CVO 및 AVS(게스트 연결 스토리지)를 사용한 재해 복구

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

목차

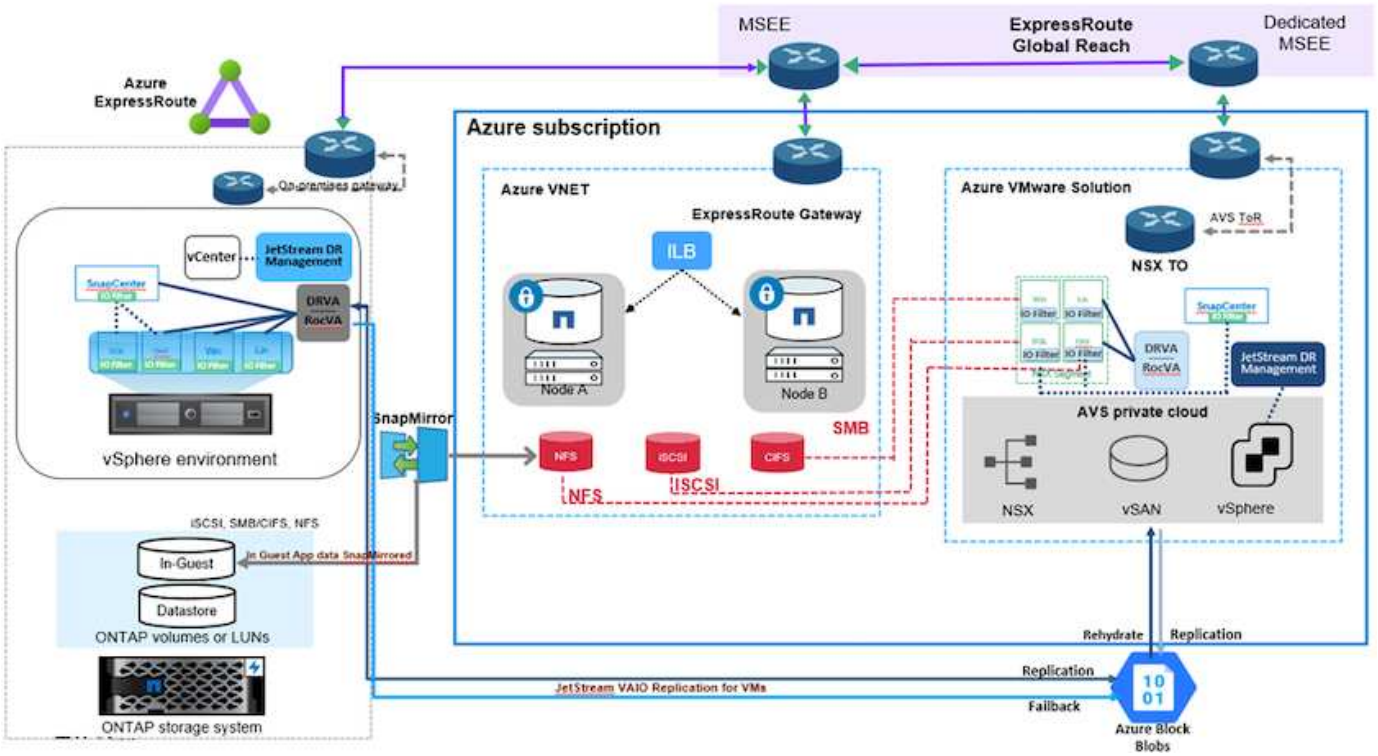
CVO 및 AVS(게스트 연결 스토리지)를 사용한 재해 복구

클라우드로 재해 복구를 수행하는 것은 랜섬웨어와 같은 사이트 중단 및 데이터 손상 사건으로부터 워크로드를 보호하는 탄력적이고 비용 효율적인 방법입니다. NetApp SnapMirror 사용하면 게스트 연결 스토리지를 사용하는 온프레미스 VMware 워크로드를 Azure에서 실행되는 NetApp Cloud Volumes ONTAP 으로 복제할 수 있습니다.

개요

```
 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.
```

이 문서에서는 NetApp SnapMirror, JetStream 및 Azure VMware 솔루션(AVS)을 사용하여 재해 복구를 설정하고 수행하기 위한 단계별 접근 방식을 제공합니다.



가정

이 문서는 애플리케이션 데이터를 위한 게스트 내부 스토리지(게스트 연결이라고도 함)에 초점을 맞추고 있으며, 온프레미스 환경에서는 애플리케이션과 일관된 백업을 위해 SnapCenter 사용한다고 가정합니다.

이 문서는 모든 타사 백업 또는 복구 솔루션에 적용됩니다. 환경에서 사용되는 솔루션에 따라 조직의 SLA를 충족하는 백업 정책을 만드는 모범 사례를 따르세요.

온-프레미스 환경과 Azure 가상 네트워크 간의 연결을 위해 Express Route Global Reach나 VPN 게이트웨이가 있는 가상 WAN을 사용하세요. 세그먼트는 온프레미스 vLAN 설계를 기반으로 만들어야 합니다.

온프레미스 데이터 센터를 Azure에 연결하는 데에는 여러 가지 옵션이 있으므로 이 문서에서는 구체적인 워크플로를 설명할 수 없습니다. 온-프레미스-Azure 연결 방법에 대한 자세한 내용은 Azure 설명서를 참조하세요.

DR 솔루션 배포

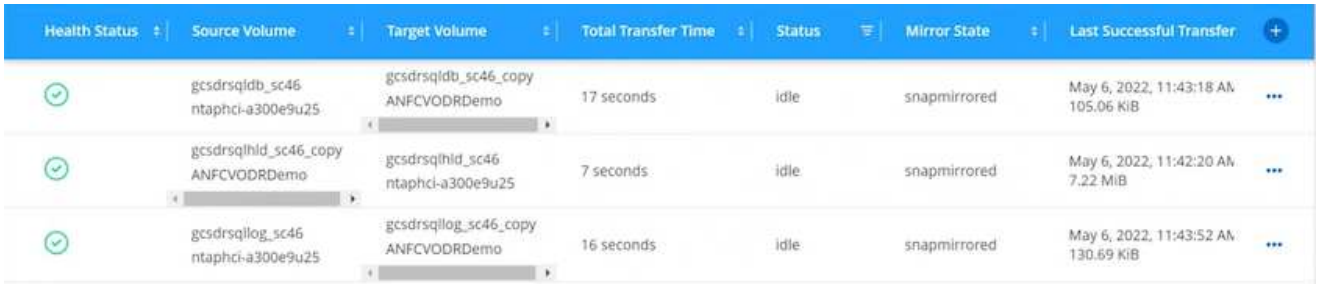
솔루션 배포 개요

1. SnapCenter 사용하여 필요한 RPO 요구 사항을 충족하는 애플리케이션 데이터를 백업하세요.
2. 적절한 구독 및 가상 네트워크 내에서 Cloud Manager를 사용하여 올바른 인스턴스 크기로 Cloud Volumes ONTAP 프로비저닝합니다.
   a. 해당 애플리케이션 볼륨에 맞게 SnapMirror 구성합니다.
   b. 예약된 작업 후 SnapMirror 업데이트를 트리거하도록 SnapCenter 의 백업 정책을 업데이트합니다.
3. 온프레미스 데이터 센터에 JetStream DR 소프트웨어를 설치하고 가상 머신에 대한 보호를 시작하세요.
4. Azure VMware Solution 프라이빗 클라우드에 JetStream DR 소프트웨어를 설치합니다.
5. 재해 발생 시 Cloud Manager를 사용하여 SnapMirror 관계를 끊고 가상 머신의 장애 조치를 지정된 AVS DR 사이트의 Azure NetApp Files 또는 vSAN 데이터 저장소로 트리거합니다.
   a. 애플리케이션 VM에 대한 ISCSI LUN과 NFS 마운트를 다시 연결합니다.
6. 기본 사이트가 복구된 후 SnapMirror 역방향으로 재동기화하여 보호된 사이트로 장애 복구를 호출합니다.

배포 세부 정보

Azure에서 **CVO**를 구성하고 볼륨을 **CVO**에 복제합니다**.**

첫 번째 단계는 Azure에서 Cloud Volumes ONTAP 구성하는 것입니다."링크") 원하는 빈도와 스냅샷 보존 기간을 설정하여 원하는 볼륨을 Cloud Volumes ONTAP 에 복제합니다.



AVS 호스트 및 **CVO** 데이터 액세스 구성

SDDC를 배포할 때 고려해야 할 두 가지 중요한 요소는 Azure VMware 솔루션의 SDDC 클러스터 크기와 SDDC를 서비스에서 유지하는 기간입니다. 재해 복구 솔루션에 대한 이 두 가지 주요 고려 사항은 전반적인 운영 비용을 줄이는 데 도움이 됩니다. SDDC는 최소 3개의 호스트로 구성될 수 있으며, 전체 규모로 배포하면 다중 호스트 클러스터까지 가능합니다.

AVS 클러스터를 배포하기로 결정하는 것은 주로 RPO/RTO 요구 사항을 기준으로 합니다. Azure VMware 솔루션을 사용하면 테스트나 실제 재해 발생에 대비하여 SDDC를 적시에 프로비저닝할 수 있습니다. 재해 발생 시가 아닌 시기에 구축된 SDDC는 ESXi 호스트 비용을 절감해줍니다. 그러나 이러한 배포 방식은 SDDC가 프로비저닝되는 동안 RTO에 몇 시간 정도 영향을 미칩니다.

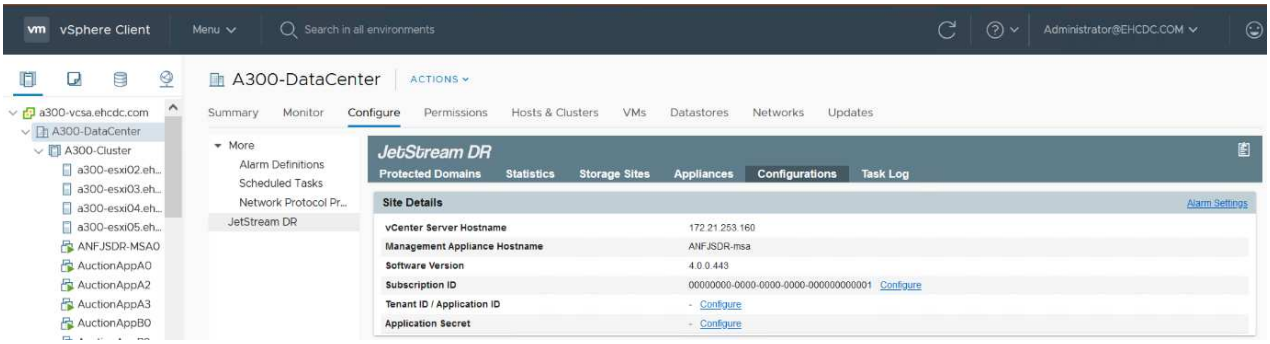
가장 일반적으로 사용되는 배포 옵션은 SDDC를 항상 켜진 조종등 모드로 실행하는 것입니다. 이 옵션은 항상 사용 가능한 세 개의 호스트라는 작은 공간을 제공하고, 시뮬레이션 활동과 규정 준수 검사를 위한 실행 기준을 제공하여 복구 작업 속도를 높여 운영 사이트와 DR 사이트 간의 운영 차이로 인한 위험을 방지합니다. 파일럿 라이트 클러스터는 실제 DR 이벤트를 처리하는 데 필요한 경우 원하는 수준까지 빠르게 확장할 수 있습니다.

AVS SDDC를 구성하려면(주문형 또는 조종등 모드) 다음을 참조하세요."Azure에서 가상화 환경 배포 및 구성" . 전제 조건으로, 연결이 설정된 후 AVS 호스트에 있는 게스트 VM이 Cloud Volumes ONTAP 의 데이터를 사용할 수 있는지 확인합니다.

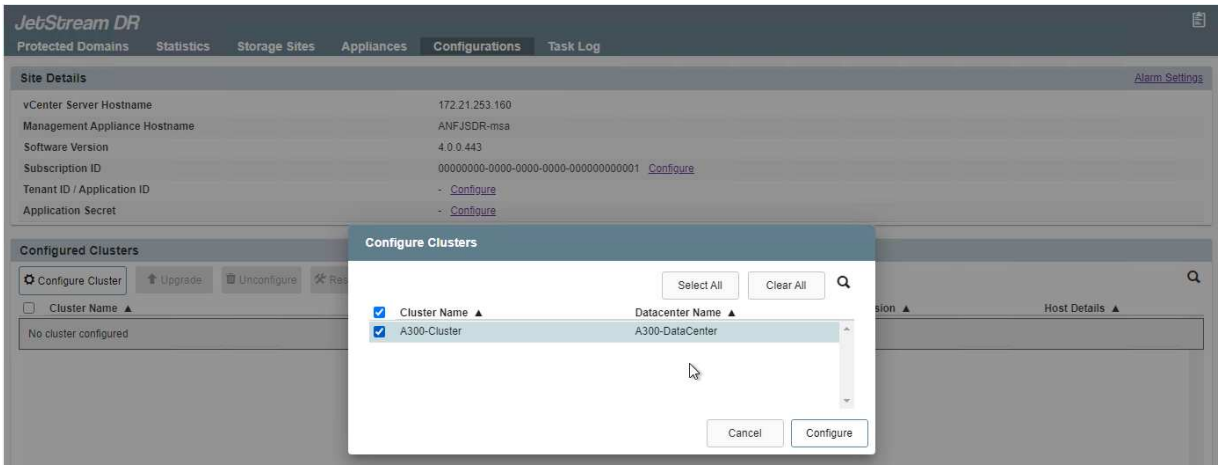
Cloud Volumes ONTAP 과 AVS가 올바르게 구성된 후 VAIO 메커니즘을 사용하고 SnapMirror 활용하여 애플리케이션 볼륨을 Cloud Volumes ONTAP에 복사하여 온프레미스 워크로드를 AVS(애플리케이션 VMDK가 있는 VM 및 게스트 스토리지가 있는 VM)로 복구하는 작업을 자동화하도록 Jetstream을 구성하기 시작 Cloud Volumes ONTAP.

JetStream DR 소프트웨어는 JetStream DR 관리 서버 가상 어플라이언스(MSA), DR 가상 어플라이언스(DRVA), 호스트 구성 요소(I/O 필터 패키지)의 세 가지 주요 구성 요소로 구성됩니다. MSA는 컴퓨팅 클러스터에 호스트 구성 요소를 설치하고 구성한 다음 JetStream DR 소프트웨어를 관리하는 데 사용됩니다. 설치 과정은 다음과 같습니다.

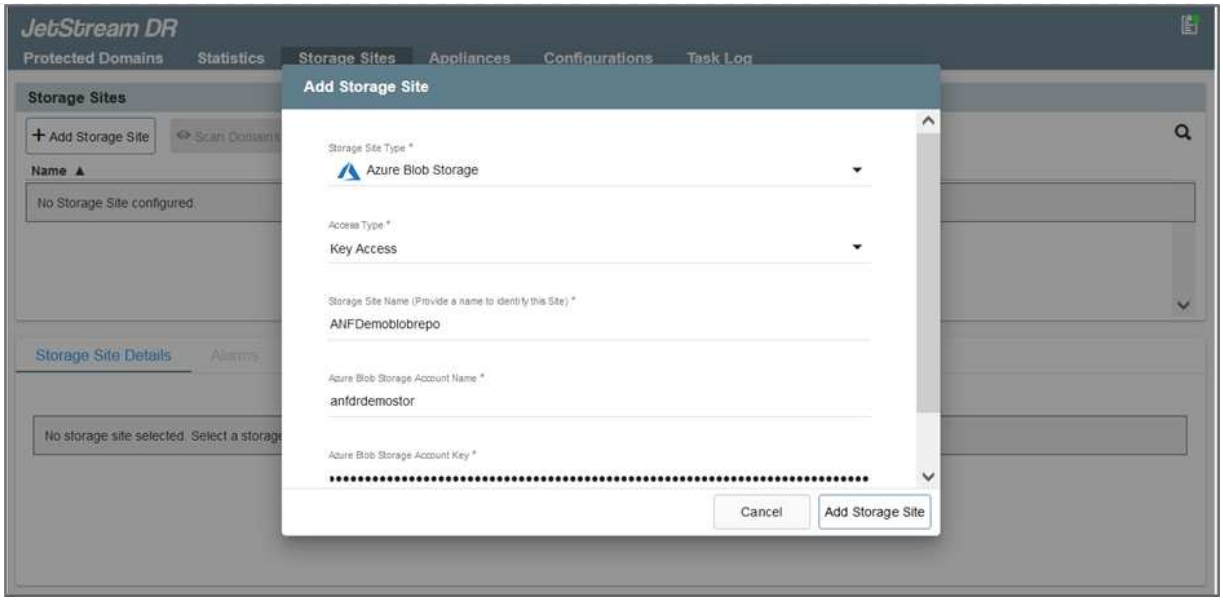
1. 필수 조건을 확인하세요.
2. 리소스 및 구성 권장 사항을 보려면 용량 계획 도구를 실행하세요.
3. 지정된 클러스터의 각 vSphere 호스트에 JetStream DR MSA를 배포합니다.
4. 브라우저에서 DNS 이름을 사용하여 MSA를 시작합니다.
5. MSA에 vCenter 서버를 등록합니다.
6. JetStream DR MSA가 배포되고 vCenter Server가 등록된 후 vSphere Web Client를 사용하여 JetStream DR 플러그인으로 이동합니다. 데이터 센터 > 구성 > JetStream DR로 이동하여 이 작업을 수행할 수 있습니다.



7. JetStream DR 인터페이스에서 다음 작업을 완료하세요.
   a. I/O 필터 패키지로 클러스터를 구성합니다.

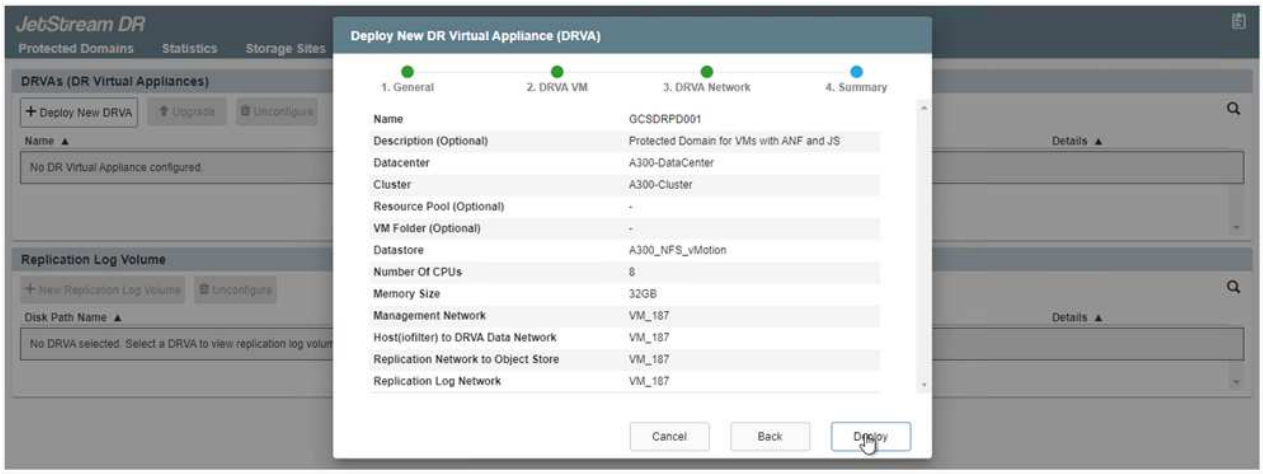


   b. 복구 사이트에 있는 Azure Blob 저장소를 추가합니다.

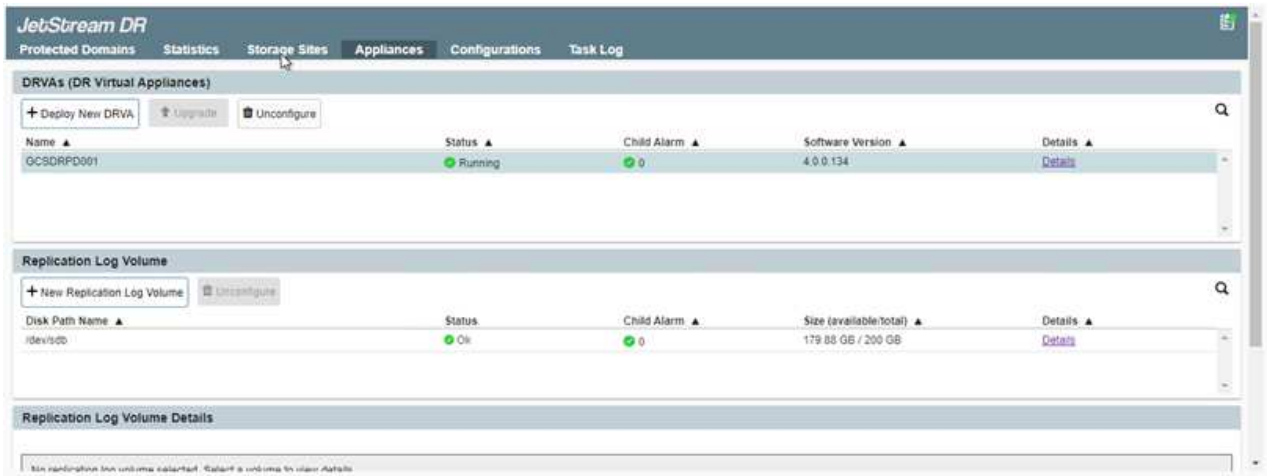


8. 어플라이언스 탭에서 필요한 수의 DR 가상 어플라이언스(DRVA)를 배포합니다.

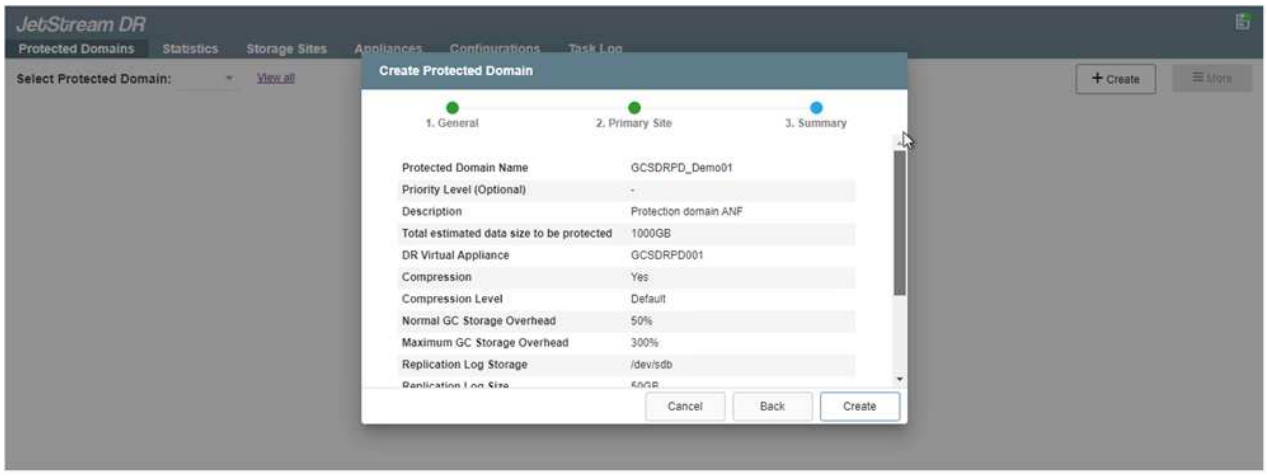
   용량 계획 도구를 사용하여 필요한 DRVA 수를 추정합니다.

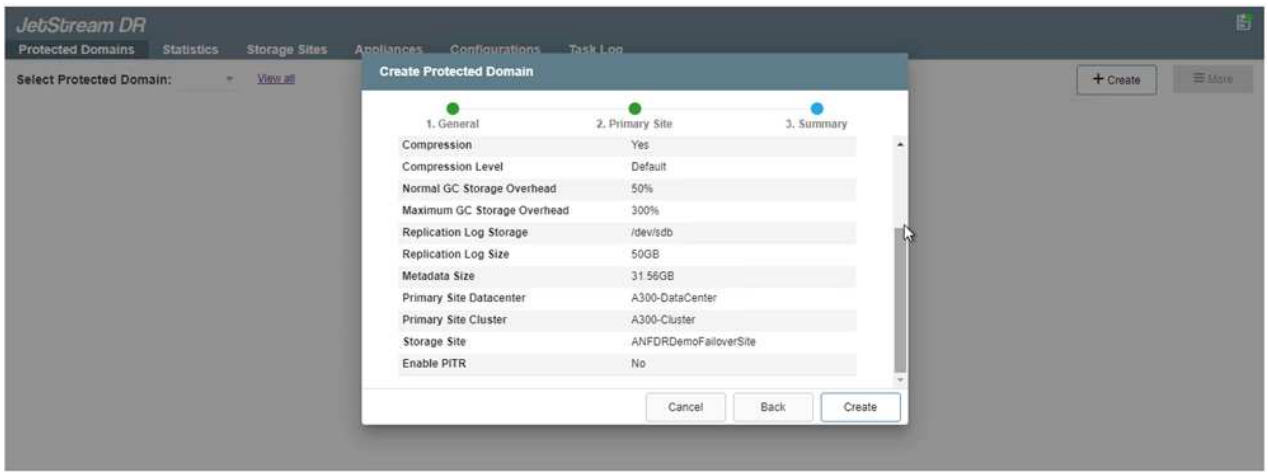


9. 사용 가능한 데이터 저장소나 독립적인 공유 iSCSI 스토리지 풀의 VMDK를 사용하여 각 DRVA에 대한 복제 로그 볼륨을 생성합니다.



10. 보호된 도메인 탭에서 Azure Blob Storage 사이트, DRVA 인스턴스 및 복제 로그에 대한 정보를 사용하여 필요한 수의 보호된 도메인을 만듭니다. 보호된 도메인은 클러스터 내에서 함께 보호되고 장애 조치/장애 복구 작업에 대한 우선 순위가 지정된 특정 VM 또는 애플리케이션 VM 세트를 정의합니다.

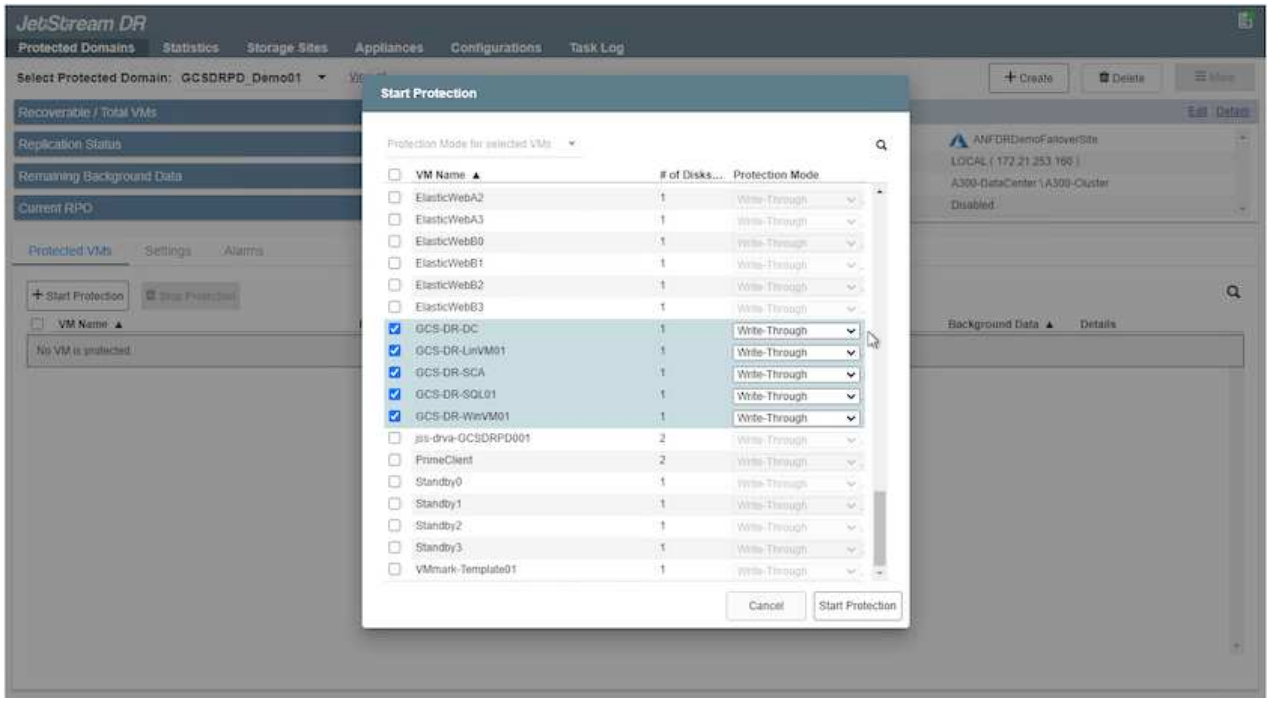




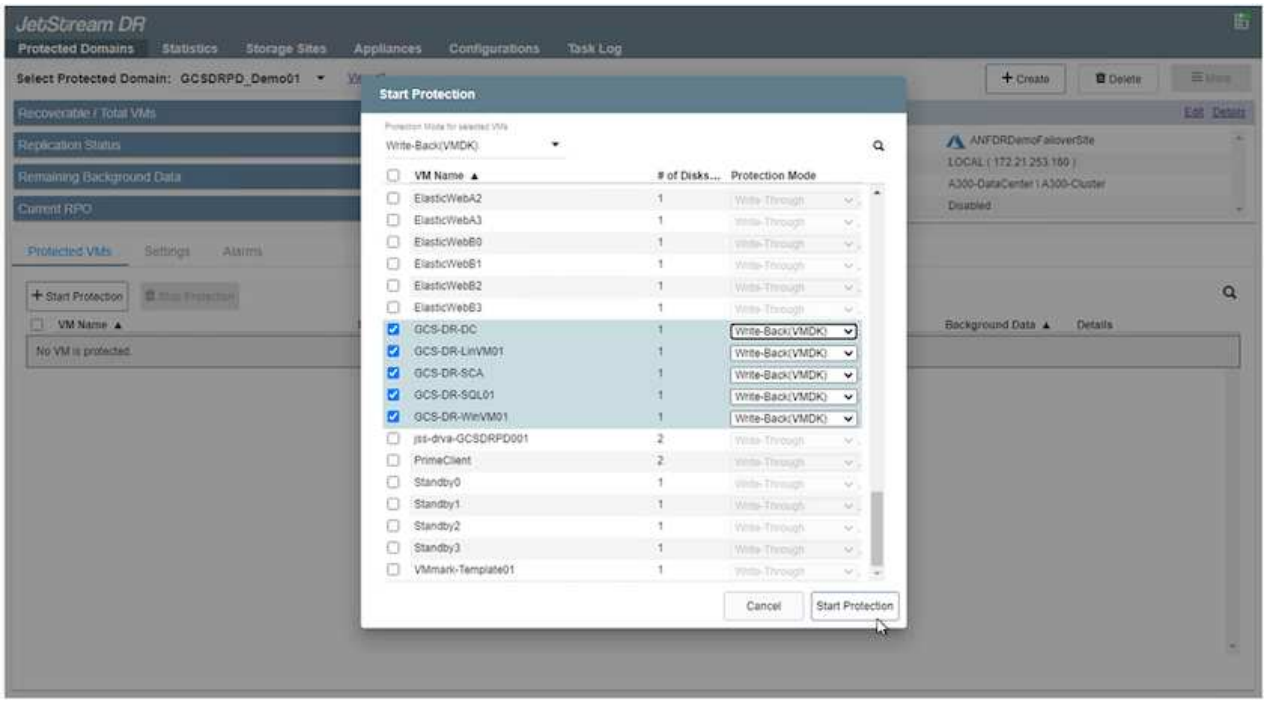
11. 보호할 VM을 선택하고 종속성에 따라 VM을 애플리케이션 그룹으로 그룹화합니다. 애플리케이션 정의를 사용하면 VM 세트를 부팅 순서, 부팅 지연, 복구 시 실행할 수 있는 선택적 애플리케이션 유효성 검사 등을 포함하는 논리적 그룹으로 그룹화할 수 있습니다.

보호된 도메인의 모든 VM에 동일한 보호 모드가 사용되는지 확인하세요.

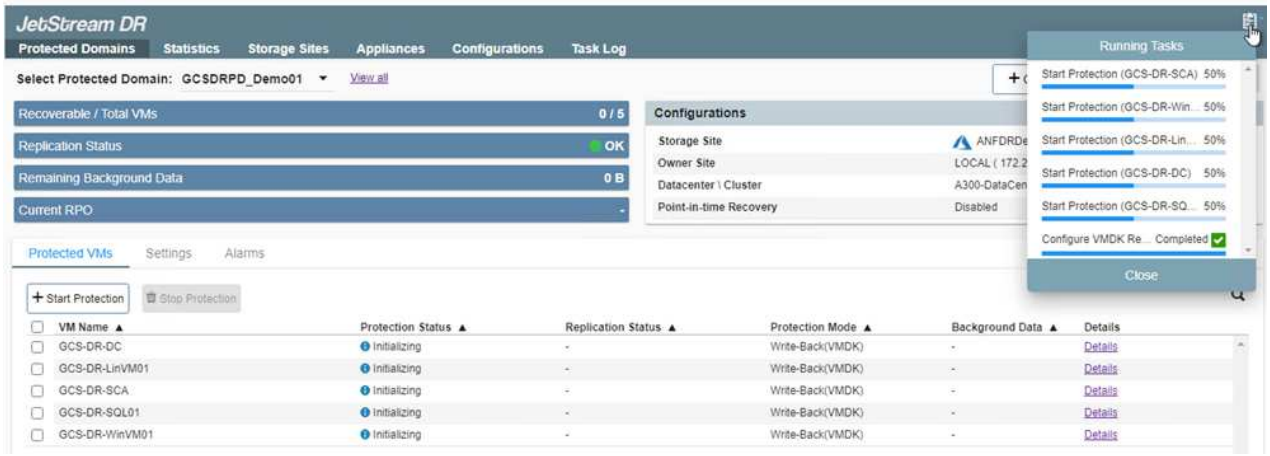
Write-Back(VMDK) 모드는 더 높은 성능을 제공합니다.



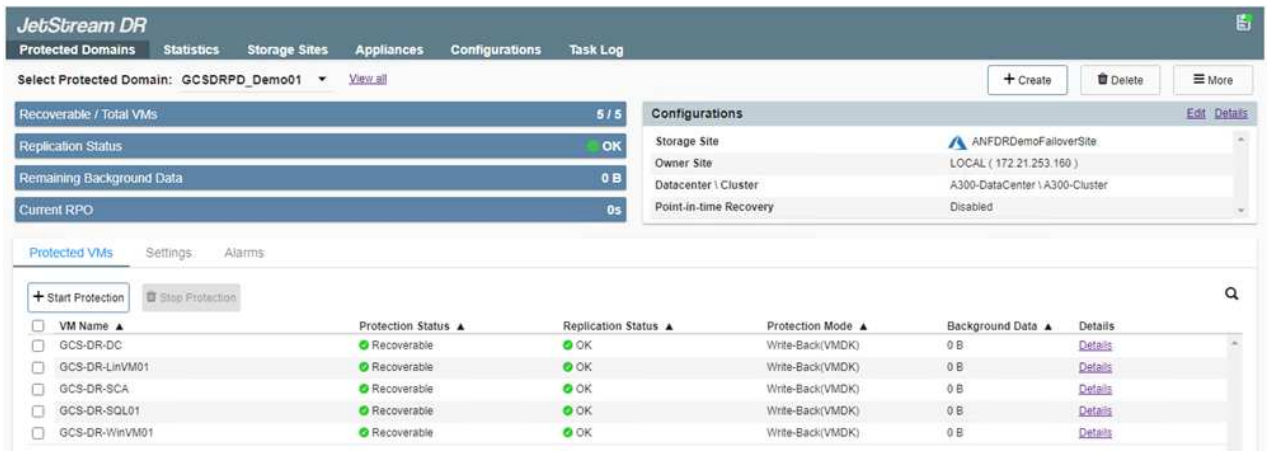
12. 복제 로그 볼륨이 고성능 스토리지에 배치되었는지 확인하세요.



13. 완료되면 보호된 도메인에 대한 보호 시작을 클릭합니다. 이렇게 하면 선택한 VM에 대한 데이터 복제가 지정된 Blob 저장소로 시작됩니다.



14. 복제가 완료되면 VM 보호 상태가 복구 가능으로 표시됩니다.

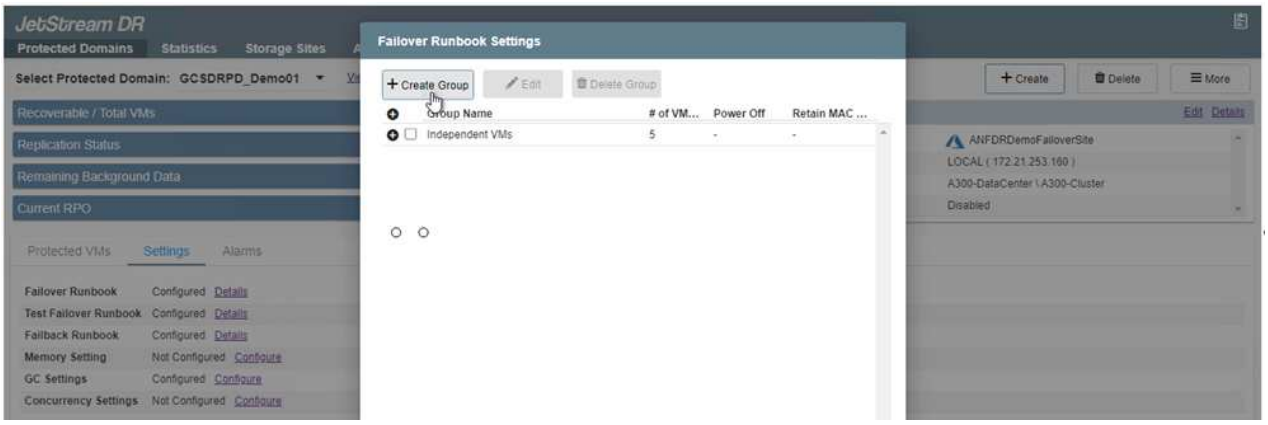


장애 조치 런북은 VM을 그룹화(복구 그룹이라고 함), 부팅 순서 순서를 설정하고 IP 구성과 함께 CPU/메모리 설정을 수정하도록 구성할 수 있습니다.

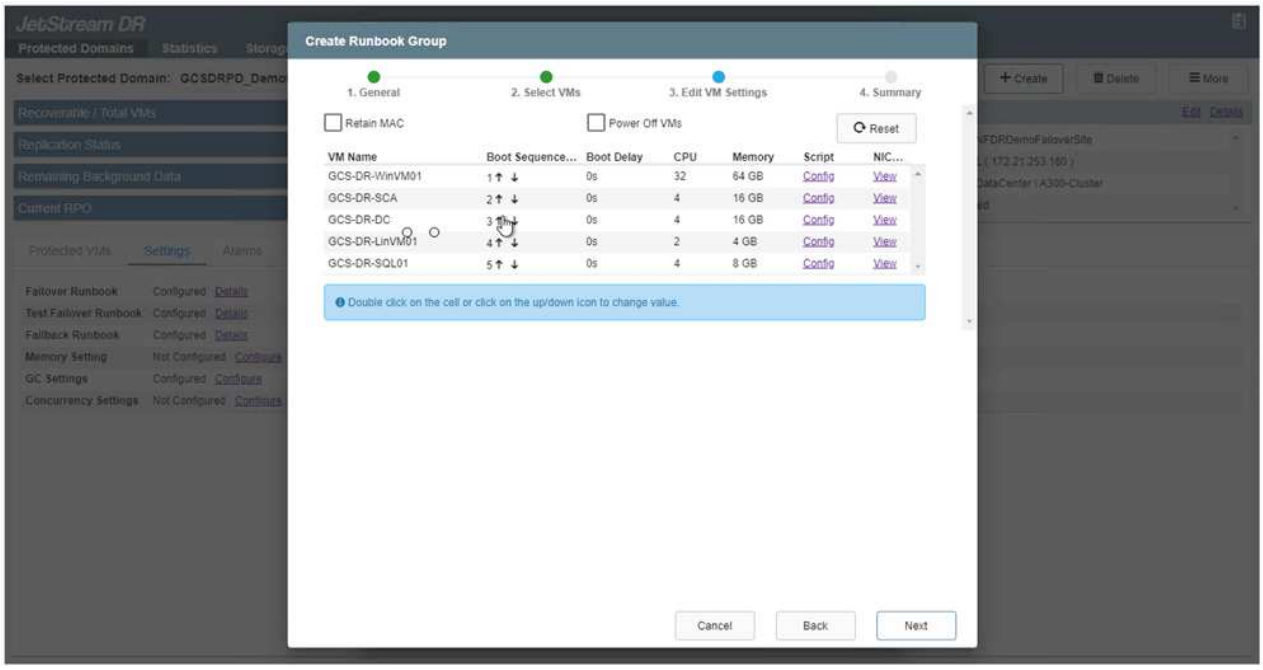
15. 설정을 클릭한 다음 런북 구성 링크를 클릭하여 런북 그룹을 구성합니다.

16. 그룹 만들기 버튼을 클릭하여 새로운 런북 그룹을 만듭니다.

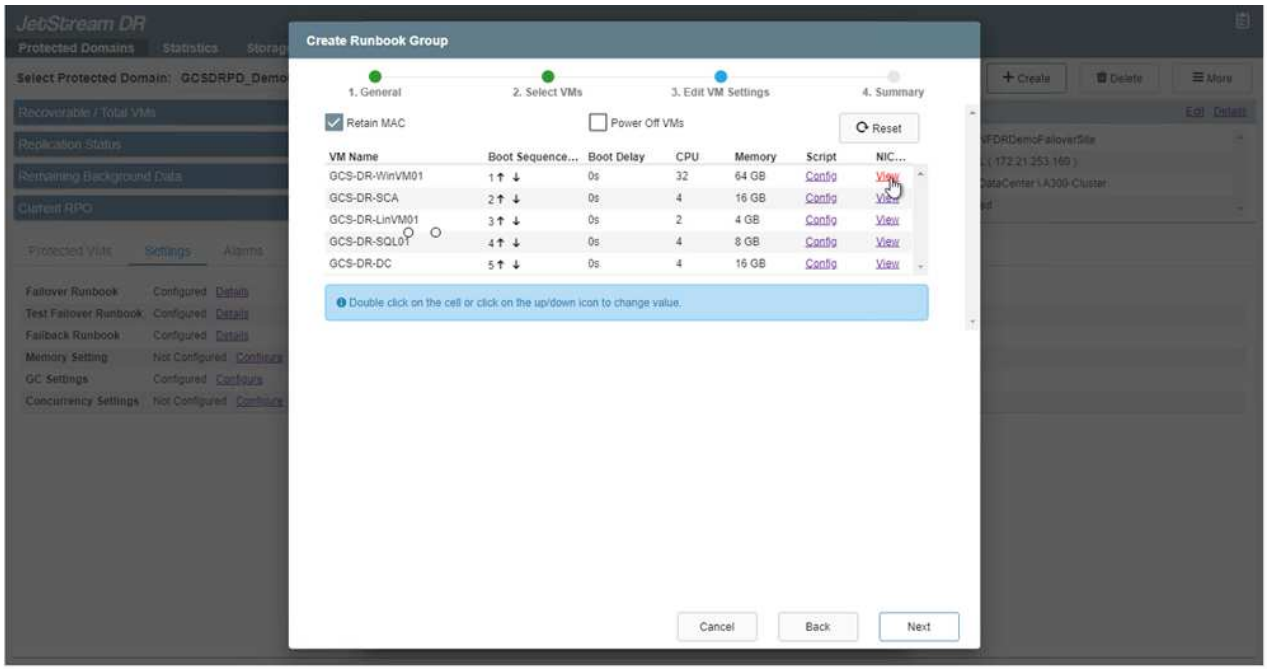
필요한 경우 화면 하단에서 사용자 지정 사전 스크립트와 사후 스크립트를 적용하여 런북 그룹의 작업 전과 후에 자동으로 실행합니다. Runbook 스크립트가 관리 서버에 있는지 확인하세요.



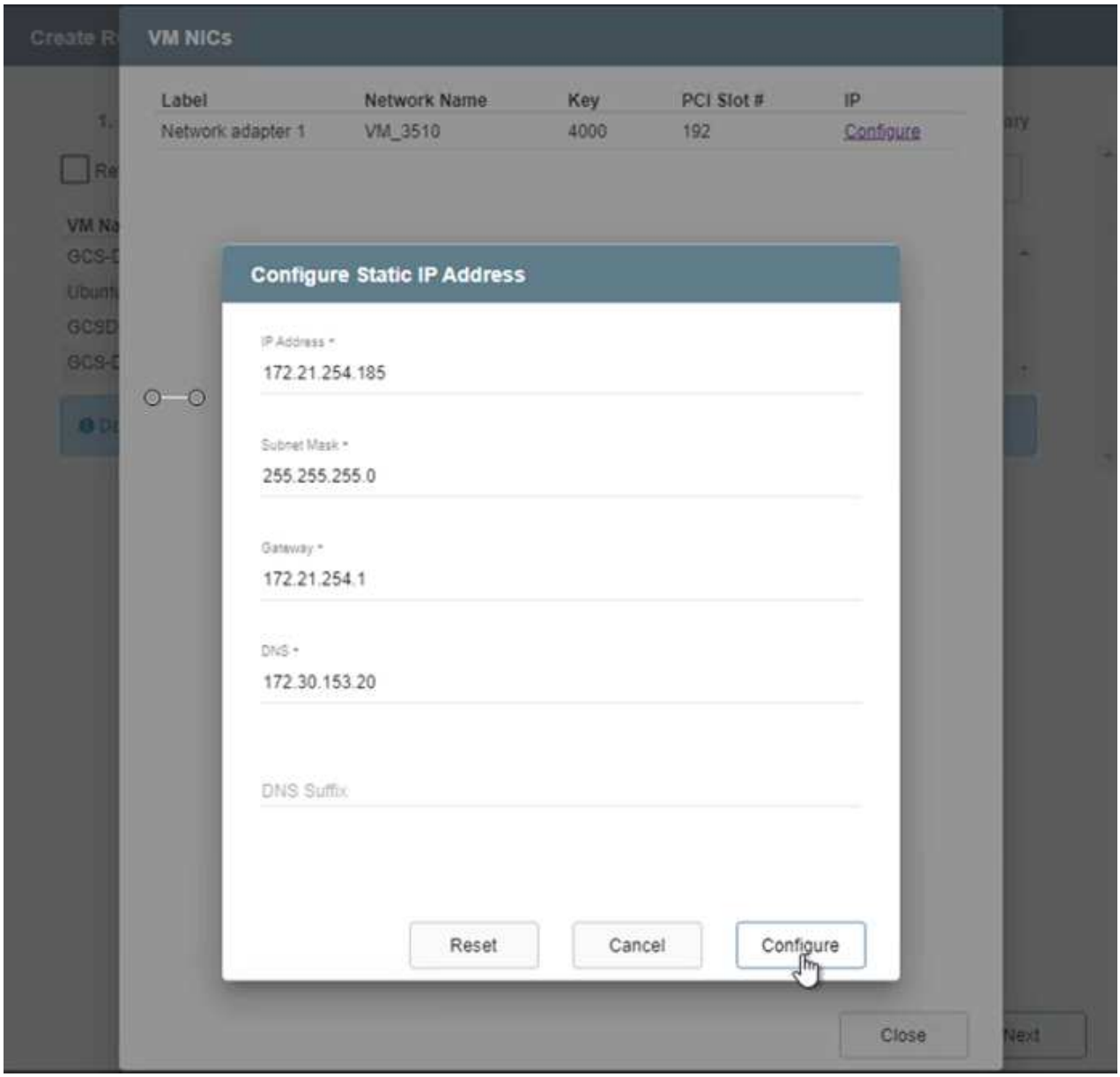
17. 필요에 따라 VM 설정을 편집합니다. 부팅 순서, 부팅 지연(초 단위), CPU 수, 할당할 메모리 양 등 VM 복구에 필요한 매개변수를 지정합니다. 위쪽 또는 아래쪽 화살표를 클릭하여 VM의 부팅 순서를 변경합니다. MAC을 유지하기 위한 옵션도 제공됩니다.

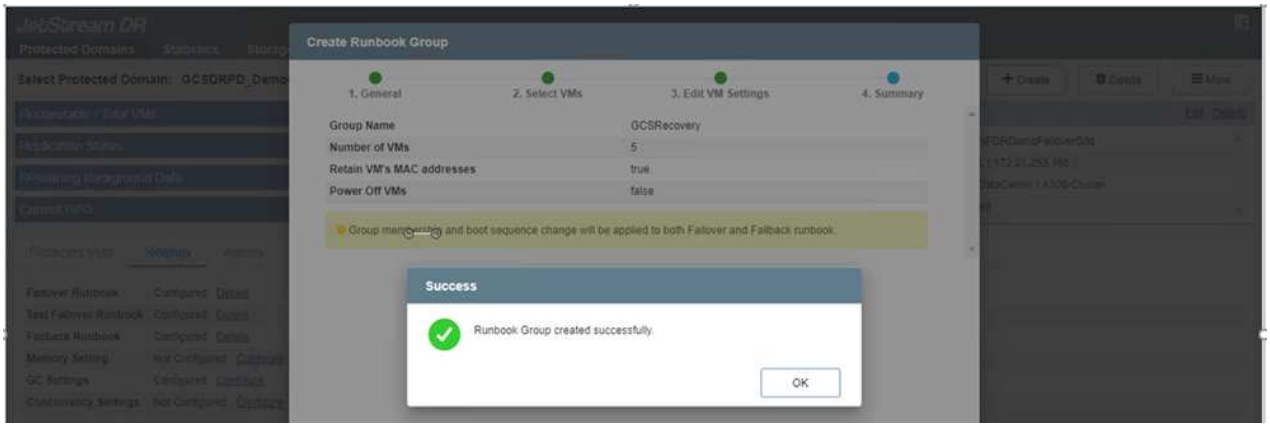


18. 고정 IP 주소는 그룹의 개별 VM에 대해 수동으로 구성할 수 있습니다. VM의 NIC 보기 링크를 클릭하여 IP 주소 설정을 수동으로 구성합니다.



19. 구성 버튼을 클릭하여 각 VM에 대한 NIC 설정을 저장합니다.





이제 장애 조치(failover) 및 장애 복구(failback) 런북의 상태가 모두 구성됨으로 나열됩니다. 장애 조치(failover) 및 장애 복구(failback) 런북 그룹은 동일한 초기 VM 그룹과 설정을 사용하여 쌍으로 생성됩니다. 필요한 경우, 각각의 '세부 정보' 링크를 클릭하고 변경하여 런북 그룹의 설정을 개별적으로 사용자 지정할 수 있습니다.

복구 사이트(AVS)의 모범 사례는 미리 3노드 파일럿 라이트 클러스터를 만드는 것입니다. 이를 통해 다음을 포함하여 복구 사이트 인프라를 미리 구성할 수 있습니다.

- 목적지 네트워킹 세그먼트, 방화벽, DHCP 및 DNS와 같은 서비스 등
- AVS용 JetStream DR 설치
- ANF 볼륨을 데이터 저장소 등으로 구성

JetStream DR은 미션 크리티컬 도메인에 대해 거의 0에 가까운 RTO 모드를 지원합니다. 이러한 도메인의 경우 대상 저장소가 미리 설치되어야 합니다. 이 경우에는 ANF가 권장되는 저장 유형입니다.

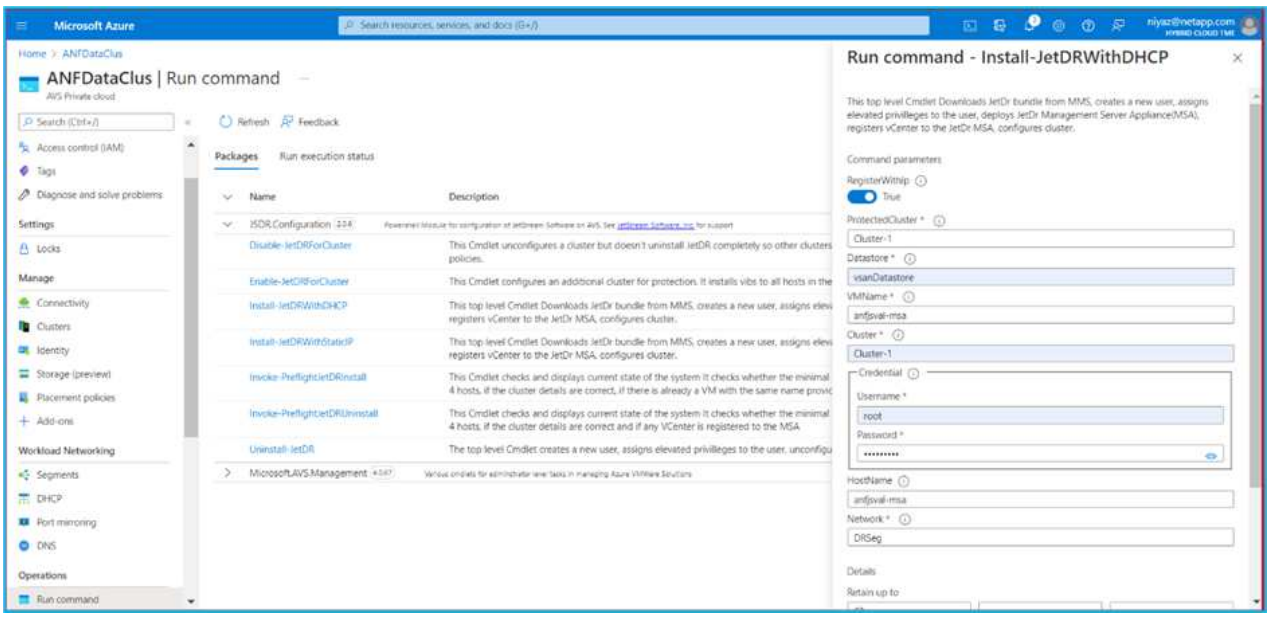
세그먼트 생성을 포함한 네트워크 구성은 온프레미스 요구 사항에 맞게 AVS 클러스터에서 구성되어야 합니다.

SLA 및 RTO 요구 사항에 따라 지속적인 장애 조치 또는 일반(표준) 장애 조치 모드를 사용할 수 있습니다. RTO가 거의 0에 가까우면 회복 부위부터 지속적인 수분 보충을 시작해야 합니다.

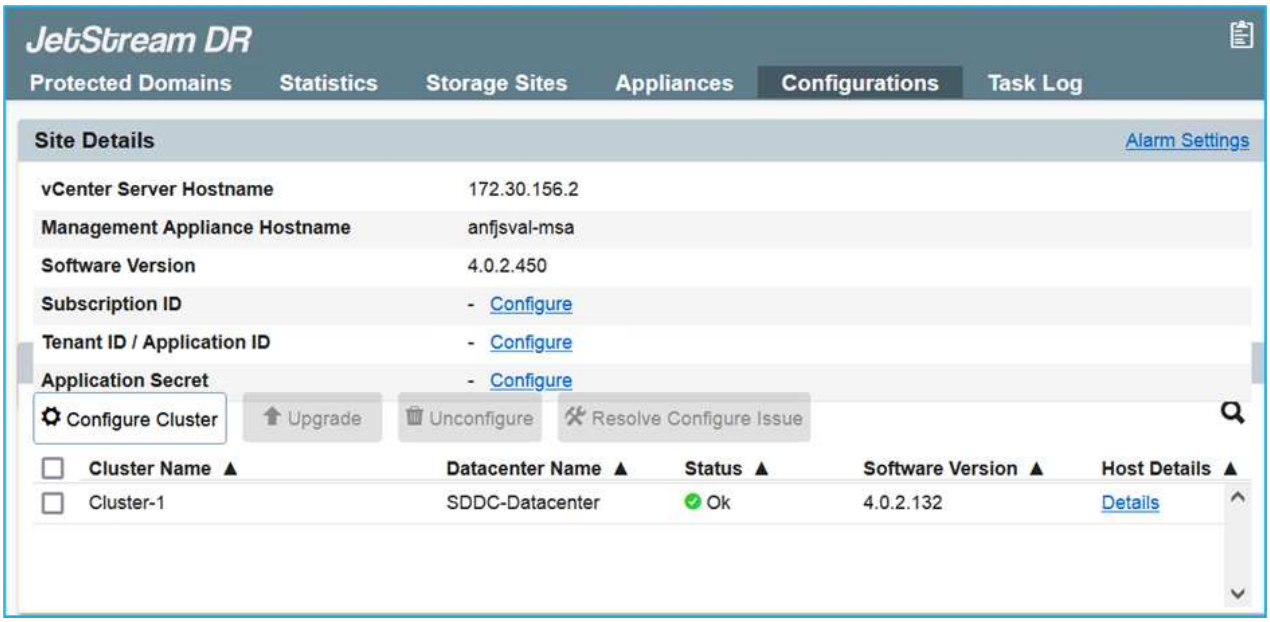
1. Azure VMware Solution 프라이빗 클라우드에 AVS용 JetStream DR을 설치하려면 실행 명령을 사용하세요. Azure Portal에서 Azure VMware 솔루션으로 이동하여 프라이빗 클라우드를 선택하고 명령 실행 > 패키지 > JSDR.Configuration을 선택합니다.

   Azure VMware Solution의 기본 CloudAdmin 사용자에게는 AVS용 JetStream DR을 설치할 수 있는 권한이 없습니다. Azure VMware Solution을 사용하면 JetStream DR에 대한 Azure VMware Solution 실행 명령을 호출하여 JetStream DR을 간단하고 자동으로 설치할 수 있습니다.

   다음 스크린샷은 DHCP 기반 IP 주소를 사용하여 설치하는 방법을 보여줍니다.



2. AVS용 JetStream DR 설치가 완료되면 브라우저를 새로 고칩니다. JetStream DR UI에 액세스하려면 SDDC 데이터센터 > 구성 > JetStream DR로 이동하세요.

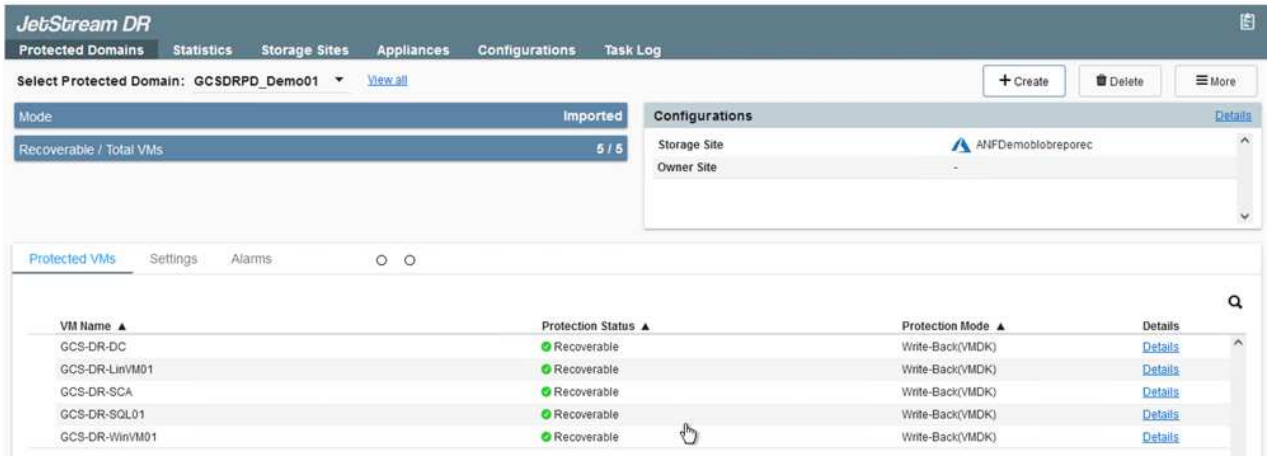


3. JetStream DR 인터페이스에서 다음 작업을 완료하세요.

   a. 온-프레미스 클러스터를 스토리지 사이트로 보호하는 데 사용된 Azure Blob Storage 계정을 추가한 다음 도메인 검사 옵션을 실행합니다.

   b. 나타나는 팝업 대화 상자에서 가져올 보호된 도메인을 선택한 다음 가져오기 링크를 클릭합니다.

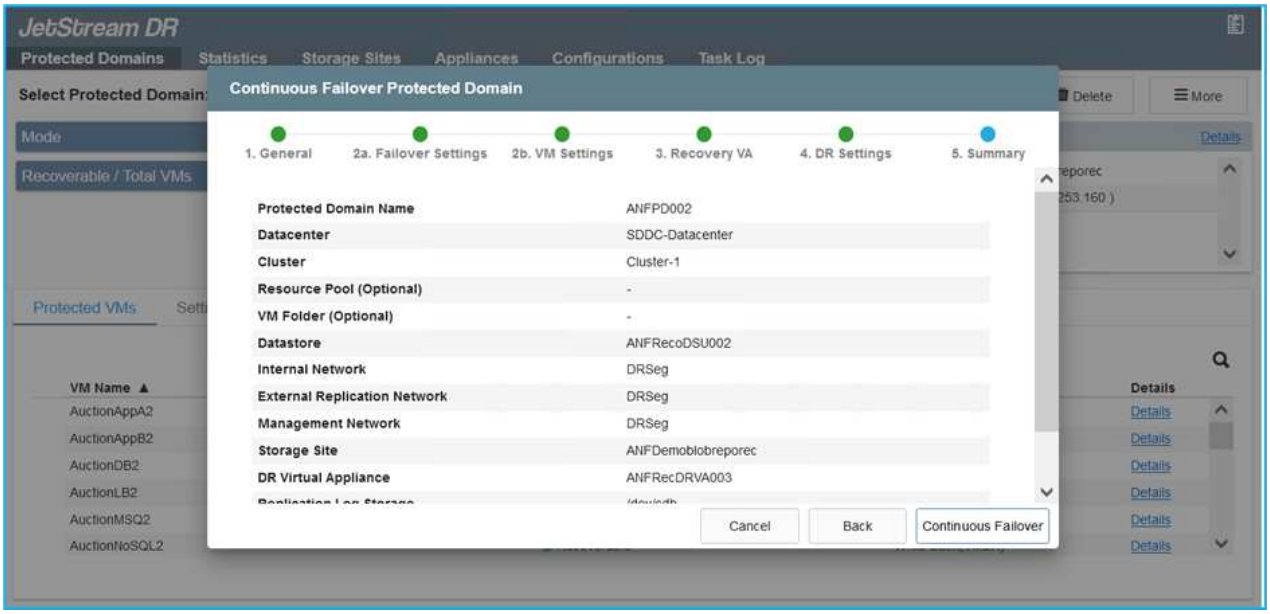
4. 도메인을 복구를 위해 가져왔습니다. 보호된 도메인 탭으로 이동하여 원하는 도메인이 선택되었는지 확인하거나 보호된 도메인 선택 메뉴에서 원하는 도메인을 선택합니다. 보호된 도메인에서 복구 가능한 VM 목록이 표시됩니다.



5. 보호된 도메인을 가져온 후 DRVA 어플라이언스를 배포합니다.

   이러한 단계는 CPT에서 만든 계획을 사용하여 자동화할 수도 있습니다.

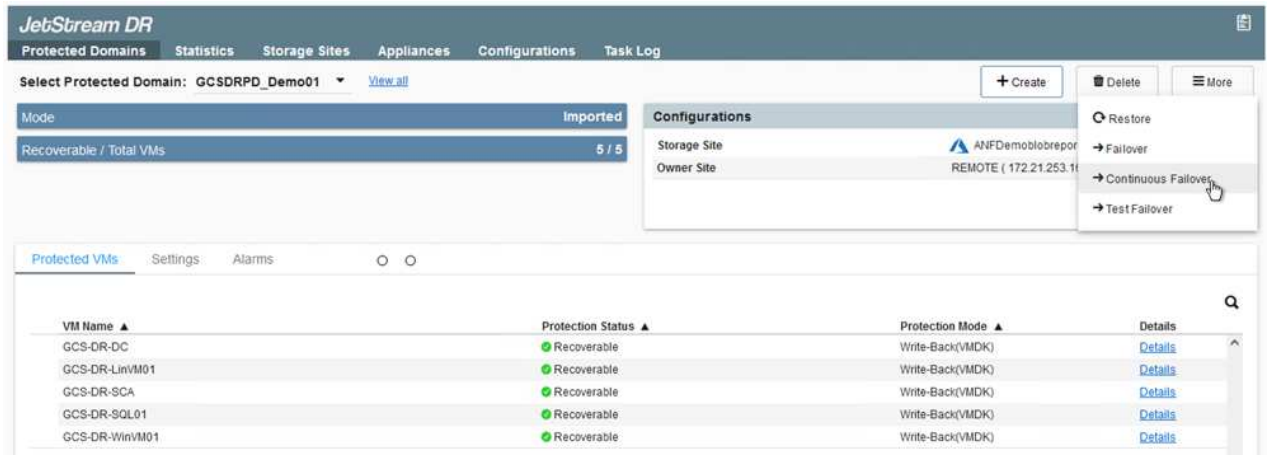
6. 사용 가능한 vSAN 또는 ANF 데이터 저장소를 사용하여 복제 로그 볼륨을 생성합니다.
7. 보호된 도메인을 가져오고 VM 배치에 ANF 데이터 저장소를 사용하도록 복구 VA를 구성합니다.



선택한 세그먼트에서 DHCP가 활성화되어 있고 충분한 IP를 사용할 수 있는지 확인하세요. 도메인이 복구되는 동안 동적 IP가 일시적으로 사용됩니다. 복구 중인 각 VM(지속적인 재수화 포함)에는 개별 동적 IP가 필요합니다. 복구가 완료되면 IP가 해제되어 재사용될 수 있습니다.

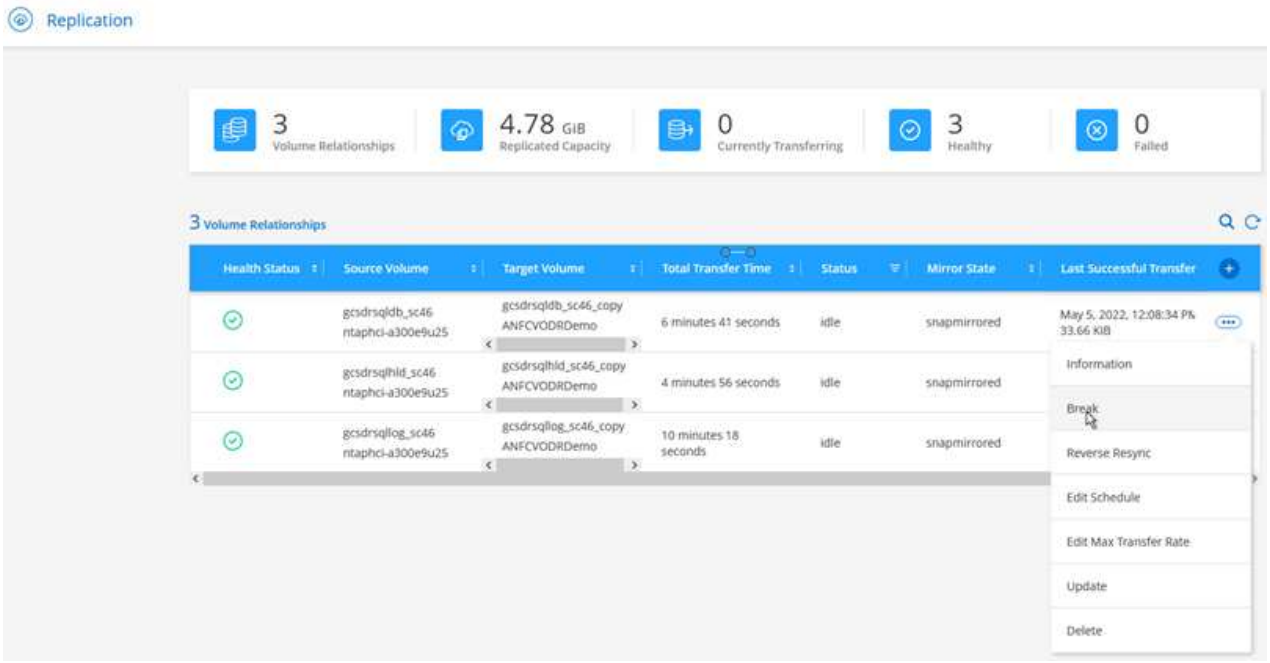
8. 적절한 장애 조치 옵션(지속적인 장애 조치 또는 장애 조치)을 선택합니다. 이 예에서는 연속 재수화(연속 장애 조치)가 선택되었습니다.

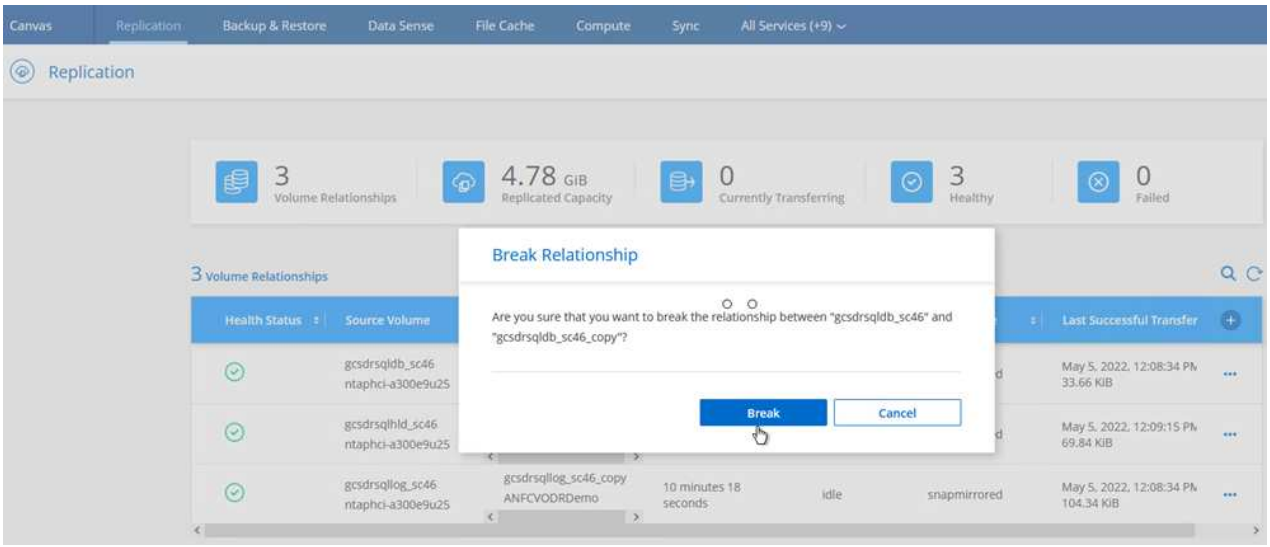
연속 장애 조치와 장애 조치 모드는 구성을 수행하는 시점에 따라 다르지만 두 장애 조치 모드는 모두 동일한 단계를 사용하여 구성됩니다. 재해 발생 시 대응하기 위해 장애 조치 단계가 함께 구성되고 수행됩니다. 지속적인 장애 조치는 언제든지 구성될 수 있으며, 정상적인 시스템 작동 중에 백그라운드에서 실행되도록 허용될 수 있습니다. 재해가 발생한 후에는 지속적인 장애 조치가 완료되어 보호된 VM의 소유권이 즉시 복구 사이트로 이전됩니다 (RTO가 거의 0에 가까움).



지속적인 장애 조치 프로세스가 시작되고, UI에서 진행 상황을 모니터링할 수 있습니다. 현재 단계 섹션의 파란색 아이콘을 클릭하면 장애 조치 프로세스의 현재 단계에 대한 세부 정보를 보여주는 팝업 창이 나타납니다.

1. 온프레미스 환경의 보호된 클러스터에서 재해(부분적 또는 완전한 장애)가 발생한 후에는 해당 애플리케이션 볼륨에 대한 SnapMirror 관계를 끊은 후 Jetstream을 사용하여 VM에 대한 장애 조치를 트리거할 수 있습니다.

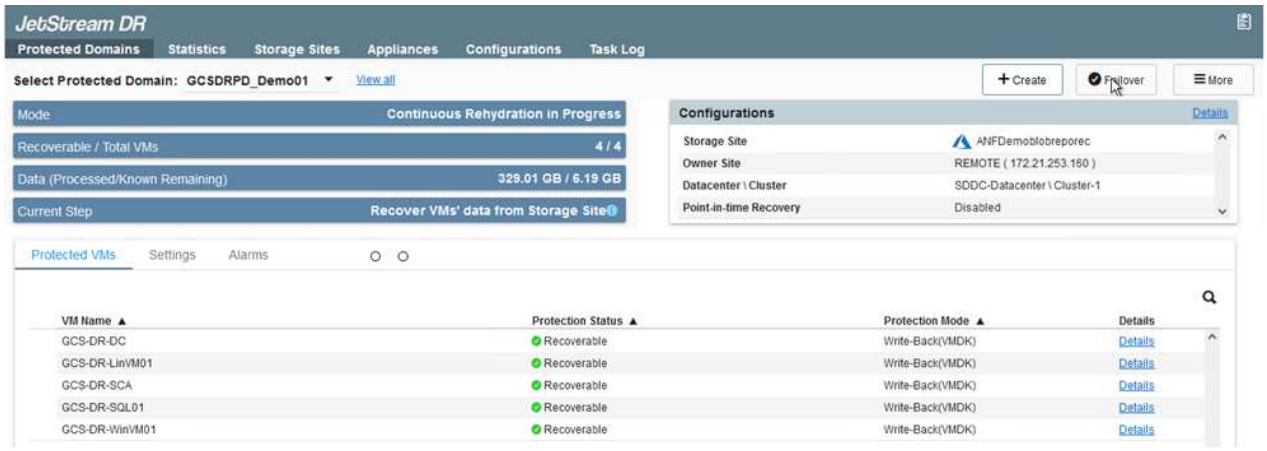


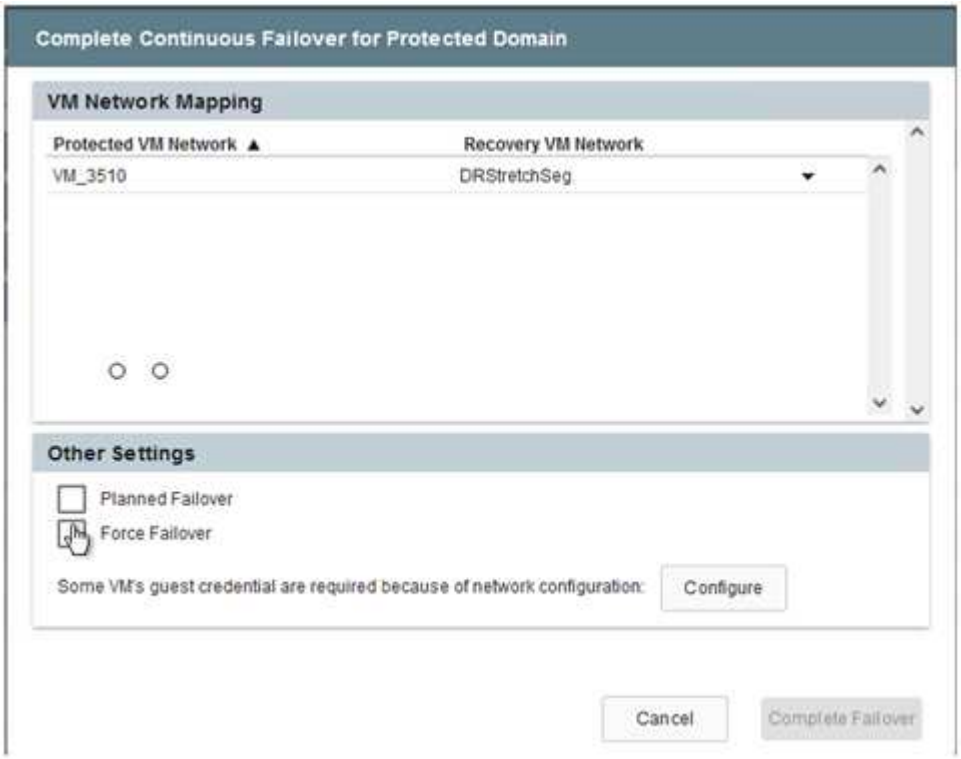


이 단계는 복구 프로세스를 용이하게 하기 위해 쉽게 자동화될 수 있습니다.

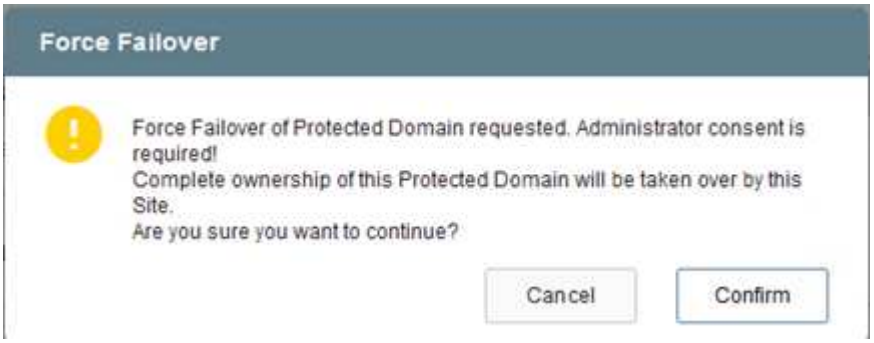
2. AVS SDDC(대상 측)에서 Jetstream UI에 액세스하고 장애 조치 옵션을 트리거하여 장애 조치를 완료합니다. 작업 표시줄에는 장애 조치 활동의 진행 상황이 표시됩니다.

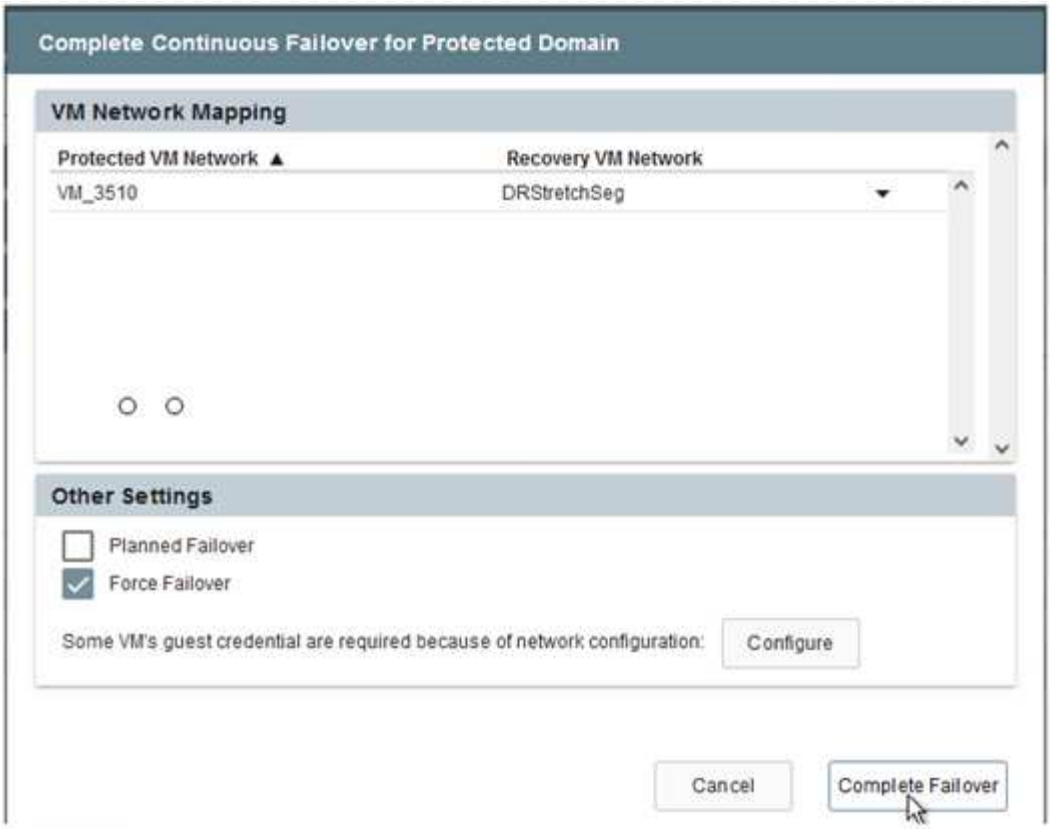
   장애 조치를 완료할 때 나타나는 대화 상자에서 장애 조치 작업을 계획된 대로 지정하거나 강제로 수행된 것으로 가정할 수 있습니다.





강제 장애 조치는 기본 사이트에 더 이상 액세스할 수 없다고 가정하고 보호된 도메인의 소유권은 복구 사이트에서 직접 인수해야 합니다.



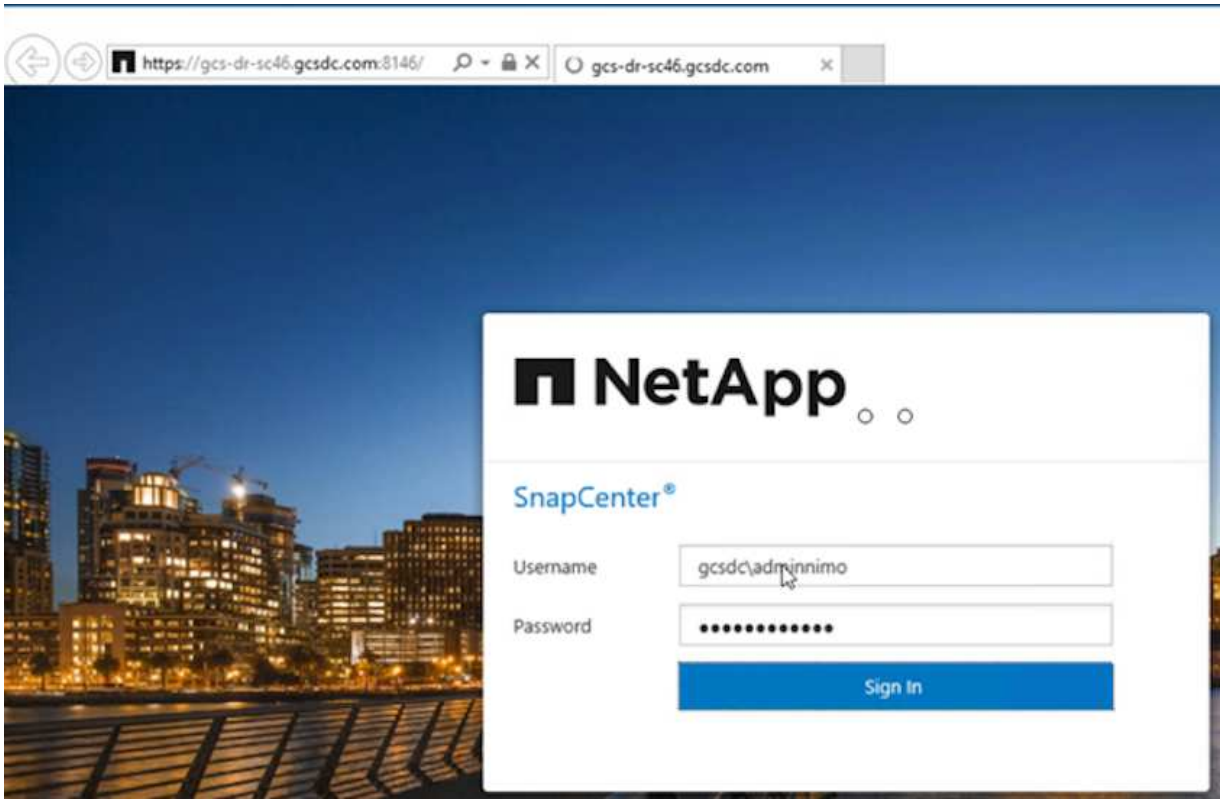


3. 지속적인 장애 조치가 완료되면 작업 완료를 확인하는 메시지가 나타납니다. 작업이 완료되면 복구된 VM에 액세스하여 ISCSI 또는 NFS 세션을 구성합니다.

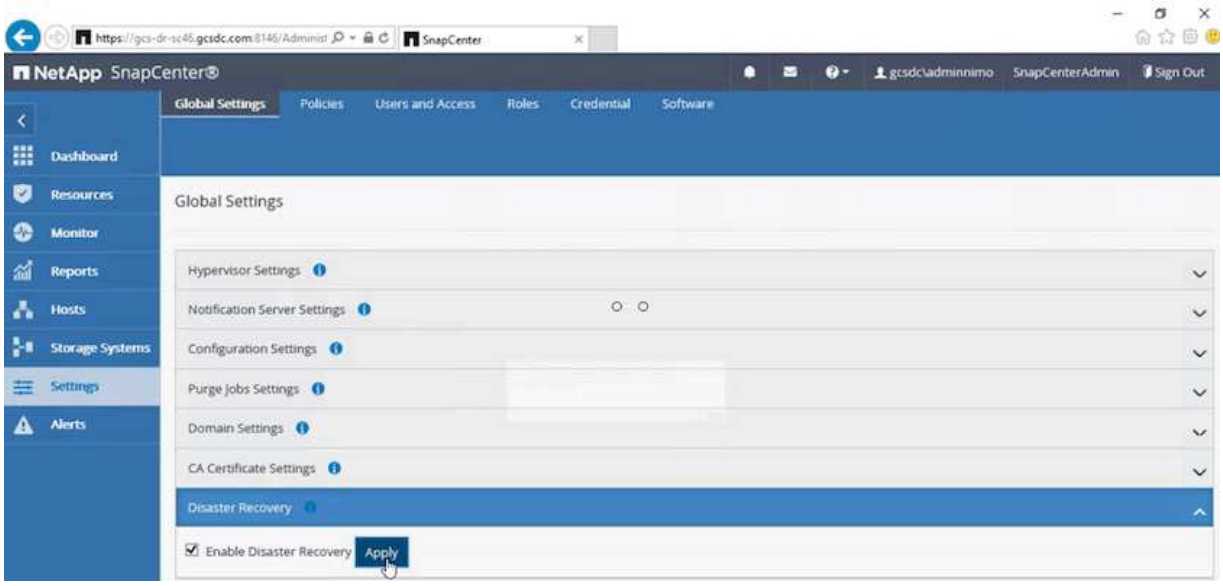
장애 조치 모드는 장애 조치 시 실행 중으로 변경되고 VM 상태는 복구 가능으로 변경됩니다. 보호된 도메인의 모든 VM은 이제 장애 조치 런북 설정에서 지정한 상태로 복구 사이트에서 실행됩니다.

장애 조치 구성 및 인프라를 검증하기 위해 JetStream DR을 테스트 모드(테스트 장애 조치 옵션)로 작동하여 가상 머신과 해당 데이터가 개체 저장소에서 테스트 복구 환경으로 복구되는 과정을 관찰할 수 있습니다. 테스트 모드에서 장애 조치 절차가 실행되면 실제 장애 조치 프로세스와 유사한 작업이 수행됩니다.

4. 가상 머신이 복구된 후에는 게스트 스토리지에 대한 스토리지 재해 복구를 사용합니다. 이 과정을 보여주기 위해 이 예에서는 SQL 서버를 사용합니다.
5. AVS SDDC에서 복구된 SnapCenter VM에 로그인하고 DR 모드를 활성화합니다.
   a. 브라우저를 사용하여 SnapCenter UI에 액세스합니다.



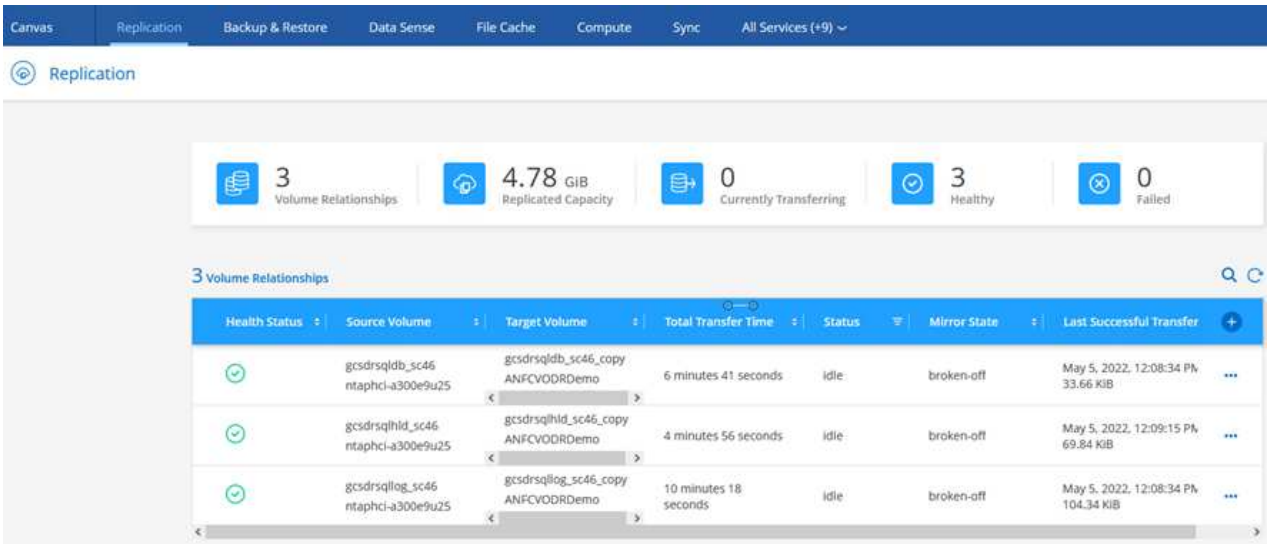
   b. 설정 페이지에서 설정 > 글로벌 설정 > 재해 복구로 이동합니다.
   c. 재해 복구 사용을 선택하세요.
   d. 적용을 클릭하세요.



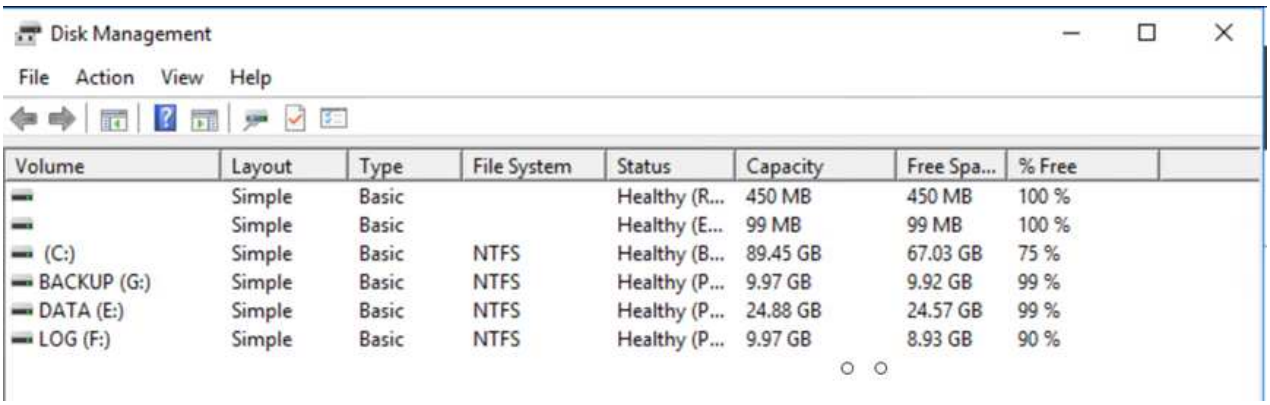
e. 모니터 > 작업을 클릭하여 DR 작업이 활성화되어 있는지 확인하세요.

스토리지 재해 복구에는 NetApp SnapCenter 4.6 이상을 사용해야 합니다. 이전 버전의 경우 애플리케이션 일관성 스냅샷(SnapMirror 사용하여 복제)을 사용해야 하며 재해 복구 사이트에서 이전 백업을 복구해야 하는 경우 수동 복구를 실행해야 합니다.

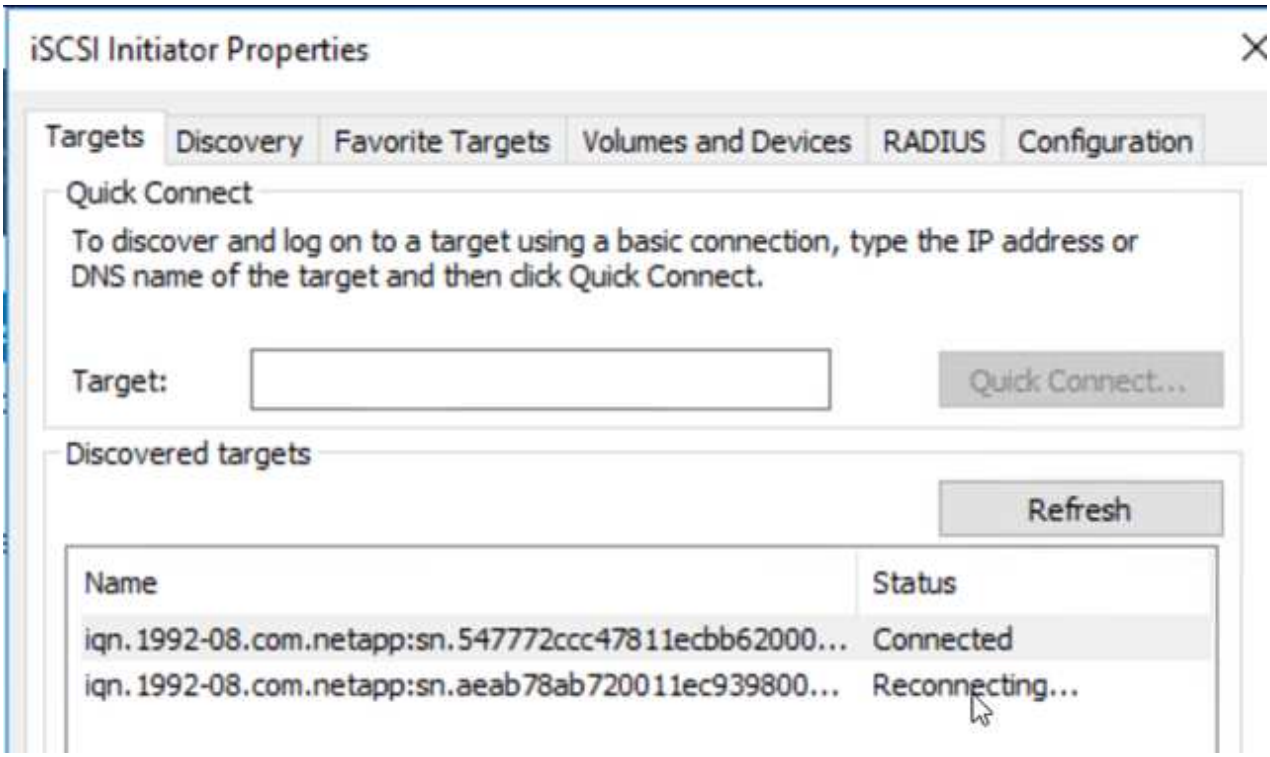
6. SnapMirror 관계가 끊어졌는지 확인하세요.



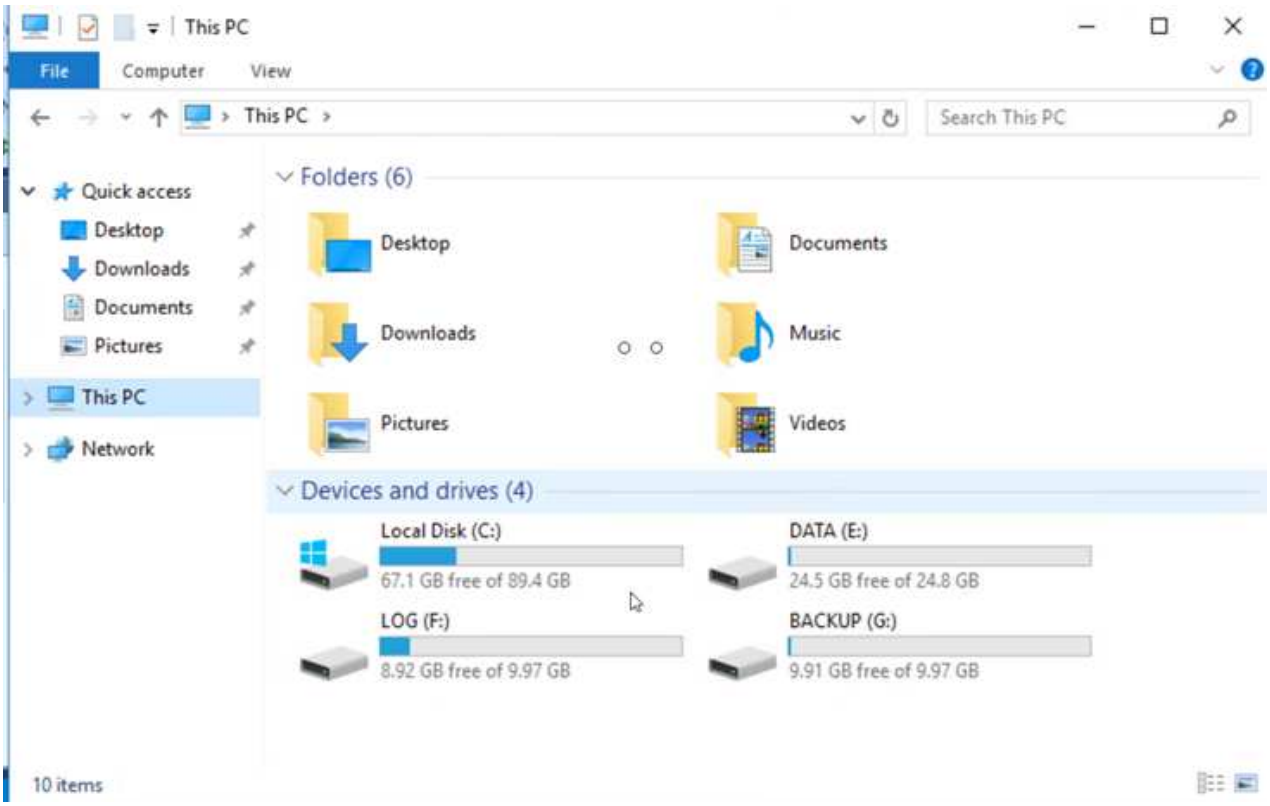
7. Cloud Volumes ONTAP 의 LUN을 동일한 드라이브 문자가 있는 복구된 SQL 게스트 VM에 연결합니다.



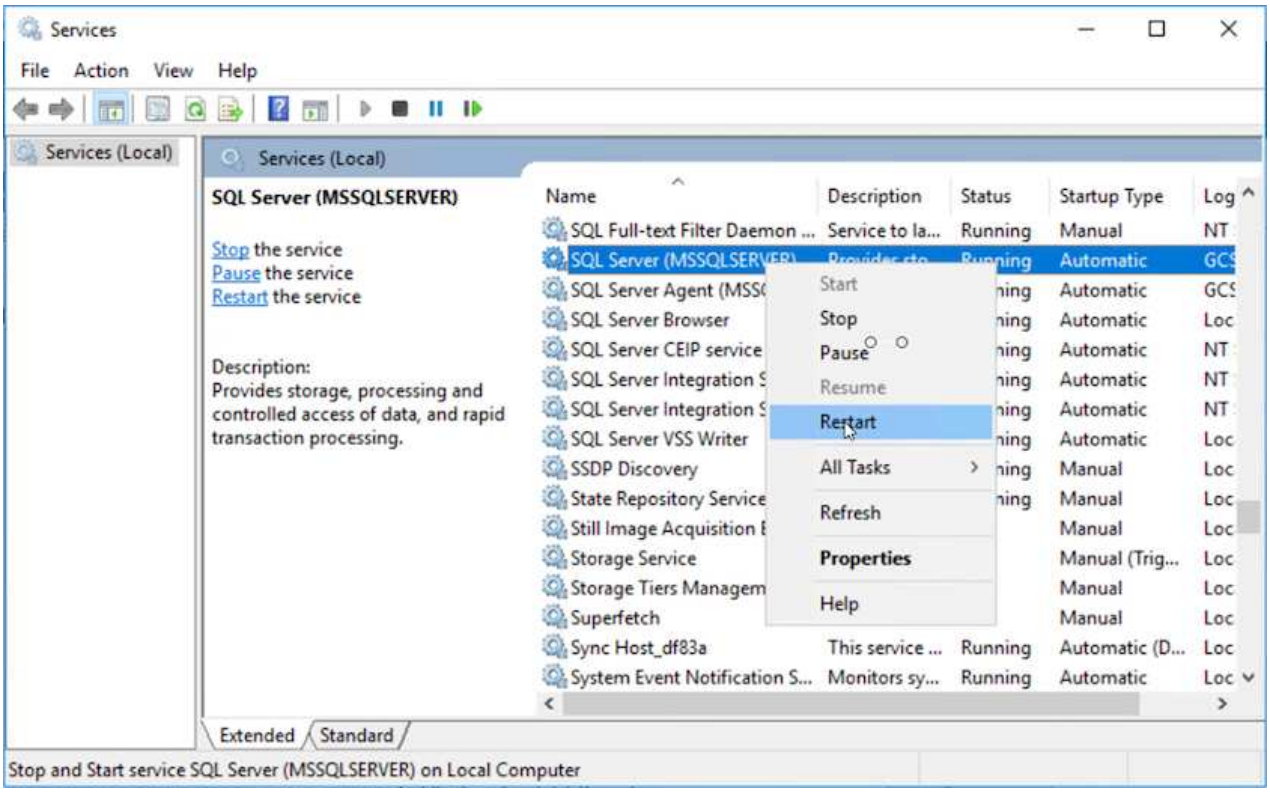
8. iSCSI Initiator를 열고 이전에 연결이 끊긴 세션을 지우고 복제된 Cloud Volumes ONTAP 볼륨에 대한 다중 경로와 함께 새 대상을 추가합니다.



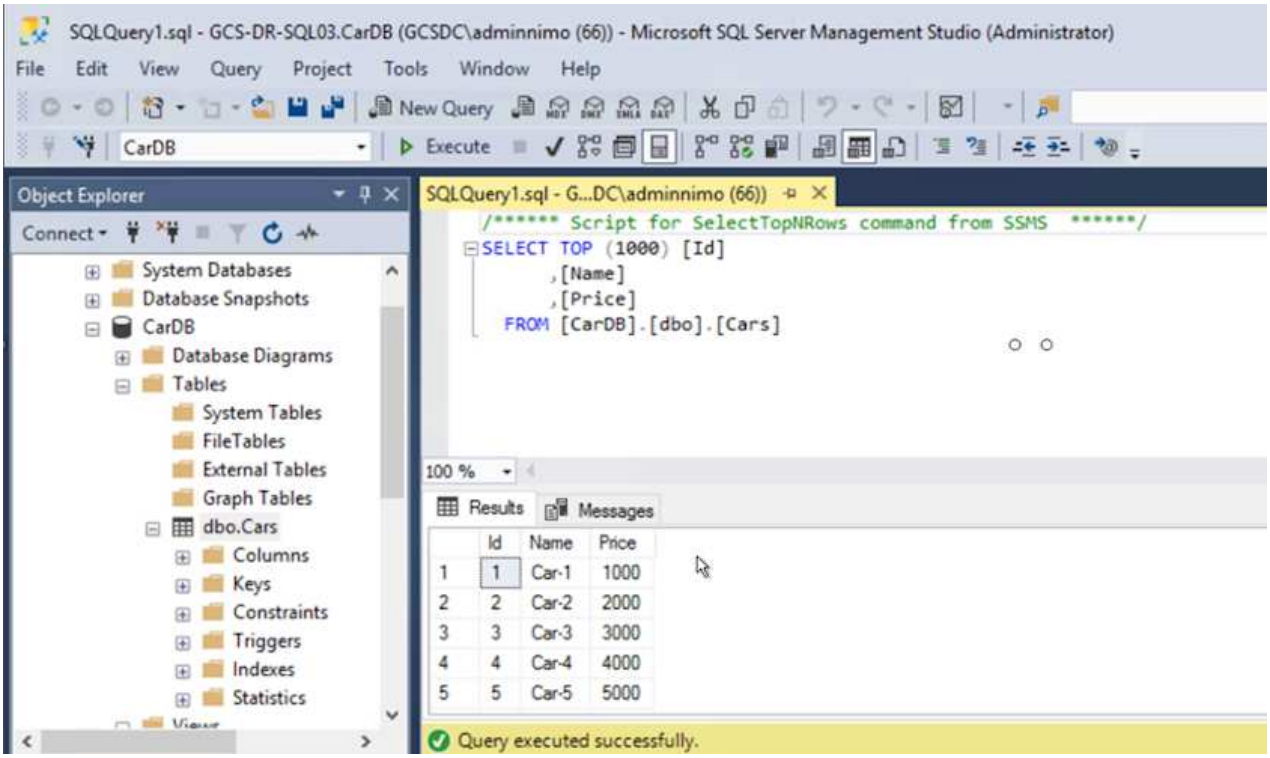
9. 모든 디스크가 DR 이전에 사용된 것과 동일한 드라이브 문자를 사용하여 연결되어 있는지 확인하세요.



10. MSSQL 서버 서비스를 다시 시작합니다.



11. SQL 리소스가 다시 온라인 상태인지 확인하세요.



NFS의 경우 mount 명령을 사용하여 볼륨을 연결하고 업데이트합니다. `/etc/fstab` 항목.

이 시점에서는 운영이 가능하며 사업은 정상적으로 계속됩니다.

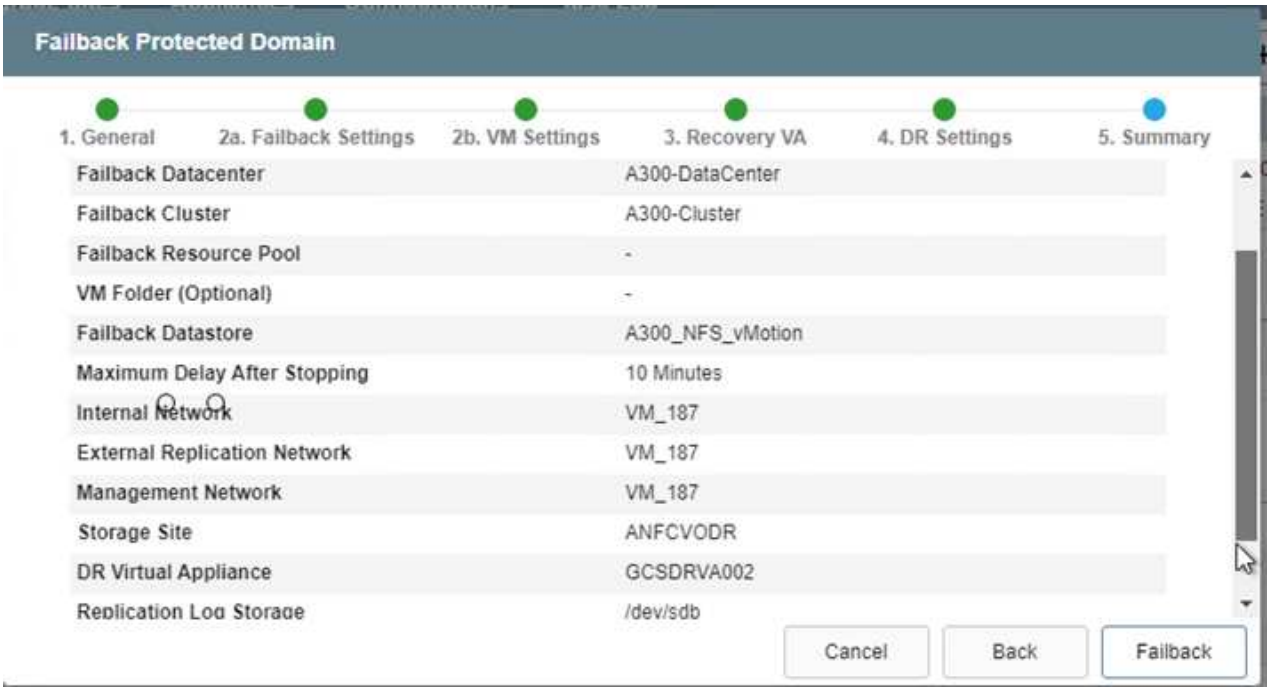
NSX-T 측에서는 장애 조치 시나리오를 시뮬레이션하기 위해 별도의 전용 Tier-1 게이트웨이를 생성할 수 있습니다. 이를 통해 모든 워크로드가 서로 통신할 수 있지만 트래픽이 환경 내부 또는 외부로 라우팅되지 않으므로 교차 오염 위험 없이 분류, 격리 또는 강화 작업을 수행할 수 있습니다. 이 작업은 이 문서의 범위를 벗어나지만, 격리를 시뮬레이션하는 경우 쉽게 수행할 수 있습니다.

기본 사이트가 다시 가동되면 장애 복구를 수행할 수 있습니다. VM 보호는 Jetstream에 의해 재개되고 SnapMirror 관계는 반전되어야 합니다.

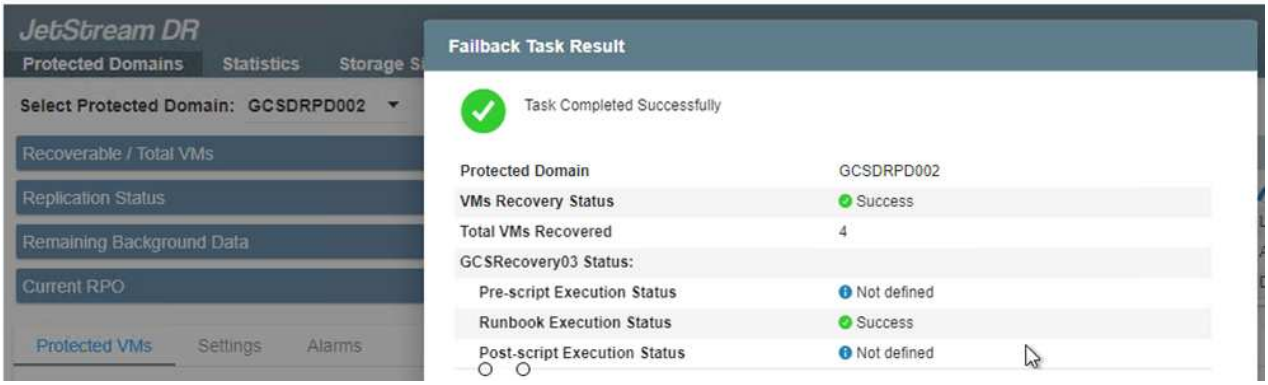
1. 온프레미스 환경을 복원합니다. 재해 사고의 유형에 따라 보호된 클러스터의 구성을 복원하거나 검증해야 할 수도 있습니다. 필요한 경우 JetStream DR 소프트웨어를 다시 설치해야 할 수도 있습니다.
2. 복원된 온프레미스 환경에 액세스하고 Jetstream DR UI로 이동하여 적절한 보호 도메인을 선택합니다. 보호된 사이트가 장애 복구 준비가 되면 UI에서 장애 복구 옵션을 선택합니다.

CPT에서 생성된 장애 복구 계획은 VM과 해당 데이터를 개체 저장소에서 원래 VMware 환경으로 반환하는 데에도 사용할 수 있습니다.

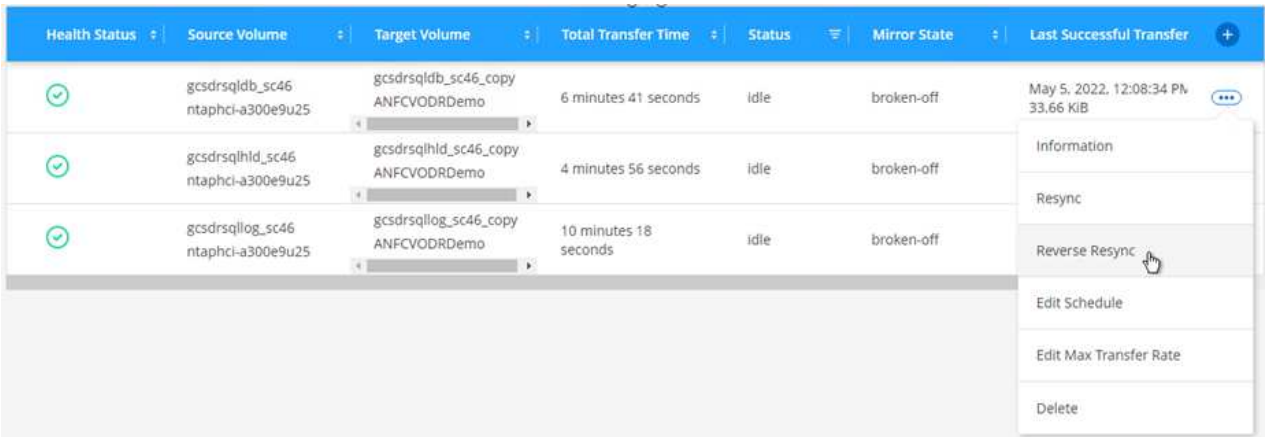
복구 사이트에서 VM을 일시 중지한 후 보호 사이트에서 다시 시작한 후의 최대 지연 시간을 지정합니다. 이 프로세스를 완료하는 데 필요한 시간에는 장애 조치 VM을 중지한 후 복제를 완료하는 데 필요한 시간, 복구 사이트를 정리하는 데 필요한 시간, 보호된 사이트에서 VM을 다시 만드는 데 필요한 시간이 포함됩니다. NetApp 10분을 권장합니다.

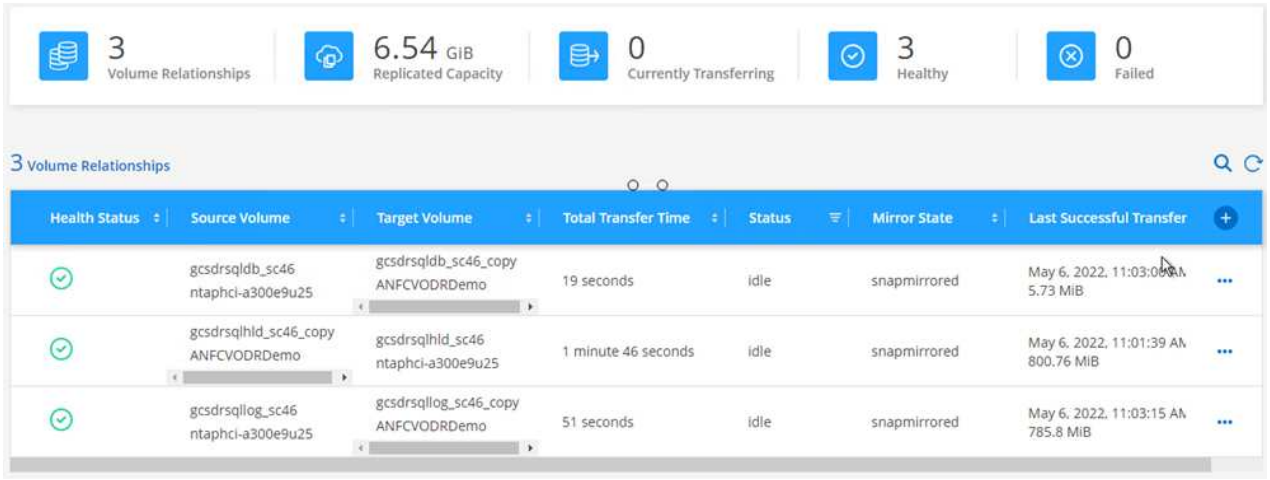


3. 장애 복구 프로세스를 완료한 후 VM 보호 및 데이터 일관성이 재개되었는지 확인합니다.

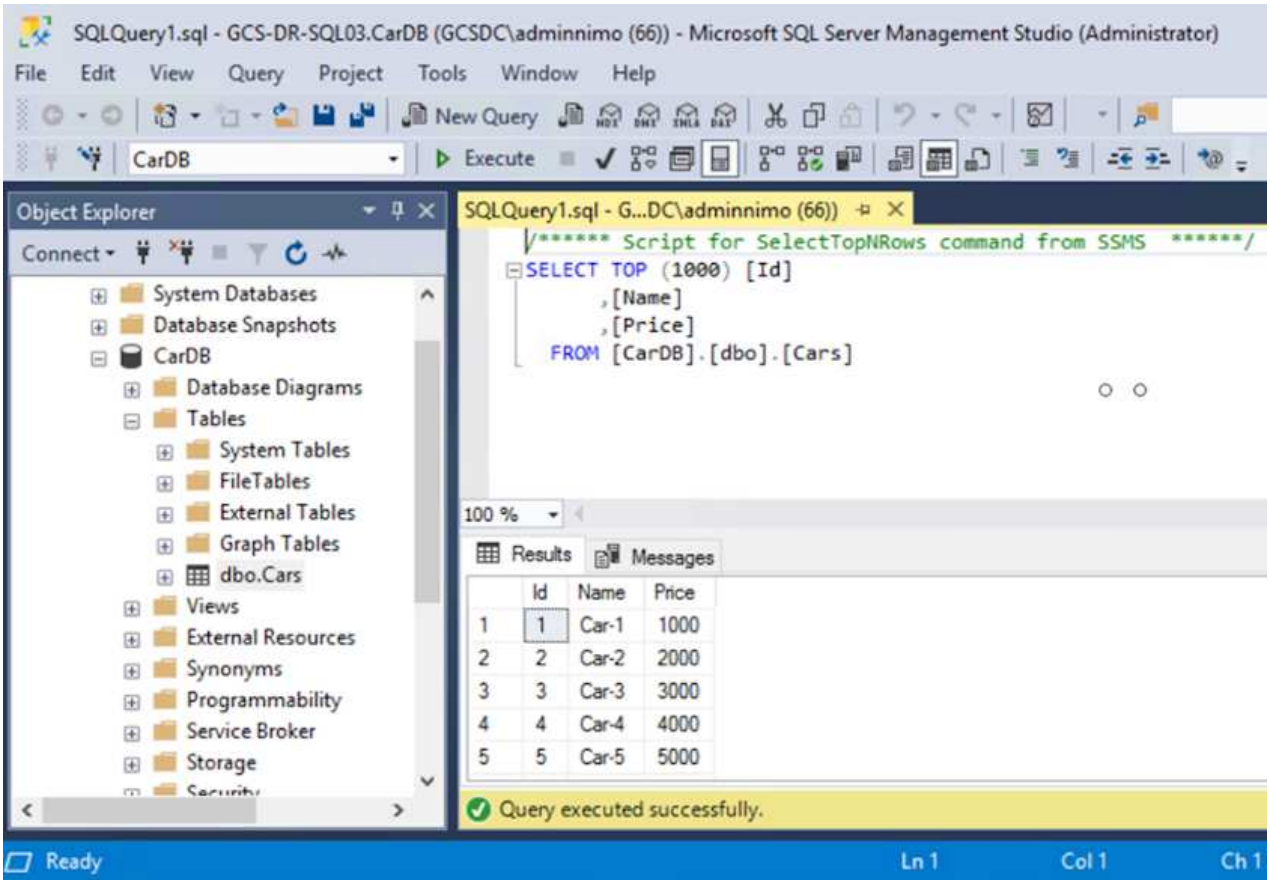


4. VM이 복구된 후 호스트에서 보조 스토리지의 연결을 끊고 기본 스토리지에 연결합니다.





5. MSSQL 서버 서비스를 다시 시작합니다.
6. SQL 리소스가 다시 온라인 상태인지 확인하세요.



기본 저장소로 장애 복구하려면 역방향 재동기화 작업을 수행하여 관계 방향이 장애 조치 전과 동일하게 유지되는지 확인하세요.

역방향 재동기화 작업 후에 기본 및 보조 저장소의 역할을 유지하려면 역방향 재동기화 작업을 다시 수행합니다.

이 프로세스는 Oracle, 유사한 데이터베이스 플레이버 및 게스트 연결 스토리지를 사용하는 다른

애플리케이션에도 적용할 수 있습니다.

항상 그렇듯이, 프로덕션에 이식하기 전에 중요한 워크로드를 복구하는 데 필요한 단계를 테스트하세요.

이 솔루션의 이점

- SnapMirror 의 효율적이고 탄력적인 복제를 사용합니다.
- ONTAP 스냅샷 보존을 통해 사용 가능한 모든 시점으로 복구합니다.
- 스토리지, 컴퓨팅, 네트워크 및 애플리케이션 검증 단계 등 수백 개에서 수천 개의 VM을 복구하는 데 필요한 모든 단계에 대한 전체 자동화가 가능합니다.
- SnapCenter 복제된 볼륨을 변경하지 않는 복제 메커니즘을 사용합니다.
  - 이렇게 하면 볼륨과 스냅샷의 데이터 손상 위험을 방지할 수 있습니다.
  - DR 테스트 워크플로우 동안 복제 중단을 방지합니다.
  - DR을 넘어 개발/테스트, 보안 테스트, 패치 및 업그레이드 테스트, 수정 테스트 등 워크플로우에 DR 데이터를 활용합니다.
- CPU 및 RAM 최적화는 더 작은 컴퓨팅 클러스터로 복구를 가능하게 하여 클라우드 비용을 낮추는 데 도움이 될 수 있습니다.