CVO と AVS (ゲスト接続ストレージ) による災害復旧

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

目次

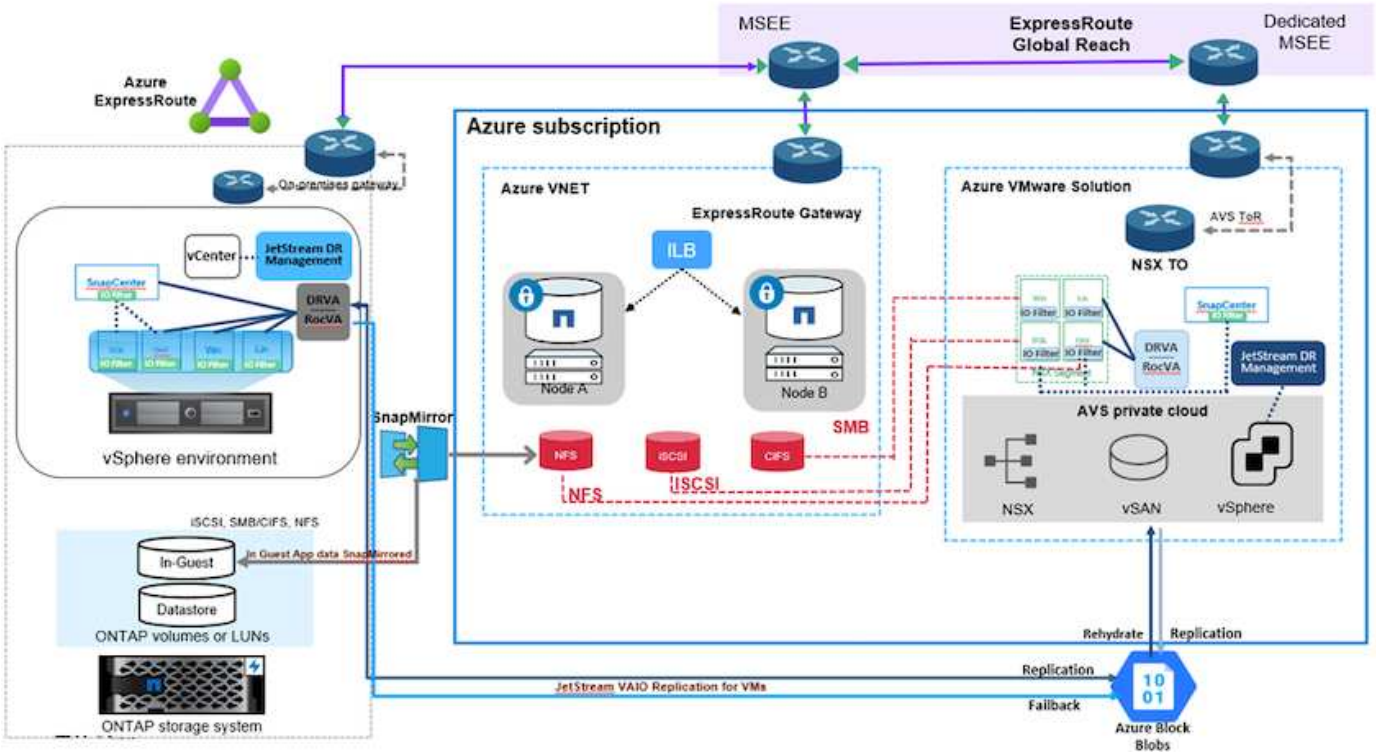
CVO と AVS (ゲスト接続ストレージ) による災害復旧

クラウドへの災害復旧は、サイトの停止やランサムウェアなどのデータ破損イベントからワークロードを保護する、回復力がありコスト効率に優れた方法です。 NetApp SnapMirror を使用すると、ゲスト接続ストレージを使用するオンプレミスの VMware ワークロードを、Azure で実行されているNetApp Cloud Volumes ONTAPに複製できます。

概要

```
 This covers application data; however, what about the actual VMs
themselves. Disaster recovery should cover all dependent components,
including virtual machines, VMDKs, application data, and more. To
accomplish this, SnapMirror along with Jetstream can be used to seamlessly
recover workloads replicated from on-premises to Cloud Volumes ONTAP while
using vSAN storage for VM VMDKs.
```

このドキュメントでは、 NetApp SnapMirror、JetStream、Azure VMware Solution (AVS) を使用した災害復旧の設定と実行の手順について説明します。



前提

このドキュメントでは、アプリケーション データ用のゲスト内ストレージ (ゲスト接続とも呼ばれます) に焦点を当てており、オンプレミス環境でアプリケーション整合性のあるバックアップにSnapCenterを使用していることを前提としています。

> このドキュメントは、サードパーティのバックアップまたはリカバリ ソリューションに適用されます。環境で使用されているソリューションに応じて、ベスト プラクティスに従って、組織の SLA を満たすバックアップ ポリシーを作成します。

オンプレミス環境と Azure 仮想ネットワーク間の接続には、Express Route Global Reach または VPN ゲートウェイを使用した仮想 WAN を使用します。セグメントは、オンプレミスの vLAN 設計に基づいて作成する必要があります。

> オンプレミスのデータセンターを Azure に接続するには複数のオプションがあるため、このドキュメントでは特定のワークフローの概要を説明することはできません。オンプレミスから Azure への適切な接続方法については、Azure のドキュメントを参照してください。

DRソリューションの導入

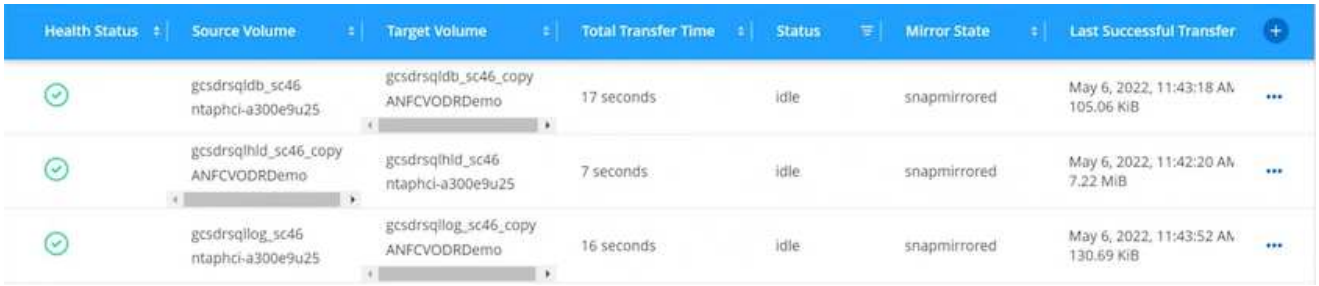
ソリューション展開の概要

1. 必要な RPO 要件に従って、 SnapCenterを使用してアプリケーション データがバックアップされていることを確認します。
2. 適切なサブスクリプションと仮想ネットワーク内で Cloud Manager を使用して、正しいインスタンス サイズでCloud Volumes ONTAP をプロビジョニングします。
   a. 関連するアプリケーション ボリュームに対してSnapMirrorを構成します。
   b. スケジュールされたジョブの後にSnapMirror の更新をトリガーするように、 SnapCenterのバックアップ ポリシーを更新します。
3. オンプレミスのデータセンターに JetStream DR ソフトウェアをインストールし、仮想マシンの保護を開始します。
4. Azure VMware Solution プライベート クラウドに JetStream DR ソフトウェアをインストールします。
5. 災害発生時には、Cloud Manager を使用してSnapMirror関係を解除し、指定された AVS DR サイト内のAzure NetApp Filesまたは vSAN データストアへの仮想マシンのフェイルオーバーをトリガーします。
   a. アプリケーション VM の ISCSI LUN と NFS マウントを再接続します。
6. プライマリ サイトが回復された後、 SnapMirror を逆再同期して、保護されたサイトへのフェイルバックを呼び出します。

導入環境の詳細

Azure で **CVO** を構成し、ボリュームを **CVO** に複製する

最初のステップは、Azure でCloud Volumes ONTAP を構成することです ("リンク" ）を作成し、必要な頻度とスナップショット保持期間で、必要なボリュームをCloud Volumes ONTAPに複製します。



AVSホストと**CVO**データアクセスを構成する

SDDC を展開する際に考慮すべき 2 つの重要な要素は、Azure VMware ソリューション内の SDDC クラスターのサイズと、SDDC をサービスに維持する期間です。災害復旧ソリューションに関するこれら 2 つの重要な考慮事項は、全体的な運用コストの削減に役立ちます。 SDDC は、最小 3 台のホストから、本格的な展開のマルチホスト クラスターまで、さまざまな規模にすることができます。

AVS クラスターを展開するかどうかの決定は、主に RPO/RTO 要件に基づいて行われます。 Azure VMware ソリューションを使用すると、テストや実際の災害イベントに備えて SDDC をジャストインタイムでプロビジョニングできます。ジャストインタイムで導入された SDDC は、災害が発生していないときに ESXi ホストのコストを節約します。ただし、この形式の展開では、SDDC のプロビジョニング中に RTO が数時間影響を受けます。

最も一般的に導入されるオプションは、SDDC を常時オンのパイロットライト動作モードで実行することです。このオプションは、常に利用可能な 3 つのホストの小さなフットプリントを提供し、シミュレーション アクティビティとコンプライアンス チェックの実行ベースラインを提供することでリカバリ操作を高速化し、実稼働サイトと DR サイト間の運用上のずれのリスクを回避します。パイロットライト クラスターは、実際の DR イベントを処理するために必要になったときに、必要なレベルまで迅速に拡張できます。

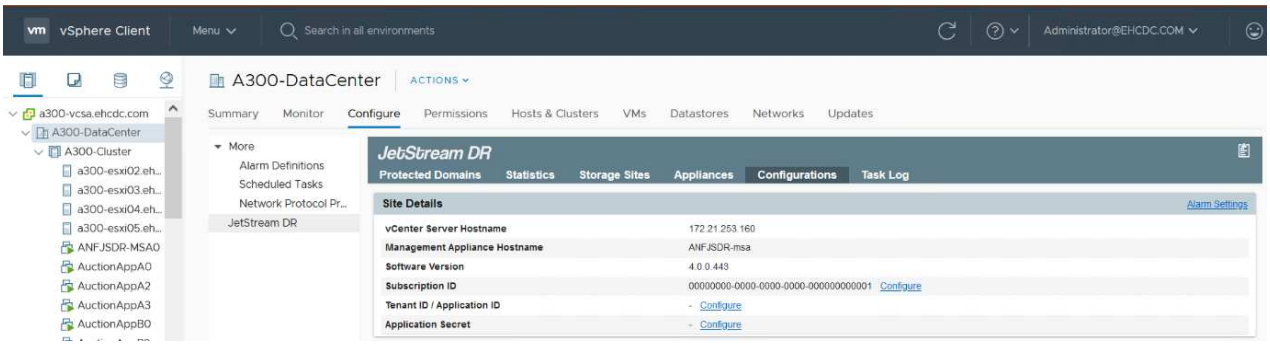
AVS SDDC（オンデマンドまたはパイロットライトモード）を構成するには、以下を参照してください。"Azure に仮想化環境を展開して構成する" 。前提条件として、接続が確立された後、AVS ホスト上にあるゲスト VM がCloud Volumes ONTAPからデータを使用できることを確認します。

Cloud Volumes ONTAPと AVS が適切に構成されたら、VAIO メカニズムを使用し、アプリケーション ボリュームのコピーにSnapMirrorを活用して、オンプレミスのワークロードの AVS (アプリケーション VMDK を持つ VM とゲスト内ストレージを持つ VM) へのリカバリを自動化するように Jetstream の構成を開始しCloud Volumes ONTAP。

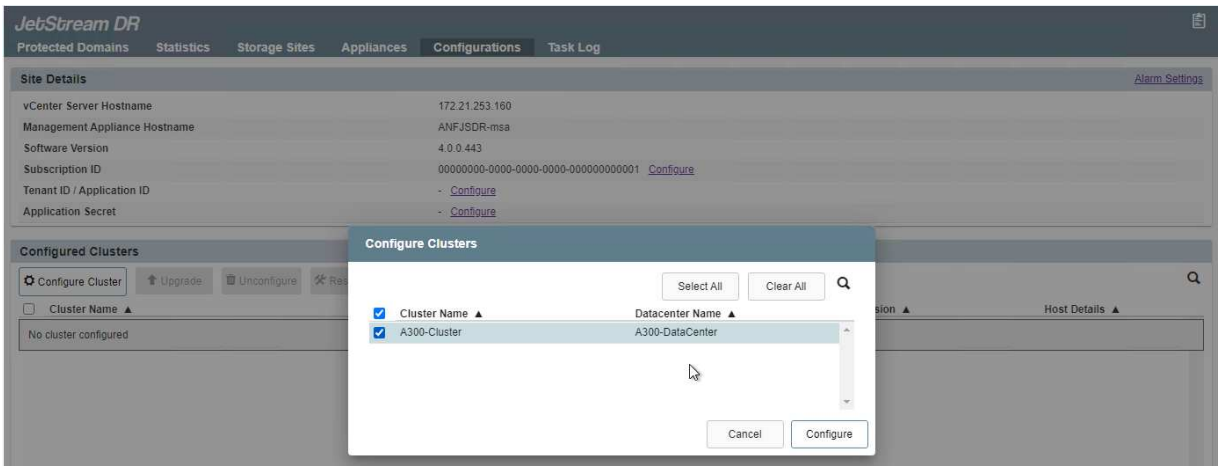
オンプレミスデータセンターに **JetStream DR** をインストールする

JetStream DR ソフトウェアは、JetStream DR 管理サーバー仮想アプライアンス (MSA)、DR 仮想アプライアンス (DRVA)、およびホスト コンポーネント (I/O フィルタ パッケージ) の 3 つの主要コンポーネントで構成されています。 MSA は、コンピューティング クラスターにホスト コンポーネントをインストールして構成し、JetStream DR ソフトウェアを管理するために使用されます。インストールプロセスは次のとおりです。

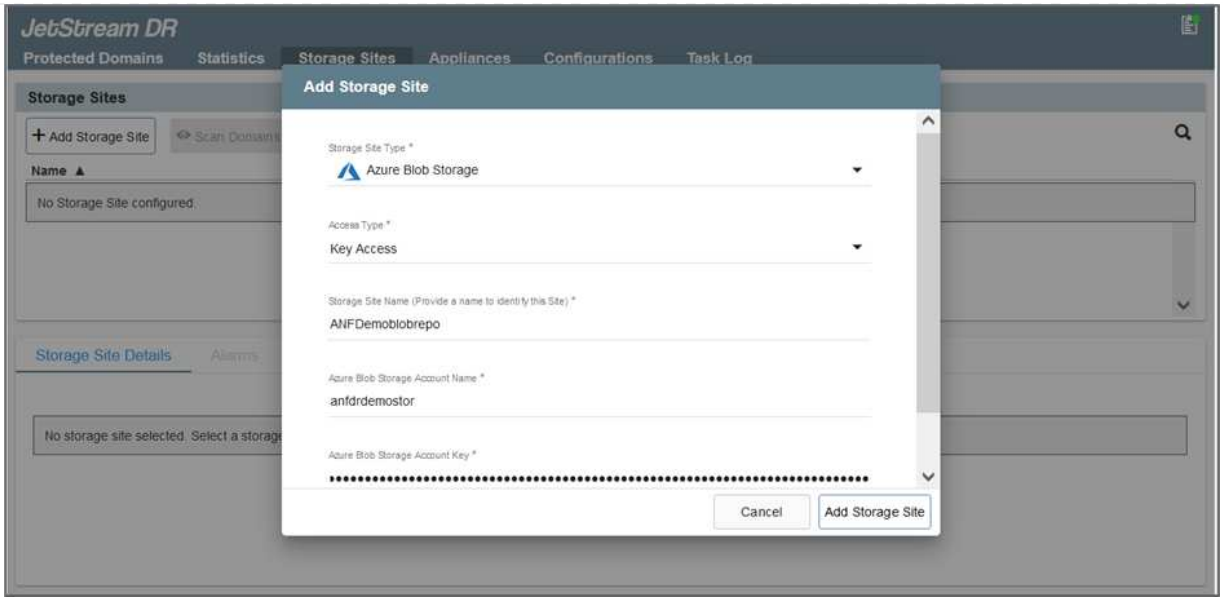
1. 前提条件を確認してください。
2. リソースと構成の推奨事項を取得するには、容量計画ツールを実行します。
3. 指定されたクラスタ内の各 vSphere ホストに JetStream DR MSA をデプロイします。
4. ブラウザで DNS 名を使用して MSA を起動します。
5. vCenter サーバーを MSA に登録します。
6. JetStream DR MSA がデプロイされ、vCenter Server が登録されたら、vSphere Web Client を使用して JetStream DR プラグインに移動します。これは、[データセンター] > [構成] > [JetStream DR] に移動することで実行できます。



7. JetStream DR インターフェースから、次のタスクを完了します。
   a. I/O フィルター パッケージを使用してクラスターを構成します。

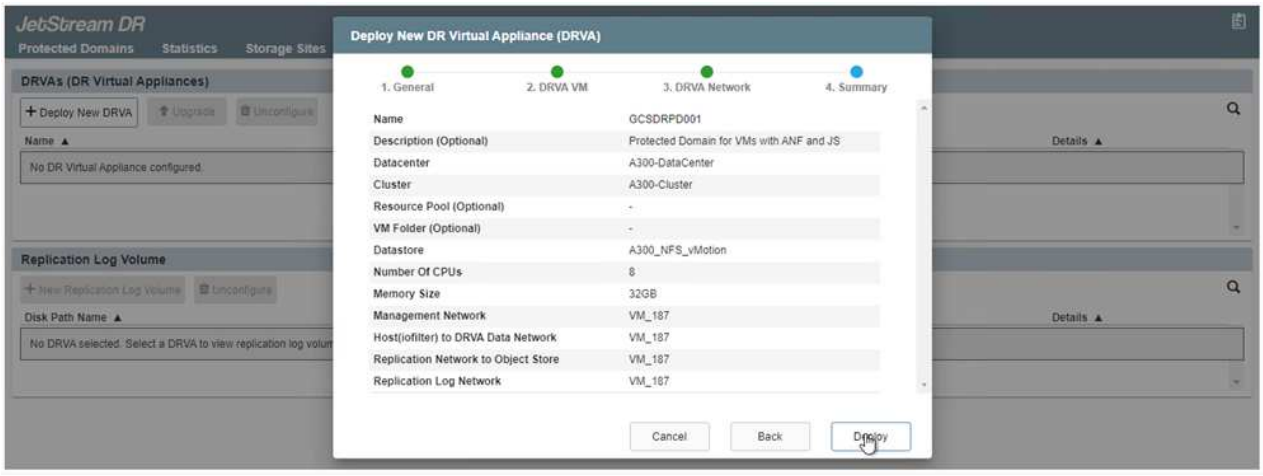


   b. リカバリ サイトにある Azure Blob ストレージを追加します。

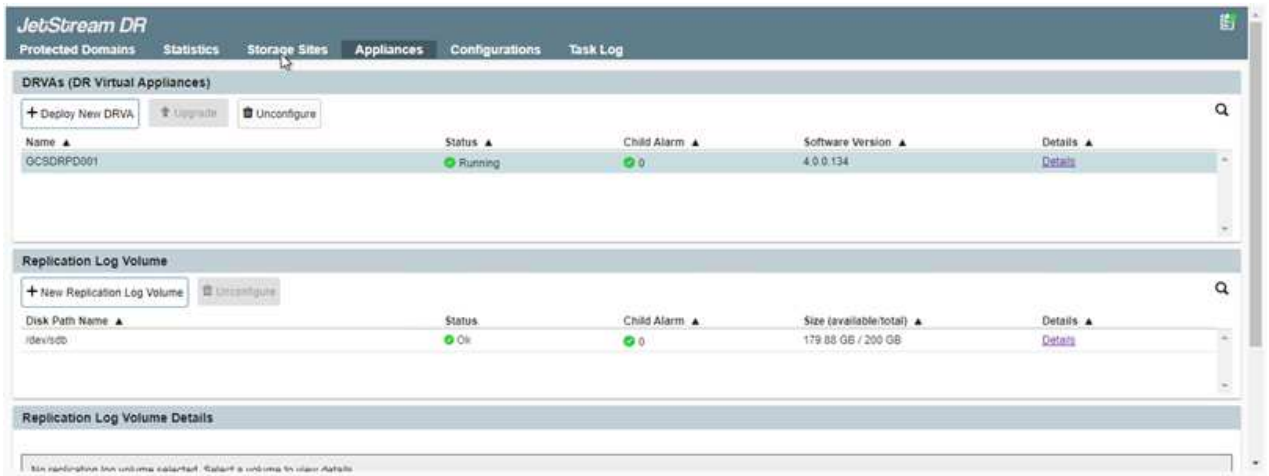


8. アプライアンス タブから必要な数の DR 仮想アプライアンス (DRVA) をデプロイします。

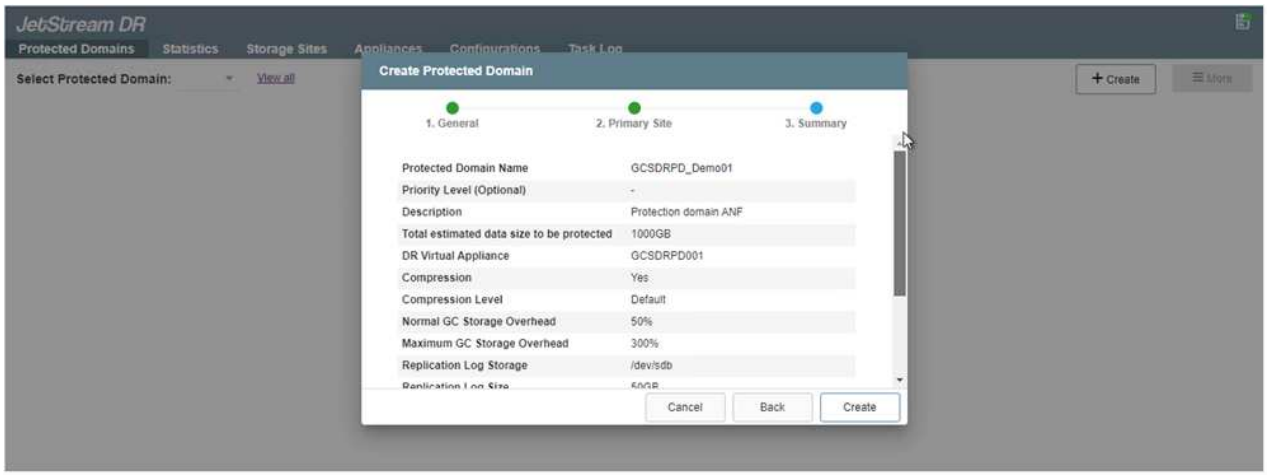
   容量計画ツールを使用して、必要な DRVA の数を見積もってください。

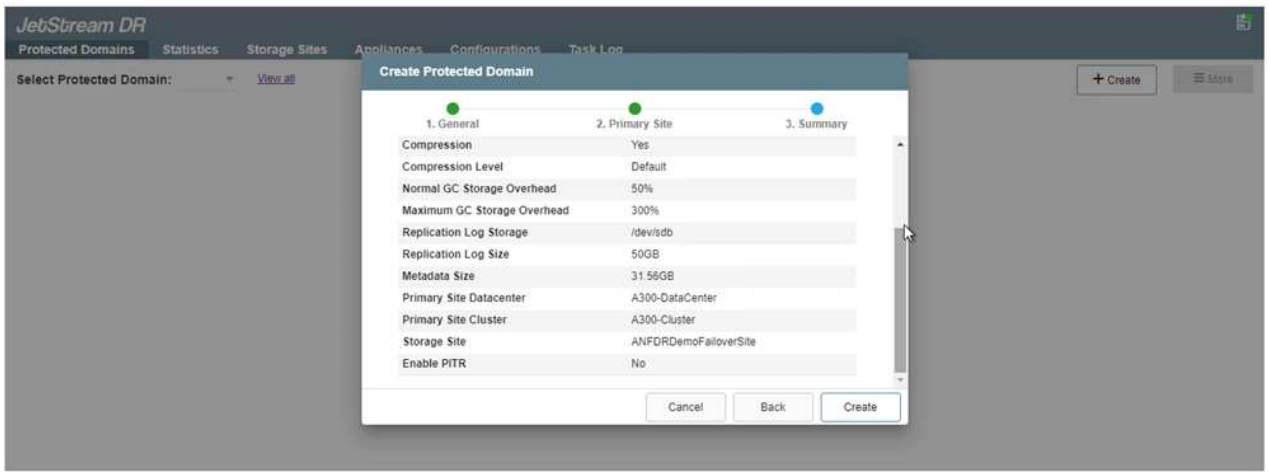


9. 使用可能なデータストアまたは独立した共有 iSCSI ストレージ プールの VMDK を使用して、各 DRVA のレプリケーション ログ ボリュームを作成します。



10. [保護されたドメイン] タブで、Azure Blob Storage サイト、DRVA インスタンス、レプリケーションログに関する情報を使用して、必要な数の保護されたドメインを作成します。保護されたドメインは、一緒に保護され、フェイルオーバー/フェイルバック操作の優先順位が割り当てられている、クラスター内の特定の VM またはアプリケーション VM のセットを定義します。

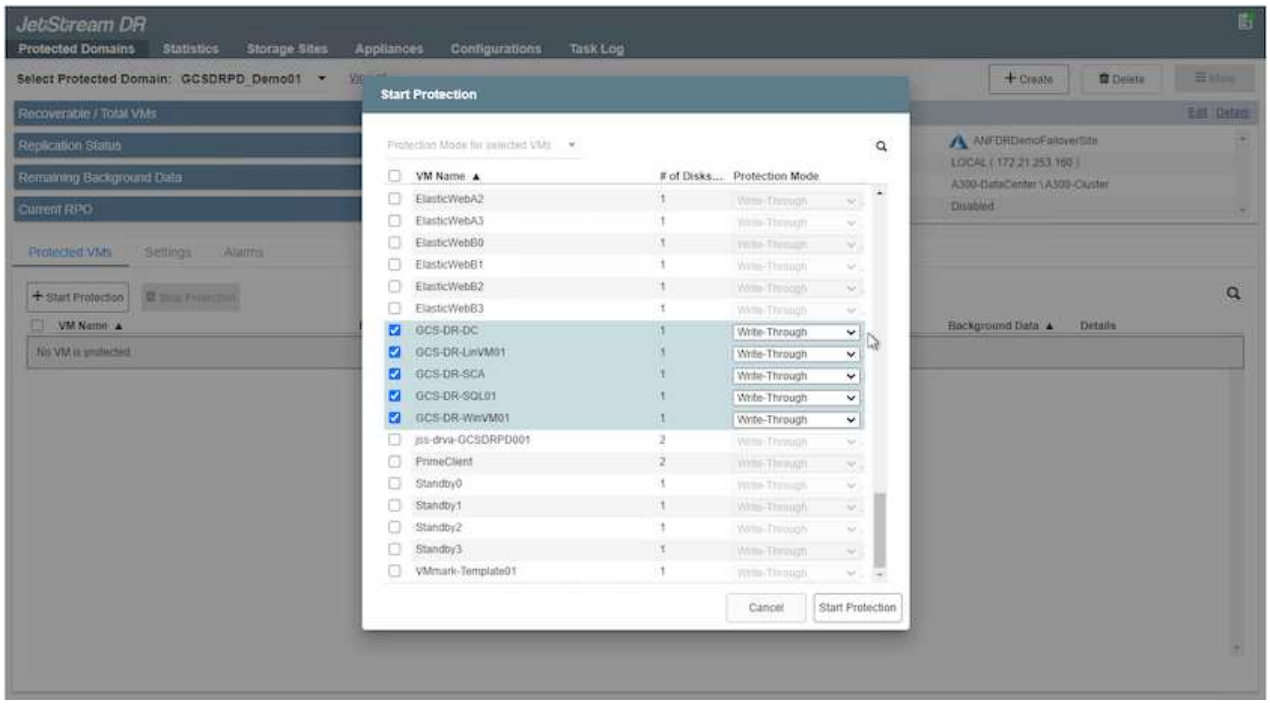




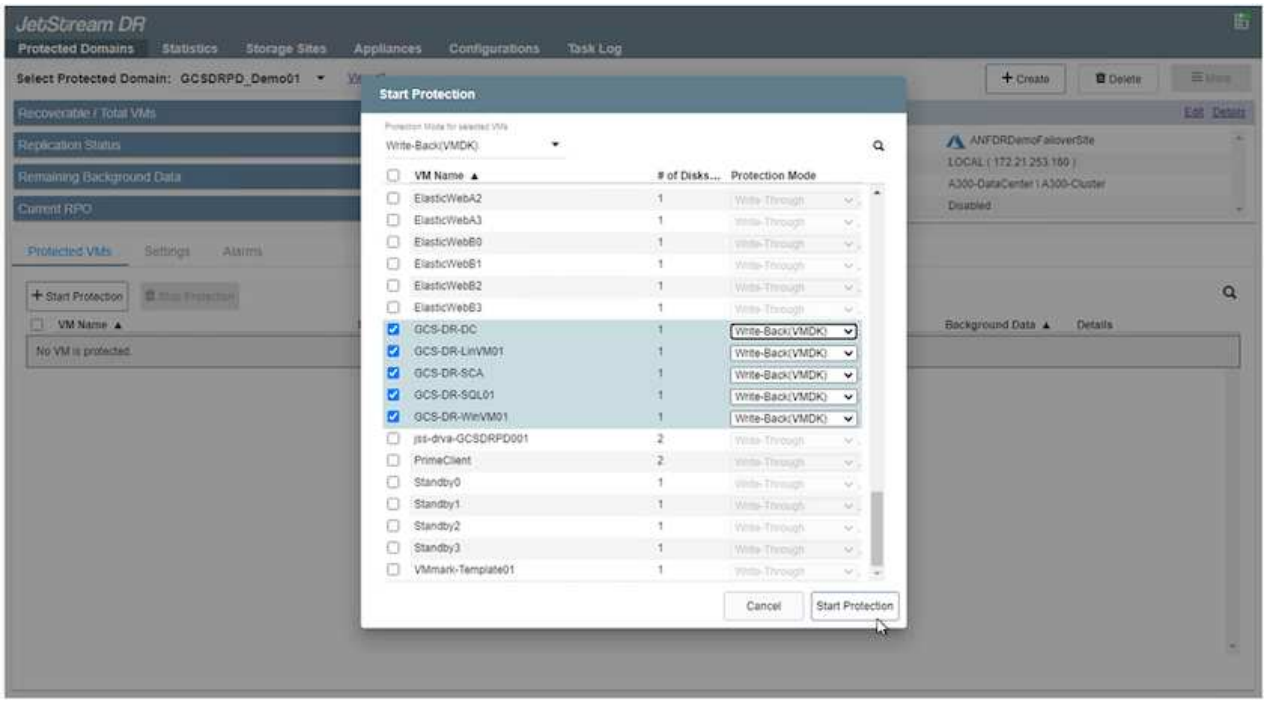
11. 保護する VM を選択し、依存関係に基づいて VM をアプリケーション グループにグループ化します。アプリケーション定義を使用すると、VM のセットを、ブート順序、ブート遅延、およびリカバリ時に実行できるオプションのアプリケーション検証を含む論理グループにグループ化できます。

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

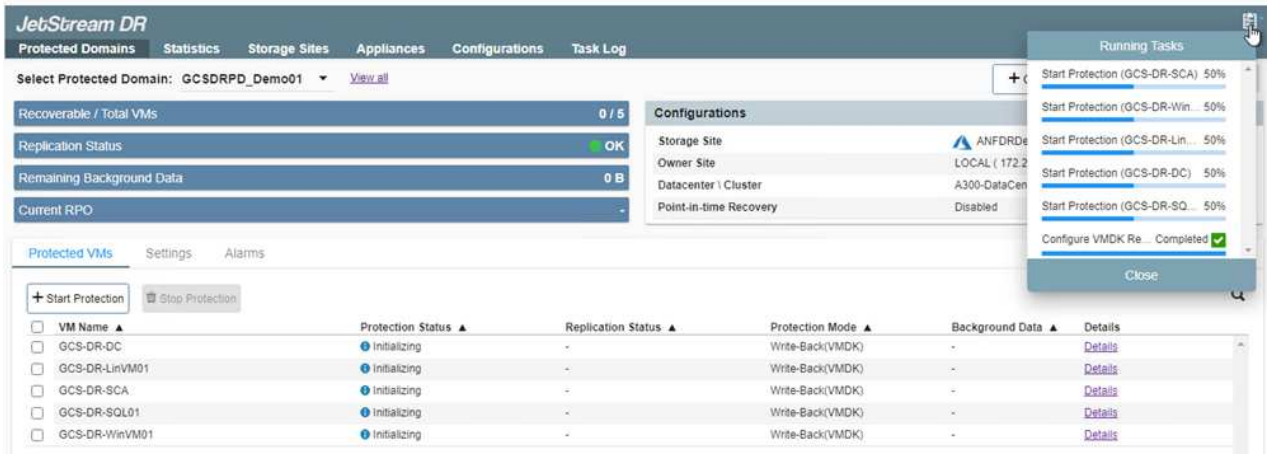
ライトバック (VMDK) モードでは、より高いパフォーマンスが提供されます。



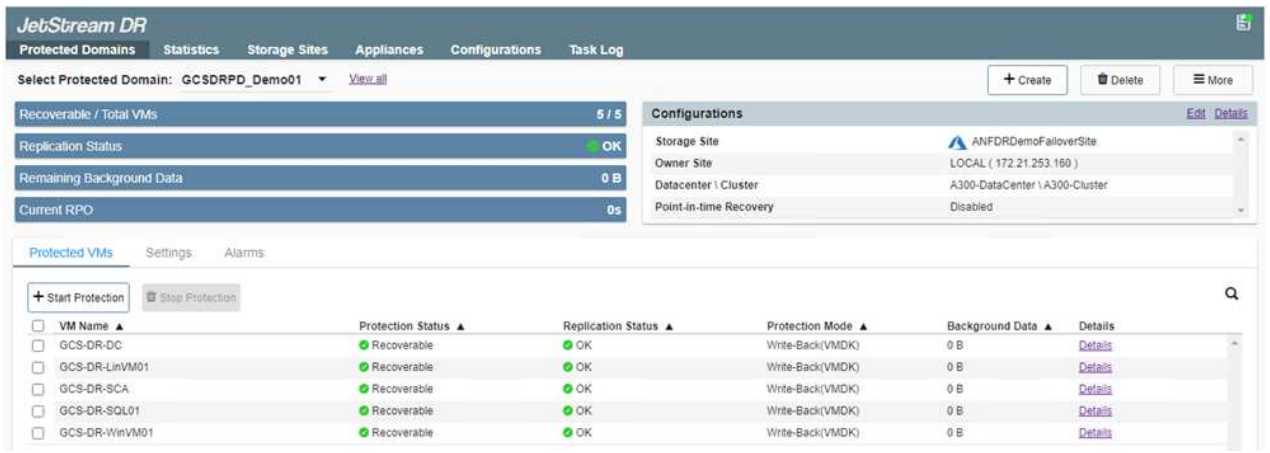
12. レプリケーション ログ ボリュームが高性能ストレージに配置されていることを確認します。



13. 完了したら、保護されたドメインの「保護の開始」をクリックします。これにより、選択した VM の指定された BLOB ストアへのデータ レプリケーションが開始されます。



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

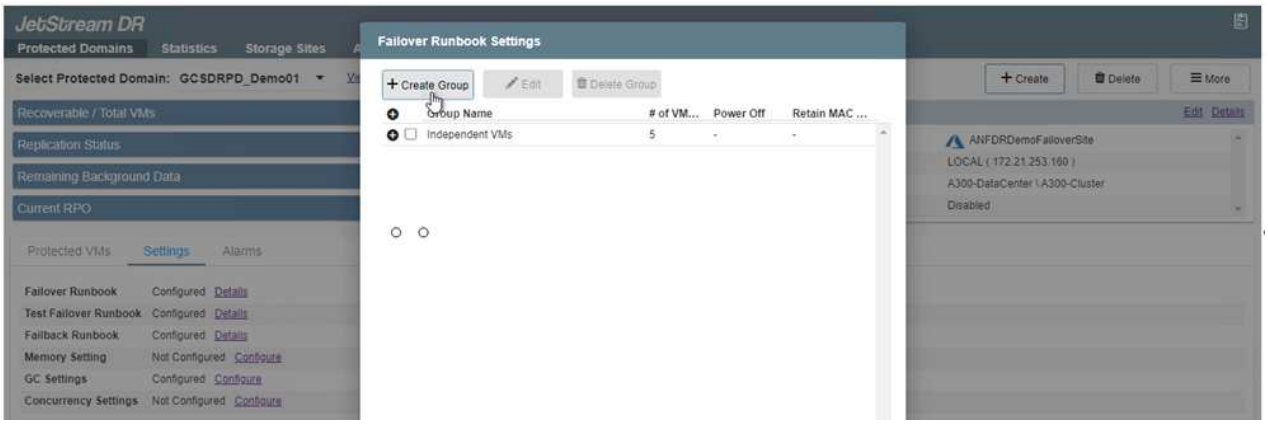


フェールオーバー ランブックは、VM をグループ化 (回復グループと呼ばれる) し、ブート順序シーケンスを設定し、CPU/メモリ設定と IP 構成を変更するように構成できます。

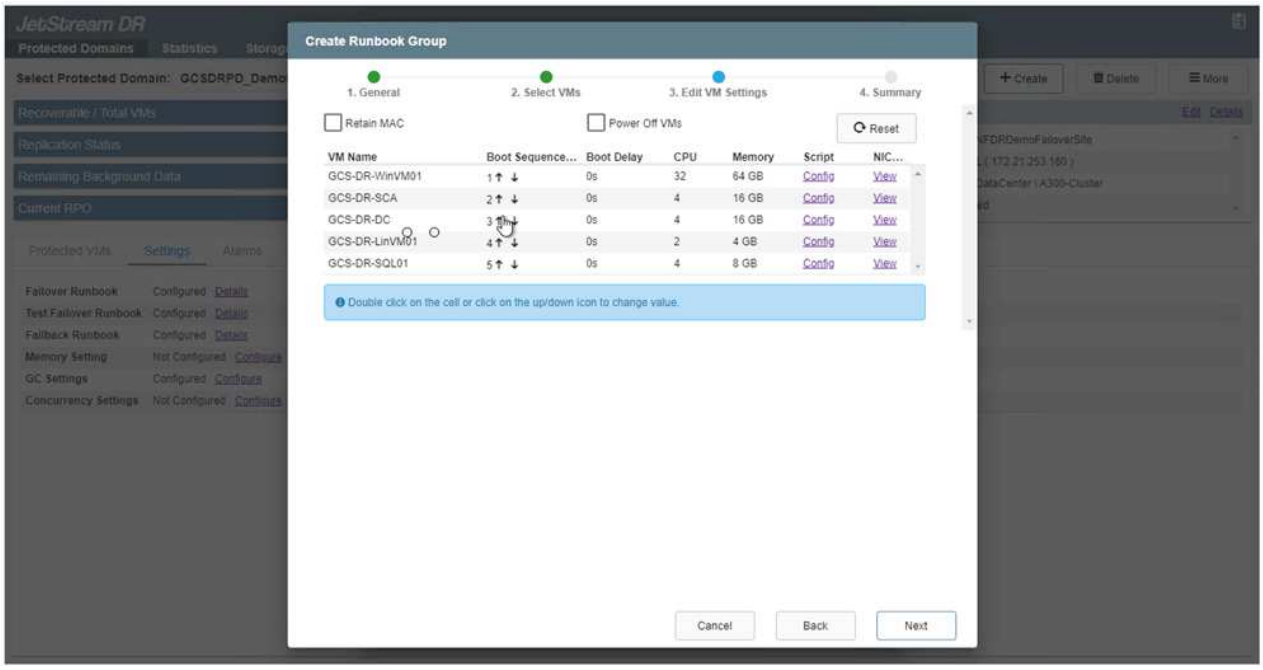
15. [設定] をクリックし、Runbook の構成リンクをクリックして、Runbook グループを構成します。

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

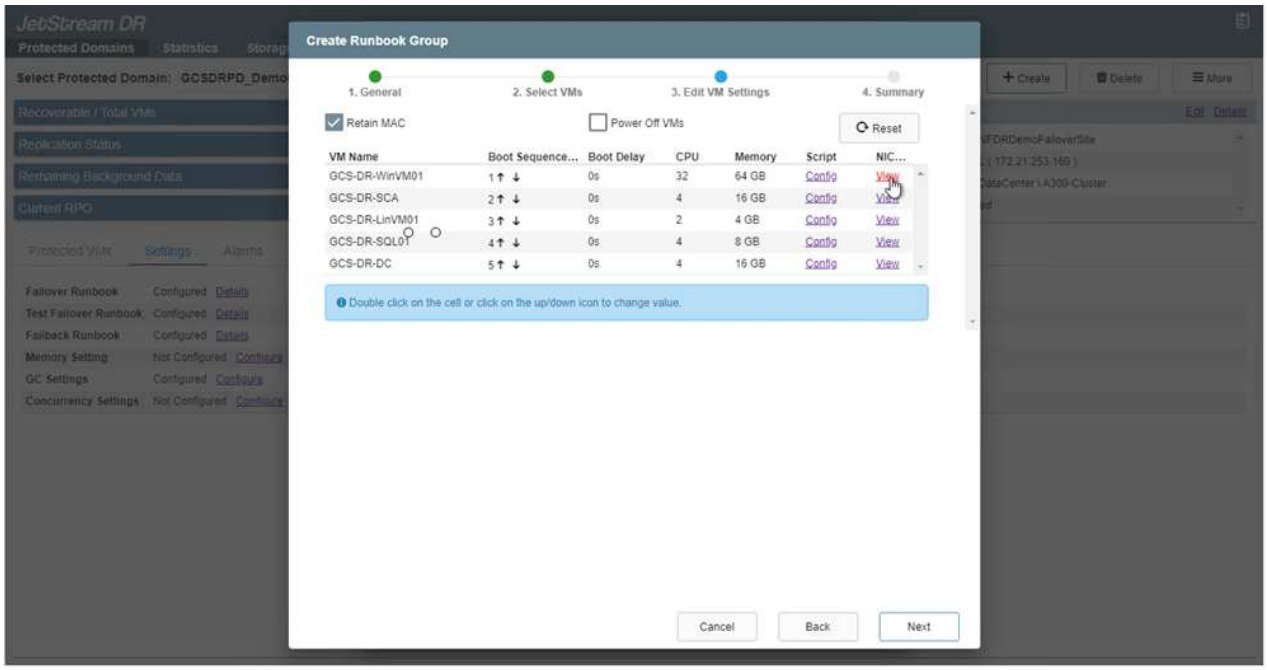
必要に応じて、画面の下部で、ランブック グループの操作の前後に自動的に実行されるカスタム事前スクリプトと事後スクリプトを適用します。 Runbook スクリプトが管理サーバー上に存在していることを確認します。



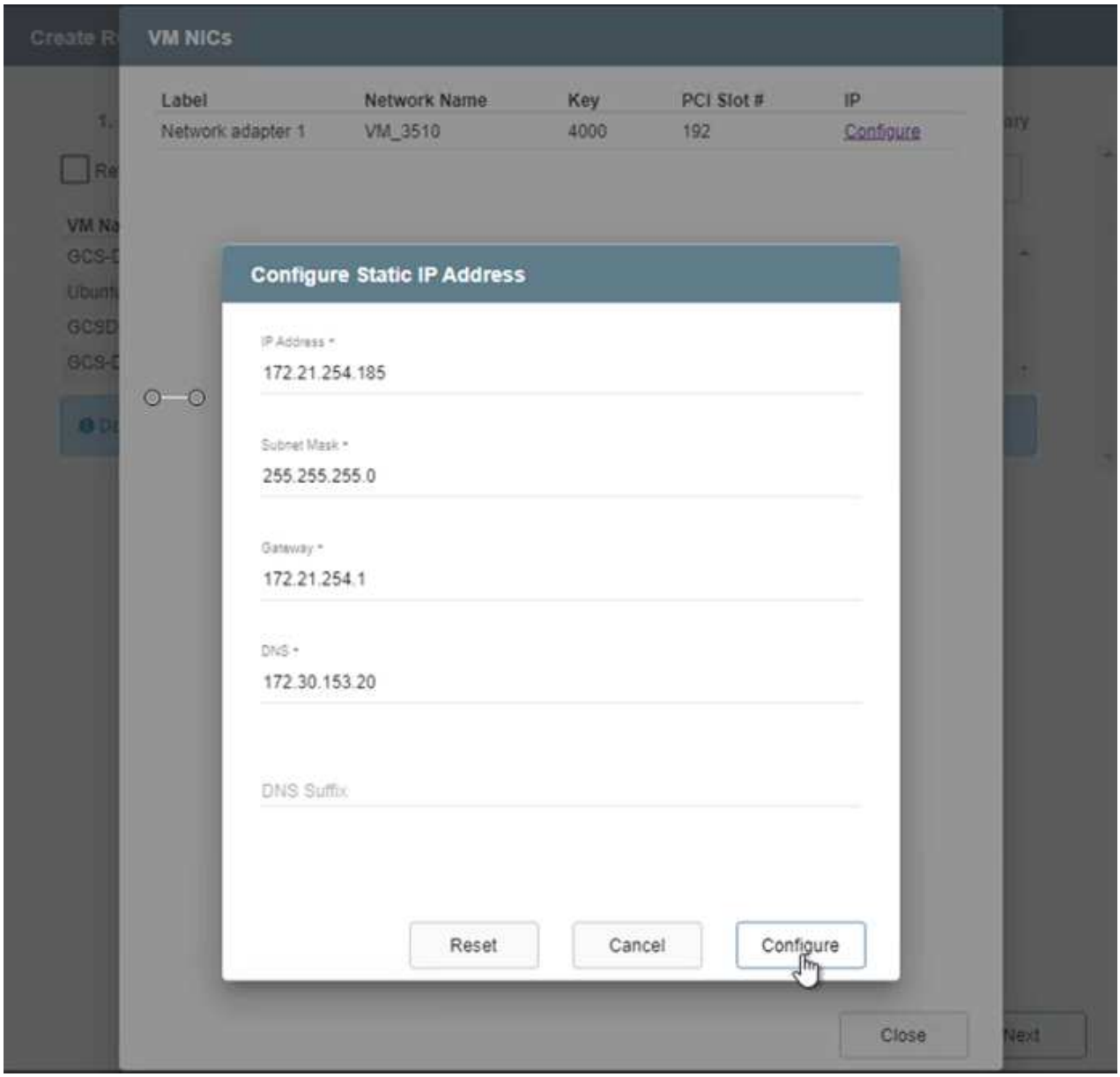
17. 必要に応じて VM 設定を編集します。ブート シーケンス、ブート遅延 (秒単位で指定)、CPU の数、割り当てるメモリの量など、VM を回復するためのパラメータを指定します。上矢印または下矢印をクリックして、VM のブート シーケンスを変更します。 MAC を保持するためのオプションも提供されています。

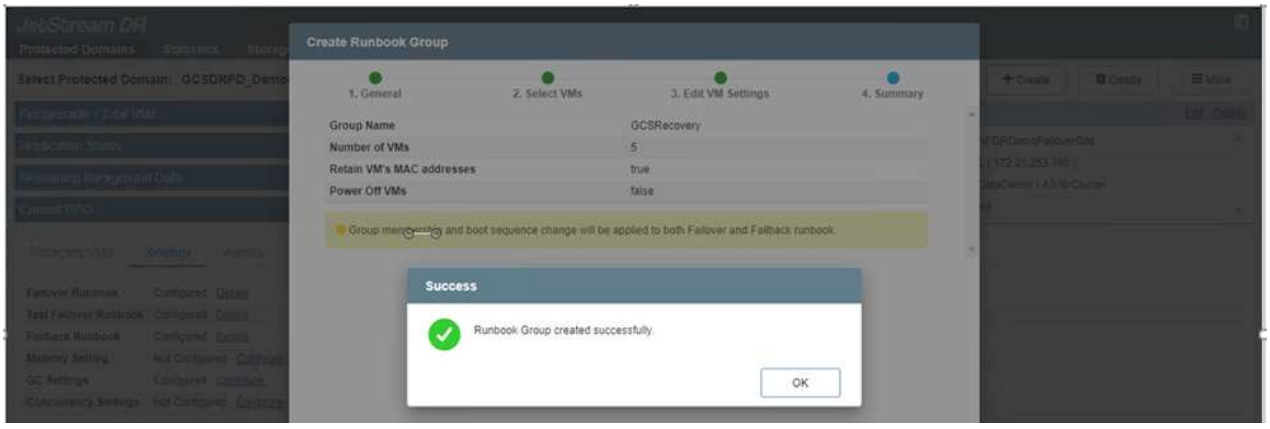


18. グループ内の個々の VM に対して静的 IP アドレスを手動で構成できます。 VM の NIC ビュー リンクをクリックして、IP アドレス設定を手動で構成します。



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





フェールオーバー ランブックとフェールバック ランブックの両方のステータスが [構成済み] として表示されます。フェールオーバー ランブック グループとフェールバック ランブック グループは、同じ初期 VM グループと設定を使用してペアで作成されます。必要に応じて、それぞれの「詳細」リンクをクリックして変更することで、ランブック グループの設定を個別にカスタマイズできます。

リカバリ サイト (AVS) のベスト プラクティスは、3 ノードのパイロット ライト クラスターを事前に作成することです。これにより、次のようなリカバリ サイトのインフラストラクチャを事前に構成できます。

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

JetStream DR は、ミッションクリティカルなドメインに対してほぼゼロの RTO モードをサポートします。これらのドメインでは、宛先ストレージが事前にインストールされている必要があります。この場合、ANF が推奨されるストレージ タイプです。

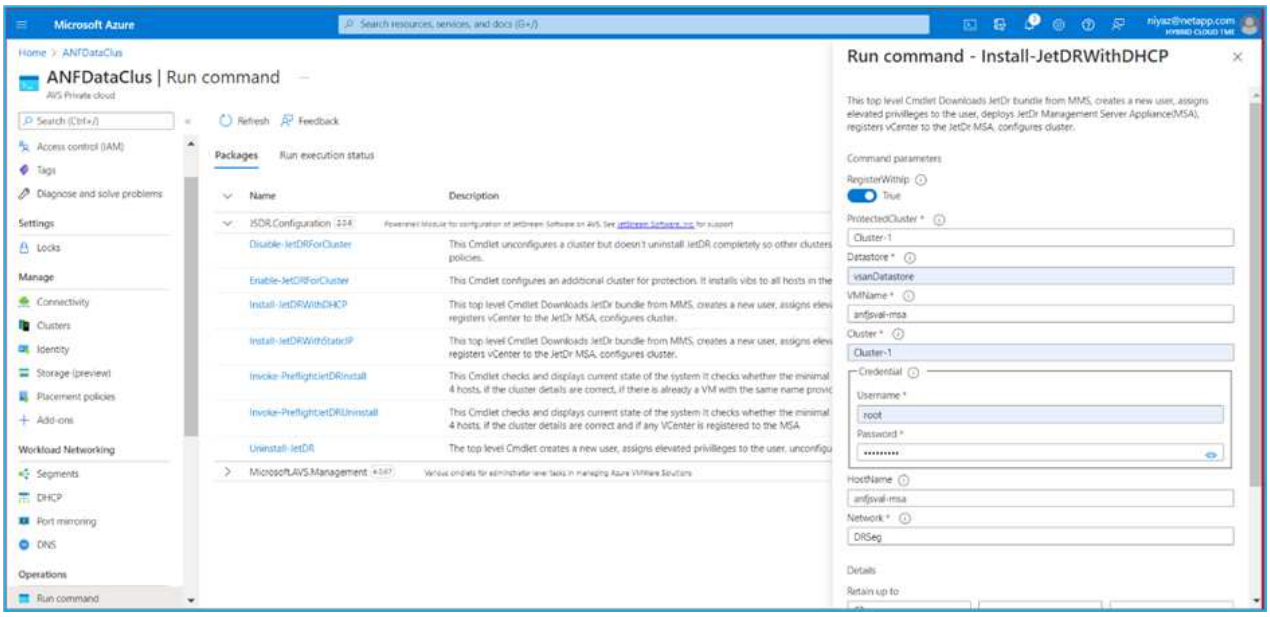
セグメント作成を含むネットワーク構成は、オンプレミスの要件に合わせて AVS クラスター上で構成する必要があります。

SLA および RTO 要件に応じて、継続的なフェイルオーバー モードまたは通常の (標準) フェイルオーバー モードを使用できます。 RTO をほぼゼロにするには、リカバリサイトで継続的な再水和を開始する必要があります。

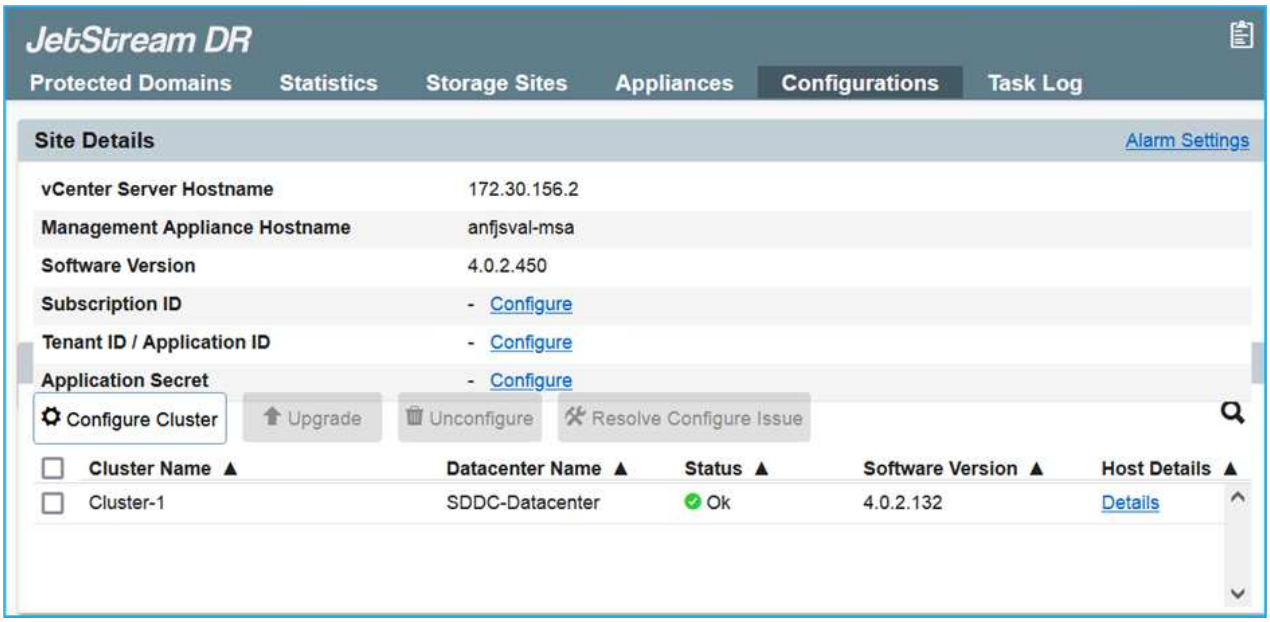
1. Azure VMware Solution プライベート クラウドに JetStream DR for AVS をインストールするには、実行コマンドを使用します。 Azure ポータルから Azure VMware ソリューションに移動し、プライベート クラウドを選択して、[コマンドの実行] > [パッケージ] > [JSDR.Configuration] を選択します。

   Azure VMware Solution のデフォルトの CloudAdmin ユーザーには、JetStream DR for AVS をインストールするための十分な権限がありません。 Azure VMware Solution では、JetStream DR の Azure VMware Solution 実行コマンドを呼び出すことで、JetStream DR のインストールを簡素化および自動化できます。

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



2. JetStream DR for AVS のインストールが完了したら、ブラウザを更新します。 JetStream DR UI にアクセスするには、[SDDC データセンター] > [構成] > [JetStream DR] に移動します。



3. JetStream DR インターフェースから、次のタスクを完了します。

   a. オンプレミス クラスターを保護するために使用された Azure Blob Storage アカウントをストレージ サイトとして追加し、スキャン ドメイン オプションを実行します。

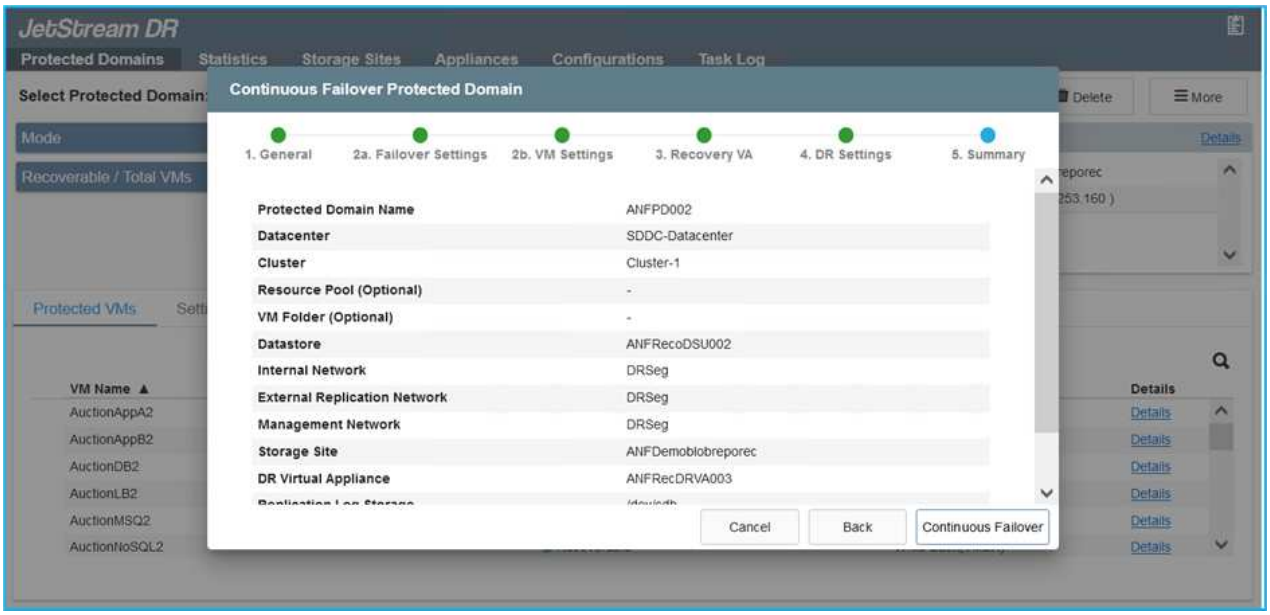
   b. 表示されるポップアップ ダイアログ ウィンドウで、インポートする保護されたドメインを選択し、そのインポート リンクをクリックします。

4. ドメインは回復のためにインポートされます。 [保護されたドメイン] タブに移動し、目的のドメインが選択されていることを確認するか、[保護されたドメインの選択] メニューから目的のドメインを選択します。保護されたドメイン内の回復可能な VM のリストが表示されます。

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

   これらの手順は、CPT が作成した計画を使用して自動化することもできます。

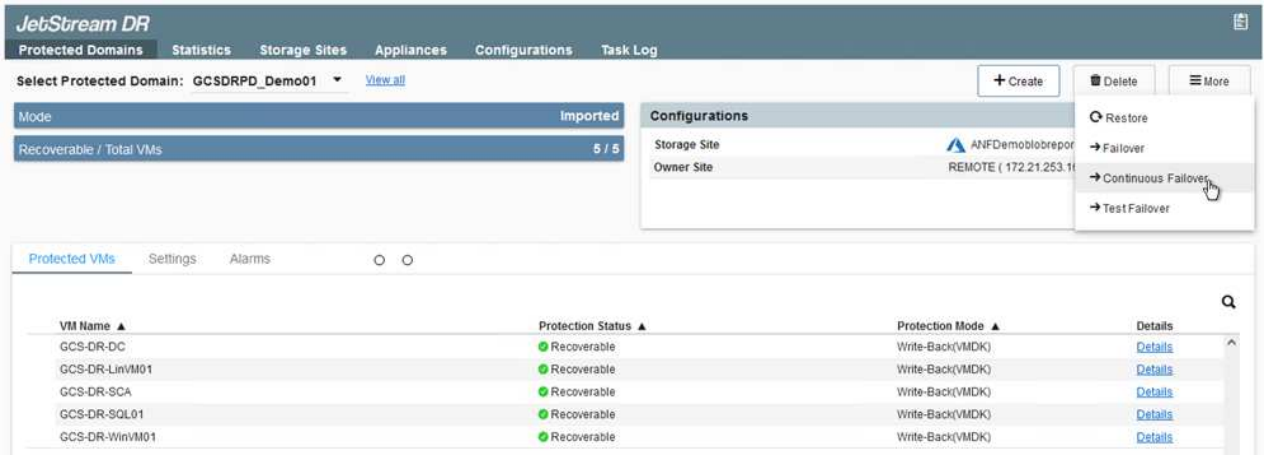
6. 利用可能な vSAN または ANF データストアを使用してレプリケーション ログ ボリュームを作成します。
7. 保護されたドメインをインポートし、VM の配置に ANF データストアを使用するようにリカバリ VA を構成します。



   選択したセグメントで DHCP が有効になっており、十分な IP が利用可能であることを確認します。ドメインが回復している間、動的 IP が一時的に使用されます。回復中の各 VM (継続的なリハイドレーションを含む) には個別の動的 IP が必要です。回復が完了すると、IP は解放され、再利用できるようになります。

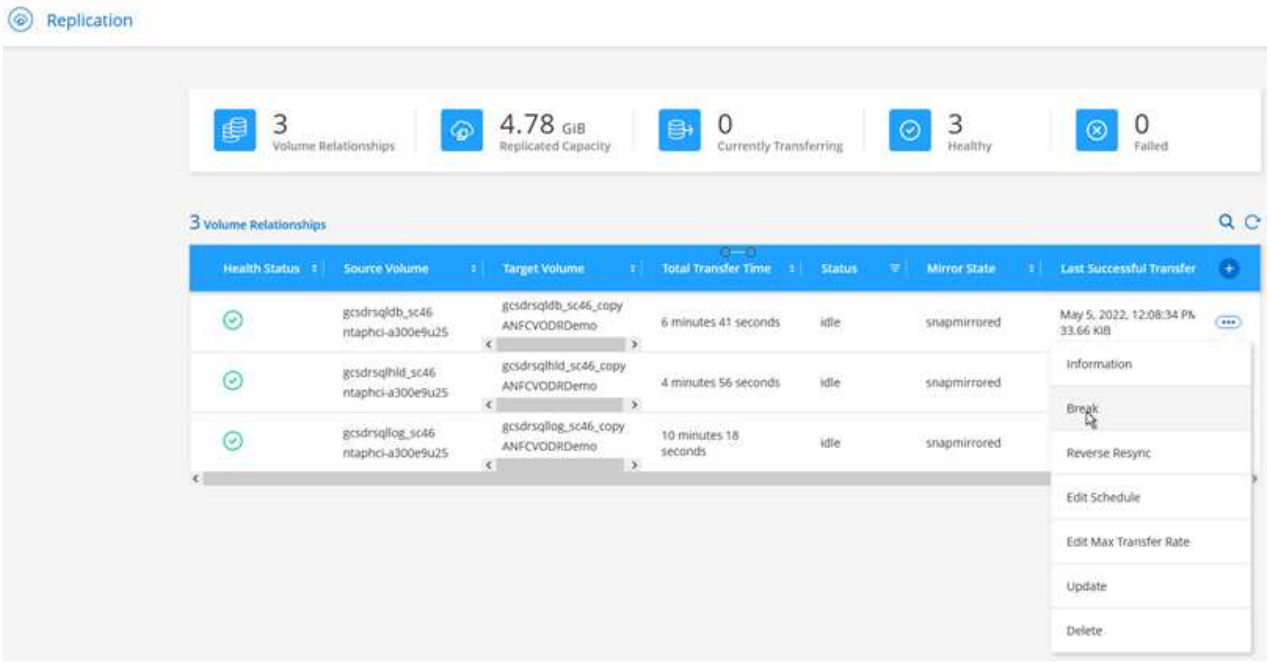
8. 適切なフェイルオーバー オプション (継続的なフェイルオーバーまたはフェイルオーバー) を選択します。この例では、継続的なリハイドレーション (継続的なフェイルオーバー) が選択されています。

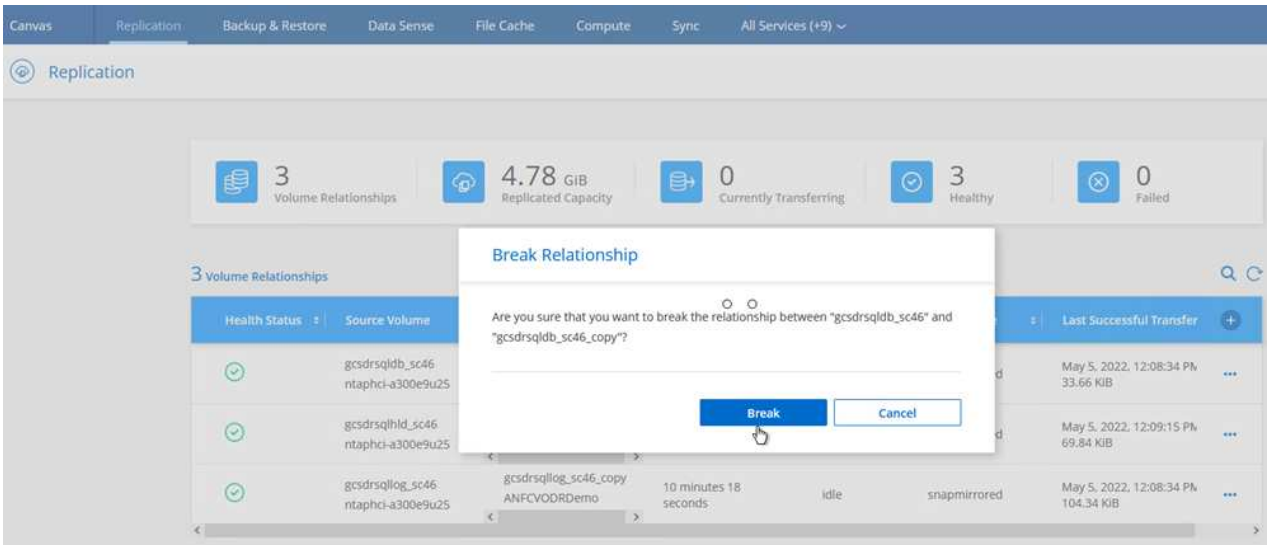
   継続的なフェイルオーバー モードとフェイルオーバー モードは構成の実行タイミングが異なりますが、両方のフェイルオーバー モードは同じ手順で構成されます。災害イベントに応じて、フェイルオーバー手順がまとめて構成され、実行されます。継続的なフェイルオーバーはいつでも構成でき、通常のシステム操作中にバックグラウンドで実行できます。災害イベントが発生すると、継続的なフェイルオーバーが完了し、保護された VM の所有権がリカバリ サイトに即座に転送されます (RTO はほぼゼロ)。



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

1. オンプレミス環境の保護されたクラスターで災害 (部分的または完全な障害) が発生した後、それぞれのアプリケーション ボリュームのSnapMirror関係を解除した後、Jetstream を使用して VM のフェイルオーバーをトリガーできます。

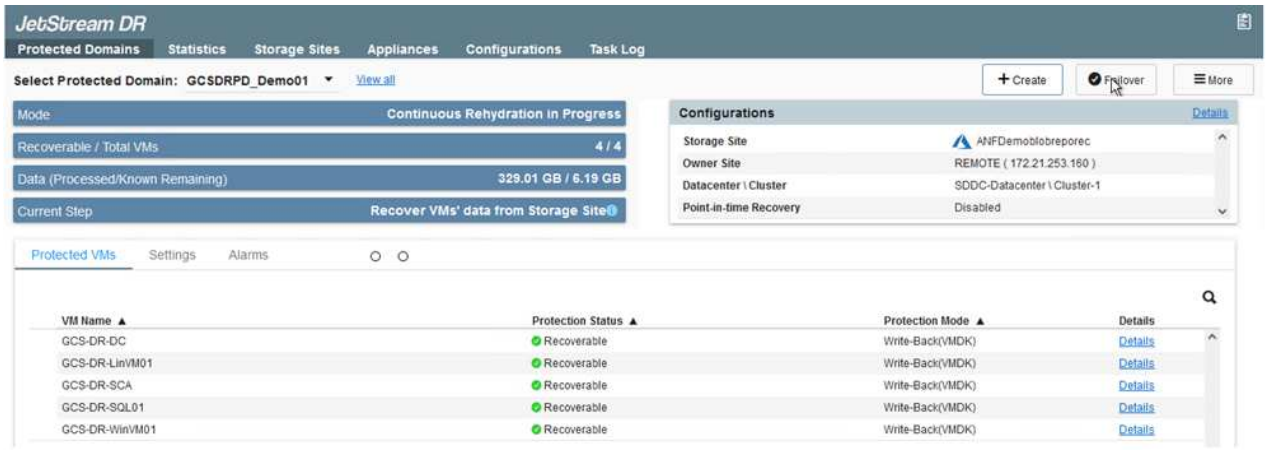


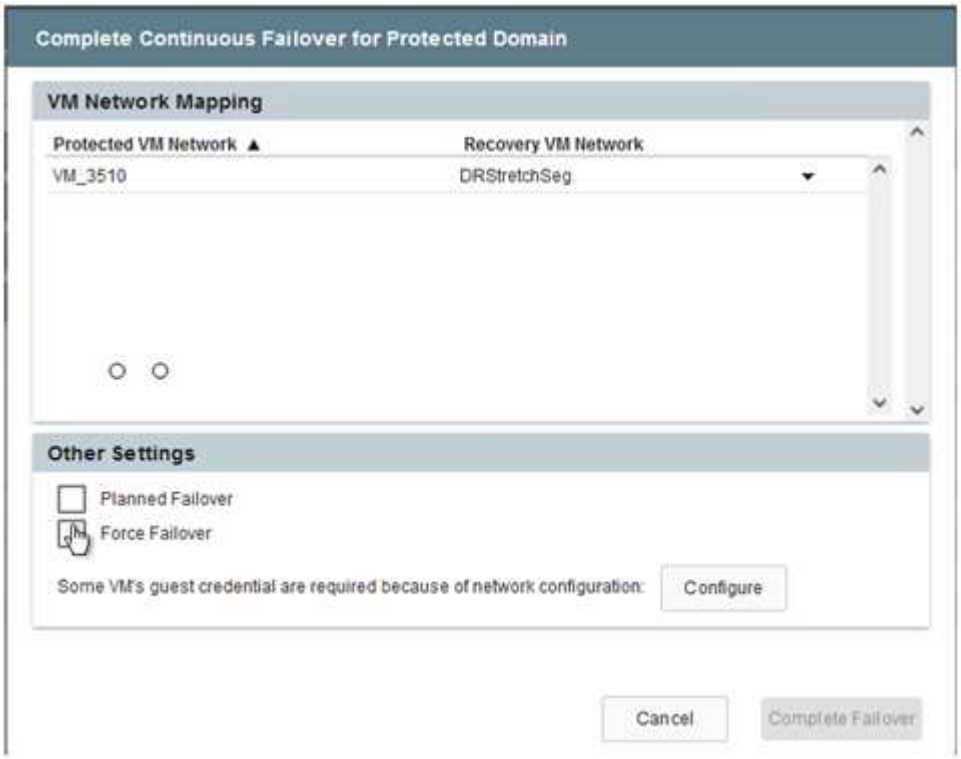


このステップは簡単に自動化でき、回復プロセスが容易になります。

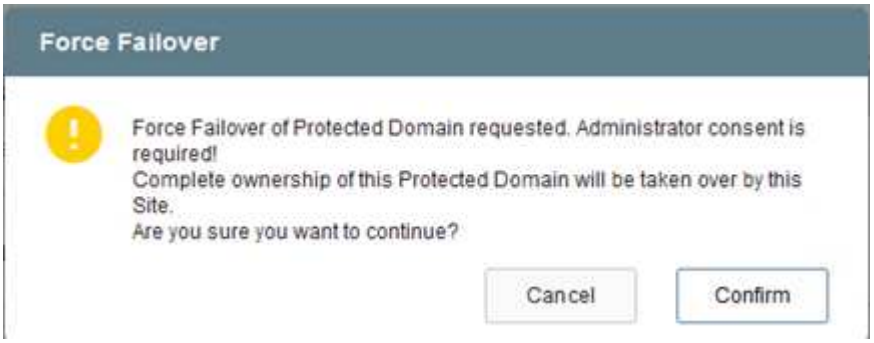
2. AVS SDDC (宛先側) の Jetstream UI にアクセスし、フェイルオーバー オプションをトリガーしてフェイルオーバーを完了します。タスク バーには、フェールオーバー アクティビティの進行状況が表示されます。

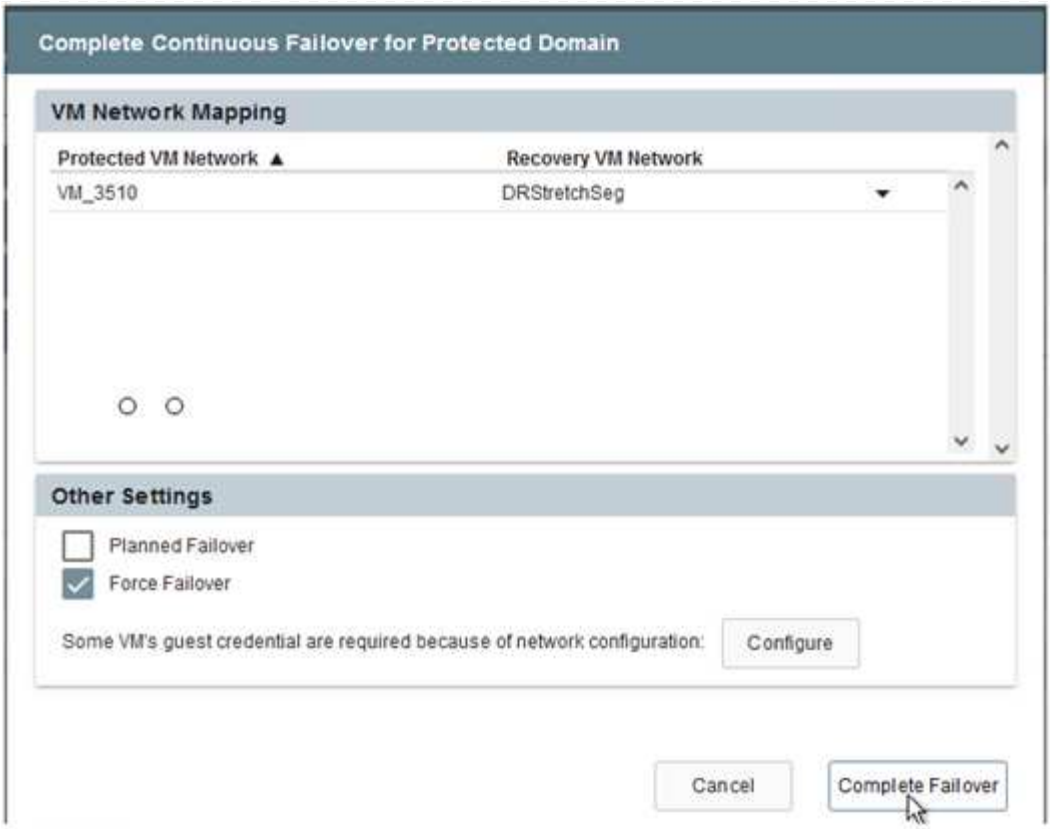
   フェイルオーバーの完了時に表示されるダイアログ ウィンドウでは、フェイルオーバー タスクを計画どおりに実行するか、強制実行するかを指定できます。





強制フェールオーバーでは、プライマリ サイトにアクセスできなくなり、保護されたドメインの所有権はリカバリ サイトが直接引き継ぐ必要があると想定されます。



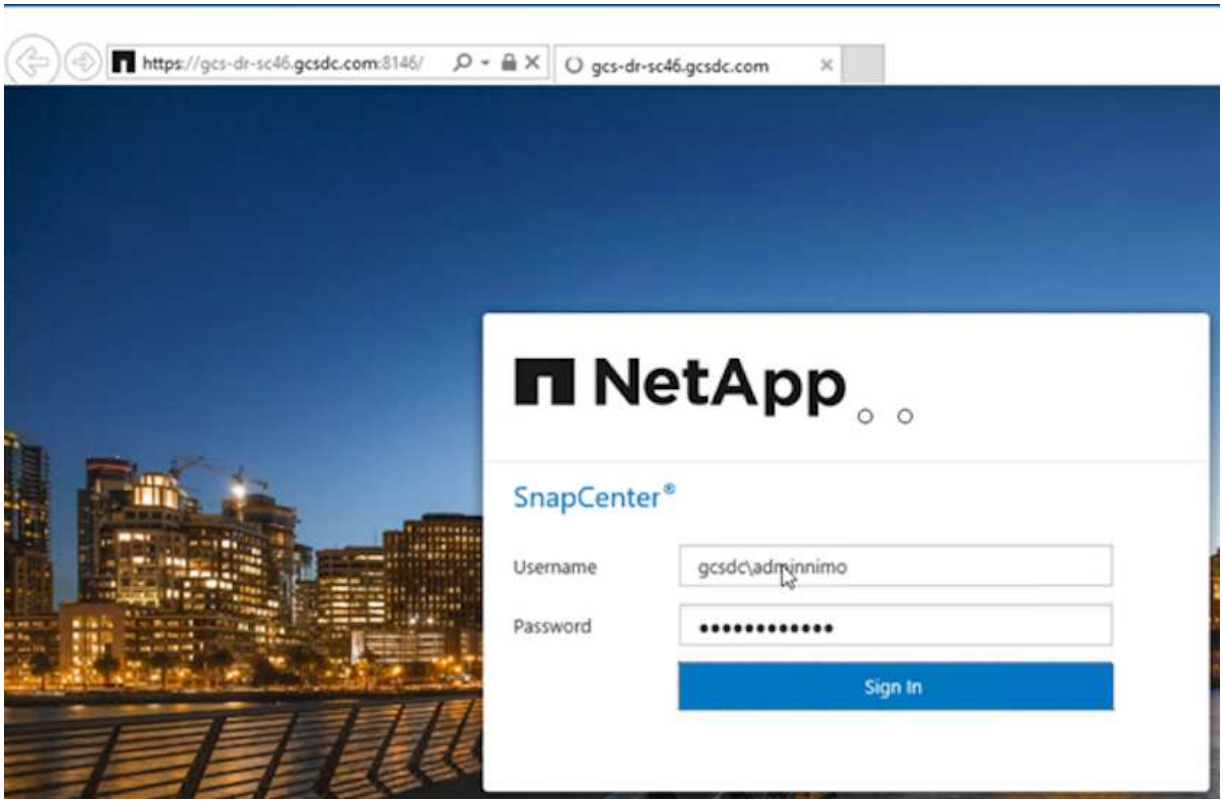


3. 継続的なフェイルオーバーが完了すると、タスクの完了を確認するメッセージが表示されます。タスクが完了したら、回復した VM にアクセスして、ISCSI または NFS セッションを構成します。

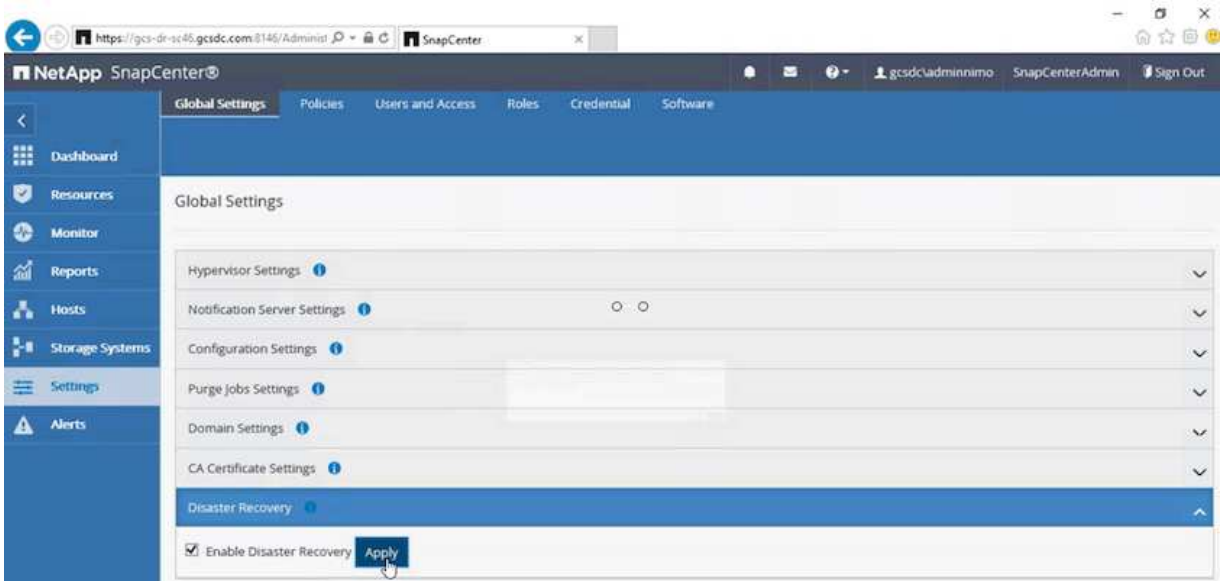
フェールオーバー モードが「フェールオーバーで実行中」に変わり、VM のステータスは「回復可能」になります。保護されたドメインのすべての VM が、フェールオーバー ランブック設定で指定された状態で回復サイトで実行されるようになりました。

フェイルオーバー構成とインフラストラクチャを検証するには、JetStream DR をテスト モード (テスト フェイルオーバー オプション) で操作して、オブジェクト ストアからテスト リカバリ環境への仮想マシンとそのデータのリカバリを観察できます。フェイルオーバー手順をテスト モードで実行すると、その操作は実際のフェイルオーバー プロセスに似たものになります。

4. 仮想マシンが復旧されたら、ゲスト内のストレージに対してストレージ ディザスタ リカバリを使用します。この例では、このプロセスを説明するために、SQL サーバーを使用します。
5. AVS SDDC 上の回復されたSnapCenter VM にログインし、DR モードを有効にします。
   a. ブラウザN を使用してSnapCenter UI にアクセスします。



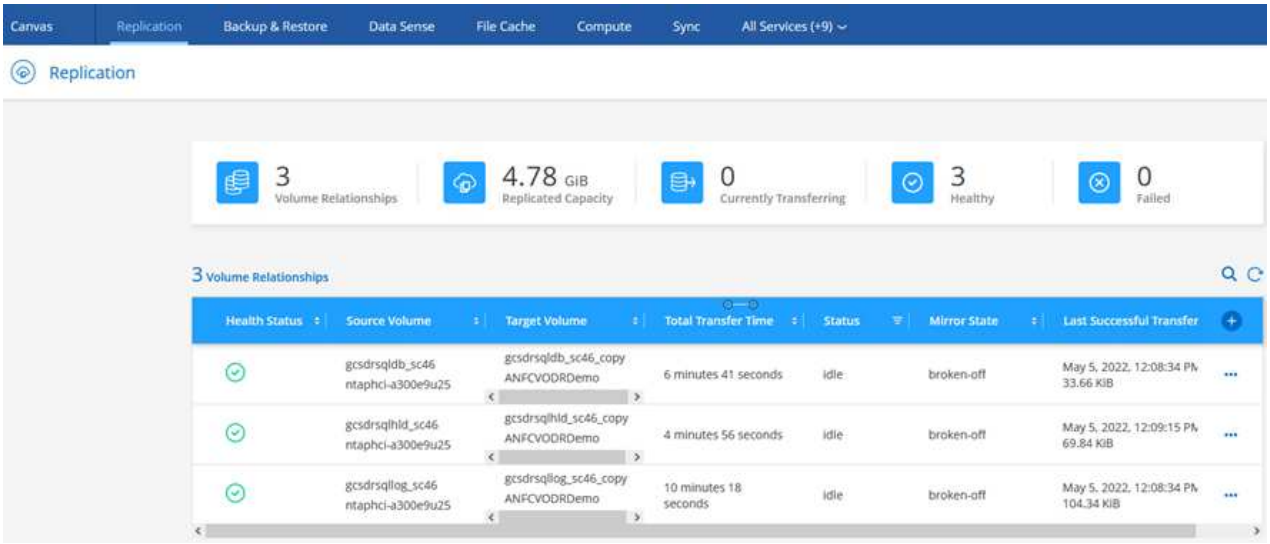
   b. [設定] ページで、[設定] > [グローバル設定] > [障害復旧] に移動します。
   c. 「災害復旧を有効にする」を選択します。
   d. [Apply]をクリックします。



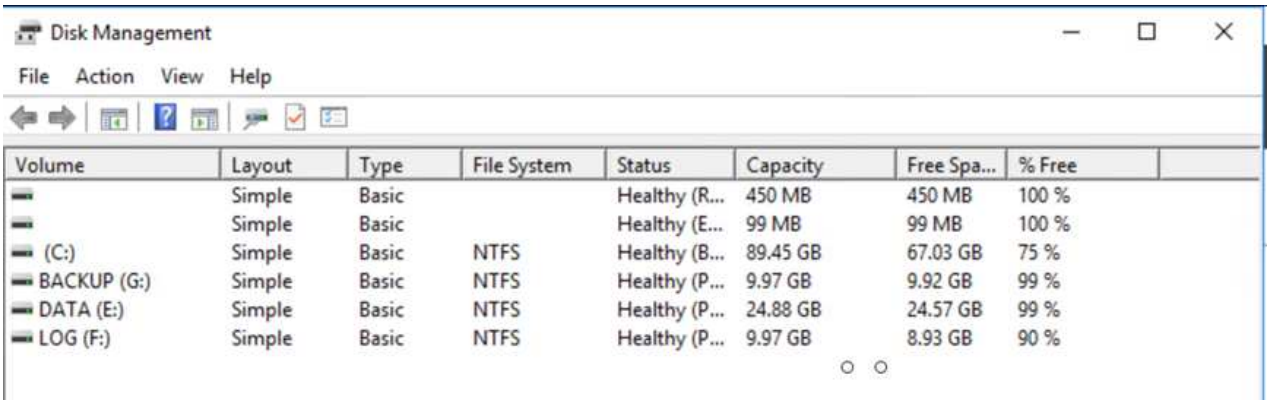
e. [モニター] > [ジョブ] をクリックして、DR ジョブが有効になっているかどうかを確認します。

ストレージの災害復旧には、 NetApp SnapCenter 4.6 以降を使用する必要があります。以前のバージョンでは、アプリケーション整合性スナップショット (SnapMirrorを使用して複製) を使用し、災害復旧サイトで以前のバックアップを復旧する必要がある場合は手動復旧を実行する必要があります。

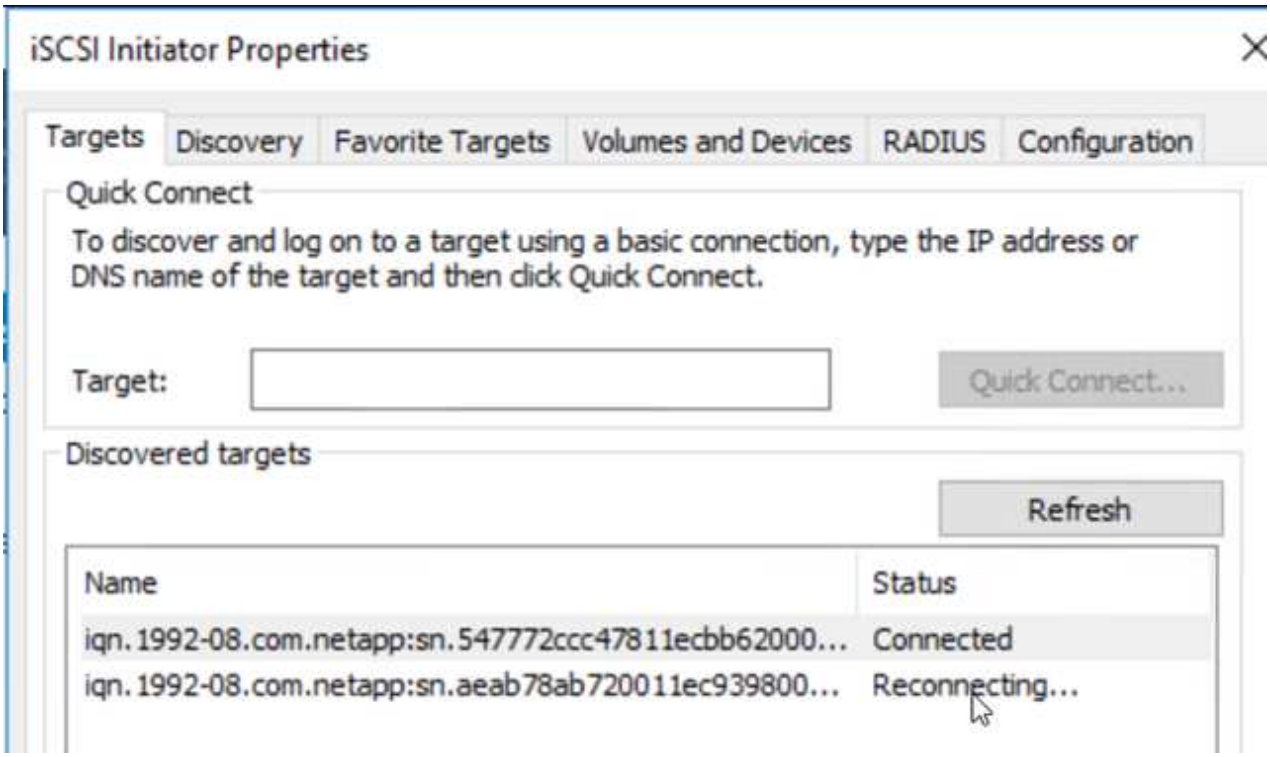
6. SnapMirror関係が解除されていることを確認します。



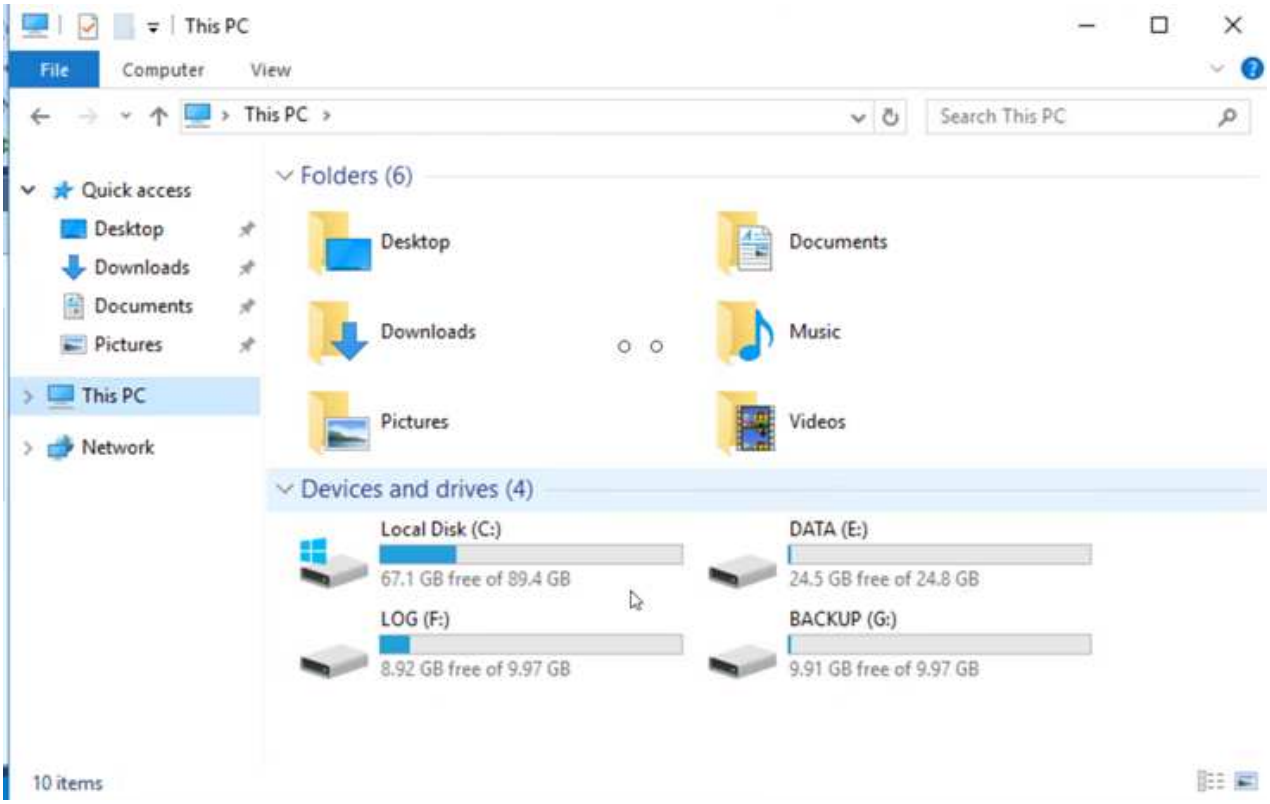
7. Cloud Volumes ONTAPからの LUN を、同じドライブ文字を使用して、回復した SQL ゲスト VM に接続します。



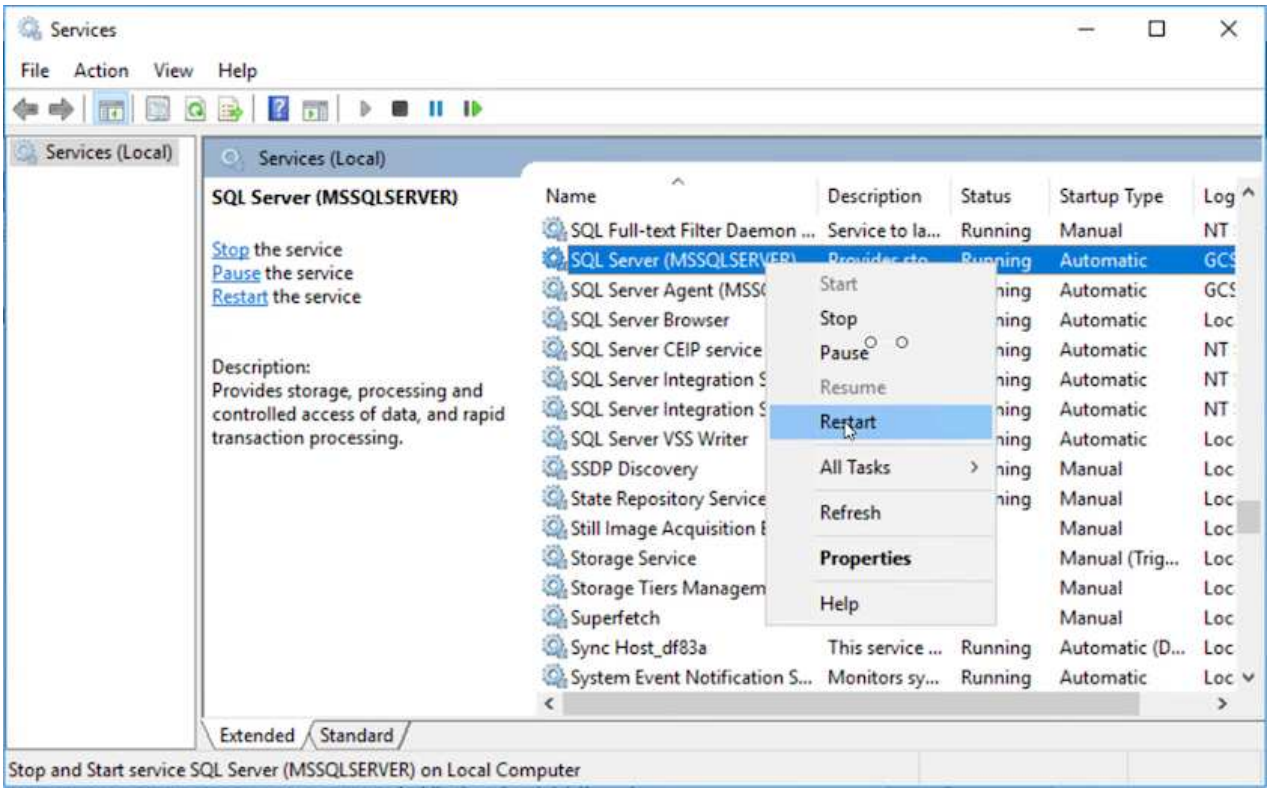
8. iSCSI イニシエーターを開き、以前の切断されたセッションをクリアし、複製されたCloud Volumes ONTAPボリュームのマルチパスとともに新しいターゲットを追加します。



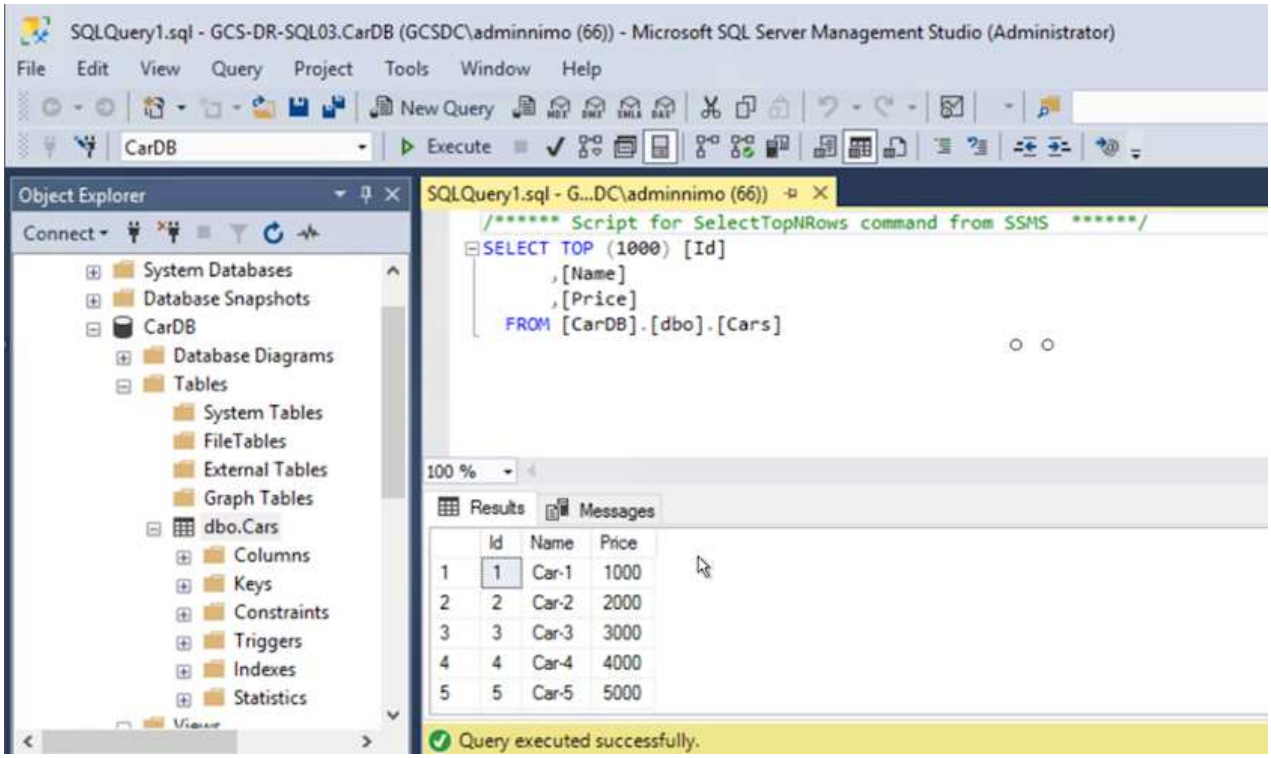
9. すべてのディスクが DR 前に使用されていたのと同じドライブ文字を使用して接続されていることを確認します。



10. MSSQL サーバー サービスを再起動します。



11. SQL リソースがオンラインに戻っていることを確認します。



NFSの場合は、マウントコマンドを使用してボリュームを接続し、 `/etc/fstab`エントリ。

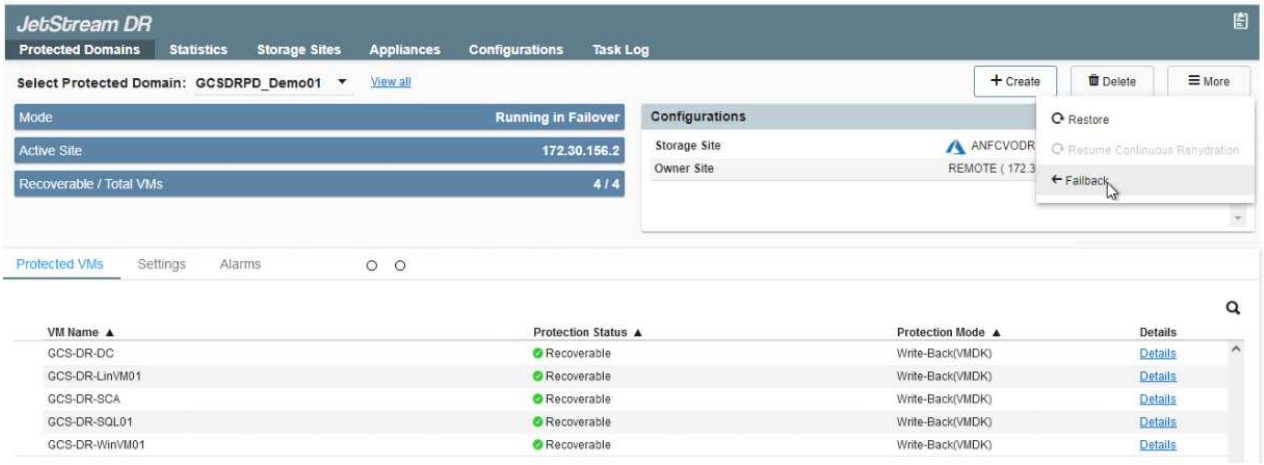
この時点で、操作を実行でき、ビジネスは正常に継続されます。

NSX-T 側では、フェイルオーバー シナリオをシミュレートするために、専用の Tier-1 ゲートウェイを別途作成できます。これにより、すべてのワークロードが相互に通信できる一方で、環境内外へのトラフィックのルーティングが不可能となり、相互汚染のリスクなしにトリアージ、封じ込め、または強化タスクを実行できるようになります。この操作はこのドキュメントの範囲外ですが、分離をシミュレートするために簡単に実行できます。

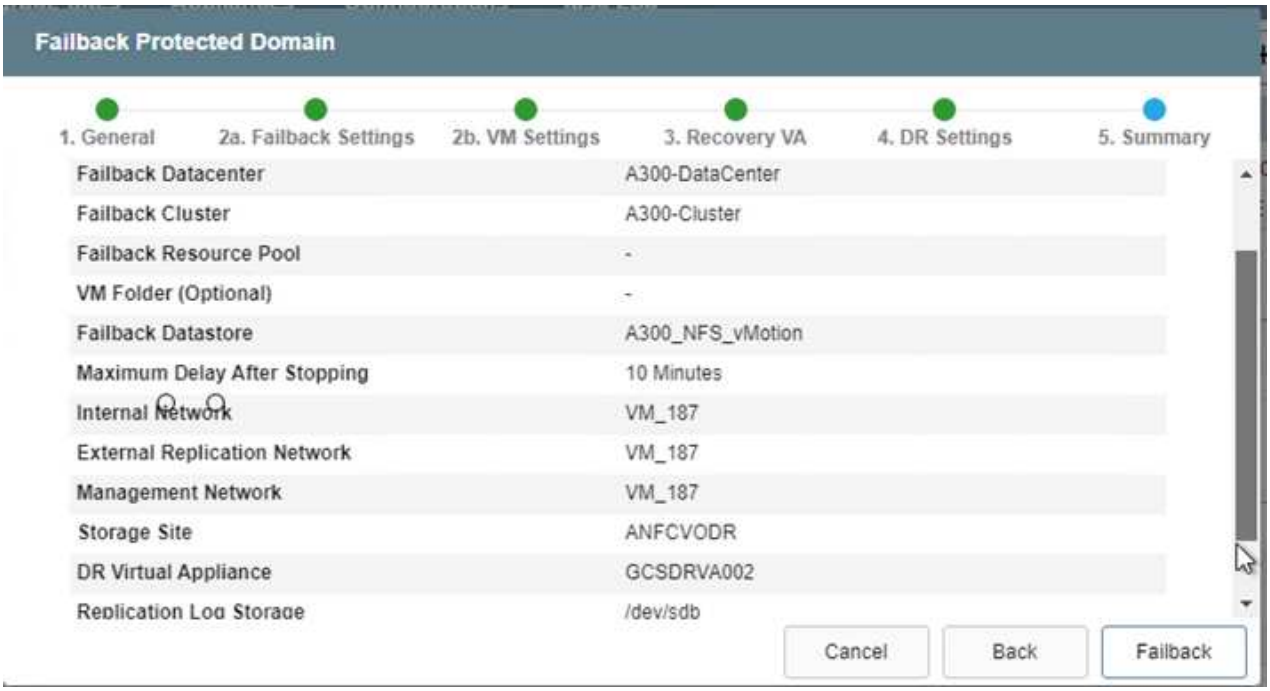
プライマリ サイトが再び稼働したら、フェイルバックを実行できます。 VM 保護は Jetstream によって再開され、 SnapMirror関係を元に戻す必要があります。

1. オンプレミス環境を復元します。災害インシデントの種類によっては、保護されたクラスターの構成を復元および/または検証する必要がある場合があります。必要に応じて、JetStream DR ソフトウェアを再インストールする必要があります。
2. 復元されたオンプレミス環境にアクセスし、Jetstream DR UI に移動して、適切な保護されたドメインを選択します。保護されたサイトのフェイルバックの準備ができたら、UI でフェイルバック オプションを選択します。

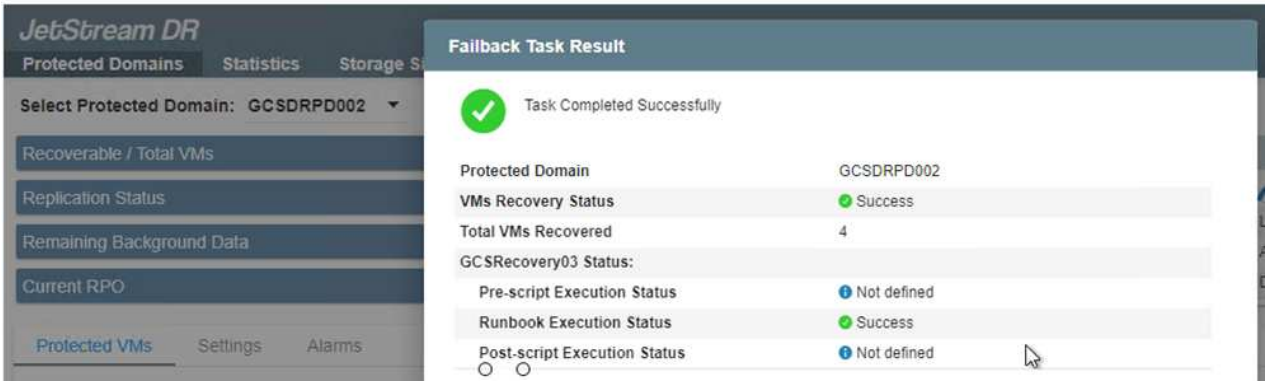
CPT によって生成されたフェイルバック プランは、VM とそのデータをオブジェクト ストアから元の VMware 環境に戻す作業を開始するためにも使用できます。



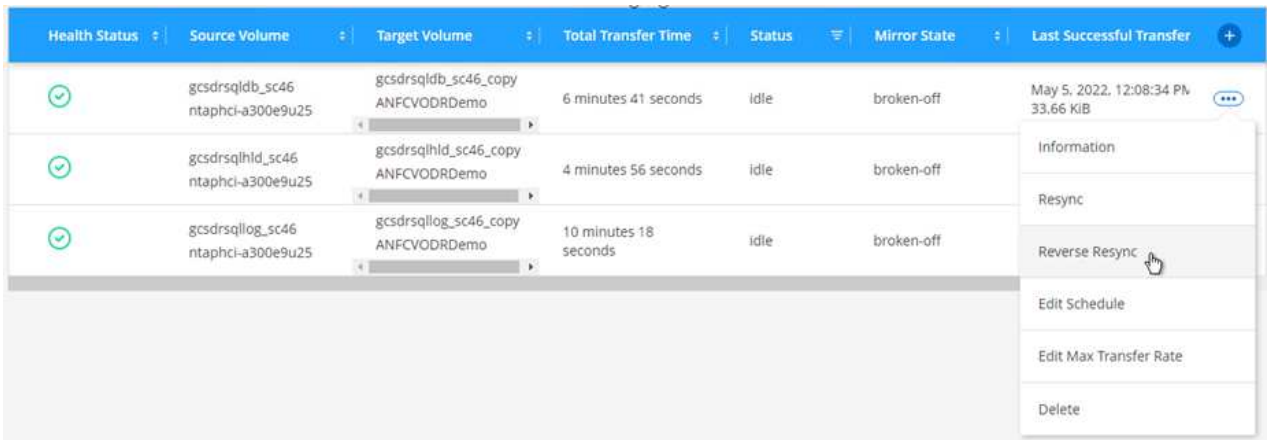
リカバリ サイトで VM を一時停止し、保護サイトで再起動した後の最大遅延を指定します。このプロセスを完了するために必要な時間には、フェールオーバー VM を停止した後のレプリケーションの完了、リカバリ サイトのクリーンアップに必要な時間、保護されたサイトで VM を再作成するために必要な時間が含まれます。 NetApp10 分を推奨します。

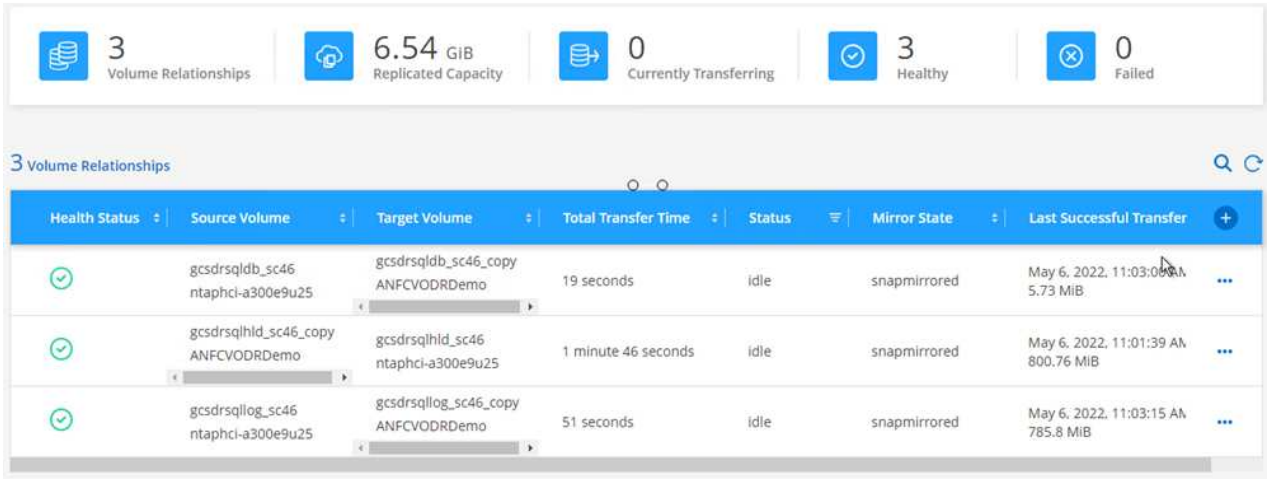


3. フェイルバック プロセスを完了し、VM 保護とデータの一貫性の再開を確認します。

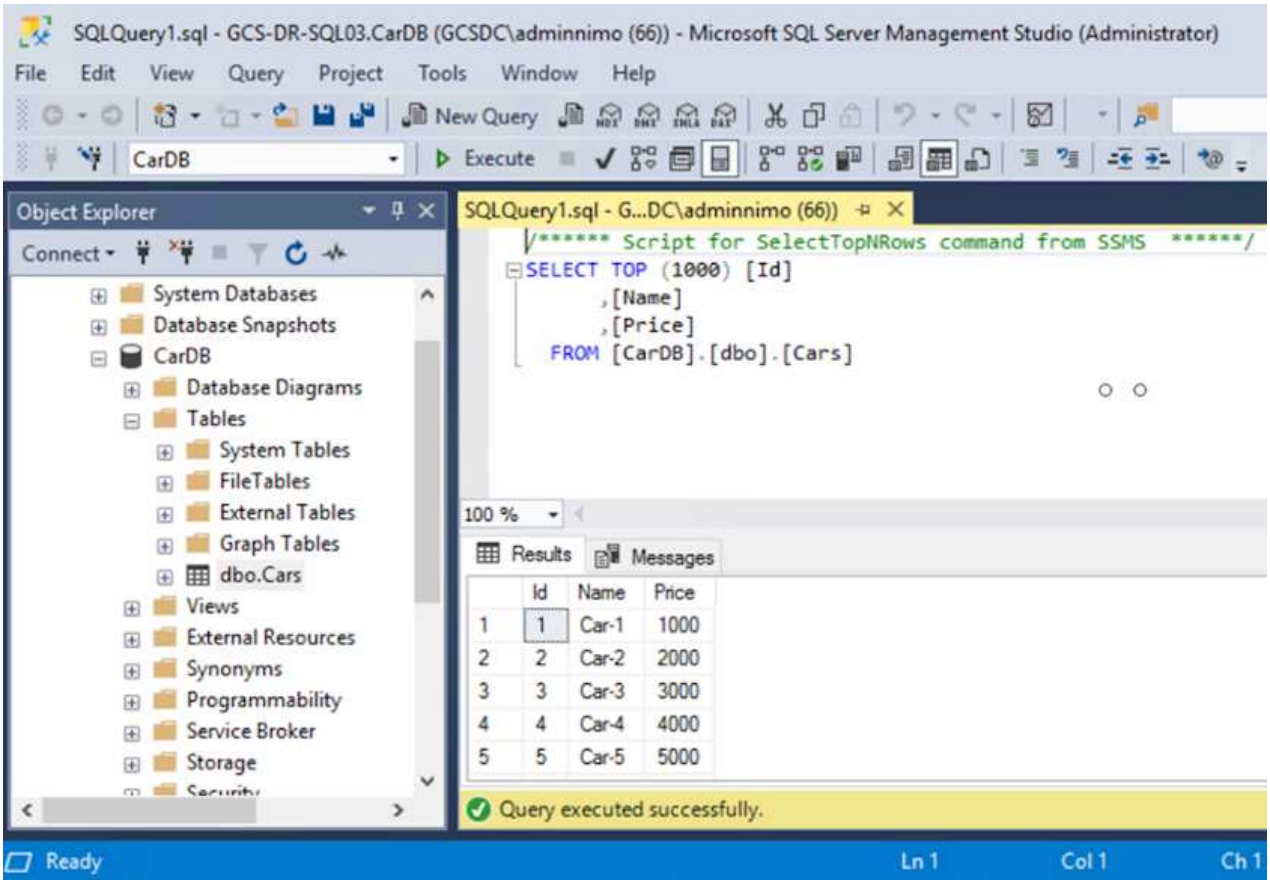


4. VM が回復したら、セカンダリ ストレージをホストから切断し、プライマリ ストレージに接続します。





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



プライマリ ストレージにフェイルバックするには、逆再同期操作を実行して、関係の方向がフェイルオーバー前と同じであることを確認します。

逆再同期操作後にプライマリ ストレージとセカンダリ ストレージの役割を保持するには、逆再同期操作を再度実行します。

このプロセスは、Oracle、同様のデータベース フレーバー、ゲスト接続ストレージを使用するその他の

アプリケーションなどにも適用できます。

いつものように、重要なワークロードを本番環境に移行する前に、その回復に必要な手順をテストします。

このソリューションの利点

- SnapMirrorの効率的で復元力のあるレプリケーションを使用します。
- ONTAPスナップショット保持を使用して、利用可能な任意の時点に回復します。
- ストレージ、コンピューティング、ネットワーク、アプリケーションの検証手順から、数百から数千の VM を復旧するために必要なすべての手順を完全に自動化できます。
- SnapCenter は、複製されたボリュームを変更しないクローン作成メカニズムを使用します。
  - これにより、ボリュームとスナップショットのデータ破損のリスクを回避できます。
  - DR テスト ワークフロー中のレプリケーションの中断を回避します。
  - 開発/テスト、セキュリティ テスト、パッチおよびアップグレード テスト、修復テストなど、DR 以外のワークフローに DR データを活用します。
- CPU と RAM の最適化により、より小規模なコンピューティング クラスターへのリカバリが可能になり、クラウド コストを削減できます。

著作権に関する情報

商標に関する情報