Azure/AVS에서 워크로드 보호

NetApp Solutions

NetApp
April 20, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/netapp-solutions/ehc/azure-native-dr-jetstream.html on April 20, 2024. Always check docs.netapp.com for the latest.

목차

Azure/AVS에서 워크로드 보호 . . . 1
ANF 및 Jetstream을 통한 재해 복구 . . . 1
CVO 및 AVS(게스트 연결 스토리지)를 통한 재해 복구 . . . 13
TR-4955: ANF(Azure NetApp Files) 및 AVS(Azure VMware Solution)를 통한 재해 복구 . . . 38
Azure VMware Solution으로 재해 복구를 위해 Veeam Replication 및 Azure NetApp Files 데이터 저장소를 사용합니다 . . . 52

Azure/AVS에서 워크로드 보호

ANF 및 Jetstream을 통한 재해 복구

클라우드로 재해 복구는 사이트 운영 중단 및 데이터 손상 이벤트(예: 랜섬웨어)로부터 워크로드를 보호하는 복원력이 있고 비용 효율적인 방법입니다. VMware VAIO 프레임워크를 사용하여 온프레미스 VMware 워크로드를 Azure Blob 스토리지에 복제하고 복구하여 데이터 손실과 제로급 RTO를 최소화하거나 최소화할 수 있습니다.

Jetstream DR을 사용하면 사내에서 AVS로, 특히 Azure NetApp Files로 복제된 워크로드를 원활하게 복구할 수 있습니다. DR 사이트에서 최소한의 리소스와 비용 효율적인 클라우드 스토리지를 사용하여 비용 효율적으로 재해 복구를 수행할 수 있습니다. Jetstream DR은 Azure Blob Storage를 통해 ANF 데이터 저장소에 대한 복구를 자동화합니다. Jetstream DR은 네트워크 매핑에 따라 독립적인 VM 또는 관련 VM 그룹을 복구 사이트 인프라로 복구하고 랜섬웨어 보호를 위한 시점 복구를 제공합니다.

이 문서에서는 Jetstream DR 운영 원리 및 주요 구성 요소에 대해 설명합니다.

1. 사내 데이터 센터에 Jetstream DR 소프트웨어를 설치합니다.
   a. Azure Marketplace(ZIP)에서 Jetstream DR 소프트웨어 번들을 다운로드하고 지정된 클러스터에 Jetstream DR MSA(OVA)를 배포합니다.
   b. I/O 필터 패키지를 사용하여 클러스터를 구성합니다(Jetstream VIB 설치).
   c. DR AVS 클러스터와 동일한 영역에서 Azure Blob(Azure Storage Account)를 프로비저닝합니다.
   d. DRVA 어플라이언스를 구축하고 복제 로그 볼륨(기존 데이터 저장소 또는 공유 iSCSI 스토리지의 VMDK)을 할당합니다.
   e. 보호된 도메인(관련 VM 그룹)을 생성하고 DRVA 및 Azure Blob Storage/ANF를 할당합니다.
   f. 보호를 시작합니다.
2. Azure VMware Solution 프라이빗 클라우드에 Jetstream DR 소프트웨어를 설치합니다.
   a. 실행 명령을 사용하여 Jetstream DR을 설치 및 구성합니다.
   b. 동일한 Azure Blob 컨테이너를 추가하고 Scan Domains 옵션을 사용하여 도메인을 검색합니다.
   c. 필요한 DRVA 어플라이언스를 배포합니다.
   d. 사용 가능한 vSAN 또는 ANF 데이터 저장소를 사용하여 복제 로그 볼륨을 생성합니다.
   e. 보호된 도메인을 가져오고 RockVA(복구 VA)를 구성하여 VM 배치에 ANF 데이터 저장소를 사용합니다.
   f. 적절한 페일오버 옵션을 선택하고 제로급 RTO 도메인 또는 VM에 대한 연속 재수화를 시작합니다.
3. 재해 이벤트 중에 지정된 AVS DR 사이트에서 Azure NetApp Files 데이터 저장소로 장애 조치를 트리거합니다.
4. 보호된 사이트를 복구한 후 보호된 사이트에 대한 페일백을 호출합니다. 시작하기 전에 이 지침에 따라 사전 요구 사항이 충족되는지 확인합니다 "링크" 또한 Jetstream Software에서 제공하는 BWT(대역폭 테스트 도구)를 실행하여 Jetstream DR 소프트웨어와 함께 사용할 경우 Azure Blob 스토리지의 잠재적 성능과 해당 복제 대역폭을 평가합니다. 연결을 포함한 사전 요구 사항이 준비된 후에는 에서 Jetstream DR for AVS를 설정하고 구독하십시오 "Azure 마켓플레이스 를 참조하십시오". 소프트웨어 번들을 다운로드한 후 위에 설명된 설치 프로세스를 진행합니다.

많은 수의 VM(예: 100+)에 대한 보호를 계획하고 시작할 때는 Jetstream DR Automation Toolkit의 CPT(Capacity Planning Tool)를 사용하십시오. RTO 및 복구 그룹 기본 설정과 함께 보호할 VM 목록을 제공한 다음 CPT를 실행합니다.

CPT는 다음과 같은 기능을 수행합니다.

- RTO에 따라 VM을 보호 도메인에 결합합니다.
- 최적의 DRVA 수 및 해당 리소스 정의
- 필요한 복제 대역폭을 추정하는 중입니다.
- 복제 로그 볼륨 특성(용량, 대역폭 등) 식별
- 필요한 오브젝트 스토리지 용량을 예측하는 등

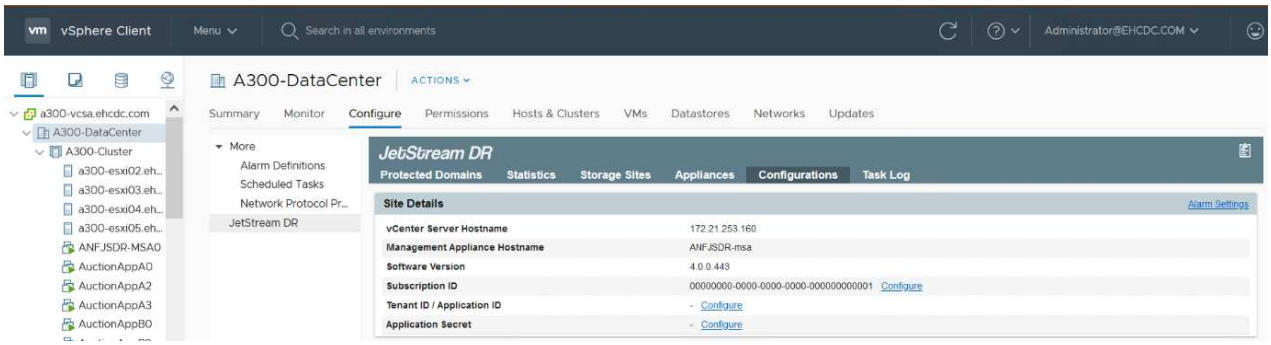
> ⓘ 규정된 도메인의 수와 컨텐츠는 평균 IOPS, 총 용량, 우선 순위(페일오버 순서를 정의하는 경우), RTO 등과 같은 다양한 VM 특성에 따라 달라집니다.

온프레미스 데이터 센터에 **Jetstream DR**을 설치합니다

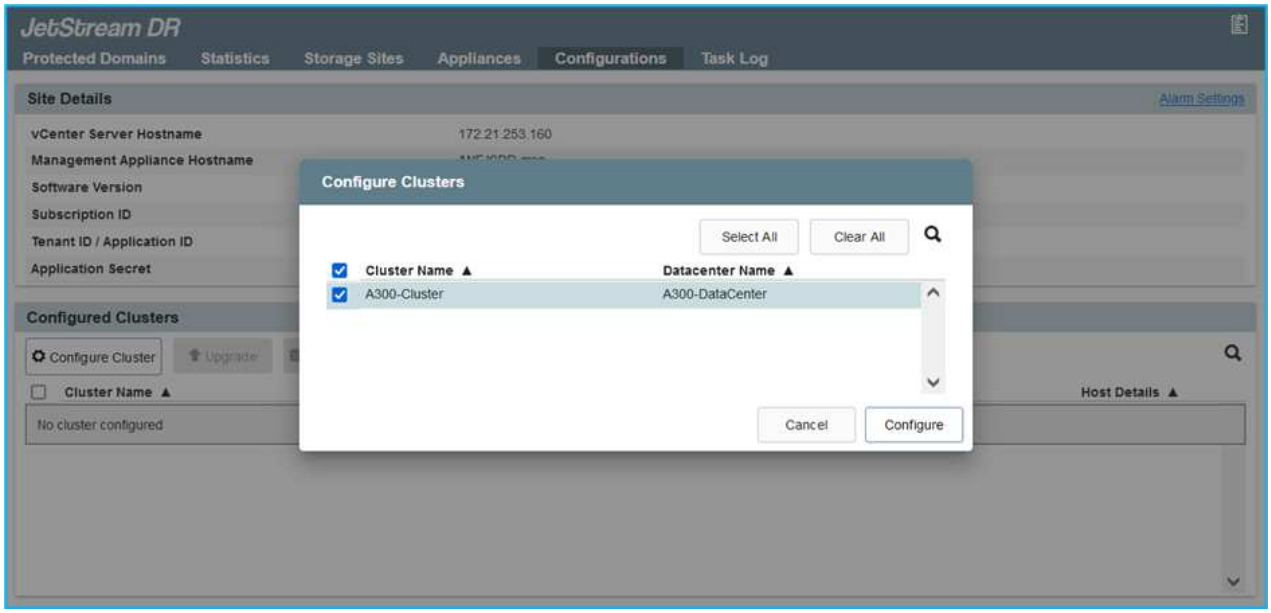
Jetstream DR 소프트웨어는 Jetstream DR Management Server Virtual Appliance(MSA), DR 가상 어플라이언스(DRVA) 및 호스트 구성 요소(I/O 필터 패키지)의 세 가지 주요 구성 요소로 구성됩니다. MSA는 컴퓨팅 클러스터에 호스트 구성 요소를 설치 및 구성한 다음 Jetstream DR 소프트웨어를 관리하는 데 사용됩니다. 다음 목록에는 설치 프로세스에 대한 자세한 설명이 나와 있습니다.

구내 **Jetstream DR**을 설치하는 방법

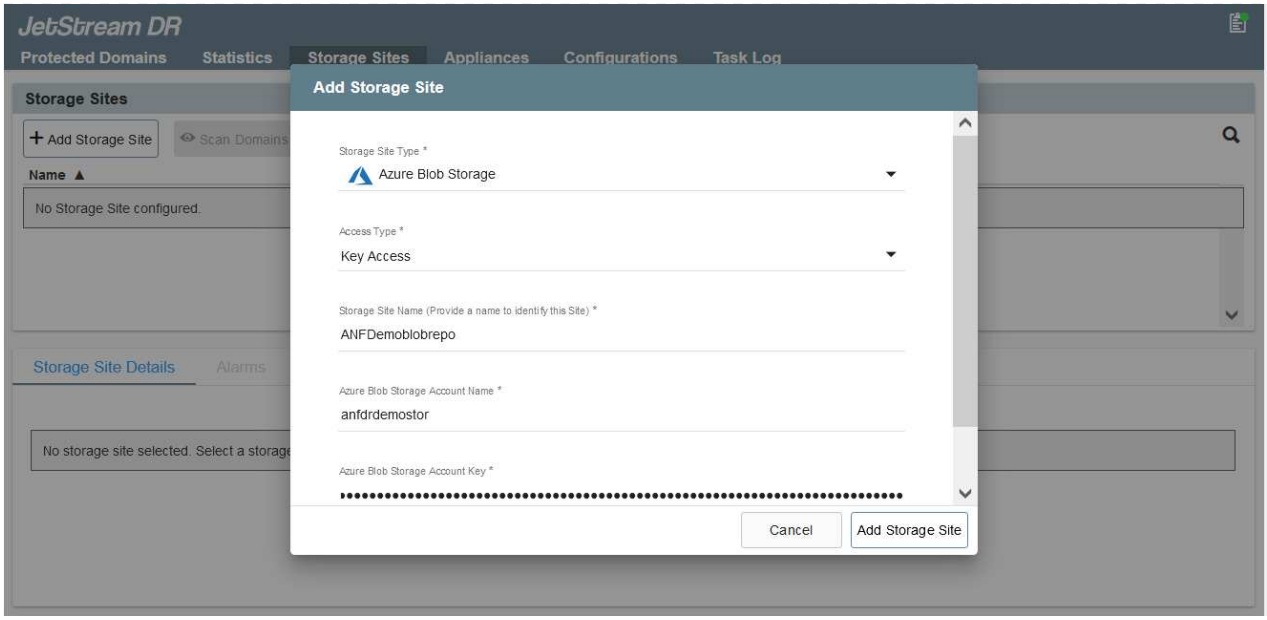
1. 필수 구성 요소를 확인하십시오.
2. 리소스 및 구성 권장 사항에 대해 용량 계획 툴을 실행합니다(선택 사항이지만 개념 증명 평가에는 권장됨).
3. Jetstream DR MSA를 지정된 클러스터의 vSphere 호스트에 구축합니다.
4. 브라우저에서 DNS 이름을 사용하여 MSA를 실행합니다.
5. MSA에 vCenter Server를 등록합니다. 설치를 수행하려면 다음 세부 단계를 완료하십시오.
6. Jetstream DR MSA를 구축하고 vCenter Server를 등록한 후에는 vSphere Web Client를 사용하여 Jetstream DR 플러그인에 액세스합니다. 이 작업은 데이터 센터 > 구성 > Jetstream DR로 이동하여 수행할 수 있습니다.



7. Jetstream DR 인터페이스에서 적절한 클러스터를 선택합니다.



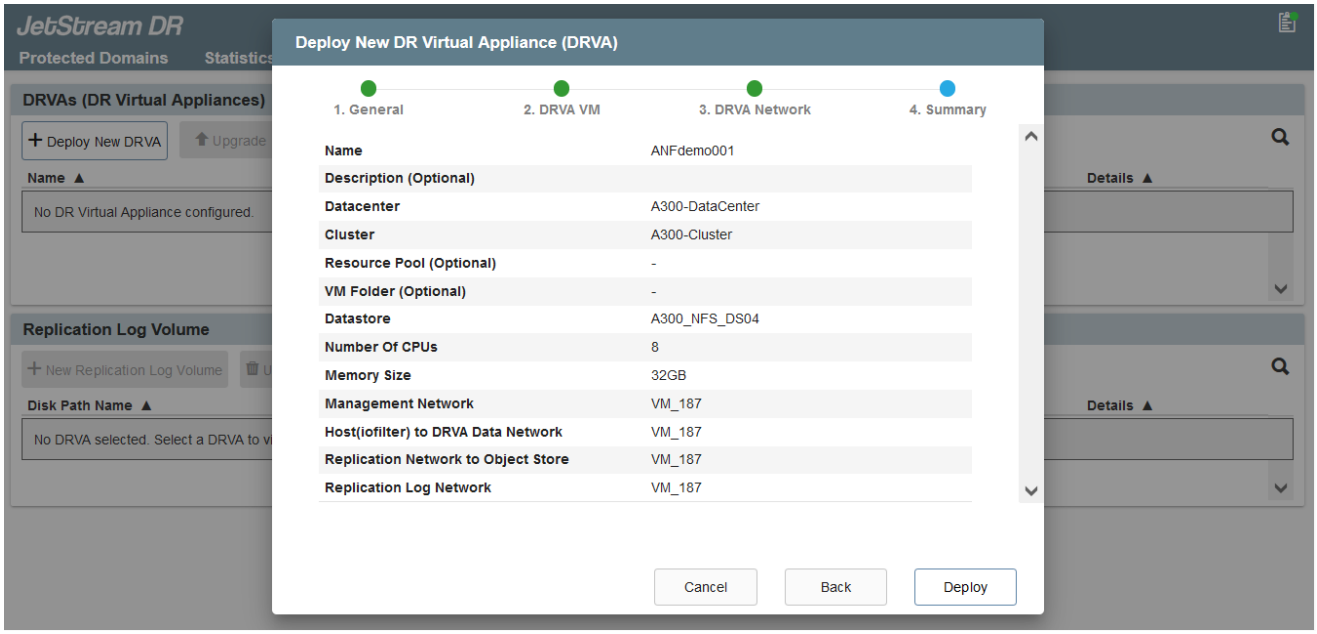
8. I/O 필터 패키지를 사용하여 클러스터를 구성합니다.



9. 복구 사이트에 있는 Azure Blob Storage를 추가합니다.
10. Appliances(어플라이언스) 탭에서 DR Virtual Appliance(DRVA)를 구축합니다.

> DRVA는 CPT에 의해 자동으로 생성될 수 있지만 POC 평가에서는 DR 주기를 수동으로 구성 및 실행하는 것이 좋습니다(시작 보호 > 장애 조치 > 장애 복구).

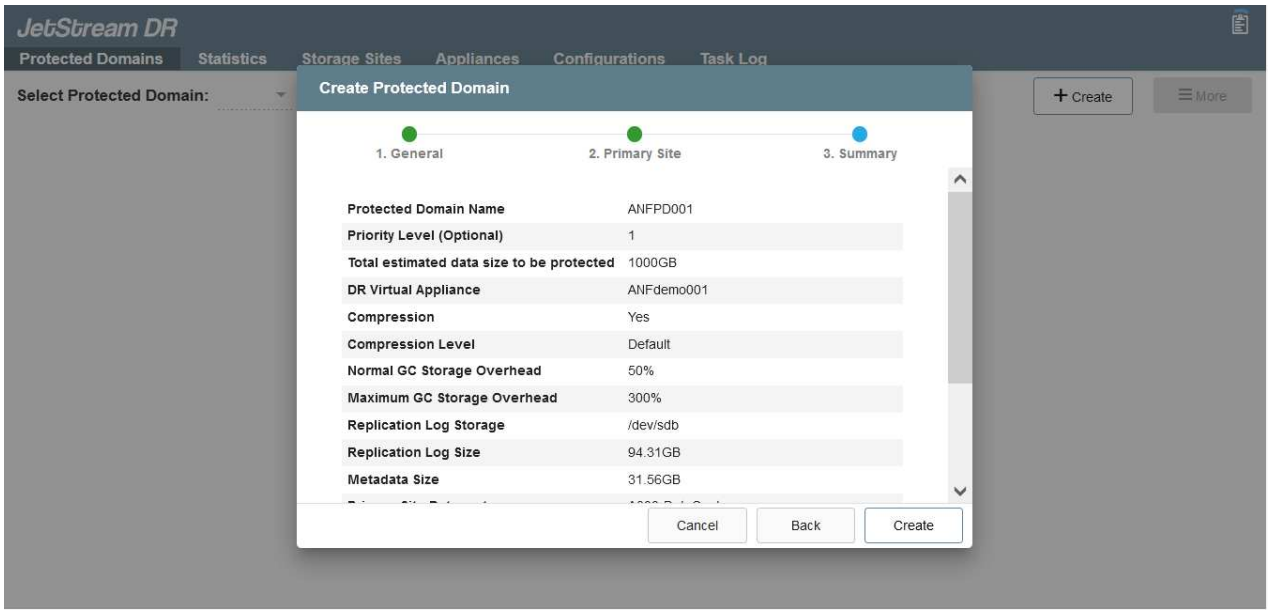
Jetstream DRVA는 데이터 복제 프로세스의 주요 기능을 용이하게 하는 가상 어플라이언스입니다. 보호되는 클러스터에는 DRVA가 하나 이상 포함되어야 하며, 일반적으로 호스트당 DRVA가 하나씩 구성됩니다. 각 DRVA는 여러 개의 보호된 도메인을 관리할 수 있습니다.



이 예에서는 80개의 가상 머신에 대해 4개의 DRVA가 생성되었습니다.

1. 사용 가능한 데이터 저장소 또는 독립 공유 iSCSI 스토리지 풀에서 VMDK를 사용하여 각 DRVA에 대한 복제 로그 볼륨을 생성합니다.

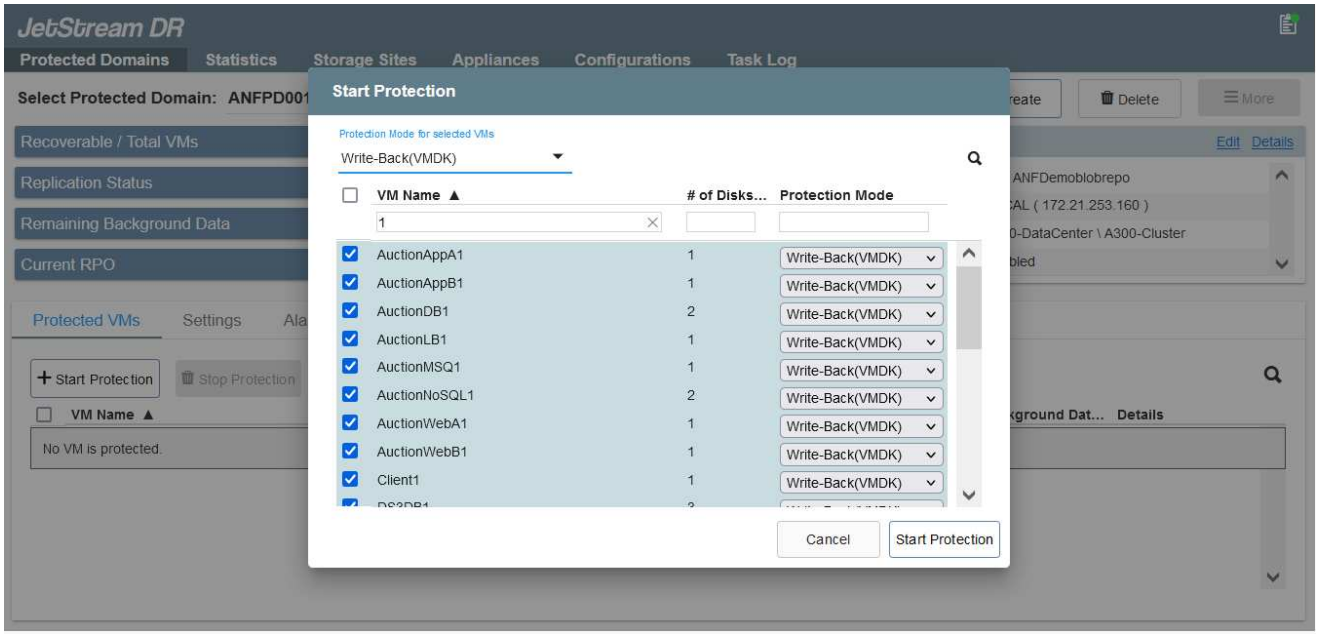
2. 보호 도메인 탭에서 Azure Blob 저장소 사이트, DRVA 인스턴스 및 복제 로그에 대한 정보를 사용하여 필요한 수의 보호된 도메인을 만듭니다. 보호 도메인은 함께 보호되고 장애 조치/장애 복구 작업에 우선 순위가 할당된 클러스터 내의 특정 VM 또는 VM 집합을 정의합니다.



3. 보호할 VM을 선택하고 보호된 도메인의 VM 보호를 시작합니다. 그러면 지정된 Blob 저장소에 대한 데이터 복제가 시작됩니다.

ⓘ 보호 도메인의 모든 VM에 동일한 보호 모드가 사용되는지 확인합니다.

ⓘ VMDK(Write-Back) 모드에서는 더 높은 성능을 제공할 수 있습니다.



복제 로그 볼륨이 고성능 스토리지에 배치되었는지 확인합니다.

> 페일오버 실행 도서를 구성하여 VM(복구 그룹)을 그룹화하고 부팅 순서 시퀀스를 설정하고 IP 구성과 함께 CPU/메모리 설정을 수정할 수 있습니다.

실행 명령을 사용하여 **Azure VMware** 솔루션 프라이빗 클라우드에 **AVS**용 **Jetstream DR**을 설치합니다

복구 사이트(AVS)의 모범 사례는 3노드 파일럿 라이트 클러스터를 미리 생성하는 것입니다. 이렇게 하면 다음 항목을 포함하여 복구 사이트 인프라를 사전 구성할 수 있습니다.

- 대상 네트워킹 세그먼트, 방화벽, DHCP 및 DNS 등의 서비스 등
- AVS용 Jetstream DR 설치
- ANF 볼륨을 데이터 저장소로 구성하고, moreJetStream DR은 미션 크리티컬 도메인에 대해 제로급 RTO 모드를 지원합니다. 이러한 도메인의 경우 대상 스토리지가 사전 설치되어 있어야 합니다. ANF는 이 경우 권장되는 스토리지 유형입니다.

> 세그먼트 생성을 포함한 네트워크 구성은 AVS 클러스터에서 사내 요구 사항과 일치하도록 구성해야 합니다.

SLA 및 RTO 요구 사항에 따라 지속적인 페일오버 또는 일반(표준) 페일오버 모드를 사용할 수 있습니다. 제로급 RTO의 경우 복구 사이트에서 연속 재수화를 시작해야 합니다.

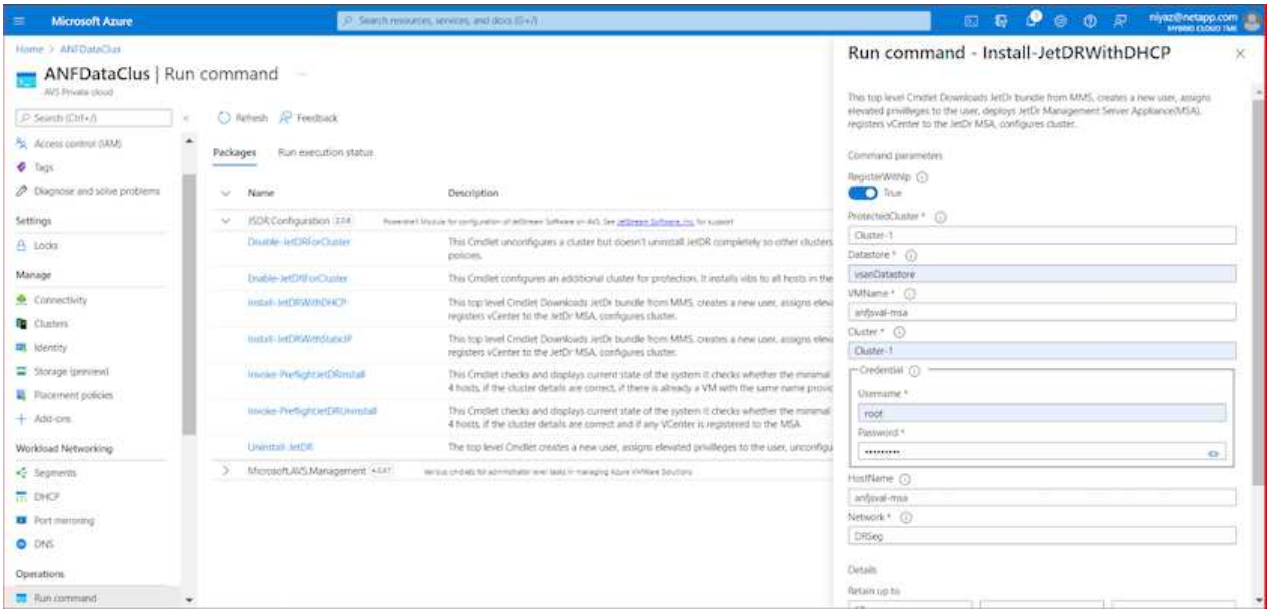
프라이빗 클라우드에 **AVS**용 **Jetstream DR**을 설치하는 방법

Azure VMware 솔루션 프라이빗 클라우드에 AVS용 Jetstream DR을 설치하려면 다음 단계를 수행하십시오.

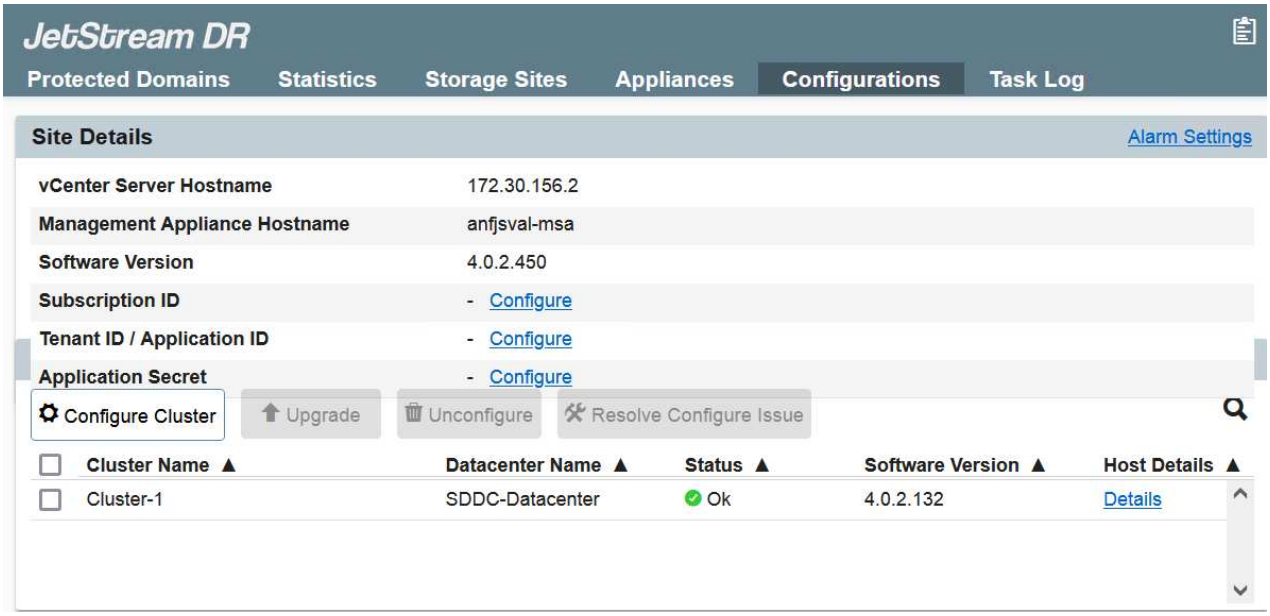
1. Azure 포털에서 Azure VMware 솔루션으로 이동하여 프라이빗 클라우드를 선택한 다음 명령 실행 > 패키지 > JSDR.Configuration을 선택합니다.

> Azure VMware 솔루션의 기본 CloudAdmin 사용자는 AVS용 Jetstream DR을 설치할 권한이 없습니다. Azure VMware 솔루션을 사용하면 Jetstream DR용 Azure VMware 솔루션 실행 명령을 호출하여 Jetstream DR을 간단하고 자동으로 설치할 수 있습니다.

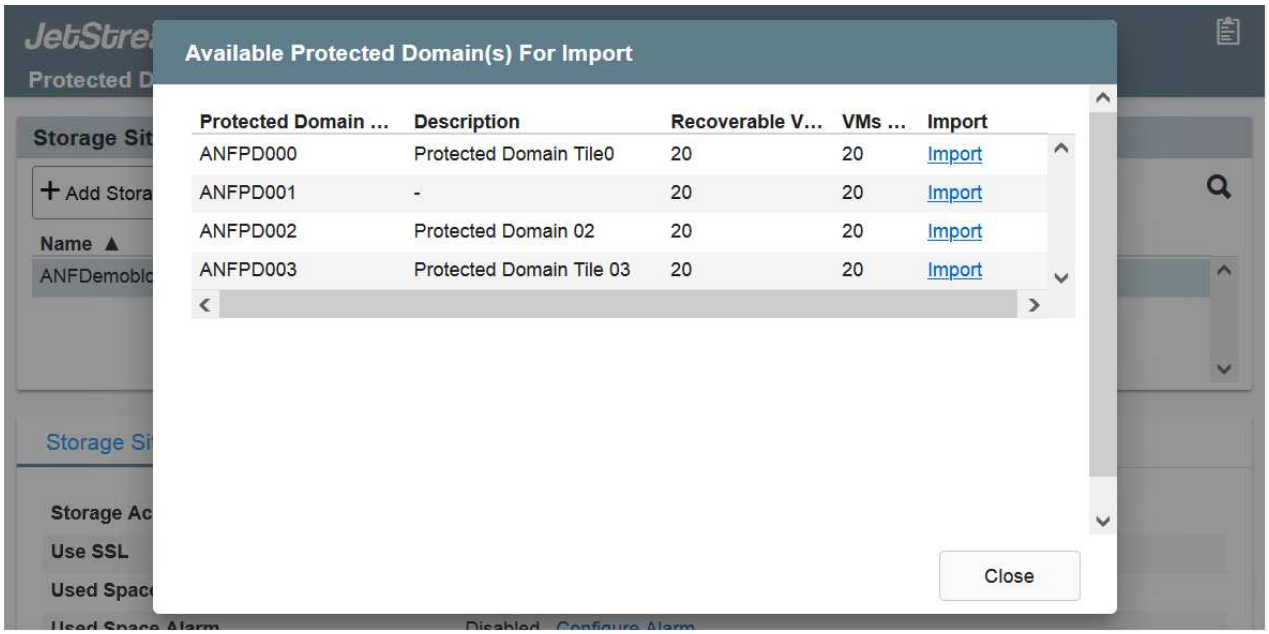
다음 스크린샷은 DHCP 기반 IP 주소를 사용한 설치를 보여 줍니다.



2. AVS 설치를 위한 Jetstream DR이 완료되면 브라우저를 새로 고칩니다. Jetstream DR UI에 액세스하려면 SDDC 데이터 센터 > 구성 > Jetstream DR로 이동하십시오.



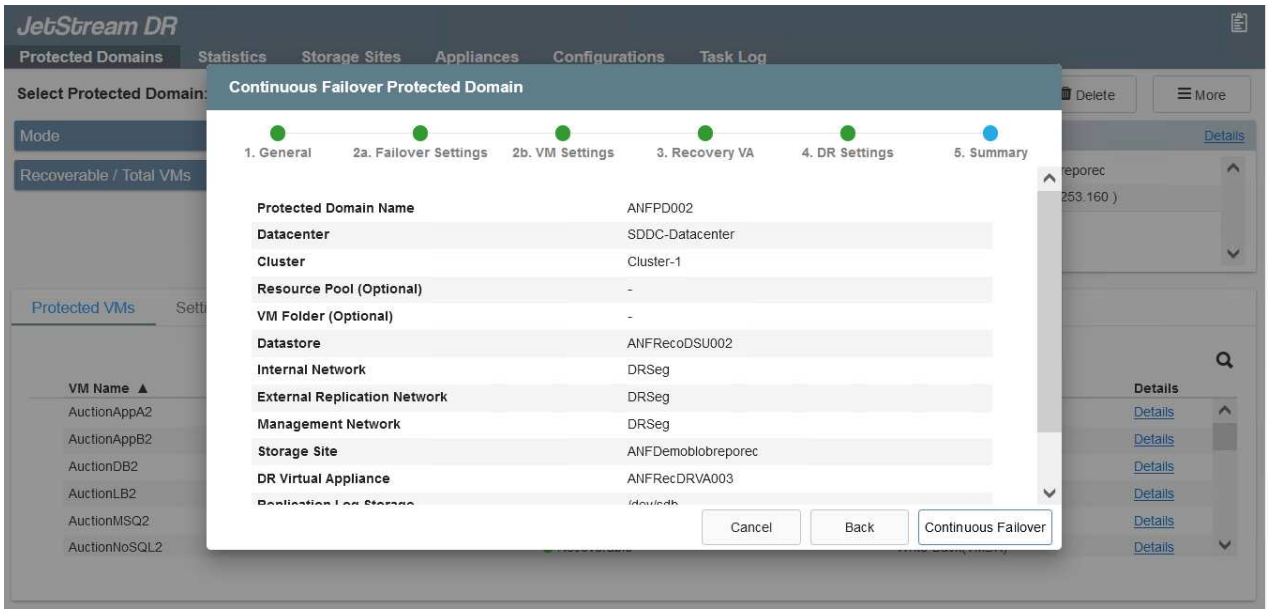
3. Jetstream DR 인터페이스에서 온프레미스 클러스터를 저장소 사이트로 보호하는 데 사용된 Azure Blob 저장소 계정을 추가한 다음 도메인 검사 옵션을 실행합니다.



4. 보호된 도메인을 가져온 후 DRVA 어플라이언스를 구축합니다. 이 예에서는 Jetstream DR UI를 사용하여 복구 사이트에서 수동으로 연속 재수화를 시작합니다.

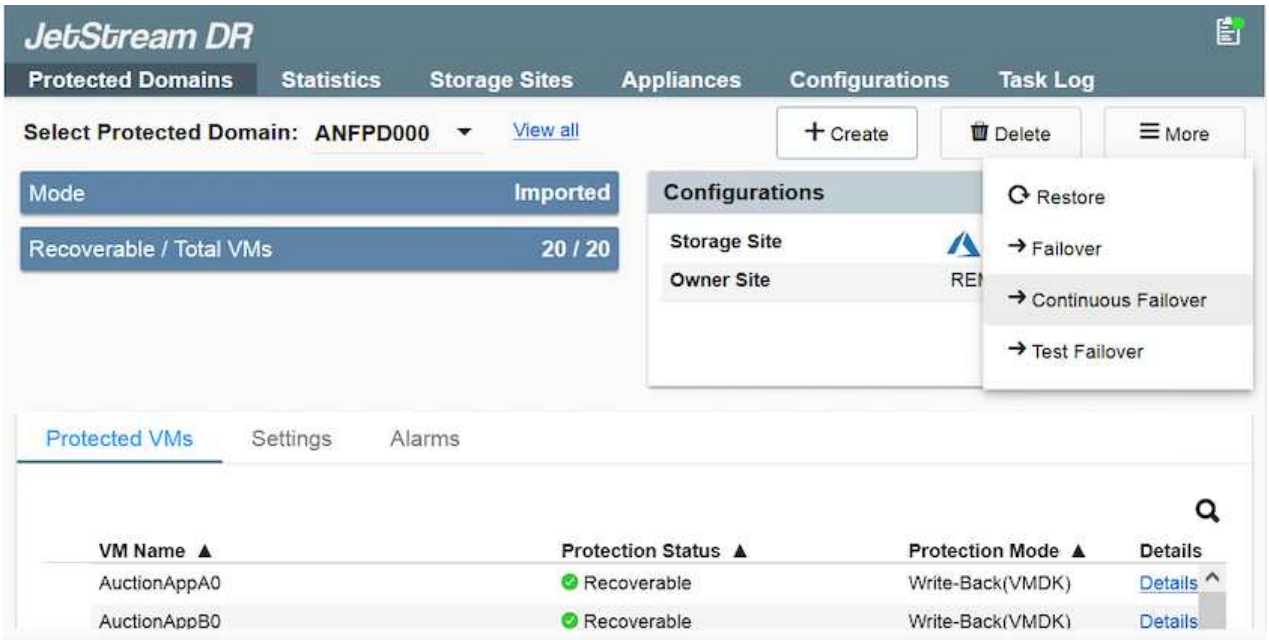
> CPT 생성 계획을 사용하여 이러한 단계를 자동화할 수도 있습니다.

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



선택한 세그먼트에서 DHCP가 활성화되어 있고 사용 가능한 IP가 충분한지 확인합니다. 도메인이 복구되는 동안 동적 IP가 일시적으로 사용됩니다. 복구 중인 각 VM(연속 재수화 포함)에는 개별 동적 IP가 필요합니다. 복구가 완료되면 IP가 해제되고 다시 사용할 수 있습니다.

7. 적절한 페일오버 옵션(무중단 페일오버 또는 페일오버)을 선택합니다. 이 예에서는 연속 재수화(연속 페일오버)가 선택됩니다.



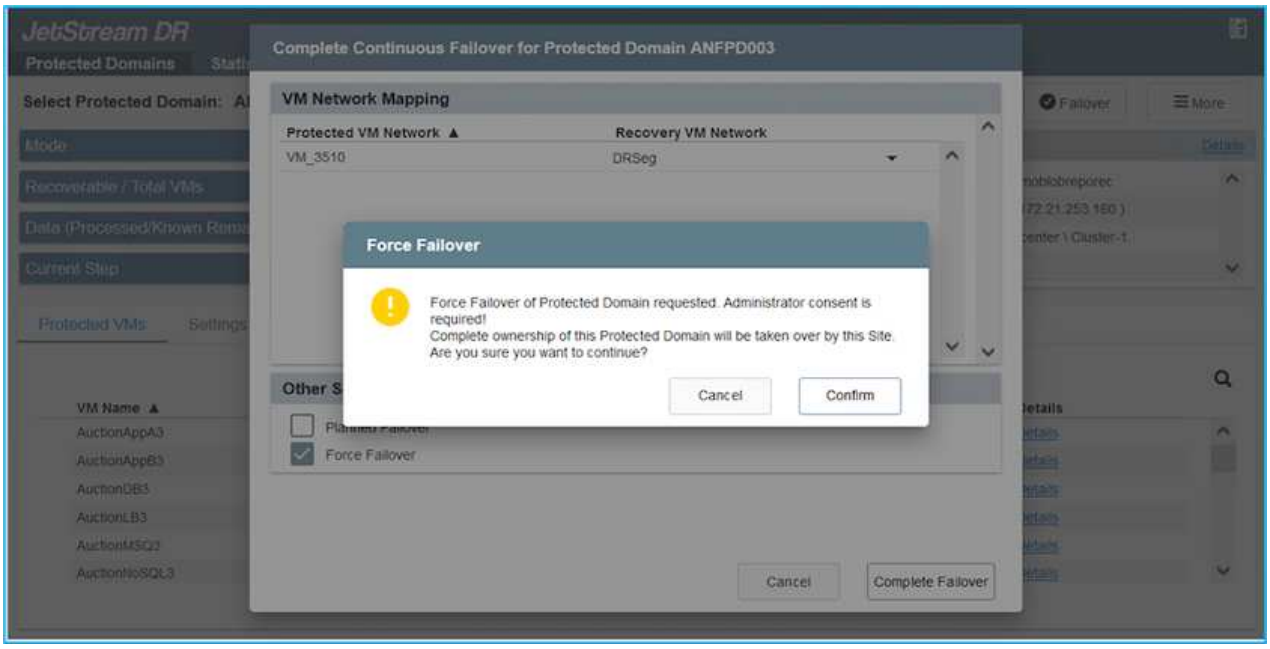
페일오버/페일백 수행

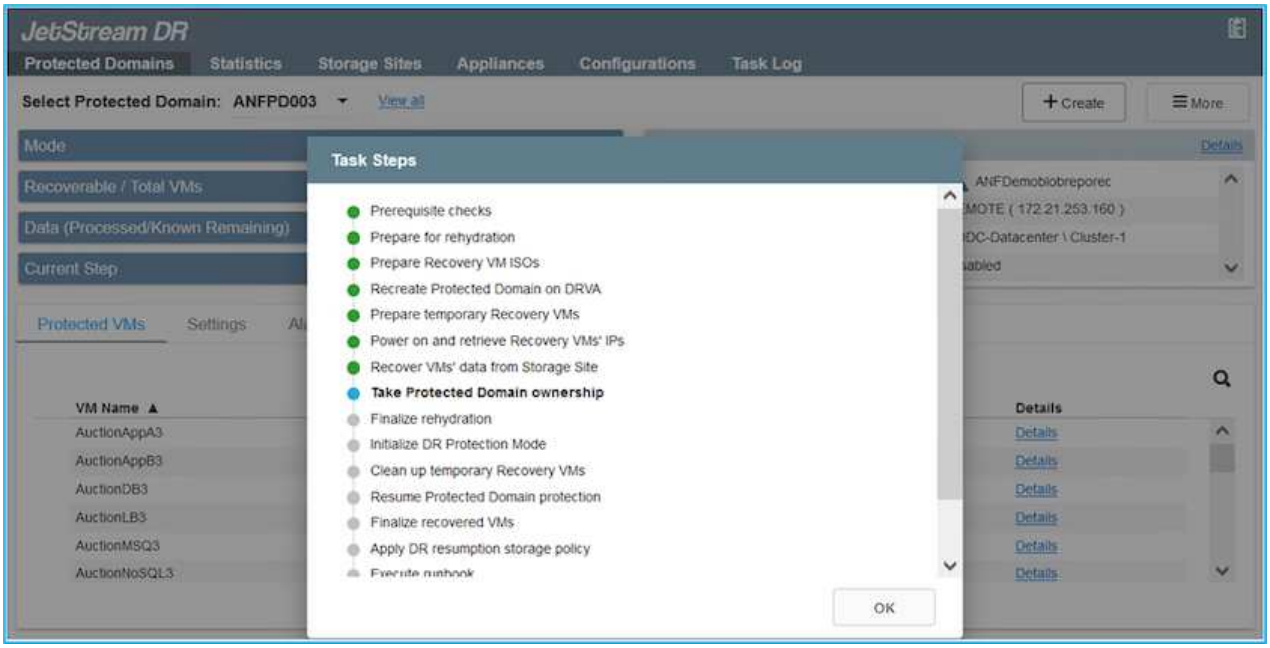
페일오버/페일백 수행 방법

1. 사내 환경의 보호 클러스터에서 재해가 발생한 후(부분 장애 또는 전체 장애) 페일오버를 트리거합니다.

> CPT를 사용하여 Azure Blob Storage에서 AVS 클러스터 복구 사이트로 VM을 복구하는 페일오버 계획을 실행할 수 있습니다.

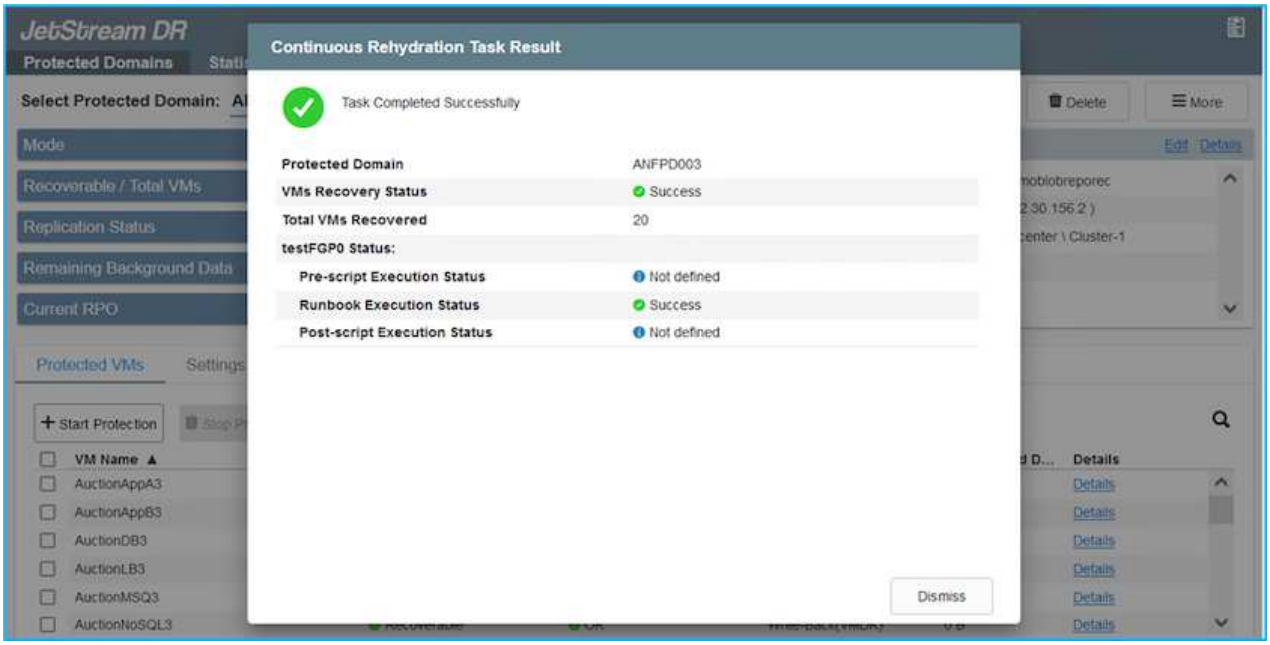
> AVS에서 보호된 VM이 시작될 때 장애 조치(연속 또는 표준 재수화) 후 보호가 자동으로 재개되고 Jetstream DR은 Azure Blob Storage의 해당/원래 컨테이너로 데이터를 계속 복제합니다.





작업 표시줄에 장애 조치 작업의 진행률이 표시됩니다.

2. 작업이 완료되면 복구된 VM에 액세스하고 비즈니스가 정상적으로 계속됩니다.

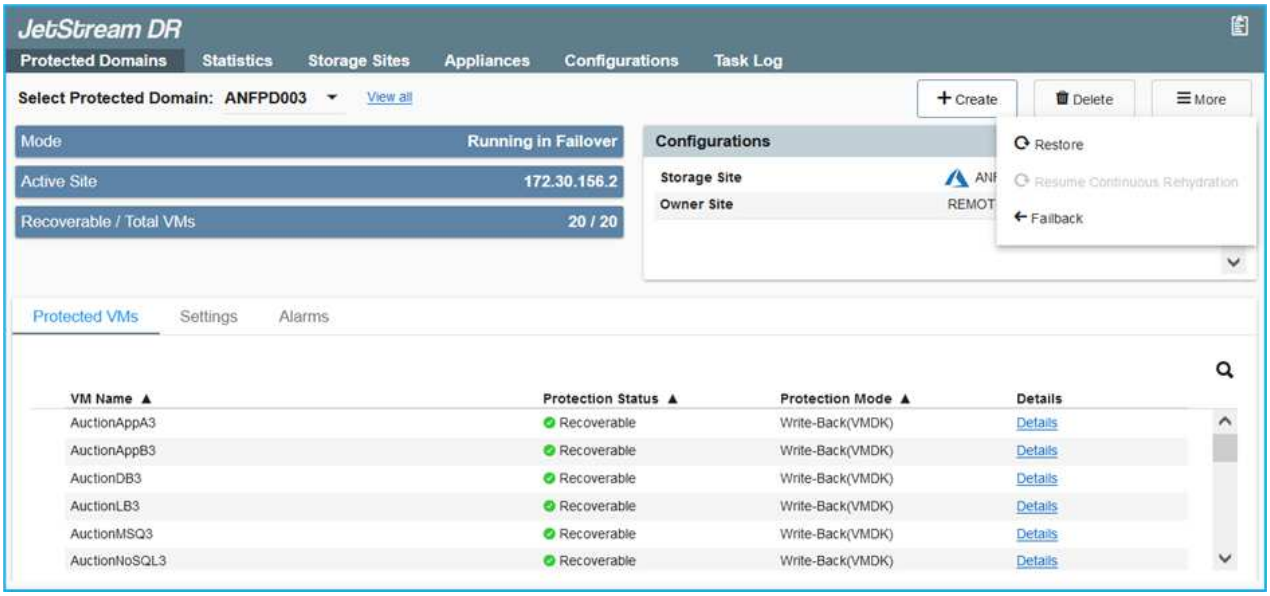


운영 사이트가 다시 가동된 후 페일백을 수행할 수 있습니다. VM 보호가 재개되고 데이터 일관성을 확인해야 합니다.

3. 사내 환경을 복원합니다. 재해 발생 유형에 따라 보호 클러스터의 구성을 복원 및/또는 확인해야 할 수도 있습니다. 필요한 경우 Jetstream DR 소프트웨어를 재설치해야 할 수 있습니다.

> 참고: 자동화 툴킷에 제공된 RECOVERY_UTILITY_Prepare_failback" 스크립트를 사용하여 오래된 VM, 도메인 정보 등의 원래 보호 사이트를 정리할 수 있습니다.

4. 복원된 온프레미스 환경에 액세스하고 Jetstream DR UI로 이동한 다음 적절한 보호 도메인을 선택합니다. 보호 사이트가 페일백될 준비가 되면 UI에서 페일백 옵션을 선택합니다.



CPT에서 생성한 페일백 계획을 사용하여 VM과 해당 데이터를 오브젝트 저장소에서 원래 VMware 환경으로 되돌릴 수도 있습니다.

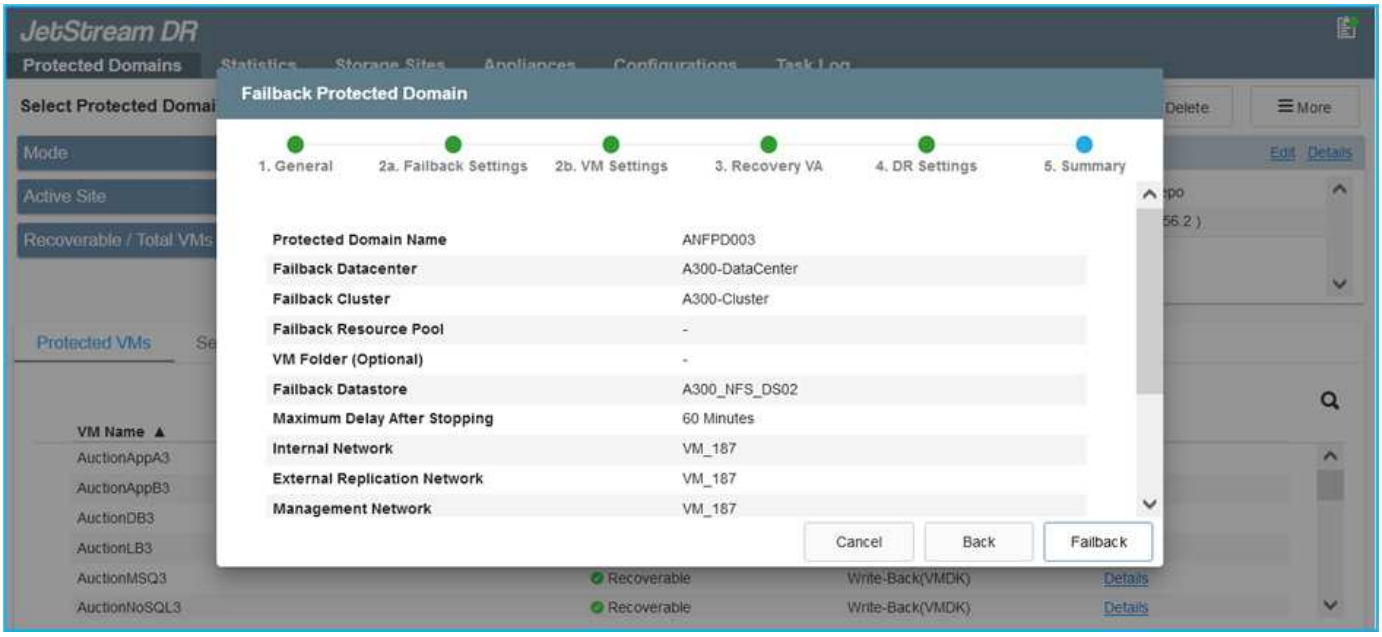
복구 사이트에서 VM을 일시 중지하고 보호 사이트에서 다시 시작한 후 최대 지연 시간을 지정합니다. 여기에는 대체 작동 VM 중지 후 복제 완료, 복구 사이트를 정리하기 위한 시간, 보호 사이트에서 VM을 다시 만드는 시간이 포함됩니다. NetApp이 권장하는 값은 10분입니다.

페일백 프로세스를 완료한 다음 VM 보호 및 데이터 정합성 재개를 확인합니다.

Ransomeware 복구

랜섬웨어에서 복구하는 것은 매우 힘든 작업이 될 수 있습니다. 특히, IT 조직이 안전한 반환 지점을 결정하고 결정된 후에는 복구된 워크로드가 재발생하는 공격으로부터 보호하는 방법(휴면 맬웨어로부터 또는 취약한 응용 프로그램을 통해)을 확인하기 어려울 수 있습니다.

Azure NetApp Files 데이터 저장소와 함께 AVS용 Jetstream DR을 사용하면 조직에서 사용 가능한 시점으로부터 복구할 수 있으므로 필요에 따라 분리된 기능적 네트워크로 워크로드를 복구할 수 있습니다. 복구 기능을 사용하면 애플리케이션이 기능을 수행하고 서로 통신하면서 남북의 트래픽에 노출되지 않도록 함으로써 보안 팀이 법의학 및 기타 필요한 조치를 수행할 수 있는 안전한 장소를 제공할 수 있습니다.



CVO 및 AVS(게스트 연결 스토리지)를 통한 재해 복구

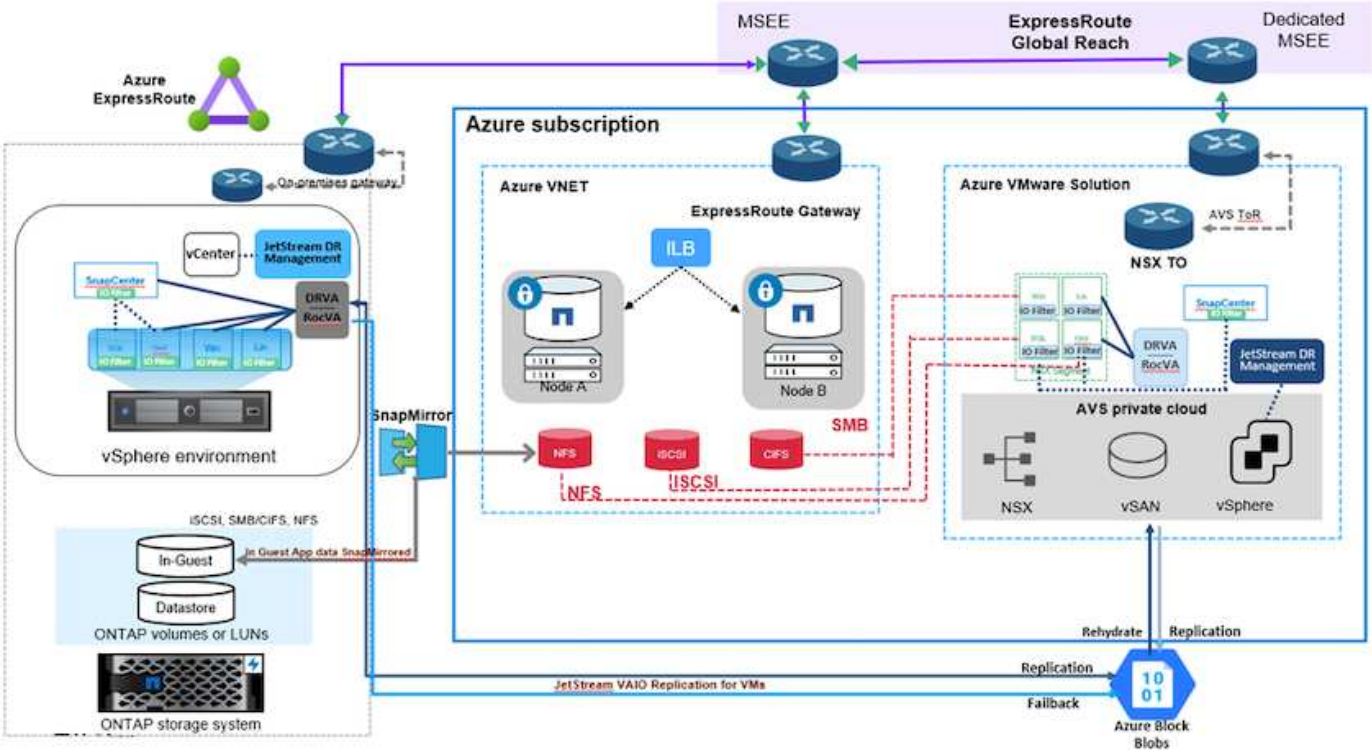
개요

저자: Ravi BCB, Niyaz Mohamed, NetApp

클라우드로 재해 복구는 랜섬웨어 등 사이트 운영 중단 및 데이터 손상 이벤트로부터 워크로드를 보호하는 복원력이 있는 비용 효율적인 방법입니다. NetApp SnapMirror를 사용하면 게스트 연결 스토리지를 사용하는 사내 VMware 워크로드를 Azure에서 실행되는 NetApp Cloud Volumes ONTAP에 복제할 수 있습니다. 여기에는 애플리케이션 데이터가 포함됩니다. 하지만 실제 VM 자체는 어떻습니까? 재해 복구는 가상 머신, VMDK, 애플리케이션 데이터 등을 비롯한 모든 종속 구성 요소를 포함해야 합니다. 이를 위해 Jetstream과 함께 SnapMirror를 사용하면 VM VMDK에

vSAN 스토리지를 사용하는 동시에 사내에서 Cloud Volumes ONTAP로 복제된 워크로드를 원활하게 복구할 수 있습니다.

이 문서에서는 NetApp SnapMirror, Jetstream 및 AVS(Azure VMware Solution)를 사용하여 재해 복구를 설정하고 수행하기 위한 단계별 접근 방식을 제공합니다.



가정

이 문서에서는 애플리케이션 데이터(게스트 연결)를 위한 게스트 내 스토리지에 초점을 두고 사내 환경에서 애플리케이션 정합성 보장 백업을 위해 SnapCenter를 사용하고 있다고 가정합니다.

> 이 문서는 타사 백업 또는 복구 솔루션에 적용됩니다. 환경에 사용된 솔루션에 따라 Best Practice를 따라 조직 SLA를 충족하는 백업 정책을 생성합니다.

온프레미스 환경과 Azure 가상 네트워크 간의 연결을 위해 고속 경로 글로벌 도달 범위 또는 VPN 게이트웨이가 있는 가상 WAN을 사용합니다. 세그먼트는 사내 VLAN 설계를 기반으로 생성해야 합니다.

> 온프레미스 데이터 센터를 Azure에 연결하는 여러 가지 옵션이 있어 이 문서의 특정 워크플로 개요를 볼 수 없습니다. Azure 설명서를 참조하여 적절한 Azure-사내와 Azure 간 연결 방법을 확인하십시오.

DR 솔루션 구축

솔루션 구축 개요

1. 필요한 RPO 요구 사항에 따라 SnapCenter를 사용하여 애플리케이션 데이터를 백업했는지 확인합니다.
2. 적절한 서브스크립션 및 가상 네트워크 내에서 Cloud Manager를 사용하여 올바른 인스턴스 크기로 Cloud Volumes ONTAP를 프로비저닝합니다.

a. 관련 애플리케이션 볼륨에 대해 SnapMirror를 구성합니다.

b. 예약된 작업 후 SnapMirror 업데이트를 트리거하도록 SnapCenter의 백업 정책을 업데이트합니다.

3. Jetstream DR 소프트웨어를 사내 데이터 센터에 설치하고 가상 시스템을 보호합니다.
4. Azure VMware Solution 프라이빗 클라우드에 Jetstream DR 소프트웨어를 설치합니다.
5. 재해 이벤트 중에 Cloud Manager를 사용하여 SnapMirror 관계를 중단시키고 지정된 AVS DR 사이트의 Azure NetApp Files 또는 vSAN 데이터스토어로 가상 시스템의 페일오버를 트리거합니다.

   a. 애플리케이션 VM에 대한 iSCSI LUN 및 NFS 마운트를 다시 연결합니다.

6. 운영 사이트가 복구된 후 SnapMirror를 다시 동기화하여 보호 사이트에 대한 페일백을 호출합니다.

배포 세부 정보

Azure에서 **CVO**를 구성하고 볼륨을 **CVO**로 복제합니다

첫 번째 단계는 Azure에서 Cloud Volumes ONTAP를 구성하는 것입니다 ("링크")를 사용하여 원하는 볼륨을 Cloud Volumes ONTAP에 복제하고 원하는 빈도와 스냅샷 보존 기능을 사용할 수 있습니다.

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 호스트 및 **CVO** 데이터 액세스를 구성합니다

SDDC를 구축할 때 고려해야 할 두 가지 중요한 요소는 Azure VMware 솔루션에서 SDDC 클러스터의 크기와 SDDC를 사용할 수 있는 기간을 결정하는 것입니다. 재해 복구 솔루션의 두 가지 주요 고려 사항은 전체 운영 비용을 절감하는 데 도움이 됩니다. SDDC는 최대 3개의 호스트까지 구성할 수 있으며, 전체 구축 환경에서 다중 호스트 클러스터까지 가능합니다.

AVS 클러스터의 구축 결정은 주로 RPO/RTO 요구 사항을 기반으로 합니다. Azure VMware 솔루션을 사용하면 SDDC를 테스트 또는 실제 재해 이벤트에 대비하여 적시에 프로비저닝할 수 있습니다. SDDC를 적시에 구축하면 재해 발생 시 ESXi 호스트 비용을 절감할 수 있습니다. 그러나 이러한 구축 형태는 SDDC를 프로비저닝하는 동안 RTO에 몇 시간 정도 영향을 줍니다.

가장 일반적인 구축 옵션은 SDDC를 상시 작동, 파일럿 라이트 모드로 실행하는 것입니다. 이 옵션은 항상 사용 가능한 호스트 세 개로 구성된 작은 공간을 제공하며 시뮬레이션 활동 및 규정 준수 검사를 위한 실행 기준을 제공하여 복구 작업 속도를 높이고 운영 사이트와 DR 사이트 간의 운영 드리프트가 발생하지 않도록 합니다. 실제 DR 이벤트를 처리하는 데 필요한 경우 파일럿 라이트 클러스터를 원하는 레벨로 신속하게 확장할 수 있습니다.

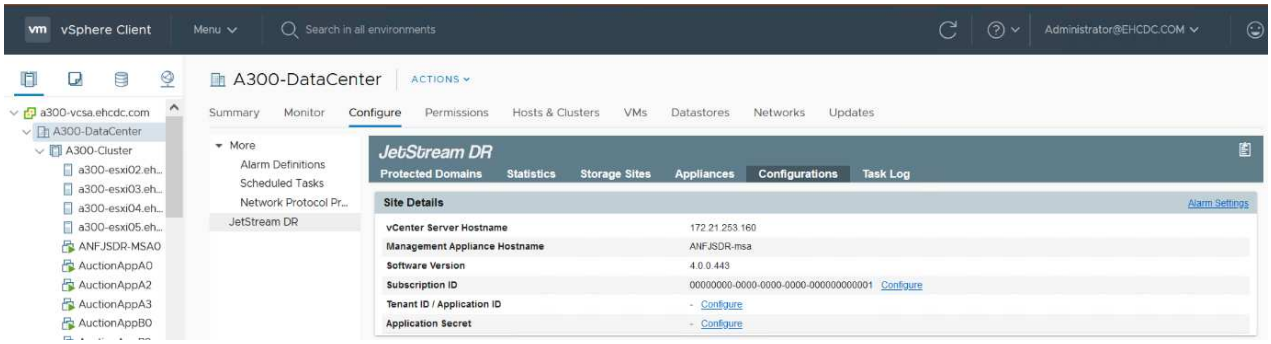
AVS SDDC를 구성하려면(온디맨드 또는 파일럿 라이트 모드여야 함) 을 참조하십시오 "Azure에서 가상화 환경을 구축하고 구성합니다". 사전 요구 사항으로, 연결이 설정된 후 AVS 호스트에 상주하는 게스트 VM이 Cloud Volumes ONTAP의 데이터를 사용할 수 있는지 확인합니다.

Cloud Volumes ONTAP 및 AVS를 올바르게 구성한 후에는 VAIO 메커니즘을 사용하고 Cloud Volumes ONTAP에 애플리케이션 볼륨 복사본을 위한 SnapMirror를 활용하여 Jetstream을 구성하여 온프레미스 워크로드를 AVS(게스트 내 스토리지가 있는 응용 프로그램 VMDK 및 VM이 있는 VM)로 자동으로 복구합니다.

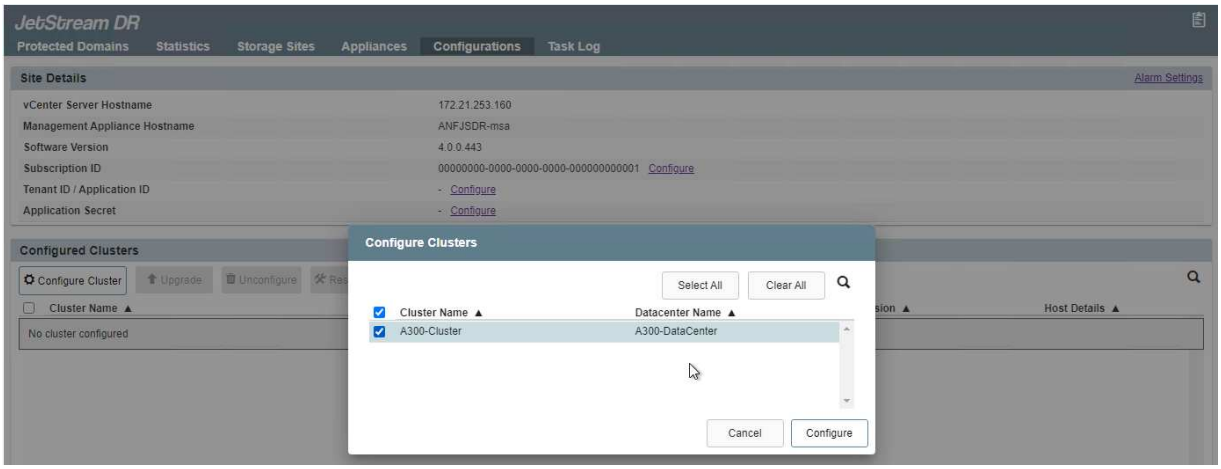
사내 데이터 센터에 **Jetstream DR**을 설치합니다

Jetstream DR 소프트웨어는 Jetstream DR Management Server Virtual Appliance(MSA), DR 가상 어플라이언스(DRVA) 및 호스트 구성 요소(I/O 필터 패키지)의 세 가지 주요 구성 요소로 구성됩니다. MSA는 컴퓨팅 클러스터에 호스트 구성 요소를 설치 및 구성한 다음 Jetstream DR 소프트웨어를 관리하는 데 사용됩니다. 설치 프로세스는 다음과 같습니다.

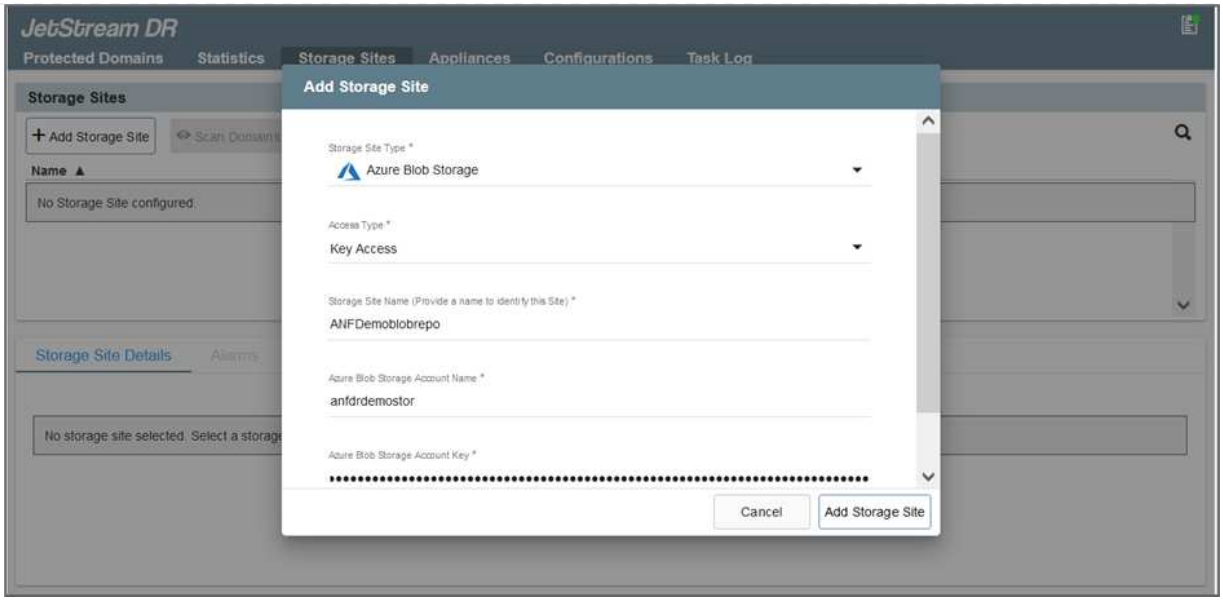
1. 필수 구성 요소를 확인하십시오.
2. 리소스 및 구성 권장 사항에 대해 용량 계획 툴을 실행합니다.
3. Jetstream DR MSA를 지정된 클러스터의 각 vSphere 호스트에 구축합니다.
4. 브라우저에서 DNS 이름을 사용하여 MSA를 실행합니다.
5. MSA에 vCenter Server를 등록합니다.
6. Jetstream DR MSA를 구축하고 vCenter Server를 등록한 후 vSphere Web Client를 사용하여 Jetstream DR 플러그인으로 이동합니다. 이 작업은 데이터 센터 > 구성 > Jetstream DR로 이동하여 수행할 수 있습니다.



7. Jetstream DR 인터페이스에서 다음 작업을 완료합니다.
   a. I/O 필터 패키지를 사용하여 클러스터를 구성합니다.

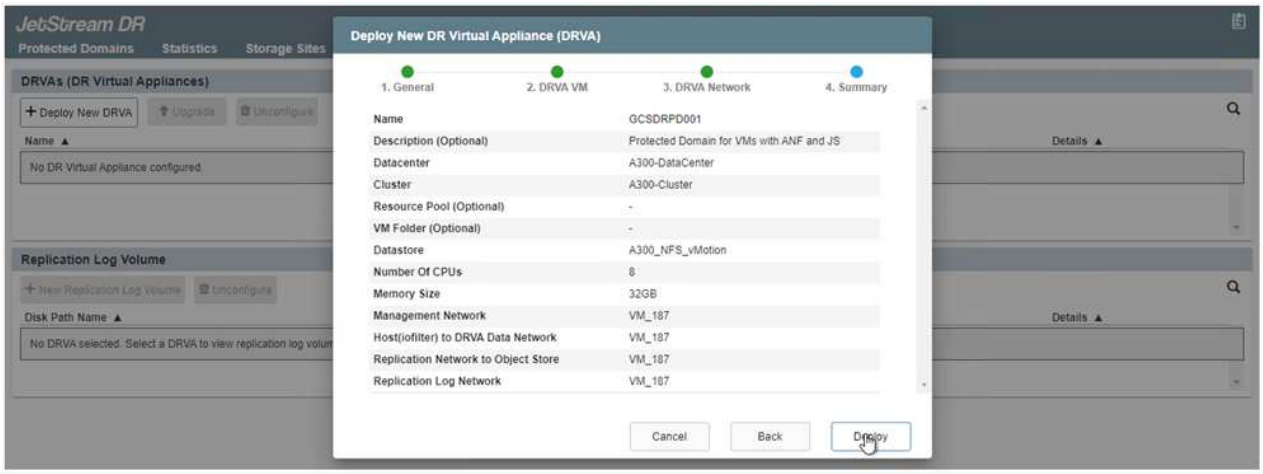


   b. 복구 사이트에 있는 Azure Blob 저장소를 추가합니다.

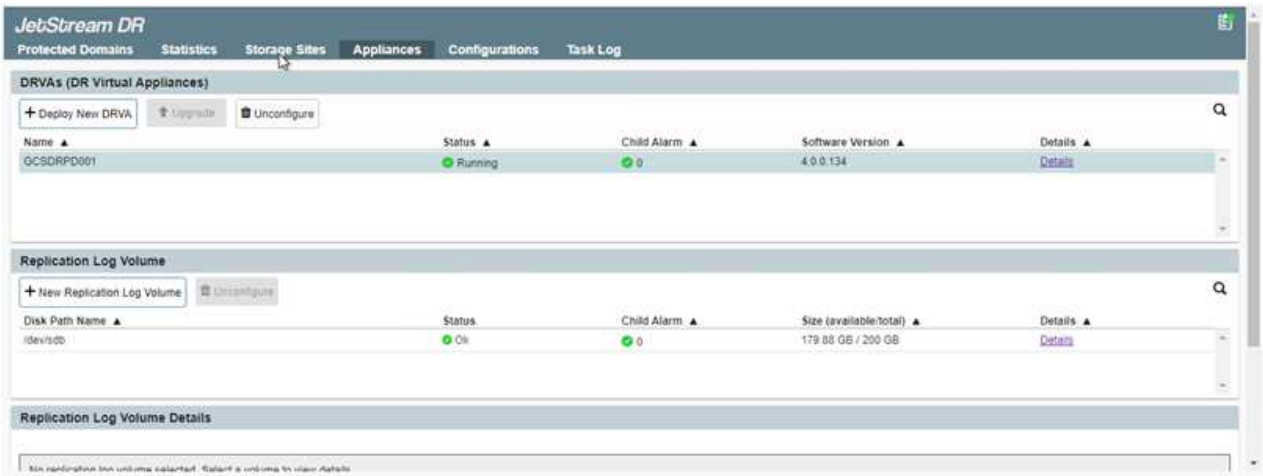


8. Appliances 탭에서 필요한 수의 DR 가상 어플라이언스(DRVA)를 구축합니다.

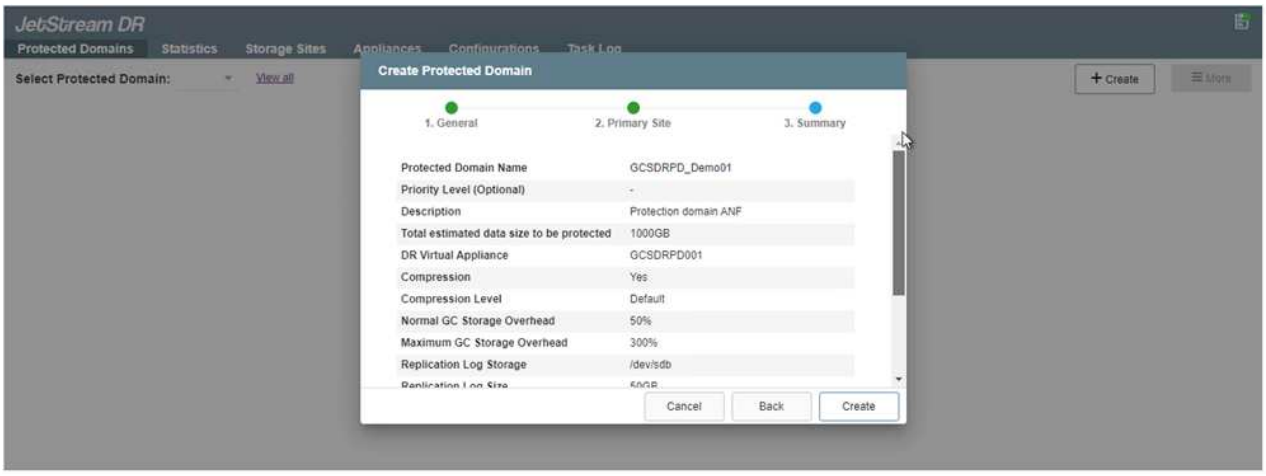
> 용량 계획 툴을 사용하여 필요한 DRVA의 수를 추정합니다.

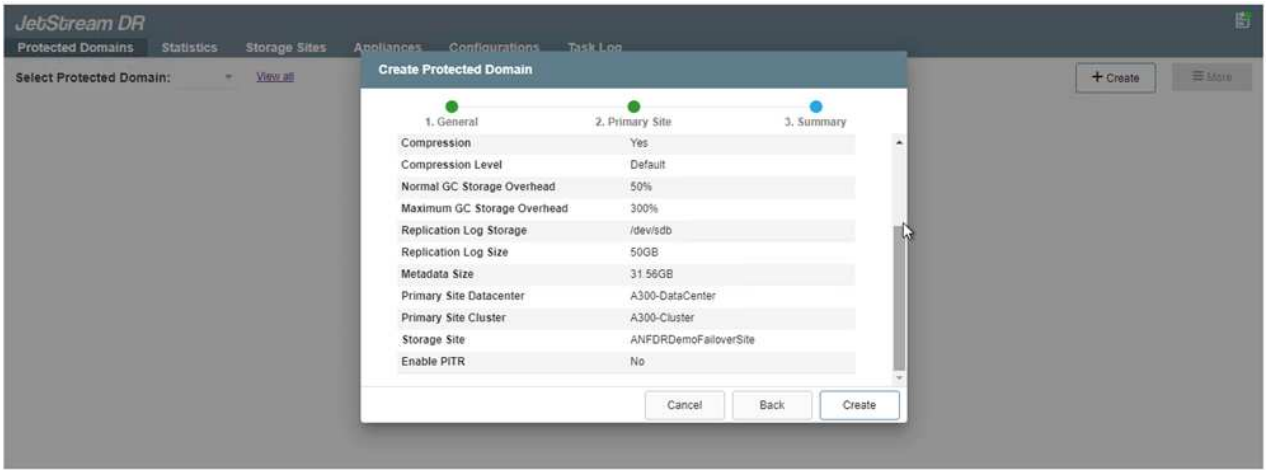


9. 사용 가능한 데이터 저장소 또는 독립 공유 iSCSI 스토리지 풀에서 VMDK를 사용하여 각 DRVA에 대한 복제 로그 볼륨을 생성합니다.



10. 보호 도메인 탭에서 Azure Blob 저장소 사이트, DRVA 인스턴스 및 복제 로그에 대한 정보를 사용하여 필요한 수의 보호된 도메인을 만듭니다. 보호 도메인은 함께 보호되고 장애 조치/장애 복구 작업에 우선 순위 순서를 할당하는 클러스터 내의 특정 VM 또는 애플리케이션 VM 세트를 정의합니다.

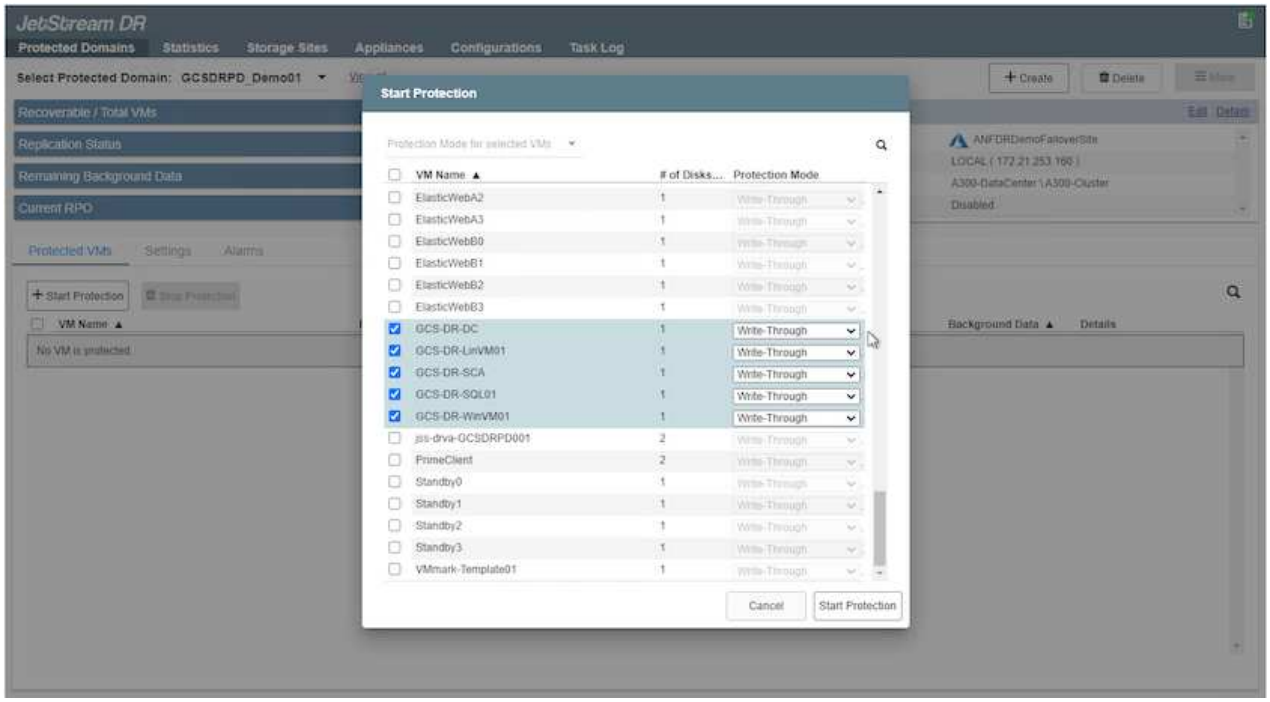




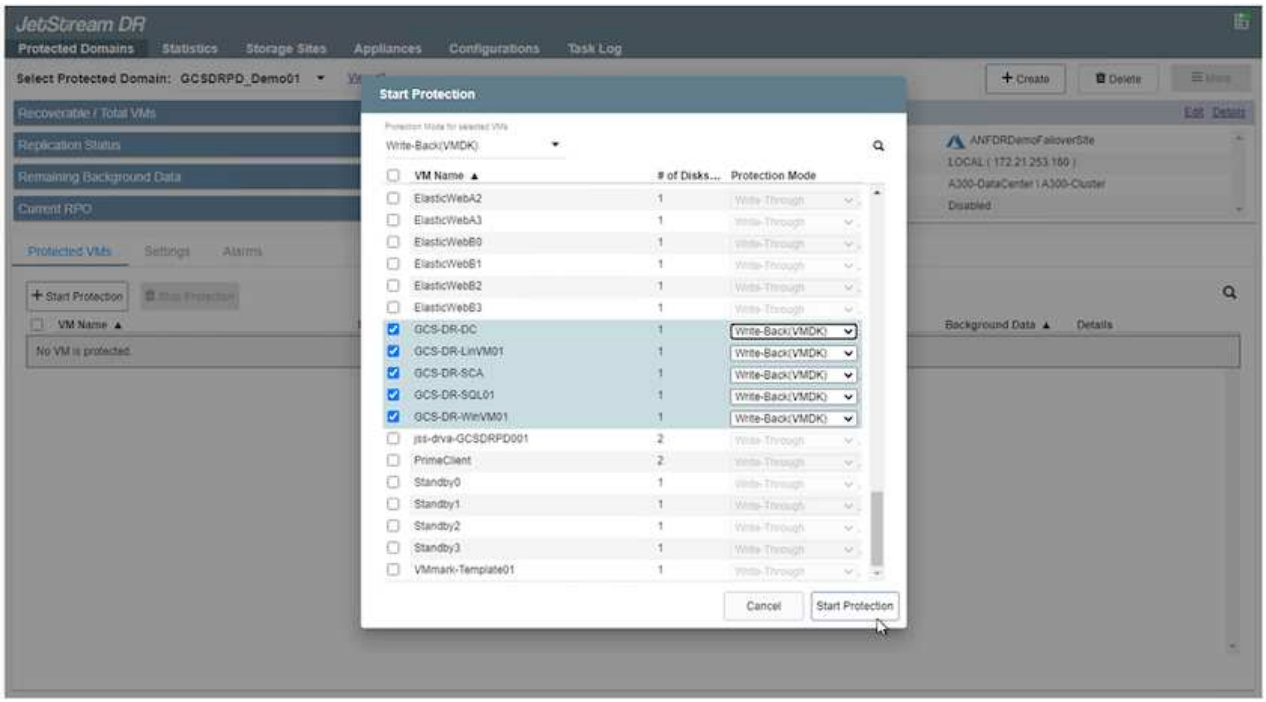
11. 보호할 VM을 선택하고 종속성을 기반으로 VM을 애플리케이션 그룹으로 그룹화합니다. 애플리케이션 정의를 사용하면 VM 세트를 부팅 순서, 부팅 지연 및 복구 시 실행할 수 있는 선택적 애플리케이션 검증을 포함하는 논리 그룹으로 그룹화할 수 있습니다.

> ⓘ 보호 도메인의 모든 VM에 동일한 보호 모드가 사용되는지 확인합니다.

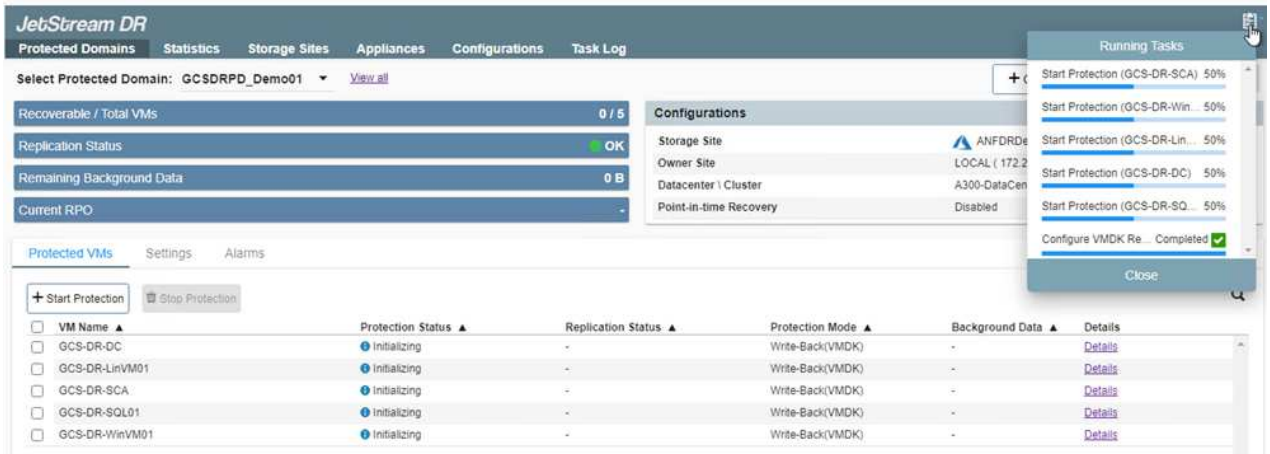
VMDK(Write-Back) 모드는 더 높은 성능을 제공합니다.



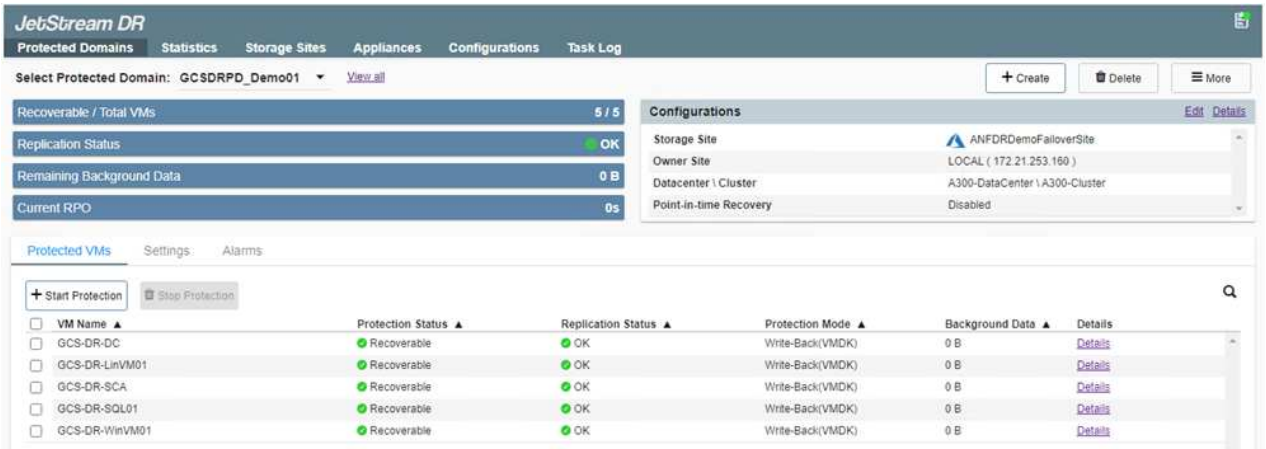
12. 복제 로그 볼륨이 고성능 스토리지에 배치되었는지 확인합니다.



13. 작업을 완료한 후 보호 도메인에 대한 보호 시작 을 클릭합니다. 그러면 선택한 VM에 대한 데이터 복제가 지정된 Blob 저장소로 시작됩니다.



14. 복제가 완료되면 VM 보호 상태가 복구 가능으로 표시됩니다.

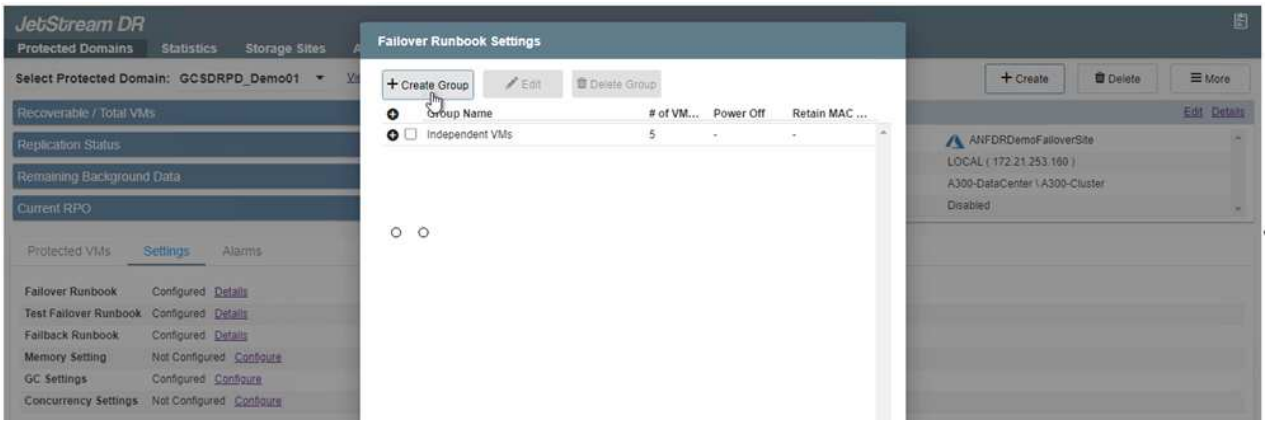


> 페일오버 런북은 VM(복구 그룹이라고 함)을 그룹화하고 부팅 순서 시퀀스를 설정하고 IP 구성과 함께 CPU/메모리 설정을 수정하도록 구성할 수 있습니다.

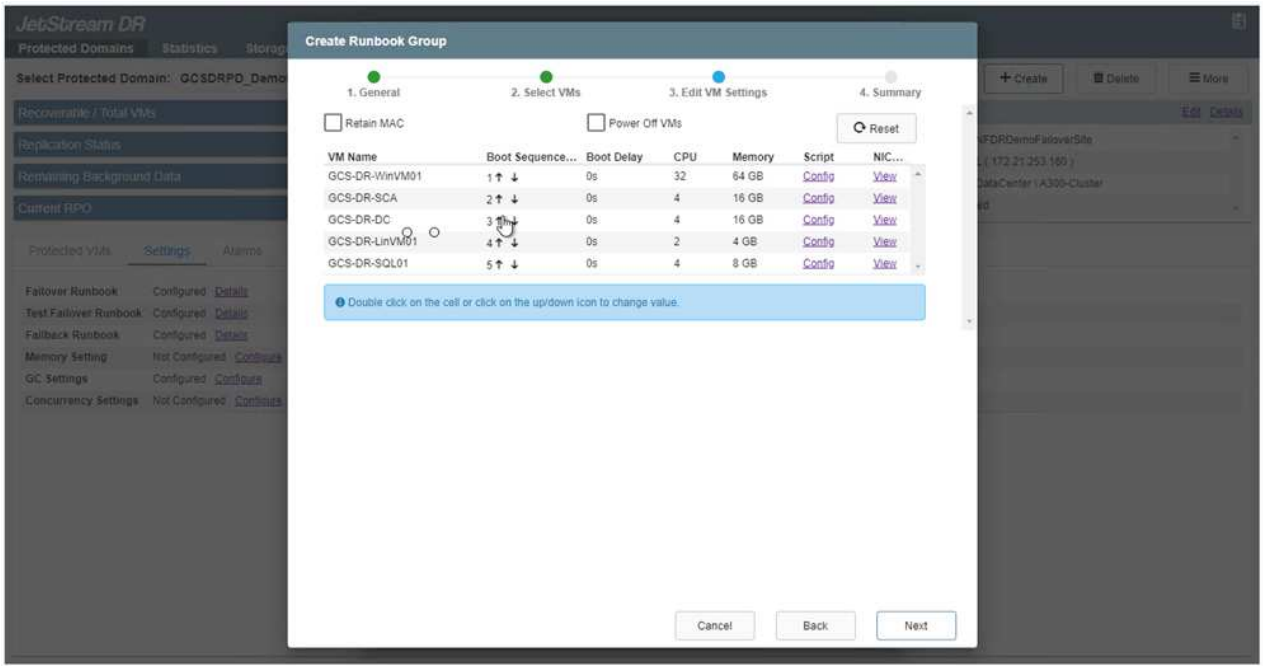
15. 설정 을 클릭한 다음 Runbook 구성 링크를 클릭하여 Runbook 그룹을 구성합니다.

16. 새 Runbook 그룹을 생성하려면 Create Group 버튼을 클릭합니다.

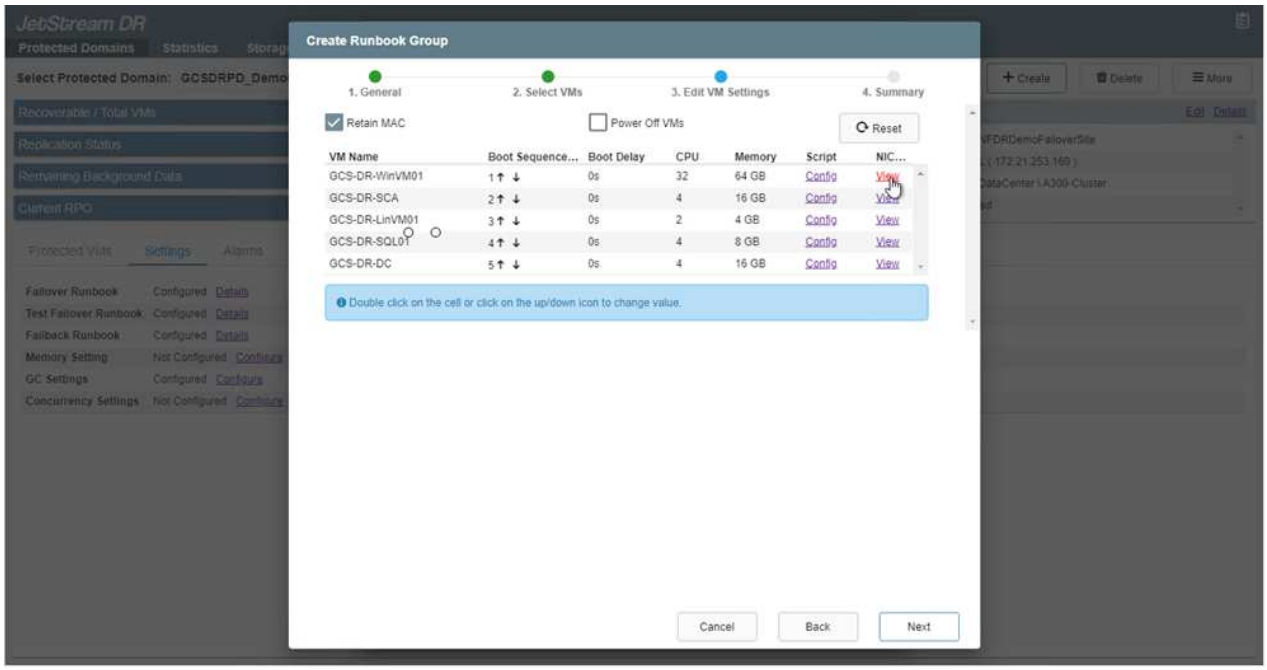
필요한 경우 화면 아래쪽에 사용자 지정 사전 스크립트 및 사후 스크립트를 적용하여 Runbook 그룹의 작업 전후에 자동으로 실행합니다. Runbook 스크립트가 관리 서버에 있는지 확인합니다.



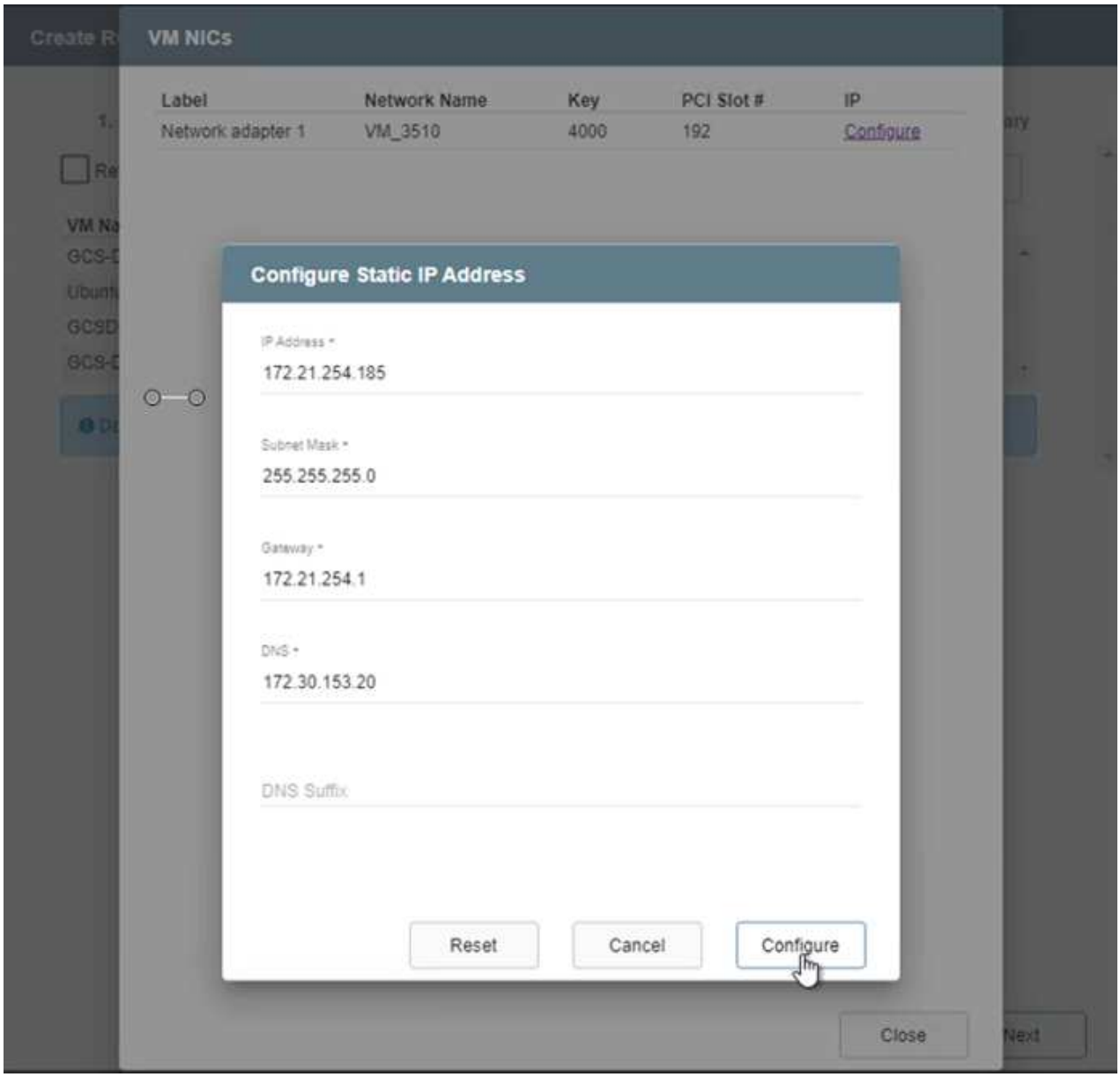
17. 필요에 따라 VM 설정을 편집합니다. 부팅 순서, 부팅 지연(초 단위로 지정), CPU 수 및 할당할 메모리 양을 포함하여 VM을 복구하기 위한 매개 변수를 지정합니다. 위쪽 또는 아래쪽 화살표를 클릭하여 VM의 부팅 순서를 변경합니다. MAC를 유지하기 위한 옵션도 제공됩니다.

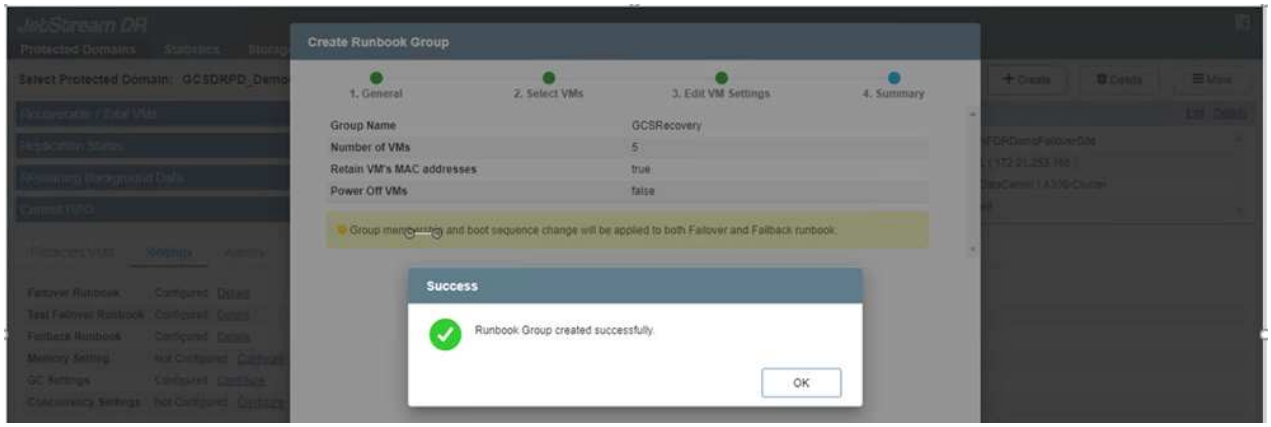


18. 정적 IP 주소는 그룹의 개별 VM에 대해 수동으로 구성할 수 있습니다. VM의 NIC View 링크를 클릭하여 IP 주소 설정을 수동으로 구성합니다.



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





이제 페일오버 및 페일백 Runbook의 상태가 모두 Configured로 표시됩니다. 페일오버 및 페일백 Runbook 그룹은 동일한 초기 VM 및 설정 그룹을 사용하여 쌍으로 생성됩니다. 필요한 경우 각 Runbook 그룹의 세부 정보 링크를 클릭하고 설정을 변경하여 Runbook 그룹의 설정을 개별적으로 사용자 지정할 수 있습니다.

프라이빗 클라우드에 **AVS**용 **Jetstream DR**을 설치합니다

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

- 대상 네트워킹 세그먼트, 방화벽, DHCP 및 DNS 등의 서비스 등
- AVS용 Jetstream DR 설치
- 데이터 저장소 등을 사용하여 ANF 볼륨 구성

Jetstream DR은 미션 크리티컬 도메인에 대해 제로급 RTO 모드를 지원합니다. 이러한 도메인의 경우 대상 스토리지가 사전 설치되어 있어야 합니다. ANF는 이 경우 권장되는 스토리지 유형입니다.

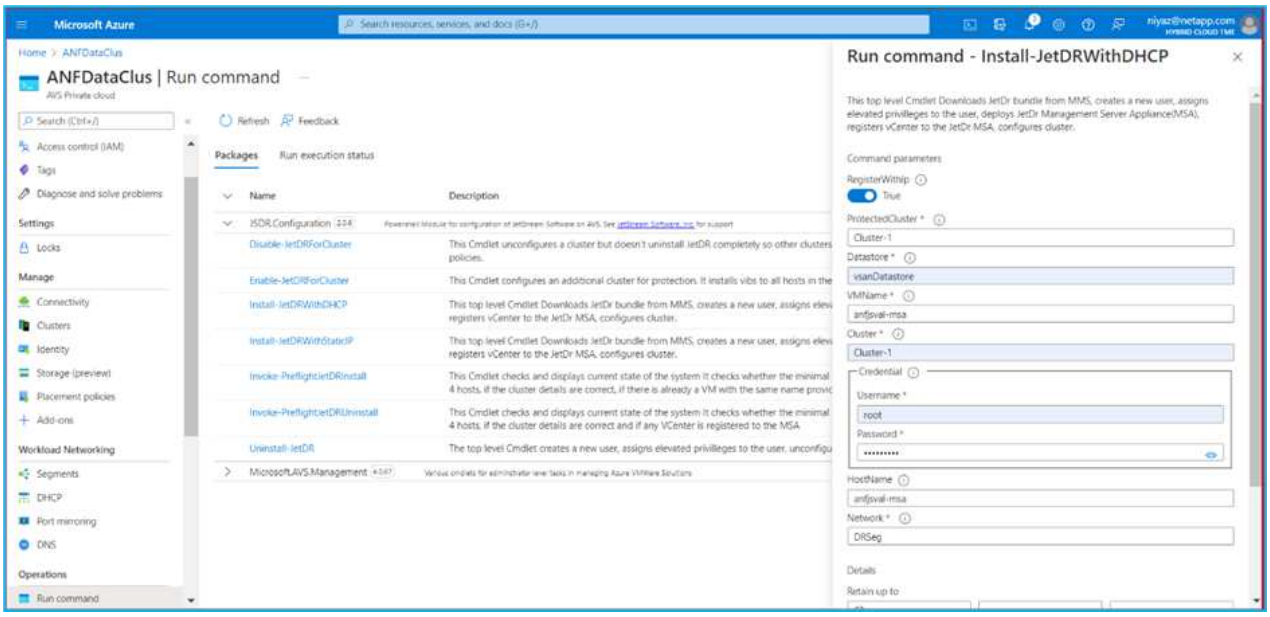
> 세그먼트 생성을 포함한 네트워크 구성은 AVS 클러스터에서 사내 요구 사항과 일치하도록 구성해야 합니다.

> SLA 및 RTO 요구 사항에 따라 연속 페일오버 또는 일반(표준) 페일오버 모드를 사용할 수 있습니다. 제로급 RTO의 경우 복구 사이트에서 연속 재수화를 시작해야 합니다.

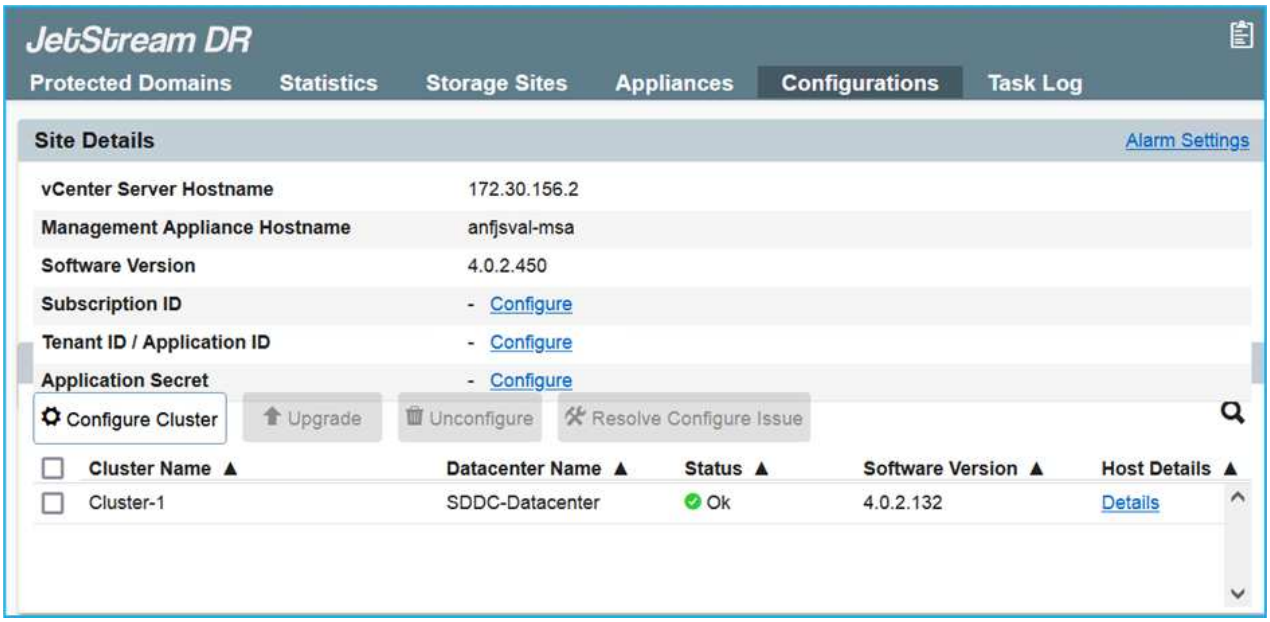
1. Azure VMware 솔루션 프라이빗 클라우드에 AVS용 Jetstream DR을 설치하려면 실행 명령을 사용하십시오. Azure 포털에서 Azure VMware 솔루션으로 이동하고 프라이빗 클라우드를 선택한 다음 명령 실행 > 패키지 > JSDR.Configuration을 선택합니다.

   > Azure VMware 솔루션의 기본 CloudAdmin 사용자는 AVS용 Jetstream DR을 설치할 권한이 없습니다. Azure VMware 솔루션을 사용하면 Jetstream DR용 Azure VMware 솔루션 실행 명령을 호출하여 Jetstream DR을 간단하고 자동으로 설치할 수 있습니다.

   다음 스크린샷은 DHCP 기반 IP 주소를 사용한 설치를 보여 줍니다.

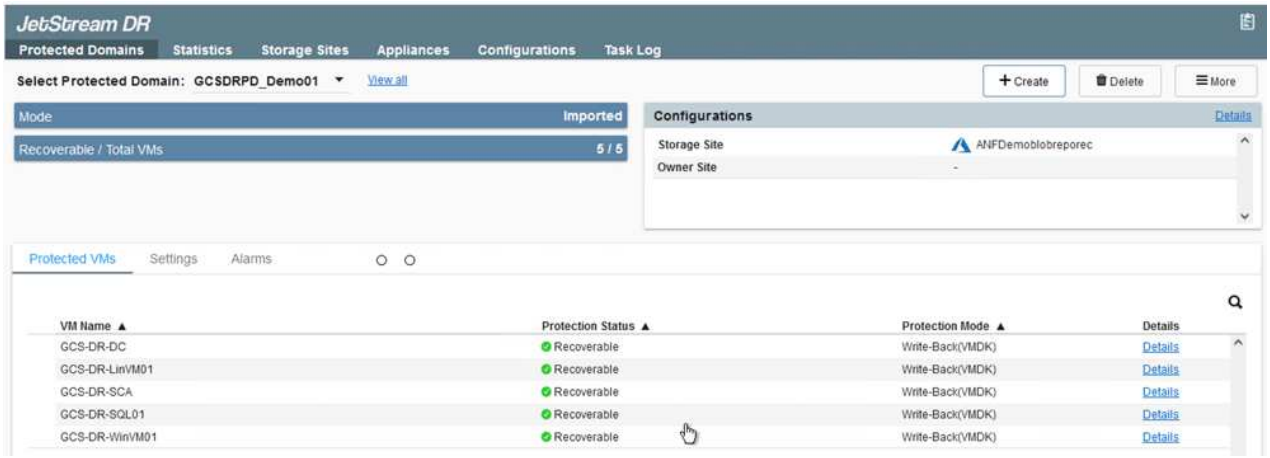


2. AVS 설치를 위한 Jetstream DR이 완료되면 브라우저를 새로 고칩니다. Jetstream DR UI에 액세스하려면 SDDC 데이터 센터 > 구성 > Jetstream DR로 이동하십시오.



3. Jetstream DR 인터페이스에서 다음 작업을 완료합니다.
   a. 온-프레미스 클러스터를 저장소 사이트로 보호하는 데 사용된 Azure Blob 저장소 계정을 추가한 다음 도메인 검사 옵션을 실행합니다.
   b. 나타나는 팝업 대화 상자에서 가져올 보호된 도메인을 선택한 다음 해당 가져오기 링크를 클릭합니다.

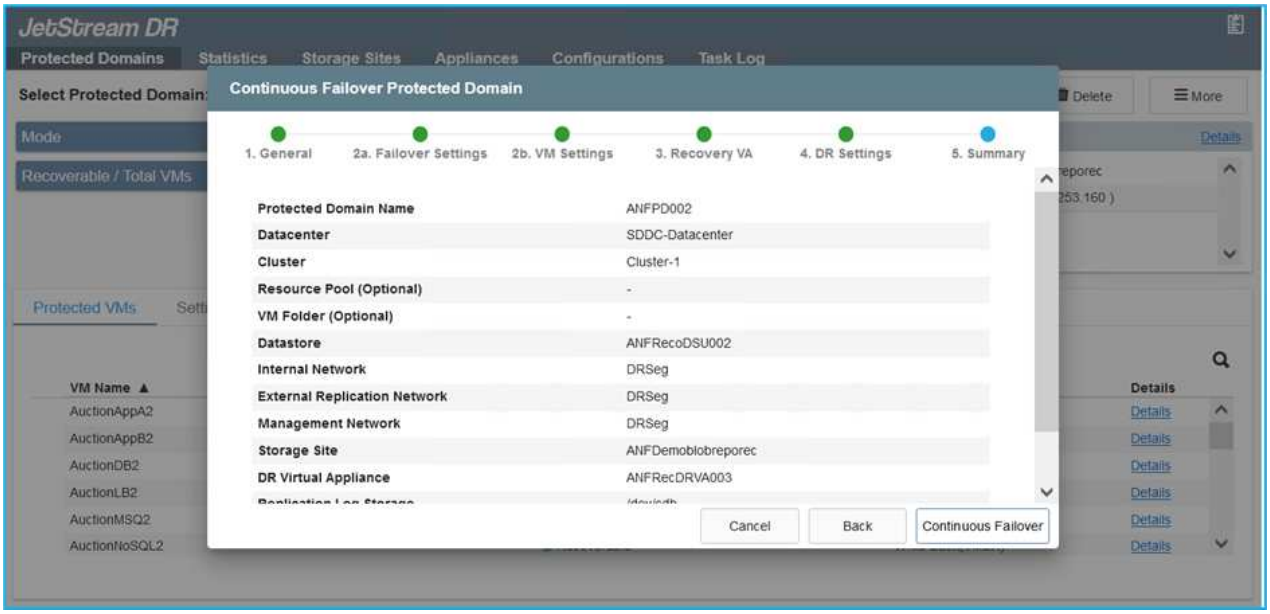
4. 복구를 위해 도메인을 가져옵니다. 보호 도메인 탭으로 이동하여 원하는 도메인이 선택되었는지 확인하거나 보호 도메인 선택 메뉴에서 원하는 도메인을 선택합니다. 보호된 도메인에 있는 복구 가능한 VM 목록이 표시됩니다.



5. 보호된 도메인을 가져온 후 DRVA 어플라이언스를 구축합니다.

> CPT 생성 계획을 사용하여 이러한 단계를 자동화할 수도 있습니다.

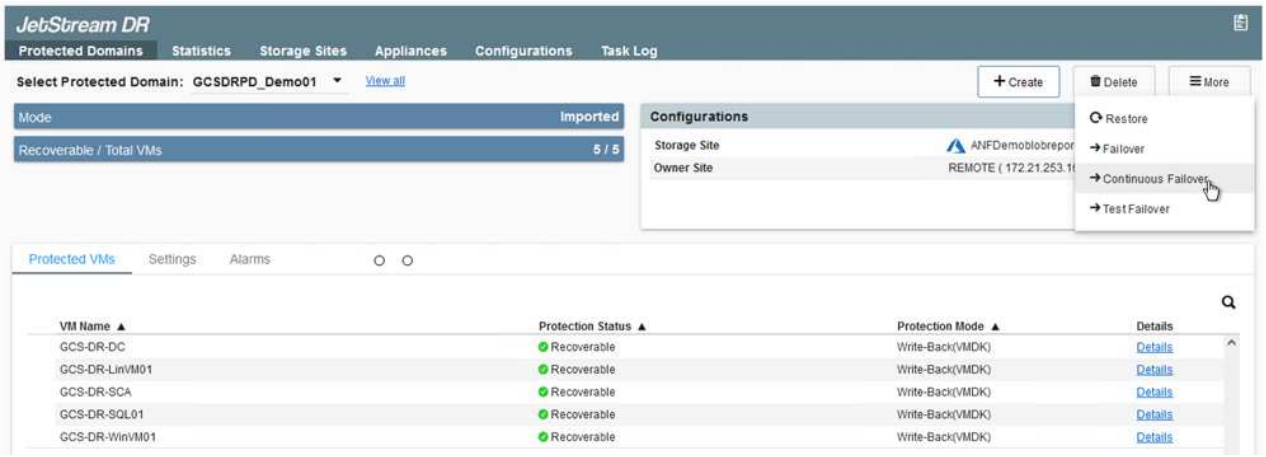
6. 사용 가능한 vSAN 또는 ANF 데이터 저장소를 사용하여 복제 로그 볼륨을 생성합니다.
7. 보호된 도메인을 가져오고 VM 배치에 ANF 데이터 저장소를 사용하도록 복구 VA를 구성합니다.



> 선택한 세그먼트에서 DHCP가 활성화되어 있고 사용 가능한 IP가 충분한지 확인합니다. 도메인이 복구되는 동안 동적 IP가 일시적으로 사용됩니다. 복구 중인 각 VM(연속 재수화 포함)에는 개별 동적 IP가 필요합니다. 복구가 완료되면 IP가 해제되고 다시 사용할 수 있습니다.

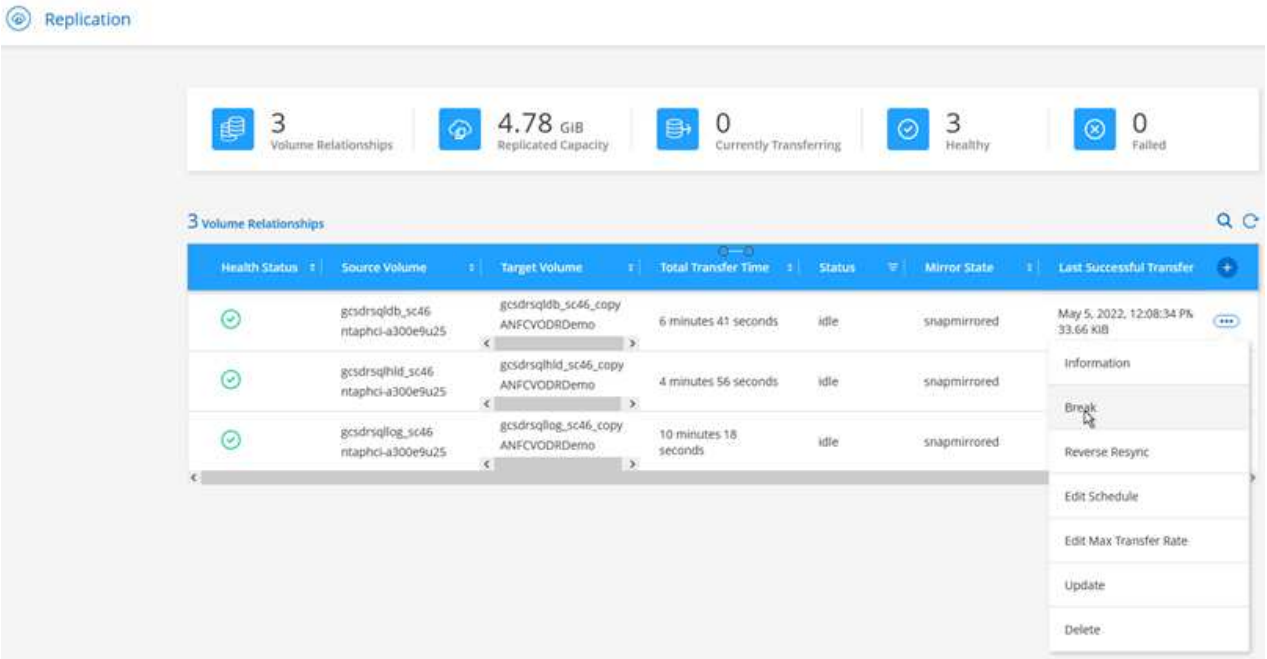
8. 적절한 페일오버 옵션(무중단 페일오버 또는 페일오버)을 선택합니다. 이 예에서는 연속 재수화(연속 페일오버)가 선택됩니다.

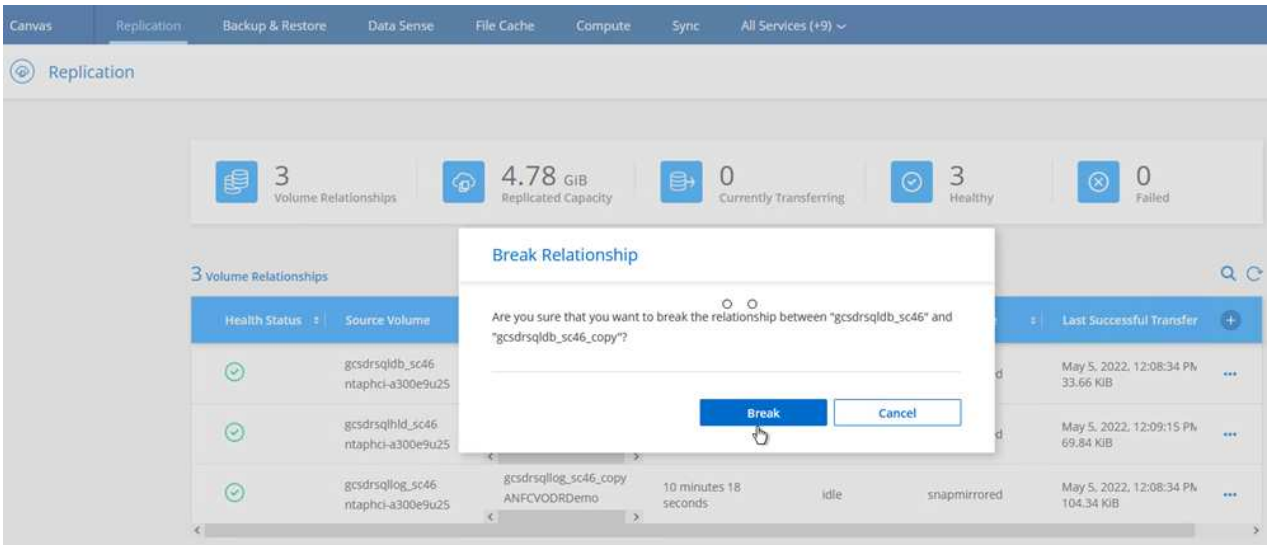
> 연속 페일오버 모드와 페일오버 모드는 구성이 수행될 때 다르지만, 두 페일오버 모드는 동일한 단계를 사용하여 구성됩니다. 장애 조치 단계는 재해 이벤트에 따라 함께 구성 및 수행됩니다. 지속적인 페일오버는 언제든지 구성할 수 있으며, 이후 정상적인 시스템 작동 중에 백그라운드에서 실행될 수 있습니다. 재해 이벤트가 발생한 후 지속적인 페일오버가 완료되어 보호된 VM의 소유권을 복구 사이트로 즉시 전송합니다(제로급 RTO).



지속적인 장애 조치 프로세스가 시작되고 UI에서 진행 상태를 모니터링할 수 있습니다. 현재 단계 섹션에서 파란색 아이콘을 클릭하면 페일오버 프로세스의 현재 단계에 대한 세부 정보를 보여주는 팝업 창이 표시됩니다.

1. 사내 환경의 보호된 클러스터에서 재해가 발생한 후(일부 또는 전체 장애) 해당 애플리케이션 볼륨에 대한 SnapMirror 관계를 끊은 후 Jetstream을 사용하여 VM에 대한 페일오버를 트리거할 수 있습니다.

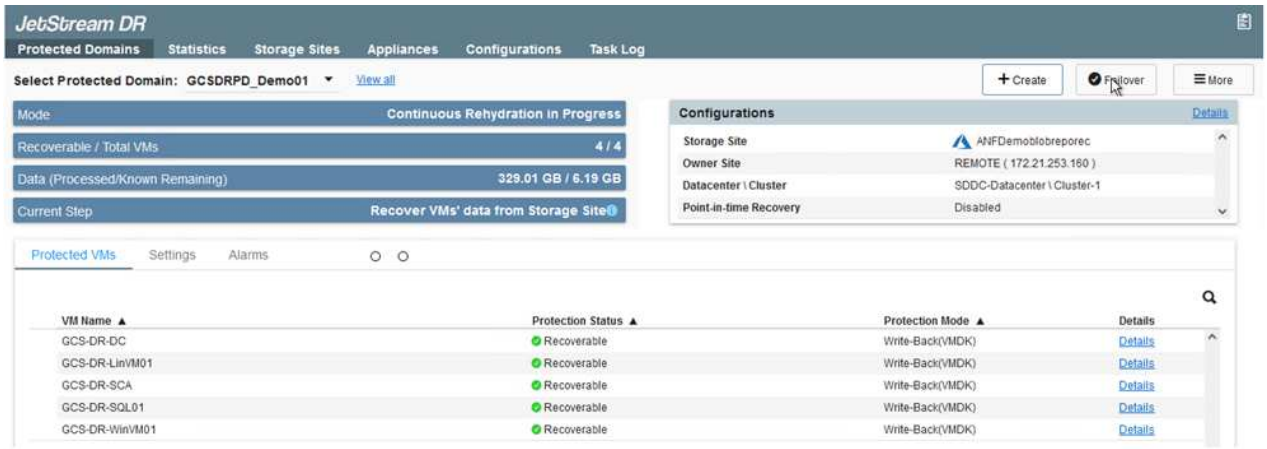


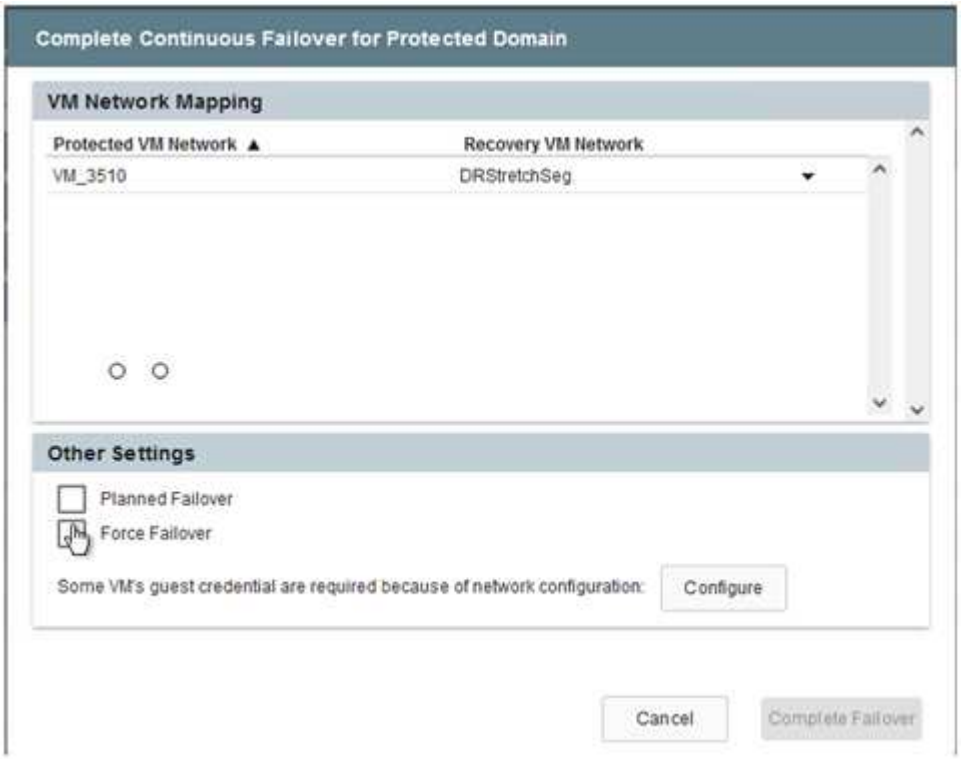


> 이 단계는 복구 프로세스를 용이하게 하기 위해 쉽게 자동화할 수 있습니다.

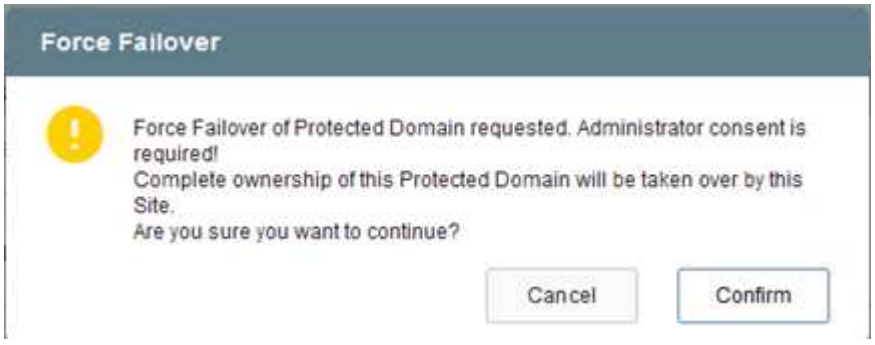
2. AVS SDDC(대상 측)에서 Jetstream UI에 액세스하고 페일오버 옵션을 트리거하여 페일오버를 완료합니다. 작업 표시줄에 장애 조치 작업의 진행률이 표시됩니다.

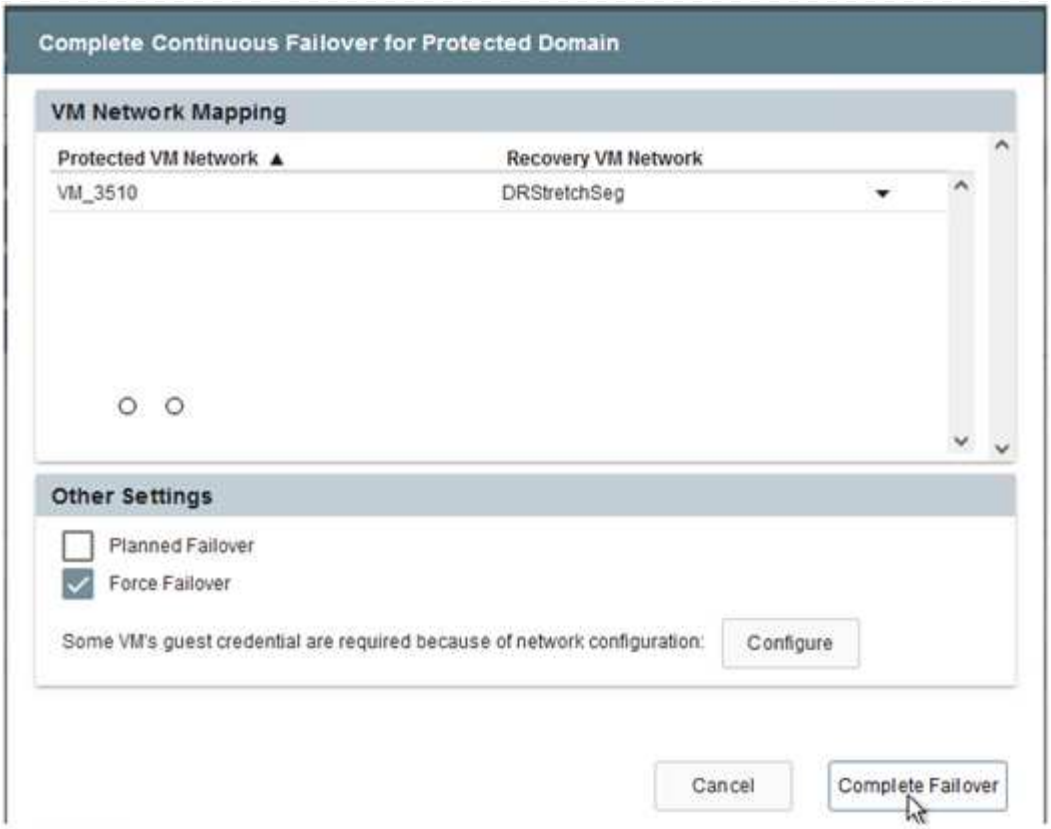
   페일오버를 완료할 때 나타나는 대화 상자에서 페일오버 작업을 계획대로 지정하거나 강제 작업으로 가정할 수 있습니다.





강제 대체 작동 에서는 운영 사이트에 더 이상 액세스할 수 없으며 보호 도메인의 소유권이 복구 사이트에 의해 직접 가정되어야 한다고 가정합니다.





3. 연속 페일오버가 완료되면 작업 완료를 확인하는 메시지가 나타납니다. 작업이 완료되면 복구된 VM에 액세스하여 iSCSI 또는 NFS 세션을 구성합니다.

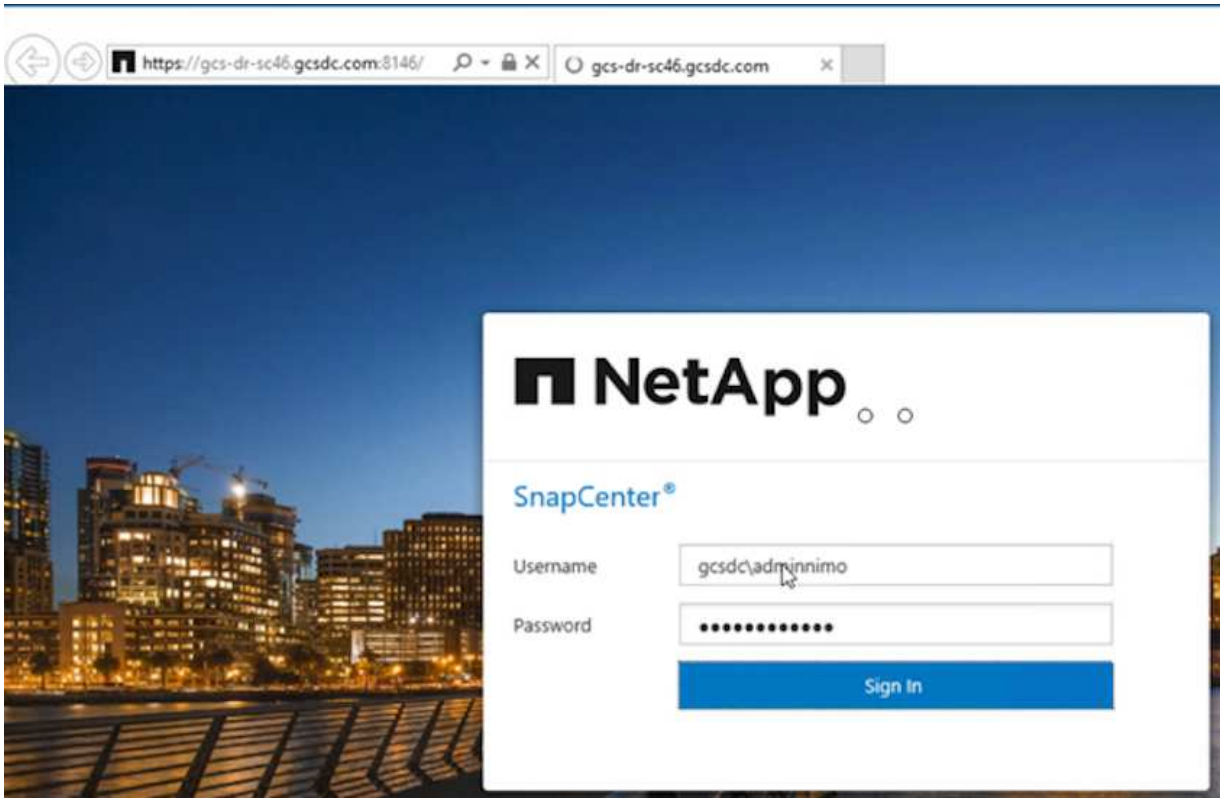
> ⓘ 페일오버 모드가 페일오버에서 실행 중으로 변경되고 VM 상태는 복구 가능합니다. 이제 보호 도메인의 모든 VM이 페일오버 Runbook 설정에 지정된 상태의 복구 사이트에서 실행됩니다.

> ⓘ 장애 조치 구성 및 인프라를 확인하기 위해 Jetstream DR을 테스트 모드(장애 조치 테스트 옵션)로 작동하여 가상 시스템 및 해당 데이터가 개체 저장소에서 테스트 복구 환경으로 복구되는 것을 관찰할 수 있습니다. 테스트 모드에서 페일오버 절차를 실행하면 실제 페일오버 프로세스와 비슷합니다.

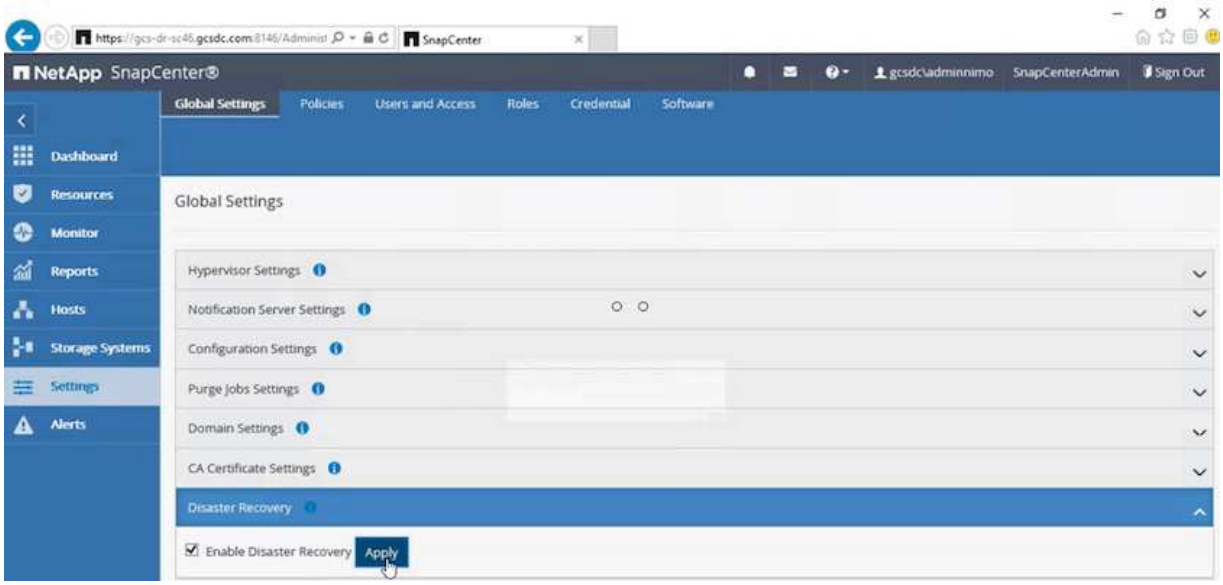
4. 가상 머신이 복구된 후 게스트 내 스토리지에 스토리지 재해 복구를 사용합니다. 이 프로세스를 시연하기 위해

이 예에서는 SQL Server가 사용됩니다.

5. AVS SDDC에서 복구된 SnapCenter VM에 로그인하고 DR 모드를 활성화합니다.
   a. browserN을 사용하여 SnapCenter UI에 액세스합니다.



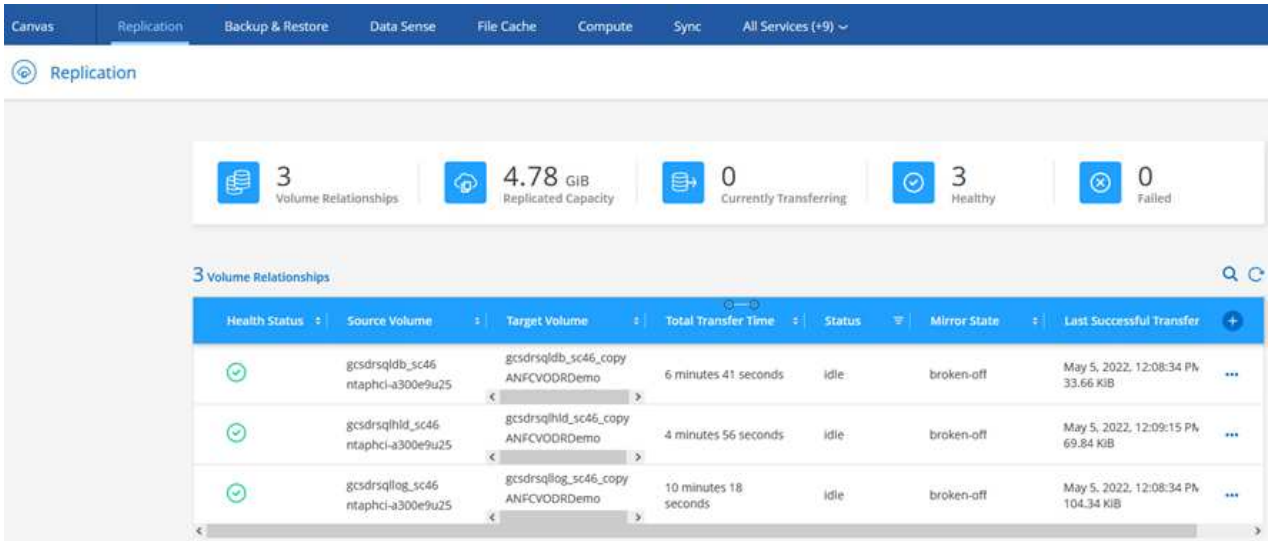
   b. 설정 페이지에서 설정 > 글로벌 설정 > 재해 복구 로 이동합니다.
   c. 재해 복구 활성화 를 선택합니다.
   d. 적용 을 클릭합니다.



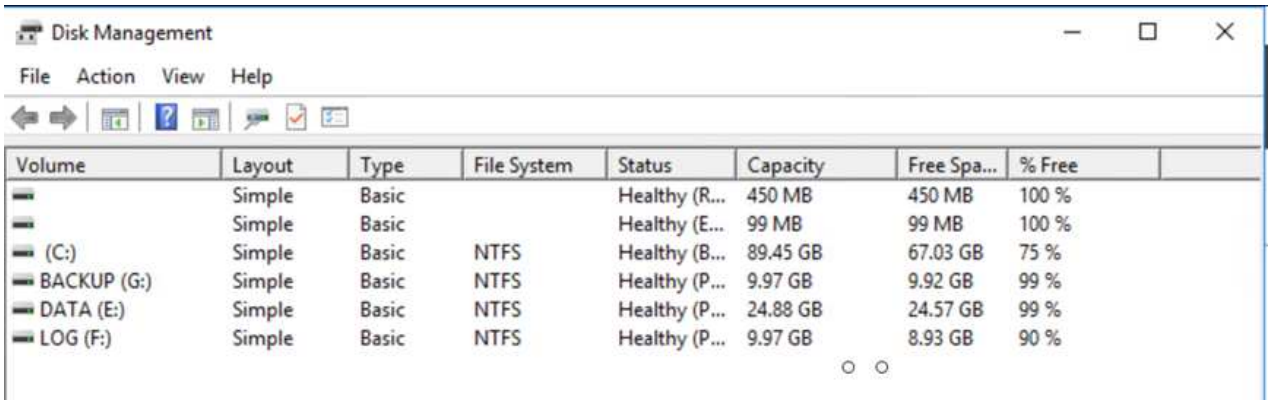
   e. 모니터 > 작업 을 클릭하여 DR 작업이 활성화되었는지 확인합니다.

> 스토리지 재해 복구에 NetApp SnapCenter 4.6 이상을 사용해야 합니다. 이전 버전의 경우 SnapMirror를 사용하여 복제된 애플리케이션 정합성 보장 스냅샷을 사용해야 하며, 재해 복구 사이트에서 이전 백업을 복구해야 하는 경우 수동 복구를 실행해야 합니다.

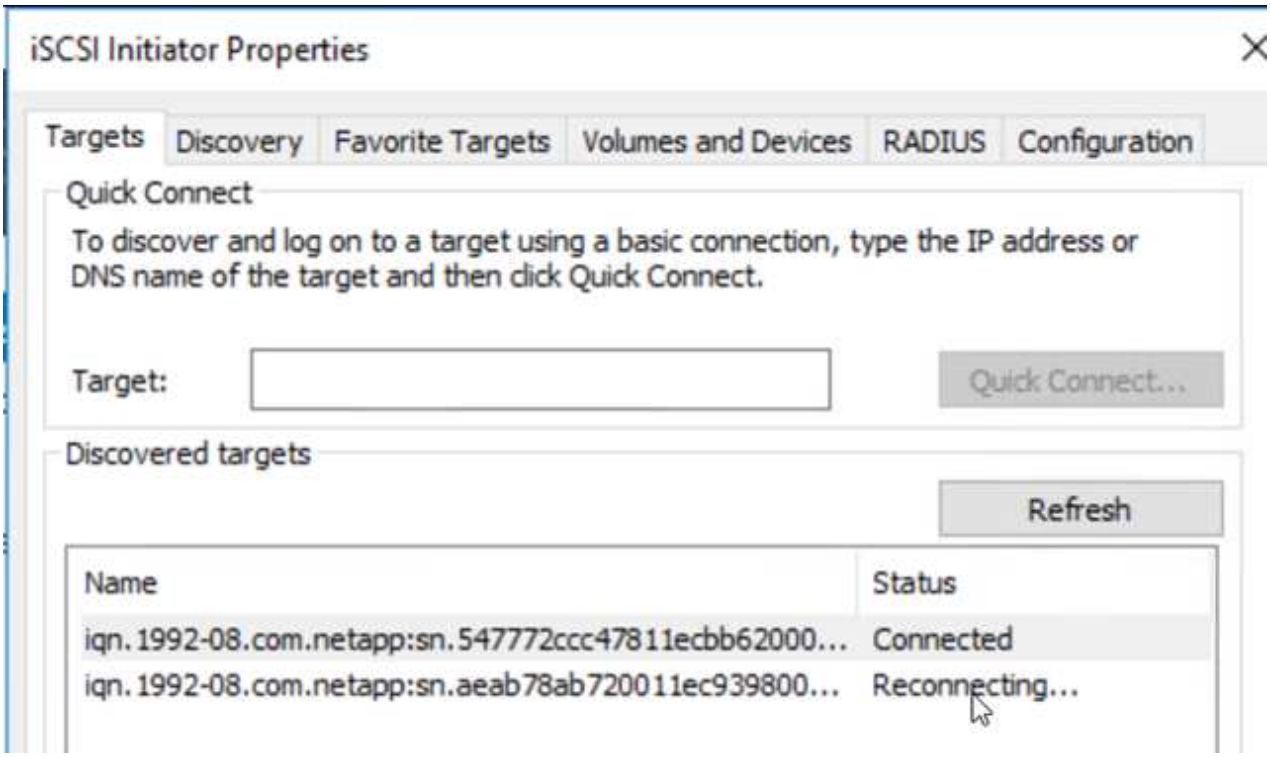
6. SnapMirror 관계가 끊어져 있는지 확인합니다.



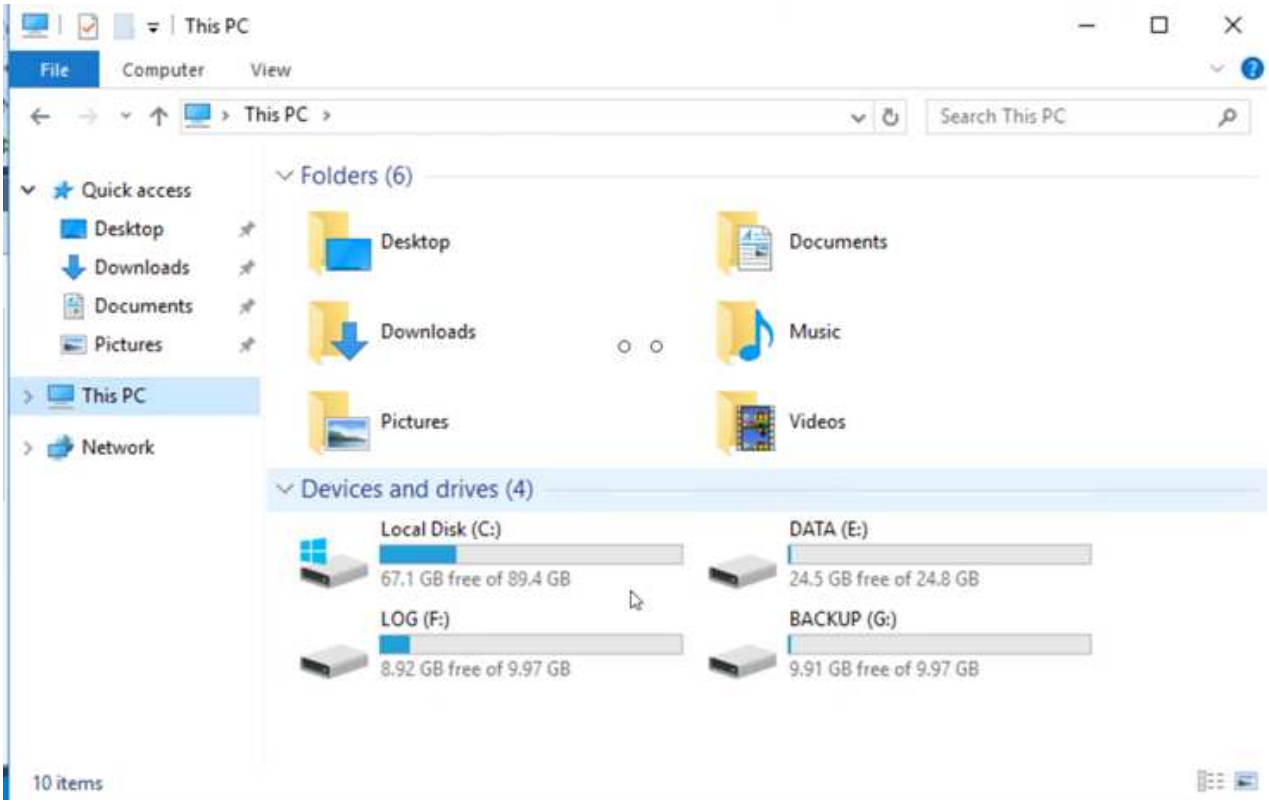
7. Cloud Volumes ONTAP의 LUN을 동일한 드라이브 문자로 복구된 SQL 게스트 VM에 연결합니다.



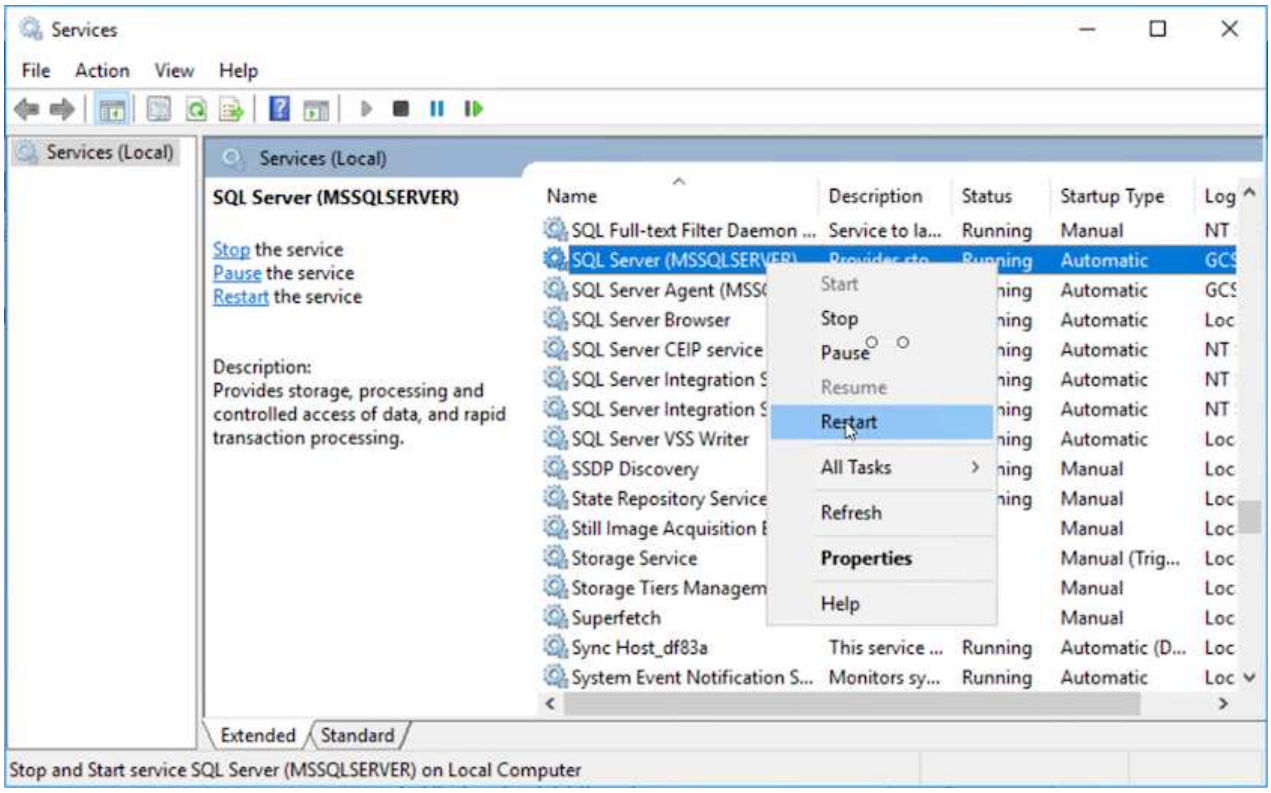
8. iSCSI 초기자를 열고, 이전에 연결이 끊긴 세션을 지우고, 복제된 Cloud Volumes ONTAP 볼륨에 대한 다중 경로와 함께 새 대상을 추가합니다.



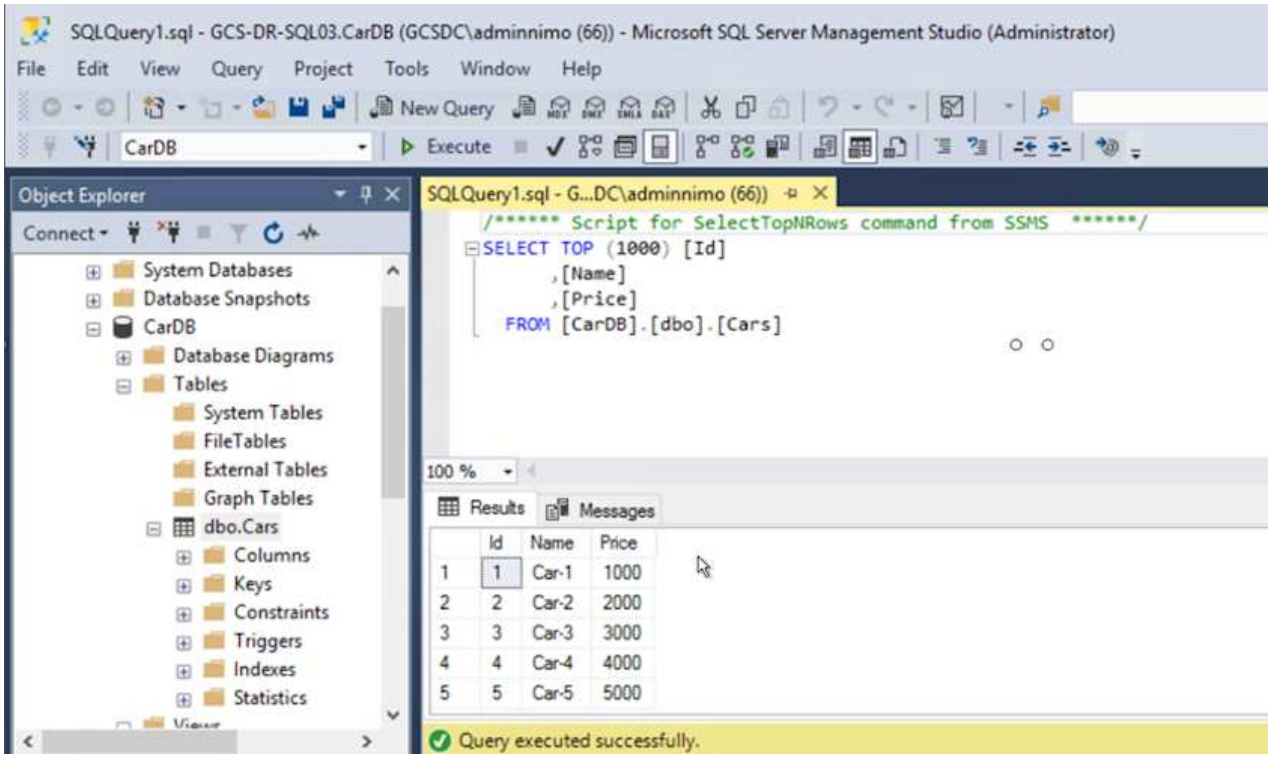
9. DR 이전에 사용한 드라이브 문자와 동일한 드라이브 문자를 사용하여 모든 디스크가 연결되어 있는지 확인합니다.



10. MSSQL 서버 서비스를 다시 시작합니다.



11. SQL 리소스가 다시 온라인 상태인지 확인합니다.



NFS의 경우 mount 명령을 사용하여 볼륨을 연결하고 '/etc/fstab' 항목을 업데이트합니다.

이 시점에서는 작업을 실행하고 정상적으로 비즈니스를 계속할 수 있습니다.

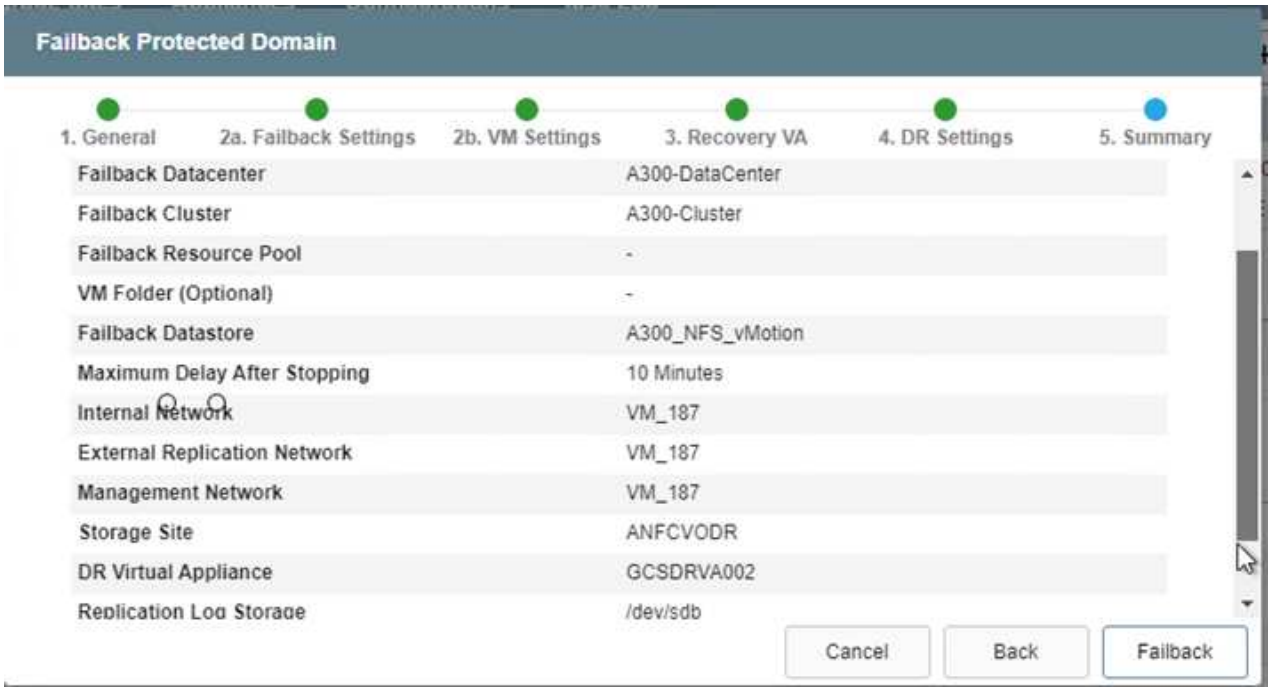
NSX-T 엔드에서는 페일오버 시나리오를 시뮬레이션하기 위해 별도의 전용 Tier-1 게이트웨이를 생성할 수 있습니다. 이렇게 하면 모든 워크로드가 서로 통신할 수 있지만, 트래픽이 환경 내외부로 라우팅될 수는 없으므로 교차 오염의 위험 없이 모든 분류, 억제 또는 강화 작업을 수행할 수 있습니다. 이 작업은 이 문서의 범위를 벗어나지만 격리 시뮬레이션을 위해 쉽게 수행할 수 있습니다.

운영 사이트가 다시 가동된 후 페일백을 수행할 수 있습니다. Jetstream에 의해 VM 보호가 재개되고 SnapMirror 관계가 역전되어야 합니다.

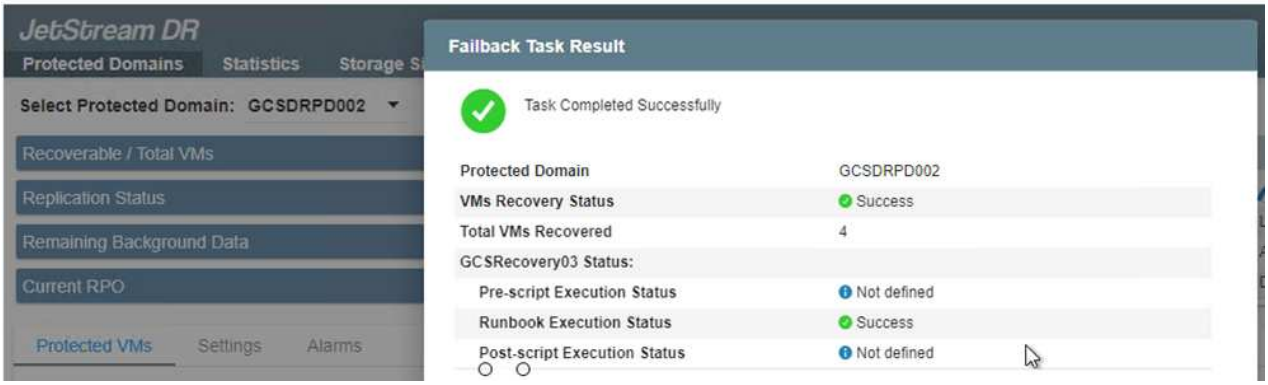
1. 사내 환경을 복원합니다. 재해 발생 유형에 따라 보호 클러스터의 구성을 복원 및/또는 확인해야 할 수도 있습니다. 필요한 경우 Jetstream DR 소프트웨어를 재설치해야 할 수 있습니다.
2. 복원된 온프레미스 환경에 액세스하고 Jetstream DR UI로 이동한 다음 적절한 보호 도메인을 선택합니다. 보호 사이트가 페일백될 준비가 되면 UI에서 페일백 옵션을 선택합니다.

CPT에서 생성한 페일백 계획을 사용하여 VM과 해당 데이터를 오브젝트 저장소에서 원래 VMware 환경으로 되돌릴 수도 있습니다.

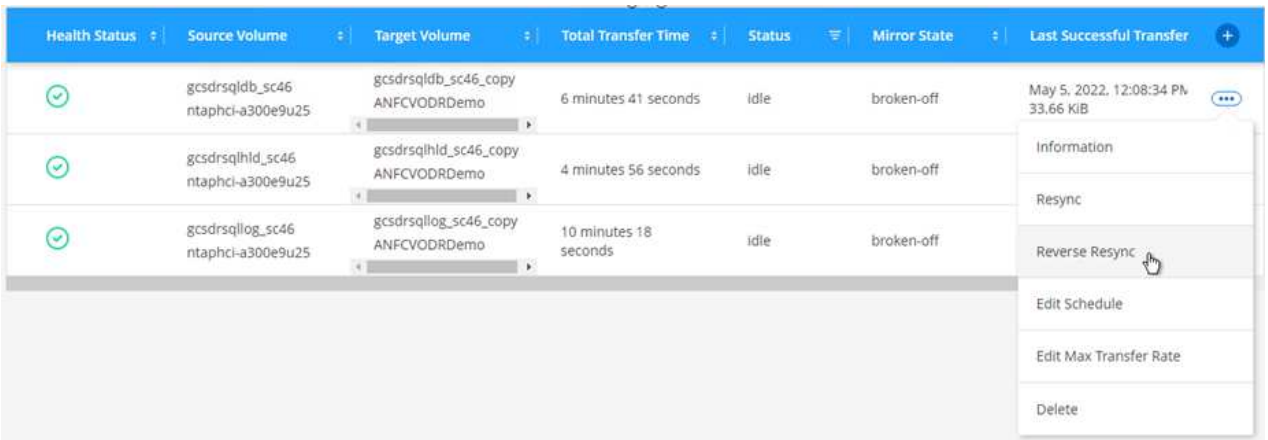
복구 사이트에서 VM을 일시 중지하고 보호 사이트에서 다시 시작한 후 최대 지연 시간을 지정합니다. 이 프로세스를 완료하는 데 필요한 시간은 장애 조치 VM을 중지한 후 복제 완료, 복구 사이트를 청소하는 데 필요한 시간, 보호 사이트에서 VM을 다시 만드는 데 필요한 시간 등을 포함합니다. 10분을 권장합니다.

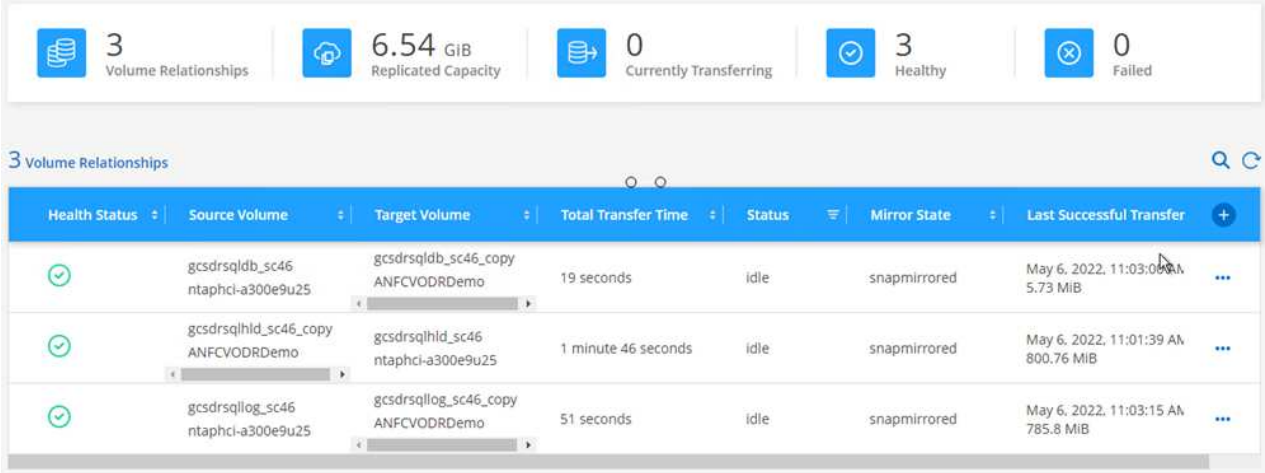


3. 페일백 프로세스를 완료한 다음 VM 보호 및 데이터 정합성 재개를 확인합니다.

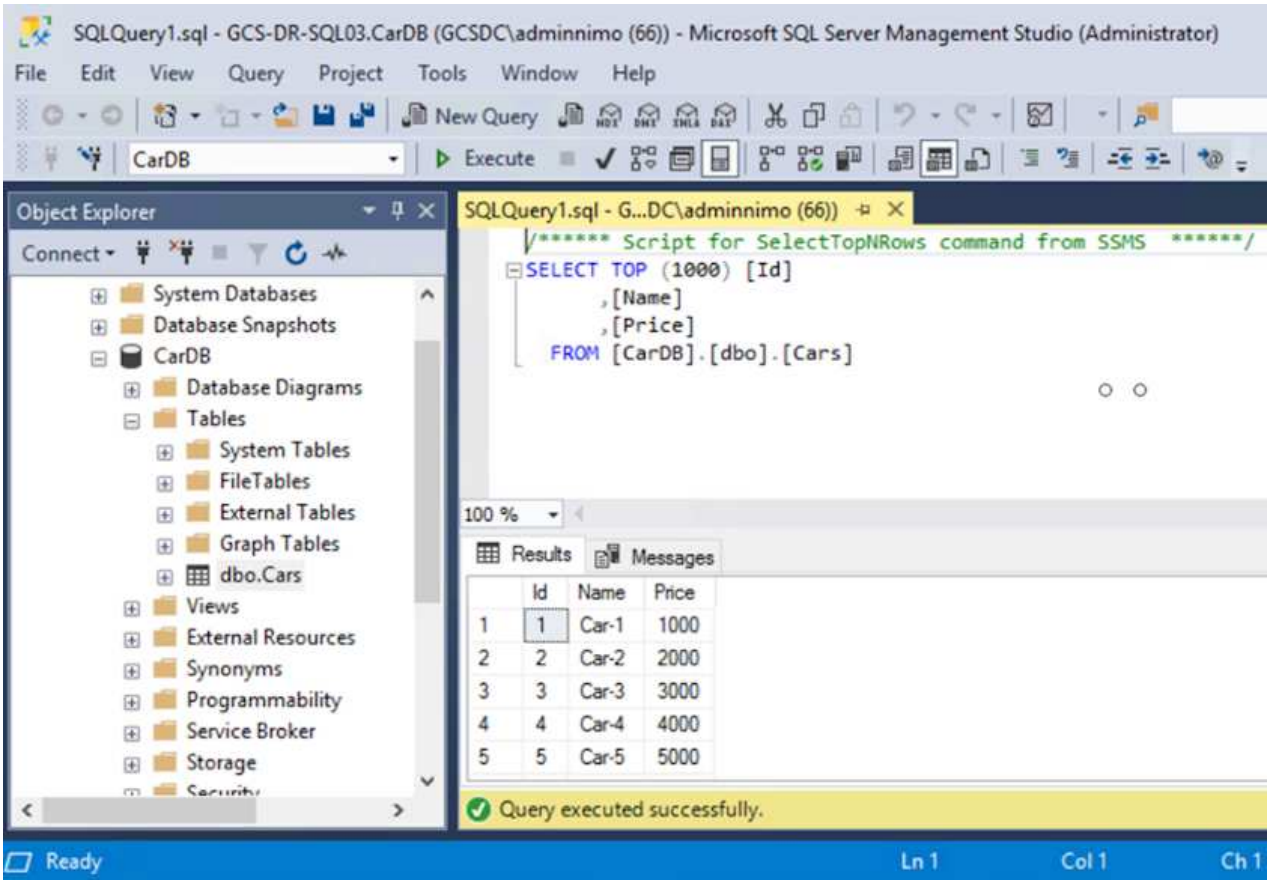


4. VM이 복구된 후 호스트에서 보조 스토리지를 분리하고 운영 스토리지에 접속합니다.





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



> 운영 스토리지로 페일백하려면 역방향 재동기화 작업을 수행하여 페일오버 전과 관계 방향이 동일한지 확인합니다.

> 역재동기화 작업 후 운영 스토리지와 보조 스토리지의 역할을 유지하려면 역방향 재동기화 작업을 다시 수행하십시오.

이 프로세스는 Oracle과 같은 다른 애플리케이션, 유사한 데이터베이스 유형 및 게스트 연결 스토리지를 사용하는

다른 애플리케이션에 적용됩니다.

항상 그렇듯이 중요한 워크로드를 운영 환경으로 포팅하기 전에 해당 워크로드를 복구하는 단계를 테스트하십시오.

이 솔루션의 이점

- SnapMirror의 효율적이고 복원력이 뛰어난 복제를 사용합니다.
- ONTAP 스냅샷 보존을 사용하여 사용 가능한 모든 시점 복구
- 스토리지, 컴퓨팅, 네트워크 및 애플리케이션 검증 단계에서 수백 또는 수천 개의 VM을 복구하는 데 필요한 모든 단계에서 완전한 자동화가 가능합니다.
- SnapCenter는 복제된 볼륨을 변경하지 않는 클론 생성 메커니즘을 사용합니다.
  - 이렇게 하면 볼륨 및 스냅숏에 대한 데이터 손상 위험이 방지됩니다.
  - DR 테스트 워크플로우 중에 복제 중단 방지
  - 개발/테스트, 보안 테스트, 패치 및 업그레이드 테스트, 수정 테스트 등 DR 이외의 워크플로우에 DR 데이터를 활용합니다.
- CPU 및 RAM 최적화를 통해 보다 작은 컴퓨팅 클러스터로 복구할 수 있으므로 클라우드 비용을 절감할 수 있습니다.

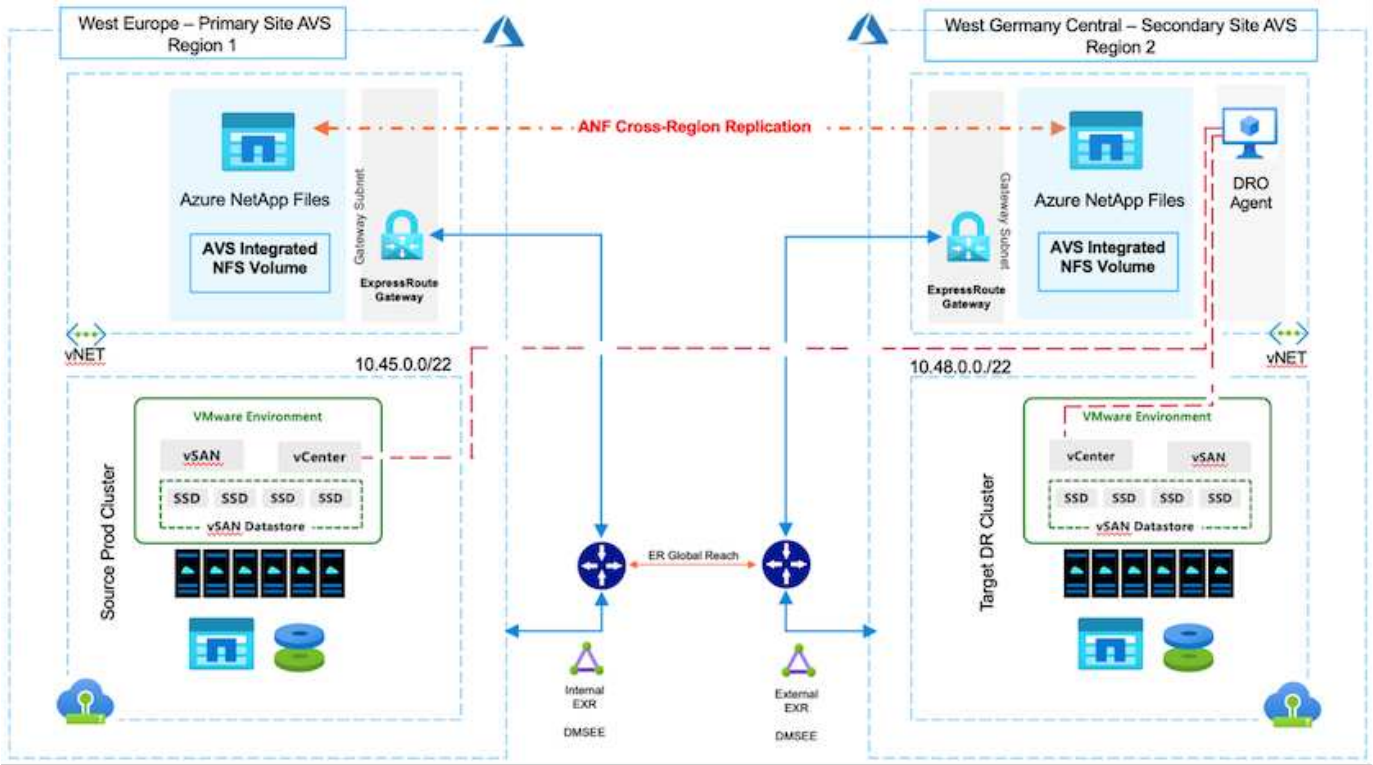
TR-4955: ANF(Azure NetApp Files) 및 AVS(Azure VMware Solution)를 통한 재해 복구

저자: Niyaz Mohamed, NetApp 솔루션 엔지니어링

개요

클라우드 내 영역 간의 블록 레벨 복제를 사용하는 재해 복구는 사이트 중단 및 데이터 손상 이벤트(예: 랜섬웨어)로부터 워크로드를 보호하는 복원력이 있고 비용 효율적인 방법입니다. ANF(Azure NetApp Files) 교차 지역 볼륨 복제를 사용하면 Azure NetApp Files 볼륨을 기본 AVS 사이트의 NFS 데이터 저장소로 사용하는 AVS(Azure VMware Solution) SDDC 사이트에서 실행되는 VMware 워크로드를 대상 복구 영역의 지정된 보조 AVS 사이트로 복제할 수 있습니다.

DRO(재해 복구 오케스트레이터)(UI가 포함된 스크립팅된 솔루션)를 사용하여 AVS SDDC 간에 복제된 워크로드를 원활하게 복구할 수 있습니다. DRO는 복제 피어링을 끊은 다음 AVS에 VM 등록을 통해 대상 볼륨을 데이터 저장소로 마운트하고 NSX-T(모든 AVS 프라이빗 클라우드에 포함)에서 직접 네트워크 매핑을 실행하여 복구를 자동화합니다.



필수 구성 요소 및 일반 권장 사항

- 복제 피어링을 생성하여 지역 간 복제를 활성화했는지 확인합니다. 을 참조하십시오 "Azure NetApp Files에 대한 볼륨 복제를 생성합니다".
- 소스 클라우드와 타겟 Azure VMware 솔루션 프라이빗 클라우드 간에 ExpressRoute Global Reach를 구성해야 합니다.
- 리소스에 액세스할 수 있는 서비스 보안 주체가 있어야 합니다.
- 기본 AVS 사이트에서 보조 AVS 사이트로 연결되는 토폴로지는 다음과 같습니다.
- 를 구성합니다 "복제" 비즈니스 요구 및 데이터 변경률에 따라 각 볼륨에 대한 일정을 적절히 조정합니다.

> 계단식 및 팬인 및 팬아웃 토폴로지는 지원되지 않습니다.

시작하기

Azure VMware 솔루션을 구축합니다

를 클릭합니다 "Azure VMware 솔루션" AVS(AVS)는 Microsoft Azure 퍼블릭 클라우드 내에 완벽하게 작동하는 VMware SDDC를 제공하는 하이브리드 클라우드 서비스입니다. AVS는 Microsoft에서 완벽하게 관리 및 지원하고 Azure 인프라를 사용하는 VMware에서 검증한 최초의 솔루션입니다. 따라서 고객은 컴퓨팅 가상화를 위한 VMware ESXi, 하이퍼 컨버지드 스토리지를 위한 vSAN 및 네트워킹 및 보안을 위한 NSX를 얻는 동시에 Microsoft Azure의 세계적인 입지, 동급 최고의 데이터 센터 시설 및 네이티브 Azure 서비스 및 솔루션의 풍부한 에코시스템에 근접할 수 있는 이점을 누릴 수 있습니다. Azure VMware 솔루션 SDDC와 Azure NetApp Files를 함께 사용하면 네트워크 지연 시간을 최소화하면서 최상의 성능을 얻을 수 있습니다.

Azure에서 AVS 프라이빗 클라우드를 구성하려면 이 단계를 수행하십시오 "링크" NetApp 제품 설명서를 참조하십시오 "링크" Microsoft 설명서를 참조하십시오. 최소 구성으로 설정된 파일럿 라이트 환경을 DR 용도로 사용할 수 있습니다. 이 설정에는 중요한 애플리케이션을 지원하는 핵심 구성 요소만 포함되며, 페일오버가 발생하는 경우 더 많은 호스트를

확장하고 확장하여 대량의 로드를 처리할 수 있습니다.

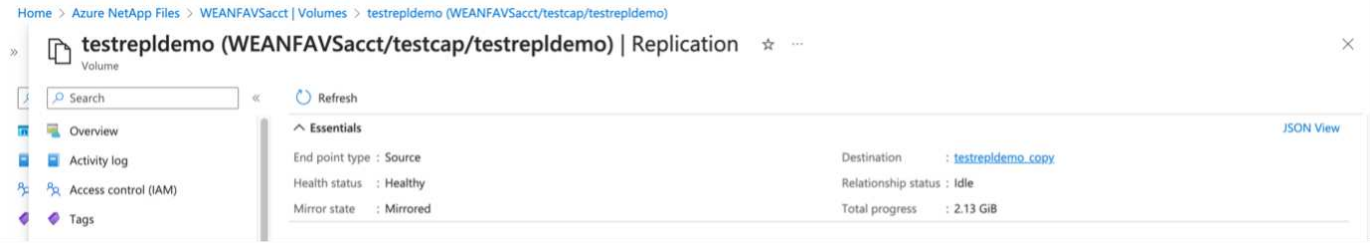
> 최초 릴리즈에서 DRO는 기존 AVS SDDC 클러스터를 지원합니다. 온디맨드 SDDC 작성은 향후 릴리스에서 제공될 예정입니다.

Azure NetApp Files 프로비저닝 및 구성

"Azure NetApp Files" 는 엔터프라이즈급 고성능 용량제 파일 스토리지 서비스입니다. 이 단계를 따릅니다 "링크" AVS 프라이빗 클라우드 구축을 최적화하기 위해 Azure NetApp Files를 NFS 데이터 저장소로 프로비저닝 및 구성합니다.

Azure NetApp Files 기반 데이터 저장소 볼륨에 대한 볼륨 복제를 생성합니다

첫 번째 단계는 AVS 기본 사이트에서 AVS 보조 사이트로 원하는 데이터 저장소 볼륨에 대한 교차 지역 복제를 적절한 빈도와 보존 기능으로 설정하는 것입니다.



이 단계를 따릅니다 "링크" 복제 피어링을 생성하여 지역 간 복제를 설정합니다. 대상 용량 풀의 서비스 수준은 소스 용량 풀의 서비스 수준과 일치할 수 있습니다. 그러나 이러한 특정 사용 사례에서 표준 서비스 수준을 선택한 다음 "서비스 수준을 수정합니다" 실제 재해 또는 DR 시뮬레이션이 발생하는 경우

> 교차 지역 복제 관계는 사전 요구 사항으로, 미리 만들어야 합니다.

DRO 설치

DRO를 시작하려면 지정된 Azure 가상 시스템에서 Ubuntu 운영 체제를 사용하고 필수 구성 요소를 충족하는지 확인하십시오. 그런 다음 패키지를 설치합니다.

- 필수 구성 요소: *
- 리소스에 액세스할 수 있는 서비스 보안 주체
- 소스 및 대상 SDDC 및 Azure NetApp Files 인스턴스에 대한 적절한 연결이 있는지 확인합니다.
- DNS 이름을 사용하는 경우 DNS 확인이 필요합니다. 그렇지 않으면 vCenter에 IP 주소를 사용합니다.
- OS 요구 사항: *
- Ubuntu Focal 20.04 (LTS) 지정된 에이전트 가상 머신에 다음 패키지를 설치해야 합니다.
- Docker 를 참조하십시오
- Docker-Compose
- JqChange `docker.sock` 이 새 권한에 대한 설명: `sudo chmod 666 /var/run/docker.sock`.

> 를 클릭합니다 `deploy.sh` 스크립트는 필요한 모든 필수 구성 요소를 실행합니다.

단계는 다음과 같습니다.

1. 지정된 가상 머신에 설치 패키지를 다운로드합니다.

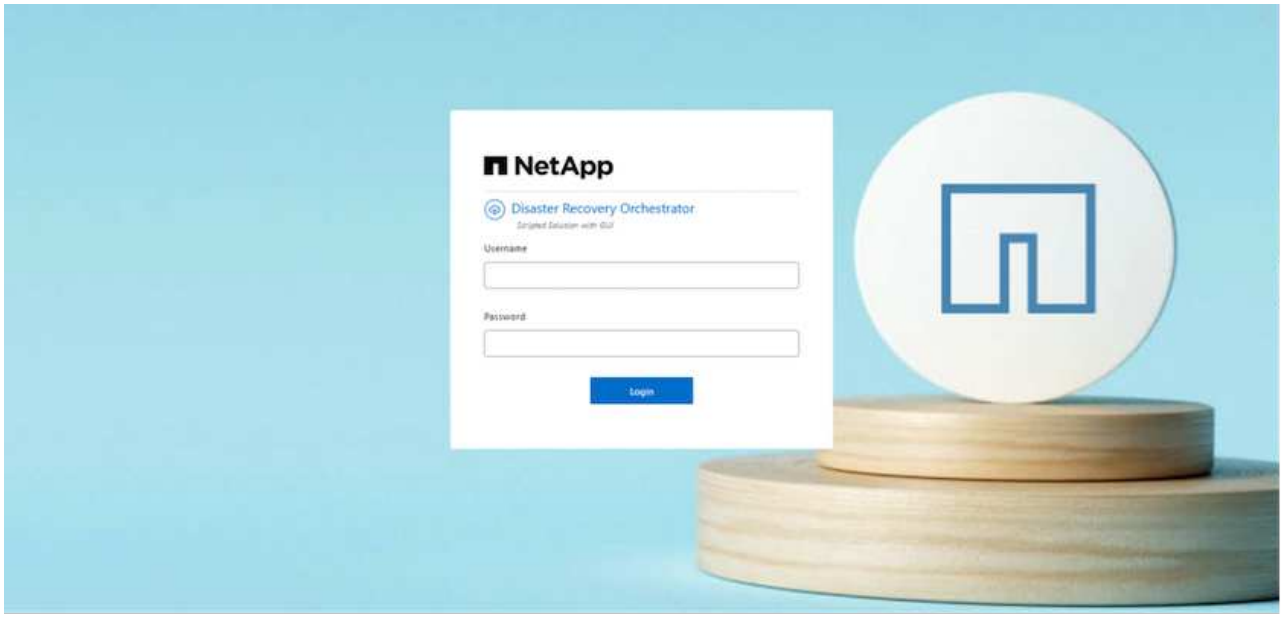
```
git clone https://github.com/NetApp/DRO-Azure.git
```

> 에이전트는 SDDC와 별도로 AVS 사이트 영역이나 기본 AVS 사이트 영역에 설치해야 합니다.

2. 패키지의 압축을 풀고 배포 스크립트를 실행한 다음 호스트 IP를 입력합니다(예: `10.10.10.10`)를 클릭합니다.

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

3. 다음 자격 증명을 사용하여 UI에 액세스합니다.
   - 사용자 이름: `admin`
   - 암호: `admin`



DRO 구성

Azure NetApp Files 및 AVS가 올바르게 구성된 후 운영 AVS 사이트에서 보조 AVS 사이트로 워크로드 복구를 자동화하도록 DRO 구성을 시작할 수 있습니다. DRO 에이전트가 네트워크를 통해 적절한 AVS 및 Azure NetApp Files 구성 요소와 통신할 수 있도록 보조 AVS 사이트에 DRO 에이전트를 구축하고 ExpressRoute 게이트웨이 연결을 구성하는 것이 좋습니다.

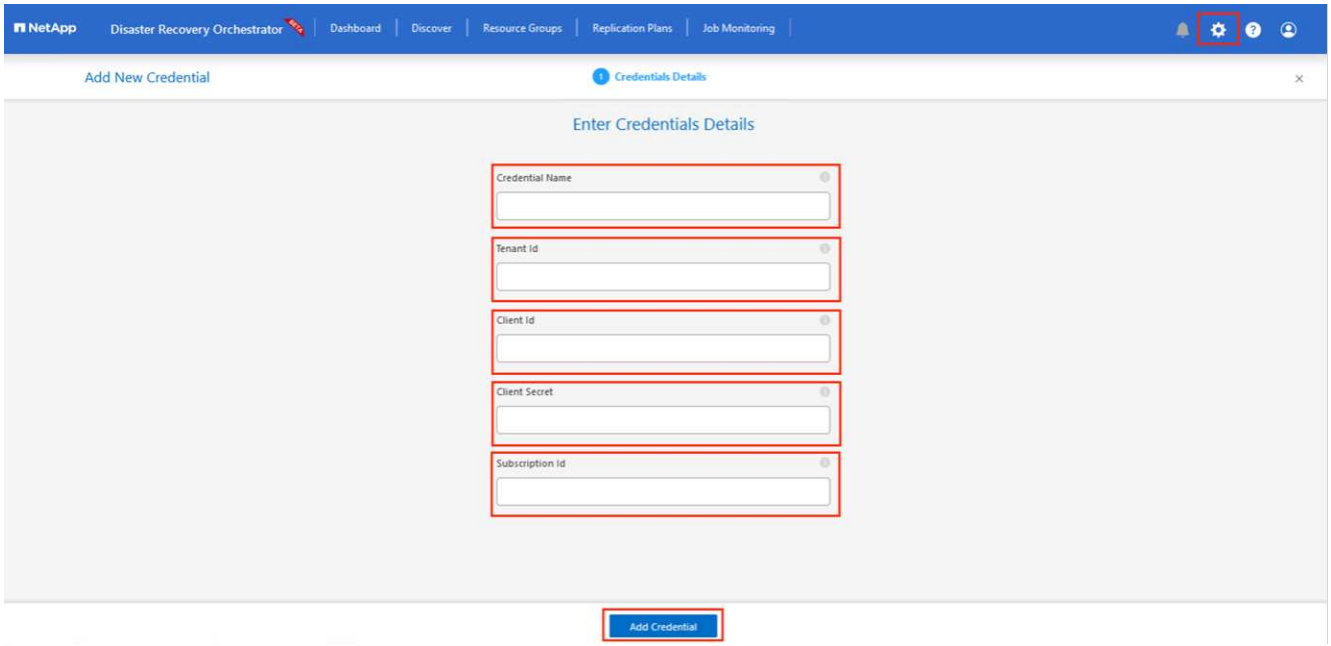
첫 번째 단계는 자격 증명을 추가하는 것입니다. DRO는 Azure NetApp Files 및 Azure VMware 솔루션을 검색할 수 있는 권한이 필요합니다. Azure AD(Active Directory) 응용 프로그램을 생성 및 설정하고 DRO에 필요한 Azure 자격 증명을 획득하여 Azure 계정에 필요한 권한을 부여할 수 있습니다. 서비스 보안 주체를 Azure 구독에 바인딩하고

필요한 관련 권한이 있는 사용자 지정 역할을 할당해야 합니다. 소스 및 대상 환경을 추가하면 서비스 보안 주체와 연결된 자격 증명을 선택하라는 메시지가 표시됩니다. 새 사이트 추가를 클릭하기 전에 이러한 자격 증명을 DRO에 추가해야 합니다.

이 작업을 수행하려면 다음 단계를 수행하십시오.

1. 지원되는 브라우저에서 DRO를 열고 기본 사용자 이름과 암호를 사용합니다 /`admin`/`admin`)를 클릭합니다. 암호는 암호 변경 옵션을 사용하여 처음 로그인한 후 재설정할 수 있습니다.
2. DRO 콘솔의 오른쪽 상단에서 * 설정 * 아이콘을 클릭하고 * 자격 증명 * 을 선택합니다.
3. 새 자격 증명 추가 를 클릭하고 마법사의 단계를 따릅니다.
4. 자격 증명을 정의하려면 필요한 권한을 부여하는 Azure Active Directory 서비스 보안 주체에 대한 정보를 입력합니다.
   - 자격 증명 이름입니다
   - 테넌트 ID입니다
   - 클라이언트 ID입니다
   - 클라이언트 암호
   - 구독 ID입니다

     AD 응용 프로그램을 만들 때 이 정보를 캡처해야 합니다.
5. 새 자격 증명에 대한 세부 정보를 확인하고 자격 증명 추가 를 클릭합니다.

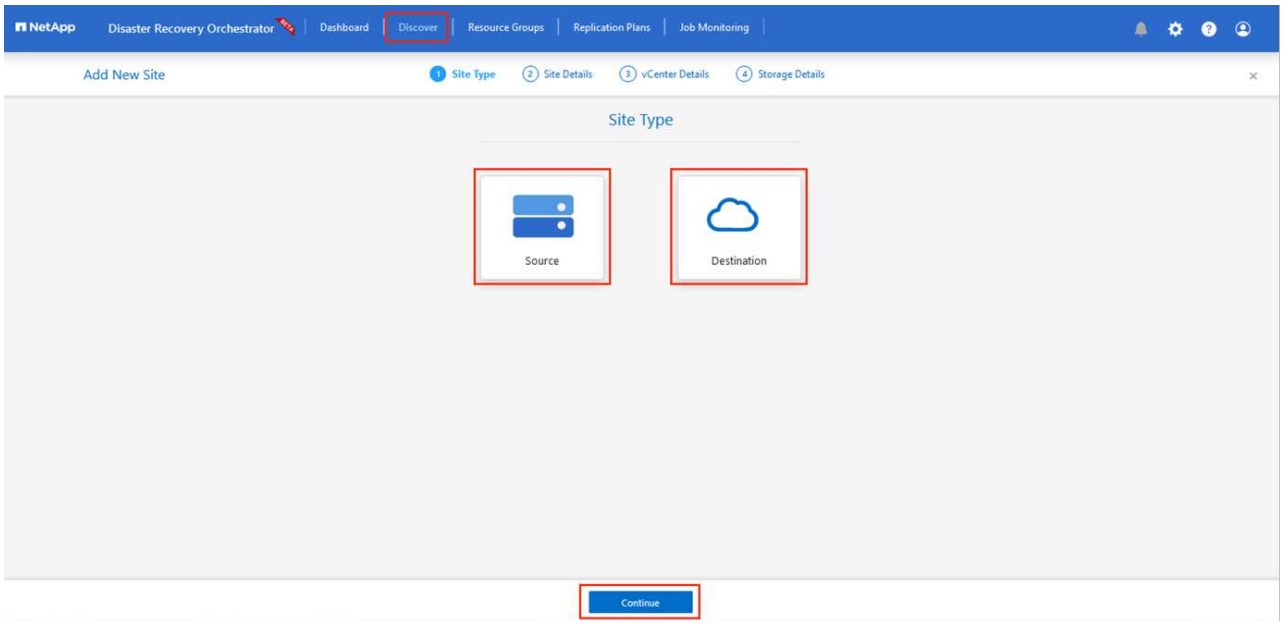


자격 증명을 추가한 후에는 운영 및 보조 AVS 사이트(vCenter 및 Azure NetApp Files 스토리지 계정 모두)를 검색하고 DRO에 추가해야 합니다. 소스 및 대상 사이트를 추가하려면 다음 단계를 수행하십시오.

6. 검색 * 탭으로 이동합니다.
7. 새 사이트 추가 * 를 클릭합니다.
8. 다음 기본 AVS 사이트(콘솔에서 * 소스 * 로 지정됨)를 추가합니다.

- SDDC vCenter
- Azure NetApp Files 스토리지 계정입니다

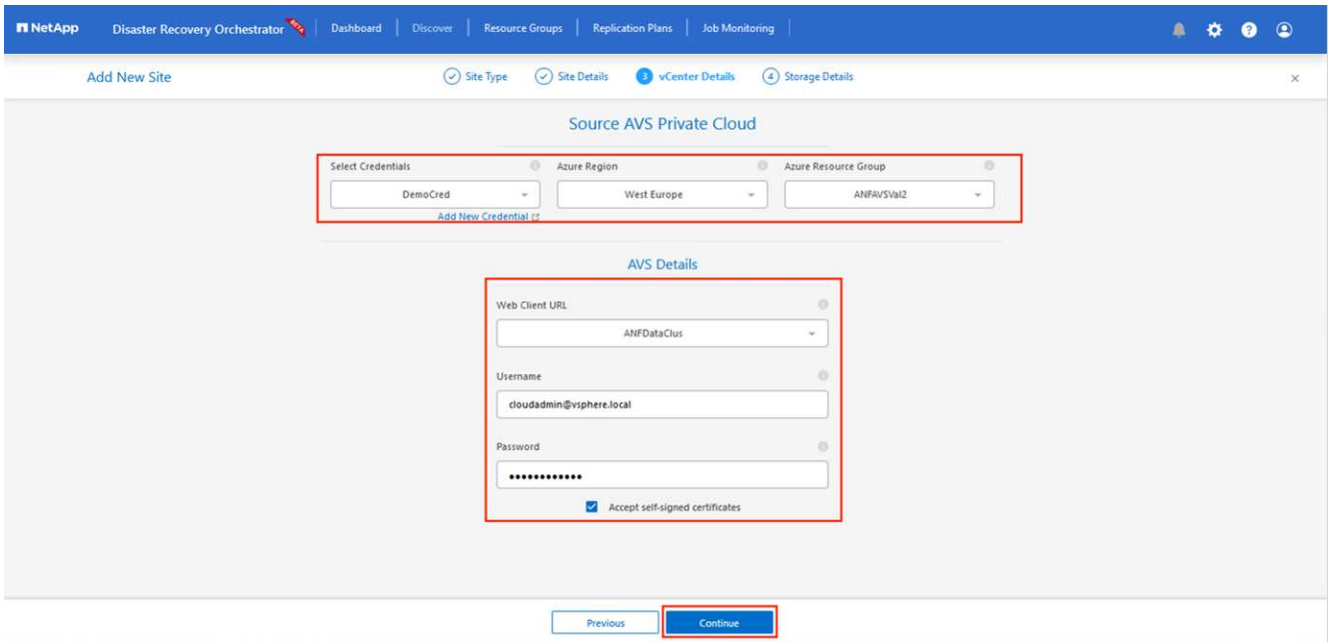
9. 다음 보조 AVS 사이트(* 콘솔에서 * 대상 * 으로 지정됨)를 추가합니다.
    - SDDC vCenter
    - Azure NetApp Files 스토리지 계정입니다



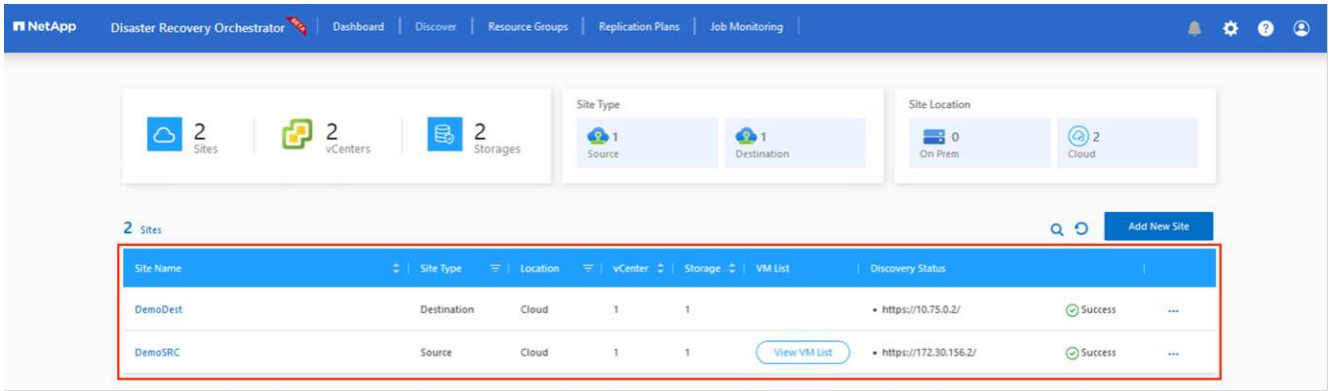
10. Source, * 를 차례로 클릭하여 사이트 세부 정보를 추가하고 친숙한 사이트 이름을 입력한 다음 커넥터를 선택합니다. 그런 다음 * 계속 * 을 클릭합니다.

    데모용으로 소스 사이트 추가는 이 문서에서 다룹니다.

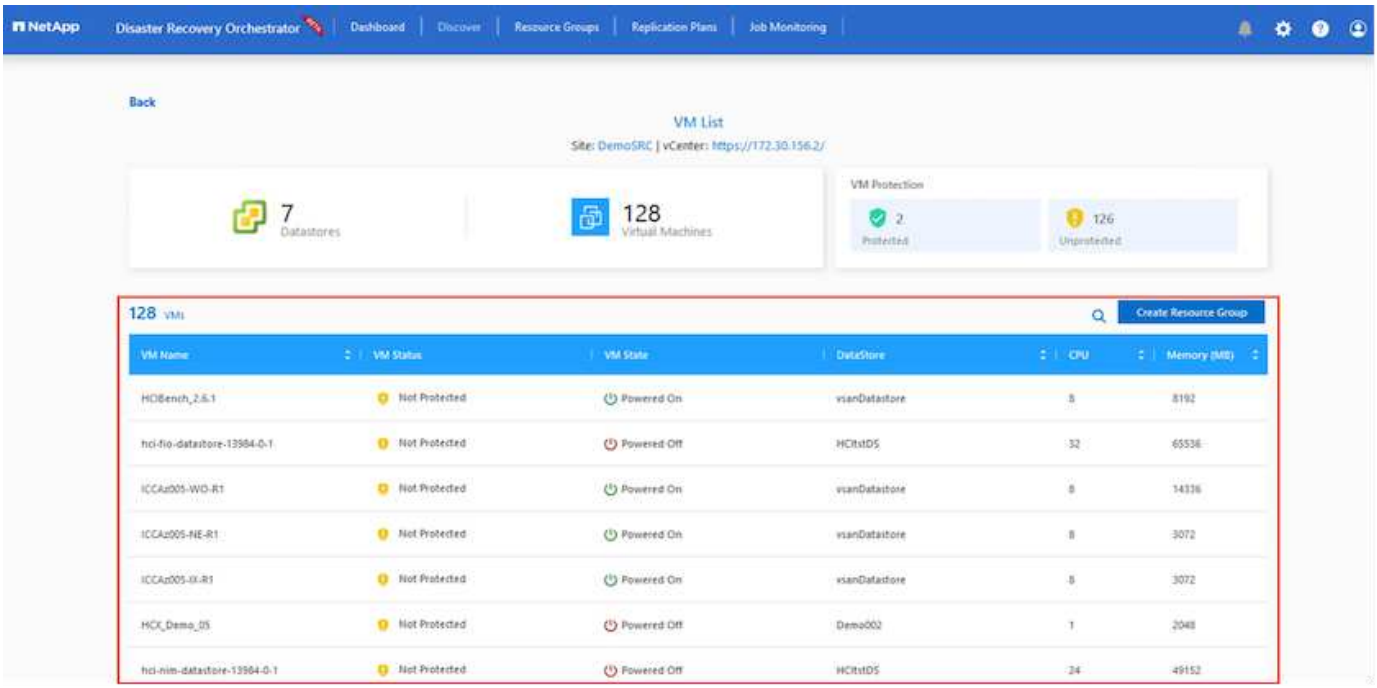
11. vCenter 세부 정보를 업데이트합니다. 이렇게 하려면 기본 AVS SDDC 드롭다운에서 자격 증명, Azure 지역 및 리소스 그룹을 선택합니다.
12. DRO는 해당 지역 내에서 사용 가능한 모든 DC를 나열합니다. 드롭다운에서 지정된 사설 클라우드 URL을 선택합니다.
13. 를 입력합니다 `cloudadmin@vsphere.local` 사용자 자격 증명. 이 기능은 Azure Portal에서 액세스할 수 있습니다. 여기에 설명된 단계를 따릅니다 "링크". 완료되면 * Continue * 를 클릭합니다.



14. Azure Resource 그룹과 NetApp 계정을 선택하여 Source Storge 세부 정보(ANF)를 선택합니다.
15. Create Site * 를 클릭합니다.



DRO가 추가되면 자동 검색을 수행하고 소스 사이트에서 대상 사이트로 해당 지역 간 복제본이 있는 VM을 표시합니다. DRO는 VM에서 사용하는 네트워크와 세그먼트를 자동으로 감지하여 채웁니다.



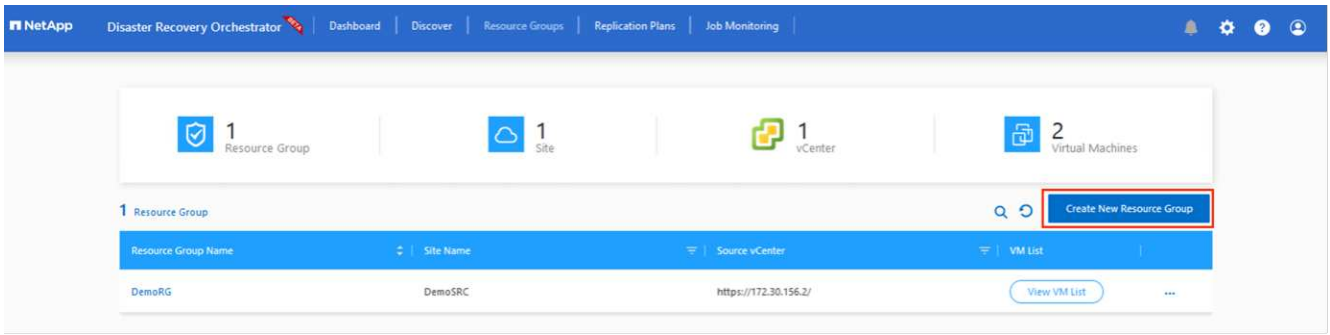
다음 단계는 필요한 VM을 자원 그룹으로 그룹화하는 것입니다.

리소스 그룹화

플랫폼을 추가한 후 복구하려는 VM을 리소스 그룹으로 그룹화합니다. DRO 리소스 그룹을 사용하면 종속 VM 집합을 부팅 순서, 부팅 지연 및 복구 시 실행할 수 있는 선택적 응용 프로그램 유효성 검사가 포함된 논리 그룹으로 그룹화할 수 있습니다.

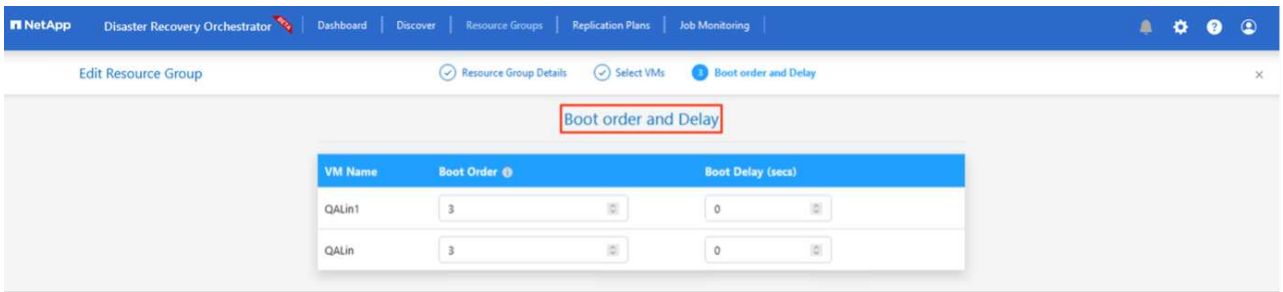
자원 그룹 만들기를 시작하려면 * 새 자원 그룹 만들기 * 메뉴 항목을 클릭합니다.

1. Resource 그룹 * PS에 액세스하고 * Create New Resource Group * 을 클릭합니다.

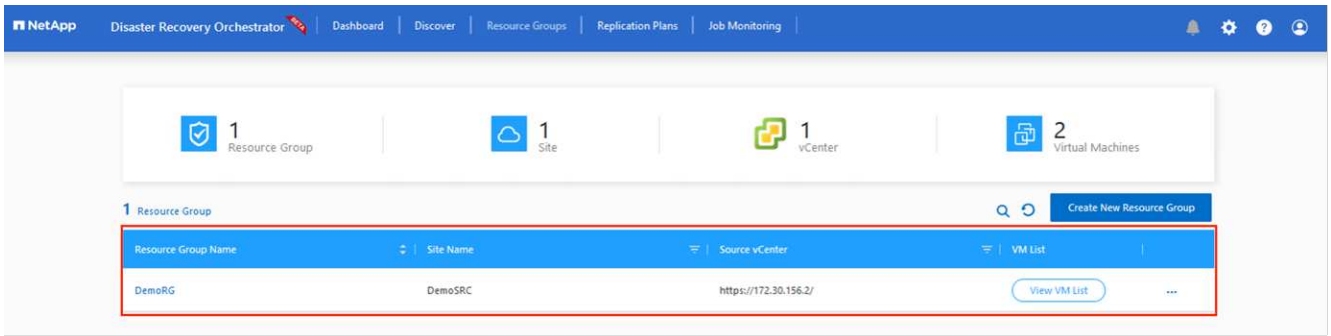


2. 새 리소스 그룹 아래의 드롭다운에서 소스 사이트를 선택하고 * 만들기 * 를 클릭합니다.
3. 리소스 그룹 세부 정보를 입력하고 * Continue * 를 클릭합니다.
4. 검색 옵션을 사용하여 적절한 VM을 선택합니다.
5. 선택한 모든 VM에 대해 * 부트 순서 * 및 * 부트 지연 * (초)을 선택합니다. 각 가상 머신을 선택하고 우선 순위를 설정하여 전원 켜기 순서의 순서를 설정합니다. 모든 가상 머신의 기본값은 3입니다. 옵션은 다음과 같습니다.
   - 전원을 켤 첫 번째 가상 시스템
   - 기본값

◦ 전원을 켤 마지막 가상 컴퓨터



6. 리소스 그룹 만들기 * 를 클릭합니다.

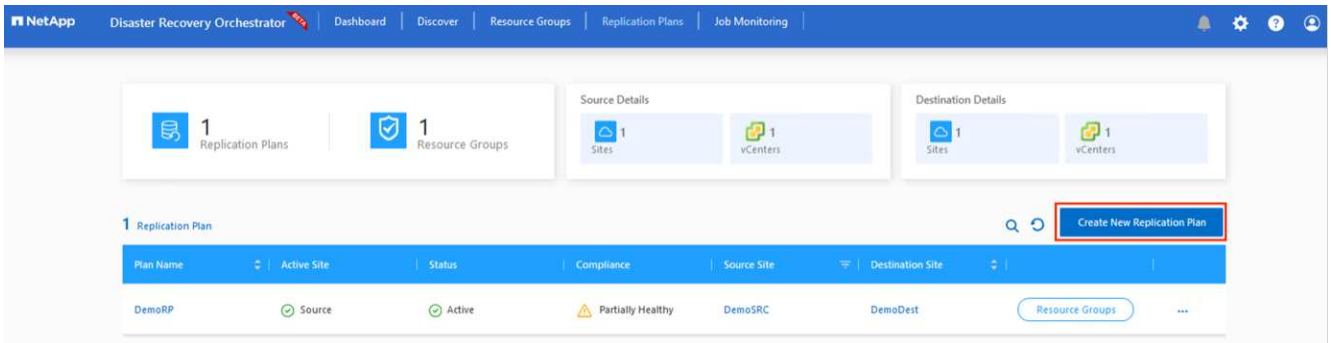


복제 계획

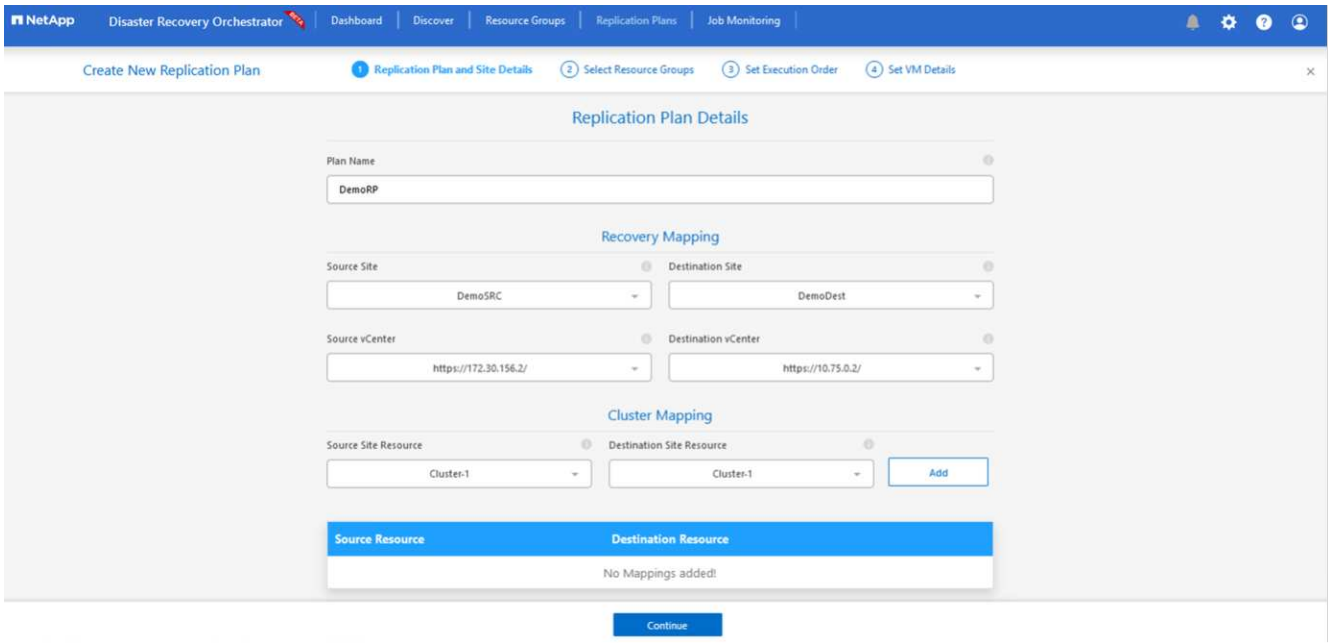
재해가 발생할 경우 애플리케이션을 복구할 계획이 있어야 합니다. 드롭다운에서 소스 및 대상 vCenter 플랫폼을 선택하고, 이 계획에 포함할 리소스 그룹을 선택하고, 애플리케이션 복구 및 전원 켜기 방식(예: 도메인 컨트롤러, 계층 1, 계층 2 등)의 그룹도 포함합니다. 계획도 종종 청사진이라고 부릅니다. 복구 계획을 정의하려면 Replication Plan 탭으로 이동하여 * New Replication Plan * 을 클릭합니다.

복제 계획 생성을 시작하려면 다음 단계를 수행하십시오.

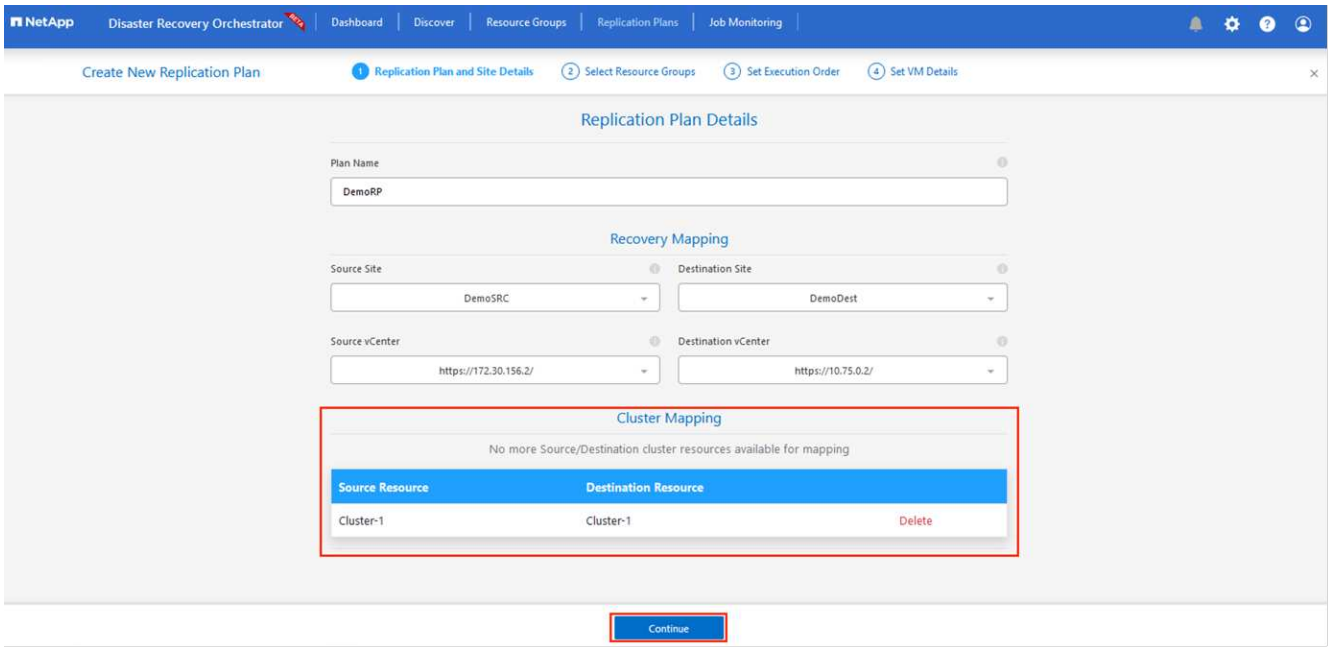
1. Replication Plans * 로 이동하고 * Create New Replication Plan * 을 클릭합니다.



2. 새 복제 계획 * 에서 소스 사이트, 연결된 vCenter, 대상 사이트 및 연결된 vCenter를 선택하여 계획의 이름을 제공하고 복구 매핑을 추가합니다.

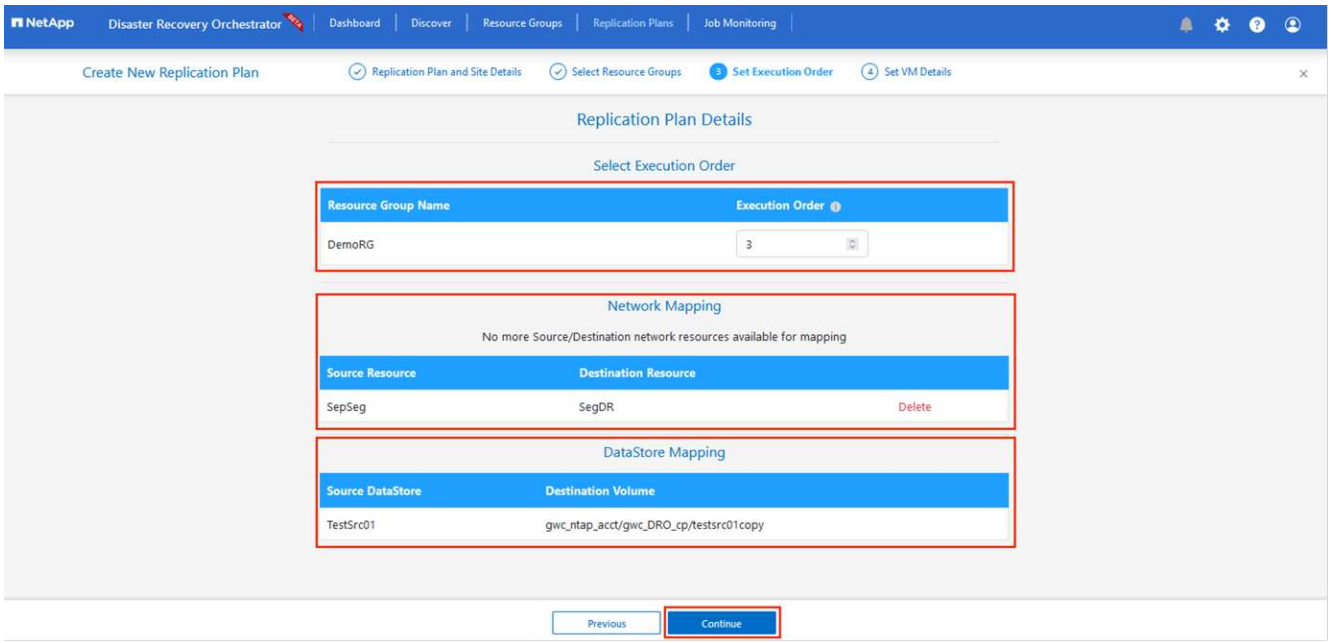


3. 복구 매핑이 완료되면 * 클러스터 매핑 * 을 선택합니다.

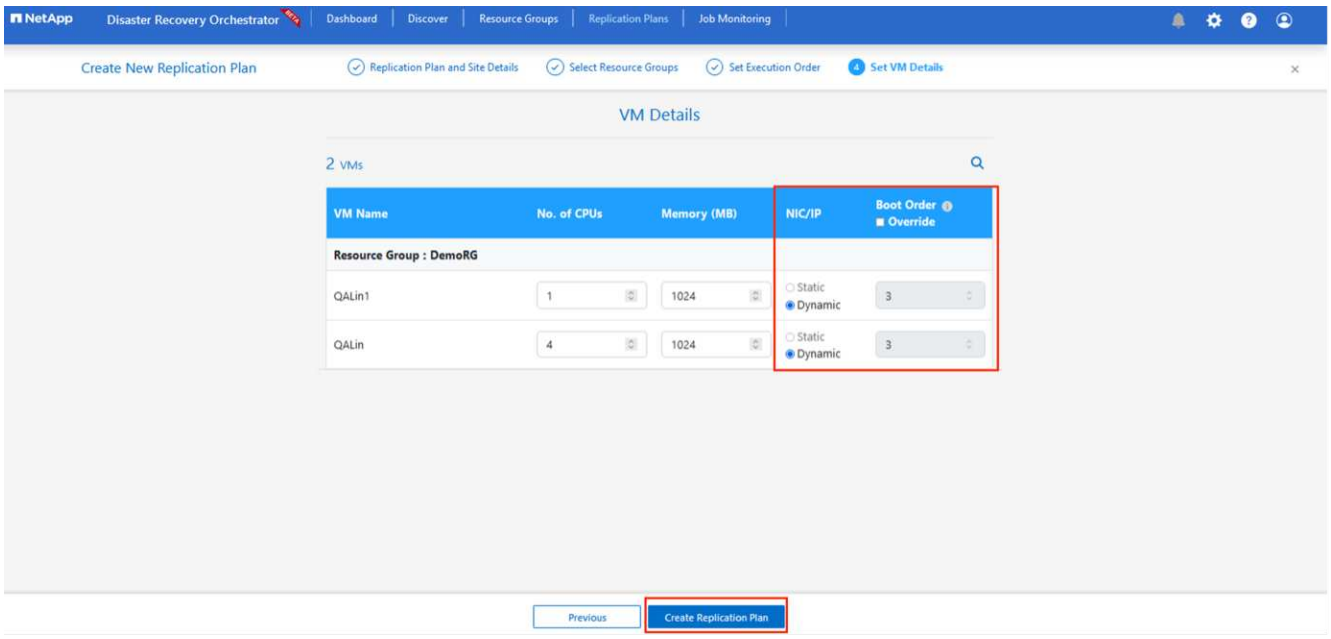


4. 리소스 그룹 세부 정보 * 를 선택하고 * 계속 * 을 클릭합니다.
5. 리소스 그룹의 실행 순서를 설정합니다. 이 옵션을 사용하면 여러 리소스 그룹이 있을 때 작업 순서를 선택할 수 있습니다.
6. 완료되면 네트워크 매핑을 해당 세그먼트에 설정합니다. 세그먼트는 이미 보조 AVS 클러스터에서 프로비저닝되어야 하며, VM을 이러한 세그먼트로 매핑하려면 적절한 세그먼트를 선택하십시오.
7. 데이터 저장소 매핑은 선택한 VM에 따라 자동으로 선택됩니다.

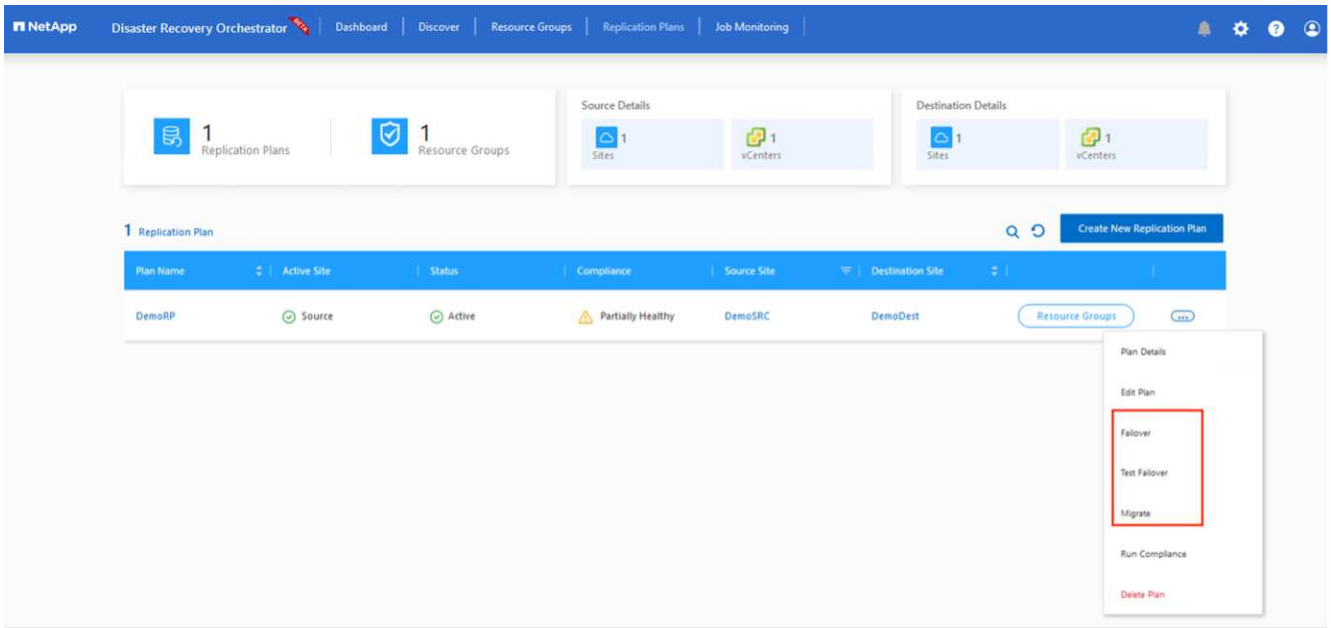
> ⓘ CRR(교차 지역 복제)이 볼륨 레벨에 있습니다. 따라서 해당 볼륨에 상주하는 모든 VM이 CRR 대상에 복제됩니다. 복제 계획에 포함된 가상 머신만 처리되므로 데이터 저장소의 일부인 모든 VM을 선택해야 합니다.



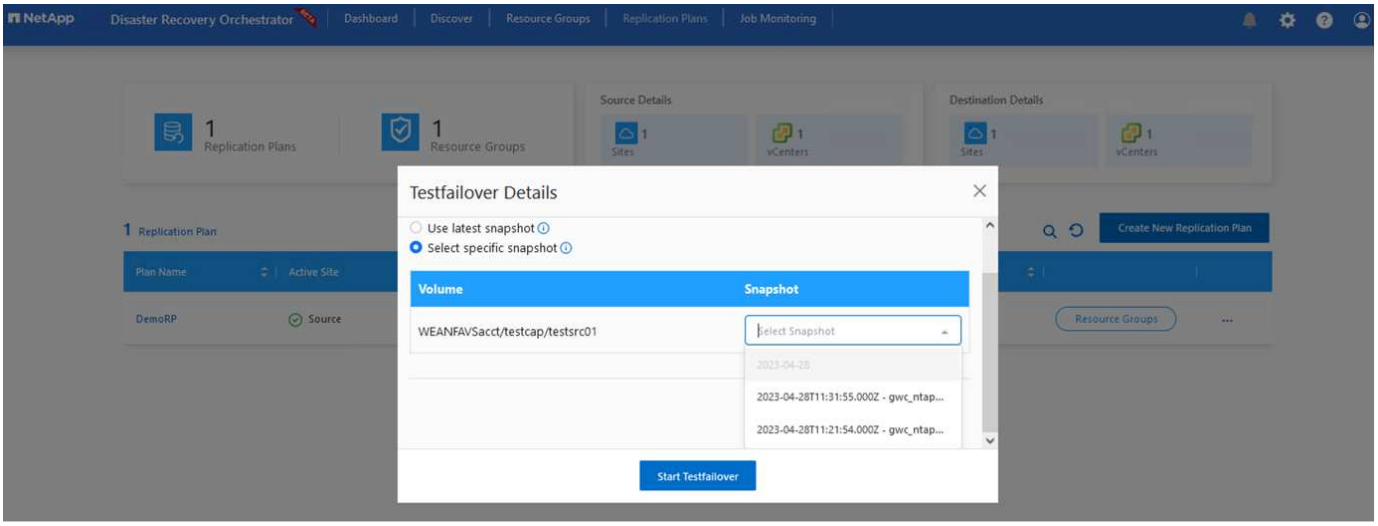
8. VM 세부 정보 아래에서 VM CPU 및 RAM 매개 변수의 크기를 선택적으로 조정할 수 있습니다. 이 기능은 대규모 환경을 소규모 타겟 클러스터로 복구하거나 일대일 물리적 VMware 인프라를 프로비저닝하지 않고 DR 테스트를 수행할 때 매우 유용합니다. 또한 리소스 그룹에서 선택한 모든 VM에 대한 부팅 순서 및 부팅 지연(초)을 수정합니다. 리소스 그룹 부팅 순서를 선택하는 동안 선택한 항목에서 변경이 필요한 경우 부팅 순서를 수정하는 추가 옵션이 있습니다. 기본적으로 리소스 그룹을 선택하는 동안 선택한 부팅 순서가 사용되지만 이 단계에서는 모든 수정 작업을 수행할 수 있습니다.



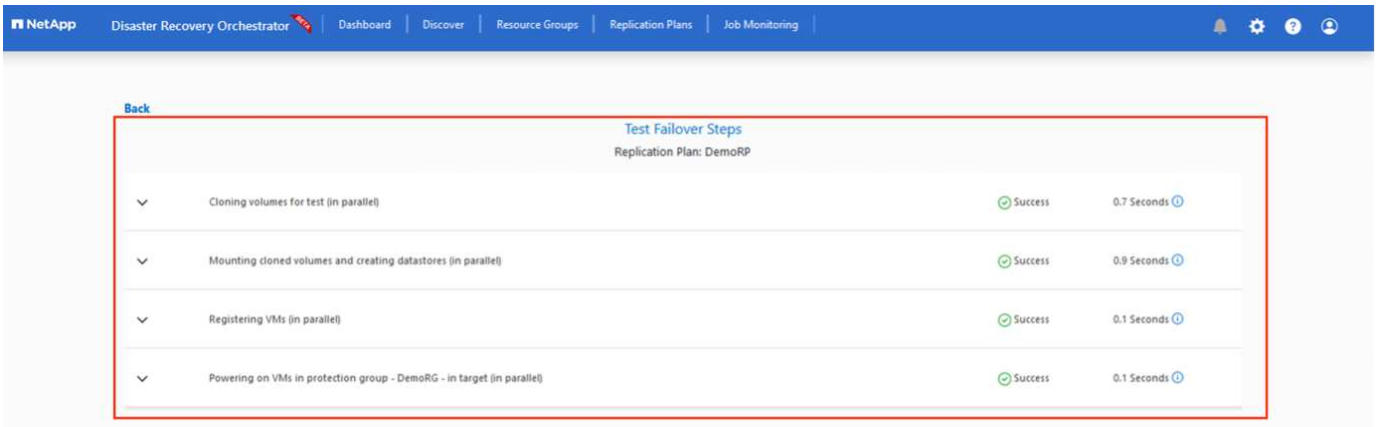
9. Create Replication Plan * 을 클릭합니다. 복제 계획이 생성되면 요구 사항에 따라 장애 조치, 테스트 대체 작동 또는 마이그레이션 옵션을 실행할 수 있습니다.



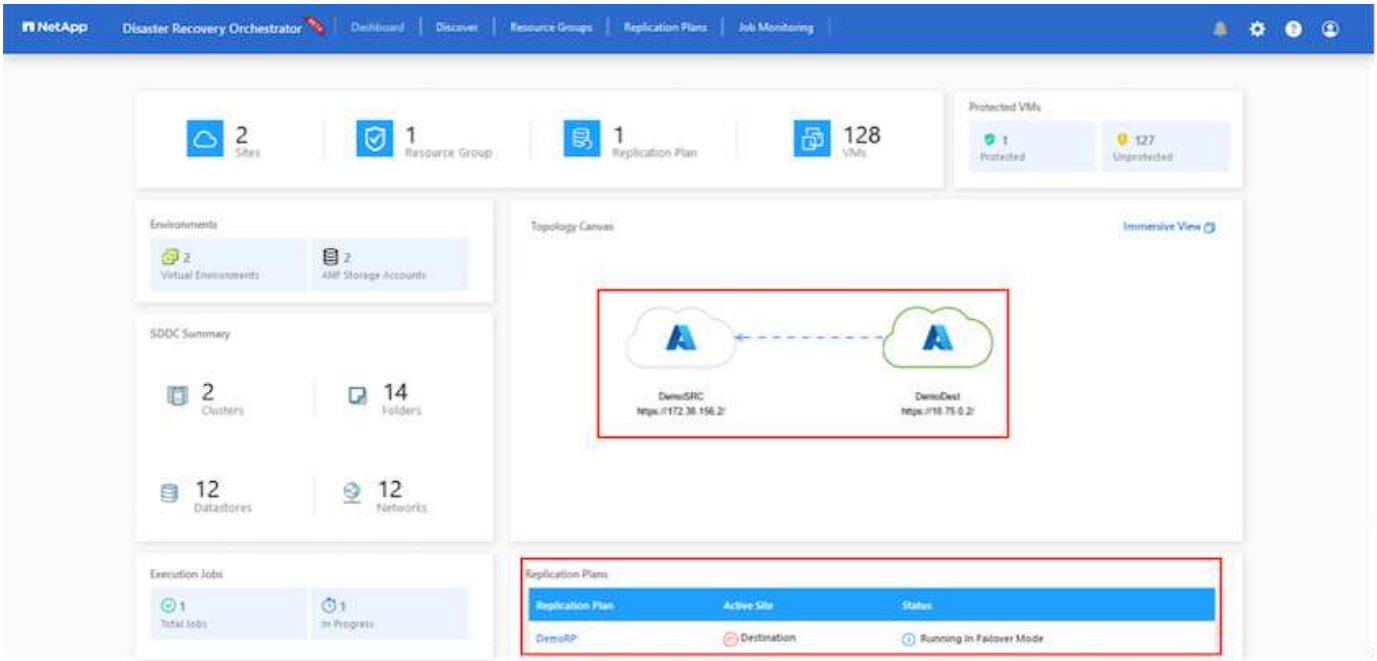
페일오버 및 테스트 페일오버 옵션 중에 최신 스냅샷이 사용되거나 특정 시점 스냅샷에서 특정 스냅샷을 선택할 수 있습니다. 가장 최근의 복제본이 이미 손상 또는 암호화된 상태에서 랜섬웨어와 같은 손상 이벤트가 발생할 경우 시점 옵션이 매우 유용할 수 있습니다. DRO는 사용 가능한 모든 시점을 표시합니다.



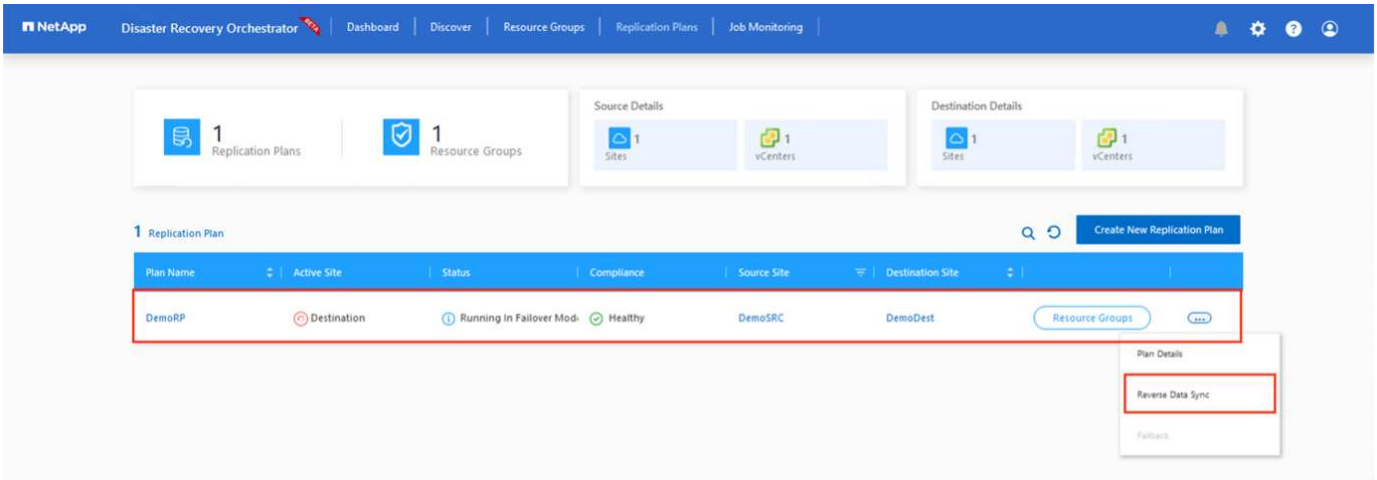
복제 계획에 지정된 구성으로 대체 작동을 트리거하거나 테스트 대체 작동을 트리거하려면 * 장애 조치 * 또는 * 테스트 장애 조치 * 를 클릭합니다. 작업 메뉴에서 복제 계획을 모니터링할 수 있습니다.



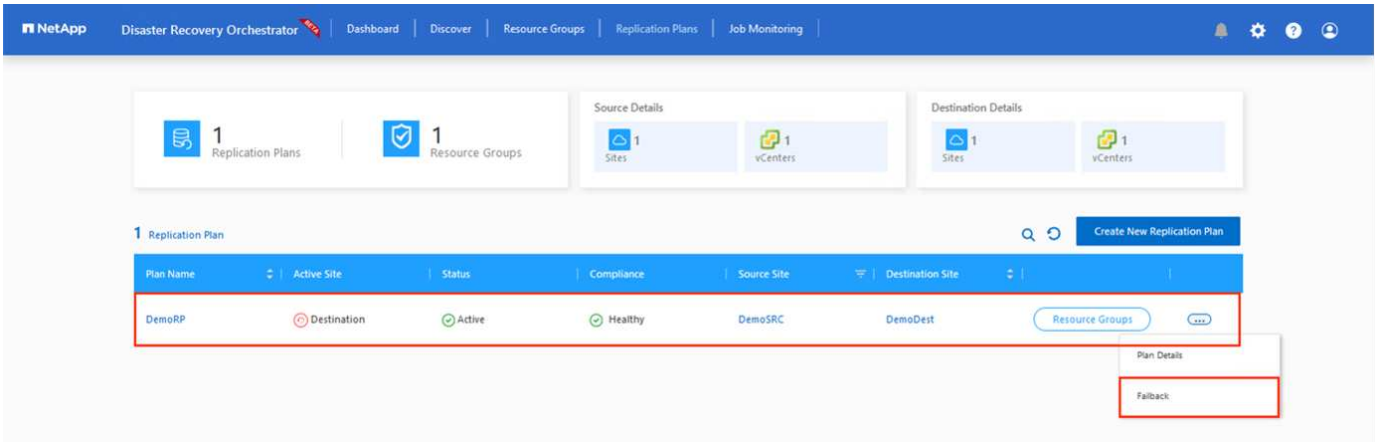
페일오버가 트리거된 후 보조 사이트 AVS SDDC vCenter(VM, 네트워크 및 데이터 저장소)에서 복구된 항목을 볼 수 있습니다. 기본적으로 VM은 Workload 폴더로 복구됩니다.

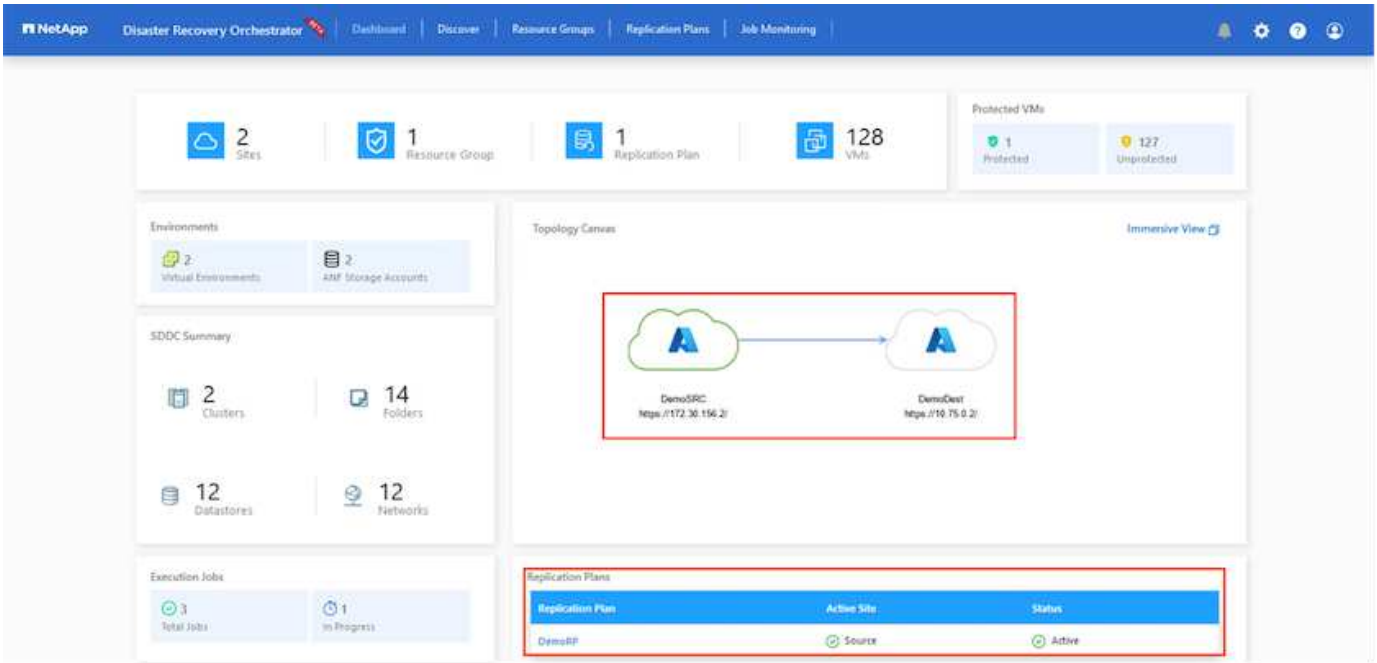


페일백은 복제 계획 레벨에서 트리거될 수 있습니다. 테스트 대체 작동의 경우, tear down 옵션을 사용하여 변경 사항을 롤백하고 새로 생성된 볼륨을 제거할 수 있습니다. 장애 조치와 관련된 장애 복구는 2단계 프로세스입니다. 복제 계획을 선택하고 * Reverse Data sync * 를 선택합니다.



이 단계가 완료된 후 페일백을 트리거하여 기본 AVS 사이트로 다시 이동합니다.





Azure 포털에서 보조 사이트 AVS SDDC에 읽기/쓰기 볼륨으로 매핑된 적절한 볼륨에 대한 복제 상태가 끊어진 것을 확인할 수 있습니다. 테스트 페일오버 중에 DRO는 대상 또는 복제본 볼륨을 매핑하지 않습니다. 대신 필요한 교차 지역 복제 스냅샷의 새 볼륨을 생성하고 볼륨을 데이터 저장소로 노출합니다. 그러면 용량 풀의 추가 물리적 용량을 사용하고 소스 볼륨이 수정되지 않습니다. 특히, DR 테스트 또는 선별적 워크플로우 중에도 복제 작업을 계속할 수 있습니다. 또한 이 프로세스를 통해 오류가 발생하거나 손상된 데이터가 복구되면 복제본이 손상될 위험 없이 복구를 정리할 수 있습니다.

랜섬웨어 복구

랜섬웨어에서 복구하는 것은 매우 힘든 작업이 될 수 있습니다. 특히, IT 조직은 안전한 반환 지점이 무엇인지 정확히 파악하기가 어려울 수 있으며, 일단 결정된 후에는 복구된 워크로드가 재발생하는 공격으로부터 보호하는 방법(예: 휴면 맬웨어로부터 또는 취약한 응용 프로그램을 통해)을 찾기가 어려울 수 있습니다.

DRO는 조직이 사용 가능한 모든 시점에서 복구할 수 있도록 함으로써 이러한 문제를 해결합니다. 그런 다음, 워크로드가 기능적/고립된 네트워크로 복구되어 애플리케이션이 서로 작동하고 통신할 수 있지만 남북 트래픽에 노출되지 않도록 합니다. 이 프로세스를 통해 보안 팀은 법의학 조사를 수행하고 숨겨진 맬웨어 또는 침낭된 맬웨어를 식별할 수 있는 안전한 장소를 확보할 수 있습니다.

결론

Azure NetApp Files 및 Azure VMware 재해 복구 솔루션은 다음과 같은 이점을 제공합니다.

- 효율적이고 탄력적인 Azure NetApp Files 교차 지역 복제 활용
- 스냅샷 보존을 통해 사용 가능한 모든 시점으로 복구합니다.
- 스토리지, 컴퓨팅, 네트워크 및 애플리케이션 검증 단계에서 수백, 수천 개의 VM을 복구하는 데 필요한 모든 단계를 완전히 자동화합니다.
- 워크로드 복구에서는 복제된 볼륨을 조작하지 않는 “최신 스냅샷에서 새 볼륨 생성” 프로세스를 활용합니다.
- 볼륨 또는 스냅샷의 데이터 손상 위험을 방지합니다.
- DR 테스트 워크플로우 중에 복제 중단을 방지합니다.
- DR 이외의 작업에 개발/테스트, 보안 테스트, 패치 및 업그레이드 테스트, 문제 해결 테스트 등 DR 데이터와 클라우드 컴퓨팅 리소스를 활용할 수 있습니다.
- CPU 및 RAM 최적화를 통해 보다 작은 컴퓨팅 클러스터로 복구할 수 있으므로 클라우드 비용을 절감할 수 있습니다.

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 문서 및/또는 웹 사이트를 검토하십시오.

- Azure NetApp Files에 대한 볼륨 복제를 생성합니다

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

- Azure NetApp Files 볼륨의 교차 지역 복제

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

- "Azure VMware 솔루션"

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

- Azure에서 가상화 환경을 구축하고 구성합니다

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

- Azure VMware 솔루션을 구축 및 구성합니다

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

Azure VMware Solution으로 재해 복구를 위해 Veeam Replication 및 Azure NetApp Files 데이터 저장소를 사용합니다

저자: Niyaz Mohamed-NetApp Solutions Engineering

개요

Azure NetApp Files(ANF) 데이터 저장소는 스토리지를 컴퓨팅에서 분리하여 모든 조직에 워크로드를 클라우드로 전환하는 데 필요한 유연성을 제공합니다. 컴퓨팅 리소스와 독립적으로 확장이 가능한 유연한 고성능 스토리지 인프라를 고객에게 제공합니다. Azure NetApp Files 데이터 저장소는 Azure VMware Solution(AVS)과 함께 온프레미스 VMware 환경을 위한 재해 복구 사이트인 구축을 간소화하고 최적화합니다.

Azure NetApp Files(ANF) 볼륨 기반 NFS 데이터 저장소를 사용하여 VM 복제 기능을 제공하는 검증된 타사 솔루션을 사용하여 사내에서 데이터를 복제할 수 있습니다. Azure NetApp Files 데이터 저장소를 추가하면 스토리지를 수용할 수 있는 엄청난 양의 ESXi 호스트를 포함하는 Azure VMware Solution SDDC를 구축하는 것보다 비용 최적화된 배포를 실현할 수 있습니다. 이러한 접근 방식을 "파일럿 라이트 클러스터"라고 합니다. 파일럿 라이트 클러스터는 Azure NetApp Files 데이터 저장소 용량과 함께 최소 AVS 호스트 구성(AVS 노드 3개)입니다.

목표는 페일오버를 처리하기 위해 모든 핵심 구성 요소를 사용하여 저렴한 인프라를 유지하는 것입니다. 페일오버가 발생하는 경우 파일럿 라이트 클러스터가 스케일아웃되고 더 많은 AVS 호스트를 프로비저닝할 수 있습니다. 그리고 페일오버가 완료되고 정상 작동이 복원되면 파일럿 라이트 클러스터를 저비용 운영 모드로 확장할 수 있습니다.

이 문서의 목적

이 기사에서는 Veeam 백업 및 복제와 함께 Azure NetApp Files 데이터 저장소를 사용하여 Veeam VM 복제 소프트웨어 기능을 사용하여 온프레미스 VMware VM용 재해 복구를 AVS(으)로 설정하는 방법을 설명합니다.

Veeam Backup & Replication은 가상 환경을 위한 백업 및 복제 애플리케이션입니다. 가상 머신이 복제되면 Veeam Backup & Replication이 AVS에서 복제되며 소프트웨어는 타겟 AVS SDDC 클러스터에 네이티브 VMware vSphere 형식으로 VM의 정확한 복제본을 생성합니다. Veeam Backup & Replication은 복제본을 원래 VM과 동기화된 상태로 유지합니다. 재해 복구 사이트에 시작 준비 상태의 VM 복제본이 마운트되어 있기 때문에 복제는 최상의 RTO(복구 시간 목표)를 제공합니다.

이 복제 메커니즘은 재해 발생 시 AVS SDDC에서 워크로드를 신속하게 시작할 수 있도록 합니다. Veeam Backup & Replication 소프트웨어는 또한 WAN을 통한 복제 및 느린 연결을 위해 트래픽 전송을 최적화합니다. 또한 중복 데이터 블록, 제로 데이터 블록, 스왑 파일 및 "제외된 VM 게스트 OS 파일"도 필터링합니다. 소프트웨어는 복제본 트래픽도 압축합니다. 복제 작업이 전체 네트워크 대역폭을 소비하는 것을 방지하기 위해 WAN 가속기 및 네트워크 조절 규칙을 활용할 수 있습니다.

Veeam Backup & Replication의 복제 프로세스는 작업 중심으로 수행되므로 복제 작업을 구성하여 복제가 수행됩니다. 재해 이벤트의 경우 해당 복제본 복제본으로 장애 조치를 수행하여 VM을 복구하기 위해 페일오버를 트리거할 수 있습니다. 페일오버가 수행되면 복제된 VM이 원래 VM의 역할을 대신합니다. 페일오버는 복제본의 최신 상태 또는 알려진 정상 복구 지점으로 수행할 수 있습니다. 따라서 필요에 따라 랜섬웨어 복구 또는 격리된 테스트가 가능합니다. Veeam Backup & Replication은 다양한 재해 복구 시나리오를 처리할 수 있는 다양한 옵션을 제공합니다.

[]

솔루션 구축

고급 단계

1. Veeam Backup and Replication 소프트웨어는 적절한 네트워크 연결을 갖춘 사내 환경에서 실행됩니다.
2. "Azure VMware Solution(AVS) 배포" 프라이빗 클라우드 및 "Azure NetApp Files 데이터 저장소를 연결합니다" Azure VMware Solution 호스트에 연결할 수 있습니다.

   최소 구성으로 설정된 파일럿 라이트 환경을 DR 목적으로 사용할 수 있습니다. 장애 발생 시 VM이 이 클러스터로 페일오버되고 추가 노드를 추가할 수 있습니다.)

3. Veeam Backup and Replication을 사용하여 VM 복제본을 생성하도록 복제 작업을 설정합니다.
4. 페일오버 계획을 만들고 페일오버를 수행합니다.
5. 재해 이벤트가 완료되고 운영 사이트가 가동되면 운영 VM으로 다시 전환합니다.

AVS 및 **ANF** 데이터 저장소로의 **Veeam VM** 복제를 위한 사전 요구 사항

1. Veeam Backup & Replication 백업 VM이 소스 및 타겟 AVS SDDC 클러스터에 연결되어 있는지 확인합니다.
2. 백업 서버는 짧은 이름을 확인하고 소스 및 타겟 vCenter에 연결할 수 있어야 합니다.
3. 타겟 Azure NetApp Files 데이터 저장소에 복제된 VM의 VMDK를 저장할 수 있는 충분한 여유 공간이 있어야 합니다.

자세한 내용은 "고려 사항 및 제한 사항"을 참조하십시오 "여기".

배포 세부 정보

1단계**: VM** 복제

Veeam Backup & Replication은 VMware vSphere 스냅샷 기능을 활용하며/ 복제 중에 Veeam Backup & Replication은 VMware vSphere에 VM 스냅샷을 생성하도록 요청합니다. VM 스냅샷은 가상 디스크, 시스템 상태, 구성 및 메타데이터를 포함하는 VM의 시점 복제본입니다. Veeam Backup & Replication은 이 스냅샷을 복제용 데이터 소스로 사용합니다.

VM을 복제하려면 다음 단계를 수행하십시오.

1. Veeam Backup & Replication Console을 엽니다.
2. 홈 보기에서. 작업 노드를 마우스 오른쪽 버튼으로 클릭하고 복제 작업 > 가상 머신 을 선택합니다.
3. 작업 이름을 지정하고 해당 고급 제어 확인란을 선택합니다. 다음 을 클릭합니다.
   - 온-프레미스와 Azure 간의 연결에 대역폭이 제한된 경우 복제 시드 확인란을 선택합니다.
     - Azure VMware Solution SDDC의 세그먼트가 온프레미스 사이트 네트워크의 세그먼트와 일치하지 않는 경우 네트워크 재매핑(네트워크가 다른 AVS SDDC 사이트의 경우) 확인란을 선택합니다.
   - 온프레미스 운영 사이트의 IP 주소 지정 체계가 타겟 AVS 사이트의 체계와 다른 경우 복제 Re-IP(IP 주소 지정 체계가 다른 DR 사이트의 경우) 확인란을 선택합니다.

     []
4. 가상 * 머신 * 단계에서 Azure VMware Solution SDDC에 연결된 Azure NetApp Files 데이터 저장소에 복제할 VM을 선택합니다. vSAN에 가상 머신을 배치하여 사용 가능한 vSAN 데이터스토어 용량을 채울 수 있습니다. 파일럿 라이트 클러스터에서는 3노드 클러스터의 가용 용량이 제한됩니다. 나머지 데이터는 Azure NetApp Files 데이터 저장소에 쉽게 배치하여 VM을 복구할 수 있으며, 클러스터를 확장하여 CPU/메모리 요구 사항을 충족할 수 있습니다. Add * 를 클릭한 다음 * Add Object * 창에서 필요한 VM 또는 VM 컨테이너를 선택하고 * Add * 를 클릭합니다. 다음 * 을 클릭합니다.

   []
5. 그런 다음 대상을 Azure VMware Solution SDDC 클러스터/호스트와 적절한 리소스 풀, VM 폴더 및 VM 복제본용 FSx for ONTAP 데이터 저장소로 선택합니다. 그런 다음 * 다음 * 을 클릭합니다.

   []
6. 다음 단계에서는 필요에 따라 소스 및 대상 가상 네트워크 간의 매핑을 생성합니다.

   []
7. 작업 설정 * 단계에서 VM 복제본, 보존 정책 등에 대한 메타데이터를 저장할 백업 리포지토리를 지정합니다.
8. 데이터 전송 * 단계에서 * 원본 * 및 * 대상 * 프록시 서버를 업데이트하고 * 자동 * 선택(기본값)을 그대로 두고 * 직접 * 옵션을 선택한 후 * 다음 * 을 클릭합니다.
9. Guest Processing * 단계에서 필요에 따라 * Enable application-aware processing * 옵션을 선택합니다. 다음 * 을 클릭합니다.

   []
10. 정기적으로 실행할 복제 작업을 실행할 복제 스케줄을 선택합니다.

    []

11. 마법사의 * Summary * 단계에서 복제 작업의 세부 정보를 검토합니다. 마법사를 닫은 후 바로 작업을 시작하려면 * 마침을 클릭하면 작업 실행 * 확인란을 선택하고, 그렇지 않으면 확인란을 선택하지 않은 상태로 둡니다. 그런 다음 * 마침 * 을 클릭하여 마법사를 닫습니다.

    []

복제 작업이 시작되면 지정된 접미사의 VM이 대상 AVS SDDC 클러스터/호스트에 채워집니다.

[]

Veeam 복제에 대한 자세한 내용은 을 참조하십시오 "복제 작동 방법"

2단계**:** 장애 조치 계획을 만듭니다

초기 복제 또는 시드가 완료되면 페일오버 계획을 생성합니다. 페일오버 계획은 종속 VM에 대해 하나씩 또는 그룹으로 자동 페일오버를 수행하는 데 도움이 됩니다. 페일오버 계획은 부팅 지연을 포함하여 VM이 처리되는 순서에 대한 청사진입니다. 또한 페일오버 계획은 중요한 종속 VM이 이미 실행 중인지 확인하는 데 도움이 됩니다.

계획을 생성하려면 * Replicas * 라는 새 하위 섹션으로 이동하여 * Failover Plan * 을 선택합니다. 적절한 VM을 선택합니다. Veeam Backup & Replication은 이 시점에 가장 가까운 복원 지점을 찾아 VM 복제를 시작하는 데 사용합니다.

ⓘ 초기 복제가 완료되고 VM 복제본이 준비 상태가 된 후에만 페일오버 계획을 추가할 수 있습니다.

ⓘ 페일오버 계획을 실행할 때 동시에 시작할 수 있는 최대 VM 수는 10개입니다

ⓘ 페일오버 프로세스 중에는 소스 VM의 전원이 꺼지지 않습니다

장애 조치 계획 * 을 만들려면 다음을 수행합니다.

1. 홈 보기에서. 복제본 노드를 마우스 오른쪽 버튼으로 클릭하고 페일오버 계획 > 페일오버 계획 > VMware vSphere를 선택합니다.

    []

2. 그런 다음 계획에 대한 이름과 설명을 입력합니다. 필요에 따라 사전 및 사후 페일오버 스크립트를 추가할 수 있습니다. 예를 들어 복제된 VM을 시작하기 전에 VM을 종료하는 스크립트를 실행합니다.

    []

3. VM을 계획에 추가하고 애플리케이션 종속성을 충족하도록 VM 부팅 순서 및 부팅 지연을 수정합니다.

    []

복제 작업 생성에 대한 자세한 내용은 을 참조하십시오 "복제 작업을 생성하는 중입니다".

3단계**:** 페일오버 계획을 실행합니다

페일오버 중에 프로덕션 사이트의 소스 VM이 재해 복구 사이트의 해당 복제본으로 전환됩니다. 페일오버 프로세스의 일부로 Veeam Backup & Replication은 VM 복제본을 필요한 복구 지점으로 복구하고 소스 VM의 모든 입출력 작업을 해당 복제본으로 이동합니다. 복제본은 재해 발생 시에만 사용할 수 있으며 DR 드릴을 시뮬레이션하는 데도 사용할 수 있습니다. 페일오버 시뮬레이션 중에는 소스 VM이 계속 실행 중입니다. 필요한 모든 테스트가 수행되면 페일오버를 취소하고 정상 작업으로 돌아갈 수 있습니다.

> 페일오버 중에 IP 충돌을 피하기 위해 네트워크 분할이 제대로 수행되었는지 확인하십시오.

장애 조치 계획을 시작하려면 * 장애 조치 계획 * 탭을 클릭하고 장애 조치 계획을 마우스 오른쪽 버튼으로 클릭합니다. 시작 * 을 선택합니다. 이렇게 하면 VM 복제본의 최신 복구 지점을 사용하여 장애 조치가 수행됩니다. VM 복제본의 특정 복원 지점으로 페일오버하려면 * 시작 * 을 선택합니다.

[]

[]

VM 복제본의 상태가 Ready에서 Failover로 변경되고 VM은 대상 AVS(Azure VMware Solution) SDDC 클러스터/호스트에서 시작됩니다.

[]

페일오버가 완료되면 VM의 상태가 "페일오버"로 변경됩니다.

[]

> Veeam Backup & Replication은 소스 VM의 복제본이 준비 상태로 돌아갈 때까지 소스 VM에 대한 모든 복제 작업을 중지합니다.

페일오버 계획에 대한 자세한 내용은 을 참조하십시오 "페일오버 계획".

4단계**:** 프로덕션 사이트로 페일백합니다

장애 조치 계획이 실행 중인 경우 중간 단계로 간주되며 요구 사항에 따라 확정되어야 합니다. 다음과 같은 옵션이 있습니다.

- * Failback to Production * - 원래 VM으로 다시 전환하고 VM 복제본이 실행되는 동안 발생한 모든 변경 사항을 원래 VM으로 전송합니다.

> 페일백을 수행하면 변경 내용이 전송되지만 게시되지는 않습니다. 원래 VM이 예상대로 작동하지 않는 경우 * 페일백 커밋 * (원래 VM이 예상대로 작동하는 것으로 확인된 경우) 또는 페일백 실행 취소 를 선택하여 VM 복제본으로 돌아갑니다.

- * 장애 조치 실행 취소 * - 원래 VM으로 다시 전환하고 실행 중에 VM 복제본의 모든 변경 사항을 취소합니다.
- * 영구 장애 조치 * - 원래 VM에서 VM 복제본으로 영구적으로 전환하고 이 복제본을 원래 VM으로 사용합니다.

이 데모에서는 Failback to Production을 선택했습니다. 마법사의 대상 단계에서 원래 VM으로 페일백이 선택되었고 "복원 후 VM 전원 켜기" 확인란이 활성화되었습니다.

[]

[]

[]

[]

페일백 커밋은 페일백 작업을 완료하는 방법 중 하나입니다. 페일백이 커밋되면 장애가 발생한 VM(운영 VM)에 전송된 변경 사항이 예상대로 작동하는지 확인합니다. 커밋 작업 후에 Veeam Backup & Replication은 운영 VM에 대한 복제 작업을 재개합니다.

페일백 프로세스에 대한 자세한 내용은 의 Veeam 문서를 참조하십시오 "복제를 위한 페일오버 및 페일백".

[]

운영 환경으로 페일백이 성공한 후 VM이 모두 원래 운영 사이트로 복구됩니다.

[]

결론

Azure NetApp Files 데이터 저장소 기능을 사용하면 Veeam 또는 검증된 타사 툴에서 VM 복제만 수용하기 위해 대규모 클러스터를 구성하는 대신 파일럿 라이트 클러스터를 활용하는 방법으로 저렴한 DR 솔루션을 제공할 수 있습니다. 이렇게 하면 맞춤형 재해 복구 계획을 효과적으로 처리하고 DR에 기존 백업 제품을 재사용할 수 있어, 온프레미스 DR 데이터 센터에서 클라우드 기반 재해 복구가 가능합니다. 재해가 발생한 경우 단추를 클릭하여 장애 조치를 수행하거나 재해가 발생한 경우 자동으로 장애 조치를 수행할 수 있습니다.

이 프로세스에 대해 자세히 알아보려면 자세한 단계별 안내 비디오를 참조하십시오.

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

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.