



# NetApp for Azure / AVS

## NetApp Solutions

NetApp  
September 26, 2024

# 目次

NetApp for Azure / AVS .....	1
Azure AVS 向けのネットアップの機能 .....	1
Azure / AVS上のワークロードを保護 .....	2
Azure / AVSでのワークロードの移行 .....	74
Region Availability - ANFの補助的なNFSデータストア .....	91

# NetApp for Azure / AVS

## Azure AVS 向けのネットアップの機能

ネットアップがAzure VMware解決策（AVS）に提供する機能の詳細をご確認ください。ゲスト接続ストレージデバイスとしてネットアップが提供する機能と、NFSデータストアの追加機能を利用して、ワークフローを移行し、クラウドへの拡張/バースト対応、バックアップ/リストア、ディザスタリカバリを実施できます。

次のオプションから選択して、目的のコンテンツのセクションに移動します。

- ["Azure で AVS を設定する"](#)
- ["AVS 向けのネットアップストレージオプション"](#)
- ["ネットアップとVMwareのクラウドソリューション"](#)

### Azure で AVS を設定する

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

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



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

セットアッププロセスは、次の手順に分けることができます。

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

詳細を表示します ["AVSの設定手順"](#)。

### AVS 向けのネットアップストレージオプション

ネットアップのストレージは、Azure AVS内で接続されたか、NFSデータストアとして追加で利用するかのいずれかの方法で利用できます。

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

Azure は、以下の構成でネットアップストレージをサポートします。

- ゲスト接続ストレージとしての Azure NetApp Files （ANF）
- Cloud Volumes ONTAP （CVO）をゲスト接続ストレージとして活用

- Azure NetApp Files (ANF) を追加のNFSデータストアとして使用できます

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

## 解決策のユースケース

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

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

["Azure AVS 向けネットアップソリューションをご覧ください"](#)

## Azure / AVS上のワークロードを保護

### ANFとJetStreamを使用したディザスタリカバリ

クラウドへのディザスタリカバリは、耐障害性に優れた対費用効果の高い方法で、サイトの停止やデータ破損からワークロードを保護します (ランサムウェアなど)。VMware VAIIOフレームワークを使用すると、オンプレミスのVMwareワークロードをAzure Blobストレージにレプリケートしてリカバリできるため、データ損失を最小限に抑えたり、ほぼゼロのRTOを実現できます。

Jetstream DRを使用すると、オンプレミスからAVS、特にAzure NetApp Files に複製されたワークロードをシームレスにリカバリできます。ディザスタリカバリサイトにある最小限のリソースと対費用効果の高いクラウドストレージを使用して、対費用効果の高いディザスタリカバリを実現します。Jetstream DRは、Azure Blob Storageを介したANFデータストアへのリカバリを自動化します。Jetstream DRは、独立したVMまたは関連するVMのグループを、ネットワークマッピングに従ってリカバリサイトインフラストラクチャにリカバリし、ランサムウェアからの保護のためのポイントインタイムリカバリを提供します。

このドキュメントでは、JetStream DRの動作原理とその主なコンポーネントについて説明します。

1. JetStream DRソフトウェアをオンプレミスのデータセンターにインストールします。
  - a. JetStream DRソフトウェアバンドルをAzure Marketplace (ZIP) からダウンロードし、JetStream DR MSA (OVA) を指定のクラスタに導入します。
  - b. I/Oフィルタパッケージを使用してクラスタを設定します(JetStream VIBをインストールします)。
  - c. DR AVSクラスタと同じリージョンでAzure Blob (Azureストレージアカウント) をプロビジョニング
  - d. DRVAアプライアンスを導入し、レプリケーションログボリューム (既存のデータストアまたは共有iSCSIストレージからVMDK) を割り当てます。
  - e. 保護されたドメイン (関連するVMのグループ) を作成し、DRVAとAzure Blob Storage / ANFを割り当てます。
  - f. 保護を開始します。
2. JetStream DRソフトウェアをAzure VMware解決策 プライベートクラウドにインストールします。
  - a. Runコマンドを使用して、JetStream DRをインストールおよび設定します。
  - b. [Scan Domains]オプションを使用して、同じAzure BLOBコンテナを追加し、ドメインを検出します。
  - c. 必要なDRVAアプライアンスを導入します。
  - d. 使用可能なvSANまたはANFデータストアを使用してレプリケーションログボリュームを作成します。
  - e. 保護されたドメインをインポートし、VMの配置にANFデータストアを使用するようにRocVA (リカバリVA) を設定します。
  - f. 適切なフェイルオーバーオプションを選択し、ほぼゼロのRTOドメインまたはVMに対して継続的なリハイドレートを開始します。
3. 災害発生時に、指定したAVS DRサイトでAzure NetApp Files データストアへのフェイルオーバーをトリガーします。
4. 保護対象サイトのリカバリ後、保護対象サイトへのフェイルバックを起動します。開始する前に、前提条件が満たされていることを確認してください "[リンク](#)" また、JetStream Softwareが提供するBandwidth Testing Tool (BWT) を実行して、JetStream DRソフトウェアで使用した場合にAzure BLOBストレージとそのレプリケーション帯域幅のパフォーマンスを評価します。接続を含む前提条件が整ったら、からJetStream DR for AVSをセットアップして登録します "[Azure Marketplace で入手できます](#)". ソフトウェアバンドルをダウンロードしたら、上記のインストールプロセスに進みます。

多数のVM (100+など) の保護を計画して開始する場合は、JetStream DR Automation ToolkitからCapacity Planning Tool (CPT) を使用します。RTOとリカバリ・グループの設定とともに保護対象のVMのリストを指定し、CPTを実行します。

CPTは次の機能を実行します。

- RTOに応じたVMを保護ドメインに統合する。
- DRVAとそのリソースの最適な数を定義する。

- 必要なレプリケーション帯域幅の見積もり
- レプリケーションログボリュームの特性（容量、帯域幅など）を特定します。
- 必要なオブジェクトストレージ容量などを見積もります。



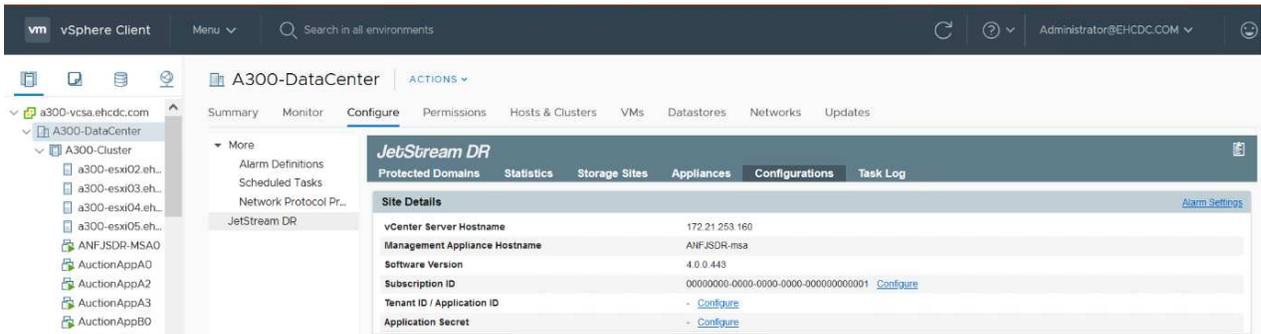
ドメインの数と内容は、平均IOPS、合計容量、優先度（フェイルオーバー順序を定義）、RTOなど、VMのさまざまな特性によって異なります。

### JetStream DRをオンプレミスのデータセンターにインストールします

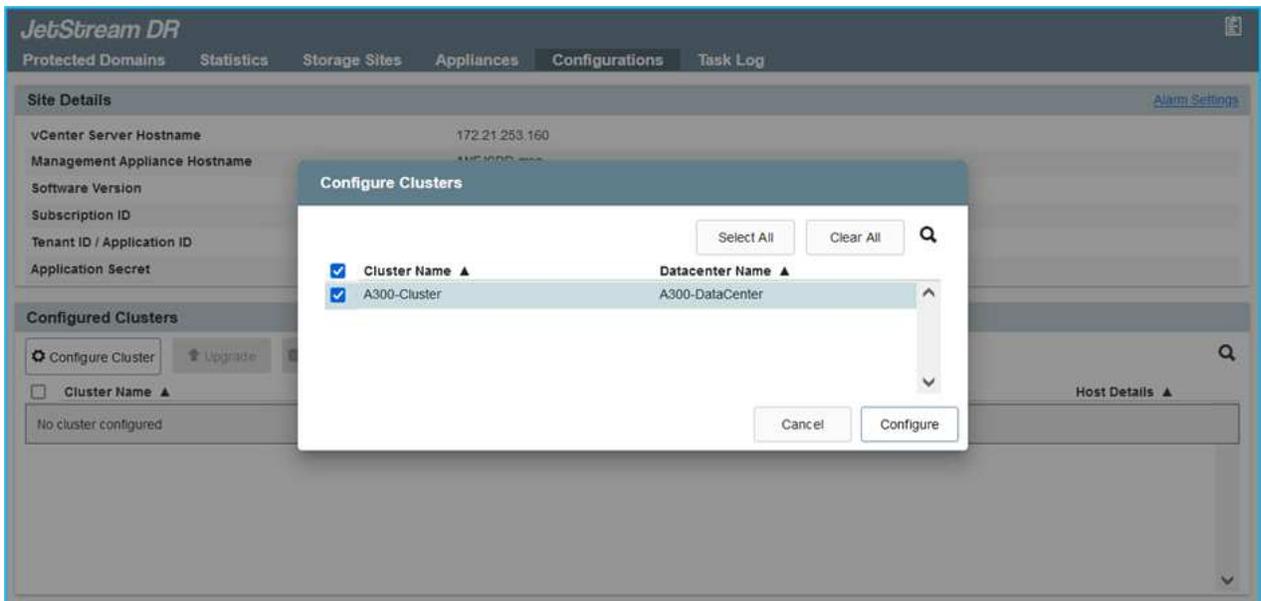
Jetstream DRソフトウェアは、JetStream DR Management Server Virtual Appliance (MSA)、DR Virtual Appliance (DRVA)、およびホストコンポーネント (I/O Filterパッケージ) の3つの主要コンポーネントで構成されています。MSAは、コンピューティングクラスタにホストコンポーネントをインストールして構成し、JetStream DRソフトウェアを管理するために使用されます。次に、インストールプロセスの概要の概要を示します。

## JetStream DRをオンプレミスにインストールする方法

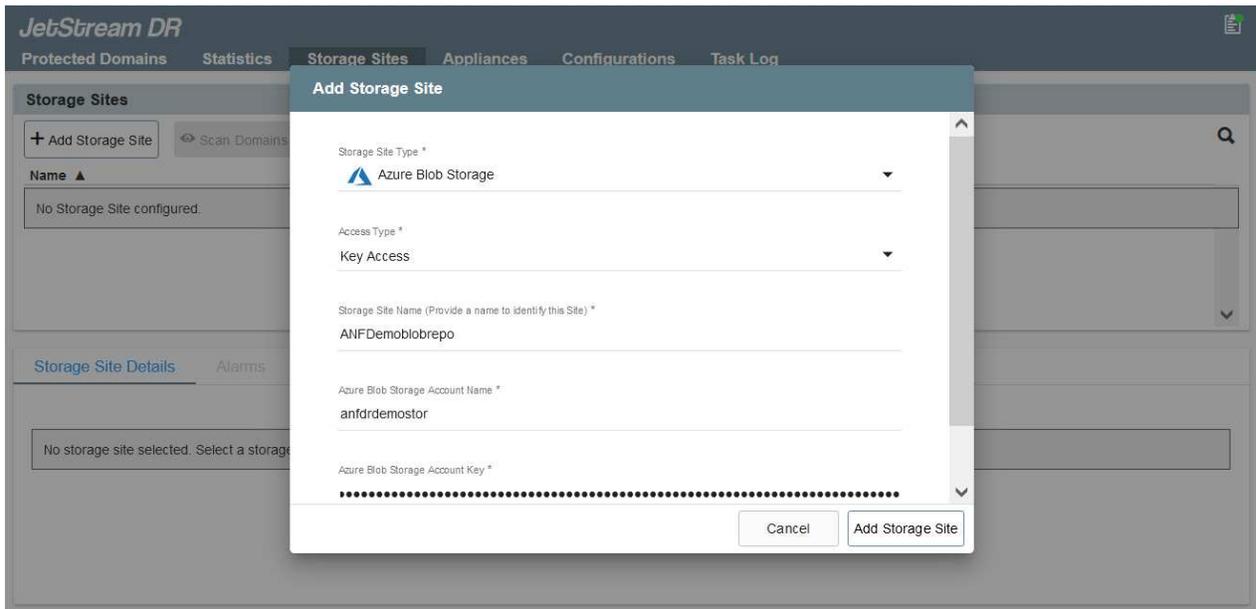
1. 前提条件を確認する。
2. キャパシティプランニングツールを実行して、リソースと構成に関する推奨事項を確認します（オプションですが、コンセプトの実証の試用には推奨されます）。
3. JetStream DR MSAを指定されたクラスタ内のvSphereホストに展開します。
4. ブラウザでDNS名を使用してMSAを起動します。
5. vCenterサーバをMSAに登録します。インストールを実行するには、次の手順を実行します。
6. JetStream DR MSAが導入され、vCenter Serverが登録されたら、vSphere Web Clientを使用してJetStream DRプラグインにアクセスします。これを行うには、[データセンター]>[設定]>[JetStream DR]に移動します。



7. JetStream DRインターフェースから、適切なクラスタを選択します。



8. I/Oフィルタパッケージを使用してクラスタを設定します。

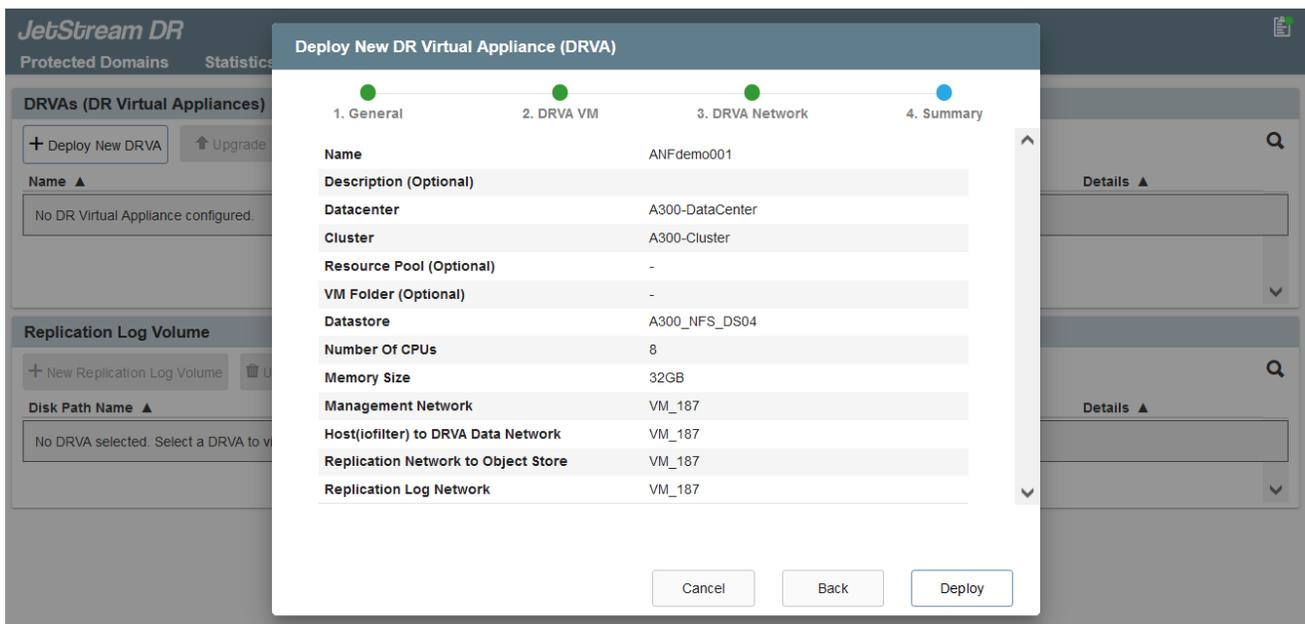


9. リカバリサイトにAzure Blob Storageを追加します。
10. アプライアンスタブからDR仮想アプライアンス (DRVA) を導入します。



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サイクルを手動で設定して実行することをお勧めします (Start protection > failover > failback)。

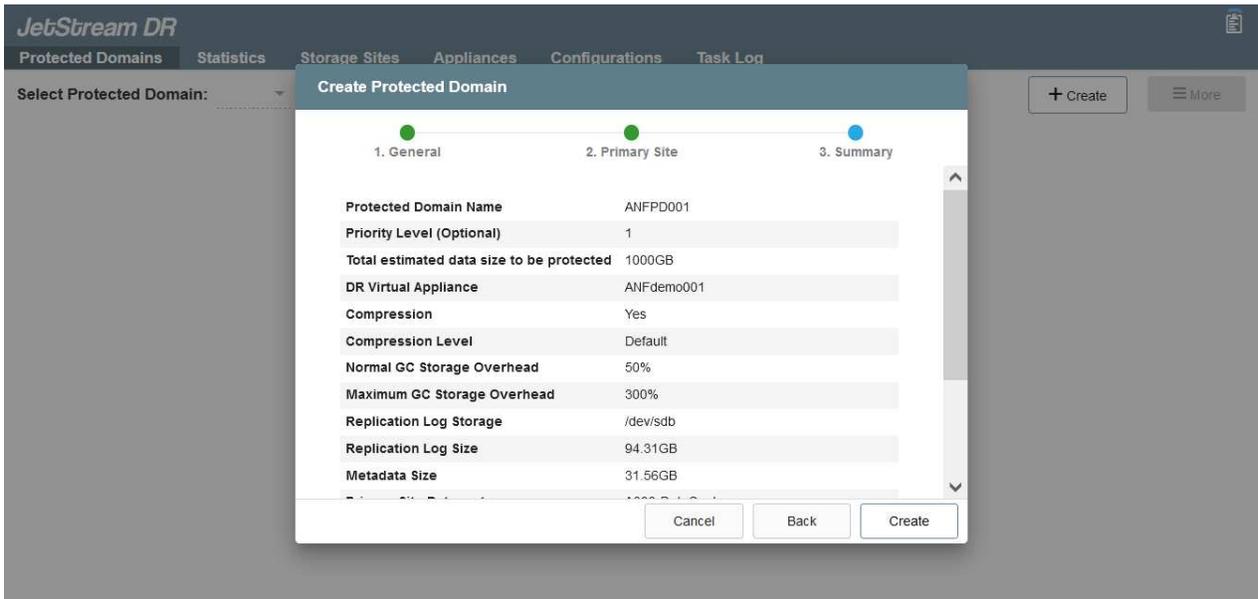
JetStream DRVAは、データ複製プロセスの主要な機能を容易にする仮想アプライアンスです。保護されたクラスタには少なくとも1つのDRVAが含まれている必要があります。通常は、ホストごとに1つのDRVAが構成されます。各DRVAは、複数の保護ドメインを管理できます。



この例では、4台のDRVAが80台の仮想マシン用に作成されています。

1. 使用可能なデータストアまたは独立した共有iSCSIストレージプールからVMDKを使用して、各DRVAのレプリケーションログボリュームを作成します。

- Protected Domainsタブで、Azure Blob Storageサイト、DRVAインスタンス、およびレプリケーションログに関する情報を使用して、必要な数の保護ドメインを作成します。保護ドメインは、クラスター内の特定のVMまたはVMのセットを定義します。これらのVMは一緒に保護され、フェイルオーバー/フェイルバック処理の優先順位が割り当てられます。



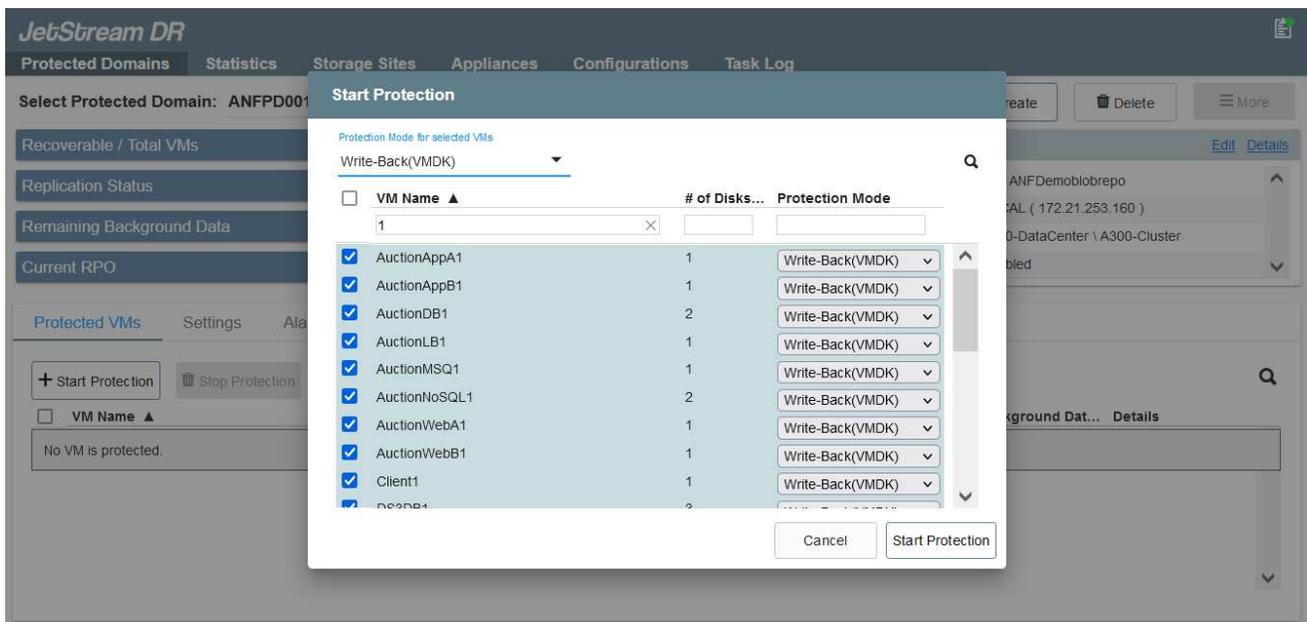
- 保護するVMを選択し、保護ドメインのVM保護を開始します。これにより、指定したBlob Storeへのデータレプリケーションが開始されます。



保護ドメイン内のすべてのVMに同じ保護モードが使用されていることを確認します。



ライトバック (VMDK) モードを使用すると、パフォーマンスが向上します。



レプリケーションログボリュームがハイパフォーマンスストレージに配置されていることを確認します。



フェイルオーバー実行ブックは、VM（回復グループ）のグループ化、起動順序の設定、およびCPU/メモリの設定とIP設定の変更を行うように構成できます。

Runコマンドを使用して、**Azure VMware**解決策 プライベートクラウドに**JetStream DR for AVS**をインストールします

リカバリサイト（AVS）では、3ノードのパイロットライトクラスタを事前に作成することを推奨します。これにより、次の項目を含むリカバリサイトのインフラを事前に設定できます。

- 宛先ネットワークセグメント、ファイアウォール、DHCPやDNSなどのサービスなど。
- AVS対応のJetStream DRのインストール
- ANFボリュームをデータストアとして構成し、moreJetStream DRではミッションクリティカルなドメインのRTOモードをほぼゼロに設定できます。これらのドメインには、デスティネーションストレージが事前にインストールされている必要があります。この場合、ANFは推奨ストレージタイプです。



セグメント作成を含むネットワーク構成は、オンプレミスの要件に合わせてAVSクラスタ上で設定する必要があります。

SLAやRTOの要件に応じて、継続的なフェイルオーバーモードや通常の（標準）フェイルオーバーモードを使用できます。RTOがほぼゼロの場合は、リカバリサイトで継続的なリハイドレートを開始する必要があります。

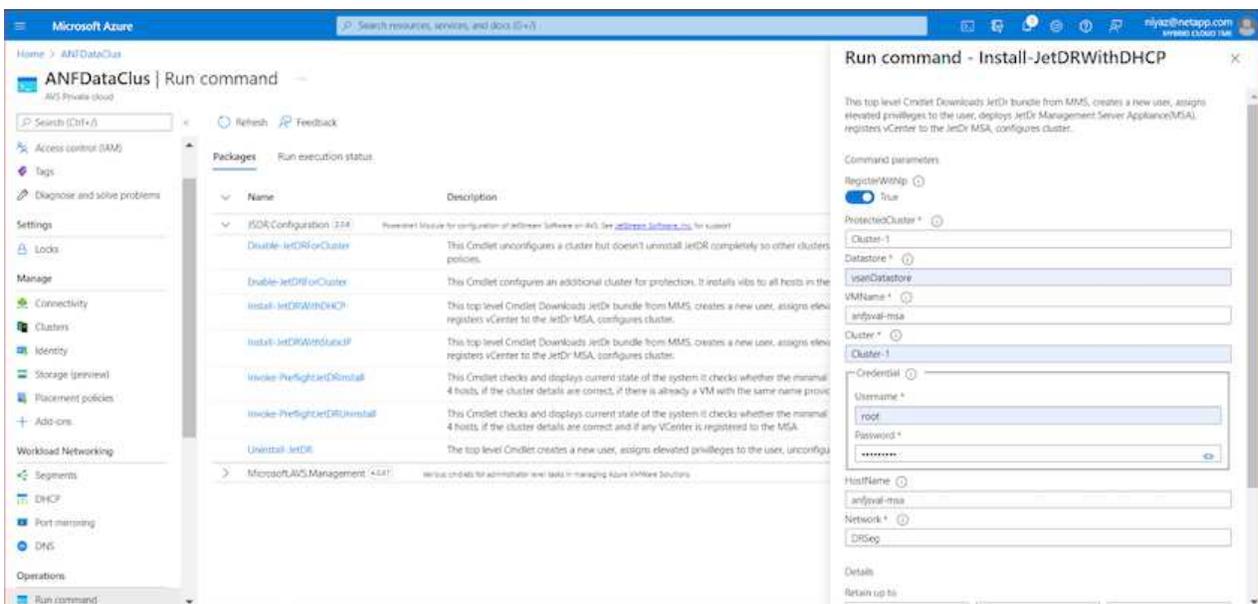
Azure VMware解決策 プライベートクラウドにJetStream DR for AVSをインストールするには、次の手順を実行します。

1. AzureポータルからAzure VMware解決策 に移動し、プライベートクラウドを選択して、実行コマンド>パッケージ> JSDR.Configurationを選択します。



Azure VMware解決策 のデフォルトCloudAdminユーザには、AVS対応のJetStream DRをインストールするための十分な権限がありません。Azure VMware解決策 では、JetStream DR用のAzure VMware解決策 実行コマンドを呼び出すことで、JetStream DRを簡単かつ自動でインストールできます。

次のスクリーンショットは、DHCPベースのIPアドレスを使用したインストール方法を示しています。



2. JetStream DR for AVSのインストールが完了したら、ブラウザをリフレッシュします。JetStream DR UIにアクセスするには、SDDC Datacenter > Configure > JetStream DRに移動します。

The screenshot shows the JetStream DR interface with the 'Configurations' tab selected. The 'Site Details' section includes the following information:

- vCenter Server Hostname: 172.30.156.2
- Management Appliance Hostname: anjfsval-msa
- Software Version: 4.0.2.450
- Subscription ID: - [Configure](#)
- Tenant ID / Application ID: - [Configure](#)
- Application Secret: - [Configure](#)

Below the details are several action buttons: 'Configure Cluster', 'Upgrade', 'Unconfigure', and 'Resolve Configure Issue'. A table below shows the following cluster details:

<input type="checkbox"/>	Cluster Name ▲	Datacenter Name ▲	Status ▲	Software Version ▲	Host Details ▲
<input type="checkbox"/>	Cluster-1	SDDC-Datacenter	Ok	4.0.2.132	<a href="#">Details</a>

3. JetStream DRインターフェイスから、オンプレミスクラスタをストレージサイトとして保護するために使用したAzure Blob Storageアカウントを追加し、Scan Domainsオプションを実行します。

The screenshot shows a dialog box titled 'Available Protected Domain(s) For Import' overlaid on the JetStream DR interface. The dialog contains a table with the following data:

Protected Domain ...	Description	Recoverable V...	VMs ...	Import
ANFPD000	Protected Domain Tile0	20	20	<a href="#">Import</a>
ANFPD001	-	20	20	<a href="#">Import</a>
ANFPD002	Protected Domain 02	20	20	<a href="#">Import</a>
ANFPD003	Protected Domain Tile 03	20	20	<a href="#">Import</a>

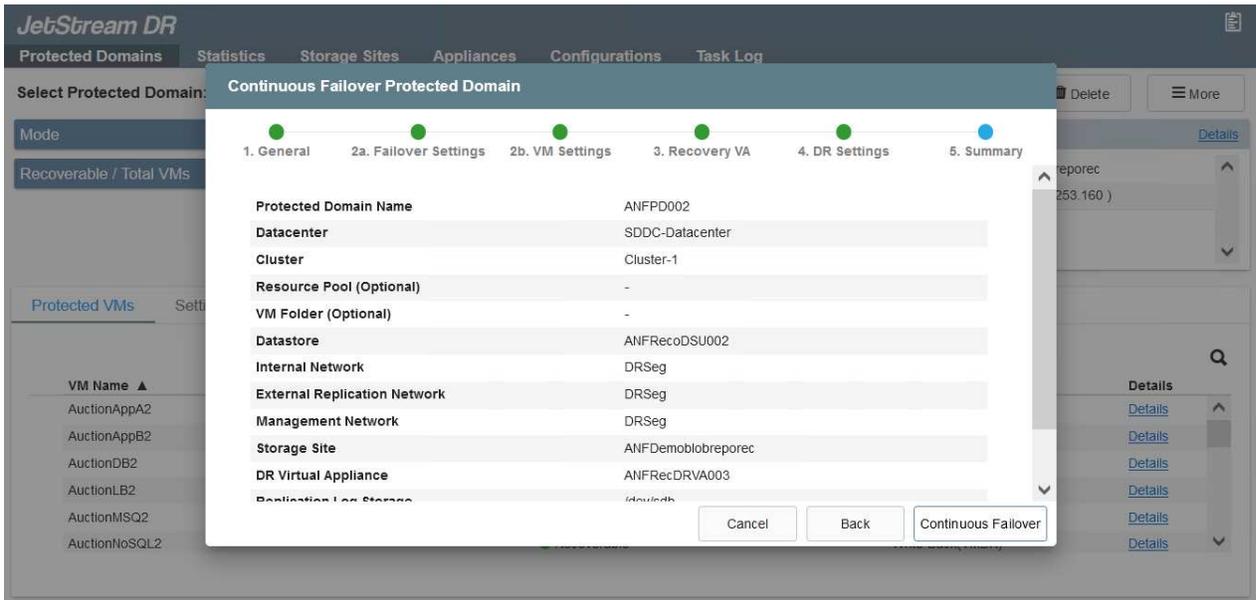
The dialog also features a 'Close' button at the bottom right.

4. 保護ドメインをインポートしたら、DRVAアプライアンスを展開します。この例では、JetStream DR UIを使用して、リカバリサイトから継続的なリハイドレートを手動で開始します。



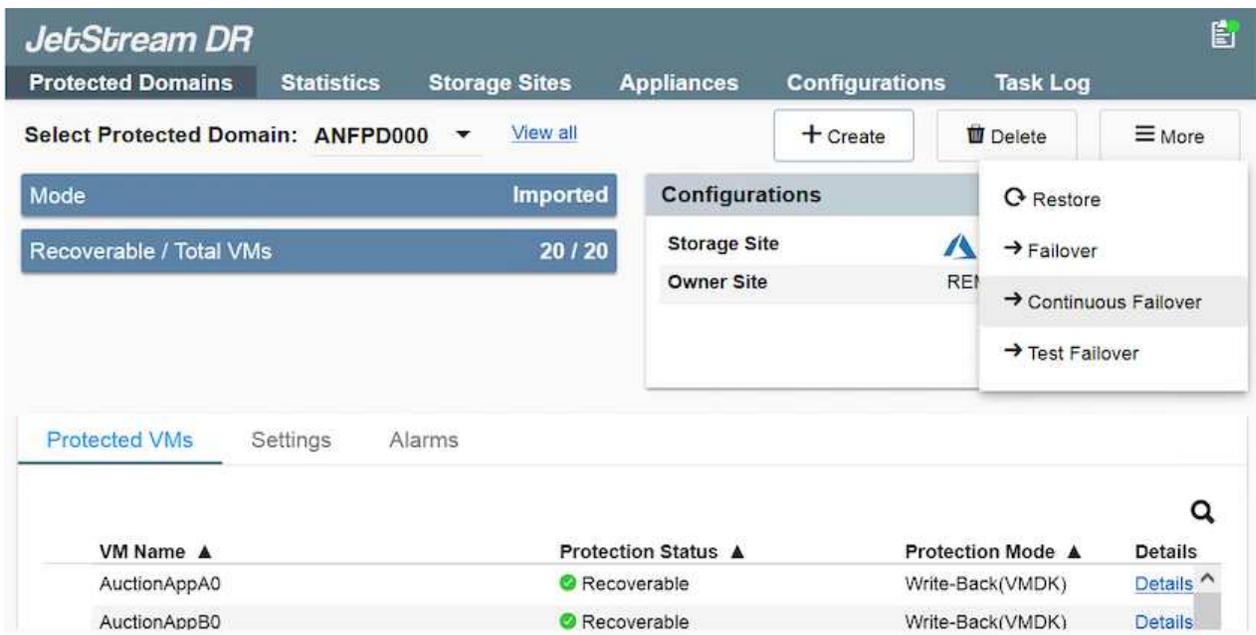
これらの手順は、CPT作成計画を使用して自動化することもできます。

5. 使用可能なvSANまたはANFデータストアを使用してレプリケーションログボリュームを作成します。
6. 保護ドメインをインポートし、VMの配置にANFデータストアを使用するようにリカバリVAを設定します。



選択したセグメントでDHCPが有効になっていて、十分なIPが使用可能であることを確認します。ダイナミックIPは、ドメインのリカバリ中に一時的に使用されます。リカバリVM（連続リハイドレートを含む）ごとに、個別のダイナミックIPが必要です。リカバリの完了後、IPは解放され、再利用できます。

- 適切なフェイルオーバーオプション（継続的フェイルオーバーまたはフェイルオーバー）を選択します。この例では、連続リハイドレート（連続フェイルオーバー）が選択されています。



フェイルオーバー/フェイルバックを実行しています

## フェールオーバー/フェールバックの実行方法

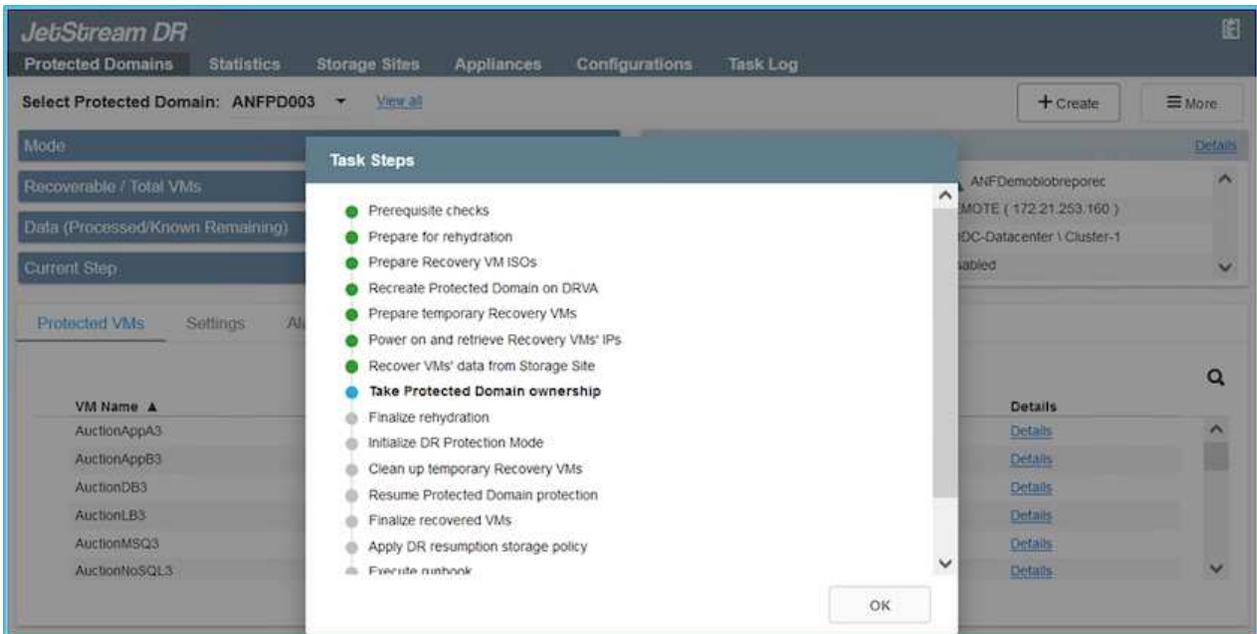
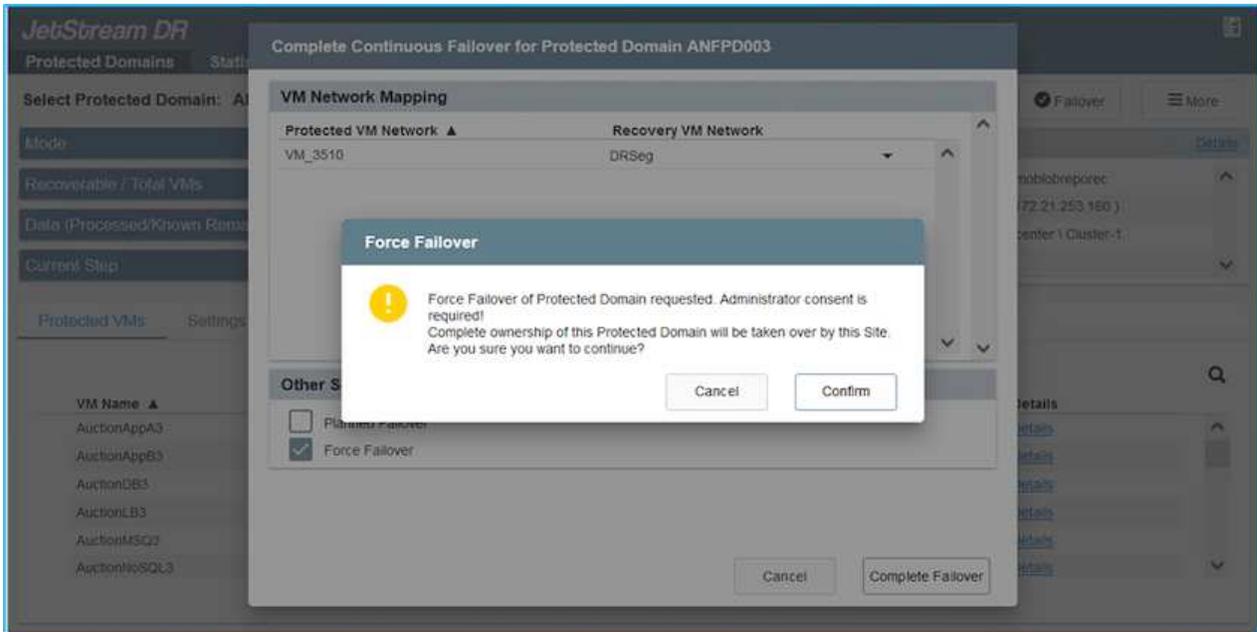
1. オンプレミス環境の保護対象クラスタで障害が発生した場合（部分的または完全な障害）、フェールオーバーをトリガーします。



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クラスタリカバリサイトにVMをリカバリできます。

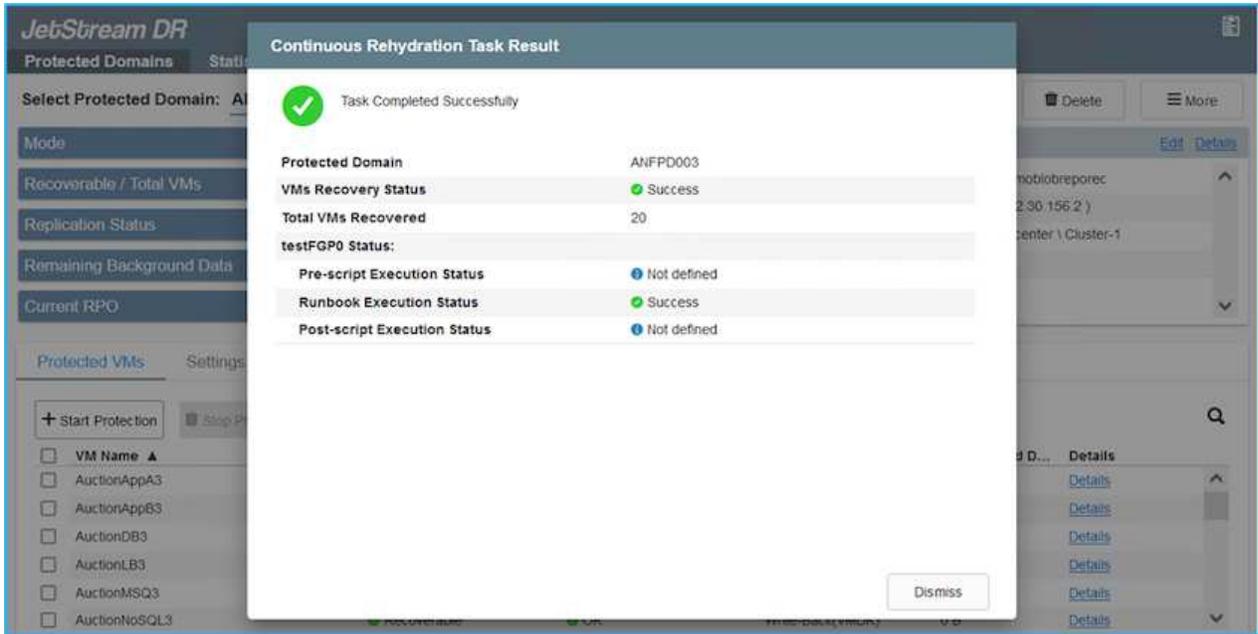


保護対象のVMがAVSで起動されると、フェールオーバー後（継続的または標準的なりハイドレート）、保護は自動的に再開され、JetStream DRは、Azure Blob Storage内の適切なコンテナまたは元のコンテナにデータをレプリケートし続けます。



タスクバーにフェ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. タスクが完了すると、リカバリされたVMとビジネスに通常どおりアクセスできます。



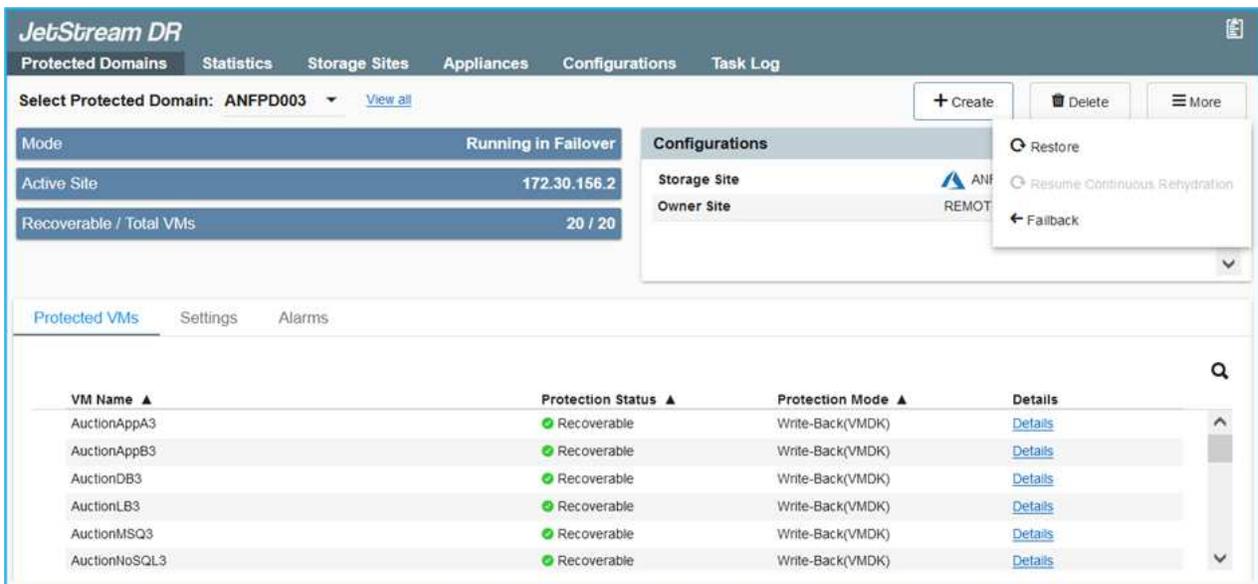
プライマリサイトが起動して再び実行されるようになったら、フェイルバックを実行できます。VM保護が再開され、データの整合性を確認する必要があります。

3. オンプレミス環境をリストア災害のタイプによっては、保護対象クラスタの構成をリストアまたは検証しなければならない場合があります。必要に応じて、JetStream DRソフトウェアを再インストールする必要があります。



注：Automation Toolkitで提供されている「recovery\_utility\_prepare\_failback」スクリプトを使用すると、古いVMやドメイン情報などの元の保護サイトをクリーンアップできます。

4. リストアされたオンプレミス環境にアクセスし、Jetstream DR UIに移動して、適切な保護ドメインを選択します。保護サイトがフェイルバックできる状態になったら、UIで[Failback]オプションを選択します。





CPTで生成されたフェイルバックプランを使用して、VMとそのデータをオブジェクトストアから元のVMware環境に戻すこともできます。



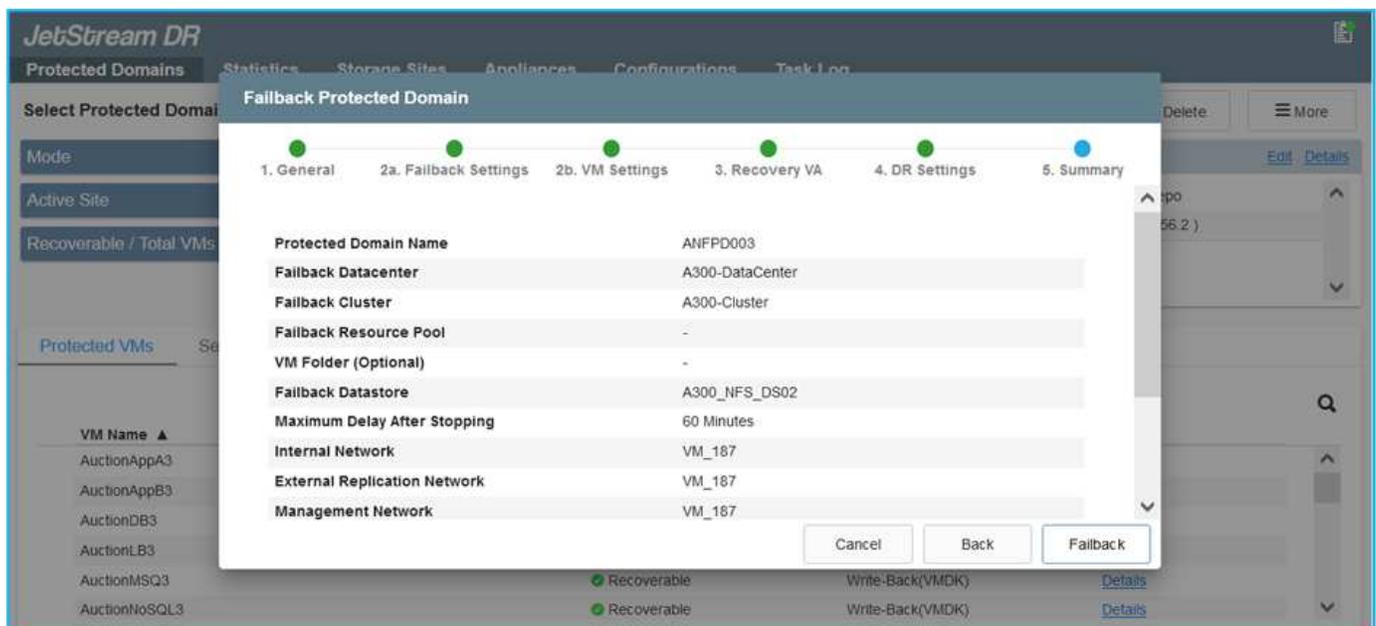
リカバリサイトのVMを一時停止して保護対象サイトで再起動したあとの最大遅延時間を指定します。この時間には、フェイルオーバーVMを停止したあとのレプリケーションの完了、リカバリサイトのクリーンアップにかかる時間、保護サイトでVMを再作成する時間などが含まれます。ネットアップの推奨値は10分です。

フェイルバックプロセスを完了し、VM保護およびデータの整合性が再開されたことを確認する。

## Ransomware回復

ランサムウェアからのリカバリは困難な作業です。具体的には、IT組織にとって、返品 of 安全ポイントを特定することは困難です。また、復旧したワークロードを、（睡眠中のマルウェアや脆弱なアプリケーションによって）再発する攻撃から確実に保護する方法が決定された場合もあります。

Jetstream DR for AVSとAzure NetApp Files データストアを併用すると、組織が使用可能なポイントインタイムからリカバリできるため、ワークロードが機能的な分離されたネットワークに必要な応じてリカバリされるため、これらの問題に対処できます。リカバリを使用すると、アプリケーションが相互に機能して通信できるようになり、南北のトラフィックにさらされることがなくなります。その結果、セキュリティチームはフォレンジックなどの必要な修復を安全に実行できます。



## CVOとAVS（ゲスト接続ストレージ）によるディザスタリカバリ

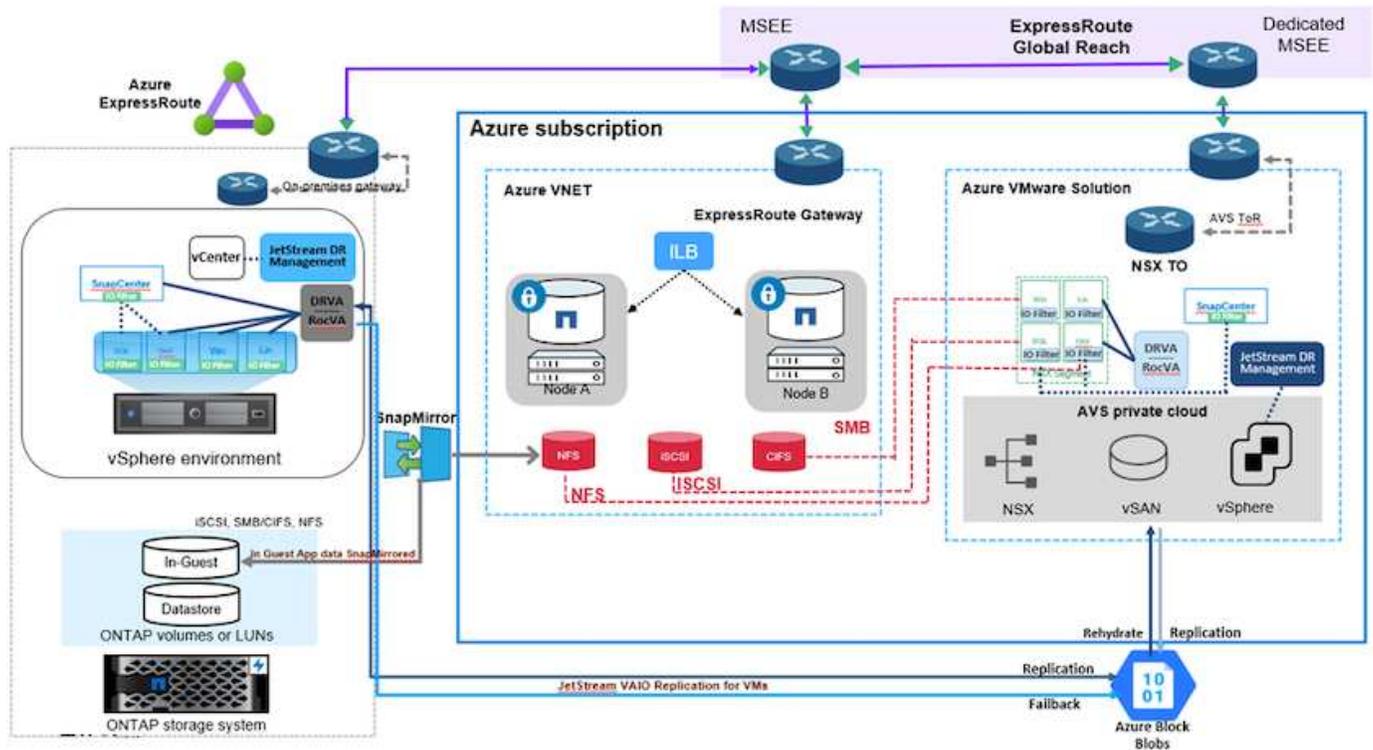
クラウドへのディザスタリカバリは、耐障害性と対費用効果に優れた方法で、サイトの停止やランサムウェアなどのデータ破損からワークロードを保護します。NetApp SnapMirrorを使用すると、ゲスト接続ストレージを使用するオンプレミスのVMwareワークロードを、Azure内で実行されているNetApp Cloud Volumes ONTAP にレプリケートできます。

## 概要

著者：Ravi BCBとNiyaz Mohamedネットアップ

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.

本ドキュメントでは、NetApp SnapMirror、JetStream、およびAzure VMware解決策（AVS）を使用してディザスタリカバリを設定および実行するためのステップバイステップ形式のアプローチを紹介します。



## 前提条件

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



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

オンプレミス環境とAzure Virtual Network間の接続には、エクスプレスルートグローバルリーチまたはVPNゲートウェイを使用した仮想WANを使用します。オンプレミスVLANの設計に基づいてセグメントを作成する必

があります。



オンプレミスのデータセンターをAzureに接続する方法は複数ありますが、これにより、本ドキュメントの特定のワークフローの概要がわかりません。適切なオンプレミスからAzureへの接続方法については、Azureのドキュメントを参照してください。

## DR解決策 の導入

### 解決策 の導入の概要

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

### 展開の詳細

#### AzureでCVOを構成し、ボリュームをCVOにレプリケート

まず、AzureでCloud Volumes ONTAPを設定します ("[リンク](#)") をクリックし、必要なボリュームを、必要な頻度とSnapshotの保持を使用してCloud Volumes ONTAP にレプリケートします。

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
✓	gcsdrsqlhd_sc46_copy ANFCVODRDemo	gcsdrsqlhd_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データアクセスを設定

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

AVSクラスタを導入するかどうかは、主にRPOとRTOの要件に基づきます。Azure VMware解決策では、テストや実際の災害に備えて、SDDCを随時プロビジョニングできます。SDDCを時間内に導入することで、災害に対処しない場合のESXiホストのコストを削減できます。ただし、このような導入形態では、SDDCのプロビジョニングに数時間かかるRTOが影響を受けます。

最も一般的な導入オプションは、SDDCを常時稼働のパイロットライトモードで実行することです。このオプションを使用すると、常に使用可能なホストを3台分のスペースに縮小できます。また、シミュレーションアクティビティとコンプライアンスチェックのベースラインを実行できるため、本番サイトとDRサイト間の運用のずれを回避できるため、リカバリ処理の時間を短縮できます。パイロットライトクラスタは、実際のDRイベントを処理する必要がある場合に、必要なレベルまで迅速に拡張できます。

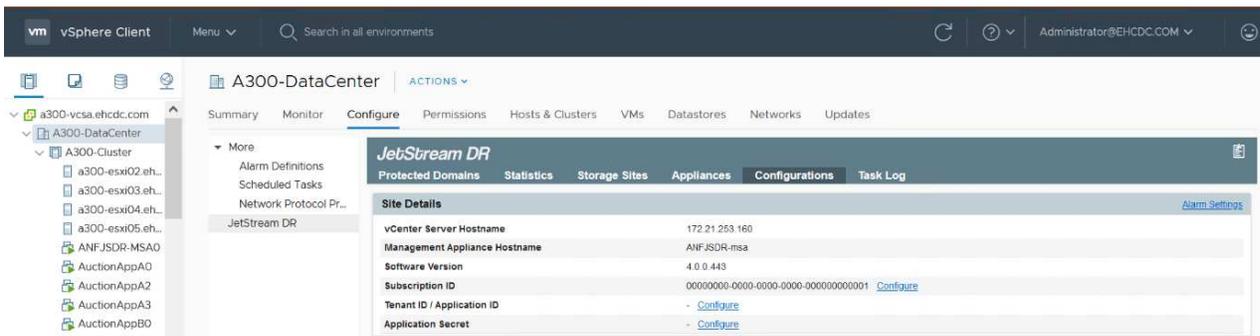
AVS SDDCを設定するには（オンデマンドモードまたはパイロットライトモード）、を参照してください ["Azure に仮想化環境を導入して設定"](#)。事前に、接続の確立後、AVSホストに常駐するゲストVMがCloud Volumes ONTAP からデータを消費できることを確認してください。

Cloud Volumes ONTAP とAVSを適切に設定したら、VAIOメカニズムを使用し、Cloud Volumes ONTAP へのアプリケーションボリュームのコピーにSnapMirrorを利用することにより、オンプレミスワークロードからAVSへのリカバリ（アプリケーションVMDKとゲストストレージを搭載したVM）を自動化するようにJetstreamを設定します。

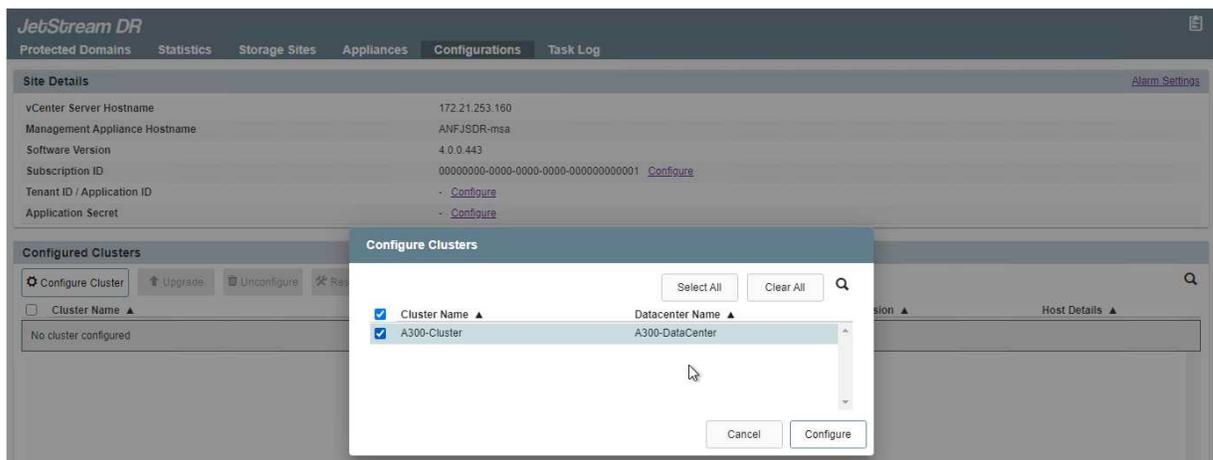
## JetStream DRをオンプレミスデータセンターにインストールします

Jetstream DRソフトウェアは、JetStream DR Management Server Virtual Appliance (MSA) 、DR Virtual Appliance (DRVA) 、およびホストコンポーネント (I/Oフィルタパッケージ) の3つの主要コンポーネントで構成されています。MSAは、コンピューティングクラスタにホストコンポーネントをインストールおよび構成し、JetStream DRソフトウェアを管理するために使用されます。インストールプロセスは次のとおりです。

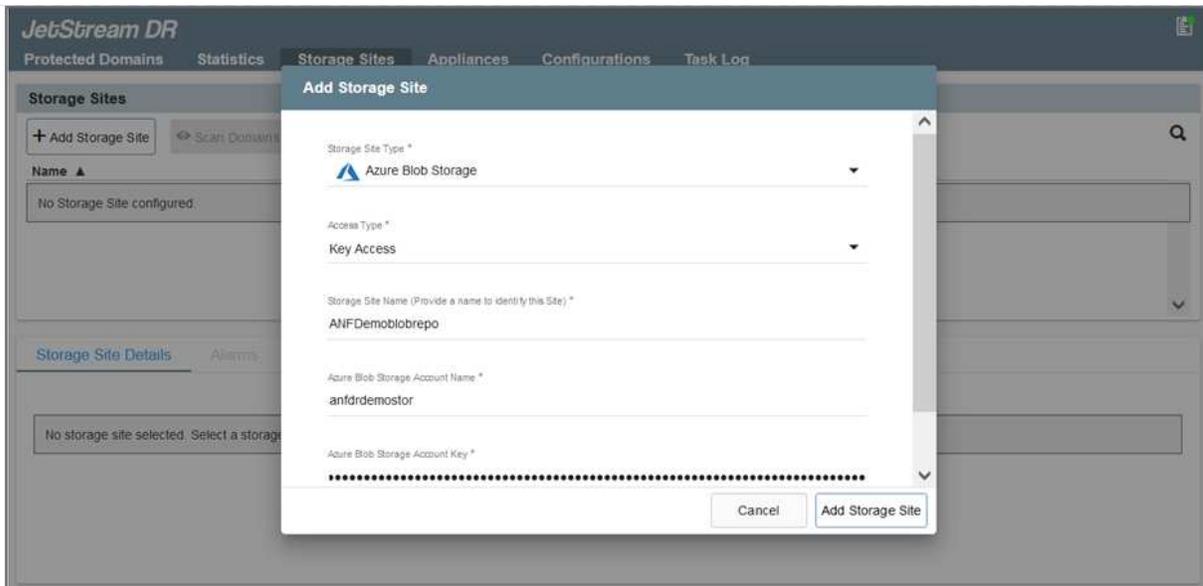
1. 前提条件を確認します。
2. リソースと構成に関する推奨事項については、Capacity Planning Toolを実行してください。
3. JetStream DR MSAを、指定されたクラスタ内の各vSphereホストに導入します。
4. ブラウザでDNS名を使用してMSAを起動します。
5. vCenterサーバをMSAに登録します。
6. JetStream DR MSAが導入され、vCenter Serverが登録されたら、vSphere Web ClientでJetStream DRプラグインに移動します。これを行うには、[データセンター]>[設定]>[JetStream DR]に移動します。



7. JetStream DRインターフェイスから、次の作業を行います。
  - a. I/Oフィルタパッケージを使用してクラスタを設定します。



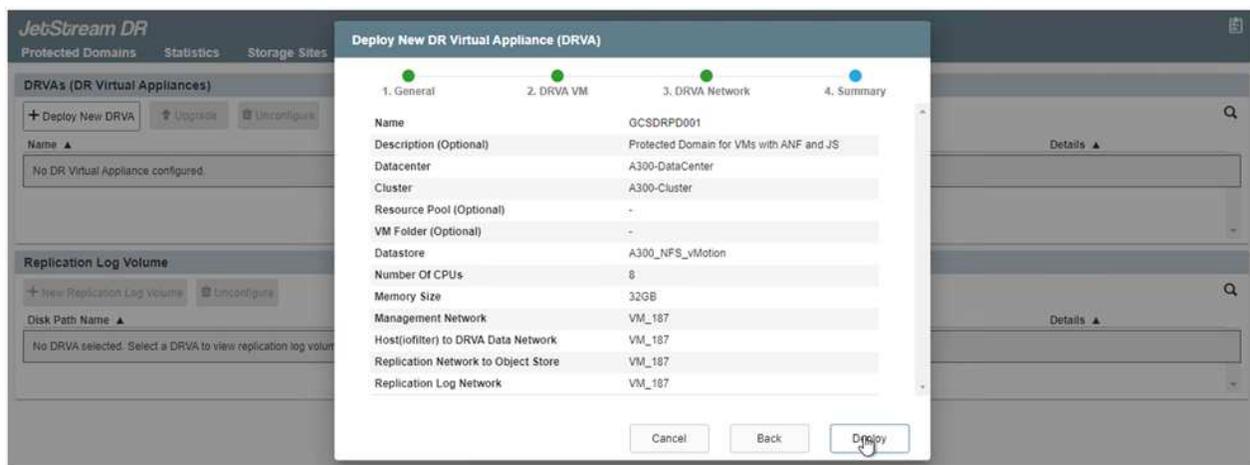
- b. リカバリサイトにあるAzure BLOBストレージを追加します。



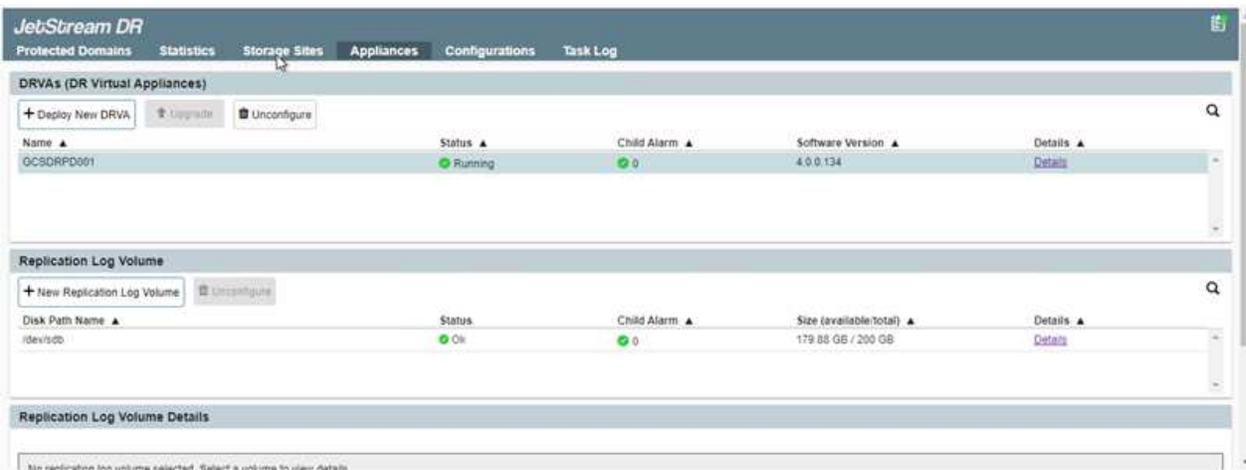
8. アプライアンスタブから必要な数のDR仮想アプライアンス（DRVA）を導入します。



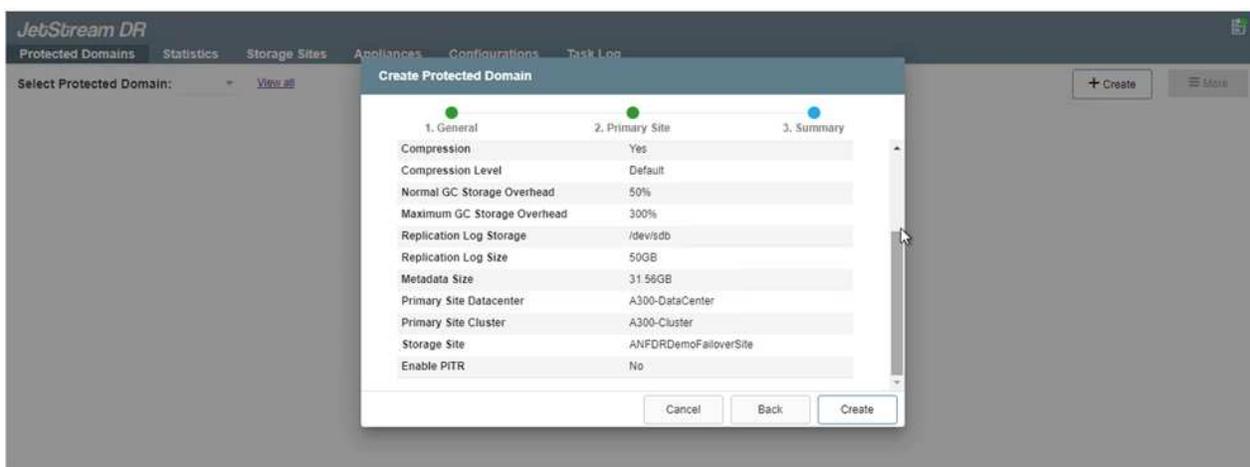
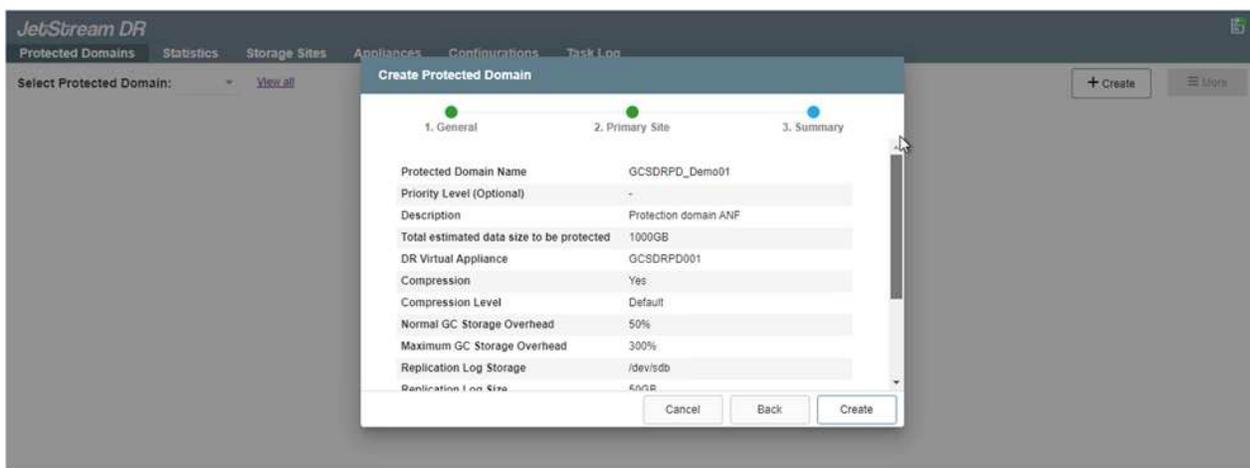
キャパシティプランニングツールを使用して、必要なDRVAの数を見積もります。



9. 使用可能なデータストアまたは独立した共有iSCSIストレージプールからVMDKを使用して、各DRVAのレプリケーションログボリュームを作成します。



10. Protected Domainsタブで、Azure Blob Storageサイト、DRVAインスタンス、およびレプリケーションログに関する情報を使用して、必要な数の保護ドメインを作成します。保護ドメインは、クラスタ内の特定のVMまたはアプリケーションVMのセットを定義します。これらのVMは一緒に保護され、フェイルオーバー/フェイルバック処理の優先順位が割り当てられます。



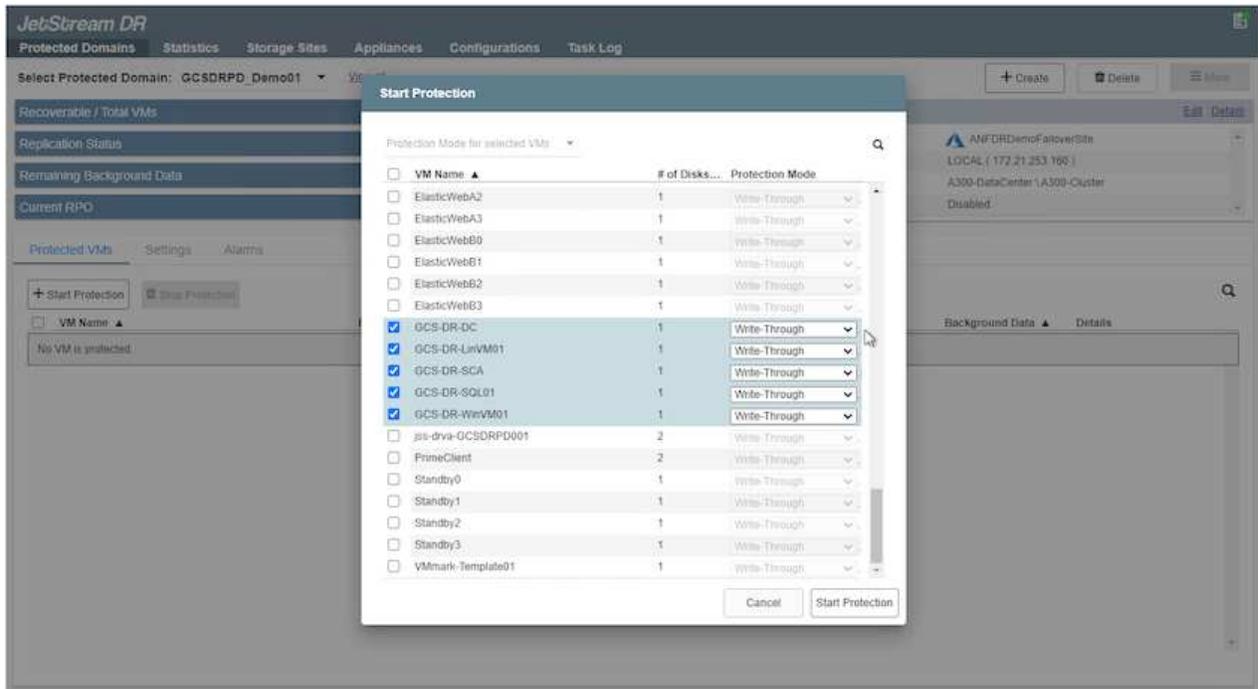
11. 保護するVMを選択し、依存関係に基づいてVMをアプリケーショングループにグループ化します。アプリケーション定義を使用すると、VMのセットを、ブート順序、ブート遅延、およびリカバリ時に実行可能なオプションのアプリケーション検証を含む論理グループにグループ化できます。



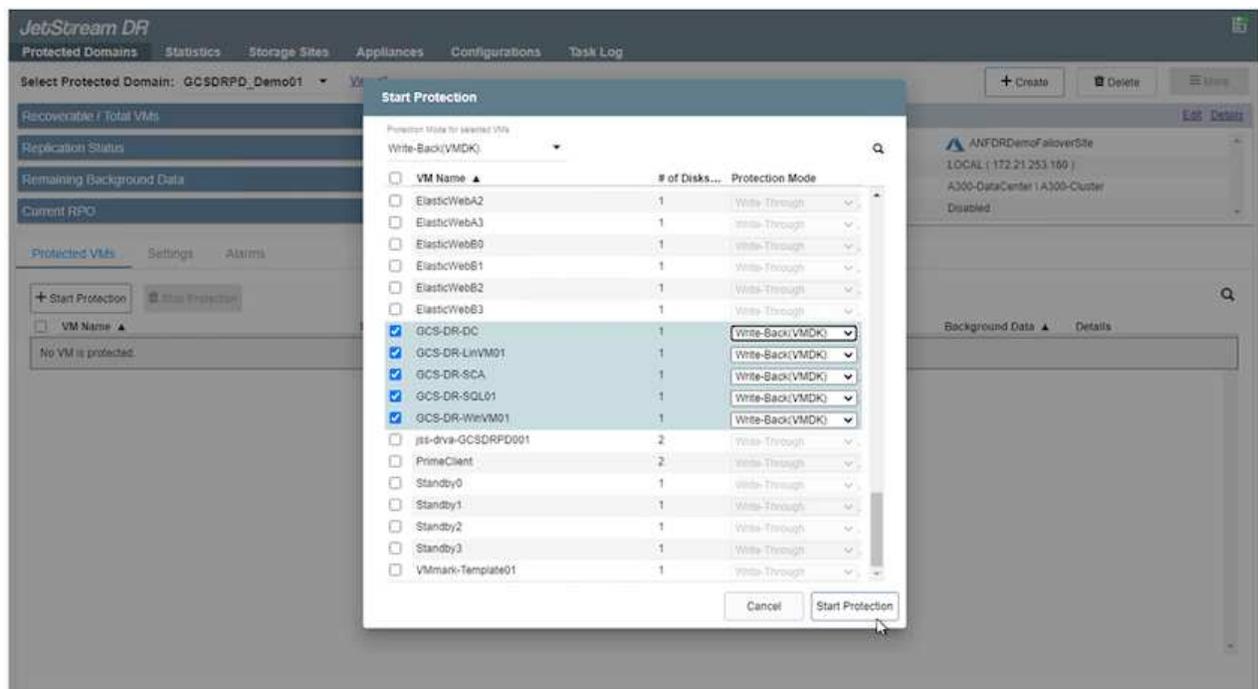
保護ドメイン内のすべてのVMに同じ保護モードを使用していることを確認します。



ライトバック (VMDK) モードを使用すると、パフォーマンスが向上します。



- レプリケーションログボリュームがハイパフォーマンスストレージに配置されていることを確認します。



- 完了したら、保護ドメインの保護の開始をクリックします。選択したVMのデータレプリケーションが開始され、指定したBLOBストアに送信されます。

JetStream DR  
Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: GCSDRPD\_Demo01 [View all](#)

Recoverable / Total VMs: 0 / 5  
Replication Status: OK  
Remaining Background Data: 0 B  
Current RPO: -

Configurations  
Storage Site: ANFDRD  
Owner Site: LOCAL ( 172.2  
Datacenter | Cluster: A300-DataCen  
Point-in-time Recovery: Disabled

Running Tasks  
Start Protection (GCS-DR-SCA) 50%  
Start Protection (GCS-DR-Win... 50%  
Start Protection (GCS-DR-Lin... 50%  
Start Protection (GCS-DR-DC) 50%  
Start Protection (GCS-DR-SQ... 50%  
Configure VMDK Re... Completed  
Close

Protected VMs | Settings | Alarms

+ Start Protection | Stop Protection

VM Name	Protection Status	Replication Status	Protection Mode	Background Data	Details
GCS-DR-DC	Initializing	-	Write-Back(VMDK)	-	Details
GCS-DR-LinVM01	Initializing	-	Write-Back(VMDK)	-	Details
GCS-DR-SCA	Initializing	-	Write-Back(VMDK)	-	Details
GCS-DR-SQL01	Initializing	-	Write-Back(VMDK)	-	Details
GCS-DR-WinVM01	Initializing	-	Write-Back(VMDK)	-	Details

14. レプリケーションが完了すると、VMの保護ステータスは「回復可能」とマークされます。

JetStream DR  
Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: GCSDRPD\_Demo01 [View all](#)

Recoverable / Total VMs: 5 / 5  
Replication Status: OK  
Remaining Background Data: 0 B  
Current RPO: 0s

Configurations  
Storage Site: ANFDRDemoFailoverSite  
Owner Site: LOCAL ( 172.21.253.160 )  
Datacenter | Cluster: A300-DataCenter | A300-Cluster  
Point-in-time Recovery: Disabled

Protected VMs | Settings | Alarms

+ Start Protection | Stop Protection

VM Name	Protection Status	Replication Status	Protection Mode	Background Data	Details
GCS-DR-DC	Recoverable	OK	Write-Back(VMDK)	0 B	Details
GCS-DR-LinVM01	Recoverable	OK	Write-Back(VMDK)	0 B	Details
GCS-DR-SCA	Recoverable	OK	Write-Back(VMDK)	0 B	Details
GCS-DR-SQL01	Recoverable	OK	Write-Back(VMDK)	0 B	Details
GCS-DR-WinVM01	Recoverable	OK	Write-Back(VMDK)	0 B	Details



フェールオーバーランブックは、VM（回復グループと呼ばれる）をグループ化し、起動順序シーケンスを設定して、CPU / メモリ設定とIP設定を変更するように構成できます。

15. 「設定」をクリックし、「Runbook設定」リンクをクリックして、Runbookグループを設定します。

JetStream DR  
Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: GCSDRPD\_Demo01 [View all](#)

Recoverable / Total VMs: 5 / 5  
Replication Status: OK  
Remaining Background Data: 0 B  
Current RPO: 0s

Configurations  
Storage Site: ANFDRDemoFailoverSite  
Owner Site: LOCAL ( 172.21.253.160 )  
Datacenter | Cluster: A300-DataCenter | A300-Cluster  
Point-in-time Recovery: Disabled

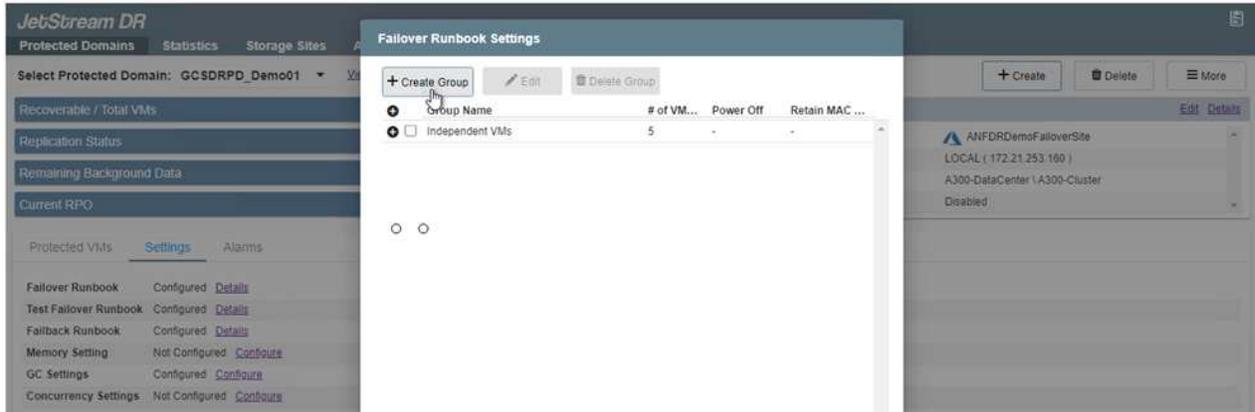
Protected VMs | Settings | Alarms

Failover Runbook: Not Configured [Configure](#)  
Test Failover Runbook: Not Configured [Configure](#)  
Fallback Runbook: Not Configured [Configure](#)  
Memory Setting: Not Configured [Configure](#)  
GC Settings: Configured [Configure](#)  
Concurrency Settings: Not Configured [Configure](#)

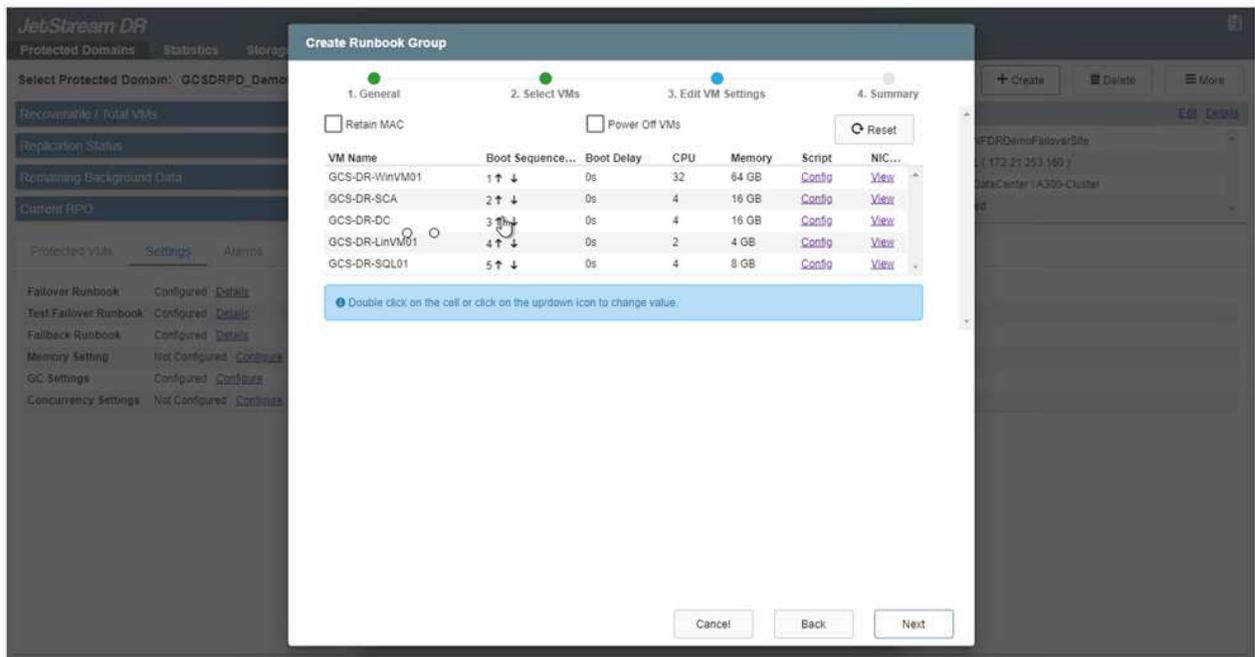
16. [グループの作成]ボタンをクリックして、新しいランブックグループの作成を開始します。



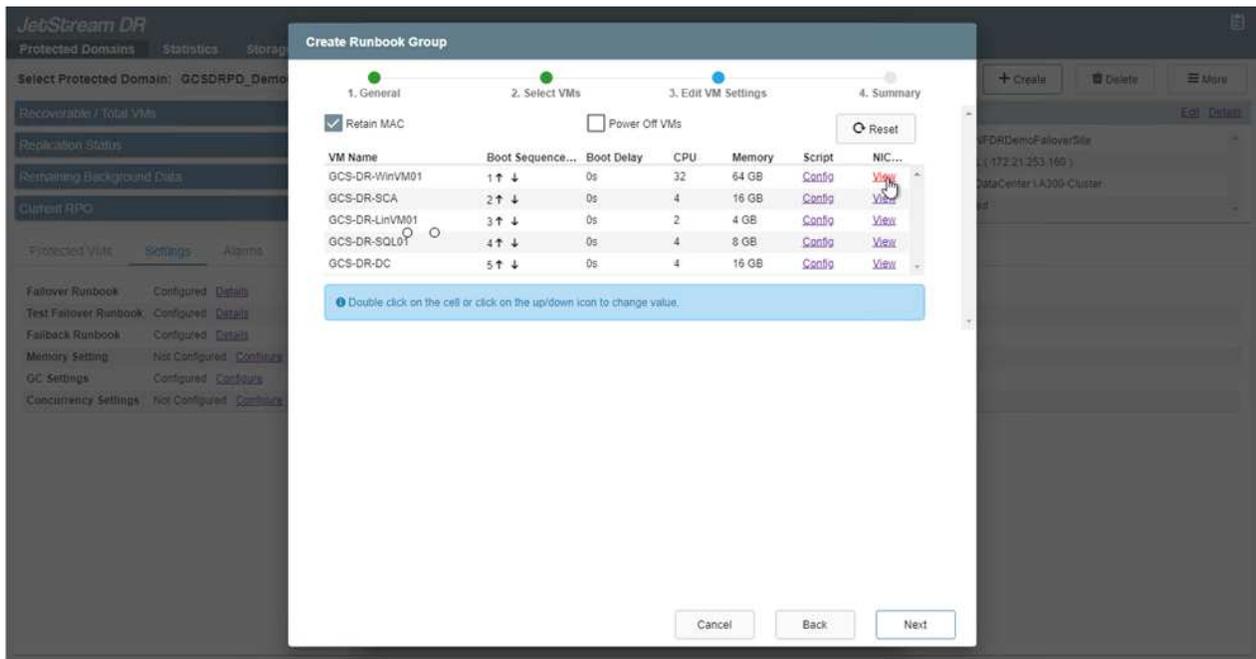
必要に応じて、画面の下部で、カスタムのプレスクリプトとポストスクリプトを適用して、ランブックグループの操作前および操作後に自動的に実行します。Runbookスクリプトが管理サーバ上に存在することを確認します。



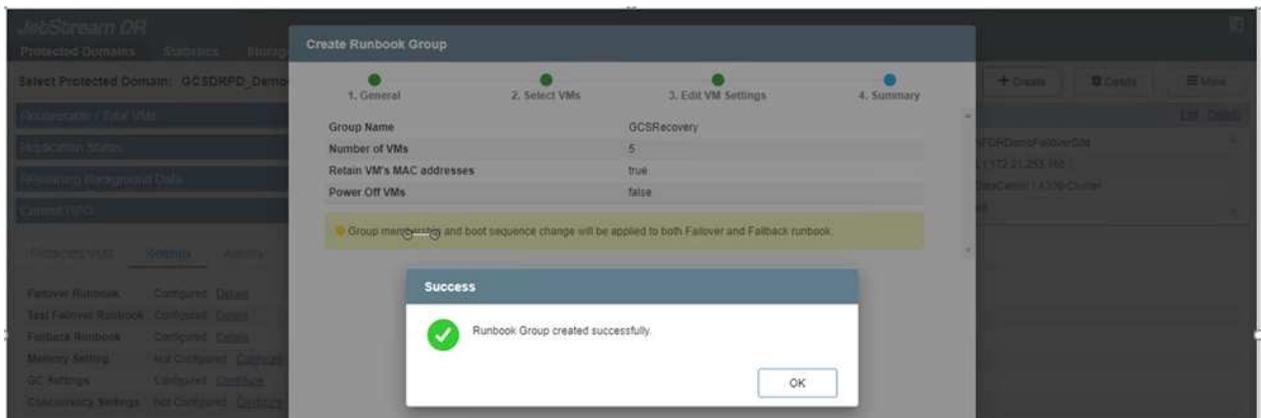
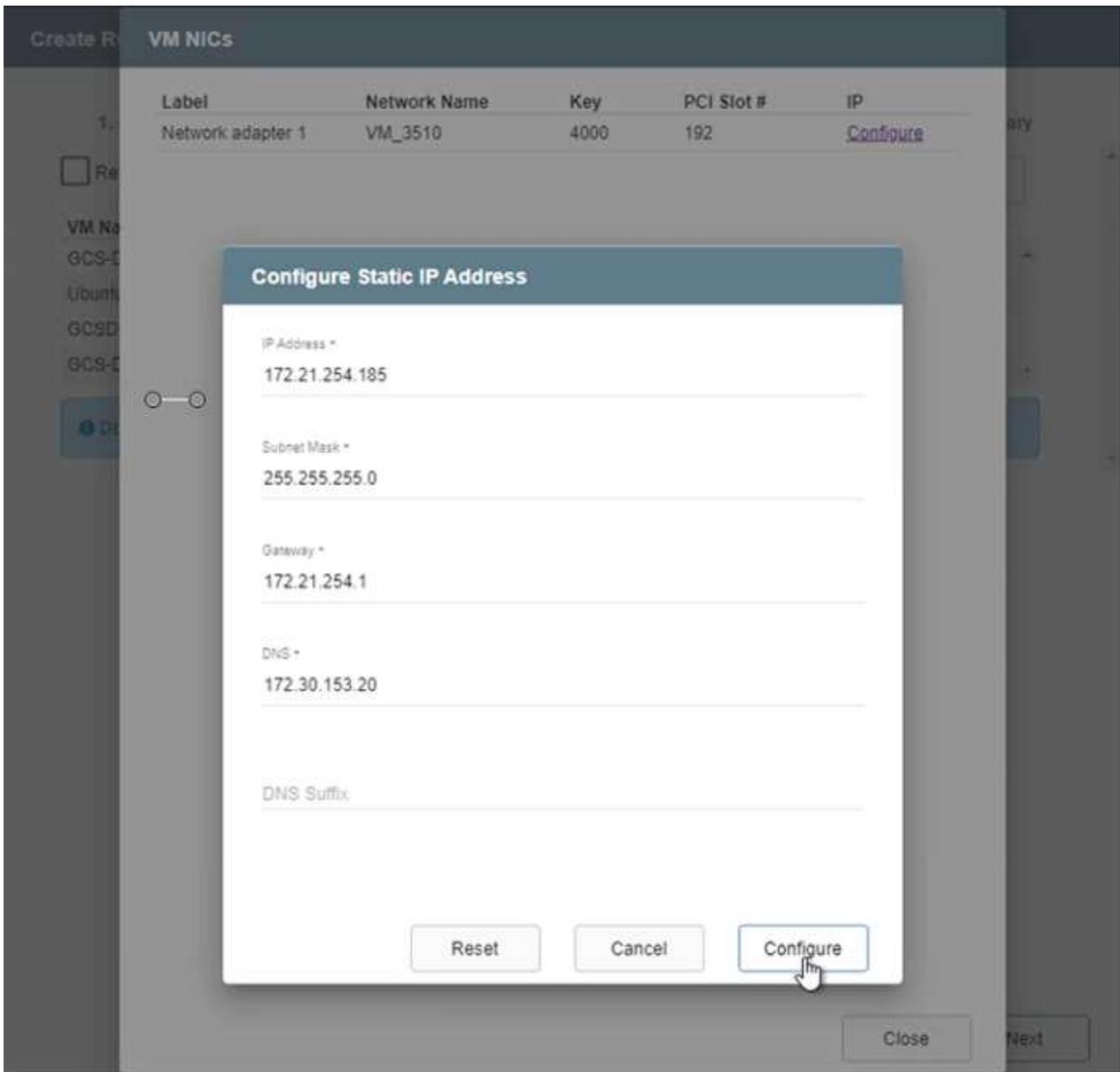
- 必要に応じてVMの設定を編集します。VMをリカバリするためのパラメータを指定します。これには、ブートシーケンス、ブート遅延（秒単位）、CPUの数、割り当てるメモリの量などが含まれます。上下の矢印をクリックして、VMのブートシーケンスを変更します。MACを保持するためのオプションも用意されています。



- 静的IPアドレスは、グループの個々のVMに手動で設定できます。VMのNICビューリンクをクリックして、IPアドレスを手動で設定します。



19. Configureボタンをクリックして、それぞれのVMのNIC設定を保存します。



フェイルオーバーとフェイルバックの両方のランブックのステータスが構成済みとして表示されるようになりました。フェイルオーバーとフェイルバックのRunbookグループは、同じVMと設定の初期グループを使用してペアで作成されます。必要に応じて、それぞれの[詳細]リンクをクリックして変更を行うことで、ランブックグループの設定を個別にカスタマイズできます。

## プライベートクラウドでAVS向けJetStream DRをインストールします

リカバリサイト (AVS) では、3ノードのパイロットライトクラスタを事前に作成することを推奨します。これにより、以下を含むリカバリサイトのインフラを事前に設定できます。

- 宛先ネットワークセグメント、ファイアウォール、DHCPやDNSなどのサービスなど
- AVS対応のJetStream DRのインストール
- ANFボリュームをデータストアなどとして設定

Jetstream DRは、ミッションクリティカルなドメインでほぼゼロのRTOモードをサポートします。これらのドメインには、デスティネーションストレージが事前にインストールされている必要があります。この場合、ANFは推奨ストレージタイプです。

**i** セグメント作成を含むネットワーク構成は、オンプレミスの要件に合わせてAVSクラスタ上で設定する必要があります。

**i** SLAやRTOの要件に応じて、継続的フェイルオーバーモードまたは通常の（標準）フェイルオーバーモードを使用できます。RTOがほぼゼロになるように、リカバリサイトで継続的なリハイドレートを開始する必要があります。

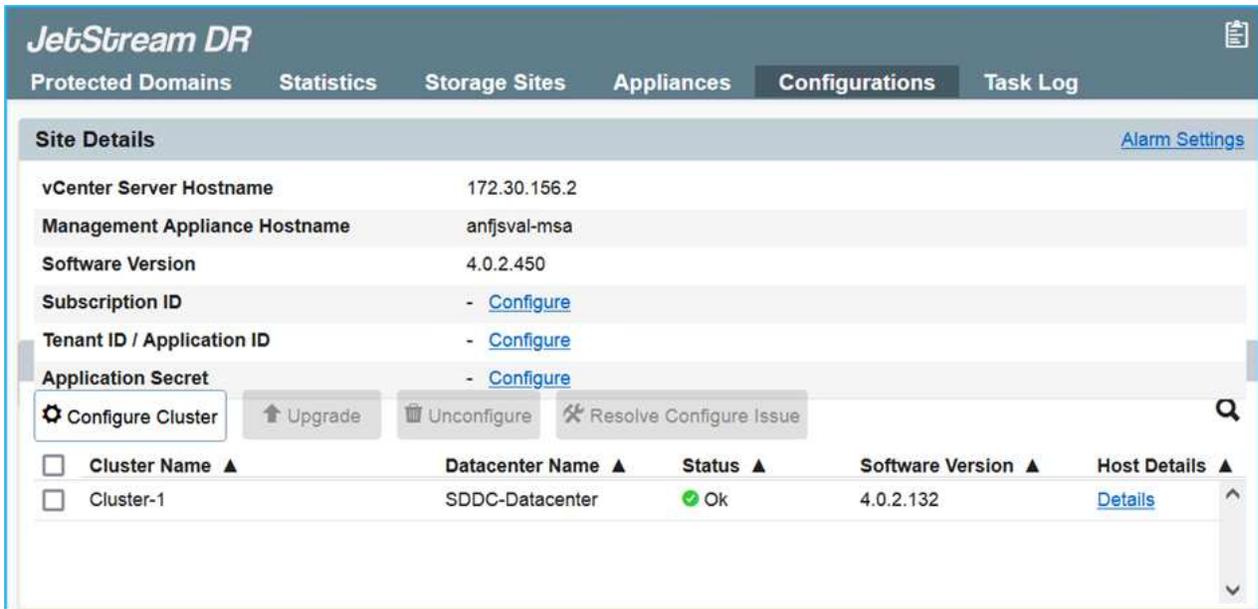
1. Azure VMware解決策 プライベートクラウドにJetStream DR for AVSをインストールするには、実行コマンドを使用します。Azureポータルで、Azure VMware解決策 に移動し、プライベートクラウドを選択して、実行コマンド>パッケージ> JSDR.Configurationを選択します。

**i** Azure VMware解決策 のデフォルトCloudAdminユーザには、AVS対応のJetStream DRをインストールするための十分な権限がありません。Azure VMware解決策 では、JetStream DR用のAzure VMware解決策 実行コマンドを呼び出すことで、JetStream DRのインストールを簡単かつ自動化できます。

次のスクリーンショットは、DHCPベースのIPアドレスを使用したインストール方法を示しています。

The screenshot shows the Azure portal interface for running a command in a private cloud. The main window displays a list of packages under the heading 'ANFDataClus | Run command'. The packages listed include 'ISDR.Configuration', 'Disable-JetDRForCluster', 'Enable-JetDRForCluster', 'Install-JetDRWithDHCP', 'Install-JetDRWithStateIP', 'Invoke-PreFlightJetDRInstall', 'Invoke-PreFlightJetDRUninstall', and 'Uninstall-JetDR'. The 'Install-JetDRWithDHCP' package is selected, and its details are shown in a right-hand pane. The details pane includes a description of the command, command parameters, and a form for entering the command parameters. The parameters include 'ProtectedCluster' (set to True), 'Cluster' (Cluster-1), 'Datastore' (vsanDatastore), 'VMName' (anfsvl-msa), 'Cluster' (Cluster-1), 'Credential' (Username: root, Password: \*\*\*\*\*), 'HostName' (anfsvl-msa), and 'Network' (DRSeg).

2. JetStream DR for AVSのインストールが完了したら、ブラウザをリフレッシュします。JetStream DR UIにアクセスするには、SDDC Datacenter > Configure > JetStream DRに移動します。



3. JetStream DRインターフェイスから、次の作業を行います。
  - a. オンプレミスクラスタをストレージサイトとして保護するために使用したAzure Blob Storageアカウントを追加し、Scan Domainsオプションを実行します。
  - b. 表示されるポップアップダイアログで、インポートする保護ドメインを選択し、そのインポートリンクをクリックします。



4. ドメインがリカバリ用にインポートされます。[保護ドメイン]タブに移動して、目的のドメインが選択されていることを確認するか、[保護ドメインの選択]メニューから目的のドメインを選択します。保護ドメイン内のリカバリ可能なVMのリストが表示されます。



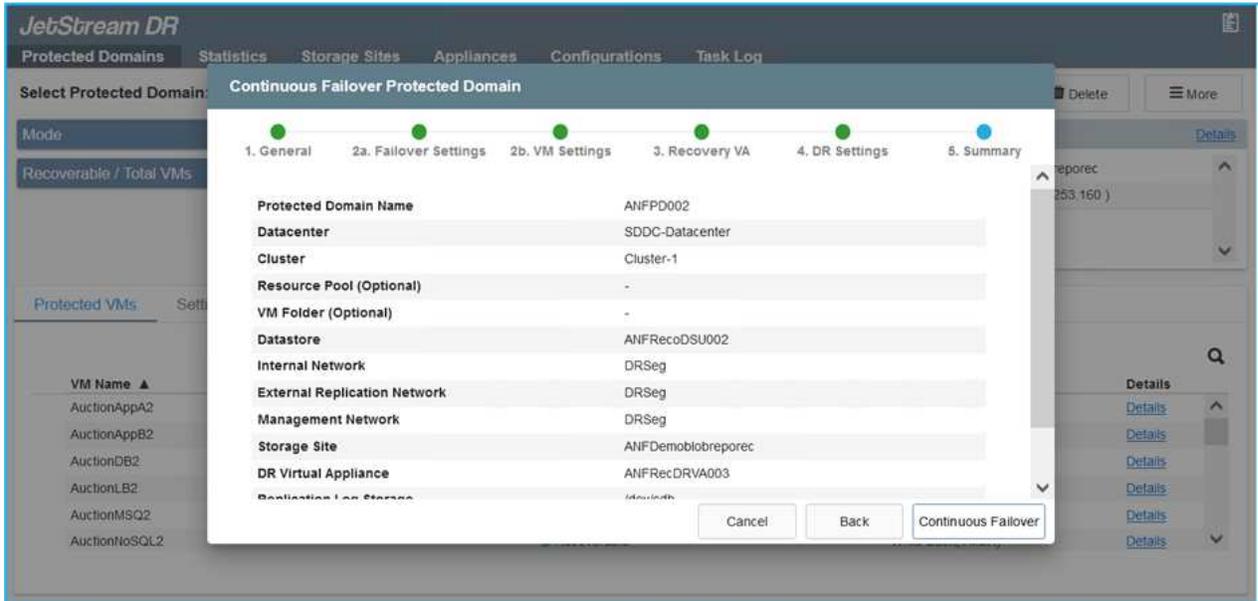
5. 保護ドメインをインポートしたら、DRVAアプライアンスを展開します。



これらの手順は、CPT作成プランを使用して自動化することもできます。

6. 使用可能なvSANまたはANFデータストアを使用してレプリケーションログボリュームを作成します。

7. 保護ドメインをインポートし、VMの配置にANFデータストアを使用するようにリカバリVAを設定します。



選択したセグメントでDHCPが有効になっていて、十分なIPが使用可能であることを確認します。ダイナミックIPは、ドメインのリカバリ中に一時的に使用されます。リカバリVM（連続リハイドレートを含む）ごとに、個別のダイナミックIPが必要です。リカバリの完了後、IPは解放され、再利用できます。

8. 適切なフェイルオーバーオプション（継続的フェイルオーバーまたはフェイルオーバー）を選択します。この例では、連続リハイドレート（連続フェイルオーバー）が選択されています。



設定の実行時には、継続的フェイルオーバーモードとフェイルオーバーモードが異なりますが、両方のフェイルオーバーモードを同じ手順で設定します。フェイルオーバー手順は、災害発生時の対応として一緒に設定および実行されます。継続的フェイルオーバーはいつでも設定でき、通常のシステム運用中はバックグラウンドで実行できます。災害が発生すると、継続的なフェイルオーバーが完了し、保護対象のVMの所有権がリカバリサイトにただちに移行されます（RTOはほぼゼロ）。

JetStream DR

Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: GCDRDP\_Demo01 [View all](#) + Create Delete More

Mode: Imported

Recoverable / Total VMs: 5 / 5

Configurations

Storage Site: ANFDemoblobrepor

Owner Site: REMOTE ( 172.21.253.11 )

- Restore
- Failover
- Continuous Failover
- Test Failover

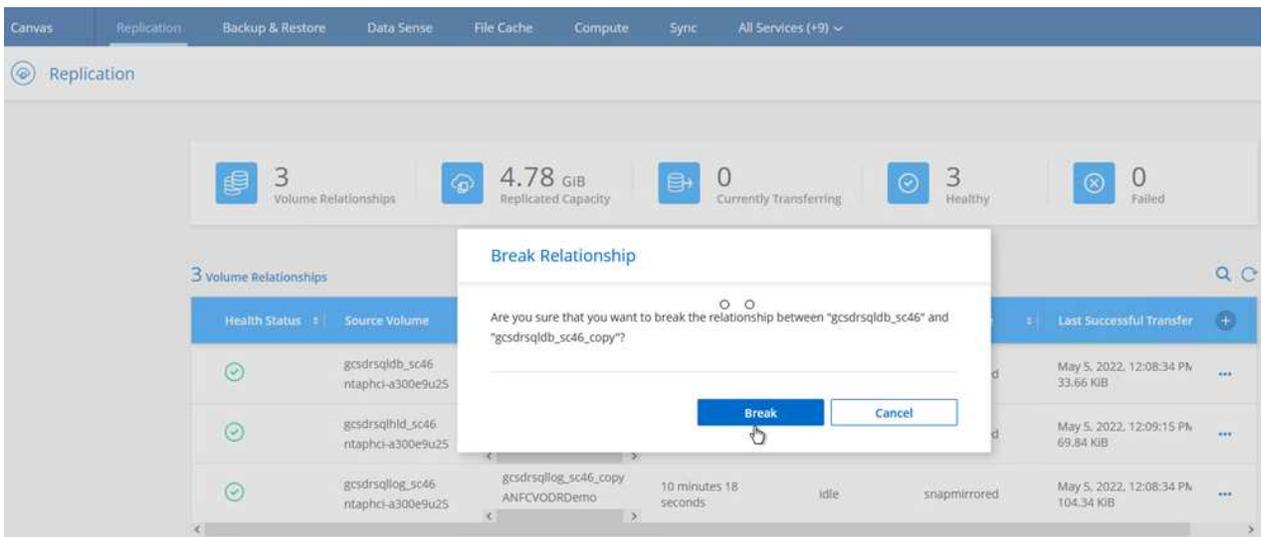
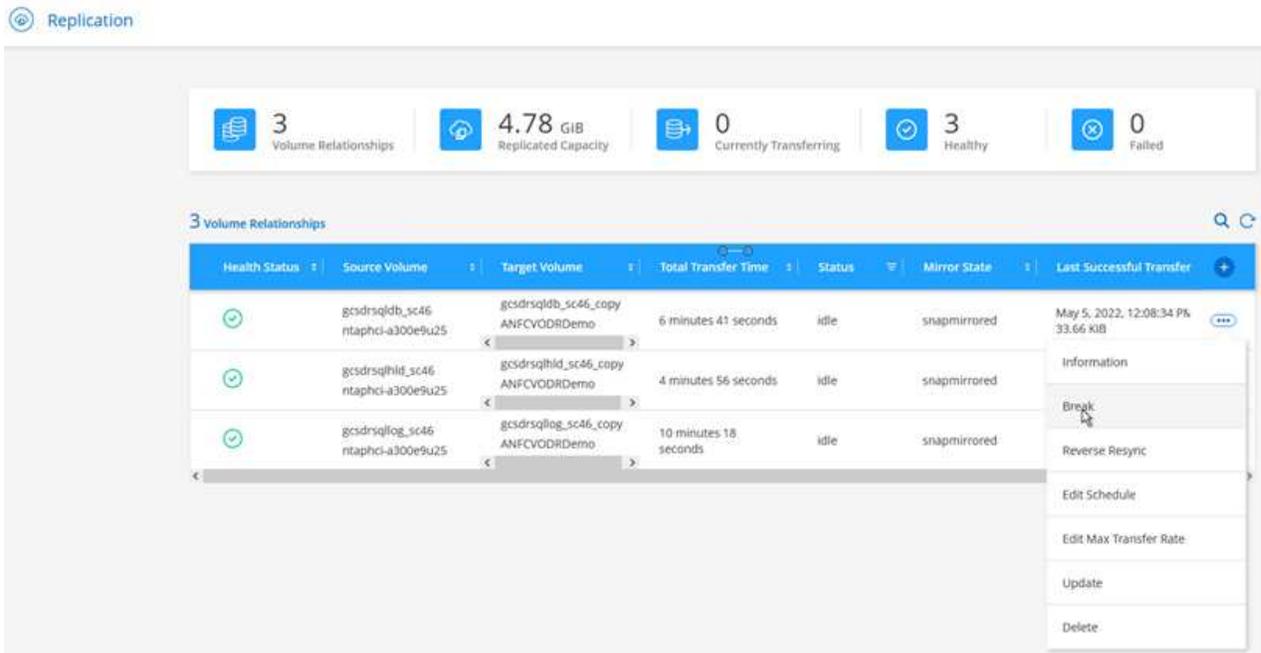
Protected VMs | Settings | Alarms

VM Name ▲	Protection Status ▲	Protection Mode ▲	Details
GCS-DR-DC	● Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-LinVM01	● Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SCA	● Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SQL01	● Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-WinVM01	● Recoverable	Write-Back(VMDK)	<a href="#">Details</a>

継続的なフェイルオーバープロセスが開始され、UIから進行状況を監視できます。[現在のステップ]セクションの青いアイコンをクリックすると、ポップアップウィンドウが開き、フェイルオーバープロセスの現在のステップの詳細が表示されます。

## 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対象クラスタで障害が発生した場合（部分的または完全な障害）、該当するアプリケーションボリュームのSnapMirror関係を解除したあと、Jetstreamを使用してVMのフェイルオーバーをトリガーできます。



この手順は簡単に自動化できるため、リカバリプロセスが容易になります。

2. AVS SDDC（宛先側）上のJetstream UIにアクセスし、フェイルオーバーオプションをトリガしてフェイルオーバーを完了します。タスクバーにフェイルオーバーアクティビティの進行状況が表示されます。

フェイルオーバーが完了したときに表示されるダイアログウィンドウで、フェイルオーバータスクを計画どおりに指定することも、強制的に実行することもできます。

JetStream DR

Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: GCSDRPD\_Demo01 [View all](#) + Create Failover More

Mode: Continuous Rehydration in Progress

Recoverable / Total VMs: 4 / 4

Data (Processed/Known Remaining): 329.01 GB / 6.19 GB

Current Step: Recover VMs' data from Storage Site

Configurations

- Storage Site: ANFDemotobreporec
- Owner Site: REMOTE ( 172.21.253.160 )
- Datacenter \ Cluster: SDDC-Datacenter \ Cluster-1
- Point-in-time Recovery: Disabled

Protected VMs | Settings | Alarms

VM Name	Protection Status	Protection Mode	Details
GCS-DR-DC	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-LinVM01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SCA	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SQL01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-WinVM01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>

### Complete Continuous Failover for Protected Domain

**VM Network Mapping**

Protected VM Network	Recovery VM Network
VM_3510	DRStretchSeg

**Other Settings**

Planned Failover

Force Failover

Some VMs' guest credential are required because of network configuration: Configure

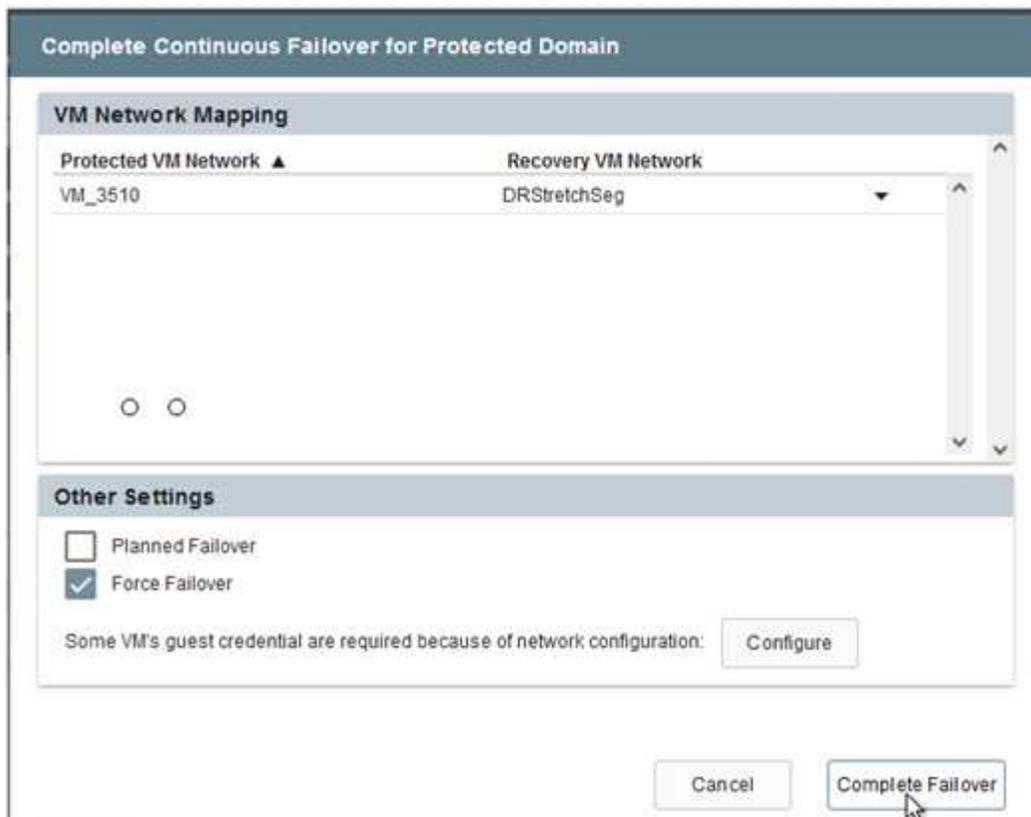
Cancel Complete Failover

強制フェイルオーバーでは、プライマリサイトがアクセス不能になり、保護ドメインの所有権がリカバリサイトによって直接引き継がれる必要があります。

### Force Failover

**!** Force Failover of Protected Domain requested. Administrator consent is required!  
Complete ownership of this Protected Domain will be taken over by this Site.  
Are you sure you want to continue?

Cancel Confirm



3. 継続的なフェイルオーバーが完了すると、タスクの完了を確認するメッセージが表示されます。タスクが完了したら、リカバリしたVMにアクセスしてiSCSIセッションまたはNFSセッションを設定します。



フェイルオーバーモードが「Running in Failover」に変わり、VMのステータスが「Recoverable」になります。保護ドメインのすべてのVMが、フェールオーバーラックブック設定で指定された状態でリカバリサイトで実行されるようになりました。



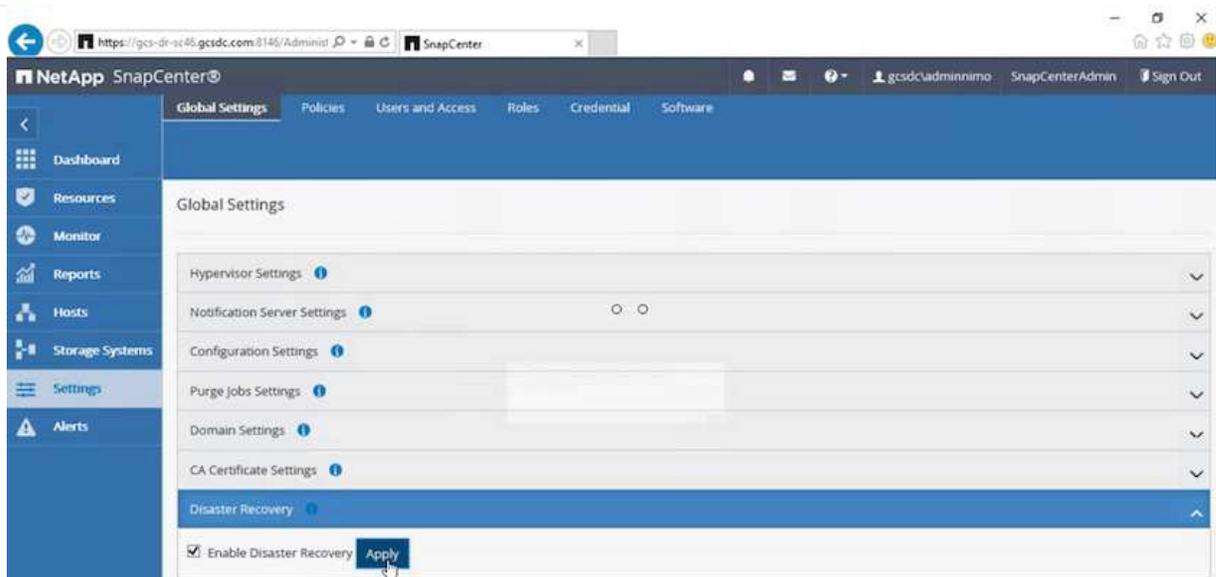
フェールオーバー構成とインフラストラクチャを検証するために、JetStream DRをテストモード（テストフェールオーバーオプション）で実行して、仮想マシンとそのデータをオブジェクトストアからテストリカバリ環境にリカバリすることができます。フェールオーバー手順がテストモードで実行されると、その動作は実際のフェールオーバープロセスに似ています。



4. 仮想マシンのリカバリが完了したら、ゲスト内ストレージにストレージディザスタリカバリを使用します。このプロセスを実証するために、この例ではSQL Serverを使用しています。
5. AVS SDDCでリカバリしたSnapCenter VMにログインし、DRモードを有効にします。
  - a. browserNを使用してSnapCenter UIにアクセスします。



- b. [設定]ページで、[設定]>[グローバル設定]>[ディザスタリカバリ]の順に選択します。
- c. Enable Disaster Recoveryを選択します。
- d. 適用をクリックします。

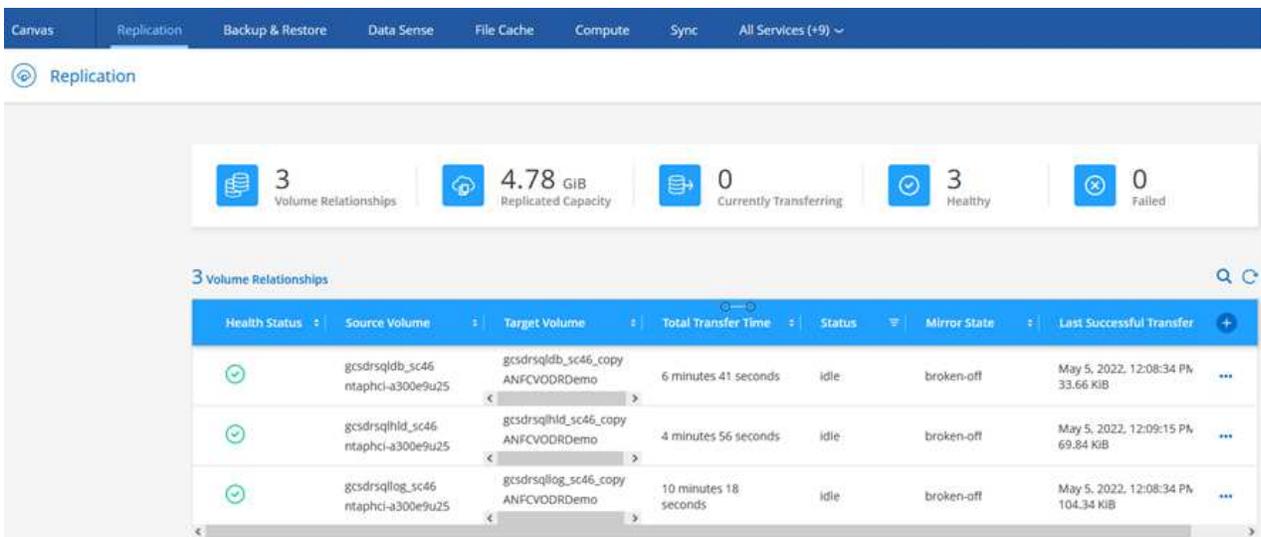


- e. [Monitor]>[Jobs]をクリックして、DRジョブが有効になっているかどうかを確認します。



ストレージのディザスタリカバリには、NetApp SnapCenter 4.6以降を使用してください。以前のバージョンでは、アプリケーションと整合性のあるSnapshot (SnapMirrorを使用してレプリケート) を使用し、ディザスタリカバリサイトで以前のバックアップをリカバリする必要がある場合に手動でリカバリする必要があります。

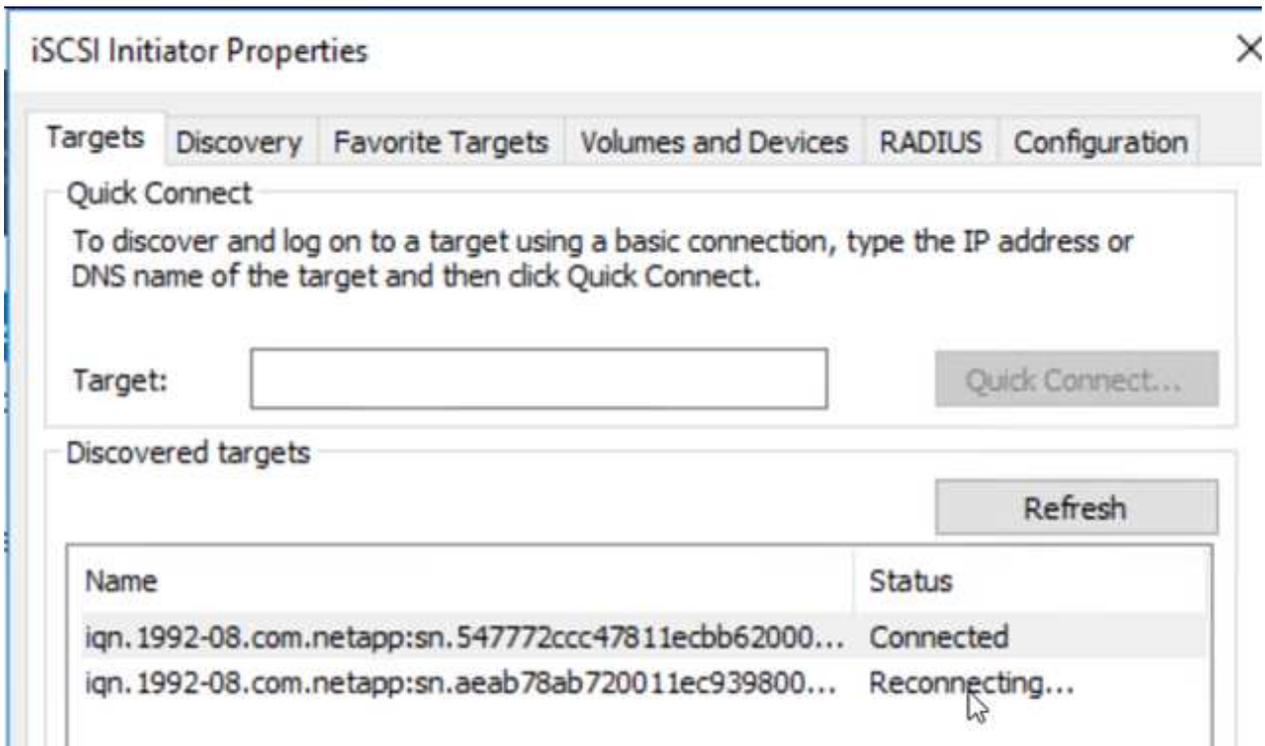
6. SnapMirror関係が解除されていることを確認します。



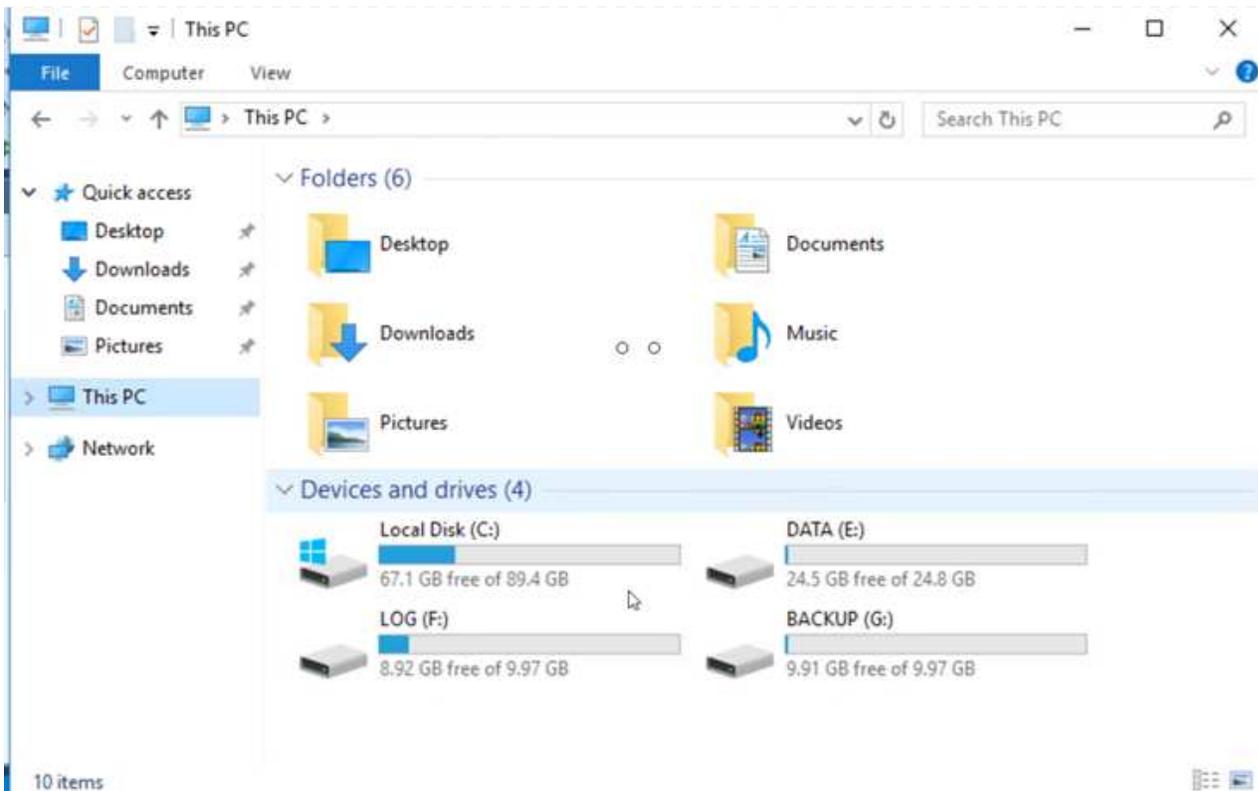
7. Cloud Volumes ONTAP からリカバリしたSQLゲストVMに、同じドライブレターを使用してLUNを接続します。

Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
	Simple	Basic		Healthy (R...	450 MB	450 MB	100 %
	Simple	Basic		Healthy (E...	99 MB	99 MB	100 %
(C:)	Simple	Basic	NTFS	Healthy (B...	89.45 GB	67.03 GB	75 %
BACKUP (G:)	Simple	Basic	NTFS	Healthy (P...	9.97 GB	9.92 GB	99 %
DATA (E:)	Simple	Basic	NTFS	Healthy (P...	24.88 GB	24.57 GB	99 %
LOG (F:)	Simple	Basic	NTFS	Healthy (P...	9.97 GB	8.93 GB	90 %

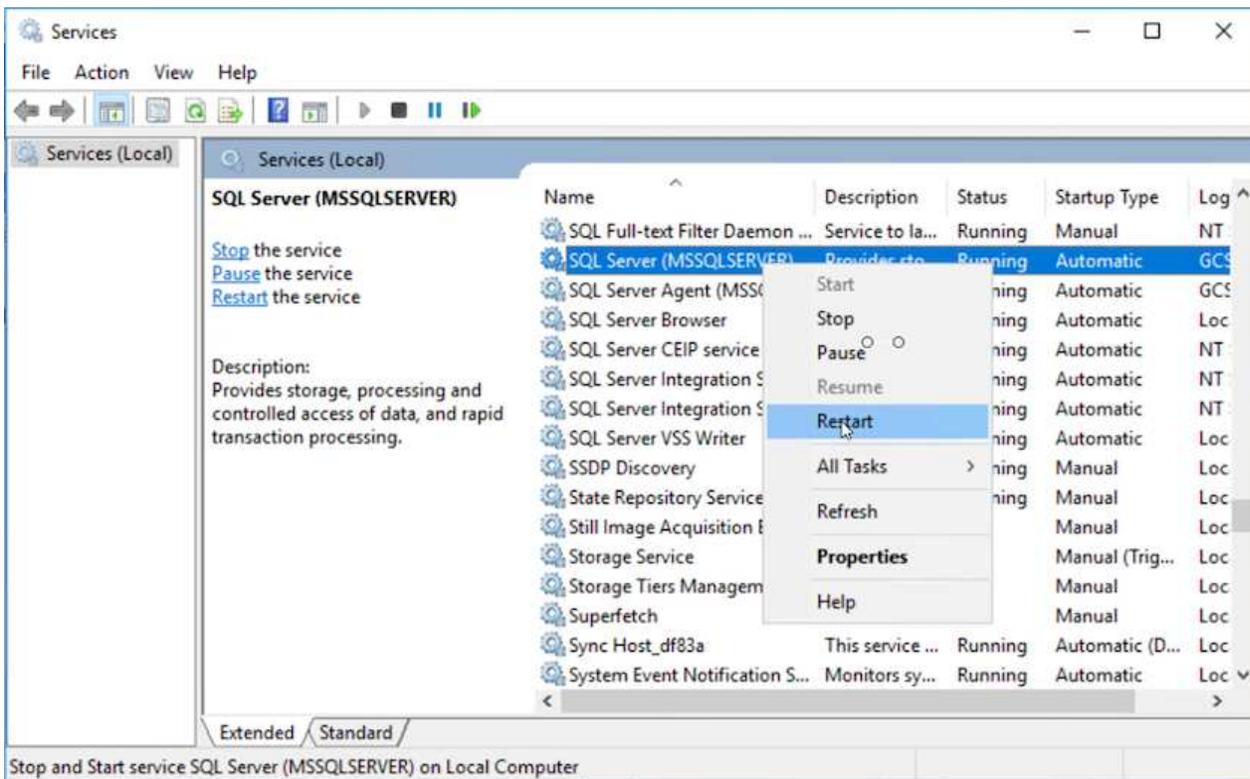
8. iSCSIイニシエータを開き、以前切断したセッションを消去して、レプリケートされたCloud Volumes ONTAP ボリュームのマルチパスとともに新しいターゲットを追加します。



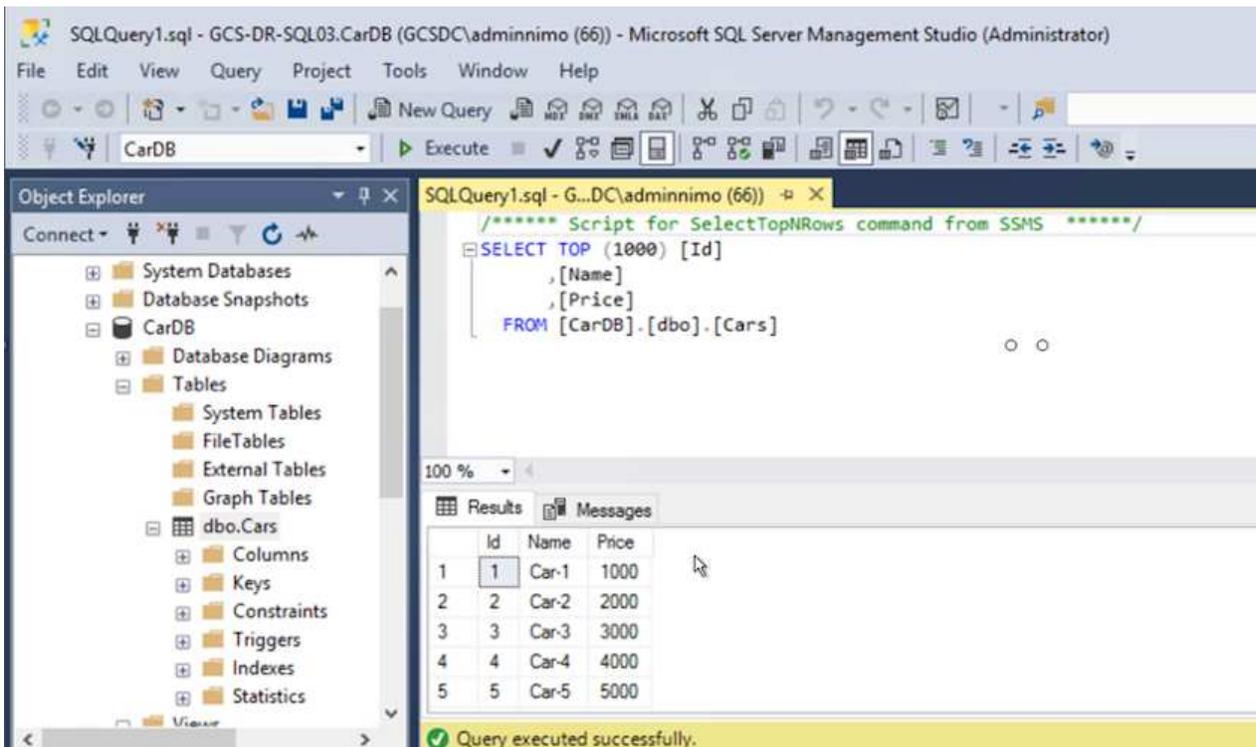
9. DR実行前に使用したのと同じドライブレターを使用して、すべてのディスクが接続されていることを確認してください。



10. MSSQLサーバサービスを再起動します。



11. SQLリソースがオンラインに戻っていることを確認します。



NFSの場合は'mount'コマンドを使用してボリュームを接続し'/etc/fstab'エントリを更新します

この時点で運用を開始し、通常どおり業務を継続できます。



NSX Tエンドでは'フェイルオーバー・シナリオをシミュレートするために'個別の専用ティア1ゲートウェイを作成できますこれにより、すべてのワークロードが相互に通信できるようになりますが、環境内や環境外にトラフィックをルーティングできないため、トリアージ、封じ込め、セキュリティ強化のタスクをクロスコンタミネーションのリスクなしに実行できます。この操作はこのドキュメントでは扱いませんが、分離をシミュレートするために簡単に行うことができます。

プライマリサイトが起動し、再び実行されるようになったら、フェイルバックを実行できます。VM保護はJetstreamで再開され、SnapMirror関係を反転する必要があります。

1. オンプレミス環境をリストア災害のタイプによっては、保護対象クラスターの構成をリストアまたは検証しなければならない場合があります。必要に応じて、JetStream DRソフトウェアを再インストールする必要があります。
2. リストアされたオンプレミス環境にアクセスし、Jetstream DR UIに移動して、適切な保護ドメインを選択します。保護サイトがフェイルバックできる状態になったら、UIで[Failback]オプションを選択します。



CPTによって生成されたフェイルバック計画を使用して、VMとそのデータをオブジェクトストアから元のVMware環境に戻すこともできます。

JetStream DR

Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: GCDRDP\_Demo01 [View all](#)

Mode: Running in Failover

Active Site: 172.30.156.2

Recoverable / Total VMs: 4 / 4

Configurations

Storage Site: ANFCVODR

Owner Site: REMOTE (172.30.156.2)

+ Create | Delete | More

Restore | Resume Continuous Rehydration | Failback

Protected VMs | Settings | Alarms

VM Name	Protection Status	Protection Mode	Details
GCS-DR-DC	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-LinVM01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SCA	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-SQL01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>
GCS-DR-WinVM01	Recoverable	Write-Back(VMDK)	<a href="#">Details</a>



リカバリサイトでVMを一時停止して保護対象サイトで再起動したあとの最大遅延時間を指定します。このプロセスには、フェイルオーバーVMを停止したあとのレプリケーションの完了、リカバリサイトのクリーンアップに必要な時間、保護サイトでVMを再作成するのに必要な時間などが含まれます。10分を推奨します。

### Failback Protected Domain

1. General | 2a. Failback Settings | 2b. VM Settings | 3. Recovery VA | 4. DR Settings | 5. Summary

Failback Datacenter	A300-DataCenter
Failback Cluster	A300-Cluster
Failback Resource Pool	-
VM Folder (Optional)	-
Failback Datastore	A300_NFS_vMotion
Maximum Delay After Stopping	10 Minutes
Internal Network	VM_187
External Replication Network	VM_187
Management Network	VM_187
Storage Site	ANFCVODR
DR Virtual Appliance	GCDRVA002
Replication Loo Storage	/dev/sdb

Cancel | Back | Failback

3. フェイルバックプロセスを完了し、VM保護およびデータの整合性が再開されたことを確認する。

JetStream DR

Protected Domains | Statistics | Storage Sites

Select Protected Domain: GCDRDP002

Recoverable / Total VMs

Replication Status

Remaining Background Data

Current RPO

Protected VMs | Settings | Alarms

### Failback Task Result

Task Completed Successfully

Protected Domain	GCDRDP002
VMs Recovery Status	Success
Total VMs Recovered	4
GCSRecovery03 Status:	
Pre-script Execution Status	Not defined
Runbook Execution Status	Success
Post-script Execution Status	Not defined

4. VMのリカバリが完了したら、セカンダリストレージをホストから切断してプライマリストレージに接続します。

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	6 minutes 41 seconds	idle	broken-off	May 5, 2022, 12:08:34 PM 33.66 KiB
✓	gcsdrsqhld_sc46 ntaphci-a300e9u25	gcsdrsqhld_sc46_copy ANFCVODRDemo	4 minutes 56 seconds	idle	broken-off	
✓	gcsdrsqlog_sc46 ntaphci-a300e9u25	gcsdrsqlog_sc46_copy ANFCVODRDemo	10 minutes 18 seconds	idle	broken-off	

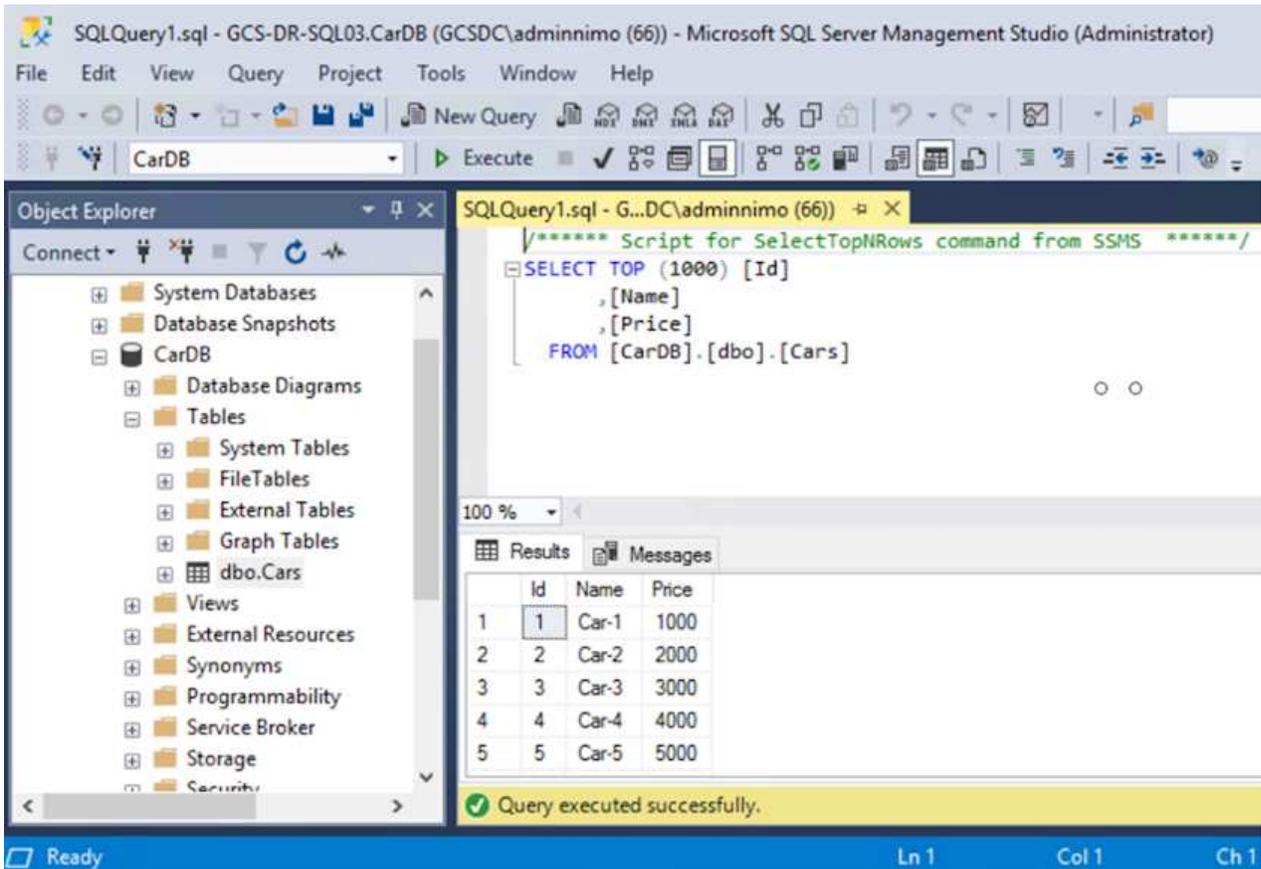
- Information
- Resync
- Reverse Resync
- Edit Schedule
- Edit Max Transfer Rate
- Delete

3 Volume Relationships    6.54 GiB Replicated Capacity    0 Currently Transferring    3 Healthy    0 Failed

3 Volume Relationships

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	19 seconds	idle	snapmirrored	May 6, 2022, 11:03:00 AM 5.73 MiB
✓	gcsdrsqhld_sc46_copy ANFCVODRDemo	gcsdrsqhld_sc46 ntaphci-a300e9u25	1 minute 46 seconds	idle	snapmirrored	May 6, 2022, 11:01:39 AM 800.76 MiB
✓	gcsdrsqlog_sc46 ntaphci-a300e9u25	gcsdrsqlog_sc46_copy ANFCVODRDemo	51 seconds	idle	snapmirrored	May 6, 2022, 11:03:15 AM 785.8 MiB

5. MSSQLサーバサービスを再起動します。  
6. SQLリソースがオンラインに戻っていることを確認します。



プライマリストレージにフェイルバックするには、逆再同期処理を実行して、フェイルオーバーの前と同じ関係の方向が維持されていることを確認します。



逆再同期処理の実行後もプライマリストレージとセカンダリストレージのロールを保持するには、逆再同期処理をもう一度実行します。

このプロセスは、Oracleなどの他のアプリケーション、類似したデータベースの種類、ゲスト接続ストレージを使用するその他のアプリケーションに適用されます。

常に同様に、重要なワークロードを本番環境に移植する前に、リカバリに必要な手順をテストしてください。

#### この解決策 の利点

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

- 開発とテスト、セキュリティテスト、パッチとアップグレードのテスト、修正テストなど、DR以外のワークフローにDRデータを活用します。
- CPUとRAMの最適化は、小規模なコンピューティングクラスタへのリカバリを可能にすることで、クラウドコストの削減に役立ちます。

## TR-4955 : 『Disaster Recovery with Azure NetApp Files (ANF) and Azure VMware 解決策 (AVS) 』

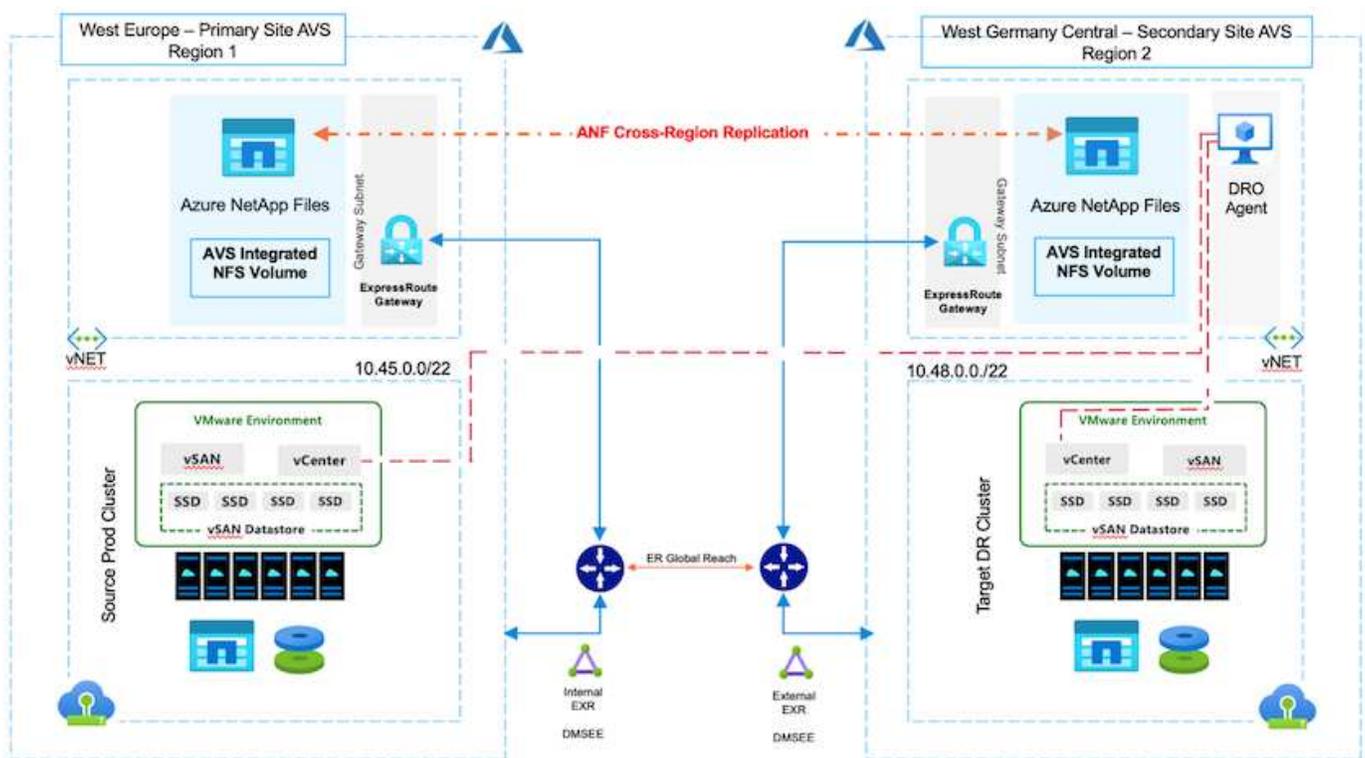
クラウド内のリージョン間でブロックレベルのレプリケーションを使用したディザスタリカバリは、耐障害性に優れた対費用効果の高い方法で、サイトの停止やデータ破損イベント（ランサムウェアなど）からワークロードを保護します。

作成者：ネットアップソリューションエンジニアリング担当Niyaz Mohamed

### 概要

Azure NetApp Files (ANF) のリージョン間ボリュームレプリケーションを使用するとAzure NetApp Files、Azure VMware解決策 (AVS) SDDCサイトで実行されているVMwareワークロードを、プライマリAVSサイトのNFSデータストアとして使用し、ターゲットリカバリリージョンの指定されたセカンダリAVSサイトにレプリケートできます。

ディザスタリカバリオーケストレーションツール (DRO) (UI付きのスク립ト化された解決策) を使用すると、AVS SDDC間でレプリケートされたワークロードをシームレスにリカバリできます。DROは、レプリケーションピアリングを解除してから、AVSへのVM登録を通じて、NSX-T (すべてのAVSプライベートクラウドに含まれる) 上のネットワークマッピングに、デスティネーションボリュームをデータストアとしてマウントすることで、リカバリを自動化します。



## 前提条件と一般的な推奨事項

- レプリケーションピアリングを作成して、リージョン間レプリケーションが有効になっていることを確認します。を参照してください "[Azure NetApp Files のボリュームレプリケーションを作成します](#)"。
- ソースとターゲットのAzure VMware解決策 プライベートクラウド間でExpressRouteグローバルリーチを設定する必要があります。
- リソースにアクセスできるサービスプリンシパルが必要です。
- サポートされるトポロジは、プライマリAVSサイトからセカンダリAVSサイトです。
- を設定します "[レプリケーション](#)" ビジネスニーズとデータ変更率に基づいて、ボリュームごとに適切なスケジュールを設定します。



カスケードトポロジ、ファンイントポロジ、ファンアウトトポロジはサポートされていません。

## はじめに

### Azure VMware解決策 を導入します

。["Azure VMware 解決策の略"](#) (AVS) は、Microsoft Azureパブリッククラウド内で完全に機能するVMware SDDCを提供するハイブリッドクラウドサービスです。AVSはMicrosoftが完全に管理およびサポートするファーストパーティの解決策で、Azureインフラストラクチャを使用するVMwareにより検証されています。そのため、お客様は、コンピューティングの仮想化にVMware ESXi、ハイパーコンバージドストレージにvSAN、ネットワークとセキュリティにNSXを利用できます。また、Microsoft Azureのグローバルなプレゼンス、クラスをリードするデータセンター施設、Azureネイティブのサービスとソリューションで構成される豊富なエコシステムへの近接性を活用できます。Azure VMware解決策 SDDCとAzure NetApp Files を組み合わせることで、ネットワークレイテンシを最小限に抑えながら最高のパフォーマンスを実現できます。

AzureでAVSプライベートクラウドを構成するには、以下の手順に従います "[リンク](#)" を参照してください "[リンク](#)" (Microsoftのマニュアル)。最小限の構成でセットアップされたパイロットライト環境は、DR目的で使用できます。このセットアップには、重要なアプリケーションをサポートするためのコアコンポーネントのみが含まれており、フェイルオーバーが発生した場合に、より多くのホストをスケールアウトして生成し、負荷の大部分を処理することができます。



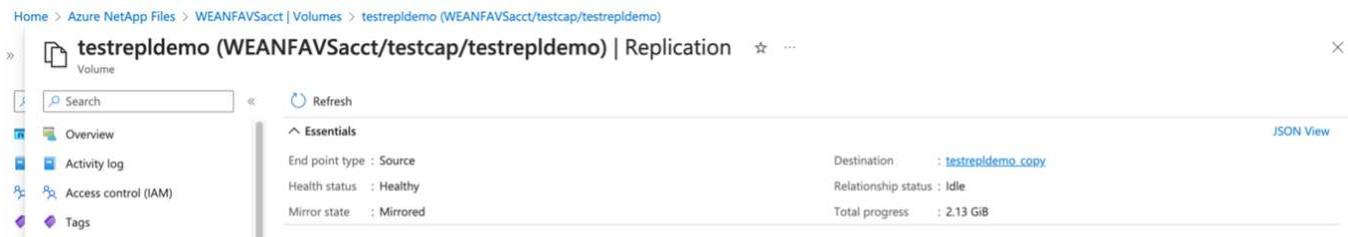
初期リリースでは、DROは既存のAVS SDDCクラスターをサポートしています。オンデマンドのSDDC作成は、今後のリリースで提供される予定です。

### Azure NetApp Files をプロビジョニングして設定

"[Azure NetApp Files の特長](#)" エンタープライズクラスのハイパフォーマンスな従量課金制ファイルストレージサービスです。以下の手順に従ってください "[リンク](#)" AVSプライベートクラウド環境を最適化するために、Azure NetApp Files をNFSデータストアとしてプロビジョニングおよび設定します。

### Azure NetApp Filesに対応したデータストアボリュームのボリュームレプリケーションを作成します

最初の手順では、AVSプライマリサイトからAVSセカンダリサイトへ、適切な頻度と保持期間を使用して、目的のデータストアボリュームのリージョン間レプリケーションを設定します。



以下の手順に従ってください。"リンク" レプリケーションピアリングを作成してリージョン間レプリケーションを設定するには、次の手順を実行します。デスティネーションの容量プールのサービスレベルは、ソースの容量プールのサービスレベルと同じにすることができます。ただし、このユースケースでは、標準のサービスレベルを選択してから選択できます。"サービスレベルを変更する" 実際に災害が発生した場合やDRシミュレーションが発生した場合。



リージョン間レプリケーション関係は前提条件であり、事前に作成しておく必要があります。

## DROのインストール

DROの使用を開始するには、指定されたAzure仮想マシンでUbuntuオペレーティングシステムを使用し、前提条件を満たしていることを確認します。次に、パッケージをインストールします。

前提条件：

- リソースにアクセスできるサービスプリンシパル。
- ソースとデスティネーションのSDDCおよびAzure NetApp Files インスタンスへの適切な接続が存在することを確認します。
- DNS名を使用する場合は、DNS解決を実施する必要があります。それ以外の場合は、vCenterのIPアドレスを使用します。
- OS要件：\*
- Ubuntu Focal 20.04 (LTS)指定されたエージェント仮想マシンに次のパッケージをインストールする必要があります。
- Docker です
- docker-composeの略
- JqChange `docker.sock` 次の新しい権限を追加します。 `sudo chmod 666 /var/run/docker.sock`



。 `deploy.sh` スクリプトは、必要なすべての前提条件を実行します。

手順は次のとおりです。

1. 指定した仮想マシンにインストールパッケージをダウンロードします。

```
git clone https://github.com/NetApp/DRO-Azure.git
```



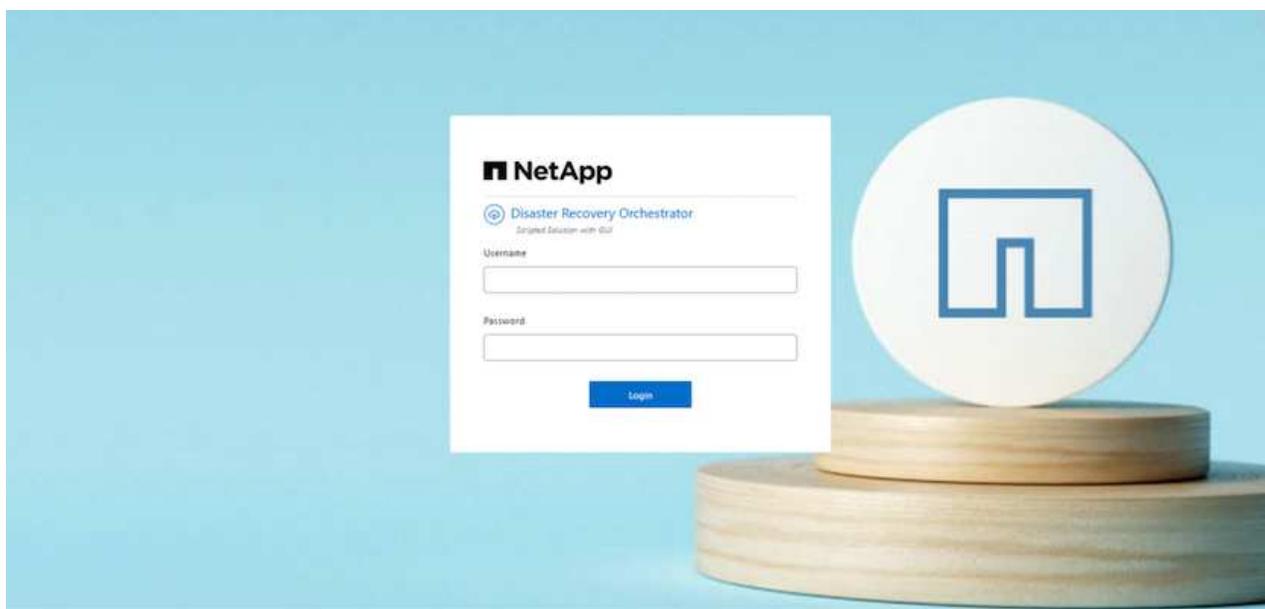
エージェントは、セカンダリAVSサイトリージョンまたはプライマリAVSサイトリージョンのSDDCとは別のAZにインストールする必要があります。

2. パッケージを解凍し、導入スクリプトを実行して、ホストIP（例：10.10.10.10）。

```
tar xvf draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

3. 次のクレデンシャルを使用してUIにアクセスします。

- ユーザ名： admin
- パスワード： admin



## DRO構成

Azure NetApp Files とAVSが正しく設定されたら、プライマリAVSサイトからセカンダリAVSサイトへのワークロードのリカバリを自動化するDROの設定を開始できます。セカンダリAVSサイトにDROエージェントを導入し、ExpressRouteゲートウェイ接続を設定して、DROエージェントが適切なAVSおよびAzure NetApp Files コンポーネントとネットワーク経由で通信できるようにすることを推奨します。

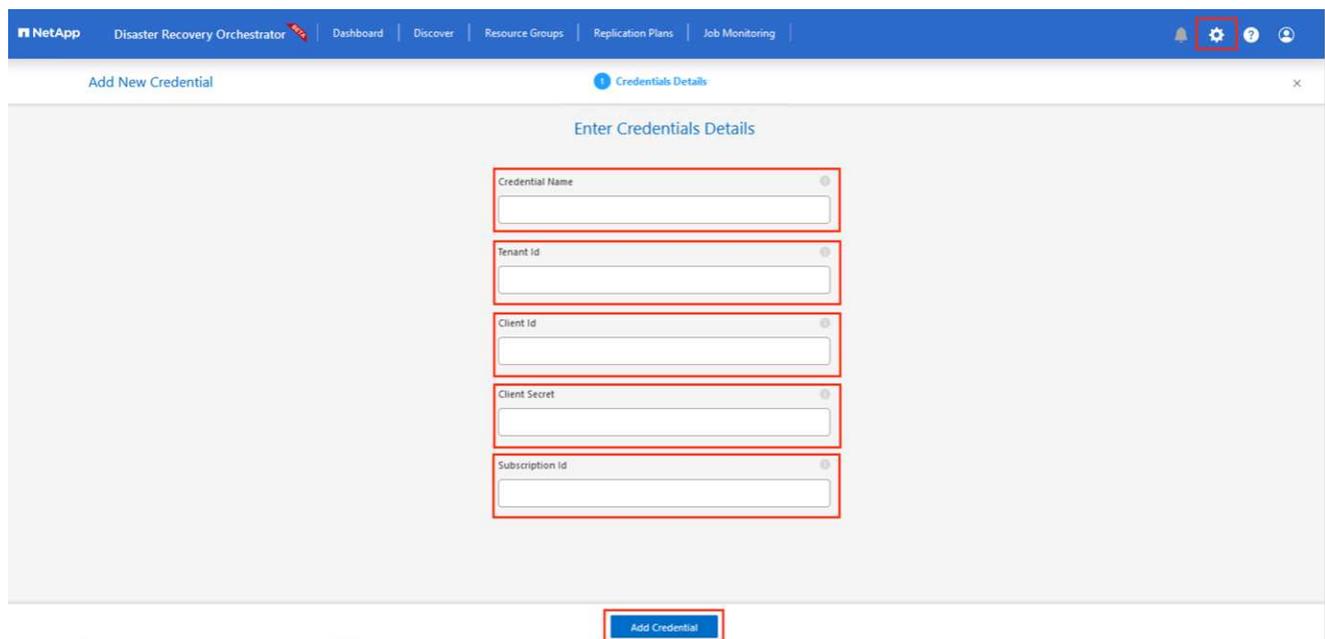
まず、クレデンシャルを追加します。DROには、Azure NetApp Files とAzure VMware解決策を検出する権限が必要です。Azure Active Directory (AD) アプリケーションを作成してセットアップし、DROに必要なAzureクレデンシャルを取得することで、Azureアカウントに必要な権限を付与できます。サービスプリンシパルをAzureサブスクリプションにバインドし、関連する必要な権限を持つカスタムロールを割り当てる必要があります。ソース環境とデスティネーション環境を追加すると、サービスプリンシパルに関連付けられているクレデンシャルを選択するように求められます。[Add New Site]をクリックする前に、これらのクレデンシャルをDROに追加する必要があります。

この処理を実行するには、次の手順を実行します。

1. サポートされているブラウザでDROを開き、デフォルトのユーザ名とパスワードを使用します (/admin /admin) 。パスワードは、[Change Password]オプションを使用して初回ログイン後にリセットできます。
2. DROコンソールの右上にある\*設定\*アイコンをクリックし、\*資格情報\*を選択します。
3. [Add New Credential]をクリックし、ウィザードの手順に従います。
4. クレデンシャルを定義するには、必要な権限を付与するAzure Active Directoryサービスプリンシパルに関する情報を入力します。
  - クレデンシャル名
  - テナントID
  - クライアント ID
  - クライアントシークレット
  - サブスクリプションID

この情報は、ADアプリケーションの作成時に取得しておく必要があります。

5. 新しいクレデンシャルの詳細を確認し、[Add Credential]をクリックします。



The screenshot shows the 'Add New Credential' wizard in the NetApp Disaster Recovery Orchestrator. The 'Enter Credentials Details' step is active, and the following fields are highlighted with red boxes:

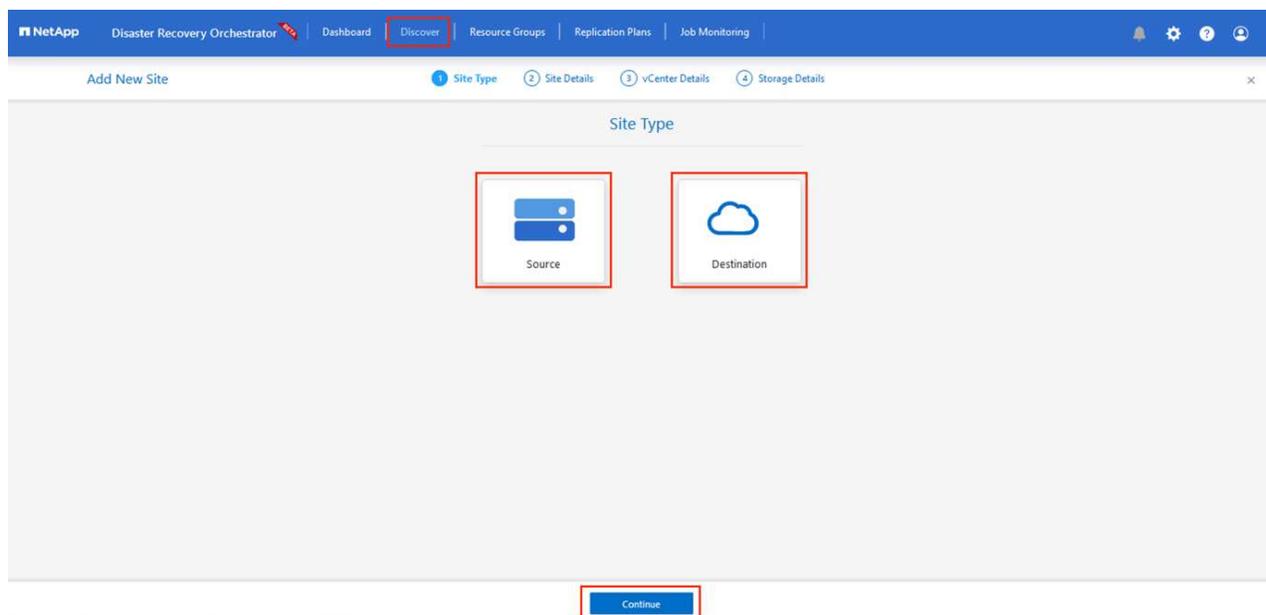
- Credential Name
- Tenant Id
- Client Id
- Client Secret
- Subscription Id

The 'Add Credential' button at the bottom is also highlighted with a red box.

クレデンシャルを追加したら、プライマリとセカンダリのAVSサイト（vCenterとAzure NetApp Files ストレージアカウントの両方）を検出してDROに追加します。ソースサイトとデスティネーションサイトを追加するには、次の手順を実行します。

6. [検出]タブに移動します。
7. [新しいサイトの追加]\*をクリックします。
8. 次のプライマリAVSサイトを追加します(コンソールで\*ソース\*として指定)。
  - SDDC vCenter
  - Azure NetApp Files ストレージアカウント
9. 次のセカンダリAVSサイト（コンソールで\* Destination \*として指定）を追加します。

- SDDC vCenter
- Azure NetApp Files ストレージアカウント



10. [ソース]をクリックしてサイト名を入力し、コネクタを選択してサイトの詳細を追加します。[\* Continue (続行) ]をクリックします。



このドキュメントでは、デモ用にソースサイトを追加する方法について説明します。

11. vCenterの詳細を更新します。これを行うには、プライマリAVS SDDCのドロップダウンからクレデンシヤル、Azureリージョン、およびリソースグループを選択します。
12. DROには、リージョン内で使用可能なすべてのSDDCが一覧表示されます。ドロップダウンから、指定したプライベートクラウドのURLを選択します。
13. を入力します `cloudadmin@vsphere.local` ユーザクレデンシヤル。これにはAzure Portalからアクセスできます。ここに記載されている手順に従ってください "[リンク](#)". 完了したら、\*[続行](#)\*をクリックします。

14. Azureリソースグループとネットアップアカウントを選択して、ソースストレージの詳細（ANF）を選択します。
15. [サイトの作成]\*をクリックします。

Site Name	Site Type	Location	vCenter	Storage	VM List	Discovery Status
DemoDest	Destination	Cloud	1	1	https://10.75.0.2/	Success
DemoSRC	Source	Cloud	1	1	<a href="#">View VM List</a> https://172.30.156.2/	Success

追加されると、DROは自動検出を実行し、ソースサイトからデスティネーションサイトへの対応するリージョン間レプリカを持つVMを表示します。DROは、VMで使用されているネットワークとセグメントを自動的に検出して入力します。

VM List  
Site: DemoSRC | vCenter: https://172.30.156.2/

7 Datastores | 128 Virtual Machines

VM Protection: 2 Protected, 126 Unprotected

VM Name	VM Status	VM State	DataStore	CPU	Memory (MB)
HD0Bench_2&1	Not Protected	Powered On	vsanDatastore	8	8192
hci-fio-datastore-13984-0-1	Not Protected	Powered Off	HCIstxDS	32	65536
ICCAz005-WD-R1	Not Protected	Powered On	vsanDatastore	8	14336
ICCAz005-HE-R1	Not Protected	Powered On	vsanDatastore	8	3072
ICCAz005-IL-R1	Not Protected	Powered On	vsanDatastore	8	3072
HCK_Demo_05	Not Protected	Powered Off	Demo002	1	2048
hci-nim-datastore-13984-0-1	Not Protected	Powered Off	HCIstxDS	34	49152

次の手順では、必要なVMをリソースグループとして機能グループにグループ化します。

#### リソースのグループ化

プラットフォームを追加したら、リカバリするVMをリソースグループにグループ化します。DROリソースグループを使用すると、依存する一連のVMを論理グループにグループ化して、それらの起動順序、ブート遅延、およびリカバリ時に実行可能なオプションのアプリケーション検証を含めることができます。

リソースグループの作成を開始するには、\*[新しいリソースグループの作成]\*メニュー項目をクリックします。

1. [PS]にアクセスし、[Create New Resource Group]\*をクリックします。

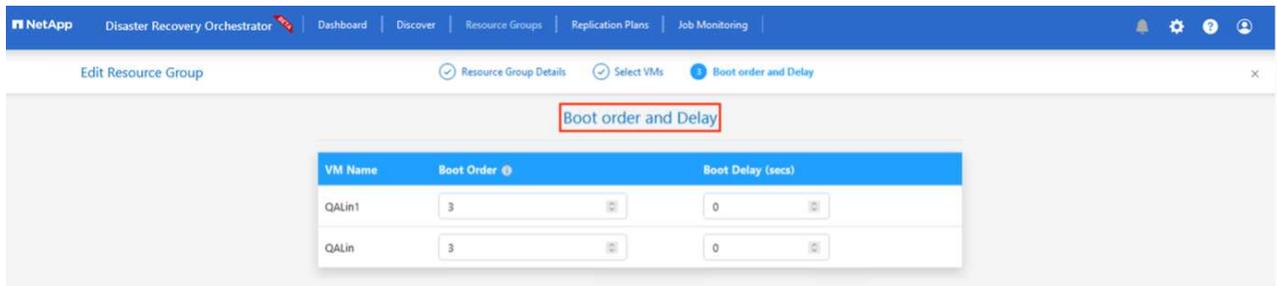
1 Resource Group | 1 Site | 1 vCenter | 2 Virtual Machines

1 Resource Group

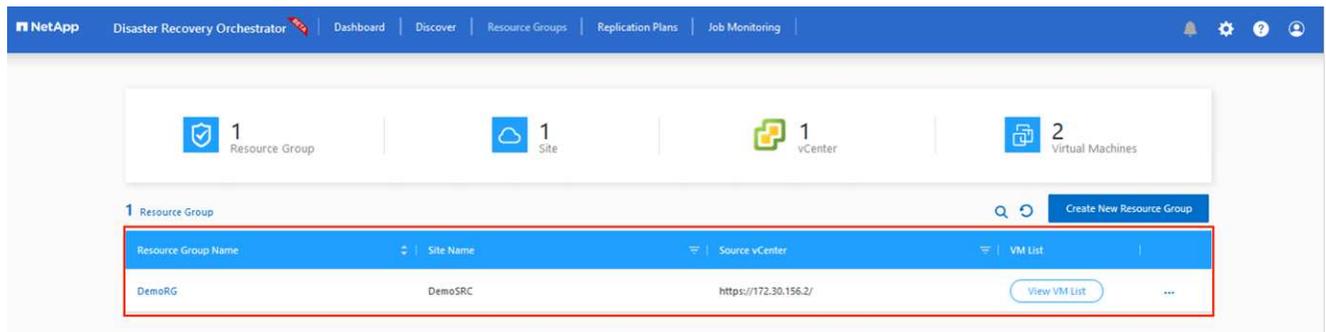
Resource Group Name	Site Name	Source vCenter	VM List
DemoRG	DemoSRC	https://172.30.156.2/	View VM List

2. [New Resource Group]で、ドロップダウンからソースサイトを選択し、\*[Create]\*をクリックします。
3. リソースグループの詳細を指定し、\*[続行]\*をクリックします。
4. 検索オプションを使用して適切なVMを選択します。
5. 選択したすべてのVMについて、と[Boot Delay] (秒)を選択します。各仮想マシンを選択して優先度を設定し、パワーオンシーケンスの順序を設定します。すべての仮想マシンのデフォルト値は3です。オプションは次のとおりです。
  - パワーオンする最初の仮想マシン

- デフォルト
- 最後にパワーオンした仮想マシン



6. [リソースグループの作成]をクリックします。

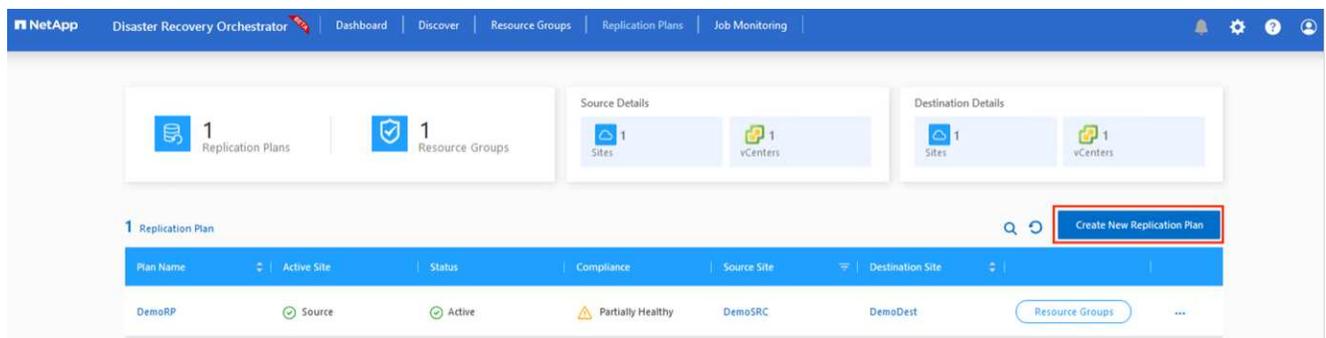


## レプリケーションプラン

災害発生時にアプリケーションをリカバリするための計画を立てておく必要があります。ドロップダウンからソースとデスティネーションのvCenterプラットフォームを選択し、このプランに含めるリソースグループを選択します。また、アプリケーションをリストアおよびパワーオンする方法（ドメインコントローラ、ティア1、ティア2など）もグループ化します。計画は設計図とも呼ばれます。リカバリプランを定義するには、[Replication Plan]タブに移動し、\*[New Replication Plan]\*をクリックします。

レプリケーションプランの作成を開始するには、次の手順を実行します。

1. に移動し、[Create New Replication Plan]\*をクリックします。



2. [New Replication Plan]\*で、プランの名前を指定し、ソースサイト、関連付けられているvCenter、デスティネーションサイト、および関連付けられているvCenterを選択してリカバリマッピングを追加します。

NetApp Disaster Recovery Orchestrator | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

Create New Replication Plan | 1 Replication Plan and Site Details | 2 Select Resource Groups | 3 Set Execution Order | 4 Set VM Details

### Replication Plan Details

Plan Name: DemoRP

#### Recovery Mapping

Source Site: DemoSRC | Destination Site: DemoDest

Source vCenter: https://172.30.156.2/ | Destination vCenter: https://10.75.0.2/

#### Cluster Mapping

Source Site Resource: Cluster-1 | Destination Site Resource: Cluster-1 | Add

Source Resource	Destination Resource
No Mappings added!	

Continue

- リカバリマッピングが完了したら、\***[クラスタマッピング]**\*を選択します。

NetApp Disaster Recovery Orchestrator | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

Create New Replication Plan | 1 Replication Plan and Site Details | 2 Select Resource Groups | 3 Set Execution Order | 4 Set VM Details

### Replication Plan Details

Plan Name: DemoRP

#### Recovery Mapping

Source Site: DemoSRC | Destination Site: DemoDest

Source vCenter: https://172.30.156.2/ | Destination vCenter: https://10.75.0.2/

#### Cluster Mapping

No more Source/Destination cluster resources available for mapping

Source Resource	Destination Resource
Cluster-1	Cluster-1 <span>Delete</span>

Continue

- [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。
- リソースグループの実行順序を設定します。このオプションを使用すると、複数のリソースグループが存在する場合の処理の順序を選択できます。
- 完了したら、適切なセグメントにネットワークマッピングを設定します。セグメントはセカンダリAVSクラスタです。すでにプロビジョニングされている必要があります。それらにVMをマッピングするには、適切なセグメントを選択します。
- データストアのマッピングは、VMの選択に基づいて自動的に選択されます。



リージョン間レプリケーション（CRR）はボリュームレベルで実行されます。そのため、該当するボリューム上のすべてのVMがCRRデスティネーションにレプリケートされます。レプリケーションプランに含まれる仮想マシンのみが処理されるため、データストアに含まれるすべてのVMを選択してください。

Replication Plan Details

Select Execution Order

Resource Group Name	Execution Order
DemoRG	3

Network Mapping

No more Source/Destination network resources available for mapping

Source Resource	Destination Resource	
SepSeg	SegDR	Delete

DataStore Mapping

Source DataStore	Destination Volume
TestSrc01	gwc_ntap_acct/gwc_DRO_cp/testsrc01copy

Previous Continue

8. [VM details]で、必要に応じてVMのCPUパラメータとRAMパラメータのサイズを変更できます。これは、大規模な環境を小規模なターゲットクラスタにリカバリする場合や、1対1の物理VMwareインフラストラクチャをプロビジョニングせずにDRテストを実行する場合に非常に役立ちます。また、リソースグループ全体で選択したすべてのVMのブート順序とブート遅延（秒）を変更します。リソースグループのブート順序の選択時に選択したものから変更が必要な場合はブート順序を変更する追加オプションがあります。デフォルトでは、リソースグループの選択時に選択された起動順序が使用されますが、この段階で変更を実行できます。

VM Details

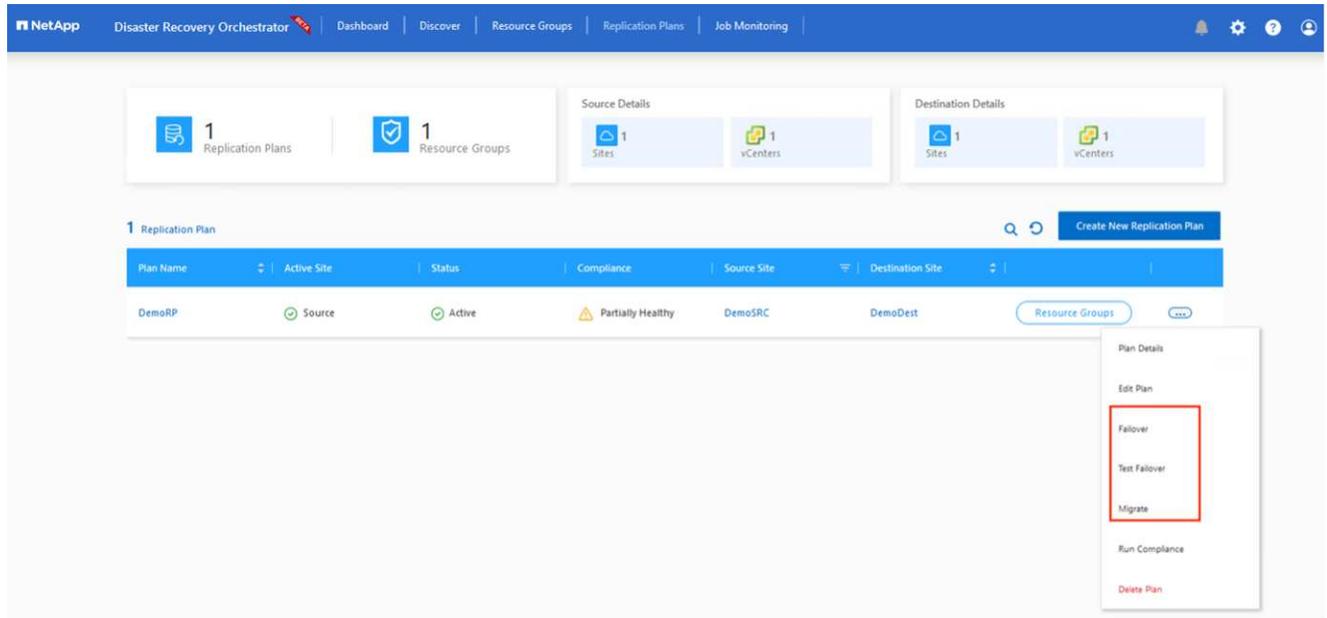
2 VMs

VM Name	No. of CPUs	Memory (MB)	NIC/IP	Boot Order
Resource Group : DemoRG				
QALin1	1	1024	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic	3
QALin	4	1024	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic	3

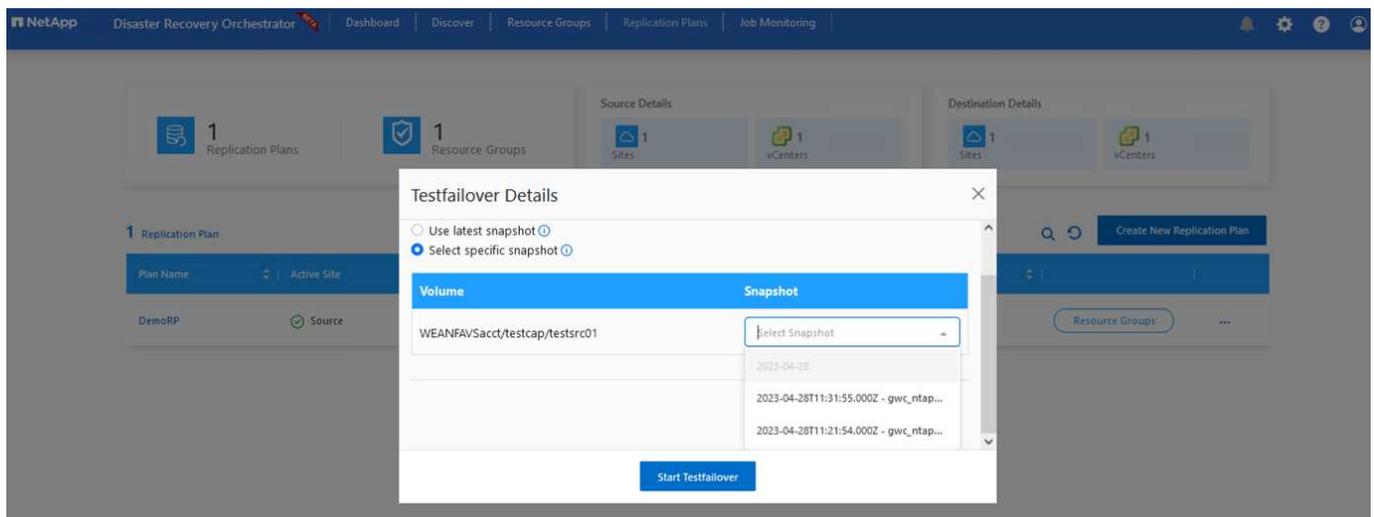
Previous Create Replication Plan

9. レプリケーションプランの作成\*をクリックします。レプリケーションプランの作成後、要件に応じてフ

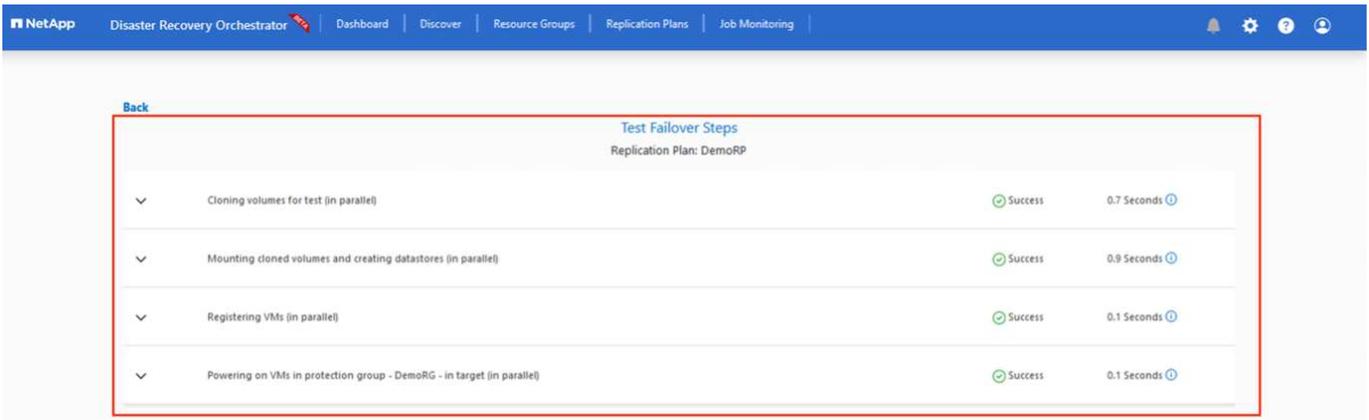
フェイルオーバー、テストフェイルオーバー、移行オプションを実行できます。



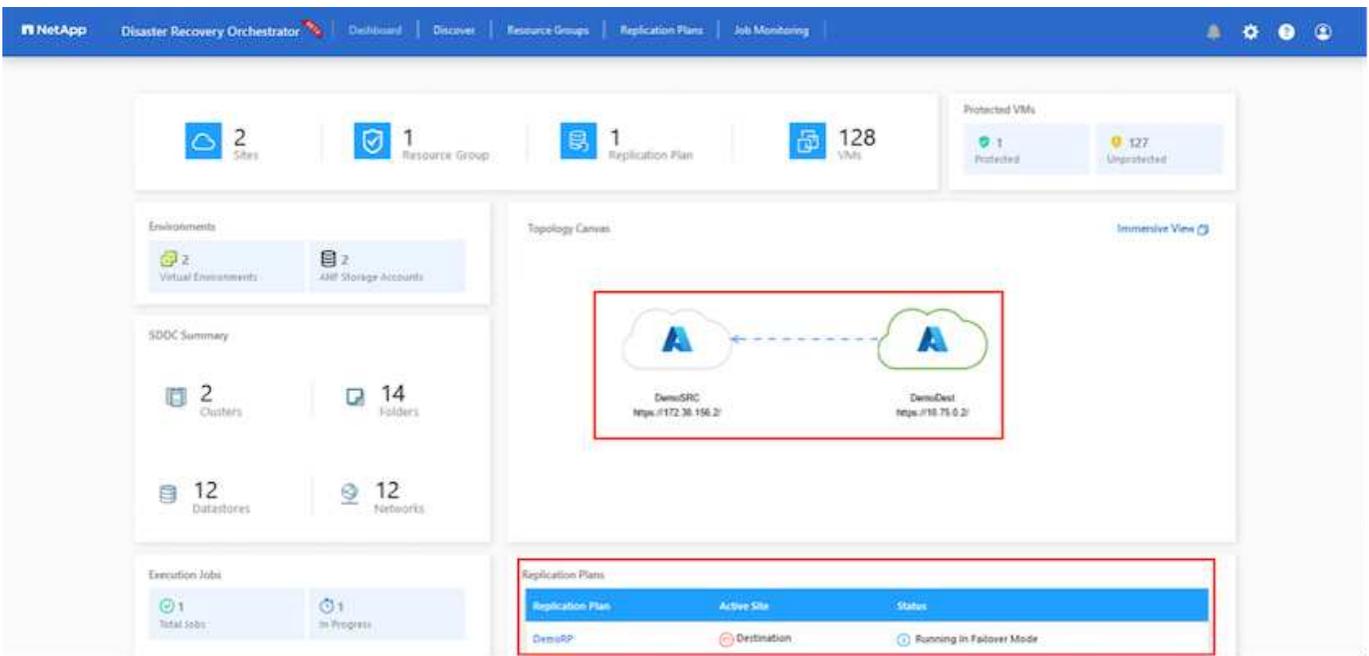
フェイルオーバーオプションとテストフェイルオーバーオプションでは、最新のSnapshotが使用されるか、ポイントインタイムSnapshotから特定のSnapshotを選択できます。ポイントインタイムオプションは、最新のレプリカがすでに侵害または暗号化されているランサムウェアなどの破損イベントに直面している場合に非常に役立ちます。DROには使用可能なすべてのタイムポイントが表示されます。



レプリケーションプランで指定した構成でフェイルオーバーまたはテストフェイルオーバーをトリガーするには、\* Failover または Test Failover \*をクリックします。タスクメニューでレプリケーション計画を監視できます。



フェイルオーバーがトリガーされると、リカバリされた項目がセカンダリサイトのAVS SDDC vCenter（VM、ネットワーク、およびデータストア）に表示されます。デフォルトでは、VMはWorkloadフォルダにリカバリされます。



フェイルバックは、レプリケーションプランレベルでトリガーできます。テストフェイルオーバーの場合は、ティアダウンオプションを使用して変更をロールバックし、新しく作成したボリュームを削除できます。フェイルオーバーに関連するフェイルバックは、2つの手順で構成されます。レプリケーション計画を選択し、\*[Reverse Data sync]\*を選択します。

The screenshot shows the NetApp Disaster Recovery Orchestrator interface. At the top, there are navigation tabs: Dashboard, Discover, Resource Groups, Replication Plans, and Job Monitoring. Below the navigation, there are summary cards for Replication Plans (1), Resource Groups (1), Source Details (1 Sites, 1 vCenters), and Destination Details (1 Sites, 1 vCenters). The main section displays a table of replication plans:

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site	Resource Groups
DemoRP	Destination	Running In Failover Mode	Healthy	DemoSRC	DemoDest	Resource Groups

A dropdown menu for 'Resource Groups' is open, showing options: 'Reverse Data Sync' and 'Failback'. The 'Reverse Data Sync' option is highlighted with a red box.

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。

This screenshot shows the same interface as above, but the status of the 'DemoRP' plan has changed to 'Active'. The 'Reverse Data Sync' option in the dropdown menu is still highlighted with a red box.

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site	Resource Groups
DemoRP	Destination	Active	Healthy	DemoSRC	DemoDest	Resource Groups

This screenshot shows a broader view of the NetApp Disaster Recovery Orchestrator interface. It includes summary cards for Sites (2), Resource Group (1), Replication Plan (1), and VMs (128). There are also cards for Protected VMs (1 Protected, 127 Unprotected), Environments (2 Virtual Environments, 2 ANF Storage Accounts), SDDC Summary (2 Clusters, 14 Folders, 12 Datastores, 12 Networks), and Execution Jobs (3 Total Jobs, 1 In Progress). The 'Topology Canvas' shows a diagram with two Azure cloud icons labeled 'DemoSRC' (https://172.30.156.2) and 'DemoDest' (https://10.75.0.2) connected by an arrow. Below the topology canvas, a table shows the replication plan status:

Replication Plan	Active Site	Status
DemoRP	Source	Active

Azureポータルから、セカンダリサイトのAVS SDDCに読み取り/書き込みボリュームとしてマッピングされた適切なボリュームについて、レプリケーションの健全性が切断されていることを確認できます。テストフェイルオーバー中、DROはデスティネーションボリュームまたはレプリカボリュームをマッピングしません。代

わりに、必要なクロスリージョンレプリケーションSnapshotの新しいボリュームを作成し、そのボリュームをデータストアとして公開します。データストアは容量プールから追加の物理容量を消費し、ソースボリュームが変更されないようにします。特に、DRテスト中やトリアージワークフロー中もレプリケーションジョブを継続できます。さらに、このプロセスにより、エラーが発生した場合や破損したデータがリカバリされた場合にレプリカが破棄されるリスクなしに、リカバリをクリーンアップできます。

#### ランサムウェアからのリカバリ

ランサムウェアからのリカバリは困難な作業です。具体的には、IT部門が安全な回収ポイントを特定し、それが決定されたら、再発生する攻撃（スリープ状態のマルウェアや脆弱なアプリケーションなど）から回復したワークロードを確実に保護する方法を特定することは困難です。

DROは、組織が利用可能な任意の時点からリカバリできるようにすることで、これらの懸念に対処します。その後、ワークロードは機能していても分離されたネットワークにリカバリされるため、アプリケーションは相互に機能して通信できますが、南北方向のトラフィックにはさらされません。このプロセスにより、セキュリティチームはフォレンジックを実行し、隠れたマルウェアや眠っているマルウェアを特定するための安全な場所を提供します。

#### まとめ

Azure NetApp Files とAzure VMwareディザスタリカバリ解決策 には、次のようなメリットがあります。

- 効率的で耐障害性に優れたAzure NetApp Files のリージョン間レプリケーションを活用できます。
- Snapshotの保持機能により、任意の時点までリカバリできます。
- ストレージ、コンピューティング、ネットワーク、アプリケーションの検証に必要なすべての手順を完全に自動化して、数百から数千のVMをリカバリします。
- ワークロードのリカバリでは、「最新のSnapshotから新しいボリュームを作成する」プロセスが利用されます。このプロセスでは、レプリケートされたボリュームは操作されません。
- ボリュームまたはSnapshotのデータ破損のリスクを回避します。
- DRテストワークフロー中のレプリケーションの中断を回避します。
- 開発とテスト、セキュリティテスト、パッチとアップグレードのテスト、修正テストなど、DR以外のワークフローにもDRデータとクラウドコンピューティングリソースを活用できます。
- CPUとRAMを最適化すると、小規模なコンピューティングクラスタへのリカバリが可能になるため、クラウドコストを削減できます。

#### 追加情報の参照先

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

- Azure NetApp Files のボリュームレプリケーションを作成します  
["https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"](https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering)
- Azure NetApp Files のリージョン間レプリケーション  
["https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"](https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives)
- "Azure VMware 解決策の略"

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

- Azure に仮想化環境を導入して設定

["AzureでAVSをセットアップ"](#)

- Azure VMware解決策 を導入して設定

<https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal>

## Veeam ReplicationとAzure NetApp Filesデータストアを使用したAzure VMware解決策へのディザスタリカバリ

Azure NetApp Files (ANF) データストアは、コンピューティングからストレージを切り離し、あらゆる組織がワークロードをクラウドに移行するために必要な柔軟性を実現します。お客様は、コンピューティングリソースとは別に拡張できる、柔軟性に優れたハイパフォーマンスなストレージインフラを利用できます。Azure NetApp Filesデータストアのは、オンプレミスのVMware環境のディザスタリカバリサイトとしてAzure VMware解決策 (AVS) とともに導入を簡易化、最適化します。

作成者：Niyaz Mohamed - NetAppソリューションエンジニアリング

### 概要

Azure NetApp Files (ANF) ボリュームベースのNFSデータストアを使用すると、VMレプリケーション機能を提供する検証済みのサードパーティ製解決策を使用して、オンプレミスからデータをレプリケートできます。Azure NetApp Filesデータストアを追加することで、ストレージに対応する膨大な量のESXiホストでAzure VMware解決策SDDCを構築するよりも、コストを最適化できます。このアプローチは「パイロットライトクラスタ」と呼ばれます。パイロットライトクラスタは、Azure NetApp Filesデータストアの容量に加えて、最小限のAVSホスト構成 (AVSノード×3) です。

その目的は、フェイルオーバーを処理するためのすべてのコアコンポーネントを備えた低コストのインフラストラクチャを維持することです。パイロットライトクラスタは、フェイルオーバーが発生した場合に、スケールアウトしてより多くのAVSホストをプロビジョニングできます。また、フェールオーバーが完了し、通常の動作が復元されると、パイロットライトクラスタは低コストの動作モードにスケールダウンできます。

### 本書の目的

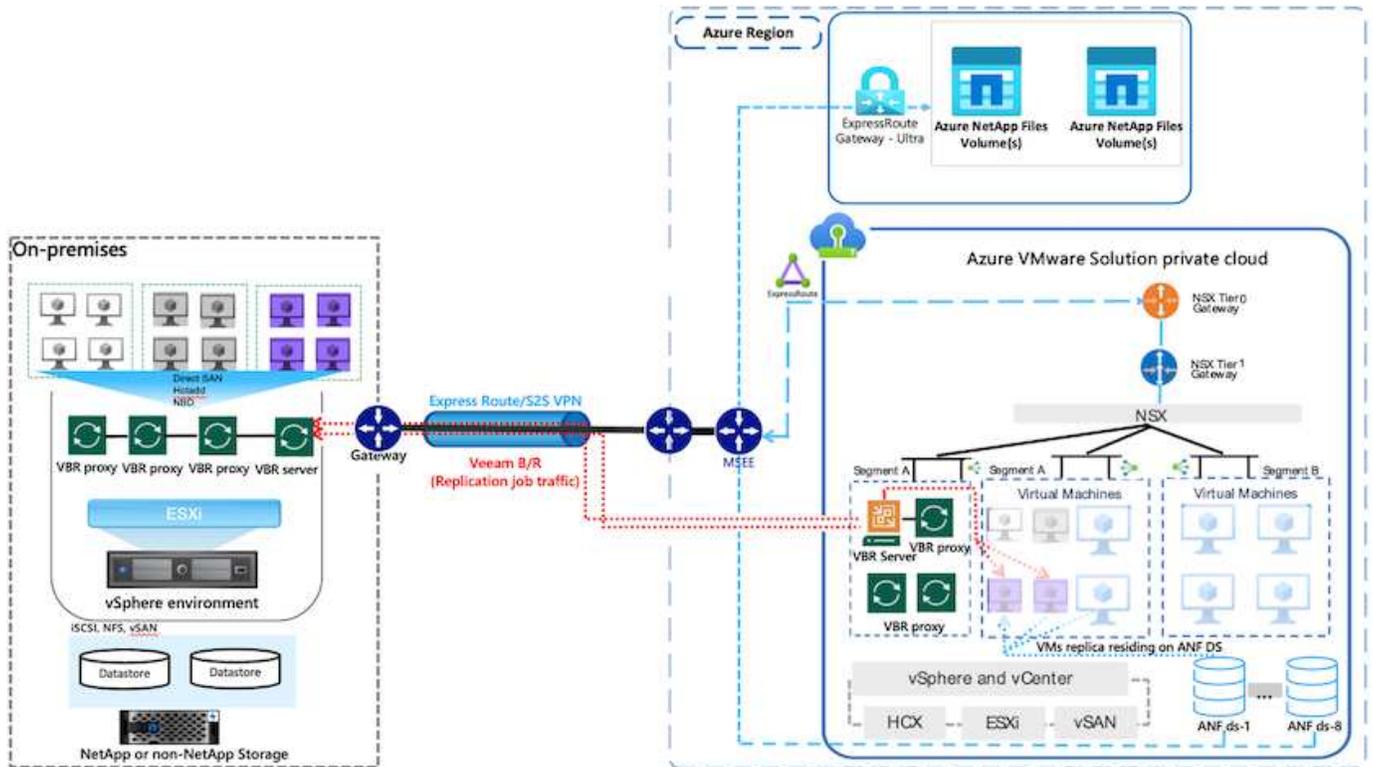
この記事では、Azure NetApp FilesデータストアとVeeam Backup and Replicationを使用して、Veeam VMレプリケーションソフトウェア機能を使用してオンプレミスのVMware VMから (AVS) へのディザスタリカバリを設定する方法について説明します。

Veeam Backup & Replicationは、仮想環境向けのバックアップおよびレプリケーションアプリケーションです。仮想マシンがレプリケートされると、Veeam Backup & ReplicationがAVS上からレプリケートされます。ソフトウェアは、ターゲットAVS SDDCクラスタに、ネイティブのVMware vSphere形式でVMの正確なコピーを作成します。Veeam Backup & Replicationは、コピーと元のVMの同期を維持します。DRサイトにはVMのコピーがすぐにマウントされているため、レプリケーションによって最適なRecovery Time Objective (RTO; 目標復旧時間) が実現します。

このレプリケーションメカニズムにより、災害発生時にAVS SDDCでワークロードを迅速に開始できます。Veeam Backup & Replicationソフトウェアは、WAN経由のレプリケーションや低速接続のトラフィック

転送も最適化します。また、重複データブロック、ゼロデータブロック、スワップファイル、「除外VMゲストOSファイル」も除外されます。ソフトウェアはレプリカトラフィックも圧縮します。レプリケーションジョブがネットワーク帯域幅全体を消費しないようにするには、WANアクセラレータとネットワークスロットリングルールを使用します。

Veeam Backup & Replicationのレプリケーションプロセスはジョブベースです。つまり、レプリケーションはレプリケーションジョブを設定して実行されます。災害が発生した場合は、レプリカコピーにフェイルオーバーすることで、フェイルオーバーをトリガーしてVMをリカバリできます。フェイルオーバーが実行されると、レプリケートされたVMが元のVMの役割を引き継ぎます。フェイルオーバーはレプリカの最新の状態または既知の任意のリストア・ポイントに対して実行できますこれにより、必要に応じてランサムウェアからのリカバリや個別のテストが可能Veeam Backup & Replicationには、さまざまなディザスタリカバリシナリオに対応するためのオプションが複数用意されています。



## 解決策の導入

### 手順の概要

1. Veeam Backup & Replicationソフトウェアは、適切なネットワーク接続を備えたオンプレミス環境で実行されます。
2. "Azure VMware解決策 (AVS) の導入" プライベートクラウドと "Azure NetApp Filesデータストアの接続" Azure VMware解決策ホストに接続します。

最小限の構成でセットアップされたパイロットライト環境は、DR目的で使用できます。インシデントが発生した場合、VMはこのクラスタにフェイルオーバーし、ノードを追加できます。

3. Veeam Backup and Replicationを使用してVMレプリカを作成するためのレプリケーションジョブを設定します。
4. フェイルオーバープランを作成し、フェイルオーバーを実行

5. 災害が完了し、プライマリサイトが稼働したら、本番環境のVMにスイッチバックします。

#### AVSおよびANFデータストアへのVeeam VMレプリケーションの前提条件

1. Veeam Backup & ReplicationバックアップVMがソースとターゲットのAVS SDDCクラスタに接続されていることを確認します。
2. バックアップサーバは、短縮名を解決し、ソースvCenterとターゲットvCenterに接続できる必要があります。
3. ターゲットのAzure NetApp Filesデータストアに、レプリケートされたVMのVMDKを格納できるだけの十分な空きスペースが必要です。

追加情報については、「考慮事項と制限事項」を参照してください。 ["こちらをご覧ください"](#)。

展開の詳細

## ステップ1：VMのレプリケート

Veeam Backup & ReplicationはVMware vSphereスナップショット機能を活用します。レプリケーション時に、Veeam Backup & ReplicationはVMware vSphereにVMスナップショットの作成を要求します。VMスナップショットは、仮想ディスク、システムの状態、設定、メタデータを含むVMのポイントインタイムコピーです。Veeam Backup & Replicationでは、Snapshotをレプリケーションのデータソースとして使用します。

VMをレプリケートするには、次の手順を実行します。

1. Veeam Backup & Replicationコンソールを開きます。
2. をクリックします。ジョブノードを右クリックし、[Replication Job]>[Virtual machine]を選択します。
3. ジョブ名を指定し、適切な詳細制御チェックボックスを選択します。次へをクリックします。
  - オンプレミスとAzure間の接続で帯域幅が制限されている場合は、[Replica seeding]チェックボックスをオンにします。
    - Azure VMware解決策SDDCのセグメントがオンプレミスサイトネットワークのセグメントと一致しない場合は、[ネットワークの再マッピング(AVS SDDCサイトと異なるネットワークの場合)]チェックボックスをオンにします。
  - オンプレミスの本番サイトのIPアドレス指定方式がターゲットAVSサイトのIPアドレス指定方式と異なる場合は、Replica Re-IP (異なるIPアドレス指定方式を使用するDRサイトの場合) チェックボックスを選択します。

**Name**  
Specify the name and description for this job, and provide information on your DR site.

**Name:**  
AVS\_20230522\_RepJob01

**Description:**  
Created by VEEAMBKPSRV05\Administrator at 5/21/2023 10:52 PM.

**Show advanced controls:**

- Replica seeding (for low bandwidth DR sites)
- Network remapping (for DR sites with different virtual networks)
- Replica re-IP (for DR sites with different IP addressing scheme)

High priority  
Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.

< Previous **Next >** Finish Cancel

4. [Virtual \* Machines]手順で、Azure VMware解決策SDDCに接続されたAzure NetApp FilesデータストアにレプリケートするVMを選択します。仮想マシンをVSANに配置して、使用可能なVSANデータストアの容量をいっぱいにすることができます。パイロットライトクラスタでは、3ノードクラスタの

使用可能容量が制限されます。残りのデータはAzure NetApp Filesデータストアに簡単に配置してVMをリカバリしたり、CPU /メモリの要件に合わせてクラスタを拡張したりできます。をクリックし、[オブジェクトの追加]ウィンドウで必要な**VM**または**VMコンテナ**を選択して[追加]\*をクリックします。「\*次へ\*」をクリックします。

**Virtual Machines**  
Select one or more VMs to replicate. Use exclusion settings to exclude specific VMs and virtual disks from replication.

Name	Type	Size
TestVeeam21	Virtual Machine	873 MB
TestVeeam22	Virtual Machine	890 MB
TestVeeam23	Virtual Machine	883 MB
TestVeeam24	Virtual Machine	879 MB
TestVeeam25	Virtual Machine	885 MB
TestVeeam26	Virtual Machine	883 MB
TestVeeam27	Virtual Machine	879 MB
TestVeeam28	Virtual Machine	880 MB
TestVeeam29	Virtual Machine	878 MB
TestVeeam30	Virtual Machine	876 MB
TestVeeam31	Virtual Machine	888 MB
TestVeeam32	Virtual Machine	881 MB
TestVeeam33	Virtual Machine	877 MB
TestVeeam34	Virtual Machine	875 MB
TestVeeam35	Virtual Machine	882 MB
WinSQL401	Virtual Machine	20.3 GB
WinSQL405	Virtual Machine	24.2 GB

Total size: 120 GB

< Previous   **Next >**   Finish   Cancel

- その後、デスティネーションをAzure VMware解決策SDDCクラスター/ホストとして選択し、VMレプリカ用の適切なリソースプール、VMフォルダ、FSx for ONTAPデータストアを選択します。次に、[\*次へ\*]をクリックします。



- [ジョブ設定]ステップで、VMレプリカのメタデータや保持ポリシーなどを格納するバックアップリポジトリを指定します。
- Data Transfer（データ転送）ステップで\* Source（ソース）および Target（ターゲット）プロキシサーバーを更新し、Automatic（自動）選択（デフォルト）のままにして Direct オプションを選択したままにして Next（次へ）\*をクリックします。
- [Guest Processing]ステップで、必要に応じて[Enable application-aware processing]オプションを選択します。「\* 次へ \*」をクリックします。

**Guest Processing**  
Choose guest OS processing options available for running VMs.

Name

Virtual Machines

Destination

Network

Job Settings

Data Transfer

**Guest Processing**

Schedule

Summary

**Enable application-aware processing**  
Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications Applications...

Guest interaction proxy:  
Automatic selection Choose...

Guest OS credentials:  
Add...

Manage accounts  
Customize guest OS credentials for individual machines and operating systems Credentials...

Verify network connectivity and credentials for each machine included in the job Test Now

< Previous Next > Finish Cancel

- レプリケーションジョブを定期的に行うレプリケーションスケジュールを選択します。



## Schedule

Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

**Name**

**Virtual Machines**

**Destination**

**Network**

**Job Settings**

**Data Transfer**

**Guest Processing**

**Schedule**

**Summary**

Run the job automatically

Daily at this time: 10:00 PM Everyday Days...

Monthly at this time: 10:00 PM Fourth Saturday Months...

Periodically every: 1 Hours Schedule...

After this job: Replication Job 2 (Created by VEEAMBKPSRV05\Administrator at 6/6/ )

**Automatic retry**

Retry failed items processing: 3 times

Wait before each retry attempt for: 10 minutes

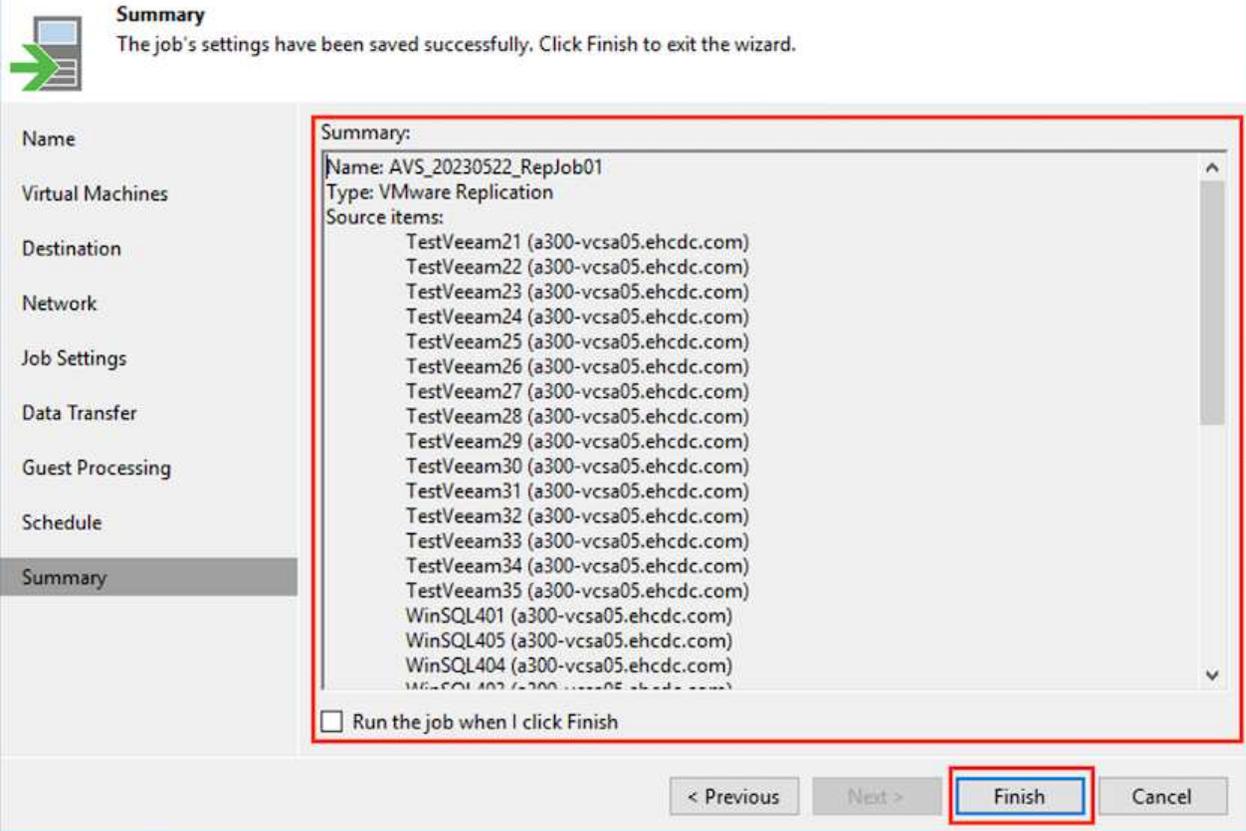
**Backup window**

Terminate job if it exceeds allowed backup window Window...

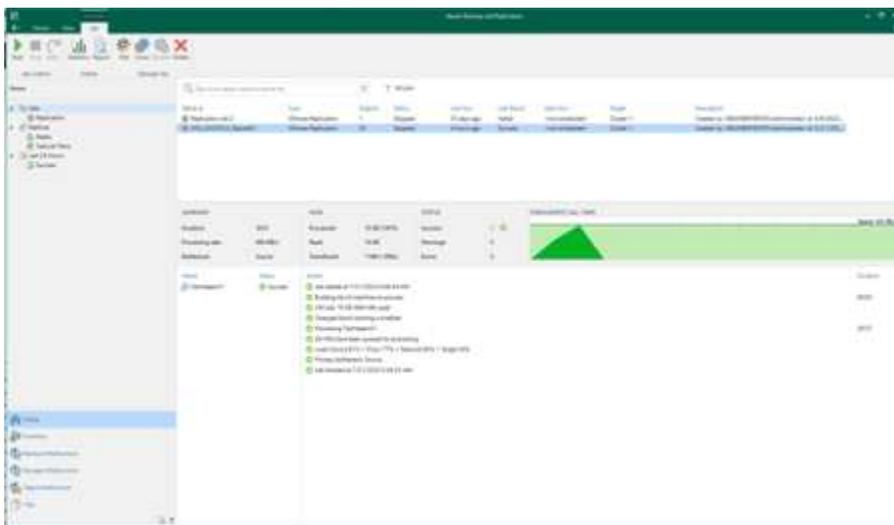
If the job does not complete within allocated backup window, it will be terminated to prevent snapshot commit during production hours.

< Previous Apply Finish Cancel

11. ウィザードの\* Summary ステップで、レプリケーションジョブの詳細を確認します。ウィザードを終了した直後にジョブを開始するには、[完了]をクリックしたときにジョブを実行する\*チェックボックスをオンにします。オンにしない場合は、チェックボックスをオフのままにします。次に、\*[完了]\*をクリックしてウィザードを閉じます。



レプリケーションジョブが開始されると、指定されたサフィックスのVMがデスティネーションAVS SDDCクラスタ/ホストに取り込まれます。



追加情報によるVeeamレプリケーションについては、"レプリケーションの仕組み"

## 手順2：フェイルオーバープランを作成する

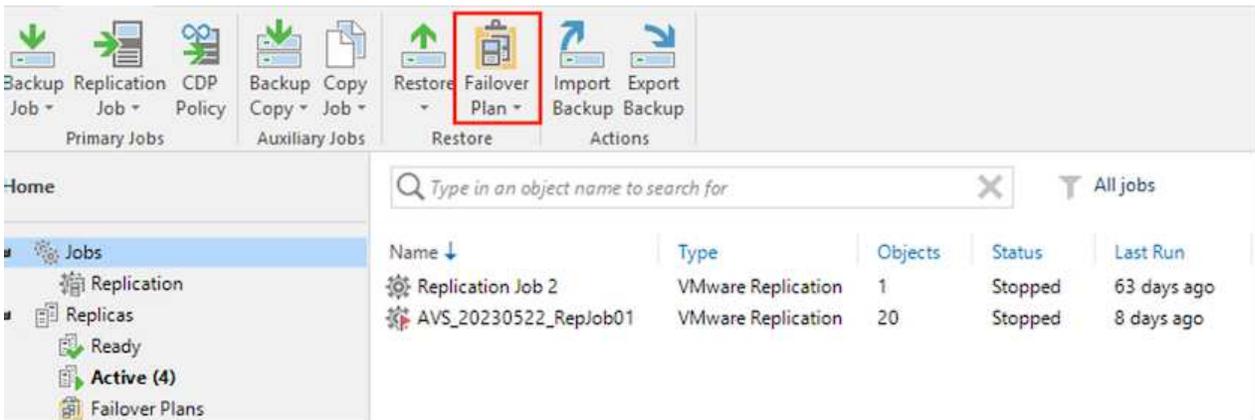
最初のレプリケーションまたはシードが完了したら、フェイルオーバープランを作成します。フェイルオーバープランは、依存するVMのフェイルオーバーを1つずつ、またはグループとして自動的に実行するのに役立ちます。フェイルオーバープランは、ブート遅延を含むVMの処理順序の青写真です。フェイルオーバープランは、重要な依存VMがすでに実行されていることを確認するのに役立ちます。

プランを作成するには、\*レプリカ\*という新しいサブセクションに移動し、\*フェイルオーバープラン\*を選択します。適切なVMを選択します。Veeam Backup & Replicationは、この時点に最も近いリストアポイントを検索し、それらを使用してVMレプリカを開始します。

-  フェイルオーバープランを追加できるのは、初期レプリケーションが完了し、VMレプリカがReady状態になってからです。
-  フェイルオーバープランの実行時に同時に起動できるVMの最大数は10です。
-  フェイルオーバープロセス中は、ソースVMの電源はオフになりません。

フェイルオーバープラン\*を作成するには、次の手順を実行します。

1. をクリックします。レプリカノードを右クリックし、[Failover Plans]>[Failover Plan]>[VMware vSphere]を選択します。



2. 次に、計画の名前と概要を入力します。必要に応じて、フェイルオーバー前およびフェイルオーバー後のスクリプトを追加できます。たとえば、スクリプトを実行して、レプリケートされたVMを起動する前にVMをシャットダウンします。

Edit Failover Plan [ANF\_AVS\_FP01] ×

**General**  
Type in name and description for this failover plan, and optionally specify scripts to trigger before and after the failover.

**General**  
Virtual Machines  
Summary

Name: ANF\_AVS\_FP01

Description: Created by VEEAMBKPSRV05\Administrator at 5/24/2023 9:08 AM.

Pre-failover script:  
 Browse...

Post-failover script:  
 Browse...

< Previous Next > Finish Cancel

3. VMを計画に追加し、VMのブート順序とブート遅延を変更して、アプリケーションの依存関係を満たすようにします。

Edit Failover Plan [ANF\_AVS\_FP01] X

 **Virtual Machines**  
Add virtual machines to be failed over as a part of this plan. Use VM order and delays to ensure all application dependencies are met.

General

Virtual Machines

Summary

Virtual machines:

Name	Delay	Replica state
TestVeeam21	2 sec	63 days ago (5:52 AM T...
TestVeeam23	2 sec	7 days ago (10:12 AM T...
TestVeeam24	2 sec	7 days ago (10:20 AM T...
TestVeeam22	2 sec	7 days ago (10:10 AM T...
WinSQL401	2 sec	7 days ago (3:52 AM Tu...
WinSQL405	2 sec	8 days ago (4:05 PM Mo...
TestVeeam25	2 sec	7 days ago (10:14 AM T...
TestVeeam26	2 sec	7 days ago (10:17 AM T...
TestVeeam27	2 sec	7 days ago (10:18 AM T...
TestVeeam28	2 sec	7 days ago (10:14 AM T...
TestVeeam29	2 sec	7 days ago (10:18 AM T...
TestVeeam30	2 sec	7 days ago (10:15 AM T...
TestVeeam31	2 sec	7 days ago (10:21 AM T...
TestVeeam32	2 sec	7 days ago (10:13 AM T...
TestVeeam33	2 sec	7 days ago (10:15 AM T...
TestVeeam34	2 sec	7 days ago (10:14 AM T...
TestVeeam35	2 sec	7 days ago (10:20 AM T...

Buttons: Add VM, Remove, Set Delay..., Up, Down

Bottom buttons: < Previous, Apply, Finish, Cancel

レプリケーションジョブを作成するための追加情報については、を参照してください。"[レプリケーションジョブの作成](#)"。

### 手順3：フェイルオーバープランを実行する

フェイルオーバー時には、本番サイトのソースVMがディザスタリカバリサイトのレプリカにスイッチオーバーされます。フェイルオーバープロセスの一環として、Veeam Backup & ReplicationはVMレプリカを必要なリストアポイントにリストアし、すべてのI/OアクティビティをソースVMからそのレプリカに移動します。レプリカは、災害発生時だけでなく、DRドリルのシミュレーションにも使用できます。フェイルオーバーのシミュレーション中は、ソースVMは引き続き実行されます。必要なテストがすべて完了したら、フェイルオーバーを元に戻して通常の運用に戻すことができます。



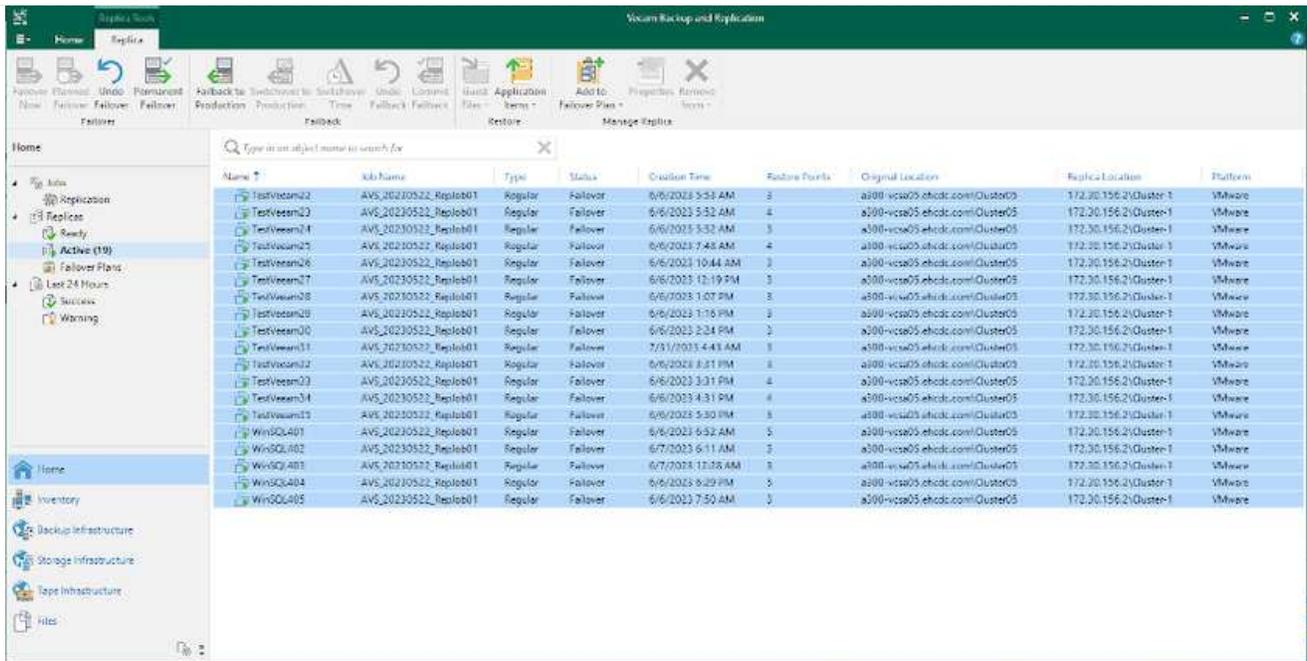
フェイルオーバー中のIP競合を回避するために、ネットワークセグメンテーションが設定されていることを確認します。

フェイルオーバープランを開始するには、\* Failover Plans タブをクリックし、フェイルオーバープランを右クリックします。[\*Start]を選択します。これにより、VMレプリカの最新のリストアポイントを使用してフェイルオーバーが実行されます。VMレプリカの特定のリストアポイントにフェイルオーバーするには、\* Start to \*を選択します。

The screenshot shows the Veeam Backup & Replication console. At the top, there is a toolbar with icons for Start, Start to..., Retry, Undo, Statistics, Edit, and Delete. Below the toolbar, the 'Home' view is visible, with a sidebar on the left containing a tree view of 'Jobs', 'Replication', 'Replicas', 'Ready', 'Active (4)', 'Failover Plans', 'Last 24 Hours', and 'Success'. The main area displays a table of failover plans. The first row is selected, and a context menu is open over it. The menu items are Start, Start to..., Undo, Statistics, Delete, and Edit... The 'Start' and 'Start to...' items are highlighted with a red box.

Name ↑	Platform	Status	Number of VMs
ANF_AVS_FP01	VMware	Completed	20





Veeam Backup & Replicationは、レプリカがReady状態に戻るまで、ソースVMのすべてのレプリケーションアクティビティを停止します。

フェイルオーバープランの詳細については、を参照してください。"フェイルオーバープラン"。

#### 手順4：本番サイトへのフェイルバック

フェイルオーバーの実行中は中間ステップとみなされ、要件に基づいて確定する必要があります。オプションには次のものがあります。

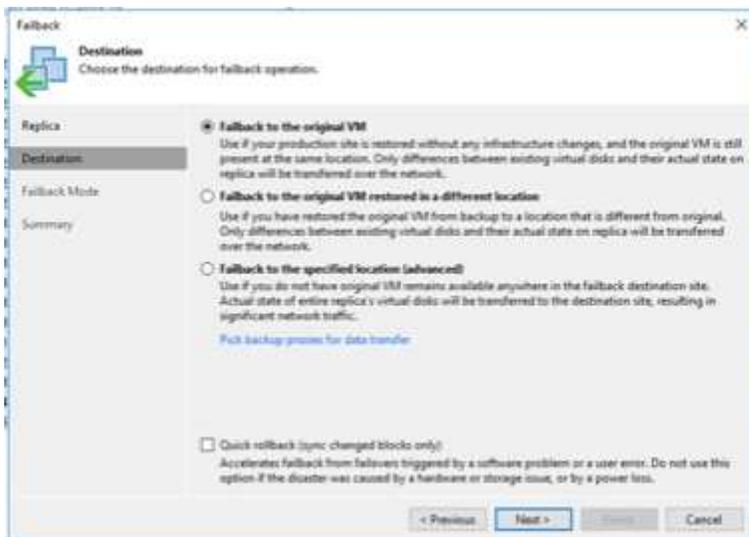
- 本番環境へのフェイルバック：元のVMに切り替えて、VMレプリカの実行中に発生したすべての変更を元のVMに転送します。

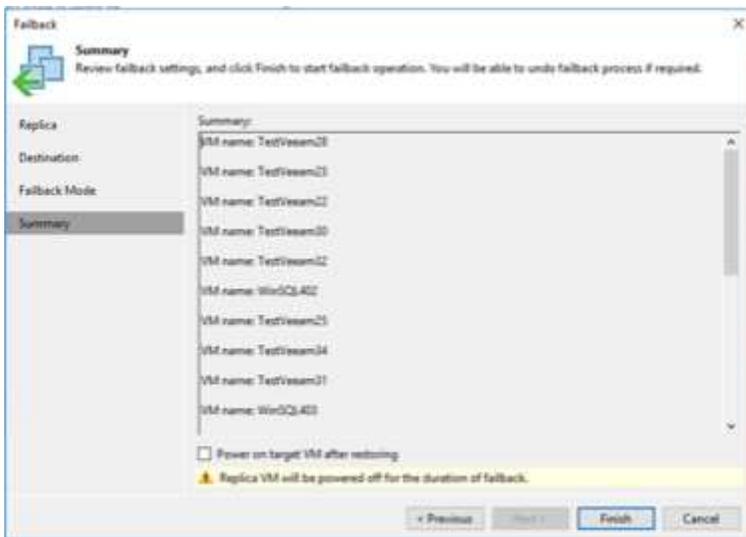
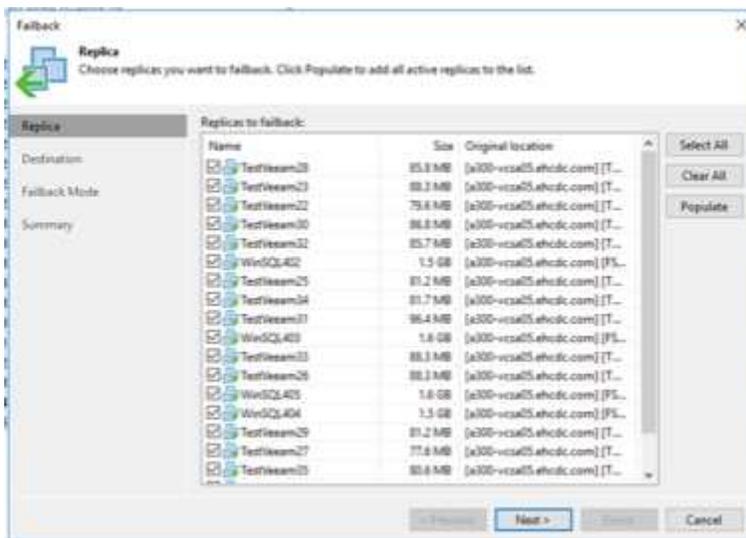
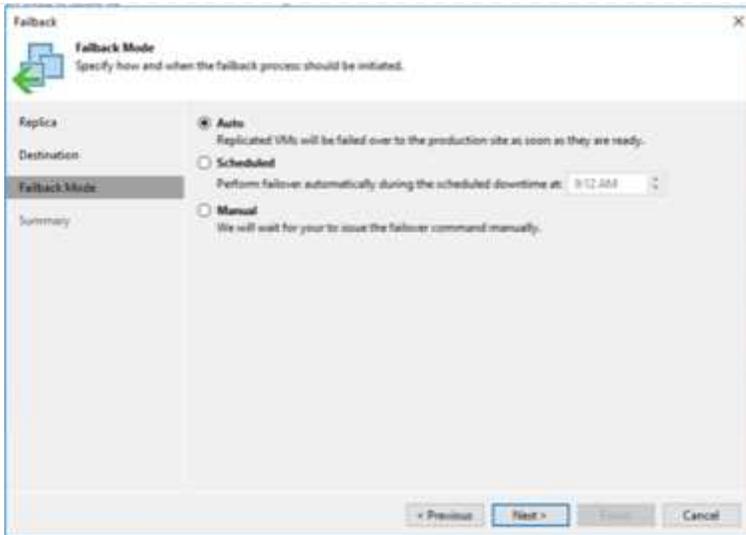


フェイルバックを実行すると、変更は転送されますが、パブリッシュされません。[Commit failback]\*（元のVMが期待どおりに動作することが確認されたら）または[Undo failback]を選択して、元のVMが期待どおりに動作していない場合はVMレプリカに戻ります。

- フェイルオーバーを元に戻す-元のVMに切り替えて、VMレプリカの実行中に行った変更をすべて破棄します。
- 永続的フェイルオーバー-元のVMからVMレプリカに永続的に切り替え、このレプリカを元のVMとして使用します。

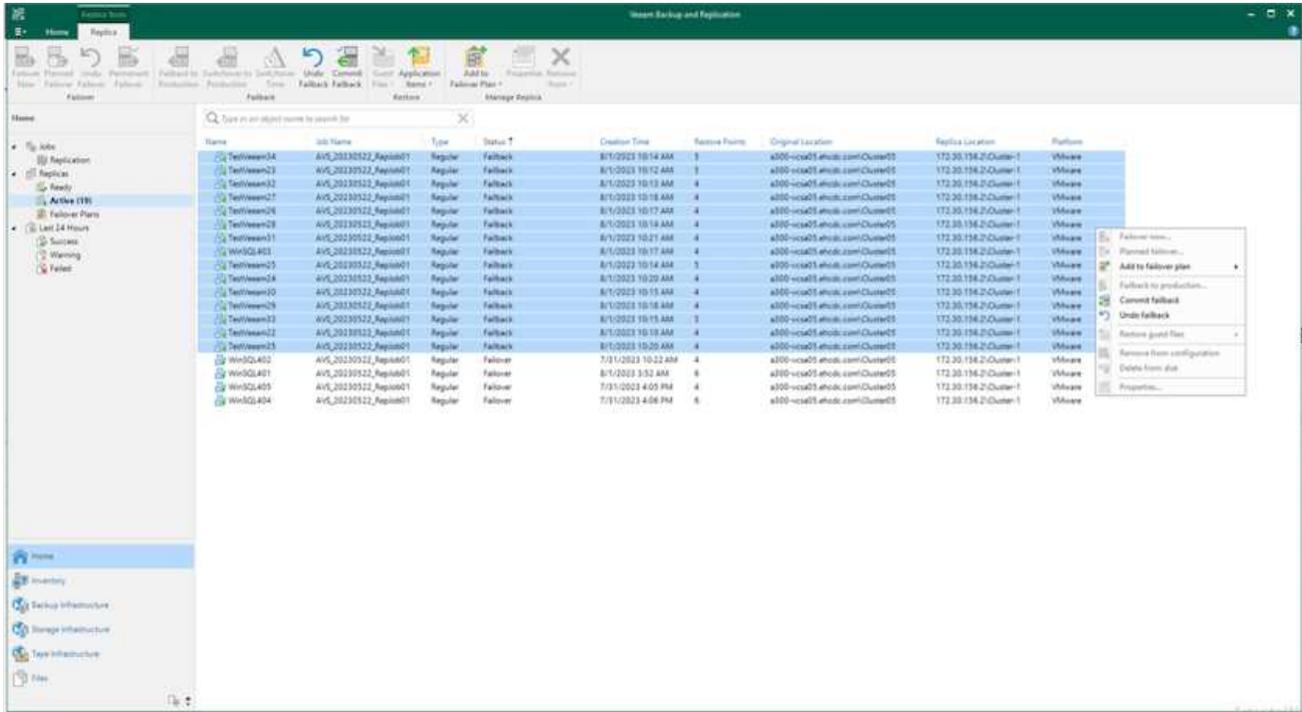
このデモでは、本番環境へのフェイルバックを選択しました。ウィザードの[Destination]ステップで[Failback to the original VM]が選択され、[Power on VM after restoring]チェックボックスが有効になっている。



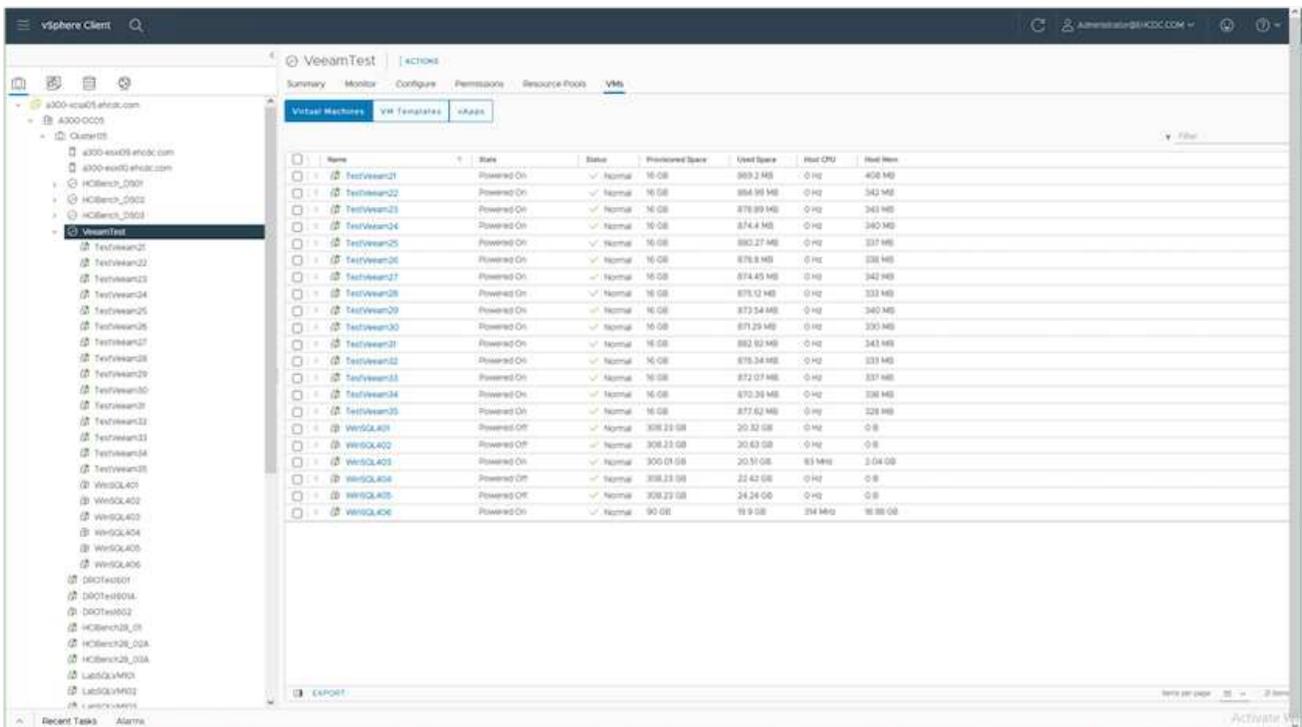


フェイルバックコミットは、フェイルバック操作を完了する方法の1つです。フェイルバックがコミットされると、フェイルバックされたVM（本番VM）に送信された変更が想定どおりに機能していることが確認されます。コミット処理が完了すると、Veeam Backup & Replicationは本番用VMのレプリケーションアクティビティを再開します。

フェイルバックプロセスの詳細については、次のVeeamのドキュメントを参照してください："[レプリケーションのフェイルオーバーとフェイルバック](#)"。



本番環境へのフェイルバックが成功すると、VMはすべて元の本番サイトにリストアされます。



## まとめ

Azure NetApp Filesデータストア機能を使用すると、Veeamまたは検証済みのサードパーティ製ツールを使用して、VMレプリカに対応するためだけに大規模なクラスタをセットアップするのではなく、パイロットライ

トクラスタを活用して低コストのDR解決策を提供できます。これにより、カスタマイズされたディザスタリカバリ計画を効率的に処理し、社内の既存のバックアップ製品をDR用に再利用できるようになり、オンプレミスのDRデータセンターを終了してクラウドベースのディザスタリカバリを実現できます。災害の場合はボタンをクリックしてフェイルオーバーしたり、災害が発生した場合は自動的にフェイルオーバーすることができます。

このプロセスの詳細については、詳細なウォークスルービデオをご覧ください。

<https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278>

## Azure / AVSでのワークロードの移行

### TR-4640 : 『VMware HCX-Quickstart guide』を使用してワークロードをAzure NetApp Files データストアに移行する

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

執筆者 : NetApp Solutions Engineering

**概要 :** VMware HCX、Azure NetApp Files データストア、Azure VMware解決策 を使用した仮想マシンの移行

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

このドキュメントでは、Azure NetApp Files データストアのプロビジョニングの手順を追ったガイダンスを示し、その後、さまざまなVM移行メカニズムを有効にするためのインターコネクト、ネットワーク拡張、WAN最適化を含む、オンプレミスおよびAzure VMware解決策 サイドのすべての主要コンポーネントを含む、VMware HCXのダウンロード、導入、設定を行います。



VMware HCXはVMレベルで移行されるため、どのデータストアタイプでも動作します。このドキュメントAzure NetApp Files は、解決策 コスト効率に優れたVMwareクラウドの導入を計画している、ネットアップの既存のお客様と、ネットアップ以外のお客様を対象としています。

## 手順の概要

次のリストは、Azureクラウド側でHCX Cloud Managerをインストールおよび設定し、オンプレミスでHCX Connectorをインストールするために必要な手順の概要を示しています。

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

## 前提条件

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

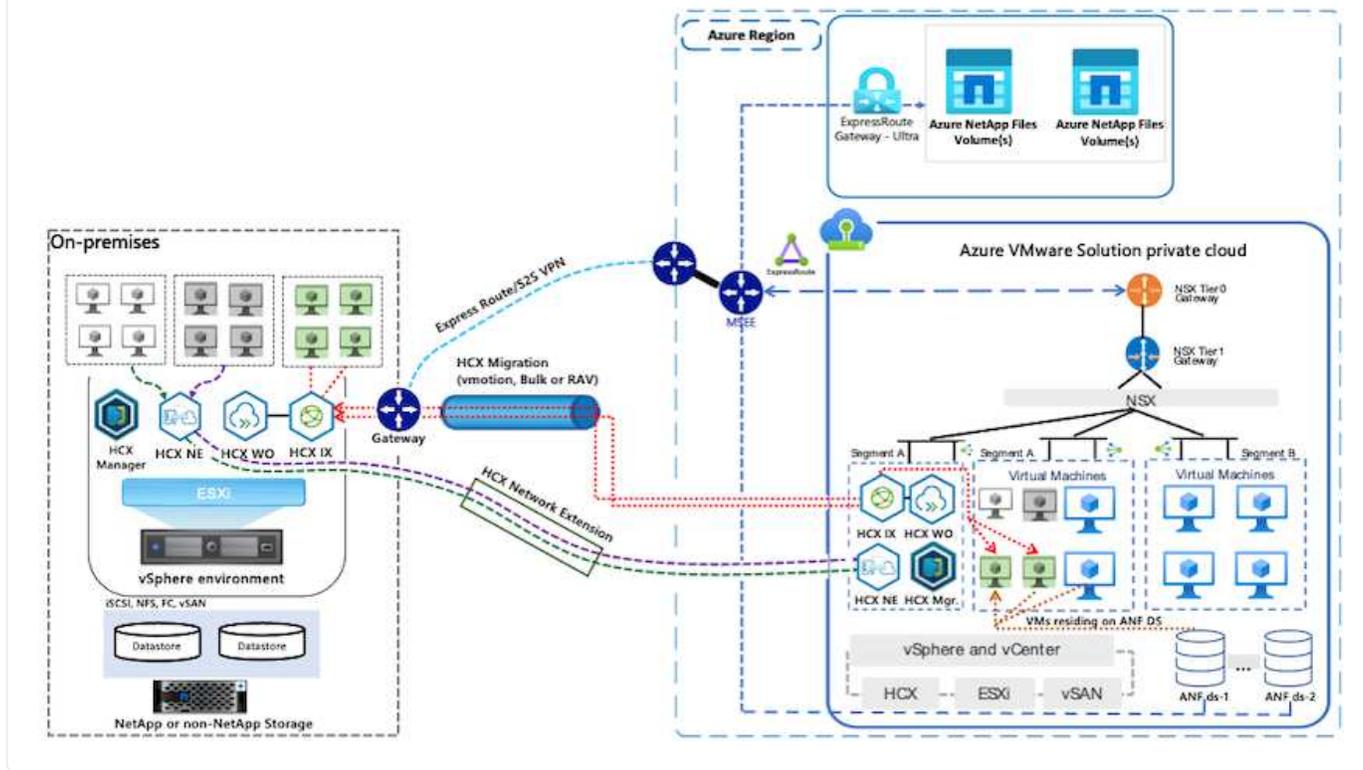


HCx advancedはデフォルトオプションであり、VMware HCX Enterprise Editionはサポートチケットを通じても利用でき、追加料金なしでサポートされます。

- 既存のAzure VMware解決策 Software-Defined Data Center (SDDC) を使用するか、またはこれを使用してプライベートクラウドを作成します ["ネットアップのリンク"](#) またはこれ ["Microsoftのリンク"](#)。
- オンプレミスのVMware vSphere対応データセンターからVMと関連データを移行するには、データセンターからSDDC環境へのネットワーク接続が必要です。ワークロードを移行する前に、["サイト間VPNまたはエクスプレスルートグローバルリーチ接続をセットアップします"](#) オンプレミス環境とそれぞれのプライベートクラウドの間。
- オンプレミスのVMware vCenter Server環境からAzure VMware解決策 プライベートクラウドへのネットワークパスで、vMotionを使用したVMの移行がサポートされている必要があります。
- 必要な確認します ["ファイアウォールルールとポート"](#) オンプレミスのvCenter ServerとSDDC vCenter間のvMotionトラフィックに許可されます。プライベートクラウドでは、vMotionネットワーク上のルーティングはデフォルトで設定されます。
- Azure NetApp Files NFSボリュームは、Azure VMware解決策 でデータストアとしてマウントする必要があります。詳細な手順を実行します ["リンク"](#) を使用して、Azure NetApp Files データストアをAzure VMwareソリューションホストに接続します。

## アーキテクチャの概要

テスト目的で、この検証に使用したオンプレミスのラボ環境はサイト間VPNを介して接続されており、オンプレミスでAzure VMware解決策に接続できます。



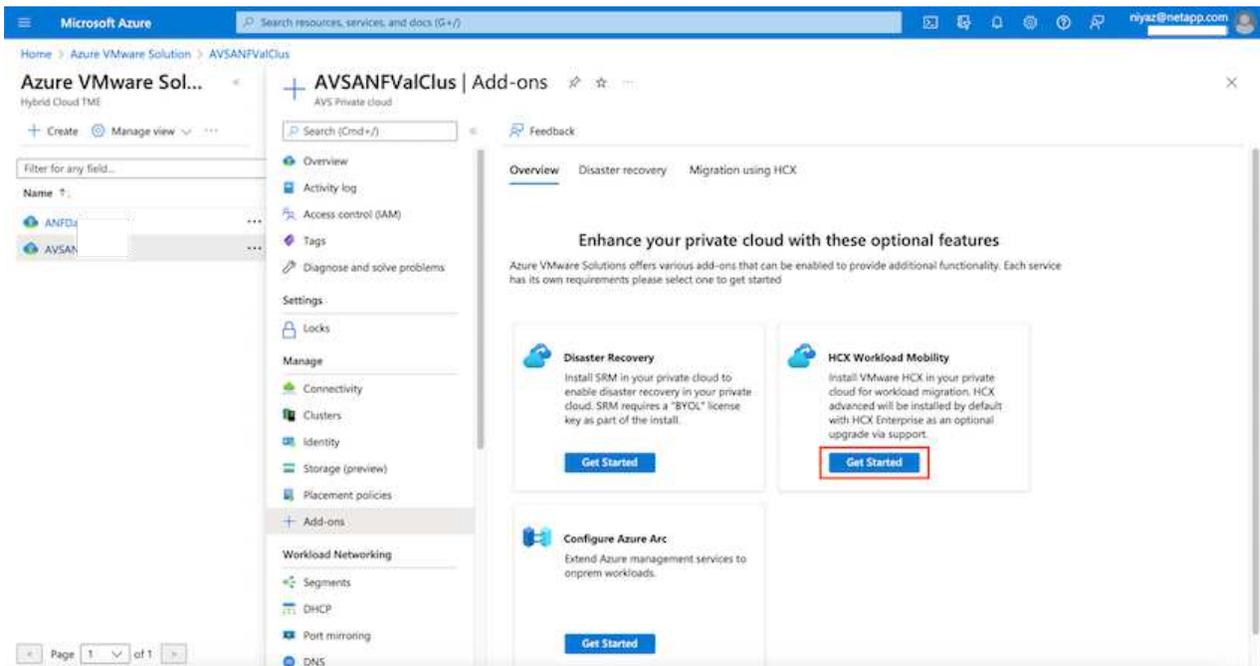
## 解決策の導入

一連の手順に従って、この解決策の導入を完了します。

## 手順1：アドオンオプションを使用して、Azure PortalからHCXをインストールする

インストールを実行するには、次の手順を実行します。

1. Azureポータルにログインし、Azure VMware解決策 プライベートクラウドにアクセスします。
2. 適切なプライベートクラウドを選択し、アドオンにアクセスします。これを行うには、\* Manage > Add-ons \*に移動します。
3. [HCX Workload Mobility]セクションで、[\* Get Started\*]をクリックします。



セクションのスクリーンショット。"]

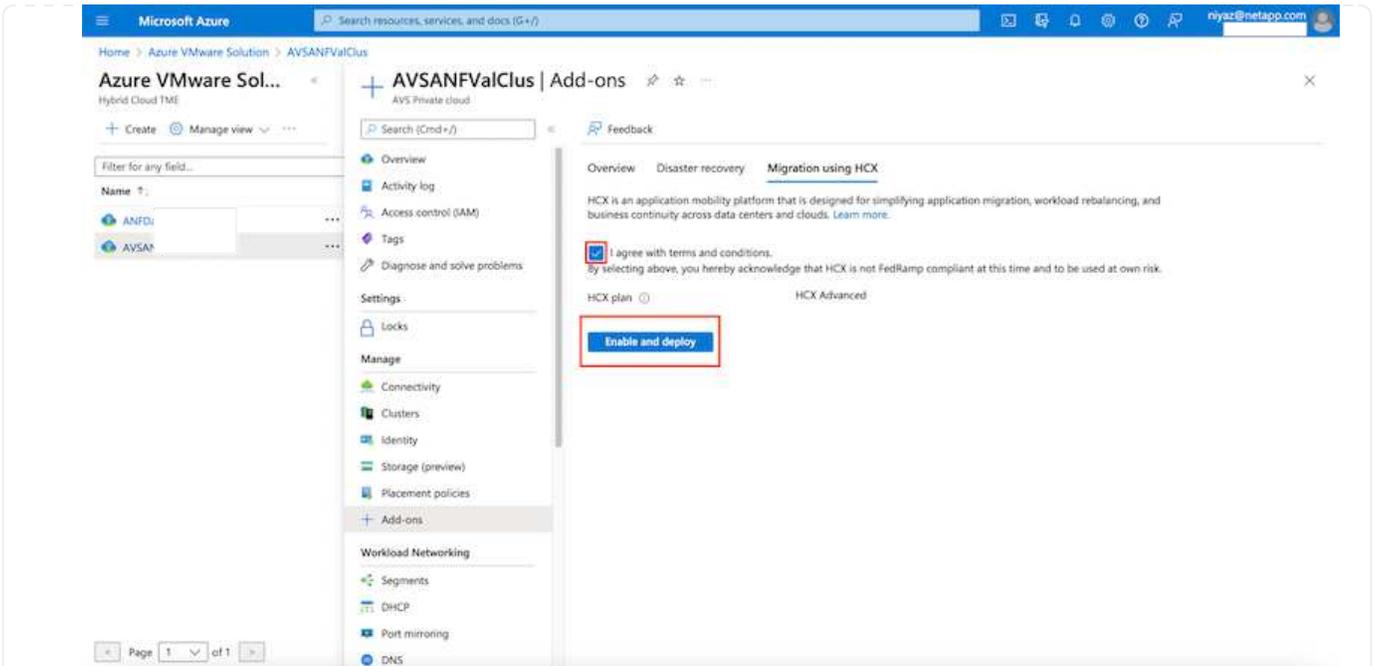
4. [契約条件に同意します]オプションを選択し、[有効化して展開]をクリックします。



デフォルトの展開はHCX Advancedです。エンタープライズエディションを有効にするには、サポートリクエストを開きます。



導入には約25～30分かかります。



セクションの完了のスクリーンショット。"]

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

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

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

1. AzureポータルからAzure VMware解決策にアクセスし、プライベートクラウドを選択して、\* Manage > Add-ons > Migration \* using HCXを選択し、HCX Cloud ManagerポータルをコピーしてOVAファイルをダウンロードします。



HCXポータルにアクセスするには、デフォルトのCloudAdminユーザー資格情報を使用します。

The screenshot shows the Azure portal interface for configuring HCX migration. The main content area is titled 'Migration using HCX' and contains the following sections:

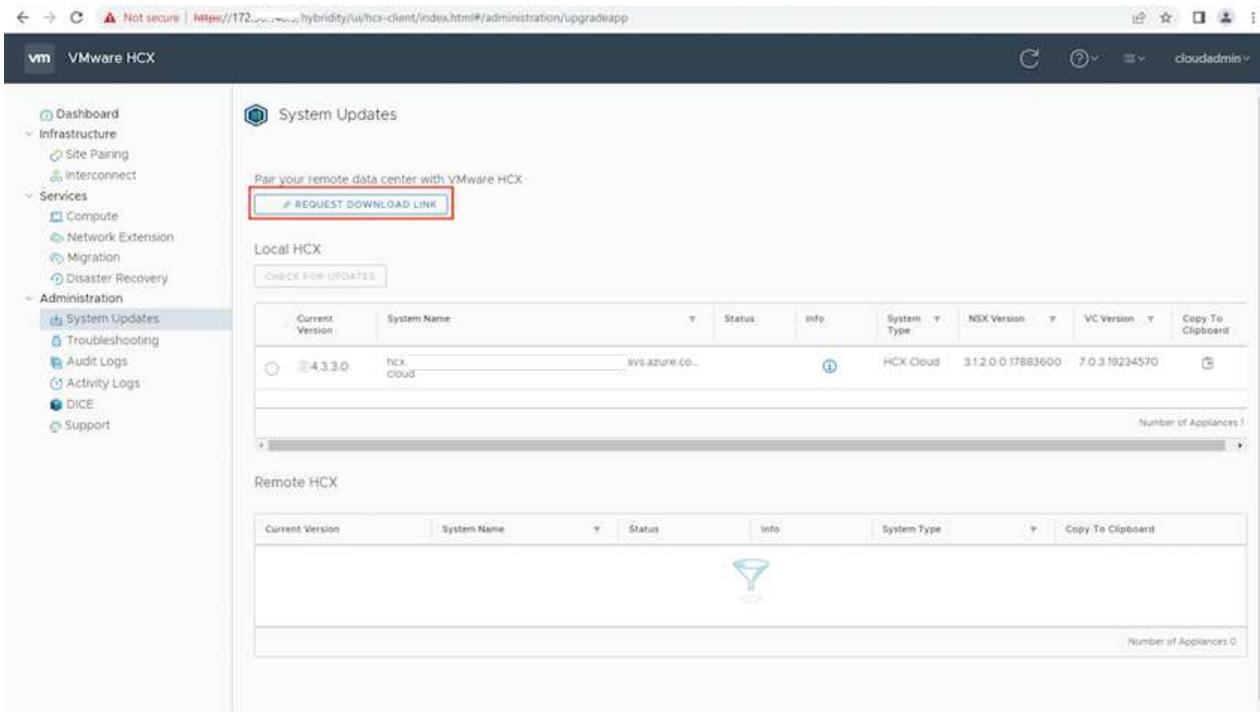
- Overview:** HCX is an application mobility platform designed for simplifying application migration, workload rebalancing, and business continuity across data centers and clouds.
- HCX plan:** HCX Advanced
- 1. Configure HCX appliance:** Using the IP address below launch the HCX portal. Download HCX appliance (OVA file) from Administration page and deploy on the site where source vCenter environment is running.
- HCX Cloud Manager IP:** A text input field containing 'https://172...' is highlighted with a red box.
- 2. Connect with on-premise using HCX keys:** After you deploy the VMware HCX Connector appliance on-premises and start the appliance, you're ready to activate using below license keys.
- HCX key table:**

HCX key name	Activation key	Status
Test-440	FADE113ADA6490ABF39C0F...	Consumed
testmig	40DD435CB2F940EF841CF41...	Consumed

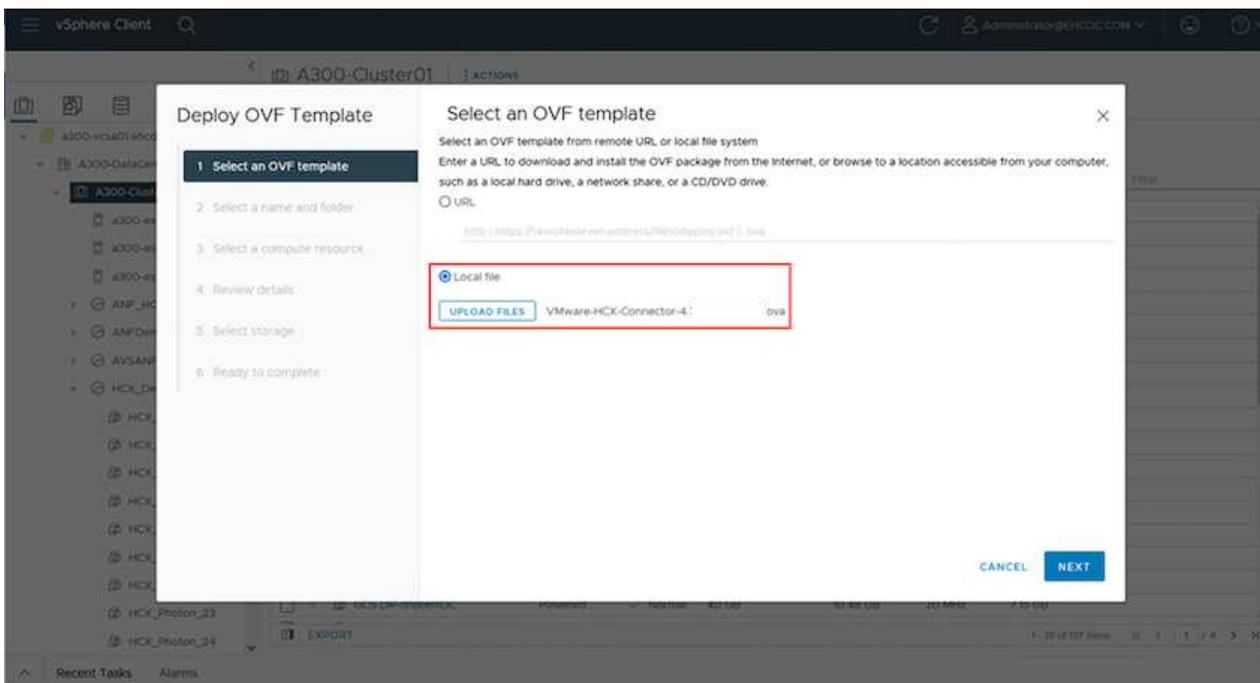
2. jumphostを使用してmailto:cloudadmin@vsphere.local | [cloudadmin@vsphere.local ^]でHCXポータルにアクセスしたら、\* Administration > System Updates に移動し、Request Download Link \*をクリックします。



OVAをダウンロードするか、OVAにコピーしてブラウザに貼り付け、オンプレミスのvCenter Serverに導入するVMware HCX Connector OVAファイルのダウンロードプロセスを開始します。



- OVAをダウンロードしたら、\* Deploy OVF Template \*オプションを使用して、OVAをオンプレミスのVMware vSphere環境に導入します。



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



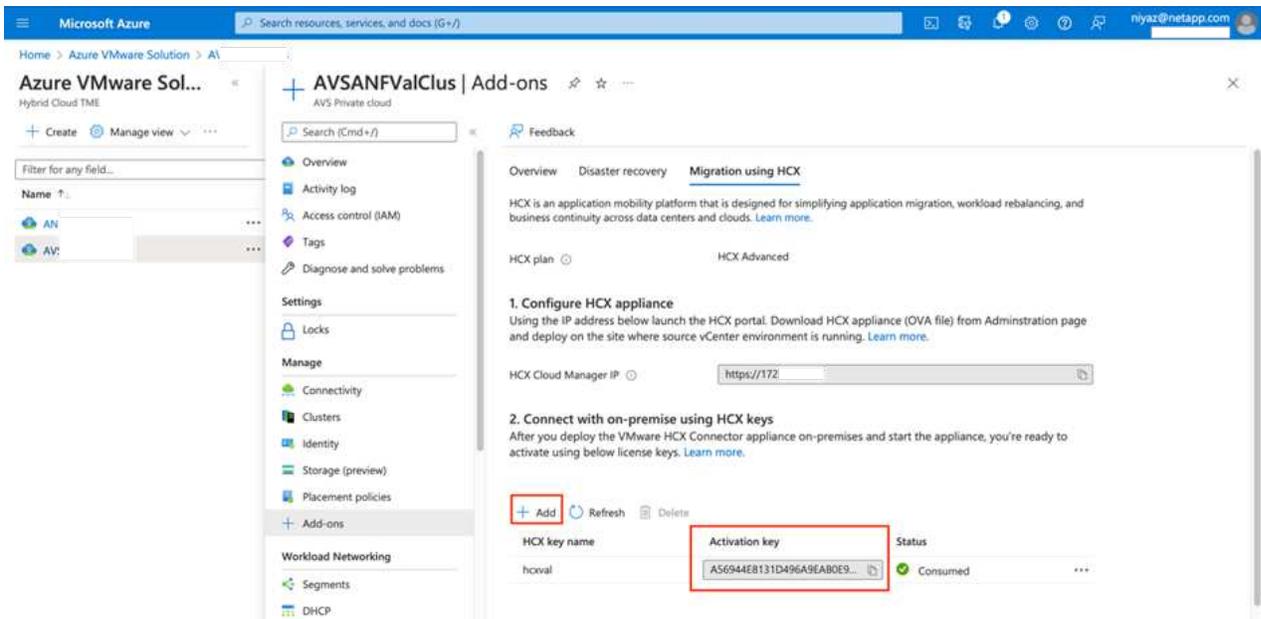
仮想アプライアンスの電源を手動でオンにします。

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

### 手順3：ライセンスキーを使用してHCXコネクタをアクティブにします

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

1. AzureポータルからAzure VMware解決策 にアクセスし、プライベートクラウドを選択して、\* Manage > Add-ons > Migration Using HCX\*を選択します。
2. [\* HCXキーを使用してオンプレミスと接続する\*]で、[\*追加]をクリックしてアクティベーションキーをコピーします。



導入されているオンプレミスのHCXコネクタごとに別々のキーが必要です。

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



OVAの導入時に定義されたパスワードを使用します。

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



オンプレミスのHCXコネクタにはインターネットアクセスが必要です。

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



あとで接続の問題が発生しないようにFQDNを使用してください。

9. Configure SSO/PSC で、プラットフォームサービスコントローラの**FQDN**または**IP**アドレスを入力し、Continue \*をクリックします。



VMware vCenter ServerのFQDNまたはIPアドレスを入力します。

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



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

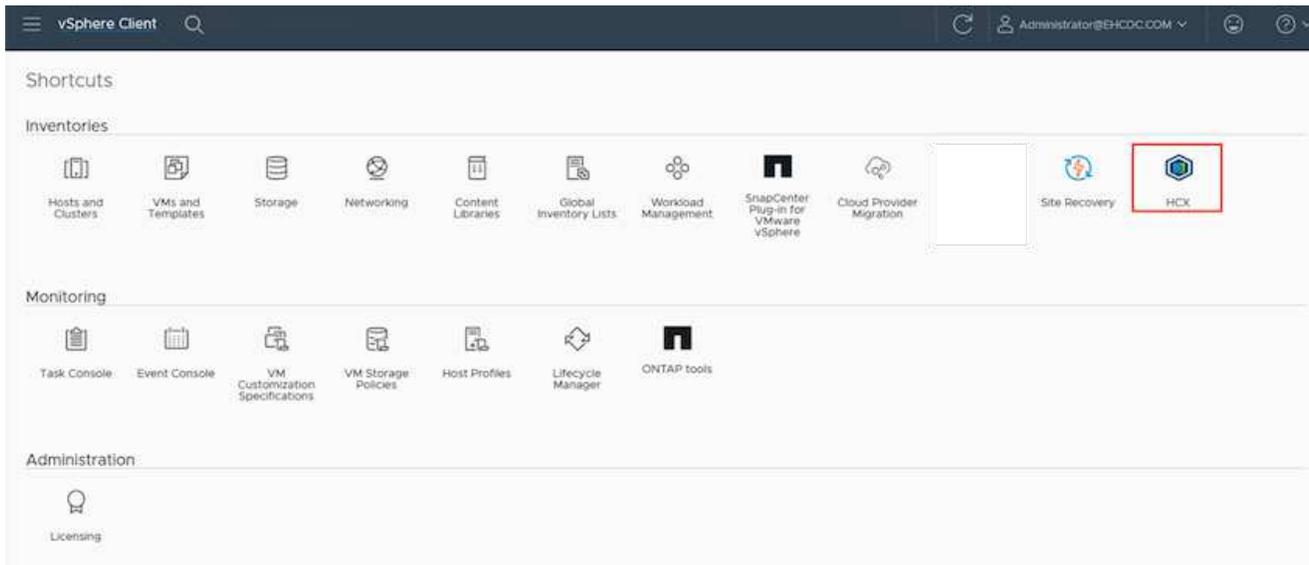
The screenshot shows the VMware HCX Manager dashboard for a device named VMware-HCX-440. The top navigation bar includes 'vm HCX Manager', 'Dashboard', 'Appliance Summary', 'Configuration', and 'Administration'. The main content area is divided into several sections:

- System Information:** FQDN: VMware-HCX-440.ehcdc.com, IP Address: 172.2, Version: 4.4.1.0, Uptime: 20 days, 21 hours, 9 minutes, Current Time: Tuesday, 13 September 2022 07:44:11 PM UTC.
- Resource Usage:** Three progress bars showing CPU (Used 1407 MHz, Free 688 MHz, Capacity 2095 MHz, 67%), Memory (Used 9691 MB, Free 2316 MB, Capacity 12008 MB, 81%), and Storage (Used 29G, Free 98G, Capacity 127G, 23%).
- Configuration Cards:** Three cards for NSX, vCenter, and SSO. The vCenter card shows the URL 'https://a300-vcasa01.ehcdc.com' with a green status indicator. The SSO card shows the URL 'https://a300-vcasa01.ehcdc.com'. Each card has a 'MANAGE' button.

#### 手順4：オンプレミスのVMware HCXコネクタをAzure VMware解決策 HCX Cloud Managerとペアリングします

オンプレミスとAzure VMware解決策 の両方にHCX Connectorをインストールした後、このペアリングを追加して、オンプレミスのVMware HCX Connector for Azure VMware解決策 プライベートクラウドを構成します。サイトペアリングを設定するには、次の手順を実行します。

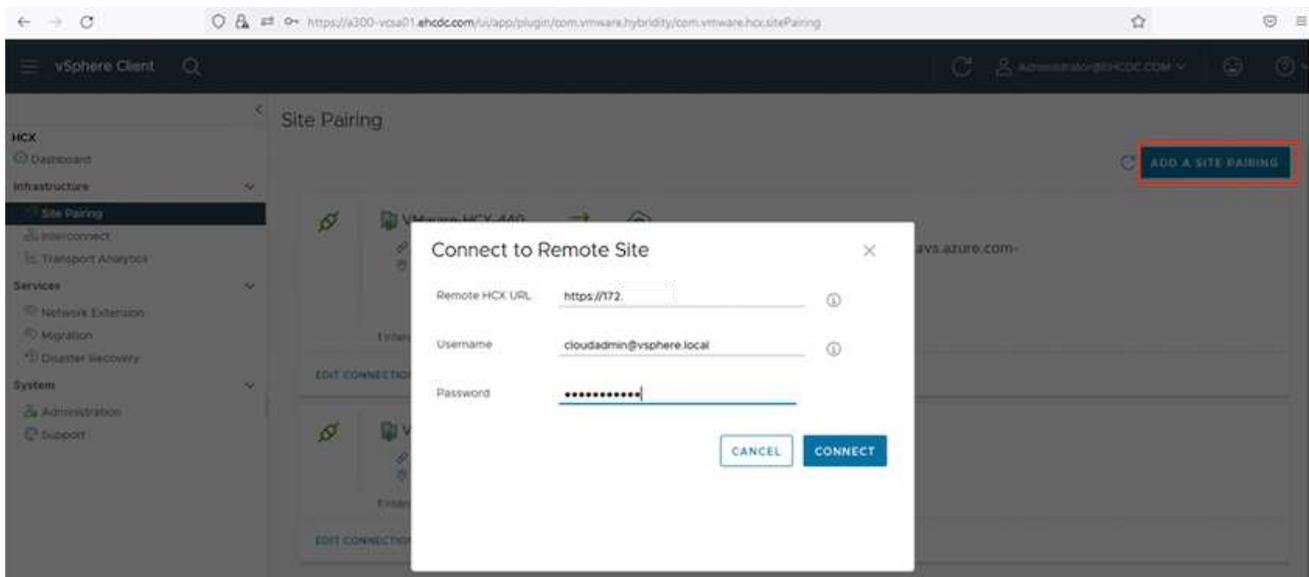
1. オンプレミスのvCenter環境とAzure VMware解決策 SDDCの間にサイトペアを作成するには、オンプレミスのvCenter Serverにログインし、新しいHCX vSphere Web Clientプラグインにアクセスします。



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



プライベートクラウドにアクセスするための、Azure VMware解決策 HCXのURLまたはIPアドレス、およびCloudAdminロールのクレデンシャルを入力します。

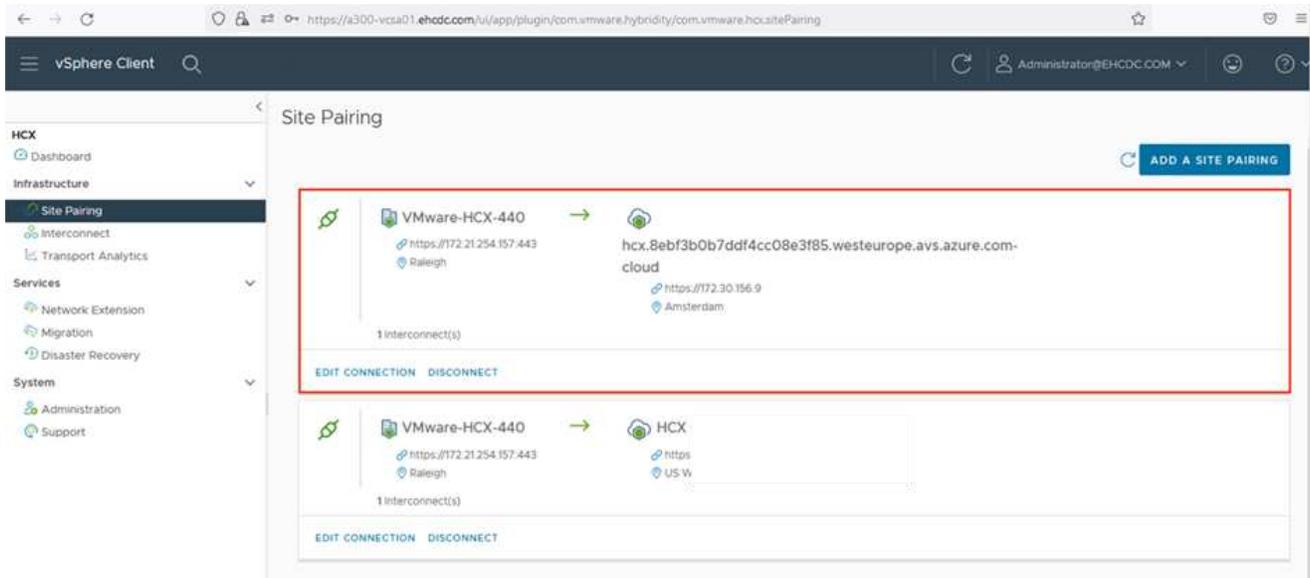


1. [接続] をクリックします。



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

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



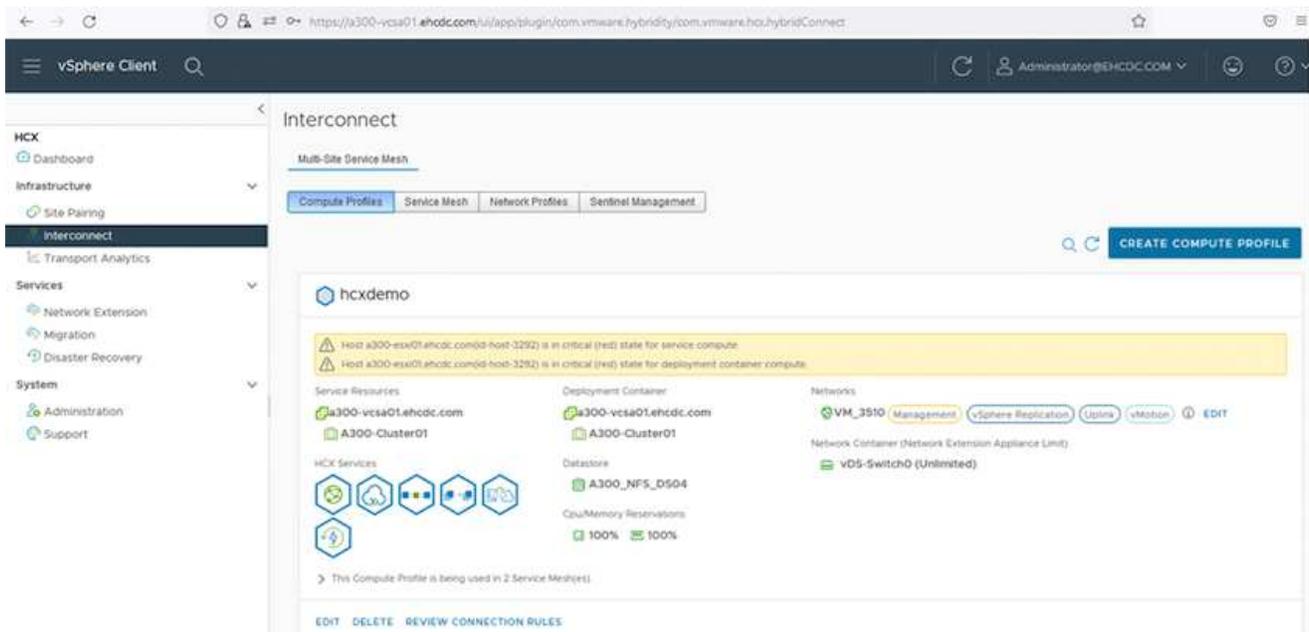
手順5：ネットワークプロファイル、コンピューティングプロファイル、およびサービスマッシュを設定します

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

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



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

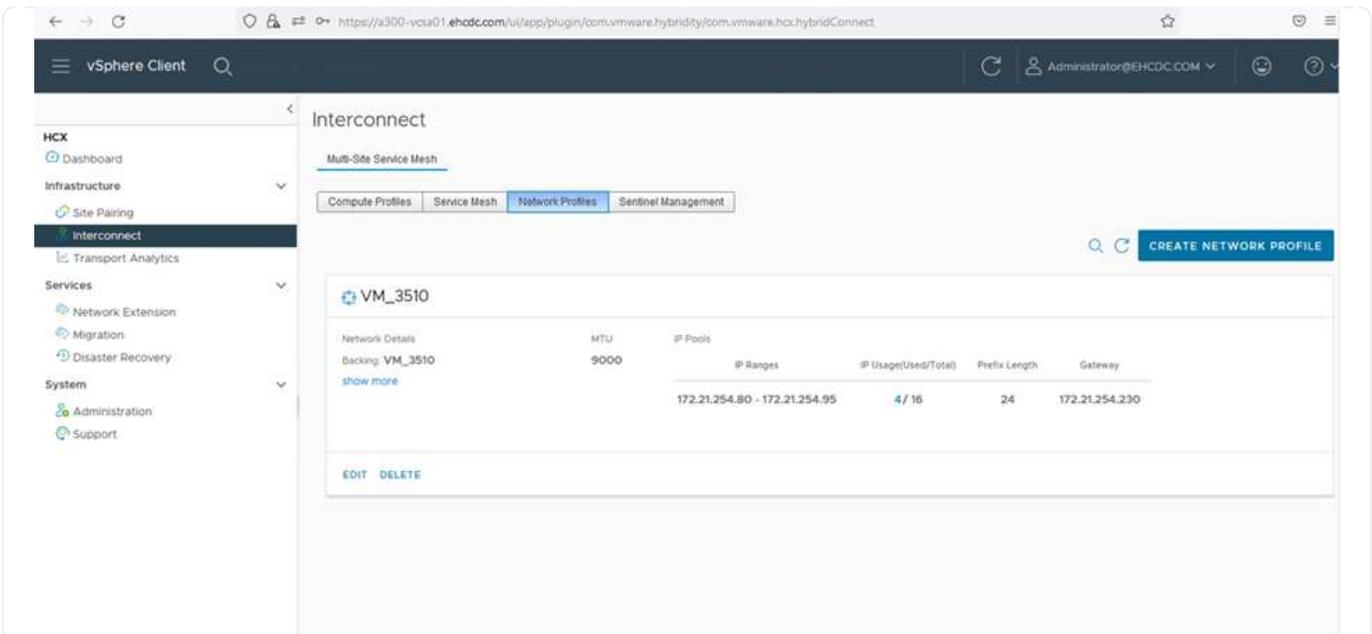


1. コンピューティングプロファイルを作成したら、\*マルチサイトサービスマッシュ>ネットワークプロファイル>ネットワークプロファイルの作成\*を選択して、ネットワークプロファイルを作成します。

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



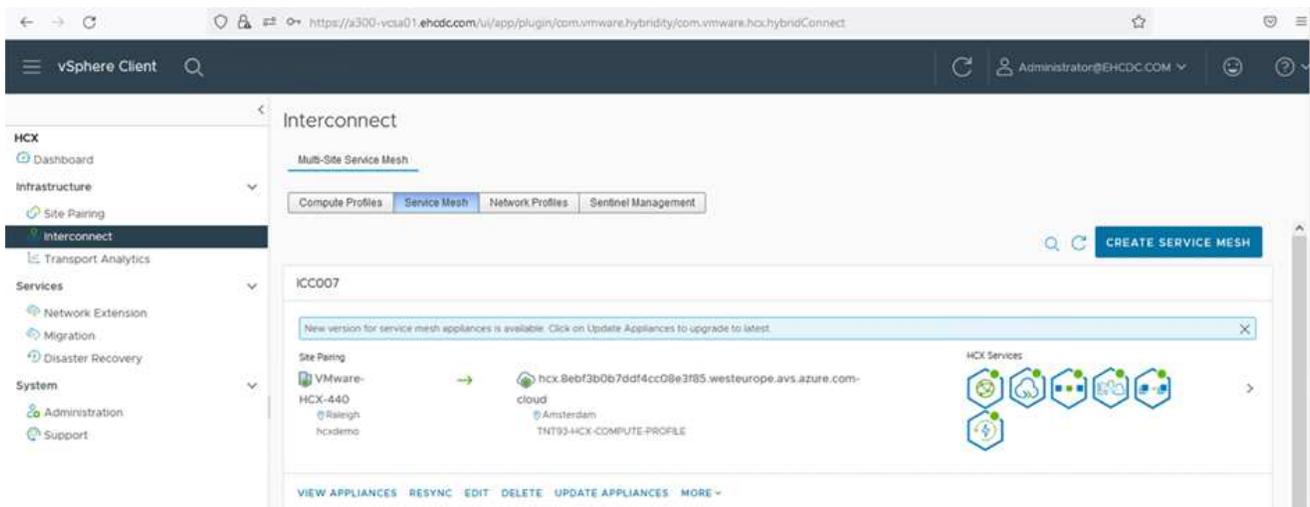
この手順には複数のIPアドレスが必要です。これらのIPアドレスは、管理ネットワークからインターコネクトアプライアンスに割り当てられます。



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



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



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

Browser address bar: <https://a300-vcsa01.ahcd.com/ui/app/plugin/com.vmware.hybridty/com.vmware.hci.hybridConnect>

Page Title: vSphere Client

Page Subtitle: Interconnect

Navigation: Home | Dashboard | Infrastructure | Networking | **Interconnect** | Transport Analysis | Services | Network Extension | Migration | Disaster Recovery | System | Administration | Support

Interconnect: **KC007** [EDIT SERVICE MESH]

Appliances

Appliance Name	Appliance Type	IP Address	Number of Appliances	Current Version	Appliance Version
KC007-HCI-0 IP: 10.20.191.10   VM: 10.20.191.10   Storage: K300_VPL_0204	HCI-VM-0	10.20.191.10	1	4.4.0	4.4.0
KC007-HCI-1 IP: 10.20.191.11   VM: 10.20.191.11   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.11	1	4.4.0	4.4.0
KC007-HCI-2 IP: 10.20.191.12   VM: 10.20.191.12   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.12	1	4.4.0	4.4.0
KC007-HCI-3 IP: 10.20.191.13   VM: 10.20.191.13   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.13	1	4.4.0	4.4.0
KC007-HCI-4 IP: 10.20.191.14   VM: 10.20.191.14   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.14	1	4.4.0	4.4.0
KC007-HCI-5 IP: 10.20.191.15   VM: 10.20.191.15   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.15	1	4.4.0	4.4.0
KC007-HCI-6 IP: 10.20.191.16   VM: 10.20.191.16   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.16	1	4.4.0	4.4.0
KC007-HCI-7 IP: 10.20.191.17   VM: 10.20.191.17   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.17	1	4.4.0	4.4.0
KC007-HCI-8 IP: 10.20.191.18   VM: 10.20.191.18   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.18	1	4.4.0	4.4.0
KC007-HCI-9 IP: 10.20.191.19   VM: 10.20.191.19   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.19	1	4.4.0	4.4.0
KC007-HCI-10 IP: 10.20.191.20   VM: 10.20.191.20   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.20	1	4.4.0	4.4.0
KC007-HCI-11 IP: 10.20.191.21   VM: 10.20.191.21   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.21	1	4.4.0	4.4.0
KC007-HCI-12 IP: 10.20.191.22   VM: 10.20.191.22   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.22	1	4.4.0	4.4.0
KC007-HCI-13 IP: 10.20.191.23   VM: 10.20.191.23   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.23	1	4.4.0	4.4.0
KC007-HCI-14 IP: 10.20.191.24   VM: 10.20.191.24   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.24	1	4.4.0	4.4.0
KC007-HCI-15 IP: 10.20.191.25   VM: 10.20.191.25   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.25	1	4.4.0	4.4.0
KC007-HCI-16 IP: 10.20.191.26   VM: 10.20.191.26   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.26	1	4.4.0	4.4.0
KC007-HCI-17 IP: 10.20.191.27   VM: 10.20.191.27   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.27	1	4.4.0	4.4.0
KC007-HCI-18 IP: 10.20.191.28   VM: 10.20.191.28   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.28	1	4.4.0	4.4.0
KC007-HCI-19 IP: 10.20.191.29   VM: 10.20.191.29   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.29	1	4.4.0	4.4.0
KC007-HCI-20 IP: 10.20.191.30   VM: 10.20.191.30   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.30	1	4.4.0	4.4.0
KC007-HCI-21 IP: 10.20.191.31   VM: 10.20.191.31   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.31	1	4.4.0	4.4.0
KC007-HCI-22 IP: 10.20.191.32   VM: 10.20.191.32   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.32	1	4.4.0	4.4.0
KC007-HCI-23 IP: 10.20.191.33   VM: 10.20.191.33   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.33	1	4.4.0	4.4.0
KC007-HCI-24 IP: 10.20.191.34   VM: 10.20.191.34   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.34	1	4.4.0	4.4.0
KC007-HCI-25 IP: 10.20.191.35   VM: 10.20.191.35   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.35	1	4.4.0	4.4.0
KC007-HCI-26 IP: 10.20.191.36   VM: 10.20.191.36   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.36	1	4.4.0	4.4.0
KC007-HCI-27 IP: 10.20.191.37   VM: 10.20.191.37   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.37	1	4.4.0	4.4.0
KC007-HCI-28 IP: 10.20.191.38   VM: 10.20.191.38   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.38	1	4.4.0	4.4.0
KC007-HCI-29 IP: 10.20.191.39   VM: 10.20.191.39   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.39	1	4.4.0	4.4.0
KC007-HCI-30 IP: 10.20.191.40   VM: 10.20.191.40   Storage: K300_VPL_0204	HCI-VM-EXT	10.20.191.40	1	4.4.0	4.4.0

Appliances on hci.5ebf3b0b7cdf4cc08e3f85.westeurope.azure.com-cloud

Appliance Name	Appliance Type	IP Address	Current Version
KC007-HCI-0	HCI-VM-0	10.20.191.10	4.4.0
KC007-HCI-1	HCI-VM-EXT	10.20.191.11	4.4.0
KC007-HCI-2	HCI-VM-EXT	10.20.191.12	4.4.0
KC007-HCI-3	HCI-VM-EXT	10.20.191.13	4.4.0
KC007-HCI-4	HCI-VM-EXT	10.20.191.14	4.4.0
KC007-HCI-5	HCI-VM-EXT	10.20.191.15	4.4.0
KC007-HCI-6	HCI-VM-EXT	10.20.191.16	4.4.0
KC007-HCI-7	HCI-VM-EXT	10.20.191.17	4.4.0
KC007-HCI-8	HCI-VM-EXT	10.20.191.18	4.4.0
KC007-HCI-9	HCI-VM-EXT	10.20.191.19	4.4.0
KC007-HCI-10	HCI-VM-EXT	10.20.191.20	4.4.0
KC007-HCI-11	HCI-VM-EXT	10.20.191.21	4.4.0
KC007-HCI-12	HCI-VM-EXT	10.20.191.22	4.4.0
KC007-HCI-13	HCI-VM-EXT	10.20.191.23	4.4.0
KC007-HCI-14	HCI-VM-EXT	10.20.191.24	4.4.0
KC007-HCI-15	HCI-VM-EXT	10.20.191.25	4.4.0
KC007-HCI-16	HCI-VM-EXT	10.20.191.26	4.4.0
KC007-HCI-17	HCI-VM-EXT	10.20.191.27	4.4.0
KC007-HCI-18	HCI-VM-EXT	10.20.191.28	4.4.0
KC007-HCI-19	HCI-VM-EXT	10.20.191.29	4.4.0
KC007-HCI-20	HCI-VM-EXT	10.20.191.30	4.4.0
KC007-HCI-21	HCI-VM-EXT	10.20.191.31	4.4.0
KC007-HCI-22	HCI-VM-EXT	10.20.191.32	4.4.0
KC007-HCI-23	HCI-VM-EXT	10.20.191.33	4.4.0
KC007-HCI-24	HCI-VM-EXT	10.20.191.34	4.4.0
KC007-HCI-25	HCI-VM-EXT	10.20.191.35	4.4.0
KC007-HCI-26	HCI-VM-EXT	10.20.191.36	4.4.0
KC007-HCI-27	HCI-VM-EXT	10.20.191.37	4.4.0
KC007-HCI-28	HCI-VM-EXT	10.20.191.38	4.4.0
KC007-HCI-29	HCI-VM-EXT	10.20.191.39	4.4.0
KC007-HCI-30	HCI-VM-EXT	10.20.191.40	4.4.0

## 手順6：ワークロードを移行する

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

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

### 一括移行

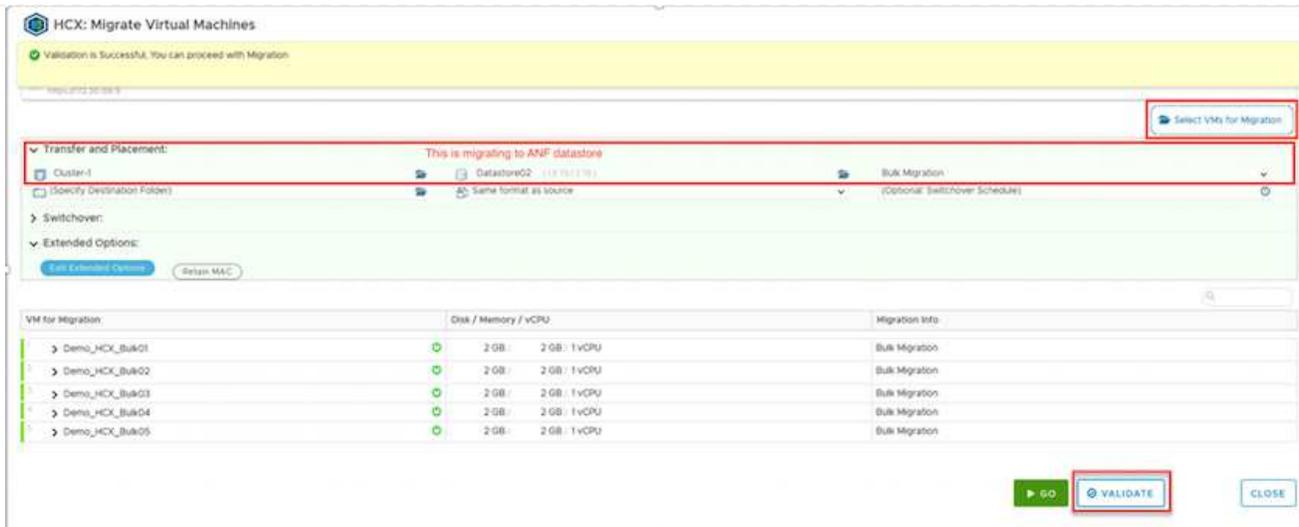
このセクションでは、一括移行のメカニズムについて詳しく説明します。HCXの一括移行機能では、移行先のvSphere HCXインスタンスでVMを再作成する際に、vSphere Replicationを使用してディスクファイルを移行します。

VMの一括移行を開始するには、次の手順を実行します。

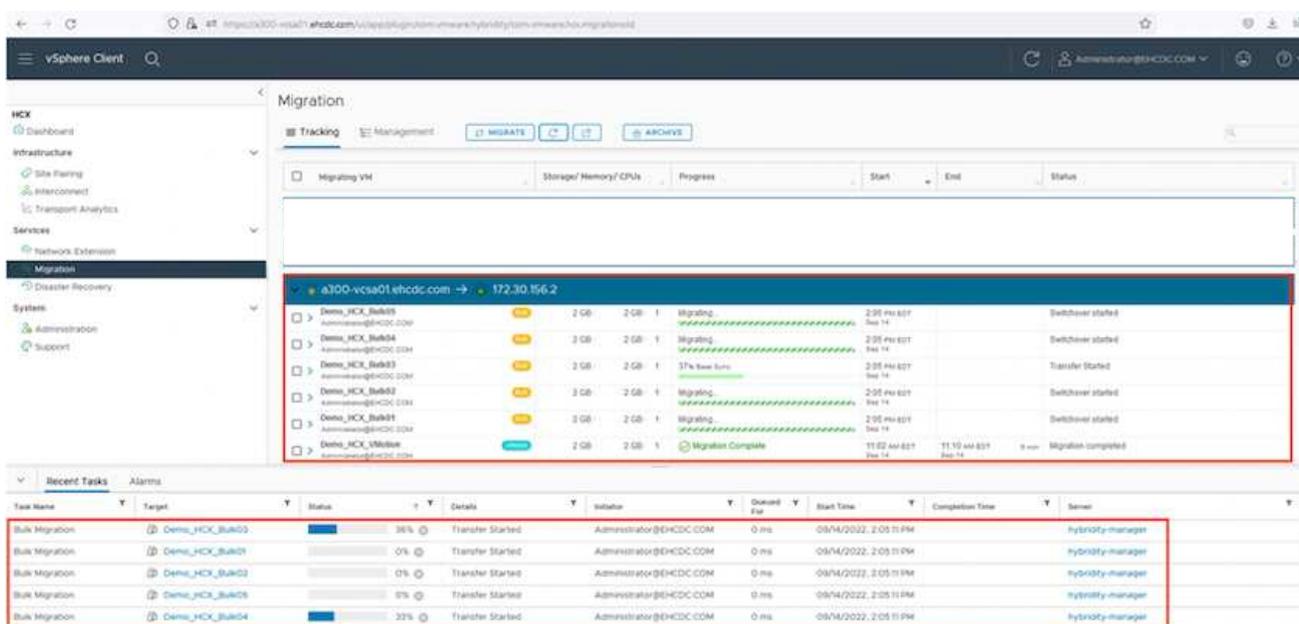
1. **[Services]>[Migration]**の下の**[Migrate]**タブにアクセスします。

Name	VM/ Storage/ Memory/ CPUs	Progress	Start	End	Status
▼ a300-vcsa01.ehcdc.com → 172.30.156.2					
> 2022-09-26 09:00 FLJVU	1 2 GB 2 GB 1	Migration Complete	--	--	
> 2022-09-26 08:35 IXMTB	1 2 GB 2 GB 1	Migration Complete	--	--	
> 2022-09-18 16:21 ERCZO	2 4 GB 4 GB 2	Draft	--	--	
> MG-18cbe94 / Sep 16	5 10 GB 10 GB 5	Migration Complete	12:44 AM Sep 16	--	
> MG-04abdee8 / Sep 16	1 2 GB 2 GB 1	Migration Complete	12:25 AM Sep 16	--	
> MG-e7374d6 / Sep 16	1 2 GB 2 GB 1	Migration Complete	12:11 AM Sep 16	--	
> MG-d2ef93ef / Sep 14	5 10 GB 10 GB 5	Migration Complete	02:05 PM Sep 14	--	
> MG-99fecac8 / Sep 14	1 2 GB 2 GB 1	Migration Complete	11:02 AM Sep 14	--	
> MG-548618cb / Sep 14	1 2 GB 2 GB 1	Migration Complete	10:04 AM Sep 14	--	
> MG-d6475274 / Sep 12	2 4 GB 4 GB 2	Migration Complete	12:25 PM	--	

1. **[リモートサイト接続\*]**で、リモートサイト接続を選択し、ソースとデスティネーションを選択します。この例では、デスティネーションはAzure VMware解決策 SDDC HCXエンドポイントです。
2. **[移行するVMの選択]**をクリックします。これにより、すべてのオンプレミスVMが一覧表示されます。match.value式に基づいてVMを選択し、\* Add \*をクリックします。
3. **[転送と配置]**セクションで、移行プロファイルを含む必須フィールド（クラスタ、ストレージ、デスティネーション、ネットワーク）を更新し、**[検証]**をクリックします。

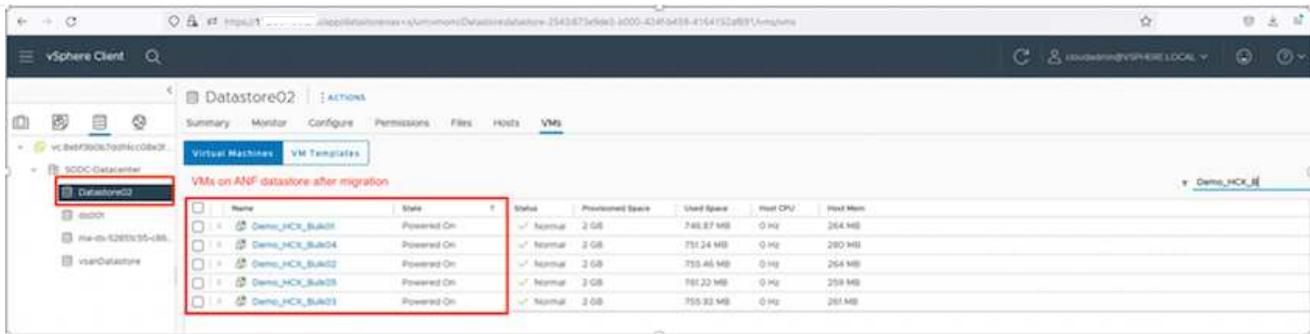


1. 検証チェックが完了したら、\*移動\*をクリックして移行を開始します。



この移行では、移行元VMディスクのデータをプレースホルダディスクにレプリケートできるように、移行先vCenter内の指定したAzure NetApp Files データストアにプレースホルダディスクが作成されます。HBRはターゲットへの完全な同期に対してトリガーされ、ベースラインが完了すると、RPO（目標復旧時点）サイクルに基づいて増分同期が実行されます。フル/増分同期が完了すると、特定のスケジュールが設定されていないかぎり、スイッチオーバーが自動的にトリガーされます。

1. 移行が完了したら、移行先のSDDC vCenterにアクセスして同じことを検証します。

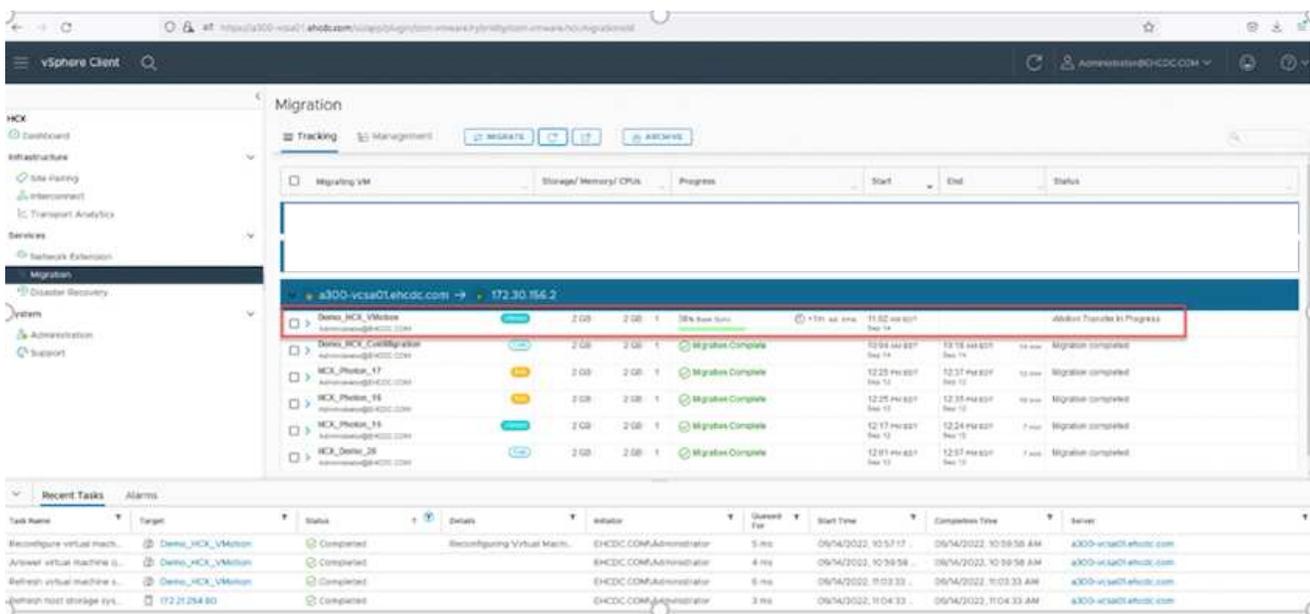


さまざまな移行オプションの詳細と、HCXを使用してオンプレミスからAzure VMware解決策にワークロードを移行する方法については、を参照してください ["VMware HCXユーザーガイド"](#)。

このプロセスの詳細については、次のビデオをご覧ください。

### HCXを使用したワークロードの移行

HCX vMotionオプションのスクリーンショットを次に示します。



このプロセスの詳細については、次のビデオをご覧ください。

### HCx vMotion



移行に十分な帯域幅を使用できることを確認します。



移行先のANFデータストアには、移行を処理するための十分なスペースが必要です。

### まとめ

オンプレミスのあらゆるタイプ/ベンダーストレージに存在するオールクラウドやハイブリッドクラウド、データのいずれをターゲットとしている場合でも、Azure NetApp Files とHCXは、アプリケーションワークロー

ドを展開して移行するための優れたオプションを提供し、データ要件をアプリケーションレイヤとシームレスにすることでTCOを削減します。どのようなユースケースでも、クラウドのメリット、一貫したインフラ、オンプレミスと複数のクラウドにわたる運用、ワークロードの双方向の移動、エンタープライズクラスの容量とパフォーマンスを迅速に実現するには、Azure VMware解決策 とAzure NetApp Files を選択してください。VMware vSphere Replication、VMware vMotion、Network File Copy (NFC；ネットワークファイルコピー) を使用してストレージの接続やVMの移行を行う場合と同じ手順を実行します。

## 重要なポイント

本ドキュメントの主な内容は次のとおりです。

- Azure NetApp Files をAzure VMware解決策 SDDC上のデータストアとして使用できるようになりました。
- オンプレミスからAzure NetApp Files データストアへのデータの移行は簡単です。
- Azure NetApp Files データストアは、移行アクティビティ中に必要な容量やパフォーマンスに合わせて簡単に拡張および縮小することができます。

## 追加情報の参照先

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

- Azure VMware解決策 のドキュメント

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

- Azure NetApp Files のドキュメント

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

- VMware HCXユーザーガイド

["https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"](https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html)

## Region Availability - ANFの補助的なNFSデータストア

Azure、AVS、ANFのグローバルリージョンサポートの詳細については、こちらをご覧ください。



NFSデータストアは、両方のサービス (AVSとANF) が利用可能な地域で利用できます。

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

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

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

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

## 商標に関する情報

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