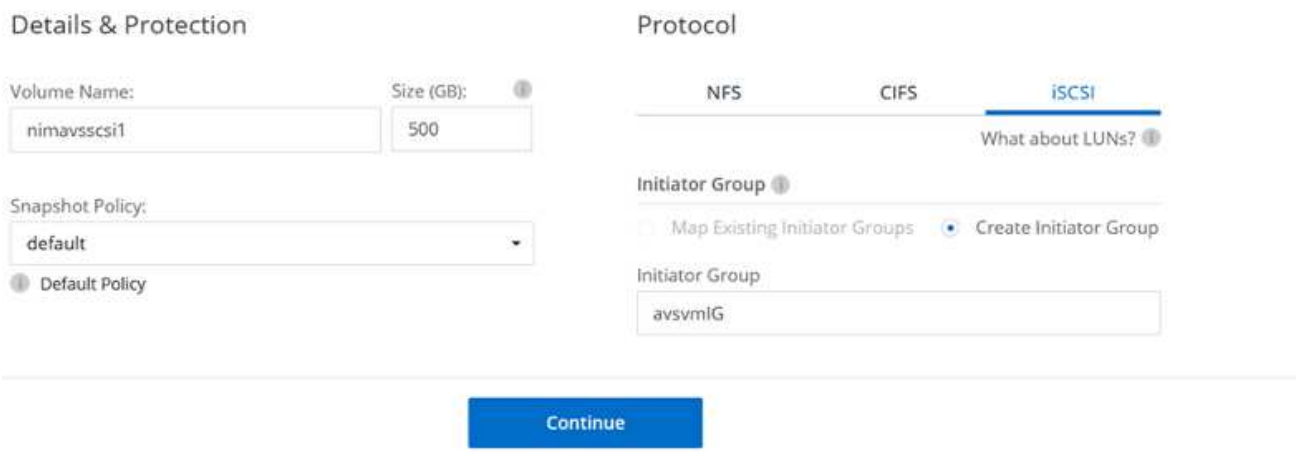




▼ **LUN**をホストに接続する

LUN をホストに接続するには、次の手順を実行します。

1. Canvas ページで、 Cloud Volumes ONTAP作業環境をダブルクリックして、ボリュームを作成および管理します。
2. [ボリュームの追加] > [新しいボリューム] をクリックし、[iSCSI] を選択して [イニシエーター グループの作成] をクリックします。[Continue]をクリックします。



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

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

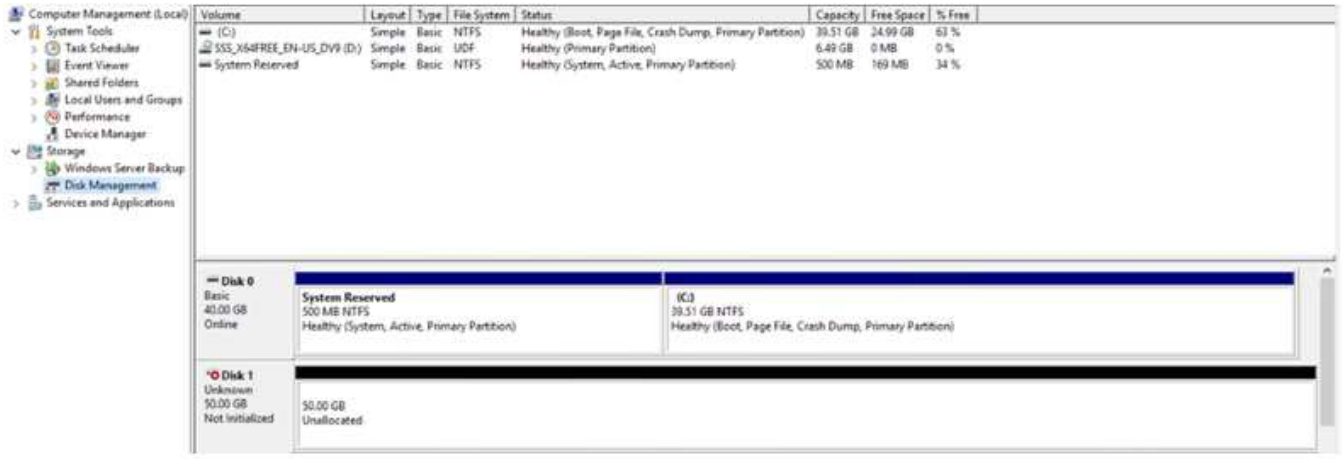
   a. Azure VMware Solution SDDC でホストされている VM に RDP 接続します。
   b. iSCSI イニシエーターのプロパティ ダイアログ ボックスを開きます: サーバー マネージャー > ダッシュボード > ツール > iSCSI イニシエーター。
   c. [検出] タブで、[ポータルの検出] または [ポータルの追加] をクリックし、iSCSI ターゲット ポートの IP アドレスを入力します。
   d. [ターゲット] タブで、検出されたターゲットを選択し、[ログオン] または [接続] をクリックします。
   e. [マルチパスを有効にする]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

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



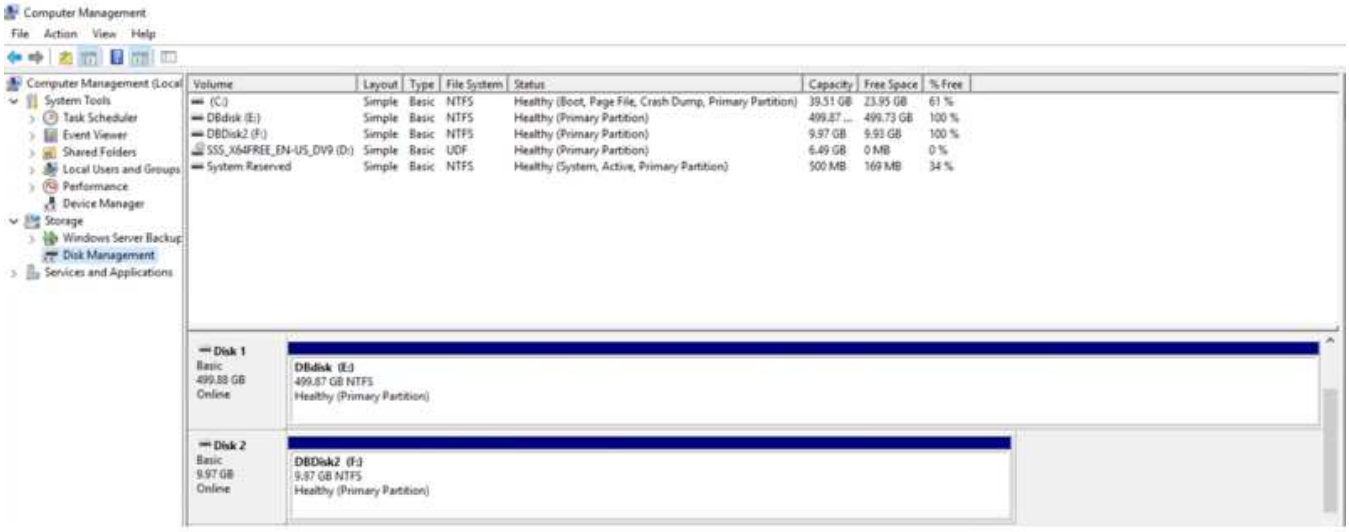
ストレージ仮想マシン (SVM) 上の LUN は、Windows ホストに対してディスクとして表示されます。追加された新しいディスクは、ホストによって自動的に検出されません。次の手順を実行して、手動での再スキャンをトリガーし、ディスクを検出します。

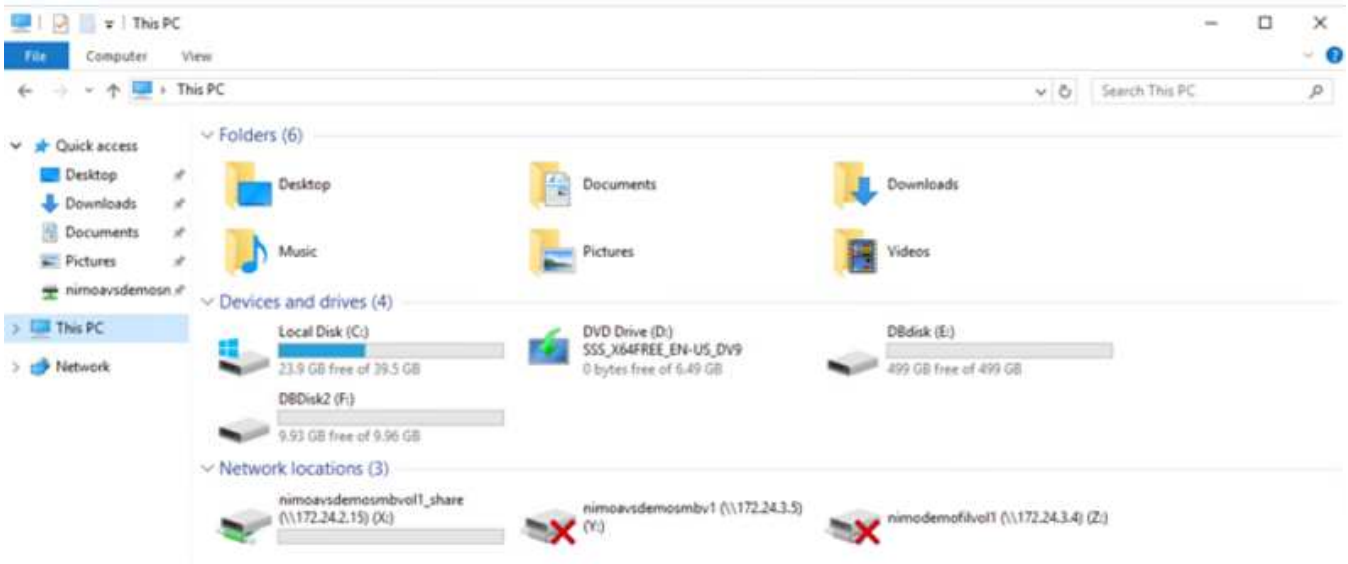
1. Windows のコンピューターの管理ユーティリティを開きます (スタート > 管理ツール > コンピューターの管理)。
2. ナビゲーション ツリーでストレージ ノードを展開します。
3. ディスクの管理をクリックします。
4. [アクション] > [ディスクの再スキャン] をクリックします。



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

1. Windowsの[ディスクの管理]を起動します。
2. LUNを右クリックし、必要なディスクまたはパーティションの種類を選択します。
3. ウィザードの指示に従います。この例では、ドライブE:がマウントされています





Google Cloud VMware Engine: NetAppストレージを使用するためのオプション

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

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

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

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

ゲスト接続ストレージとしての**NetApp CVO**

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

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

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

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

詳細については、"ゲスト接続ストレージとしてのNetApp CVO"

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

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

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

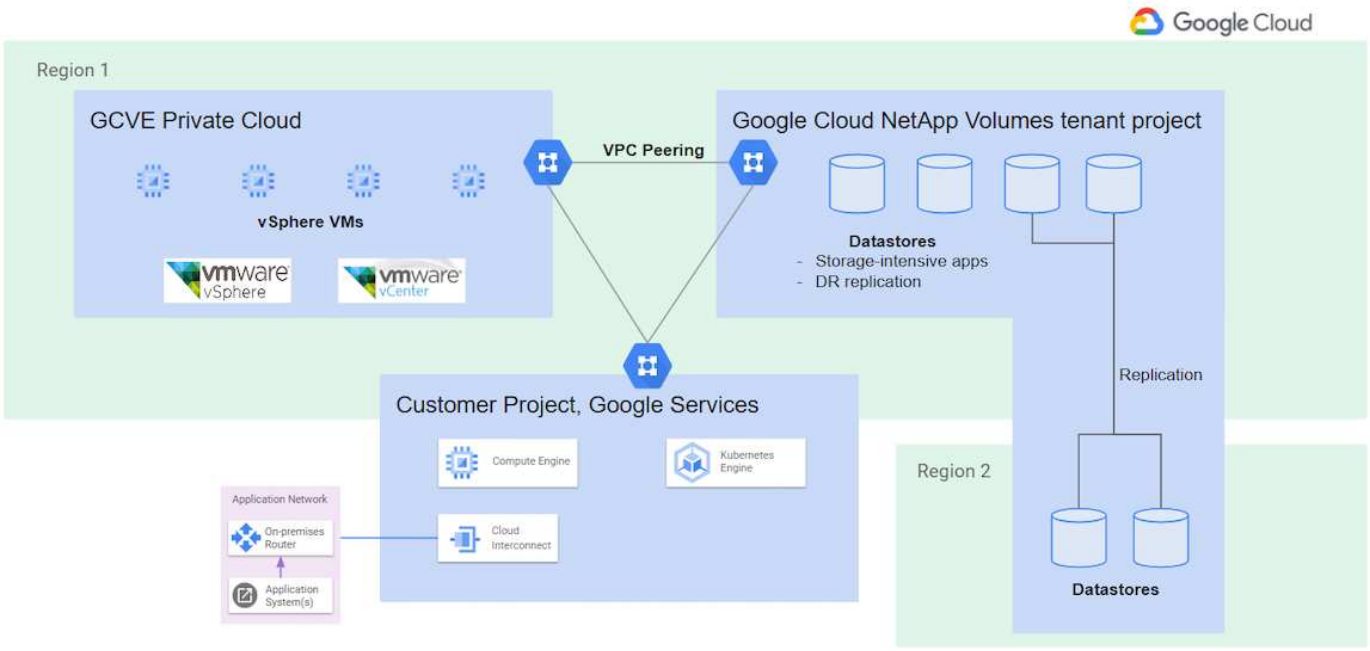
詳細については、"ゲスト接続ストレージとしてのGoogle Cloud NetApp Volumes (NetApp Volumes)"

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

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

概要

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



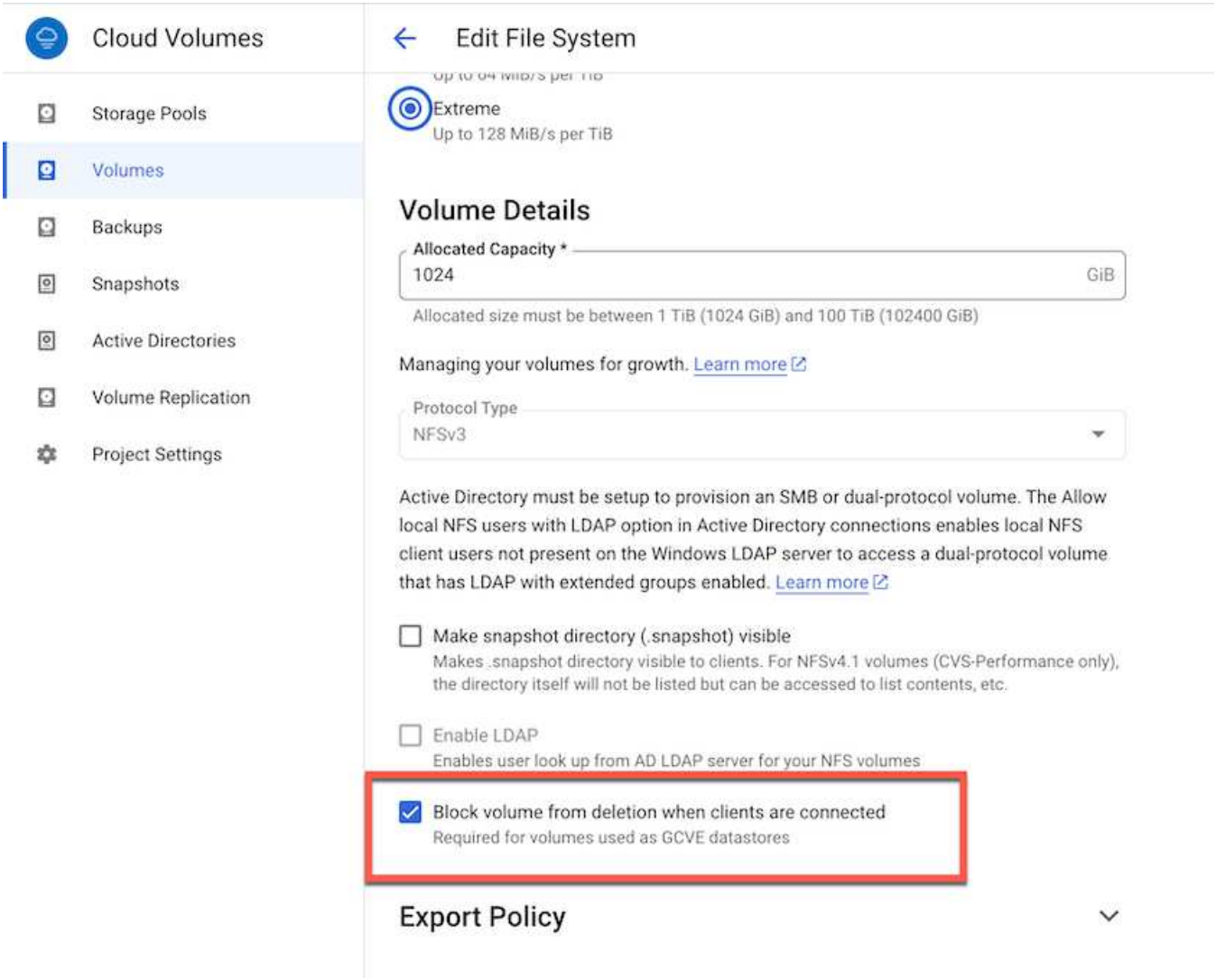
GCVE 上の**Google Cloud NetApp Volumes (NetApp Volumes)** から **NFS** データストアをマウントするためのデプロイメント手順

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

Google Cloud NetApp Volumesボリュームは、次のいずれかでプロビジョニングできます。"Google Cloud Console の使用" "Google Cloud CLI または API を使用する"

▼ **NetApp Volumes**ボリュームを削除不可としてマークする

VMの実行中にボリュームが誤って削除されるのを防ぐため、以下のスクリーンショットに示すように、ボリュームが削除不可としてマークされていることを確認してくださ
い。



詳細については、"NFSボリュームの作成"のドキュメントを参照してください。

▼ **NetApp Volumes Tenant VPC** に対して **GCVE** 上のプライベート接続が存在することを確認します。

NFS データストアをマウントするには、GCVE とNetApp Volumes プロジェクト間にプライベート接続が存在している必要があります。詳細については、"プライベートサービスアクセスの設定方法"

▼ **NFS**データストアをマウントする

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

vSphere ホストは Google によって管理されているため、NFS vSphere API for Array Integration (VAAI) vSphere Installation Bundle (VIB) をインストールする権限はありません。仮想ボリューム (vVol) のサポートが必要な場合は、お知らせください。ジャンボフレームを使用する場合は、"GCP でサポートされる最大 MTU サイズ"

Google Cloud NetApp Volumesによる節約

GCVEでのストレージ要件に対するGoogle Cloud NetApp Volumesによる潜在的なコスト削減について詳しくは、次をご確認ください"NetApp ROI 計算ツール"

参考リンク

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

GCP 向け**NetApp**ストレージ オプション

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

Cloud Volumes ONTAP（CVO）

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

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

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

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

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

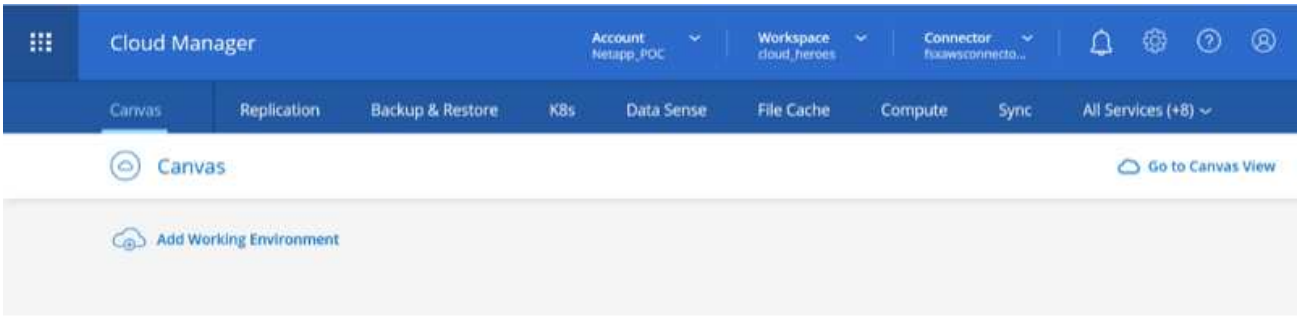
▼ **Google Cloud** に**Cloud Volumes ONTAP**をデプロイする（自分で行う）

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

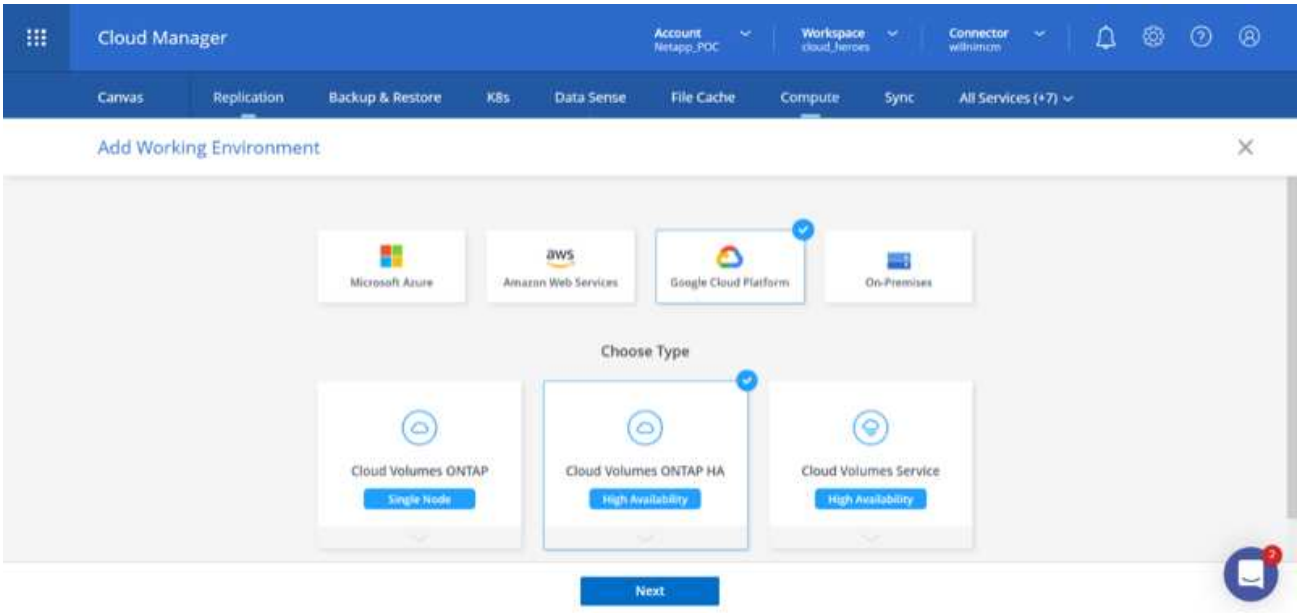
障害復旧または移行の目的でオンプレミス環境からクラウドにボリュームを複製するには、サイト間 VPN または Cloud Interconnect を使用して Google Cloud へのネットワーク接続を確立します。オンプレミスからCloud Volumes ONTAPへのデータの複製については、このドキュメントの範囲外です。オンプレミスとCloud Volumes ONTAPシステム間でデータを複製するには、"システム間のデータ複製の設定" 。

> "Cloud Volumes ONTAPサイザー" を使用して、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サイザーの入力として使用します。

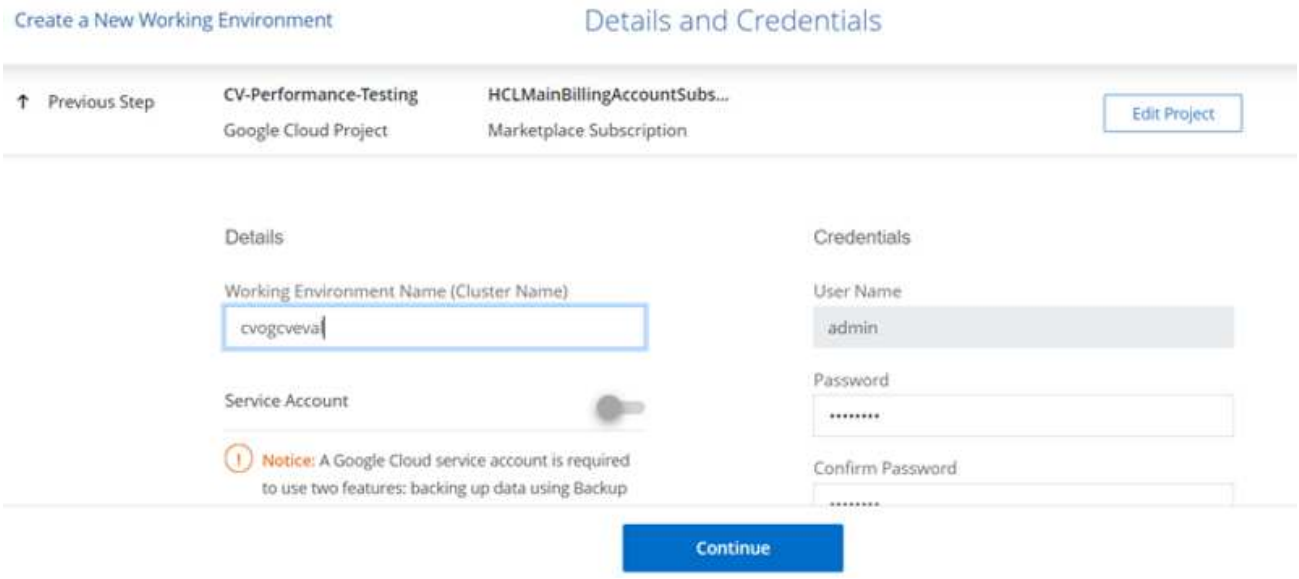
1. NetApp Cloud Central にログインすると、Fabric View 画面が表示されます。 Cloud Volumes ONTAPタブを見つけて、「Go to Cloud Manager」を選択します。ログインすると、Canvas 画面が表示されます。



2. Cloud Manager Canvas タブで、「作業環境の追加」をクリックし、クラウドとして Google Cloud Platform を選択し、システム構成のタイプを選択します。次に、「次へ」をクリックします。



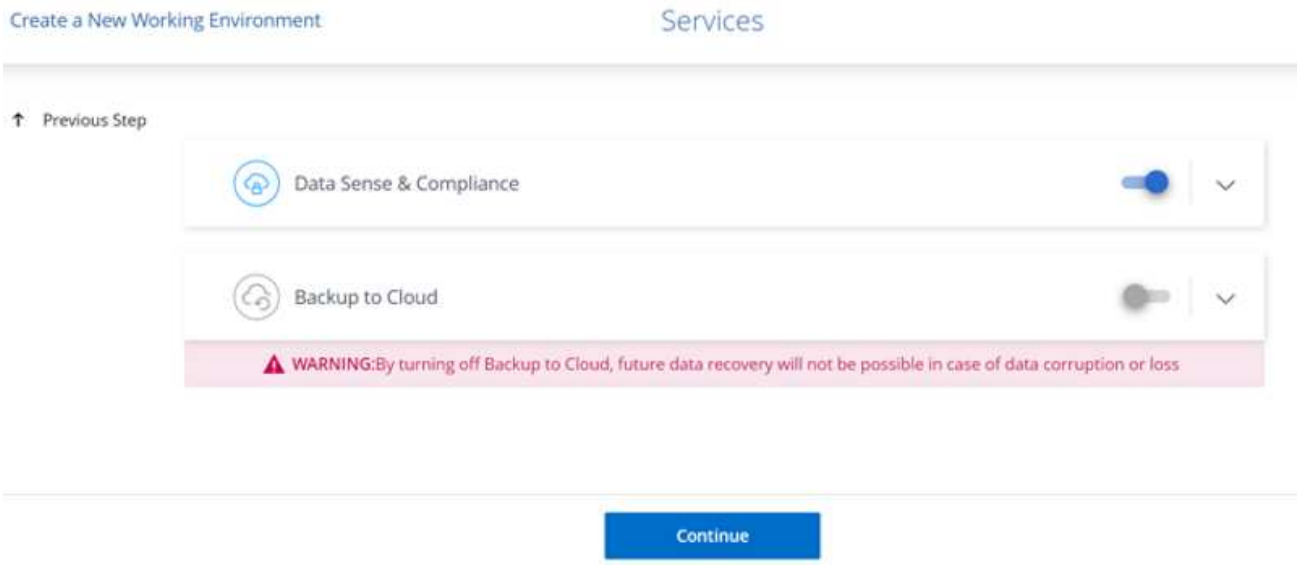
3. 環境名や管理者の資格情報など、作成する環境の詳細を指定します。完了したら、「続行」をクリックします。



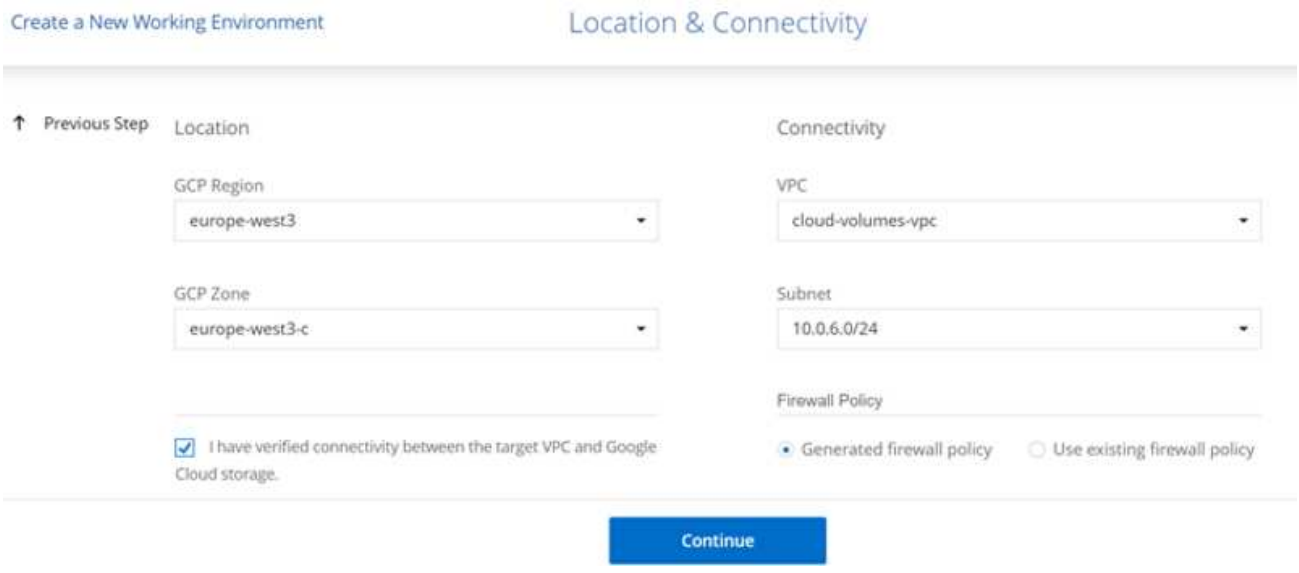
4. Data Sense & Compliance や Backup to Cloud など、 Cloud Volumes ONTAPデプロイメントのアドオ

ン サービスを選択または選択解除します。次に、「続行」をクリックします。

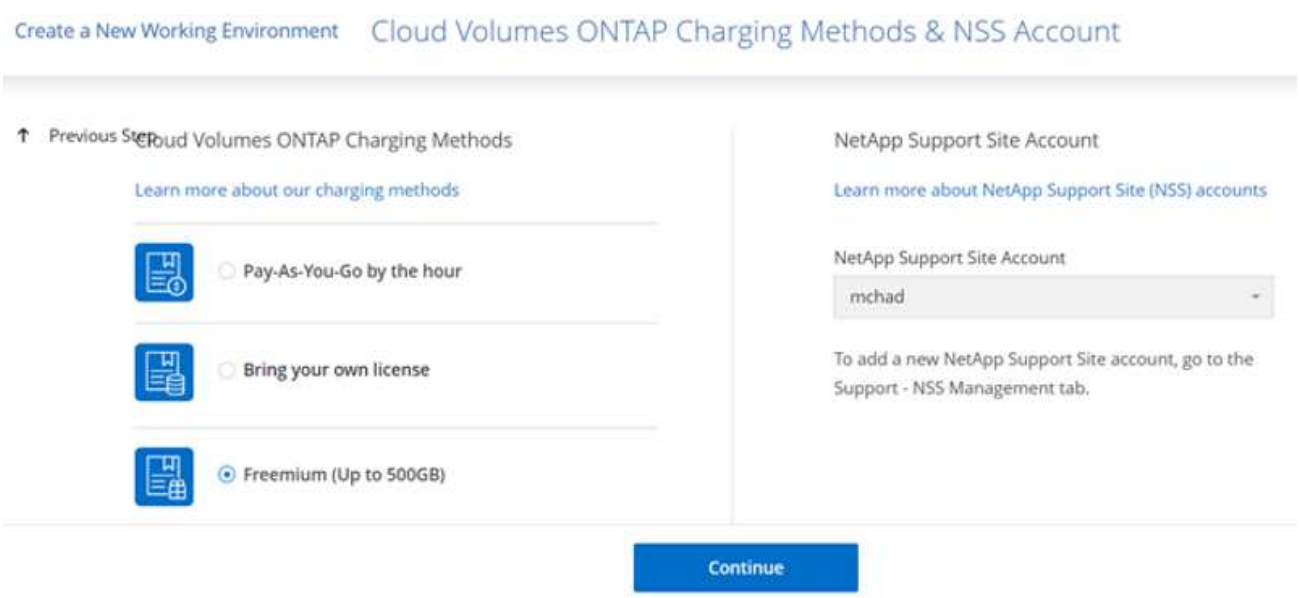
ヒント: アドオン サービスを非アクティブ化すると、確認のポップアップ メッセージが表示されます。アドオン サービスは CVO の導入後に追加/削除できますが、コストを避けるために最初から必要ない場合は選択解除することを検討してください。



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

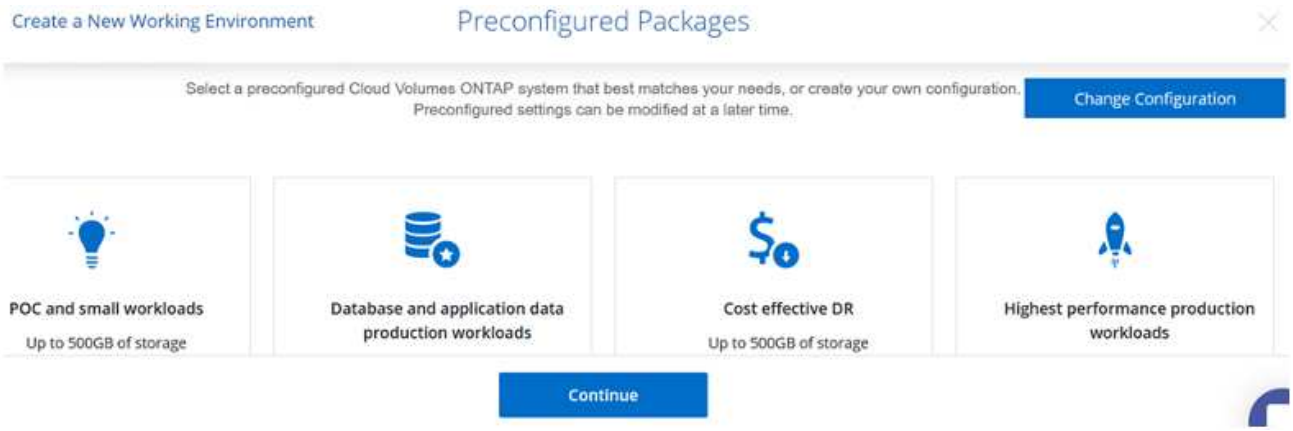


6. 既存のライセンスを使用する場合は、ライセンス オプション (Pay-As-You-Go または BYOL) を選択します。この例では、Freemium オプションが使用されています。次に、「続行」をクリックします。

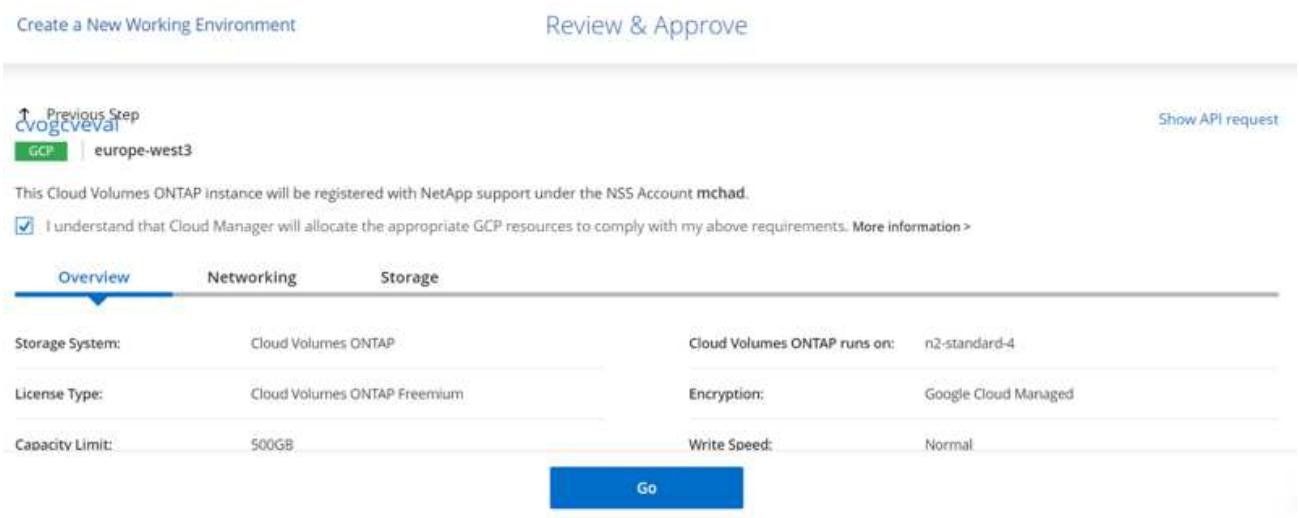


7. VMware Cloud on AWS SDDC で実行されている VM に展開されるワークロードのタイプに基づいて、利用可能ないくつかの事前構成済みパッケージから選択します。

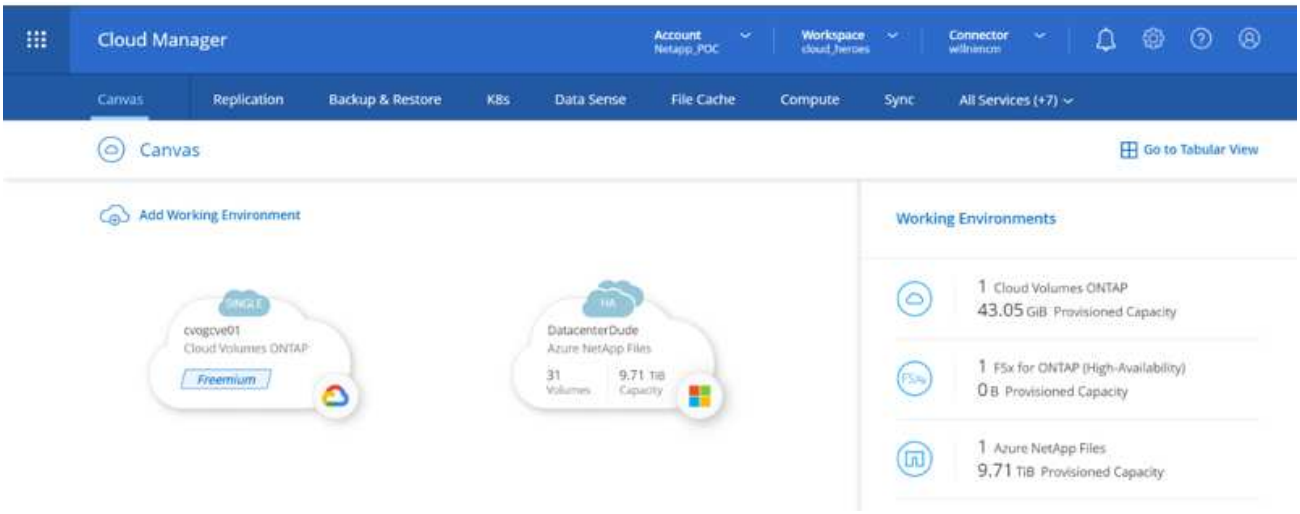
   ヒント: タイルの上にマウスを移動すると詳細が表示されます。また、[構成の変更] をクリックして CVO コンポーネントとONTAPバージョンをカスタマイズすることもできます。



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



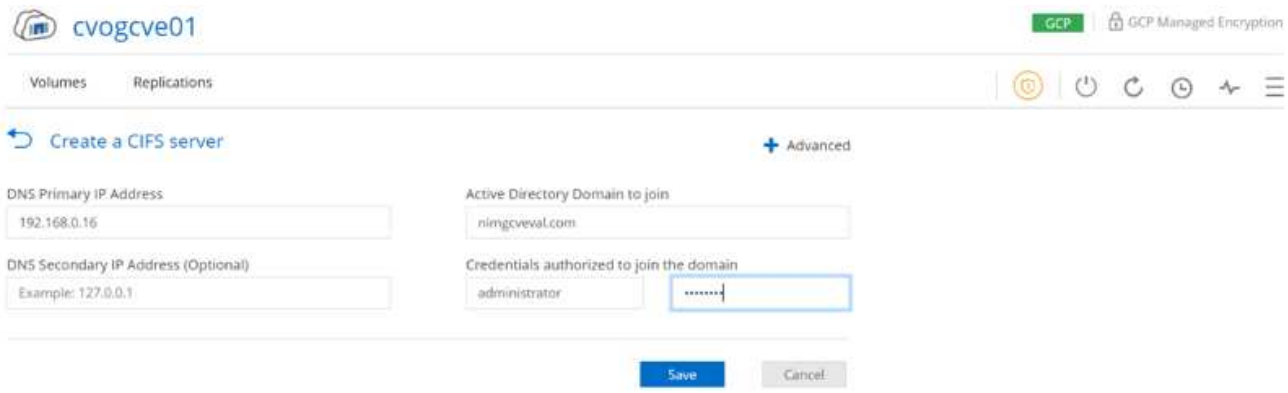
9. Cloud Volumes ONTAPがプロビジョニングされると、Canvas ページの作業環境にリストされます。



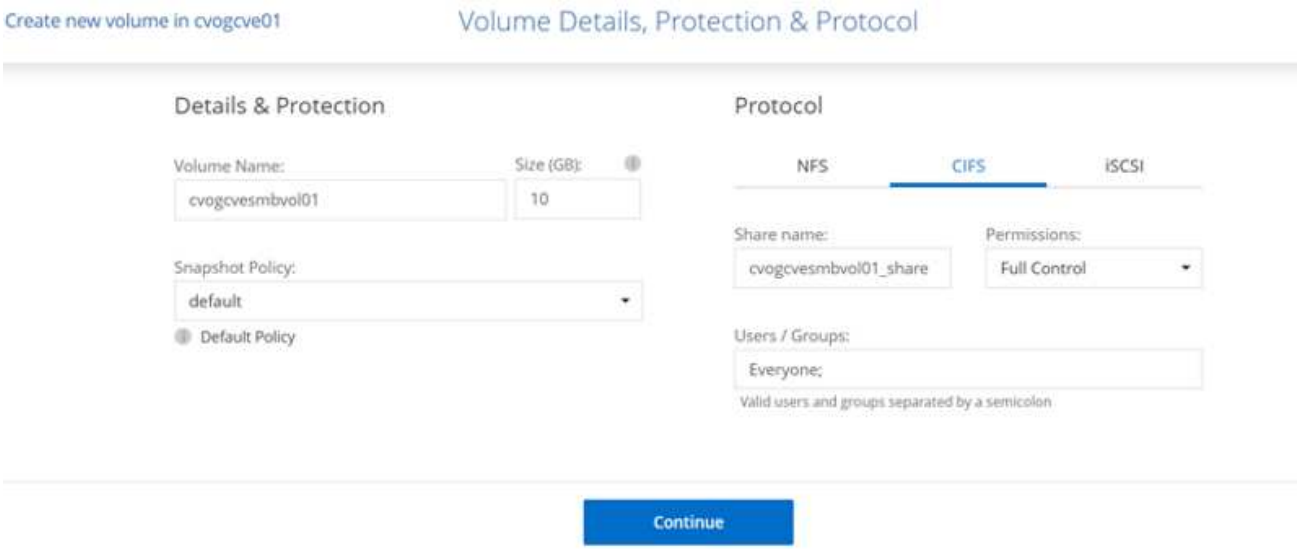
▼ **SMB**ボリュームの追加構成

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

   ヒント: メニュー アイコン (⁰) をクリックし、[詳細設定] を選択してその他のオプションを表示し、[CIFS セットアップ] を選択します。



2. SMB ボリュームの作成は簡単なプロセスです。 Canvas で、 Cloud Volumes ONTAP作業環境をダブルクリックしてボリュームを作成および管理し、[ボリュームの作成] オプションをクリックします。適切なサイズを選択すると、クラウド マネージャーはそれを含むアグリゲートを選択するか、高度な割り当てメカニズムを使用して特定のアグリゲートに配置します。このデモでは、プロトコルとして CIFS/SMB が選択されています。



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

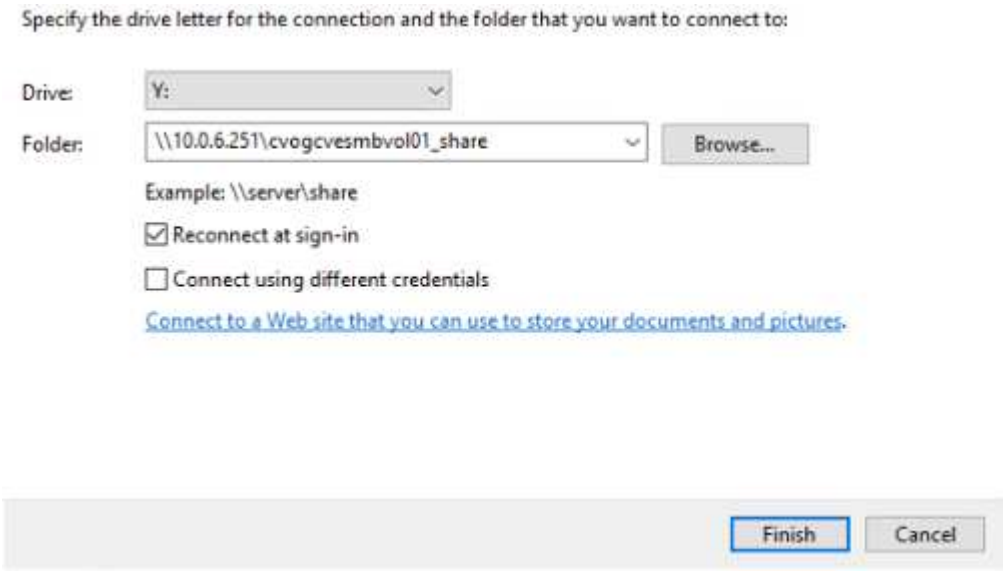
   ヒント: 音量メニュー (⁰) をクリックするとオプションが表示されます。



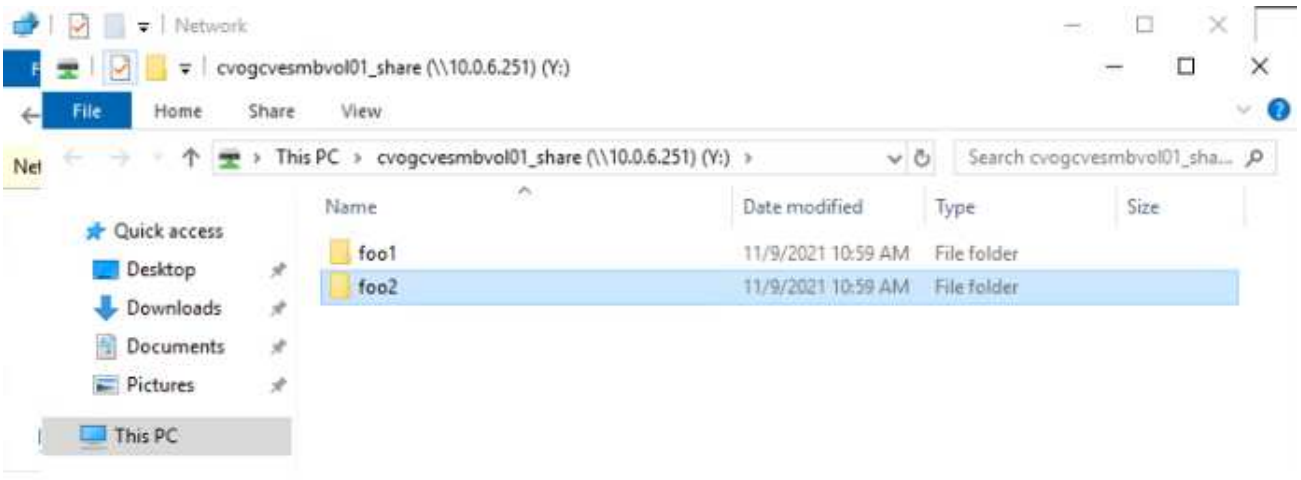
4. ボリュームが作成されたら、マウント コマンドを使用してボリュームの接続手順を表示し、Google Cloud VMware Engine 上の VM から共有に接続します。



5. 次のパスをコピーし、ネットワーク ドライブのマップ オプションを使用して、Google Cloud VMware Engine で実行されている VM にボリュームをマウントします。



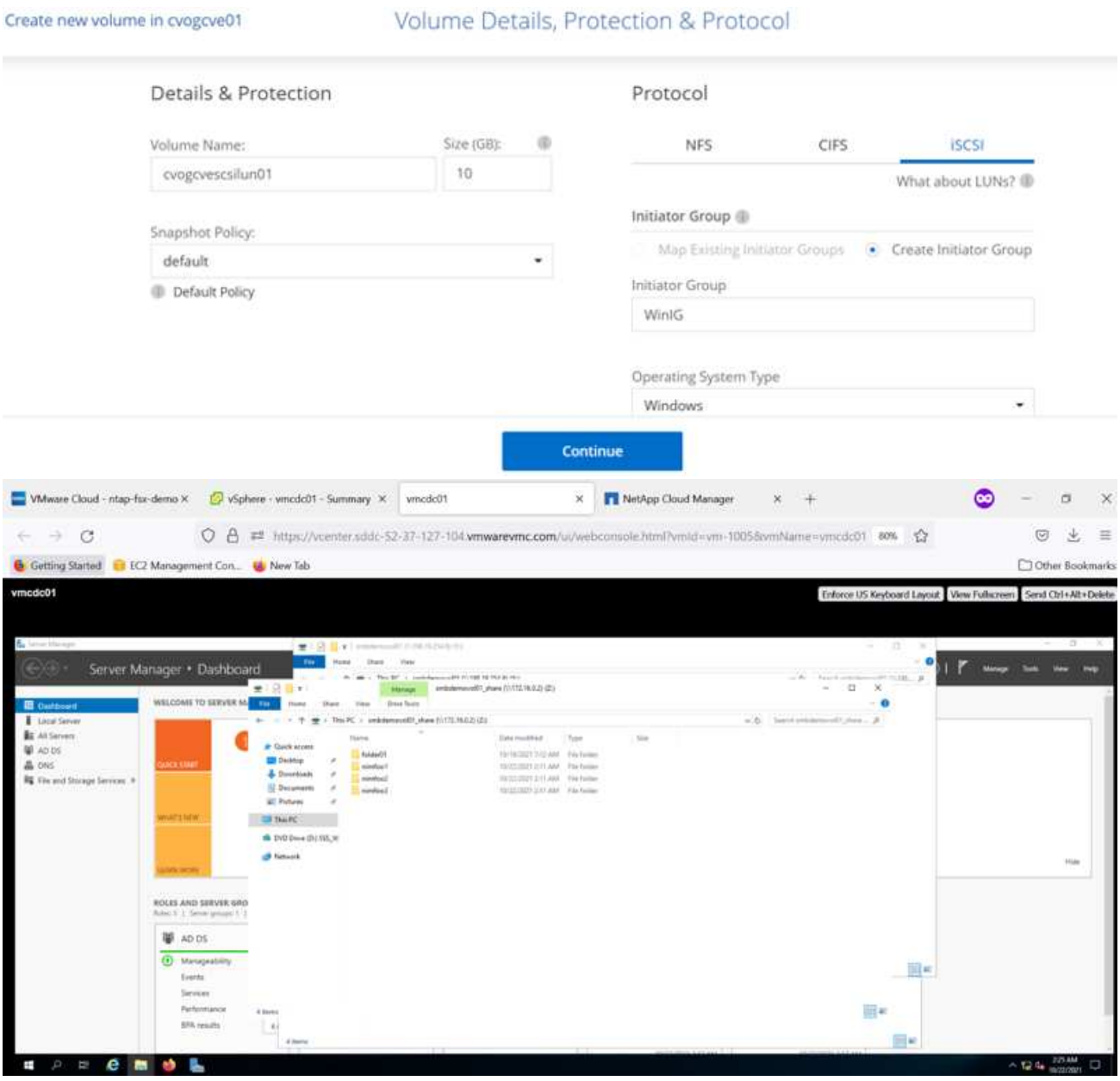
一度マップすると、簡単にアクセスできるようになり、それに応じて NTFS アクセス許可を設定できます。



▼ **Cloud Volumes ONTAP**上の**LUN**をホストに接続する

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

1. Canvas ページで、 Cloud Volumes ONTAP作業環境をダブルクリックして、ボリュームを作成および管理します。
2. [ボリュームの追加] > [新しいボリューム] をクリックし、[iSCSI] を選択して [イニシエーター グループの作成] をクリックします。[Continue]をクリックします。



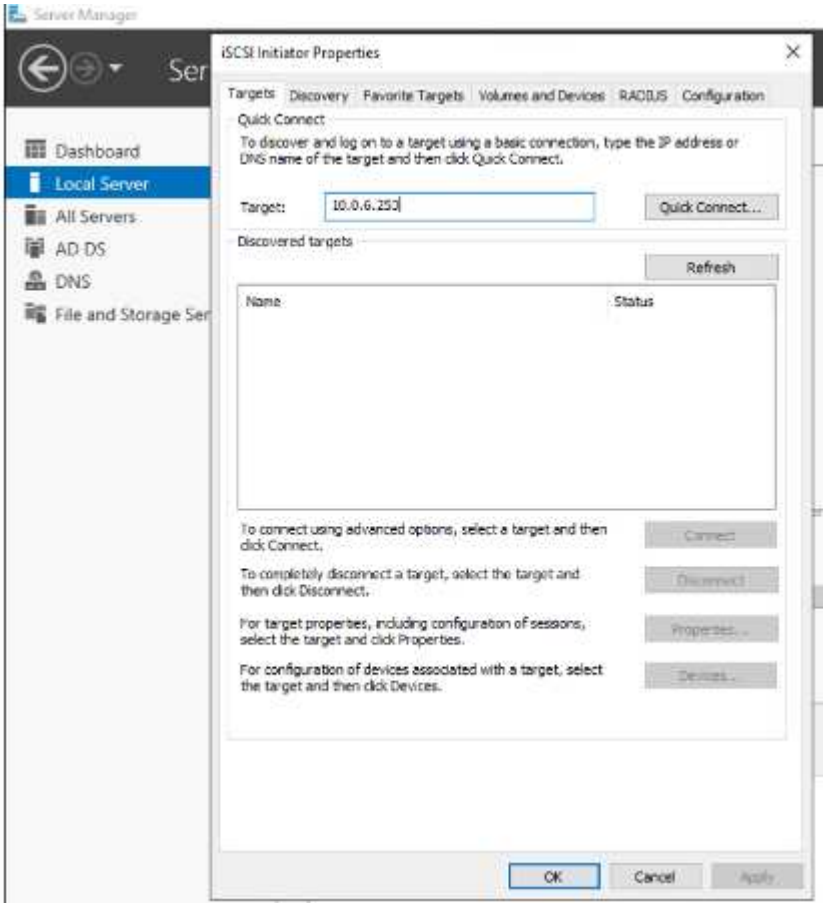
3. ボリュームがプロビジョニングされたら、ボリューム メニュー (º) を選択し、[ターゲット iQN] をクリックします。 iSCSI 修飾名 (iQN) をコピーするには、[コピー] をクリックします。ホストから LUN への iSCSI 接続を設定します。

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

1. Google Cloud VMware Engine でホストされている VM に RDP 接続します。
2. iSCSI イニシエーターのプロパティ ダイアログ ボックスを開きます: サーバー マネージャー > ダッシュボード > ツール > iSCSI イニシエーター。

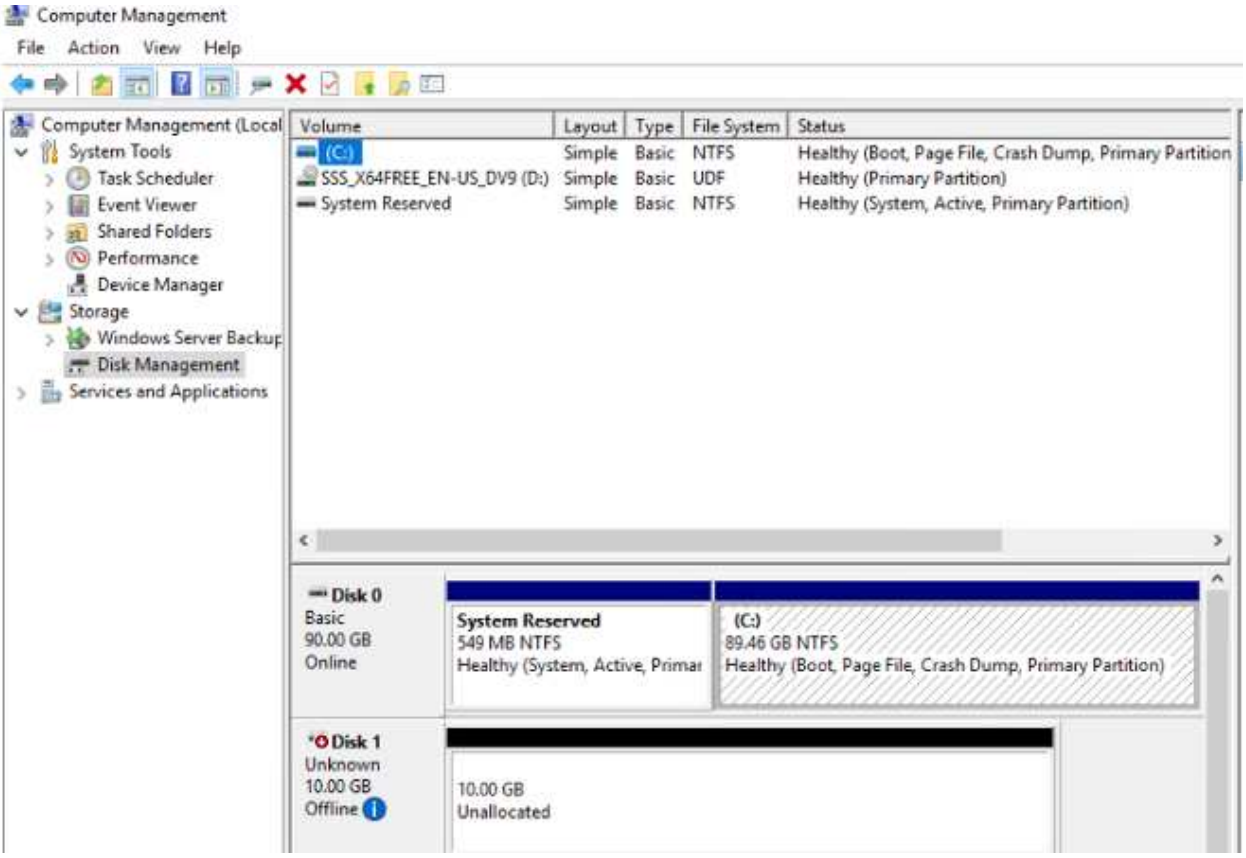
3. [検出] タブで、[ポータルの検出] または [ポータルの追加] をクリックし、iSCSI ターゲット ポートの IP アドレスを入力します。
4. [ターゲット] タブで、検出されたターゲットを選択し、[ログオン] または [接続] をクリックします。
5. [マルチパスを有効にする] を選択し、[コンピューターの起動時にこの接続を自動的に復元する] または [この接続をお気に入りのターゲットのリストに追加する] を選択します。[Advanced]をクリックします。

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



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

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

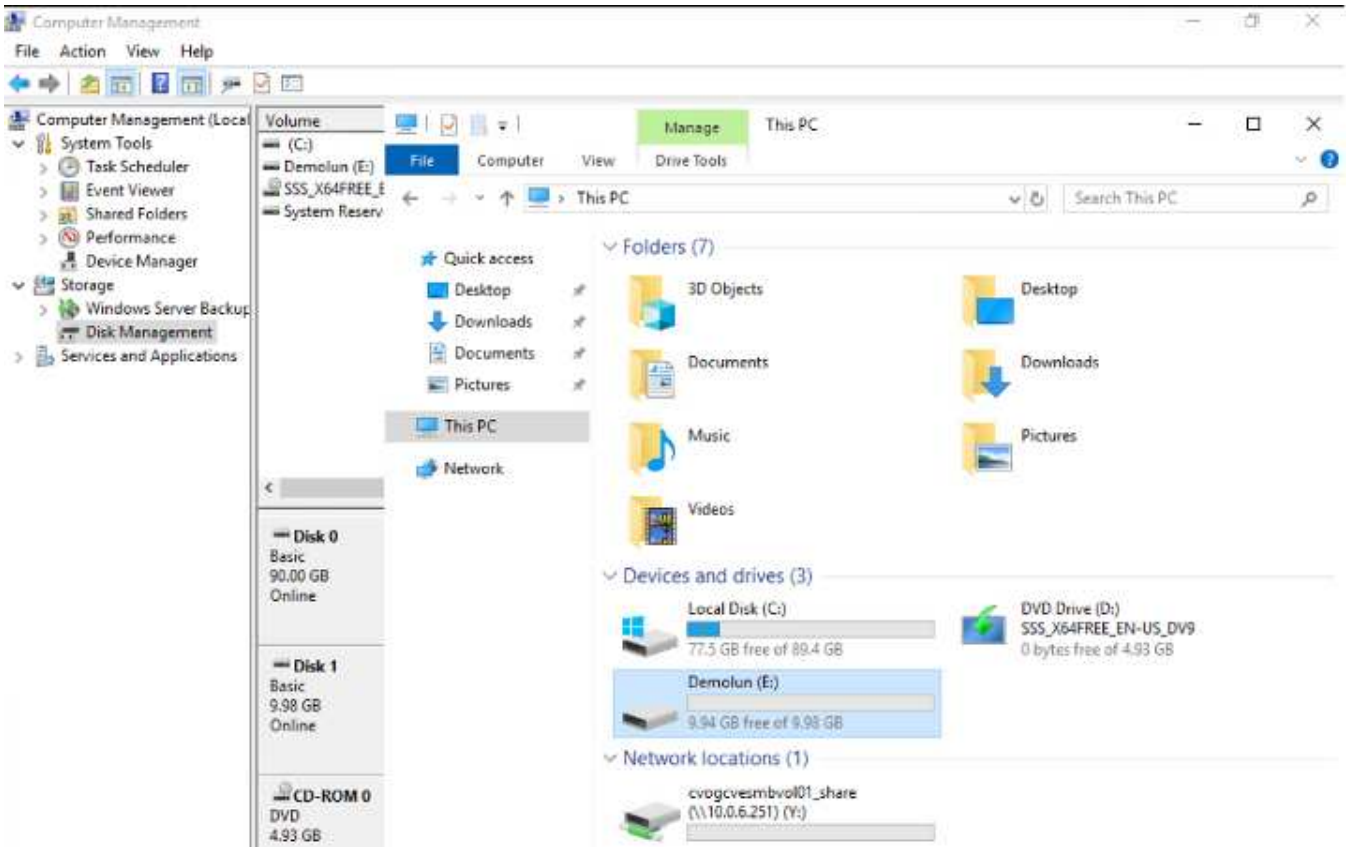


Windowsホストから初めてアクセスした時点では、新しいLUNにはパーティションやファイルシステムは設定されていません。LUN を初期化し、オプションで次の手順を実行して、LUN をファイル システムでフォーマットします。

a. Windowsの[ディスクの管理]を起動します。

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種類を選択します。

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



Linux クライアントで、iSCSI デーモンが実行されていることを確認します。 LUN がプロビジョニングされたら、Ubuntu を例として iSCSI 構成に関する詳細なガイダンスをここで参照してください。確認するには、シェルから lsblk cmd を実行します。

```
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
```

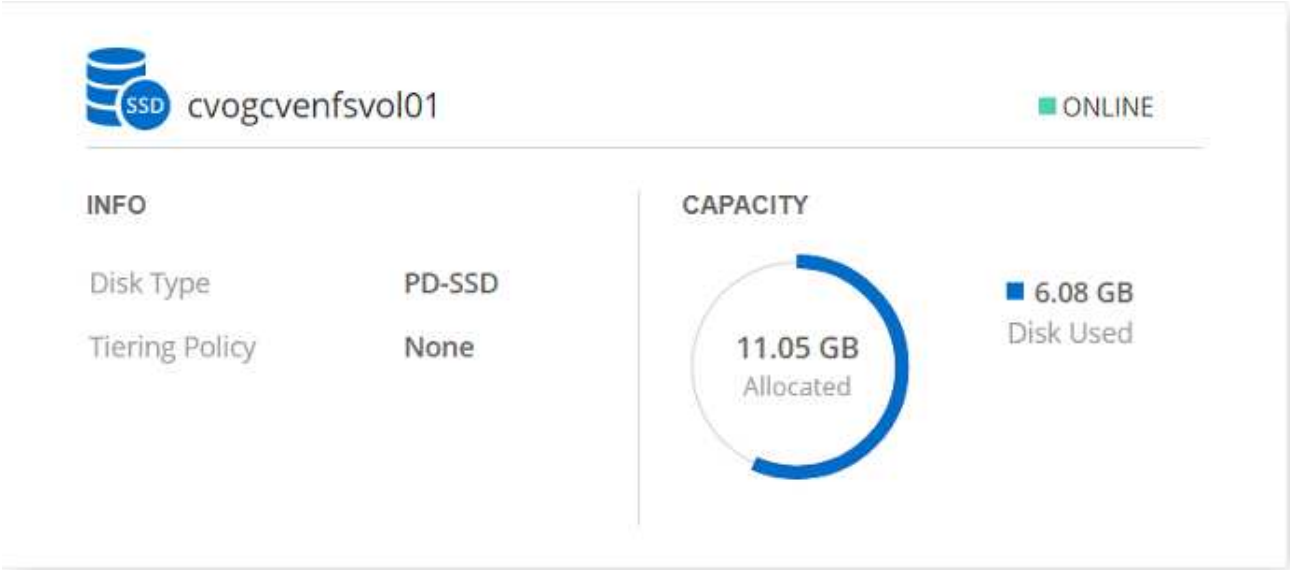
```
niyaz@nimubu01:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           394M  1.5M  392M   1% /run
/dev/sda5        16G  7.6G  6.9G  53% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs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

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

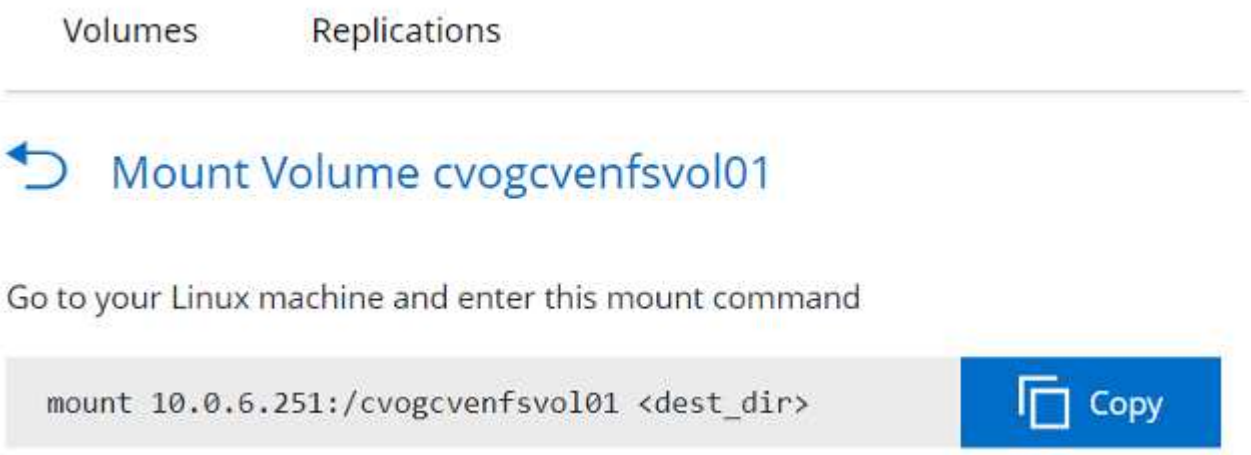
Google Cloud VMware Engine 内の VM からCloud Volumes ONTAP （DIY）ファイル システムをマウントするには、次の手順に従います。

以下の手順に従ってボリュームをプロビジョニングします。

1. [ボリューム] タブで、[新しいボリュームの作成] をクリックします。
2. [新しいボリュームの作成] ページで、ボリュームの種類を選択します。



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



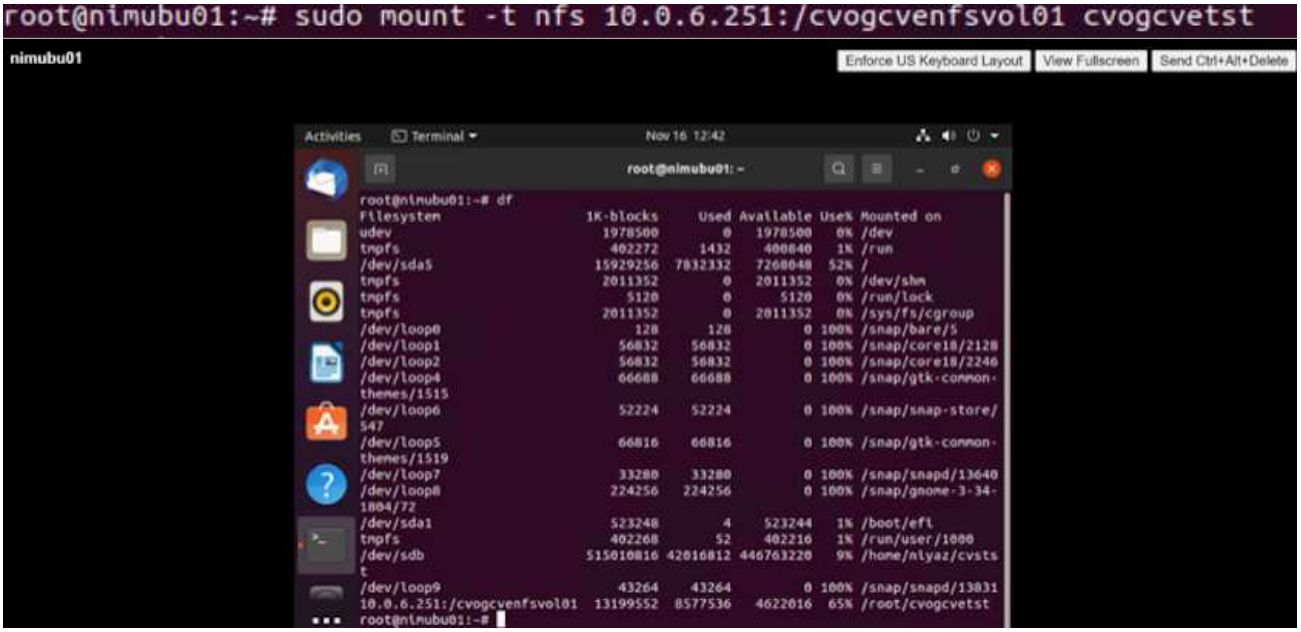
4. [コピー]をクリックします。
5. 指定された Linux インスタンスに接続します。
6. セキュア シェル (SSH) を使用してインスタンス上でターミナルを開き、適切な資格情報でログインします。
7. 次のコマンドを使用して、ボリュームのマウント ポイントのディレクトリを作成します。

```
$ sudo mkdir /cvogcvetst
```

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

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

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



Google Cloud NetApp Volumes(NetAppボリューム)

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

その他の利点と機能には、スナップショットによるデータ保護と復元、オンプレミスまたはクラウド内のデータの保存先を複製、同期、移行するための特別な機能、専用フラッシュ ストレージ システム レベルの一貫した高パフォーマンスなどがあります。

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

▼ **VMware Engine** で**NetApp Volumes** を構成する

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

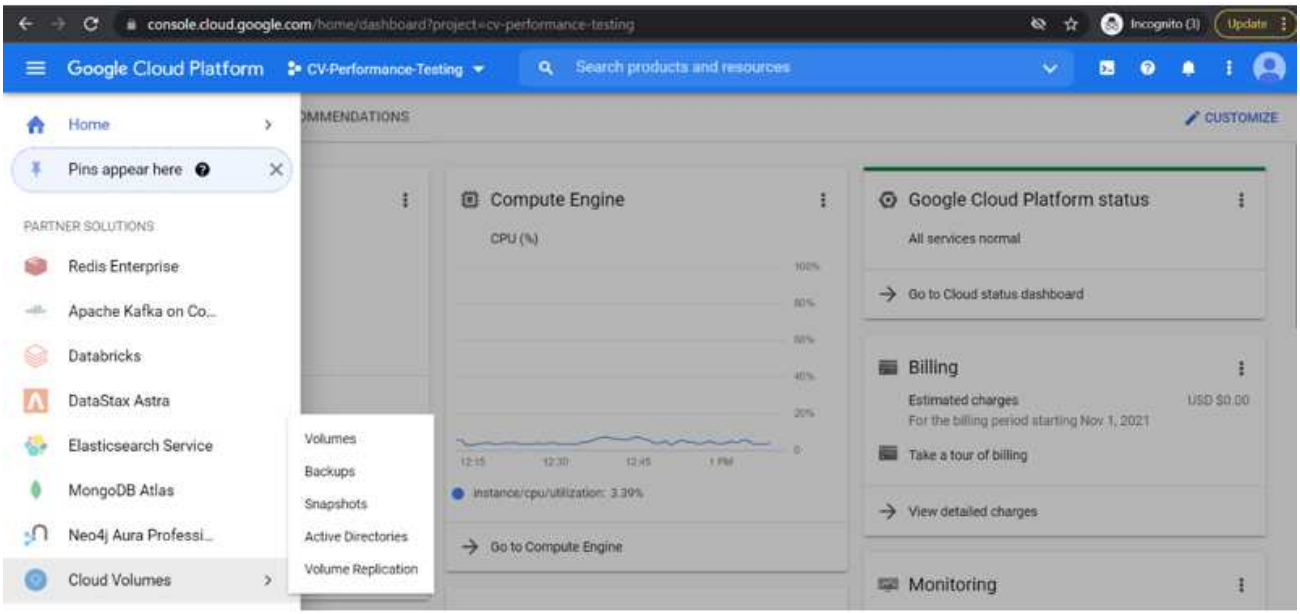
Google Cloud NetApp Volumesと Google Cloud VMware Engine プライベート クラウドは同じリージョンに存在する必要があります。

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

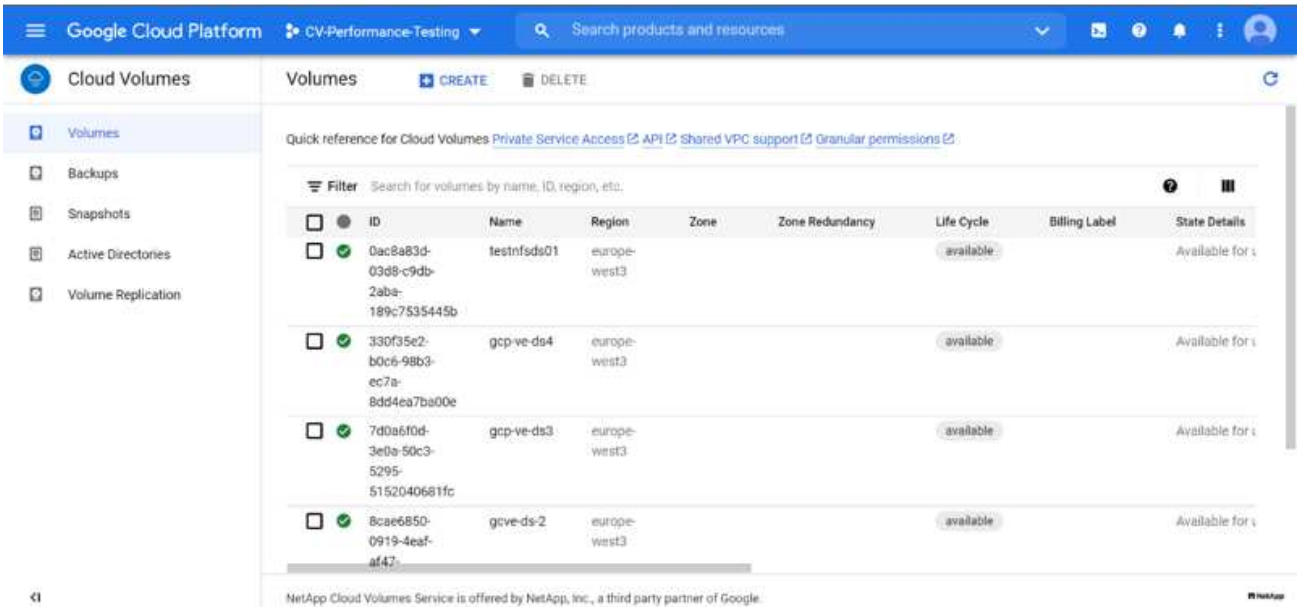
▼ **GCVE**プライベートクラウドに**NetApp Volumes NFS**ボリュームを作成する

NFS ボリュームを作成してマウントするには、次の手順を実行します。

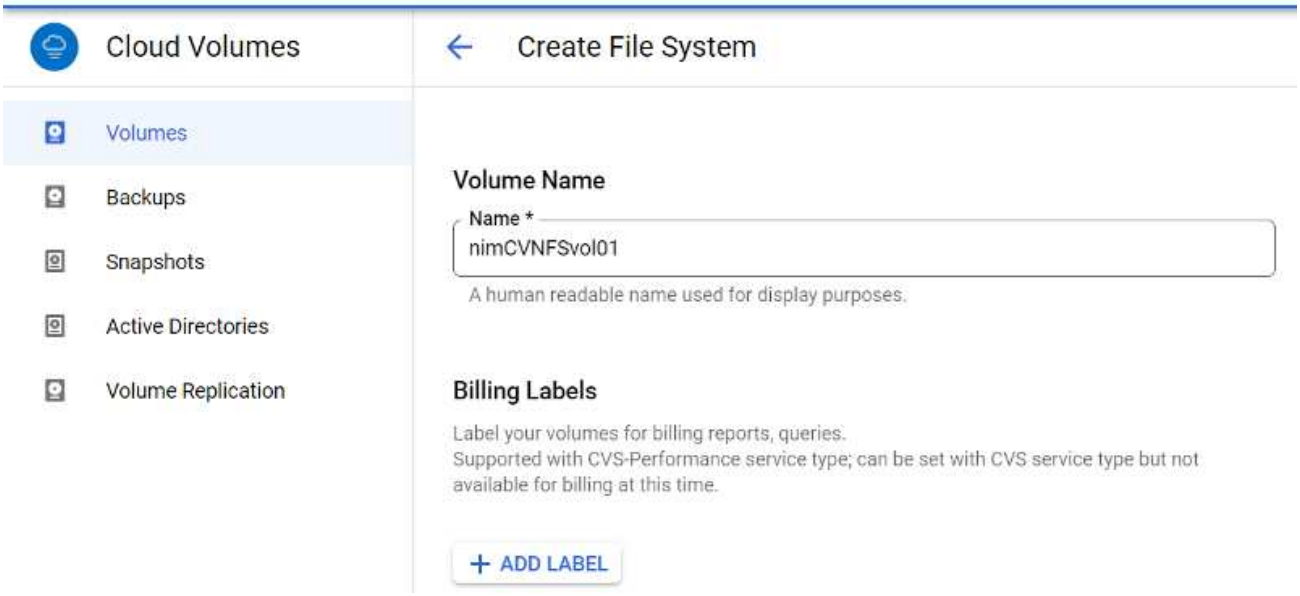
1. Google クラウド コンソール内のパートナー ソリューションから Cloud Volumes にアクセスします。



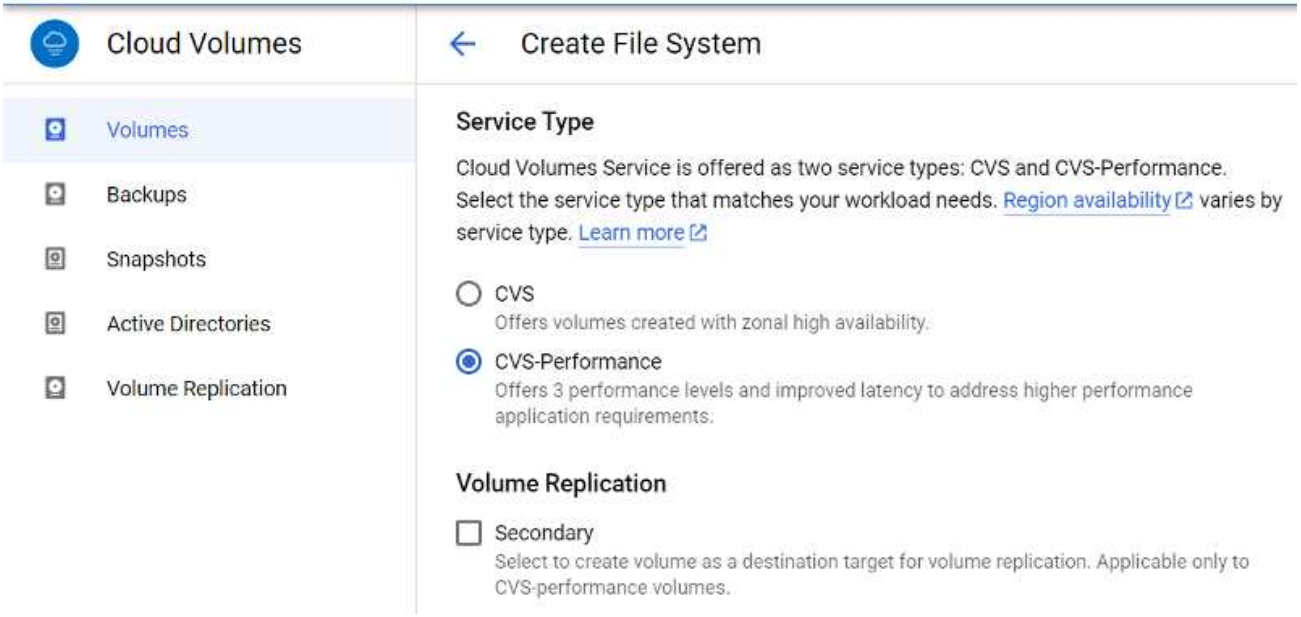
2. Cloud Volumes コンソールで、「ボリューム」ページに移動し、「作成」をクリックします。



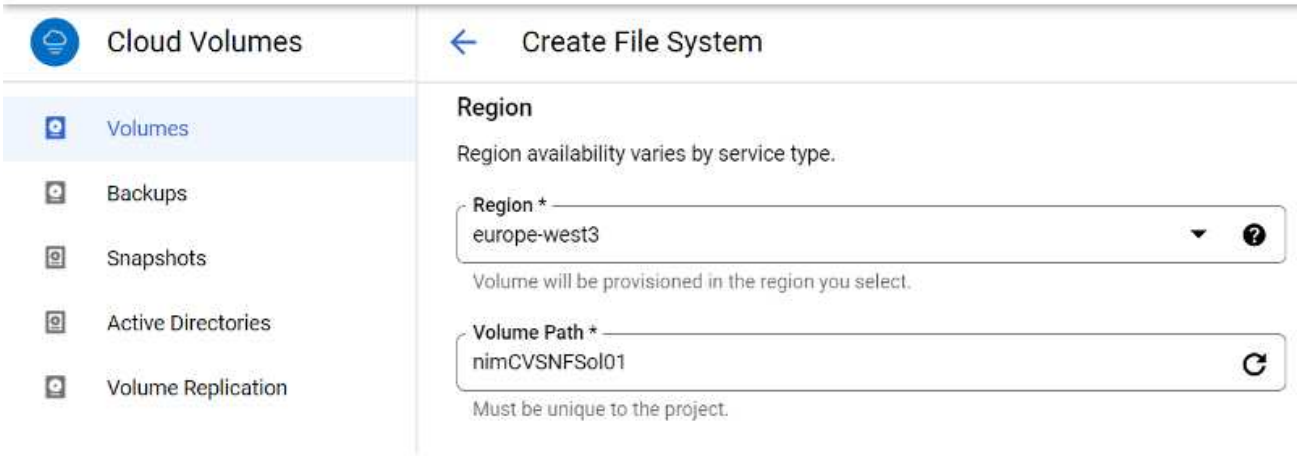
3. 「ファイル システムの作成」ページで、チャージバック メカニズムに必要なボリューム名と課金ラベルを指定します。



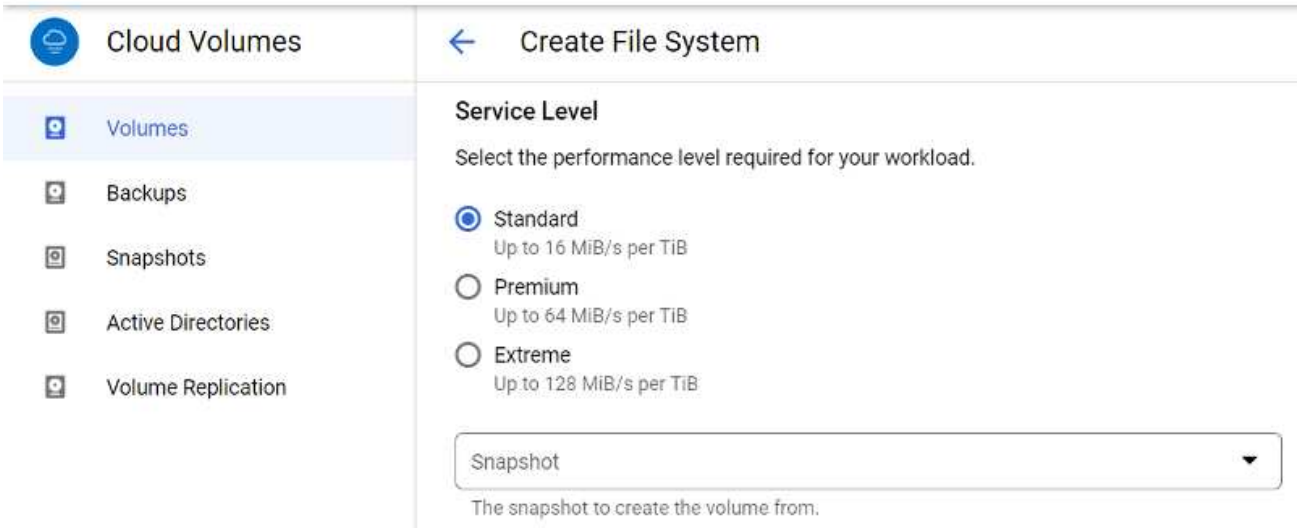
4. 適切なサービスを選択してください。 GCVE の場合、アプリケーションのワークロード要件に基づいて、レイテンシの改善とパフォーマンスの向上を実現するために、 NetApp Volumes-Performance と必要なサービス レベルを選択します。



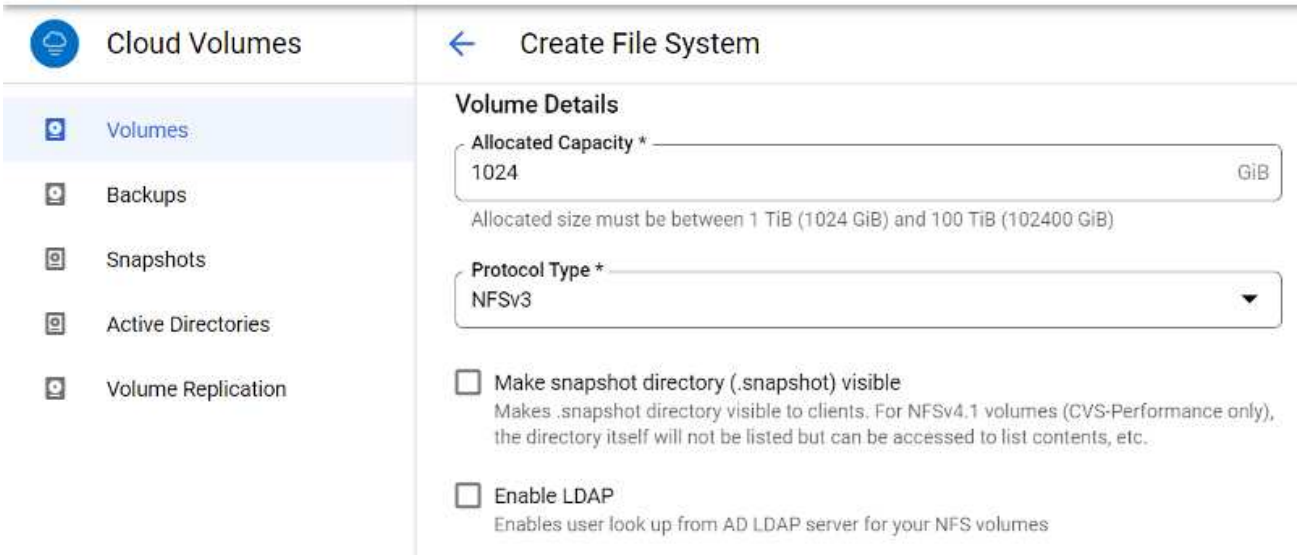
5. ボリュームとボリューム パスの Google Cloud リージョンを指定します (ボリューム パスは、プロジェクト内のすべてのクラウド ボリュームで一意である必要があります)



6. ボリュームのパフォーマンス レベルを選択します。

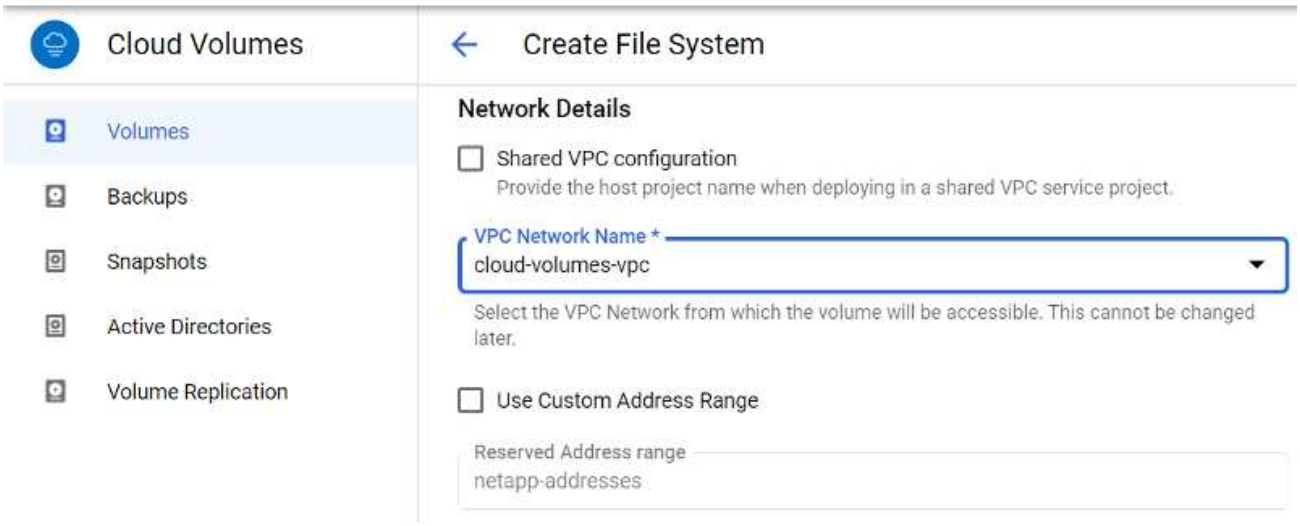


7. ボリュームのサイズとプロトコルの種類を指定します。このテストでは、NFSv3 が使用されます。



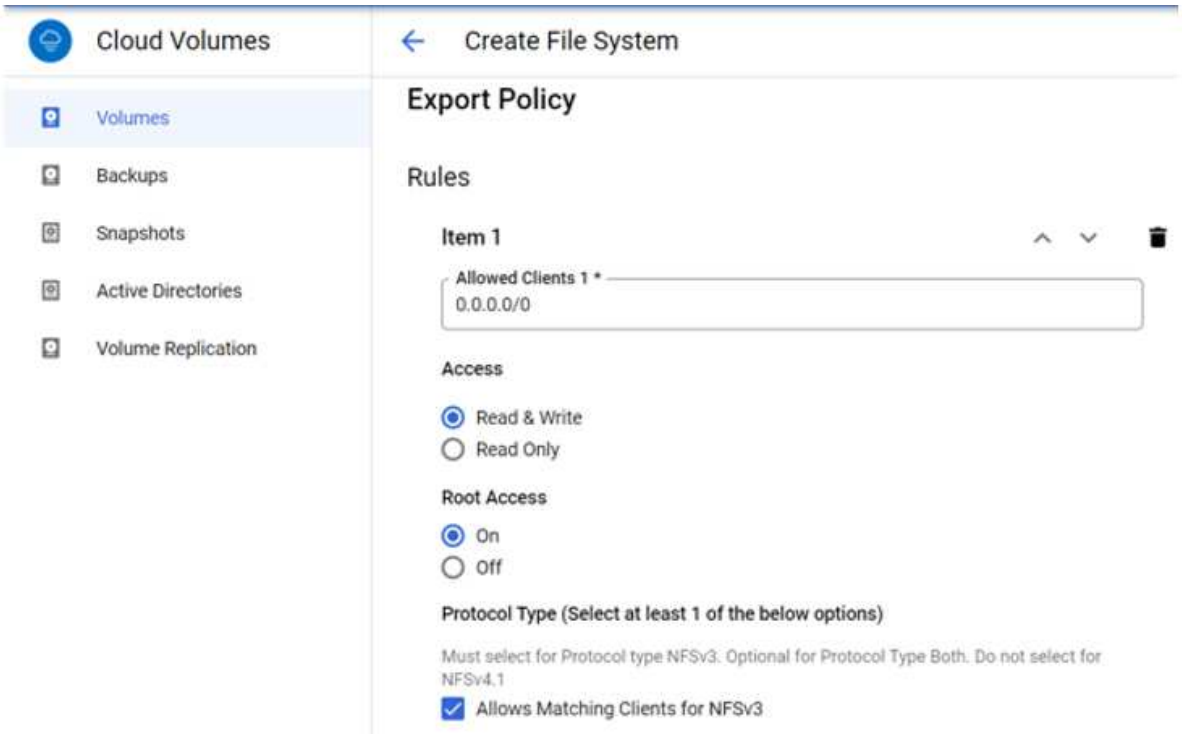
8. このステップでは、ボリュームにアクセスできる VPC ネットワークを選択します。 VPC ピアリングが確立されていることを確認します。

   ヒント: VPC ピアリングが実行されていない場合は、ピアリング コマンドを案内するポップアップ ボタンが表示されます。 Cloud Shell セッションを開き、適切なコマンドを実行して、VPC をGoogle Cloud NetApp Volumesプロデューサーとピアリングします。事前に VPC ピアリングを準備する場合は、こちらの手順を参照してください。

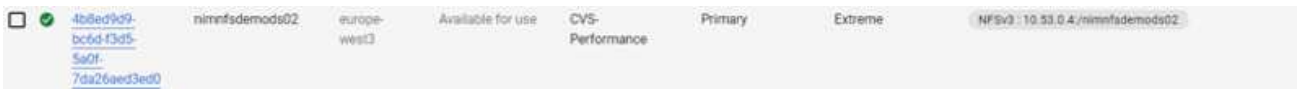


9. 適切なルールを追加してエクスポート ポリシー ルールを管理し、対応する NFS バージョンのチェックボックスを選択します。

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



10. 「保存」をクリックしてボリュームを作成します。



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

NFS ボリュームをマウントする準備をする前に、プライベート接続のピアリング ステータスがアクティブとしてリストされていることを確認してください。ステータスがアクティブになったら、マウント コマンドを使用します。

NFS ボリュームをマウントするには、次の手順を実行します。

1. Cloud Console で、[Cloud Volumes] > [ボリューム] に移動します。
2. ボリュームページへ
3. NFS エクスポートをマウントする NFS ボリュームをクリックします。
4. 右にスクロールし、「詳細を表示」の下の「マウント手順」をクリックします。

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

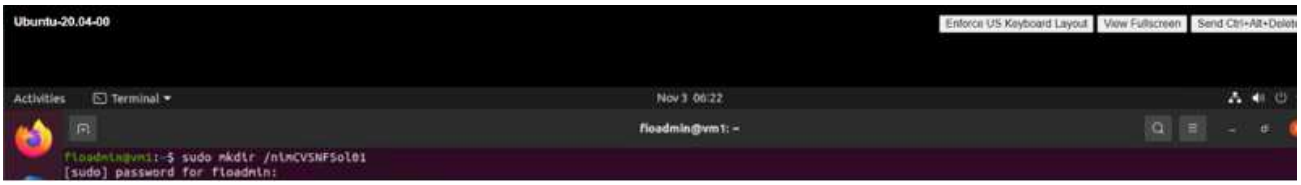
1. SSH クライアントを使用して仮想マシンに SSH 接続します。
2. インスタンスに NFS クライアントをインストールします。
   a. Red Hat Enterprise Linux または SuSE Linux インスタンスの場合:

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

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

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

```
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。ラボからのコマンドの例は次のとおりです。

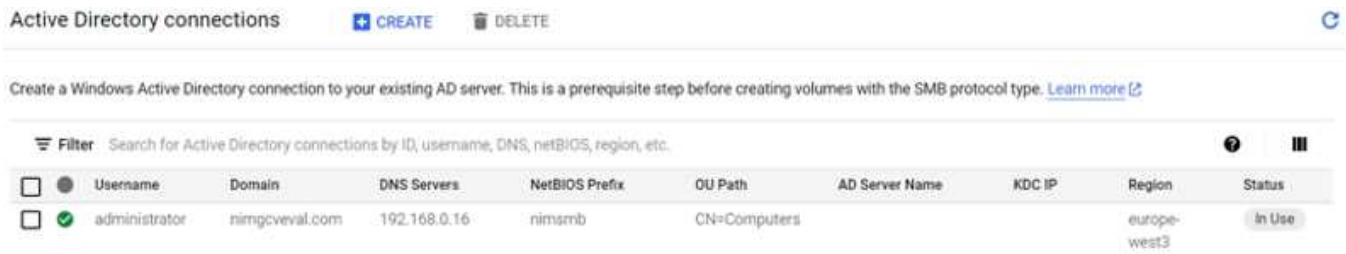
```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp
10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```



```
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:/nimCVSNFSol01     107374182400        256 107374182144   1% /nimCVSNFSol01
root@vm1:~#
```

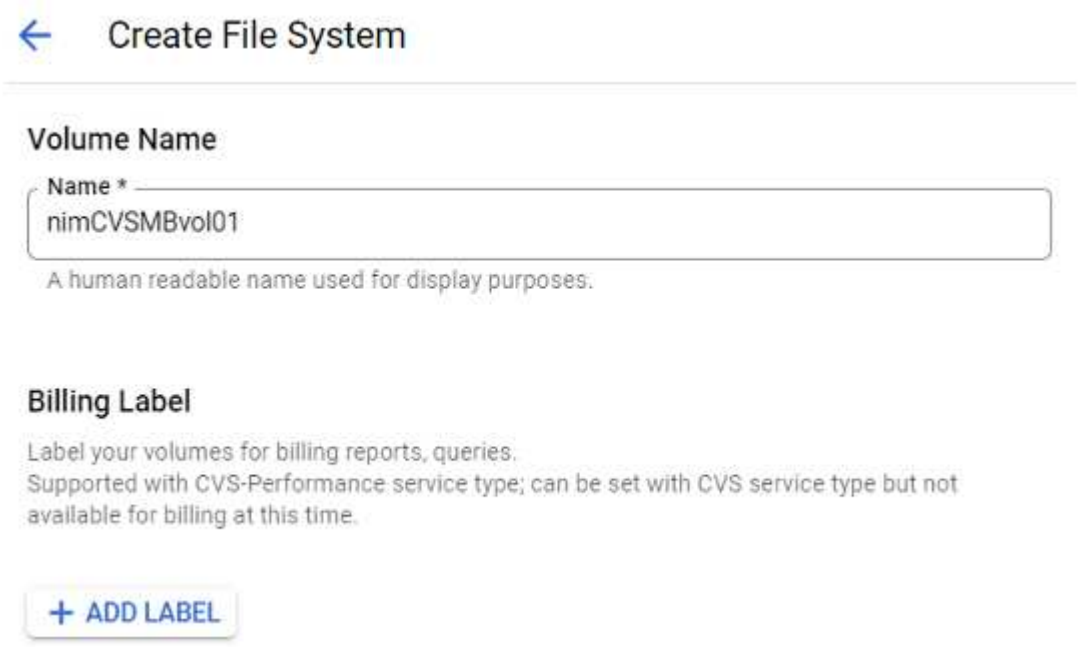
▼ **VMware Engine** 上で実行されている **VM** への **SMB** 共有の作成とマウント

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

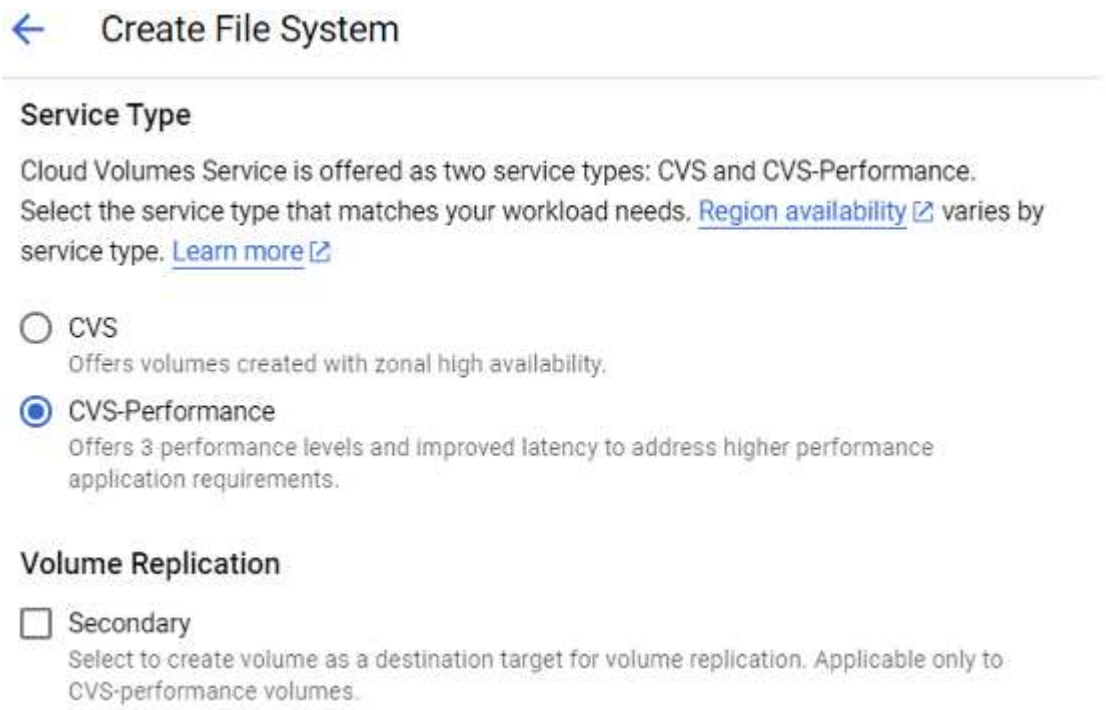


AD 接続が確立されたら、必要なサービス レベルでボリュームを作成します。適切なプロトコルを選択することを除いて、手順は NFS ボリュームを作成する場合と同様です。

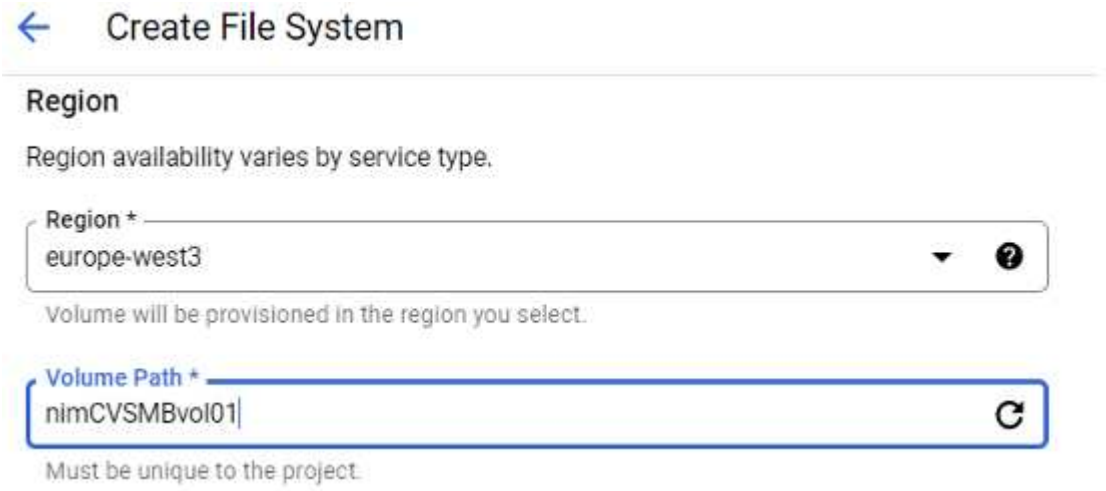
1. Cloud Volumes コンソールで、「ボリューム」ページに移動し、「作成」をクリックします。
2. 「ファイル システムの作成」ページで、チャージバック メカニズムに必要なボリューム名と課金ラベルを指定します。



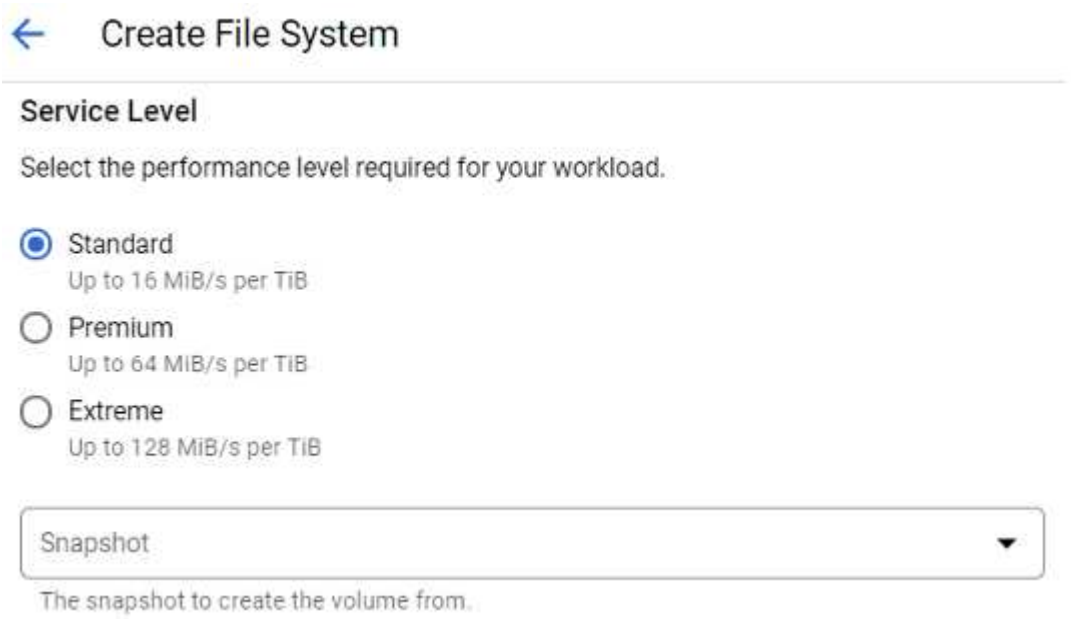
3. 適切なサービスを選択してください。 GCVE の場合、 NetApp Volumes-Performance と、ワークロード要件に基づいてレイテンシの改善とパフォーマンスの向上を図る必要なサービス レベルを選択します。



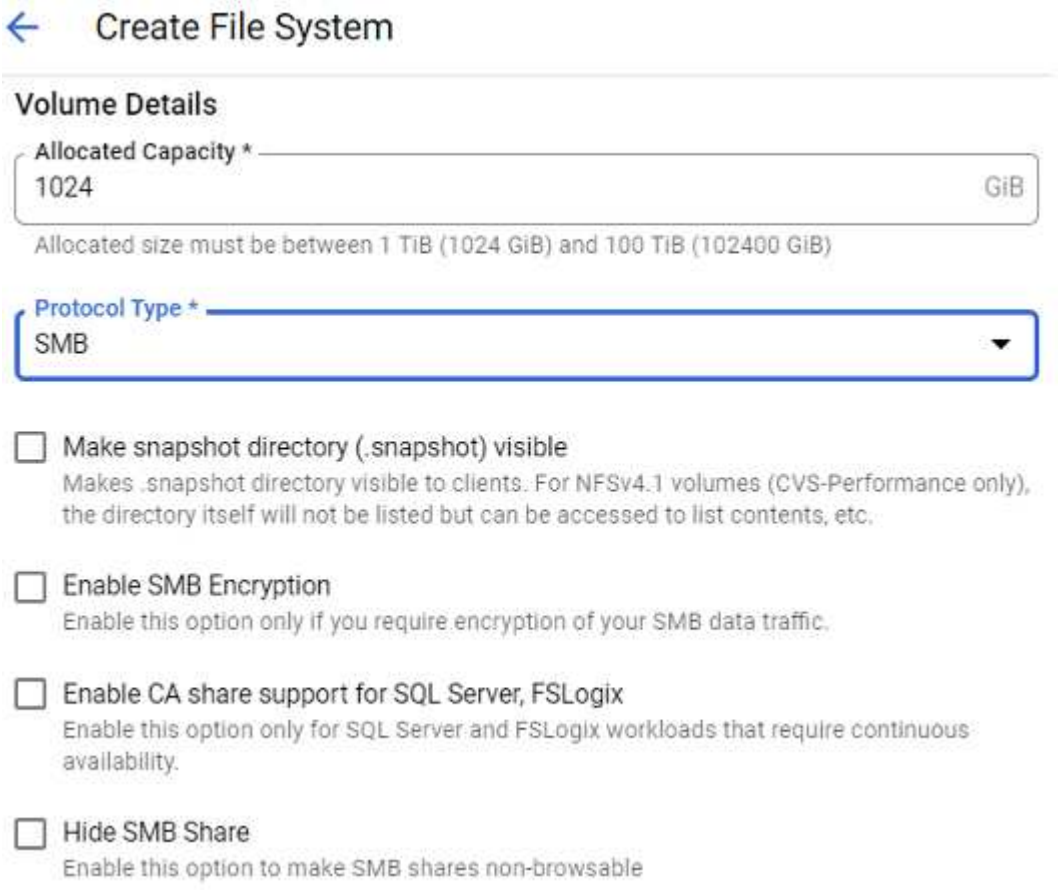
4. ボリュームとボリューム パスの Google Cloud リージョンを指定します (ボリューム パスは、プロジェクト内のすべてのクラウド ボリュームで一意である必要があります)



5. ボリュームのパフォーマンス レベルを選択します。



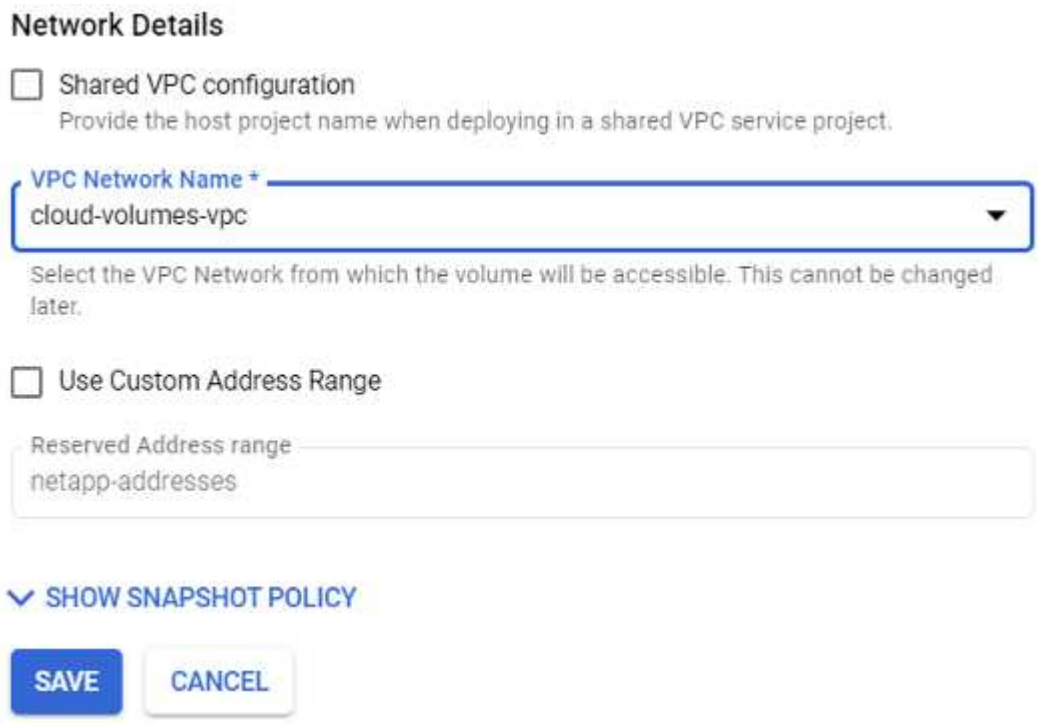
6. ボリュームのサイズとプロトコルの種類を指定します。このテストでは、SMB が使用されます。



7. このステップでは、ボリュームにアクセスできる VPC ネットワークを選択します。 VPC ピアリングが確立されていることを確認します。

   ヒント：VPCピアリングが完了していない場合は、ピアリングコマンドの手順を案内するポップアップボタンが表示されます。Cloud Shellセッションを開き、適切なコマンドを実行して、VPCをGoogle Cloud NetApp Volumesプロデューサとピアリングします。VPCピアリングを事前に準備する場合は、

これらの"確認方法"を参照してください。



8. 「保存」をクリックしてボリュームを作成します。



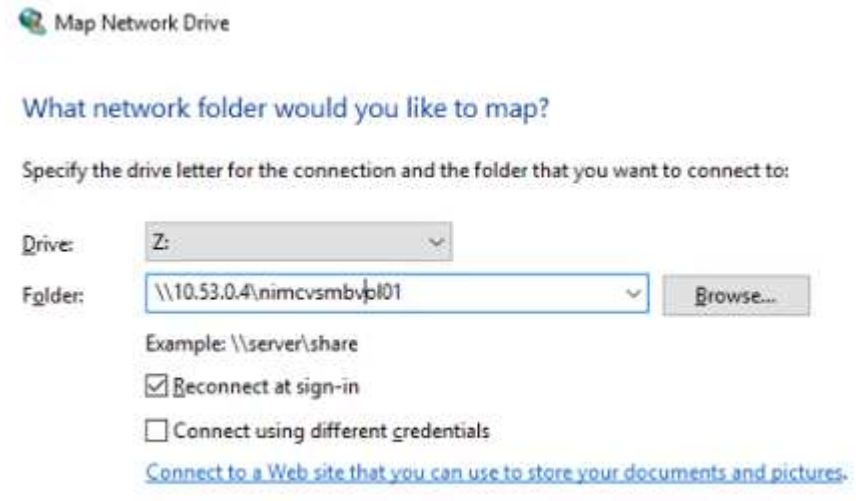
SMB ボリュームをマウントするには、次の手順を実行します。

1. Cloud Console で、[Cloud Volumes] > [ボリューム] に移動します。
2. ボリュームページへ
3. SMB 共有をマップする SMB ボリュームをクリックします。
4. 右にスクロールし、「詳細を表示」の下の「マウント手順」をクリックします。

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

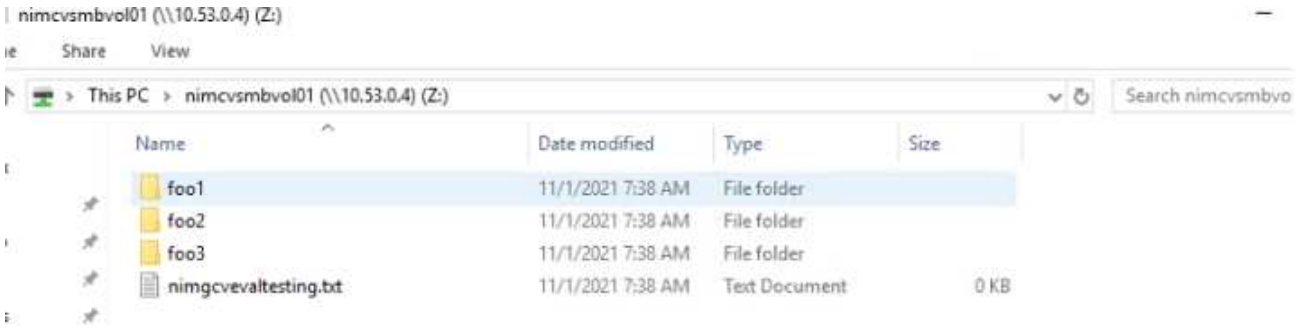
1. [スタート] ボタンをクリックし、[コンピューター] をクリックします。
2. [ネットワーク ドライブの割り当て]をクリックします。
3. ドライブ リストで、使用可能なドライブ文字をクリックします。
4. フォルダー ボックスに次のように入力します。

```
\\nimsmb-3830.nimgcveval.com\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する] チェック ボックスをオンにします。

5. [Finish]をクリックします。



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

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

ユースケース1: ストレージの最適化

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

NetApp Cloud Volumes を統合することで、組織はプラットフォームの再設定、IP の変更、アーキテクチャの変更を必要とせず、シンプルな移行アプローチで vSphere ベースのクラウド ソリューションを実現できます。さらに、この最適化により、vSphere で必要なホスト数を最小限に抑えながら、ストレージ フットプリントを拡張できますが、ストレージ階層、セキュリティ、または使用可能なファイルには変更が加えられません。これにより、導入を最適化し、全体的な TCO を 35～45% 削減できます。この統合により、ウォーム ス

トレージから実稼働レベルのパフォーマンスまで、ストレージを数秒で拡張することもできます。

ユースケース**2:** クラウド移行

組織は、近づいているリースの期限、資本支出 (capex) から運用支出 (opex) に移行するという財務上の指示、すべてをクラウドに移行するというトップダウンの指示など、さまざまな理由から、オンプレミスのデータ センターからパブリック クラウドにアプリケーションを移行するようプレッシャーを受けています。

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

ユースケース**3:** データセンターの拡張

季節的な需要の急増や、単に安定した有機的成長によりデータセンターの容量が限界に達した場合、クラウドでホストされる VMware とNetApp Cloud Volumes に移行するのが簡単な解決策です。 NetApp Cloud Volumes を活用すると、可用性ゾーン全体にわたる高可用性と動的なスケーリング機能が提供され、ストレージの作成、レプリケーション、拡張が非常に簡単になります。 NetApp Cloud Volumes を活用すると、ストレッチ クラスタの必要性を克服し、ホスト クラスタの容量を最小限に抑えることができます。

ユースケース **#4:** クラウドへの災害復旧

従来のアプローチでは、災害が発生した場合、クラウドに複製された VM を復元するには、クラウド独自のハイパーバイザー プラットフォームに変換する必要があり、これは危機時に処理すべきタスクではありません。

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

ユースケース **#5:** アプリケーションのモダナイゼーション

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

まとめ

オールクラウドまたはハイブリッド クラウドのどちらをターゲットにしているかに関係なく、 NetApp Cloud Volumes は、データ要件をアプリケーション層にシームレスにすることで TCO を削減しながら、ファイル サービスとブロック プロトコルとともにアプリケーション ワークロードを導入および管理するための優れたオプションを提供します。

ユースケースに関係なく、お気に入りのクラウド/ハイパースケーラーをNetApp Cloud Volumes と組み合わせ

て選択することで、クラウドのメリット、オンプレミスと複数のクラウドにわたる一貫したインフラストラクチャと運用、ワークロードの双方向の移植性、エンタープライズ グレードの容量とパフォーマンスを迅速に実現できます。

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

VMware ハイブリッド クラウドのユースケース

VMware を使用したNetApp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 ファーストの展開を計画する際に IT 組織にとって重要なユース ケースの概要。

人気のユースケース

使用例は次のとおりです:

- 災害復旧、
- データセンターのメンテナンス中にワークロードをホスティングする、* ローカルデータセンターでプロビジョニングされているリソースを超えて追加のリソースが必要となる急激なバースト、
- VMwareサイトの拡張、
- クラウドへの迅速な移行、
- 開発/テスト、そして
- クラウド補足テクノロジーを活用したアプリの最新化。

このドキュメント全体を通じて、VMware のユースケースを使用してクラウド ワークロードの参照について詳しく説明します。これらのユースケースは次のとおりです。

- 保護（災害復旧とバックアップ/復元の両方を含む）
- 移行
- 拡張

ITの旅の内側

ほとんどの組織は変革と近代化への道を歩んでいます。このプロセスの一環として、企業は既存の VMware 投資を活用しながらクラウドのメリットを活用し、移行プロセスを可能な限りシームレスに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内にあるため、近代化の取り組みが非常に簡単になります。

このシナリオに対する最も簡単な答えは、各ハイパースケーラーで VMware 製品を提供することです。NetApp Cloud Volumes 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する方法を提供しており、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、クラウドでネイティブにワークロードを実行できます。これにより、サービスの中断や IP 変更の必要がなくなり、IT チームが既存のスキルとツールを使用してオンプレミスと同じように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、クラウド移行が加速され、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よりスムーズになります。

どのクラウドでも VMware はすべての顧客に独自のハイブリッド機能を提供しますが、補足的な NFS ストレージ オプションが限られているため、ストレージ負荷の高いワークロードを持つ組織にとってその有用性が制限されています。ストレージはホストに直接結び付けられているため、ストレージを拡張する唯一の方法はホストを追加することであり、これによりストレージを集中的に使用するワークロードのコストが 35 ～ 40% 以上増加する可能性があります。これらのワークロードに必要なのは追加のストレージのみであり、追加の処理能力は必要ありません。しかし、それは追加のホストに料金を支払うことを意味します。

次のシナリオを考えてみましょう。

顧客は CPU とメモリ用に 5 台のホストしか必要としませんが、ストレージのニーズが多く、ストレージ要件を満たすには 12 台のホストが必要です。この要件により、ストレージを増やすだけで済むのに、追加の処理能力を購入しなければならなくなり、財務上の問題が大きくなってしまいます。

クラウドの導入と移行を計画するときは、常に最善のアプローチを評価し、総投資額を削減する最も簡単なパスを採用することが重要です。アプリケーション移行の最も一般的かつ最も簡単なアプローチは、仮想マシン (VM) やデータ変換を行わない再ホスティング (リフト アンド シフトとも呼ばれます) です。 NetApp Cloud Volumes を VMware ソフトウェア定義データセンター (SDDC) と併用することで、vSAN を補完し、簡単なリフトアンドシフト オプションが提供されます。

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

ワークフローの移行、クラウドへの拡張/バースト、バックアップ/リストア、災害復旧など、 NetApp が各ハイパースケーラーに VMware 環境をもたらすソリューションについて詳しくご覧ください。

VMware 環境向け**NetApp**ソリューション

ハイブリッド クラウド モデルで運用している場合も、「クラウド ファースト」モデルで運用している場合も、 NetApp は、クラウドまたはハイブリッド クラウド モデルでワークロードを管理するための最も一般的なユースケースに対応する幅広いソリューションを提供します。

NetApp は、ゲスト内 (ゲスト接続) ストレージとして、または各ハイパースケーラー内の補足 NFS データストアとしてプロビジョニングされるストレージ向けのソリューションも提供しています。すべてのソリューションは、VMware のクラウド ワークロードの分類に従って分類されます。これらの分類には次のものが含まれます。

- 保護（災害復旧とバックアップ/復元の両方を含む）
- 移行
- 拡張

各ハイパースケーラーで利用可能なソリューションの詳細については、以下をご覧ください。

- "AWS / VMC向けソリューション"
- "Azure / AVS向けソリューション"
- "GCP / GCVE向けソリューション"

Amazon VMware Managed Cloud (VMC) 向けNetAppソリューション

NetApp がAWS に提供するソリューションの詳細をご覧ください。

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定義しています。

- 保護（災害復旧とバックアップ/復元の両方を含む）
- 移行
- 拡張

次のセクションで利用可能なソリューションを参照してください。

守る

- "VMC on AWS による災害復旧 (ゲスト接続)"
- "FSx ONTAPを使用した VMC での Veeam バックアップ リストア"
- "FSx ONTAPと VMC による災害復旧 (DRO)"
- "Veeam Replication と FSx ONTAPを使用して VMware Cloud on AWS への災害復旧を行う"

移行

- "VMware HCX を使用してワークロードを FSx ONTAPデータストアに移行する"

拡張

近日公開！！

Azure VMware Solution (AVS) 向けNetAppソリューション

NetApp がAzure に提供するソリューションの詳細をご覧ください。

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定義しています。

- 保護（災害復旧とバックアップ/復元の両方を含む）
- 移行
- 拡張

次のセクションで利用可能なソリューションを参照してください。

守る

- "ANF と JetStream (補足 NFS データストア) を使用した災害復旧"
- "ANF と CVO (ゲスト接続ストレージ) による災害復旧"
- "ANF と AVS による災害復旧 (DRO)"
- "Veeam Replication とAzure NetApp Filesデータストアを使用して Azure VMware Solution への災害復旧を行う"

移行

- "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する"

拡張

近日公開！！

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

NetApp がGCP に提供するソリューションの詳細をご覧ください。

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定義しています。

- 保護（災害復旧とバックアップ/復元の両方を含む）
- 移行
- 拡張

次のセクションで利用可能なソリューションを参照してください。

守る

- "SnapCenter、 Cloud Volumes ONTAP 、Veeam Replication を使用したアプリケーションの災害復旧"
- "NetApp SnapCenterと Veeam による GCVE 上のNetAppボリュームへのレプリケーションによるアプリケーション整合性のある災害復旧"

移行

- "VMware HCX を使用したGoogle Cloud NetApp Volumes NFS データストアへのワークロード移行"
- "Veeam を使用したGoogle Cloud NetApp Volumes NFS データストアへの VM レプリケーション"

拡張

近日公開！！

AWS/VMC向けNetApp

AWS VMC 向けNetApp の機能

NetApp がAWS VMware Cloud (VMC) にもたらす機能について詳しく説明します。ゲスト接続ストレージ デバイスまたは補助的な NFS データストアとしてのNetAppから、ワークフローの移行、クラウドへの拡張/バースト、バックアップ/リストア、災害復旧まで、さまざまな機能について説明します。

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 での VMC の構成"

- "VMC向けNetAppストレージオプション"
- "NetApp / VMware クラウド ソリューション"

AWS での VMC の構成

オンプレミスの場合と同様に、VM の作成と移行のための本番環境を正常に構築するには、クラウド ベースの仮想化環境を計画することが重要です。

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

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

セットアッププロセスは次の手順に分けられます。

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

詳細を表示"VMCの設定手順"。

VMC向けNetAppストレージオプション

NetAppストレージは、AWS VMC 内で、仮想接続として、または補助的な NFS データストアとして、さまざまな方法で利用できます。

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

AWS は、次の構成でNetAppストレージをサポートしています。

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

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

ソリューションのユースケース

NetAppと VMware のクラウド ソリューションを使用すると、多くのユース ケースを AWS VMC に簡単に導入できます。 VMware が定義したクラウド領域ごとにユースケースが定義されています。

- 保護（災害復旧とバックアップ/復元の両方を含む）
- 拡張
- 移行

"AWS VMC向けNetAppソリューションをご覧ください"

AWS/VMC 上のワークロードを保護する

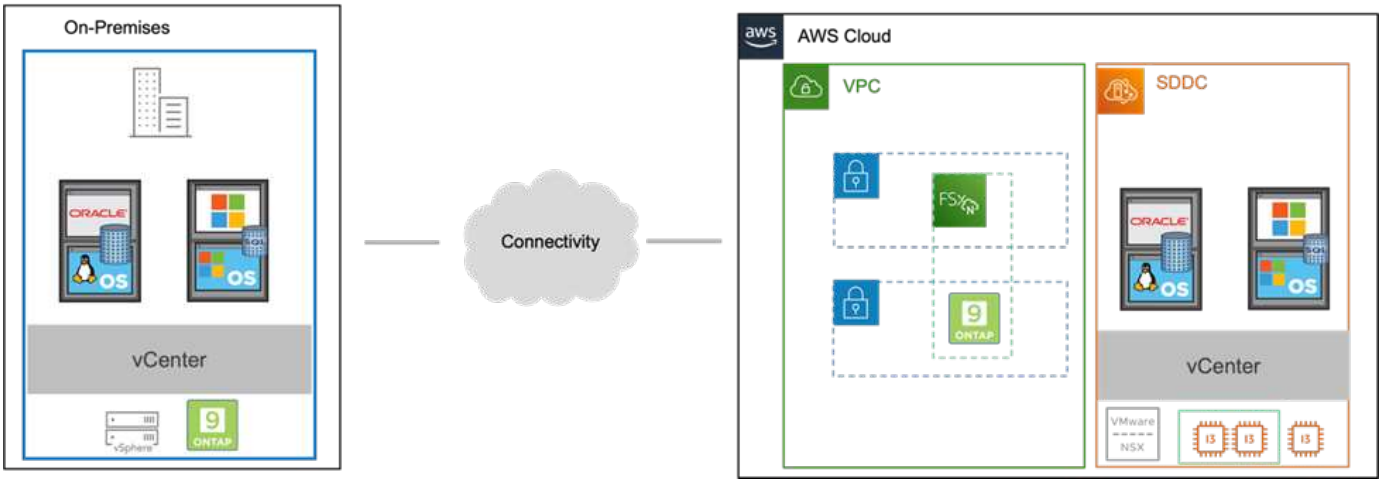
TR-4931: VMware Cloud on Amazon Web Services とゲストコネクトによる災害復旧

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復旧できるようにするために、組織にとって実証済みの災害復旧 (DR) 環境と計画が不可欠です。このソリューションは、オンプレミスと VMware Cloud on AWS の両方で、VMware およびNetAppテクノロジーに重点を置いた DR ユースケースのデモンストレーションに重点を置いています。

概要

NetApp はVMware との統合において長い歴史を誇ります。これは、仮想化環境のストレージ パートナーとしてNetAppを選択した何万もの顧客によって証明されています。この統合は、クラウド内のゲスト接続オプションや、最近の NFS データストアとの統合でも継続されます。このソリューションは、一般的にゲスト接続ストレージと呼ばれるユースケースに重点を置いています。

ゲスト接続ストレージでは、ゲスト VMDK は VMware によってプロビジョニングされたデータストアに展開され、アプリケーション データは iSCSI または NFS に格納され、VM に直接マップされます。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 シナリオを説明します。



前提、前提条件、コンポーネントの概要

このソリューションを展開する前に、コンポーネントの概要、ソリューションを展開するために必要な前提条件、およびこのソリューションを文書化する際に行われた仮定を確認してください。

"DRソリューションの要件、前提条件、および計画"

SnapCenterで**DR**を実行する

このソリューションでは、 SnapCenter はSQL Server および Oracle アプリケーション データに対してアプリケーション整合性のあるスナップショットを提供します。この構成は、 SnapMirrorテクノロジーと組み合わせることで、オンプレミスのAFFと FSx ONTAPクラスター間の高速データ レプリケーションを実現します。さらに、Veeam Backup & Replication は仮想マシンのバックアップと復元機能を提供します。

このセクションでは、バックアップとリストアの両方における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構成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構成する

SnapCenter は、長期アーカイブと保持を目的として、プライマリ ストレージ システム内 (プライマリ > ミラー) およびセカンダリ ストレージ システム (プライマリ > ボールト) のSnapMirror関係を更新できます。そのためには、 SnapMirrorを使用して、宛先ボリュームとソース ボリューム間のデータ複製関係を確立し、初期化する必要があります。

ソースと宛先のONTAPシステムは、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 を使用してピアリングされたネットワーク内にある必要があります。

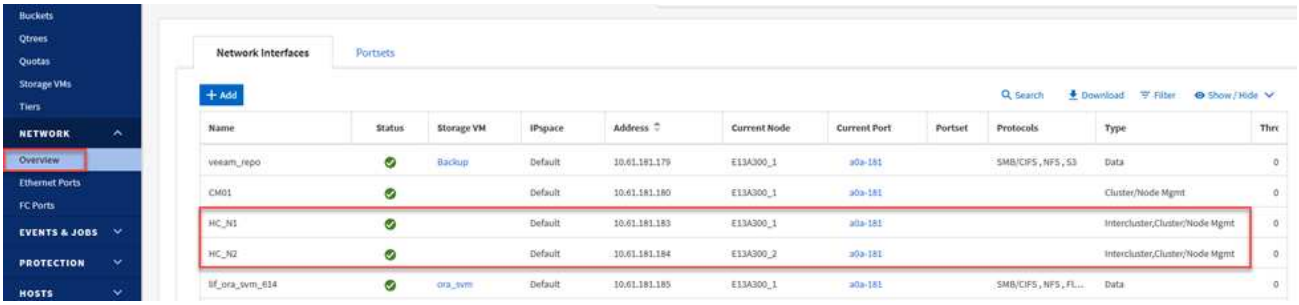
オンプレミスのONTAPシステムと FSx ONTAPの間にSnapMirror関係を設定するには、次の手順が必要です。

> 参照 "FSx ONTAP – ONTAPユーザーガイド"FSx とのSnapMirror関係の作成の詳細については、こちらをご覧ください。

▼ 送信元と宛先のクラスタ間論理インターフェースを記録する

オンプレミスにあるソースONTAPシステムの場合、System Manager または CLI からクラスタ間 LIF 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、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るタイプ: クラスタ間の IP アドレスを取得します。



2. FSx のクラスター間 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.
```

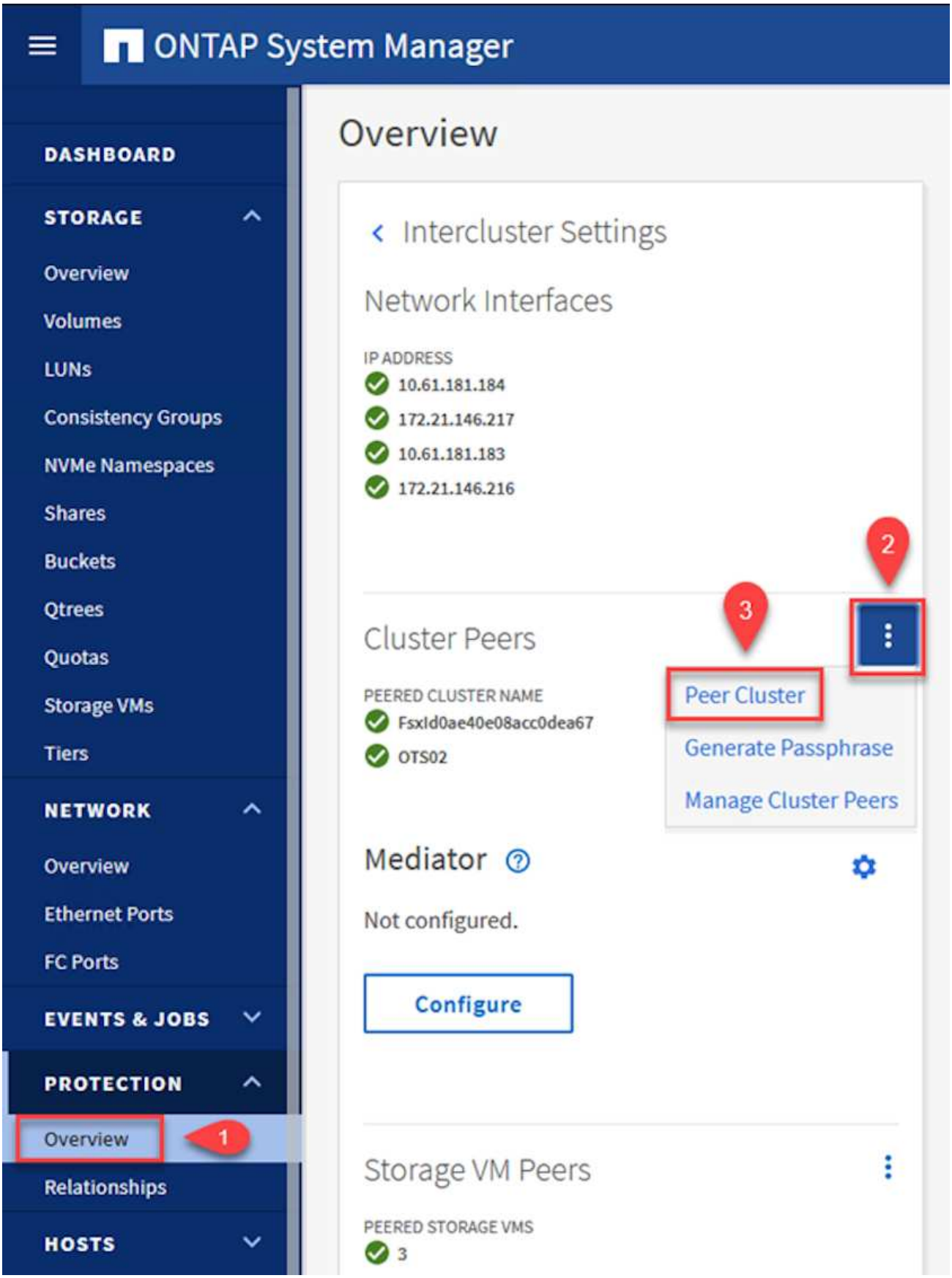
▼ **ONTAP**と**FSx**間のクラスタピアリングを確立する

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、他のピア クラスタで確認する必要があります。

1. 宛先FSxクラスタでピアリングを設定するには、 `cluster peer create`指示。プロンプトが表示されたら、後でソース クラスターで作成プロセスを完了するために使用する一意のパスフレーズを入力します。

```
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 から、[Protection] > [Overview] に移動し、[Peer Cluster] を選択します。



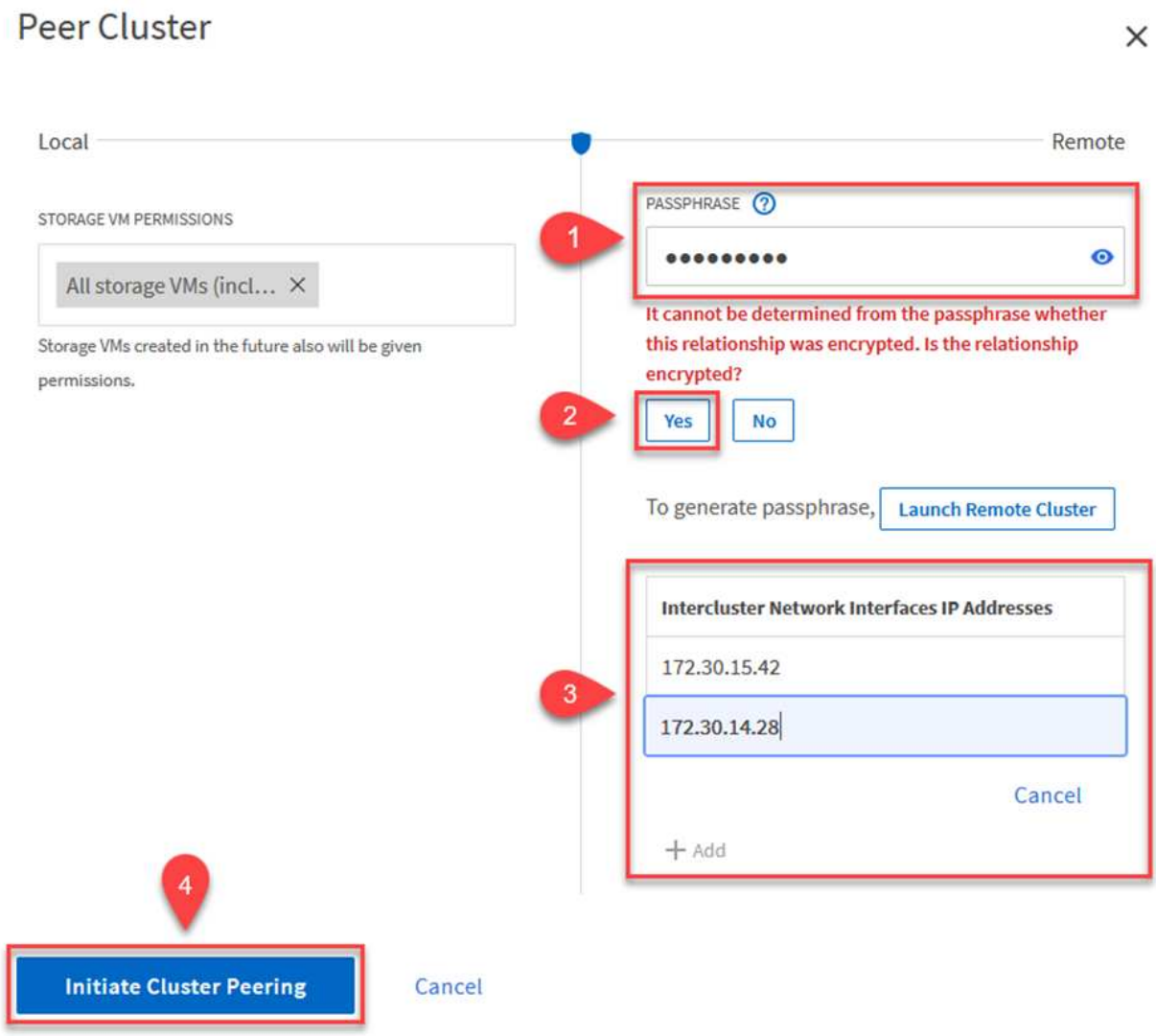
3. [ピア クラスター] ダイアログ ボックスで、必要な情報を入力します。
   a. 宛先 FSx クラスターでピア クラスター関係を確立するために使用されたパスフレーズを入力しま

す。

b. 選択 `Yes`暗号化された関係を確立します。

c. 宛先 FSx クラスタのクラスタ間 LIF IP アドレスを入力します。

d. プロセスを終了するには、「クラスター ピアリングの開始」をクリックします。



4. 次のコマンドを使用して、FSx クラスターからクラスター 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**ピアリング関係を確立する

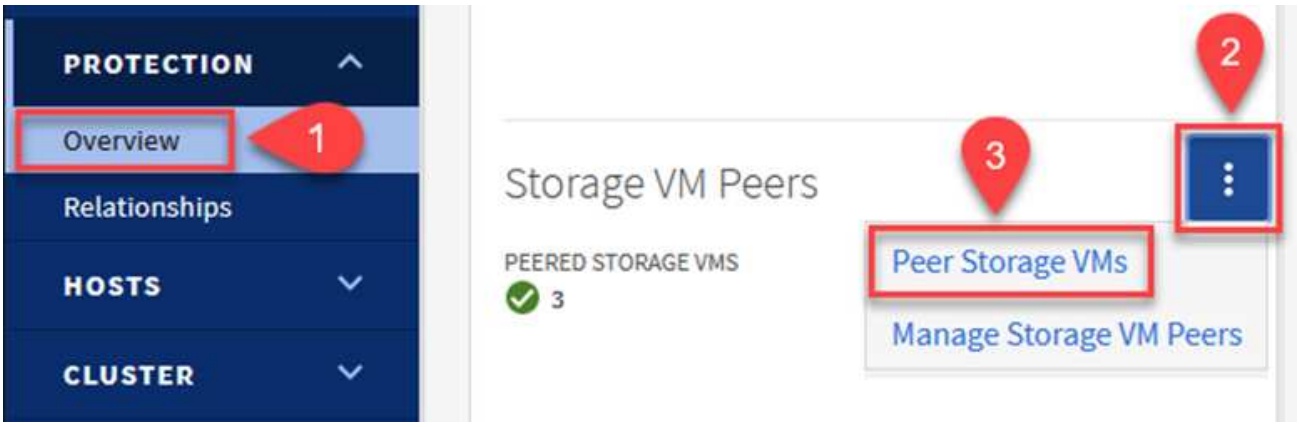
次の手順では、 SnapMirror関係になるボリュームを含む宛先ストレージ仮想マシンとソース ストレージ仮

想マシン間の SVM 関係を設定します。

1. ソース FSx クラスターから、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クラスタから、 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受け入れます。
3. ONTAP System Manager から、[Protection] > [Overview] に移動し、[Storage VM Peers] の下の [Peer Storage VMs] を選択します。



4. ピア ストレージ VM のダイアログ ボックスで、必須フィールドに入力します。
   - ソースストレージVM
   - 宛先クラスター
   - 宛先ストレージVM



5. SVM ピアリング プロセスを完了するには、[ピア ストレージ VM] をクリックします。

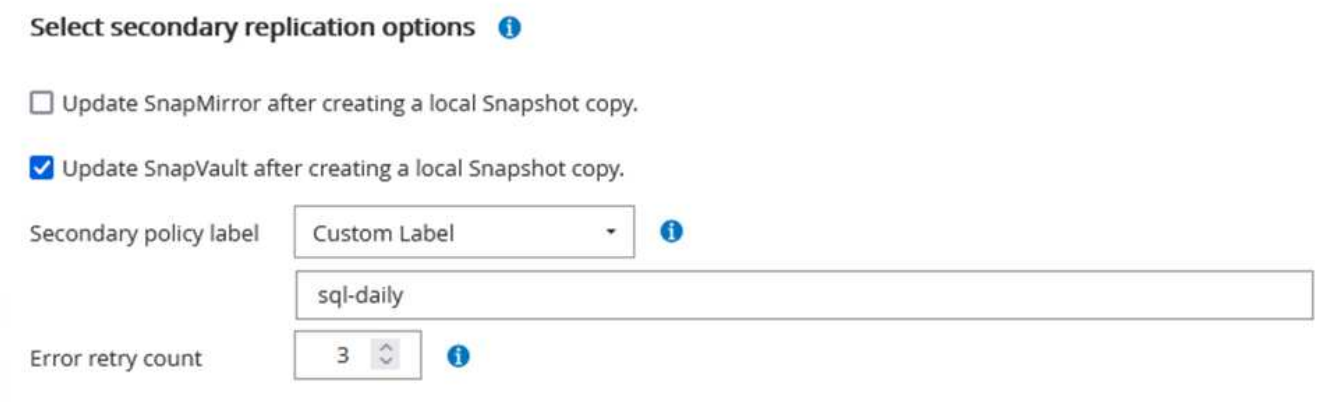
▼ スナップショット保持ポリシーを作成する

SnapCenter は、プライマリ ストレージ システム上にスナップショット 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 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を管理しません。これらのポリシーは、セカンダリ FSx クラスター上に作成され、ソース ボリュームとSnapMirror関係にある宛先ボリュームに関連付けられたSnapMirrorポリシーを通じて個別に管理されます。

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スナップショットのSnapMirrorラベルに追加されるセカンダリ ポリシー ラベルを指定するオプションがあります。

> ⓘ セカンダリ ストレージでは、これらのラベルは、スナップショットの保持を強制する目的で、宛先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 データベースとログ ボリュームの毎日のバックアップに使用されるポリシーの一部として生成されたすべてのスナップショットに存在するSnapMirrorラベルを示しています。



SQL Serverデータベース用のSnapCenterポリシーの作成の詳細については、 "SnapCenterのドキュメント" 。

まず、保持するスナップショット コピーの数を指定するルールを含むSnapMirrorポリシーを作成する必要があります。

1. FSx クラスターに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ラベルを使用して、ポリシーにルールを追加します。

```
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
```

各SnapMirrorラベルと保持するスナップショットの数 (保持期間) に対して追加のルールを作成します。

▼ 宛先ボリュームを作成する

ソース ボリュームからのスナップショット コピーの受信者となる FSx 上の宛先ボリュームを作成するには、FSx ONTAP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宛先ボリューム間の**SnapMirror**関係を作成する

ソース ボリュームと宛先ボリュームの間に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**関係を初期化する

SnapMirror関係を初期化します。このプロセスは、ソース ボリュームから生成された新しいスナップショットを開始し、それを宛先ボリュームにコピーします。

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

オンプレミスで **Windows SnapCenter**サーバーを展開および構成します。

▼ **Windows SnapCenter Server** をオンプレミスに導入

このソリューションは、 NetApp SnapCenterを使用して、SQL Server および Oracle データベースのアプリケーション整合性のあるバックアップを取得します。仮想マシン VMDK をバックアップする Veeam Backup & Replication と組み合わせることで、オンプレミスおよびクラウドベースのデータセンター向けの包括的な災害復旧ソリューションが提供されます。

SnapCenter softwareはNetApp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存在する 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、 "NetAppドキュメント センター" 。

SnapCenter softwareは以下から入手できます。 "このリンク" 。

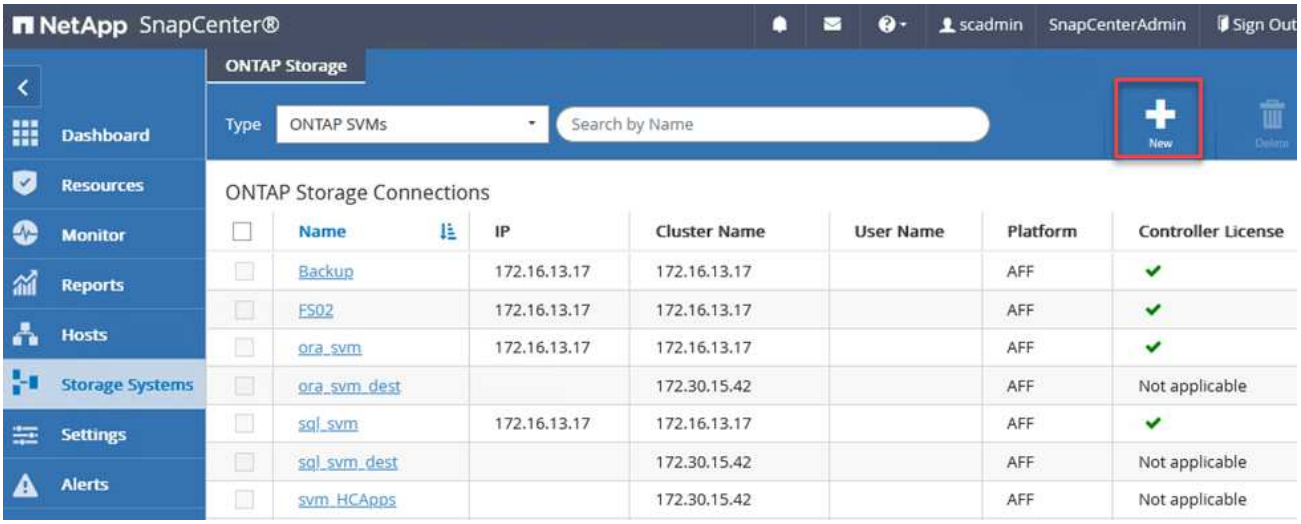
インストール後、*https://Virtual_Cluster_IP_or_FQDN:8146* を使用して Web ブラウザーからSnapCenterコンソールにアクセスできるようになります。

コンソールにログインしたら、SQL Server および Oracle データベースのバックアップ用にSnapCenter を構成する必要があります。

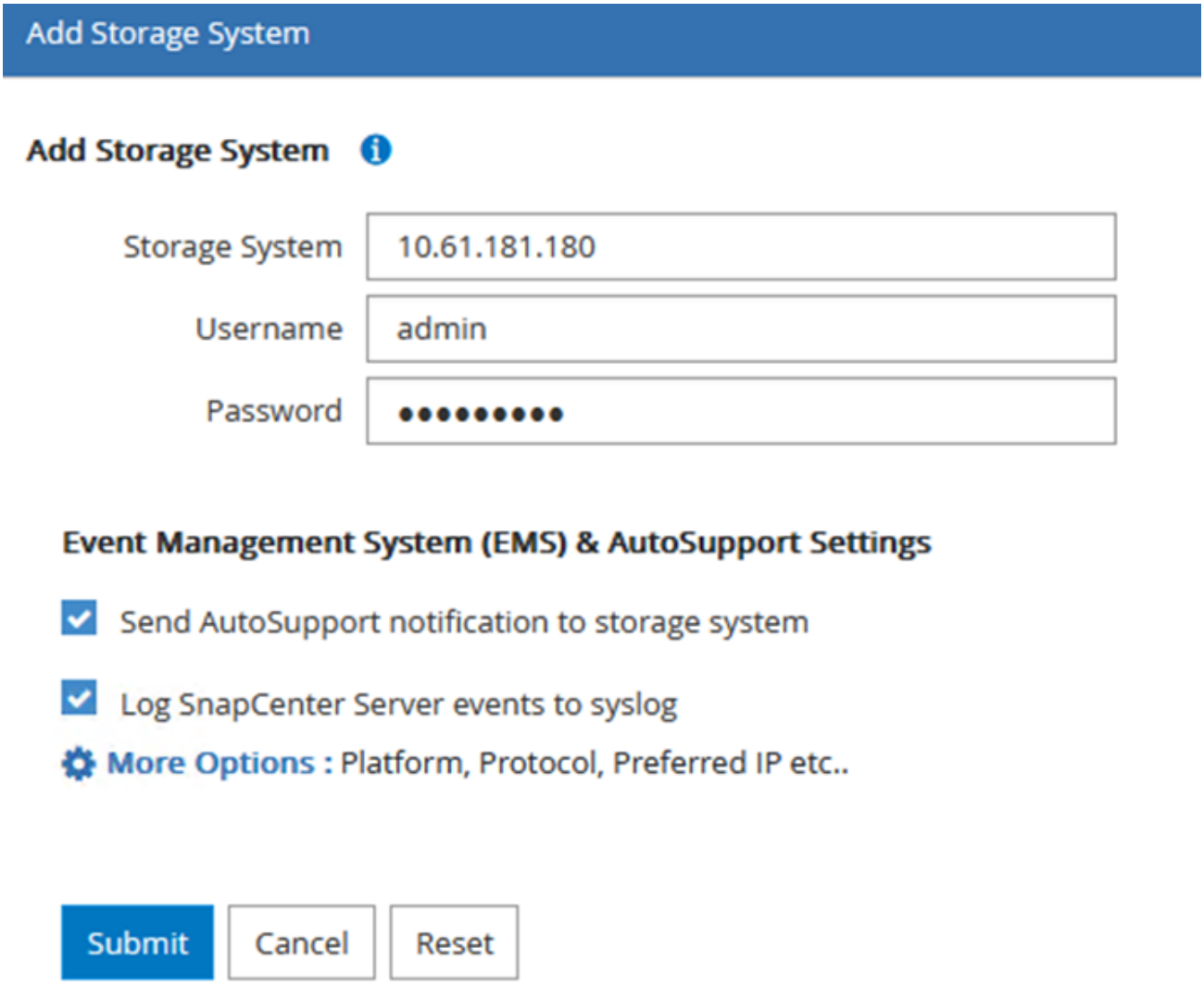
▼ **SnapCenter**にストレージコントローラを追加する

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

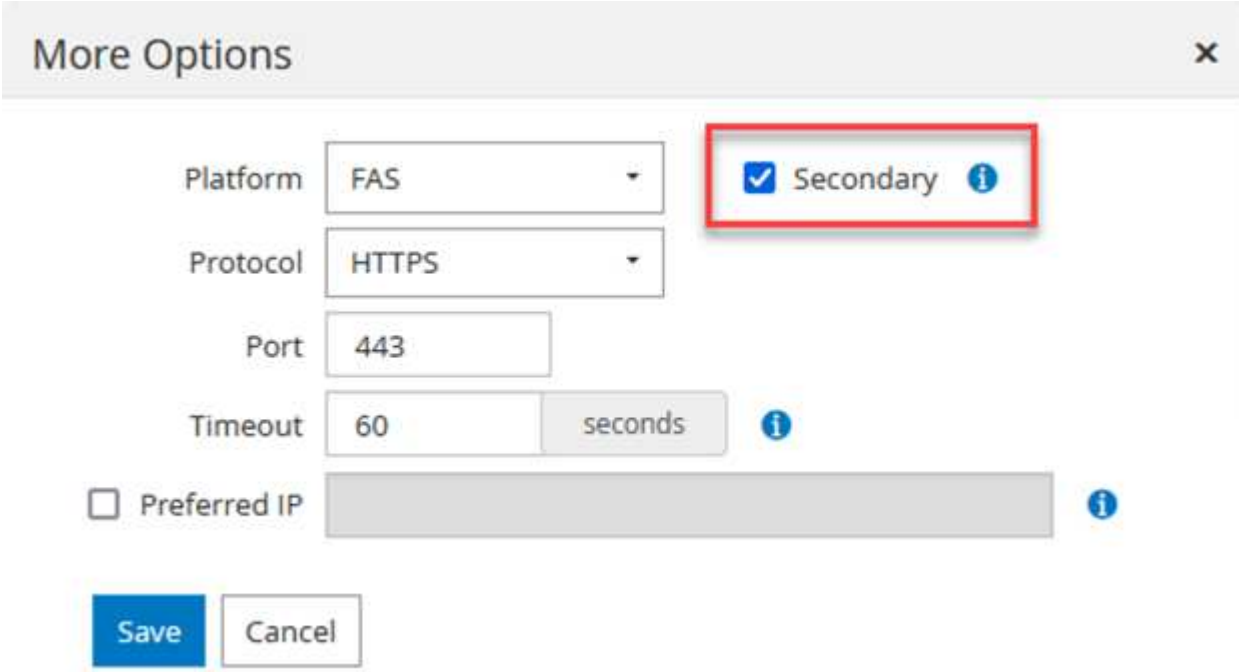
1. 左側のメニューから [ストレージ システム] を選択し、[新規] をクリックして、ストレージ コントローラーをSnapCenterに追加するプロセスを開始します。



2. [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クラスターの管理 IP アドレスとユーザー名およびパスワードを追加します。次に、「送信」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. このプロセスを繰り返して、FSx ONTAPシステムをSnapCenterに追加します。この場合、「ストレージ システムの追加」ウィンドウの下部にある「その他のオプション」を選択し、「セカンダリ」のチェック ボックスをクリックして、FSx システムを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。

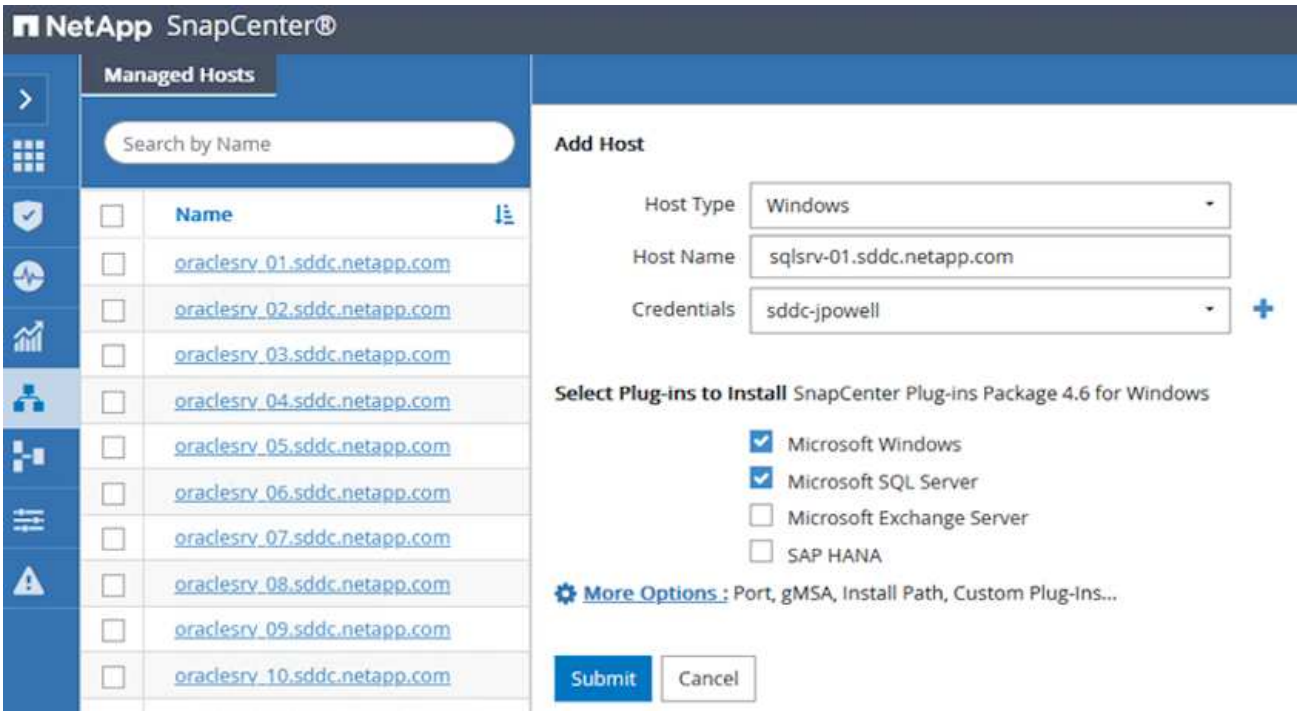


SnapCenterへのストレージシステムの追加に関する詳細については、次のドキュメントを参照してください。 "このリンク" 。

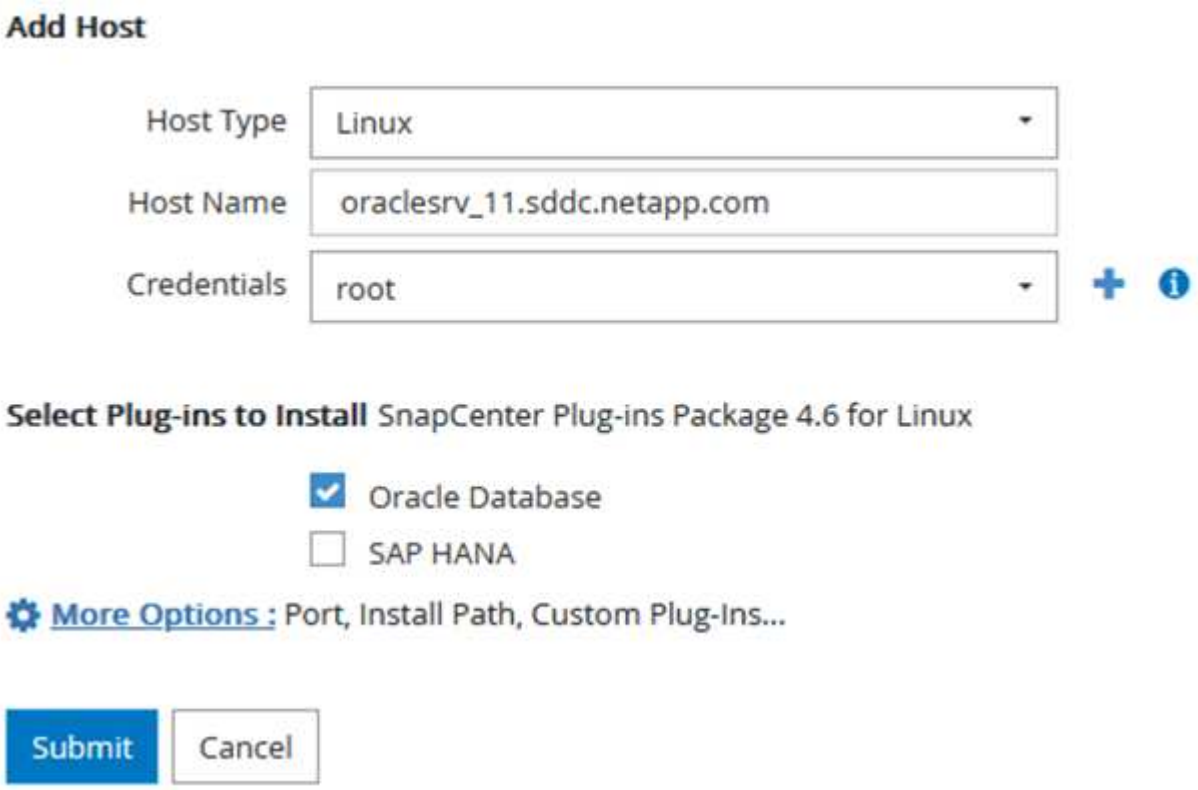
▼ **SnapCenter**にホストを追加する

次のステップは、ホスト アプリケーション サーバーをSnapCenterに追加することです。プロセスは SQL Server と Oracle の両方で同様です。

1. 左側のメニューから [ホスト] を選択し、[追加] をクリックして、 SnapCenterにストレージ コントローラーを追加するプロセスを開始します。
2. [ホストの追加] ウィンドウで、ホスト タイプ、ホスト名、およびホスト システムの資格情報を追加します。プラグインの種類を選択します。 SQL Server の場合は、Microsoft Windows および Microsoft SQL Server プラグインを選択します。



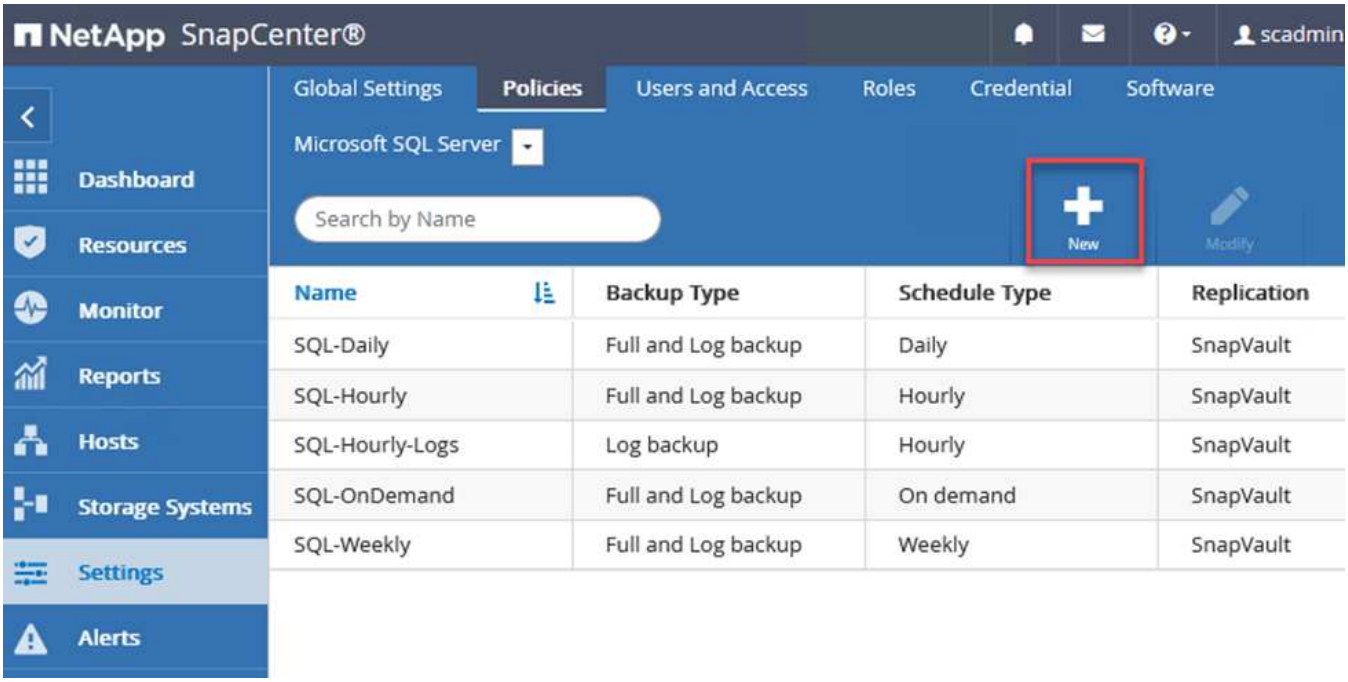
3. Oracleの場合、「ホストの追加」ダイアログボックスの必須フィールドに入力し、Oracle Databaseプラグインのチェックボックスをオンにします。「送信」をクリックすると検出プロセスが開始され、ホストがSnapCenterに追加されます。



▼ **SnapCenter**ポリシーを作成する

ポリシーは、バックアップ ジョブに従う特定のルールを確立します。これらには、バックアップ スケジュール、レプリケーション タイプ、 SnapCenter がトランザクション ログのバックアップと切り捨てを処理する方法などが含まれますが、これらに限定されません。

SnapCenter Web クライアントの [設定] セクションでポリシーにアクセスできます。



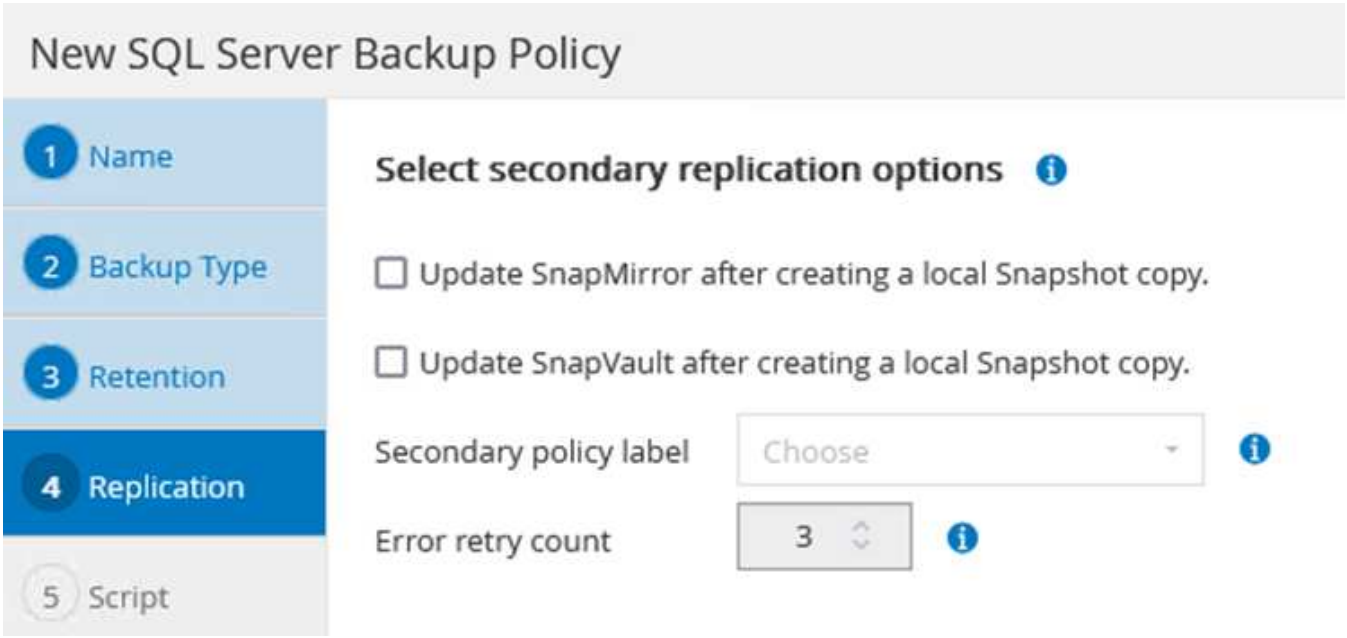
SQL Serverバックアップのポリシー作成の詳細については、 "SnapCenterのドキュメント" 。

Oracleバックアップのポリシー作成の詳細については、 "SnapCenterのドキュメント" 。

注記:

- ポリシー作成ウィザードを進める際には、レプリケーション セクションに特に注意してください。このセクションでは、バックアップ プロセス中に取得するセカンダリSnapMirrorコピーの種類を指定します。
- 「ローカル Snapshot コピーの作成後にSnapMirrorを更新する」設定は、同じクラスタに存在する 2 つのストレージ仮想マシン間にSnapMirror関係が存在する場合に、そ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 を更新する」設定は、2 つの別個のクラスター間、およびオンプレミスのONTAPシステムとCloud Volumes ONTAPまたは FSx ONTAP間に存在するSnapMirror関係を更新するために使用されます。

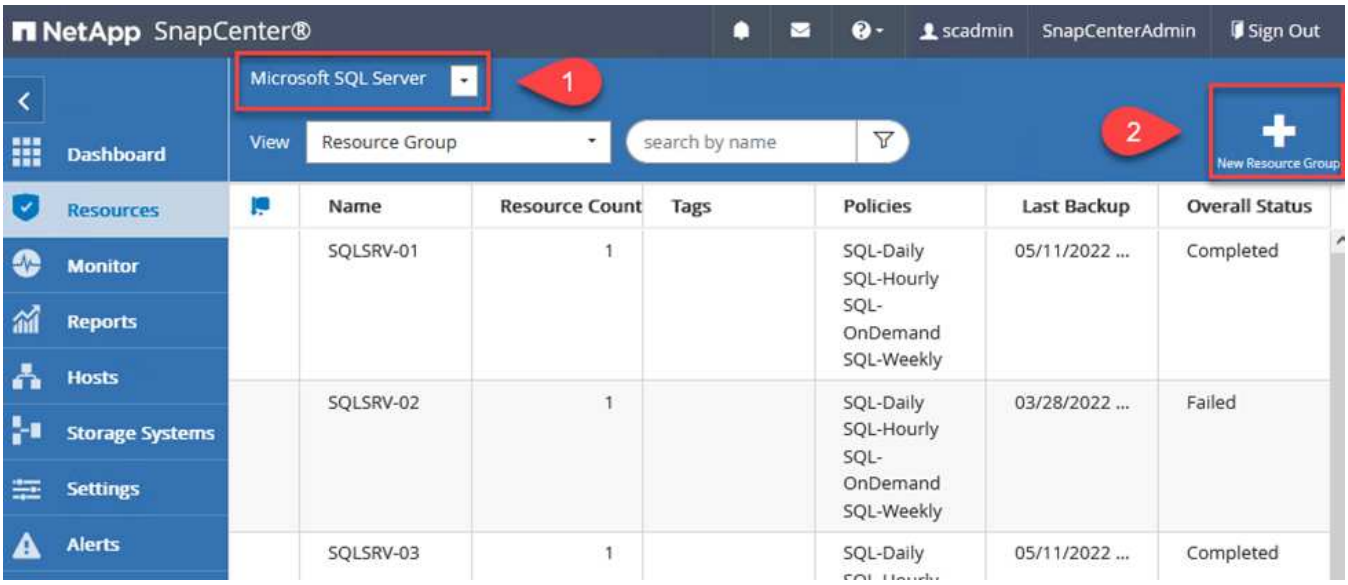
次の画像は、上記のオプションと、それらがバックアップ ポリシー ウィザードでどのように表示されるかを示しています。



▼ **SnapCenter**リソース グループを作成する

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 リソースと、それらのリソースに適用するポリシーを選択できます。

1. 左側のメニューの「リソース」セクションに移動します。
2. ウィンドウの上部で、操作するリソース 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 と Oracle データベースの両方のリソース グループを作成する手順が詳細に説明されています。

SQLリソースをバックアップするには、 "このリンク" 。

Oracleリソースのバックアップについては、 "このリンク" 。

Veeam バックアップ サーバーの導入と構成

このソリューションでは、Veeam Backup & Replication ソフトウェアを使用してアプリケーション仮想マシンをバックアップし、Veeam スケールアウト バックアップ リポジトリ (SOBR) を使用してバックアップのコピーを Amazon S3 バケットにアーカイブします。このソリューションでは、Veeam は Windows サーバーに展開されます。 Veeamの導入に関する具体的なガイダンスについては、 "Veeamヘルプセンター 技術ドキュメント" 。

▼ Veeamスケールアウトバックアップリポジトリを構成する

ソフトウェアを展開してライセンスを取得したら、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、災害復旧のために VM データのオフサイト バックアップとして S3 バケットも含める必要があります。

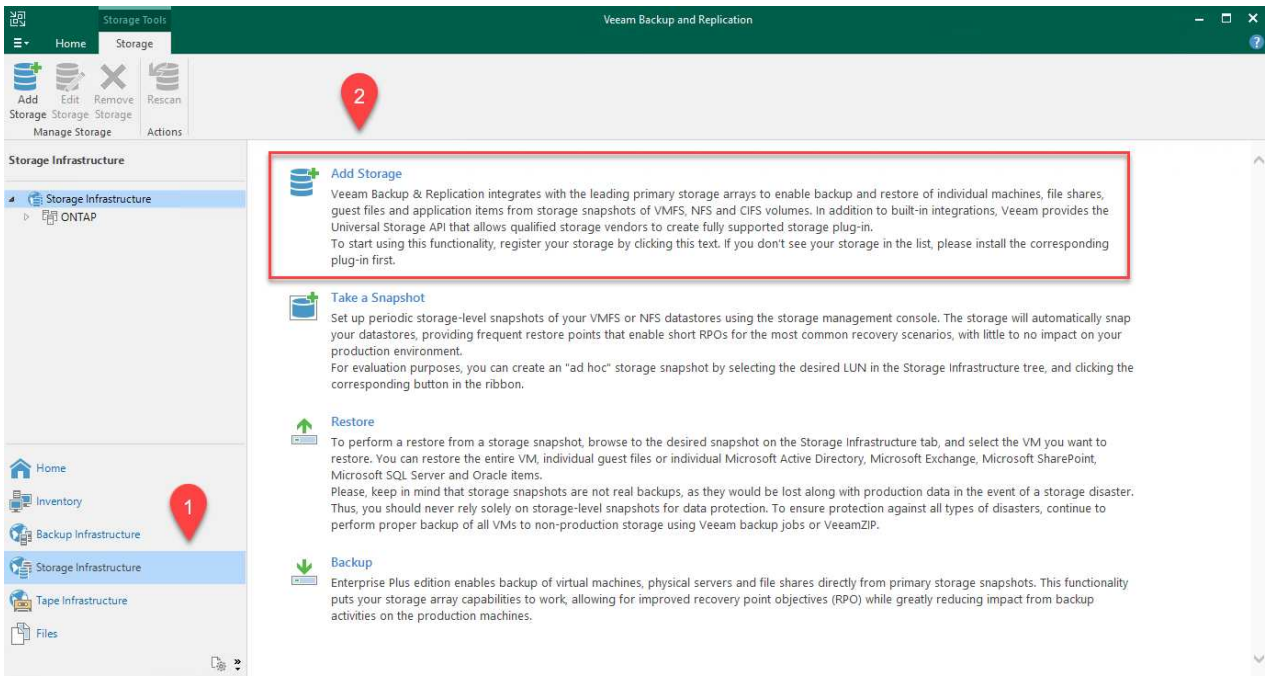
始める前に次の前提条件を確認してください。

1. オンプレミスのONTAPシステムに、バックアップのターゲット ストレージとして 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 バックアップのリポジトリです。

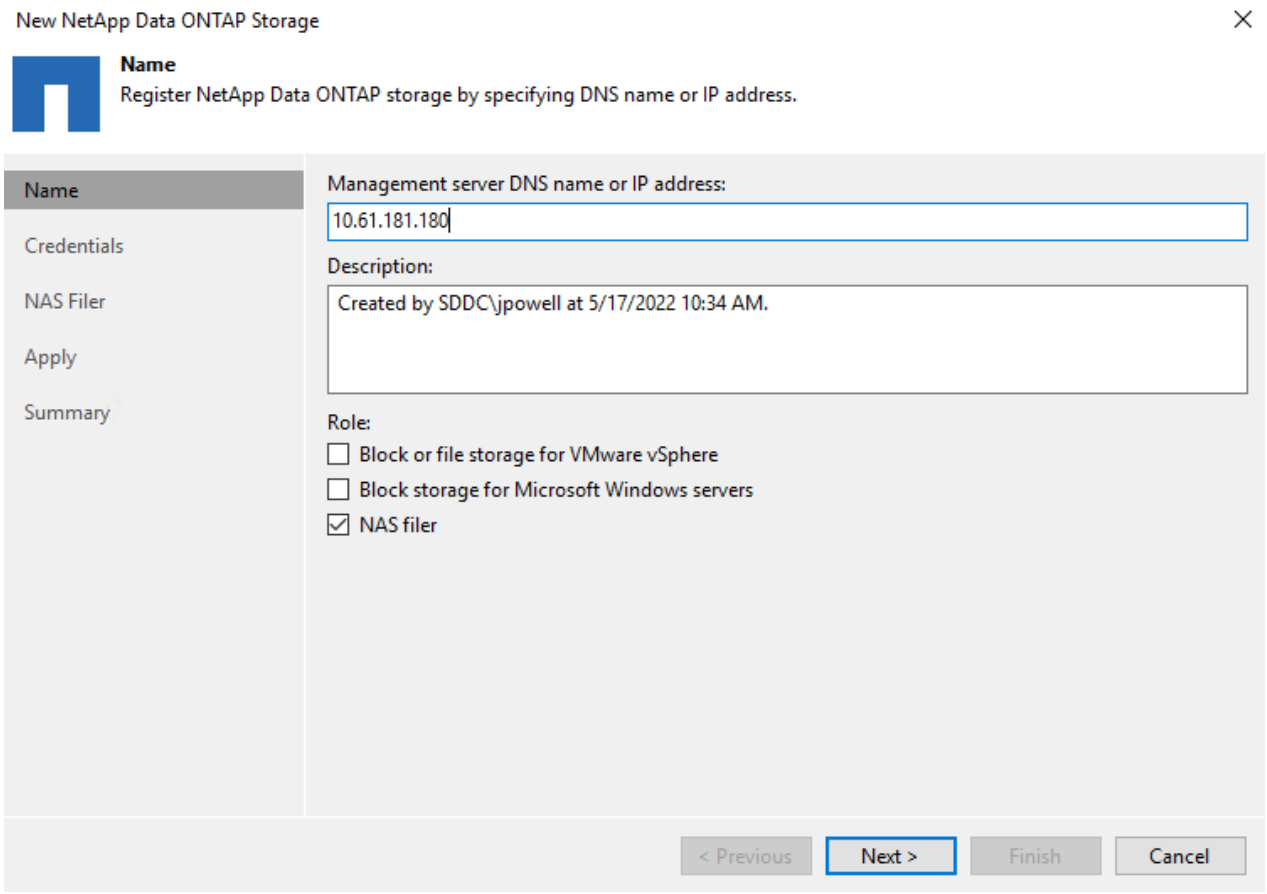
▼ VeeamにONTAPストレージを追加

まず、 ONTAPストレージ クラスターと関連する SMB/NFS ファイルシステムを Veeam のストレージ インフラストラクチャとして追加します。

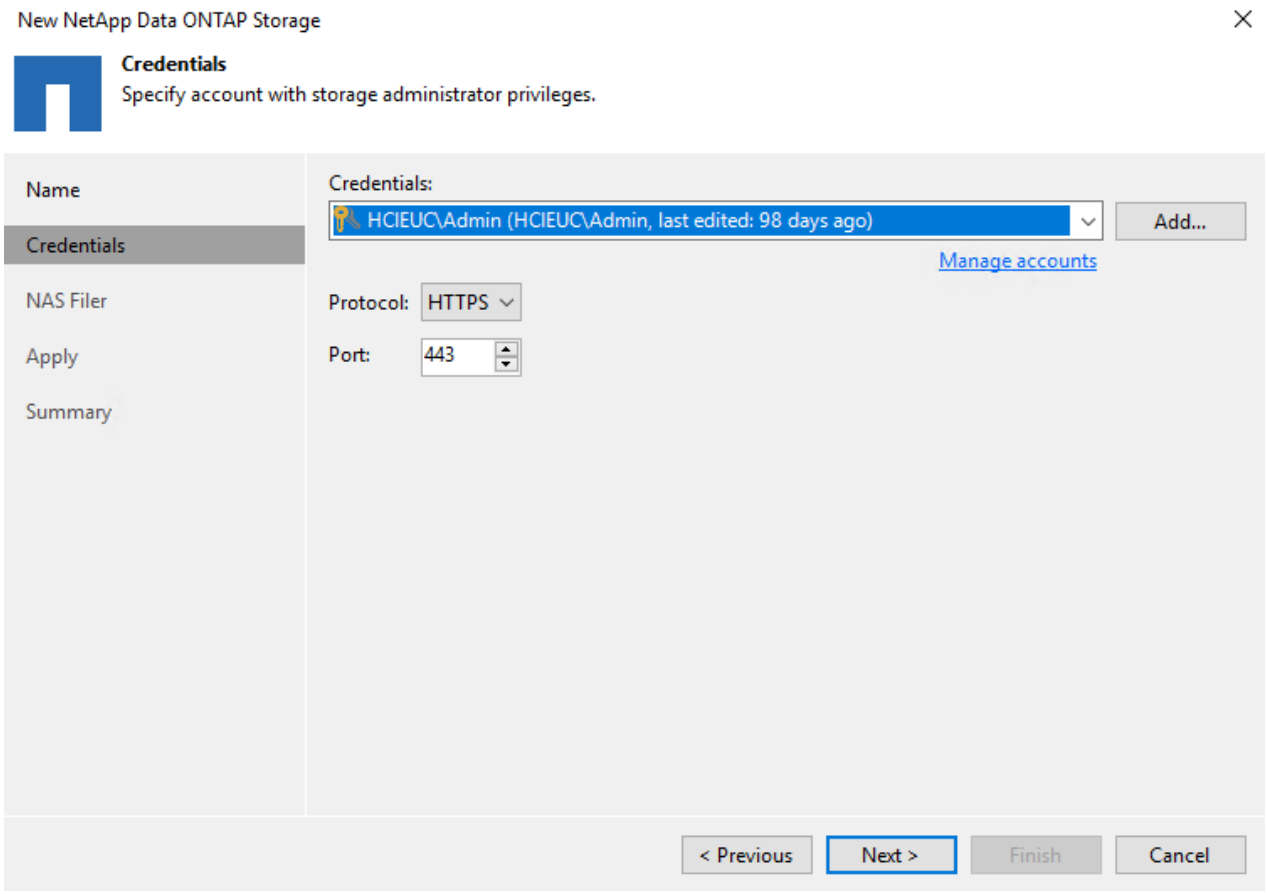
1. Veeam コンソールを開いてログインします。「ストレージ インフラストラクチャ」に移動し、「ストレージの追加」を選択します。



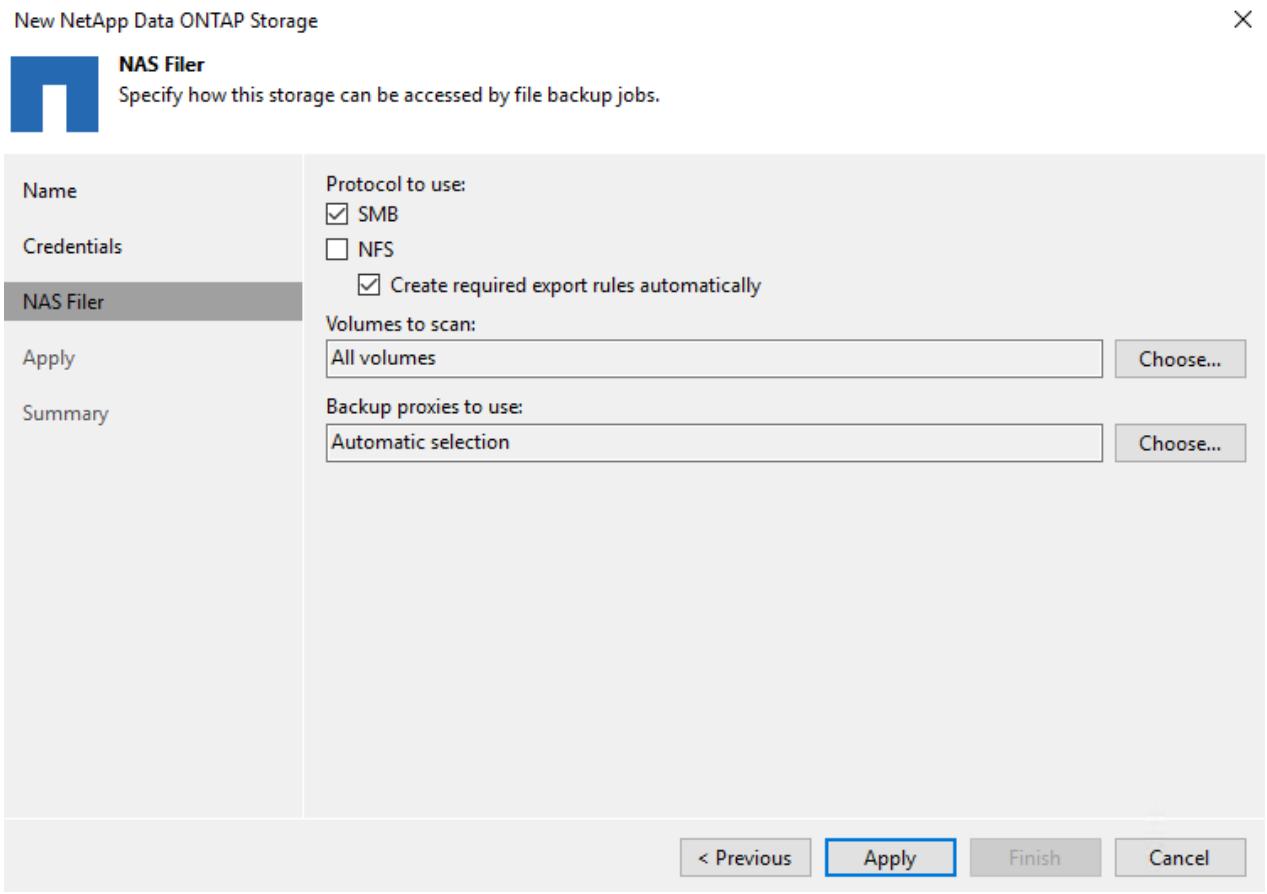
2. ストレージの追加ウィザードで、ストレージ ベンダーとしてNetAppを選択し、 Data ONTAPを選択します。
3. 管理 IP アドレスを入力し、NAS Filer ボックスをオンにします。[Next]をクリックします。



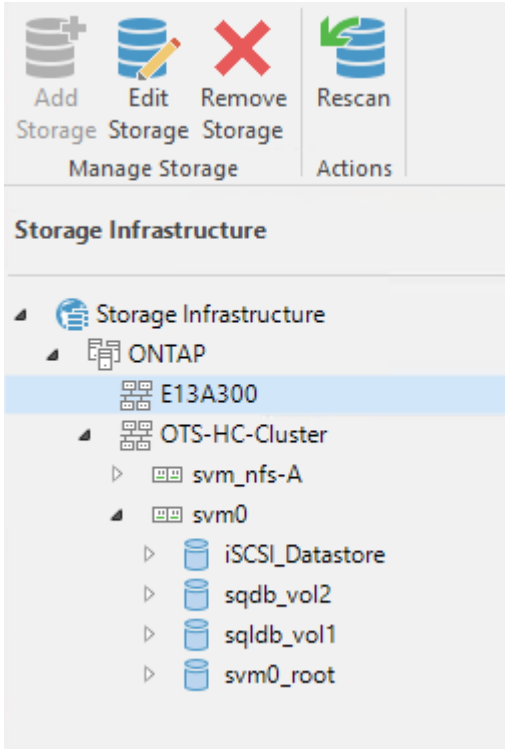
4. ONTAPクラスターにアクセスするための資格情報を追加します。



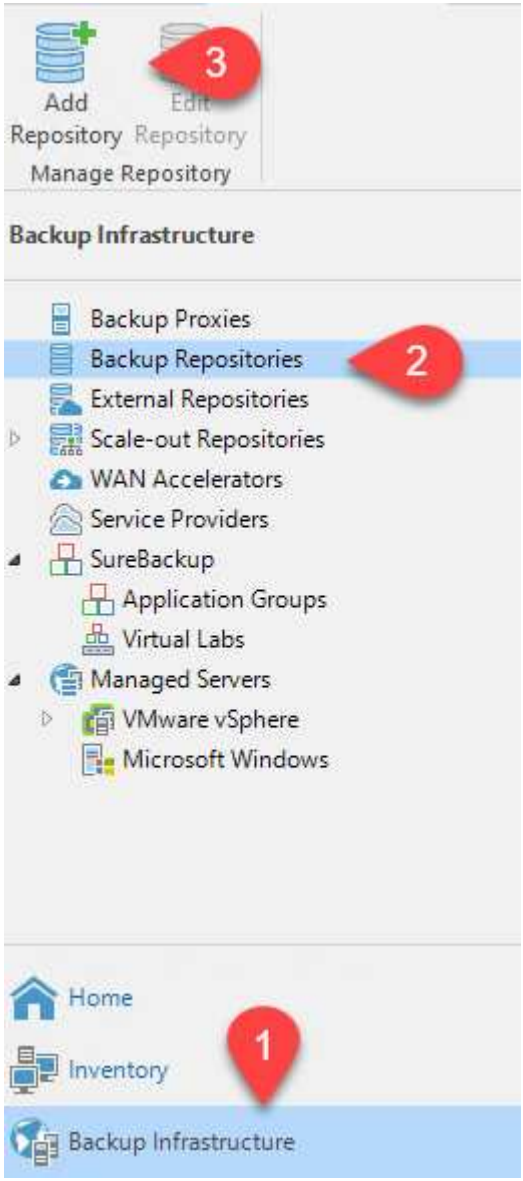
5. NAS Filer ページで、スキャンするプロトコルを選択し、「次へ」を選択します。



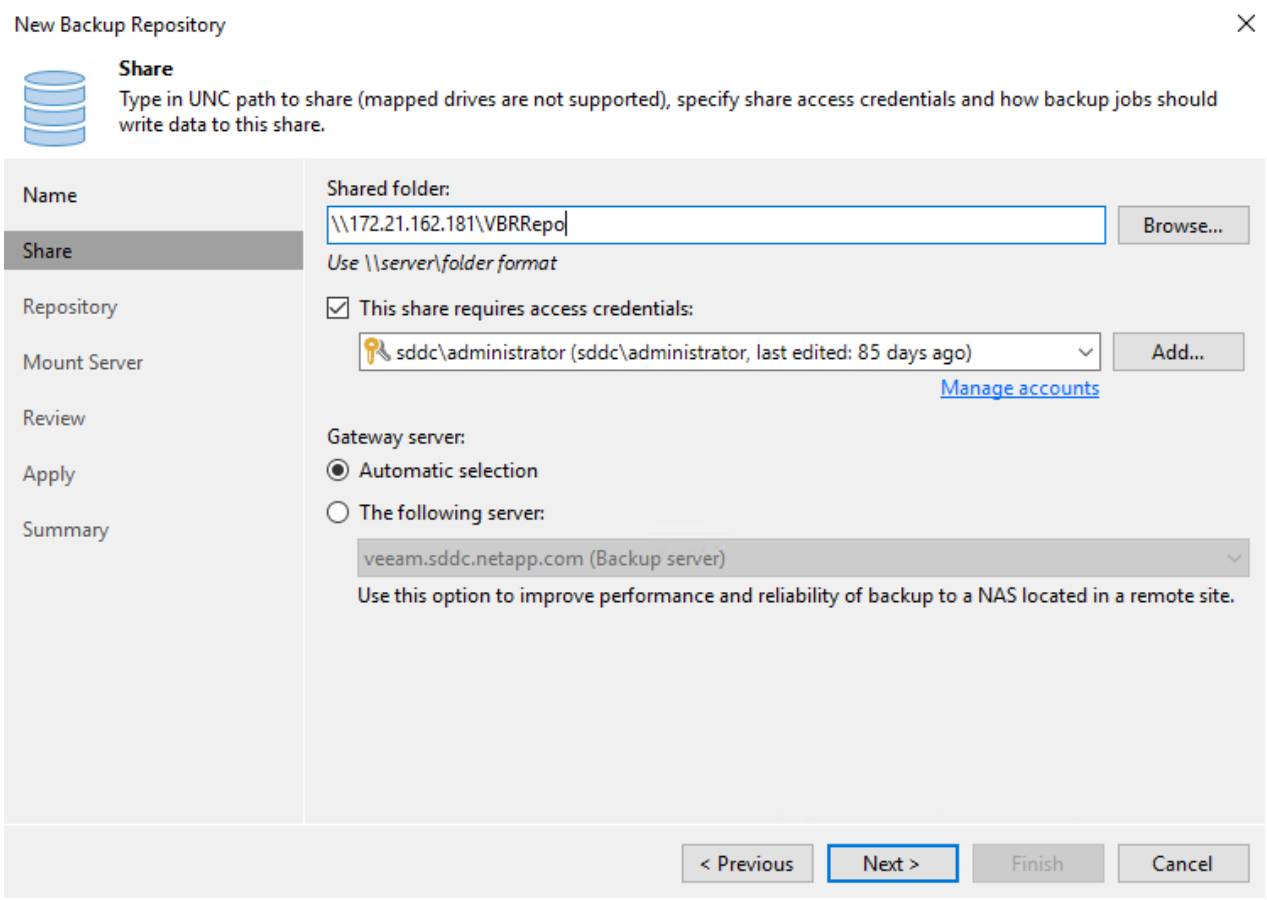
6. ウィザードの [適用] ページと [概要] ページを完了し、[完了] をクリックしてストレージ検出プロセスを開始します。スキャンが完了すると、 ONTAPクラスターが NAS ファイラーとともに使用可能なリソースとして追加されます。



7. 新しく検出された 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から、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項目をクリックします。



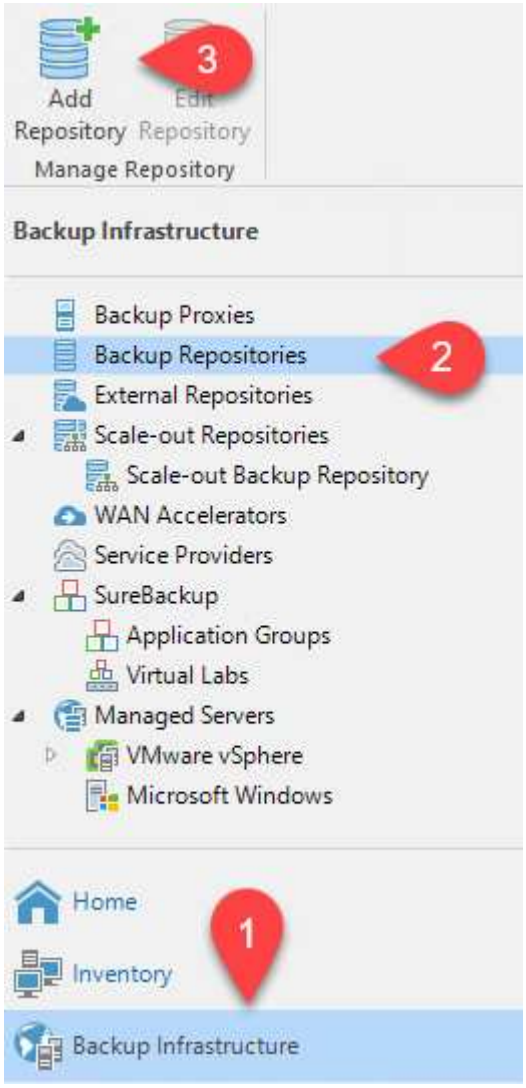
8. 新しいバックアップ リポジトリ ウィザードのすべての手順に従ってリポジトリを作成します。Veeamバックアップリポジトリの作成の詳細については、 "Veeamのドキュメント" 。



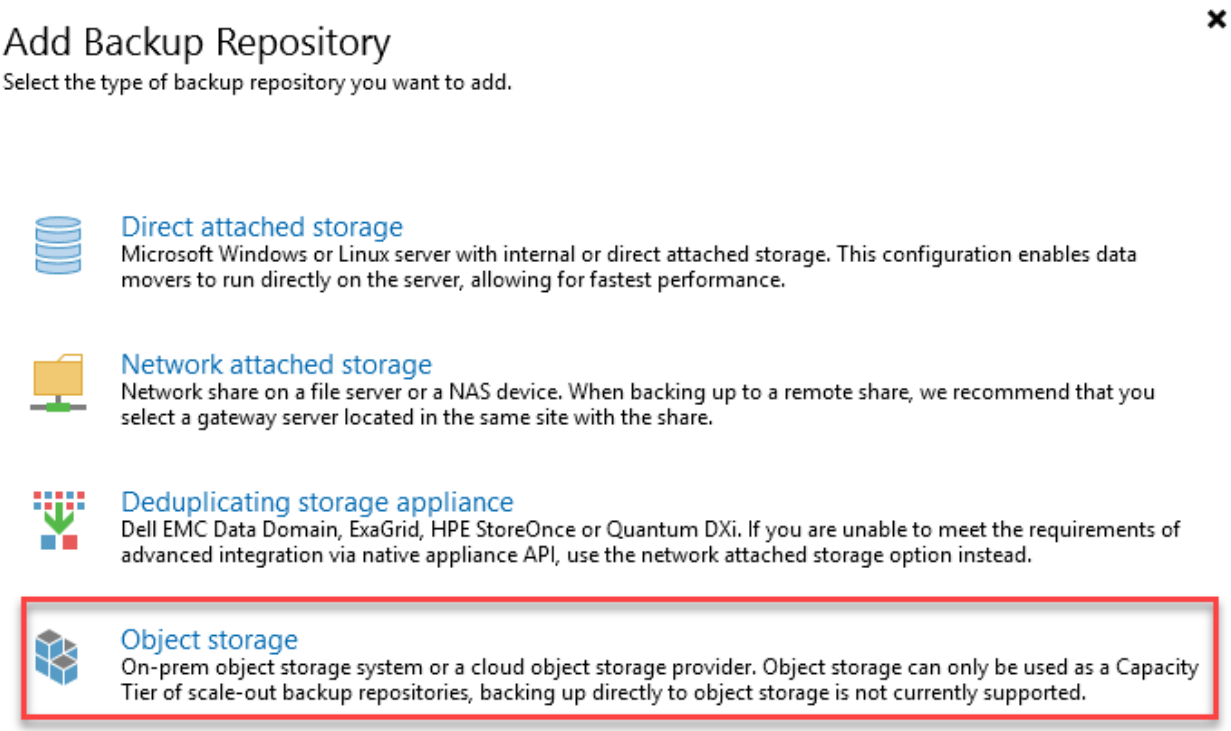
▼ **Amazon S3** バケットをバックアップリポジトリとして追加する

次のステップは、Amazon S3 ストレージをバックアップ リポジトリとして追加することです。

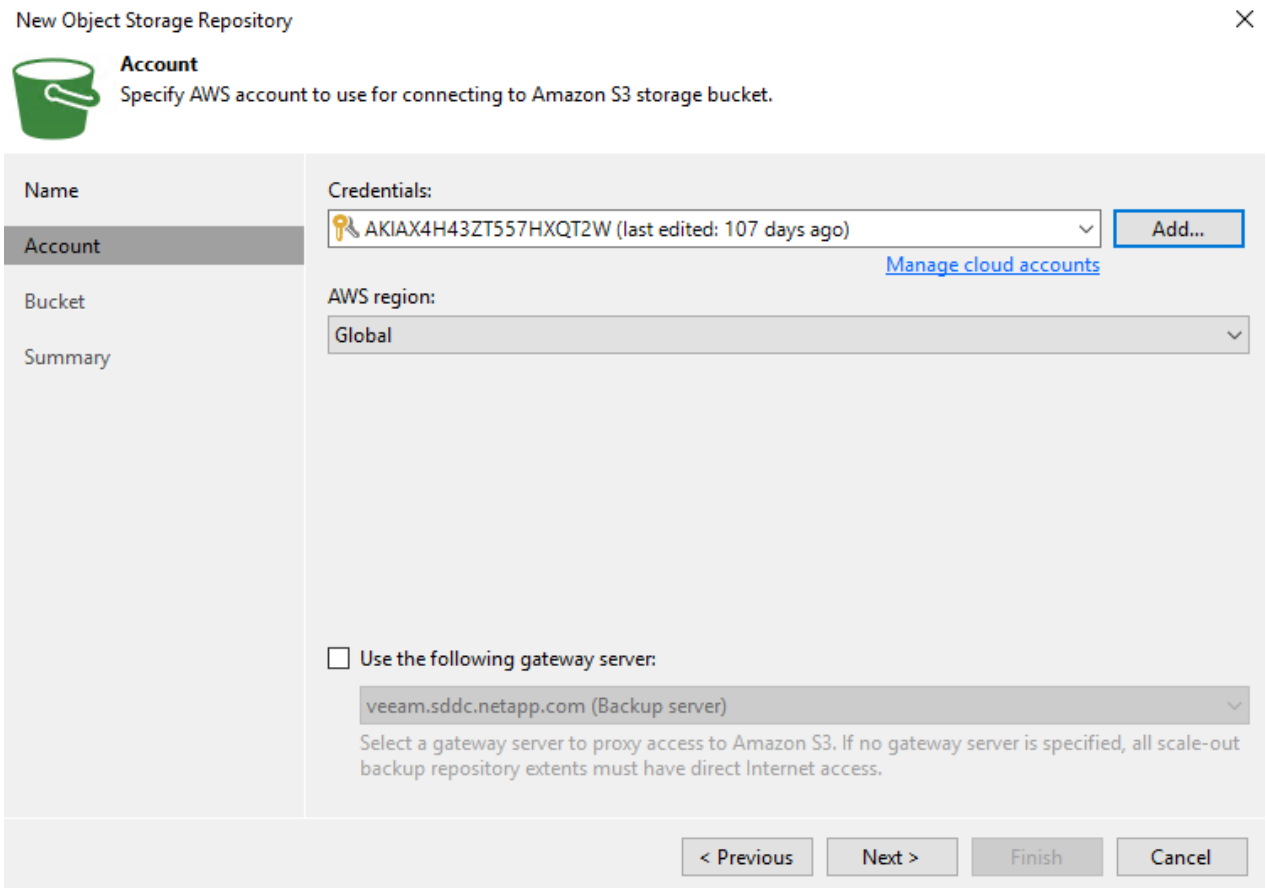
1. [バックアップ インフラストラクチャ] > [バックアップ リポジトリ] に移動します。リポジトリの追加をクリックします。



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 ストレージを選択し、Amazon S3 を選択します。これにより、新しいオブジェクト 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指定して、「次へ」をクリックします。
4. 次のセクションで、資格情報を入力します。 AWS アクセスキーとシークレットキーが必要です。



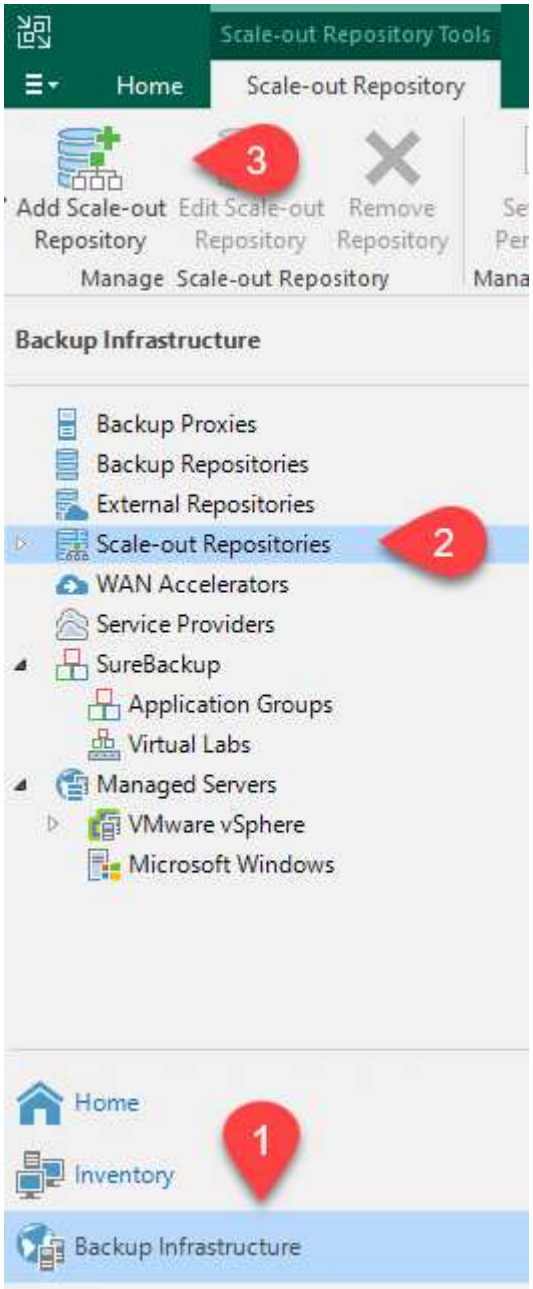
5. Amazon 構成が読み込まれたら、データセンター、バケット、フォルダーを選択し、「適用」をクリ

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。

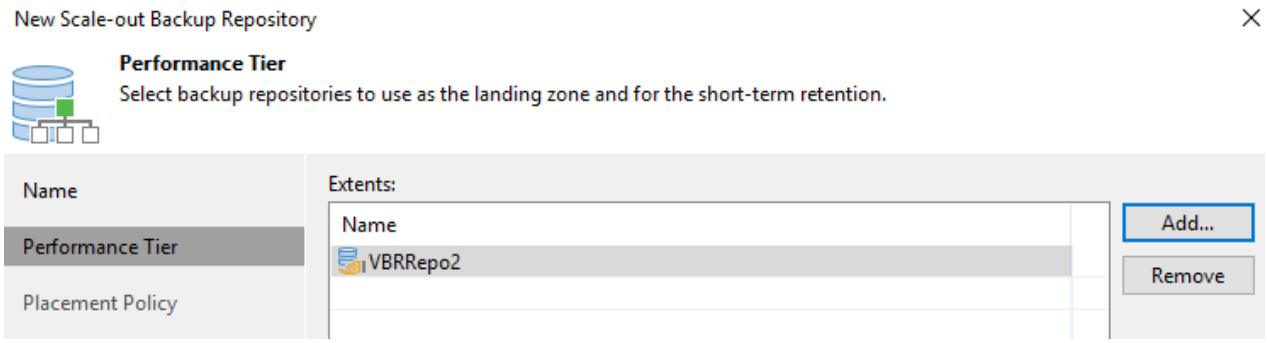
▼ スケールアウトバックアップリポジトリを作成する

ストレージ リポジトリを Veeam に追加したので、災害復旧のためにオフサイトの 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する SOBR を作成できます。

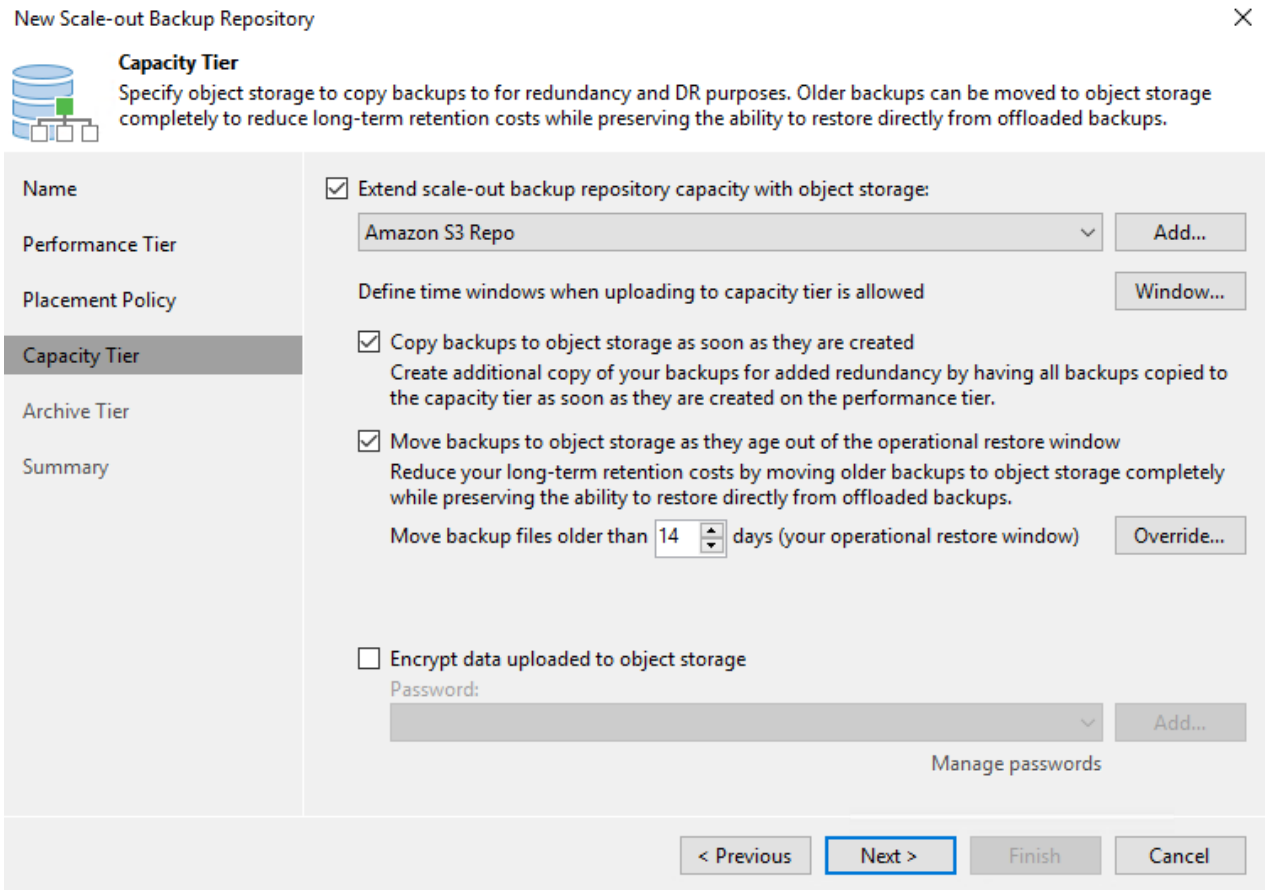
1. バックアップ インフラストラクチャから、スケールアウト リポジトリを選択し、スケールアウト リポジトリの追加メニュー項目をクリックします。



2. 新しいスケールアウト バックアップ リポジトリで SOBR の名前を入力し、[次へ] をクリックします。
3. パフォーマンス層では、ローカル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. 配置ポリシーでは、要件に基づいてデータのローカリティまたはパフォーマンスのいずれかを選択します。次へを選択します。
5. 容量層では、Amazon S3 オブジェクト ストレージを使用して SOBR を拡張します。災害復旧のために、セカンダリ バックアップがタイムリーに配信されるように、[バックアップが作成され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」と「完了」を選択して、SOBR の作成を完了します。

▼ スケールアウトバックアップリポジトリジョブを作成する

Veeam を構成する最後の手順は、新しく作成された SOBR をバックアップ先として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通常の業務の一部であるため、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作成の詳細については、 "Veeamヘルプセンター技術ドキュメント" 。

NetApp Backup and Recoveryツールと構成

AWS で実行されている VMware Cloud Volumes サービスへのアプリケーション VM とデータベース ボリュームのフェイルオーバーを実行するには、 SnapCenter Server 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構成する必要があります。フェー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ールバックが計画され実行されるまで、通常のバックアップ操作を再開するようにこれらのツールを構成する必要もあります。

▼ セカンダリ **Windows SnapCenter Server** を展開する

SnapCenter Server は、VMware Cloud SDDC にデプロイされるか、VMware Cloud 環境にネットワーク接続された VPC にある EC2 インスタンスにインストールされます。

SnapCenter softwareはNetApp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存在する 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、 "NetAppドキュメント センター" 。

SnapCenter softwareは次の場所にあります。 "このリンク" 。

▼ セカンダリ **Windows SnapCenter Server** を構成する

FSx ONTAPにミラーリングされたアプリケーション データの復元を実行するには、まずオンプレミスのSnapCenterデータベースの完全復元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、FSx ONTAP をプライマリ ストレージとして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。

これを実現するには、 SnapCenterサーバーで次の項目を完了する必要があります。

1. コンピューター名を元のオンプレミスのSnapCenter Server と同じになるように構成します。
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構成します。
3. SnapCenterデータベースを復元する手順を完了します。
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て、FSx がバックアップのプライマリ ストレージになっていることを確認します。
5. 復元され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**サーバーを導入する

Veeam Backup & Replication サーバーは、VMware Cloud on AWS 内の Windows サーバーまたは EC2 インスタンスにインストールできます。詳細な実装ガイダンスについては、 "Veeamヘルプセンター技術ドキュメント" 。

▼ セカンダリ **Veeam Backup & Replication** サーバーを構成する

Amazon S3 ストレージにバックアップされた仮想マシンの復元を実行するには、Windows サーバーに Veeam Server をインストールし、VMware Cloud、FSx ONTAP、および元のバックアップ リポジトリを含む S3 バケットと通信するように構成する必要があります。また、VM を復元した後に新しいバックアップを実行するには、FSx ONTAPに新しいバックアップ リポジトリを構成する必要があります。

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ようにネットワークを構成します。
2. FSx ONTAP上の SMB 共有を新しいバックアップ リポジトリとして構成します。

3. オンプレミスのスケールアウト バックアップ リポジトリの一部として使用されていた元の S3 バケットをマウントします。
4. VM を復元した後、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の復元の詳細については、セクションを参照してください。"Veeam Full Restore でアプリケーション VM を復元する" 。

災害復旧のための**SnapCenter**データベースバックアップ

SnapCenter、災害発生時にSnapCenterサーバーを復旧できるように、基盤となる MySQL データベースと構成データのバックアップと復旧が可能です。私たちのソリューションでは、VPC にある AWS EC2 インスタンス上のSnapCenterデータベースと構成を復元しました。 SnapCenterの災害復旧の詳細については、以下を参照してください。 "このリンク" 。

▼ **SnapCenter**バックアップの前提条件

SnapCenterバックアップには次の前提条件が必要です。

- バックアップされたデータベースと構成ファイルを見つけるためにオンプレミスのONTAPシステム上に作成されたボリュームと SMB 共有。
- 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 間のSnapMirror関係。この関係は、バックアップされたSnapCenterデータベースと構成ファイルを含むスナップショットを転送するために使用されます。
- EC2 インスタンスまたは VMware Cloud SDDC 内の VM のいずれかのクラウド アカウントにインストールされた Windows Server。
- VMware Cloud の Windows EC2 インスタンスまたは VM にインストールされたSnapCenter 。

▼ **SnapCenter** のバックアップと復元プロセスの概要

- バックアップ db および構成ファイルをホストするための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関係を設定します。
- SMB 共有をマウントします。
- API タスクを実行するための Swagger 認証トークンを取得します。
- db 復元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します (オンプレミスからSnapMirror経由でコピーされます)。
- FSx から EC2/VMware Cloud に SMB 共有をマウントします。
- 復元ディレクトリを SMB 共有からローカル ディレクトリにコピーします。
- Swagger から SQL Server の復元プロセスを実行します。

▼ **SnapCenter**データベースと構成をバックアップする

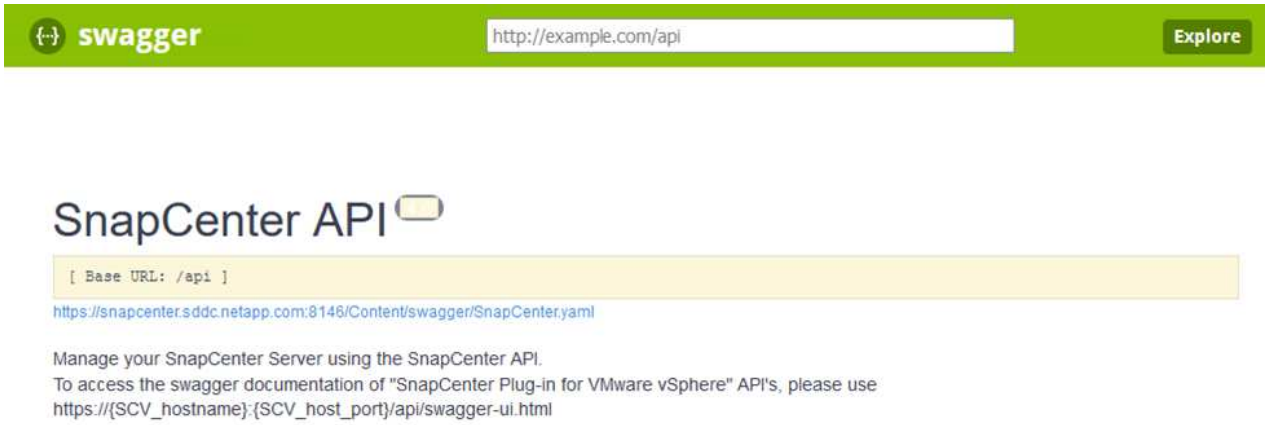
SnapCenter は、REST API コマンドを実行するための Web クライアント インターフェイスを提供します。 Swaggerを介してREST APIにアクセスする方法については、 SnapCenterのドキュメントを参照して

ください。 "このリンク" 。

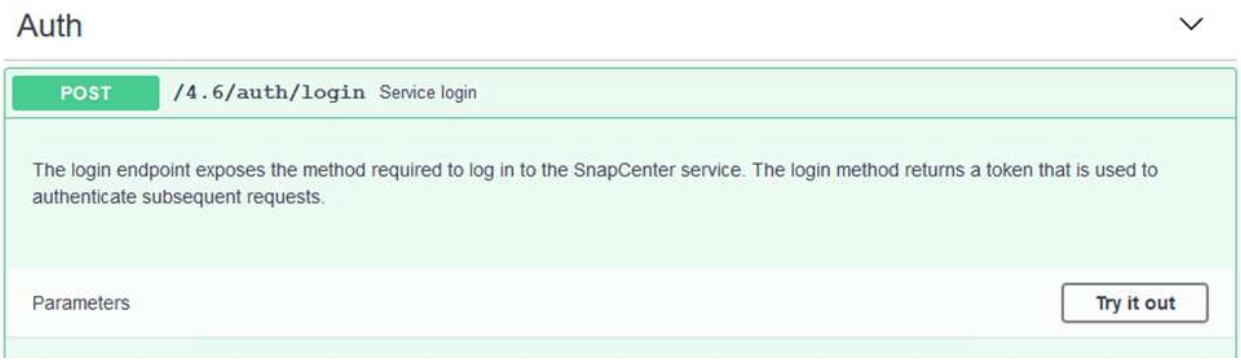
▼ **Swagger**にログインして認証トークンを取得する

Swagger ページに移動した後、データベース復元プロセスを開始するために認証トークンを取得する必要があります。

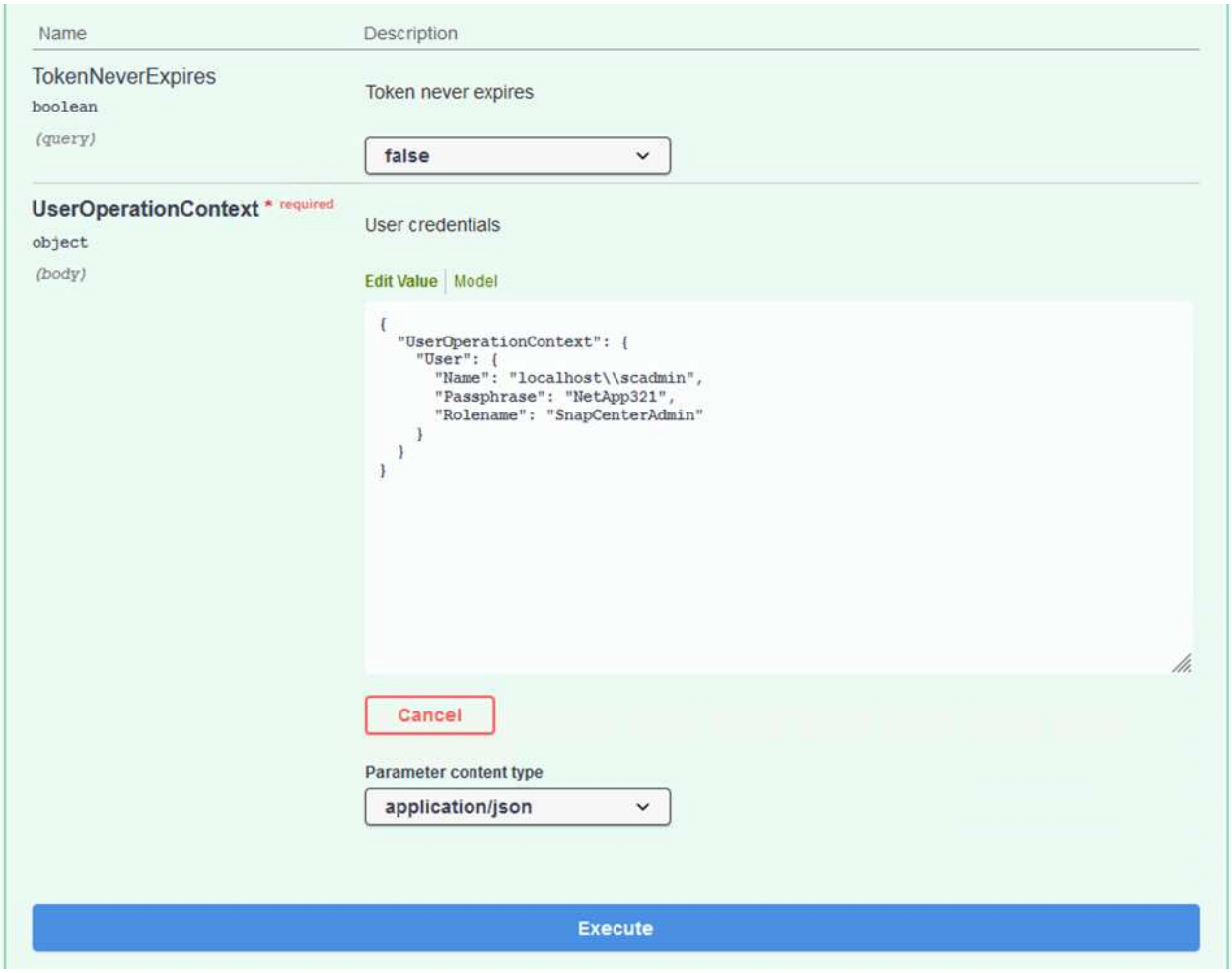
1. *https://< SnapCenter Server IP>:8146/swagger/* にあるSnapCenter Swagger API Web ページにアクセスします。



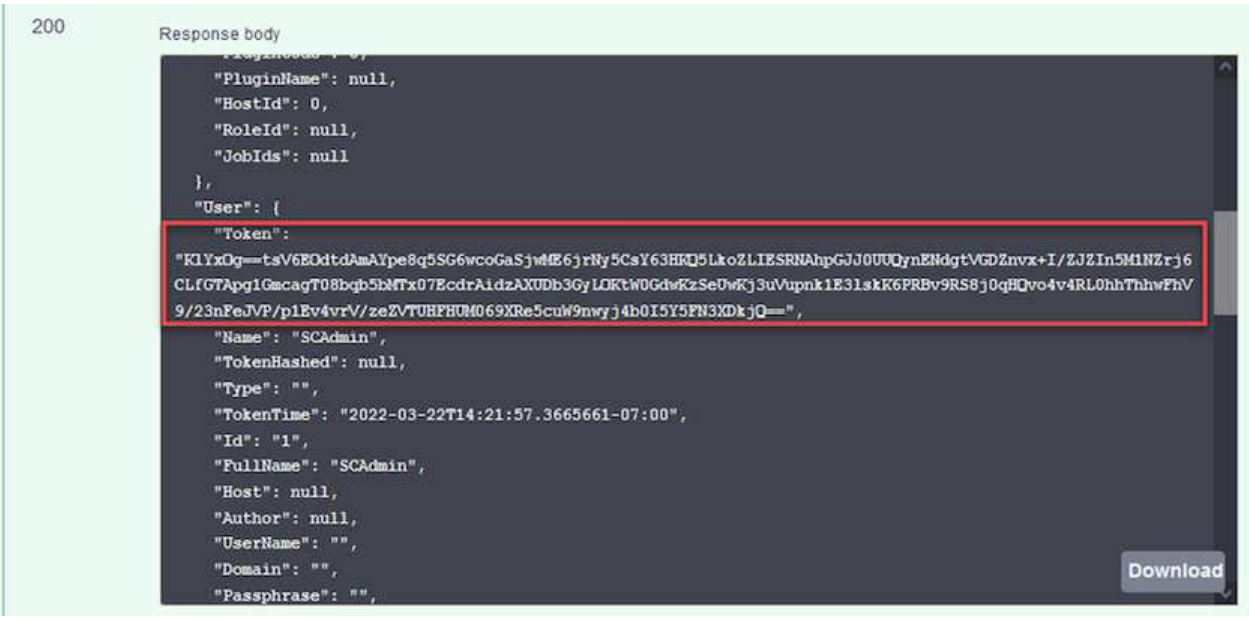
2. 認証セクションを展開し、「試してみる」をクリックします。



3. UserOperationContext 領域で、 SnapCenter の資格情報とロールを入力し、[実行] をクリックします。



4. 以下のレスポンス本文でトークンを確認できます。バックアッププロセスを実行するときに、認証用のトークンテキストをコピーします。

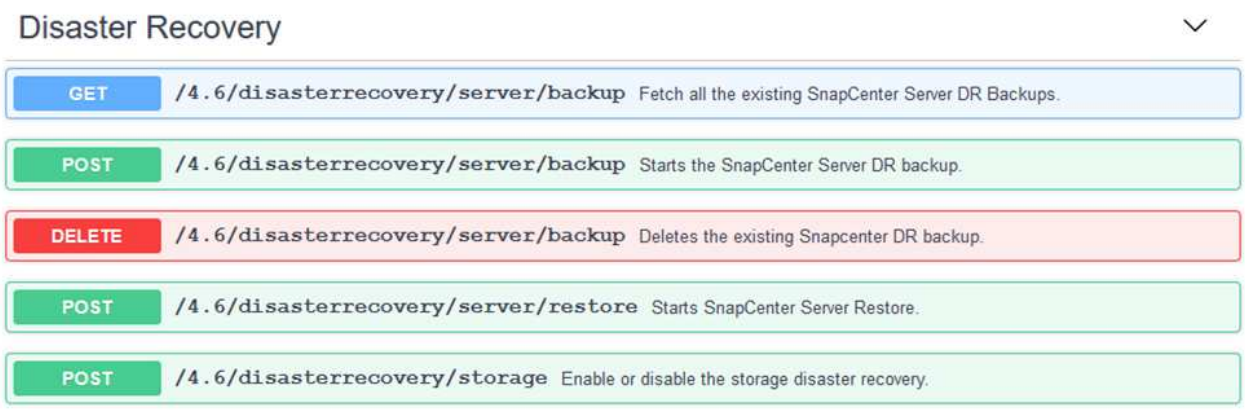


▼ **SnapCenter**データベースのバックアップを実行する

次に、Swagger ページの Disaster Recovery 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. 災害復旧領域をクリックして展開します。

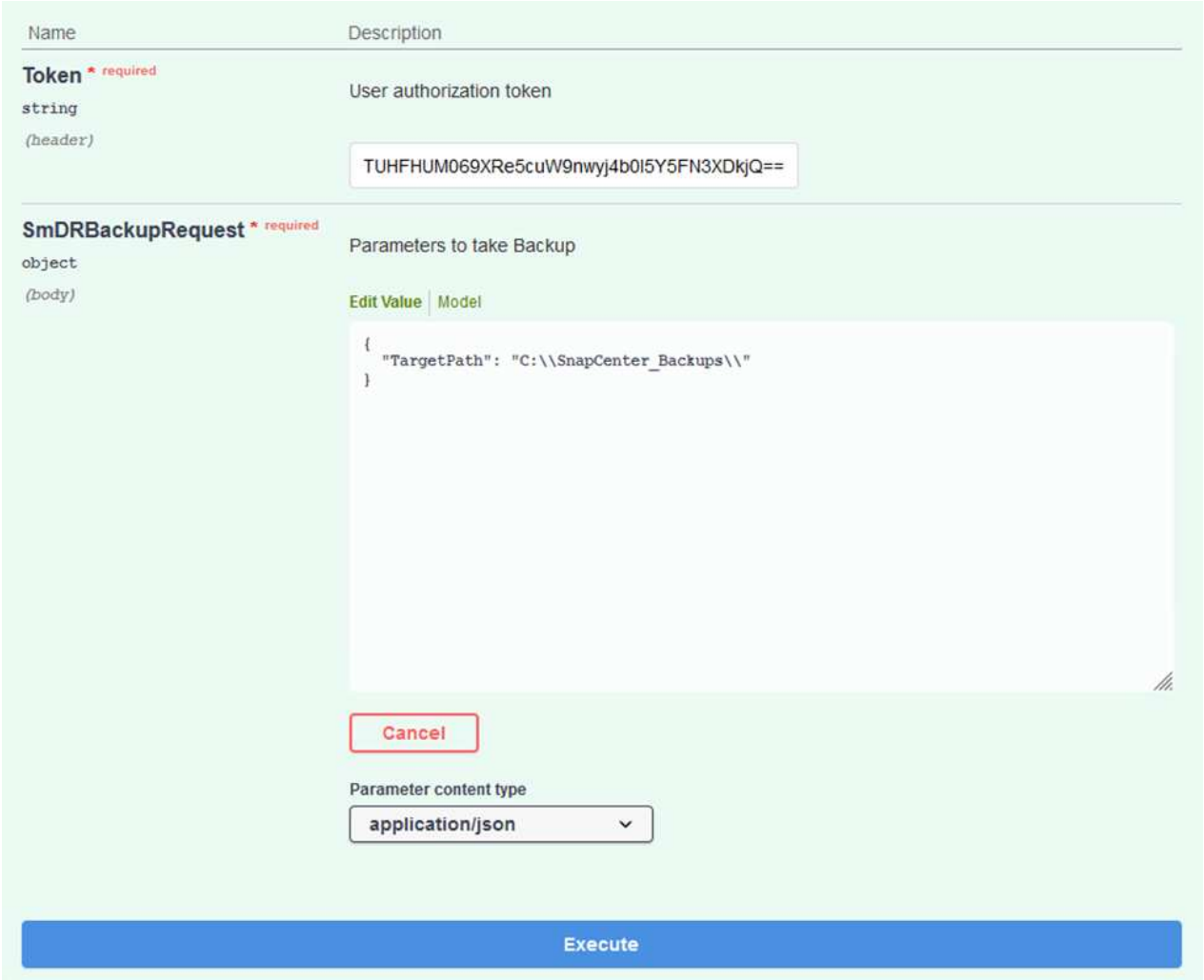


2. 拡大する `/4.6/disasterrecovery/server/backup`セクションにアクセスし、[試してみる] をクリックします。



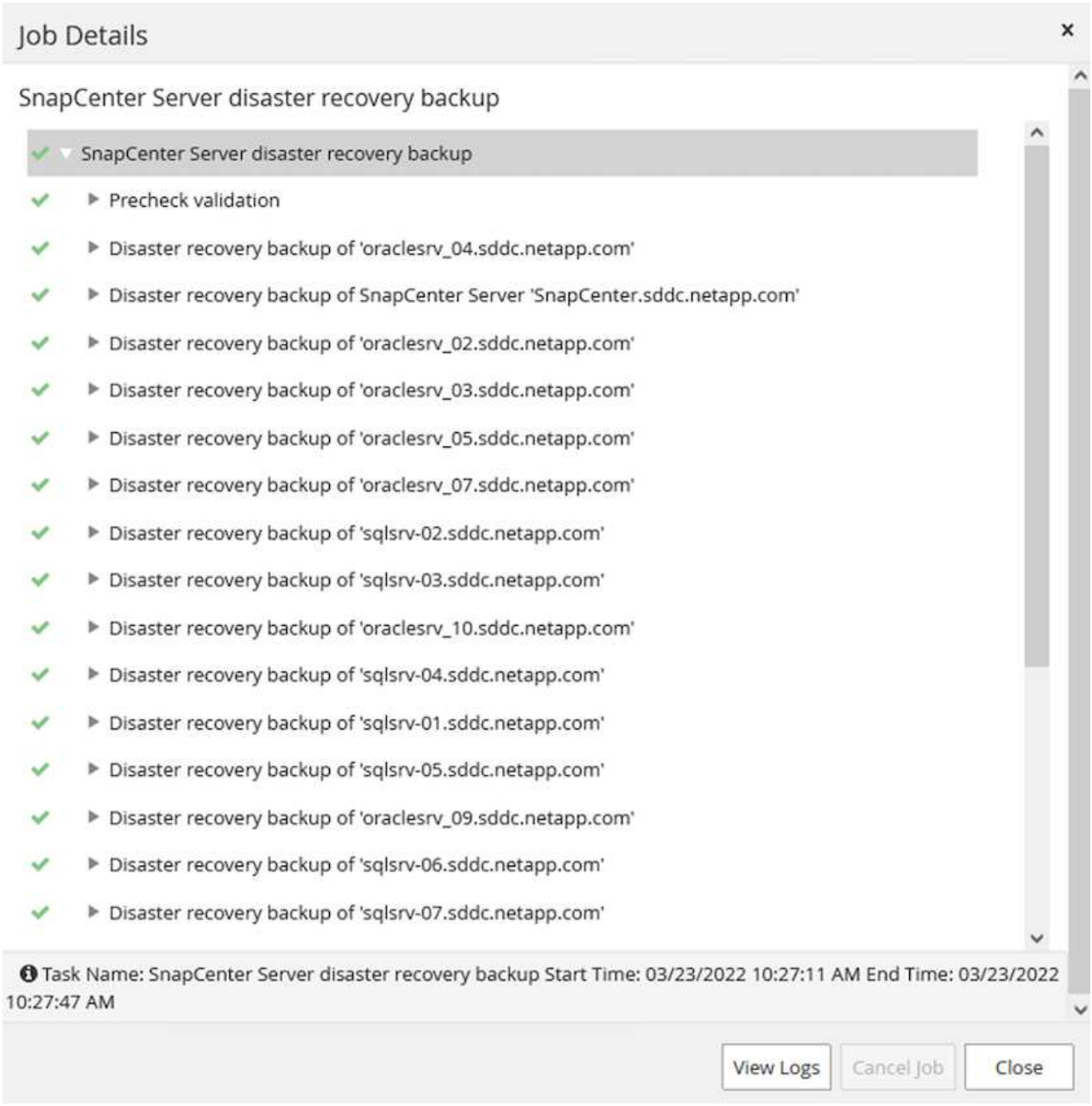
3. SmDRBackupRequest セクションで、正しいローカル ターゲット パスを追加し、[実行] を選択してSnapCenterデータベースと構成のバックアップを開始します。

> バックアップ プロセスでは、NFS または CIFS 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。



▼ **SnapCenter**からバックアップジョブを監視する

データベースの復元プロセスを開始するときは、 SnapCenterにログインしてログ ファイルを確認します。 [モニター] セクションでは、 SnapCenterサーバーの災害復旧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、データベースのバックアップファイルを**SMB**共有にコピーします。

次に、 SnapCenterサーバー上のローカル ドライブから、AWS の FSx インスタンスにあるセカンダリロケーションにデータをSnapMirrorコピーするために使用される CIFS 共有にバックアップを移動する必要があります。ファイルの権限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から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

▼ プライマリサイトで災害が発生

プライマリオンプレミスデータセンターで災害が発生した場合、VMware Cloud on AWS を使用して Amazon Web Services インフラストラクチャにあるセカンダリサイトへのフェイルオーバーがシナリオに含まれます。仮想マシンとオンプレミスのONTAPクラスターにはアクセスできなくなっていると想定します。さらに、 SnapCenterと Veeam の両方の仮想マシンにアクセスできなくなり、セカンダリ 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、インフラストラクチャのクラウドへのフェイルオーバーについて説明し、次のトピックを取り上げます。

- SnapCenterデータベースの復元。新しいSnapCenterサーバーが確立されたら、MySQL データベースと構成ファイルを復元し、データベースを災害復旧モードに切り替えて、セカンダリ FSx ストレージがプライマリ ストレージ デバイスになることができるようにします。
- Veeam Backup & Replication を使用してアプリケーション仮想マシンを復元します。 VM バックアップが含まれている S3 ストレージを接続し、バックアップをインポートして、VMware Cloud on AWS に復元します。
- SnapCenterを使用して SQL Server アプリケーション データを復元します。
- SnapCenterを使用して Oracle アプリケーション データを復元します。

▼ **SnapCenter**データベースの復元プロセス

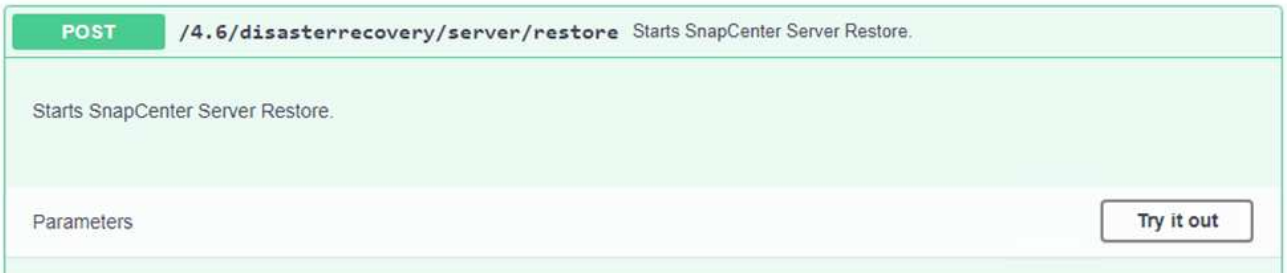
SnapCenter は、MySQL データベースと構成ファイルのバックアップと復元を可能にすることで、災害復旧シナリオをサポートします。これにより、管理者はオンプレミス データセンターでSnapCenterデータベースの定期的なバックアップを維持し、後でそのデータベースをセカンダリSnapCenterデータベースに復元できるようになります。

リモートSnapCenterサーバー上の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。

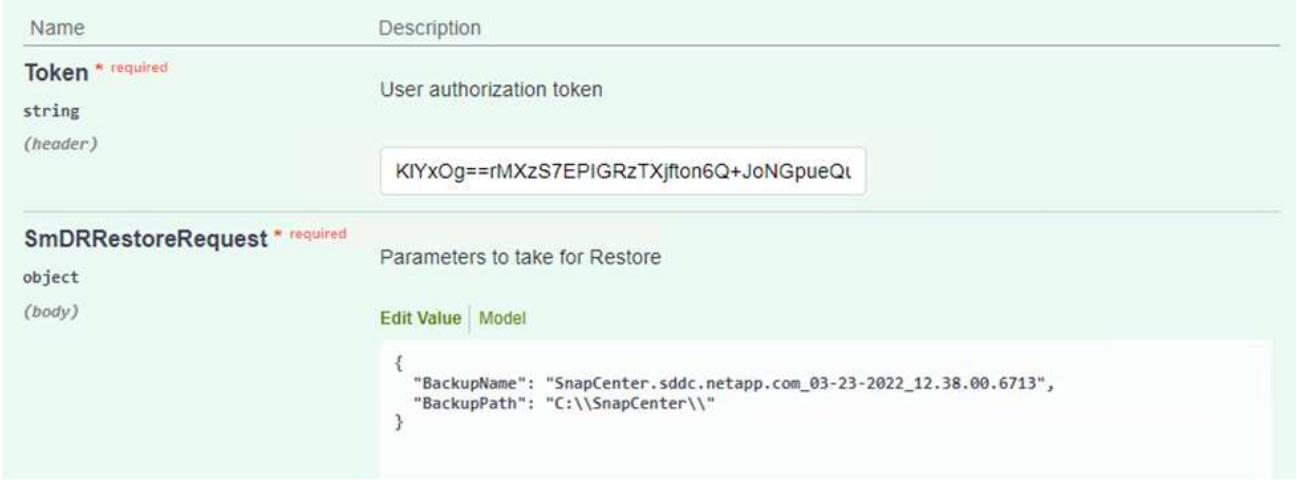
1. FSx クラスターからSnapMirror関係を解除し、ボリュームを読み取り/書き込み可能にします。
2. CIFS サーバーを作成し (必要な場合)、クローン ボリュームのジャンクション パスを指す CIFS 共有を作成します。
3. xcopy を使用して、バックアップ ファイルをセカンダリSnapCenterシステムのローカル ディレクトリにコピーします。
4. SnapCenter v4.6 をインストールします。
5. SnapCenterサーバーの FQDN が元のサーバーと同じであることを確認します。これは、DB の復元を成功させるために必要です。

復元プロセスを開始するには、次の手順を実行します。

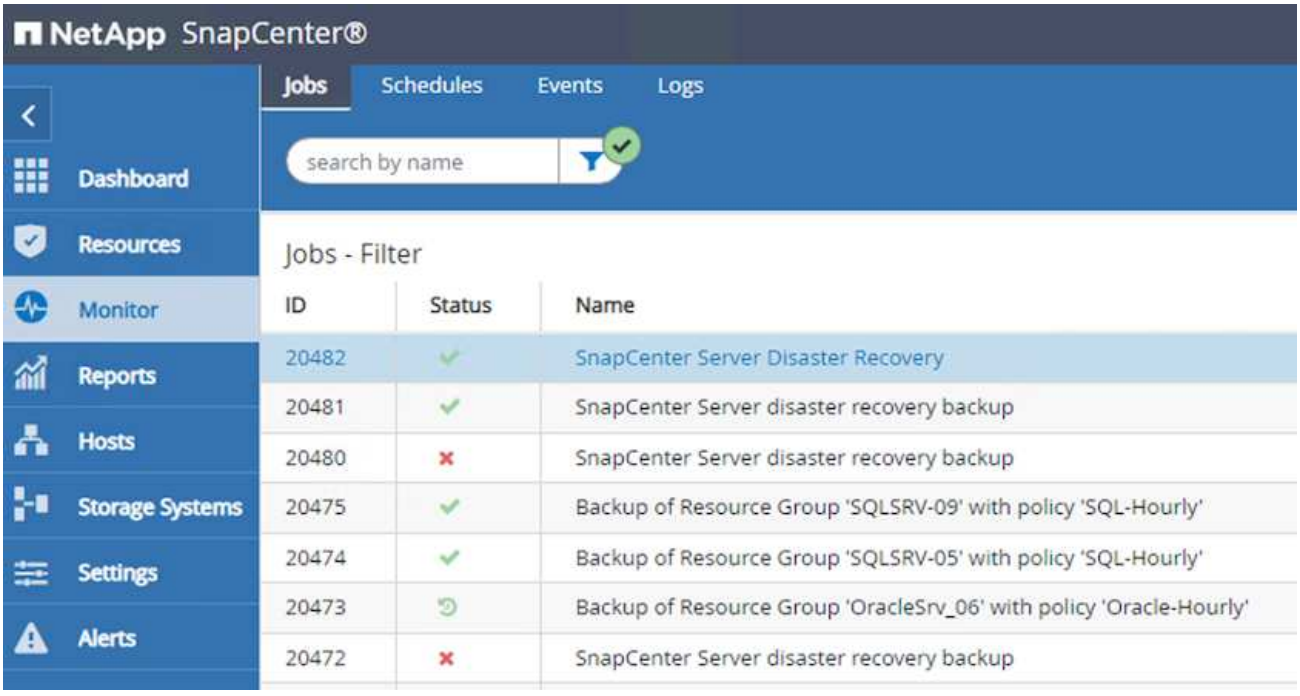
1. セカンダリSnapCenterサーバーの Swagger API Web ページに移動し、前の手順に従って認証トークンを取得します。
2. Swaggerページの災害復旧セクションに移動し、 `/4.6/disasterrecovery/server/restore`をクリックし、「試してみる」をクリックします。

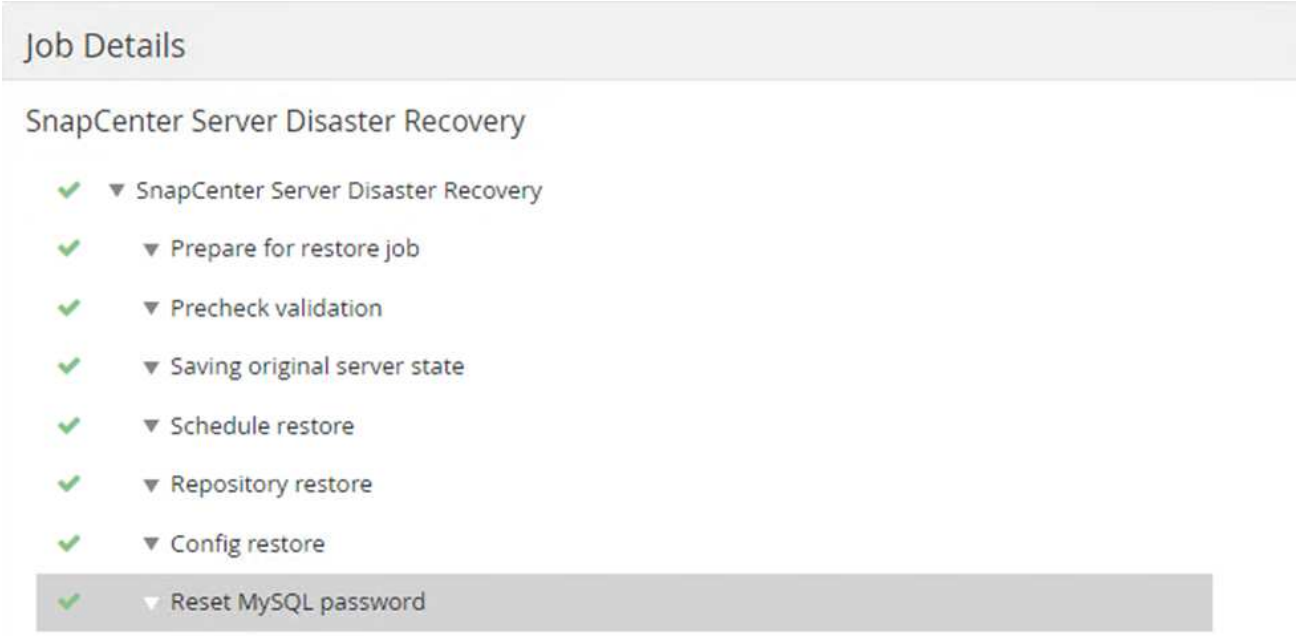


3. 認証トークンを貼り付け、SmDRResterRequest セクションにバックアップの名前とセカンダリSnapCenterサーバー上のローカル ディレクトリを貼り付けます。



4. 復元プロセスを開始するには、[実行] ボタンを選択します。
5. SnapCenterから [モニター] セクションに移動して、復元ジョブの進行状況を表示します。





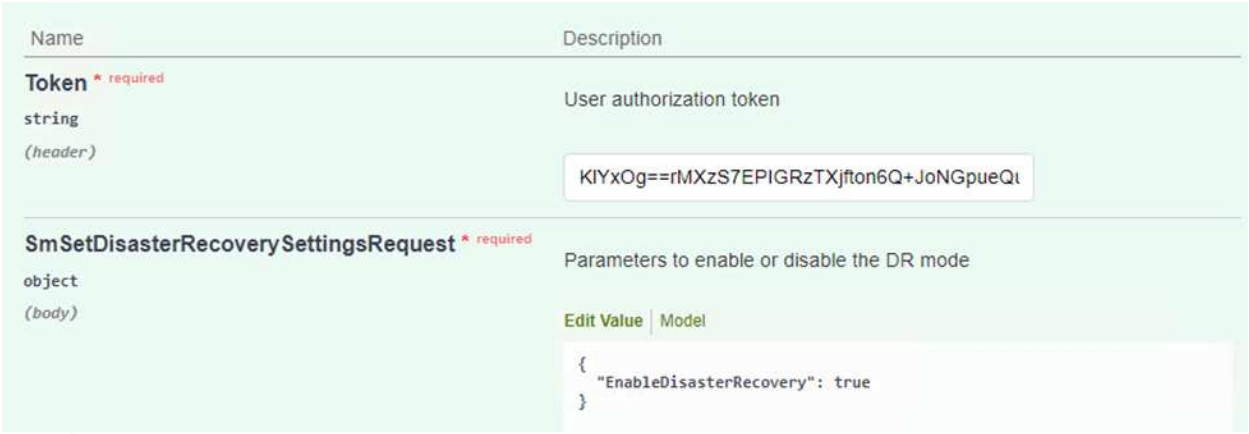
6. セカンダリ ストレージからの SQL Server の復元を有効にするには、 SnapCenterデータベースをディザスタ リカバリ モードに切り替える必要があります。これは個別の操作として実行され、Swagger API Web ページで開始されます。

   a. 災害復旧セクションに移動してクリックします `/4.6/disasterrecovery/storage`。

   b. ユーザー認証トークンを貼り付けます。

   c. SmSetDisasterRecoverySettingsRequestセクションで、変更します。 `EnableDisasterRecover`に `true`。

   d. [実行] をクリックして、SQL Server の災害復旧モードを有効にします。



追加の手順に関するコメントを参照してください。

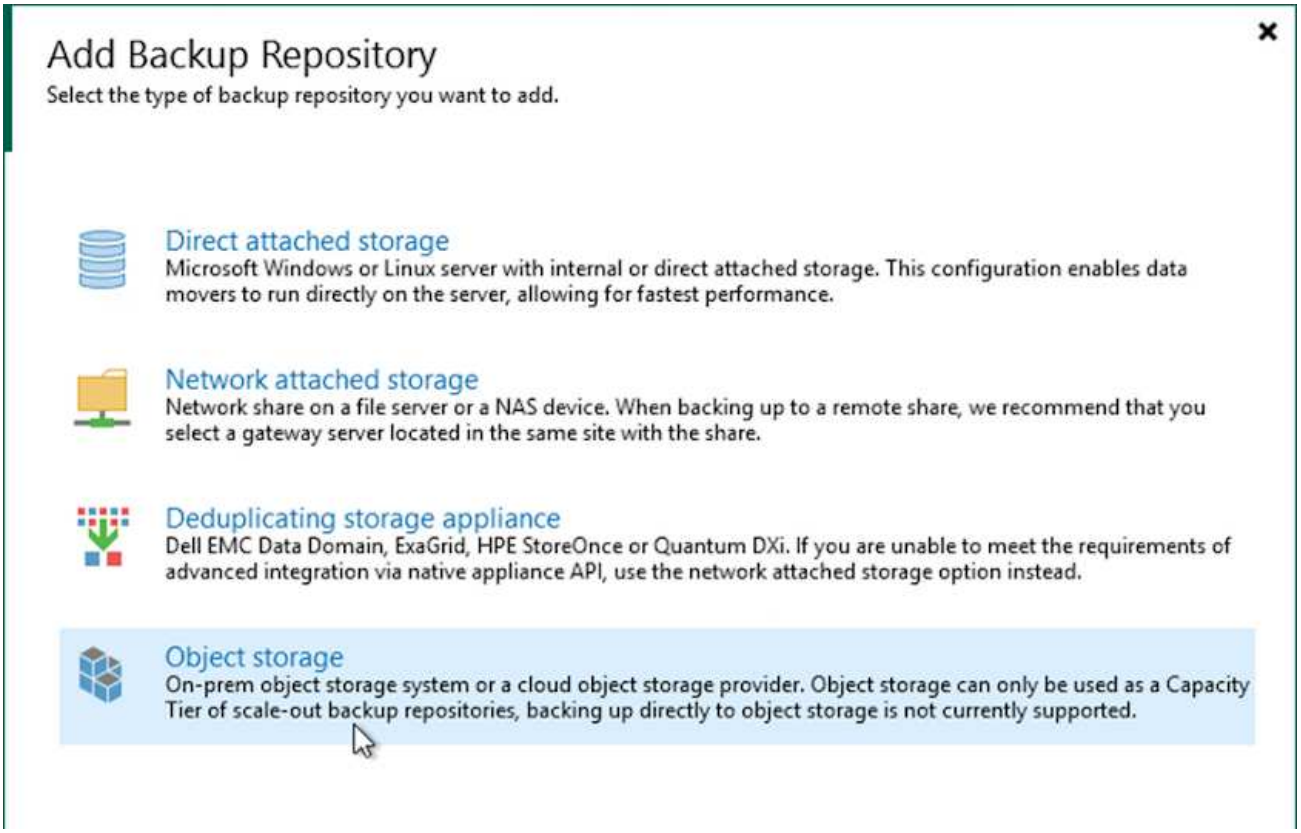
Veeam の完全復元でアプリケーション **VM** を復元する

▼ バックアップリポジトリを作成し、**S3**からバックアップをインポートする

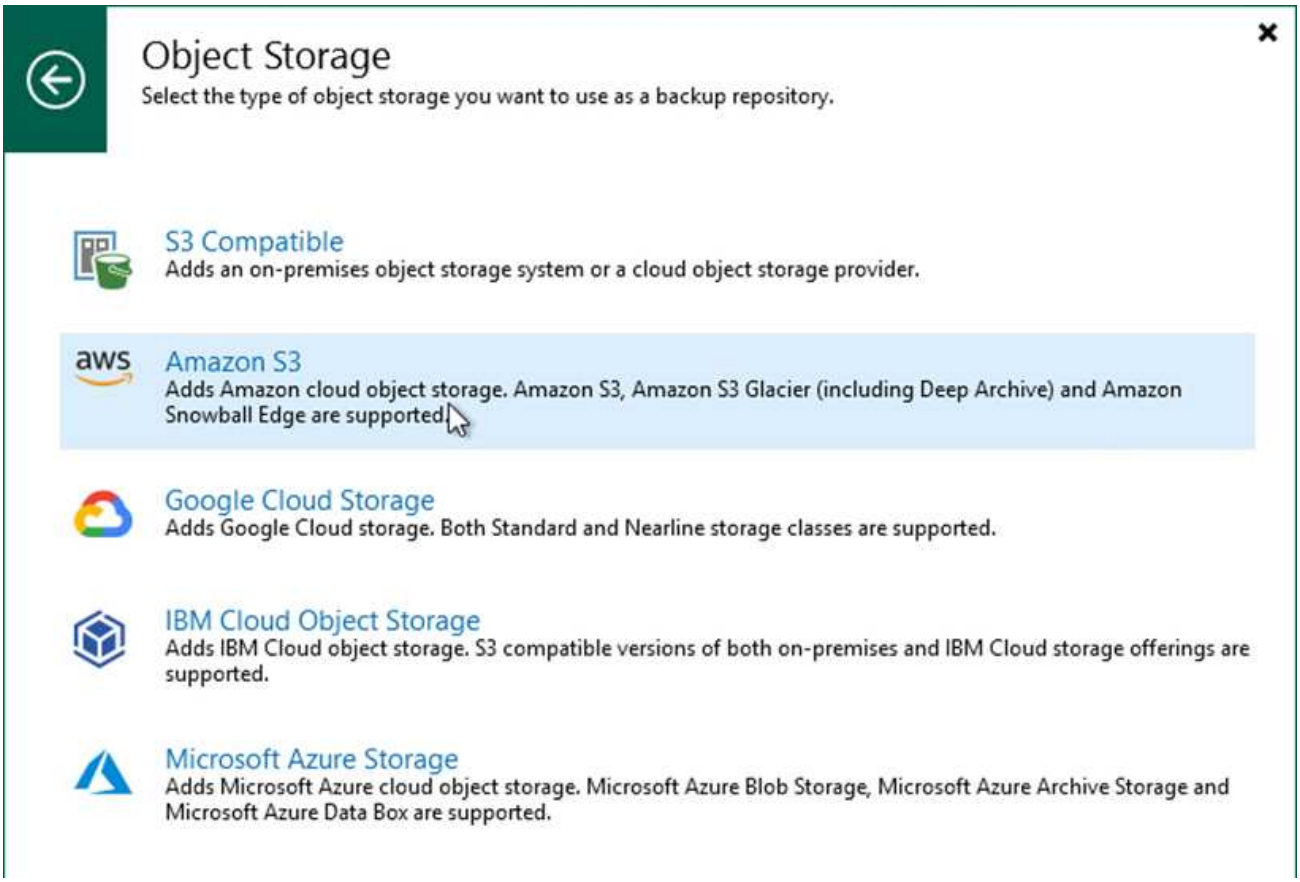
セカンダリ Veeam サーバーで、S3 ストレージからバックアップをインポートし、SQL Server および Oracle VM を VMware Cloud クラスターに復元します。

オンプレミスのスケールアウト バックアップ リポジトリの一部であった 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。

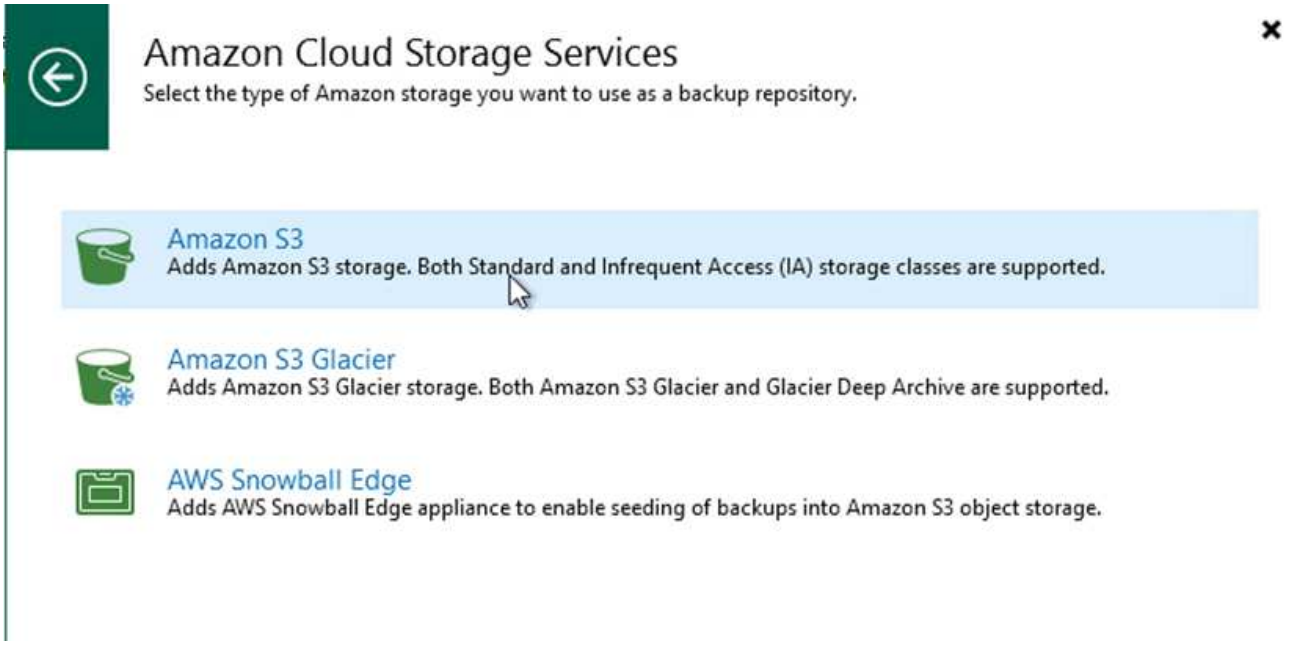
1. [バックアップ リポジトリ] に移動し、上部のメニューで [リポジトリの追加] をクリックして、[バックアップ リポジトリの追加] ウィザードを起動します。ウィザードの最初のページで、バックアップ リポジトリの種類としてオブジェクト ストレージを選択します。



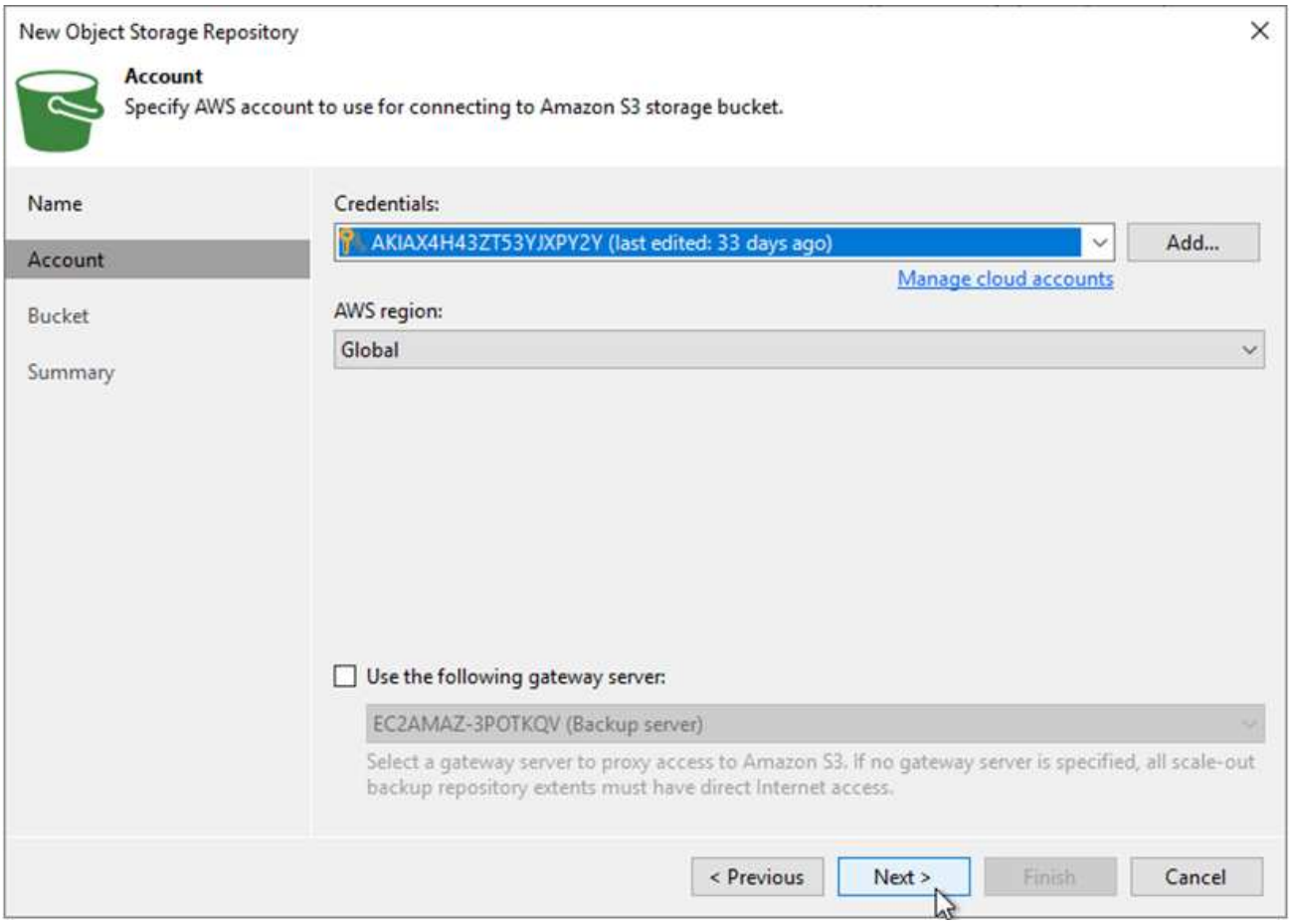
2. オブジェクトストレージタイプとして Amazon S3 を選択します。



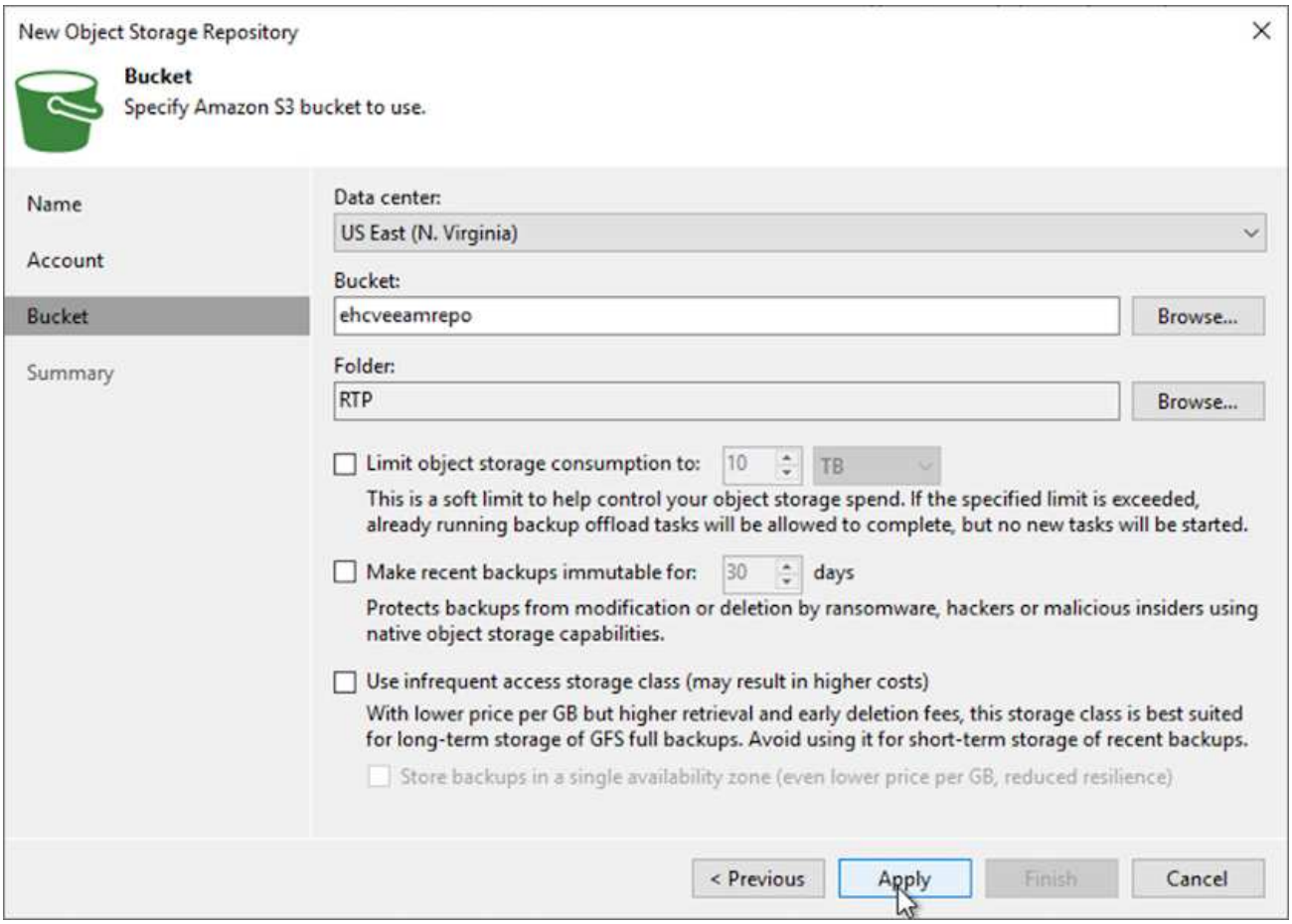
3. Amazon クラウド ストレージ サービスのリストから、Amazon S3 を選択します。



4. ドロップダウン リストから事前に入力した資格情報を選択するか、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資格情報を追加します。 「次へ」をクリックして続行します。



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

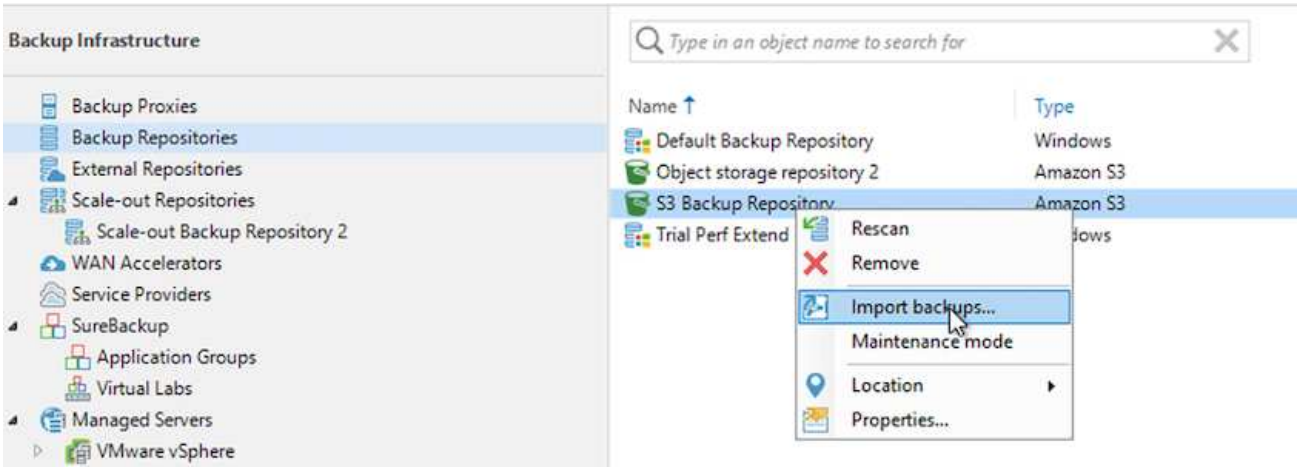


6. 最後に、「完了」を選択してプロセスを完了し、リポジトリを追加します。

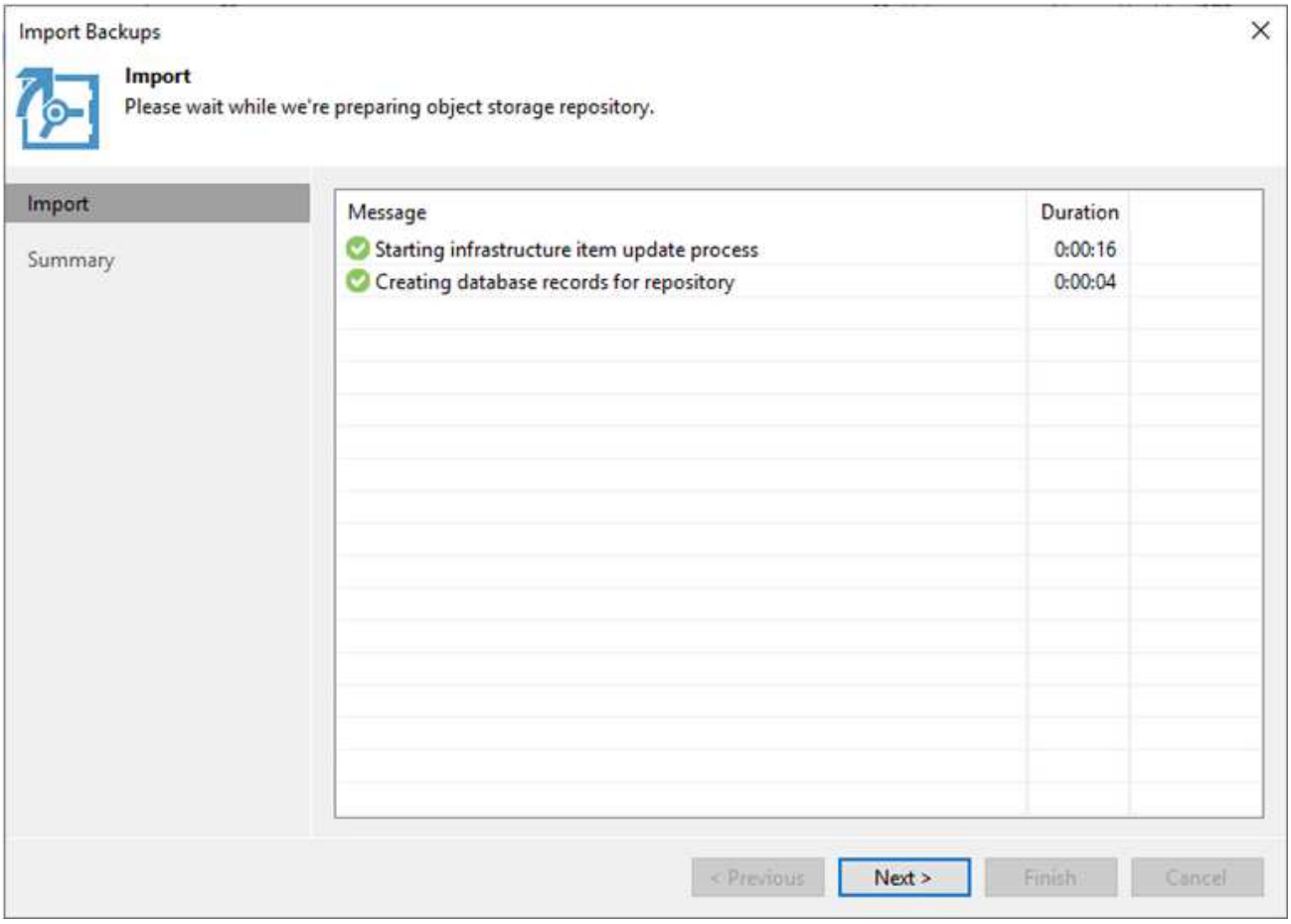
▼ **S3** オブジェクトストレージからバックアップをインポートする

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。

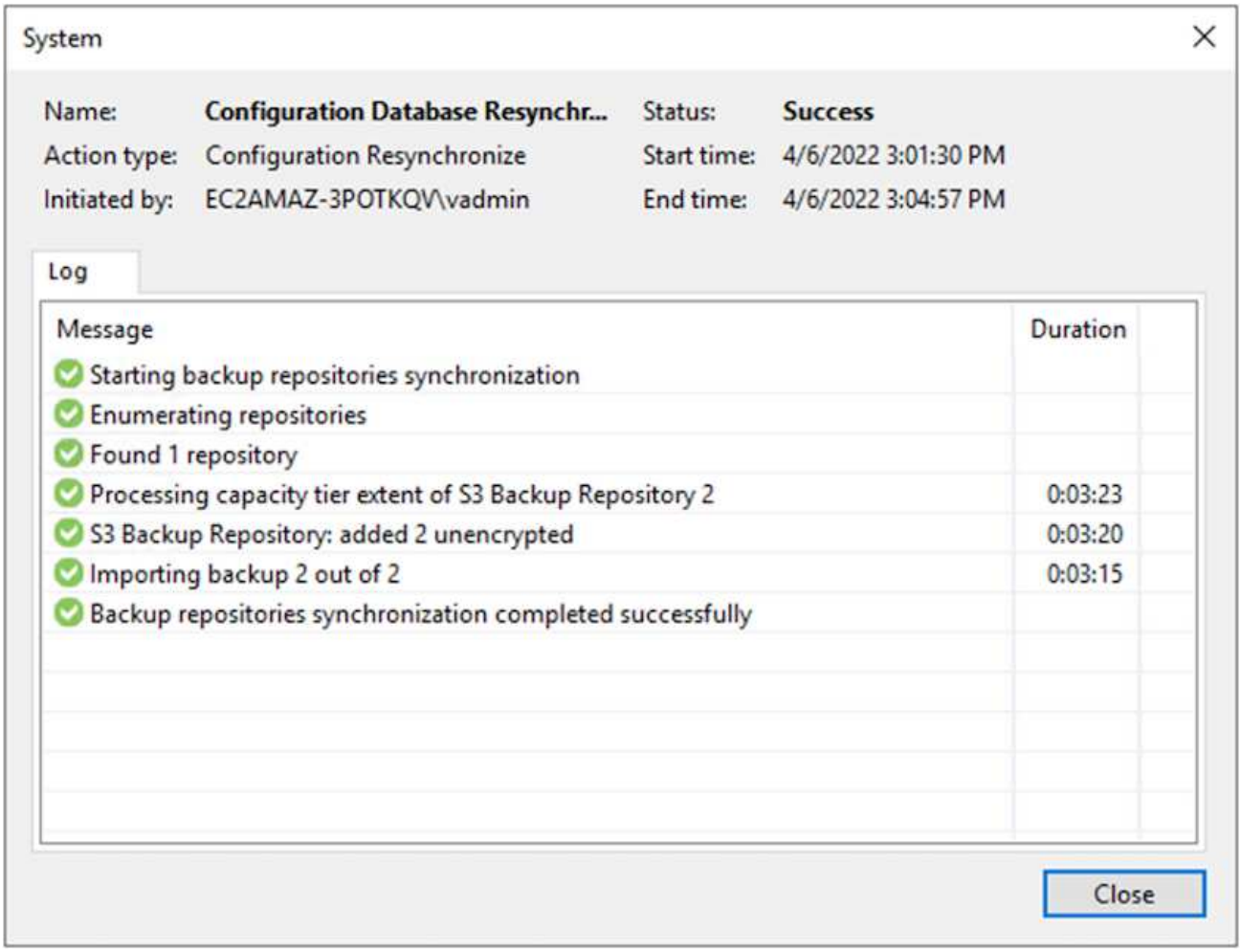
1. S3 バックアップ リポジトリから、[バックアップのインポート] を選択して、[バックアップのインポート] ウィザードを起動します。



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、概要画面で [次へ] を選択し、[完了] を選択してインポート プロセスを開始します。



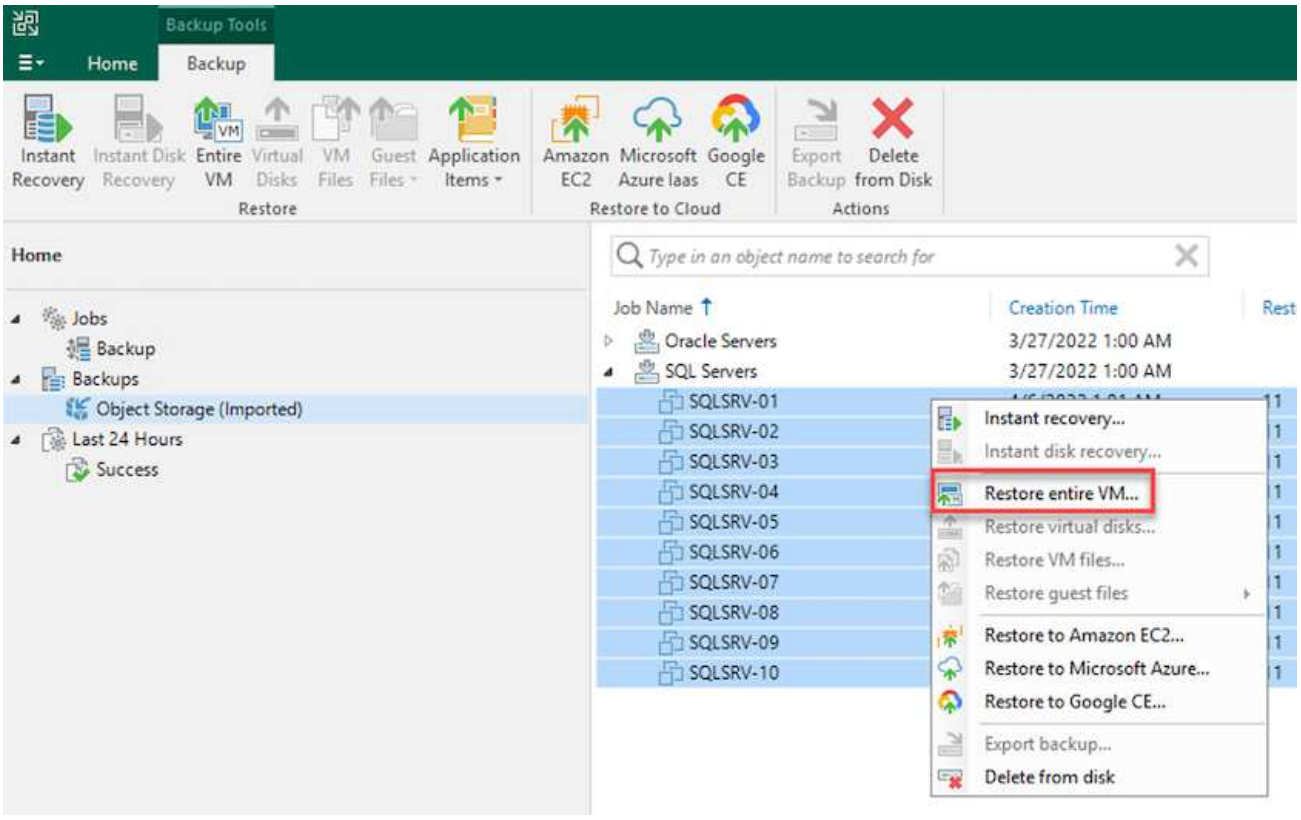
3. インポートが完了したら、VM を VMware Cloud クラスターに復元できます。



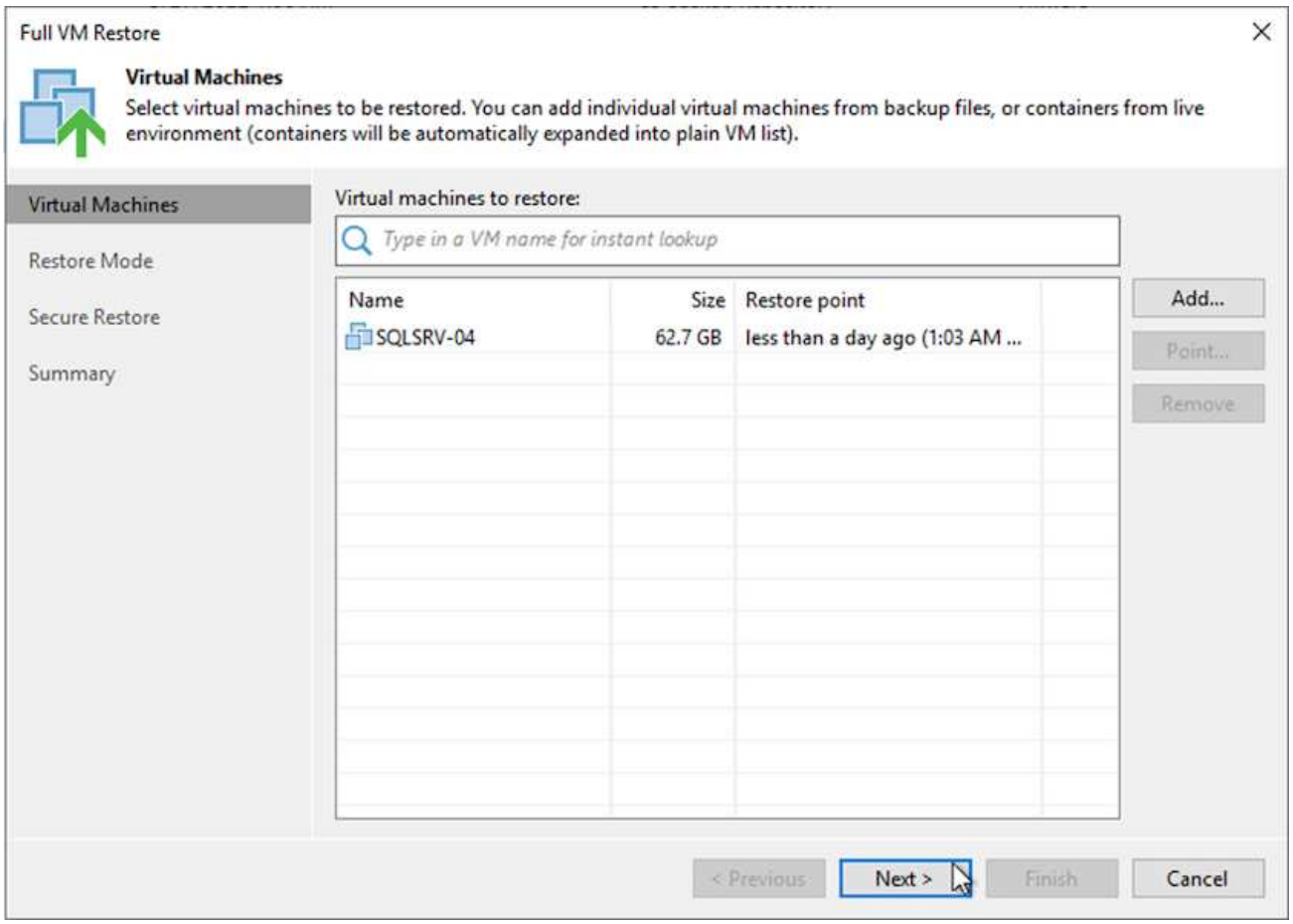
▼ **Veeam** の完全リストアを使用してアプリケーション **VM** を **VMware Cloud** にリストアする

SQL および Oracle 仮想マシンを VMware Cloud on AWS ワークロード ドメイン/クラスタに復元するには、次の手順を実行します。

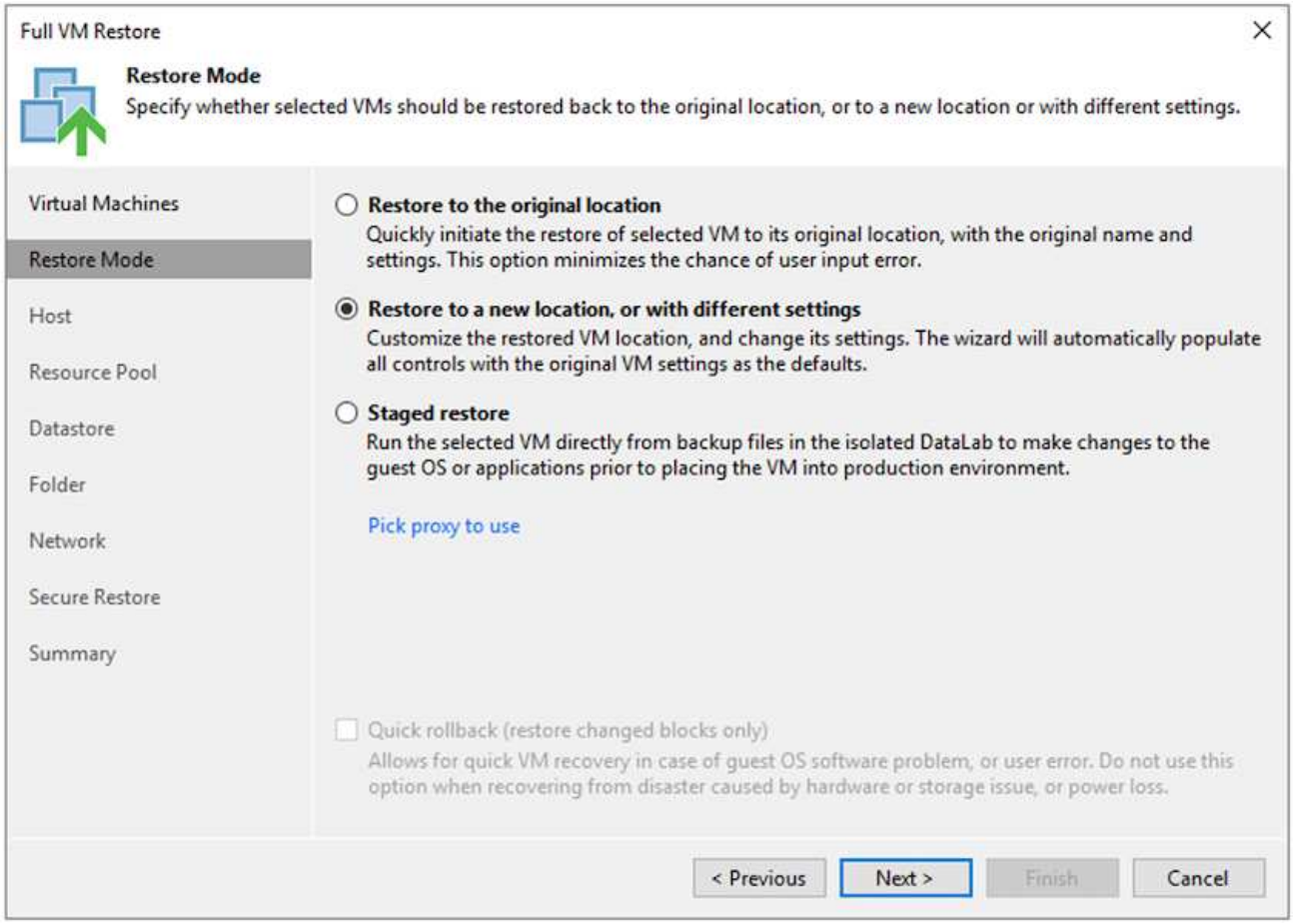
1. Veeam ホーム ページで、インポートされたバックアップを含むオブジェクト ストレージを選択し、復元する VM を選択して、右クリックし、[VM 全体の復元] を選択します。



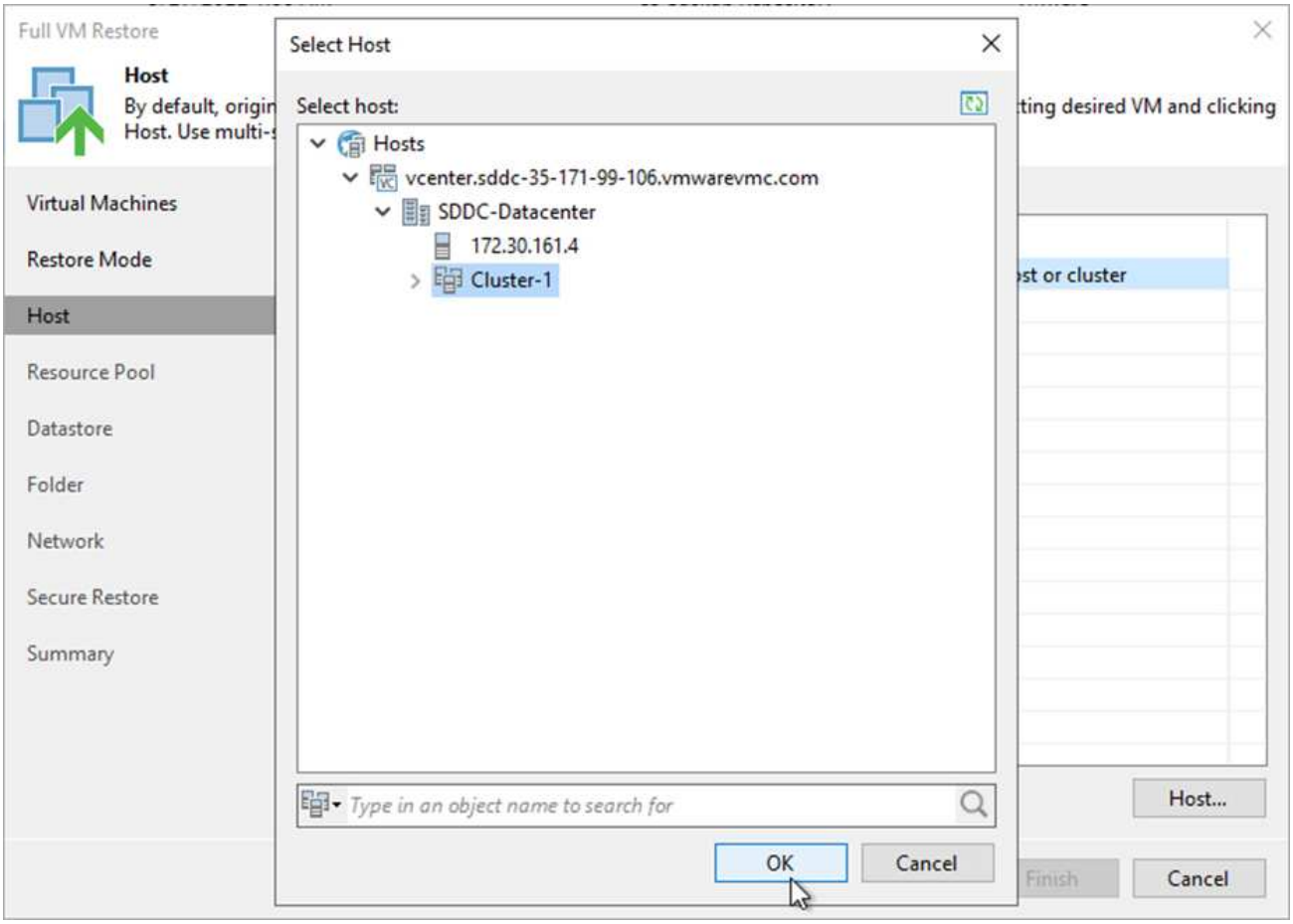
2. 完全な VM の復元ウィザードの最初のページで、必要に応じてバックアップする VM を変更し、[次へ]を選択します。



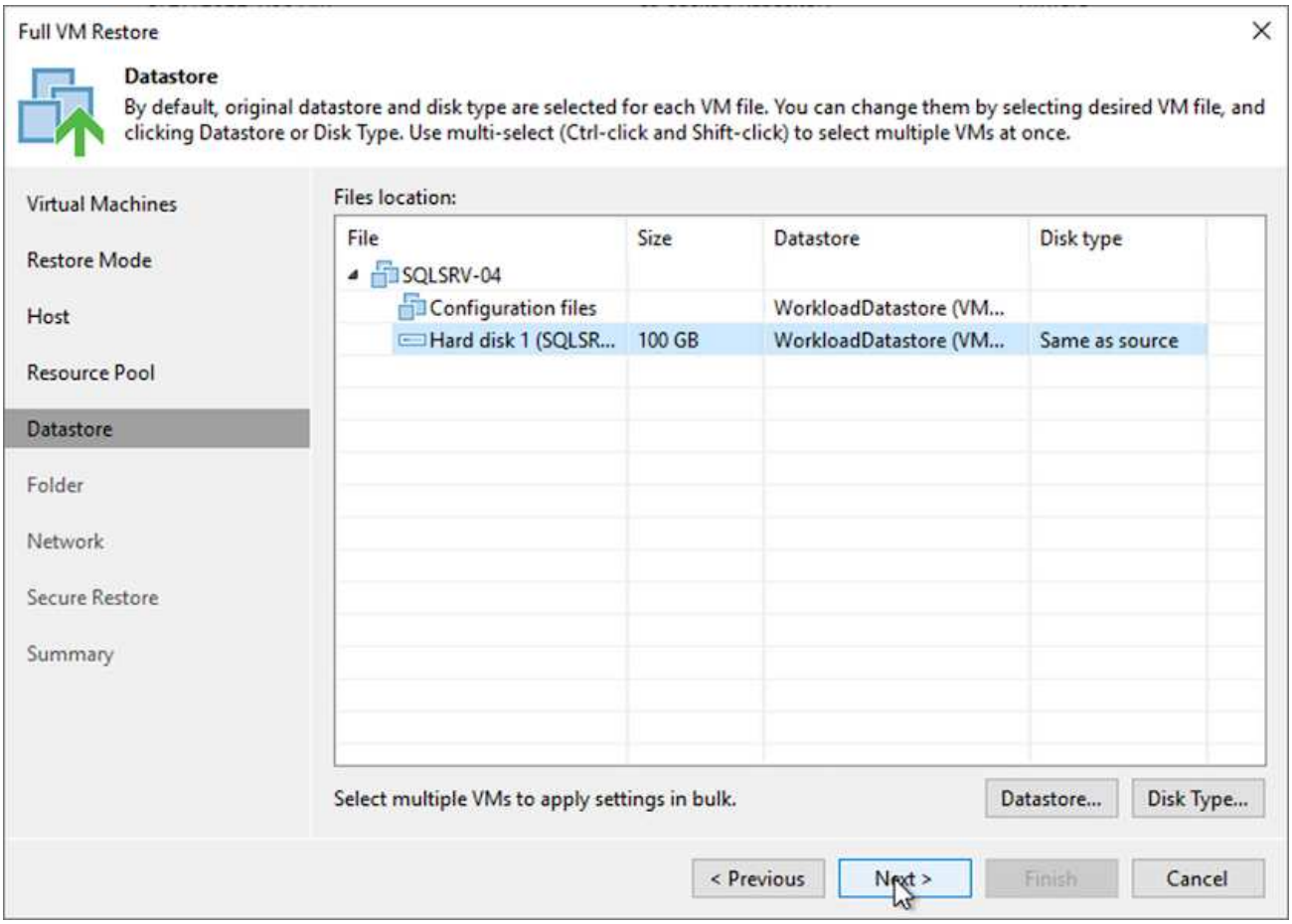
3. [復元モード] ページで、[新しい場所に復元] または [異なる設定で復元] を選択します。



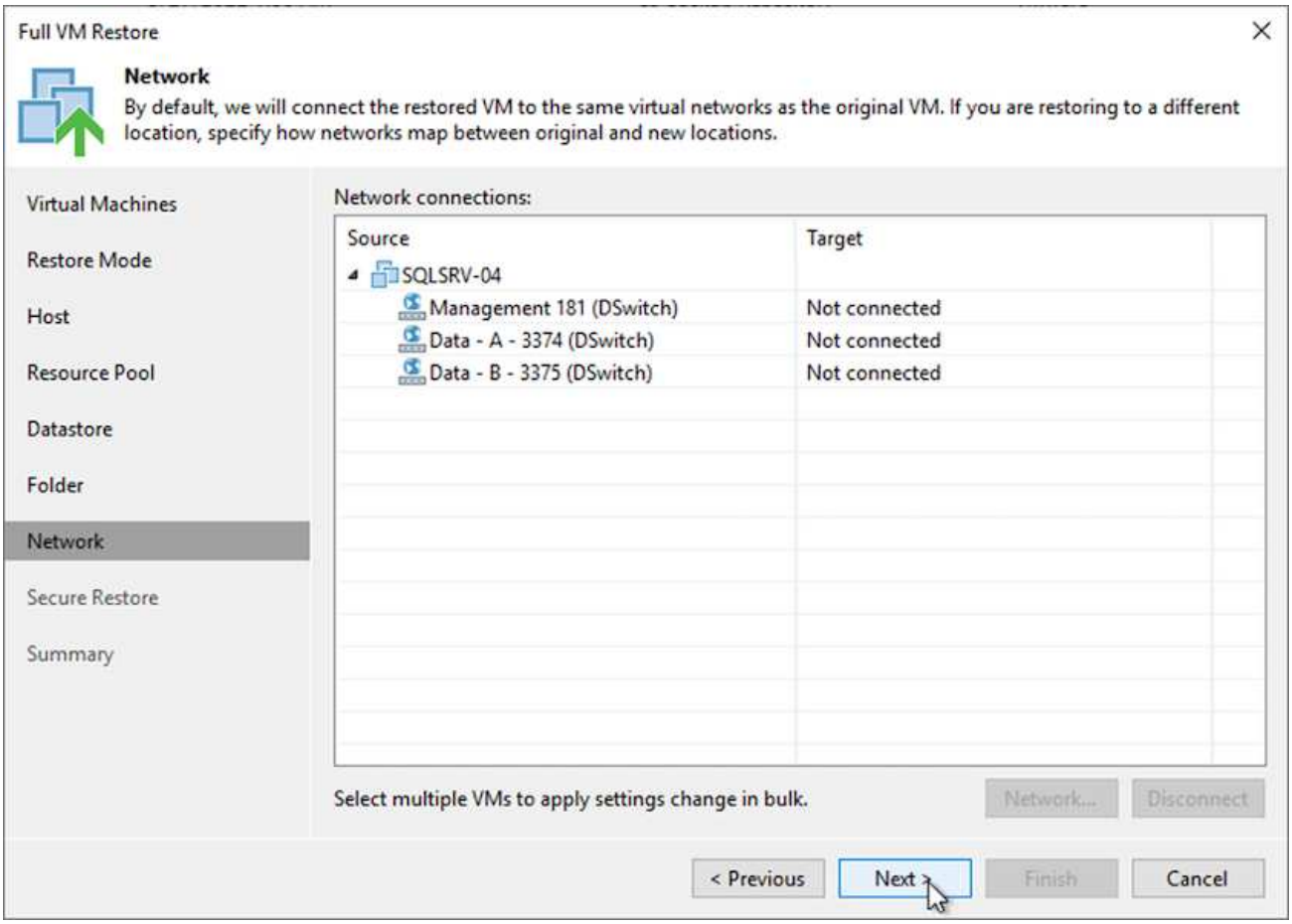
4. ホスト ページで、VM を復元するターゲット ESXi ホストまたはクラスターを選択します。

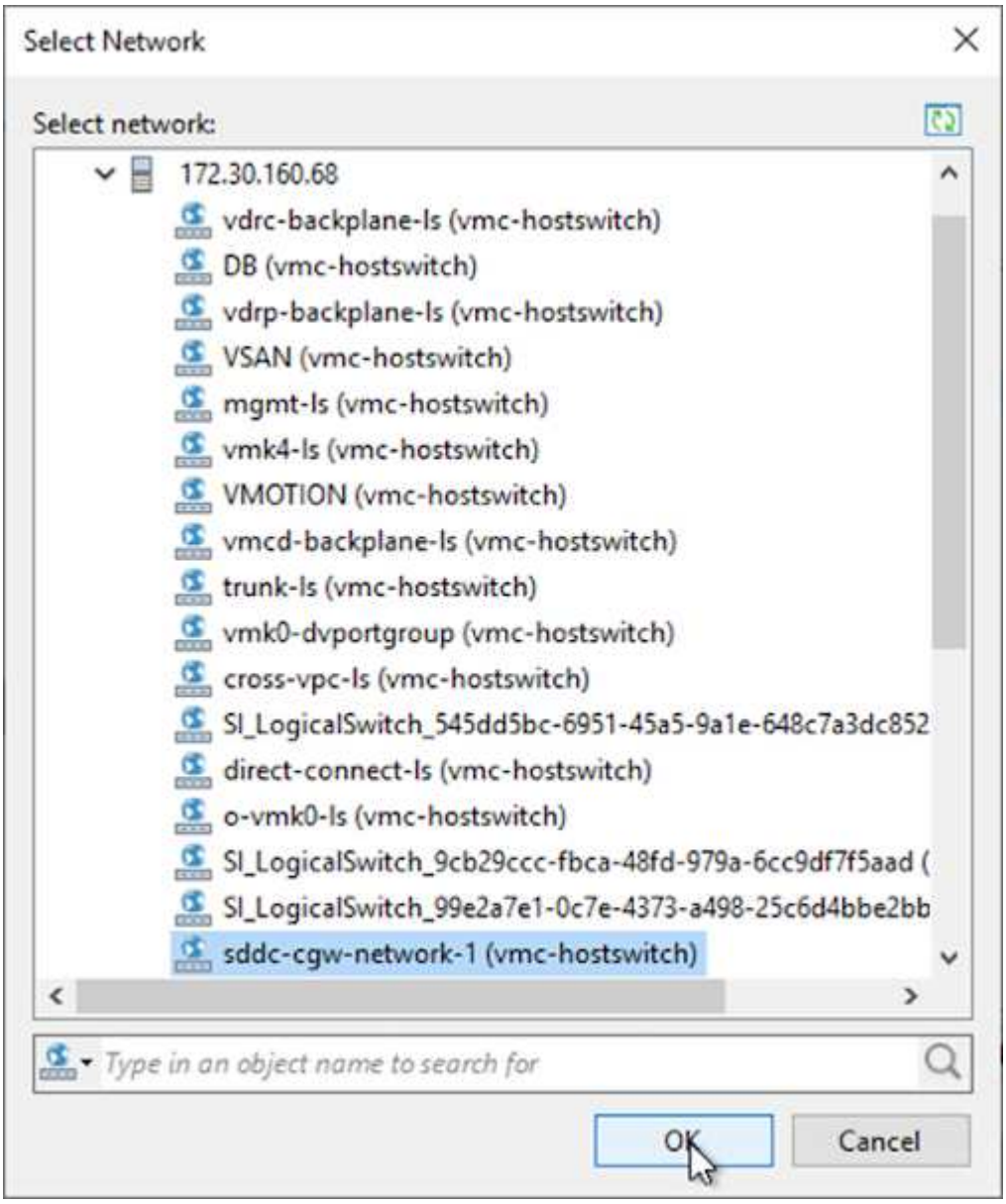


5. [データストア] ページで、構成ファイルとハード ディスクの両方のターゲット データストアの場所を選択します。



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のネットワークにマップします。


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 をマルウェアスキャンするかどうかを選択し、概要ページを確認して、[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 データを復元する

次のプロセスでは、オンプレミス サイトが動作不能になる災害が発生した場合に、AWS の VMware Cloud Services で SQL Server を復旧する方法について説明します。

回復手順を続行するには、次の前提条件が完了している必要があります。

1. Windows Server VM は、Veeam Full Restore を使用して VMware Cloud SDDC に復元されました。
2. セカンダリSnapCenterサーバーが確立され、 SnapCenterデータベースの復元と構成が、セクションに記載されている手順を使用して完了しました。"SnapCenter のバックアップおよび復元プロセスの概要。"

▼ **VM: SQL Server VM** の復元後の構成

VM の復元が完了したら、 SnapCenter内でホスト VM を再検出する準備として、ネットワークなどの項目を構成する必要があります。

1. 管理および iSCSI または NFS に新しい IP アドレスを割り当てます。
2. ホストを Windows ドメインに参加させます。
3. ホスト名を DNS またはSnapCenterサーバー上のホスト ファイルに追加します。

SnapCenterプラグインが現在のドメインとは異なるドメイン資格情報を使用して展開された場合は、SQL Server VM 上の Windows 用プラグイン 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後、 SnapCenter SMCore、Plug-in for Windows、および Plug-in for SQL Server サービスを再起動します。

SnapCenterで復元された VM を自動的に再検出するには、FQDN がオンプレミスのSnapCenterに最初に追加された VM と同一である必要があります。

▼ **SQL Server** の復元用に **FSx** ストレージを構成する

SQL Server VM の災害復旧復元プロセスを実行するには、FSx クラスターから既存のSnapMirror関係を解除し、ボリュームへのアクセスを許可する必要があります。そのためには、次の手順を実行します。

1. SQL Server データベースとログ 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ー 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
```

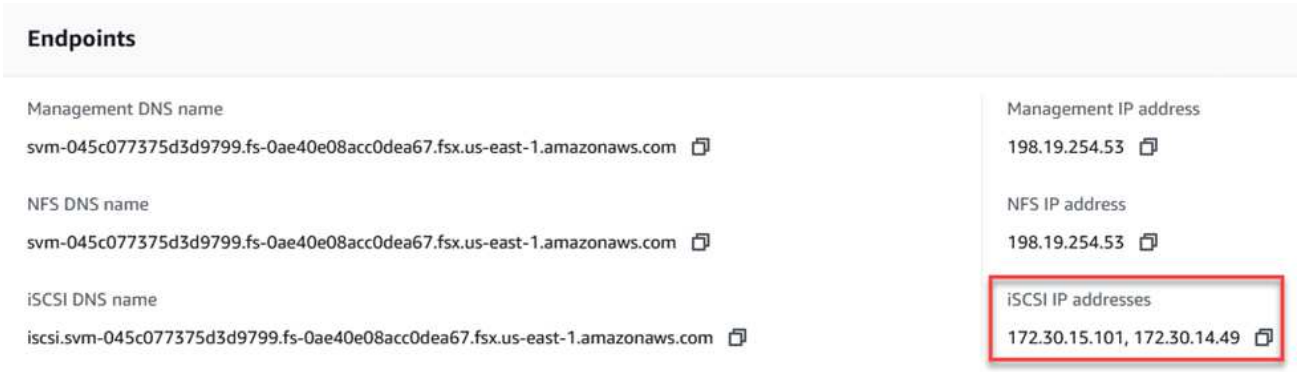
3. 最後に、作成したイニシエーター グループに LUN をマップします。

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

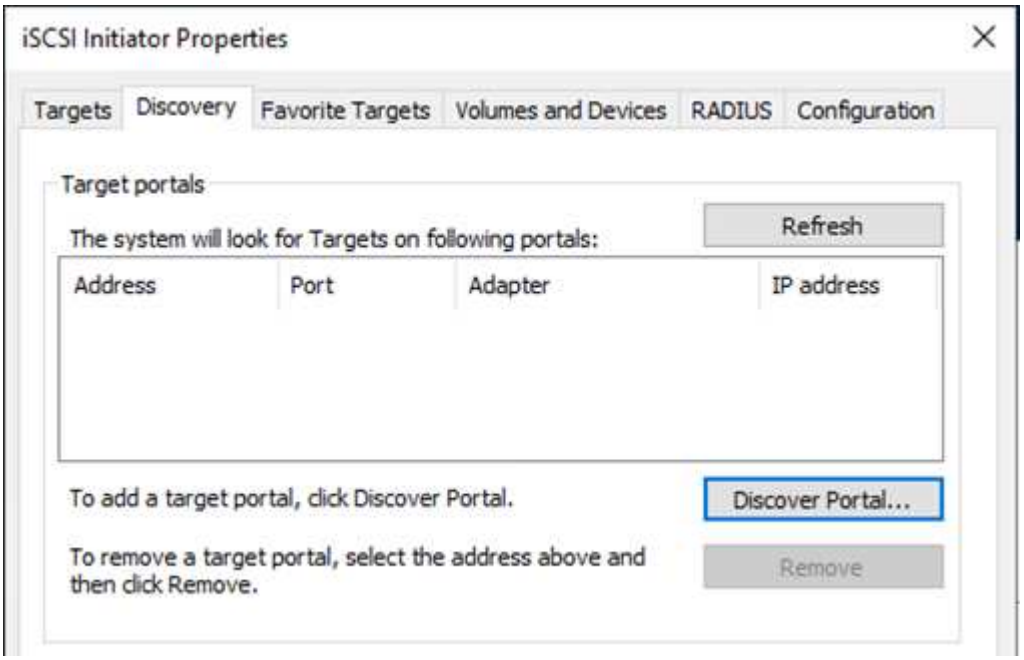
4. パス名を見つけるには、 `lun show`指示。

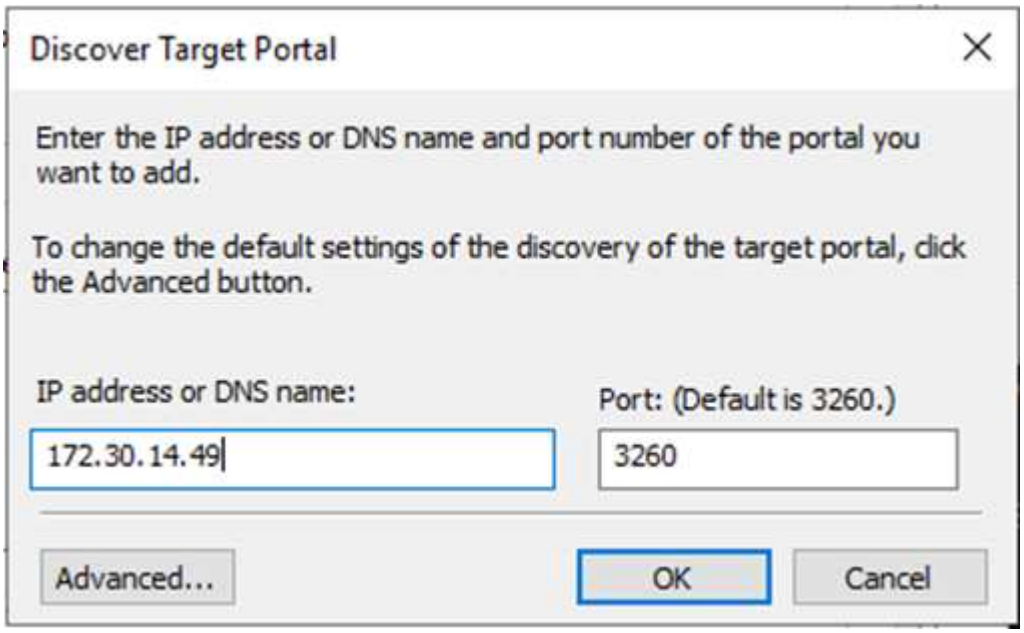
▼ **Windows VM**を**iSCSI**アクセス用にセットアップし、ファイルシステムを検出する

1. SQL Server VM から、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 グループで通信するように iSCSI ネットワーク アダプターを設定します。
2. iSCSI イニシエーターのプロパティ ユーティリティを開き、[検出]、[お気に入りのターゲット]、および [ターゲット] タブの古い接続設定をクリアします。
3. FSx インスタンス/クラスター上の iSCSI 論理インターフェイスにアクセスするための IP アドレスを見つけます。これは、AWS コンソールのAmazon FSx > ONTAP > Storage Virtual Machines にあります。



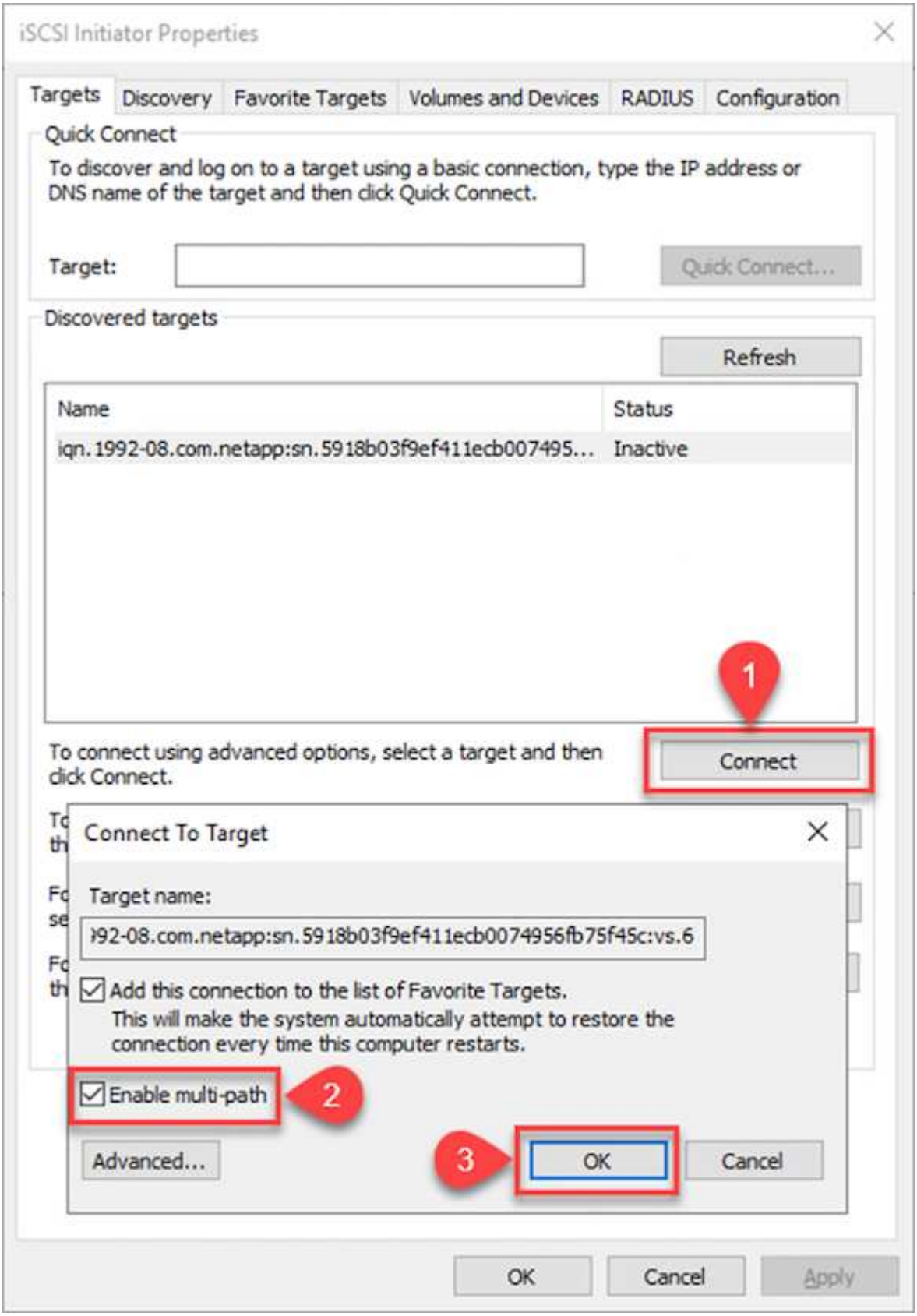
4. [検出] タブから [ポータルの検出] をクリックし、FSx iSCSI ターゲットの IP アドレスを入力します。



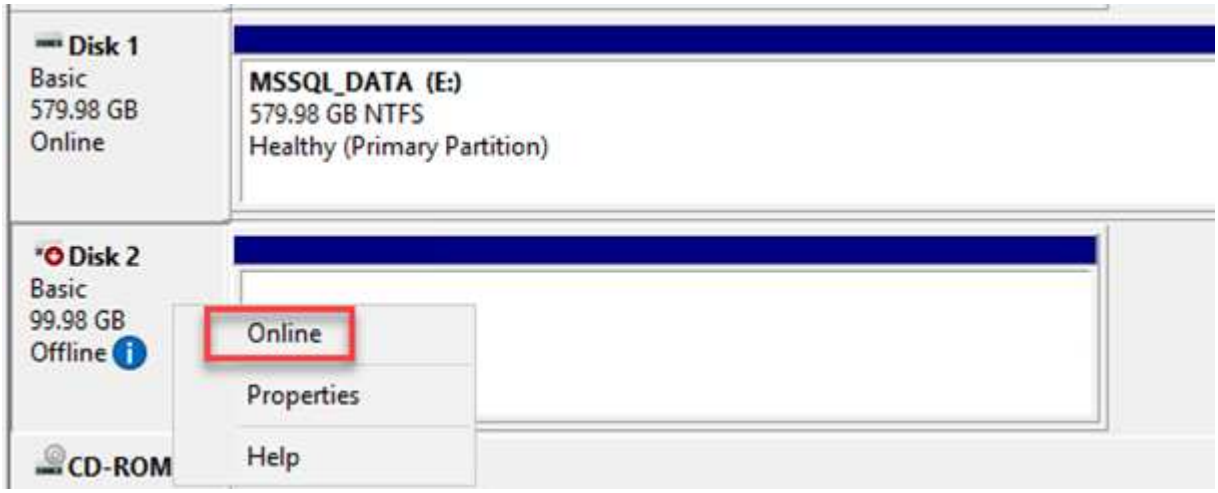


5. [ターゲット] タブで [接続] をクリックし、構成に応じて [マルチパスを有効にする] を選択してから

[OK] をクリックし、ターゲットに接続します。

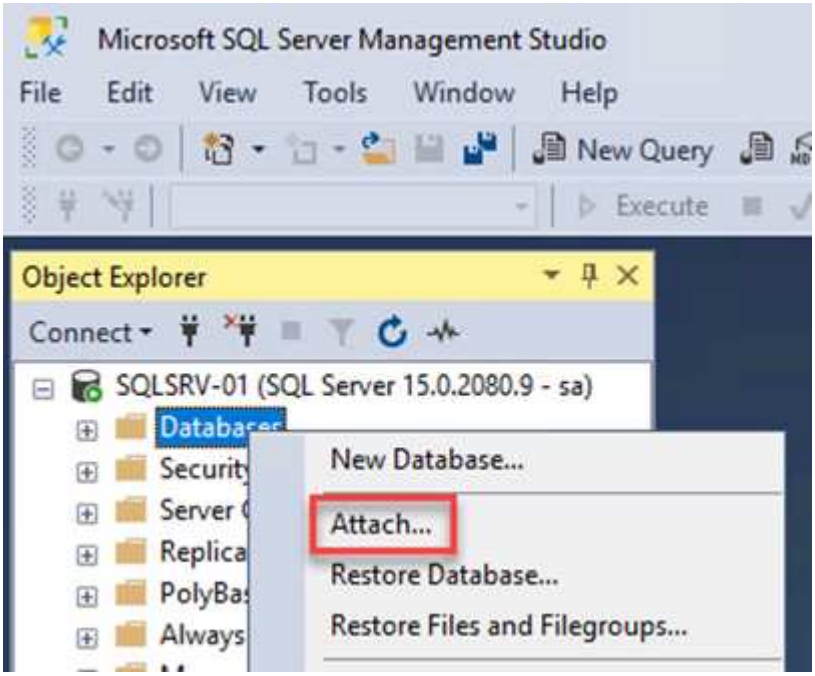


6. コンピュータの管理ユーティリティを開き、ディスクをオンラインにします。以前と同じドライブ文字が保持されていることを確認します。

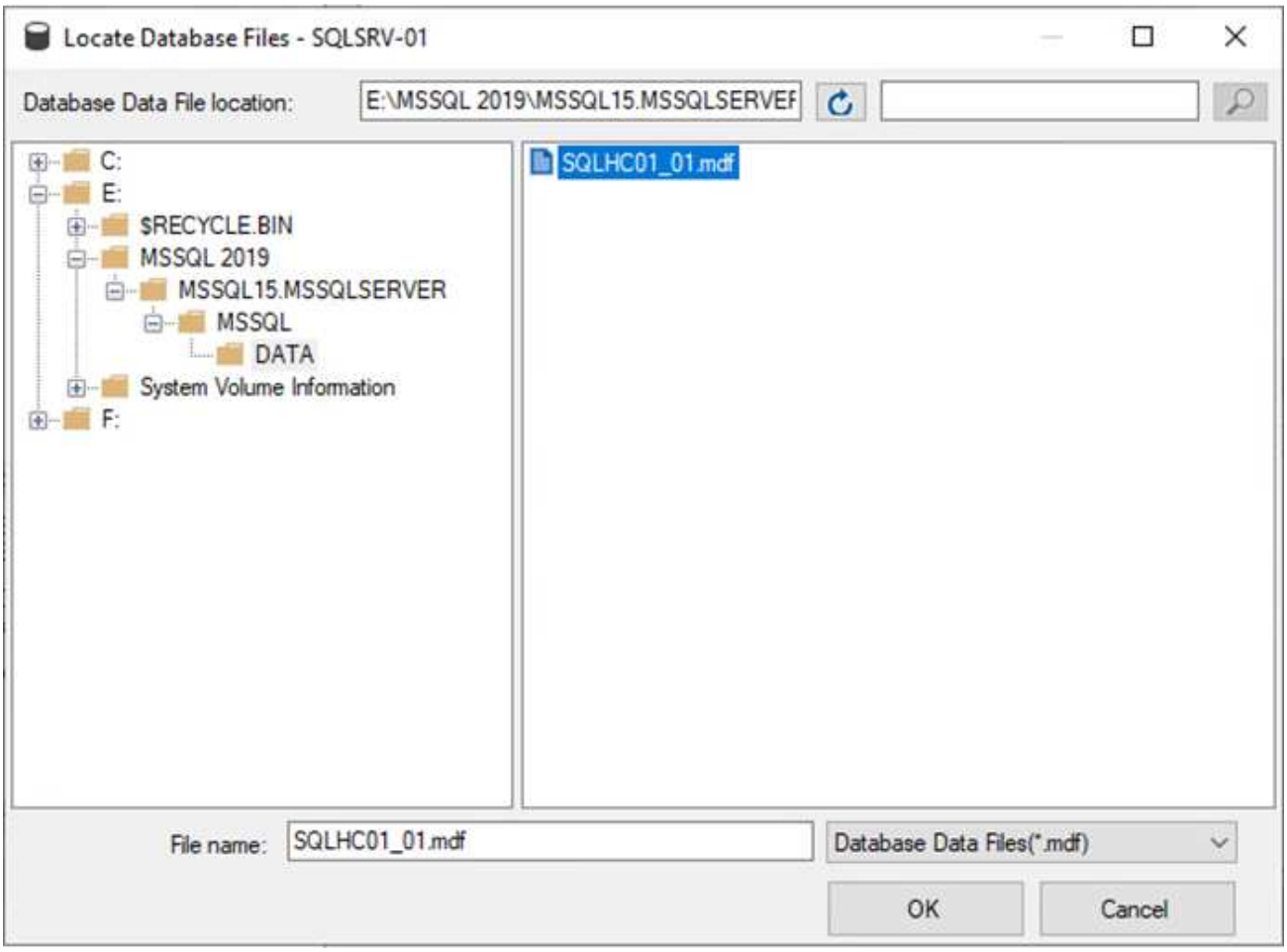


▼ **SQL Server**データベースを接続する

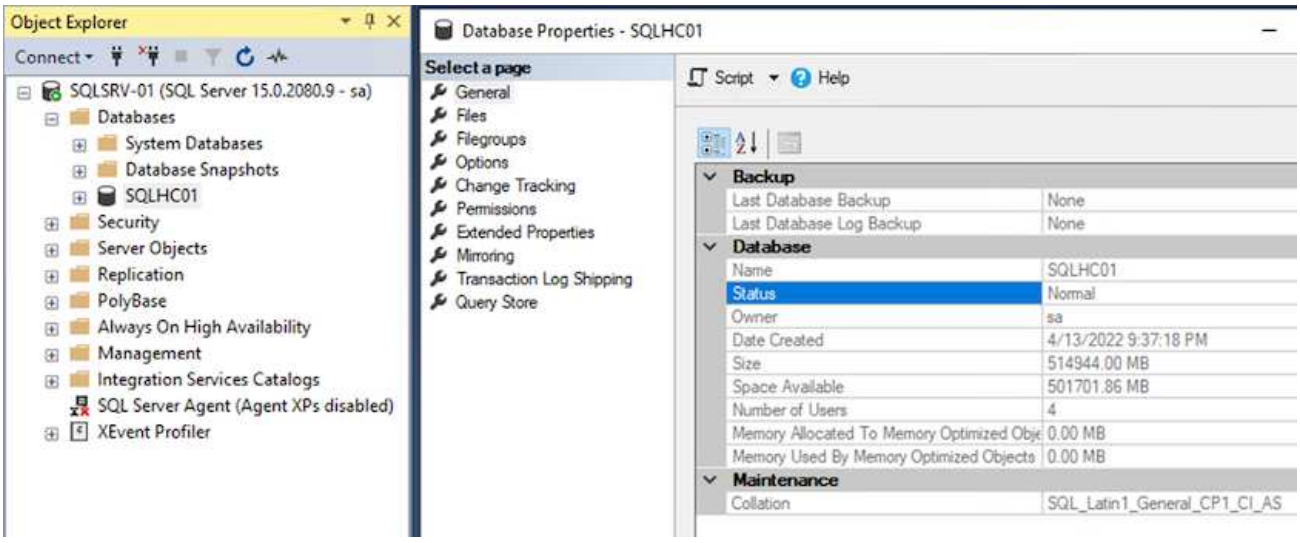
1. SQL Server VM から Microsoft SQL Server Management Studio を開き、[アタッチ] を選択してデータベースへの接続プロセスを開始します。



2. [追加] をクリックし、SQL Server プライマリ データベース ファイルが含まれているフォルダーに移動して選択し、[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 ログが含まれているフォルダーを選択します。
4. 完了したら、「OK」をクリックしてデータベースを接続します。

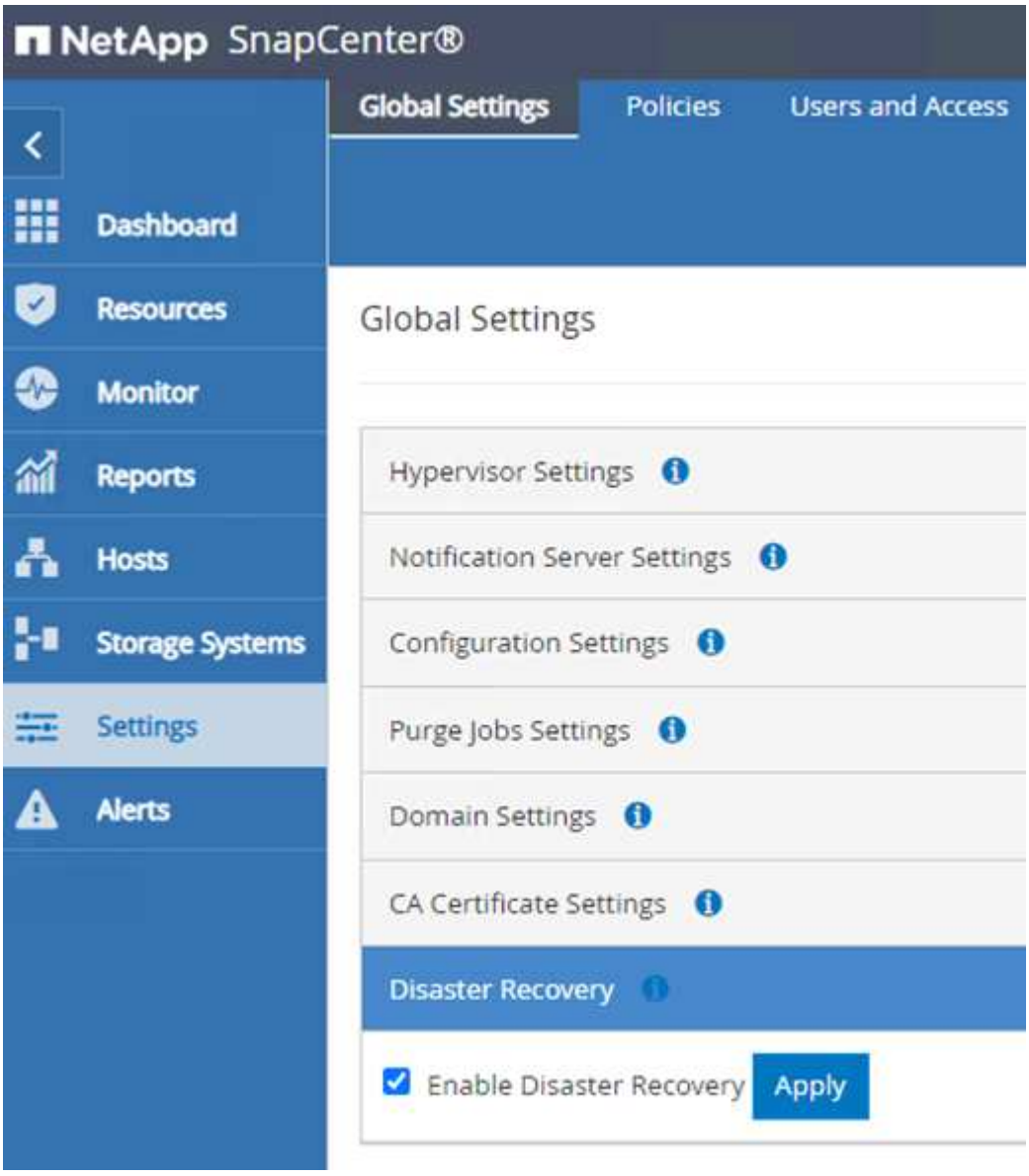


▼ **SnapCenterと SQL Server** プラグインの通信を確認する

SnapCenterデータベースが以前の状態に復元されると、SQL Server ホストが自動的に再検出されます。これが正しく機能するには、次の前提条件に留意してください。

- SnapCenter を災害復旧モードにする必要があります。これは、Swagger API または災害復旧のグローバル設定を通じて実行できます。
- 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一である必要があります。
- 元のSnapMirror関係を解除する必要があります。
- データベースを含む LUN は、SQL Server インスタンスにマウントされ、データベースが接続されている必要があります。

SnapCenterが災害復旧モードになっていることを確認するには、 SnapCenter Web クライアント内から [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。 「災害復旧を有効にする」チェックボックスが有効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の復元

次のプロセスでは、オンプレミス サイトが動作不能になる災害が発生した場合に、AWS の VMware Cloud Services で Oracle アプリケーション データを復旧する方法について説明します。

回復手順を続行するには、次の前提条件を完了してください。

1. Oracle Linux サーバー VM は、Veeam Full Restore を使用して VMware Cloud SDDC に復元されました。
2. セカンダリSnapCenterサーバーが確立され、このセクションで概説されている手順を使用してSnapCenterデータベースと構成ファイルが復元されました。"SnapCenter のバックアップおよび復元プロセスの概要。"

▼ **FSx for Oracle** の復元を構成する **– SnapMirror**関係を解除する

FSx ONTAP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 ボリュームを Oracle サーバー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::>
```

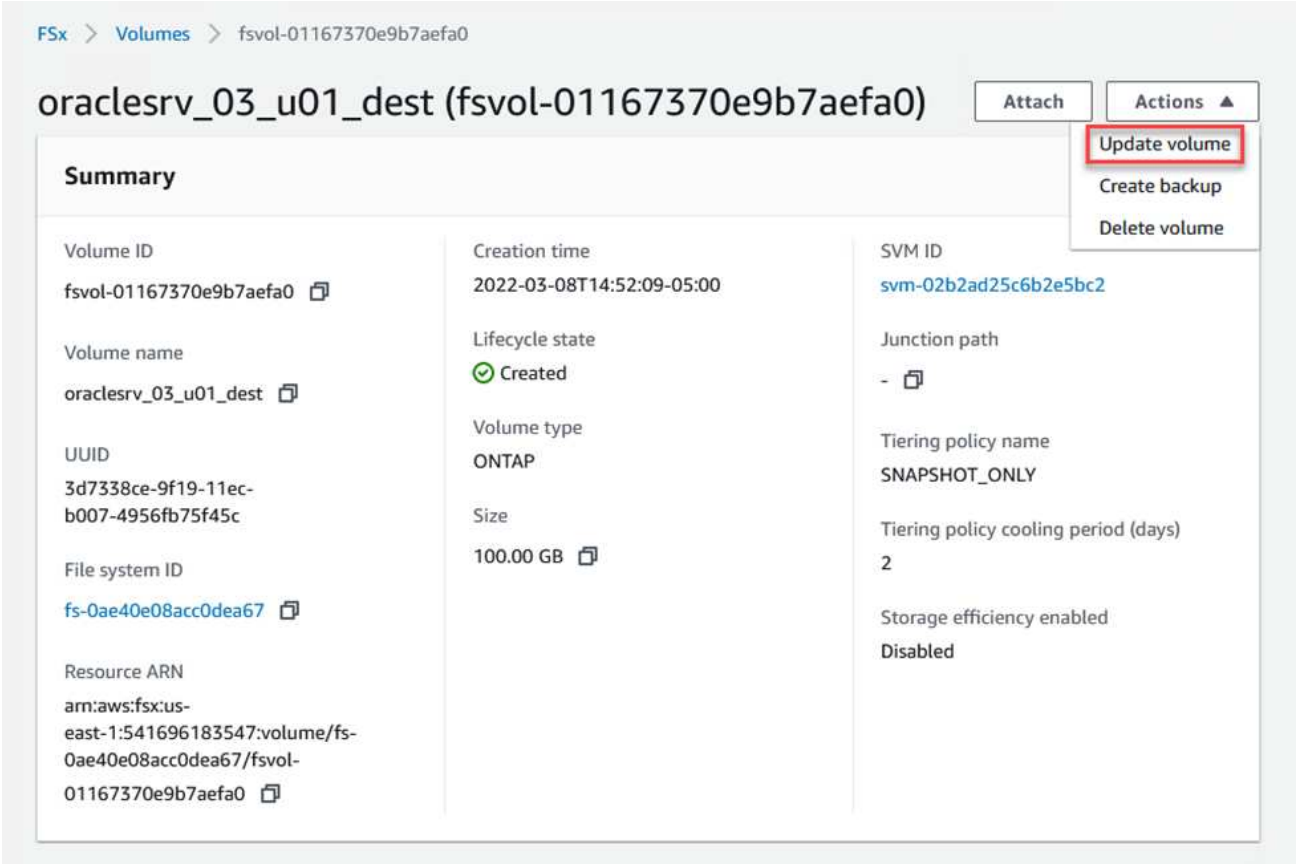
2. 既存のSnapMirror関係を解除するには、次のコマンドを実行します。

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

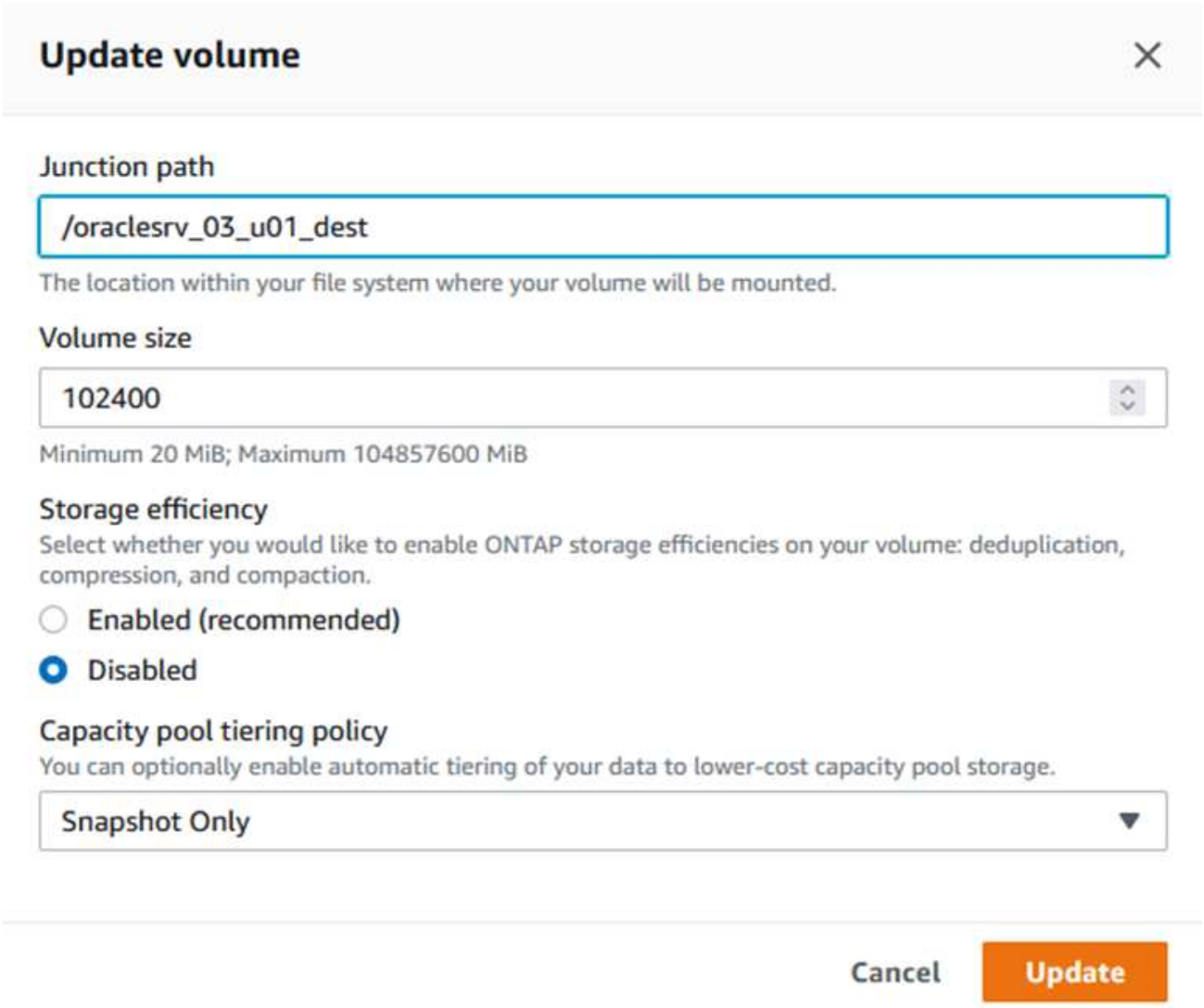
```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

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ウェブクライアントでジャンクションパスを更新します。



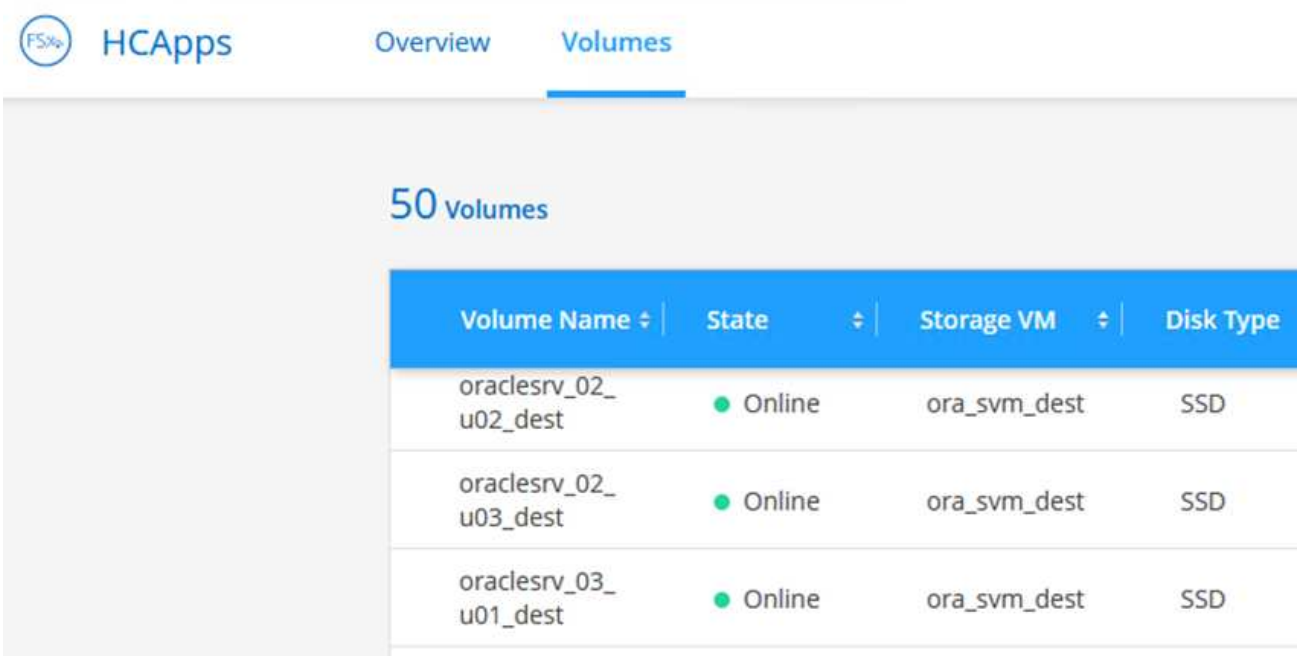
4. ジャンクション パス名を追加し、[更新] をクリックします。 Oracle サーバーから NFS ボリュームをマウントするときに、このジャンクション パスを指定します。



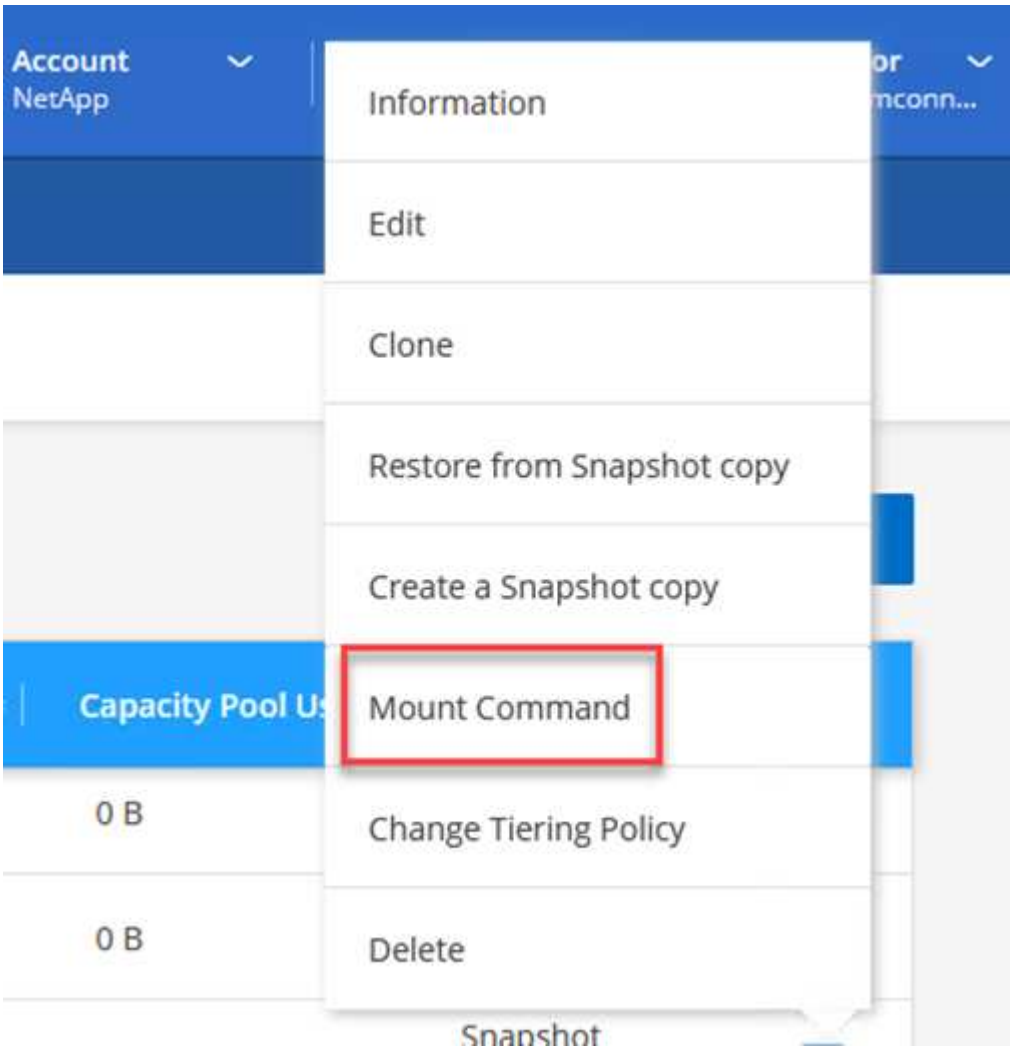
▼ **Oracle Server**に**NFS**ボリュームをマウントする

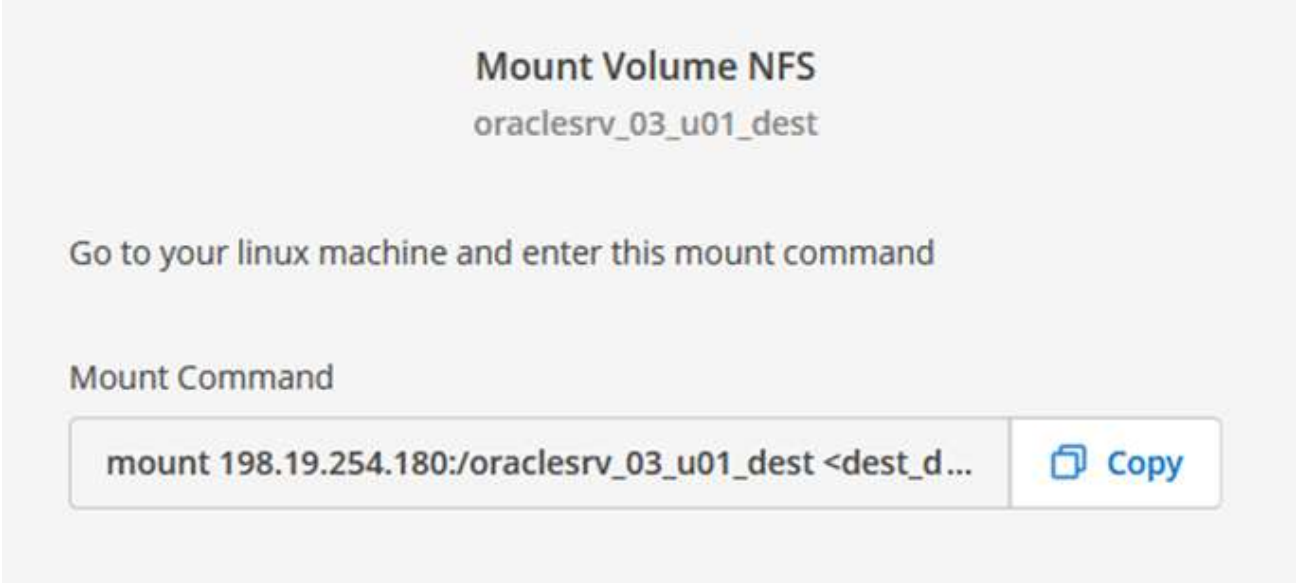
Cloud Manager では、Oracle データベース ファイルとログを含む NFS ボリュームをマウントするための正しい NFS LIF IP アドレスを指定したマウント コマンドを取得できます。

1. Cloud Manager で、FSx クラスター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 サーバーで使用するマウント コマンドを表示およびコピーします。





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は、Oracle Linux ホストにすでに存在します。
4. Oracle Linux サーバーから、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ているボリュームごとにこの手順を繰り返します。

再起動後もNFSマウントを永続化するには、 `/etc/fstab`マウント コマンドを含めるファイル。

5. Oracle サーバーを再起動します。 Oracle データベースは正常に起動し、使用可能になります。

フェイルバック

このソリューションで概説され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 は AWS で実行されているバックアップ機能を再開し、FSx ONTAPは元のオンプレミス データセンターとの既存のSnapMirror関係がないプライマリ 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、このドキュメントで説明されているプロセスと同じプロセスを使用して、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。

このドキュメントでも説明されているように、 SnapCenterを構成して、FSx ONTAPのアプリケーション データ ボリュームをオンプレミスのONTAPストレージ システムにミラーリングすることができます。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バックアップ コピーを Amazon S3 に複製するように Veeam を構成して、それらのバックアップがオンプレミス データセンターにある Veeam バックアップ サーバーにアクセスできるようにすることができます。

フェイルバックはこのドキュメントの範囲外ですが、フェイルバックはここで概説した詳細なプロセスとほとんど変わりません。

まとめ

このドキュメントで紹介するユースケースは、 NetAppと VMware の統合を強調する実証済みの災害復旧テクノロジに重点を置いています。 NetApp ONTAPストレージ システムは、実績のあるデータ ミラーリング テクノロジを提供し、組織がオンプレミスと主要なクラウド プロバイダーが提供するONTAPテクノロジにまたがる災害復旧ソリューションを設計できるようにします。

FSx ONTAP on AWS は、 SnapCenterおよびSyncMirrorとのシームレスな統合を可能にし、アプリケーションデータをクラウドに複製するソリューションの 1 つです。 Veeam Backup & Replication は、 NetApp ONTAP ストレージ システムと適切に統合され、vSphere ネイティブ ストレージへのフェイルオーバーを提供できる、もう 1 つのよく知られたテクノロジーです。

このソリューションは、SQL Server および Oracle アプリケーション データをホストするONTAPシステムのゲスト接続ストレージを使用した災害復旧ソリューションを提示しました。 SnapCenterとSnapMirrorは、ONTAPシステム上のアプリケーション ボリュームを保護し、クラウドにある FSx または CVO に複製するための、管理しやすいソリューションを提供します。 SnapCenter は、すべてのアプリケーション データを VMware Cloud on AWS にフェイルオーバーするための DR 対応ソリューションです。

VMware Cloud での **Veeam** のバックアップとリストア **(Amazon FSx ONTAP**を使用**)**

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ソリューションです。このソリューションは、Veeam Backup and Replication を使用して、VMware Cloud の FSx ONTAP NFS データストアに存在するアプリケーション VM をバックアップおよび復元するための適切なセットアップと構成を示します。

概要

VMware Cloud (AWS 内) は、補助ストレージとしての NFS データストアの使用をサポートしており、FSx 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に大量のデータを保存する必要があるお客様にとって安全なソリューションです。この統合 AWS ストレージ サービスは、従来のNetApp ONTAP機能すべてを備えた非常に効率的なストレージを提供します。

ユースケース

このソリューションは、次のユースケースに対応します。

- FSx ONTAP をバックアップ リポジトリとして使用して、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復元。
- FSx 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復元します。
- FSx ONTAP をバックアップ リポジトリとして使用して、Oracle アプリケーション データをバックアップおよび復元します。

Amazon FSx ONTAPを使用した **NFS** データストア

このソリューションのすべての仮想マシンは、FSx ONTAP補足 NFS データストアに存在します。 FSx ONTAP を補足の NFS データストアとして使用すると、いくつかの利点があります。たとえば、次のことが可能になります。

- 複雑なセットアップや管理を必要とせずに、スケーラブルで可用性の高いファイルシステムをクラウド内

に作成します。

- 既存の VMware 環境と統合することで、使い慣れたツールとプロセスを使用してクラウド リソースを管理できます。
- スナップショット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、その可用性を確保します。

▼ ソリューション展開の概要

このリストには、Veeam Backup & Replication を構成し、FSx ONTAP をバックアップ リポジトリとして使用してバックアップおよび復元ジョブを実行し、SQL Server および Oracle VM とデータベースの復元を実行するために必要な高レベルの手順が示されています。

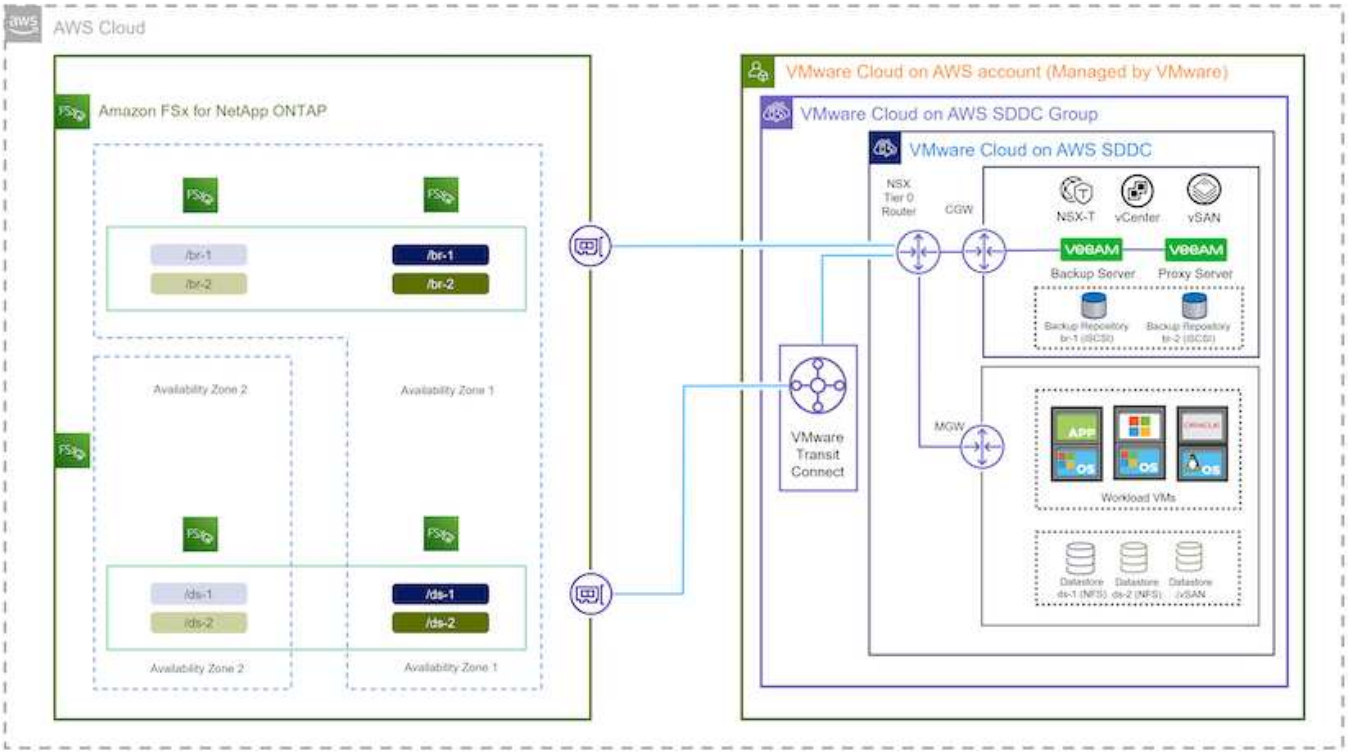
1. Veeam Backup & Replication の iSCSI バックアップ リポジトリとして使用する FSx ONTAPファイル システムを作成します。
2. Veeam Proxy を導入してバックアップ ワークロードを分散し、FSx ONTAPでホストされている iSCSI バックアップ リポジトリをマウントします。
3. Veeam バックアップ ジョブを構成して、SQL Server、Oracle、Linux、および Windows 仮想マシンをバックアップします。
4. SQL Server 仮想マシンと個々のデータベースを復元します。
5. Oracle 仮想マシンと個々のデータベースを復元します。

▼ 前提条件

このソリューションの目的は、VMware Cloud で実行され、FSx ONTAPによってホストされる NFS データストアに配置されている仮想マシンのデータ保護を実証することです。このソリューションでは、次のコンポーネントが構成され、使用できる状態になっていることを前提としています。

1. VMware Cloud に接続された 1 つ以上の NFS データストアを持つ FSx ONTAPファイルシステム。
2. Veeam Backup & Replication ソフトウェアがインストールされた Microsoft Windows Server VM。
    - vCenter サーバーは、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 サーバーによって検出されました。
3. ソリューションの展開中に Veeam Backup Proxy コンポーネントとともにインストールされる Microsoft Windows Server VM。
4. VMDK とアプリケーション データを備えた Microsoft SQL Server VM は FSx ONTAP NFS データストア上にあります。このソリューションでは、2 つの別々の VMDK に 2 つの SQL データベースがありました。
    - 注: ベスト プラクティスとして、データベース ファイルとトランザクション ログ ファイルを別々のドライブに配置すると、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 ログは順番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という事実に一部起因します。
5. VMDK とアプリケーション データを備えた Oracle Database VM は FSx ONTAP NFS データストア上にあります。
6. FSx ONTAP NFS データストアに VMDK が存在する Linux および Windows ファイル サーバー VM。
7. Veeam では、バックアップ環境内のサーバー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 インフラストラクチャ 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の要件の完全なリストについては、 "Veeam バックアップおよびレプリケーション VMware vSphere 向けユーザー ガイド" 。

このソリューションのテスト/検証は、最終的な展開環境と一致する場合も一致しない場合もあるラボで実行されました。詳細については、以下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

このソリューションの目的は、VMware Cloud で実行され、FSx ONTAPによってホストされる NFS データストアに配置されている仮想マシンのデータ保護を実証することです。このソリューションでは、次のコンポーネントがすでに構成され、使用できる状態になっていることを前提としています。

- FSx ONTAP NFS データストアに配置されている Microsoft Windows VM
- FSx ONTAP NFS データストアに配置されている Linux (CentOS) VM
- FSx ONTAP NFS データストアに配置されている Microsoft SQL Server VM
  - 別々の VMDK でホストされる 2 つのデータベース
- Oracle VMはFSx ONTAP NFSデータストア上に配置されています

ソリューションの展開

このソリューションでは、AWS 上の VMware Cloud SDDC で SQL Server、Oracle、Windows および Linux ファイル サーバー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、Veeam Backup and Replication ソフトウェアを利用したソリューションを展開および検証するための詳細な手順を説明します。このソリューションの仮想マシンは、FSx ONTAPによってホストされる補足 NFS データストア上に存在します。さらに、Veeam バックアップ リポジトリに使用される iSCSI ボリュームをホストするために、別の FSx ONTAP ファイル システムが使用されます。

FSx 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 およびデータベースの復元の実行について説明します。

FSx ONTAPの詳細については、 "FSx ONTAPユーザーガイド" 。

Veeam Backup and Replicationの詳細については、 "Veeamヘルプセンター技術ドキュメント"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については、以下を参照してください。 "VMware Cloud on AWS および VMware Cloud on Dell EMC のサポート。考慮事項と制限事項" 。

Veeam Proxyサーバーの導入

Veeam プロキシ サーバーは、Veeam Backup & Replication ソフトウェアのコンポーネントであり、ソースとバックアップまたはレプリケーション ターゲット間の仲介役として機能します。プロキシ サーバーは、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を最適化および高速化するのに役立ち、VMware vStorage API for Data Protection または直接ストレージ アクセスを通じて、さまざまなトランスポート モードを使用してデータにアクセスできます。

Veeam プロキシ サーバーの設計を選択するときは、同時タスクの数と、必要な転送モードまたはストレージ アクセスの種類を考慮することが重要です。

プロキシサーバーの台数とシステム要件については、 "Veeam VMware vSphere ベストプラクティスガイド" 。

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 モードを利用します。トランスポート モードは、バックアップ ジョブの構成時に指定されます。直接ストレージ 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の効率を高めることができます。

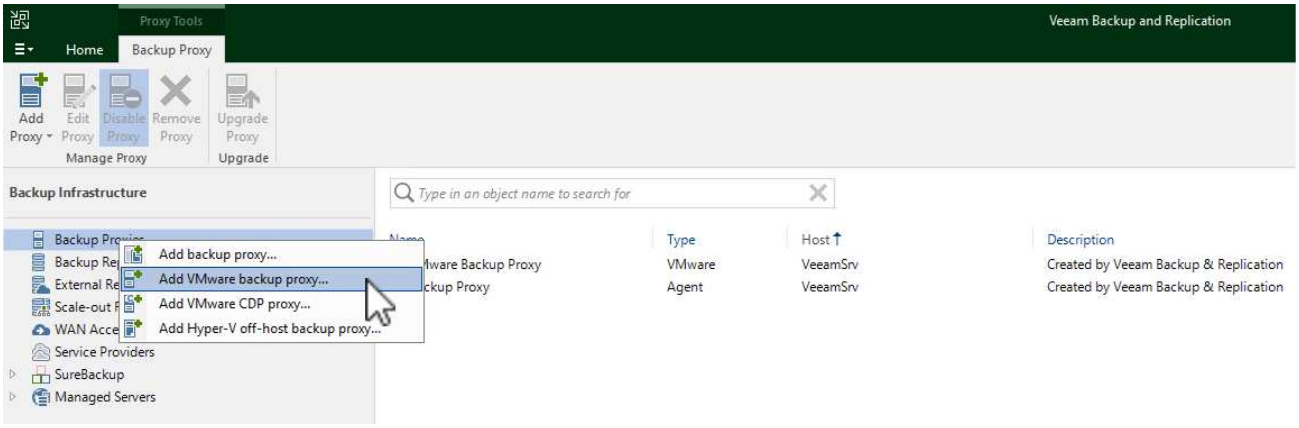
トランスポートモードの詳細については、 "Veeam バックアップおよびレプリケーション VMware vSphere 向けユーザー ガイド" 。

次の手順では、VMware Cloud SDDC 内の Windows VM への Veeam Proxy Server の展開について説明します。

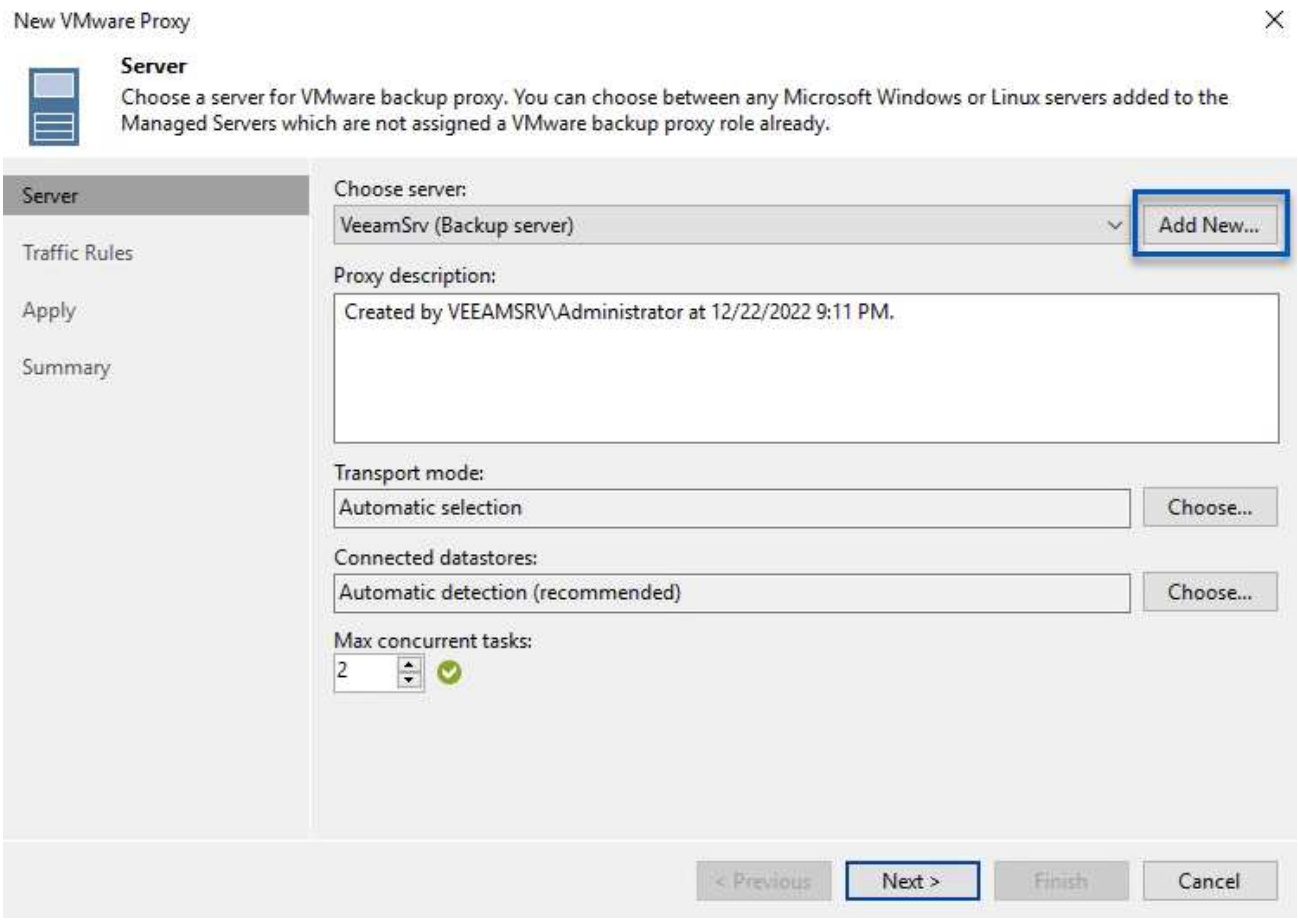
▼ **Veeam Proxy**を導入してバックアップワークロードを分散する

この手順では、Veeam Proxy が既存の Windows VM に展開されます。これにより、バックアップ ジョブをプライマリ Veeam バックアップ サーバーと Veeam プロキシの間で分散できるようになります。

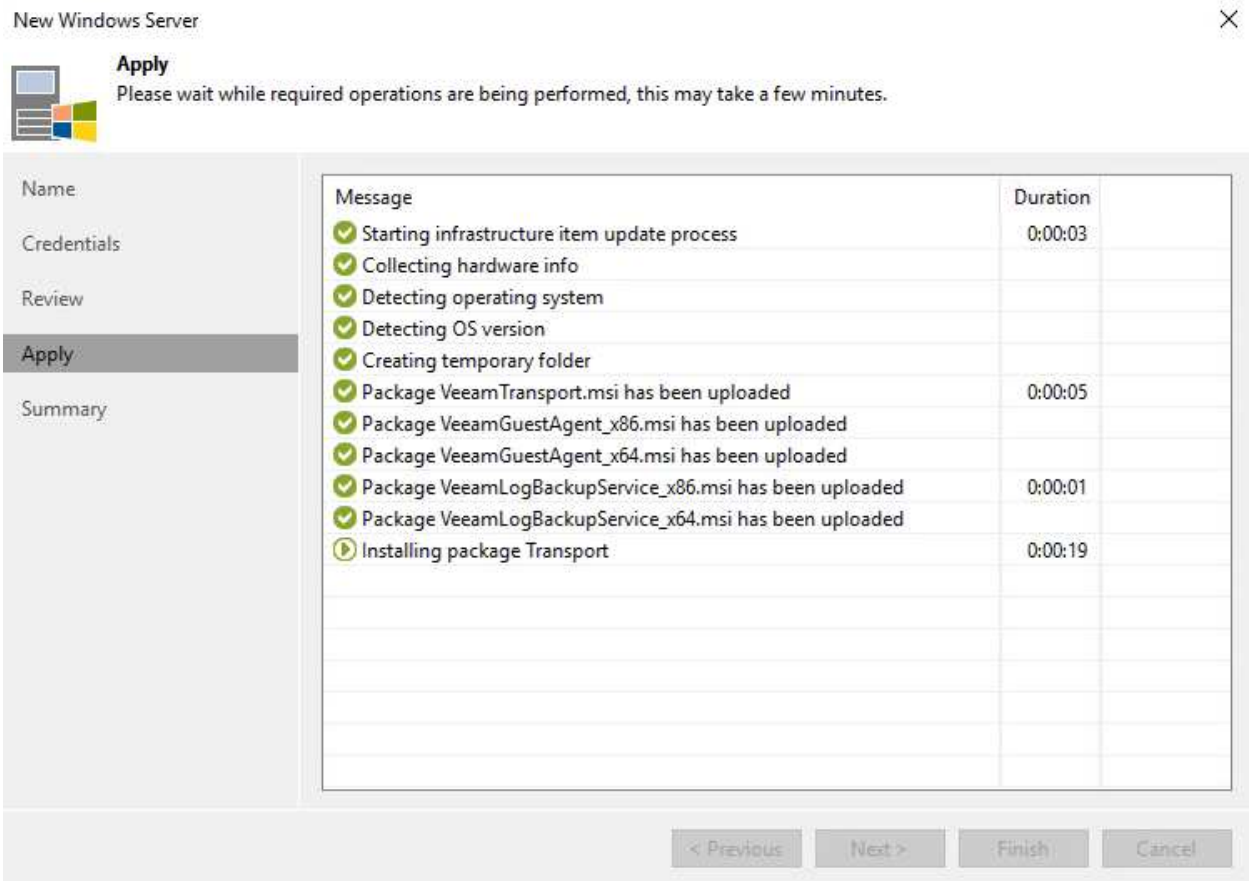
1. Veeam Backup and Replication サーバーで管理コンソールを開き、左下のメニューで バックアップ インフラストラクチャ を選択します。
2. バックアップ プロキシ を右クリックし、**VMware** バックアップ プロキシの追加... をクリックしてウィザードを開きます。



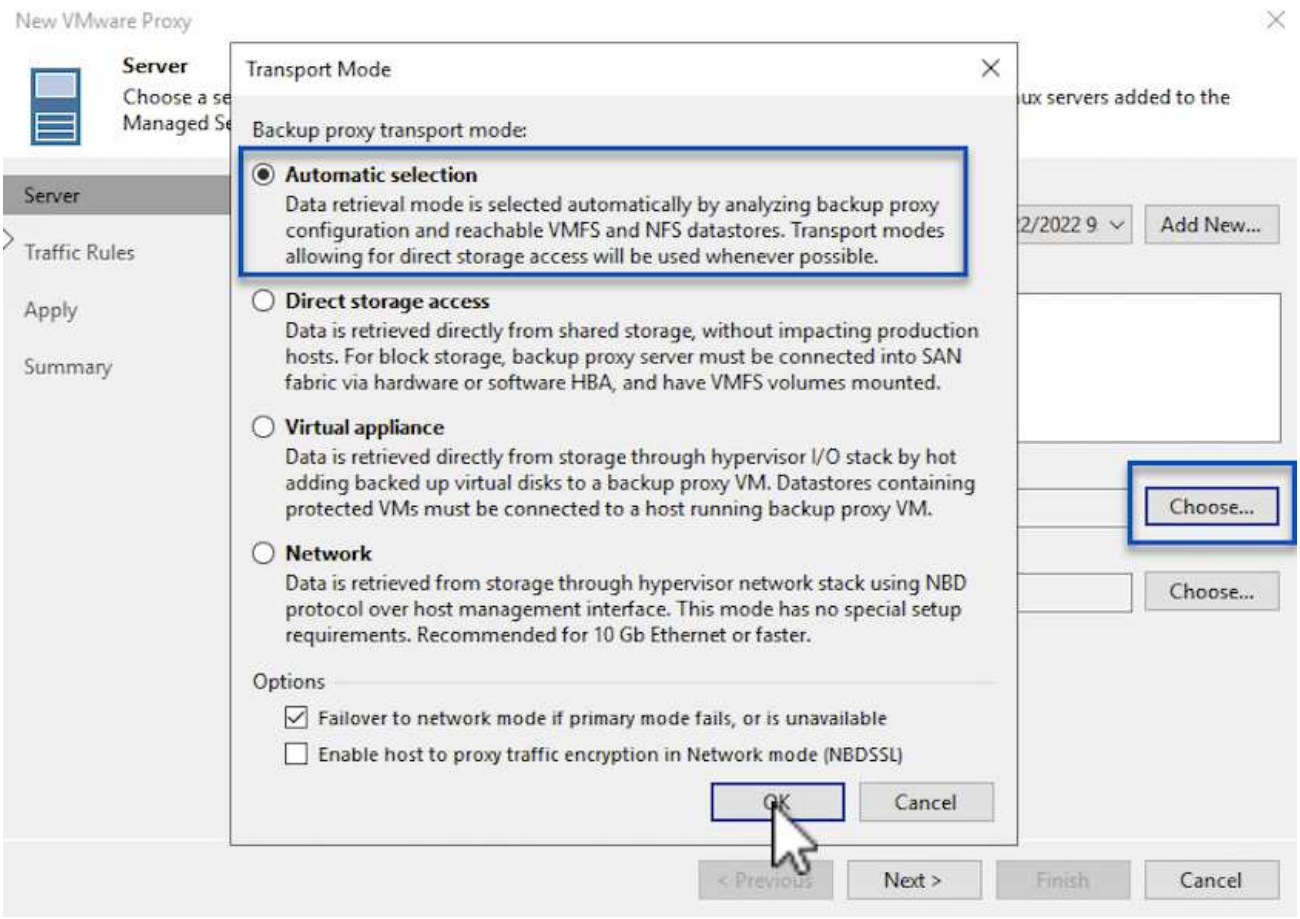
3. *VMware プロキシの追加*ウィザードで*新規追加...*ボタンをクリックして、新しいプロキシ サーバーを追加します。



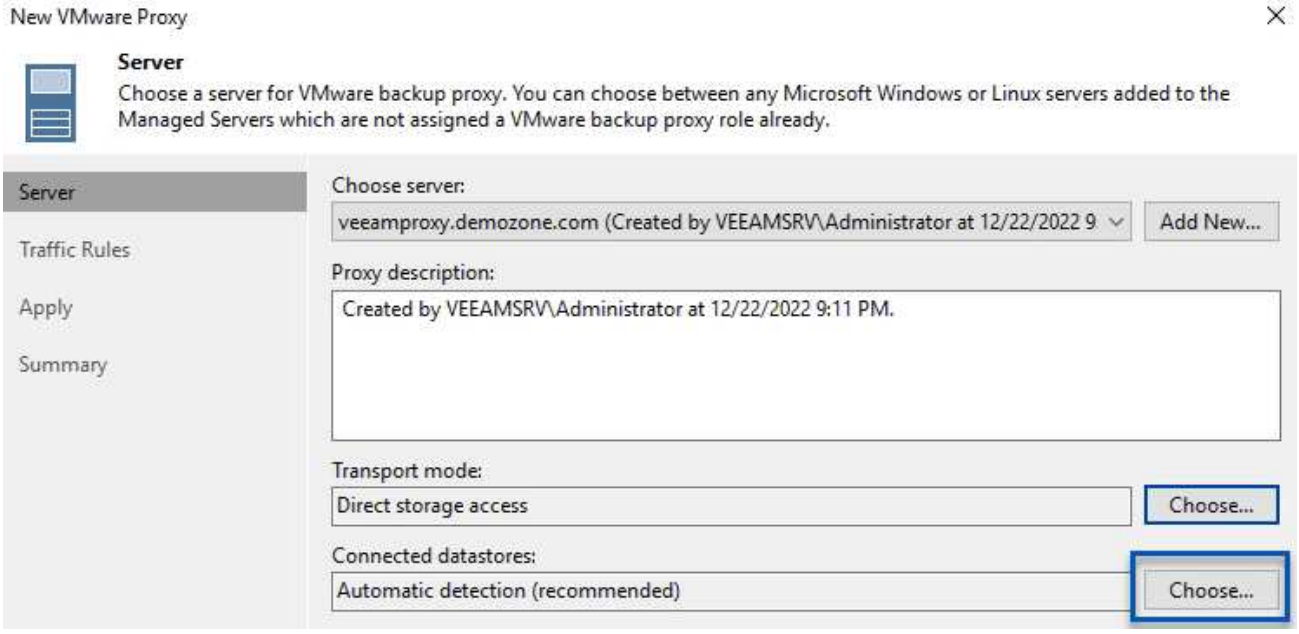
4. Microsoft Windows を追加するように選択し、プロンプトに従ってサーバーを追加します。
   - DNS名またはIPアドレスを入力してください
   - 新しいシステムの資格情報に使用するアカウントを選択するか、新しい資格情報を追加します
   - インストールするコンポーネントを確認し、「適用」をクリックして展開を開始します。

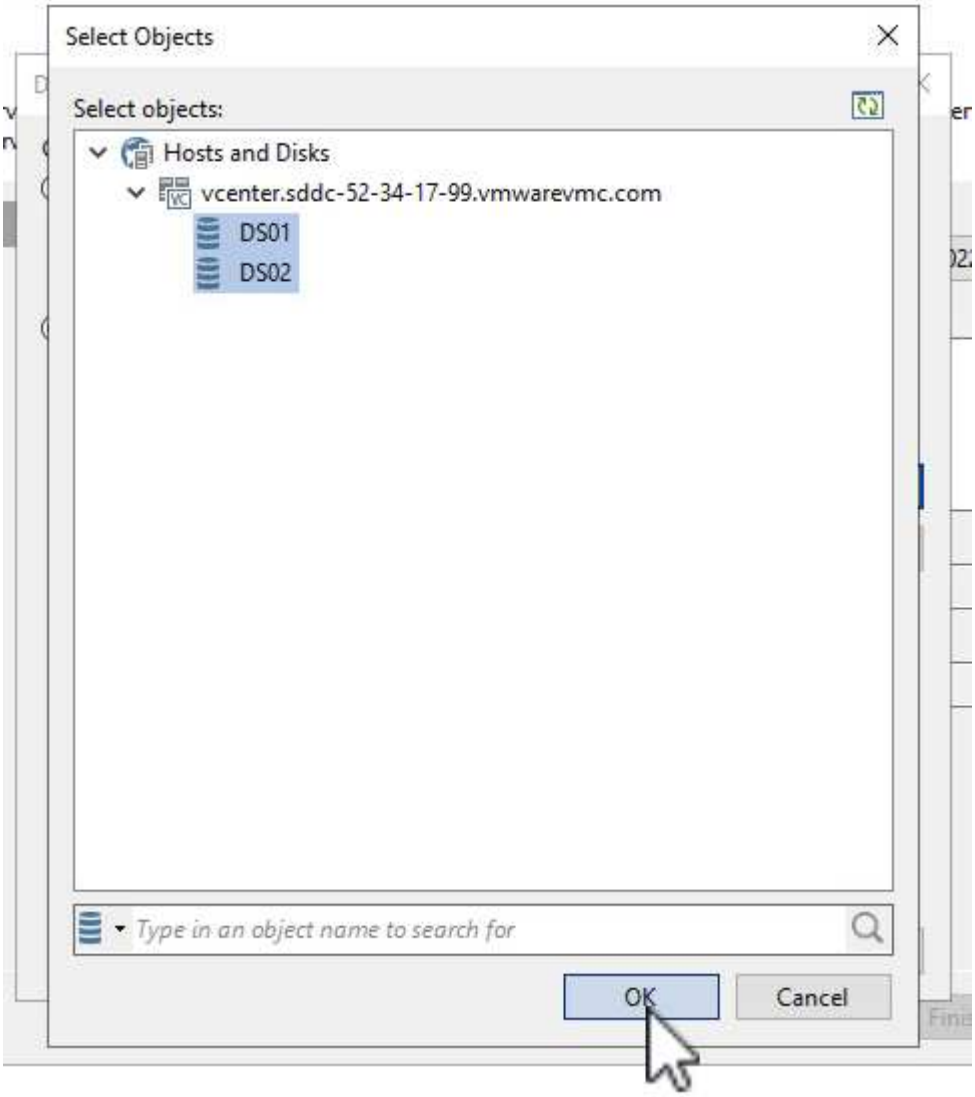


5. 新しい **VMware Proxy** ウィザードに戻り、トランスポート モードを選択します。私たちの場合は、「自動選択」を選択しました。

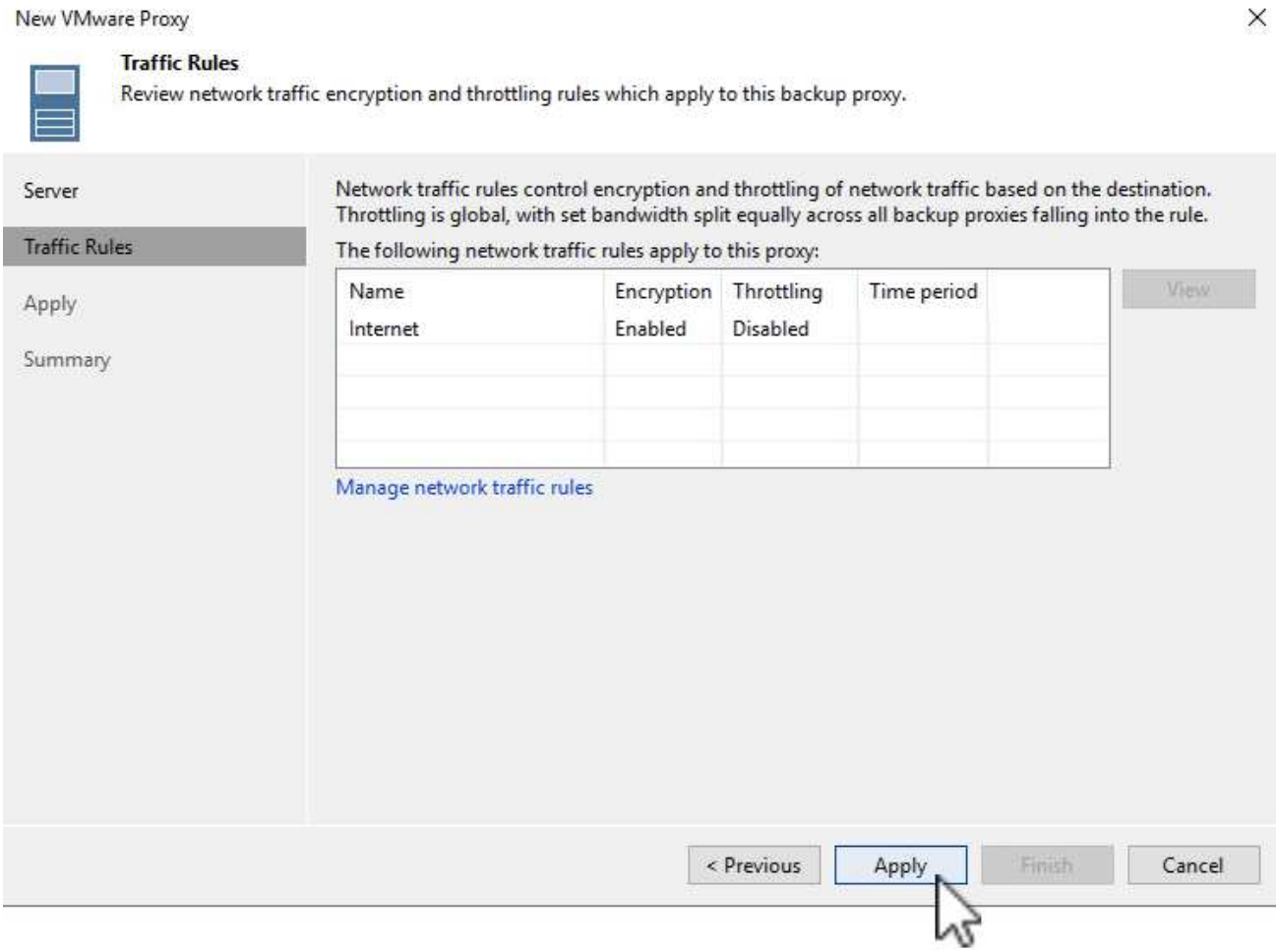


6. VMware Proxy が直接アクセスできるようにする接続されたデータストアを選択します。





7. 必要な暗号化やスロットルなどの特定のネットワーク トラフィック ルールを構成して適用します。完了したら、[適用] ボタンをクリックしてデプロイを完了します。



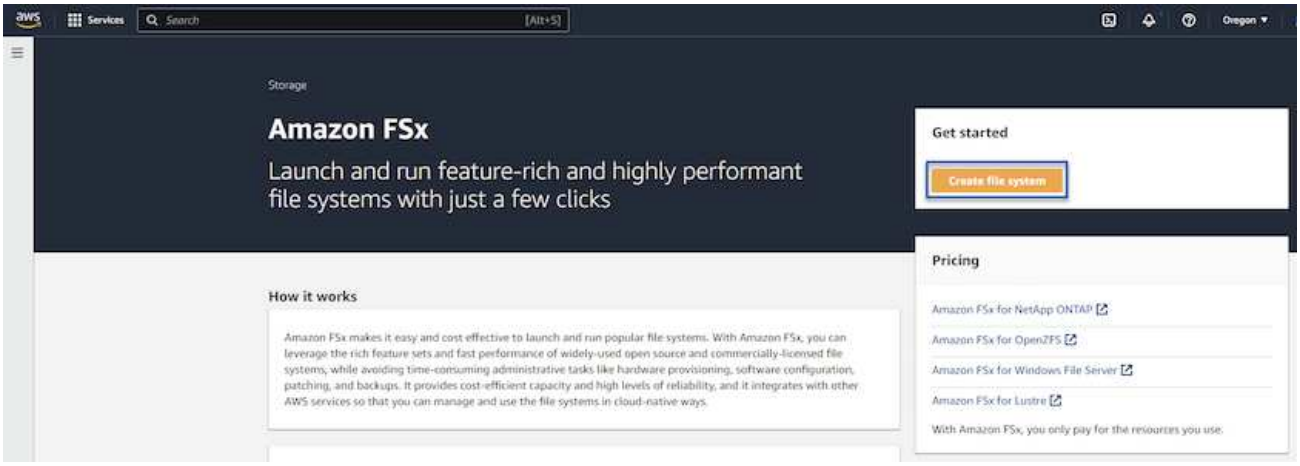
ストレージとバックアップリポジトリを構成する

プライマリ Veeam バックアップ サーバーと Veeam プロキシ サーバーは、直接接続されたストレージの形式でバックアップ リポジトリにアクセスできます。このセクションでは、FSx ONTAPファイル システムの作成、iSCSI LUN の Veeam サーバーへのマウント、およびバックアップ リポジトリの作成について説明します。

▼ **FSx ONTAP**ファイルシステムを作成する

Veeam バックアップ リポジトリの iSCSI ボリュームをホストするために使用される FSx ONTAPファイル システムを作成します。

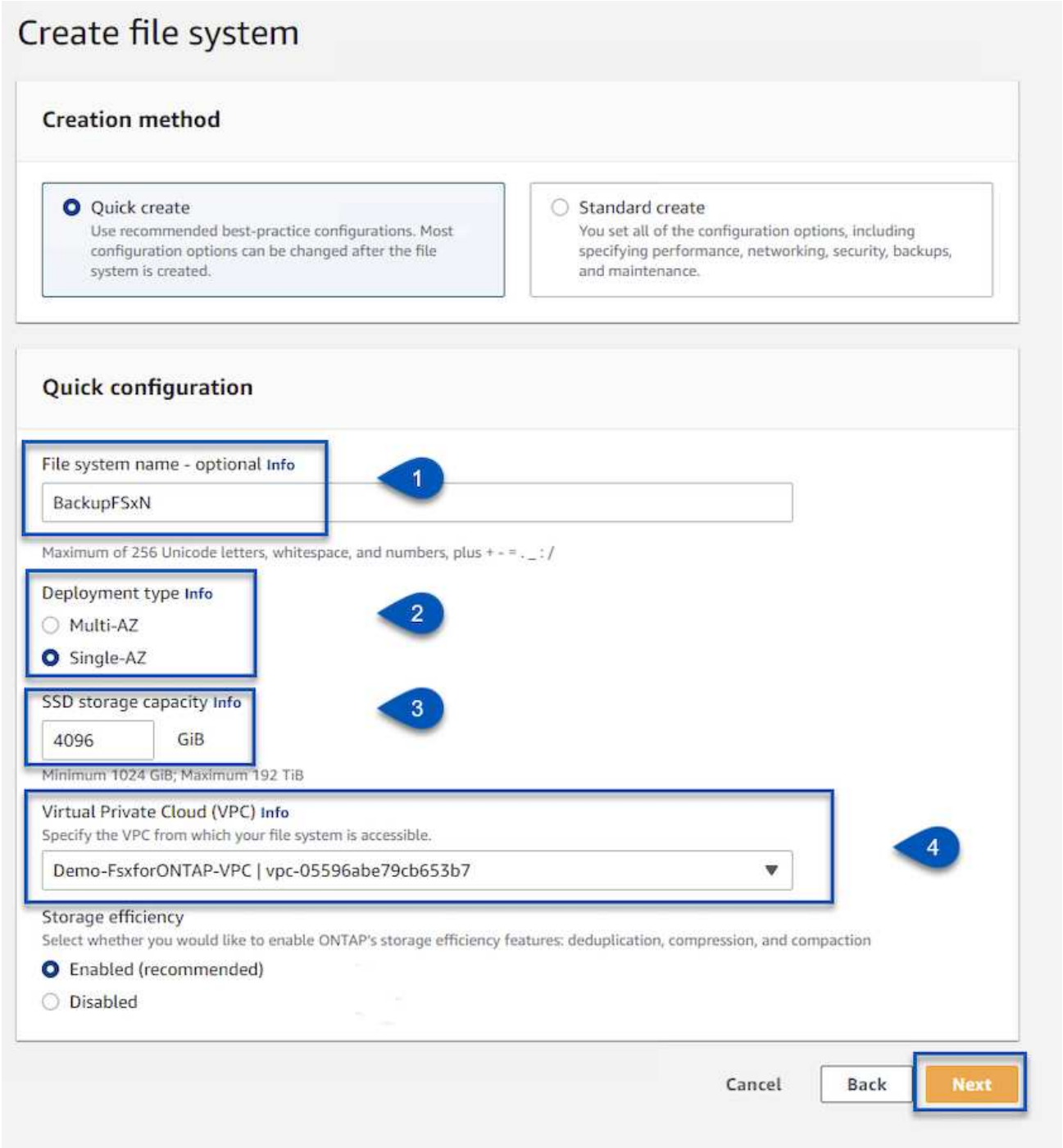
1. AWSコンソールでFSxに移動し、*ファイルシステムの作成*を選択します。



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



3. ファイルシステム名、デプロイメントタイプ、SSD ストレージ容量、および FSx ONTAPクラスターが存在する 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構成された VPC である必要があります。 *次へ*をクリックします。



4. 展開手順を確認し、「ファイル システムの作成」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** の構成とマウント

FSx ONTAPで iSCSI LUN を作成および構成し、Veeam バックアップ サーバーとプロキシ サーバーにマウントします。これらの LUN は、後で Veeam バックアップ リポジトリを作成するために使用されます。

FSx ONTAPで iSCSI LUN を作成するには、複数のステップが必要です。ボリュームを作成する最初のステップは、Amazon FSxコンソールまたはNetApp ONTAP CLI を使用して実行できます。

FSx ONTAP の使用に関する詳細については、 "FSx ONTAPユーザーガイド" 。

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 サーバーとプロキシ サーバーの iSCSI IQN を含むイニシエーター グループを作成して、LUN へのアクセスを許可します。

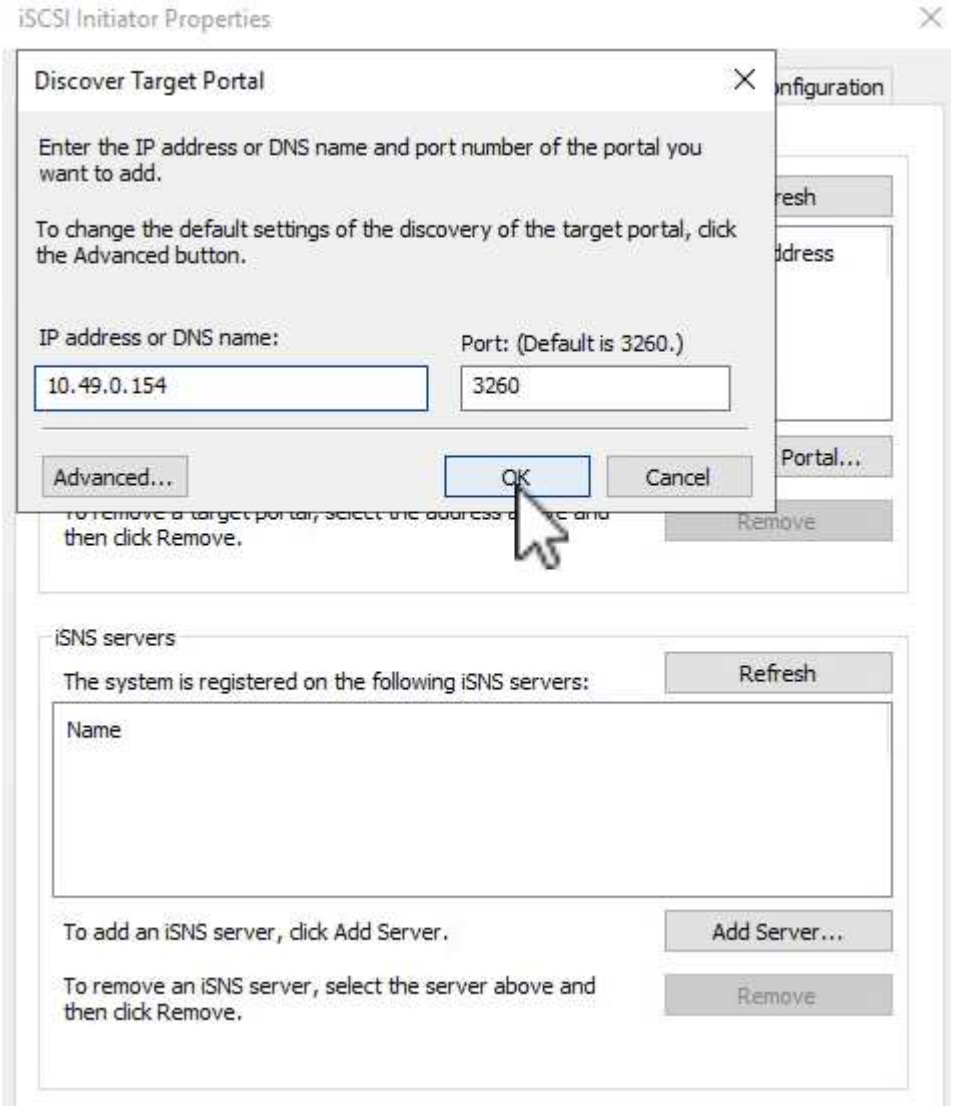
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

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

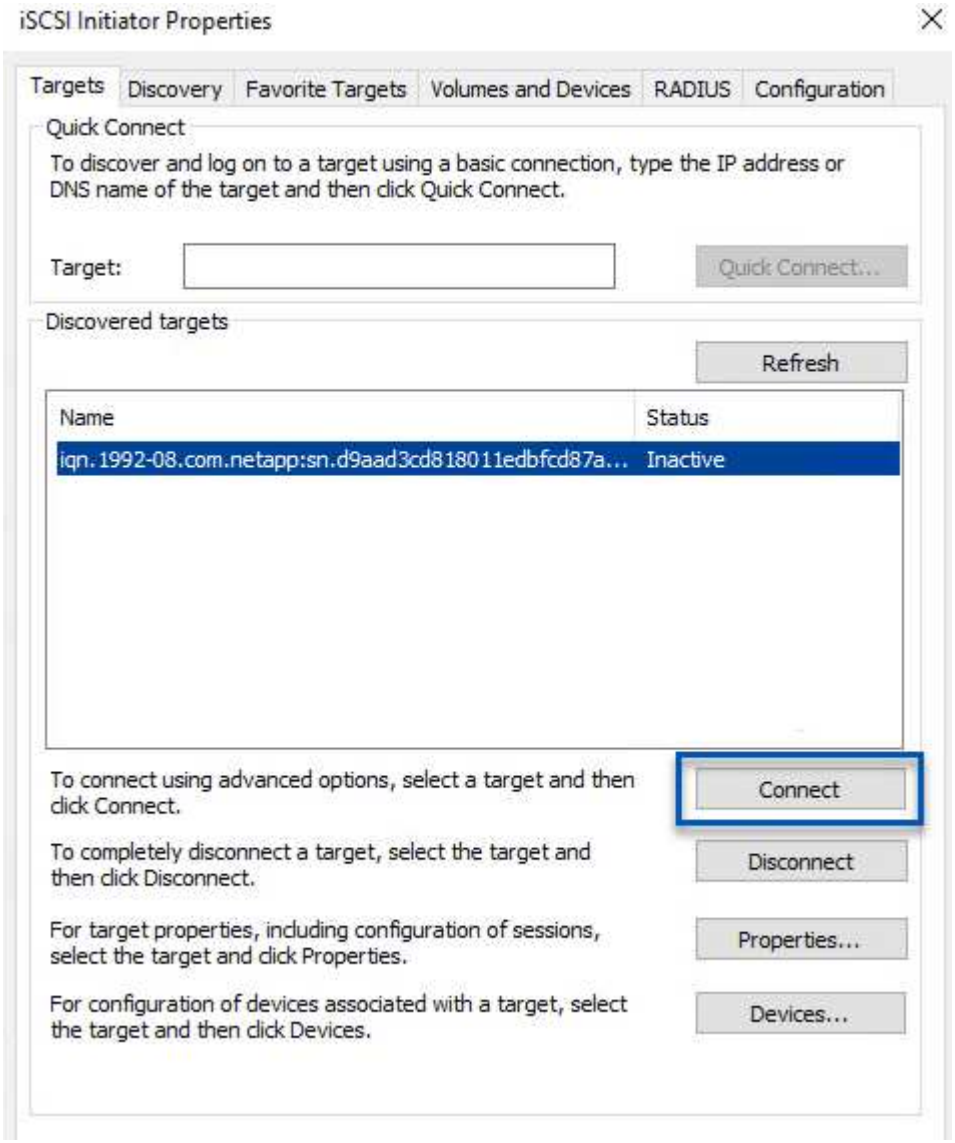
4. 最後に、作成したイニシエーター グループに LUN をマップします。

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

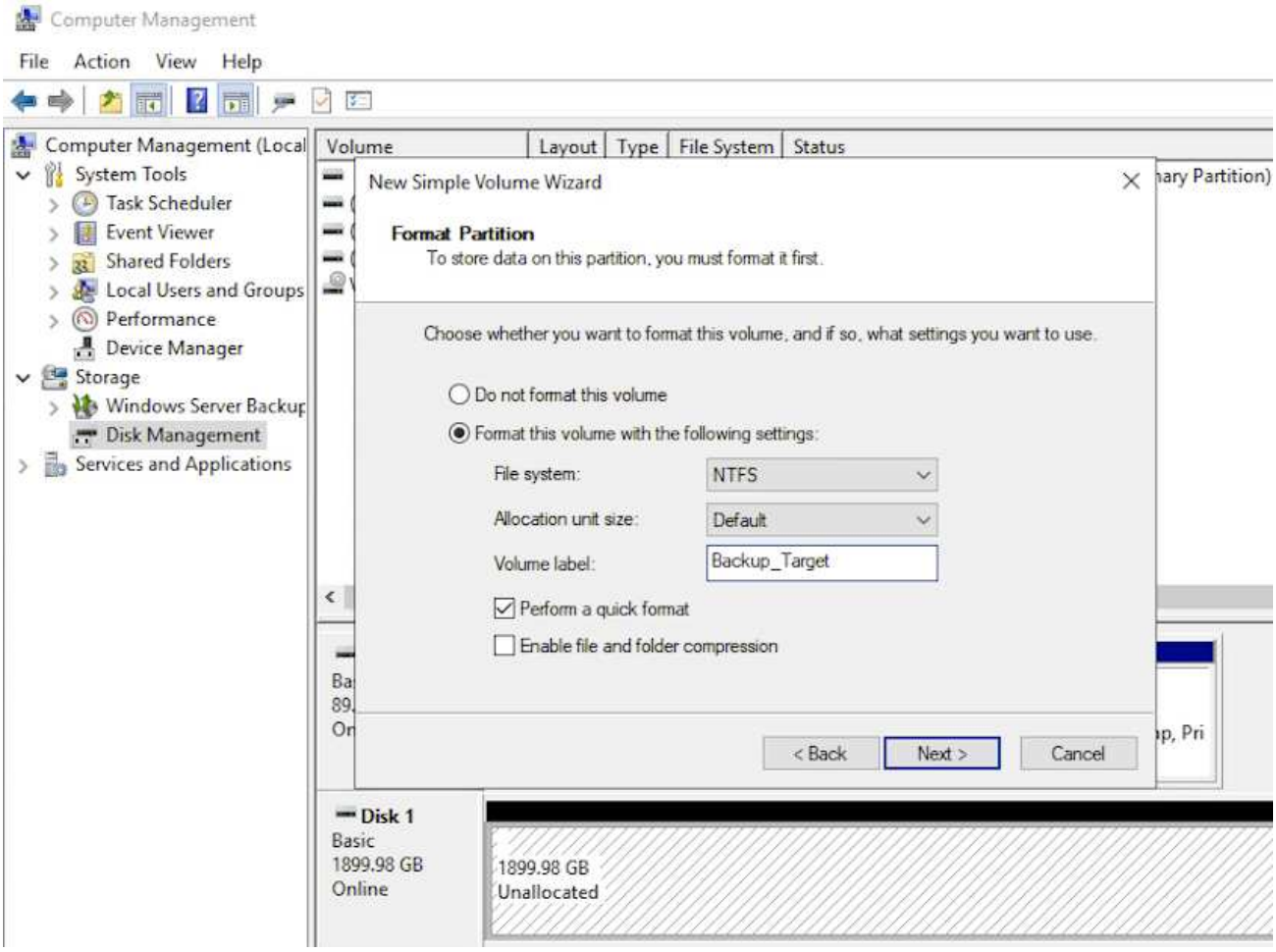
5. iSCSI LUN をマウントするには、Veeam Backup & Replication Server にログインし、iSCSI イニシエーターのプロパティを開きます。 *検出*タブに移動し、iSCSI ターゲットの IP アドレスを入力します。



6. ターゲット タブで、非アクティブな LUN を強調表示し、接続 をクリックします。 *マルチパスを有効にする*ボックスをチェックし、*OK*をクリックして LUN に接続します。



7. ディスク管理ユーティリティで、新しい LUN を初期化し、希望の名前とドライブ文字を持つボリュームを作成します。 *マルチパスを有効にする*ボックスをチェックし、*OK*をクリックして LUN に接続します。

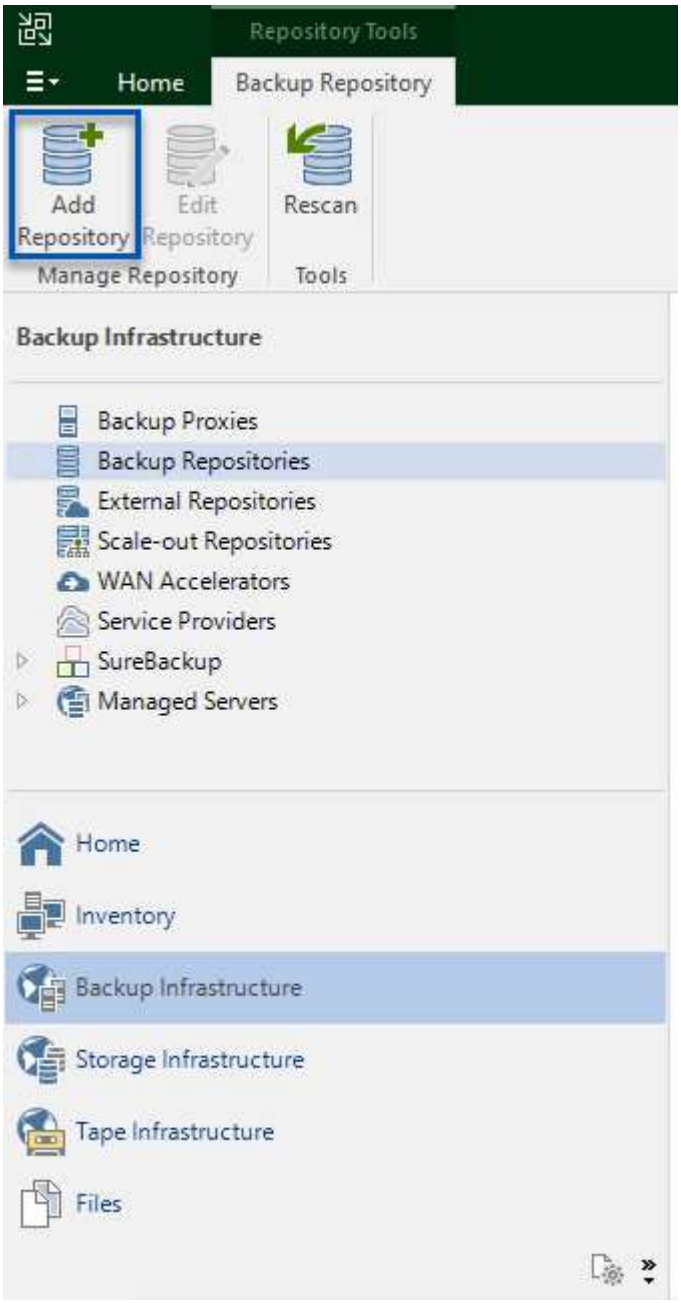


8. これらの手順を繰り返して、iSCSI ボリュームを Veeam Proxy サーバーにマウントします。

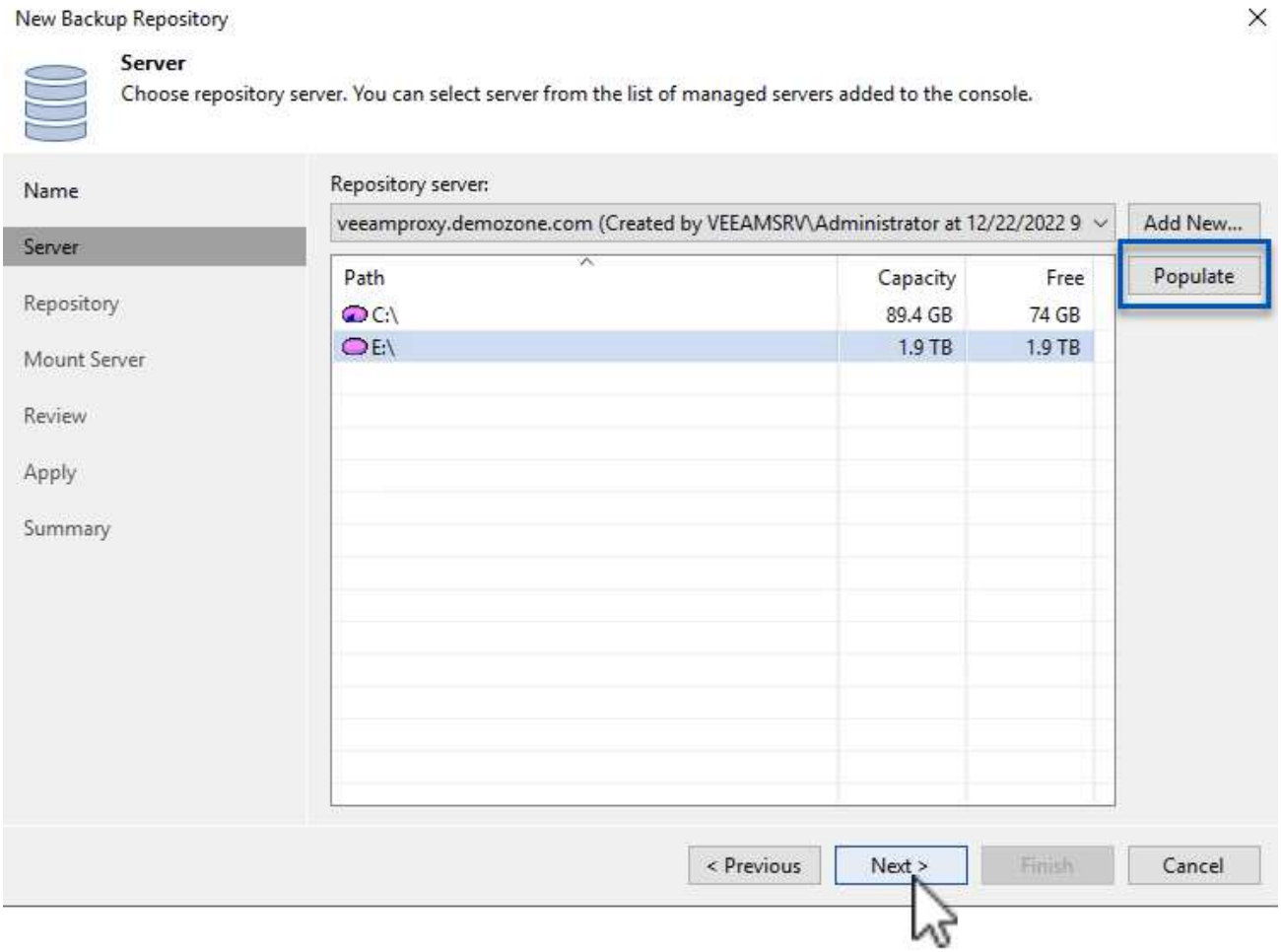
▼ **Veeam** バックアップ リポジトリを作成する

Veeam Backup and Replication コンソールで、Veeam Backup サーバーと Veeam Proxy サーバーのバックアップ 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。

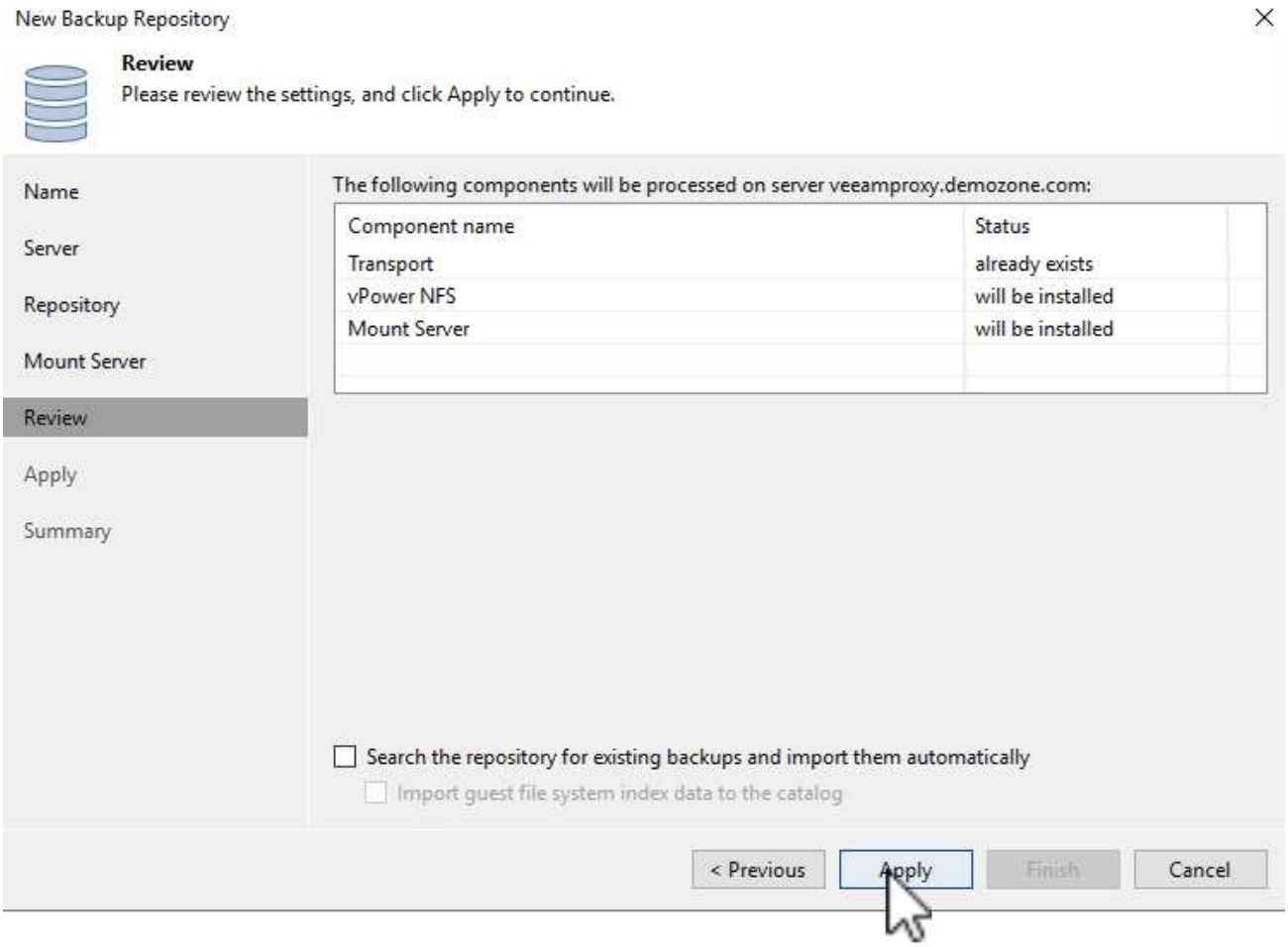
1. Veeam Backup and Replicationコンソールで、左下にある*バックアップインフラストラクチャ*をクリックし、*リポジトリの追加*を選択します。



2. 新しいバックアップ リポジトリ 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 リストからサーバーを選択して、**Populate** ボタンをクリックして、使用する NTFS ボリュームを選択します。



3. 次のページで、高度な復元を実行するときにバックアップをマウントするために使用するマウント サーバーを選択します。デフォルトでは、これはリポジトリ ストレージが接続されているサーバーと同じサーバーです。
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 サーバーに対してこれらの手順を繰り返します。

Veeam バックアップジョブを構成する

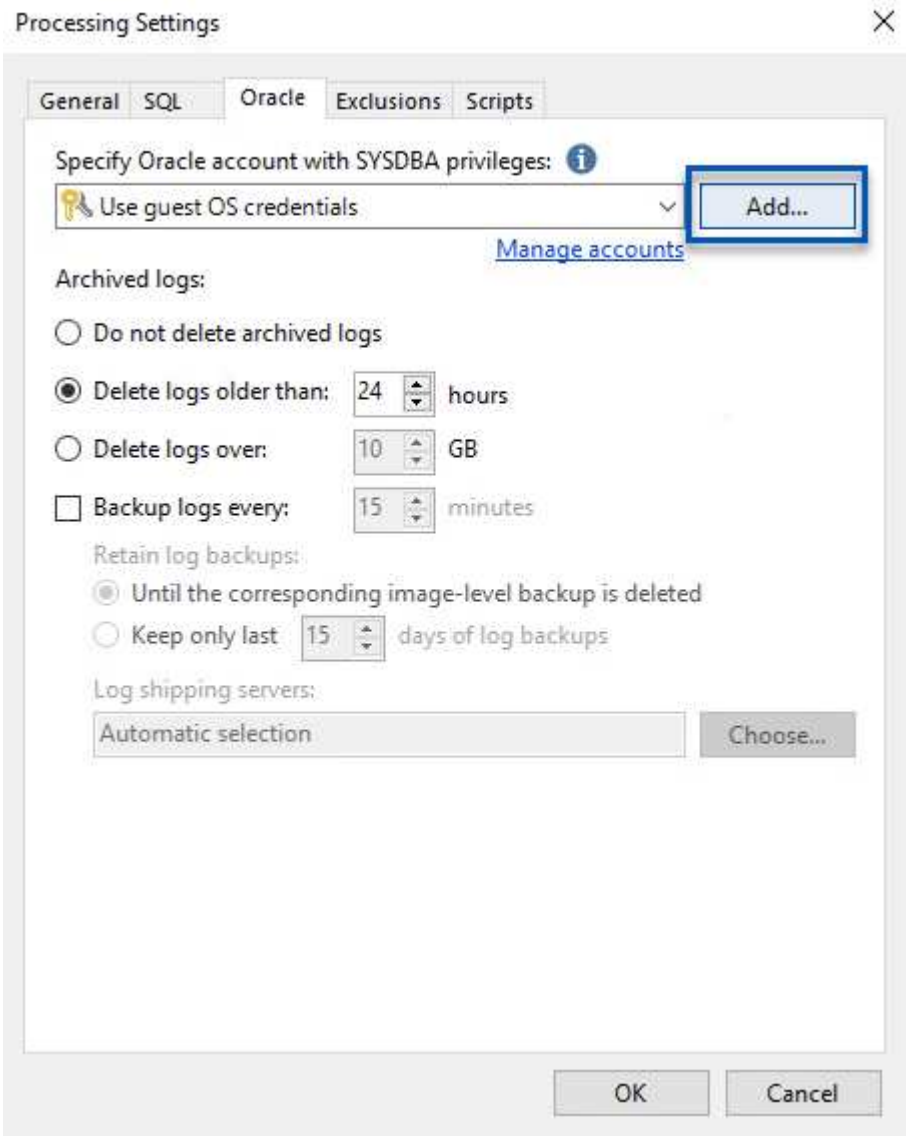
バックアップ ジョブは、前のセクションのバックアップ リポジトリを利用して作成する必要があります。バックアップ ジョブの作成は、ストレージ管理者の通常の業務の一部であり、ここではすべての手順を説明するわけではありません。 Veeamでのバックアップジョブ作成の詳細については、 "Veeamヘルプセンター技術ドキュメント" 。

このソリューションでは、次の個別のバックアップ ジョブが作成されました。

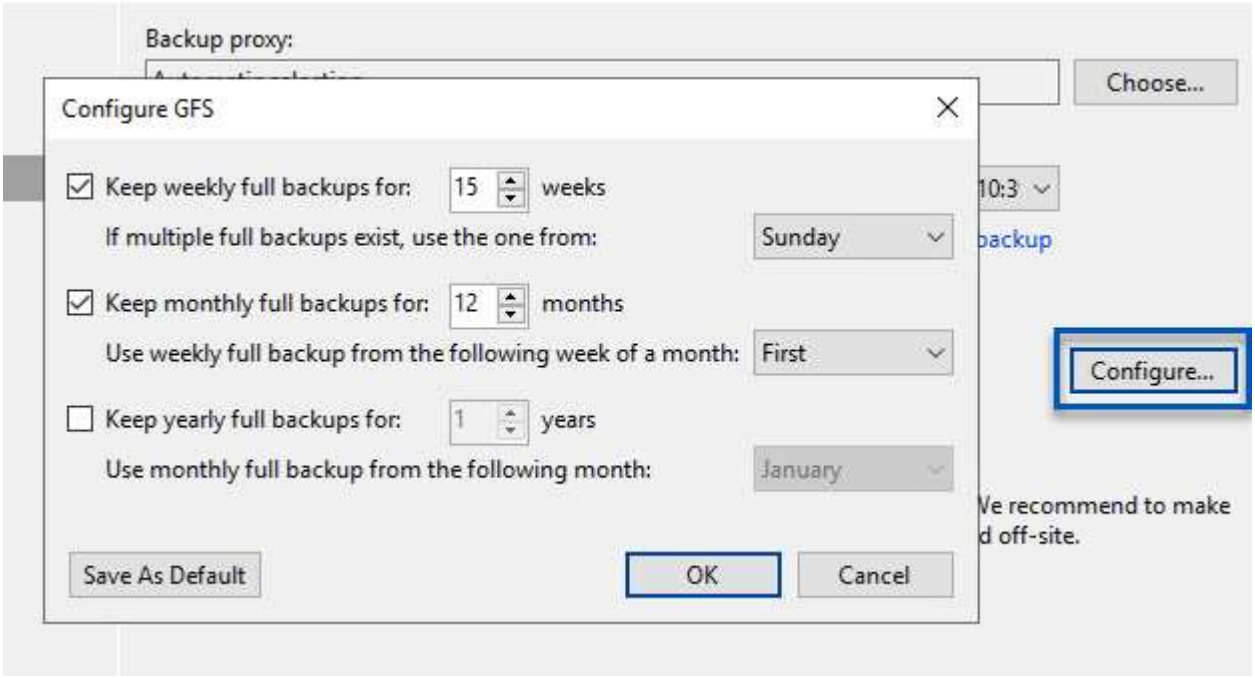
- Microsoft Windows SQL サーバー
- Oracleデータベースサーバー
- Windows ファイルサーバー
- Linux ファイルサーバー

▼ **Veeam** バックアップジョブを構成する際の一般的な考慮事項

1. アプリケーション対応の処理を有効にして、一貫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します。
2. アプリケーション対応処理を有効にした後、ゲスト OS の資格情報とは異なる可能性があるため、管理者権限を持つ正しい資格情報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、[アーカイブ目的で特定の完全バックアップを長期間保持する] をオンにし、[構成...] ボタンをクリックしてポリシーを構成します。



Veeam の完全復元でアプリケーション **VM** を復元する

Veeam を使用して完全復元を実行することは、アプリケーションの復元を実行するための最初のステップです。 VM の完全復元がオンになり、すべてのサービスが正常に実行されていることを検証しました。

サーバーの復元は、ストレージ管理者の通常の業務の一部であり、ここではすべての手順を説明するわけではありません。 Veeamでフルリストアを実行する方法の詳細については、 "Veeamヘルプセンター技術ドキュメント" 。

SQL Server データベースを復元する

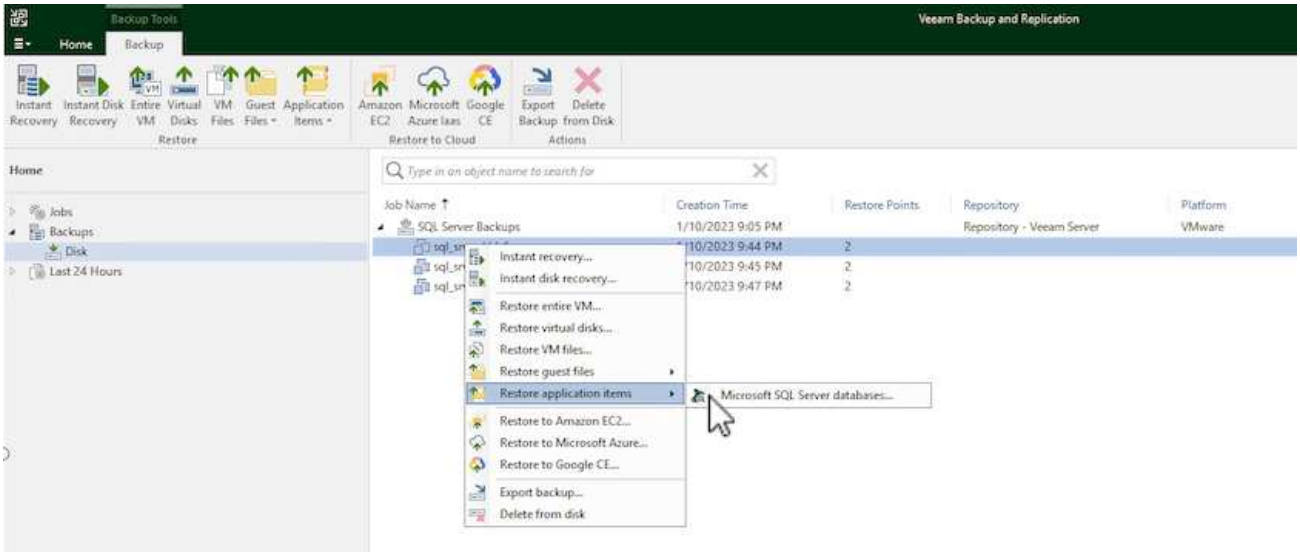
Veeam Backup & Replication には、SQL Server データベースを復元するためのいくつかのオプションが用意されています。この検証では、Veeam Explorer for SQL Server と Instant Recovery を使用して、SQL Server データベースの復元を実行しました。 SQL Server インスタント リカバリは、データベースの完全復元を待たずに SQL Server データベースを迅速に復元できる機能です。この迅速な回復プロセスにより、ダウンタイムが最小限に抑えられ、ビジネスの継続性が確保されます。仕組みは以下のとおりです:

- Veeam Explorer は、復元する 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直接データベースを公開し、ターゲットの 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操作できるようにします。
- バックグラウンドでは、Veeam は 完全なデータベースの復元を実行 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。
- 完全なデータベースの復元が完了すると、Veeam Explorer はユーザー クエリを元のデータベースに切り替え、一時データベースを削除します。

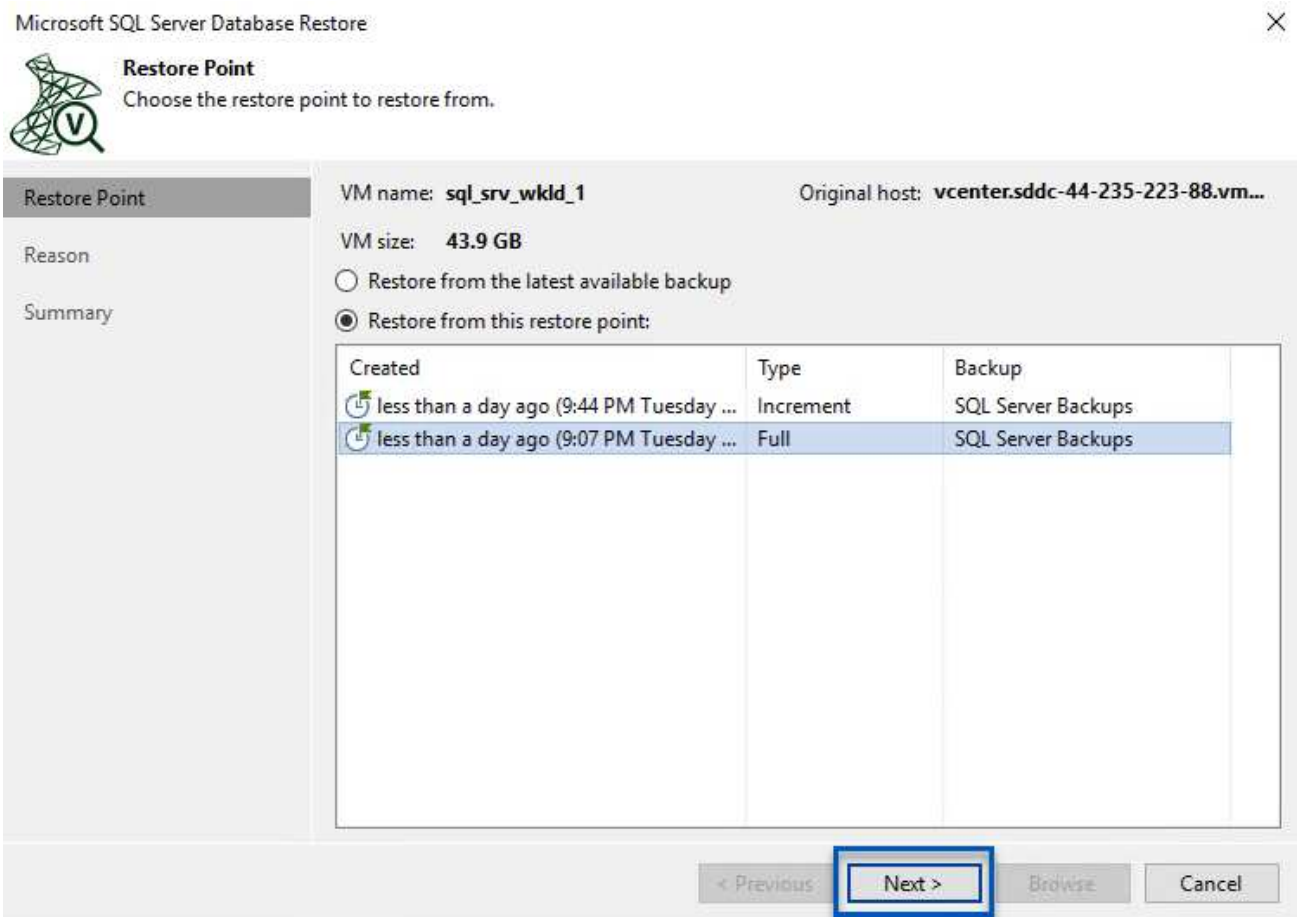
▼ **Veeam Explorer Instant Recovery** を使用して **SQL Server** データベースを復元する

1. Veeam Backup and Replication コンソールで、SQL Server バックアップのリストに移動し、サーバー上で右クリックして、アプリケーション項目の復元 を選択し、次に **Microsoft SQL Server** データベー

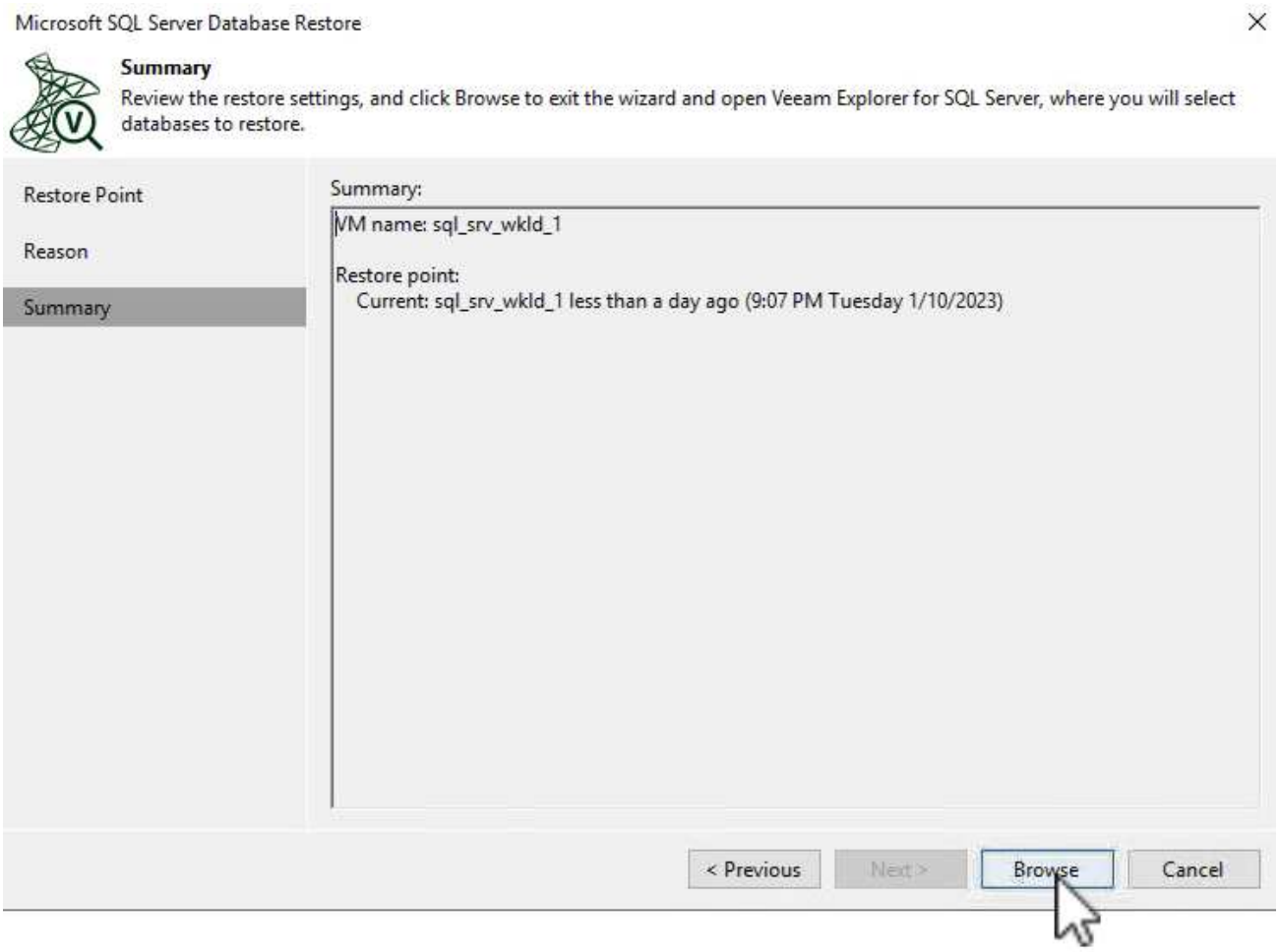
ス... を選択します。



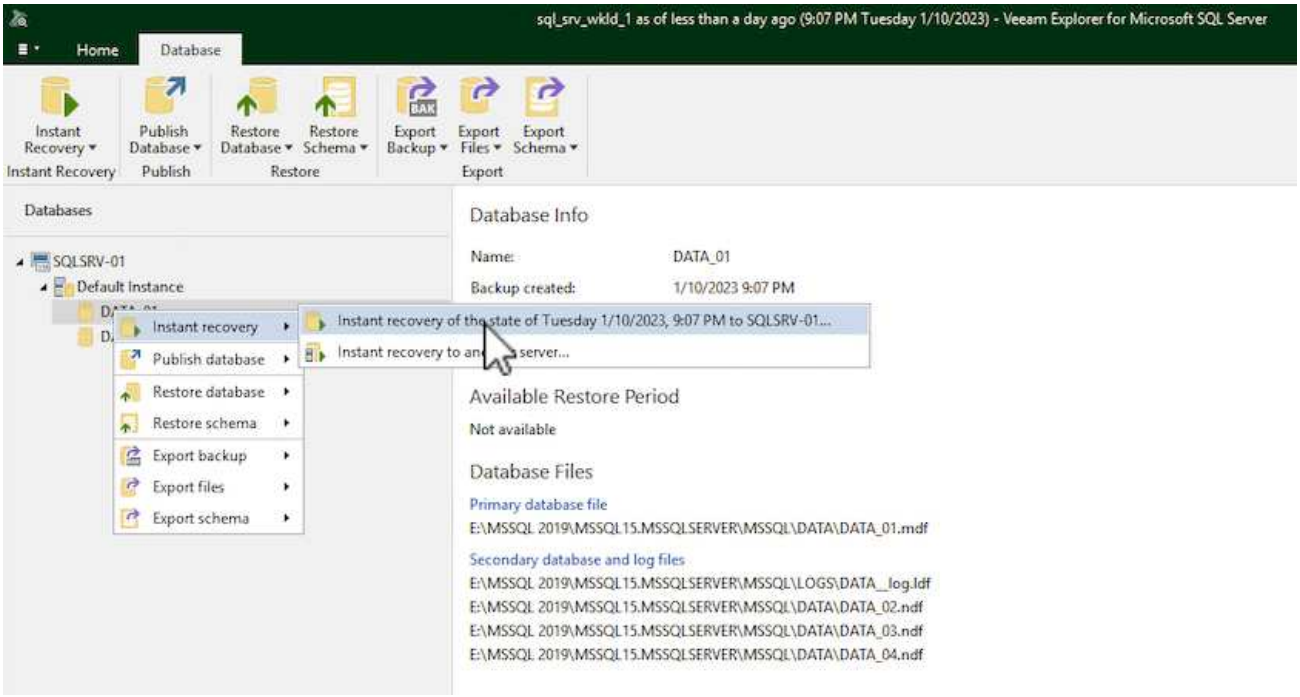
2. Microsoft SQL Server データベース復元ウィザードで、リストから復元ポイントを選択し、[次へ] をクリックします。



3. 必要に応じて 復元理由 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。

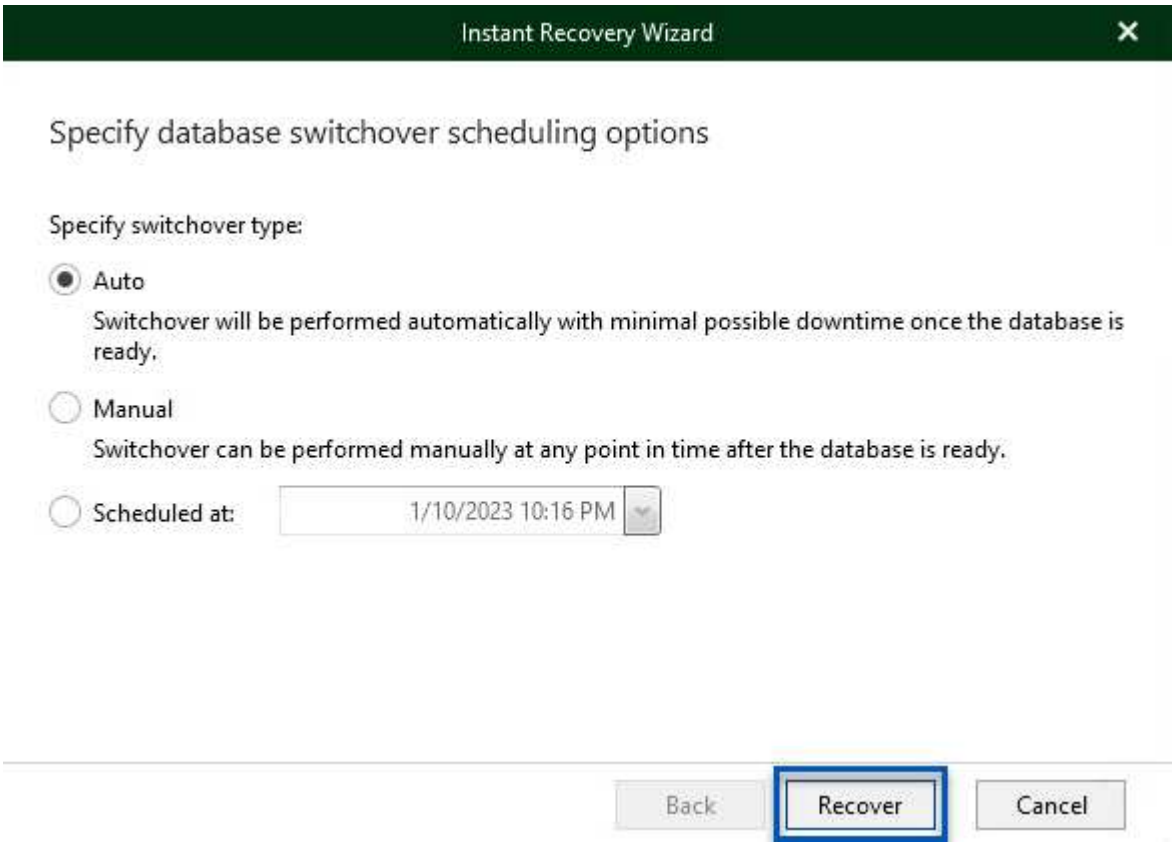


4. Veeam Explorer でデータベース インスタンスのリストを展開し、右クリックして インスタント リカバリ を選択し、復元先の特定の復元ポイントを選択します。

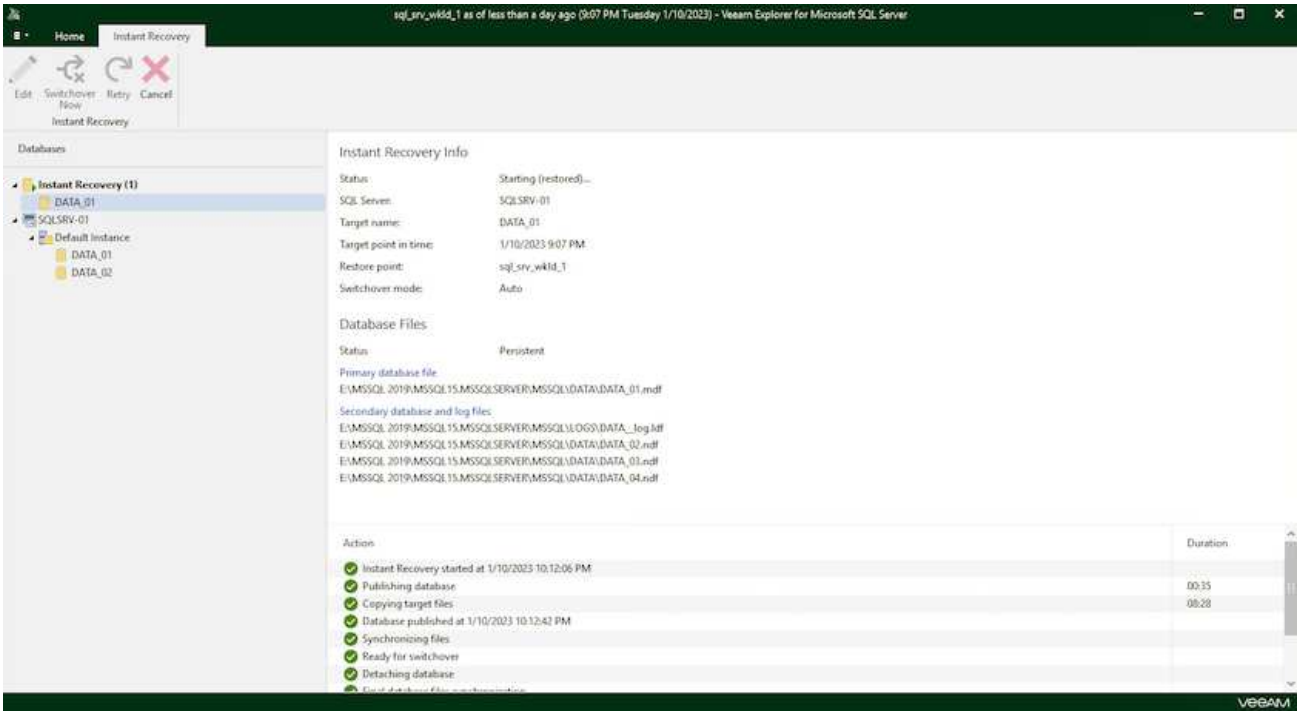


5. インスタント リカバリ ウィザードでスイッチオーバー タイプを指定します。これは、最小限のダウン

タイムで自動的に実行することも、手動で実行することも、指定された時間に実行することもできます。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でSQL Serverの復元操作を実行する方法の詳細については、 "Veeam Explorer ユーザーガイド" 。

Veeam ExplorerでOracleデータベースを復元する

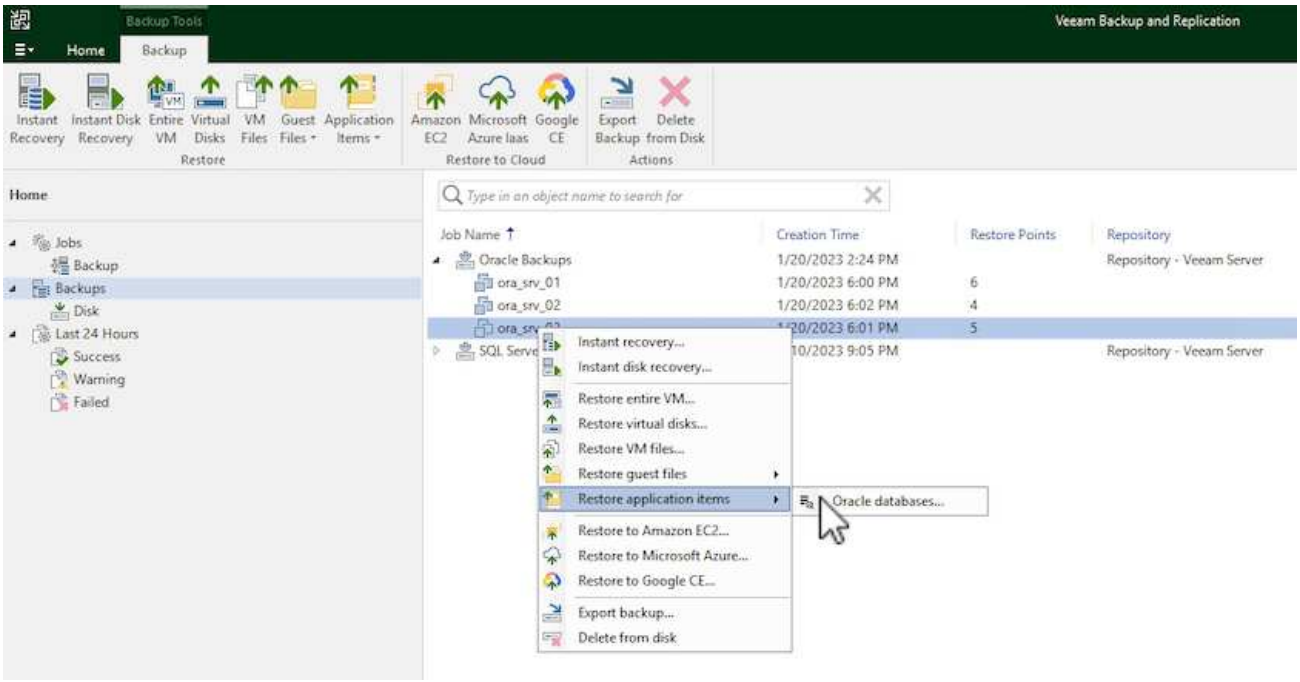
Veeam Explorer for Oracle データベースは、標準の Oracle データベース復元または Instant Recovery を使用した中断のない復元を実行する機能を提供します。また、高速アクセスのためのデータベースの公開、Data Guard データベースのリカバリ、RMAN バックアップからの復元もサポートしています。

Veeam Explorerを使用したOracleデータベースの復元操作の詳細については、 "Veeam Explorer ユーザーガイド" 。

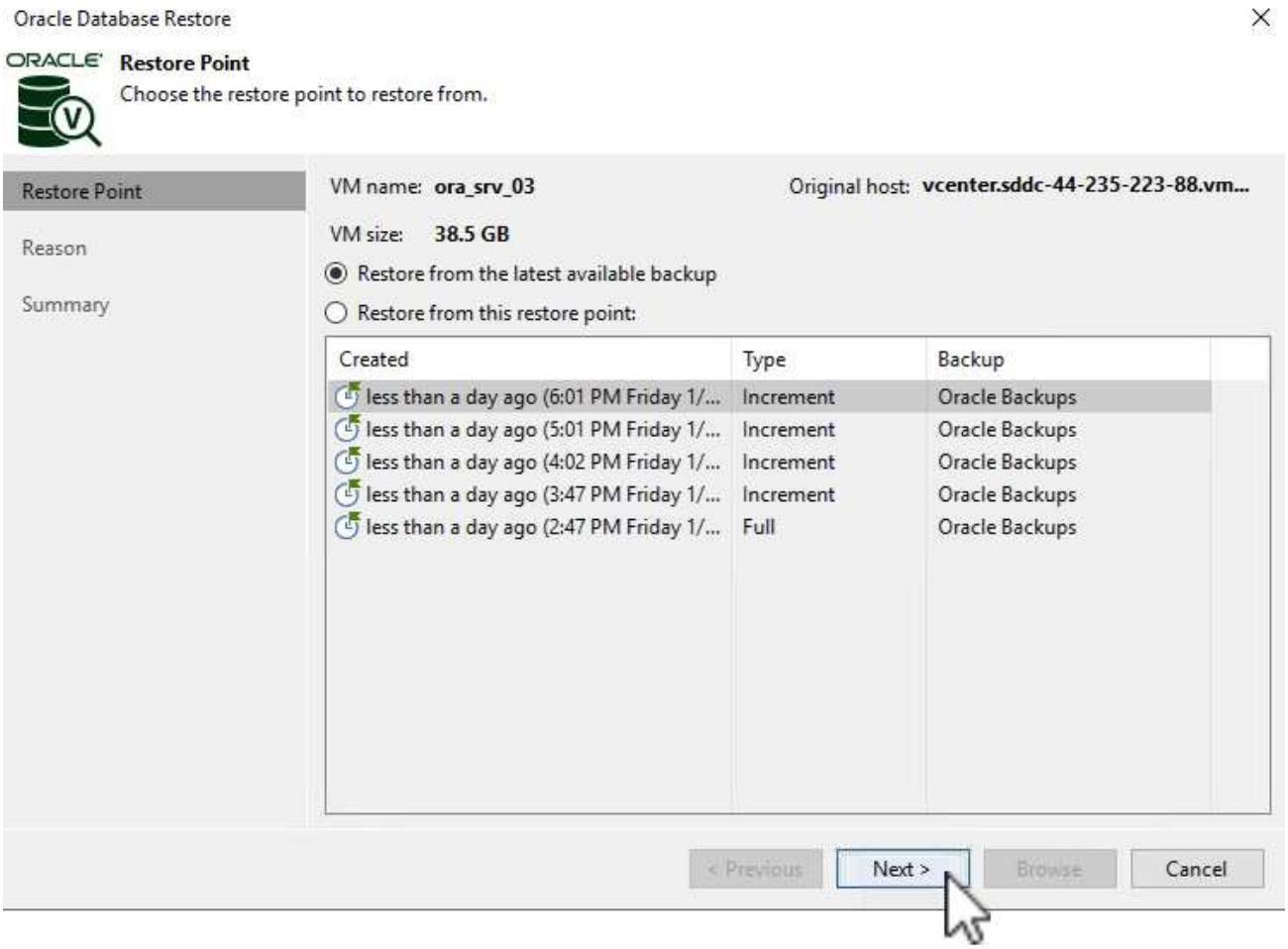
▼ Veeam ExplorerでOracleデータベースを復元する

このセクションでは、Veeam Explorer を使用して Oracle データベースを別のサーバーに復元する方法について説明します。

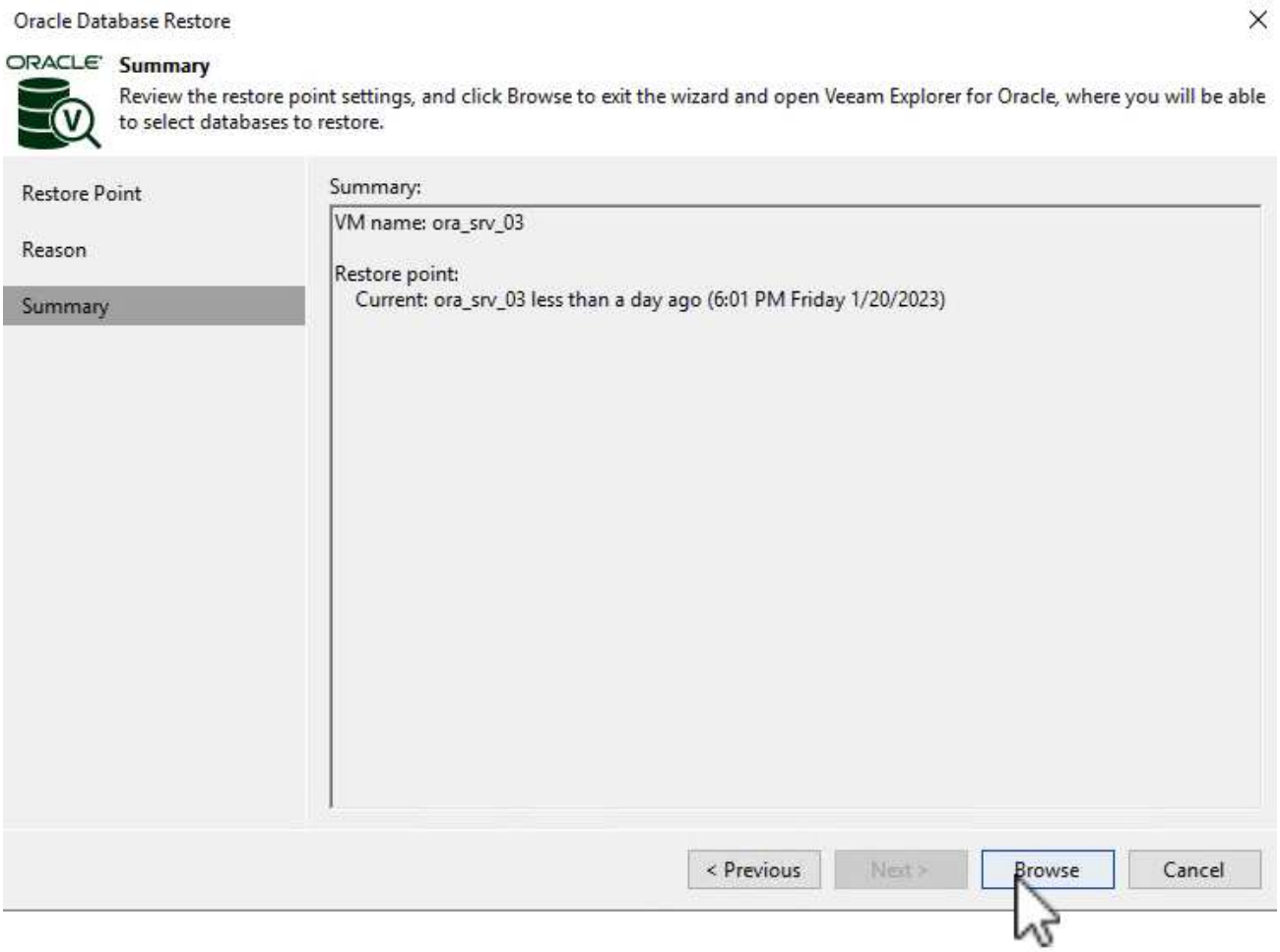
1. Veeam Backup and Replication コンソールで、Oracle バックアップのリストに移動し、サーバー上で右クリックして アプリケーション項目の復元 を選択し、次に **Oracle** データベース… を選択します。



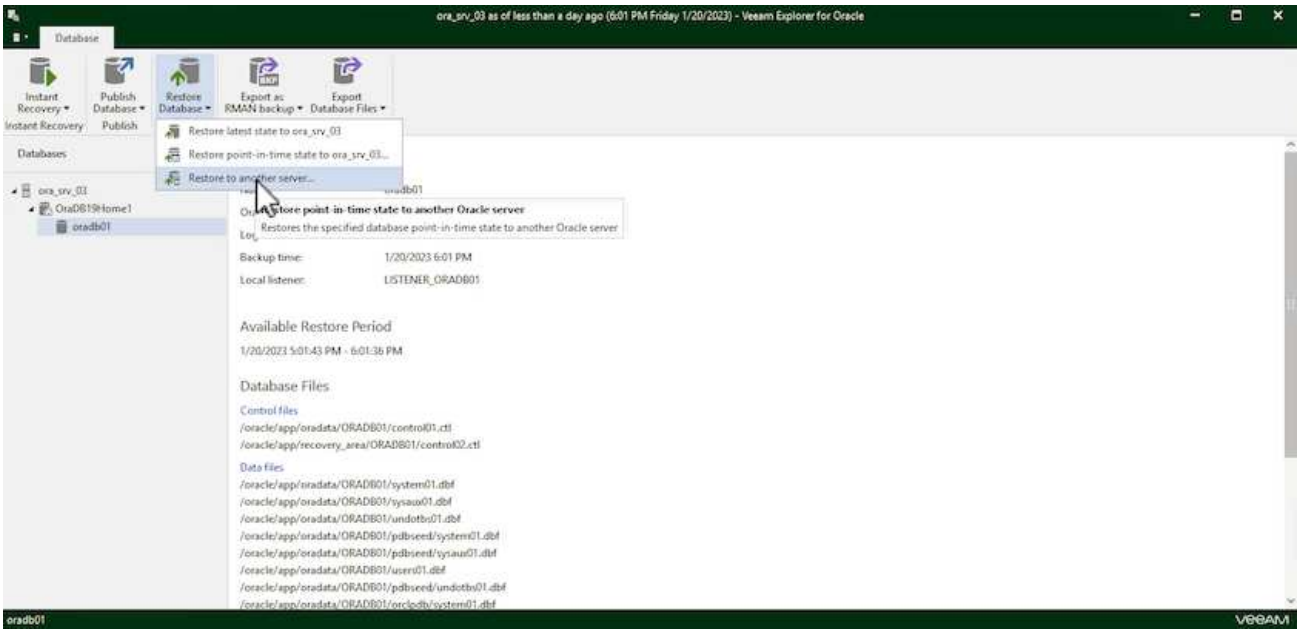
2. Oracle データベース復元ウィザードで、リストから復元ポイントを選択し、「次へ」をクリックします。



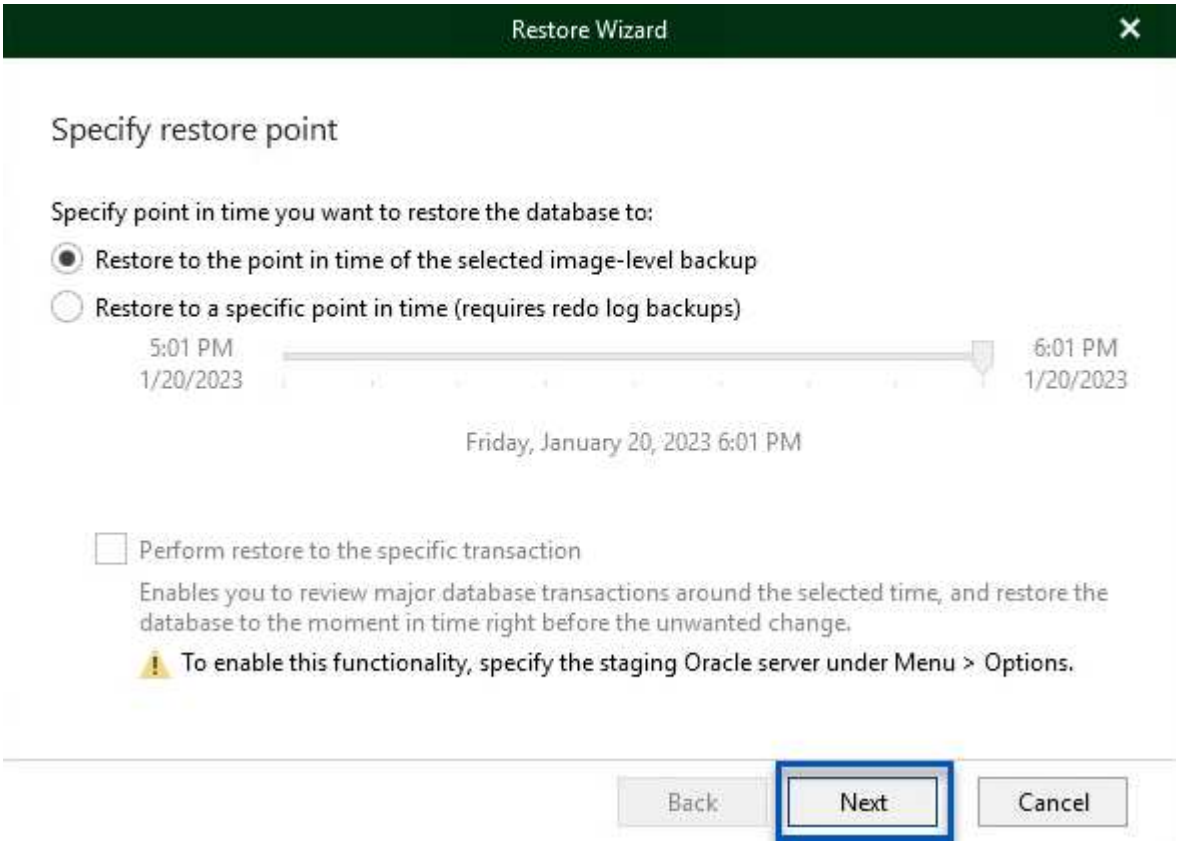
3. 必要に応じて*復元理由*を入力し、[概要] ページで 参照 ボタンをクリックして Veeam Explorer for Oracle を起動します。



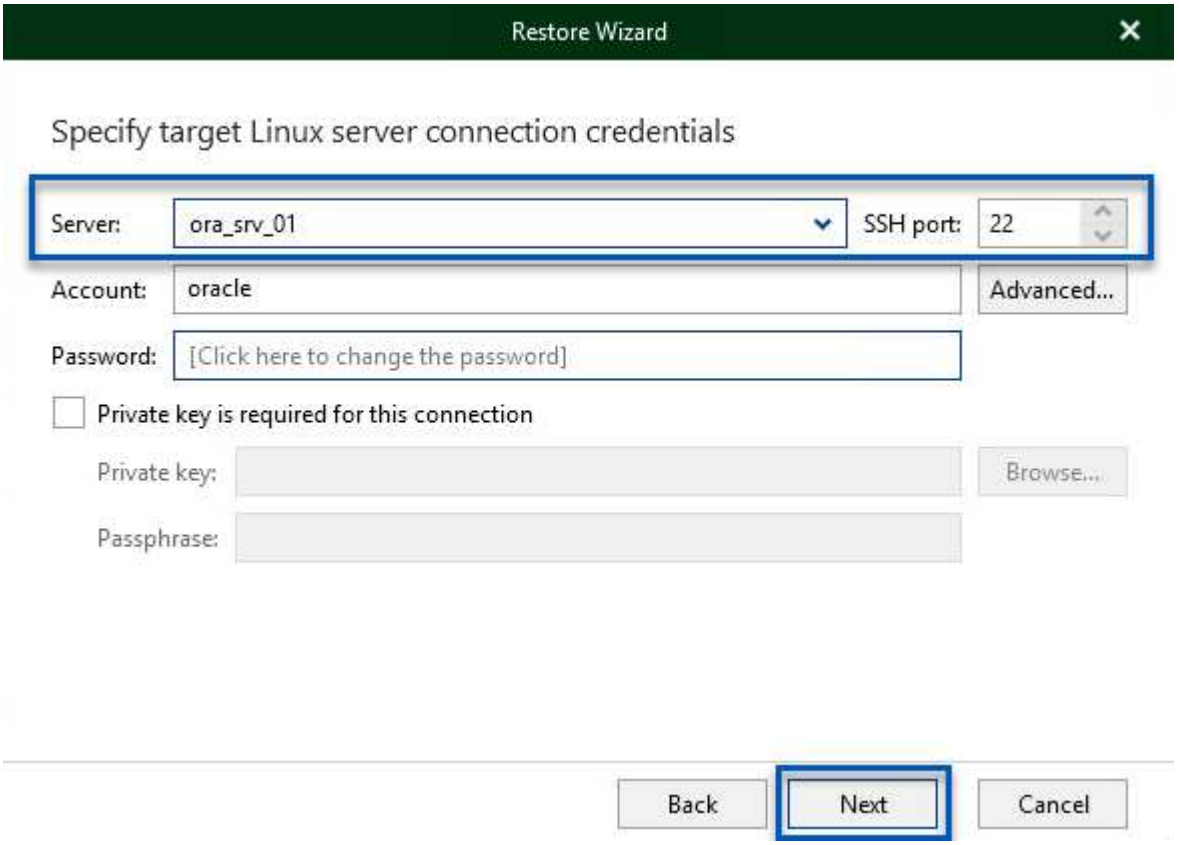
4. Veeam Explorer でデータベース インスタンスのリストを展開し、復元するデータベースをクリックして、上部の データベースの復元 ドロップダウン メニューから 別のサーバーに復元... を選択します。



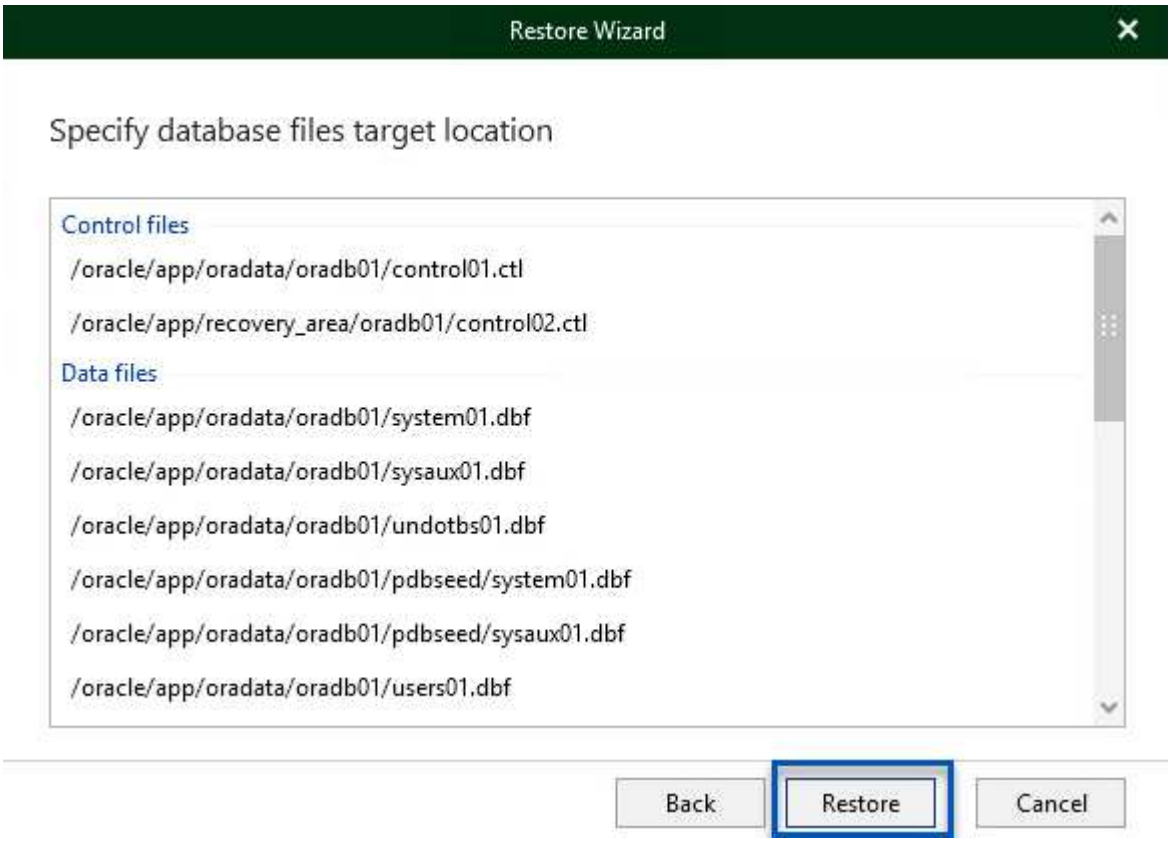
5. 復元ウィザードで、復元する復元ポイントを指定し、「次へ」をクリックします。



6. データベースを復元するターゲット サーバーとアカウント資格情報を指定して、[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、[復元] ボタンをクリックして復元プロセスを開始します。

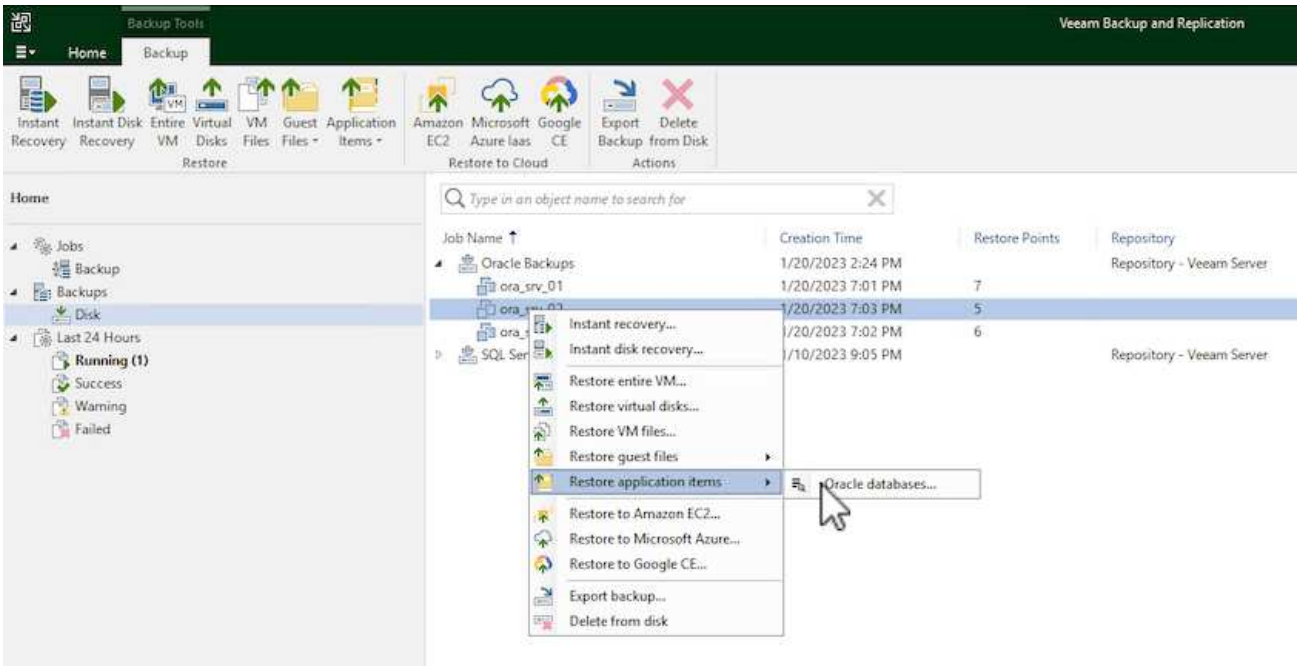


8. データベースのリカバリが完了したら、Oracle データベースがサーバー上で正常に起動していることを確認します。

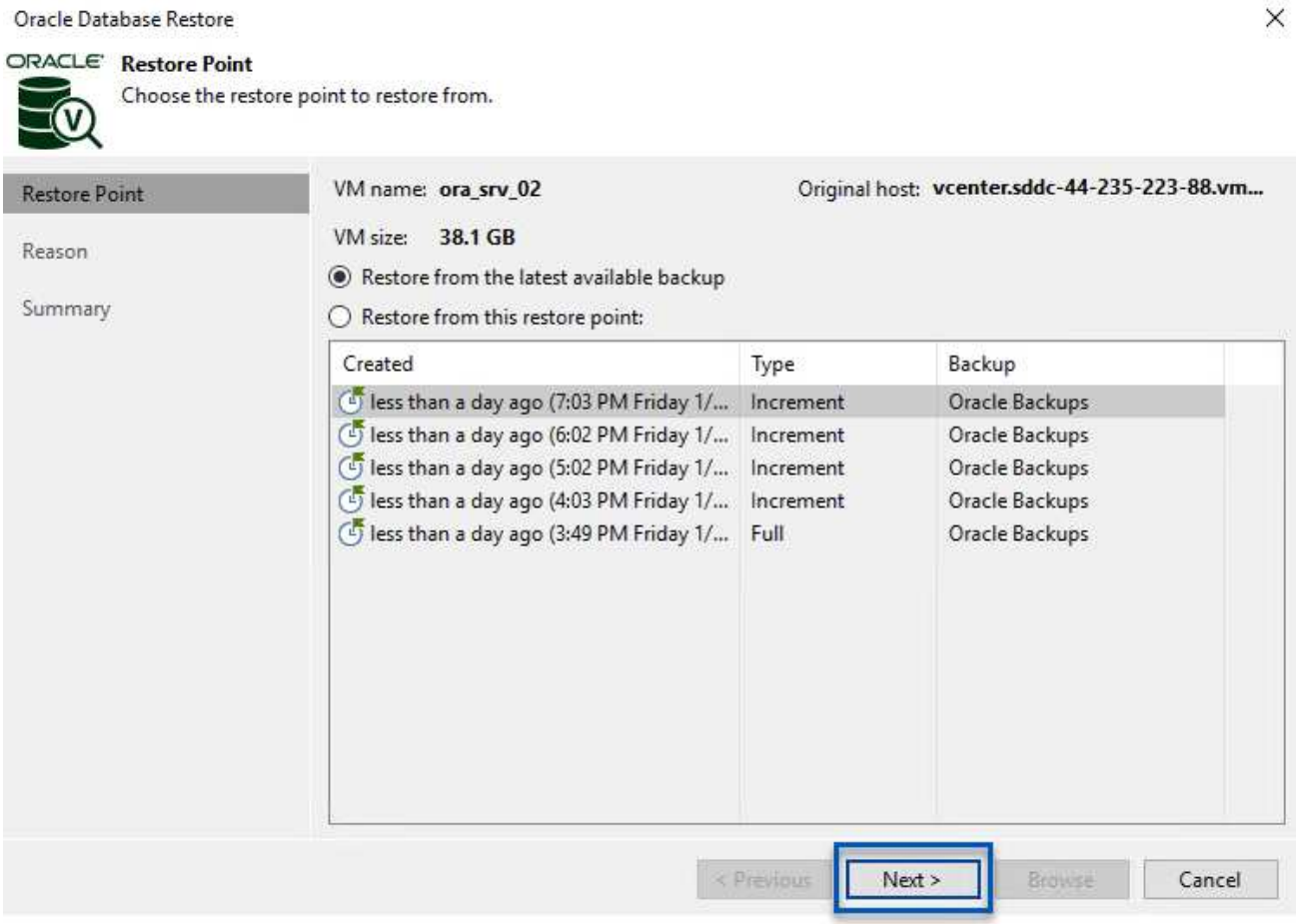
▼ **Oracle**データベースを代替サーバーに公開する

このセクションでは、完全な復元を実行せずに高速アクセスを実現するために、データベースを代替サーバーに公開します。

1. Veeam Backup and Replication コンソールで、Oracle バックアップのリストに移動し、サーバー上で右クリックして アプリケーション項目の復元 を選択し、次に **Oracle** データベース... を選択します。

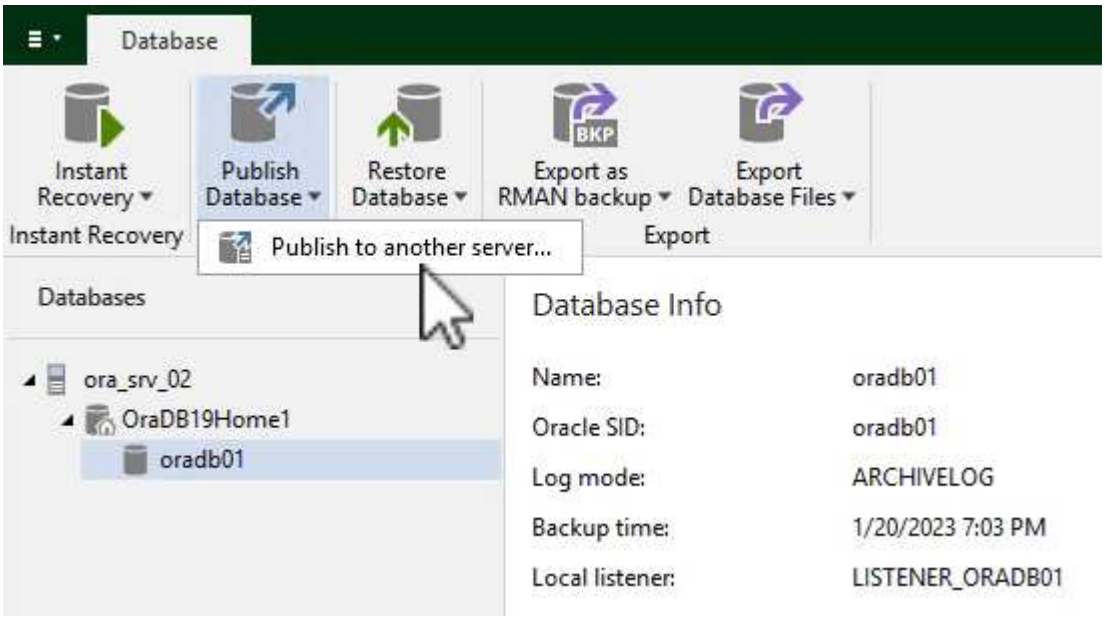


2. Oracle データベース復元ウィザードで、リストから復元ポイントを選択し、「次へ」をクリックします。

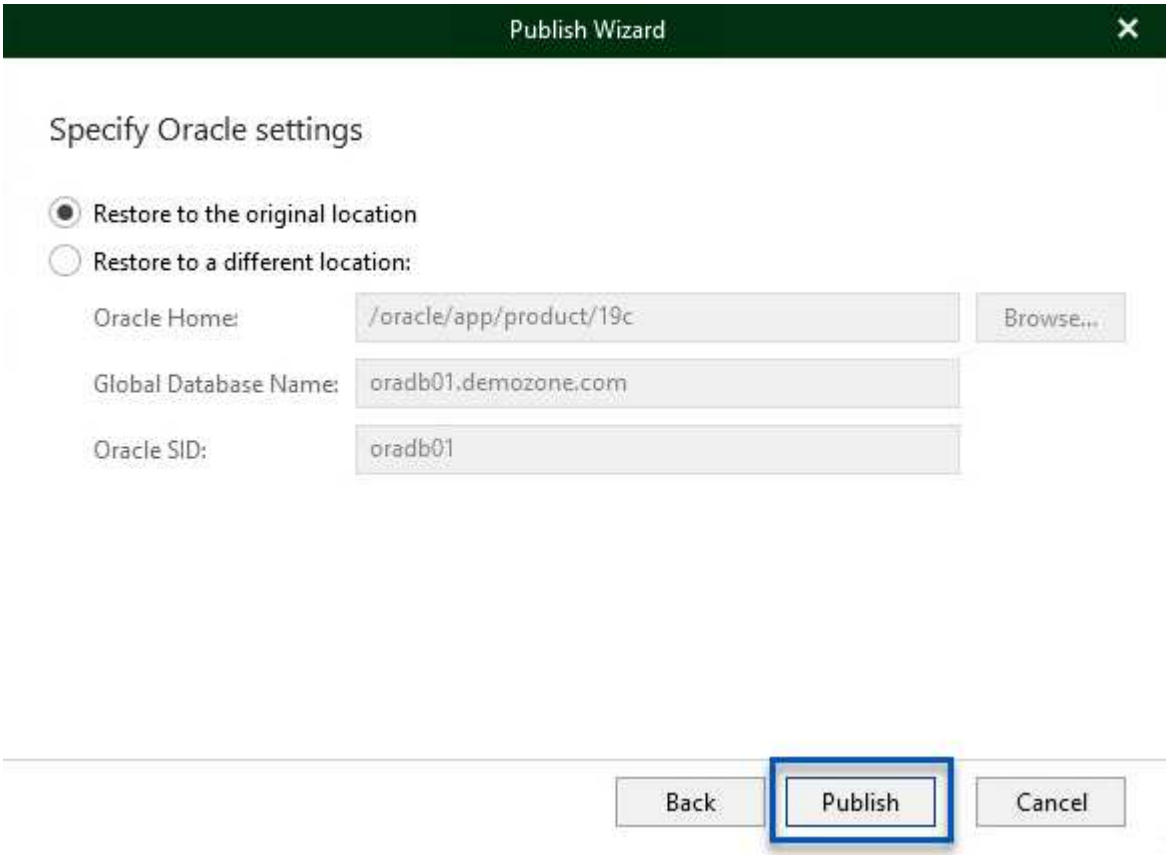


3. 必要に応じて*復元理由*を入力し、[概要] ページで 参照 ボタンをクリックして Veeam Explorer for Oracle を起動します。

4. Veeam Explorer でデータベース インスタンスのリストを展開し、復元するデータベースをクリックして、上部の データベースの公開 ドロップダウン メニューから 別のサーバーに公開... を選択します。



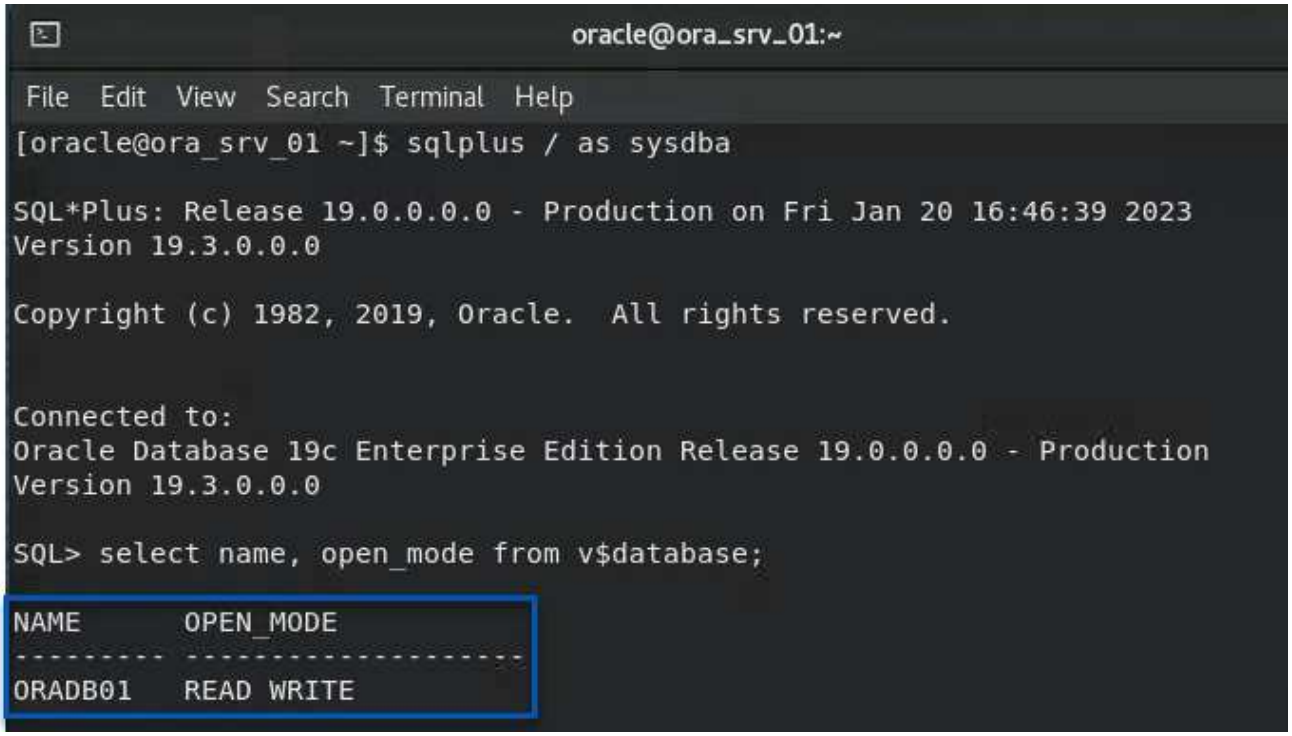
5. 公開ウィザードで、データベースを公開する復元ポイントを指定し、[次へ] をクリックします。
6. 最後に、ターゲットの Linux ファイル システムの場所を指定し、[公開] をクリックして復元プロセスを開始します。



7. 公開が完了したら、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中であ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。 VMware Cloud を利用してビジネスの継続性を確保し、サイバー脅威やデータ損失から保護する企業にとって、安全なデータ保護ソリューションは不可欠です。信頼性が高く堅牢なデータ保護ソリューションを選択することで、企業は重要なデータがどのような状況でも安全に保護されていると確信できます。

このドキュメントで紹介するユースケースは、 NetApp、VMware、および Veeam 間の統合を強調する実証済みのデータ保護テクノロジに重点を置いています。 FSx ONTAP は、AWS の VMware Cloud の補足 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およびアプリケーション データに使用されます。 Veeam Backup & Replication は、企業のバックアップおよびリカバリ 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ソリューションです。 Veeam は、FSx ONTAPでホストされる iSCSI バックアップ ターゲット ボリュームと組み合わせて使用され、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ソリューションを提供します。

追加情報

このソリューションで紹介されているテクノロジーの詳細については、次の追加情報を参照してください。

- "FSx ONTAPユーザーガイド"
- "Veeamヘルプセンター技術ドキュメント"
- "VMware Cloud on AWS サポート。考慮事項と制限事項"

TR-4955: FSx ONTAPと VMC を使用した災害復旧 (AWS VMware Cloud)

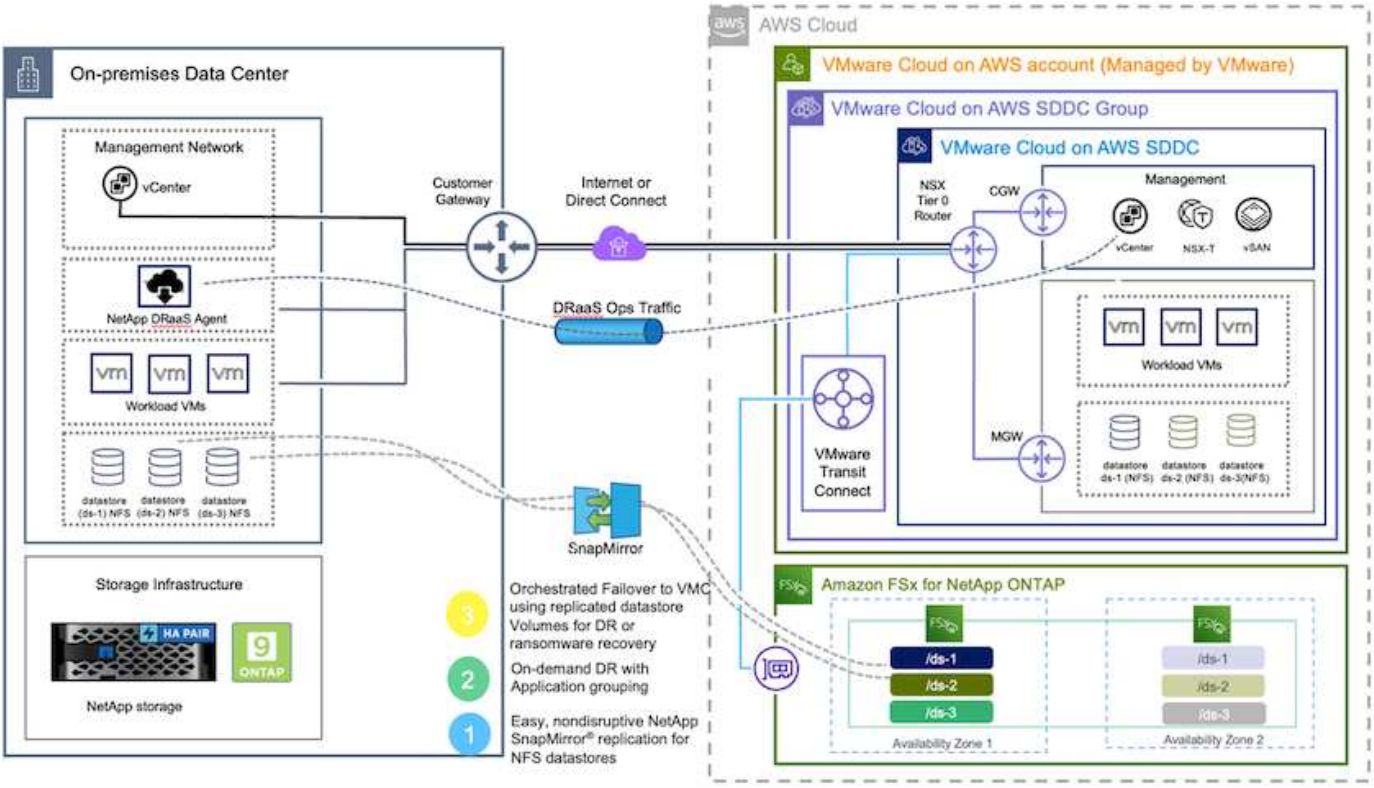
ディザスタ リカバリ オーケストレーター (DRO、UI 付きのスクリプト ソリューション) を使用すると、オンプレミスから FSx ONTAPに複製されたワークロードをシームレスにリカバリできます。 DROは、 SnapMirrorレベルからVMCへのVM登録、そしてNSX-T上のネットワークマッピングまで、リカバリを自動化します。この機能はすべてのVMC環境に含まれています。

ニヤズ・モハメド、 NetApp

概要

クラウドへの災害復旧は、サイトの停止やデータ破損イベント (ランサムウェアなど) からワークロードを保護する、回復力がありコスト効率に優れた方法です。 NetApp SnapMirrorテクノロジーを使用すると、オンプレミスの VMware ワークロードを AWS で実行されている FSx ONTAPに複製できます。

ディザスタ リカバリ オーケストレーター (DRO、UI 付きのスクリプト ソリューション) を使用すると、オンプレミスから FSx ONTAP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。 DROは、 SnapMirrorレベルからVMCへのVM登録、そしてNSX-T上のネットワークマッピングまで、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。



開始

VMware Cloud on AWS の導入と構成

"VMware Cloud on AWS"AWS エコシステム内の VMware ベースのワークロードにクラウドネイティブのエクスペリエンスを提供します。各 VMware ソフトウェア定義データセンター (SDDC) は Amazon Virtual Private Cloud (VPC) で実行され、完全な VMware スタック (vCenter Server を含む)、NSX-T ソフトウェア定義ネットワーク、vSAN ソフトウェア定義ストレージ、およびワークロードにコンピューティング リソースとスト

レージ リソースを提供する 1 つ以上の ESXi ホストを提供します。 AWS上でVMC環境を構成するには、次の手順に従ってください。"リンク" 。パイロットライト クラスターは DR 目的にも使用できます。

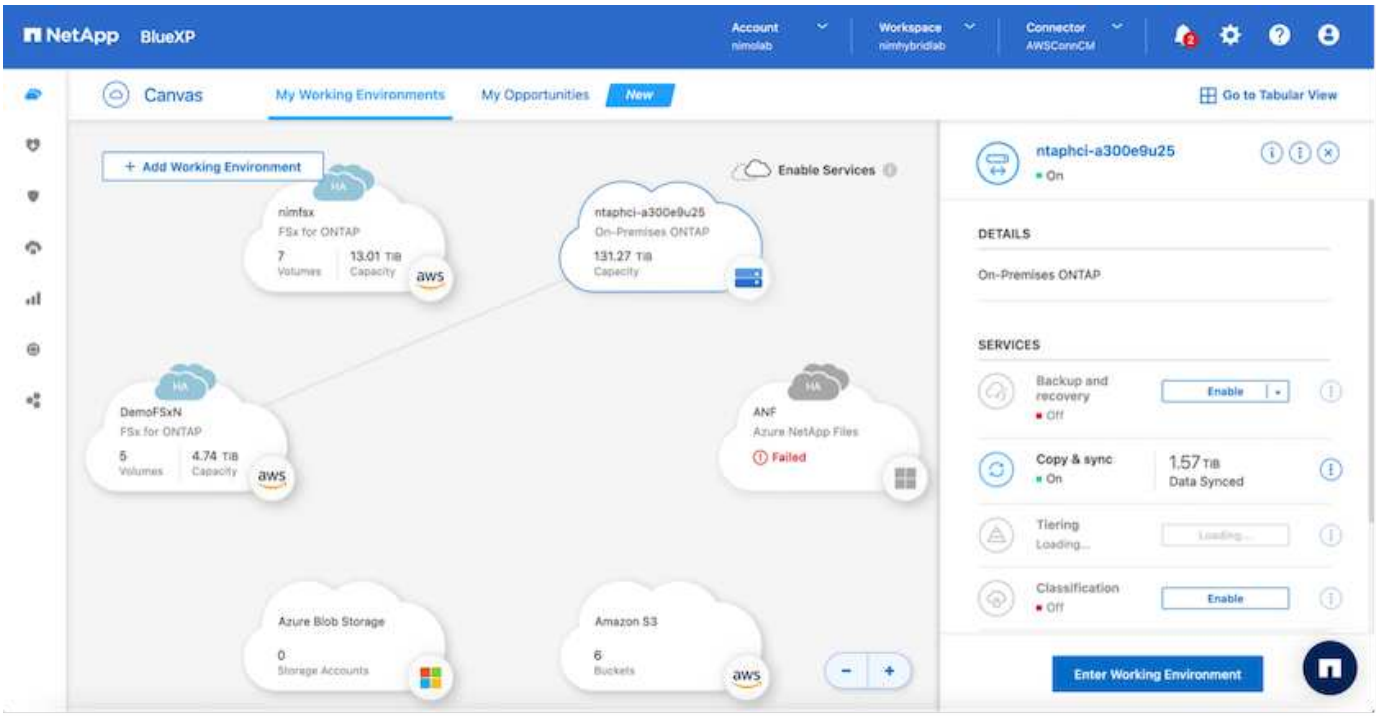
最初のリリースでは、DRO は既存のパイロットライト クラスターをサポートします。オンデマンド SDDC 作成は、今後のリリースで利用可能になります。

FSx ONTAP のプロビジョニングと構成

Amazon FSx ONTAP は、人気のNetApp ONTAPファイルシステム上に構築された、信頼性が高く、スケーラブルで、高性能かつ機能豊富なファイルストレージを提供するフルマネージドサービスです。この手順に従ってください"リンク"FSx ONTAP をプロビジョニングおよび構成します。

SnapMirrorをFSx ONTAPに導入して設定する

次のステップは、NetApp Consoleを使用してプロビジョニングされたAWS上のFSx ONTAPインスタンスを検出し、目的のデータストアボリュームをオンプレミス環境からFSx ONTAPへ、適切な頻度とNetApp Snapshotコピーの保持期間でレプリケートすることです：



DROを設定するには、このリンクの手順に従ってください。また、このリンクに従ってNetApp ONTAP CLIを使用して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、事前に作成する必要があります。

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で 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

- ソースおよびターゲットの 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ます。
- DNS 名を使用している場合は、DNS 解決を実施する必要があります。それ以外の場合は、vCenter およびストレージ システムに IP アドレスを使用する必要があります。
- ルート権限を持つユーザーを作成します。 EC2 インスタンスで sudo を使用することもできます。

OSの要件

- Ubuntu 20.04 (LTS)、最低 2GB および 4 つの vCPU
- 指定されたエージェント VM 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
  - Docker-compose
  - Jq

権限を変更する `docker.sock`： `sudo chmod 666 /var/run/docker.sock` 。

その `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する

1. 指定され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
```

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、デプロイメント スクリプトを実行して、ホスト IP (例: 10.10.10.10) を入力します。

```
tar xvf DRO-prereq.tar
```

3. ディレクトリに移動し、次のようにデプロイ スクリプトを実行します。

```
sudo sh deploy.sh
```

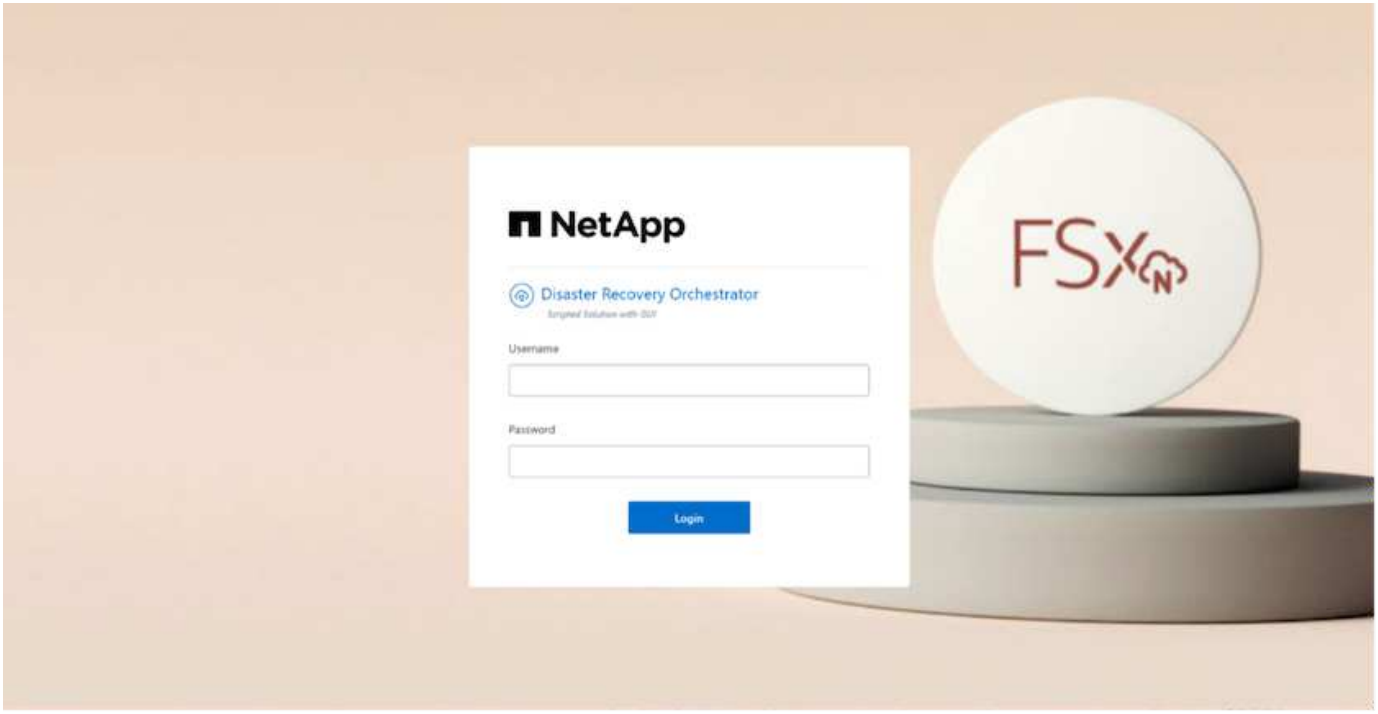
4. 次の方法で UI にアクセスします。

```
https://<host-ip-address>
```

次のデフォルトの資格情報を使用します。

```
Username: admin
Password: admin
```

パスワードは「パスワードの変更」オプションを使用して変更できます。



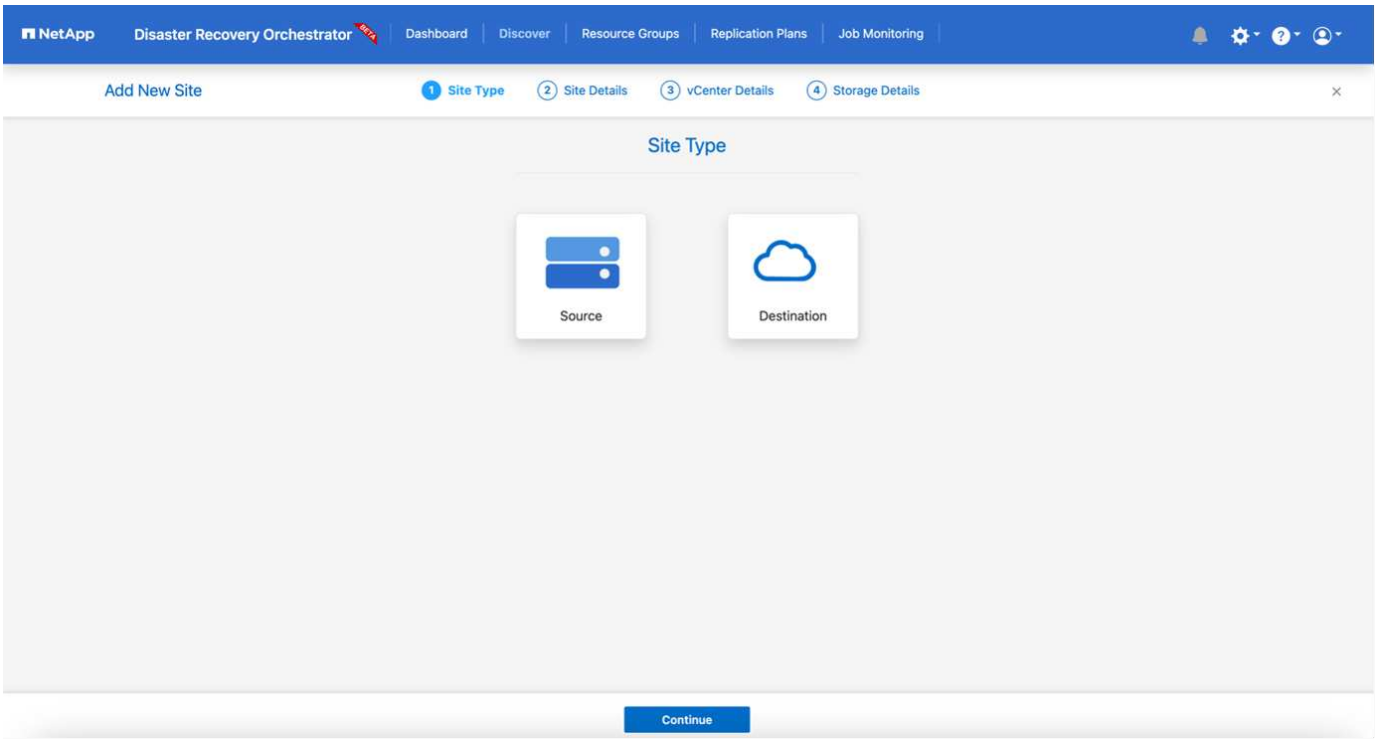
DRO構成

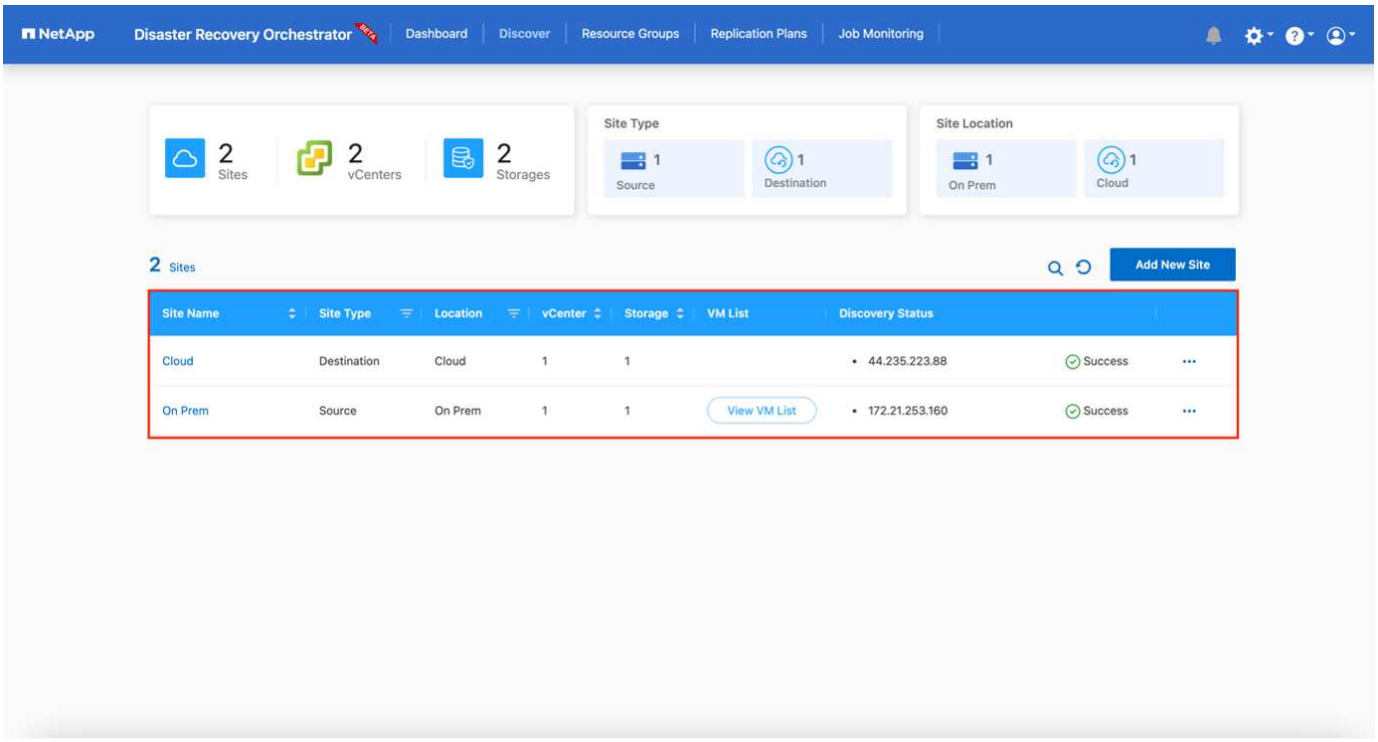
FSx ONTAPと VMC が適切に構成されたら、FSx ONTAP上の読み取り専用SnapMirrorコピーを使用してオンプレミスのワークロードを VMC に自動的にリカバリするように DRO の構成を開始できます。

NetApp、DRO エージェントがオンプレミスのコンポーネントだけでなく、FSx ONTAPや VMC リソースともネットワークを介して通信できるように、DRO エージェントを AWS に導入し、さらに FSx ONTAPが導入されているのと同じ VPC (ピア接続も可能) にも導入することを推奨しています。

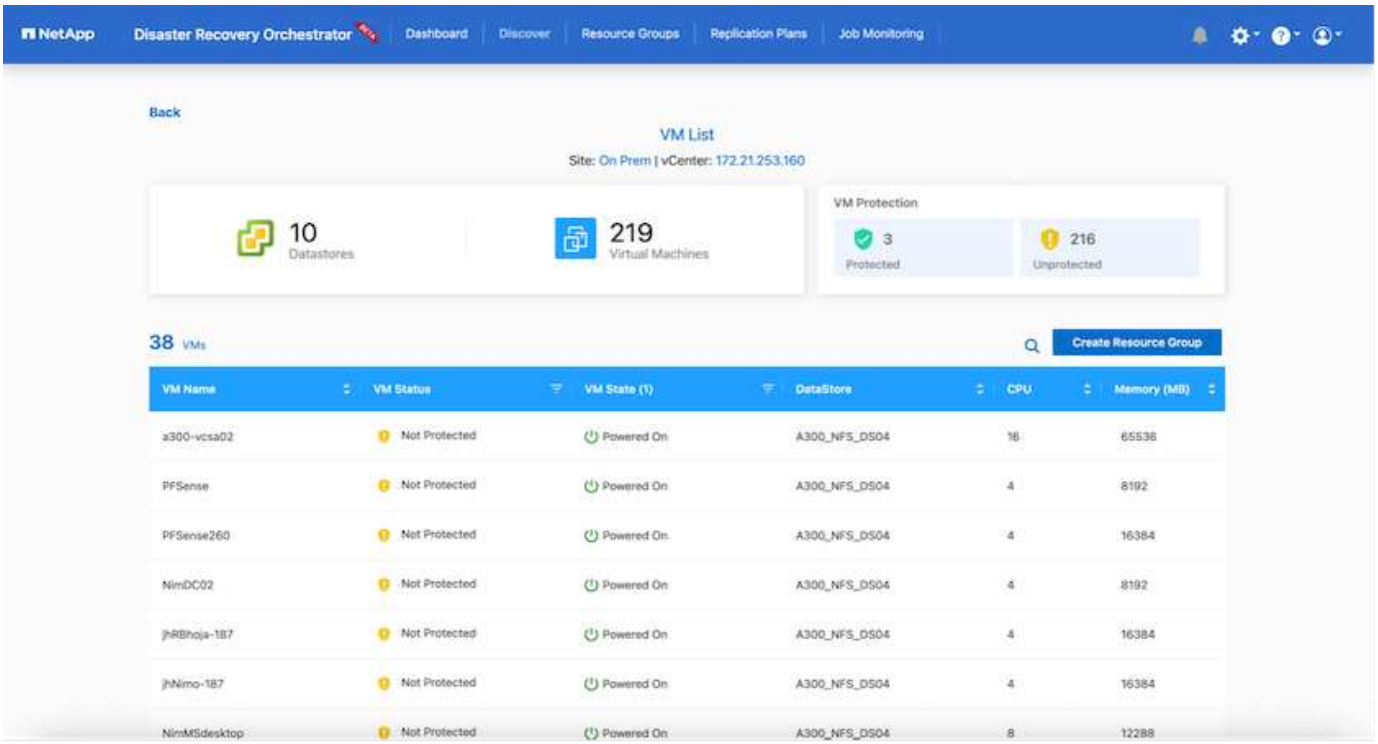
最初のステップは、オンプレミスとクラウドのリソース (vCenter とストレージの両方) を検出して DRO に追加することです。サポートされているブラウザで DRO を開き、デフォルトのユーザー名とパスワード (admin/admin) を使用して、サイトを追加します。検出オプションを使用してサイトを追加することもできます。次のプラットフォームを追加します。

- 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 ONTAP





追加されると、DRO は自動検出を実行し、ソース ストレージから FSx ONTAPに対応するSnapMirrorレプリカを持つ VM を表示します。 DRO は、VM で使用されるネットワークとポートグループを自動的に検出し、それらを入力します。



次のステップは、必要な VM を機能グループにグループ化し、リソース グループとして機能するようにすることです。

リソースのグループ化

プラットフォームを追加したら、回復する VM をリソース グループにグループ化できます。 DRO リソース グループを使用すると、依存する VM のセットを、ブート順序、ブート遅延、および回復時に実行できる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。

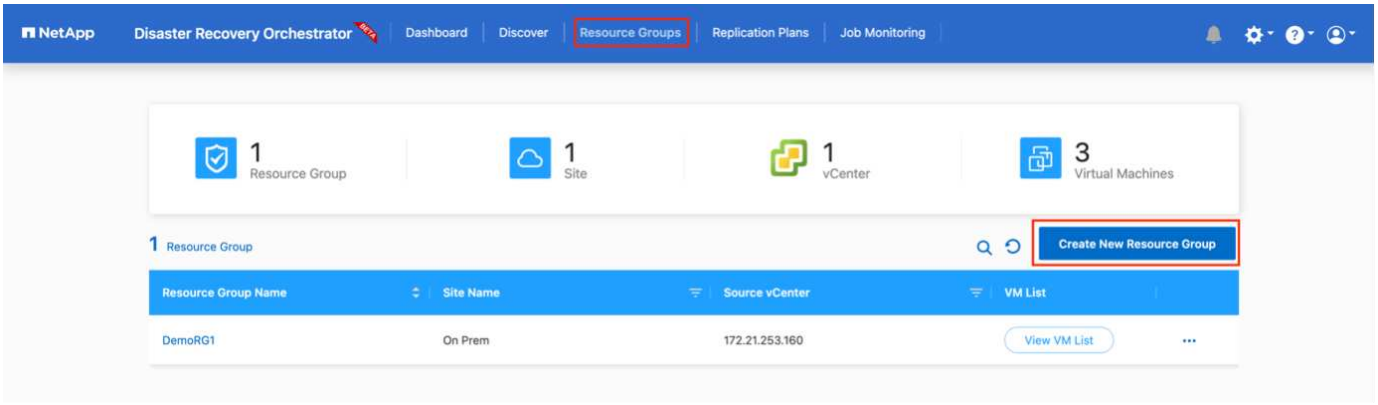
リソース グループの作成を開始するには、次の手順を実行します。

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 の下で、ドロップダウンからソース サイトを選択し、作成 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、その優先順位を設定することで、電源オン シーケンスの順序を設定します。すべての VM のデフォルト値は 3 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。

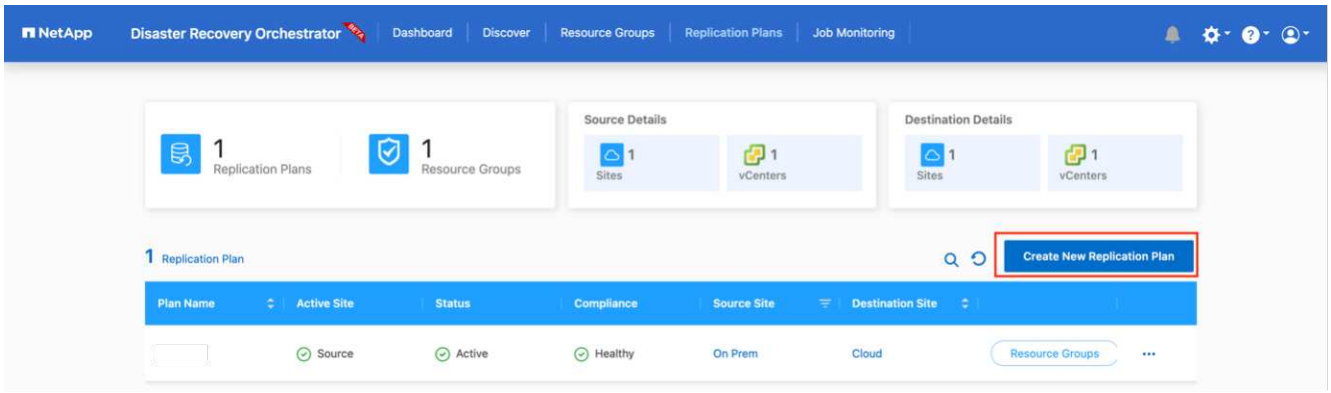


レプリケーションプラン

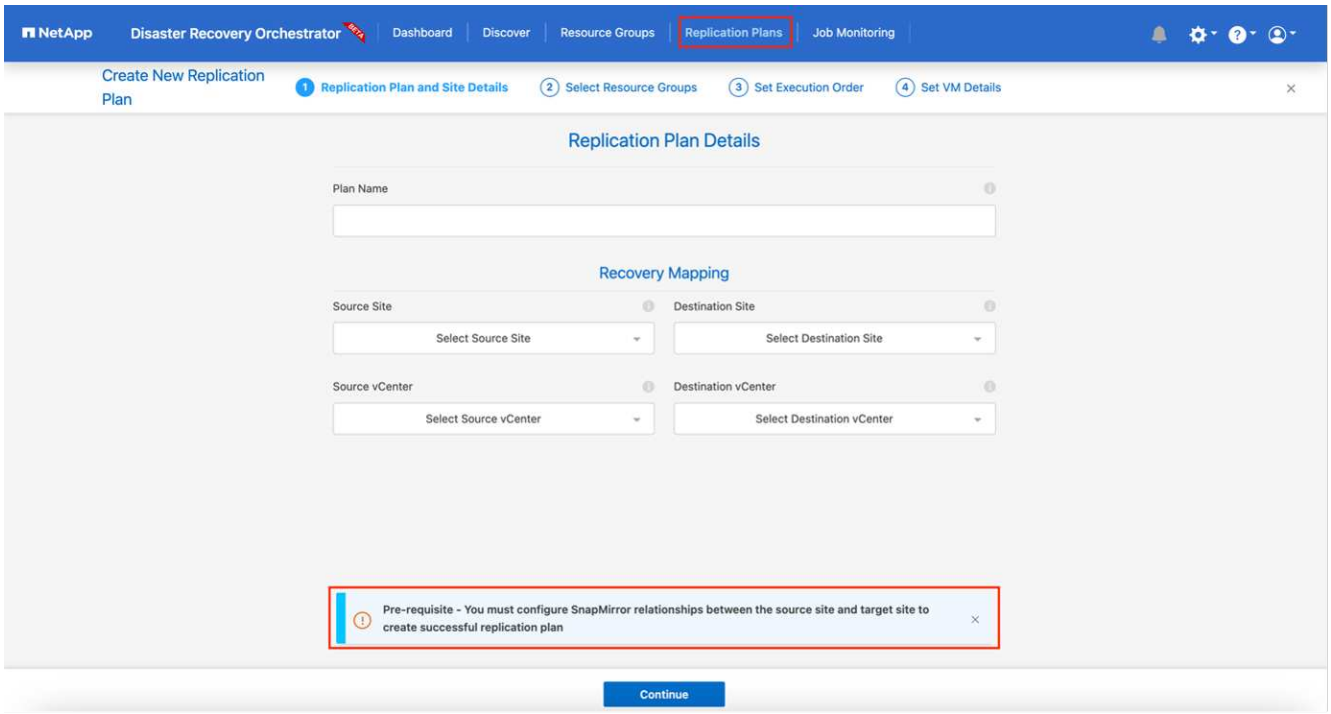
災害が発生した場合にアプリケーションを回復するための計画が必要です。ドロップダウンからソースとターゲットの vCenter プラットフォームを選択し、このプランに含めるリソース グループと、アプリケーションを復元してパワーオンする方法のグループ化 (たとえば、ドメイン コントローラ、次に Tier 1、次に Tier 2 など) を選択します。このような計画は、青写真と呼ばれることもあります。リカバリ プランを定義するには、[レプリケーション プラン] タブに移動し、[新しいレプリケーション プラン] をクリックします。

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。

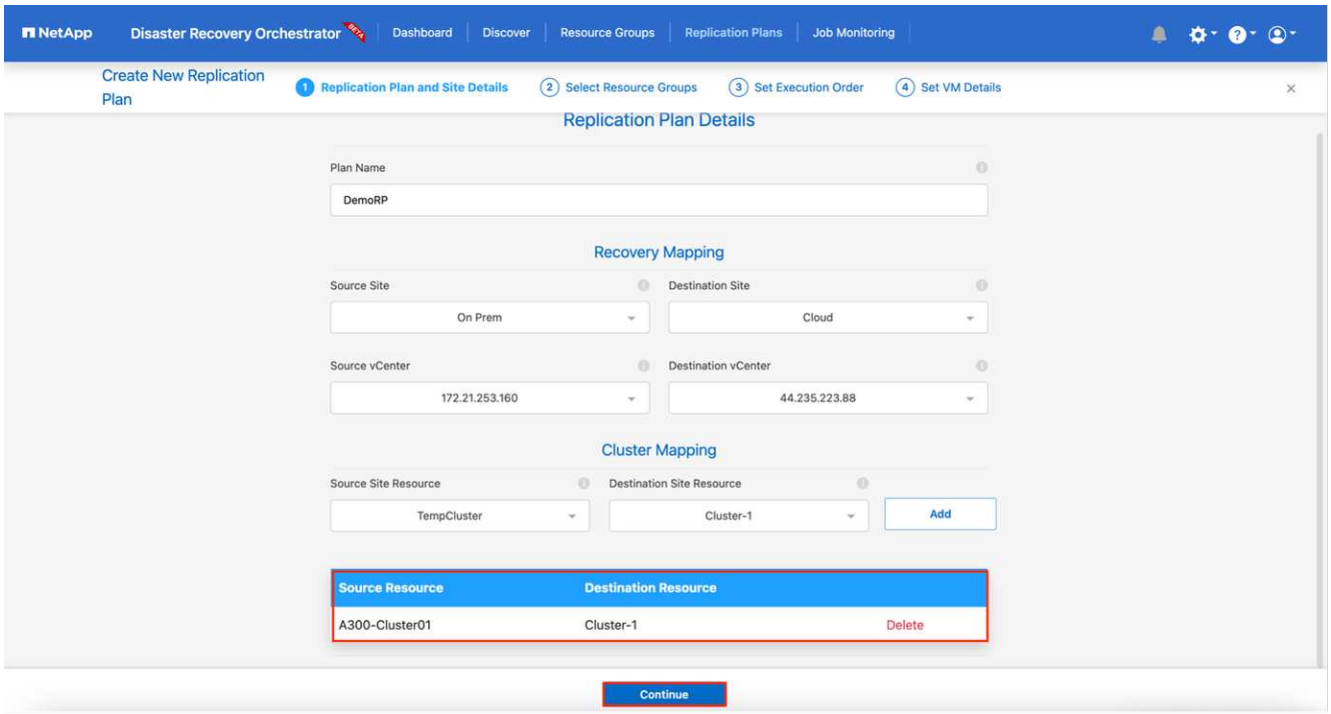
1. *レプリケーション プラン*にアクセスし、*新しいレプリケーション プランの作成*をクリックします。



2. 新しいレプリケーション プラン で、プランの名前を指定し、ソース サイト、関連付けられた vCenter、宛先サイト、および関連付けられた vCenter を選択して、リカバリ マッピングを追加します。

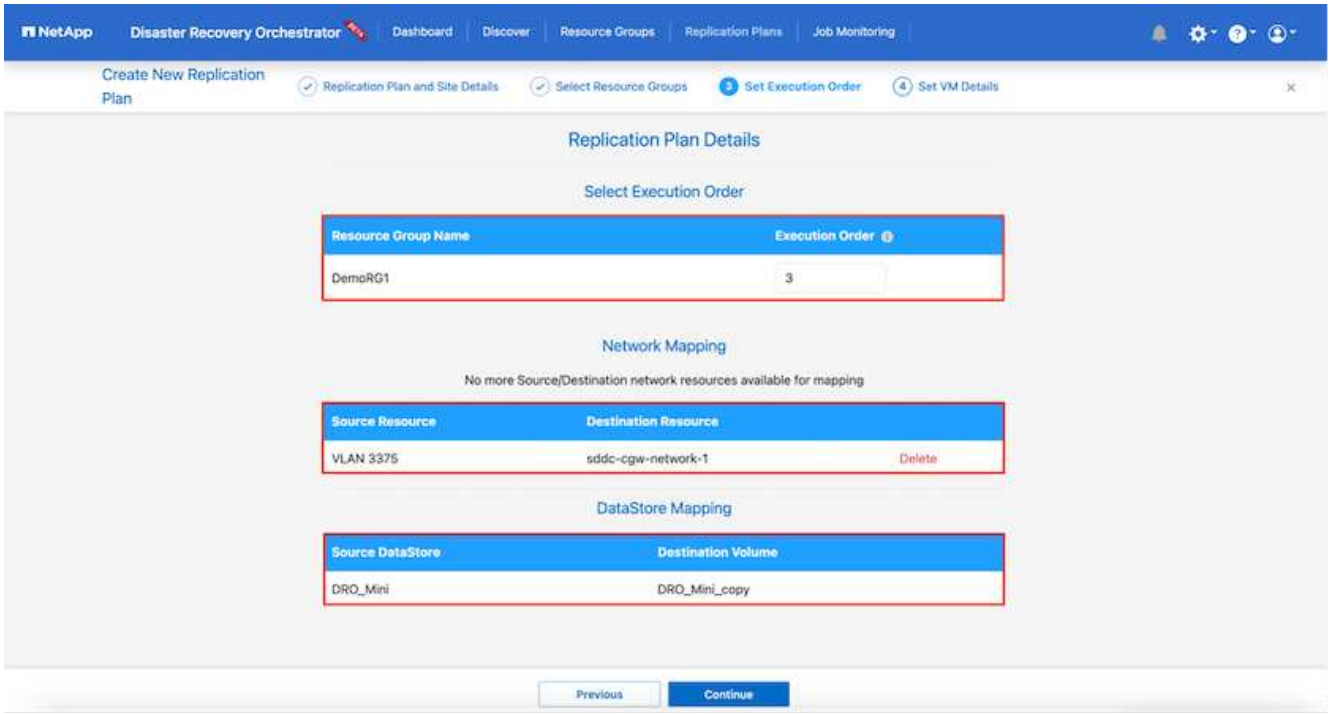


3. リカバリ マッピングが完了したら、クラスター マッピングを選択します。

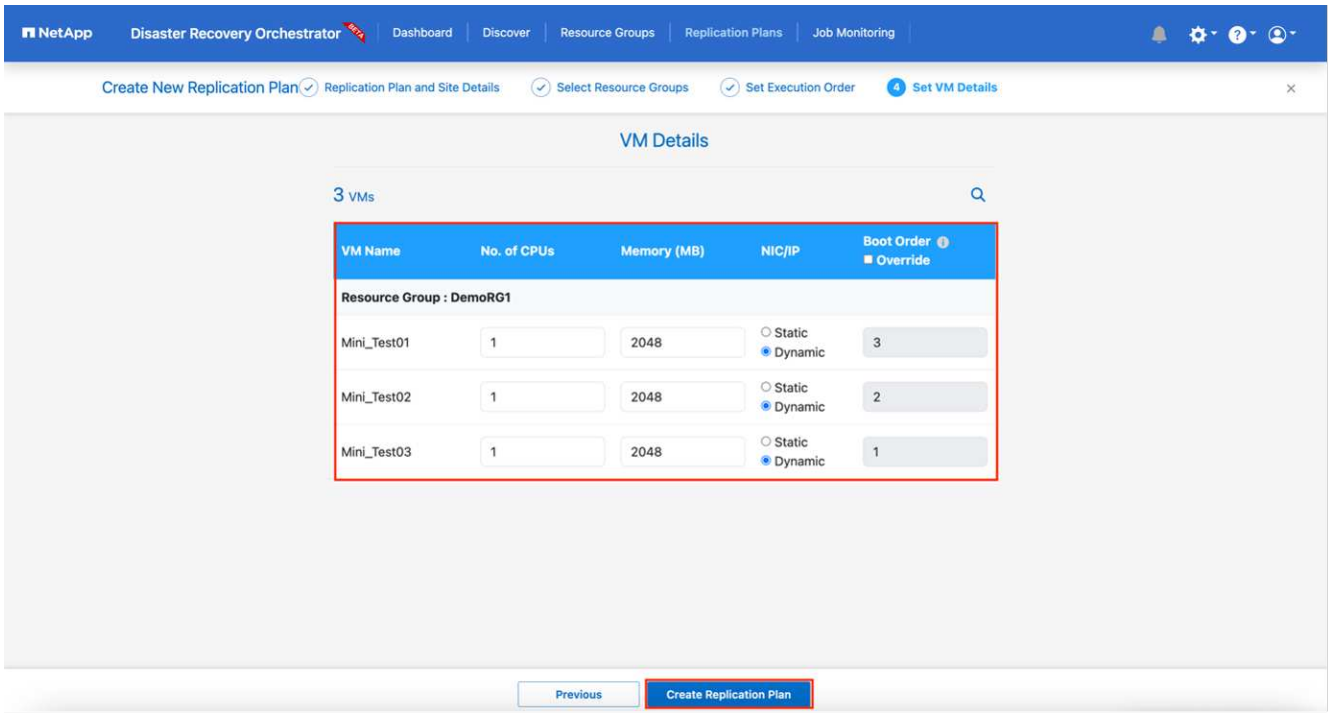


4. *リソース グループの詳細*を選択し、*続行*をクリックします。
5. リソース グループの実行順序を設定します。このオプションを使用すると、複数のリソース グループが存在する場合に操作のシーケンスを選択できます。
6. 完了したら、適切なセグメントへのネットワーク マッピングを選択します。セグメントはすでに VMC 内でプロビジョニングされているはずなので、適切なセグメントを選択して VM をマップします。
7. VM の選択に基づいて、データストア マッピングが自動的に選択されます。

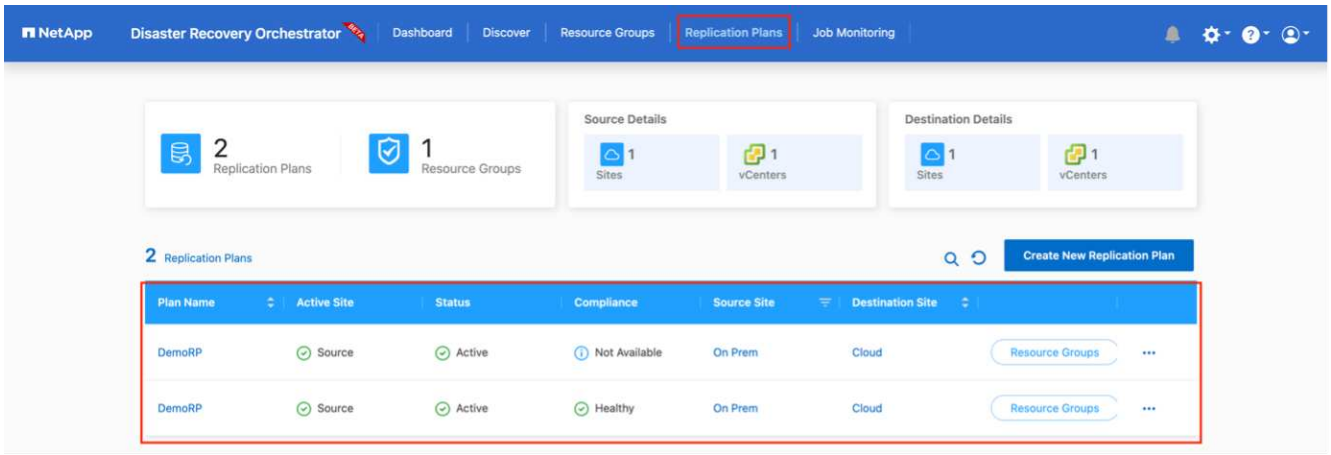
SnapMirrorはボリューム レベルで行われます。したがって、すべての VM がレプリケーション先にレプリケートされます。データストアの一部であるすべての VM を選択してください。選択されていない場合は、レプリケーション プランの一部である VM のみが処理されます。



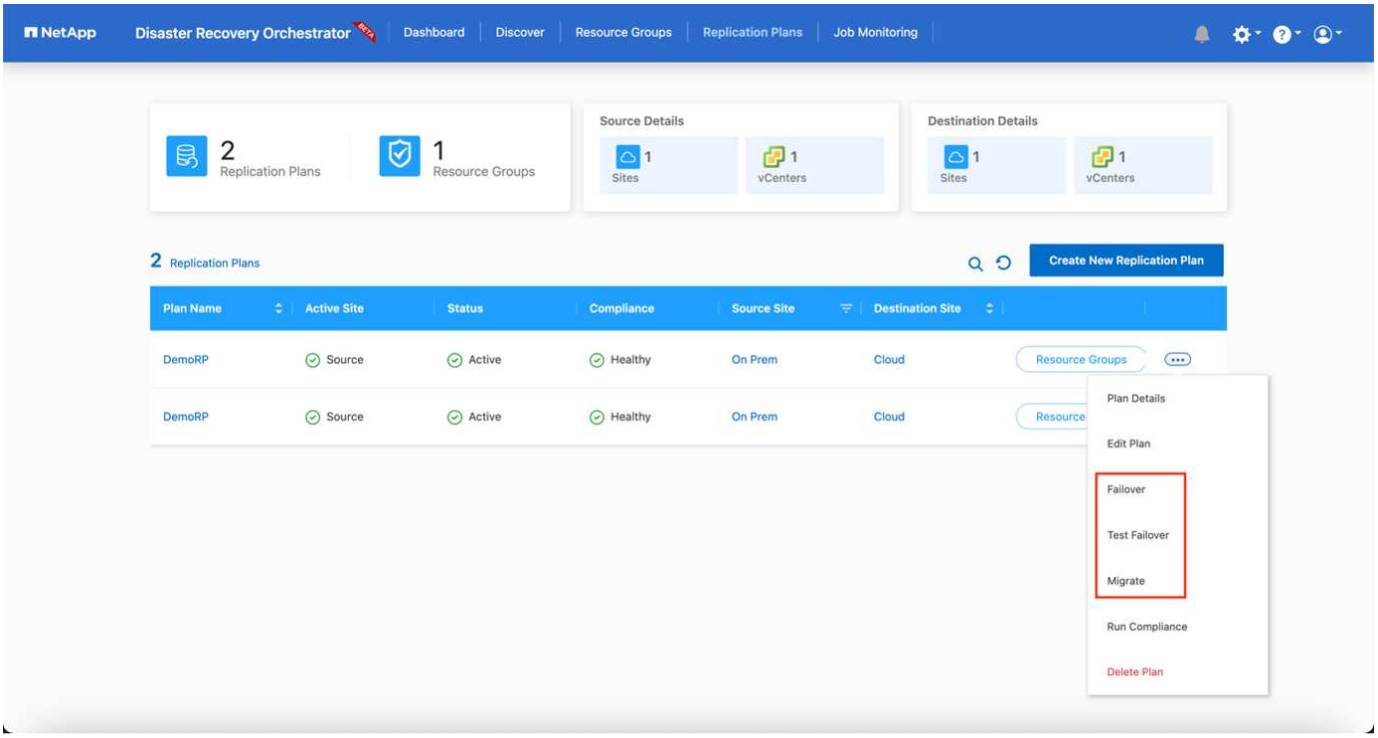
8. VM の詳細では、オプションで VM の CPU および RAM パラメータのサイズを変更できます。これは、大規模な環境を小規模なターゲット クラスターに回復する場合や、1 対 1 の物理 VMware インフラストラクチャをプロビジョニングせずに DR テストを実施する場合に非常に役立ちます。また、リソース グループ全体で選択したすべての VM のブート順序とブート遅延 (秒) を変更することもできます。リソース グループのブート順序の選択時に選択したものから変更が必要な場合、ブート順序を変更するための追加オプションがあります。デフォルトでは、リソース グループの選択時に選択されたブート順序が使用されますが、この段階で変更を実行することもできます。

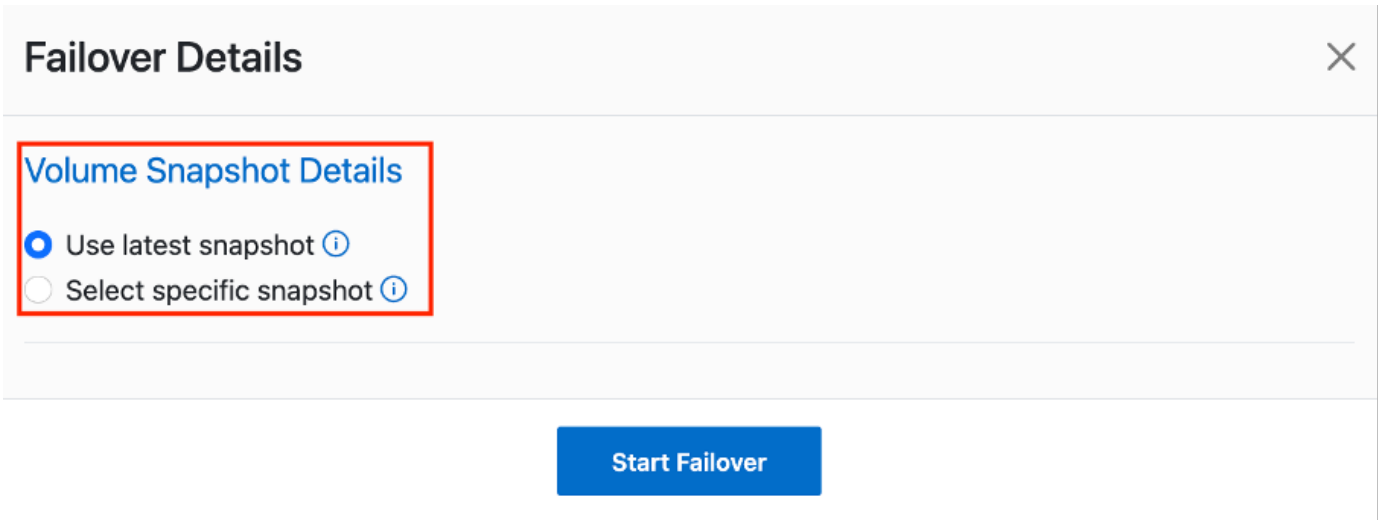


9. *レプリケーション プランの作成*をクリックします。

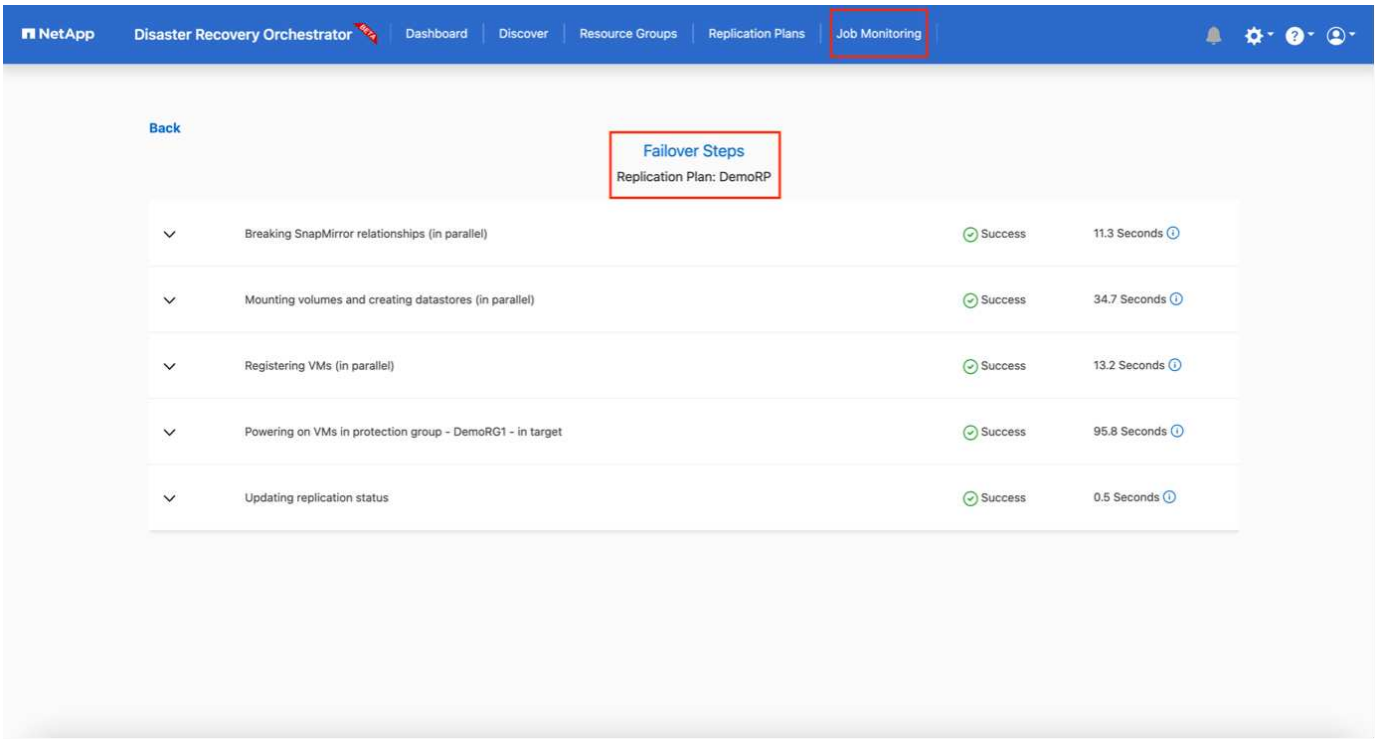


レプリケーション プランが作成された後、要件に応じて、フェールオーバー オプション、テスト フェールオーバー オプション、または移行オプションを実行できます。フェイルオーバーおよびテストフェイルオーバーのオプション中は、最新のSnapMirrorスナップショット コピーが使用されるか、または特定のスナップショット コピーをポイントインタイム スナップショット コピーから選択できます (SnapMirrorの保持ポリシーに従って)。ランサムウェアなどの破損イベントに直面していて、最新のレプリカがすでに侵害されたり暗号化されたりしている場合は、ポイントインタイム オプションが非常に役立ちます。 DRO は利用可能なすべての時点を表示します。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 [フェイルオーバーのテスト] をクリックします。

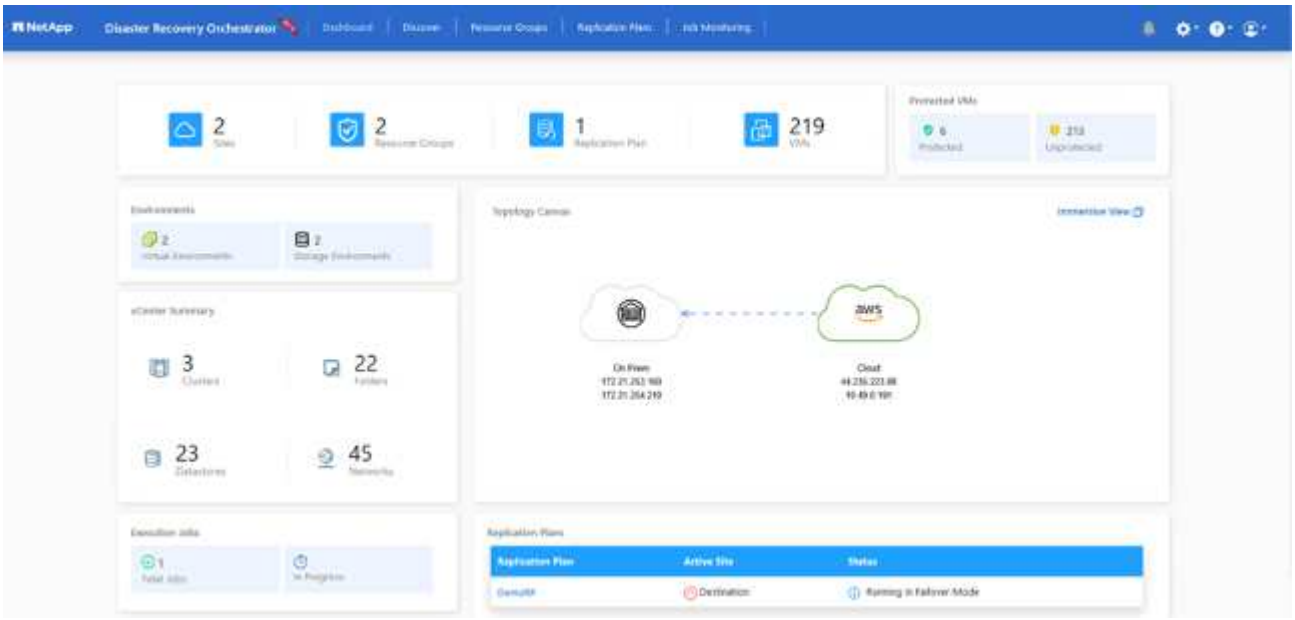




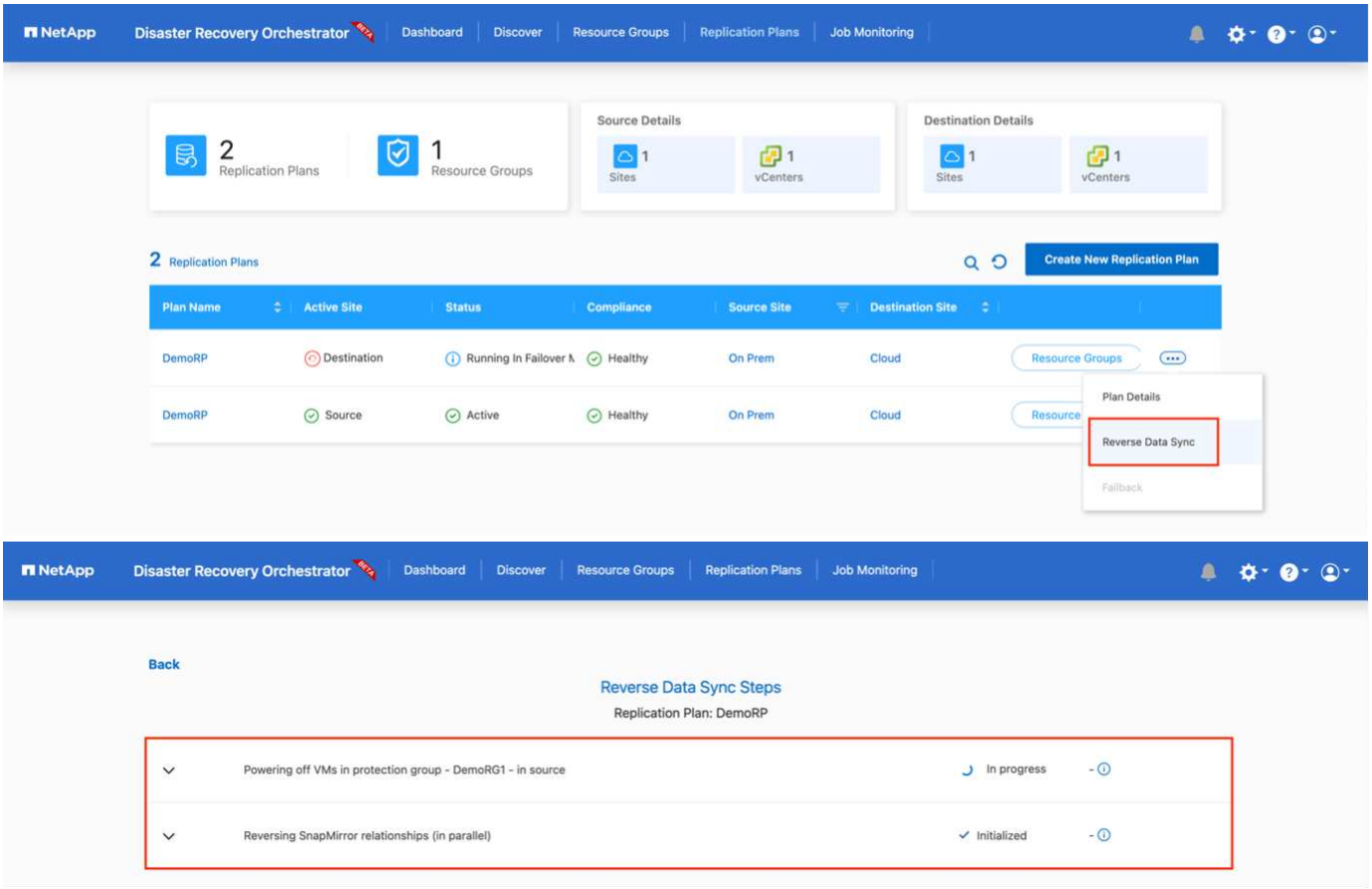
レプリケーション プランはタスク メニューで監視できます。



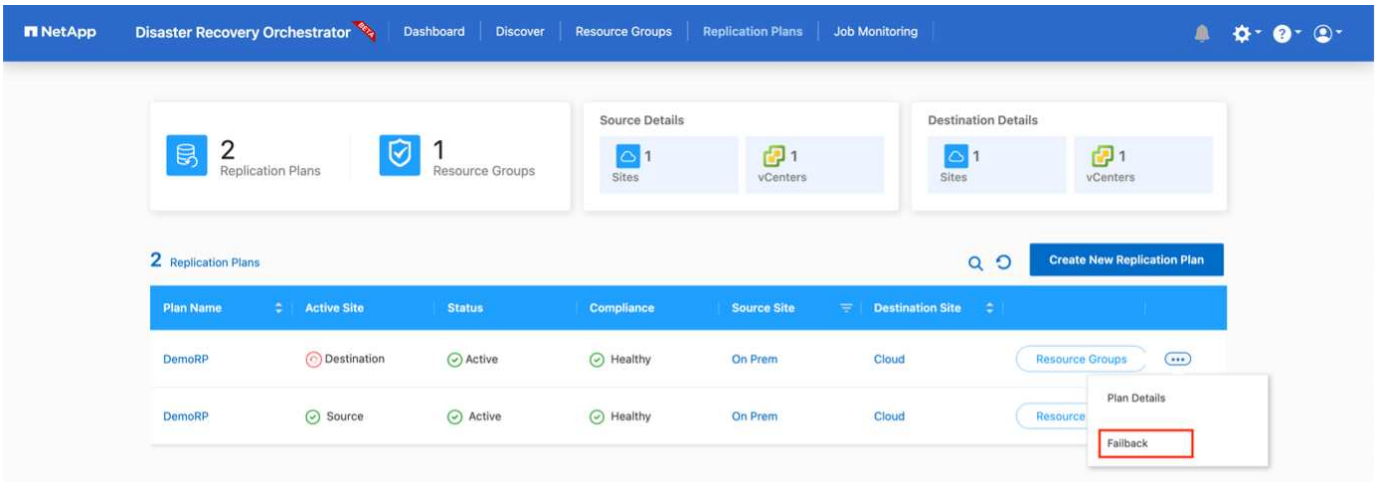
フェイルオーバーがトリガーされると、回復された項目が VMC vCenter (VM、ネットワーク、データストア)に表示されます。デフォルトでは、VM はワークロード フォルダーに回復されます。

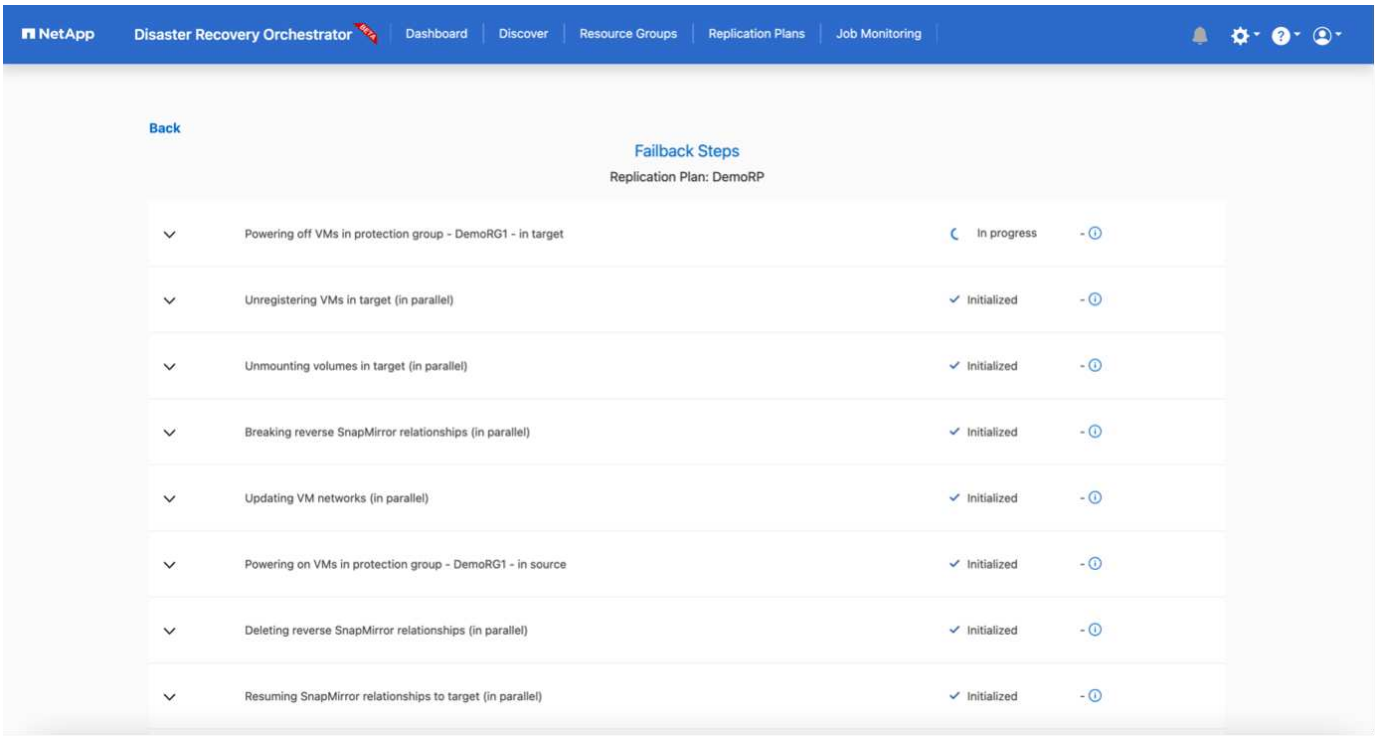


フェイルバックはレプリケーション プラン レベルでトリガーできます。テストフェイルオーバーの場合、ティアダウン オプションを使用して変更をロールバックし、 FlexClone関係を削除できます。フェイルオーバーに関連するフェイルバックは 2 段階のプロセスです。レプリケーション プランを選択し、逆データ同期 を選択します。

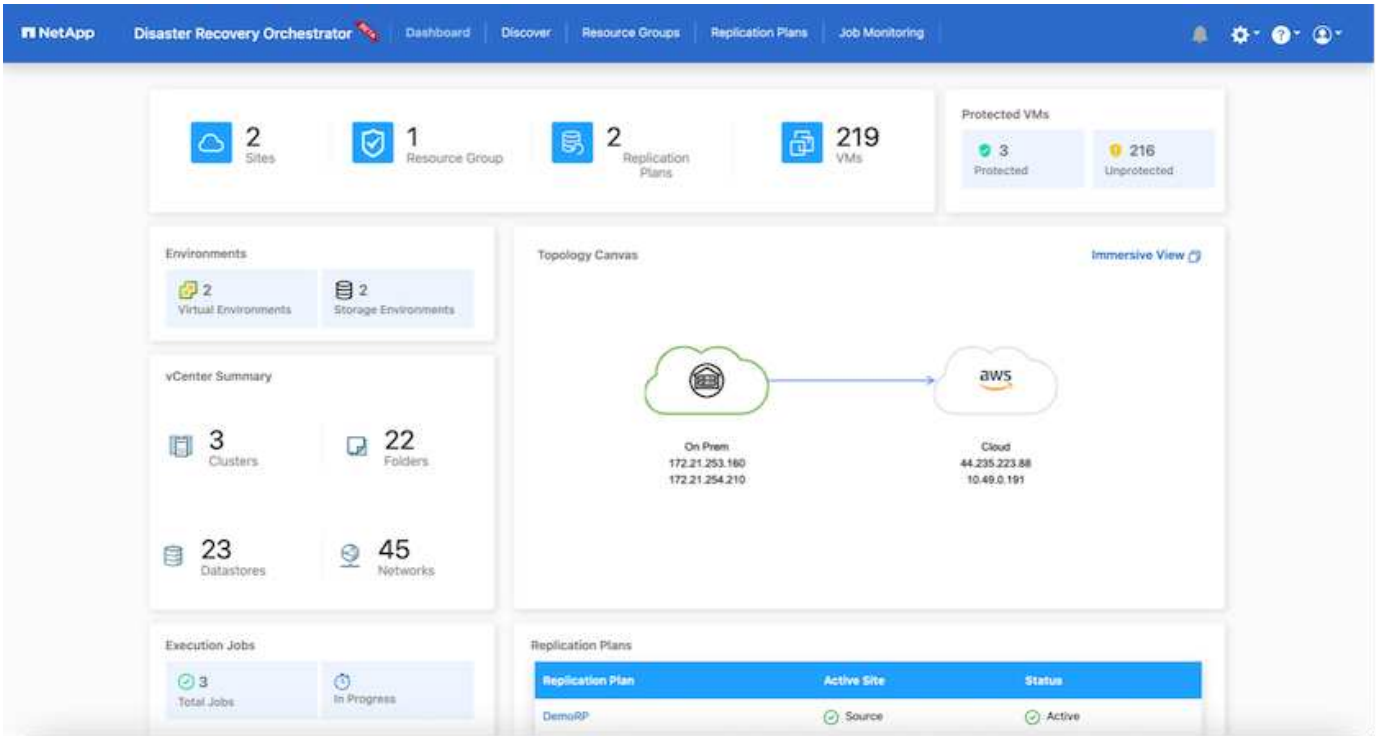


完了したら、フェイルバックをトリガーして元の運用サイトに戻ることができます。





NetApp Console では、（読み書きボリュームとして VMC にマッピングされた）該当ボリュームのレプリケーション ヘルス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 は宛先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 コピーを作成して FlexClone インスタンスを公開します。これにより、FSx ONTAP の追加の物理容量を消費しません。このプロセスにより、ボリュームが変更されないことが保証され、DR テストやトリアージ ワークフロー中もレプリカ ジョブを継続できます。また、このプロセスにより、エラーが発生したり破損データが回復されたりした場合でも、レプリカが破壊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回復

ランサムウェアからの回復は困難な作業になる可能性があります。具体的には、IT 組織にとって、安全な復帰ポイントがどこにあるかを正確に特定することは困難であり、また、それが特定された後、たとえば休眠中のマルウェアや脆弱なアプリケーションによる再発する攻撃から回復したワークロードを保護することも困難です。

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、これらの懸念に対処します。また、アプリケーションが南北トラフィックにさらされていない場所でも機能し、相互に通信できるように、ワークロードを機能しながらも分離されたネットワークにリカバリすることもできます。これにより、セキュリティ チームは安全な場所でフォレンジックを実施し、隠れたマルウェアや潜伏中のマルウェアがないことを確認できます。

利点

- 効率的で回復力のあるSnapMirrorレプリケーションの使用。
- スナップショット コピーの保持により、利用可能な任意の時点にリカバリできます。
- 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手順から数百から数千の VM を回復するために必要なすべての手順を完全に自動化します。
- 複製されたボリュームを変更しない方法を使用した、 ONTAP FlexCloneテクノロジーによるワークロードのリカバリ。
  - ボリュームまたはスナップショット コピー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。
  - DevTest、セキュリティ テスト、パッチまたはアップグレード テスト、修復テストなど、DR 以外のワークフローにクラウド コンピューティング リソースで DR データを使用する可能性。
- CPU と RAM の最適化により、より小規模なコンピューティング クラスターへのリカバリが可能になり、クラウド コストが削減されます。

Veeam Replication と **FSx ONTAP**を使用して **VMware Cloud on AWS** への災害復旧を行う

Amazon FSx ONTAPと VMware Cloud on AWS の統合は、SDDC 内のクラスターに接続できる NetApp のONTAPファイルシステム上に構築された AWS 管理の外部 NFS データストアです。コンピューティング リソースとは独立して拡張できる、柔軟で高性能な仮想化ストレージ インフラストラクチャを顧客に提供します。

概要

VMware Cloud on AWS SDDC を災害復旧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、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 ソリューションを使用して、FSx ONTAPデータストアでオンプレミスからデータを複製できます。 FSx 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膨大な数の ESXi ホストを使用して VMware Cloud on AWS SDDC を構築するよりもコストを最適化した展開が可能になります。

このアプローチは、VM レプリカをホストするために、VMC のパイロット ライト クラスタと FSx ONTAPデータストアを使用するのにも役立ちます。レプリケーション プランを正常にフェイルオーバーすることで、同じプロセスを VMware Cloud on AWS への移行オプションとして拡張することもできます。

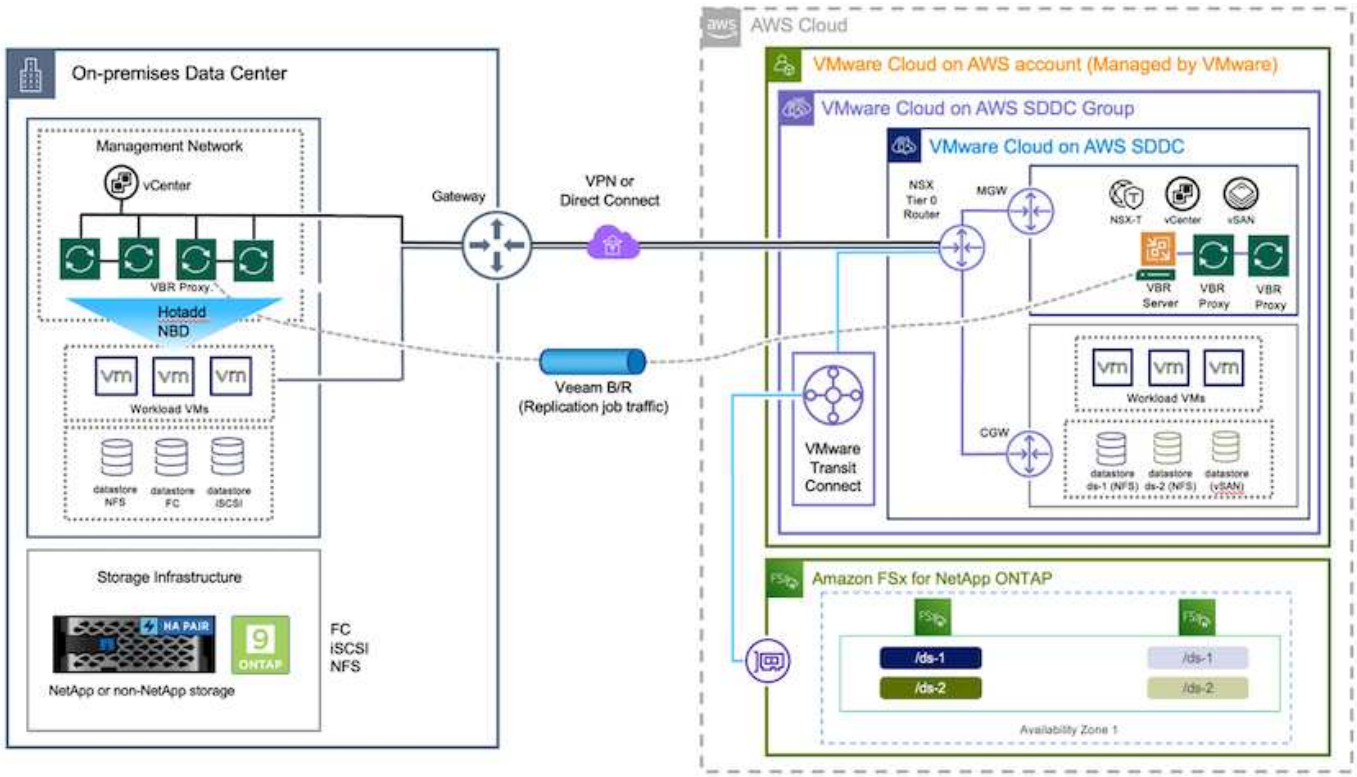
このドキュメントでは、FSx ONTAPデータストアと Veeam Backup and replication を使用して、VM レプリケーション機能によりオンプレミスの VMware VM から VMware Cloud on AWS へのディザスタ リカバリを設定する方法について説明します。

Veeam Backup & Replication を使用すると、災害復旧 (DR) のためのオンサイトおよびリモートのレプリケーションが可能になります。仮想マシンが複製されると、Veeam Backup & Replication は、ターゲットの VMware Cloud on AWS SDDC クラスター上にネイティブ VMware vSphere 形式で仮想マシンの正確なコピーを作成し、そのコピーを元の仮想マシンと同期した状態に保ちます。

レプリケーションでは、起動準備完了状態の VM のコピーが存在するため、最適な復旧時間目標 (RTO) 値が提供されます。このレプリケーション メカニズムにより、災害発生時にワークロードを VMware Cloud on AWS SDDC で迅速に開始できるようになります。 Veeam Backup & Replication ソフトウェアは、WAN および低速接続を介したレプリケーションのトラフィック転送も最適化します。さらに、重複したデータ ブロック、ゼロ データ ブロック、スワップ ファイル、除外された VM ゲスト OS ファイルも除外し、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するのを防ぐために、WAN アクセラレータとネットワーク スロットリング ルールを導入できます。 Veeam Backup & Replication のレプリケーション プロセスはジョブ駆動型であり、レプリケーション ジョブを構成することによってレプリケーションが実行されます。災害が発生した場合、フェイルオーバーをトリガーしてレプリカ コピーにフェイルオーバーすることで VM を復旧できます。

フェイルオーバーが実行されると、複製された 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その既知の復元ポイントのいずれか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の回復や分離されたテストが可能になります。 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、後で最終的に決定する必要があります。 Veeam Backup & Replication は、さまざまな災害復旧シナリオを処理するための複数のオプションを提供します。



高レベルの手順

1. Veeam Backup and 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 を設定し、VMware Cloud on AWS SDDC と FSx ONTAP を NFS データストアとしてデプロイおよび構成するには、VMware Cloud Tech Zone の記事 "VMware Cloud on AWS とAmazon FSx ONTAP の統合の導入ガイド" を参照してください。（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の目的で使用できます。インシデントの発生時には、VMはこのクラスタにフェイルオーバーされ、追加の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します。
5. 災害イベントが完了し、プライマリ サイトが稼働したら、本番環境の VM に切り替えます。

VMC および **FSx 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 バックアップ VM がソース vCenter とターゲット VMware cloud on AWS SDDC クラスターに接続されていることを確認します。
2. バックアップ サーバーは、短い名前を解決し、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FSx ONTAPデータストアには、複製されたVMのVMDKを保存するのに十分な空き容量が必要です。

詳細については、「考慮事項と制限事項」を参照してください。"ここをクリックしてください。" 。

導入環境の詳細

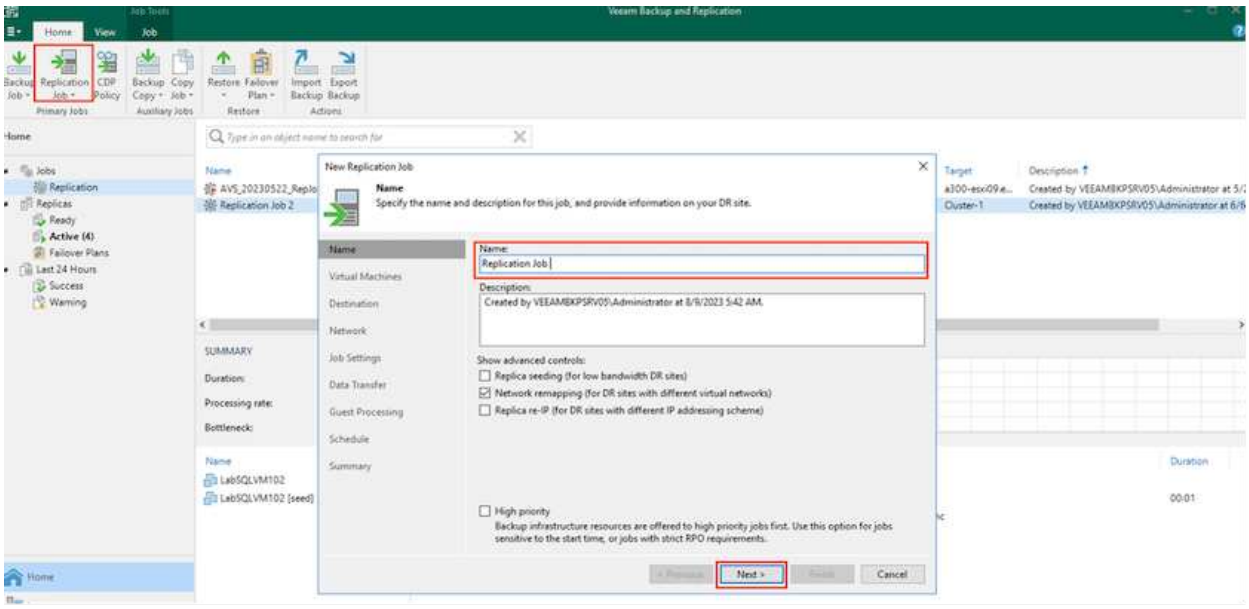
▼ ステップ**1: VM**を複製する

Veeam Backup & Replication は VMware vSphere の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、システム状態、構成などを含む VM の特定時点のコピーです。 Veeam Backup & Replication は、スナップショットをレプリケーションのデータ ソースとして使用します。

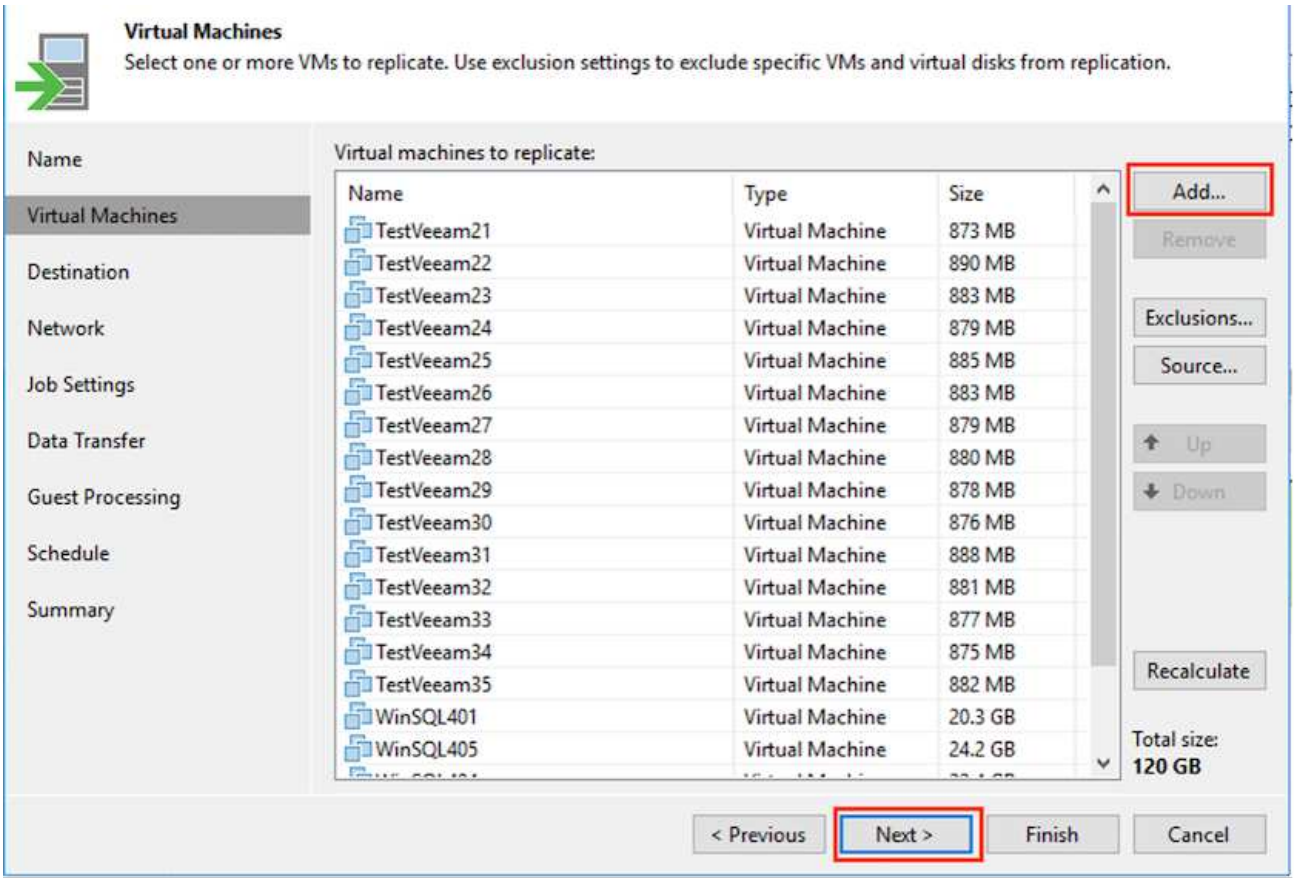
VM をレプリケートするには、次の手順に従います。

1. Veeam Backup & Replication コンソールを開きます。
2. ホーム ビューで、レプリケーション ジョブ > 仮想マシン > 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。[Next]をクリックします。
   - オンプレミスと AWS 間の接続の帯域幅が制限されている場合は、レプリカ シーディング 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のサイト 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（異なるネットワークを持つ AWS VMC サイトの場合）] 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 アドレス指定スキームが AWS VMC サイトのスキームと異なる場合は、[レプリカ再 IP (IP アドレス指定スキームが異なる DR サイト用)] チェック ボックスをオン

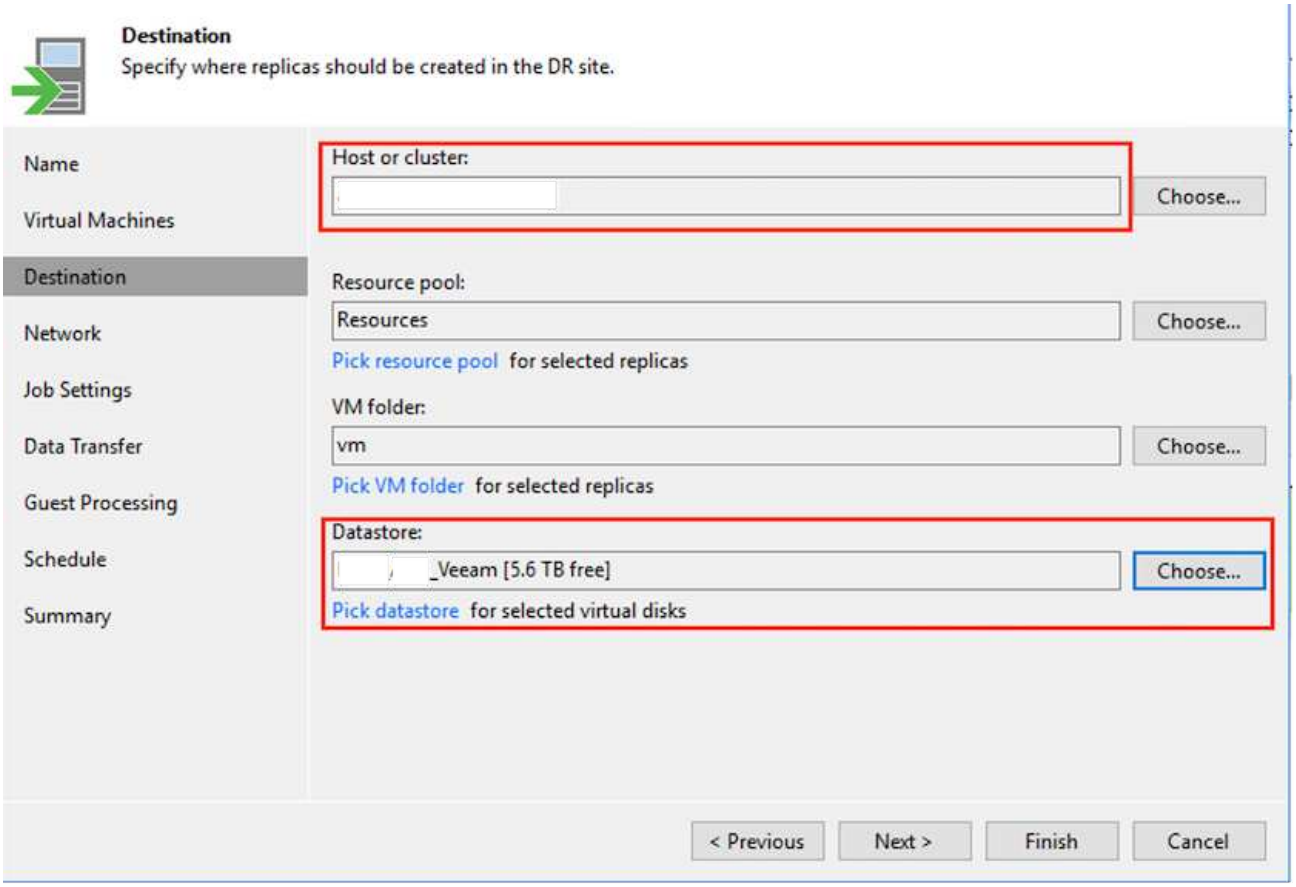
にします。



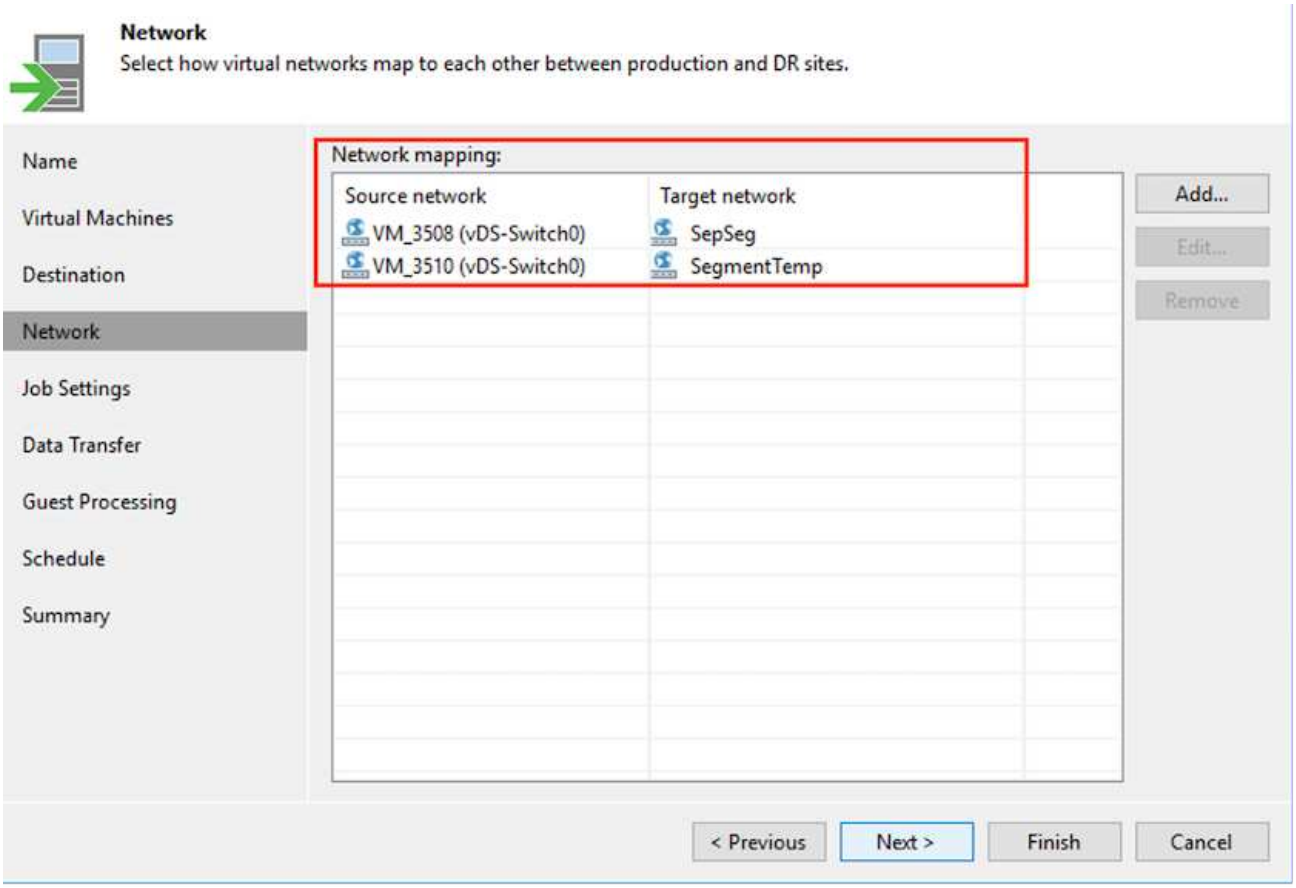
4. 仮想マシン ステップで、VMware Cloud on AWS SDDC に接続された FSx ONTAPデータストアに複製する必要がある仮想マシンを選択します。使用可能な vSAN データストアの容量を満たすために、仮想マシンを vSAN 上に配置できます。パイロット ライト クラスターでは、3 ノード クラスターの使用可能な容量が制限されます。残りのデータは FSx ONTAPデータストアに複製できます。 [追加] をクリックし、[オブジェクトの追加] ウィンドウで必要な VM または VM コンテナを選択して [追加] をクリックします。*次へ*をクリックします。



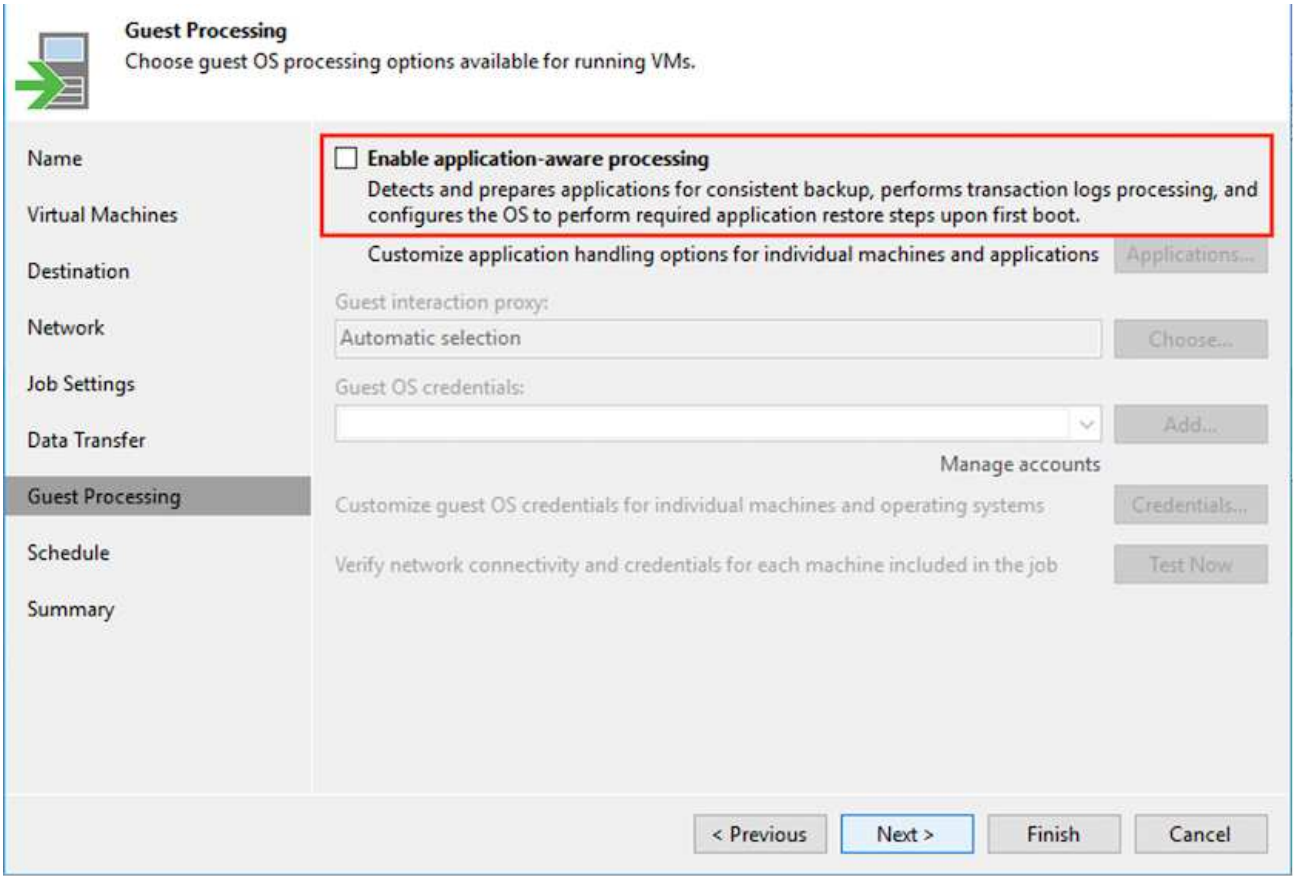
5. その後、宛先として VMware Cloud on AWS SDDC クラスタ/ホストを選択し、VM レプリカ用の適切なリソース プール、VM フォルダ、および FSx ONTAPデータストアを選択します。次に、[次へ]をクリックします。



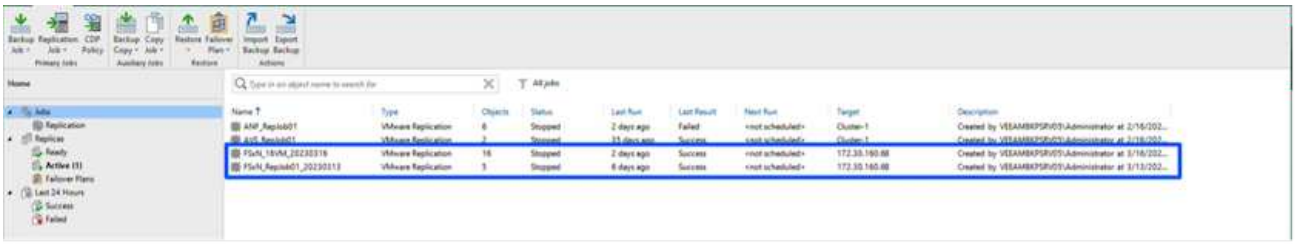
6. 次の手順では、必要に応じて、ソース仮想ネットワークと宛先仮想ネットワーク間のマッピングを作成します。



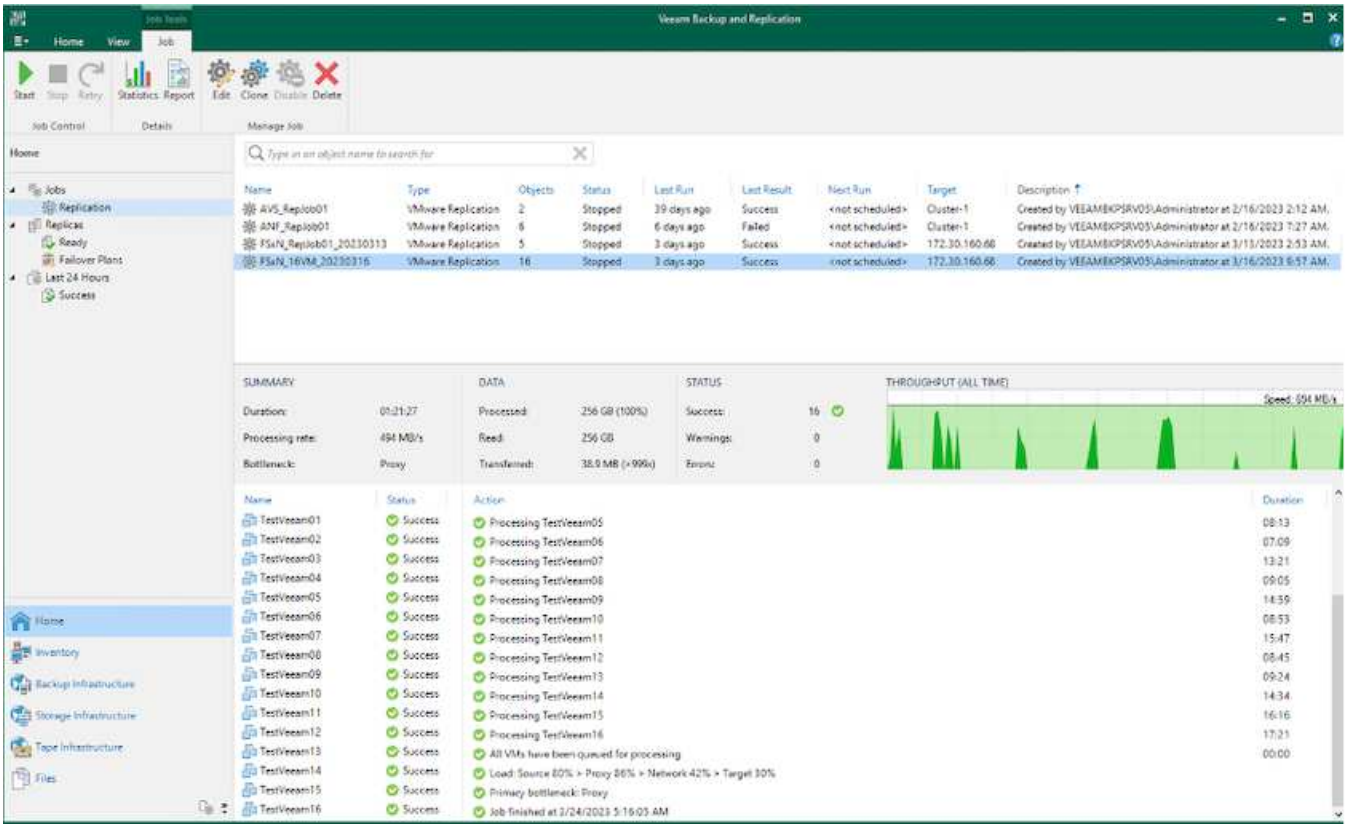
7. ジョブ設定 ステップで、VM レプリカのメタデータ、保持ポリシーなどを保存するバックアップ リポジトリを指定します。
8. *データ転送*手順で*ソース*および*ターゲット*プロキシ サーバーを更新し、*自動*選択 (デフォルト) のままにして、*直接*オプションを選択したままにして、*次へ*をクリックします。
9. *ゲスト処理*のステップで、必要に応じて*アプリケーション対応処理を有効にする*オプションを選択します。*次へ*をクリックします。



10. 定期的に実行するレプリケーション ジョブを実行するには、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*概要*手順で、レプリケーション ジョブの詳細を確認します。ウィザードを閉じ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。それ以外の場合は、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を持つ VM が宛先 VMC SDDC クラスタ/ホストに配置されます。



Veeamレプリケーションの詳細については、以下を参照してください。"レプリケーションの仕組み" 。

▼ ステップ**2:** フェイルオーバー計画を作成する

初期レプリケーションまたはシードが完了したら、フェールオーバー 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、ブートの遅延を含め、VM が処理される順序の青写真です。フェールオーバー 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、「フェールオーバー 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復元ポイントを探し、それを使用して VM レプリカを起動します。

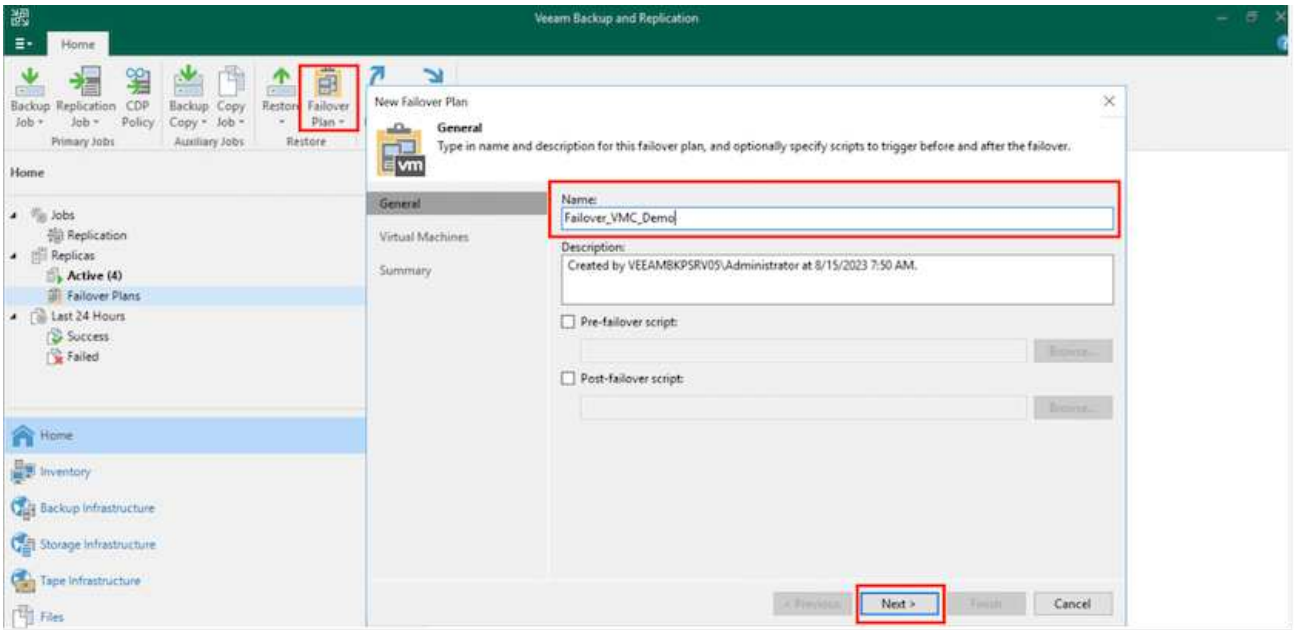
ⓘ フェールオーバー プランは、初期レプリケーションが完了し、VM レプリカが準備完了状態になった後にのみ追加できます。

ⓘ 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。

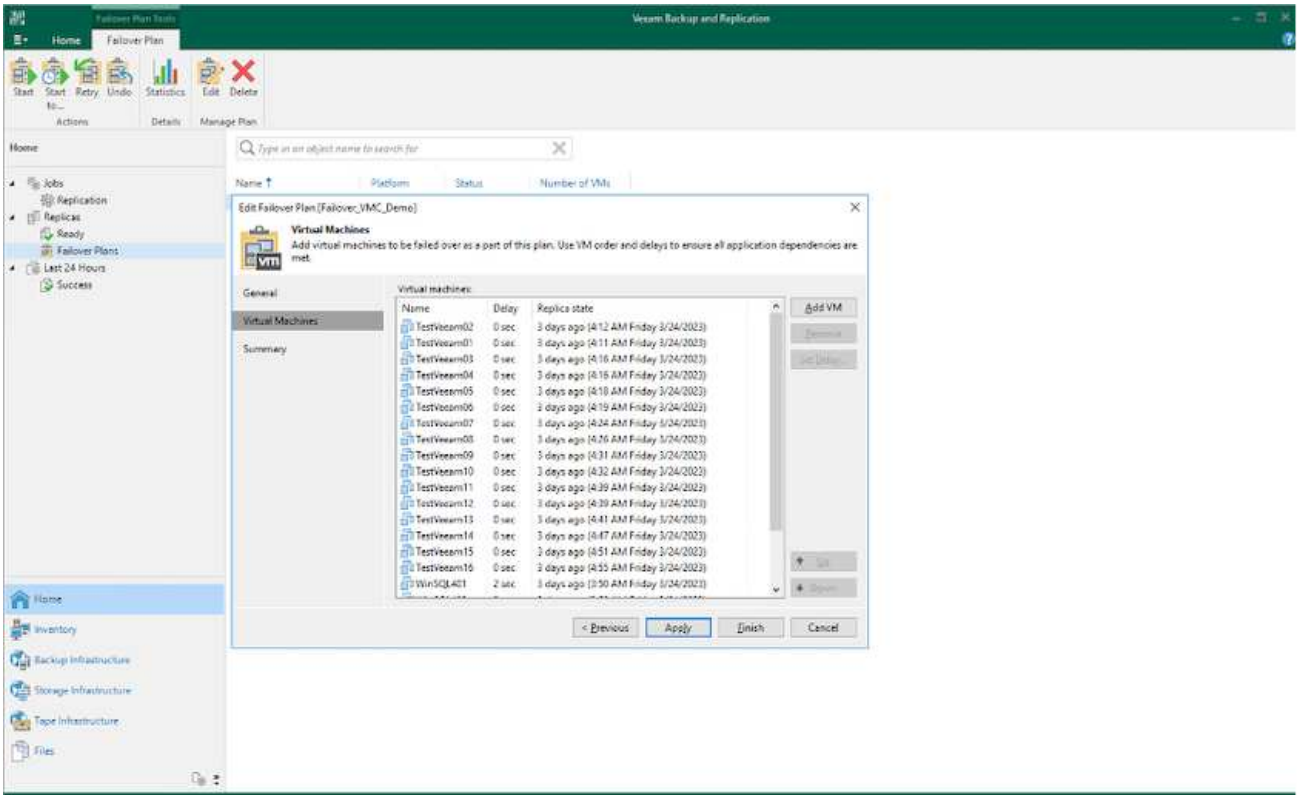
ⓘ フェールオーバー プロセス中、ソース VM の電源はオフになりません。

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、プランの名前と説明を入力します。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、複製された VM を起動する前に VM をシャットダウンするスクリプトを実行します。



3. VM を計画に追加し、アプリケーションの依存関係を満たすように VM のブート順序とブート遅延を変更します。



レプリケーションジョブの作成に関する追加情報については、以下を参照してください。"レプリケーションジョブの作成" 。

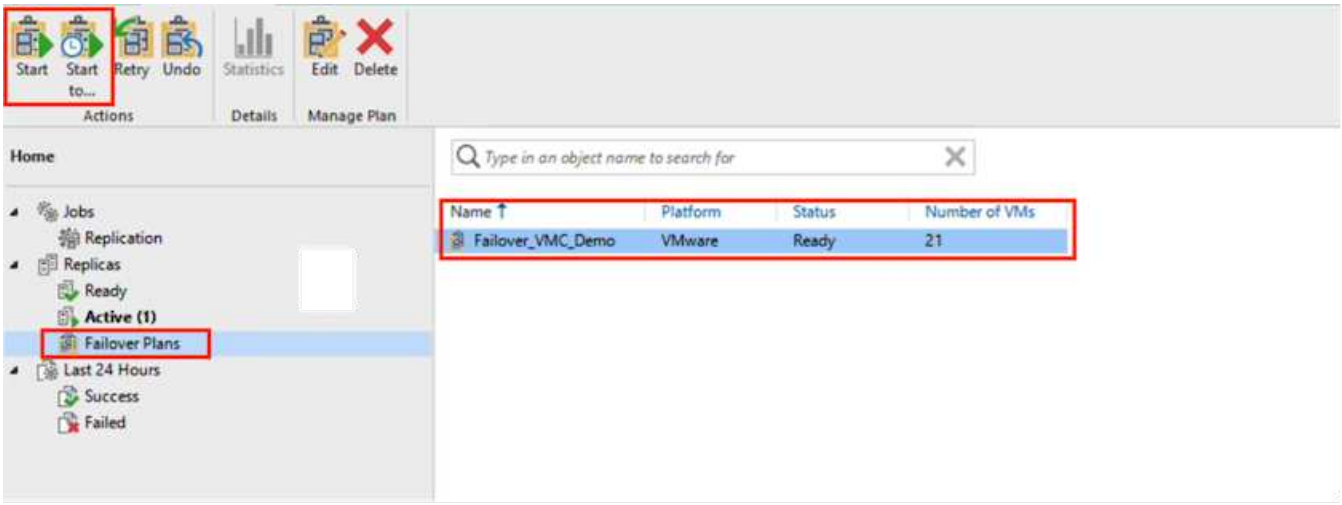
▼ ステップ**3:** フェイルオーバープランを実行する

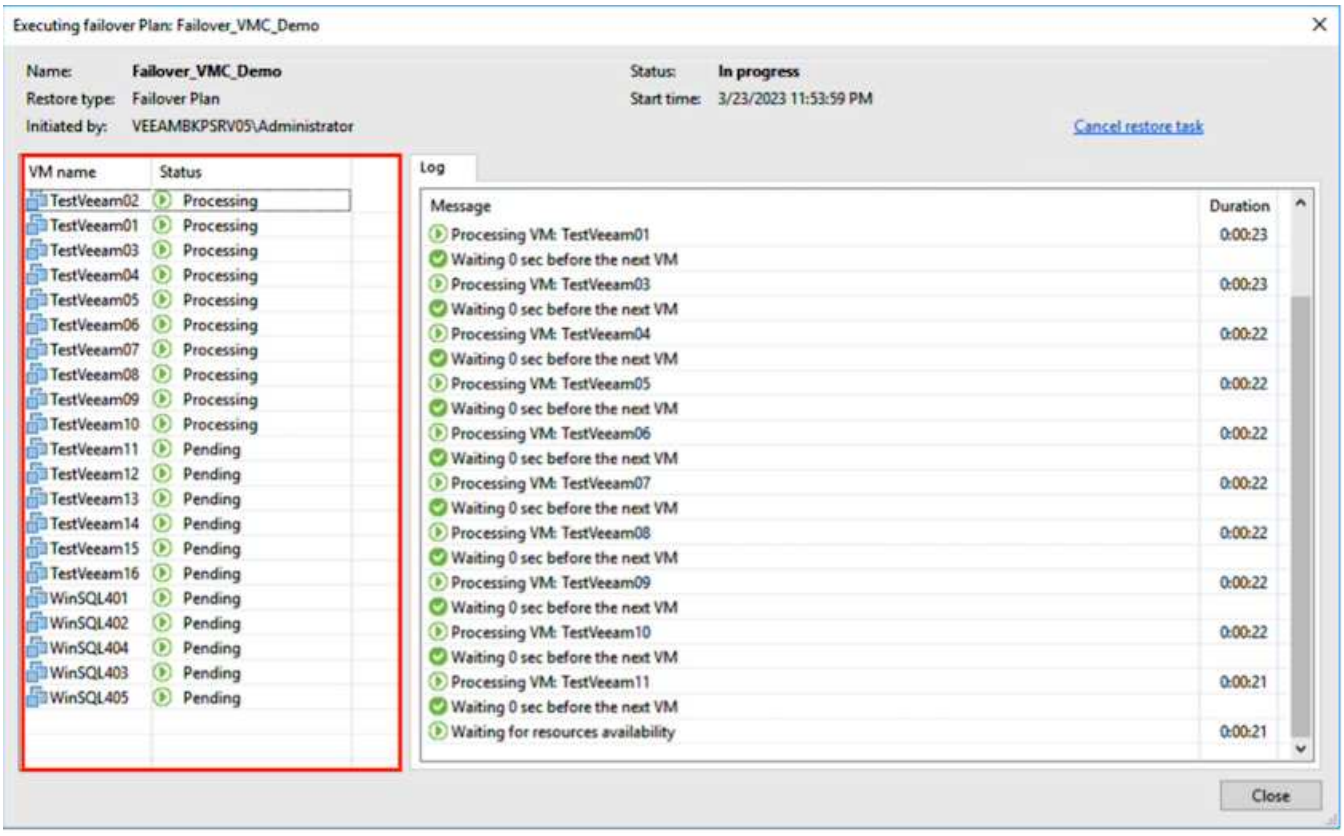
フェイルオーバー中、運用サイトのソース VM は災害復旧サイトのレプリカに切り替えられます。フェイルオーバー プロセスの一環として、Veeam Backup & Replication は VM レプリカを必要な復元ポイントに復元し、すべての I/O アクティビティをソース VM からそのレプリカに移動します。レプリカは災害時だ

けでなく、DR 訓練のシミュレーションにも使用できます。フェールオーバー シミュレーション中、ソース VM は実行を継続します。必要なテストがすべて実行されたら、フェイルオーバーを元に戻して通常の操作に戻ることができます。

DR ドリル中の 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確実に実施されていることを確認してください。

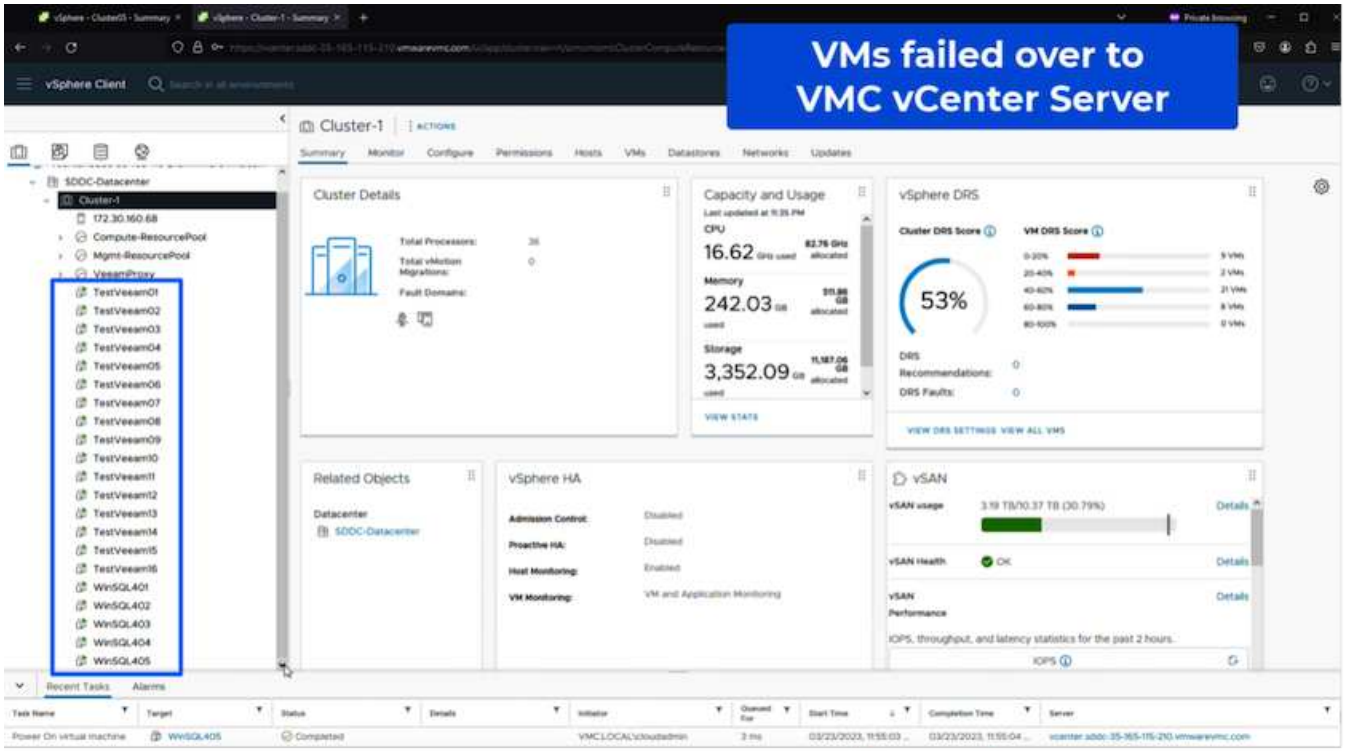
フェールオーバー プランを開始するには、[フェールオーバー プラン] タブをクリックし、フェールオーバー プランを右クリックするだけです。 *開始*を選択します。これにより、VM レプリカの最新の復元ポイントを使用してフェイルオーバーが行われます。 VM レプリカの特定の復元ポイントにフェールオーバーするには、[開始] を選択します。



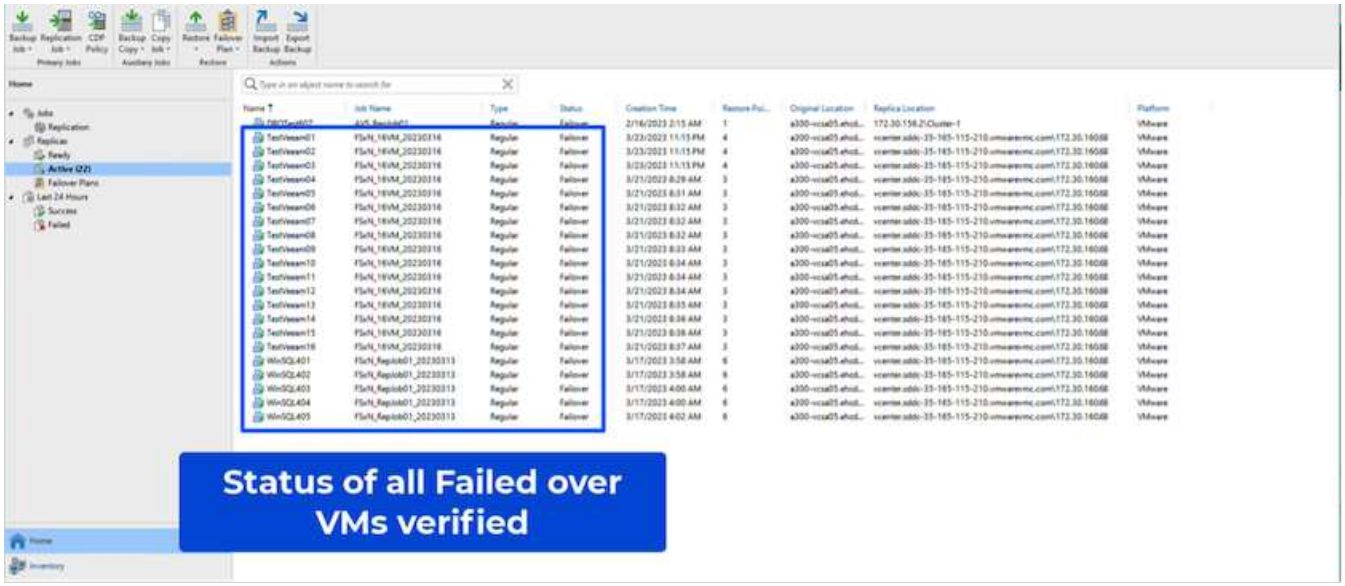


VM レプリカの状態が「準備完了」から「フェイルオーバー」に変わり、VM は宛先の VMware Cloud on

AWS SDDC クラスタ/ホストで起動します。



フェイルオーバーが完了すると、VM のステータスが「フェイルオーバー」に変わります。



Veeam Backup & Replication は、レプリカが準備完了状態に戻るまで、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、以下を参照してください。"フェイルオーバー計画" 。

▼ ステップ**4:** 本番サイトへのフェイルバック

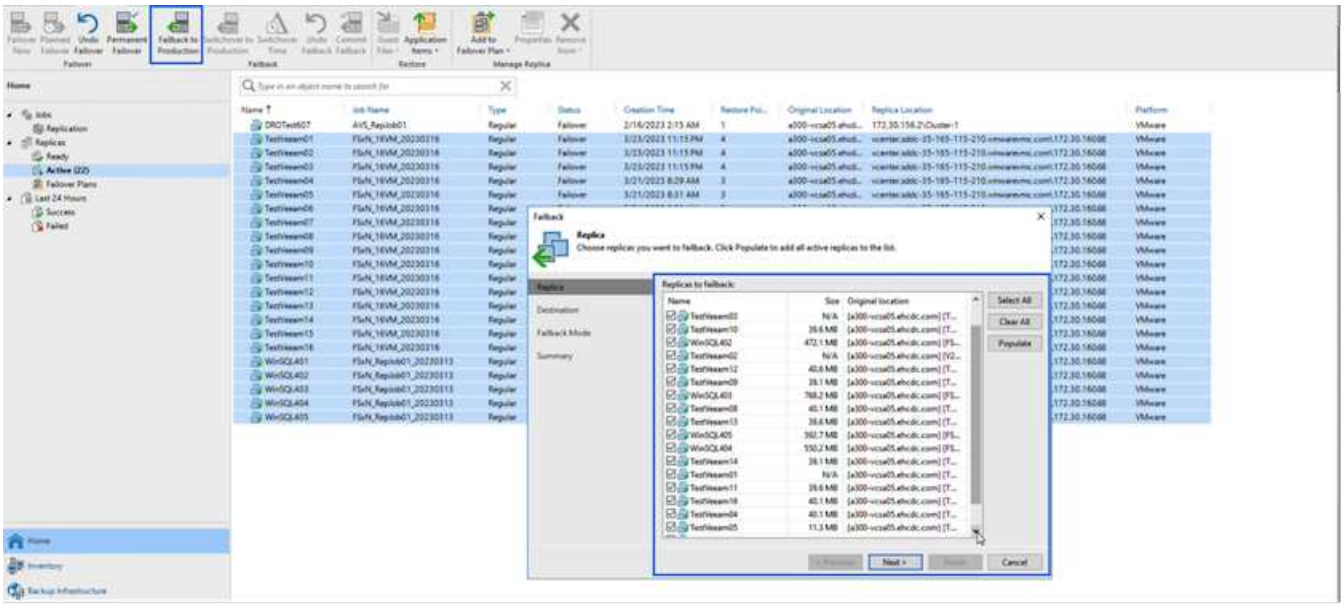
フェイルオーバー プランが実行中の場合、それは中間ステップとみなされ、要件に基づいて確定する必要があります。オプションには次のものがあります。

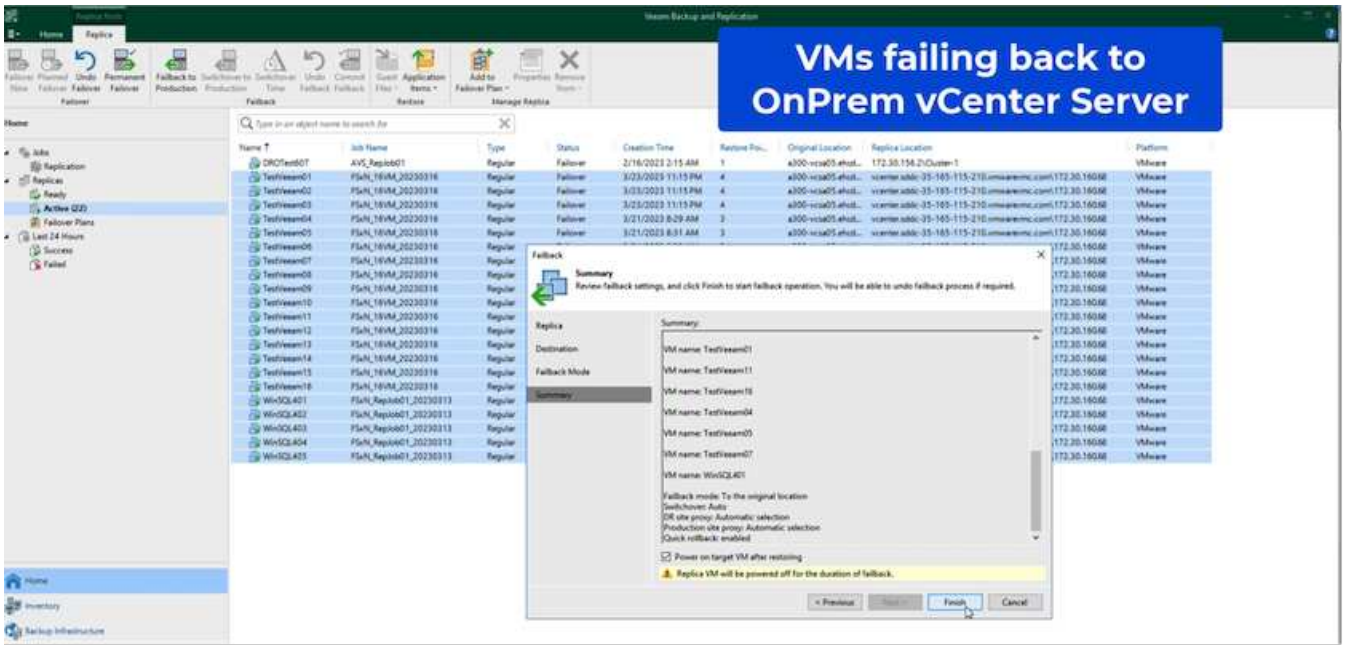
- 本番環境へのフェールバック - 元の VM に切り替えて、VM レプリカの実行中に行われたすべての変更を元の VM に転送します。

> フェイルバックを実行すると、変更は転送されるだけで公開されません。元の VM が期待どおりに動作していることが確認されたら、フェイルバックのコミット を選択するか、元の VM が期待どおりに動作していない場合は、フェイルバックを元に戻す を選択して 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われたすべての変更を破棄します。
- 永続的なフェイルオーバー - 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。

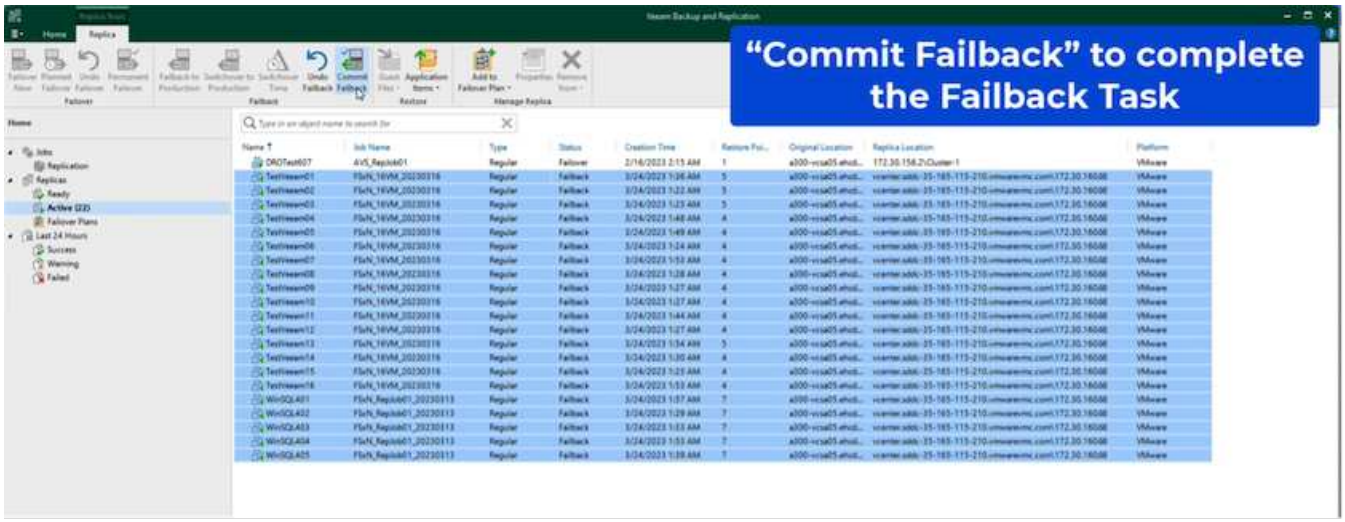
このデモでは、本番環境へのフェールバックが選択されました。ウィザードの宛先ステップで元の VM へのフェールバックが選択され、「復元後に VM をパワーオンする」チェックボックスが有効になりました。

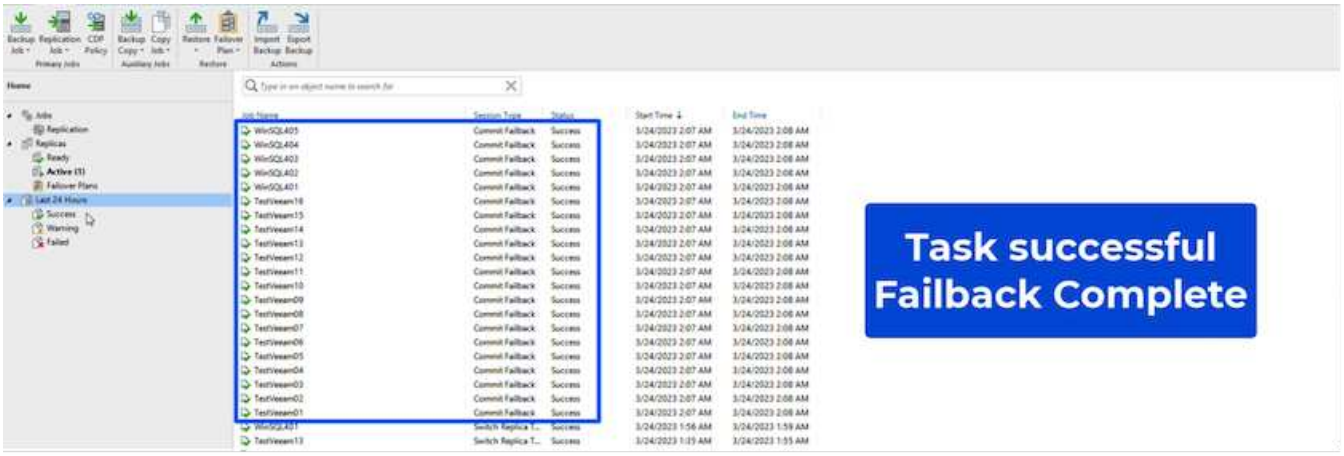




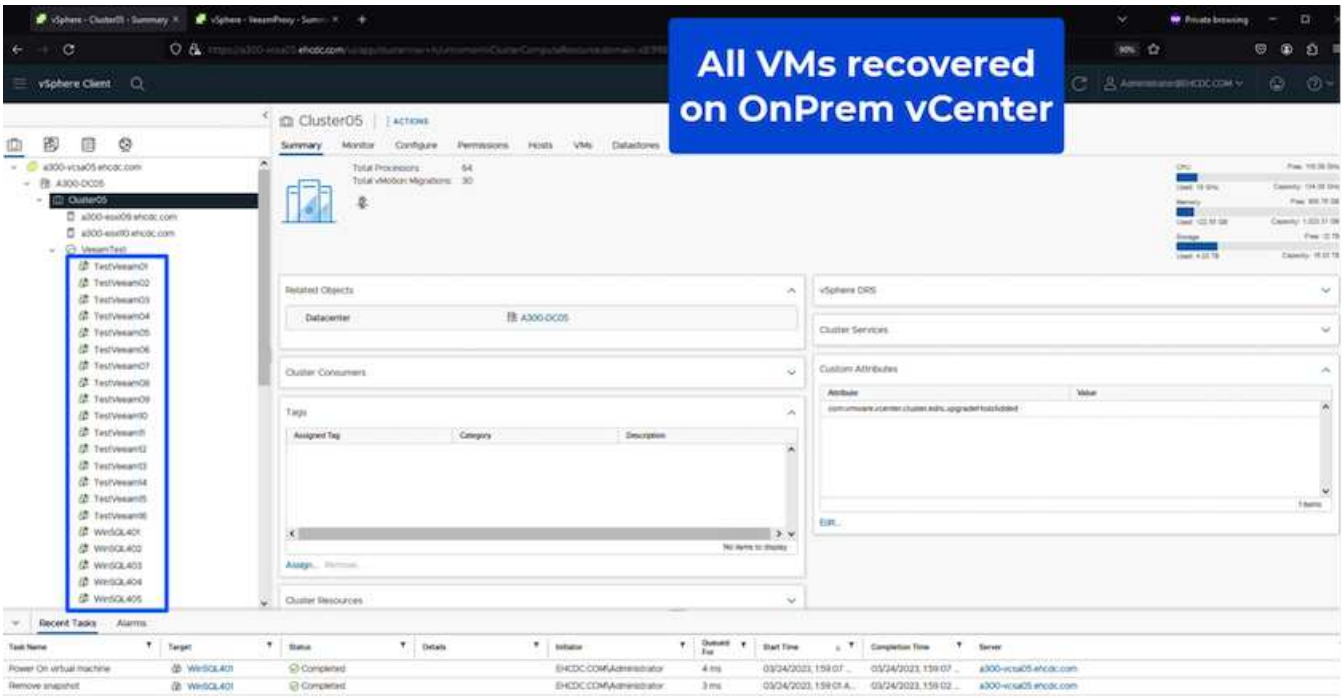
フェイルバックコミットは、フェイルバック操作を完了する方法の 1 つです。フェイルバックがコミットされると、フェイルバックされた VM (運用 VM) に送信された変更が期待どおりに機能していることが確認されます。コミット操作の後、Veeam Backup & Replication は実稼働 VM のレプリケーション アクティビティを再開します。

フェイルバックプロセスの詳細については、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" 。





運用環境へのフェイルバックが成功すると、VM はすべて元の運用サイトに復元されます。



まとめ

FSx ONTAPデータストア機能により、Veeam または検証済みのサードパーティ ツールは、VM レプリカ コピーに対応するためだけにクラスター内に多数のホストを立ち上げることなく、Pilot light クラスターを使用して低コストの DR ソリューションを提供できるようになります。これにより、調整されカスタマイズされた災害復旧計画を処理するための強力なソリューションが提供され、DR のニーズを満たすために社内の既存のバックアップ製品を再利用することも可能になり、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災害復旧が可能になります。フェイルオーバーは、計画的なフェイルオーバーとして実行することも、災害発生時にボタンをクリックするだけでフェイルオーバーを実行することもでき、DR サイトをアクティブ化する決定が下されます。

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

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a

AWS/VMC 上のワークロードを移行する

TR 4942: VMware HCX を使用してワークロードを FSx ONTAPデータストアに移行する

Amazon FSx ONTAP上の補足 NFS データストアを使用した、Amazon Web Services (AWS) 上の VMware Cloud (VMC) の一般的な使用例は、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、VMware がサポートする任意のデータストアで実行されているオンプレミスの仮想マシン (VM) とそのデータを、FSx ONTAP上の補足 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提供します。

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

VMware HCX は主に、クラウド間でのワークロードの移行、ワークロードの再調整、および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。これは VMware Cloud on AWS の一部として含まれており、ワークロードを移行するためのさまざまな方法を提供し、災害復旧 (DR) 操作に使用できます。

このドキュメントでは、オンプレミスとクラウド データ センター側でさまざまな VM 移行メカニズムを有効にする、VMware HCX の展開と構成に関する手順ごとのガイダンスを提供します。これには、そのすべての主要コンポーネントが含まれます。

詳細については、 "VMware HCX ユーザーガイド"そして "インストール チェックリスト B - VMware Cloud on AWS SDDC 移行先環境での HCX"。

▼ 大まかな手順

このリストには、VMware HCX をインストールして構成するための大まかな手順が示されています。

1. VMware Cloud Services コンソールを通じて、VMC ソフトウェア定義データセンター (SDDC) の HCX をアクティブ化します。
2. オンプレミスの vCenter Server に HCX コネクタ OVA インストーラーをダウンロードしてデプロイします。
3. ライセンス キーを使用して HCX をアクティブ化します。
4. オンプレミスの VMware HCX コネクタと 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 メッシュを構成します。
6. (オプション) 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 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します。

▼ 前提条件

始める前に、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、以下を参照してください。 "インストールの準備" 。接続などの前提条件が整ったら、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 プラグインが展開され、管理のために 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。

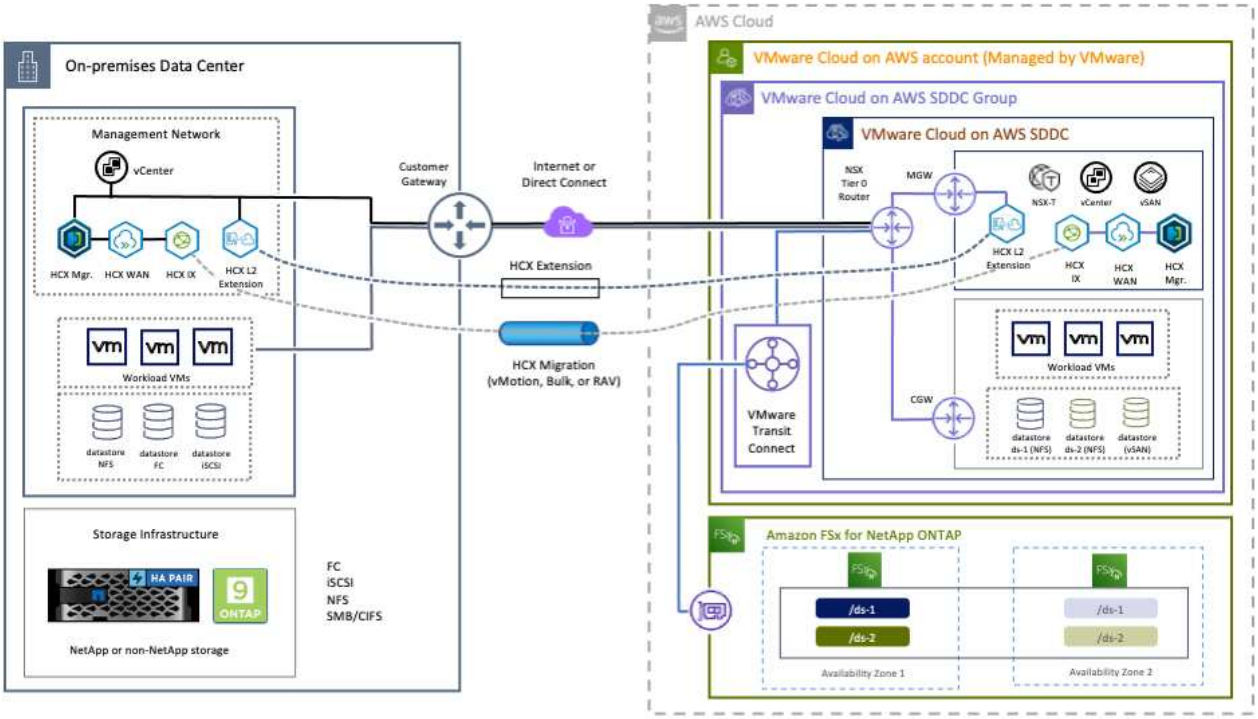
HCX のアクティベーションとデプロイメントを続行する前に、次のインストール手順を完了する必要があります。

1. 既存のVMC SDDCを使用するか、これに従って新しいSDDCを作成します。"NetAppリンク"またはこれ "VMware 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 パスは、vMotion を使用した仮想マシンの移行をサポートしている必要があります。
3. 必要な "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 トラフィックが許可されます。
4. FSx ONTAP NFS ボリュームは、VMC SDDC の補足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、この手順に従ってください。"NetAppリンク"またはこれ "VMware リンク"。

▼ 高レベルアーキテクチャ

テストの目的で、この検証に使用されたオンプレミスのラボ環境は、サイト間 VPN を介して AWS VPC に接続され、オンプレミスから AWS および外部トランジットゲートウェイ経由の VMware Cloud SDDC への接続が可能になりました。 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 クラウドの宛先 SDDC 間をインターネット経由で流れます。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、高レベルのアーキテクチャを示しています。



ソリューションの展開

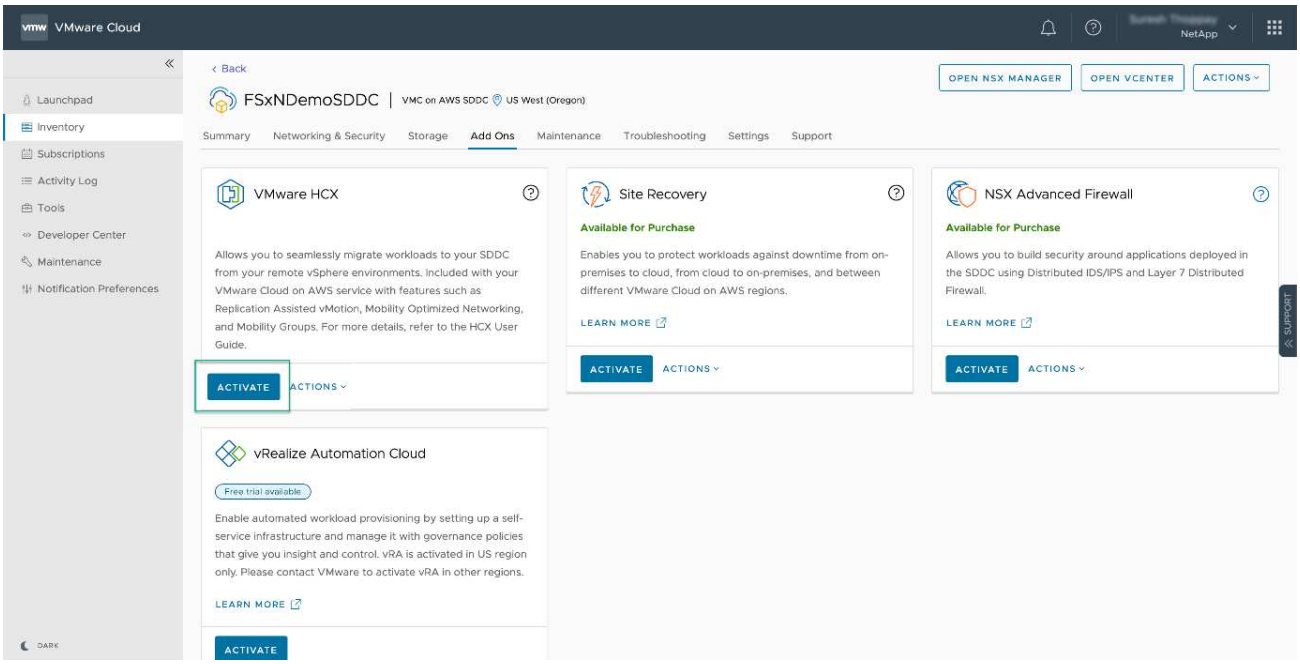
このソリューションの展開を完了するには、次の一連の手順に従います。

▼ ステップ**1:** アドオンオプションを使用して**VMC SDDC**経由で**HCX**をアクティブ化する

インストールを実行するには、次の手順を実行します。

1. VMCコンソールにログインします "vmc.vmware.com"インベントリにアクセスします。
2. 適切な SDDC を選択してアドオンにアクセスするには、SDDC の [詳細の表示] をクリックし、[アドオン] タブを選択します。
3. VMware HCX の [アクティブ化] をクリックします。

   このステップが完了するまでに最大 25 分かかります。

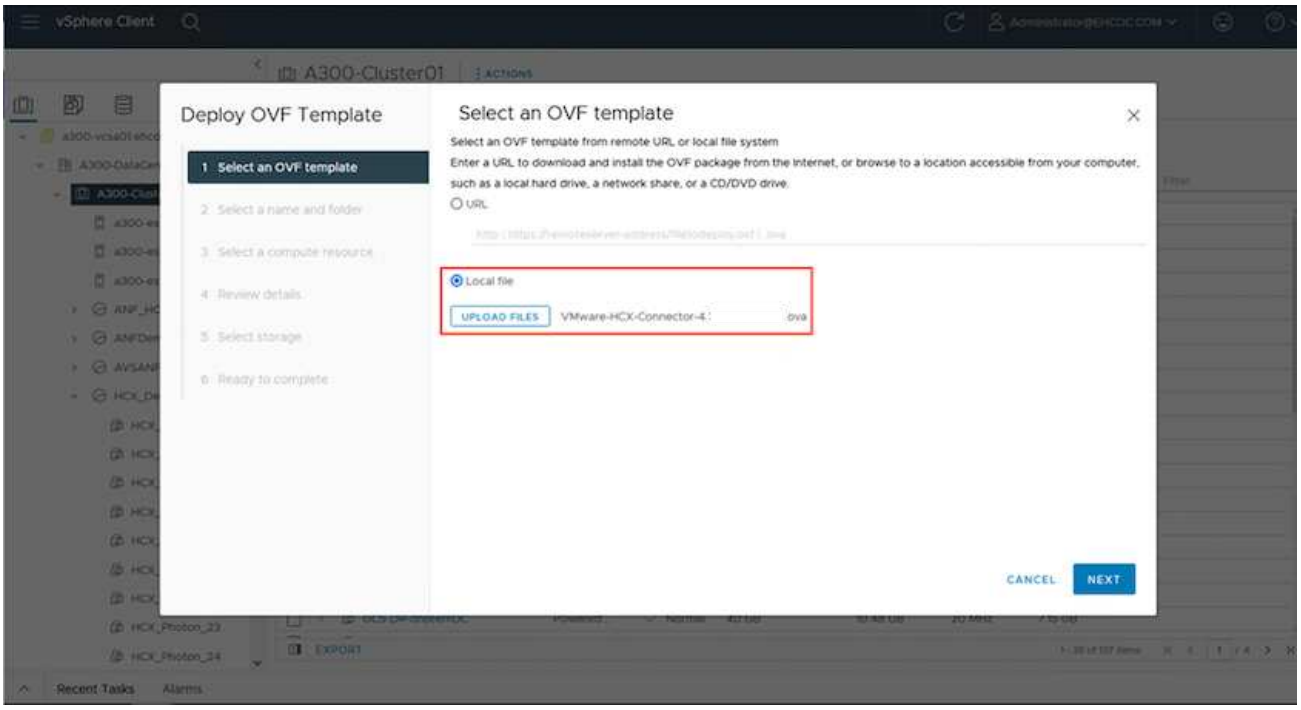


4. デプロイが完了したら、HCX Manager とそれに関連付けられたプラグインが vCenter Console で使用できることを確認して、デプロイを検証します。
5. 適切な管理ゲートウェイ ファイアウォールを作成して、HCX Cloud Manager にアクセスするために必要なポートを開きます。これで、HCX Cloud Manager は HCX 操作の準備が整いました。

▼ ステップ**2:** オンプレミスの**vCenter Server**にインストーラ**OVA**を展開する

オンプレミスのコネクタが VMC 内の HCX マネージャーと通信するには、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てください。

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 アップデート] タブを選択します。 HCX コネクタ OVA イメージのダウンロード リンクの要求をクリックします。
2. HCX コネクタをダウンロードしたら、オンプレミスの vCenter Server に OVA をデプロイします。vSphere クラスターを右クリックし、OVF テンプレートのデプロイ オプションを選択します。

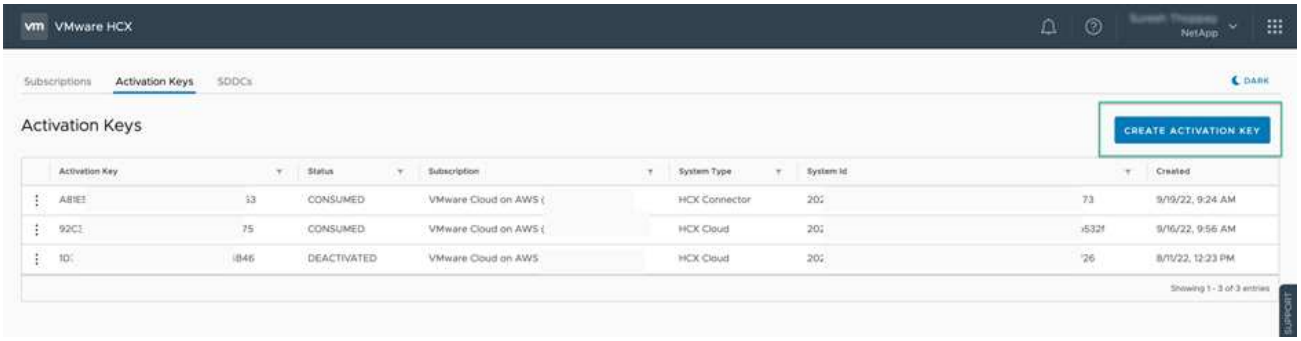


3. OVF テンプレートのデプロイ ウィザードに必要な情報を入力し、[次へ] をクリックしてから [完了] をクリックして、VMware HCX コネクタ OVA をデプロイします。
4. 仮想アプライアンスを手動で電源オンにします。手順については、 "VMware HCX ユーザーガイド" 。

▼ ステップ**3:** ライセンスキーを使用して**HCX**コネクタをアクティブ化する

VMware HCX コネクタ OVA をオンプレミスにデプロイし、アプライアンスを起動したら、次の手順を実行して HCX コネクタをアクティブ化します。 VMC の VMware HCX コンソールからライセンス キーを生成し、VMware HCX コネクタのセットアップ中にライセンスを入力します。

1. VMware Cloud コンソールから、インベントリに移動し、SDDC を選択して、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. 「アクティベーション キー」タブから、「アクティベーション キーの作成」をクリックします。システム タイプとして HCX コネクタを選択し、[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。



オンプレミスに展開される 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コネクタにログインします。 `"https://hcxconnectorIP:9443"`管理者の資格情報を使用します。

OVA 展開時に定義されたパスワードを使用します。

4. ライセンスセクションで、手順 2 でコピーしたアクティベーション キーを入力し、[アクティベート] をクリックします。

アクティベーションを正常に完了するには、オンプレミスの 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、オンプレミスの VMware HCX Manager をインストールするための希望の場所を指定します。[Continue]をクリックします。
6. 「システム名」の下で名前を更新し、「続行」をクリックします。
7. 「はい」を選択し、「続行」を選択します。
8. [vCenter への接続] で、vCenter Server の IP アドレスまたは完全修飾ドメイン名 (FQDN) と資格情報を入力し、[続行] をクリックします。

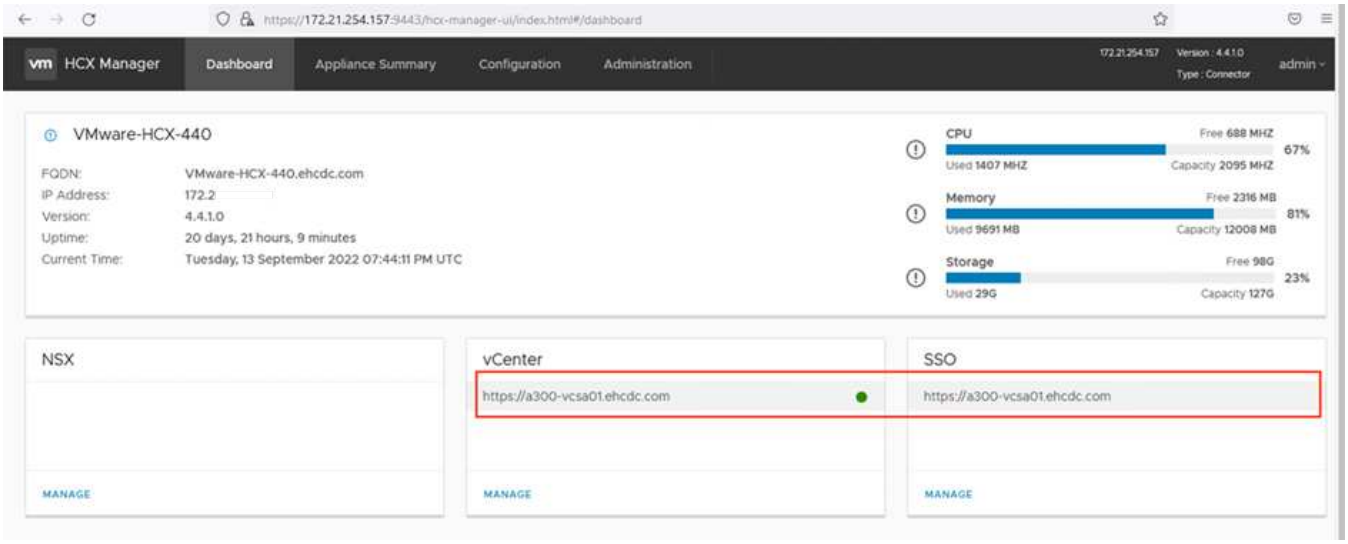
後で通信上の問題を回避するために、FQDN を使用してください。

9. [SSO/PSC の構成] で、Platform Services Controller の FQDN または IP アドレスを入力し、[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 が緑色で表示されます。 vCenter Server と SSO の両方に正しい構成パラメータが設定されている必要があります。これは前のページと同じである必要があります。

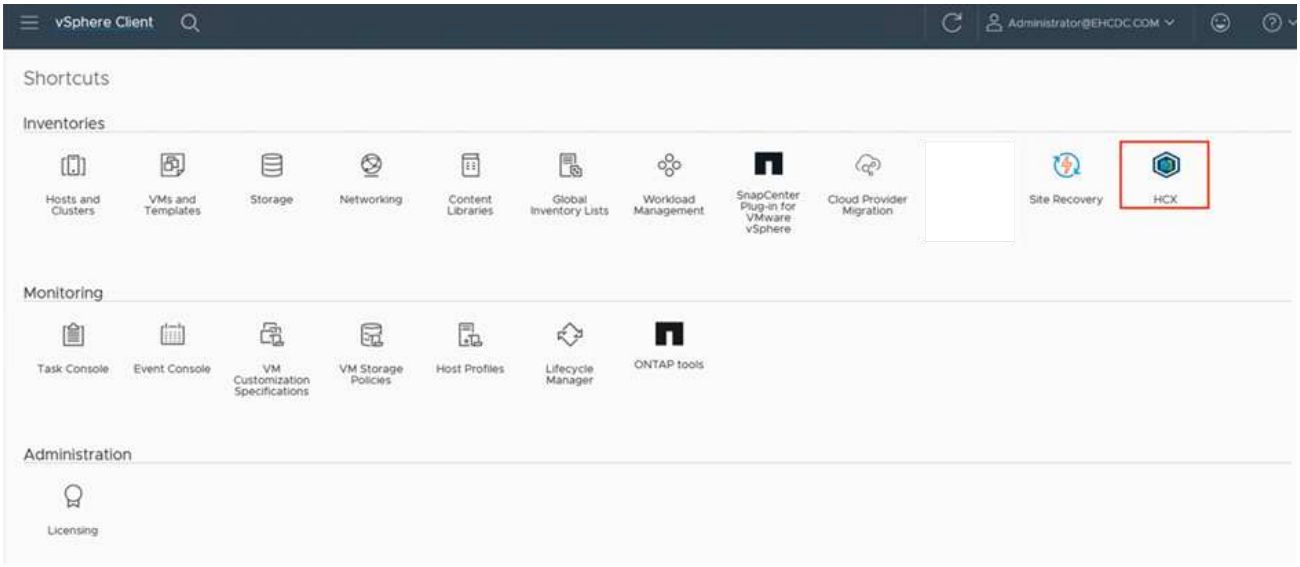
このプロセスには、プラグインが vCenter Server に追加されるまでに約 10 ～ 20 分かかります。



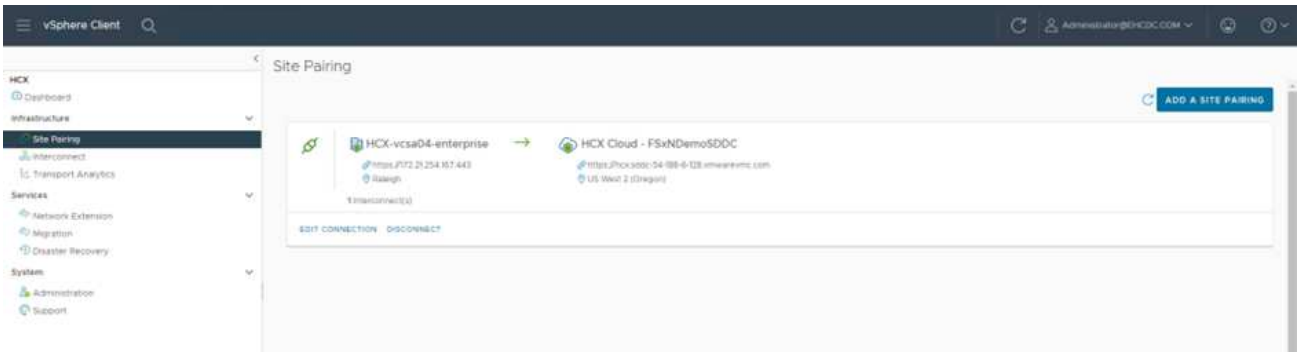
▼ ステップ**4**：オンプレミスの**VMware HCX**コネクタと**VMC HCX Cloud Manager**をペアリングする

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

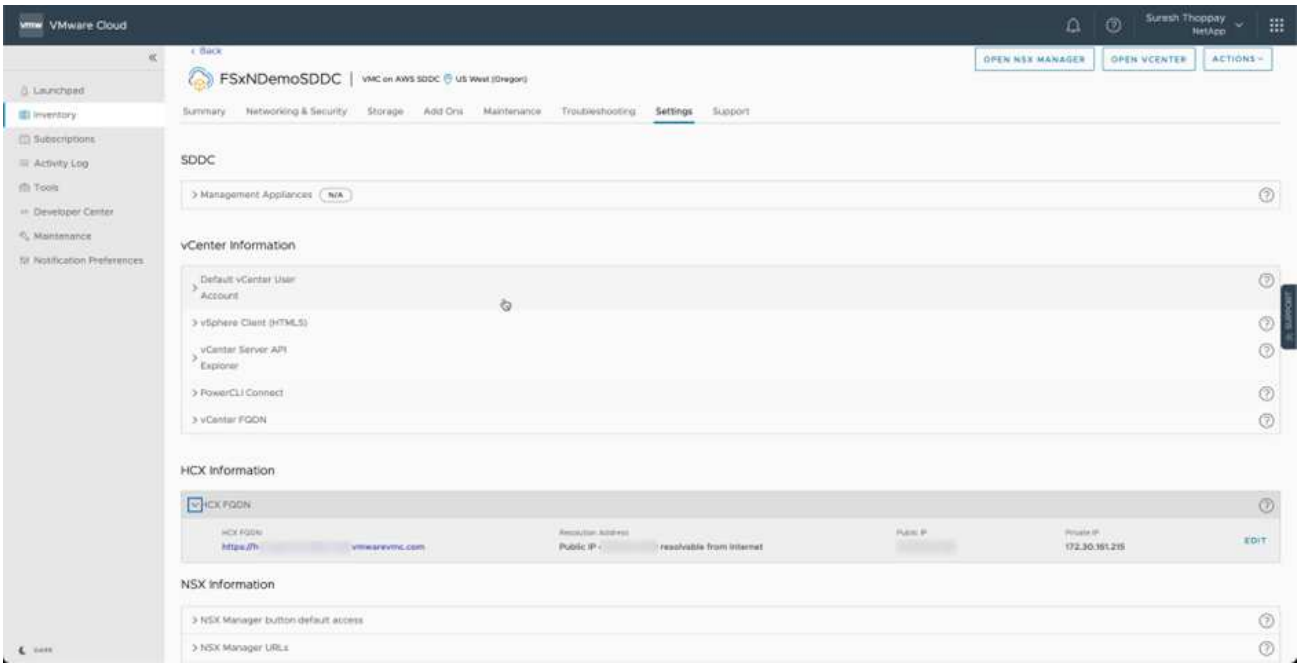
vCenter Server にログインし、HCX vSphere Web Client プラグインにアクセスします。

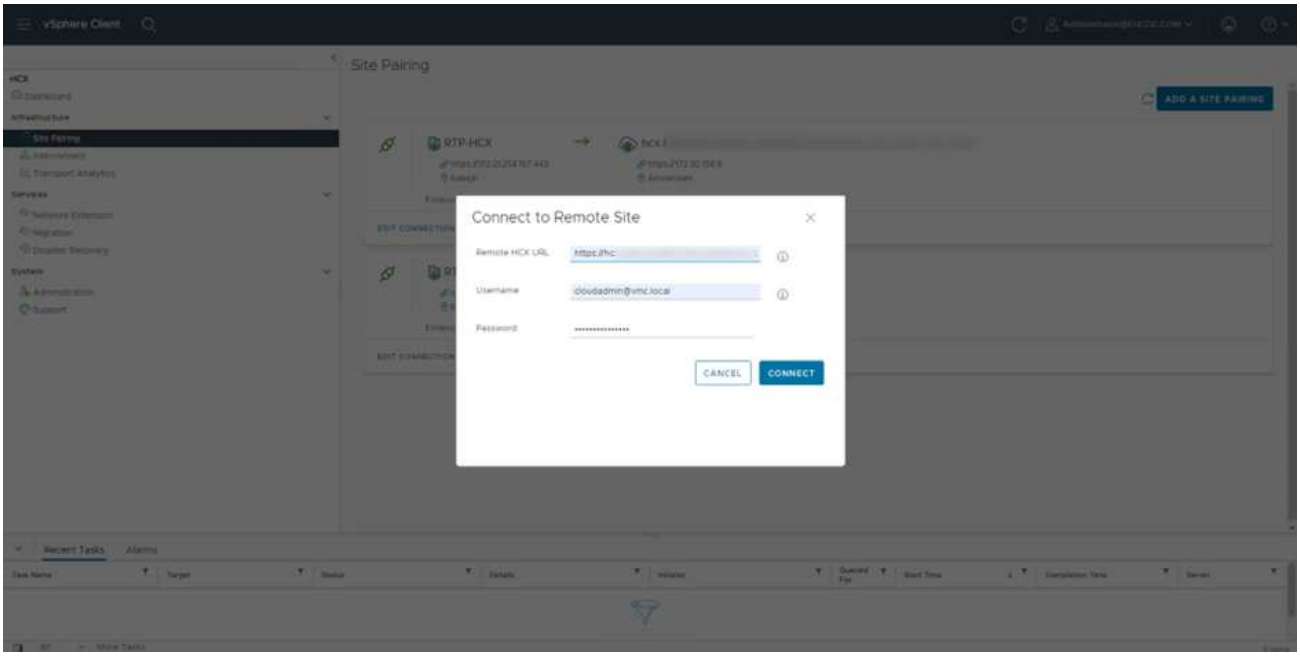


2. [インフラストラクチャ] の下で、[サイト ペアリングの追加] をクリックします。リモート サイトを認証するには、VMC HCX Cloud Manager の URL または IP アドレスと、CloudAdmin ロールの資格情報を入力します。



HCX 情報は、SDDC 設定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 コネクタは、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 ダッシュボードで利用できるようになります。

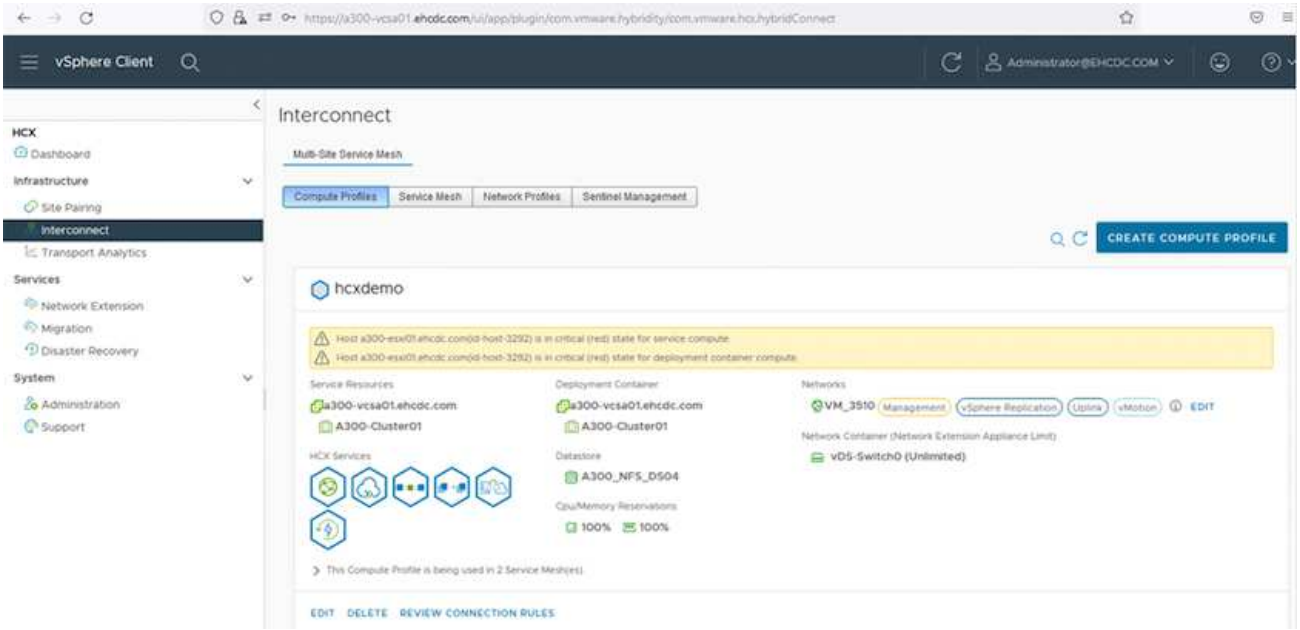
▼ ステップ**5:** ネットワークプロファイル、コンピューティングプロファイル、サービスメッシュを構成する

VMware HCX Interconnect (HCX-IX) アプライアンスは、インターネット経由の安全なトンネル機能と、レプリケーションおよび vMotion ベースの機能を有効にするターゲット サイトへのプライベート接続を提供します。相互接続により、暗号化、トラフィック エンジニアリング、SD-WAN が提供されます。 HCI-IX 相互接続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] で、[相互接続] > [マルチサイト サービス メッシュ] > [コンピューティング プロファイル] > [コンピューティング プロファイルの作成] を選択します。

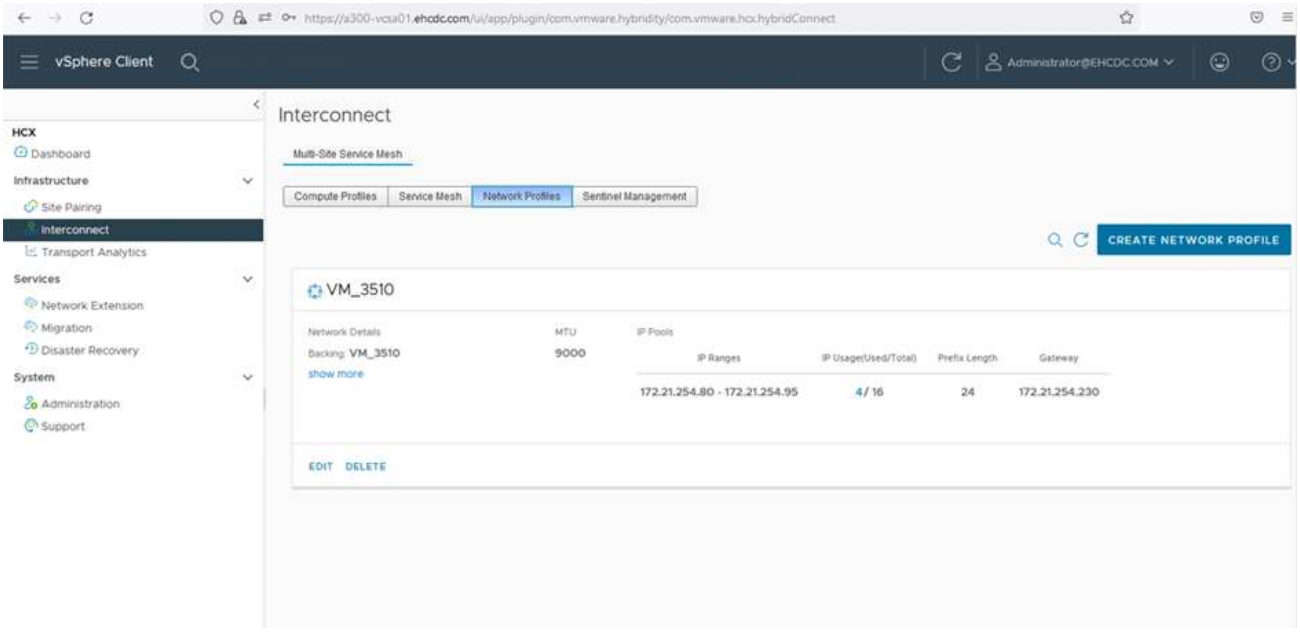
   コンピューティング プロファイルには、相互接続仮想アプライアンスの展開に必要なコンピューティング、ストレージ、およびネットワーク展開パラメータが含まれています。また、VMware データセンターのどの部分が HCX サービスにアクセス可能になるかを指定します。

   詳しい手順については、 "コンピューティングプロファイルの作成" 。



2. コンピューティング プロファイルが作成されたら、[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。
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 アドレスが必要になります。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。

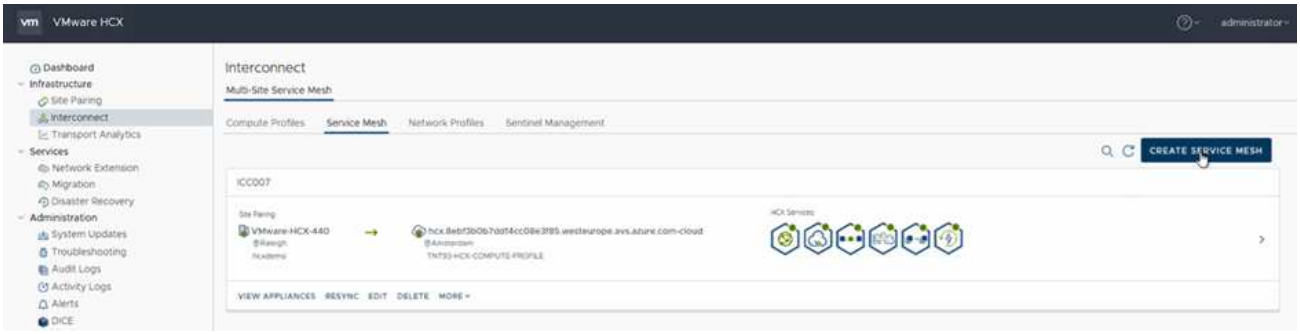


詳しい手順については、 "ネットワークプロファイルの作成" 。

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。

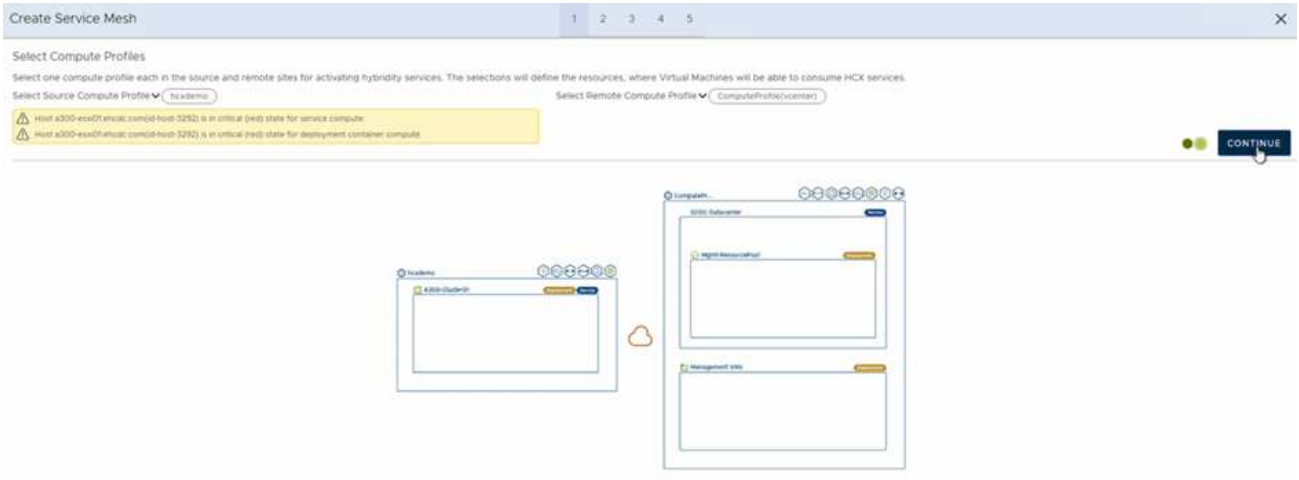
4. サービス メッシュを作成するには、[相互接続] オプション内の [サービス メッシュ] タブを選択し、オンプレミスと VMC SDDC サイトを選択します。

   サービス メッシュは、ローカルおよびリモートのコンピューティングとネットワーク プロファイルのペアを確立します。

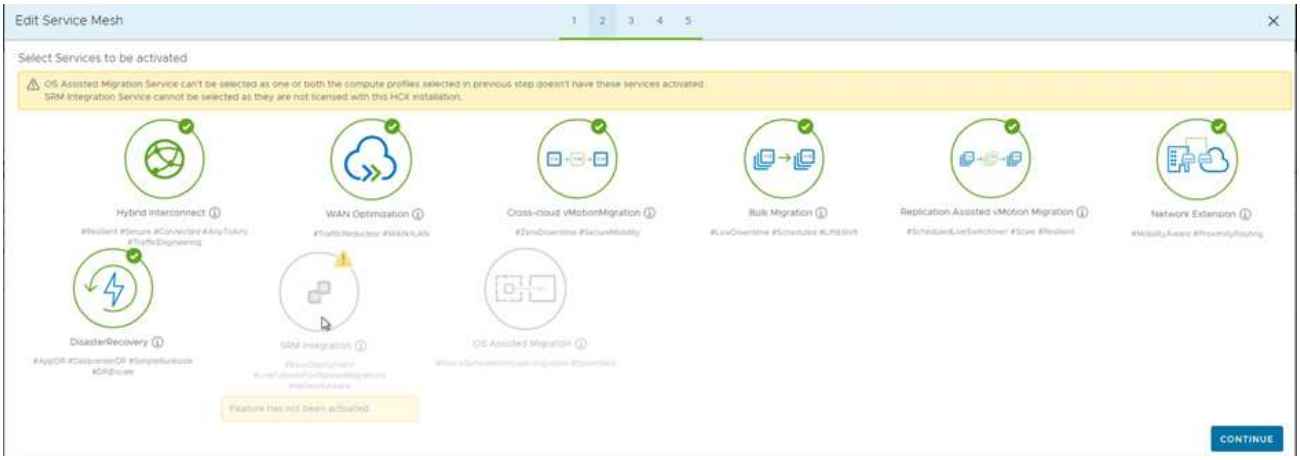


このプロセスには、ソース サイトとターゲット サイトの両方で自動的に構成される HCX アプライアンスの導入が含まれ、安全なトランスポート ファブリックが作成されます。

5. ソースおよびリモート コンピューティング プロファイルを選択し、[続行] をクリックします。

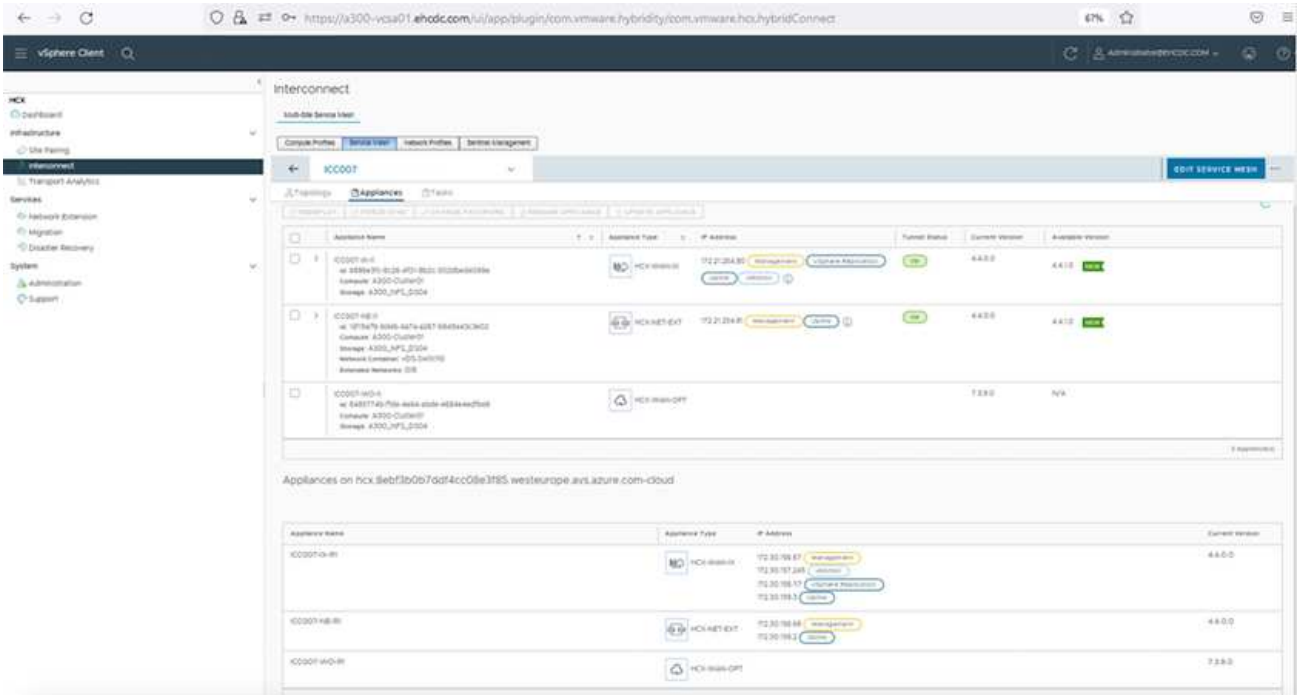


6. 有効にするサービスを選択し、「続行」をクリックします。



> レプリケーション アシスト vMotion 移行、SRM 統合、および OS アシスト移行には、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。展開が完了するまでに約 30 分かかります。サービス メッシュが構成されると、ワークロード VM の移行に必要な仮想インフラストラクチャとネットワークが作成されます。



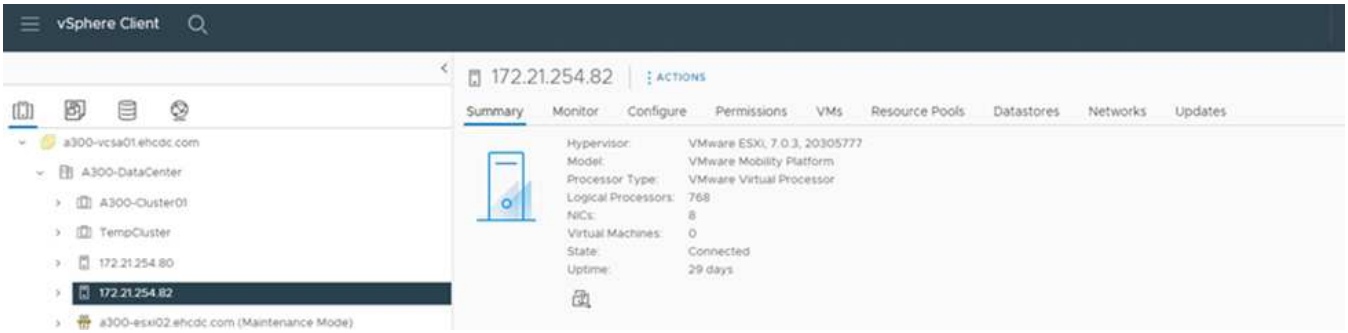
▼ ステップ**6:** ワークロードの移行

HCX は、オンプレミスや VMC SDDC などの 2 つ以上の異なる環境間の双方向の移行サービスを提供します。アプリケーション ワークロードは、HCX 一括移行、HCX vMotion、HCX コールド移行、HCX レプリケーション アシスト vMotion (HCX Enterprise エディションで利用可能)、HCX OS アシスト移行 (HCX Enterprise エディションで利用可能) などのさまざまな移行テクノロジーを使用して、HCX がアクティブ化されたサイト間で移行できます。

利用可能なHCX移行テクノロジーの詳細については、以下を参照してください。 "VMware HCX 移行の種類"

HCX-IX アプライアンスは、Mobility Agent サービスを使用して、vMotion、Cold、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 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上の実際の消費量を表すものではありません。



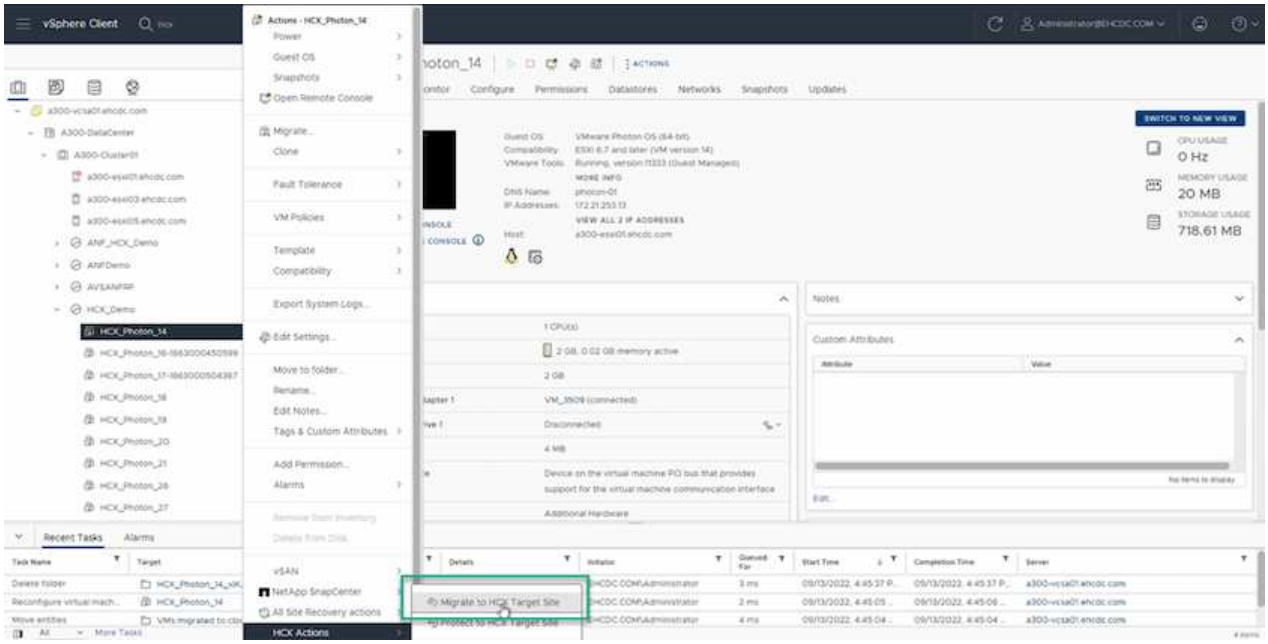
▼ **VMware HCX vMotion**

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ーは、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

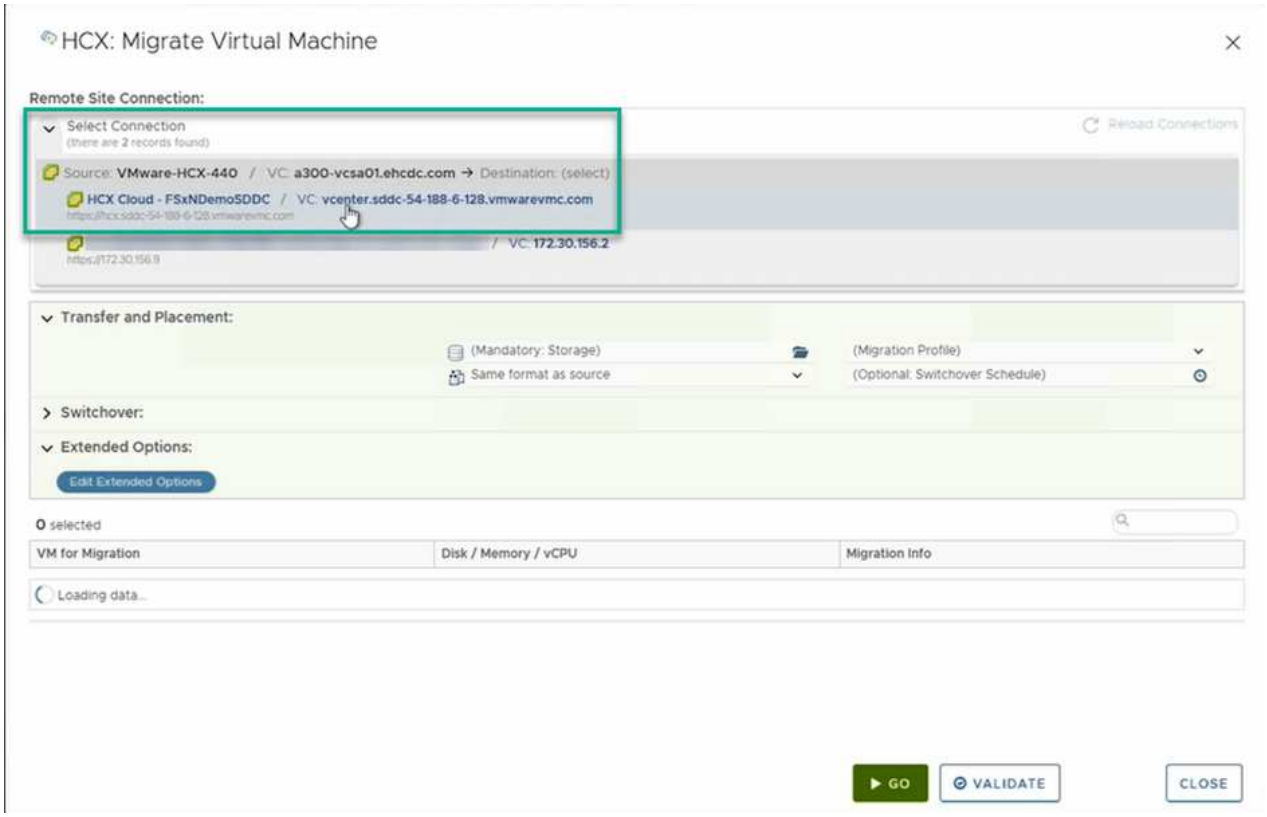
ンは、一度に 1 つの VM の VM 状態を移行するために使用されます。この移行方法ではサービスの中断は発生しません。

IP アドレスを変更せずに VM を移行するには、ネットワーク拡張機能 (VM が接続されているポート グループに対して) が配置されている必要があります。

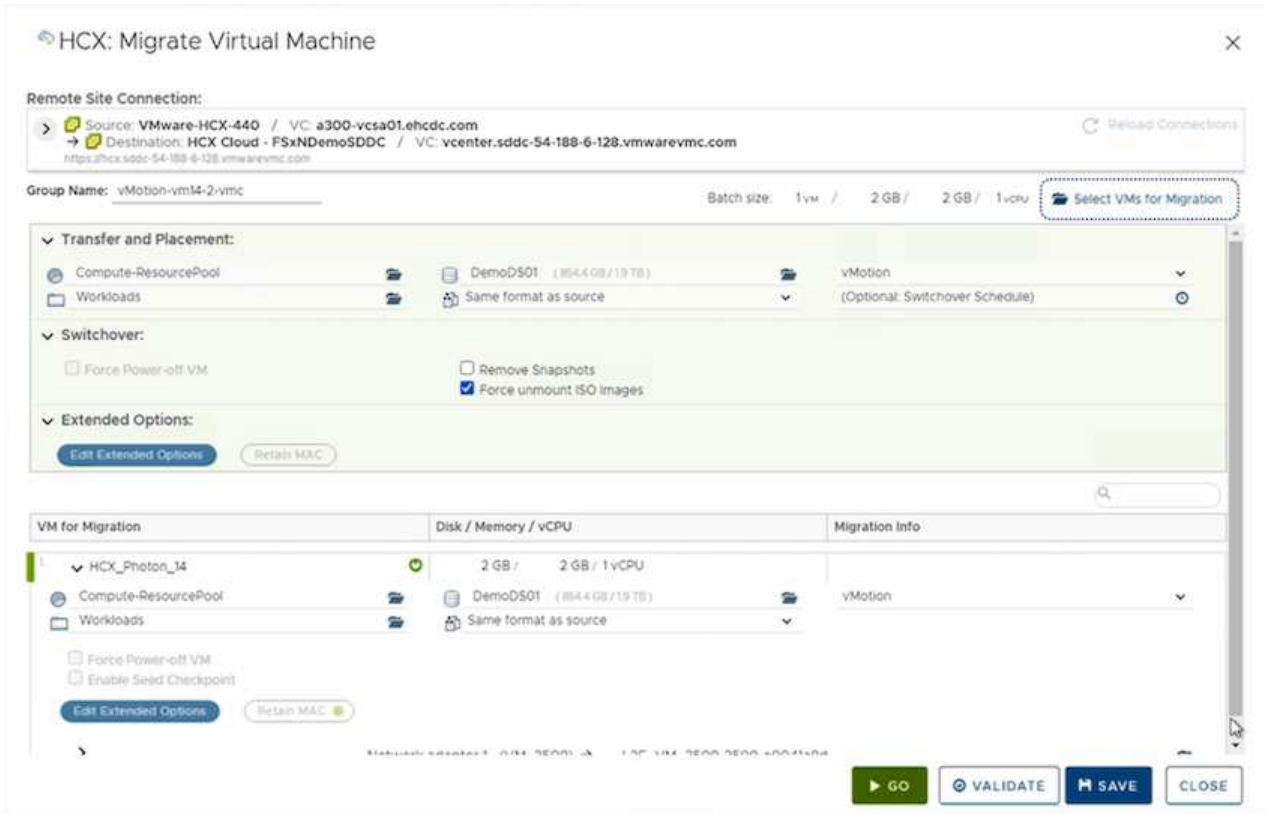
1. オンプレミスの vSphere クライアントから [インベントリ] に移動し、移行する VM を右クリックして、[HCX アクション] > [HCX ターゲット サイトに移行] を選択します。



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。



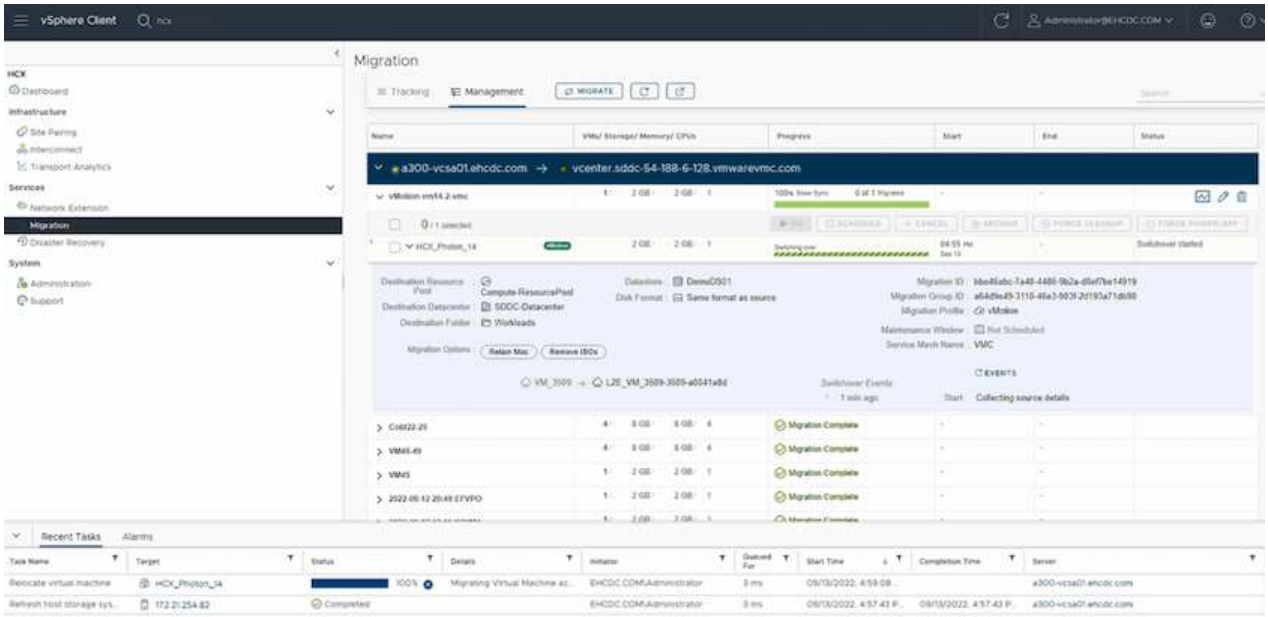
3. グループ名を追加し、「転送と配置」の下で必須フィールド (クラスター、ストレージ、および宛先ネットワーク) を更新し、「検証」をクリックします。



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 転送では、VM のアクティブ メモリ、実行状態、IP アドレス、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、以下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の理解" 。

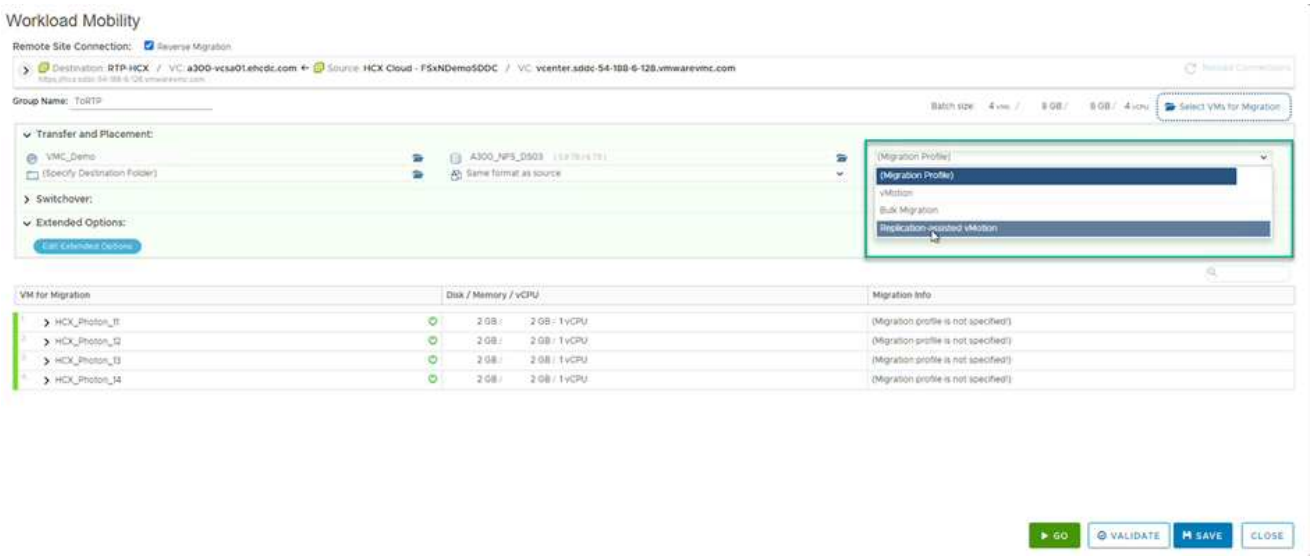
5. HCX > 移行ダッシュボードから、vMotion の進行状況と完了を監視できます。



▼ **VMware** レプリケーション アシスト **vMotion**

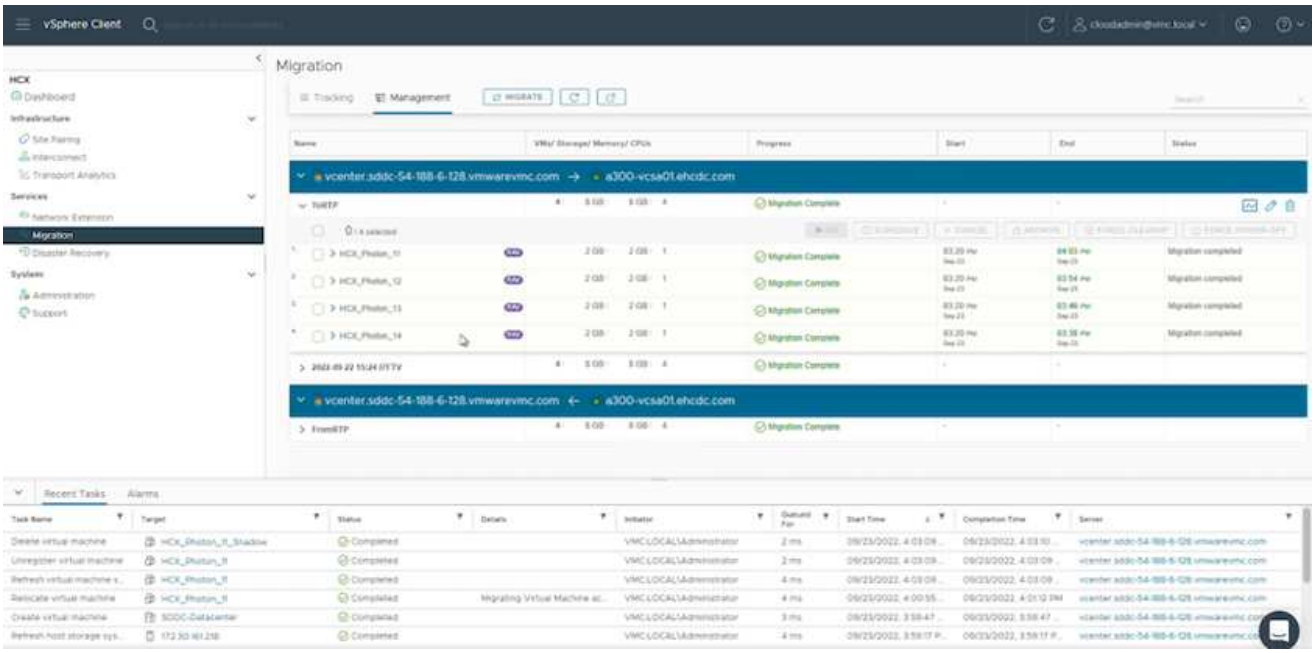
VMware のドキュメントからお気づきかもしれませんが、VMware HCX Replication Assisted vMotion (RAV) は、一括移行と vMotion の利点を兼ね備えています。一括移行では、vSphere Replication を使用して複数の VM を並行して移行します。VM は切り替え中に再起動されます。 HCX vMotion はダウンタイムなしで移行しますが、レプリケーション グループ内の VM が 1 つずつ順番に実行されます。 RAV は VM を並列に複製し、切り替えウィンドウまで同期を維持します。切り替えプロセス中は、VM のダウンタイムなしで一度に 1 つの VM が移行されます。

次のスクリーンショットは、Replication Assisted vMotion としての移行プロファイルを示しています。



少数の VM の vMotion と比較すると、レプリケーションの期間は長くなる可能性があります。 RAV で

は、デルタのみを同期し、メモリの内容を含めます。以下は移行ステータスのスクリーンショットです。移行の開始時刻は同じですが、終了時刻が各 VM ごとに異なることがわかります。



HCX 移行オプションと、HCX を使用してオンプレミスから VMware Cloud on AWS にワークロードを移行する方法の詳細については、 "VMware HCX ユーザーガイド" 。

VMware HCX vMotion には 100Mbps 以上のスループット機能が必要です。

ターゲット VMC FSx ONTAPデータストアには、移行に対応できる十分なスペースが必要です。

まとめ

オールクラウドまたはハイブリッドクラウドをターゲットにしていて、データがオンプレミスのあらゆるタイプ/ベンダーのストレージに存在する場合でも、 Amazon FSx ONTAPと HCX を組み合わせることで、データ要件をアプリケーション層にシームレスにすることで TCO を削減しながらワークロードをデプロイおよび移行するための優れたオプションが得られます。ユースケースに関係なく、VMC と FSx ONTAPデータストアを併せて選択すると、クラウドのメリットの迅速な実現、オンプレミスと複数のクラウドにわたる一貫したインフラストラクチャと運用、ワークロードの双方向の移植性、エンタープライズ グレードの容量とパフォーマンスが実現します。これは、ストレージを接続し、VMware vSphere レプリケーション、VMware vMotion、または NFC コピーを使用して VM を移行するために使用される、使い慣れたプロセスと手順と同じです。

まとめ

このドキュメントの主なポイントは次のとおりです。

- VMC SDDC でAmazon FSx ONTAP をデータストアとして使用できるようになりました。
- FSx ONTAPデータストアで稼働しているVMCに、オンプレミスのデータセンターからデータを簡単に移行できます。
- 移行アクティビティ中の容量とパフォーマンスの要件を満たすために、FSx ONTAPデータストアを簡単に拡大および縮小できます。

詳細情報の入手方法

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

- VMware Cloud ドキュメント

  "https://docs.vmware.com/en/VMware-Cloud-on-AWS/"

- Amazon FSx ONTAPドキュメント

  "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"

  VMware HCX ユーザーガイド

- "https://techdocs.broadcom.com/us/en/vmware-cis/hcx/vmware-hcx/4-10/vmware-hcx-user-guide-4-10.html"

AWS / EVS 向けNetApp

FSx ONTAPをEVSの外部データストアとしてマウントする

Amazon FSx for NetApp ONTAP を**Amazon Elastic VMware Service** の外部データストアとしてマウントする方法

このドキュメントでは、FSx for ONTAPファイルシステムを作成し、Amazon EVS で使用するために Internet Small Computer System Interface (iSCSI) または Network File System (NFS) データストアとして使用するために接続するための詳細な手順を説明します。

はじめに

オンプレミスの VMware に既に投資している組織は、AWS でコピーを移行、バースト、拡張、または保護 (バックアップ、災害復旧) することで、効率的かつコスト効率の高い方法で展開を最新化することを模索しており、いくつかの課題に直面しています。 Amazon Elastic VMware Service (Amazon EVS) のリリースにより、Amazon Virtual Private Cloud (VPC) で VMware Cloud Foundation (VCF) を直接実行できるネイティブ AWS サービスが提供されるようになりました。

Amazon EVS を使用すると、既存の VCF デプロイメントを AWS に拡張し、ピーク使用時にパフォーマンスを拡張するために AWS にバーストし、AWS 上で VCF ワークロードを完全に実行して、近代化、データセンターの撤退、統合、その他のユースケースを促進することが可能になります。

Amazon EVS は大きなメリットをもたらしますが、デフォルトのハイパーコンバージドアーキテクチャではコンピューティングとストレージが結合されているため、ビジネスニーズに応じて一方を独立して拡張することはできません。今日のデータ中心の世界では、多くの組織においてストレージの需要がコンピューティングの需要よりも高くなっています。ただし、VMware ハイパーコンバージド アーキテクチャでは、ストレージ リソースがコンピューティング リソースと結合されます。つまり、ストレージの拡張は、決して使用されないコンピューティング ホストを追加することによってのみ実行できます。これは、特にストレージを多用するワークロードでは、コストが大幅に上昇する可能性がある状況です。

この問題を解決するために、AWS とNetApp は、Amazon EVS の外部ストレージサービスとしてAmazon FSx for NetApp ONTAP (FSx for ONTAP) を提供しています。 FSx for ONTAPは、 NetApp ONTAPソフトウェアの高パフォーマンス、データ復元力、コスト効率の機能を実現する AWS ネイティブのストレージサービスで

す。 FSx for ONTAP を外部ストレージとして使用することで、Amazon EVS ユーザーはコンピューティング リソースとストレージ リソースを個別に拡張でき、総所有コスト (TCO) を最適化できます。

概要

このドキュメントでは、FSx for ONTAPファイルシステムを作成し、Amazon EVS で使用するために Internet Small Computer System Interface (iSCSI) または Network File System (NFS) データストアとして使用するために接続するための詳細な手順を説明します。

このガイドの目的

このガイドでは、Amazon EVS 用の FSx for ONTAPデータストアを設定する方法のほか、ベストプラクティス、サポート要件、サイズに関する考慮事項、および統合の計画、設計、実装に役立つその他の情報について説明します。

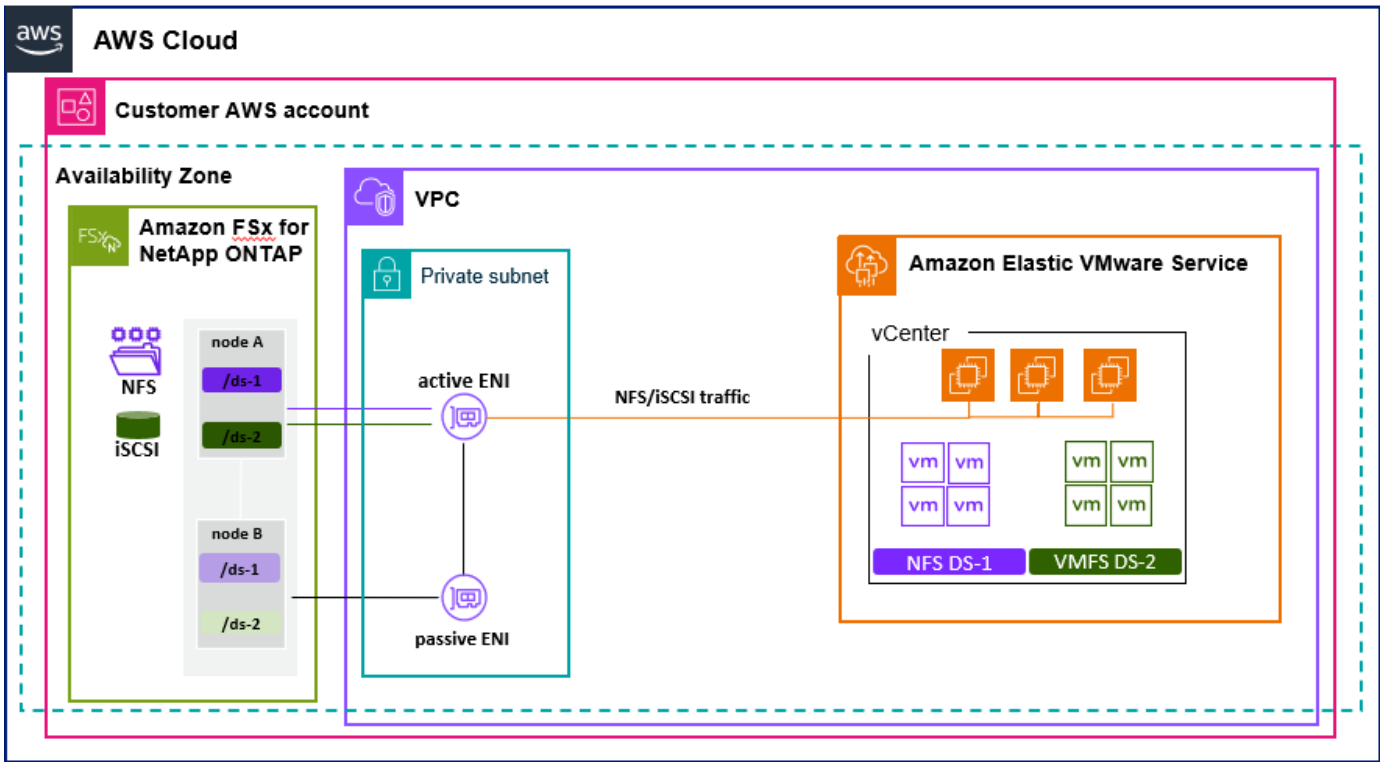
観客

このチュートリアルは、VMware vSphere、Amazon EVS、AWS コンソール、FSx for ONTAPに精通しているクラウドアーキテクトおよびクラウド管理者を対象としています。

高レベルアーキテクチャ

このセクションでは、FSx for ONTAP をAmazon EVS のデータストアとして使用するためのソリューション アーキテクチャの概要を説明します。

以下に、AWS VPC 内の Amazon EVS 環境を備えた FSx for ONTAPデータストアのアーキテクチャの概要を示します。



FSx for ONTAP をNFS データストアとして使用するための導入手順

このセクションでは、FSx for ONTAP をNFS データストアとして導入する手順を説明します。 iSCSI データストアを展開する手順については、次のセクションで詳しく説明します。

大まかな展開手順

Amazon EVS の NFS データストアとして使用するために FSx for ONTAPファイルシステムをデプロイし、2つのサービス間の接続を確立するには、次の手順を実行します。

- Amazon EVS VCF 環境が配置されているのと同じ VPC に FSx for ONTAPファイルシステムをセットアップします。
- セキュリティ グループとルーティング テーブルを検証しています。
- Amazon EVS の NFS データストアとして使用するために FSx for ONTAPストレージボリュームを接続します。

前提条件

FSx for ONTAP をAmazon EVS の NFS データストアとしてセットアップするプロセスを開始する前に、次の前提条件を満たしている必要があります。

- Amazon EVS 仮想化環境。詳細については、次のドキュメントを参照してください。"Amazon EVS 入門ガイド" 。
- 適切な SSD ストレージ容量、プロビジョニングされた IOPS およびスループットを備えた、 ONTAP用のシングル アベイラビリティ ゾーン (AZ) FSx を作成します。
- 最適なパフォーマンスを得るには、FSx for ONTAPファイルシステムを Amazon EVS インスタンスと同じ VPC 内に配置します。 FSx for ONTAPが別の VPC にデプロイされている場合にも、VPC ピアリングがサポートされることに注意してください。
- パフォーマンス要件に基づいて、Single-AZ FSx for ONTAPファイル システムに必要な適切な IOPS とスループットを選択します。見る"FSx for ONTAPのパフォーマンス仕様の詳細"利用可能な各オプションが提供するスループットと IOPS を理解します。

> このガイドでは、FSx for ONTAPファイル システムをサービス アクセス サブネットと同じサブネットにデプロイします。

Amazon EVS 仮想化環境が VPC にデプロイされたら、NFS データストアとして使用される Single-AZ FSx for ONTAPファイルシステムのセットアップに進むことができます。

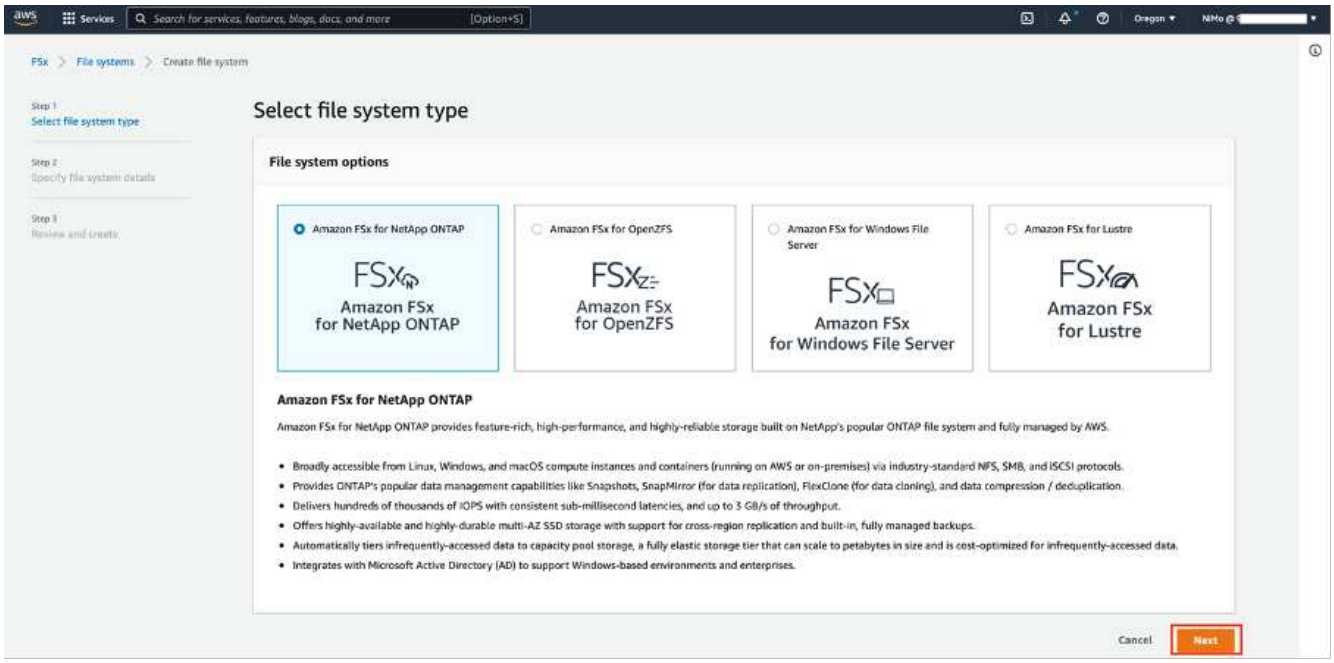
> FSx for ONTAPファイルシステムは、Amazon EVS SDDC と同じ AZ にデプロイする必要があります。

FSx for ONTAPファイルシステムを作成する

次の手順では、FSx for ONTAPファイル システムをプロビジョニングおよびマウントする方法を示します。

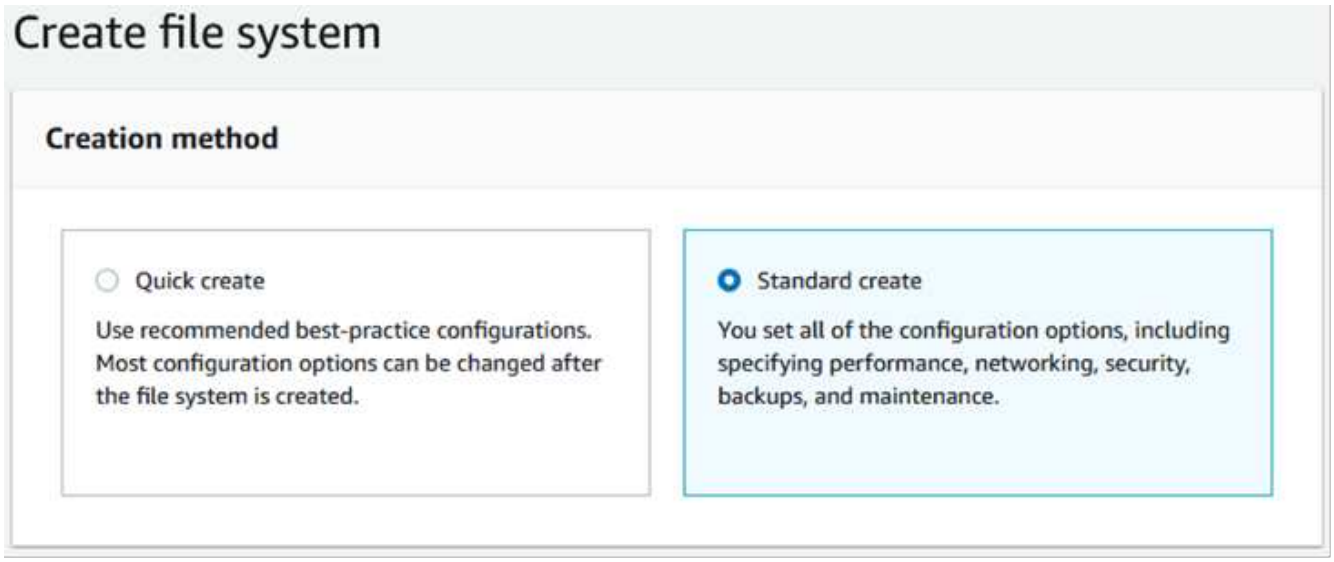
1. Amazon FSxコンソールへアクセスしてください `https://console.aws.amazon.com/fsx/`インターネット ブラウザを使用して、資格情報でサインインします。

2. コンソールで、「ファイル システムの作成」を選択します。これにより、FSx for ONTAPファイル システムを作成するためのセットアップ ウィザードが開始されます。
3. まず、ファイルシステムの種類を選択します。利用可能なファイルシステムオプションから「Amazon FSx for NetApp ONTAP」を選択し、「次へ」ボタンをクリックして続行します。

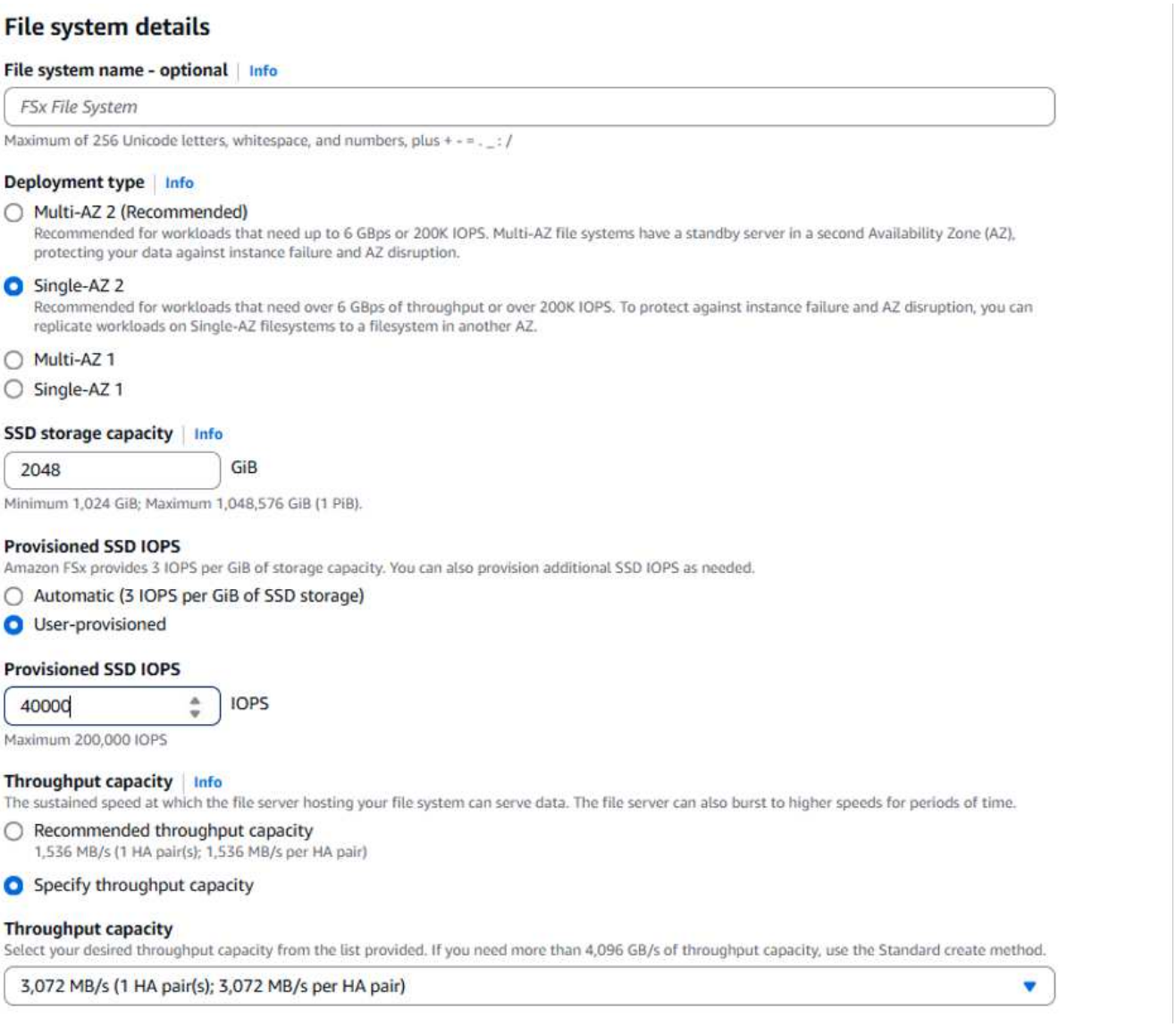


4. クイック作成オプションと標準作成オプションのどちらかを選択できます。クイック作成では事前定義された構成が提供され、標準作成では独自の構成を定義できます。

「標準作成」オプションを選択します。

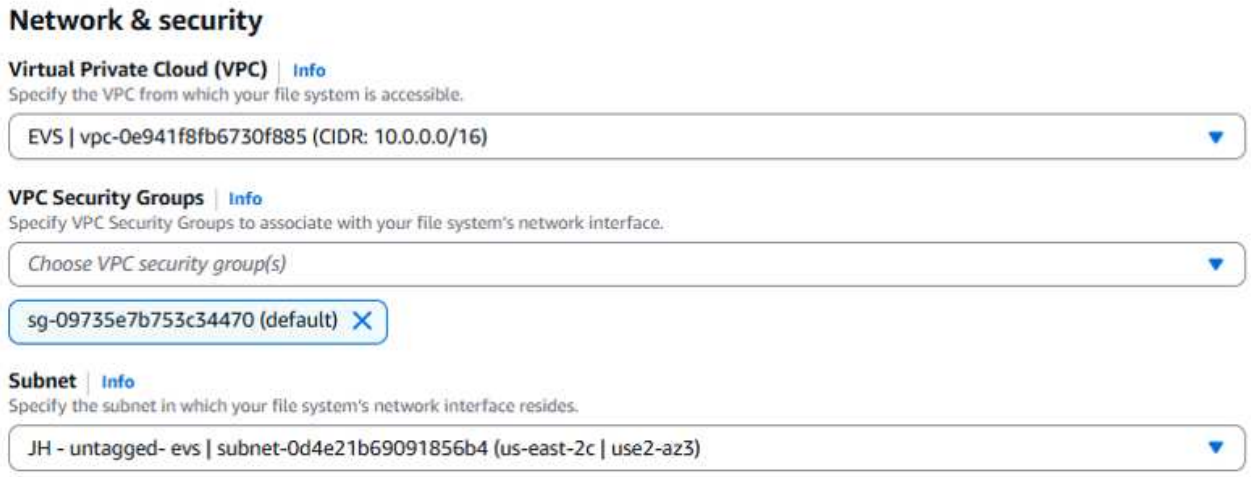


これで、標準のファイル システム作成セットアップ ウィザードが起動します。ファイル システムの詳細ページで、次の画像に示すのと同じ情報を選択して入力します。



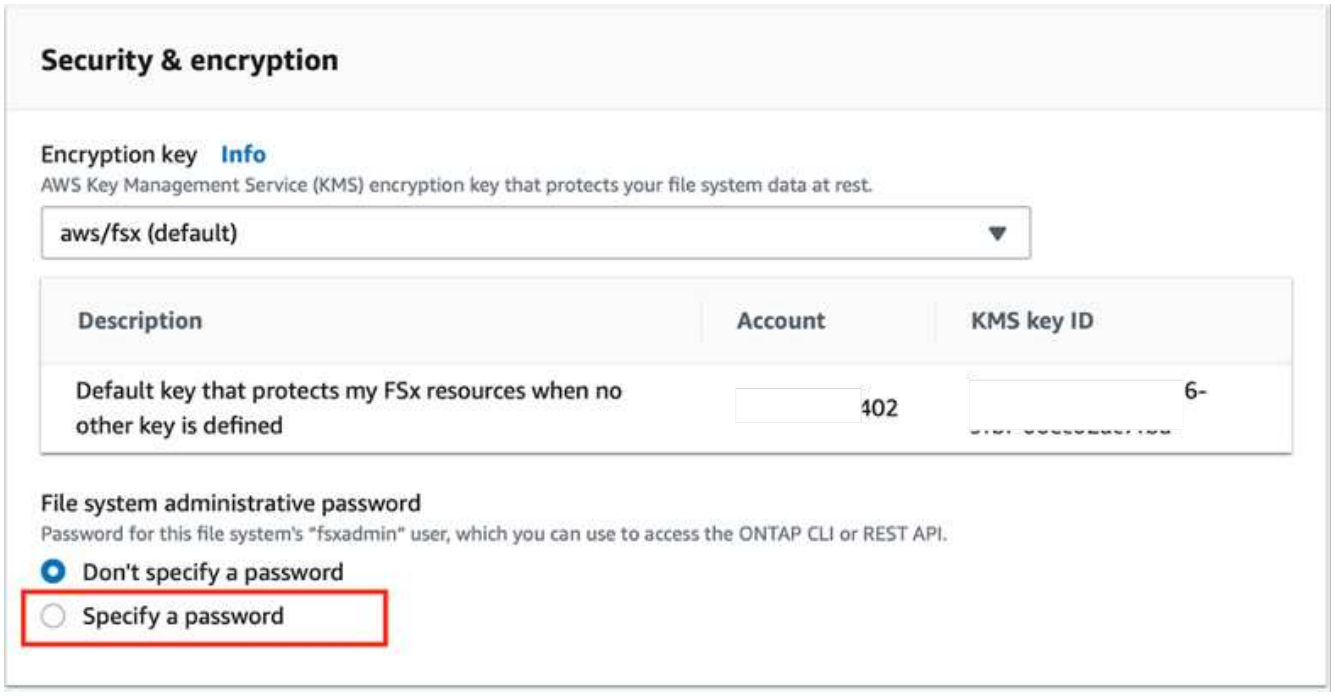
5. 「ネットワークとセキュリティ」というセクションまで下にスクロールします。このセクションでは、サブネットと VPC の詳細を設定します。このガイドでは、ドロップダウン メニューから「EVS-VPC」を選択し、EVS 仮想環境のサブネットとしてサービス アクセス サブネット (タグなし VLAN) を選択しました。

> ⓘ サブネットは、VPC 内のタグなしのプライベート サブネットにすることができます。適切なルーティングが設定されている限り、VPC ピアリング経由で接続された別の VPC/サブネットに配置することもできます。

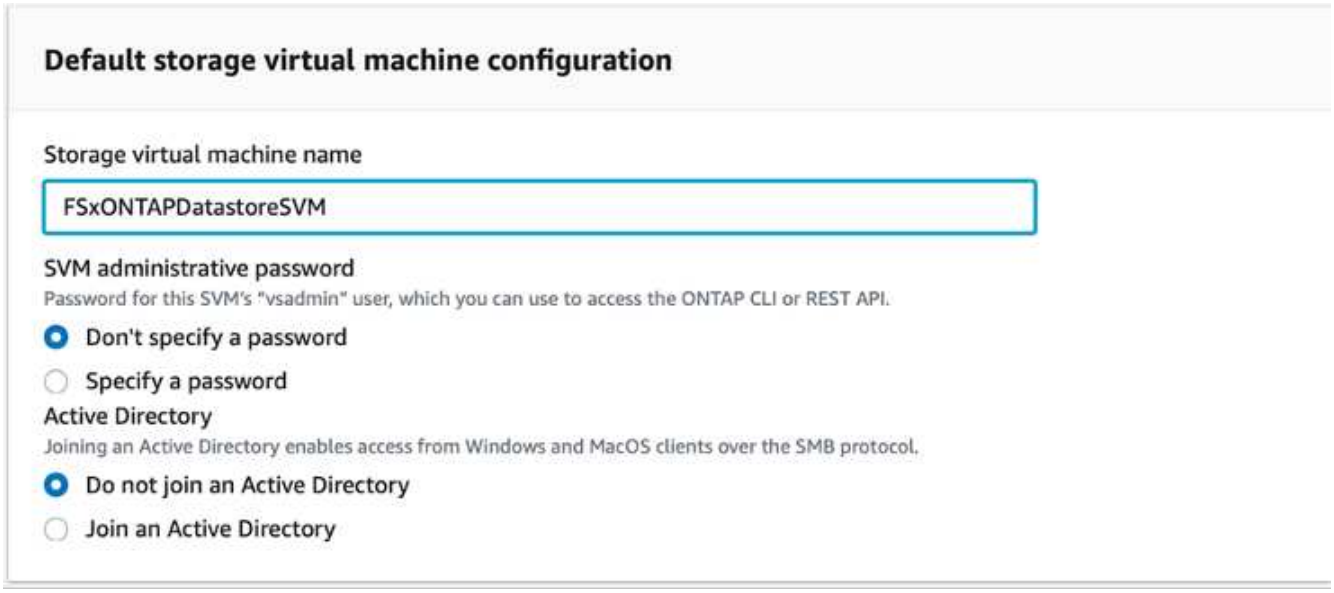


6. 下にスクロールすると、「セキュリティと暗号化」セクションがあります。ここで、ドロップダウン メニューから暗号化キーを選択します。これらのキーは AWS Key Management Service (AWS KMS) によって提供され、FSx for ONTAPファイルシステム内の保存データを保護します。

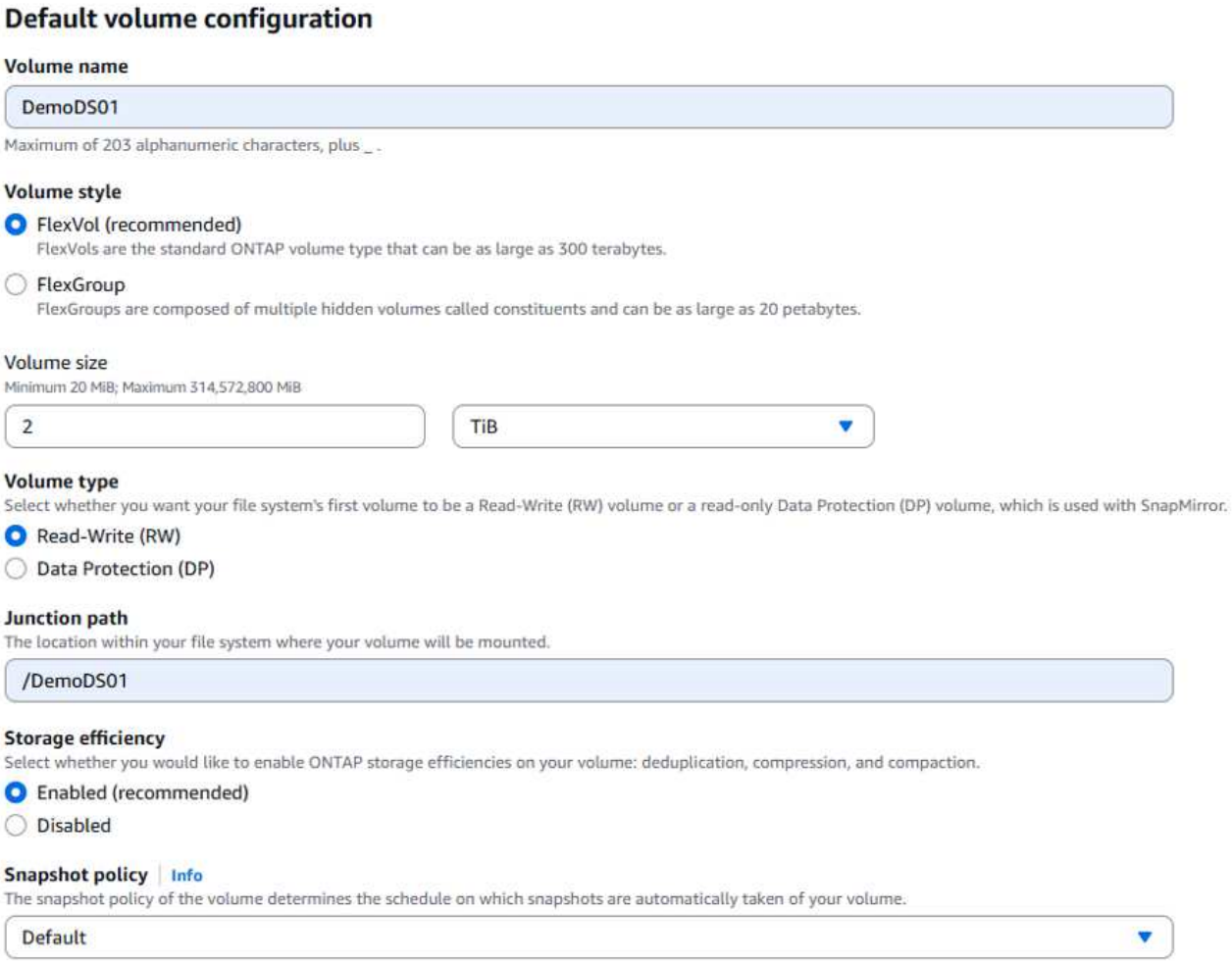
   次に、「ファイルシステム管理パスワード」設定で、ファイルシステムを管理する fsxadmin ユーザーの一意のパスワードを指定します。



7. 次に、「デフォルトのストレージ仮想マシン構成」というセクションまで下にスクロールします。ここで、ストレージ仮想マシン (SVM) の名前を指定する必要があります。

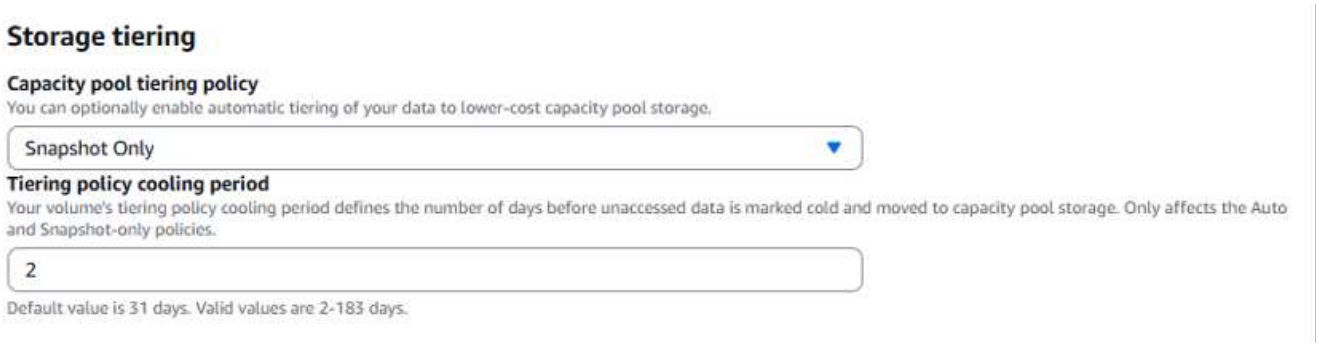


8. 次に、「デフォルトのボリューム構成」というセクションまで下にスクロールします。ここでボリュームの名前を指定し、ボリューム サイズを設定します。ボリューム プロトコルは NFS v3 (デフォルトで有効) である必要があります。オプションをクリックして、ストレージ効率機能 (圧縮、重複排除、圧縮) を有効にし、全体的なストレージ使用量とコストを削減します。



9. ストレージ階層化オプションでは、ドロップダウン メニューから「スナップショットのみ」を選択し、階

層化ポリシーの冷却期間を設定します。デフォルトは 31 日ですが、この例では 2 日間の冷却期間を設定します。

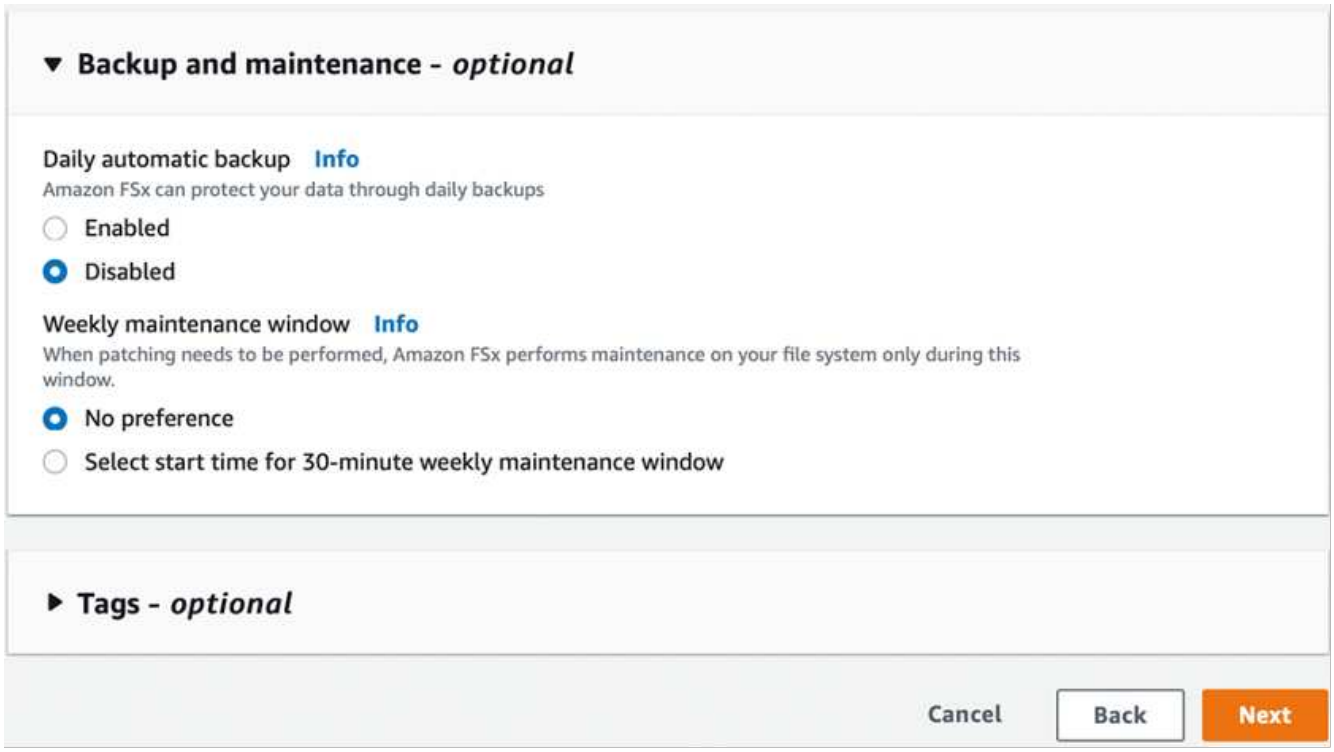


10. ボリュームを作成したら、 ONTAPコマンドライン インターフェイス (ONTAP CLI) を使用して次のパラメータを変更します。

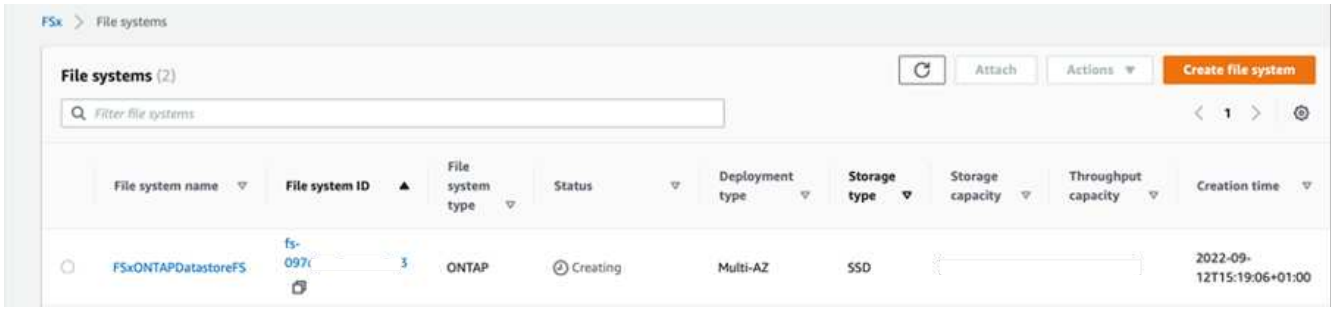
設定	構成
ボリューム ギャランティ	なし（シンプロビジョニング）
fractional_reserve	0%
snap_reserve	0%
自動サイズ調整	grow_shrink
ストレージ効率	有効
ボリューム階層化ポリシー	Snapshot のみ
アクセス時刻の更新 (-atime-update)	間違い
最小先読み (-min-readahead)	間違い
スナップショットポリシー	なし

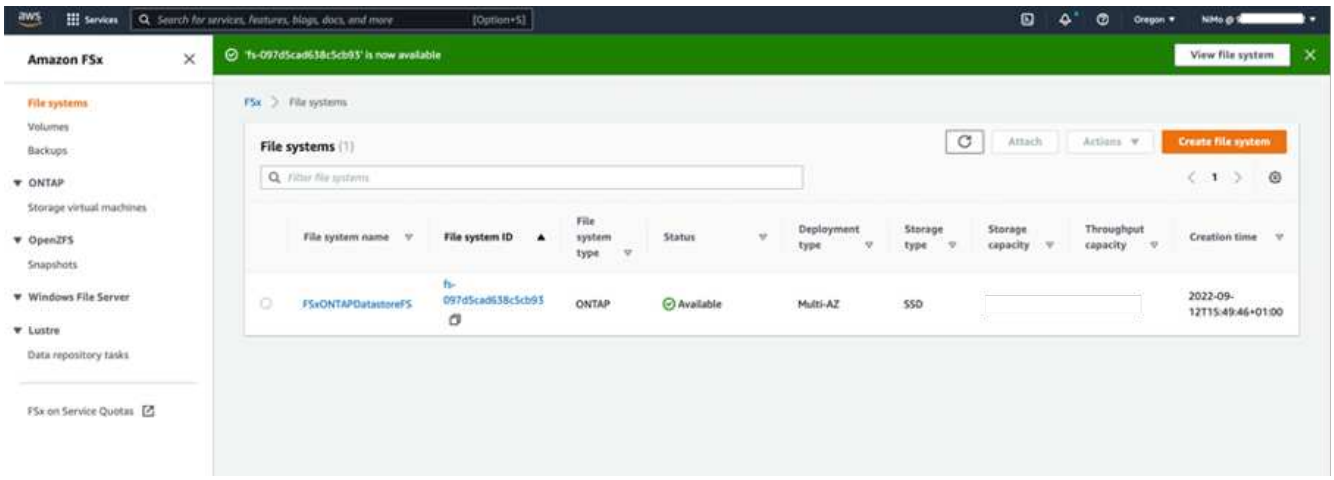
11. オプションの「バックアップとメンテナンス」手順で、毎日の自動バックアップを無効にし、毎週のメンテナンス ウィンドウに「優先なし」を選択します。

    完了したら「次へ」をクリックします。



12. 前の手順に従って設定したファイル システム構成全体の確認が行われます。すべてのパラメータが正しいことを確認し、「ファイルシステムの作成」ボタンをクリックしてセットアップを完了します。





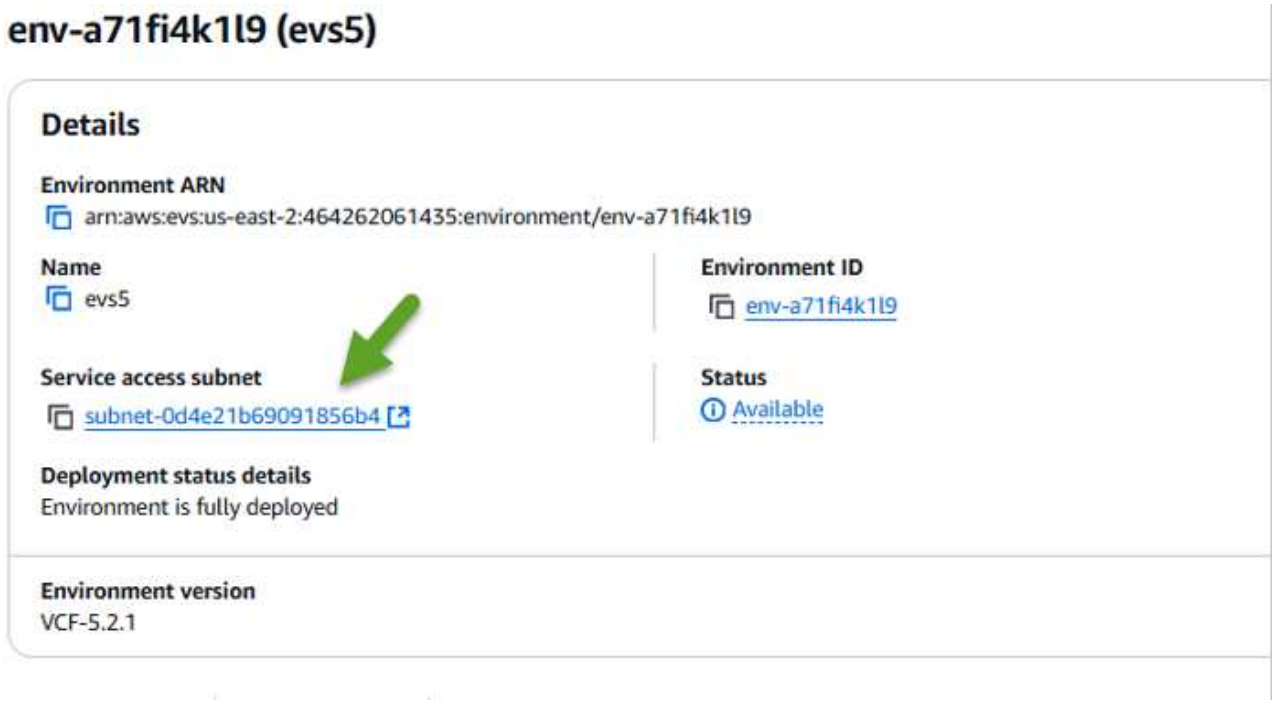
追加の FSx for ONTAPファイル システムを作成するには、上記の手順に従い、必要に応じてパフォーマンスとディスク容量に影響する値を調整します。 FSx for ONTAPのパフォーマンスオプションの詳細については、以下を参照してください。"このドキュメントページ"

。

VPC および仮想化環境のルーティングとセキュリティ グループの検証

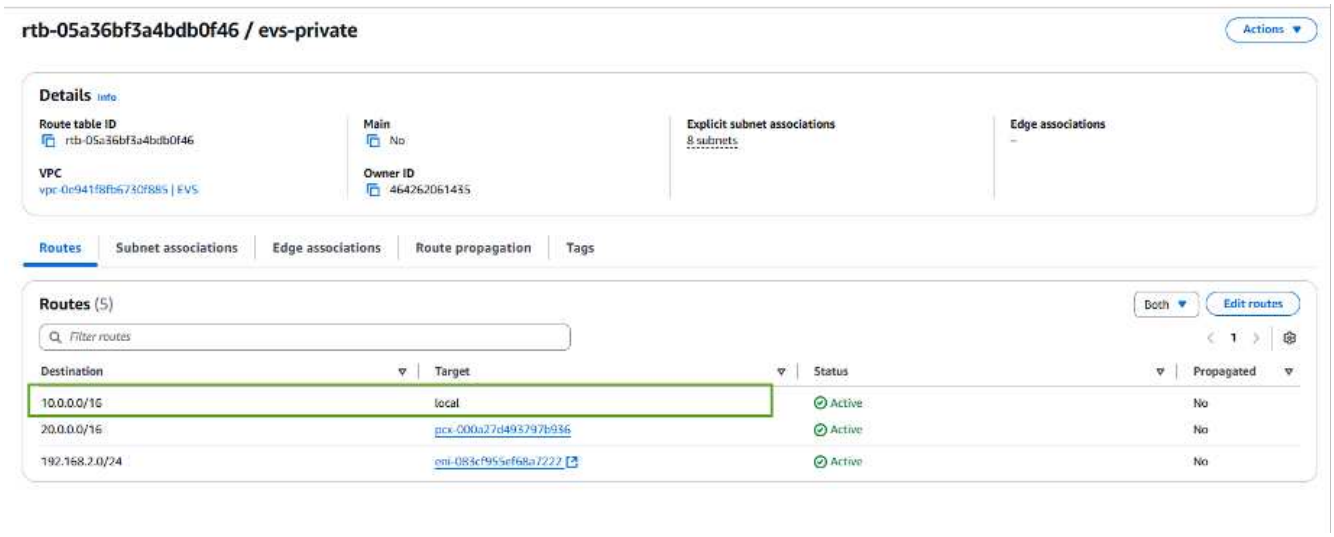
VPC および SDDC のルーティングとセキュリティ グループを検証することは、Amazon EVS 仮想化環境と FSx for ONTAPファイルシステム コンポーネントが適切に連携できることを確認するために重要です。

1. Elastic VMware サービス > 仮想化環境 > [Amazon EVS 環境] を参照し、以下の緑色の矢印で示されているように、サービス アクセス サブネットを選択します。



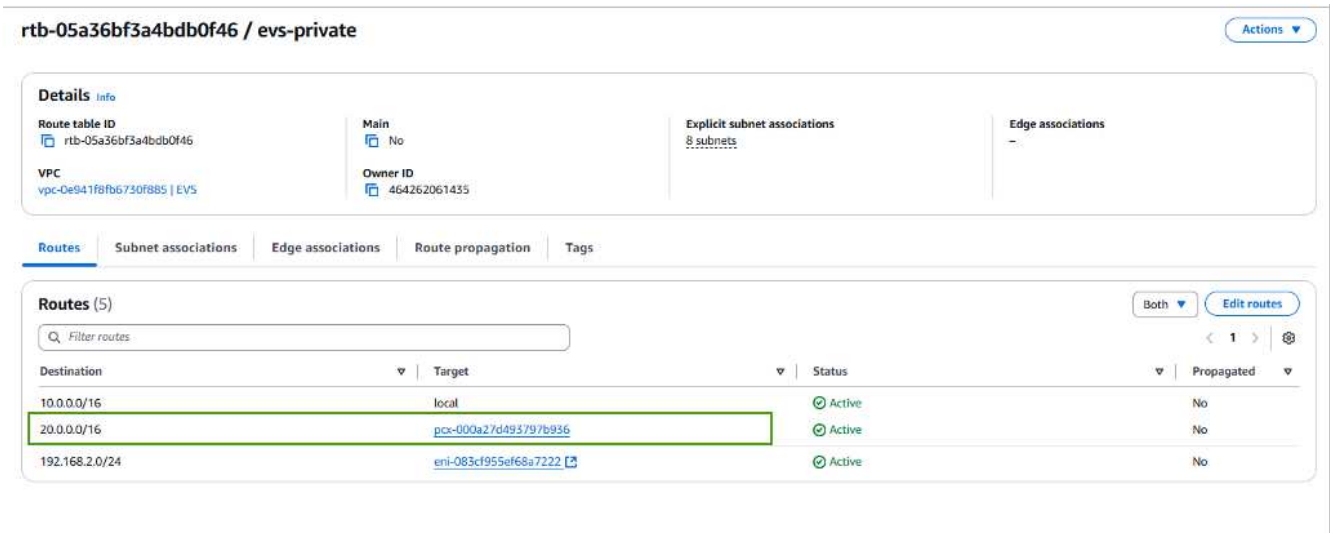
2. サブネット パネルが開きます。このパネルでルート テーブルを見つけてクリックします。

   この例では、FSxN ONTAPファイルシステムは Amazon EVS VCF 環境と同じ VPC 内にあるため、デフォルトのルートで十分です。



   FSx for ONTAPファイル システムが別の VPC にある場合は、その VPC へのルートが追加されていること

を確認します。この例では、FSx for ONTAPシステムが存在する VPC への VPC ピアリングのルートが追加されています。

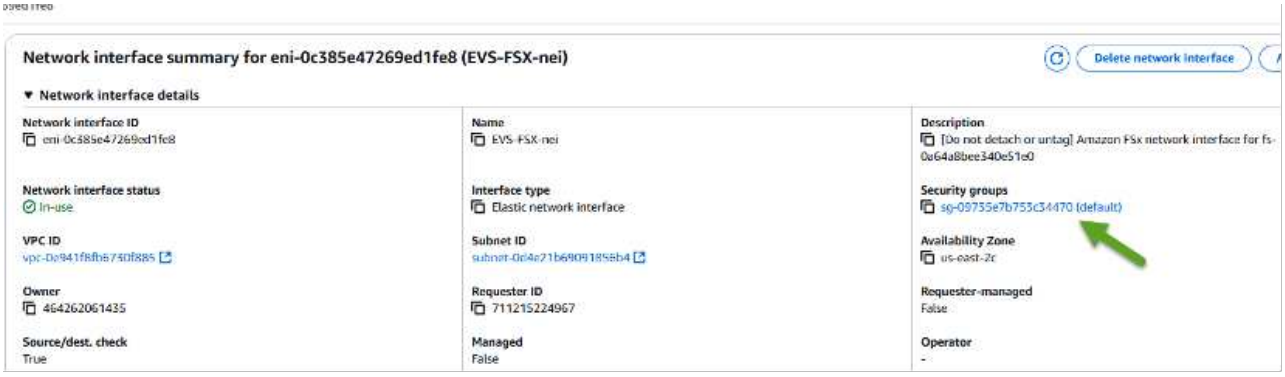


3. 次に、FSx for ONTAPファイル システムに接続されているセキュリティ グループ (つまり、Elastic Network Interface (ENI) に接続されているセキュリティ グループ) が NFS ポートへのアクセスを許可していることを確認する必要があります。

   NFSおよびiSCSIプロトコルポートの完全なリストについては、リンクhttps://docs.aws.amazon.com/fsx/latest/ONTAPGuide/limit-access-security-groups.html]Amazon VPCを使用したファイルシステムアクセスコントロールのドキュメントを参照してください。

   FSx for ONTAPファイル システムがセキュリティ グループに関連付けられていることを確認するには、次の手順を実行します。

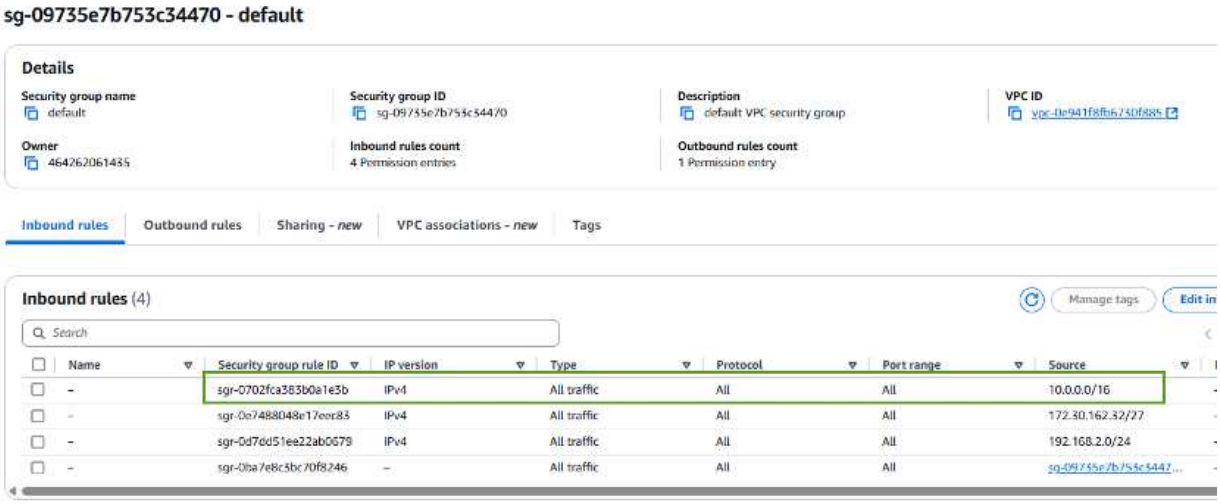
   a. AWS コンソールで、[FSx] > [ファイルシステム] > [FSx for ONTAPファイルシステム] に移動します。
   b. [ネットワークとセキュリティ] タブで、ENI をクリックします。
   c. ネットワーク インターフェイスの詳細の下にリストされている、ENI に関連付けられたセキュリティ グループを見つけます (下の画像では緑色の矢印で示されています)。



   d. ポートを検証します。次の画面に示す例では、すべてのトラフィックが許可されています。ただし、これらを NFS ポートのみに制限することもできます。ポートのリストは次のとおりです。

      - ポート 111 TCP: ポートマッパー。NFS 要求で使用されるポートをネゴシエートするために使用されます。

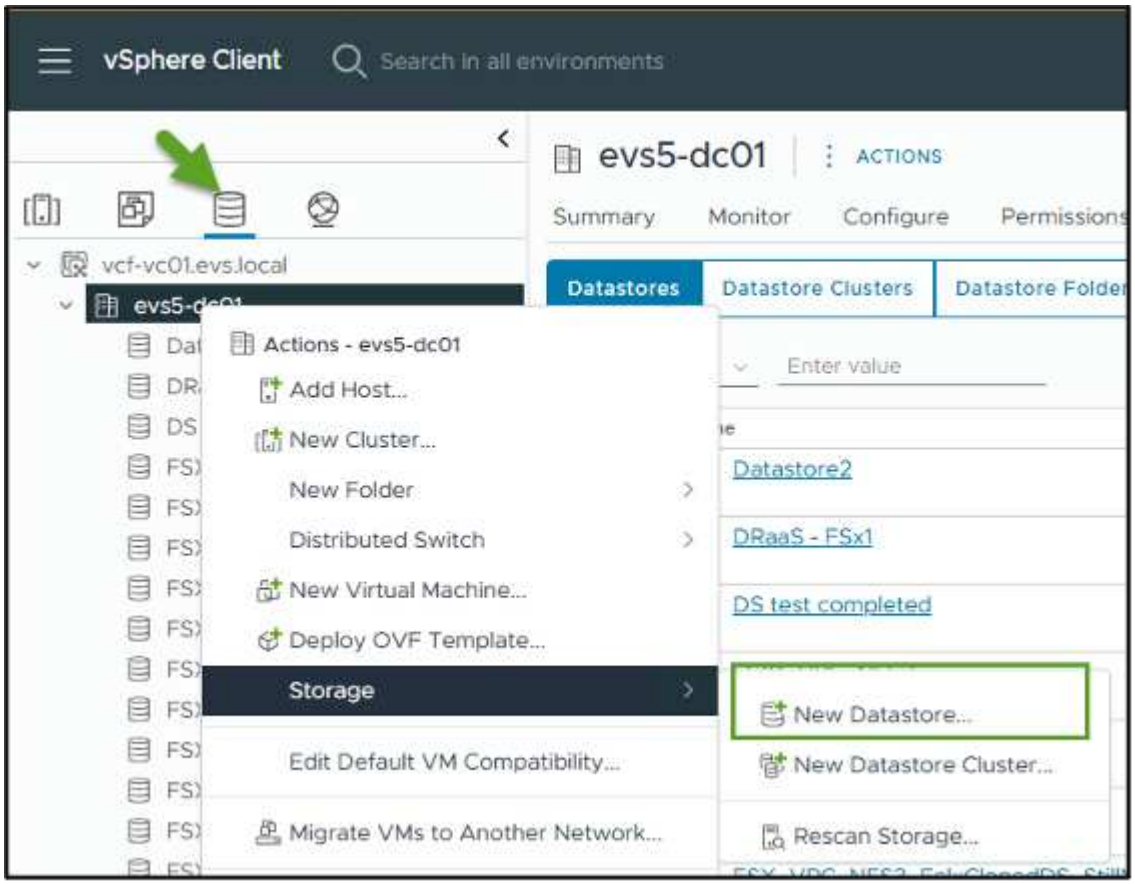
- ポート 635 TCP: 着信マウント要求を受信するための Mountd。
- ポート 2049 TCP: NFS。NFS トラフィックを処理します。
- ポート 4045 TCP: ロック要求を処理するネットワーク ロック マネージャー (NLM)。
- ポート 4046 TCP: ネットワーク ステータス モニター (NSM)。サーバーがロック管理のために再起動すると、NFS クライアントに通知を送信します。



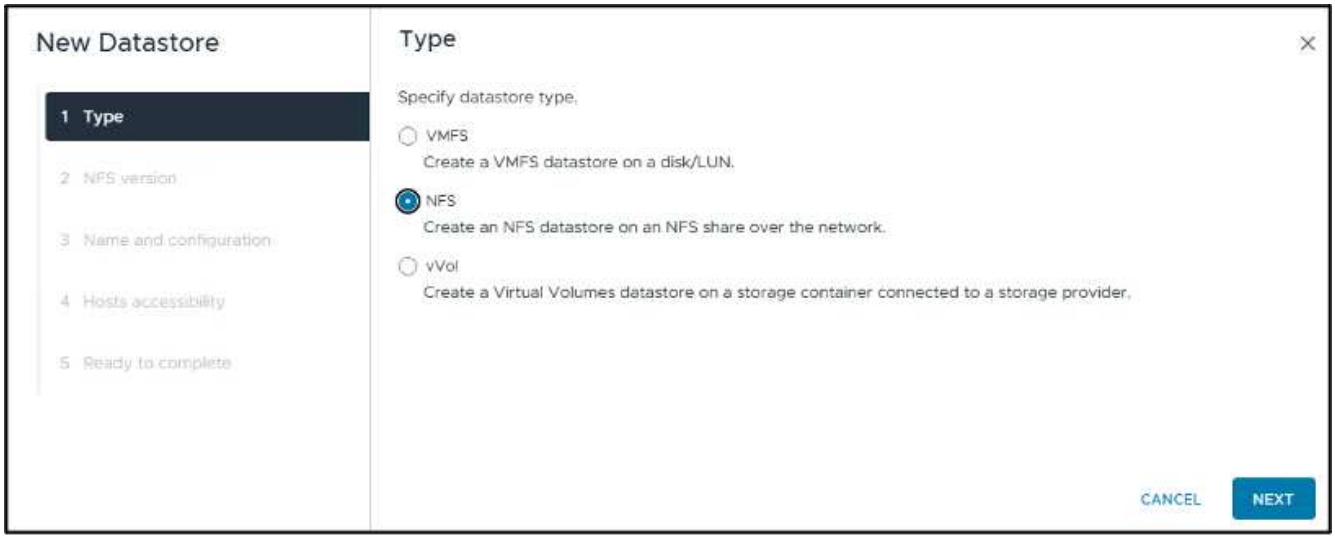
FSx for ONTAP NFS ボリュームを **Amazon EVS** に接続してデータストアとして使用する

FSx for ONTAPファイルシステムがプロビジョニングされ、適切な接続パラメータがすべて検証されたので、次は FSx for ONTAPストレージボリュームを Amazon EVS に接続します。次の手順では、vCenter にアクセスし、FSx for ONTAPボリュームを NFS データストアとしてマウントする方法を示します。

1. vSphere クライアントで、「データストア」タブに移動します。以下に示すように、データセンターを見つけて、[ストレージ] > [新しいデータストア] に移動します。

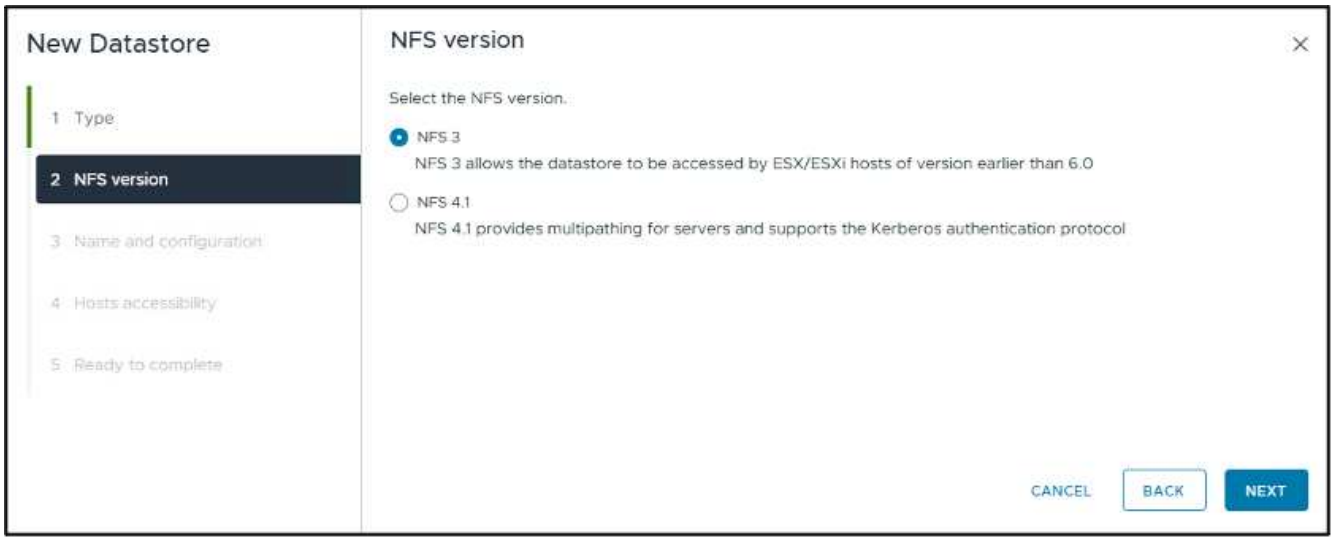


2. 新しいデータストア ウィザードが起動します。「タイプ」ステップでは、データストアのタイプを選択します。「NFS」を選択し、「次へ」をクリックして続行します。



3. 「NFS バージョン」の手順では、NFS バージョンを選択します。

この例では、「NFS 3」を選択しますが、NFS v4.1 も使用できることに注意してください。



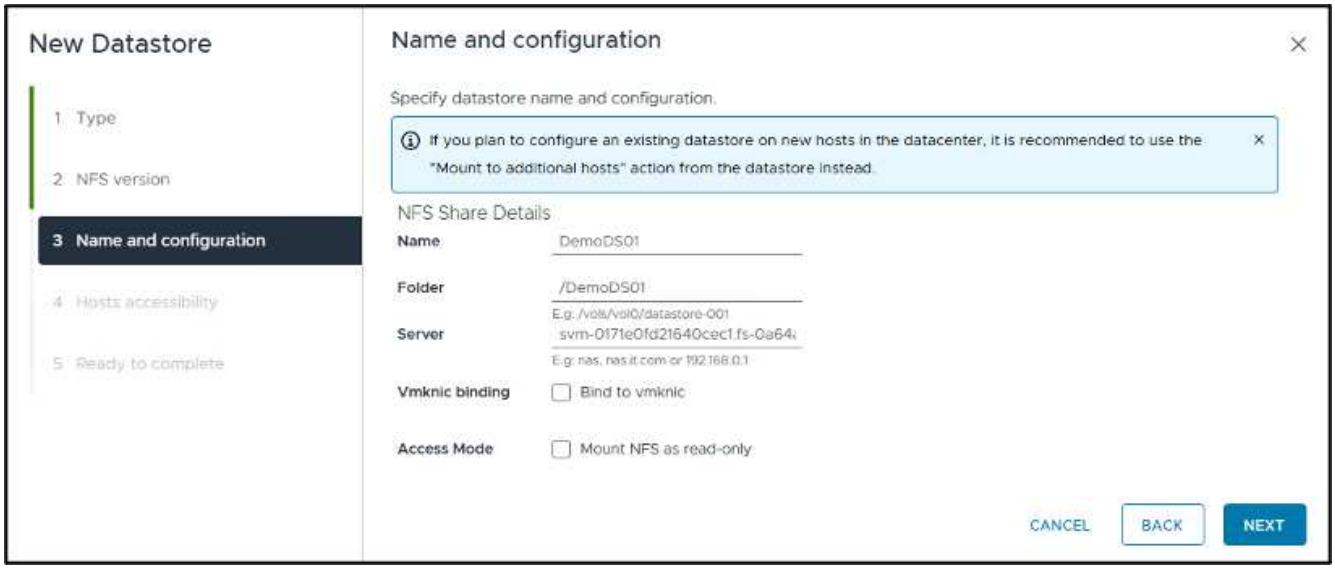
4. 「名前と構成」の手順では、次の操作を行います。

   a. データストアに名前を付けます。

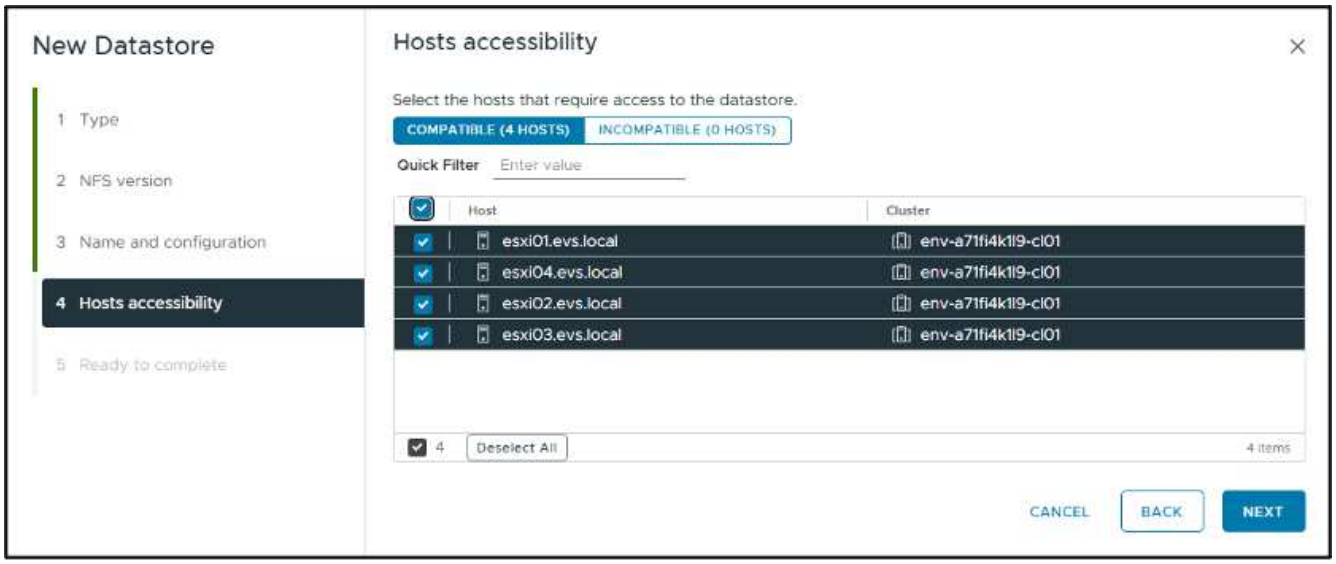
   b. フォルダに名前を付けます。 NFS ボリュームへのジャンクション パスを使用します。

   c. サーバーに名前を付けます。 SVM の NFS DNS 名または NFS の IP アドレスのいずれかを使用します。

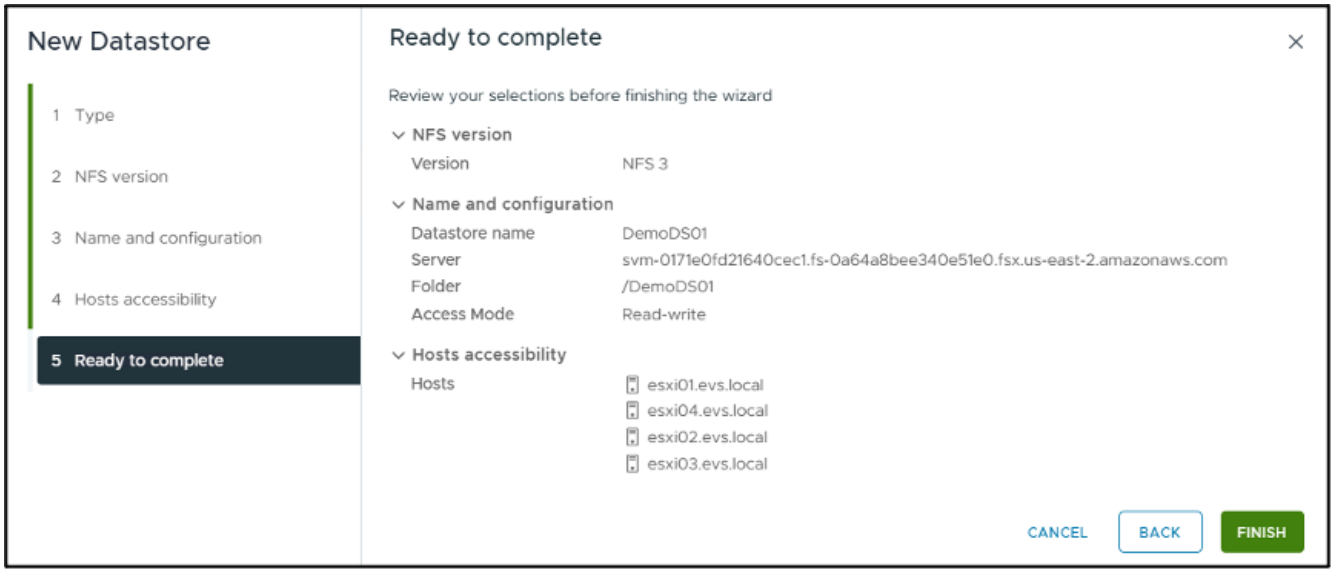
   「次へ」をクリックして続行します。



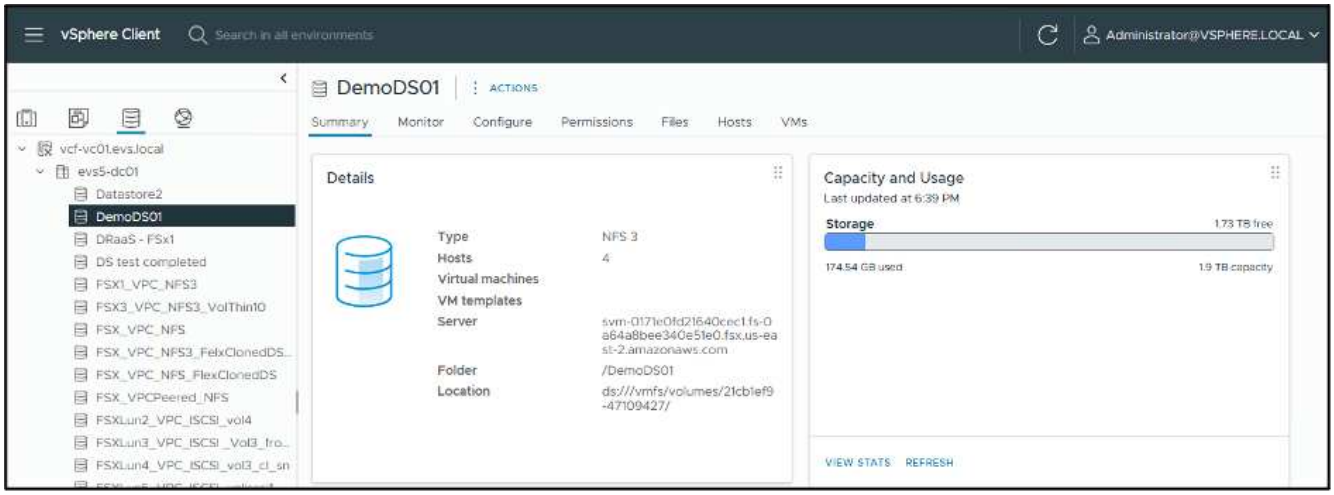
5. 「ホスト アクセシビリティ」の手順で、データストアへのアクセスを必要とするすべてのホストを選択し、「次へ」をクリックして続行します。



6. 「完了準備完了」のステップでデータを確認し、「完了」をクリックしてセットアップを完了します。



7. 以下に示すように、vCenter にアクセスして NFS データストアが接続されていることを確認します。



FSx for ONTAP をiSCSI データストアとして使用するための導入手順

このセクションでは、FSx for ONTAPを使用して iSCSI データストアを構成する手順について説明します。

前提条件

FSx for ONTAP をiSCSI 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 Amazon EVS 仮想化環境をデプロイする必要があります。詳細については、「Amazon EVS の開始方法」ガイドのドキュメントを参照してください。このセクションでは、FSx for ONTAPファイル システムを導入済みであることを前提としています。適切な手順については、上記の詳細なアプローチのセクションを参照してください。

大まかな展開手順

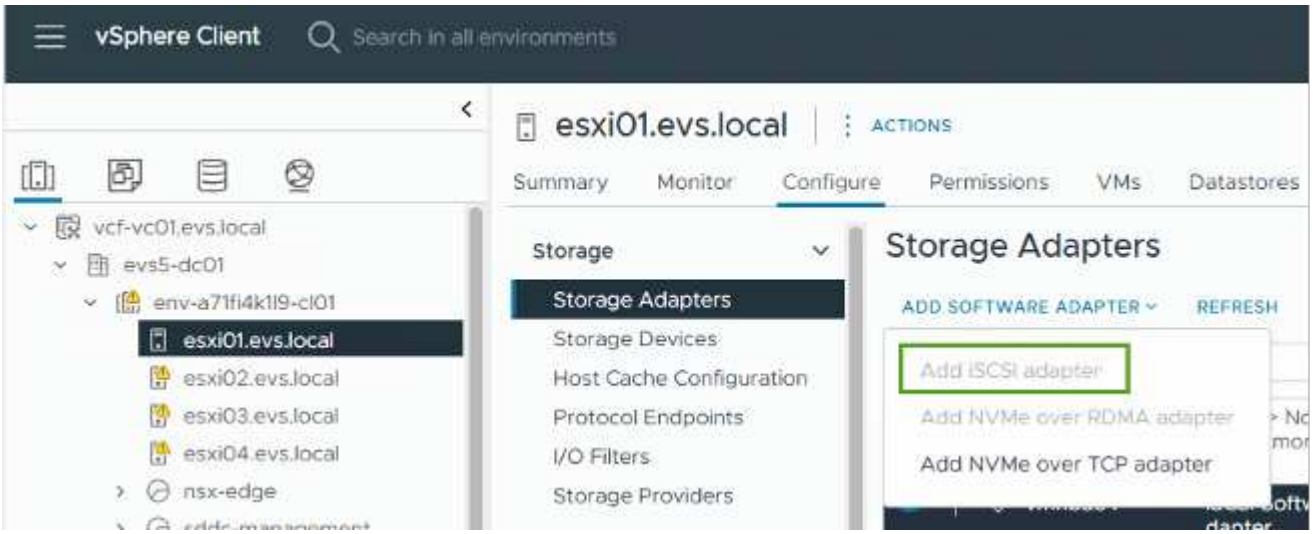
Amazon EVS の iSCSI データストアとして使用するために FSx for ONTAPファイルシステムをデプロイし、2 つのサービス間の接続を確立するには、次の手順を実行します。

- 各 ESXi ホストに iSCSI ネットワーク アダプタを設定します。
- FSx for ONTAPファイル システム、ボリューム、LUN などの作成と構成。
- ESXi ホストを FSx for ONTAPファイル システム サーバーに接続します。
- iSCSI データストア仮想マシン ファイル システム (VMFS) を作成します。

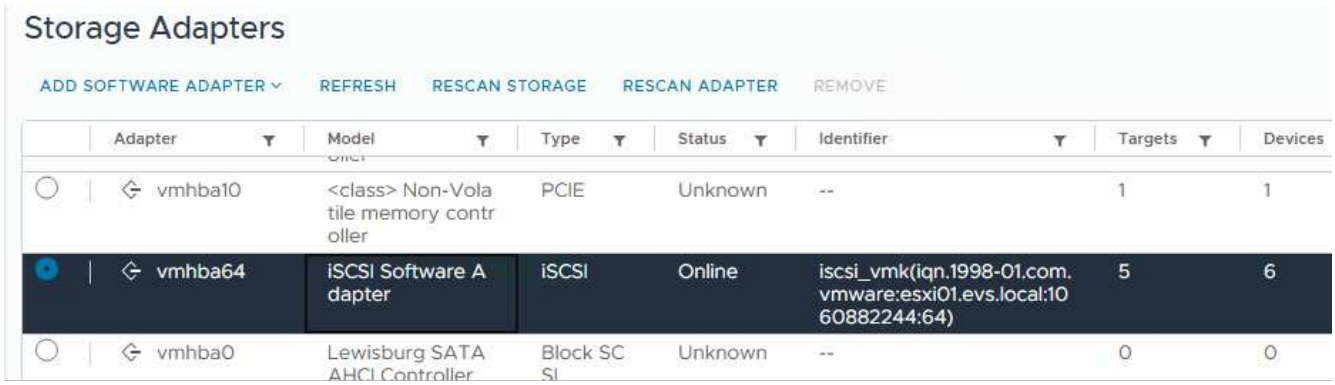
iSCSIネットワークアダプタを追加する

環境内の各 ESXi ホストで次の手順を実行する必要があります。

1. vSphere クライアントに入り、ESXi ホストを選択します。 [構成] タブで、[ソフトウェア アダプタの追加] を選択し、次に示すように、ドロップダウン メニューから [iSCSI アダプタの追加] を選択します。

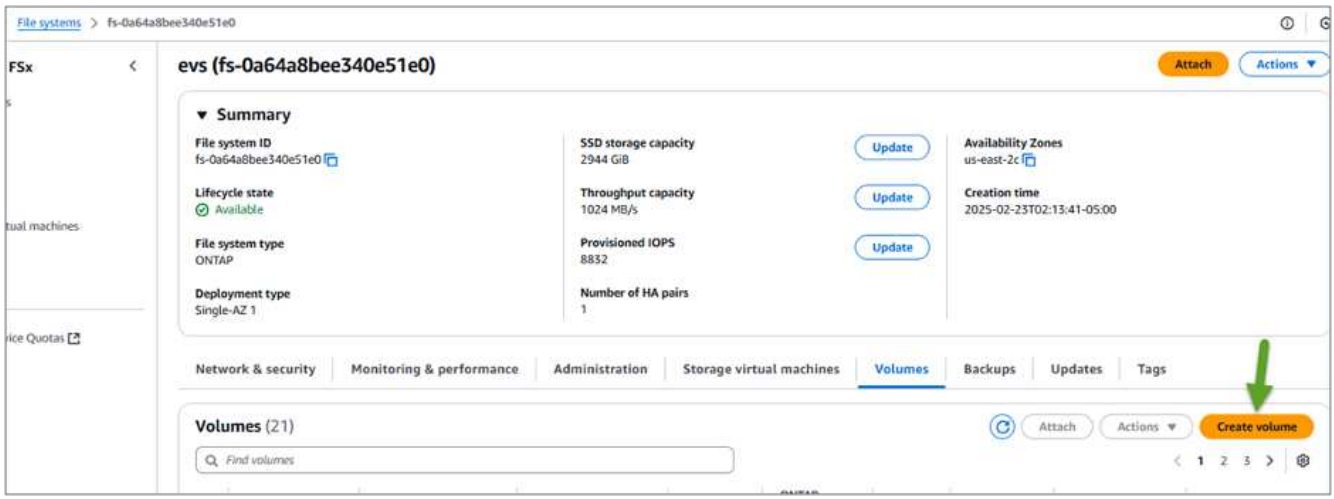


2. インストールが完了すると、ストレージ アダプタ画面が表示されます。メニューバーから「アダプタの再スキャン」を選択します。 iSCSI アダプタの IQN を記録します: iqn.xxxx。この値は、後で LUN マッピング手順で使用されます。



FSx for ONTAPボリュームを作成する

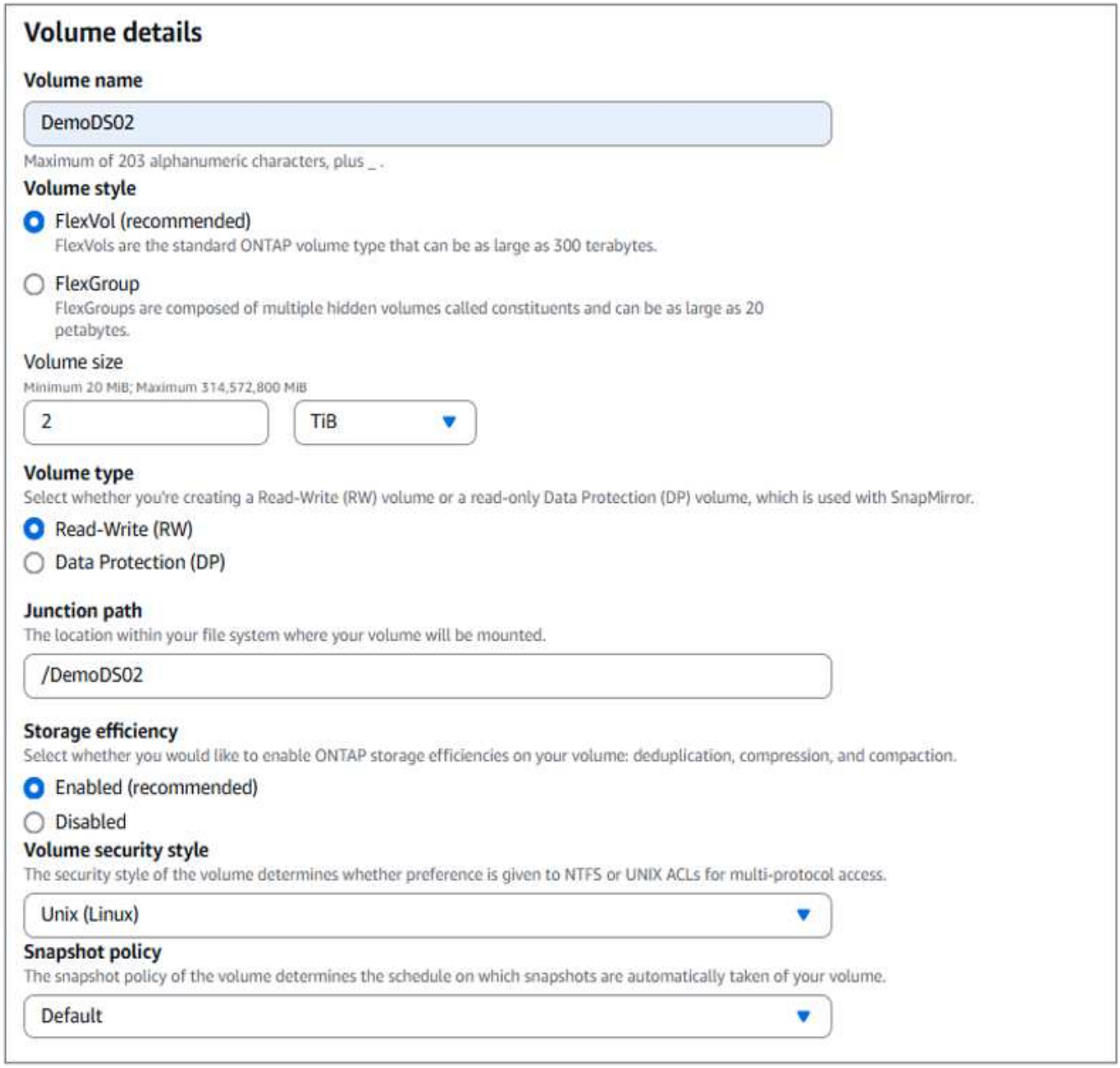
1. AWS コンソールに移動し、FSx for ONTAPファイルシステムのページにアクセスして、「ボリュームの作成」をクリックします。



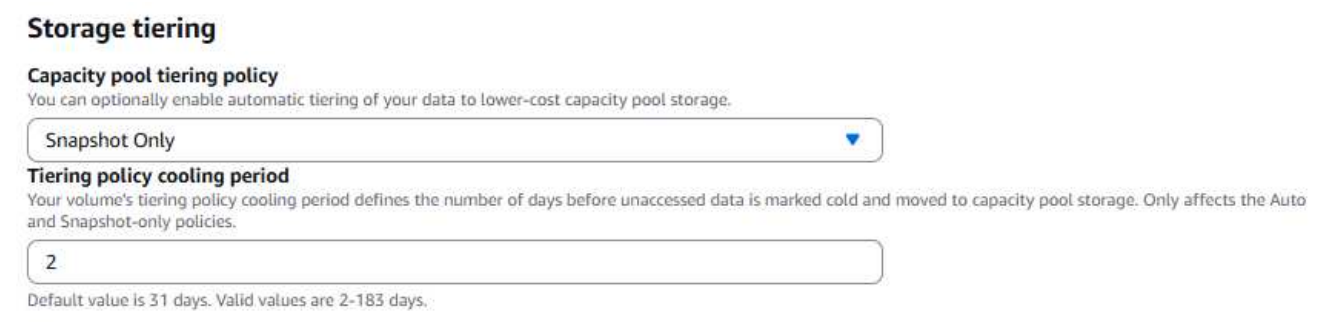
2. ボリュームを作成する SVM を選択します。



3. 「ボリュームの詳細」ページで、下のスクリーンショットに示すように詳細を入力します。完了したら、「作成」をクリックしてボリュームを設定します。 ONTAPストレージ効率機能 (圧縮、重複排除、および圧縮) をオンにするには、「有効」を選択します。



4. ストレージ階層化オプションでは、ドロップダウン メニューから「スナップショットのみ」を選択し、階層化ポリシーの冷却期間を設定します。デフォルトは 31 日ですが、この例では 2 日間の冷却期間を設定します。



5. ボリュームが作成されたら、 ONTAP CLI を使用して次の値を設定します。

設定	構成
ボリューム ギャランティ	なし（シンプロビジョニング）
fractional_reserve	0%
snap_reserve	0%
自動サイズ調整	grow_shrink
ストレージ効率	有効
ボリューム階層化ポリシー	Snapshot のみ
アクセス時刻の更新 (-atime-update)	間違い
最小先読み (-min-readahead)	間違い
スナップショットポリシー	なし
LUNスペース予約	無効
LUNスペース割り当て	有効

LUN、igroup、およびLUNのマッピングを作成する

このセクションでは、vSphere でディスクとして表示される LUN を作成する方法を示します。また、LUN にアクセスできるイニシエータのリストであるイニシエータ グループ (igroup) を作成する方法も説明します。igroup は vSphere ESXi ホストから LUN へのアクセスを許可します。最後に、igroup を LUN にマップする方法を示します。

1. ONTAP CLI にアクセスするには、次のコマンドを実行して、FSx for ONTAPファイルシステムまたは SVM の管理ポートで SSH セッションを確立します。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

2. LUNを作成必ずスペース割り当てとスペース予約を有効に設定してください。サイズはボリューム サイズの最大 90% にする必要があります。

```
Fsxid::> lun create -vserver fsx -path /vol/DemoDS02/lun_name -size 1.8T
-ostype vmware -space-allocation enabled -space-reservation disabled
```

3. igroup を作成し、クラスタ内のすべての ESXi ホストの IQN を追加します。

```
Fsxid::> lun igroup create -vserver fsx -igroup evs1 -protocol iscsi
-ostype vmware -initiator iqn.1998-
01.com.vmware:esxi01.evs.local:1060882244:64,iqn.1998-
01.com.vmware:esxi02.evs.local:1911302492:64,iqn.1998-
01.com.vmware:esxi03.evs.local:2069609753:64,iqn.1998-
01.com.vmware:esxi04.evs.local:1165297648:64
```

4. 次のコードを使用して LUN をマップします。

```
Fsxid::> lun mapping create -vserver fsx -path /vol/DemoDS02/lun1
-igroup evs1 -lun-id 2
```

5. LUN マッピングを確認し、状態が「マップ済み」に変更されたことを確認します。これは、LUN がマップされた状態であることを確認するために必要な二重チェックです。

```
Fsxid::> lun show
Vserver   Path                              State   Mapped   Type
Size
--------- ------------------------------- ------- -------- --------
--------
fsx       /vol/DemoDS02/lun1              online  mapped   vmware
1.80TB
```

SVMからiSCSI構成情報を取得する

1. iSCSI ショーを実行し、ターゲット名を記録します。これは、FSx for ONTAPディスクの vSphere 検出で使用されます (注: このターゲット名は SVM に固有です)。

```
Fsxid::> iscsi show -vserver fsx
                 Vserver: fsx
             Target Name: iqn.1992-
08.com.netapp:sn.c083e374f1b711ef9d9f8123a3ebcf46:vs.3
            Target Alias: fsx
   Administrative Status: up
```

2. iSCSI IP アドレスを記録します。

```
Fsxid::> network interface show -vserver fsx -data-protocol iscsi
-fields address
vserver lif       address
------- -------   -----------
fsx     iscsi_1   10.0.10.134
fsx     iscsi_2   10.0.10.227
```

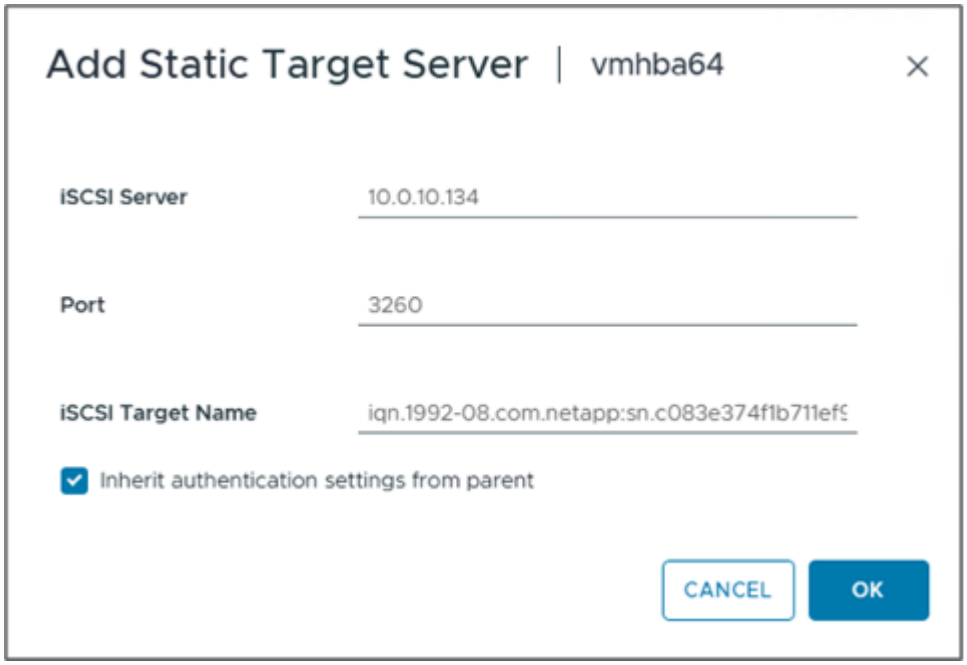
FSx for ONTAP iSCSIサーバの検出

LUN がマップされたので、SVM の FSx for ONTAP iSCSI サーバーを検出できます。 SDDC 内に存在する ESXi ホストごとに、ここで説明する手順を繰り返す必要があることに注意してください。

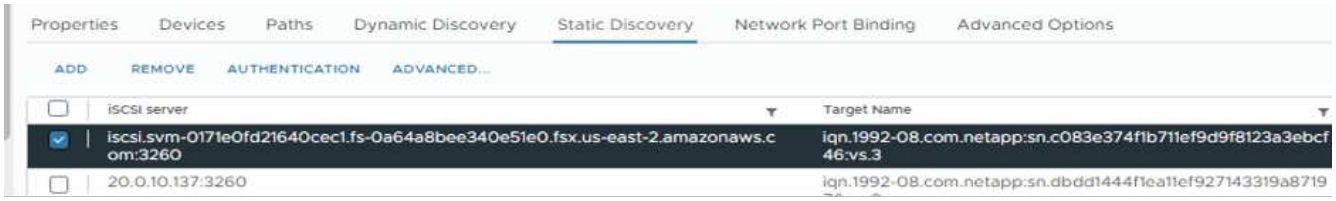
1. まず、FSx for ONTAPファイル システムにリンクされているセキュリティ グループ (つまり、ENI に接続されているセキュリティ グループ) が iSCSI ポートを許可していることを確認します。

iSCSIプロトコルポートの完全なリストとその適用方法については、以下を参照してください。"Amazon VPC によるファイルシステムのアクセス制御" 。

2. vSphere Client で、ESXi ホスト > ストレージ アダプタ > 静的検出に移動し、「追加」をクリックします。
3. 上記の iSCSI サーバーの IP アドレスを入力します (ポートは 3260)。 iSCSI ターゲット名は、iSCSI show コマンドからの IQN です。 「OK」をクリックして続行します。



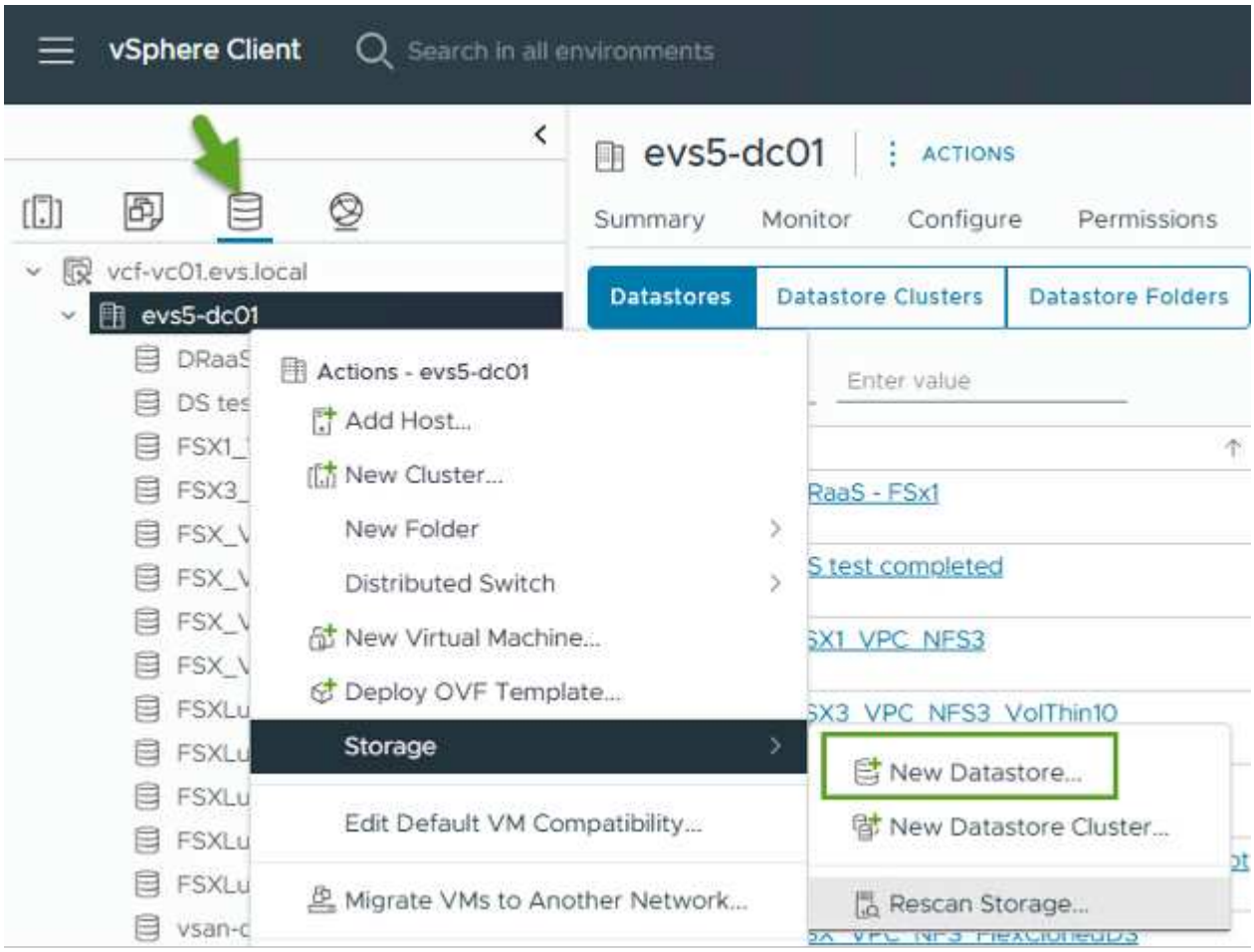
4. ウィザードが閉じて、データストアの静的検出画面が表示されます。このページの表で、ターゲットが検出されたかどうかを確認できます。



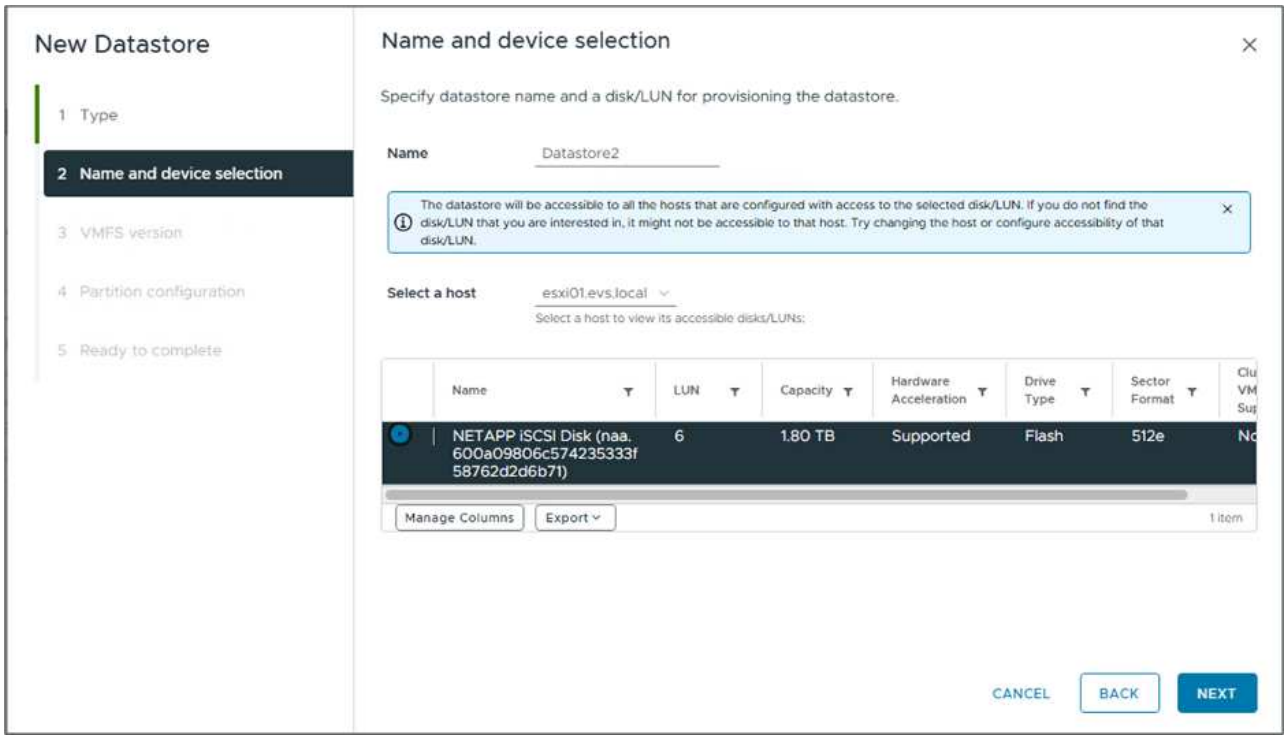
iSCSIデータストアを作成する

iSCSI サーバーを検出したので、iSCSI データストアを作成できます。

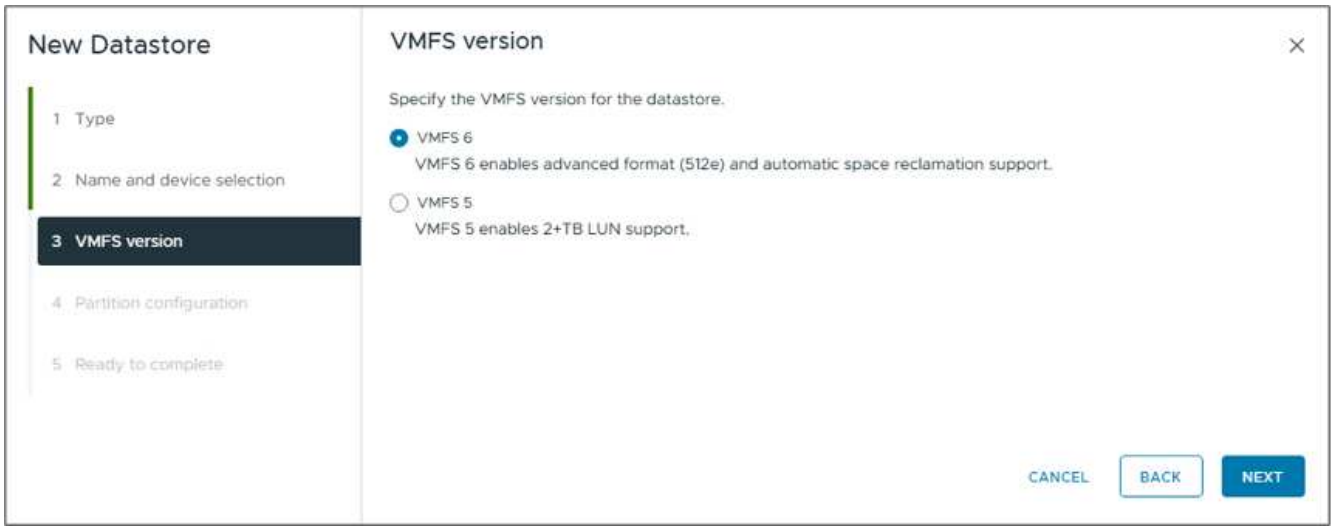
1. vSphere クライアントで、[データストア] タブに移動し、データストアを展開する SDDC を選択します。右クリックしてストレージ アイコン (下のスクリーンショットでは緑色の矢印で示されています) を選択し、ドロップダウン メニューから [新しいデータストア] を選択します。



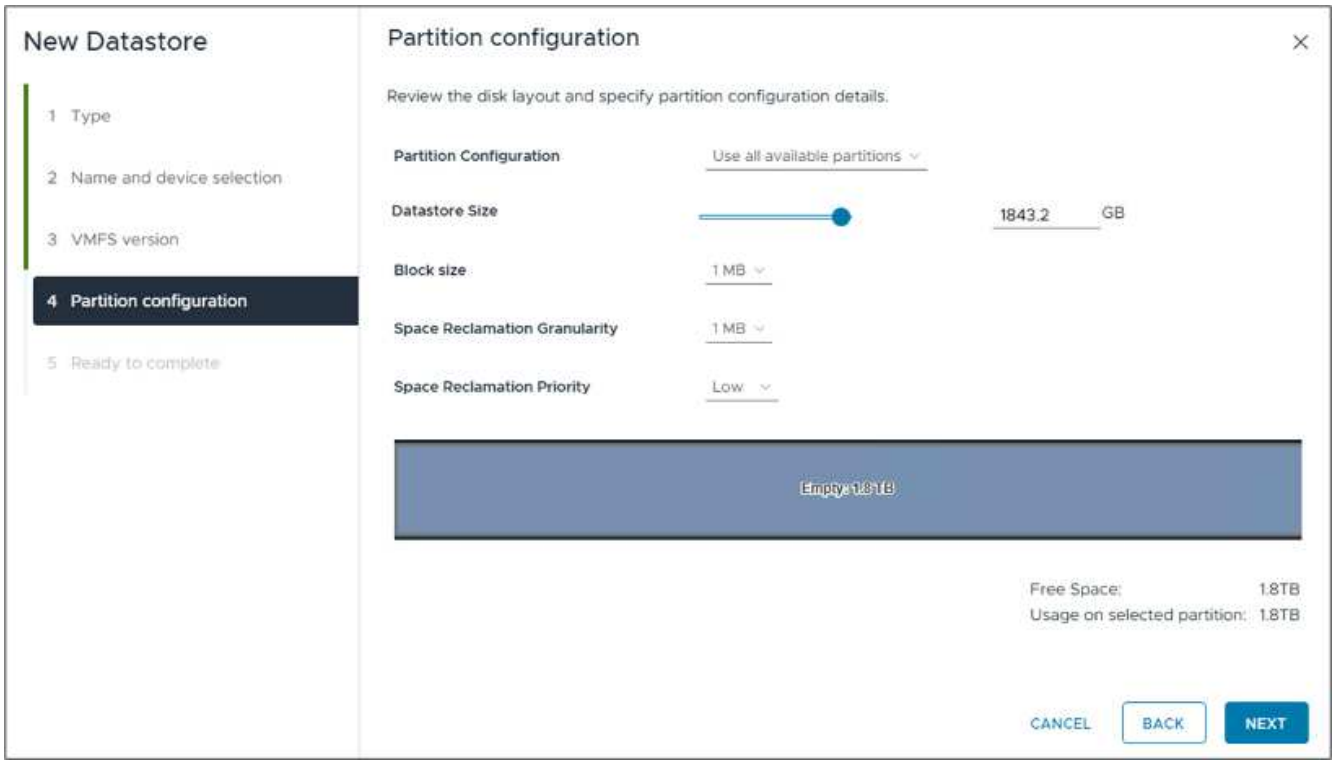
2. 新しいデータストア ウィザードが起動します。 「タイプ」ステップで、VMFS オプションを選択します。
3. 「名前とデバイスの選択」の手順:
   a. データストアの名前を指定します。
   b. データストアに接続する ESXi ホストを選択します。
   c. 検出されたディスク (LUN) を選択し、「次へ」をクリックします。



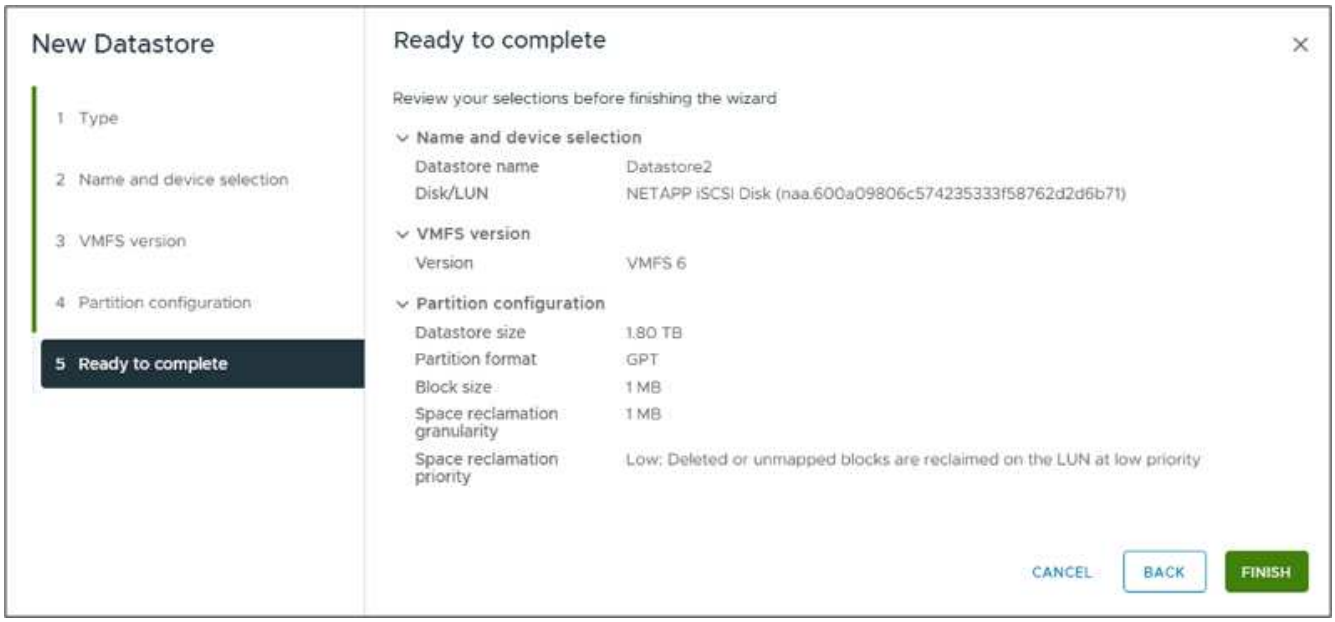
4. 「VMFS バージョン」の手順で、「VMFS 6」を選択します。



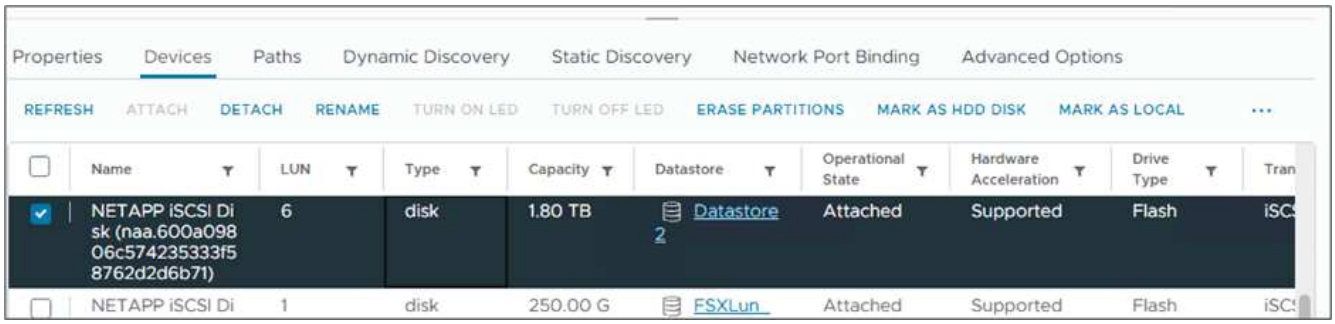
5. 「パーティション構成」の手順では、「利用可能なすべてのパーティションを使用する」オプションを含め、デフォルト設定をそのままにしておきます。「次へ」をクリックして続行します。



6. 「完了の準備」の手順で、設定が正しいことを確認します。完了したら、「完了」をクリックしてセットアップを完了します。



7. [デバイス] ページに戻り、データストアが接続されていることを確認します。



まとめ

このドキュメントでは、NFS プロトコルと iSCSI プロトコルの両方で使用するために、FSx for ONTAPを Amazon EVS の外部ストレージとして設定する方法について説明しました。

FSx for ONTAPを Amazon EVS の外部ストレージとして使用すると、明確な運用上およびビジネス上の価値が得られます。 ONTAPテクノロジーにより、データの復元力、保護、レプリケーション、コスト効率が向上し、VMware ハイパーコンバージド アーキテクチャを分離することで TCO が最適化されます。 FSx for ONTAPを使用すると、Amazon EVS ユーザーはコンピューティングリソースを追加したりコストを膨らませたりすることなく、ストレージを拡張できます。これにより、AWS クラウドが提供する弾力性と拡張性の可能性が最大限に引き出されます。

詳細については、Amazon の新着情報をご覧ください。"Amazon EVS が FSx for ONTAPと統合" 、およびNetAppブログ:"Amazon EVSがFSx for ONTAPのサポートを発表" 。

EVS用FSx ONTAPデータストアの保護

Amazon Elastic VMware Service を使用して、**Amazon FSx for NetApp ONTAP** データストアを **NetApp SnapCenter Plug-in for VMware** で保護する方法

このガイドでは、NetApp SnapCenter® Plug-in for VMware vSphere（SCV）バックアップおよびリカバリ ソリューションを使用して、FSx for ONTAP Network File System（NFS）およびiSCSI Amazon EVSデータストアと関連するVMを保護するためのシンプルな導入アプローチを紹介します。

はじめに

Amazon FSx for NetApp ONTAP（FSx for ONTAP）ベースのAmazon Elastic VMware Service（Amazon EVS）用補足データストアは、nConnectの活用、Amazon Virtual Private Cloud（Amazon VPC）ピアリング、データストアマウントごとの複数のネットワーク接続の使用などのパフォーマンス要求の高いワークロードと、ストレージ集約型ワークロードの両方を実行するための優れたソリューションを提供します。

この機能により、顧客は仮想ストレージ エリア ネットワーク（vSAN）によって提供されるローカル インスタンス ストレージの制限を克服し、コンピューティングとは独立してストレージを拡張し、全体的な総所有コストを削減できます。総所有コスト（TCO）のメリット以外にも、FSx for ONTAPはAmazon EVSにエンタープライズクラスの機能を提供します。これらの機能はオンプレミスONTAP®の顧客にとって馴染み深いもので、導入の最適化と合理化に役立ちます。FSx for ONTAPを使用すると、NetApp® Snapshot™、SnapMirror®、およびSnapVault®テクノロジにアクセスでき、仮想マシン（VM）、データストア、仮想マシン ディスク（VMDK）のバックアップおよび復元操作をサポートします。重要な機能の 1 つは、Snapshot ベースの保護です。

概要

組織が環境を拡張および統合するにつれて、それらのワークロードと基盤となるストレージを保護する必要性がますます重要になります。SCVを使用すると、Amazon EVS vSphereクライアントから直接データストアと仮想マシンをバックアップできます。

このガイドの目的

このガイドでは、SCV を使用して Amazon EVS 用の FSx for ONTAP データストアを保護する方法について説明します。VM とデータベースの保護およびリストアのシナリオ例も提供されます。

観客

このチュートリアルは、VMware vSphere、Amazon EVS、AWS コンソール、FSx for ONTAPに精通しているクラウドアーキテクトおよびクラウド管理者を対象としています。

導入と設定の概要手順

以下は、Amazon EVS 上の VM とデータストアを保護するために SCV を展開および構成する概要手順です：

1. SCV Open Virtual Appliance（OVA）をダウンロードします。
2. vSphere Client の認証情報を使用して Amazon EVS にログインします。
3. Open Virtualization Format（OVF）テンプレートを展開して、VMware 展開ウィザードを起動します。
4. プラグインにアクセスするには、メニューから SnapCenter Plug-in for VMware を選択します。
5. ストレージを追加します。
6. バックアップ ポリシーを作成します。
7. リソース グループを作成します。
8. リソース グループをバックアップします。
9. 仮想マシン全体、または特定の仮想ディスクやゲスト ファイルを復元します。

VMware用SnapCenterプラグインのセットアップ手順

このセクションでは、VMware 用の SnapCenter プラグインをセットアップする手順について説明します。

前提条件

開始する前に、次の前提条件が必要です。

1. OVAの導入時にvCenterサーバーを登録するには、vCenterの完全修飾ドメイン名（FQDN）またはIPアドレスを指定します。
2. vCenterのクレデンシャルには、必要最小限の権限を持つアカウントを使用してください
3. vCenter Server にアクセスするためのファイアウォールポートを開きます。
4. FSx for ONTAPが実行されているAmazon VPCのセキュリティグループを更新して、SCVからFSx for ONTAPへのアクセスを許可します。

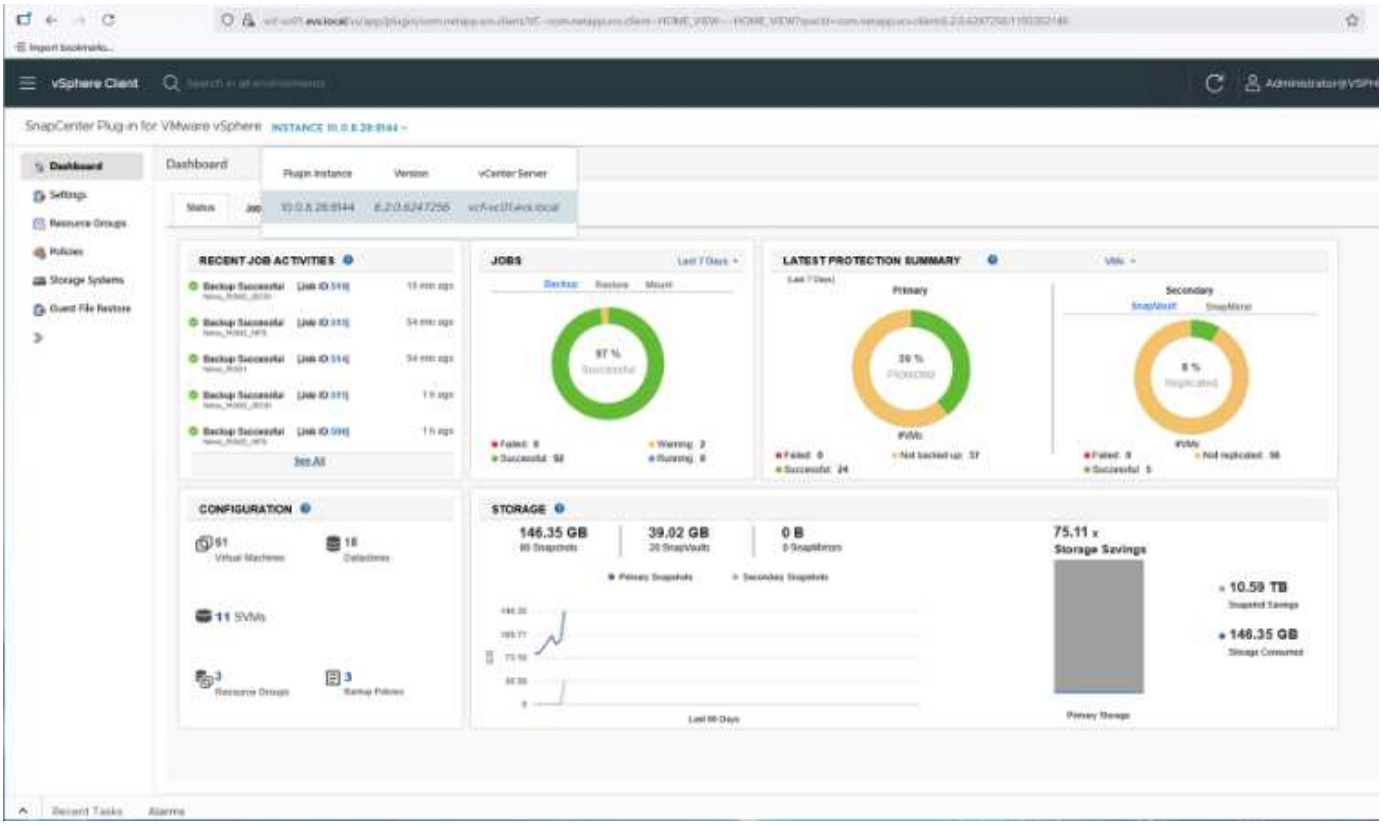
SCVは無料でご利用いただけます。

SnapCenter Plug-in for VMwareの設定

VM とそれらをホストする NFS/iSCSI ベースのデータストアを保護するには、 SCV を導入する必要があります。単純な OVF インポートです。

導入手順は次のとおりです：

1. "NetAppサポート サイト"からOVAをダウンロードします。
2. Amazon EVS vCenterにログインします。
3. vCenter内で、データセンター、フォルダ、クラスタ、ホストなどのインベントリオブジェクトを右クリックし、「Deploy OVF template」を選択します。
4. ストレージ、セグメント、テンプレートのカスタマイズなど、適切な設定を選択して、vCenterとその認証情報を更新し、SCV認証情報とIP詳細を作成します。確認後、「完了」を選択します。
5. OVF のインポートおよびデプロイメントタスクが完了するまで待ちます。
6. SCVが正常に展開されると、vCenter内に登録されます。
7. プラグインにアクセスするには、vCenter Webクライアントページの左側のサイドバーに移動し、「SnapCenter Plug-in for VMware」を選択します。



VMware用SnapCenterプラグインの設定手順

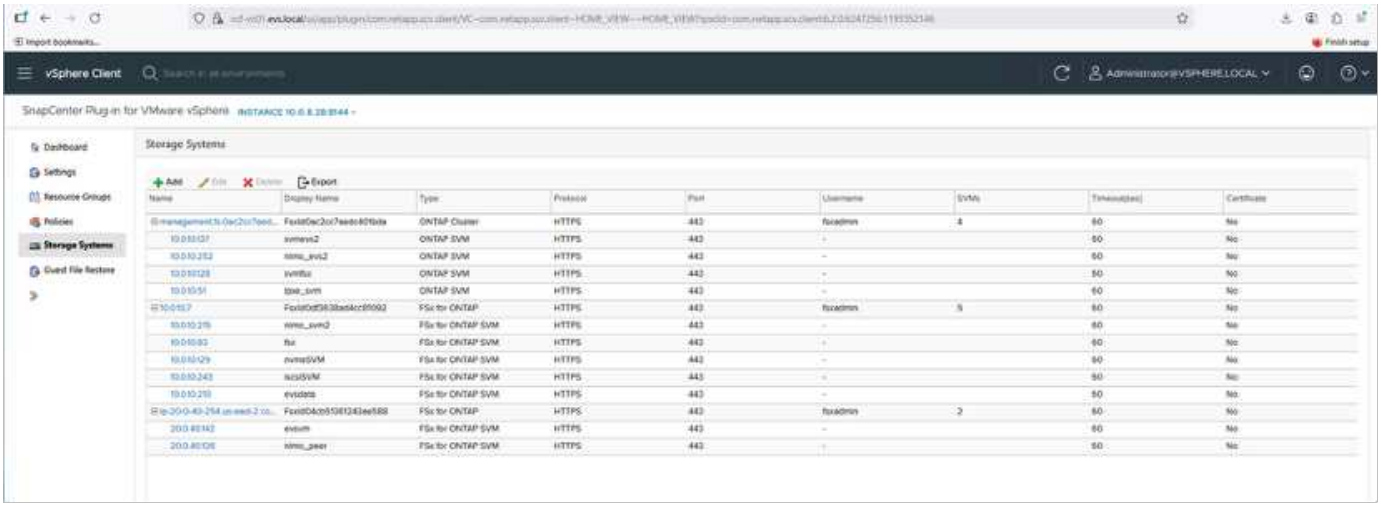
このセクションでは、SnapCenter Plug-in for VMware の設定手順について説明します。次のセクションでは、ストレージの追加方法、バックアップ ポリシーの作成方法、およ

びリソース グループの作成方法について説明します。

ストレージシステムの追加

SVC でワークロードを保護する次のステップは、"ストレージ システム"を追加することです。ストレージを追加すると、SCV は vCenter 内でバックアップおよびリストア処理を検出して管理できるようになります。FSx for NetApp ONTAP 管理エンドポイントまたは Storage Virtual Machine（SVM）管理エンドポイント IP をストレージ システムとして追加して、VM のバックアップとリストアを有効にします。

1. EVS vCenter の左側のナビゲーションメニューから、「SnapCenter Plug-in for VMware」を選択します。
2. 「Storage System」を選択します。
3. 「追加」を選択して、FSx for ONTAP の詳細を追加します。
4. 「認証として資格情報を使用する」方法を使用し、ユーザー名とパスワードとして FSxadmin を入力します。次に「追加」を選択して設定を保存します。



ファイル システムが追加されると、すべての SVM が自動的に追加されます。

SCVバージョンが6.2の場合は、"SCV サポート ページ"にアクセスしてSCV 6.2P1リリースをダウンロードしてください。

バックアップ ポリシーを作成する

堅牢なバックアップ戦略では、バックアップ スケジュール、バックアップするデータ、バックアップの保持期間などの重要な要素を定義する必要があります。Snapshotコピーを時間単位または日単位でスケジュール設定して、データストア全体を保護できます。このようにバックアップをスケジュールすると、データストアが保護されるだけでなく、それらのデータストアに含まれるVMおよびVMDKのバックアップおよびリストア操作もサポートされます。

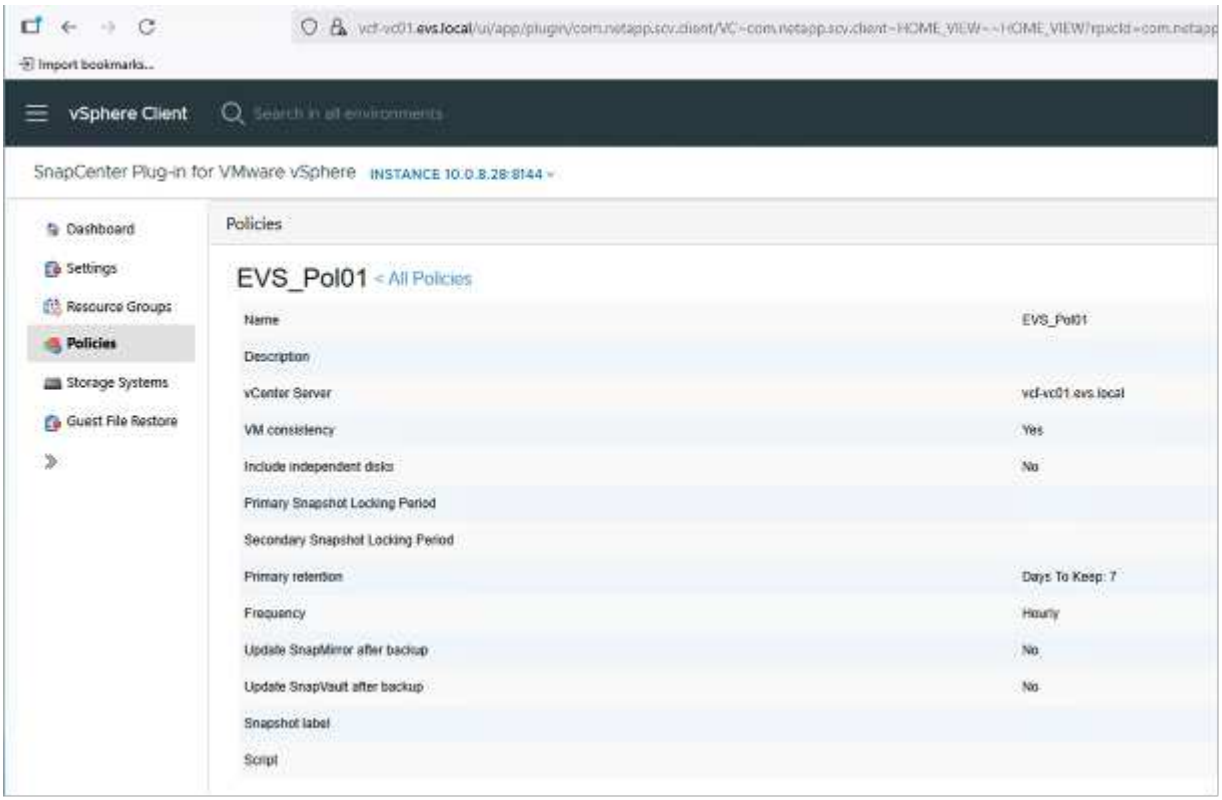
VMとデータストアのバックアップを開始する前に、"バックアップ ポリシー"およびリソース グループを作成します。バックアップ ポリシーでは、バックアップ スケジュールや保持設定などのパラメータを指定します。

バックアップ ポリシーを作成する手順は次のとおりです。

1. SCV の左側のナビゲーション メニューに移動し、「ポリシー」を選択します。

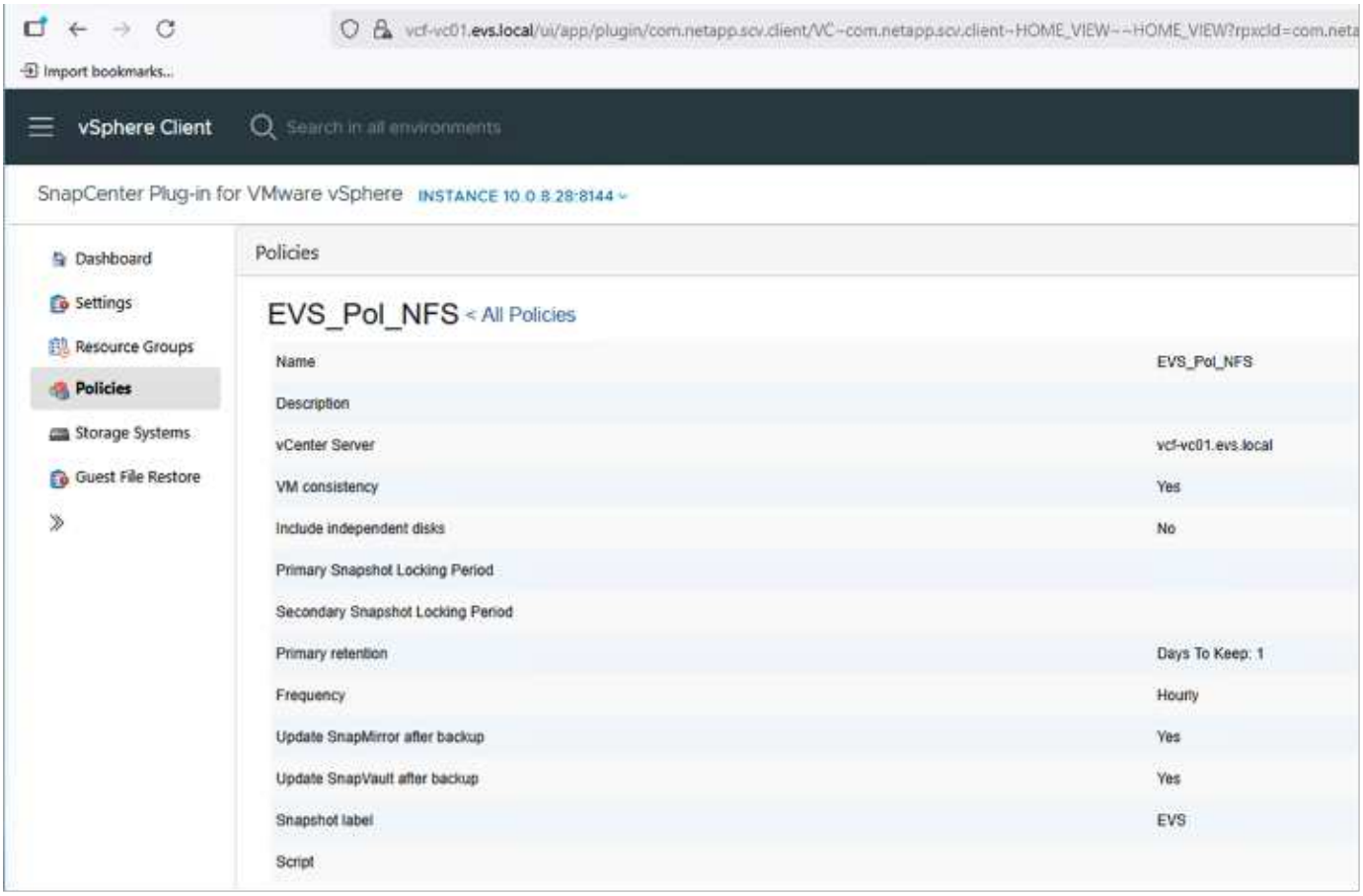
2. 「ポリシー」ページで「作成」を選択してウィザードを起動します。
3. 「新しいバックアップ ポリシー ページ」で、ポリシーの名前を入力します。
4. 保持期間、バックアップ頻度、レプリケーション設定を指定します。
5. Snapshot ロックを有効にするには、「ロック期間」チェックボックスを選択します。プライマリおよびセカンダリの Snapshot ロック期間を日数/月数/年数として選択できます。

SnapMirrorポリシーで定義された保持値に関係なく、指定されたセカンダリSnapshotのロック期間が終了するまで、セカンダリSnapshotコピーはそのまま残ります。



VM 整合性バックアップを有効にするには、VMware ツールがインストールされ、実行されている必要があります。VM 整合性ボックスをオンにすると、VM は最初に停止し、次に VMware が VM 整合性スナップショット（メモリを除く）を実行し、次に SnapCenter Plug-in for VMware vSphere がバックアップ操作を実行し、その後 VM 操作が再開されます。

Snapshot コピーをセカンダリ ミラーまたはボールト ファイル システムにレプリケートするには、事前に関係を設定しておく必要があります。



ポリシーが作成されたら、次のステップは、バックアップする必要がある適切な NFS または iSCSI データストアと VM を定義するリソース グループを作成することです。

リソースグループを作成する

リソース グループは、保護が必要な VM およびデータストアのコンテナーとして機能します。リソースはいつでもリソース グループに追加したり、リソース グループから削除したりできるため、バックアップ構成を柔軟に管理できます。

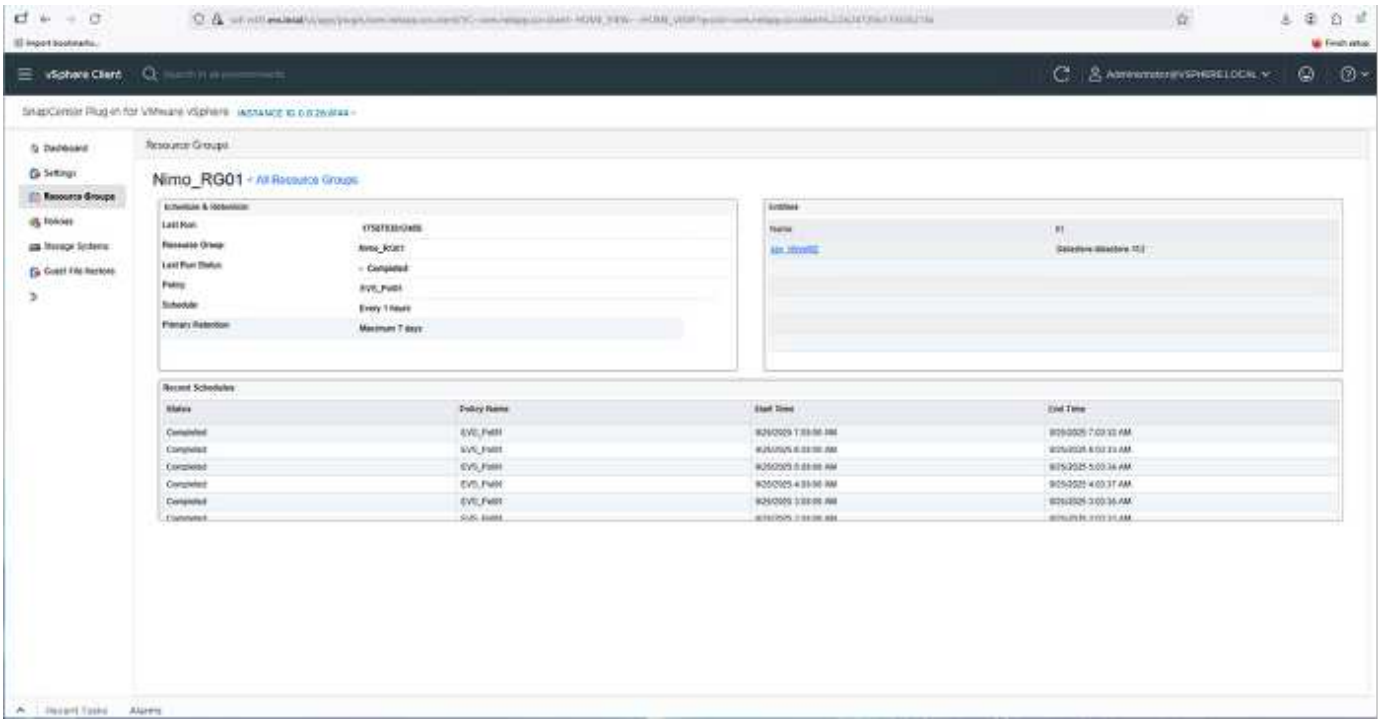
"リソース グループ"は、以下の手順で作成できます：

1. SCV の左側のナビゲーション ペインに移動し、「リソース グループ」を選択します。
2. 「リソース グループ」ページで「作成」を選択して、リソース グループ作成ウィザードを開始します。

> リソース グループを作成する別のオプションは、個々の VM またはデータストアを選択し、そのリソースのみを含むリソース グループを作成することです。

3. 「リソース」ページで、スコープ（VM またはデータストア）とデータセンターを選択します。
4. 「スパニング ディスク」ページで、「複数のデータストアにわたる複数の VMDK を持つ仮想マシン」オプションを選択します。
5. 次に、バックアップ ポリシーを関連付けます。既存のポリシーを選択するか、新しいバックアップ ポリシーを作成します。
6. 「スケジュール」ページで、選択したポリシーごとにバックアップ スケジュールを設定します。

7. 適切な選択を行ったら、「完了」を選択します。これにより、新しいリソース グループが作成され、リソース グループ リストに追加されます。



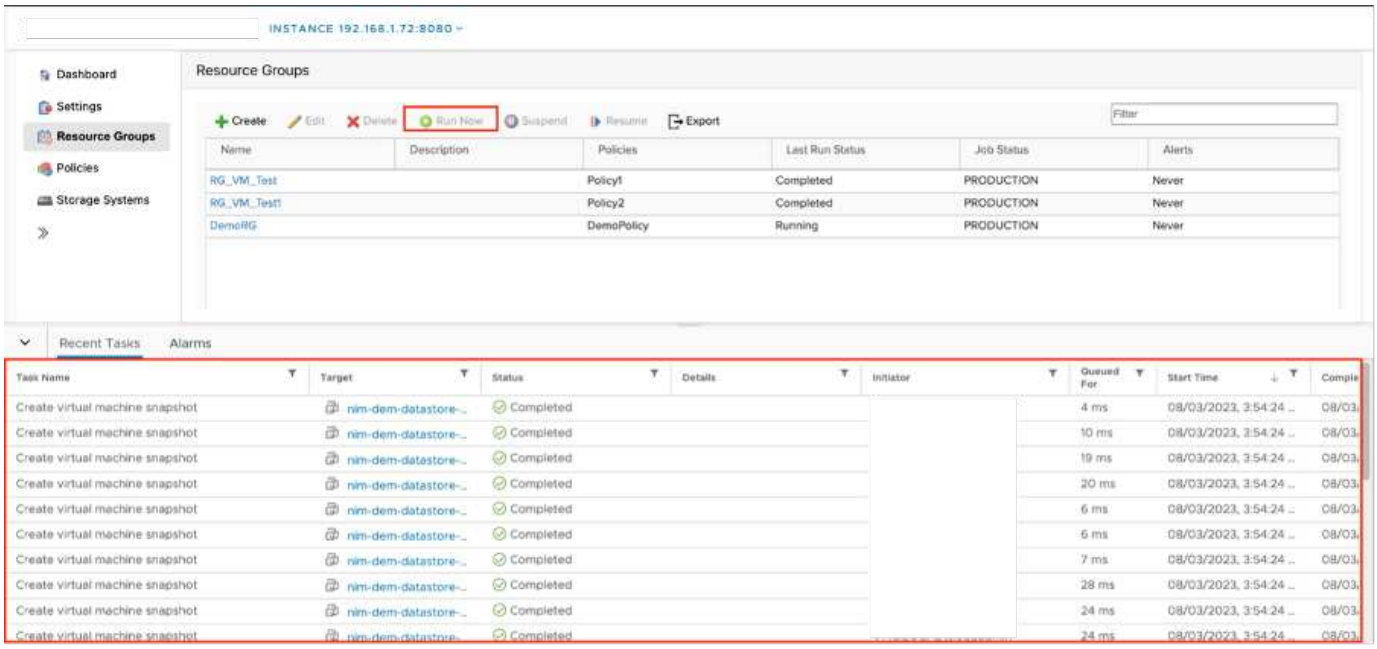
リソースグループのバックアップ

バックアップ操作は、リソース グループ内で定義されているすべてのリソースに対して実行されます。リソース グループにポリシーが関連付けられ、スケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが実行されます。

1. vCenter Web クライアント ページの左側のナビゲーションで、「SnapCenter Plug-in for VMware」、「リソース グループ」の順に選択します。
2. 「リソース グループ」ページで、指定されたリソース グループを見つけて、「今すぐ実行」を選択し、手動バックアップを開始します。



3. リソース グループに複数のポリシーが設定されている場合は、「今すぐバックアップ」ダイアログ ボックスでバックアップ操作のポリシーを選択します。
4. 「OK」を選択してバックアップを開始します。

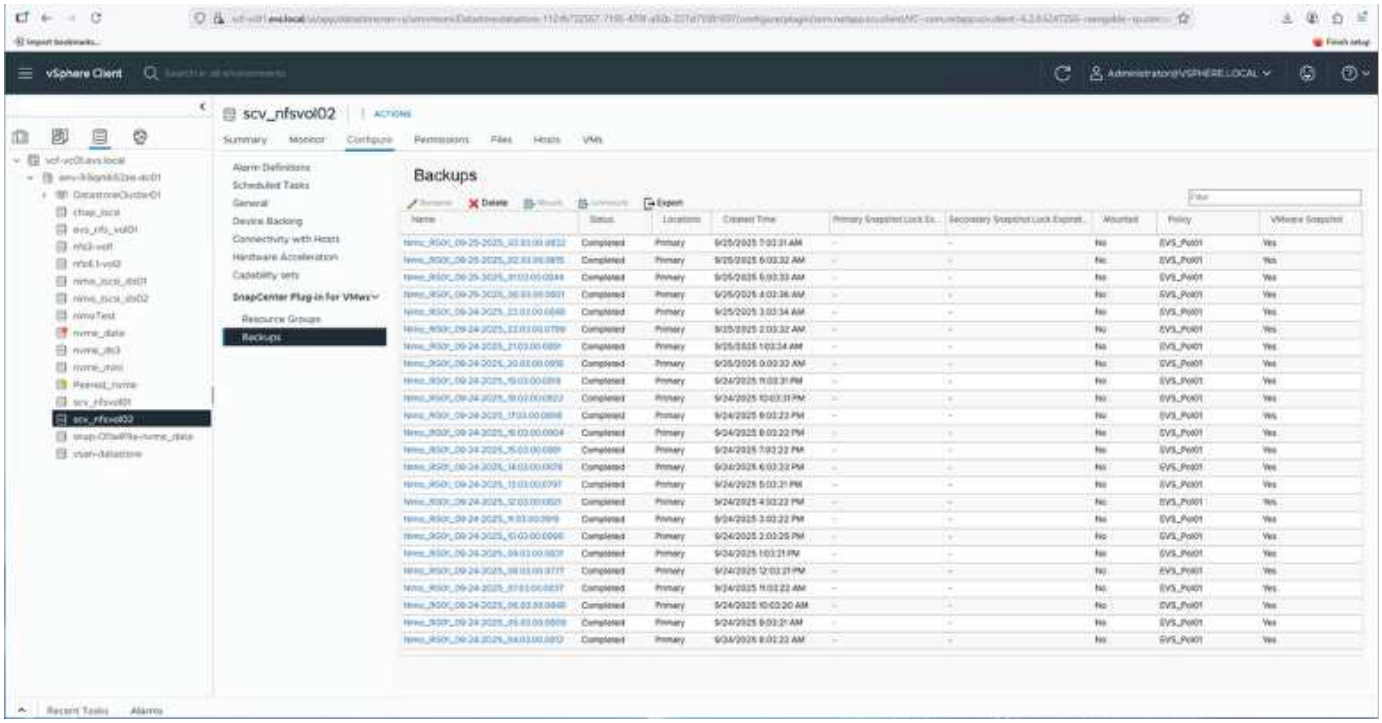


ウィンドウの下部にある「最近のタスク」を選択して操作の進行状況を監視するか、ダッシュボードで「ジョブ モニター」を選択して詳細を確認します。

バックアップ ポリシーの作成、リソース グループの設定、およびバックアップ操作の実行のプロセスは、NFS や iSCSI などのさまざまなストレージ プロトコル間で一貫しています。

バックアップは、ポリシーで定義されたスケジュールに従って実行されます。

バックアップが完了したら、ドロップダウン リストから「SnapCenter Plug-in for VMware vSphere」を選択し、「リストア」を選択することで、データストア レベルまたは個々の VM について表示できます。



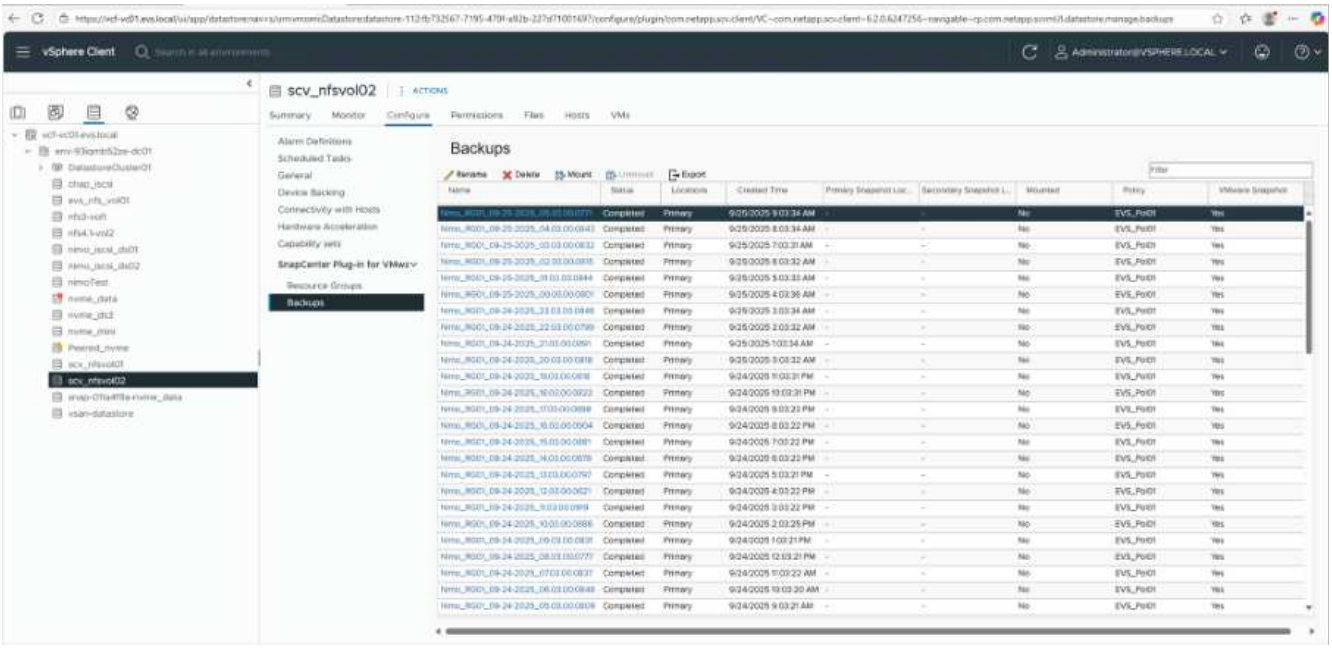
SnapCenter Plug-in for VMware vSphereで保護されているVMのリストア手順

このセクションでは、バックアップから VM を復元する手順について説明します。SCV を使用すると、vCenter 内で VM を復元でき、元の ESXi ホスト上の元のデータストアへの復元（既存のコンテンツを上書き）、バックアップコピーから削除または名前変更された VM の復元、元の ESXi ホスト上の別のデータストアへの復元、同じ vCenter で管理されている別の ESXi ホスト上の元のデータストアへの復元、または同じ vCenter 環境内の別の ESXi ホスト上の別のデータストアへの復元が可能です。

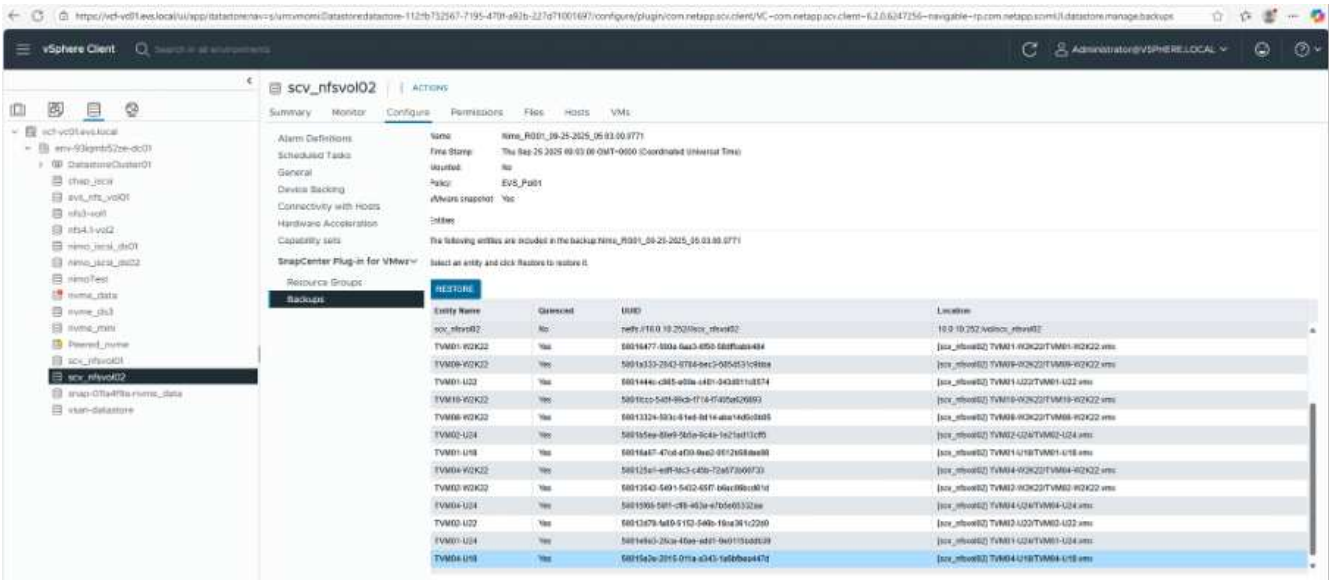
リストア操作を実行する手順

リストア処理を実行するには、次の手順を実行します。

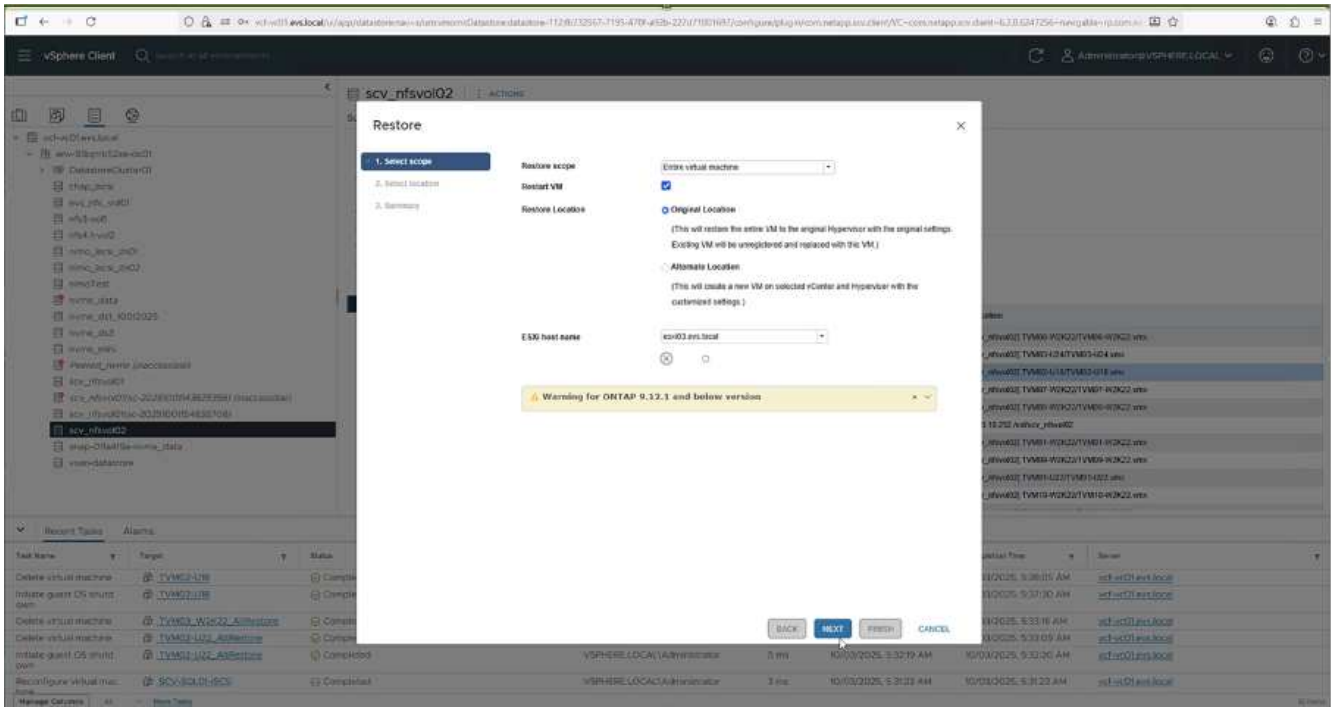
1. EVS vSphere Web クライアント GUI で、「インベントリ > データストア」に移動し、目的のデータストアを選択します。次に、「SnapCenter Plug-in for VMware vSphere」セクションの「設定 > バックアップ」に移動します。



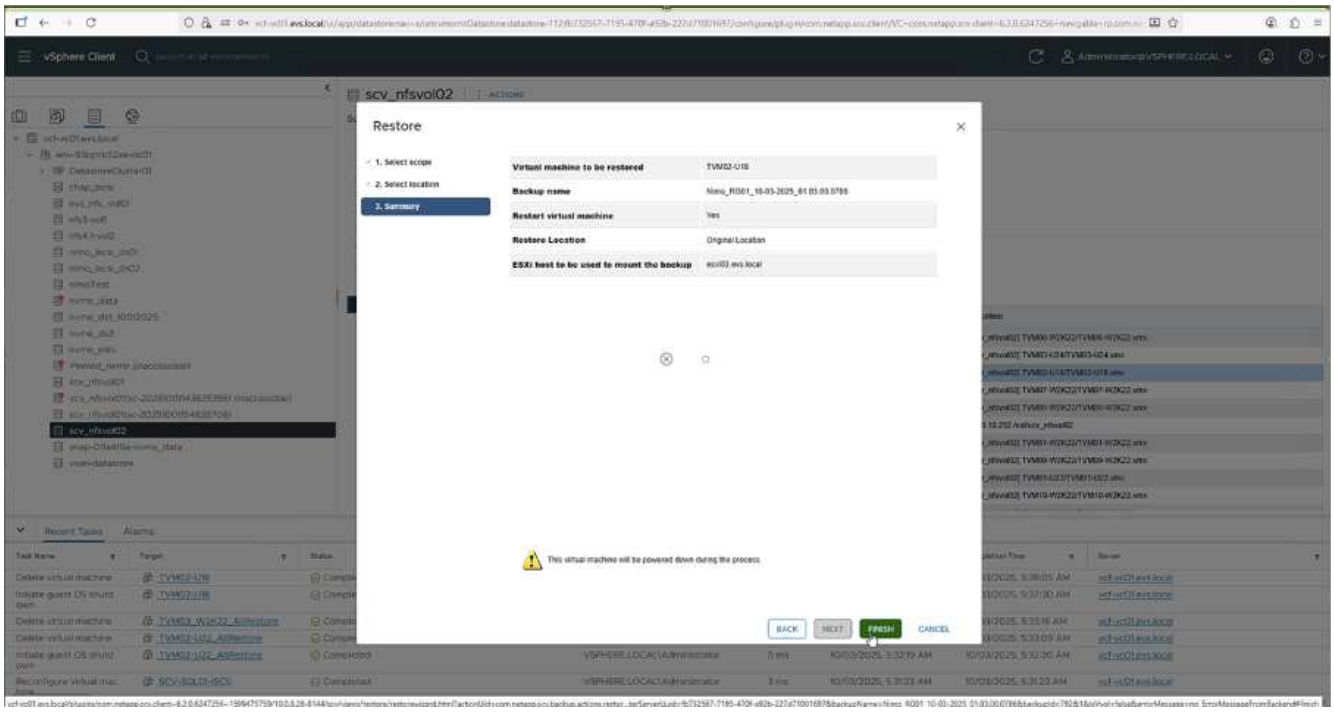
2. バックアップをダブルクリックすると、そのバックアップに含まれるすべての VM が表示されます。リストから復元する VM を見つけて、「復元」を選択します。



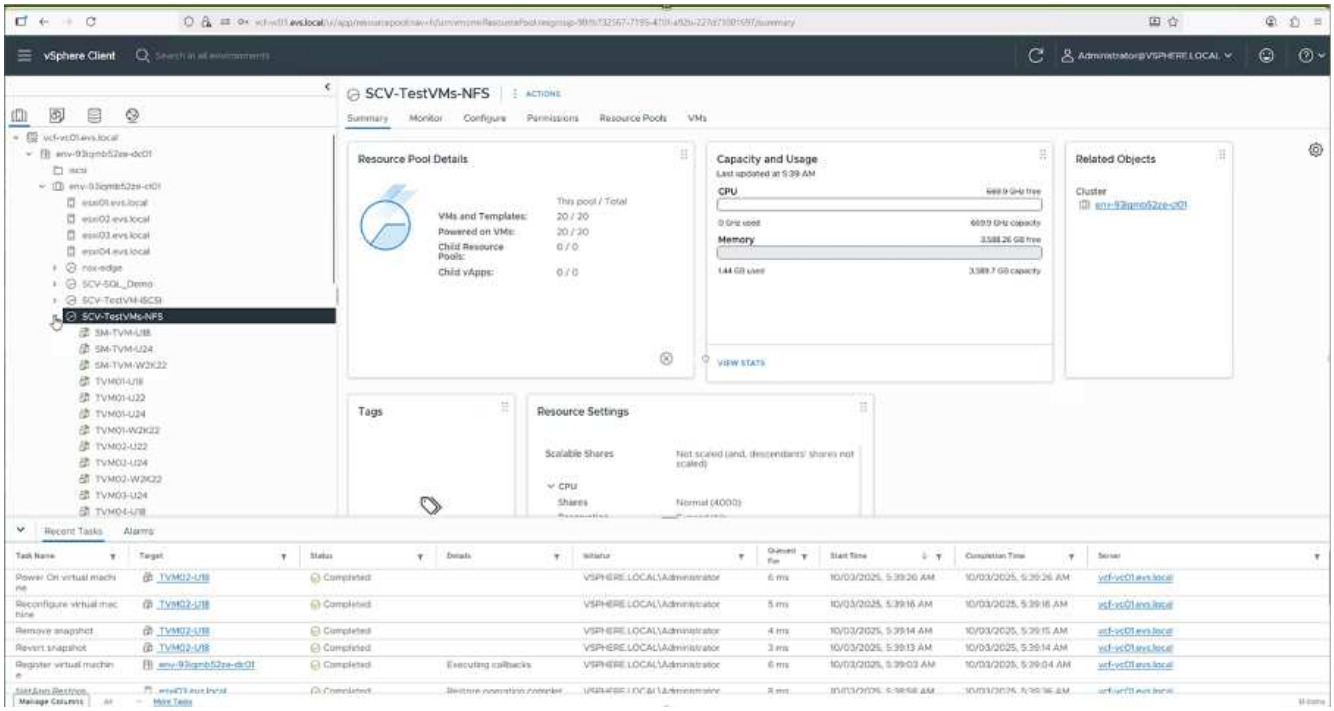
3. 「範囲の選択」ページで、「復元範囲」フィールドで「仮想マシン全体」を選択し、「復元場所」を選択して、バックアップをマウントする宛先ESXi情報を入力します。
4. 復元操作後に VM の電源をオンにする必要がある場合は、「VM を再起動」チェックボックスを有効にします。
5. 「場所の選択ページ」で、プライマリロケーションを選択します。



6. 「概要」ページを確認し、「完了」を選択します。



7. 画面下部の「最近のタスク」を選択して、操作の進行状況を監視します。



VM は復元されますが、以前のリソース グループに自動的に追加されるわけではありません。これらの VM を保護する場合は、適切なリソース グループに手動で追加します。

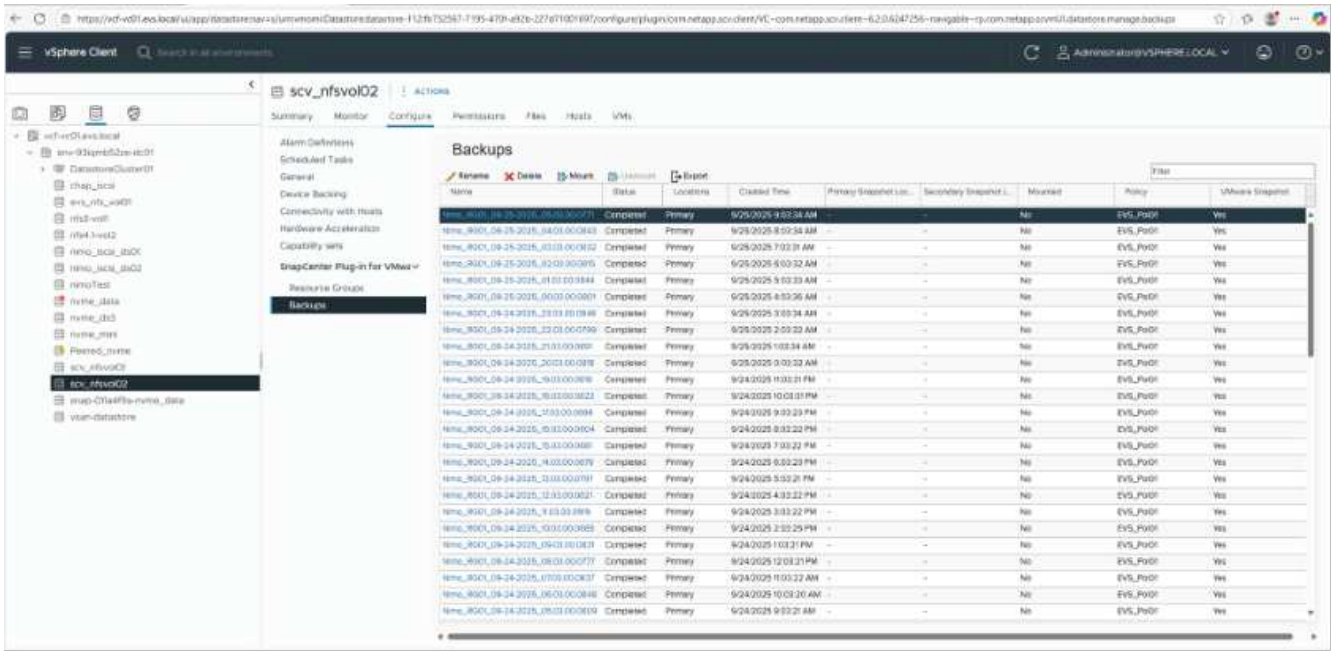
リストア処理は、個々の VM レベルからトリガーすることもできます。

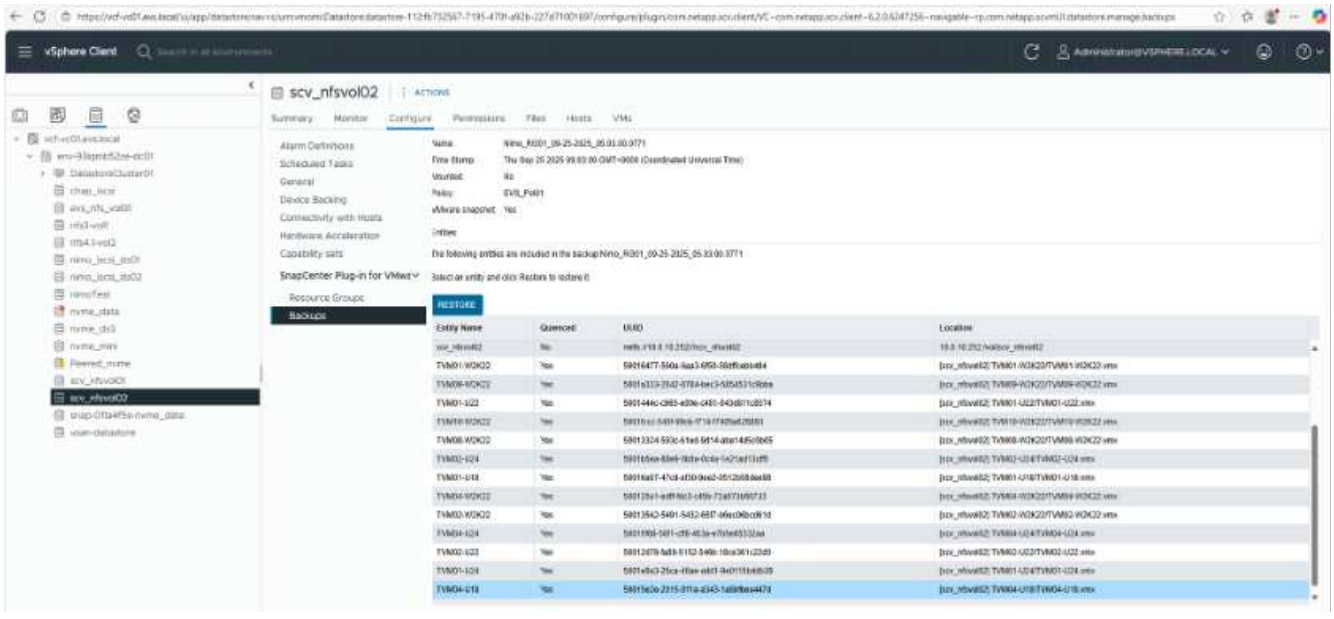
削除された **VM** を復元する手順

削除された VM のリストアは、SCV を使用すると簡単なプロセスです。

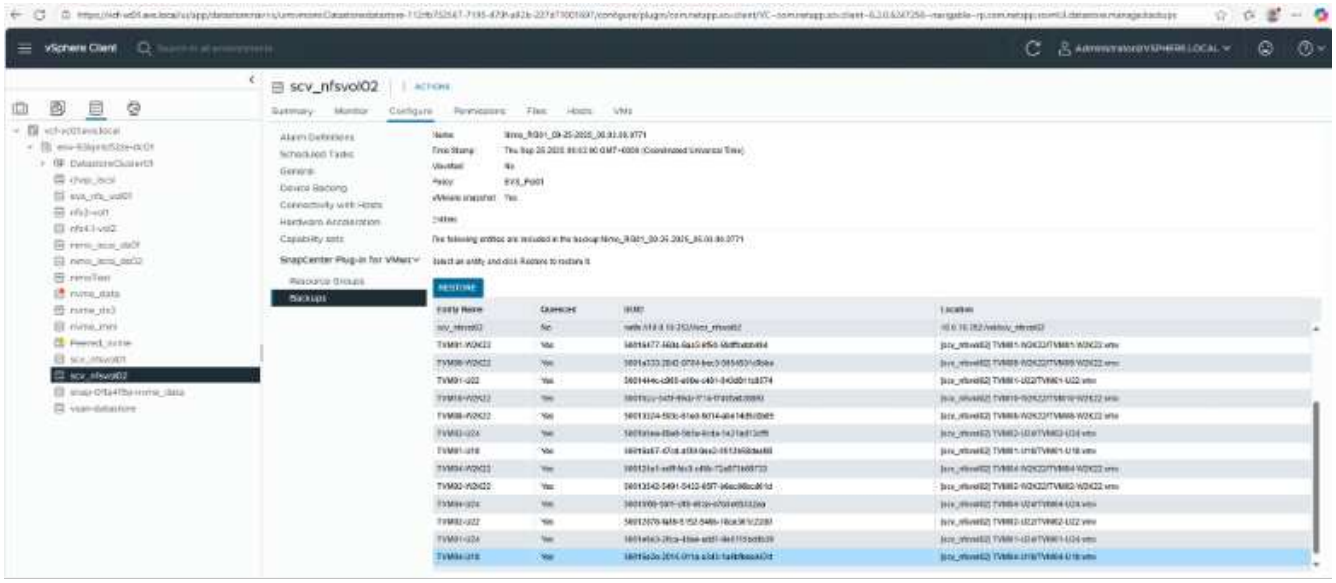
削除された VM の復元操作は、データストア レベルから実行できます。

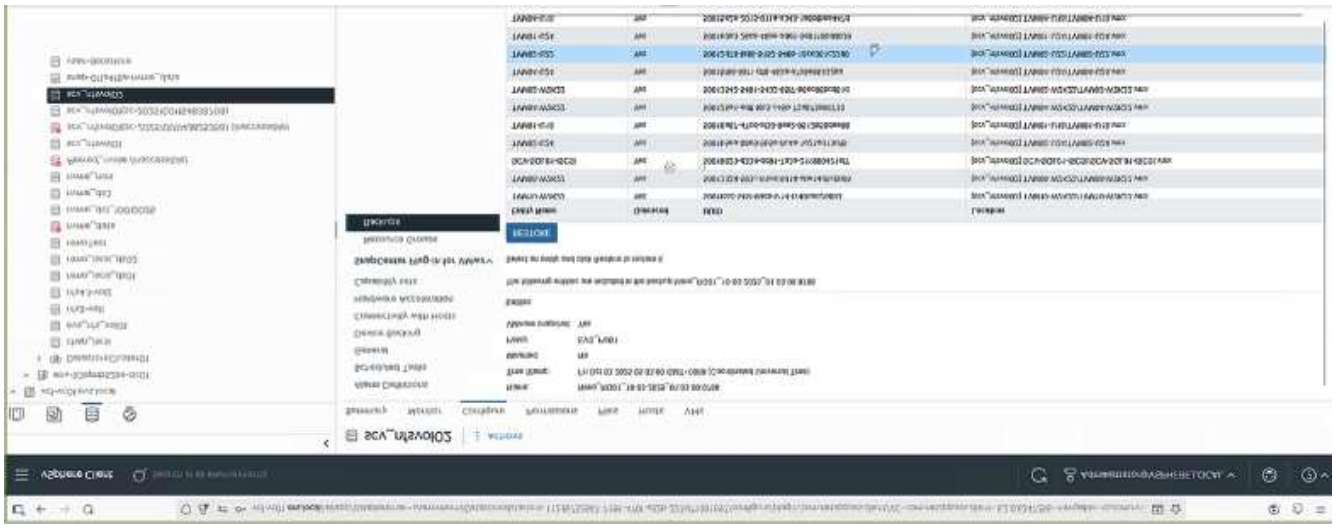
1. それぞれのデータストア > 構成 > バックアップに移動します。そこで、削除された VM を選択し、「復元」を選択します。

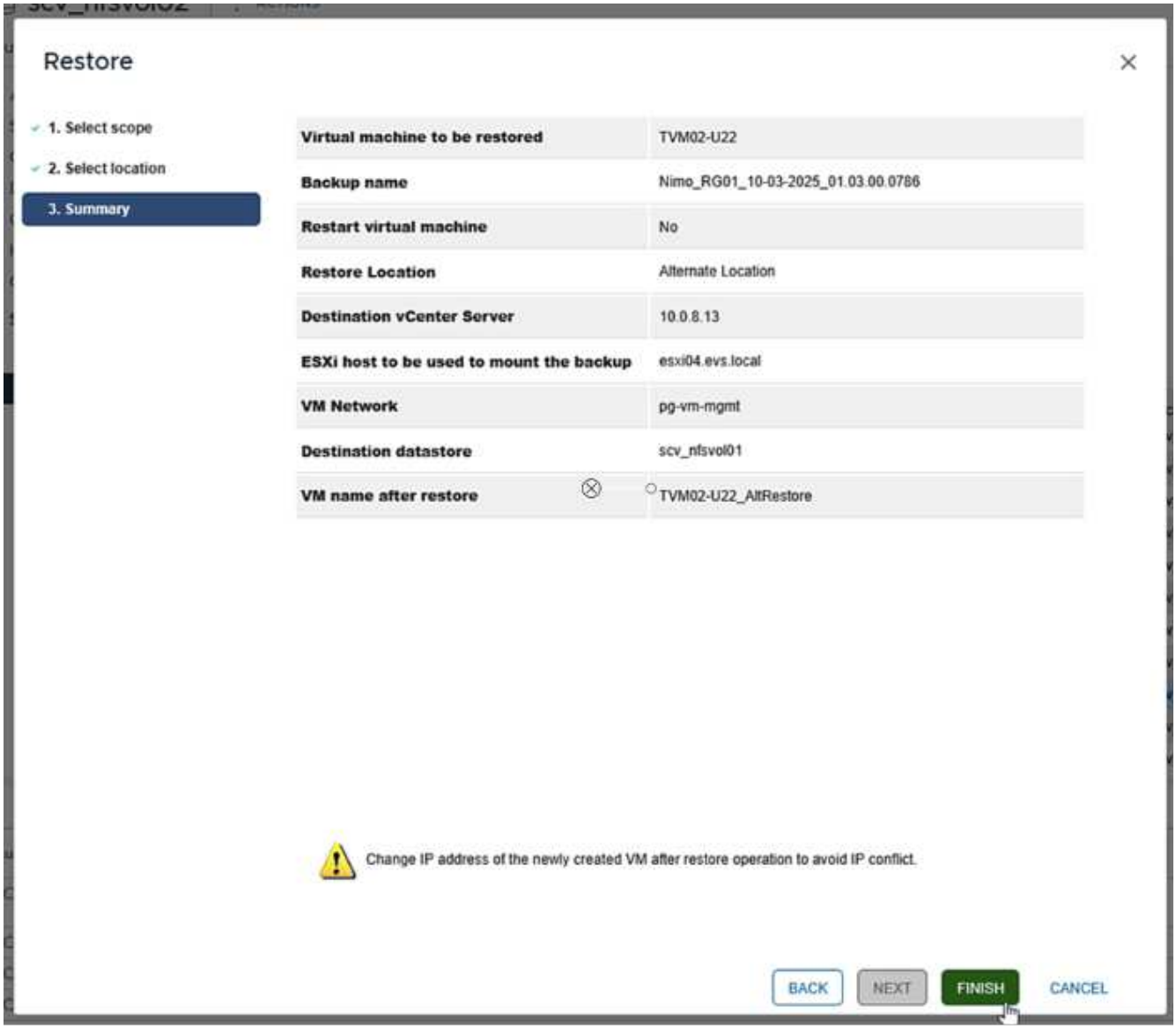


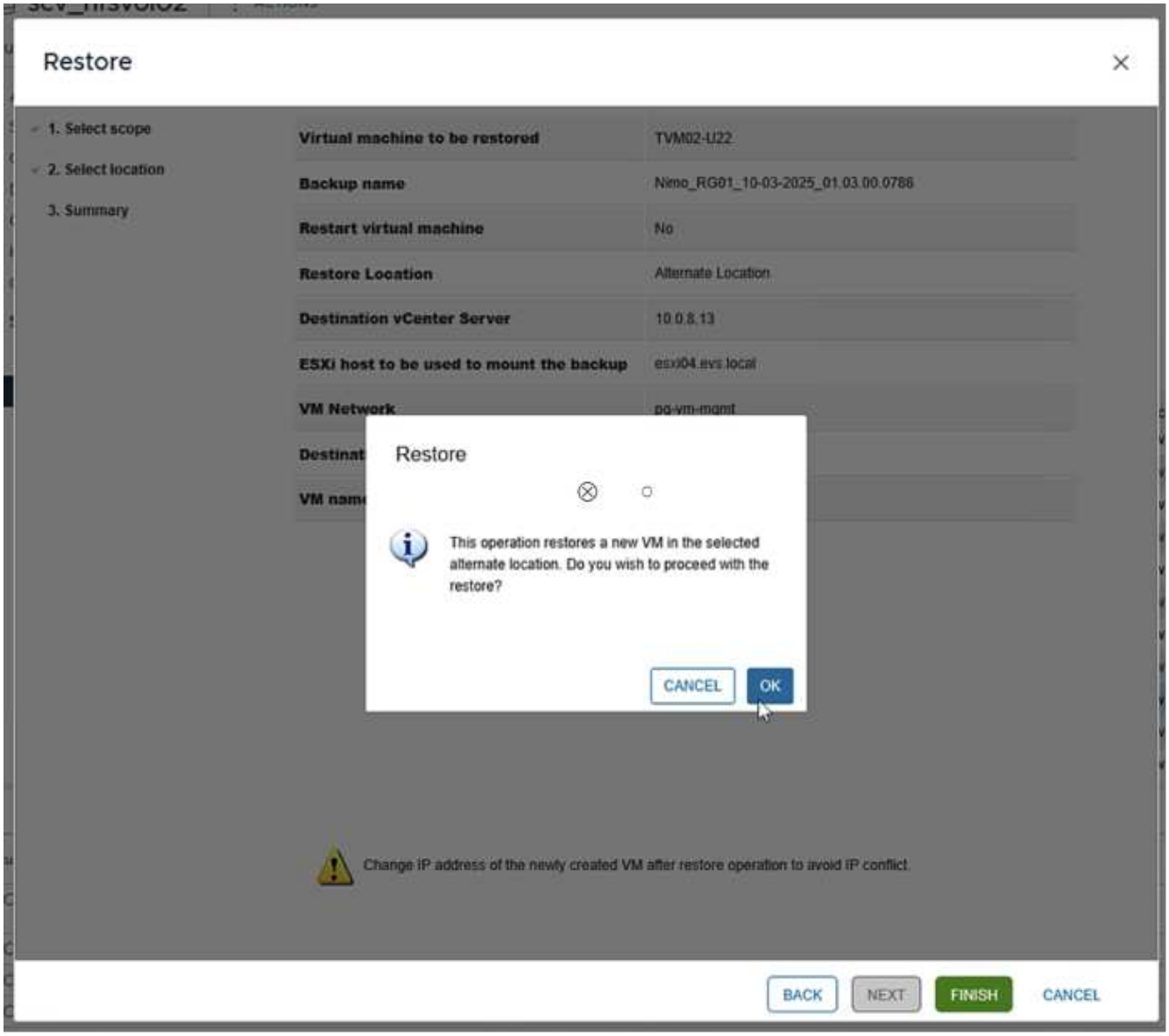


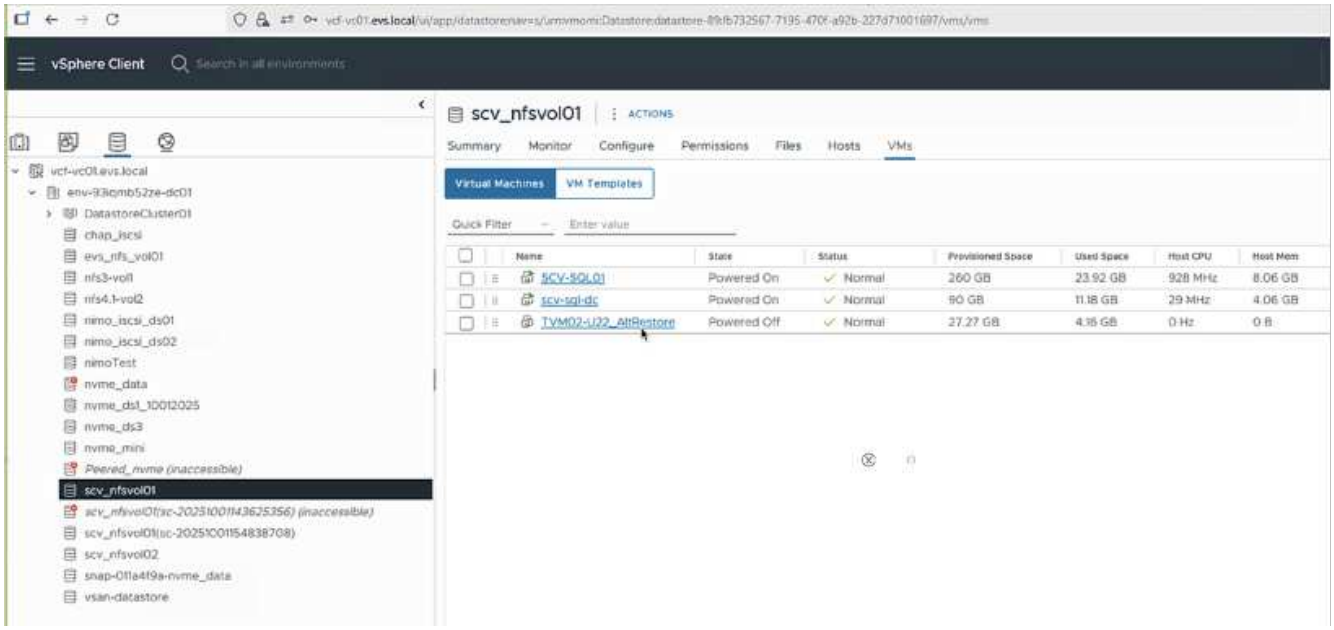
2. 次のスクリーンショットのフローは、代替 ESXi ホストと別のデータストアへの VM のリストアについて説明します。


vSphere Client
scv_nfsvol02
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
SnapCenter Plug-in for VMware
Resource Groups
Backups
RESTORE


vSphere Client
scv_nfsvol02
SnapCenter Plug-in for VMware
Backups
RESTORE


Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Destination datastore
scv_nfsvol01
VM name after restore
TVM02-U22_AltRestore
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL

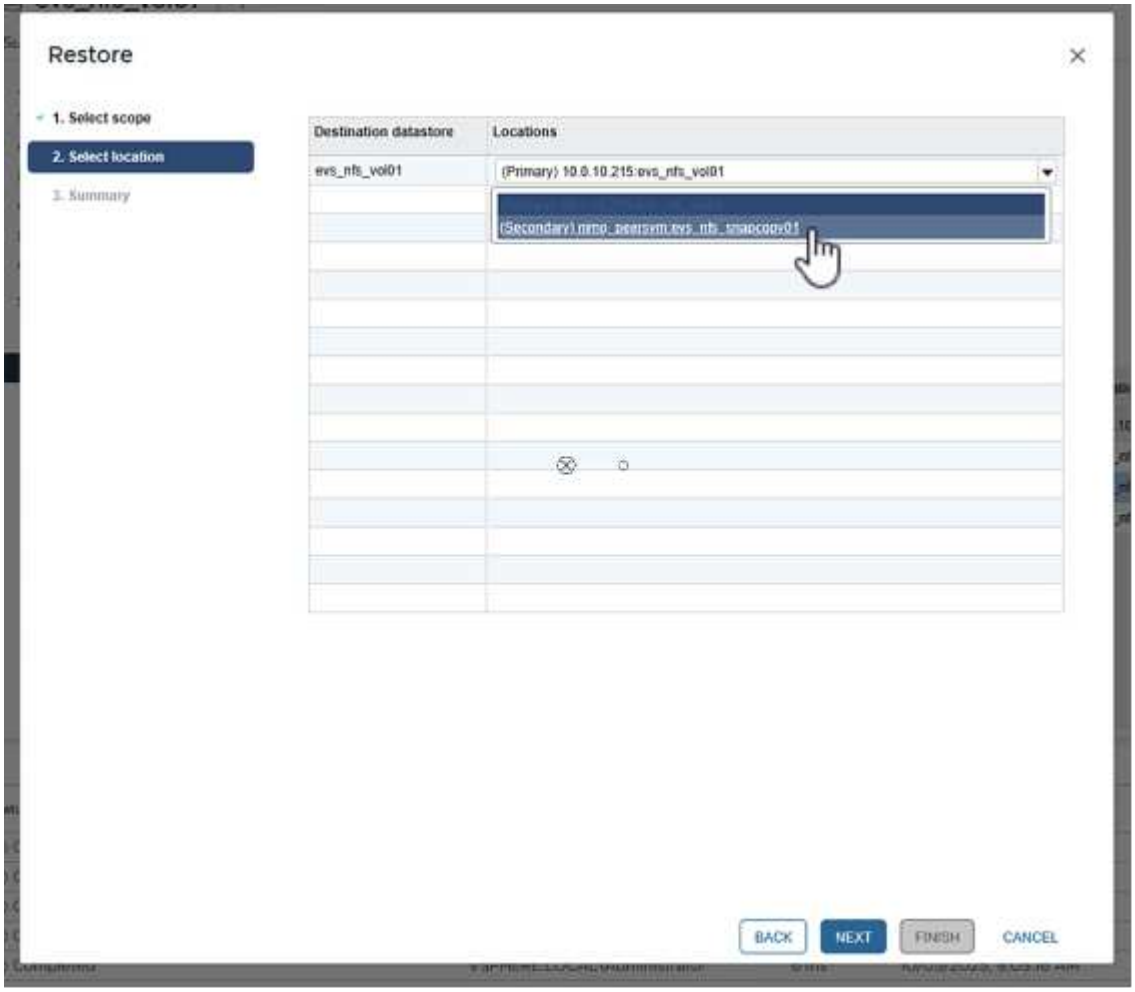

Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Restore
This operation restores a new VM in the selected alternate location. Do you wish to proceed with the restore?
CANCEL
OK
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL


vSphere Client
scv_nfsvol01
ACTIONS
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
Virtual Machines
VM Templates
Quick Filter
Enter value
Name
State
Status
Provisioned Space
Used Space
Host CPU
Host Mem
SCV-SQL01
Powered On
Normal
260 GB
23.92 GB
928 MHz
8.06 GB
scv-sql-dc
Powered On
Normal
90 GB
11.18 GB
29 MHz
4.06 GB
TVM02-U22_AltRestore
Powered Off
Normal
27.27 GB
4.16 GB
0 Hz
0 B
vcf-vc01.evs.local
env-93ojmb52ze-dc01
DatastoreCluster01
chap_iscsi
evs_nfs_vol01
nfs3-vol1
nfs4.1-vol2
nimo_iscsi_ds01
nimo_iscsi_ds02
nimoTest
nvme_data
nvme_ds1_10012025
nvme_ds3
nvme_mini
Peered_nvme (inaccessible)
scv_nfsvol01
scv_nfsvol01(sc-20251001154838708)
scv_nfsvol02
snap-011a4f9a-nvme_data
vsan-datastore

宛先データストアには十分な空き容量が必要であり、「別の場所に復元」フィールドに指定されているvCenterはDNS解決可能である必要があります。

NFS環境での復元効率を高めるには、VMware vStorage API for Array Integration（VAAI）を有効にします。

復元は、SnapMirrorデスティネーションなどのセカンダリロケーションから実行することもできます。



+

SnapCenter Plug-in for VMwareで保護されているゲストファイルとフォルダの復元手順

次のセクションでは、VMDK からゲスト ファイルとフォルダーを復元する方法を示します。

SnapCenterは、ゲスト オペレーティング システムが Windows の場合にのみ、VMDK からのファイルとフォルダーの復元をサポートします。

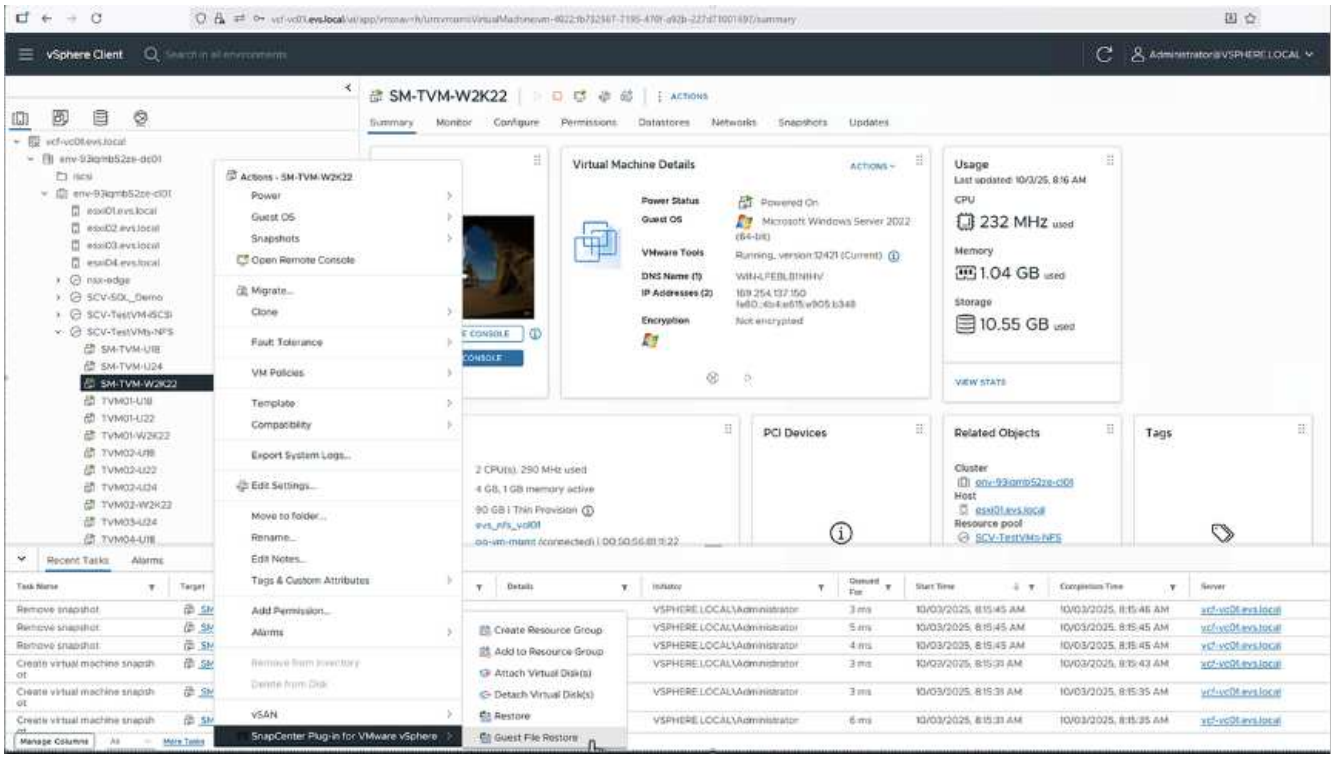
SCV を使用したゲスト ファイルとフォルダのリストアに関する考慮事項：

- VM 上で VMware ツールが実行されている必要があります。

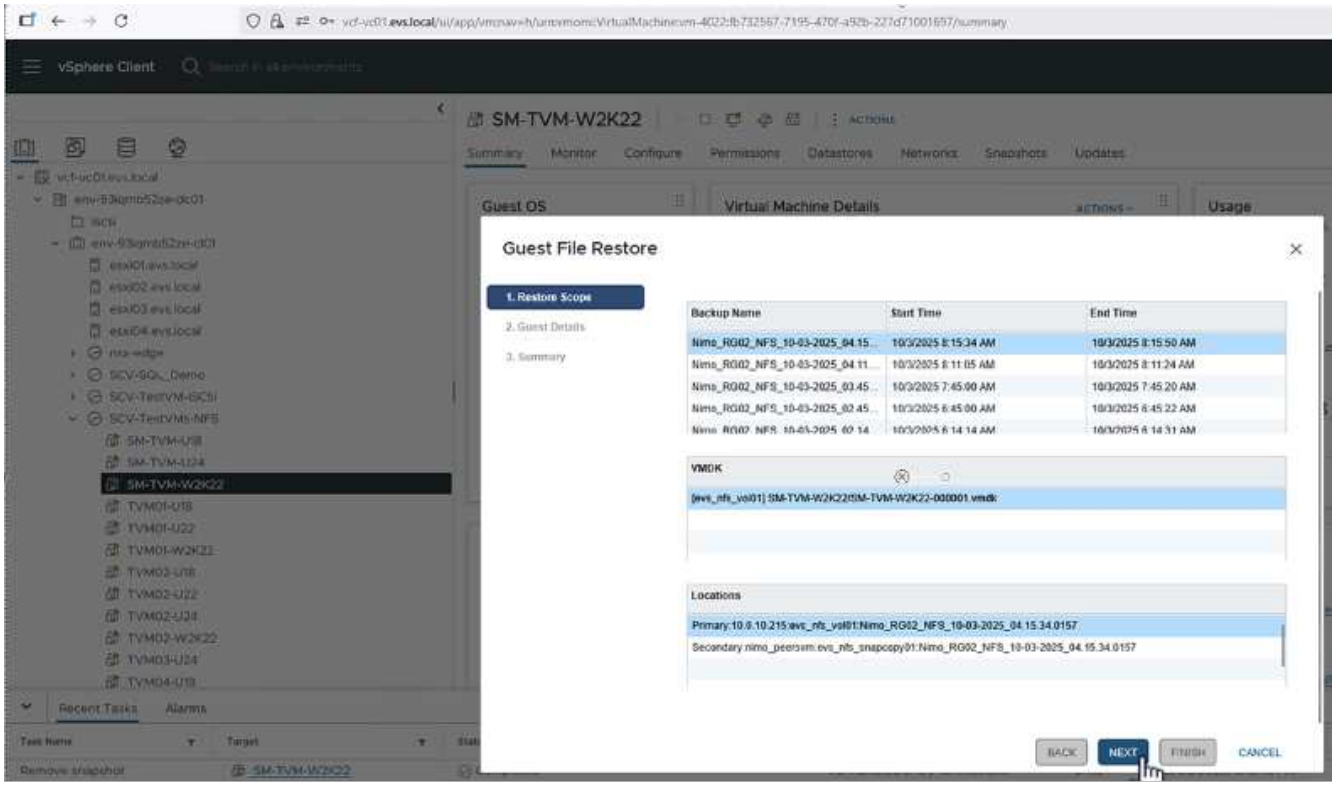
- アタッチされた VMDK には、デフォルトで 24 時間アクセスできます。
- 仮想マシンでは一度に 1 つのリストアまたは接続操作のみ実行できます。
- システム ファイル、隠しファイル、暗号化されたファイルは復元できますが、元の属性は保持されません。
- 暗号化されたファイルを暗号化されたフォルダーに復元したり、システム ファイルを上書きしたりしないでください。

ゲストファイルとフォルダの復元手順：

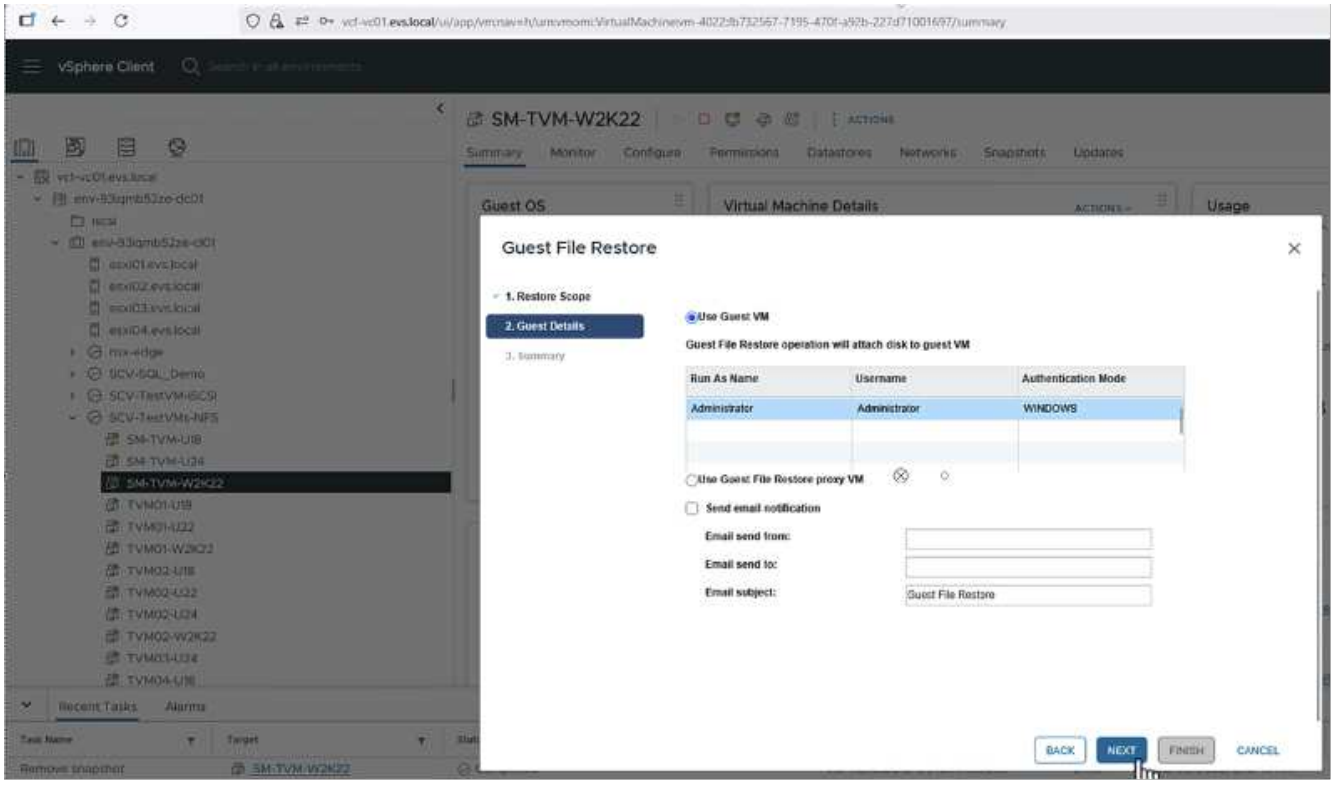
1. 対象のVMを右クリックし、「NetApp SnapCenter > Guest File Restore」を選択します。



2. 必要な VMDK を含むバックアップを選択します。VMDK とその場所（プライマリまたはセカンダリ）を指定します。

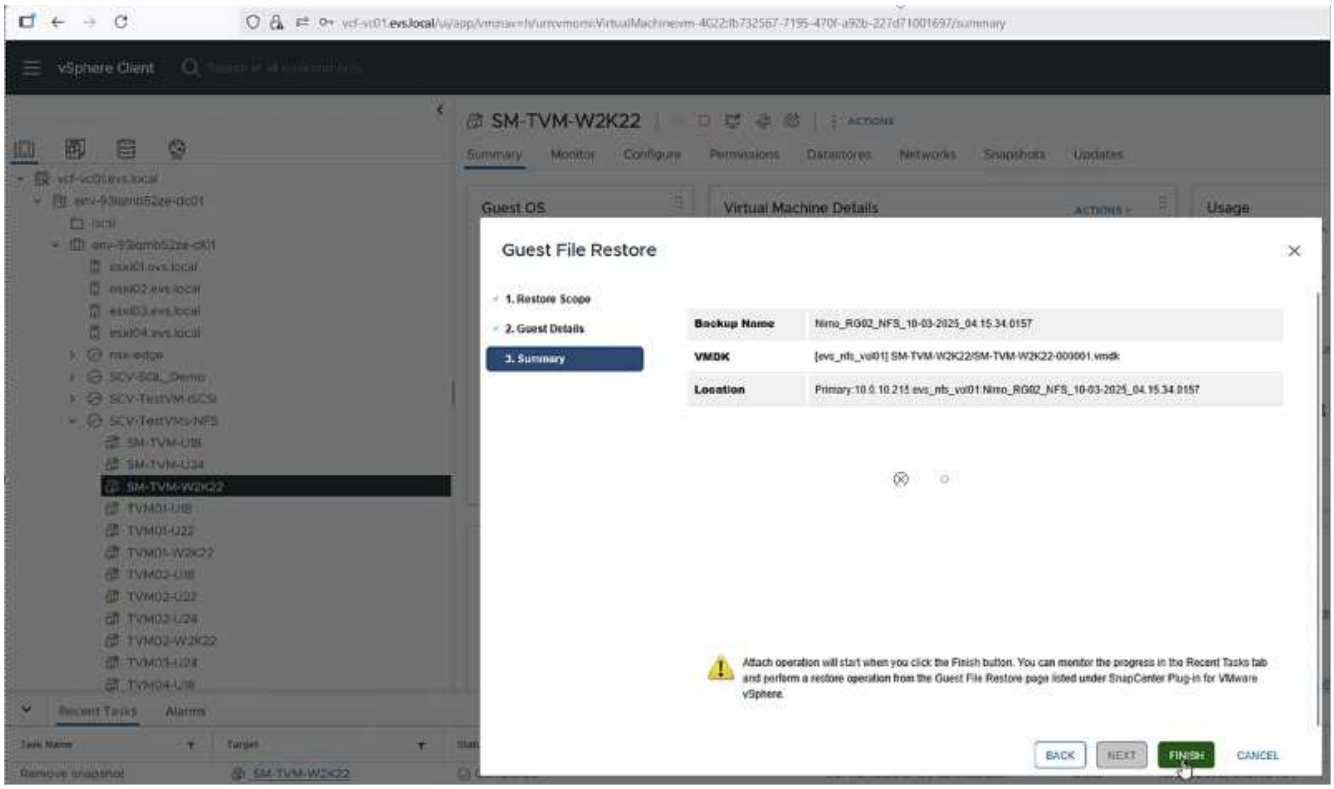


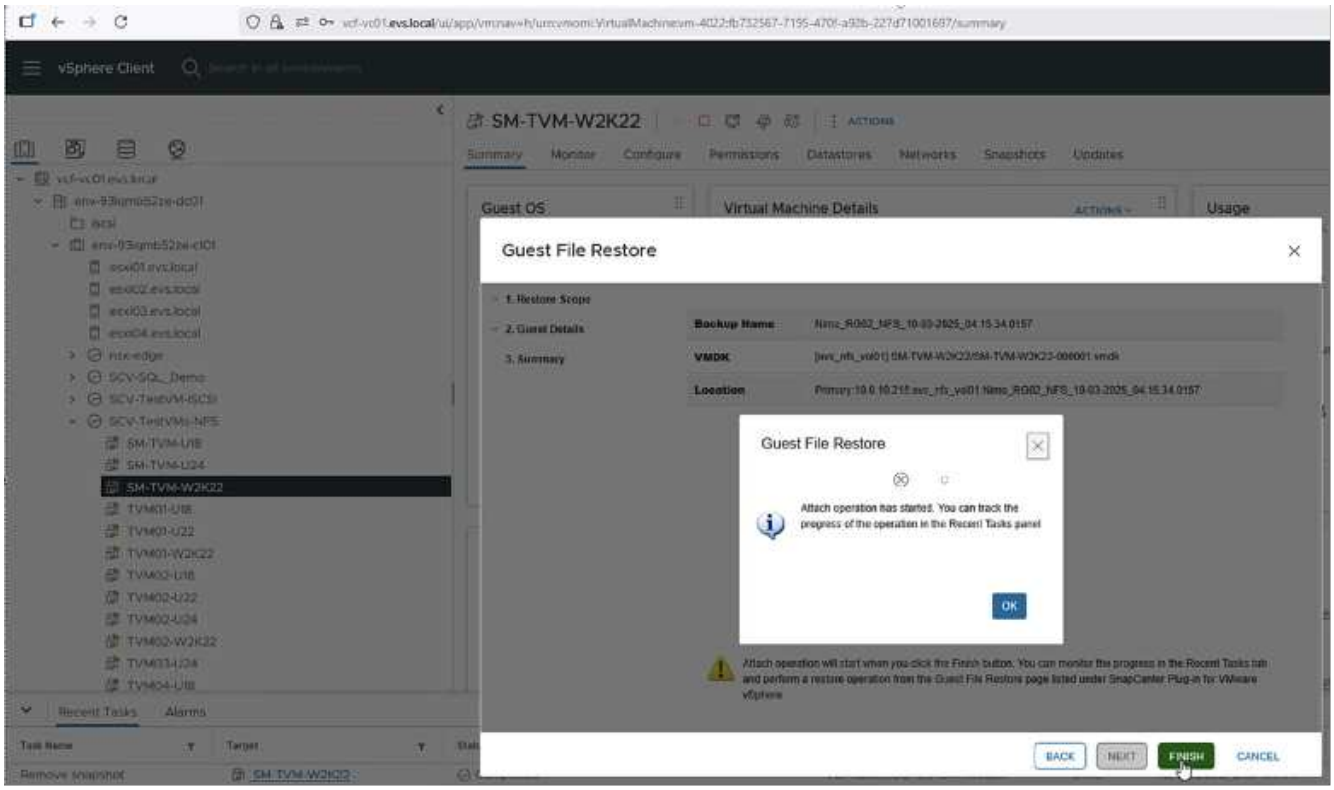
3. 「ディスク接続方法」を選択します。



- ゲスト VM オプション：ディスクを元の VM に接続します（事前に構成された資格情報が必要です）。これは、このデモで使用されるオプションです。
- プロキシ VM オプション：指定されたプロキシ VM にディスクを接続します（事前に構成する必要があります）。

4. ファイルを参照して復元する前に、添付操作が完了するまで待機してください。操作が完了すると、SnapCenter はゲスト ファイルの復元セッションを自動的に作成します。





5. ゲスト ファイル復元セッションで VMDK を参照し、必要なファイルまたはフォルダーを選択して、指定された場所に復元します。

VMware VMDK上で実行されるデータベースの保護手順（SnapCenter for SQL（SCSQL））

次のセクションでは、SnapCenter for SQL（SCSQL）を使用して、VMware VMDK上で実行されているデータベースを保護する方法を説明します。

SCSQLのセットアップ

SCSQL を使用して VMDK 上のデータベースを保護するための設定は次のとおりです：

1. "インストールと設定" SnapCenter Server。
2. SnapCenterにログインします。
3. SnapCenter 環境を設定します。
   - "追加または割り当て"ストレージ システム接続。
   - "作成"クレデンシャル。
4. VMware VMDK 上の Microsoft SQL Server データベースの場合：
   - "SCVを導入する"（セットアップのセクションで既に説明されています）。
   - プラグインをSnapCenterに登録します。
5. "SQL Server ホストとプラグインのインストール"を追加：
   - "SQL プラグインを設定する"。
   - "データベースとログの保護プランとスケジュールを設定する"。

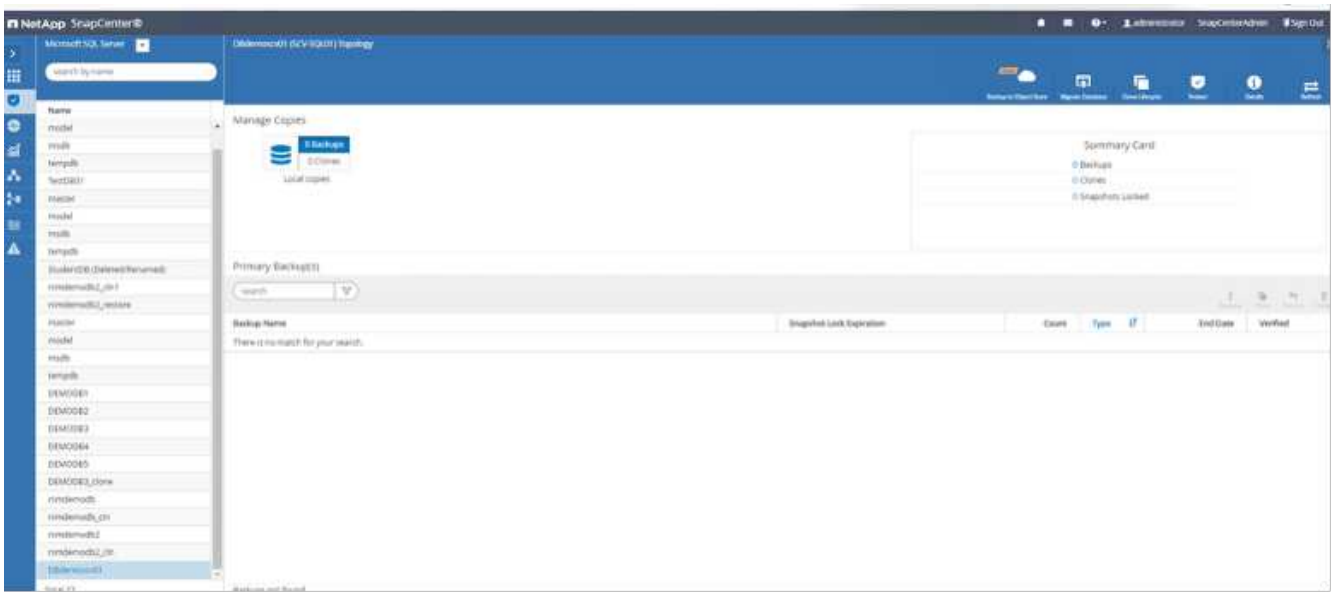


バックアップ ポリシーの設定

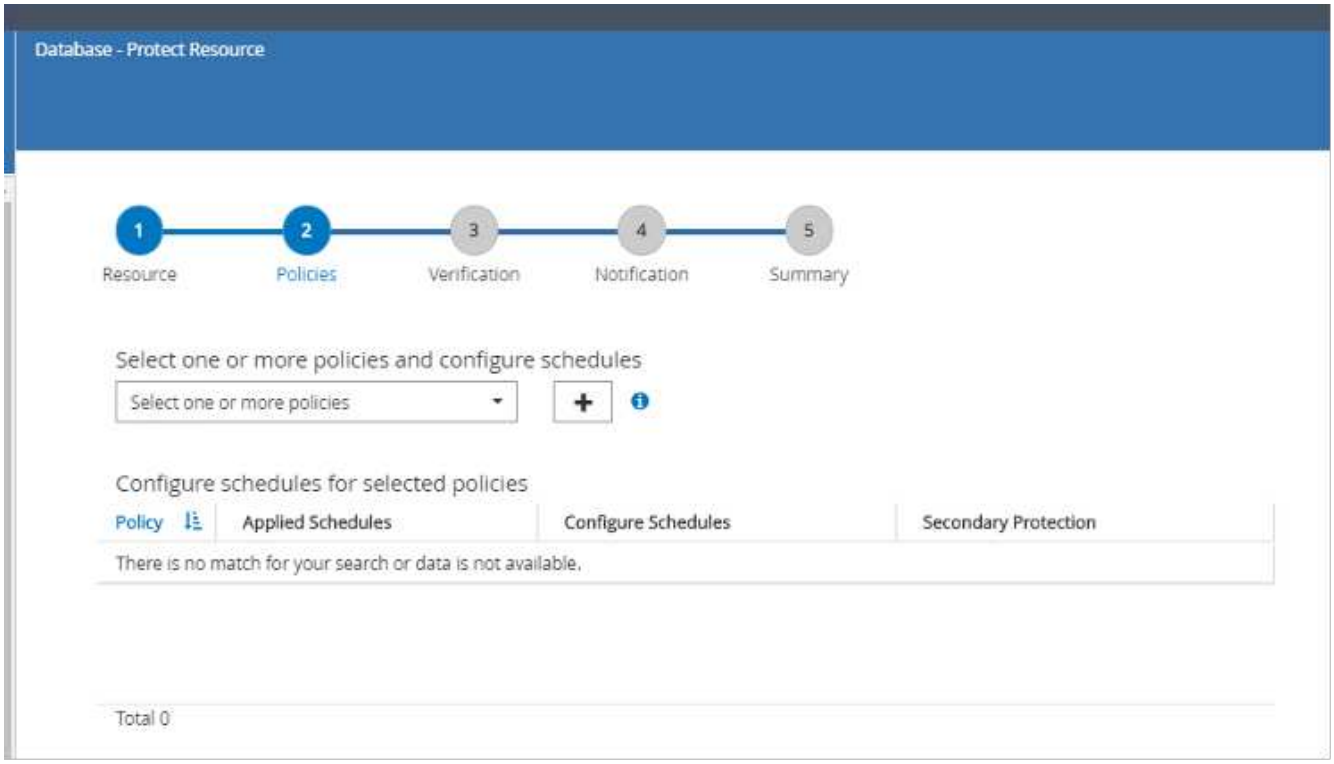
次の手順では、バックアップ ポリシーの設定方法を説明します。

1. リソース タブからデータベースを選択し、右上隅の「保護」を選択します。

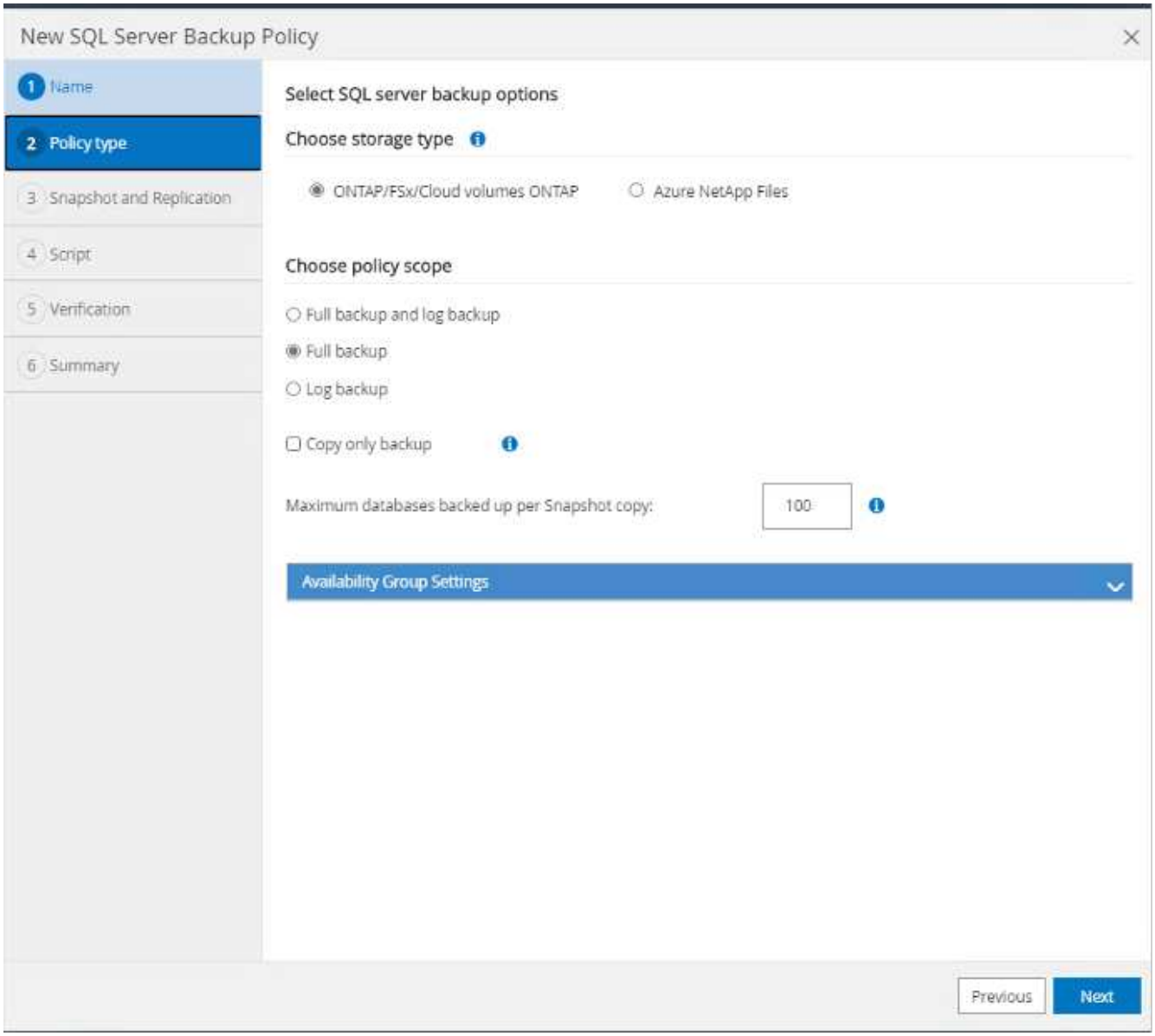
検証は、ゲスト VM 上で実行されている Microsoft SQL Server データベースに対して実行されます。



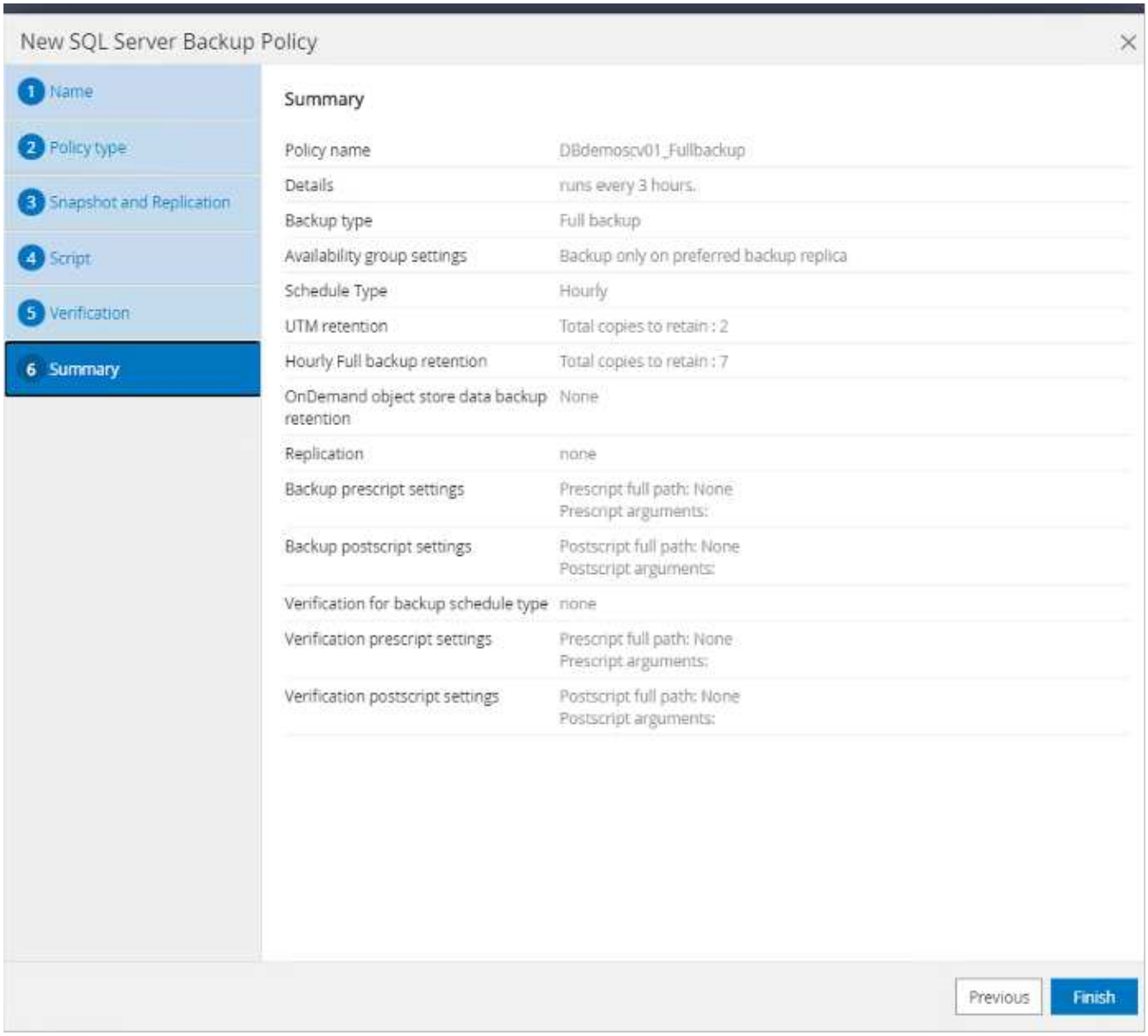
2. プラス記号アイコンをクリックして、Microsoft SQL Serverのバックアップ ポリシーを設定します。



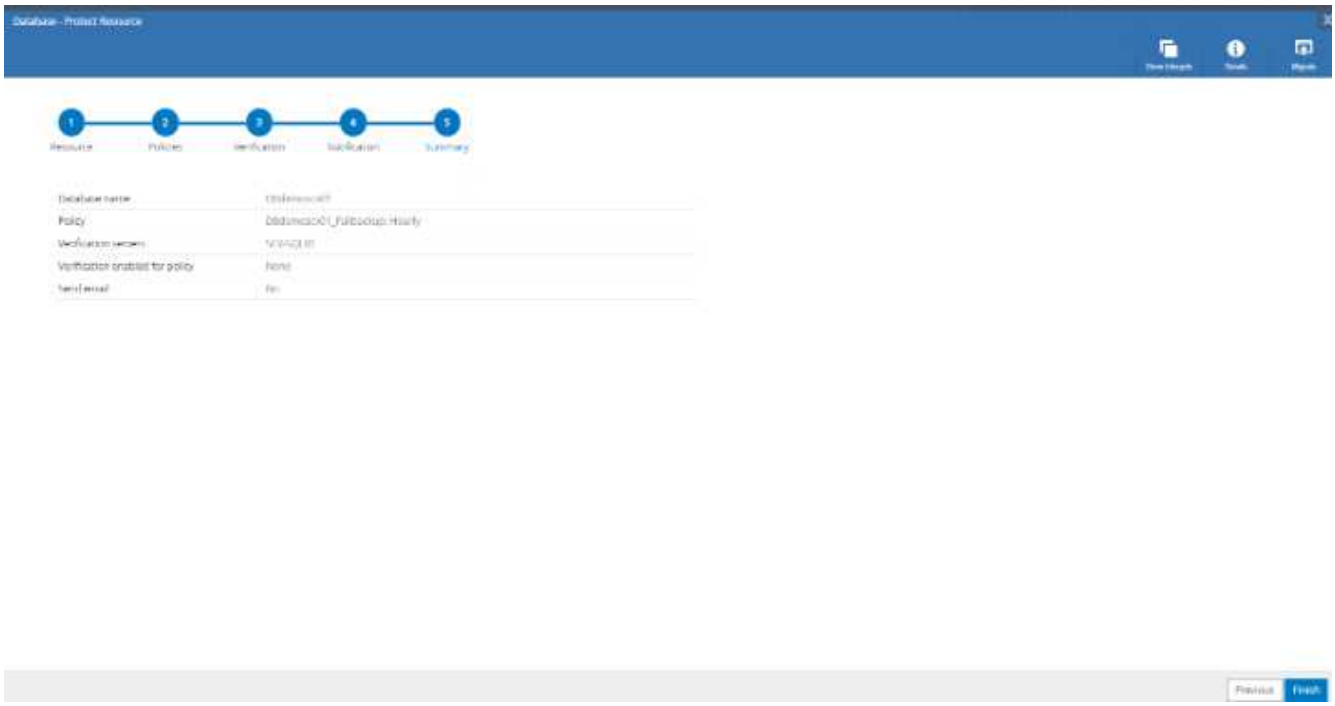
3. このデモでは、「フルバックアップ」が選択されています。「次へ」を選択して続行します。



4. 概要ページで、「完了」を選択します。


New SQL Server Backup Policy
1 Name
2 Policy type
3 Snapshot and Replication
4 Script
5 Verification
6 Summary
Summary
Policy name
DBdemoscv01_Fullbackup
Details
runs every 3 hours.
Backup type
Full backup
Availability group settings
Backup only on preferred backup replica
Schedule Type
Hourly
UTM retention
Total copies to retain : 2
Hourly Full backup retention
Total copies to retain : 7
OnDemand object store data backup retention
None
Replication
none
Backup prescript settings
Prescript full path: None
Prescript arguments:
Backup postscript settings
Postscript full path: None
Postscript arguments:
Verification for backup schedule type
none
Verification prescript settings
Prescript full path: None
Prescript arguments:
Verification postscript settings
Postscript full path: None
Postscript arguments:
Previous
Finish

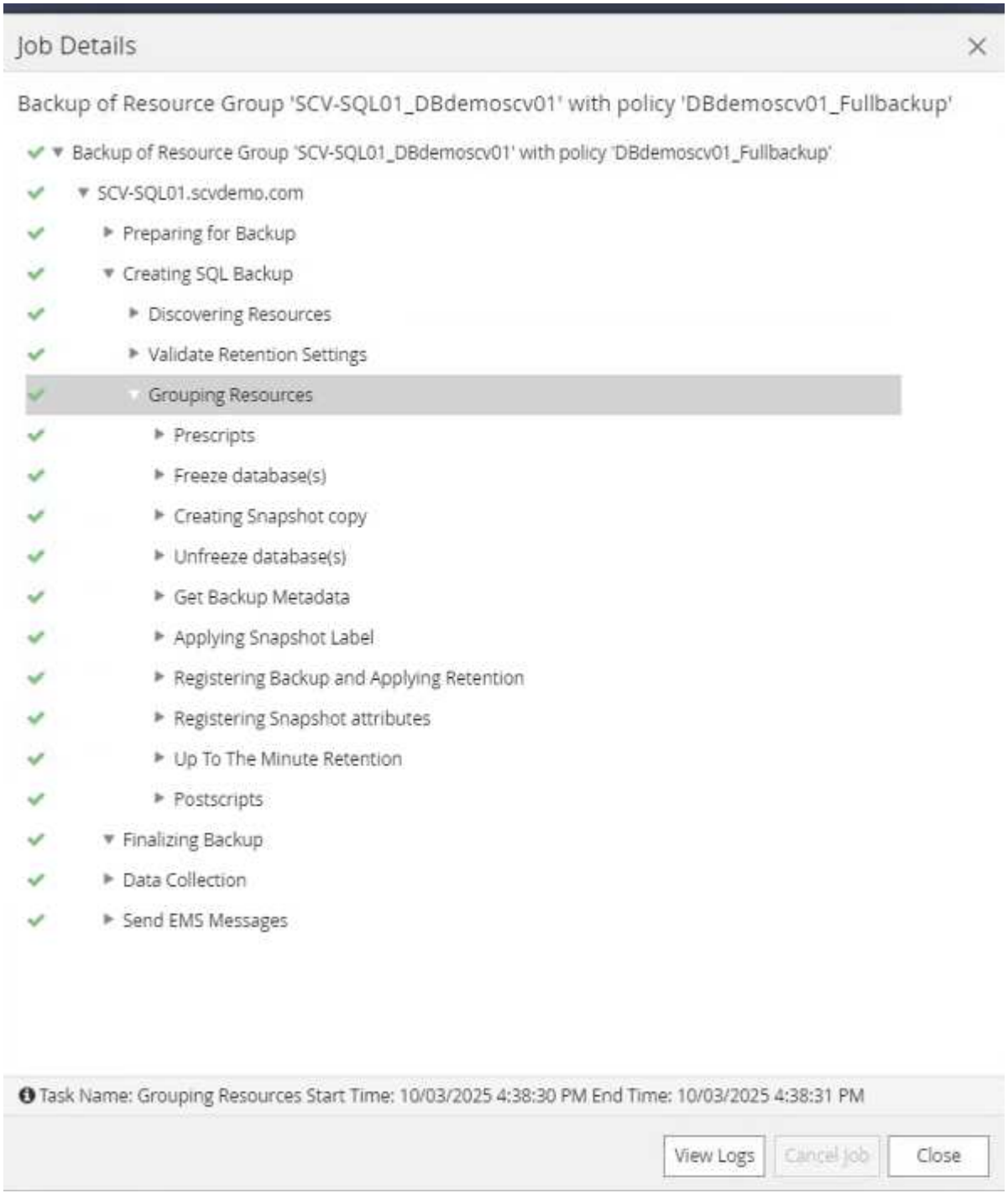
5. 「完了」に進みます。



バックアップの監視

バックアップ ポリシーを設定したら、バックアップ操作の実行を監視できます。これを行うには、今すぐバックアップをクリックしてオンデマンド バックアップ操作をトリガーするか、スケジュールされたバックアップ ポリシーが開始されるまで待ちます。

1. 「モニター > ジョブ」を使用してジョブの進行状況を監視します。
2. バックアップ ジョブを選択し、「詳細」をクリックすると、以下のようにジョブの詳細が表示されます。

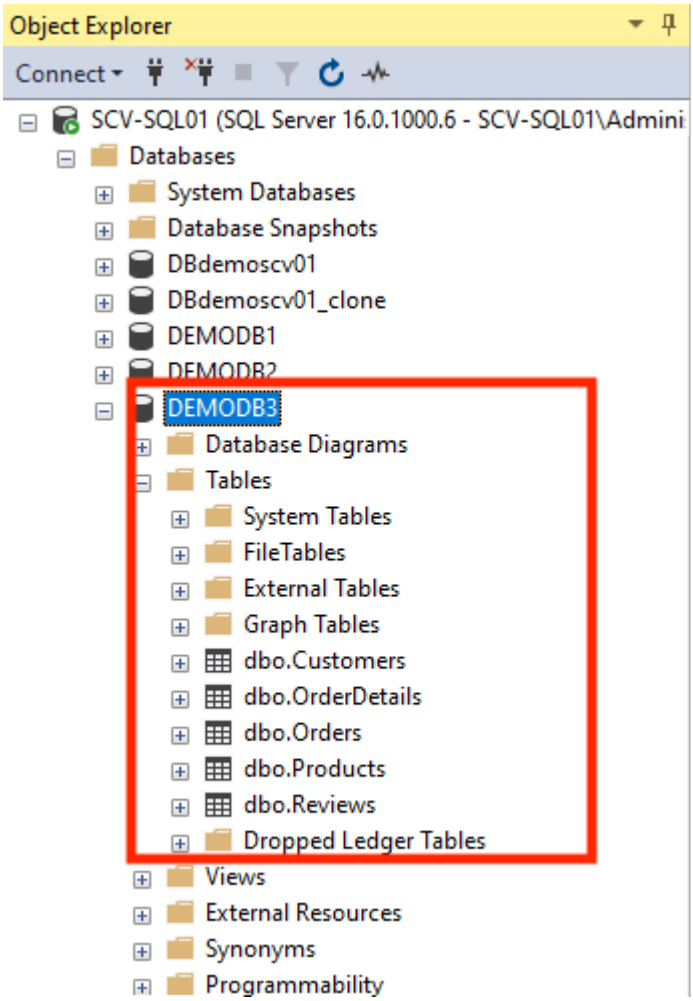


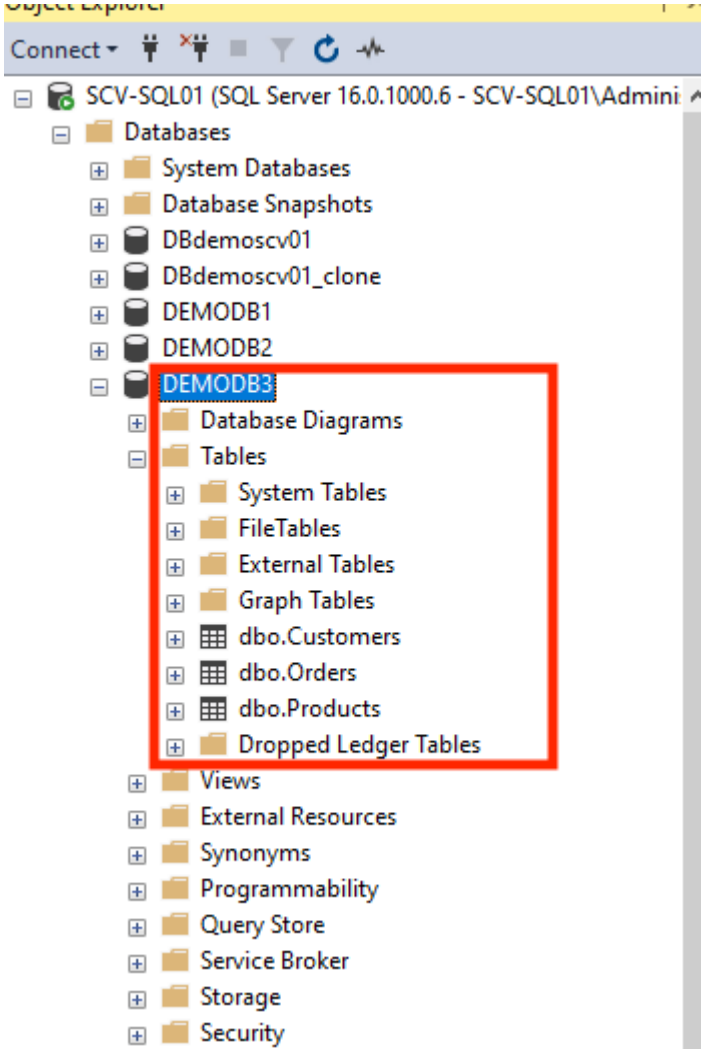
VMDK 上にあるデータベースのリストア

VMDK 上のデータベースを特定の時点に復元できます。

データベース内のいくつかのテーブルを削除することで、この重要性をシミュレートすることができます。その後、ポイントインタイム リストアを実行することで修正されます。

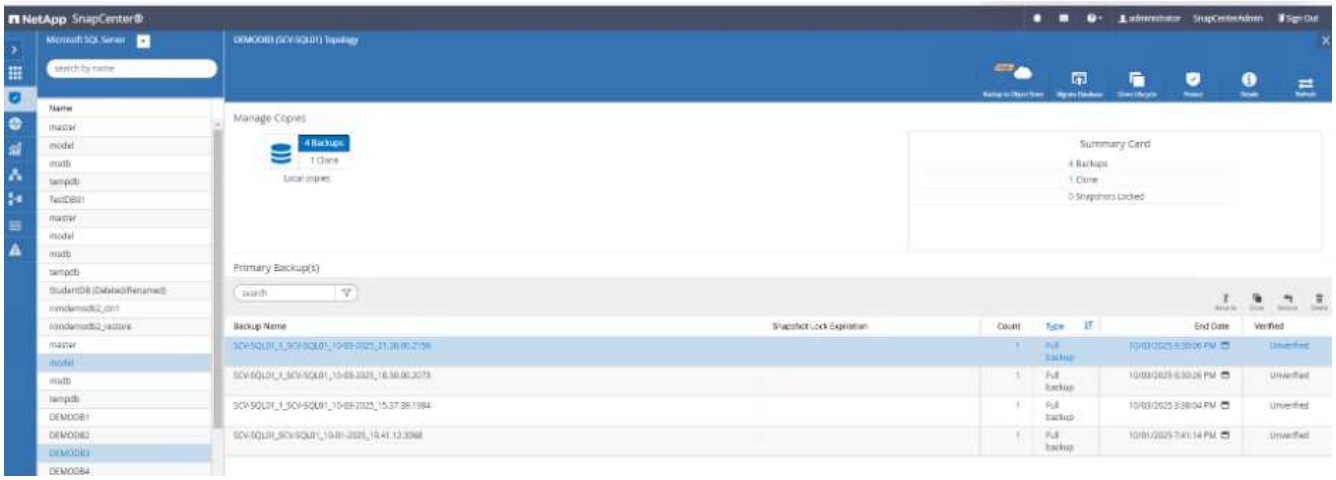
以下では、最初のスクリーンショットに表示されていたデータベースのいくつかのテーブルが、2番目のスクリーンショットでは削除されていることがわかります：


Object Explorer
Connect
SCV-SQL01 (SQL Server 16.0.1000.6 - SCV-SQL01\Admini
Databases
System Databases
Database Snapshots
DBdemoscv01
DBdemoscv01_clone
DEMODB1
DEMODB2
DEMODB3
Database Diagrams
Tables
System Tables
FileTables
External Tables
Graph Tables
dbo.Customers
dbo.OrderDetails
dbo.Orders
dbo.Products
dbo.Reviews
Dropped Ledger Tables
Views
External Resources
Synonyms
Programmability

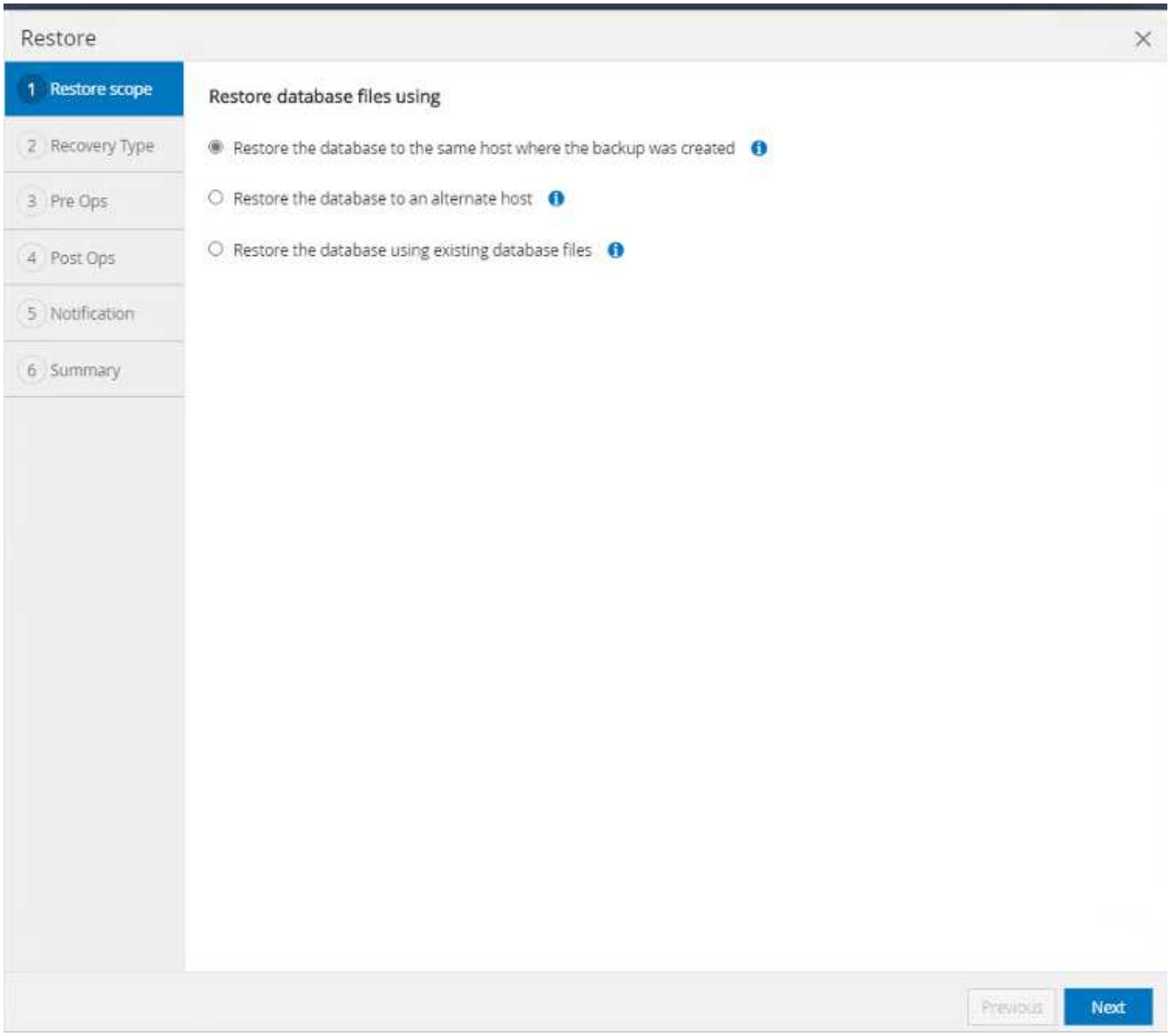


次の手順は、削除されたテーブルを回復するために復元を実行する方法を示しています：

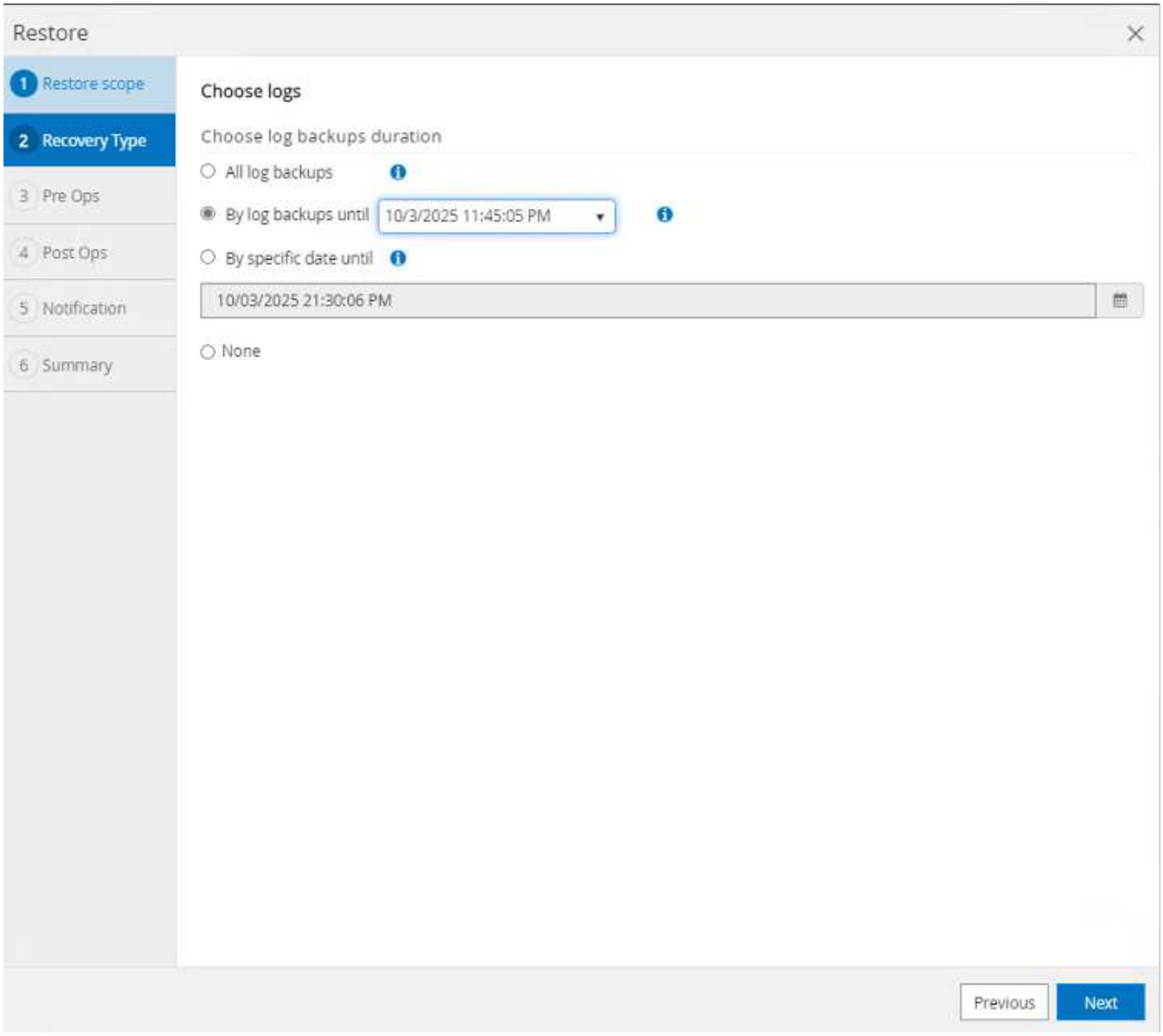
1. リソース グループからデータベースを選択します。



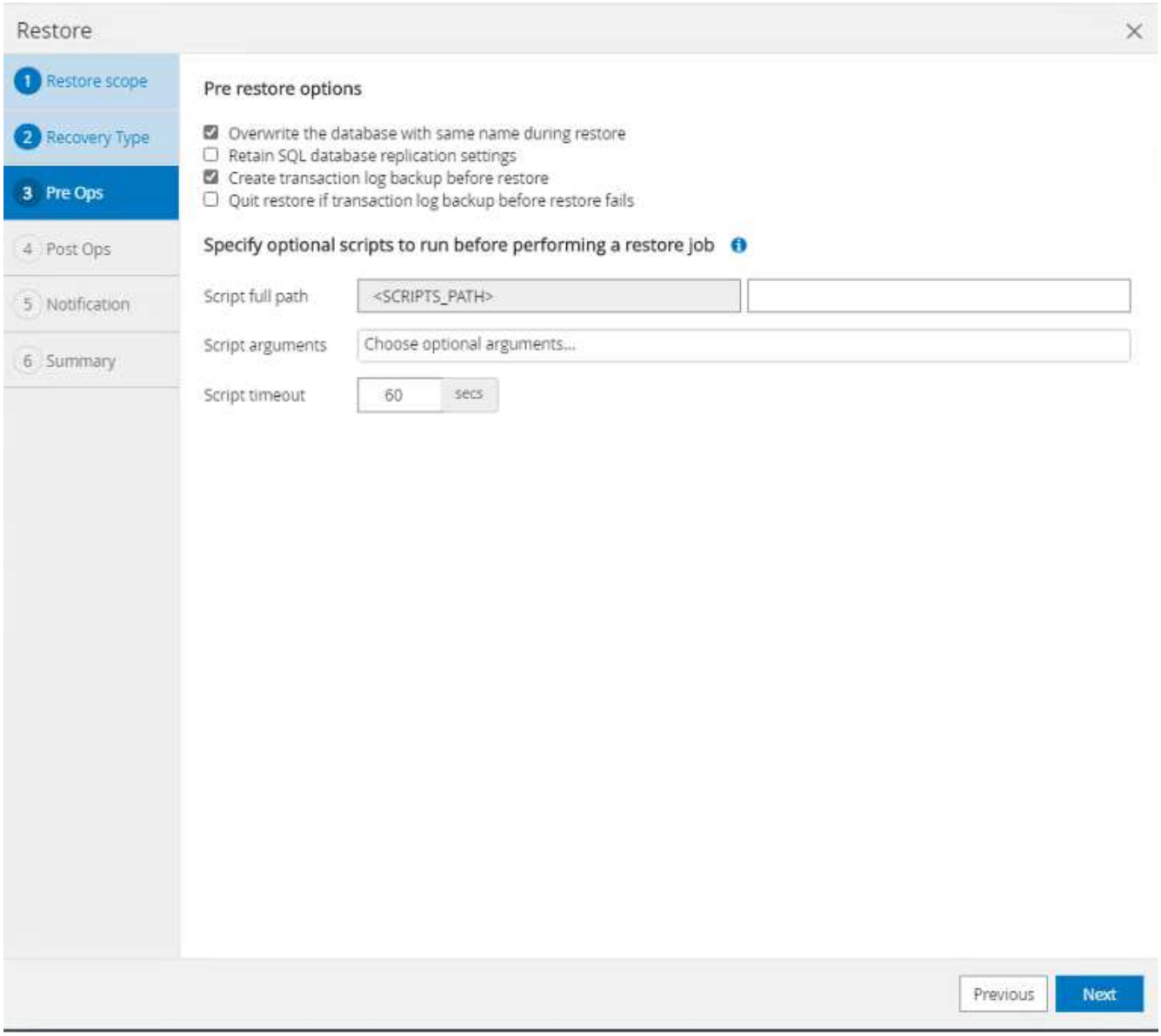
2. 「復元」ページで、「バックアップが作成されたのと同じホストにデータベースを復元する」オプションを選択します。



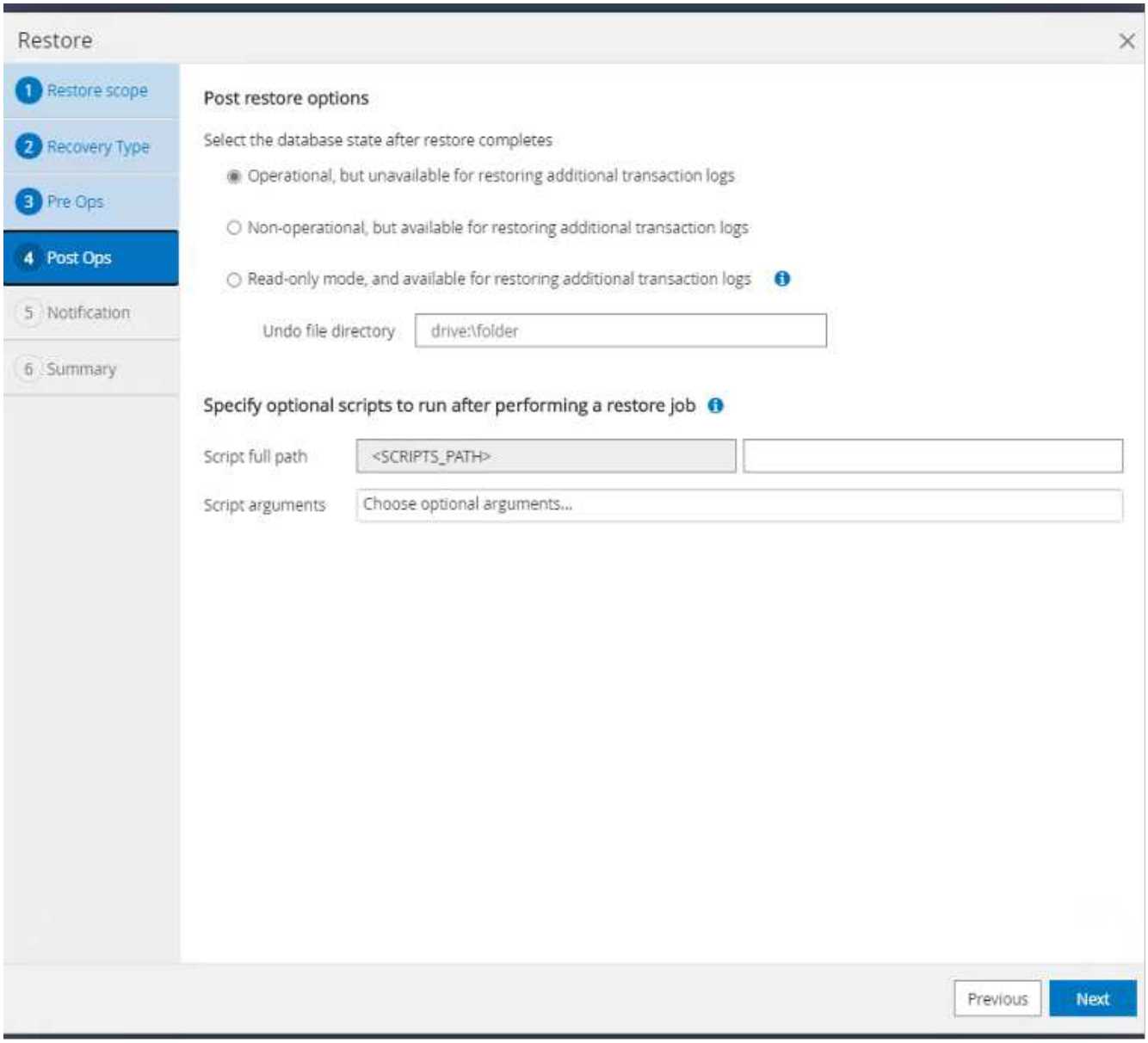
3. 特定の時点までのログ バックアップを使用するオプションを選択します。



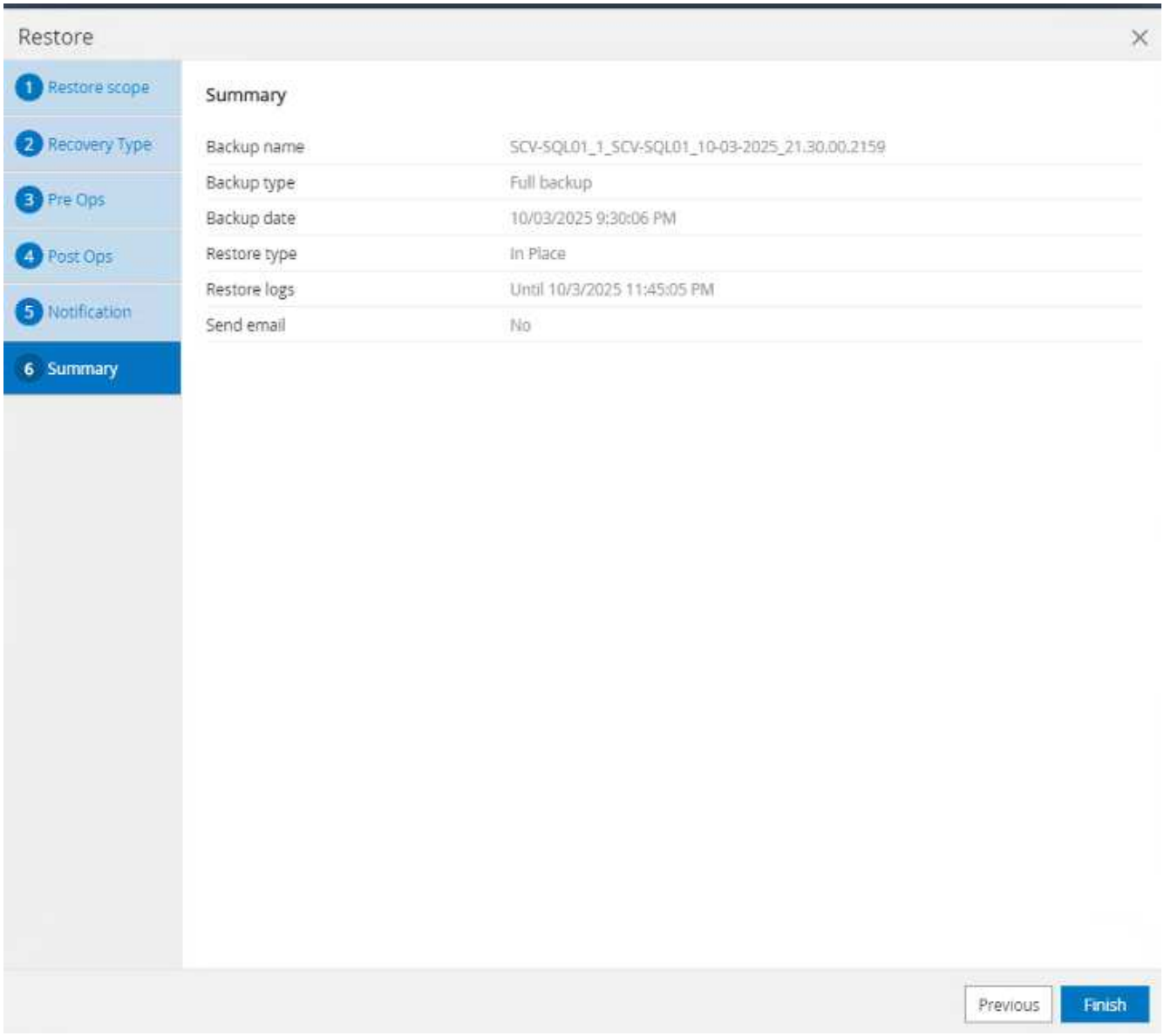
4. 「復元中に同じ名前のデータベースを上書きし、復元前にトランザクション ログのバックアップを作成する」を選択し、「次へ」を選択します。



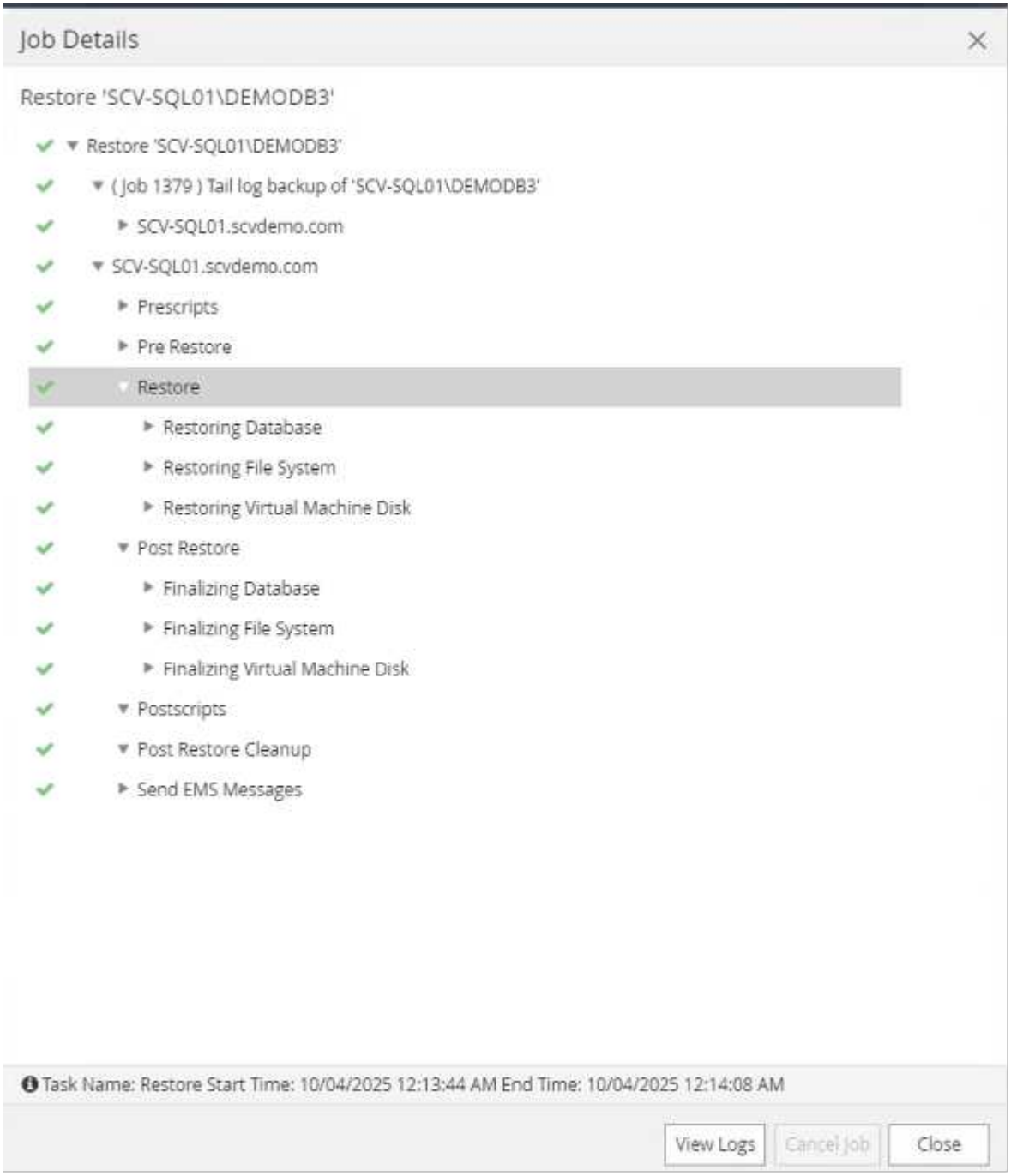
5. リスト オプションからデータベースが想定する復元後の状態を選択し、「次へ」を選択します。



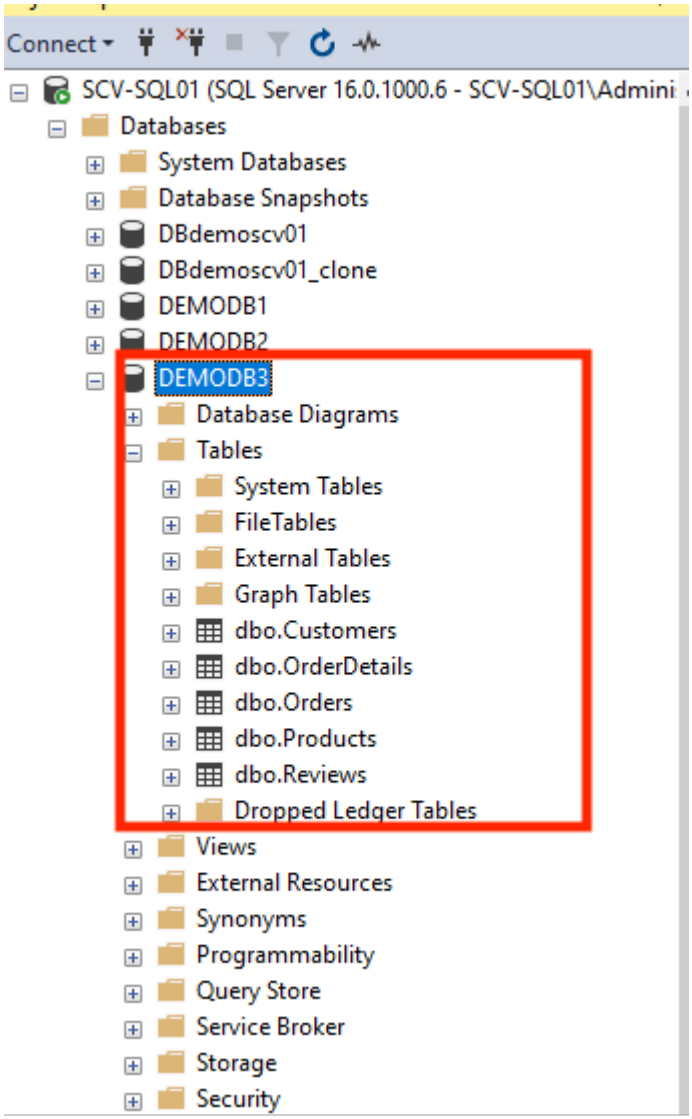
6. 概要ページで、「完了」を選択します。



7. ジョブが完了するまで監視します。



8. 削除されたテーブルが正常に復元されたことを確認します。



まとめ

このドキュメントでは、Amazon EVS クラスタの補助データストアとして FSx for ONTAP を使用しながら、SCV と"SnapCenter Plug-in for SQL Server（SCSQL）"を導入、設定、使用するための詳細な手順を説明します。

まとめ

まとめると、FSx for ONTAPを使用してAmazon EVS展開のTCOを最適化する場合、SCVはVMをバックアップするためのシンプルで効率的な方法を提供します。Snapshotコピーを利用するため、VMをシームレスかつ迅速にバックアップおよび復元でき、完了までに文字通り数秒しかかかりません。

"SnapCenter Plug-in for VMware vSphereを今すぐ無料でお試しください"。

Azure / AVS 向けNetApp

Azure AVS 向けNetApp の機能

NetApp がAzure VMware Solution (AVS) にもたらす機能について詳しく説明します。ゲスト接続ストレージ デバイスまたは補助的な NFS データストアとしてのNetAppから、ワークフローの移行、クラウドへの拡張/バースト、バックアップ/リストア、ディザスター リカバリーまで、さまざまな機能について説明します。

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。

- "Azure での AVS の構成"
- "AVS 向けNetAppストレージ オプション"
- "NetApp / VMware クラウド ソリューション"

Azure での AVS の構成

オンプレミスの場合と同様に、VM の作成と移行のための本番環境を正常に構築するには、クラウド ベースの仮想化環境を計画することが重要です。

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

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

セットアッププロセスは次の手順に分けられます。

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

詳細を表示"AVSの設定手順"。

AVS 向けNetAppストレージ オプション

NetAppストレージは、Azure AVS 内で、仮想接続として、または補助的な NFS データストアとして、さまざまな方法で利用できます。

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

Azure は、次の構成のNetAppストレージをサポートしています。

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

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

ソリューションのユースケース

NetAppおよび VMware クラウド ソリューションを使用すると、多くのユース ケースを Azure AVS に簡単に展開できます。VMware が定義したクラウド領域ごとに、次のようなユース ケースが定義されています。

- 保護（災害復旧とバックアップ/復元の両方を含む）
- 拡張
- 移行

"Azure AVS 向けNetAppソリューションを参照する"

Azure / AVS 上のワークロードを保護する

ANFと**JetStream**による災害復旧

クラウドへの災害復旧は、サイトの停止やデータ破損イベント (ランサムウェアなど) からワークロードを保護する、回復力がありコスト効率に優れた方法です。 VMware VAIO フレームワークを使用すると、オンプレミスの VMware ワークロードを Azure Blob ストレージに複製して回復できるため、データ損失を最小限に抑えるか、ほぼゼロにすることができ、RTO はほぼゼロになります。

JetStream DR を使用すると、オンプレミスから AVS、具体的にはAzure NetApp Filesに複製されたワークロードをシームレスに回復できます。 DR サイトでの最小限のリソースとコスト効率の高いクラウド ストレージを使用することで、コスト効率の高い災害復旧が可能になります。 JetStream DR は、Azure Blob Storage を介して ANF データストアへのリカバリを自動化します。 JetStream DR は、ネットワーク マッピングに従って、独立した VM または関連する VM のグループをリカバリ サイト インフラストラクチャに復元し、ランサムウェア保護のためのポイントインタイム リカバリを提供します。

このドキュメントでは、JetStream DR の動作原理と主なコンポーネントについて説明します。

▼ ソリューション展開の概要

1. オンプレミスのデータ センターに JetStream DR ソフトウェアをインストールします。
    a. Azure Marketplace (ZIP) から JetStream DR ソフトウェア バンドルをダウンロードし、指定されたクラスターに JetStream DR MSA (OVA) をデプロイします。
    b. I/O フィルター パッケージを使用してクラスターを構成します (JetStream VIB をインストールします)。
    c. DR AVS クラスターと同じリージョンに Azure Blob (Azure ストレージ アカウント) をプロビジョニングします。
    d. DRVA アプライアンスを展開し、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 ストレージからの 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. Azure VMware Solution プライベート クラウドに JetStream DR ソフトウェアをインストールします。
    a. 実行コマンドを使用して、JetStream DR をインストールおよび構成します。

b. 同じ Azure Blob コンテナーを追加し、[ドメインのスキャン] オプションを使用してドメインを検出します。

c. 必要な DRVA アプライアンスを展開します。

d. 利用可能な 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 配置に ANF データストアを使用するように RocVA (回復 VA) を構成します。

f. 適切なフェイルオーバー オプションを選択し、RTO がほぼゼロのドメインまたは VM の継続的なリハイドレーションを開始します。

3. 災害発生時に、指定された AVS DR サイト内のAzure NetApp Filesデータストアへのフェールオーバーをトリガーします。

4. 保護されたサイトが回復された後、保護されたサイトへのフェイルバックを呼び出します。開始する前に、この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 が提供する帯域幅テスト ツール (BWT) を実行して、JetStream DR ソフトウェアと併用した場合の Azure Blob ストレージの潜在的なパフォーマンスとレプリケーション帯域幅を評価します。接続などの前提条件が整ったら、JetStream DR for AVSをセットアップしてサブスクライブします。 "Azureマーケットプレイス" 。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 (たとえば、100 台以上) の保護を計画して開始する場合は、JetStream DR Automation Toolkit の容量計画ツール (CPT) を使用します。保護する VM のリストと、その RTO およびリカバリ グループの設定を指定して、CPT を実行します。

CPT は次の機能を実行します。

- RTO に応じて VM を保護ドメインに結合します。
- DRVA の最適な数とそのリソースを定義します。
- 必要なレプリケーション帯域幅を見積もります。
- 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) を識別します。
- 必要なオブジェクト ストレージ容量の見積もりなど。

規定される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 などのさまざまな VM 特性によって異なります。

オンプレミスデータセンターに **JetStream DR** をインストールする

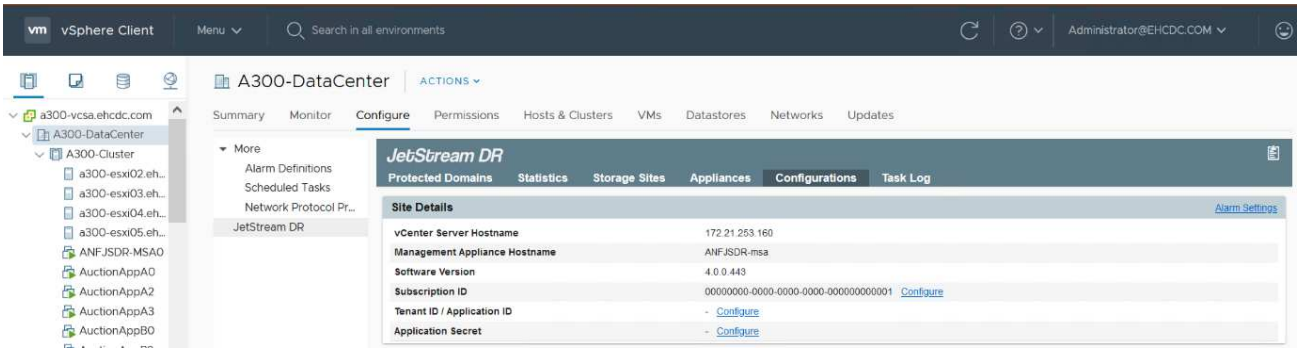
JetStream DR ソフトウェアは、JetStream DR 管理サーバー仮想アプライアンス (MSA)、DR 仮想アプライアンス (DRVA)、およびホスト コンポーネント (I/O フィルター パッケージ) の 3 つの主要コンポーネントで構成されています。 MSA は、コンピューティング クラスターにホスト コンポーネントをインストールして構成し、JetStream DR ソフトウェアを管理するために使用されます。次のリストは、インストール プロセスの概要を示しています。

▼ オンプレミス向け**JetStream DR**のインストール方法

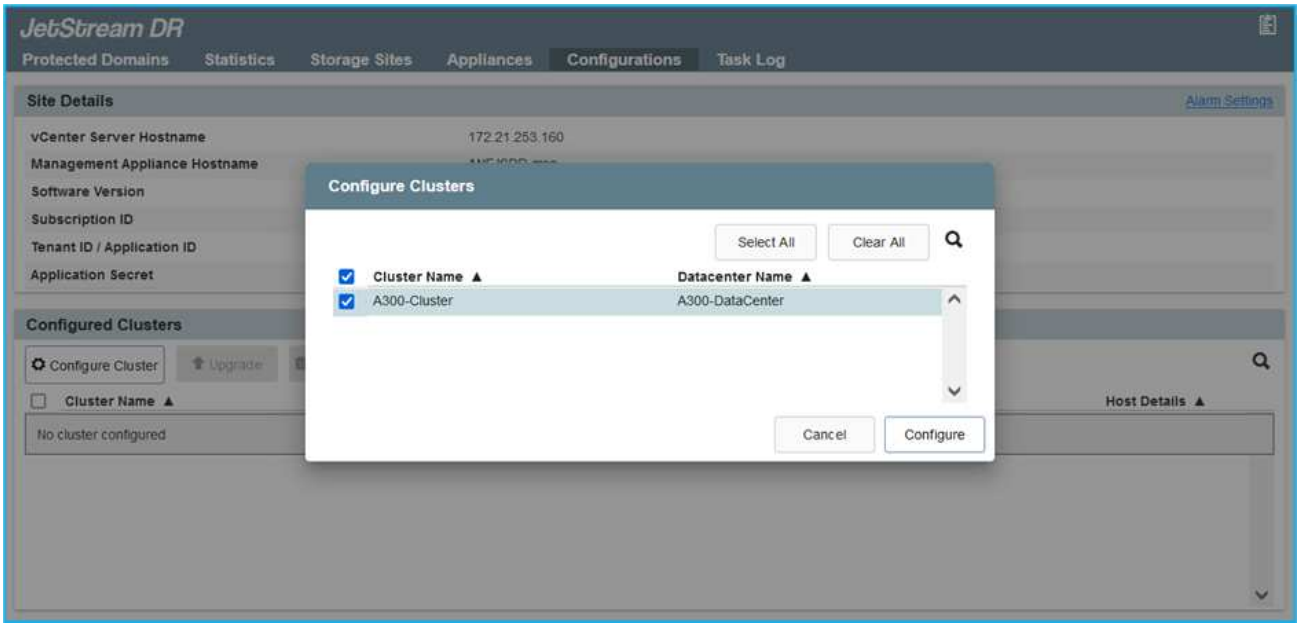
1. 前提条件を確認してください。

2. リソースと構成の推奨事項を取得するには、容量計画ツールを実行します (オプションですが、概念実証のトライアルには推奨されます)。

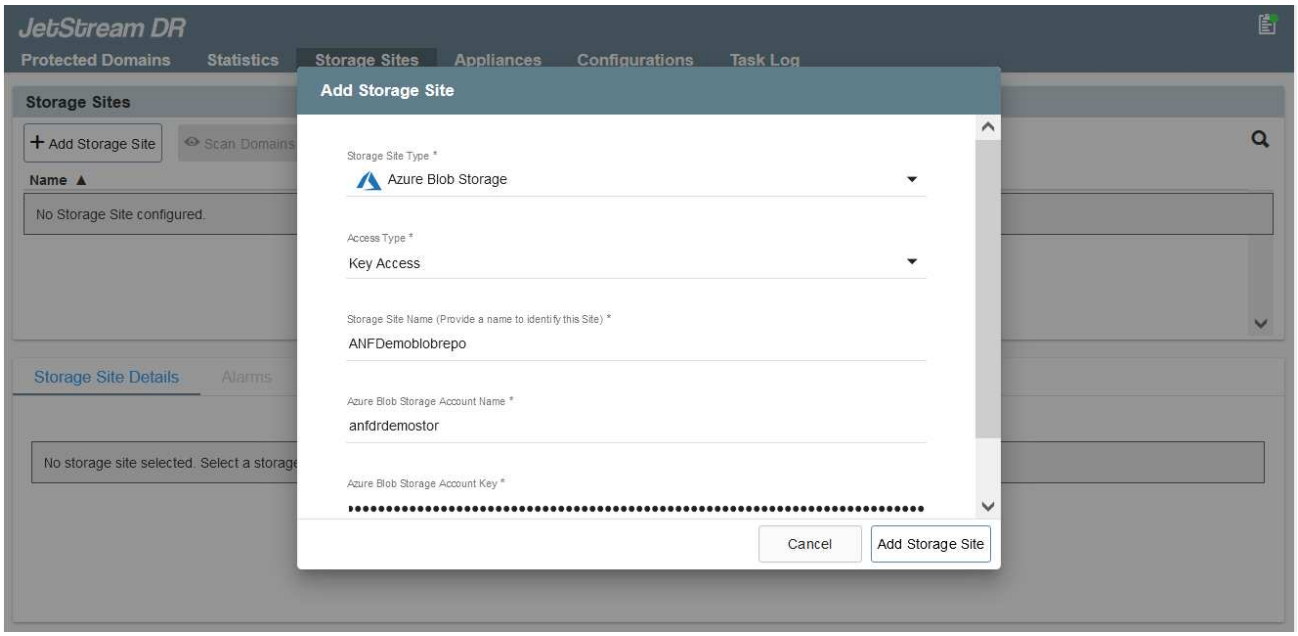
3. 指定されたクラスタ内の vSphere ホストに JetStream DR MSA をデプロイします。
4. ブラウザで DNS 名を使用して MSA を起動します。
5. vCenter サーバーを MSA に登録します。インストールを実行するには、次の詳細な手順を実行します。
6. JetStream DR MSA がデプロイされ、vCenter Server が登録されたら、vSphere Web Client を使用して JetStream DR プラグインにアクセスします。これは、[データセンター] > [構成] > [JetStream DR] に移動することで実行できます。



7. JetStream DR インターフェースから適切なクラスターを選択します。



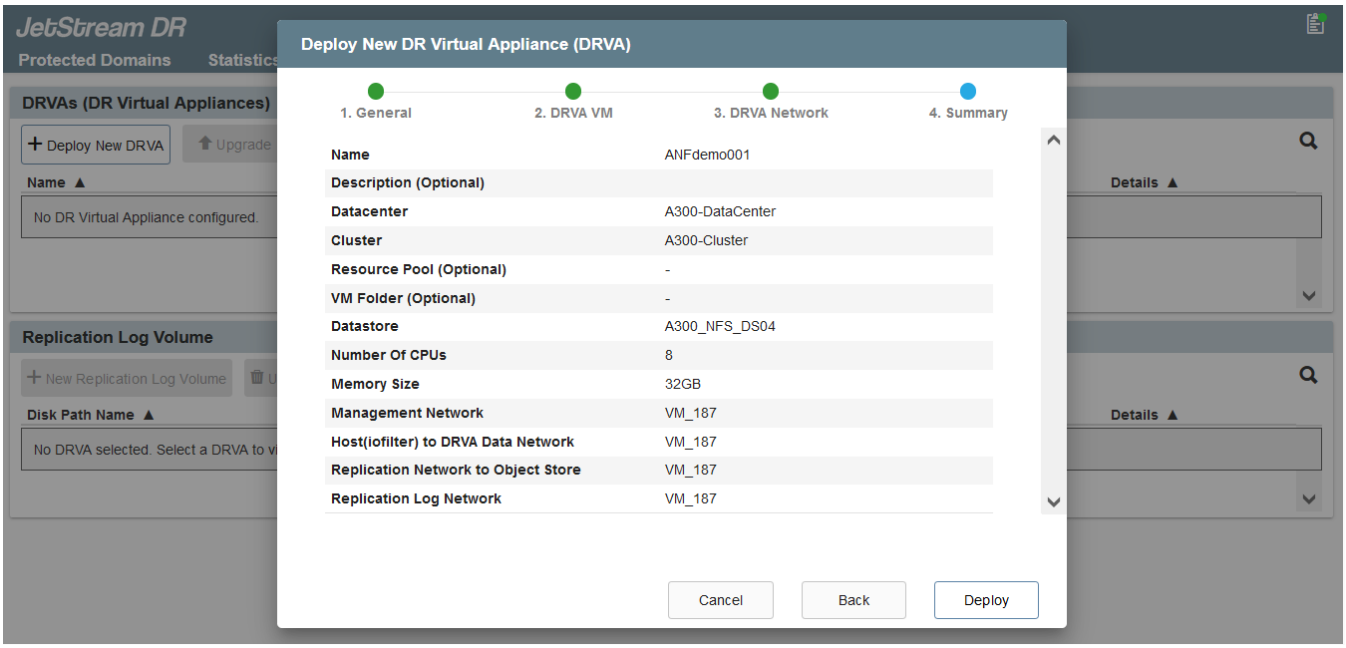
8. I/O フィルター パッケージを使用してクラスターを構成します。



9. リカバリ サイトにある 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) をデプロイします。

> DRVA 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 サイクルを手動で構成して実行することをお勧めします (保護の開始 > フェールオーバー > フェールバック)。

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ーには少なくとも 1 つの DRVA が含まれている必要があり、通常はホストごとに 1 つの DRVA が構成されます。各 DRVA は複数の保護されたドメインを管理できます。

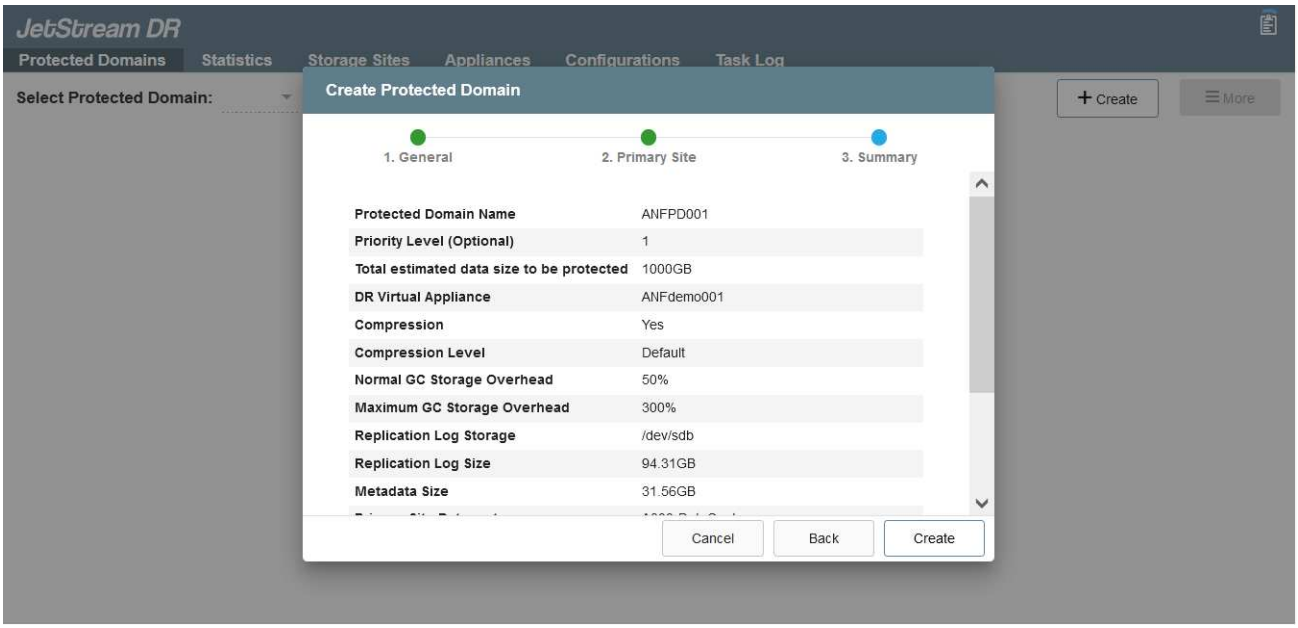


この例では、80 台の仮想マシンに対して 4 つの DRVA が作成されました。

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。

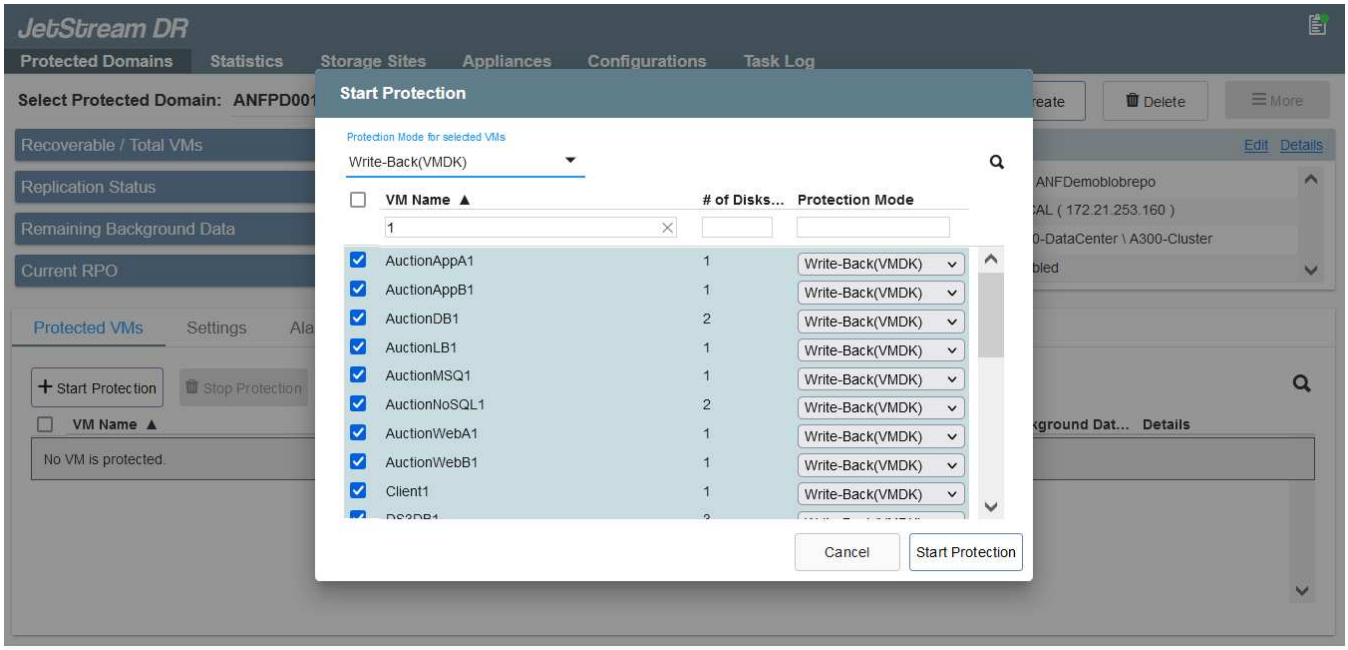
2. [保護されたドメイン] タブで、Azure Blob Storage サイト、DRVA インスタンス、レプリケーション ログに関する情報を使用して、必要な数の保護されたドメインを作成します。保護されたドメインは、一緒に保護され、フェイルオーバー/フェイルバック操作の優先順位が割り当てられている、クラスター内の特定の VM または VM セットを定義します。



3. 保護する VM を選択し、保護されたドメインの VM 保護を開始します。これにより、指定された BLOB ストアへのデータのレプリケーションが開始されます。

保護された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) モードでは、より高いパフォーマンスを提供できます。



レプリケーション ログ ボリュームが高パフォーマンス ストレージに配置されていることを確認します。

フェールオーバー実行ブックは、VM をグループ化 (リカバリ グループと呼ばれる) し、ブート順序シーケンスを設定し、CPU/メモリ設定と IP 構成を変更するように構成できます。

実行コマンドを使用して、**Azure VMware Solution** プライベート クラウドに **JetStream DR for AVS** をインストールする

リカバリ サイト (AVS) のベスト プラクティスは、3 ノードのパイロット ライト クラスターを事前に作成することです。これにより、次の項目を含むリカバリ サイトのインフラストラクチャを事前に構成できます。

- 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用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するなど、JetStream DR はミッションクリティカルなドメイン向けにほぼゼロの RTO モードをサポートします。これらのドメインでは、宛先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 が推奨されるストレージ 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 クラスター上で構成する必要があります。

SLA および RTO 要件に応じて、継続的なフェイルオーバーまたは通常の (標準) フェイルオーバー モードを使用できます。 RTO をほぼゼロにするには、リカバリサイトで継続的な再水和を開始する必要があります。

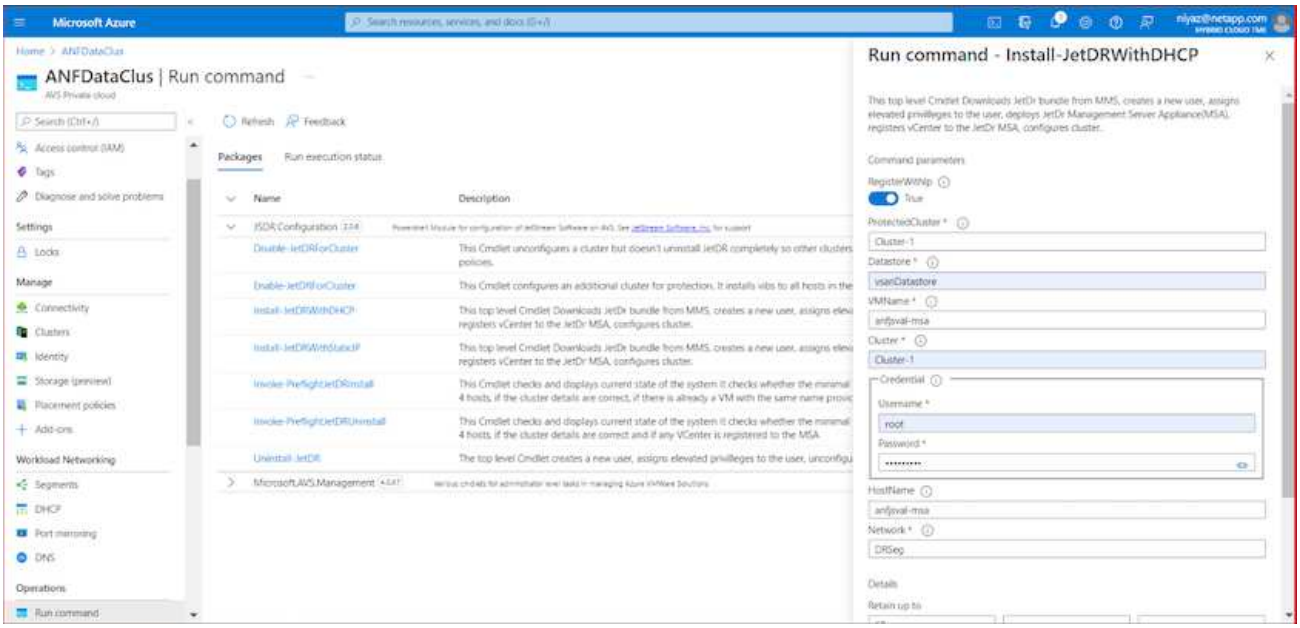
▼ プライベートクラウドに **JetStream DR for AVS** をインストールする方法

Azure VMware Solution 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。

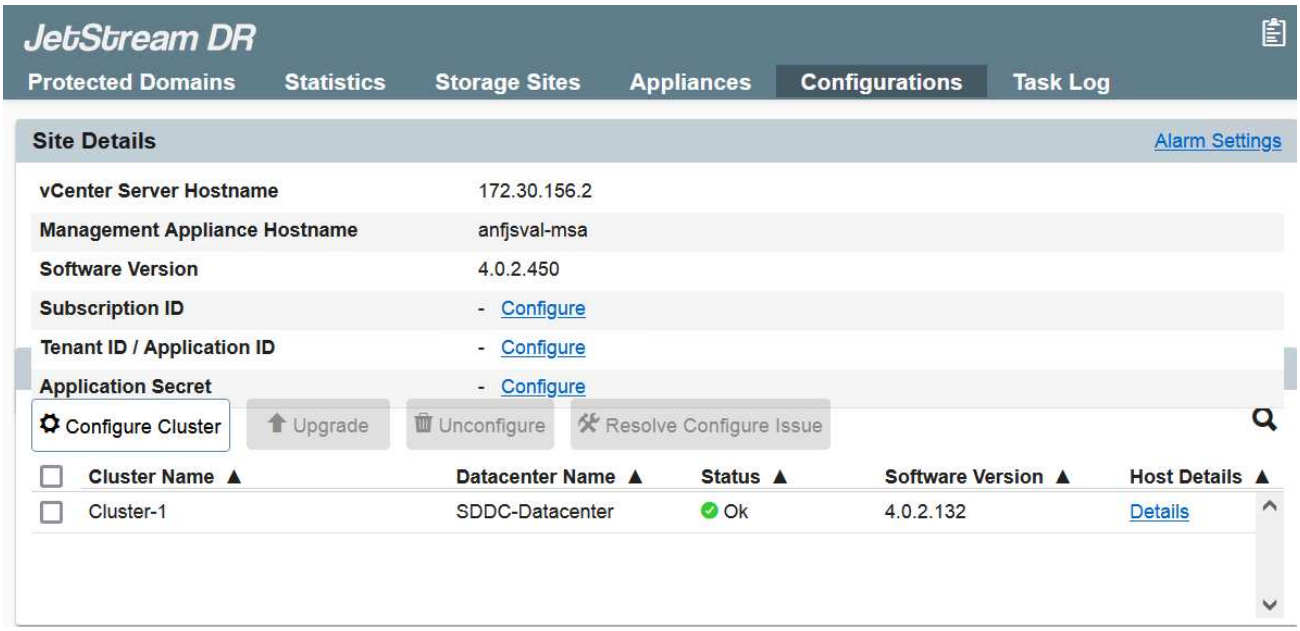
1. Azure ポータルから Azure VMware ソリューションに移動し、プライベート クラウドを選択して、[コマンドの実行] > [パッケージ] > [JSDR.Configuration] を選択します。

Azure VMware Solution のデフォルトの CloudAdmin ユーザーには、JetStream DR for AVS 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 Solution では、JetStream DR の Azure VMware Solution 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素化および自動化できます。

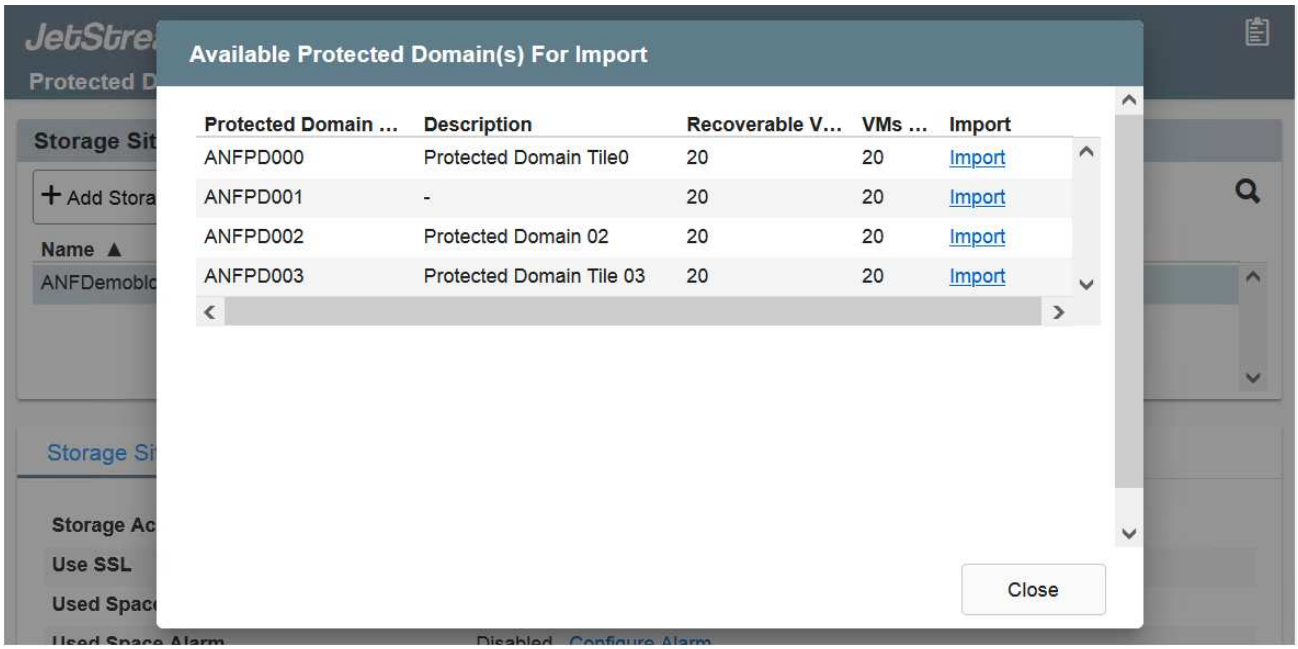
次のスクリーンショットは、DHCP ベースの IP アドレスを使用したインストールを示しています。



2. JetStream DR for AVS のインストールが完了したら、ブラウザを更新します。 JetStream DR UI にアクセスするには、[SDDC データセンター] > [構成] > [JetStream DR] に移動します。



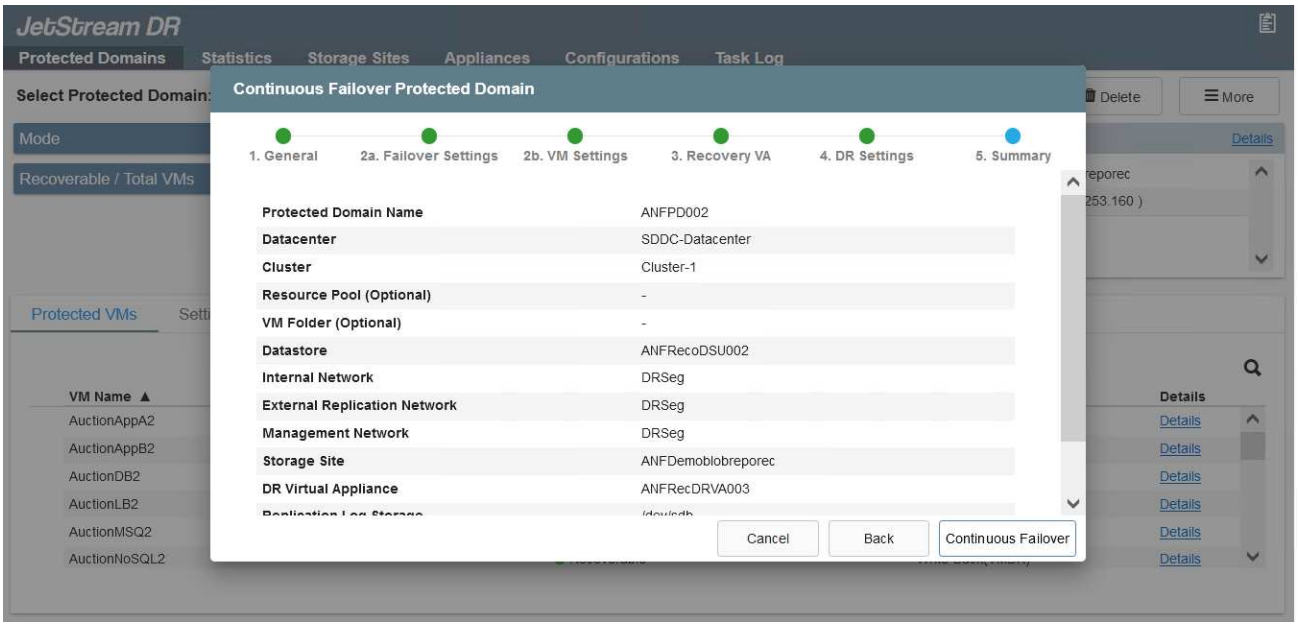
3. JetStream DR インターフェイスから、オンプレミス クラスターをストレージ サイトとして保護するために使用された Azure Blob Storage アカウントを追加し、スキャン ドメイン オプションを実行します。



4. 保護されたドメインをインポートした後、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ションを手動で開始します。

> これらの手順は、CPT が作成したプランを使用して自動化することもできます。

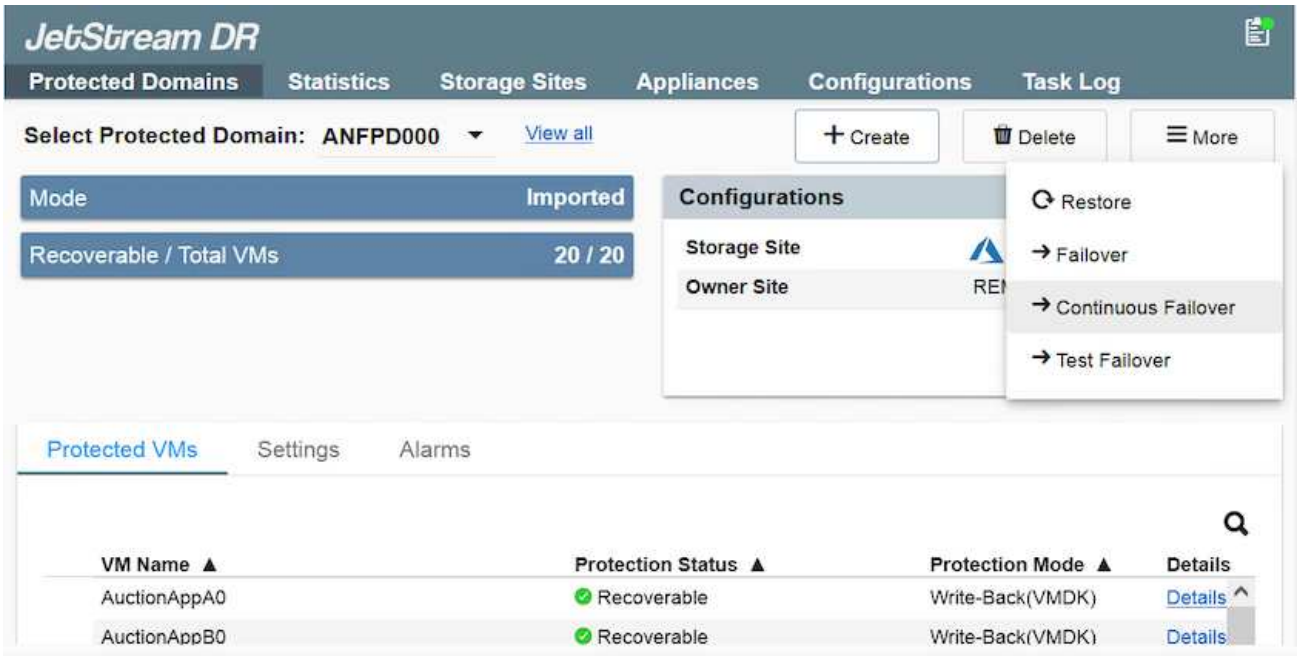
5. 利用可能な vSAN または ANF データストアを使用してレプリケーション ログ ボリュームを作成します。
6. 保護されたドメインをインポートし、VM の配置に ANF データストアを使用するように Recovery VA を構成します。



> 選択したセグメントで DHCP が有効になっており、十分な IP が利用可能であることを確認します。ドメインが回復している間、動的 IP が一時的に使用されます。回復中の各 VM (継続的なリハイドレーションを含む) には個別の動的 IP が必要です。回復が完了す

ると、IP は解放され、再利用できるようになります。

7. 適切なフェイルオーバー オプション (継続的な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、継続的なリハイドレーション (継続的なフェイルオーバー) が選択されています。



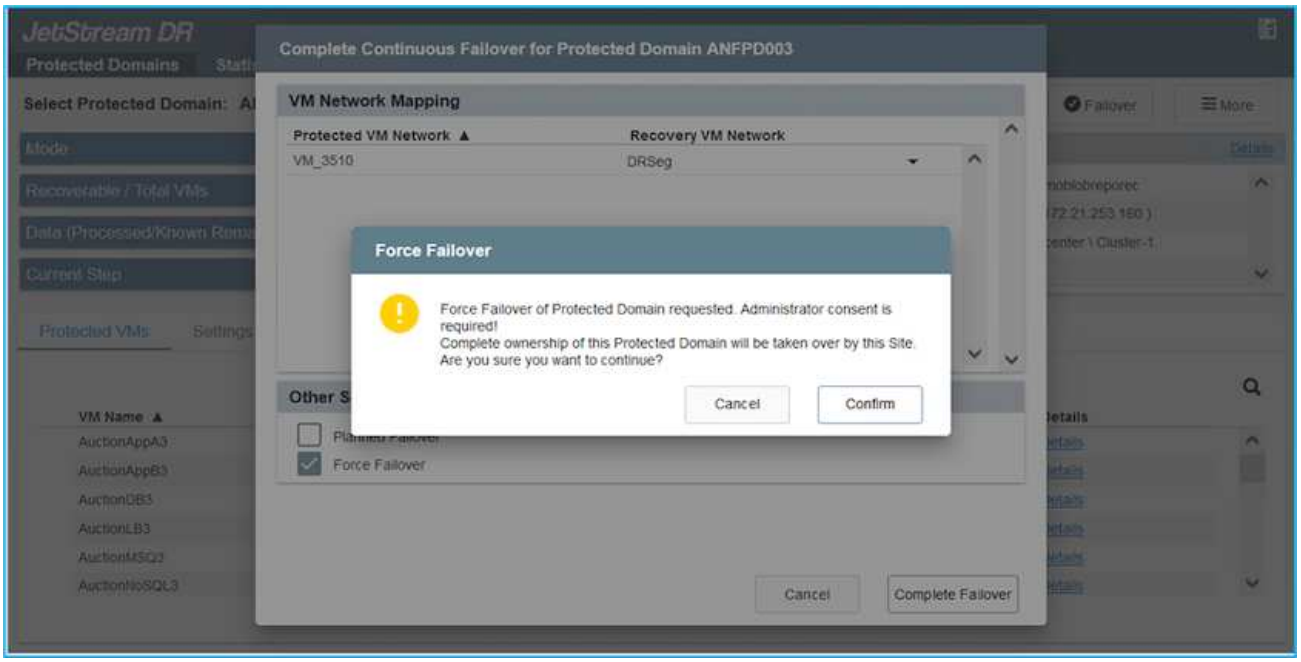
フェイルオーバー/フェイルバックの実行

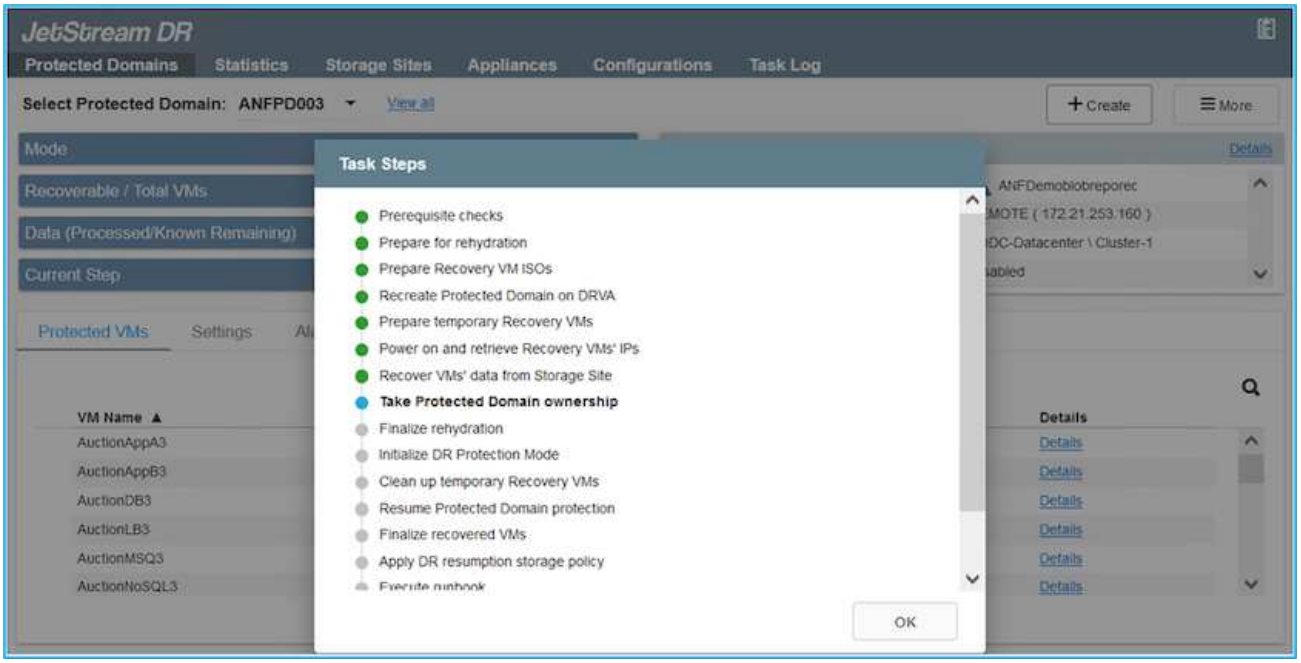
▼ フェイルオーバー/フェイルバックを実行する方法

1. オンプレミス環境の保護されたクラスターで災害 (部分的または完全な障害) が発生した後、フェイルオーバーをトリガーします。

CPT を使用すると、フェールオーバー プランを実行して、Azure Blob Storage から AVS クラスター回復サイトに VM を回復できます。

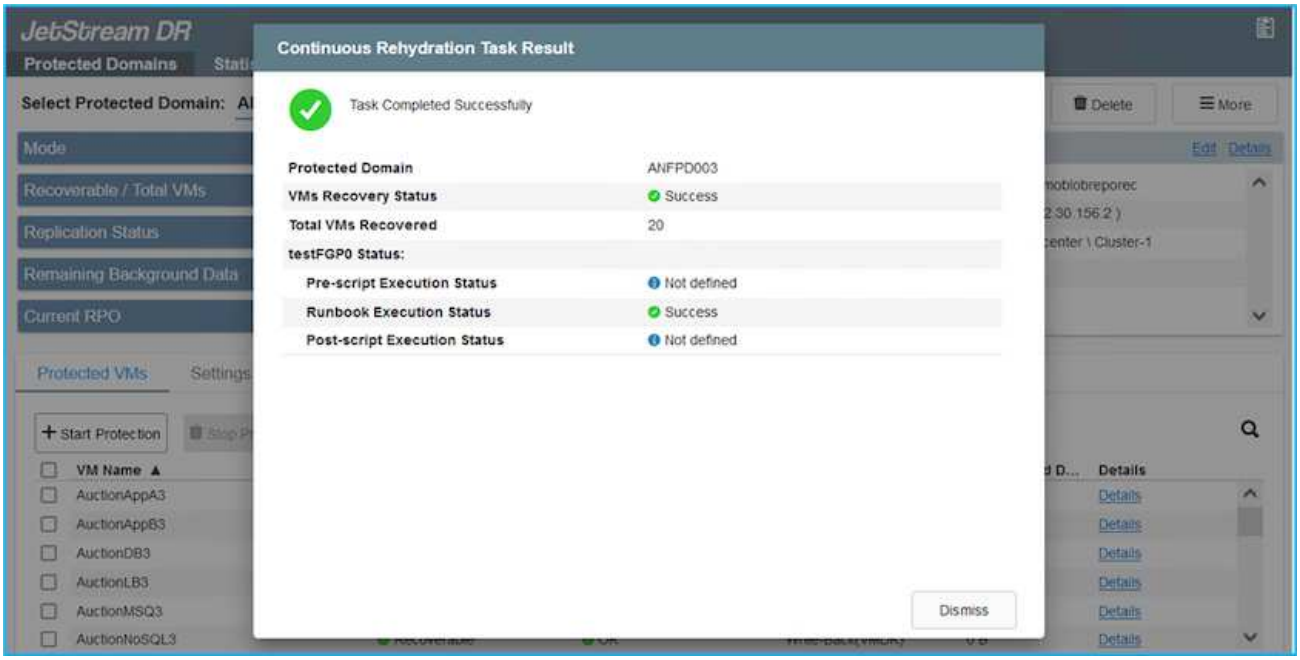
フェールオーバー後 (継続的または標準のリハイドレーション)、保護された VM が AVS で起動されると、保護は自動的に再開され、JetStream DR は引き続きデータを Azure Blob Storage 内の適切な元のコンテナーに複製します。





タスク バーには、フェールオーバー アクティビティの進行状況が表示されます。

2. タスクが完了したら、回復した VM にアクセスし、業務を通常どおり継続します。

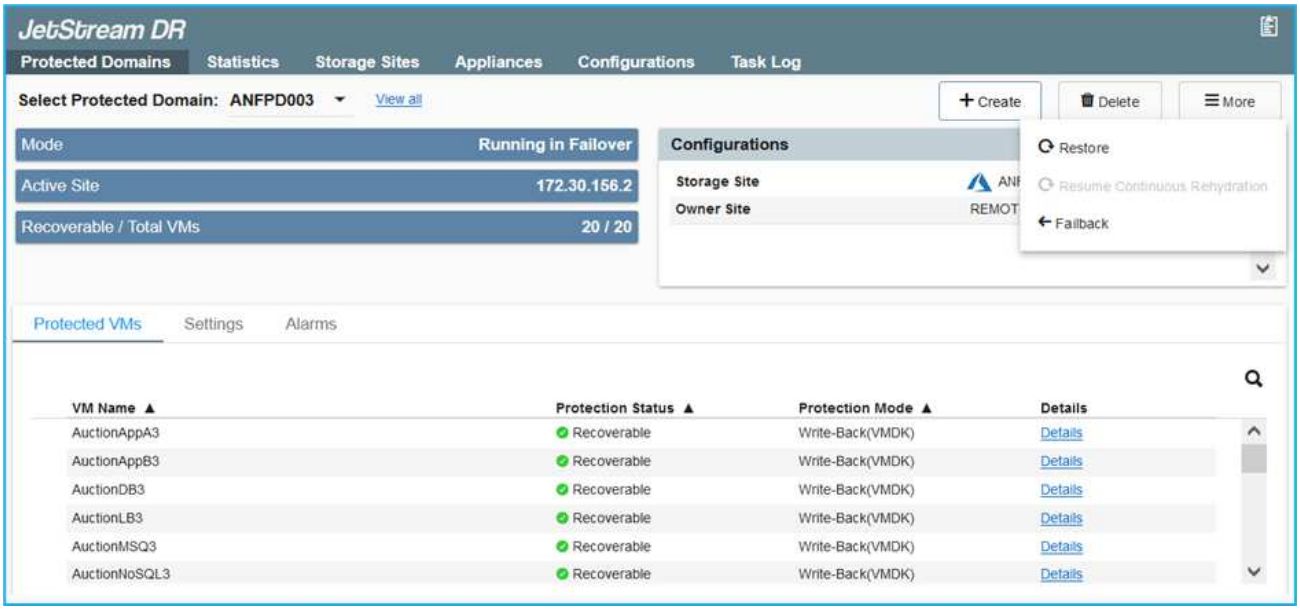


プライマリ サイトが再び稼働したら、フェイルバックを実行できます。 VM 保護が再開され、データの一貫性がチェックされる必要があります。

3. オンプレミス環境を復元します。災害インシデントの種類によっては、保護されたクラスターの構成を復元および/または検証する必要がある場合があります。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: `recovery_utility_prepare_failback` Automation Toolkit で提供されるスクリプトを使用すると、元の保護されたサイトから古い VM、ドメイン情報などを削除できます。

4. 復元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、適切な保護されたドメインを選択します。保護されたサイトのフェイルバックの準備ができたら、UI でフェイルバック 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 プランは、VM とそのデータをオブジェクト ストアから元の VMware 環境に戻す作業を開始するためにも使用できます。

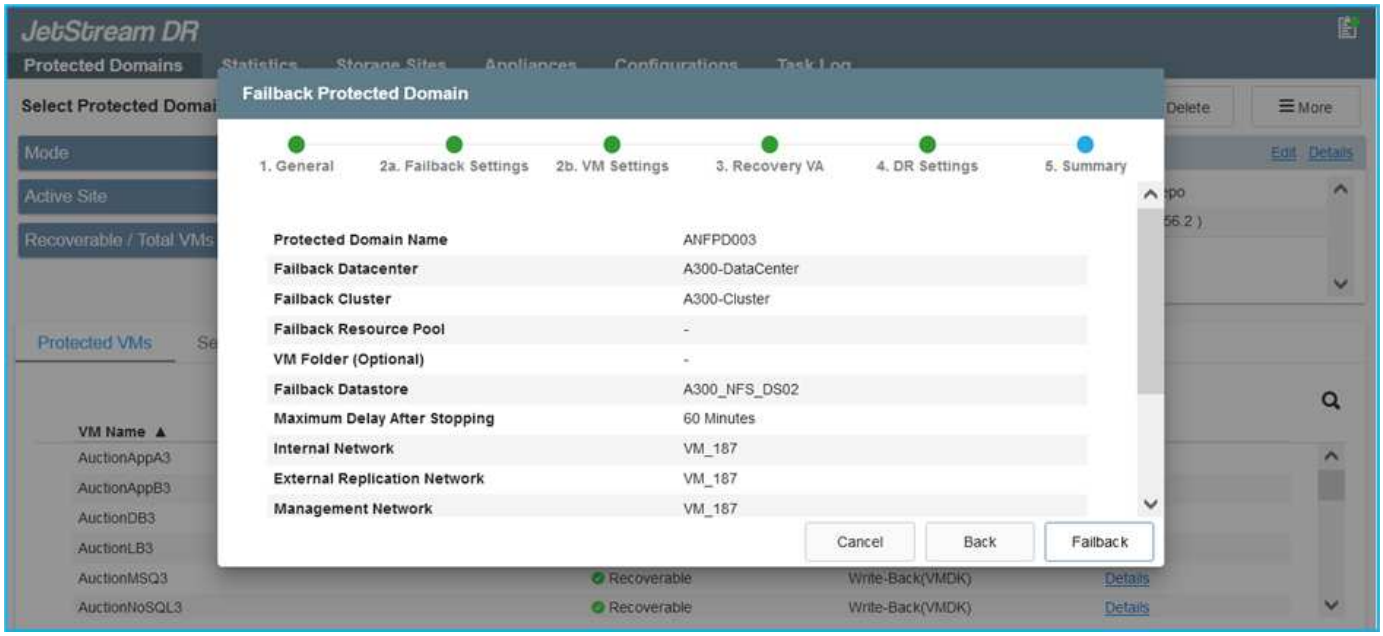
リカバリ サイトで VM を一時停止し、保護サイトで再起動した後の最大遅延を指定します。この時間には、フェールオーバー VM を停止した後のレプリケーションの完了、リカバリ サイトのクリーンアップにかかる時間、保護されたサイトで VM を再作成する時間が含まれます。 NetApp の推奨値は 10 分です。

フェイルバック プロセスを完了し、VM 保護とデータの整合性の再開を確認します。

ランサムウェアの回復

ランサムウェアからの回復は困難な作業になる可能性があります。具体的には、IT 組織にとって、安全な復帰ポイントを決定すること、また、決定した後で、回復したワークロードが再発する攻撃（休眠中のマルウェアや脆弱なアプリケーションによる攻撃）から確実に保護されるようにする方法を決定することが困難になることがあります。

JetStream DR for AVS をAzure NetApp Filesデータストアと組み合わせると、組織が利用可能な時点から回復できるようにすることでこれらの懸念に対処でき、必要に応じてワークロードを機能する分離されたネットワークに回復できます。リカバリにより、アプリケーションは North-South トラフィックに公開されることなく機能し、相互に通信できるようになるため、セキュリティ チームはフォレンジックやその他の必要な修復を安全に実行できるようになります。



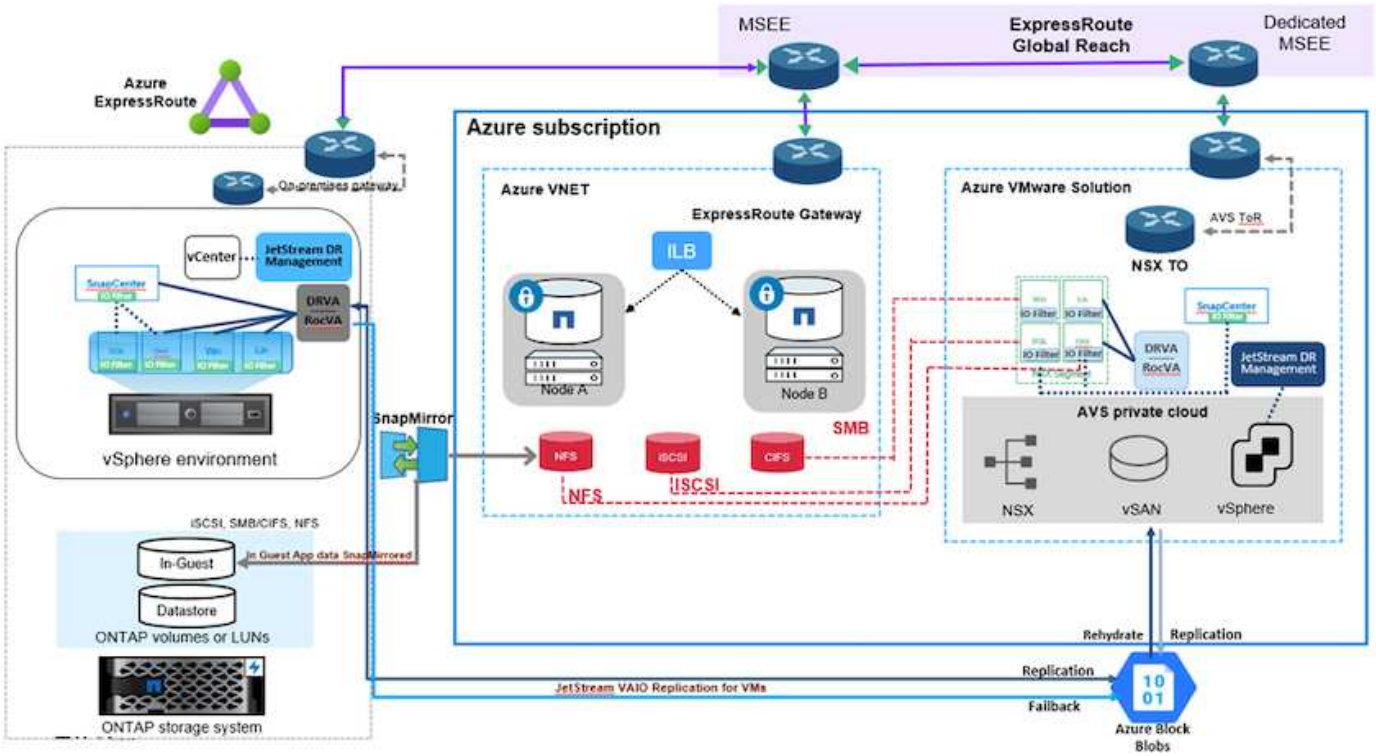
CVO と **AVS (**ゲスト接続ストレージ**)** による災害復旧

クラウドへの災害復旧は、サイトの停止やランサムウェアなどのデータ破損イベントからワークロードを保護する、回復力がありコスト効率に優れた方法です。 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 で実行されているNetApp Cloud Volumes ONTAPに複製できます。

概要

```
 This covers application data; however, what about the actual VMs
themselves. Disaster recovery should cover all dependent components,
including virtual machines, VMDKs, application data, and more. To
accomplish this, SnapMirror along with Jetstream can be used to seamlessly
recover workloads replicated from on-premises to Cloud Volumes ONTAP while
using vSAN storage for VM VMDKs.
```

このドキュメントでは、 NetApp SnapMirror、JetStream、Azure VMware Solution (AVS) を使用した災害復旧の設定と実行の手順について説明します。



前提

このドキュメントでは、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) に焦点を当てており、オンプレミス環境でアプリケーション整合性のあるバックアップにSnapCenterを使用していることを前提としています。

> このドキュメントは、サードパーティのバックアップまたはリカバリ ソリューションに適用されます。環境で使用されているソリューションに応じて、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 ポリシーを作成します。

オンプレミス環境と Azure 仮想ネットワーク間の接続には、Express Route Global Reach または VPN ゲートウェイを使用した仮想 WAN を使用します。セグメントは、オンプレミスの vLAN 設計に基づいて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 に接続するには複数のオプションがあるため、このド

キュメントでは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 Azure への適切な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ソリューションの導入

ソリューション展開の概要

1. 必要な RPO 要件に従って、 SnapCenterを使用し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ます。
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、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. 関連するアプリケーション ボリュームに対してSnapMirrorを構成します。
   b. スケジュールされたジョブの後にSnapMirror の更新をトリガーするように、 SnapCenterのバックアップ ポリシーを更新します。
3. オンプレミスのデータセンターに JetStream DR ソフトウェアをインストールし、仮想マシンの保護を開始します。
4. Azure VMware Solution プライベート クラウドに JetStream DR ソフトウェアをインストールします。
5. 災害発生時には、Cloud Manager を使用してSnapMirror関係を解除し、指定された AVS DR サイト内の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 と NFS マウントを再接続します。
6. プライマリ サイトが回復された後、 SnapMirror を逆再同期して、保護されたサイトへのフェイルバックを呼び出します。

導入環境の詳細

▼ **Azure** で **CVO** を構成し、ボリュームを **CVO** に複製する

最初のステップは、Azure でCloud Volumes ONTAP を構成することです (["リンク"] ）を作成し、必要な頻度とスナップショット保持期間で、必要なボリュームをCloud Volumes ONTAPに複製します。

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	17 seconds	idle	snapmirrored	May 6, 2022, 11:43:18 AM 105.06 KiB
✓	gcsdrsqlhld_sc46_copy ANFCVODRDemo	gcsdrsqlhld_sc46 ntaphci-a300e9u25	7 seconds	idle	snapmirrored	May 6, 2022, 11:42:20 AM 7.22 MiB
✓	gcsdrsqllog_sc46 ntaphci-a300e9u25	gcsdrsqllog_sc46_copy ANFCVODRDemo	16 seconds	idle	snapmirrored	May 6, 2022, 11:43:52 AM 130.69 KiB

▼ **AVS**ホストと**CVO**データアクセスを構成する

SDDC を展開する際に考慮すべき 2 つの重要な要素は、Azure VMware ソリューション内の SDDC クラスターのサイズと、SDDC をサービスに維持する期間です。災害復旧ソリューションに関するこれら 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、最小 3 台のホストから、本格的な展開のマルチホスト クラスターまで、さまざまな規模にすることができます。

AVS クラスターを展開するかどうかの決定は、主に RPO/RTO 要件に基づいて行われます。 Azure VMware ソリューションを使用すると、テストや実際の災害イベントに備えて SDDC をジャストインタイムでプロビジョニングできます。ジャストインタイムで導入された SDDC は、災害が発生していないとき

に ESXi ホストのコストを節約します。ただし、この形式の展開では、SDDC のプロビジョニング中に RTO が数時間影響を受けます。

最も一般的に導入されるオプションは、SDDC を常時オンのパイロットライト動作モードで実行することです。このオプションは、常に利用可能な 3 つのホストの小さなフットプリントを提供し、シミュレーション アクティビティとコンプライアンス チェックの実行ベースラインを提供することでリカバリ操作を高速化し、実稼働サイトと DR サイト間の運用上のずれのリスクを回避します。パイロットライト クラスターは、実際の DR イベントを処理するために必要になったときに、必要なレベルまで迅速に拡張できます。

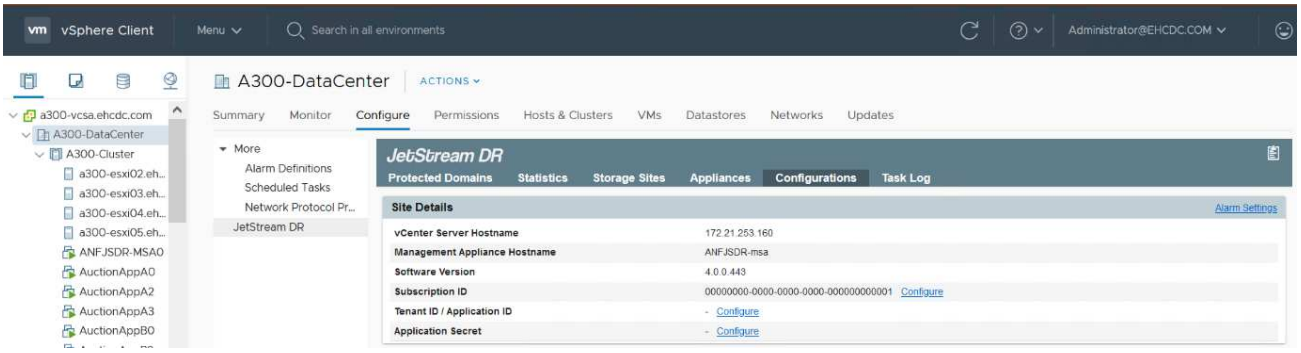
AVS SDDC（オンデマンドまたはパイロットライトモード）を構成するには、以下を参照してください。"Azure に仮想化環境を展開して構成する" 。前提条件として、接続が確立された後、AVS ホスト上にあるゲスト VM がCloud Volumes ONTAPからデータを使用できることを確認します。

Cloud Volumes ONTAPと AVS が適切に構成されたら、VAIO メカニズムを使用し、アプリケーション ボリュームのコピーにSnapMirrorを活用して、オンプレミスのワークロードの AVS (アプリケーション VMDK を持つ VM とゲスト内ストレージを持つ VM) へのリカバリを自動化するように Jetstream の構成を開始しCloud Volumes ONTAP。

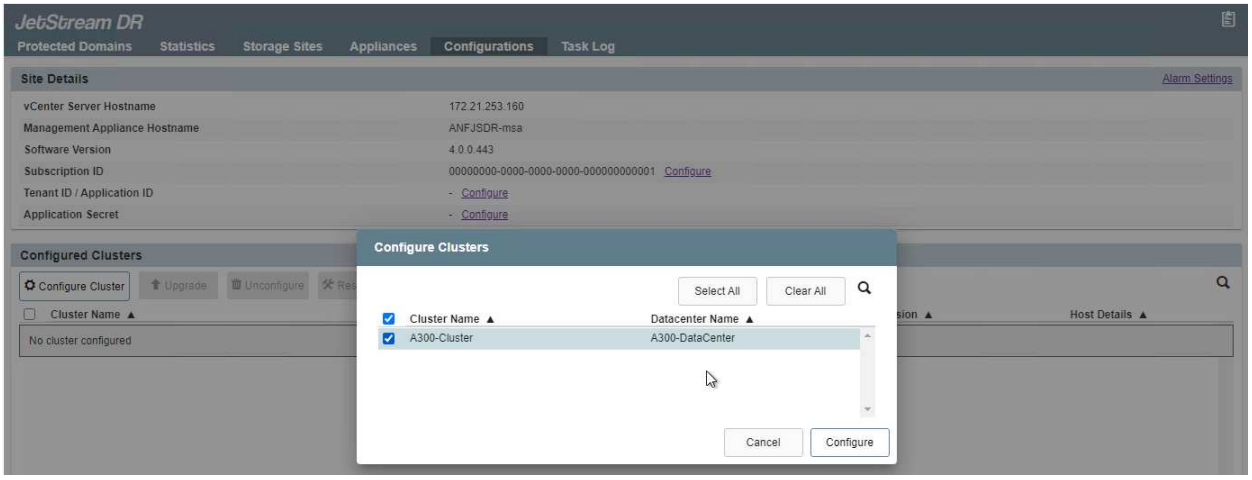
▼ オンプレミスデータセンターに **JetStream DR** をインストールする

JetStream DR ソフトウェアは、JetStream DR 管理サーバー仮想アプライアンス (MSA)、DR 仮想アプライアンス (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 クラスターにホスト 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。インストールプロセスは次のとおりです。

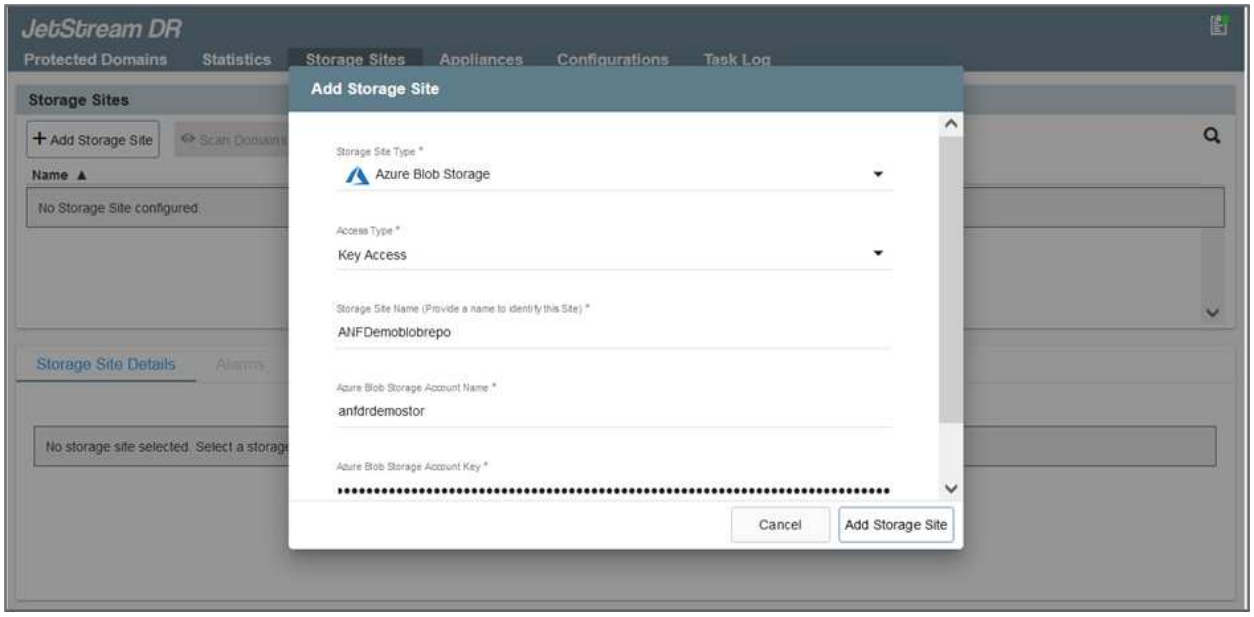
1. 前提条件を確認してください。
2. リソースと構成の推奨事項を取得するには、容量計画ツールを実行します。
3. 指定されたクラスタ内の各 vSphere ホストに JetStream DR MSA をデプロイします。
4. ブラウザで DNS 名を使用して MSA を起動します。
5. vCenter サーバーを MSA に登録します。
6. JetStream DR MSA がデプロイされ、vCenter Server が登録されたら、vSphere Web Client を使用して JetStream DR プラグインに移動します。これは、[データセンター] > [構成] > [JetStream DR] に移動することで実行できます。



7. JetStream DR インターフェースから、次のタスクを完了します。
   a. I/O フィルター パッケージを使用してクラスターを構成します。



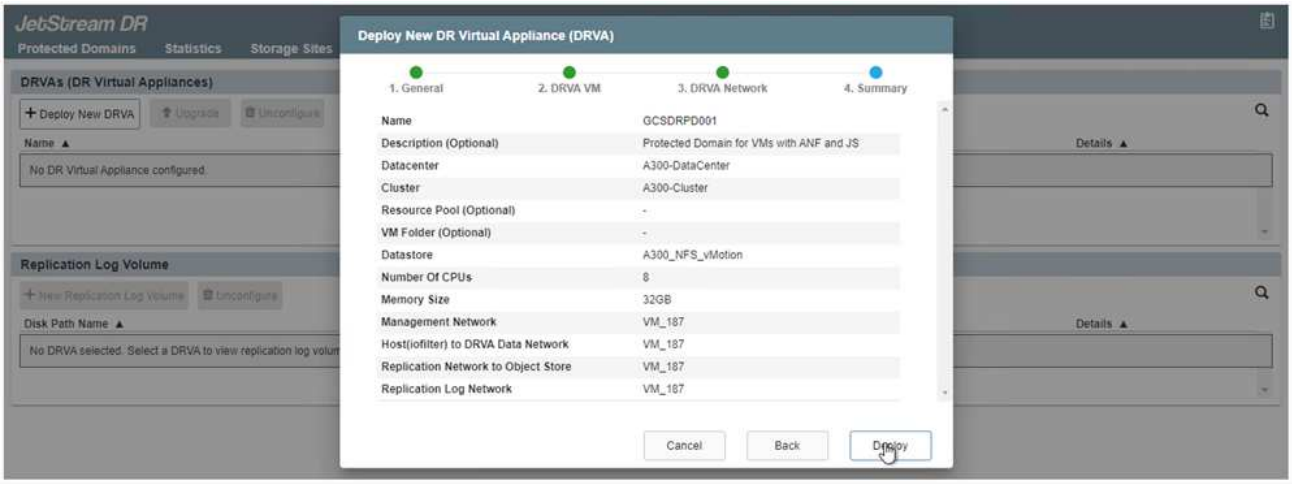
b. リカバリ サイトにある Azure Blob ストレージを追加します。



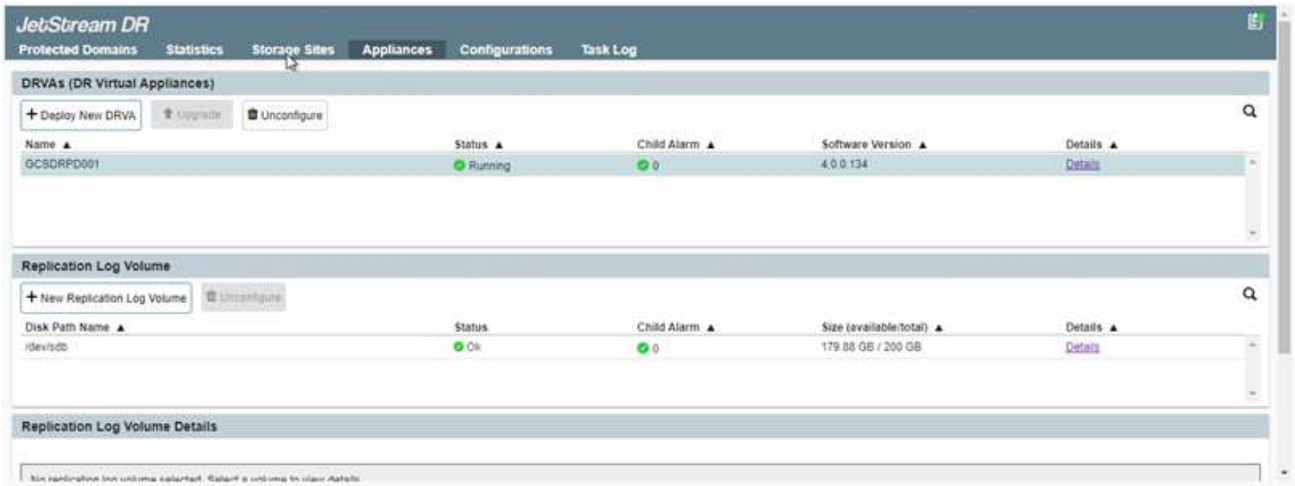
8. アプライアンス タブから必要な数の DR 仮想アプライアンス (DRVA) をデプロイします。

容量計画ツールを使用して、必要な DRVA の数を見積もってください。

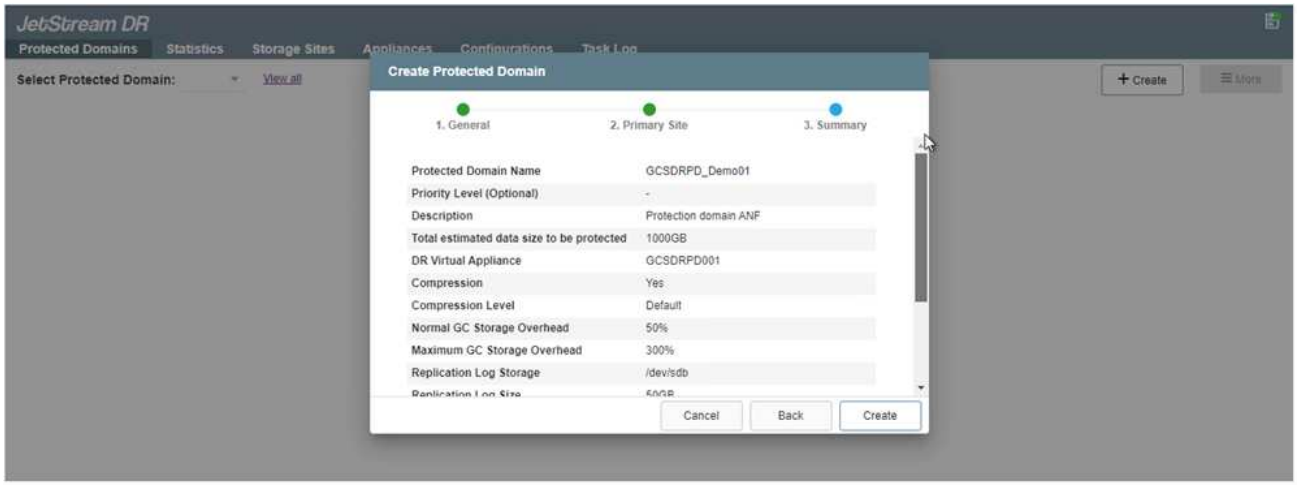


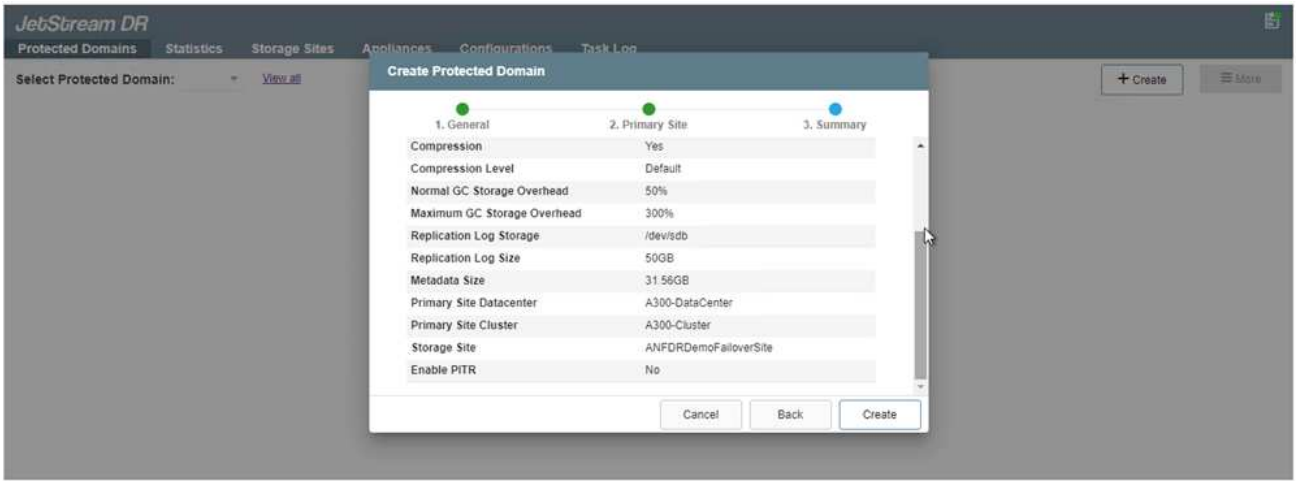


9. 使用可能なデータストアまたは独立した共有 iSCSI ストレージ プールの VMDK を使用して、各 DRVA のレプリケーション ログ ボリュームを作成します。



10. [保護されたドメイン] タブで、Azure Blob Storage サイト、DRVA インスタンス、レプリケーション ログに関する情報を使用して、必要な数の保護されたドメインを作成します。保護されたドメインは、一緒に保護され、フェイルオーバー/フェイルバック操作の優先順位が割り当てられている、クラスター内の特定の VM またはアプリケーション VM のセットを定義します。

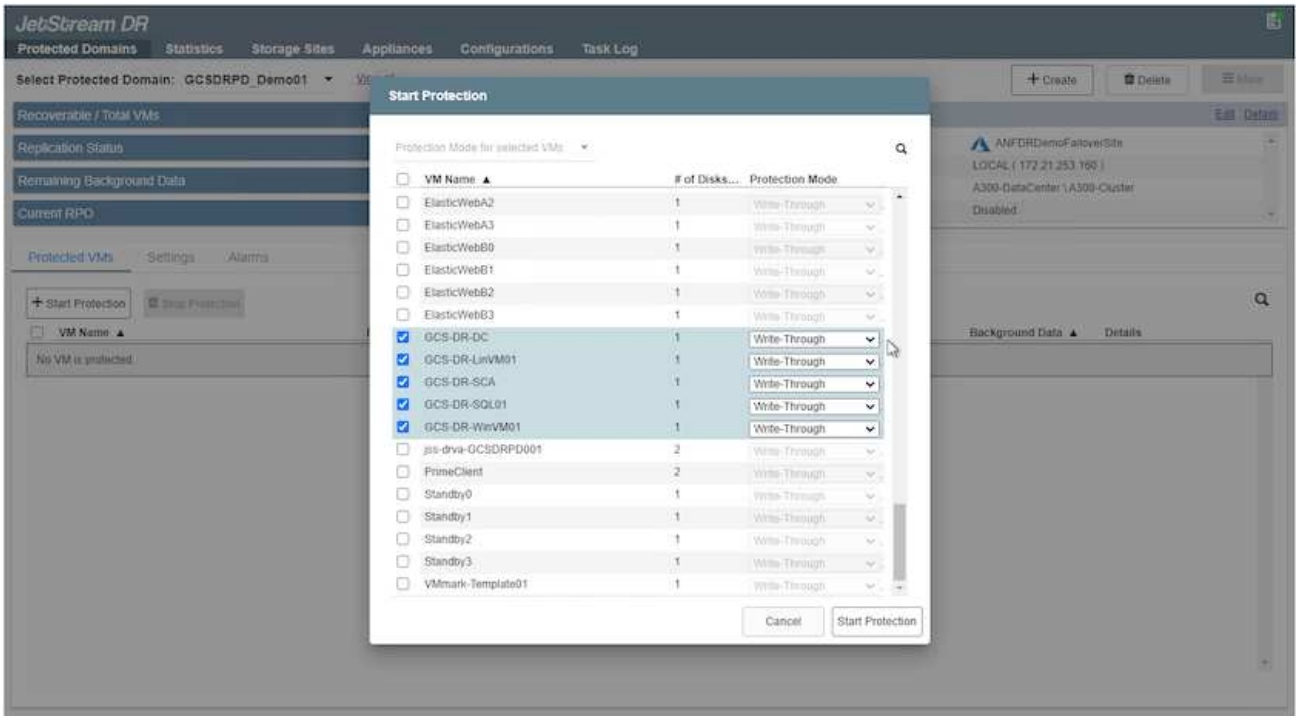




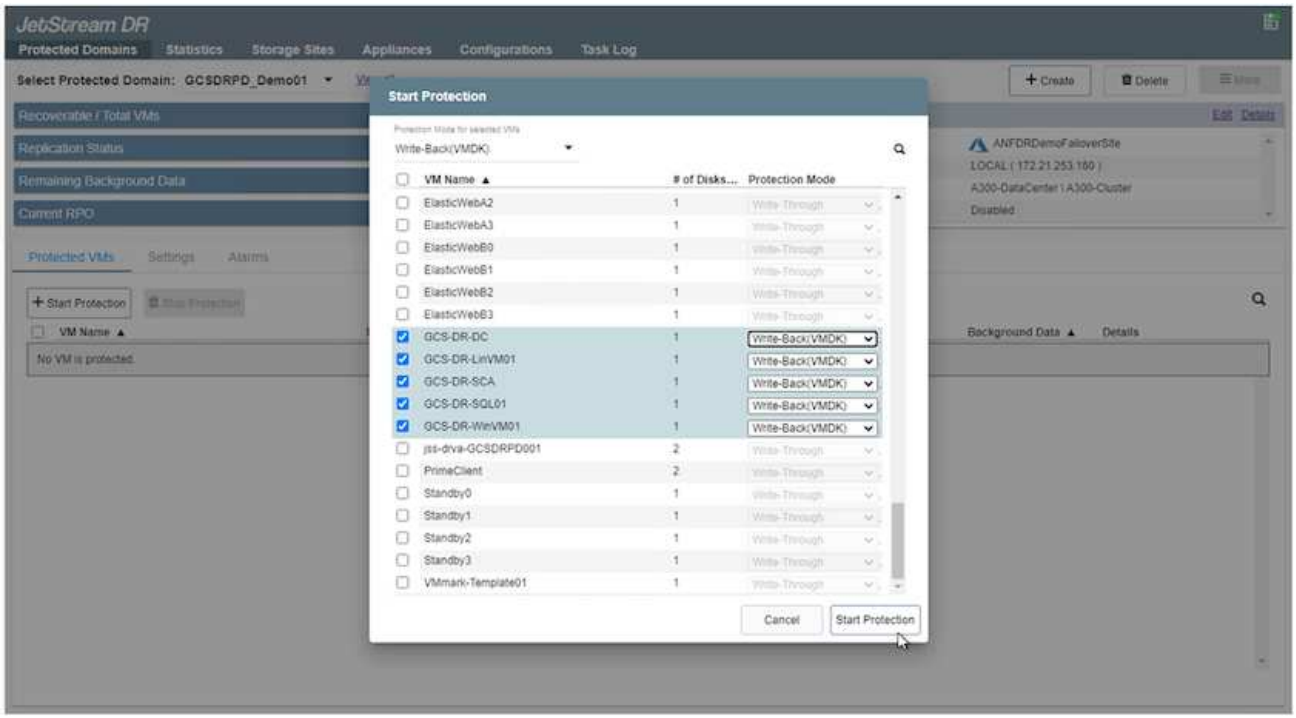
11. 保護する VM を選択し、依存関係に基づいて VM をアプリケーション グループにグループ化します。アプリケーション定義を使用すると、VM のセットを、ブート順序、ブート遅延、およびリカバリ時に実行できるオプションのアプリケーション検証を含む論理グループにグループ化できます。

保護された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。

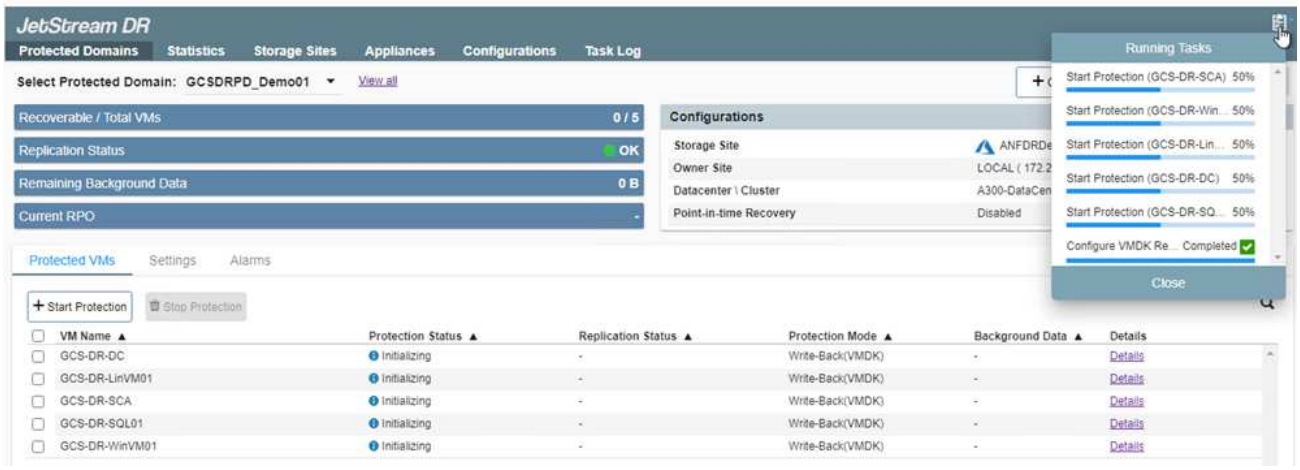
ライトバック (VMDK) モードでは、より高いパフォーマンスが提供されます。



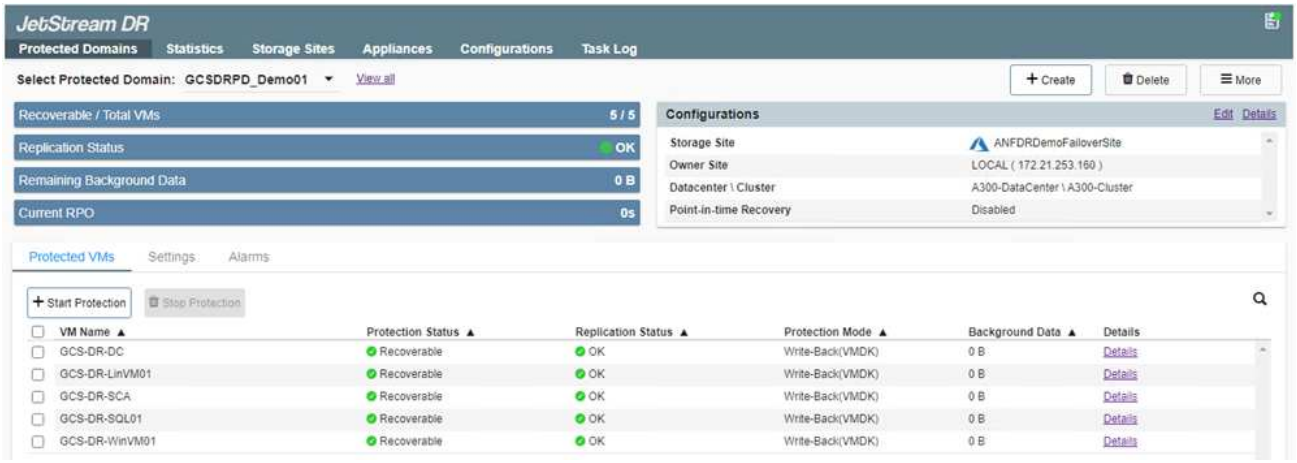
12. レプリケーション ログ ボリュームが高性能ストレージに配置されていることを確認します。



13. 完了したら、保護されたドメインの「保護の開始」をクリックします。これにより、選択した VM の指定された BLOB ストアへのデータ レプリケーションが開始されます。



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してマークされます。



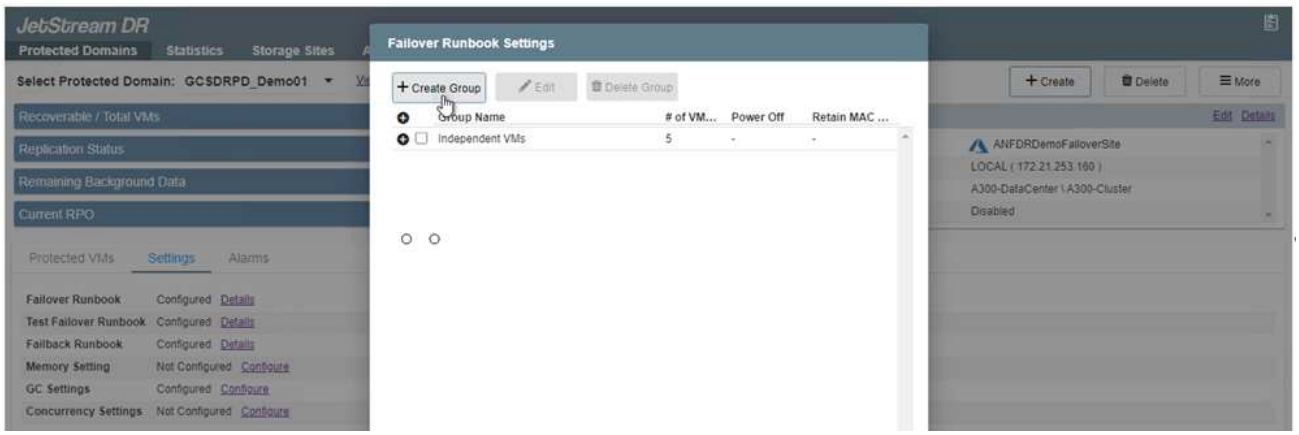
フェールオーバー ランブックは、VM をグループ化 (回復グループと呼ばれる) し、ブート順序シーケンスを設定し、CPU/メモリ設定と IP 構成を変更するように構成できます。

15. [設定] をクリックし、Runbook の構成リンクをクリックして、Runbook グループを構成します。

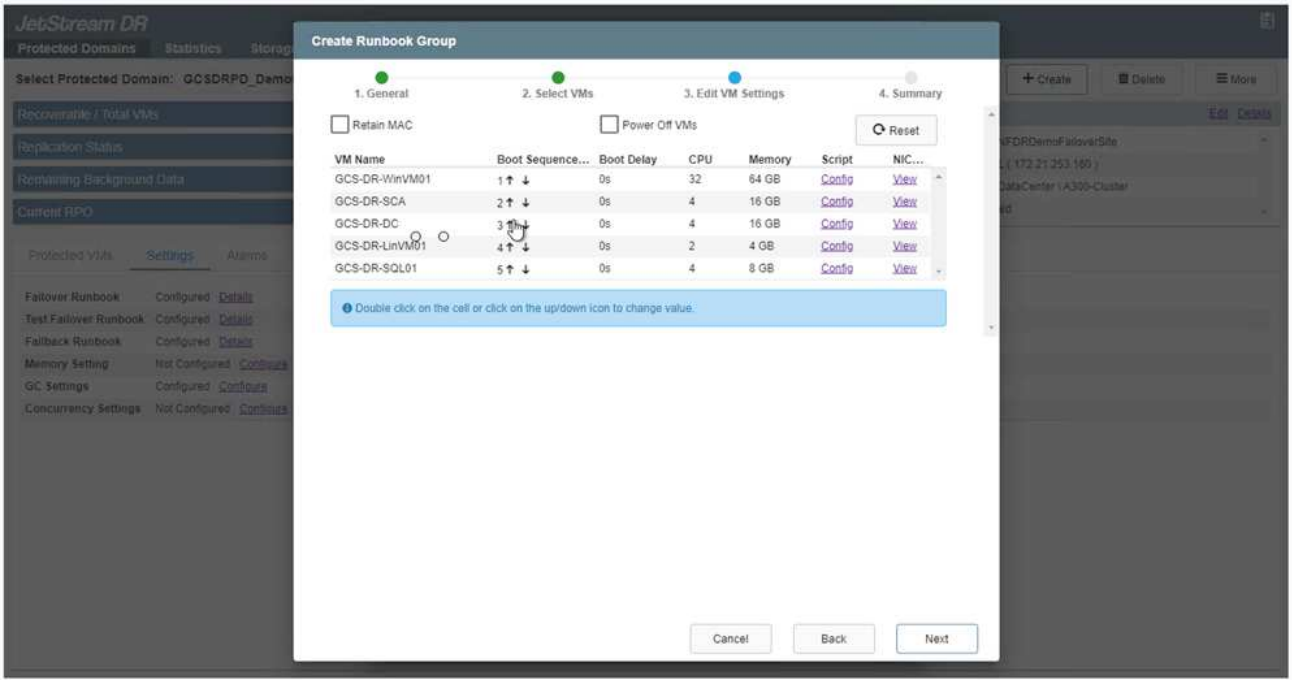


16. [グループの作成] ボタンをクリックして、新しい Runbook グループの作成を開始します。

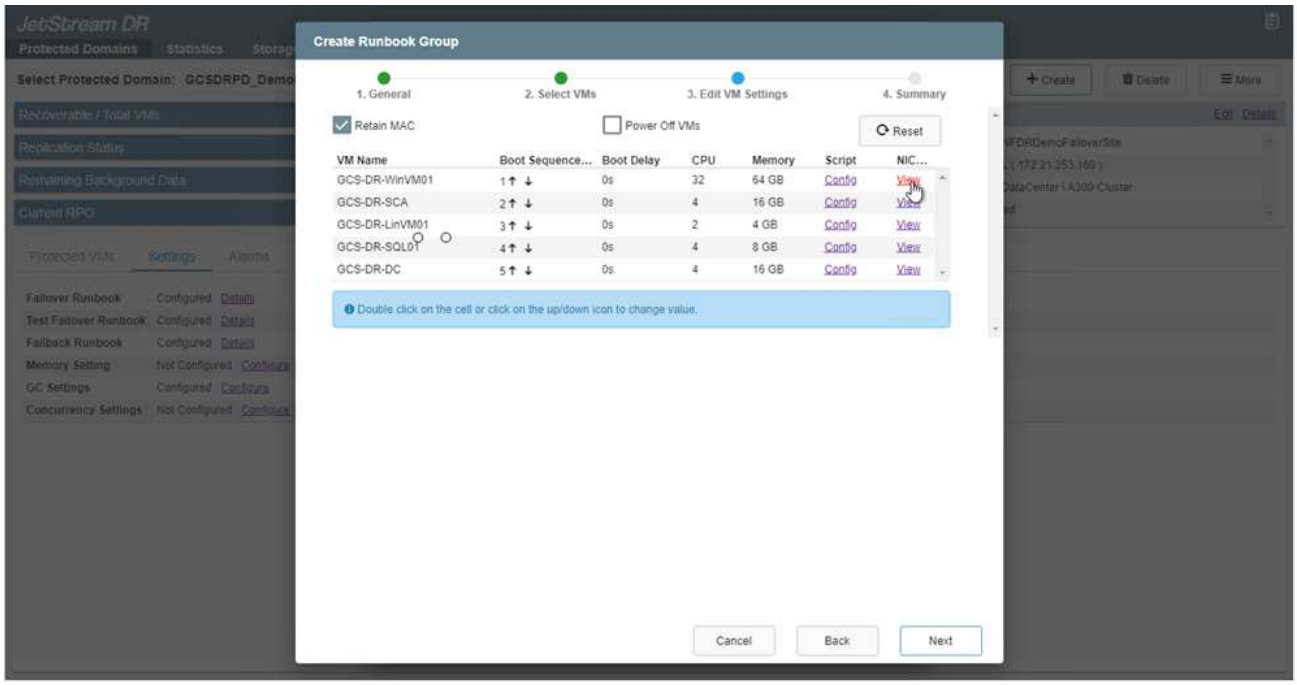
必要に応じて、画面の下部で、ランブック グループの操作の前後に自動的に実行されるカスタム事前スクリプトと事後スクリプトを適用します。 Runbook スクリプトが管理サーバー上に存在していることを確認します。



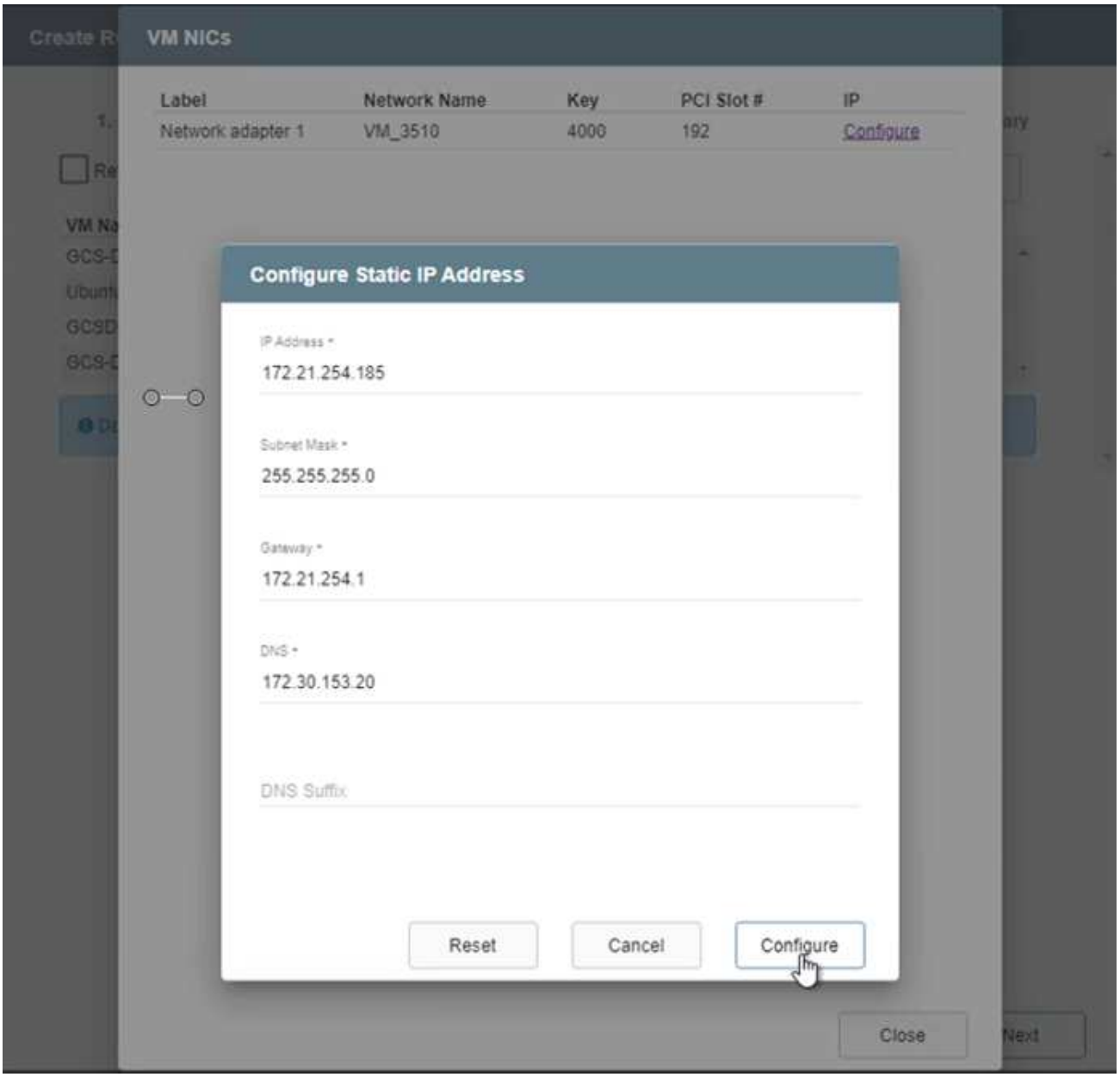
17. 必要に応じて VM 設定を編集します。ブート シーケンス、ブート遅延 (秒単位で指定)、CPU の数、割り当てるメモリの量など、VM を回復するためのパラメータを指定します。上矢印または下矢印をクリックして、VM のブート シーケンスを変更します。 MAC を保持するためのオプションも提供されています。

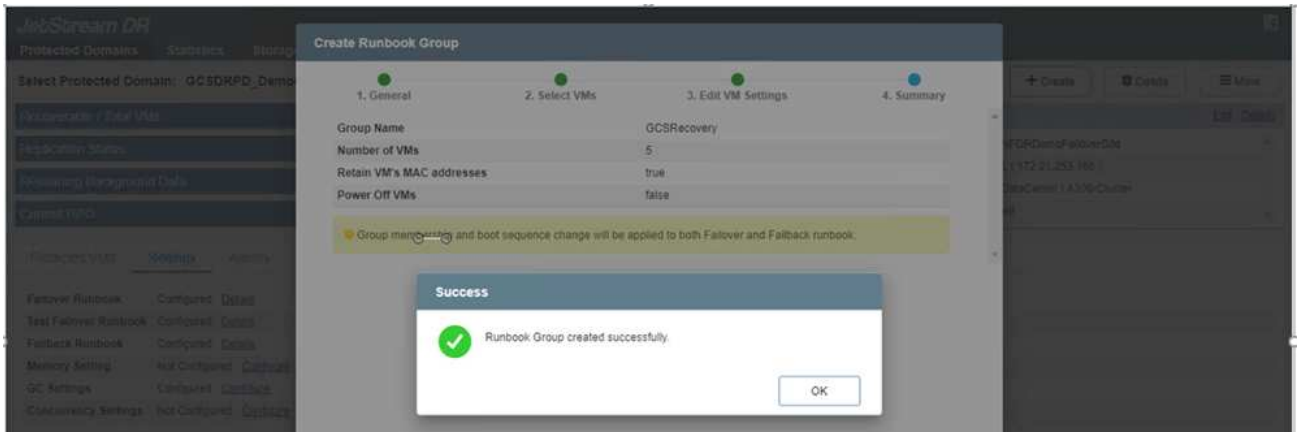


18. グループ内の個々の VM に対して静的 IP アドレスを手動で構成できます。 VM の NIC ビュー リンクをクリックして、IP アドレス設定を手動で構成します。



19. [構成] 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。





フェールオーバー ランブックとフェールバック ランブックの両方のステータスが [構成済み] として表示されます。フェールオーバー ランブック グループとフェールバック ランブック グループは、同じ初期 VM グループと設定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

て変更することで、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。

▼ プライベートクラウドに **JetStream DR for AVS** をインストールする

リカバリ サイト (AVS) のベスト プラクティスは、3 ノードのパイロット ライト クラスターを事前に作成することです。これにより、次のようなリカバリ サイトのインフラストラクチャを事前に構成できます。

- 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用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構成する

JetStream DR は、ミッションクリティカルなドメインに対してほぼゼロの RTO モードをサポートします。これらのドメインでは、宛先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 が推奨されるストレージ タイプです。

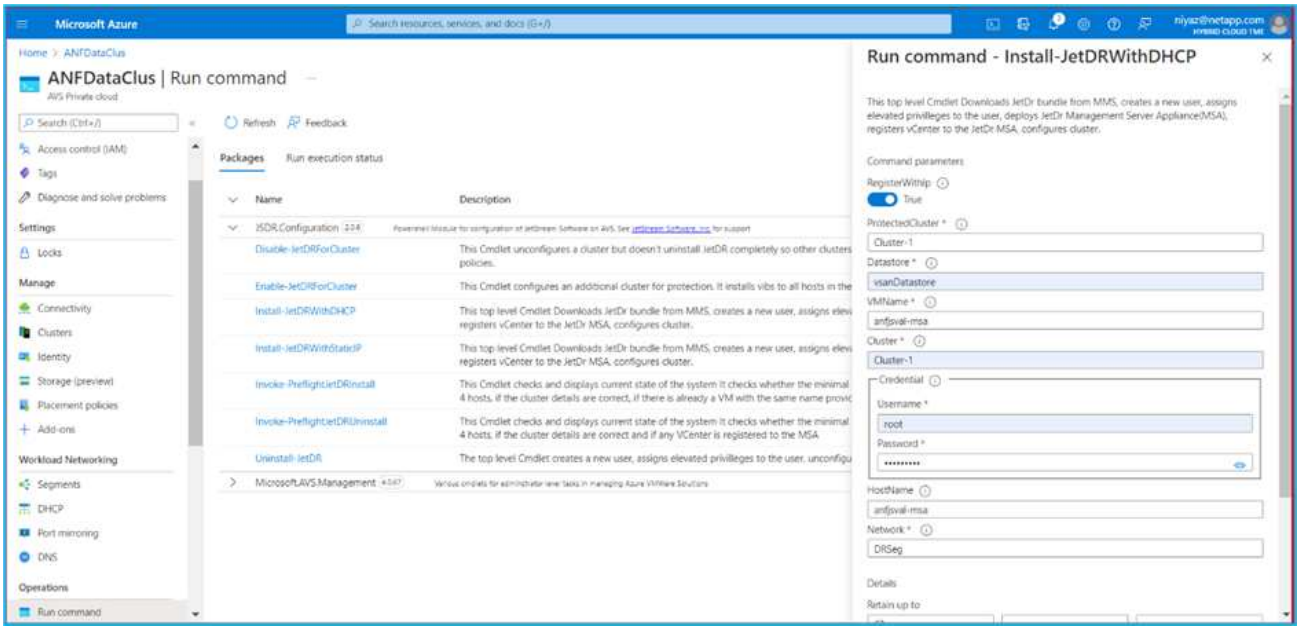
ⓘ セグメント作成を含むネットワーク構成は、オンプレミスの要件に合わせて AVS クラスター上で構成する必要があります。

ⓘ SLA および RTO 要件に応じて、継続的なフェイルオーバー 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 をほぼゼロにするには、リカバリサイトで継続的な再水和を開始する必要があります。

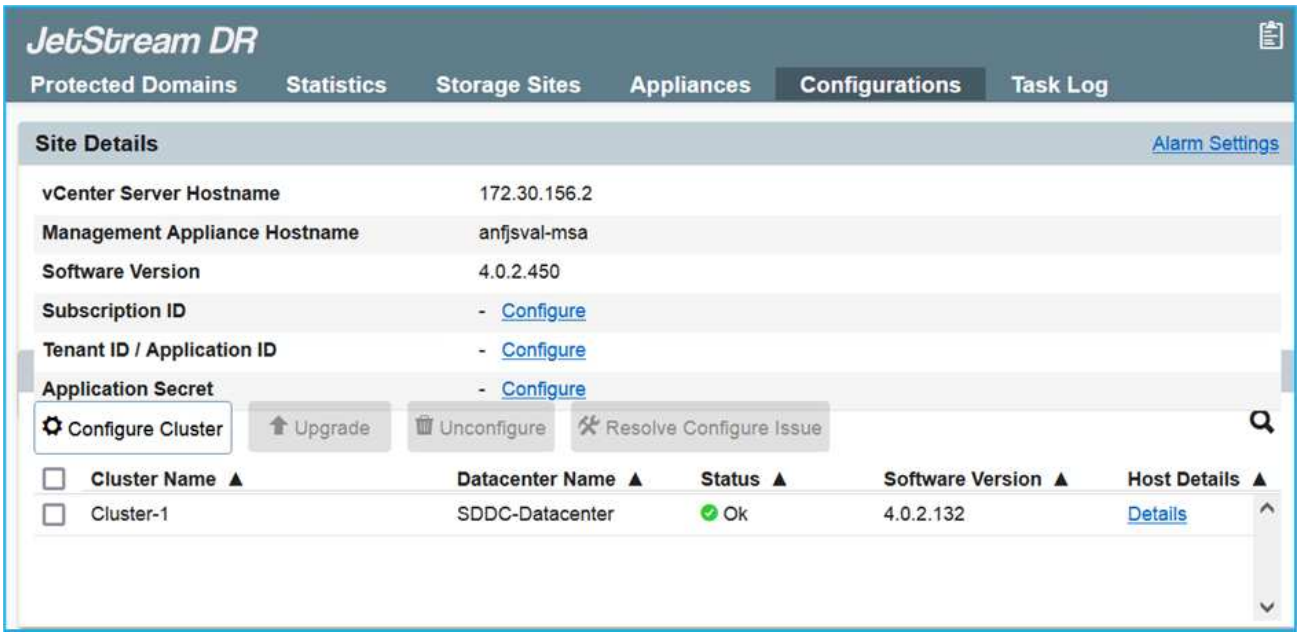
1. Azure VMware Solution プライベート クラウドに JetStream DR for AVS をインストールするには、実行コマンドを使用します。 Azure ポータルから Azure VMware ソリューションに移動し、プライベート クラウドを選択して、[コマンドの実行] > [パッケージ] > [JSDR.Configuration] を選択します。

ⓘ Azure VMware Solution のデフォルトの CloudAdmin ユーザーには、JetStream DR for AVS 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 Solution では、JetStream DR の Azure VMware Solution 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素化および自動化できます。

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。



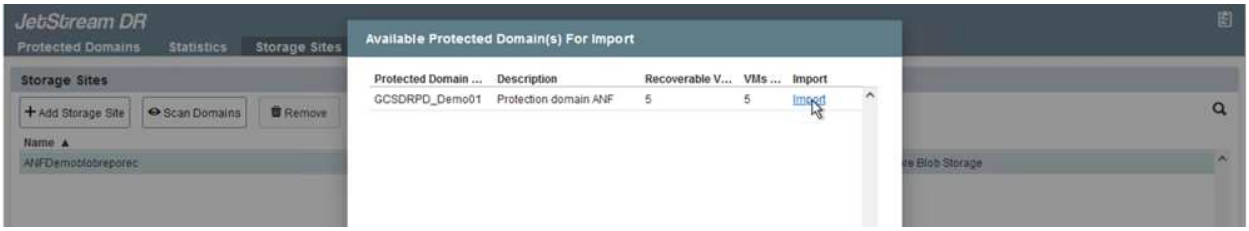
2. JetStream DR for AVS のインストールが完了したら、ブラウザを更新します。 JetStream DR UI にアクセスするには、[SDDC データセンター] > [構成] > [JetStream DR] に移動します。



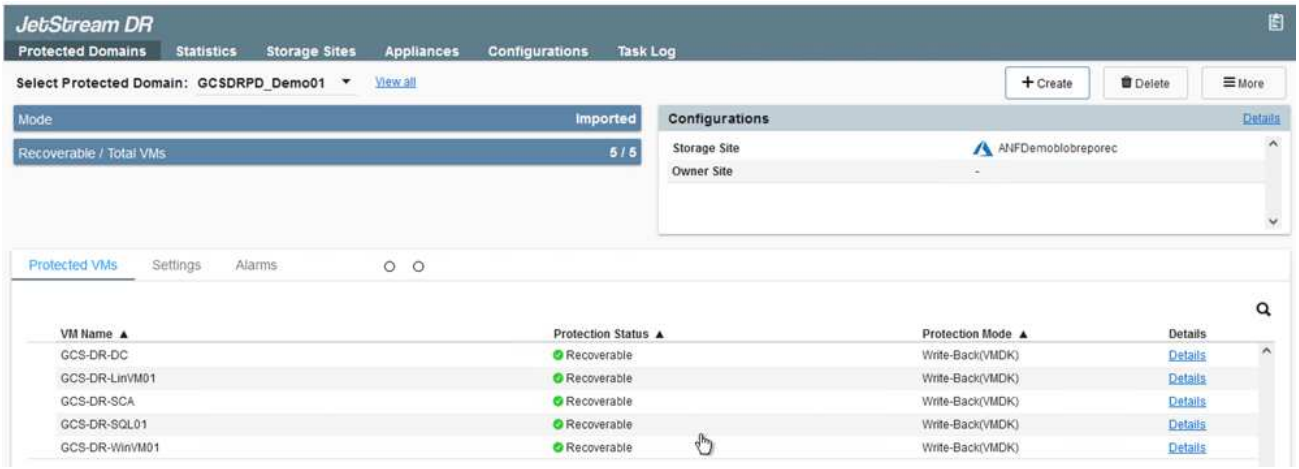
3. JetStream DR インターフェースから、次のタスクを完了します。

   a. オンプレミス クラスターを保護するために使用された Azure Blob Storage アカウントをストレージ サイトとして追加し、スキャン ドメイン 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 ウィンドウで、インポートする保護されたドメインを選択し、そのインポート リンクをクリックします。



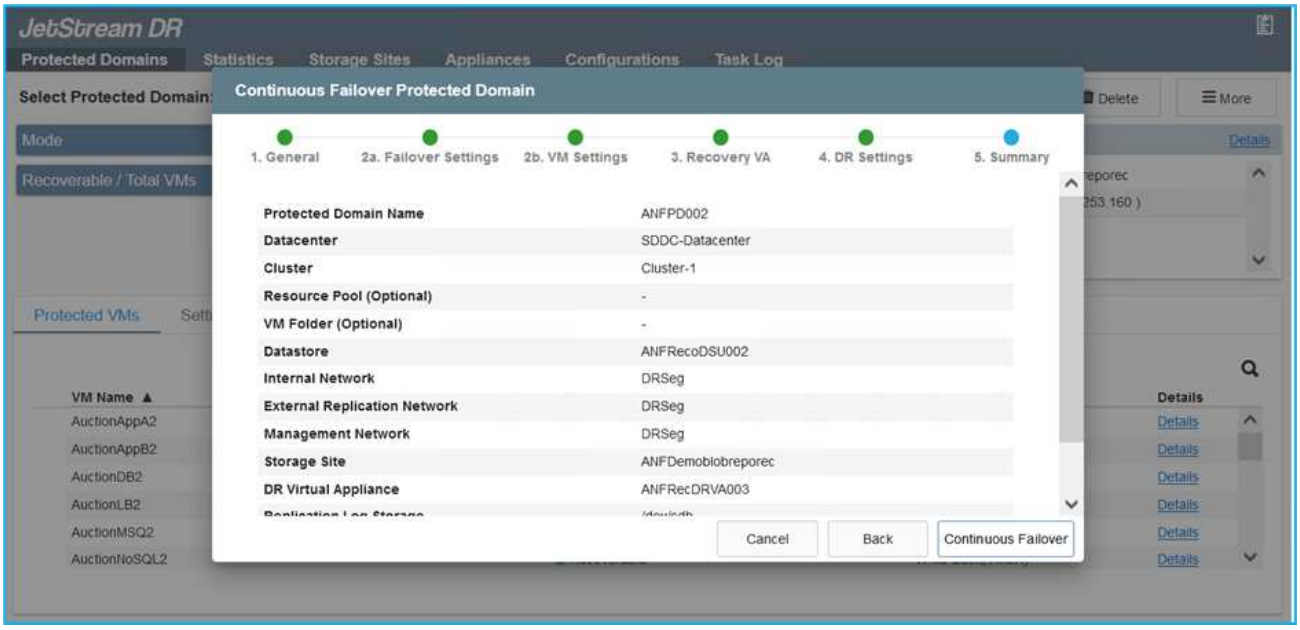
4. ドメインは回復のためにインポートされます。 [保護されたドメイン] タブに移動し、目的のドメインが選択されていることを確認するか、[保護されたドメインの選択] メニューから目的のドメインを選択します。保護されたドメイン内の回復可能な VM のリストが表示されます。



5. 保護されたドメインをインポートした後、DRVA アプライアンスを展開します。

> これらの手順は、CPT が作成した計画を使用して自動化することもできます。

6. 利用可能な 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リカバリ VA を構成します。

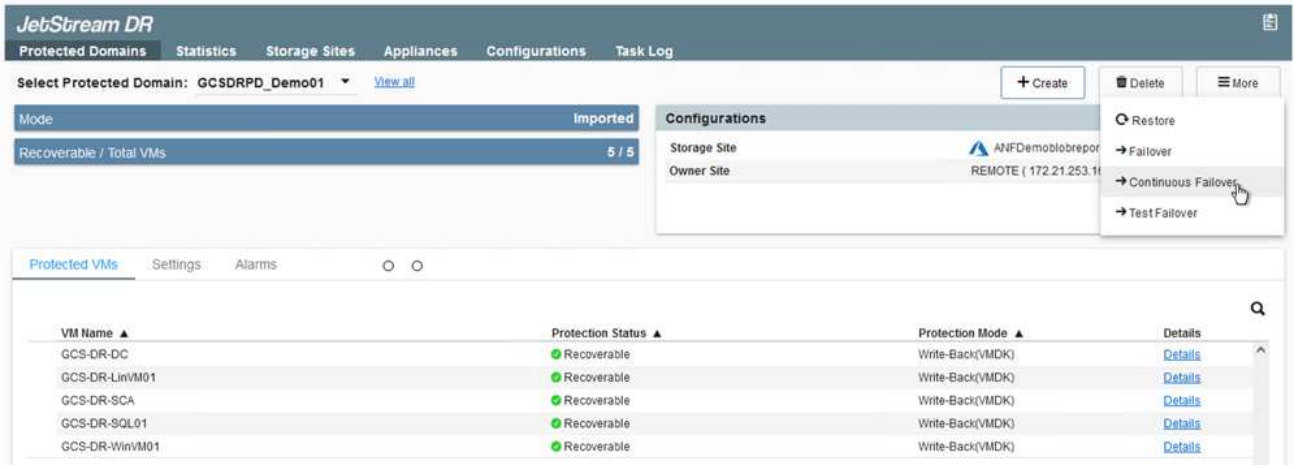


> 選択したセグメントで DHCP が有効になっており、十分な IP が利用可能であることを確認します。ドメインが回復している間、動的 IP が一時的に使用されます。回復中の各 VM (継続的なリハイドレーションを含む) には個別の動的 IP が必要です。回復が完了すると、IP は解放され、再利用できるようになります。

8. 適切なフェイルオーバー オプション (継続的な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、継続的なリハイドレーション (継続的なフェイルオーバー) が選択されています。

> 継続的なフェイルオーバー モードとフェイルオーバー モードは構成の実行タイミングが

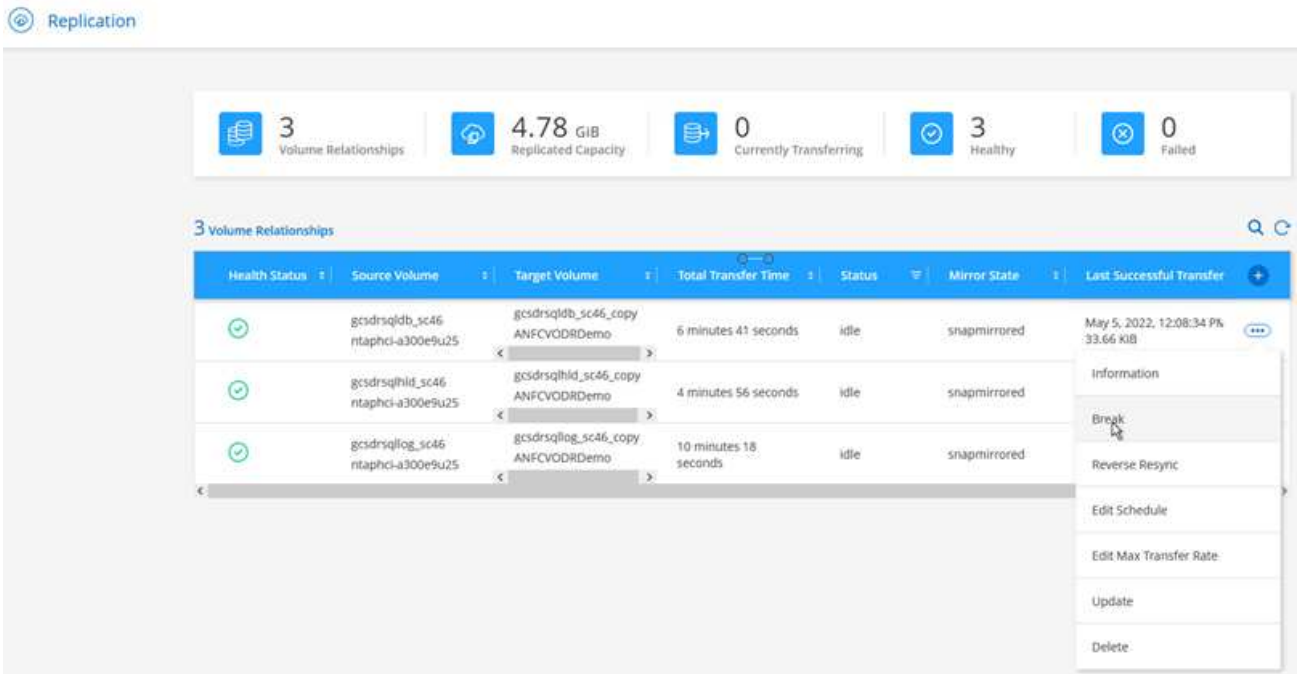
異なりますが、両方のフェイルオーバー モードは同じ手順で構成されます。災害イベントに応じて、フェイルオーバー手順がまとめて構成され、実行されます。継続的なフェイルオーバーはいつでも構成でき、通常のシステム操作中にバックグラウンドで実行できます。災害イベントが発生すると、継続的なフェイルオーバーが完了し、保護された VM の所有権がリカバリ サイトに即座に転送されます (RTO はほぼゼロ)。

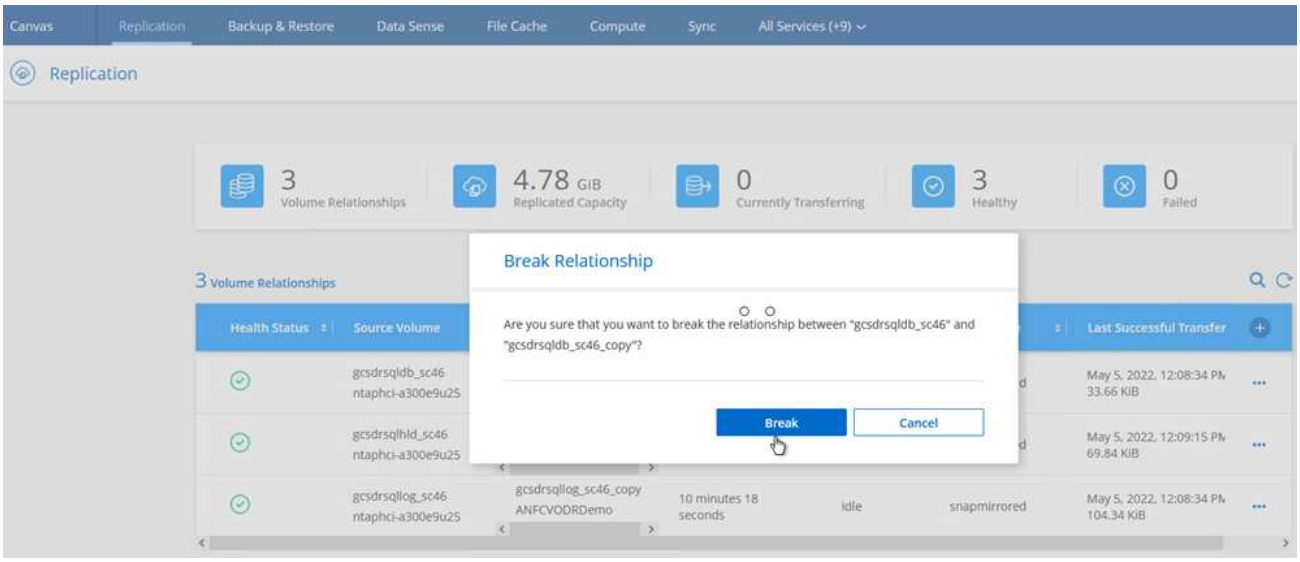


継続的なフェイルオーバー プロセスが開始され、その進行状況を UI から監視できます。 [現在のステップ] セクションの青いアイコンをクリックすると、フェイルオーバー プロセスの現在のステップの詳細を示すポップアップ ウィンドウが表示されます。

▼ フェイルオーバーとフェイルバック

1. オンプレミス環境の保護されたクラスターで災害 (部分的または完全な障害) が発生した後、それぞれのアプリケーション ボリュームのSnapMirror関係を解除した後、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。

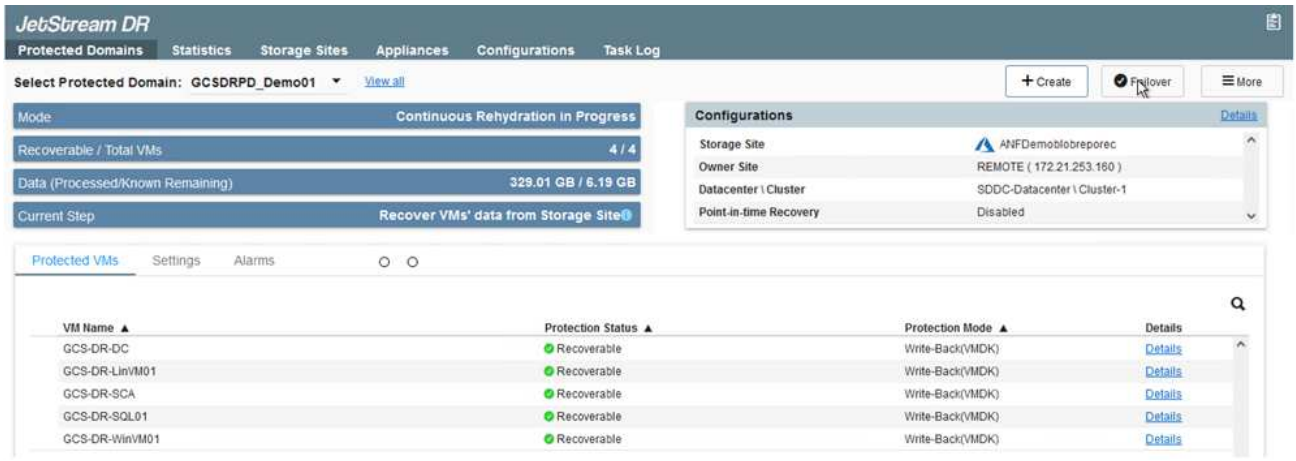


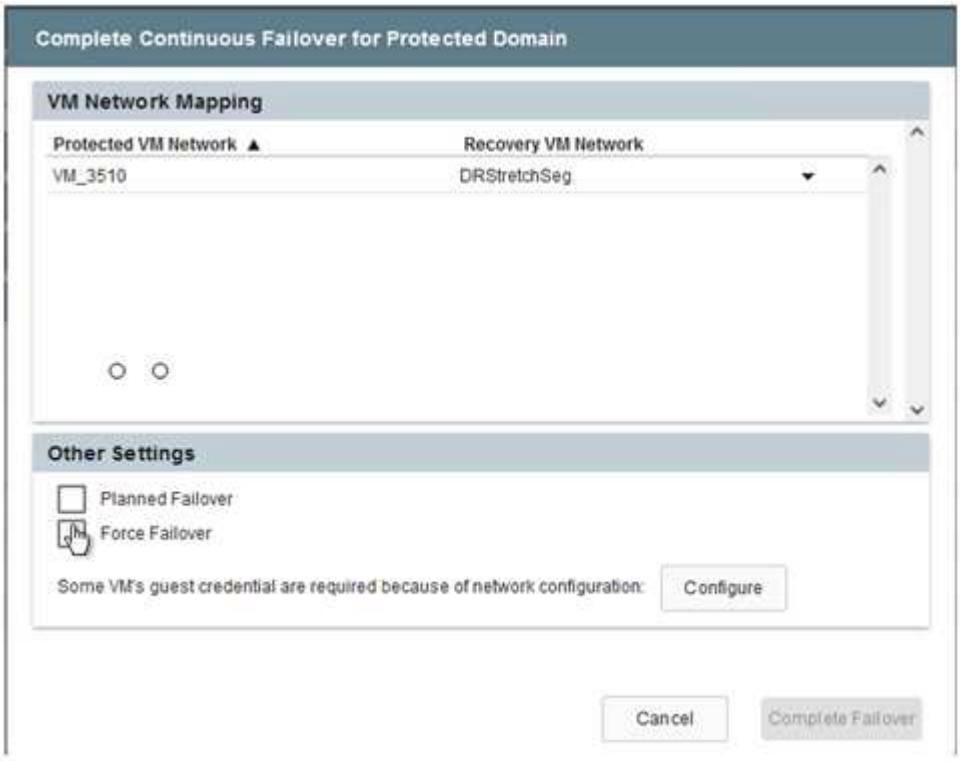


このステップは簡単に自動化でき、回復プロセスが容易になります。

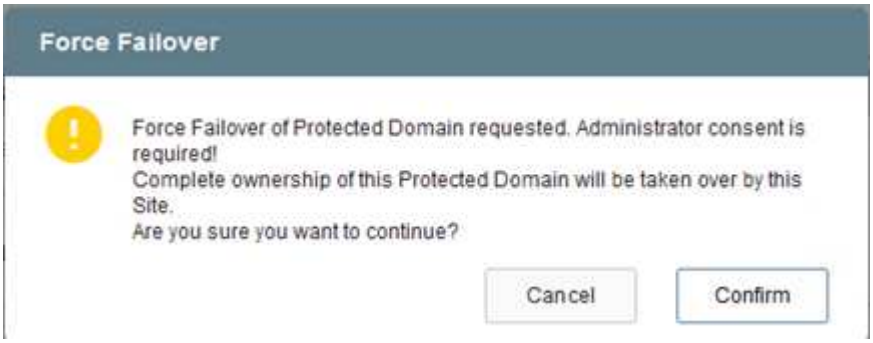
2. AVS SDDC (宛先側) の Jetstream UI にアクセスし、フェイルオーバー オプションをトリガーしてフェイルオーバーを完了します。タスク バーには、フェールオーバー アクティビティの進行状況が表示されます。

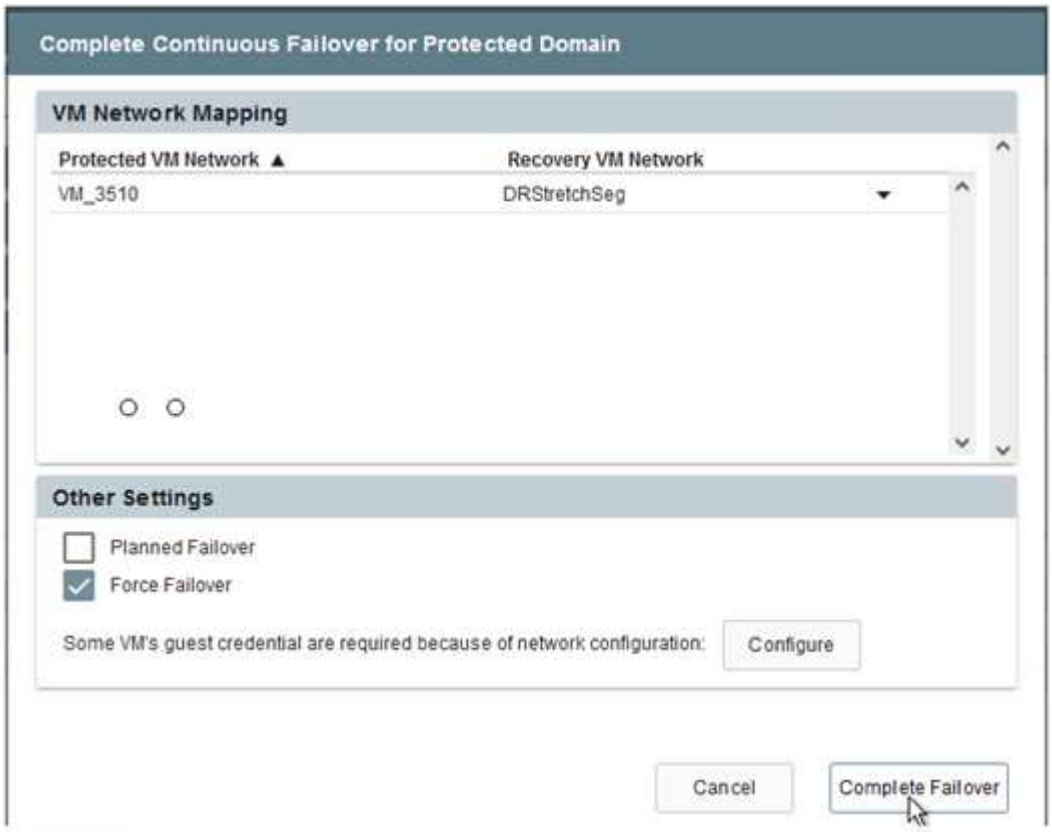
   フェイルオーバーの完了時に表示されるダイアログ ウィンドウでは、フェイルオーバー タスクを計画どおりに実行するか、強制実行するかを指定できます。





強制フェールオーバーでは、プライマリ サイトにアクセスできなくなり、保護されたドメインの所有権はリカバリ サイトが直接引き継ぐ必要があると想定されます。





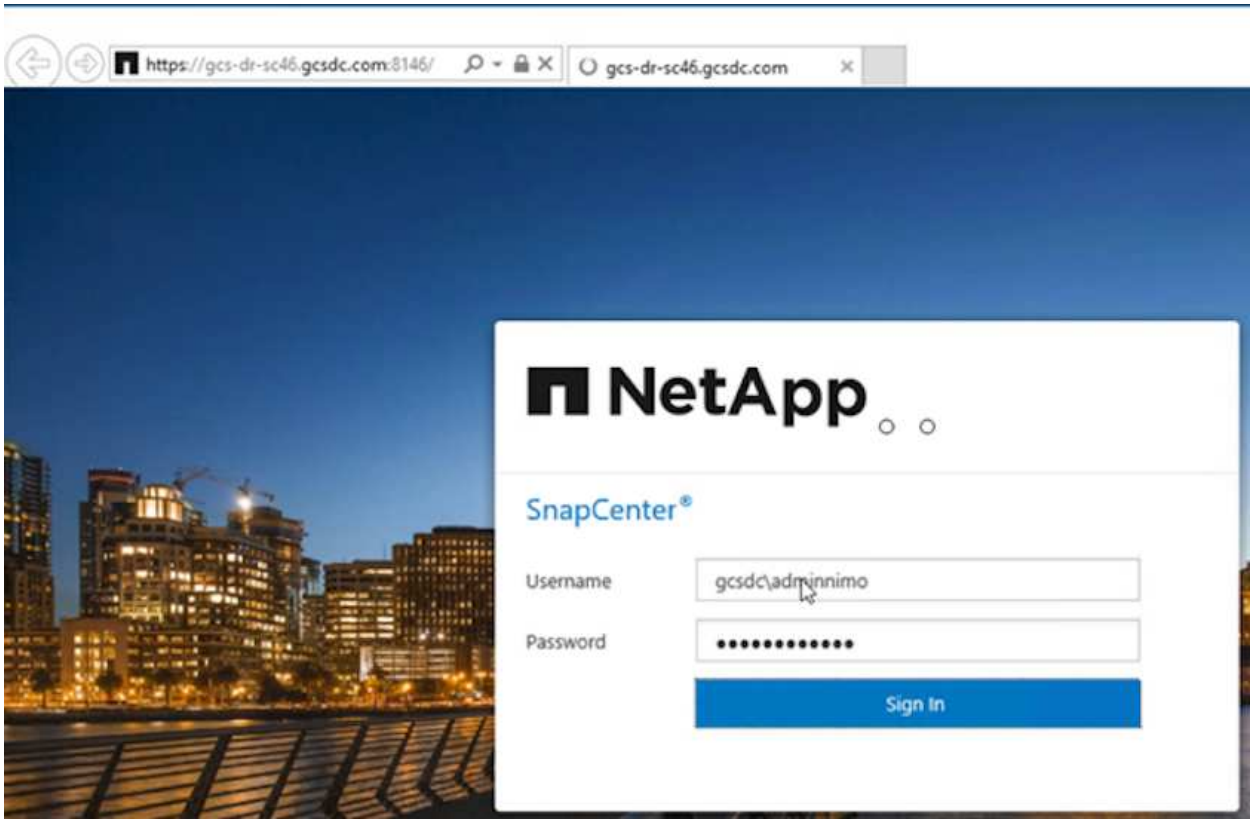
3. 継続的なフェイルオーバーが完了すると、タスクの完了を確認するメッセージが表示されます。タスクが完了したら、回復した VM にアクセスして、ISCSI または NFS セッションを構成します。

フェールオーバー モードが「フェールオーバーで実行中」に変わり、VM のステータスは「回復可能」になります。保護された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回復サイトで実行されるようになりました。

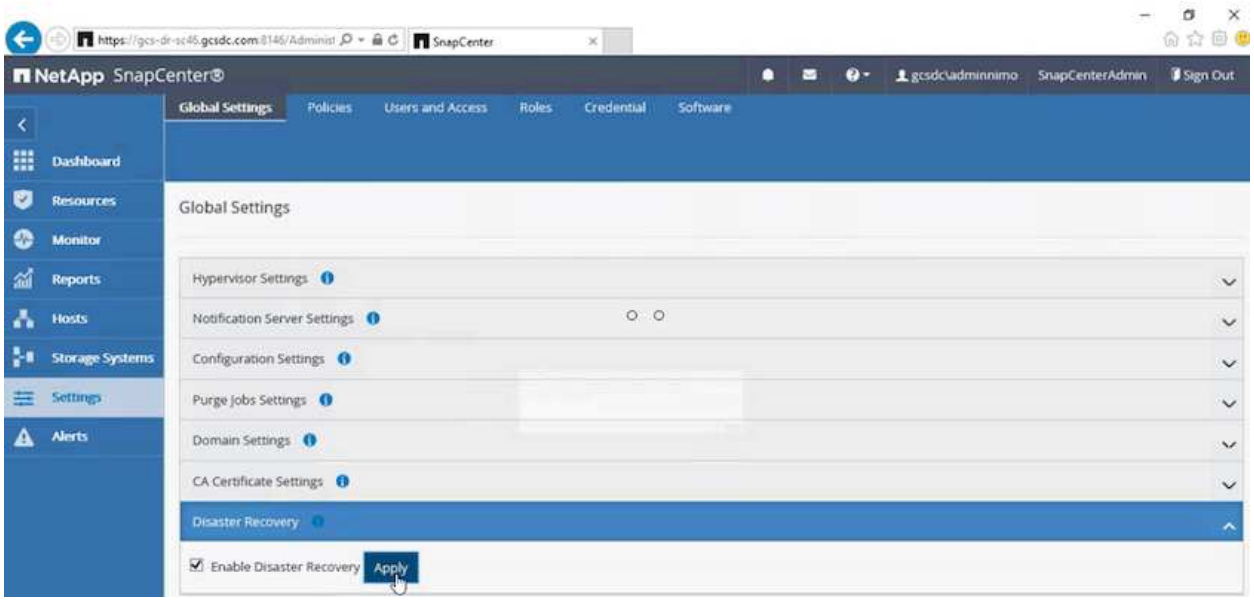
フェイルオーバー構成とインフラストラクチャを検証するには、JetStream DR をテスト モード (テスト フェイルオーバー オプション) で操作して、オブジェクト ストアからテスト リカバリ環境への仮想マシンとそのデータのリカバリを観察できます。フェイルオーバー手順をテスト モードで実行すると、その操作は実際のフェイルオーバー プロセスに似たものになります。



4. 仮想マシンが復旧されたら、ゲスト内のストレージに対してストレージ ディザスタ リカバリを使用します。この例では、このプロセスを説明するために、SQL サーバーを使用します。
5. AVS SDDC 上の回復されたSnapCenter VM にログインし、DR モードを有効にします。
   a. ブラウザN を使用してSnapCenter UI にアクセスします。



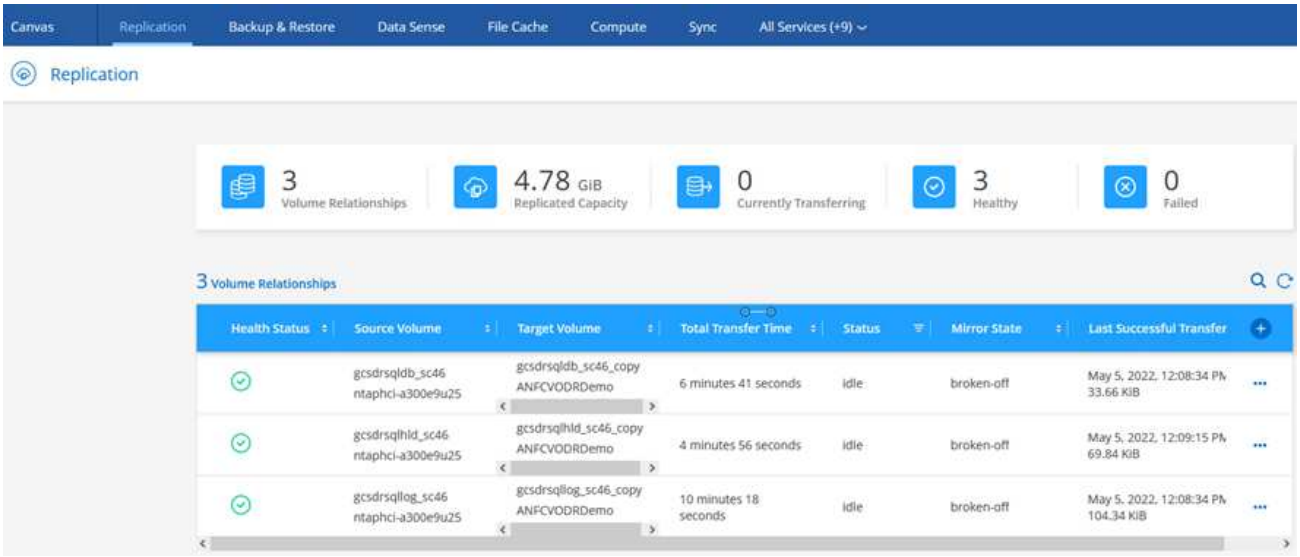
   b. [設定] ページで、[設定] > [グローバル設定] > [障害復旧] に移動します。
   c. 「災害復旧を有効にする」を選択します。
   d. [Apply]をクリックします。



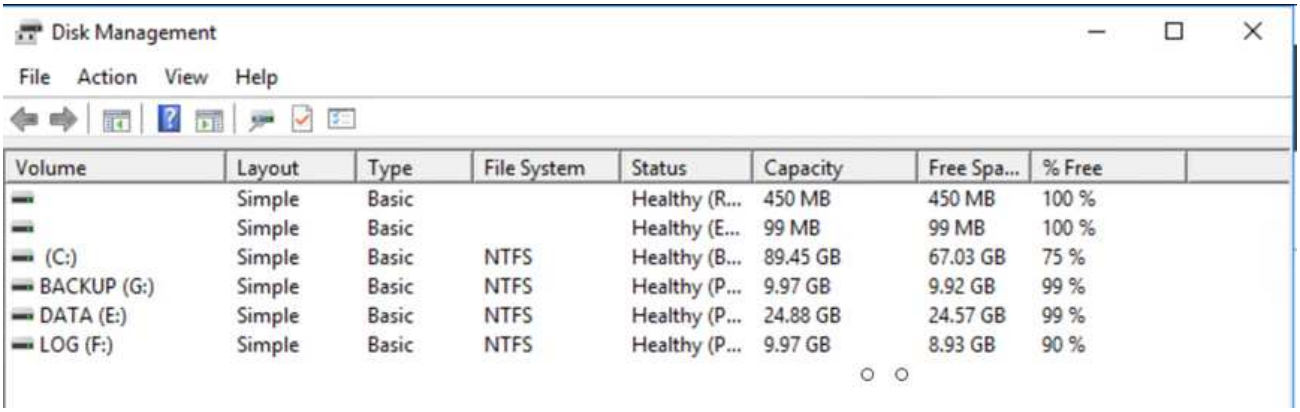
e. [モニター] > [ジョブ] をクリックして、DR ジョブが有効になっているかどうかを確認します。

ストレージの災害復旧には、 NetApp SnapCenter 4.6 以降を使用する必要があります。以前のバージョンでは、アプリケーション整合性スナップショット (SnapMirror を使用して複製) を使用し、災害復旧サイトで以前のバックアップを復旧する必要がある場合は手動復旧を実行する必要があります。

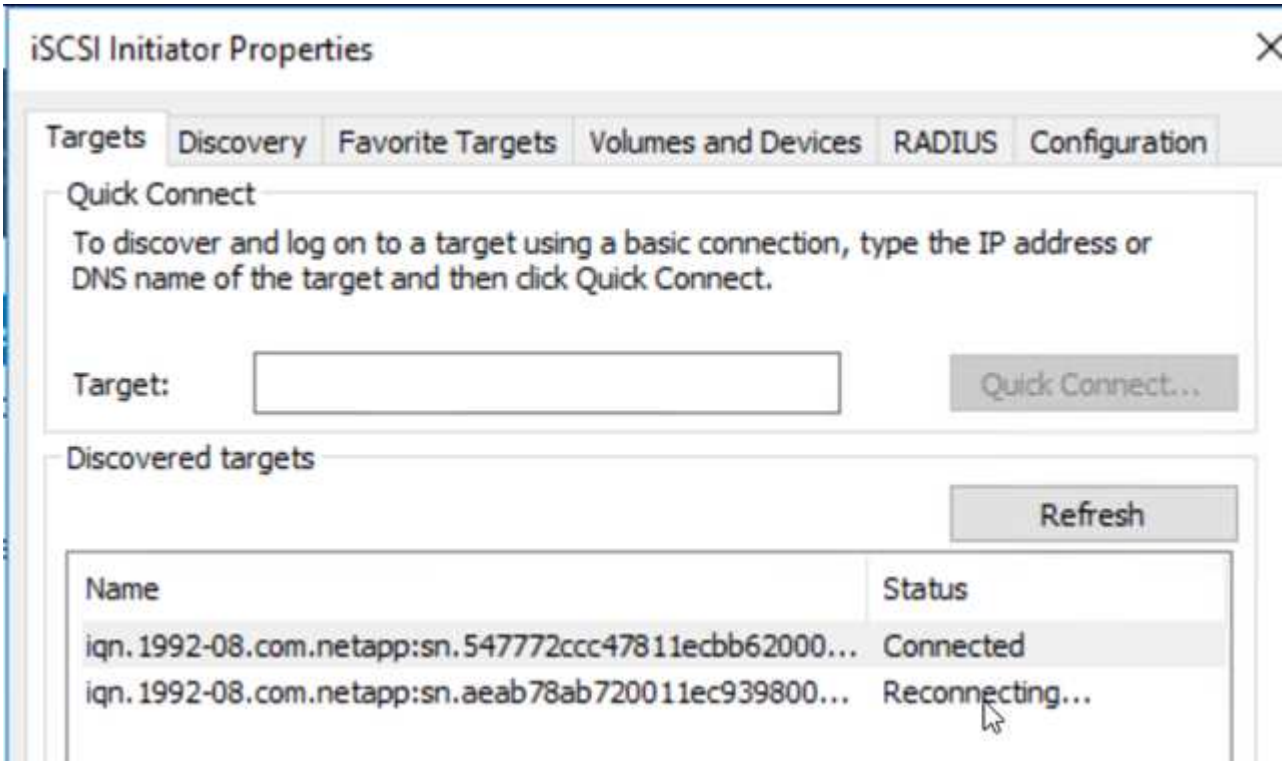
6. SnapMirror関係が解除されていることを確認します。



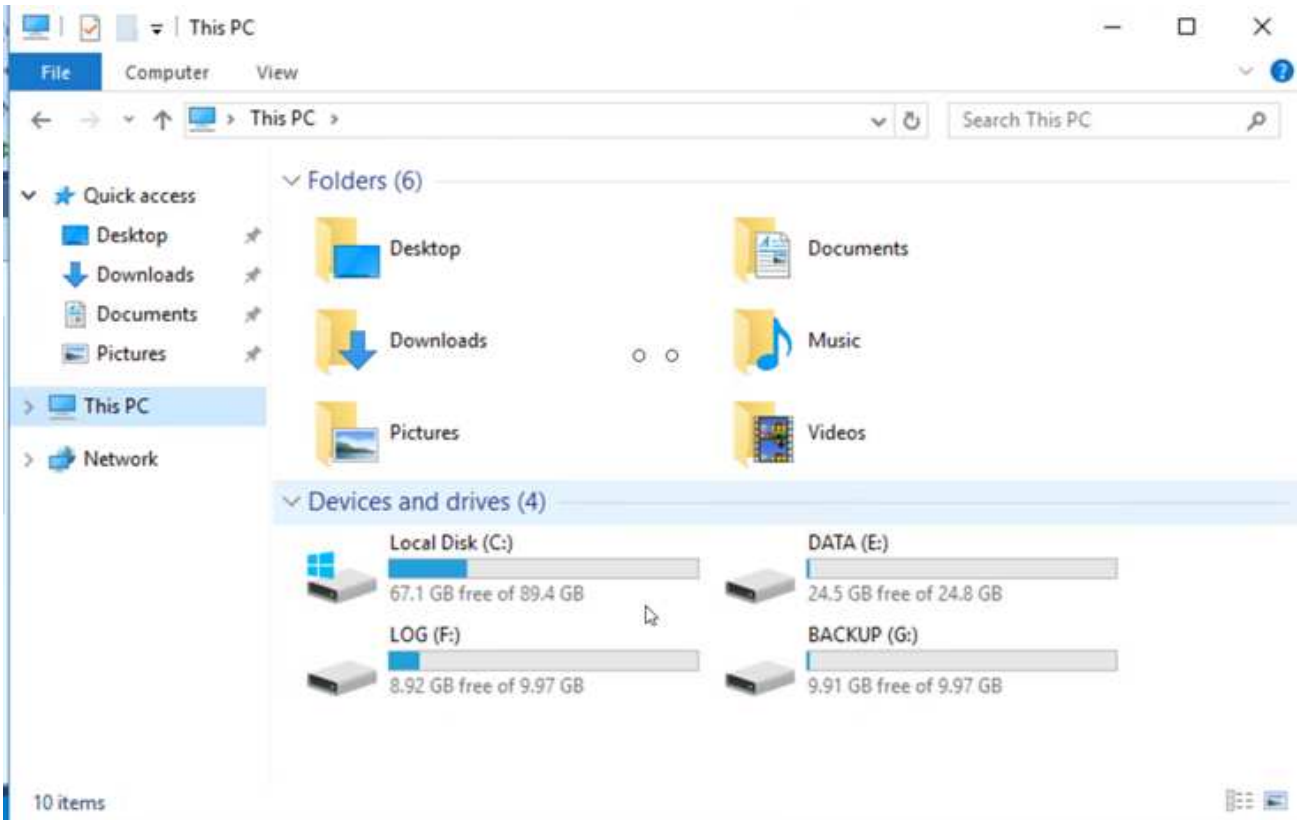
7. Cloud Volumes ONTAPからの LUN を、同じドライブ文字を使用して、回復した SQL ゲスト VM に接続します。



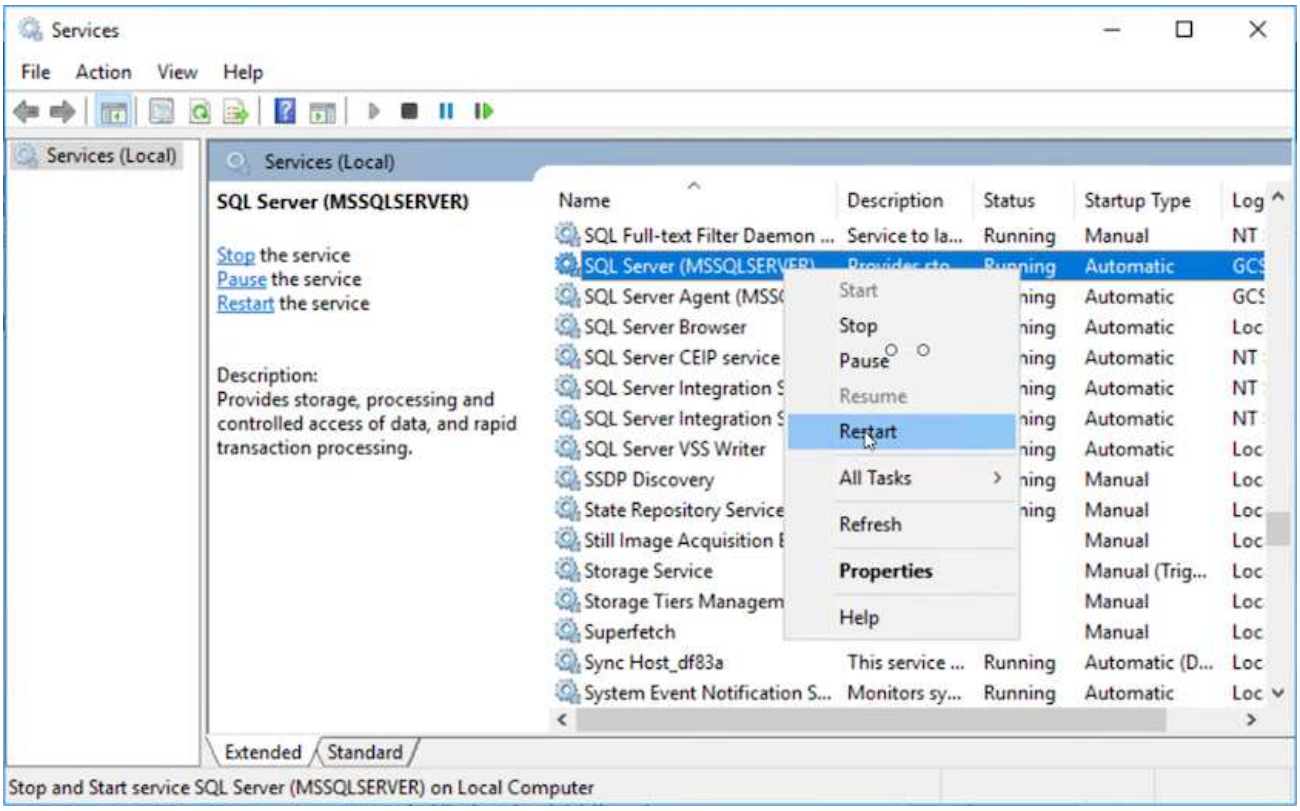
8. iSCSI イニシエーターを開き、以前の切断されたセッションをクリアし、複製されたCloud Volumes ONTAPボリュームのマルチパスとともに新しいターゲットを追加します。



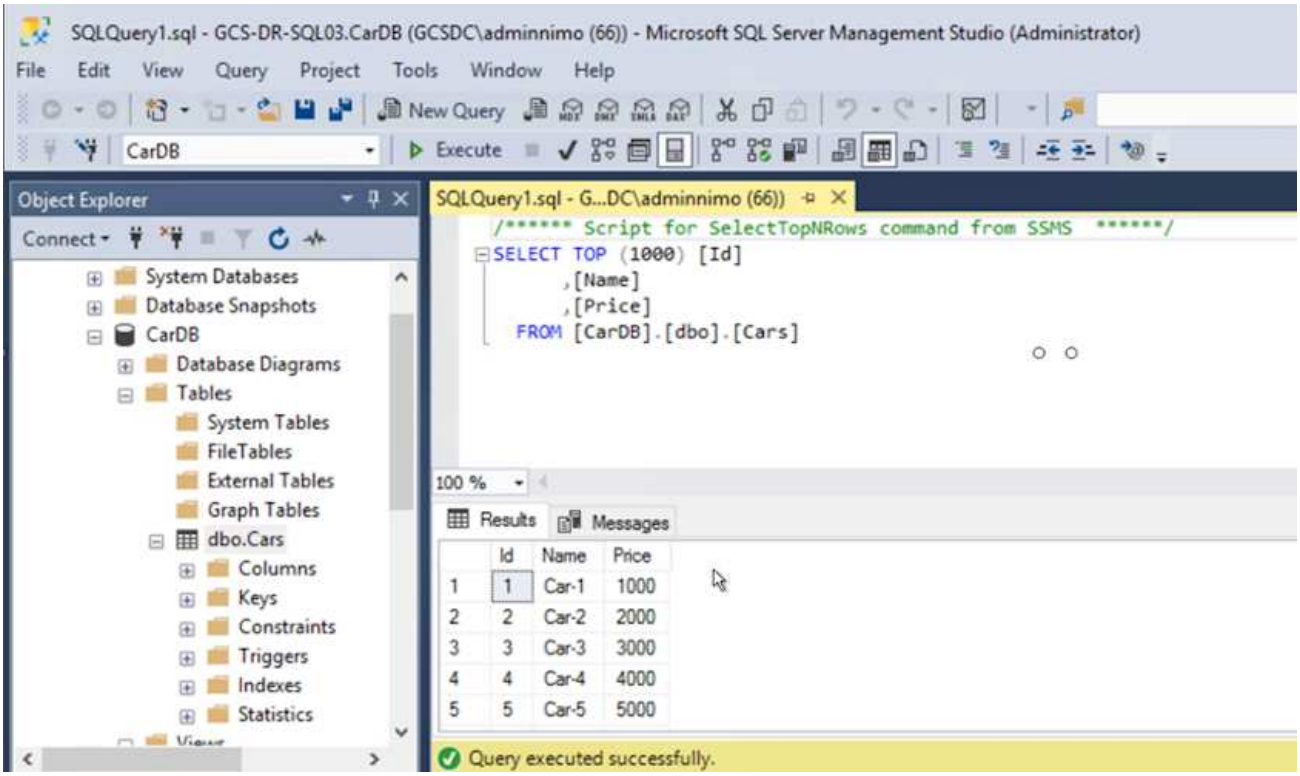
9. すべてのディスクが DR 前に使用されていたのと同じドライブ文字を使用して接続されていることを確認します。



10. MSSQL サーバー 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、マウントコマンドを使用してボリュームを接続し、 `/etc/fstab`エントリ。

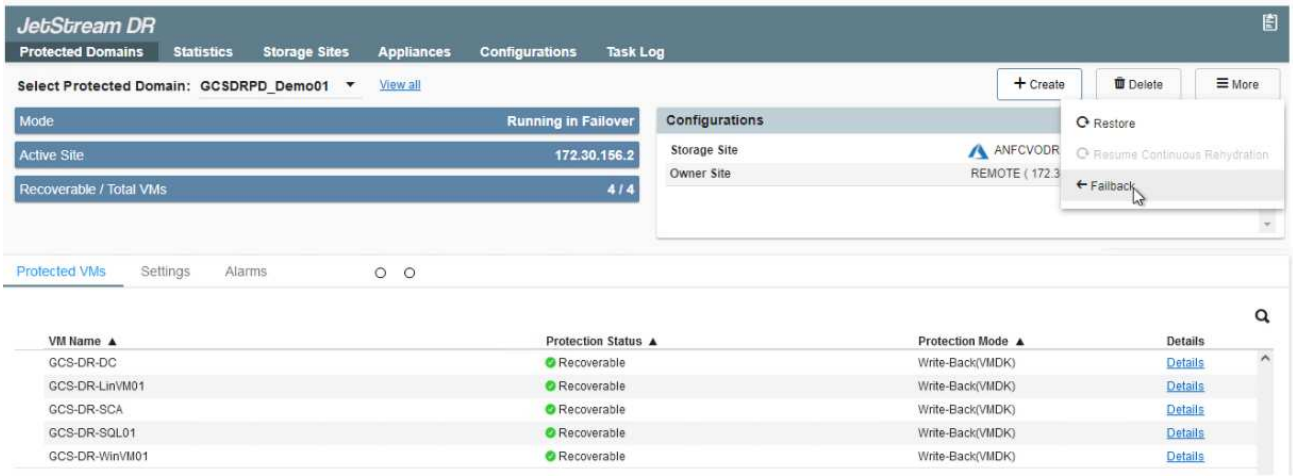
この時点で、操作を実行でき、ビジネスは正常に継続されます。

NSX-T 側では、フェイルオーバー シナリオをシミュレートするために、専用の Tier-1 ゲートウェイを別途作成できます。これにより、すべてのワークロードが相互に通信できる一方で、環境内外へのトラフィックのルーティングが不可能となり、相互汚染のリスクなしにトリアージ、封じ込め、または強化タスクを実行できるようになります。この操作はこのドキュメントの範囲外ですが、分離をシミュレートするために簡単に実行できます。

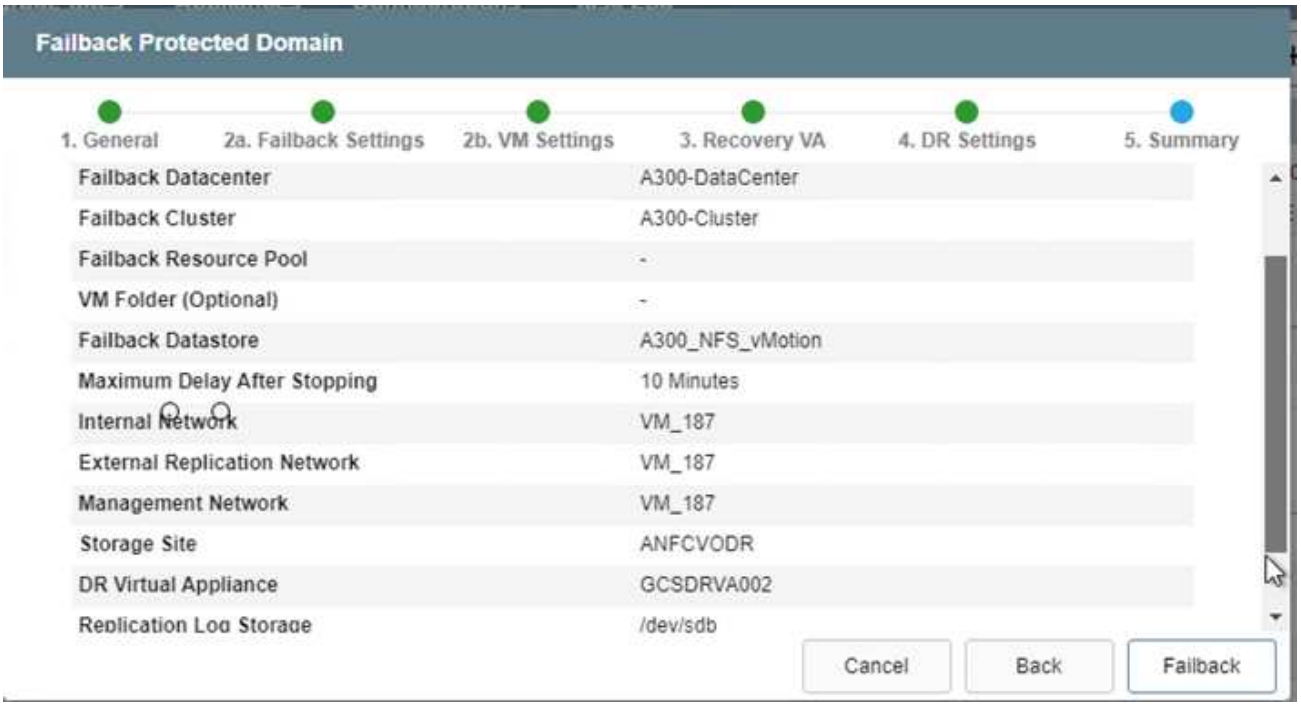
プライマリ サイトが再び稼働したら、フェイルバックを実行できます。 VM 保護は Jetstream によって再開され、 SnapMirror関係を元に戻す必要があります。

1. オンプレミス環境を復元します。災害インシデントの種類によっては、保護されたクラスターの構成を復元および/または検証する必要がある場合があります。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. 復元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、適切な保護されたドメインを選択します。保護されたサイトのフェイルバックの準備ができたら、UI でフェイルバック オプションを選択します。

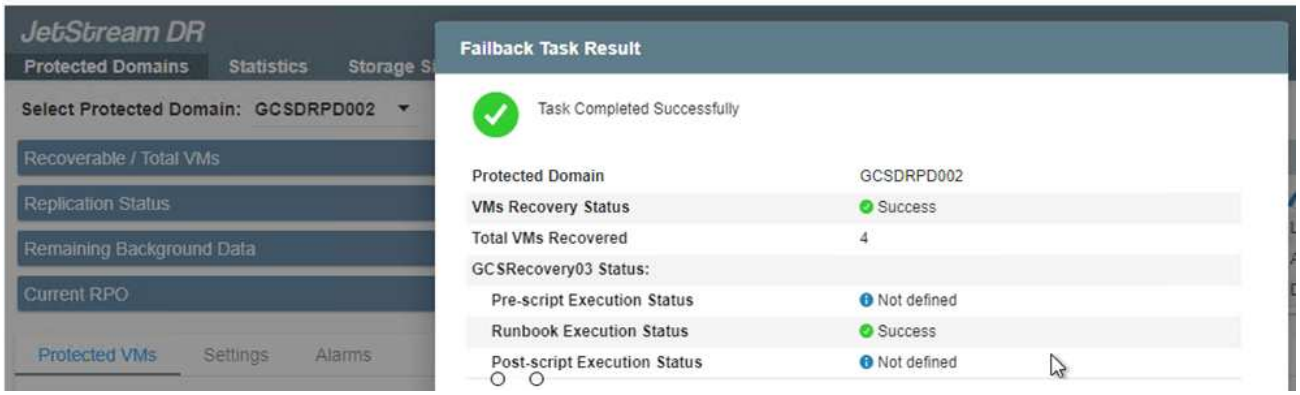
CPT によって生成されたフェイルバック プランは、VM とそのデータをオブジェクト ストアから元の VMware 環境に戻す作業を開始するためにも使用できます。



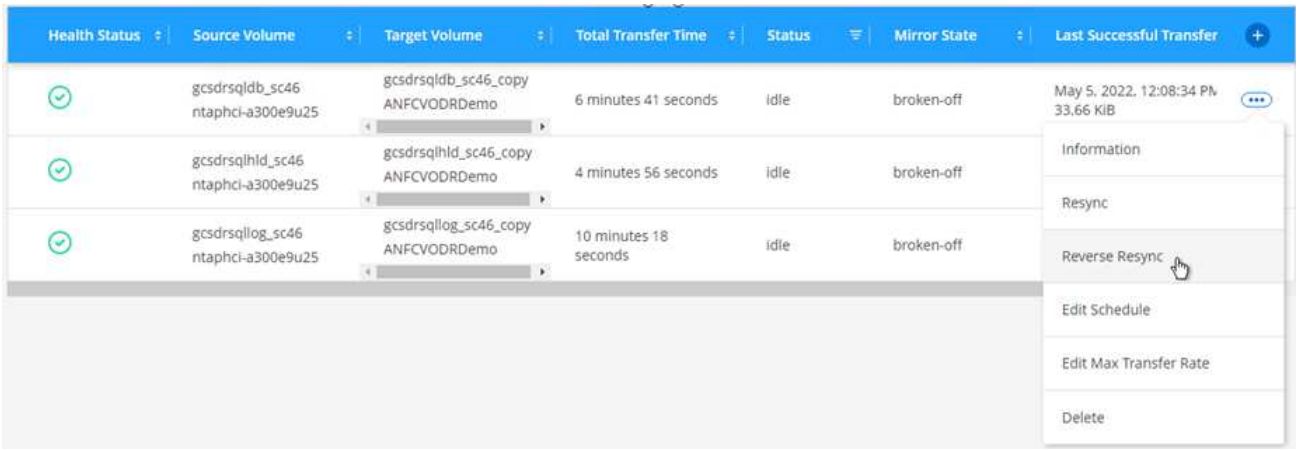
リカバリ サイトで VM を一時停止し、保護サイトで再起動した後の最大遅延を指定します。このプロセスを完了するために必要な時間には、フェールオーバー VM を停止した後のレプリケーションの完了、リカバリ サイトのクリーンアップに必要な時間、保護されたサイトで VM を再作成するために必要な時間が含まれます。 NetApp10 分を推奨します。

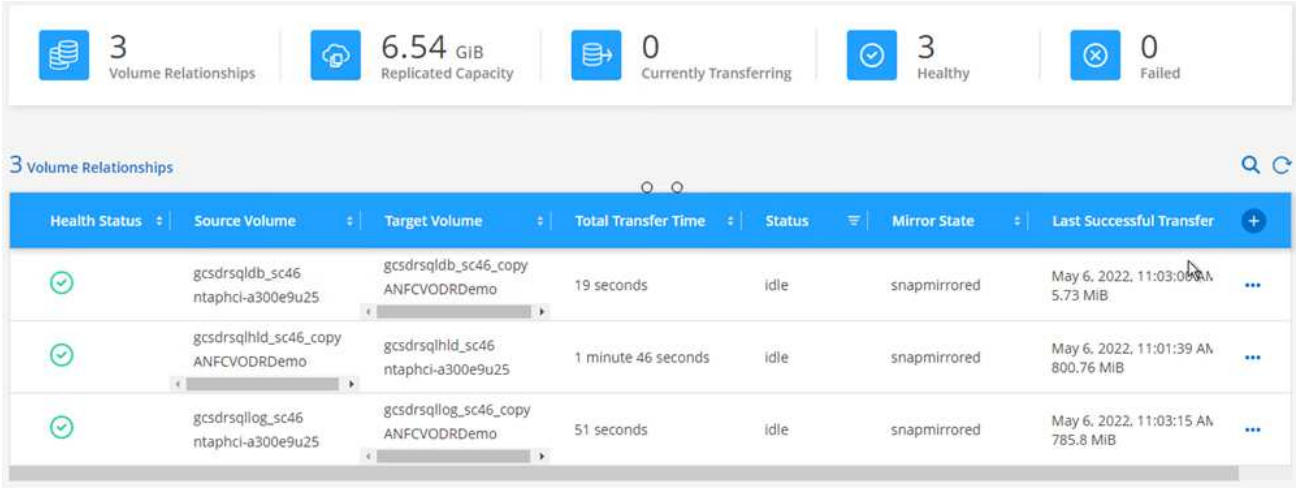


3. フェイルバック プロセスを完了し、VM 保護とデータの一貫性の再開を確認します。

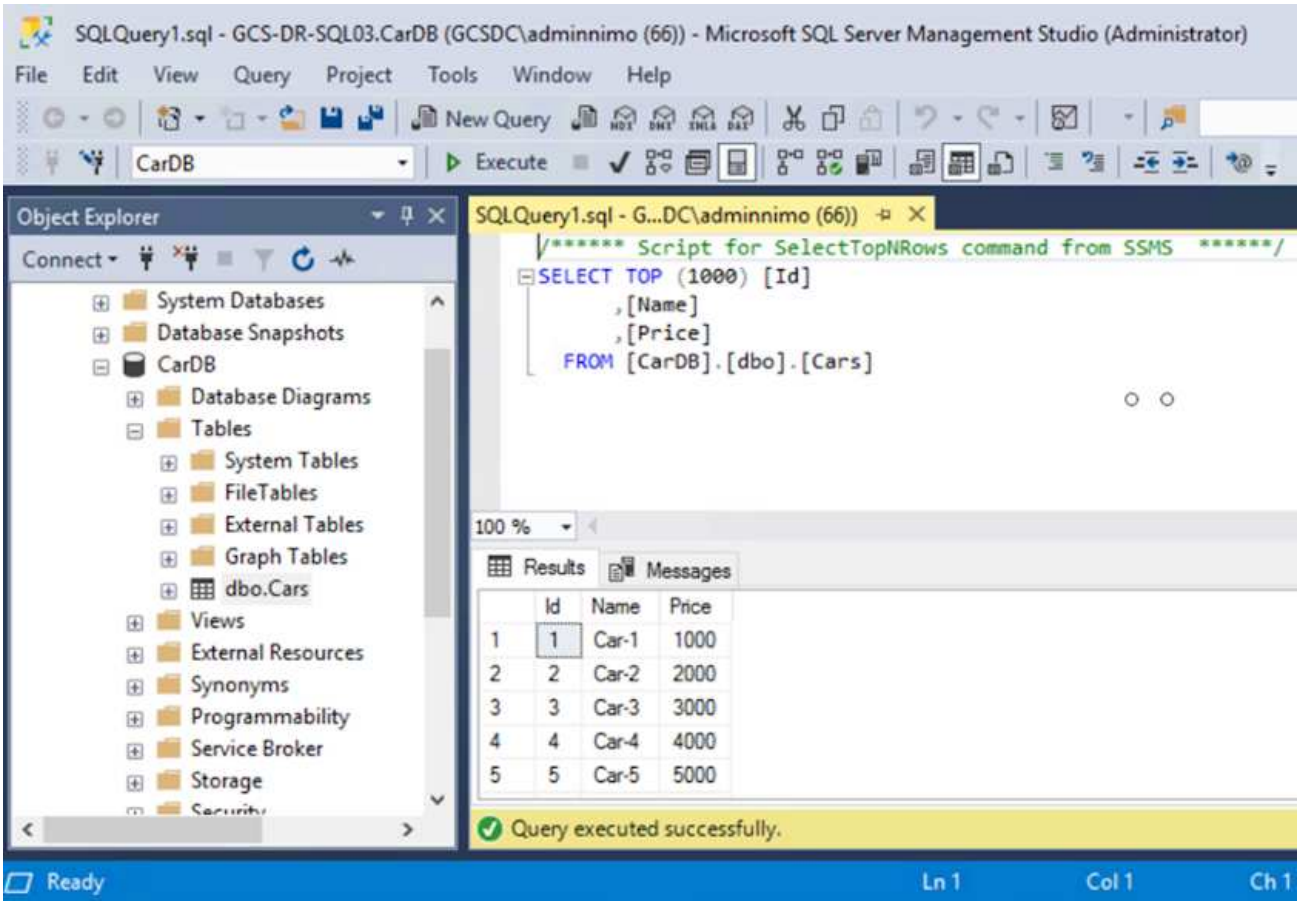


4. VM が回復したら、セカンダリ ストレージをホストから切断し、プライマリ ストレージに接続します。





5. MSSQL サーバー 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たことを確認します。



プライマリ ストレージにフェイルバックするには、逆再同期操作を実行して、関係の方向がフェイルオーバー前と同じであることを確認します。

逆再同期操作後にプライマリ ストレージとセカンダリ ストレージの役割を保持するには、逆再同期操作を再度実行します。

このプロセスは、Oracle、同様のデータベース フレーバー、ゲスト接続ストレージを使用するその他のア

プリケーションなどにも適用できます。

いつものように、重要なワークロードを本番環境に移行する前に、その回復に必要な手順をテストします。

このソリューションの利点

- SnapMirrorの効率的で復元力のあるレプリケーションを使用します。
- ONTAPスナップショット保持を使用して、利用可能な任意の時点に回復します。
- 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手順から、数百から数千の VM を復旧するために必要なすべての手順を完全に自動化できます。
- SnapCenter は、複製されたボリュームを変更しないクローン作成メカニズムを使用します。
  - これにより、ボリュームとスナップショットのデータ破損のリスクを回避できます。
  - 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/テスト、セキュリティ テスト、パッチおよびアップグレード テスト、修復テストなど、DR 以外のワークフローに DR データを活用します。
- CPU と RAM の最適化により、より小規模なコンピューティング クラスターへのリカバリが可能になり、クラウド コストを削減できます。

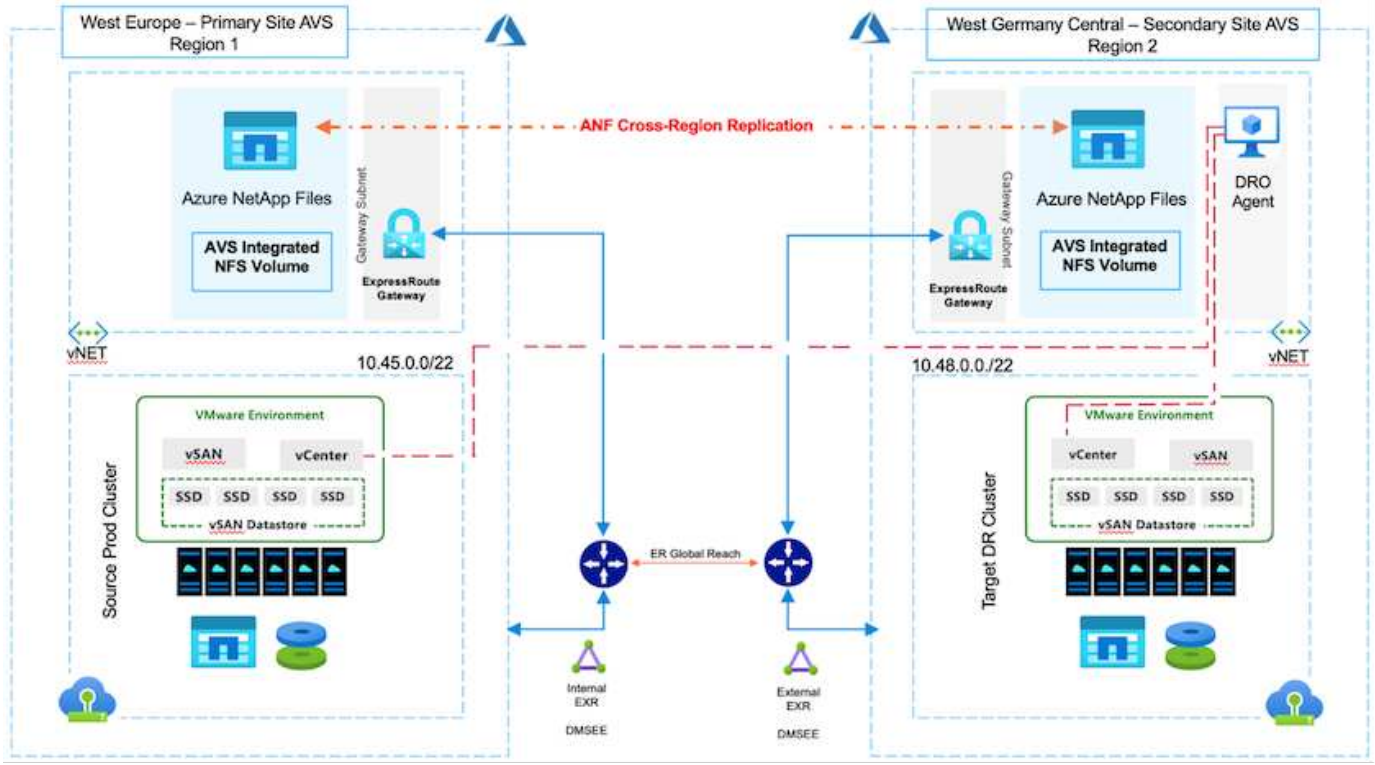
TR-4955: Azure NetApp Files (ANF) と **Azure VMware Solution (AVS)** を使用した災害復旧

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する災害復旧は、サイトの停止やデータ破損イベント (ランサムウェアなど) からワークロードを保護する、回復力がありコスト効率に優れた方法です。

概要

Azure NetAppファイル (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、プライマリ AVS サイトで NFS データストアとして Azure NetAppファイル ボリュームを使用している Azure VMware Solution (AVS) SDDC サイトで実行されている VMware ワークロードを、ターゲット回復リージョン内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 オーケストレータ (DRO) (UI を備えたスクリプト ソリューション) を使用すると、ある AVS SDDC から別の AVS SDDC 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。 DRO は、レプリケーション ピアリングを切断し、宛先ボリュームをデータストアとしてマウントし、AVS への VM 登録を通じて NSX-T (すべての AVS プライベート クラウドに含まれています) 上のネットワーク マッピングに直接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。見る "Azure NetApp Filesのボリューム レプリケーションを作成する"。
- ソースとターゲットの Azure VMware Solution プライベート クラウド間に ExpressRoute Global Reach を構成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。
- プライマリ AVS サイトからセカンダリ AVS サイトへのトポロジがサポートされています。
- 設定する "複製"ビジネスニーズとデータ変更率に基づいて、各ボリュームのスケジュールを適切に設定します。

カスケードおよびファンイン/ファンアウト トポロジはサポートされていません。

開始

Azure VMware ソリューションをデプロイする

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

AzureでAVSプライベートクラウドを構成するには、次の手順に従ってください。"リンク" NetAppのドキュメ

ントとこの "リンク"Microsoft ドキュメント。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 の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は、スケールアウトしてより多くのホストを生成し、負荷の大部分を処理できます。

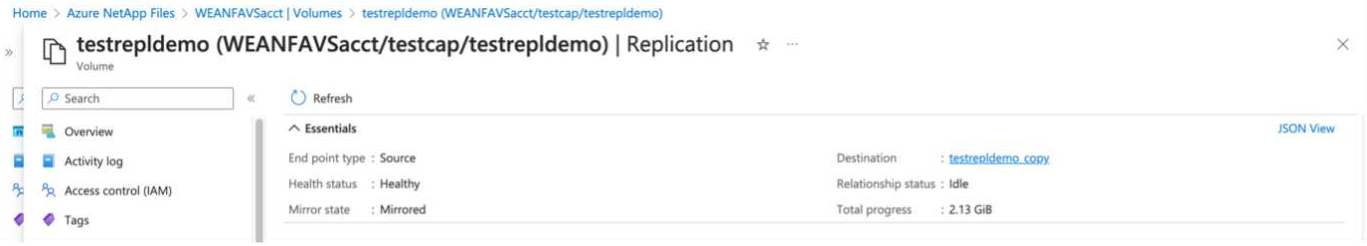
最初のリリースでは、DRO は既存の AVS SDDC クラスターをサポートします。オンデマンド SDDC 作成は、今後のリリースで利用可能になります。

Azure NetApp Files のプロビジョニングと構成

"Azure NetApp Files"は、高性能でエンタープライズ クラスの従量制ファイル ストレージ サービスです。この手順に従ってください "リンク"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構成し、AVS プライベート クラウドの展開を最適化します。

Azure NetApp Filesを利用したデータストア ボリュームのボリューム レプリケーションを作成する

最初のステップは、適切な頻度と保持期間で、AVS プライマリ サイトから AVS セカンダリ サイトへの目的のデータストア ボリュームのクロスリージョン レプリケーションを設定することです。



こ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します。宛先容量プールのサービス レベルは、ソース容量プールのサービス レベルと一致できます。ただし、この特定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、 "サービスレベルを変更する"実際の災害や DR シミュレーションの場合に使用します。

リージョン間のレプリケーション関係は前提条件であり、事前に作成する必要があります。

DROのインストール

DRO を開始するには、指定された 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。
- ソースと宛先の 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 名を使用している場合は、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
- Docker-compose
- JqChange `docker.sock`この新しい権限に： `sudo chmod 666 /var/run/docker.sock`。

その `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. 指定され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。

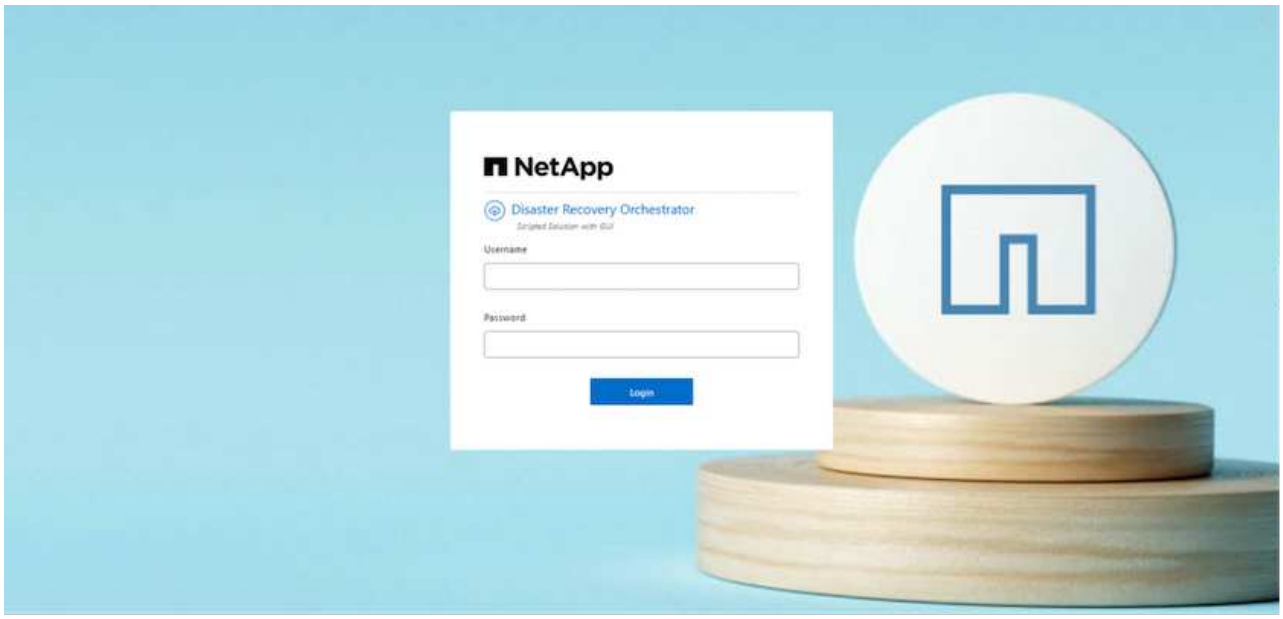
```
git clone https://github.com/NetApp/DRO-Azure.git
```

エージェントは、セカンダリ AVS サイト リージョンまたは SDDC とは別の AZ 内のプライマリ AVS サイト リージョン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、デプロイメントスクリプトを実行して、ホストIPを入力します（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. 次の資格情報を使用して UI にアクセスします。
   - ユーザー名: `admin`
   - パスワード： `admin`



DRO構成

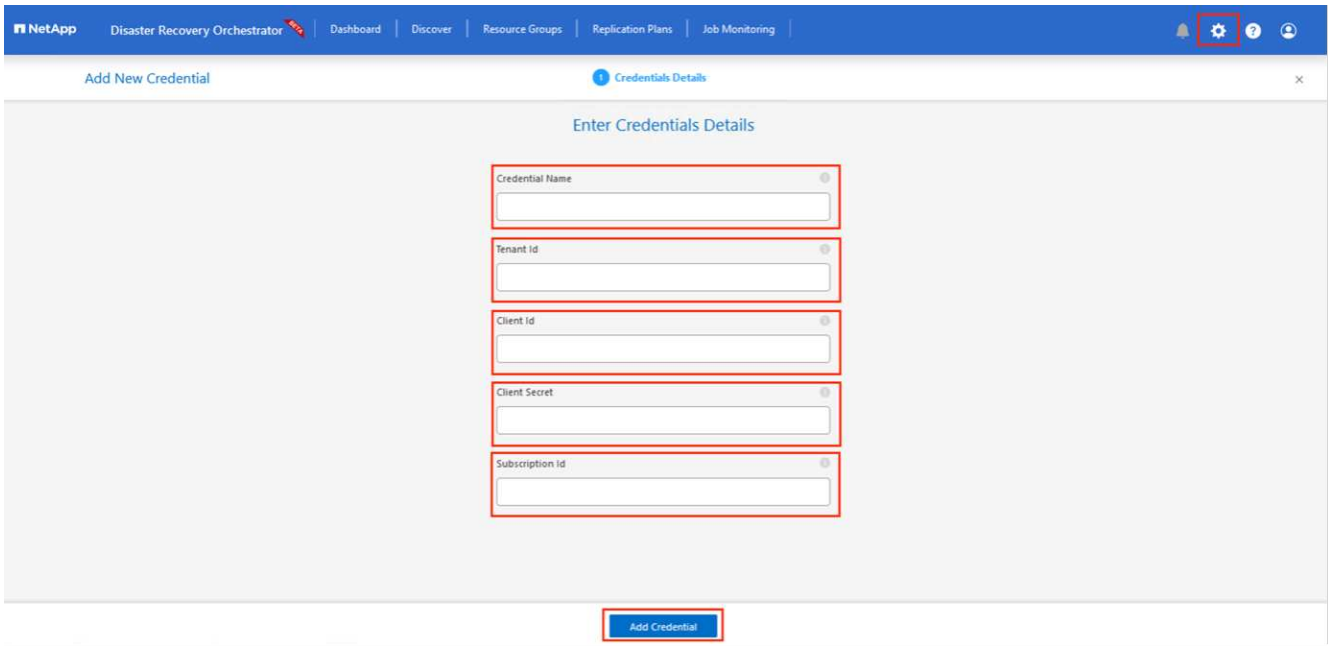
Azure NetApp Filesと AVS が適切に構成されたら、プライマリ AVS サイトからセカンダリ AVS サイトへのワークロードの回復を自動化するための DRO の構成を開始できます。 NetApp、DRO エージェントをセカンダリ AVS サイトに展開し、ExpressRoute ゲートウェイ接続を構成して、DRO エージェントが適切な AVS およびAzure NetApp Filesコンポーネントとネットワーク経由で通信できるようにすることをお勧めします。

最初のステップは資格情報を追加することです。 DRO には、Azure NetApp Filesと Azure VMware Solution を検出するためのアクセス許可が必要です。 Azure Active Directory (AD) アプリケーションを作成して設定し、DRO に必要な Azure 資格情報を取得することで、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、関連する必要なアクセス許可を持つカスタム ロールを割り当てる必要があります。ソース環境と宛先環境を追加すると、サービス プリンシパルに関連付けられている資格情報を選択するように求められます。 「新しいサイトの追加」をクリックする前に、これらの資格情報を DRO に追加する必要があります。

この操作を実行するには、次の手順を実行します。

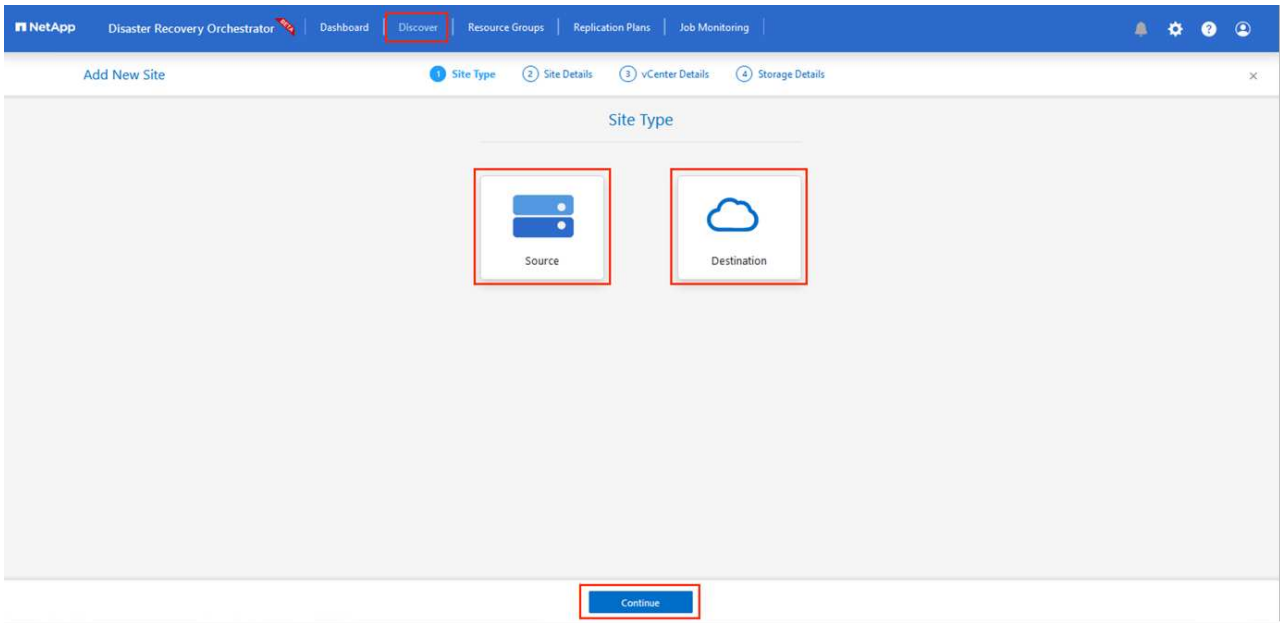
1. サポートされているブラウザでDROを開き、デフォルトのユーザー名とパスワードを使用します。 `/admin/admin` ）。最初のログイン後に、「パスワードの変更」オプションを使用してパスワードをリセットできます。
2. DRO コンソールの右上にある 設定 アイコンをクリックし、資格情報 を選択します。
3. 「新しい資格情報の追加」をクリックし、ウィザードの手順に従います。
4. 資格情報を定義するには、必要なアクセス許可を付与する Azure Active Directory サービス プリンシパルに関する情報を入力します。
   - 資格情報名
   - テナントID
   - クライアントID
   - Client secret
   - サブスクリプション ID

     AD アプリケーションを作成したときに、この情報を取得しておく必要があります。
5. 新しい資格情報の詳細を確認し、「資格情報の追加」をクリックします。



資格情報を追加したら、プライマリおよびセカンダリ AVS サイト (vCenter と Azure NetAppファイル 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。ソースサイトと宛先サイトを追加するには、次の手順を実行します。

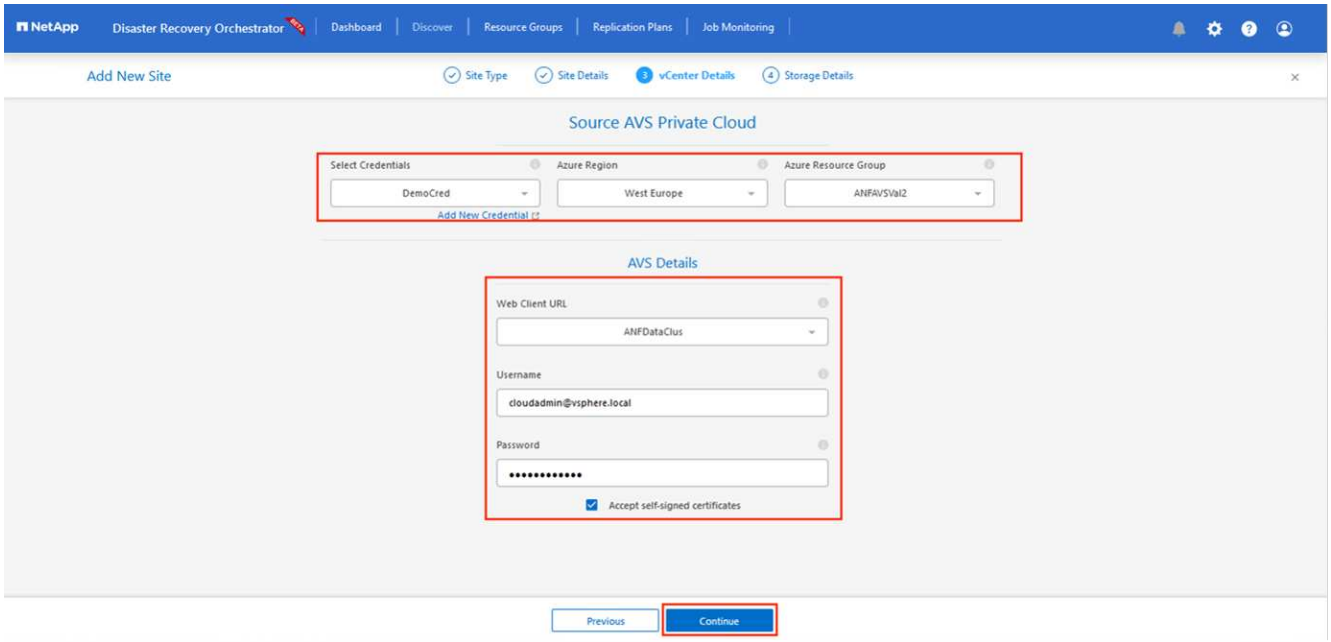
6. *Discover*タブに移動します。
7. *新しいサイトを追加*をクリックします。
8. 次のプライマリ AVS サイトを追加します (コンソールでは ソース として指定されます)。
   - SDDC vCenter
   - Azure NetApp Filesストレージ アカウント
9. 次のセカンダリ AVS サイトを追加します (コンソールで **Destination** として指定)。
   - SDDC vCenter
   - Azure NetApp Filesストレージ アカウント



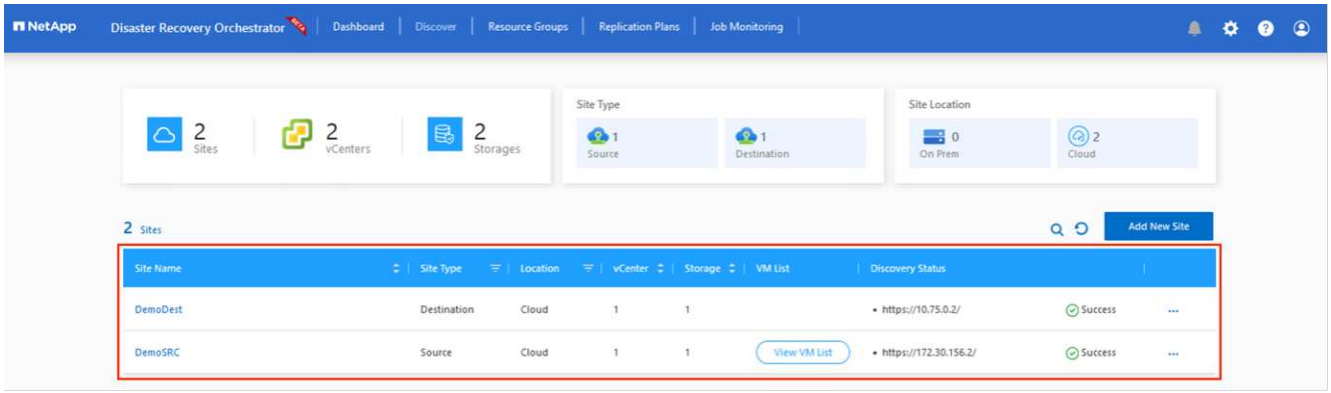
10. ソース をクリックし、わかりやすいサイト名を入力してコネクタを選択し、サイトの詳細を追加します。次に、[続行] をクリックします。

> このドキュメントでは、デモンストレーションの目的で、ソース サイトの追加について説明します。

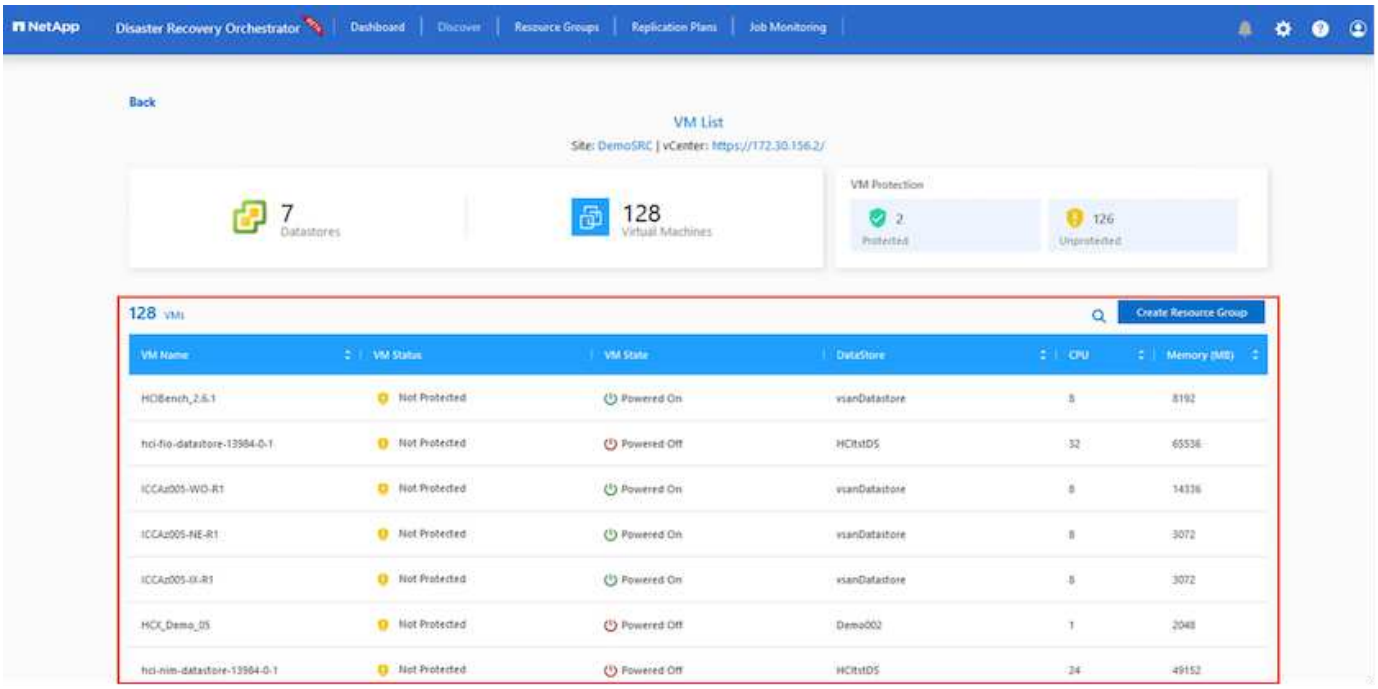
11. vCenter の詳細を更新します。これを行うには、プライマリ AVS SDDC のドロップダウンから資格情報、Azure リージョン、リソース グループを選択します。
12. DRO には、リージョン内で利用可能なすべての SDDC が一覧表示されます。ドロップダウンから指定されたプライベート クラウド URL を選択します。
13. 入力してください `cloudadmin@vsphere.local`ユーザー資格情報。 Azure Portal からアクセスできます。この手順に従う "リンク"。完了したら、[続行] をクリックします。



14. Azure リソース グループとNetAppアカウントを選択して、ソース 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 サイトから宛先サイトへの対応するクロスリージョン レプリカを持つ VM を表示します。 DRO は、VM が使用するネットワークとセグメントを自動的に検出し、それらを入力します。



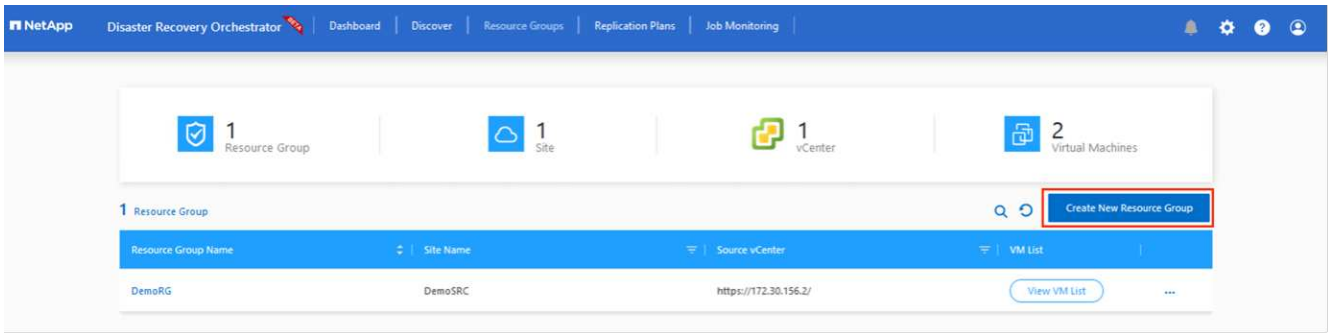
次のステップは、必要な VM をリソース グループとして機能グループにグループ化することです。

リソースのグループ化

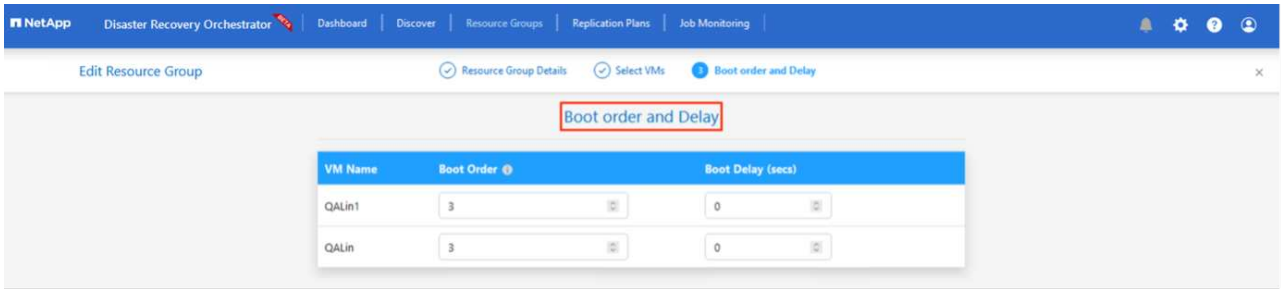
プラットフォームを追加したら、回復する VM をリソース グループにグループ化します。 DRO リソース グループを使用すると、依存する VM のセットを、ブート順序、ブート遅延、および回復時に実行できるオプションのアプリケーション検証を含む論理グループにグループ化できます。

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。

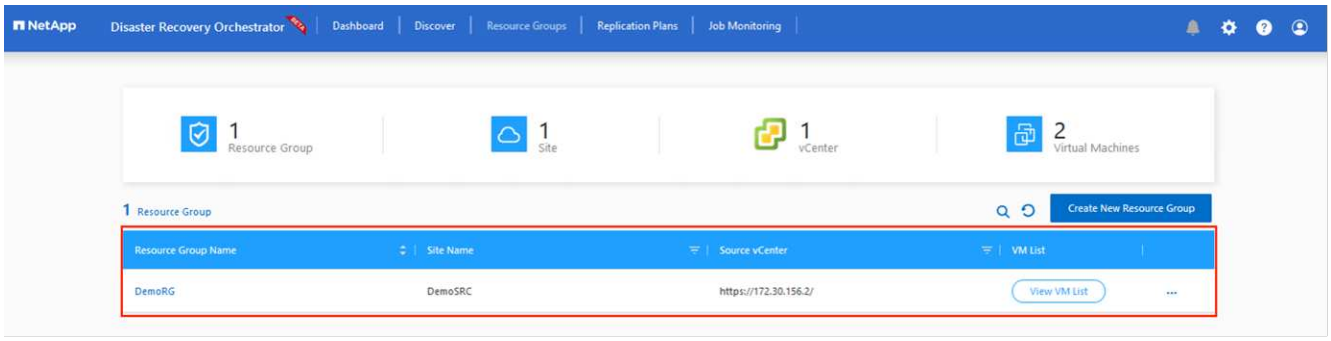
1. *リソース グループ*にアクセスし、*新しいリソース グループの作成*をクリックします。



2. [新しいリソース グループ] の下で、ドロップダウンからソース サイトを選択し、[作成] 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. 選択したすべての VM の ブート順序 と ブート遅延 (秒) を選択します。各仮想マシンを選択し、その優先順位を設定することで、電源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。
   - 最初に電源を入れる仮想マシン
   - デフォルト
   - 最後に電源をオンにした仮想マシン



6. *リソース グループの作成*をクリックします。



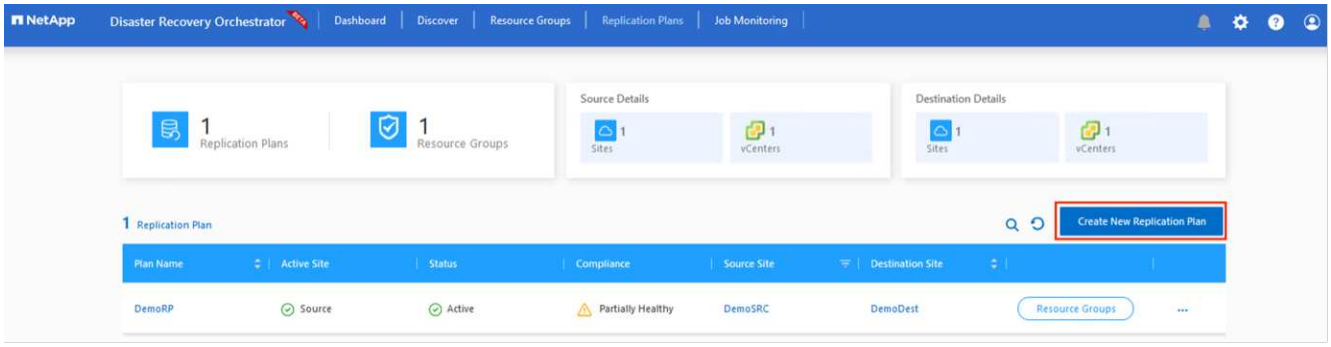
レプリケーションプラン

災害が発生した場合にアプリケーションを回復するための計画が必要です。ドロップダウンからソースとターゲットの 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復元してパワーオンする方法のグループ化も含めます (たとえば、ドメイン コントローラ、Tier-1、Tier-2 など)。計画は青写真とも呼ばれることがあります。リカバリ プランを定義するには、[レ

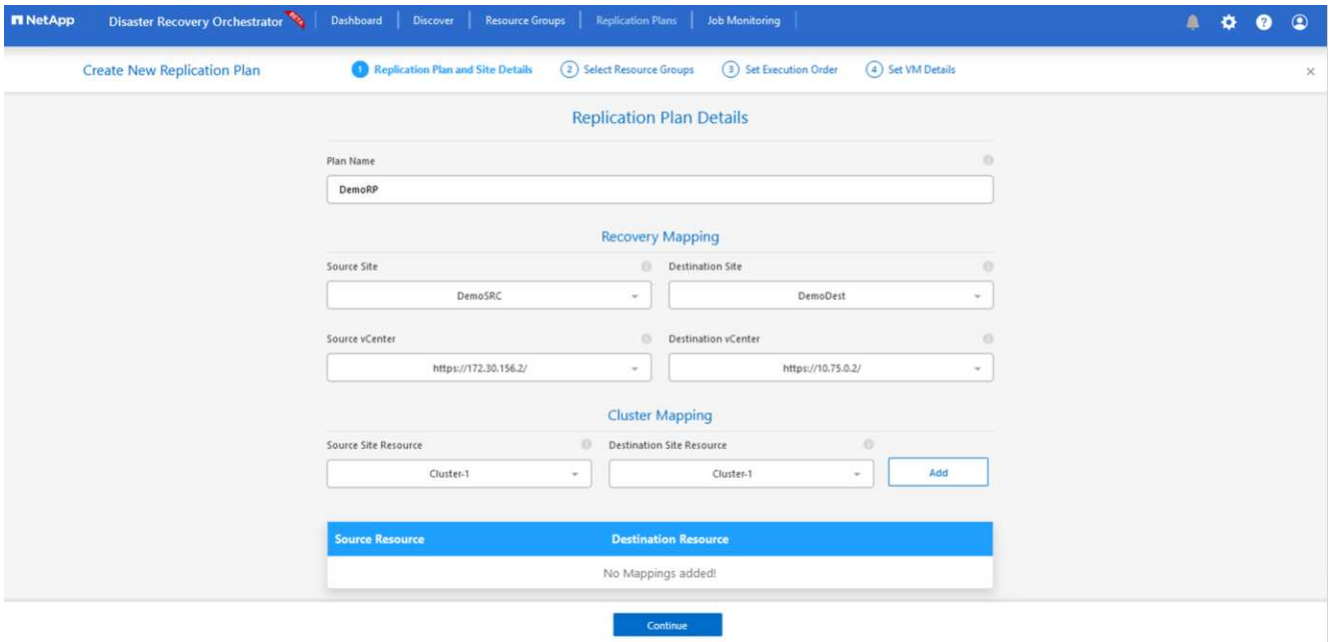
プリケーション プラン] タブに移動し、[新しいレプリケーション プラン] をクリックします。

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。

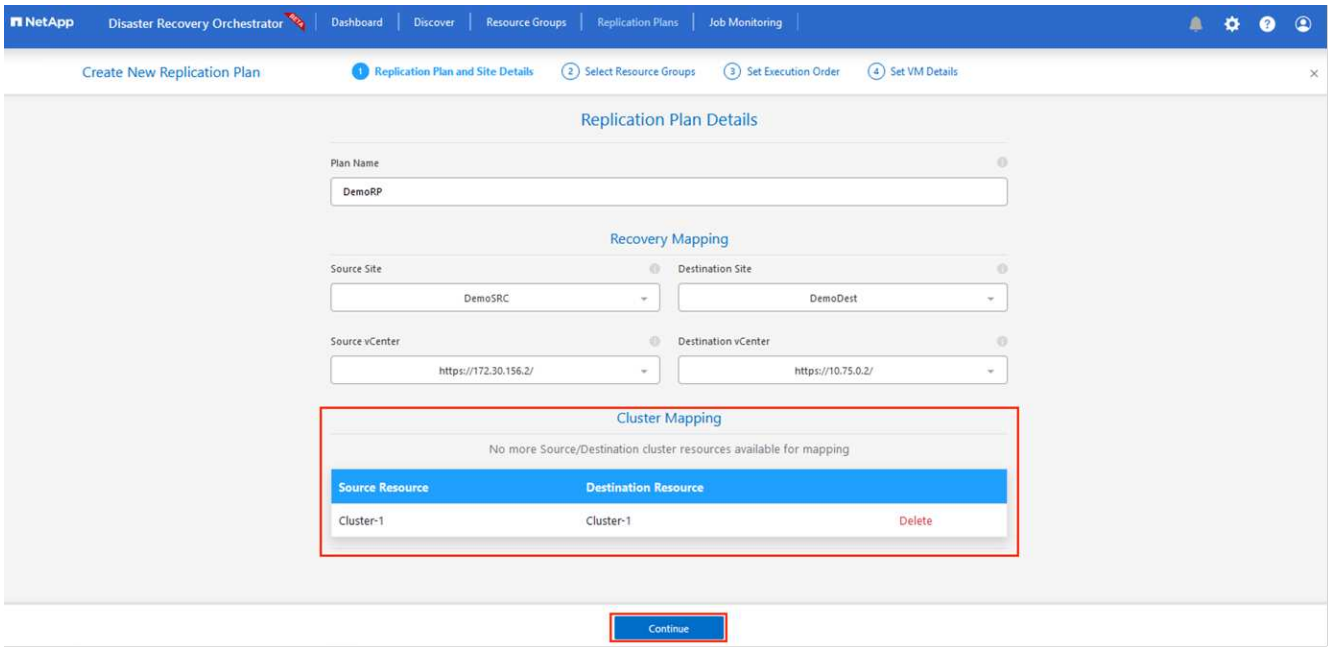
1. レプリケーション プラン に移動し、新しいレプリケーション プランの作成 をクリックします。



2. 新しいレプリケーション プラン で、プランの名前を指定し、ソース サイト、関連する vCenter、宛先サイト、および関連する vCenter を選択してリカバリ マッピングを追加します。

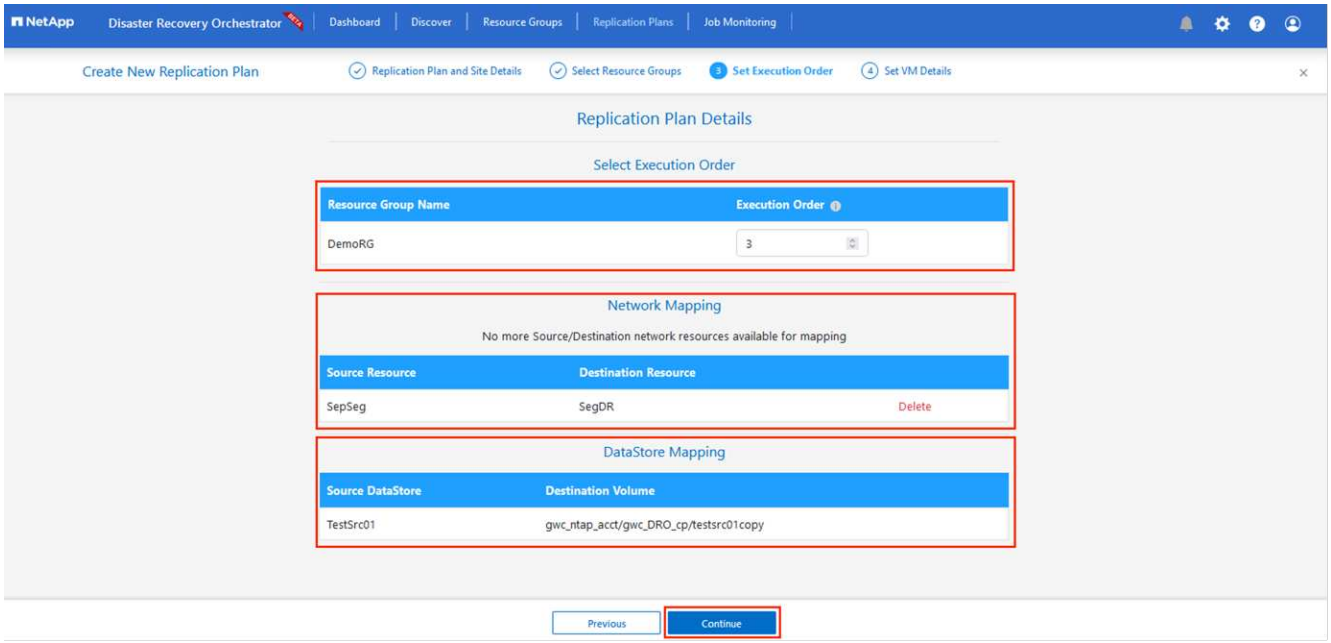


3. リカバリ マッピングが完了したら、クラスター マッピング を選択します。

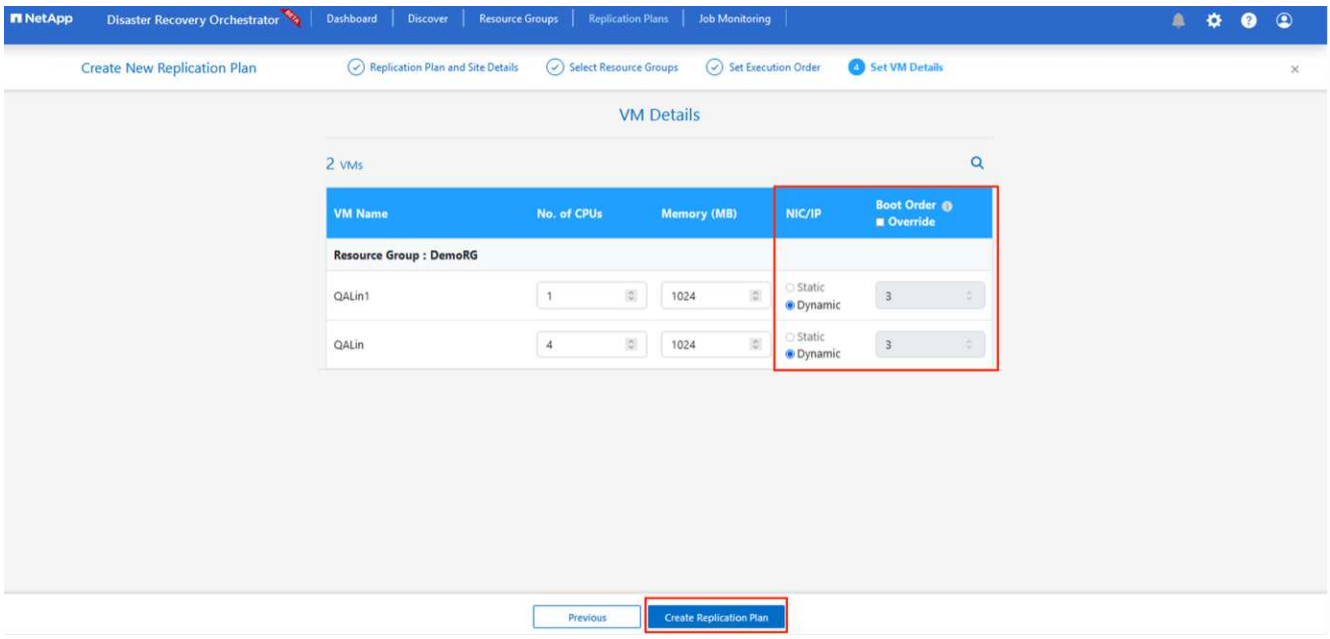


4. *リソース グループの詳細*を選択し、*続行*をクリックします。
5. リソース グループの実行順序を設定します。このオプションを使用すると、複数のリソース グループが存在する場合に操作のシーケンスを選択できます。
6. 完了したら、ネットワーク マッピングを適切なセグメントに設定します。セグメントはすでにセカンダリ AVS クラスターにプロビジョニングされているはずなので、VM をそれらにマップするには適切なセグメントを選択します。
7. データストア マッピングは、VM の選択に基づいて自動的に選択されます。

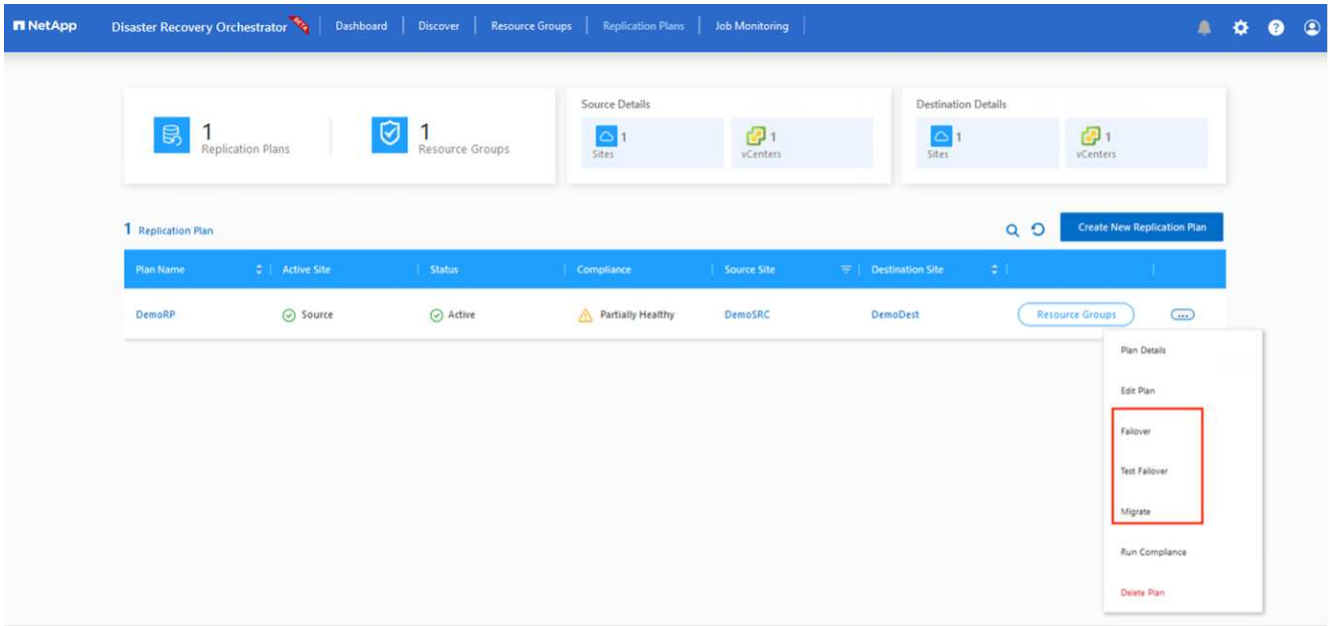
クロスリージョンレプリケーション (CRR) はボリューム レベルで行われます。したがって、それぞれのボリュームに存在するすべての VM が CRR の宛先に複製されます。レプリケーション プランの一部である仮想マシンのみが処理されるため、データストアの一部であるすべての仮想マシンを選択してください。



8. VM の詳細では、オプションで VM の CPU および 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 クラスター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 テストを実施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内容を変更する必要がある場合は、ブート順序を変更するための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ブート順序が使用されますが、この段階で変更を実行することもできます。

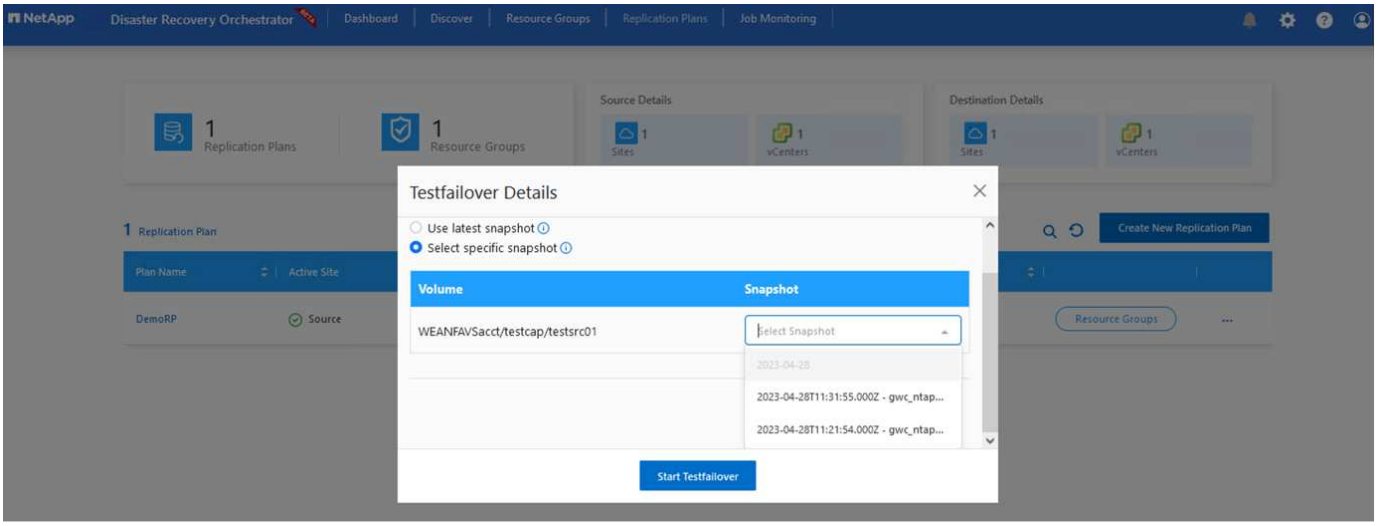


9. *レプリケーション プランの作成*をクリックします。レプリケーション プランが作成されたら、要件に応じてフェールオーバーを実行したり、フェールオーバーをテストしたり、オプションを移行したりできます。

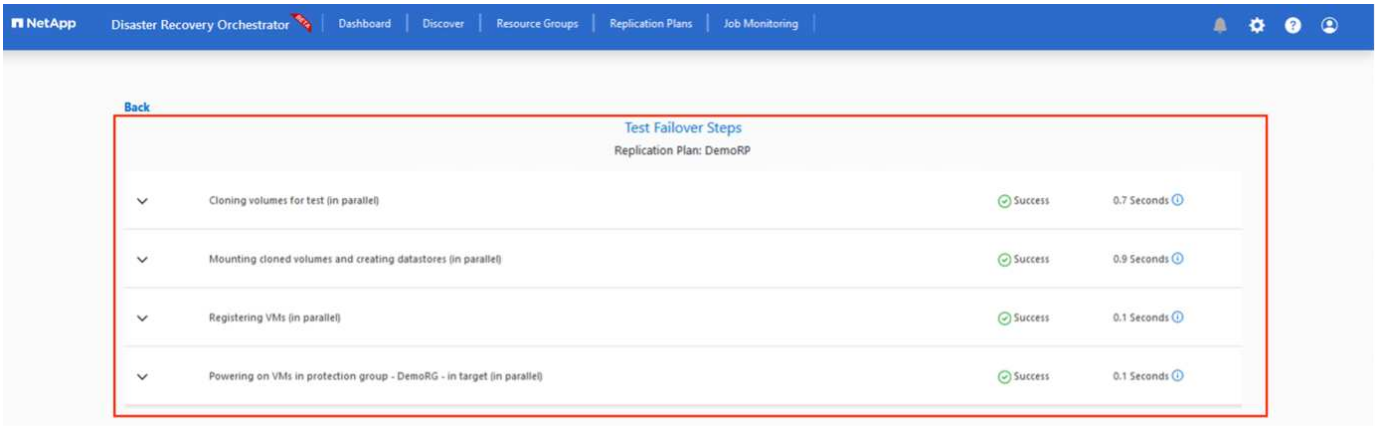


フェールオーバーおよびテスト フェールオーバーのオプションでは、最新のスナップショットが使用されるか、または特定の時点のスナップショットから特定のスナップショットを選択することもできます。最新のレプリカがすでに侵害または暗号化されているランサムウェアなどの破損イベントに直面している場合、ポイン

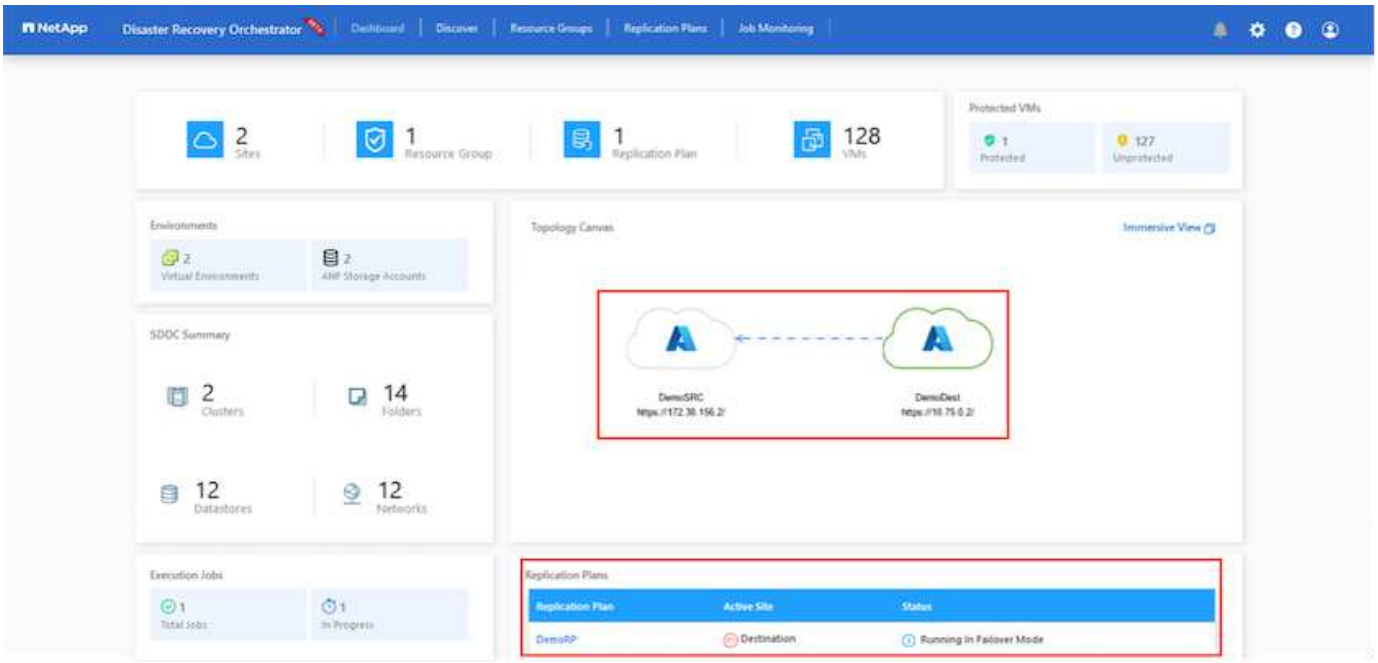
トインタイム オプションは非常に役立ちます。 DRO は利用可能なすべての時点を表示します。



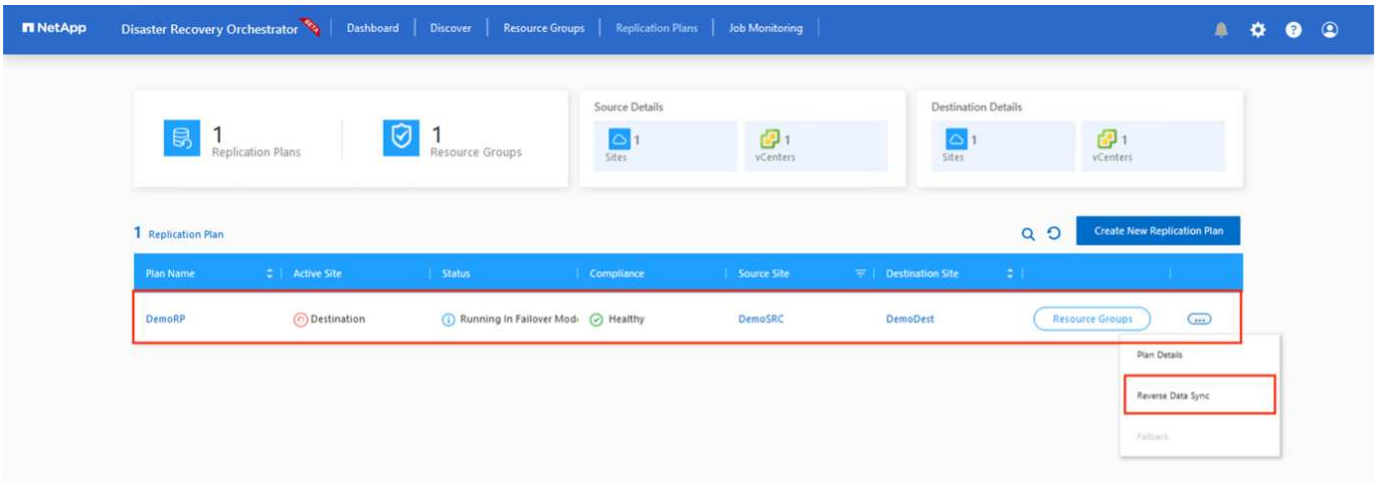
レプリケーション プランで指定された構成でフェイルオーバーをトリガーするか、フェイルオーバーをテストするには、フェイルオーバー または フェイルオーバーのテスト をクリックします。タスク メニューでレプリケーション プランを監視できます。



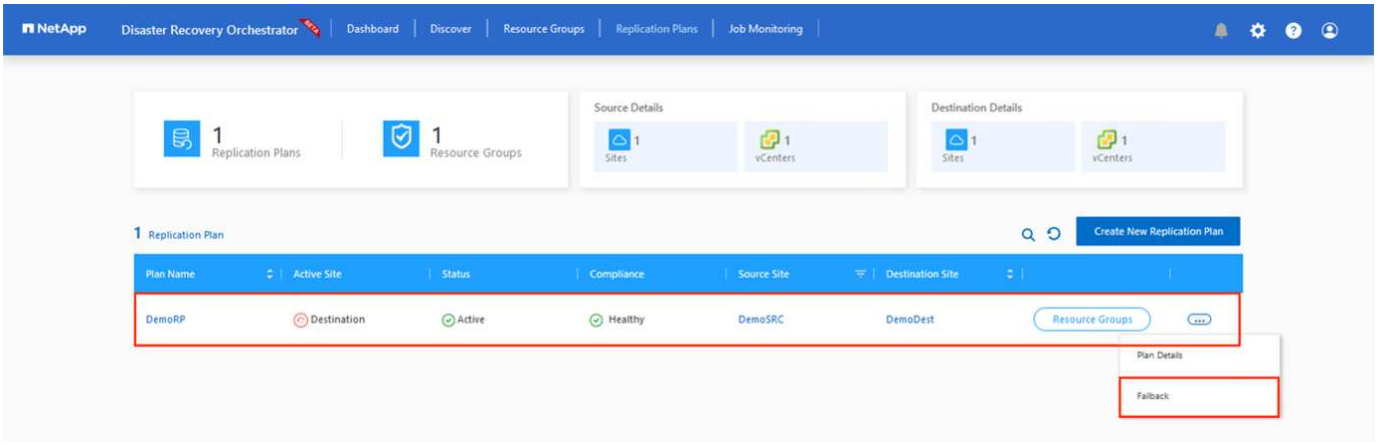
フェイルオーバーがトリガーされると、回復されたアイテムがセカンダリ サイトの AVS SDDC vCenter (VM、ネットワーク、データストア) に表示されます。デフォルトでは、VM はワークロード フォルダーに回復されます。

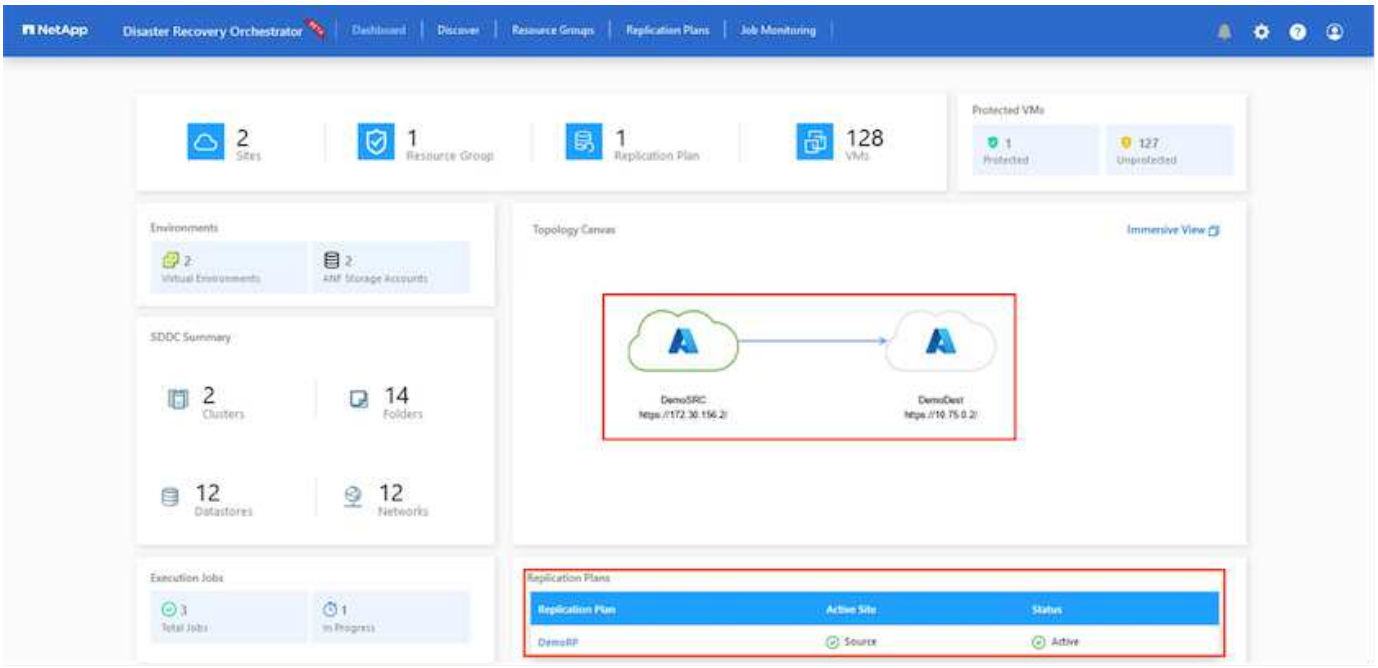


フェイルバックはレプリケーション プラン レベルでトリガーできます。テストフェイルオーバーの場合、ティアダウン オプションを使用して変更をロールバックし、新しく作成されたボリュームを削除できます。フェイルオーバーに関連するフェイルバックは 2 段階のプロセスです。レプリケーション プランを選択し、逆データ同期 を選択します。



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プされた適切なボリュームのレプリケーションの正常性が失わ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 は宛先ボリュームまたはレプリカ ボリュームをマップしません。代わりに、必要なリージョン間レプリケーション スナップショット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。これにより、容量プールから追加の物理容量が消費され、ソース ボリュームが変更されないようになります。特に、レプリケーション ジョブは DR テスト中またはトリアージ ワークフロー中でも継続できます。さらに、このプロセスにより、エラーが発生したり破損したデータが回復されたりした場合にレプリカが破壊されるリスクなしに、回復をクリーンアップできるようになります。

ランサムウェアからの回復

ランサムウェアからの回復は困難な作業になる可能性があります。具体的には、IT 組織にとって、安全な復帰ポイントがどこなのかを正確に特定することが困難になる可能性があり、また、それが決定された後、回復したワークロードが再発する攻撃 (たとえば、休眠中のマルウェアや脆弱なアプリケーションによるもの) から確実に保護されるようにする方法も困難になります。

DRO は、組織が利用可能な任意の時点から回復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的でありながら分離されたネットワークに回復され、アプリケーションは機能し相互に通信できるようになりますが、南北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 チームは安全な場所でフォレンジックを実施し、隠れたマルウェアや潜伏中のマルウェアを特定できるように

なります。

まとめ

Azure NetApp Filesと Azure VMware ディザスター リカバリー ソリューションには、次の利点があります。

- 効率的で回復力のあるAzure NetApp Files のリージョン間レプリケーションを活用します。
- スナップショット保持により、利用可能な任意の時点に回復します。
- 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手順から数百から数千の VM を回復するために必要なすべての手順を完全に自動化します。
- ワークロードのリカバリでは、複製されたボリュームを操作しない「最新のスナップショットから新しいボリュームを作成する」プロセスが活用されます。
- ボリュームまたはスナップショット上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/テスト、セキュリティ テスト、パッチおよびアップグレード テスト、修復テストなど、DR 以外のワークフローに DR データとクラウド コンピューティング リソースを活用します。
- CPU と RAM の最適化により、より小規模なコンピューティング クラスターへのリカバリが可能になり、クラウド コストを削減できます。

詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、次のドキュメントや 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する

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Azure NetApp Filesボリューム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 ソリューション"

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

- Azure に仮想化環境を展開して構成する

  "Azure で AVS をセットアップする"

- Azure VMware Solution のデプロイと構成

  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て **Azure VMware Solution** への災害復旧を行う

Azure NetApp Files (ANF) データストアは、ストレージをコンピューティングから分離

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。コンピューティング リソースとは独立して拡張できる、柔軟で高性能なストレージ インフラストラクチャを顧客に提供します。 Azure NetApp Filesデータストアは、オンプレミスの VMWare 環境のディザスター リカバリー サイトとして Azure VMware Solution (AVS) と連携して展開を簡素化および最適化します。

概要

Azure NetApp Files (ANF) ボリューム ベースの NFS データストアは、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 ソリューションを使用してオンプレミスからデータをレプリケートするために使用できます。 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ために膨大な数の ESXi ホストを備えた Azure VMware Solution SDDC を構築する場合と比較して、コストを最適化した展開が可能になります。このアプローチは「パイロット ライト クラスター」と呼ばれます。パイロット ライト クラスターは、 Azure NetApp Filesデータストアの容量と最小限の AVS ホスト構成 (3 つの AVS ノード) で構成されます。

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 クラスターは、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。フェイルオーバーが完了し、通常の運用が回復すると、パイロット ライト クラスターは低コストの運用モードにスケールダウンできます。

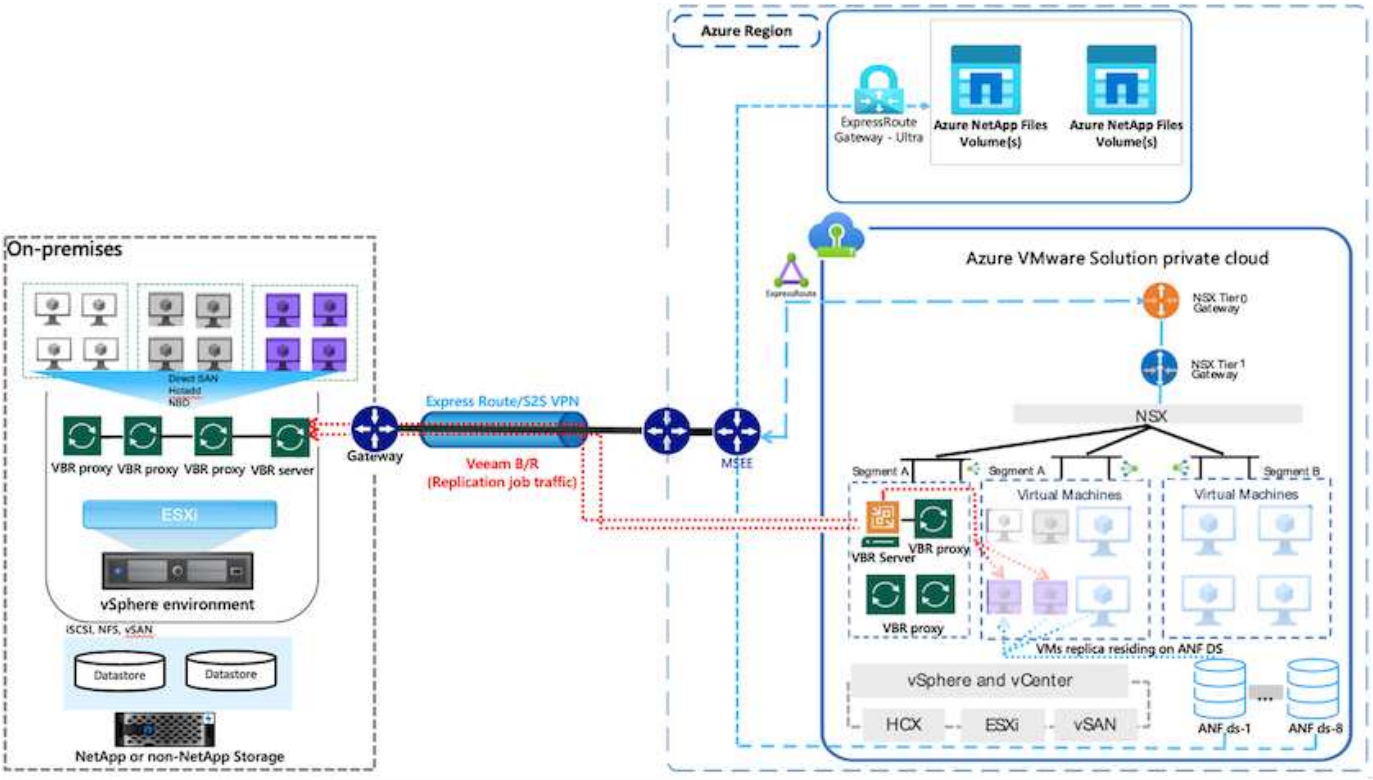
この文書の目的

この記事では、Veeam バックアップおよびレプリケーションを備えたAzure NetApp Filesデータストアを使用して、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 のディザスター リカバリーを (AVS) に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。仮想マシンが複製されると、Veeam Backup & Replication は AVS から複製され、ソフトウェアはターゲットの AVS SDDC クラスター上にネイティブ VMware vSphere 形式で仮想マシンの正確なコピーを作成します。 Veeam Backup & Replication は、コピーを元の VM と同期した状態に保ちます。レプリケーションでは、DR サイトに起動準備完了状態の VM のコピーがマウントされるため、最適な復旧時間目標 (RTO) が実現されます。

このレプリケーション メカニズムにより、災害発生時にワークロードを AVS SDDC で迅速に開始できるようになります。 Veeam Backup & Replication ソフトウェアは、WAN および低速接続を介したレプリケーションのトラフィック転送も最適化します。さらに、重複したデータ ブロック、ゼロ データ ブロック、スワップ ファイル、および「除外された VM ゲスト OS ファイル」も除外します。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するのを防ぐには、WAN アクセラレータとネットワーク スロットリング ルールを利用できます。

Veeam Backup & Replication のレプリケーション プロセスはジョブ駆動型であり、レプリケーション ジョブを構成することによってレプリケーションが実行されます。災害が発生した場合、フェイルオーバーをトリガーしてレプリカ コピーにフェイルオーバーすることで VM を復旧できます。フェイルオーバーが実行されると、複製された 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その既知の復元ポイントのいずれか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の回復や分離されたテストが可能になります。 Veeam Backup & Replication は、さまざまな災害復旧シナリオを処理するための複数のオプションを提供します。



ソリューションの展開

高レベルの手順

1. Veeam Backup and 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. "Azure VMware Solution (AVS) をデプロイする"プライベートクラウドと"Azure NetApp Filesデータストアを接続する"Azure VMware Solution ホストへ。

   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 の目的で使用できます。インシデント発生時には VM はこのクラスターにフェールオーバーされ、追加の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します。
5. 災害イベントが完了し、プライマリ サイトが稼働したら、本番環境の VM に切り替えます。

Veeam VM レプリケーションの **AVS** および **ANF** データストアへの前提条件

1. Veeam Backup & Replication バックアップ VM がソースとターゲットの AVS SDDC クラスターに接続されていることを確認します。
2. バックアップ サーバーは、短い名前を解決し、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データストアには、レプリケートされた VM の VMDK を格納するのに十分な空き領域が必要です。

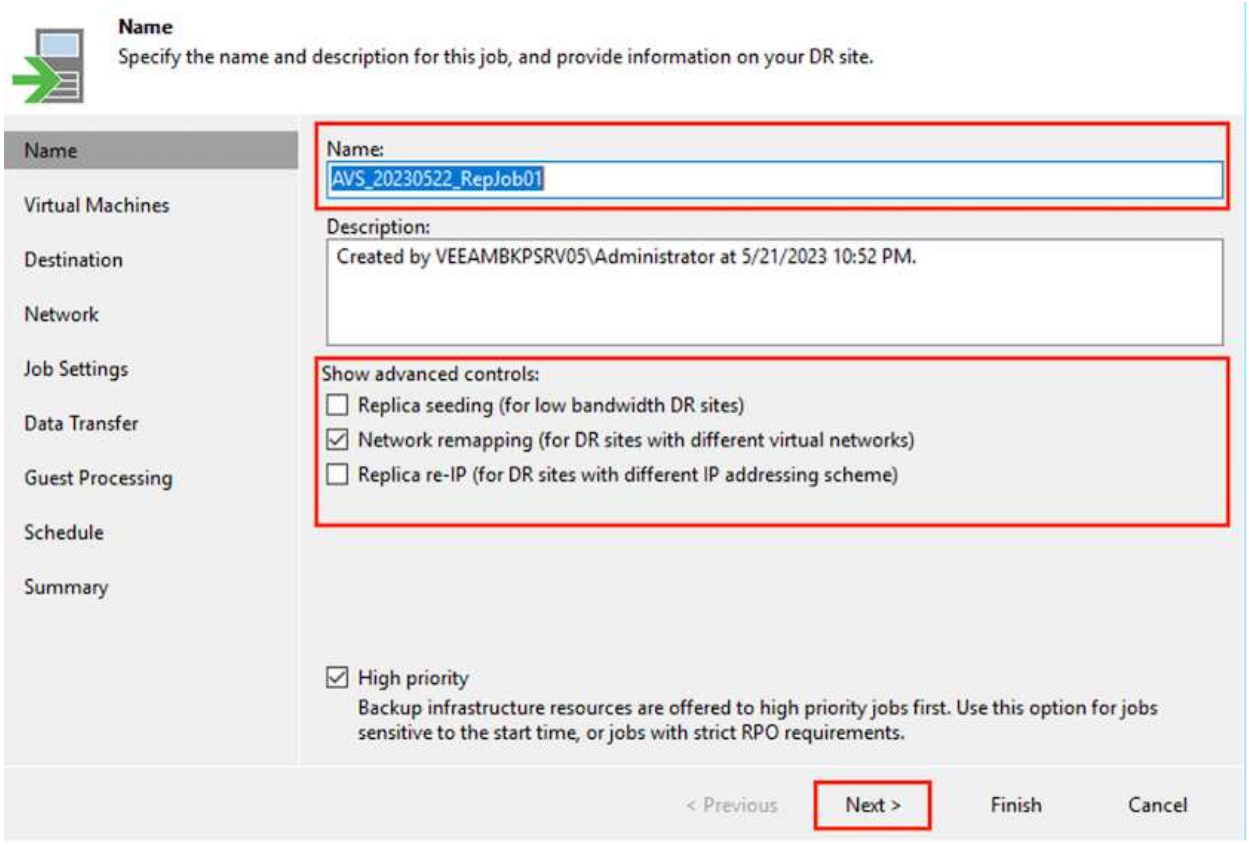
詳細については、「考慮事項と制限事項」を参照してください。"ここをクリックしてください。" 。

▼ ステップ**1: VM**を複製する

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、システム状態、構成、メタデータを含む VM の特定時点のコピーです。 Veeam Backup & Replication は、スナップショットをレプリケーションのデータ ソースとして使用します。

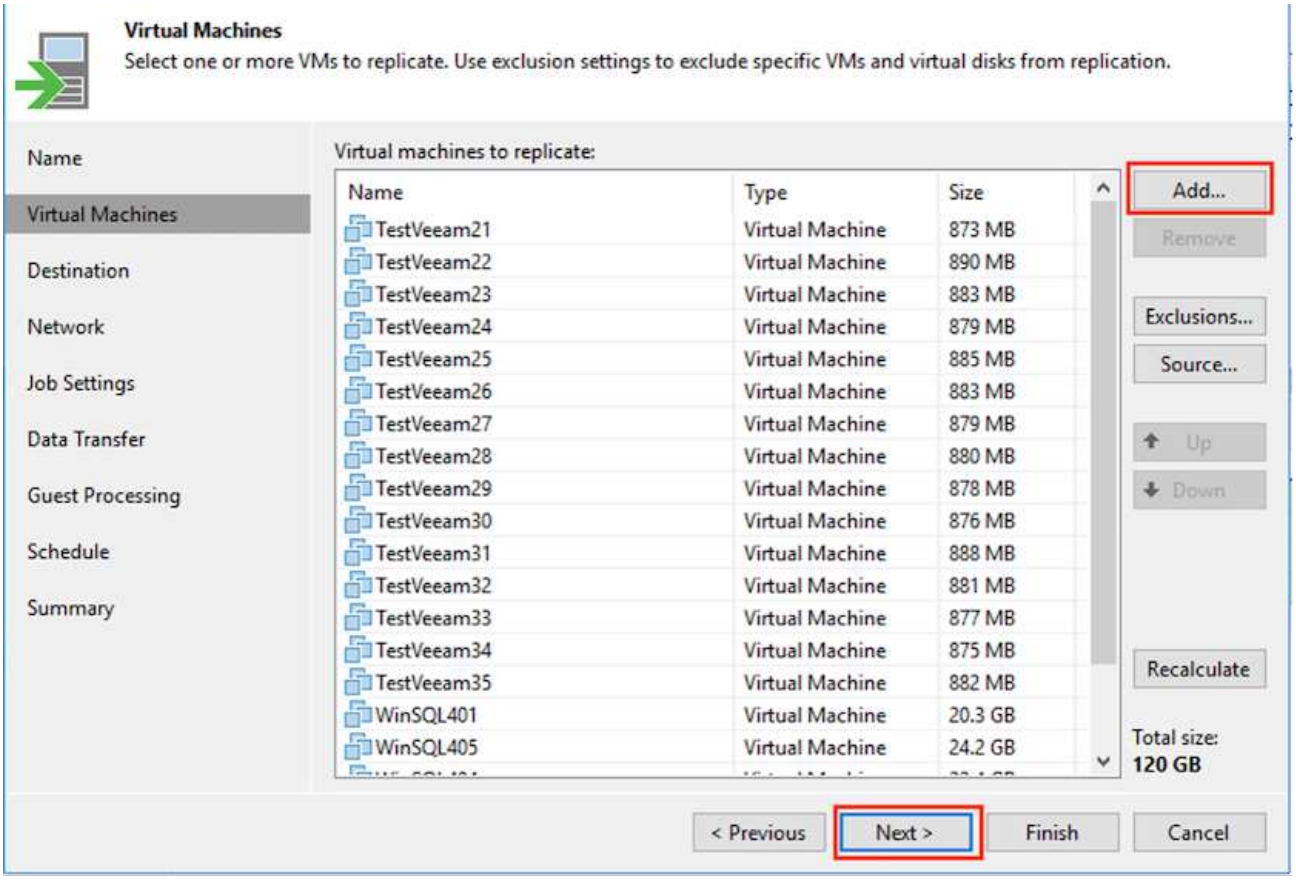
VM をレプリケートするには、次の手順に従います。

1. Veeam Backup & Replication コンソールを開きます。
2. ホームビューで。ジョブ ノードを右クリックし、レプリケーション ジョブ > 仮想マシンを選択します。
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。[Next]をクリックします。
   - オンプレミスと Azure 間の接続の帯域幅が制限されている場合は、[レプリカ シード] チェック ボックスをオンにします。 *Azure VMware Solution SDDC 上のセグメントがオンプレミスのサイト 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 (異なるネットワークを持つ AVS SDDC サイトの場合)] チェック ボックスをオンにします。
   - オンプレミスの運用サイトの IP アドレス指定スキームがターゲット AVS サイトのスキームと異なる場合は、[レプリカ再 IP (IP アドレス指定スキームが異なる DR サイト用)] チェック ボックスをオンにします。

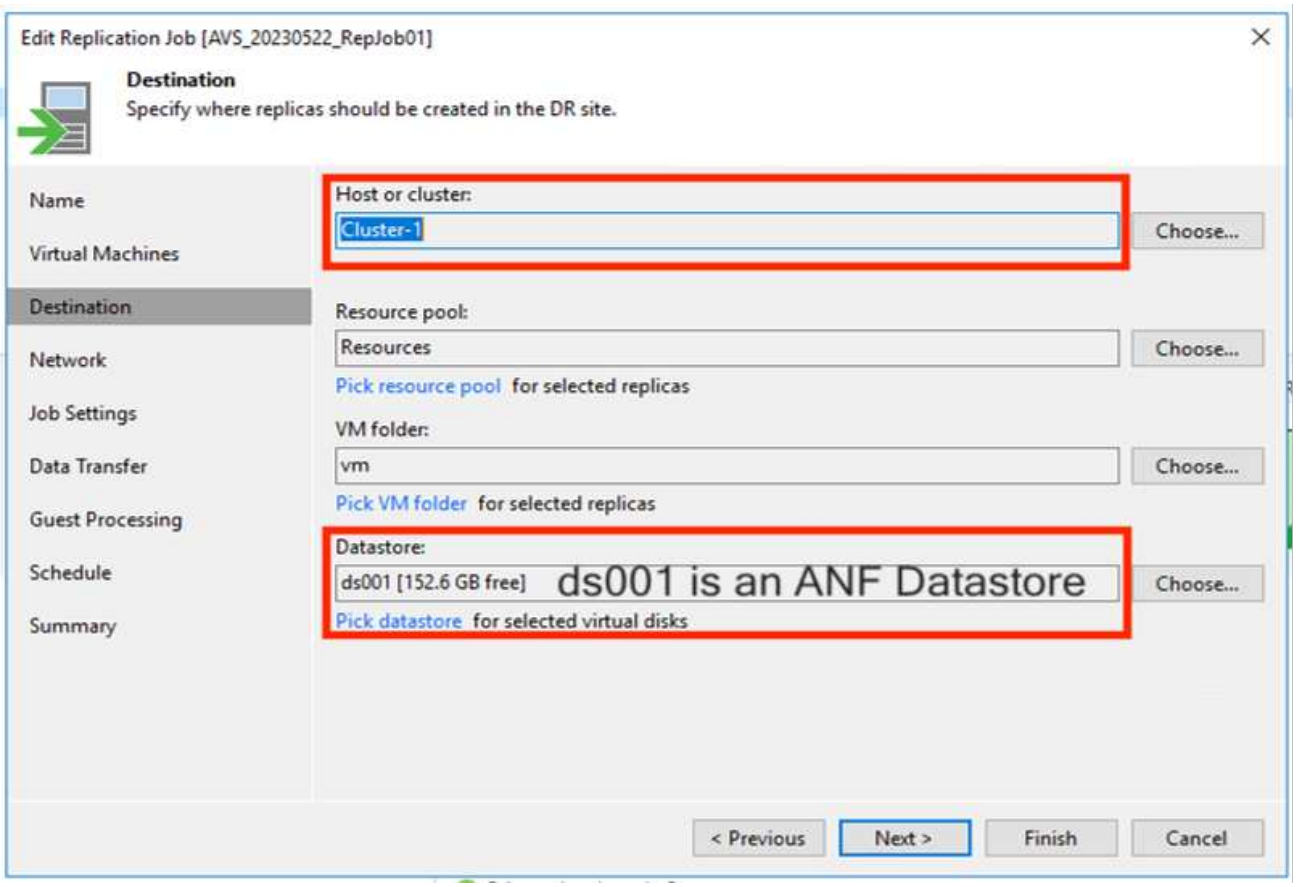


4. 仮想マシン の手順で、Azure VMware Solution SDDC に接続されているAzure NetApp Filesデータストアにレプリケートする VM を選択します。使用可能な vSAN データストアの容量を満たすために、仮想マシンを vSAN 上に配置できます。パイロット ライト クラスターでは、3 ノード クラスターの使用可

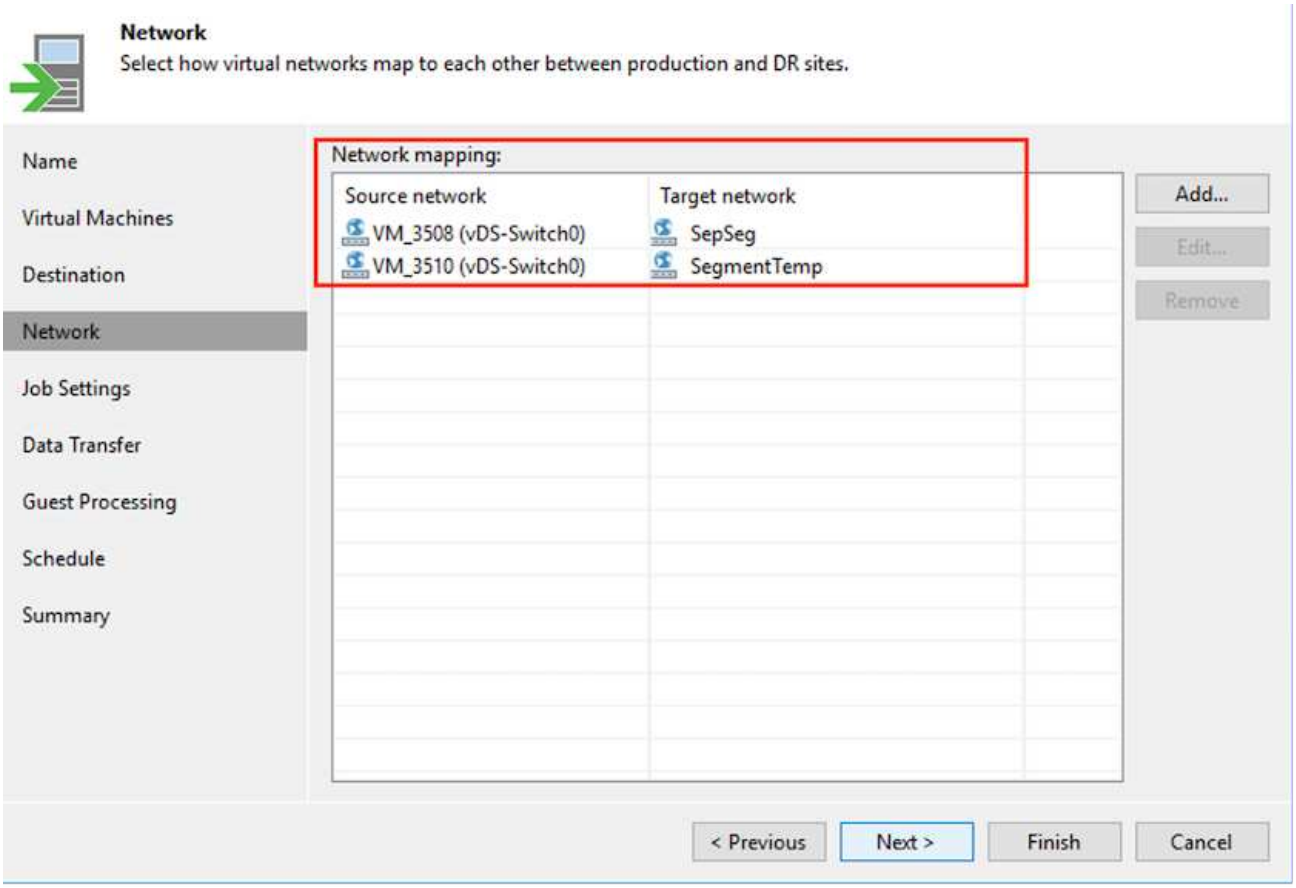
能な容量が制限されます。残りのデータはAzure NetApp Filesデータストアに簡単に配置できるため、VM を回復し、CPU/メモリ要件を満たすようにクラスターを拡張できます。 [追加] をクリックし、[オブジェクトの追加] ウィンドウで必要な VM または VM コンテナを選択して [追加] をクリックします。*次へ*をクリックします。



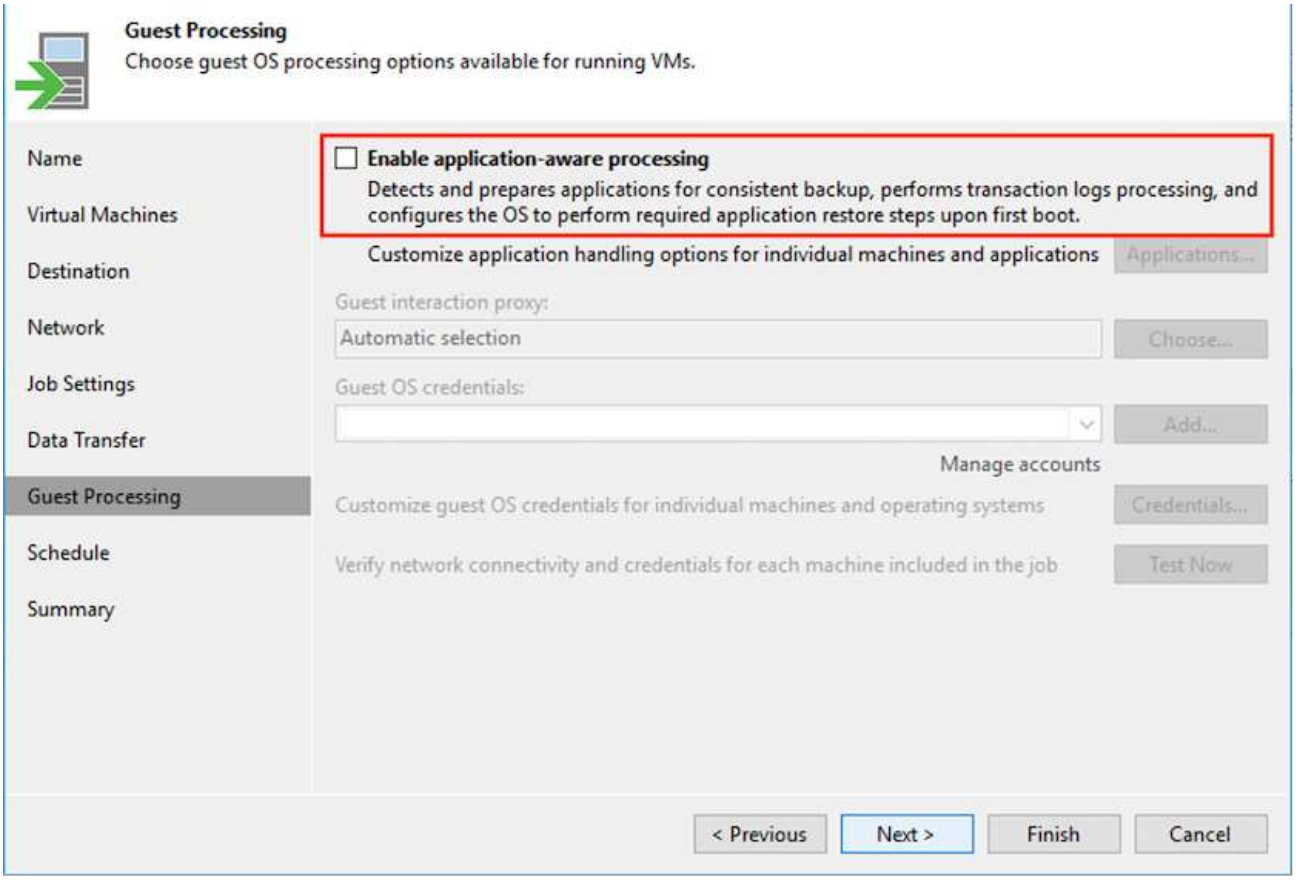
5. その後、宛先として Azure VMware Solution SDDC クラスター/ホストを選択し、VM レプリカ用の適切なリソース プール、VM フォルダー、および FSx ONTAPデータストアを選択します。次に、[次へ] をクリックします。



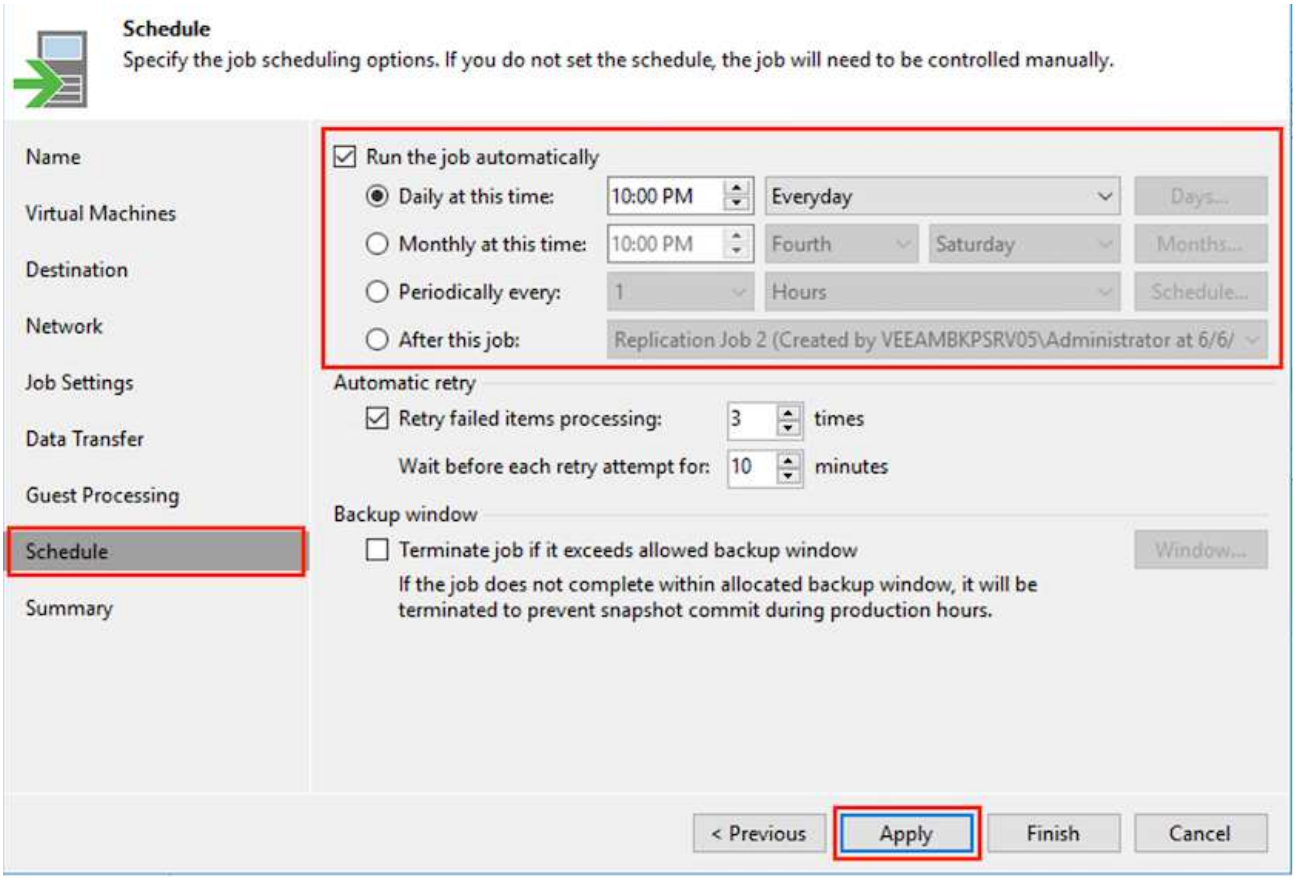
6. 次の手順では、必要に応じて、ソース仮想ネットワークと宛先仮想ネットワーク間のマッピングを作成します。



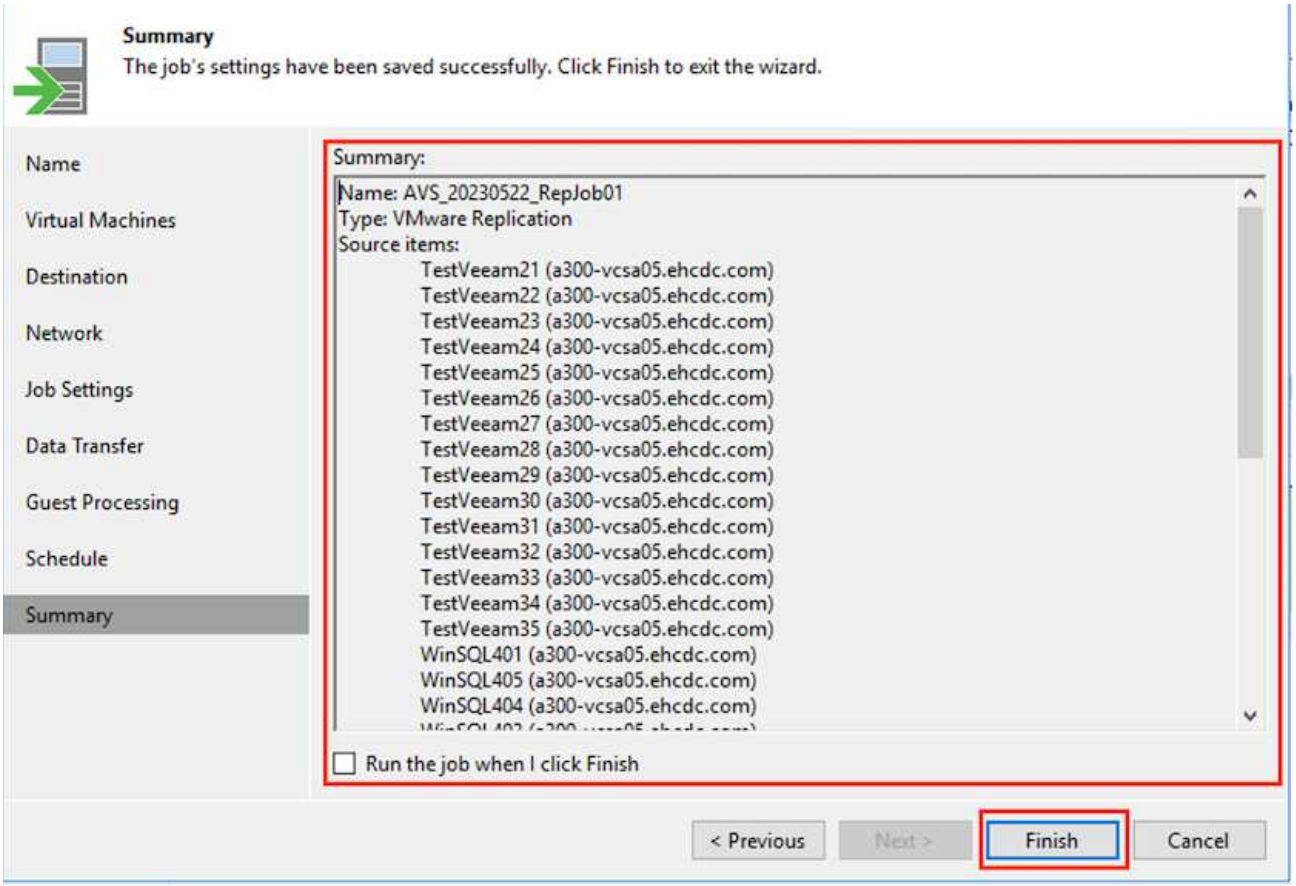
7. ジョブ設定 ステップで、VM レプリカのメタデータ、保持ポリシーなどを保存するバックアップ リポジトリを指定します。
8. *データ転送*手順で*ソース*および*ターゲット*プロキシ サーバーを更新し、*自動*選択 (デフォルト) のままにして、*直接*オプションを選択したままにして、*次へ*をクリックします。
9. *ゲスト処理*のステップで、必要に応じて*アプリケーション対応処理を有効にする*オプションを選択します。*次へ*をクリックします。



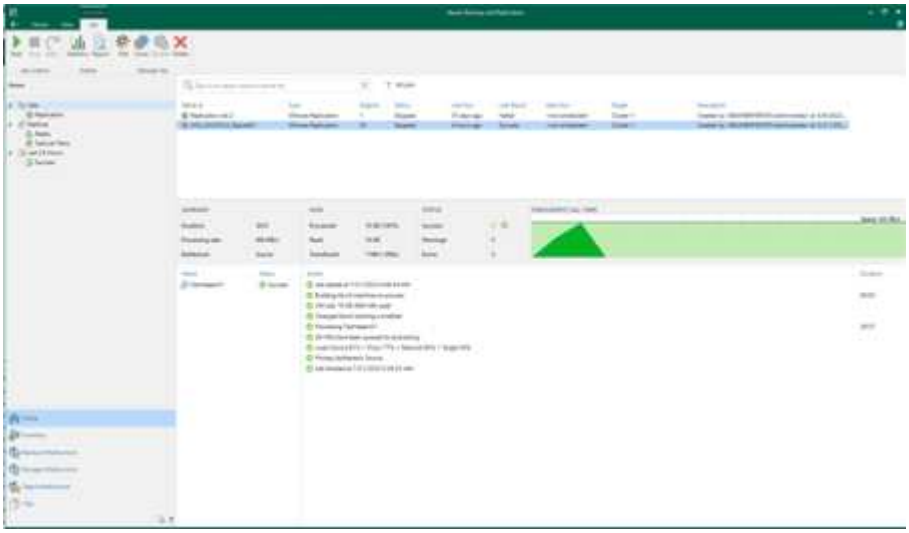
10. 定期的に実行するレプリケーション ジョブを実行するには、レプリケーション スケジュールを選択します。



11. ウィザードの*概要*手順で、レプリケーション ジョブの詳細を確認します。ウィザードを閉じ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。それ以外の場合は、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を持つ VM が宛先の AVS SDDC クラスター/ホストに配置されます。



Veeamレプリケーションの詳細については、以下を参照してください。"レプリケーションの仕組み"

▼ ステップ**2:** フェイルオーバー計画を作成する

初期レプリケーションまたはシードが完了したら、フェールオーバー 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、ブートの遅延を含め、VM が処理される順序の青写真です。フェールオーバー 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。

計画を作成するには、「レプリカ」という新しいサブセクションに移動し、「フェールオーバー 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復元ポイントを探し、それを使用して VM レプリカを起動します。

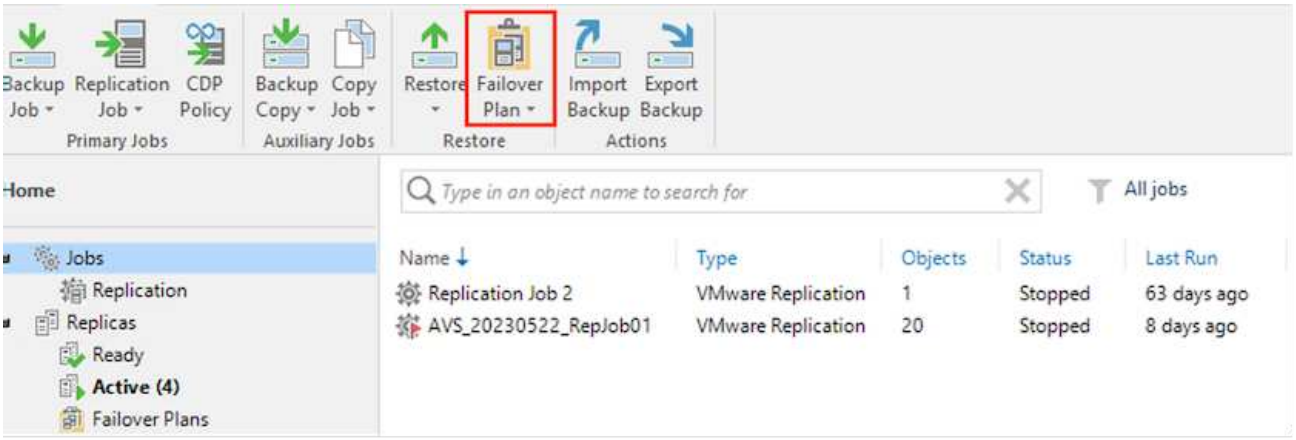
フェールオーバー プランは、初期レプリケーションが完了し、VM レプリカが準備完了状態になった後にのみ追加できます。

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。

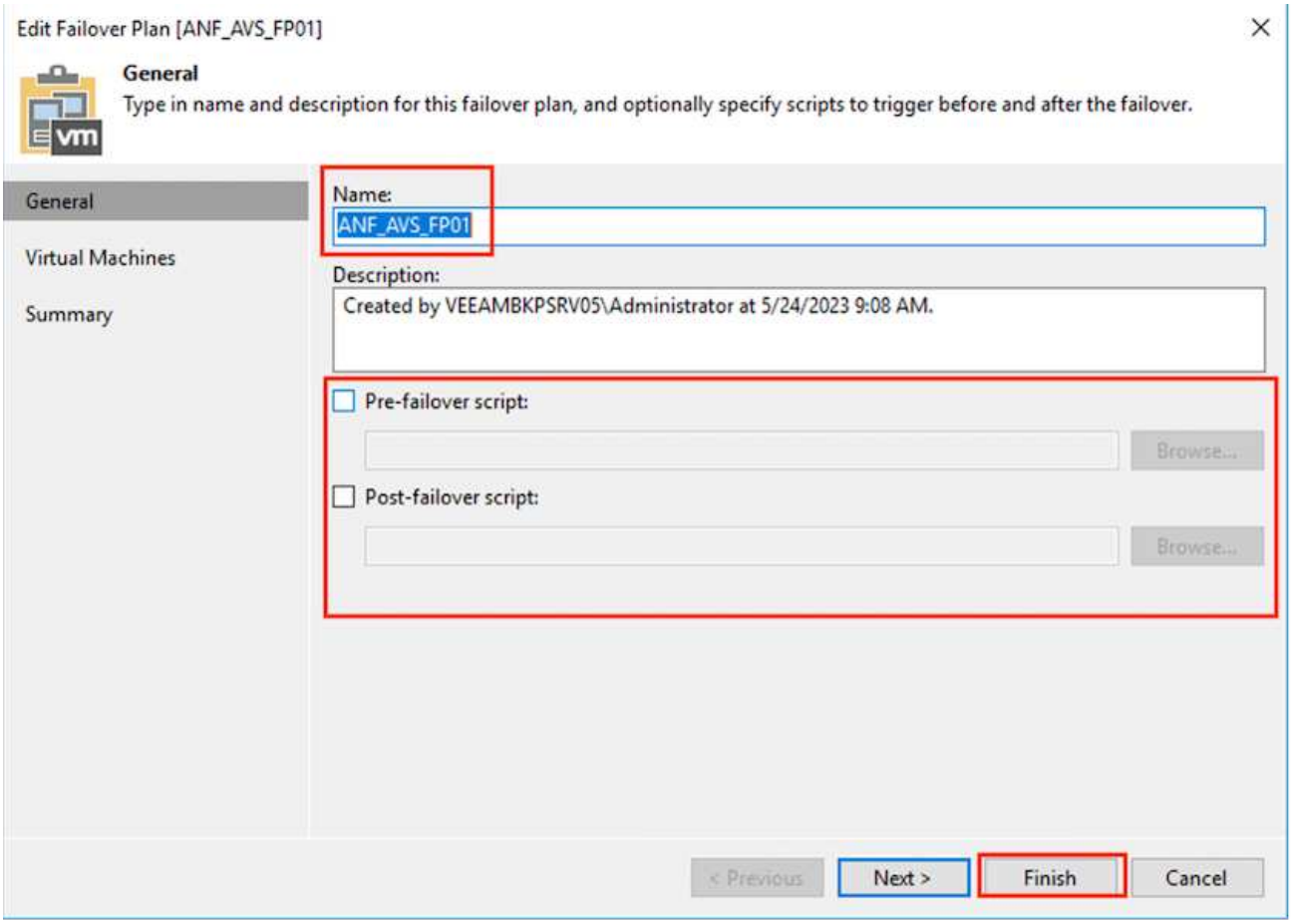
フェイルオーバープロセス中、ソースVMの電源はオフになりません

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。

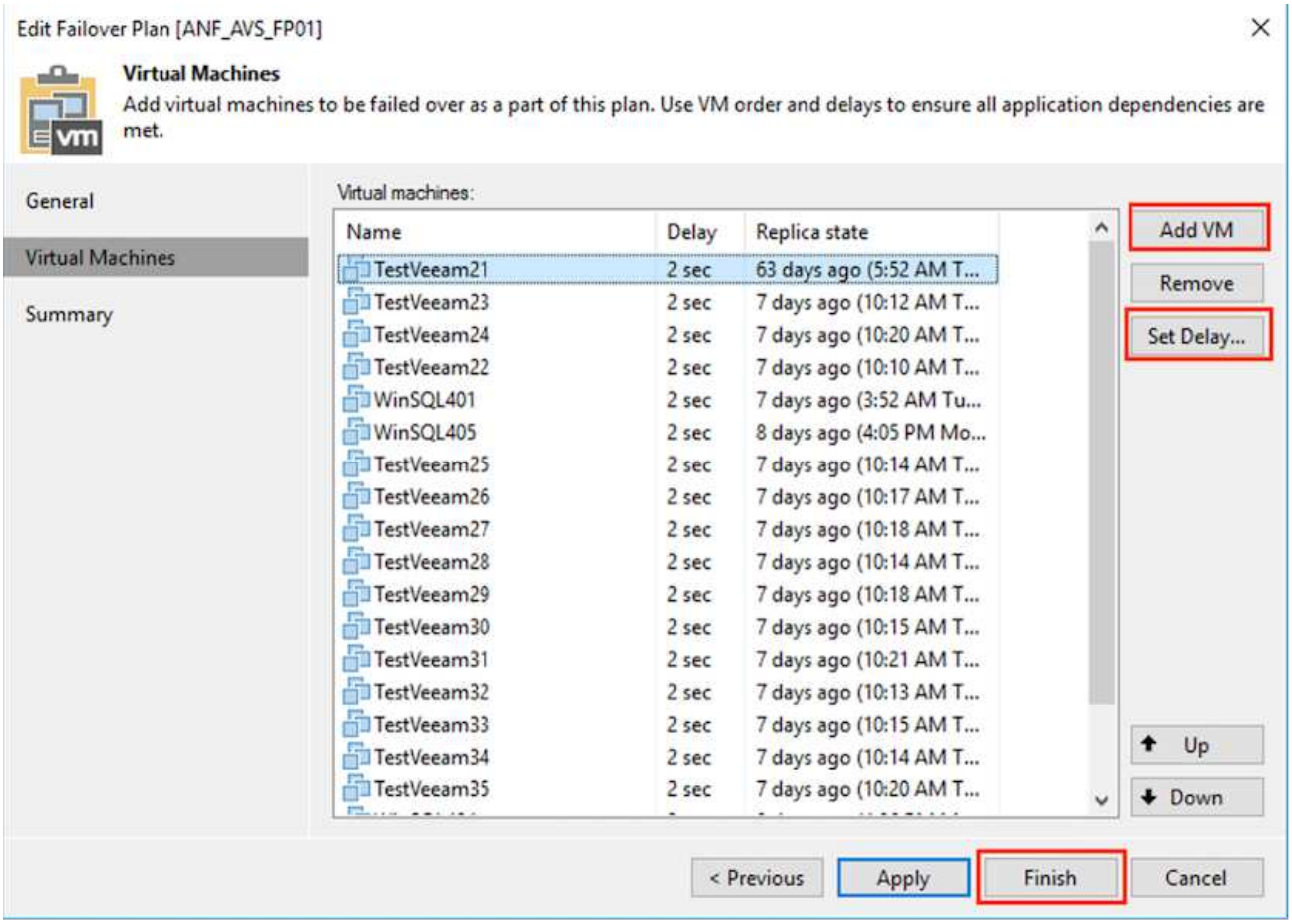
1. ホームビューで。レプリカ ノードを右クリックし、フェイルオーバー プラン > フェイルオーバー プラン > VMware vSphere を選択します。



2. 次に、プランの名前と説明を入力します。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、複製された VM を起動する前に VM をシャットダウンするスクリプトを実行します。



3. VM を計画に追加し、アプリケーションの依存関係を満たすように VM のブート順序とブート遅延を変更します。



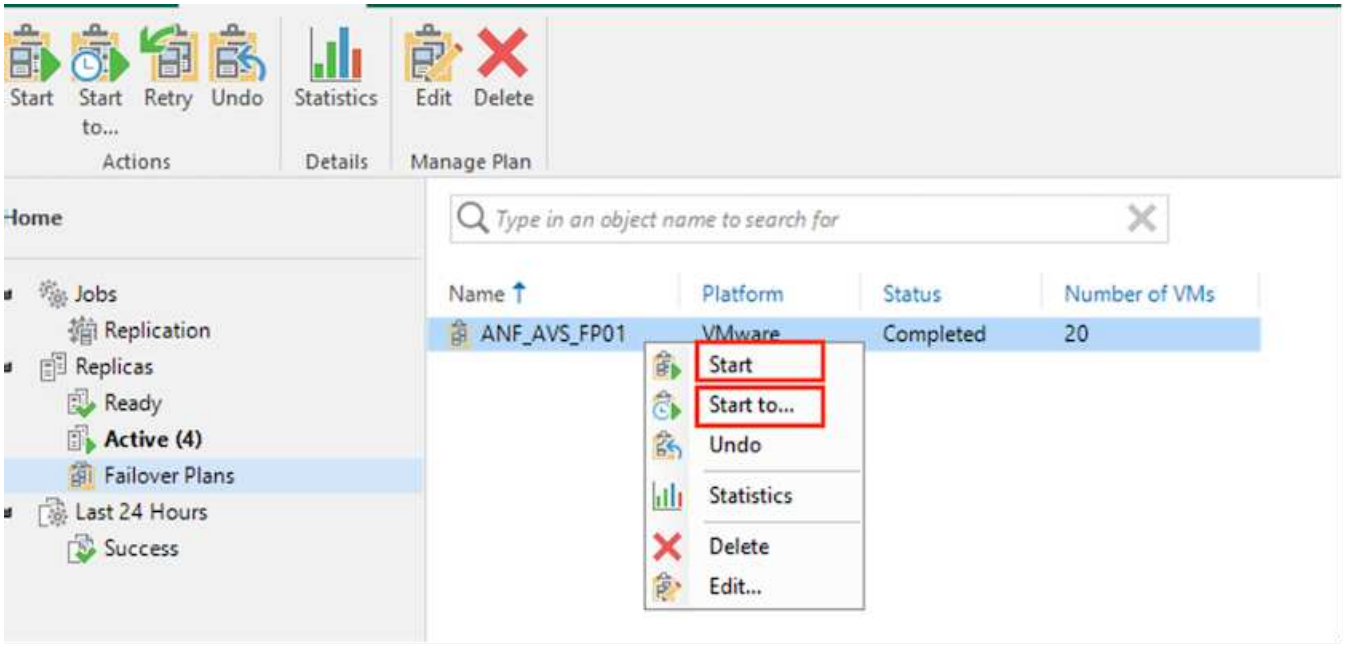
レプリケーションジョブの作成に関する追加情報については、以下を参照してください。"レプリケーションジョブの作成" 。

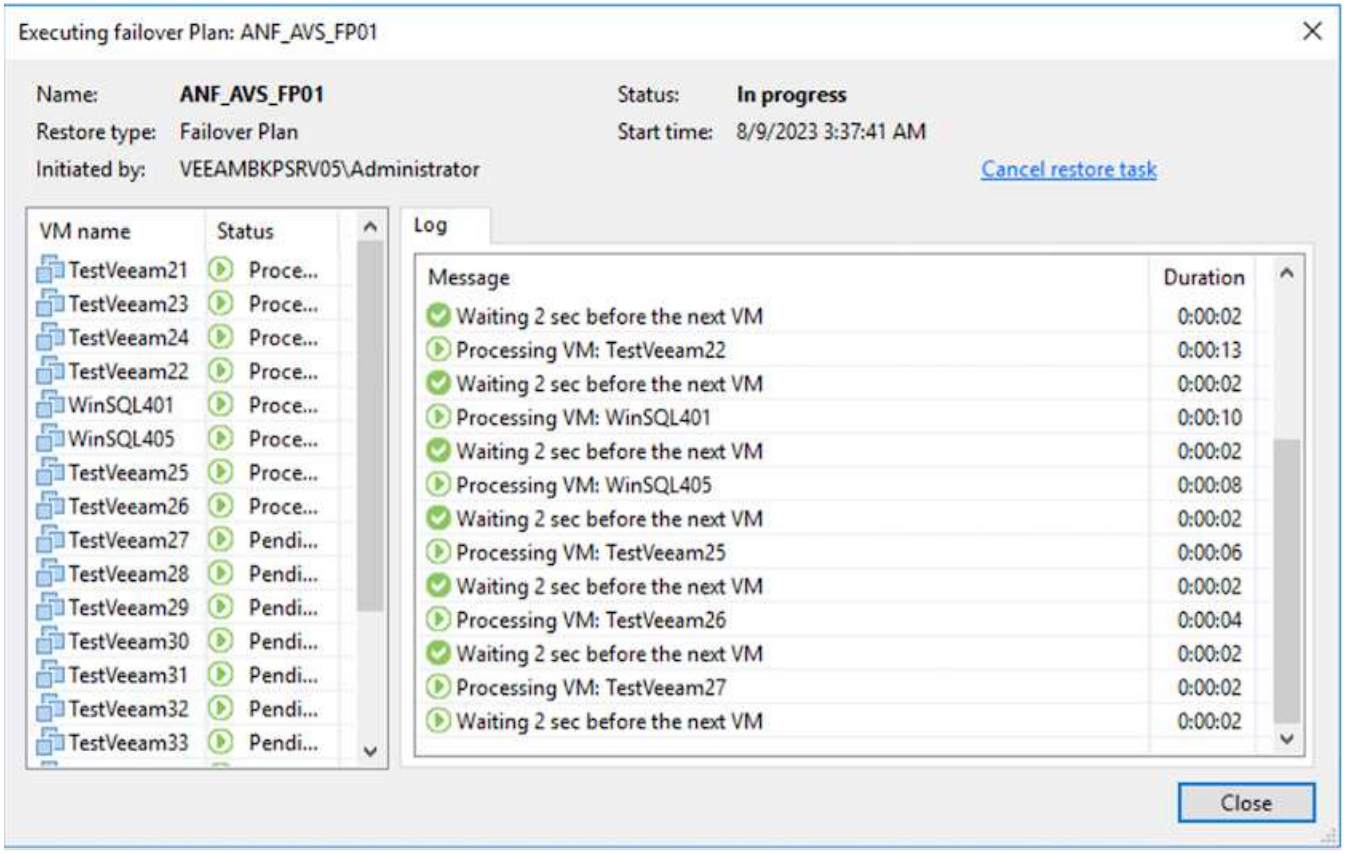
▼ ステップ**3:** フェイルオーバープランを実行する

フェイルオーバー中、運用サイトのソース VM は災害復旧サイトのレプリカに切り替えられます。フェイルオーバー プロセスの一環として、Veeam Backup & Replication は VM レプリカを必要な復元ポイントに復元し、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。レプリカは災害時だけでなく、DR 訓練のシミュレーションにも使用できます。フェールオーバー シミュレーション中、ソース VM は実行を継続します。必要なテストがすべて実行されたら、フェイルオーバーを元に戻して通常の操作に戻ることができます。

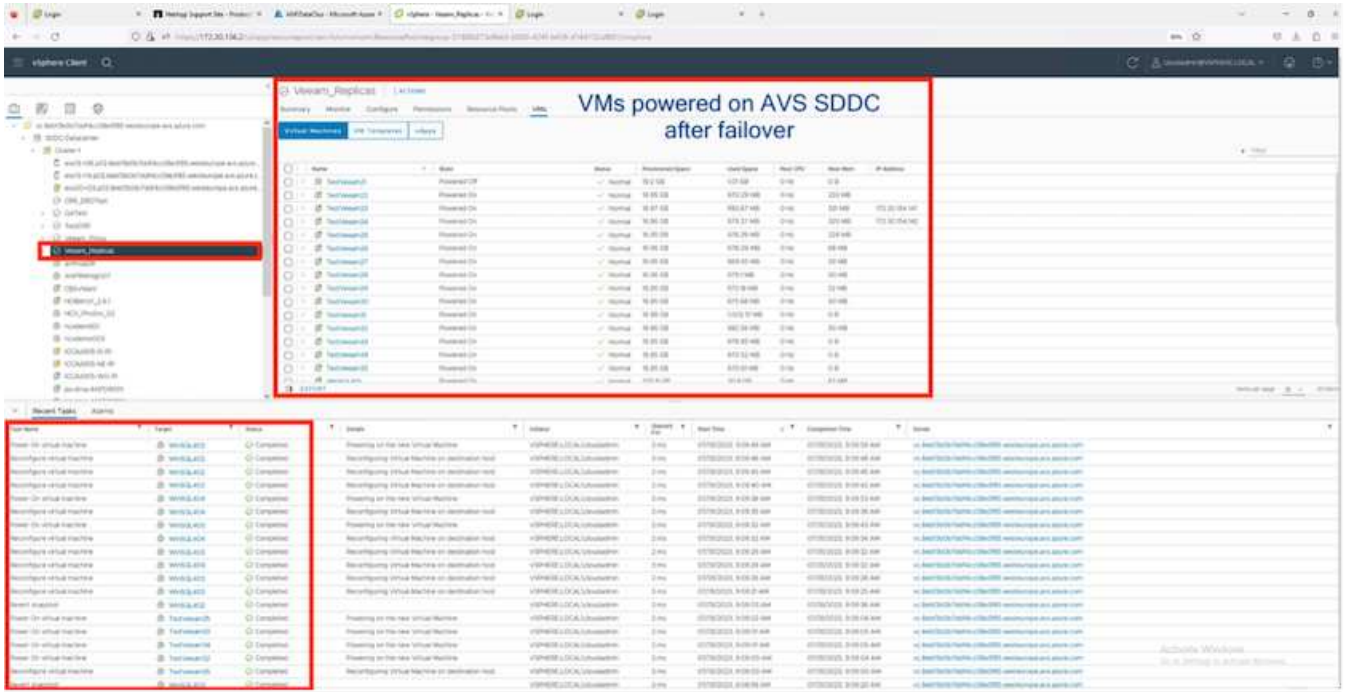
ⓘ フェイルオーバー中の IP 競合を回避するために、ネットワーク セグメンテーションが適切に行われていることを確認してください。

フェールオーバー プランを開始するには、[フェールオーバー プラン] タブをクリックし、フェールオーバー プランを右クリックするだけです。 **[開始]*を選択します。これにより、VM レプリカの最新の復元ポイントを使用してフェイルオーバーが行われます。 VM レプリカの特定の復元ポイントにフェールオーバーするには、[開始] を選択します。

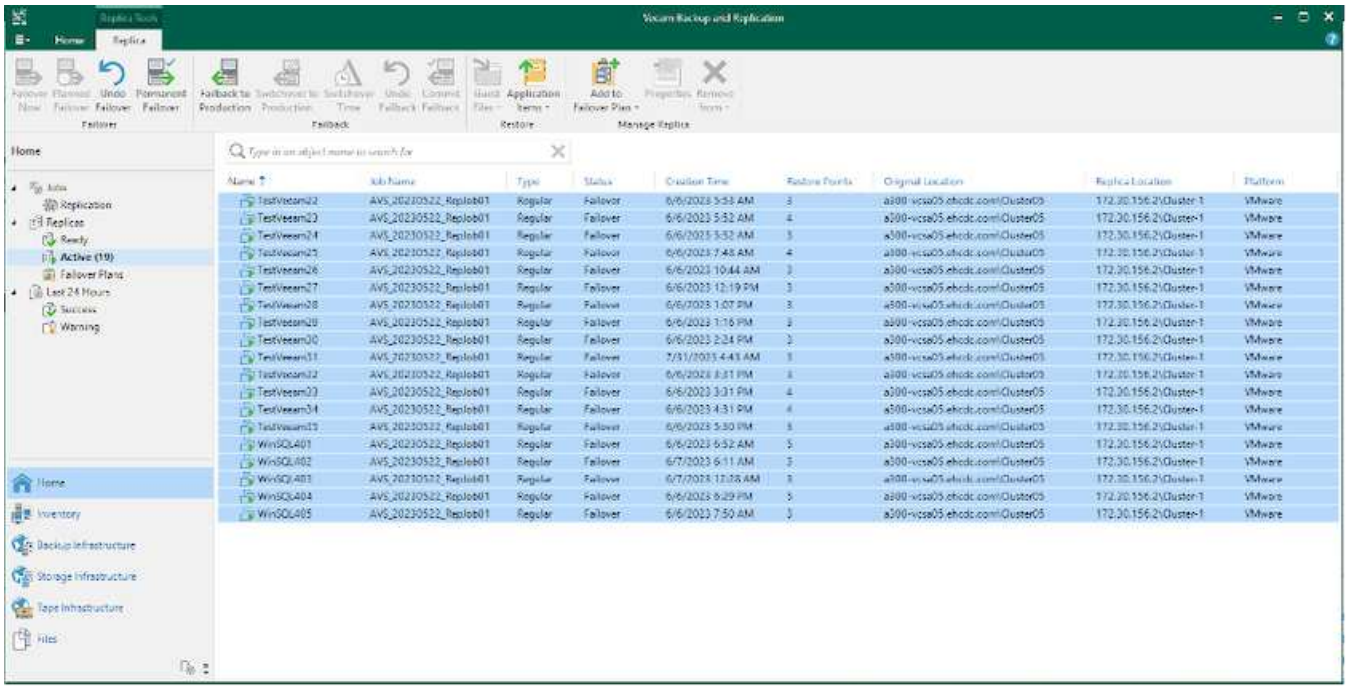




VM レプリカの状態が「準備完了」から「フェールオーバー」に変わり、VM は宛先の Azure VMware Solution (AVS) SDDC クラスター/ホストで起動します。



フェイルオーバーが完了すると、VM のステータスが「フェイルオーバー」に変わります。



Veeam Backup & Replication は、レプリカが準備完了状態に戻るまで、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、以下を参照してください。"フェイルオーバー計画" 。

▼ ステップ**4:** 本番サイトへのフェイルバック

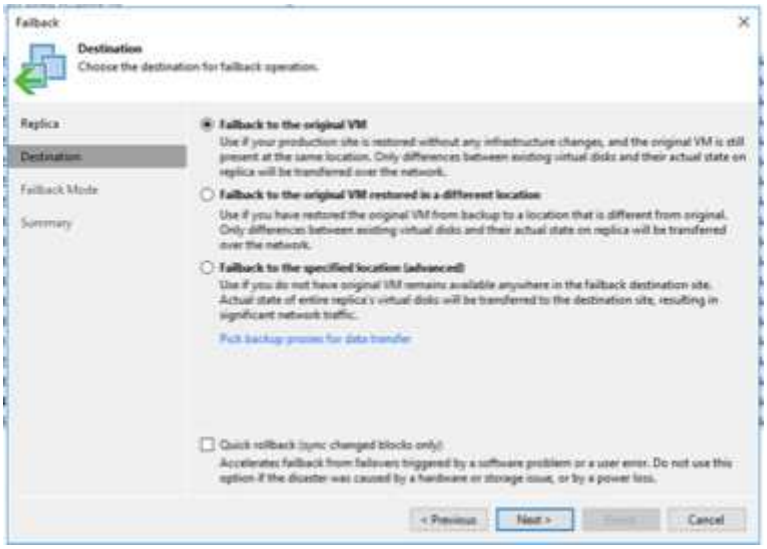
フェイルオーバー プランが実行中の場合、それは中間ステップとみなされ、要件に基づいて確定する必要があります。オプションには次のものがあります。

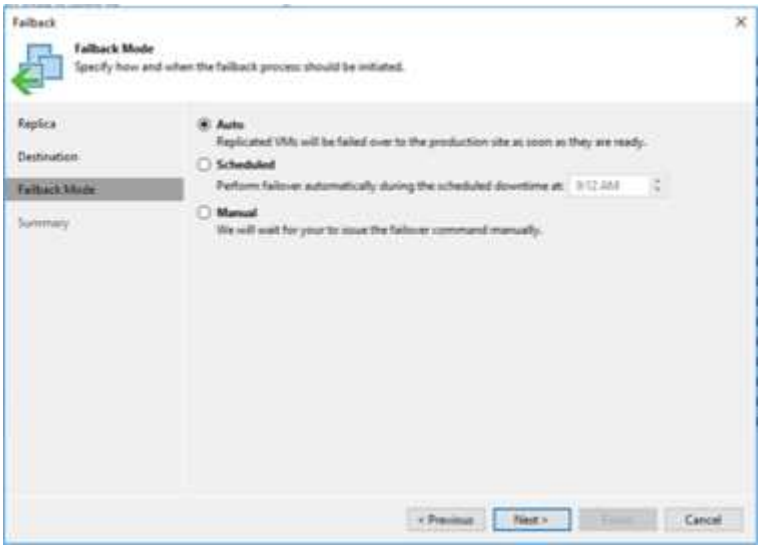
- 本番環境へのフェールバック - 元の VM に切り替えて、VM レプリカの実行中に行われたすべての変更を元の VM に転送します。

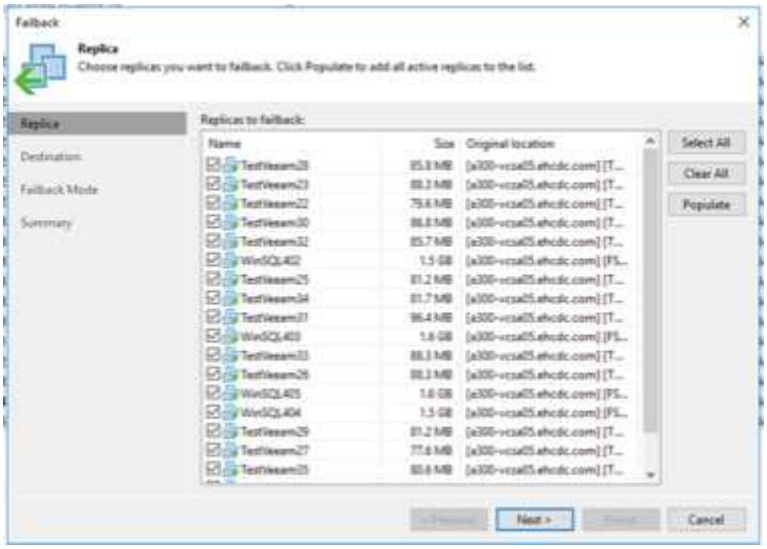
> フェイルバックを実行すると、変更は転送されるだけで公開されません。元の VM が期待どおりに動作していることが確認されたら、*フェイルバックのコミット*を選択するか、元の VM が期待どおりに動作していない場合は、フェイルバックを元に戻すを選択して VM レプリカに戻ります。

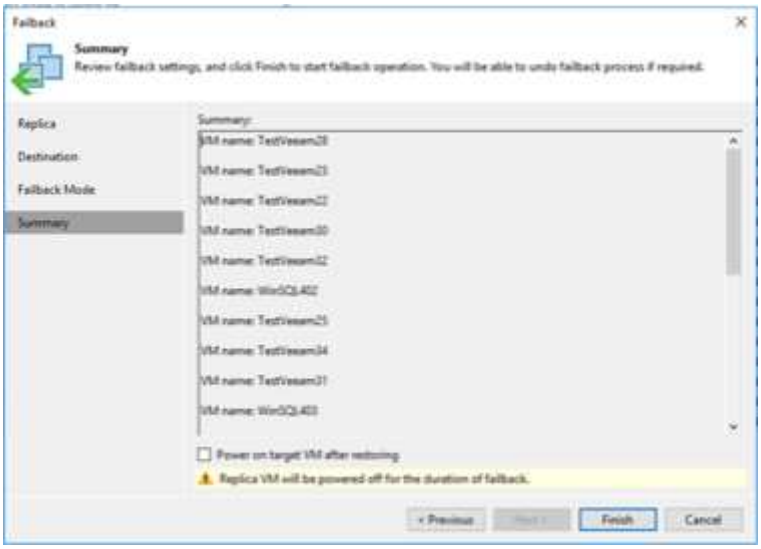
- フェイルオーバーを元に戻す - 元の VM に切り替えて、VM レプリカの実行中に行われたすべての変更を破棄します。
- 永続的なフェイルオーバー - 元の VM から VM レプリカに永続的に切り替え、このレプリカを元の VM として使用します。

このデモでは、本番環境へのフェールバックが選択されました。ウィザードの宛先ステップで元の VM へのフェールバックが選択され、「復元後に VM をパワーオンする」チェックボックスが有効になりました。



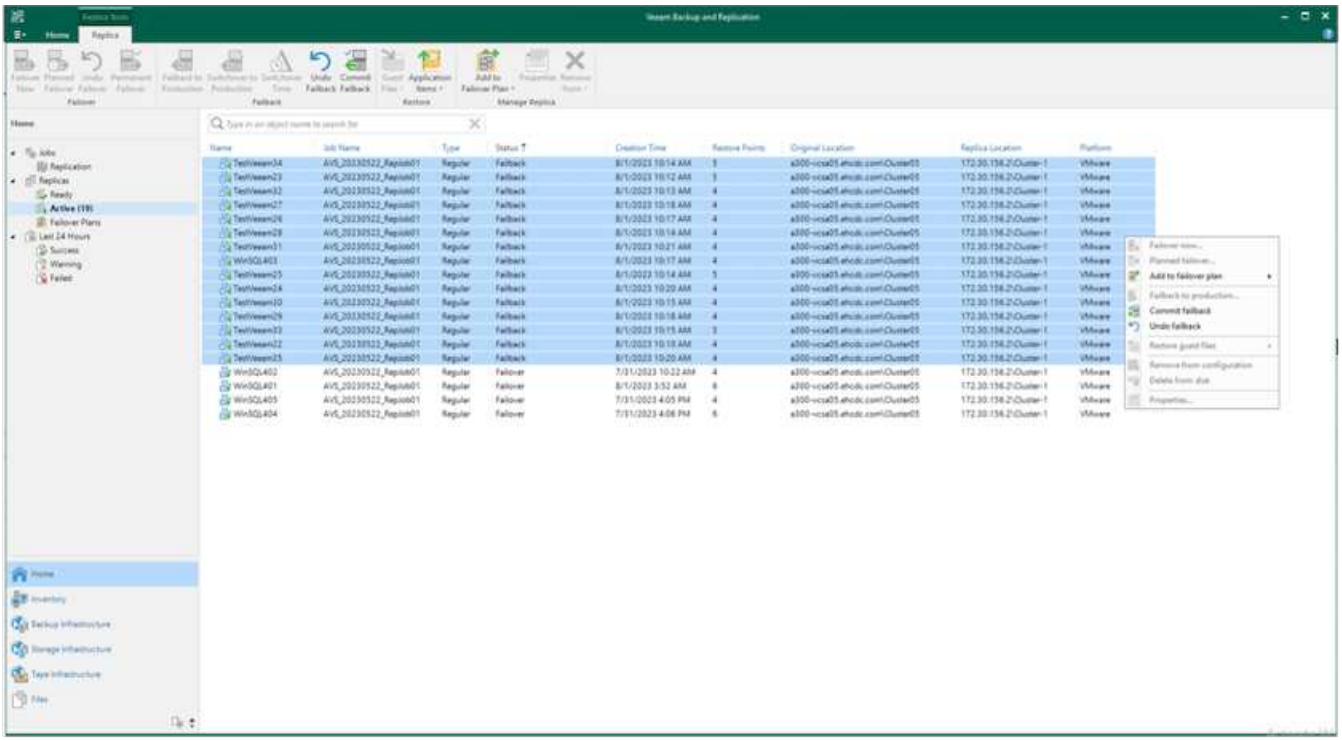




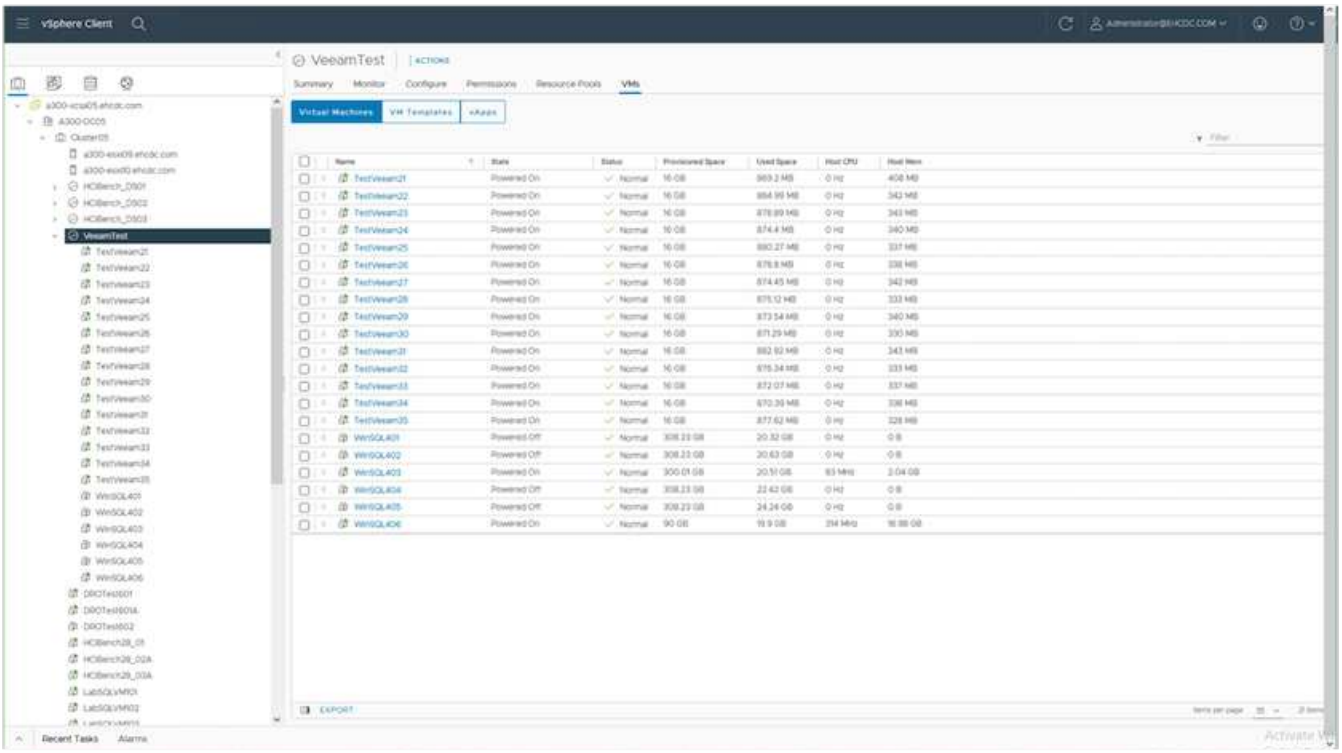


フェイルバックコミットは、フェイルバック操作を完了する方法の 1 つです。フェイルバックがコミットされると、フェイルバックされた VM (運用 VM) に送信された変更が期待どおりに機能していることが確認されます。コミット操作の後、Veeam Backup & Replication は実稼働 VM のレプリケーション アクティビティを再開します。

フェイルバックプロセスの詳細については、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" 。



運用環境へのフェイルバックが成功すると、VM はすべて元の運用サイトに復元されます。



まとめ

Azure NetApp Filesデータストア機能により、Veeam または検証済みのサードパーティ ツールは、VM レプリカを収容するためだけに大規模なクラスターを立ち上げるのではなく、パイロット ライト クラスターを活用して低コストの DR ソリューションを提供できるようになります。これにより、調整されカスタマイズされた災害復旧計画を効率的に処理し、既存のバックアップ製品を社内で DR に再利用して、オンプレミスの DR データセンターを廃止してクラウドベースの災害復旧を実現できるようになります。災害時にはボタンをクリッ

クすることでフェイルオーバーしたり、災害発生時に自動的にフェイルオーバーしたりすることが可能。

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

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278

Azure/AVS 上のワークロードを移行する

TR-4940: 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する **-** クイックスタート ガイド

Azure VMware Solution と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。

概要: **VMware HCX**、 **Azure NetApp Files**データストア、**Azure VMware** ソリューションを使用した仮想マシンの移行

VMware HCX は主に、アプリケーションの移行、ワークロードの再調整、さらにはクラウド間のビジネス継続性を簡素化するように設計された移行プラットフォームです。これは Azure VMware Solution プライベートクラウドの一部として含まれており、ワークロードを移行するためのさまざまな方法を提供し、ディザスターリカバリー (DR) 操作に使用できます。

このドキュメントでは、 Azure NetApp Filesデータストアをプロビジョニングし、その後、オンプレミスと Azure VMware Solution 側のすべての主要コンポーネント (相互接続、ネットワーク拡張、さまざまな VM 移行メカニズムを有効にするための WAN 最適化など) を含む VMware HCX をダウンロード、デプロイ、構成するための手順を詳しく説明します。

> VMware HCX は、移行が VM レベルで行われるため、どのデータストア タイプでも動作します。したがって、このドキュメントは、コスト効率の高い VMware クラウド展開のために Azure VMware Solution を使用してAzure NetApp Filesを展開することを計画している既存のNetApp顧客と非NetApp顧客に適用されます。

▼ 大まかな手順

このリストには、Azure クラウド側に HCX Cloud Manager をインストールして構成し、オンプレミスに HCX Connector をインストールするために必要な手順の概要が示されています。

1. Azure ポータルから HCX をインストールします。
2. オンプレミスの VMware vCenter Server に HCX コネクタ Open Virtualization Appliance (OVA) インストーラーをダウンロードしてデプロイします。
3. ライセンス キーを使用して HCX をアクティブ化します。
4. オンプレミスの VMware HCX コネクタを Azure VMware Solution 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 メッシュを構成します。
6. (オプション) 移行中に IP の再割り当てを避けるため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します。

▼ 前提条件

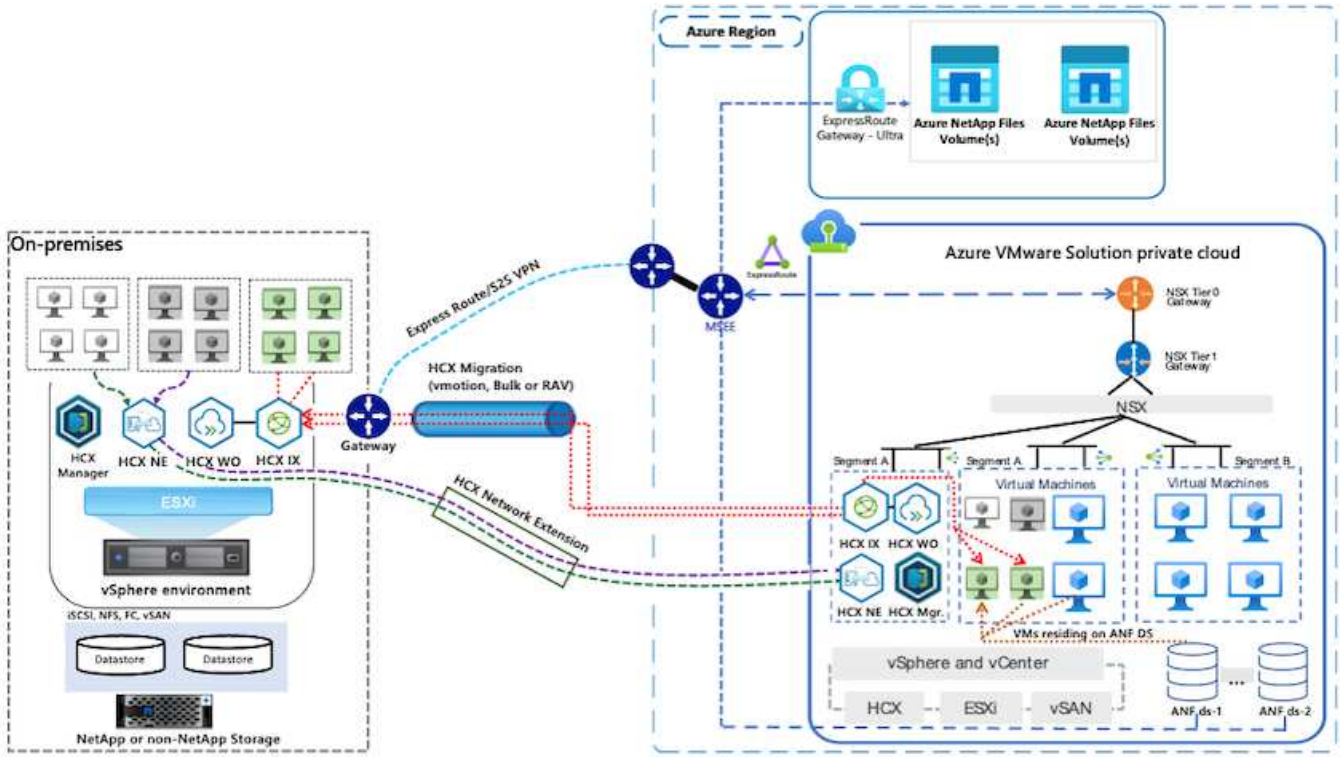
始める前に、次の前提条件が満たされていることを確認してください。詳細については、こちらをご覧ください "リンク"。接続などの前提条件が整ったら、Azure VMware Solution ポータルからライセンス キーを生成して、HCX を構成してアクティブ化します。 OVA インストーラをダウンロードしたら、以下の説明に従ってインストール プロセスを続行します。

HCX アドバンスドはデフォルトのオプションであり、VMware HCX エンタープライズ エディションもサポート チケットを通じて利用可能で、追加費用なしでサポートされます。

- 既存のAzure VMwareソリューションのソフトウェア定義データセンター（SDDC）を使用するか、これを使用してプライベートクラウドを作成します。"NetAppリンク"またはこれ "マイクロソフトリンク"。
- 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Express Route Global Reach接続を設定する"オンプレミス環境とそれぞれのプライベート クラウド間。
- オンプレミスの VMware vCenter Server 環境から Azure VMware Solution プライベート クラウドへのネットワーク パスは、vMotion を使用した VM の移行をサポートする必要があります。
- 必要な "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 トラフィックが許可されます。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がデフォルトで構成されています。
- Azure NetApp Files NFS ボリュームは、Azure VMware Solution のデータストアとしてマウントする必要があります。この手順に従ってください "リンク"Azure NetApp Filesデータストアを Azure VMware Solutions ホストに接続します。

▼ 高レベルアーキテクチャ

テストの目的で、この検証に使用されたオンプレミスのラボ環境は、オンプレミスから Azure VMware Solution への接続を可能にするサイト間 VPN を介して接続されました。



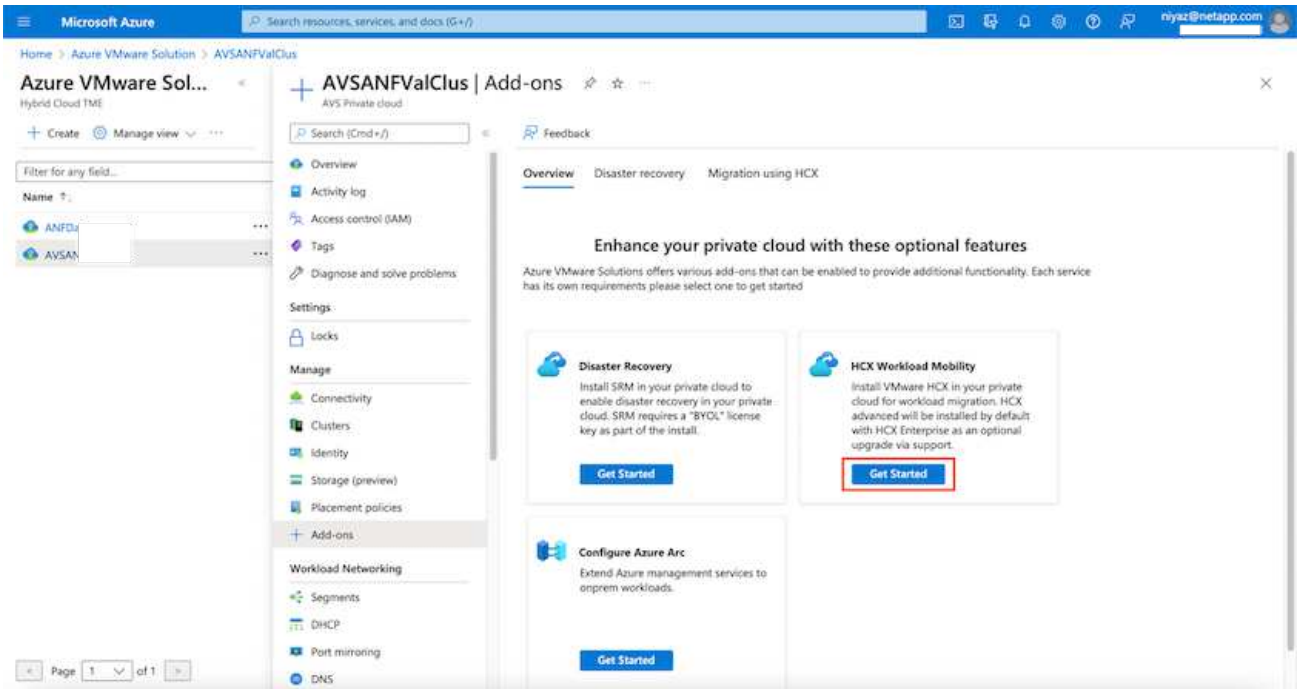
ソリューションの展開

このソリューションの展開を完了するには、次の一連の手順に従います。

▼ ステップ **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。

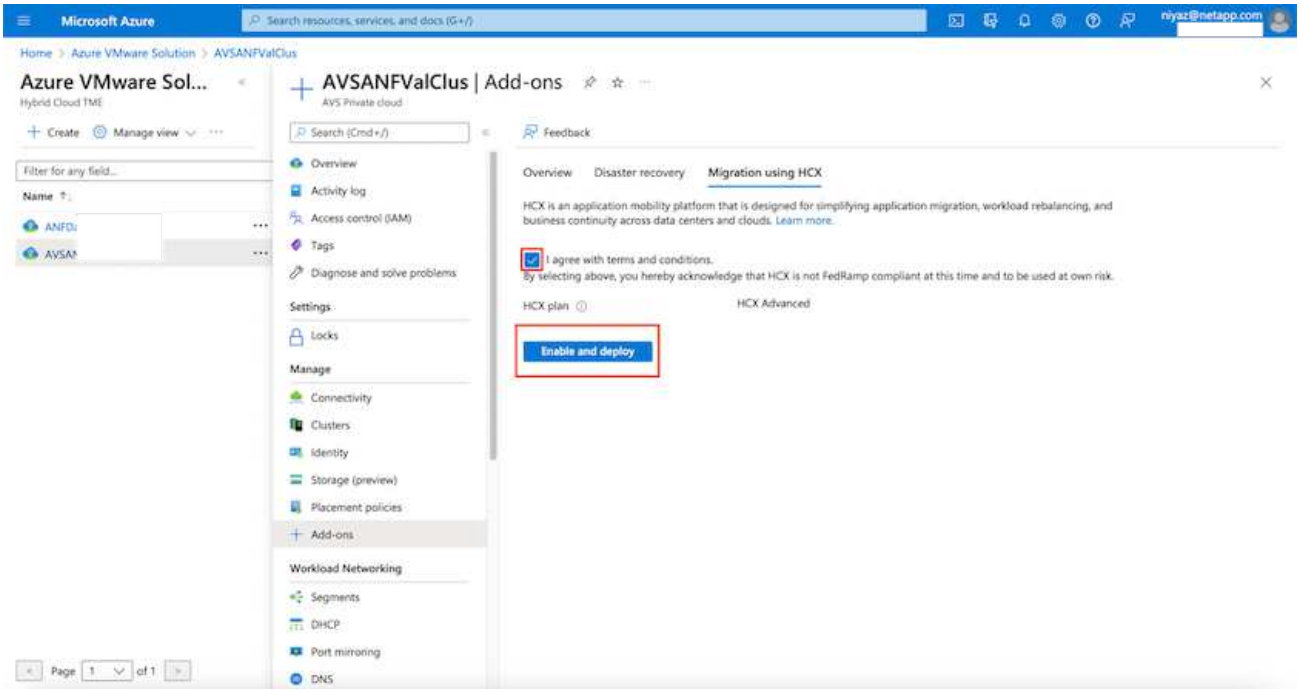
1. Azure Portal にログインし、Azure VMware Solution プライベート クラウドにアクセスします。
2. 適切なプライベート クラウドを選択し、アドオンにアクセスします。これは、*管理 > アドオン*に移動することで実行できます。
3. HCX ワークロード モビリティ セクションで、[開始] をクリックします。



4. *利用規約に同意します*オプションを選択し、*有効化してデプロイ*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。

展開には約 25 ～ 30 分かかります。



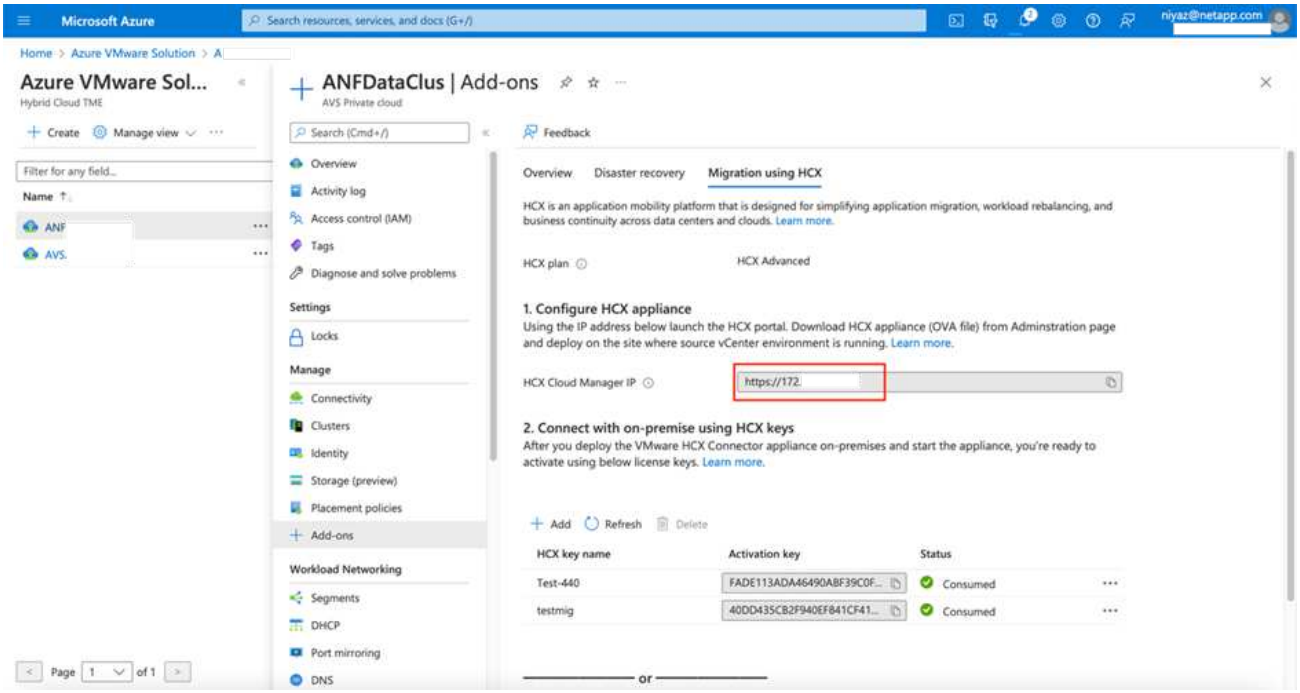
▼ ステップ**2:** オンプレミスの**vCenter Server**にインストーラ**OVA**を展開する

オンプレミスのコネクタを Azure VMware Solution の HCX マネージャーに接続するには、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てください。

オンプレミスの vCenter Server に HCX コネクタを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。

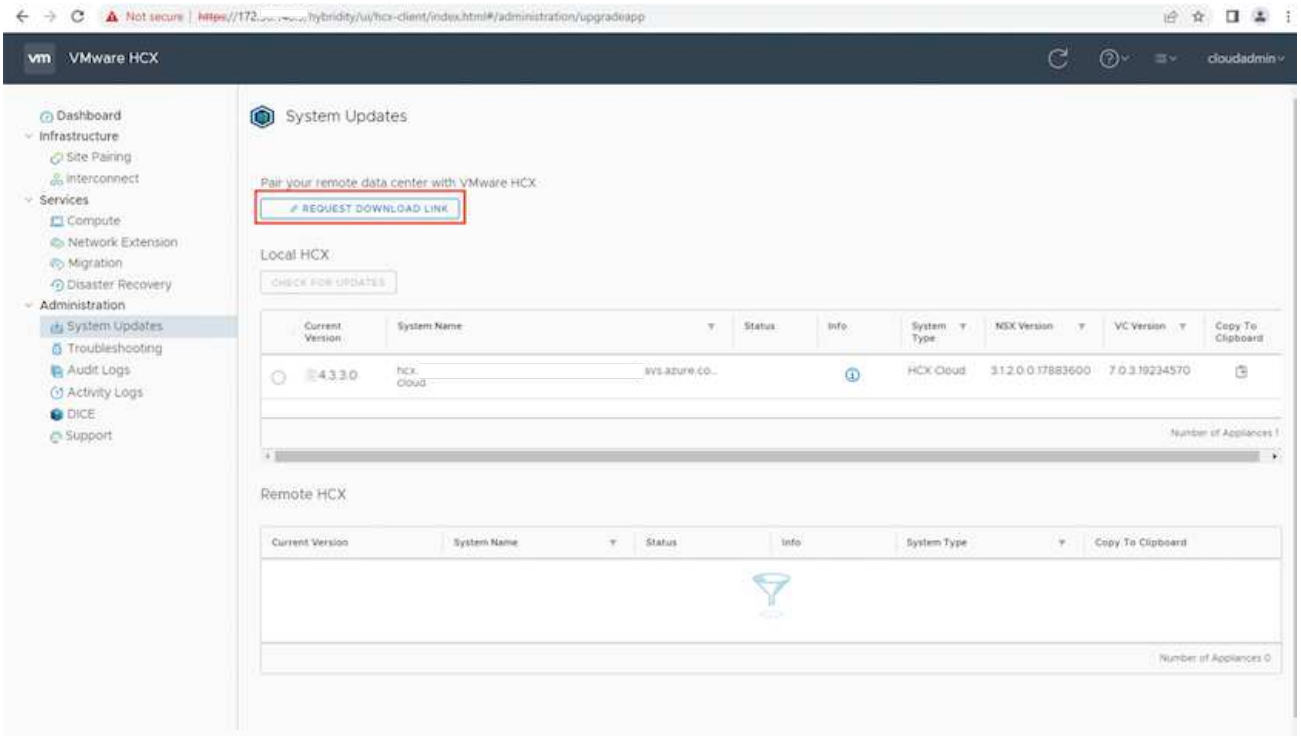
1. Azure ポータルから Azure VMware Solution に移動し、プライベート クラウドを選択して、HCX を使用して 管理 > アドオン > 移行 を選択し、HCX Cloud Manager ポータルをコピーして OVA ファイルをダウンロードします。

デフォルトの CloudAdmin ユーザー資格情報を使用して HCX ポータルにアクセスします。

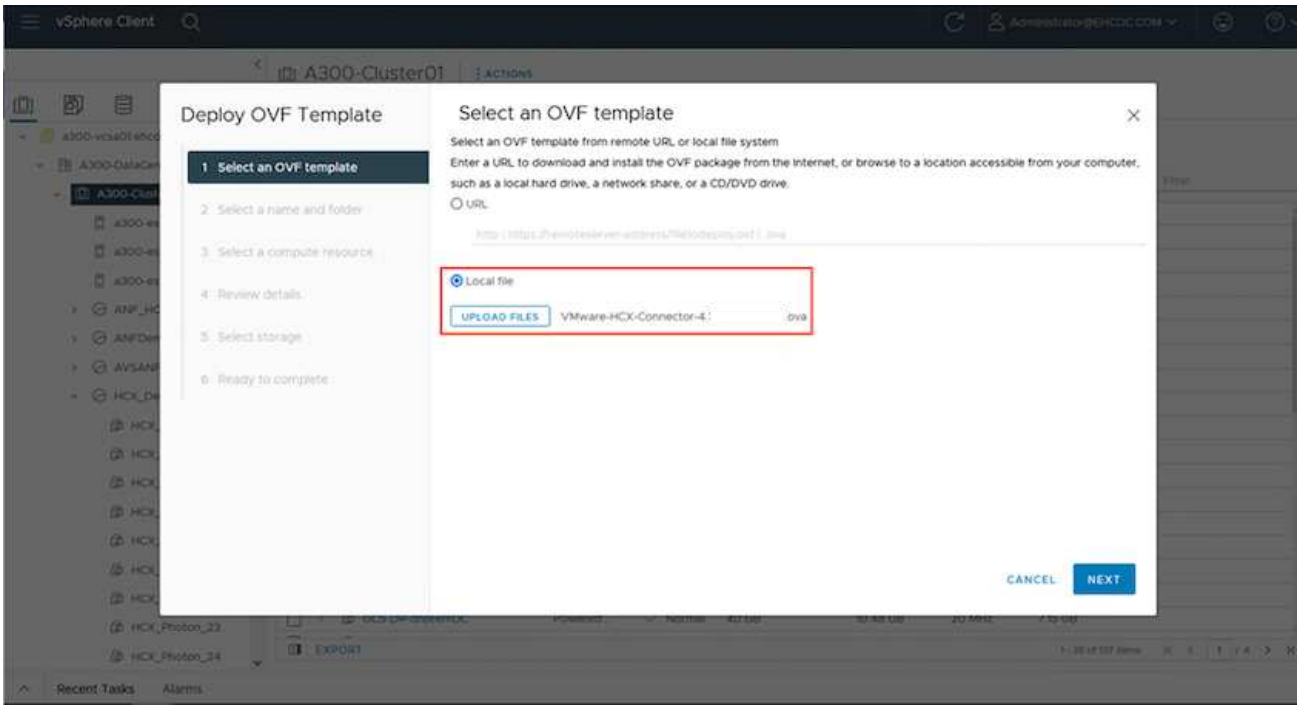


2. ジャンプホストを使用して cloudadmin@vsphere.local で HCX ポータルにアクセスした後、管理 > システム更新 に移動し、ダウンロード リンクの要求 をクリックします。

OVA へのリンクをダウンロードするかコピーしてブラウザに貼り付け、オンプレミスの vCenter Server にデプロイする 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。



3. OVA をダウンロードしたら、[OVF テンプレートのデプロイ] オプションを使用して、オンプレミスの VMware vSphere 環境にデプロイします。



4. OVA 展開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 コネクタ OVA を展開します。

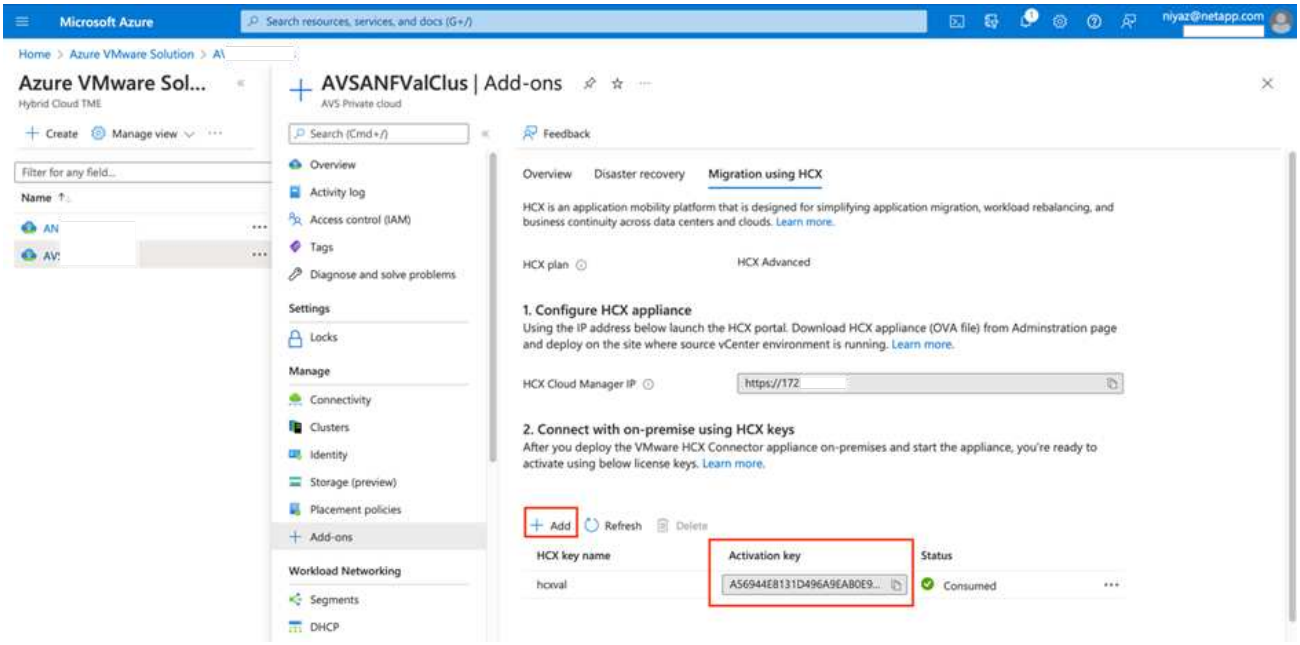
仮想アプライアンスを手動で電源オンします。

詳しい手順については、 "VMware HCX ユーザーガイド" 。

▼ ステップ**3:** ライセンスキーを使用して**HCX**コネクタをアクティブ化する

VMware HCX コネクタ OVA をオンプレミスにデプロイし、アプライアンスを起動したら、次の手順を実行して HCX コネクタをアクティブ化します。 Azure VMware Solution 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. Azure ポータルから Azure VMware Solution に移動し、プライベート クラウドを選択して、管理 **>** アドオン **> HCX** を使用した移行 を選択します。
2. オンプレミスの **HCX** キーを使用して接続 の下で、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。



展開されるオンプレミスの 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 Managerにログインします。 `"https://hcxmanagerIP:9443"`管理者の資格情報を使用します。

OVA 展開時に定義されたパスワードを使用します。

4. ライセンスで、手順 3 でコピーしたキーを入力し、[アクティブ化] 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。

5. データセンターの場所 で、オンプレミスの VMware HCX Manager をインストールするための最も近い場所を指定します。 *続行*をクリックします。
6. *システム名*の下で名前を更新し、*続行*をクリックします。
7. *はい、続行*をクリックします。
8. **vCenter** への接続 で、vCenter Server の完全修飾ドメイン名 (FQDN) または IP アドレスと適切な資格情報を入力し、続行 をクリックします。

後で接続の問題を回避するには、FQDN を使用します。

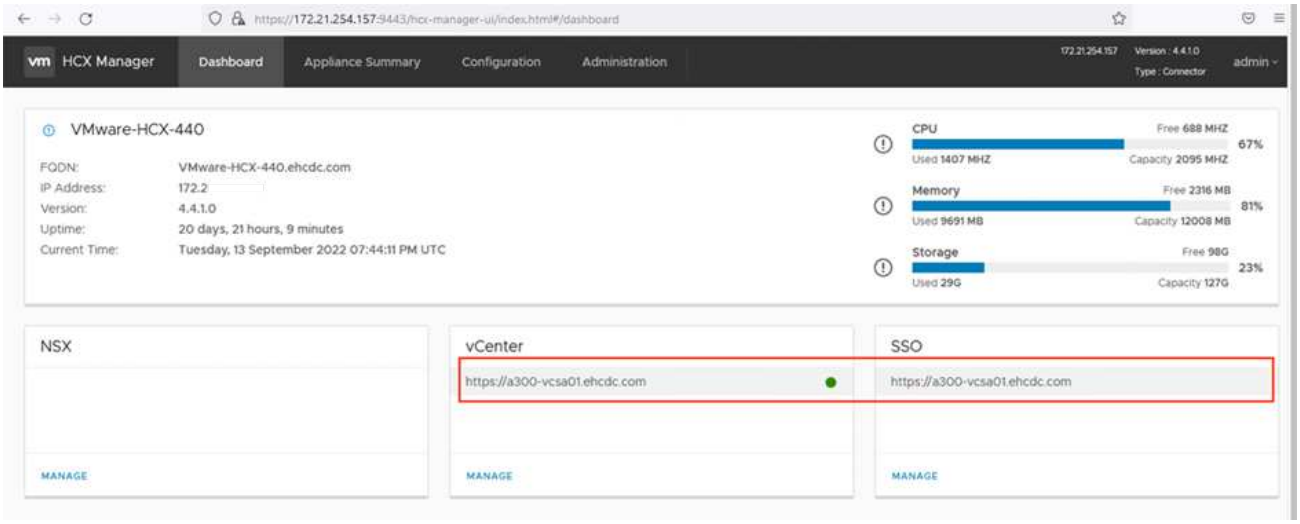
9. **SSO/PSC** の構成 で、Platform Services Controller の FQDN または IP アドレスを入力し、続行 をクリックします。

   VMware vCenter Server の FQDN または IP アドレスを入力します。

10. 入力した情報が正しいことを確認して、[再起動] をクリックします。

11. サービスが再起動すると、表示されるページで vCenter Server が緑色で表示されます。 vCenter Server と SSO の両方に適切な構成パラメータが設定されている必要があります。これは前のページと同じである必要があります。

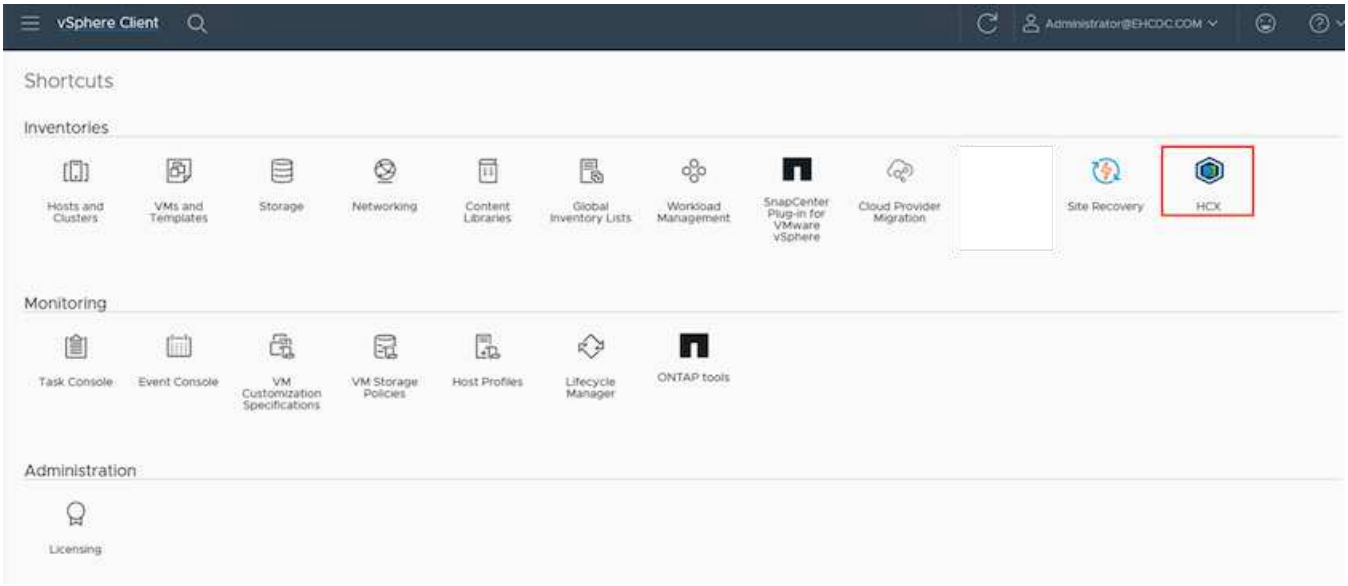
    このプロセスには、プラグインが vCenter Server に追加されるまでに約 10 ～ 20 分かかります。



▼ ステップ **4:** オンプレミスの **VMware HCX** コネクタと **Azure VMware Solution HCX Cloud Manager** をペアリングする

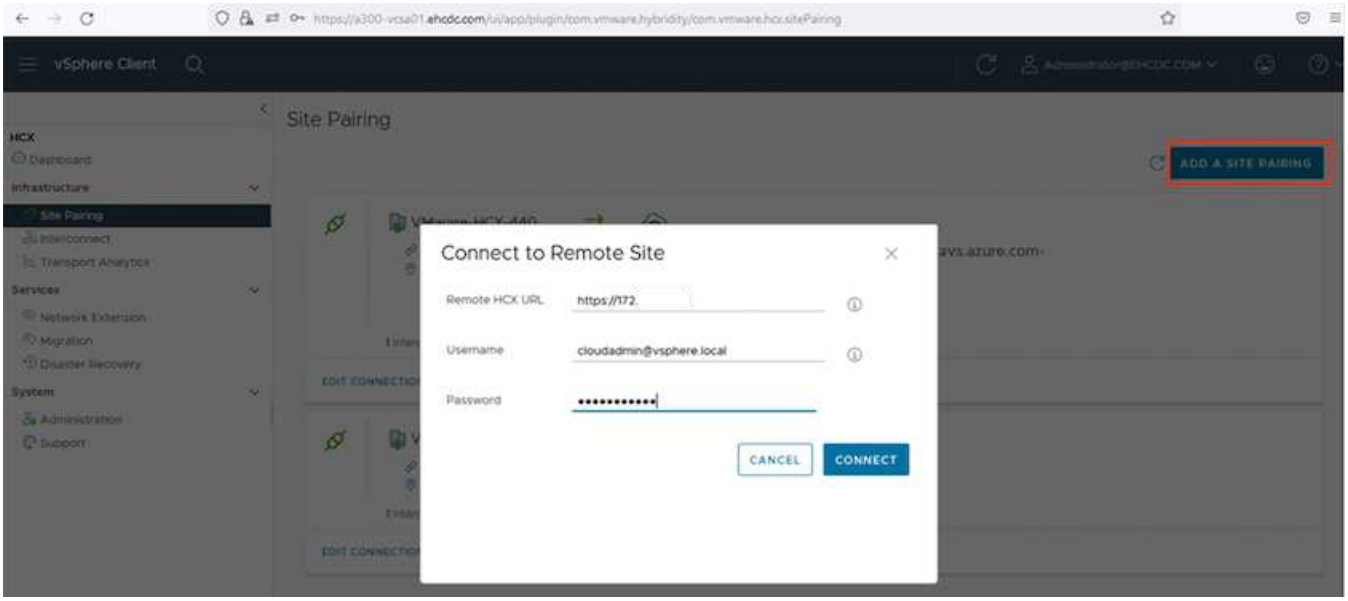
HCX コネクタをオンプレミスと Azure VMware Solution の両方にインストールした後、ペアリングを追加して、Azure VMware Solution プライベート クラウド用にオンプレミスの VMware HCX コネクタを構成します。サイトのペアリングを構成するには、次の手順を実行します。

1. オンプレミスの vCenter 環境と Azure VMware Solution 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の下で、[サイトペアリングを追加]をクリックします。

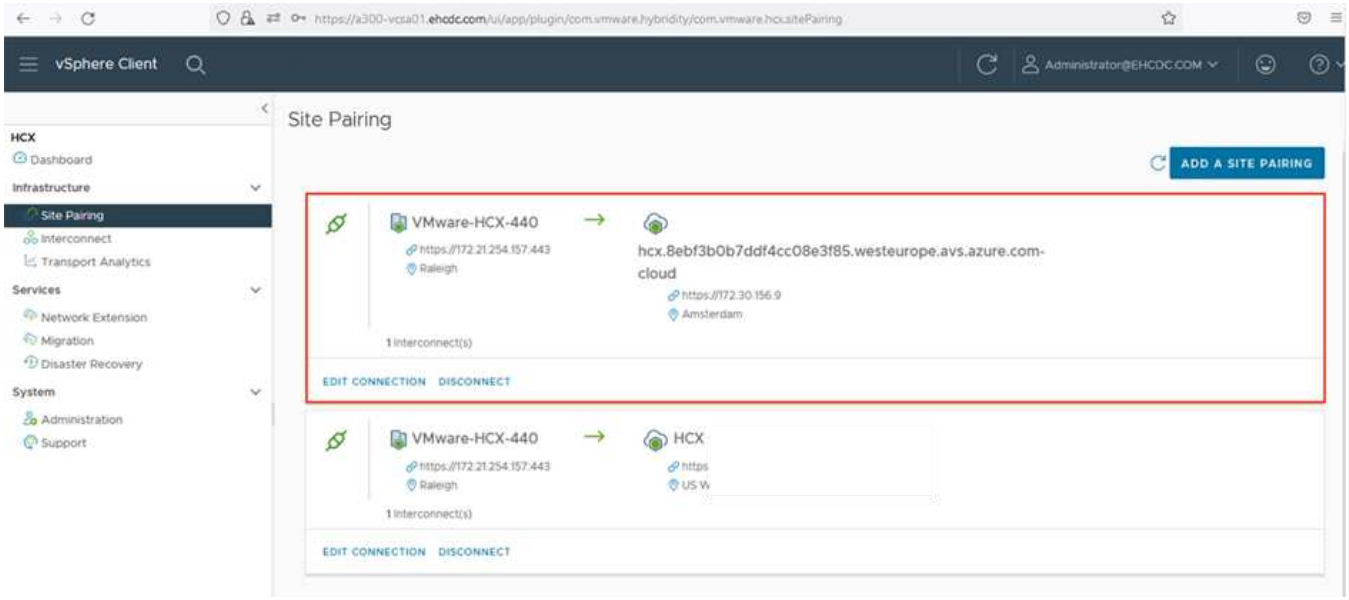
プライベート クラウドにアクセスするための Azure VMware Solution HCX Cloud Manager の URL または IP アドレスと CloudAdmin ロールの資格情報を入力します。



1. *接続*をクリックします。

VMware HCX コネクタは、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 ダッシュボードで利用できるようになります。

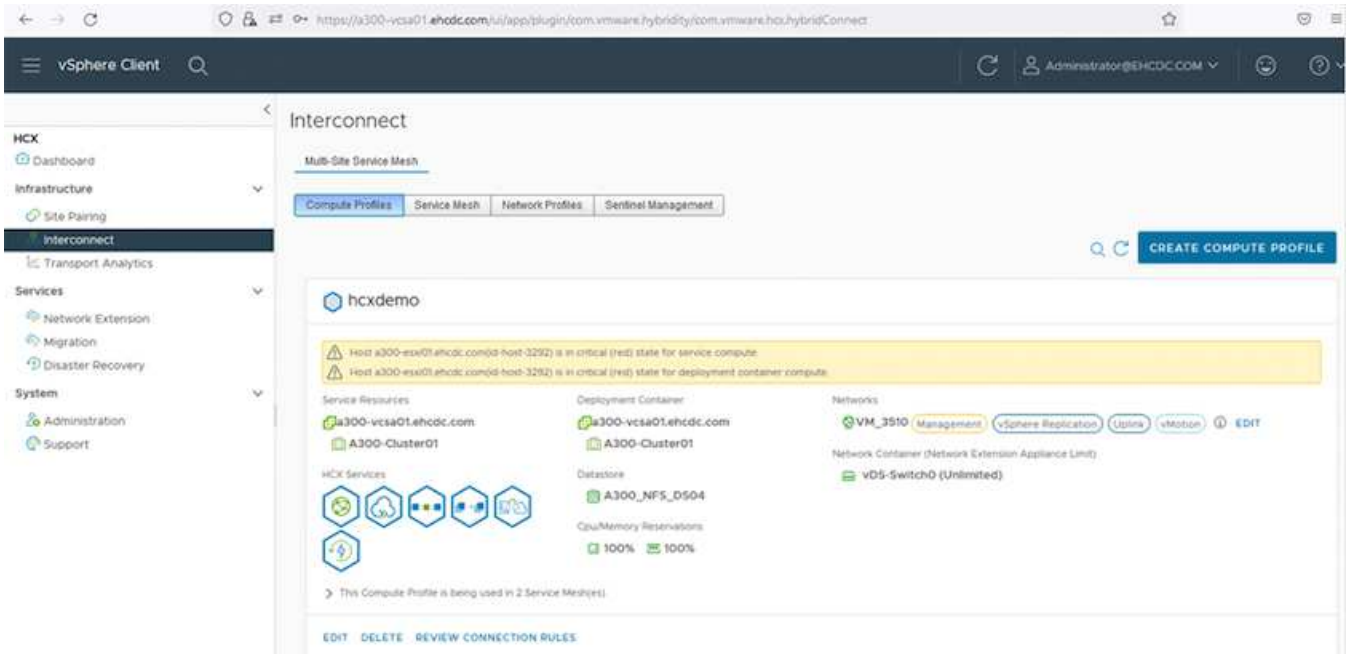


▼ ステップ**5:** ネットワークプロファイル、コンピューティングプロファイル、サービスメッシュを構成する

VMware HCX Interconnect サービス アプライアンスは、インターネット経由およびターゲット サイトへのプライベート接続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ます。相互接続は、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。 Interconnect 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] で、**[**相互接続**] > [**マルチサイト サービス メッシュ**] > [**コンピューティング プロファイル**] > [**コンピューティング プロファイルの作成**]** を選択します。

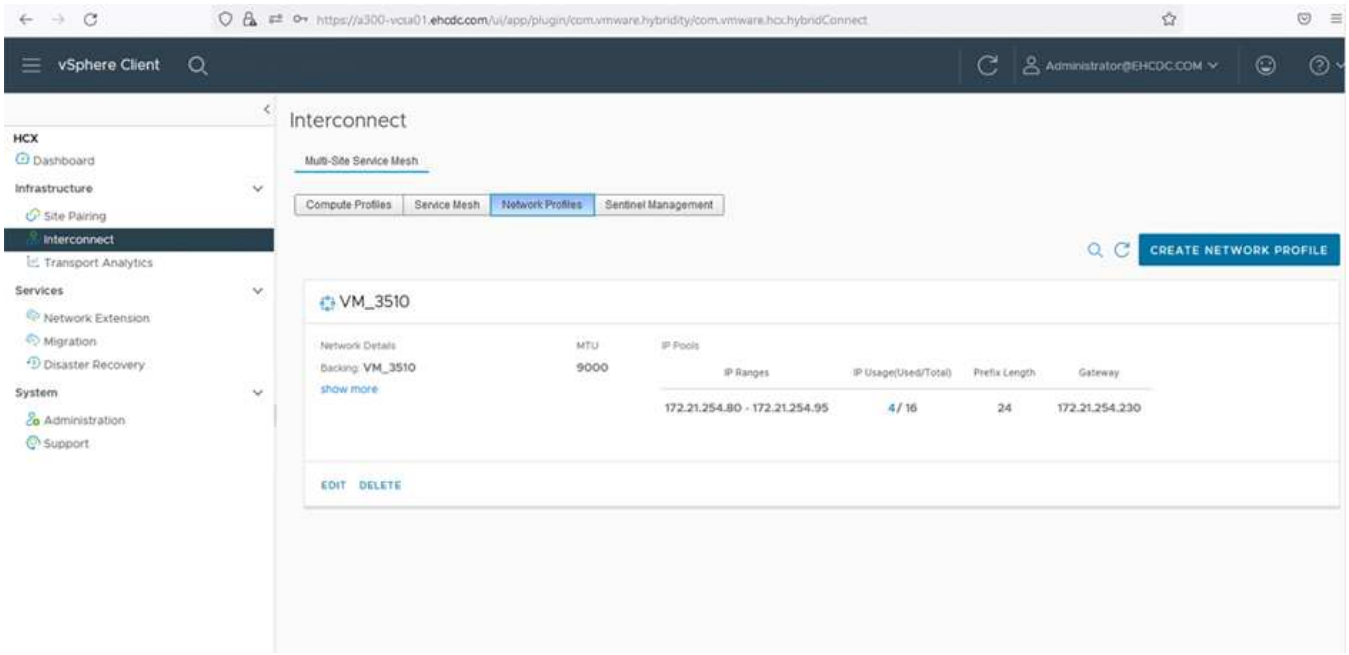
コンピューティング プロファイルは、展開されるアプライアンスや、HCX サービスにアクセス可能な VMware データセンターの部分などの展開パラメータを定義します。



1. コンピューティング プロファイルが作成されたら、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。

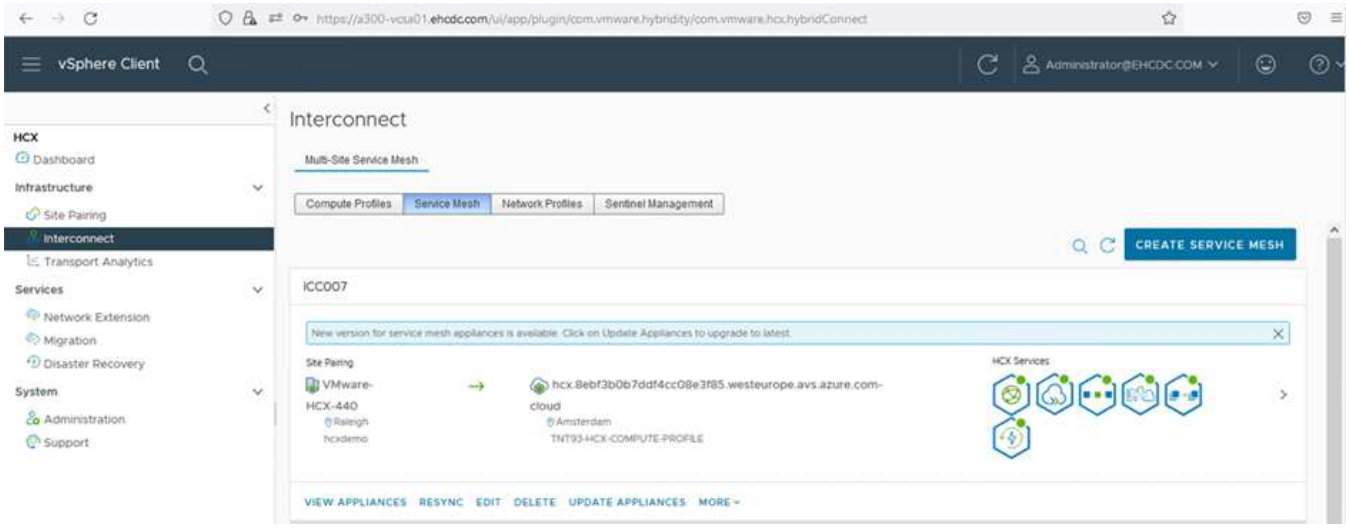
ネットワーク プロファイルは、HCX が仮想アプライアンスに使用する IP アドレスとネットワークの範囲を定義します。

この手順では 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 Interconnect Appliances に割り当てられます。

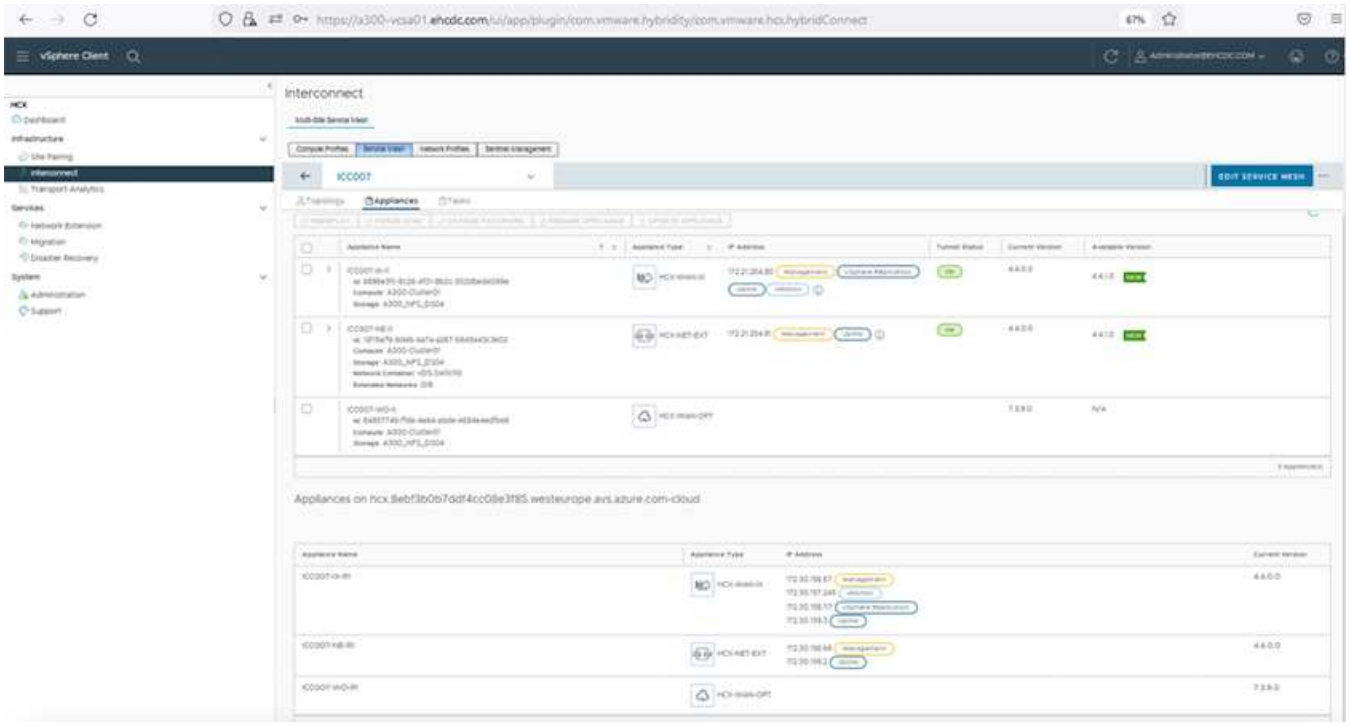


1. この時点で、コンピューティング プロファイルとネットワーク プロファイルが正常に作成されました。
2. **Interconnect** オプション内の **Service Mesh** タブを選択して Service Mesh を作成し、オンプレミスと Azure SDDC サイトを選択します。
3. サービス メッシュは、ローカルおよびリモートのコンピューティングとネットワーク プロファイルのペアを指定します。

このプロセスの一環として、安全なトランスポート ファブリックを作成するために、HCX アプライアンスがソース サイトとターゲット サイトの両方に展開され、自動的に構成されます。



1. これは設定の最終ステップです。デプロイメントが完了するまでに約 30 分かかります。サービス メッシュが構成されると、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、環境が準備されます。



▼ ステップ**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。 HCX 一括移行、HCX vMotion、HCX コールド移行、HCX レプリケーション アシスト vMotion (HCX Enterprise エディションで利用可能)、HCX OS アシスト移行 (HCX Enterprise エディションで利用可能) などの複数の移行テクノロジーを使用して、VMware HCX がアクティブ化されたエンティティ間で VM を移動できます。

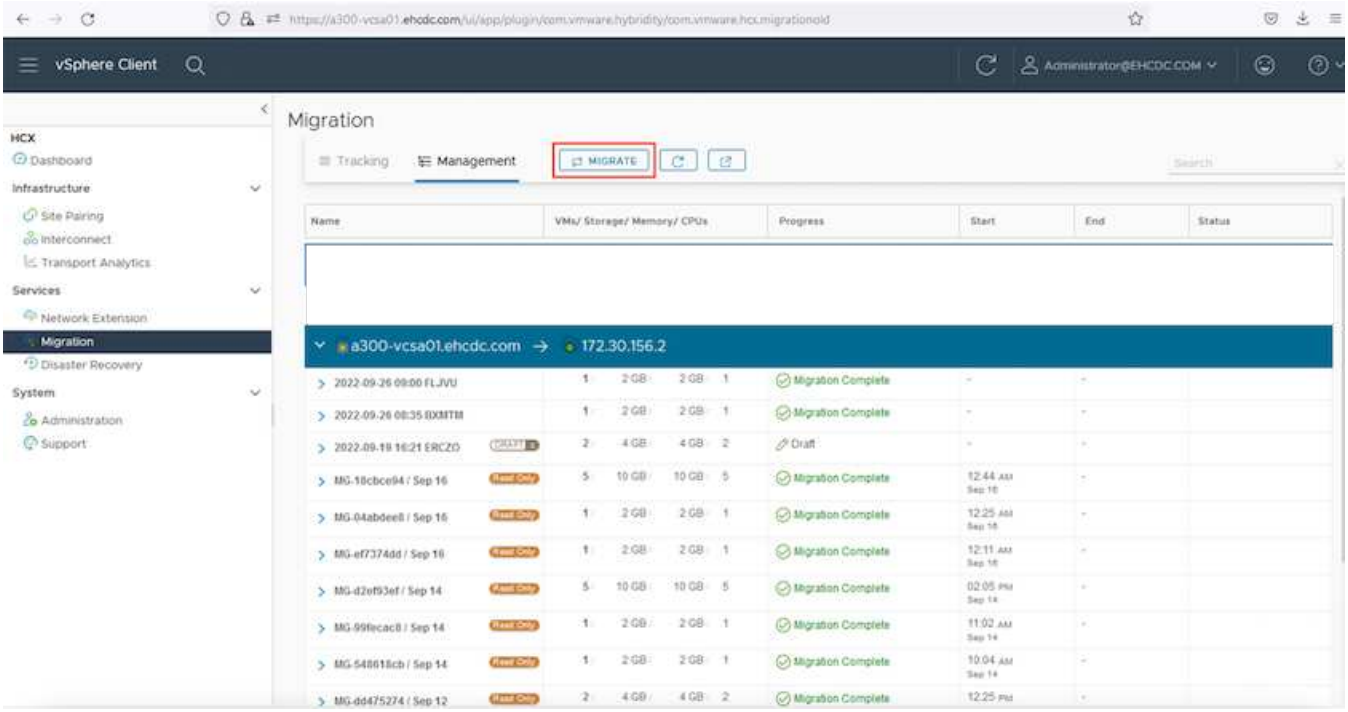
さまざまなHCX移行メカニズムの詳細については、以下を参照してください。 "VMware HCX 移行の種類"。

一括移行

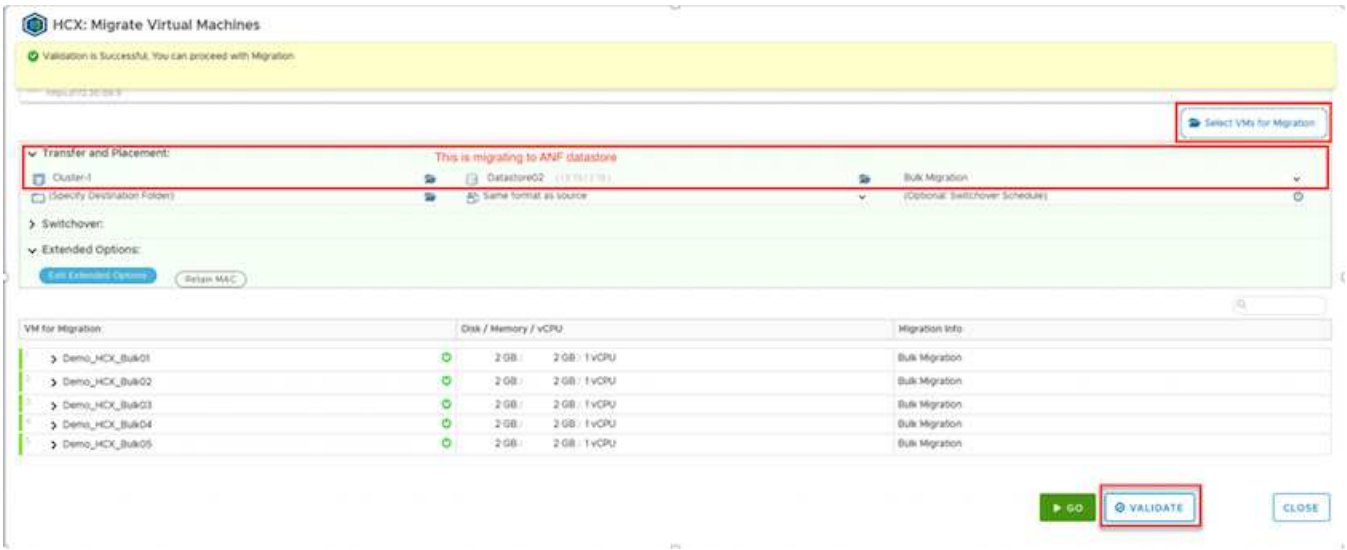
このセクションでは、一括移行のメカニズムについて詳しく説明します。一括移行中、HCX の一括移行機能は vSphere Replication を使用してディスク ファイルを移行し、同時に宛先 vSphere HCX インスタンス上に VM を再作成します。

一括 VM 移行を開始するには、次の手順を実行します。

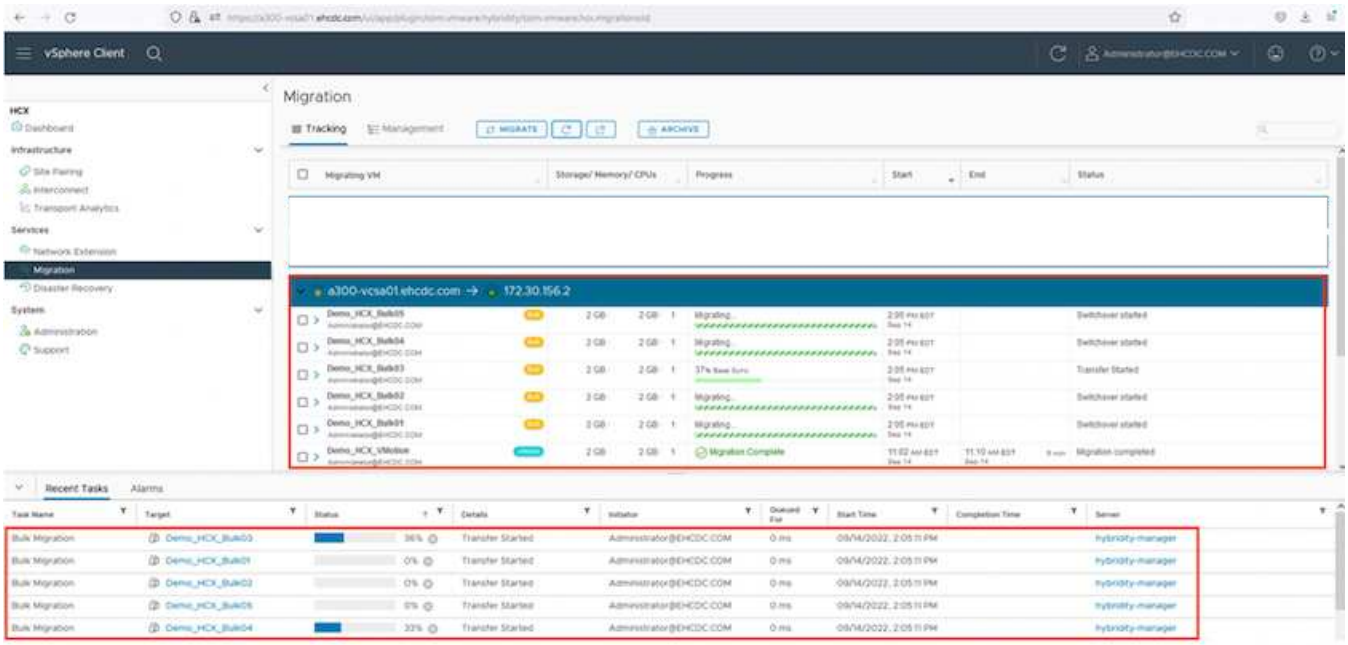
1. サービス > 移行 の 移行 タブにアクセスします。



1. リモート サイト接続 の下で、リモート サイト接続を選択し、ソースと宛先を選択します。この例では、宛先は Azure VMware Solution SDDC HCX エンドポイントです。
2. 移行する**VM**を選択*をクリックします。これにより、オンプレミスのすべての **VM** のリストが提供されます。 **match:value** 式に基づいて **VM** を選択し、[*追加] 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（*クラスター、ストレージ、宛先、および*ネットワーク*）を更新し、*検証*をクリックします。

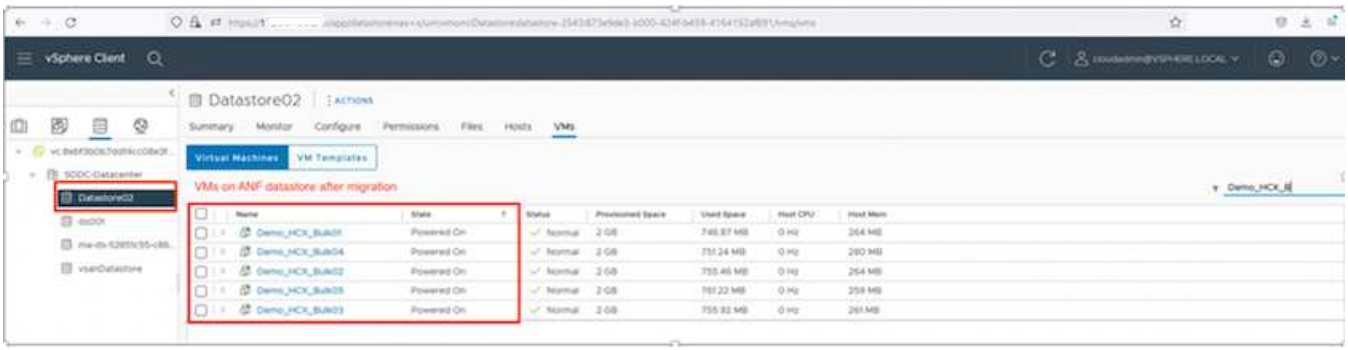


1. 検証チェックが完了したら、[Go] をクリックして移行を開始します。



この移行中に、ターゲット vCenter 内の指定されたAzure NetApp Filesデータストアにプレースホルダー ディスクが作成され、ソース VM ディスクのデータをプレースホルダー ディスクにレプリケーションできるようになります。 HBR はターゲットへの完全同期のためにトリガーされ、ベースラインが完了した後、復旧ポイント目標 (RPO) サイクルに基づいて増分同期が実行されます。完全同期または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限り、切り替え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 にアクセスして移行を検証します。

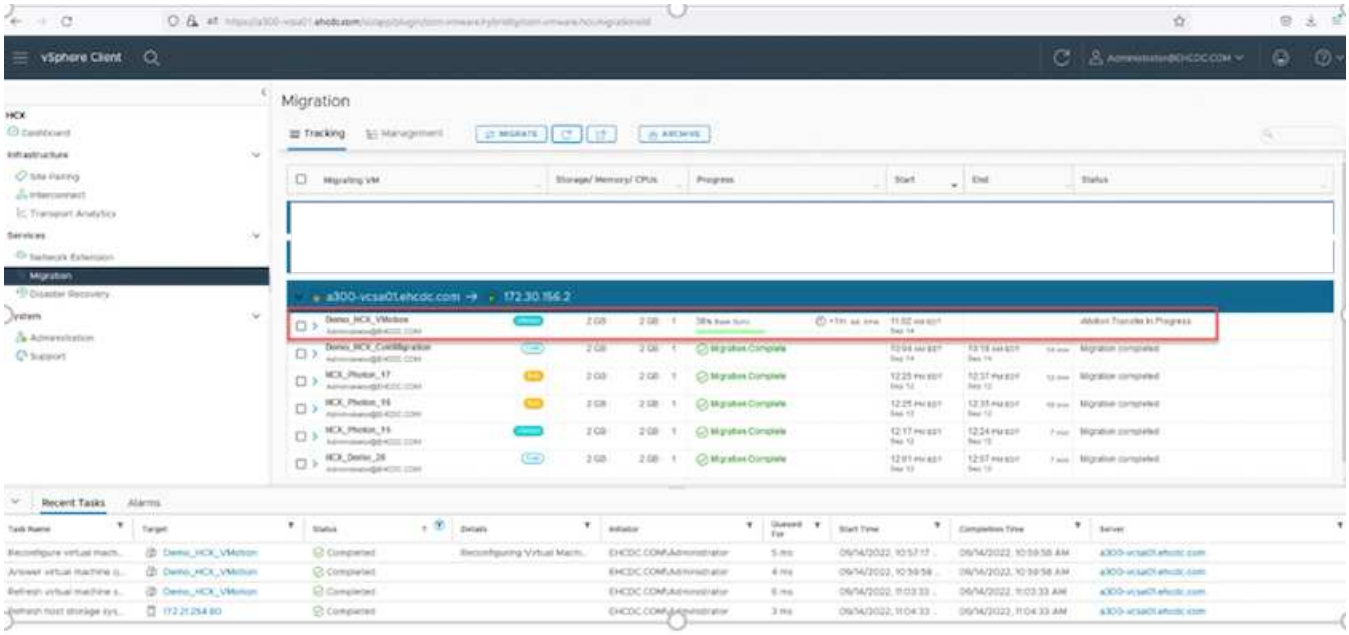


さまざまな移行オプションと、HCX を使用してオンプレミスから Azure VMware Solution にワークロードを移行する方法の詳細については、以下を参照してください。 "VMware HCX 移行の考慮事項" 。

このプロセスについて詳しく知りたい場合は、次のビデオをご覧ください。

HCX を使用したワークロード移行

以下は HCX vMotion オプションのスクリーンショットです。



このプロセスについて詳しく知りたい場合は、次のビデオをご覧ください。

HCX vMotion

移行を処理するために十分な帯域幅が利用可能であることを確認してください。

ターゲット ANF データストアには、移行を処理するのに十分なスペースが必要です。

まとめ

オールクラウドまたはハイブリッド クラウドをターゲットにしていて、データがオンプレミスのあらゆるタイプ/ベンダーのストレージに存在する場合でも、 Azure NetApp Filesと HCX は、データ要件をアプリケーション レイヤーにシームレスにすることで TCO を削減しながら、アプリケーション ワークロードを展開および移行するための優れたオプションを提供します。ユース ケースがどのようなものであっても、Azure VMware Solution とAzure NetApp Filesを併せて選択すると、クラウドのメリットを迅速に実現でき、オンプレミスと複数のクラウドにわたる一貫したインフラストラクチャと運用、ワークロードの双方向の移植性、エンタープライズ レベルの容量とパフォーマンスが得られます。これは、VMware vSphere Replication 、VMware vMotion、またはネットワーク ファイル コピー (NFC) を使用してストレージを接続し、VMware 仮想マシンを移行するために使用される、使い慣れたプロセスと手順と同じです。

まとめ

このドキュメントの主なポイントは次のとおりです。

- Azure VMware Solution SDDC 上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。
- オンプレミスからAzure NetApp Filesデータストアにデータを簡単に移行できます。
- 移行アクティビティ中の容量とパフォーマンスの要件を満たすために、 Azure NetApp Filesデータストアを簡単に拡大および縮小できます。

詳細情報の入手方法

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

- Azure VMware ソリューションのドキュメント

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

- Azure NetApp Files のドキュメント

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

- VMware HCX 移行の考慮事項

"https://learn.microsoft.com/en-us/azure/azure-vmware/architecture-migrate"

GCP/GCVE 向けNetApp

Google Cloud Platform GCVE 向けNetApp の機能

NetAppが Google Cloud Platform (GCP) Google Cloud VMware Engine (GCVE) にもたらす機能について詳しく説明します。ゲスト接続ストレージ デバイスまたは補助的な NFS データストアとしてのNetAppから、ワークフローの移行、クラウドへの拡張/バースト、バックアップ/リストア、災害復旧まで、さまざまな機能について説明します。

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。

- "GCP での GCVE の設定"
- "GCVE 向けNetAppストレージ オプション"
- "NetApp / VMware クラウド ソリューション"

GCP での GCVE の設定

オンプレミスの場合と同様に、VM の作成と移行のための本番環境を正常に構築するには、クラウド ベースの仮想化環境を計画することが重要です。

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

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

セットアッププロセスは次の手順に分けられます。

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

詳細を表示"GCVEの設定手順"。

GCVE 向けNetAppストレージ オプション

NetAppストレージは、GCP GCVE 内で、仮想接続として、または補助的な NFS データストアとしてなど、さまざまな方法で利用できます。

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

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

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

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

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

ソリューションのユースケース

NetAppおよび VMware クラウド ソリューションを使用すると、多くのユース ケースを Azure AVS に簡単に展開できます。VMware が定義したクラウド領域ごとに、次のようなユース ケースが定義されています。

- 保護（災害復旧とバックアップ/復元の両方を含む）
- 拡張
- 移行

"Google Cloud GCVE 向けNetAppソリューションを参照"

GCP/GCVE 上のワークロードを保護する

NetApp SnapCenterと Veeam レプリケーションによるアプリケーション整合性のある災害復旧

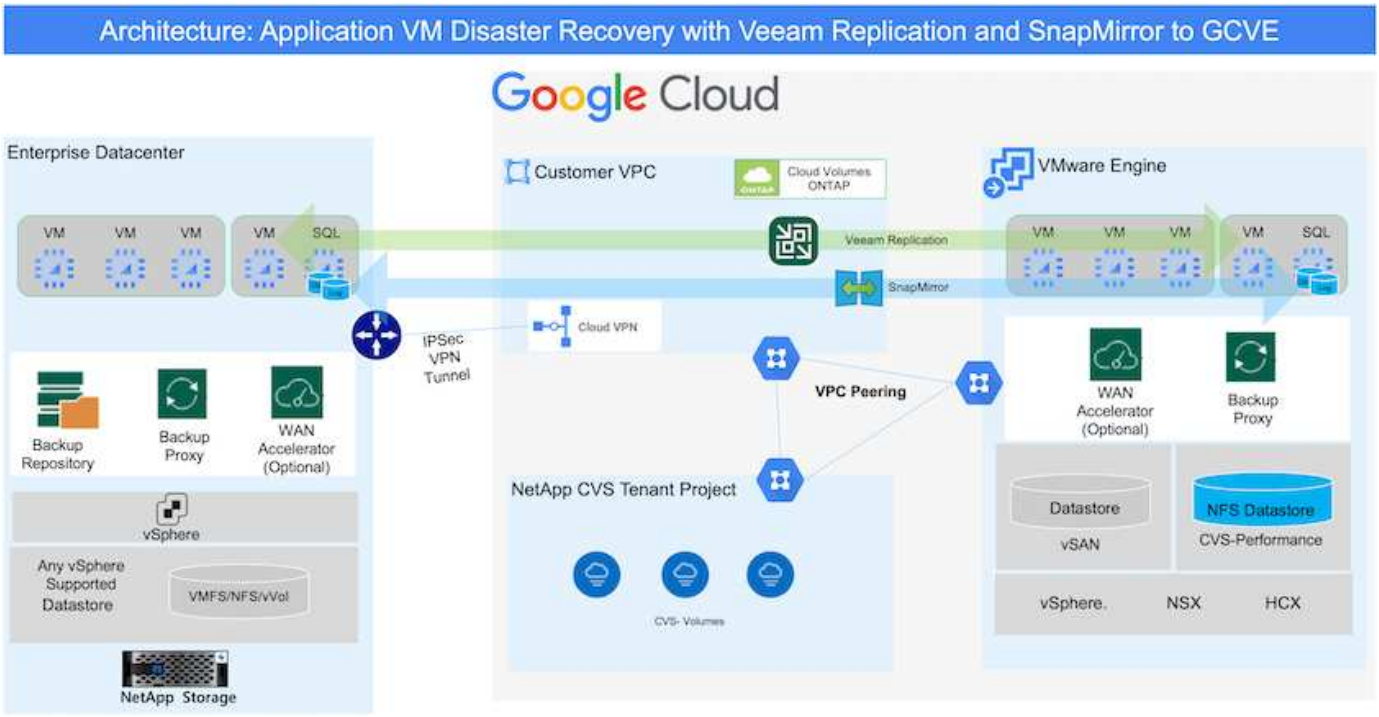
クラウドへの災害復旧は、サイトの停止やランサムウェアなどのデータ破損イベントからワークロードを保護する、回復力がありコスト効率に優れた方法です。 NetApp SnapMirror を使用すると、ゲスト接続ストレージを使用するオンプレミスの VMware ワークロードを、Google Cloud で実行されているNetApp Cloud Volumes ONTAPに複製できます。

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 向けの効果的な災害復旧ソリューションを求めています。災害時の復旧には、既存のバックアップ ソリューションを使用する企業が多くあります。多くの場合、このソリューションは RTO を増加させ、顧客の期待を満たしません。 RPO と RTO を削減するために、ネットワーク接続と適切な権限を持つ環境が利用可能であれば、オンプレミスから GCVE まで Veeam VM レプリケーションを利用できます。注意: Veeam VM レプリケーションは、ゲスト VM 内の iSCSI や NFS マウントなどの VM ゲスト接続ストレージ デバイスを保護しません。これらを別々に保護する必要があります。

SQL VM のアプリケーション整合性のあるレプリケーションと RTO の削減を実現するために、 SnapCenter を使用して SQL データベースとログ ボリュームの snapmirror 操作を調整しました。

このドキュメントでは、 NetApp SnapMirror、Veeam、Google Cloud VMware Engine（GCVE）を使用した災害復旧の設定と実行の手順を詳しく説明します。



前提

このドキュメントでは、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) に焦点を当てており、オンプレミス環境でアプリケーション整合性のあるバックアップにSnapCenterを使用していることを前提としています。

> このドキュメントは、サードパーティのバックアップまたはリカバリ ソリューションに適用されます。環境で使用されているソリューションに応じて、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 ポリシーを作成します。

オンプレミス環境と Google Cloud ネットワーク間の接続には、専用相互接続や Cloud VPN などの接続オプションを使用します。セグメントは、オンプレミスの VLAN 設計に基づいて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 に接続するには複数のオプションがあるため、このドキュメントでは具体的なワークフロー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ソリューションの導入

ソリューション展開の概要

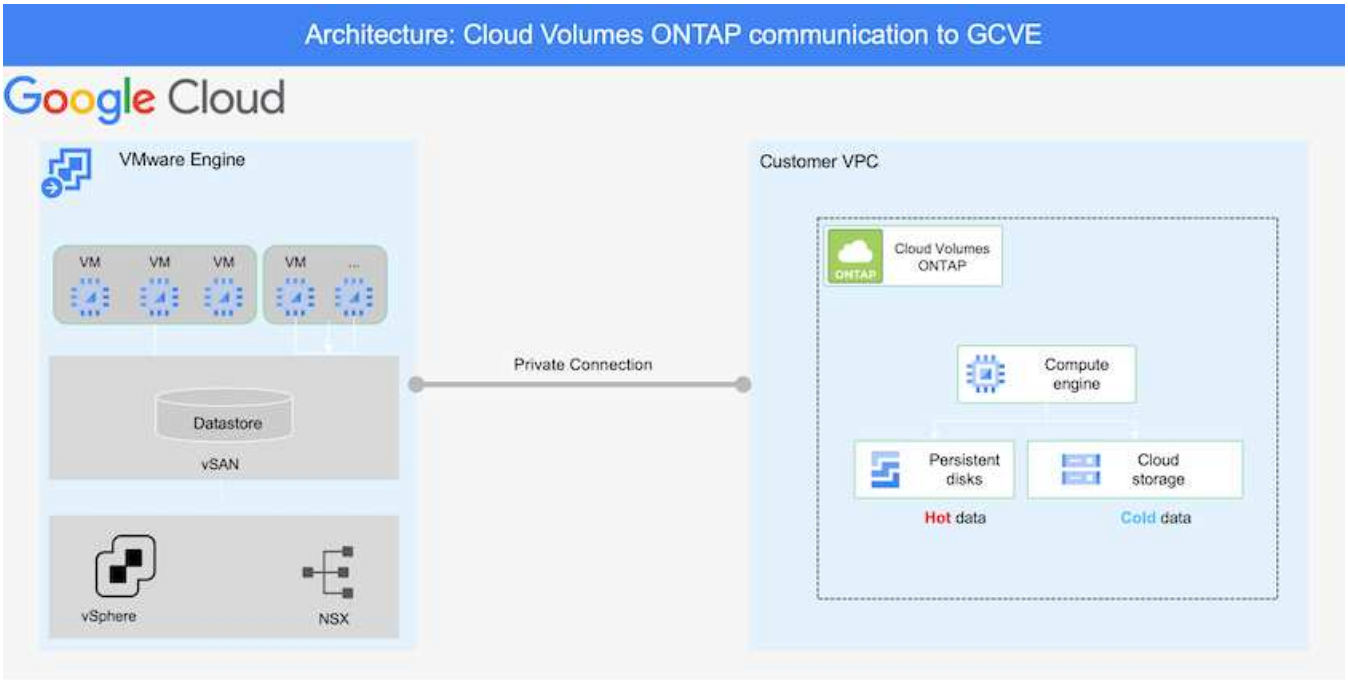
1. 必要な RPO 要件に従って、 SnapCenterを使用してアプリケーション データがバックアップされていることを確認します。

2. 適切なサブスクリプションと仮想ネットワーク内で、NetApp Consoleを使用して適切なインスタンスサイズのCloud Volumes ONTAPをプロビジョニングします。
   a. 関連するアプリケーション ボリュームに対してSnapMirrorを構成します。
   b. スケジュールされたジョブの後にSnapMirror の更新をトリガーするように、 SnapCenterのバックアップ ポリシーを更新します。
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、NetApp Console 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 と 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で起動します。
5. プライマリ サイトが回復された後、 SnapMirror を逆再同期して、保護されたサイトへのフェイルバックを呼び出します。

導入環境の詳細

▼ **Google Cloud** で **CVO** を構成し、ボリュームを **CVO** に複製する

最初のステップは、Google Cloud でCloud Volumes ONTAP を構成することです ("最高経営責任者" ）を作成し、必要な頻度とスナップショット保持期間で、必要なボリュームをCloud Volumes ONTAPに複製します。



SnapCenterの設定とデータの複製に関するサンプルの手順については、以下を参照してください。"SnapCenterでレプリケーションを設定する"

SnapCenterによる SQL VM 保護のレビュー

▼ **GCVE**ホストと**CVO**データアクセスを構成する

SDDC を展開する際に考慮すべき 2 つの重要な要素は、GCVE ソリューション内の SDDC クラスターのサ

イズと、SDDC をサービスに維持する期間です。災害復旧ソリューションに関するこれら 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、最小 3 台のホストから、本格的な展開のマルチホスト クラスターまで、さまざまな規模にすることができます。

Google Cloud NetApp Volumes for NFS データストアとCloud Volumes ONTAP for SQL データベースおよびログは任意の VPC にデプロイできますが、GCVE は NFS データストアをマウントし、VM を iSCSI LUN に接続するためにその VPC へのプライベート接続が必要です。

GCVE SDDCを構成するには、以下を参照してください。"Google Cloud Platform (GCP) に仮想化環境をデプロイして構成する" 。前提条件として、接続が確立された後、GCVE ホスト上にあるゲスト 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 が適切に構成されたら、Veeam レプリケーション機能を使用し、アプリケーション ボリュームのコピーにSnapMirrorを活用して、オンプレミスのCloud Volumes ONTAPの GCVE (アプリケーション VMDK を持つ VM とゲスト内ストレージを持つ VM) へのリカバリを自動化するように Veeam の構成を開始します。

▼ **Veeam**コンポーネントをインストールする

展開シナリオに基づいて、展開する必要がある Veeam バックアップ サーバー、バックアップ リポジトリ、およびバックアップ プロキシ。このユースケースでは、Veeam のオブジェクト ストアを展開する必要はなく、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/vsphere/replication_components.html?ver=120["インストール手順については、Veeamのドキュメントを参照してください。"]詳細については、"Veeam Replicationによる移行"

▼ **Veeam** で **VM** レプリケーションを設定する

オンプレミスの vCenter と GCVE vCenter の両方を 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のセットアップ"ウィザードのゲスト処理手順では、アプリケーション対応のバックアップとリカバリにSnapCenterを利用するため、アプリケーション処理を無効にすることを選択します。

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

このソリューションの利点

- SnapMirrorの効率的で復元力のあるレプリケーションを使用します。
- ONTAPスナップショット保持を使用して、利用可能な任意の時点に回復します。
- 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手順から、数百から数千の VM を復旧するために必要なすべての手順を完全に自動化できます。
- SnapCenter は、複製されたボリュームを変更しないクローン作成メカニズムを使用します。
  - これにより、ボリュームとスナップショットのデータ破損のリスクを回避できます。
  - 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/テスト、セキュリティ テスト、パッチおよびアップグレード テスト、修復テストなど、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 サイト上の VM IP アドレスを変更できます。

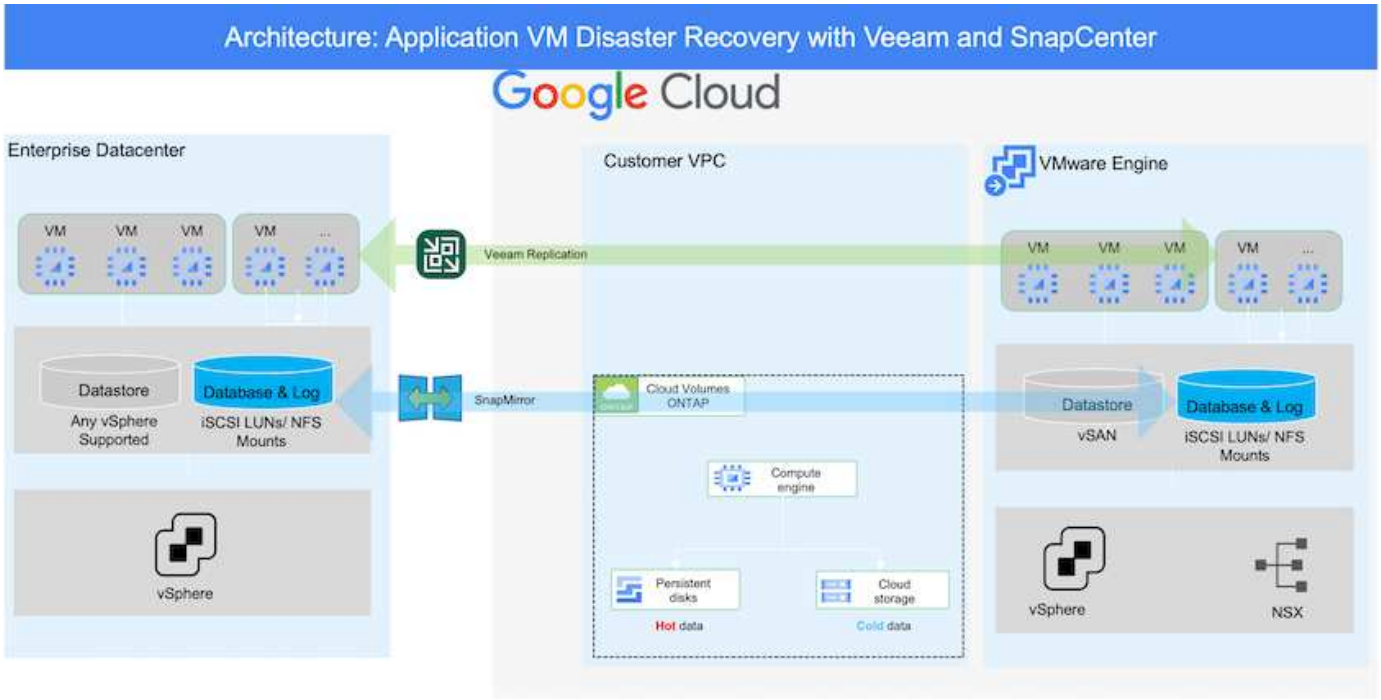
SnapCenter、 Cloud Volumes ONTAP 、Veeam Replication を使用したアプリケーションの災害復旧

クラウドへの災害復旧は、サイトの停止やランサムウェアなどのデータ破損イベントからワークロードを保護する、回復力がありコスト効率に優れた方法です。 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に複製できます。

概要

これはアプリケーション データをカバーしますが、実際の VM 自体についてはどうでしょうか。災害復旧は、仮想マシン、VMDK、アプリケーション データなど、すべての依存コンポーネントをカバーする必要があります。これを実現するために、 SnapMirror をVeeam と併用することで、VM VMDK に 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。

このドキュメントでは、 NetApp SnapMirror、Veeam、Google Cloud VMware Engine（GCVE）を使用した災害復旧の設定と実行の手順を詳しく説明します。



前提

このドキュメントでは、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) に焦点を当てており、オンプレミス環境でアプリケーション整合性のあるバックアップにSnapCenterを使用していることを前提としています。

> このドキュメントは、サードパーティのバックアップまたはリカバリ ソリューションに適用されます。環境で使用されているソリューションに応じて、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 ポリシーを作成します。

オンプレミス環境と Google Cloud ネットワーク間の接続には、専用相互接続や Cloud VPN などの接続オプションを使用します。セグメントは、オンプレミスの VLAN 設計に基づいて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 に接続するには複数のオプションがあるため、このドキュメントでは具体的なワークフロー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ソリューションの導入

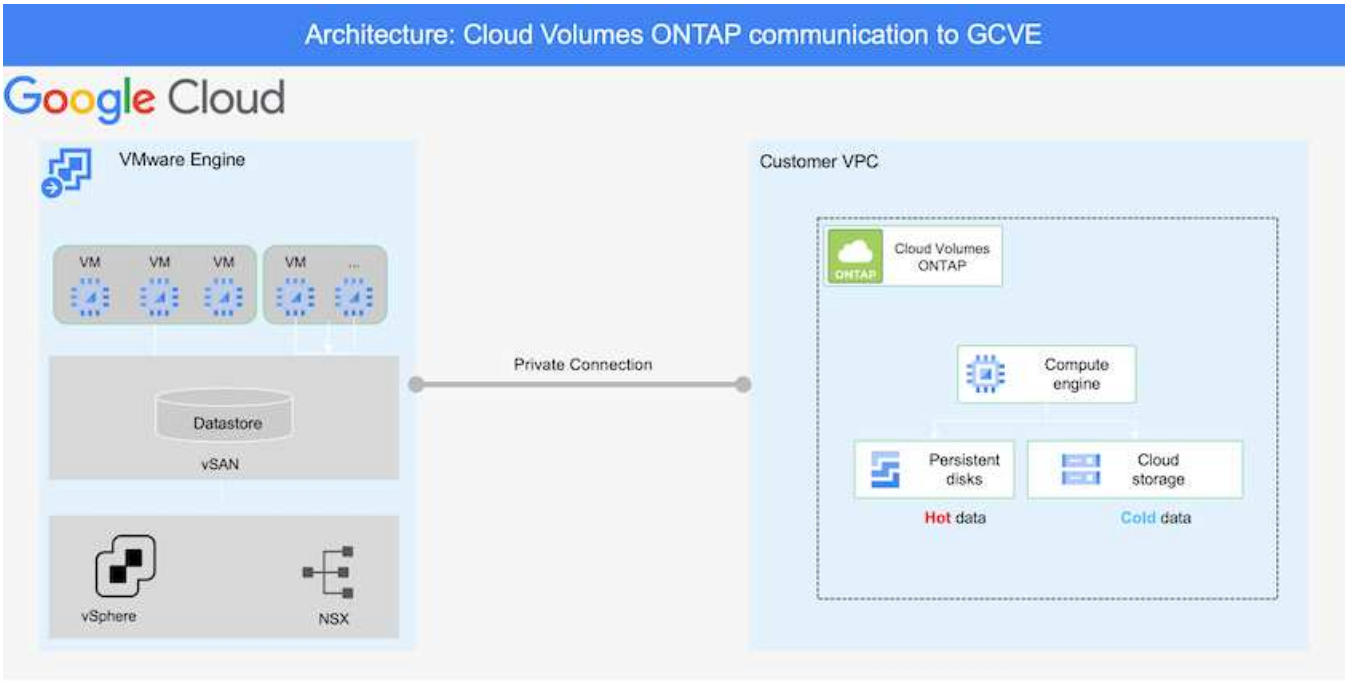
ソリューション展開の概要

1. 必要な RPO 要件に従って、 SnapCenterを使用し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ます。
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、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. 関連するアプリケーション ボリュームに対してSnapMirrorを構成します。
   b. スケジュールされたジョブの後にSnapMirror の更新をトリガーするように、 SnapCenterのバックアップ ポリシーを更新します。
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、Cloud Manager を使用してSnapMirror関係を解除し、Veeam を使用して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 と 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で起動します。
5. プライマリ サイトが回復された後、 SnapMirror を逆再同期して、保護されたサイトへのフェイルバックを呼び出します。

導入環境の詳細

▼ **Google Cloud** で **CVO** を構成し、ボリュームを **CVO** に複製する

最初のステップは、Google Cloud でCloud Volumes ONTAP を構成することです ("最高経営責任者" ）を作成し、必要な頻度とスナップショット保持期間で、必要なボリュームをCloud Volumes ONTAPに複製します。



SnapCenterの設定とデータの複製に関するサンプルの手順については、以下を参照してください。"SnapCenterでレプリケーションを設定する"

SnapCenterでレプリケーションを設定する

▼ **GCVE**ホストと**CVO**データアクセスを構成する

SDDC を展開する際に考慮すべき 2 つの重要な要素は、GCVE ソリューション内の SDDC クラスターのサイズと、SDDC をサービスに維持する期間です。災害復旧ソリューションに関するこれら 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、最小 3 台のホストから、本格的な展開のマルチホスト クラスターまで、さまざまな規模にすることができます。

Cloud Volumes ONTAP は任意の VPC にデプロイできますが、VM を iSCSI LUN に接続するために、GCVE はその VPC へのプライベート接続を持っている必要があります。

GCVE SDDCを構成するには、以下を参照してください。"Google Cloud Platform (GCP) に仮想化環境をデプロイして構成する" 。前提条件として、接続が確立された後、GCVE ホスト上にあるゲスト 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 が適切に構成されたら、Veeam レプリケーション機能を使用し、アプリケーション ボリュームのコピーにSnapMirrorを活用して、オンプレミスのCloud Volumes ONTAPの GCVE (アプリケーション VMDK を持つ VM とゲスト内ストレージを持つ VM) へのリカバリを自動化するように Veeam の構成を開始します。

▼ **Veeam**コンポーネントをインストールする

展開シナリオに基づいて、展開する必要がある Veeam バックアップ サーバー、バックアップ リポジトリ、およびバックアップ プロキシ。このユースケースでは、Veeam のオブジェクト ストアを展開する必要はなく、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のドキュメントを参照してください。"]

▼ **Veeam** で **VM** レプリケーションを設定する

オンプレミスの vCenter と GCVE vCenter の両方を 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のセットアップ"ウィザードのゲスト処理手順では、アプリケーション対応のバックアップとリカバリにSnapCenterを利用するため、アプリケーション処理を無効にすることを選択します。

vSphere VM レプリケーションジョブのセットアップ

▼ **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

このソリューションの利点

- SnapMirrorの効率的で復元力のあるレプリケーションを使用します。
- ONTAPスナップショット保持を使用して、利用可能な任意の時点に回復します。
- 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手順から、数百から数千の VM を復旧するために必要なすべての手順を完全に自動化できます。
- SnapCenter は、複製されたボリュームを変更しないクローン作成メカニズムを使用します。
  - これにより、ボリュームとスナップショットのデータ破損のリスクを回避できます。
  - 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/テスト、セキュリティ テスト、パッチおよびアップグレード テスト、修復テストなど、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 サイト上の VM IP アドレスを変更できます。

Veeam Replication と**Google Cloud NetApp Volumes**データストアを使用して **Google Cloud VMware Engine** への災害復旧を行う

危機的状況にある企業にとって、包括的な災害復旧計画は非常に重要です。多くの組織は、日常業務と災害復旧にクラウド コンピューティングを活用しています。この積極的なアプローチにより、コストのかかる業務の中断を軽減または排除できます。

この記事では、Veeam Backup & Replication を使用して、 Google Cloud NetApp Volumes （NetApp Volumes ）を備えた Google Cloud VMware Engine（GCVE）へのオンプレミス VMware VM の災害復旧を設定する方法について説明します。

概要

Google Cloud NetApp Volumes は、 Google Cloud で利用できる Google とNetAppのストレージ サービスです。 NetApp Volumes サービスは、高パフォーマンスの NFS/SMB ストレージを提供します。 VMware 認定のNetApp Volumes NFS ストレージは、GCVE 内の ESXi ホストの外部データストアとして使用できます。ユーザーは、GCVE プライベート クラウドとNetApp Volumes プロジェクトの間にピアリング接続を確立する必要があります。リージョン内でのストレージ アクセスによるネットワーク料金は発生しません。ユーザーは、Google Cloud コンソールでNetApp Volumes ボリュームを作成し、ボリュームをデータストアとして ESXi ホストにマウントする前に削除保護を有効にすることができます。

NetApp Volumes ベースの NFS データストアは、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 ソリューションを使用してオンプレミスからデータを複製するために使用できます。 NetApp Volumes 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に多数の ESXi ホストを備えた Google Cloud VMware Engine（GCVE）ベースの SDDC を構築する代わりに、コストを最適化した導入が可能になります。このアプローチは「パイロット ライト クラスター」と呼ばれます。パイロット ライト クラスターは、最小限の GCVE ホスト構成 (3 台の GCVE ESXi ホスト) とNetApp Volumes データストアの容量を組み合わせ

たもので、容量要件を満たすための独立したスケーリングを可能にします。

目的は、フェイルオーバーを管理するためのコア コンポーネントのみを使用して、コスト効率の高い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 クラスターは、フェイルオーバーが発生した場合に拡張して GCVE ホストを追加できます。フェイルオーバーが解決され、通常の運用が再開されると、パイロット ライト クラスターは規模を縮小し、低コストの運用モードに戻ることができます。

この文書の目的

この記事では、Google Cloud NetApp Volumesデータストアを Veeam Backup & Replication と併用し、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 の GCVE への災害復旧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。仮想マシンが複製されると、Veeam Backup & Replication は、ターゲットの GCVE SDDC クラスター上にネイティブ VMware vSphere 形式で仮想マシンの正確なコピーを作成します。 Veeam Backup & Replication は、コピーを元の VM と同期した状態に保ちます。レプリケーションでは、DR サイトに起動準備完了状態の VM のコピーがマウントされるため、最適な復旧時間目標 (RTO) が実現されます。

このレプリケーション メカニズムにより、災害が発生した場合でも GCVE でワークロードを迅速に開始できるようになります。 Veeam Backup & Replication ソフトウェアは、WAN および低速接続を介したレプリケーションのトラフィック転送も最適化します。さらに、重複したデータ ブロック、ゼロ データ ブロック、スワップ ファイル、および「除外された VM ゲスト OS ファイル」も除外します。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するのを防ぐには、WAN アクセラレータとネットワーク スロットリング ルールを利用できます。

Veeam Backup & Replication のレプリケーション プロセスはジョブ駆動型であり、レプリケーション ジョブを構成することによってレプリケーションが実行されます。災害が発生した場合、フェイルオーバーをトリガーしてレプリカ コピーにフェイルオーバーすることで VM を復旧できます。フェイルオーバーが実行されると、複製された 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、またはその既知の正常な復元ポイントのいずれか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の回復や分離されたテストが可能になります。 Veeam Backup & Replication は、さまざまな災害復旧シナリオを処理するための複数のオプションを提供します。

ソリューションの概要

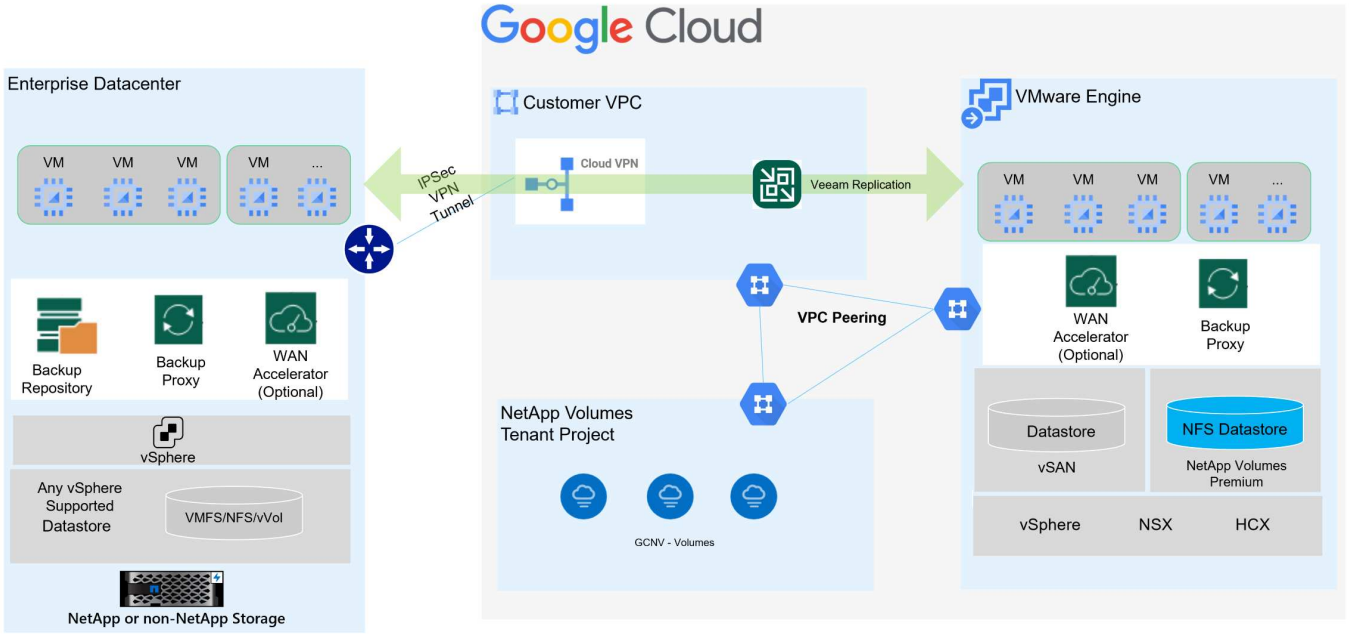
このソリューションは、次の大まかな手順をカバーします。

1. Google Cloud NetApp Volumesを使用して NFS ボリュームを作成する
2. GCP プロセスに従って、 NetApp Volumes NFS ボリュームから GCVE データストアを作成します。
3. Veeam Backup & 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します。
5. 災害イベントが完了し、プライマリ サイトが稼働したら、本番環境の VM に切り替えます。

> NetApp Volumes でボリュームを作成し、GCVE データストアとして使用する場合、NFS v3 のみがサポートされます。

NetApp Volumes NFSボリュームをGCVEのデータストアとして使用する方法の詳細については、以下を参照してください。 "Google Cloud NetApp Volumesでホストされる vSphere データストアとして NFS ボリュームを使用する" 。

次の図は、このドキュメントで紹介されているソリューションのアーキテクチャを示しています。推奨されるベスト プラクティスは、オンプレミス サイトと GCVE SDDC の両方に Veeam Backup & Replication サーバーを配置することです。バックアップとリカバリはオンプレミスの Veeam サーバーによって実行および管理され、レプリケーションは GCVE SDDC 内の Veeam サーバーによって管理されます。このアーキテクチャは、プライマリ データセンターで障害が発生した場合に最高の可用性を提供します。



GCVE および**NetApp Volumes** データストアへの **Veeam** レプリケーションの前提条件

このソリューションには、次のコンポーネントと構成が必要です。

1. NetApp Volumes には、作成する NFS ボリュームを収容するのに十分な空き容量を備えたストレージ プールが用意されています。
2. Veeam Backup and 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。
3. Veeam Backup & Replication バックアップ VM がソースとターゲットの GCVE SDDC クラスターに接続されていることを確認します。
4. Veeam Backup & Replication バックアップ VM が、ソース GCVE クラスターとターゲット GCVE クラスターの両方で Veeam Proxy サーバー VM に接続されていることを確認します。
5. バックアップ サーバーは、短い名前を解決し、ソース vCenter とターゲット vCenter に接続できる必要があります。

ユーザーは、VMware Engine Cloud コンソール UI 内の VPC ネットワーク ピアリングまたはプライベート接続ページを使用して、GCVE プライベート クラウドとNetApp Volumes プロジェクト間のピアリング接続を確立する必要があります。



Veeamでは、GCVEのvCenterサーバーをVeeam Backup and Replicationのインベントリに追加する際に、昇格された権限を持つGCVEソリューションユーザーアカウントが必要です。詳細については、Google Cloud Platform（GCP）のドキュメントを参照してください "VMware Engine 権限の昇格"。

詳細については、 "考慮事項と制限事項" Veeam Backup & Replication のドキュメント。

導入手順

次のセクションでは、 Google Cloud NetApp Volumes を使用して NFS データストアを作成してマウントし、Veeam Backup and Replication を使用してオンプレミス データセンターと Google Cloud VMware Engine 間の完全な障害復旧ソリューションを実装するための導入手順について説明します。

GCVE 用のNetApp Volumes NFS ボリュームとデータストアを作成する

参照 "Google Cloud NetApp Volumesでホストされる vSphere データストアとして NFS ボリュームを使用する"GCVE のデータストアとしてGoogle Cloud NetApp Volumes を使用する方法の概要をご覧ください。

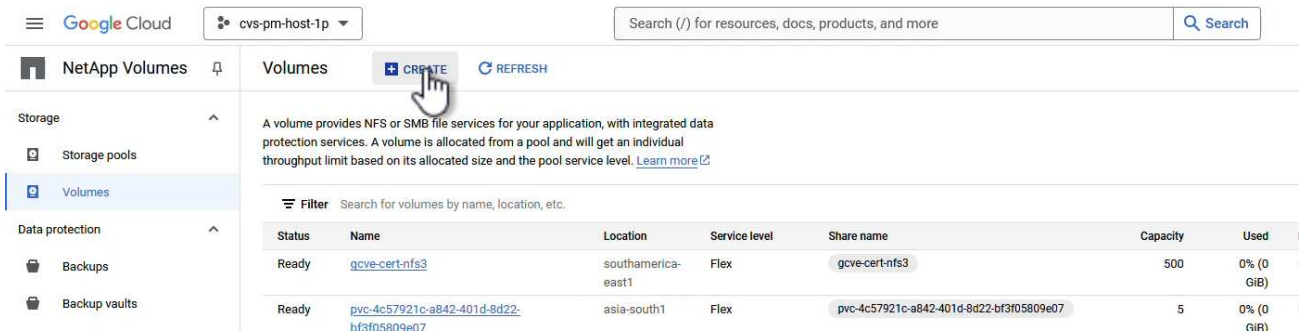
NetApp Volumes を使用して GCVE 用の NFS データストアを作成して使用するには、次の手順を実行します。

▼ NetApp Volumes NFSボリュームを作成する

Google Cloud NetApp Volumes には、 Google Cloud Platform (GCP) コンソールからアクセスします。

参照 "ボリュームの作成"この手順の詳細については、 Google Cloud NetApp Volumes のドキュメントをご覧ください。

1. ウェブブラウザで、 https://console.cloud.google.com/ GCP コンソールにログインします。開始するには、* NetApp Volumes* を検索してください。
2. * NetApp Volumes* 管理インターフェースで、作成 をクリックして NFS ボリュームの作成を開始します。

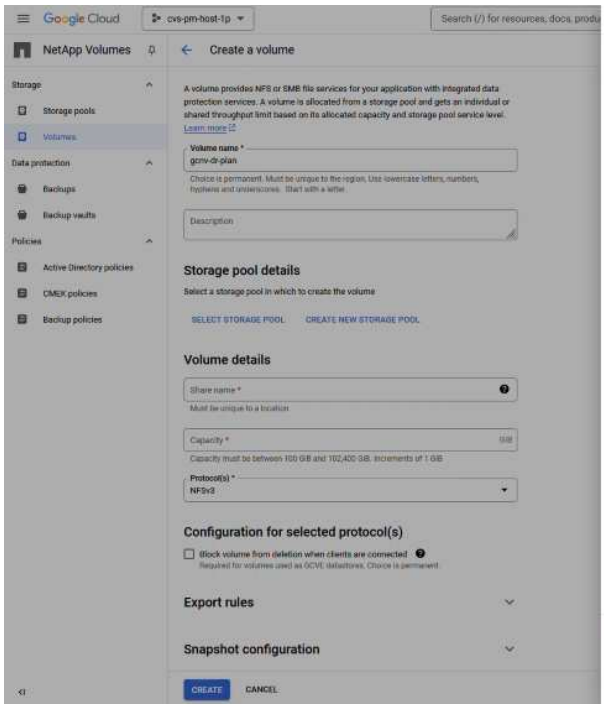


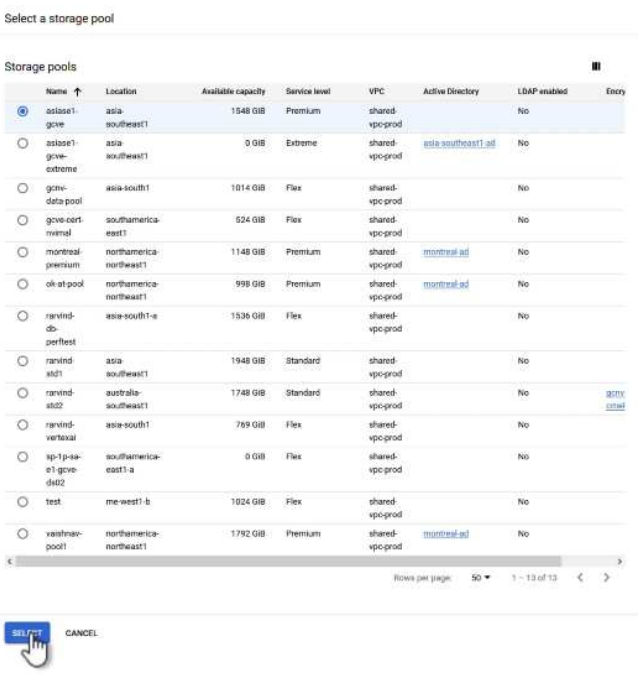
3. *ボリュームの作成*ウィザードで、必要な情報をすべて入力します。
   - ボリュームの名前。
   - ボリュームを作成するストレージ プール。
   - NFS ボリュームをマウントするときに使用される共有名。
   - ボリュームの容量（GiB 単位）。
   - 使用するストレージ プロトコル。
   - クライアントが接続されたときにボリュームの削除をブロックする のボックスをチェックします (データストアとしてマウントするときに GCVE によって必要)。
   - ボリュームにアクセスするためのエクスポート ルール。これは、NFS ネットワーク上の ESXi アダ

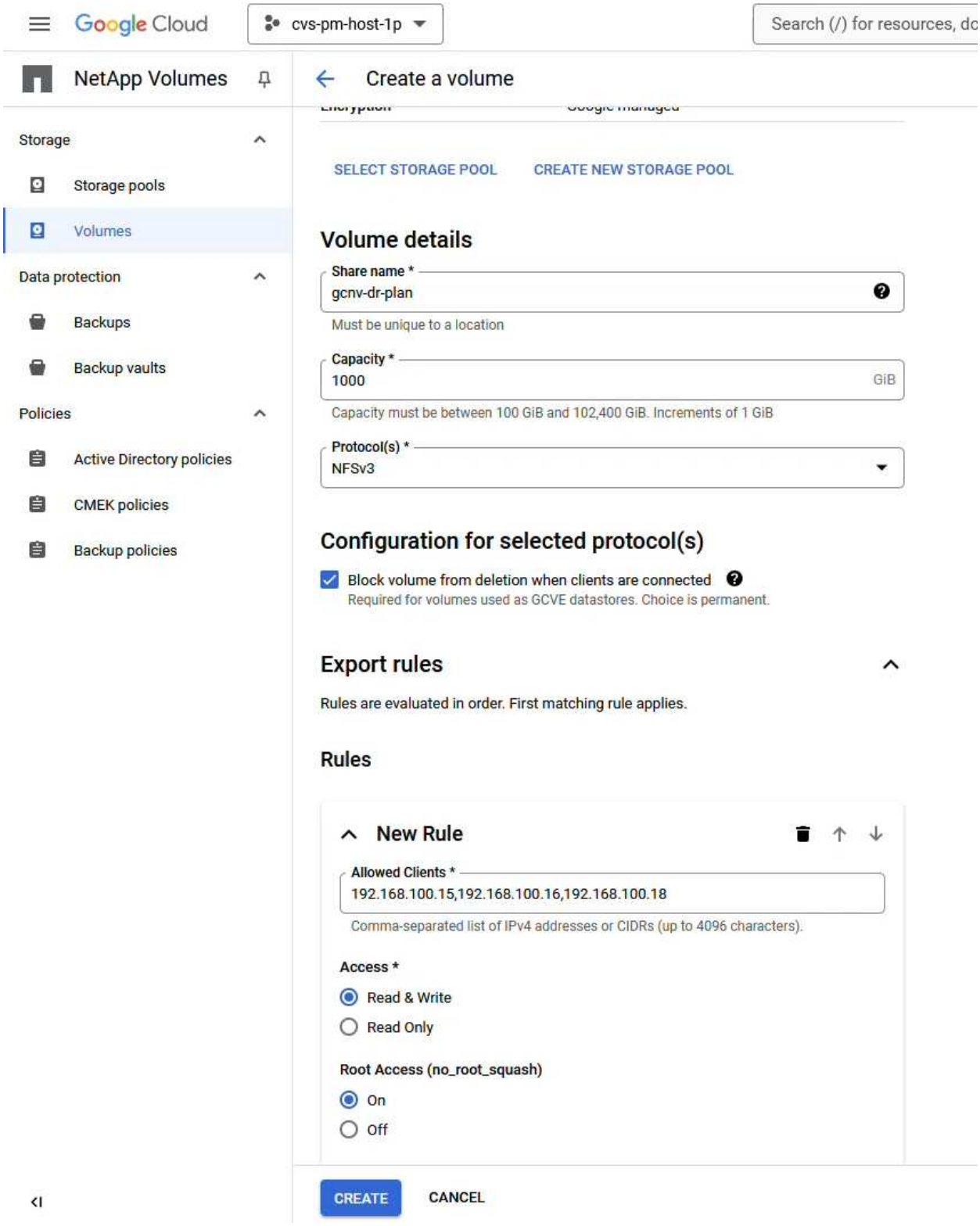
プタの IP アドレスです。

- ローカル スナップショットを使用してボリュームを保護するために使用されるスナップショット スケジュール。
- 必要に応じて、ボリュームをバックアップするか、ボリュームのラベルを作成するかを選択します。

NetApp Volumes でボリュームを作成し、GCVE データストアとして使用する場合、NFS v3 のみがサポートされます。

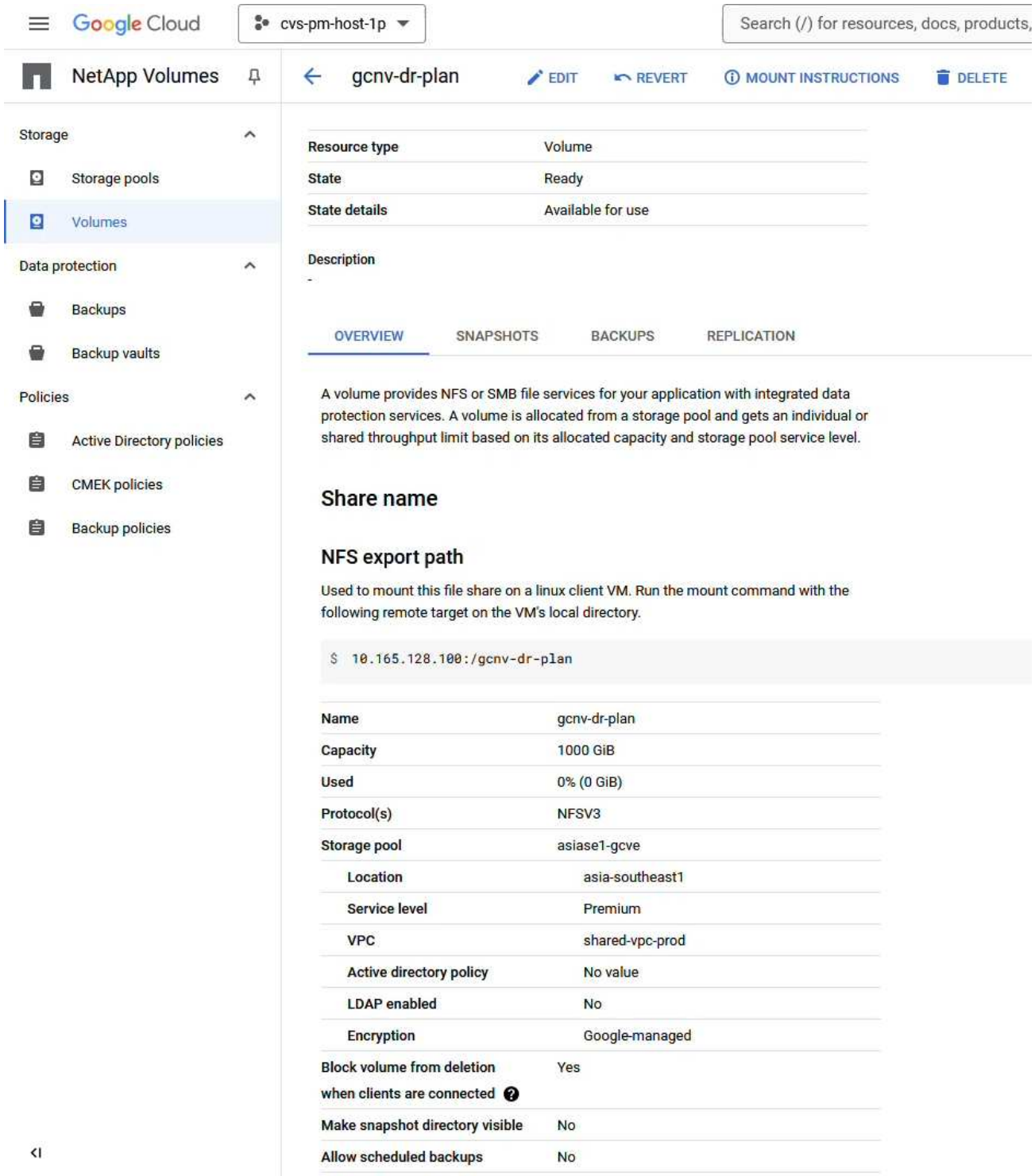






ボリュームの作成を完了するには、[作成] をクリックします。

4. ボリュームが作成されると、ボリュームのマウントに必要な NFS エクスポート パスがボリュームのプロパティ ページから表示できるようになります。



▼ **GCVEでNFSデータストアをマウントする**

この記事の執筆時点では、GCVE でデータストアをマウントするプロセスでは、ボリュームを NFS データストアとしてマウントするために GCP サポート チケットを開く必要があります。

参照 "Google Cloud NetApp Volumesでホストされる vSphere データストアとして NFS ボリュームを使用する"詳細についてはこちらをご覧ください。

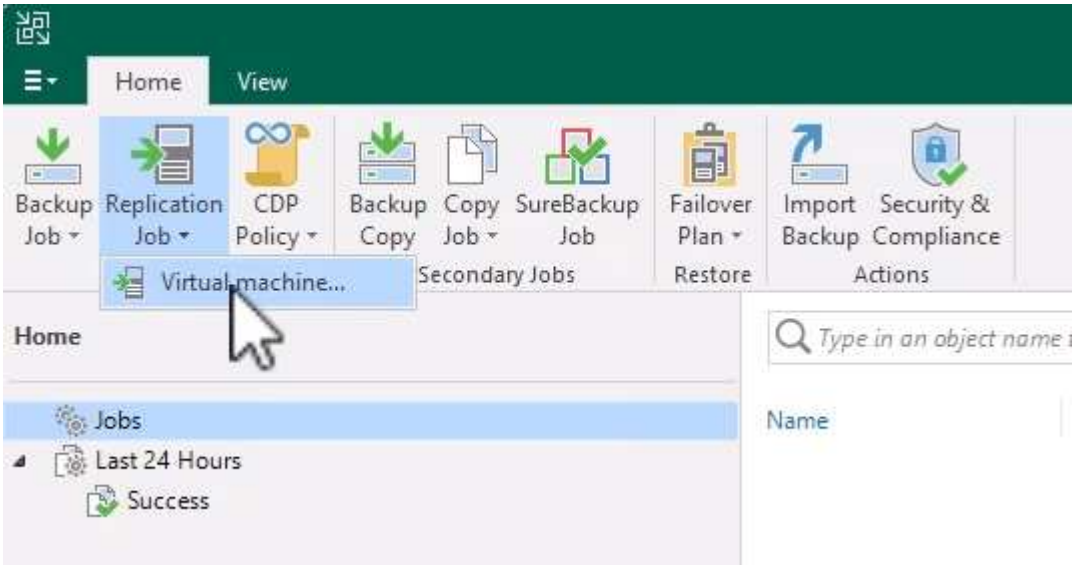
VMをGCVEに複製し、フェイルオーバープランとフェイルバックを実行する

▼ GCVE の NFS データストアに VM を複製する

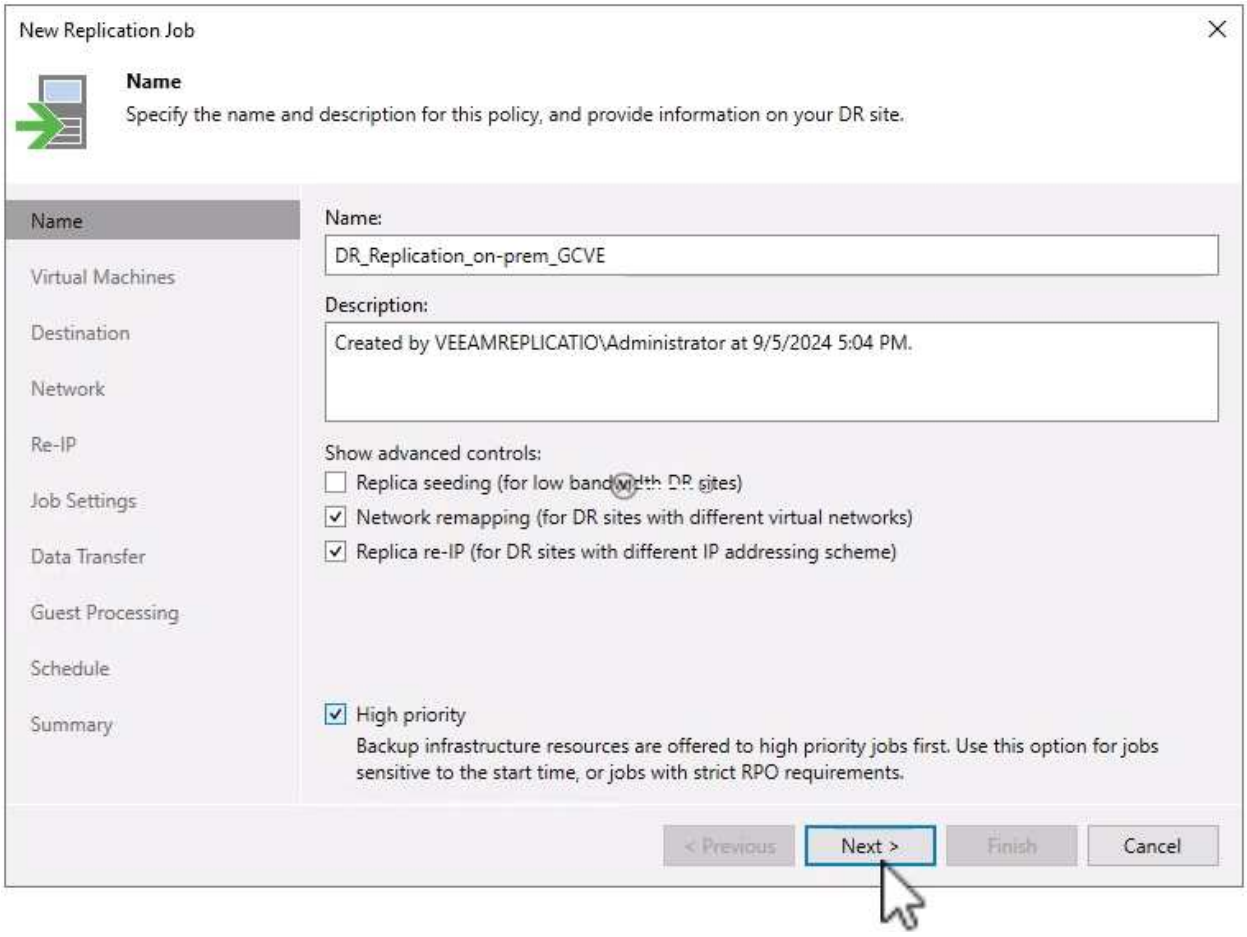
Veeam Backup & Replication はレプリケーション中に VMware vSphere スナップショット機能を活用し、VMware vSphere に VM スナップショットの作成を要求します。 VM スナップショットは、仮想ディスク、システム状態、構成、メタデータを含む VM の特定時点のコピーです。 Veeam Backup & Replication は、スナップショットをレプリケーションのデータ ソースとして使用します。

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. ホーム タブで、レプリケーション ジョブ > 仮想マシン... をクリックします。

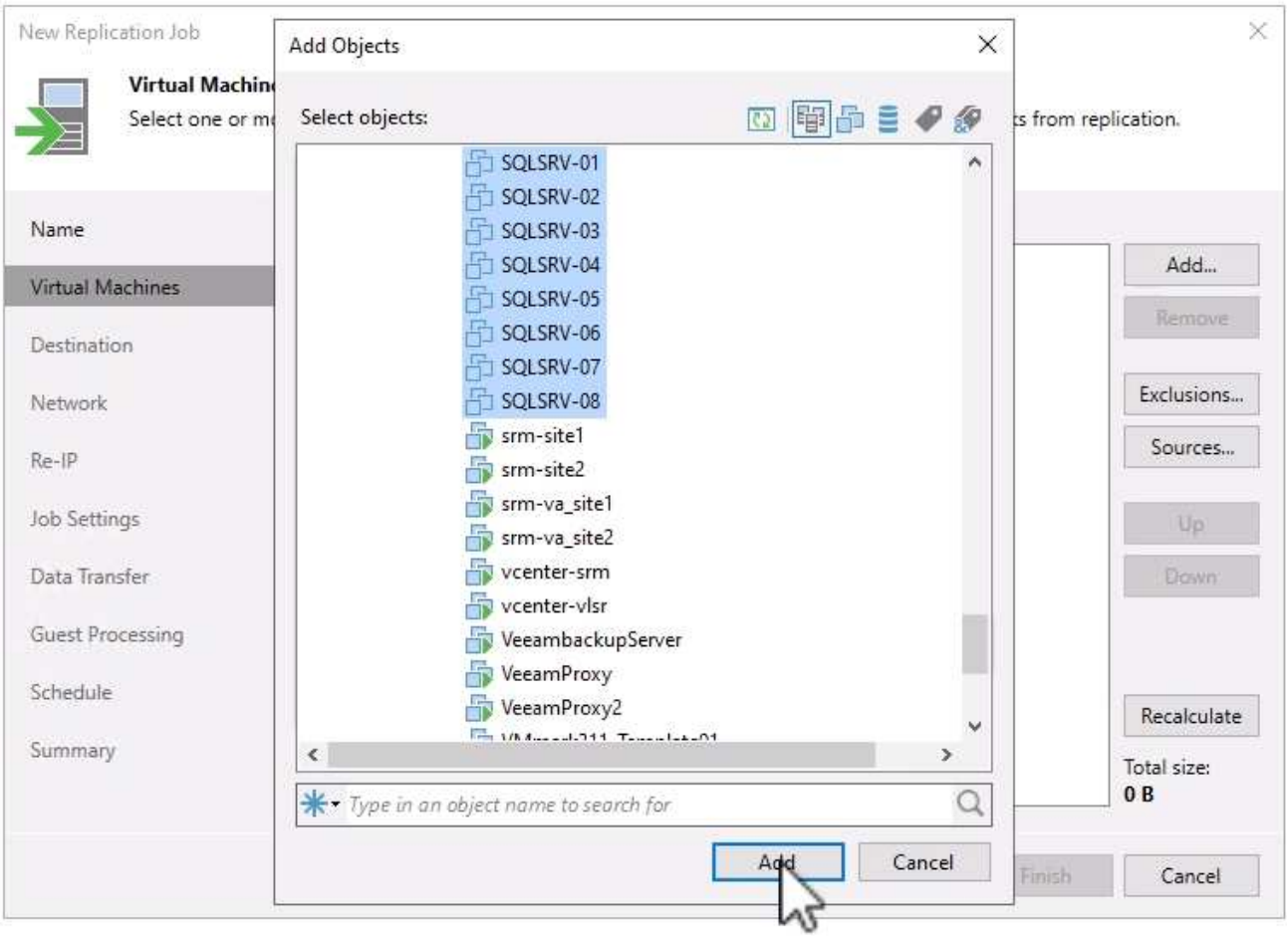


3. 新しいレプリケーション ジョブ ウィザードの 名前 ページで、ジョブ名を指定し、適切な詳細制御のチェックボックスを選択します。
   - オンプレミスと GCP 間の接続の帯域幅が制限されている場合は、[レプリカ シーディング] チェック ボックスをオンにします。
   - GCVE SDDC 上のセグメントがオンプレミスのサイト ネットワークのセグメントと一致しない場合は、[ネットワークの再マッピング (異なるネットワークを持つ GCVE SDDC サイトの場合)] チェック ボックスをオンにします。
   - オンプレミスの運用サイトの IP アドレス指定スキームがターゲット GCVE サイトのスキームと異なる場合は、[レプリカ再 IP (異なる IP アドレス指定スキームを持つ DR サイト用)] チェック ボックスをオンにします。

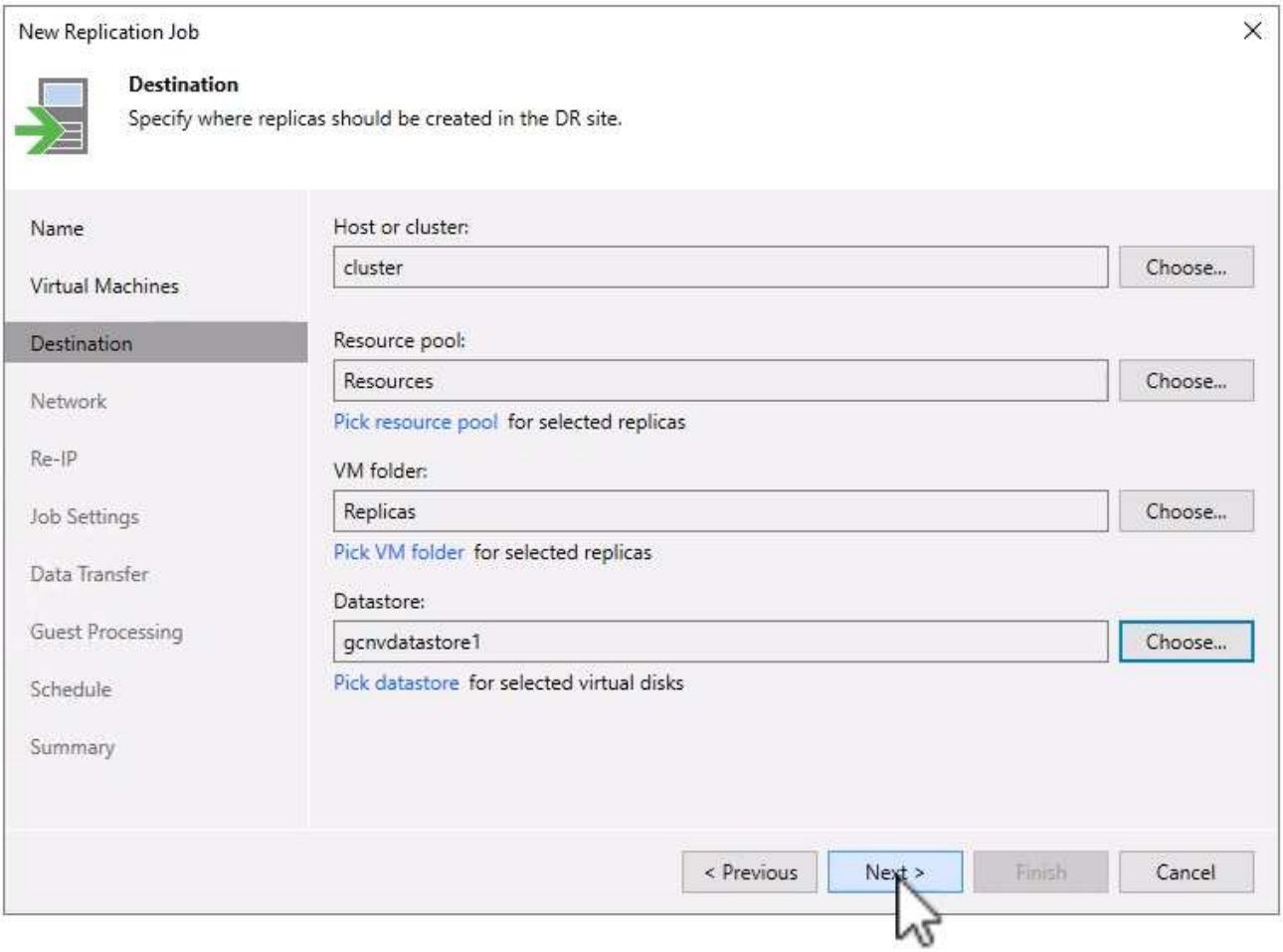


4. 仮想マシン ページで、GCVE SDDC に接続されたNetApp Volumes データストアに複製する仮想マシンを選択します。 [追加] をクリックし、[オブジェクトの追加] ウィンドウで必要な VM または VM コンテナを選択して [追加] をクリックします。*次へ*をクリックします。

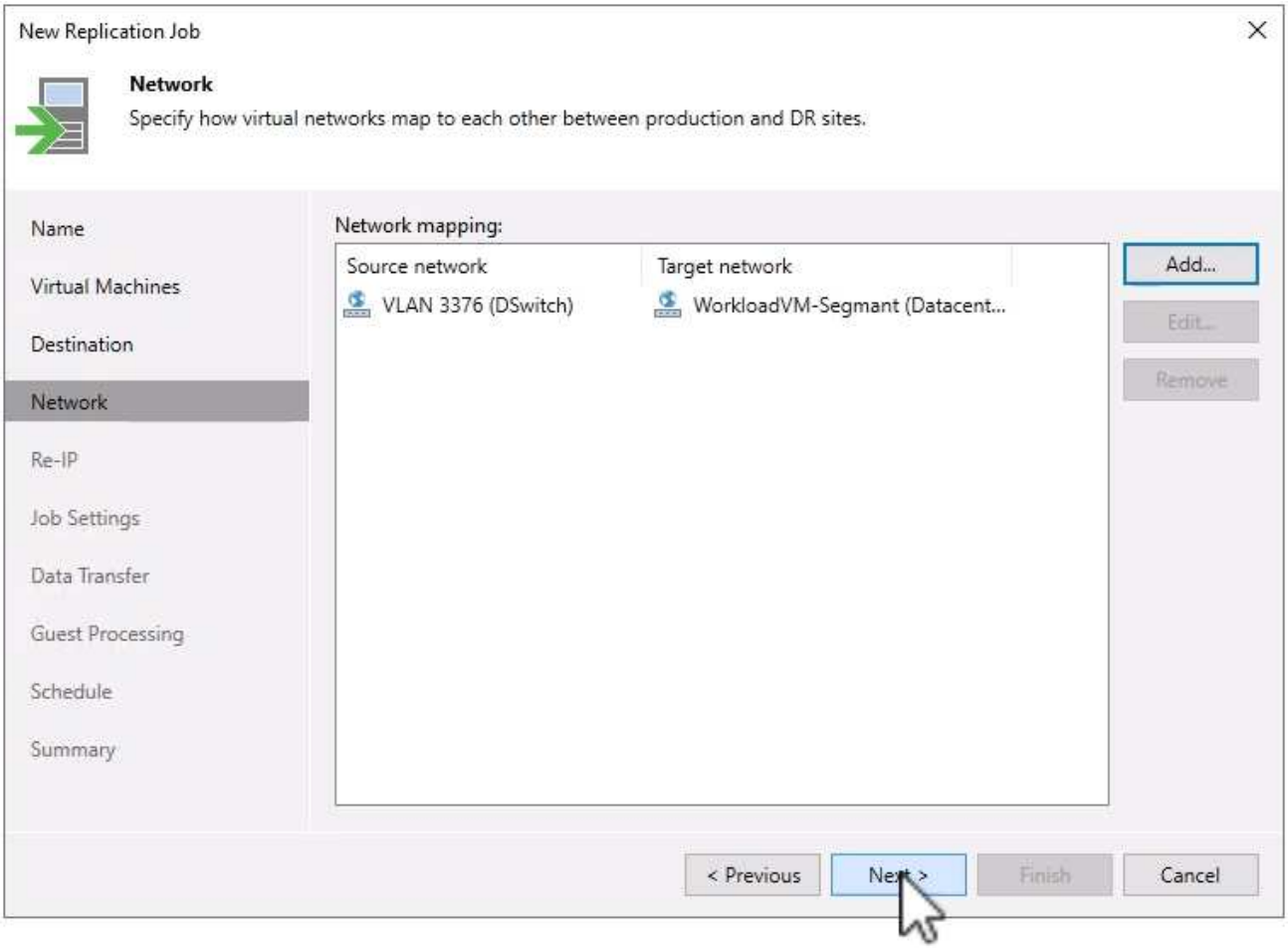
> 使用可能な vSAN データストアの容量を満たすために、仮想マシンを vSAN 上に配置できます。パイロット ライト クラスタでは、3 ノードの vSAN クラスタの使用可能な容量が制限されます。残りのデータはGoogle Cloud NetApp Volumesデータストアに簡単に配置できるため、VM を復元し、後で CPU/メモリ要件を満たすようにクラスタを拡張できます。



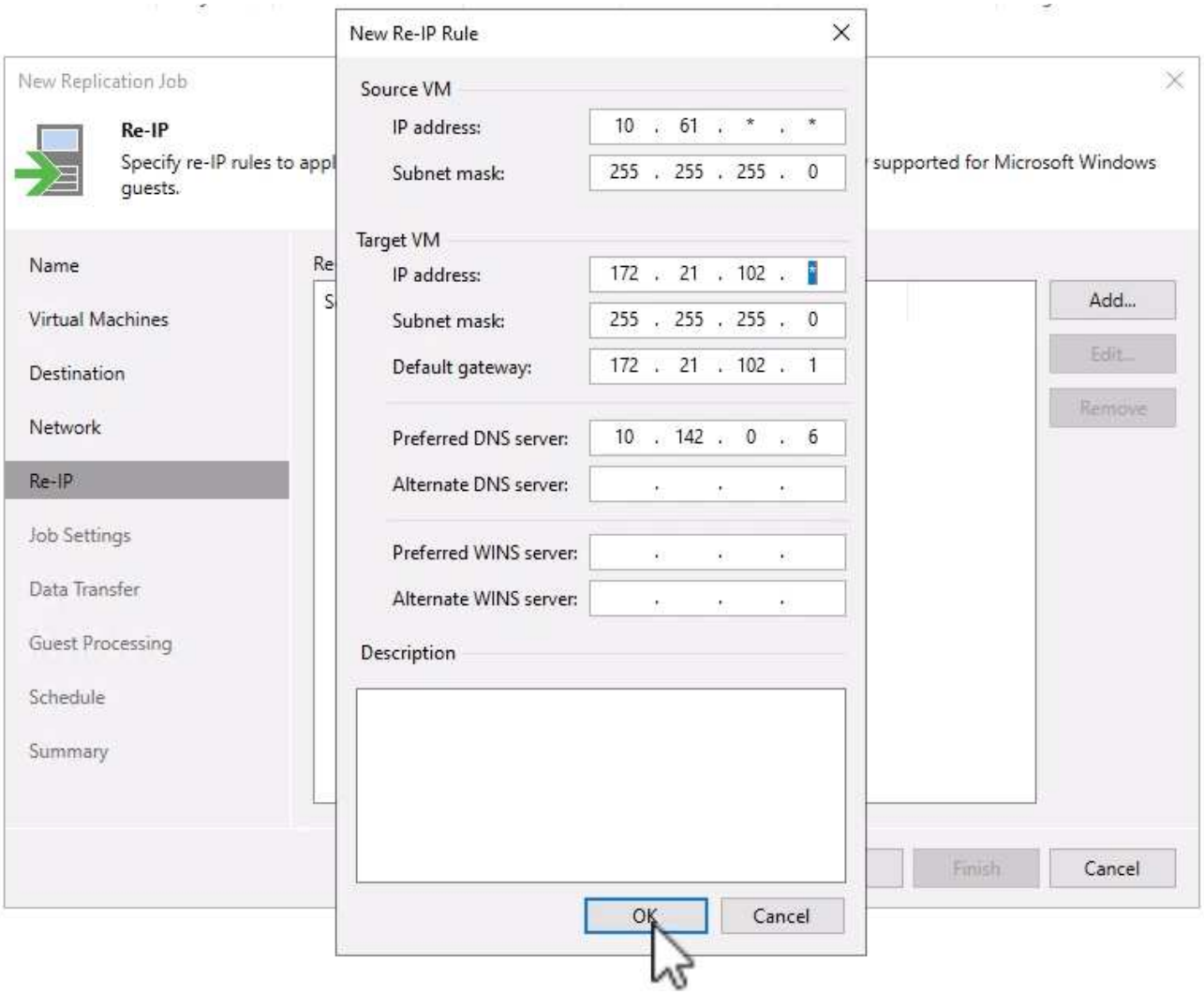
5. 宛先 ページで、宛先として GCVE SDDC クラスター/ホストを選択し、VM レプリカの適切なリソースプール、VM フォルダー、およびNetApp Volumes データストアを選択します。続行するには、[次へ]をクリックします。



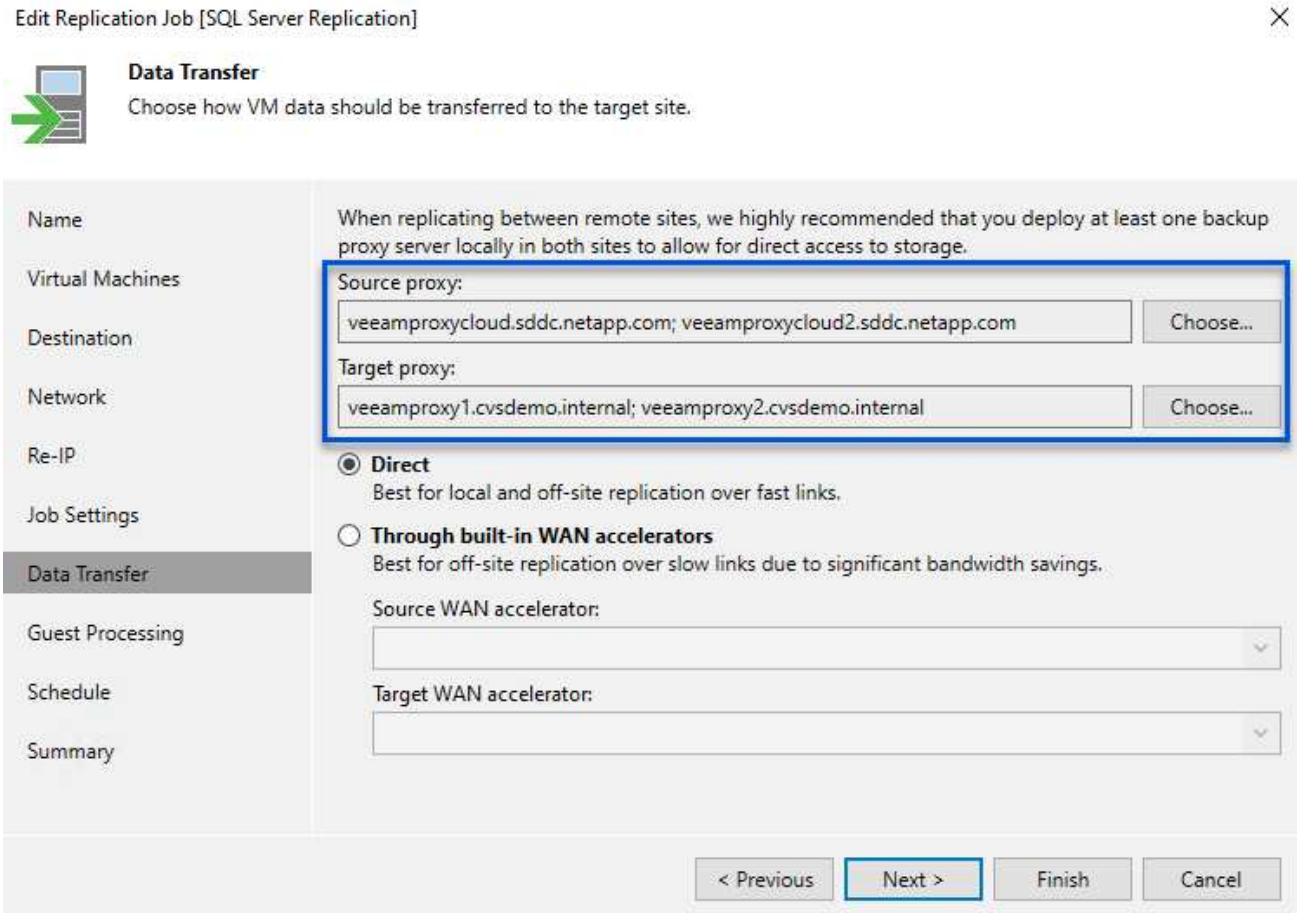
6. ネットワーク ページで、必要に応じてソース仮想ネットワークとターゲット仮想ネットワーク間のマッピングを作成します。続行するには、[次へ] をクリックします。



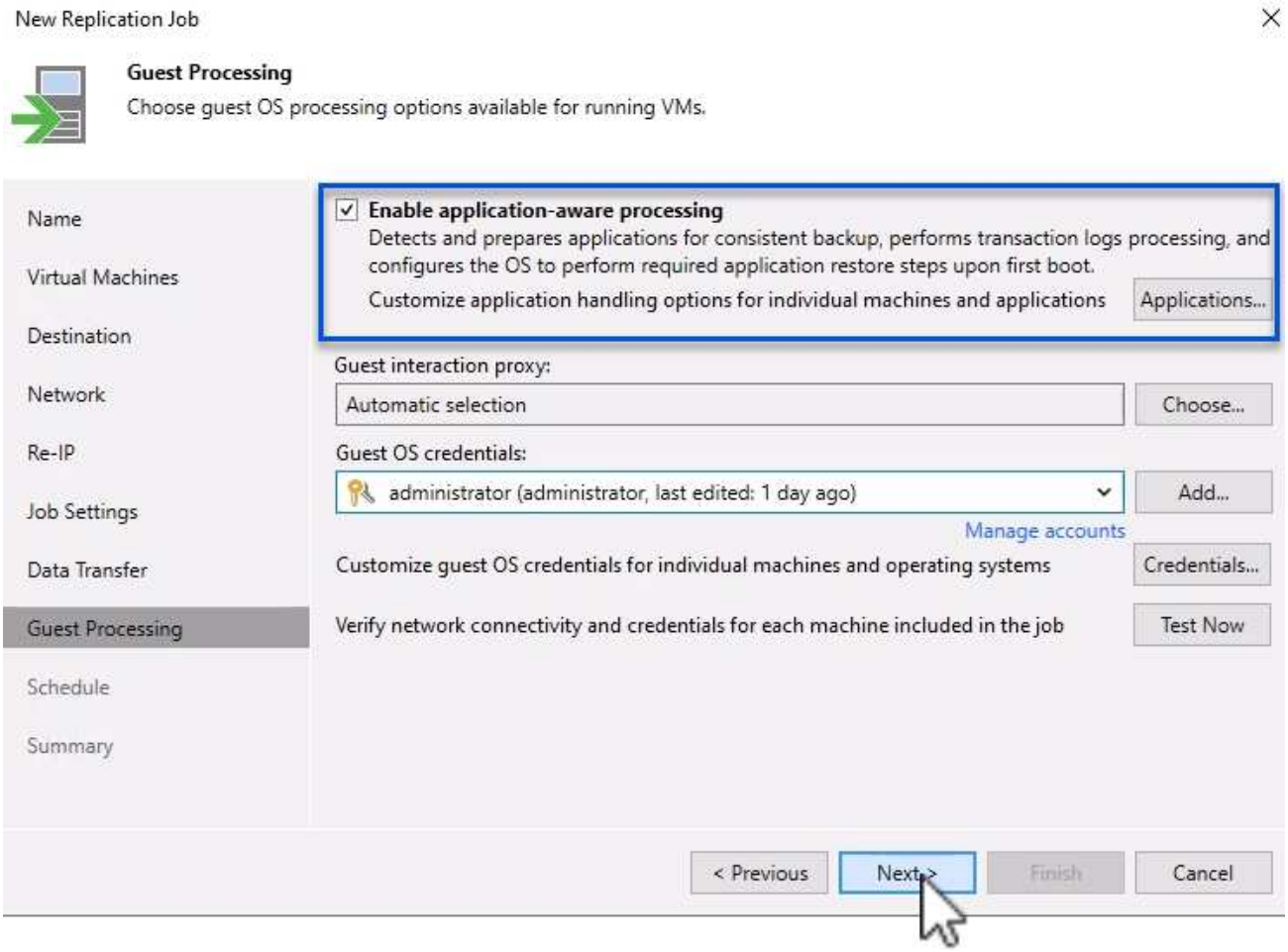
7. **Re-IP** ページで、追加**...** ボタンをクリックして、新しい re-IP ルールを追加します。フェイルオーバーの際にソース VM に適用されるネットワークを指定するには、ソース VM とターゲット VM の IP 範囲を入力します。そのオクテットに示されたアドレスの範囲を指定するには、アスタリスクを使用します。続行するには、[次へ] をクリックします。



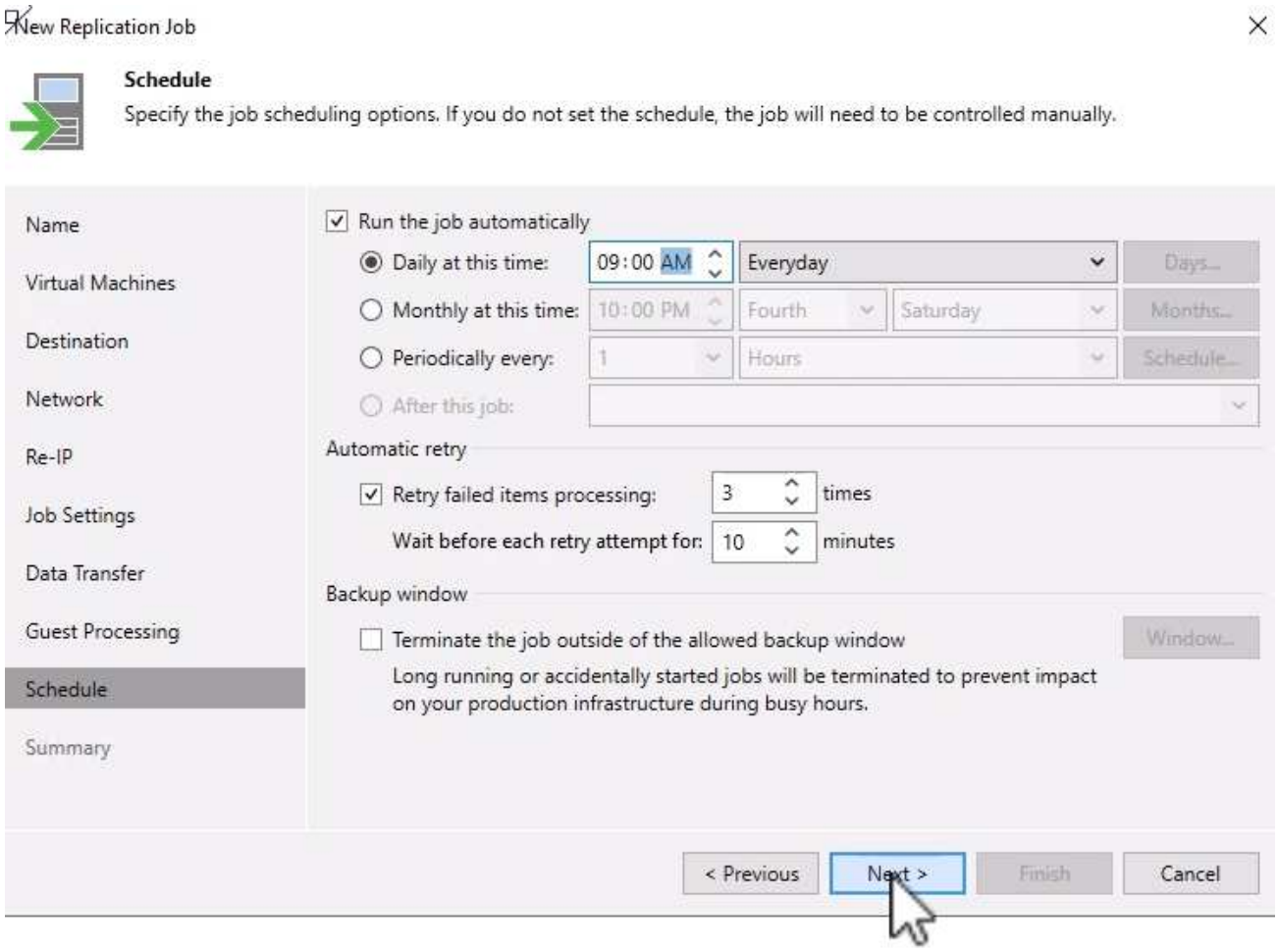
8. *ジョブ設定*ページで、VMレプリカのメタデータを保存するバックアップ リポジトリ、保持ポリシーを指定し、下部にある*詳細設定...*ボタンを選択して、追加のジョブ設定を行います。続行するには、[次へ] をクリックします。
9. *データ転送*で、ソース サイトとターゲット サイトにあるプロキシ サーバーを選択し、[直接] オプションを選択したままにします。構成されている場合は、ここで WAN アクセラレータも選択できます。続行するには、[次へ] をクリックします。



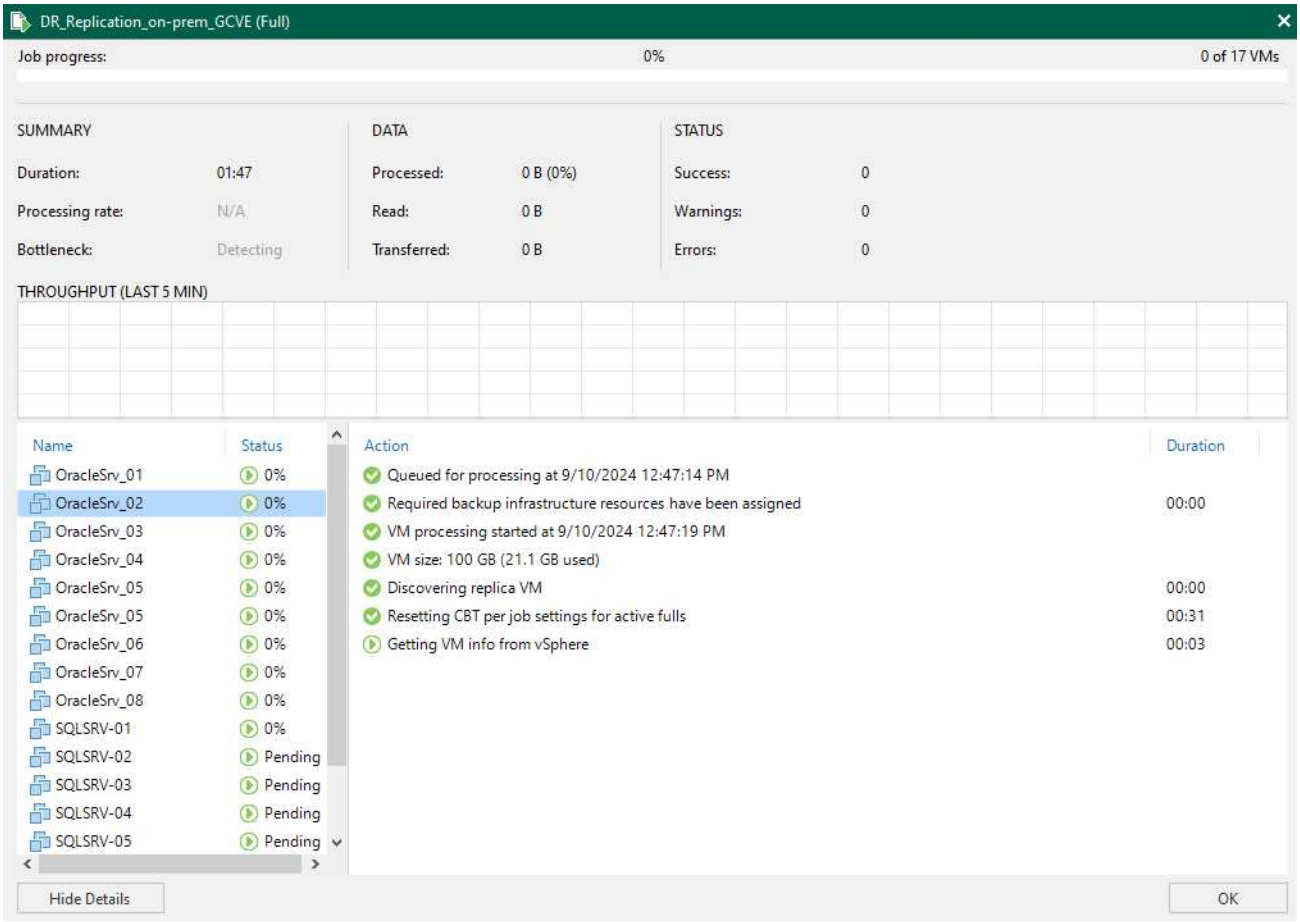
10. *ゲスト処理*ページで、必要に応じて*アプリケーション認識処理を有効にする*チェックボックスをオンにし、*ゲスト OS 資格情報*を選択します。続行するには、[次へ] をクリックします。



11. スケジュール ページで、レプリケーション ジョブを実行する時間と頻度を定義します。続行するには、[次へ] をクリックします。



12. 最後に、概要*ページでジョブ設定を確認します。 **[完了]** をクリックしたときにジョブを実行する のボックスをオンにし、[完了] をクリックしてレプリケーション ジョブの作成を完了します。
13. 実行すると、レプリケーション ジョブはジョブ ステータス ウィンドウで確認できます。



Veeamレプリケーションの詳細については、以下を参照してください。"レプリケーションの仕組み"

▼ フェイルオーバープランを作成する

初期レプリケーションまたはシードが完了したら、フェールオーバー 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、ブートの遅延を含め、VM が処理される順序の青写真です。フェールオーバー 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。

初期レプリケーションまたはシードが完了したら、フェールオーバー プランを作成します。この計画は、依存する VM のフェイルオーバーを個別またはグループとして調整するための戦略的な青写真として機能します。 VM の処理順序を定義し、必要なブート遅延を組み込み、重要な依存 VM が他の VM よりも先に動作することを保証します。適切に構成されたフェイルオーバー計画を実装することで、組織は災害復旧プロセスを合理化し、ダウンタイムを最小限に抑え、フェイルオーバー イベント中に相互依存するシステムの整合性を維持できます。

プランを作成するときに、Veeam Backup & Replication は最新の復元ポイントを自動的に識別して使用し、VM レプリカを開始します。

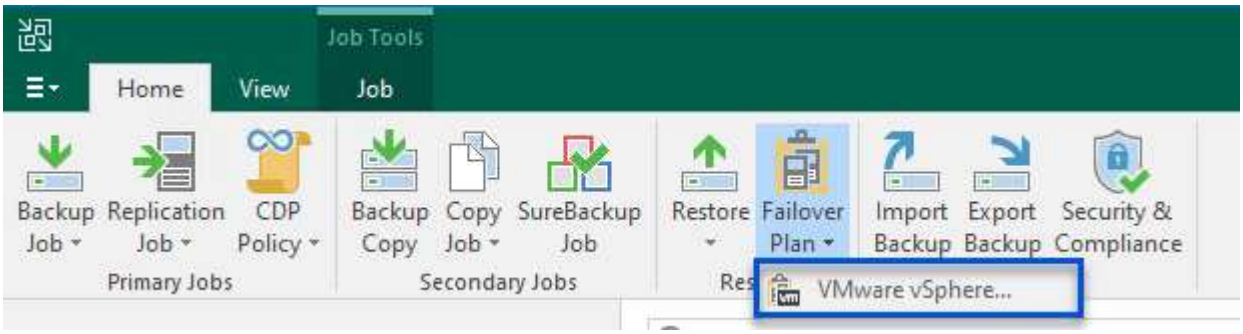
ⓘ フェールオーバー プランは、初期レプリケーションが完了し、VM レプリカが準備完了状態になった後にのみ作成できます。

ⓘ 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。

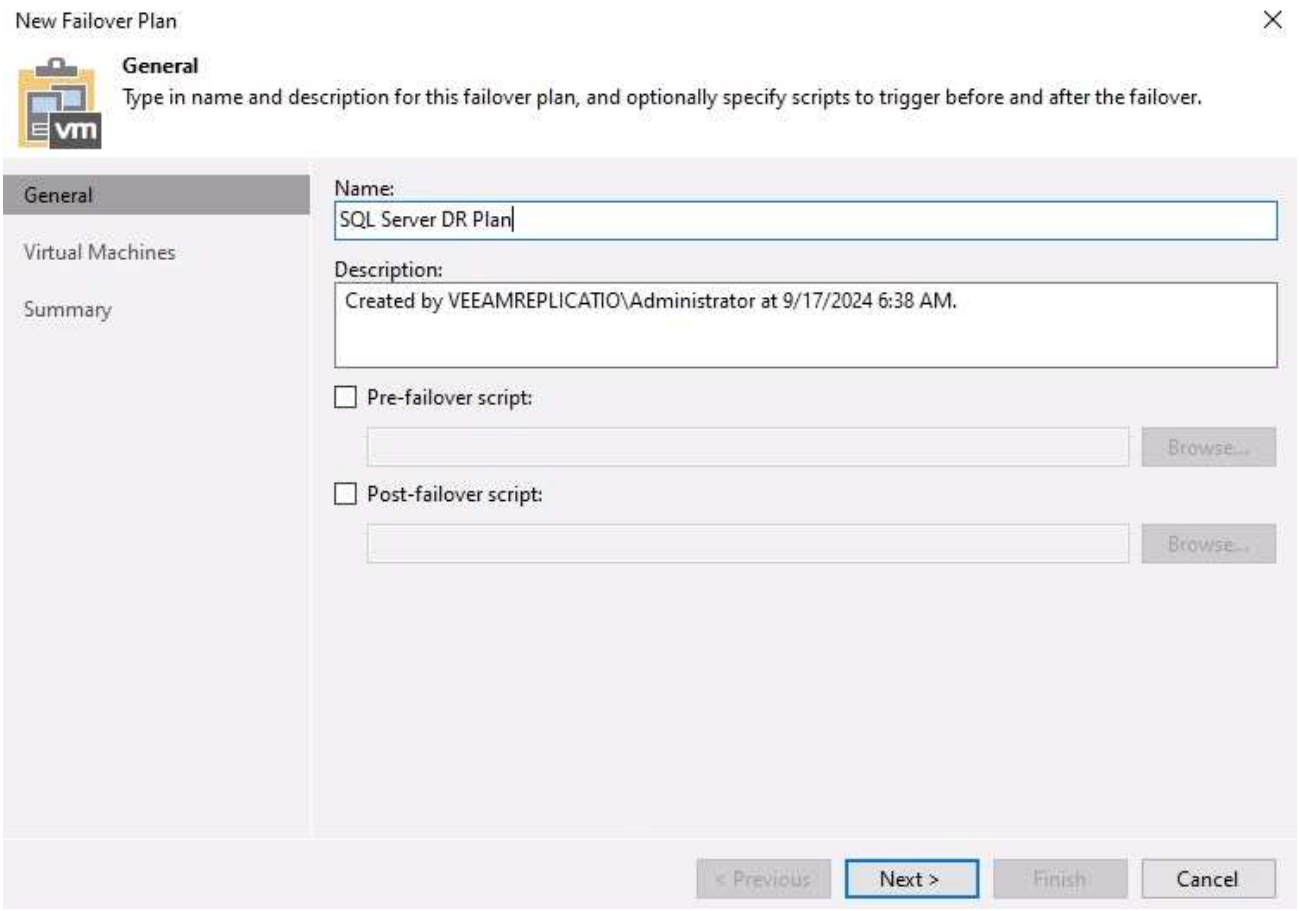
ⓘ フェールオーバー プロセス中、ソース VM の電源はオフになりません。

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。

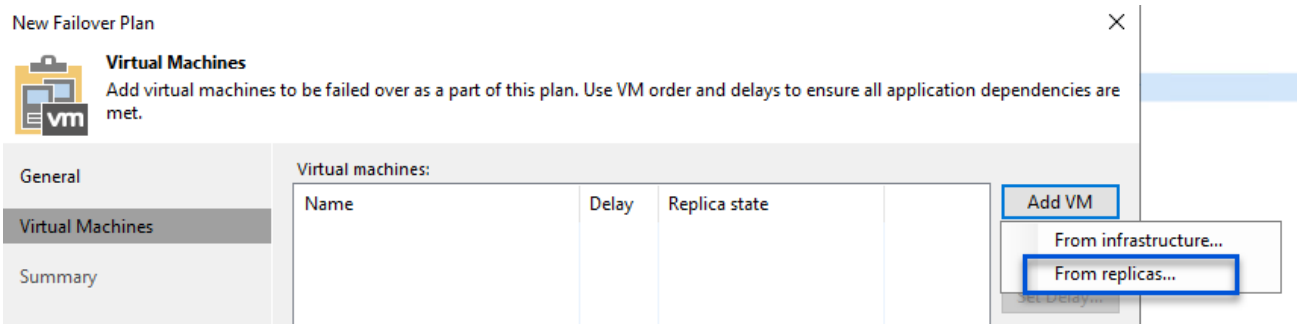
1. ホーム ビューで、復元 セクションの フェールオーバー プラン ボタンをクリックします。ドロップダウンで、**VMware vSphere…** を選択します。

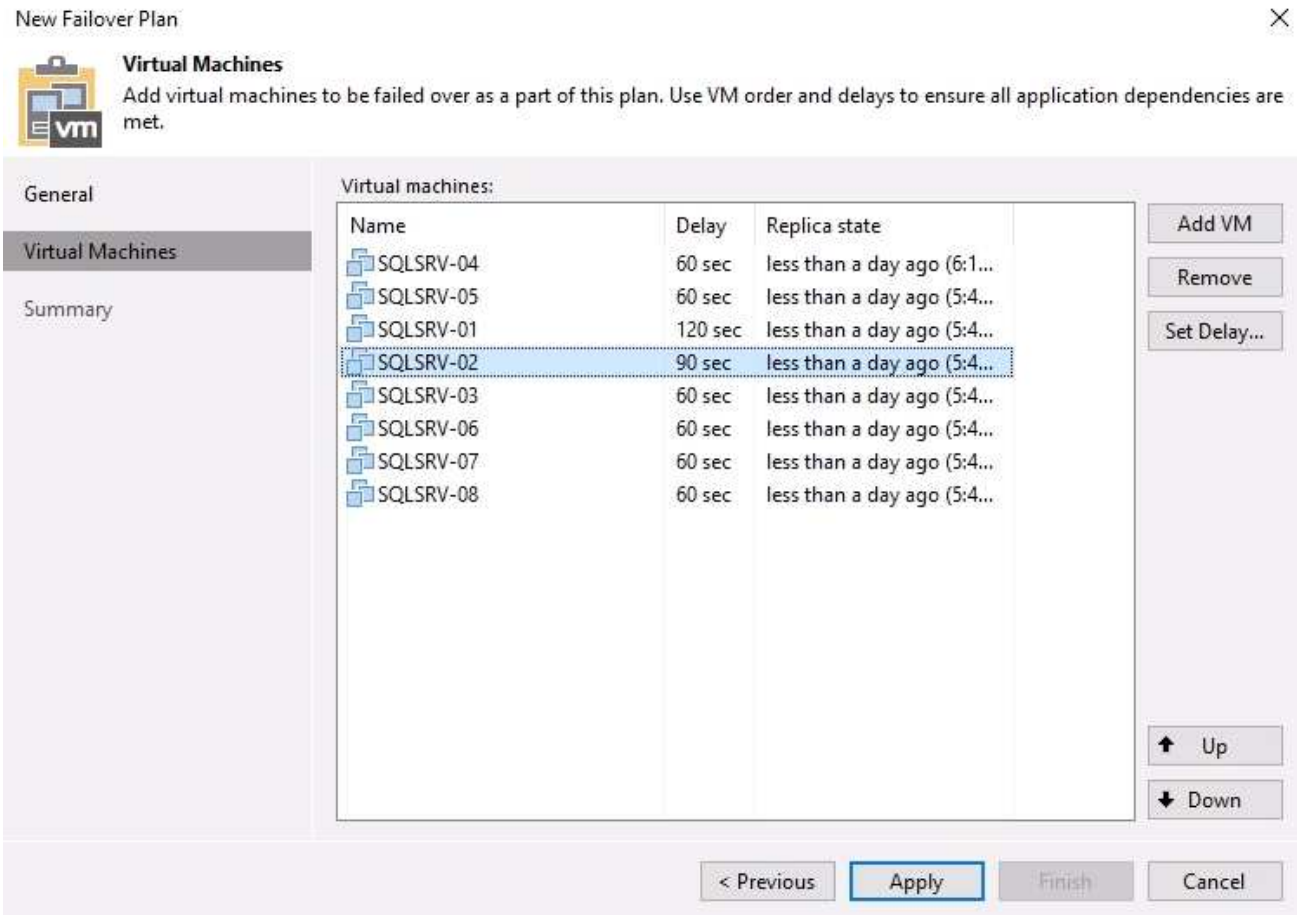


2. 新しいフェイルオーバー プラン ウィザードの 全般 ページで、プランの名前と説明を入力します。必要に応じて、フェイルオーバー前およびフェイルオーバー後のスクリプトを追加できます。たとえば、複製された VM を起動する前に VM をシャットダウンするスクリプトを実行します。



3. *仮想マシン*ページで、*VMの追加*ボタンをクリックし、*レプリカから…*を選択します。フェールオーバー プランの一部となる VM を選択し、アプリケーションの依存関係を満たすために VM のブート順序と必要なブート遅延を変更します。





続行するには、[適用] をクリックします。

4. 最後に、すべてのフェールオーバー プラン設定を確認し、[完了] をクリックしてフェールオーバー プランを作成します。

レプリケーションジョブの作成に関する詳細については、"レプリケーションジョブの作成" 。

▼ フェイルオーバープランを実行する

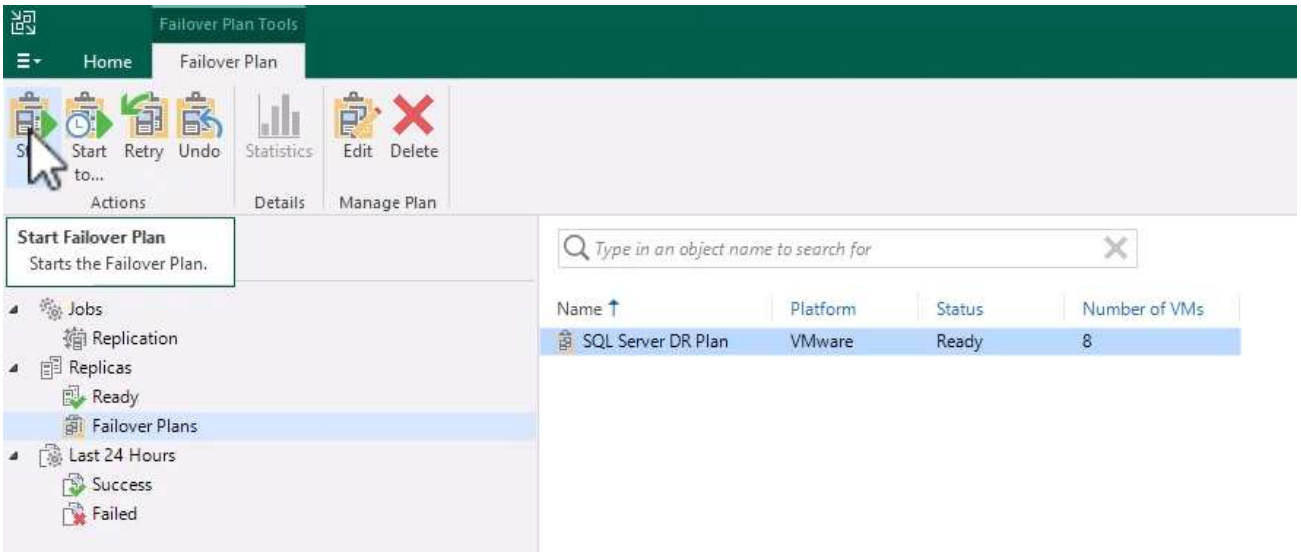
フェイルオーバー中、運用サイトのソース VM は災害復旧サイトのレプリカに切り替わります。プロセスの一環として、Veeam Backup & Replication は VM レプリカを必要な復元ポイントに復元し、すべての I/O アクティビティをソース VM からそのレプリカに転送します。レプリカは実際の災害だけでなく、DR 訓練のシミュレーションにも役立ちます。フェイルオーバー シミュレーションでは、ソース VM は引き続き実

行されます。必要なテストが完了したら、フェイルオーバーを元に戻し、操作を通常の状態に戻すことができます。

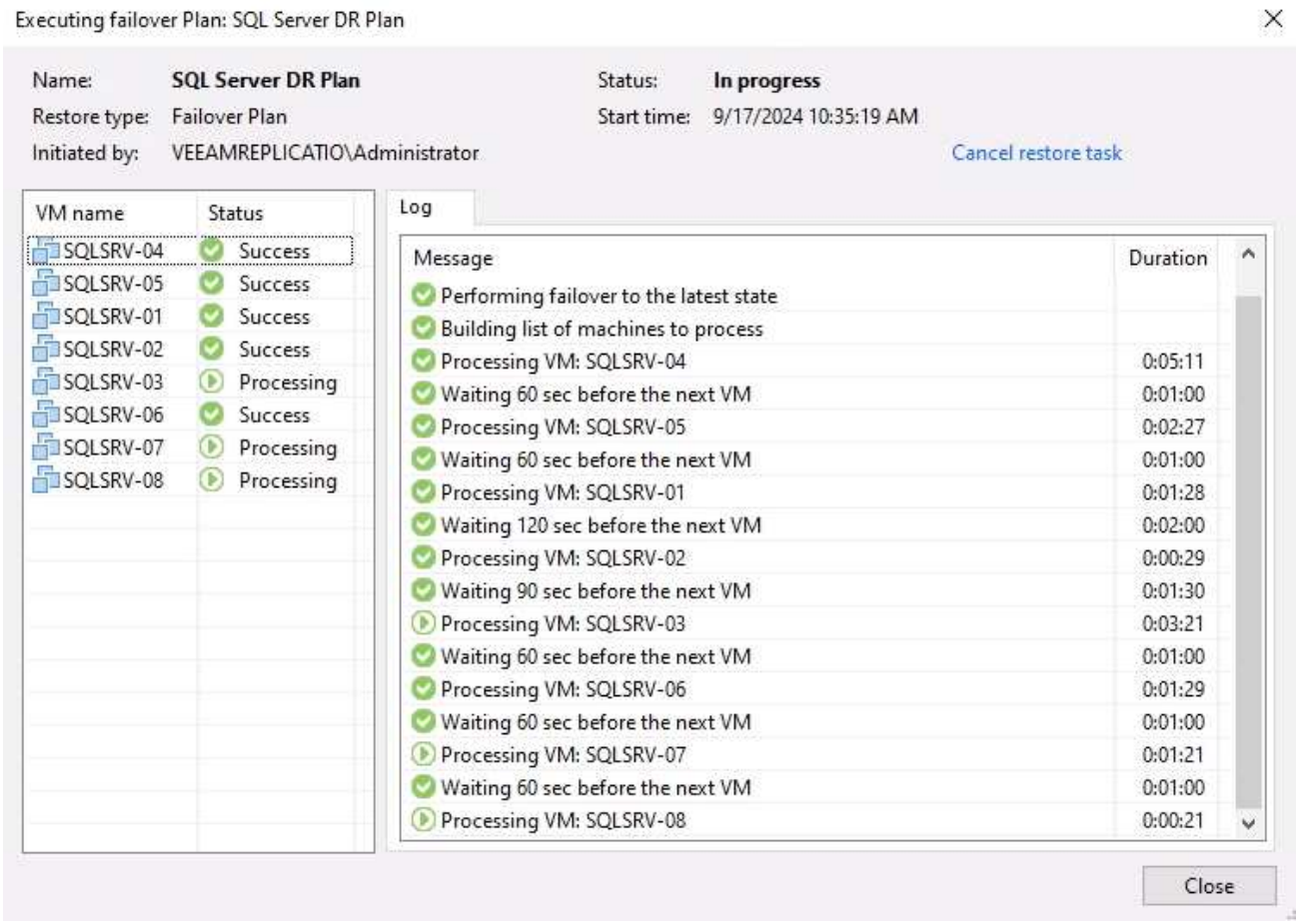
フェイルオーバー中の IP 競合を回避するために、ネットワーク セグメンテーションが適切に行われていることを確認してください。

フェールオーバー プランを開始するには、次の手順を実行します。

1. 開始するには、ホーム ビューで、左側のメニューの レプリカ > フェールオーバー プラン をクリックし、開始 ボタンをクリックします。あるいは、[開始...] ボタンを使用して、以前の復元ポイントにフェールオーバーすることもできます。



2. フェイルオーバー プランの実行 ウィンドウでフェイルオーバーの進行状況を監視します。



Veeam Backup & Replication は、レプリカが準備完了状態に戻るまで、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、以下を参照してください。"フェイルオーバー計画" 。

▼ 本番サイトへのフェイルバック

フェイルオーバーの実行は中間ステップとみなされ、要件に基づいて最終決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。

- 本番環境へのフェールバック - 元の VM に戻り、レプリカのアクティブ期間中に行われたすべての変更をソース VM に同期します。

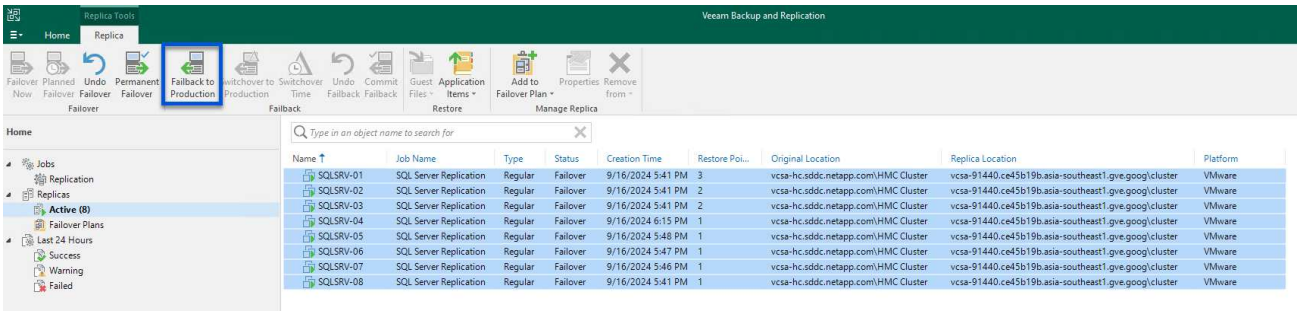
フェイルバック中、変更は転送されますが、すぐには適用されません。元の VM の機能が検証されたら、[コミット フェイルバック] を選択します。あるいは、元の VM が予期しない動作を示す場合は、[フェイルバックを元に戻す] を選択して VM レプリカに戻します。

- フェイルオーバーを元に戻す - 運用期間中に VM レプリカに加えられたすべての変更を破棄し、元の VM に戻します。
- 永続的なフェイルオーバー - 元の VM からそのレプリカに永続的に切り替え、レプリカを進行中の操作用の新しいプライマリ VM として確立します。

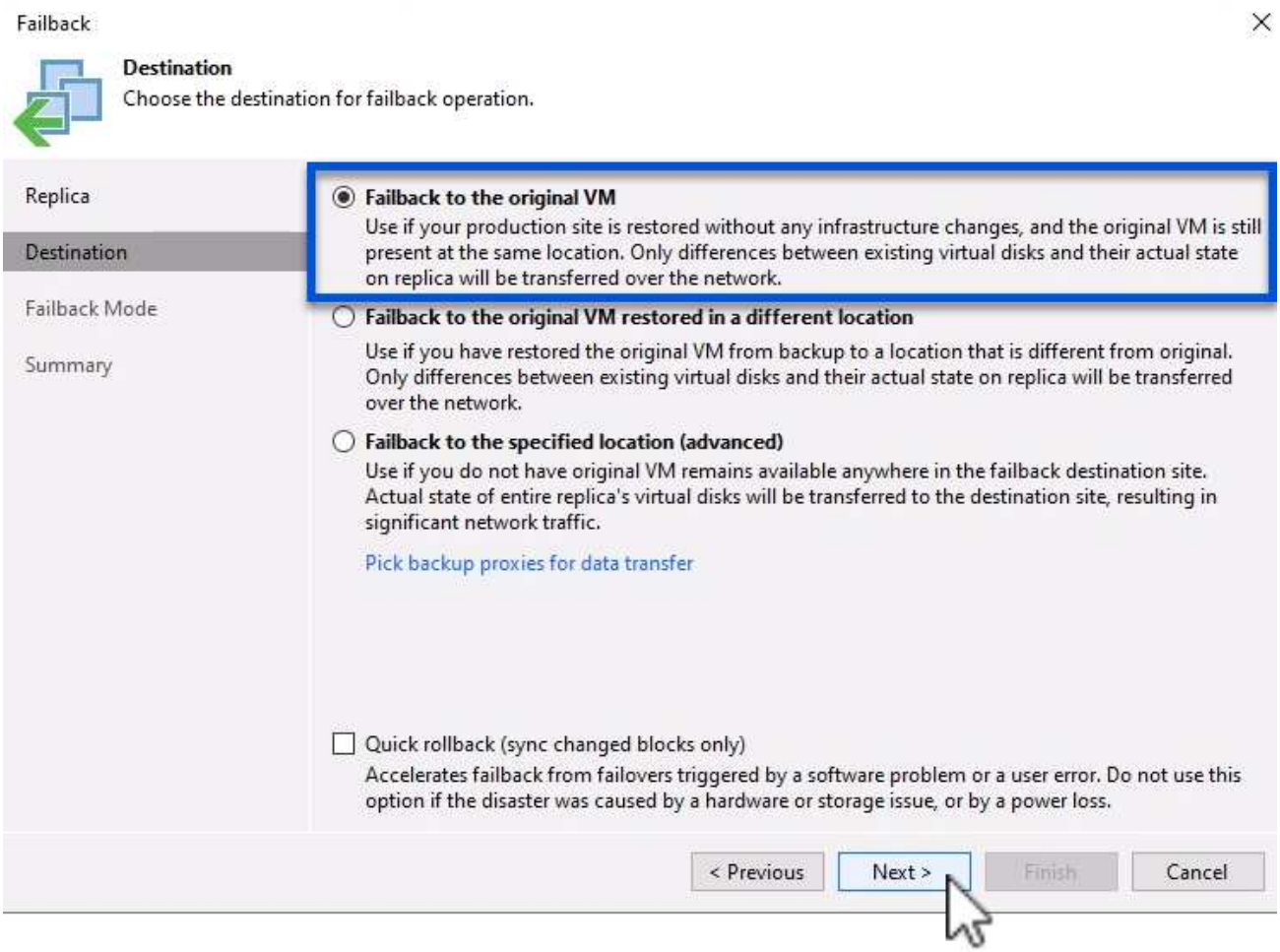
このシナリオでは、「本番環境へのフェールバック」オプションが選択されました。

実稼働サイトへのフェイルバックを実行するには、次の手順を実行します。

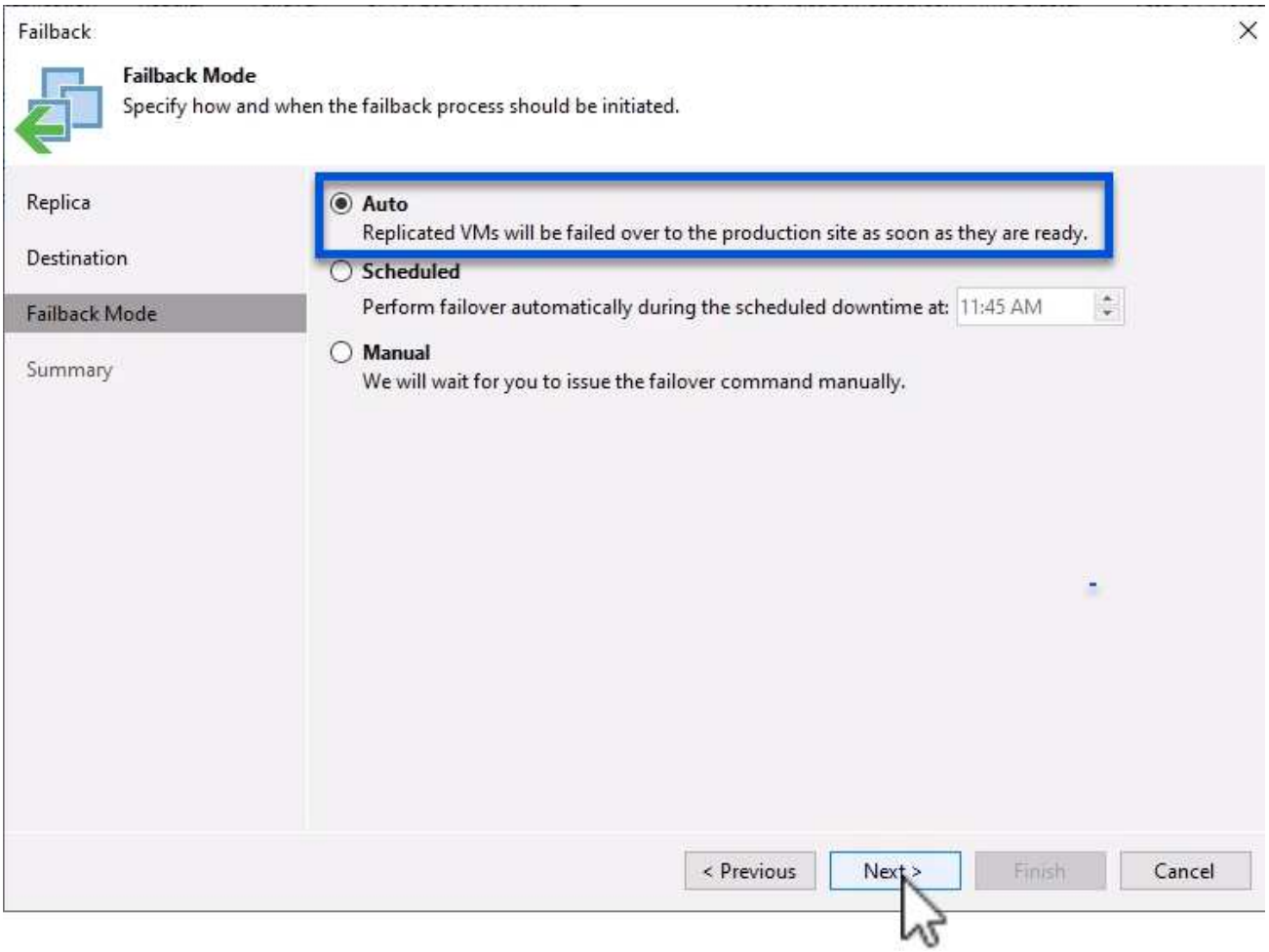
1. ホーム ビューから、左側のメニューの レプリカ > アクティブ をクリックします。含める VM を選択し、上部メニューの 実稼働へのフェールバック ボタンをクリックします。



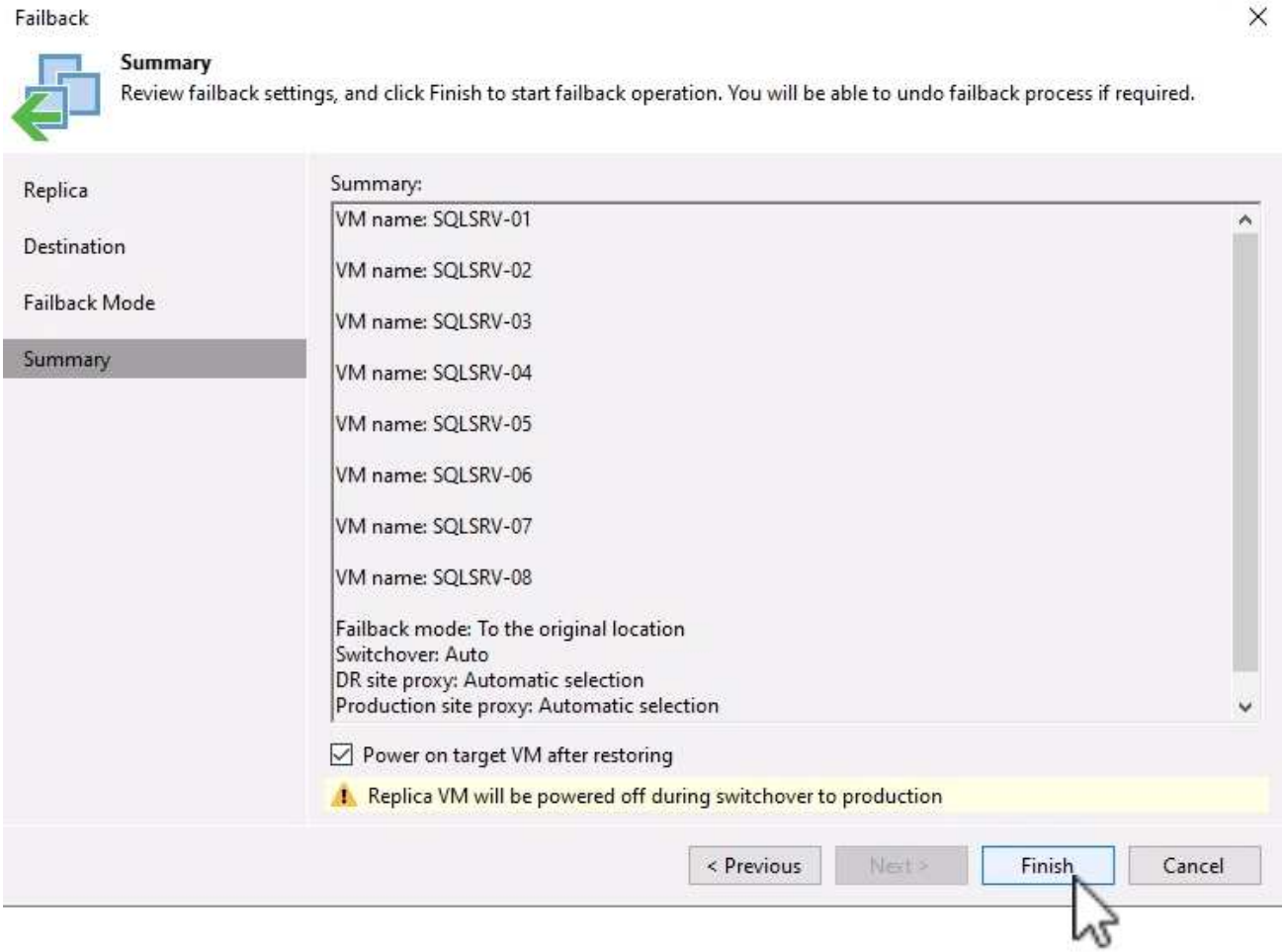
2. フェールバック ウィザードの レプリカ ページで、フェールバック ジョブに含めるレプリカを選択します。
3. *宛先*ページで、*元のVMにフェールバック*を選択し、*次へ*をクリックして続行します。



4. フェールバック モード ページで、自動 を選択して、できるだけ早くフェールバックを開始します。

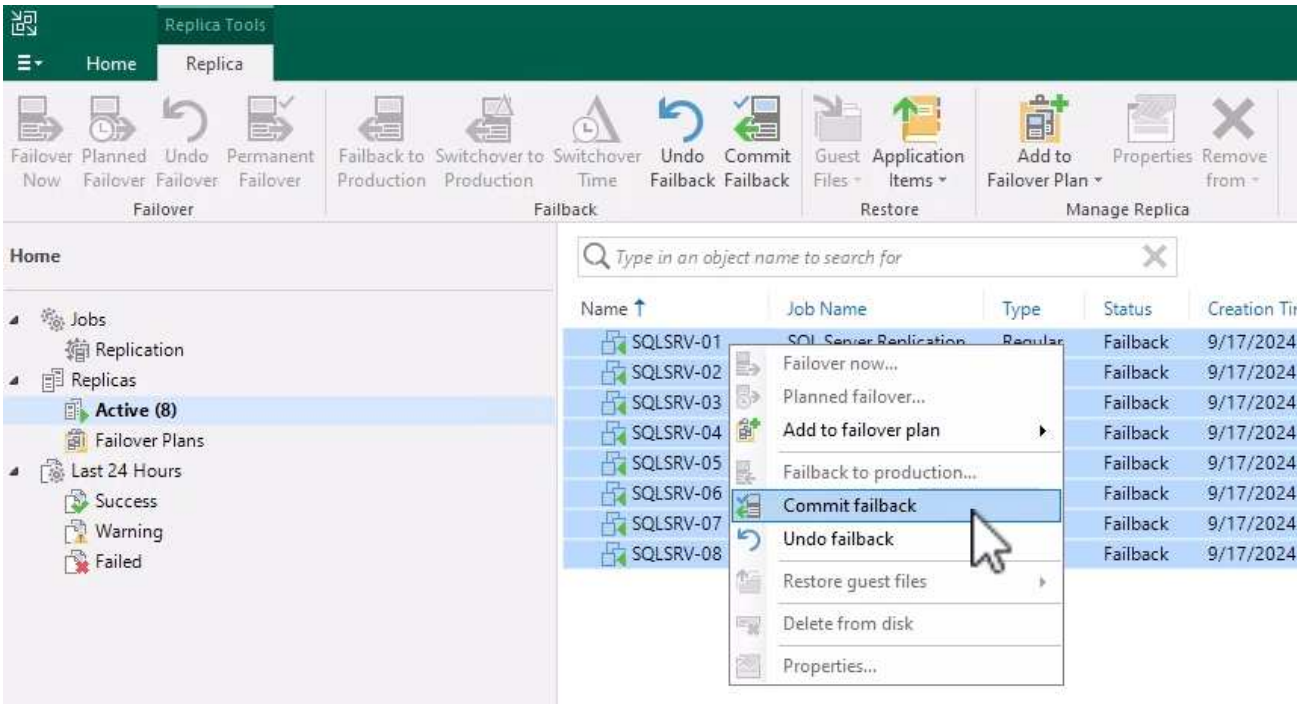


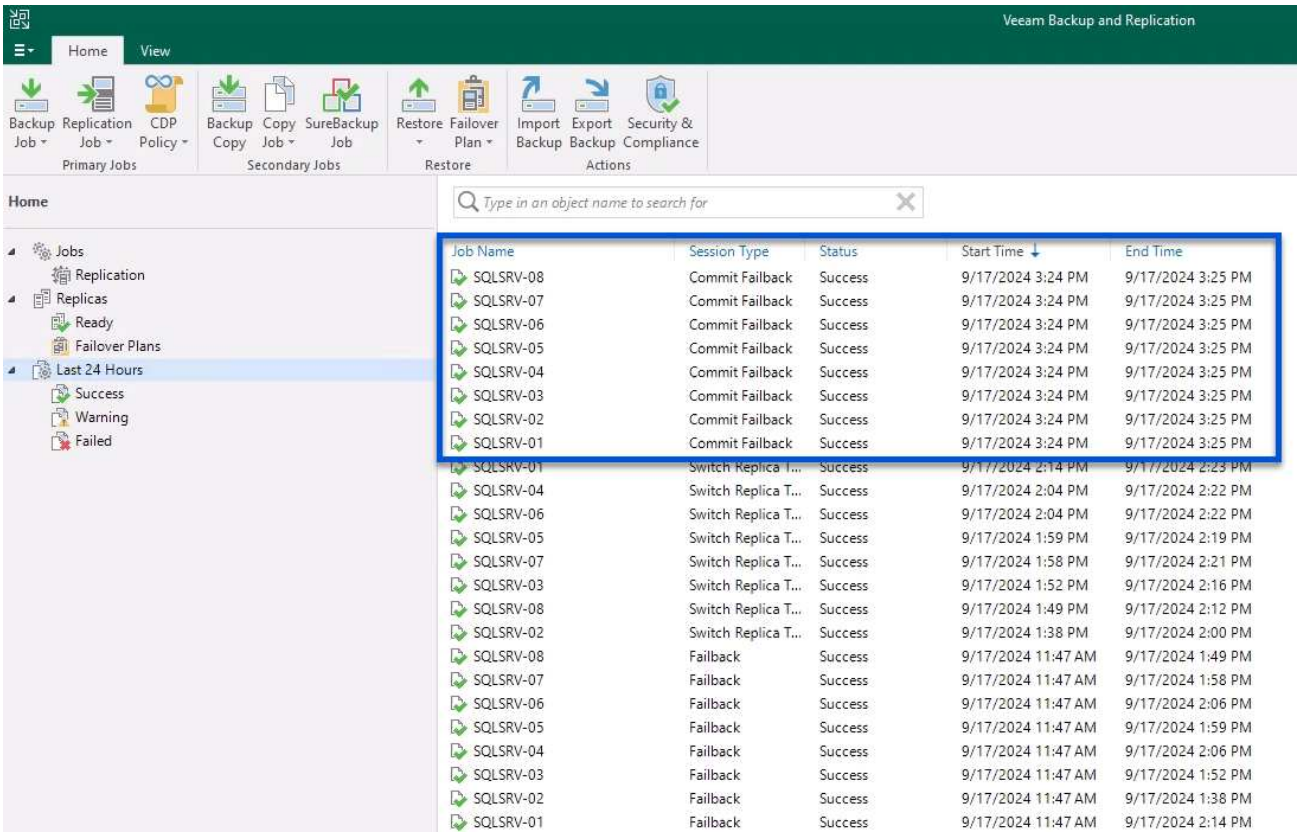
5. *概要*ページで、*復元後にターゲットVMをパワーオンする*かどうかを選択し、[完了]をクリックしてフェイルバックジョブを開始します。



フェイルバック コミットによりフェイルバック操作が完了し、本番 VM への変更が正常に統合されたことが確認されます。コミットすると、Veeam Backup & Replication は復元された本番 VM の通常のレプリケーション アクティビティを再開します。これにより、復元されたレプリカのステータスが「*Failback*」から「*Ready*」に変わります。

1. フェイルバックをコミットするには、レプリカ > アクティブ に移動し、コミットする VM を選択して右クリックし、フェイルバックのコミット を選択します。





実稼働環境へのフェイルバックが成功すると、VM はすべて元の実稼働サイトに復元されます。

フェイルバックプロセスの詳細については、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"。

まとめ

Google Cloud NetApp Volumesデータストア機能により、Veeam やその他の検証済みのサードパーティ ツールでコスト効率の高い災害復旧 (DR) ソリューションを提供できるようになります。 VM レプリカ用の大規模な専用クラスターの代わりに Pilot light クラスターを利用することで、組織は経費を大幅に削減できます。このアプローチにより、クラウドベースの災害復旧に既存の社内バックアップ ソリューションを活用するカスタマイズされた DR 戦略が可能になり、追加のオンプレミス データセンターが不要になります。災害が発生した場合、フェイルオーバーは 1 回のクリックで開始するか、自動的に実行されるように構成できるため、最小限のダウンタイムでビジネスの継続性を確保できます。

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

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=b2fb8597-c3fe-49e2-8a84-b1f10118db6d

GCP/GCVE 上のワークロードを移行する

VMware HCX を使用して **Google Cloud VMware Engine** 上の **Google Cloud Google Cloud NetApp Volumes**データストアにワークロードを移行する **-** クイックスタート ガイド

Google Cloud VMware Engine と Cloud Volume Service データストアの最も一般的な使用例の 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。

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

VMware HCX は主に、アプリケーションの移行、ワークロードの再調整、さらにはクラウド間のビジネス継続性を簡素化するように設計された移行プラットフォームです。これは Google Cloud VMware Engine プライベート クラウドの一部として含まれており、ワークロードを移行するためのさまざまな方法を提供し、災害復旧 (DR) オペレーションに使用できます。

このドキュメントでは、Cloud Volume Service データストアをプロビジョニングし、その後、オンプレミスと Google Cloud VMware Engine 側のすべての主要コンポーネント（相互接続、ネットワーク拡張、さまざまな VM 移行メカニズムを有効にするための WAN 最適化など）を含む VMware HCX をダウンロード、デプロイ、構成するための手順を詳しく説明します。

> VMware HCX は、移行が VM レベルで行われるため、どのデータストア タイプでも動作します。したがって、このドキュメントは、コスト効率の高い VMware クラウドの導入のために Google Cloud VMware Engine を使用して Cloud Volume Service を導入することを計画している既存のNetApp のお客様と非NetApp のお客様に適用されます。

▼ 大まかな手順

このリストには、オンプレミスの HCX コネクタから 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が示されています。

1. Google VMware Engine ポータルを通じて HCX を準備します。
2. オンプレミスの VMware vCenter Server に HCX コネクタ Open Virtualization Appliance (OVA) インストーラーをダウンロードしてデプロイします。
3. ライセンス キーを使用して HCX をアクティブ化します。

4. オンプレミスの VMware HCX コネクタと Google Cloud VMware Engine 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 メッシュを構成します。
6. (オプション) 移行中に IP の再割り当てを避けるため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します。

▼ 前提条件

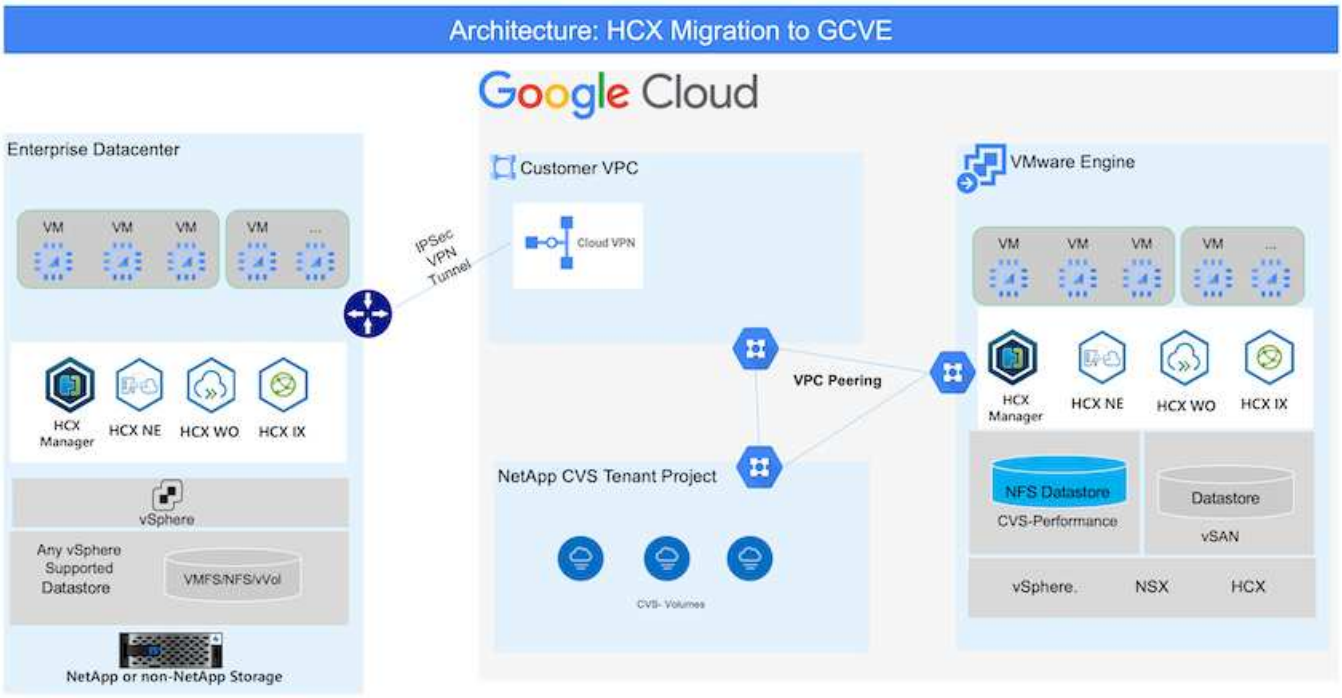
始める前に、次の前提条件が満たされていることを確認してください。詳細については、こちらをご覧ください "リンク"。接続などの前提条件が整ったら、Google Cloud VMware Engine ポータルから HCX ライセンス キーをダウンロードします。 OVA インストーラをダウンロードしたら、以下の説明に従ってインストール プロセスを続行します。

> ⓘ HCX アドバンスドはデフォルトのオプションであり、VMware HCX エンタープライズ エディションもサポート チケットを通じて利用可能で、追加費用なしでサポートされます。参照する "このリンク"

- 既存のGoogle Cloud VMware Engineソフトウェア定義データセンター（SDDC）を使用するか、これを使用してプライベートクラウドを作成します。"NetApp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 または Cloud Interconnect 接続を設定する"オンプレミス環境とそれぞれのプライベート クラウド間。
- 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 パスは、vMotion を使用した VM の移行をサポートしている必要があります。
- 必要な "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 トラフィックが許可されます。
- Cloud Volume Service NFS ボリュームは、Google Cloud VMware Engine にデータストアとしてマウントする必要があります。この手順に従ってください "リンク"Cloud Volume Service データストアを Google Cloud VMware Engines ホストに接続します。

▼ 高レベルアーキテクチャ

テストの目的で、この検証に使用されたオンプレミスのラボ環境は、オンプレミスから Google Cloud VPC への接続を可能にする Cloud VPN を介して接続されました。



GoogleでのVMware HCXの使用に関する詳細については、以下を参照してください。 "VMware リンク"

ソリューションの展開

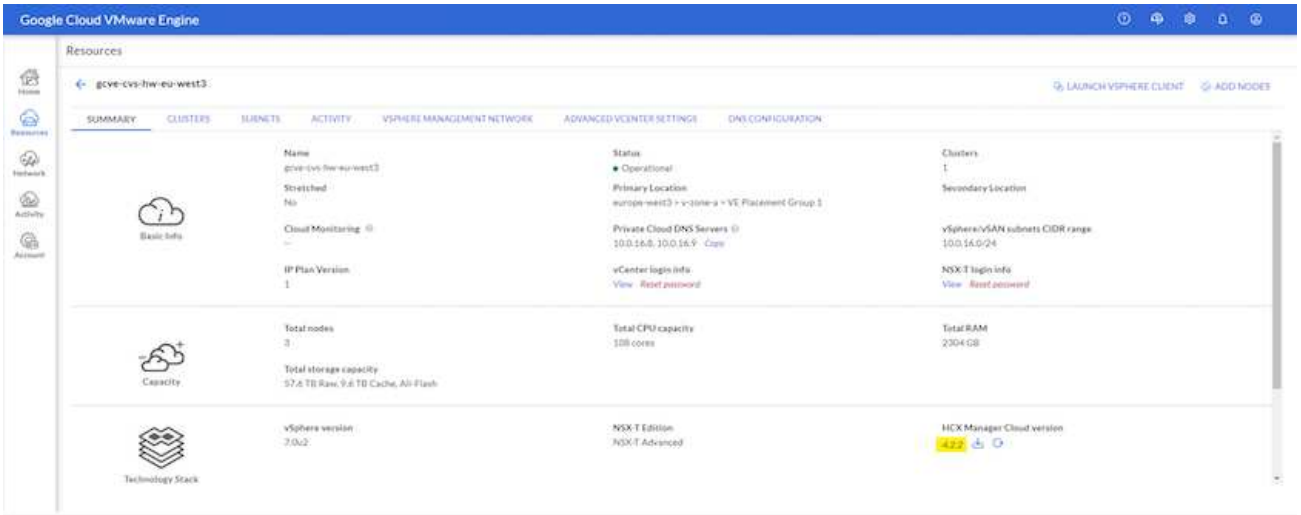
このソリューションの展開を完了するには、次の一連の手順に従います。

▼ ステップ **1: Google VMware Engine** ポータルで **HCX** を準備する

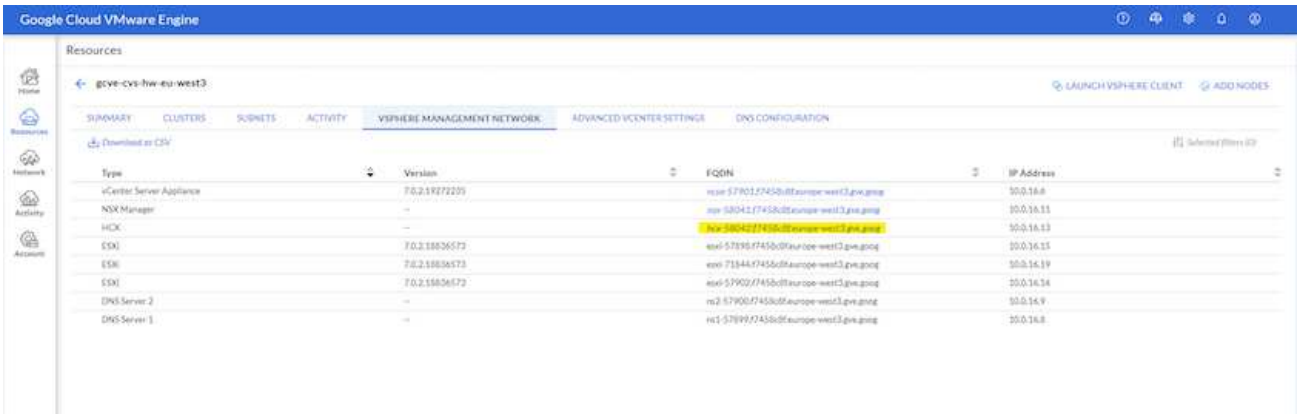
VMware Engine を使用してプライベート クラウドをプロビジョニングすると、HCX Cloud Manager コンポーネントが自動的にインストールされます。サイトのペアリングを準備するには、次の手順を実行します。

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

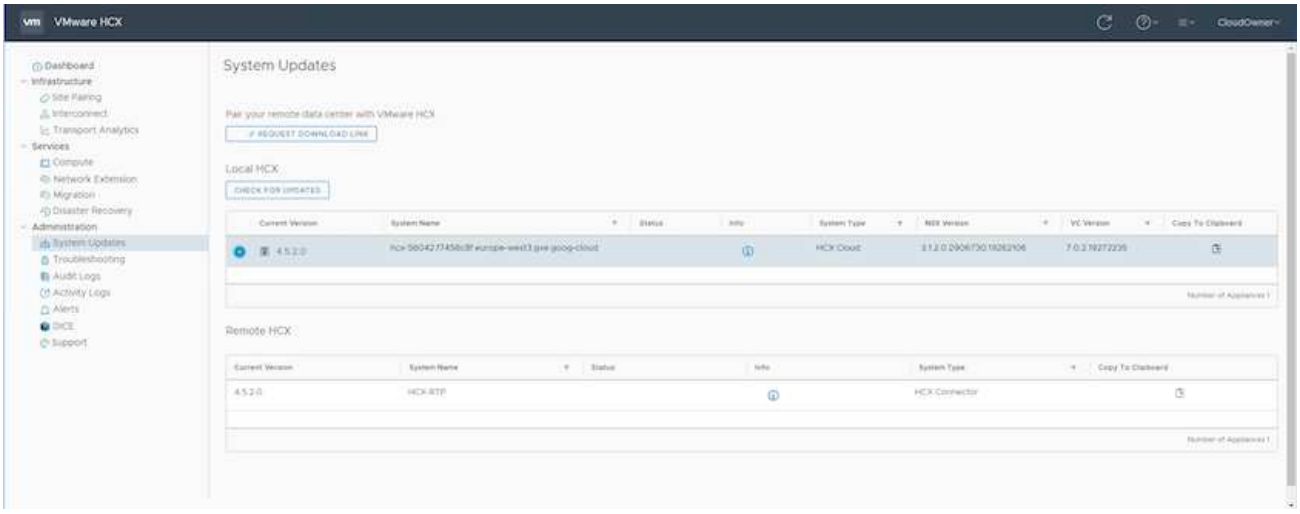
   HCXバージョンリンクをクリックしてHCXコンソールにログインすることができます。



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



2. HCX Cloud Manager で、管理 > システム アップデート に移動します。
3. ダウンロードリンクをリクエスト をクリックして、OVA ファイルをダウンロードします。



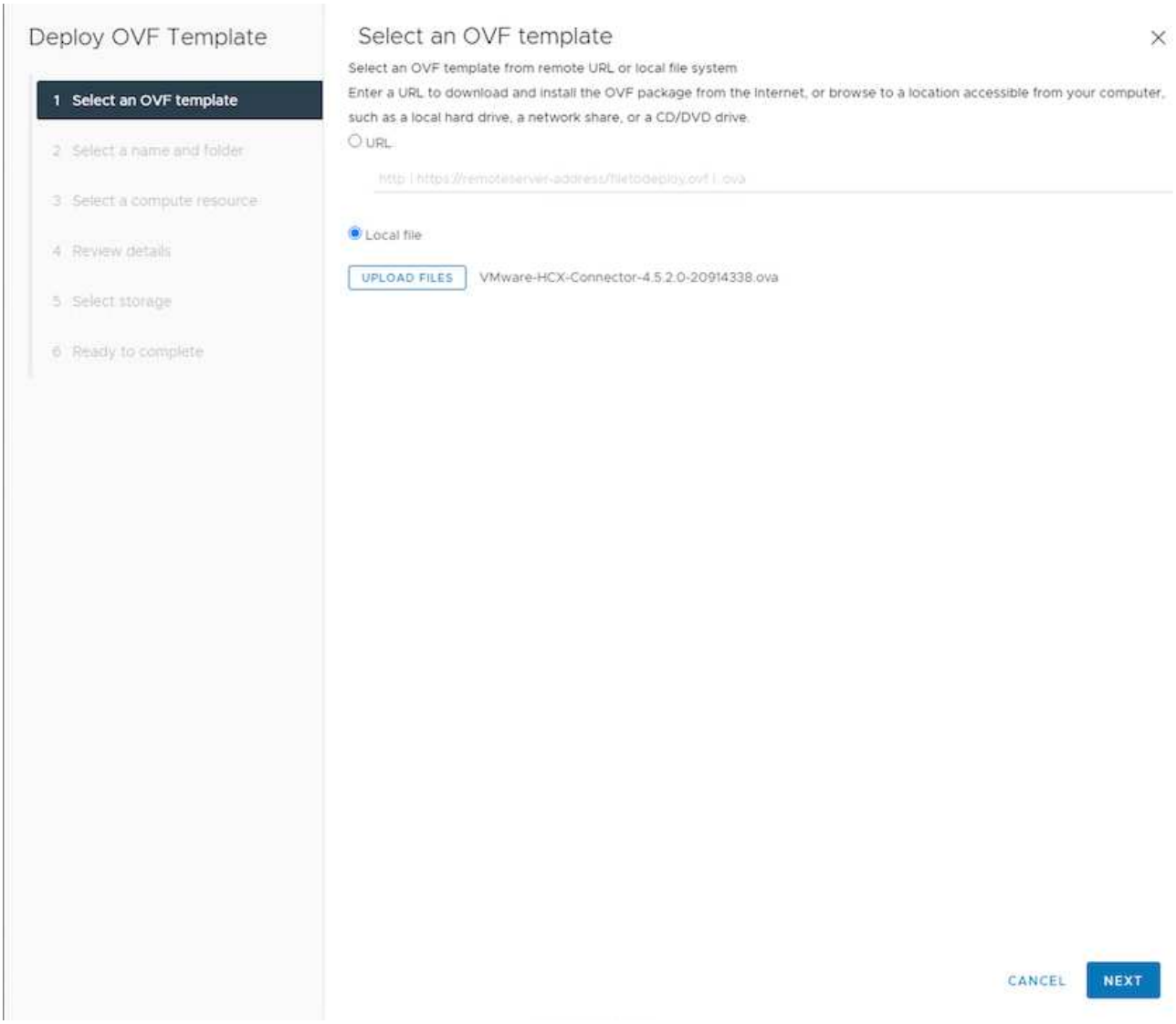
4. HCX Cloud Manager を HCX Cloud Manager UI から入手可能な最新バージョンに更新します。

▼ ステップ**2:** オンプレミスの**vCenter Server**にインストーラ**OVA**を展開する

オンプレミス コネクタを Google Cloud VMware Engine の HCX マネージャーに接続するには、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てください。

オンプレミスの vCenter Server に HCX コネクタを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 の HCX コンソールから ova をダウンロードします。
2. OVA をダウンロードしたら、[OVF テンプレートのデプロイ] オプションを使用して、オンプレミスの VMware vSphere 環境にデプロイします。



3. OVA 展開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 コネクタ OVA を展開します。

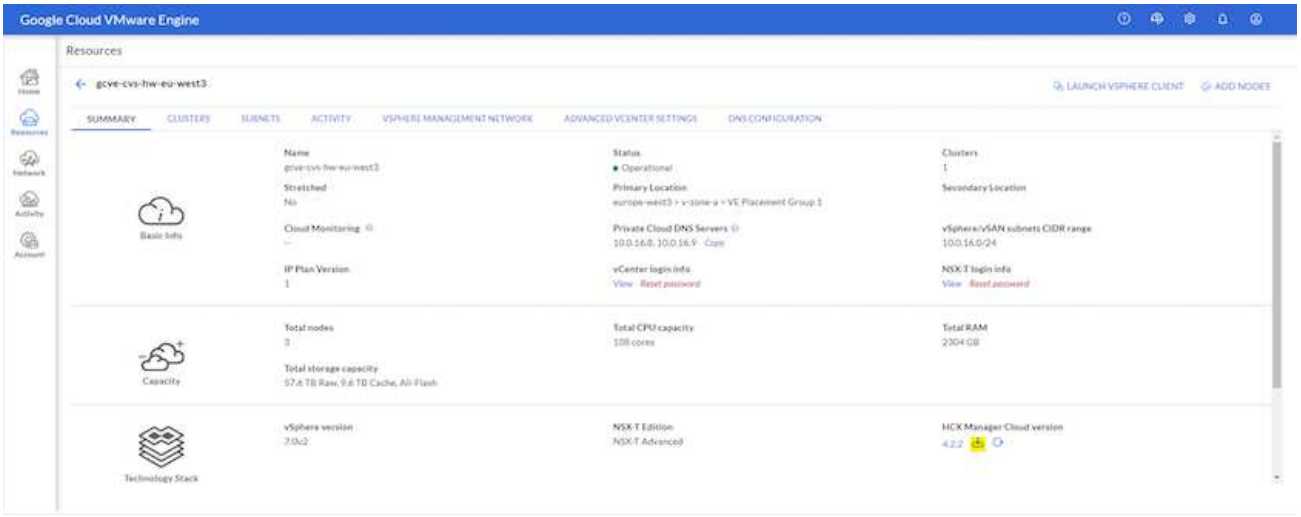
   仮想アプライアンスを手動で電源オンします。

詳しい手順については、 "Google HCX ドキュメント" 。

▼ ステップ**3:** ライセンスキーを使用して**HCX**コネクタをアクティブ化する

VMware HCX コネクタ OVA をオンプレミスにデプロイし、アプライアンスを起動したら、次の手順を実行して HCX コネクタをアクティブ化します。 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 ポータルから、[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** の下のダウンロード 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"`管理者の資格情報を使用します。

   OVA 展開中に定義された hcxmanagerIP とパスワードを使用します。

3. ライセンスで、手順 3 でコピーしたキーを入力し、[アクティブ化] 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. データセンターの場所 で、オンプレミスの VMware HCX Manager をインストールするための最も近い場所を指定します。 *続行*をクリックします。
5. *システム名*の下で名前を更新し、*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** への接続 で、vCenter Server の完全修飾ドメイン名 (FQDN) または IP アドレスと適切な資格情報を入力し、続行 をクリックします。

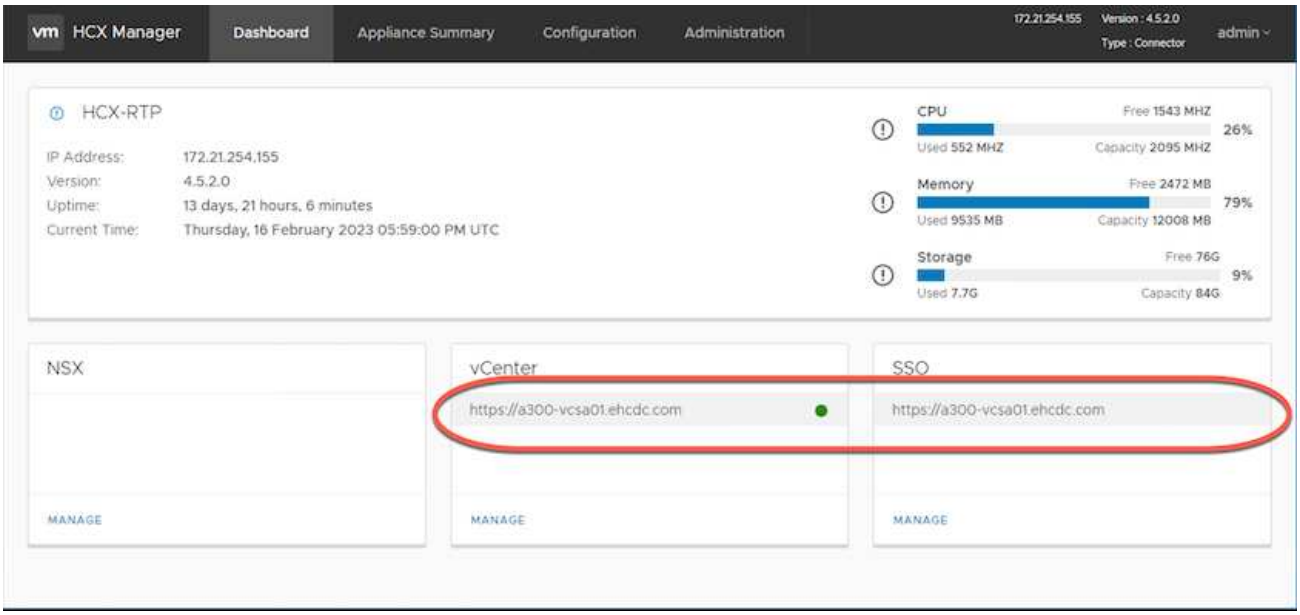
   後で接続の問題を回避するには、FQDN を使用します。

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

   組み込み PSC の場合は、VMware vCenter Server の FQDN または IP アドレスを入力します。

9. 入力した情報が正しいことを確認して、[再起動] をクリックします。
10. サービスが再起動すると、表示されるページで vCenter Server が緑色で表示されます。 vCenter Server と SSO の両方に適切な構成パラメータが設定されている必要があります。これは前のページと同じである必要があります。

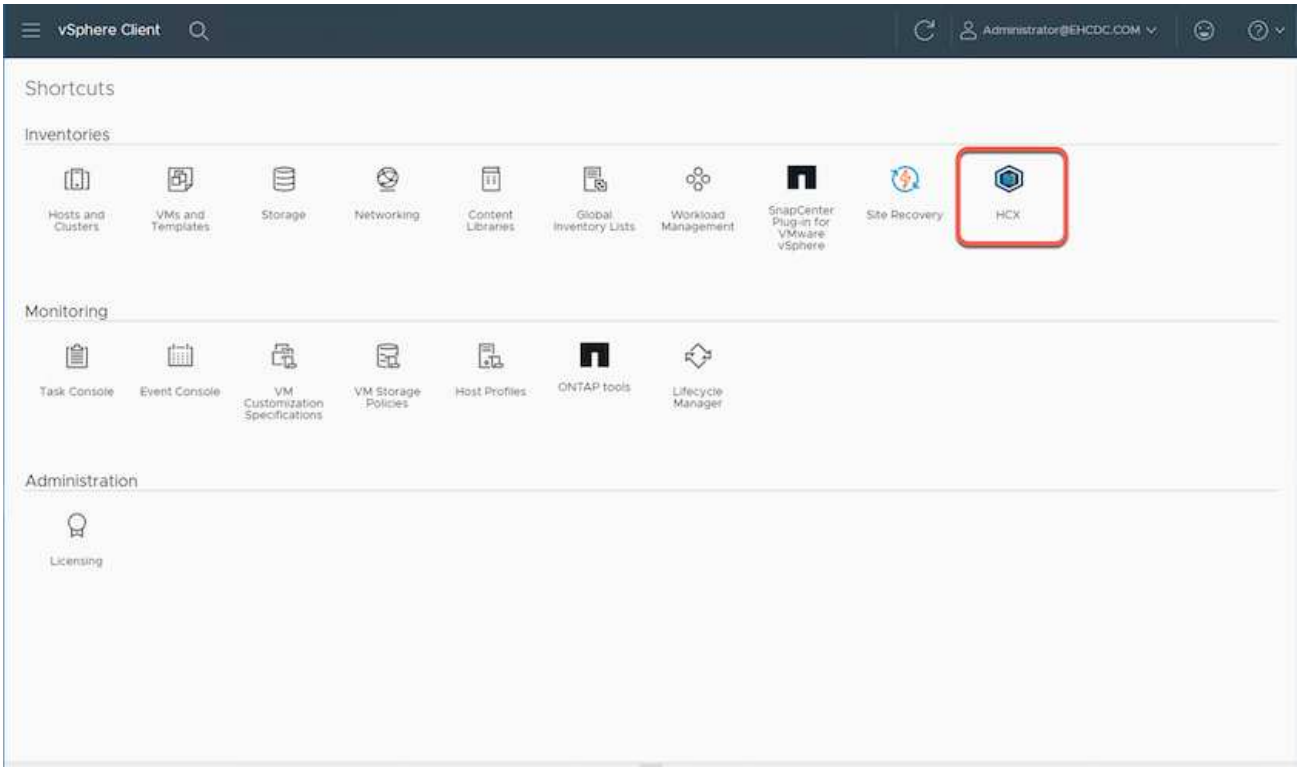
    このプロセスには、プラグインが vCenter Server に追加されるまでに約 10 ～ 20 分かかります。



▼ ステップ **4:** オンプレミスの **VMware HCX** コネクタと **Google Cloud VMware Engine HCX Cloud Manager** をペアリングする

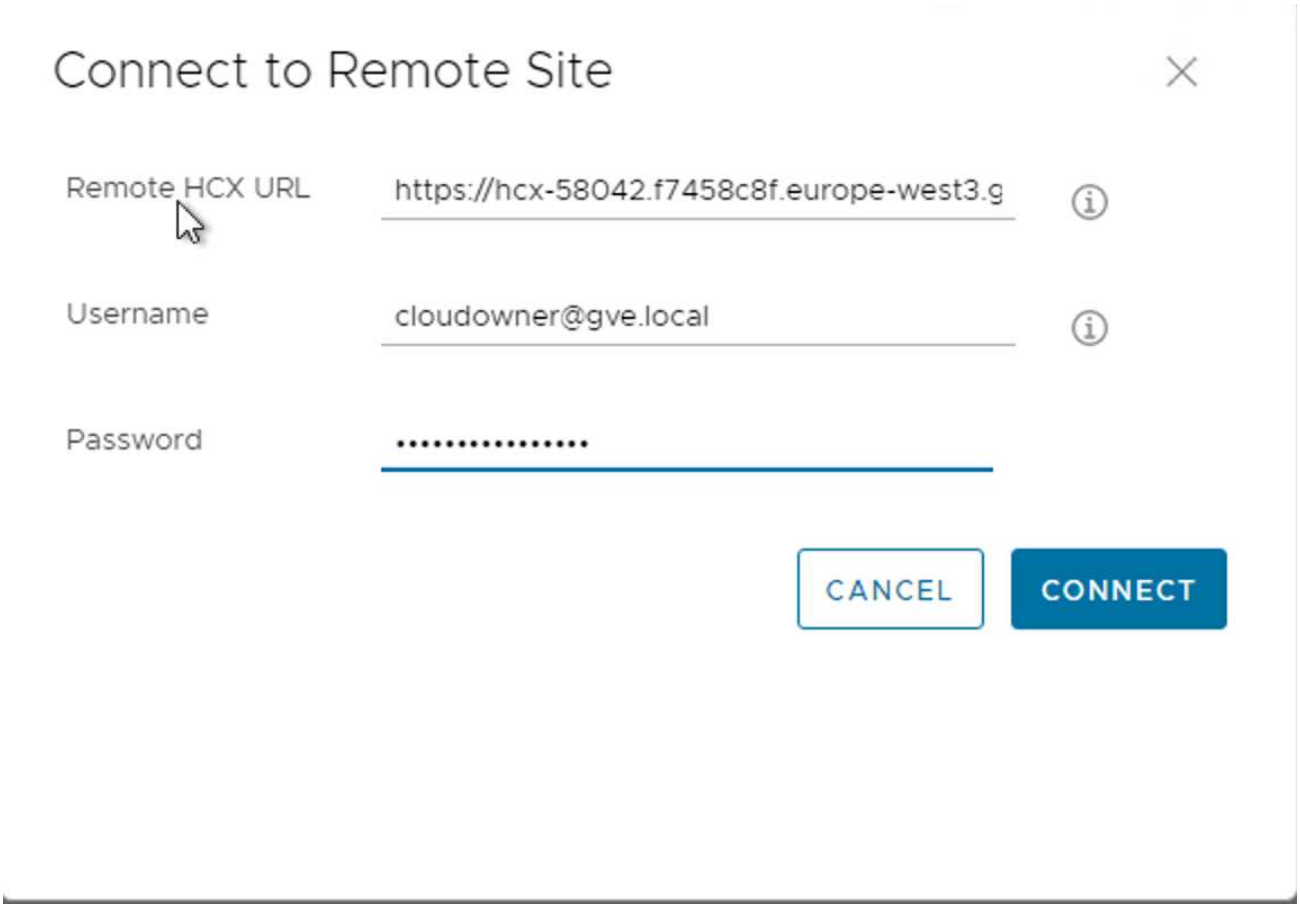
HCX コネクタをオンプレミスの vCenter にデプロイして構成したら、ペアリングを追加して Cloud Manager への接続を確立します。サイトのペアリングを構成するには、次の手順を実行します。

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の下で、[サイトペアリングを追加]をクリックします。

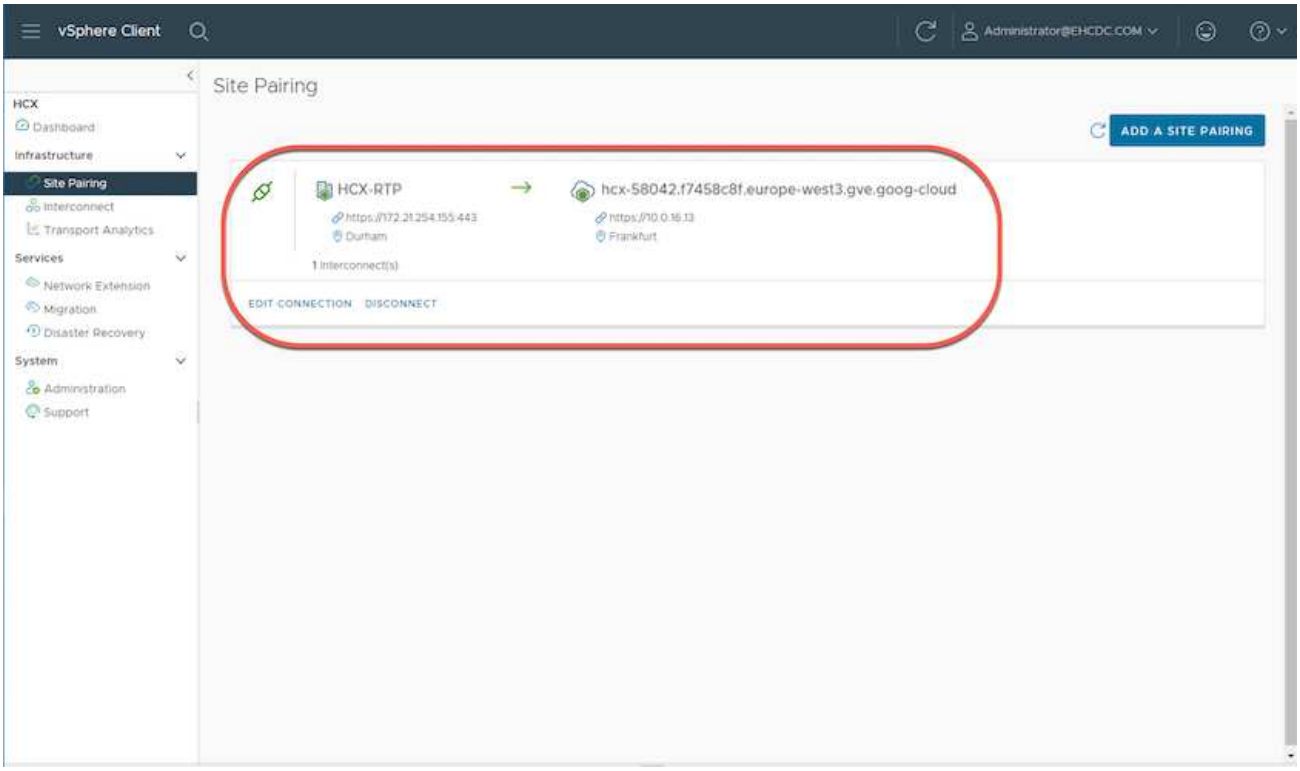
Google Cloud VMware Engine HCX Cloud Manager の URL または IP アドレスと、プライベート クラウドにアクセスするための Cloud-Owner-Role 権限を持つユーザーの認証情報を入力します。



3. *接続*をクリックします。

VMware HCX コネクタは、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 ダッシュボードで利用できるようになります。

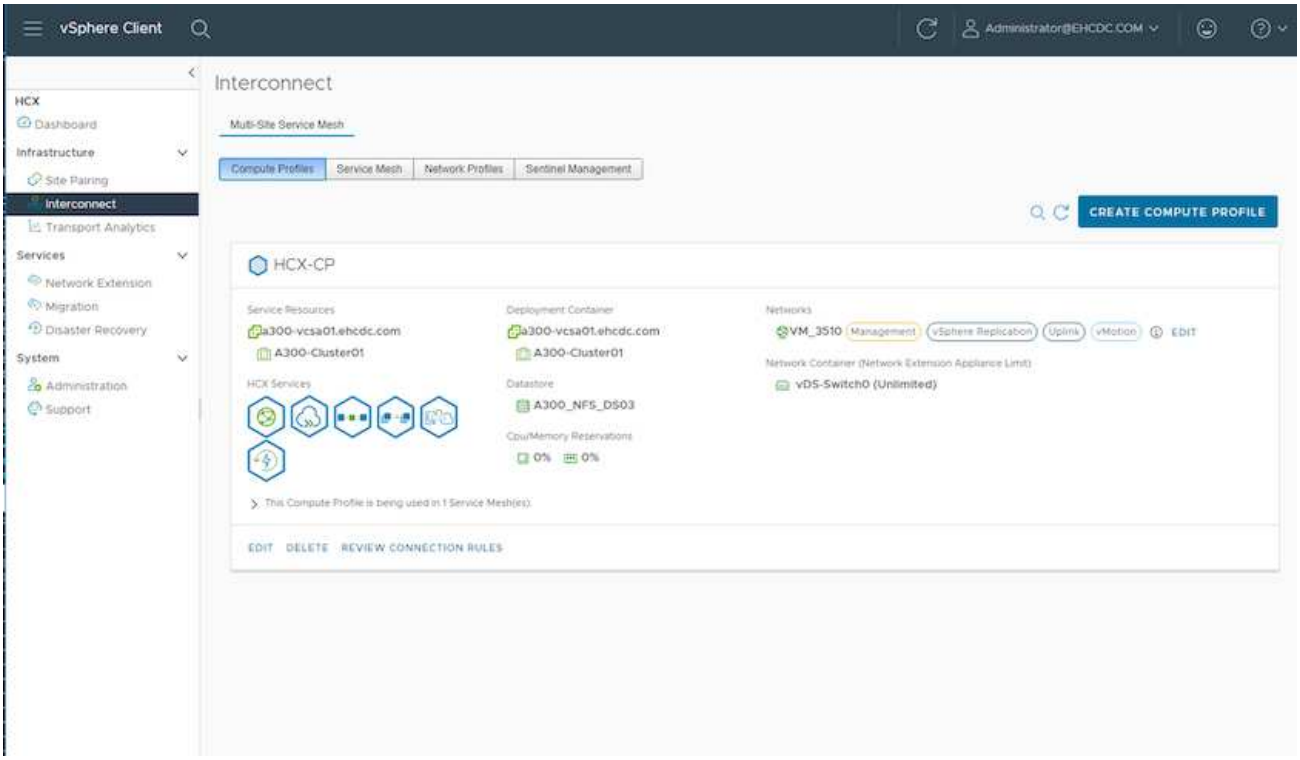


▼ ステップ**5:** ネットワークプロファイル、コンピューティングプロファイル、サービスメッシュを構成する

VMware HCX Interconnect サービス アプライアンスは、インターネット経由およびターゲット サイトへのプライベート接続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ます。相互接続は、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。 Interconnect 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] で、**[**相互接続**] > [**マルチサイト サービス メッシュ**] > [**コンピューティング プロファイル**] > [**コンピューティング プロファイルの作成**]** を選択します。

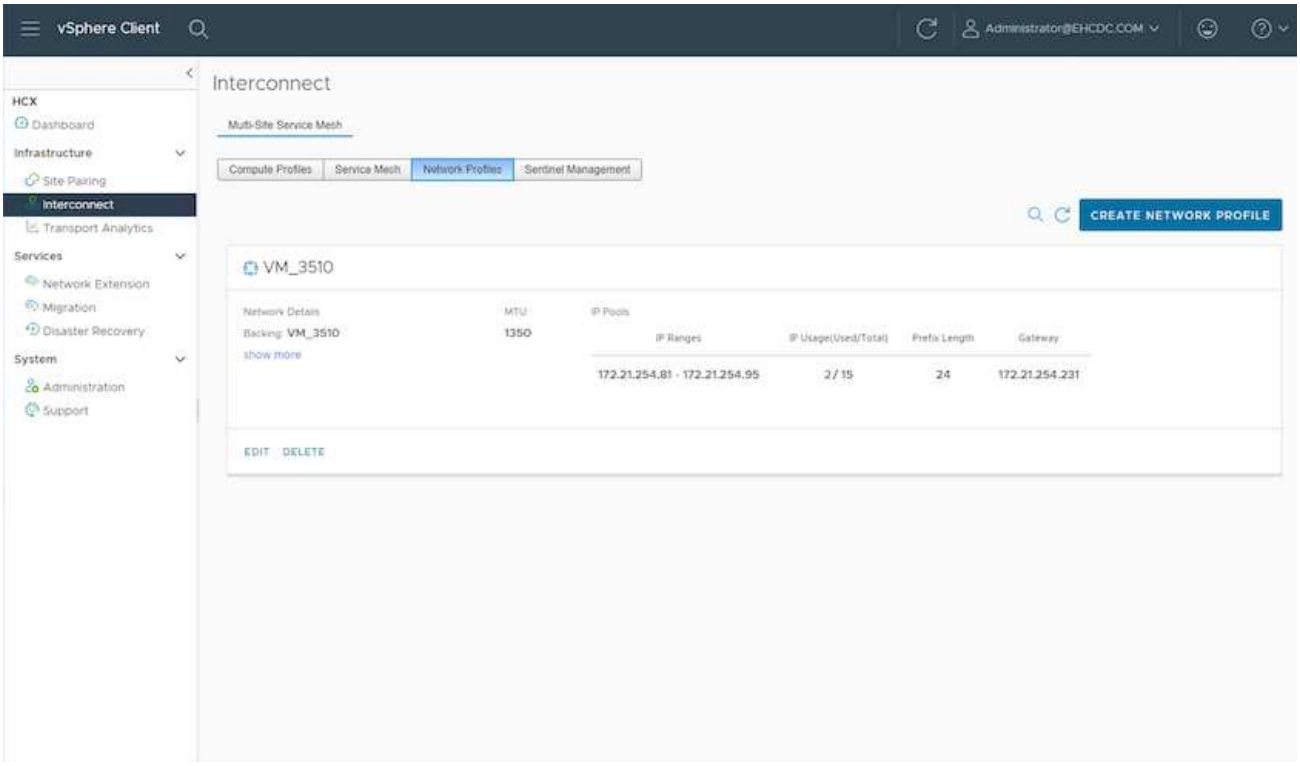
> ⓘ コンピューティング プロファイルは、展開されるアプライアンスや、HCX サービスにアクセス可能な VMware データセンターの部分などの展開パラメータを定義します。



2. コンピューティング プロファイルが作成されたら、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。

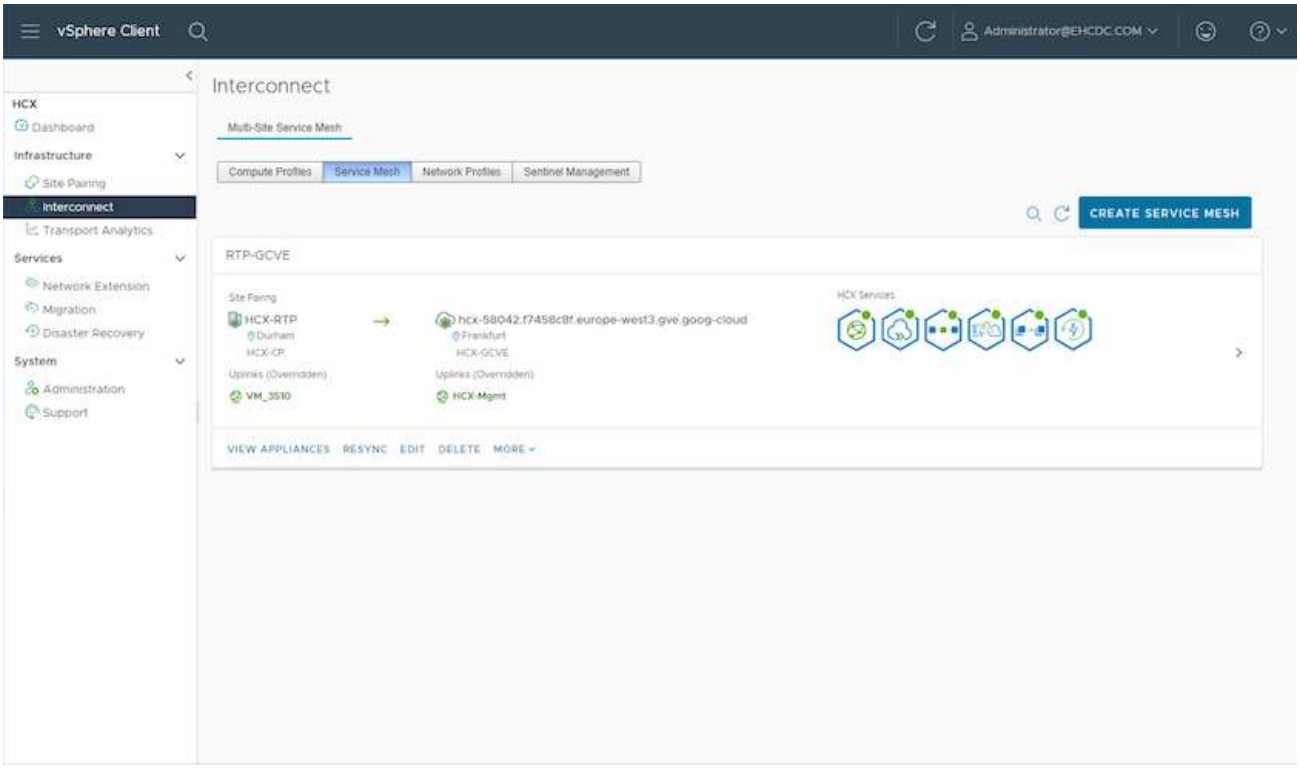
   ネットワーク プロファイルは、HCX が仮想アプライアンスに使用する IP アドレスとネットワークの範囲を定義します。

   この手順では 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 Interconnect Appliances に割り当てられます。

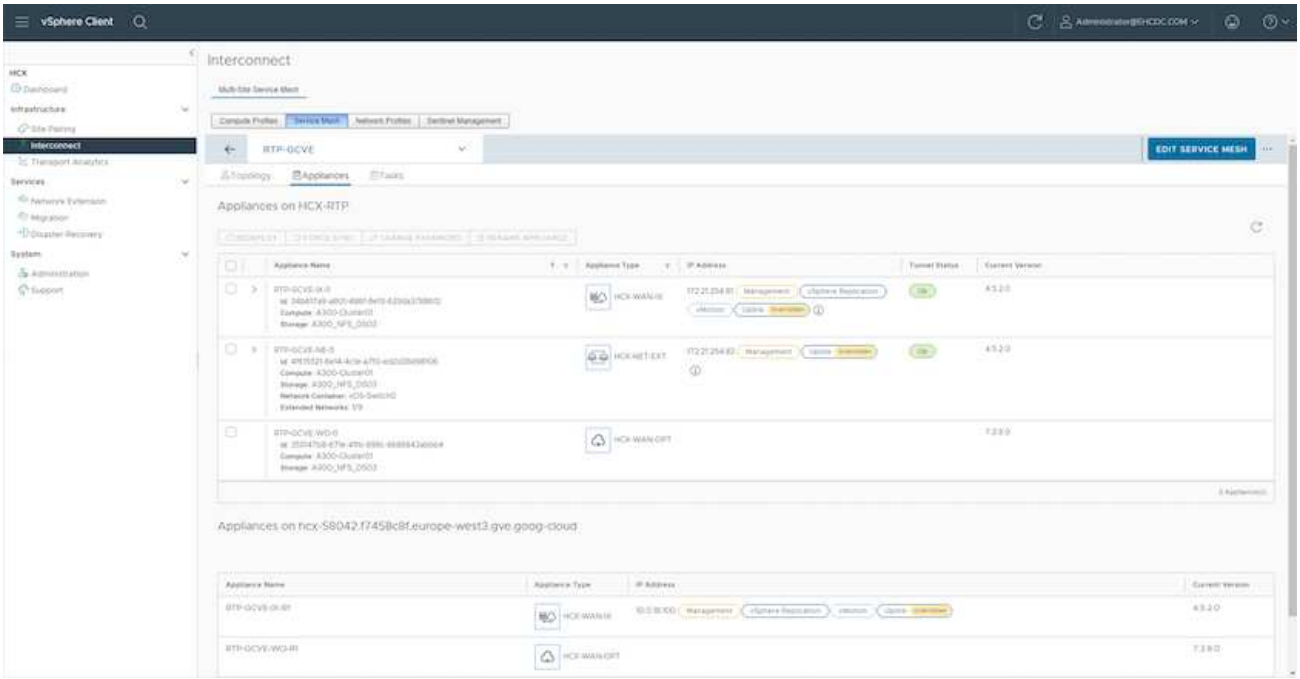


3. この時点で、コンピューティング プロファイルとネットワーク プロファイルが正常に作成されました。
4. **Interconnect** オプション内の **Service Mesh** タブを選択してサービス メッシュを作成し、オンプレミスと GCVE SDDC サイトを選択します。
5. サービス メッシュは、ローカルおよびリモートのコンピューティングとネットワーク プロファイルのペアを指定します。

> このプロセスの一環として、安全なトランスポート ファブリックを作成するために、HCX アプライアンスがソース サイトとターゲット サイトの両方に展開され、自動的に構成されます。



6. これは設定の最終ステップです。デプロイメントが完了するまでに約 30 分かかります。サービス メッシュが構成されると、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、環境が準備されます。



▼ ステップ**6:** ワークロードを移行する

さまざまな VMware HCX 移行テクノロジーを使用して、オンプレミスと GCVE SDDC 間でワークロードを双方向に移行できます。 HCX 一括移行、HCX vMotion、HCX コールド移行、HCX レプリケーション アシスト vMotion (HCX Enterprise エディションで利用可能)、HCX OS アシスト移行 (HCX Enterprise エディションで利用可能) などの複数の移行テクノロジーを使用して、VMware HCX がアクティブ化されたエンティティ間で VM を移動できます。

さまざまなHCX移行メカニズムの詳細については、以下を参照してください。 "VMware HCX ドキュメントを使用した VMware VM の移行" 。

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

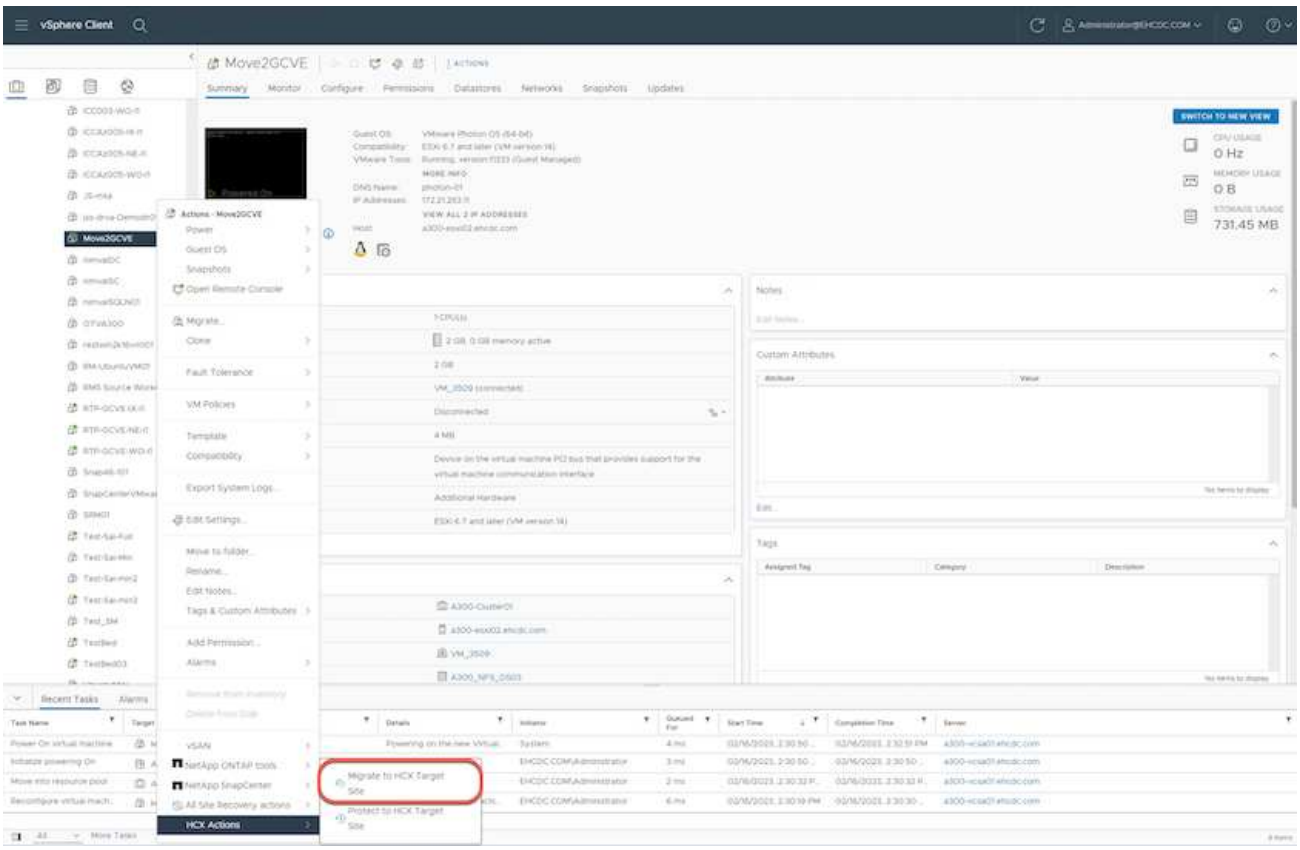
> ⓘ HCX-IX アプライアンスは、Mobility Agent サービスを vCenter Server のホスト オブジェクトとして追加します。このオブジェクトに表示されるプロセッサ、メモリ、ストレージ、およびネットワーク リソースは、IX アプライアンスをホストする物理ハイパーバイザー上の実際の消費量を表すものではありません。

HCX vMotion

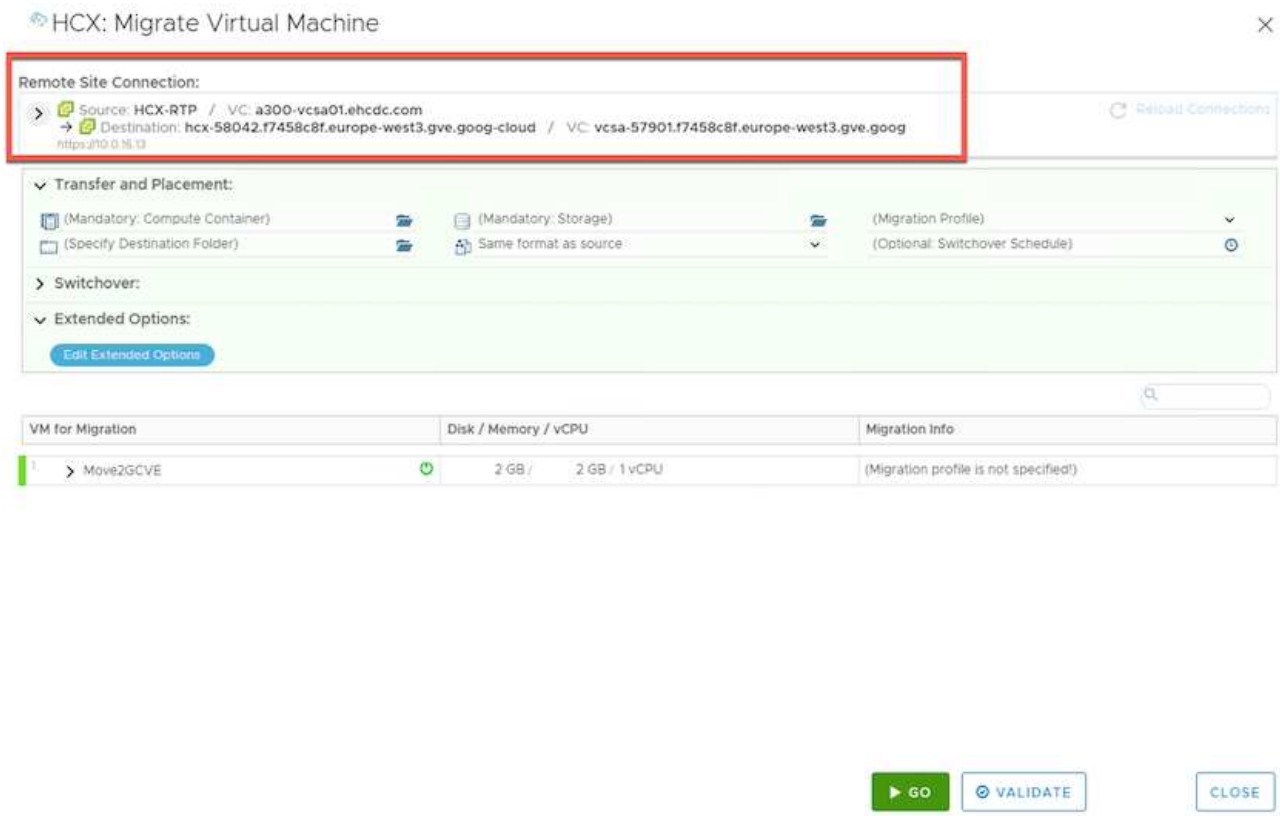
このセクションでは、HCX vMotion メカニズムについて説明します。この移行テクノロジーは、VMware vMotion プロトコルを使用して VM を GCVE に移行します。 vMotion 移行オプションは、一度に 1 つの VM の VM 状態を移行するために使用されます。この移行方法ではサービスの中断は発生しません。

> ⓘ IP アドレスを変更せずに VM を移行するには、ネットワーク拡張機能 (VM が接続されているポート グループに対して) が配置されている必要があります。

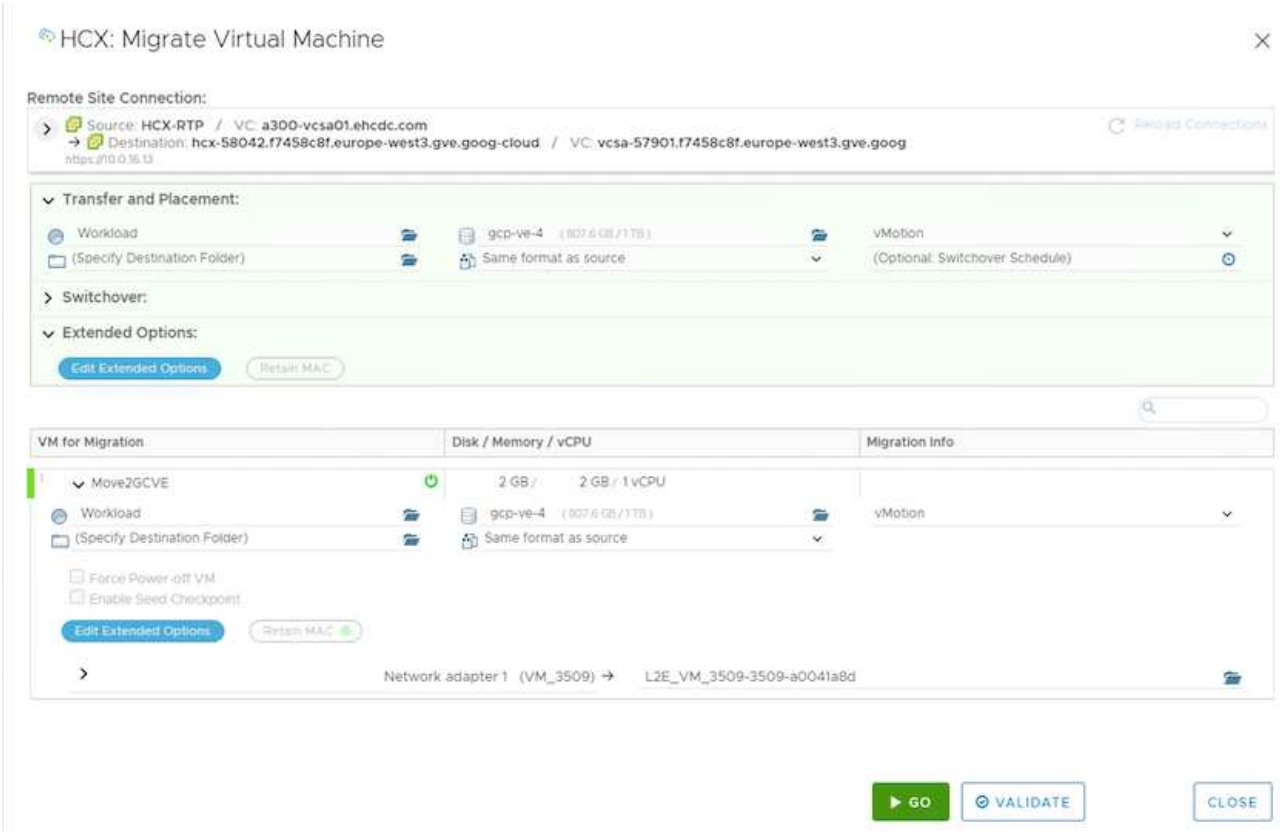
1. オンプレミスの vSphere クライアントから [インベントリ] に移動し、移行する VM を右クリックして、[HCX アクション] > [HCX ターゲット サイトに移行] を選択します。



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。



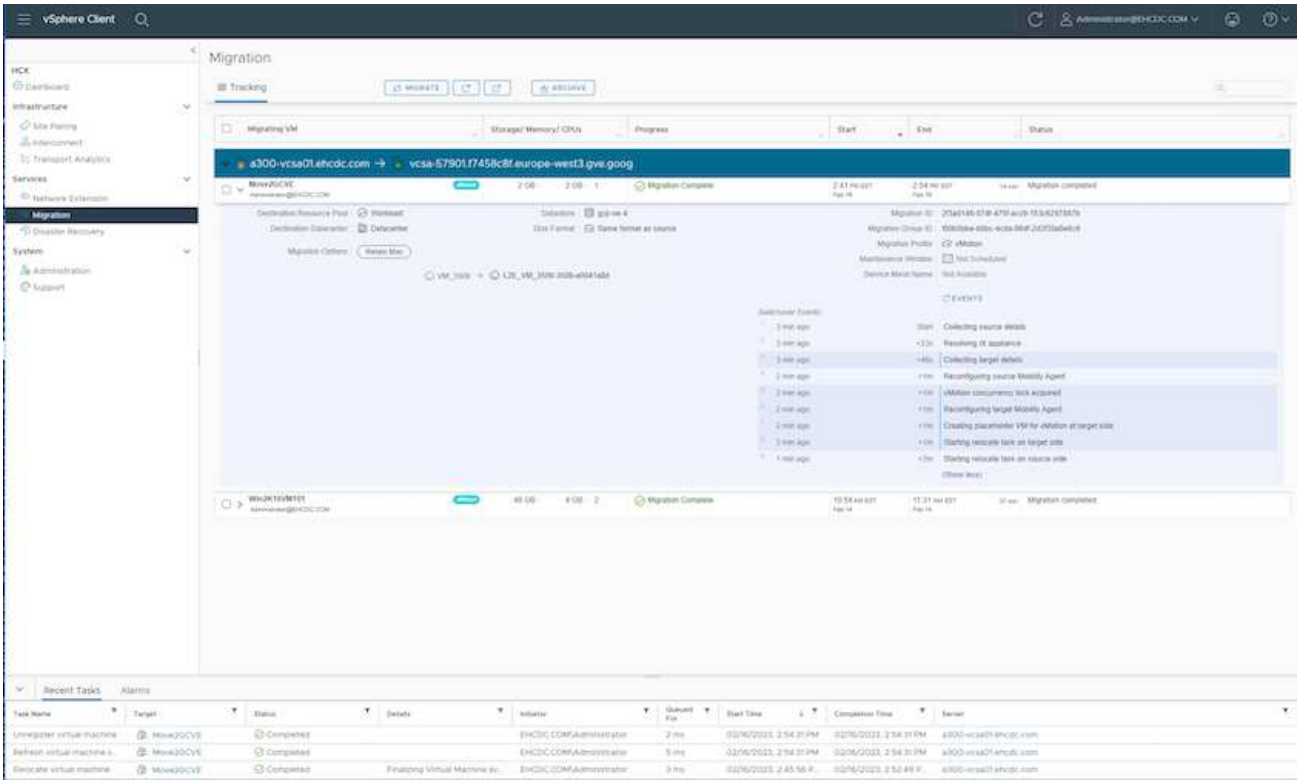
3. 必須フィールド (クラスター、ストレージ、宛先ネットワーク) を更新し、[検証] をクリックします。



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 転送では、VM のアクティブ メモリ、実行状態、IP アドレス、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、以下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の理解" 。

5. HCX > 移行ダッシュボードから、vMotion の進行状況と完了を監視できます。



ターゲットのGoogle Cloud NetApp Volumes (NetApp Volumes) NFS データストアには、移行を処理するのに十分なスペースが必要です。

まとめ

オールクラウドまたはハイブリッド クラウドを対象としており、データがオンプレミスのあらゆるタイプ/ベンダーのストレージに存在する場合でも、Cloud Volume Service と HCX は、データ要件をアプリケーション層にシームレスにすることで TCO を削減しながら、アプリケーション ワークロードを展開および移行するための優れたオプションを提供します。ユースケースを問わず、Google Cloud VMware Engine と Cloud Volume Service を併せて選択すると、クラウドのメリットを迅速に実現でき、オンプレミスと複数のクラウドにわたる一貫したインフラストラクチャと運用、ワークロードの双方向の移植性、エンタープライズ グレードの容量とパフォーマンスが得られます。これは、VMware vSphere Replication、VMware vMotion、またはネットワーク ファイル コピー (NFC) を使用してストレージを接続し、VMware 仮想マシンを移行するために使用される、使い慣れたプロセスと手順と同じです。

まとめ

このドキュメントの主なポイントは次のとおりです。

- Google Cloud VMware Engine SDDC 上のデータストアとして Cloud Volume Service を使用できるようになりました。
- オンプレミスから Cloud Volume Service データストアにデータを簡単に移行できます。

- 移行アクティビティ中の容量とパフォーマンスの要件を満たすために、Cloud Volume Service データストアを簡単に拡大および縮小できます。

参考として**Google**と**VMware**のビデオ

▼ **Google**から

- "GCVE を使用して HCX コネクタをデプロイする"
- "GCVE を使用して HCX ServiceMesh を構成する"
- "HCX を搭載した VM を GCVE に移行する"

▼ **VMware**から

- "GCVE 向け HCX コネクタの展開"
- "GCVE の HCX ServiceMesh 構成"
- "HCX ワークロードの GCVE への移行"

詳細情報の入手方法

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

- Google Cloud VMware Engine ドキュメント

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

- Cloud Volume Service ドキュメント

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- VMware HCX ユーザーガイド

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

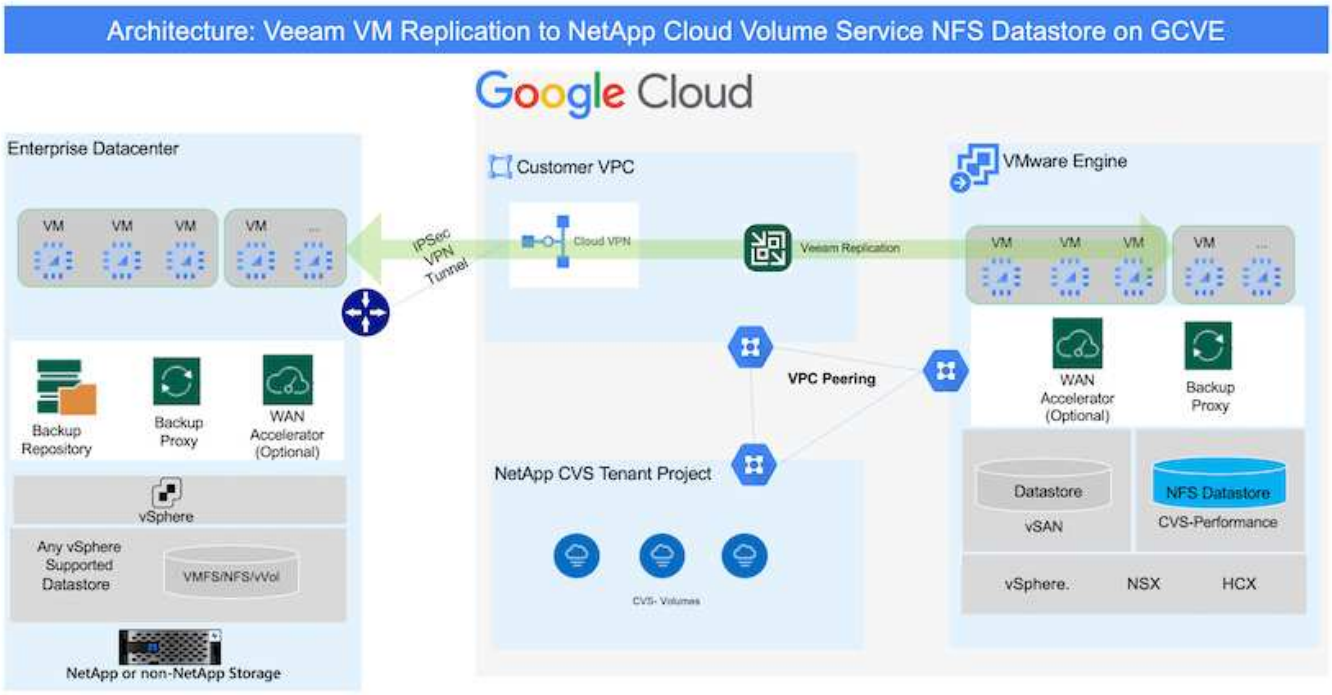
Veeam レプリケーション機能を使用した **Google Cloud VMware Engine** 上の**Google Cloud NetApp Volumes NFS** データストアへの **VM** 移行

現在、データ保護の要件に Veeam を使用しているお客様は、引き続きそのソリューションを使用してワークロードを GCVE に移行し、 Google Cloud NetApp Volumes NFS データストアのメリットを享受できます。

概要

VMware vSphere 上で実行されている VM ワークロードは、Veeam レプリケーション機能を利用して Google Cloud VMware Engine (GCVE) に移行できます。

このドキュメントでは、Google Cloud NetApp Volumes、Veeam、Google Cloud VMware Engine（GCVE）を使用した VM 移行を設定および実行するための手順を詳しく説明します。



前提

このドキュメントでは、既存の vSphere サーバーから 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 または Cloud Interconnect またはその他のネットワーク オプションが準備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 に接続するには複数のオプションがあるため、このドキュメントでは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。参照"Google Cloud ドキュメント"オンプレミスから Google への適切な接続方法については、こちらをご覧ください。

移行ソリューションの導入

ソリューション展開の概要

1. Google Cloud NetApp Volumes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する
3. レプリケーション ジョブを作成して、仮想マシンを Google Cloud VMware Engine インスタンスにレプリケーションし始めます。
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 で永続的なフェイルオーバーを実行します。

導入環境の詳細

Google Cloud NetApp Volumes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、十分なスペースのある NFS データストアが利用可能であることを確認しま

す。そうでない場合は、"GCVE でNetAppボリュームを NFS データストアとしてマウントする"

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

参照してください"Veeam レプリケーション 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、仮想マシンを **Google Cloud VMware Engine** インスタンスにレプリケーションし始めます。

オンプレミスの vCenter と GCVE vCenter の両方を 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のセットアップ"方法を説明したビデオはこちら"レプリケーションジョブの構成"。

> ⓘ 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、上記のビデオをご覧ください。

Veeam レプリケーションジョブのフェイルオーバーを実行する

VMを移行するには、以下を実行します。"フェイルオーバーを実行する"

Veeam で永続的なフェイルオーバーを実行します。

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

このソリューションの利点

- 既存の Veeam バックアップ インフラストラクチャを移行に利用できます。
- Veeam Replication では、ターゲット サイトの VM IP アドレスを変更できます。
- Veeamの外部で複製された既存のデータを再マッピングする機能があります（NetAppシステムから複製されたデータなど）
- ターゲット サイトで異なるネットワーク ポート グループを指定する機能があります。
- VM の電源をオンにする順序を指定できます。
- VMware Change Block Tracking を利用して、WAN 経由で送信されるデータの量を最小限に抑えます。
- レプリケーションの事前スクリプトと事後スクリプトを実行する機能。
- スナップショットの事前スクリプトと事後スクリプトを実行する機能。

Google Cloud のGoogle Cloud NetApp Volumesでデータを保護

TR-4918: セキュリティの概要 **- Google Cloud** の**Google Cloud NetApp Volumes**

オリバー・クラウス、ジャスティン・パリシ、 NetApp

インフラストラクチャがストレージ管理者の管理下にないクラウド環境では特に、クラウドプロバイダーが提供するサービスにデータを安心して預けるためにセキュリティが極めて重要です。このドキュメントは、セキュリティサービスの概要です "Google Cloud NetApp VolumesはGoogle Cloudで"。

対象読者

このドキュメントの対象読者には、以下の役割を持つ方が含まれますが、これに限定されません。

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

この技術レポートの内容についてご質問がある場合は、"お問い合わせ。"

略語	定義
NetAppボリューム-SW	Google Cloud NetApp Volumes、サービスタイプNetApp Volumes
NetAppボリュームパフォーマンス	クラウド ボリューム サービス、サービス タイプNetApp Volumes-Performance
公共広告	

Google Cloud NetApp Volumes がデータを保護する仕組み

Google Cloud のGoogle Cloud NetApp Volumes は、データをネイティブに保護するためのさまざまな方法を提供します。

安全なアーキテクチャとテナントモデル

Google Cloud NetApp Volumes は、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）を異なるエンドポイントに分割することで、Google Cloud で安全なアーキテクチャを提供します。これにより、どちらが他方に影響を与えなくなります（セクションを参照）。"Google Cloud NetApp Volumes アーキテクチャ" ）。 Googleの "プライベートサービスアクセス"（PSA）フレームワークを使用してサービスを提供します。このフレームワークは、 NetAppによって提供および運用されるサービス プロデューサーと、 Google Cloud NetApp Volumes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内の仮想プライベート クラウド (VPC) であるサービス コンシューマーを区別します。

このアーキテクチャでは、テナント（セクション"賃貸モデル"）は、ユーザーが明示的に接続しない限り、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。テナントでは、Google Cloud NetApp Volumes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、ソリューションのその他の重要な部分を他のテナントから完全に分離できます。 Google Cloud NetApp Volumes プラットフォームは VPC ピアリングを介して接続されているため、その分離も適用されます。共有VPCを使用すると、複数のプロジェクト間でGoogle Cloud NetApp Volumesボリュームを共有できます（セクションを参照）。"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して、データセットを表示または変更できるユーザーまたは機能を制限できます。

コントロールプレーンの強力な**ID**管理

Google Cloud NetApp Volumesの設定が行われるコントロールプレーンでは、ID管理は以下を使用して管理されます。 "アイデンティティアクセス管理（IAM）" 。 IAM は、Google Cloud プロジェクト インスタンスへの認証（ログイン）と承認（権限）を制御できる標準サービスです。すべての構成は、TLS 1.2 暗号化を使用した安全な HTTPS トランスポート経由でGoogle Cloud NetApp Volumes API を使用して実行され、セキュリテ

ィ強化のために JWT トークンを使用して認証が実行されます。 Google Cloud NetApp Volumesの Google コンソール UI は、ユーザー入力をGoogle Cloud NetApp Volumes API 呼び出しに変換します。

セキュリティ強化 - 攻撃対象領域の制限

効果的なセキュリティの一環として、サービス内で利用可能な攻撃対象領域の数を制限することが重要です。攻撃対象領域には、保存中のデータ、転送中のデータ、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 サービスでは、その設計上、攻撃対象領域の一部が本質的に排除されます。インフラストラクチャ管理については、セクション"サービス運営、"専任チームによって処理され、自動化されているため、人間が実際に構成に触れる回数が減り、意図的および意図しないエラーの数を減らすことができます。必要なサービスのみが相互にアクセスできるように、ネットワークが隔離されています。暗号化はデータ ストレージに組み込まれており、 Google Cloud NetApp Volumes管理者によるセキュリティ上の注意が必要なのはデータ プレーンのみです。管理の大部分を API インターフェースの背後に隠すことで、攻撃対象領域を制限し、セキュリティを実現します。

ゼロトラストモデル

歴史的に、IT セキュリティの哲学は「信頼はするが検証もする」であり、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) のみに依存するという形で現れてきました。しかし、攻撃や侵害は進化し、フィッシング、ソーシャル エンジニアリング、内部脅威、およびネットワークに侵入して大混乱を引き起こすための検証を提供するその他の方法を通じて、環境内の検証を回避するようになりました。

ゼロ トラストはセキュリティにおける新しい方法論となり、現在のモットーは「何も信頼せず、すべてを検証する」です。したがって、デフォルトでは何もアクセスが許可されません。このマントラは、標準的なファイアウォールや侵入検知システム (IDS) などのさまざまな方法で実施されるほか、次の方法でも実施されます。

- 強力な認証方法（AES暗号化KerberosやJWTトークンなど）
- 単一の強力な ID 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テーションと安全なマルチテナント（デフォルトではテナントのみアクセスが許可されます）
- 最小権限アクセスポリシーによるきめ細かなアクセス制御
- デジタル監査と書類による記録を備えた、信頼できる専任管理者の限定リスト

Google Cloud で実行されるGoogle Cloud NetApp Volumes は、 「何も信頼せず、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（セクションを参照）"保存時のデータ暗号化" ）は、 NetAppボリューム暗号化（NVE）とXTS-AES-256暗号を使用して、"SMB暗号化"または NFS Kerberos 5p サポート。リージョン間レプリケーション転送は TLS 1.2 暗号化によって保護されているので安心です (セクション "リージョン間レプリケーション" を参照)。さらに、Googleネットワークでは暗号化された通信も提供しています（"転送中のデータ暗号化") を追加して、攻撃に対する保護を強化します。トランスポート暗号化の詳細については、セクション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、攻撃を防ぐことだけではありません。また、攻撃が発生した場合に、どのように回復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。 Google Cloud NetApp Volumesは、障害発生時に他のリージョンにレプリケーションする方法を提供します（セクションを参照）。"クロスリージョンレプリケーション") 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ている場合。また、 Google Cloud NetApp Volumesインスタンスの外部の場所に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。"Google Cloud NetApp Volumes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 イベントの軽減にかかる時間が短縮され、管理者のコストと負担を軽減できます。

業界をリードするスナップショットコピーによる迅速なランサムウェア対策

Google Cloud NetApp Volumesは、データ保護とバックアップに加えて、不変のスナップショットコピーのサポートも提供します（セクションを参照）。"不変のスナップショットコピー"ランサムウェア攻撃からの回復を可能にするボリューム（セクションを参照）"サービス運営" ）が問題を発見してから数秒以内に、最小限の混乱で対応します。リカバリ時間と影響はスナップショットの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のわずか 1 時間の差分を提供するスナップショット コピーを作成できます。スナップショット コピーはパフォーマンスと容量の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ためのリスクが低く、メリットが大きいアプローチです。

セキュリティ上の考慮事項と攻撃対象領域

データを保護する方法を理解するための最初のステップは、リスクと潜在的な攻撃対象領域を特定することです。

これらには、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
- 飛行中のデータ
- 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

攻撃対象領域を理解することで、環境をより安全に保護することができます。 Google Cloud のGoogle Cloud NetApp Volumes はすでにこれらのトピックの多くを考慮しており、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。

安全なログインの確保

重要なインフラストラクチャ コンポーネントを保護するときは、承認されたユーザーだけ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。悪意のある人物が管理者の資格情報を侵害した場合、彼らは城の鍵を入手し、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など、何でも実行できるようになります。

Google Cloud NetApp Volumes for Google Cloud は、ストレージ サービス (StaaS) を難読化することで、不正な管理者ログインから保護します。 Google Cloud NetApp Volumes はクラウド プロバイダーによって完全に管理されており、外部からログインすることはできません。すべてのセットアップおよび構成操作は完全に自動化されているため、非常にまれな状況を除いて、人間の管理者がシステムと対話する必要はありません。

ログインが必要な場合、Google Cloud のGoogle Cloud NetApp Volumes は、システムにログインするアクセス権を持つ信頼できる管理者の非常に短いリストを維持することで、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悪意のある行為者の数を減らすのに役立ちます。さらに、Google Cloud ネットワークはシステムをネットワーク セキュリティの層の背後に隠し、外部には必要なものだけを公開します。 Google Cloud、 Google Cloud NetApp Volumesアーキテクチャの詳細については、次のセクションをご覧ください。"Google Cloud NetApp Volumes のアーキテクチャ。"

クラスタ管理とアップグレード

潜在的なセキュリティ リスクがある 2 つの領域には、クラスター管理 (悪意のあるユーザーが管理者アクセス権を取得した場合に何が起こるか) 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何が起こるか) が含まれます。

ストレージ管理保護

サービスとして提供されるストレージは、クラウド データ センター外部のエンド ユーザーへのアクセスを排除することで、管理者に対する追加の露出リスクを排除します。代わりに、顧客が行う構成は、データ アクセス プレーンに対してのみです。各テナントは独自のボリュームを管理し、どのテナントも他のGoogle Cloud NetApp Volumes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ており、セクションで説明されているプロセスを通じてシステムへのアクセス権が付与される信頼できる管理者のごく少数のリストが存在します。"サービス運営。"

NetApp Volumes-Performance サービス タイプは、リージョン障害が発生した場合に別のリージョンにデータ保護を提供するオプションとして、リージョン間レプリケーションを提供します。このような場合、 Google Cloud NetApp Volumes を影響を受けていないリージョン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

更新は脆弱なシステムを保護するのに役立ちます。各アップデートでは、攻撃対象領域を最小限に抑えるセキュリティ強化とバグ修正が提供されます。ソフトウェア更新は集中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、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悪意のある人物によって侵害されていないことが確認されます。

Google Cloud NetApp Volumesでは、更新はクラウド プロバイダ チームによって処理されます。これにより、構成とアップグレードに精通した専門家がプロセスを自動化し、完全にテストすることで、管理者チームのリスク露出が排除されます。アップグレードは中断なく行われ、 Google Cloud NetApp Volumes は最新のアップデートを維持し、全体的に最良の結果を実現します。

これらのサービスアップグレードを実行する管理チームの詳細については、セクションを参照してください。"サービス運営。"

保存データの保護

ディスクの盗難、返却、転用に際して保存されている機密データを保護するには、保存データ暗号化が重要です。Google Cloud NetApp Volumes内のデータは、ソフトウェアベースの暗号化を使用して保存時に保護されます。

- Google が生成したキーはNetApp Volumes-SW に使用されます。
- NetApp Volumes-Performance の場合、ボリュームごとのキーはGoogle Cloud NetApp Volumesに組み込まれたキー マネージャーに保存され、 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の認定モジュール リストに掲載されています。見る "FIPS 140-2 証明書 #4144"。

2021 年 11 月から、プレビュー版のカスタマー管理暗号化 (CMEK) 機能がNetApp Volumes-Performance で利

用できるようになりました。この機能を使用すると、Google Key Management Service（KMS）でホストされているプロジェクトごと、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。 KMS を使用すると、外部キー マネージャーを接続できます。

NetApp Volumes-PerformanceのKMSの設定方法の詳細については、 "Google Cloud NetApp Volumesのドキュメントをご覧ください"。

アーキテクチャの詳細については、セクションを参照してください。"Google Cloud NetApp Volumes のアーキテクチャ。"

転送中のデータの保護

保存中のデータを保護するだけでなく、 Google Cloud NetApp Volumes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。 Google Cloud NetApp Volumes は、 Kerberos を使用した SMB 暗号化、パケットの署名/シール、NFS Kerberos 5p によるエンドツーエンドのデータ転送暗号化などの暗号化方式を使用して、NAS プロトコル経由で転送中のデータを暗号化します。

Google Cloud NetApp Volumesボリュームのレプリケーションでは、AES-GCM 暗号化方式を利用する TLS 1.2 が使用されます。

Telnet、NDMP などの安全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Google Cloud NetApp Volumesによって暗号化されないため（DNS Sec はサポートされていません）、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。セクションを参照"転送中のデータ暗号化"転送中のデータのセキュリティ保護の詳細については、こちらをご覧ください。

NASプロトコル暗号化の詳細については、セクションを参照してください。"NAS プロトコル。"

NAS権限のユーザーとグループ

クラウド内のデータのセキュリティ保護には、適切なユーザーおよびグループの認証が含まれます。これにより、データにアクセスするユーザーは環境内の実際のユーザーとして検証され、グループには有効なユーザーが含まれます。これらのユーザーとグループは、初期の共有およびエクスポート アクセス、およびストレージ システム内のファイルとフォルダーに対する権限の検証を提供します。

Google Cloud NetApp Volumes は、 SMB 共有と Windows スタイルの権限に標準の Active Directory ベースの Windows ユーザー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 UNIX ユーザーおよびグループ用の LDAP などの UNIX ID プロバイダーも活用できます。

現在、Google Cloud NetApp Volumes の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、ウイルスの検出、防止、軽減

ランサムウェア、マルウェア、ウイルスは管理者にとって継続的な脅威であり、企業組織ではこれらの脅威の検出、防止、軽減が常に最優先事項となっています。重要なデータセットに対する 1 回のランサムウェア攻撃で、数百万ドルの損害が発生する可能性があるため、リスクを最小限に抑えるためにできることを行うことが有益です。

Google Cloud NetApp Volumes には現在、ウイルス対策保護や "自動ランサムウェア検出"などのネイティブな検出または防止策は含まれていませんが、定期的なスナップショットスケジュールを有効にすることで、ランサムウェアイベントから迅速に復旧する方法があります。スナップショットコピーは不変かつ読み取り専用の

ポインタであり、ファイルシステム内の変更されたブロックを参照し、ほぼ瞬時に処理され、パフォーマンスへの影響は最小限であり、データが変更または削除された場合にのみ容量を消費します。スナップショットコピーのスケジュールを設定することで、希望する目標復旧ポイント（RPO）/目標復旧時間（RTO）に合わせることができ、ボリュームごとに最大 1,024 個のスナップショットコピーを保持できます。

Google Cloud NetApp Volumesには、スナップショット サポートが追加料金なしで（スナップショット コピーによって保持される変更されたブロック/データに対するデータ ストレージ料金以外）含まれており、ランサムウェア攻撃が発生した場合は、攻撃が発生する前のスナップショット コピーにロールバックするために使用できます。スナップショットの復元はわずか数秒で完了し、その後は通常どおりデータの提供を再開できます。詳細については、以下を参照してください。 "ランサムウェアに対するNetAppソリューション" 。

ランサムウェアがビジネスに影響を及ぼすのを防ぐには、次の 1 つ以上の要素を含む多層的な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脅威からの保護
- データ異常の検出
- 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復元テスト
- 変更不可能な読み取り専用のNetAppスナップショットコピー
- 重要インフラ向け多要素認証
- システムログインのセキュリティ監査

このリストは網羅的なものではありませんが、ランサムウェア攻撃の可能性に対処する際に従うべき良い青写真となります。 Google Cloud のGoogle Cloud NetApp Volumes は、ランサムウェア イベントから保護し、その影響を軽減するためのさまざまな方法を提供します。

不変のスナップショットコピー

Google Cloud NetApp Volumes は、カスタマイズ可能なスケジュールに基づいて作成される不変の読み取り専用スナップショット コピーをネイティブに提供し、データが削除された場合やボリューム全体がランサムウェア攻撃の被害に遭った場合に、迅速なポイントインタイム リカバリを実現します。以前の正常なスナップショット コピーへのスナップショットの復元は高速で、スナップショット スケジュールと RTO/RPO の保持期間に基づいてデータ損失を最小限に抑えます。スナップショット 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。

Google Cloud NetApp Volumesのスナップショット コピーは読み取り専用であるため、ランサムウェアが気付かれずにデータセットに侵入し、ランサムウェアに感染したデータのスナップショット コピーが取得されない限り、ランサムウェアに感染することはありません。このため、データの異常に基づくランサムウェア検出も検討する必要があります。 Google Cloud NetApp Volumes は現在ネイティブ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できます。

バックアップおよびリストア

Google Cloud NetApp Volumes 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。

- NetApp Volumes-Performanceは、他のNetApp Volumes-Performanceボリュームへのクロスリージョンボリュームレプリケーションを提供します。詳細については、Google Cloud NetApp Volumesドキュメント

の "ボリュームレプリケーション"を参照してください。

- NetApp Volumes-SWは、サービスネイティブなボリュームのバックアップ/リストア機能を提供します。詳細については、Google Cloud NetApp Volumesのドキュメントの "クラウドバックアップ"を参照してください。

ボリューム レプリケーションは、ランサムウェア イベントなどの災害発生時に高速フェイルオーバーを実現するために、ソース ボリュームの正確なコピーを提供します。

クロスリージョンレプリケーション

NetApp Volumes-Performance を使用すると、Google のネットワークで実行されるレプリケーションに使用される特定のインターフェースを使用して、 NetAppが管理するバックエンド サービス ネットワーク上で TLS1.2 AES 256 GCM 暗号化を使用することで、データ保護とアーカイブのユースケースのために 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含まれており、セカンダリ (宛先) ボリュームに複製されてプライマリ データセットの正確なレプリカが提供されます。

初期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送信されます。たとえば、プライマリ ボリュームにある 1 TB のデータベースがセカンダリ ボリュームに複製される場合、最初のレプリケーションで 1 TB の領域が転送されます。そのデータベースに、初期化と次回の更新の間に変更される数百行 (仮に数 MB) がある場合、変更された行を含むブロックのみがセカンダリ (数 MB) に複製されます。これにより、転送時間が短くなり、レプリケーション料金が抑えられます。

ファイルとフォルダーに対するすべてのアクセス許可はセカンダリ ボリュームに複製されますが、共有アクセス アクセス許可 (エクスポート ポリシーとルール、SMB 共有と共有 ACL など) は個別に処理する必要があります。サイトのフェールオーバーの場合、宛先サイトでは同じ名前サービスと Active Directory ドメイン接続を活用して、ユーザーとグループの ID およびアクセス許可を一貫して処理する必要があります。レプリケーション関係を解除してセカンダリ ボリュームを読み取り/書き込み可能に変換することで、災害発生時にセカンダリ ボリュームをフェイルオーバー ターゲットとして使用できます。

ボリューム レプリカは読み取り専用であり、ウイルスがデータに感染した場合やランサムウェアがプライマリ データセットを暗号化した場合に、データを迅速に回復できるように、オフサイトでデータの不変のコピーを提供します。読み取り専用データは暗号化されませんが、プライマリ ボリュームが影響を受けてレプリケーションが発生すると、感染したブロックも複製されます。影響を受けていない古いスナップショット コピーを使用して回復することもできますが、攻撃の検出速度によっては、SLA が約束された RTO/RPO の範囲外になる可能性があります。

さらに、Google Cloudのクロスリージョンレプリケーション（CRR）管理を使用することで、ボリュームの削除、Snapshotの削除、Snapshotスケジュールの変更などの悪意のある管理アクションを防ぐことができます。これは、ソースボリュームを削除できるがミラーを解除できず、したがってデスティネーションボリュームを削除できないボリューム管理者と、ボリューム操作を一切実行できないCRR管理者を分離するカスタムロールを作成することによって実現されます。各管理者グループに許可されている権限については、Google Cloud NetApp Volumesのドキュメントの "セキュリティに関する考慮事項"を参照してください。

Google Cloud NetApp Volumesバックアップ

Google Cloud NetApp Volumes は高いデータ耐久性を提供しますが、外部イベントによってデータが失われる可能性があります。ウイ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、データ アクセスをタイムリーに再開するには、バックアップと復元が重要になります。管理者がGoogle Cloud NetApp Volumesボリュームを誤って削除してしまう可能性があります。あるいは、ユーザーはデータのバックアップ バージョンを数か月間保持したいだけなので、ボリューム内に追加のスナップショット コピー スペースを保持するとコスト上の課題が発生します。スナップショット コピーは、失われたデータを復元するために過去

数週間のバックアップ バージョンを保持するのに適した方法ですが、スナップショット コピーはボリューム内に保存されるため、ボリュームが消失すると失われます。

これらの理由から、Google Cloud NetApp Volumesは "Google Cloud NetApp Volumesバックアップ"を通じてバックアップサービスを提供しています。

Google Cloud NetApp Volumesバックアップでは、Google Cloud Storage (GCS) 上にボリュームのコピーが生成されます。ボリューム内に保存されている実際のデータのみがバックアップされ、空き領域はバックアップされません。これは永久増分として機能します。つまり、ボリュームの内容を一度転送し、それ以降は変更されたデータのみをバックアップし続けます。複数の完全バックアップを伴う従来のバックアップ概念と比較すると、大量のバックアップストレージを節約し、コストを削減します。バックアップ スペースの月額料金はボリュームに比べて低いため、バックアップ バージョンを長期間保存するのに最適な場所です。

ユーザーは、 Google Cloud NetApp Volumes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 バージョンを復元できます。ソースボリュームが削除された場合でも、バックアップデータは保持されるため、個別に管理（削除など）する必要があります。

Google Cloud NetApp Volumes バックアップは、オプションとして Google Cloud NetApp Volumes に組み込まれています。ユーザーは、ボリュームごとに Google Cloud NetApp Volumes バックアップを有効化することで、保護するボリュームを選択できます。バックアップ、 "サポートされる最大バックアップバージョンの数"、スケジュール、および "価格設定"の詳細については、 "Google Cloud NetApp Volumesバックアップのドキュメント"を参照してください。

プロジェクトのすべてのバックアップ データは GCS バケット内に保存されます。このバケットはサービスによって管理され、ユーザーには表示されません。各プロジェクトは異なるバケットを使用します。現在、バケットはGoogle Cloud NetApp Volumesボリュームと同じリージョンにありますが、さらに多くのオプションが検討されています。最新のステータスについてはドキュメントを参照してください。

Google Cloud NetApp Volumesバケットから GCS へのデータ転送には、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 が管理するキーを使用して保存時に暗号化されます。

Google Cloud NetApp Volumesのバックアップ（バックアップの作成、削除、復元）を管理するには、ユーザーに "roles/netapp.admin"ロールが必要です。

概要

クラウド ソリューションを信頼するには、アーキテクチャとそのセキュリティ保護方法を理解することが重要です。このセクションでは、Google のGoogle Cloud NetApp Volumesアーキテクチャのさまざまな側面について説明し、データのセキュリティ保護方法に関する潜在的な懸念を軽減するとともに、最も安全なデプロイメントを実現するために追加の構成手順が必要になる可能性がある領域について説明します。

Google Cloud NetApp Volumes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

Google Cloud NetApp Volumesのコントロール プレーンは、Google Cloud NetApp Volumes管理者とNetAppネイティブ自動化ソフトウェアによって管理されるバックエンド インフラストラクチャです。このプレーンはエンドユーザーに対して完全に透過的であり、ネットワーク、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、 Google Cloud NetApp Volumesなどのクラウド常駐ソリューションに価値

をもたらします。

データプレーン

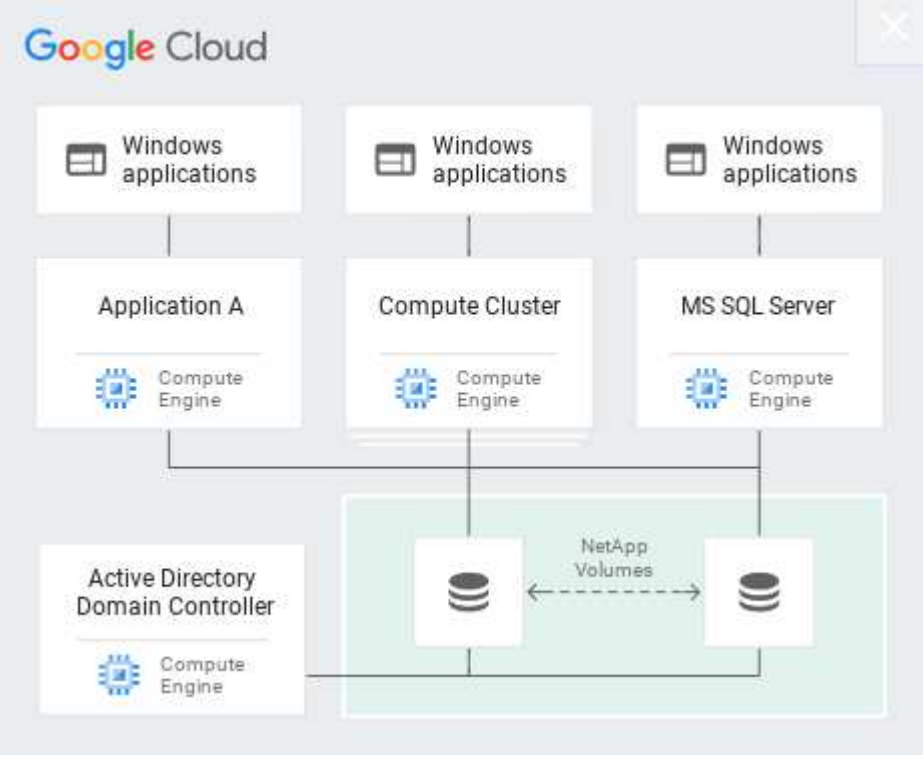
Google Cloud NetApp Volumesのデータプレーンには、実際のデータ ボリュームと、 Google Cloud NetApp Volumes の全体的な構成（アクセス制御、Kerberos 認証など）が含まれます。データ プレーンは、エンド ユーザーとGoogle Cloud NetApp Volumesプラットフォームの消費者によって完全に制御されます。

各飛行機の安全確保と管理の方法には明確な違いがあります。次のセクションでは、 Google Cloud NetApp Volumes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。

Google Cloud NetApp Volumesアーキテクチャ

CloudSQL、Google Cloud VMware Engine（GCVE）、FileStoreなどの他のGoogle Cloudネイティブサービスと同様に、 Google Cloud NetApp Volumesは "GoogleのPSA" サービスを提供するため。 PSAでは、サービスはサービスプロデューサープロジェクト内で構築され、 "VPC ネットワークピアリング"サービス コンシューマーに接続します。サービス プロデューサーはNetAppによって提供および運用され、サービス コンシューマーは顧客プロジェクト内の VPC であり、 Google Cloud NetApp Volumesファイル共有にアクセスするクライアントをホストします。

以下の図は、 "Google Cloud NetApp Volumes のドキュメント"から参照されたもので、概要を示しています。



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。左の青いボックスはユーザー VPC (サービス コンシューマー) を示し、右の青いボックスはNetAppによって提供されるサービス プロデューサーを示します。両方とも VPC ピアリングを介して接続されています。

賃貸モデル

Google Cloud NetApp Volumesでは、個々のプロジェクトは固有のテナントとして扱われます。つまり、ボリューム、スナップショット コピーなどの操作はプロジェクトごとに実行されます。つまり、すべてのボリュームは、それが作成されたプロジェクトによって所有され、デフォルトではそのプロジェクトのみが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 ビューと考えられます。

共有**VPC**

データ プレーン ビューでは、 Google Cloud NetApp Volumes は共有 VPC に接続できます。ホスティング プロジェクト内、または共有 VPC に接続されたいずれかのサービス プロジェクト内にボリュームを作成できます。その共有 VPC に接続されているすべてのプロジェクト (ホストまたはサービス) は、ネットワーク層 (TCP/IP) でボリュームにアクセスできます。共有 VPC 上でネットワーク接続を持つすべてのクライアントは NAS プロトコルを介してデータにアクセスする可能性があるため、個々のボリュームのアクセス制御 (ユーザー/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ーを制御する必要があります。

Google Cloud NetApp Volumes 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、プロジェクトを使用すると、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管理できます。データプレーンでは、VPC は互いに分離されており、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、ネットワーク層では、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 プレーンによって所有者プロジェクトのみがボリュームを表示できます。

VPC サービスコントロール

VPC Service Controls は、インターネットに接続され、世界中からアクセス可能な Google Cloud サービスの周囲にアクセス制御境界を確立します。これらのサービスは、ユーザー ID を通じてアクセス制御を提供しますが、ネットワーク ロケーション要求の発信元を制限することはできません。 VPC Service Controls 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。

Google Cloud NetApp Volumesデータプレーンは、外部インターネットに接続されておらず、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 に接続されています。その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すべて、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を提供しないため、有効な資格情報を持つ誰でもどこからでもアクセスできます（ "JWTトークン" ）。

つまり、 Google Cloud NetApp Volumesデータプレーンは、VPC Service Controls をサポートする必要がなく、VPC Service Controls を明示的に使用せずに、ネットワーク アクセス制御の機能を提供します。

パケットスニッフィング/トレースの考慮事項

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、ネットワーク IP アドレス、MAC アドレス、ユーザー名とグループ名、エンドポイントで使用されているセキュリティ レベルに関する情報を取得するために悪意を持って使用される可能性もあります。 Google Cloudのネットワーク、VPC、ファイアウォールルールの構成により、ユーザーのログイン認証情報や"JWTトークン"クラウド インスタンスに。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、共有 VPC や外部ネットワーク トンネル/IP 転送を使用してエンドポイントへ

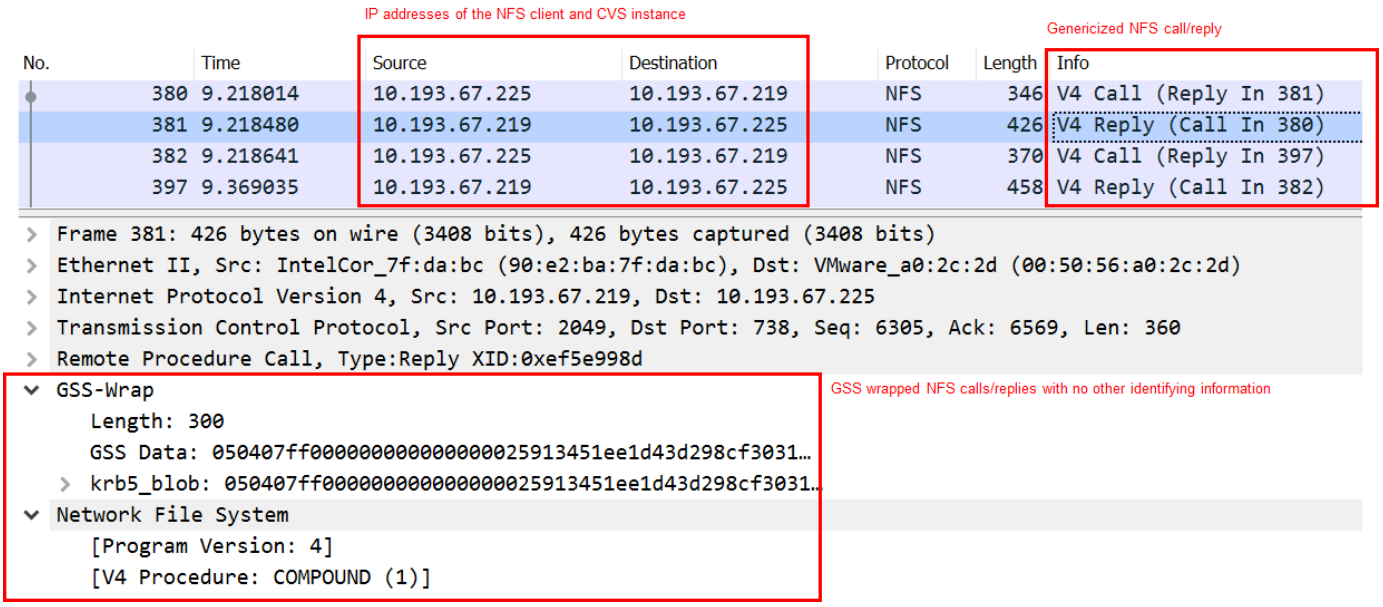
の外部トラフィックを明示的に許可していない限り、VPC の内部エンドポイントでのみ可能です。クライアント外部のトラフィックをスニッフィングする方法はありません。

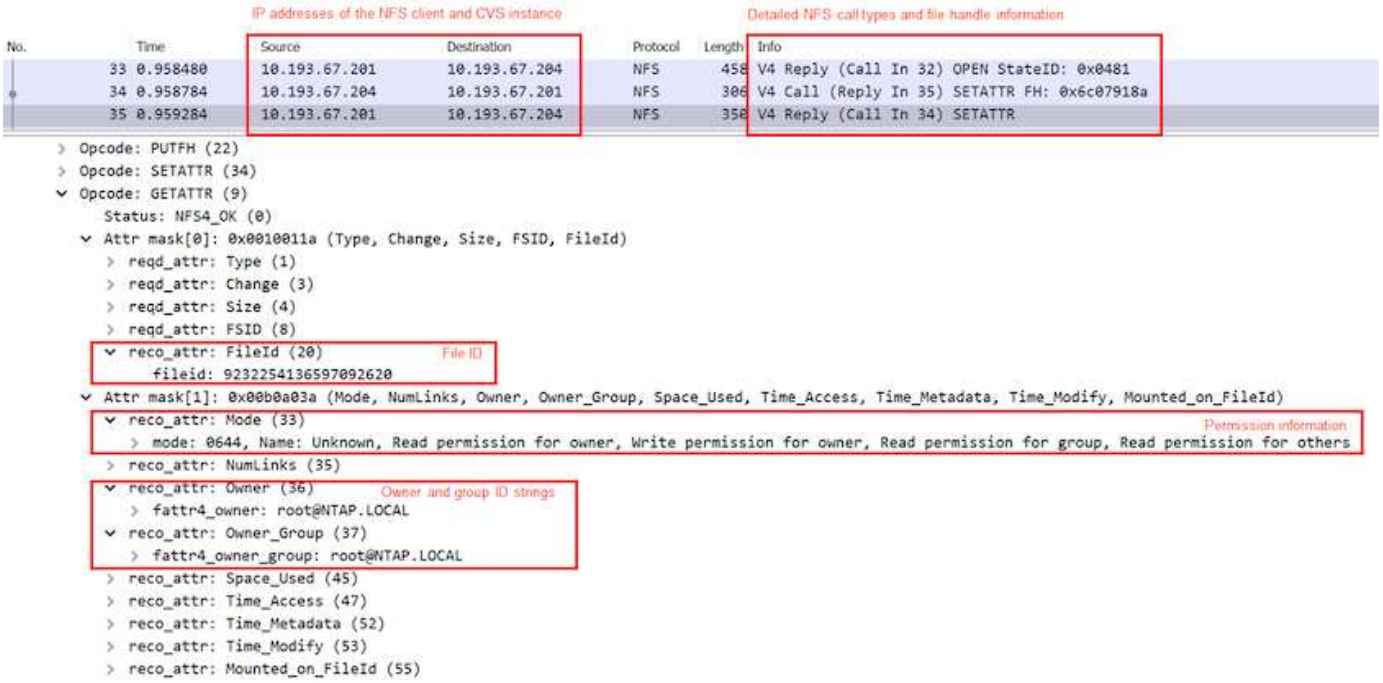
共有VPCを使用する場合、NFS Kerberosおよび/または"SMB暗号化"痕跡から得られる情報の多くを隠すことができます。ただし、一部のトラフィックは依然として平文で送信されます。"DNS"そして"LDAPクエリ"。次の図は、Google Cloud NetApp Volumesから発信されたプレーンテキスト LDAP クエリからのパケット キャプチャと、公開される可能性のある識別情報を示しています。 Google Cloud NetApp Volumesの LDAP クエリは現在、暗号化または SSL 経由の LDAP をサポートしていません。 NetApp Volumes-Performance は、Active Directory から要求された場合に LDAP 署名をサポートします。 NetApp Volumes-SW は LDAP 署名をサポートしていません。



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付きハッシュで送信されます。デフォルトでは、Windows LDAP は unixUserPassword フィールドに値を入力しません。このフィールドは、LDAP を介してクライアントへの対話型ログインに Windows LDAP を利用する必要がある場合にのみ必要です。 Google Cloud NetApp Volumes は、インスタンスへの対話型 LDAP ログインをサポートしていません。

次の図は、AUTH_SYS 経由の NFS のキャプチャの横に、NFS Kerberos 会話からのパケット キャプチャを示しています。トレースで利用できる情報が 2 つ間でどのように異なるか、また、インフライト暗号化を有効にすると NAS トラフィックの全体的なセキュリティがどのように強化されるかに注意してください。





VMネットワークインターフェース

攻撃者が試みる可能性のあるトリックの1つは、VMに新しいネットワークインターフェースカード（NIC）を追加することです。 "乱交モード" (ポートミラーリング) または、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ッフィングします。 Google Cloud では、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、アラートが生成されるため、攻撃者は気付かれずにこれを実行することはできません。

さらに、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 でアラートがトリガーされます。

コントロールプレーンアーキテクチャ

Google Cloud NetApp Volumesに対するすべての管理アクションは API を介して実行さ

れます。 GCP Cloud Console に統合されたGoogle Cloud NetApp Volumes管理でも、Google Cloud NetApp Volumes API が使用されます。

アイデンティティとアクセス管理

アイデンティティとアクセス管理("私は"）は、Google Cloud プロジェクト インスタンスへの認証（ログイン）と承認（権限）を制御できる標準サービスです。 Google IAM は、権限の承認と削除の完全な監査証跡を提供します。現在、 Google Cloud NetApp Volumes 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/許可の概要

IAMは、Google Cloud NetApp Volumesの組み込みのきめ細かな権限を提供します。 "詳細な権限の完全なリストはこちら"を確認できます。

IAMには、 `netappcloudvolumes.admin`そして `netappcloudvolumes.viewer`。これらのロールは、特定のユーザーまたはサービス アカウントに割り当てることができます。

IAM ユーザーがGoogle Cloud NetApp Volumesを管理できるように、適切なロールと権限を割り当てます。

きめ細かな権限の使用例は次のとおりです。

- ユーザーがボリュームを削除できないように、取得/一覧表示/作成/更新権限のみを持つカスタム ロールを構築します。
- カスタムロールを使用する `snapshot.*`アプリケーション整合性のあるスナップショット統合を構築するために使用されるサービス アカウントを作成する権限。
- 委任するカスタムロールを構築する `volumereplication.*`特定のユーザーに。

サービスアカウント

Google Cloud NetApp Volumes API呼び出しをスクリプトまたは "テラフォーム"、サービスアカウントを作成する必要があります。 `roles/netappcloudvolumes.admin`役割。このサービス アカウントを使用すると、Google Cloud NetApp Volumes API リクエストを認証するために必要な JWT トークンを 2 つの方法で生成できます。

- JSON キーを生成し、Google API を使用してそこから JWT トークンを派生します。これは最も単純なアプローチですが、手動での秘密 (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"と `roles/iam.serviceAccountTokenCreator`。コード（スクリプト、Terraformなど）は次のように実行されます。 "アプリケーションのデフォルト資格情報"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。

詳細については、Google Cloudのドキュメントの "サービスアカウントと秘密鍵の作成"を参照してください。

Google Cloud NetApp VolumesAPI

Google Cloud NetApp Volumes APIは、基盤となるネットワークトランスポートとしてHTTPS（TLSv1.2）を使用したRESTベースのAPIを採用しています。最新のAPI定義とAPIの使用方法に関する情報は、 "Google クラウド ドキュメントの Cloud Volumes API"で確認できます。

API エンドポイントは、標準の HTTPS (TLSv1.2) 機能を使用してNetAppによって運用および保護されます。

JWTトークン

APIへの認証はJWTベアラートークンで実行される("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。これは、サービス アカウント JSON キーを指定して IAM からトークンを取得することによって実行する必要があります。

監査ロギング

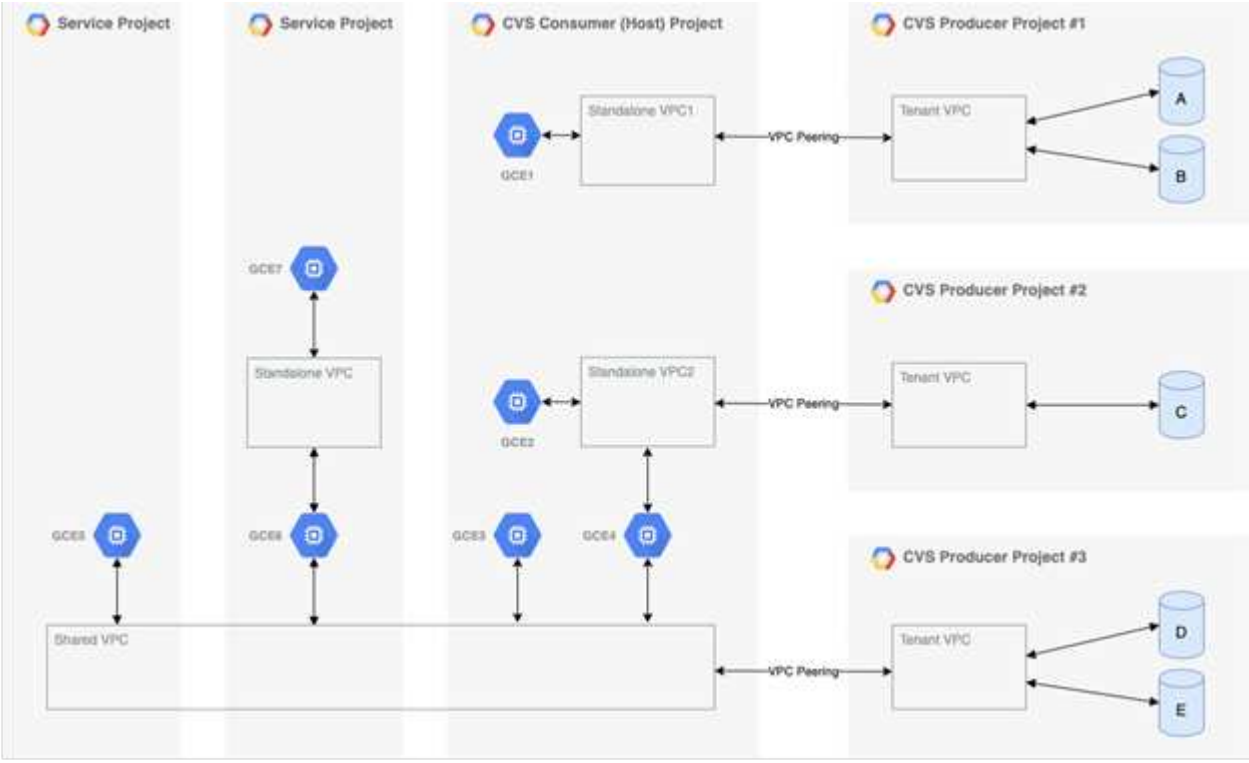
現在、ユーザーがアクセスできるコントロール プレーン監査ログは利用できません。

データプレーンアーキテクチャ

Google Cloud NetApp Volumes for Google CloudはGoogle Cloudを活用しています "プライベートサービスアクセス"フレームワーク。このフレームワークでは、ユーザーはGoogle Cloud NetApp Volumesに接続できます。このフレームワークは、他の Google Cloud サービスと同様にサービス ネットワーキングと VPC ピアリング構造を使用して、テナント間の完全な分離を保証します。

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

ユーザー VPC（スタンドアロンまたは共有）は、ボリュームをホストするGoogle Cloud NetApp Volumes管理対象テナント プロジェクト内の VPC にピアリングされます。



上の図は、Google Cloud NetApp Volumesに接続された 3 つの VPC ネットワークと、ボリュームを共有する複数の Compute Engine VM (GCE1～7) を含むプロジェクト (中央のNetApp Volumes コンシューマー プロジェクト) を示しています。

- VPC1 は GCE1 がボリューム A と B にアクセスできるようにします。

- 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 番目の VPC ネットワークは、2 つのサービス プロジェクトで共有される共有 VPC です。これにより、GCE3、GCE4、GCE5、GCE6 がボリューム D と 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、 NetApp Volumes-Performance 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 または SMB 暗号化を使用）とGoogle Cloud NetApp Volumesでの保存中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、次のセクションで説明するように、Google Cloud ネットワーク自体も暗号化されます。

Google Cloud ネットワーク

Google Cloudは、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 ドキュメントに記載されています。 「Google Cloud NetApp Volumes のアーキテクチャ」セクションで述べたように、Google Cloud NetApp Volumes はNetApp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。

NetApp Volumes-SW 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Google Cloud NetApp Volumes 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。

NetApp Volumes-Performanceのデータパスはネットワーク層で完全に暗号化されていないが、 NetAppとGoogleは "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、 Google Cloud NetApp Volumes NetApp Volumes-Performance サービスタイプと Google Cloud の間で転送中の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、プロトコル層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 データのエンドツーエンドの暗号化を提供し、信頼でき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/サーバー データ接続 (SMB3.x 対応クライアントのみ使用可能) とサーバー/ドメイン コントローラー認証の両方の暗号化を有効にすることができます。

SMB 暗号化を有効にすると、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なくなります。

Google Cloud NetApp Volumes は、 SMB 暗号化に RC4-HMAC、AES-128-CTS-HMAC-SHA1、AES-256-CTS-HMAC-SHA1 のセキュリティ暗号をサポートしています。 SMB は、サーバーでサポートされている最高の暗号化タイプにネゴシエートします。

NFSv4.1 ケルベロス

NFSv4.1では、 NetApp Volumes-PerformanceはKerberos認証を提供します。 "RFC7530"ボリュームごとに Kerberos を有効にすることができます。

Kerberos で現在使用できる最も強力な暗号化タイプは AES-256-CTS-HMAC-SHA1 です。 Google Cloud NetApp Volumes は、 NFS に対して AES-256-CTS-HMAC-SHA1、AES-128-CTS-HMAC-SHA1、DES3 、DES をサポートしています。また、CIFS/SMB トラフィックでは ARCFOUR-HMAC (RC4) をサポートしますが、NFS ではサポートしません。

Kerberos は、NFS マウントに対して 3 つの異なるセキュリティ レベルを提供し、Kerberos セキュリティの強度を選択できます。

RedHatによると "一般的なマウントオプション"ドキュメント:

```
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.
```

一般的な規則として、Kerberos セキュリティ レベルが高くなるほど、クライアントとサーバーが送信されたパケットごとに NFS 操作の暗号化と復号化に時間を費やすため、パフォーマンスは低下します。多くのクライアントと NFS サーバーは、全体的なエクスペリエンスを向上させるために CPU への AES-NI オフロードをサポートしていますが、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 (ユーザー認証) の影響よりも大幅に大きくなります。

次の表は、各レベルでのセキュリティとパフォーマンスの違いを示しています。

セキュリティレベル	セキュリティ	パフォーマンス
NFSv3—システム	• 最も安全性が低い。数値のユーザー ID/グループ ID を含むプレーンテキスト • パケットキャプチャで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、権限を表示可能	• ほとんどの場合に最適
NFSv4.x—システム	• NFSv3（クライアントID、名前文字列/ドメイン文字列のマッチング）よりも安全ですが、プレーンテキストのままです • パケットキャプチャでUID 、GID、クライアントIPアドレス、名前文字列、ドメインID、エクスポートパス、ファイル名、権限を表示できます。	• 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）に適しています • ファイル数が多い/メタデータが多いと悪い（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パケットの認証情報にKerberos暗号化を適用し、RPC呼び出しのユーザー/グループのUID/GIDをGSSラッパーでラップします。 • マウントへのアクセスを要求するユーザーは、有効な Kerberos チケット (ユーザー名/パスワードまたは手動のキータブ交換経由) が必要です。チケットは指定された期間後に期限切れとなり、ユーザーはアクセスするために再認証を行う必要があります。 • NFS 操作やマウント/ポートマッパー/nlm などの補助プロトコルは暗号化されません (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、パケット キャプチャの atime/mtime を確認できます)	• Kerberos の場合、ほとんどの場合に最適。AUTH_SYS より劣る。
NFS—krb5i	• すべてのNFSパケットの認証情報にKerberos暗号化を適用し、RPC呼び出しのユーザー/グループのUID/GIDをGSSラッパーでラップします。 • マウントへのアクセスを要求するユーザーは、有効な Kerberos チケット (ユーザー名/パスワードまたは手動のキータブ交換経由) が必要です。チケットは指定された期間後に期限切れとなり、ユーザーはアクセスするために再認証を行う必要があります。 • NFS 操作やマウント/ポートマッパー/nlm などの補助プロトコルは暗号化されません (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、パケット キャプチャの atime/mtime を確認できます) • パケットが傍受されないよう、すべてのパケットに Kerberos GSS チェックサムが追加されます。チェックサムが一致する場合、会話が許可されます。	• NFS ペイロードが暗号化されないため、krb5p よりも優れています。krb5 と比較して、追加されるオーバーヘッドは整合性チェックサムのみです。krb5i のパフォーマンスは krb5 より大幅に劣ることはありませんが、若干の低下が見られます。

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パケットの認証情報にKerberos暗号化を適用し、RPC呼び出しのユーザー/グループのUID/GIDをGSSラッパーでラップします。 • マウントへのアクセスを要求するユーザーは、有効な Kerberos チケット (ユーザー名/パスワードまたは手動のキータブ交換経由) が必要です。チケットは指定された期間後に期限切れとなり、ユーザーはアクセスするために再認証を行う必要があります。 • 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 キャプチャ内のファイル ハンドル、権限、ファイル名、atime/mtime は表示されません)。 • 整合性チェックが含まれます。 • NFS 操作タイプが表示されます (FSINFO、ACCESS 、GETATTR など)。 • 補助プロトコル（マウント、ポートマップ、nlm など）は暗号化されません（エクスポートパス、IP アドレスは確認できます）	• セキュリティ レベルの中で最もパフォーマンスが悪く、krb5p ではより多くの暗号化/復号化を行う必要があります。 • ファイル数の多いワークロードでは、NFSv4.x を使用した krb5p よりもパフォーマンスが向上します。

Google Cloud NetApp Volumesでは、構成された Active Directory サーバーが Kerberos サーバーおよび LDAP サーバーとして使用されます（RFC2307 互換スキーマからユーザー ID を検索するため）。他の Kerberos または LDAP サーバーはサポートされていません。 NetApp、Google Cloud NetApp Volumesでの ID 管理に LDAP を使用することを強くおすすめします。 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、セクション "Packet sniffing/trace considerations." を参照してください。

保存時のデータ暗号化

Google Cloud NetApp Volumesのすべてのボリュームは、AES-256 暗号化を使用して保存時に暗号化されます。つまり、メディアに書き込まれたすべてのユーザー データは暗号化され、ボリュームごとのキーでのみ復号化できます。

- NetApp Volumes-SW の場合、Google が生成したキーが使用されます。
- NetApp Volumes-Performance の場合、ボリュームごとのキーは、 Google Cloud NetApp Volumesに組み込まれたキー マネージャーに保存されます。

2021 年 11 月から、プレビュー版の顧客管理暗号化キー (CMEK) 機能が利用可能になりました。これにより、ボリュームごとのキーを、プロジェクトごと、リージョンごとにホストされているマスターキーで暗号化

できるようになります。 "Google キー管理サービス (KMS)。" KMS を使用すると、外部キー マネージャーを接続できます。

NetApp Volumes-PerformanceのKMSの設定については、 "顧客管理暗号化キーの設定"を参照してください。

ファイアウォール

Google Cloud NetApp Volumes は、 NFS および SMB 共有を提供するために複数の TCP ポートを公開します。

- "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、SMB、Kerberosを含むLDAPを使用した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です。Active Directory接続は、リージョンごとに "構成された"する必要があります。Active Directoryドメインコントローラ（DC）は、指定されたDNSサーバと "DNSベースのDC検出"を使用して識別されます。返されたDCのいずれかが使用されます。対象となるDCのリストは、Active Directoryサイトを指定することで制限できます。

Google Cloud NetApp Volumes は、 "Google Cloud NetApp Volumesのオンボーディング"中に `gcloud compute address`コマンドで割り当てられた CIDR 範囲の IP アドレスを使用して接続します。この CIDR をソースアドレスとして使用し、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 "ここで述べたように、ポートをGoogle Cloud NetApp Volumes CIDR に公開します。"する必要があります。

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) が含まれます。これらのプロトコルにより、 NetApp Volumes は複数の NAS クライアント間でデータへの共有アクセスを可能にします。さらに、 Google Cloud NetApp Volumes は、NAS 共有内のファイルとフォルダのすべての ID と権限の設定を尊重しながら、NFS クライアントと SMB/CIFS クライアントへの同時アクセス（デュアル プロトコル）を提供できます。可能な限り最高のデータ転送セキュリティを維持するために、 Google Cloud NetApp Volumes 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NetApp Volumes-Performance でのみ使用できます。

NASプロトコルの基礎

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Google Cloud NetApp Volumes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 は定義された NAS プロトコルであり、 Google Cloud NetApp Volumes がサーバーとして機能するクライアント/サーバー ベースで動作します。クライアントはアクセス、読み取り、書き込みの要求をサーバーに送信し、サーバーはファイルのロック メカニズムの調整、アクセス許可の保存、ID および認証要求の処理を担当

します。

たとえば、NAS クライアントがフォルダー内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. クライアントはサーバーに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) を要求します。サーバーは、要求元のクライアントとユーザーが親フォルダーに対する必要な権限を持っている場合に、その情報で応答します。
2. ディレクトリの権限でアクセスが許可されている場合、クライアントは、作成す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ーに問い合わせます。ファイル名がすでに使用されている場合、作成は失敗します。ファイル名が存在しない場合は、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. クライアントは、ディレクトリ ハンドルとファイル名を使用してファイルを作成するためにサーバーに呼び出しを発行し、アクセス時刻と変更時刻を設定します。サーバーはファイルに一意のファイル ID を発行し、同じファイル ID を持つ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、WRITE 操作の前にファイル属性を確認するための呼び出しを送信します。権限が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/アプリケーションによってロックが使用される場合、クライアントは、データの破損を防ぐためにロックされている間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、サーバーにロックを要求します。

NFS

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

Google Cloud NetApp Volumes内のボリュームは、クライアントまたはクライアント セットが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権限は、 Google Cloud NetApp Volumes管理者が構成できるエクスポート ポリシーとルールによって定義されます。

NetApp 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ており、数え切れないほどのエンタープライズ NAS 環境で使用されています。次のセクションでは、Google Cloud NetApp Volumesで利用できる NFS と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**ユーザーとグループ

Google Cloud NetApp Volumes には、さまざまな基本機能のためのデフォルトの UNIX ユーザーとグループがいくつか含まれています。現在、これらのユーザーとグループを変更または削除することはできません。現在、新しいローカル ユーザーとグループをGoogle Cloud NetApp Volumesに追加することはできません。デフォルトのユーザーとグループ以外の UNIX ユーザーとグループは、外部の LDAP ネーム サービスによって提供される必要があります。

次の表は、デフォルトのユーザーとグループ、およびそれらに対応する数値 ID を示しています。 NetApp、これらの数値 ID を再利用する LDAP またはローカル クライアントに新しいユーザーまたはグループを作成しないことを推奨しています。

デフォルトユーザー: 数値ID	デフォルトグループ: 数値ID
• ルート:0 • pcuser:65534 • 誰も:65535	• ルート:0 • デーモン:1 • pcuser:65534 • 誰も:65535

NFSv4.1 を使用する場合、NFS クライアントでディレクトリ一覧コマンドを実行すると、ルート ユーザーが anyone として表示される場合があります。これは、クライアントの ID ドメイン マッピング構成によるものです。セクションを参照してくださいNFSv4.1とnobodyユーザー/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。

ルートユーザー

Linux では、root アカウントは Linux ベースのファイル システム内のすべてのコマンド、ファイル、およびフォルダーにアクセスできます。このアカウントの権限が大きいため、セキュリティのベスト プラクティスでは、多くの場合、ルート ユーザーを無効にするか、何らかの方法で制限する必要があります。 NFS エクスポートでは、 Google Cloud NetApp Volumesで、エクスポート ポリシーとルール、およびルート スカッシュと呼ばれる概念を通じて、ファイルとフォルダに対するルートユーザーの権限を制御できます。

ルートスカッシングは、NFSマウントにアクセスするルートユーザーが匿名の数値ユーザー65534にスカッシュされることを保証します（「[匿名ユーザー] ）であり、現在はエクスポート ポリシー ルールの作成時にルート アクセスに対してオフを選択して、 NetApp Volumes-Performance を使用する場合にのみ使用できます。ルートユーザーが匿名ユーザーに変更された場合、chown を実行する権限がなくなり、 "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ー、およびルート ユーザーによって作成されたファイルまたはフォルダーには、所有者/グループとして anon UID が表示されます。さらに、NFSv4 ACL は root ユーザーによって変更できません。ただし、ルート ユーザーは、明示的な権限がない chmod および削除されたファイルには引き続きアクセスできます。ルートユーザーのファイルとフォルダの権限へのアクセスを制限したい場合は、NTFS ACLを持つボリュームの使用を検討し、次の名前のWindowsユーザーを作成します。 `root`ファイルまたはフォルダーに必要な権限を適用します。

匿名ユーザー

匿名 (anon) ユーザー ID は、有効な NFS 資格情報なしで到着するクライアント要求にマップされる UNIX ユーザー ID またはユーザー名を指定します。ルート スカッシングが使用される場合、これにはルート ユーザーが含まれる場合があります。 Google Cloud NetApp Volumesの匿名ユーザーは 65534 です。

このUIDは通常ユーザー名に関連付けられています `nobody`または `nfsnobody`Linux 環境では。 Google Cloud NetApp Volumesは、ローカルUNIXユーザー`pcuser`として65534も使用します（「デフォルトのローカルUNIXユーザーとグループ （）は、LDAP 内に有効な一致する UNIX ユーザーが見つからない場合に、Windows から UNIX への名前マッピングのデフォルトのフォールバック ユーザーでもあります。

Linux とGoogle Cloud NetApp Volumesの UID 65534 のユーザー名が異なるため、NFSv4.1 を使用する場合、65534 にマッピングされたユーザーの名前文字列が一致しない可能性があります。その結果、次のようなことが起こります `nobody`一部のファイルおよびフォルダーのユーザーとして。 「NFSv4.1とnobodyユーザー/グループこの問題とその解決方法については、「」を参照してください。

アクセス制御/エクスポート

NFS マウントの初期エクスポート/共有アクセスは、エクスポート ポリシー内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。 NFS 共有をマウントするためのアクセスと、ホストに許

可されるアクセス レベルを許可するために、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ます。エクスポート ポリシー ルールの構成オプションは、Google Cloud NetApp Volumes のレベルによって異なります。

NetApp Volumes-SW の場合、エクスポート ポリシー構成には次のオプションを使用できます。

- クライアントの一致。 IP アドレスのコンマ区切りリスト、ホスト名、サブネット、ネットグループ、ドメイン名のコンマ区切りリスト。
- *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。NetApp Volumes-Performance では、以下のオプションが提供されます。
- クライアントの一致。 IP アドレスのコンマ区切りリスト、ホスト名、サブネット、ネットグループ、ドメイン名のコンマ区切りリスト。
- *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（「[ルートユーザー]詳細は「」をご覧ください。
- *プロトコルタイプ*これにより、NFS マウントへのアクセスが特定のプロトコル バージョンに制限されます。ボリュームに NFSv3 と NFSv4.1 の両方を指定する場合は、両方を空白のままにするか、両方の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)。*読み取り専用または読み取り/書き込みアクセス用の krb5、krb5i、および/または 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**）

Google Cloud NetApp Volumes上の NFS では、ファイルとフォルダに対して chown/chgrp を実行できるのは root ユーザーのみです。他のユーザーは `Operation not permitted`所有するファイルであってもエラーが発生します。根カボチャを使用する場合（「[ルートユーザー] （）の場合、ルートは非ルートユーザーに変更され、chown および chgrp へのアクセスは許可されません。現在、 Google Cloud NetApp Volumesには、非 root ユーザーに chown と chgrp を許可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 ボリュームの使用を検討し、セキュリティ スタイルを NTFS に設定して、Windows 側からアクセス許可を制御します。

権限管理

Google Cloud NetApp Volumes は、 UNIX セキュリティ スタイルを使用するボリュームの NFS クライアントの権限を制御するために、モード ビット（rwx の場合は 644、777 など）と NFSv4.1 ACL の両方をサポートしています。これらには標準の権限管理 (chmod、chown、nfs4_setfacl など) が使用され、それらをサポートする任意の Linux クライアントで動作します。

さらに、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 ユーザーへのGoogle Cloud NetApp Volumes の名前マッピングを活用でき、これを使用して NTFS 権限を解決できます。 Google Cloud NetApp Volumes有効な UNIX ユーザー名を Windows ユーザー名に適切にマッピングする必要があるため、数値 ID からユーザー名への変換を行うにはGoogle Cloud NetApp VolumesへのLDAP 接続が必要です。

NFSv3にきめ細かな**ACL**を提供する

モード ビットの権限は、セマンティクスにおいて所有者、グループ、およびその他すべてのユーザーのみを対象とします。つまり、基本的な NFSv3 にはきめ細かなユーザー アクセス制御は用意されていません。Google Cloud NetApp Volumes はPOSIX ACL も拡張属性（chattr など）もサポートしていないため、きめ細

かな ACL は NFSv3 を使用した次のシナリオでのみ可能です。

- 有効な UNIX から Windows へのユーザー マッピングを備えた NTFS セキュリティ スタイルのボリューム (CIFS サーバーが必要)。
- ACL を適用するために NFSv4.1 をマウントする管理クライアントを使用して適用された NFSv4.1 ACL。

どちらの方法でも、UNIX ID管理用のLDAP接続と、有効なUNIXユーザーおよびグループ情報の入力が必要です（セクションを参照）。"LDAP") であり、 NetApp Volumes-Performance インスタンスでのみ使用できます。 NFS で NTFS セキュリティ スタイルのボリュームを使用するには、SMB 接続が確立されていない場合でも、デュアル プロトコル (SMB と NFSv3) またはデュアル プロトコル (SMB と 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、以下を選択する必要があります。 `Both (NFSv3/NFSv4.1)`プロトコルタイプとして。

通常の UNIX モード ビットでは、NTFS または NFSv4.x ACL が提供するのと同じレベルの細分化されたアクセス許可は提供されません。次の表は、NFSv3 モード ビットと NFSv4.1 ACL 間の権限の粒度を比較したものです。 NFSv4.1 ACLの詳細については、以下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を設定する • 実行時にグループIDを設定する • 交換され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権限の検索 • グループの読み取り権限 • グループの書き込み権限 • ファイルに対する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権限を検索します。 • 他の人の読み取り権限 • 他の人の書き込み権限 • ファイルに対する他のユーザーの実行権限、またはディレクトリ内の他のユーザーの権限を参照（検索）する	アクセス制御エントリ（ACE）の種類（許可/拒否/監査） * 継承フラグ * ディレクトリ継承 * ファイル継承 * 非伝播継承 * 継承のみ 権限 * データの読み取り (ファイル) / ディレクトリの一覧表示 (ディレクトリ) * データの書き込み (ファイル) / ファイルの作成 (ディレクトリ) * データの追加 (ファイル) / サブディレクトリの作成 (ディレクトリ) * 実行 (ファイル) / ディレクトリの変更 (ディレクトリ) * 削除 * 子の削除 * 属性の読み取り * 属性の書き込み * 名前付き属性の読み取り * 名前付き属性の書き込み * ACL の読み取り * ACL の書き込み * 所有者の書き込み * 同期

最後に、NFS グループ メンバーシップ (NFSv3 と NFSV4.x の両方) は、RPC パケット制限に従って、AUTH_SYS のデフォルトの最大値 16 に制限されます。 NFS Kerberos は最大 32 個のグループを提供し、NFSv4 ACL はきめ細かなユーザーおよびグループ ACL (ACE あたり最大 1024 エントリ) によって制限を解除します。

さらに、Google Cloud NetApp Volumesは拡張グループサポートを提供し、サポートされるグループの最大数を32まで拡張します。これには、有効なUNIXユーザおよびグループ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、Googleドキュメントの "NFSボリュームの作成と管理"を参照してください。

NFSv3 ユーザーおよびグループ ID

NFSv3 のユーザー ID とグループ ID は、名前ではなく数値 ID として送信されます。 Google Cloud NetApp Volumes は、 NFSv3 ではこれらの数値 ID のユーザー名解決を行わず、UNIX セキュリティ スタイルのボリュームではモード ビットのみを使用します。 NFSv4.1 ACL が存在する場合、NFSv3 を使用している場合でも、ACL を適切に解決するには数値 ID の検索や名前文字列の検索が必要です。 NTFS セキュリティ スタイルのボリュームでは、 Google Cloud NetApp Volumes は数値 ID を有効な UNIX ユーザーに解決し、有効な Windows ユーザー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 ユーザーおよびグループ ID のセキュリティ制限

NFSv3 では、クライアントとサーバーは、数値 ID を使用して読み取りまたは書き込みを試行するユーザーが有効なユーザーであることを確認する必要はなく、暗黙的に信頼されるだけです。これにより、数値 ID を偽装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 ホールを防ぐために、 Google Cloud NetApp Volumesにはいくつかのオプションが用意されています。

- NFS に Kerberos を実装すると、マウントへのアクセスを許可する Kerberos チケットを取得するために、ユーザーはユーザー名とパスワードまたはキータブ ファイルを使用して認証を行う必要があります。 Kerberos は、 NetApp Volumes-Performance インスタンスでのみ NFSv4.1 で使用できます。
- 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と、 Google Cloud NetApp Volumesボリュームにアクセスできる NFSv3 クライアントが制限されます。
- デュアルプロトコル ボリュームを使用し、ボリュームに NTFS ACL を適用すると、NFSv3 クライアントは数値 ID を有効な UNIX ユーザー名に解決して、マウントへのアクセスを適切に認証するようになります。これには、LDAP を有効にし、UNIX ユーザーおよびグループ ID を構成する必要があります。
- ルート ユーザーを潰すと、ルート ユーザーが NFS マウントに与える損害は制限されますが、リスクが完全になくなるわけではありません。詳細については、「[ルートユーザー] 。"

結局のところ、NFS セキュリティは、使用しているプロトコル バージョンが提供するものに制限されます。 NFSv3 は、一般的に NFSv4.1 よりもパフォーマンスが優れていますが、同じレベルのセキュリティは提供しません。

NFSv4.1

NFSv4.1 は、次の理由により、NFSv3 と比較してセキュリティと信頼性が向上しています。

- 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
- すべての NFS 機能を単一ポート (2049) で実行
- TCPのみ
- IDドメインマッピング
- Kerberos 統合 (NFSv3 は Kerberos を使用できますが、NFS のみで使用でき、NLM などの補助プロトコルでは使用できません)

NFSv4.1 の依存関係

NFSv4.1 の追加のセキュリティ機能により、NFSv3 を使用するには必要のなかったいくつかの外部依存関係が関係しています (SMB が Active Directory などの依存関係を必要とするのと同様)。

NFSv4.1 ACL

Google Cloud NetApp Volumes はNFSv4.x ACL をサポートしており、次のような通常の POSIX スタイルの権限に比べて明確な利点があります。

- 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セキュリティの向上
- CIFS/SMBとの相互運用性の向上
- AUTH_SYSセキュリティでのユーザあたりの最大NFSグループ数（16）の解除
- ACL はグループ ID（GID）解決の必要性を回避し、GID 制限を事実上排除します。NFSv4.1 ACL は、Google Cloud NetApp Volumesからではなく、NFS クライアントから制御されます。 NFSv4.1 ACL を使用するには、クライアントのソフトウェア バージョンがそれをサポートしており、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クライアント間の互換性

NFSv4 ACL は Windows ファイル レベル 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 環境では、NFSv4.1 ACL が存在し、デュアルプロトコル アクセス (同じデータセット上の NFS と 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 セキュリティ タブから ACL を表示または管理できません。

NFSv4.1 ACLの仕組み

参考までに、次の用語が定義されています。

- *アクセス制御リスト (ACL)*権限エントリのリスト。
- *アクセス制御エントリ (ACE)。*リスト内の権限エントリ。

クライアントが SETATTR 操作中にファイルに NFSv4.1 ACL を設定すると、 Google Cloud NetApp Volumes はオブジェクトにその ACL を設定し、既存の ACL を置き換えます。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 操作中にファイルの NFSv4.1 ACL を取得すると、 Google Cloud NetApp Volumes 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、そのリストを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が作成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) と任意 ACL (DACL) で構成されます。 NFSv4.1 が CIFS/SMB と相互運用する場合、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。

基本的な `chmod`NFSv4.1 ACL が設定されたファイルまたはフォルダーで実行すると、既存のユーザーおよびグループ ACL は保持されますが、デフォルトの OWNER@、GROUP@、EVERYONE@ ACL は変更されます。

NFSv4.1 ACLを使用しているクライアントは、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を持つディレクトリに新しいファイルまたはサブディレクトリが作成

されると、そのオブジェクトは適切なタグが付けられたACL内のすべてのACEを継承します。 "継承フラグ" 。

ファイルまたはディレクトリに NFSv4.1 ACL がある場合、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、その ACL を使用して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、親ディレクトリに継承不可能な ACL がある場合、要求に渡されたモード ビットに基づくデフォルトの ACL が新しいオブジェクトに設定されます。
- 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がある場合、親ディレクトリのACLのACEに該当する継承フラグが設定されていれば、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の権限は、大文字と小文字の一連の値（例： `rxtncy`) を使用してアクセスを制御します。これらの文字値の詳細については、 "NFSv4 ACLを使用する方法" 。

NFSv4.1 ACL の動作（umask と ACL 継承）

"NFSv4 ACLはACL継承を提供する機能を提供する" 。ACL継承とは、NFSv4.1 ACLが設定されたオブジェクトの下に作成されたファイルやフォルダが、 "ACL継承フラグ" 。

"umask"管理者の介入なしにディレクトリ内にファイルとフォルダが作成される際の権限レベルを制御するために使用されます。デフォルトでは、 Google Cloud NetApp VolumesはumaskがACLを上書きすることを許可しており、これは期待される動作です。 "RFC 5661" 。

ACLの形式

NFSv4.1のACLには独自の形式があります。次の例は、ファイルに設定された ACE です。

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

上記の例は、次の ACL 形式のガイドラインに従っています。

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

一種の `A`「許可する」という意味です。この場合、プリンシパルはグループではなく、継承が含まれていないため、継承フラグは設定されません。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、以下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 (または名前文字列がクライアントとサーバーによって解決できない場合)、ACL が期待どおりに動作しないか、ACL の変更が適用されずエラーが発生する可能性があります。

サンプルエラーには次のようなものがあります:

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

明示的な**DENY**

NFSv4.1 権限には、OWNER、GROUP、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 がデフォルトで拒否されているためです。つまり、ACL が ACE によって明示的に許可されていない場合は拒否されます。明示的な DENY 属性は、明示的かどうかに関係なく、すべての ACCESS ACE をオーバーライドします。

DENY ACEは属性タグで設定されます `D`。

以下の例では、GROUP@ にはすべての読み取りおよび実行権限が許可されていますが、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 は混乱を招き、複雑になる可能性があるため、可能な限り使用を避ける必要があります。明示的に定義されていない ALLOW 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 ACE セットはモード ビット 755 に相当し、次のことを意味します。

- 所有者にはフル アクセス権がある。
- グループには読み取り専用アクセス権がある。
- それ以外には読み取り専用アクセス権がある。

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ドメインマッピングの依存関係

NFSv4.1 は、ID ドメイン マッピング ロジックをセキュリティ レイヤーとして活用し、NFSv4.1 マウントにアクセスしようとしているユーザーが本当に本人であるかどうかを確認します。このような場合、NFSv4.1 クライアントから取得されたユーザー名とグループ名に名前文字列が追加され、 Google Cloud NetApp Volumesインスタンスに送信されます。ユーザー名/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、ユーザーまたはグループは、 `/etc/idmapd.conf`クライアント上のファイル。

この ID 文字列は、特に NFSv4.1 ACL や Kerberos が使用されている場合に、適切な権限を遵守するための要件です。その結果、適切なユーザー名とグループ名 ID 解決のために、クライアントとGoogle Cloud NetApp Volumes間の一貫性を確保するには、LDAP サーバーなどの名前サービス サーバーの依存関係が必要になります。

Google Cloud NetApp Volumesは、静的なデフォルトIDドメイン名値を使用します。 `defaultv4iddomain.com` 。 NFSクライアントはIDドメイン名設定にDNSドメイン名をデフォルトとして設定しますが、IDドメイン名を手動で調整することができます。 `/etc/idmapd.conf` 。

Google Cloud NetApp Volumesで LDAP が有効になっている場合、 Google Cloud NetApp Volumes はNFS ID ドメインを DNS の検索ドメインに設定されているものに自動的に変更するため、クライアントは異なる 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。

Google Cloud NetApp Volumes がローカル ファイルまたは LDAP 内のユーザー名またはグループ名を解決できる場合、ドメイン文字列が使用され、一致しないドメイン ID は anyone に押し下げられます。 Google Cloud NetApp Volumes がローカル ファイルまたは LDAP でユーザー名またはグループ名を見つけられない場合は、数値 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 (これは NFSv3 の動作に似ています)。

Google Cloud NetApp Volumesボリュームが使用しているものと一致するようにクライアントの NFSv4.1 ID ドメインを変更しないと、次の動作が見られます。

- Google Cloud NetApp Volumesにローカル エントリを持つ UNIX ユーザーとグループ（ローカル UNIX ユーザーとグループで定義されている root など）は、nobody 値に圧縮されます。
- NFS クライアントと Google Google Cloud NetApp Volumes Google Cloud NetApp Volumes Volumes が LDAP を使用するように設定されている場合）は、nobody に押しつぶされます。
- ローカル エントリまたは LDAP エントリを持たない UNIX ユーザーとグループは、数値 ID 値を使用し、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。

次は、前述のシナリオの結果を示しています。

```
# 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ーの ID ドメインが一致する場合、同じファイル リストは次のようになります。

```
# 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、「NFSv4.1とnobodyユーザー/グループ 。"

Kerberosの依存関係

NFS で Kerberos を使用する予定の場合は、 Google Cloud NetApp Volumesで次のものが必要です。

- Kerberos 配布センター サービス (KDC) 用の Active Directory ドメイン
- LDAP 機能のために UNIX 情報が設定されたユーザー属性とグループ属性を持つ Active Directory ドメイン（ Google Cloud NetApp Volumesの NFS Kerberos では、適切に機能するためにユーザー SPN と UNIX ユーザーのマッピングが必要です）。
- Google Cloud NetApp Volumesインスタンスで LDAP が有効になっています
- DNS サービス用の Active Directory ドメイン

NFSv4.1と**nobody**ユーザー/グループ

NFSv4.1構成でよく見られる問題の一つは、ファイルまたはフォルダが以下のコマンドでリストに表示される場合です。 `ls`所有されているものとして `user:group`の組み合わせ `nobody:nobody。

例えば：

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

そして数値IDは 99。

```
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がありますが、 `nobody`グループとして。

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

誰でもない人は誰ですか?

その `nobody`NFSv4.1のユーザーは、 `nfsnobody`ユーザー。 NFSクライアントが各ユーザーをどのように認識しているかを確認するには、 `id`指示：

```
# 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、 `nobody`ユーザーは、 `idmapd.conf`ファイルであり、使用したい任意のユーザーとして定義できます。

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

なぜこのようなことが起こるのでしょうか?

名前文字列のマッピングによるセキュリティは NFSv4.1 操作の重要な原則であるため、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では、そのユーザーは、通常、ユーザーとグループが所有するファイルとフォルダーにアクセスできない状態に押し込められます。

見ると `nobody`ファイル リスト内のユーザーおよび/またはグループの場合、これは通常、NFSv4.1 で何かが誤って構成されていることを意味します。ここでは大文字と小文字の区別が重要になります。

たとえば、user1@CVSDEMO.LOCAL (uid 1234、gid 1234) がエクスポートにアクセスしている場合、Google Cloud NetApp Volumes はuser1@CVSDEMO.LOCAL (uid 1234、gid 1234) を見つけることができる必要があります。 Google Cloud NetApp Volumesのユーザーが USER1@CVSDEMO.LOCAL の場合、一致しません (大文字の USER1 と小文字の user1)。多くの場合、クライアントのメッセージ ファイルには次の内容が表示されます。

```
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の両方が、ユーザーが実際にその本人であることに同意する必要があるため、クライアントが認識するユーザーの情報がGoogle Cloud NetApp Volumes が認識するユーザーの情報と同じであることを確認するために、次の点を確認する必要があります。

- *NFSv4.x ID ドメイン。*クライアント： `idmapd.conf`ファイル; Google Cloud NetApp Volumesは `defaultv4iddomain.com`手動で変更することはできません。 NFSv4.1 で LDAP を使用する場合、 Google Cloud NetApp Volumes はID ドメインを DNS 検索ドメインが使用しているもの（AD ドメインと同じ）に変更します。
- *ユーザー名と数値 ID。*これにより、クライアントがユーザー名を検索する場所が決定され、ネーム サービス スイッチ構成 (クライアント: `nsswitch.conf`および/またはローカルの passwd ファイルと group ファイル。Google Google Cloud NetApp Volumesこれに対する変更は許可されませんが、LDAP が有効にな

っている場合は自動的に構成に追加されます。

- *グループ名と数値 ID。*これにより、クライアントがグループ名を検索する場所が決定され、ネーム サービス スイッチ構成 (クライアント: `nsswitch.conf`および/またはローカルの passwd ファイルと group ファイル。Google Google Cloud NetApp Volumesこれに対する変更は許可されませんが、LDAP が有効になっている場合は自動的に構成に追加されます。

ほとんどの場合、 `nobody`クライアントからのユーザーとグループのリストでは、 Google Cloud NetApp Volumesと NFS クライアント間のユーザー名またはグループ名ドメイン ID の変換に問題があります。このシナリオを回避するには、LDAP を使用して、クライアントとGoogle Cloud NetApp Volumes間のユーザーとグループの情報を解決します。

クライアント上の **NFSv4.1** の名前 **ID** 文字列の表示

NFSv4.1 を使用している場合は、前述のように、NFS 操作中に名前と文字列のマッピングが行われます。

使用に加えて `/var/log/messages`NFSv4 IDの問題を見つけるには、 "nfsidmap -l" NFS クライアントでコマンドを実行して、どのユーザー名が NFSv4 ドメインに適切にマッピングされているかを確認します。

たとえば、クライアントで検出できるユーザーとGoogle Cloud NetApp Volumes がNFSv4.x マウントにアクセスした後のコマンドの出力は次のとおりです。

```
# 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ドメインに正しくマッピングされていないユーザー（この場合は `netapp-user`）が同じマウントにアクセスしてファイルに触れると、割り当てられる `nobody:nobody`予想通りです。

```
# 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
```

その `nfsidmap -l`出力はユーザーに表示されます `pcuser`ディスプレイには表示されるが `netapp-

user; これはエクスポートポリシールールの匿名ユーザーです(65534）。

```
# 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あり、イーサネットネットワークを介して複数のSMBクライアントに対し、一元的なユーザ/グループ認証、権限、ロック、およびファイル共有を提供します。ファイルやフォルダは共有を介してクライアントに提供され、共有にはさまざまな共有プロパティを設定でき、共有レベルの権限によるアクセス制御が可能です。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あらゆるクライアントに提供できます。

Google Cloud NetApp Volumes は、 SMB 2.1 および 3.x バージョンのプロトコルをサポートしています。

アクセス制御/SMB共有

- Windows ユーザー名がGoogle Cloud NetApp Volumesボリュームへのアクセスを要求すると、 Google Cloud NetApp Volumes はGoogle Cloud NetApp Volumes管理者が設定した方法を使用して UNIX ユーザー名を検索します。
- 外部 UNIX ID プロバイダー (LDAP) が設定されていて、Windows/UNIX ユーザー名が同一の場合、追加の設定を必要とせずに、Windows ユーザー名が UNIX ユーザー名に 1:1 でマップされます。 LDAP が有効になっている場合、ユーザーおよびグループ オブジェクトの UNIX 属性をホストするために Active Directory が使用されます。
- Windows名とUNIX名が一致しない場合は、 Google Cloud NetApp VolumesがLDAP名マッピング設定を使用できるようにLDAPを設定する必要があります（セクションを参照）。"非対称名マッピングにLDAPを使用する" ）。
- LDAPが使用されていない場合、Windows SMBユーザーはデフォルトのローカルUNIXユーザーにマップされます。 `pcuser` Google Cloud NetApp Volumesで。これは、Windowsでユーザーが書き込んだファイルで、 `pcuser` UNIXの所有権を次のように表示する `pcuser`マルチプロトコル `NAS` 環境で。 `pcuser`ここでは、 `nobody` Linux 環境のユーザー (UID 65534)。

SMBのみの展開では、 `pcuser`マッピングは依然として発生しますが、Windows ユーザーとグループの所有権が正しく表示され、SMB 専用ボリュームへの NFS アクセスは許可されないため、問題にはなりません。さらに、SMB 専用ボリュームは、作成後に NFS またはデュアルプロトコル ボリュームへの変換をサポートしません。

Windows は、Active Directory ドメイン コントローラでのユーザー名認証に Kerberos を活用します。そのためには、 Google Cloud NetApp Volumesインスタンスの外部にある AD DC とのユーザー名とパスワードの交換が必要です。 Kerberos認証は、 `\\SERVERNAME` UNC パスは SMB クライアントによって使用され、次の

ようになります。

- SERVERNAME に DNS A/AAAA エントリが存在します
- SERVERNAME には SMB/CIFS アクセス用の有効な SPN が存在します

Google Cloud NetApp Volumes SMBボリュームが作成されると、セクションで定義されたとおりにマシンアカウント名が作成されます。"Google Cloud NetApp Volumes がActive Directory にどのように表示されるか。" Google Cloud NetApp Volumes はダイナミック DNS（DDNS）を活用して DNS に必要な A/AAAA および PTR エントリを作成し、マシン アカウント プリンシパルに必要な SPN エントリを作成するため、そのマシン アカウント名は SMB 共有アクセス パスにもなります。

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

たとえば、このGoogle Cloud NetApp Volumesボリュームは次の UNC 共有パスを使用します。 `\\cvs-east- 433d.cvsdemo.local` 。

Active Directory では、 Google Cloud NetApp Volumesによって生成された SPN エントリは次のとおりです。

```
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
```

これは DNS の順方向/逆方向検索の結果です。

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

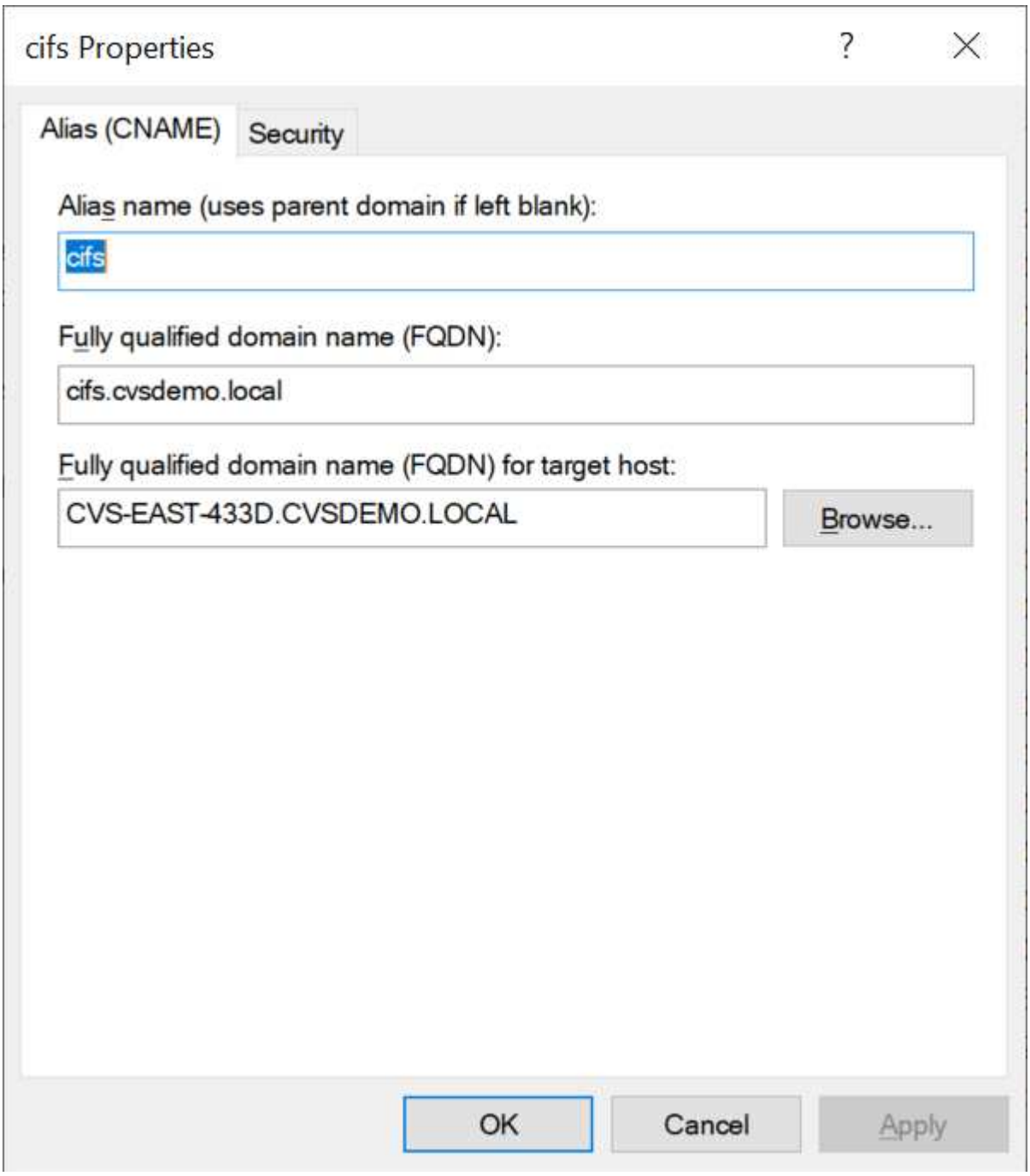
オプションで、 Google Cloud NetApp Volumesの SMB 共有に対して SMB 暗号化を有効化/必須化することで、より多くのアクセス制御を適用できます。いずれかのエンドポイントで SMB 暗号化がサポートされていない場合、アクセスは許可されません。

SMB名エイリアスの使用

場合によっては、エンドユーザーがGoogle Cloud NetApp Volumesに使用されているマシン アカウント名を知ることがセキュリティ上の懸念となることがあります。場合によっては、エンド ユーザーに単純なアクセス パスを提供したいだけの場合もあります。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 の CNAME レコードと呼ばれるものを活用できます。例えば、 `\\CIFS`代わりに共有にアクセスする `\\cvs-east- 433d.cvsdemo.local`ただし、Kerberos 認証を引き続き使用したい場合は、既存の 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

された追加の SPN によって Kerberos アクセスが提供されます。



これは、CNAME を追加した後の DNS 前方参照の結果です。

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

これは、新しい SPN を追加した後の SPN クエリの結果です。

```
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 セットアップ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認証方言

Google Cloud NetApp Volumesは次のものをサポートしています "方言"SMB認証の場合:

- LM
- NTLM
- NTLMv2
- Kerberos

SMB 共有アクセス用の Kerberos 認証は、使用できる認証の中で最も安全なレベルです。 AES および SMB 暗号化を有効にすると、セキュリティ レベルがさらに向上します。

Google Cloud NetApp Volumes は、 LM 認証と NTLM 認証の下位互換性もサポートしています。 Kerberos が誤って構成されている場合 (SMB エイリアスを作成する場合など)、共有アクセスはより弱い認証方法 (NTLMv2 など) にフォールバックします。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。弱い認証方法が無効になっており、Kerberos が適切に構成されていない場合、フォールバックでき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を構成/表示する方法の詳細については、以下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" 。

権限モデル

NTFS/ファイル権限

NTFS アクセス許可は、NTFS ロジックに準拠したファイル システム内のファイルとフォルダーに適用される

アクセス許可です。 NTFS権限を適用できるのは `Basic`または `Advanced`設定できる `Allow`または `Deny`アクセス制御用。

基本的な権限には次のものが含まれます。

- 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

ユーザーまたはグループに権限（ACE と呼ばれる）を設定すると、それは ACL に存在します。 NTFS アクセス許可は、UNIX モード ビットと同じ読み取り/書き込み/実行の基本を使用しますが、所有権の取得、フォルダーの作成/データの追加、属性の書き込みなど、よりきめ細かな拡張アクセス制御 (特殊なアクセス許可とも呼ばれます) に拡張することもできます。

標準の UNIX モード ビットでは、NTFS アクセス許可と同じレベルの細分性 (ACL 内の個々のユーザーおよびグループ オブジェクトに対するアクセス許可の設定や拡張属性の設定など) は提供されません。ただし、NFSv4.1 ACL は NTFS ACL と同じ機能を提供します。

NTFS アクセス許可は共有アクセス許可よりも具体的であり、共有アクセス許可と組み合わせて使用できます。 NTFS アクセス許可構造では、最も制限の厳しいものが適用されます。そのため、アクセス権を定義するときに、ユーザーまたはグループに対する明示的な拒否はフル コントロールよりも優先されます。

NTFS アクセス許可は Windows SMB クライアントから制御されます。

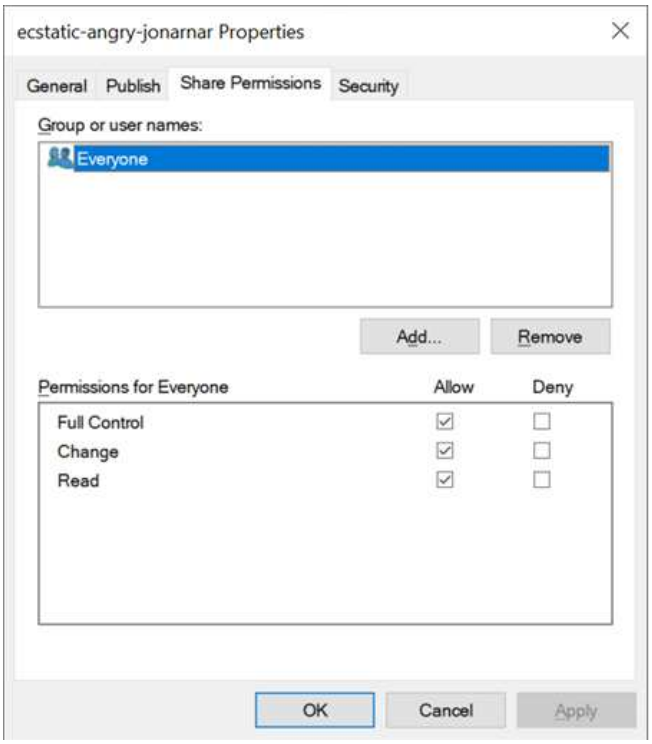
共有権限

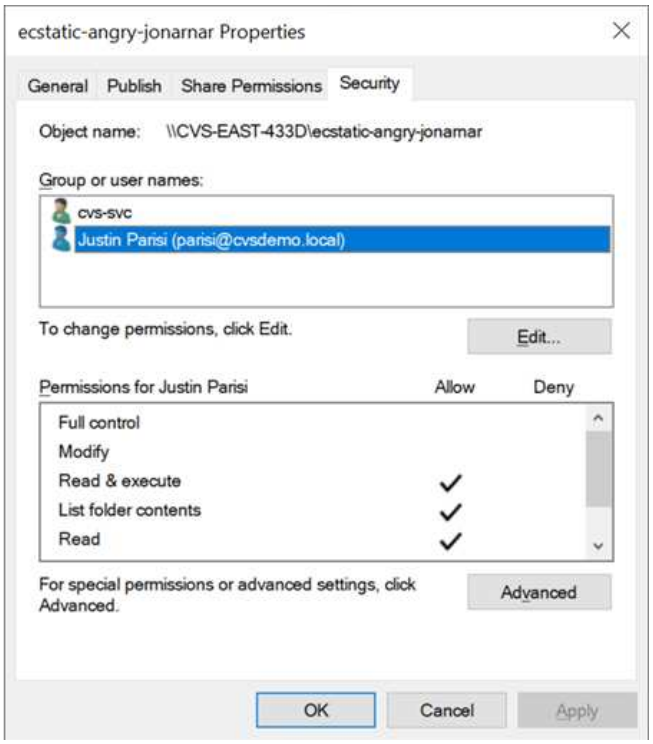
共有アクセス許可は、NTFS アクセス許可 (読み取り/変更/フル コントロールのみ) よりも一般的であり、NFS エクスポート ポリシー ルールの動作と同様に、SMB 共有への最初のエントリを制御します。

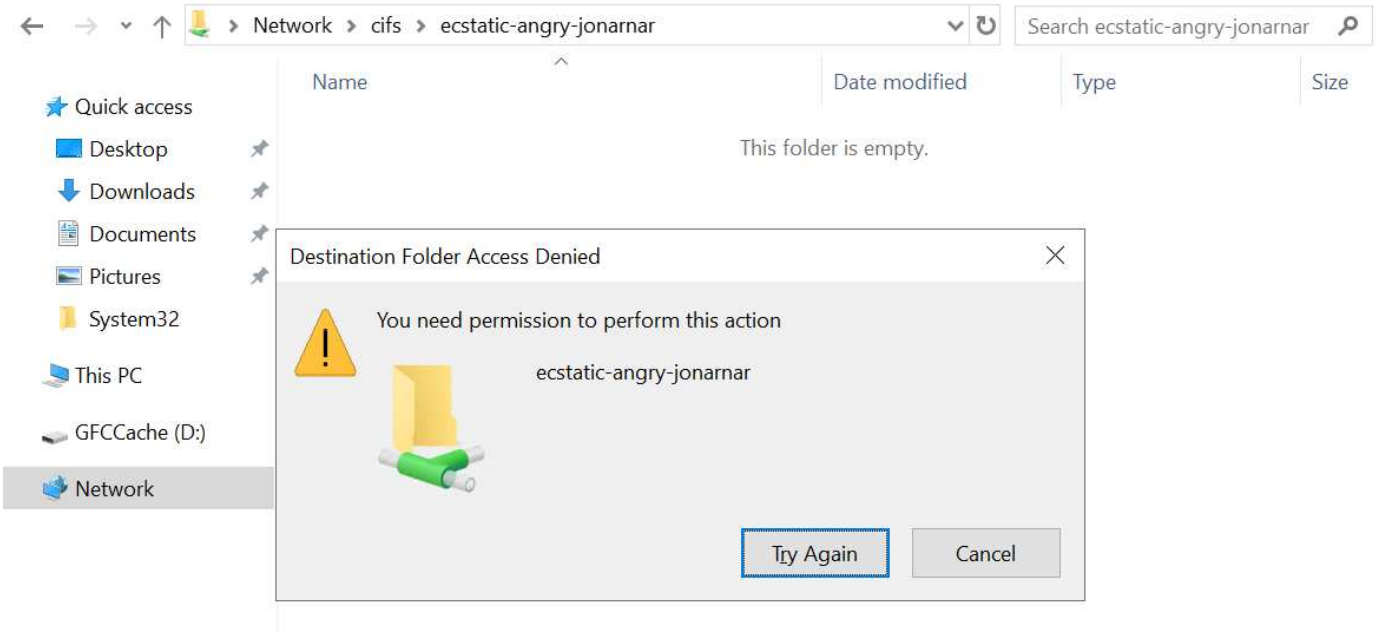
NFS エクスポート ポリシー ルールは、IP アドレスやホスト名などのホストベースの情報を通じてアクセスを制御しますが、SMB 共有アクセス許可は、共有 ACL 内のユーザーおよびグループ ACE を使用してアクセスを制御できます。共有 ACL は、Windows クライアントまたはGoogle Cloud NetApp Volumes管理 UI から設定できます。

デフォルトでは、共有 ACL と初期ボリューム ACL にはフル コントロールを持つ Everyone が含まれます。ファイル ACL を変更する必要がありますが、共有のアクセス許可は共有内のオブジェクトのファイルアクセス許可によって上書きされます。

たとえば、ユーザーにGoogle Cloud NetApp Volumes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 コントロールを持つすべてのユーザー」に設定されているにもかかわらず、ファイルやフォルダを作成するアクセスは拒否されます。







最高のセキュリティ結果を得るには、次の操作を行ってください。

- 共有およびファイル ACL から Everyone を削除し、代わりにユーザーまたはグループの共有アクセスを設定します。
- 管理を容易にし、グループ管理を通じて ACL を共有するためにユーザーの削除/追加を高速化するために、個々のユーザーの代わりにグループを使用してアクセス制御を行います。
- 共有権限の ACE に対して、制限の少ない、より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ーとグループへのアクセスをロックダウンして、よりきめ細かなアクセス制御を実現します。
- 明示的な拒否 ACL は許可 ACL を上書きするため、一般的な使用は避けてください。ファイル システムへのアクセスをすぐに制限する必要があるユーザーまたはグループに対して、明示的な拒否 ACL の使用を

制限します。

- 必ず注意してください "ACL継承"権限を変更するときの設定。ファイル数が多いディレクトリまたはボリュームの最上位レベル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にある各ファイルに継承された権限が追加されるため、各ファイルが調整されるたびに、意図しないアクセス/拒否や権限変更の長時間にわたる変更などの望ましくない動作が発生する可能性があります。

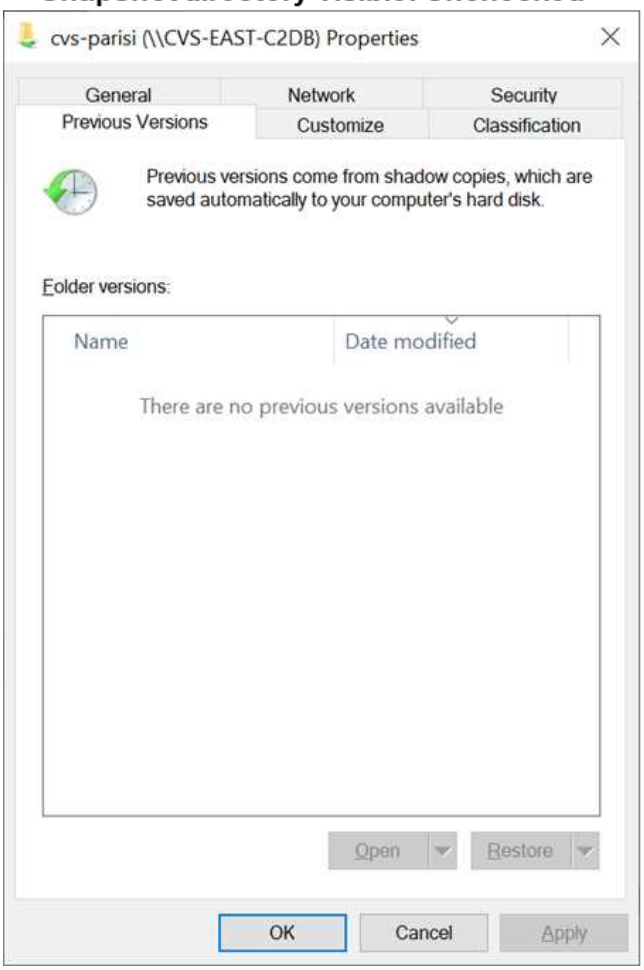
SMB共有のセキュリティ機能

Google Cloud NetApp Volumesで SMB アクセスを使用してボリュームを初めて作成すると、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。

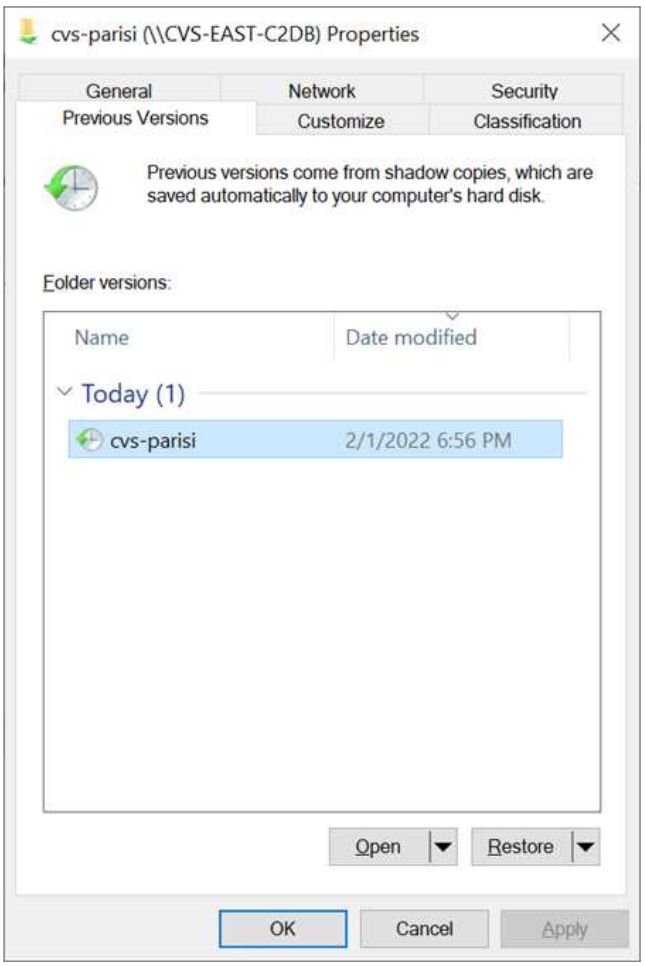
これらの選択肢の一部は、Google Cloud NetApp Volumes のレベル（パフォーマンスまたはソフトウェア）によって異なり、次のような選択肢があります。

- *スナップショット ディレクトリを表示します (NetApp Volumes-Performance とNetApp Volumes-SW の両方で使用可能)。*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`および/または以前のバージョンタブ)。デフォルト設定は「チェックなし」で、ボリュームはデフォルトで非表示になり、アクセスが禁止されます。 `~snapshot`ディレクトリが存在し、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が表示されません。

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)、または設定により、エンド ユーザーからスナップショット コピーを非表示にすることが望ましい場合がありま

す。 Google Cloud NetApp Volumes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したり変更したりすることはできません。スナップショット コピーが作成された時点のファイルまたはフォルダに対するファイル権限が適用されます。ファイルまたはフォルダの権限がスナップショット コピー間で変更された場合、その変更はスナップショット 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。ユーザーとグループは、権限に基づいてこれらのファイルまたはフォルダーにアクセスできます。スナップショット ディレクトリ内のファイルの削除や変更はできませんが、スナップショット ディレクトリからファイルまたはフォルダをコピーすることは可能です。

- **SMB** 暗号化を有効にします **(NetApp Volumes-Performance** と**NetApp Volumes-SW** の両方で使用可能)。 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 (チェックなし)。このボックスをチェックすると SMB 暗号化が有効になり、SMB クライアントとサーバー間のトラフィックは、サポートされている最高の暗号化レベルがネゴシエートされて、転送中に暗号化されます。 Google Cloud NetApp Volumes は、 SMB に対して最大 AES-256 暗号化をサポートします。 SMB 暗号化を有効にすると、SMB クライアントで目立たない程度のパフォーマンスの低下 (約 10 ～ 20 %) が発生します。 NetApp、パフォーマンスの低下が許容できるかどうかを確認するためのテストを強く推奨しています。
- *SMB 共有を非表示にします (NetApp Volumes-Performance とNetApp Volumes-SW の両方で使用可能)。*このオプションを設定すると、SMB 共有パスが通常のブラウジングから非表示になります。つまり、共有パスを知らないクライアントは、デフォルトのUNCパス（ `\\NetApp Volumes-SMB` ）。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認識し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共有パスが定義されているクライアントのみがアクセスできるようになります (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 (NetApp Volumes-SW のみ)。*これは SMB 共有を非表示にするのと似ていますが、共有またはファイルは、オブジェクトにアクセスする権限を持たないユーザーまたはグループに対してのみ非表示になります。例えば、Windowsユーザーの場合 `joe`権限によって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ユーザーは `joe`SMB 共有またはファイルをまったく見ることができません。これはデフォルトでは無効になっていますが、チェックボックスを選択することで有効にすることができます。 ABEの詳細については、 NetAppナレッジベースの記事を参照してください。 "アクセスベースの列挙 (ABE) はどのように機能しますか?"
- 継続的可用性 **(CA)** 共有サポートを有効にします **(NetApp Volumes-Performance** のみ)。 "継続的に利用可能なSMB共有" Google Cloud NetApp Volumesバックエンド システム内のノード間でロック状態を複製することにより、フェイルオーバー イベント中のアプリケーションの中断を最小限に抑える方法を提供します。これはセキュリティ機能ではありませんが、全体的な回復力が向上します。現在、この機能は SQL Server および FSLogix アプリケーションのみでサポートされています。

デフォルトの隠し共有

Google Cloud NetApp VolumesにSMBサーバーを作成すると、 "隠し管理共有" ($ 命名規則を使用) データ ボリューム SMB 共有に加えて作成されます。これらには、C$ (名前空間アクセス) と IPC$ (Microsoft 管理コンソール (MMC) アクセスに使用されるリモート プロシージャ コール (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。

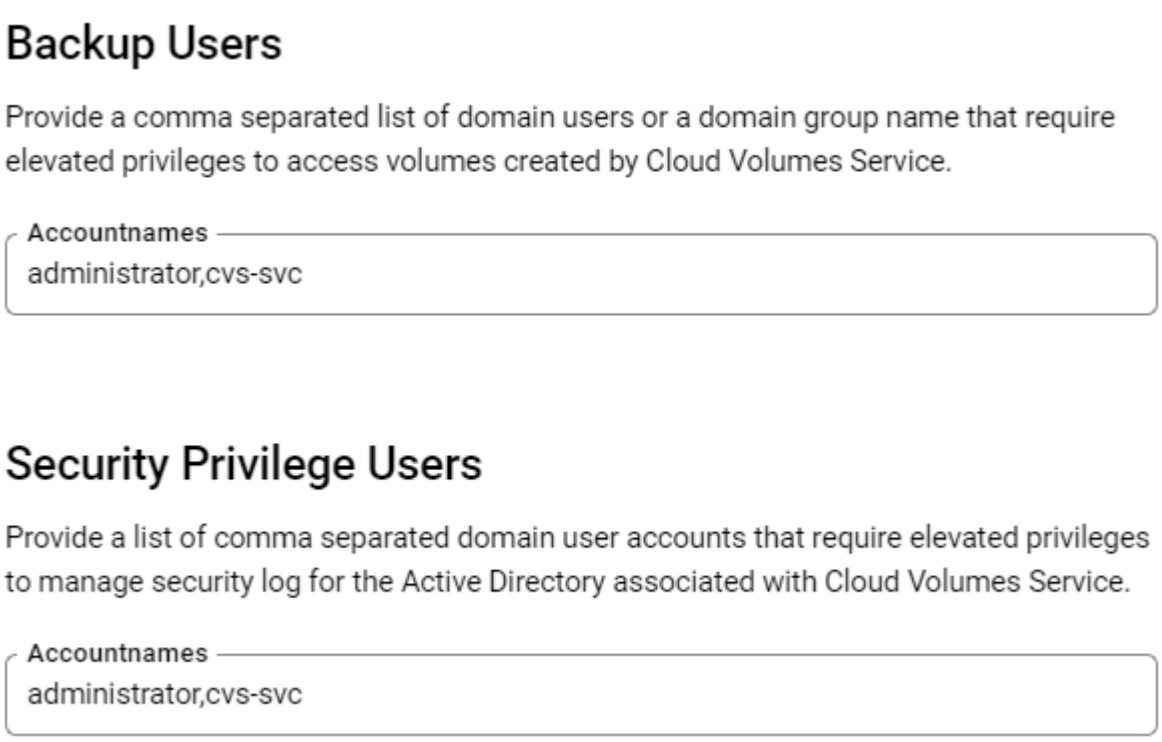
IPC$共有には共有ACLが含まれず、変更できません。RPC呼び出しと "Windowsはデフォルトでこれらの共有への匿名アクセスを許可しません"。

C$ 共有はデフォルトで BUILTIN/Administrators アクセスを許可しますが、 Google Cloud NetApp Volumes の自動化により共有 ACL が削除され、誰に対してもアクセスが許可されなくなります。これは、C$ 共有へのアクセスにより、Google Cloud NetApp Volumesファイル システムにマウントされているすべてのボリュームが可視化されるためです。その結果、 `\\SERVER\C$`失敗。

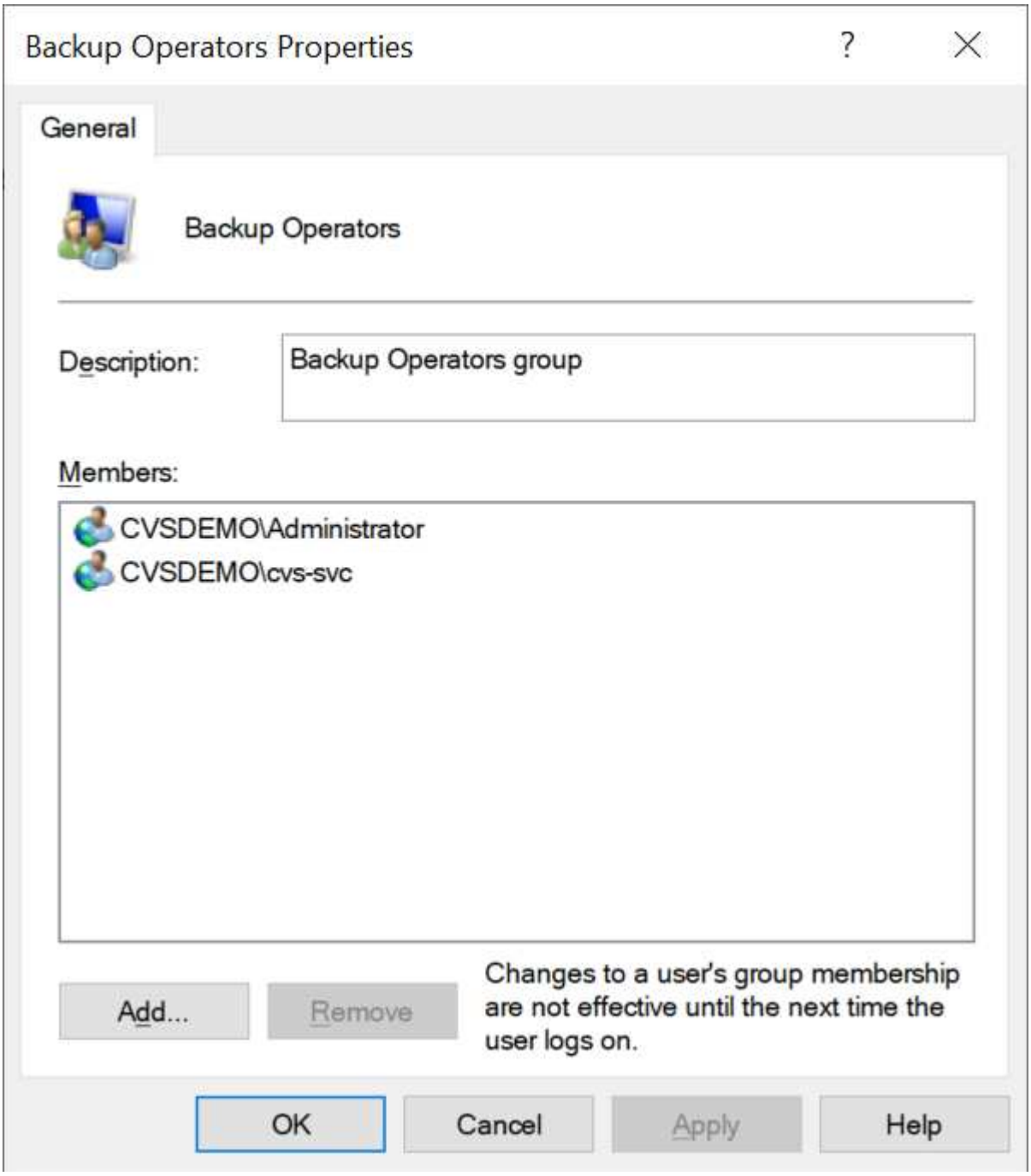
Google Cloud NetApp Volumes SMB サーバーは、選択したドメイン ユーザーとグループにアクセス権を適用するローカル グループ (BUILTIN\Administrators など) があるという点で、通常の Windows SMB サーバーと同様の機能を維持しています。

バックアップユーザーに追加するユーザーを指定すると、そのユーザーは、そのActive Directory接続を使用するGoogle Cloud NetApp VolumesインスタンスのBUILTIN\Backup Operatorsグループに追加され、"SeBackupPrivilege と SeRestorePrivilege" 。

セキュリティ権限ユーザーにユーザーを追加すると、ユーザーにはSeSecurityPrivilegeが付与されます。これは、次のような一部のアプリケーションの使用例で役立ちます。 "SMB 共有上の SQL Server" 。



適切な権限があれば、MMC を通じてGoogle Cloud NetApp Volumes のローカル グループ メンバーシップを表示できます。次の図は、Google Cloud NetApp Volumesコンソールを使用して追加されたユーザーを示しています。

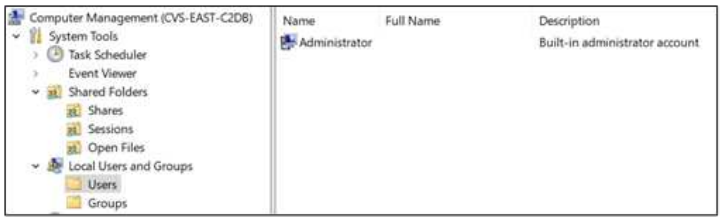


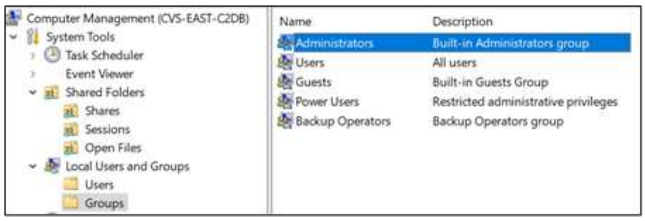
次の表は、デフォルトの BUILTIN グループのリストと、デフォルトで追加されるユーザー/グループを示しています。

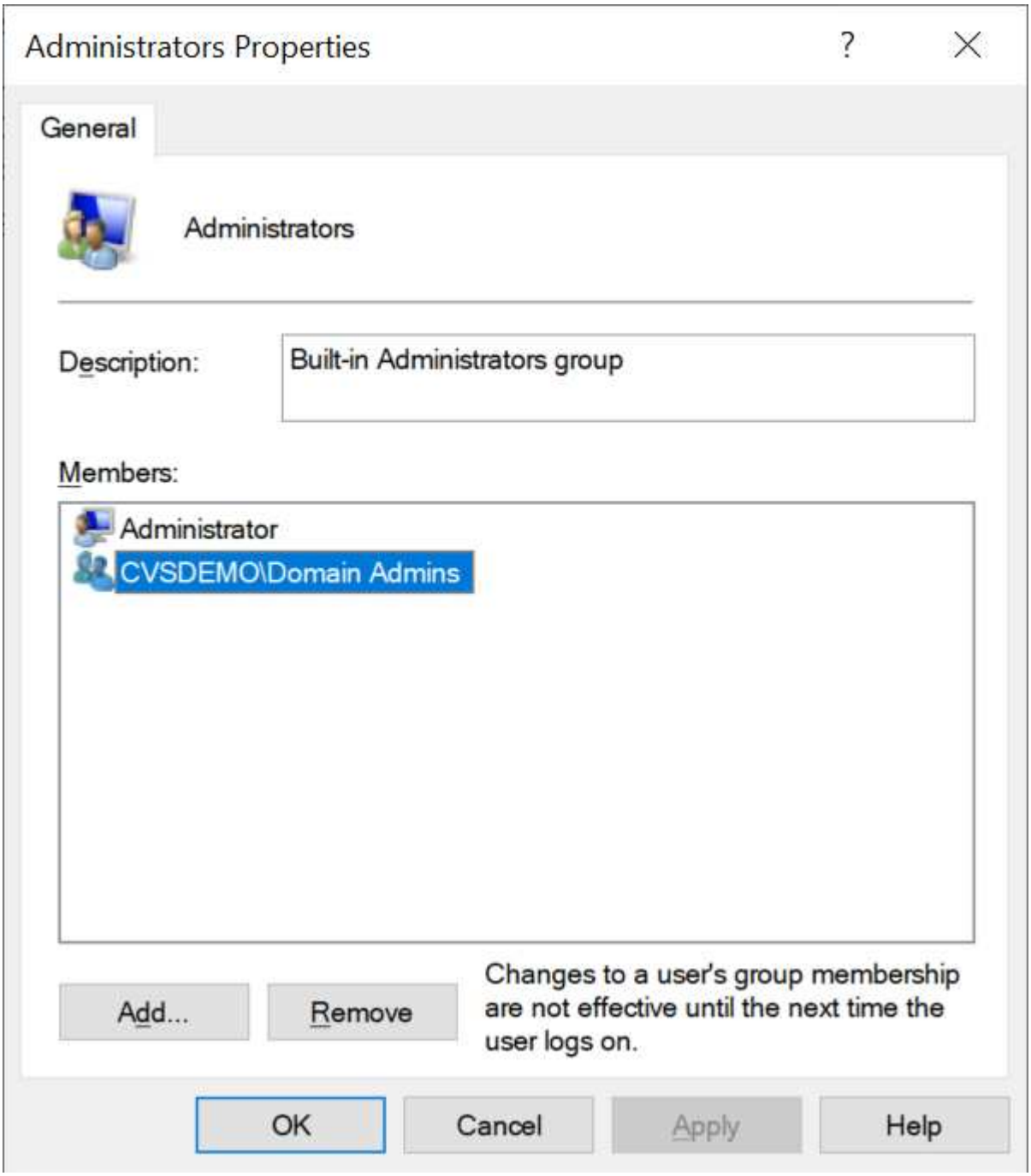
ローカル/**BUILTIN**グループ	デフォルトメンバー
組み込み\管理者*	ドメイン\ドメイン管理者
組み込み\バックアップオペレーター*	なし
ビルトインゲスト	ドメイン\ドメインゲスト
BUILTIN\Power Users	なし
BUILTIN\ドメインユーザー	ドメイン\ドメインユーザー

*グループ メンバーシップは、Google Cloud NetApp Volumes Active Directory 接続構成で制御されます。

MMC ウィンドウではローカル ユーザーとグループ (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を追加または削除したり、グループ メンバーシップを変更したりすることはできません。デフォルトでは、 Google Cloud NetApp Volumesの BUILTIN\Administrators グループには、Domain Admins グループと管理者のみが追加されます。現在、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

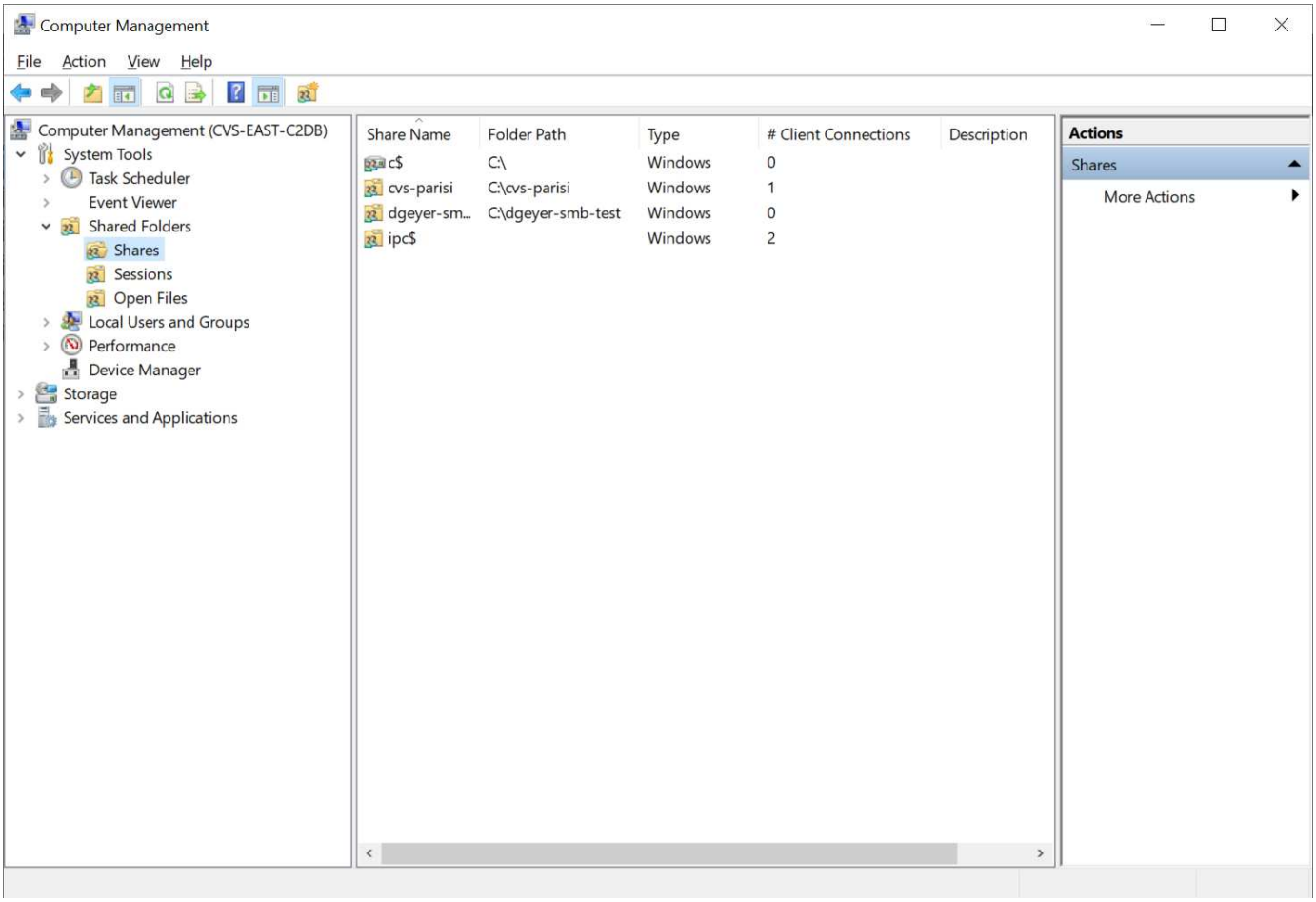
Google Cloud NetApp Volumesの SMB アクセスは、コンピュータ管理 MMC への接続を提供し、共有の表示、共有 ACL の管理、SMB セッションの表示/管理、ファイルのオープンを可能にします。

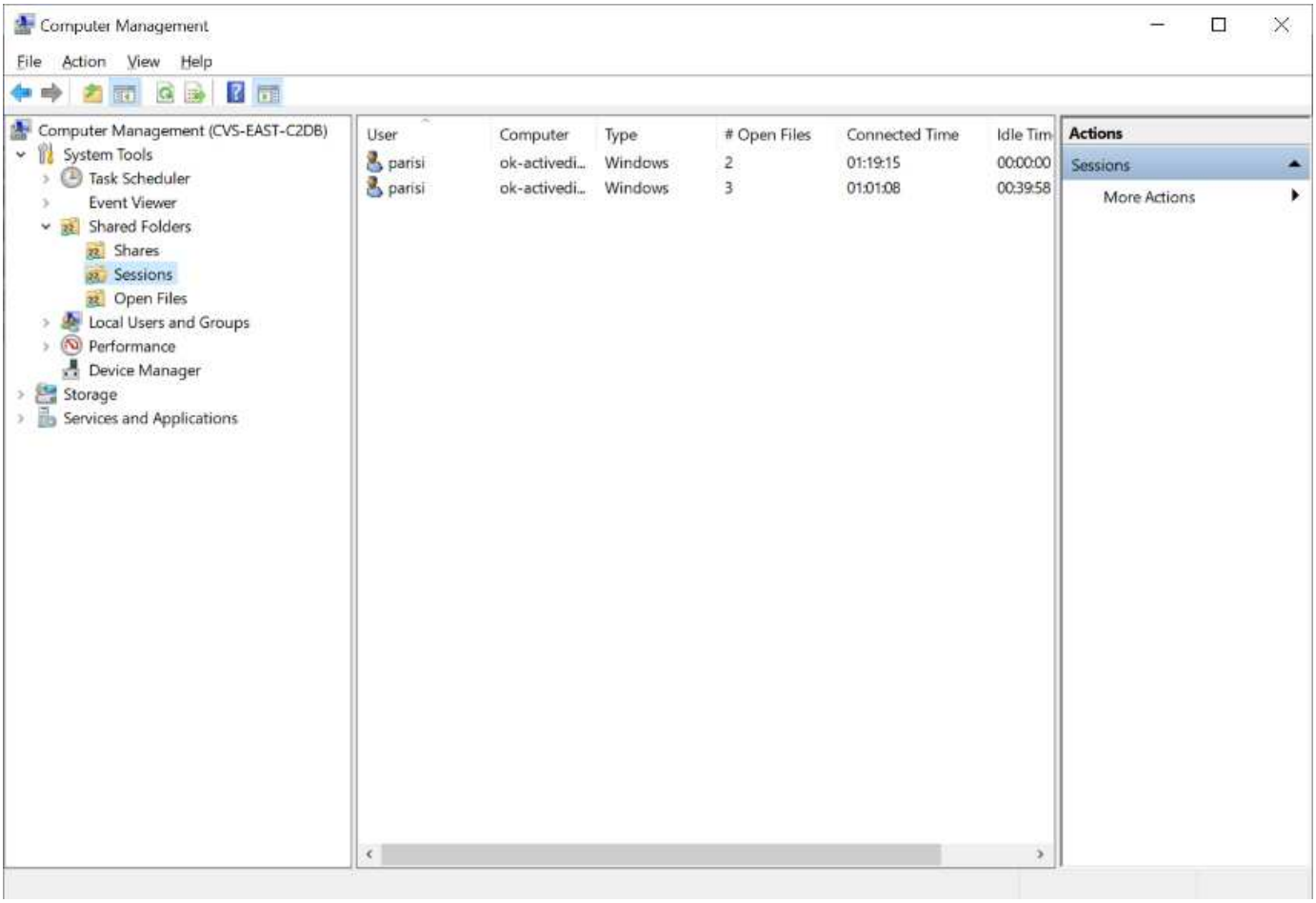
MMC を使用してGoogle Cloud NetApp Volumes内の SMB 共有とセッションを表示するには、現在ログインしているユーザーがドメイン管理者である必要があります。他のユーザーには、MMC から SMB サーバーを表示または管理するアクセス権が付与されており、 Google Cloud NetApp Volumes SMB インスタンス上の共有またはセッションを表示しようとすると、「権限がありません」というダイアログ ボックスが表示されます。

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。これにより、[コンピュータの選択] ダイアログ ボックスが開き、SMB サーバー名 (Google Cloud NetApp Volumes のボリューム情報に記載) 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Google Cloud NetApp Volumesインスタンスで利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、 Google Cloud NetApp Volumesボリューム インスタンスで SMB 共有を非表示にするオプションを設定します。

リージョンごとに 1 つの Active Directory 接続のみが許可されることに注意してください。





次の表は、MMC でサポートされている機能とサポートされていない機能の一覧を示しています。

サポートされている機能	サポートされていない機能
• シェアを見る • アクティブなSMBセッションを表示する • 開いているファイルを表示する • ローカルユーザーとグループを表示する • ローカルグループのメンバーシップを表示する • システム内のセッション、ファイル、ツリー接続のリストを列挙する • システム内の開いているファイルを閉じる • 開いているセッションを閉じる • 共有の作成/管理	• 新しいローカルユーザー/グループの作成 • 既存のローカルユーザー/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する • 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サーバーのセキュリティ情報

Google Cloud NetApp Volumesの SMB サーバーは、Kerberos 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。

次の表には、これらのオプション、その機能、デフォルト構成、 Google Cloud NetApp Volumesで変更でき

るかどうかのリストが含まれています。一部のオプションはGoogle Cloud NetApp Volumesには適用されません。

セキュリティオプション	何をするのか	デフォルト値	変更できますか?
最大 Kerberos クロックスキュー (分)	Google Cloud NetApp Volumesとドメイン コントローラ間の最大時間差。時間のずれが 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 チケットの更新が必要になるまでの最大有効期間。 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。 Google Cloud NetApp Volumes はこれらの更新を自動的に実行します。 10 時間は Active Directory のデフォルト値です。	10	いいえ
Kerberos チケットの最大更新日数（日数）	新しい承認要求が必要になる前に Kerberos チケットを更新できる最大日数。 Google Cloud NetApp Volumes は、SMB 接続のチケットを自動的に更新します。 7 日は Active Directory のデフォルト値です。	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	SMB トラフィックに署名を要求する設定。 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。	間違い	
ローカル ユーザ アカウントに複雑なパスワードを要求	ローカル SMB ユーザーのパスワードに使用されます。 Google Cloud NetApp Volumes はローカル ユーザーの作成をサポートしていないため、このオプションはGoogle Cloud NetApp Volumesには適用されません。	True	いいえ

セキュリティオプション	何をするのか	デフォルト値	変更できますか?
Active Directory LDAP 接続に start_tls を使用する	Active Directory LDAP の TLS 接続の開始を有効にするために使用されます。 Google Cloud NetApp Volumes は現在、これの有効化をサポートしていません。	間違い	いいえ
KerberosのAES-128およびAES-256暗号化は有効になっていますか	これは、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 認証に AES 暗号化を有効にする」オプションで制御されます。	間違い	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方言のレベル。 「SMB認証方言詳細については、「」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	すべての共有に SMB 暗号化が必要です。これはGoogle Cloud NetApp Volumesでは使用されません。代わりに、ボリュームごとに暗号化を設定します（「SMB共有のセキュリティ機能 」）。	間違い	いいえ
クライアントセッションセキュリティ	LDAP 通信の署名および/または封印を設定します。これは現在Google Cloud NetApp Volumesでは設定されていませんが、将来のリリースで対処するために必要になる可能性があります。Windowsパッチによる LDAP認証の問題の修復については、次のセクションで説明します。"LDAP チャネル バインディング。" 。	なし	いいえ
DC接続用のSMB2対応	DC 接続には 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	何をするのか	デフォルト値	変更できますか?
LDAP 参照追跡	複数の LDAP サーバーを使用する場合、参照追跡により、最初のサーバーにエントリが見つからないときにクライアントはリスト内の他の LDAP サーバーを参照できます。これは現在、Google Cloud NetApp Volumesではサポートされていません。	間違い	いいえ
安全な Active Directory 接続には LDAPS を使用する	SSL 経由の LDAP の使用を有効にします。現在、Google Cloud NetApp Volumesではサポートされていません。	間違い	いいえ
DC接続には暗号化が必要です	DC 接続を正常に行うには暗号化が必要です。Google Cloud NetApp Volumesではデフォルトで無効になっています。	間違い	いいえ

デュアルプロトコル/マルチプロトコル

Google Cloud NetApp Volumes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に同じデータセットを共有する機能を提供します("デュアルプロトコル"）。これは、プロトコル間のIDマッピングを調整し、一元化されたバックエンドLDAPサーバを使用してUNIX IDをGoogle Cloud NetApp Volumesに提供することで実現されます。使いやすさを考慮して、Windows Active Directoryを使用してWindowsユーザとUNIXユーザの両方を提供できます。

アクセス制御

- アクセス制御を共有します。 NAS 共有にアクセスできるクライアント、ユーザー、グループを決定します。 NFS の場合、エクスポート ポリシーとルールによってエクスポートへのクライアント アクセスが制御されます。 NFS エクスポートは、Google Cloud NetApp Volumes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、ユーザーおよびグループ レベルでよりきめ細かな制御を提供します。 SMBクライアントから共有レベルのACLを構成するには、https://library.netapp.com/ecmdocs/ECMP1401220/html/GUID-C1772CDF-8AEE-422B-AB87-CFCB7E50FF94.html[MMC/コンピューターの管理^]を使用し、 Google Cloud NetApp Volumesインスタンスの管理者権限を持つアカウントを使用する必要があります（「link:gcp-gcnv-smb.html#Accounts with local/BUILTIN administrator/backup rights["Accounts with local/BUILTIN administrator/backup rights."]」のセクションを参照してください）。
- *ファイル アクセス制御。*ファイルまたはフォルダー レベルでアクセス許可を制御し、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 を利用できます。 SMB クライアントは NTFS アクセス許可を活用します。

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、使用され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の詳細については、「[権限モデル] 。"

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、 Google Cloud NetApp Volumes は、着信ユーザーを反対方向の有効なユーザーにマッピングしようとします。これは、プロトコル全体で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ーが実際に本人であることを確認するために必要です。

たとえば、Windowsユーザーが `joe`SMB経由でUNIX権限を持つボリュームにアクセスしようとすると、 Google Cloud NetApp Volumesは検索を実行し、対応するUNIXユーザーを見つけます。 `joe`。存在する場合、WindowsユーザーとしてSMB共有に書き込まれたファイルは `joe`UNIXユーザーとして表示される `joe`NFS クライアントから。

あるいは、UNIXユーザーが `joe`Windows 権限を使用してGoogle Cloud NetApp Volumesボリュームにアクセスしようとする場合、UNIX ユーザーは有効な Windows ユーザーにマップできる必要があります。それ以外の場合、ボリュームへのアクセスは拒否されます。

現在、LDAPによる外部UNIX ID管理では、Active Directoryのみがサポートされています。このサービスへのアクセス設定の詳細については、 "AD接続の作成"を参照してください。

権限モデル

デュアルプロトコル設定を使用する場合、 Google Cloud NetApp Volumes はボリュームのセキュリティ スタイルを使用して ACL のタイプを決定します。これらのセキュリティ スタイルは、指定された NAS プロトコルに基づいて設定されます。デュアル プロトコルの場合は、 Google Cloud NetApp Volumesボリュームの作成時に選択されます。

- NFS のみを使用している場合、 Google Cloud NetApp Volumesボリュームは UNIX 権限を使用します。
- SMB のみを使用している場合、 Google Cloud NetApp Volumes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 スタイルを選択できます。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。ユーザーが Windows/SMB クライアントから権限を管理する場合は、NTFS を選択します。ユーザーが NFS クライアントと chmod/chown の使用を好む場合は、UNIX セキュリティ スタイルを使用します。

Active Directory 接続を作成する際の考慮事項

Google Cloud NetApp Volumes は、 SMB ユーザーと UNIX ユーザーの両方の ID 管理のために、Google Cloud NetApp Volumesインスタンスを外部 Active Directory サーバーに接続する機能を提供します。 Google Cloud NetApp Volumes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。

この構成では、セキュリティを考慮する必要があるいくつかのオプションが提供されます。外部 Active Directory サーバーは、オンプレミス インスタンスまたはクラウド ネイティブにすることができます。オンプレミスの Active Directory サーバー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、安全なプライベートトンネルまたはVPN、一方向のフォレスト信頼、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てください。 "プライベートGoogleアクセス" 。詳細については、Google Cloudのドキュメントをご覧ください。 "Google Cloud での Active Directory の使用に関するベスト プラクティス" 。

NetApp Volumes-SW では、Active Directory サーバーが同じリージョンに配置されている必要があります。 NetApp Volumes-SW で別のリージョンへの DC 接続を試行すると、失敗します。 NetApp Volumes-SW を使用する場合は、Active Directory DC を含む Active Directory サイトを作成し、 Google Cloud NetApp Volumesでサイトを指定して、リージョン間の DC 接続の

試行を回避するようにしてください。

Active Directory の資格情報

NFS 用の SMB または LDAP が有効になっている場合、 Google Cloud NetApp Volumes はActive Directory コントローラと対話して、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変わらず、Active Directory 内の組織単位 (OU) への同じアクセス権が必要です。

多くの場合、セキュリティ グループでは、 Google Cloud NetApp Volumesなどの外部サーバー上での Windows 管理者アカウントの使用は許可されません。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 管理者ユーザーが完全に無効にされることがあります。

SMBマシンアカウントを作成するために必要な権限

Google Cloud NetApp VolumesマシンオブジェクトをActive Directoryに追加するには、ドメインの管理者権限を持つアカウントか、 "マシンアカウントオブジェクトを作成および変更するための委任された権限"指定された OU へのアクセス許可が必要です。 Active Directory のコントロールの委任ウィザードを使用して、次のアクセス権限が付与されたコンピューター 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 タスクを作成することにより、これを実行できます。

- 読み取り / 書き込み
- すべての子オブジェクトの作成/削除
- 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

これを行うと、定義されたユーザーのセキュリティ ACL が Active Directory 内の 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。ユーザーが委任された後、そのユーザー名とパスワードをこのウィンドウで Active Directory 資格情報として提供できます。

Active Directory ドメインに渡されるユーザー名とパスワードは、マシン アカウント オブジェクトのクエリおよび作成中に 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

`https://docs.cloud.google.com/netapp/volumes/docs/configure-and-use/active-directory/about-ad["Active Directory` 接続の詳細"^]は、管理者がマシンアカウントの配置に関する特定の `Active Directory` スキーマ情報を提供するためのガイダンスを提供します（次のようなもの）：

- *Active Directory 接続タイプ。*リージョン内の Active Directory 接続をGoogle Cloud NetApp VolumesまたはNetApp Volumes-Performance 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されます。既存の接続でこれを誤って設定すると、使用または編集時に正しく機能しない可能性があります。
- ドメイン。 Active Directory ドメイン名。
- *サイト*セキュリティとパフォーマンスのために、Active Directory サーバーを特定のサイトに制限します "考慮事項"。これは、複数の Active Directory サーバーが複数のリージョンにまたがっている場合に必要になります。Google Cloud NetApp Volumes は現在、Google Cloud NetApp Volumes インスタンスとは異な

るリージョンの Active Directory サーバーへの Active Directory 認証リクエストの許可をサポートしていないためです。（たとえば、Active Directory ドメイン コントローラが NetApp Volumes-Performance のみがサポートするリージョンにあるが、NetApp Volumes-SW インスタンスで SMB 共有が必要な場合など。）

- *DNS サーバー*名前の検索に使用する DNS サーバー。
- *NetBIOS 名 (オプション)。*必要に応じて、サーバーの NetBIOS 名。これは、Active Directory 接続を使用して新しいマシン アカウントが作成されるときに使用されます。たとえば、NetBIOS 名がNetApp Volumes-EAST に設定されている場合、マシン アカウント名はNetApp Volumes-EAST-{1234} になります。セクションを参照"Google Cloud NetApp Volumes がActive Directory に表示される仕組み"詳細についてはこちらをご覧ください。
- *組織単位 (OU)。*コンピュータ アカウントを作成する特定の OU。これは、特定の OU のマシン アカウントの制御をユーザーに委任する場合に便利です。
- *AES 暗号化*また、「AD 認証に 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 認証に AES 暗号化を有効にすると、ユーザーとグループの検索時にGoogle Cloud NetApp Volumesから Active Directory への通信のセキュリティが強化されます。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 コントローラーが 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 サーバーは弱い暗号（DES や RC4-HMAC など）を無効にしません。ただし、弱い暗号を無効にする場合は、 Google Cloud NetApp Volumes 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。そうでない場合、認証失敗が発生します。 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、 Google Cloud NetApp Volumes 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レルムの詳細

このオプションは SMB サーバーには適用されません。むしろ、 Google Cloud NetApp Volumesシステム用に NFS Kerberos を構成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 レルムが構成され（Linux の krb5.conf ファイルと同様）、 Google Cloud NetApp Volumesボリュームの作成時に NFS Kerberos が指定されたときに使用されます。これは、Active Directory 接続が NFS Kerberos 配布センター（KDC）として機能するためです。

> 現在、Windows 以外の KDC は、Google Cloud NetApp Volumesでの使用はサポートされていません。

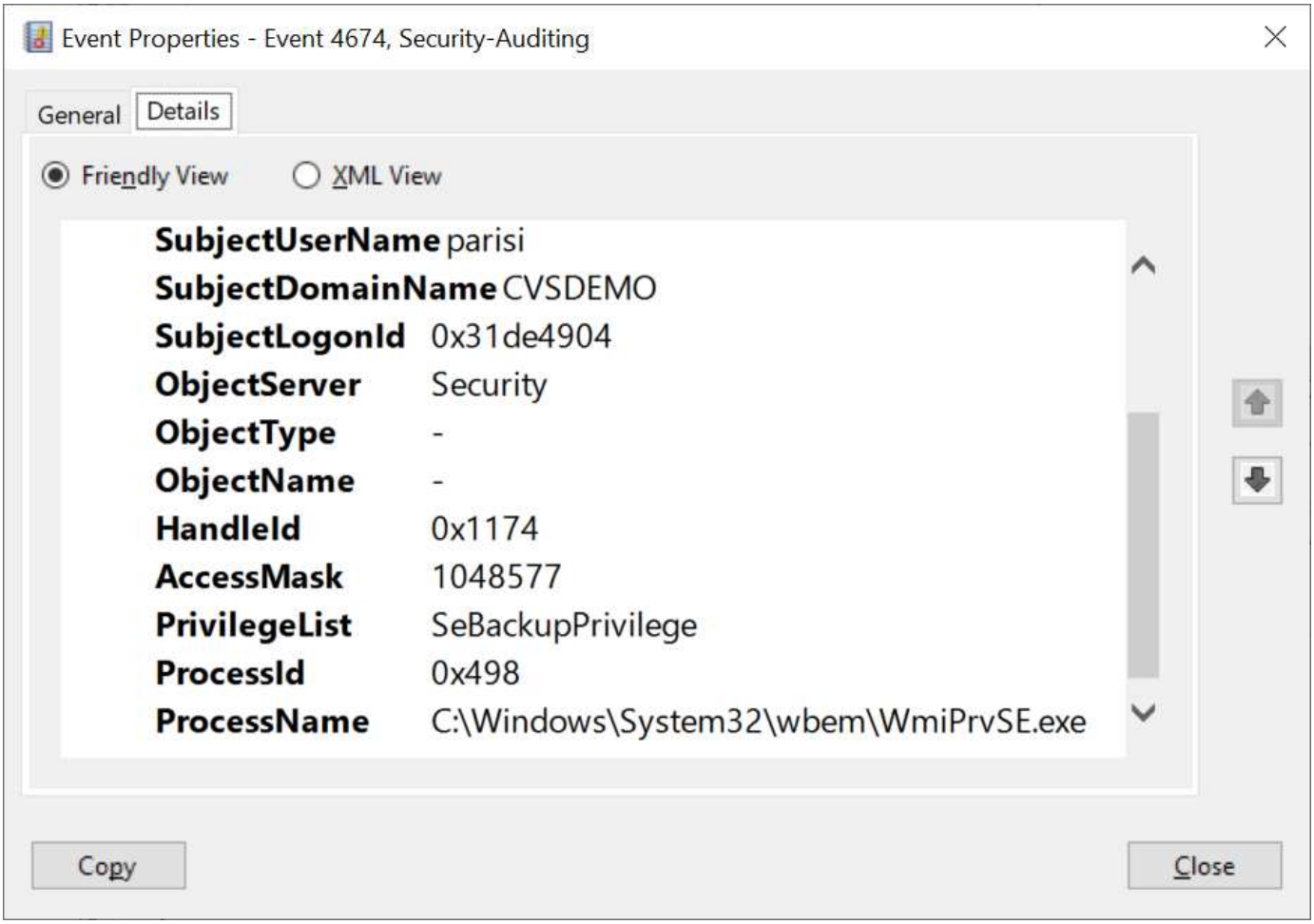
リージョン

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、Google Cloud NetApp Volumesボリュームと同じリージョンである必要があります。

- *LDAP を使用したローカル NFS ユーザー。*このセクションには、LDAP を使用してローカル NFS ユーザーを許可するオプションもあります。 UNIX ユーザー グループ メンバーシップのサポートを NFS (拡張グループ) の 16 グループ制限を超えて拡張する場合は、このオプションを選択解除したままにする必要があります。ただし、拡張グループを使用するには、UNIX ID 用に設定済みの LDAP サーバーが必要です。 LDAP サーバーがない場合は、このオプションを選択しないでください。 LDAP サーバーがあり、ローカル UNIX ユーザー (root など) も使用したい場合は、このオプションを選択します。

バックアップユーザー

このオプションを使用すると、Google Cloud NetApp Volumesボリュームへのバックアップ権限を持つ Windows ユーザーを指定できます。一部のアプリケーションでは、NAS ボリューム内のデータを適切にバックアップおよび復元するために、バックアップ権限 (SeBackupPrivilege) が必要です。このユーザーはボリューム内のデータに高いレベルのアクセス権を持っているため、 "そのユーザーアクセスの監査を有効にする" 。有効にすると、監査イベントがイベント ビューアー > Windows ログ > セキュリティに表示されます。



セキュリティ権限ユーザー

このオプションを使用すると、Google Cloud NetApp Volumesボリュームに対するセキュリティ変更権限を持つ Windows ユーザーを指定できます。一部のアプリケーションではセキュリティ権限（SeSecurityPrivilege）が必要です("SQL Serverなど") をインストール中に権限を適切に設定します。セキュリティ ログを管理するにはこの権限が必要です。この権限はSeBackupPrivilegeほど強力ではありませんが、 NetAppは "ユーザーのユーザーアクセスの監査"必要に応じてこの権限レベルを使用します。

詳細については、以下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" 。

Google Cloud NetApp Volumes がActive Directory に表示される仕組み

Google Cloud NetApp Volumes は、 Active Directory に通常のマシン アカウント オブジェクトとして表示されます。命名規則は次のとおりです。

- CIFS/SMB と NFS Kerberos は個別のマシン アカウント オブジェクトを作成します。

- LDAP が有効になっている NFS は、Kerberos LDAP バインド用に Active Directory にマシン アカウントを作成します。
- LDAP を使用したデュアル プロトコル ボリュームは、LDAP と SMB の CIFS/SMB マシン アカウントを共有します。
- CIFS/SMB マシン アカウントでは、マシン アカウントに NAME-1234 (10 文字未満の名前にハイフンが追加されたランダムな 4 桁の ID) という命名規則が使用されます。 Active Directory接続のNetBIOS名設定でNAMEを定義できます（「Active Directory接続の詳細 」）。
- NFS Kerberos は命名規則として NFS-NAME-1234 (最大 15 文字) を使用します。 15 文字を超える場合、名前は NFS-TRUNCATED-NAME-1234 になります。
- LDAP が有効になっている NFS のみのNetApp Volumes-Performance 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 サーバー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マシンアカウントが作成されると、デフォルトで非表示の管理共有（セクションを参照）が作成されます。"デフォルトの隠し共有") も作成されます (c$、admin$、ipc$) が、これらの共有には ACL が割り当てられておらず、アクセスできません。
- マシン アカウント オブジェクトは、既定では 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。 「SMBマシンアカウントを作成するために必要な権限 Google Cloud NetApp Volumes のマシン アカウント オブジェクトを追加/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。

Google Cloud NetApp Volumes がSMB マシン アカウントを Active Directory に追加すると、次のフィールドにデータが入力されます。

- cn (指定されたSMBサーバー名)
- 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 暗号化が有効な場合は、SMB のマシン アカウントとの Kerberos チケット交換で DES_CBC_MD5、RC4_HMAC_MD5、AES128_CTS_HMAC_SHA1_96、AES256_CTS_HMAC_SHA1_96 が許可されます)
- 名前（SMBサーバー名を含む）
- sAMAccountName（SMBserver$付き）
- servicePrincipalName (Kerberos の host/smbserver.domain.com および host/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 値	**Enctype**が有効
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

msDS-SupportedEncryptionTypes 値	**Enctype**が有効
30	DES_CBC_MD5、RC4_HMAC、AES128_CTS_HMAC_SHA1_96、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 接続を作成するときに [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、 "Google Cloud NetApp Volumesのドキュメントをご覧ください"。

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**、**DNS)**

NAS 共有にGoogle Cloud NetApp Volumesを使用する場合、適切な機能には外部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発生します。次の表は、さまざまな構成オプションと、必要な依存関係（ある場合）を示しています。

構成	依存関係が必要
NFSv3のみ	なし
NFSv3 Kerberosのみ	Windows アクティブ ディレクトリ: * KDC * DNS * LDAP
NFSv4.1のみ	クライアント ID マッピング構成 (/etc/idmap.conf)
NFSv4.1 Kerberosのみ	• クライアント ID マッピング構成 (/etc/idmap.conf) • Windows アクティブ ディレクトリ: KDC DNS LDAP
SMBのみ	アクティブディレクトリ: * KDC * DNS
マルチプロトコル NAS (NFS および SMB)	• クライアント ID マッピング構成 (NFSv4.1 のみ; /etc/idmap.conf) • Windows アクティブ ディレクトリ: KDC DNS LDAP

マシン アカウント オブジェクトの **Kerberos** キータブのローテーション/パスワードのリセット

SMB マシン アカウントの場合、 Google Cloud NetApp Volumes はSMB マシン アカウントのパスワードの定期的なリセットをスケジュールします。これらのパスワード リセットは Kerberos 暗号化を使用して実行され、毎月第 4 日曜日の午後 11 時から午前 1 時までのランダムな時間にスケジュールに従って実行されます。これらのパスワード リセットにより、Kerberos キーのバージョンが変更され、 Google Cloud NetApp Volumesシステムに保存されているキータブがローテーションされ、 Google Cloud NetApp Volumesで実行されている SMB サーバーのセキュリティ レベルが向上します。マシン アカウントのパスワードはランダム化されており、管理者にはわかりません。

NFS Kerberos マシン アカウントの場合、パスワードのリセットは、新しいキータブが KDC で作成または交換された場合にのみ実行されます。現在、 Google Cloud NetApp Volumesではこれを実行できません。

LDAP および **Kerberos** で使用するネットワーク ポート

LDAPとKerberosを使用する場合は、これらのサービスが使用するネットワークポートを特定する必要があります。Google Cloud NetApp Volumesで使用されているポートの完全なリストは、 "Google Cloud NetApp Volumes のセキュリティに関する考慮事項に関するドキュメント"で確認できます。

LDAP

Google Cloud NetApp Volumes はLDAP クライアントとして機能し、UNIX ID のユーザーおよびグループの検索に標準の LDAP 検索クエリを使用します。 Google Cloud NetApp Volumesによって提供される標準のデフォルト ユーザー以外のユーザーとグループを使用する場合は、LDAP が必要です。ユーザー プリンシパル (user1@domain.com など) で NFS Kerberos を使用する予定の場合も、LDAP が必要です。現在、Microsoft Active Directory を使用した LDAP のみがサポートされています。

Active Directory を UNIX LDAP サーバーとして使用するには、UNIX ID に使用する予定のユーザーとグループに必要な UNIX 属性を設定する必要があります。 Google Cloud NetApp Volumesは、以下の基準に基づいて属性をクエリするデフォルトのLDAPスキーマテンプレートを使用します。 "RFC-2307-bis" 。その結果、次の表は、ユーザーとグループに入力する必要がある最小限の Active Directory 属性と、各属性の使用目的を示しています。

Active Directory で LDAP 属性を設定する方法の詳細については、以下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	何をするのか
uid*	UNIXユーザー名を指定します
uid番号*	UNIXユーザーの数値IDを指定します
gid番号*	UNIXユーザーのプライマリグループの数値IDを指定します
オブジェクトクラス*	使用されているオブジェクトのタイプを指定します。Google Google Cloud NetApp Volumes、オブジェクト クラスのリストに「user」が含まれている必要があります（ほとんどの Active Directory デプロイメントではデフォルトで含まれています）。
名前	アカウントに関する一般情報（実名、電話番号など、gecos とも呼ばれます）
unixユーザーパスワード	これを設定する必要がありません。NAS 認証の UNIX ID 検索では使用されません。これを設定すると、構成された unixUserPassword 値がプレーンテキストで保存されます。
unixホームディレクトリ	ユーザーが Linux クライアントから LDAP に対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 ディレクトリ機能に LDAP を使用する場合はこれを設定します。
ログインシェル	ユーザーが LDAP に対して認証するときに、Linux クライアントの bash/profile シェルへのパスを定義します。

- Google Cloud NetApp Volumesで適切に機能するには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されます。

属性	何をするのか
cn*	UNIX グループ名を指定します。 LDAP に Active Directory を使用する場合、これはオブジェクトが最初に作成されるときに設定されますが、後で変更できます。この名前は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、UNIX ユーザーの user1 が Linux クライアントの user1 という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。この問題を回避するには、Windows ユーザーの名前を一意の名前（user1-UNIX など）に変更します。Google Google Cloud NetApp Volumesの LDAP では、UNIX ユーザー名に uid 属性が使用されます。
gid番号*	UNIX グループの数値 ID を指定します。
オブジェクトクラス*	使用されているオブジェクトのタイプを指定します。Google Google Cloud NetApp Volumes、オブジェクト クラスのリストにグループが含まれている必要があります (この属性は、ほとんどの Active Directory デプロイメントにデフォルトで含まれています)。
メンバーUid	UNIX グループのメンバーとなる UNIX ユーザーを指定します。 Google Cloud NetApp Volumesの Active Directory LDAP では、このフィールドは必要ありません。 Google Cloud NetApp Volumes LDAP スキーマは、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。このフィールドは、Windows ユーザーを Windows グループに追加することによって入力されます。ただし、Windows グループに UNIX 属性が設定されていない場合、その Windows グループは UNIX ユーザーのグループ メンバーシップ リストに含まれません。 NFS で使用可能にする必要があるグループには、この表にリストされている必須の UNIX グループ属性を設定する必要があります。

- Google Cloud NetApp Volumesで適切に機能するには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されます。

LDAPバインド情報

LDAP でユーザーを照会するには、 Google Cloud NetApp Volumes を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、ディレクトリ検索のために LDAP UNIX 属性を照会するために使用されます。現在、LDAP バインドは SMB マシン アカウントを使用することによってのみ可能です。

LDAPを有効にできるのは `NetApp Volumes-Performance`インスタンスを作成し、NFSv3、NFSv4.1、またはデュアルプロトコル ボリュームに使用します。 LDAP 対応ボリュームを正常にデプロイするには、 Google Cloud NetApp Volumesボリュームと同じリージョンで Active Directory 接続を確立する必要があります。

LDAP が有効になっている場合、特定のシナリオでは次のようになります。

- Google Cloud NetApp Volumesプロジェクトに NFSv3 または NFSv4.1 のみが使用されている場合、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、 Google Cloud NetApp Volumesの LDAP クライアントはマシン アカウントの認証情報を使用して Active Directory にバインドされます。 NFSボリュームおよびデフォルトの隠し管理共有に対してSMB共有は作成されません（セクションを参照）。"デフォルトの隠し共有") の共有 ACL が削除されました。
- Google Cloud NetApp Volumesプロジェクトでデュアルプロトコル ボリュームが使用されている場合、SMB アクセス用に作成された単一のマシン アカウントのみを使用して、 Google Cloud NetApp Volumes内の 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 ボリュームが別途作成される場合 (LDAP を使用した NFS ボリュームが有効になる前または後)、LDAP バインドのマシン 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、SMB 共有および/または LDAP バインド用と NFS Kerberos 認証用の 2 つのマシン アカウントが作成されます。

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ネットワーク経由で渡されます。この既知のポートは現在、 Google Cloud NetApp Volumesでは変更できません。その結果、ネットワーク内でパケット スニッフィングにアクセスできるユーザーは、ユーザー名とグループ名、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ッフィングすることはできません。 LDAP トラフィックにアクティブに参加している (つまり、バインド可能な) VM のみが、LDAP サーバーからのトラフィックを確認できます。 Google Cloud NetApp Volumesのパケットスニッフィングの詳細については、次のセクションをご覧ください。"パケット 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

Google Cloud NetApp Volumesインスタンスで LDAP が有効になっている場合、デフォルトで特定の構成詳細を含む LDAP クライアント構成が作成されます。場合によっては、オプションがGoogle Cloud NetApp Volumesに適用されない（サポートされていない）か、構成できないことがあります。

LDAPクライアントオプション	何をするのか	デフォルト値	変更できますか?
LDAPサーバーリスト	クエリに使用する LDAP サーバー名または IP アドレスを設定します。これはGoogle Cloud NetApp Volumes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 サーバーを定義します。	未設定	いいえ

LDAPクライアントオプション	何をするのか	デフォルト値	変更できますか**?**
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。 Google Cloud NetApp Volumes は、 DNS 内の LDAP の SRV レコードを活用して、ドメイン内の LDAP サーバーを検索します。	Active Directory 接続で指定された 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 に使用する優先 Active Directory サーバーを設定します。 Google Cloud NetApp Volumes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 サーバーの選択を制御します。	設定されていません。	いいえ
SMBサーバー資格情報を使用してバインドする	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、 Google Cloud NetApp Volumesでサポートされている唯一の LDAP バインド方法。	True	いいえ
スキーマテンプレート	LDAP クエリに使用されるスキーマ テンプレート。	MS-AD-BIS	いいえ
LDAP サーバーポート	LDAP クエリに使用されるポート番号。 Google Cloud NetApp Volumes は現在、標準の LDAP ポート 389 のみを使用しています。 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か	クエリとバインドに LDAP over Secure Sockets Layer (SSL) を使用するかどうかを制御します。現在、 Google Cloud NetApp Volumesではサポートされていません。	間違い	いいえ
クエリタイムアウト（秒）	クエリのタイムアウト。クエリの実行時間が指定された値よりも長い場合、クエリは失敗します。	3	いいえ

LDAPクライアントオプション	何をするのか	デフォルト値	変更できますか?
最小バインド認証レベル	サポートされている最小のバインド レベル。 Google Cloud NetApp Volumes はLDAP バインドにマシン アカウントを使用し、Active Directory はデフォルトで匿名バインドをサポートしていないため、このオプションはセキュリティには影響しません。	匿名	いいえ
バインドDN	シンプル バインドが使用される場合にバインドに使用されるユーザー名/識別名 (DN)。 Google Cloud NetApp Volumes は、LDAP バインドにマシン アカウントを使用しており、現在、シンプル バインド認証はサポートされていません。	未設定	いいえ
ベースDN	LDAP 検索に使用されるベース DN。	Active Directory 接続に使用する Windows ドメイン (DN 形式、つまり DC = ドメイン、DC = ローカル)。	いいえ
基本検索範囲	ベース DN 検索の検索範囲。値には、base 、onelevel、または subtree を含めることができます。 Google Cloud NetApp Volumes はサブツリー検索のみをサポートしています。	サブツリー	いいえ
ユーザーDN	LDAP クエリのユーザー検索が開始される DN を定義します。現在、 Google Cloud NetApp Volumesではサポートされていないため、すべてのユーザー検索はベース 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	何をするのか	デフォルト値	変更できますか?
ユーザー検索範囲	ユーザー DN 検索の検索範囲。値には、base 、onelevel、または subtree を含めることができます。 Google Cloud NetApp Volumes は、ユーザー検索範囲の設定をサポートしていません。	サブツリー	いいえ
グループDN	LDAP クエリのグループ検索が開始される DN を定義します。現在、Google Cloud NetApp Volumes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
グループ検索範囲	グループ DN 検索の検索範囲。値には、base 、onelevel、または subtree を含めることができます。 Google Cloud NetApp Volumes は、グループ検索範囲の設定をサポートしていません。	サブツリー	いいえ
ネットグループDN	LDAP クエリのネットグループ検索が開始される DN を定義します。現在、Google Cloud NetApp Volumesではサポートされていないため、すべてのネット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
ネットグループの検索範囲	ネットグループ DN 検索の検索範囲。値には、base、onelevel、または subtree を含めることができます。 Google Cloud NetApp Volumes は、ネットグループの検索範囲の設定をサポートしていません。	サブツリー	いいえ
LDAP 経由で start_tls を使用する	ポート 389 経由の証明書ベースの LDAP 接続に Start TLS を活用します。現在、 Google Cloud NetApp Volumesではサポートされていません。	間違い	いいえ

LDAPクライアントオプション	何をするのか	デフォルト値	変更できますか?
ホストによるネットグループ検索を有効にする	ネットグループを拡張してすべてのメンバーをリストするのではなく、ホスト名によるネットグループの検索を有効にします。現在、 Google Cloud NetApp Volumesではサポートされていません。	間違い	いいえ
ホスト別ネットグループDN	LDAP クエリのホスト別ネットグループ検索が開始される DN を定義します。ホストごとのネットグループは現在、 Google Cloud NetApp Volumesではサポートされていません。	未設定	いいえ
ネットグループ別ホスト検索範囲	ネットグループ別ホスト DN 検索の検索範囲。値には、base、onelevel、または subtree を含めることができます。ホストごとのネットグループは現在、 Google Cloud NetApp Volumesではサポートされていません。	サブツリー	いいえ
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 (署名、シール、なし) を定義します。 Active Directory から要求された場合、LDAP 署名はNetApp Volumes-Performance によってサポートされます。 NetApp Volumes-SW は LDAP 署名をサポートしていません。どちらのサービス タイプでも、シーリングは現在サポートされていません。	なし	いいえ

LDAPクライアントオプション	何をするのか	デフォルト値	変更できますか**?**
LDAP 参照追跡	複数の LDAP サーバーを使用する場合、参照追跡により、最初のサーバーにエントリが見つからないときにクライアントはリスト内の他の LDAP サーバーを参照できます。これは現在、Google Cloud NetApp Volumesではサポートされていません。	間違い	いいえ
グループメンバーシップフィルター	LDAP サーバーからグループ メンバーシップを検索するときに使用するカスタム LDAP 検索フィルターを提供します。現在、 Google Cloud NetApp Volumesではサポートされていません。	未設定	いいえ

非対称名マッピングに**LDAP**を使用する

Google Cloud NetApp Volumes は、デフォルトでは、特別な設定を行わなくても、同じユーザー名を持つ Windows ユーザーと UNIX ユーザーを双方向にマッピングします。 Google Cloud NetApp Volumes が有効な UNIX ユーザー（LDAP を使用）を見つけられる限り、1:1 の名前マッピングが行われます。例えば、Windowsユーザーの場合 `johnsmith`が使用されている場合、 `Google Cloud NetApp Volumes`が`UNIX`ユーザーを見つけることができれば、 `johnsmith` LDAPでは、そのユーザーの名前マッピングが成功し、そのユーザーが作成したすべてのファイル/フォルダが `johnsmith`正しいユーザー所有権と、影響するすべてのACLを表示します。 `johnsmith`使用されている NAS プロトコルに関係なく尊重されます。これは対称名前マッピングと呼ばれます。

非対称名マッピングは、Windows ユーザーと UNIX ユーザー ID が一致しない場合に発生します。例えば、Windowsユーザーの場合 `johnsmith`UNIXのアイデンティティを持つ `jsmith`Google Cloud NetApp Volumes、変動について通知する方法が必要です。 Google Cloud NetApp Volumes は現在、静的な名前マッピング 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必要な権限を確保するには、LDAP を使用して Windows と UNIX の両方の ID のユーザー ID を検索する必要があります。

Google Cloud NetApp Volumesにはデフォルトで `LDAP`名前マップ データベースのインスタンスの ns-switch で、非対称名に LDAP を使用して名前マッピング機能を提供するには、 Google Cloud NetApp Volumes が検索する内容を反映するようにユーザー/グループ属性の一部を変更するだけで済みます。

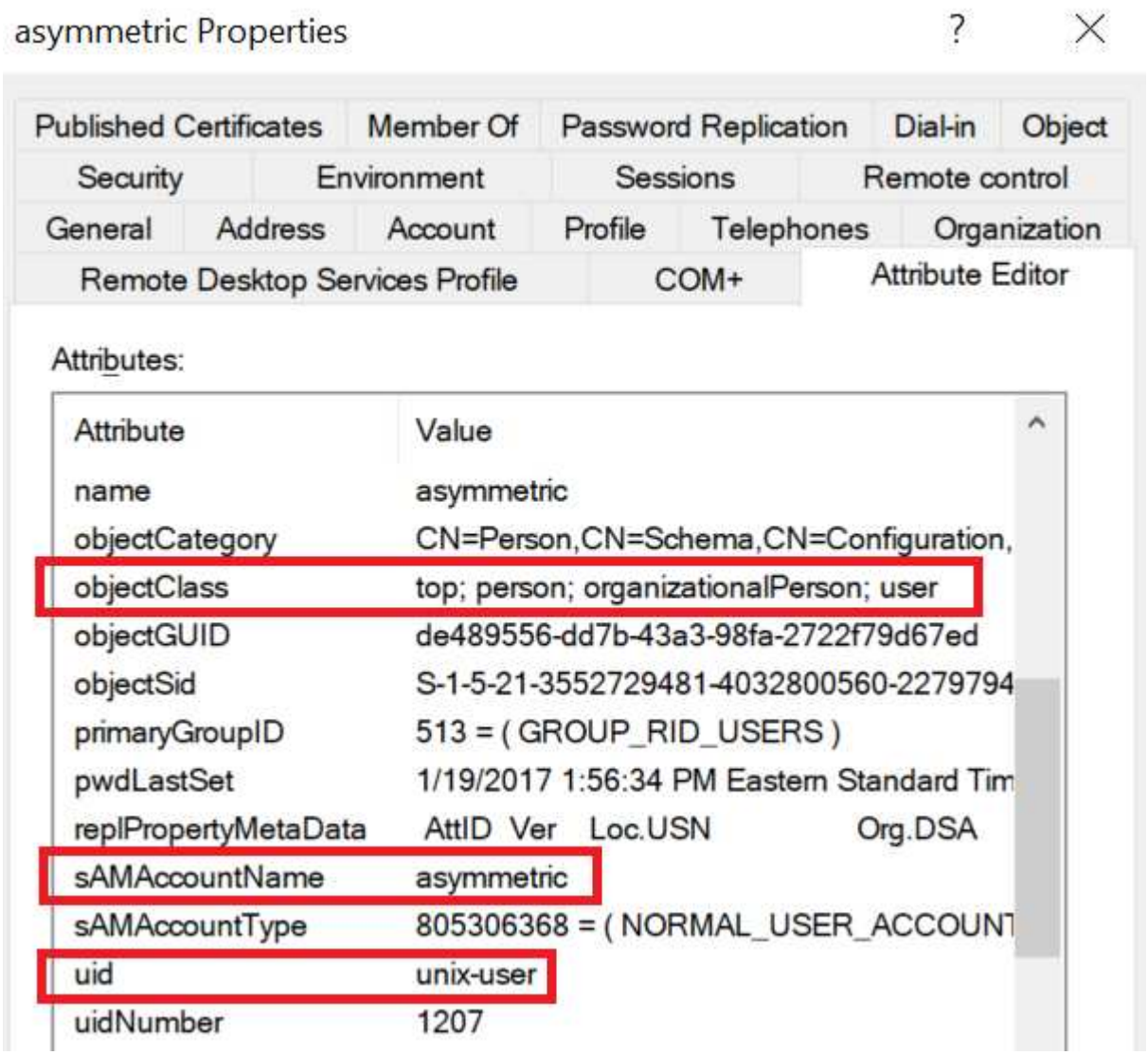
次の表は、非対称名マッピング機能のために LDAP に入力する必要がある属性を示しています。ほとんどの場合、Active Directory はすでにこれを行うように構成されています。

Google Cloud NetApp Volumes属性	何をするのか	**Google Cloud NetApp Volumes**が名前マッピングに使用する値
Windows から UNIX へのオブジェクトクラス	使用されているオブジェクトのタイプを指定します。 (つまり、ユーザー、グループ、posixAccount など)	ユーザーを含める必要があります (必要に応じて他の複数の値を含めることができます)。
WindowsからUNIXへの属性	作成時に Windows ユーザー名を定義します。 Google Cloud NetApp Volumes は、 Windows から UNIX へのルックアップにこれを使用します。	ここで変更する必要はありません。sAMAccountName は Windows ログイン名と同じです。
UID	UNIX ユーザー名を定義します。	希望する UNIX ユーザー名。

Google Cloud NetApp Volumes は現在、LDAP ルックアップでドメイン プレフィックスを使用していないため、複数ドメインの LDAP 環境は LDAP 名前マップ ルックアップでは正しく機能しません。

次の例は、Windows名が `asymmetric`、UNIX名 `unix-user`SMB と NFS の両方からファイルを書き込むときの動作について説明します。

次の図は、Windows サーバーから見た LDAP 属性の外観を示しています。



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
```

NFSからファイルが書き込まれると、 `unix-user` NFS クライアントからの結果は次のとおりです。

```
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 クライアントからは、ファイルの所有者が適切な Windows ユーザーに設定されていることがわかります。

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

逆に、Windowsユーザーが作成したファイルは `asymmetric`SMB クライアントからは、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。

中小企業：

```
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 チャネルバインディング

Windows Active Directoryドメインコントローラの脆弱性のため、 "マイクロソフト セキュリティ アドバイザリ ADV190023" DC が LDAP バインドを許可する方法を変更します。

Google Cloud NetApp Volumesへの影響は、他の LDAP クライアントの場合と同じです。 Google Cloud NetApp Volumes は現在、チャネル バインディングをサポートしていません。 Google Cloud NetApp Volumes 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 バインディングは問題になりません。チャネル バインディングが有効になっている状態で LDAP へのバインディングに問題がある場合は、ADV190023 の修復手順に従って、 Google Cloud NetApp Volumesからの LDAP バインディングが成功す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 または IP からホスト名への解決に DNS に依存しています。 DNS ではポート 53 が開いている必要があります。 Google Cloud NetApp VolumesはDNSレコードに変更を加えず、また現在DNSレコードの使用もサポートしていません。 "動的DNS"ネットワーク インターフェイス上。

Active Directory DNS を構成して、DNS レコードを更新できるサーバーを制限できます。詳細については、以下を参照してください。 "安全な Windows DNS" 。

Google プロジェクト内のリソースはデフォルトで Google Cloud DNS を使用するようになっており、これは Active Directory DNS に接続されていないことに注意してください。 Cloud DNS を使用するクライアント

は、Google Cloud NetApp Volumesによって返される 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 を使用するように構成されており、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DNS構成を設定する必要があります。オプションとして、Cloud DNSを設定して、リクエストをActive Directory DNSに転送することもできます。詳細については、 "クライアントが 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。

> Google Cloud NetApp Volumes 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。

ファイルアクセス監査

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

ウイルス対策保護

NAS 共有のクライアントで、 Google Cloud NetApp Volumesでウイルス対策スキャンを実行する必要があります。現在、 Google Cloud NetApp Volumesとのネイティブウイルス対策統合はありません。

サービス運営

Google Cloud NetApp Volumesチームは、Google Cloud のバックエンド 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。

各顧客には、デフォルトで他の顧客からアクセスが隔離された独自のサブネットが与えられ、 Google Cloud NetApp Volumes内のすべてのテナントには、完全なデータ分離を実現する独自の名前空間と VLAN が与えられます。ユーザーが認証されると、サービス配信エンジン (SDE) はそのテナントに固有の構成データのみを読み取ることができます。

物理的なセキュリティ

適切な事前承認があれば、オンサイト エンジニアとNetAppバッジを持つフィールド サポート エンジニア (FSE) のみがケージとラックにアクセスして物理的な作業を行うことができます。ストレージおよびネットワーク管理は許可されません。ハードウェア メンテナンス タスクを実行できるのは、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、ラック ID とデバイスの場所 (RU) を含む作業明細書 (SOW) のチケットが発行され、その他のすべての詳細がチケットに含まれます。 NetApp FSE の場合、サイト訪問チケットを COLO に提出する必要があり、そのチケットには監査の目的で訪問者の詳細、日付、時刻が記載されます。 FSE の SOW はNetAppに内部的に伝達されます。

運用チーム

Google Cloud NetApp Volumesの運用チームは、Google Cloud NetApp Volumesのプロダクション エンジニアリングとサイト信頼性エンジニア（SRE）、ハードウェアのNetApp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 での作業の認定を受けており、発行されたチケットごとに詳細な作業記録が保持されます。さらに、各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導入されています。

SRE チームは、コントロール プレーンと、データが UI リクエストからGoogle Cloud NetApp Volumesのバッ

クエンドのハードウェアとソフトウェアにルーティングされる方法を管理します。 SRE チームは、ボリュームや inode の最大値などのシステム リソースも管理します。 SRE は顧客データに対話したり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 ハードウェアの新しいディスクやメモリの交換リクエストなどの返品承認 (RMA) の調整も行います。

お客様の責任範囲

Google Cloud NetApp Volumesのお客様は、組織の Active Directory とユーザーロールの管理、およびボリュームとデータの操作を管理します。お客様は管理者ロールを持つことができ、 NetAppと Google Cloud が提供する 2 つの定義済みロール（管理者と閲覧者）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ーに権限を委任できます。

管理者は、顧客プロジェクト内の任意の VPC を、顧客が適切と判断したGoogle Cloud NetApp Volumes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を管理し、データプレーンにアクセスできる VPC を管理するのはお客様の責任です。

悪意のある**SRE**からの保護

懸念されるのは、悪意のある SRE が存在する場合や SRE の認証情報が侵害された場合に、Google Cloud NetApp Volumes がどのように保護するかということです。

実稼働環境へのアクセスは、限られた数の SRE 担当者のみ可能です。管理者権限は、経験豊富な少数の管理者にさらに制限されます。 Google Cloud NetApp Volumes の本番環境で誰かが実行したすべてのアクションはログに記録され、ベースラインに対する異常や疑わしいアクティビティは、Google の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、Google Cloud NetApp Volumesバックエンドに大きな損害が発生する前に、悪意のあるアクションを追跡して軽減することができます。

ボリュームライフサイクル

Google Cloud NetApp Volumes は、ボリューム内のデータではなく、サービス内のオブジェクトのみを管理します。ボリュームにアクセスするクライアントのみが、データ、ACL、ファイル所有者などを管理できます。これらのボリューム内のデータは保存時に暗号化され、アクセスはGoogle Cloud NetApp Volumesインスタンスのテナントに制限されます。

Google Cloud NetApp Volumesのボリューム ライフサイクルは、作成、更新、削除です。ボリュームは削除されるまでボリュームのスナップショット コピーを保持し、検証されたGoogle Cloud NetApp Volumes管理者のみがGoogle Cloud NetApp Volumes内のボリュームを削除できます。管理者によってボリュームの削除が要求された場合、削除を確認するためにボリューム名を入力する追加の手順が必要になります。ボリュームを削除すると、そのボリュームは消えてしまい、回復できなくなります。

Google Cloud NetApp Volumes の契約が終了した場合、 NetApp は一定期間後にボリュームを削除対象としてマークします。その期間が終了する前に、顧客の要求に応じてボリュームを回復することができます。

認定資格

Google Cloud NetApp Volumes for Google Cloud は現在、ISO/IEC 27001:2013 および ISO/IEC 27018:2019 規格の認定を受けています。このサービスは最近、SOC2 タイプ I 認証レポートも受け取りました。 NetApp のデータセキュリティとプライバシーへの取り組みについては、以下をご覧ください。 "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

プライバシーおよび GDPR への準拠に関するコミットメントは、欧州委員会が提供する "標準契約条項" を含む "顧客Data Processing補足契約"など、弊社の複数の "顧客契約" に記載されています。また、これらのコミットメントは、弊社の企業行動規範に定めるコアバリューに基づき、プライバシーポリシーにも明記されています。

追加情報と連絡先

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、次のドキュメントや Web サイトを参照してください。

- Google Google Cloud NetApp Volumes Cloud ドキュメント

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- Google プライベート サービス アクセス

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

- NetApp製品ドキュメント

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

- 暗号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"

- ランサムウェアに対するNetAppソリューション

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

- TR-4616: ONTAPでの NFS Kerberos

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

お問い合わせ

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。

doccomments@netapp.com までお問い合わせください。ご連絡の際は、件名に「TECHNICAL REPORT 4918」と添えてください。

NetApp Disaster Recovery

VMwareワークロードを保護するための、SnapCenterプラグインおよびNetApp Backup and Recoveryを使用したVMware向け3-2-1データ保護

3-2-1 バックアップ戦略は業界で認められたデータ保護方法であり、貴重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、予期しない災害が発生した場合でも、データのコピーが利用可能であることを保証します。

概要

この戦略は、次の 3 つの基本ルールで構成されます。

1. データのコピーを少なくとも 3 つ保存してください。これにより、1 つのコピーが失われたり破損したりした場合でも、少なくとも 2 つのコピーが残っているので、それを頼りにすることができます。
2. 2 つのバックアップ コピーを異なるストレージ メディアまたはデバイスに保存します。ストレージ メディアを多様化することで、デバイス固有またはメディア固有の障害から保護することができます。 1 つのデバイスが破損したり、ある種類のメディアに障害が発生したりしても、他のバックアップ 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、オンサイト コピーが使用できなくなる可能性のある火災や洪水などの局所的な災害に対するフェイルセーフとして機能します。

この解決策ドキュメントでは、オンプレミスの仮想マシンのプライマリおよびセカンダリバックアップを作成するSnapCenter Plug-in for VMware vSphere（SCV）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仮想マシン向けNetApp Backup and Recoveryを使用した3-2-1バックアップ解決策について説明します。

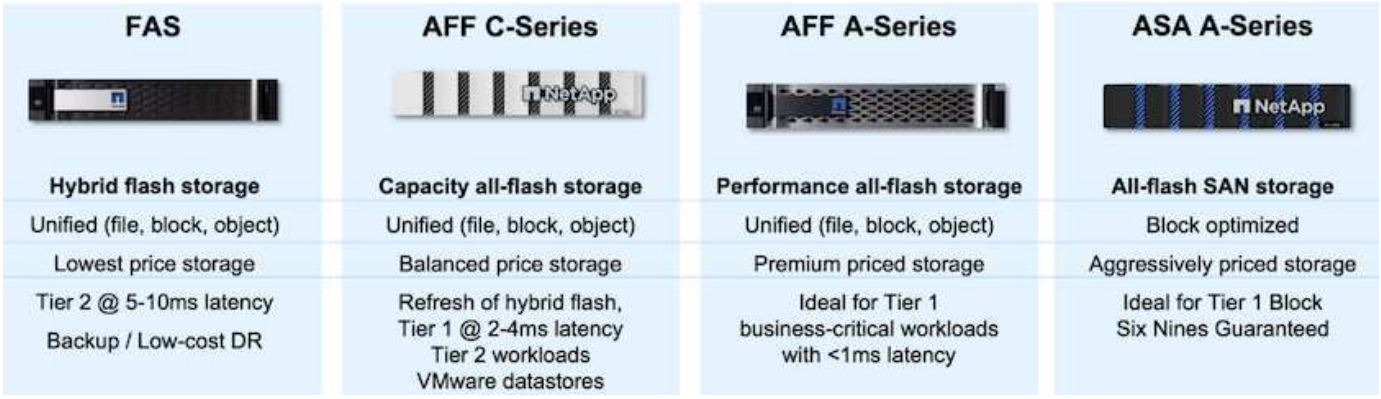
ユースケース

このソリューションは、次のユースケースに対応します。

- SnapCenter Plug-in for VMware vSphereを使用して、オンプレミスの仮想マシンとデータストアをバックアップおよび復元します。
- ONTAPクラスタでホストされ、仮想マシン向けNetApp Backup and Recoveryを使用してオブジェクトストレージにバックアップされる、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。

NetApp ONTAPデータストレージ

ONTAP は、SAN プロトコルまたは NAS プロトコルのどちらでアクセスする場合でも統合ストレージを提供する、NetApp の業界をリードするストレージ ソリューションです。 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 タイプで保護されることが保証され、 NetApp は高速フラッシュから低コストのメディアに至るまでのプラットフォームを提供します。



NetAppのハードウェアプラットフォームの詳細については、以下をご覧ください。 "NetAppデータストレージ" 。

SnapCenter Plug-in for VMware vSphere

SnapCenter Plugin for VMware vSphere は、VMware vSphere と緊密に統合され、仮想マシンのバックアップとリストアの管理を容易にするデータ保護サービスです。このソリューションの一部として、 SnapMirror は、セカンダリONTAPストレージ クラスタ上に仮想マシン データの 2 番目の不変バックアップ コピーを作成するための高速で信頼性の高い方法を提供します。このアーキテクチャを導入すると、プライマリ バックアップの場所またはセカンダリ バックアップの場所から仮想マシンの復元操作を簡単に開始できるようになります。

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展開されます。プラグインはリモート プラグイン アーキテクチャを使用するようになりました。リモート プラグインは vCenter サーバーの外部で実行され、SCV 仮想アプライアンス上でホストされます。

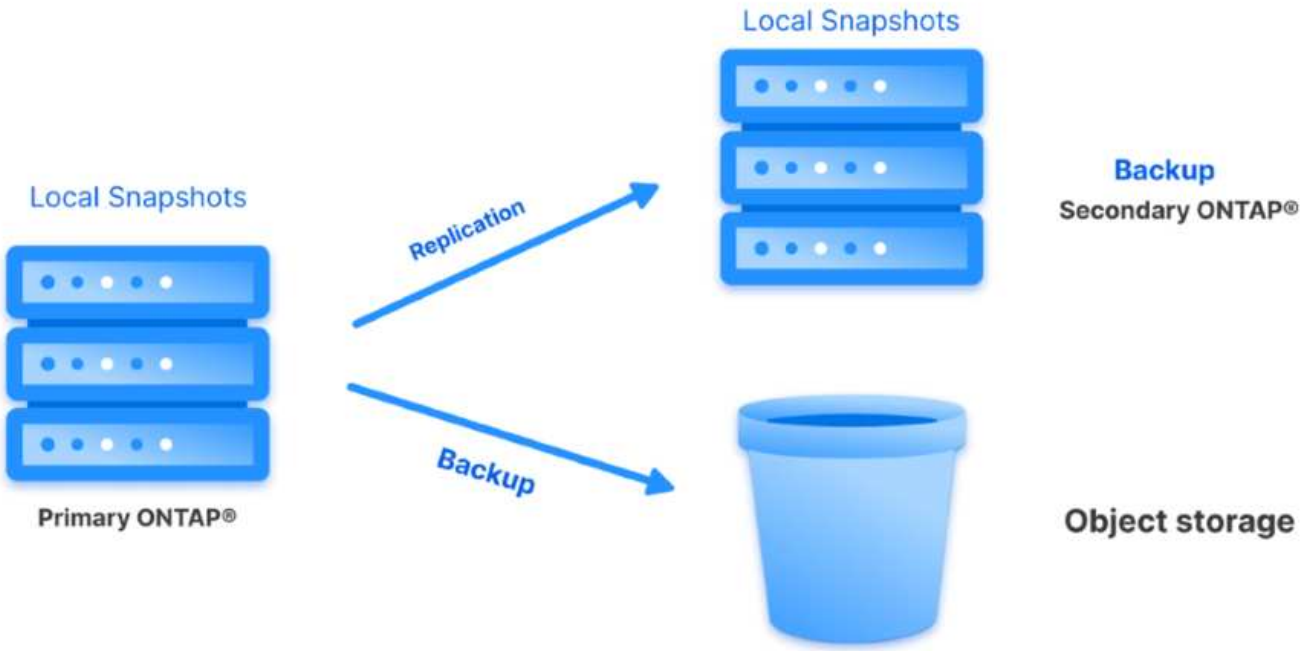
SCVの詳細については、 "SnapCenter Plug-in for VMware vSphereのドキュメント" 。

NetApp Backup and RecoveryによるVMwareワークロードの保護

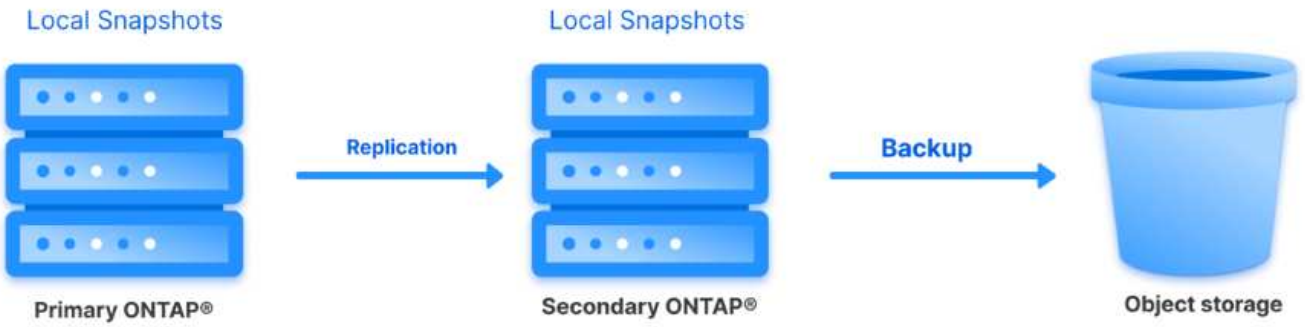
NetApp Backup and Recoveryは、オンプレミス環境とクラウド環境の両方にわたる幅広いバックアップおよびリカバリ操作に単一のコントロール プレーンを提供する、データ管理用のクラウドベースのツールです。NetApp Backup and Recovery for VMスイートの一部として、SnapCenter Plug-in for VMware vSphere（オンプレミス）と統合して、データのコピーをクラウド内のオブジェクトストレージに拡張する機能があります。これにより、プライマリまたはセカンダリストレージのバックアップから取得した、データの3つ目のコピーがオフサイトに作成されます。NetApp Backup and Recovery for VMsを使用すると、これら2つのオンプレミスの場所のいずれ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。

NetApp Backup and Recoveryで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をソースとして選択するかによって、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がバックアップを開始すると、ローカル スナップショットが即座に取得されます。次に、SCVは最新のスナップショットをセカンダリONTAPクラスタにレプリケートするSnapMirror処理を開始します。NetApp Backup and Recoveryでは、選択したクラウド プロバイダのオブジェクト ストレージに転送されるデータのスナップショット コピーのソースとして、ポリシーでプライマリONTAPクラスタを指定します。



カスケードトポロジ – SCVを使用してプライマリおよびセカンダリのデータコピーを作成する手順は、上記のファンアウトトポロジと同じです。ただし今回は、オブジェクトストレージへのバックアップがセカンダリONTAPクラスタから開始されることを指定するポリシーをNetApp Backup and Recoveryで作成します。



NetApp Backup and Recoveryは、オンプレミスのONTAPスナップショットのバックアップコピーをAWS Glacier、Azure Blob、およびGCP Archiveストレージに作成できます。



AWS Glacier
and Deep Glacier



Azure
Blob Archive



GCP
Archive Storage

さらに、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" 。

▼ ソリューション展開の概要

このリストは、この解決策を構成し、SCVおよびNetApp Consoleからバックアップおよびリストア操作を実行するために必要な概要の手順を示しています：

1. プライマリおよびセカンダリ データ コピーに使用するONTAPクラスタ間のSnapMirror関係を構成します。
2. VMware vSphere 用のSnapCenterプラグインを構成します。
   a. ストレージシステムを追加する
   b. バックアップ ポリシーの作成
   c. リソース グループの作成
   d. 最初のバックアップジョブを実行する
3. 仮想マシンのNetApp Backup and Recoveryを設定する
   a. 作業環境を追加する
   b. SCVおよびvCenterアプライアンスの検出
   c. バックアップ ポリシーの作成
   d. バックアップを有効にする
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復元します。
5. NetApp Consoleを使用して、オブジェクトストレージから仮想マシンを復元します。

▼ 前提条件

このソリューションの目的は、VMware vSphere で実行され、 NetApp ONTAPによってホストされる NFS データストアに配置されている仮想マシンのデータ保護を実証することです。このソリューションでは、次のコンポーネントが構成され、使用できる状態になっていることを前提としています。

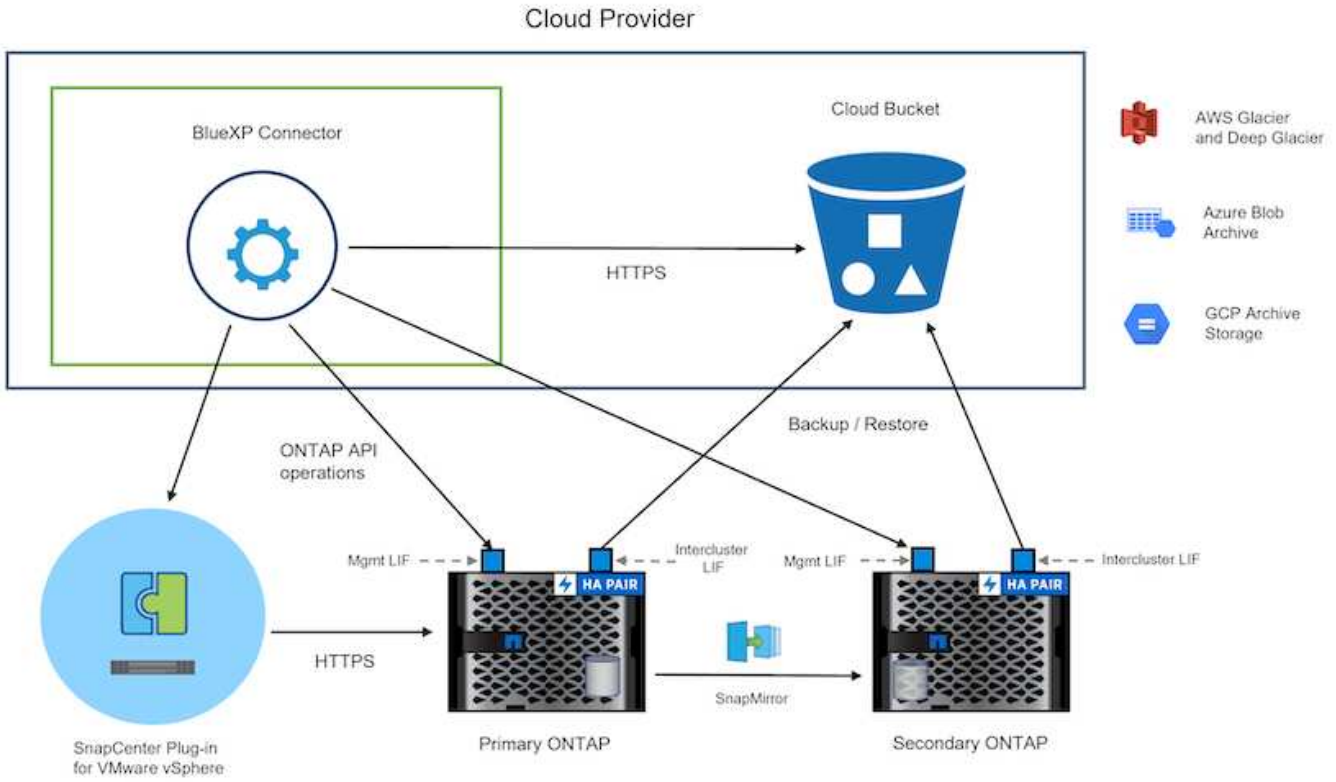
1. VMware vSphere に接続された NFS または VMFS データストアを備えたONTAPストレージ クラスター。 NFS と VMFS の両方のデータストアがサポートされています。このソリューションでは NFS データストアが利用されました。
2. NFS データストアに使用されるボリュームに対してSnapMirror関係が確立されたセカンダリONTAPス

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されるクラウド プロバイダ用にConsoleエージェントがインストールされていること。
4. バックアップされる仮想マシンは、プライマリONTAPストレージ クラスタにある NFS データストア上にあります。
5. ConsoleエージェントとオンプレミスONTAPストレージクラスタ管理インターフェース間のネットワーク接続。
6. ConsoleエージェントとオンプレミスSCVアプライアンスVMの間、およびConsoleエージェントと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 サービス間のネットワーク接続。
8. プライマリおよびセカンダリONTAPストレージ クラスタ上の管理 SVM 用に設定された DNS。詳細については、 "ホスト名解決に使用するDNSの設定" 。

高レベルアーキテクチャ

このソリューションのテスト/検証は、最終的な展開環境と一致する場合も一致しない場合もあるラボで実行されました。



ソリューションの展開

この解決策では、VMware vSphere 向け SnapCenter Plug-in for VMware vSphere と Backup and Recovery を活用して、オンプレミス データ センターに配置された 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解決策のデプロイおよび検証に関する詳細な手順を提供します。このセットアップの仮想マシンは、ONTAP A300 ストレージ クラスタがホストする NFS データストアに格納されています。さらに、別の ONTAP A300 ストレージ クラスタが、SnapMirror を使用してレプリケートされた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。また、Amazon Web Services および

Azure Blob でホストされるオブジェクト ストレージが、データの第 3 のコピーのターゲットとして使用されました。

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およびNetApp Consoleの両方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" 。

バックアップとリカバリの詳細については、 "バックアップとリカバリに関するドキュメント"を参照してください。

ONTAPクラスタ間のSnapMirror関係を確立する

SnapCenter Plug-in for VMware vSphereは、 ONTAP SnapMirrorテクノロジを使用して、セカンダリSnapMirrorおよび/またはSnapVaultコピーのセカンダリONTAPクラスタへの転送を管理します。

SCV バックアップ ポリシーには、 SnapMirrorまたはSnapVault関係を使用するオプションがあります。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用に構成された保持スケジュールがプライマリ ロケーションとセカンダリ ロケーションで同じになることです。 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と、セカンダリONTAPストレージ クラスタ上のスナップショット コピーに対してSnapMirror関係を使用して個別の保持スケジュールを確立できます。

SnapMirror関係のセットアップは、多くの手順が自動化されているNetApp Consoleで実行するか、System ManagerおよびONTAP CLIを使用して実行できます。これらの方法はすべて以下で説明します。

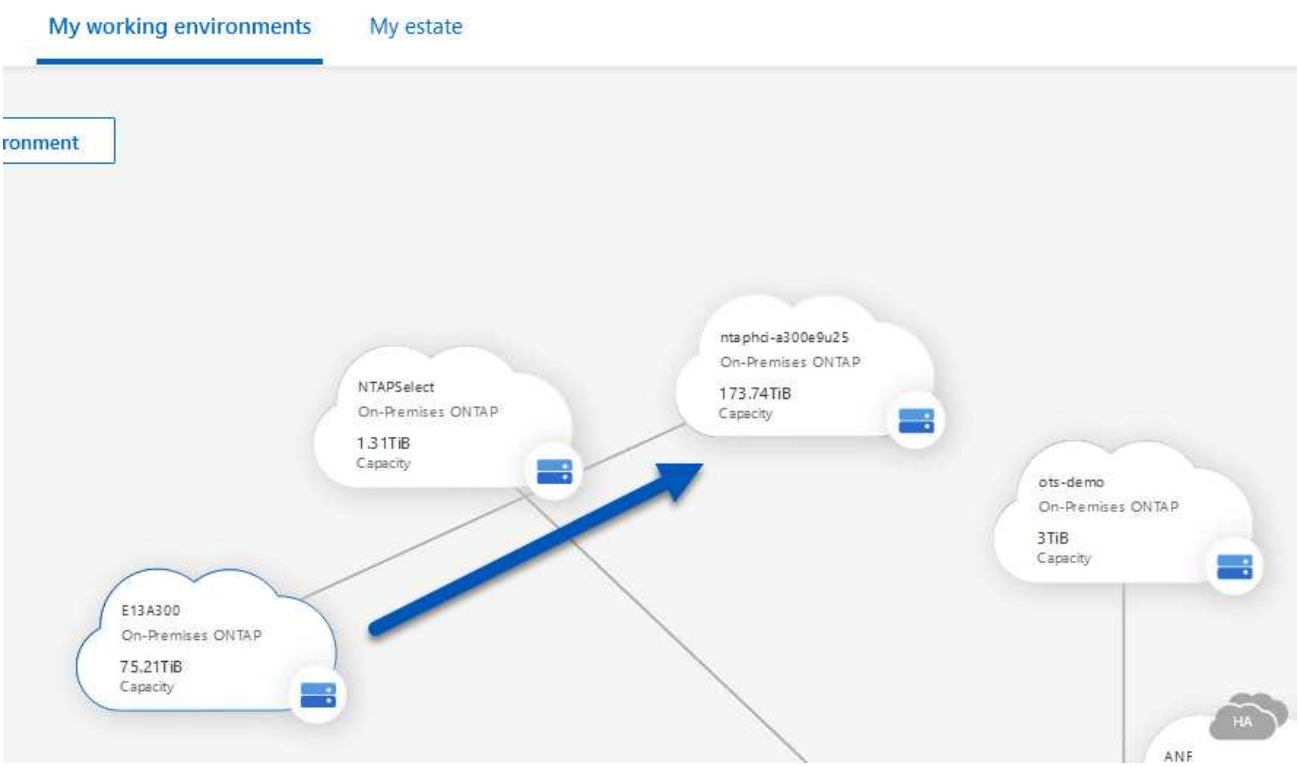
SnapMirror関係をNetApp Consoleで確立する

NetApp Console から以下の手順を完了する必要があります：

▼ プライマリおよびセカンダリONTAPストレージ システムのレプリケーション設定

まず、NetApp Consoleにログインし、システムに移動します。

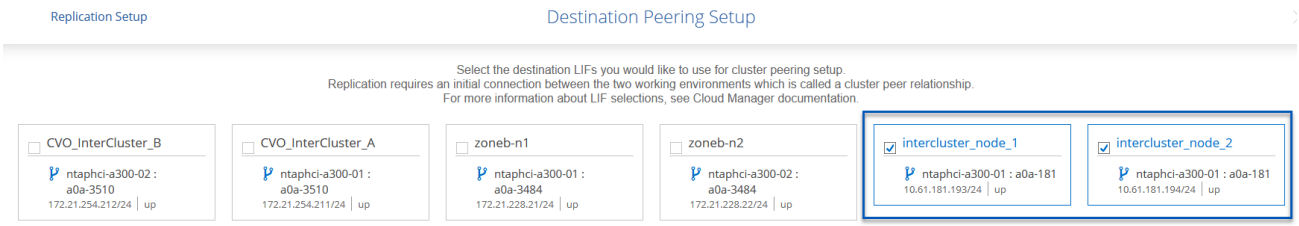
1. ソース (プライマリ) ONTAPストレージ システムを、宛先 (セカンダリ) ONTAPストレージ システムにドラッグ アンド ドロップします。



2. 表示されるメニューから*レプリケーション*を選択します。

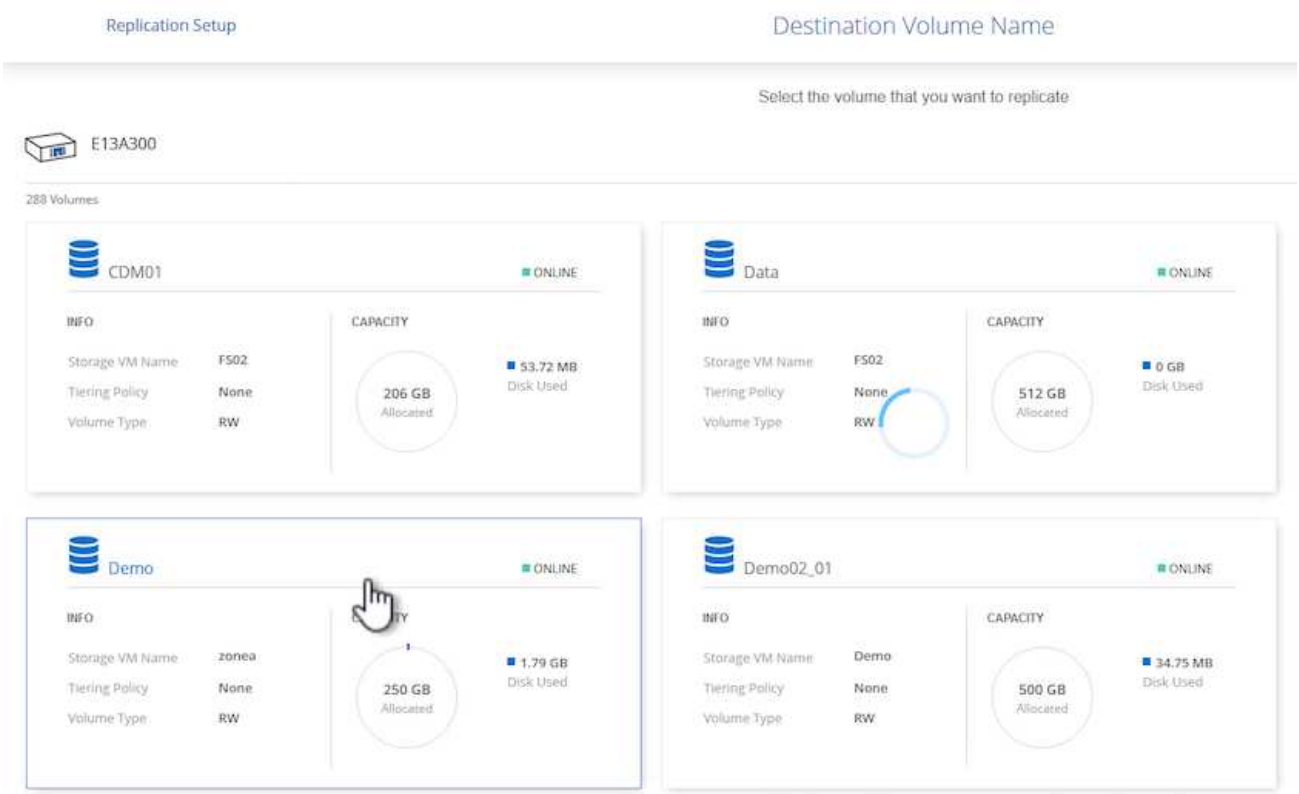


3. 宛先ピアリング設定 ページで、ストレージ システム間の接続に使用する宛先クラスタ間 LIF を選択します。



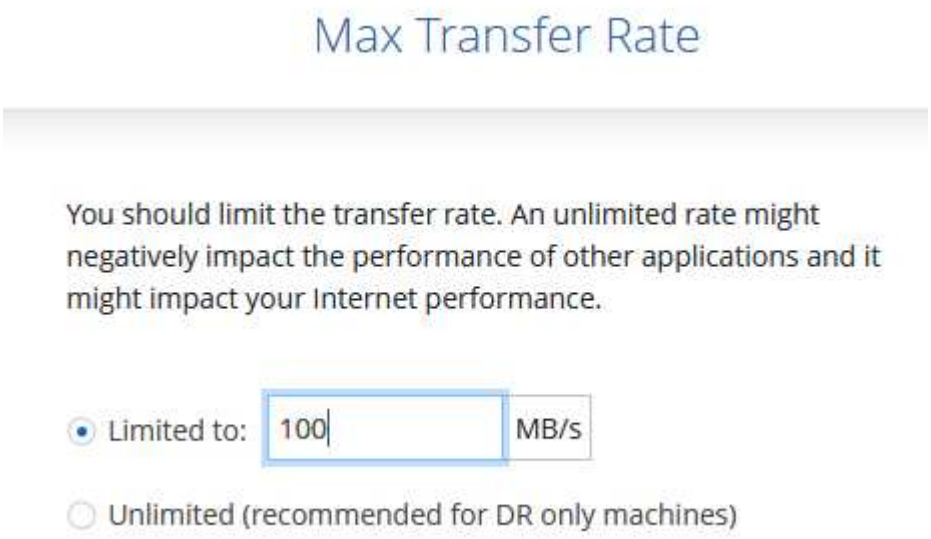
4. 宛先ボリューム名 ページで、最初にソース ボリュームを選択し、次に宛先ボリューム名を入力して、

宛先 SVM とアグリゲートを選択します。続行するには、[次へ] をクリックします。

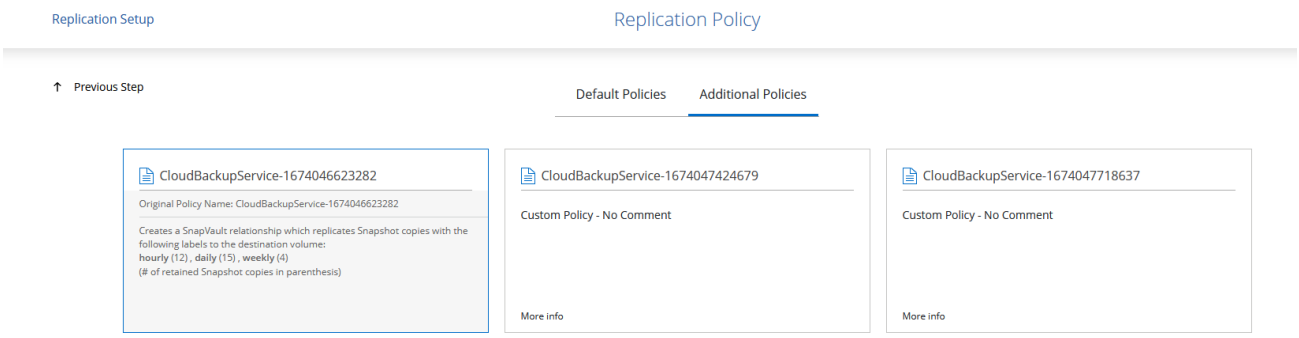




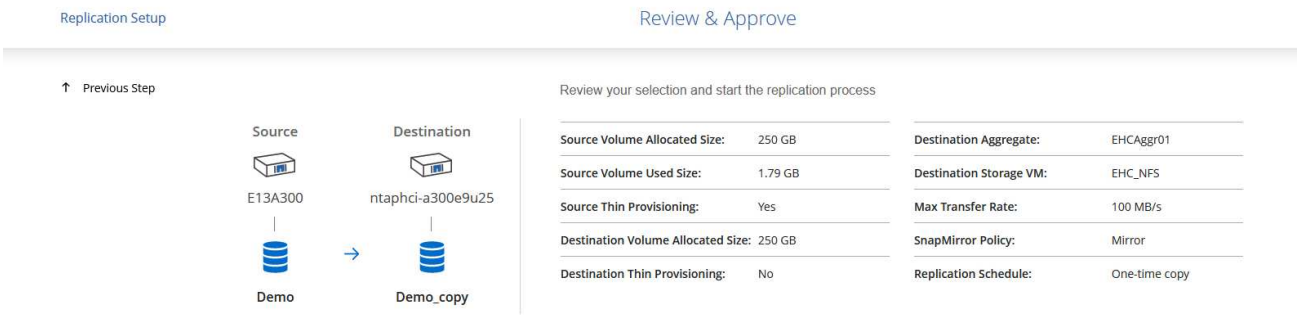
5. レプリケーションを実行するための最大転送速度を選択します。



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 (以下の「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)、必要に応じて事後に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のセットアップ プロセスを開始します。



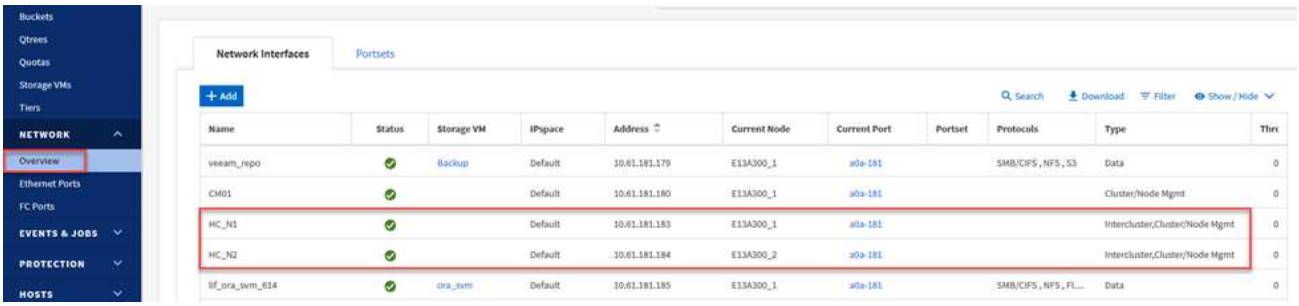
System ManagerとONTAP CLIを使用してSnapMirror関係を確立する

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 を使用して実行できます。次のセクションでは、両方の方法について詳細な情報を提供します。

▼ 送信元と宛先のクラスタ間論理インターフェースを記録する

ソースおよびデスティネーションのONTAPクラスタについては、System Manager または CLI からクラスタ間 LIF 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、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るタイプ: クラスタ間の IP アドレスを取得します。



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
```

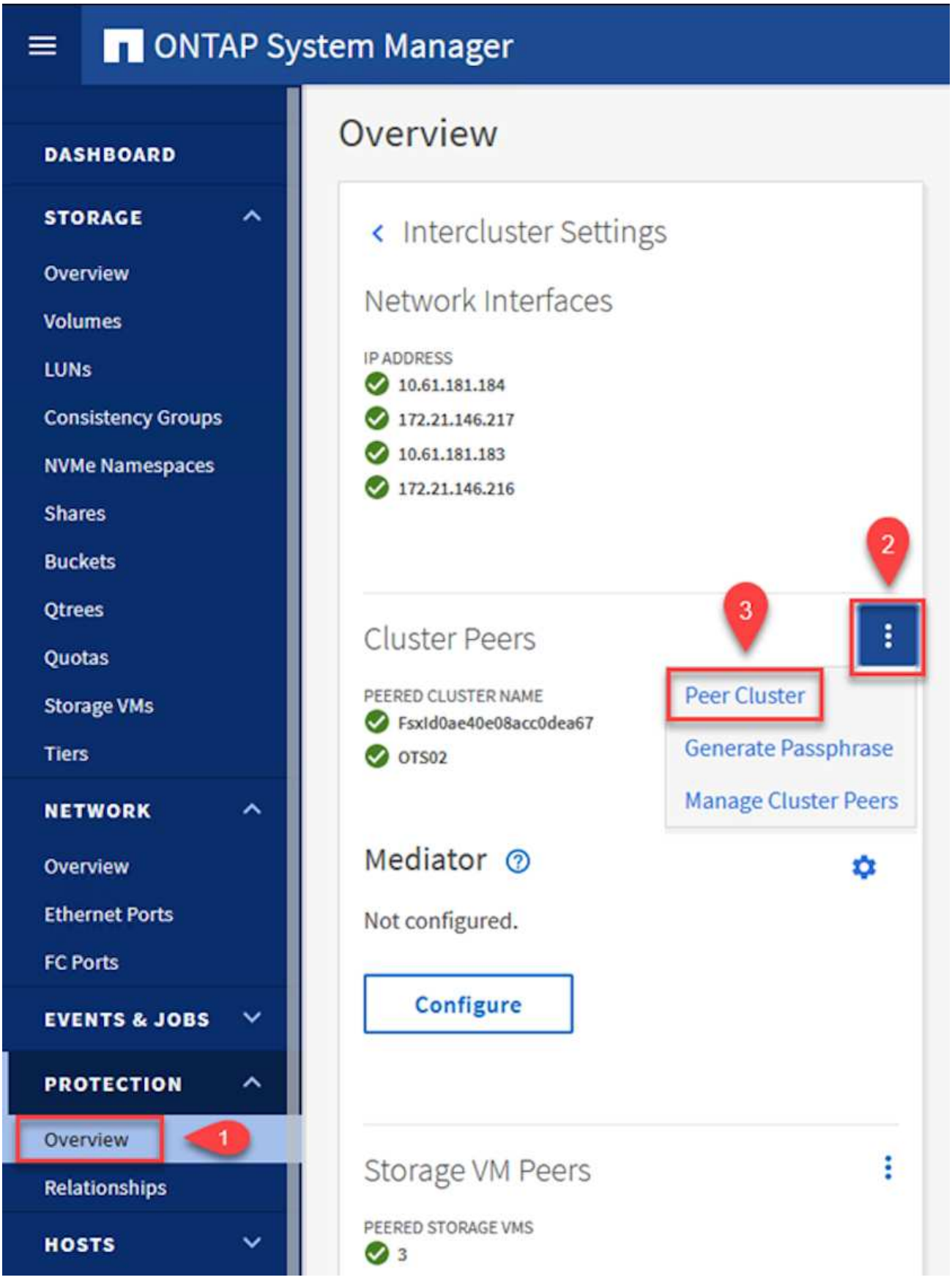
▼ **ONTAP**クラスタ間のクラスタピアリングを確立する

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、他のピア クラスタで確認する必要があります。

1. 宛先ONTAPクラスタでピアリングを設定するには、 `cluster peer create`指示。プロンプトが表示されたら、後でソース クラスターで作成プロセスを完了するために使用する一意のパスフレーズを入力します。

```
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 から、[Protection] > [Overview] に移動し、[Peer Cluster] を選択します。



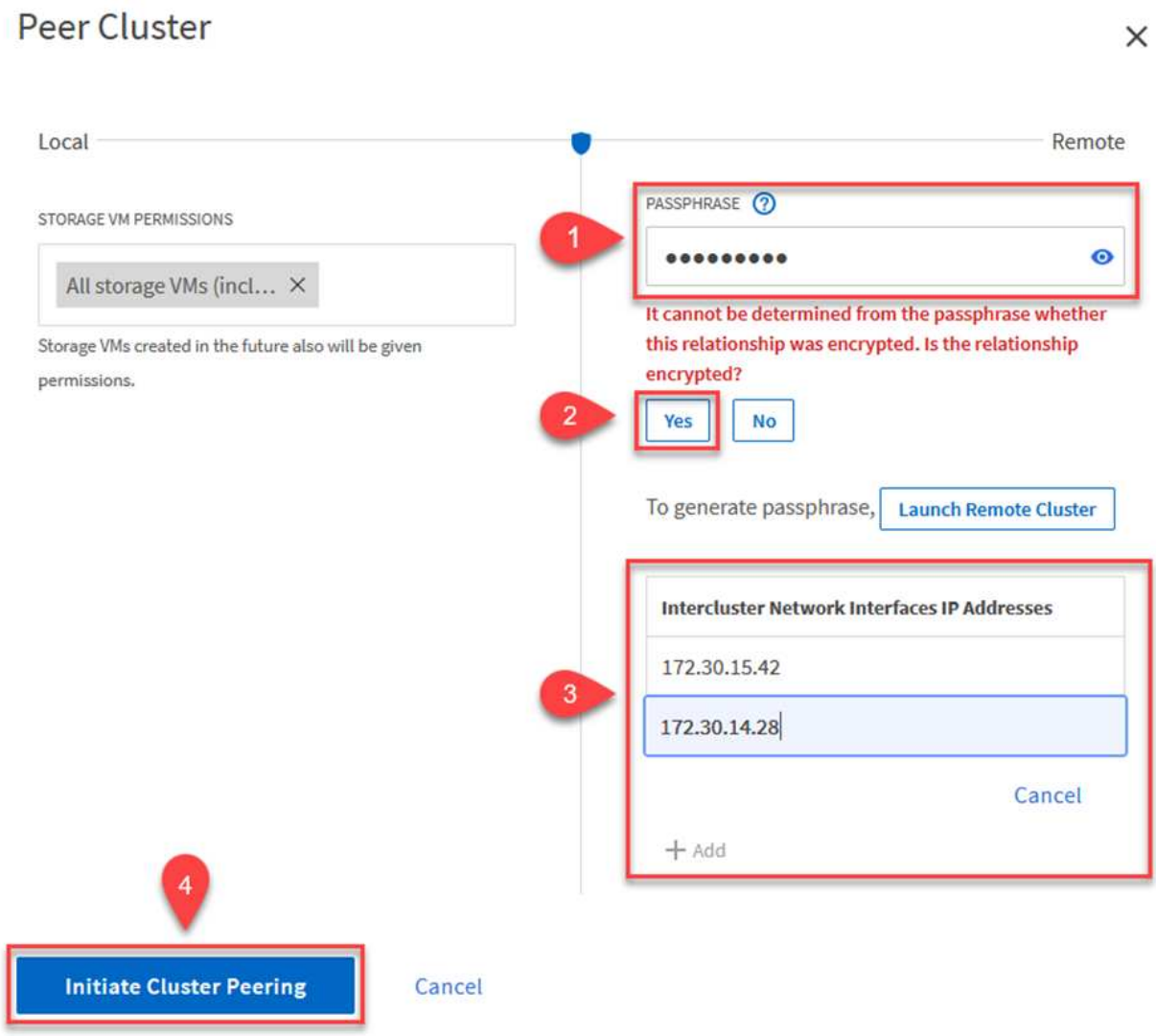
3. [ピア クラスター] ダイアログ ボックスで、必要な情報を入力します。
   a. 宛先ONTAPクラスタでピア クラスタ関係を確立するために使用されたパスフレーズを入力しま

す。

b. 選択 `Yes`暗号化された関係を確立します。

c. 宛先ONTAPクラスタのクラスタ間 LIF IP アドレスを入力します。

d. プロセスを終了するには、「クラスター ピアリングの開始」をクリックします。



4. 次のコマンドを使用して、宛先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**ピアリング関係を確立する

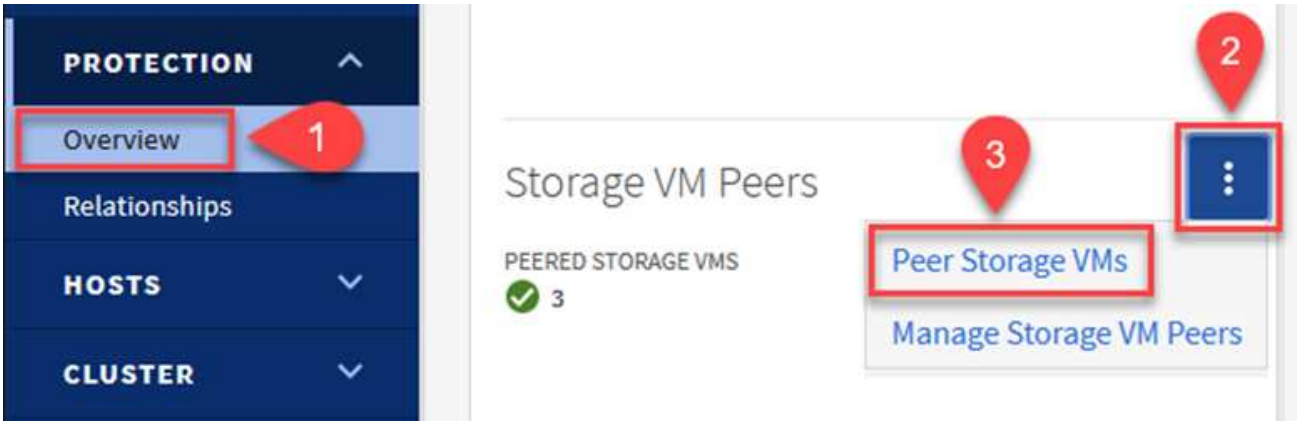
次の手順では、 SnapMirror関係になるボリュームを含む宛先ストレージ仮想マシンとソース ストレージ仮想マシン間の SVM 関係を設定します。

1. 宛先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。

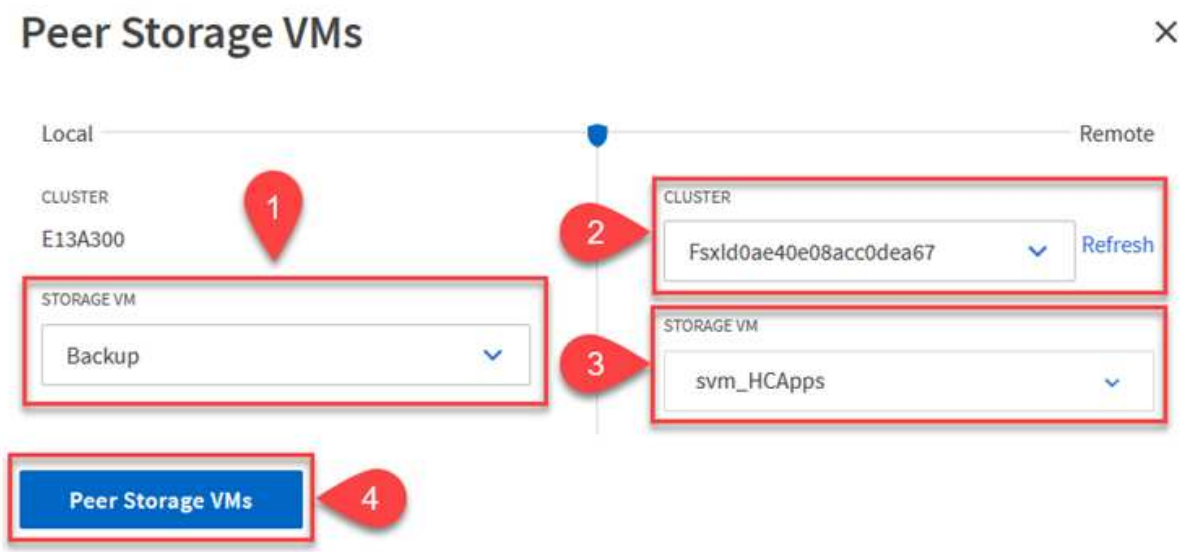
```
ONTAP-Dest::> vserver peer create -vserver DestSVM -peer-vserver
```

```
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. ソースONTAPクラスタから、 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受け入れます。
3. ONTAP System Manager から、[Protection] > [Overview] に移動し、[Storage VM Peers] の下の [Peer Storage VMs] を選択します。



4. ピア ストレージ VM のダイアログ ボックスで、必須フィールドに入力します。
   - ソースストレージVM
   - 宛先クラスター
   - 宛先ストレージVM



5. SVM ピアリング プロセスを完了するには、[ピア ストレージ VM] をクリックします。

▼ スナップショット保持ポリシーを作成する

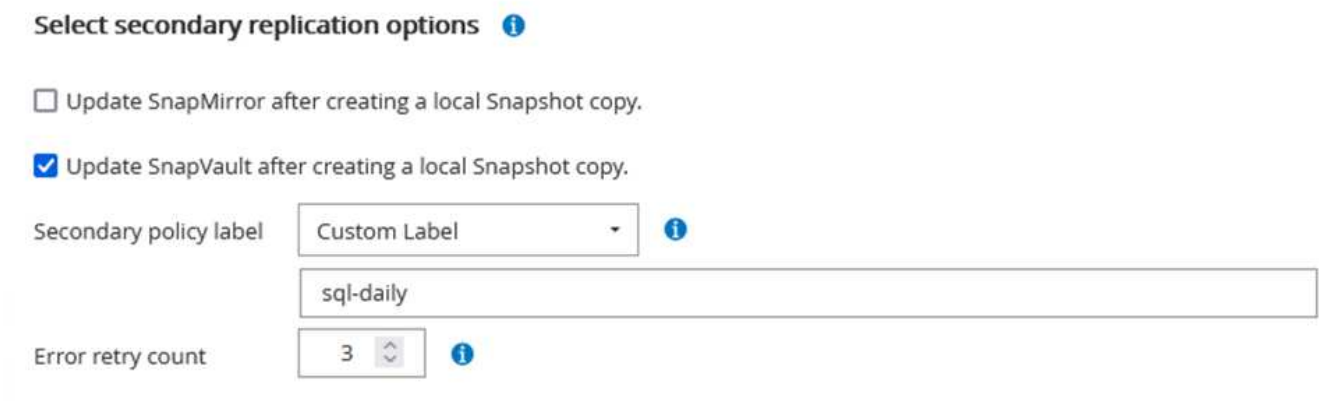
SnapCenter は、プライマリ ストレージ システム上にスナップショット コピーとして存在するバックアップの保持スケジュールを管理します。これは、 SnapCenterでポリシーを作成するときに確立されます。SnapCenter は、セカンダリ ストレージ システムに保持されるバックアップの保持ポリシーを管理しません。これらのポリシーは、セカンダリ FSx クラスター上に作成され、ソース ボリュームとSnapMirror関係

にある宛先ボリュームに関連付けられたSnapMirrorポリシーを通じて個別に管理されます。

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スナップショットのSnapMirrorラベルに追加されるセカンダリ ポリシー ラベルを指定するオプションがあります。

> セカンダリ ストレージでは、これらのラベルは、スナップショットの保持を強制する目的で、宛先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 データベースとログ ボリュームの毎日のバックアップに使用されるポリシーの一部として生成されたすべてのスナップショットに存在するSnapMirrorラベルを示しています。



SQL Serverデータベース用のSnapCenterポリシーの作成の詳細については、 "SnapCenterのドキュメント" 。

まず、保持するスナップショット コピーの数を指定するルールを含むSnapMirrorポリシーを作成する必要があります。

1. FSx クラスターに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ラベルを使用して、ポリシーにルールを追加します。

```
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
```

各SnapMirrorラベルと保持するスナップショットの数 (保持期間) に対して追加のルールを作成します。

▼ 宛先ボリュームを作成する

ソース ボリュームからのスナップショット コピーの受信者となる宛先ボリュームをONTAP上に作成するには、宛先ONTAPクラスター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宛先ボリューム間の**SnapMirror**関係を作成する

ソース ボリュームと宛先ボリュームの間にSnapMirror関係を作成するには、宛先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**関係を初期化する

SnapMirror関係を初期化します。このプロセスは、ソース ボリュームから生成された新しいスナップショットを開始し、それを宛先ボリュームにコピーします。

ボリュームを作成するには、宛先のONTAPクラスター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を構成する

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、Windows および 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。

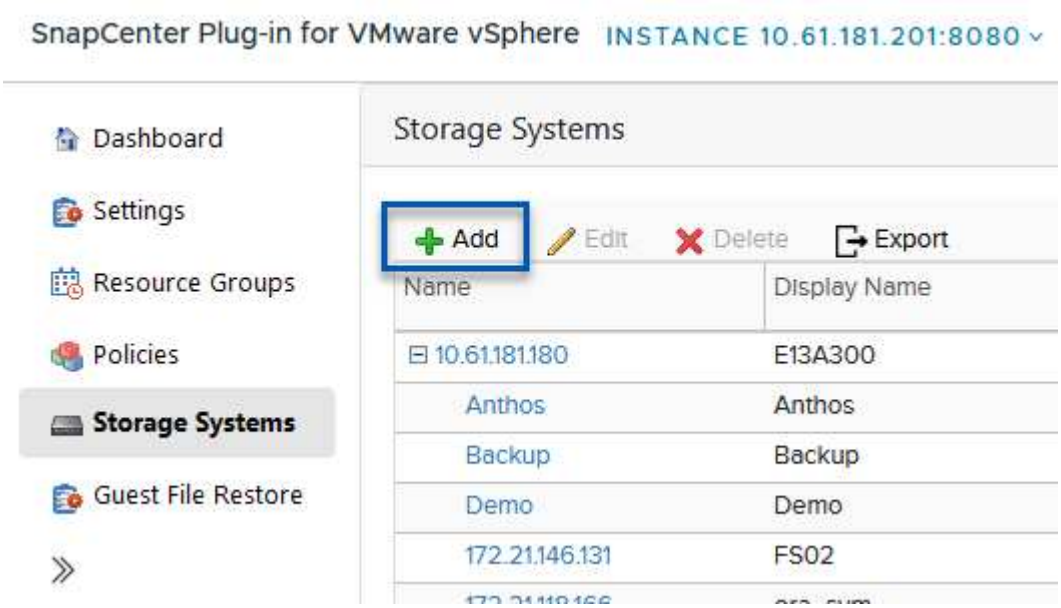
レビュー "データ保護のワークフロー"バックアップの構成手順の詳細については、SCV ドキュメントのセクションを参照してください。

仮想マシンとデータストアのバックアップを構成するには、プラグイン インターフェイスから次の手順を完了する必要があります。

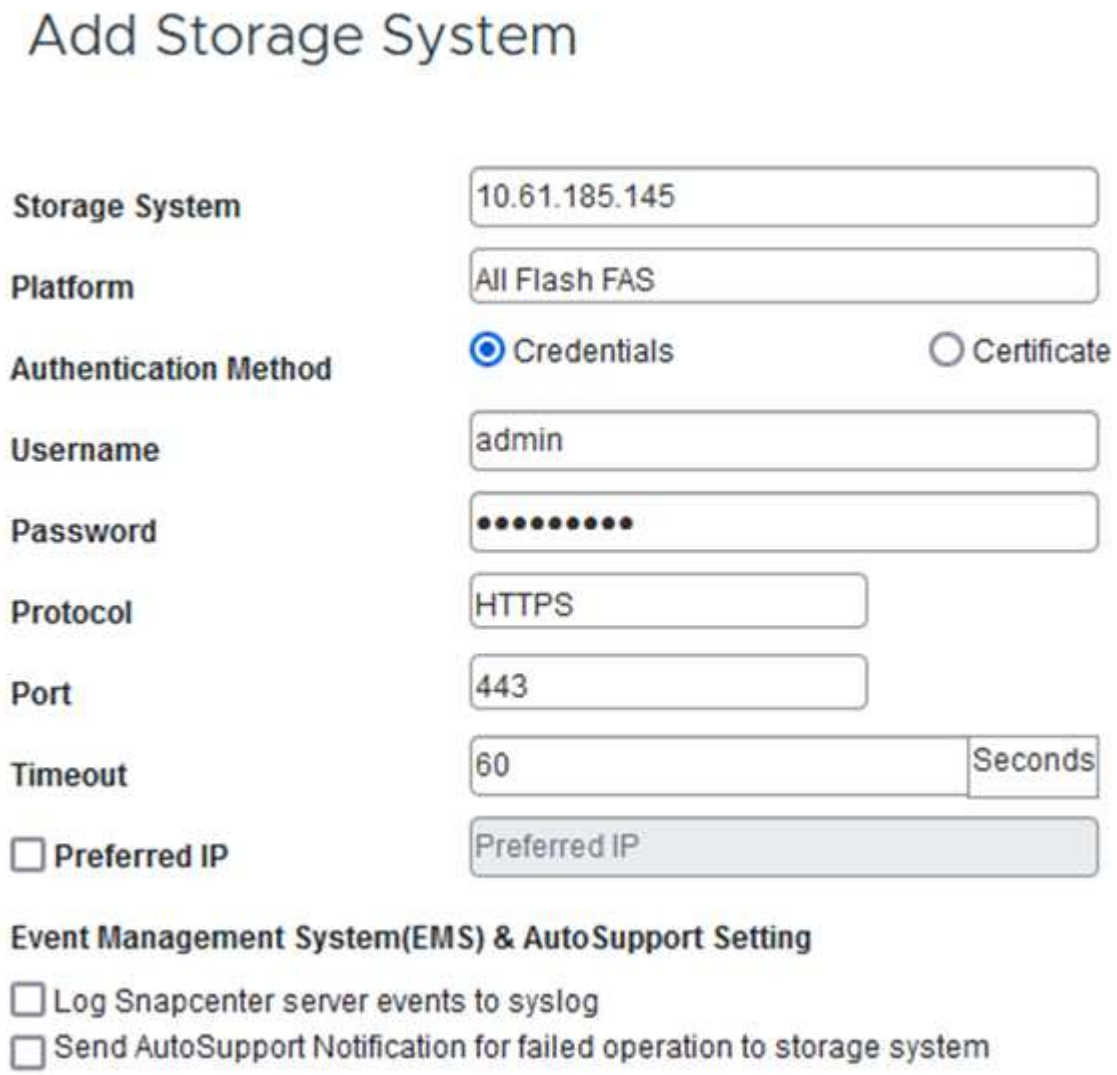
▼ **Discovery ONTAP**ストレージシステム

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されるONTAPストレージ クラスターを検出します。

1. SnapCenter Plug-in for VMware vSphereで、左側のメニューの ストレージ システム 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 システムの資格情報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。

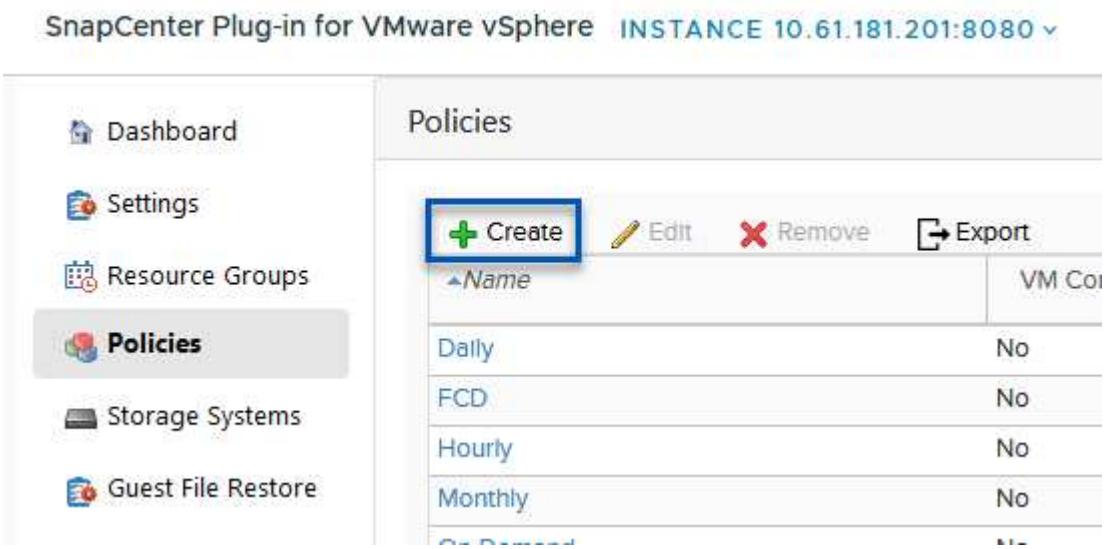
▼ **SCV**バックアップポリシーを作成する

ポリシーは、SCV によって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。

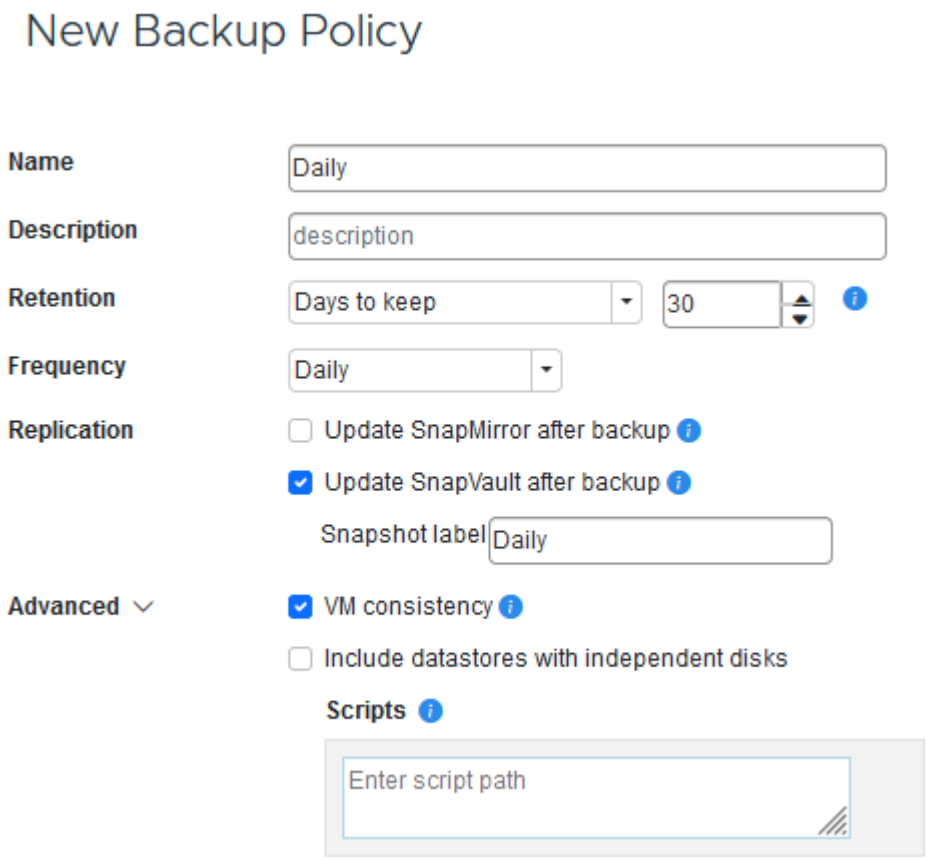
レビュー "VMとデータストアのバックアップ ポリシーの作成"詳細については、ドキュメントのセクションを参照してください。

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 ポリシー に移動し、作成 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、スナップショット ラベルを指定します。



SnapCenterプラグインでポリシーを作成すると、 SnapMirrorとSnapVaultのオプションが表示されます。 SnapMirrorを選択した場合、ポリシーで指定された保持スケジュールはプライマリ スナップショットとセカンダリ スナップショットの両方で同じになります。 SnapVaultを選択した場合、セカンダリ スナップショットの保持スケジュールは、SnapMirror関係で実装された別のスケジュールに基づいて決定されます。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コピーに対して、特定の保持期間を持つポリシーを適用するために使用できるという点で便利です。SCVをNetApp Data Servicesと組み合わせて使用する場合、Snapshotラベルフィールドは空白であるか、バックアップ ポリシーで指定されたラベルと[underline]#一致#している必要があります。

3. 必要なポリシーごとにこの手順を繰り返します。たとえば、毎日、毎週、毎月のバックアップに個別のポリシーを設定します。

▼ リソース グループの作成

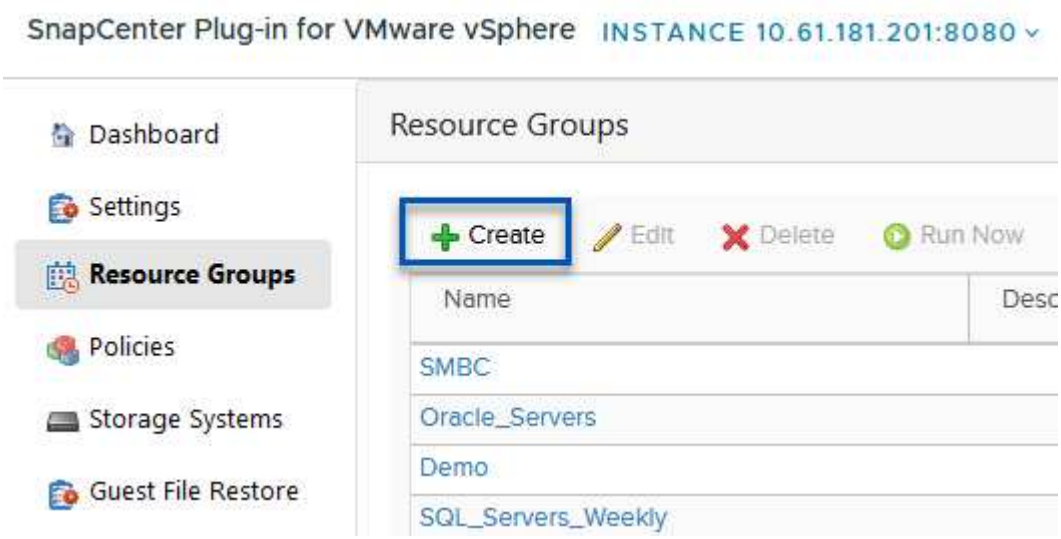
リソース グループには、バックアップ ジョブに含めるデータストアと仮想マシン、および関連するポリシーとバックアップ スケジュールが含まれます。

レビュー "リソース グループの作成"詳細については、ドキュメントのセクションを参照してください。

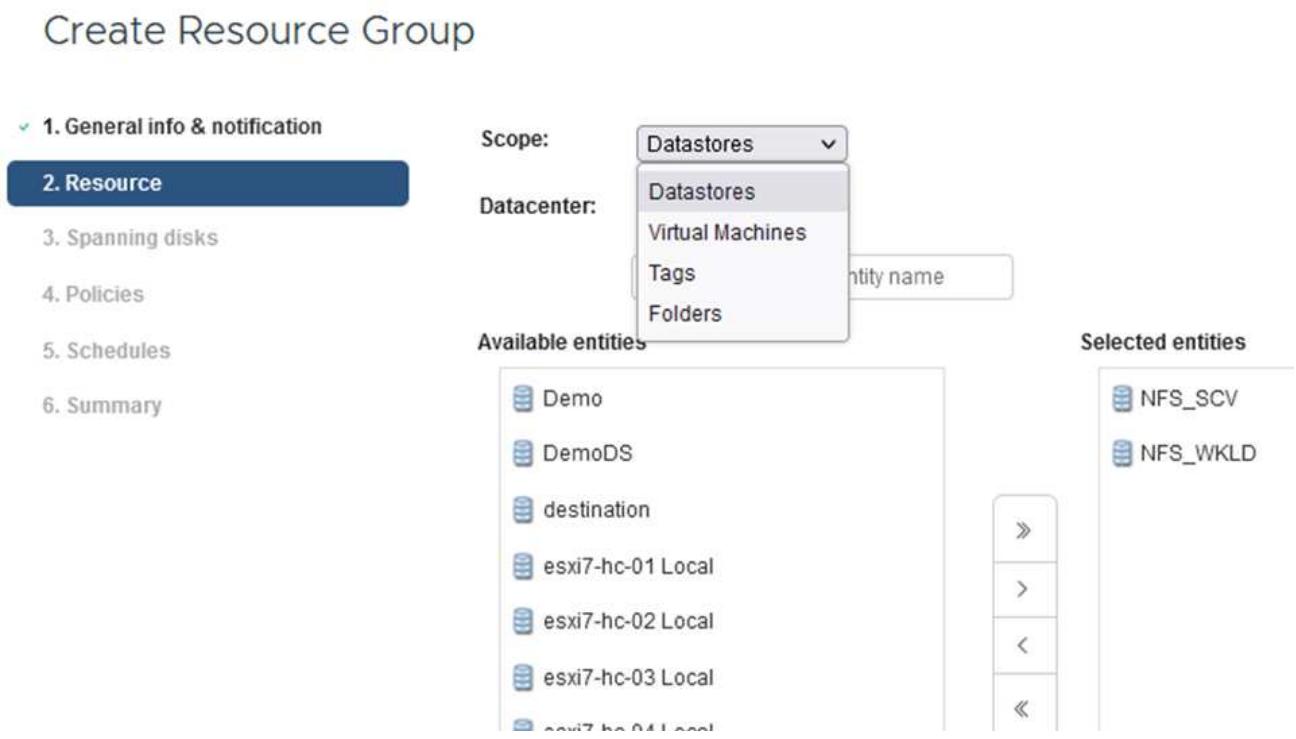
リソース グループを作成するには、次の手順を実行します。

1. SnapCenter Plug-in for VMware vSphereで、左側のメニューの リソース グループ に移動し、作成 ボ

タンをクリックします。

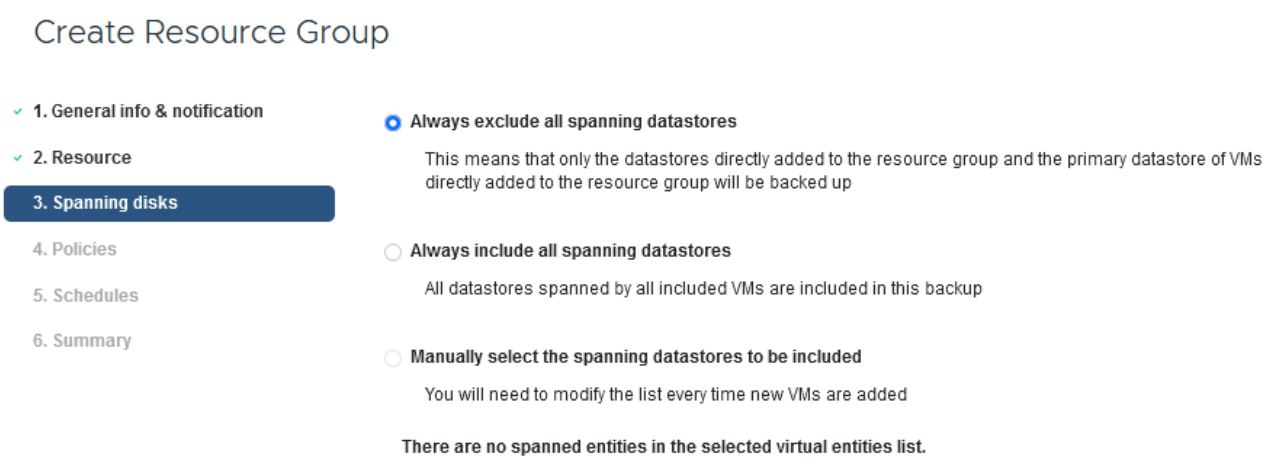


2. リソース グループの作成ウィザードで、グループの名前と説明、および通知を受信するために必要な情報を入力します。 「次へ」をクリックします
3. 次のページで、バックアップ ジョブに含めるデータストアと仮想マシンを選択し、[次へ] をクリックします。



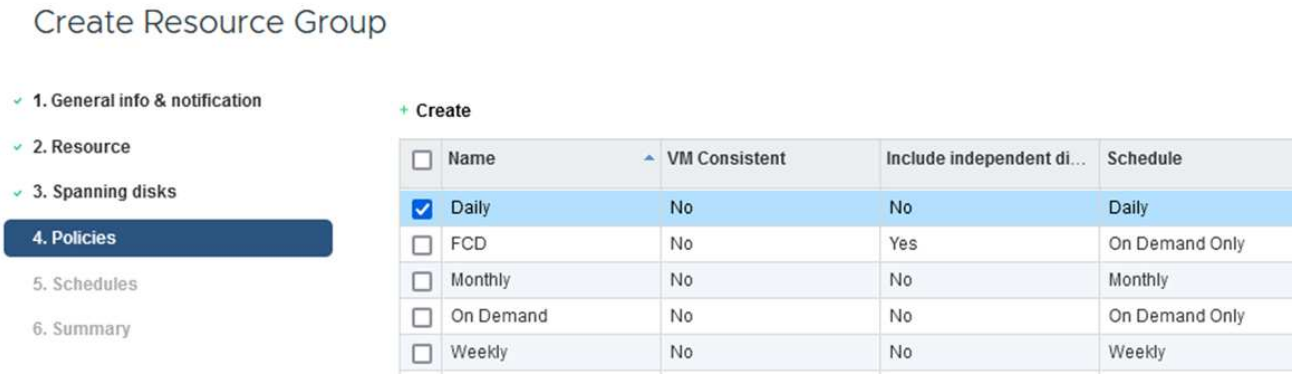
特定の VM またはデータストア全体を選択するオプションがあります。どちらを選択した場合でも、バックアップは基礎となるボリュームのスナップショットを取得した結果であるため、ボリューム全体 (およびデータストア) がバックアップされます。ほとんどの場合、データストア全体を選択するのが最も簡単です。ただし、復元時に使用可能な VM のリストを制限する場合は、バックアップ対象として VM のサブセットのみを選択できます。

4. 複数のデータストアに存在する VMDK を持つ VM のデータストアをまたぐためのオプションを選択し、[次へ] をクリックします。



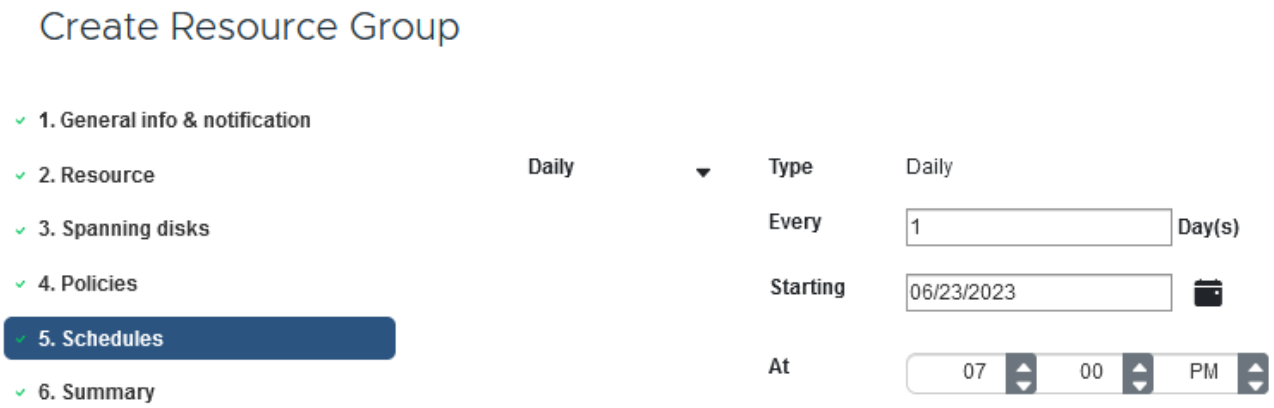
VMwareワークロードを保護するBackup and Recoveryは、現在、複数のデータストアにまたがるVMDKを持つVMのバックアップをサポートしていません。

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。



Backup and Recoveryを使用してSCV管理スナップショットをオブジェクトストレージにバックアップする場合、各リソースグループには1つのポリシーのみを関連付けることができます。

6. バックアップが実行され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。

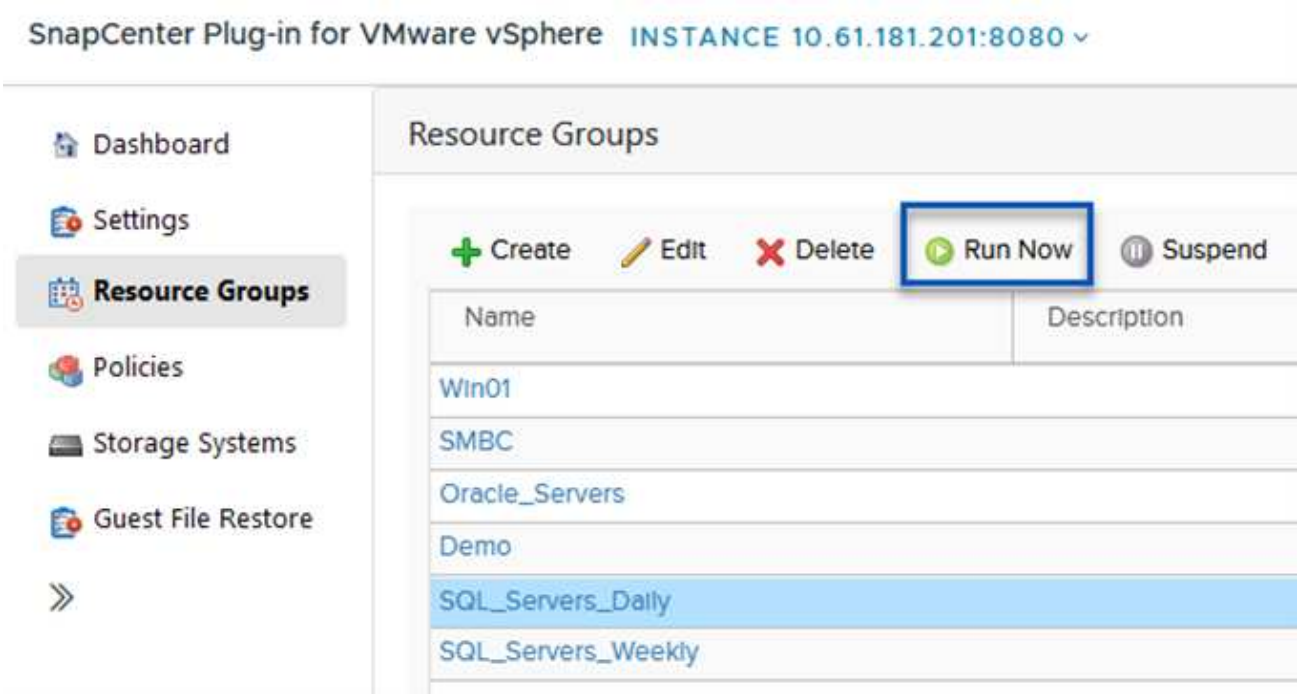


7. 最後に、概要ページを確認し、[完了] をクリックしてリソース グループの作成を完了します。

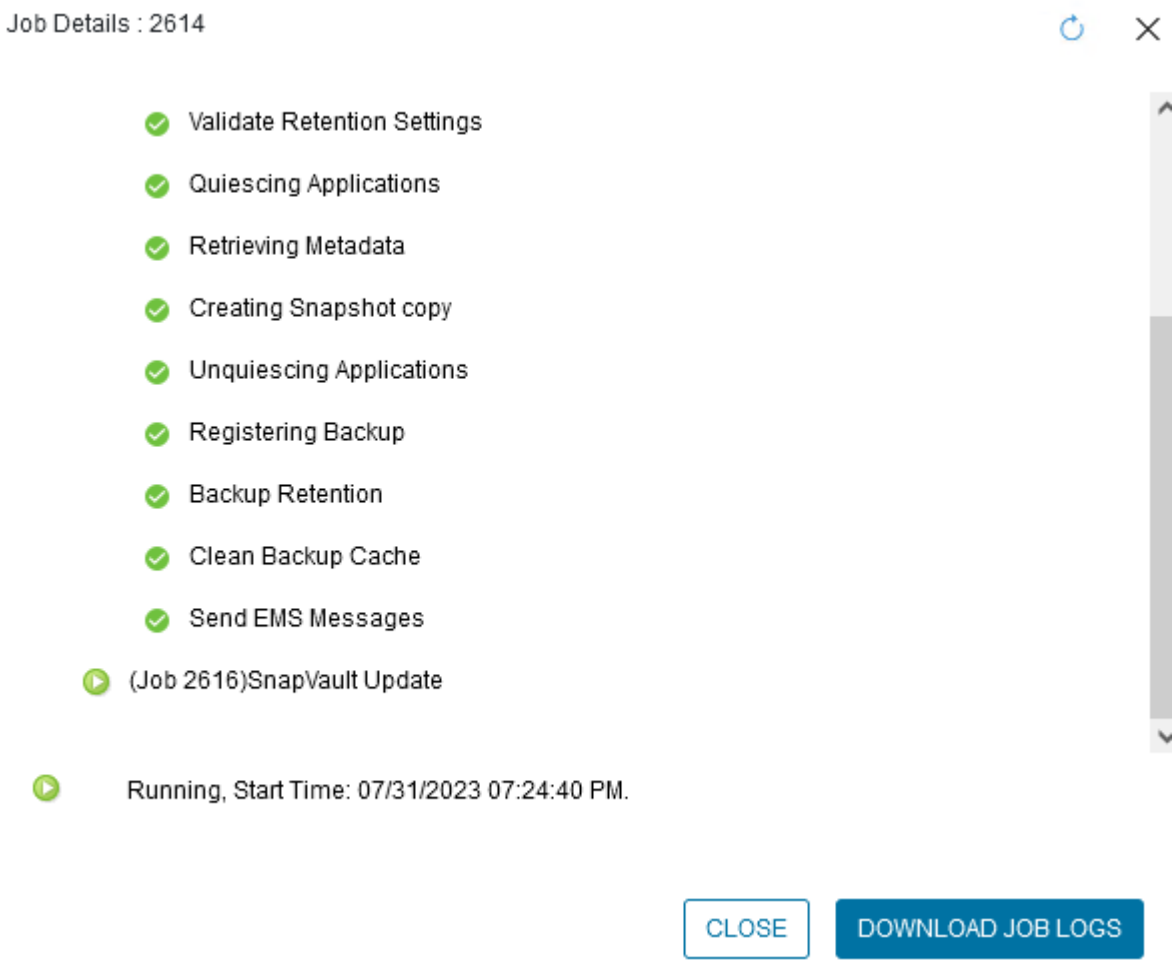
▼ バックアップジョブを実行する

最後のステップとして、バックアップジョブを実行し、その進行状況を監視してください。SCV で少なくとも 1 つのバックアップ ジョブが正常に完了してからでないと、NetApp Console からリソースを検出できません。

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。 最近のジョブ アクティビティ の下でジョブ ID 番号をクリックして、ジョブの進行状況を監視します。



NetApp Consoleでオブジェクトストレージへのバックアップを構成する

NetApp Consoleがデータインフラを効果的に管理するには、事前にConsoleエージェントをインストールする必要があります。Consoleエージェントは、リソースの検出とデータ処理の管理に関連するアクションを実行します。

Consoleエージェントの詳細については、NetApp Consoleドキュメントの "コンソールエージェントについて学ぶ"を参照してください。

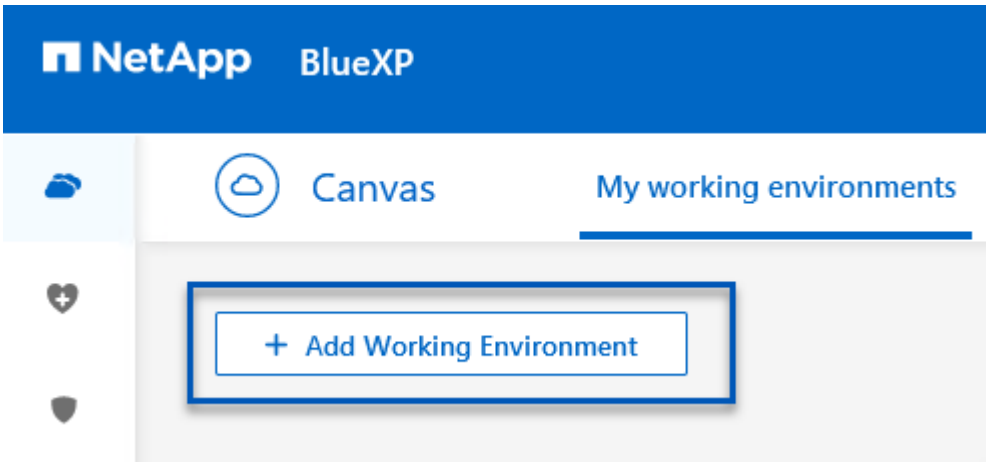
利用中のクラウド プロバイダにエージェントがインストールされると、オブジェクト ストレージのグラフィック表示がシステムから閲覧可能になります。

オンプレミスのSCVで管理されているデータをバックアップするようにBackup and Recoveryを設定するには、以下の手順を実行します：

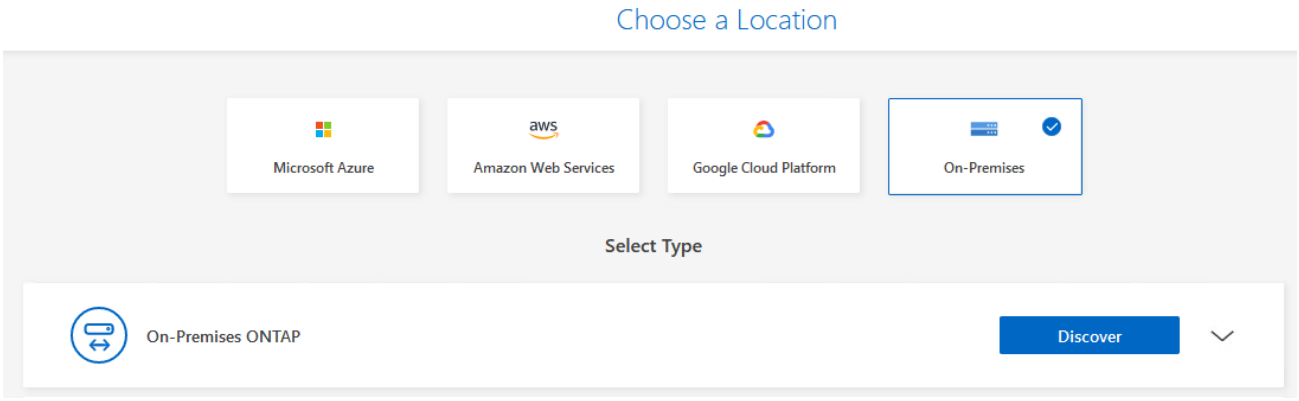
▼ **ONTAP**ストレージシステムをシステムに追加

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NetApp Consoleに追加することです。

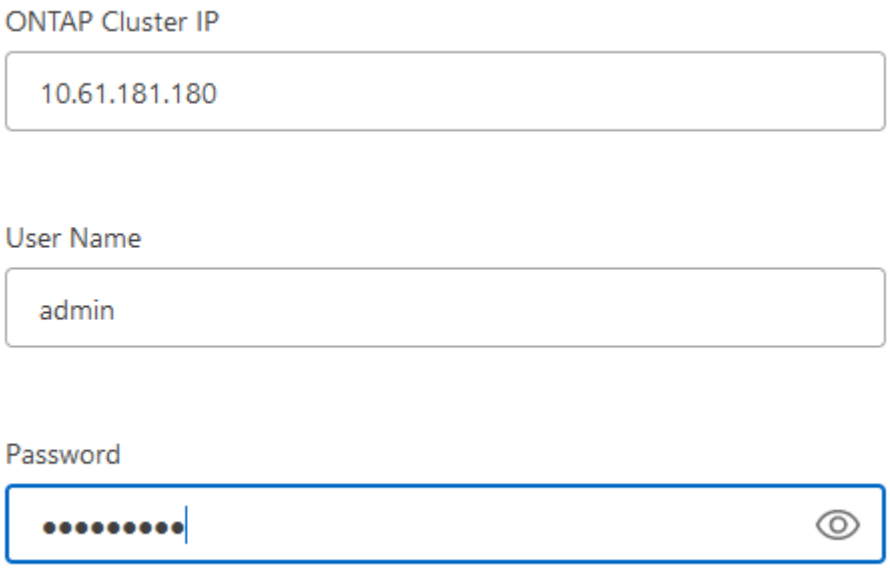
1. システムから **+**追加 をクリックして開始します。



2. 場所の選択肢から「オンプレミス」を選択し、「検出」ボタンをクリックします。



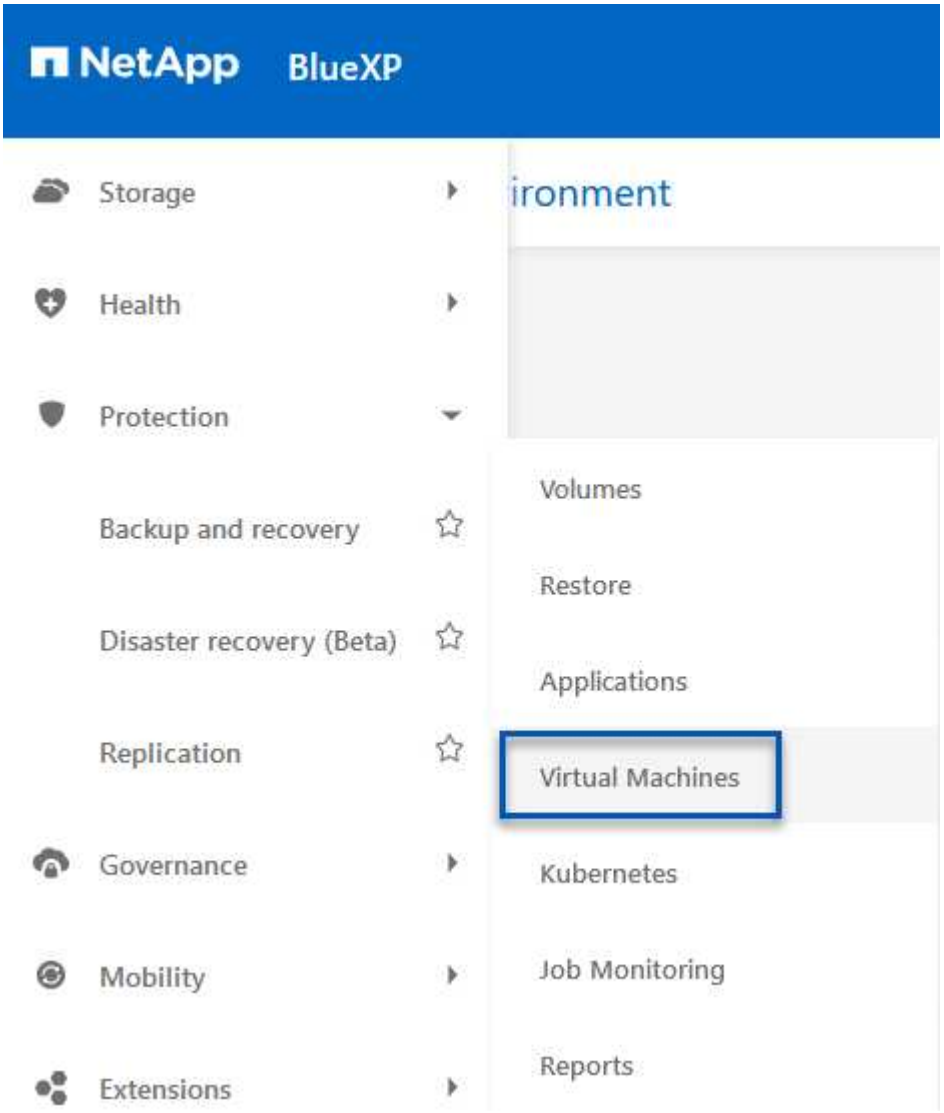
3. ONTAPストレージ システムの資格情報を入力し、[検出] ボタンをクリックして作業環境を追加します。



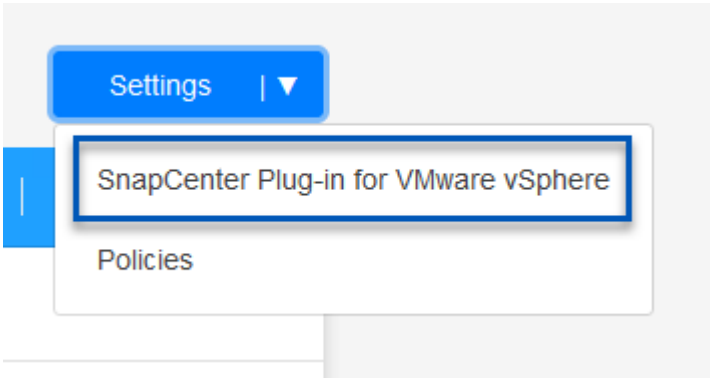
▼ オンプレミスの **SCV** アプライアンスと **vCenter** の検出

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資格情報を追加します。

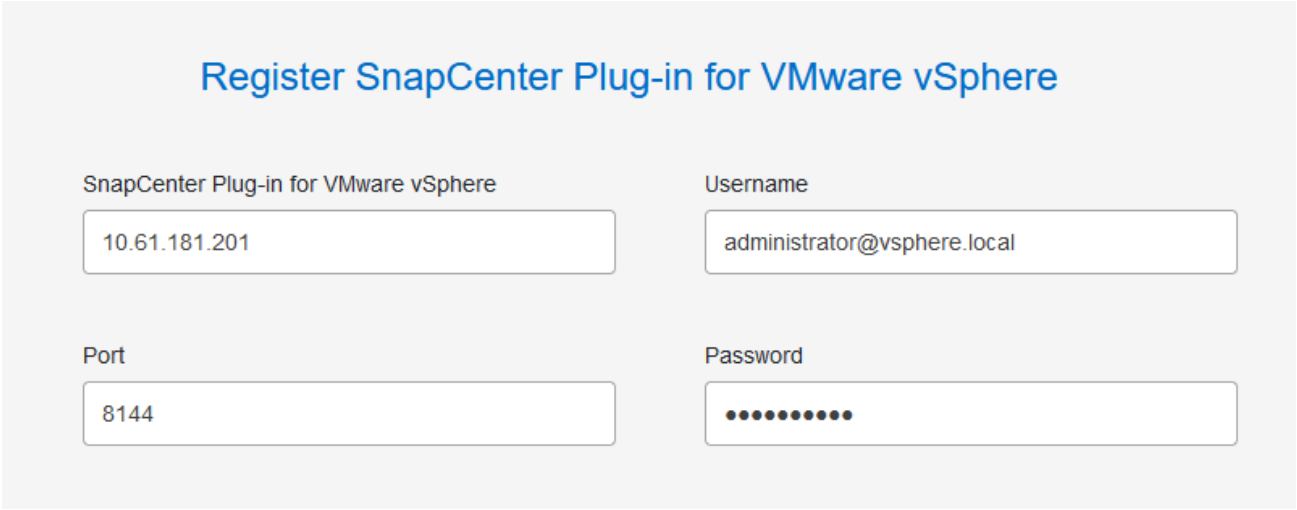
1. NetApp Consoleの左側のメニューから、*保護 > バックアップとリカバリ > ワークロード >VMware*を選択します。



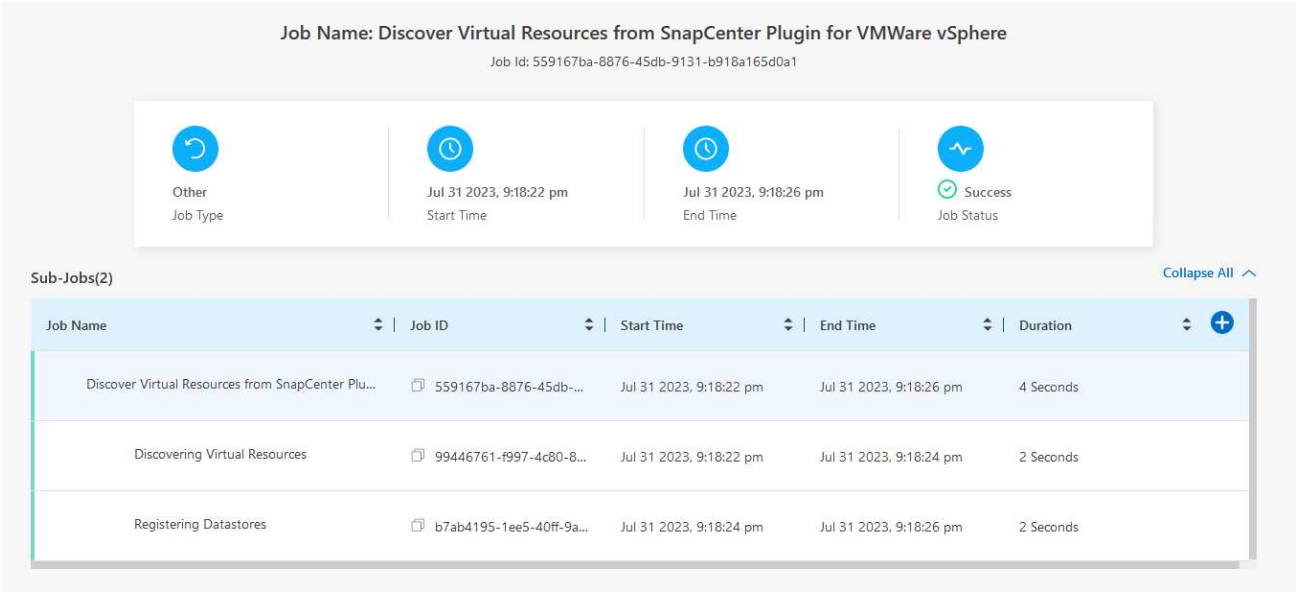
2. 仮想マシンのメイン画面から [設定] ドロップダウン メニューにアクセスし、[SnapCenter Plug-in for VMware vSphere] を選択します。



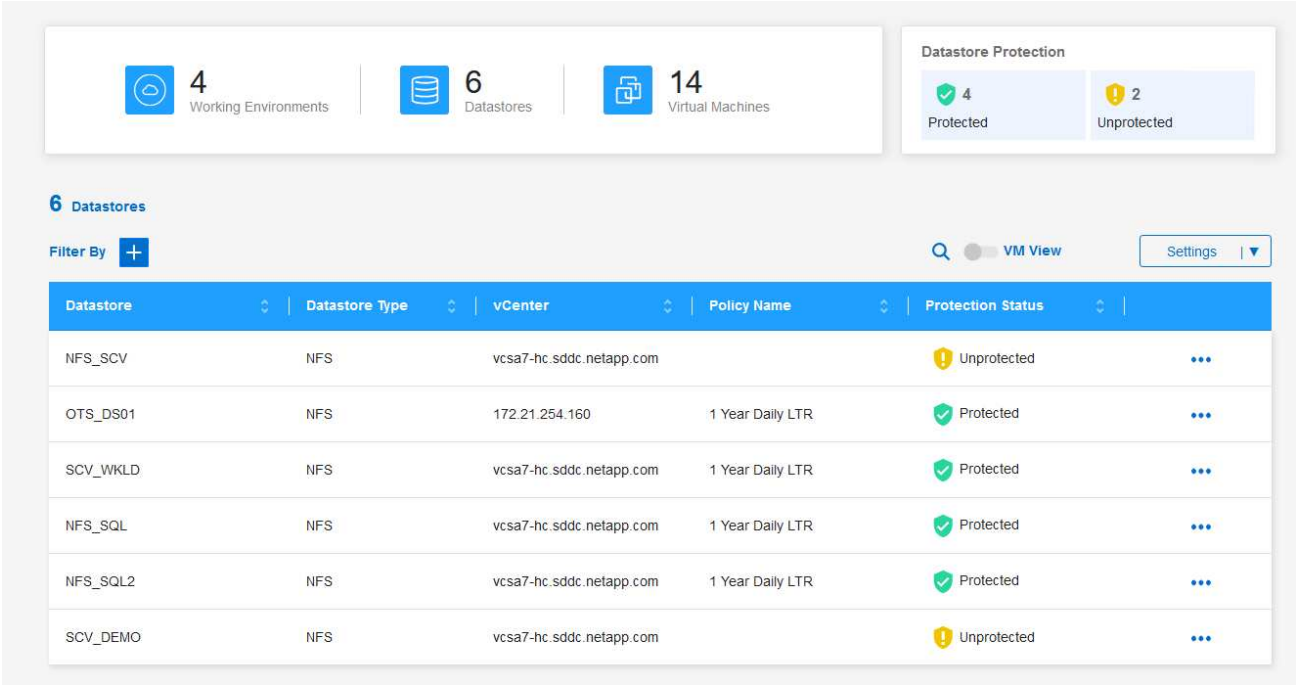
3. 登録 ボタンをクリックし、 SnapCenterプラグイン アプライアンスの IP アドレスとポート番号、および vCenter 管理アプライアンスのユーザー名とパスワードを入力します。検出プロセスを開始するには、[登録] ボタンをクリックします。



4. ジョブの進行状況は、「ジョブ監視」タブから監視できます。



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。

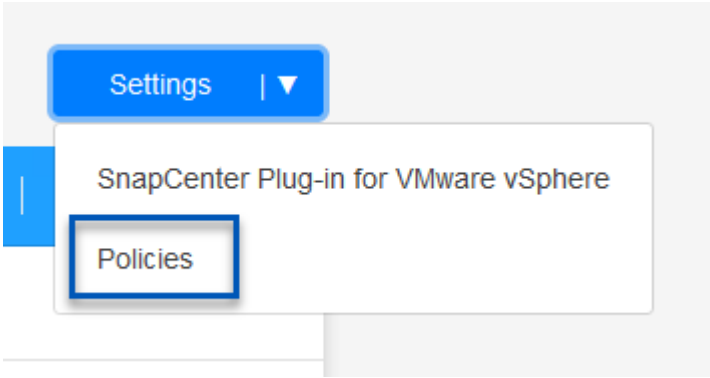


▼ バックアップ ポリシーの作成

仮想マシン向けNetApp Backup and Recoveryでは、保持期間、バックアップ元、アーカイブポリシーを指定するポリシーを作成します。

保護グループの作成の詳細については、 "保護グループを作成する"を参照してください。

1. NetApp Backup and Recovery for Virtual Machinesのメイン ページから、*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。



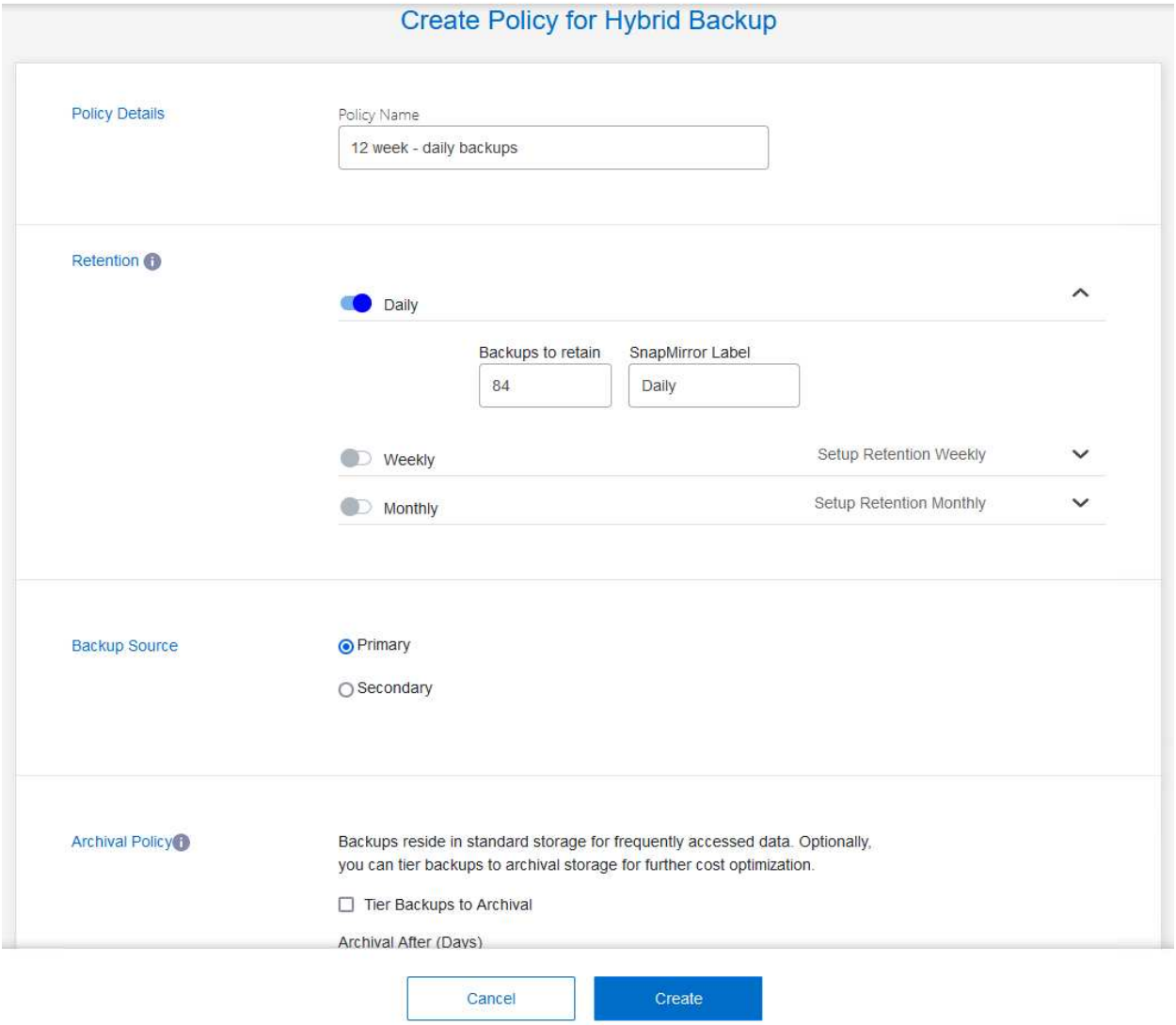
2. ポリシーの作成 をクリックして、ハイブリッド バックアップのポリシーの作成 ウィンドウにアクセスします。

   a. ポリシーの名前を追加する

   b. 希望する保存期間を選択してください

   c. バックアップをプライマリまたはセカンダリのオンプレミスONTAPストレージ システムから取得するかどうかを選択します。

   d. オプションで、追加のコスト削減のために、どのくらいの期間後にバックアップがアーカイブ ストレージに階層化されるかを指定します。



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の SCV ポリシーのラベル名と一致する必要があります。

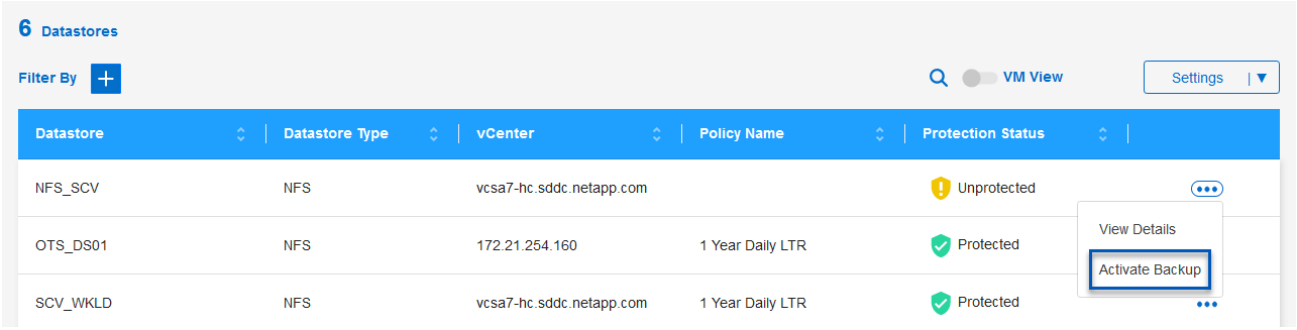
3. *作成*をクリックしてポリシーの作成を完了します。

▼ **Amazon Web Services** へのデータストアのバックアップ

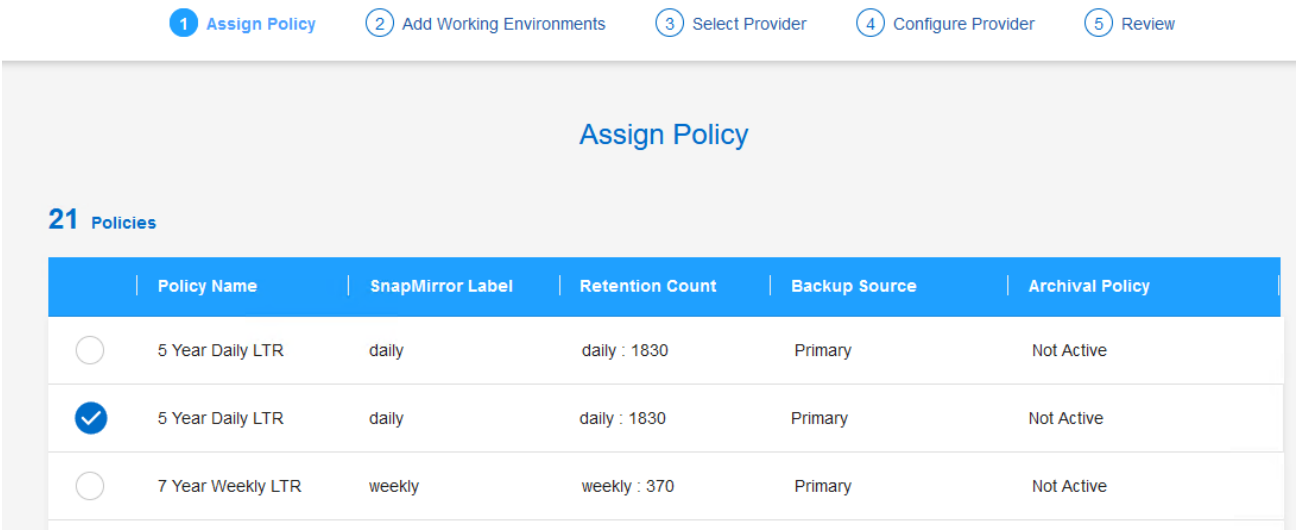
最後のステップは、個々のデータストアと仮想マシンのデータ保護を有効にすることです。次の手順では、AWS へのバックアップをアクティブ化する方法を説明します。

詳細については、 "VMwareワークロードをバックアップする"を参照してください。

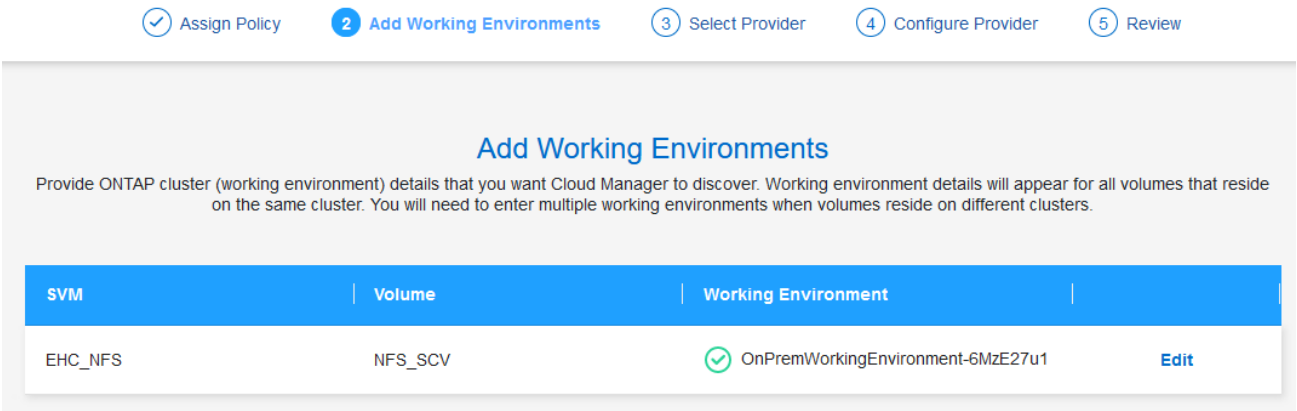
1. NetApp Backup and Recovery for Virtual Machinesのメイン ページから、バックアップするデータストアの設定ドロップダウンにアクセスし、*Activate Backup*を選択します。



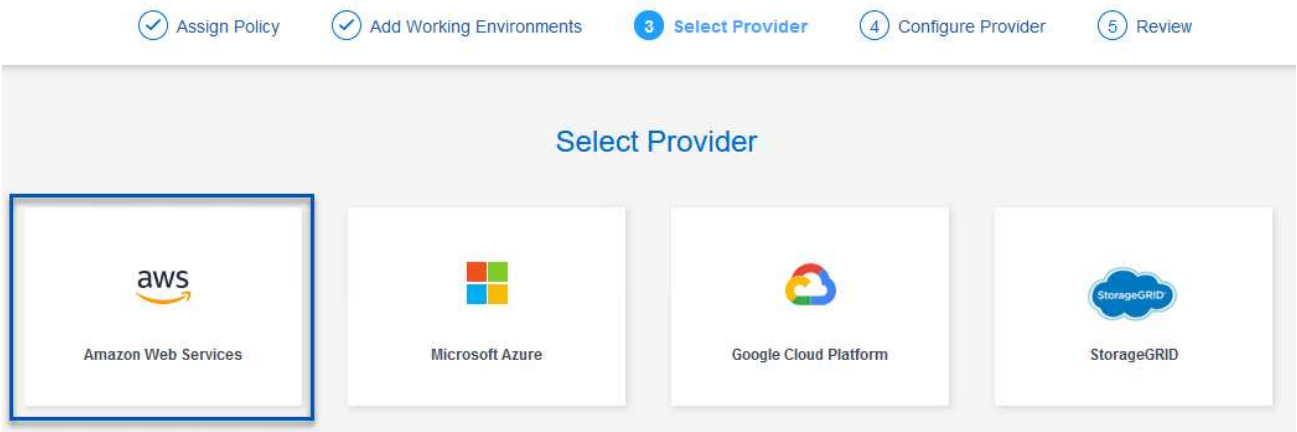
2. データ保護操作に使用するポリシーを割り当て、[次へ] をクリックします。



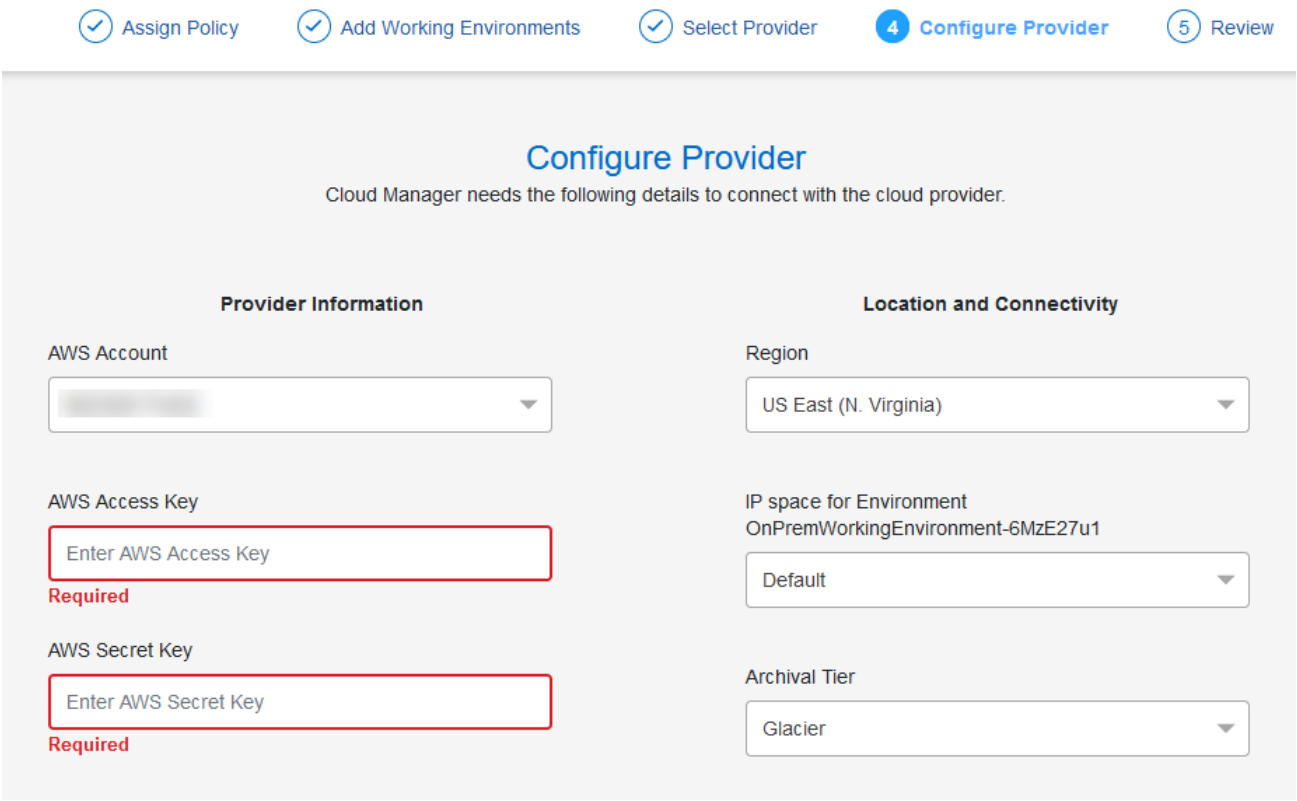
3. 作業環境が以前に検出されている場合は、「作業環境の追加」ページに、チェックマークが付いたデータストアと作業環境が表示されます。作業環境が以前に検出されていない場合は、ここで追加できます。続行するには、[次へ] をクリックします。



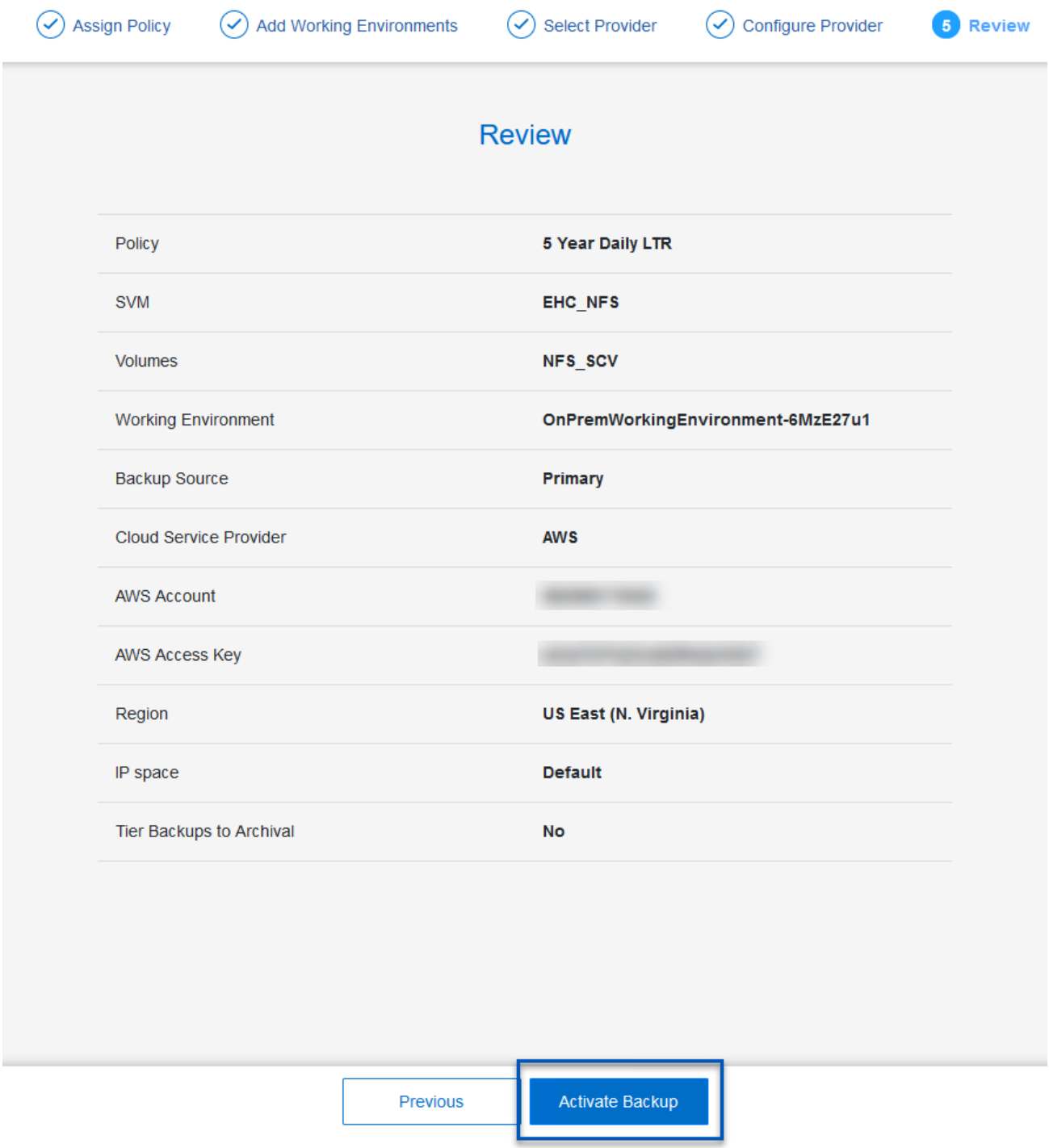
4. *プロバイダーの選択*ページでAWSをクリックし、*次へ*ボタンをクリックして続行します。



5. 使用する 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、AWS のプロバイダー固有の認証情報を入力します。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、[バックアップのアクティブ化] 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。NetApp Backup and Recoveryは、1時間ごとに未完了のスナップショットをスキャンし、オブジェクトストレージに転送します。

データ損失の場合の仮想マシンの復元

データの安全を確保することは、包括的なデータ保護の 1 つの側面にすぎません。同様に重要なのは、データの損失やランサムウェア攻撃が発生した場合に、どこからでも迅速にデータを復元できる機能です。この機能は、シームレスなビジネス運用を維持し、リカバリポイント目標を達成するために不可欠です。

NetApp は、適応性に優れた 3-2-1 戦略を提供し、プライマリ、セカンダリ、およびオブジェクト ストレージ

の場所で保持スケジュールをカスタマイズして制御できます。この戦略により、データ保護のアプローチを特定のニーズに合わせて柔軟にカスタマイズできるようになります。

このセクションでは、仮想マシン向けのSnapCenter Plug-in for VMware vSphereとNetApp Backup and Recoveryの両方からのデータ復元プロセスの概要を説明します。

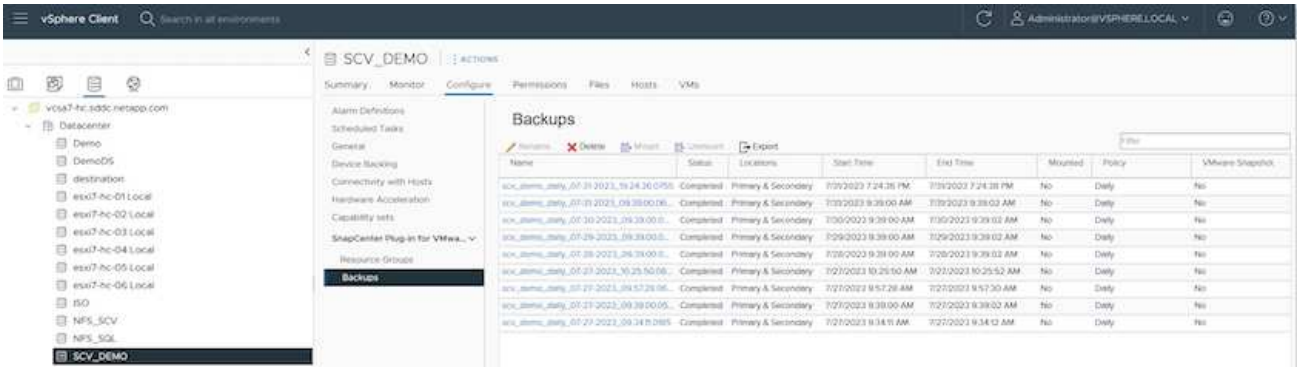
SnapCenter Plug-in for VMware vSphereからの仮想マシンの復元

このソリューションでは、仮想マシンが元の場所と別の場所に復元されました。このソリューションでは、SCV のデータ復元機能のすべての側面がカバーされるわけではありません。 SCVが提供するすべての詳細情報については、 "バックアップからのVMのリストア"製品ドキュメントに記載されています。

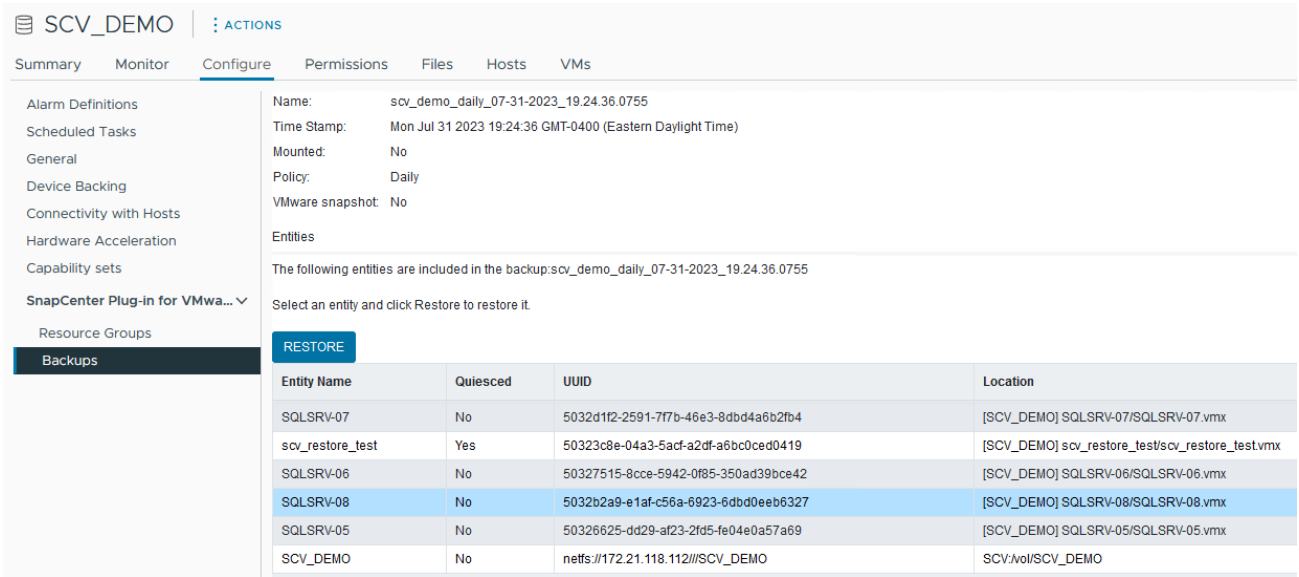
▼ SCVから仮想マシンを復元する

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復元するには、次の手順を実行します。

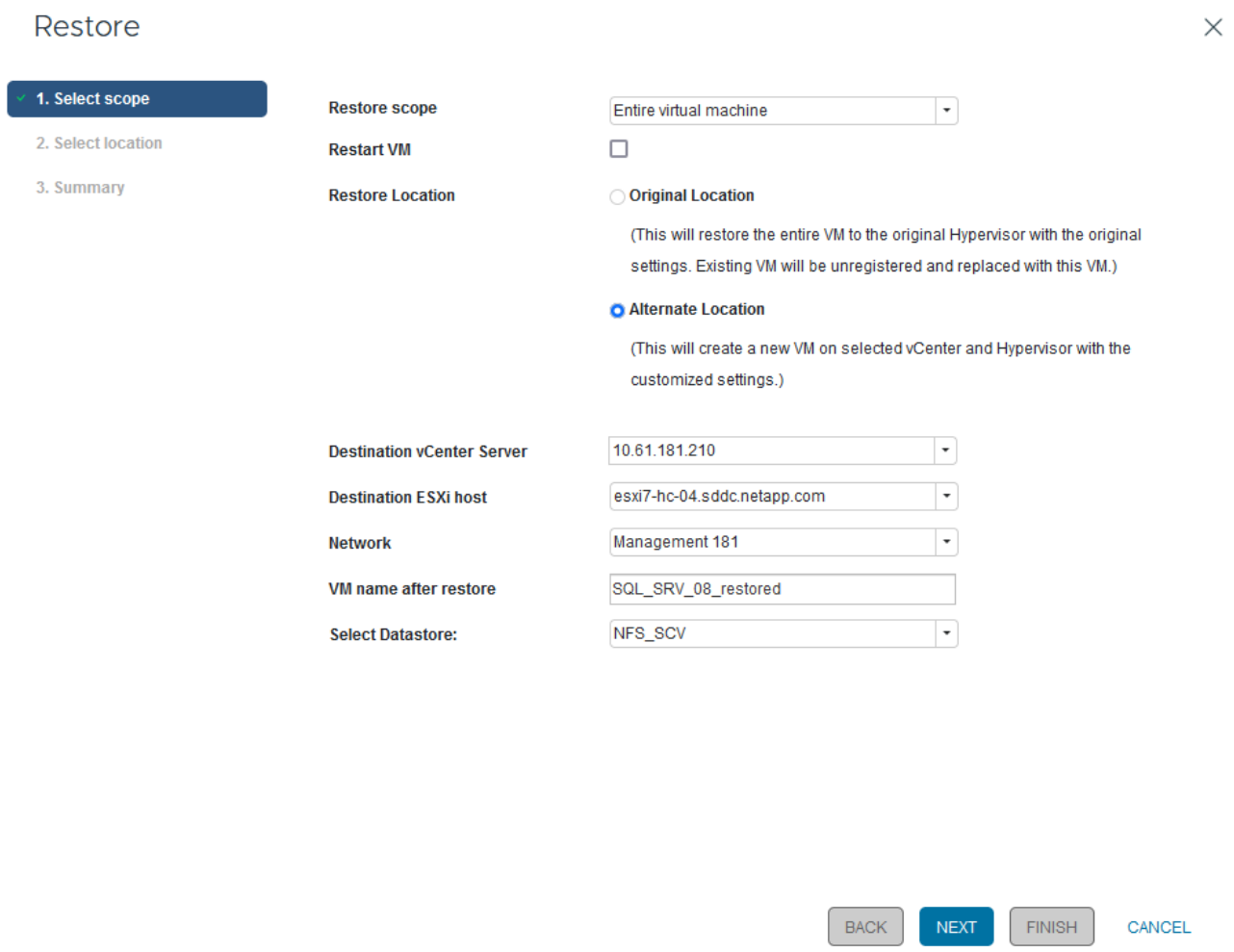
1. vCenter クライアントから インベントリ > ストレージ に移動し、復元する仮想マシンが含まれているデータストアをクリックします。
2. 構成 タブから バックアップ をクリックして、利用可能なバックアップのリストにアクセスします。



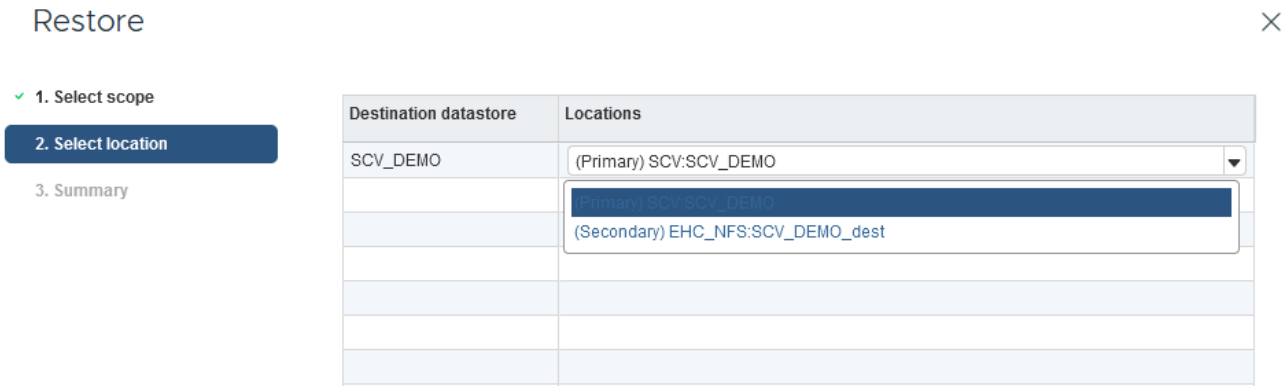
3. バックアップをクリックして VM のリストにアクセスし、復元する VM を選択します。 *復元*をクリックします。



4. 復元ウィザードから、仮想マシン全体を復元するか、特定の VMDK を復元するかを選択します。元の場所または別の場所にインストールすることを選択し、復元後の VM 名と宛先データストアを指定します。*次へ*をクリックします。



5. プライマリまたはセカンダリのストレージ場所からバックアップすることを選択します。



6. 最後に、バックアップ ジョブの概要を確認し、「完了」をクリックして復元プロセスを開始します。

NetApp Backup and Recovery for Virtual Machinesからの仮想マシンの復元

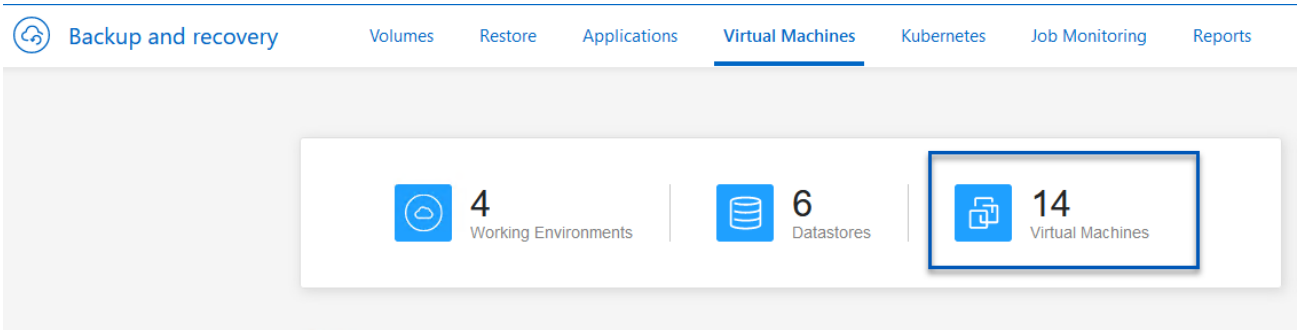
NetApp Backup and Recovery for Virtual Machinesを使用すると、仮想マシンを元の場所に復元できます。復元機能には、NetApp Backup and Recovery Webコンソールからアクセスします。

詳細については、 "クラウドから仮想マシンのデータを復元する"を参照してください。

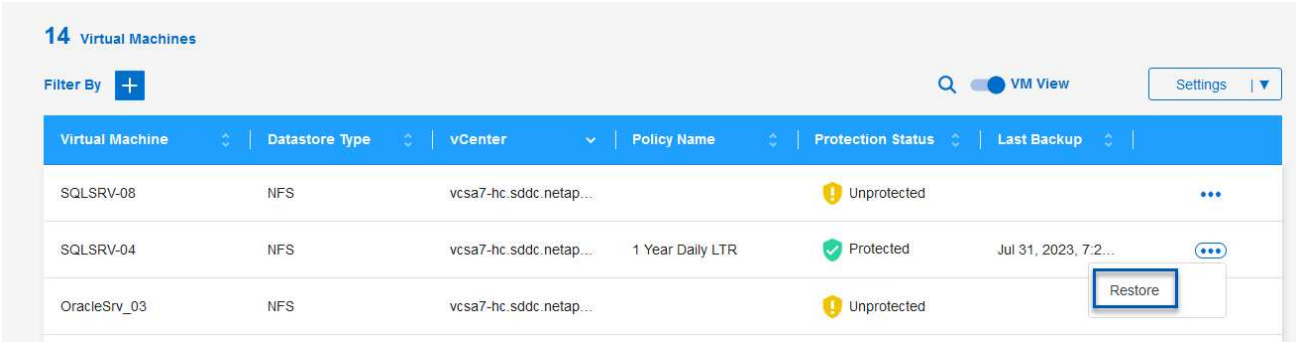
▼ NetApp Backup and Recoveryから仮想マシンを復元する

NetApp Backup and Recoveryから仮想マシンを復元するには、次の手順を実行します。

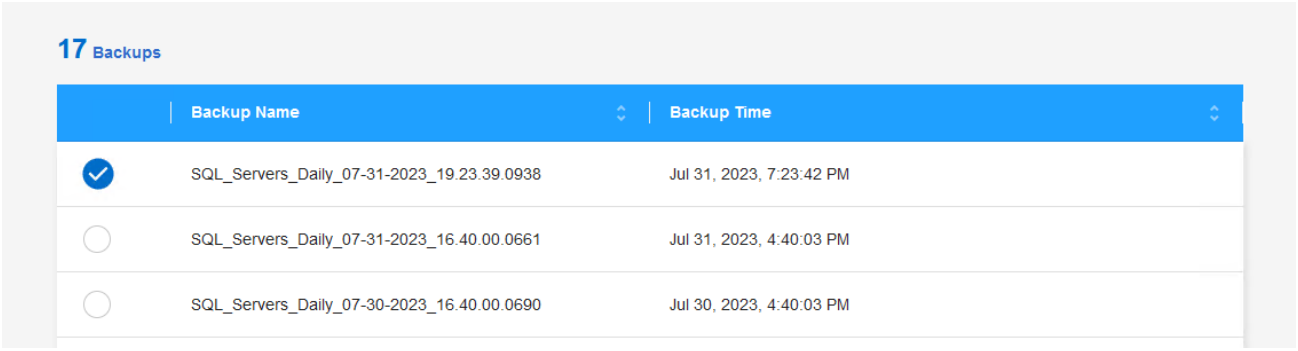
1. 保護 > バックアップとリカバリ > 仮想マシン に移動し、仮想マシンをクリックして、復元可能な仮想マシンのリストを表示します。



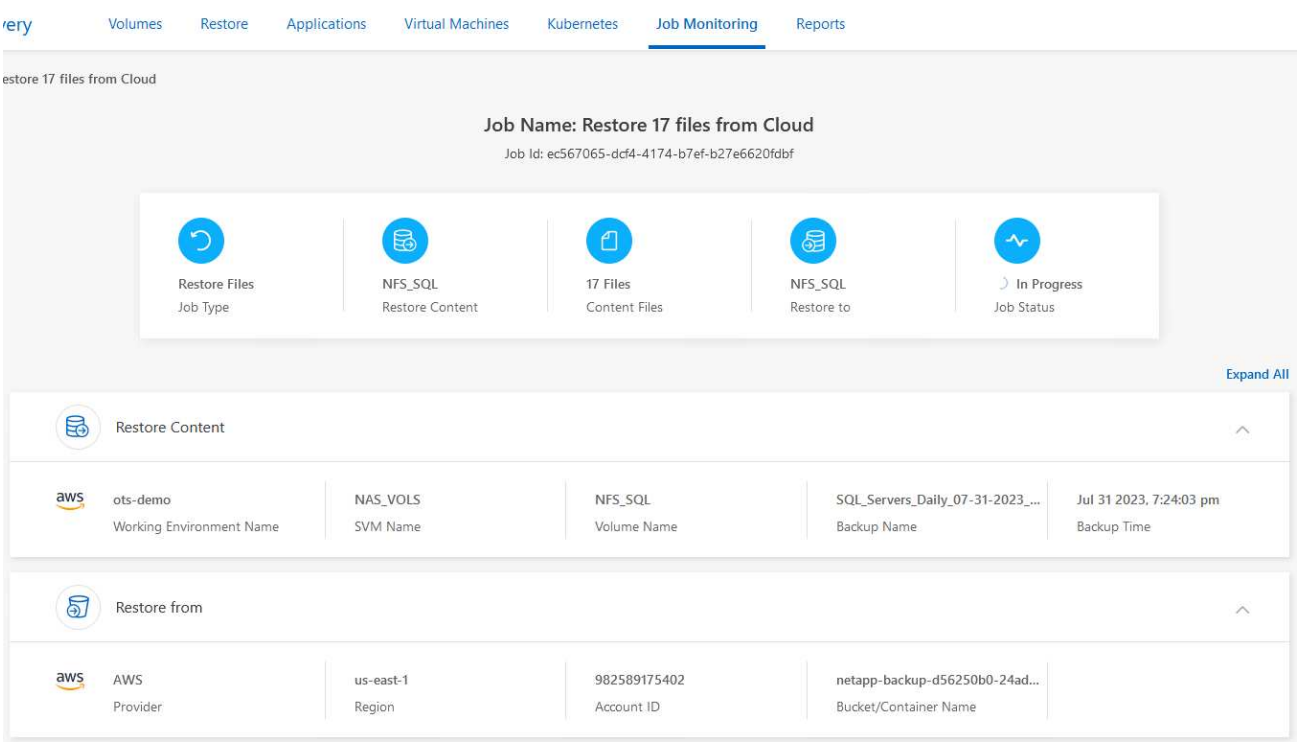
2. 復元するVMの設定ドロップダウンメニューにアクセスし、



3. 復元するバックアップを選択し、「次へ」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、[復元] をクリックして復元プロセスを開始します。
5. *ジョブ監視*タブから復元ジョブの進行状況を監視します。



まとめ

3-2-1バックアップ戦略を、仮想マシン向けのSnapCenter Plug-in for VMware vSphereおよびNetApp Backup and Recoveryを使用して実装すると、データ保護のための堅牢で信頼性が高く、対費用効果の高い解決策が提供されます。この戦略は、データの冗長性とアクセス性を確保するだけでなく、あらゆる場所から、またオンプレミスの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復元できる柔軟性も提供します。

このドキュメントで紹介するユースケースは、NetApp、VMware、および主要なクラウド プロバイダ間の統合を強調する、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とのシームレスな統合を提供し、データ保護操作の効率的かつ一元的な管理を可能にします。この統合により、仮想マシンのバックアップとリカバリのプロセスが効率化され、VMwareエコシステム内での容易なスケジュール設定、監視、および柔軟な復元操作が可能になります。仮想マシン向けのNetApp Backup and Recoveryは、仮想マシン データをクラウドベースのオブジェクト ストレージに安全かつエアギャップされた状態でバックアップすることで、3-2-1の1（1）を提供します。直感的なインターフェースと論理的なワークフローにより、重要なデータの長期保存のための安全なプラットフォームを提供します。

追加情報

このソリューションで紹介されているテクノロジーの詳細については、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"
- "NetApp Console のドキュメント"

NetApp Disaster Recovery

概要

災害復旧は、すべてのVMware管理者にとって最優先事項です。VMwareはサーバー全体

を仮想マシンを構成する一連のファイルにカプセル化するため、管理者はクローン、スナップショット、レプリカといったブロックストレージベースの技術を利用してこれらの仮想マシンを保護します。ONTAPアレイは、ボリュームデータ、ひいては指定されたデータストアLUN上に存在する仮想マシンを、あるサイトから別のサイトに転送するための組み込みレプリケーション機能を提供します。NetApp Disaster RecoveryはvSphereと統合されており、災害発生時のシームレスなフェイルオーバーとフェイルバックのためにワークフロー全体を自動化します。ストレージレプリケーションとインテリジェントな自動化を組み合わせることで、管理者は災害復旧計画の設定、自動化、テストを容易に行えるだけでなく、災害発生時にそれらを簡単に実行できる手段も手に入れることができます。

VMware vSphere 環境での DR フェイルオーバーで最も時間のかかる部分は、DR サイトでの VM のインベントリ、登録、再構成、および電源投入に必要な手順の実行です。理想的なソリューションは、RPO (分単位で測定) と RTO (分から時間単位で測定) の両方が低いものです。 DR ソリューションで見落とされがちな要素の 1 つは、DR ソリューションを定期的に効率的にテストする機能です。

DR ソリューションを設計するには、次の要素を考慮してください。

- 目標復旧時間 (RTO)。 RTO とは、企業が災害からどれだけ早く回復できるか、より具体的には、ビジネス サービスを再び利用できるようにするために回復プロセスを実行するのにどれだけの時間がかかるかということです。
- 回復ポイント目標 (RPO)。 RPO は、災害が発生した時間に対して、回復されたデータが利用可能になってからどのくらい経っているかを示します。
- スケーラビリティと適応性。この要素には、需要の増加に応じてストレージ リソースを段階的に拡張する機能が含まれます。

利用可能なソリューションに関する詳細な技術情報については、以下を参照してください。

- "NFSデータストア向けNetApp Disaster Recovery"
- "VMFSデータストア向けNetApp Disaster Recovery"

NFSデータストア向けNetApp Disaster Recovery

NFSデータストア向けNetApp Disaster Recovery

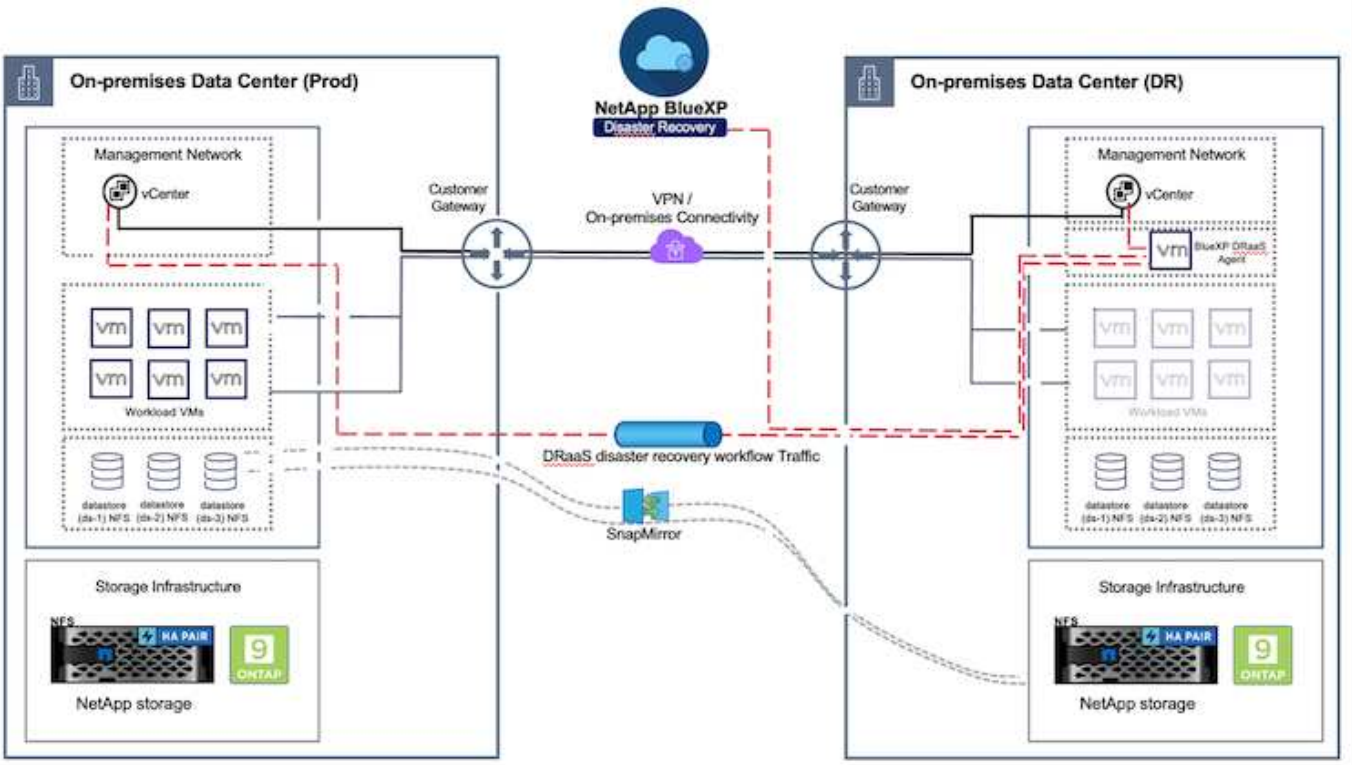
運用サイトから災害復旧サイトへのブロックレベルのレプリケーションを通じて災害復旧を実装することは、サイトの停止やランサムウェア攻撃などのデータ破損イベントからワークロードを保護するための、回復力がありコスト効率に優れた方法です。 NetApp SnapMirrorレプリケーションを使用すると、NFS データストアを備えたオンプレミスのONTAPシステムで実行されている VMware ワークロードを、VMware も導入されている指定されたリカバリ データセンターにある別のONTAPストレージ システムに複製できます。

このドキュメントのこのセクションでは、オンプレミスのVMware VMを別の指定サイトにディザスタリカバリするように設定するためのNetApp Disaster Recoveryの構成について説明します。このセットアップの一環として、Consoleエージェント、ONTAPアレイのオンボーディング、サイトの定義、およびVMware vCenterの関連付けを行います。さらに、このドキュメントでは、サイト間のレプリケーションの設定方法、および復旧計画のセットアップとテスト方法について詳しく説明します。最後のセクションでは、サイト全体のフェイ

ルオーバーを実行する手順と、プライマリサイトが復旧してオンラインになったときにフェイルバックする方法について説明します。

NetApp Data Servicesの一部であるDisaster Recoveryを活用することで、企業はオンプレミスのVMware vCentersとONTAPストレージを簡単に検出できます。その後、組織はリソースグループを作成し、災害復旧計画を作成してリソースグループに関連付け、フェイルオーバーとフェイルバックのテストまたは実行を行うことができます。SnapMirrorは、ストレージレベルのブロックレプリケーションを提供して、増分変更により2つのサイトを最新の状態に保ち、最大5分のリカバリポイント目標（RPO）を実現します。さらに、本番環境に影響を与えたり、追加のストレージコストを発生させたりすることなく、災害復旧手順をシミュレーションすることが可能です。

Disaster Recoveryは、ONTAPのFlexCloneテクノロジを活用して、ディザスタリカバリサイトで最後にレプリケートされたSnapshotから、スペース効率に優れたNFSデータストアのコピーを作成します。ディザスタリカバリのテスト完了後、お客様は実際のレプリケートされた本番リソースに影響を与えることなく、テスト環境を簡単に削除できます。実際のフェイルオーバーが発生した場合、Disaster Recoveryはわずか数回のクリックで、指定されたディザスタリカバリサイトで保護対象の仮想マシンを自動的に起動するために必要なすべての手順をオーケストレーションします。また、このサービスは必要に応じて、プライマリサイトへのSnapMirror関係を反転させ、フェイルバック処理のためにセカンダリからプライマリへ変更をレプリケートします。これらの機能はすべて、他のよく知られた代替製品と比較して、はるかに低いコストで利用できます。



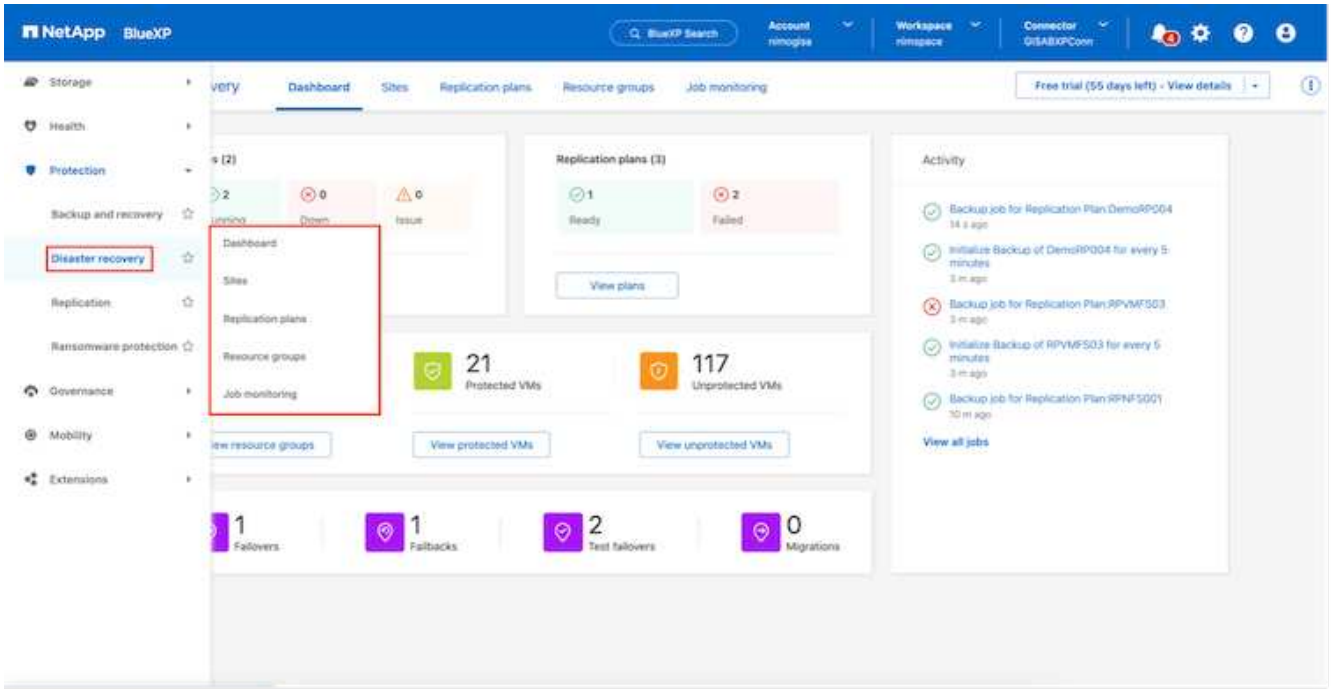
ディザスタリカバリ向けのvCenter Server、ESXi、およびONTAPの最新情報とサポートされるバージョンについては、"災害復旧のサポート対象構成"を参照してください。

開始

はじめに、NetApp Disaster Recoveryの利用を開始するには、NetApp コンソールを使用してサービスにアクセスします。

1. Consoleにログインします。

2. Consoleの左側のナビゲーションから、「保護」＞「災害復旧」を選択します。
3. 災害復旧ダッシュボードが表示されます。

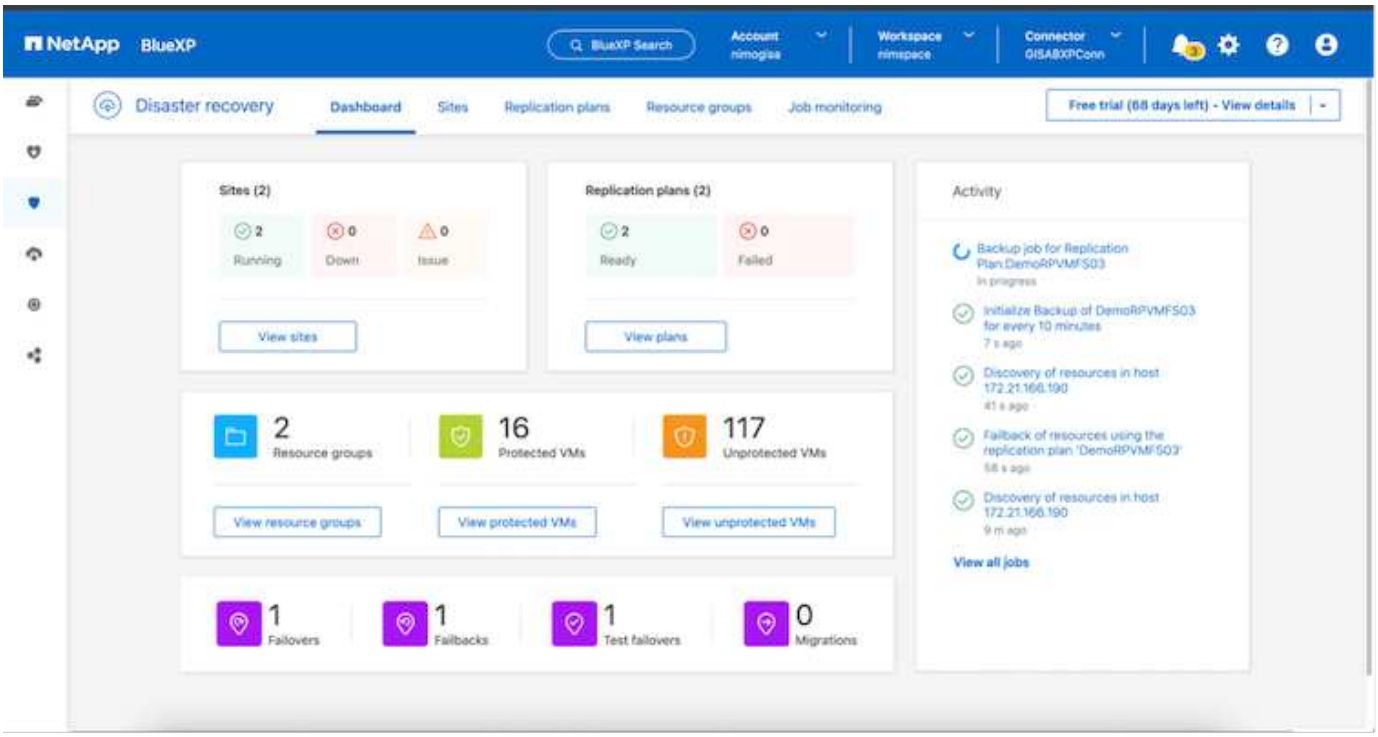


災害復旧計画を設定する前に、以下の前提条件が満たされていることを確認してください：

- Consoleエージェントがデプロイされました。
- エージェントは、送信元と宛先のvCenterおよびストレージシステムへの接続性を備えています。
- NFSサービスが有効なSVMを備えたONTAPクラスタが利用可能です。
- VMware用のNFSデータストアをホストするオンプレミスのNetAppストレージシステムは、Consoleに追加されます。
- 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。
- 指定された NFS ベースのデータストア ボリュームに対してSnapMirrorレプリケーションが構成されます。
- 環境にサポートされているバージョンの vCenter Server および ESXi サーバーがインストールされていることを確認します。

ソースサイトと宛先サイト間の接続が確立されたら、構成手順に進みます。これには数回のクリックと約 3 ～ 5 分かかります。

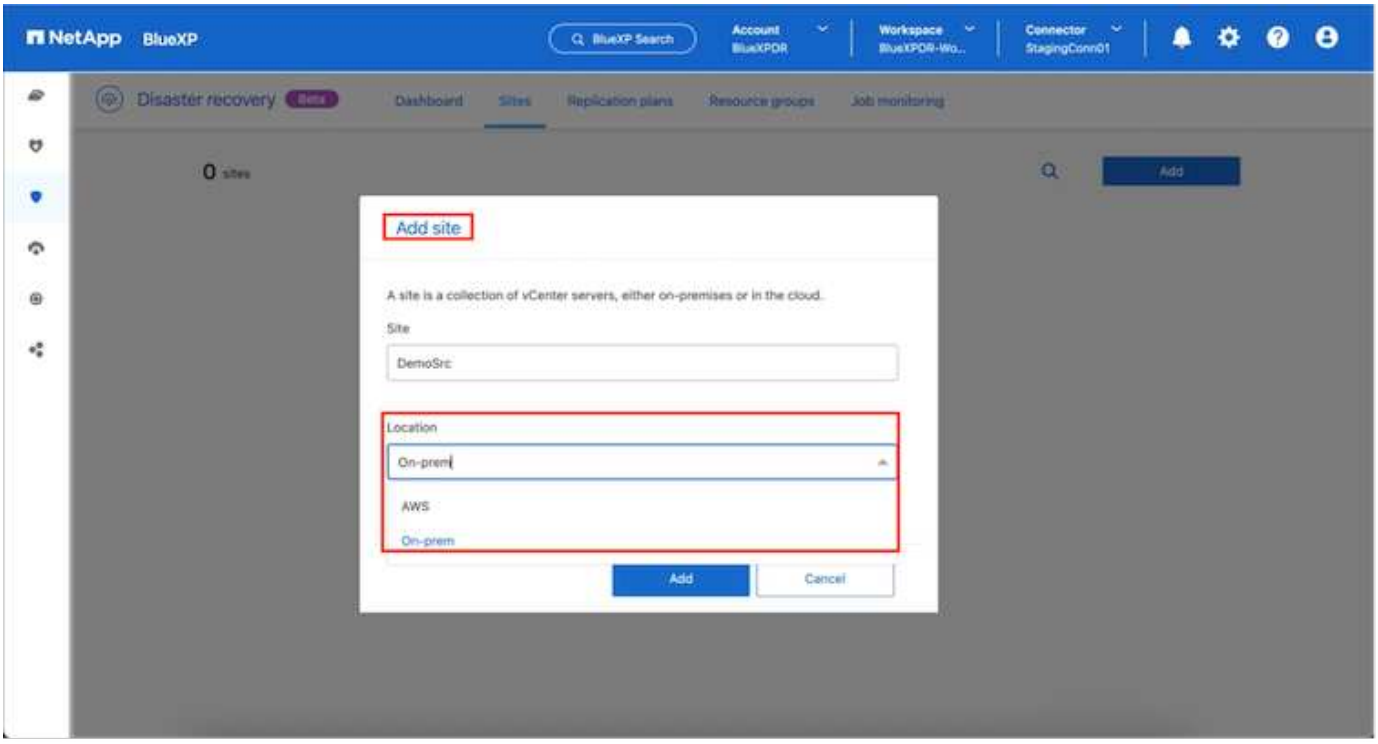
NetAppは、Consoleエージェントがネットワークを介して送信元および宛先のリソースと通信できるように、Consoleエージェントを宛先サイトまたは第3のサイトに導入することを推奨しています。



NetApp Disaster Recovery構成

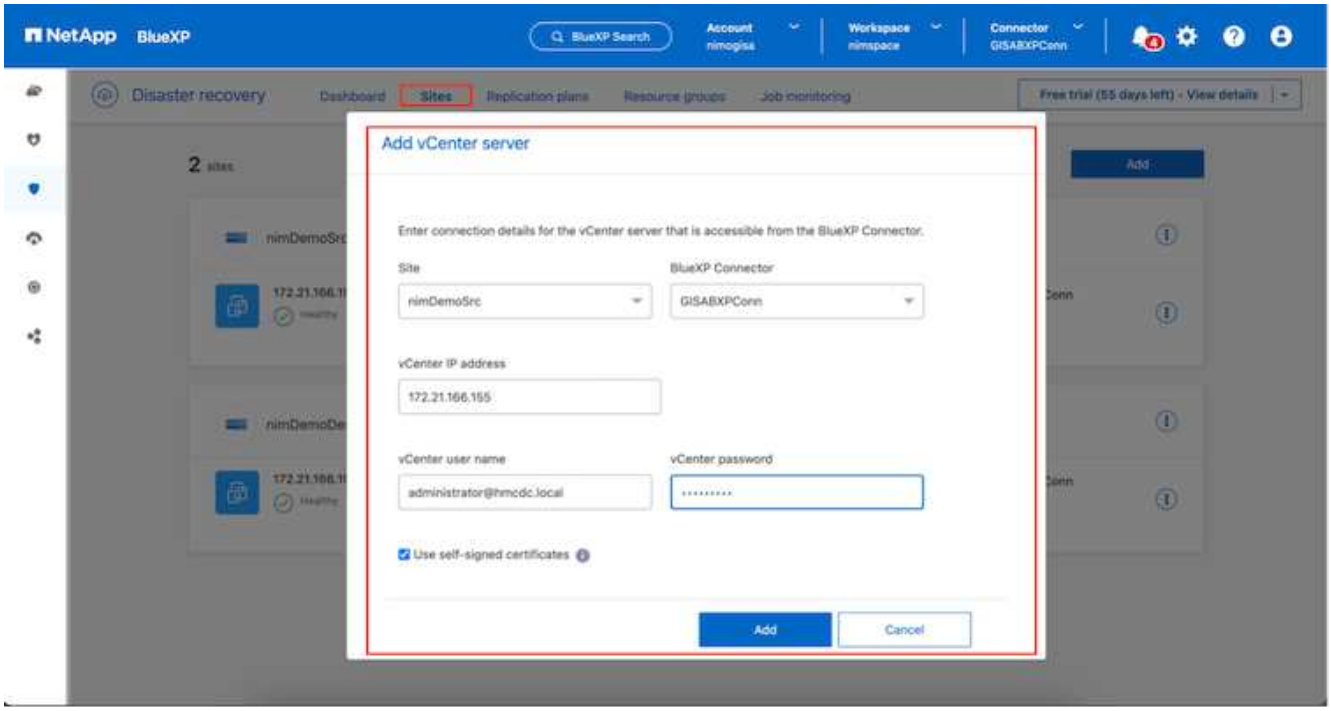
災害復旧の準備の最初のステップは、オンプレミスのvCenterおよびストレージリソースを検出してNetApp Disaster Recoveryに追加することです。

Consoleを開き、左側のナビゲーションから*保護 > ディザスタリカバリ*を選択します。*サイト*をクリックし、名前を指定して場所のタイプを選択します。次に、*vCenterの追加*ボタンをクリックします。

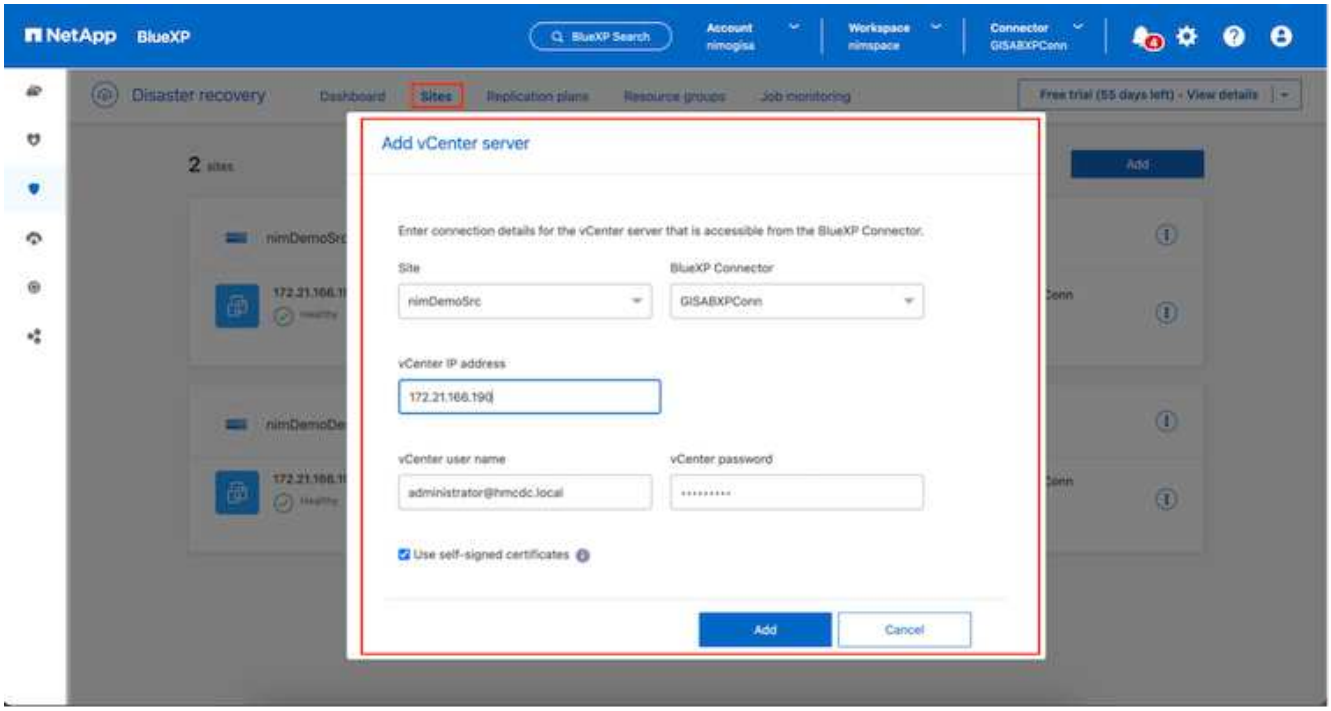


次のプラットフォームを追加します。

- ソース。オンプレミスの vCenter。



- 行き先。 VMC SDDC vCenter。



vCenter が追加されると、自動検出がトリガーされます。

ソースサイトアレイと宛先サイトアレイ間のストレージレプリケーションの構成

SnapMirrorは、NetApp環境でデータレプリケーションを提供します。NetApp Snapshotテクノロジを基盤とするSnapMirrorレプリケーションは、前回の更新以降に変更または追加されたブロックのみをレプリケートするため、非常に効率的です。SnapMirrorは、NetApp OnCommand System ManagerまたはONTAP CLIを使用

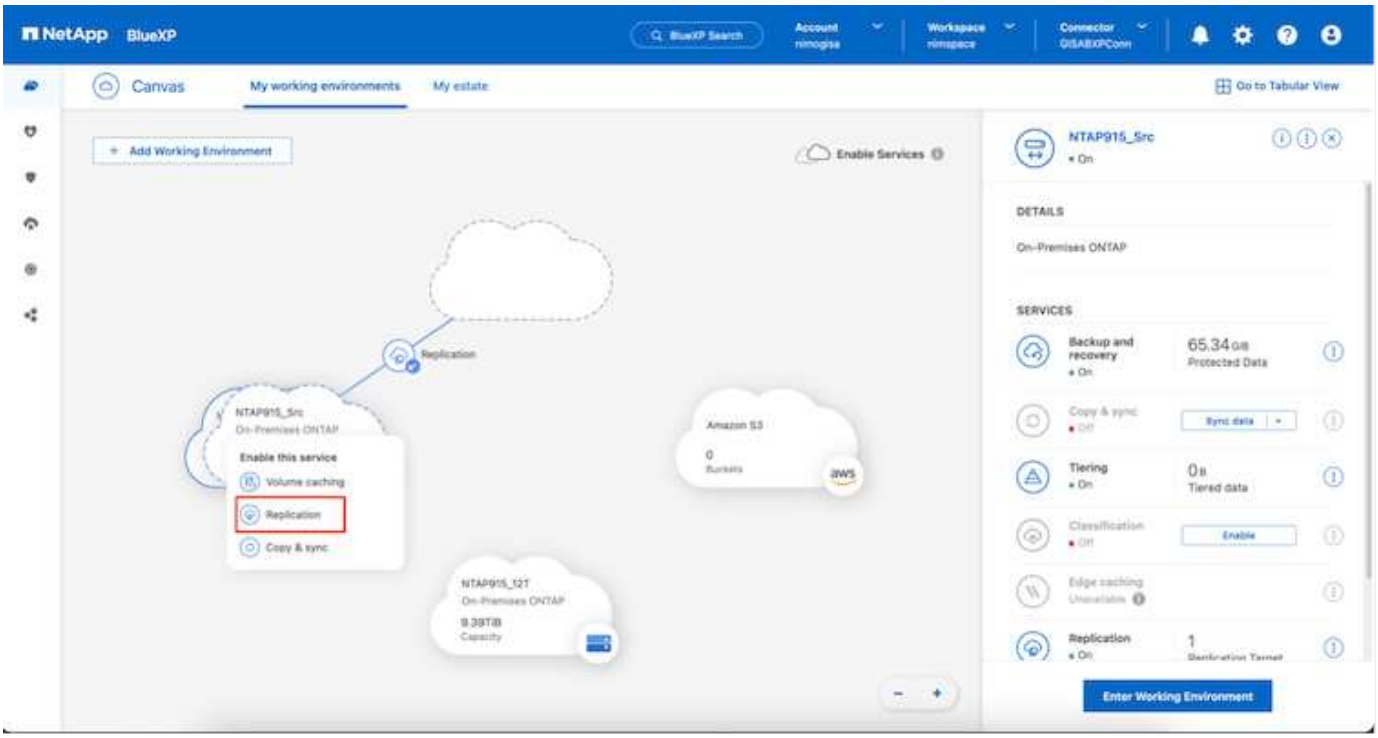
して簡単に設定できます。事前にクラスタとSVMのピアリングが設定されていれば、NetApp Data ServicesでもSnapMirror関係が作成されます。

プライマリストレージが完全に失われていない場合、SnapMirrorはプライマリサイトとDRサイトを効率的に再同期させる手段を提供します。SnapMirrorは、SnapMirror関係を反転させるだけで、変更されたデータや新しいデータのみをDRサイトからプライマリサイトに転送し、2つのサイトを再同期することができます。これにより、Disaster Recoveryのレプリケーションプランは、フェイルオーバー後にボリューム全体を再コピーすることなく、どちらの方向にも再同期できます。関係が逆方向に再同期される場合、Snapshotコピーの最後の同期が成功してから書き込まれた新しいデータのみが宛先に送信されます。

CLIまたはSystem Managerを使用してボリュームのSnapMirror関係がすでに設定されている場合、NetApp Data Servicesはその関係を引き継ぎ、残りのワークフロー操作を続行します。

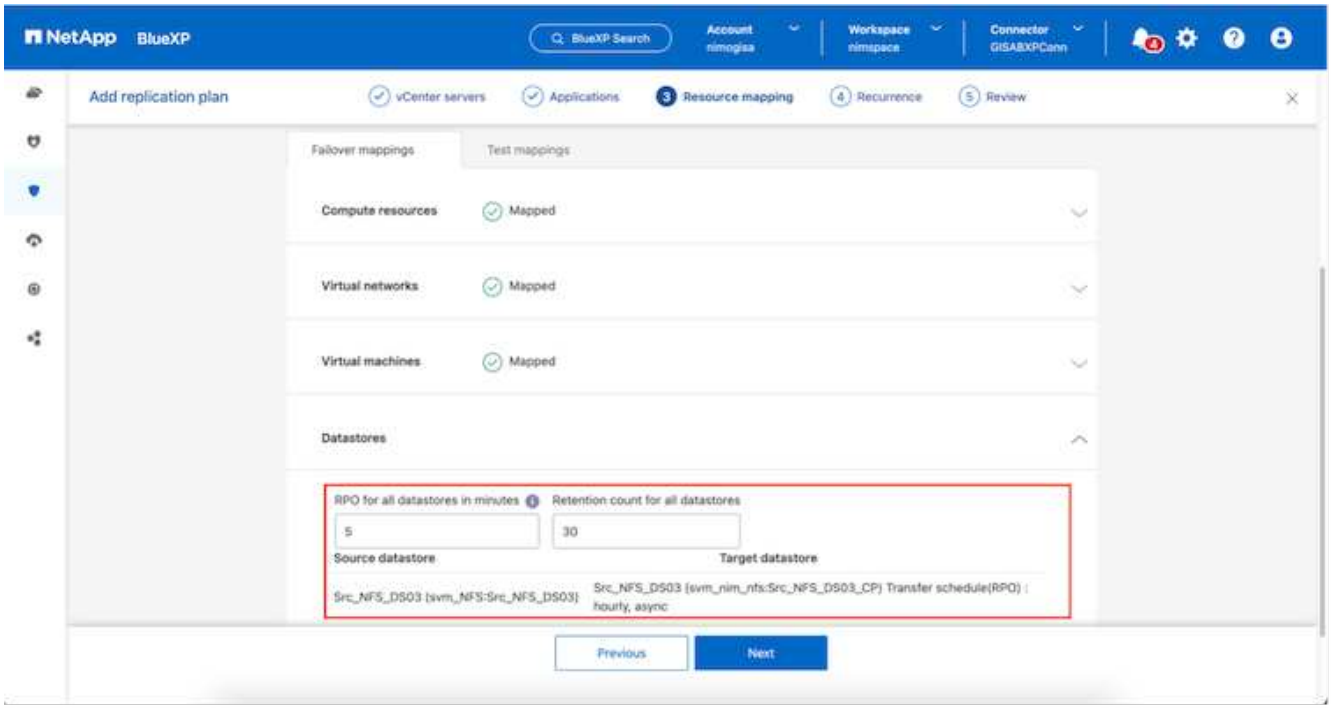
VMware Disaster Recoveryの設定方法

SnapMirrorレプリケーションを作成するプロセスは、どのアプリケーションでも同じです。このプロセスは、手動または自動で実行できます。最も簡単な方法は、NetApp Consoleを活用してSnapMirrorレプリケーションを設定することです。環境内のソースONTAPシステムをデスティネーションにドラッグ＆ドロップするだけで、残りのプロセスをガイドするウィザードが起動します。



Disaster Recoveryも、以下の2つの条件を満たせば自動化できます：

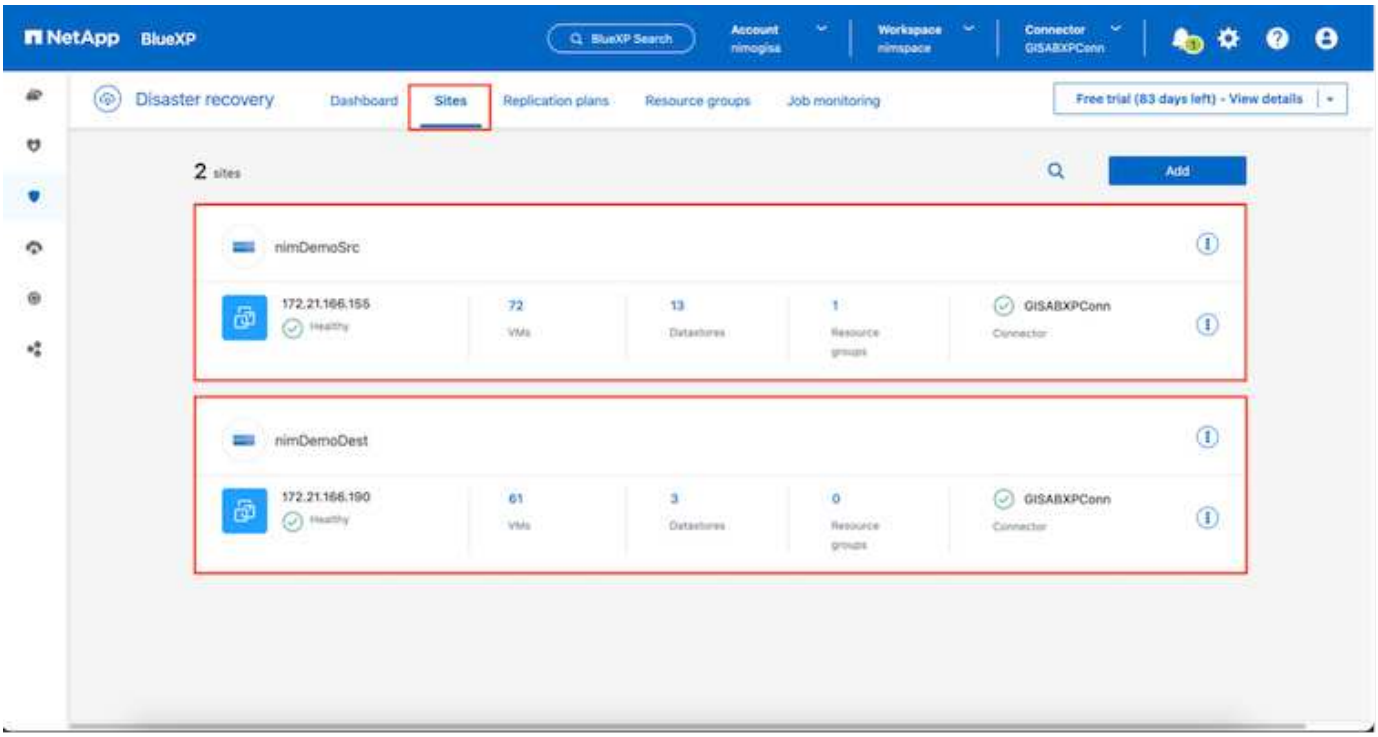
- ソース クラスターと宛先クラスターにはピア関係があります。
- ソース SVM と宛先 SVM にはピア関係があります。



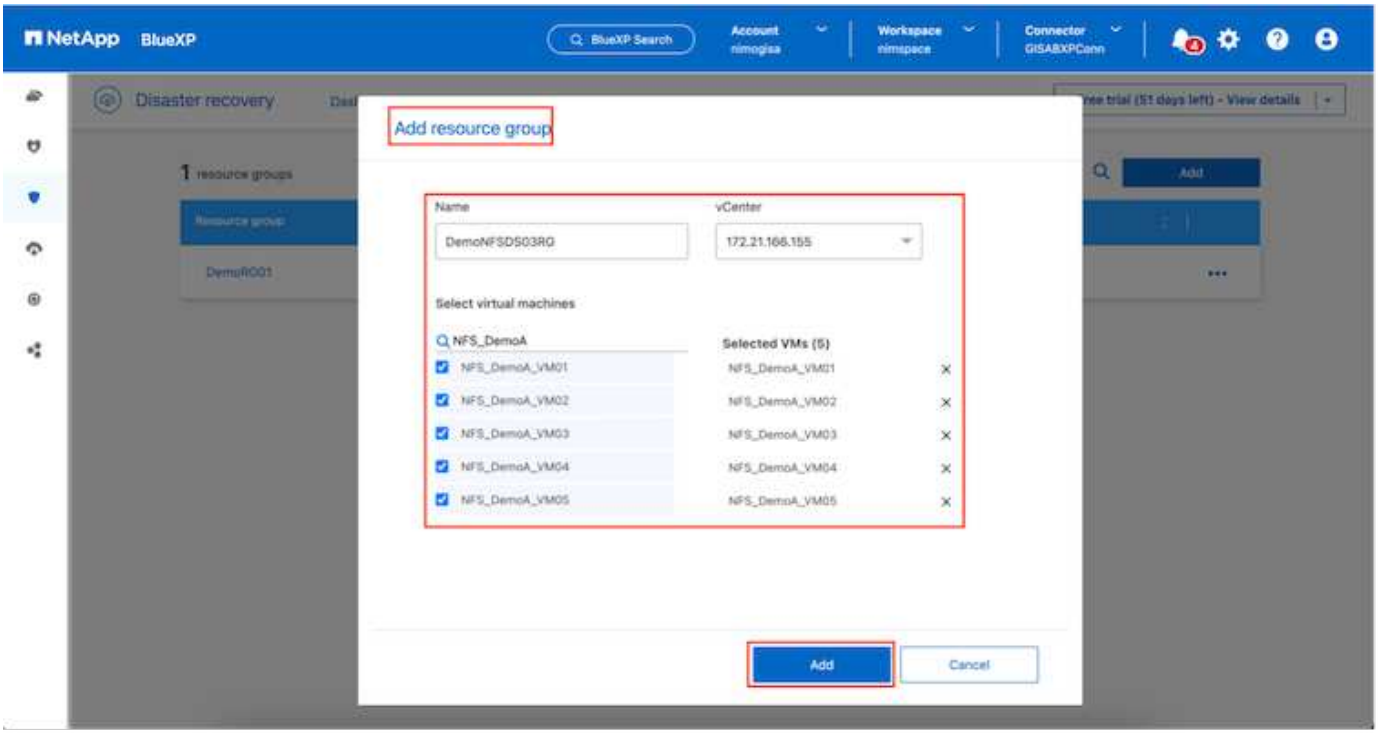
CLI経由でボリュームにSnapMirror関係がすでに設定されている場合、Disaster Recoveryはその関係を認識し、残りのワークフロー操作を続行します。

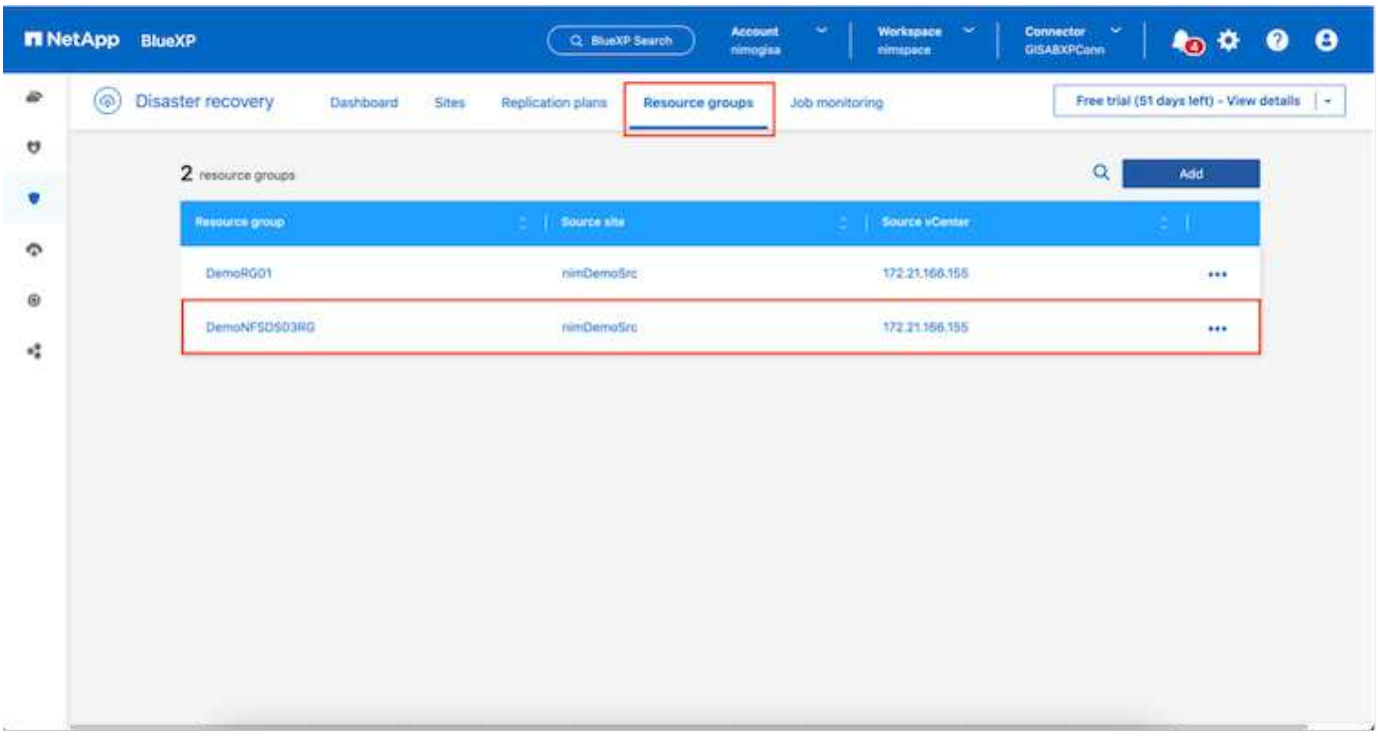
Disaster Recoveryはお客様にどのようなメリットをもたらすのでしょうか？

ソースサイトと宛先サイトが追加されると、Disaster Recoveryは自動的に詳細な検出を実行し、VMsと関連するメタデータを表示します。また、Disaster Recoveryは、VMs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、それらを設定します。



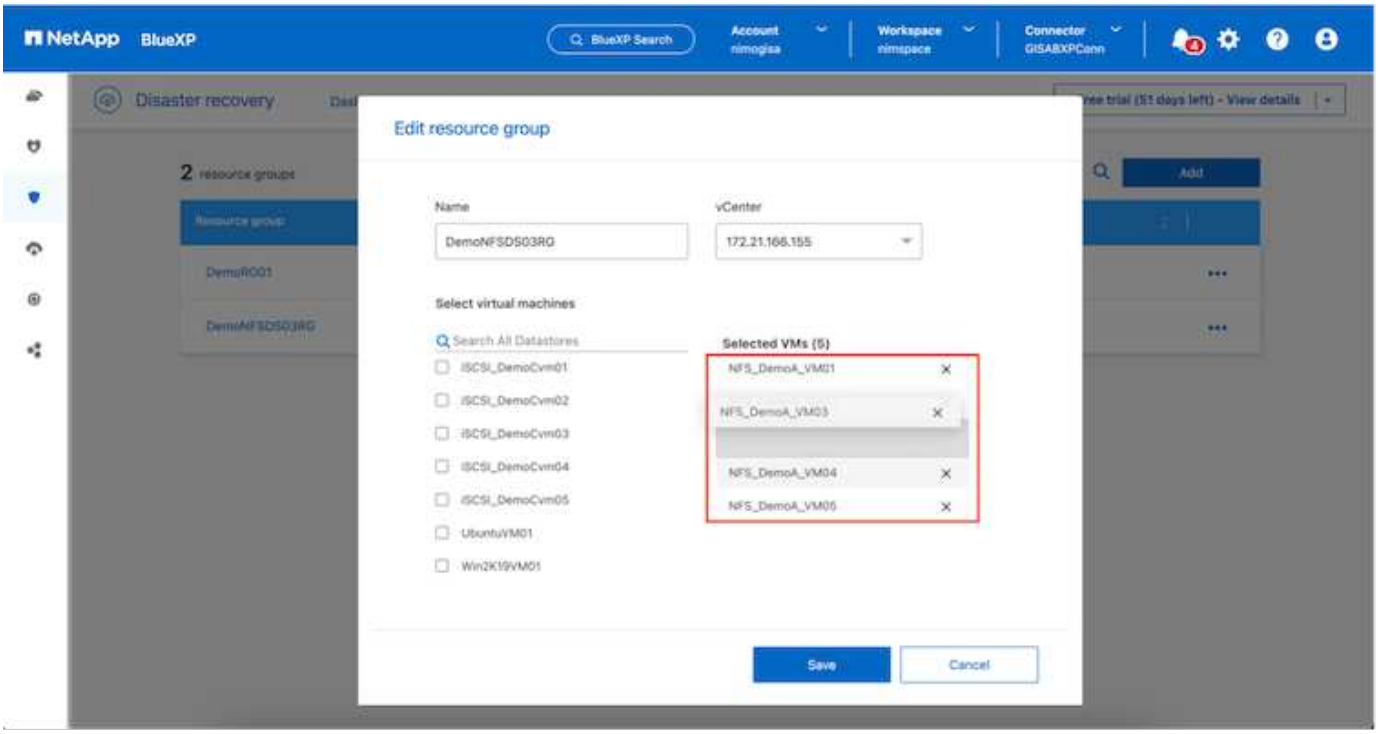
サイトが追加された後、仮想マシンをリソースグループにグループ化できます。ディザスタリカバリのリソースグループを使用すると、依存関係のある仮想マシンを論理グループにまとめることができ、各グループにはリカバリ時に実行できる起動順序と起動遅延が含まれます。リソースグループの作成を開始するには、「リソースグループ」に移動し、「新しいリソースグループの作成」をクリックします。



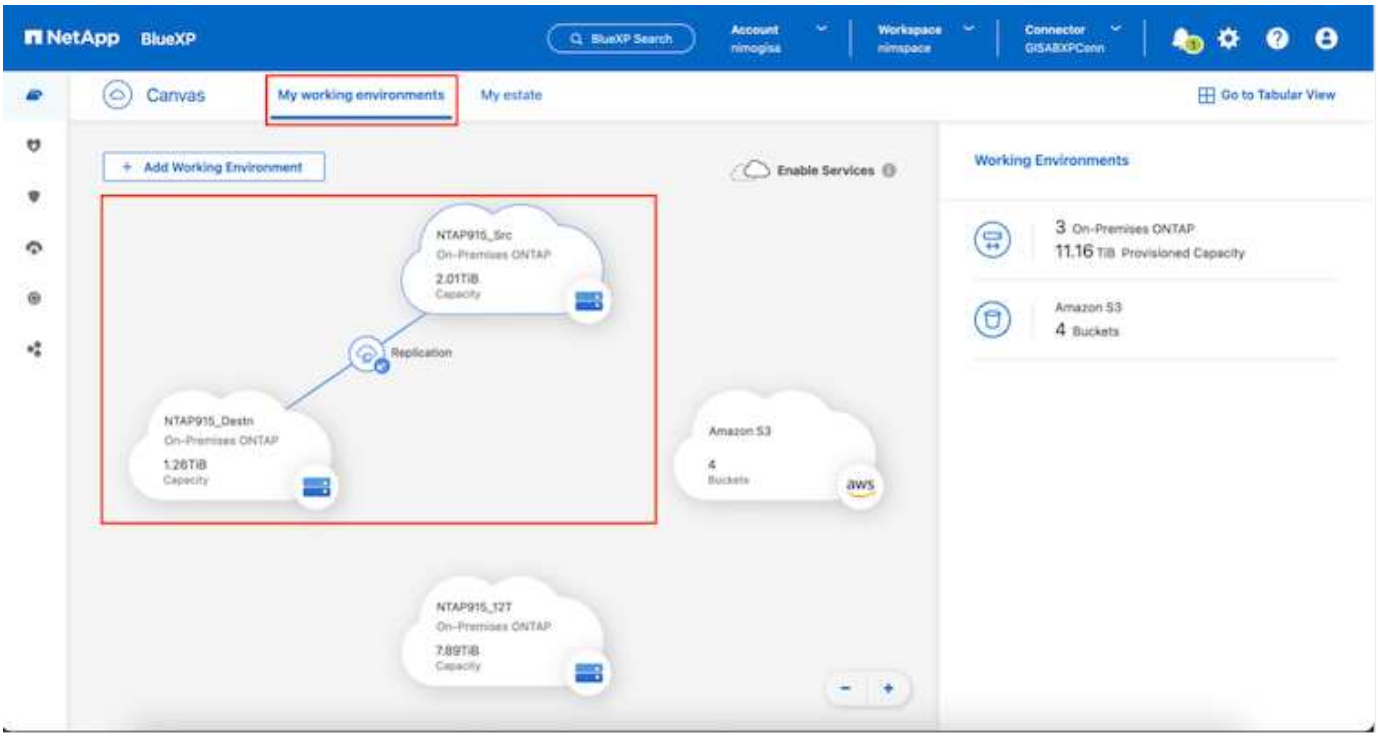


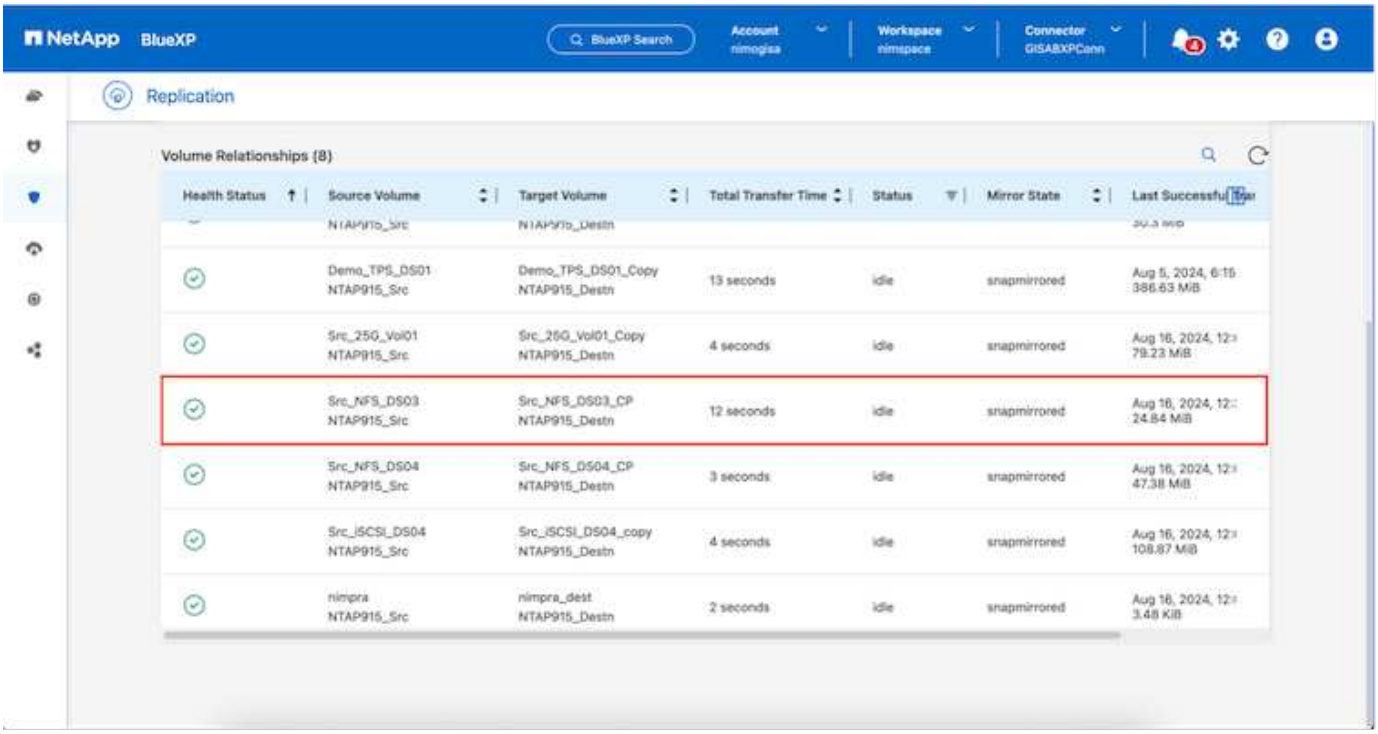
レプリケーション プランの作成時にリソース グループを作成することもできます。

VM のブート順序は、リソース グループの作成中に、簡単なドラッグ アンド ドロップ メカニズムを使用して定義または変更できます。



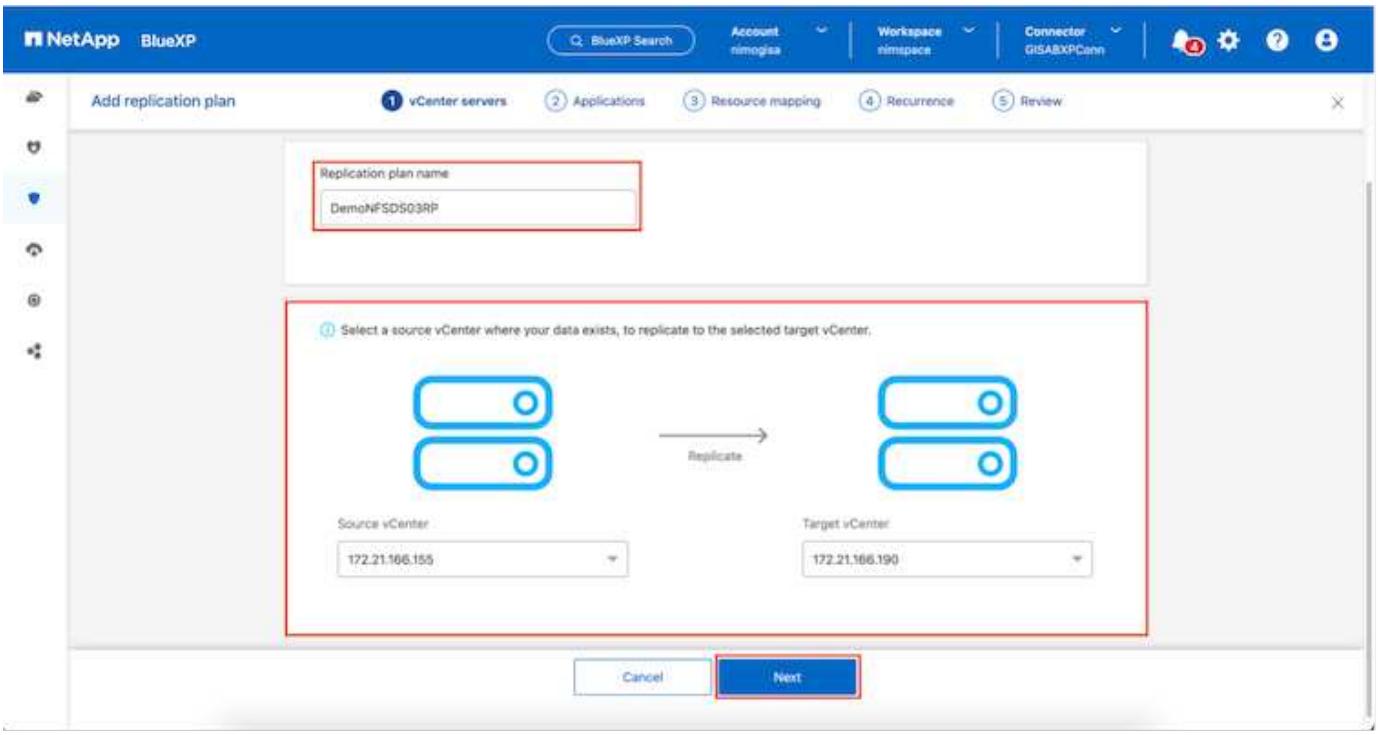
リソース グループを作成したら、次のステップは、災害発生時に仮想マシンとアプリケーションを復旧するための実行ブループリントまたは計画を作成することです。前提条件で述べたように、 SnapMirrorレプリケーションは事前に構成することも、レプリケーション プランの作成時に指定された RPO と保持数を使用して DRaaS で構成することもできます。





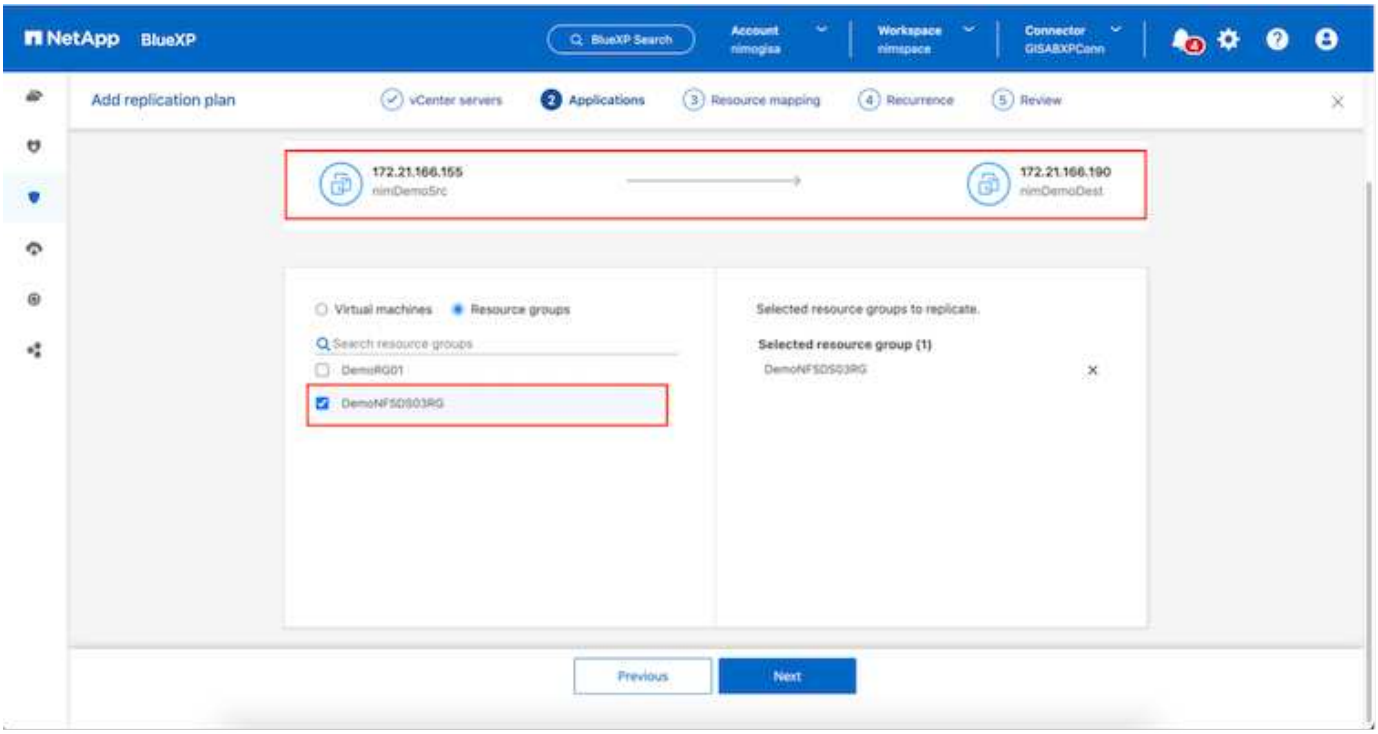
ドロップダウンからソースと宛先の vCenter プラットフォームを選択してレプリケーション プランを構成し、プランに含めるリソース グループ、アプリケーションの復元方法と電源オン方法のグループ化、およびクラスタとネットワークのマッピングを選択します。リカバリ プランを定義するには、[レプリケーション プラン] タブに移動し、[プランの追加] をクリックします。

まず、ソース vCenter を選択し、次に宛先 vCenter を選択します。



次のステップは、既存のリソース グループを選択することです。リソース グループが作成されていない場合、ウィザードは、回復目標に基づいて必要な仮想マシンをグループ化します (基本的には機能リソース グループを作成します)。これは、アプリケーション仮想マシンを復元する操作シーケンスを定義するのにも役立

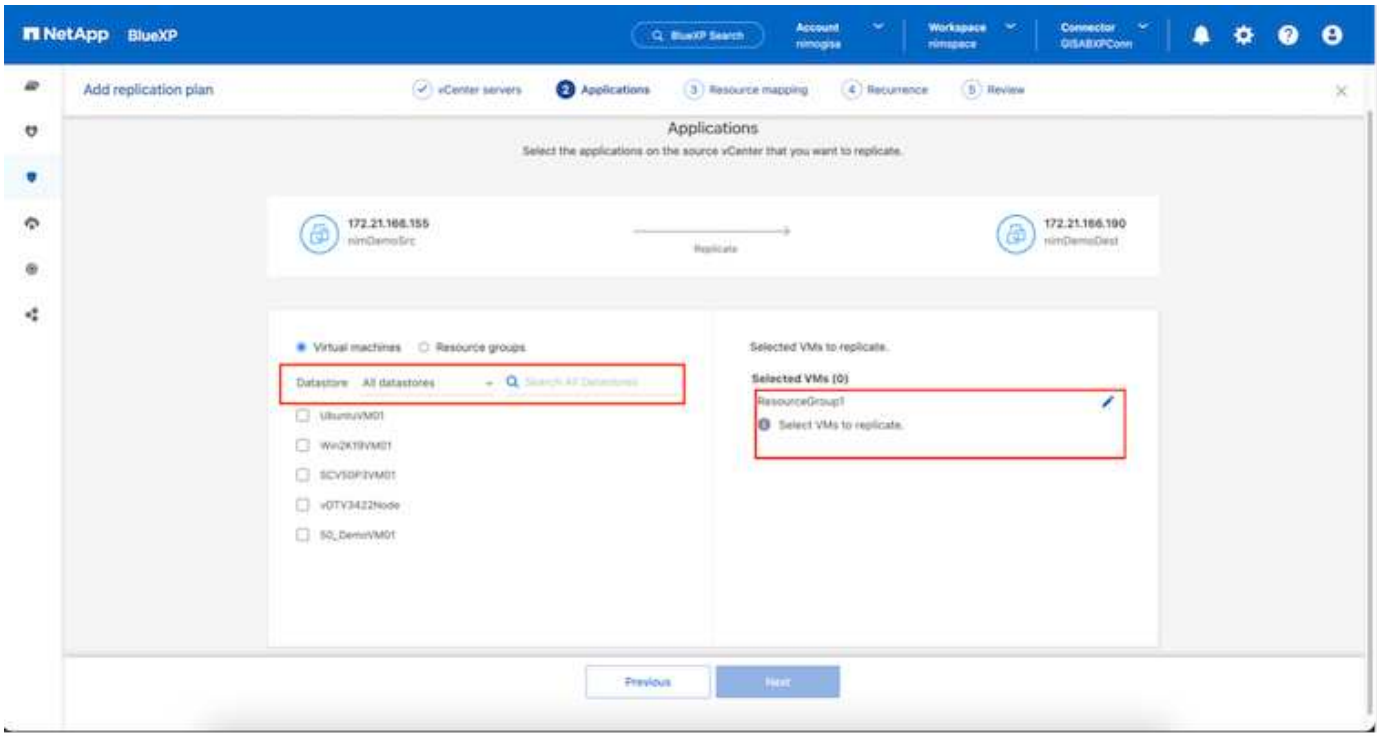
ちます。



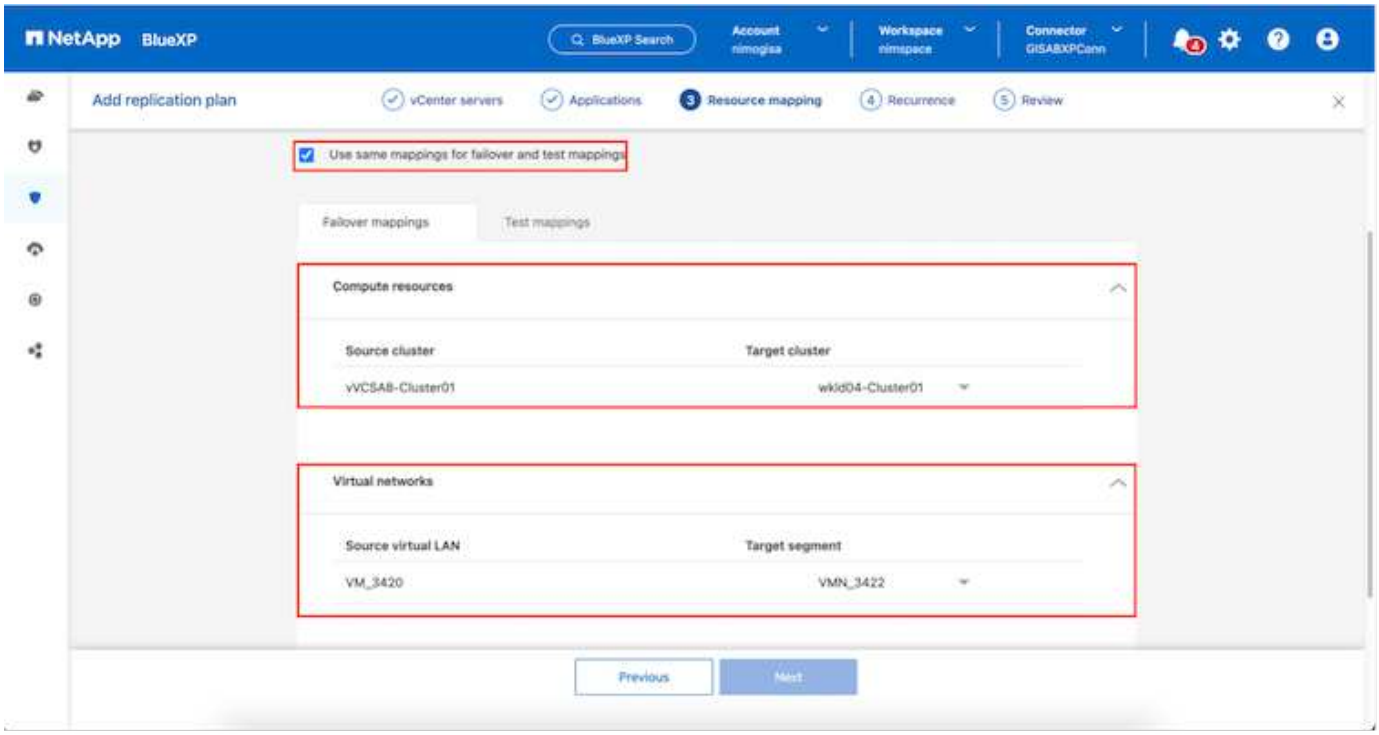
リソース グループでは、ドラッグ アンド ドロップ機能を使用してブート順序を設定できます。これを使用すると、リカバリプロセス中に VM の電源がオンになる順序を簡単に変更できます。

リソース グループ内の各仮想マシンは、順序に基づいて順番に起動されます。 2 つのリソース グループが並行して開始されます。

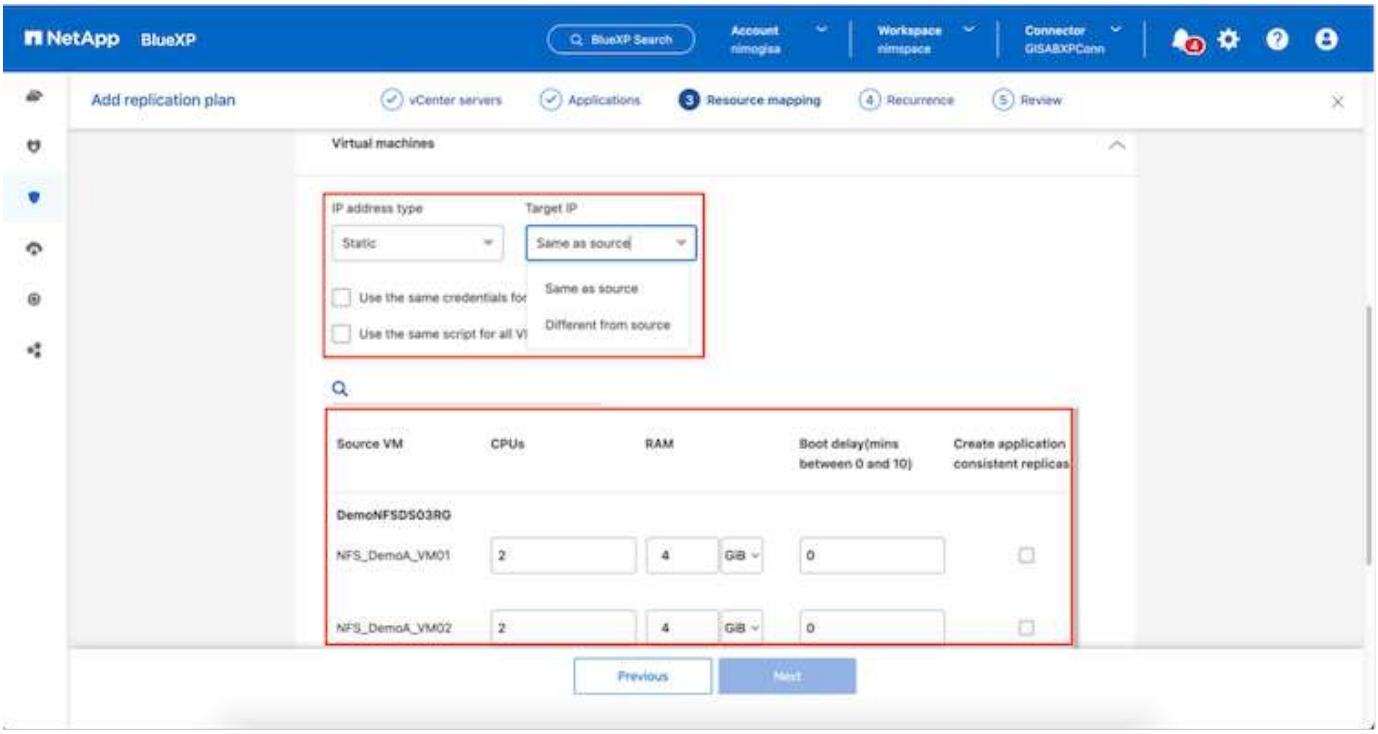
以下のスクリーンショットは、リソース グループが事前に作成されていない場合に、組織の要件に基づいて仮想マシンまたは特定のデータストアをフィルターするオプションを示しています。



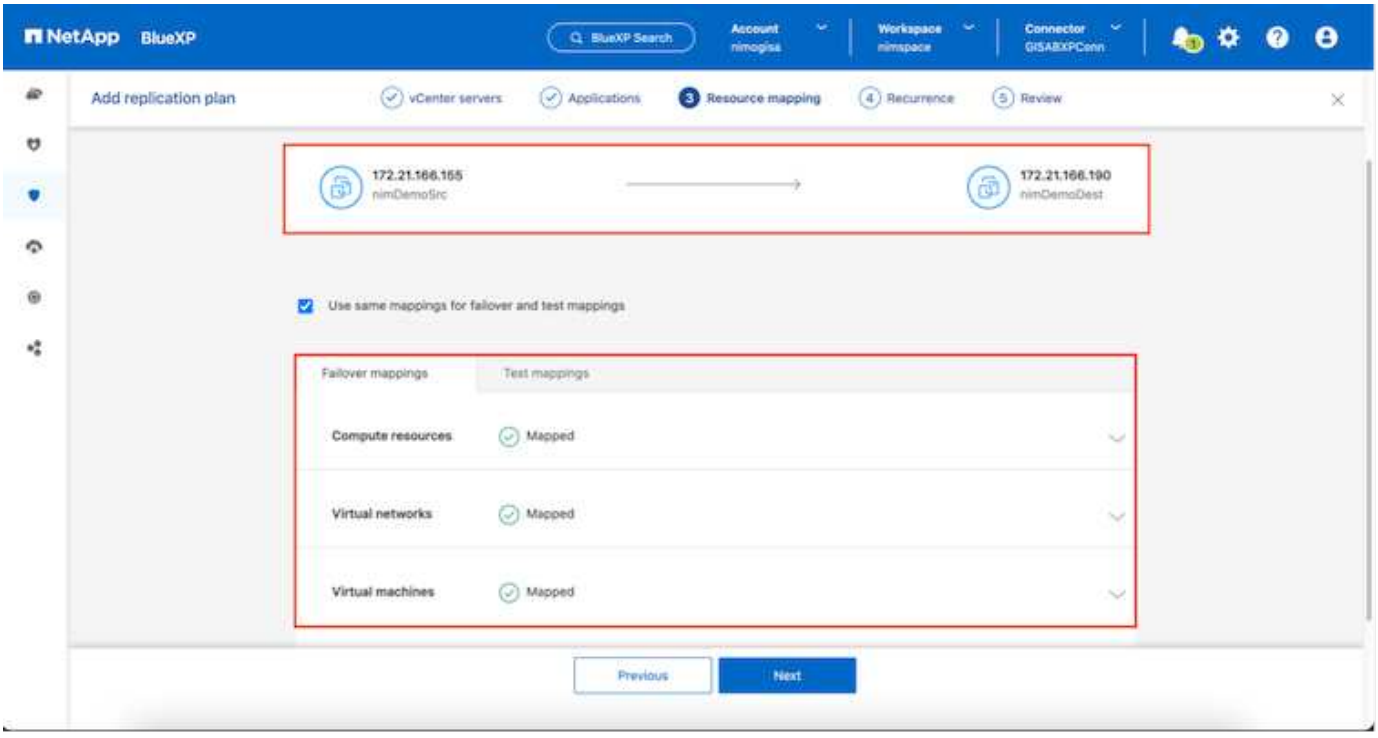
リソースグループを選択したら、フェイルオーバーマッピングを作成します。このステップでは、ソース環境のリソースをデスティネーションにマッピングする方法を指定します。これには、コンピューティングリソース、仮想ネットワークが含まれます。IPのカスタマイズ、プリスクリプトとポストスクリプト、ブート遅延、アプリケーションの整合性などです。詳細については、"レプリケーションプランを作成する"を参照してください。



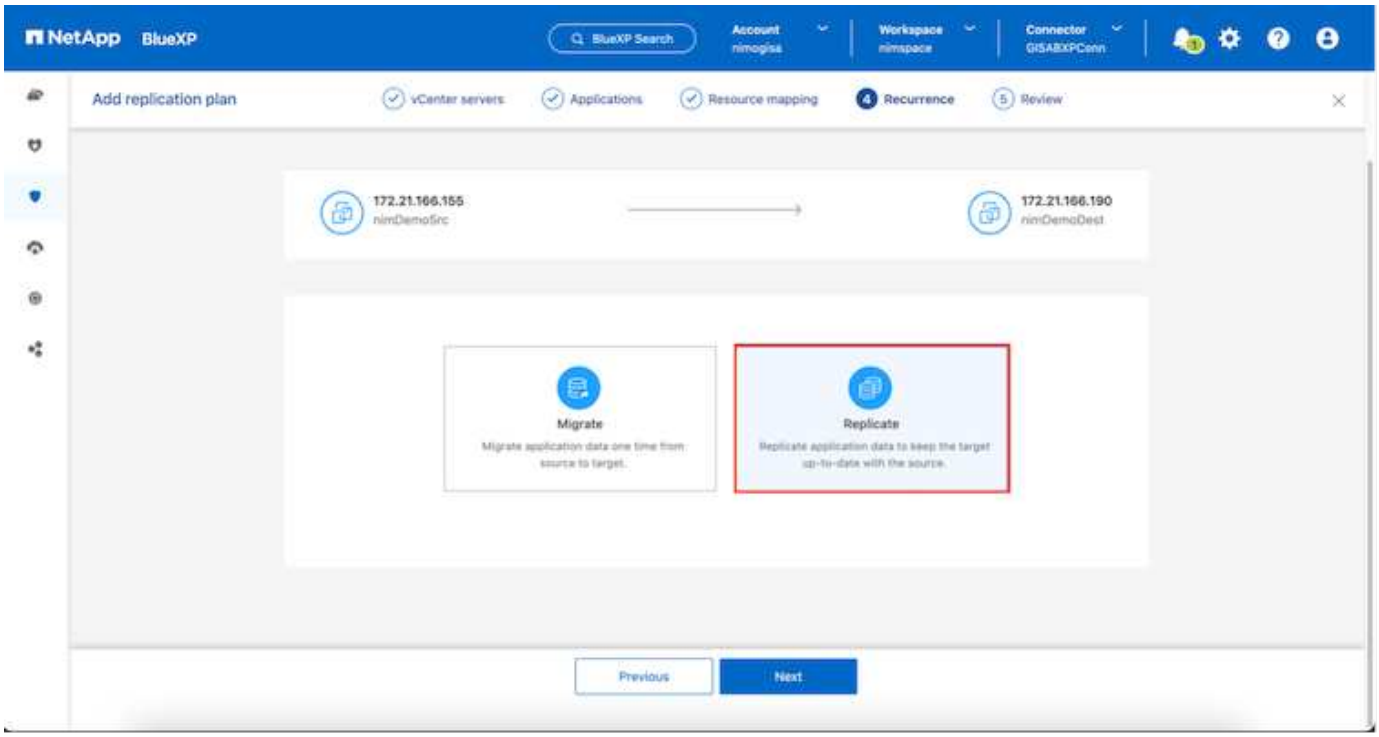
デフォルトでは、テスト操作とフェイルオーバー操作の両方に同じマッピング パラメータが使用されます。テスト環境に異なるマッピングを設定するには、以下に示すようにチェックボックスをオフにした後、テスト マッピング オプションを選択します。



リソース マッピングが完了したら、[次へ] をクリックします。

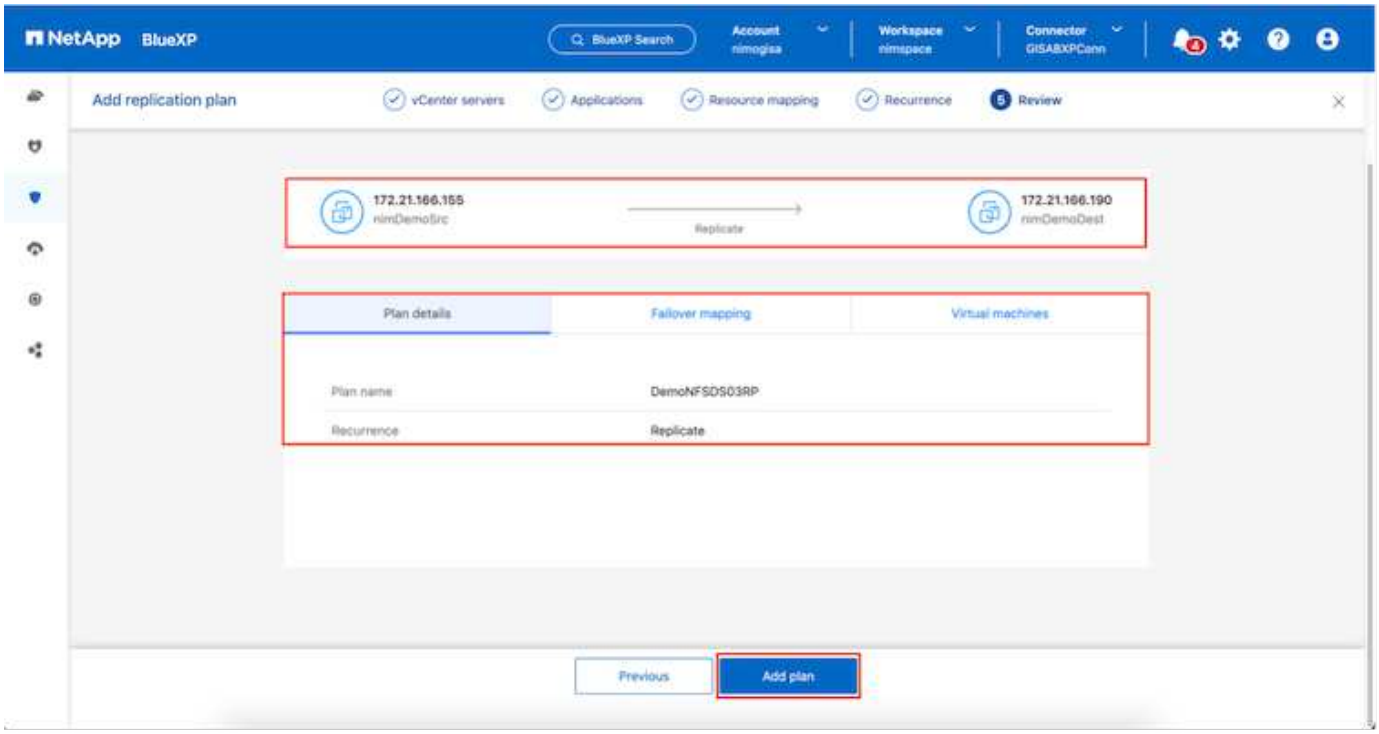


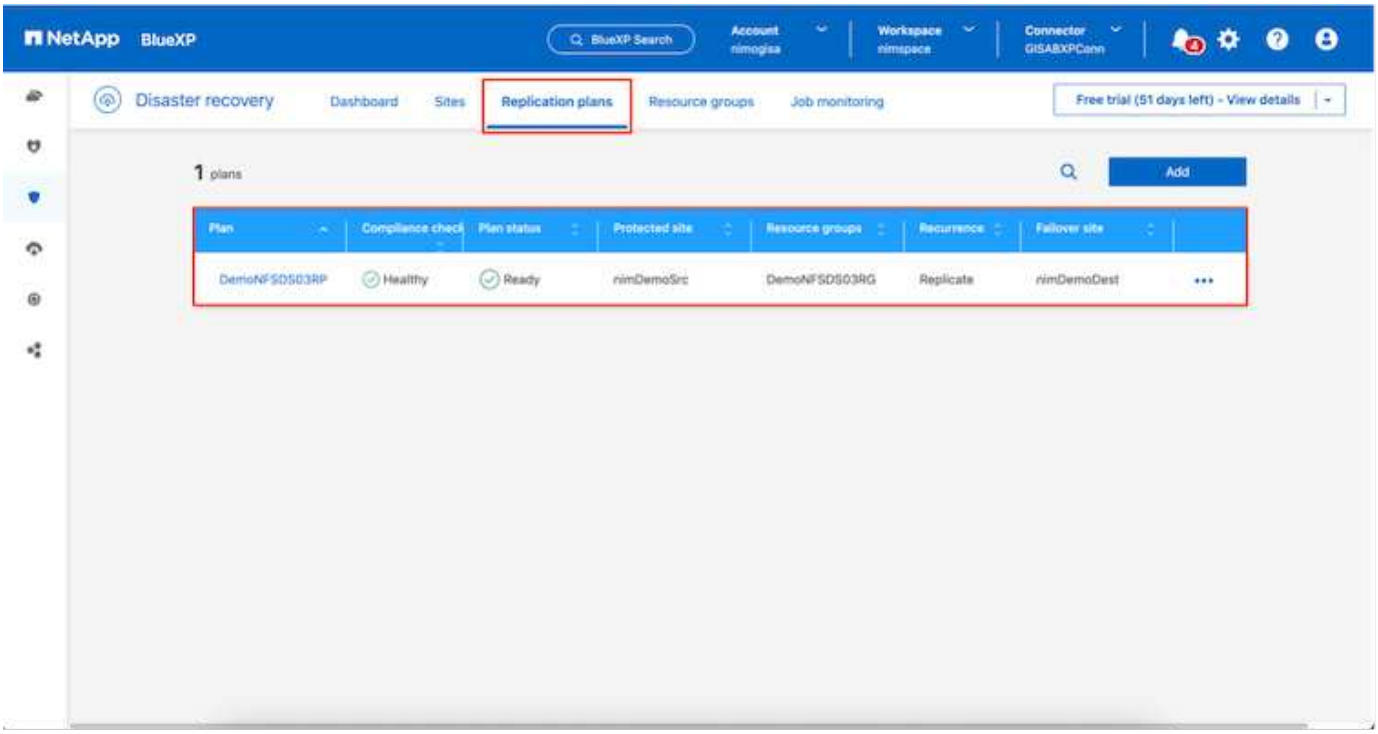
繰り返しタイプを選択します。簡単に言えば、「移行」（フェイルオーバーを使用した 1 回限りの移行）または定期的な連続レプリケーション オプションを選択します。このチュートリアルでは、「複製」オプションが選択されています。



完了したら、作成されたマッピングを確認し、「プランの追加」をクリックします。

異なるボリュームやSVMのVMをレプリケーションプランに含めることができます。VMの配置場所（同じSVM内の同じボリューム上か別のボリューム上か、異なるSVM上の別のボリューム上か）に応じて、Disaster Recoveryは整合性グループSnapshotを作成します。



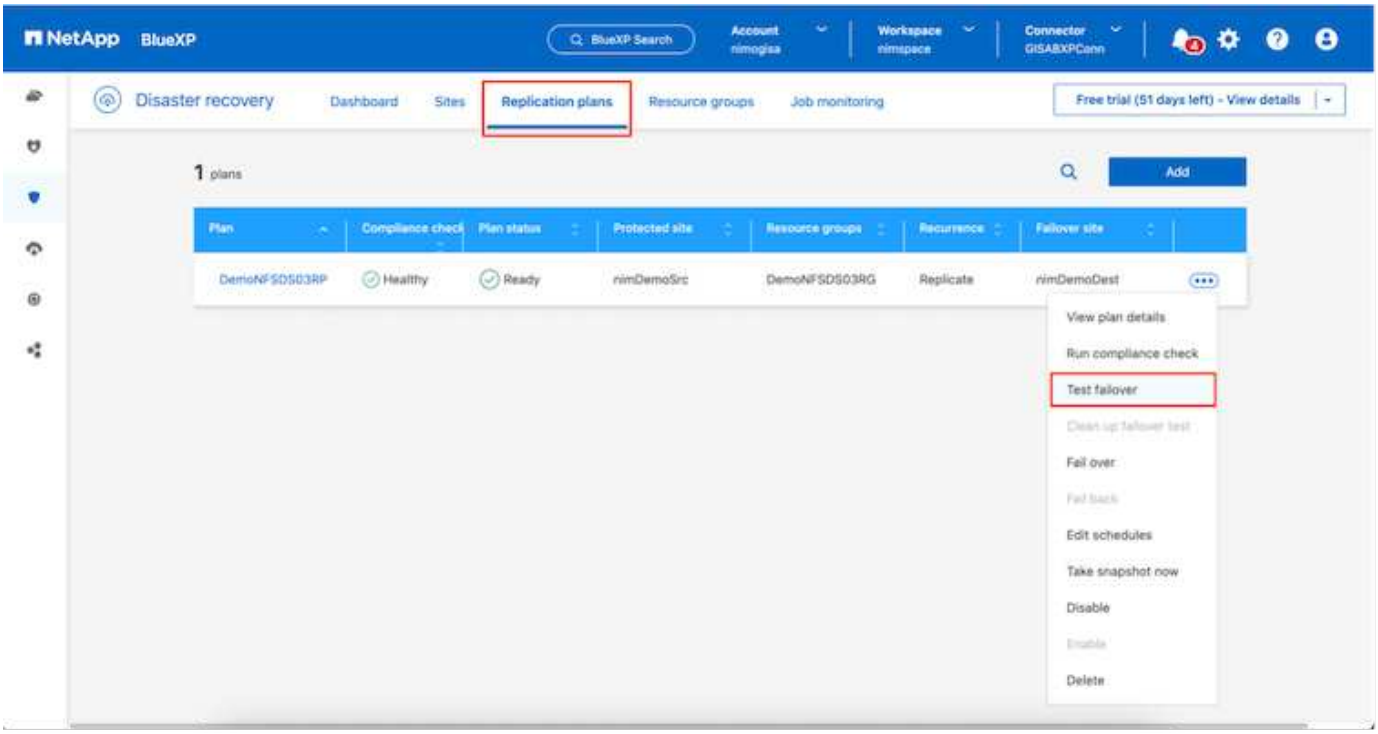


災害復旧は、以下のワークフローで構成されます：

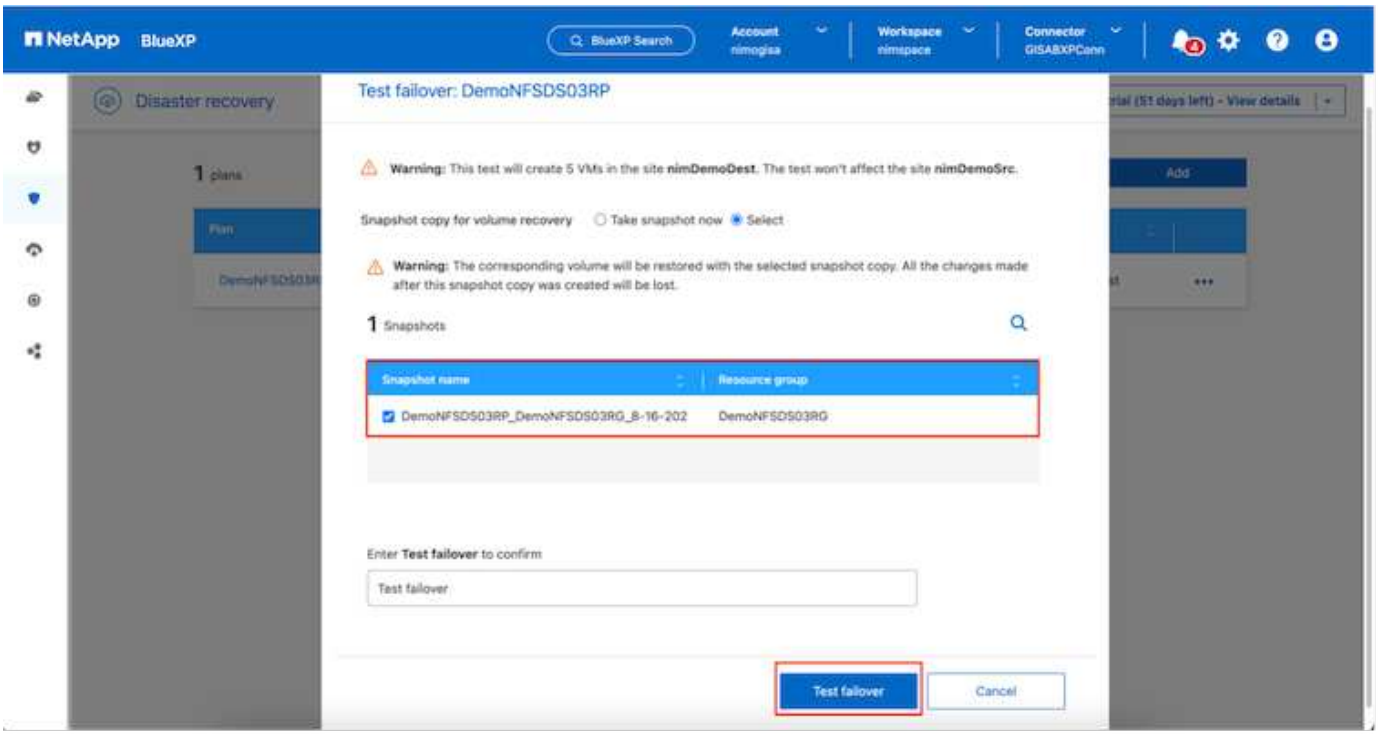
- テストフェイルオーバー（定期的な自動シミュレーションを含む）
- クリーンアップフェイルオーバーテスト
- フェイルオーバー
- フェイルバック

テストフェイルオーバー

Disaster Recoveryでのテストフェイルオーバーは、VMware管理者が本番環境を中断することなくリカバリプランを完全に検証できるようにする運用手順です。テストフェイルオーバー中、Disaster Recoveryは、DRストレージシステム上のレプリケートされたNFSデータストアボリュームの、スペース効率に優れたNetApp FlexCloneコピーを作成します。その後、これらのFlexCloneボリュームはDRサイトのESXiホストにマウントされ、VMは隔離されたテストネットワーク内で電源がオンになります。このプロセスにより、管理者は、実際の災害発生時にディザスタリカバリプランが意図したとおりに機能することを検証できます。



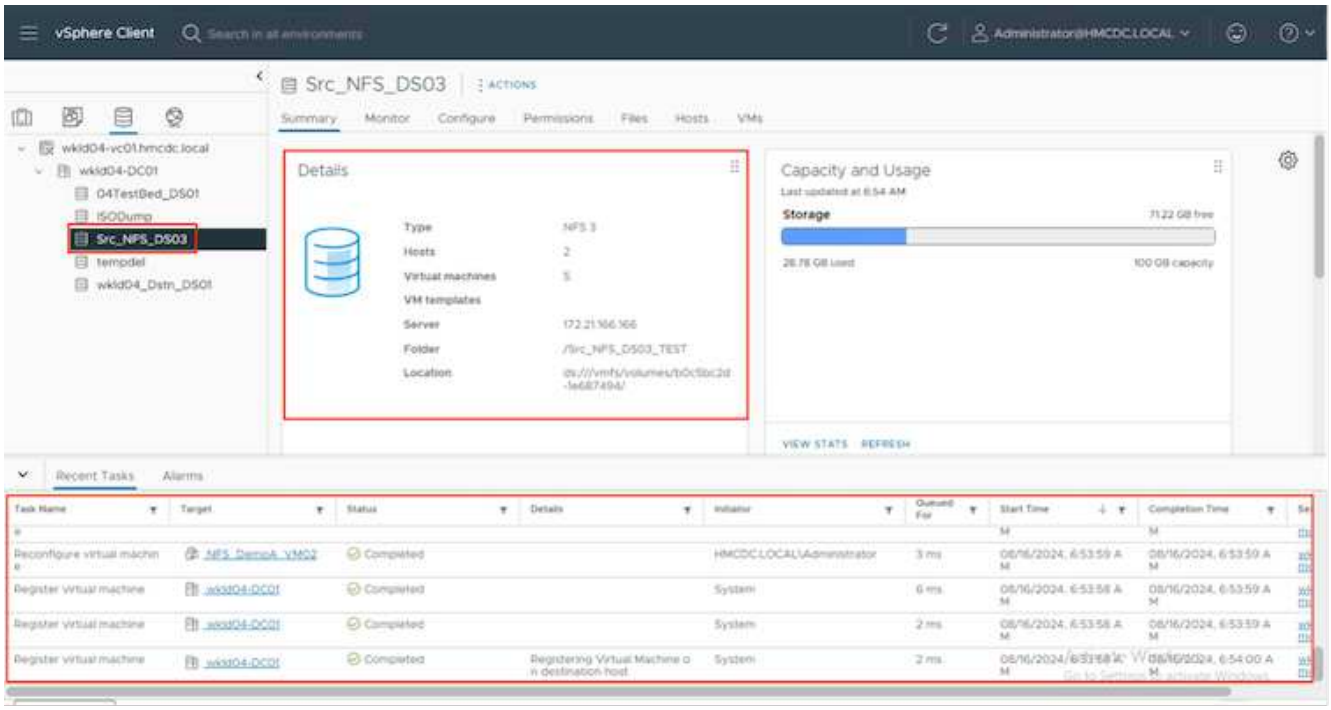
Disaster Recoveryには、テストフェイルオーバー操作においてスナップショットをオプション機能として選択できる機能が組み込まれています。この機能により、VMware管理者は、環境内で最近行われた変更が宛先サイトに複製され、テスト中に反映されていることを確認できます。こうした変更には、VMゲストオペレーティングシステムへのパッチが含まれます



VMware管理者がテストフェイルオーバー操作を実行すると、Disaster Recoveryは次のタスクを自動化します：

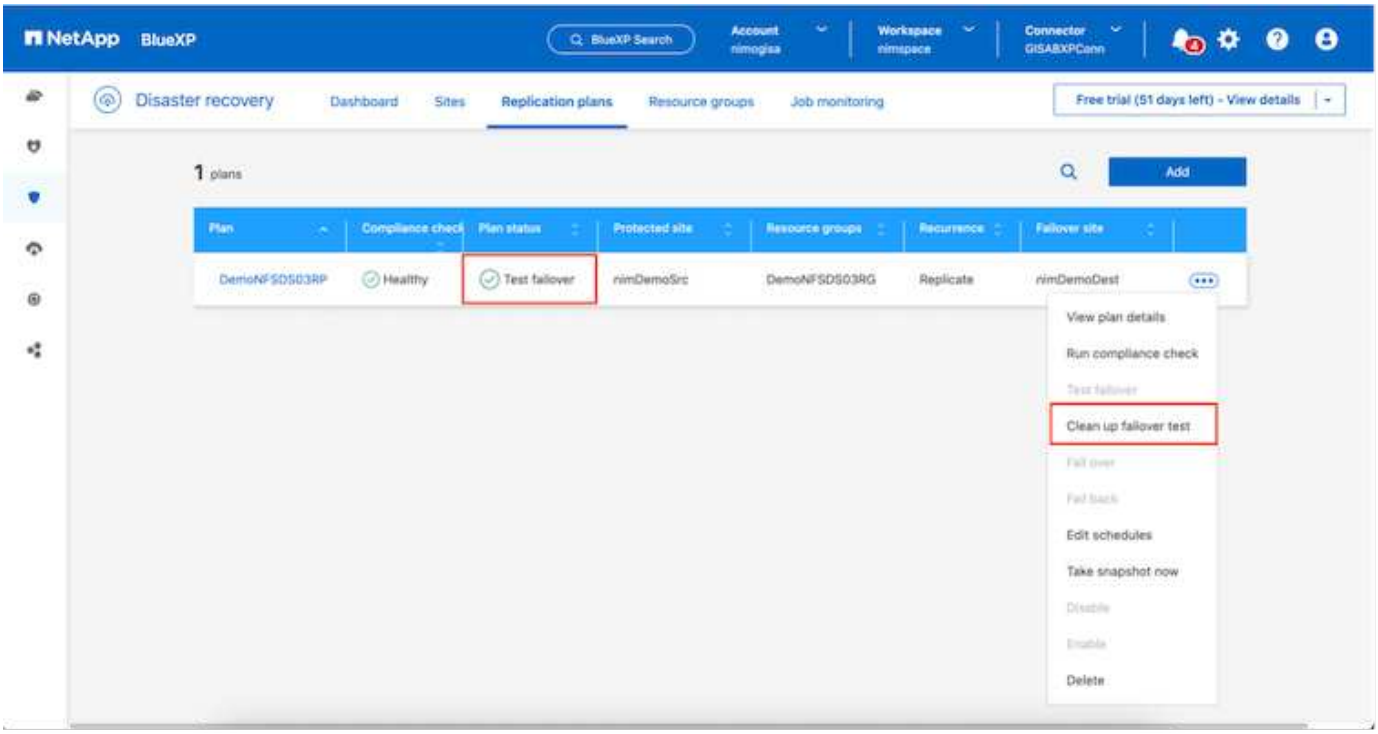
- SnapMirror関係をトリガーして、本番サイトで行われた最近の変更を宛先サイトのストレージに反映します。

- DR ストレージ アレイ上のFlexVolボリュームのNetApp FlexCloneボリュームを作成します。
- FlexCloneボリューム内の NFS データストアを DR サイトの ESXi ホストに接続します。
- マッピング中に指定されたテスト ネットワークに VM ネットワーク アダプターを接続します。
- DR サイトのネットワークの定義に従って、VM ゲスト オペレーティング システムのネットワーク設定を再構成します。
- レプリケーション プランに保存されているカスタム コマンドを実行します。
- レプリケーション プランで定義された順序で VM の電源をオンにします。



クリーンアップフェイルオーバーテスト操作

クリーンアップ フェイルオーバー テスト操作は、レプリケーション プラン テストが完了し、VMware 管理者がクリーンアップ プロンプトに応答した後に実行されます。



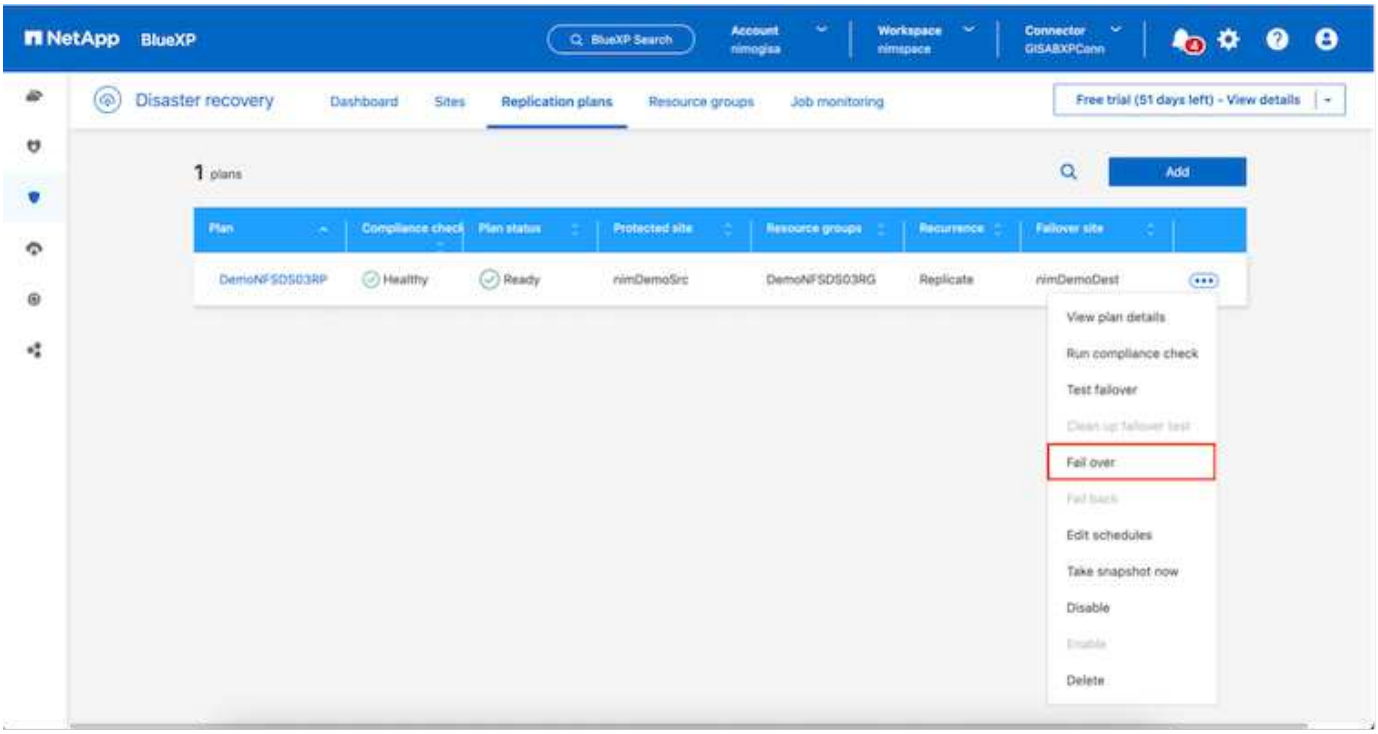
このアクションにより、仮想マシン (VM) とレプリケーション プランのステータスが準備完了状態にリセットされます。

VMware管理者が復旧操作を実行すると、Disaster Recoveryは以下のプロセスを完了します：

1. テストに使用されたFlexCloneコピー内の回復された各 VM の電源をオフにします。
2. テスト中に回復された VM を表示するために使用されたFlexCloneボリュームを削除します。

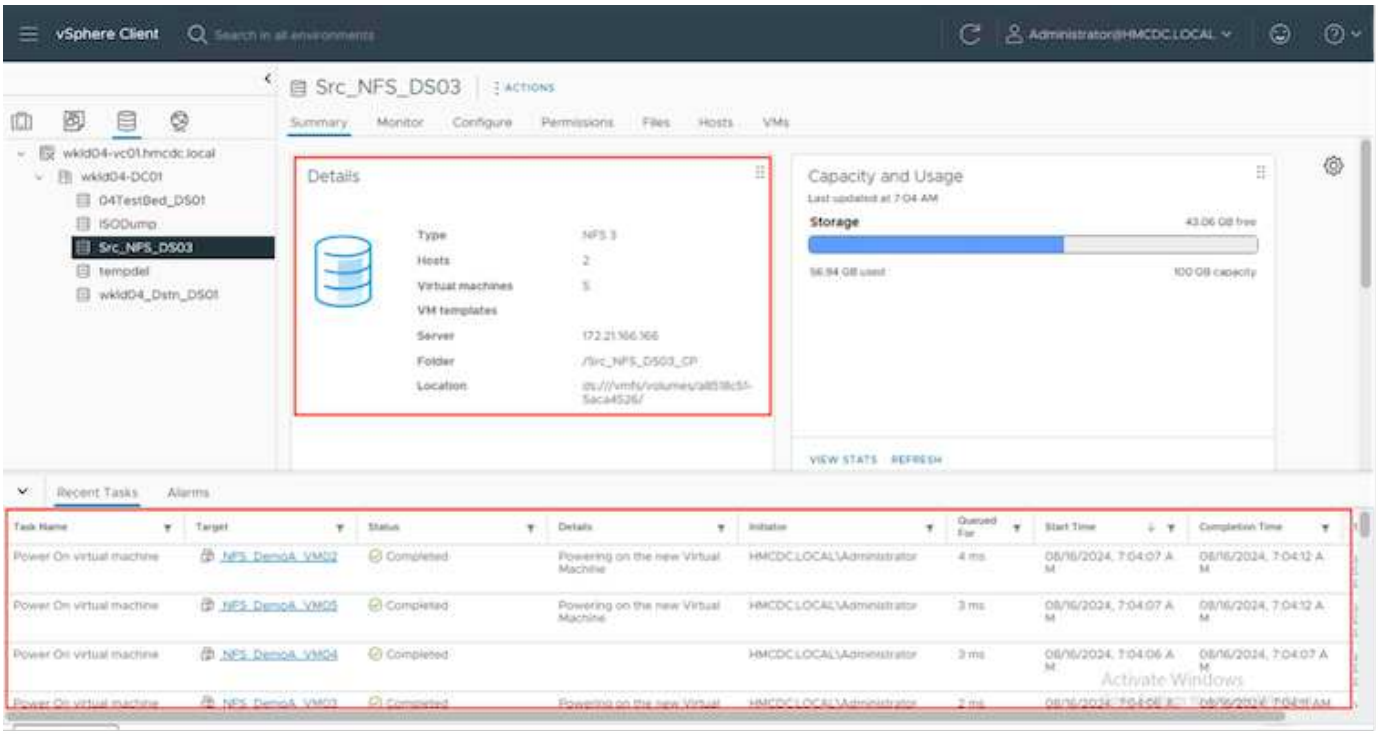
計画的な移行とフェイルオーバー

災害復旧には、実際のフェイルオーバーを実行するための2つの方法があります：計画的移行とフェイルオーバー。最初の方法である計画的移行では、VMのシャットダウンとストレージレプリケーションの同期をプロセスに組み込み、VMを移行先サイトに復旧または効果的に移動します。計画的移行には、移行元サイトへのアクセスが必要です。2つ目の方法であるフェイルオーバーは、計画的または計画外のフェイルオーバーであり、正常に完了した最後のストレージレプリケーション間隔から、移行先サイトでVMが復旧されます。ソリューションに設計されたRPOによっては、DRシナリオにおいてある程度のデータ損失が予想されます。



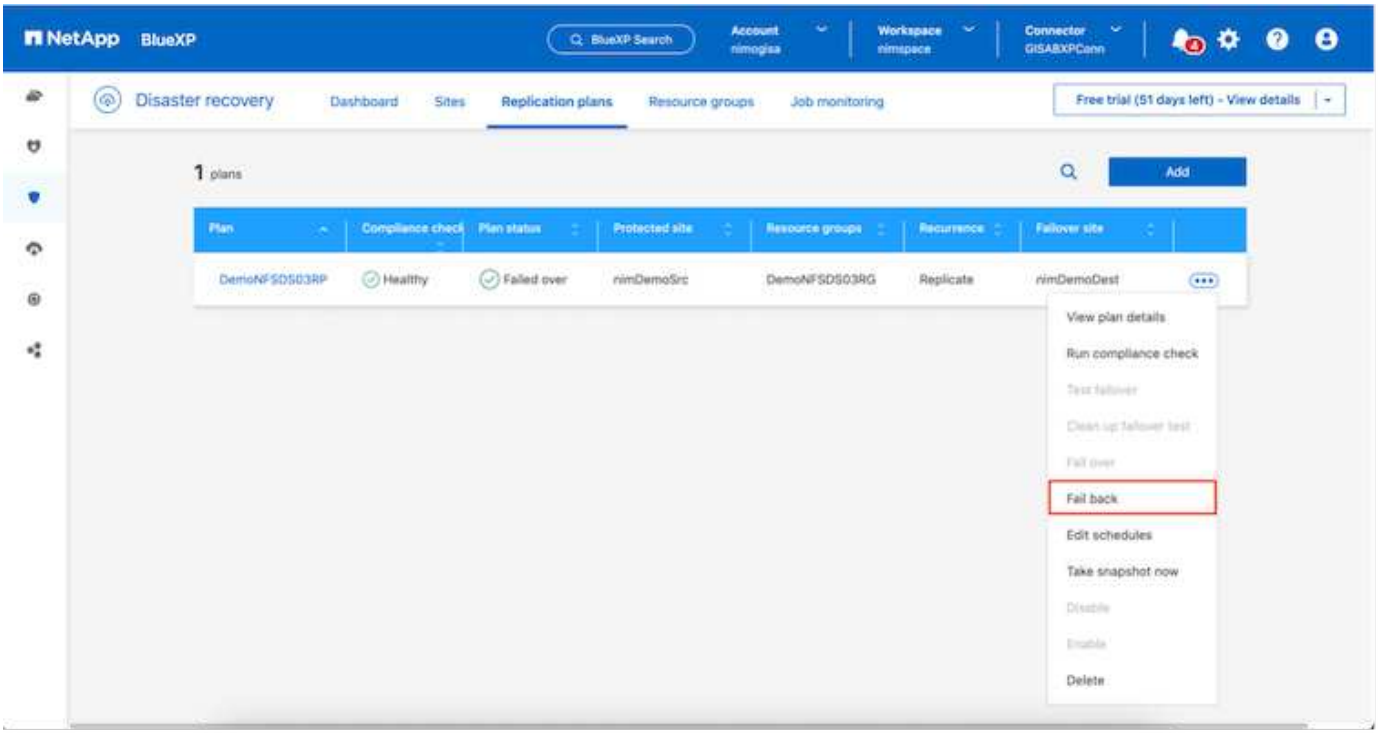
VMware管理者がフェイルオーバー操作を実行すると、Disaster Recoveryは以下のタスクを自動化します：

- NetApp SnapMirror関係を解除してフェイルオーバーします。
- 複製された NFS データストアを DR サイトの ESXi ホストに接続します。
- VM ネットワーク アダプターを適切な宛先サイト ネットワークに接続します。
- 宛先サイトのネットワークの定義に従って、VM ゲスト オペレーティング システムのネットワーク設定を再構成します。
- レプリケーション プランに保存されているカスタム コマンド (存在する場合) を実行します。
- レプリケーション プランで定義された順序で VM の電源をオンにします。



フェイルバック

フェイルバックは、回復後にソース サイトと宛先サイトの元の構成を復元するオプションの手順です。



VMware 管理者は、サービスを元のソース サイトに復元する準備ができたら、フェイルバック手順を構成して実行できます。

注： ディザスタリカバリは、レプリケーションの方向を反転する前に、変更内容を元のソース仮想マシンに複製（再同期）します。このプロセスは、ターゲットへのフェイルオーバーが完了した関係から始まり、次の

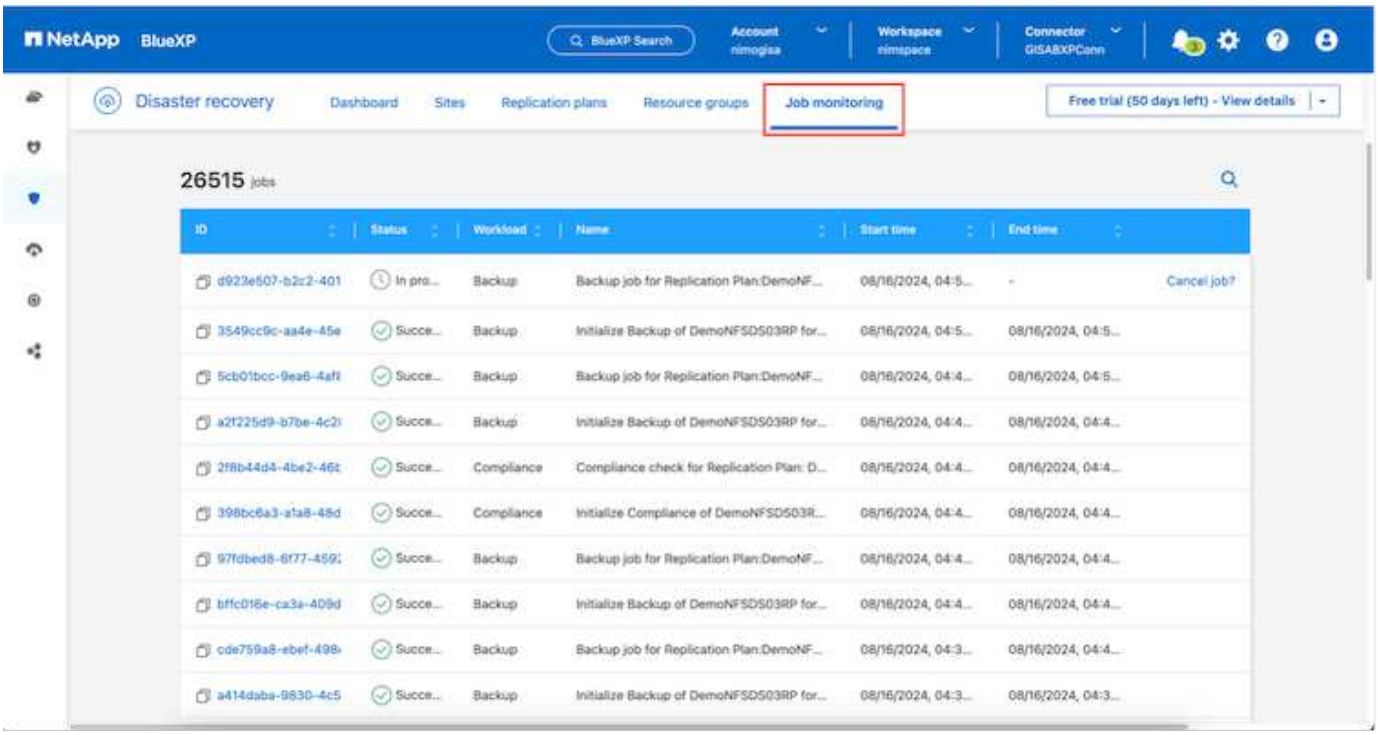
手順が含まれます：

- 仮想マシンの電源をオフにして登録を解除すると、宛先サイトのボリュームがマウント解除されます。
- 元のソースのSnapMirror関係を解除して、読み取り/書き込み可能にします。
- レプリケーションを元に戻すには、 SnapMirror関係を再同期します。
- ソースにボリュームをマウントし、ソース仮想マシンをパワーオンして登録します。

ディザスタリカバリへのアクセスと構成の詳細については、"VMware向けNetApp Disaster Recoveryについて"を参照してください。

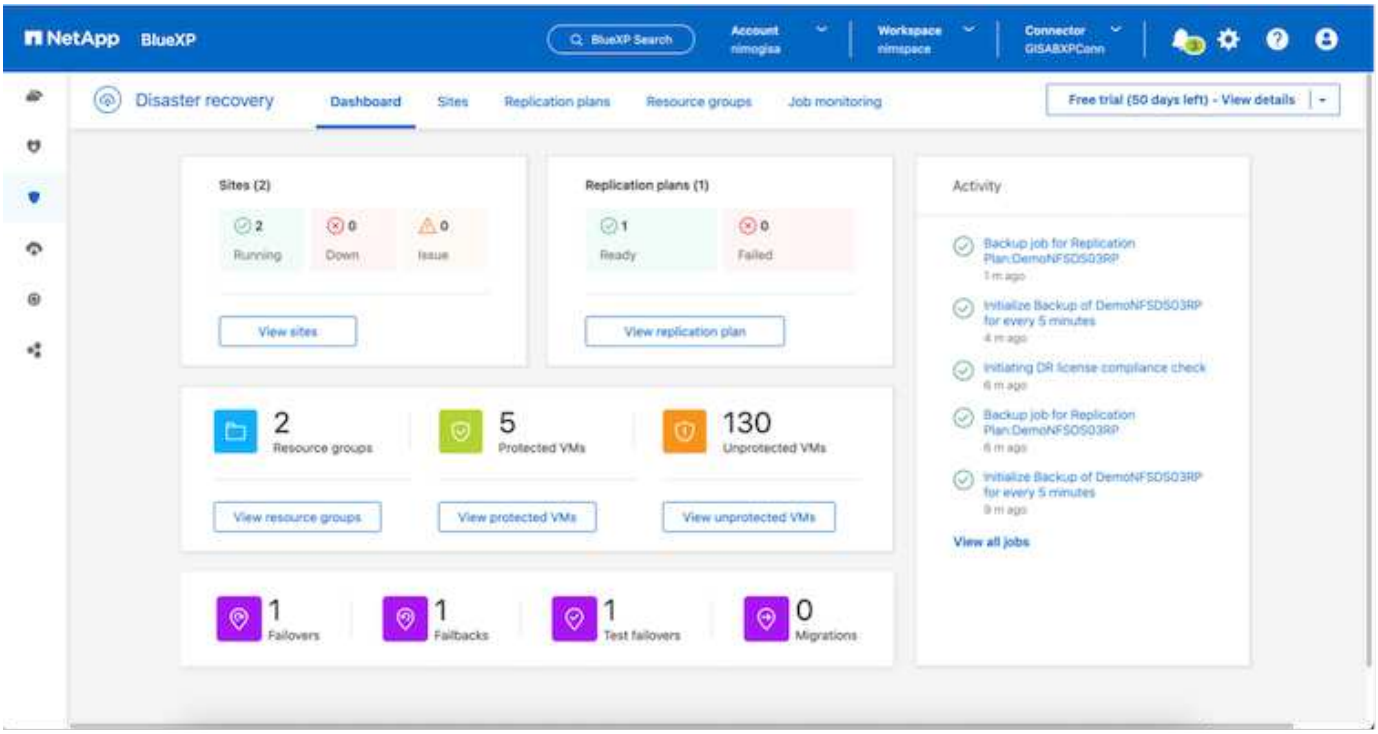
監視とダッシュボード

ConsoleまたはONTAP CLIから、該当するデータストアボリュームのレプリケーションの健全性ステータスを監視でき、フェイルオーバーまたはテストフェイルオーバーのステータスはジョブ監視で追跡できます。



ジョブが現在進行中またはキューに入っており、それを停止したい場合は、キャンセルするオプションがあります。

災害復旧ダッシュボードを使用すれば、災害復旧サイトとレプリケーション計画の状況を自信を持って評価できます。これにより、管理者は正常なサイト、接続が切断されたサイト、または劣化しているサイトやプランを迅速に特定できます。



これにより、調整およびカスタマイズされた災害復旧計画を処理するための強力なソリューションが提供されます。フェイルオーバーは、計画されたフェイルオーバーとして実行することも、災害が発生して DR サイトをアクティブ化する決定が下されたときにボタンをクリックするだけでフェイルオーバーを実行することもできます。

このプロセスについて詳しく知りたい場合は、詳細なウォークスルービデオをご覧いただくか、"ソリューションシミュレータ" 。

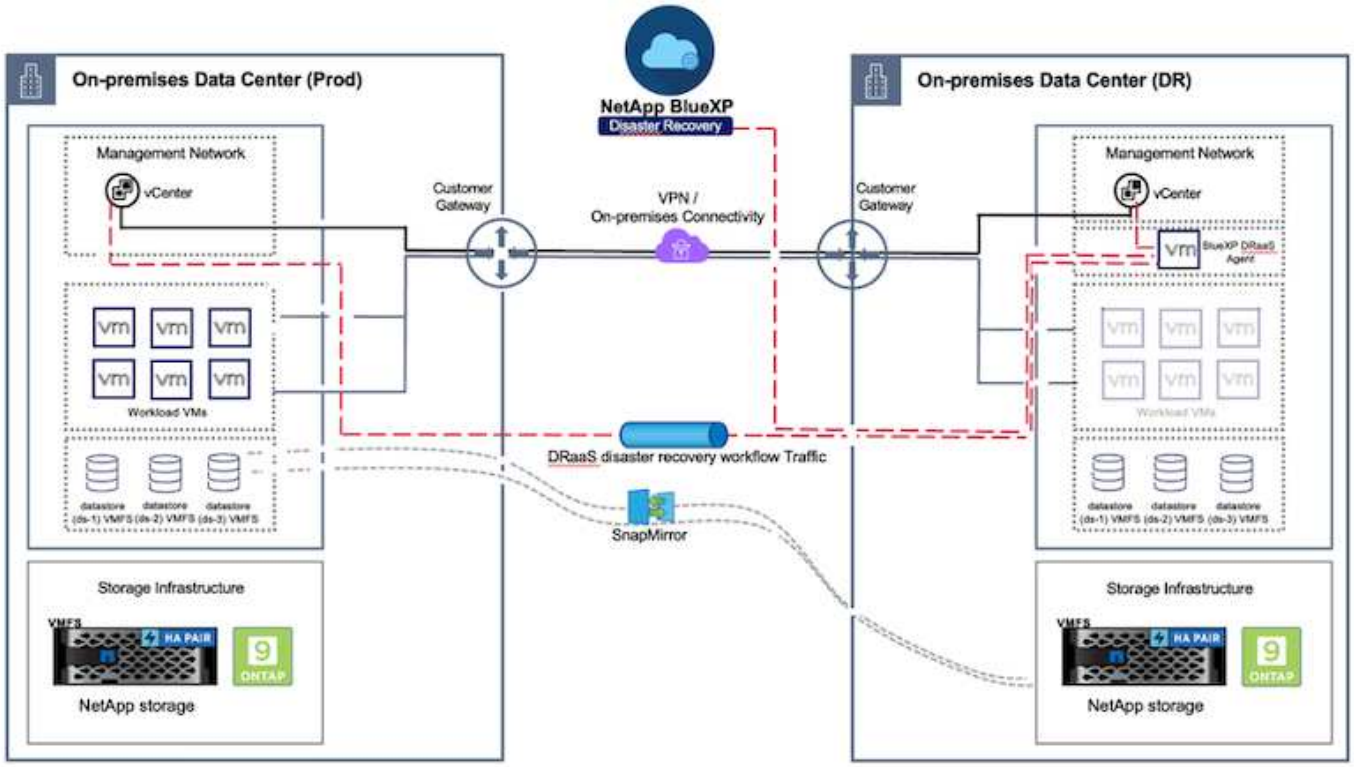
VMFSデータストア向けNetApp Disaster Recovery

運用サイトから災害復旧サイトへのブロックレベルのレプリケーションを使用した災害復旧は、サイトの停止やランサムウェア攻撃などのデータ破損イベントからワークロードを保護する、回復力がありコスト効率に優れた方法です。 NetApp SnapMirrorレプリケーションを使用すると、VMFSデータストアを使用してオンプレミスのONTAPシステムで実行されているVMwareワークロードを、VMwareが存在する指定されたリカバリデータセンター内の別のONTAPストレージシステムに複製できます。

このドキュメントのこのセクションでは、オンプレミスのVMware VMのディザスタリカバリを別の指定サイトにセットアップするためのNetApp Disaster Recoveryの構成について説明します。このセットアップの一環として、Consoleエージェント、ONTAPアレイのオンボーディング、サイトの定義、およびVMware vCenterの関連付けを行います。さらに、このドキュメントでは、サイト間のレプリケーションの設定方法、および復旧計画のセットアップとテスト方法について詳しく説明します。最後のセクションでは、サイト全体のフェイルオーバーを実行する方法と、プライマリサイトが復旧してオンラインになったときにフェイルバックする方法について説明します。

NetApp Data Servicesの一部であるDisaster Recoveryを活用することで、お客様はオンプレミスのVMware vCentersとONTAPストレージを検出し、リソースグループを作成し、ディザスタリカバリ計画を作成してリソースグループに関連付け、フェイルオーバーとフェイルバックのテストまたは実行を行うことができます。SnapMirrorは、ストレージレベルのブロックレプリケーションを提供して、増分変更により2つのサイトを最新の状態に保ち、最大5分のRPOを実現します。また、本番環境やレプリケートされたデータストアに影

響を与えたり、追加のストレージコストを発生させたりすることなく、通常の訓練としてDR手順をシミュレートすることも可能です。NetApp Data Servicesは、ONTAPのFlexCloneテクノロジを活用して、DRサイトで最後にレプリケートされたSnapshotから、スペース効率に優れたVMFSデータストアのコピーを作成します。DRテストが完了すると、お客様はテスト環境を簡単に削除でき、実際のレプリケートされた本番リソースに影響を与えることはありません。実際のフェイルオーバーが必要になった場合（計画的か計画外かを問わず）、数回クリックするだけで、Disaster Recoveryは保護対象の仮想マシンを指定されたディザスタリカバリサイトで自動的に起動するために必要なすべての手順をオーケストレーションします。また、このサービスは、必要に応じてプライマリサイトへのSnapMirror関係を反転させ、フェイルバック処理のためにセカンダリからプライマリへ変更をレプリケートします。これらはすべて、他のよく知られた代替手段と比較して、わずかなコストで実現できます。

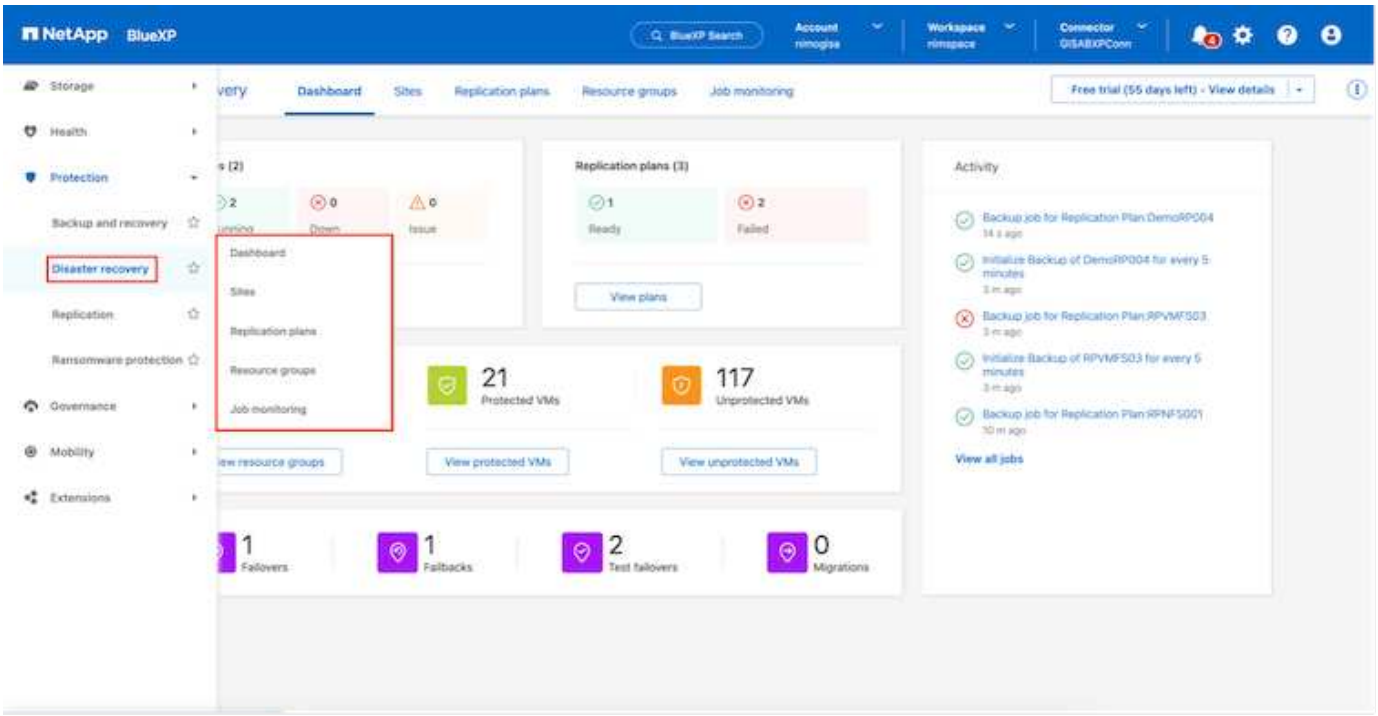


ディザスタリカバリ向けのvCenter Server、ESXi、およびONTAPの最新情報とサポートされるバージョンについては、"災害復旧のサポート対象構成"を参照してください。

開始

ディザスタリカバリを開始するには、NetApp Consoleを使用してサービスにアクセスします。

1. Consoleにログインします。
2. Consoleの左側のナビゲーションから、「保護」>「災害復旧」を選択します。
3. 災害復旧ダッシュボードが表示されます。

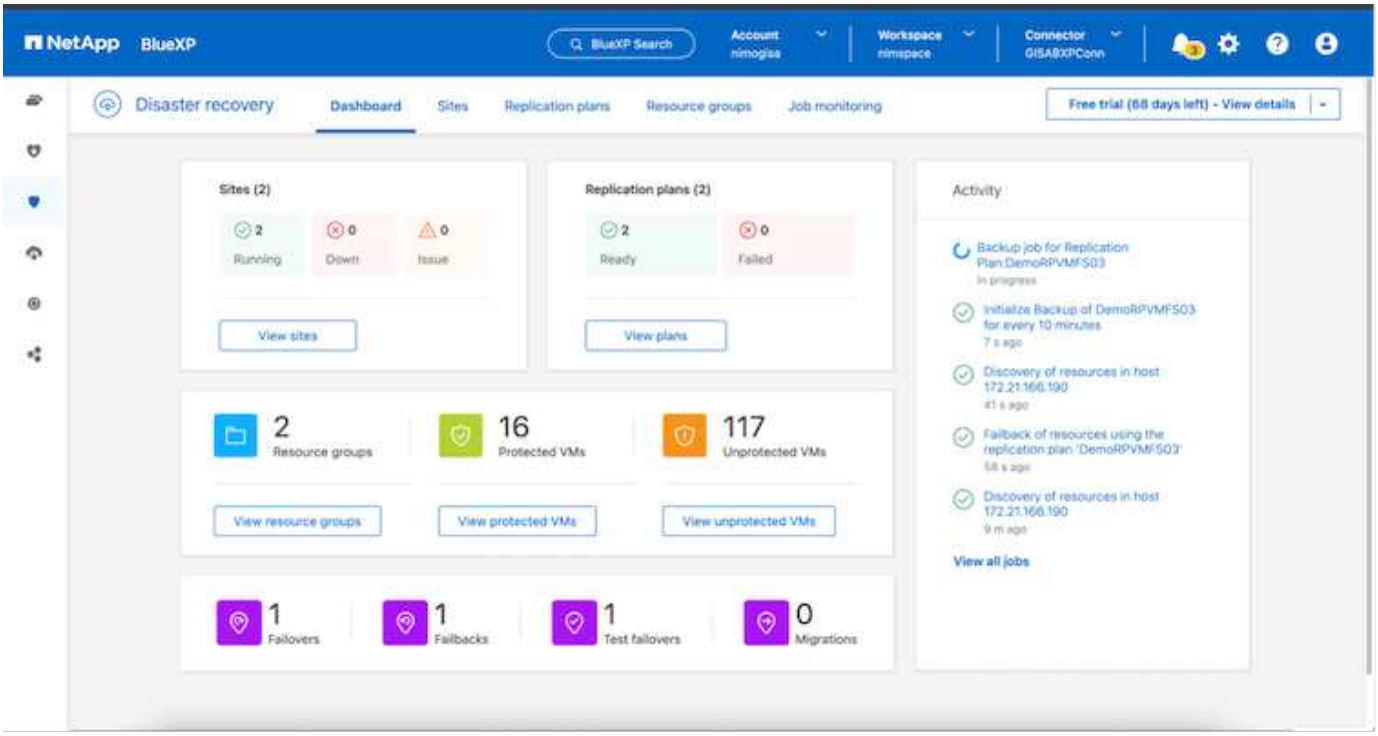


災害復旧計画を構成する前に、次の前提条件が満たされていることを確認してください。

- ConsoleエージェントはAWS VPCにデプロイされています。
- Consoleエージェントインスタンスは、送信元と宛先のvCenterおよびストレージシステムへの接続性を備えています。
- VMware用のVMFSデータストアをホストするオンプレミスのNetAppストレージシステムがConsoleに追加されます。
- 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。
- 指定された VMFS ベースのデータストア ボリュームに対してSnapMirrorレプリケーションが構成されます。

ソース サイトと宛先サイト間の接続が確立されたら、構成手順に進みます。これには約 3 ～ 5 分かかります。

NetAppは、実際の障害や自然災害の発生時にConsoleエージェントがネットワークを介して送信元および宛先のリソースと通信できるように、Consoleエージェントを災害復旧サイトまたは第3のサイトに導入することを推奨しています。

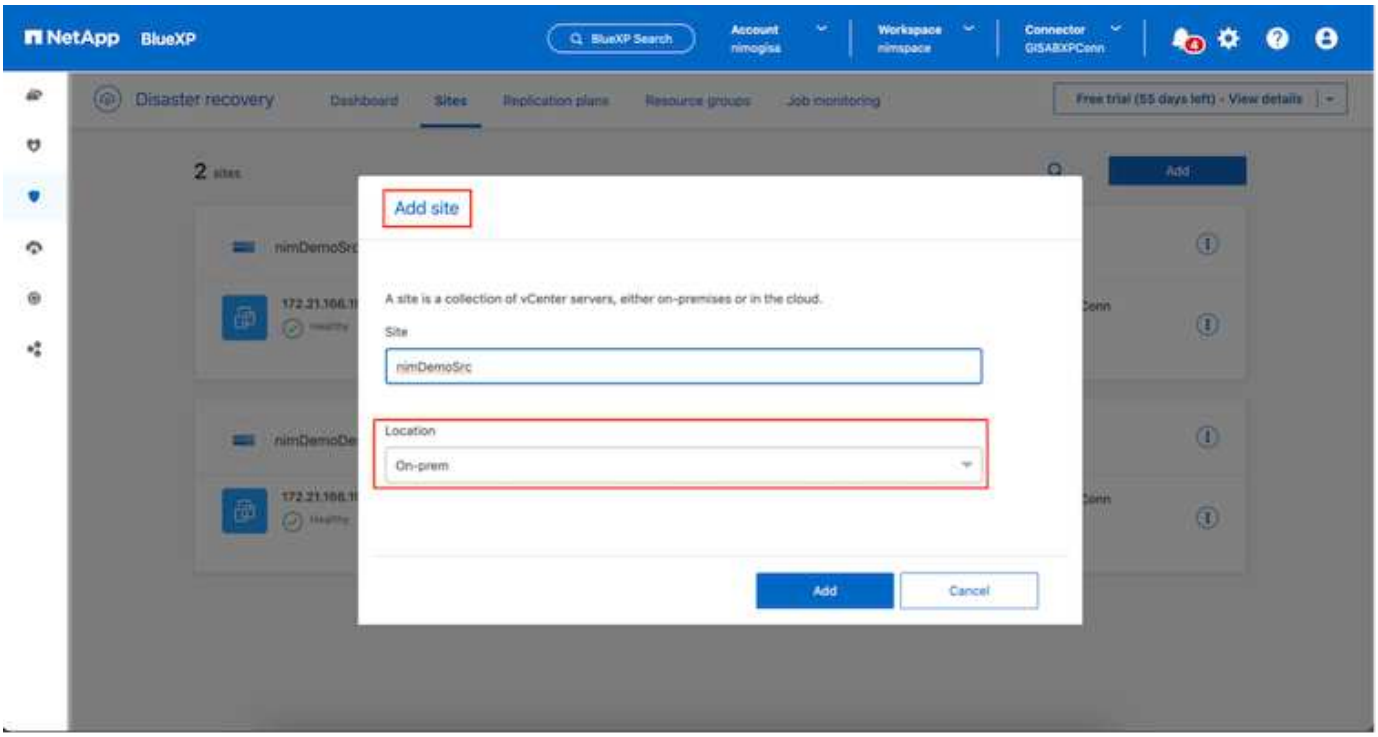


このドキュメントの執筆時点では、オンプレミスからオンプレミスへの VMFS データストアのサポートはテクノロジー プレビュー段階です。この機能は、FC および ISCSI プロトコル ベースの VMFS データストアの両方でサポートされます。

災害復旧構成

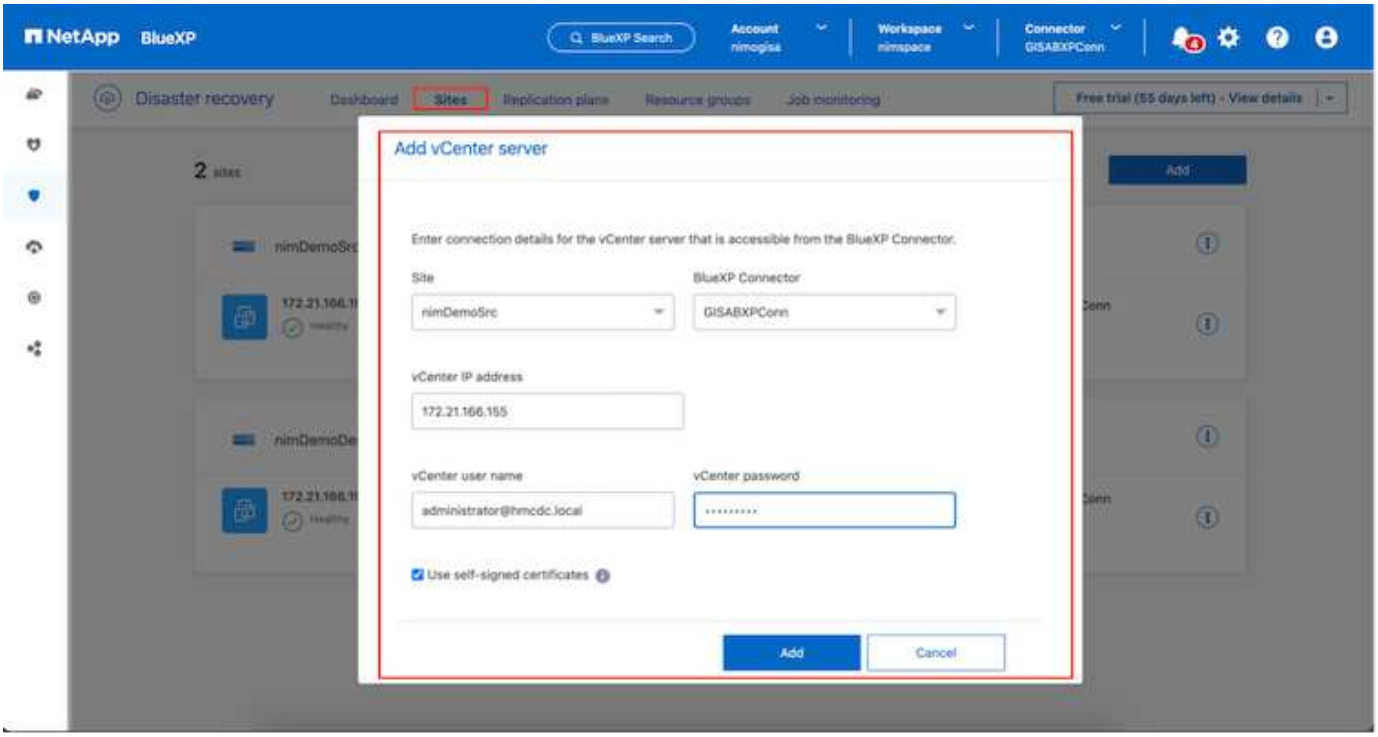
ディザスタリカバリの準備の最初のステップは、オンプレミスのvCenterおよびストレージリソースを検出してDisaster Recoveryに追加することです。

ONTAPストレージシステムがキャンバス内の作業環境に追加されていることを確認します。Consoleを開き、左側のナビゲーションから*保護 > 災害復旧*を選択します。*vCenterサーバーの検出*を選択するか、トップメニューを使用して*サイト > 追加 > vCenterの追加*を選択します。

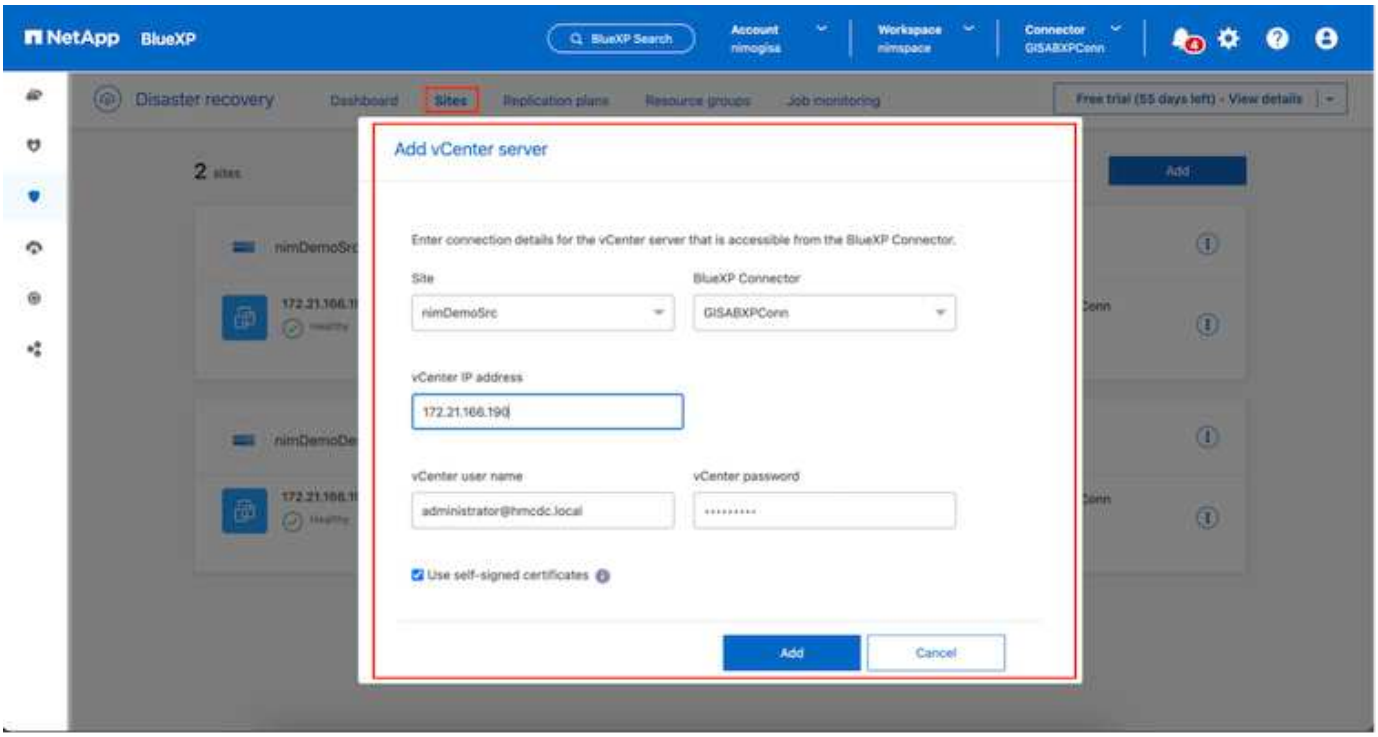


次のプラットフォームを追加します。

- ソース。オンプレミスの vCenter。



- 行き先。 VMC SDDC vCenter。



vCenter が追加されると、自動検出がトリガーされます。

ソースサイトと宛先サイト間のストレージレプリケーションの構成

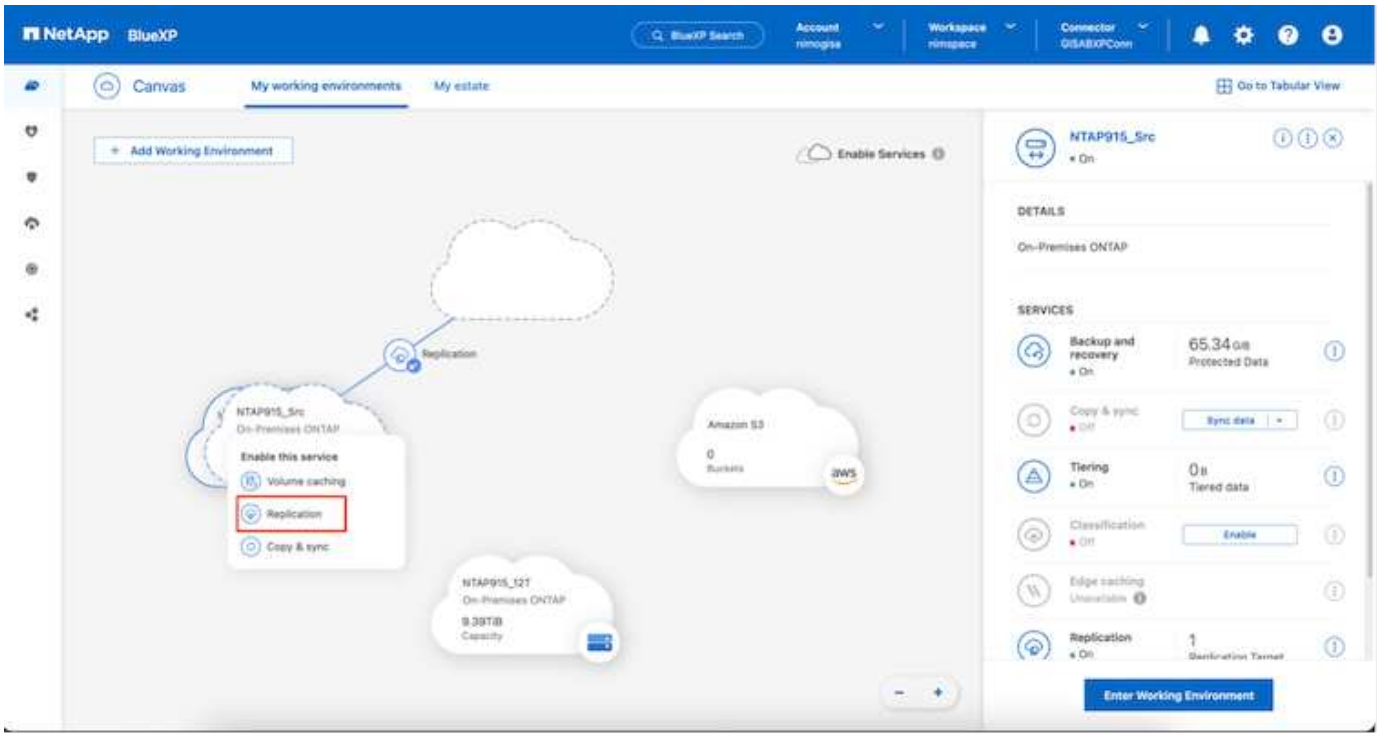
SnapMirror はONTAPスナップショットを利用して、ある場所から別の場所へのデータの転送を管理します。最初に、ソース ボリュームのスナップショットに基づく完全なコピーが宛先にコピーされ、ベースライン同期が実行されます。ソースでデータの変更が発生すると、新しいスナップショットが作成され、ベースラインスナップショットと比較されます。変更されたと判明したブロックは宛先に複製され、新しいスナップショットが現在のベースライン、つまり最新の共通スナップショットになります。これにより、プロセスを繰り返し、増分更新を宛先に送信できるようになります。

SnapMirror関係が確立されると、宛先ボリュームはオンライン読み取り専用状態になり、引き続きアクセス可能になります。 SnapMirror は、ファイルやその他の論理レベルではなく、ストレージの物理ブロックで動作します。つまり、複製先ボリュームは、スナップショット、ボリューム設定などを含め、複製元ボリュームと同一のレプリカになります。データ圧縮やデータ重複排除などのONTAPスペース効率機能が複製元ボリュームで使用されている場合、複製されたボリュームではこれらの最適化が保持されます。

SnapMirror関係を解除すると、宛先ボリュームが書き込み可能になり、通常はSnapMirrorを使用して DR 環境にデータを同期しているときにフェイルオーバーを実行するために使用されます。 SnapMirror は非常に洗練されており、フェイルオーバー サイトで変更されたデータをプライマリ システムに効率的に再同期し、プライマリ システムが後でオンラインに戻ったときに、元のSnapMirror関係を再確立することができます。

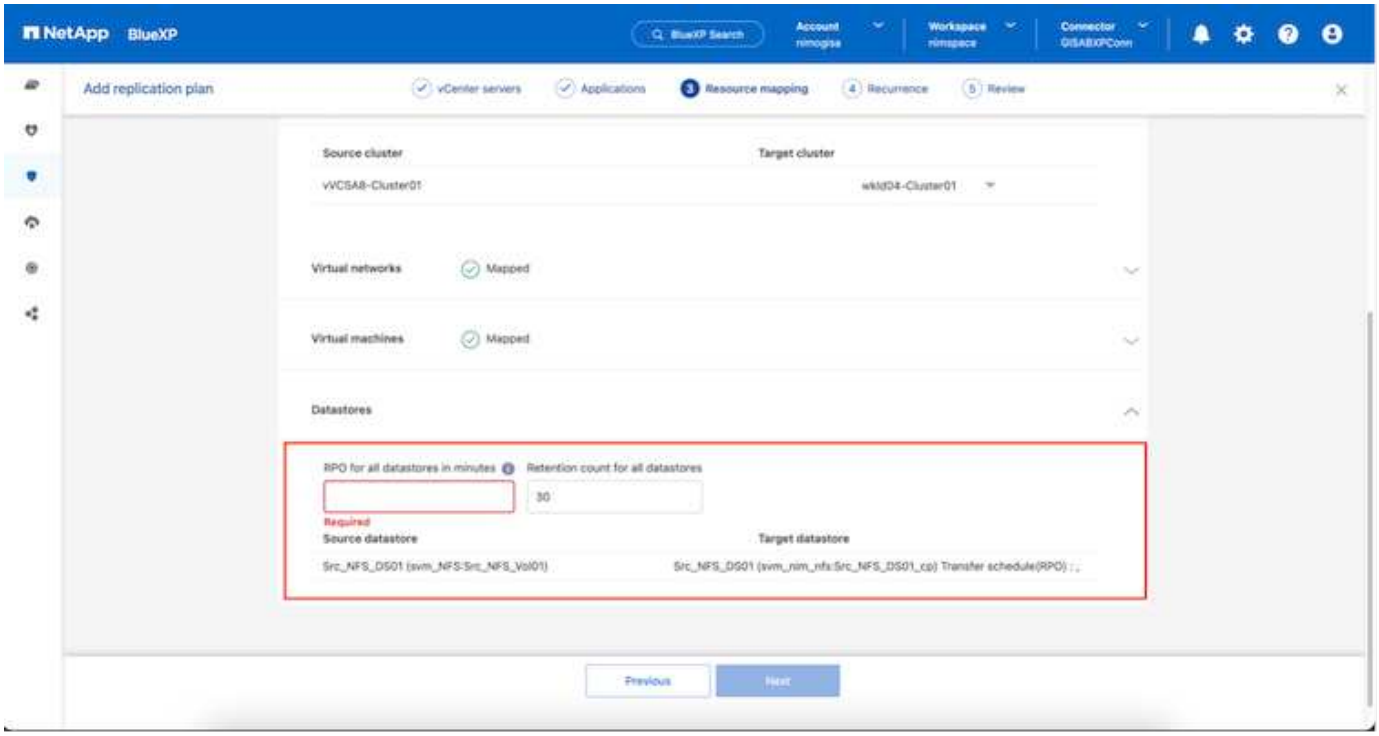
VMware Disaster Recoveryの設定方法

SnapMirrorレプリケーションを作成するプロセスは、どのアプリケーションでも同じです。プロセスは手動または自動で行うことができます。最も簡単な方法は、Consoleを活用してSnapMirrorレプリケーションを設定することです。環境内のソースONTAPシステムを宛先にドラッグ＆ドロップするだけで、残りのプロセスをガイドするウィザードが起動します。



NetApp Data Servicesも、以下の2つの条件を満たせば、同様の処理を自動化できます：

- ソース クラスターと宛先クラスターにはピア関係があります。
- ソース SVM と宛先 SVM にはピア関係があります。

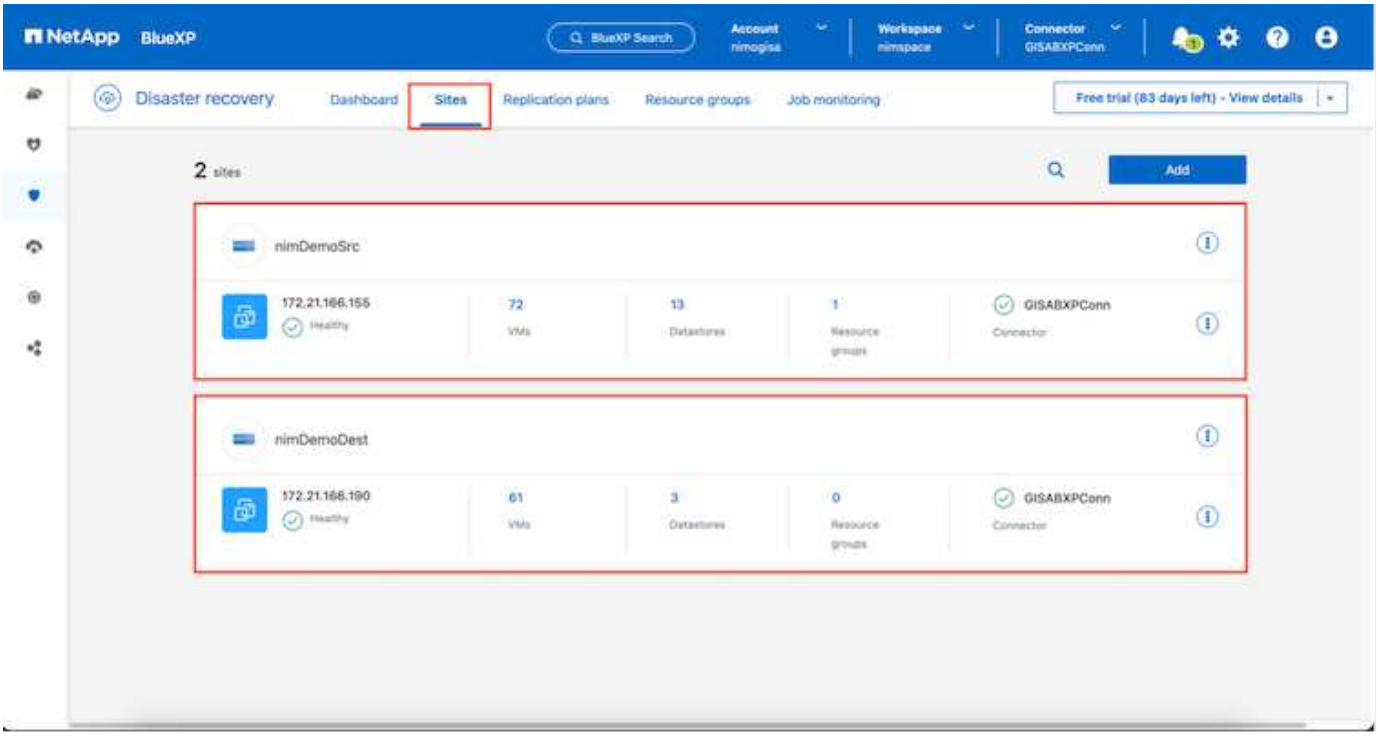


CLIを使用してボリュームにSnapMirror関係がすでに設定されている場合、Consoleはその関係を認識し、残りのワークフロー操作を続行します。

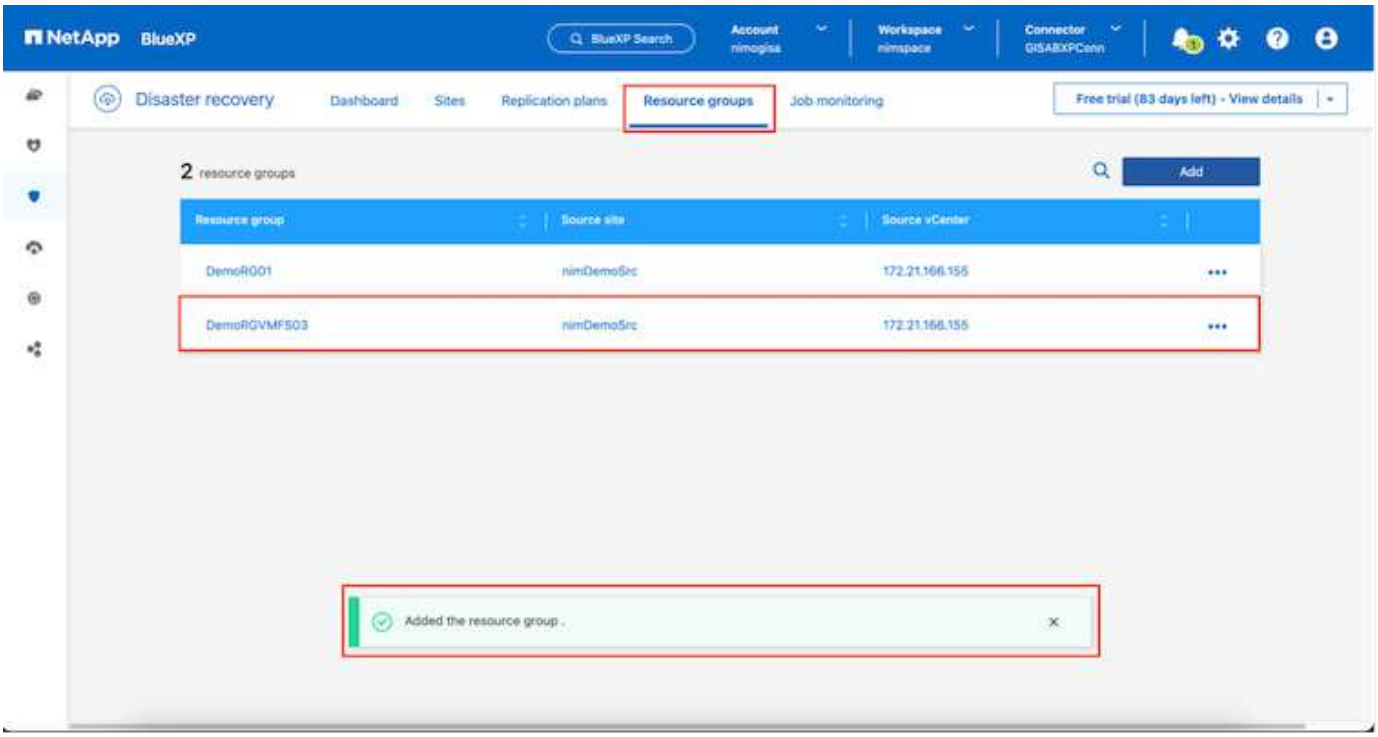
上記のアプローチとは別に、SnapMirrorレプリケーションはONTAP CLIやSystem Managerを使用して作成することもできます。SnapMirrorを使用してデータを同期するアプローチに関係なく、Disaster Recoveryは、シームレスかつ効率的なディザスタリカバリ処理のためのワークフローをオーケストレーションします。

Disaster Recoveryはお客様にどのようなメリットをもたらすのでしょうか？

ソースサイトと宛先サイトが追加されると、Disaster Recoveryは自動的に詳細な検出を実行し、VMsと関連するメタデータを表示します。また、Disaster Recoveryは、VMs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、それらを設定します。

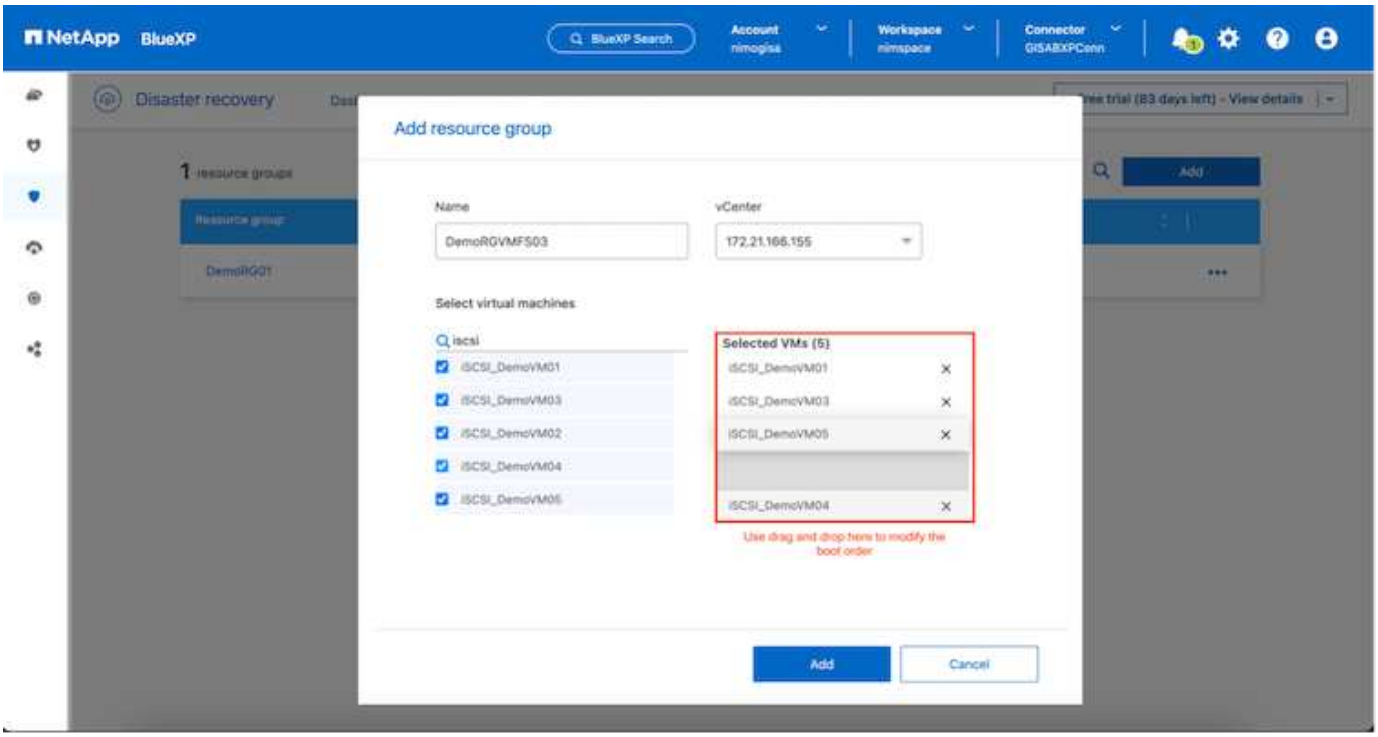


サイトが追加された後、仮想マシンをリソースグループにグループ化できます。ディザスタリカバリのリソースグループを使用すると、依存関係のある仮想マシンを論理グループにまとめることができ、各グループにはリカバリ時に実行できる起動順序と起動遅延が含まれます。リソースグループの作成を開始するには、「リソースグループ」に移動し、「新しいリソースグループの作成」をクリックします。

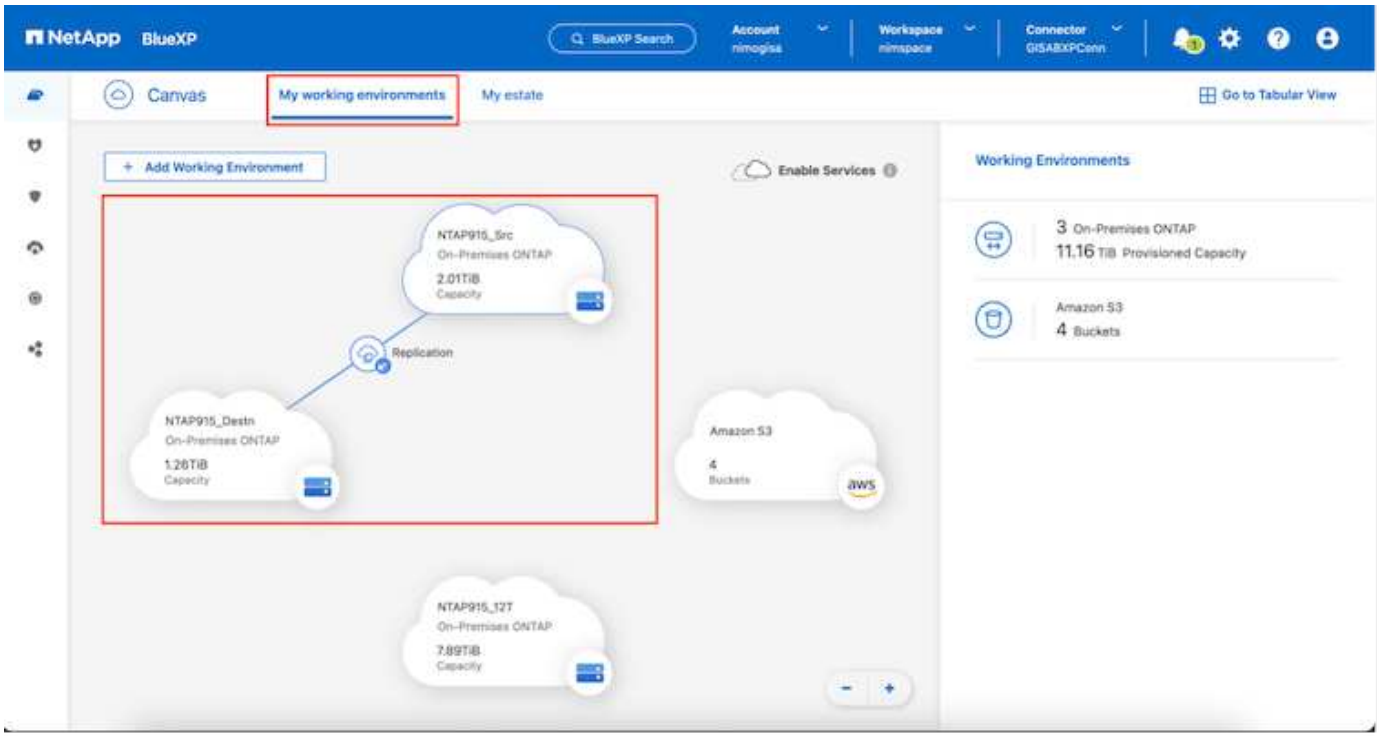


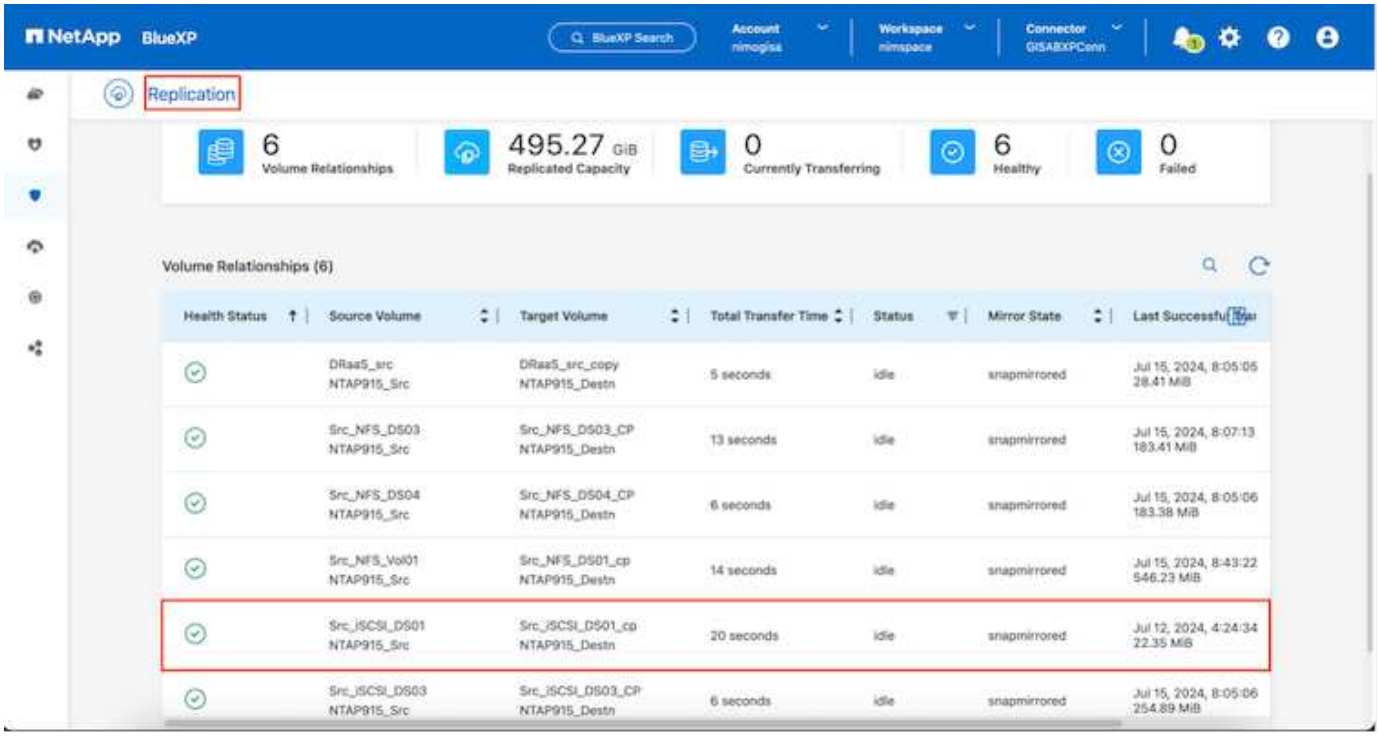
レプリケーション プランの作成時にリソース グループを作成することもできます。

VM のブート順序は、リソース グループの作成中に、簡単なドラッグ アンド ドロップ メカニズムを使用して定義または変更できます。



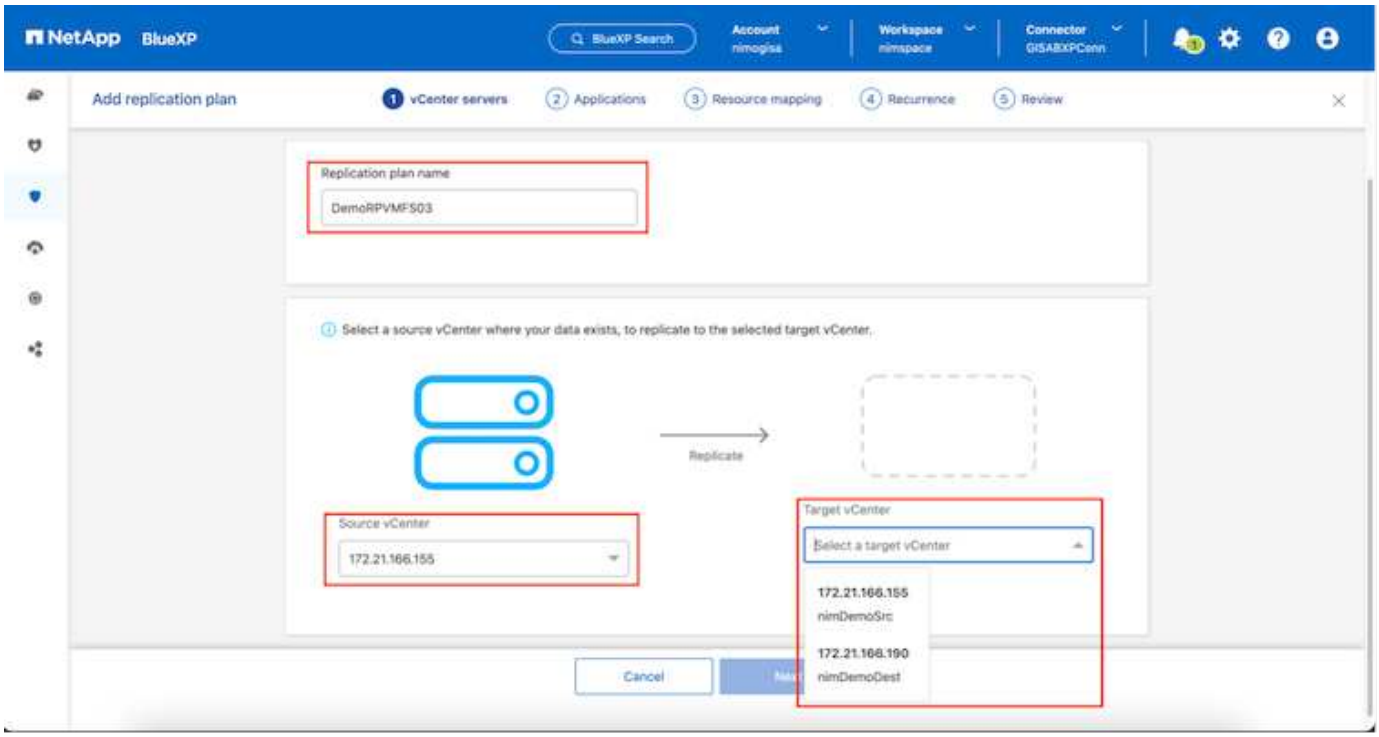
リソース グループを作成したら、次のステップは、災害発生時に仮想マシンとアプリケーションを復旧するための実行ブループリントまたは計画を作成することです。前提条件で述べたように、 SnapMirrorレプリケーションは事前に構成することも、レプリケーション プランの作成時に指定された RPO と保持数を使用して DRaaS で構成することもできます。



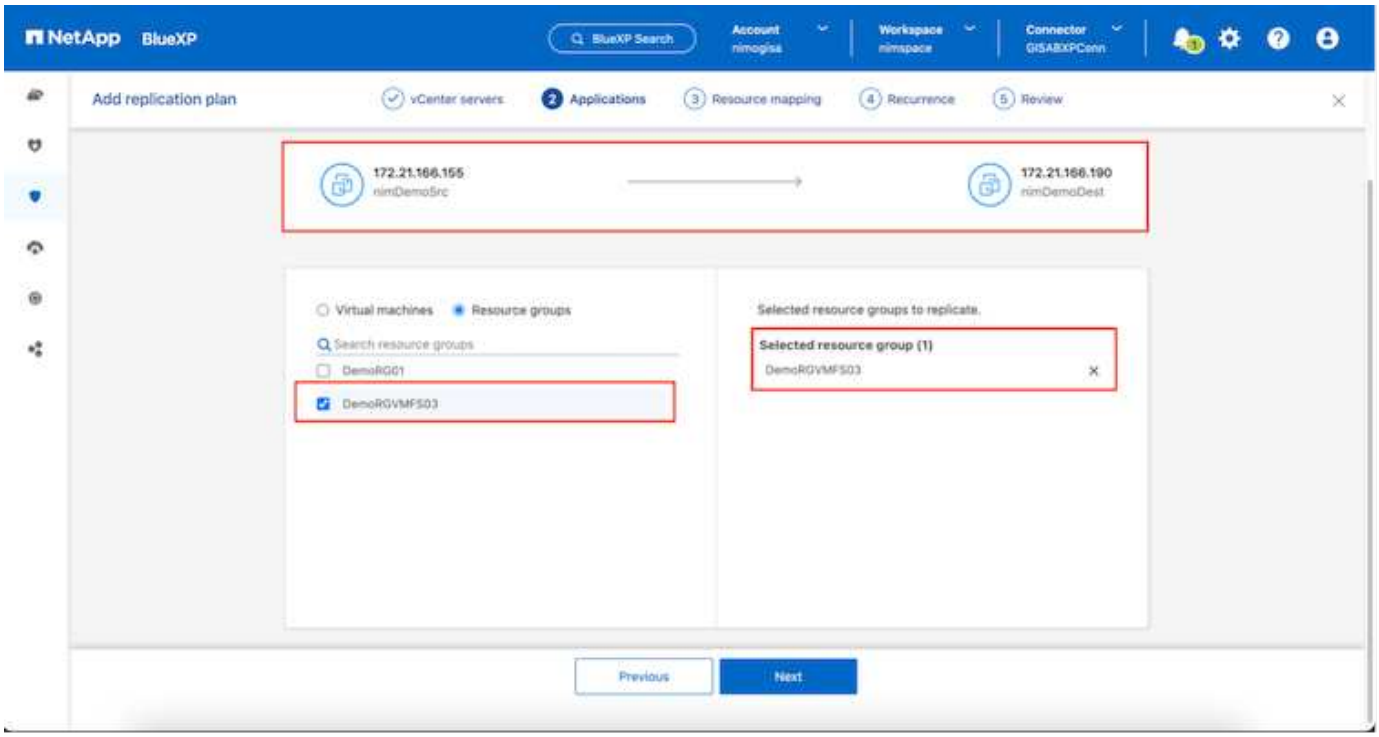


ドロップダウンからソースと宛先の vCenter プラットフォームを選択してレプリケーション プランを構成し、プランに含めるリソース グループ、アプリケーションの復元方法と電源オン方法のグループ化、およびクラスタとネットワークのマッピングを選択します。リカバリ プランを定義するには、[レプリケーション プラン] タブに移動し、[プランの追加] をクリックします。

まず、ソース vCenter を選択し、次に宛先 vCenter を選択します。



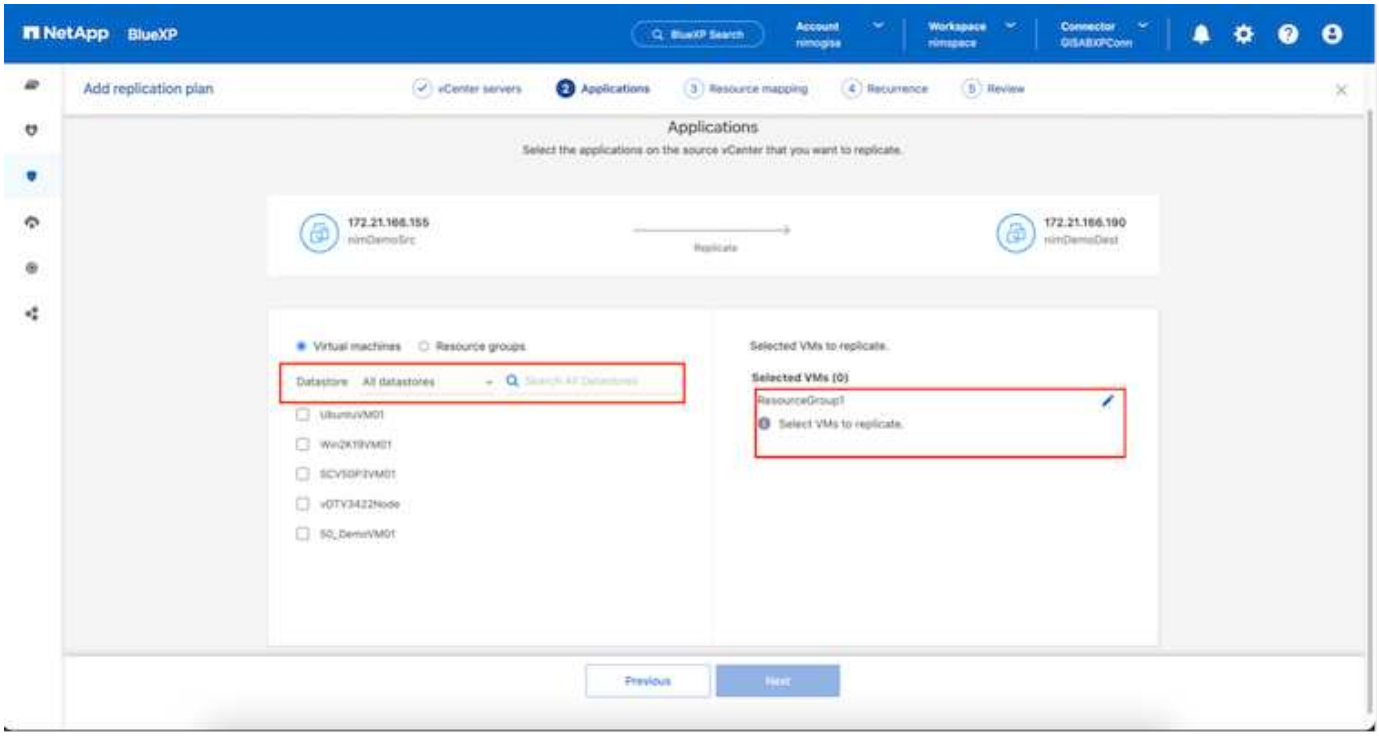
次のステップは、既存のリソース グループを選択することです。リソース グループが作成されていない場合、ウィザードは、回復目標に基づいて必要な仮想マシンをグループ化します (基本的には機能リソース グループを作成します)。これは、アプリケーション仮想マシンを復元する操作シーケンスを定義するのにも役立ちます。



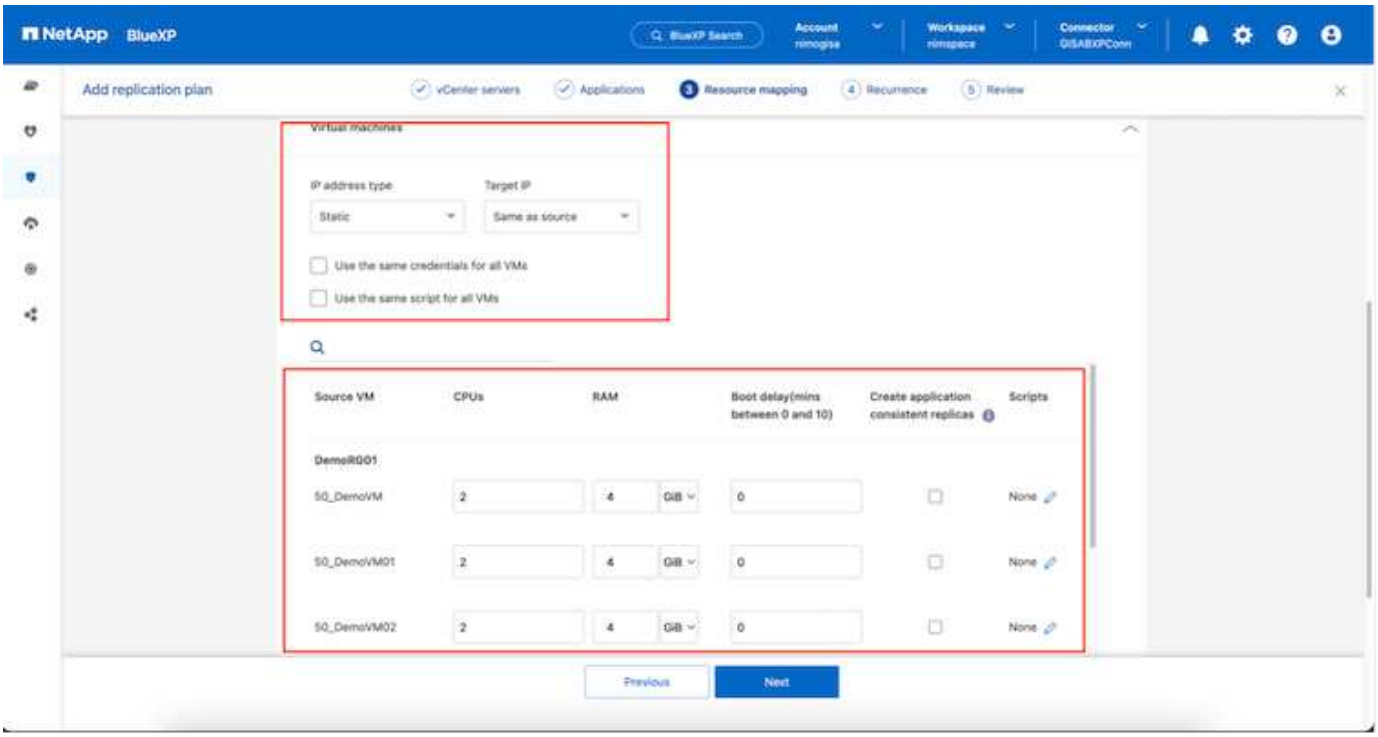
リソース グループでは、ドラッグ アンド ドロップ機能を使用してブート順序を設定できます。これを使用すると、リカバリプロセス中に VM の電源がオンになる順序を簡単に変更できます。

リソース グループ内の各仮想マシンは、順序に基づいて順番に起動されます。 2 つのリソース グループが並行して開始されます。

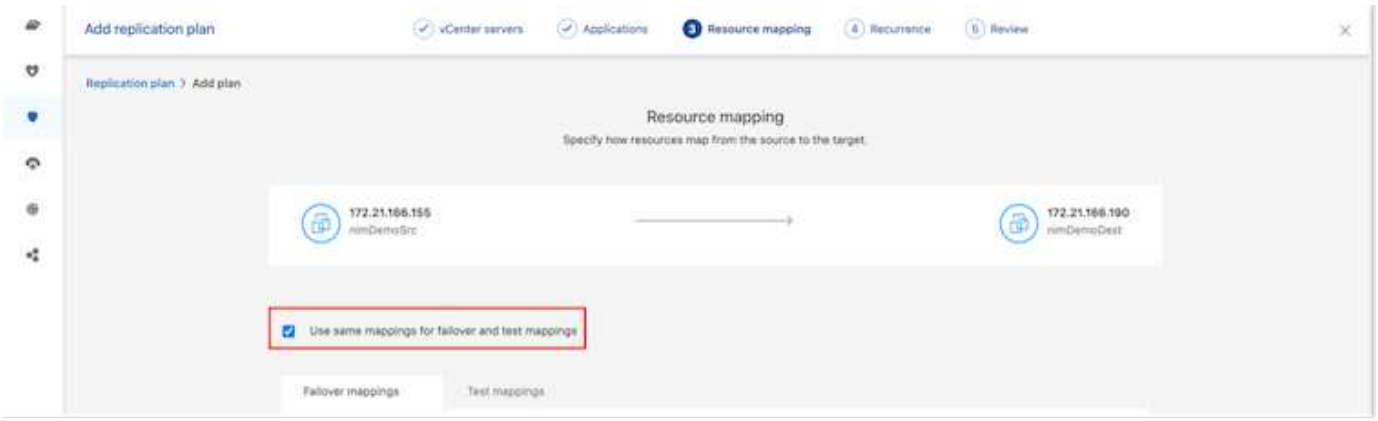
以下のスクリーンショットは、リソース グループが事前に作成されていない場合に、組織の要件に基づいて仮想マシンまたは特定のデータストアをフィルターするオプションを示しています。



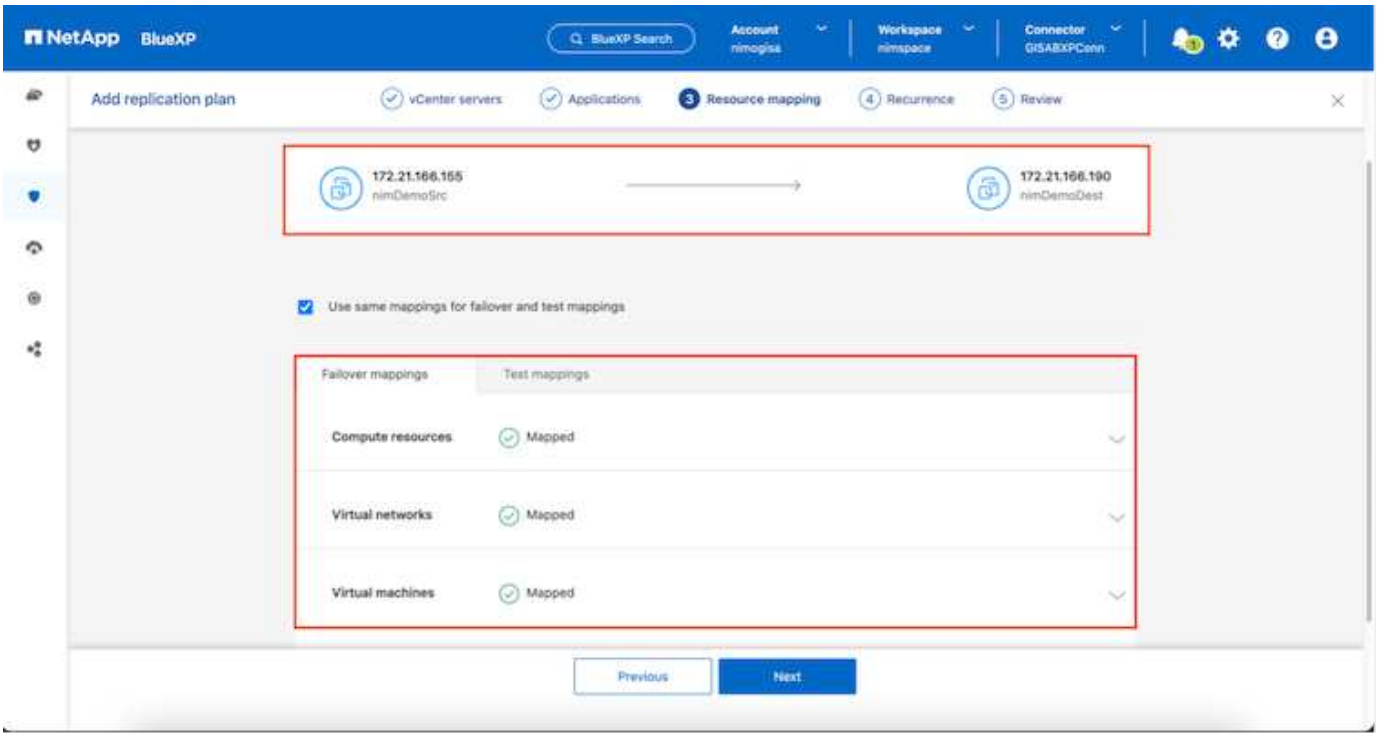
リソースグループを選択したら、フェイルオーバーマッピングを作成します。このステップでは、ソース環境のリソースが宛先にどのようにマッピングされるかを指定します。これには、コンピューティングリソース、仮想ネットワークが含まれます。IPのカスタマイズ、プレスクリプトとポストスクリプト、起動遅延、アプリケーションの整合性などです。詳細については、"レプリケーションプランを作成する"を参照してください。



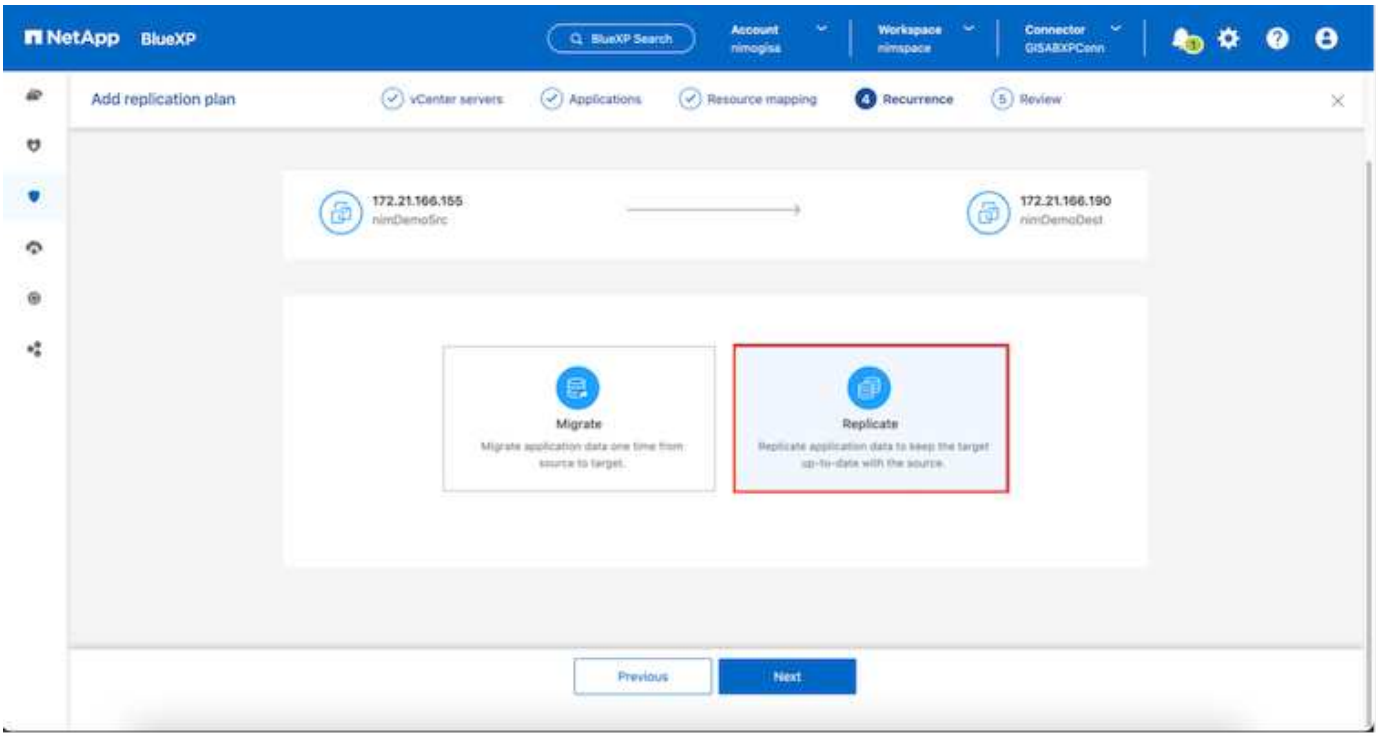
デフォルトでは、テスト操作とフェイルオーバー操作の両方に同じマッピング パラメータが使用されます。テスト環境に異なるマッピングを適用するには、以下に示すようにチェックボックスをオフにした後、テスト マッピング オプションを選択します。



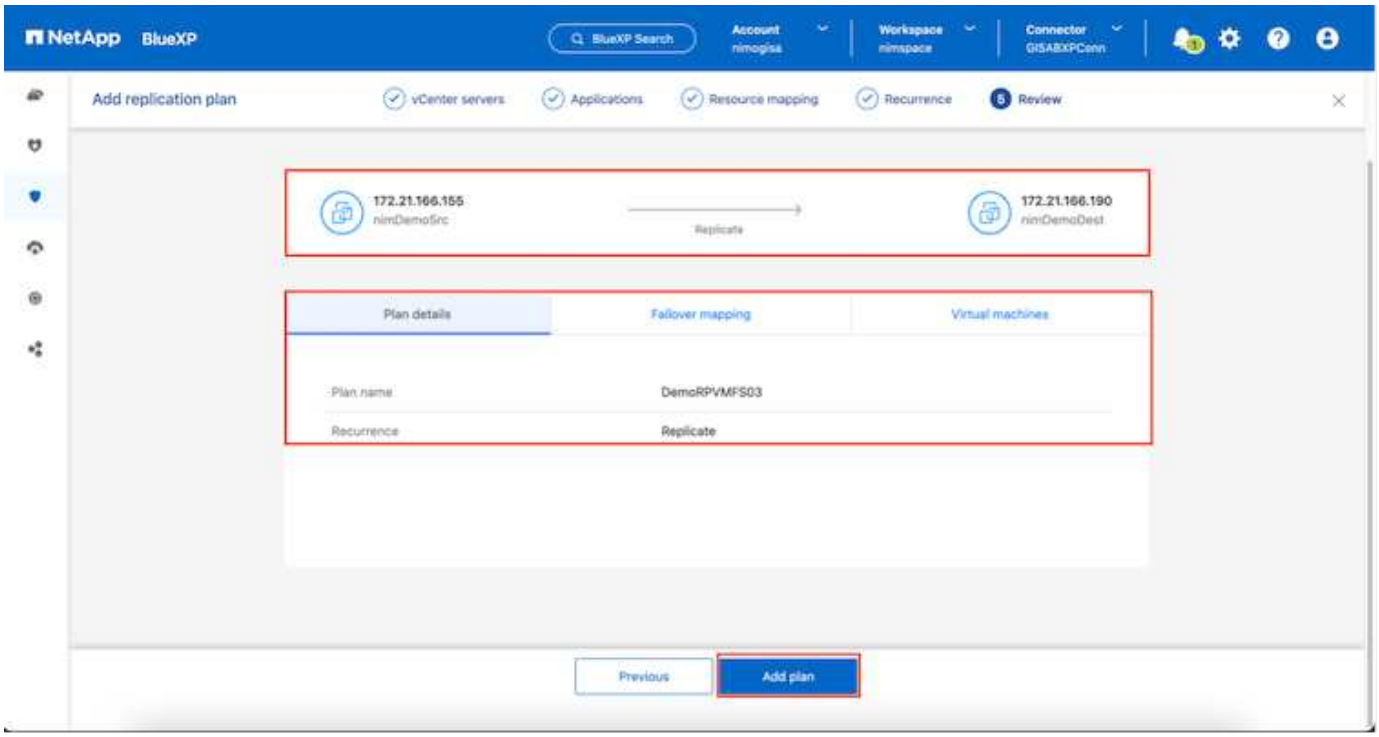
リソース マッピングが完了したら、[次へ] をクリックします。

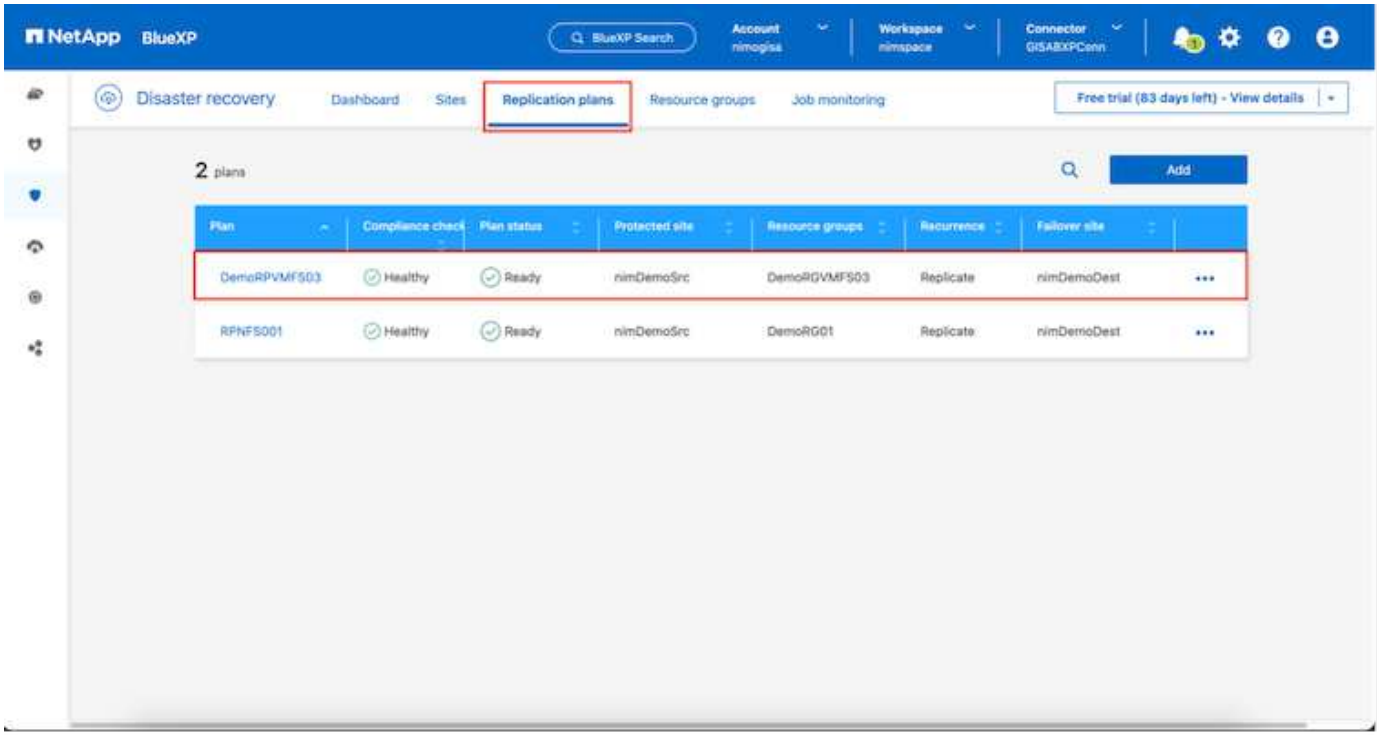


繰り返しタイプを選択します。簡単に言えば、「移行」（フェイルオーバーを使用した 1 回限りの移行）または定期的な連続レプリケーション オプションを選択します。このチュートリアルでは、「複製」オプションが選択されています。

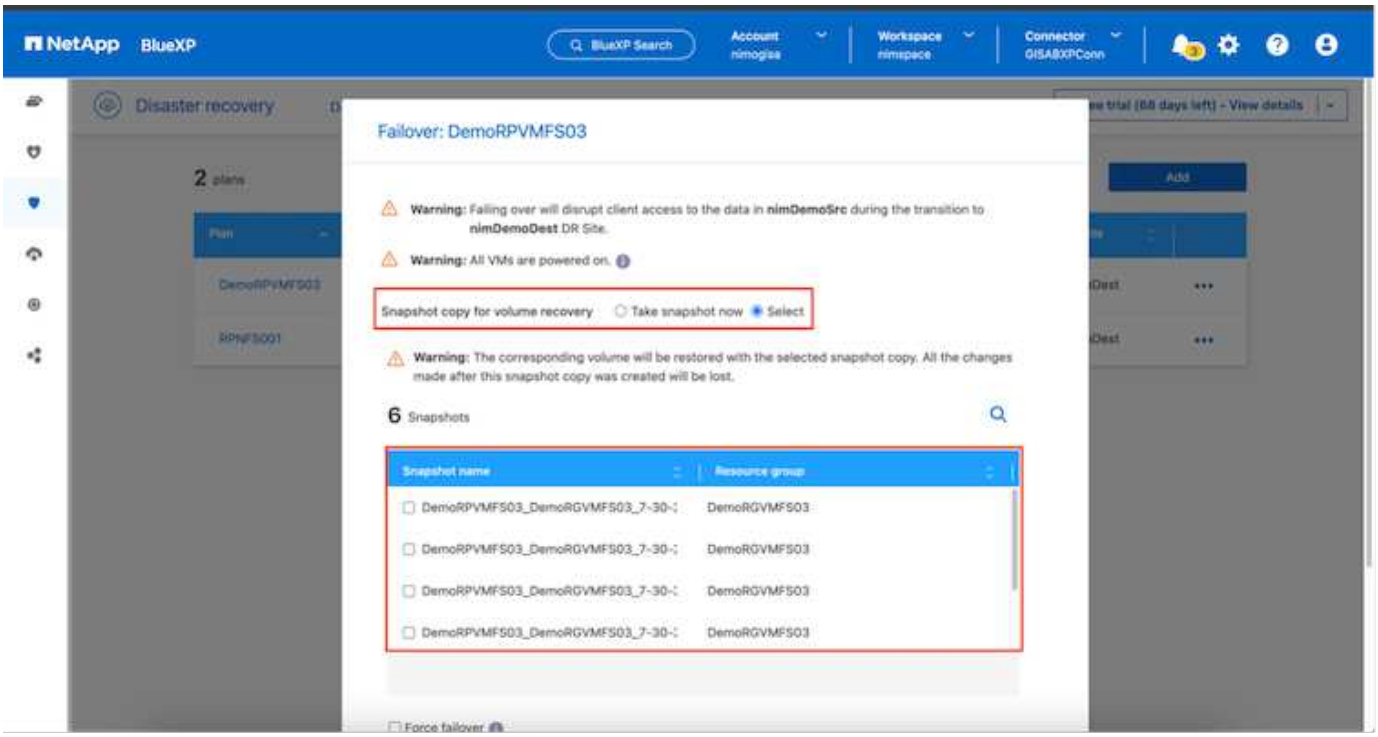


完了したら、作成されたマッピングを確認し、「プランの追加」をクリックします。

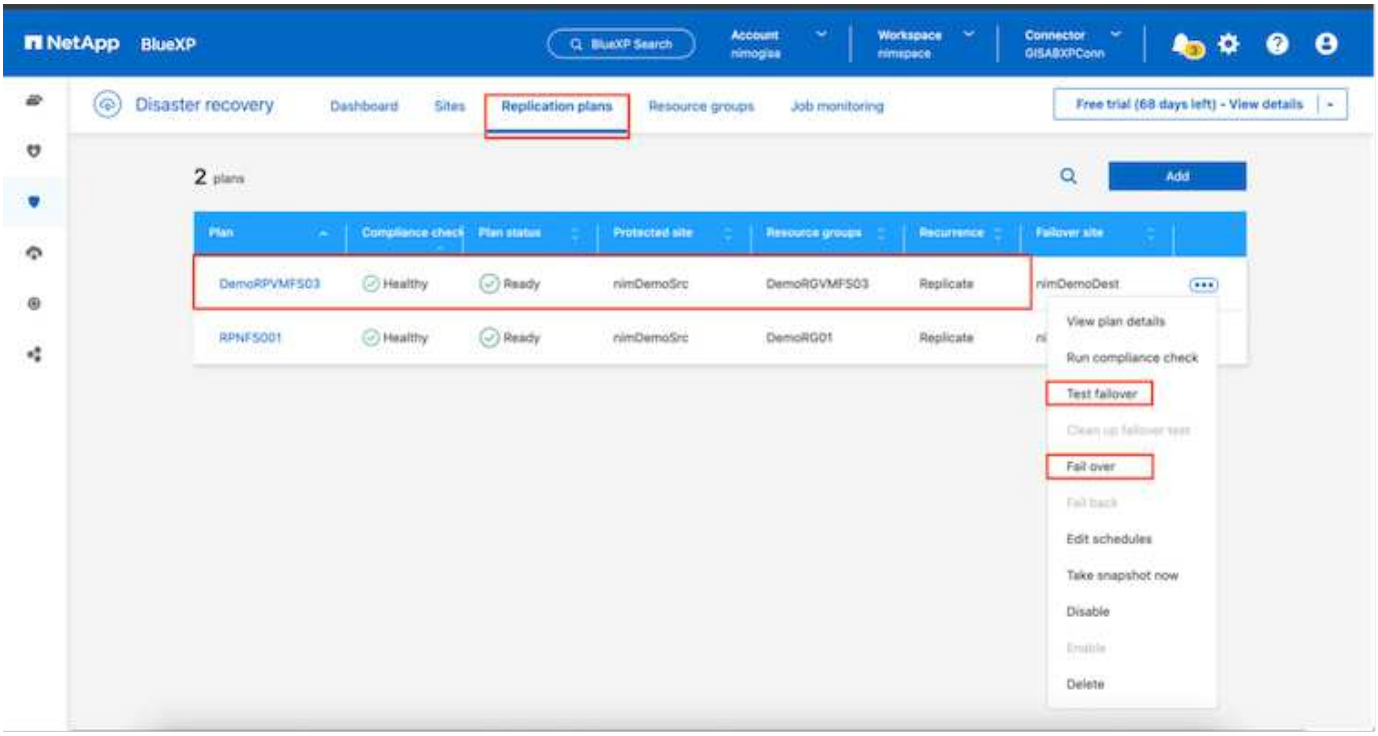




レプリケーションプランの作成後、要件に応じてフェイルオーバーオプション、テストフェイルオーバーオプション、または移行オプションを選択して、フェイルオーバーを実行できます。Disaster Recoveryは、レプリケーションプロセスが計画に従って30分ごとに実行されることを保証します。フェイルオーバーおよびテストフェイルオーバーオプションでは、最新のSnapMirror Snapshotコピーを使用するか、ポイントインタイムのSnapshotコピー（SnapMirrorの保持ポリシーに基づく）から特定のSnapshotコピーを選択できます。ポイントインタイムオプションは、ランサムウェアなどの破損イベントが発生し、最新のレプリカがすでに侵害または暗号化されている場合に非常に役立ちます。Disaster Recoveryには、利用可能なすべてのリカバリ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 [フェイルオーバーのテスト] をクリックします。

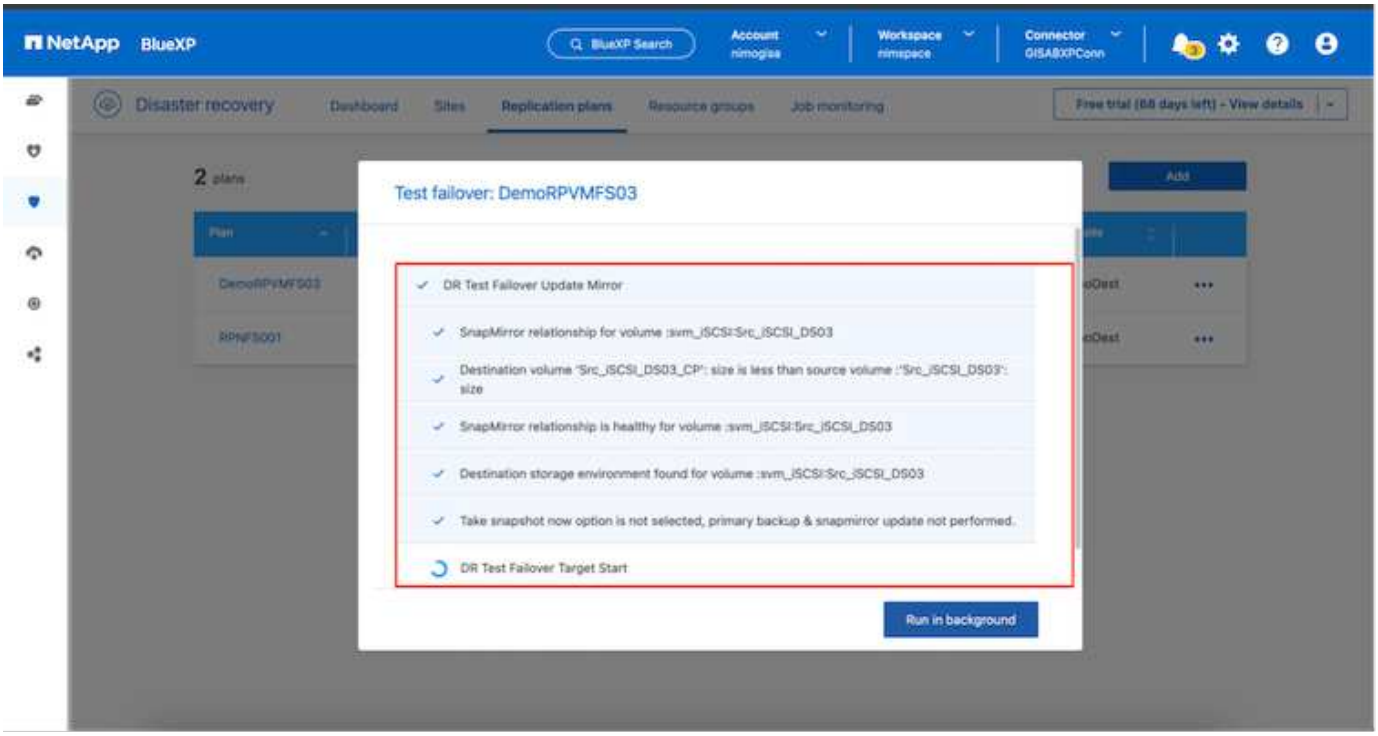


フェイルオーバーまたはテストフェイルオーバー操作中に何が起こりますか**?**

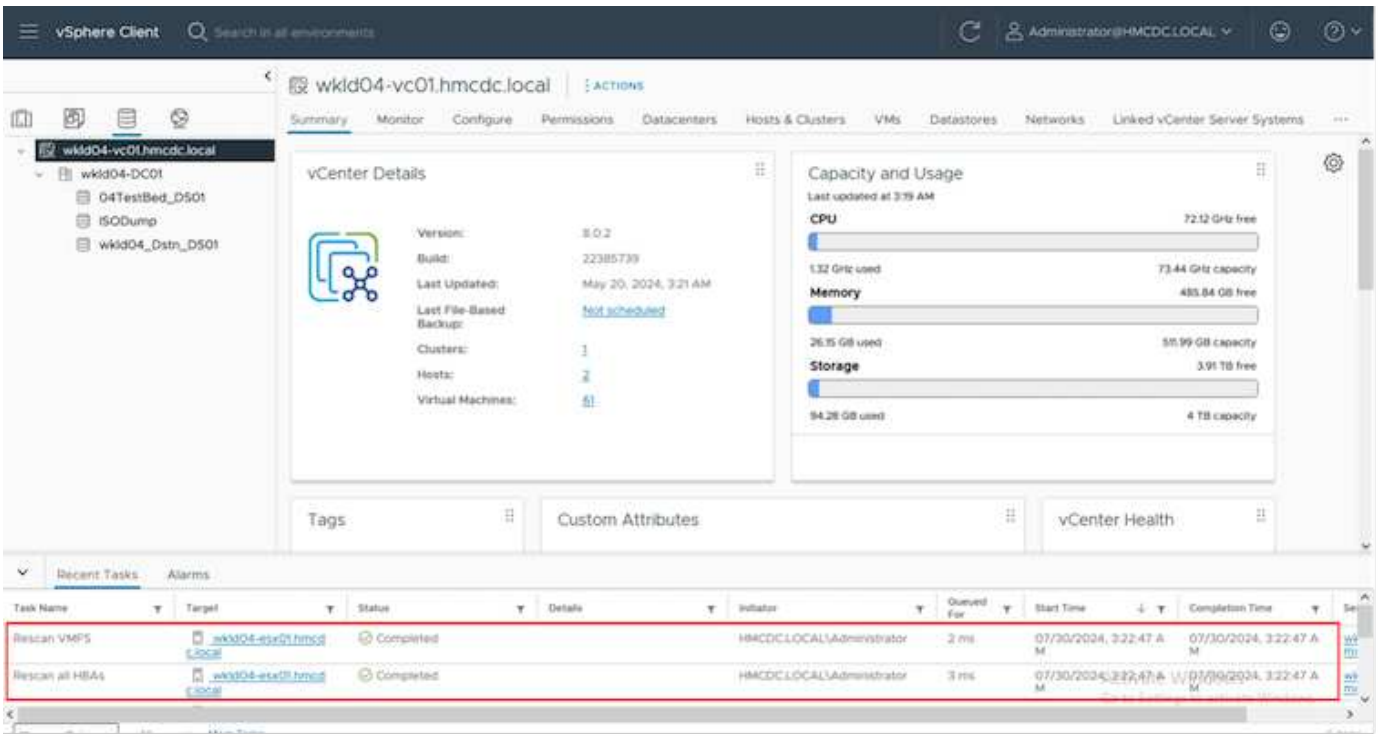
テストフェイルオーバー操作中、Disaster Recoveryは、宛先ボリュームの最新のSnapshotコピーまたは選択したスナップショットを使用して、宛先のONTAPストレージシステム上にFlexCloneボリュームを作成します。

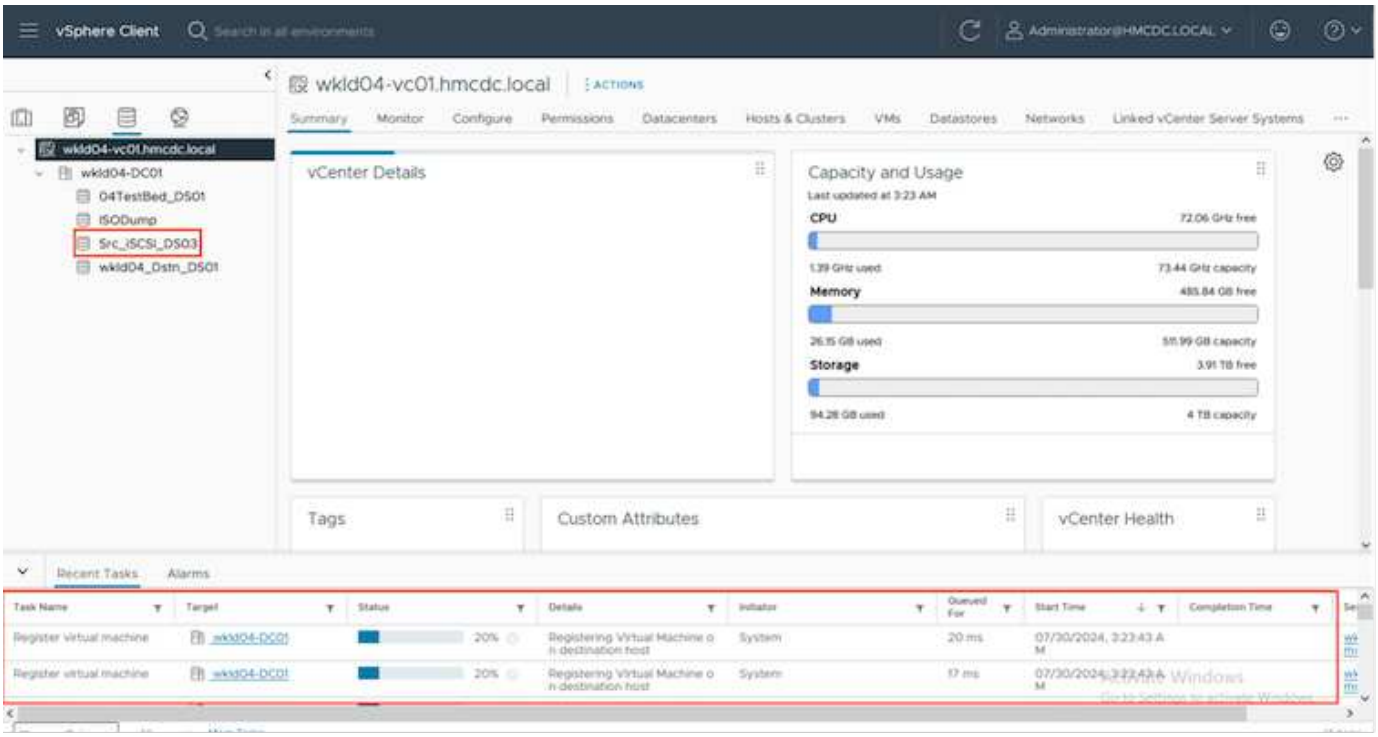
テスト フェイルオーバー操作では、宛先のONTAPストレージ システムにクローン ボリュームが作成されます。

テスト リカバリ操作を実行しても、 SnapMirrorレプリケーションには影響しません。



処理中、Disaster Recoveryは元のターゲットボリュームをマッピングしません。代わりに、選択したSnapshotから新しいFlexCloneボリュームが作成され、そのFlexCloneボリュームをバッキングする一時データストアがESXiホストにマッピングされます。

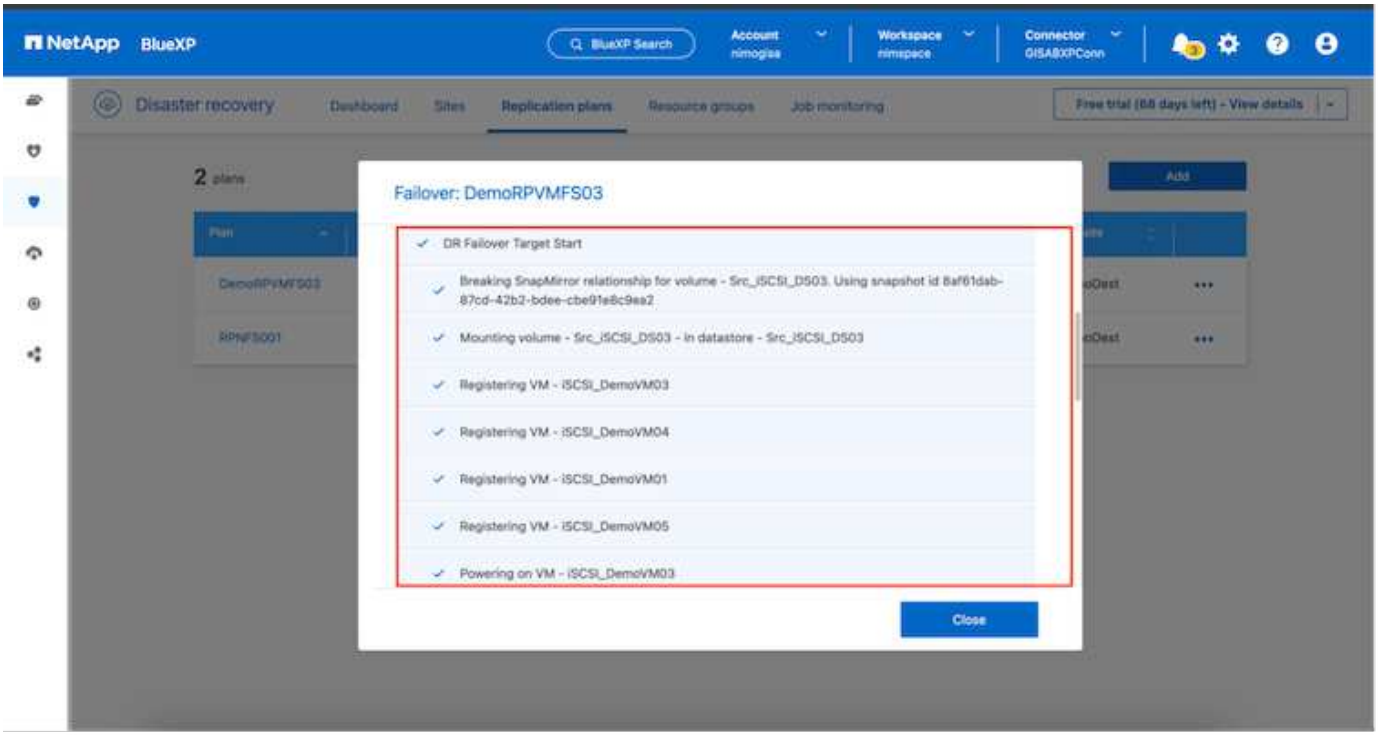




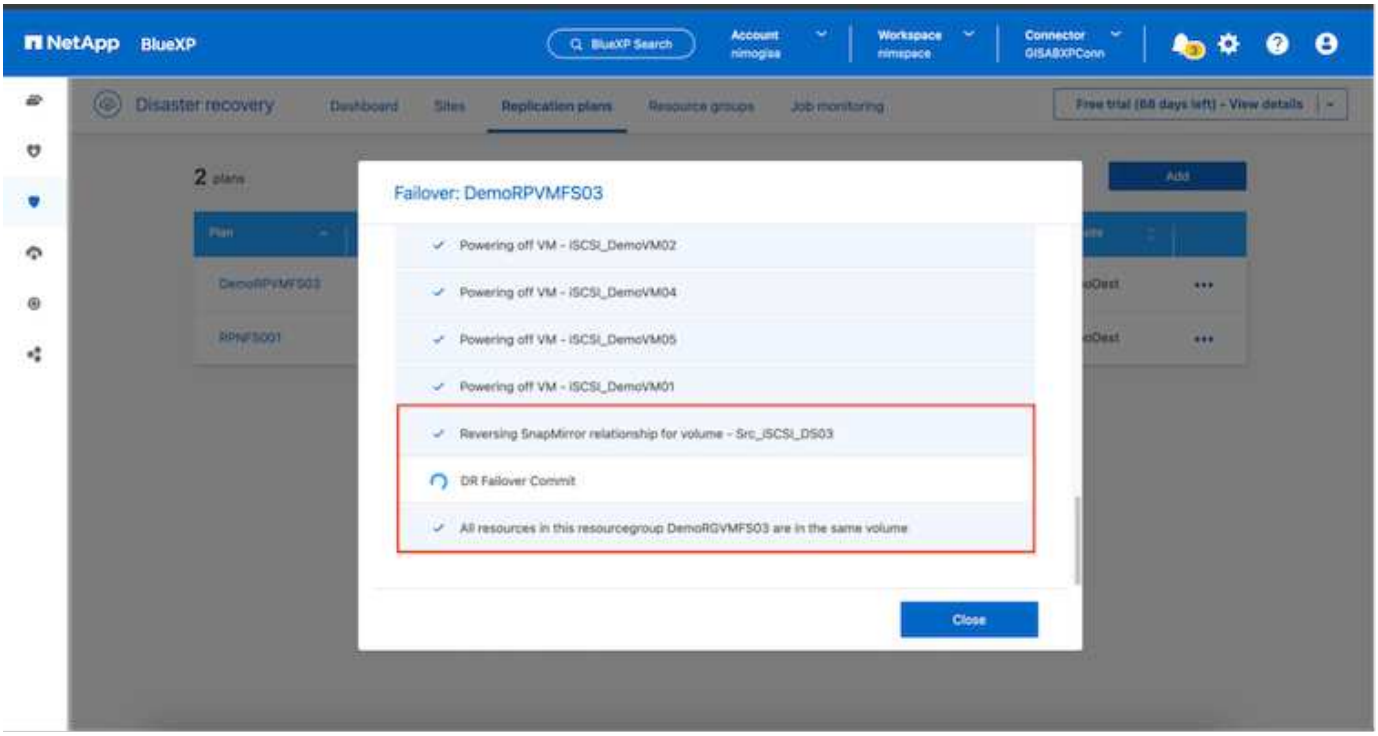
テストフェイルオーバー操作が完了したら、*「Clean Up failover test」*を使用してクリーンアップ操作を開始できます。この操作中、Disaster Recoveryは操作で使用されたFlexCloneボリュームを破棄します。

実際に災害が発生した場合、Disaster Recoveryは次の手順を実行します：

1. サイト間のSnapMirror関係を解除します。
2. 再署名後に VMFS データストア ボリュームをマウントし、すぐに使用できるようにします。
3. VMを登録する
4. VMの電源をオンにする

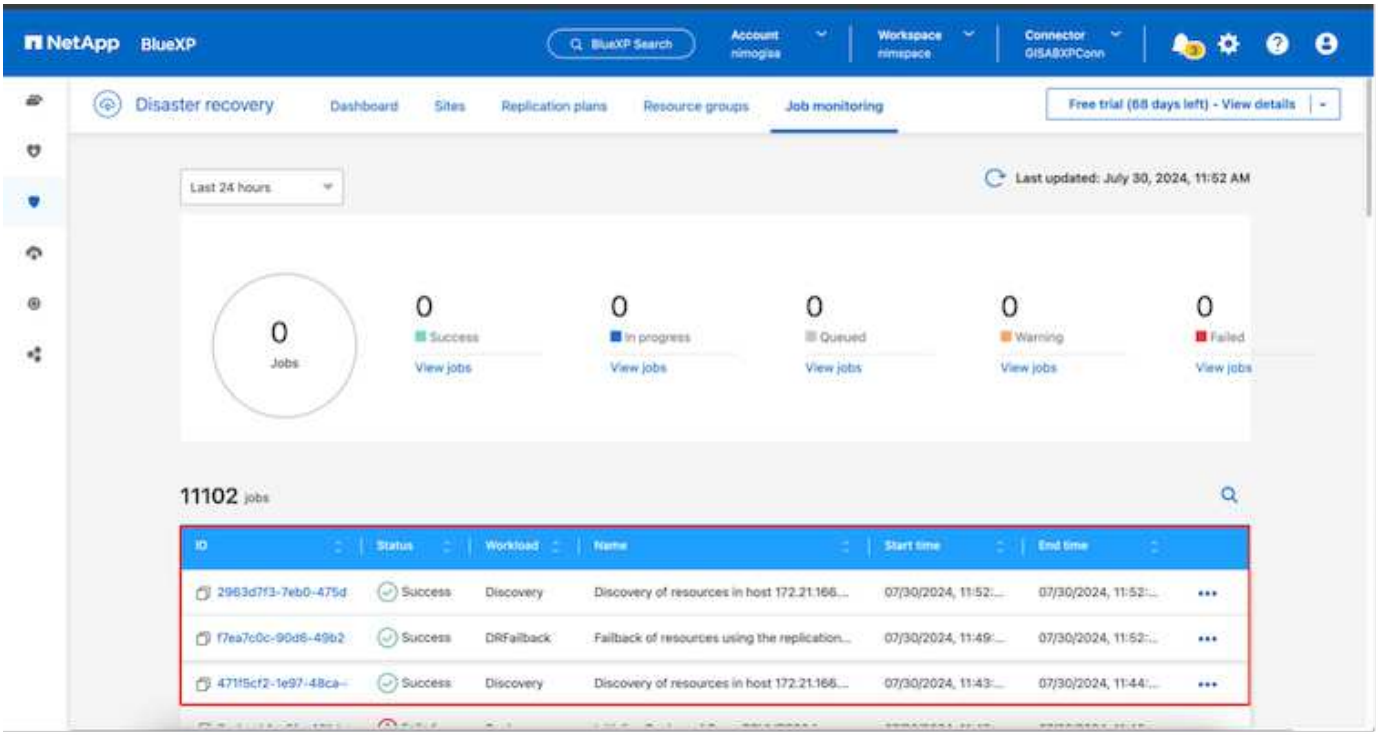


プライマリサイトが稼働すると、ディザスタリカバリによってSnapMirrorの逆方向の再同期とフェイルバックが可能になり、これもボタンをクリックするだけで実行できます。



移行オプションを選択した場合は、計画されたフェイルオーバー イベントと見なされます。この場合、ソース サイトの仮想マシンをシャットダウンする追加の手順がトリガーされます。残りの手順はフェイルオーバー イベントと同じままです。

ConsoleまたはONTAP CLIから、該当するデータストアボリュームのレプリケーションの健全性ステータスを監視でき、フェイルオーバーまたはテストフェイルオーバーのステータスはジョブ監視で追跡できます。



これにより、調整およびカスタマイズされた災害復旧計画を処理するための強力なソリューションが提供されます。フェイルオーバーは、計画されたフェイルオーバーとして実行することも、災害が発生して DR サイトをアクティブ化する決定が下されたときにボタンをクリックするだけでフェイルオーバーを実行することもできます。

このプロセスについて詳しく知りたい場合は、詳細なウォークスルービデオをご覧いただくか、"ソリューションシミュレータ" 。

NetAppハイブリッド マルチクラウドと Red Hat OpenShift コンテナ ワークロード

始めましょう

Red Hat OpenShift Container ワークロード向けのNetAppハイブリッド マルチクラウド ソリューション

NetApp、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、レガシー エンタープライズ アプリケーションを最新化し、新しいアプリケーションを構築する顧客が大幅に増加しています。 Red Hat OpenShift Container Platform は、多くのお客様に採用されている一例です。

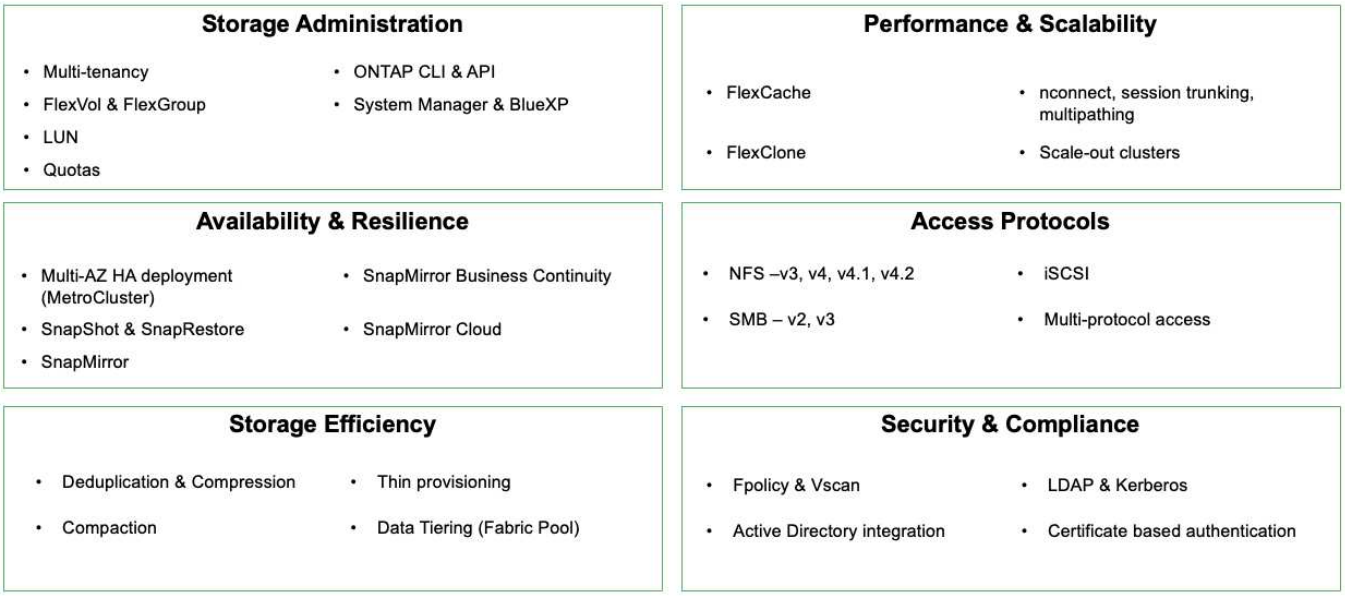
概要

企業内でコンテナを導入する顧客がますます増える中、 NetApp は、ステートフル アプリケーションの永続的なストレージ ニーズや、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ニーズに応える最適な立場にあります。ただし、これらのニーズは、さまざまな戦略、ツール、および方法を使用して満たされます。

以下にリストされている **NetApp ONTAP** ベースのストレージ オプションは、コンテナーと Kubernetes の展開にセキュリティ、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:
  - NetAppファブリック接続ストレージ (FAS)、 NetAppオールフラッシュFASアレイ (AFF)、 NetAppオール SAN アレイ (ASA)、およびONTAP Select
- オンプレミスのプロバイダー管理ストレージ:
  - NetApp Keystoneはストレージ・アズ・ア・サービス（STaaS）を提供します
- クラウド内の自己管理型ストレージ:
  - NetApp Cloud Volumes ONTAP（CVO）は、ハイパースケーラーにセルフマネージドストレージを提供します。
- クラウド内のプロバイダー管理ストレージ:
  - Amazon FSx for NetApp ONTAP、 Azure NetApp Files、 Google Cloud NetApp Volumes は、クラウド内でファイルベースのストレージを提供します。

ONTAP feature highlights

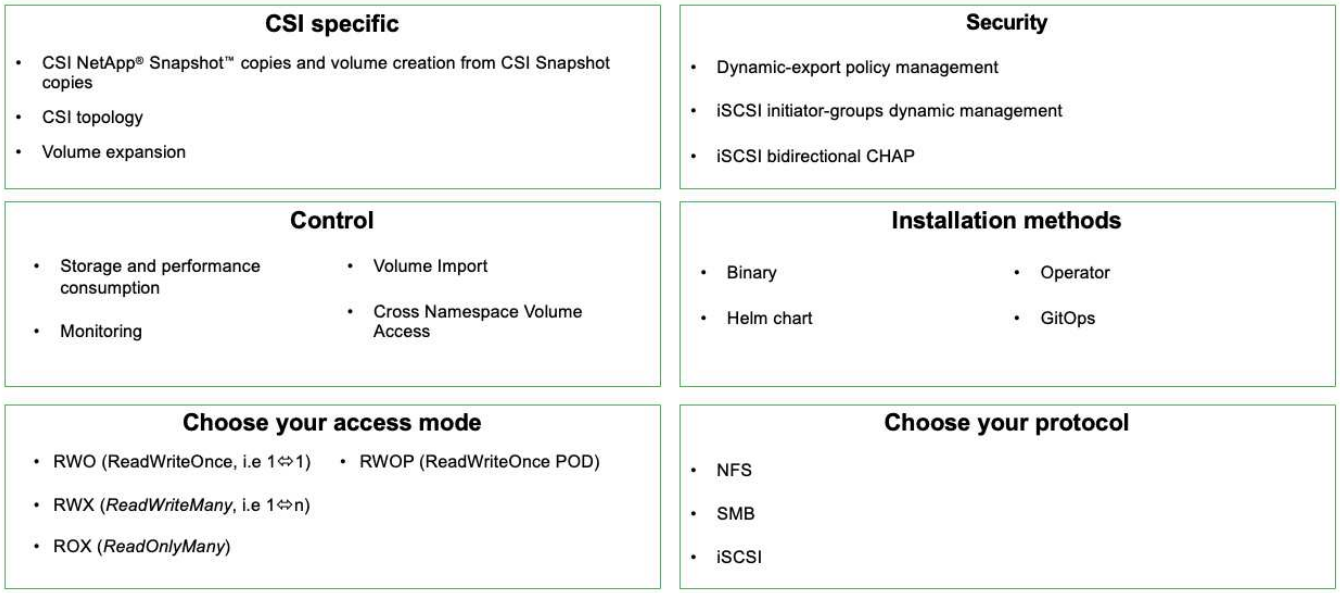


NetApp Consoleを使用すると、単一のコントロール プレーン/インタフェースからすべてのストレージとデータ資産を管理できます。

NetApp Console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、および多くのオンプレミスやエッジのストレージデバイスの制御を行うことができます。

- NetApp Trident** は、CSI 準拠のストレージ オーケストレーターであり、前述のさまざまなNetAppストレージ オプションを活用した永続ストレージを迅速かつ簡単に利用できるようになります。これは、NetAppによって保守およびサポートされているオープンソース ソフトウェアです。

Astra Trident CSI feature highlights



ビジネスクリティカルなコンテナ ワークロードには、永続ボリューム以上のものが必要です。データ管理要件には、アプリケーション 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、ユーザー データに加えて Kubernetes オブジェクトが含まれます。例は次のとおりです。 - ポッド仕様、PVC、デプロイメント、サービスなどの Kubernetes オブジェクト - 構成マップやシークレットなどのカスタム構成オブジェクト - スナップショット コピー、バックアップ、クローンなどの永続データ - CR や CRD などのカスタム リソース

NetApp Trident Protectは、NetApp Tridentの無料アドオンとして利用でき、NetApp ONTAPストレージシステムでサポートされるステートフルKubernetesアプリケーションの機能性と可用性を強化する高度なアプリケーションデータ管理機能を提供します。Trident Protectは、パブリッククラウドとオンプレミス環境の両方でコンテナ化されたワークロードの管理、保護、移動を簡素化します。また、APIとCLIを通じて強力な自動化機能も提供します。

このリファレンス ドキュメントでは、 Trident Protect を使用して RedHat OpenShift プラットフォームにデプロイされたコンテナーベースのアプリケーションのデータ保護の検証について説明します。さらに、このソリューションは、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高レベルの詳細を提供します。このドキュメントでは、 Trident CSI プロビジョナーを使用したNetAppストレージと Red Hat OpenShift コンテナ プラットフォームの統合の詳細についても説明します。

Red Hat OpenShift Container ワークロード向け**NetApp**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

ほとんどの顧客は、既存のインフラストラクチャなしで Kubernetes ベースの環境の構築を開始するわけではありません。おそらく、ほとんどのエンタープライズ アプリケーションを仮想マシン (大規模な VMware 環境など) 上で実行している従来の IT ショップでしょう。次に、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、小さなコンテナベースの環境の構築を開始します。こうした取り組みは通常、小規模から始まり、チームが新しいテクノロジーやスキルを習得し、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、より広範囲に広がり始めます。お客様にとって朗報なのは、 NetApp が両方の環境のニーズに対応できることです。 Red Hat OpenShift を使用したハイブリッド マルチクラウド向けのこのソリューション セットにより、 NetApp のお客様は、インフラストラクチャと組織全体を刷新することなく、最新のクラウド テクノロジーとサービスを導入できるようになります。顧客のアプリケーションとデータがオンプレミス、クラウド、仮想マシン、コンテナのいずれでホストされているかに関係なく、 NetApp は一貫したデータ管理、保護、セキュリティ、移植性を提供できます。これらの新しいソリューションにより、 NetAppがオンプレミス データセンター環境で数十年にわたって提供してきたのと同じ価値が、企業のデータ 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、新しいスキルの獲得、新しいチームの構築などに多大な投資をする必要はありません。 NetApp は、お客様がクラウド導入のどの段階にいても、これらのビジネス課題の解決を支援できる体制が整っています。

NetAppハイブリッド マルチクラウドと Red Hat Openshift:

- Red Hat OpenShift をNetAppベースのストレージ ソリューションと組み合わせて使用する場合、データとアプリケーションを管理、保護、セキュリティ保護、移行するための最適な方法を示す検証済みの設計とプラクティスを顧客に提供します。

- VMware 環境、ベアメタル インフラストラクチャ、またはその両方の組み合わせでNetAppストレージを使用して Red Hat OpenShift を実行している顧客向けのベスト 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の両方、および両方が使用されるハイブリッド環境の戦略とオプションを示します。

Red Hat OpenShift Container ワークロード向け**NetApp**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

このソリューションは、OpenShift Container Platform（OCP）、OpenShift Advanced Cluster Manager（ACM）、NetApp ONTAP、NetApp Console、およびNetApp Trident Protectを使用した移行と集中型データ保護をテストおよび検証します。

このソリューションでは、次のシナリオがNetAppによってテストおよび検証されています。ソリューションは、次の特性に基づいて複数のシナリオに分かれています。

- オンプレミス
- cloud
  - セルフマネージド OpenShift クラスタとセルフマネージドNetAppストレージ
  - プロバイダー管理の OpenShift クラスターとプロバイダー管理のNetAppストレージ

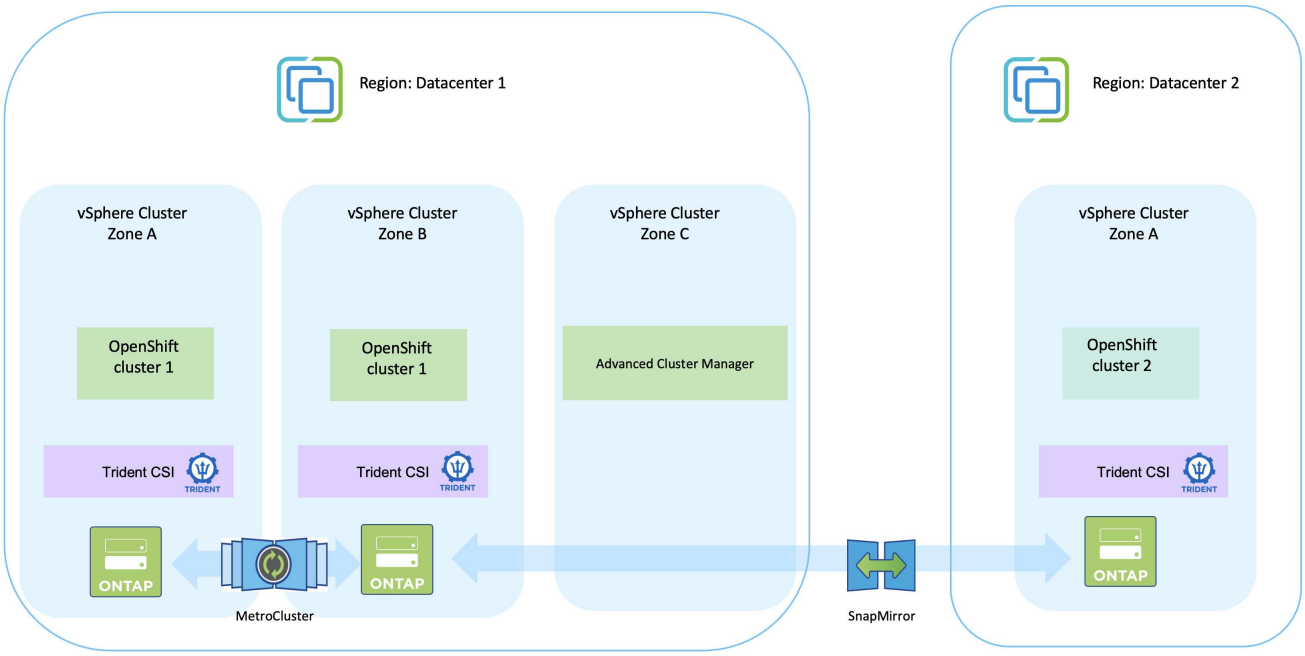
今後、追加のソリューションとユースケースを構築していく予定です。

シナリオ **1: Trident Protect** 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: セルフマネージド **OpenShift** クラスターとセルフマネージド**NetApp**ストレージ

- Trident Protectを使用して、アプリケーションを保護し、オンプレミスクラスター間の移行をサポートします。

シナリオ**1**

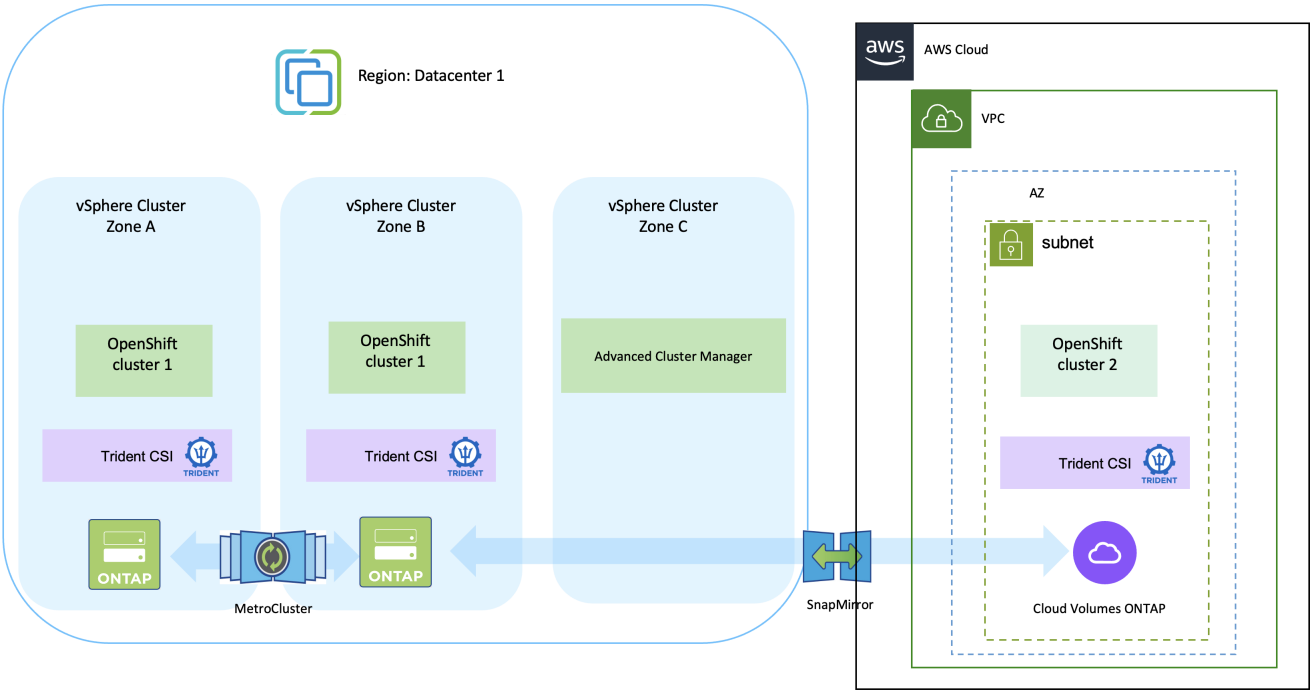


シナリオ **2: Trident Protect** を使用したオンプレミス環境から **AWS** 環境へのデータ保護と移行

オンプレミス: セルフマネージド **OpenShift** クラスターとセルフマネージド ストレージ **AWS** クラウド: セルフマネージド **OpenShift** クラスターとセルフマネージド ストレージ

- Trident Protectを使用して、アプリケーションを保護し、オンプレミスクラスタとAWSの自己管理型OpenShiftクラスタ間の移行をサポートします。

シナリオ**2**

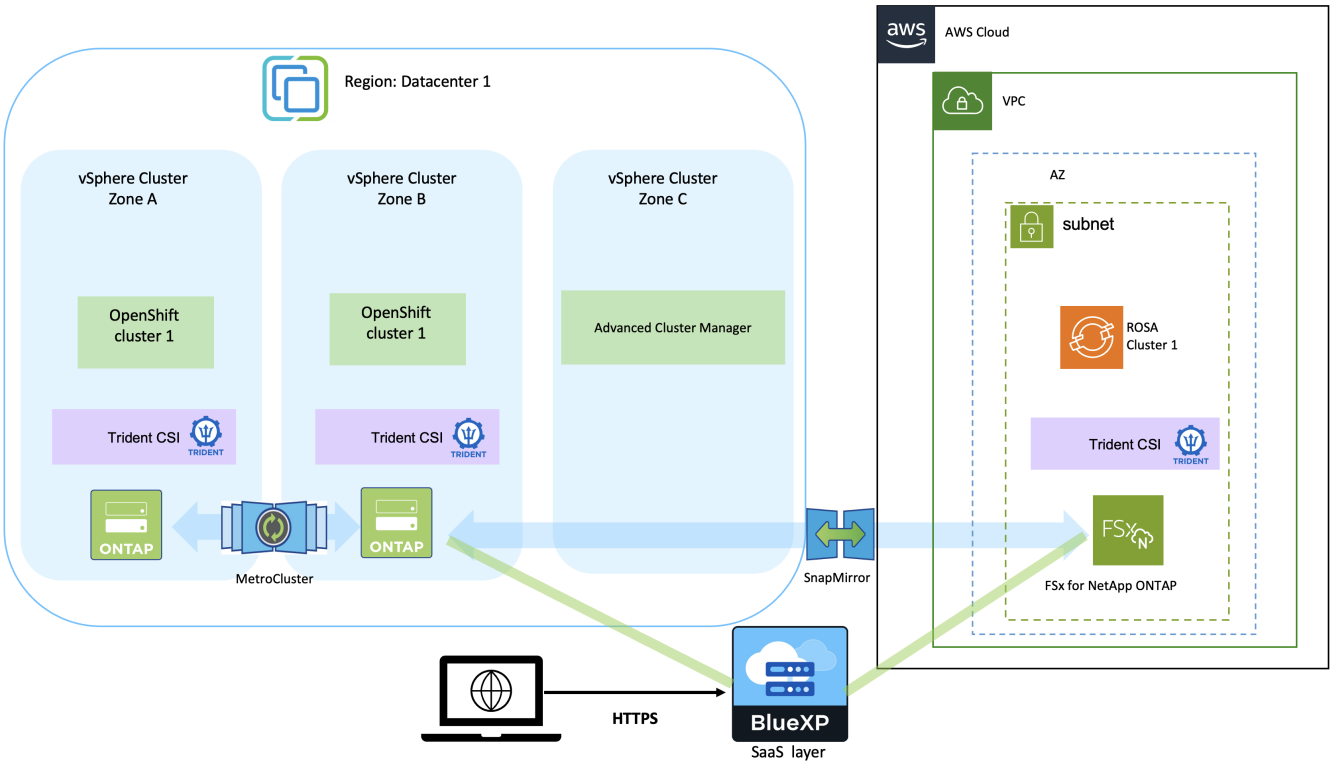


シナリオ**3:** オンプレミス環境から**AWS**環境へのデータ保護と移行

オンプレミス: セルフマネージド **OpenShift** クラスターとセルフマネージド ストレージ **AWS** クラウド: プロバイダー管理 **OpenShift** クラスター **(ROSA)** とプロバイダー管理ストレージ **(FSx ONTAP)**

- NetApp Consoleを使用して、永続ボリューム（FSx ONTAP）のレプリケーションを実行します。
- 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。

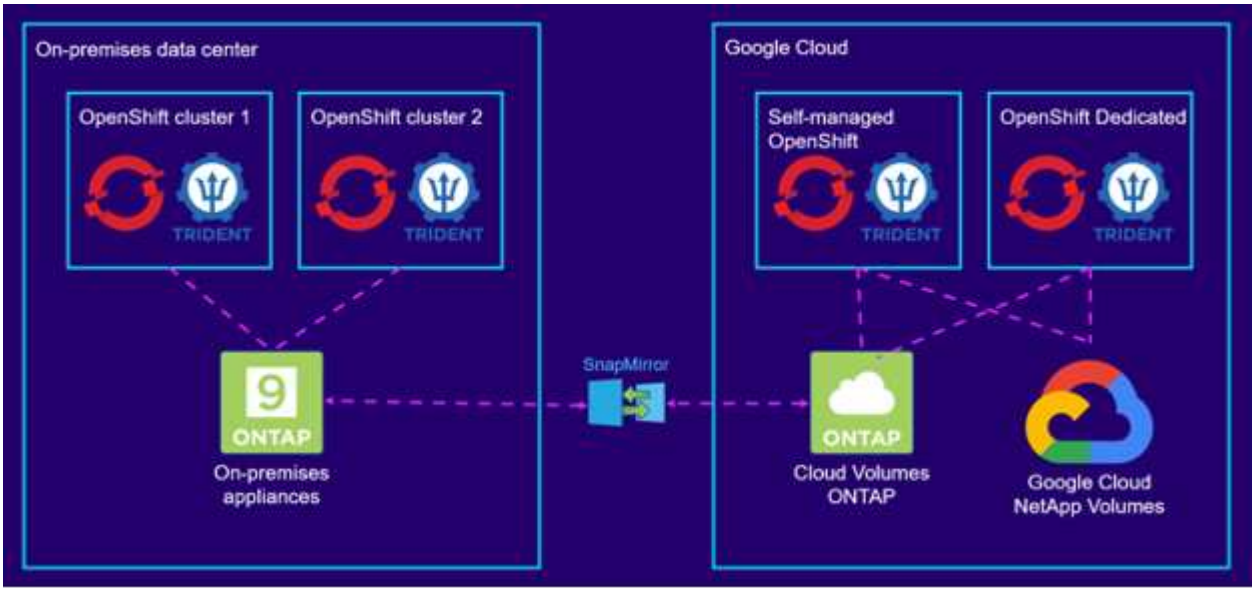
シナリオ**3**



シナリオ **4: Trident Protect** 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: セルフマネージド **OpenShift** クラスタとセルフマネージド ストレージ **Google Cloud:** セルフマネージド **OpenShift** クラスタとセルフマネージド ストレージ

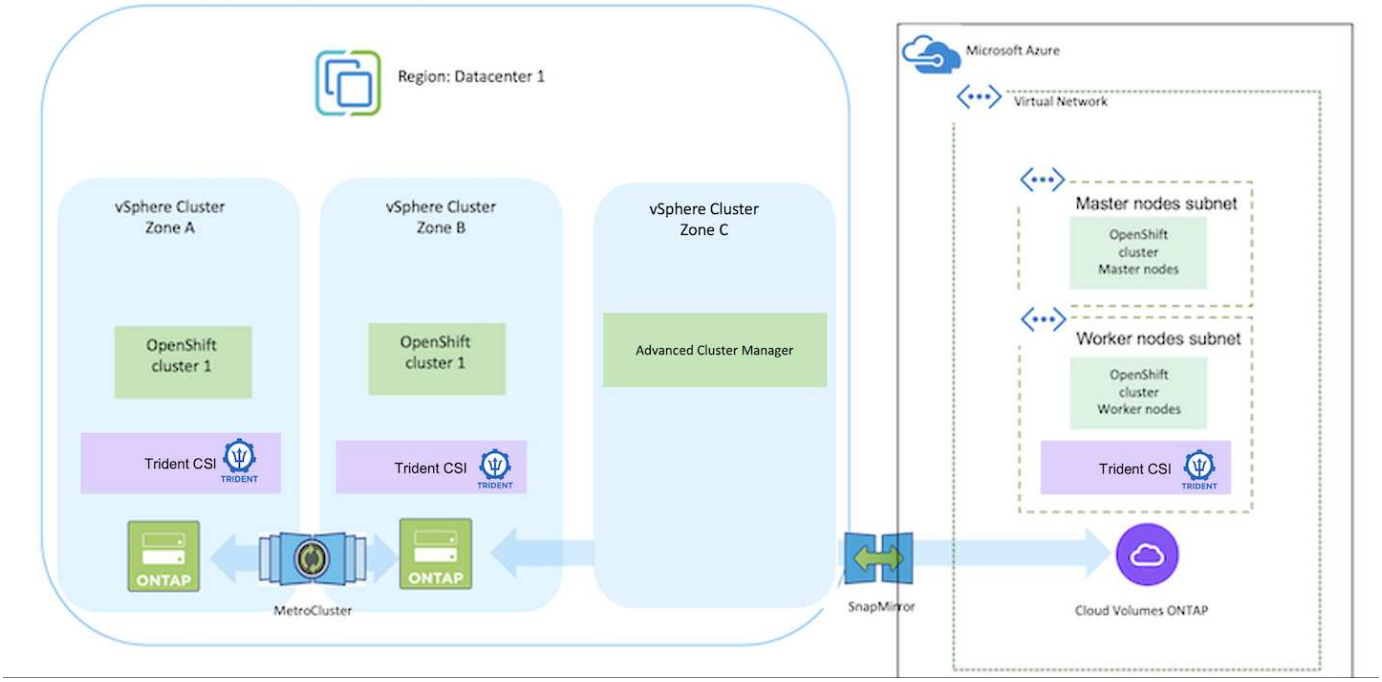
- Trident Protectを使用して、アプリケーションを保護し、オンプレミスとGoogle Cloud OpenShiftクラスター間の移行をサポートします。



MetroCluster構成でONTAPを使用する場合の考慮事項については、"ここをクリックしてください。"。

オンプレミス: セルフマネージド OpenShift クラスターとセルフマネージド ストレージ Azure クラウド: セルフマネージド OpenShift クラスターとセルフマネージド ストレージ

- Trident Protect を使用して、アプリケーションを保護し、オンプレミスと Azure の OpenShift クラスター間の移行をサポートします。



MetroCluster構成でONTAPを使用する場合の考慮事項については、"ここをクリックしてください。" 。

ソリューション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

このソリューションは、OpenShift コンテナ プラットフォーム、OpenShift Advanced Cluster Manager、 NetApp ONTAP、 NetApp Trident Protect を使用して、移行と集中データ保護をテストおよび検証します。

ソリューションのシナリオ 1、2、3 は、以下の表に示すバージョンを使用して検証されました。

成分	バージョン
ヴイエムウェア	vSphere Client バージョン 8.0.0.10200 VMware ESXi、8.0.0、20842819
ハブクラスター	オープンシフト 4.11.34
ソースクラスターと宛先クラスター	OpenShift 4.12.9（オンプレミスおよびAWS）
NetAppTrident	Tridentサーバーおよびクライアント 23.04.0
NetAppTridentプロテクト	Tridentプロテクト 22.11.0-82
NetAppONTAP	ONTAP 9.12.1

AWS FSx ONTAP	単一AZ

ソリューションのシナリオ 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。

成分	バージョン
ヴイエムウェア	vSphere Client バージョン 8.0.2.00000 VMware ESXi、8.0.2、22380479
ハブクラスター	オープンシフト 4.13.13
ソースクラスターと宛先クラスター	オンプレミスおよび Google Cloud の OpenShift 4.13.12
NetAppTrident	Tridentサーバーおよびクライアント 23.07.0
NetAppONTAP	ONTAP 9.12.1
Cloud Volumes ONTAP	単一 AZ、単一ノード、9.14.0

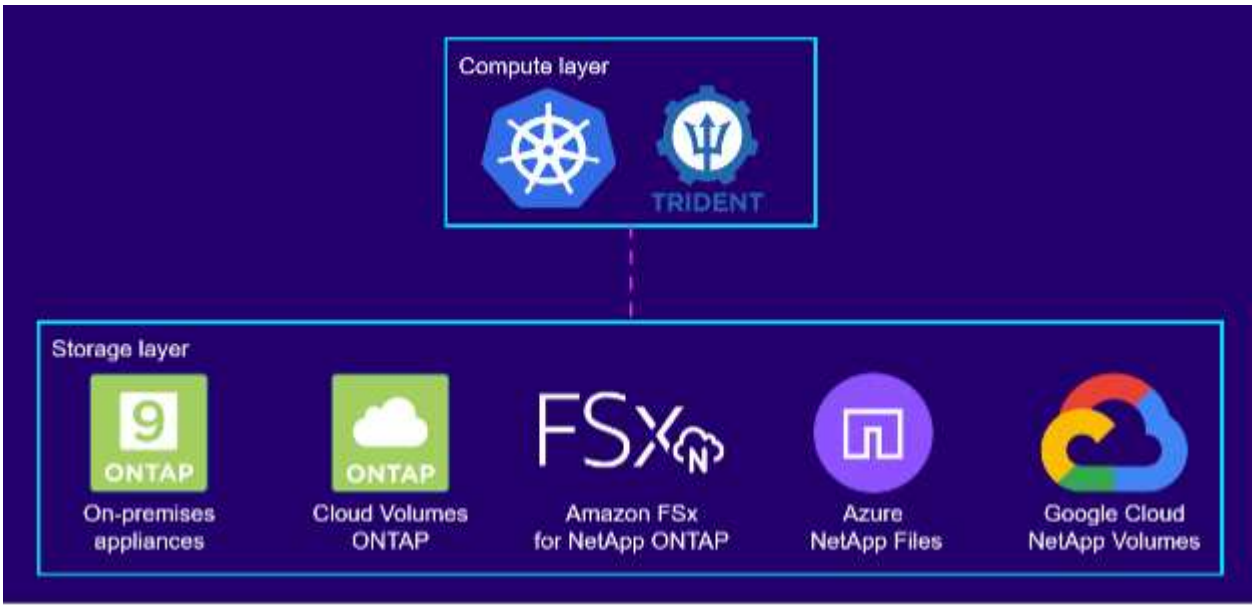
ソリューションのシナリオ 5 は、次の表に示すバージョンを使用して検証されました。

成分	バージョン
ヴイエムウェア	vSphere Client バージョン 8.0.2.00000 VMware ESXi、8.0.2、22380479
ソースクラスターと宛先クラスター	オンプレミスおよび Azure の OpenShift 4.13.25
NetAppTrident	Tridentサーバとクライアント23.10.0
NetAppTridentプロテクト	Tridentプロテクト 23.10
NetAppONTAP	ONTAP 9.12.1
Cloud Volumes ONTAP	単一 AZ、単一ノード、9.14.0

Red Hat OpenShift Containers とサポートされる**NetApp**ストレージの統合

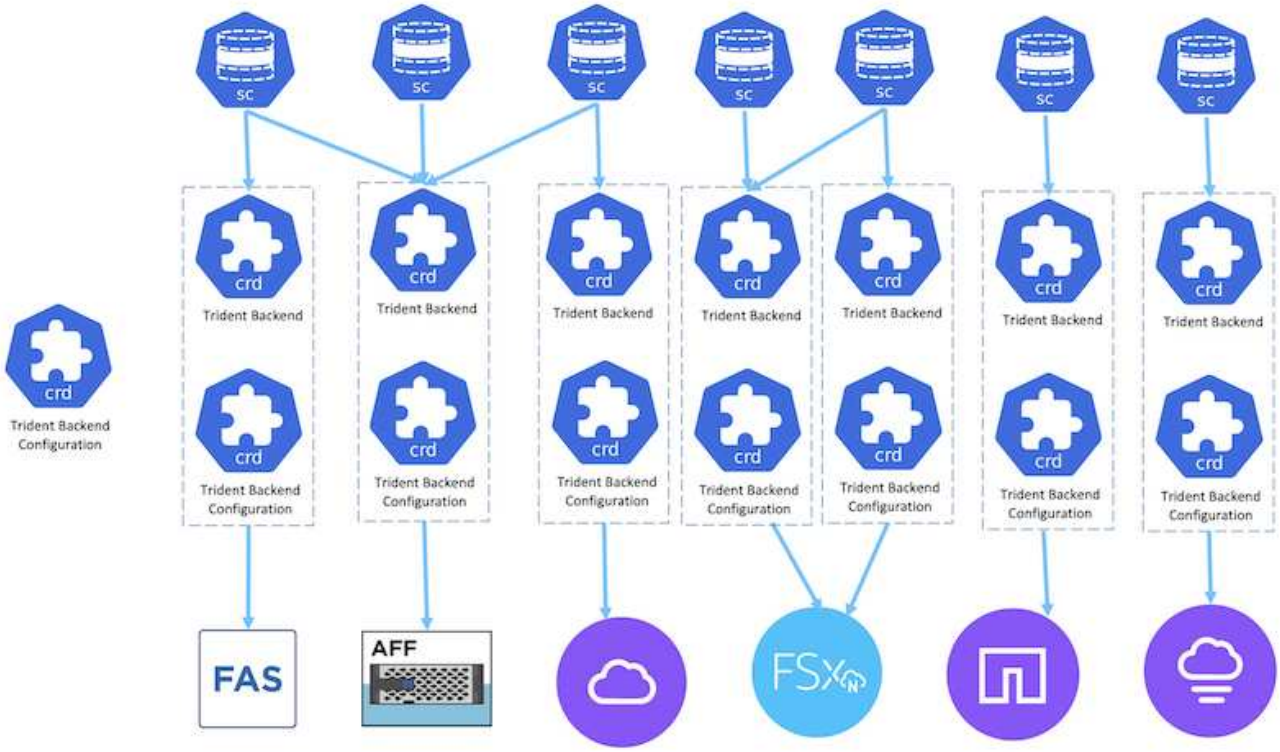
Red Hat OpenShift コンテナが VMware 上で実行されているか、ハイパースケーラー内で実行されているかに関係なく、 NetApp Trident は、サポートされるさまざまなタイプのバックエンドNetAppストレージの CSI プロビジョナーとして使用できます。

次の図は、 NetApp Tridentを使用して OpenShift クラスターと統合できるさまざまなバックエンドNetAppストレージを示しています。



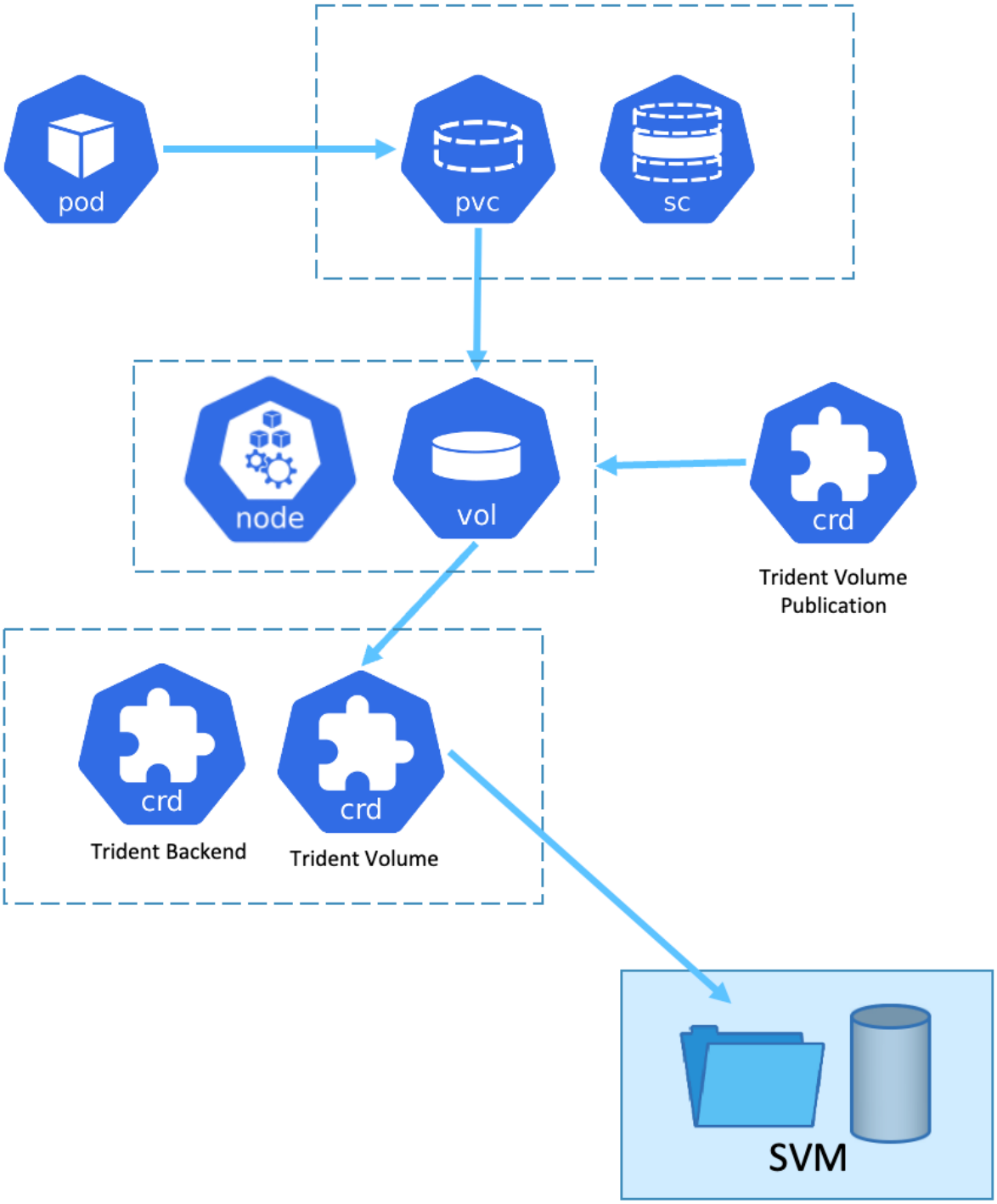
ONTAPストレージ仮想マシン (SVM) は、安全なマルチテナント機能を提供します。単一の OpenShift クラスターは、単一の SVM または複数の SVM、さらには複数のONTAPクラスターに接続できます。ストレージ クラスは、パラメータまたはラベルに基づいてバックエンド ストレージをフィルターします。ストレージ管理者は、Trident バックエンド構成を使用してストレージ システムに接続するためのパラメータを定義します。接続が正常に確立されると、トライデント バックエンドが作成され、ストレージ クラスがフィルターできる情報が入力されます。

ストレージクラスとバックエンドの関係を以下に示します。



アプリケーション所有者は、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。ストレージ クラスはバックエンド ストレージをフィルターします。

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。



コンテナストレージインターフェース（**CSI**）オプション

vSphere 環境では、お客様は VMware CSI ドライバーや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はローカル SCSI ディスクとして消費されますが、 Tridentではネットワークで消費されます。

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 ベースの展開では、VMware CSI が優先され、SnapMirror Business Continuity (SMBC) によってゾーン レベルの高可用性が提供されます。

VMware CSIはサポートしています

- コアブロックベースのデータストア（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（ブロックおよびファイル）

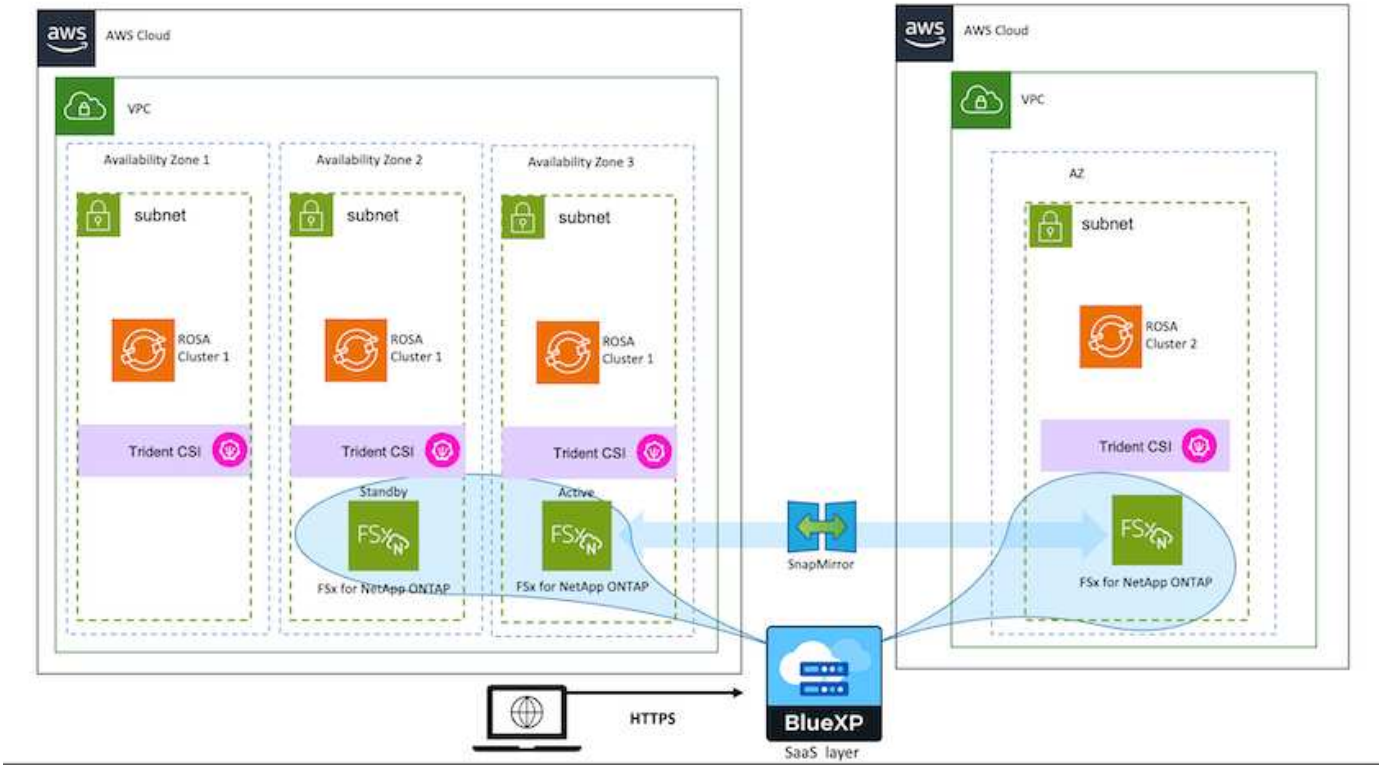
Tridentには**ONTAP**をサポートする以下のドライバーがあります

- ontapさん（専用ボリューム）
- ontap-san-economy（共有ボリューム）
- ontap-nas（専用ボリューム）
- ontap-nas-economy（共有ボリューム）
- ontap-nas-flexgroup (専用の大規模ボリューム)

VMware CSI とTrident CSI の両方において、 ONTAP はNFS の場合は nconnect、セッション トランキング、Kerberos など、ブロック プロトコルの場合はマルチパス、CHAP 認証などをサポートします。

AWS では、 Amazon FSx for NetApp ONTAP (FSx ONTAP) を単一のアベイラビリティーゾーン (AZ) またはマルチ AZ にデプロイできます。高可用性を必要とする本番ワークロードの場合、マルチ AZ はゾーンレベルのフォールト トレランスを提供し、単一 AZ と比較して NVMe 読み取りキャッシュが向上します。詳細については、"AWSパフォーマンスガイドライン" 。

災害復旧サイトのコストを節約するために、単一の AZ FSx ONTAP を利用できます。



FSx ONTAPでサポートされているSVMの数については、"FSx ONTAPストレージ仮想マシンの管理"

追加ドキュメント

以下に参考となる追加ドキュメントを示します。

1. "VMware vSphere"
2. "OpenShift Container プラットフォーム製品ドキュメント"
3. "OpenShift コンテナ プラットフォーム クラスターのインストール"
4. "高度なクラスタ管理製品ドキュメント"
5. "ACM を使用してクラスターを作成する"
6. "OpenShift への Red Hat Quay のデプロイ"
7. "Trident"
8. "ONTAP 9"
9. "NetAppヴェルダ" - Verda（オープンソース）には、一般的なクラウドネイティブのデータ集約型アプリケーション向けの参照実行フックのコレクションがあります
10. "NetApp データサービス"
11. "Red Hat OpenShift Service on AWS クラシックアーキテクチャ"
12. "Amazon FSx ONTAP"
13. "GCP への OpenShift クラスターのインストール"
14. "Azure への OpenShift クラスターのインストール"

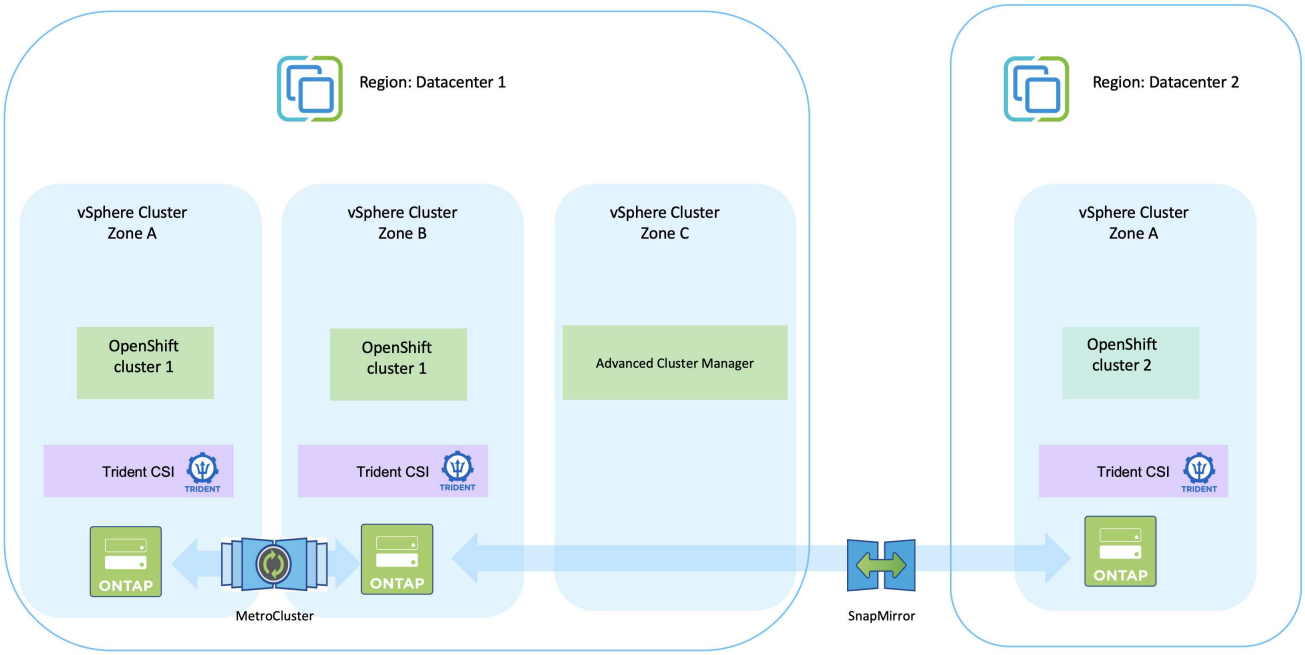
オンプレミス向け**OpenShift**

VMware 上の **Red Hat OpenShift Container** プラットフォーム ワークロードを使用したNetAppソリューション

お客様が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ストラクチャ上で実行する必要がある場合は、それを行うことができます。コンテナ ワークロードをデプロイするための本番環境を正常に構築するには、Red Hat OpenShift コンテナ プラットフォーム (OCP) を計画してデプロイする必要があります。OCP クラスターは、VMware またはベアメタル上に展開できます。

NetApp ONTAPストレージは、コンテナの導入においてデータ保護、信頼性、柔軟性を実現します。 Tridentは、顧客のステートフル アプリケーション用に永続的なONTAPストレージを使用する動的ストレージ プロビジョナーとして機能します。 NetApp Trident Protect は、データ保護、移行、ビジネス継続性など、ステートフル アプリケーションのさまざまなデータ管理要件に使用できます。

VMware vSphere では、 NetApp ONTAPツールは、データストアのプロビジョニングに使用できる vCenter プラグインを提供します。タグを適用し、OpenShift で使用してノード構成とデータを保存します。 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。

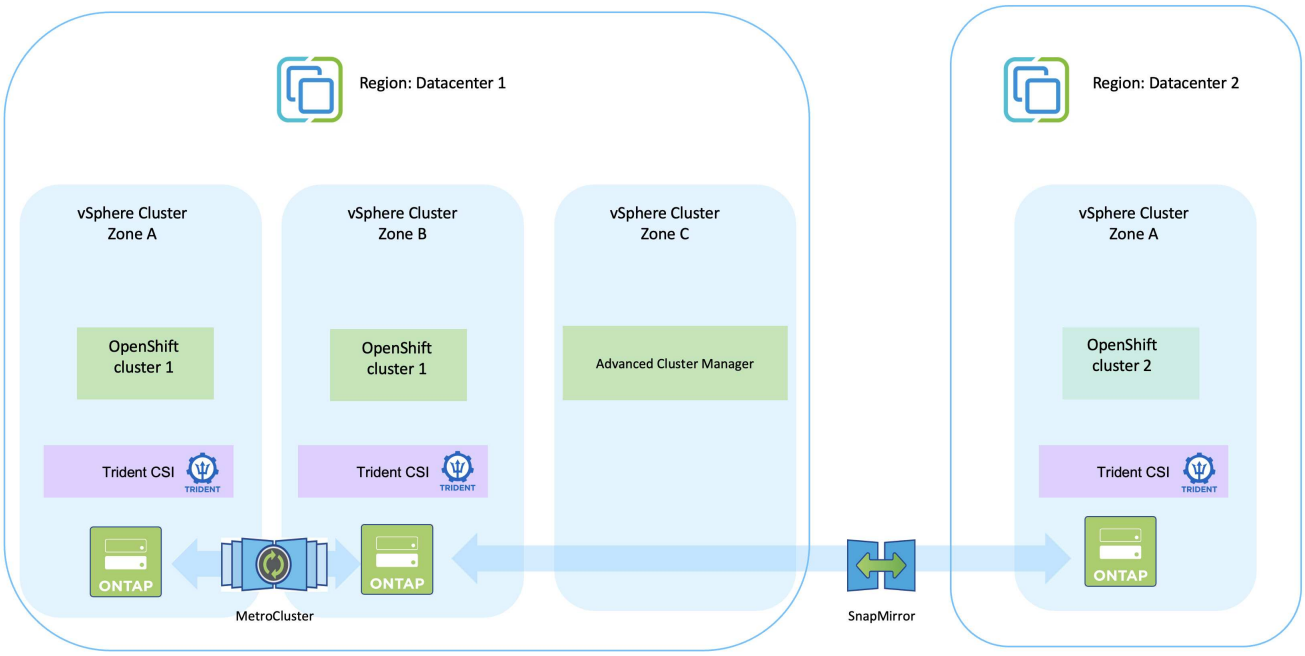


VMware 上で Red Hat OpenShift Container プラットフォームをデプロイおよび構成する

このセクションでは、OpenShift クラスターをセットアップおよび管理し、その上でステートフル 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。これは、永続ボリュームを提供するためにTridentを活用したNetApp ONTAPストレージ アレイの使用方法を示しています。

> Red Hat OpenShift Container プラットフォーム クラスターをデプロイする方法はいくつかあります。このセットアップの概要説明には、使用された特定の方法に関するドキュメント リンクが提供されます。その他の方法については、以下の関連リンクを参照してください。"リソースセクション"。

以下は、データセンター内の VMware に展開されたクラスターを示す図です。



セットアッププロセスは次の手順に分けられます。

▼ **CentOS VM**のデプロイと構成

- VMware vSphere 環境に展開されます。
- この VM は、ソリューションのNetApp TridentやNetApp Trident Protect などのコンポーネントを展開するために使用されます。
- インストール中にこの VM にルート ユーザーが構成されます。

▼ **VMware vSphere (**ハブ クラスター**)** 上に **OpenShift Container Platform** クラスターをデプロイして構成する

OCPクラスタをデプロイするための"支援展開"方法の手順を参照してください。

次の点に注意してください: - インストーラーに提供する ssh 公開キーと秘密キーを作成します。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。 - アシストインストーラーからインストーラー プログラムをダウンロードします。このプログラムは、マスター ノードとワーカー ノード用に VMware vSphere 環境で作成した VM を起動するために使用されます。 - VM には最低限の CPU、メモリ、ハード ディスクの要件が必要です。 （vm createコマンドについては、"事項を"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 でディスク UUID を有効にする必要があります。 - マスター用に最低 3 つのノード、ワーカー用に最低 3 つのノードを作成します。 - インストーラー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。

▼ ハブクラスタに高度なクラスタ管理をインストールする

これは、ハブ クラスター上の Advanced Cluster Management Operator を使用してインストールされます。説明書を参照してください"ここをクリックしてください。"。

▼ **2**つの追加の**OCP**クラスタ（ソースと宛先）をインストールする

- 追加のクラスターは、ハブ クラスター上の ACM を使用してデプロイできます。

- 説明書を参照してください"ここをクリックしてください。"。

▼ **NetApp ONTAP**ストレージを構成する

- VMWare 環境内の OCP VM に接続できるONTAPクラスターをインストールします。
- SVMを作成する
- SVM 内のストレージにアクセスできるように NAS データ ライフを設定します。

▼ **OCP** クラスタに**NetApp Trident**をインストールする

- ハブ、ソース、および宛先クラスタの3つのクラスタすべてにNetApp Tridentをインストールします。
- 説明書を参照してください"ここをクリックしてください。"。
- ontap-nas のストレージ バックエンドを作成します。
- ontap-nas のストレージ クラスを作成します。
- 説明書を参照してください"ここをクリックしてください。"。

▼ ソースクラスタにアプリケーションをデプロイする

OpenShift GitOps を使用してアプリケーションをデプロイします。 (例: Postgres、Ghost)

次のステップは、 Trident Protect を使用してデータ保護と、ソース クラスターから宛先クラスターへのデータ移行を行うことです。参照する"ここをクリックしてください。"手順についてはこちらをご覧ください。

Trident Protectを使用したデータ保護

このページでは、Trident Protect を使用して VMware vSphere 上で稼働する Red Hat OpenShift コンテナベースアプリケーションのデータ保護オプションを表示します。

ユーザーがRed Hat OpenShiftでアプリケーションを近代化する過程において、誤って削除したり、その他の人為的なエラーが発生したりしないように、データ保護戦略を策定する必要があります。多くの場合、規制やコンプライアンス上の理由から、災害からデータを保護するための保護戦略も必要になります。

データ保護の要件は、ある時点のコピーに戻すことから、人間の介入なしに別の障害ドメインに自動的にフェイルオーバーすることまで多岐にわたります。多くのお客様が、マルチテナンシー、マルチプロトコル、高パフォーマンスと高容量の提供、複数サイト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を備えているため、Kubernetes アプリケーション用の優先ストレージ プラットフォームとしてONTAPを選択しています。

Trident Protectを使用したコンテナワークロードの保護と移行の詳細については、次のセクションを参照してください：- "Trident Protectを使用したコンテナアプリの保護と移行"

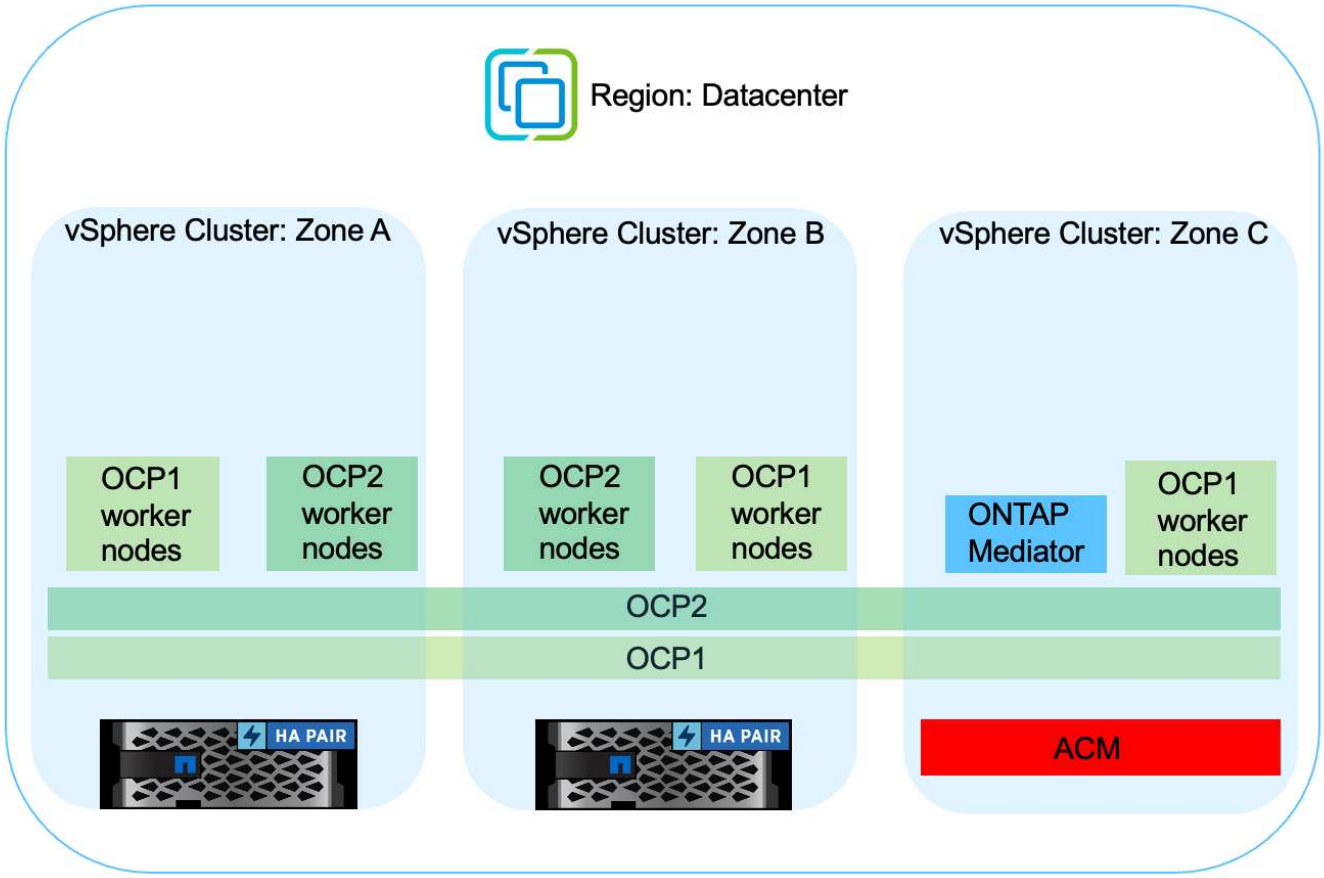
MetroClusterによるビジネス継続性

ONTAP向けの当社のハードウェア プラットフォームのほとんどには、デバイス障害から保護し、災害復旧を実行する必要性を回避する高可用性機能が備わっています。しかし、火災やその他の災害から保護し、RPO ゼロ、RTO の低さでビジネスを継続するために、 MetroClusterソリューションが使用されることがよくあります。

現在ONTAPシステムをお持ちのお客様は、距離制限内でサポートされているONTAPシステムを追加することでMetroClusterに拡張し、ゾーン レベルの災害復旧を提供できます。 Trident 、CSI (Container Storage Interface) は、 MetroCluster構成を含むNetApp ONTAP のほか、 Cloud Volumes ONTAP、 Azure NetApp

Files、AWS FSx ONTAPなどのオプションもサポートします。TridentはONTAP用に 5 つのストレージ ドライバー オプションを提供し、すべてMetroCluster構成でサポートされています。参照する"ここをクリックしてください。"Tridentでサポートされ ているONTAPストレージ ドライバーの詳細については、 を参照してください。

MetroClusterソリューションでは、レイヤー 2 ネットワーク拡張または両方の障害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機能が必要です。 MetroCluster構成が設定されると、 MetroCluster SVM 内のすべてのボリュームが保護され、 SyncMirror (ゼロ RPO) の利点が得られるため、ソリューションはアプリケーション所有者に対して透過的になります。



Tridentバックエンド構成 (TBC) の場合、 MetroCluster構成を使用するときは、dataLIF と SVM を指定しないでください。管理LIF の SVM 管理 IP を指定し、vsadmin ロールの資格情報を使用します。

Trident Protectデータ保護機能の詳細については、"ここをクリックしてください。"を参照してください。

自己管理コンポーネントを備えたハイブリッドクラウド

ハイブリッドクラウドにおける **Red Hat OpenShift Container** プラットフォームのワークロードに対応した**NetApp**ソリューション

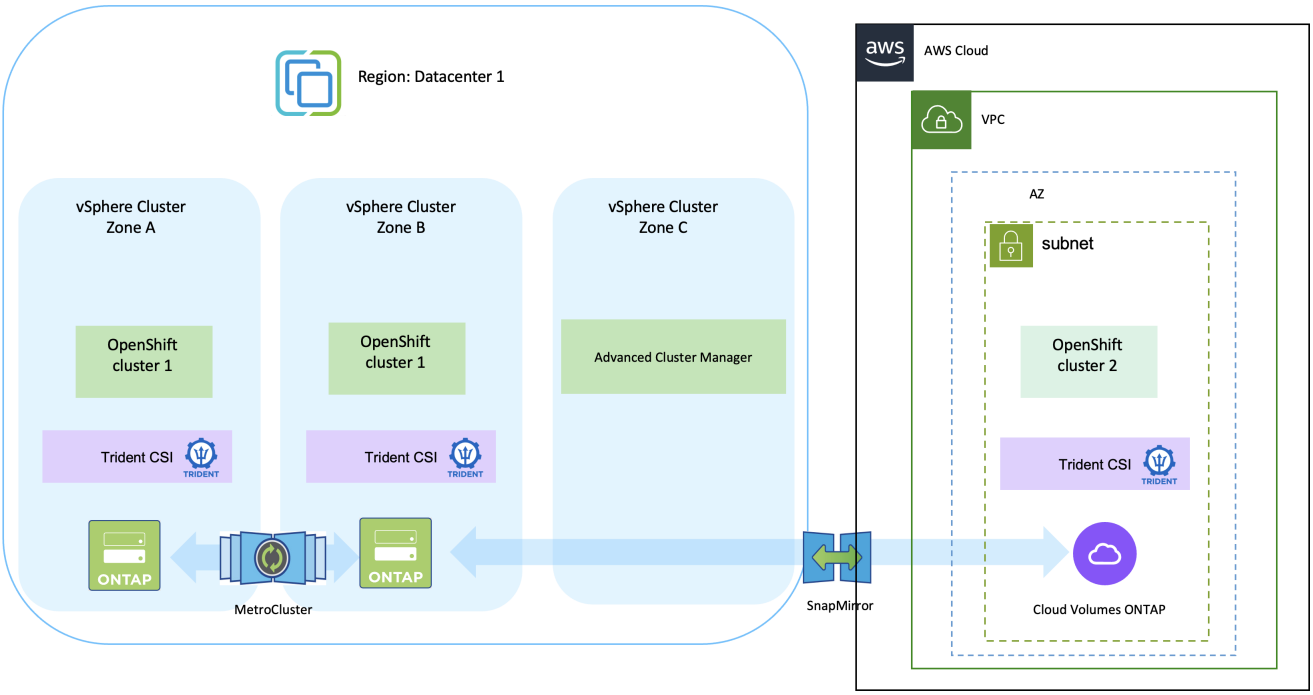
顧客は、モダナイゼーションの取り組みの中で、一部の選択したワークロードまたはすべてのワークロードをデータセンターからクラウドに移行する準備が整っている場合があります。さまざまな理由から、クラウドでセルフ管理型 OpenShift コンテナとセルフ

管理型NetAppストレージを使用することを選択する場合があります。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を正常に構築するには、クラウドで Red Hat OpenShift コンテナ プラットフォーム (OCP) を計画して導入する必要があります。 OCP クラスターは、データセンター内の VMware またはベアメタル、およびクラウド環境内の AWS、Azure、または Google Cloud に展開できます。

NetApp Cloud Volumes ONTAP ストレージは、AWS、Azure、Google Cloud でのコンテナ展開にデータ保護、信頼性、柔軟性を提供します。Trident は、顧客のステートフル アプリケーション用の永続的な Cloud Volumes ONTAP ストレージを消費するための動的ストレージプロビジョナーとして機能します。Trident Protect は、データ保護、移行、ビジネス継続性などのステートフル アプリケーションのデータ管理要件に使用できます。

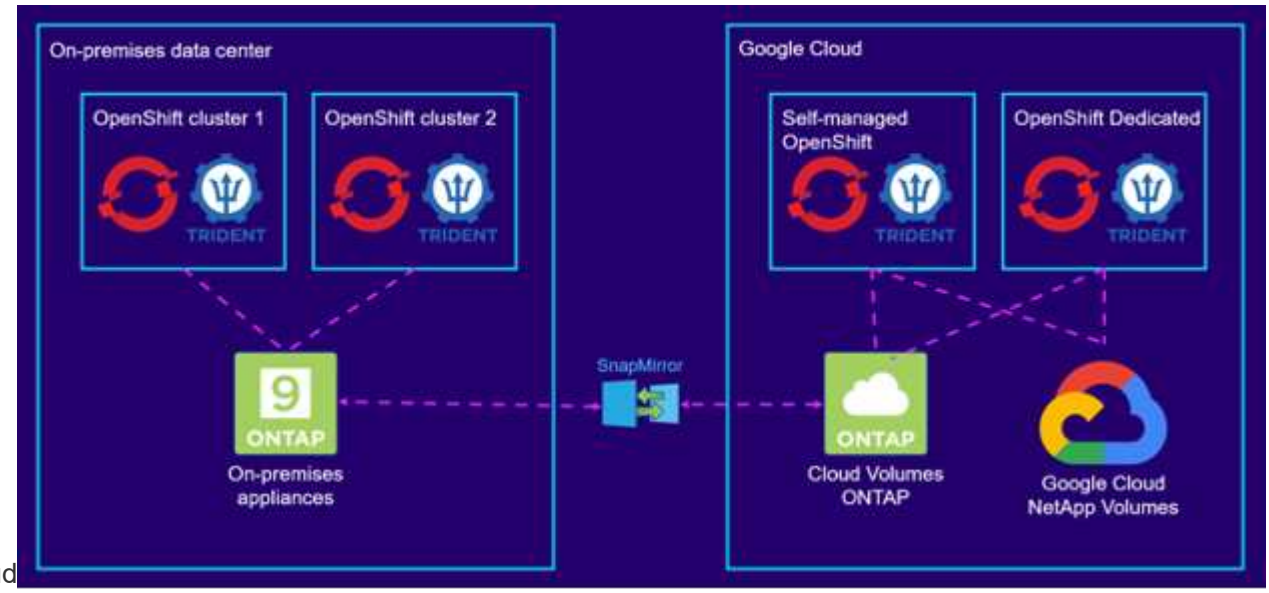
Trident Protectを使用したハイブリッド クラウドにおける **OpenShift Container** ワークロードのデータ保護および移行ソリューション

オンプレミスと
AWS

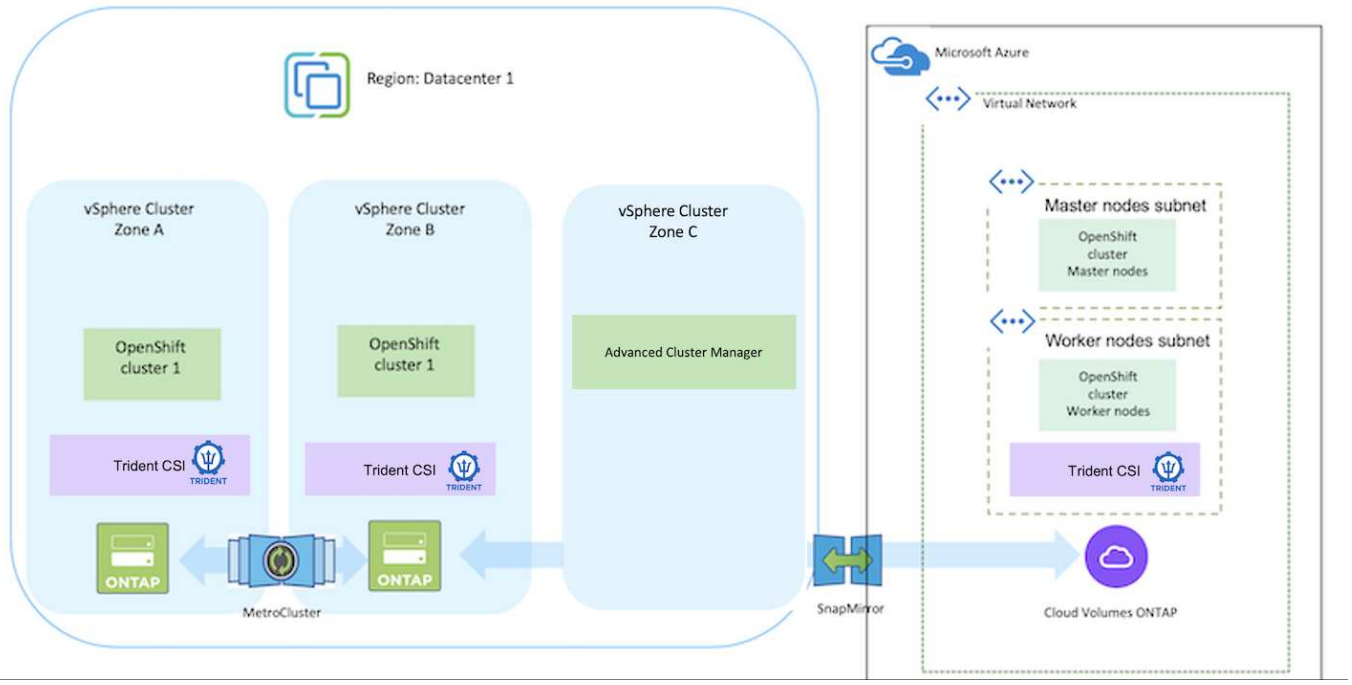


オンプレミスとGoogle

Cloud



オンプレミスとAzureクラウド



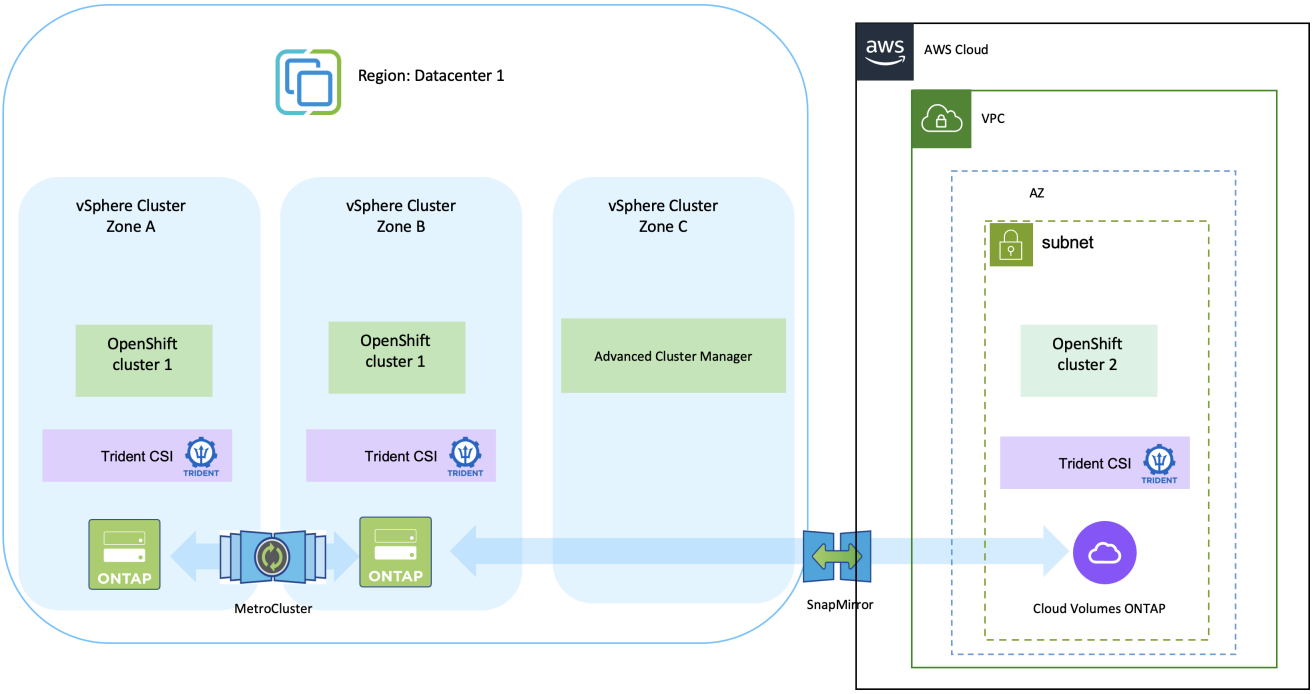
AWS 上で Red Hat OpenShift Container プラットフォームをデプロイおよび構成する

このセクションでは、AWS で OpenShift クラスターをセットアップおよび管理し、そこにステートフルアプリケーションをデプロイする方法の高レベルのワークフローについて説明します。これは、永続ボリュームを提供するためにTridentを活用したNetApp Cloud Volumes ONTAPストレージの使用方法を示しています。 Trident Protect を使用してステートフル アプリケーションのデータ保護および移行アクティビティを実行する方法について詳しく説明します。

AWS に Red Hat OpenShift Container プラットフォーム クラスターをデプロイする方法はいく

つかあります。このセットアップの概要説明には、使用された特定の方法に関するドキュメント リンクが提供されます。その他の方法については、以下の関連リンクを参照してください。"リソースセクション" 。

以下は、AWS にデプロイされ、VPN を使用してデータセンターに接続されたクラスターを示す図です。



セットアッププロセスは次の手順に分けられます。

▼ 高度なクラスター管理から **AWS** に **OCP** クラスターをインストールします。

- オンプレミス ネットワークに接続するために、サイト間 VPN 接続 (pfsense を使用) を持つ VPC を作成します。
- オンプレミス ネットワークにはインターネット接続があります。
- 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 用の Route 53 プライベートホストゾーンと DNS リゾルバーを作成します。

Advanced Cluster Management（ACM）ウィザードからAWS上にOpenShiftクラスタを作成します。手順を参照してください"ここをクリックしてください。"。

OpenShift Hybrid Cloud コンソールから AWS にクラスタを作成することもできます。手順については、"ここをクリックしてください。" を参照してください。

ACM を使用してクラスターを作成する場合、フォーム ビューに詳細を入力した後に 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。クラスターが作成された後、トラブルシューティングや追加の手動構成のために、クラスターのノードに SSH ログインできます。インストール時に指定した SSH キーとユーザー名 core を使用してログインします。

▼ **NetApp Console** を使用して、**AWS** に **Cloud Volumes ONTAP** を展開します。

- 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。説明書を参照してください"ここをクリックしてください。"。
- コネクタを使用して AWS に CVO インスタンスをデプロイします。説明書を参照してください"ここをクリックしてください。"。

> コネクタはクラウド環境にもインストールできます。参照する"ここをクリックしてください。"追加情報については。

▼ **OCP** クラスターに**Trident**をインストールする

- Helm を使用して Trident Operator をデプロイします。手順を参照してください"ここをクリックしてください。"
- バックエンドとストレージ クラスを作成します。説明書を参照してください"ここをクリックしてください。"。

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する

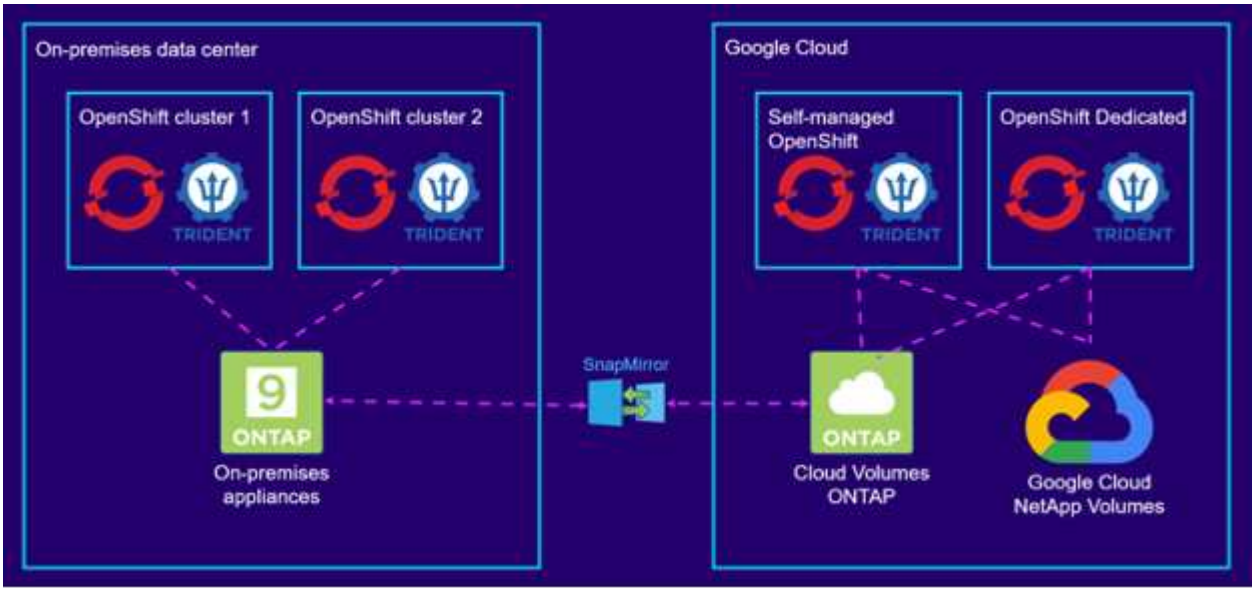
現在、クラウド プロバイダーは、Kubernetes/OpenShift クラスター管理者がゾーン ベースのクラスターのノードを生成できるようにしています。ノードは、リージョン内の異なるアベイラビリティーゾーン、または複数のリージョンに配置できます。マルチゾーン アーキテクチャでのワークロードのボリュームのプロビジョニングを容易にするために、 Trident はCSI トポロジを使用します。 CSI トポロジ機能を使用すると、リージョンとアベイラビリティーゾーンに基づいて、ボリュームへのアクセスをノードのサブセットに制限できます。参照する"ここをクリックしてください。"詳細については、こちらをご覧ください。

> Kubernetes は 2 つのボリューム バインディング モードをサポートしています。 - ***VolumeBindingMode*** が ***Immediate*** (デフォルト) に設定されている場合、 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、要求元の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 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、PVC の永続ボリュームの作成とバインドは遅延されます。このようにして、トポロジ要件によって適用されるスケジュール制約を満たすボリュームが作成されます。 Tridentストレージ バックエンドは、可用性ゾーンに基づいてボリュームを選択的にプロビジョニングするように設計できます (トポロジ対応バックエンド)。このようなバックエンドを利用する StorageClasses の場合、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によって要求された場合にのみ作成されます。 （トポロジー対応ストレージクラス）参照"ここをクリックしてください。"詳細については、こちらをご覧ください。

Google Cloud に Red Hat OpenShift Container Platform をデプロイして構成する

このセクションでは、GCP で OpenShift クラスターをセットアップおよび管理し、そこにステートフル アプリケーションをデプロイする方法のワークフローの概要について説明します。これは、永続ボリュームを提供するためにTridentを利用してGoogle Cloud NetApp VolumesとNetApp Cloud Volumes ONTAPストレージを使用する方法を示しています。

以下は、GCP にデプロイされ、VPN を使用してデータセンターに接続されたクラスターを示す図です。



GCP に Red Hat OpenShift Container Platform クラスターをデプロイする方法はいくつかあります。このセットアップの概要説明には、使用された特定の方法に関するドキュメント リンクが提供されます。その他の方法については、以下の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られます。

CLI から **GCP** に **OCP** クラスタをインストールする

- 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てください"ここをクリックしてください。"。
- オンプレミスと GCP 間の VPN 接続用に、pfsense VM が作成および構成されました。手順については、"ここをクリックしてください。" 。
  - 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構成できます。
  - フェーズ 2 のリモート ネットワーク IP アドレスは、OpenShift クラスター インストール プログラムが実行され、クラスター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構成できます。
  - 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構成できます。
- 次に、GCP に OpenShift クラスター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取得し、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デプロイします "ここをクリックしてください。"。
  - インストールにより、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、A 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。
  - クラスターのインストールが完了し、クラスターのコンソールにログインするための kubeconfig ファ

イルとユーザー名とパスワードが提供されます。

Google Cloud NetApp Volumesをデプロイする

- Google Cloud NetApp Volumesは、概要に従ってプロジェクトに追加できます。"ここをクリックしてください。" 。

NetApp Consoleを使用して**GCP**に**Cloud Volumes ONTAP**を展開する

- Google CloudにConsoleエージェントをインストールします。手順を参照してください "ここをクリックしてください。"。
- エージェントを使用して、Google Cloud に CVO インスタンスをデプロイします。手順を参照してください "ここをクリックしてください。"。

GCP の **OCP** クラスタに**Trident**をインストールする

- 以下に示すように、Trident を導入する方法は多数あります "ここをクリックしてください。"。
- このプロジェクトでは、 "ここをクリックしてください。"の手順に従って Trident Operator を手動でデプロイすることで、Trident をインストールしました。
- バックエンドとストレージ クラスを作成します。説明書を参照してください"ここをクリックしてください。"。

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する

現在、クラウド プロバイダーは、Kubernetes/OpenShift クラスター管理者がゾーン ベースのクラスターのノードを生成できるようにしています。ノードは、リージョン内の異なるアベイラビリティーゾーン、または複数のリージョンに配置できます。マルチゾーン アーキテクチャでのワークロードのボリュームのプロビジョニングを容易にするために、 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、リージョンとアベイラビリティーゾーンに基づいて、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。参照する"ここをクリックしてください。"詳細については、こちらをご覧ください。

> Kubernetes は 2 つのボリューム バインディング モードをサポートしています。 - ***VolumeBindingMode*** が ***Immediate*** (デフォルト) に設定されている場合、 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、要求元の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 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、PVC の永続ボリュームの作成とバインドは遅延されます。このようにして、トポロジ要件によって適用されるスケジュール制約を満たすボリュームが作成されます。 Tridentストレージ バックエンドは、可用性ゾーンに基づいてボリュームを選択的にプロビジョニングするように設計できます (トポロジ対応バックエンド)。このようなバックエンドを利用する StorageClasses の場合、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によって要求された場合にのみ作成されます。 （トポロジー対応ストレージクラス）参照"ここをクリックしてください。"詳細については、こちらをご覧ください。

デモビデオ

Google Cloud Platform への OpenShift Cluster のインストール

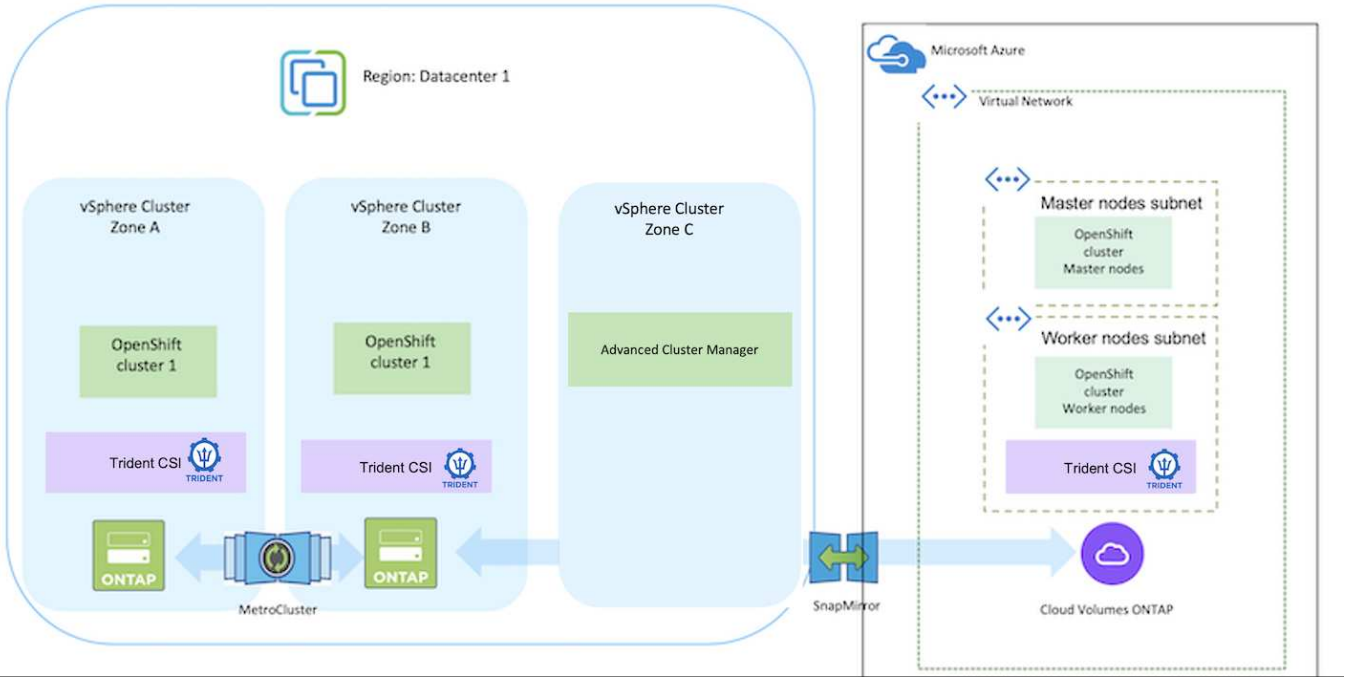
OpenShift クラスターをTrident Protect にインポートする

Azure に Red Hat OpenShift Container プラットフォームをデプロイして構成する

このセクションでは、Azure で OpenShift クラスターをセットアップおよび管理し、そ

こにステートフル アプリケーションをデプロイする方法の大まかなワークフローについて説明します。これは、永続ボリュームを提供するためにTridentを活用したNetApp Cloud Volumes ONTAPストレージの使用方法を示しています。 Trident Protect を使用してステートフル アプリケーションのデータ保護および移行アクティビティを実行する方法について詳しく説明します。

以下は、Azure にデプロイされ、VPN を使用してデータ センターに接続されたクラスターを示す図です。



Azure に Red Hat OpenShift Container Platform クラスターをデプロイする方法はいくつかあります。このセットアップの概要説明には、使用された特定の方法に関するドキュメント リンクが提供されます。その他の方法については、以下の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られます。

▼ **CLI** から **Azure** に **OCP** クラスター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てください"ここをクリックしてください。"。
- 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 ゲートウェイとサイト間 VPN 接続を作成します。
- オンプレミスと Azure 間の VPN 接続用に、pfsense VM が作成および構成されました。手順については、"ここをクリックしてください。" 。
- インストールプログラムとプルシークレットを取得し、ドキュメントに記載されている手順に従ってクラスターをデプロイします"ここをクリックしてください。"。
- クラスターのインストールが完了し、クラスターのコンソールにログインするための kubeconfig ファイルとユーザー名とパスワードが提供されます。

サンプルの install-config.yaml ファイルを以下に示します。

```
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:
```

▼ **NetApp Console**を使用して**Azure**に**Cloud Volumes ONTAP**を展開します。

- Azure に NetApp Console エージェントをインストールします。手順を参照してください "ここをクリックしてください。"。
- エージェントを使用して、AzureにCVOインスタンスをデプロイします。手順"ここをクリックしてください。"を参照してください。

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する

現在、クラウド プロバイダーは、Kubernetes/OpenShift クラスター管理者がゾーン ベースのクラスターのノードを生成できるようにしています。ノードは、リージョン内の異なるアベイラビリティーゾーン、または複数のリージョンに配置できます。マルチゾーン アーキテクチャでのワークロードのボリュームのプロビジョニングを容易にするために、 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、リージョンとアベイラビリティーゾーンに基づいて、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。参照する"ここをクリックしてください。"詳細については、こちらをご覧ください。

> Kubernetes は 2 つのボリューム バインディング モードをサポートしています。 - ***VolumeBindingMode*** が ***Immediate*** (デフォルト) に設定されている場合、 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、要求元の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 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、PVC の永続ボリュームの作成とバインドは遅延されます。このようにして、トポロジ要件によって適用されるスケジュール制約を満たすボリュームが作成されます。 Tridentストレージ バックエンドは、可用性ゾーンに基づいてボリュームを選択的にプロビジョニングするように設計できます (トポロジ対応バックエンド)。このようなバックエンドを利用する StorageClasses の場合、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によって要求された場合にのみ作成されます。 （トポロジー対応ストレージクラス）参照"ここをクリックしてください。"詳細については、こちらをご覧ください。

Trident Protectを使用したデータ保護

Trident Protectを使用したコンテナワークロードの保護と移行の詳細については、次のセクションを参照してください：- "Trident Protectを使用したコンテナアプリの保護と移行"

プロバイダー管理コンポーネントを備えたハイブリッドクラウド

マネージド Red Hat OpenShift Container プラットフォーム ワークロードを備えたNetAppソリューション

お客様は「クラウド生まれ」の場合もあれば、モダナイゼーションの過程で、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ている場合もあります。ワークロードを実行するために、クラウド内のプロバイダー管理の OpenShift コンテナとプロバイダー管理のNetAppストレージを使用することを選択できます。コンテナ ワークロードに適した本番環境を正常に構築するには、マネージド Red Hat OpenShift コンテナ クラスターをクラウドで計画して導入する必要があります。 NetApp は、3 つの主要なパブリック クラウドすべてにおいて、マネージド Red Hat ソリューション向けに完全に管理されたストレージ サービスを提供します。

- Amazon FSx for NetApp ONTAP (FSx ONTAP)*

FSx ONTAP は、AWS でのコンテナ展開にデータ保護、信頼性、柔軟性を提供します。 Trident は、顧客のステートフル アプリケーション用に永続的な FSx ONTAPストレージを使用する動的ストレージ プロビジョナーとして機能します。

ROSA は、コントロール プレーン ノードを複数のアベイラビリティ ゾーンに分散して HA モードで展開できるため、FSx ONTAPも、高可用性を提供し、AZ 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できます。

- Google Cloud NetApp Volumes*

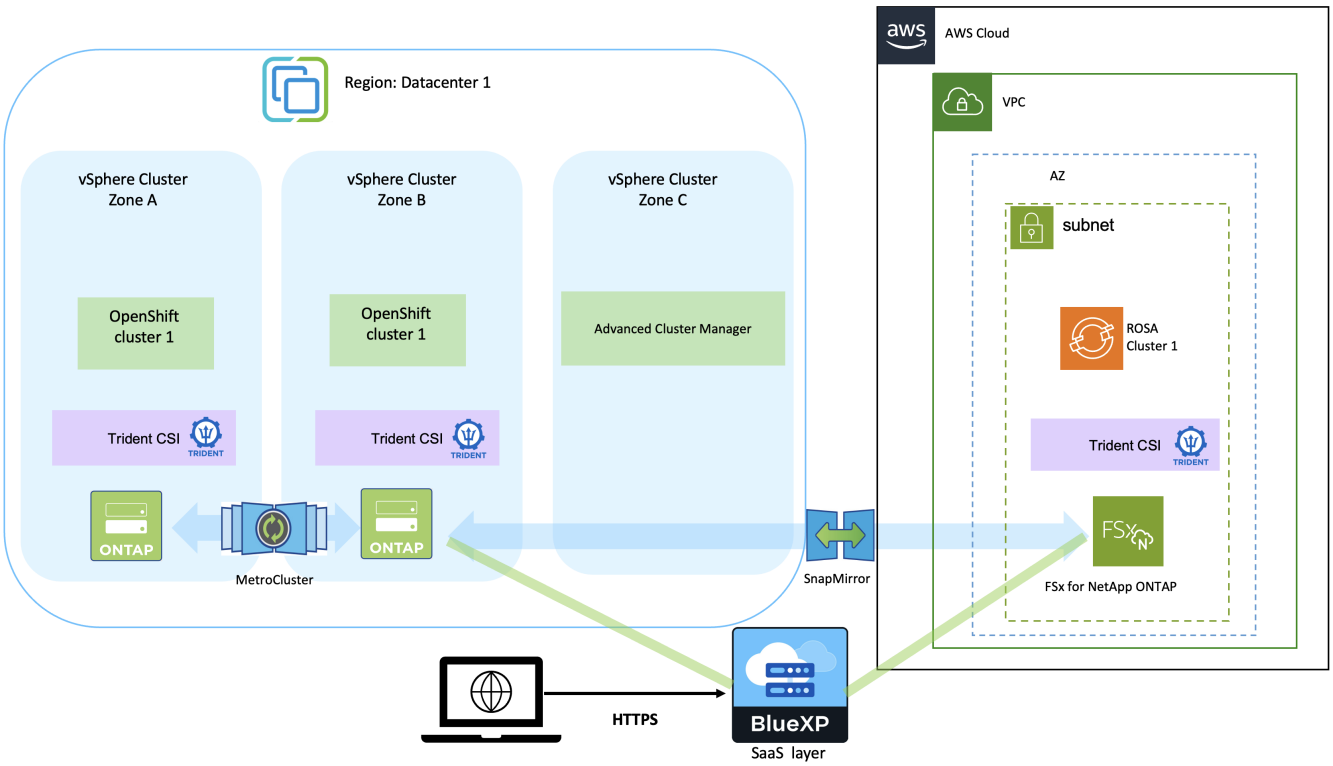
Red Hat OpenShift Dedicated は、ハイブリッド クラウド全体でアプリケーションを迅速に構築、デプロイ、拡張できる、完全に管理されたアプリケーション プラットフォームです。 Google Cloud NetApp Volumes は永続ボリュームを提供し、ONTAP のエンタープライズ データ管理機能の完全なスイートを Google Cloud の OpenShift デプロイメントに提供します。

AWS 上でマネージド Red Hat OpenShift Container プラットフォームをデプロイおよび構成する

このセクションでは、AWS（ROSA）上でマネージドRed Hat OpenShiftクラスタを設定する概要ワークフローについて説明します。ここでは、永続ボリュームを提供するために、Tridentがストレージバックエンドとしてマネージドamazon FSx for NetApp ONTAP（FSx ONTAP）を使用する方法を示します。NetApp Consoleを使用したAWS上でのFSx ONTAPの導入について詳しく説明します。また、NetApp ConsoleとOpenShift GitOps（Argo CD）を使用して、ROSAクラスタ上のステートフルアプリケーションの

データ保護および移行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。

以下は、AWS にデプロイされ、バックエンドストレージとして FSx ONTAPを使用している ROSA クラスターを示す図です。



このソリューションは、AWS の 2 つの VPC 内の 2 つの ROSA クラスターを使用して検証されました。各 ROSA クラスターは、 Tridentを使用して FSx ONTAPと統合されました。 AWS に ROSA クラスターと FSx ONTAPをデプロイする方法はいくつかあります。このセットアップの概要説明には、使用された特定の方法に関するドキュメント リンクが提供されます。その他の方法については、以下の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られます。

ROSAクラスタをインストールする

- 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。
- ROSAクラスタのインストール手順については、"ここをクリックしてください。"を参照してください。

FSx ONTAPをインストールする

- NetApp ConsoleからVPCにFSx ONTAPをインストールします。NetApp Consoleアカウントの作成と利用開始については、"ここをクリックしてください。"を参照してください。FSx ONTAPのインストールについては、"ここをクリックしてください。"を参照してください。FSx ONTAPを管理するためのAWSでのコネクタの作成については、"ここをクリックしてください。"を参照してください。
- AWS を使用して FSx ONTAPをデプロイします。参照する"ここをクリックしてください。"AWS コンソールを使用してデプロイします。

ROSA クラスターに**Trident**をインストールする **(Helm** チャートを使用)

- Helm チャートを使用して ROSA クラスターに Trident をインストールします。ドキュメントへのリンク

を参照してください：https://docs.netapp.com/us-en/trident/trident-install/kubernetes-deploy-helm.html[ここ^]。

ROSA クラスタ向け FSx ONTAPとTridentの統合

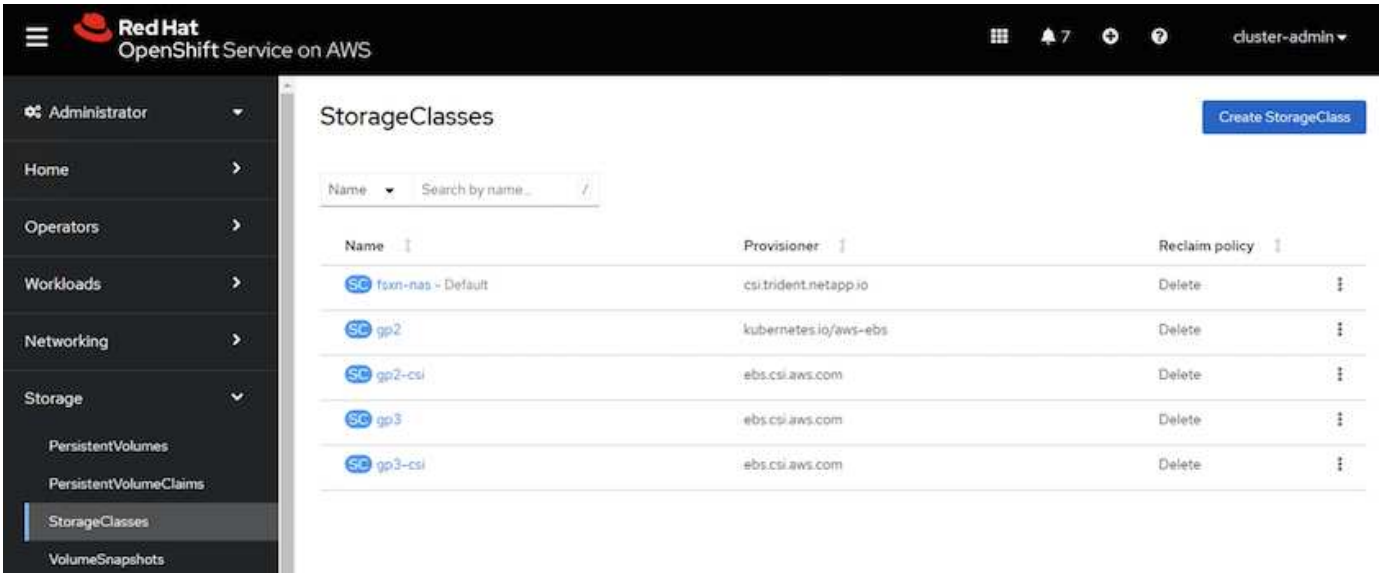
OpenShift GitOps を利用すると、ApplicationSet を使用して ArgoCD に登録されたすべての管理対象クラスターにTrident CSI をデプロイできます。

```
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を使用してバックエンドとストレージ クラスを作成する **(FSx ONTAP**用**)**

- 参照する"ここをクリックしてください。"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、こちらをご覧ください。
- OpenShift コンソールから、 Trident CSI を使用して FsxN 用に作成されたストレージ クラスをデフォルトにします。下のスクリーンショットを参照してください。



OpenShift GitOps (Argo CD) を使用してアプリケーションをデプロイする

- クラスターにOpenShift GitOpsオペレーターをインストールします。手順"ここをクリックしてください。"を参照してください。
- クラスター用の新しいArgo CDインスタンスをSetUpします。手順"ここをクリックしてください。"を参照してください。

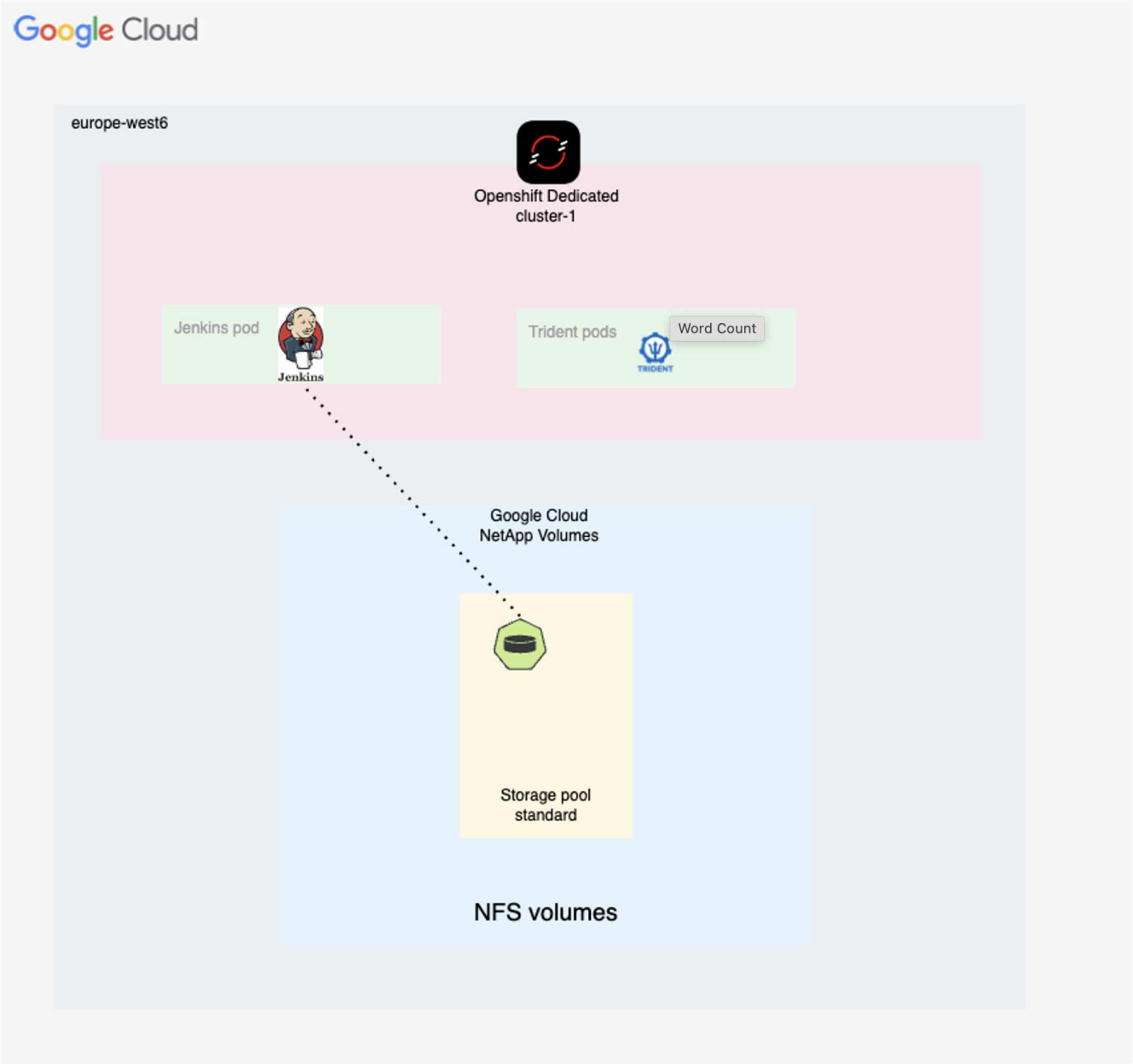
Argo CD のコンソールを開き、アプリケーションをデプロイします。例えば、Argo CD と Helm チャートを使用して Jenkins アプリをデプロイすることができます。アプリケーションを作成する際に、以下の詳細情報が提供されました： Project: default cluster: 'https://kubernetes.default.svc'[]（引用符なし） Namespace: Jenkins Helm チャートの URL: 'https://charts.bitnami.com/bitnami'[]（引用符なし）

Helm パラメータ: global.storageClass: fsxn-nas

Google Cloud NetApp Volumesを使用して **Google Cloud** に **OpenShift Dedicated** をデプロイおよび構成する

このセクションでは、Google Cloud プラットフォームで OpenShift Dedicated（OSD）クラスタを設定するための大まかなワークフローについて説明します。これは、 NetApp TridentがGoogle Cloud NetApp Volumes をストレージ バックエンドとして使用し、Kubernetes で実行されるステートフル アプリケーションに永続ボリュームを提供する様子を示しています。

以下は、Google Cloud にデプロイされ、バックエンド ストレージとしてNetApp Volumes を使用しているOSD クラスタを示す図です。



セットアッププロセスは次の手順に分けられます。

Google Cloud に **OSD** クラスタをインストールする

- クラスターに既存の VPC を使用する場合は、OSD クラスター用に VPC、2 つのサブネット、クラウドルーター、および 2 つの GCP クラウド NAT を作成する必要があります。参照する"ここをクリックしてください。"手順についてはこちらをご覧ください。
- Customer Cloud Subscription（CCS）課金モデルを使用してGCPにOSDクラスターをインストールする手順については、"ここをクリックしてください。"を参照してください。OSDはGoogle Cloud Marketplaceにも含まれています。Google Cloud Marketplaceソリューションを使用してOSDをインストールする方法を示すビデオは、"ここをクリックしてください。"にあります。

Google Cloud NetApp Volumesを有効にする

- 参照する"ここをクリックしてください。"Google Cloud NetApp Volumesへのアクセスの設定方法については、こちらをご覧ください。ここまでのすべての手順に従ってください

- ストレージ プールを作成します。参照する"ここをクリックしてください。"Google Cloud NetApp Volumesでストレージ プールを設定する方法については、こちらをご覧ください。 OSD 上で実行されるステートフル Kubernetes アプリケーションのボリュームは、ストレージ プール内に作成されます。

OSD クラスターに**Trident**をインストールする **(Helm** チャートを使用**)**

- Helm チャートを使用して、OSD クラスタに Trident をインストールします。Helm Chart のインストール方法については、"ここをクリックしてください。"を参照してください。

OSD クラスタ用の**NetApp Volumes** と**NetApp Trident**の統合

Tridentを使用してバックエンドとストレージ クラスを作成する (Google Cloud NetApp Volumes用)

- バックエンドの作成の詳細については、ここを参照してください。
- Kubernetes の現在のストレージ クラスのいずれかがデフォルトとしてマークされている場合は、ストレージ クラスを編集してその注釈を削除します。
- Trident CSI プロビジョナーを使用して、 NetAppボリューム用に少なくとも 1 つのストレージ クラスを作成します。アノテーションを使用して、ストレージ クラスの 1 つだけをデフォルトにします。これにより、PVC マニフェストで明示的に呼び出されていない場合でも、PVC はこのストレージ クラスを使用できるようになります。注釈付きの例を以下に示します。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-standard-k8s
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: true
```

OpenShift GitOps (Argo CD) を使用してアプリケーションをデプロイする

- クラスターにOpenShift GitOpsオペレーターをインストールします。手順"ここをクリックしてください。"を参照してください。
- クラスター用の新しいArgo CDインスタンスをSetUpします。手順"ここをクリックしてください。"を参照してください。

Argo CD のコンソールを開き、アプリケーションをデプロイします。例えば、Argo CD と Helm チャートを使用して Jenkins アプリをデプロイすることができます。アプリケーションを作成する際に、以下の詳細情報が提供されました： Project: default cluster: 'https://kubernetes.default.svc'[]（引用符なし） Namespace: Jenkins Helm チャートの URL: 'https://charts.bitnami.com/bitnami'[]（引用符なし）

データ保護

Trident Protectを使用したコンテナワークロードの保護と移行の詳細については、次のセクションを参照してください：- "Trident Protectを使用したコンテナアプリの保護と移

行"

Red Hat OpenShift ワークロード向けの追加のNetAppハイブリッド マルチクラウド ソリューション

以下の追加ソリューションも参照してください。

- "Red Hat OpenShift Container Solutionオンプレミス"
- "Red Hat OpenShift Service on AWS コンテナソリューション"
- "Red Hat OpenShift Virtualization ソリューションオンプレミス"
- "Red Hat OpenShift Service on AWS 仮想化ソリューション"

Trident Protectを使用してデータを保護する

Trident Protectを使用したOpenShift Container Platformのコンテナアプリのデータ保護

このリファレンスドキュメントのこのセクションでは、Trident Protect を使用して Container Apps のスナップショットおよびバックアップを作成する方法の詳細を提供します。NetApp Trident Protect は、NetApp ONTAP ストレージシステムおよび NetApp Trident CSI ストレージプロビジョナーによってサポートされるステートフルな Kubernetes アプリケーションの機能性と可用性を強化する高度なアプリケーションデータ管理機能を提供します。Trident Protect はアプリケーションのスナップショットおよびバックアップを作成します。つまり、永続ボリューム内のアプリケーションデータだけでなく、アプリケーションメタデータについてもスナップショットおよびバックアップが作成されます。Trident Protect によって作成されたスナップショットおよびバックアップは、以下のいずれかのオブジェクトストレージに保存でき、後でそこからリストアすることができます。

- AWS S3
- Azure BLOB ストレージ
- Google Cloud Storage
- ONTAP S3
- ストレージグリッド
- その他の S3 互換ストレージ

Trident Protect は Kubernetes モデルのロールベースアクセス制御（RBAC）を使用します。デフォルトでは、Trident Protect は trident-protect と呼ばれる単一のシステムネームスペースと、それに関連付けられたデフォルトのサービスアカウントを提供します。多数のユーザーを抱える組織や特定のセキュリティニーズを持つ組織の場合は、Trident Protect の RBAC 機能を使用して、リソースとネームスペースへのアクセスをより細かく制御できます。

Trident Protect のロールベースアクセス制御に関する追加情報については、"Trident Protect ドキュメント"を参照してください。

クラスター管理者は、デフォルトの trident-protect 名前空間内のリソースにアクセスでき、他のすべての名前空間内のリソースにもアクセスできます。ユーザーは、trident-protect 名前空間にスナップショットやバックアップ CR などのアプリケーション データ管理カスタム リソース (CR) を作成することはできません。ベストプラクティスとして、ユーザーはアプリケーション名前空間にこれらの CR を作成する必要があります。

Trident Protect はドキュメントに記載されている手順に従ってインストールできます"ここをクリックしてください。"。このセクションでは、Trident Protect を使用したコンテナアプリケーションのデータ保護とアプリケーションの復元のワークフローを示します。1.Snapshot の作成（オンデマンドまたはスケジュール）2.Snapshot からの復元（同じ名前空間と異なる名前空間への復元）3.バックアップ作成 4.バックアップからの復元

▼ 前提条件

アプリケーションのスナップショットとバックアップを作成する前に、スナップショットとバックアップを保存するために Trident Protect でオブジェクトストレージを設定する必要があります。これはバケット CR を使用して行われます。バケット CR を作成して設定できるのは管理者のみです。バケット CR は Trident Protect では AppVault として知られています。AppVault オブジェクトは、ストレージバケットの宣言的な Kubernetes ワークフロー表現です。AppVault CR には、バックアップ、スナップショット、リストア操作、SnapMirror レプリケーションなどの保護操作でバケットを使用するために必要な設定が含まれています。

この例では、ONTAP S3 をオブジェクトストレージとして使用する方法を示します。ONTAP S3 用の AppVault CR を作成するワークフローは次のとおりです：1.ONTAP クラスタの SVM に S3 オブジェクトストアサーバーを作成します。2.オブジェクトストアサーバーにバケットを作成します。3.SVM に S3 ユーザーを作成します。アクセスキーとシークレットキーを安全な場所に保管してください。4.OpenShift で、ONTAP S3 クレデンシャルを格納するシークレットを作成します。5.ONTAP S3 用の AppVault オブジェクトを作成します

ONTAP S3用のTrident Protect AppVaultを設定

ONTAP S3をAppVaultとして使用してTrident Protectを設定するためのサンプルYAMLファイル

```
# alias tp='tridentctl-protect'

appvault-secret.yaml

apiVersion: v1
stringData:
  accessKeyID: "<access key id created for a user to access ONTAP S3
bucket>"
  secretAccessKey: "corresponding Secret Access Key"
#data:
# base 64 encoded values
#  accessKeyID: <base64 access key id created for a user to access ONTAP
S3 bucket>
#  secretAccessKey: <base 64  Secret Access Key>
kind: Secret
metadata:
  name: appvault-secret
```

```
  namespace: trident-protect
type: Opaque

appvault.yaml

apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: <bucket-name for storing the snapshots and backups>
      endpoint: <endpoint IP for S3>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost openshift-benchmark]#
[root@localhost openshift-benchmark]# tp get appvault -n trident-protect
+------------------+----------+-----------+------+-------+
|       NAME       | PROVIDER |   STATE   | AGE  | ERROR |
+------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 2d2h |       |
+------------------+----------+-----------+------+-------+
[root@localhost openshift-benchmark]#
```

postgresql アプリをインストールするためのサンプル **yaml** ファイル

```
postgres.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: postgres
spec:
  replicas: 1
  selector:
    matchLabels:
      app: postgres
  template:
    metadata:
      labels:
        app: postgres
    spec:
      containers:
      - name: postgres
        image: postgres:14
        env:
        - name: POSTGRES_USER
          #value: "myuser"
          value: "admin"
        - name: POSTGRES_PASSWORD
          #value: "mypassword"
          value: "adminpass"
        - name: POSTGRES_DB
          value: "mydb"
        - name: PGDATA
          value: "/var/lib/postgresql/data/pgdata"
        ports:
        - containerPort: 5432
        volumeMounts:
        - name: postgres-storage
          mountPath: /var/lib/postgresql/data
      volumes:
      - name: postgres-storage
        persistentVolumeClaim:
          claimName: postgres-pvc
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: postgres-pvc
spec:
```

```
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 5Gi
---
apiVersion: v1
kind: Service
metadata:
  name: postgres
spec:
  selector:
    app: postgres
  ports:
  - protocol: TCP
    port: 5432
    targetPort: 5432
  type: ClusterIP

Now create the Trident Protect application CR for the postgres app.
Include the objects in the namespace postgres and create it in the
postgres namespace.
# tp create app postgres-app --namespaces postgres -n postgres
```

```
[root@localhost RedHat]# tp get app -n postgres
+--------------+------------+-------+-----+
|     NAME     | NAMESPACES | STATE | AGE |
+--------------+------------+-------+-----+
| postgres-app | postgres   | Ready | 24s |
+--------------+------------+-------+-----+
[root@localhost RedHat]#
```

▼ スナップショットを作成する

オンデマンド スナップショットの作成

```
# tp create snapshot postgres-snap1 --app postgres-app --appvault ontap-
s3-appvault -n postgres
Snapshot "postgres-snap1" created.
```

```
[root@localhost RedHat]# tp get snapshot -n postgres
+-----------------+--------------+-----------+-----+-------+
|      NAME       |   APP REF    |   STATE   | AGE | ERROR |
+-----------------+--------------+-----------+-----+-------+
| postgres-snap1 | postgres-app | Completed | 19s |       |
+-----------------+--------------+-----------+-----+-------+
[root@localhost RedHat]#
```

```
[root@localhost DataProtection]# oc get all,pvc,volumesnapshot -n postgres
Warning: apps.openshift.io/v1 DeploymentConfig is deprecated in v4.14+, unavailable in v4.10000+
Warning: kubevirt.io/v1 VirtualMachineInstancePresets is now deprecated and will be removed in v2.
NAME                            READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-jfx49     1/1     Running   0          3h47m

NAME               TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)    AGE
service/postgres   ClusterIP   172.30.132.112   <none>        5432/TCP   3h47m

NAME                       READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/postgres   1/1     1            1           3h47m

NAME                                  DESIRED   CURRENT   READY   AGE
replicaset.apps/postgres-cd9d6ccb     1         1         1       3h47m

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAG
ECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/data-postgres-postgresql-0    Bound    pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   8Gi        RWO            sc-zon
ea-nas   <unset>                 4h40m
persistentvolumeclaim/postgres-pvc                  Bound    pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   5Gi        RWO            sc-zon
ea-nas   <unset>                 3h47m

NAME                                                                                                                                READYTO
USE   SOURCEPVC                SOURCESNAPSHOTCONTENT   RESTORESIZE   SNAPSHOTCLASS           SNAPSHOTCONTENT
          CREATIONTIME   AGE
volumesnapshot.snapshot.storage.k8s.io/snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true
      postgres-pvc                                      53676Ki       trident-snapshotclass   snapcontent-796ea7f8-59a0-493e-bbd8-3a
e76fe9036c   13m            13m
volumesnapshot.snapshot.storage.k8s.io/snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true
      data-postgres-postgresql-0                        368Ki         trident-snapshotclass   snapcontent-86a464d4-ffd8-4279-9cf7-88
88a097c001   13m            13m
```

スケジュールの作成 次のコマンドを使用すると、スナップショットは毎日 15:33 に作成され、2 つのスナップショットとバックアップが保持されます。

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+-----+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE | ERROR |
+-----------+--------------+----------------------+---------+-------+-----+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 17s |       |
+-----------+--------------+----------------------+---------+-------+-----+-------+
[root@localhost DataProtection]#
```

yaml を使用してスケジュールを作成する

```
# tp create schedule schedule2 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres --dry-run >
hourly-snapshotschedule.yaml

cat hourly-snapshotschedule.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: schedule2
  namespace: postgres
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: postgres-app
  backupRetention: "2"
  dataMover: Restic
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  #hour: "15"
  minute: "33"
  recurrenceRule: ""
  snapshotRetention: "2"
status: {}
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+-------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP     |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+-------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 8d7h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 8d7h |       |
+-----------+-------------+----------------------+---------+-------+------+-------+
[root@localhost DataProtection]#
```

このスケジュールで作成されたスナップショットを表示できます。

```
[root@localhost DataProtection]# tp get snap -n postgres
+-----------------------------+--------------+-----------+-------+-------+
|            NAME             |   APP REF    |   STATE   |  AGE  | ERROR |
+-----------------------------+--------------+-----------+-------+-------+
| hourly-3f1ee-20250214183300 | postgres-app | Completed | 19s   |       |
| postgres-snap1              | postgres-app | Completed | 1h25m |       |
+-----------------------------+--------------+-----------+-------+-------+
[root@localhost DataProtection]#
```

ボリュームのスナップショットも作成されます。

```
[root@localhost DataProtection]# oc get volumesnapshots -n postgres
NAME                                                                                                READYTOUSE   SOURCEPVC
                          CREATIONTIME   AGE
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-59a0-493e-bbd8-3ae76fe9036c   114m           114m
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-ffd8-4279-9cf7-8888a097c001   114m           114m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-7adc-4042-a8c9-7606d1103ead   30m            30m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-3a82-43f6-9868-dcadd2cc04e2   30m            30m
```

▼ アプリケーションを削除してアプリケーションの損失をシミュレートします

```
# oc delete deployment/postgres -n postgres
# oc get pod,pvc -n postgres
No resources found in postgres namespace.
```

▼ スナップショットから同じ名前空間に復元する

```
# tp create sir postgres-sir --snapshot postgres/hourly-3f1ee-
20250214183300 -n postgres
SnapshotInplaceRestore "postgres-sir" created.
```

```
[root@localhost DataProtection]# tp get sir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-sir | ontap-s3-appvault | Completed | 2m39s |       |
+--------------+--------------------+-----------+-------+-------+
```

アプリケーションとその PVC は同じ名前空間に復元されます。

```
[root@localhost DataProtection]# oc get pods,pvc -n postgres
NAME                         READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-x85tg   1/1     Running   0          98s

NAME                                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/data-postgres-postgresql-0   Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>                 105s
persistentvolumeclaim/postgres-pvc                 Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>                 105s
[root@localhost DataProtection]#
```

▼ スナップショットから別の名前空間に復元する

```
# tp create snapshotrestore postgres-restore --snapshot postgres/hourly-3f1ee-20250214183300 --namespace-mapping postgres:postgres-restore -n postgres-restore
SnapshotRestore "postgres-restore" created.
```

```
[root@localhost DataProtection]# tp get snapshotrestore -n postgres-restore
+------------------+--------------------+-----------+-------+-------+
|       NAME       |      APPVAULT      |   STATE   |  AGE  | ERROR |
+------------------+--------------------+-----------+-------+-------+
| postgres-restore | ontap-s3-appvault | Completed | 1m15s |       |
+------------------+--------------------+-----------+-------+-------+
```

アプリケーションが新しい名前空間に復元されたことがわかります。

```
[root@localhost DataProtection]#
[root@localhost DataProtection]# oc get pods,pvc -n postgres-restore
NAME                         READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-pfxw9   1/1     Running   0          8d

NAME                                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/data-postgres-postgresql-0   Bound    pvc-3dff4e42-828d-49f9-84e9-4daf75479292   8Gi        RWO            sc-zonea-nas
persistentvolumeclaim/postgres-pvc                 Bound    pvc-f57321b2-f21f-4eb7-8f86-4a17f915318b   5Gi        RWO            sc-zonea-nas
[root@localhost DataProtection]#
```

▼ バックアップを作成する

オンデマンド バックアップの作成

```
# tp create backup postgres-backup1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup1" created.
```

```
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d12h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d10h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 10h36m |       |
| hourly-3f1ee-20250224003300 | postgres-app | Completed | 1h36m  |       |
| hourly-3f1ee-20250224013300 | postgres-app | Completed | 36m27s |       |
| postgres-backup1             | postgres-app | Completed | 6m19s  |       |
+------------------------------+--------------+-----------+--------+-------+
```

バックアップのスケジュールを作成

上記のリストにある毎日のバックアップと毎時のバックアップは、以前に設定されたスケジュールから作成されます。

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+--------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 9d8h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 9d8h |       |
+-----------+--------------+----------------------+---------+-------+------+-------+
```

▼ バックアップからの復元

データ損失をシミュレートするには、アプリケーションと **PVC** を削除します。

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                    READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-dftkt   1/1     Running   0          11s
[root@localhost DataProtection]# oc get deployment -n postgres
NAME       READY   UP-TO-DATE   AVAILABLE   AGE
postgres   1/1     1            1           20s
[root@localhost DataProtection]# oc delete deployment/postgres -n postgres
deployment.apps "postgres" deleted
[root@localhost DataProtection]# oc get pods -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                        STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTE
SCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>
         5d13h
postgres-pvc                 Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>
         5d13h
[root@localhost DataProtection]# oc delete pvc/data-postgres-postgresql-0  -n postgres
persistentvolumeclaim "data-postgres-postgresql-0" deleted
[root@localhost DataProtection]# oc delete pvc/postgres-pvc -n postgres
persistentvolumeclaim "postgres-pvc" deleted
[root@localhost DataProtection]# oc get pvc -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

同じ名前空間に復元 #tp create bir postgres-bir --backup postgres/hourly-3f1ee-20250224023300 -n postgres BackupInplaceRestore "postgres-bir" が作成されました。

```
[root@localhost DataProtection]# tp get bir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-bir | ontap-s3-appvault | Completed | 2m19s |       |
+--------------+--------------------+-----------+-------+-------+
```

アプリケーションと PVC は同じ名前空間に復元されます。

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                      READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-t857w   1/1     Running   0          10m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-0a849c19-16fe-466f-9733-85e82a8b1677   8Gi        RWO            sc-zonea-nas   <unset>
          10m
postgres-pvc                  Bound    pvc-ded304ea-02d4-4225-b606-63007666ad66   5Gi        RWO            sc-zonea-nas   <unset>
          10m
```

別の名前空間に復元 新しい名前空間を作成します。バックアップから新しい名前空間に復元します。

```
[root@localhost DataProtection]# oc create ns postgres-restore-from-backup
namespace/postgres-restore-from-backup created
[root@localhost DataProtection]# tp create backuprestore postgres-restore-from-backup --backup postgres/postgres-backup1 --namespace-map
ping postgres:postgres-restore-from-backup -n postgres-restore-from-backup
BackupRestore "postgres-restore-from-backup" created.
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE     ERROR   AGE
postgres-restore-from-backup   Running           37s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE     ERROR   AGE
postgres-restore-from-backup   Running           56s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE       ERROR   AGE
postgres-restore-from-backup   Completed           2m52s
[root@localhost DataProtection]# oc get pods -n postgres-restore-from-backup
NAME                      READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-p659p   1/1     Running   0          2m9s
[root@localhost DataProtection]# oc get pvc -n postgres-restore-from-backup
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-36df7399-95da-4c67-a621-af9434015bdb   8Gi        RWO            sc-zonea-nas   <unset>
          2m18s
postgres-pvc                  Bound    pvc-633de3aa-a4f9-4f3b-93cc-e91afbd4fe02   5Gi        RWO            sc-zonea-nas   <unset>
          2m18s
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

▼ アプリケーションの移行

アプリケーションを別のクラスタに複製または移行するには（クラスタ間複製を実行する）、ソース クラスタでバックアップを作成し、そのバックアップを別のクラスタにリストアします。Trident Protectがデスティネーション クラスタにインストールされていることを確認してください。

ソース クラスターで、次の図に示す手順を実行します。

```
[root@localhost DataProtection]# tp create backup postgres-backup-cluster1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup-cluster1" created.
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 12h18m |       |
| hourly-3f1ee-20250224023300  | postgres-app | Completed | 1h18m  |       |
| hourly-3f1ee-20250224033300  | postgres-app | Completed | 18m26s |       |
| postgres-backup-cluster1     | postgres-app | Running   | 35s    |       |
| postgres-backup1             | postgres-app | Completed | 1h48m  |       |
+------------------------------+--------------+-----------+--------+-------+
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 12h19m |       |
| hourly-3f1ee-20250224023300  | postgres-app | Completed | 1h19m  |       |
| hourly-3f1ee-20250224033300  | postgres-app | Completed | 19m41s |       |
| postgres-backup-cluster1     | postgres-app | Completed | 1m50s  |       |
| postgres-backup1             | postgres-app | Completed | 1h49m  |       |
+------------------------------+--------------+-----------+--------+-------+
```

Activate Windows
Go to Settings to activate Windows.

ソース クラスターから、コンテキストを宛先クラスターに切り替えます。次に、宛先クラスター コンテキ

ストから AppVault にアクセスできることを確認し、宛先クラスターから AppVault の内容を取得します。

```
[root@localhost DataProtection]# kubectl config use-context default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin
Switched to context "default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin".
[root@localhost DataProtection]# tp get appvault -n trident-protect
+-------------------+----------+-----------+------+-------+
|       NAME        | PROVIDER |   STATE   | AGE  | ERROR |
+-------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 3d6h |       |
+-------------------+----------+-----------+------+-------+
[root@localhost DataProtection]# tp get appvaultcontent ontap-s3-appvault --show-resources backup --show-paths
+---------------+-------------+--------+---------------------------+--------------------------+-----------------------------------
----------------------------------------------------------------------------------+
|    CLUSTER    |     APP     |  TYPE  |           NAME            |        TIMESTAMP         |
                                                                                  |
+---------------+-------------+--------+---------------------------+--------------------------+-----------------------------------
----------------------------------------------------------------------------------+
| ocp-cluster11 | bbox        | backup | bboxbackup1               | 2025-01-17 15:57:49 (UTC) | bbox_68b4f05f-d5f1-4304-8c69-ad67514
fe393/backups/bboxbackup1_3960c945-8ee0-42fe-945c-c57bb0a3af6f                    |
| ocp-cluster11 | postgres-app | backup | backup1                   | 2025-02-18 13:31:50 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/backup1_28e1bd9a-9b04-4412-8b96-811f9b62e2e3                |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250222153300  | 2025-02-22 15:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250222153300_23d1386b-09f0-456f-aa49-a5865fd48abd  |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250223153300  | 2025-02-23 15:34:42 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250223153300_c492a4d1-38a9-4472-9684-4705c12a206d  |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224033300 | 2025-02-24 03:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224033300_3d09ab81-f6fe-47fa-a699-28006160cdbc |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224043300 | 2025-02-24 04:34:47 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224043300_66805e4f-7631-48a6-98f7-d34bb8626031 |
| ocp-cluster11 | postgres-app | backup | postgres-backup-cluster1  | 2025-02-24 03:52:36 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/postgres-backup-cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3  |
```

リストのバックアップ パスを使用して、以下のコマンドに示すように、backuprestore CR オブジェクトを作成します。

```
# tp create backuprestore backup-restore-cluster2 --namespace-mapping
postgres:postgres --appvault ontap-s3-appvault --path postgres-
app_4d798ed5-cfa8-49ff-a5b6-c5e2d89aeb89/backups/postgres-backup-
cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3 -n postgres
BackupRestore "backup-restore-cluster2" created.
```

```
[root@localhost DataProtection]# tp get backuprestore -n postgres
+--------------------------+--------------------+-----------+--------+-------+
|           NAME           |      APPVAULT      |   STATE   |  AGE   | ERROR |
+--------------------------+--------------------+-----------+--------+-------+
| backup-restore-cluster2 | ontap-s3-appvault | Completed | 12m41s |       |
+--------------------------+--------------------+-----------+--------+-------+
```

アプリケーション ポッドと PVC が宛先クラスターに作成されたことがわかります。

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                   READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-2lvcq   1/1     Running   0          13m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                         STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-872a5182-601b-4848-b410-fef368337d07   8Gi        RWO            sc-zoneb-san   <unset>
          13m
postgres-pvc                 Bound    pvc-caf9fa71-76a8-4645-9bb5-2ed72e72948b   5Gi        RWO            sc-zoneb-san   <unset>
          13m
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

Trident Protectを使用してRed Hat OpenShift VirtualizationのVMを保護

OpenShift Virtualization の VM をスナップショットとバックアップを使用して保護します。この手順には、ONTAP S3 オブジェクトストレージを使用した AppVault の作成、Kubernetes リソースオブジェクト、永続ボリューム、内部イメージなどの VM データをキャプチャするための Trident Protect の設定、および必要に応じたデータのリストアが含まれます。

OpenShift Virtualization 環境の仮想マシンは、OpenShift Container プラットフォームのワーカーノードで実行されるコンテナー化されたアプリケーションです。 VM のメタデータと永続ディスクを保護して、それらが失われたり破損したりした場合に回復できるようにすることが重要です。

OpenShift Virtualization VMの永続ディスクは、"TridentCSI"を使用してOpenShiftクラスタに統合されたONTAPストレージによってバックアップできます。このセクションでは、"Trident Protect"を使用して、データボリュームを含むVMのスナップショットとバックアップをONTAPオブジェクトストレージに作成します。

必要に応じてスナップショットまたはバックアップから復元します。

Trident Protectは、OpenShiftクラスタ上のアプリケーションとVMのスナップショット、バックアップ、リストア、ディザスタリカバリを可能にします。OpenShift Virtualization VMの場合、Trident Protectで保護できるデータには、VMに関連付けられたKubernetesリソースオブジェクト、永続ボリューム、および内部イメージが含まれます。

以下は、このセクションの例で使用されているさまざまなコンポーネントのバージョンです

- "OpenShift クラスター 4.17"
- "Red Hat が提供する OpenShift Virtualization Operator 経由でインストールされた OpenShift Virtualization"
- "Trident25.02"
- "Trident Protect 25.02"
- "ONTAP 9.16"

オブジェクトストレージ用のAppVaultを作成する

▼ **AppVault**を作成する

アプリケーションまたはVMのスナップショットとバックアップを作成する前に、Trident Protectでオブジェクトストレージを設定して、スナップショットとバックアップを保存する必要があります。これはバケットCRを使用して行われます。バケットCRを作成して設定できるのは管理者のみです。バケットCRは、Trident ProtectではAppVaultとして知られています。AppVaultオブジェクトは、ストレージバケットの宣言的なKubernetesワークフロー表現です。AppVault CRには、バックアップ、スナップショット、リストア操作、SnapMirrorレプリケーションなどの保護操作でバケットを使用するために必要な設定が含まれています。

この例では、ONTAP S3 をオブジェクトストレージとして使用する方法を示します。ONTAP S3 用の AppVault CR を作成するワークフローは次のとおりです：1.ONTAP クラスタの SVM に S3 オブジェクトストアサーバーを作成します。2.オブジェクトストアサーバーにバケットを作成します。3.SVM に S3 ユーザーを作成します。アクセスキーとシークレットキーを安全な場所に保管してください。4.OpenShift で、ONTAP S3 クレデンシャルを格納するシークレットを作成します。5.ONTAP S3 用の AppVault オブジェクトを作成します

ONTAP S3用のTrident Protect AppVaultを設定

```
# alias tp='tridentctl-protect'

# cat appvault-secret.yaml
apiVersion: v1
stringData:
  accessKeyID: "<access key of S3>"
  secretAccessKey: "<secret access key of S3>"
# you can also provide base 64 encoded values instead of string values
#data:
# base 64 encoded values
#  accessKeyID: < base 64 encoded access key>
#  secretAccessKey: <base 64 encoded secretAccess key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque

# cat appvault.yaml
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: trident-protect
      endpoint: <lif for S3 access>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
```

```
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost VM-DataProtection]# tp get appvault
+--------------------+----------+-----------+-------+---------+-------+
|        NAME        | PROVIDER |   STATE   | ERROR | MESSAGE |  AGE  |
+--------------------+----------+-----------+-------+---------+-------+
| ontap-s3-appvault  | OntapS3  | Available |       |         | 8d17h |
+--------------------+----------+-----------+-------+---------+-------+
[root@localhost VM-DataProtection]#
```

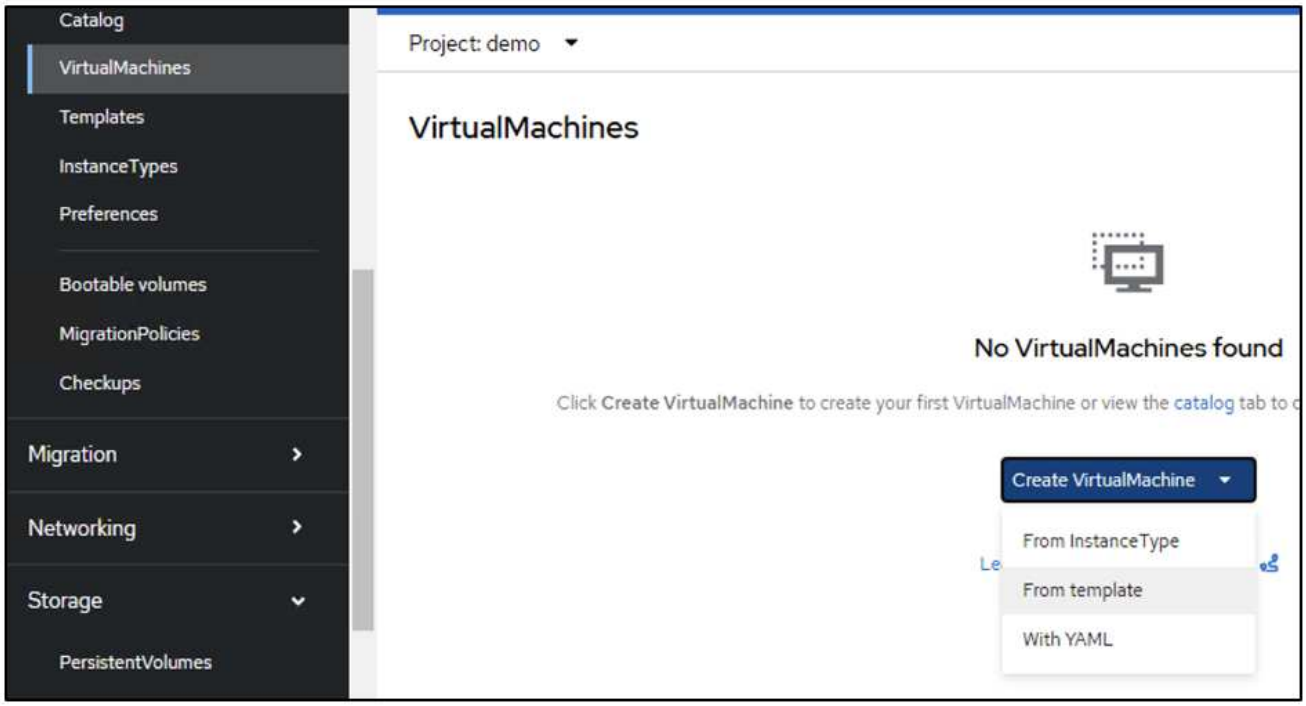
OpenShift Virtualization で VM を作成する

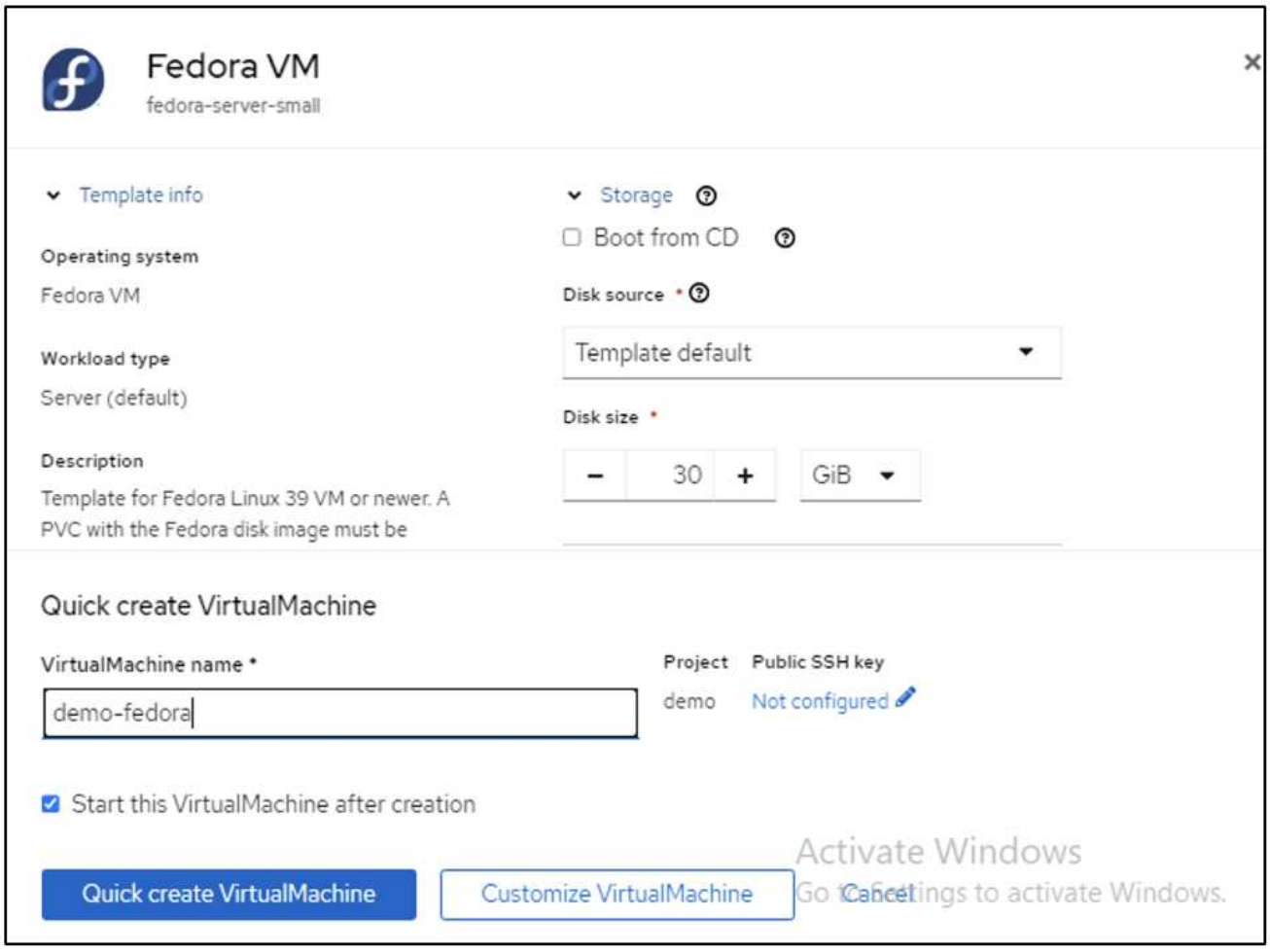
▼ **OpenShift Virtualization で VM を作成する**

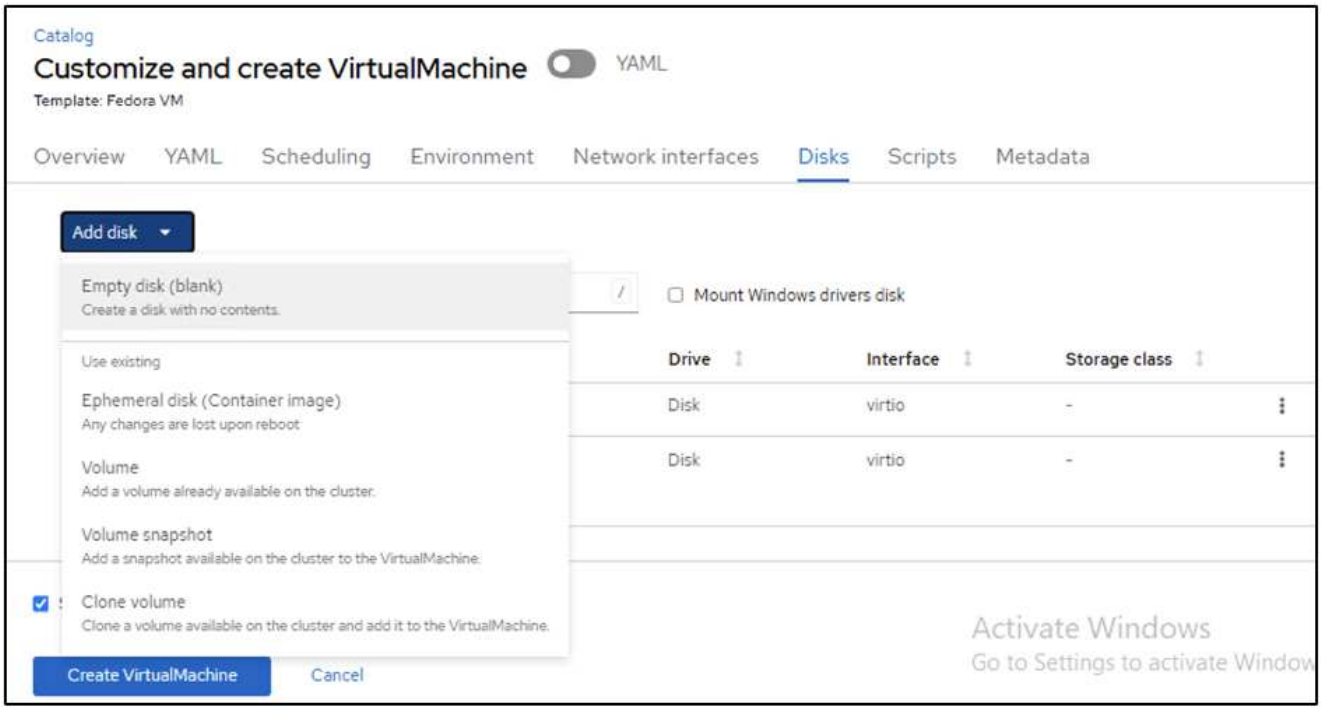
次のスクリーンショットは、テンプレートを使用してコンソールから VM (名前空間 demo 内の demo-fedora) を作成する様子を示しています。ルート ディスクはデフォルトのストレージ クラスを自動的に選択するため、デフォルトのストレージ クラスが適切に設定されていることを確認します。このセットアップでは、デフォルトのストレージ クラスは **sc-zonea-san** です。追加のディスクを作成するときは、ストレージ クラス sc-zonea-san を選択し、「最適化されたストレージ設定を適用する」チェックボックスをオンにしてください。これにより、アクセス モードが RWX に、ボリューム モードがブロックに設定されます。

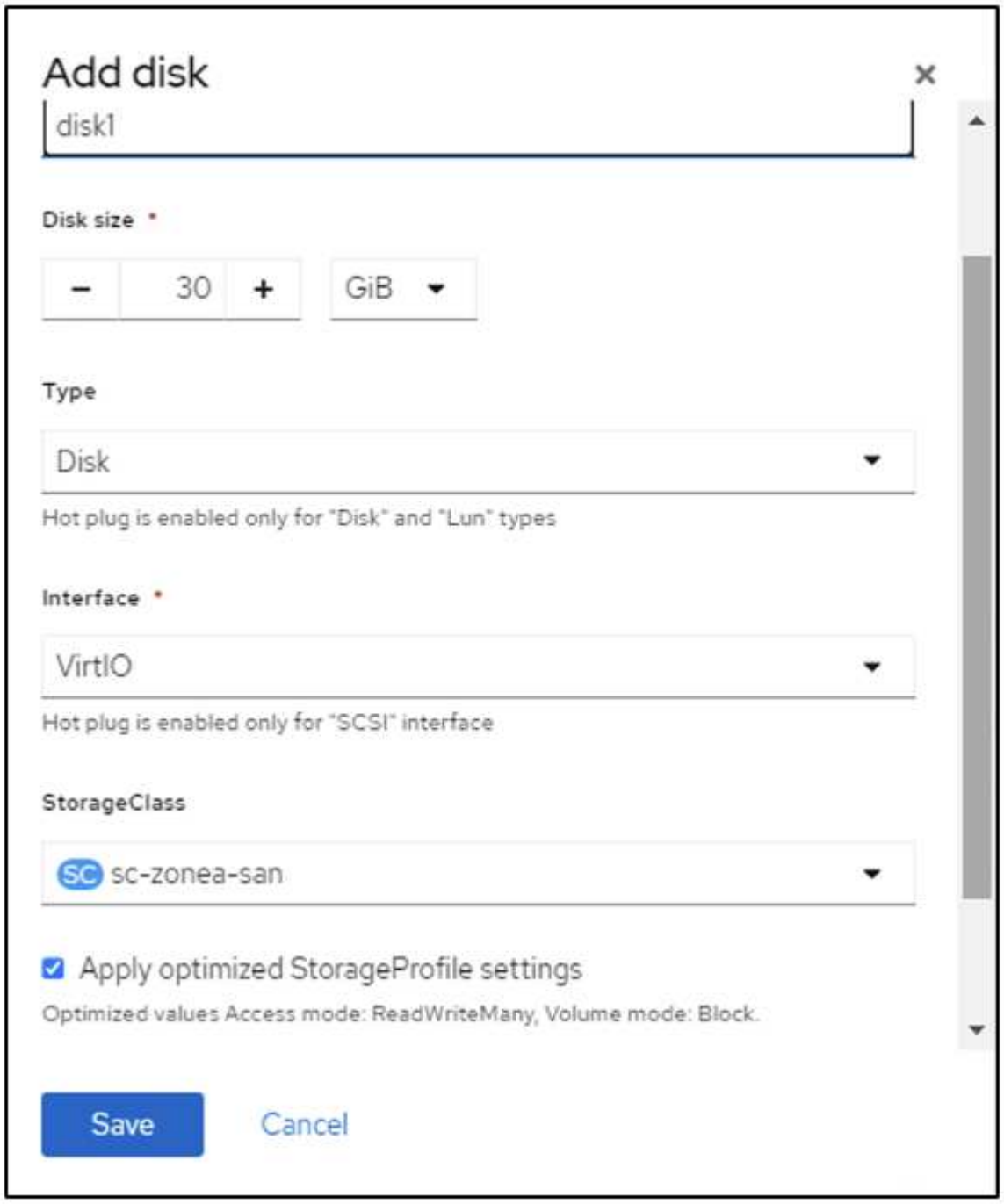
Trident は、SAN (iSCSI、NVMe/TCP、FC) のブロック ボリューム モードで RWX アクセス モードをサポートします。 (NAS のデフォルトのアクセス モードです)。後で VM のライブ マイグレーションを実行する必要がある場合は、RWX アクセス モードが必要です。

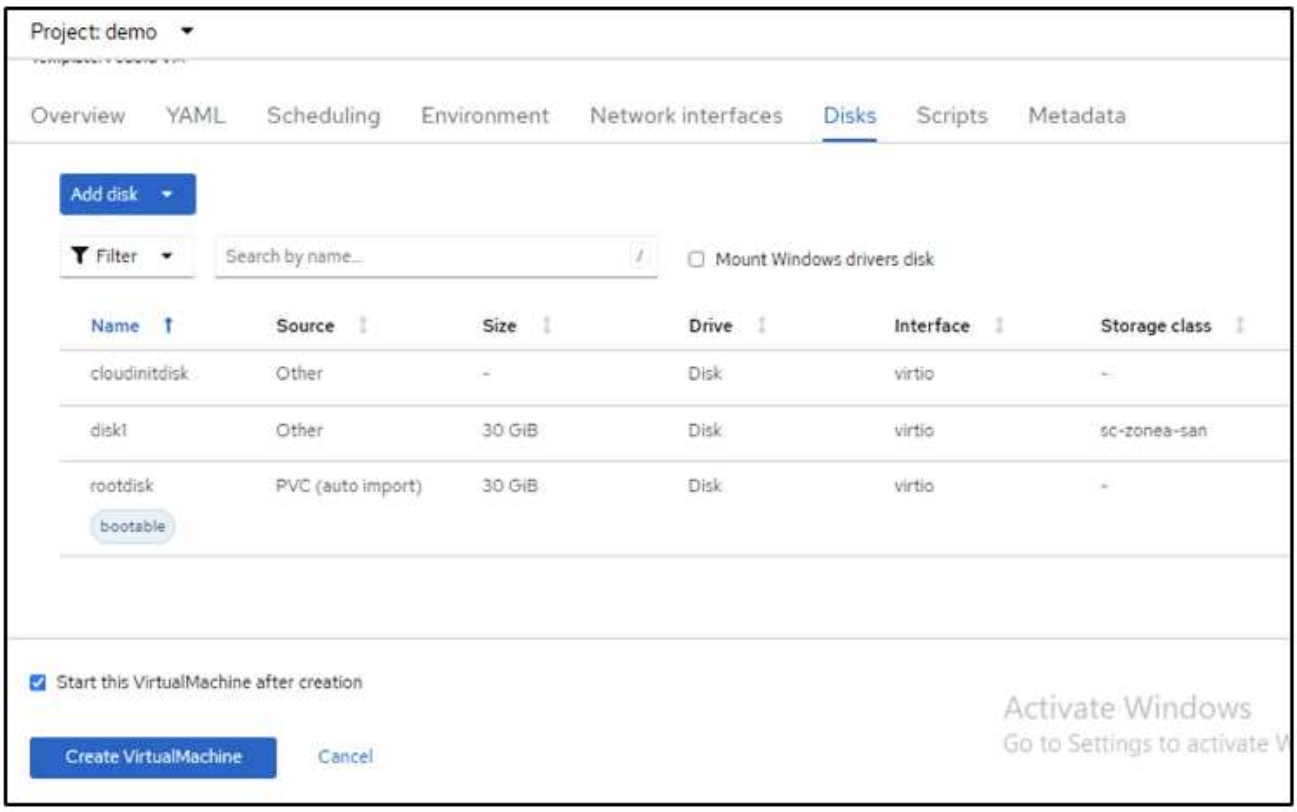



Catalog
VirtualMachines
Templates
InstanceTypes
Preferences
Bootable volumes
MigrationPolicies
Checkups
Migration
Networking
Storage
PersistentVolumes
Project: demo
VirtualMachines
No VirtualMachines found
Click Create VirtualMachine to create your first VirtualMachine or view the catalog tab to
Create VirtualMachine
From InstanceType
From template
With YAML


Fedora VM
fedora-server-small
Template info
Operating system
Fedora VM
Workload type
Server (default)
Description
Template for Fedora Linux 39 VM or newer. A PVC with the Fedora disk image must be
Storage
Boot from CD
Disk source *
Template default
Disk size *
30
GiB
Quick create VirtualMachine
VirtualMachine name *
demo-fedora
Project
demo
Public SSH key
Not configured
Start this VirtualMachine after creation
Activate Windows
Go to Settings to activate Windows.
Quick create VirtualMachine
Customize VirtualMachine
Cancel


Catalog
Customize and create VirtualMachine
YAML
Template: Fedora VM
Overview
YAML
Scheduling
Environment
Network interfaces
Disks
Scripts
Metadata
Add disk
Empty disk (blank)
Create a disk with no contents.
Use existing
Ephemeral disk (Container image)
Any changes are lost upon reboot
Volume
Add a volume already available on the cluster.
Volume snapshot
Add a snapshot available on the cluster to the VirtualMachine.
Clone volume
Clone a volume available on the cluster and add it to the VirtualMachine.
Mount Windows drivers disk
Drive
Interface
Storage class
Disk
virtio
-
Disk
virtio
-
Create VirtualMachine
Cancel
Activate Windows
Go to Settings to activate Windows


Add disk
disk1
Disk size *
30
GiB
Type
Disk
Hot plug is enabled only for "Disk" and "Lun" types
Interface *
VirtIO
Hot plug is enabled only for "SCSI" interface
StorageClass
SC sc-zonea-san
Apply optimized StorageProfile settings
Optimized values Access mode: ReadWriteMany, Volume mode: Block.
Save
Cancel




```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                   AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   2m54s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          110s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

アプリを作成する

▼ アプリを作成

VM の Trident Protect アプリを作成する

この例では、demo ネームスペースには 1 つの VM があり、アプリの作成時にネームスペースのすべてのリソースが含まれます。

```
# alias tp='tridentctl-protect'
# tp create app demo-vm --namespaces demo -n demo --dry-run > app.yaml

# cat app.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-vm
```

```
  namespace: demo
spec:
  includedNamespaces:
  - namespace: demo
# oc create -f app.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+---------+------------+-------+-----+
|  NAME   | NAMESPACES | STATE | AGE |
+---------+------------+-------+-----+
| demo-vm | demo       | Ready | 45s |
+---------+------------+-------+-----+
[root@localhost VM-DataProtection]#
```

バックアップを作成してアプリを保護する

▼ バックアップを作成する

オンデマンド バックアップを作成する

以前に作成したアプリ (demo-vm) のバックアップを作成します。これには、デモ名前空間内のすべてのリソースが含まれます。バックアップを保存する AppVault 名を指定します。

```
# tp create backup demo-vm-backup-on-demand --app demo-vm --appvault
ontap-s3-appvault -n demo
Backup "demo-vm-backup-on-demand" created.
```

```
[root@localhost VM-DataProtection]# tp get backup -n demo
+--------------------------+---------+----------------+-----------+-------+--------+
|           NAME           |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+--------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand | demo-vm | Retain         | Completed |       | 12m53s |
+--------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

スケジュールに従ってバックアップを作成する

保持するバックアップの粒度と数を指定して、バックアップのスケジュールを作成します。

```
# tp create schedule backup-schedule1 --app demo-vm --appvault ontap-s3-
appvault --granularity Hourly --minute 45 --backup-retention 1 -n demo
--dry-run>backup-schedule-demo-vm.yaml
schedule.protect.trident.netapp.io/backup-schedule1 created
```

```
#cat backup-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: backup-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "1"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "45"
  recurrenceRule: ""
  snapshotRetention: "0"
status: {}
# oc create -f backup-schedule-demo-vm.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+------------------+---------+---------------+---------+-------+-------+-----+
|       NAME       |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR | AGE |
+------------------+---------+---------------+---------+-------+-------+-----+
| backup-schedule1 | demo-vm | Hourly:min=45 | true    |       |       | 9s  |
+------------------+---------+---------------+---------+-------+-------+-----+
```

```
[root@localhost VM-DataProtection]# tp get backups -n demo
+-----------------------------+---------+----------------+-----------+-------+--------+
|            NAME             |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-----------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand    | demo-vm | Retain         | Completed |       | 44m4s  |
| hourly-4c094-20250312144500 | demo-vm | Retain         | Completed |       | 20m34s |
+-----------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

バックアップからの復元

▼ バックアップからの復元

VMを同じ名前空間に復元する

この例では、バックアップ demo-vm-backup-on-demand に、fedora VM の demo-app を含むバックアップが含まれています。

まず、VMを削除し、PVC、ポッド、VMオブジェクトが名前空間「demo」から削除されていることを確認します。

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   59m   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          58m

NAME                                                 STATUS   VOLUME                                     CAPACITY
CLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                    Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi
a-san   <unset>                 59m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi
a-san   <unset>                 59m
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc delete vm demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
No resources found in demo namespace.
[root@localhost VM-DataProtection]#
```

次に、バックアップインプレース復元オブジェクトを作成します。

```
# tp create bir demo-fedora-restore --backup demo/demo-vm-backup-on-
demand -n demo --dry-run>vm-demo-bir.yaml

# cat vm-demo-bir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo-fedora-restore
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/demo-vm-backup-on-demand_f6af3513-9739-480e-88c7-
4cca45808a80
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-bir.yaml -n demo
backupinplacerestore.protect.trident.netapp.io/demo-fedora-restore
created
```

```
[root@localhost VM-DataProtection]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo-fedora-restore | ontap-s3-appvault | Completed |       | 28m17s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

VM、ポッド、PVCが復元されたことを確認する

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   116s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-9kfxh   1/1     Running   0          116s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

VM を別の名前空間に復元する

まず、アプリを復元する新しい名前空間 (この例では demo2) を作成します。次に、バックアップ復元オブジェクトを作成します

```
# tp create br demo2-fedora-restore --backup demo/hourly-4c094-
20250312154500 --namespace-mapping demo:demo2 -n demo2 --dry-run>vm
-demo2-br.yaml

# cat vm-demo2-br.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo2-fedora-restore
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/hourly-4c094-20250312154500_aaa14543-a3fa-41f1-
a04c-44b1664d0f81
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
```

```
  conditions: null
  postRestoreExecHooksRunResults: null
  state: ""
# oc create -f vm-demo2-br.yaml -n demo2
```

```
[root@localhost VM-DataProtection]# tp get br -n demo2
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-fedora-restore | ontap-s3-appvault | Completed |       | 38m52s |
+----------------------+--------------------+-----------+-------+--------+
```

VM、ポッド、および PVC が新しい名前空間 demo2 に作成されていることを確認します。

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                  STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                     Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

スナップショットを使用してアプリを保護する

▼ スナップショットを作成する

オンデマンド スナップショットを作成する アプリのスナップショットを作成し、保存する必要がある AppVault を指定します。

```
# tp create snapshot demo-vm-snapshot-ondemand --app demo-vm --appvault
ontap-s3-appvault -n demo --dry-run
# cat demo-vm-snapshot-on-demand.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  creationTimestamp: null
  name: demo-vm-snapshot-ondemand
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  completionTimeout: 0s
  volumeSnapshotsCreatedTimeout: 0s
  volumeSnapshotsReadyToUseTimeout: 0s
status:
  conditions: null
```

```
  postSnapshotExecHooksRunResults: null
  preSnapshotExecHooksRunResults: null
  state: ""

# oc create -f demo-vm-snapshot-on-demand.yaml
snapshot.protect.trident.netapp.io/demo-vm-snapshot-ondemand created
```

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                   Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

スナップショットのスケジュールを作成する スナップショットのスケジュールを作成します。保持するスナップショットの粒度と数を指定します。

```
# tp create Schedule snapshot-schedule1 --app demo-vm --appvault ontap-s3-appvault --granularity Hourly --minute 50 --snapshot-retention 1 -n demo --dry-run>snapshot-schedule-demo-vm.yaml

# cat snapshot-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: snapshot-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "0"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "50"
  recurrenceRule: ""
  snapshotRetention: "1"
status: {}

# oc create -f snapshot-schedule-demo-vm.yaml
```

```
schedule.protect.trident.netapp.io/snapshot-schedule1 created
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+--------------------+---------+---------------+---------+-------+-------+-------+
|        NAME        |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR |  AGE  |
+--------------------+---------+---------------+---------+-------+-------+-------+
| backup-schedule1   | demo-vm | Hourly:min=45 | true    |       |       | 5d23h |
| snapshot-schedule1 | demo-vm | Hourly:min=50 | true    |       |       | 12s   |
+--------------------+---------+---------------+---------+-------+-------+-------+
[root@localhost VM-DataProtection]#
```

```
[root@localhost VM-DataProtection]# tp get snapshots -n demo
+-----------------------------------------+---------+----------------+-----------+-------+--------+
|                  NAME                   |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-----------------------------------------+---------+----------------+-----------+-------+--------+
| backup-39b67e1c-f875-4045-93df-78634bae9dfb | demo-vm | Delete         | Completed |       | 6m29s  |
| demo-vm-snapshot-ondemand               | demo-vm | Delete         | Completed |       | 21m30s |
| hourly-51839-20250318135000             | demo-vm | Delete         | Completed |       | 1m29s  |
+-----------------------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

スナップショットからの復元

▼ スナップショットからの復元

スナップショットから同じ名前空間に **VM** を復元します demo2 名前空間から VM demo-fedora を削除します。

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   28h   Running   True

NAME                                                  STATUS   VOLUME
ORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                     Bound    pvc-e0d5f79d-dff9-450d-be0e-90ab6880b7af
-zonea-san   <unset>                 28h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-e6f7890a-70c7-4538-9035-5e2e9379511d
-zonea-san   <unset>                 28h
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost RedHat]#
```

VM のスナップショットからスナップショットインプレース復元オブジェクトを作成します。

```
# tp create sir demo-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand -n demo --dry-run>vm-demo-sir.yaml

# cat vm-demo-sir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  creationTimestamp: null
  name: demo-fedora-restore-from-snapshot
```

```
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  conditions: null
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-sir.yaml
snapshotinplacerestore.protect.trident.netapp.io/demo-fedora-restore-
from-snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sir -n demo
+----------------------------------+------------------+-----------+-------+--------+
|               NAME               |     APPVAULT     |   STATE   | ERROR |  AGE   |
+----------------------------------+------------------+-----------+-------+--------+
| demo-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 58m17s |
+----------------------------------+------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

VM とその PVC がデモ名前空間に作成されていることを確認します。

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                   AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m17s   Running   True

NAME                                                STATUS   VOLUME
persistentvolumeclaim/demo-fedora                   Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
[root@localhost RedHat]#
```

スナップショットから別の名前空間に**VM**を復元する

以前にバックアップから復元した demo2 名前空間内の VM を削除します。

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   3m12s   Running   True
virtualmachine.kubevirt.io/demo-fedora   3m11s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-w77rr   1/1     Running   0          3m11s
pod/virt-launcher-demo-fedora-wwdtc   1/1     Running   0          3m11s

NAME                                                    STATUS   VOLUME                                     CAPACITY   ACCESS MODES
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-7aafd5e2-d4cf-4af6-a259-c68e016ec6cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m26s
persistentvolumeclaim/demo-fedora                       Bound    pvc-c1f8145a-56ea-42c5-abb4-6457b6853e1c   30Gi       RWX
  sc-zonea-san   <unset>                 3m25s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-e82b6d98-6762-4473-9bb8-7e98efcb7987   30Gi       RWX
  sc-zonea-san   <unset>                 3m20s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-ee13cfbc-2921-4129-a214-a0f6b10335cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m16s
[root@localhost VM-DataProtection]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo2
virtualmachine.kubevirt.io "demo-fedora" deleted
```

スナップショットからスナップショット復元オブジェクトを作成し、名前空間マッピングを提供します。

```
# tp create sr demo2-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand --namespace-mapping demo:demo2 -n demo2 --dry
-run>vm-demo2-sr.yaml

# cat vm-demo2-sr.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  creationTimestamp: null
  name: demo2-fedora-restore-from-snapshot
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo2-sr.yaml
snapshotrestore.protect.trident.netapp.io/demo2-fedora-restore-from-
snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sr -n demo2
+-------------------------------------+--------------------+-----------+-------+--------+
|                NAME                 |      APPVAULT      |   STATE   | ERROR |  AGE   |
+-------------------------------------+--------------------+-----------+-------+--------+
| demo2-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 15m22s |
+-------------------------------------+--------------------+-----------+-------+--------+
```

VM とその PVC が新しい名前空間 demo2 に復元されていることを確認します。

```
[root@localhost RedHat]# oc get vm,pvc -n demo2
NAME                                      AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora    29h   Running   True

NAME                                                    STATUS   VOLUME
ORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                       Bound    pvc-35dcd9b2-4fca-486c-af9e-596bc5b4dc15
-zonea-san   <unset>                 29h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-575a3111-382f-4933-a778-0089fa1ea2af
-zonea-san   <unset>                 29h
[root@localhost RedHat]#
```

特定の**VM**を復元する

▼ 名前空間内の特定の**VM**を選択してスナップショット/バックアップを作成し、復元する

前の例では、名前空間内に 1 つの VM がありました。名前空間全体をバックアップに含めることで、その VM に関連付けられたすべてのリソースがキャプチャされました。次の例では、同じ名前空間に別の VM を追加し、ラベル セレクターを使用してこの新しい VM 専用のアプリを作成します。

デモ名前空間に新しい**VM**（**demo-centos vm**）を作成します

```
[root@localhost VM-DataProtection]# oc get vm,pod,pvc -n demo
NAME                                  AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   2m47s   Running   True
virtualmachine.kubevirt.io/demo-fedora   81m     Running   True

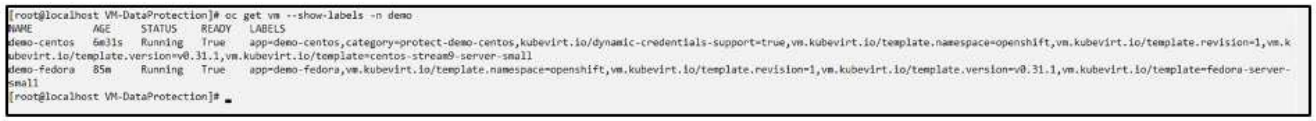
NAME                                READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-2nq6g   1/1     Running   0          113s
pod/virt-launcher-demo-fedora-9kfxh   1/1     Running   0          81m

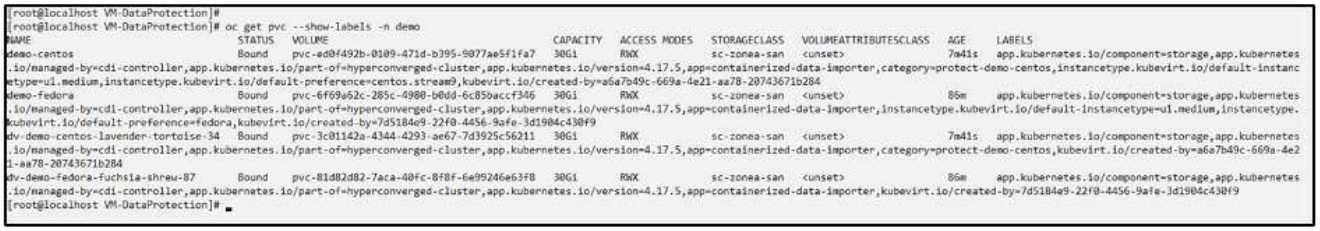
NAME                                                    STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-centos                       Bound    pvc-ed0f492b-0109-471d-b395-9077ae5f1fa7   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/demo-fedora                       Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-3c01142a-4344-4293-ae67-7d3925c56211   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

demo-centos vm とその関連リソースにラベルを付ける

```
[root@localhost VM-DataProtection]# oc label vm demo-centos category=protect-demo-centos -n demo
virtualmachine.kubevirt.io/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc demo-centos category=protect-demo-centos -n demo
persistentvolumeclaim/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc dv-demo-centos-lavender-tortoise-34 category=protect-demo-centos -n demo
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34 labeled
[root@localhost VM-DataProtection]#
```

demo-centos vm と **pvcs** にラベルが付与されていることを確認します





ラベルセレクターを使用して特定の**VM**（**demo-centos**）専用のアプリを作成する

```
# tp create app demo-centos-app --namespaces 'demo(category=protect-
demo-centos)' -n demo --dry-run>demo-centos-app.yaml

# cat demo-centos-app.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-centos-app
  namespace: demo
spec:
  includedNamespaces:
  - labelSelector:
      matchLabels:
        category: protect-demo-centos
    namespace: demo
status:
  conditions: null

# oc create -f demo-centos-app.yaml -n demo
application.protect.trident.netapp.io/demo-centos-app created
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+------------------+------------+-------+------+
|      NAME        | NAMESPACES | STATE | AGE  |
+------------------+------------+-------+------+
| demo-centos-app  | demo       | Ready | 56s  |
| demo-vm          | demo       | Ready | 4h6m |
+------------------+------------+-------+------+
```

オンデマンドおよびスケジュールに従ってバックアップとスナップショットを作成する方法は、前に示したものと同じです。スナップショットまたはバックアップの作成に使用されている trident-protect アプリには名前空間の特定の VM のみが含まれているため、そこから復元すると特定の VM のみが復元されます。以下に、サンプルのバックアップ/復元操作の例を示します。

対応するアプリを使用して、名前空間内の特定の **VM** のバックアップを作成します

前の手順では、ラベル セレクターを使用して、デモ名前空間に centos vm のみを含むアプリを作成しました。このアプリのバックアップ (この例ではオンデマンド バックアップ) を作成します。

```
# tp create backup demo-centos-backup-on-demand --app demo-centos-app
--appvault ontap-s3-appvault -n demo
Backup "demo-centos-backup-on-demand" created.
```

```
+-------------------------------+-----------------+----------------+-----------+-------+--------+
|              NAME             |       APP       | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-------------------------------+-----------------+----------------+-----------+-------+--------+
| demo-centos-backup-on-demand  | demo-centos-app | Retain         | Completed |       | 13m22s |
| demo-vm-backup-on-demand      | demo-vm         | Retain         | Completed |       | 4h19m  |
| hourly-4c094-20250312174500   | demo-vm         | Retain         | Completed |       | 56m17s |
+-------------------------------+-----------------+----------------+-----------+-------+--------+
```

特定の **VM** を同じ名前空間に復元する 特定の VM (centos) のバックアップは、対応するアプリを使用して作成されました。これからバックアップ・インプレース・リストアまたはバックアップ・リストアが作成されると、この特定の VM のみが復元されます。 Centos VM を削除します。

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   4m27s   Running   True
virtualmachine.kubevirt.io/demo-fedora   4m27s   Running   True

NAME                                                                 STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                                    Bound    pvc-e8faeaf8-fc0c-4d92-96de-c83a335a7a17
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/demo-fedora                                    Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34            Bound    pvc-66eb7996-1420-4513-a67c-2824f08534da
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87                Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
  sc-zonea-san   <unset>                 4m32s
```

```
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-centos -n demo
virtualmachine.kubevirt.io "demo-centos" deleted
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m17s   Running   True

NAME                                                    STATUS   VOLUME
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
```

demo-centos-backup-on-demand からバックアップのインプレース リストアを作成し、centos VM が再作成されたことを確認します。

```
#tp create bir demo-centos-restore --backup demo/demo-centos-backup-on-demand -n demo
BackupInplaceRestore "demo-centos-restore" created.
```

```
[root@localhost RedHat]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+-------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE  |
+----------------------+--------------------+-----------+-------+-------+
| demo-centos-restore  | ontap-s3-appvault  | Completed |       | 57m9s |
| demo-fedora-restore  | ontap-s3-appvault  | Completed |       | 7d5h  |
+----------------------+--------------------+-----------+-------+-------+
```

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                  AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   29m   Running   True
virtualmachine.kubevirt.io/demo-fedora   85m   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-82954bf7-4a7e-4e0c-9a04-4fa152e1b0ef
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
  sc-zonea-san   <unset>                 85m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-2a8d4eb5-ed6d-4408-b85d-e218e9a5d4b0
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
  sc-zonea-san   <unset>                 85m
[root@localhost RedHat]#
```

特定の **VM** を別の名前空間に復元する demo-centos-backup-on-demand から別の名前空間 (demo3) へのバックアップ復元を作成し、centos VM が再作成されたことを確認します。

```
# tp create br demo2-centos-restore --backup demo/demo-centos-backup-on-demand --namespace-mapping demo:demo3 -n demo3
BackupRestore "demo2-centos-restore" created.
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# tp get br -n demo3
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-centos-restore | ontap-s3-appvault | Completed |       | 52m57s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost RedHat]#
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# oc get vm,pvc -n demo3
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   19m   Running   True

NAME                                                                STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                                   Bound    pvc-0a14e38f-07de-4e09-8f88-14a9a8bb45c2
  sc-zonea-san   <unset>                 19m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-d4f9cf2f-264c-4d02-94bf-0db28b427acc
  sc-zonea-san   <unset>                 19m
[root@localhost RedHat]#
```

ビデオデモンストレーション

次のビデオは、スナップショットを使用してVMを保護するデモを示しています。

VMの保護

サードパーティのツールを使用してコンテナアプリを保護する

OpenShift API for Data Protection (OADP) を使用した **OpenShift Container Platform** のコンテナー アプリのデータ保護

リファレンス ドキュメントのこのセクションでは、 NetApp ONTAP S3 またはNetApp StorageGRID S3 上の Velero で OpenShift API for Data Protection (OADP) を使用してコンテナー アプリのバックアップを作成する方法について詳しく説明します。アプリの永続ボリューム (PV) を含む名前空間スコープのリソースのバックアップは、CSI Tridentスナップショットを使用して作成されます。

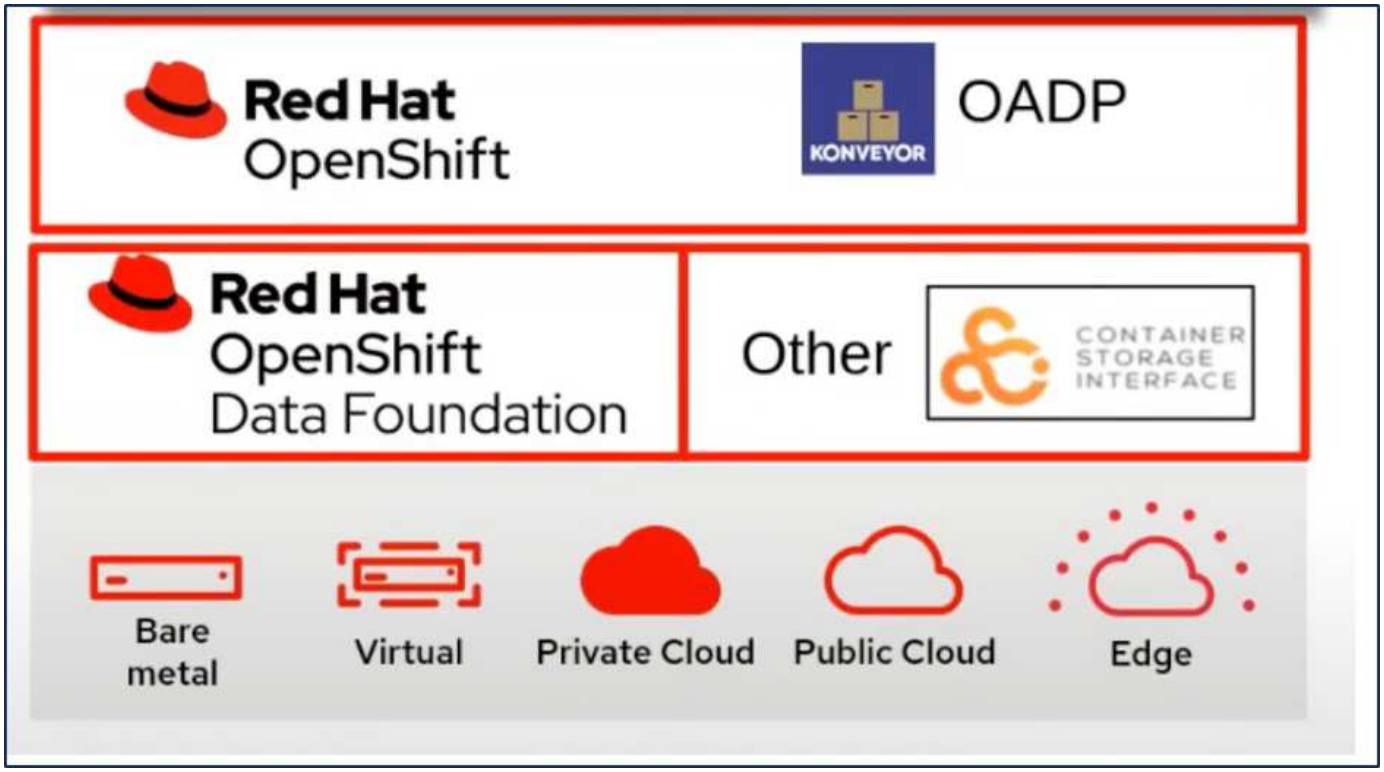
コンテナアプリの永続ストレージは、"TridentCSI"を使用してOpenShiftクラスタに統合されたONTAPストレージをバックエンドとして使用できます。このセクションでは、"データ保護のための OpenShift API (OADP)"を使用して、データボリュームを含むアプリのバックアップを

- ONTAPオブジェクトストレージ
- ストレージグリッド

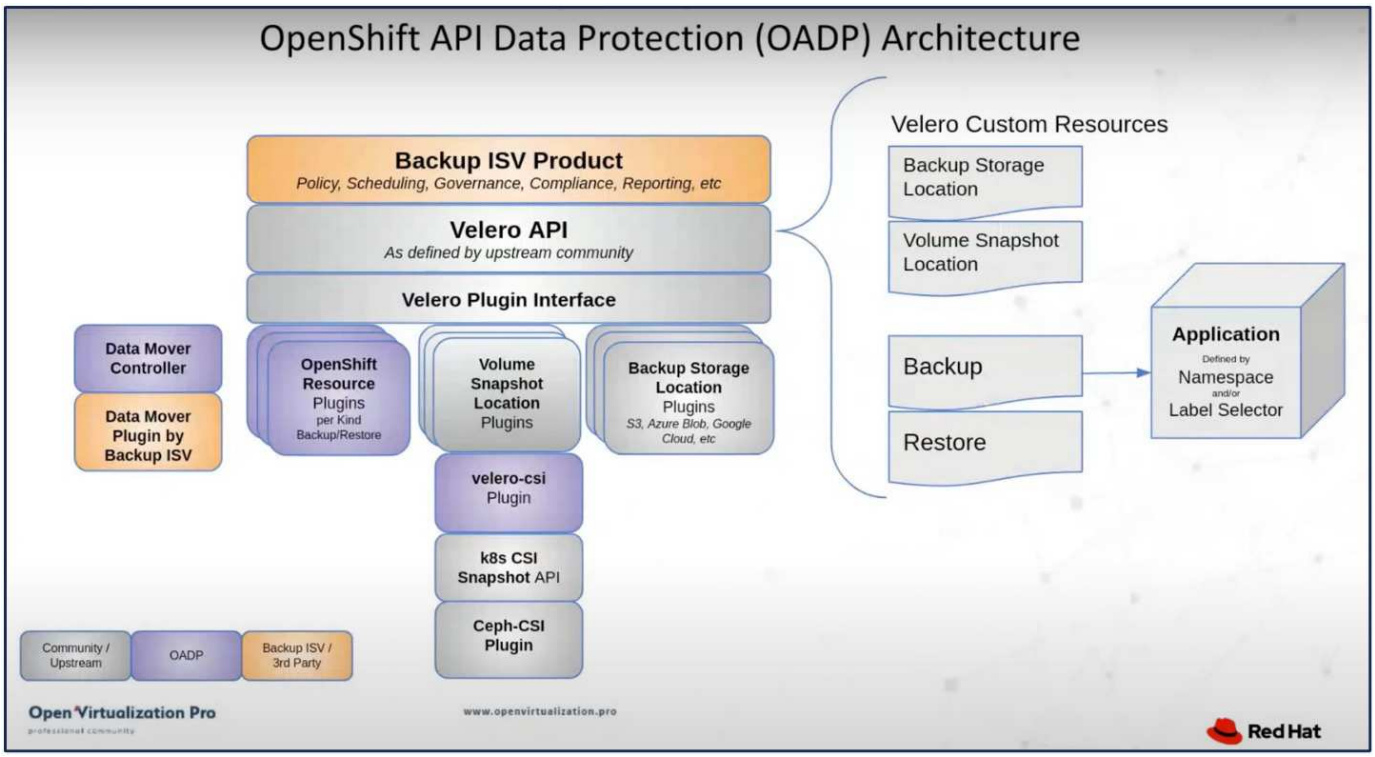
必要に応じてバックアップから復元します。アプリは、バックアップが作成されたクラスターにのみ復元できることに注意してください。

OADP は、OpenShift クラスター上のアプリケーションのバックアップ、復元、および災害復旧を可能にします。 OADP で保護できるデータには、Kubernetes リソース オブジェクト、永続ボリューム、内部イメージな

どがあります。



Red Hat OpenShift は、データ保護のためにオープンソース コミュニティによって開発されたソリューションを活用しています。"ベレロ" Kubernetes クラスター リソースと永続ボリュームを安全にバックアップおよび復元し、災害復旧を実行し、移行するためのオープンソース ツールです。 Velero を簡単に使用できるように、OpenShift は OADP オペレーターと、CSI ストレージ ドライバーと統合する Velero プラグインを開発しました。公開されている OADP API の中核は、Velero API に基づいています。 OADP オペレータをインストールして構成した後、実行できるバックアップ/復元操作は、Velero API によって公開される操作に基づいて行われます。



OADP 1.3 は、OpenShift クラスター 4.12 以降のオペレーター ハブから入手できます。 CSI ボリューム スナップショットをリモート オブジェクト ストアに移動できるデータ ムーバーが組み込まれています。これにより、バックアップ中にスナップショットをオブジェクト ストレージの場所に移動することで、移植性と耐久性が実現します。スナップショットは災害後の復元に利用できます。

以下は、このセクションの例で使用されているさまざまなコンポーネントのバージョンです

- OpenShift クラスター 4.14
- Red Hat が提供する OADP Operator 1.13
- Linux 用 Velero CLI 1.13
- Trident24.02
- ONTAP 9.12
- helm を使用してインストールされた postgresql。

"TridentCSI" "データ保護のための OpenShift API (OADP)" "ベレロ"

OpenShift API for Data Protection (OADP) オペレーターのインストール

このセクションでは、OpenShift API for Data Protection (OADP) Operator のインストールについて概説します。

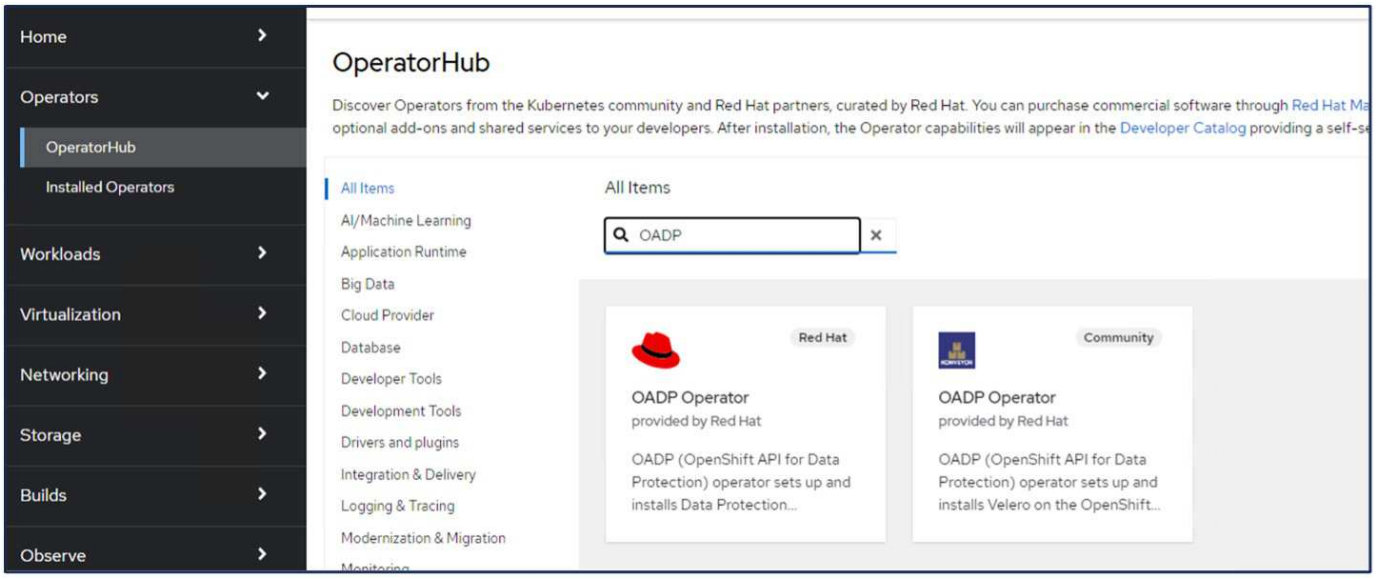
前提条件

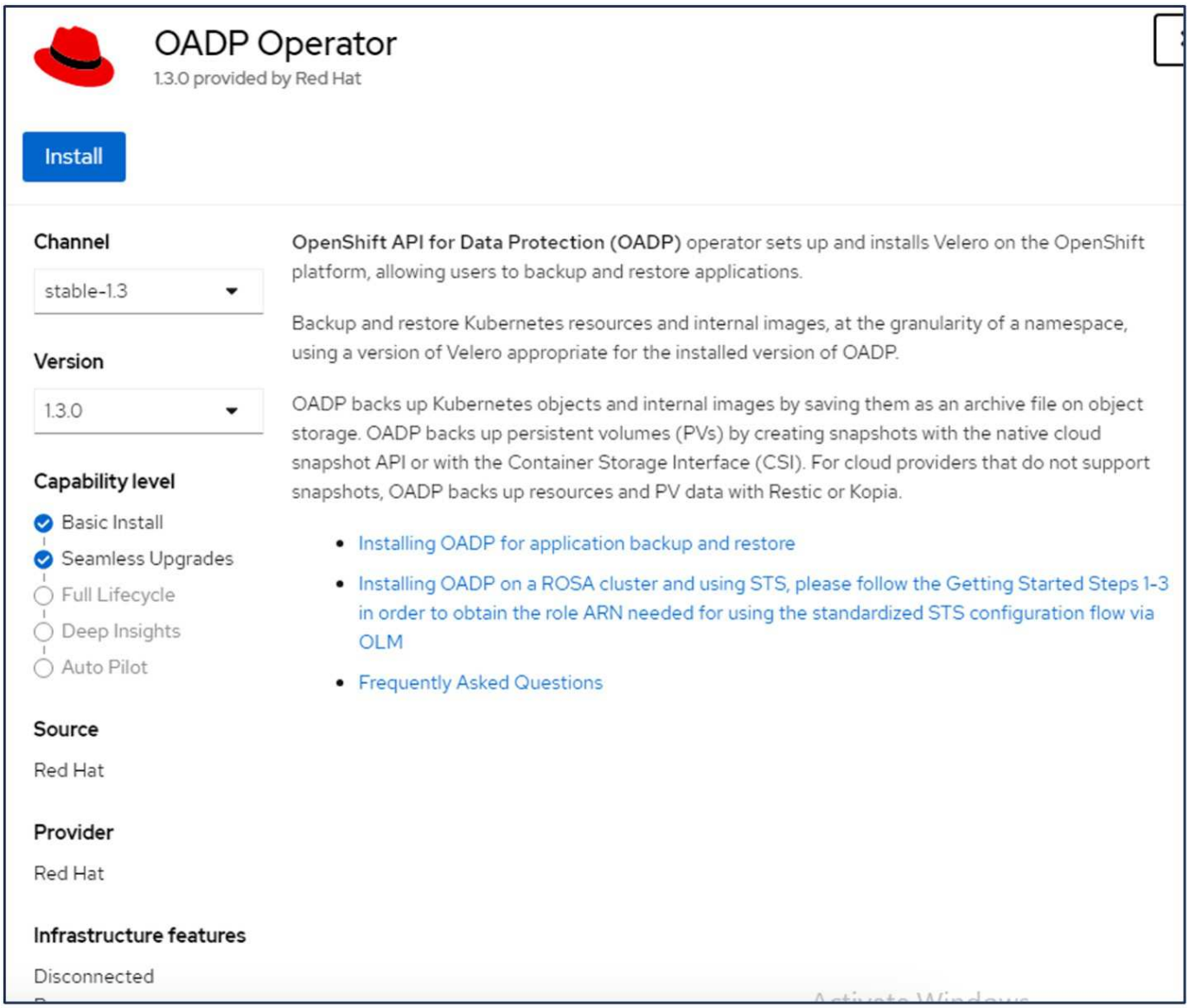
- RHCOS ワーカーノードを備えたベアメタル インフラストラクチャにインストールされた Red Hat OpenShift クラスター (バージョン 4.12 以降)
- Tridentを使用してクラスタに統合されたNetApp ONTAPクラスタ

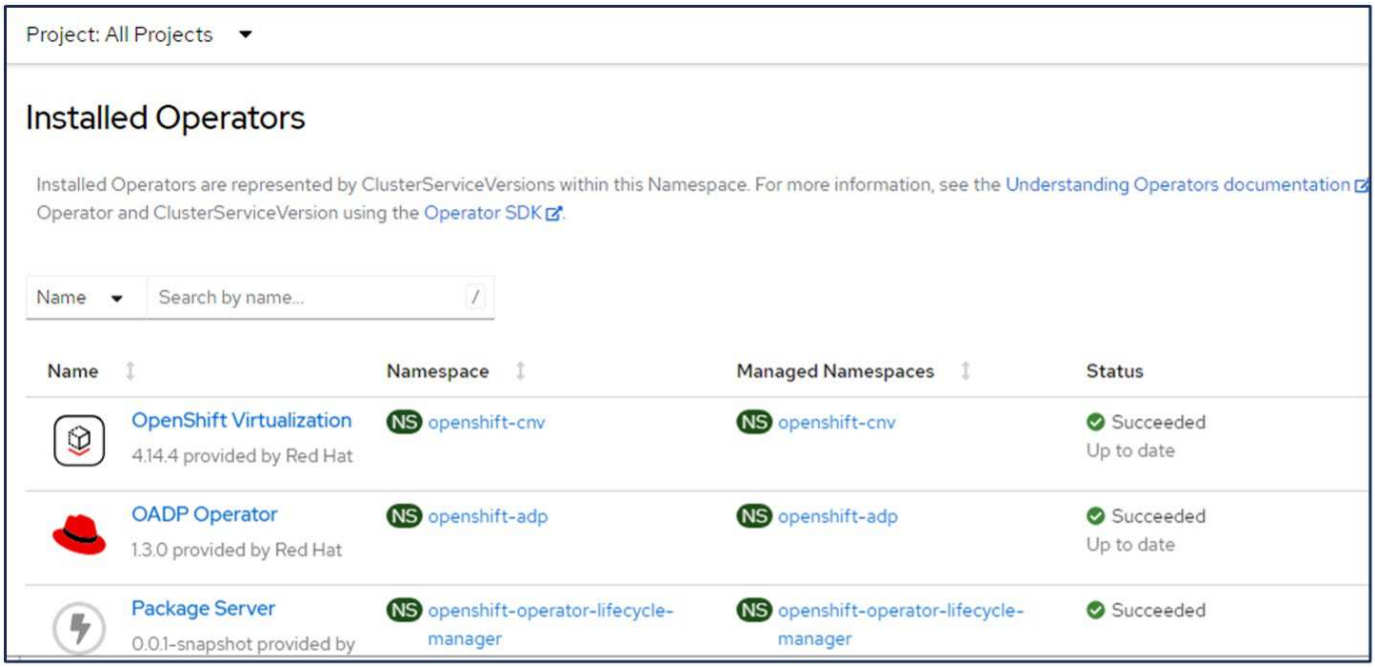
- ONTAPクラスタ上のSVMで構成されたTridentバックエンド
- Tridentをプロビジョナーとして OpenShift クラスター上に構成された StorageClass
- クラスター上に作成されたTridentスナップショット クラス
- Red Hat OpenShift クラスターへのクラスター管理者アクセス
- NetApp ONTAPクラスタへの管理者アクセス
- クラスタにデプロイされたアプリケーション（例：postgresql）
- tridentctl および oc ツールがインストールされ、$PATH に追加された管理ワークステーション

OADPオペレーターのインストール手順

1. クラスターのオペレーター ハブに移動し、Red Hat OADP オペレーターを選択します。インストール ページで、すべてのデフォルトの選択を使用して、インストールをクリックします。次のページでは、再度すべてのデフォルトを使用し、「インストール」をクリックします。 OADP オペレーターは、名前空間 openshift-adp にインストールされます。




OADP Operator
1.3.0 provided by Red Hat
Install
Channel
stable-1.3
Version
1.3.0
Capability level
Basic Install
Seamless Upgrades
Full Lifecycle
Deep Insights
Auto Pilot
Source
Red Hat
Provider
Red Hat
Infrastructure features
Disconnected
OpenShift API for Data Protection (OADP) operator sets up and installs Velero on the OpenShift platform, allowing users to backup and restore applications.
Backup and restore Kubernetes resources and internal images, at the granularity of a namespace, using a version of Velero appropriate for the installed version of OADP.
OADP backs up Kubernetes objects and internal images by saving them as an archive file on object storage. OADP backs up persistent volumes (PVs) by creating snapshots with the native cloud snapshot API or with the Container Storage Interface (CSI). For cloud providers that do not support snapshots, OADP backs up resources and PV data with Restic or Kopia.
Installing OADP for application backup and restore
Installing OADP on a ROSA cluster and using STS, please follow the Getting Started Steps 1-3 in order to obtain the role ARN needed for using the standardized STS configuration flow via OLM
Frequently Asked Questions


Project: All Projects
Installed Operators
Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the Understanding Operators documentation
Operator and ClusterServiceVersion using the Operator SDK
Name
Search by name...
Name
Namespace
Managed Namespaces
Status
OpenShift Virtualization
4.14.4 provided by Red Hat
openshift-cnv
openshift-cnv
Succeeded
Up to date
OADP Operator
1.3.0 provided by Red Hat
openshift-adp
openshift-adp
Succeeded
Up to date
Package Server
0.0.1-snapshot provided by
openshift-operator-lifecycle-manager
openshift-operator-lifecycle-manager
Succeeded

Ontap S3 を使用した Velero 構成の前提条件の詳細

オペレーターのインストールが成功したら、Velero のインスタンスを構成します。 Velero は、S3 互換のオブジェクト ストレージを使用するように構成できます。 ONTAP S3を設定するには、"ONTAPドキュメントのオブジェクトストレージ管理セクション" 。 Velero と統合するには、 ONTAP S3 構成から次の情報が必要になります。

- S3にアクセスするために使用できる論理インターフェース（LIF）
- アクセスキーとシークレットアクセスキーを含む、S3 にアクセスするためのユーザー認証情報
- ユーザーのアクセス権限を持つバックアップ用のS3のバケット名
- オブジェクト ストレージへの安全なアクセスのために、オブジェクト ストレージ サーバーに TLS 証明書をインストールする必要があります。

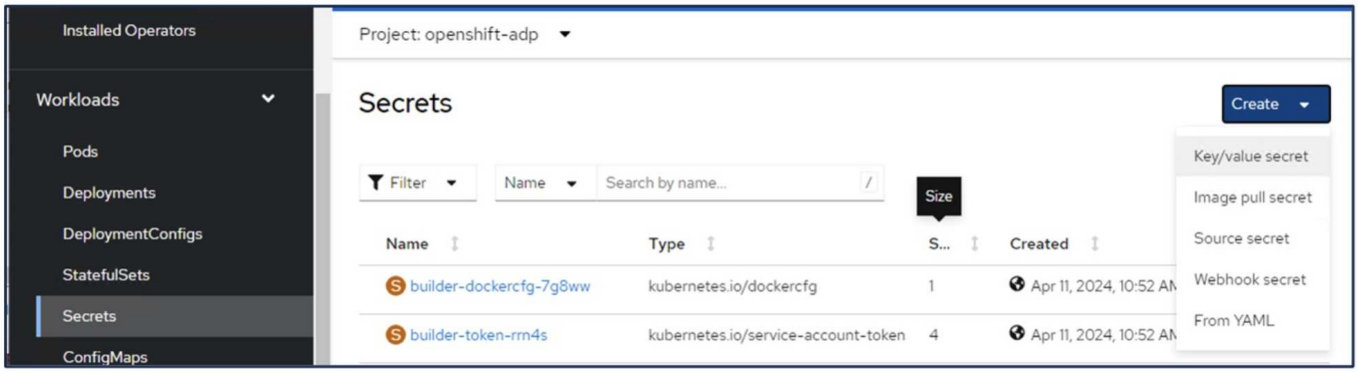
StorageGrid S3 を使用した Velero 構成の前提条件の詳細

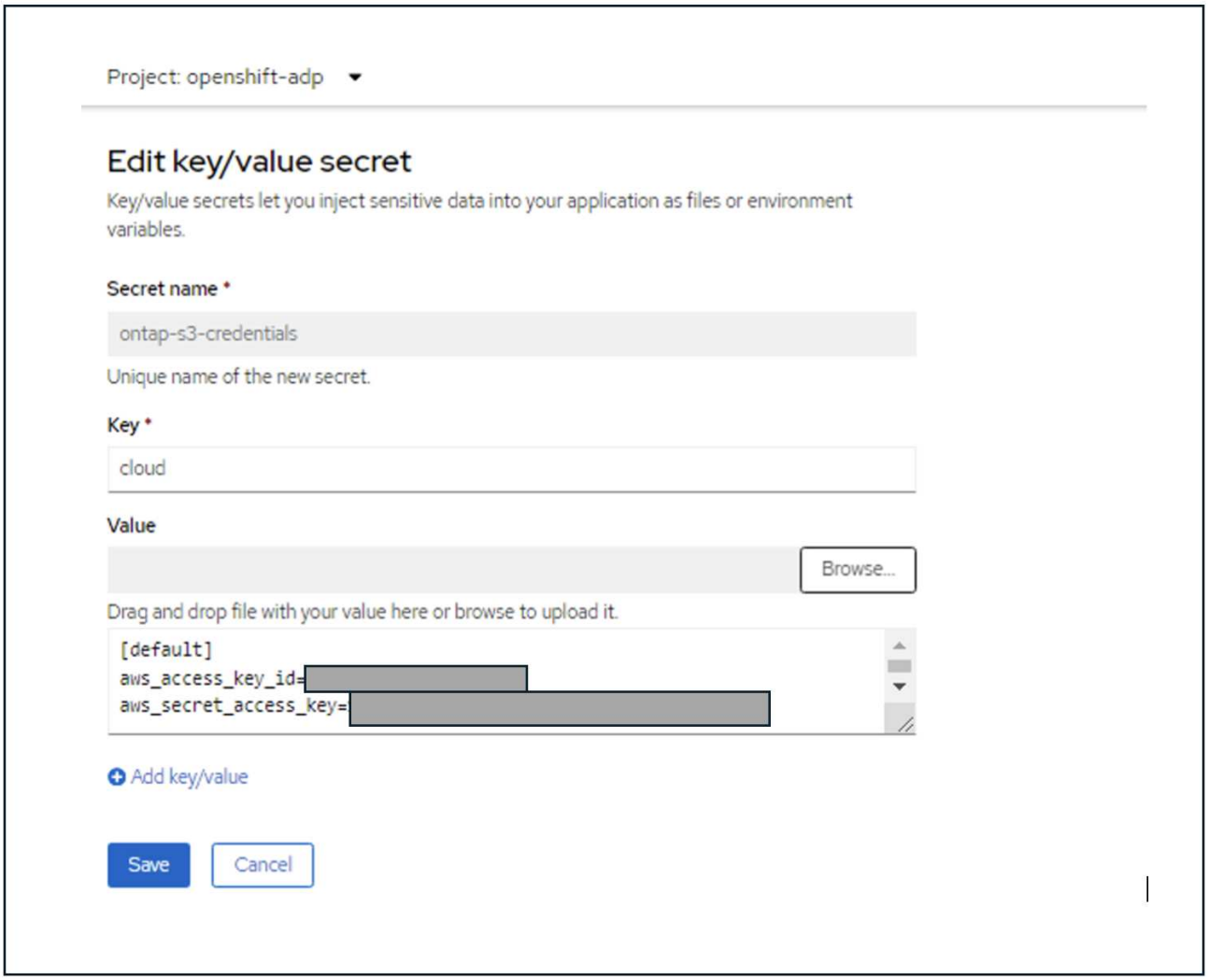
Velero は、S3 互換のオブジェクト ストレージを使用するように構成できます。 StorageGrid S3は、以下の手順で設定できます。"StorageGrid ドキュメント" 。 Velero と統合するには、StorageGrid S3 構成から次の情報が必要になります。

- S3にアクセスするために使用できるエンドポイント
- アクセスキーとシークレットアクセスキーを含む、S3 にアクセスするためのユーザー認証情報
- ユーザーのアクセス権限を持つバックアップ用のS3のバケット名
- オブジェクト ストレージへの安全なアクセスのために、オブジェクト ストレージ サーバーに TLS 証明書をインストールする必要があります。

Veleroの設定手順

- まず、 ONTAP S3 ユーザー認証情報または StorageGrid テナント ユーザー認証情報のシークレットを作成します。これは後で Velero を構成するために使用されます。 CLI または Web コンソールからシークレットを作成できます。 Web コンソールからシークレットを作成するには、「シークレット」を選択し、「キー/値シークレット」をクリックします。示されているように、資格情報名、キー、および値の値を指定します。 S3 ユーザーのアクセス キー ID とシークレット アクセス キーを必ず使用してください。秘密に適切な名前を付けます。以下のサンプルでは、ontap-s3-credentials という名前のONTAP S3 ユーザー認証情報を持つシークレットが作成されます。





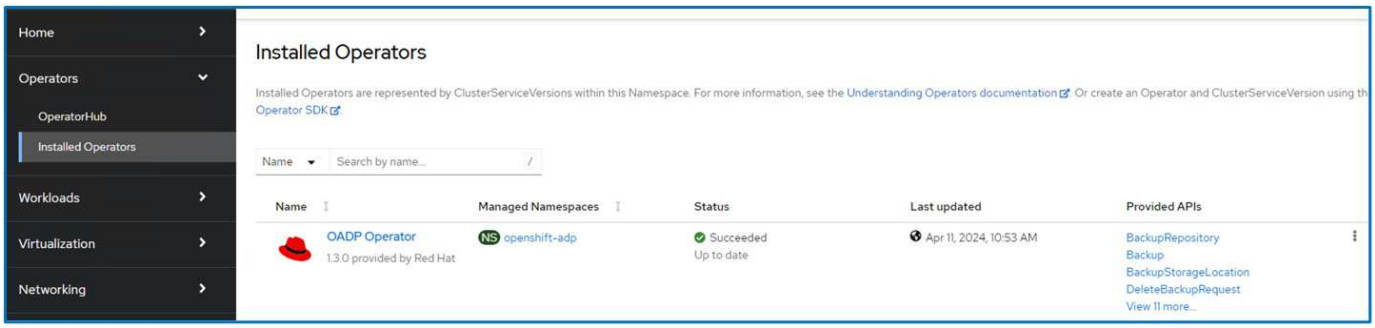
CLI から sg-s3-credentials という名前のシークレットを作成するには、次のコマンドを使用できます。

```
# oc create secret generic sg-s3-credentials --namespace openshift-adp --from-file
cloud=cloud-credentials.txt

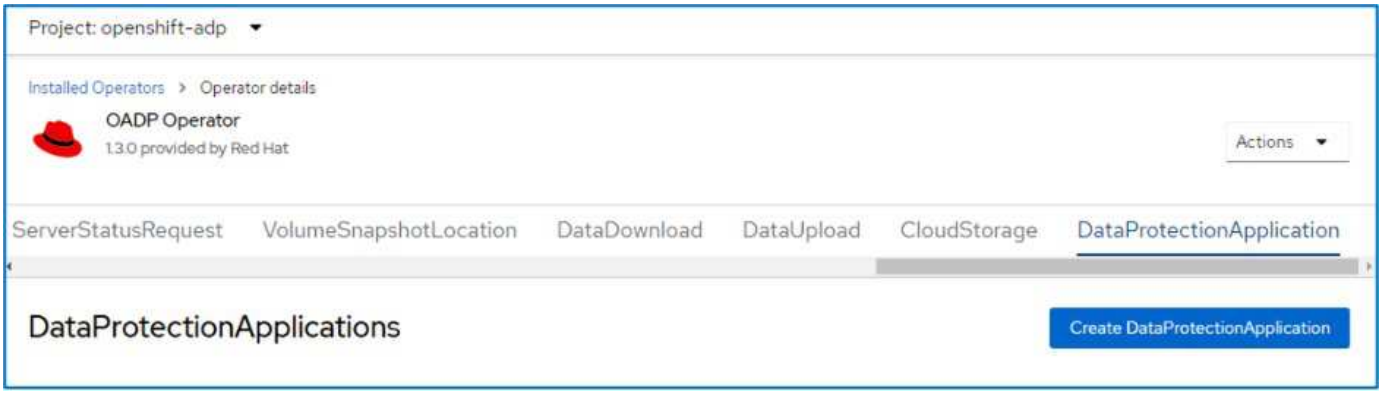
Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3
user in the following format:

[default]
aws_access_key_id=< Access Key ID of S3 user>
aws_secret_access_key=<Secret Access key of S3 user>
```

- 次に、Velero を構成するには、[Operators] の下のメニュー項目から [Installed Operators] を選択し、[OADP Operator] をクリックして、[**DataProtectionApplication**] タブを選択します。



「DataProtectionApplication の作成」をクリックします。フォーム ビューで、DataProtection アプリケーションの名前を入力するか、既定の名前を使用します。



次に、YAML ビューに移動し、以下の yaml ファイルの例に示すように仕様情報を置き換えます。

- ONTAP S3 をバックアップ場所として Velero を構成するためのサンプル yaml ファイル**

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false' ->use this for https
communication with ONTAP S3
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'  ->This allows use of IP in s3URL
          s3Url: 'https://10.61.181.161' ->Ensure TLS certificate for S3
is configured
        credential:
          key: cloud
          name: ontap-s3-credentials -> previously created secret
        default: true
        objectStorage:
          bucket: velero -> Your bucket name previously created in S3 for
backups
          prefix: container-demo-backup ->The folder that will be created
in the bucket
```

```
          caCert: <base64 encoded CA Certificate installed on ONTAP
Cluster with the SVM Scope where the bucker exists>
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
      #default Data Mover uses Kopia to move snapshots to Object Storage
    velero:
      defaultPlugins:
        - csi ->This plugin to use CSI snapshots
        - openshift
        - aws
        - kubevirt -> This plugin to use Velero with OIpenShift
Virtualization
```

StorageGrid S3 をバックアップ場所として **Velero** を構成するためのサンプル **yaml** ファイル

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true'
          profile: default
          region: us-east-1 ->region of your StorageGrid system
          s3ForcePathStyle: 'True'
          s3Url: 'https://172.21.254.25:10443' ->the IP used to access S3
        credential:
          key: cloud
          name: sg-s3-credentials ->secret created earlier
        default: true
        objectStorage:
          bucket: velero
          prefix: demobackup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
```

```
        - kubevirt
```

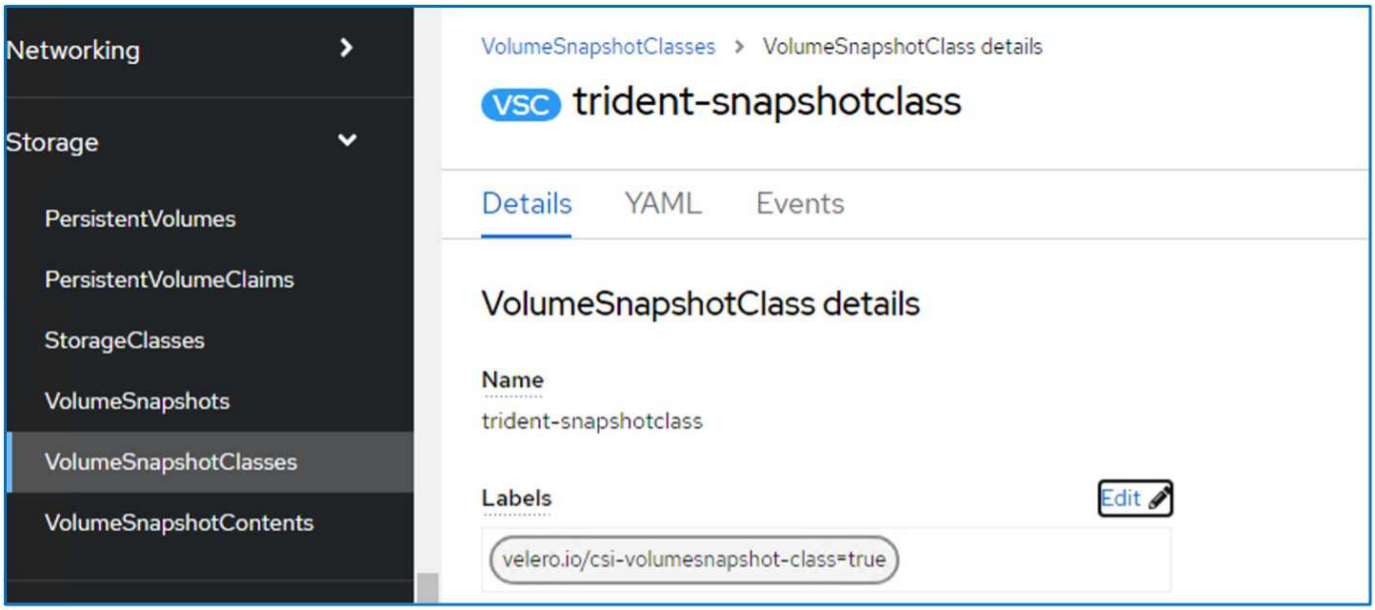
yaml ファイルの spec セクションは、上記の例と同様に、次のパラメータに対して適切に構成する必要があります。

backupLocations ONTAP S3 または StorageGrid S3 (yaml に示されている認証情報とその他の情報を含む) が、velero のデフォルトの BackupLocation として設定されています。

snapshotLocations Container Storage Interface (CSI) スナップショットを使用する場合は、CSI ドライバーを登録するために VolumeSnapshotClass CR を作成するため、スナップショットの場所を指定する必要はありません。この例では、 Trident CSI を使用し、以前にTrident CSI ドライバーを使用して VolumeSnapShotClass CR を作成しました。

CSI プラグインを有効にする CSI スナップショットを使用して永続ボリュームをバックアップするには、Velero の defaultPlugins に csi を追加します。 Velero CSI プラグインは、CSI でバックアップされた PVC をバックアップするために、**velero.io/csi-volumesnapshot-class** ラベルが設定されたクラスター内の VolumeSnapshotClass を選択します。このために

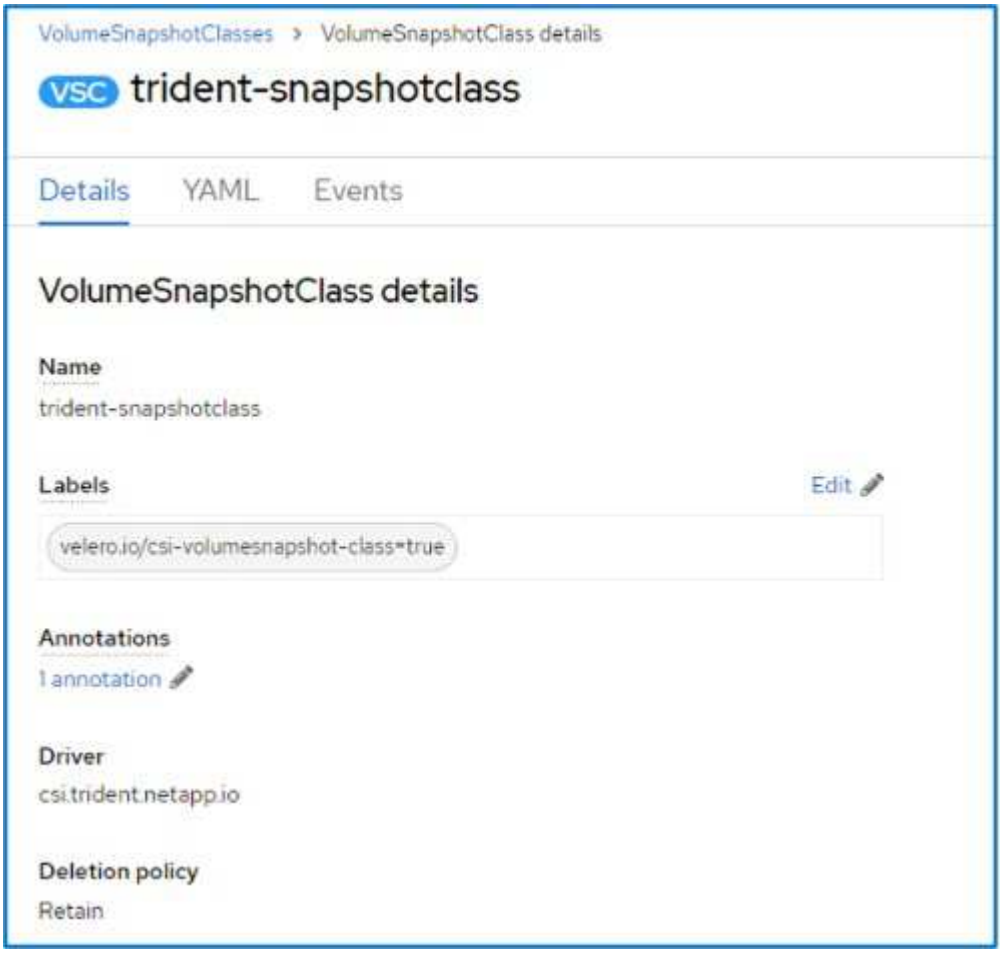
- trident VolumeSnapshotClass を作成する必要があります。
- trident-snapshotclass のラベルを編集し、以下に示すように **velero.io/csi-volumesnapshot-class=true** に設定します。



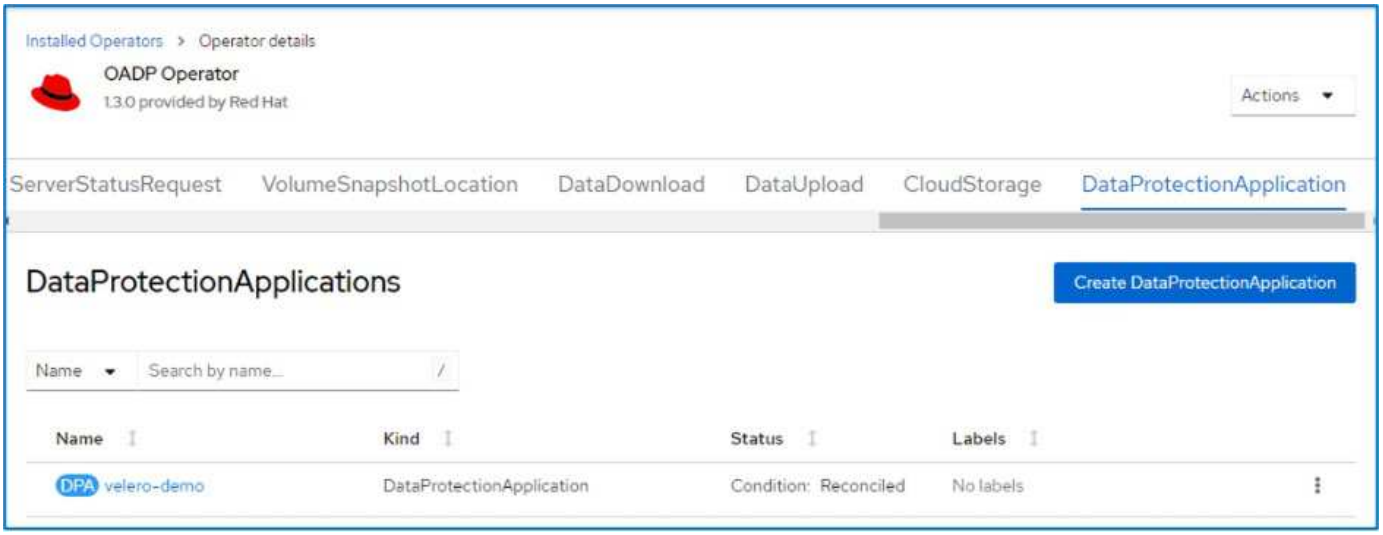
VolumeSnapshot オブジェクトが削除された場合でもスナップショットが保持されることを確認します。これは、**deletionPolicy** を Retain に設定することで実行できます。そうでない場合、名前空間を削除すると、そこにバックアップされたすべての PVC が完全に失われます。

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
```

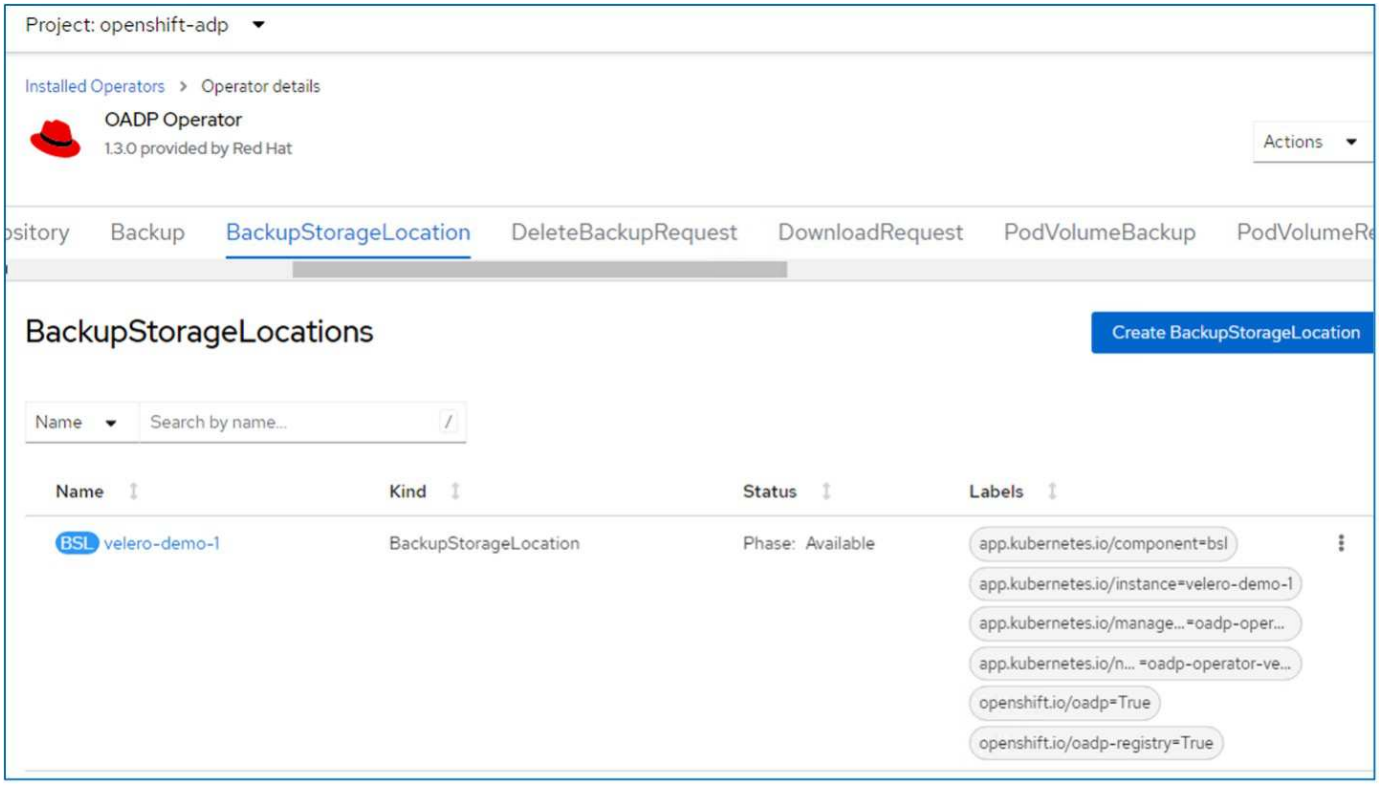
```
deletionPolicy: Retain
```



DataProtectionApplication が作成され、状態が Reconciled であることを確認します。



OADP オペレータは対応する BackupStorageLocation を作成します。これはバックアップの作成時に使用されます。



OpenShift Container Platform のアプリのオンデマンド バックアップの作成

このセクションでは、OpenShift Virtualization で VM のオンデマンド バックアップを作成する方法について説明します。

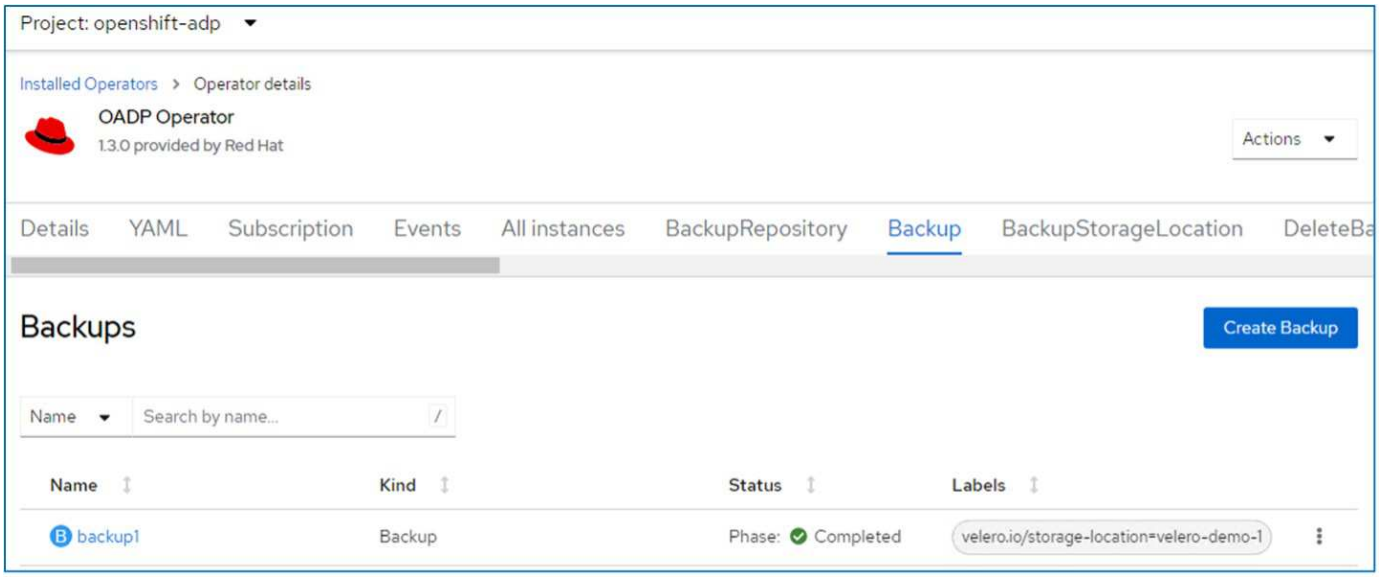
アプリのバックアップを作成する手順

アプリのオンデマンドバックアップ（アプリのメタデータとアプリの永続ボリューム）を作成するには、**Backup**タブをクリックしてBackup Custom Resource（CR）を作成します。Backup CRを作成するためのサンプルyamlが提供されています。このyamlを使用すると、指定された名前空間内のアプリとその永続ストレージがバックアップされます。追加のパラメータは、"ドキュメント"に示すように設定できます。

指定された名前空間内の永続ボリュームとアプリ リソースのスナップショットが CSI によって作成されます。このスナップショットは、yaml で指定されたバックアップの場所に保存されます。バックアップは、TTL で指定されたとおり 30 日間システム内に残ります。

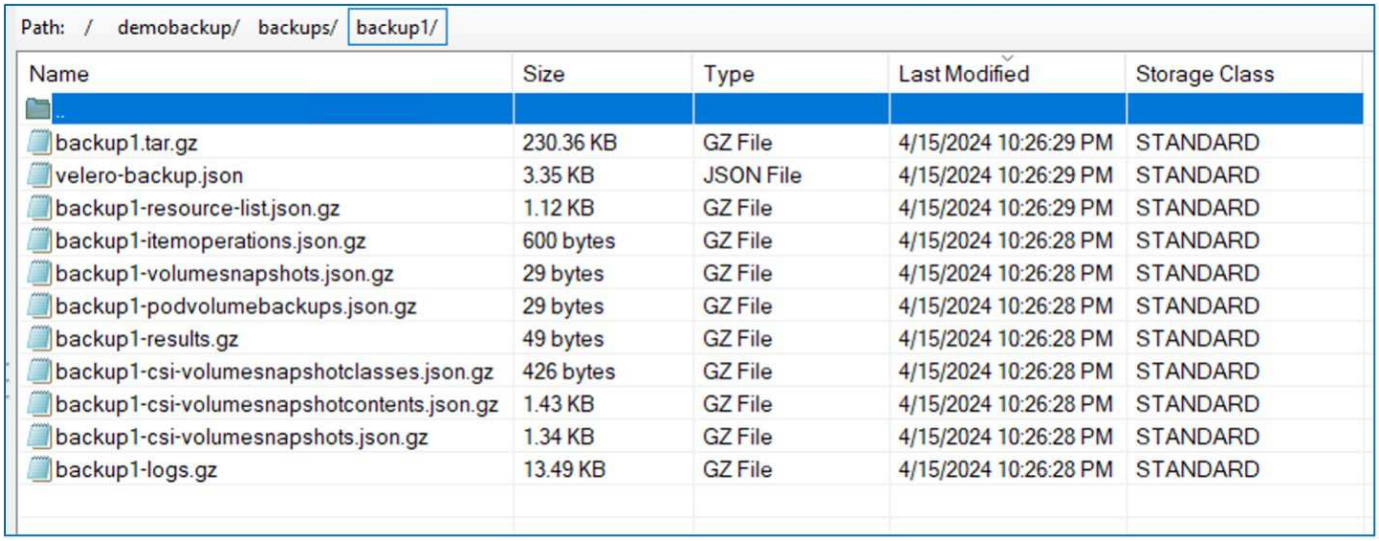
```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql ->namespace of the app
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: false
  storageLocation: velero-container-backup-ontap-1 -->this is the
backupStorageLocation previously created when Velero is configured.
  ttl: 720h0m0s
```

バックアップが完了すると、そのフェーズは完了として表示されます。



S3 ブラウザ アプリケーションを使用して、オブジェクト ストレージ内のバックアップを検査できます。バックアップのパスは、プレフィックス名 (velero/container-demo-backup) が付いた構成されたバケットに表示されます。バックアップの内容には、ボリューム スナップショット、ログ、アプリケーションのその他のメタデータが含まれていることがわかります。

StorageGrid では、テナント マネージャーから利用できる S3 コンソールを使用してバックアップ オブジェクトを表示することもできます。



アプリのスケジュールバックアップの作成

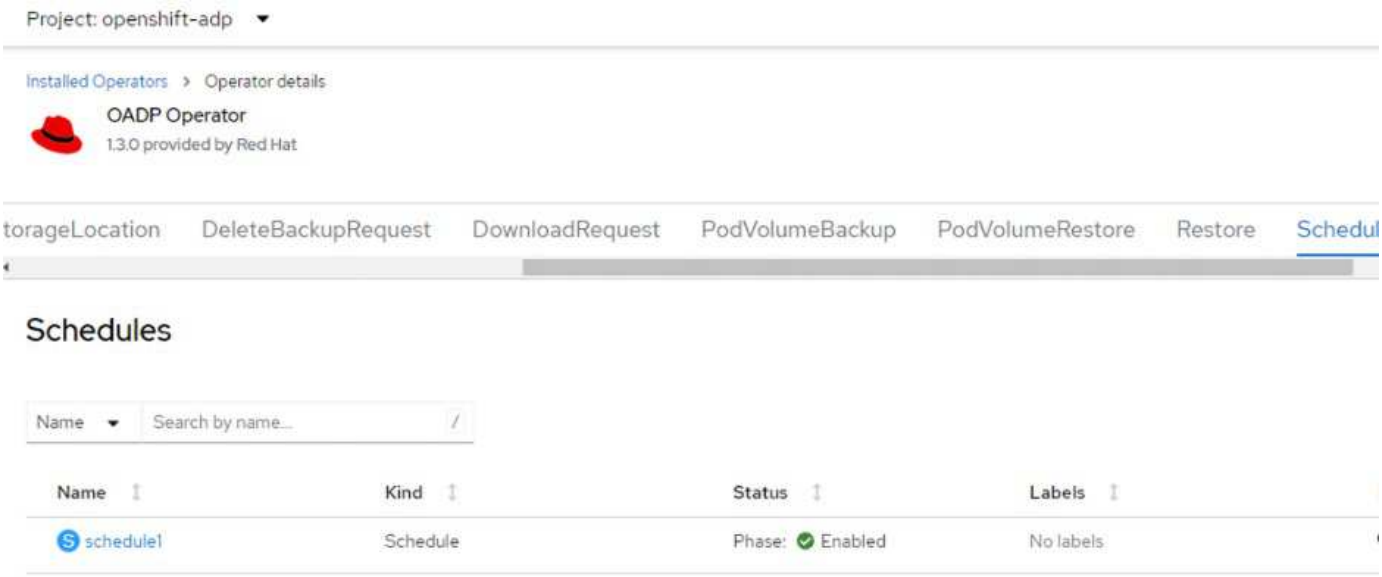
スケジュールに従ってバックアップを作成するには、スケジュール CR を作成する必要があります。スケジュールは、バックアップを作成する時間を指定できる単純な Cron 式です。スケジュール CR を作成するためのサンプル yaml を以下に示します。

```
apiVersion: velero.io/v1
kind: Schedule
```

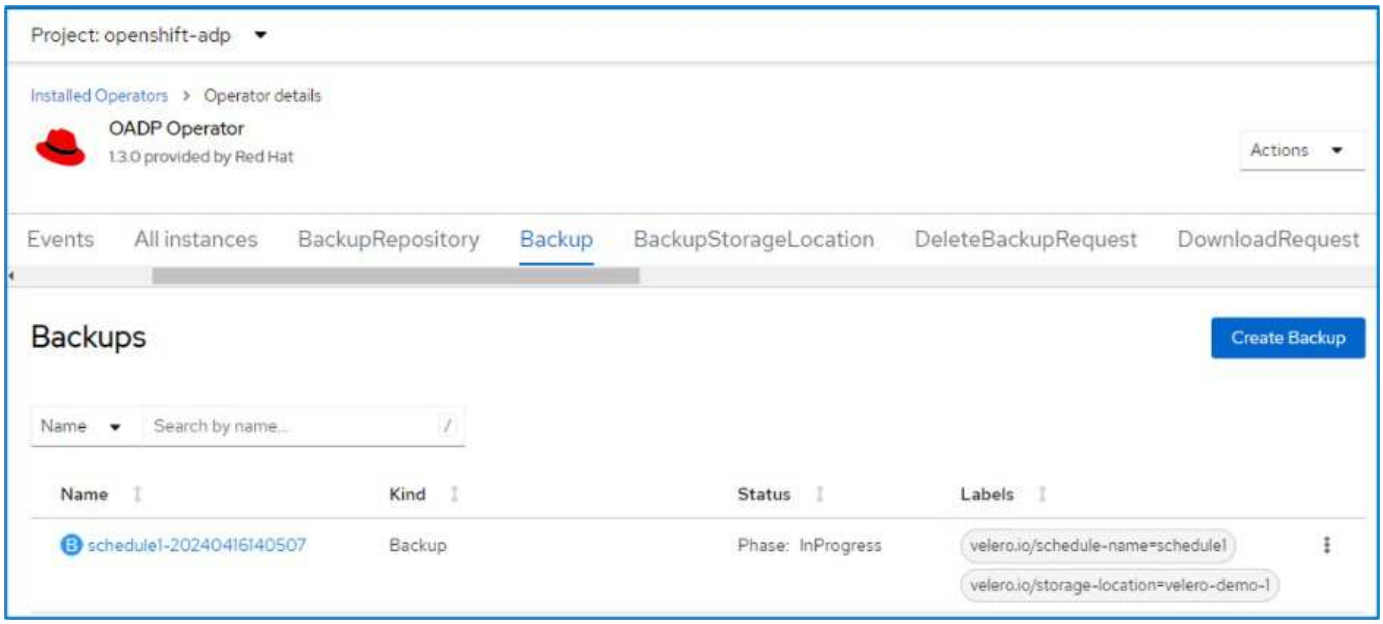
```
metadata:
  name: schedule1
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    includedNamespaces:
      - postgresql
    storageLocation: velero-container-backup-ontap-1
```

Cron 式 0 7 * * * は、毎日 7:00 にバックアップが作成されることを意味します。バックアップに含める名前空間とバックアップの保存場所も指定します。したがって、バックアップ CR の代わりに、スケジュール CR を使用して、指定された時間と頻度でバックアップを作成します。

スケジュールが作成されると、有効になります。



バックアップはこのスケジュールに従って作成され、[バックアップ] タブから表示できます。



あるクラスターから別のクラスターにアプリを移行する

Velero のバックアップおよび復元機能は、クラスター間でデータを移行するための貴重なツールになります。このセクションでは、あるクラスターのオブジェクト ストレージにアプリのバックアップを作成し、同じオブジェクト ストレージから別のクラスターにアプリを復元することで、あるクラスターから別のクラスターにアプリを移行する方法について説明します。 。

▼ 最初のクラスターからのバックアップ

クラスター **1** の前提条件

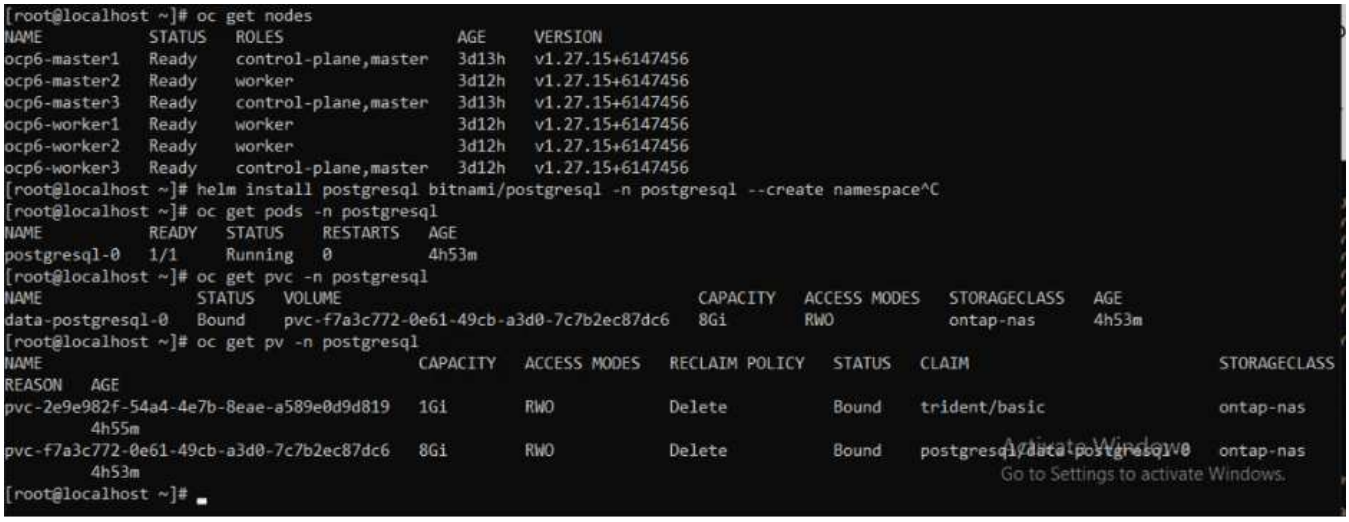
- クラスターにTridentをインストールする必要があります。
- トライデント バックエンドとストレージ クラスを作成する必要があります。
- OADP オペレータをクラスターにインストールする必要があります。
- DataProtectionApplication を構成する必要があります。

DataProtectionApplication オブジェクトを構成するには、次の仕様を使用します。

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false'
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'
          s3Url: 'https://10.61.181.161'
        credential:
          key: cloud
```

```
          name: ontap-s3-credentials
        default: true
        objectStorage:
          bucket: velero
          caCert: <base-64 encoded tls certificate>
          prefix: container-backup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

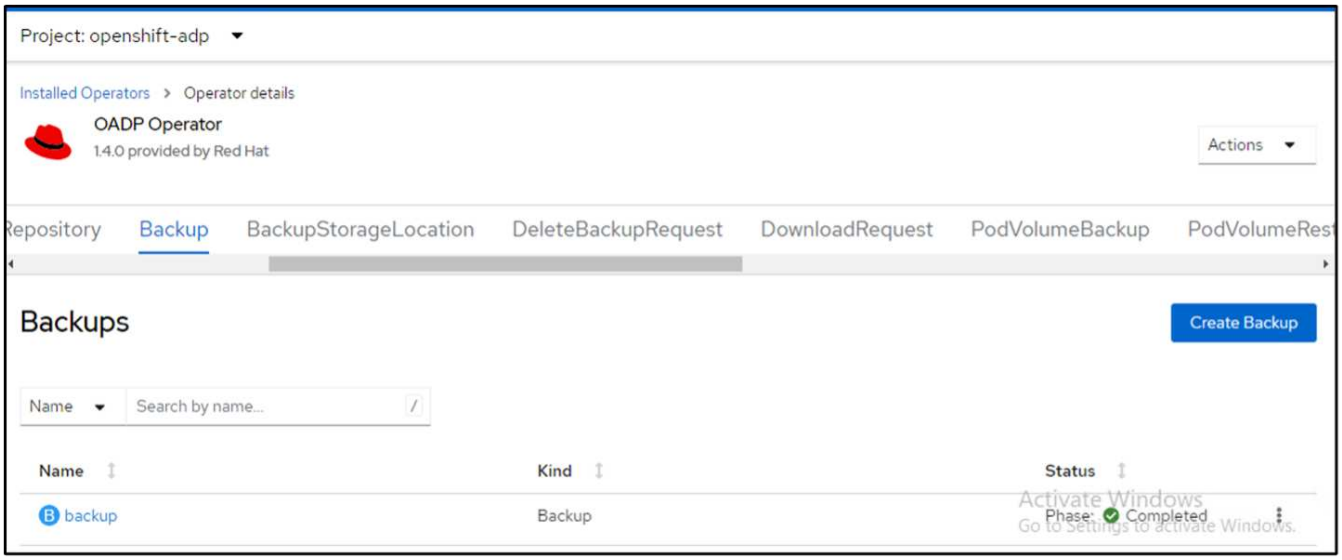
- クラスター上にアプリケーションを作成し、このアプリケーションのバックアップを取得します。例として、postgres アプリケーションをインストールします。



- バックアップ CR には次の仕様を使用します。

```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: true
  storageLocation: velero-sample-1
```

```
    ttl: 720h0m0s
```



すべてのインスタンス タブをクリックすると、さまざまなオブジェクトが作成され、さまざまなフェーズを経て最終的にバックアップが 完了 フェーズに到達する様子を確認できます。

名前空間 postgresql 内のリソースのバックアップは、OADP 仕様の backupLocation で指定されたオブジェクト ストレージの場所 (ONTAP S3) に保存されます。

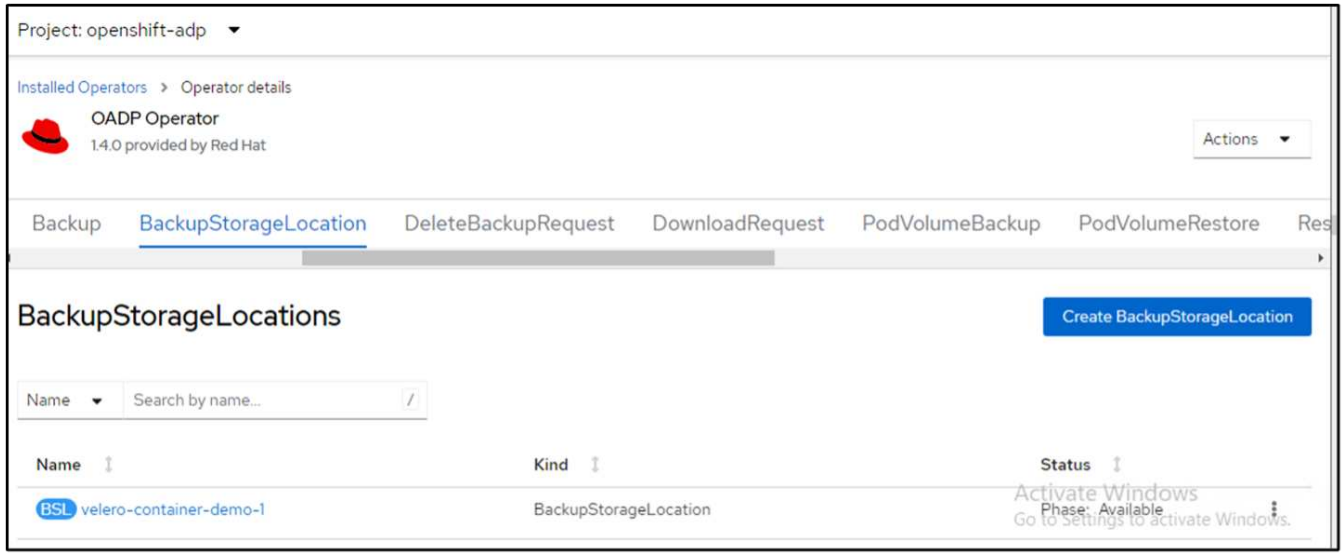
▼ 2番目のクラスターに復元する

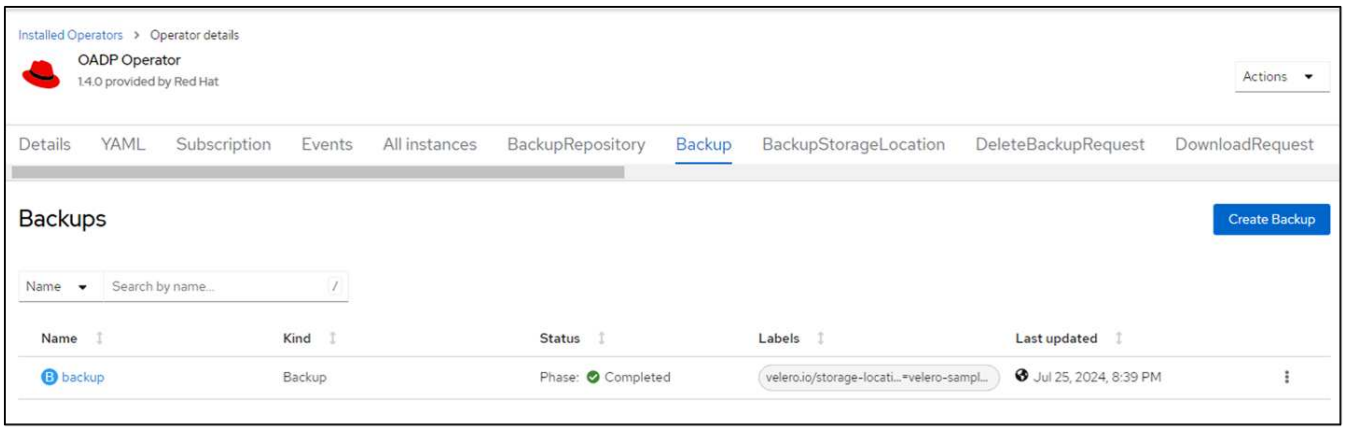
クラスター **2** の前提条件

- Trident はクラスター 2 にインストールする必要があります。
- postgresql アプリは postgresql 名前空間にまだインストールされていない必要があります。
- OADP オペレータはクラスター 2 にインストールする必要があり、BackupStorage Location は最初のクラスターからバックアップが保存されたのと同じオブジェクト ストレージの場所を指している必要があります。
- バックアップ CR は 2 番目のクラスターから見える必要があります。

```
[root@localhost ~]# oc get pods -n trident
NAME                                READY   STATUS    RESTARTS   AGE
trident-controller-6799cfb77f-8rzvk   6/6     Running   6          2d7h
trident-node-linux-7wvjz            2/2     Running   2          2d7h
trident-node-linux-8vvm2            2/2     Running   0          2d7h
trident-node-linux-bgs6f            2/2     Running   2          2d7h
trident-node-linux-njwb8            2/2     Running   0          2d7h
trident-node-linux-scqjl            2/2     Running   0          2d7h
trident-node-linux-swr69            2/2     Running   2          2d7h
trident-operator-b88b86fc8-7fk68    1/1     Running   1          2d7h
[root@localhost ~]#
```

```
[root@localhost ~]# oc get nodes
NAME           STATUS   ROLES                  AGE   VERSION
ocp7-master1   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master2   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master3   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-worker1   Ready    worker                 3d    v1.27.15+6147456
ocp7-worker2   Ready    worker                 3d    v1.27.15+6147456
ocp7-worker3   Ready    worker                 3d    v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pvc -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pv -n postgresql
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                 STORAGECLASS   REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic         ontap-nas               11m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc      vsphere-sc              2d7
h
[root@localhost ~]#
```



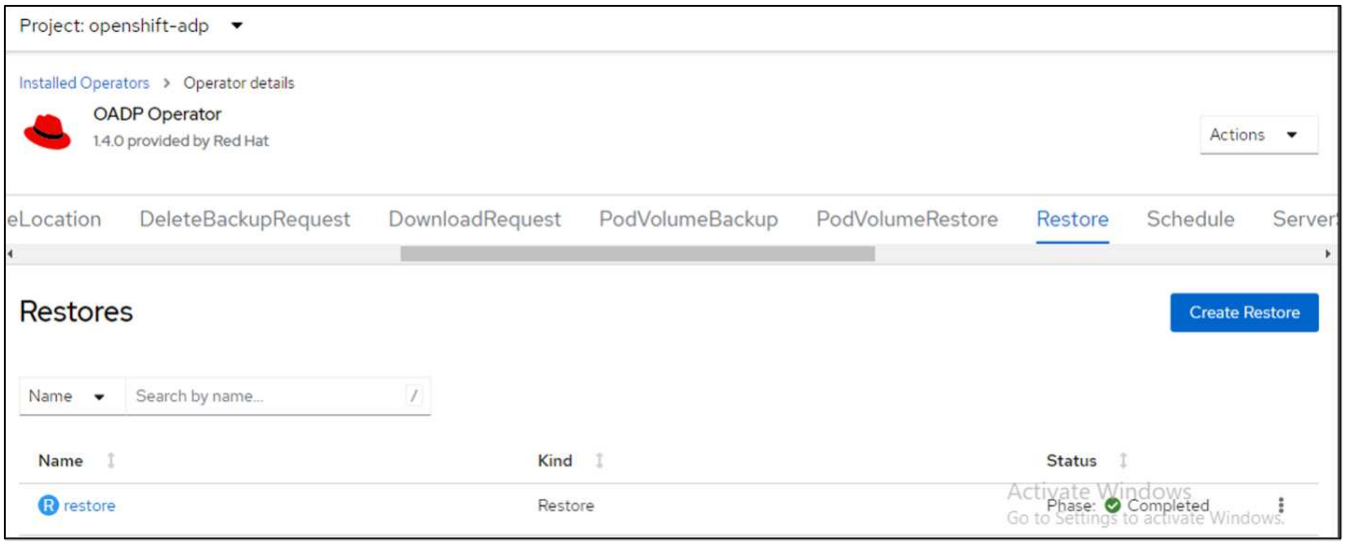


このクラスター上のアプリをバックアップから復元します。次の yaml を使用して復元 CR を作成します。

```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
```

```
  backupName: backup
  restorePVs: true
```

復元が完了すると、postgresql アプリがこのクラスター上で実行されており、pvc および対応する pv に関連付けられていることがわかります。アプリの状態はバックアップを取ったときと同じです。




```
[root@localhost ~]# export KUBECONFIG=ocp-cluster7/kubeconfig-ocp-cluster7
[root@localhost ~]# oc get nodes
NAME          STATUS   ROLES                  AGE    VERSION
ocp7-master1  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-master2  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-master3  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-worker1  Ready    worker                 3d3h   v1.27.15+6147456
ocp7-worker2  Ready    worker                 3d3h   v1.27.15+6147456
ocp7-worker3  Ready    worker                 3d3h   v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          31m
[root@localhost ~]# oc get pvc -n postgresql
NAME              STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-ce7044e3-2ba5-4934-8bad-553fa7d35128   8Gi        RWO            ontap-nas      31m
[root@localhost ~]# oc get pv
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                          STORAGECLASS
REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic                  ontap-nas
         3h27m
pvc-ce7044e3-2ba5-4934-8bad-553fa7d35128   8Gi        RWO            Delete           Bound    postgresql/data-postgresql-0   ontap-nas
         31m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc               vsphere-sc
         2d10h
[root@localhost ~]#
```

Activate Windows
Go to Settings to activate Windows.

バックアップからアプリを復元する

このセクションでは、バックアップからアプリを復元する方法について説明します。

前提条件

バックアップから復元するには、アプリが存在していた名前空間が誤って削除されたと仮定します。

```
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          102s
[root@localhost ~]# oc delete ns postgresql
namespace "postgresql" deleted

[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]#
```

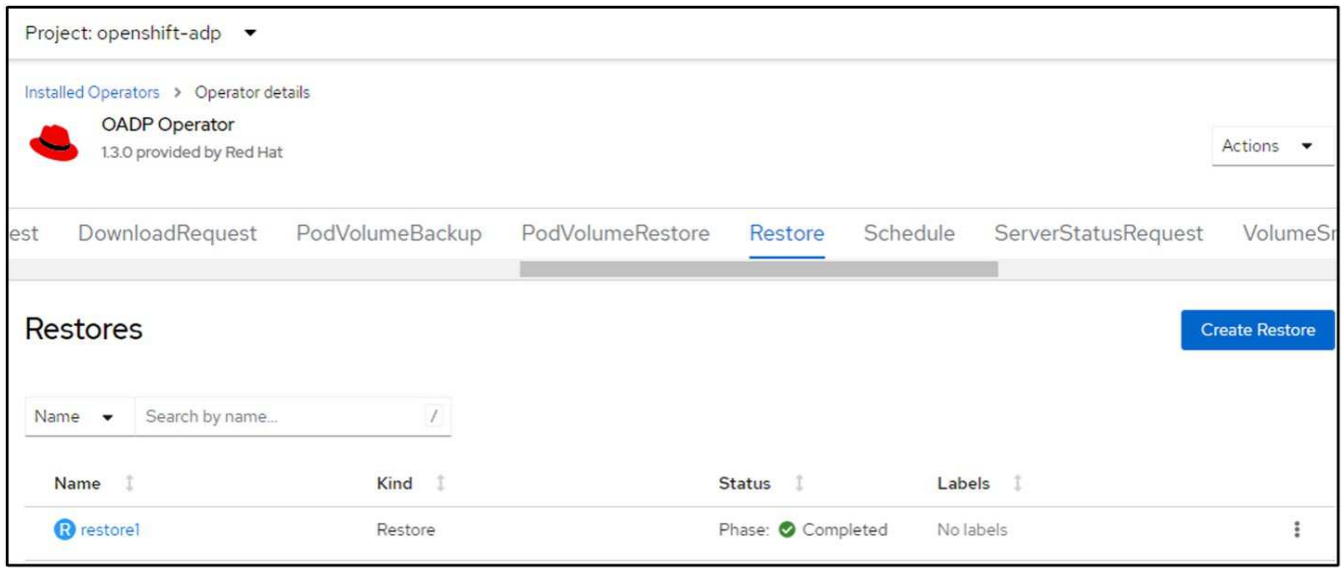
▼ 同じ名前空間に復元する

先ほど作成したバックアップから復元するには、復元カスタムリソース（CR）を作成する必要があります。名前を付け、復元元のバックアップの名前を指定し、restorePVsをtrueに設定する必要があります。追加のパラメータは、"ドキュメント"に示すように設定できます。「作成」ボタンをクリックします。




```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
```

フェーズが完了したことが表示されると、アプリがスナップショットが取得された時点の状態に復元されたことがわかります。アプリは同じ名前空間に復元されます。




```
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS              RESTARTS   AGE
postgresql-0   0/1     ContainerCreating   0          16s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   0/1     Running   0          22s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   0/1     Running   0          29s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          37s
[root@localhost ~]#
```

▼ 別の名前空間に復元する

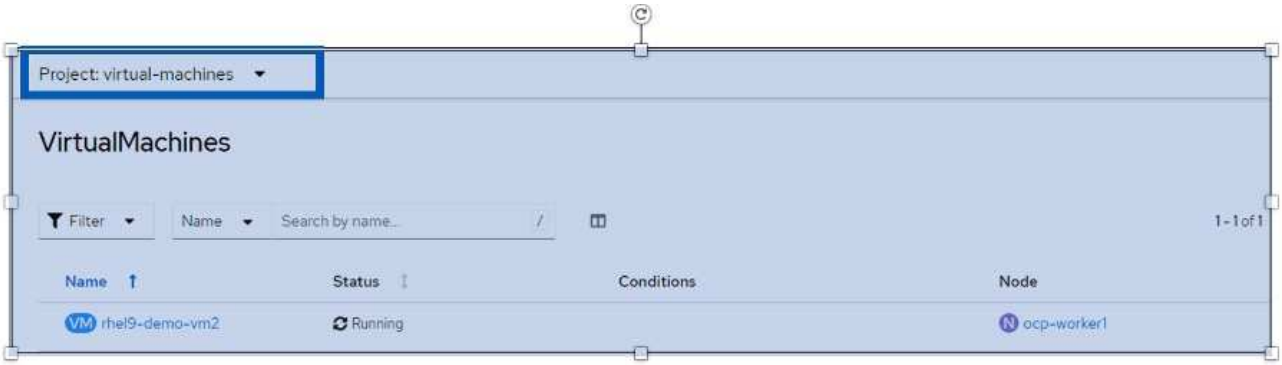
アプリを別の名前空間に復元するには、復元 CR の yaml 定義で namespaceMapping を指定できます。

次のサンプル yaml ファイルは、アプリとその永続ストレージを postgresql 名前空間から新しい名前空間 postgresql-restored に復元するための復元 CR を作成します。

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
```

```
  includedNamespaces:
  - postgresql
  namespaceMapping:
    postgresql: postgresql-restored
```

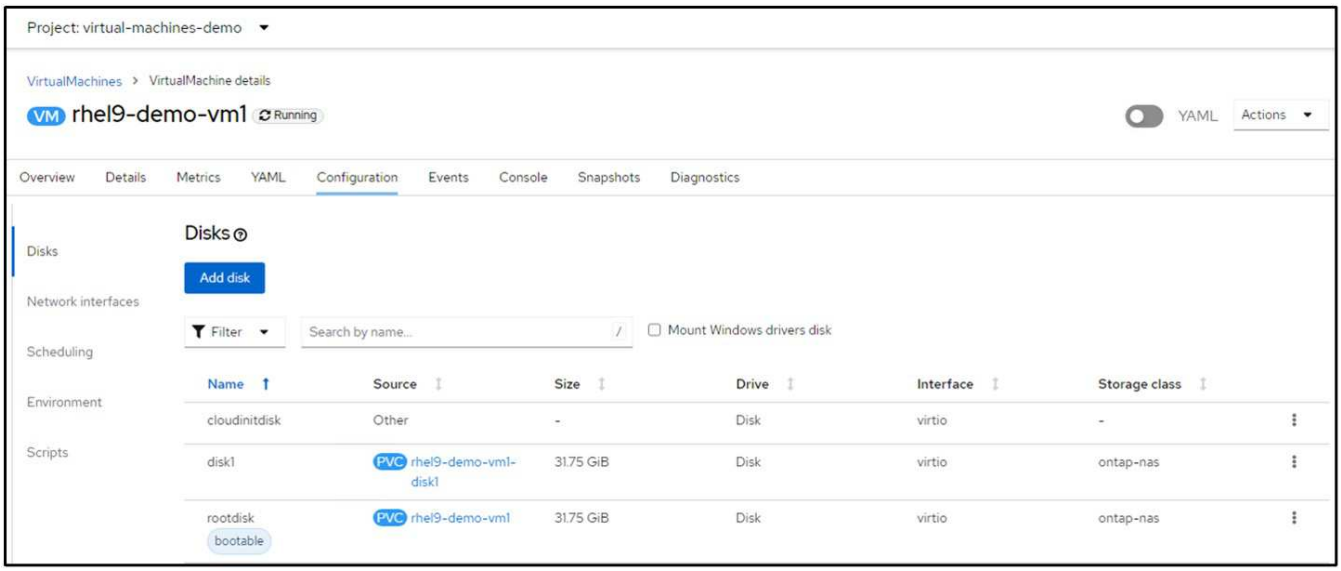
フェーズが完了したことが表示されると、アプリがスナップショットが取得された時点の状態に復元されたことがわかります。アプリは、yaml で指定された別の名前空間に復元されます。

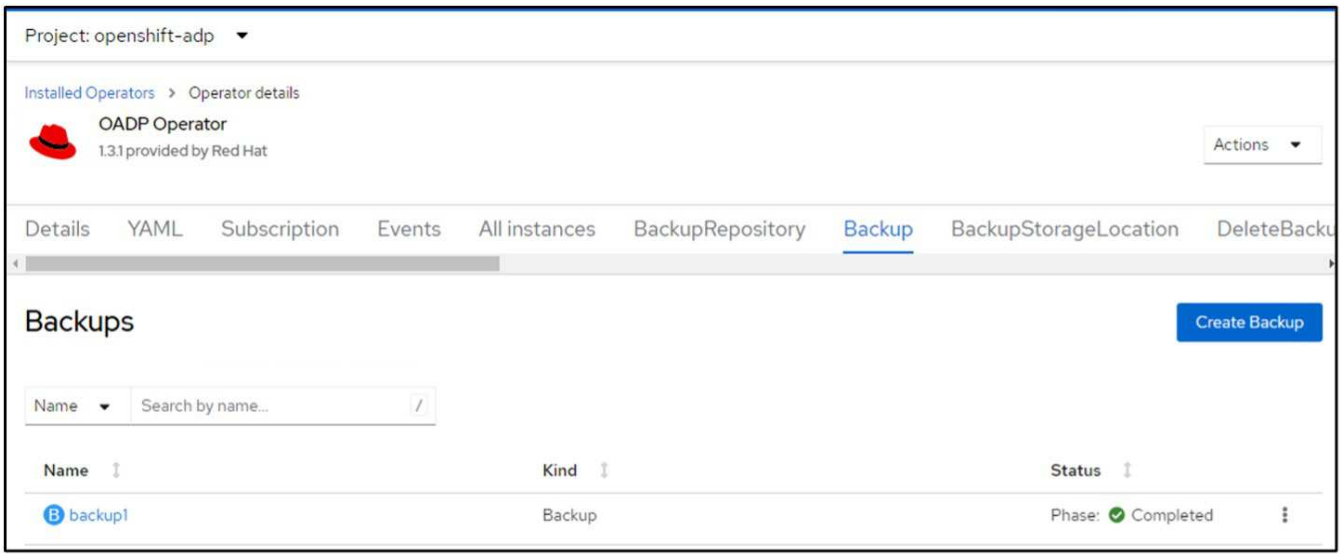


▼ 別のストレージクラスに復元する

Velero は、json パッチを指定して復元中にリソースを変更する一般的な機能を提供します。リソースが復元される前に、json パッチが適用されます。 json パッチは configmap で指定され、configmap は復元コマンドで参照されます。この機能を使用すると、異なるストレージ クラスを使用して復元できます。

以下の例では、アプリはデプロイメント中に、永続ボリュームのストレージ クラスとして ontap-nas を使用します。 「backup-postgresql-ontaps3」という名前のアプリのバックアップが作成されます。





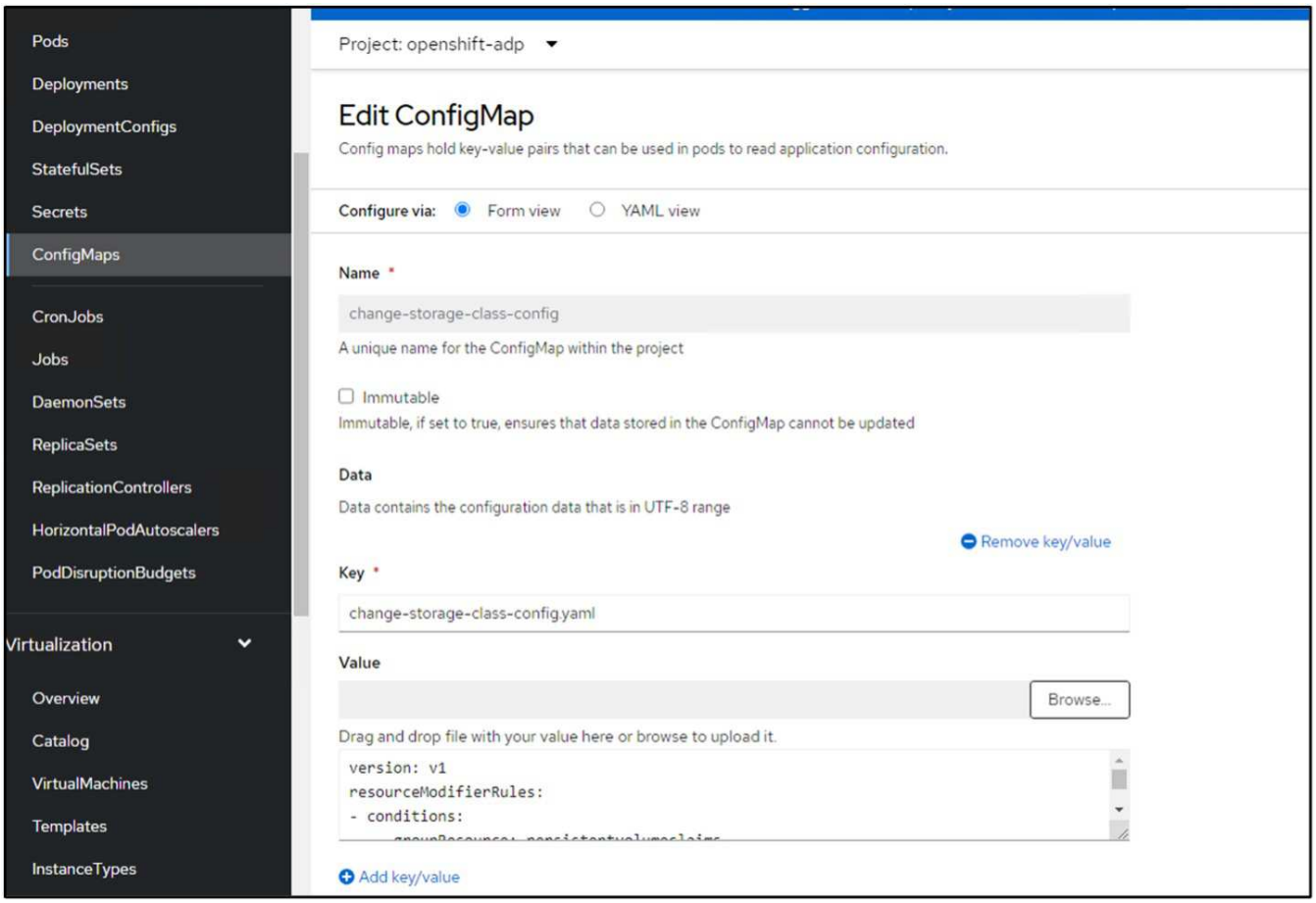
アプリをアンインストールして、アプリの損失をシミュレートします。

別のストレージ クラス (ontap-nas-eco ストレージ クラスなど) を使用して VM を復元するには、次の 2 つの手順を実行する必要があります。

ステップ**1**

次のように、openshift-adp 名前空間に構成マップ (コンソール) を作成します。スクリーンショットに示すように詳細を入力します。名前空間を選択: openshift-adp 名前: change-ontap-sc (任意の名前にすることができます) キー: change-ontap-sc-config.yaml: 値:

```
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "data-postgresql*"
     namespaces:
     - postgresql
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"
```



結果の構成マップ オブジェクトは次のようになります (CLI)。

```
# kubectl describe cm/change-storage-class-config -n openshift-
adp
Name:         change-storage-class-config
Namespace:    openshift-adp
Labels:       velero.io/change-storage-class=RestoreItemAction
              velero.io/plugin-config=
Annotations:  <none>

Data
====
change-storage-class-config.yaml:
----
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "^rhel*"
     namespaces:
     - virtual-machines-demo
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"



BinaryData
====

Events:  <none>
```

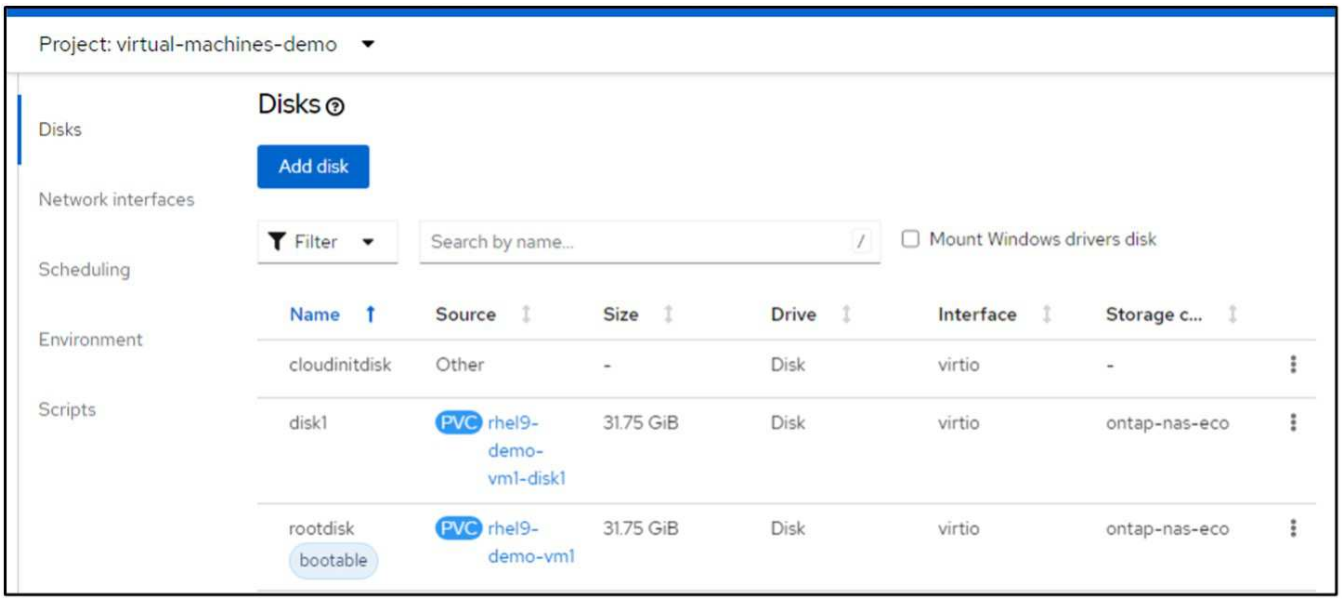
この構成マップは、復元の作成時にリソース修飾子ルールを適用します。 rhel で始まるすべての永続ボリューム要求のストレージ クラス名を ontap-nas-eco に置き換えるパッチが適用されます。

ステップ**2**

VM を復元するには、Velero CLI から次のコマンドを使用します。

```
#velero restore create restore1 --from-backup backup1 --resource
-modifier-configmap change-storage-class-config -n openshift-adp
```

アプリは、ストレージ クラス ontap-nas-eco を使用して作成された永続ボリューム要求と同じ名前空間に復元されます。



Velero を使用したバックアップと復元の削除

このセクションでは、Velero を使用して OpenShift コンテナー プラットフォーム内のアプリのバックアップを削除および復元する方法について説明します。

すべてのバックアップを一覧表示する

OC CLI ツールまたは Velero CLI ツールを使用して、すべてのバックアップ CR を一覧表示できます。指示に従ってVelero CLIをダウンロードしてください。"Velero ドキュメント" 。

```
[root@localhost ~]# oc get backups -n openshift-adp
NAME                      AGE
backup-postgresql-ontaps3   23h
backup2                     26s
schedule1-20240717070005    6h42m
[root@localhost ~]# velero get backups -n openshift-adp
NAME                      STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3   Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                     Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005    Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

バックアップの削除

OC CLI ツールを使用して、オブジェクト ストレージ データを削除せずにバックアップ CR を削除できます。バックアップは CLI/コンソール出力から削除されます。ただし、対応するバックアップはオブジェクト ストレージから削除されないため、CLI/コンソール出力に再度表示されます。

```
[root@localhost ~]# oc delete backup backup2 -n openshift-adp
backup.velero.io "backup2" deleted
[root@localhost ~]# oc get backups -n openshift-adp
NAME                          AGE
backup-postgresql-ontaps3     23h
schedule1-20240717070005      6h49m
[root@localhost ~]# oc get backups -n openshift-adp
NAME                          AGE
backup-postgresql-ontaps3     23h
backup2                       24s
schedule1-20240717070005      6h50m
[root@localhost ~]#
```

バックアップ **CR** と関連するオブジェクト ストレージ データを削除する場合は、**Velero CLI** ツールを使用して削除できます。

```
[root@localhost ~]# velero get backups -n openshift-adp
NAME                          STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3     Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                       Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005      Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]# velero delete backup backup2 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete backup "backup2" submitted successfully.
The backup will be fully deleted after all associated data (disk snapshots, backup files, restores) are removed.
[root@localhost ~]# velero get backups -n openshift-adp
NAME                          STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3     Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005      Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

復元の削除

OC CLI または Velero CLI を使用して、復元 CR オブジェクトを削除できます。

```
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                    STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3   Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
restore1   backup-postgresql-ontaps3   Completed   2024-07-16 16:36:37 -0400 EDT   2024-07-16 16:36:59 -0400 EDT   0        9          2024-07-16 16:36:37 -0400 EDT   <none>
[root@localhost ~]# velero restore delete restore1 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete restore "restore1" submitted successfully.
The restore will be fully deleted after all associated data (restore files in object storage) are removed.
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                    STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3   Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
[root@localhost ~]#
[root@localhost ~]# oc delete restore restore -n openshift-adp
restore.velero.io "restore" deleted
[root@localhost ~]# oc get restore -n openshift-adp
No resources found in openshift-adp namespace.
[root@localhost ~]# velero get restore -n openshift-adp
[root@localhost ~]#
```

Activate Windows

NetAppのハイブリッド マルチクラウド ソリューションに関するビデオとデモをご覧ください

NetAppを使用した Amazon Web Services 向けハイブリッド マルチクラウド ソリューションに関するビデオを見る

NetAppによる AWS 向けハイブリッド マルチクラウド ソリューションを紹介する NetApp の包括的なビデオ ライブラリをご覧ください。ゲスト接続ストレージ、TCO 削減、補足データストア、VMware Cloud on AWS およびAmazon FSx for ONTAPの移行ワークフロー（Windows および Linux のシナリオを含む）に関するビデオをご覧ください。

ゲスト接続ストレージ

iSCSI を使用した FSx ONTAPによる Windows ゲスト接続ストレージ

NFS を使用した FSx ONTAPによる Linux ゲスト接続ストレージ

TCOと補足データストア

Amazon FSx ONTAPによる VMware Cloud on AWS の TCO 削減

VMware Cloud on AWS 補足データストア (Amazon FSx ONTAP搭載)

移行ワークフロー (HCX)

VMC 向けの VMware HCX の展開と構成のセットアップ

VMC および FSx ONTAP向け VMware HCX を使用した vMotion 移行のデモンストレーション

VMC および FSx ONTAP向け VMware HCX を使用したコールド マイグレーションのデモンストレーション

NetAppを使用した Azure VMware クラウド向けハイブリッド マルチクラウド ソリューションに関するビデオを見る

NetAppを使用した Azure VMware Solution (AVS) のハイブリッド マルチクラウド ソリューションを紹介する NetApp の包括的なビデオ ライブラリをご覧ください。このコレクションには、補足データストア、災害復旧、移行ワークフローに関するビデオが含まれています。

補足データストア

Azure NetApp Filesを使用した Azure VMware Solution 補足データストアの概要

ディザスタ リカバリ

Cloud Volumes ONTAP、 SnapCenter 、JetStream を使用した Azure VMware Solution DR

移行ワークフロー (HCX)

VMware HCX による AVS および ANF 向けコールド マイグレーションのデモンストレーション

AVS および ANF 向け VMware HCX を使用した vMotion のデモンストレーション

VMware HCX による AVS および ANF の一括移行のデモ

NetAppを使用した Red Hat OpenShift 向けハイブリッド マルチクラウド ソリューションに関するビデオを見る

NetAppによる Red Hat OpenShift 向けハイブリッド マルチクラウド ソリューションを紹介する NetApp の包括的なビデオ ライブラリをご覧ください。このコレクションには、FSx ONTAPを使用した OpenShift on AWS (ROSA) のスナップショットと復元、Tridentとの統合、アプリのフェイルオーバーとフェイルバック、Ansible を使用したFlexPodでの Oracle RAC の自動デプロイメントに関するデモが含まれています。

スナップショットと復元

Amazon FSx ONTAPストレージを使用した Red Hat OpenShift Service on AWS (ROSA) クラスター上のアプリケーションのスナップショット/リストア

ストレージ統合

FSx ONTAPとTridentの統合

フェイルオーバーとフェイルバック

FSx ONTAPを使用した ROSA 上のアプリのフェイルオーバーとフェイルバック

ソリューション自動化



Ansibleを使用した**FlexPod**への**Oracle 19c RAC**の自動導入

NetApp の専門家によるクラウド ソリューションのブログを読む

ONTAPストレージとNetAppクラウド ソリューションを統合するための実用的なガイダンスとベスト プラクティスを紹介するブログをお読みください。

VMware と AWS およびAmazon FSx for ONTAP の統合

- "Amazon EC2 とAmazon FSx ONTAP iSCSI プロトコルを使用して VMware VM を AWS に移行する"
- "Amazon EVS が FSx for ONTAPと統合"
- "Amazon EVSがFSx for ONTAPのサポートを発表"
- "VMware HCX を使用して FSx ONTAPと VMware Cloud on AWS SDDC でハイブリッド クラウドを構成する"

Azure VMware ソリューション

- "あらゆるクラウドでストレージとデータ集約型の VMware ワークロードを最適化"
- "VMware ワークロードを Azure VMware Solution へ移行しますか？まずこちらをお読みください。"

Google Cloud VMware エンジン

- "Google Cloud VMware Engine (NetApp) 向けの Google Cloud Google Cloud NetApp Volumesデータストアのサポート"
- "NetApp Volumes を Google Cloud VMware Engine のデータストアとして使用する方法 (Google)"
- "NetAppブログ - ストレージを多用するアプリを Google Cloud に移行するよりよい方法"

データ保護と管理

- "SnapCenter プラグインおよび NetApp Backup and Recovery for VMs を使用した VMware 向け 3-2-1 データ保護"
- "NetApp Cloud Insightsによる最新データセンターの可観測性"

OpenShift コンテナ ワークロード向けNetApp

- "NetApp ONTAPはRed Hat OpenShiftコンテナプラットフォームのログストレージとしても機能します"

VMware ソブリンクラウド

- "新しいソブリンクラウドイニシアチブのご紹介"

法律上の表示

法的通知から、著作権情報、商標、特許などを確認できます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp、NetAppのロゴ、NetAppの商標一覧のページに掲載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

現在NetAppが所有する特許の一覧は以下のページから閲覧できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシー ポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

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

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

商標に関する情報

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