# Azure / AVS上のワークロードを保護

NetApp Solutions

NetApp
April 10, 2024

# 目次

# Azure / AVS上のワークロードを保護

## ANFとJetStreamを使用したディザスタリカバリ

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

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

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

解決策 の導入の概要

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

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

CPTは次の機能を実行します。

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

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

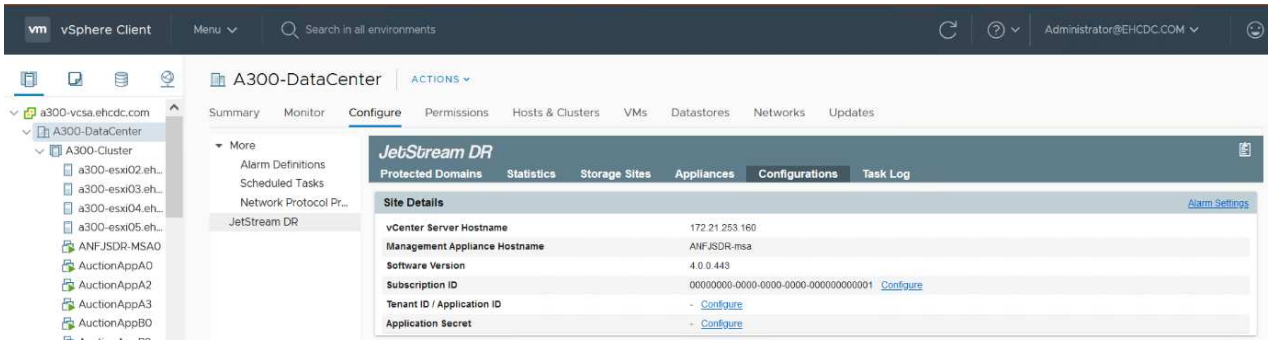
ドメインの数と内容は、平均IOPS、合計容量、優先度（フェイルオーバー順序を定義）、RTOなど、VMのさまざまな特性によって異なります。

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

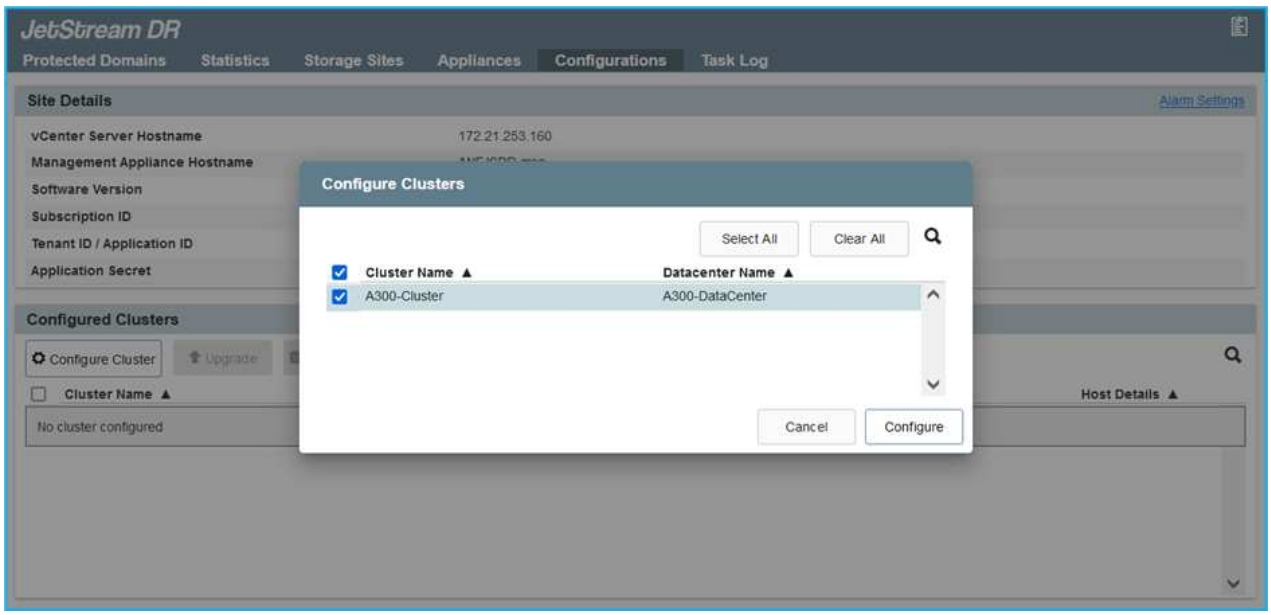
Jetstream DRソフトウェアは、JetStream DR Management Server Virtual Appliance（MSA）、DR Virtual Appliance（DRVA）、およびホストコンポーネント（I/O Filterパッケージ）の3つの主要コンポーネントで構成されています。MSAは、コンピューティングクラスタにホストコンポーネントをインストールして構成し、JetStream DRソフトウェアを管理するために使用されます。次に、インストールプロセスの概要 の概要を示します。

**JetStream DR**をオンプレミスにインストールする方法

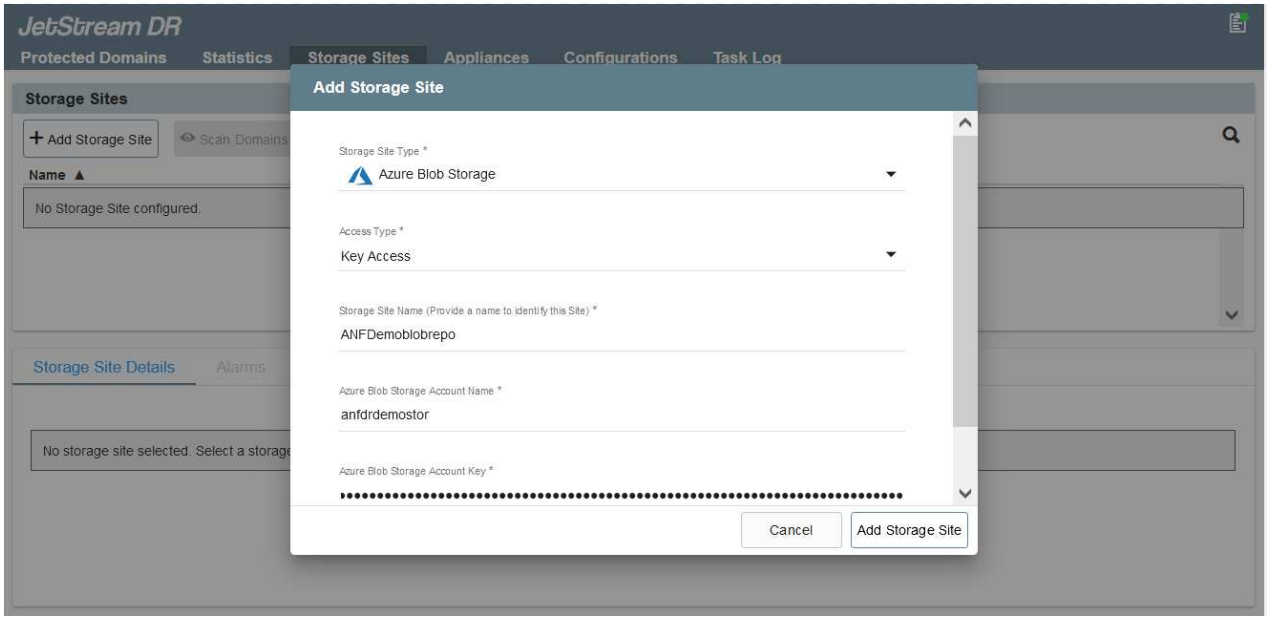
1. 前提条件を確認する。
2. キャパシティプランニングツールを実行して、リソースと構成に関する推奨事項を確認します（オプションですが、コンセプトの実証の試用には推奨されます）。
3. JetStream DR MSAを指定されたクラスタ内のvSphereホストに展開します。
4. ブラウザでDNS名を使用してMSAを起動します。
5. vCenterサーバをMSAに登録します。インストールを実行するには、次の手順を実行します。
6. JetStream DR MSAが導入され、vCenter Serverが登録されたら、vSphere Web Clientを使用してJetStream DR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




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



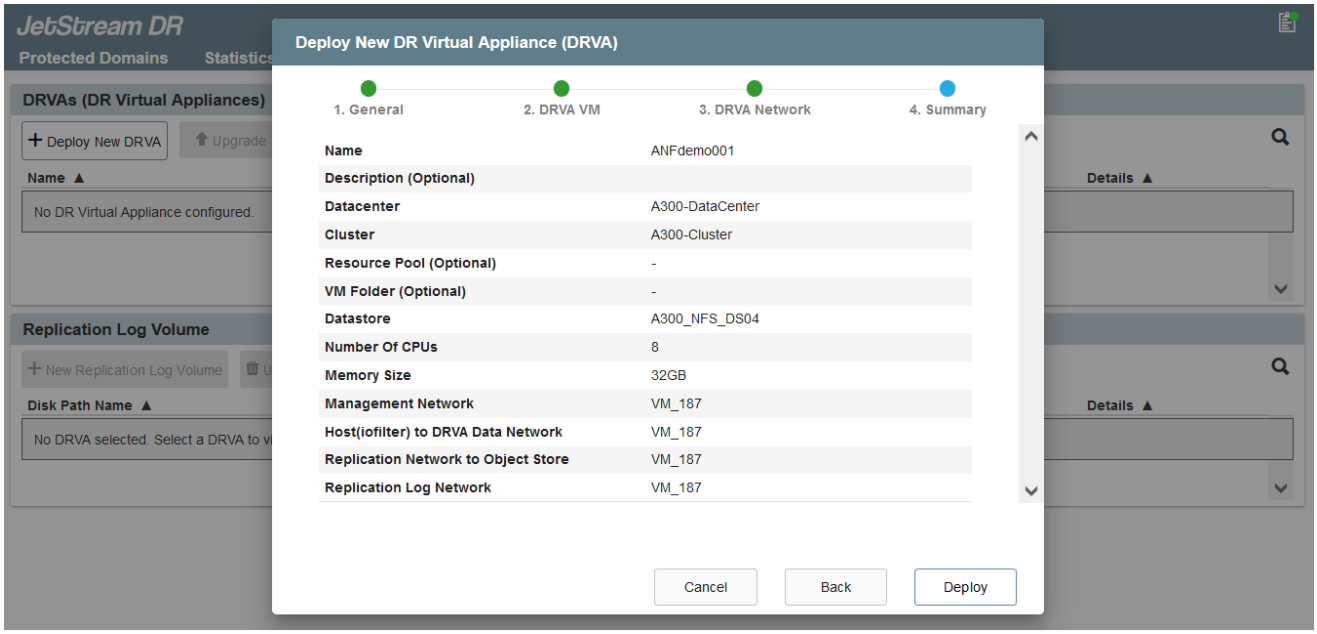

8. I/Oフィルタパッケージを使用してクラスタを設定します。




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

> DRFAはCPTによって自動的に作成できますが、POCトライアルの場合は、DRサイクルを手動で設定して実行することをお勧めします（Start protection > failover > failback）。

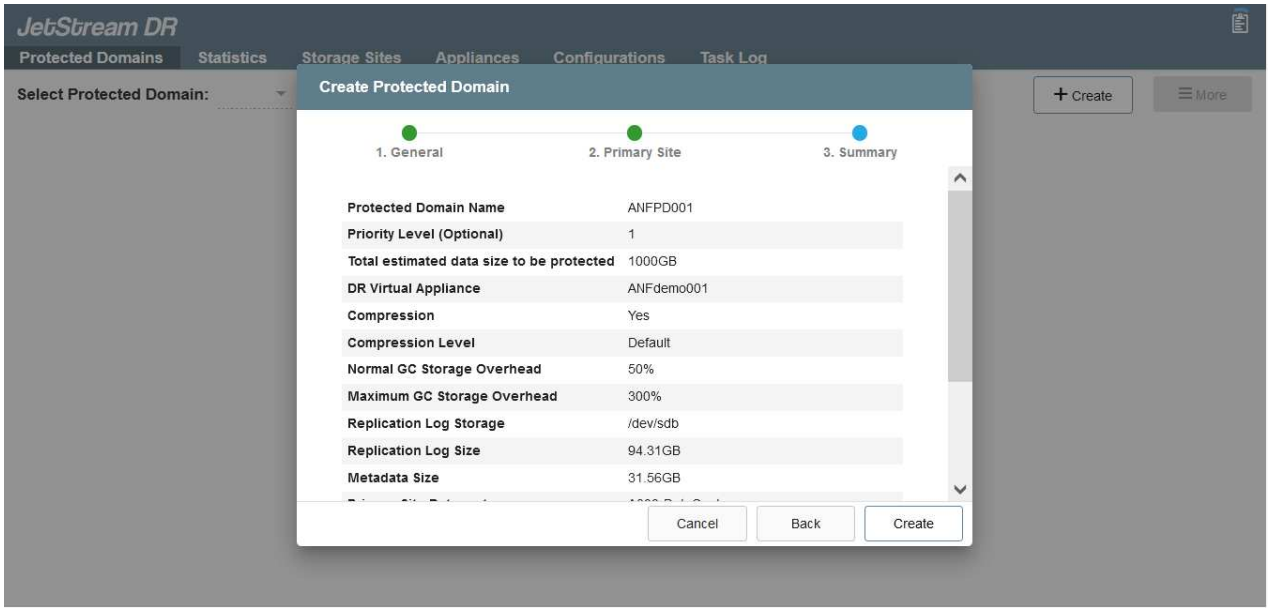
JetStream DRVAは、データ複製プロセスの主要な機能を容易にする仮想アプライアンスです。保護されたクラスタには少なくとも1つのDRVAが含まれている必要があります。通常は、ホストごとに1つのDRVAが構成されます。各DRVAは、複数の保護ドメインを管理できます。




この例では、4台のDRVAが80台の仮想マシン用に作成されています。

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

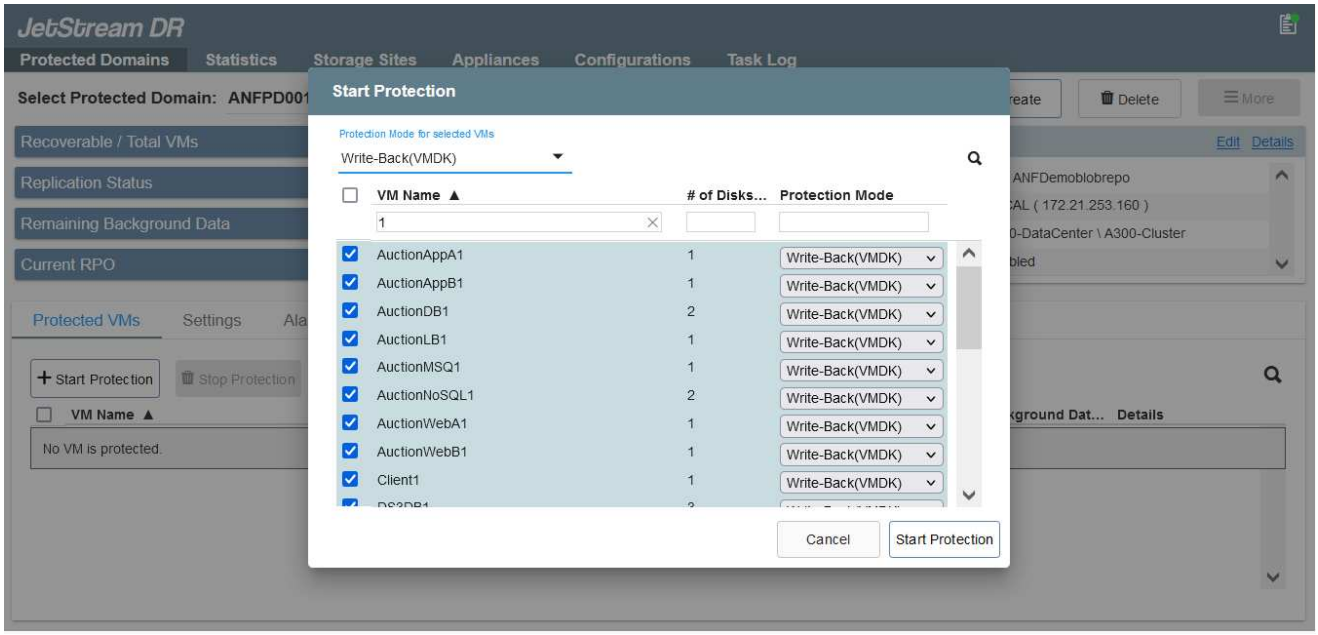
2. Protected Domainsタブで、Azure Blob Storageサイト、DRVAインスタンス、およびレプリケーションログに関する情報を使用して、必要な数の保護ドメインを作成します。保護ドメインは、クラスタ内の特定のVMまたはVMのセットを定義します。これらのVMは一緒に保護され、フェイルオーバー/フェイルバック処理の優先順位が割り当てられます。




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

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

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




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

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

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

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

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

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

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

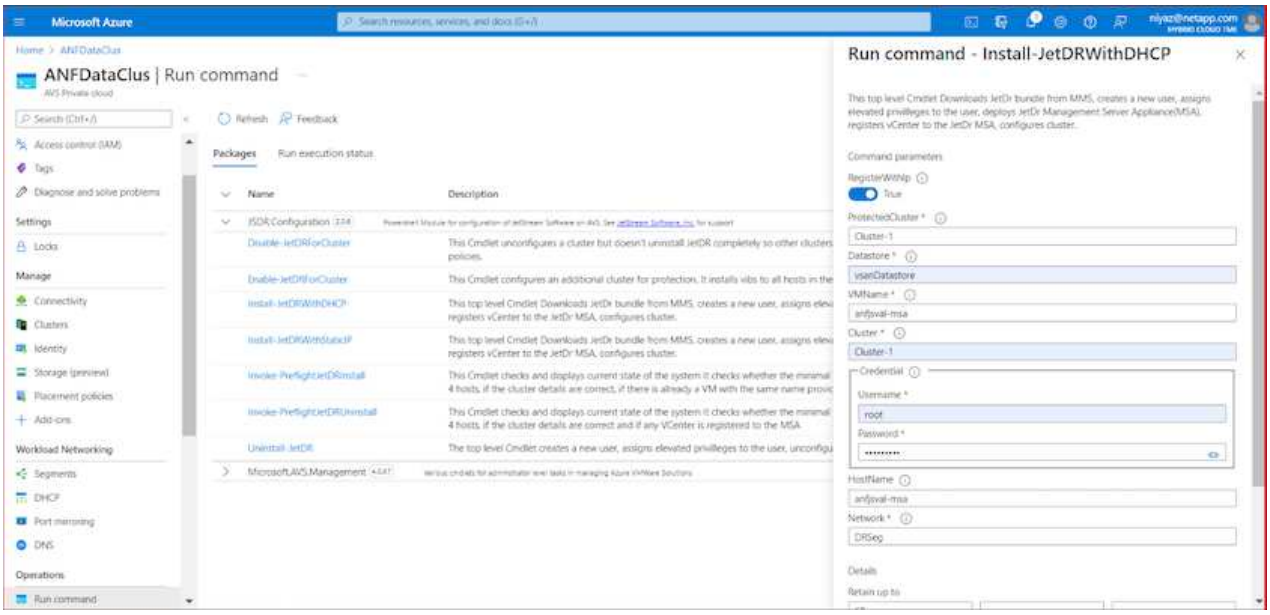
プライベートクラウドに**JetStream DR for AVS**をインストールする方法

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

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

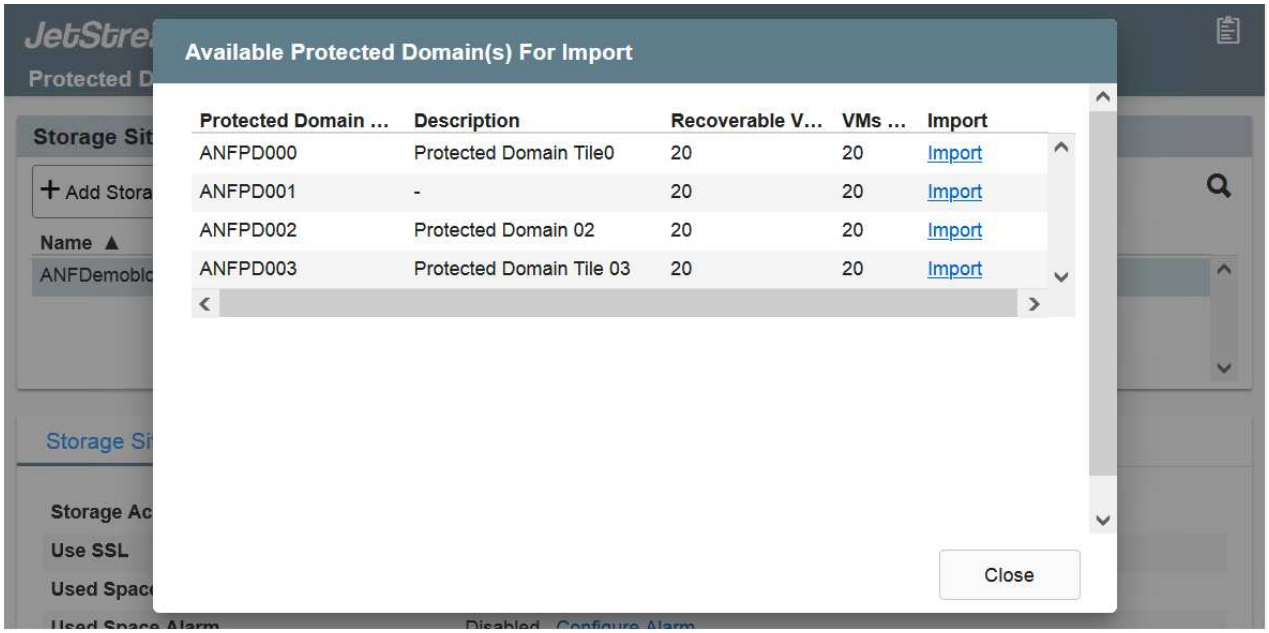
> Azure VMware解決策 のデフォルトCloudAdminユーザには、AVS対応のJetStream DRをインストールするための十分な権限がありません。Azure VMware解決策 では、JetStream DR用のAzure VMware解決策 実行コマンドを呼び出すことで、JetStream DRを簡単かつ自動でインストールできます。

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




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

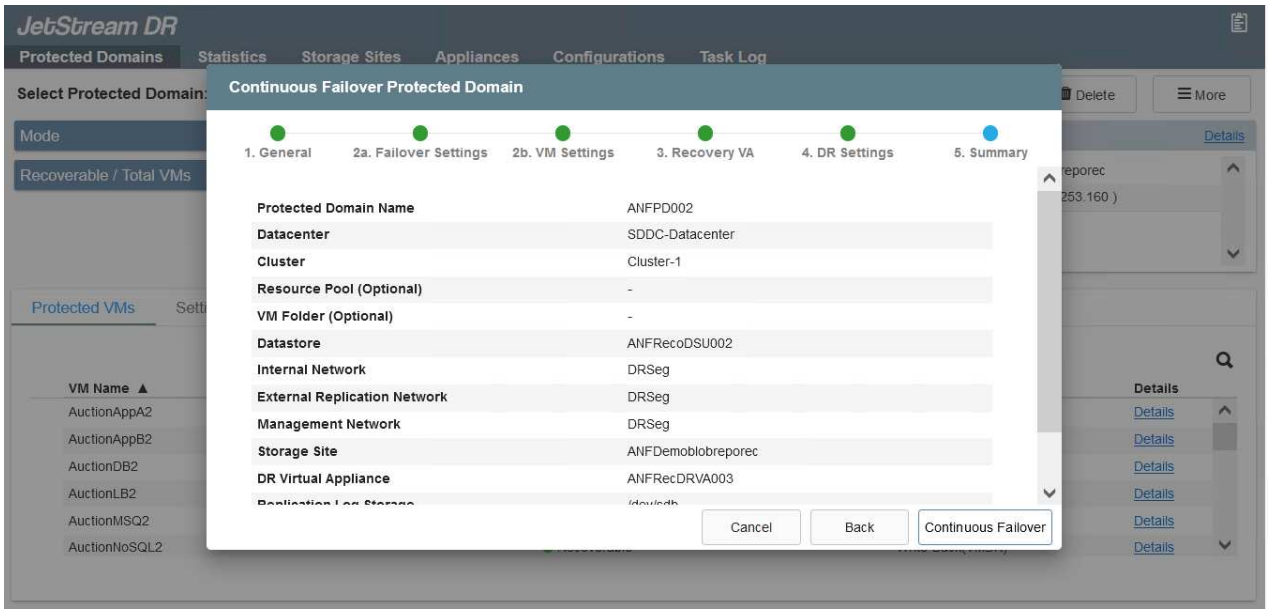

3. JetStream DRインターフェイスから、オンプレミスクラスタをストレージサイトとして保護するために使用したAzure Blob Storageアカウントを追加し、Scan Domainsオプションを実行します。




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

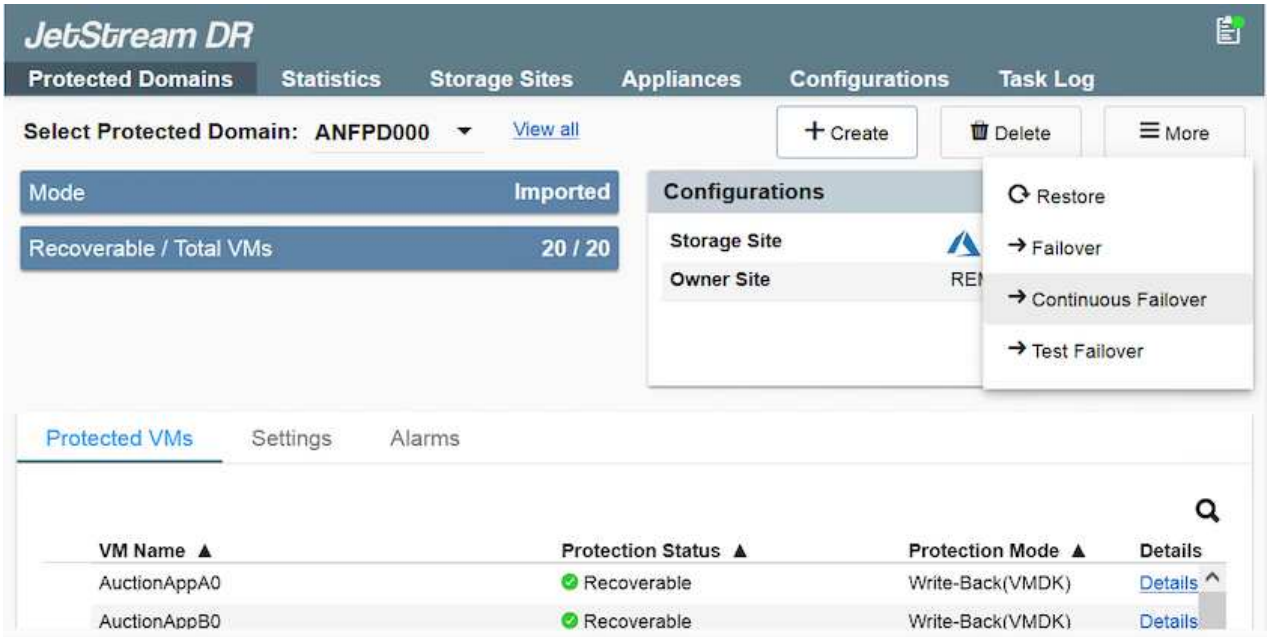
> これらの手順は、CPT作成計画を使用して自動化することもできます。

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




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

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



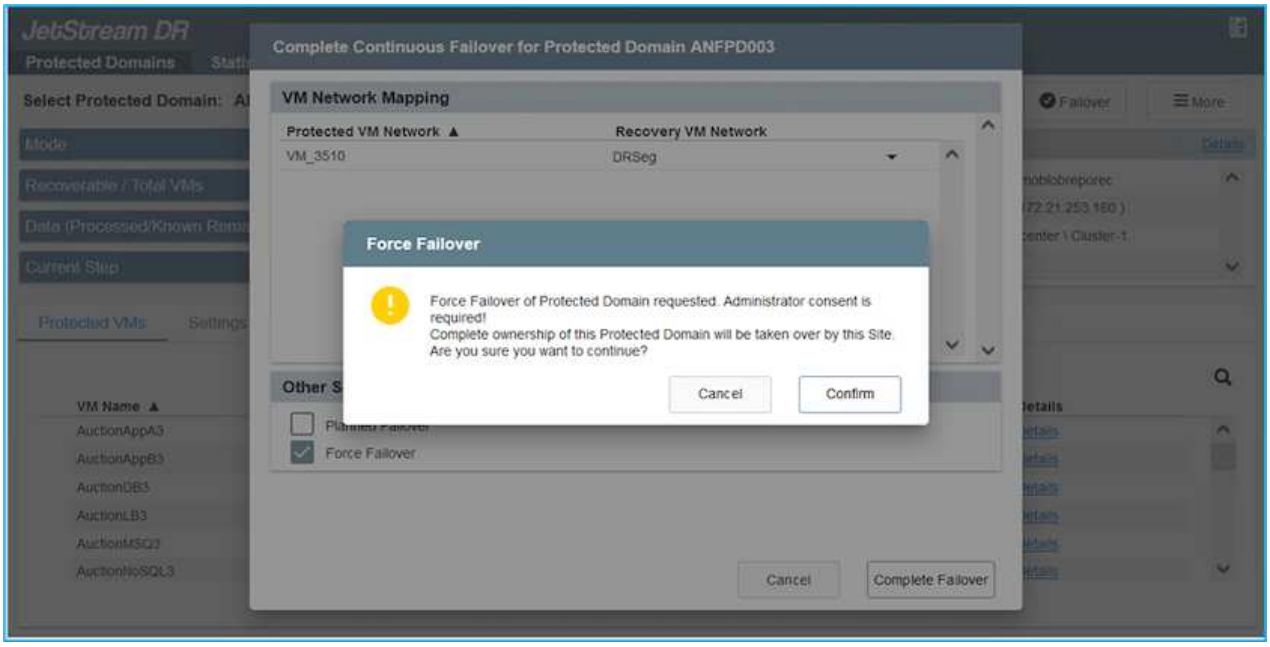

## フェイルオーバー/フェイルバックを実行しています

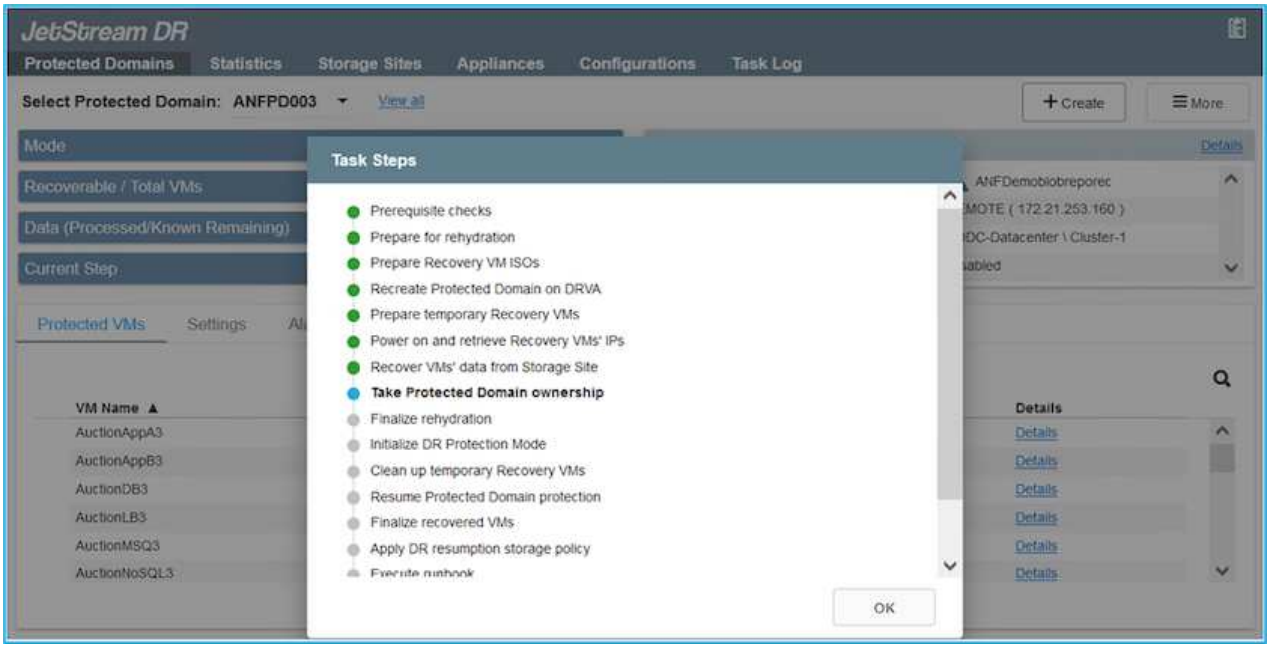
フェールオーバー/フェールバックの実行方法

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

> CPTを使用すると、フェイルオーバープランを実行して、Azure Blob StorageからAVSクラスタリカバリサイトにVMをリカバリできます。

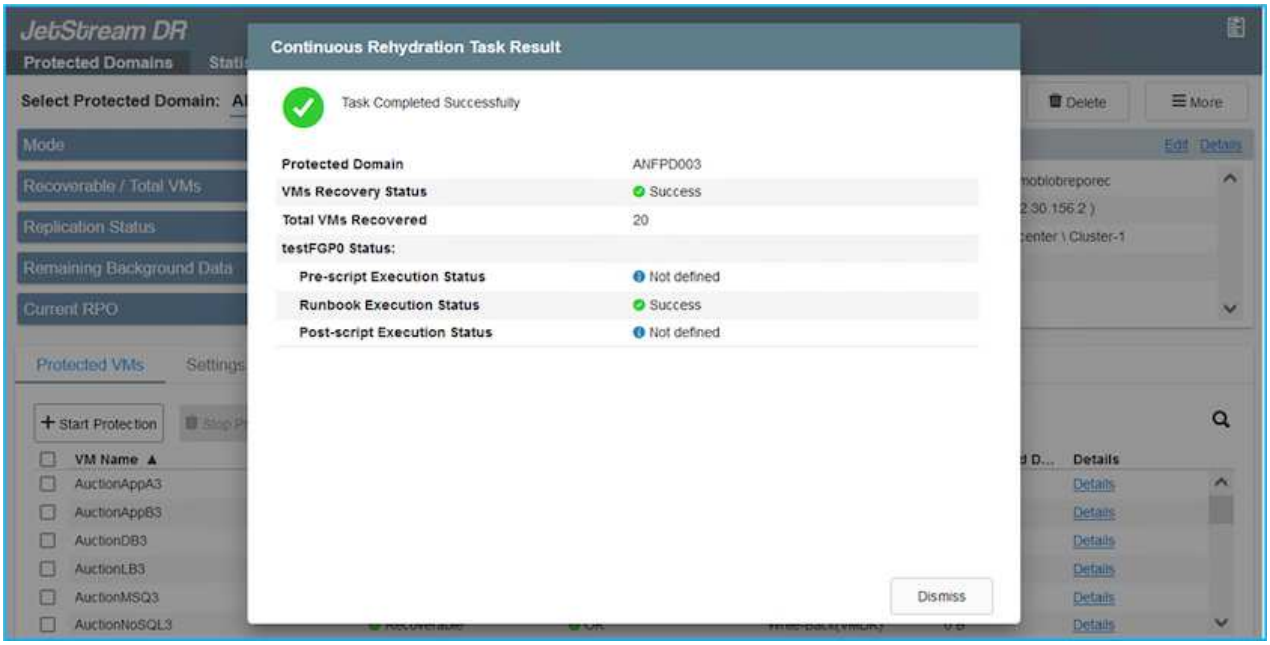
> 保護対象のVMがAVSで起動されると、フェイルオーバー後（継続的または標準的なリハイドレート）、保護は自動的に再開され、JetStream DRは、Azure Blob Storage内の適切なコンテナまたは元のコンテナにデータをレプリケートし続けます。




タスクバーにフェイルオーバーアクティビティの進行状況が表示されます。

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

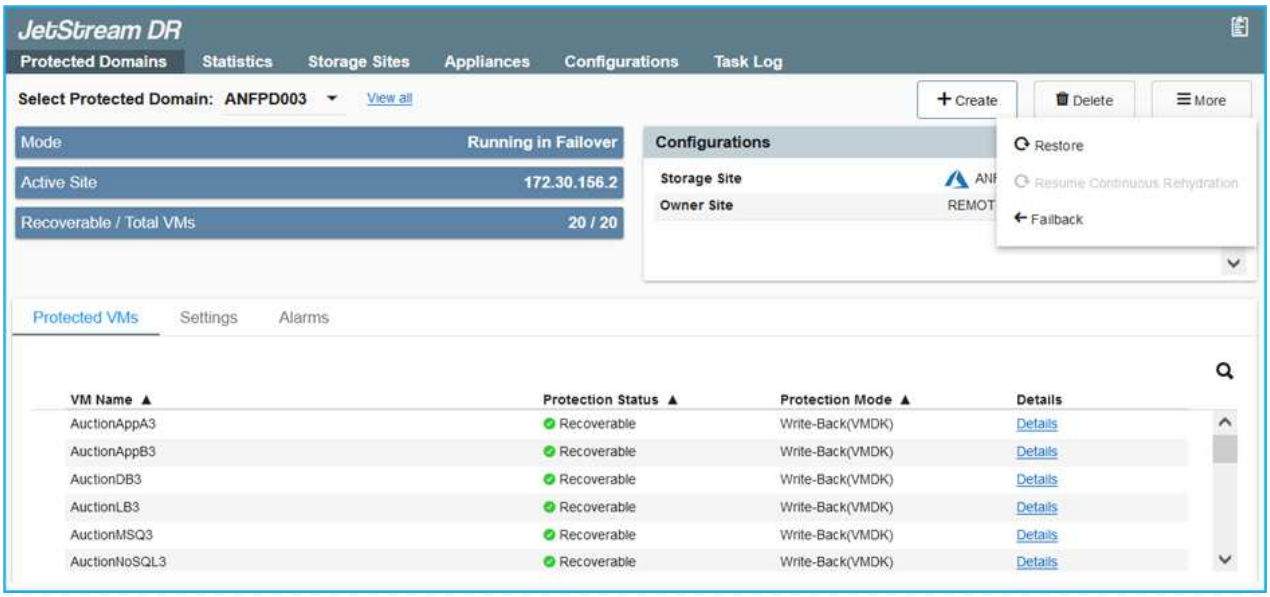



プライマリサイトが起動して再び実行されるようになったら、フェイルバックを実行できます。VM保護が再開され、データの整合性を確認する必要があります。

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

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

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



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

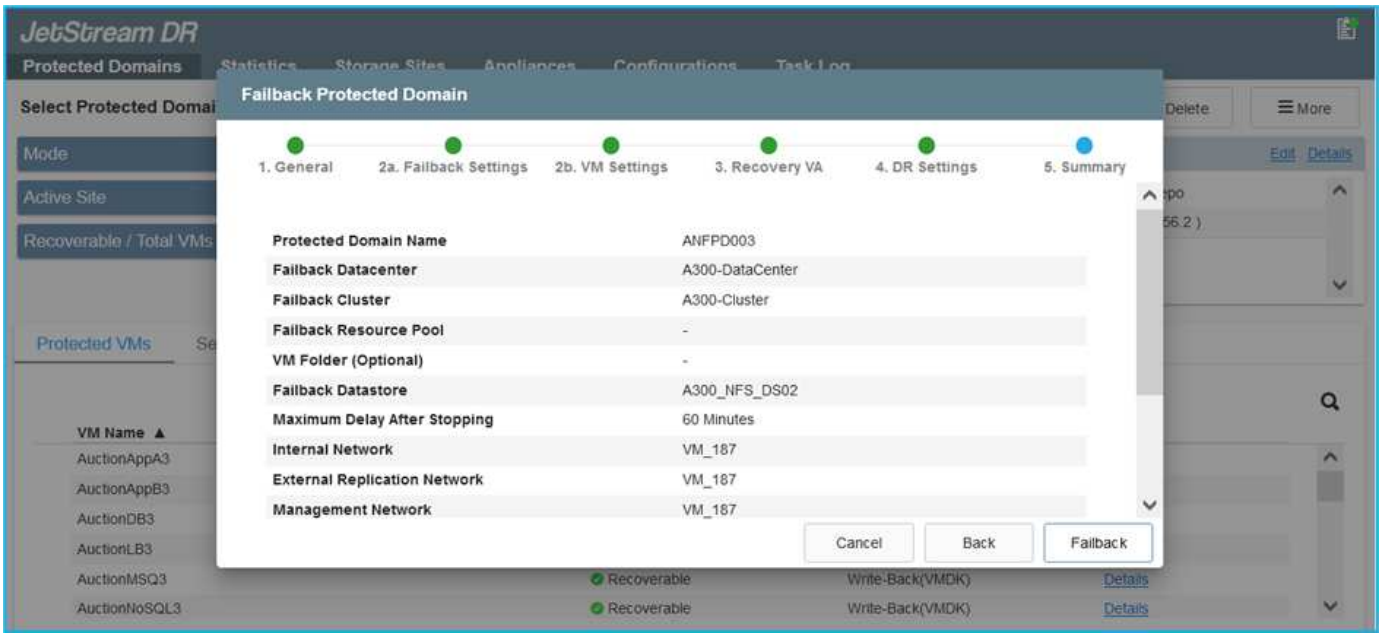
リカバリサイトのVMを一時停止して保護対象サイトで再起動したあとの最大遅延時間を指定します。この時間には、フェイルオーバーVMを停止したあとのレプリケーションの完了、リカバリサイトのクリーンアップにかかる時間、保護サイトでVMを再作成する時間などが含まれます。ネットアップの推奨値は10分です。

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

### Ransomware回復

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

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




# CVOとAVS（ゲスト接続ストレージ）によるディザスタリカバリ

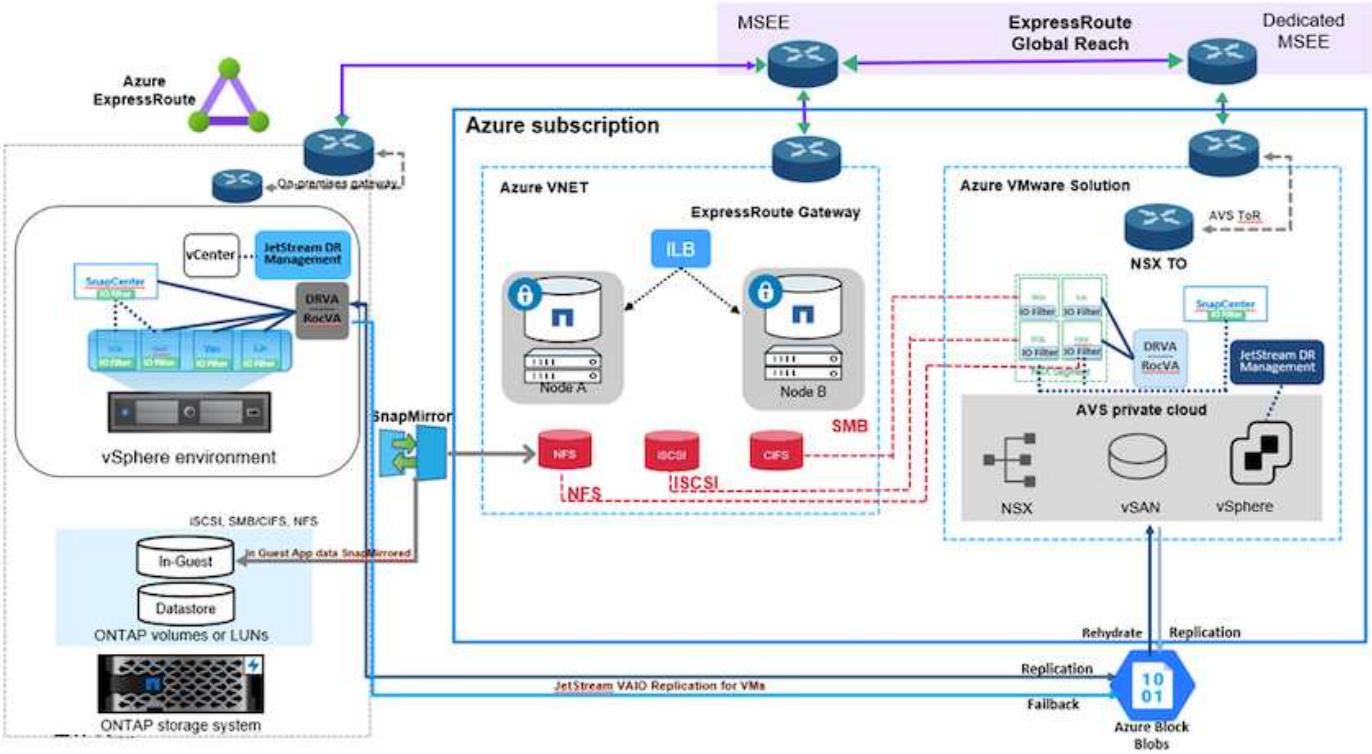
## 概要

著者：Ravi BCBとNiyaz Mohamedネットアップ

クラウドへのディザスタリカバリは、耐障害性と対費用効果に優れた方法で、サイトの停止やランサムウェア

などのデータ破損からワークロードを保護します。NetApp SnapMirrorを使用すると、ゲスト接続ストレージを使用するオンプレミスのVMwareワークロードを、Azure内で実行されているNetApp Cloud Volumes ONTAP にレプリケートできます。これはアプリケーションデータに適用されますが、実際のVM自体についてはどうでしょうか。ディザスタリカバリは、仮想マシン、VMDK、アプリケーションデータなど、依存するすべてのコンポーネントを対象にする必要があります。これを実現するために、JetstreamとSnapMirrorを併用すると、VM VMDK用のVSANストレージを使用しながら、オンプレミスからCloud Volumes ONTAP にレプリケートされたワークロードをシームレスにリカバリできます。

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




## 前提条件

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

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

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

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

## DR解決策 の導入

### 解決策 の導入の概要

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

### 展開の詳細

#### **Azure**で**CVO**を構成し、ボリュームを**CVO**にレプリケート

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

| Health Status | Source Volume | Target Volume | Total Transfer Time | Status | Mirror State | Last Successful Transfer |
|---|---|---|---|---|---|---|
| ✓ | gcsdrsqldb_sc46 ntaphci-a300e9u25 | gcsdrsqldb_sc46_copy ANFCVODRDemo | 17 seconds | idle | snapmirrored | May 6, 2022, 11:43:18 AM 105.06 KiB |
| ✓ | gcsdrsqlhld_sc46_copy ANFCVODRDemo | gcsdrsqlhld_sc46 ntaphci-a300e9u25 | 7 seconds | idle | snapmirrored | May 6, 2022, 11:42:20 AM 7.22 MiB |
| ✓ | gcsdrsqllog_sc46 ntaphci-a300e9u25 | gcsdrsqllog_sc46_copy ANFCVODRDemo | 16 seconds | idle | snapmirrored | May 6, 2022, 11:43:52 AM 130.69 KiB |

**AVS**ホストと**CVO**データアクセスを設定

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

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

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

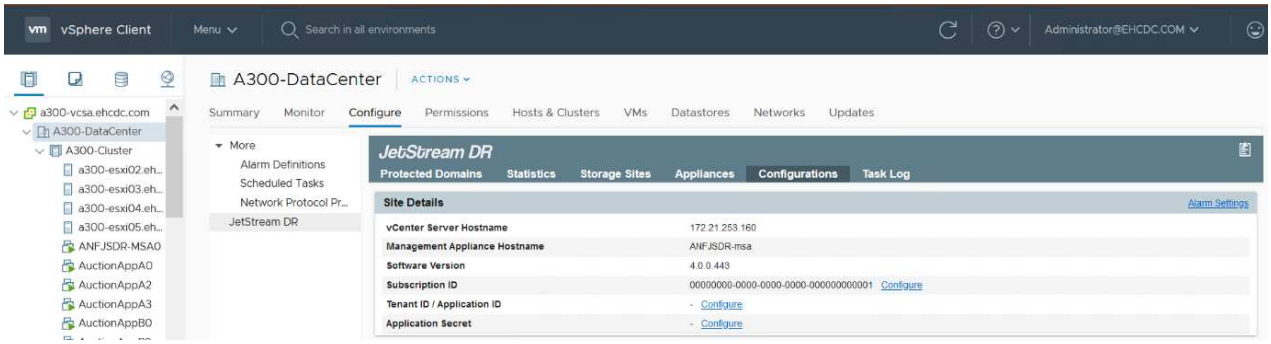
AVS SDDCを設定するには（オンデマンドモードまたはパイロットライトモード）、を参照してください "Azure に仮想化環境を導入して設定"。事前に、接続の確立後、AVSホストに常駐するゲストVMがCloud Volumes ONTAP からデータを消費できることを確認してください。

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

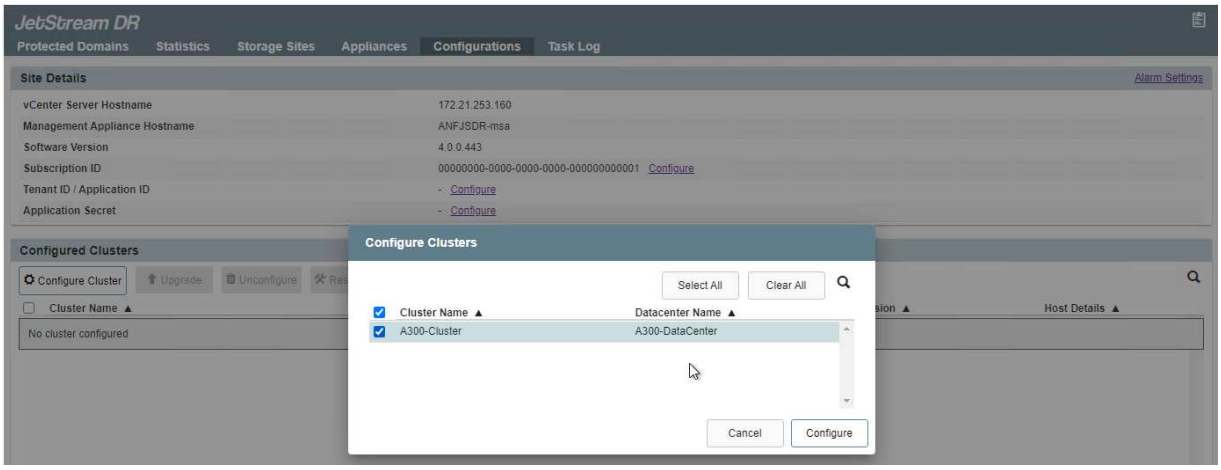
### JetStream DRをオンプレミスデータセンターにインストールします

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

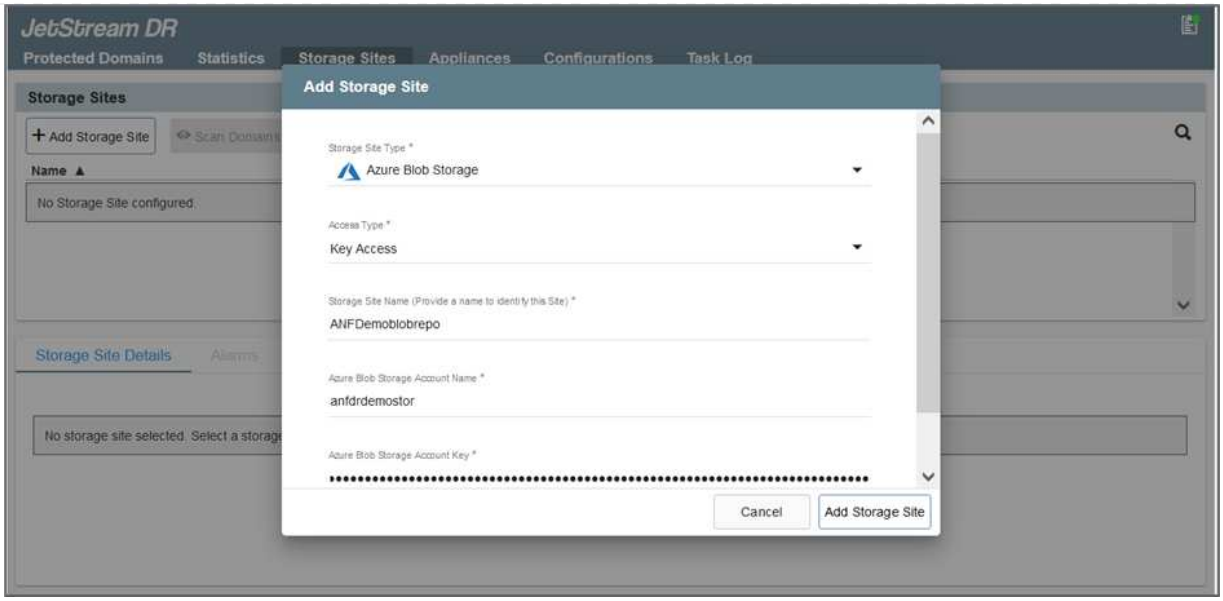
1. 前提条件を確認します。
2. リソースと構成に関する推奨事項については、Capacity Planning Toolを実行してください。
3. JetStream DR MSAを、指定されたクラスタ内の各vSphereホストに導入します。
4. ブラウザでDNS名を使用してMSAを起動します。
5. vCenterサーバをMSAに登録します。
6. JetStream DR MSAが導入され、vCenter Serverが登録されたら、vSphere Web ClientでJetStream DRプラグインに移動します。これを行うには、[データセンター]>[設定]>[JetStream DR]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




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

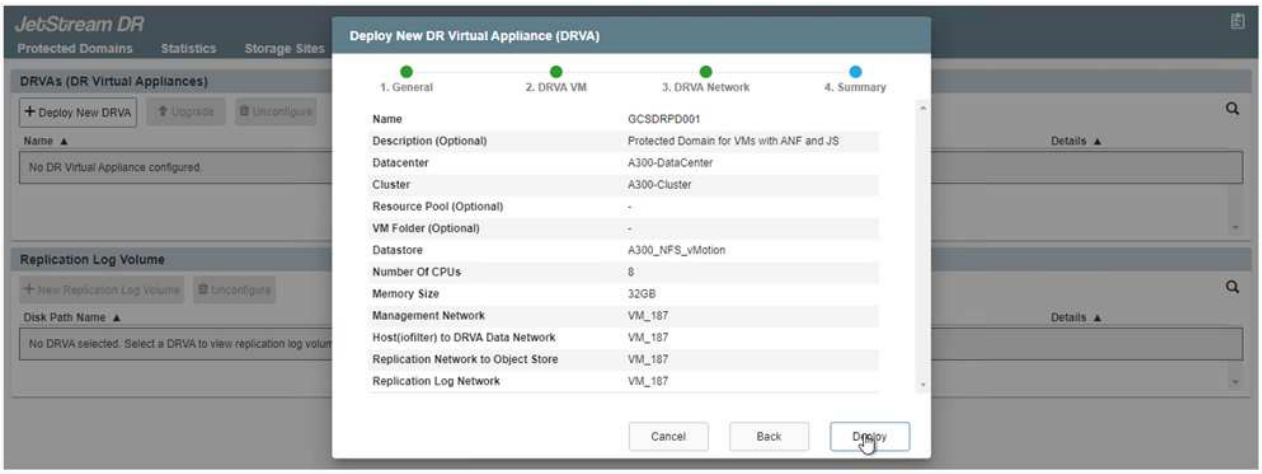



   b. リカバリサイトにあるAzure BLOBストレージを追加します。

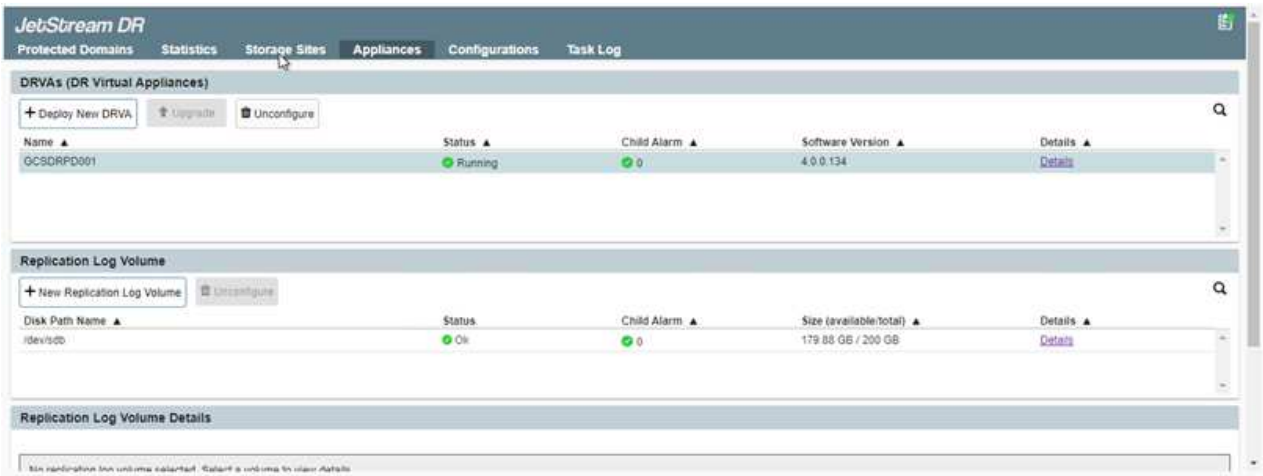



8. アプライアンスタブから必要な数のDR仮想アプライアンス（DRVA）を導入します。

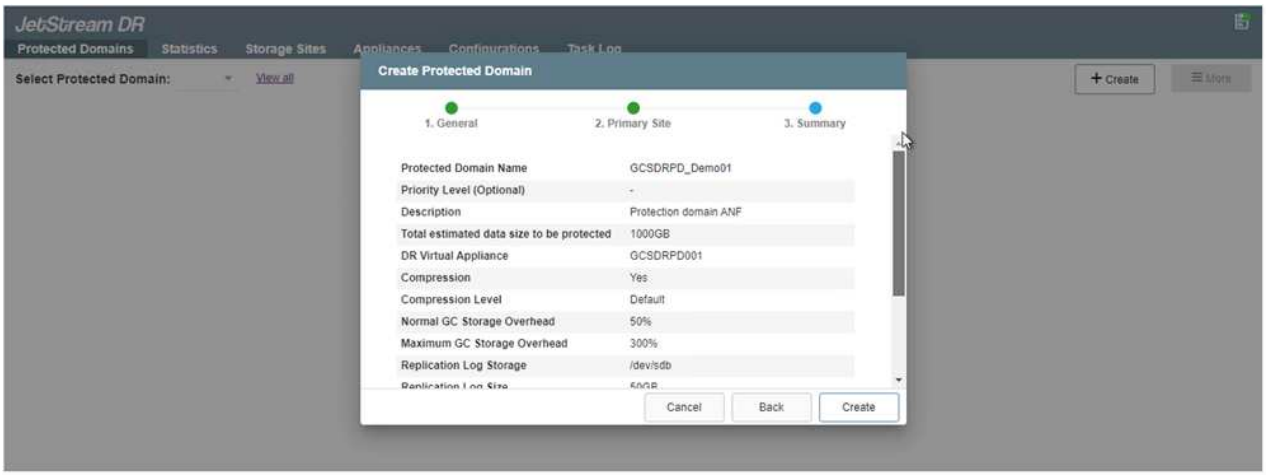
キャパシティプランニングツールを使用して、必要なDRVAの数を見積もります。

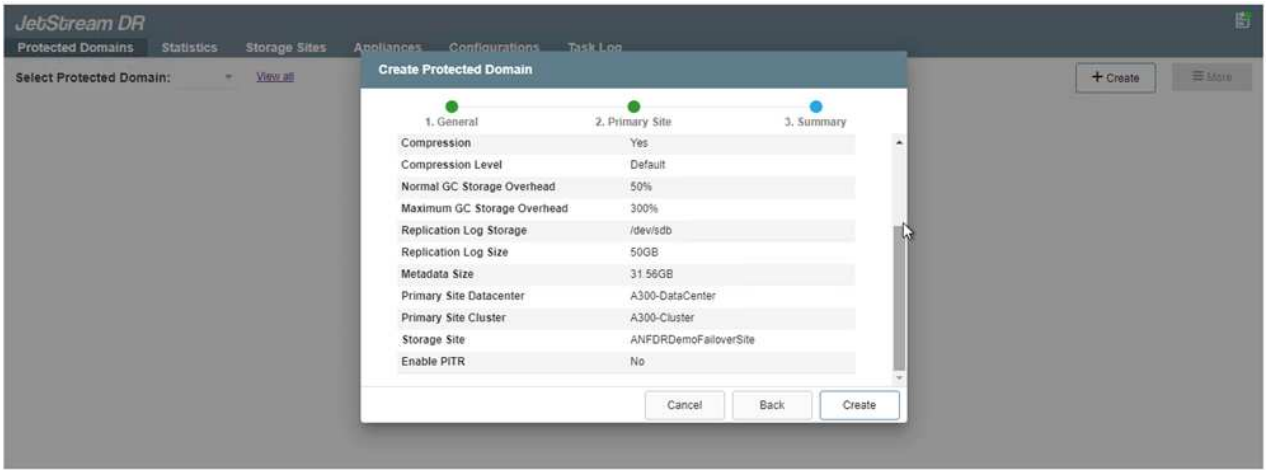




9. 使用可能なデータストアまたは独立した共有iSCSIストレージプールからVMDKを使用して、各DRVAのレプリケーションログボリュームを作成します。




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

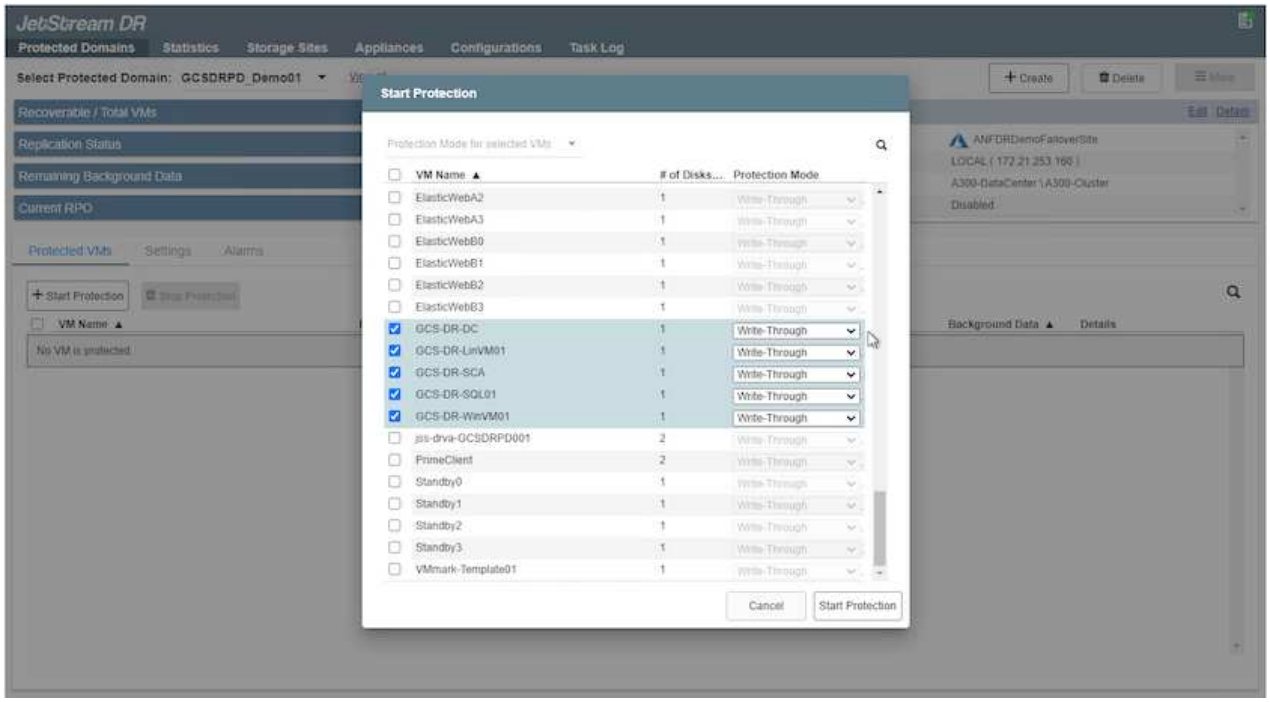


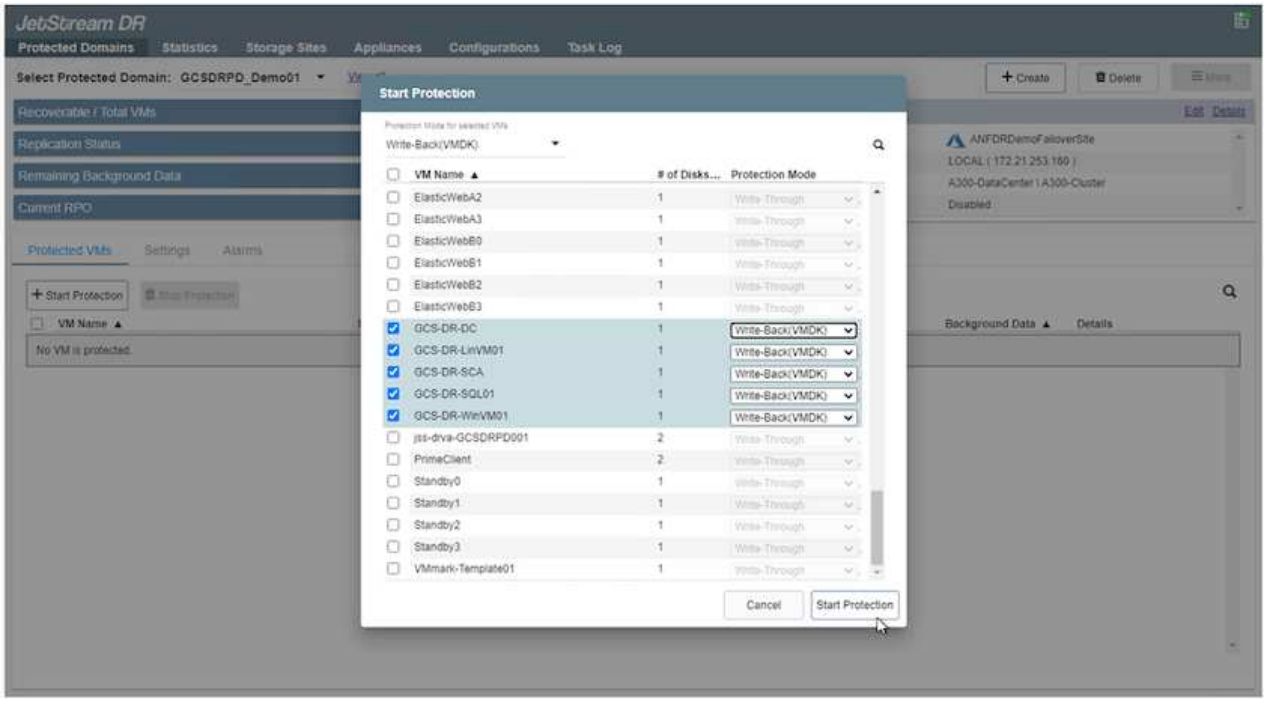

11. 保護するVMを選択し、依存関係に基づいてVMをアプリケーショングループにグループ化します。アプリケーション定義を使用すると、VMのセットを、ブート順序、ブート遅延、およびリカバリ時に実行可能なオプションのアプリケーション検証を含む論理グループにグループ化できます。

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

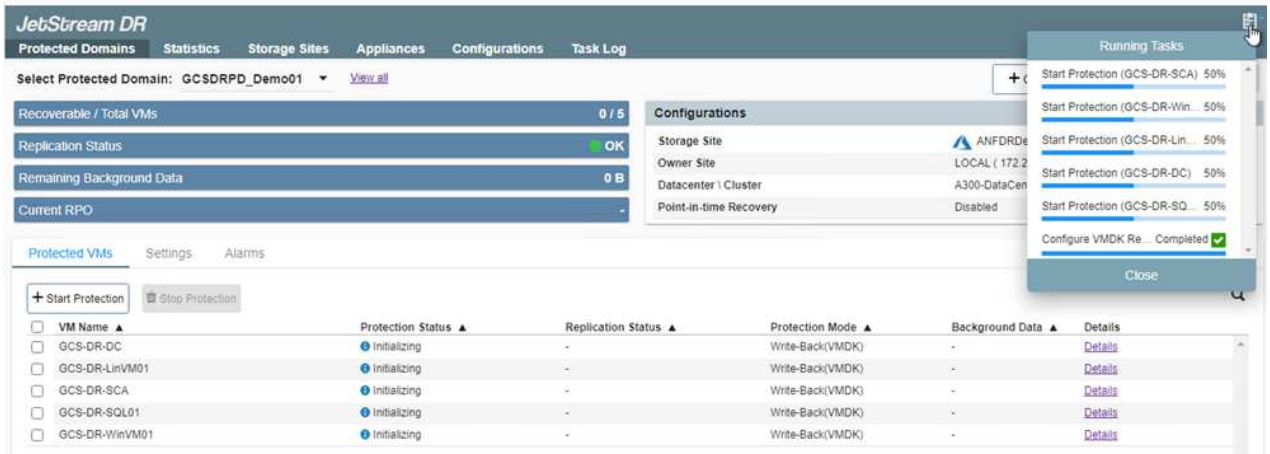
ライトバック（VMDK）モードを使用すると、パフォーマンスが向上します。



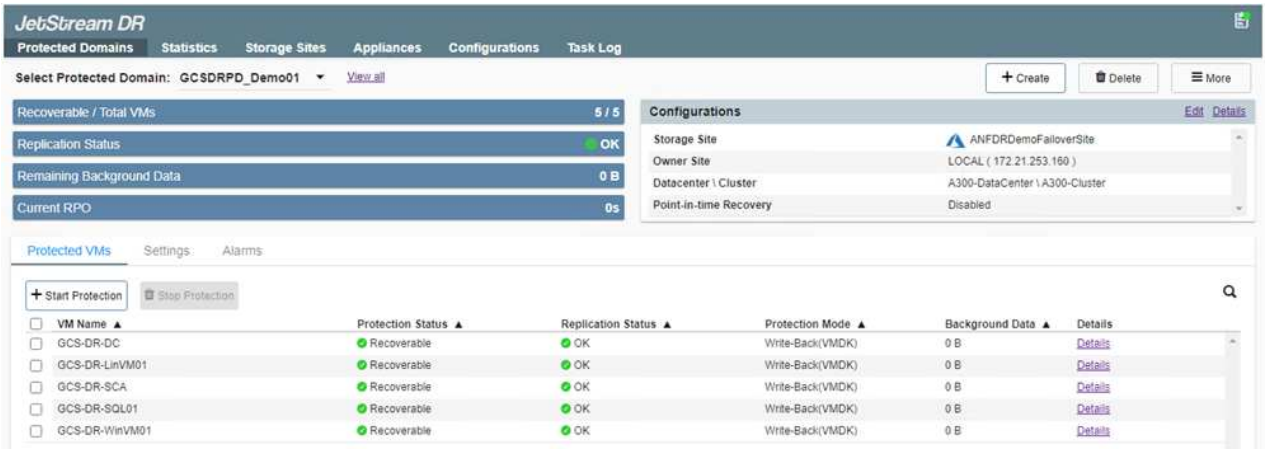

12. レプリケーションログボリュームがハイパフォーマンスストレージに配置されていることを確認します。




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




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

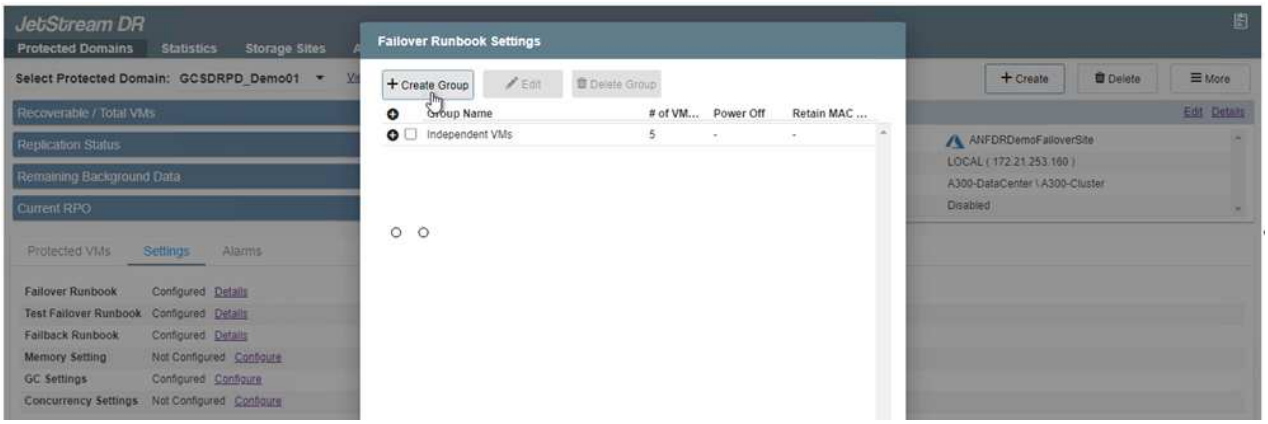



フェールオーバーランブックは、VM（回復グループと呼ばれる）をグループ化し、起動順序シーケンスを設定して、CPU /メモリ設定とIP設定を変更するように構成できます。

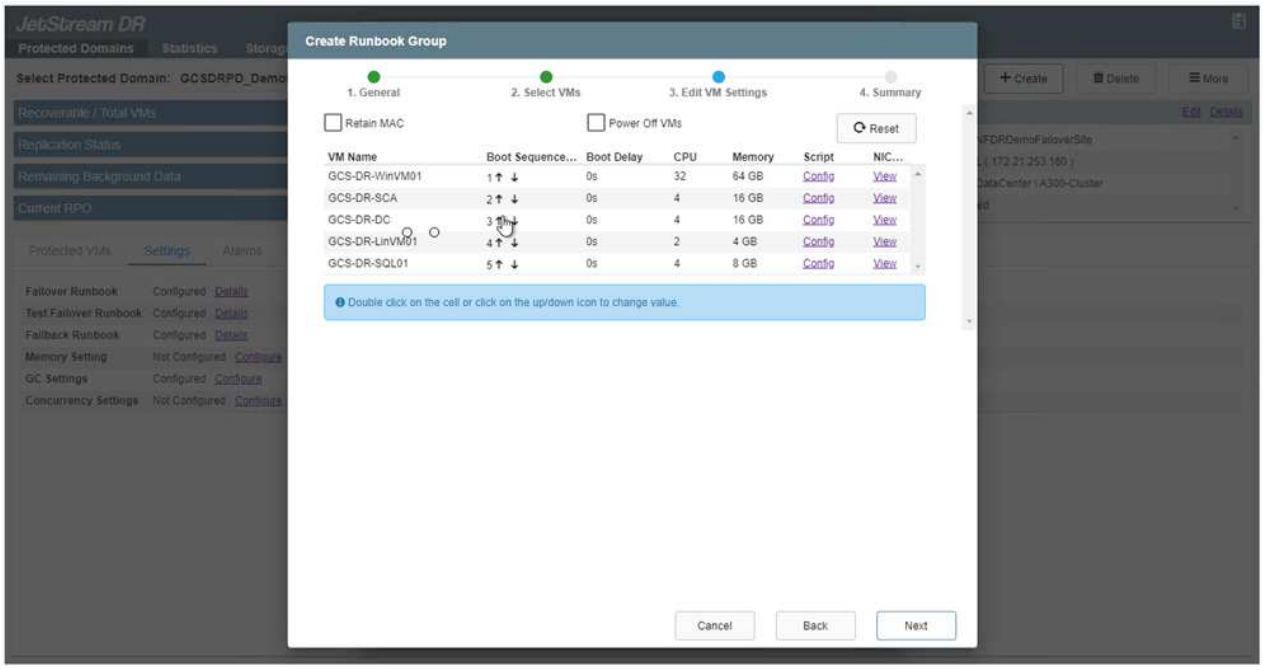
15. 「設定」をクリックし、「Runbook設定」リンクをクリックして、Runbookグループを設定します。


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

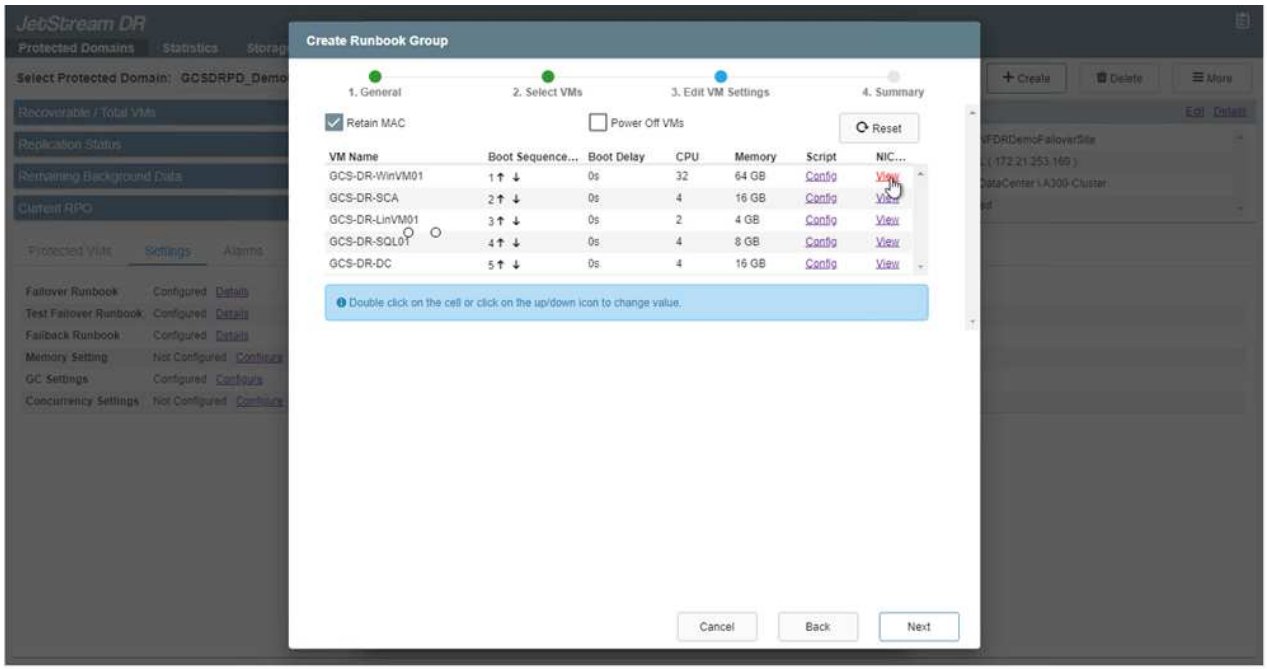
必要に応じて、画面の下部で、カスタムのプレスクリプトとポストスクリプトを適用して、ランブックグループの操作前および操作後に自動的に実行します。Runbookスクリプトが管理サーバ上に存在することを確認します。



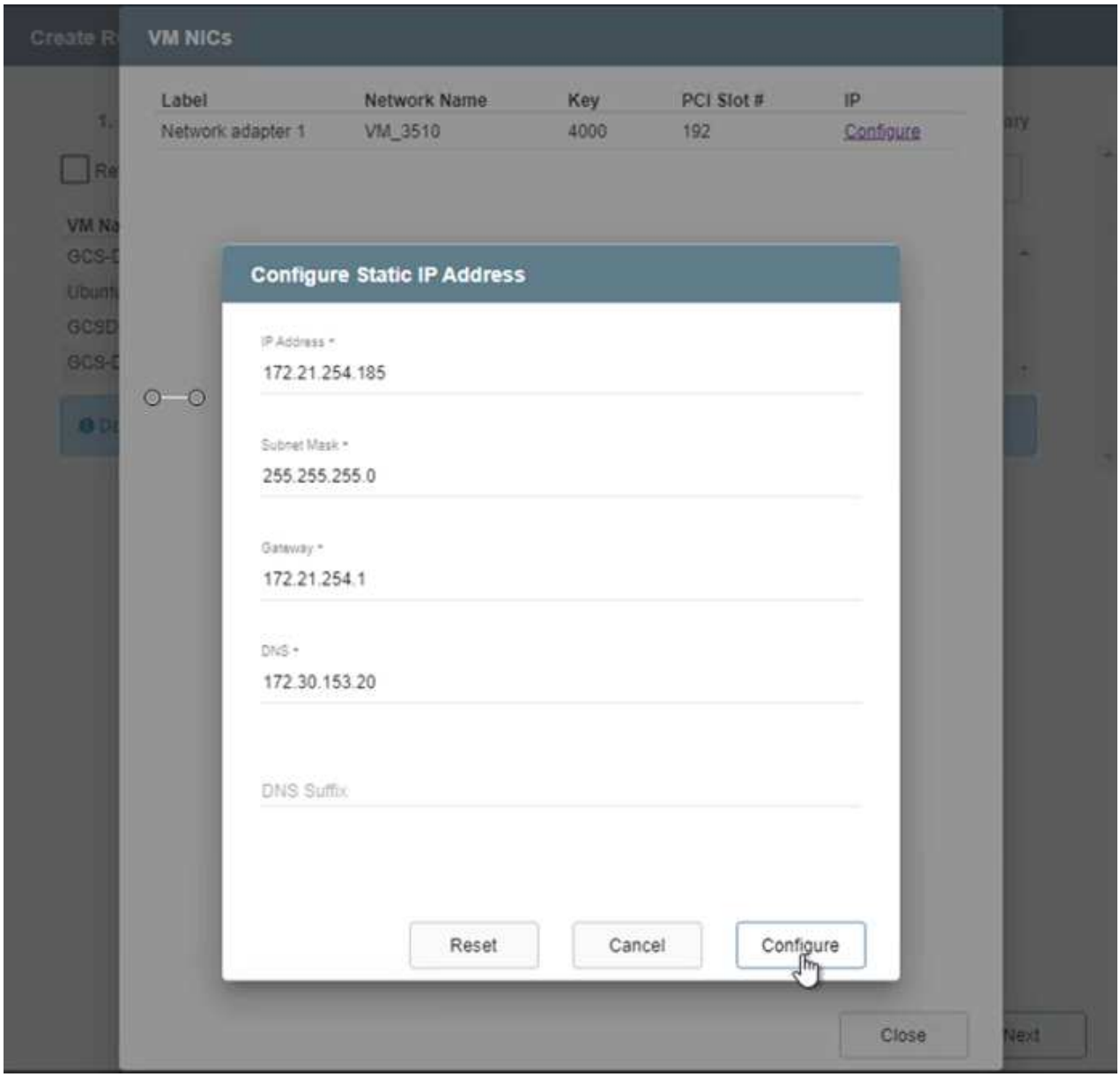

17. 必要に応じてVMの設定を編集します。VMをリカバリするためのパラメータを指定します。これには、ブートシーケンス、ブート遅延（秒単位）、CPUの数、割り当てるメモリの量などが含まれます。上下の矢印をクリックして、VMのブートシーケンスを変更します。MACを保持するためのオプションも用意されています。

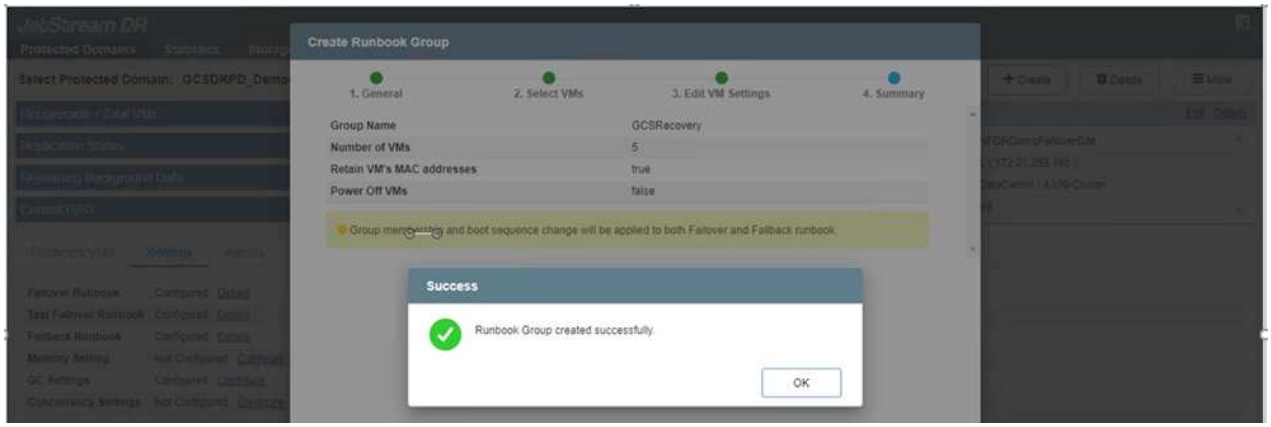



18. 静的IPアドレスは、グループの個々のVMに手動で設定できます。VMのNICビューリンクをクリックして、IPアドレスを手動で設定します。




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




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

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。

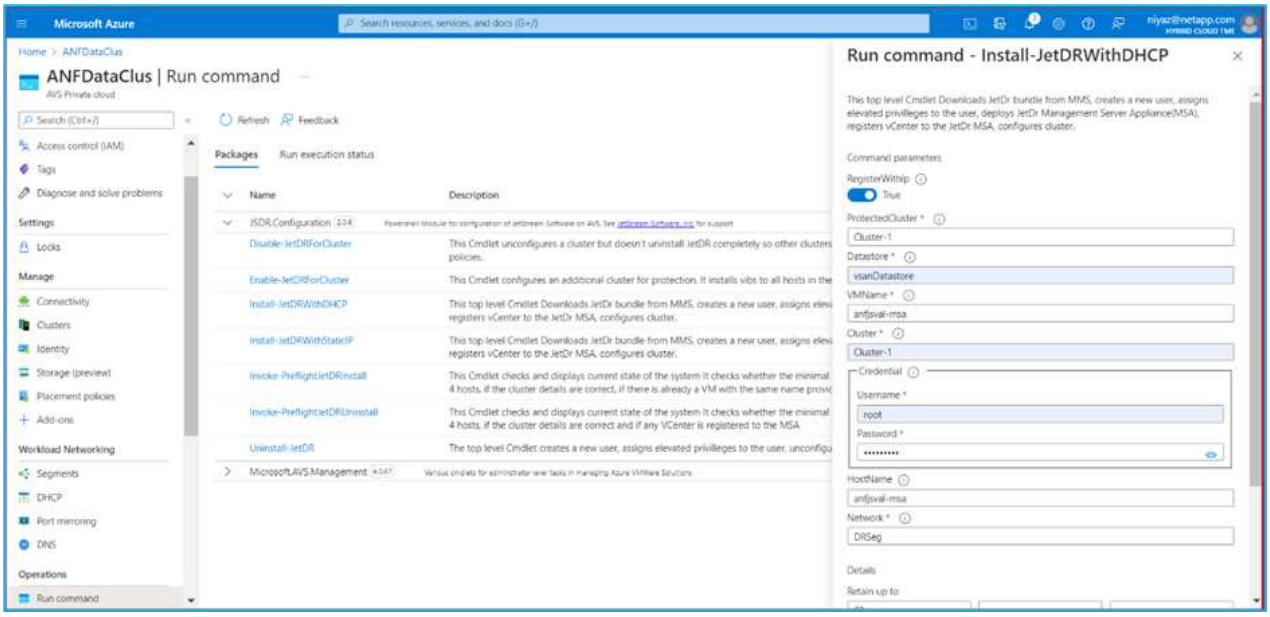
> セグメント作成を含むネットワーク構成は、オンプレミスの要件に合わせてAVSクラスタ上で設定する必要があります。

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

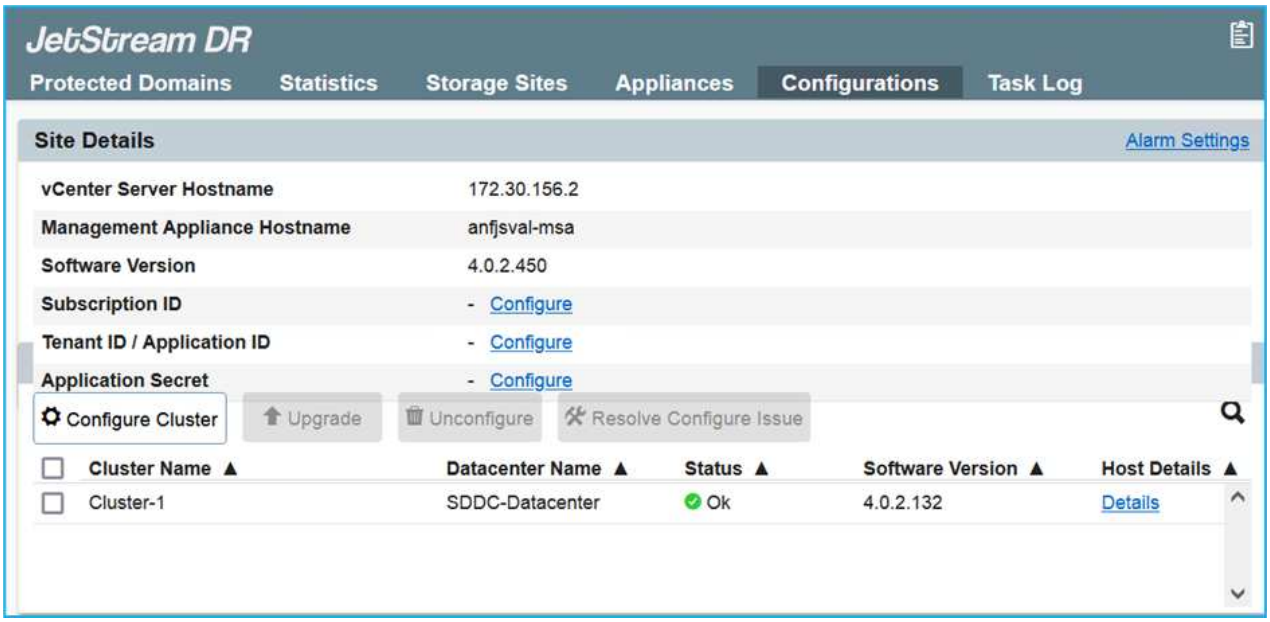
1. Azure VMware解決策 プライベートクラウドにJetStream DR for AVSをインストールするには、実行コマンドを使用します。Azureポータルで、Azure VMware解決策 に移動し、プライベートクラウドを選択して、実行コマンド>パッケージ> JSDR.Configurationを選択します。

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

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



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




3. JetStream DRインターフェイスから、次の作業を行います。

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

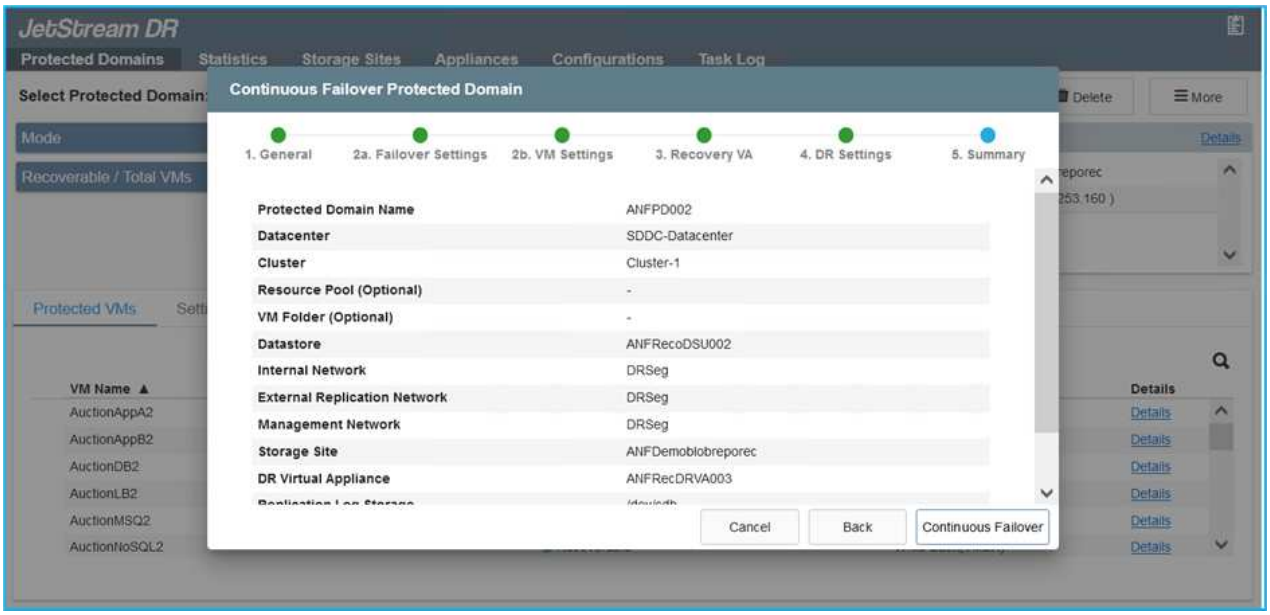
   b. 表示されるポップアップダイアログで、インポートする保護ドメインを選択し、そのインポートリンクをクリックします。


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

5. 保護ドメインをインポートしたら、DRVAアプライアンスを展開します。

> これらの手順は、CPT作成プランを使用して自動化することもできます。

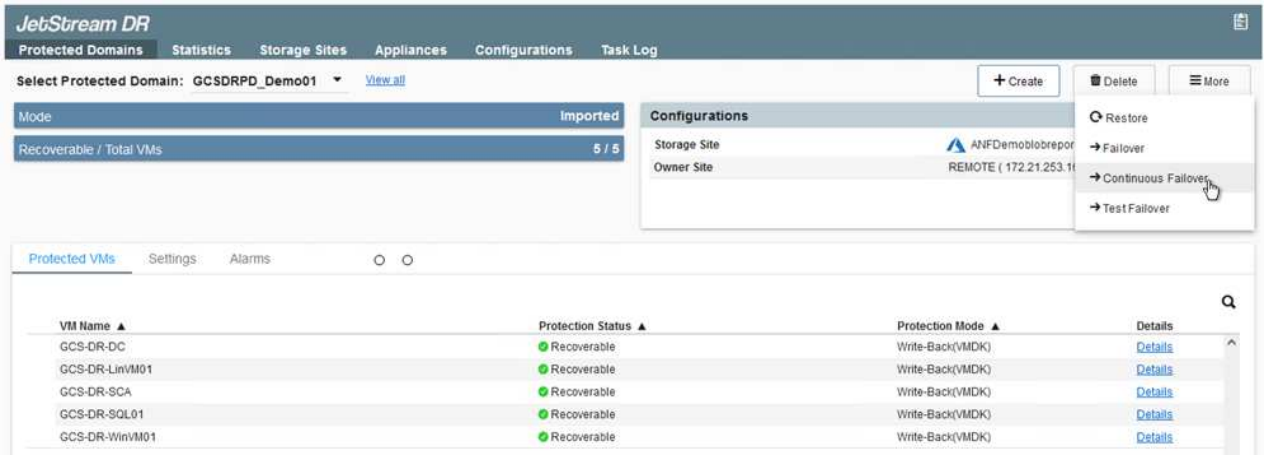
6. 使用可能なvSANまたはANFデータストアを使用してレプリケーションログボリュームを作成します。
7. 保護ドメインをインポートし、VMの配置にANFデータストアを使用するようにリカバリVAを設定します。




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

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

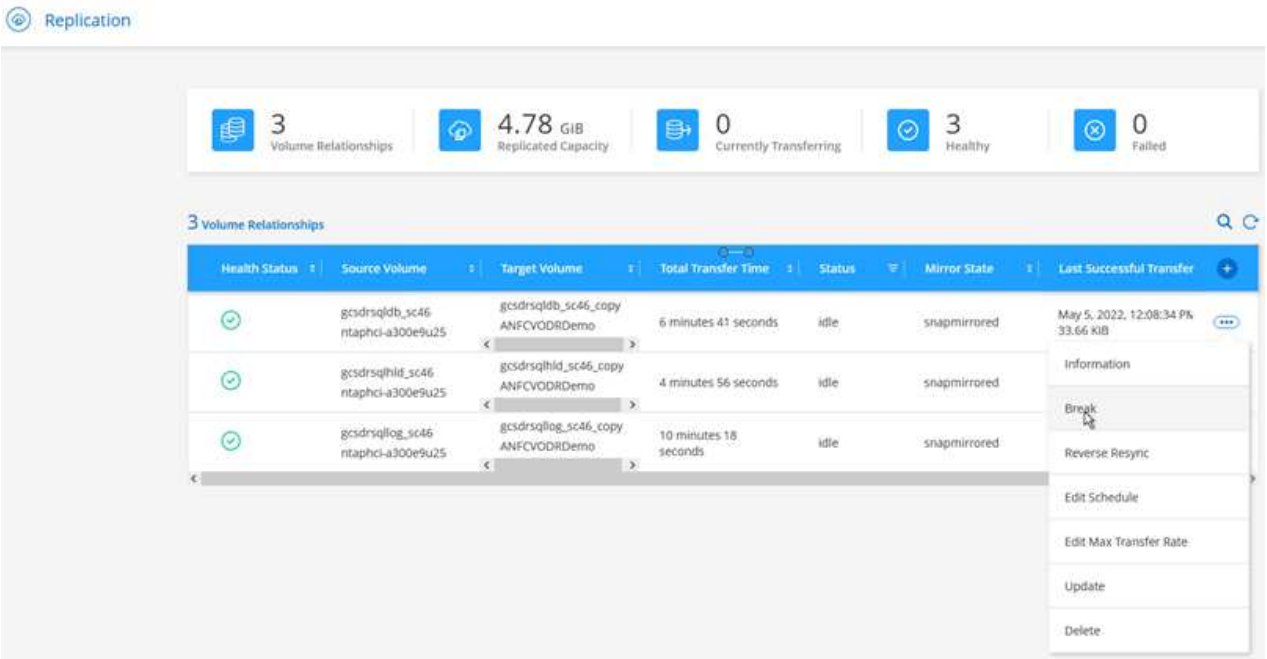
> 設定の実行時には、継続的フェイルオーバーモードとフェイルオーバーモードが異なりますが、両方のフェイルオーバーモードを同じ手順で設定します。フェイルオーバー手順は、災害発生時の対応として一緒に設定および実行されます。継続的フェイルオーバーはいつでも設定でき、通常のシステム運用中はバックグラウンドで実行できます。災害が発生すると、継続的なフェイルオーバーが完了し、保護対象のVMの所有権がリカバリサイトにただちに移行されます（RTOはほぼゼロ）。

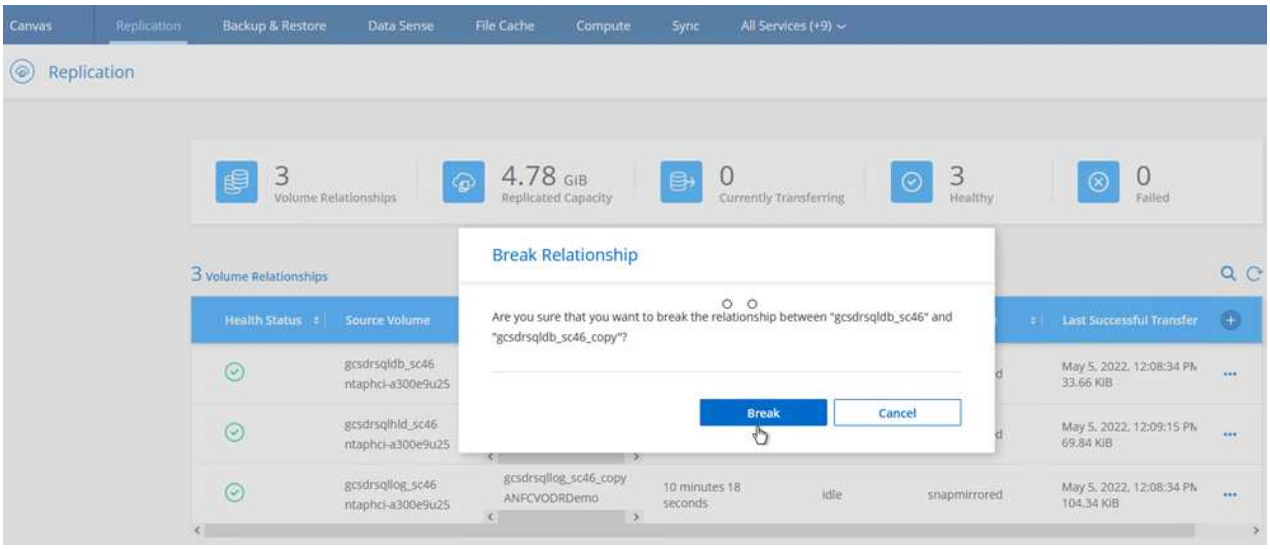



継続的なフェイルオーバープロセスが開始され、UIから進行状況を監視できます。[現在のステップ]セクションの青いアイコンをクリックすると、ポップアップウィンドウが開き、フェイルオーバープロセスの現在のステップの詳細が表示されます。

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。

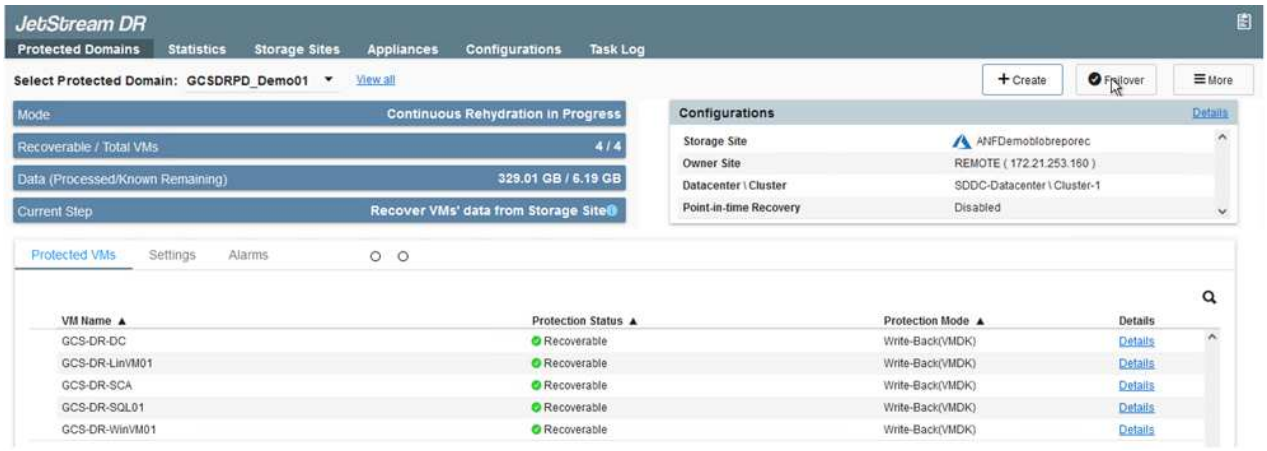


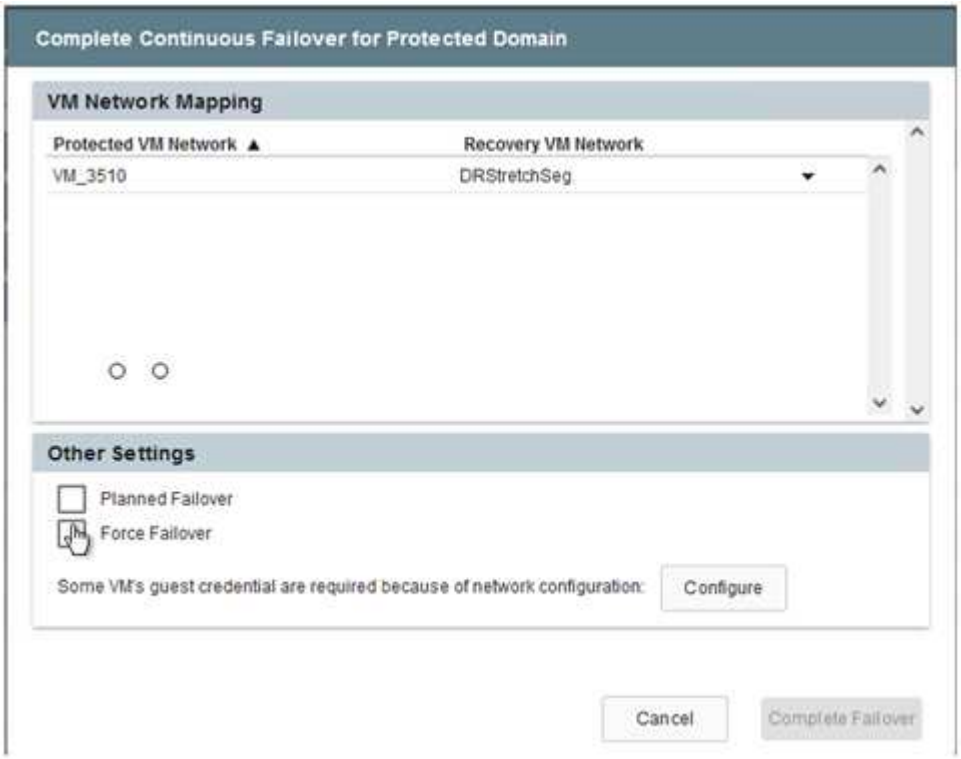




この手順は簡単に自動化できるため、リカバリプロセスが容易になります。

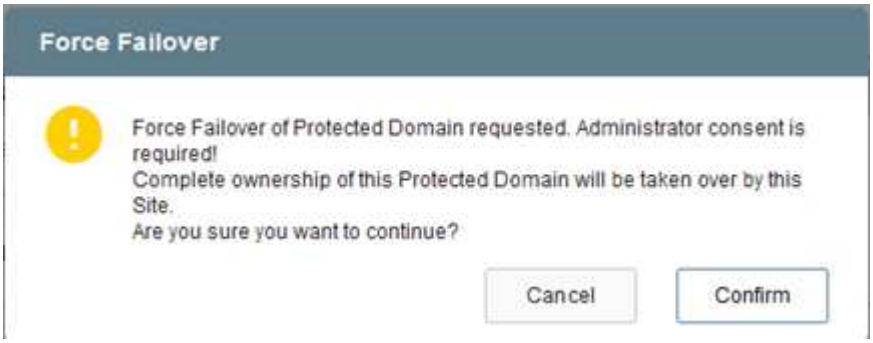
2. AVS SDDC（宛先側）上のJetstream UIにアクセスし、フェールオーバーオプションをトリガしてフェールオーバーを完了します。タスクバーにフェイルオーバーアクティビティの進行状況が表示されます。

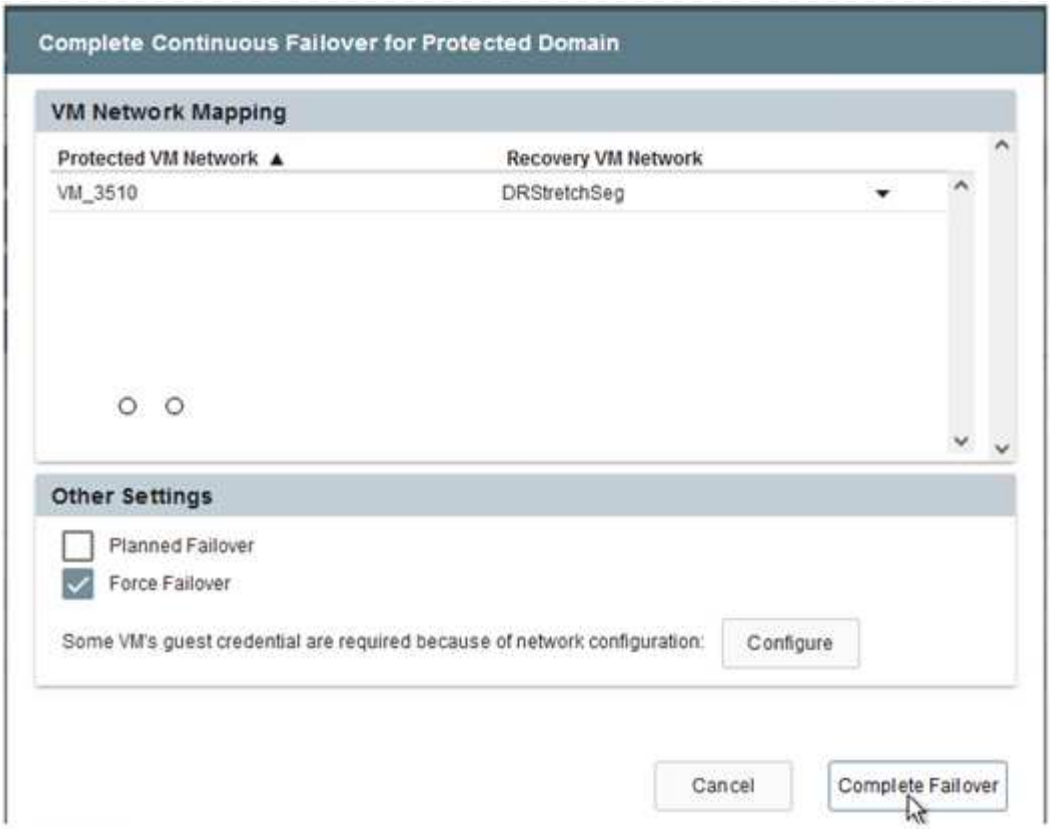
   フェイルオーバーが完了したときに表示されるダイアログウィンドウで、フェイルオーバータスクを計画どおりに指定することも、強制的に実行することもできます。




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



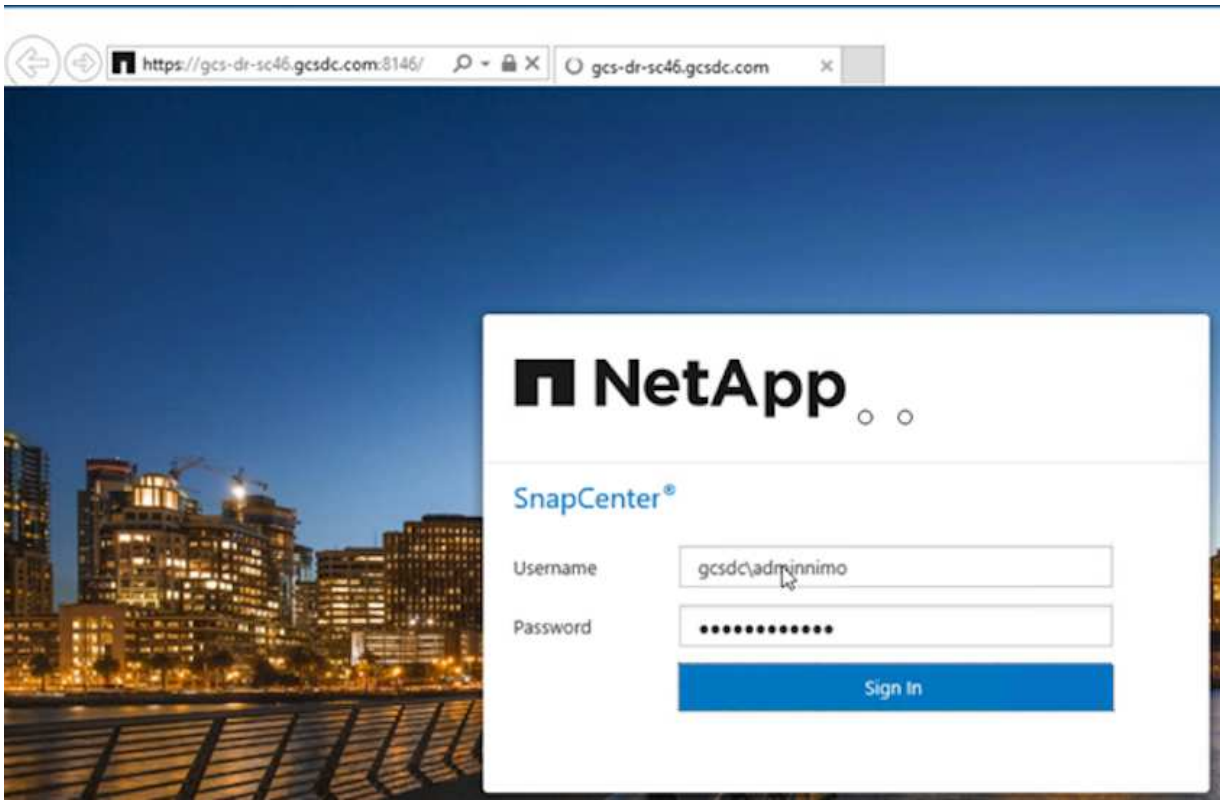



3. 継続的なフェイルオーバーが完了すると、タスクの完了を確認するメッセージが表示されます。タスクが完了したら、リカバリしたVMにアクセスしてiSCSIセッションまたはNFSセッションを設定します。

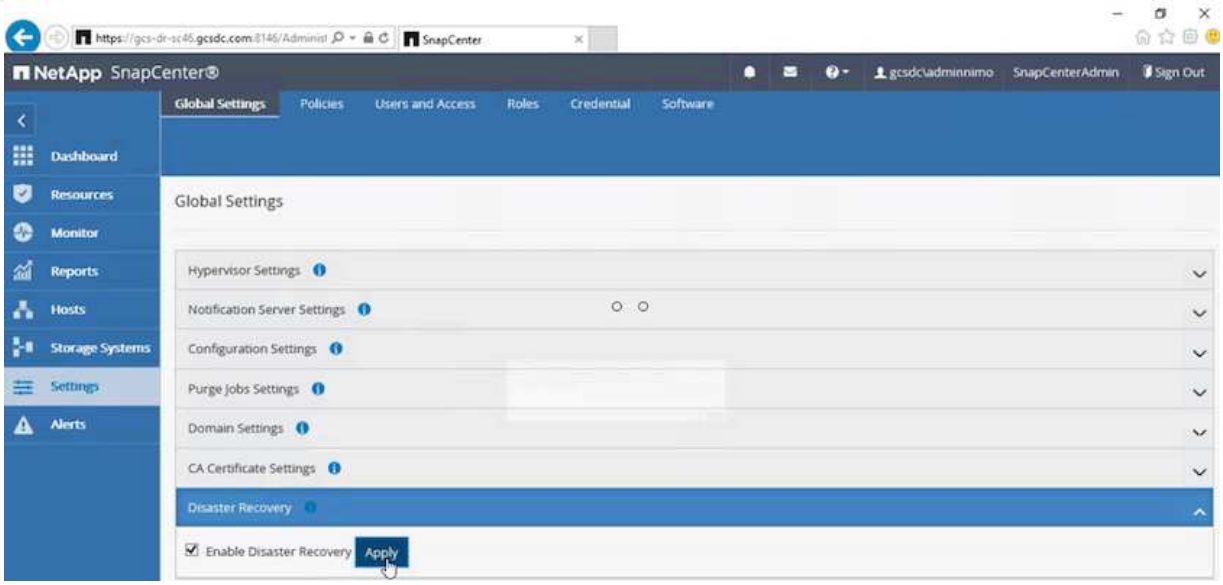
> フェイルオーバーモードが「Running in Failover」に変わり、VMのステータスが「Recoverable」になります。保護ドメインのすべてのVMが、フェールオーバーランブック設定で指定された状態でリカバリサイトで実行されるようになりました。

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


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



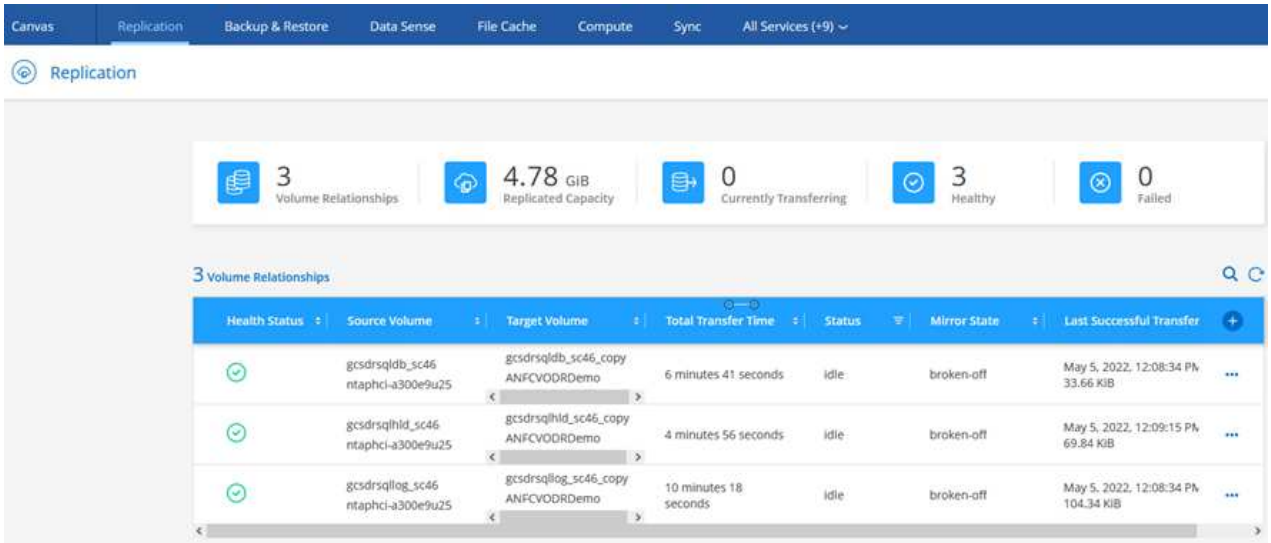

   b. [設定]ページで、[設定]>[グローバル設定]>[ディザスタリカバリ]の順に選択します。
   c. Enable Disaster Recoveryを選択します。
   d. 適用をクリックします。



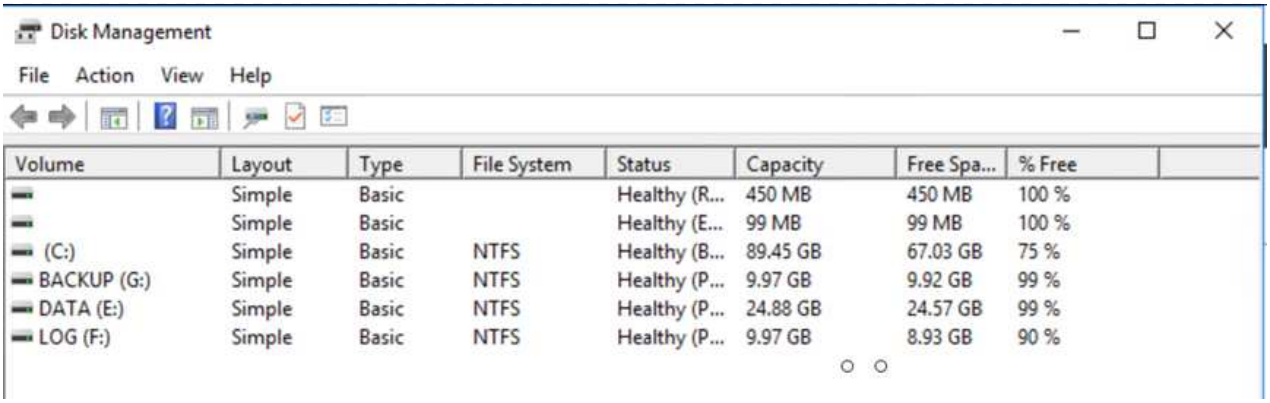

e. [Monitor]>[Jobs]をクリックして、DRジョブが有効になっているかどうかを確認します。

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

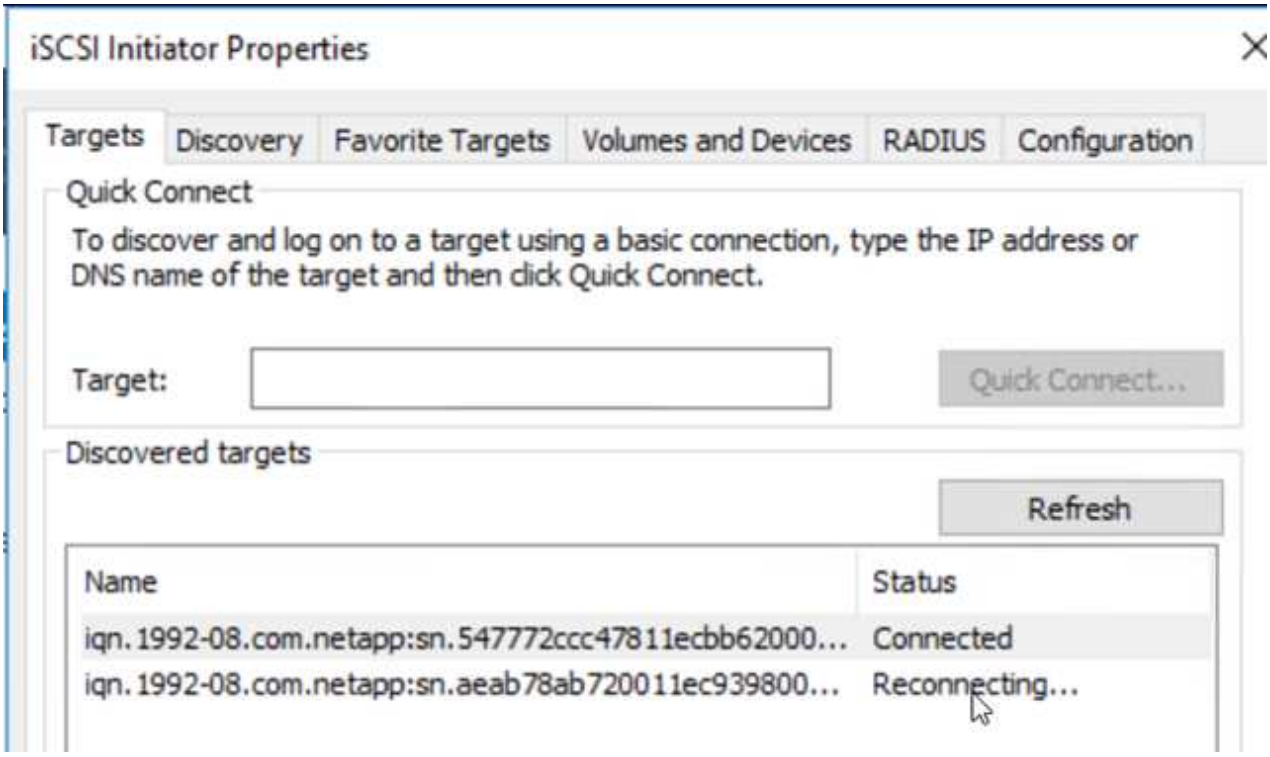
6. SnapMirror関係が解除されていることを確認します。



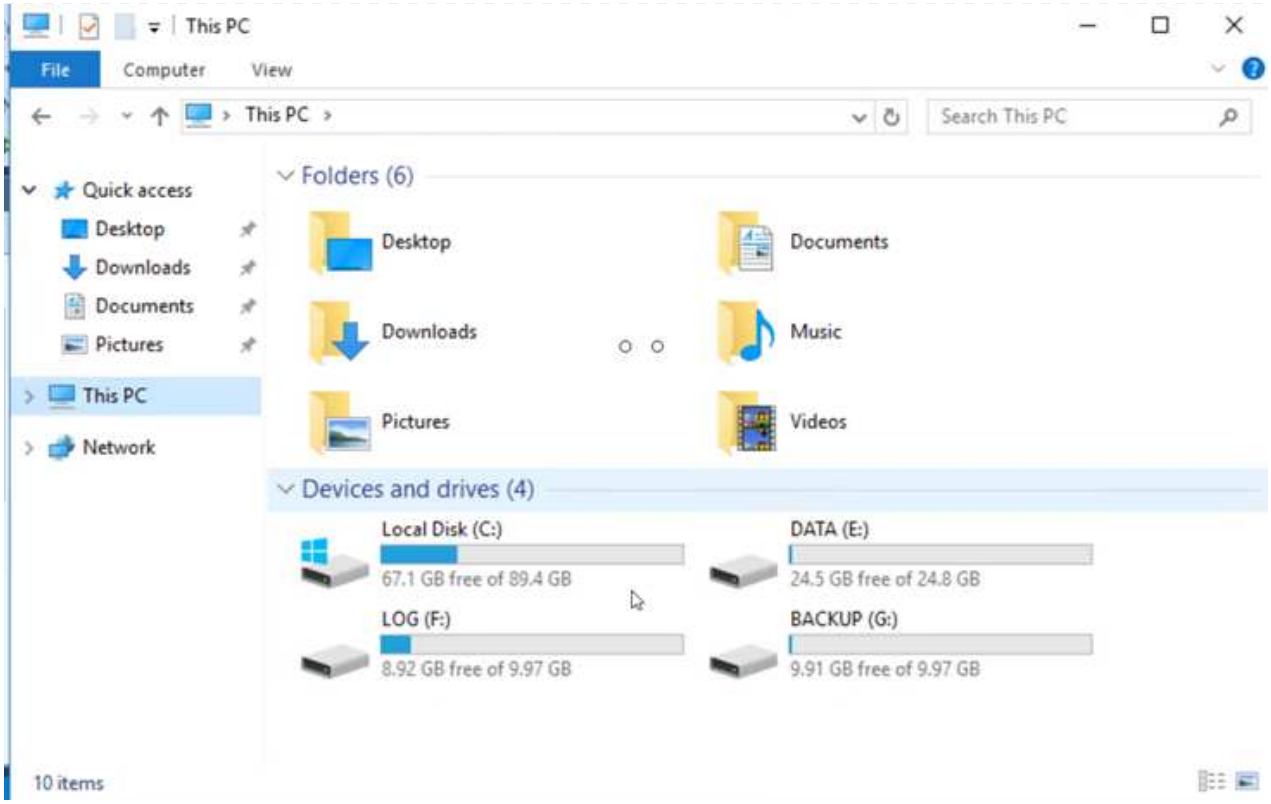

7. Cloud Volumes ONTAP からリカバリしたSQLゲストVMに、同じドライブレターを使用してLUNを接続します。



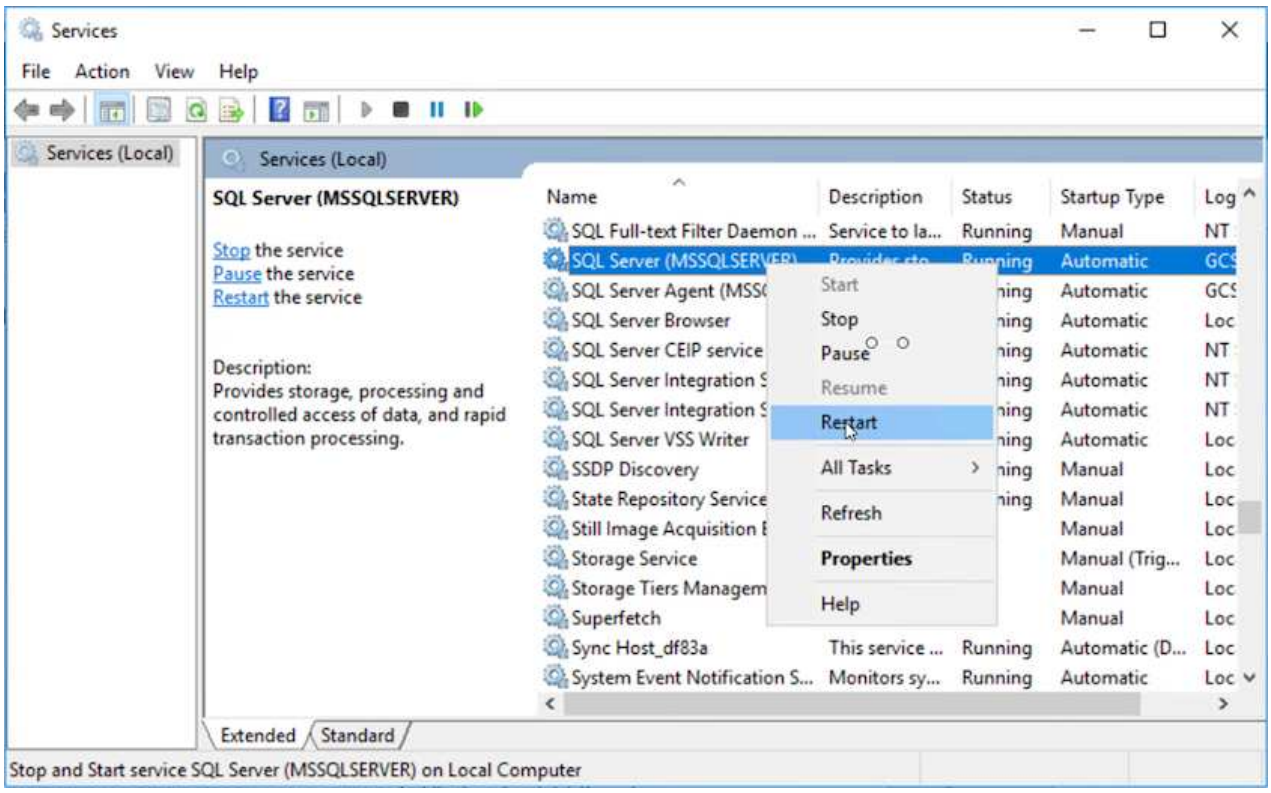

8. iSCSIイニシエータを開き、以前切断したセッションを消去して、レプリケートされたCloud Volumes ONTAP ボリュームのマルチパスとともに新しいターゲットを追加します。



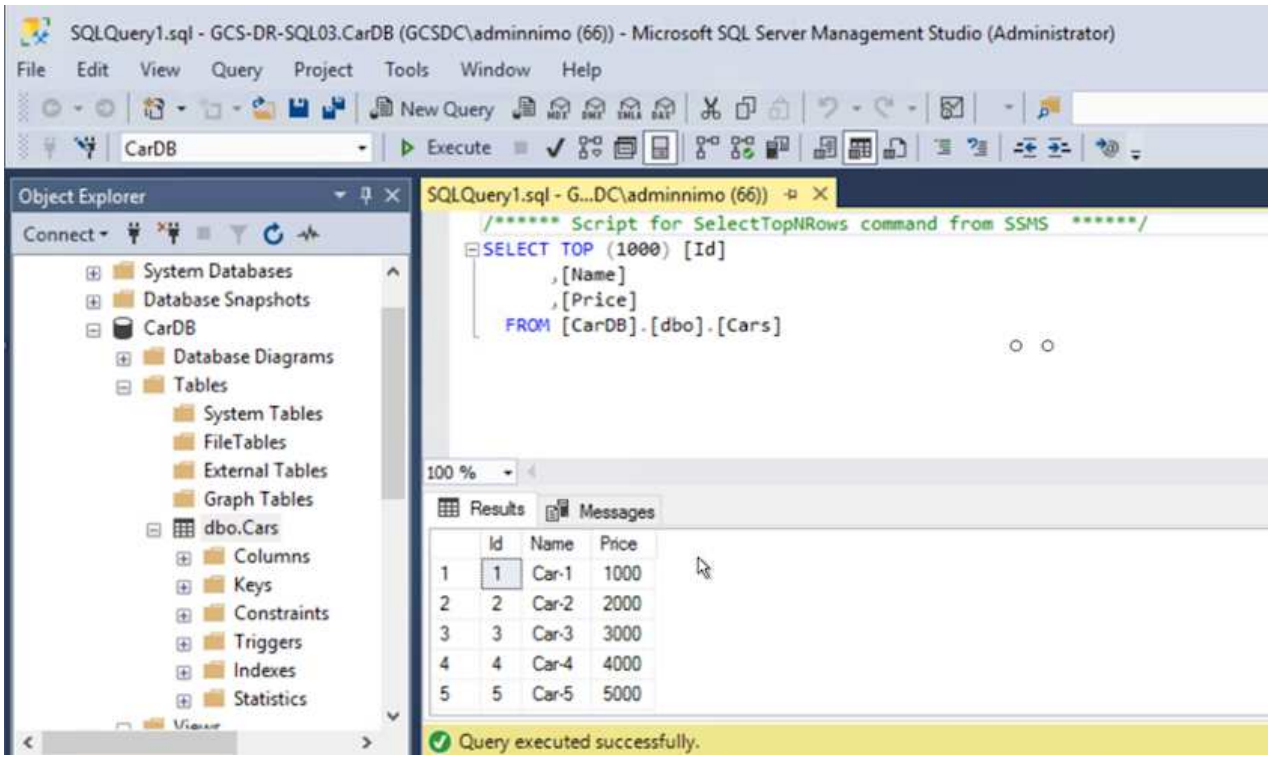

9. DR実行前に使用したのと同じドライブレターを使用して、すべてのディスクが接続されていることを確認してください。




10. MSSQLサーバサービスを再起動します。




11. SQLリソースがオンラインに戻っていることを確認します。




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

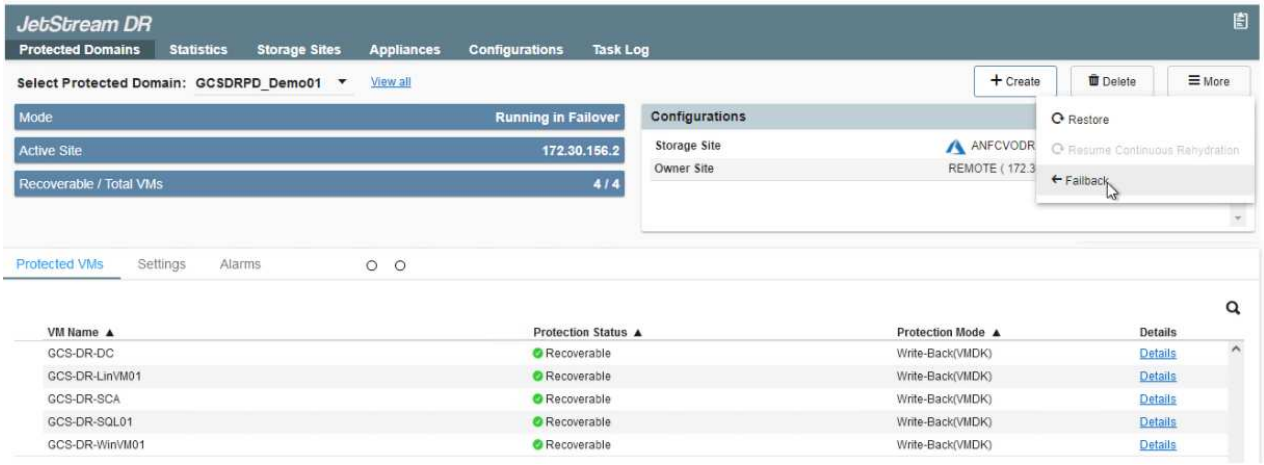
この時点で運用を開始し、通常どおり業務を継続できます。

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

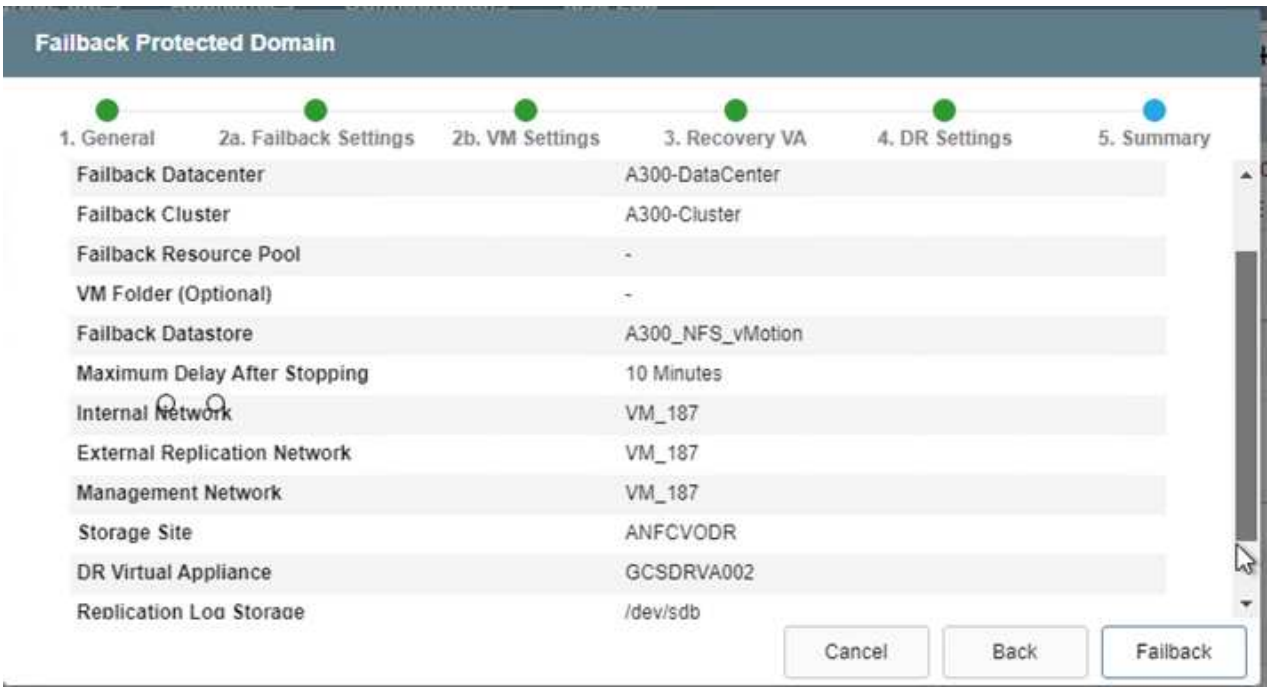
プライマリサイトが起動し、再び実行されるようになったら、フェイルバックを実行できます。VM保護はJetstreamで再開され、SnapMirror関係を反転する必要があります。

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

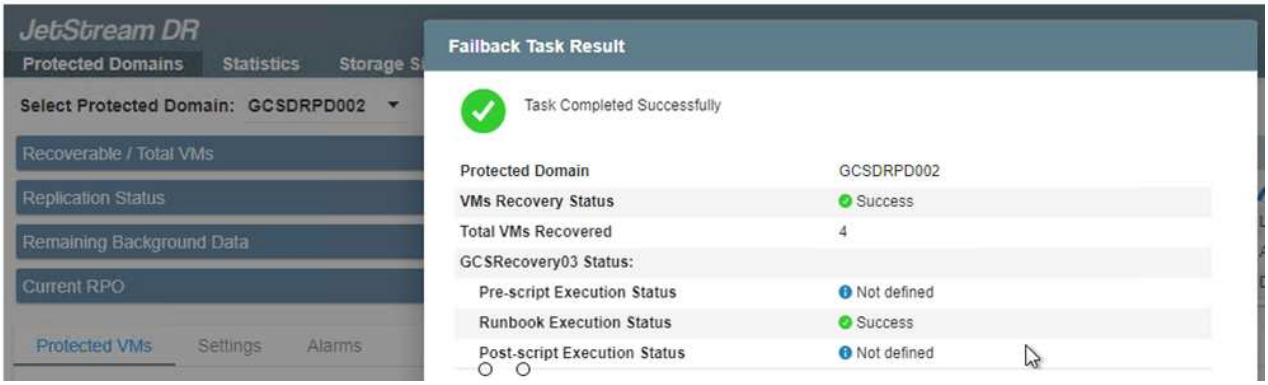
CPTによって生成されたフェイルバック計画を使用して、VMとそのデータをオブジェクトストアから元のVMware環境に戻すこともできます。



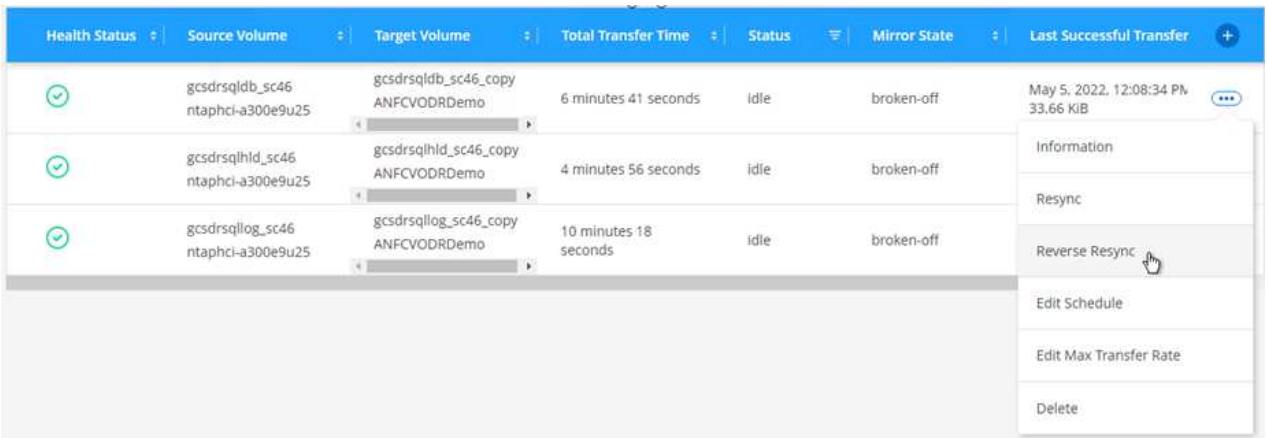

リカバリサイトでVMを一時停止して保護対象サイトで再起動したあとの最大遅延時間を指定します。このプロセスには、フェイルオーバーVMを停止したあとのレプリケーションの完了、リカバリサイトのクリーンアップに必要な時間、保護サイトでVMを再作成するのに必要な時間などが含まれます。10分を推奨します。

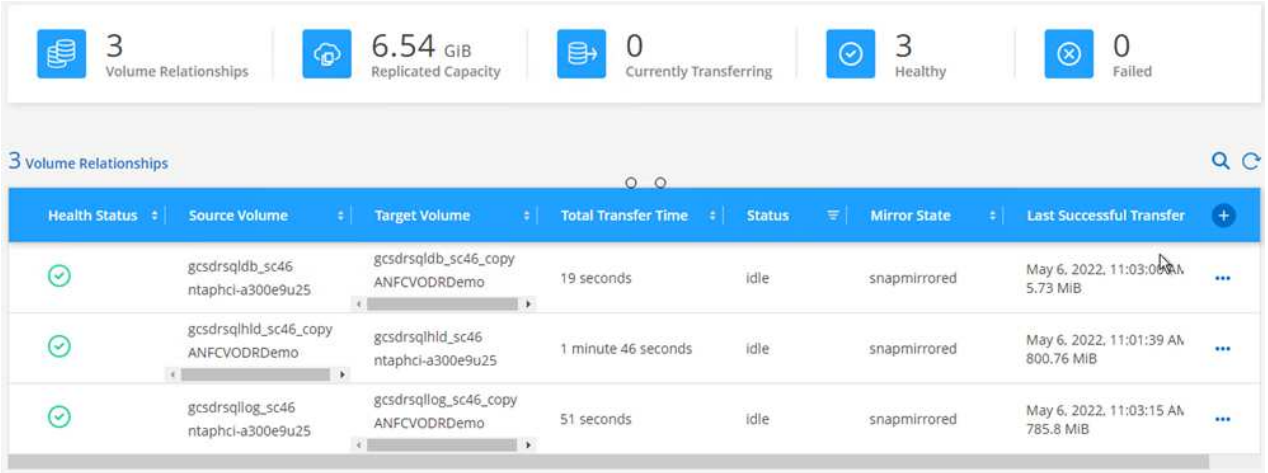



3. フェイルバックプロセスを完了し、VM保護およびデータの整合性が再開されたことを確認する。

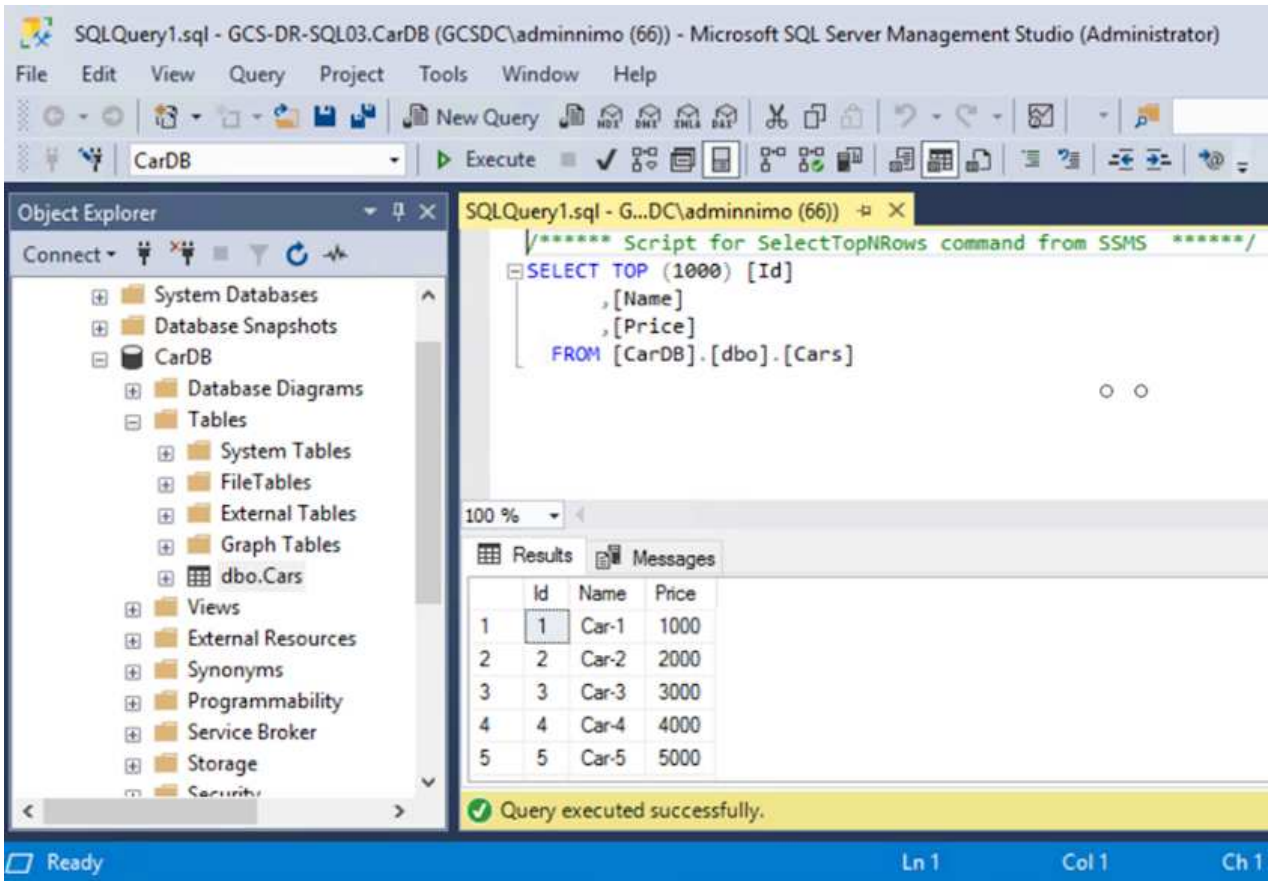


4. VMのリカバリが完了したら、セカンダリストレージをホストから切断してプライマリストレージに接続します。




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




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

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

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

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

## この解決策 の利点

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

- 開発とテスト、セキュリティテスト、パッチとアップグレードのテスト、修正テストなど、DR以外のワークフローにDRデータを活用します。

- CPUとRAMの最適化は、小規模なコンピューティングクラスタへのリカバリを可能にすることで、クラウドコストの削減に役立ちます。

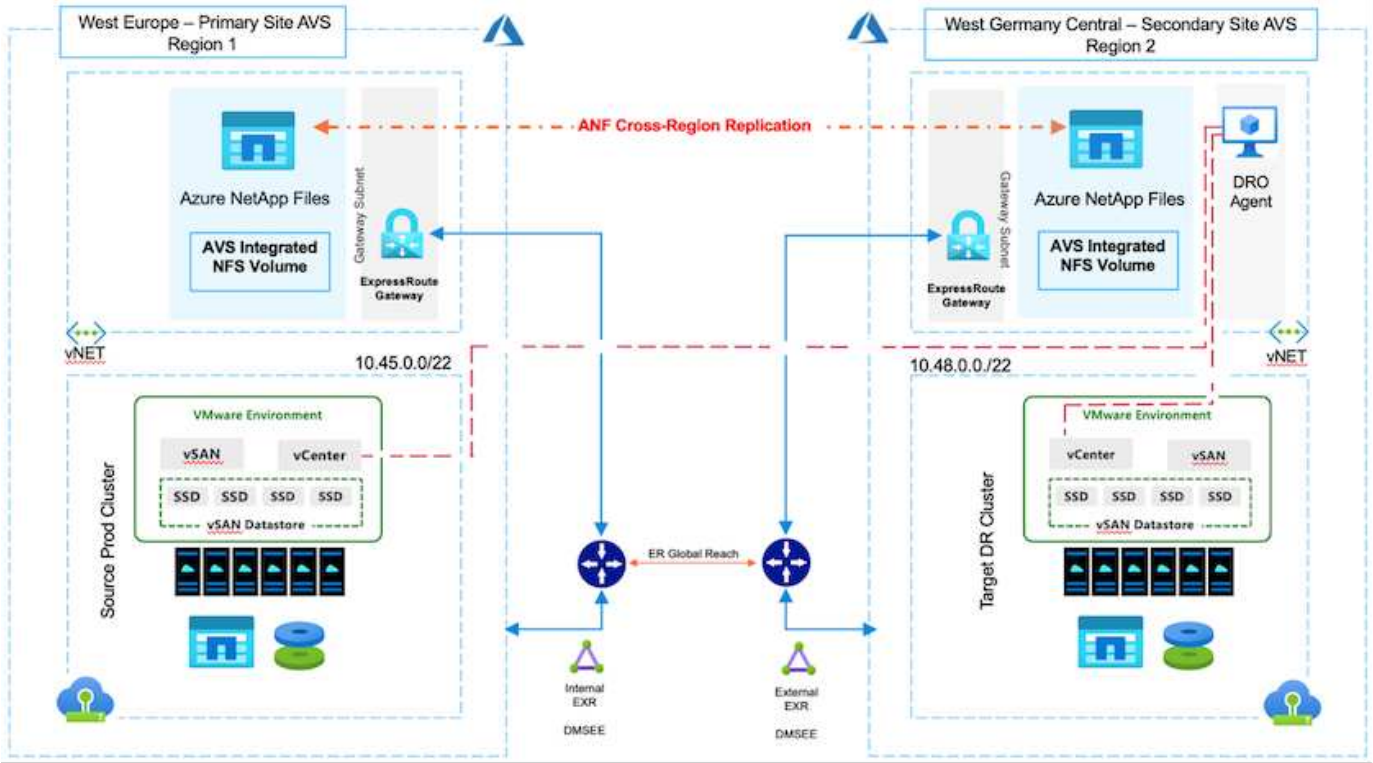
# TR-4955：『Disaster Recovery with Azure NetApp Files（ANF）and Azure VMware解決策 （AVS）』

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

## 概要

クラウド内のリージョン間でブロックレベルのレプリケーションを使用したディザスタリカバリは、耐障害性に優れた対費用効果の高い方法で、サイトの停止やデータ破損イベント（ランサムウェアなど）からワークロードを保護します。Azure NetApp Files （ANF）のリージョン間ボリュームレプリケーションを使用するとAzure NetApp Files 、Azure VMware解決策 （AVS）SDDCサイトで実行されているVMwareワークロードを、プライマリAVSサイトのNFSデータストアとして使用し、ターゲットリカバリリージョンの指定されたセカンダリAVSサイトにレプリケートできます。

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



前提条件と一般的な推奨事項

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

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

## はじめに

### Azure VMware解決策 を導入します

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

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

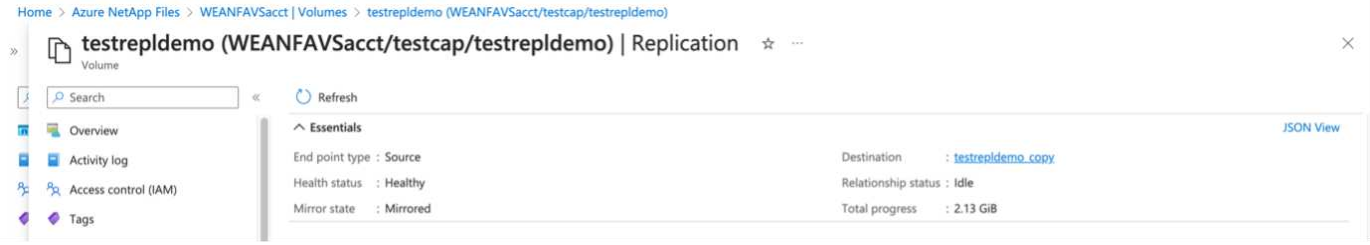
> 初期リリースでは、DROは既存のAVS SDDCクラスタをサポートしています。オンデマンドのSDDC作成は、今後のリリースで提供される予定です。

### Azure NetApp Files をプロビジョニングして設定

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

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

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




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

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

## DROのインストール

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

前提条件：

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

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

手順は次のとおりです。

1. 指定した仮想マシンにインストールパッケージをダウンロードします。

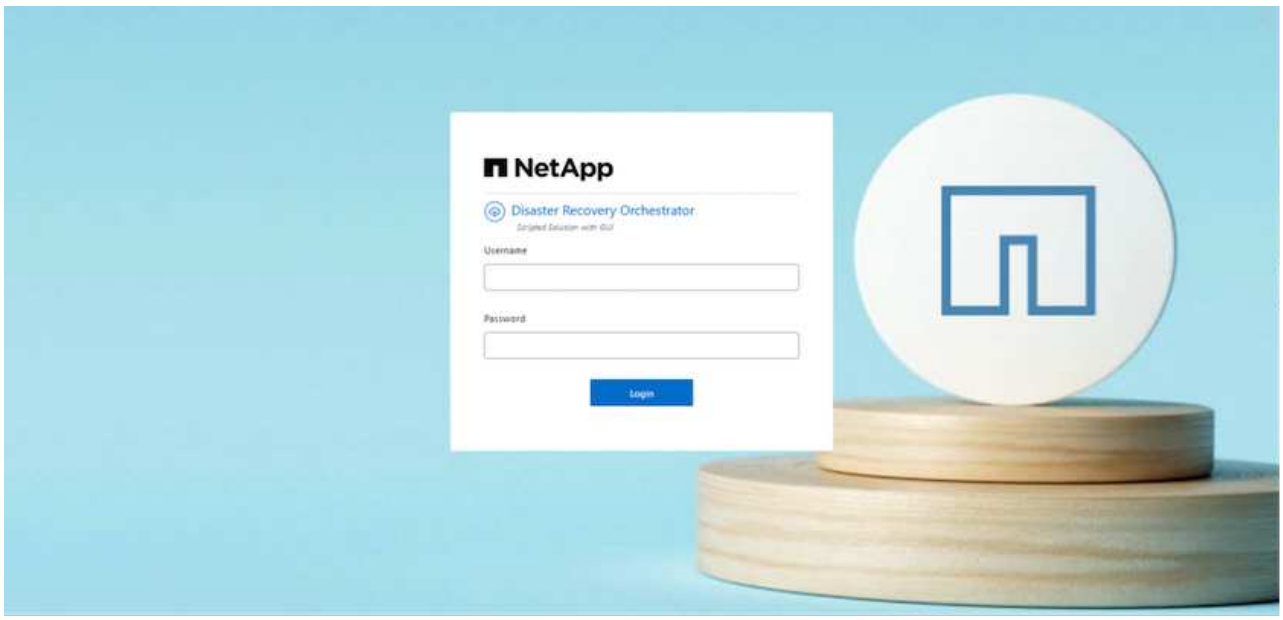
```
git clone https://github.com/NetApp/DRO-Azure.git
```

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

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

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

3. 次のクレデンシャルを使用してUIにアクセスします。
   - ユーザ名： `admin`
   - パスワード： `admin`




## DRO構成

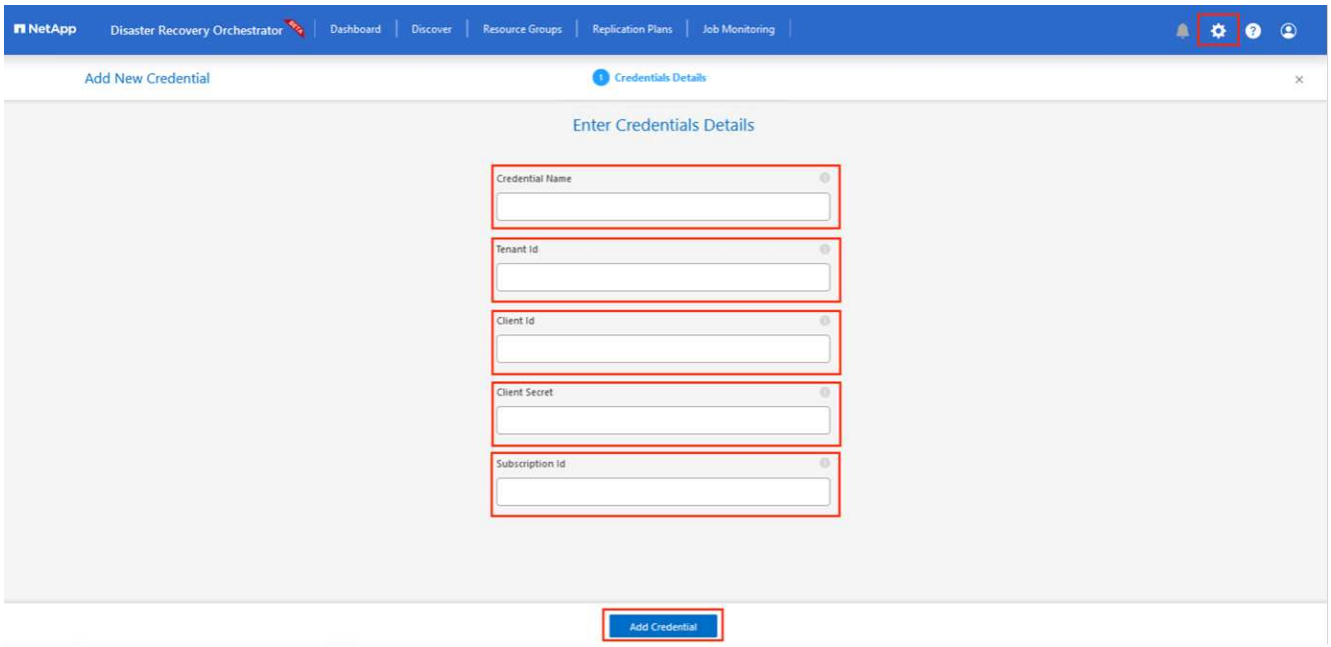
Azure NetApp Files とAVSが正しく設定されたら、プライマリAVSサイトからセカンダリAVSサイトへのワークロードのリカバリを自動化するDROの設定を開始できます。セカンダリAVSサイトにDROエージェントを導入し、ExpressRouteゲートウェイ接続を設定して、DROエージェントが適切なAVSおよびAzure NetApp Files コンポーネントとネットワーク経由で通信できるようにすることを推奨します。

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

この処理を実行するには、次の手順を実行します。

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

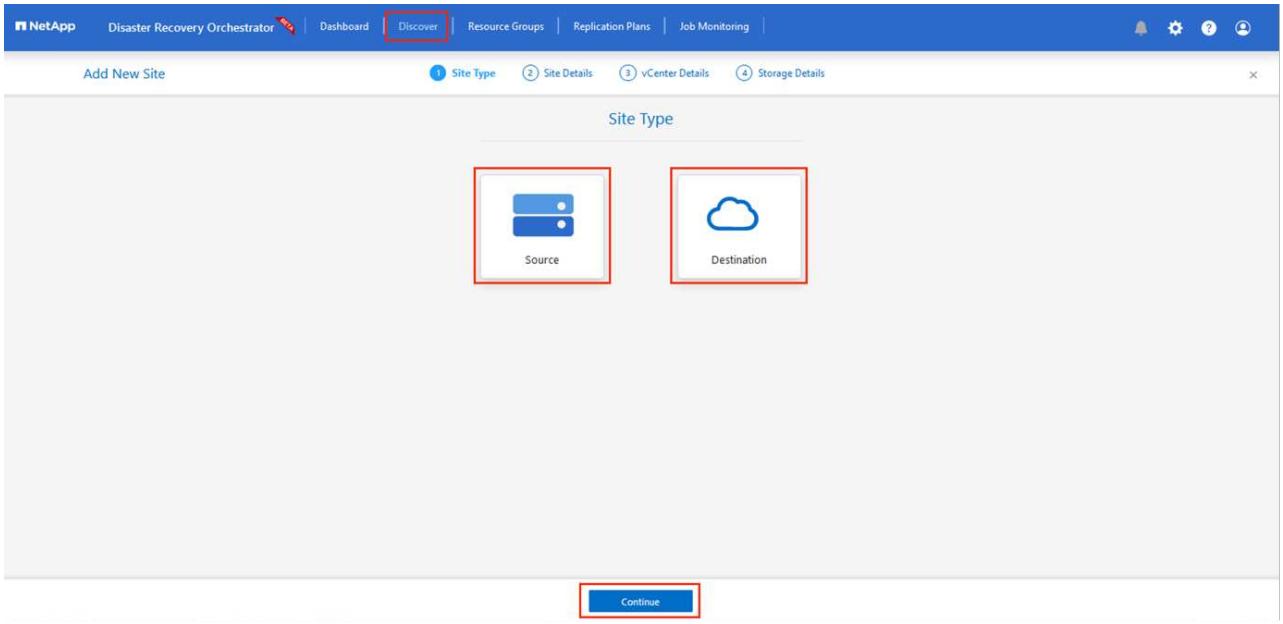
     この情報は、ADアプリケーションの作成時に取得しておく必要があります。
5. 新しいクレデンシャルの詳細を確認し、[Add Credential]をクリックします。




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

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

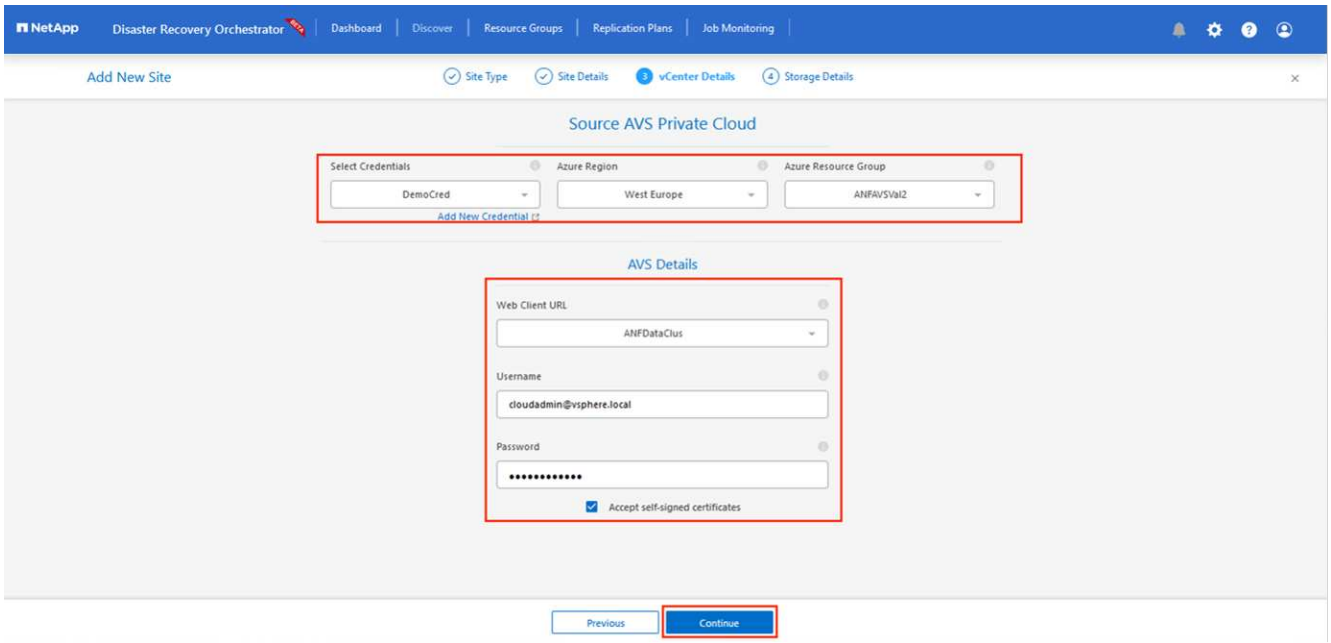
- SDDC vCenter
- Azure NetApp Files ストレージアカウント



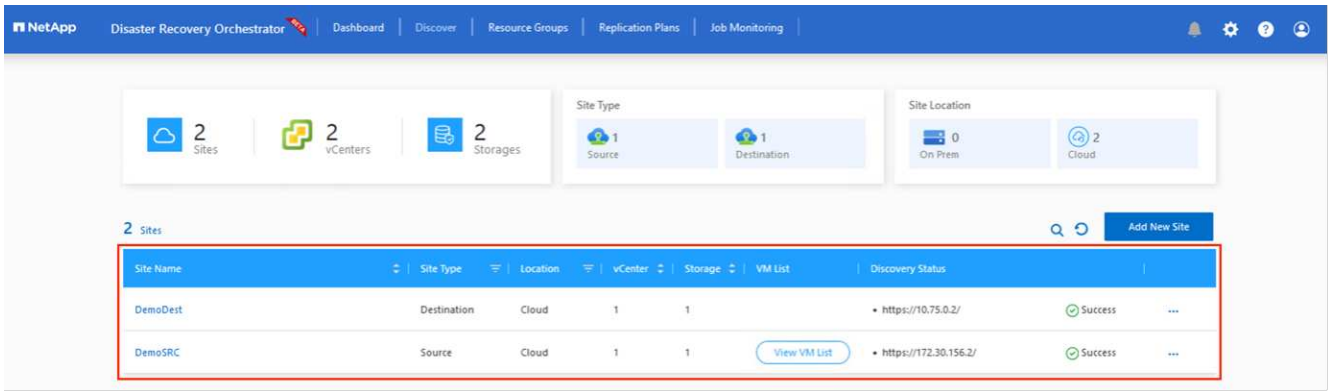

10. [ソース]をクリックしてサイト名を入力し、コネクタを選択してサイトの詳細を追加します。[* Continue（続行） ] をクリックします。

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

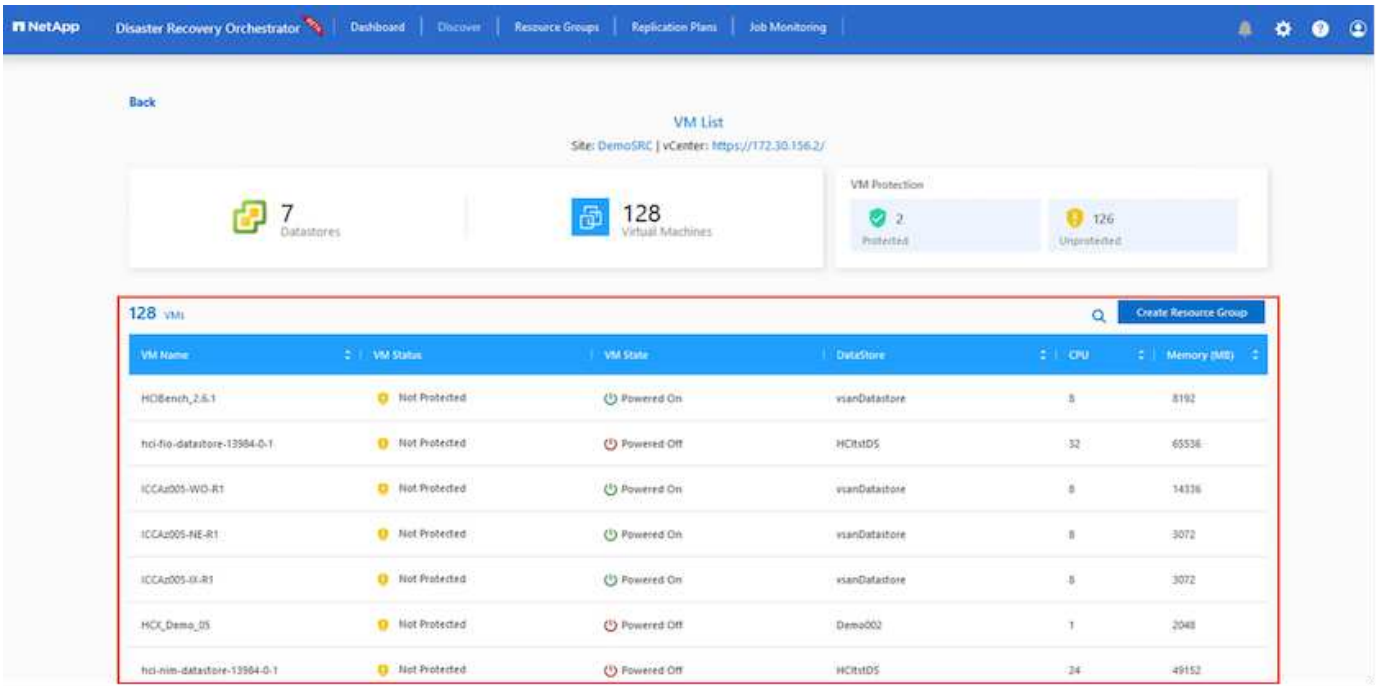
11. vCenterの詳細を更新します。これを行うには、プライマリAVS SDDCのドロップダウンからクレデンシャル、Azureリージョン、およびリソースグループを選択します。
12. DROには、リージョン内で使用可能なすべてのSDDCが一覧表示されます。ドロップダウンから、指定したプライベートクラウドのURLを選択します。
13. を入力します `cloudadmin@vsphere.local` ユーザクレデンシャル。これにはAzure Portalからアクセスできます。ここに記載されている手順に従ってください "リンク"。完了したら、*[続行]*をクリックします。




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




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



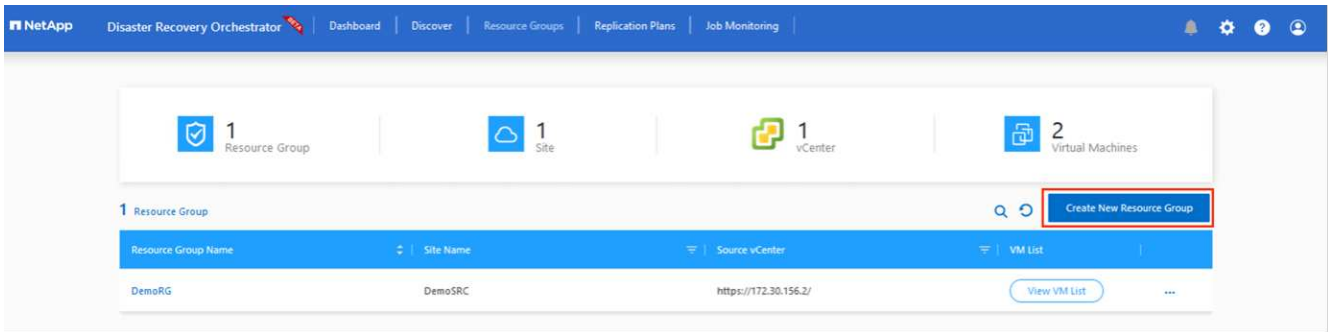

次の手順では、必要なVMをリソースグループとして機能グループにグループ化します。

リソースのグループ化

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

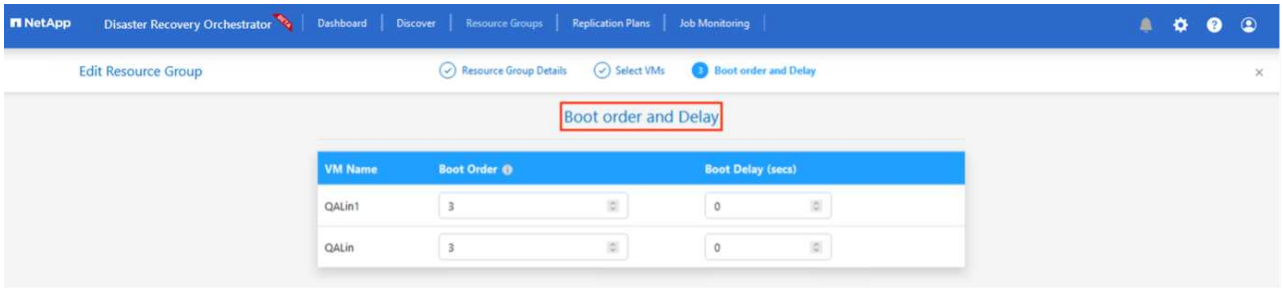
リソースグループの作成を開始するには、*[新しいリソースグループの作成]*メニュー項目をクリックします。

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

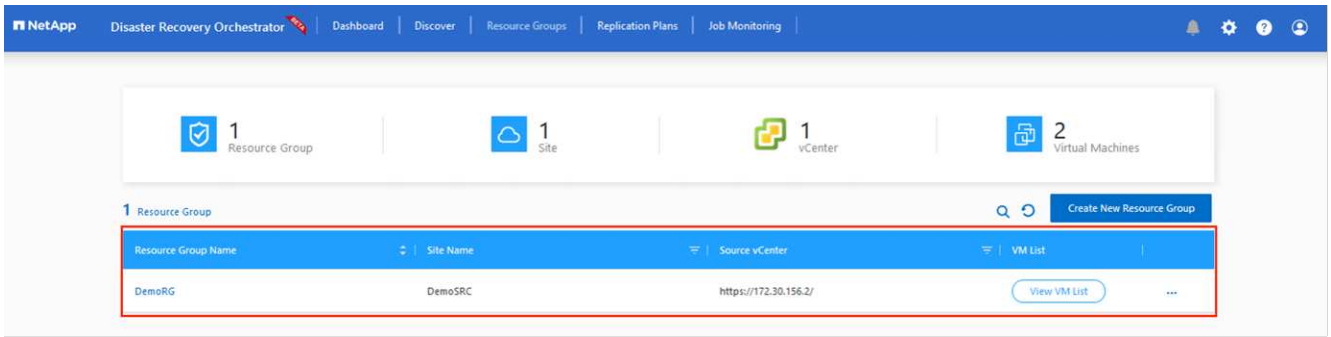



2. [New Resource Group]で、ドロップダウンからソースサイトを選択し、*[Create]*をクリックします。
3. リソースグループの詳細を指定し、*[続行]*をクリックします。
4. 検索オプションを使用して適切なVMを選択します。
5. 選択したすべてのVMについて、と**[Boot Delay]**（秒）を選択します。各仮想マシンを選択して優先度を設定し、パワーオンシーケンスの順序を設定します。すべての仮想マシンのデフォルト値は3です。オプションは次のとおりです。
    - パワーオンする最初の仮想マシン

- デフォルト
- 最後にパワーオンした仮想マシン




6. [リソースグループの作成]をクリックします。

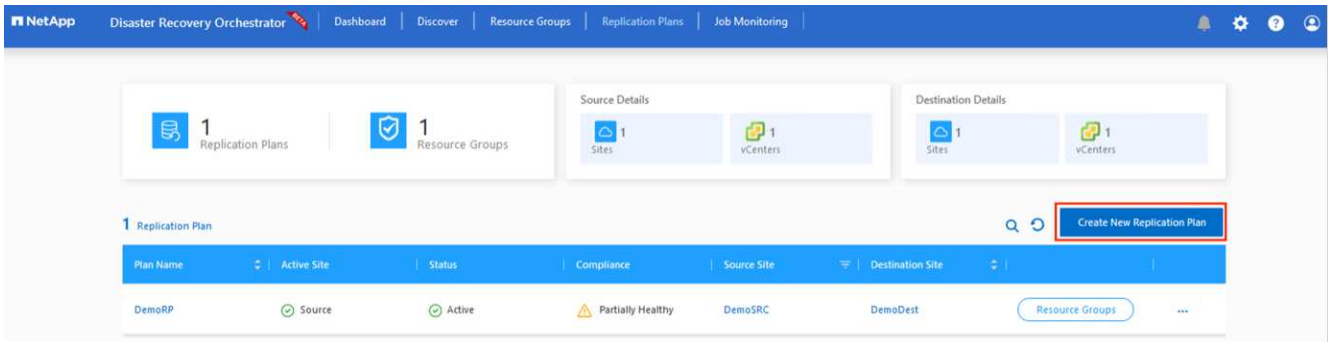



レプリケーションプラン

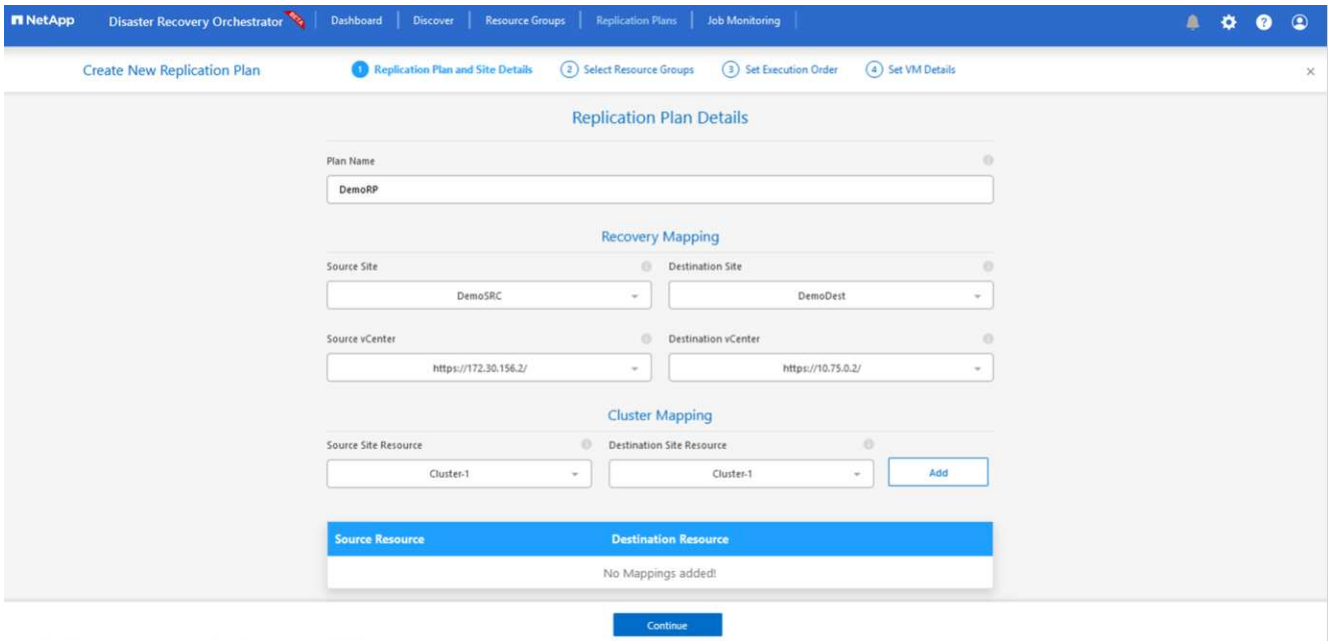
災害発生時にアプリケーションをリカバリするための計画を立てておく必要があります。ドロップダウンからソースとデスティネーションのvCenterプラットフォームを選択し、このプランに含めるリソースグループを選択します。また、アプリケーションをリストアおよびパワーオンする方法（ドメインコントローラ、ティア1、ティア2など）もグループ化します。計画は設計図とも呼ばれます。リカバリプランを定義するには、[Replication Plan]タブに移動し、*[New Replication Plan]*をクリックします。

レプリケーションプランの作成を開始するには、次の手順を実行します。

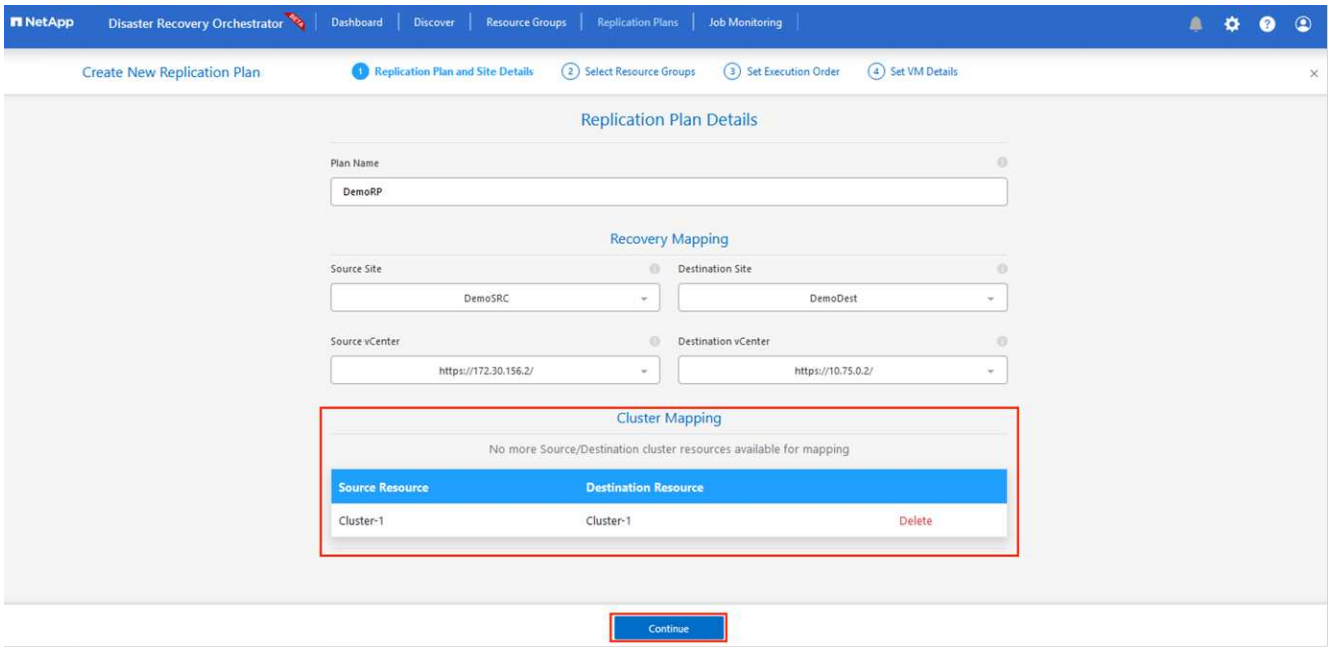
1. に移動し、[Create New Replication Plan]*をクリックします。




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

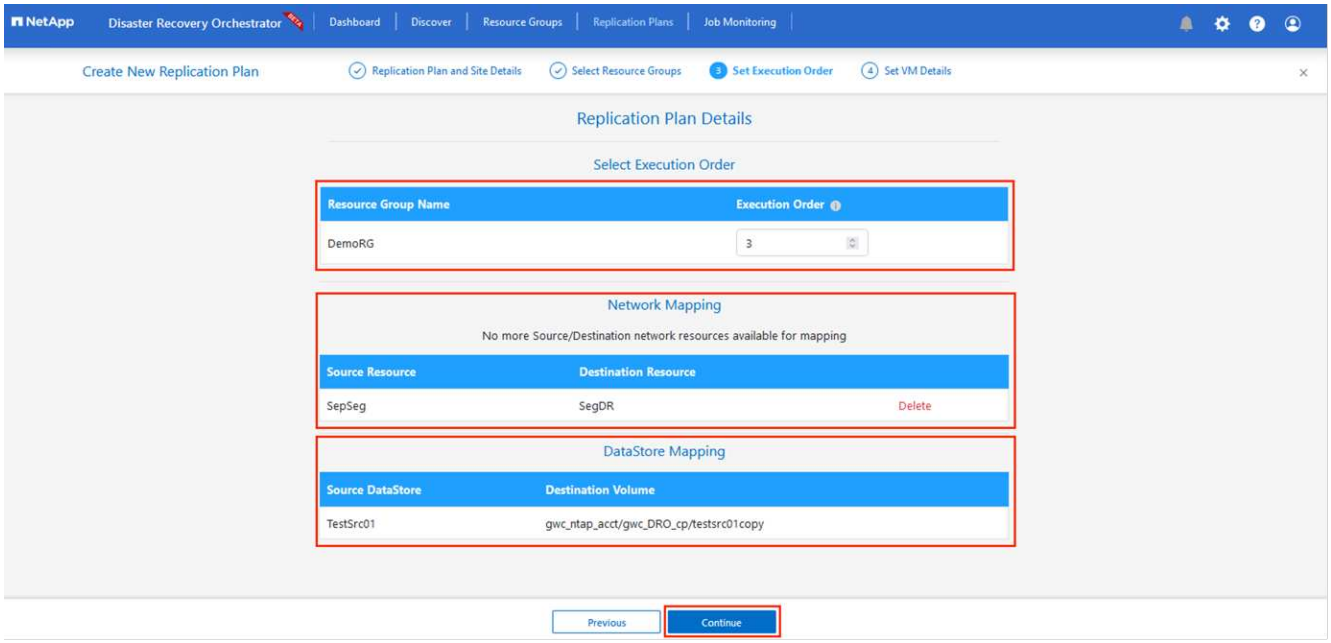



3. リカバリマッピングが完了したら、*[クラスタマッピング]*を選択します。

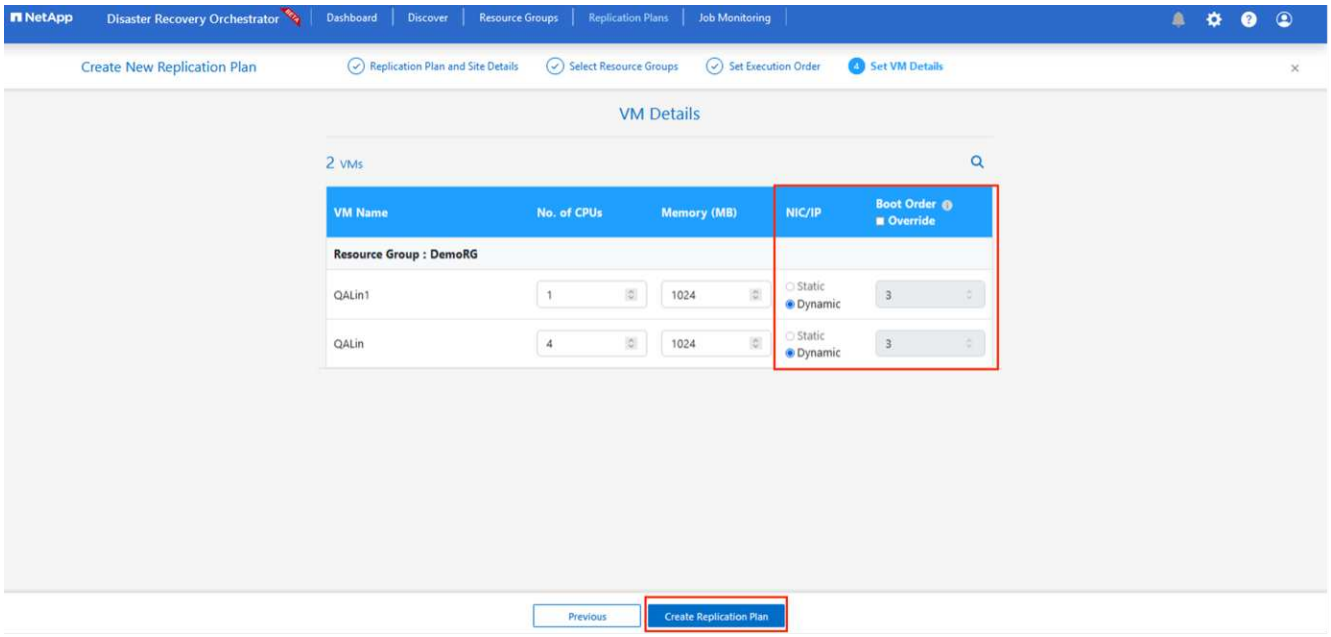



4. [リソースグループの詳細]を選択し、[*続行]をクリックします。
5. リソースグループの実行順序を設定します。このオプションを使用すると、複数のリソースグループが存在する場合の処理の順序を選択できます。
6. 完了したら、適切なセグメントにネットワークマッピングを設定します。セグメントはセカンダリAVSクラスタですでにプロビジョニングされている必要があります。それらにVMをマッピングするには、適切なセグメントを選択します。
7. データストアのマッピングは、VMの選択に基づいて自動的に選択されます。

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

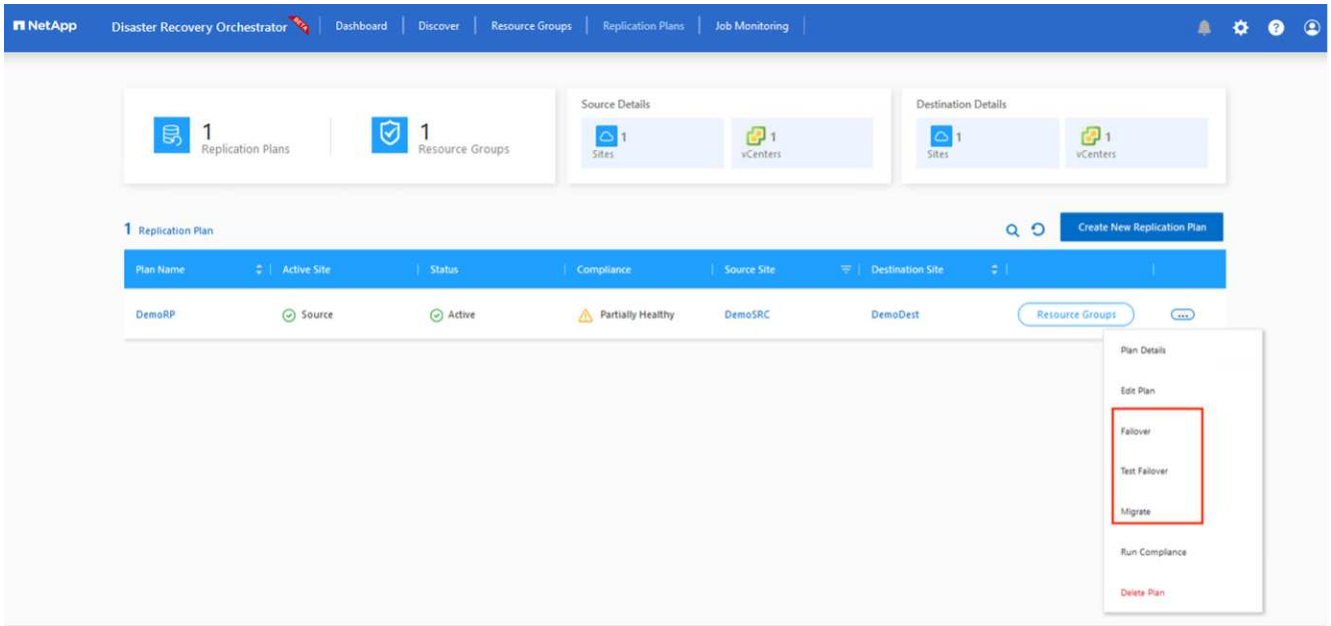



8. [VM details]で、必要に応じてVMのCPUパラメータとRAMパラメータのサイズを変更できます。これは、大規模な環境を小規模なターゲットクラスタにリカバリする場合や、1対1の物理VMwareインフラストラクチャをプロビジョニングせずにDRテストを実行する場合に非常に役立ちます。また、リソースグループ全体で選択したすべてのVMのブート順序とブート遅延（秒）を変更します。リソースグループのブート順序の選択時に選択したものから変更が必要な場合は'ブート順序を変更する追加オプションがありますデフォルトでは、リソースグループの選択時に選択された起動順序が使用されますが、この段階で変更を実行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

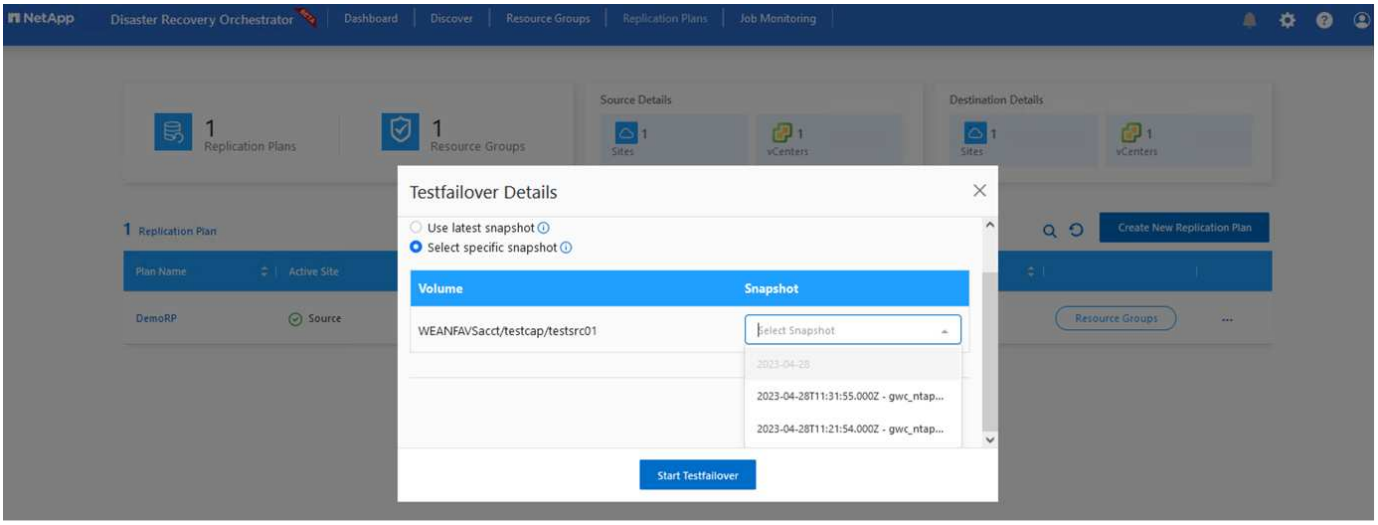



9. レプリケーションプランの作成*をクリックします。レプリケーションプランの作成後、要件に応じてフ

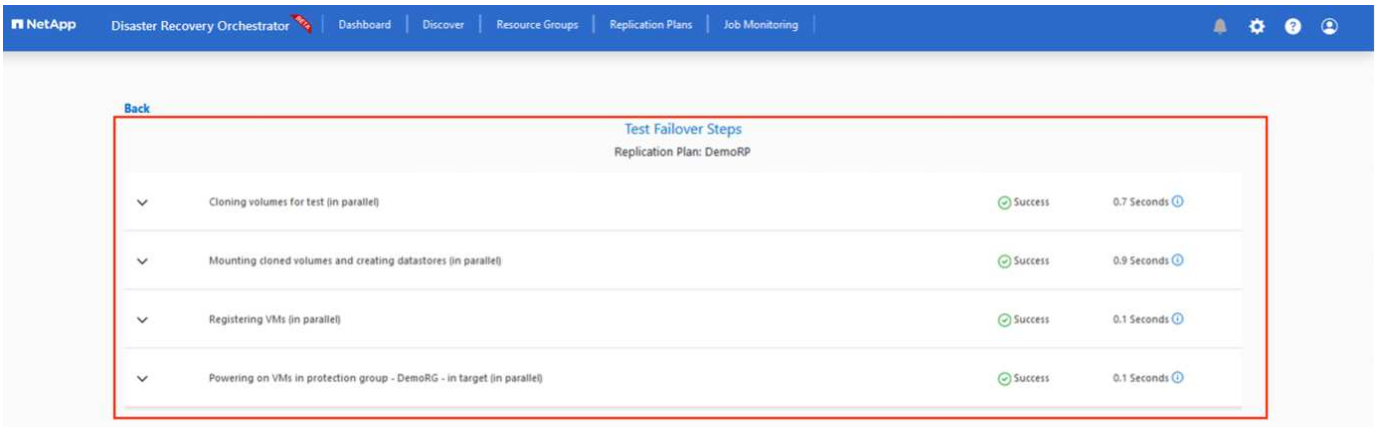
ェイルオーバー、テストフェイルオーバー、移行オプションを実行できます。



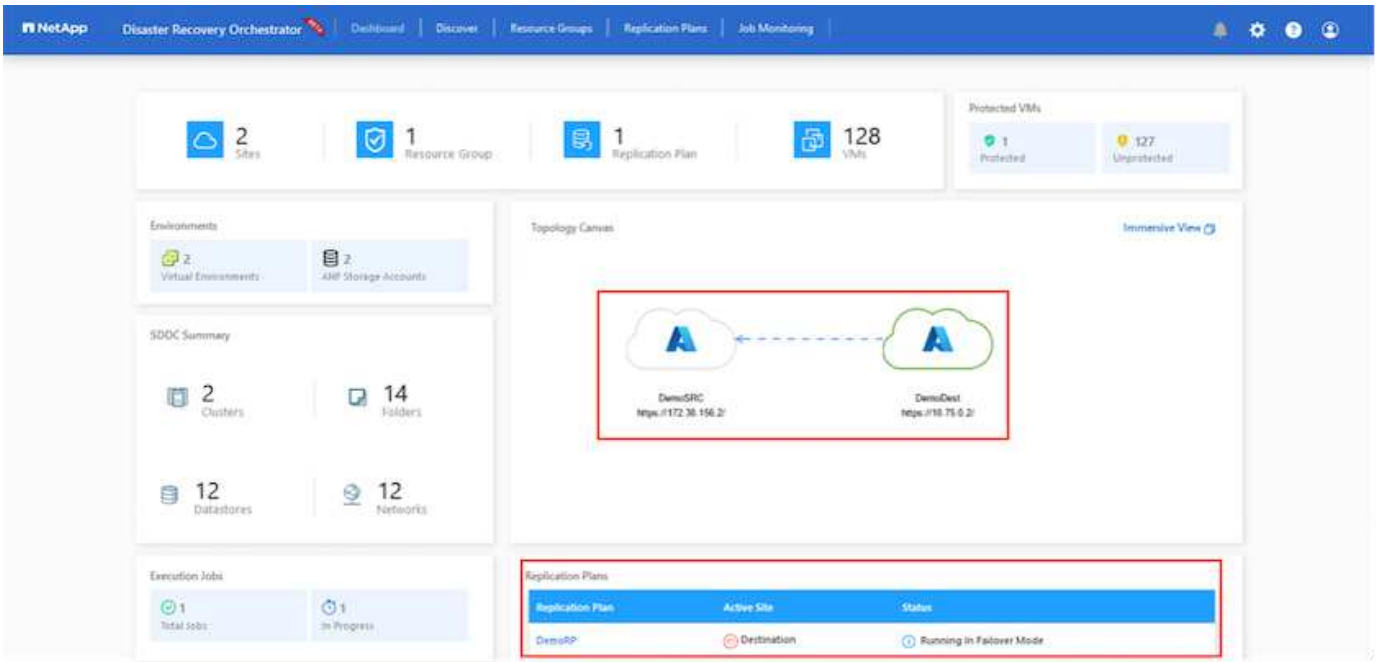

フェイルオーバーオプションとテストフェイルオーバーオプションでは、最新のSnapshotが使用されるか、ポイントインタイムSnapshotから特定のSnapshotを選択できます。ポイントインタイムオプションは、最新のレプリカがすでに侵害または暗号化されているランサムウェアなどの破損イベントに直面している場合に非常に役立ちます。DROには使用可能なすべてのタイムポイントが表示されます。



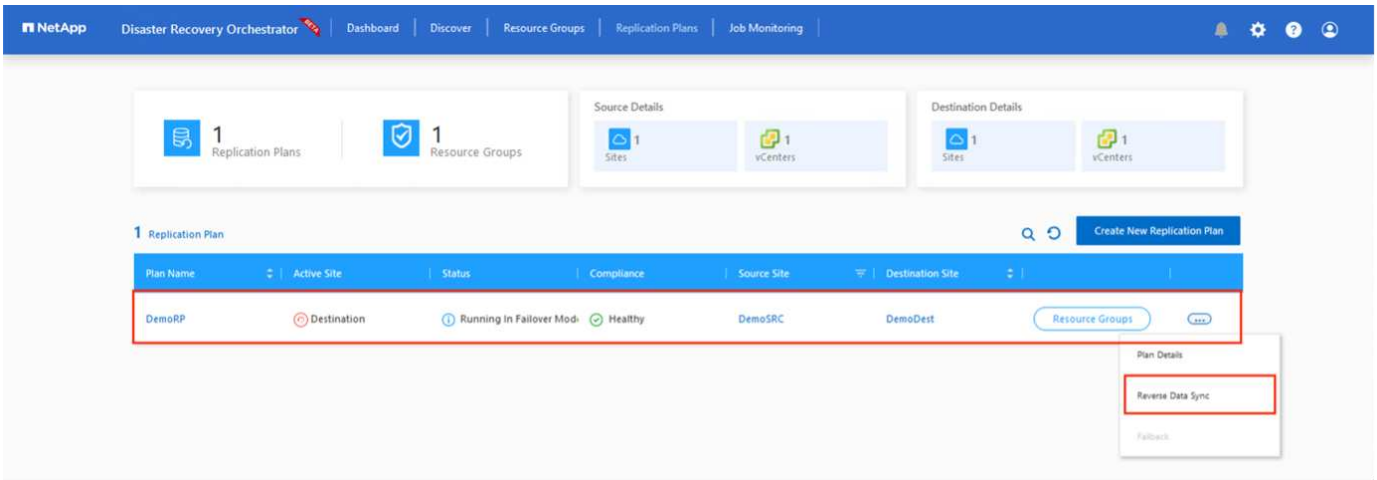

レプリケーションプランで指定した構成でフェイルオーバーまたはテストフェイルオーバーをトリガーするには、* Failover または Test Failover *をクリックします。タスクメニューでレプリケーション計画を監視できます。



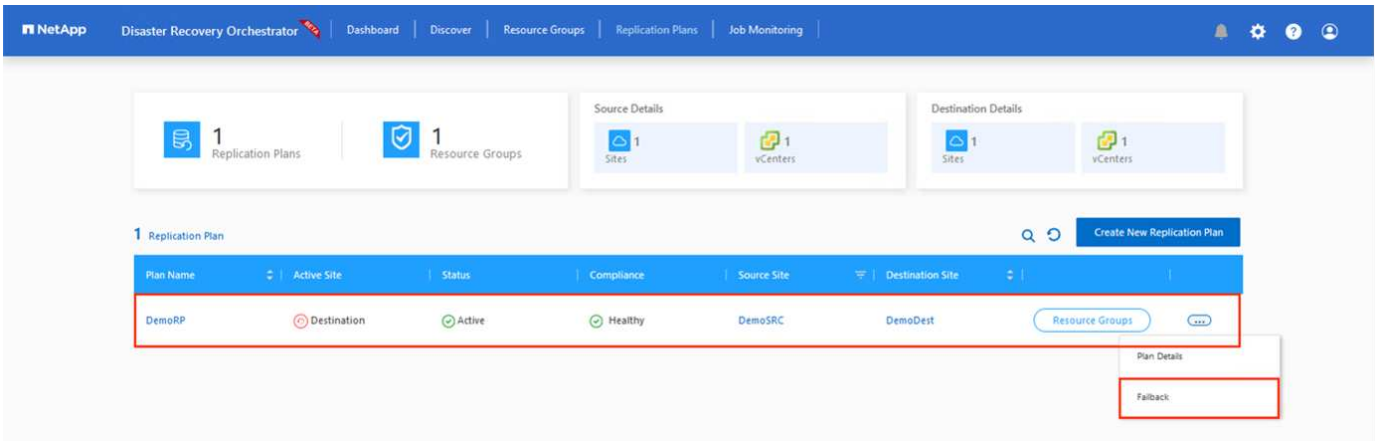

フェイルオーバーがトリガーされると、リカバリされた項目がセカンダリサイトのAVS SDDC vCenter（VM、ネットワーク、およびデータストア）に表示されます。デフォルトでは、VMはWorkloadフォルダにリカバリされます。

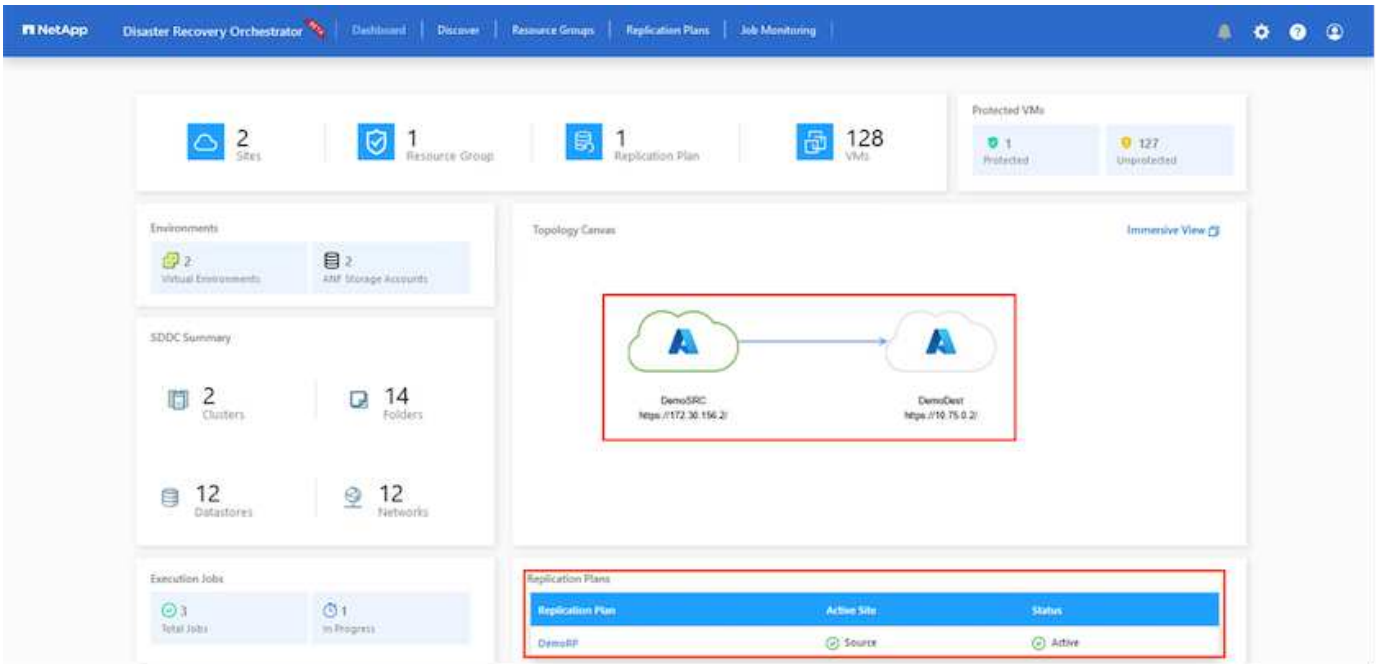



フェイルバックは、レプリケーションプランレベルでトリガーできます。テストフェイルオーバーの場合は、ティアダウンオプションを使用して変更をロールバックし、新しく作成したボリュームを削除できます。フェイルオーバーに関連するフェイルバックは、2つの手順で構成されます。レプリケーション計画を選択し、*[Reverse Data sync]*を選択します。




この手順が完了したら、フェイルバックをトリガーしてプライマリAVSサイトに戻ります。




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

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

ランサムウェアからのリカバリ

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

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

## まとめ

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

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

追加情報の参照先

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

- Azure NetApp Files のボリュームレプリケーションを作成します

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Azure NetApp Files のリージョン間レプリケーション

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"

- "Azure VMware 解決策の略"

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

- Azure に仮想化環境を導入して設定

  "https://docs.netapp.com/us-en/netapp-solutions/ehc/azure-setup.html"

- Azure VMware解決策 を導入して設定

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

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

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

## 概要

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

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

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

## 本書の目的

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

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

このレプリケーションメカニズムにより、災害発生時にAVS SDDCでワークロードを迅速に開始できま

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

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

[]

## 解決策 の導入

### 手順の概要

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

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

3. Veeam Backup and Replicationを使用してVMレプリカを作成するためのレプリケーションジョブを設定します。
4. フェイルオーバープランを作成し、フェイルオーバーを実行
5. 災害が完了し、プライマリサイトが稼働したら、本番環境のVMにスイッチバックします。

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

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

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

### 展開の詳細

ステップ**1**：**VM**のレプリケート

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

VMをレプリケートするには、次の手順を実行します。

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

     []
4. [Virtual * Machines]手順で、Azure VMware解決策SDDCに接続されたAzure NetApp Filesデータストアにレプリケートするを選択します。仮想マシンをVSANに配置して、使用可能なVSANデータストアの容量をいっぱいにすることができます。パイロットライトクラスタでは、3ノードクラスタの使用可能容量が制限されます。残りのデータはAzure NetApp Filesデータストアに簡単に配置してVMをリカバリしたり、CPU /メモリの要件に合わせてクラスタを拡張したりできます。をクリックし、[オブジェクトの追加]ウィンドウで必要な**VM**または**VM**コンテナを選択して[追加]*をクリックします。「 * 次へ * 」をクリックします。

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

   []
6. 次の手順では、必要に応じてソースとデスティネーションの仮想ネットワーク間のマッピングを作成します。

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

9. [Guest Processing]ステップで、必要に応じて[Enable application-aware processing]オプションを選択します。「 * 次へ * 」をクリックします。

   []

10. レプリケーションジョブを定期的に実行するレプリケーションスケジュールを選択します。

    []

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

    []

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

[]

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

手順**2**：フェイルオーバープランを作成する

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

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

ⓘ フェイルオーバープランを追加できるのは、初期レプリケーションが完了し、VMレプリカがReady状態になってからです。

ⓘ フェイルオーバープランの実行時に同時に起動できるVMの最大数は10です。

ⓘ フェイルオーバープロセス中は、ソースVMの電源はオフになりません。

フェイルオーバープラン*を作成するには、次の手順を実行します。

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

   []

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

   []

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

   []

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

手順**3**：フェイルオーバープランを実行する

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

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

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

[]

[]

VMレプリカの状態がReadyからFailoverに変わり、デスティネーションAzure VMware解決策（AVS）SDDCクラスタ/ホストでVMが起動します。

[]

フェイルオーバーが完了すると、VMのステータスが「Failover」に変わります。

[]

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

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

手順**4**：本番サイトへのフェイルバック

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

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

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

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

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

[]

[]

[]

[]

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

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

[]

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

[]

## まとめ

Azure NetApp Filesデータストア機能を使用すると、Veeamまたは検証済みのサードパーティ製ツールを使用して、VMレプリカに対応するためだけに大規模なクラスタをセットアップするのではなく、パイロットライトクラスタを活用して低コストのDR解決策を提供できます。これにより、カスタマイズされたディザスタリカバリ計画を効率的に処理し、社内の既存のバックアップ製品をDR用に再利用できるようになり、オンプレミスのDRデータセンターを終了してクラウドベースのディザスタリカバリを実現できます。災害の場合はボ

タンをクリックしてフェイルオーバーしたり、災害が発生した場合は自動的にフェイルオーバーすることができます。

このプロセスの詳細については、詳細なウォークスルービデオをご覧ください。

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