NetApp 퍼블릭 및 하이브리드 클라우드 솔루션

NetApp public and hybrid cloud solutions

NetApp
November 11, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/netapp-solutions-cloud/index.html on November 11, 2026. Always check docs.netapp.com for the latest.

목차

NetApp 퍼블릭 및 하이브리드 클라우드 솔루션 . . . 1
NetApp 퍼블릭 및 하이브리드 클라우드 솔루션의 새로운 기능 . . . 2
VMware 솔루션을 활용한 NetApp 하이브리드 멀티클라우드 . . . 3
퍼블릭 클라우드를 위한 VMware . . . 3
VMware를 활용한 NetApp 하이브리드 멀티클라우드 개요 . . . 3
하이퍼스케일러를 위한 VMware용 NetApp 솔루션 . . . 6
VMware를 사용한 NetApp 하이브리드 멀티클라우드에 지원되는 구성 . . . 9
하이퍼스케일러 구성의 VMware . . . 10
퍼블릭 클라우드의 NetApp 스토리지 . . . 34
요약 및 결론: VMware와 NetApp 하이브리드 멀티클라우드를 함께 사용하는 이유 . . . 131
VMware 하이브리드 클라우드 사용 사례 . . . 133
VMware를 활용한 NetApp 하이브리드 멀티클라우드 사용 사례 . . . 133
하이퍼스케일러를 위한 VMware용 NetApp 솔루션 . . . 134
Amazon VMware Managed Cloud(VMC)를 위한 NetApp 솔루션 . . . 134
Azure VMware 솔루션(AVS)을 위한 NetApp 솔루션 . . . 135
Google Cloud VMware Engine(GCVE)을 위한 NetApp 솔루션 . . . 135
AWS/VMC용 NetApp . . . 136
AWS VMC를 위한 NetApp 기능 . . . 136
AWS/VMC에서 워크로드 보호 . . . 137
AWS/VMC에서 워크로드 마이그레이션 . . . 250
AWS/EVS용 NetApp . . . 265
EVS의 외부 데이터 저장소로 FSx ONTAP 마운트 . . . 265
EVS용 FSx ONTAP 데이터 저장소 보호 . . . 289
Azure/AVS용 NetApp . . . 322
Azure AVS를 위한 NetApp 기능 . . . 323
Azure/AVS에서 워크로드 보호 . . . 324
Azure/AVS에서 워크로드 마이그레이션 . . . 389
GCP/GCVE용 NetApp . . . 402
Google Cloud Platform GCVE를 위한 NetApp 기능 . . . 402
GCP/GCVE에서 워크로드 보호 . . . 403
GCP/GCVE에서 워크로드 마이그레이션 . . . 434
Google Cloud의 Google Cloud NetApp Volumes 로 데이터 보호 . . . 451
NetApp Disaster Recovery . . . 512
VMware 워크로드를 보호하기 위한 SnapCenter 플러그인 및 NetApp Backup and Recovery를 활용한 VMware용 3-2-1 데이터 보호 . . . 512
NetApp Disaster Recovery . . . 545
Red Hat OpenShift 컨테이너 워크로드를 활용한 NetApp 하이브리드 멀티클라우드 . . . 585
시작하기 . . . 585
Red Hat OpenShift 컨테이너 워크로드를 위한 NetApp 하이브리드 멀티클라우드 솔루션 . . . 585

Red Hat OpenShift 컨테이너 워크로드를 위한 NetApp 하이브리드 멀티클라우드 솔루션의 가치 제안 . . . 587
Red Hat OpenShift 컨테이너 워크로드를 위한 NetApp Hybrid Multicloud 지원 솔루션 . . . 588
솔루션 검증에 사용된 다양한 구성 요소의 버전 . . . 591
Red Hat OpenShift 컨테이너와 지원되는 NetApp 스토리지 통합 . . . 592
추가 문서 . . . 596
온프레미스용 OpenShift . . . 596
VMware에서 Red Hat OpenShift Container 플랫폼 워크로드를 지원하는 NetApp 솔루션 . . . 596
VMware에서 Red Hat OpenShift Container 플랫폼 배포 및 구성 . . . 597
Trident Protect를 사용한 데이터 보호 . . . 599
자체 관리 구성 요소를 갖춘 하이브리드 클라우드 . . . 600
하이브리드 클라우드에서 Red Hat OpenShift 컨테이너 플랫폼 워크로드를 지원하는 NetApp 솔루션 . . . 600
AWS에서 Red Hat OpenShift 컨테이너 플랫폼 배포 및 구성 . . . 602
Google Cloud에서 Red Hat OpenShift Container Platform 배포 및 구성 . . . 604
Azure에서 Red Hat OpenShift 컨테이너 플랫폼 배포 및 구성 . . . 606
Trident Protect를 사용한 데이터 보호 . . . 609
공급자 관리 구성 요소를 갖춘 하이브리드 클라우드 . . . 609
관리형 Red Hat OpenShift 컨테이너 플랫폼 워크로드를 갖춘 NetApp 솔루션 . . . 609
AWS에서 관리형 Red Hat OpenShift 컨테이너 플랫폼 배포 및 구성 . . . 609
Google Cloud NetApp Volumes 사용하여 Google Cloud에 OpenShift Dedicated 배포 및 구성 . . . 612
데이터 보호 . . . 614
Red Hat OpenShift 워크로드를 위한 추가 NetApp 하이브리드 멀티클라우드 솔루션 . . . 614
Trident Protect를 사용하여 데이터 보호 . . . 615
Trident Protect를 사용하여 OpenShift Container Platform의 컨테이너 앱 데이터 보호 . . . 615
Trident Protect를 사용하여 Red Hat OpenShift Virtualization의 VM 보호 . . . 626
타사 도구를 사용하여 컨테이너 앱 보호 . . . 647
OpenShift API for Data Protection(OADP)을 사용하여 OpenShift Container Platform의 컨테이너 앱에 대한 데이터 보호 . . . 647
데이터 보호를 위한 OpenShift API(OADP) 운영자 설치 . . . 648
OpenShift 컨테이너 플랫폼에서 앱에 대한 주문형 백업 생성 . . . 657
한 클러스터에서 다른 클러스터로 앱 마이그레이션 . . . 660
백업에서 앱 복원 . . . 664
Velero를 사용하여 백업 및 복원 삭제 . . . 671
NetApp 사용한 하이브리드 멀티클라우드 솔루션에 대한 비디오와 데모를 시청하세요 . . . 673
NetApp 사용한 Amazon Web Services용 하이브리드 멀티클라우드 솔루션에 대한 비디오를 시청하세요 . . . 673
게스트 연결 스토리지 . . . 673
TCO 및 보충 데이터 저장소 . . . 673
마이그레이션 워크플로(HCX) . . . 673
NetApp 사용한 Azure VMware 클라우드를 위한 하이브리드 멀티클라우드 솔루션에 대한 비디오를 시청하세요 . . . 673
보충 데이터 저장소 . . . 673
재해 복구 . . . 673
마이그레이션 워크플로(HCX) . . . 674

NetApp 과 Red Hat OpenShift를 위한 하이브리드 멀티클라우드 솔루션에 대한 비디오를 시청하세요 . . . 674
스냅샷 및 복원 . . . 674
스토리지 통합 . . . 674
장애 조치 및 장애 복구 . . . 674
솔루션 자동화 . . . 674
NetApp 전문가의 클라우드 솔루션 블로그를 읽어보세요 . . . 675
AWS 및 Amazon FSx for ONTAP 과 VMware 통합 . . . 675
Azure VMware 솔루션 . . . 675
구글 클라우드 VMware 엔진 . . . 675
데이터 보호 및 관리 . . . 675
OpenShift 컨테이너 워크로드를 위한 NetApp . . . 675
VMware Sovereign Cloud . . . 675
법적 고지 사항 . . . 676
저작권 . . . 676
상표 . . . 676
특허 . . . 676
개인정보 보호정책 . . . 676

NetApp 퍼블릭 및 하이브리드 클라우드 솔루션

NetApp 퍼블릭 및 하이브리드 클라우드 솔루션의 새로운 기능

퍼블릭 및 하이브리드 클라우드 솔루션의 새로운 소식을 알아보세요.

[[18-august-2025]]
== 2025년 8월 18일

NetApp Solutions 사이트는 이제"NetApp 솔루션 제품군" 다음 사이트를 포함합니다.

- "NetApp 인공지능 솔루션"
- "NetApp 컨테이너 솔루션"
- "NetApp 데이터 관리 솔루션"
- "NetApp 데이터베이스 솔루션"
- NetApp 퍼블릭 및 하이브리드 클라우드 솔루션
- "SAP용 NetApp 솔루션"
- "NetApp 가상화 솔루션"

VMware 솔루션을 활용한 NetApp 하이브리드 멀티클라우드

퍼블릭 클라우드를 위한 VMware

VMware를 활용한 NetApp 하이브리드 멀티클라우드 개요

대부분의 IT 조직은 하이브리드 클라우드 우선 접근 방식을 따릅니다. 이러한 조직은 변화 단계에 있으며, 고객은 현재 IT 환경을 평가한 다음 평가 및 발견 활동을 기반으로 워크로드를 클라우드로 마이그레이션하고 있습니다.

고객이 클라우드로 마이그레이션하는 데에는 탄력성과 폭발성, 데이터 센터 종료, 데이터 센터 통합, 수명 종료 시나리오, 합병, 인수 등이 포함될 수 있습니다. 이러한 마이그레이션의 이유는 각 조직과 해당 비즈니스 우선순위에 따라 다를 수 있습니다. 하이브리드 클라우드로 전환할 때 클라우드 배포의 힘과 탄력성을 최대한 활용하기 위해 클라우드에서 올바른 스토리지를 선택하는 것이 매우 중요합니다.

퍼블릭 클라우드의 VMware Cloud 옵션

이 섹션에서는 각 클라우드 공급업체가 각자의 퍼블릭 클라우드 서비스 내에서 VMware 소프트웨어 정의 데이터 센터(SDDC) 및/또는 VMware Cloud Foundation(VCF) 스택을 지원하는 방식을 설명합니다.

Azure VMware 솔루션

Azure VMware Solution은 Microsoft Azure 퍼블릭 클라우드 내에서 완벽한 기능을 갖춘 VMware SDDC를 구현할 수 있는 하이브리드 클라우드 서비스입니다. Azure VMware 솔루션은 Microsoft에서 완벽하게 관리하고 지원하는 자체 솔루션으로, Azure 인프라를 활용하여 VMware에서 검증되었습니다. 즉, Azure VMware Solution을 배포하면 고객은 컴퓨팅 가상화를 위한 VMware ESXi, 하이퍼 컨버지드 스토리지를 위한 vSAN, 네트워킹 및 보안을 위한 NSX를 모두 이용할 수 있으며, Microsoft Azure의 글로벌 입지, 동급 최고의 데이터 센터 시설, 풍부한 네이티브 Azure 서비스 및 솔루션 생태계와의 근접성을 활용할 수 있습니다.

AWS의 VMware 클라우드

AWS의 VMware Cloud는 기본 AWS 서비스에 대한 최적화된 액세스를 통해 VMware의 엔터프라이즈급 SDDC 소프트웨어를 AWS 클라우드에 제공합니다. VMware Cloud Foundation 기반의 VMware Cloud on AWS는 VMware의 컴퓨팅, 스토리지 및 네트워크 가상화 제품(VMware vSphere, VMware vSAN 및 VMware NSX)과 VMware vCenter Server 관리를 통합하여 전용의 탄력적 베어메탈 AWS 인프라에서 실행되도록 최적화되었습니다.

구글 클라우드 VMware 엔진

Google Cloud VMware Engine은 Google Cloud의 고성능 확장형 인프라와 VMware Cloud Foundation 스택(VMware vSphere, vCenter, vSAN, NSX-T)을 기반으로 구축된 서비스형 인프라(IaaS) 제품입니다. 이 서비스를 통해 기존 VMware 워크로드를 온프레미스 환경에서 Google Cloud Platform으로 원활하게 마이그레이션하거나 확장하여 클라우드로 빠르게 전환할 수 있으며, 애플리케이션 재설계나 운영 재구축에 따른 비용, 노력 또는 위험 부담 없이 운영을 재구축할 수 있습니다. Google에서 판매 및 지원하는 서비스로, VMware와 긴밀히 협력하고 있습니다.

SDDC 프라이빗 클라우드와 NetApp Cloud Volumes 콜로케이션은 최소한의 네트워크 지연 시간으로 최고의 성능을 제공합니다.

알고 계셨나요**?**

어떤 클라우드를 사용하든 VMware SDDC가 배포되면 초기 클러스터에는 다음 제품이 포함됩니다.

- 관리를 위한 vCenter Server 어플라이언스를 사용한 컴퓨팅 가상화를 위한 VMware ESXi 호스트
- 각 ESXi 호스트의 물리적 스토리지 자산을 통합한 VMware vSAN 하이퍼 컨버지드 스토리지
- 관리를 위한 NSX Manager 클러스터를 갖춘 가상 네트워킹 및 보안을 위한 VMware NSX

스토리지 구성

스토리지 집약적 워크로드를 호스팅하고 클라우드 호스팅 VMware 솔루션에서 확장하려는 고객의 경우, 기본 하이퍼 컨버지드 인프라는 컴퓨팅 및 스토리지 리소스 모두에서 확장이 이루어져야 함을 나타냅니다.

Azure NetApp Files, Amazon FSx ONTAP, Cloud Volumes ONTAP (3대 하이퍼스케일러에서 모두 사용 가능), Google Cloud NetApp Volumes for Google Cloud 등의 NetApp Cloud Volumes와 통합함으로써 이제 고객은 스토리지를 개별적으로 독립적으로 확장하고 필요에 따라서만 SDDC 클러스터에 컴퓨팅 노드를 추가할 수 있습니다.

참고사항**:**

- VMware에서는 불균형적인 클러스터 구성을 권장하지 않습니다. 따라서 스토리지를 확장하면 호스트를 더 추가해야 하며, 이는 TCO 증가로 이어집니다.
- vSAN 환경은 하나만 가능합니다. 따라서 모든 스토리지 트래픽은 프로덕션 워크로드와 직접적으로 경쟁하게 됩니다.
- 애플리케이션 요구 사항, 성능 및 비용을 조정하기 위해 여러 성능 계층을 제공하는 옵션은 없습니다.
- 클러스터 호스트 위에 구축된 vSAN의 저장 용량 한계에 도달하는 것은 매우 쉽습니다. NetApp Cloud Volumes를 사용하면 스토리지를 확장하여 활성 데이터 세트를 호스팅하거나 쿨러 데이터를 영구 스토리지로 계층화할 수 있습니다.

Azure NetApp Files, Amazon FSx ONTAP, Cloud Volumes ONTAP (3대 주요 하이퍼스케일러에서 모두 사용 가능), Google Cloud용 Google Cloud NetApp Volumes 게스트 VM과 함께 사용할 수 있습니다. 이 하이브리드 스토리지 아키텍처는 게스트 운영 체제와 애플리케이션 바이너리 데이터를 보관하는 vSAN 데이터스토어로 구성됩니다. 애플리케이션 데이터는 게스트 기반 iSCSI 초기자 또는 Google Cloud용 Amazon FSx ONTAP, Cloud Volume ONTAP, Azure NetApp Files 및 Google Cloud NetApp Volumes 와 직접 통신하는 NFS/SMB 마운트를 통해 VM에 연결됩니다. 이 구성을 사용하면 vSAN의 경우 저장 용량과 관련된 문제를 쉽게 극복할 수 있습니다. 사용 가능한 여유 공간은 여유 공간과 사용하는 저장 정책에 따라 달라집니다.

AWS의 VMware Cloud에서 3노드 SDDC 클러스터를 고려해 보겠습니다.

- 3노드 SDDC의 총 원시 용량은 31.1TB(노드당 약 10TB)입니다.
- 추가 호스트를 추가하기 전에 유지해야 할 여유 공간 = 25% = (.25 x 31.1TB) = 7.7TB.
- 여유 공간을 차감한 후 사용 가능한 원시 용량 = 23.4TB
- 사용 가능한 유효 여유 공간은 적용되는 저장 정책에 따라 달라집니다.

  예를 들어:

  - RAID 0 = 유효 여유 공간 = 23.4TB(사용 가능한 원시 용량/1)
  - RAID 1 = 유효 여유 공간 = 11.7TB(사용 가능한 원시 용량/2)
  - RAID 5 = 유효 여유 공간 = 17.5TB(사용 가능한 원시 용량/1.33)

따라서 NetApp Cloud Volumes를 게스트 연결 스토리지로 사용하면 성능 및 데이터 보호 요구 사항을 충족하는 동시에 스토리지를 확장하고 TCO를 최적화하는 데 도움이 됩니다.

이 문서가 작성되었을 당시에는 게스트 내 스토리지가 유일한 사용 가능한 옵션이었습니다.

기억해야 할 점

- 하이브리드 스토리지 모델에서는 호스트 자체의 일부이며 근접해 있기 때문에 특정 지연 시간 요구 사항을 해결하기 위해 vSAN 데이터 저장소에 1계층 또는 높은 우선순위의 워크로드를 배치합니다. 트랜잭션 지연이 허용되는 모든 워크로드 VM에 대해 게스트 내 메커니즘을 사용합니다.
- 블록 수준 메커니즘을 사용하여 마이그레이션을 간소화하려면 NetApp SnapMirror 기술을 사용하여 온프레미스 ONTAP 시스템의 워크로드 데이터를 Cloud Volumes ONTAP 또는 Amazon FSx ONTAP으로 복제하십시오. 이는 Azure NetApp Files 및 Google Cloud NetApp Volumes에는 적용되지 않습니다. Azure NetApp Files 또는 Google Cloud NetApp Volumes로 데이터를 마이그레이션하려면 사용되는 파일 프로토콜에 따라 NetApp XCP, NetApp Copy and Sync, rysnc 또는 robocopy를 사용하십시오.
- 테스트 결과, 각 SDDC에서 스토리지에 액세스하는 동안 2~4ms의 추가 지연이 발생하는 것으로 나타났습니다. 저장소를 매핑할 때 애플리케이션 요구 사항에 이러한 추가 지연 시간을 고려하세요.
- 테스트 장애 조치 및 실제 장애 조치 중에 게스트 연결 스토리지를 마운트하려면 iSCSI 이니시에이터가 재구성되었는지, SMB 공유에 대한 DNS가 업데이트되었는지, NFS 마운트 지점이 fstab에 업데이트되었는지 확인하세요.
- VM 내부에서 게스트 Microsoft Multipath I/O(MPIO), 방화벽 및 디스크 시간 초과 레지스트리 설정이 올바르게 구성되었는지 확인하세요.

이는 게스트 연결 스토리지에만 적용됩니다.

NetApp 클라우드 스토리지의 이점

NetApp 클라우드 스토리지는 다음과 같은 이점을 제공합니다.

- 컴퓨팅과 독립적으로 스토리지를 확장하여 컴퓨팅-스토리지 밀도를 개선합니다.
- 호스트 수를 줄여 전반적인 TCO를 절감할 수 있습니다.
- 컴퓨팅 노드 장애는 스토리지 성능에 영향을 미치지 않습니다.
- Azure NetApp Files 의 볼륨 재구성 및 동적 서비스 수준 기능을 사용하면 안정적인 작업 부하에 맞춰 크기를 조정하여 비용을 최적화하고 과도한 프로비저닝을 방지할 수 있습니다.
- Cloud Volumes ONTAP 의 스토리지 효율성, 클라우드 계층화, 인스턴스 유형 수정 기능을 통해 스토리지를 추가하고 확장하는 최적의 방법을 제공합니다.
- 과도한 프로비저닝을 방지하고 필요할 때만 스토리지 리소스가 추가됩니다.
- 효율적인 스냅샷 복사 및 복제를 사용하면 성능에 영향을 주지 않고 빠르게 복사본을 만들 수 있습니다.
- 스냅샷 복사본을 통한 빠른 복구를 통해 랜섬웨어 공격에 대응하는 데 도움이 됩니다.
- 효율적인 증분형 블록 전송 기반 지역 재해 복구를 제공하고, 지역 전반에 걸쳐 통합된 백업 블록 수준을 제공하여 더 나은 RPO와 RTO를 제공합니다.

가정

- SnapMirror 기술이나 기타 관련 데이터 마이그레이션 메커니즘이 활성화되어 있습니다. 온프레미스부터

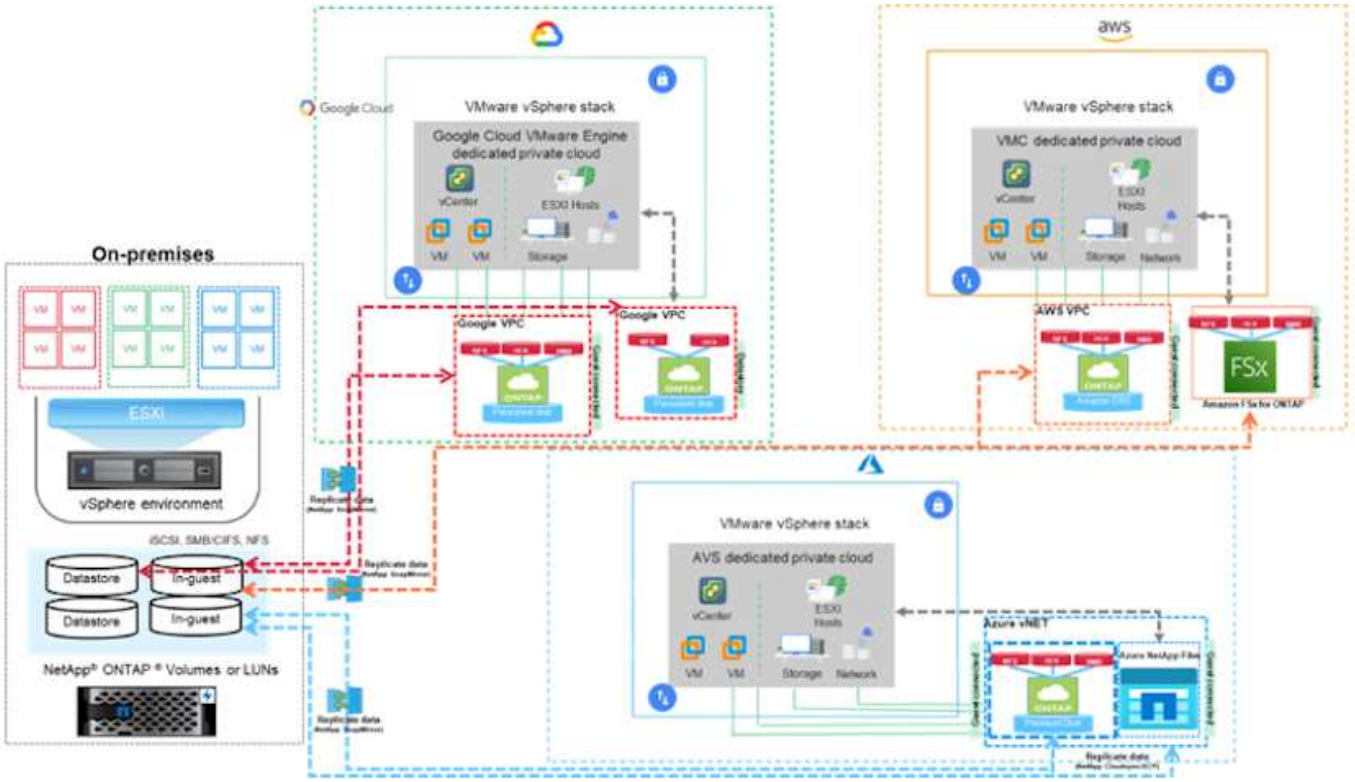
하이퍼스케일러 클라우드까지 다양한 연결 옵션이 있습니다. 적절한 경로를 사용하고 관련 네트워킹 팀과 협력하세요.

- 이 문서가 작성되었을 당시에는 게스트 내 스토리지가 유일한 사용 가능한 옵션이었습니다.

> ⓘ 스토리지 계획 및 크기 조정, 필요한 호스트 수를 위해 NetApp 솔루션 아키텍트와 해당 하이퍼스케일러 클라우드 아키텍트를 참여시킵니다. NetApp Cloud Volumes ONTAP 사이저를 사용하기 전에 스토리지 성능 요구 사항을 파악하여 스토리지 인스턴스 유형이나 적절한 처리량을 갖춘 적절한 서비스 수준을 확정할 것을 권장합니다.

세부적인 아키텍처

높은 수준의 관점에서 볼 때, 이 아키텍처(아래 그림 참조)는 NetApp Cloud Volumes ONTAP, Google Cloud NetApp Volumes for Google Cloud 및 Azure NetApp Files 추가 게스트 스토리지 옵션으로 사용하여 여러 클라우드 공급자 간에 하이브리드 멀티클라우드 연결 및 앱 이동성을 달성하는 방법을 다룹니다.



하이퍼스케일러를 위한 **VMware**용 **NetApp** 솔루션

NetApp 이 세 가지(3) 주요 하이퍼스케일러에 제공하는 기능에 대해 자세히 알아보세요. NetApp 은 게스트 연결 스토리지 장치 또는 보조 NFS 데이터 저장소로 사용되거나 워크플로 마이그레이션, 클라우드로 확장/버스팅, 백업/복원 및 재해 복구에 사용됩니다.

클라우드를 선택하고 나머지는 NetApp 에 맡겨보세요!



특정 하이퍼스케일러의 기능을 보려면 해당 하이퍼스케일러에 적합한 탭을 클릭하세요.

다음 옵션 중에서 선택하여 원하는 콘텐츠 섹션으로 이동하세요.

- "하이퍼스케일러 구성의 VMware"
- "NetApp 스토리지 옵션"
- "NetApp / VMware 클라우드 솔루션"

하이퍼스케일러 구성의 **VMware**

온프레미스와 마찬가지로, VM을 만들고 마이그레이션하기 위한 성공적인 프로덕션 준비 환경을 위해서는 클라우드 기반 가상화 환경을 계획하는 것이 중요합니다.

AWS / VMC

이 섹션에서는 AWS SDDC에서 VMware Cloud를 설정하고 관리하는 방법과 NetApp 스토리지를 연결하는 데 사용 가능한 옵션과 함께 사용하는 방법을 설명합니다.

게스트 내 스토리지는 Cloud Volumes ONTAP AWS VMC에 연결하는 데 지원되는 유일한 방법입니다.

설정 과정은 다음 단계로 나눌 수 있습니다.

- AWS용 VMware Cloud 배포 및 구성
- VMware Cloud를 FSx ONTAP 에 연결

자세한 내용을 보려면"VMC 구성 단계" .

Azure / AVS

이 섹션에서는 Azure VMware Solution을 설정하고 관리하는 방법과 NetApp 스토리지를 연결하는 데 사용 가능한 옵션과 함께 사용하는 방법을 설명합니다.

게스트 내 스토리지는 Cloud Volumes ONTAP Azure VMware Solution에 연결하는 데 지원되는 유일한 방법입니다.

설정 과정은 다음 단계로 나눌 수 있습니다.

- 리소스 공급자를 등록하고 프라이빗 클라우드를 생성하세요
- 새 ExpressRoute 가상 네트워크 게이트웨이 또는 기존 ExpressRoute 가상 네트워크 게이트웨이에 연결
- 네트워크 연결을 검증하고 프라이빗 클라우드에 액세스합니다.

자세한 내용을 보려면"AVS 구성 단계" .

GCP/GCVE

이 섹션에서는 GCVE를 설정하고 관리하는 방법과 NetApp 스토리지 연결에 사용 가능한 옵션과 함께 사용하는 방법을 설명합니다.

게스트 내 스토리지는 Cloud Volumes ONTAP 및 Google Cloud NetApp Volumes GCVE에 연결하는 데 지원되는 유일한 방법입니다.

설정 과정은 다음 단계로 나눌 수 있습니다.

- GCVE 배포 및 구성
- GCVE에 대한 개인 액세스 활성화

자세한 내용을 보려면"GCVE 구성 단계" .

NetApp 스토리지 옵션

NetApp 스토리지는 3대 주요 하이퍼스케일러 내에서 게스트 연결 또는 보조 NFS 데이터 저장소로 등 여러 가지 방법으로 활용할 수 있습니다.

방문해주세요"지원되는 NetApp 스토리지 옵션" 자세한 내용은.

AWS / VMC

AWS는 다음 구성에서 NetApp 스토리지를 지원합니다.

- 게스트 연결 스토리지로서의 FSx ONTAP
- 게스트 연결 스토리지로서의 Cloud Volumes ONTAP (CVO)
- 보충 NFS 데이터 저장소로서의 FSx ONTAP

자세한 내용을 보려면"VMC용 게스트 연결 스토리지 옵션" . 자세한 내용을 보려면"VMC에 대한 보충 NFS 데이터 저장소 옵션" .

Azure / AVS

Azure는 다음 구성에서 NetApp 스토리지를 지원합니다.

- 게스트 연결 스토리지로서의 Azure NetApp Files (ANF)

- 게스트 연결 스토리지로서의 Cloud Volumes ONTAP (CVO)
- 보조 NFS 데이터 저장소로서의 Azure NetApp Files (ANF)

자세한 내용을 보려면"AVS용 게스트 연결 스토리지 옵션" . 자세한 내용을 보려면"AVS를 위한 보충 NFS 데이터 저장소 옵션" .

GCP/GCVE

Google Cloud는 다음 구성에서 NetApp 스토리지를 지원합니다.

- 게스트 연결 스토리지로서의 Cloud Volumes ONTAP (CVO)
- 게스트 연결 스토리지로서의 Google Cloud NetApp Volumes (NetApp Volumes)
- Google Cloud NetApp Volumes (NetApp Volumes)를 보조 NFS 데이터 저장소로 사용

자세한 내용을 보려면"GCVE를 위한 게스트 연결 스토리지 옵션" . 자세한 내용을 보려면"GCVE에 대한 보충 NFS 데이터 저장소 옵션" .

더 자세히 알아보세요"Google Cloud NetApp Volumes 데이터 저장소 지원(NetApp 블로그)" 또는"Google Cloud NetApp Volumes Google Cloud VMware Engine의 데이터 저장소로 사용하는 방법(Google 블로그)"

NetApp / VMware 클라우드 솔루션

NetApp 및 VMware 클라우드 솔루션을 사용하면 많은 사용 사례를 원하는 하이퍼스케일러에 간편하게 배포할 수 있습니다. VMware는 주요 클라우드 워크로드 사용 사례를 다음과 같이 정의합니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 이주하다
- 연장하다

AWS / VMC

"AWS/VMC용 NetApp 솔루션 찾아보기"

Azure / AVS

"Azure/AVS용 NetApp 솔루션 찾아보기"

GCP/GCVE

"Google Cloud Platform(GCP)/GCVE를 위한 NetApp 솔루션을 찾아보세요"

VMware를 사용한 NetApp 하이브리드 멀티클라우드에 지원되는 구성

주요 하이퍼스케일러에서 NetApp 스토리지 지원 조합을 이해합니다.

	게스트 연결	보충 **NFS** 데이터 저장소
아마존	CVO FSx ONTAP"세부"	FSx ONTAP"세부"
하늘빛	CVO ANF"세부"	ANF"세부"

지씨피	CVO NetApp 볼륨"세부"	NetApp 볼륨"세부"

하이퍼스케일러 구성의 **VMware**

클라우드 공급자에서 가상화 환경 구성

지원되는 각 하이퍼스케일러에서 가상화 환경을 구성하는 방법에 대한 자세한 내용은 여기에서 다룹니다.

AWS / VMC

이 섹션에서는 AWS SDDC에서 VMware Cloud를 설정하고 관리하는 방법과 NetApp 스토리지를 연결하는 데 사용 가능한 옵션과 함께 사용하는 방법을 설명합니다.

게스트 내 스토리지는 Cloud Volumes ONTAP AWS VMC에 연결하는 데 지원되는 유일한 방법입니다.

설정 과정은 다음 단계로 나눌 수 있습니다.

- AWS용 VMware Cloud 배포 및 구성
- VMware Cloud를 FSx ONTAP 에 연결

자세한 내용을 보려면"VMC 구성 단계" .

Azure / AVS

이 섹션에서는 Azure VMware Solution을 설정하고 관리하는 방법과 NetApp 스토리지를 연결하는 데 사용 가능한 옵션과 함께 사용하는 방법을 설명합니다.

게스트 내 스토리지는 Cloud Volumes ONTAP Azure VMware Solution에 연결하는 데 지원되는 유일한 방법입니다.

설정 과정은 다음 단계로 나눌 수 있습니다.

- 리소스 공급자를 등록하고 프라이빗 클라우드를 생성하세요
- 새 ExpressRoute 가상 네트워크 게이트웨이 또는 기존 ExpressRoute 가상 네트워크 게이트웨이에 연결
- 네트워크 연결을 검증하고 프라이빗 클라우드에 액세스합니다.

자세한 내용을 보려면"AVS 구성 단계" .

GCP/GCVE

이 섹션에서는 GCVE를 설정하고 관리하는 방법과 NetApp 스토리지 연결에 사용 가능한 옵션과 함께 사용하는 방법을 설명합니다.

게스트 내 스토리지는 Cloud Volumes ONTAP 및 Google Cloud NetApp Volumes GCVE에 연결하는 데 지원되는 유일한 방법입니다.

설정 과정은 다음 단계로 나눌 수 있습니다.

- GCVE 배포 및 구성
- GCVE에 대한 개인 액세스 활성화

자세한 내용을 보려면"GCVE 구성 단계" .

AWS에서 가상화 환경 배포 및 구성

온프레미스와 마찬가지로, VM을 만들고 마이그레이션하기 위한 성공적인 프로덕션 준비 환경을 조성하려면 VMware Cloud on AWS를 계획하는 것이 중요합니다.

이 섹션에서는 AWS SDDC에서 VMware Cloud를 설정하고 관리하는 방법과 NetApp 스토리지를 연결하는 데 사용 가능한 옵션과 함께 사용하는 방법을 설명합니다.

현재 Cloud Volumes ONTAP (CVO)을 AWS VMC에 연결하는 데 지원되는 유일한 방법은 게스트 내부 스토리지입니다.

설정 과정은 다음 단계로 나눌 수 있습니다.

▼ **AWS**용 **VMware Cloud** 배포 및 구성

"AWS의 VMware 클라우드"AWS 생태계에서 VMware 기반 워크로드에 대한 클라우드 네이티브 경험을 제공합니다. 각 VMware 소프트웨어 정의 데이터 센터(SDDC)는 Amazon Virtual Private Cloud(VPC)에서 실행되며 전체 VMware 스택(vCenter Server 포함), NSX-T 소프트웨어 정의 네트워킹, vSAN 소프트웨어 정의 스토리지, 그리고 워크로드에 컴퓨팅 및 스토리지 리소스를 제공하는 하나 이상의 ESXi 호스트를 제공합니다.

이 섹션에서는 AWS에서 VMware Cloud를 설정하고 관리하는 방법과 게스트 스토리지를 사용하여 AWS에서 Amazon FSx ONTAP 및/또는 Cloud Volumes ONTAP 과 함께 사용하는 방법을 설명합니다.

현재 Cloud Volumes ONTAP (CVO)을 AWS VMC에 연결하는 데 지원되는 유일한 방법은 게스트 내부 스토리지입니다.

설정 과정은 세 부분으로 나눌 수 있습니다.

▼ **AWS** 계정 등록

등록하세요"Amazon 웹 서비스 계정" .

시작하려면 AWS 계정이 필요합니다(아직 계정이 생성되어 있지 않은 경우). 새 계정이든 기존 계정이든 이 절차의 여러 단계를 수행하려면 계정에 대한 관리자 권한이 필요합니다. 이것을 보세요"링크" AWS 자격 증명에 대한 자세한 내용은 다음을 참조하세요.

▼ **My VMware** 계정 등록

등록하세요"내 VMware" 계정.

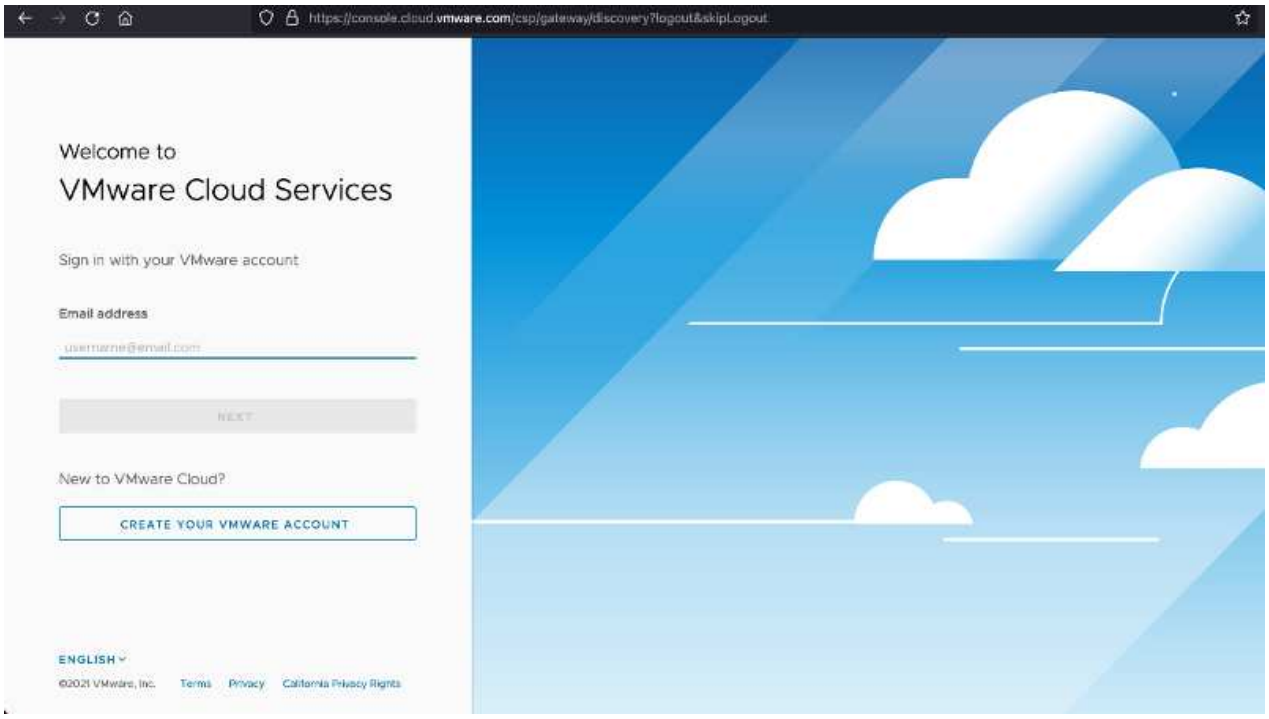
VMware의 클라우드 포트폴리오(VMware Cloud on AWS 포함)에 액세스하려면 VMware 고객 계정이나 My VMware 계정이 필요합니다. 아직 생성하지 않았다면 VMware 계정을 생성하세요."여기" .

▼ **VMware Cloud**에서 **SDDC** 프로비저닝

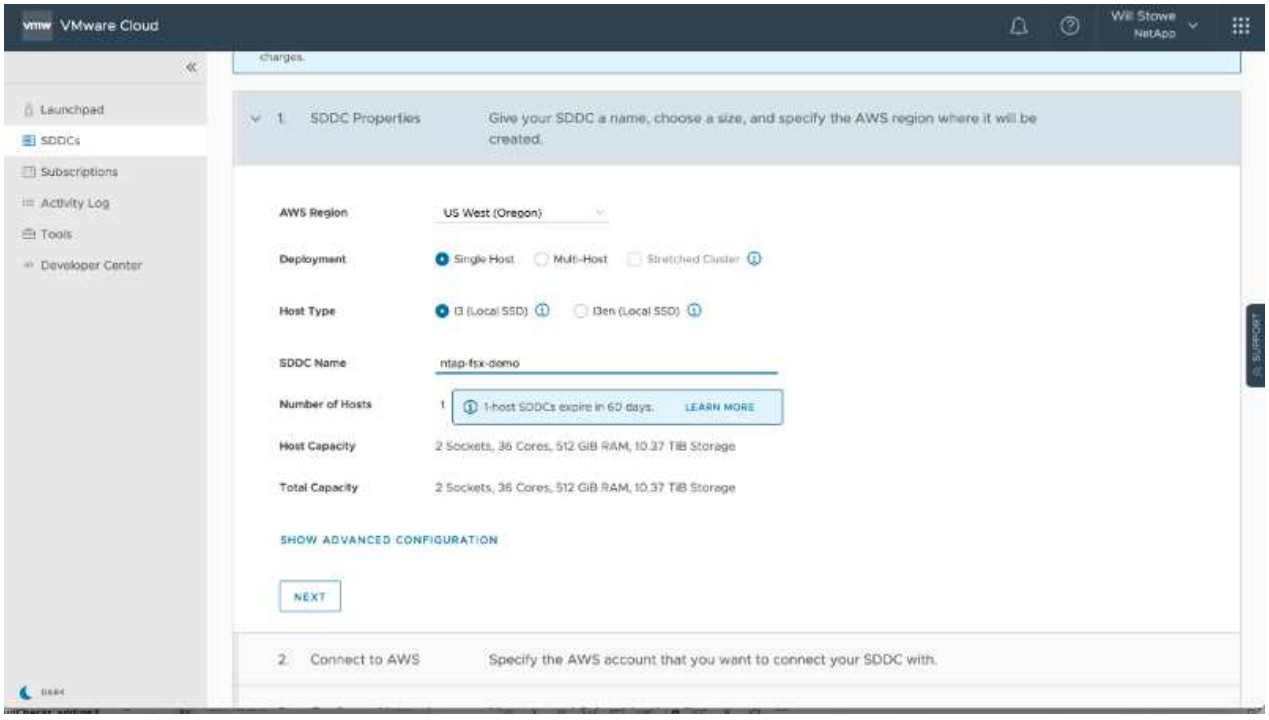
VMware 계정을 구성하고 적절한 크기 조정을 수행한 후 VMware Cloud on AWS 서비스를 사용하기 위한 다음 단계는 소프트웨어 정의 데이터 센터를 배포하는 것입니다. SDDC를 생성하려면 호스팅할 AWS 지역을 선택하고, SDDC 이름을 지정하고, SDDC에 포함할 ESXi 호스트 수를 지정합니다. 아직 AWS 계정이 없더라도 단일 ESXi

호스트를 포함하는 스타터 구성 SDDC를 만들 수 있습니다.

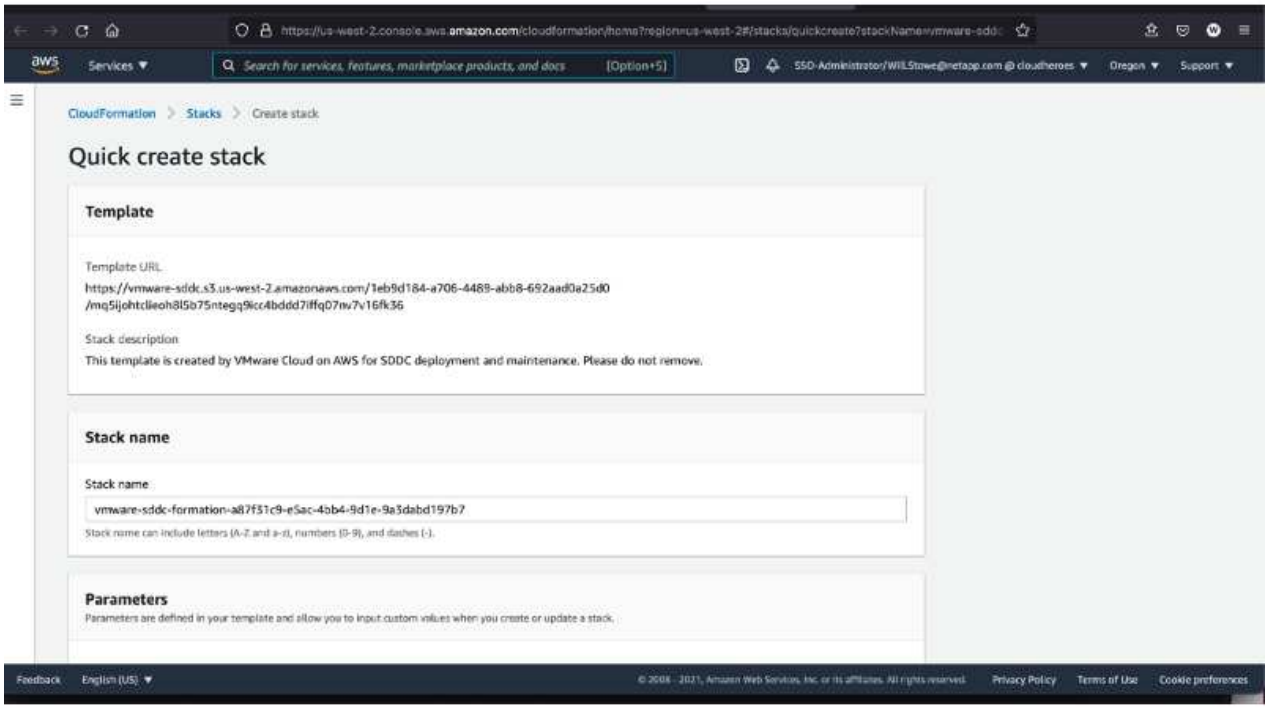
1. 기존 또는 새로 만든 VMware 자격 증명을 사용하여 VMware Cloud Console에 로그인합니다.

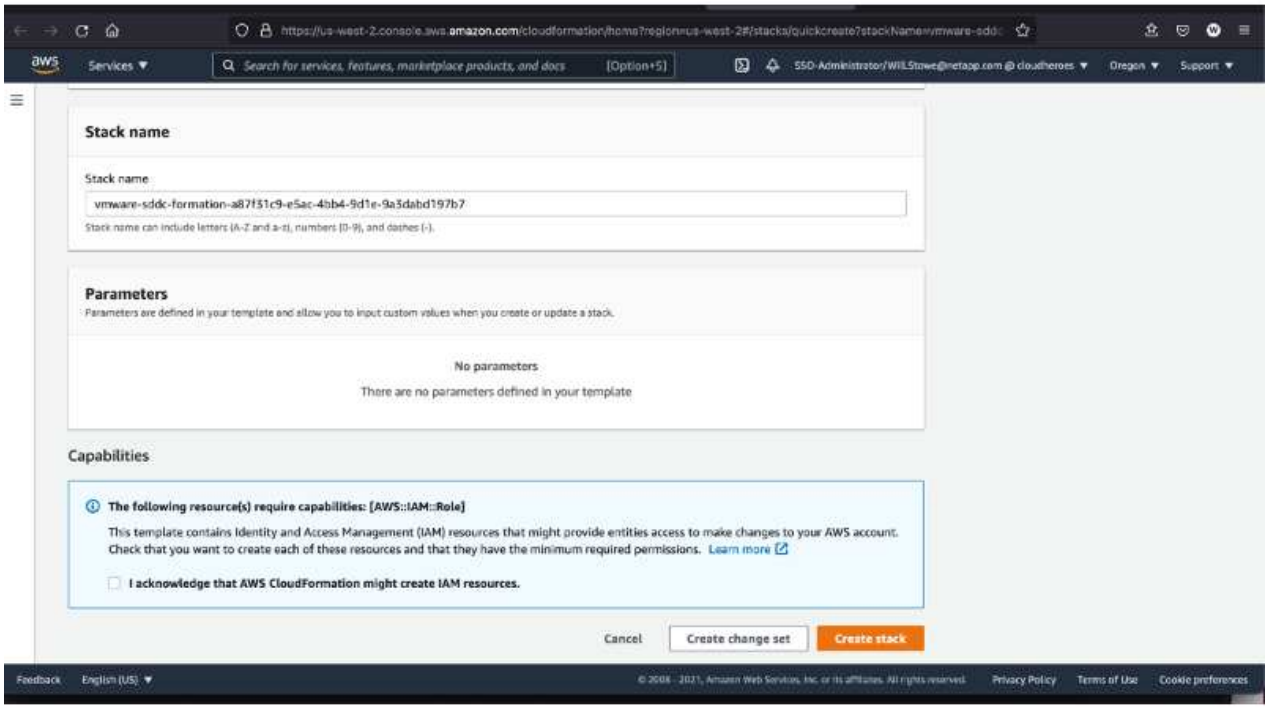


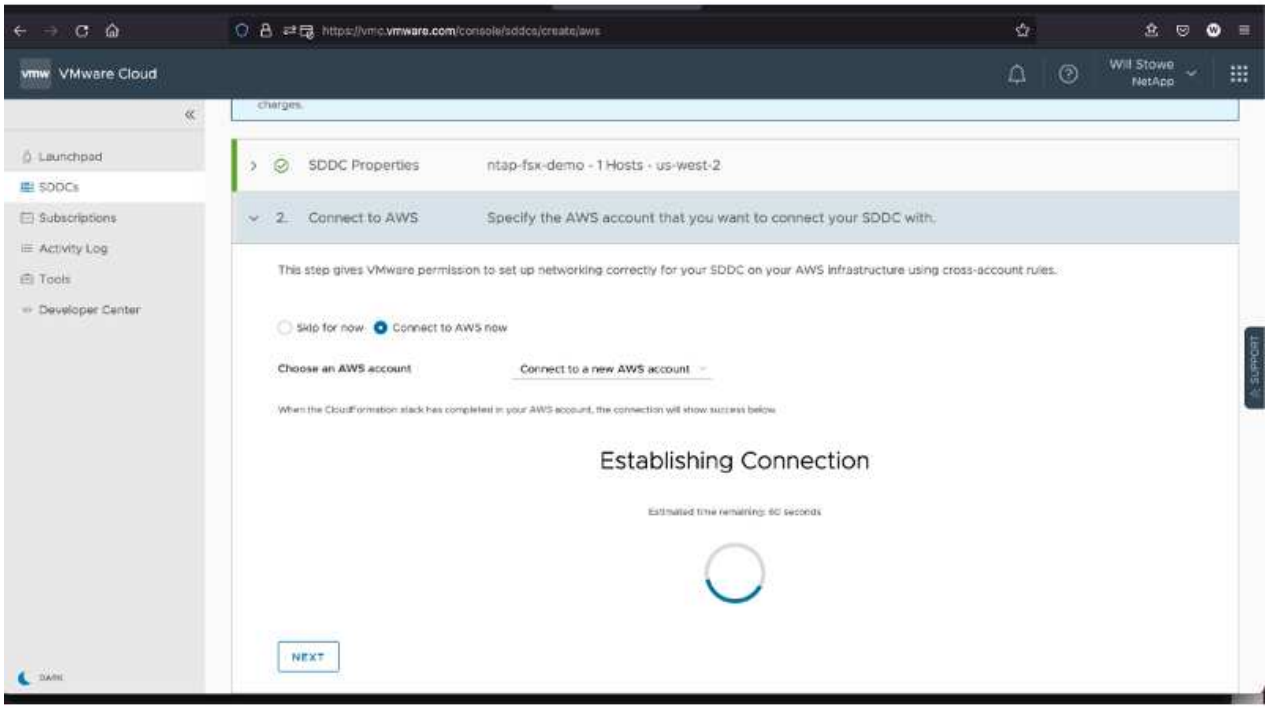
2. AWS 지역, 배포, 호스트 유형 및 SDDC 이름을 구성합니다.

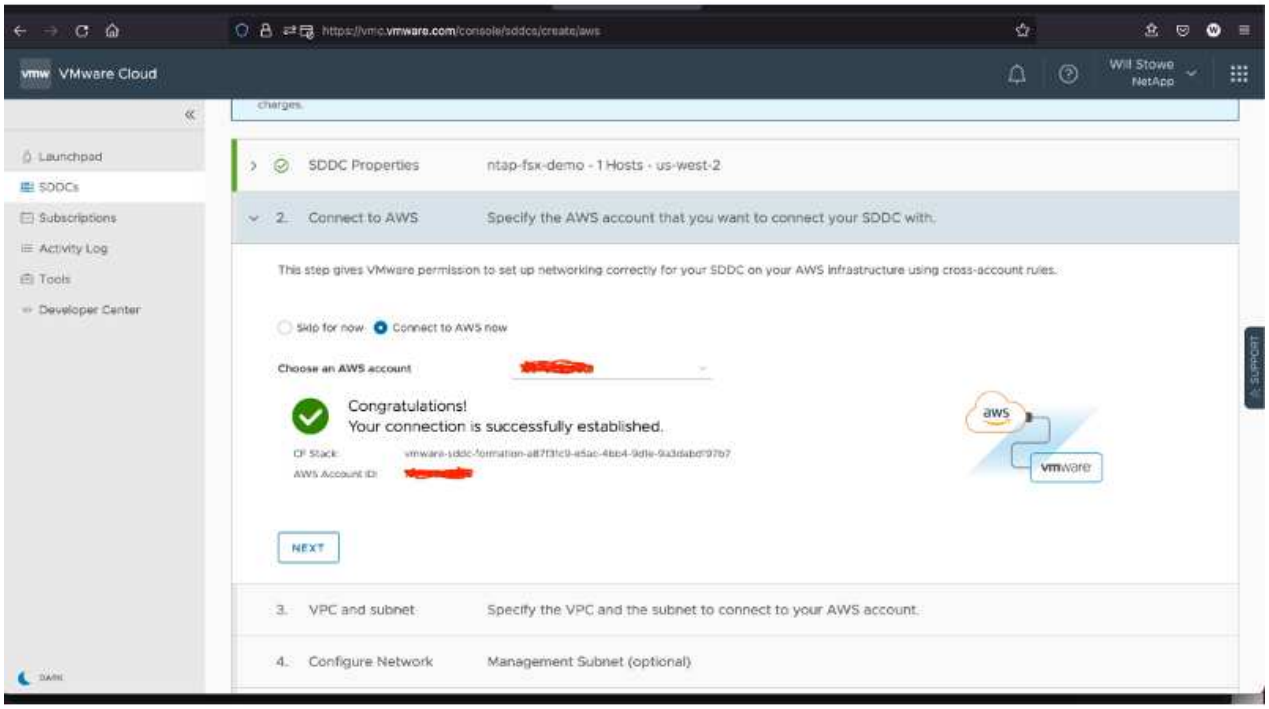


3. 원하는 AWS 계정에 연결하고 AWS Cloud Formation 스택을 실행합니다.


Services
Search for services, features, marketplace products, and docs [Option+S]
Oregon
Support
CloudFormation > Stacks > Create stack
Quick create stack
Template
Template URL
https://vmware-sddc.s3.us-west-2.amazonaws.com/1eb9d184-a706-4489-abb8-692aad0a25d0/mq5ljohtclieoh8l5b75ntegq9icc4bddd7iffq07nv7v16fk36
Stack description
This template is created by VMware Cloud on AWS for SDDC deployment and maintenance. Please do not remove.
Stack name
Stack name
vmware-sddc-formation-a87f31c9-e5ac-4bb4-9d1e-9a3dabd197b7
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
Feedback
English (US)
Privacy Policy
Terms of Use
Cookie preferences

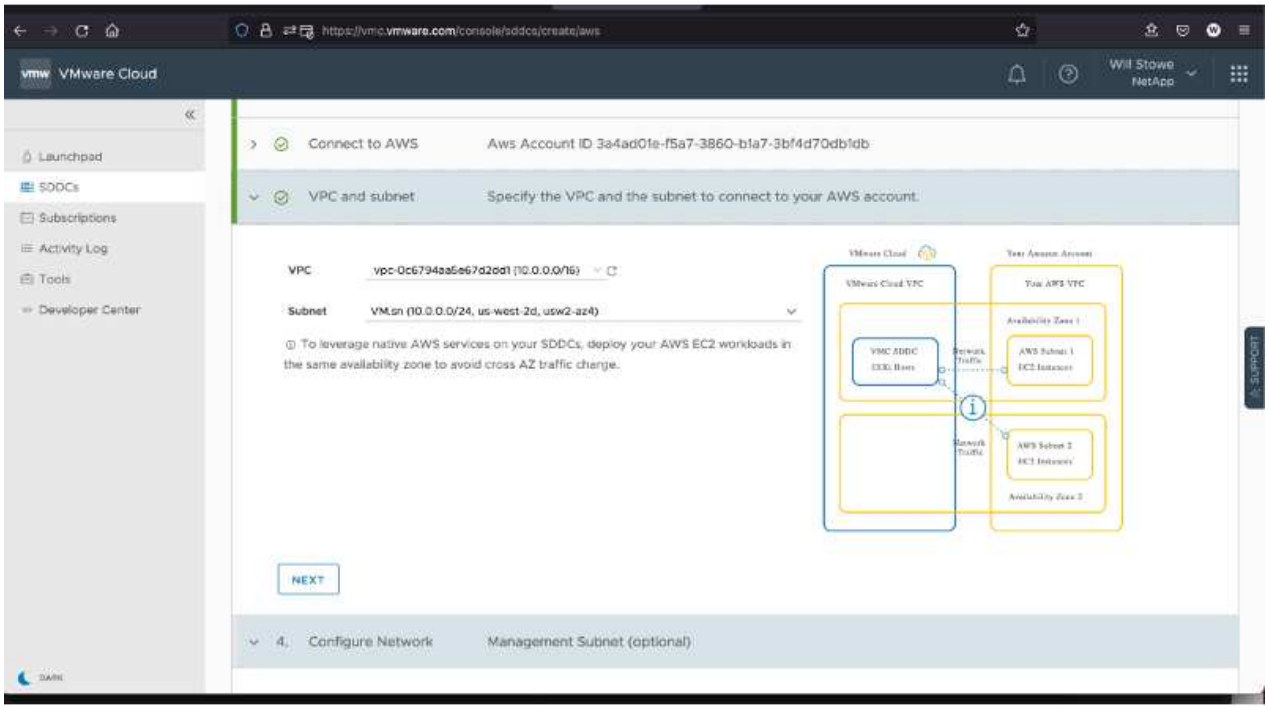

Services
Search for services, features, marketplace products, and docs [Option+S]
Oregon
Support
Stack name
Stack name
vmware-sddc-formation-a87f31c9-e5ac-4bb4-9d1e-9a3dabd197b7
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
No parameters
There are no parameters defined in your template
Capabilities
The following resource(s) require capabilities: [AWS::IAM::Role]
This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. Learn more
I acknowledge that AWS CloudFormation might create IAM resources.
Cancel
Create change set
Create stack
Feedback
English (US)
Privacy Policy
Terms of Use
Cookie preferences



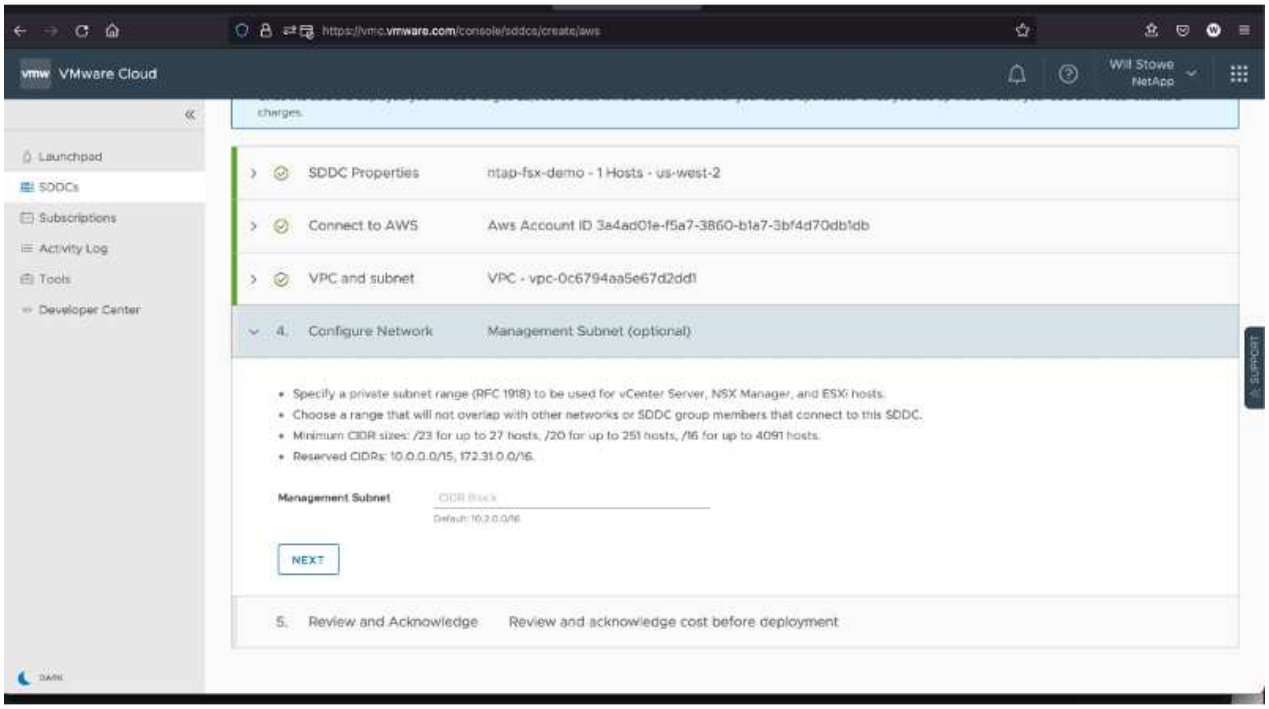


이 검증에서는 단일 호스트 구성이 사용됩니다.

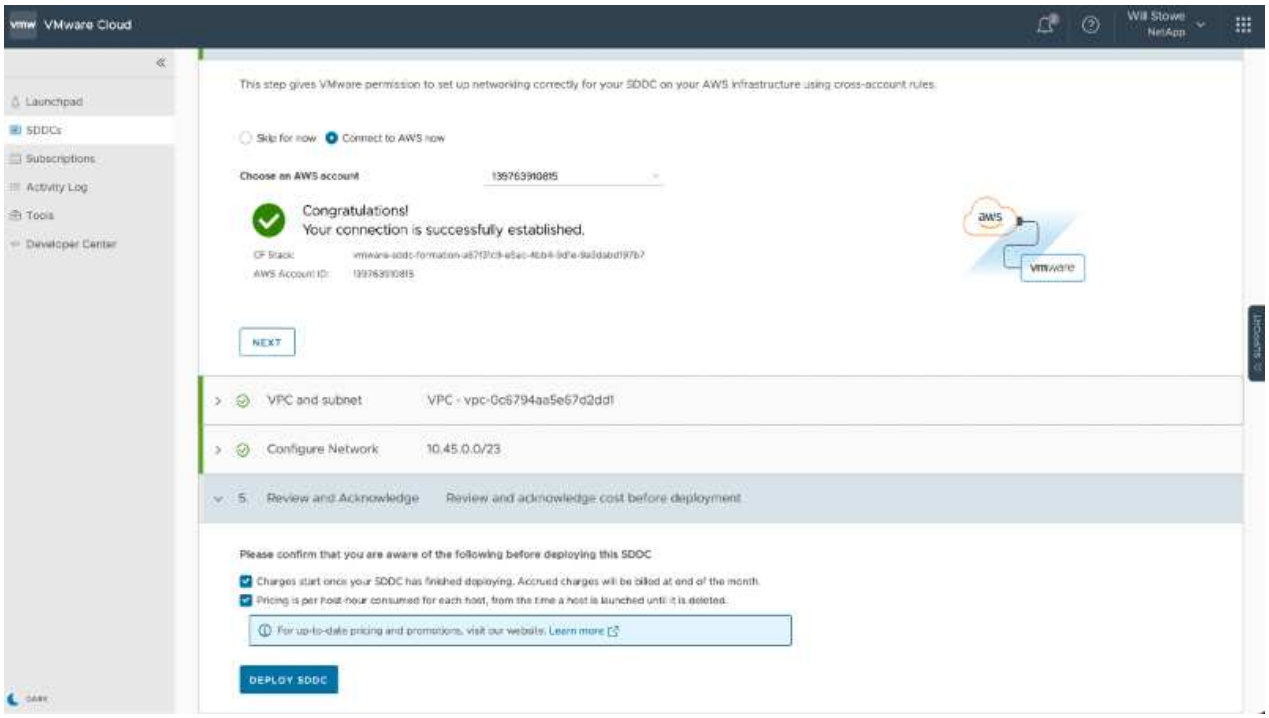
4. VMC 환경을 연결할 AWS VPC를 선택합니다.



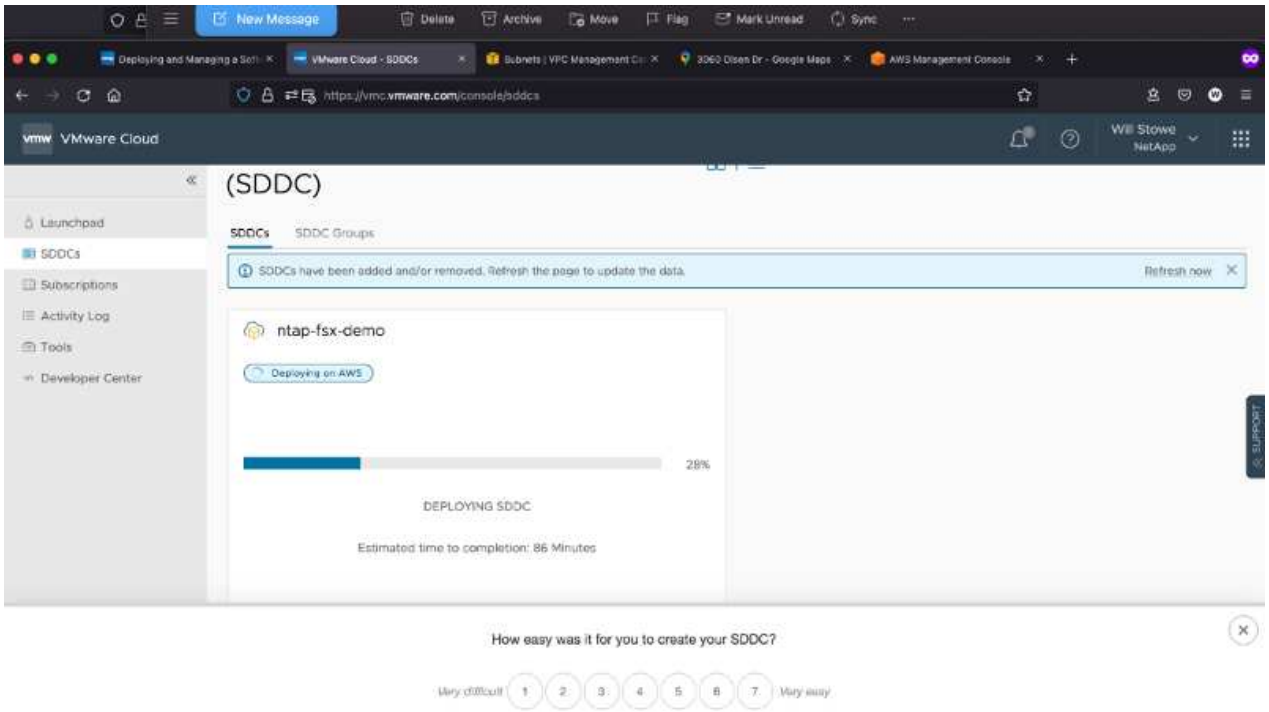
5. VMC 관리 서브넷을 구성합니다. 이 서브넷에는 vCenter, NSX 등과 같은 VMC 관리 서비스가 포함되어 있습니다. SDDC 환경에 연결해야 하는 다른 네트워크와 겹치는 주소 공간을 선택하지 마세요. 마지막으로, 아래에 표시된 CIDR 크기에 대한 권장 사항을 따르세요.



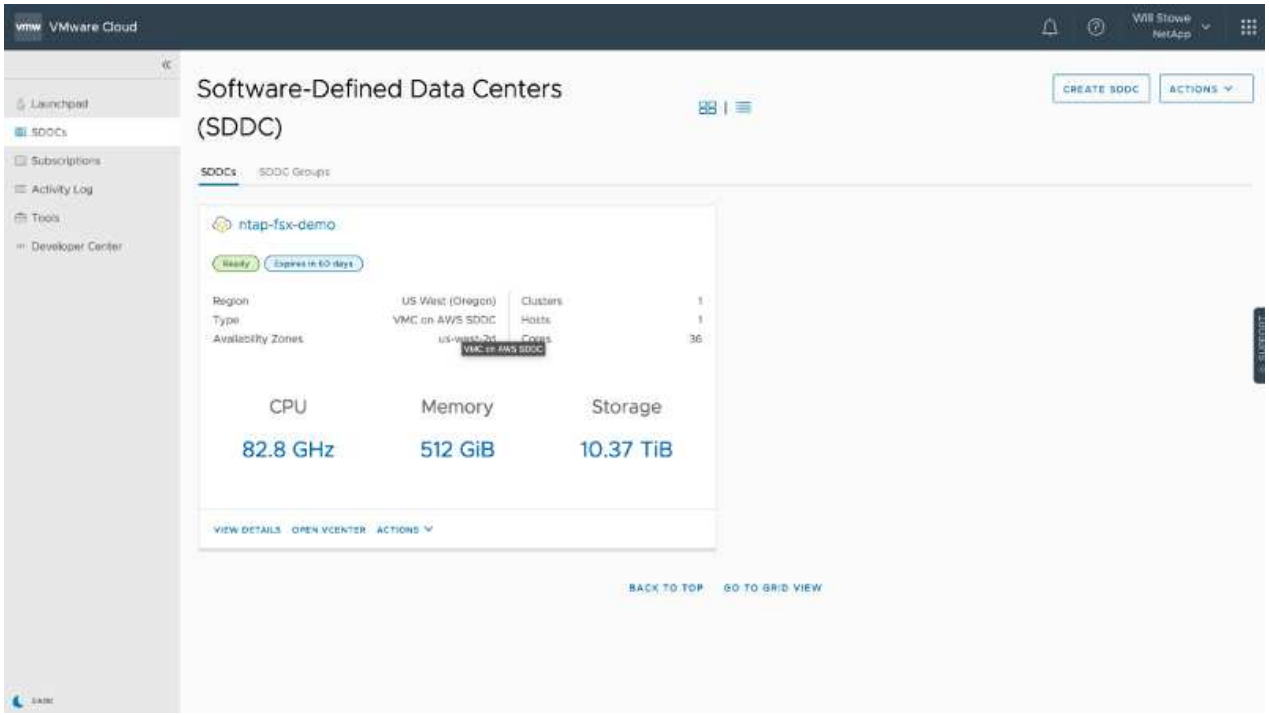
6. SDDC 구성을 검토하고 확인한 다음 SDDC 배포를 클릭합니다.



배포 프로세스는 일반적으로 완료하는 데 약 2시간이 걸립니다.



7. 완료되면 SDDC를 사용할 수 있습니다.

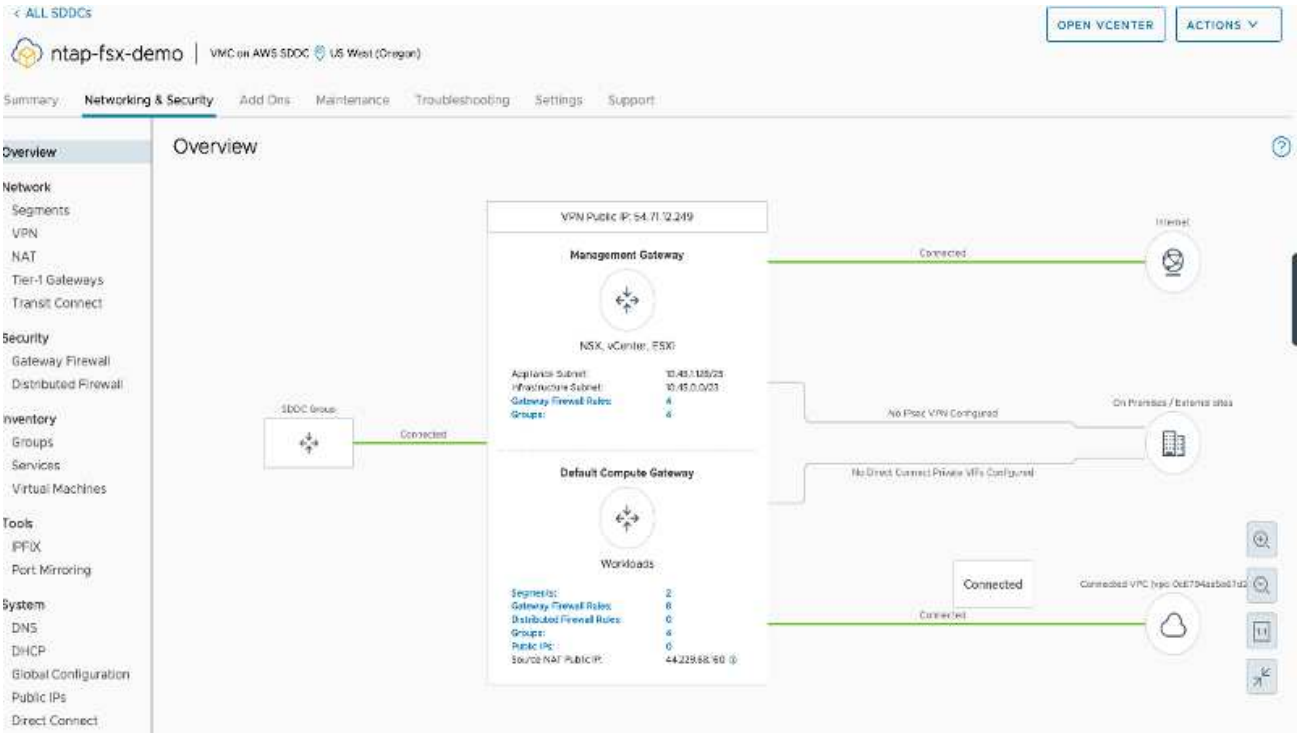


SDDC 배포에 대한 단계별 가이드는 다음을 참조하세요."VMC 콘솔에서 SDDC 배포" .

▼ **VMware Cloud**를 **FSx ONTAP** 에 연결

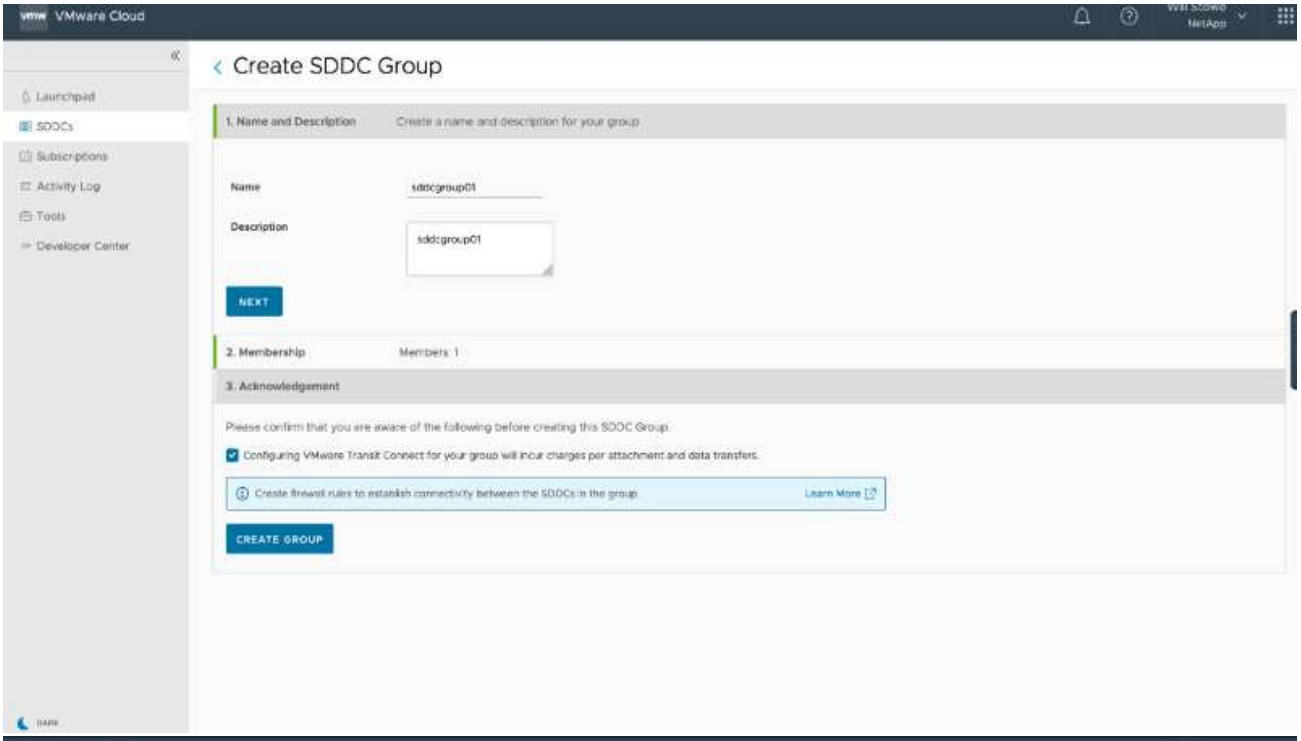
VMware Cloud를 FSx ONTAP 에 연결하려면 다음 단계를 완료하세요.

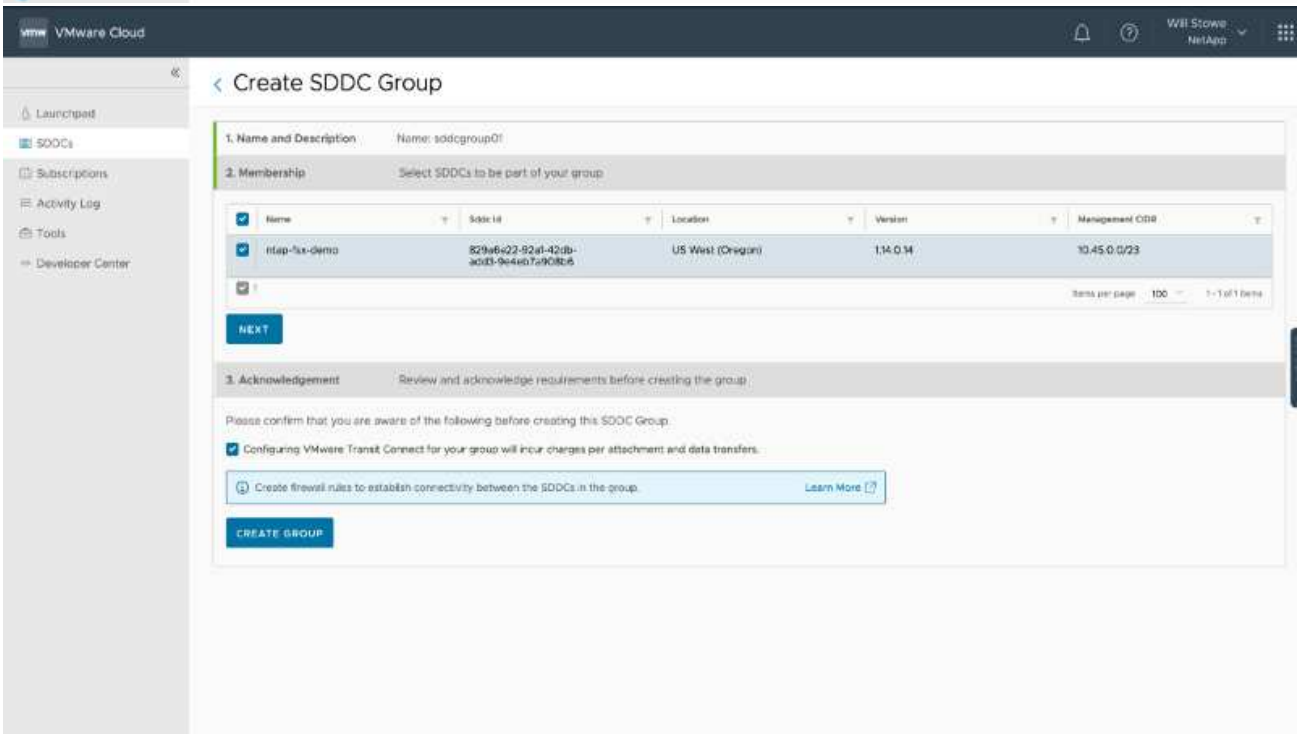
1. VMware Cloud 배포가 완료되고 AWS VPC에 연결되면 원래 연결된 VPC가 아닌 새 VPC에 Amazon FSx ONTAP 배포해야 합니다(아래 스크린샷 참조). FSx(NFS 및 SMB 유동 IP)는 연결된 VPC에 배포된 경우 액세스할 수 없습니다. Cloud Volumes ONTAP 과 같은 ISCSI 엔드포인트는 연결된 VPC에서도 정상적으로 작동한다는 점을 명심하세요.

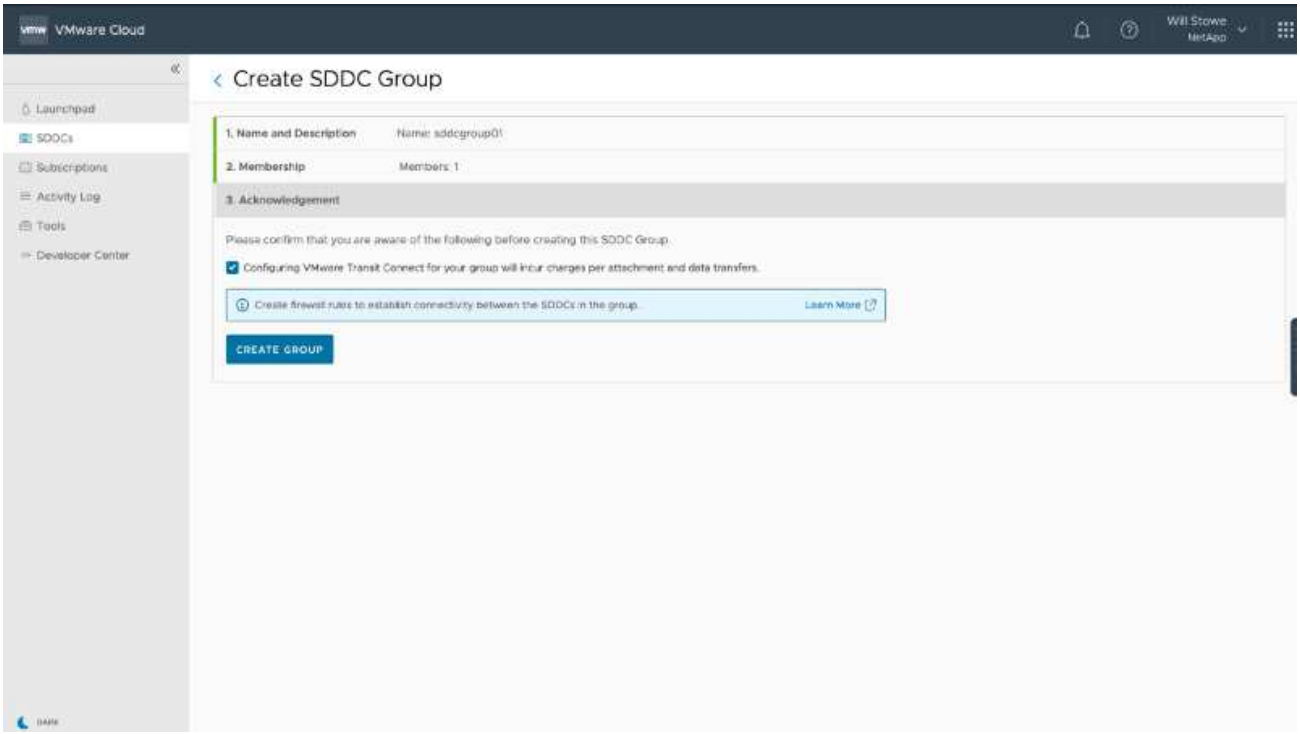


2. 동일한 지역에 추가 VPC를 배포한 다음, 새 VPC에 Amazon FSx ONTAP 배포합니다.

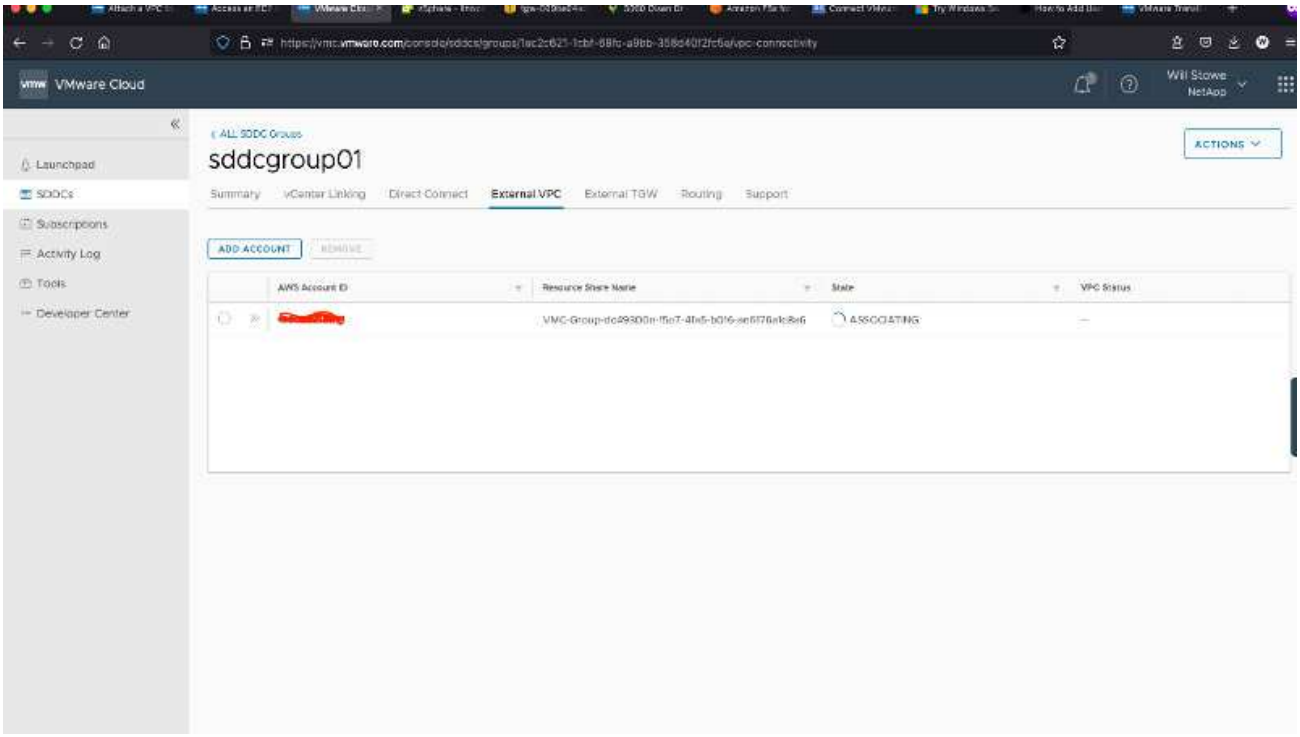
   VMware Cloud 콘솔에서 SDDC 그룹을 구성하면 FSx가 배포된 새 VPC에 연결하는 데 필요한 네트워킹 구성 옵션이 활성화됩니다. 3단계에서 "그룹에 VMware Transit Connect를 구성하면 첨부 파일 및 데이터 전송당 요금이 부과됩니다"가 선택되어 있는지 확인한 다음, 그룹 만들기를 선택합니다. 이 과정을 완료하는 데 몇 분이 걸릴 수 있습니다.

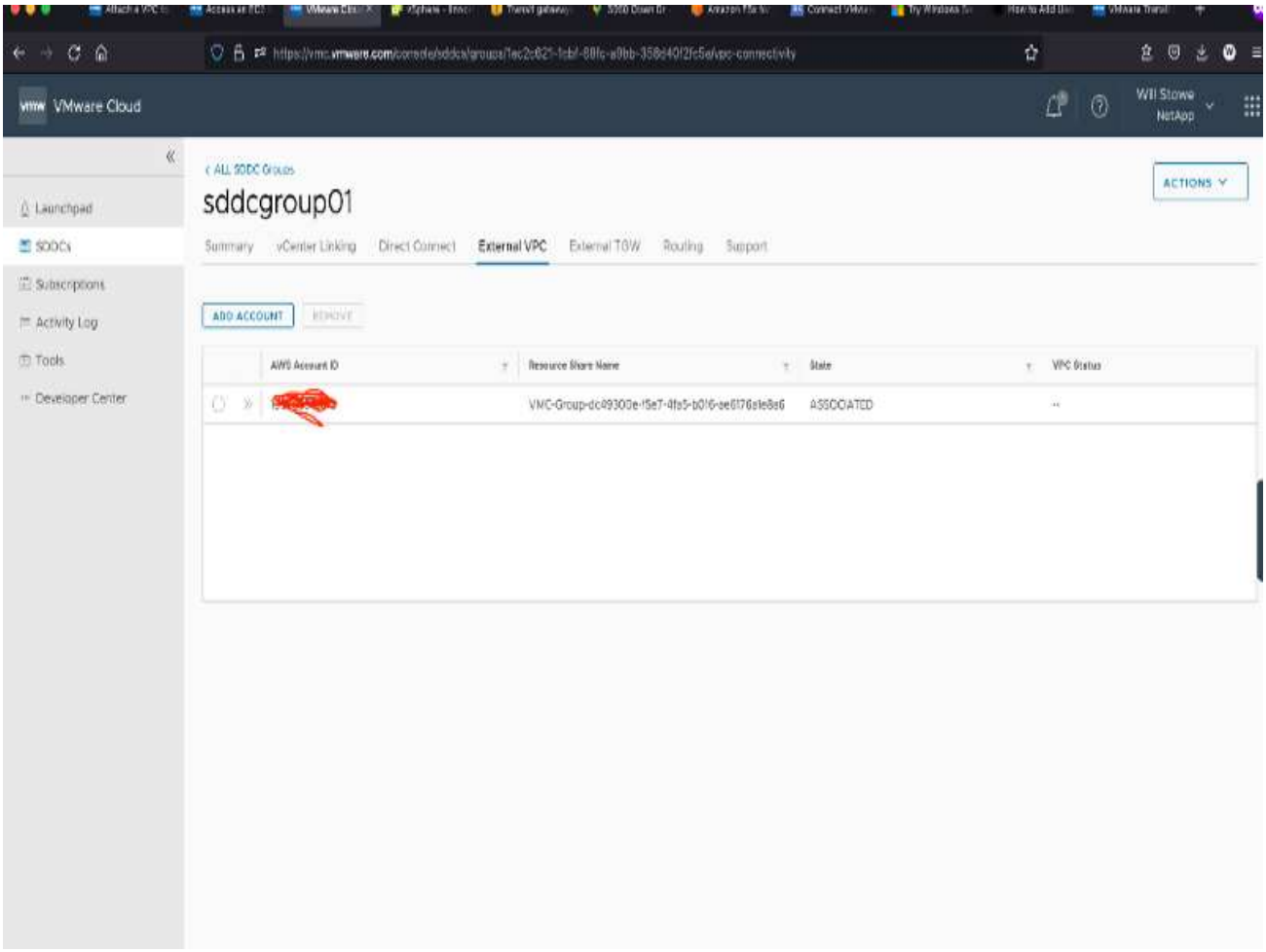




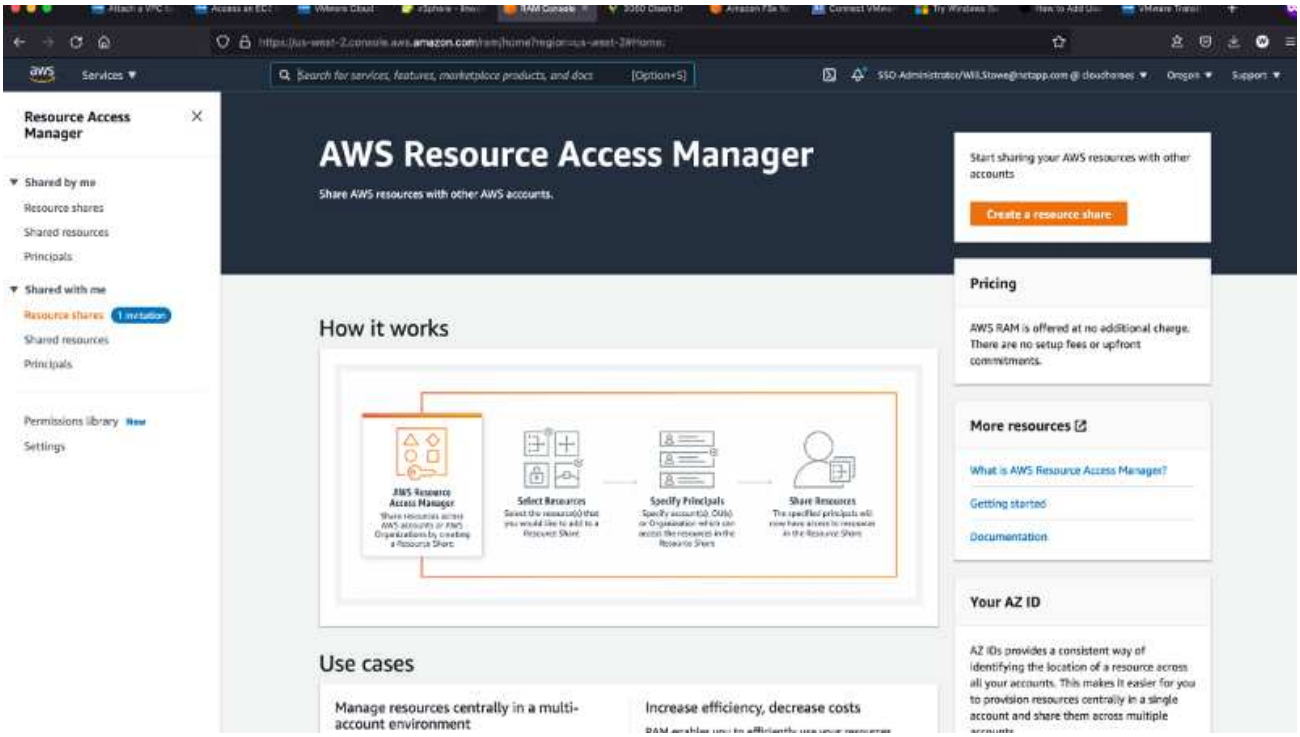


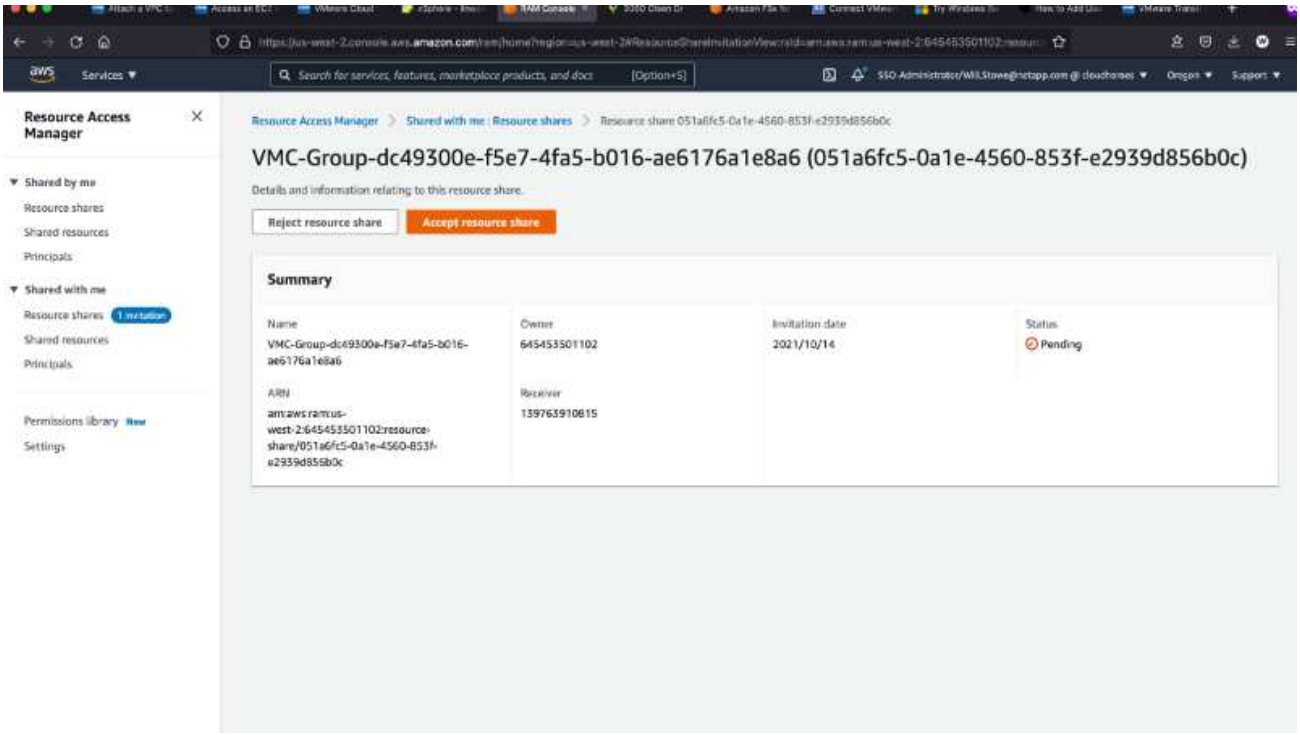
3. 새로 만든 VPC를 방금 만든 SDDC 그룹에 연결합니다. 외부 VPC 탭을 선택하고 다음을 따르세요."외부 VPC 연결 지침" 그룹에. 이 과정을 완료하는 데 10~15분이 걸릴 수 있습니다.



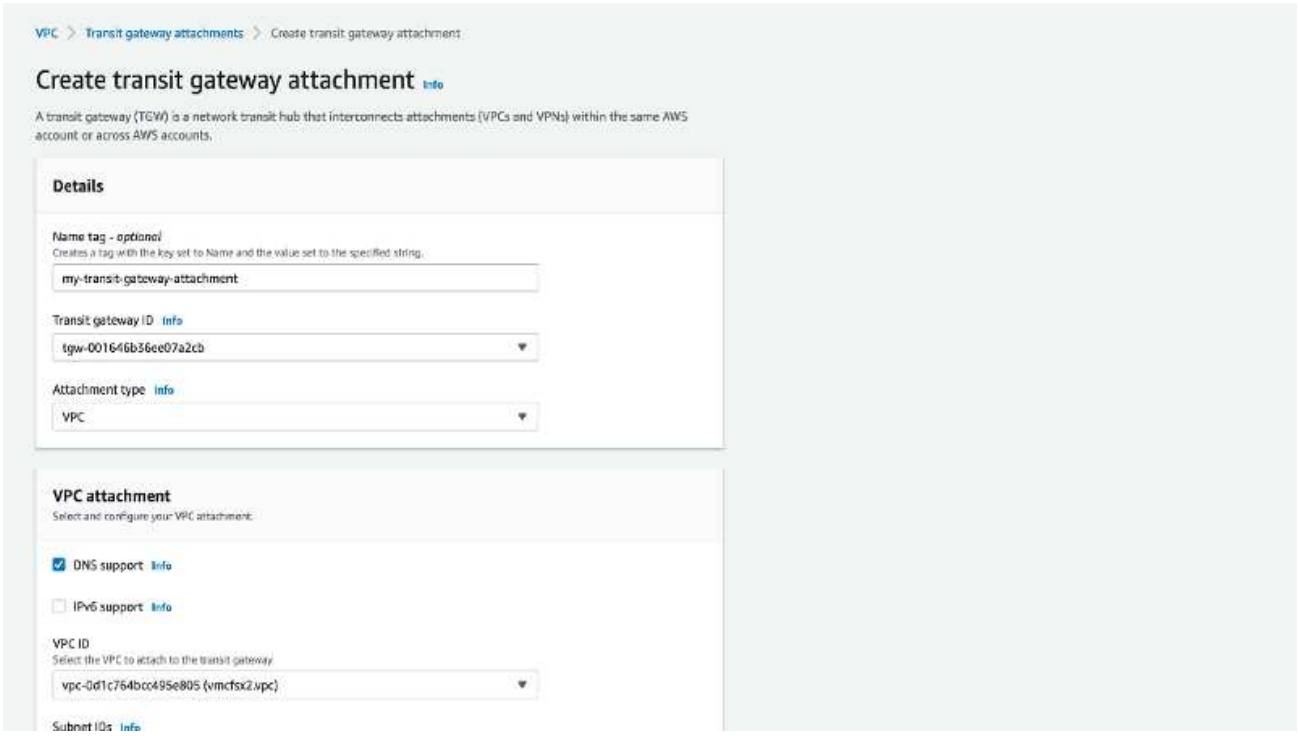


4. 외부 VPC 프로세스의 일부로 AWS 콘솔을 통해 Resource Access Manager를 통해 새로운 공유 리소스에 대한 메시지가 표시됩니다. 공유 리소스는"AWS 트랜짓 게이트웨이" VMware Transit Connect에서 관리합니다.

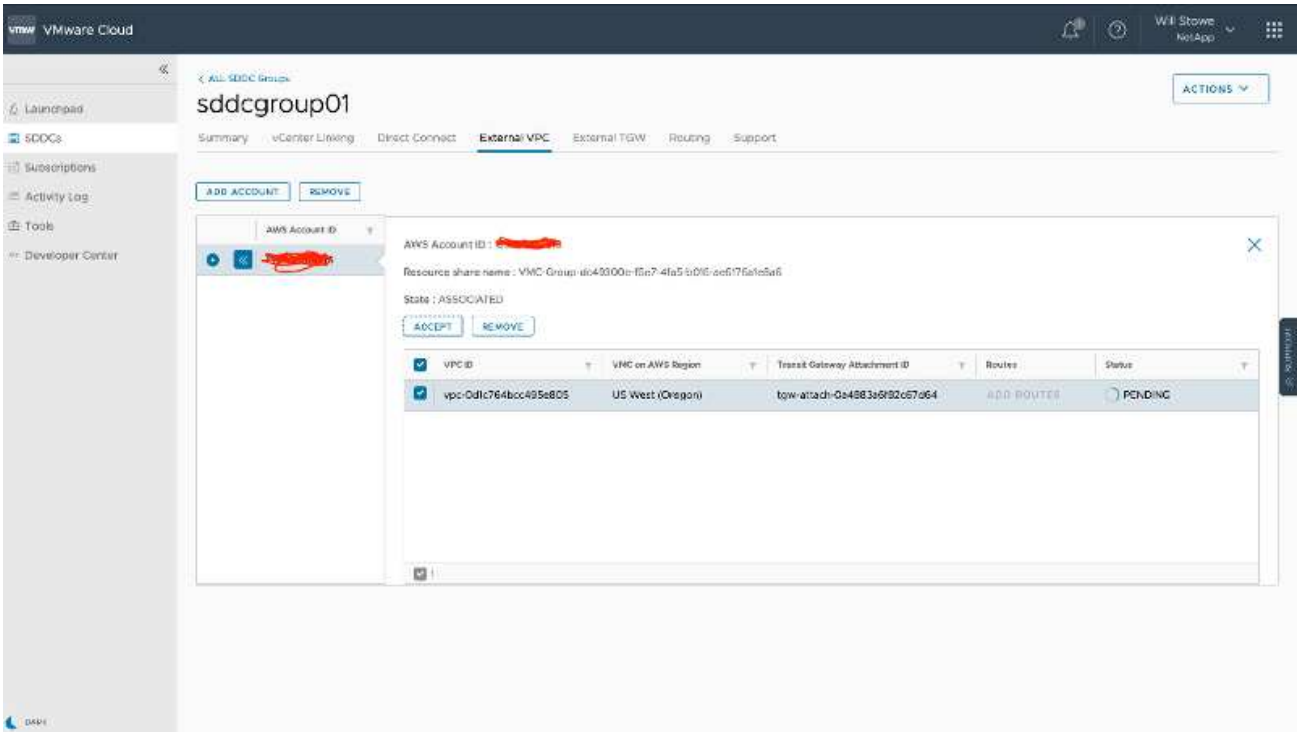




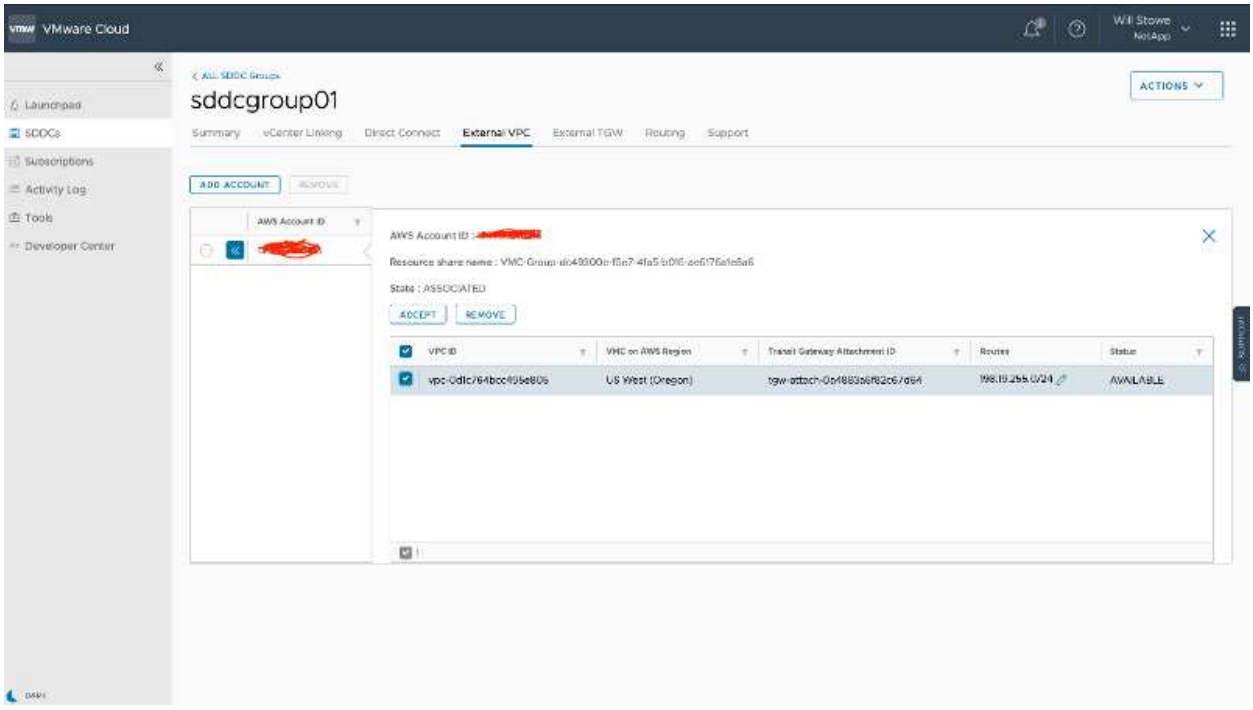
5. Transit Gateway 첨부 파일을 만듭니다.



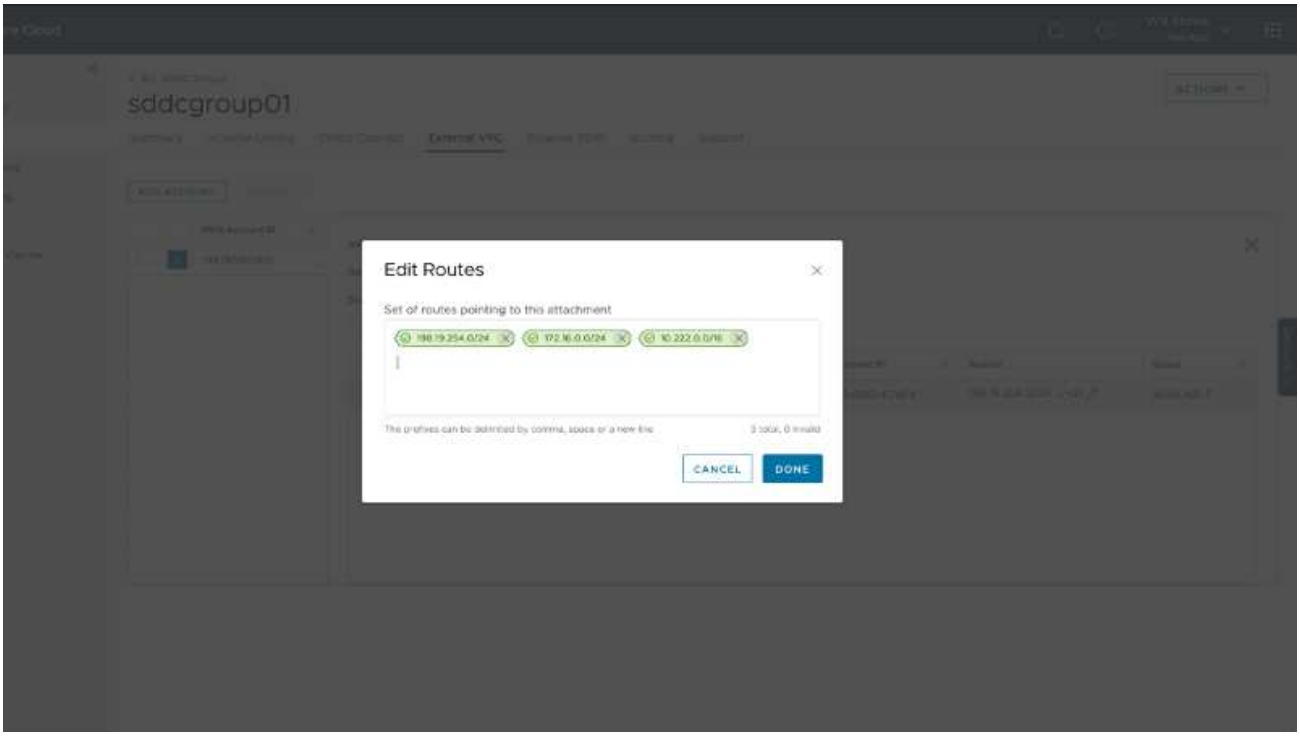
6. VMC 콘솔로 돌아와서 VPC 첨부 파일을 수락합니다. 이 과정을 완료하는 데 약 10분이 걸릴 수 있습니다.



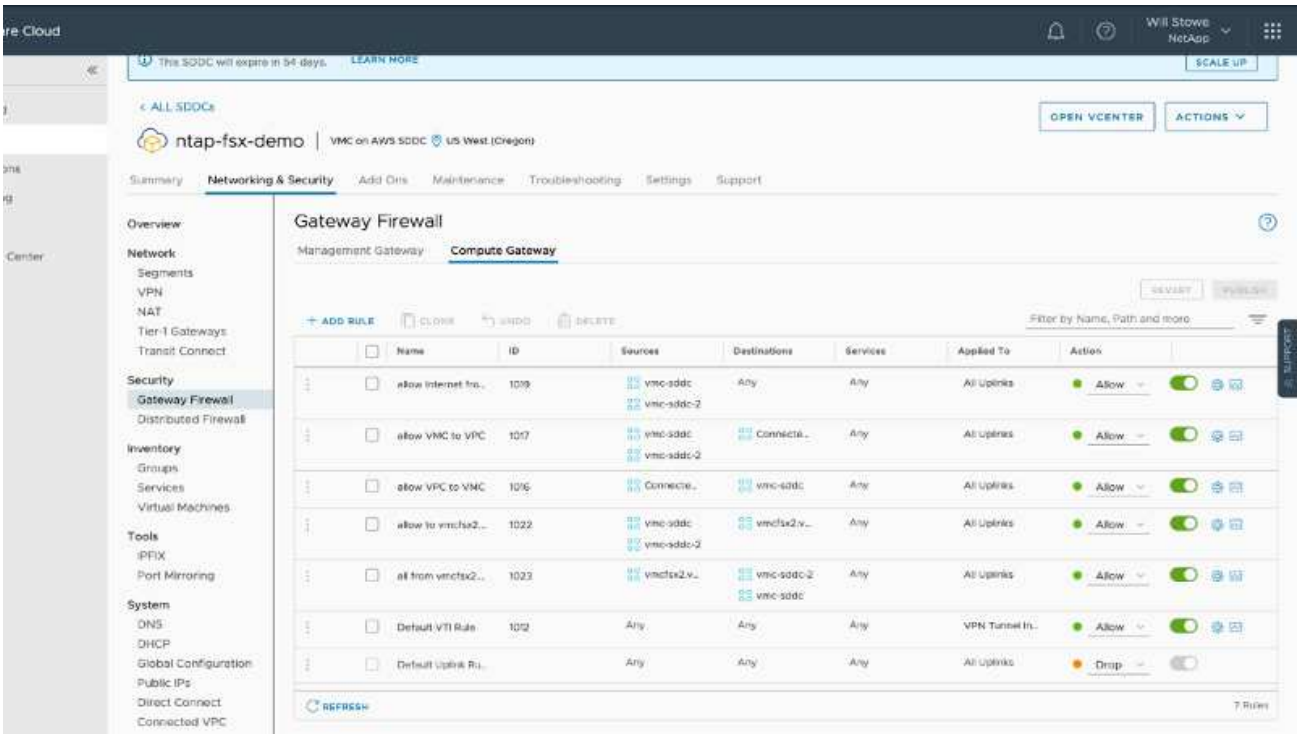
7. 외부 VPC 탭에서 경로 열의 편집 아이콘을 클릭하고 다음과 같은 필수 경로를 추가합니다.
   - Amazon FSx ONTAP 의 플로팅 IP 범위에 대한 경로"유동 IP" .
   - Cloud Volumes ONTAP 의 플로팅 IP 범위에 대한 경로(해당되는 경우).
   - 새로 생성된 외부 VPC 주소 공간에 대한 경로입니다.



8. 마지막으로 양방향 트래픽을 허용합니다."방화벽 규칙" FSx/CVO에 접속하려면 이것을 따르세요"자세한 단계" SDDC 워크로드 연결을 위한 컴퓨팅 게이트웨이 방화벽 규칙입니다.



9. 관리 게이트웨이와 컴퓨팅 게이트웨이 모두에 대한 방화벽 그룹이 구성된 후에는 다음과 같이 vCenter에 액세스할 수 있습니다.



다음 단계는 요구 사항에 따라 Amazon FSx ONTAP 또는 Cloud Volumes ONTAP 이 구성되었는지 확인하고, 배포를 최적화하기 위해 vSAN에서 스토리지 구성 요소를 오프로드하도록 볼륨이 프로비저닝되었는지 확인하는 것입니다.

온프레미스와 마찬가지로 VM을 만들고 마이그레이션하기 위한 성공적인 프로덕션 준비 환경을 조성하려면 Azure VMware 솔루션을 계획하는 것이 중요합니다.

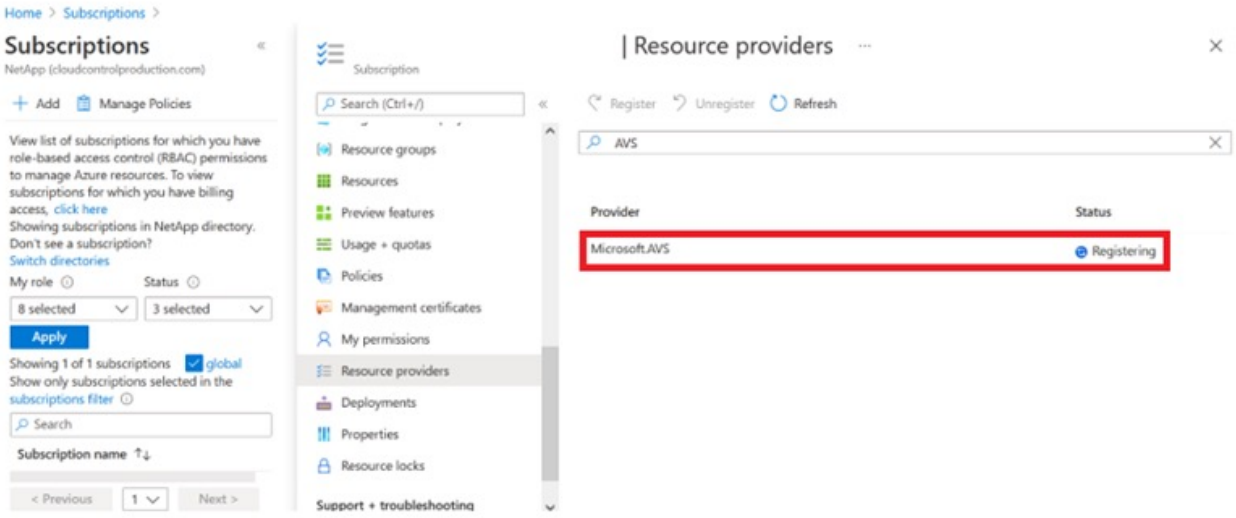
이 섹션에서는 Azure VMware Solution을 설정하고 관리하는 방법과 NetApp 스토리지를 연결하는 데 사용 가능한 옵션과 함께 사용하는 방법을 설명합니다.

설정 과정은 다음 단계로 나눌 수 있습니다.

▼ 리소스 공급자를 등록하고 프라이빗 클라우드를 생성하세요

Azure VMware Solution을 사용하려면 먼저 식별된 구독 내에서 리소스 공급자를 등록하세요.

1. Azure Portal에 Sign in .
2. Azure Portal 메뉴에서 모든 서비스를 선택합니다.
3. 모든 서비스 대화 상자에서 구독을 입력한 다음 구독을 선택합니다.
4. 보려면 구독 목록에서 구독을 선택하세요.
5. 리소스 공급자를 선택하고 검색에 Microsoft.AVS를 입력합니다.
6. 리소스 제공자가 등록되지 않은 경우 등록을 선택하세요.

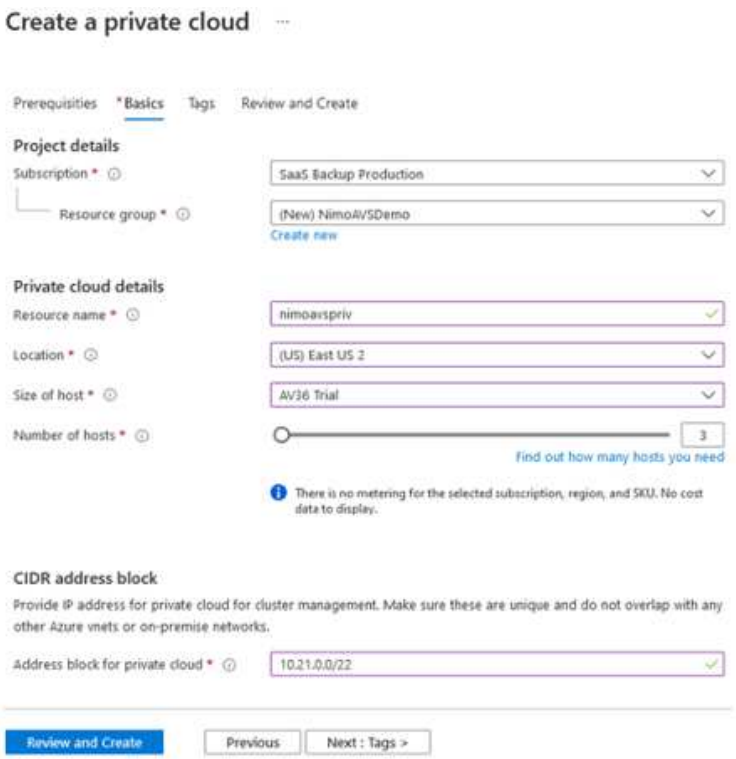




7. 리소스 공급자를 등록한 후 Azure Portal을 사용하여 Azure VMware Solution 프라이빗 클라우드를 만듭니다.
8. Azure Portal에 Sign in .
9. 새 리소스 만들기를 선택하세요.
10. 마켓플레이스 검색 텍스트 상자에 Azure VMware Solution을 입력하고 결과에서 선택합니다.
11. Azure VMware 솔루션 페이지에서 만들기를 선택합니다.
12. 기본 탭에서 필드에 값을 입력하고 검토 + 생성을 선택합니다.

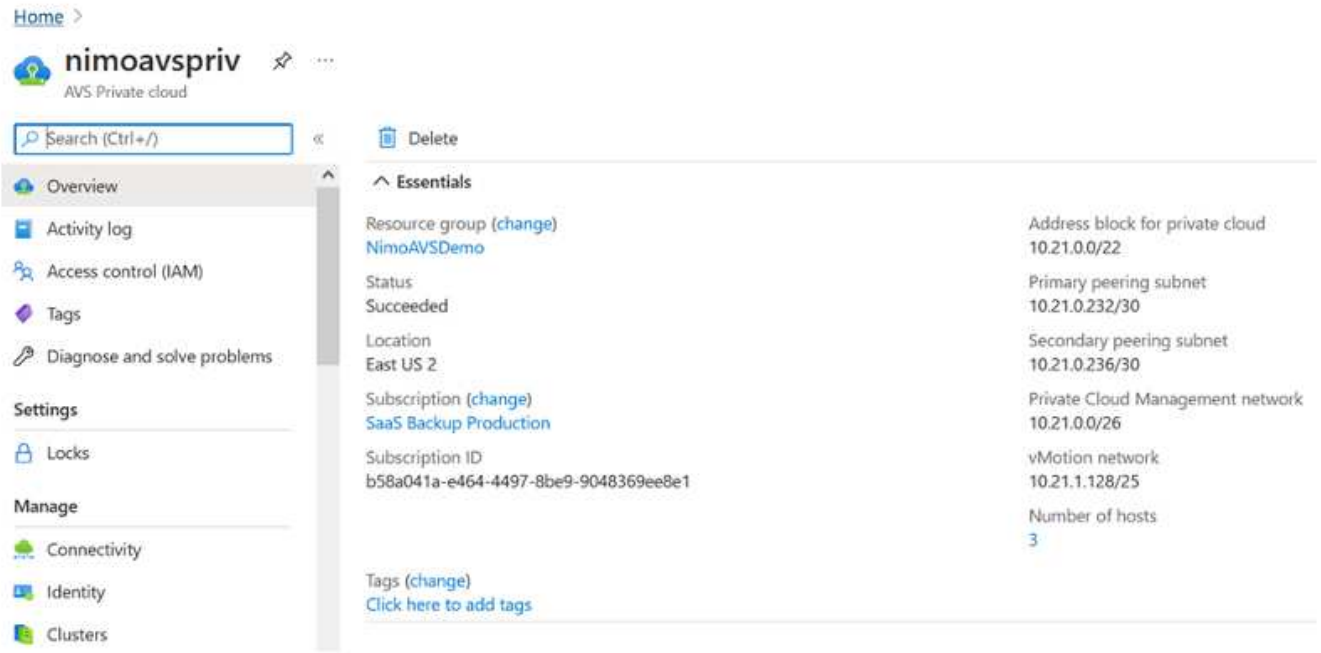
참고사항:

- 빠르게 시작하려면 계획 단계에서 필요한 정보를 수집하세요.
- 기존 리소스 그룹을 선택하거나 프라이빗 클라우드에 대한 새 리소스 그룹을 만듭니다. 리소스 그룹은 Azure 리소스가 배포되고 관리되는 논리적 컨테이너입니다.
- CIDR 주소가 고유하고 다른 Azure Virtual Network 또는 온프레미스 네트워크와 겹치지 않는지 확인하세요. CIDR은 프라이빗 클라우드 관리 네트워크를 나타내며 vCenter Server 및 NSX-T Manager와 같은 클러스터 관리 서비스에 사용됩니다. NetApp /22 주소 공간을 사용할 것을 권장합니다. 이 예에서는 10.21.0.0/22가 사용되었습니다.



프로비저닝 프로세스는 약 4~5시간이 소요됩니다. 프로세스가 완료되면 Azure Portal에서 프라이빗 클라우드에 액세스하여 배포가 성공했는지 확인하세요. 배포가 완료되면 '성공' 상태가 표시됩니다.

Azure VMware Solution 프라이빗 클라우드에는 Azure Virtual Network가 필요합니다. Azure VMware Solution은 온프레미스 vCenter를 지원하지 않으므로 기존 온프레미스 환경과 통합하려면 추가 단계가 필요합니다. ExpressRoute 회로와 가상 네트워크 게이트웨이를 설정하는 것도 필요합니다. 클러스터 프로비저닝이 완료될 때까지 기다리는 동안 새 가상 네트워크를 만들거나 기존 가상 네트워크를 사용하여 Azure VMware Solution에 연결합니다.



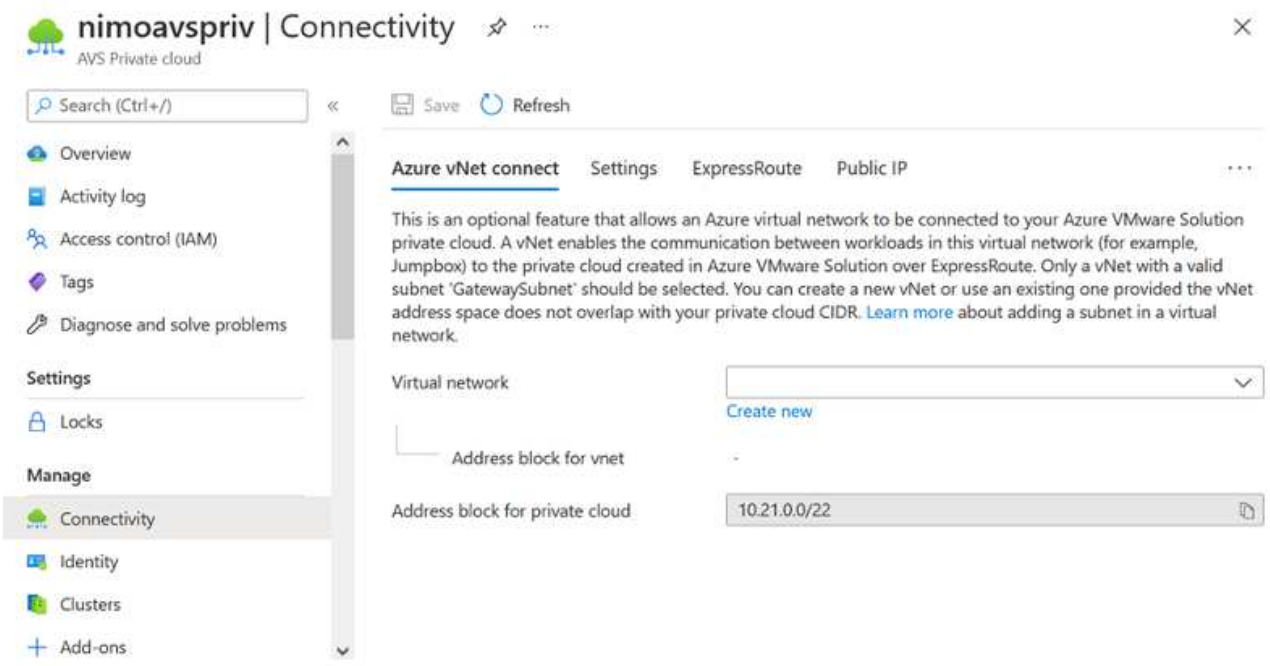
▼ 새 **ExpressRoute** 가상 네트워크 게이트웨이 또는 기존 **ExpressRoute** 가상 네트워크 게이트웨이에 연결

새로운 Azure Virtual Network(VNet)를 만들려면 Azure VNet 연결 탭을 선택하세요. 또는 Azure Portal에서 가상 네트워크 만들기 마법사를 사용하여 수동으로 만들 수 있습니다.

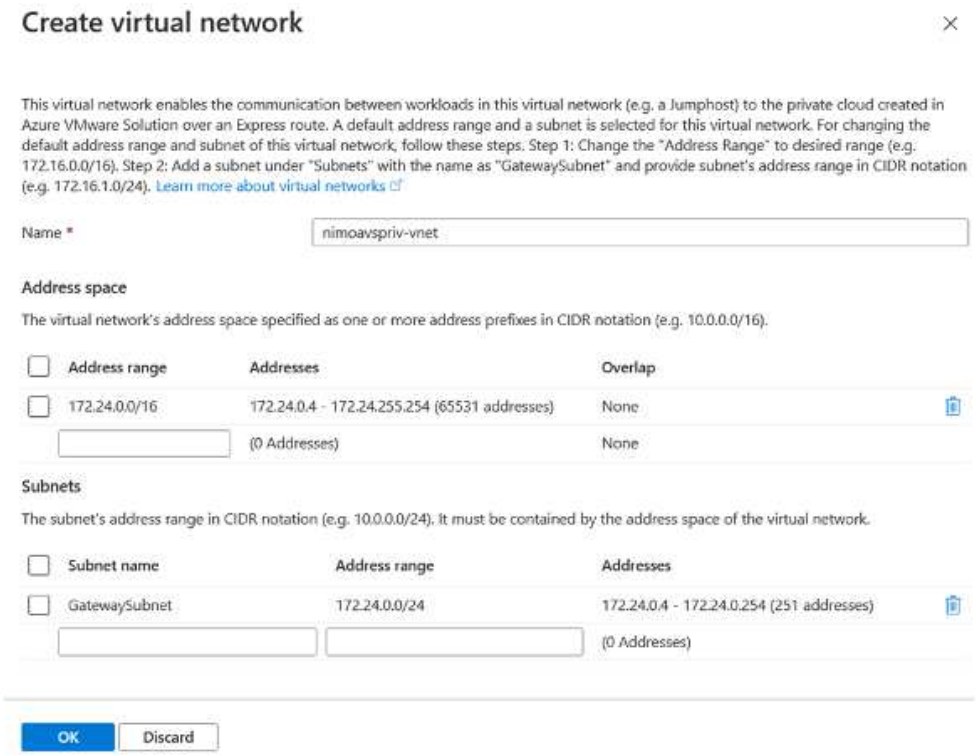
1. Azure VMware Solution 프라이빗 클라우드로 이동하여 관리 옵션에서 연결에 액세스합니다.
2. Azure VNet Connect를 선택하세요.
3. 새로운 VNet을 만들려면 새로 만들기 옵션을 선택하세요.

   이 기능을 사용하면 VNet을 Azure VMware Solution 프라이빗 클라우드에 연결할 수 있습니다. VNet은 ExpressRoute를 통해 Azure VMware Solution에서 생성된 프라이빗 클라우드에 필요한 구성 요소(예: 점프 박스, Azure NetApp Files, Cloud Volume ONTAP 등의 공유 서비스)를 자동으로 생성하여 이 가상 네트워크의 워크로드 간 통신을 가능하게 합니다.

   참고**:** VNet 주소 공간은 프라이빗 클라우드 CIDR과 겹치면 안 됩니다.



4. 새 VNet에 대한 정보를 제공하거나 업데이트하고 확인을 선택합니다.

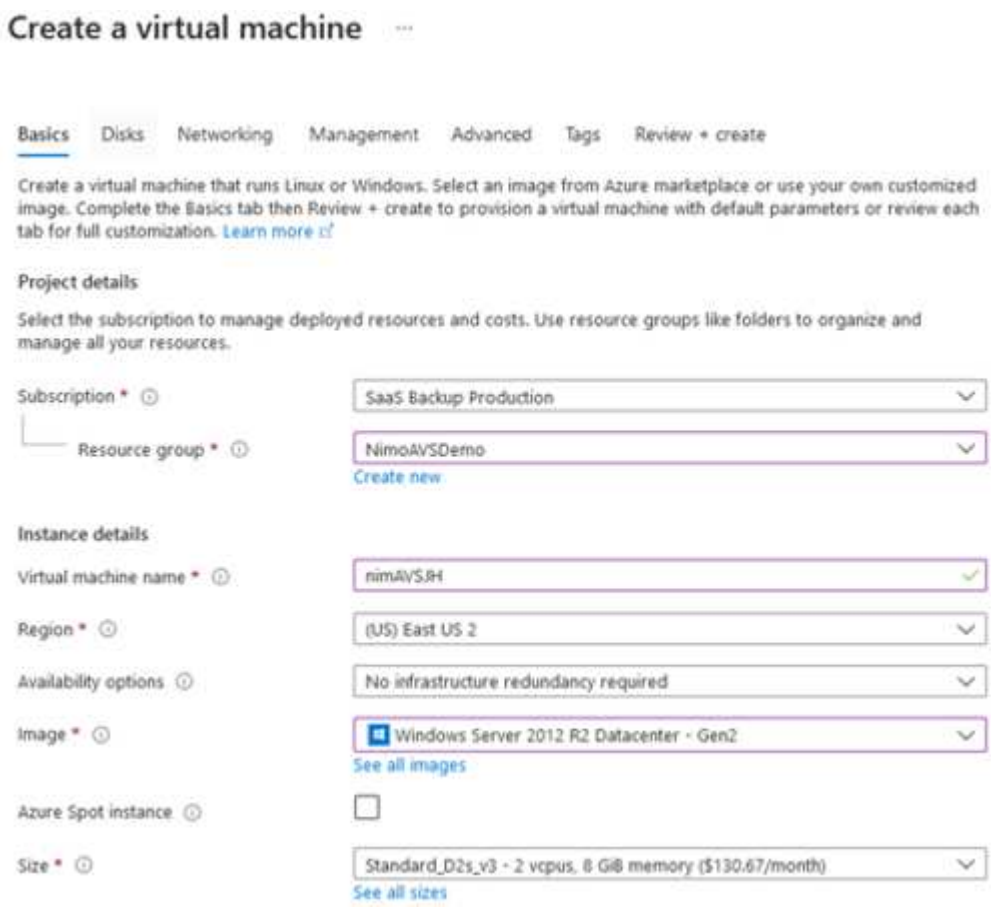


제공된 주소 범위와 게이트웨이 서브넷을 사용하는 VNet이 지정된 구독 및 리소스 그룹에 생성됩니다.

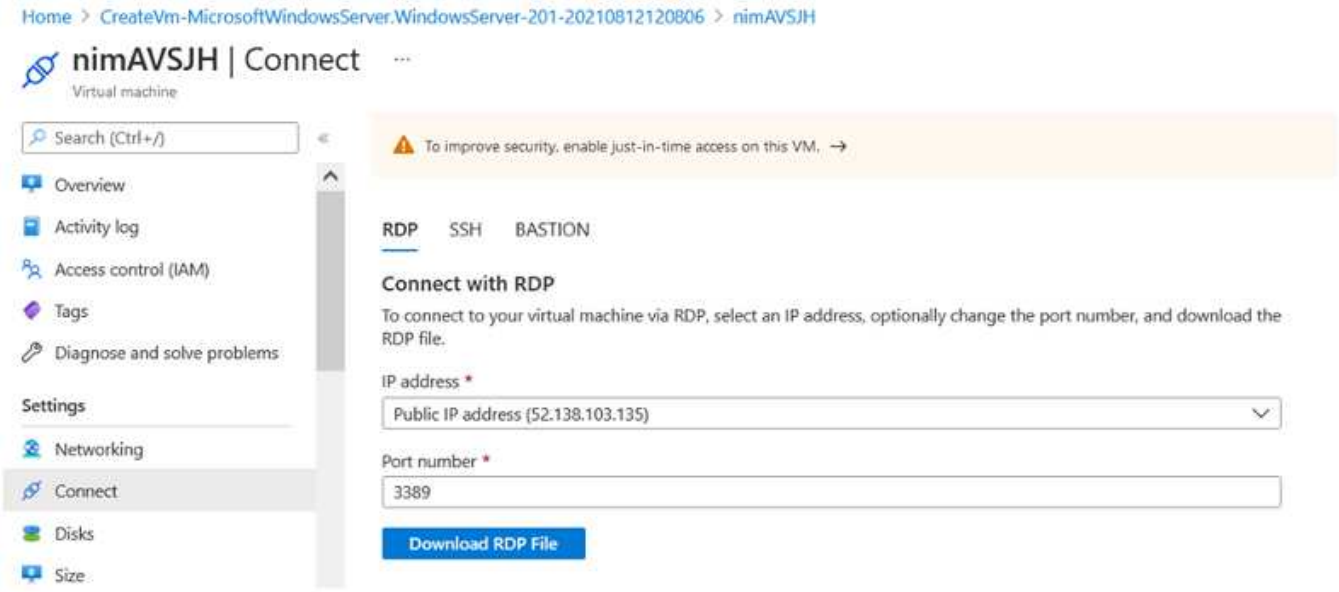
VNet을 수동으로 생성하는 경우 적절한 SKU와 게이트웨이 유형으로 ExpressRoute를 사용하여 가상 네트워크 게이트웨이를 생성합니다. 배포가 완료되면 인증 키를 사용하여 Azure VMware Solution 프라이빗 클라우드가 포함된 가상 네트워크 게이트웨이에 ExpressRoute 연결을 연결합니다. 자세한 내용은 다음을 참조하세요. "Azure에서 VMware 프라이빗 클라우드에 대한 네트워킹 구성" .

▼ **Azure VMware Solution** 프라이빗 클라우드에 대한 네트워크 연결 및 액세스를 검증합니다**.**

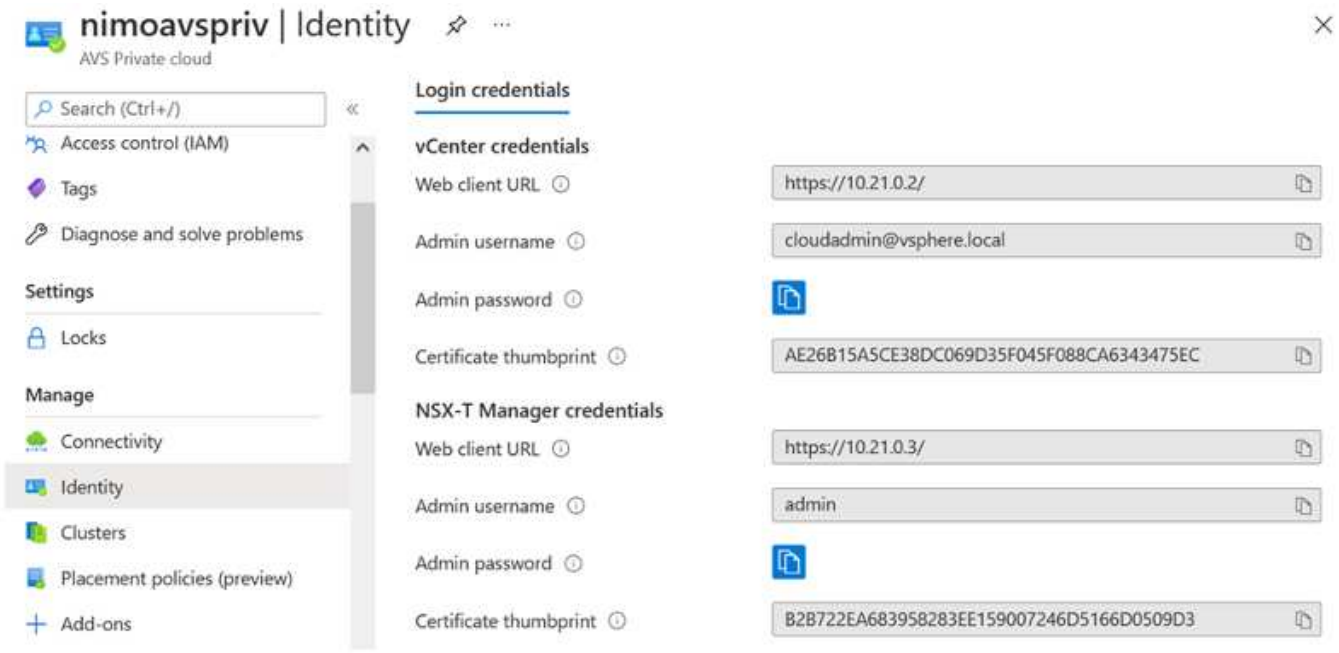
Azure VMware 솔루션을 사용하면 온프레미스 VMware vCenter를 사용하여 프라이빗 클라우드를 관리할 수 없습니다. 대신 Azure VMware Solution vCenter 인스턴스에 연결하려면 점프 호스트가 필요합니다. 지정된 리소스 그룹에서 점프 호스트를 만들고 Azure VMware Solution vCenter에 로그인합니다. 이 점프 호스트는 연결을 위해 생성된 동일한 가상 네트워크에 있는 Windows VM이어야 하며 vCenter와 NSX Manager에 대한 액세스를 제공해야 합니다.



가상 머신이 프로비저닝된 후 연결 옵션을 사용하여 RDP에 액세스합니다.



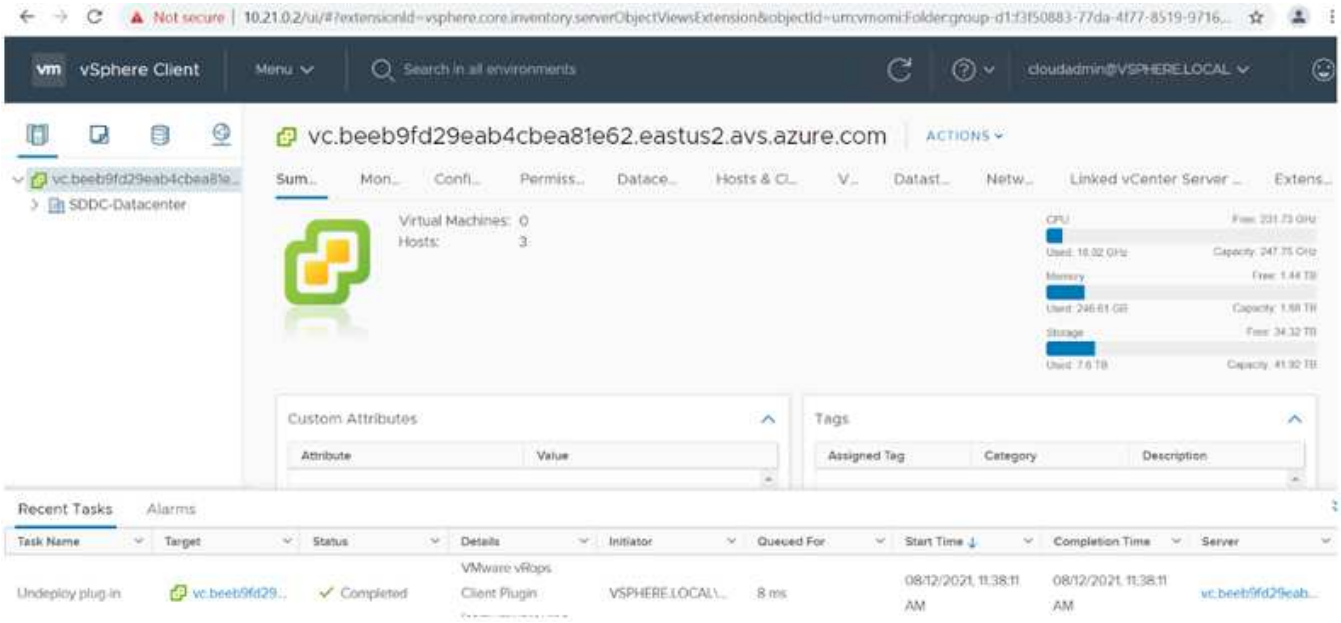
클라우드 관리자 사용자를 사용하여 새로 생성된 점프 호스트 가상 머신에서 vCenter에 Sign in . 자격 증명에 액세스하려면 Azure Portal로 이동하여 ID(프라이빗 클라우드의 관리 옵션 아래)로 이동합니다. 프라이빗 클라우드 vCenter 및 NSX-T Manager의 URL과 사용자 자격 증명을 여기에서 복사할 수 있습니다.



Windows 가상 머신에서 브라우저를 열고 vCenter 웹 클라이언트 URL로 이동합니다.("`https://10.21.0.2/`") 관리자 사용자 이름을 *cloudadmin@vsphere.local*로 사용하고 복사한 비밀번호를 붙여넣습니다. 마찬가지로 NSX-T 관리자는 웹 클라이언트 URL을 사용하여 액세스할 수도 있습니다.("`https://10.21.0.3/`") 관리자 사용자 이름을 사용하고 복사한 비밀번호를 붙여넣어 새로운 세그먼트를 만들거나 기존 계층 게이트웨이를 수정합니다.

웹 클라이언트 URL은 프로비저닝된 각 SDDC마다 다릅니다.





Azure VMware Solution SDDC가 배포되고 구성되었습니다. ExpressRoute Global Reach를 활용하여 온프레미스 환경을 Azure VMware Solution 프라이빗 클라우드에 연결합니다. 자세한 내용은 다음을 참조하세요. "온프레미스 환경을 Azure VMware 솔루션에 피어링" .

Google Cloud Platform(GCP)에서 가상화 환경 배포 및 구성

온프레미스와 마찬가지로, VM을 만들고 마이그레이션하기 위한 성공적인 프로덕션 준비 환경을 조성하려면 Google Cloud VMware Engine(GCVE)을 계획하는 것이 중요합니다.

이 섹션에서는 GCVE를 설정하고 관리하는 방법과 NetApp 스토리지 연결에 사용 가능한 옵션과 함께 사용하는 방법을 설명합니다.

설정 과정은 다음 단계로 나눌 수 있습니다.

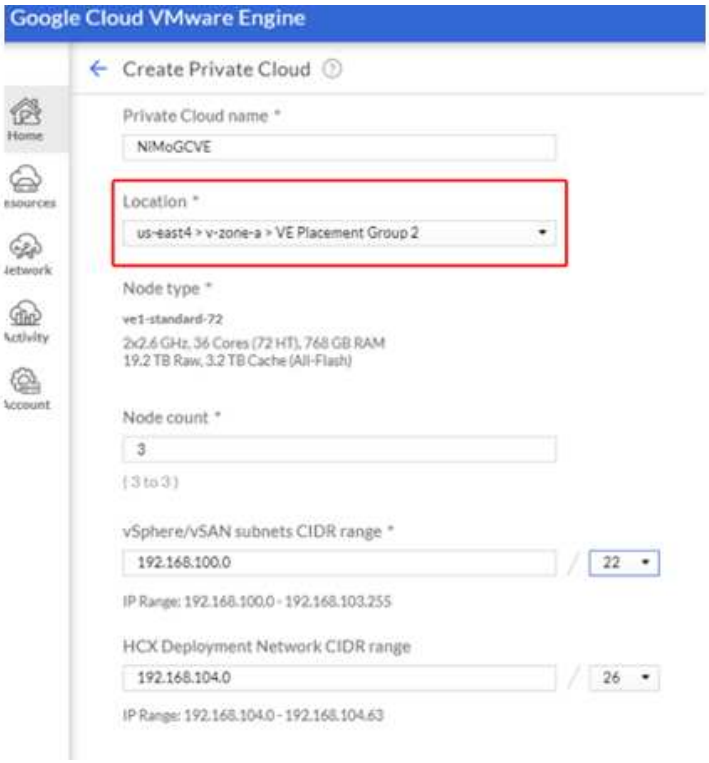
▼ **GCVE** 배포 및 구성

GCP에서 GCVE 환경을 구성하려면 GCP 콘솔에 로그인하고 VMware Engine 포털에 액세스합니다.

"새로운 프라이빗 클라우드" 버튼을 클릭하고 GCVE 프라이빗 클라우드에 대한 원하는 구성을 입력하세요. 최상의 성능과 가장 낮은 지연 시간을 보장하려면 "위치"에서 NetApp Volumes/CVO가 배포된 동일한 지역/영역에 프라이빗 클라우드를 배포해야 합니다.

필수 조건:

- VMware Engine 서비스 관리자 IAM 역할 설정
- "VMWare Engine API 액세스 및 노드 할당량 활성화"
- CIDR 범위가 온프레미스 또는 클라우드 서브넷과 겹치지 않는지 확인하세요. CIDR 범위는 /27 이상이어야 합니다.



참고: 프라이빗 클라우드 생성에는 30분에서 2시간이 걸릴 수 있습니다.

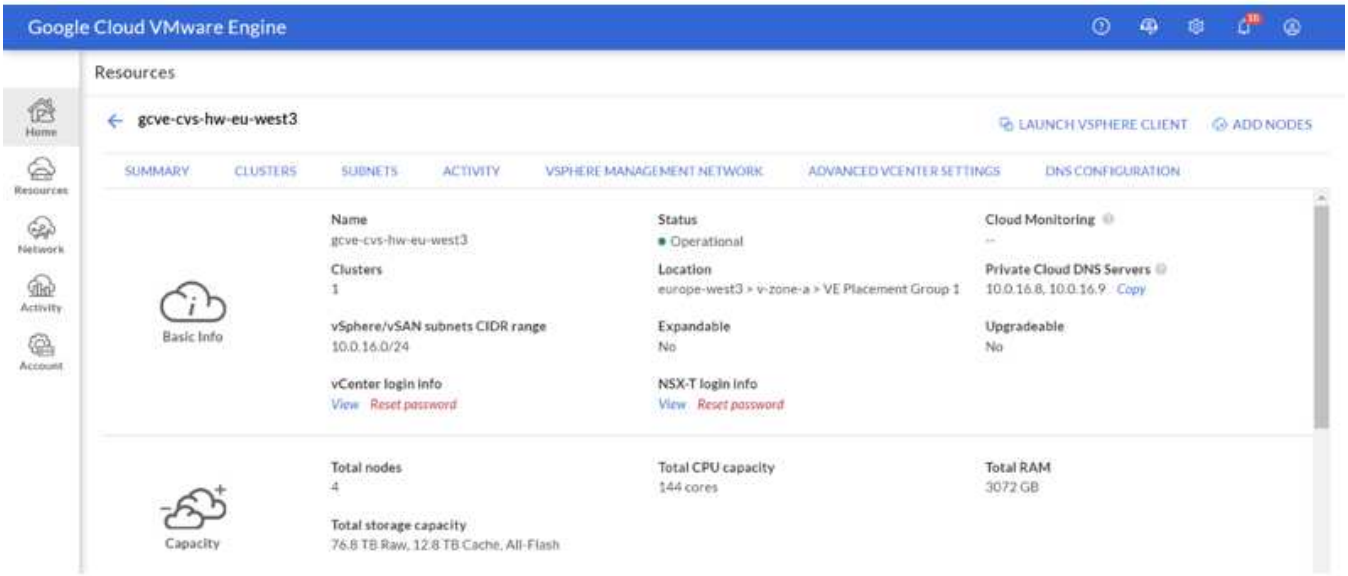
▼ **GCVE**에 대한 개인 액세스 활성화

프라이빗 클라우드가 프로비저닝되면 높은 처리량과 낮은 지연 시간의 데이터 경로 연결을 위해 프라이빗 클라우드에 대한 개인 액세스를 구성합니다.

이렇게 하면 Cloud Volumes ONTAP 인스턴스가 실행되는 VPC 네트워크가 GCVE 프라이빗 클라우드와 통신할 수 있게 됩니다. 이를 위해 다음 "GCP 문서"을 따르십시오. Cloud Volume Service의 경우, 테넌트 호스트 프로젝트 간에 일회성 피어링을 수행하여 VMware Engine과 Google Cloud NetApp Volumes 간의 연결을 설정하십시오. 자세한 단계는 이 "링크"를 따르십시오.

Tenant P	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Sta...	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	Active	Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	Active	Connected

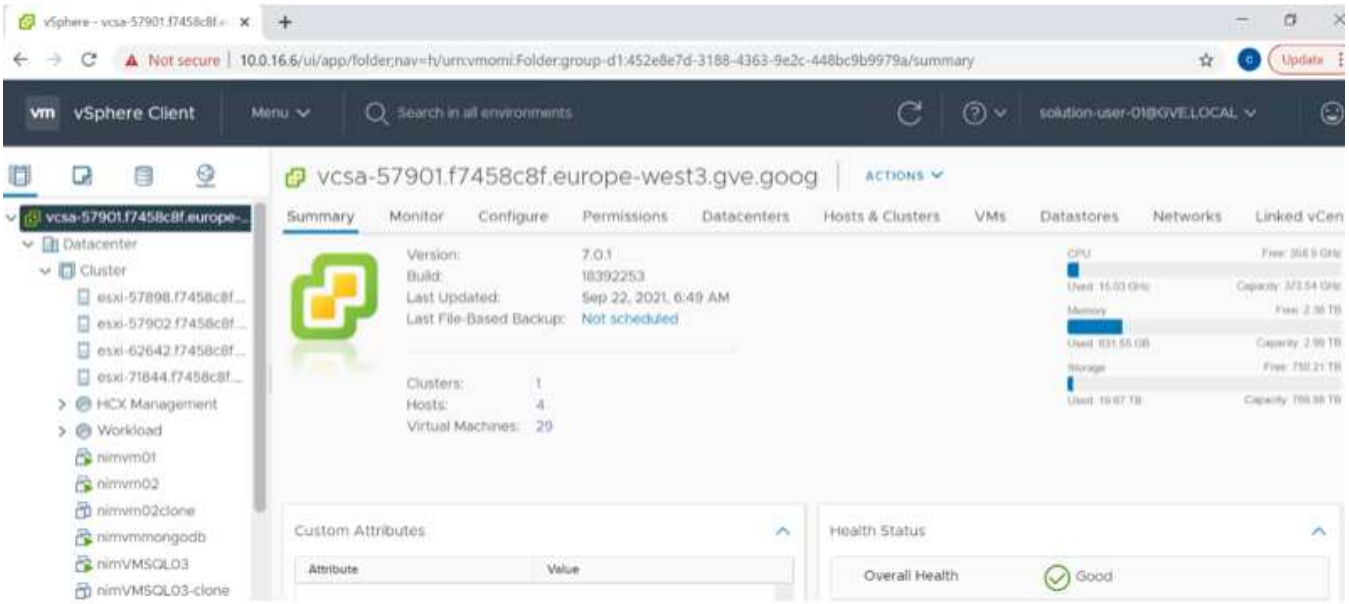
CloudOwner@gve.local 사용자를 사용하여 vCenter에 Sign in . 자격 증명에 액세스하려면 VMware Engine 포털로 이동하고, 리소스로 이동한 다음 적절한 프라이빗 클라우드를 선택하세요. 기본 정보 섹션에서 vCenter 로그인 정보(vCenter Server, HCX Manager) 또는 NSX-T 로그인 정보(NSX Manager)에 대한 보기 링크를 클릭합니다.



Windows 가상 머신에서 브라우저를 열고 vCenter 웹 클라이언트 URL로 이동합니다.("`https://10.0.16.6/`") 관리자 사용자 이름을 CloudOwner@gve.local로 사용하고 복사한 비밀번호를 붙여넣습니다. 마찬가지로 NSX-T 관리자는 웹 클라이언트 URL을 사용하여 액세스할 수도 있습니다.("`https://10.0.16.11/`") 관리자 사용자 이름을 사용하고 복사한 비밀번호를 붙여넣어 새로운 세그먼트를 만들거나 기존 계층 게이트웨이를 수정합니다.

온프레미스 네트워크에서 VMware Engine 프라이빗 클라우드에 연결하려면 적절한 연결을 위해 클라우드 VPN이나 Cloud Interconnect를 활용하고 필요한 포트가 열려 있는지 확인하세요. 자세한 단계는 다음을 따르세요."링크" .





▼ **GCVE**에 **Google Cloud NetApp Volumes** 보충 데이터 저장소 배포

나타내다"NetApp Volumes를 사용하여 GCVE에 보충 NFS 데이터 저장소를 배포하는 절차"

퍼블릭 클라우드의 **NetApp** 스토리지

퍼블릭 클라우드 공급업체를 위한 **NetApp** 스토리지 옵션

3대 하이퍼스케일러에서 NetApp 의 스토리지 옵션을 살펴보세요.

AWS / VMC

AWS는 다음 구성에서 NetApp 스토리지를 지원합니다.

- 게스트 연결 스토리지로서의 FSx ONTAP
- 게스트 연결 스토리지로서의 Cloud Volumes ONTAP (CVO)
- 보충 NFS 데이터 저장소로서의 FSx ONTAP

자세한 내용을 보려면"VMC용 게스트 연결 스토리지 옵션" . 자세한 내용을 보려면"VMC에 대한 보충 NFS 데이터 저장소 옵션" .

Azure / AVS

Azure는 다음 구성에서 NetApp 스토리지를 지원합니다.

- 게스트 연결 스토리지로서의 Azure NetApp Files (ANF)
- 게스트 연결 스토리지로서의 Cloud Volumes ONTAP (CVO)
- 보조 NFS 데이터 저장소로서의 Azure NetApp Files (ANF)

자세한 내용을 보려면"AVS용 게스트 연결 스토리지 옵션" . 자세한 내용을 보려면"AVS를 위한 보충 NFS 데이터 저장소 옵션" .

GCP/GCVE

Google Cloud는 다음 구성에서 NetApp 스토리지를 지원합니다.

- 게스트 연결 스토리지로서의 Cloud Volumes ONTAP (CVO)
- 게스트 연결 스토리지로서의 Google Cloud NetApp Volumes (NetApp Volumes)
- Google Cloud NetApp Volumes (NetApp Volumes)를 보조 NFS 데이터 저장소로 사용

자세한 내용을 보려면"GCVE를 위한 게스트 연결 스토리지 옵션" . 자세한 내용을 보려면"GCVE에 대한 보충 NFS 데이터 저장소 옵션" .

더 자세히 알아보세요"Google Cloud NetApp Volumes 데이터 저장소 지원(NetApp 블로그)" 또는"Google Cloud NetApp Volumes Google Cloud VMware Engine의 데이터 저장소로 사용하는 방법(Google 블로그)"

Amazon Web Services: NetApp 스토리지 사용 옵션

NetApp 스토리지는 게스트 연결 또는 보조 스토리지로 Amazon Web Services에 연결될 수 있습니다.

보충 **NFS** 데이터 저장소로서 **Amazon FSx for NetApp ONTAP (FSx ONTAP)**

Amazon FSx ONTAP 데이터 요구 사항을 애플리케이션 계층에 원활하게 전달하여 TCO를 줄이는 동시에 파일 서비스와 함께 애플리케이션 워크로드를 배포하고 관리할 수 있는 탁월한 옵션을 제공합니다. 어떤 사용 사례든 Amazon FSx ONTAP 과 함께 VMware Cloud on AWS를 선택하면 클라우드의 이점을 빠르게 실현하고, 온프레미스에서 AWS로 일관된 인프라와 운영을 구현하고, 워크로드를 양방향으로 이식하고, 엔터프라이즈급 용량과 성능을 확보할 수 있습니다. 이는 저장소를 연결하는 데 사용되는 익숙한 프로세스 및 절차와 동일합니다.

자세한 내용은 다음 웹사이트를 방문하세요.

- "보충 NFS 데이터 저장소로서의 FSx ONTAP : 개요"
- "보충 데이터 저장소로서 ONTAP 용 Amazon FSx"

게스트 연결 스토리지로서 **Amazon FSx for NetApp ONTAP**

Amazon FSx ONTAP NetApp의 인기 있는 ONTAP 파일 시스템을 기반으로 높은 안정성, 확장성, 고성능, 다양한 기능을 갖춘 파일 스토리지를 제공하는 완전 관리형 서비스입니다. FSx ONTAP NetApp 파일 시스템의 친숙한 기능, 성능, 기능 및 API 운영과 완벽하게 관리되는 AWS 서비스의 민첩성, 확장성 및 단순성을 결합합니다.

FSx ONTAP AWS나 온프레미스에서 실행되는 Linux, Windows, macOS 컴퓨팅 인스턴스에서 광범위하게 액세스할 수 있는 기능이 풍부하고 빠르며 유연한 공유 파일 스토리지를 제공합니다. FSx ONTAP 밀리초 미만의 지연 시간을 제공하는 고성능 SSD(Solid State Drive) 스토리지를 제공합니다. FSx ONTAP 사용하면 데이터의 일부에만 SSD 스토리지 비용을 지불하는 동시에 워크로드에 대해 SSD 수준의 성능을 달성할 수 있습니다.

FSx ONTAP 사용하면 버튼을 클릭하기만 하면 파일의 스냅샷을 생성하고, 복제하고, 복제할 수 있으므로 데이터를 관리하는 것이 더 쉬워집니다. 또한 FSx ONTAP 비용이 저렴하고 탄력적인 스토리지에 데이터를 자동으로 계층화하므로 용량을 프로비저닝하거나 관리할 필요성이 줄어듭니다.

FSx ONTAP 완벽하게 관리되는 백업과 지역 간 재해 복구 지원을 통해 가용성과 내구성이 뛰어난 스토리지를 제공합니다. FSx ONTAP 널리 사용되는 데이터 보안 및 바이러스 백신 애플리케이션을 지원하여 데이터를 보다 쉽게 보호하고 보안을 강화합니다.

자세한 내용은 다음을 방문하세요."게스트 연결 스토리지로서의 FSx ONTAP"

게스트 연결 스토리지로서의 **Cloud Volumes ONTAP (CVO)**

클라우드 볼륨 ONTAP 또는 CVO는 NetApp의 ONTAP 스토리지 소프트웨어를 기반으로 구축된 업계 최고의 클라우드 데이터 관리 솔루션으로, Amazon Web Services(AWS), Microsoft Azure 및 Google Cloud Platform(GCP)에서 기본적으로 제공됩니다.

ONTAP 은 클라우드 기반 스토리지를 사용하는 소프트웨어 정의 버전으로, 클라우드와 온프레미스에서 동일한 스토리지 소프트웨어를 사용할 수 있어 데이터를 관리하는 완전히 새로운 방법에 대한 IT 직원의 재교육 필요성이 줄어듭니다.

CVO를 사용하면 고객은 엣지에서 데이터 센터, 클라우드로 원활하게 데이터를 이동할 수 있으며, 하이브리드 클라우드를 하나로 통합할 수 있습니다. 이 모든 기능은 단일 창 관리 콘솔인 NetApp Cloud Manager를 통해 관리할 수 있습니다.

CVO는 설계상 클라우드에서 가장 까다로운 애플리케이션도 만족시킬 수 있는 극한의 성능과 고급 데이터 관리 기능을 제공합니다.

자세한 내용은 다음을 방문하세요."게스트 연결 스토리지로서의 CVO" .

TR-4938: VMware Cloud on AWS에서 **Amazon FSx ONTAP NFS** 데이터 저장소로 마운트

이 문서에서는 VMware Cloud on AWS에서 Amazon FSx ONTAP NFS 데이터 저장소로 마운트하는 방법을 설명합니다.

소개

모든 성공적인 조직은 변화와 현대화의 길을 걷고 있습니다. 이 과정의 일환으로 기업은 일반적으로 기존 VMware 투자를 활용하여 클라우드의 이점을 활용하고 프로세스에 대한 마이그레이션, 버스트, 확장 및 재해 복구를 가능한 한 원활하게 제공하는 방법을 모색합니다. 클라우드로 마이그레이션하는 고객은 탄력성과 폭발성, 데이터 센터 종료, 데이터 센터 통합, 수명 종료 시나리오, 합병, 인수 등에 대한 사용 사례를 평가해야 합니다.

VMware Cloud on AWS는 고객에게 고유한 하이브리드 기능을 제공하기 때문에 대부분의 고객에게 선호되는 옵션이지만, 기본 스토리지 옵션이 제한적이어서 스토리지 사용량이 많은 작업 부하가 있는 조직에서는 유용성이 제한됩니다. 스토리지는 호스트에 직접 연결되므로 스토리지를 확장하는 유일한 방법은 호스트를 추가하는 것인데, 스토리지를 많이 사용하는 작업의 경우 비용이 35~40% 이상 증가할 수 있습니다. 이러한 작업에는 추가 마력이 아닌 추가 스토리지와 분리된 성능이 필요하지만, 이는 추가 호스트에 대한 비용을 지불해야 함을 의미합니다. 여기가 바로 "최근 통합" FSx ONTAP 은 AWS의 VMware Cloud를 사용하여 스토리지와 성능을 많이 필요로 하는 워크로드에 유용합니다.

다음 시나리오를 생각해 보겠습니다. 고객에게 마력(vCPU/vMem)을 위해 8개의 호스트가 필요하지만, 저장 용량도 상당히 필요합니다. 평가에 따르면 저장 요구 사항을 충족하려면 16개의 호스트가 필요합니다. 실제로 필요한 것이 저장 공간뿐인데도 추가 마력을 모두 구매해야 하므로 전반적인 TCO가 증가합니다. 이는 마이그레이션, 재해 복구, 버스팅, 개발/테스트 등 모든 사용 사례에 적용할 수 있습니다.

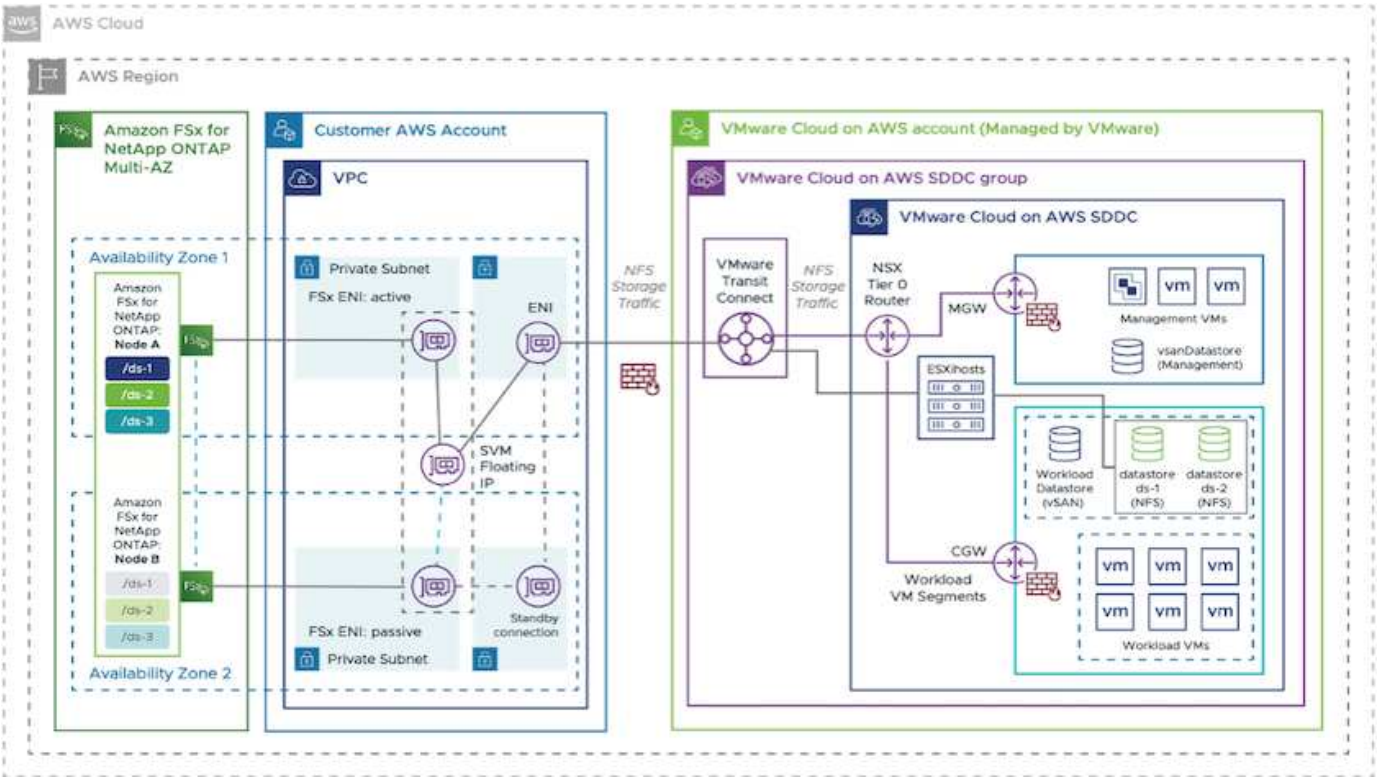
이 문서에서는 VMware Cloud on AWS에서 FSx ONTAP NFS 데이터 저장소로 프로비저닝하고 연결하는 데 필요한 단계를 안내합니다.

ⓘ 이 솔루션은 VMware에서도 제공됩니다. 방문해주세요"AWS의 VMware Cloud 문서" 자세한 내용은.

연결 옵션

AWS의 VMware Cloud는 FSx ONTAP 의 다중 AZ 및 단일 AZ 배포를 모두 지원합니다.

이 섹션에서는 추가 호스트를 추가하지 않고도 SDDC 클러스터의 스토리지를 확장하는 솔루션을 구현하는 데 필요한 단계와 함께 고수준 연결 아키텍처를 설명합니다.



상위 수준의 배포 단계는 다음과 같습니다.

1. 새로 지정된 VPC에 Amazon FSx ONTAP 생성합니다.
2. SDDC 그룹을 만듭니다.
3. VMware Transit Connect와 TGW 첨부 파일을 만듭니다.
4. 라우팅(AWS VPC 및 SDDC)과 보안 그룹을 구성합니다.
5. SDDC 클러스터에 데이터 저장소로 NFS 볼륨을 연결합니다.

FSx ONTAP NFS 데이터 저장소로 프로비저닝하고 연결하기 전에 먼저 VMware on Cloud SDDC 환경을 설정하거나 기존 SDDC를 v1.20 이상으로 업그레이드해야 합니다. 자세한 내용은 다음을 참조하십시오. "AWS에서 VMware Cloud 시작하기" .

FSx ONTAP 현재 스트레치드 클러스터에서 지원되지 않습니다.

결론

이 문서에서는 AWS에서 VMware 클라우드를 사용하여 Amazon FSx ONTAP 구성하는 데 필요한 단계를 설명합니다. Amazon FSx ONTAP 데이터 요구 사항을 애플리케이션 계층에 원활하게 전달하여 TCO를 줄이는 동시에 파일 서비스와 함께 애플리케이션 워크로드를 배포하고 관리할 수 있는 탁월한 옵션을 제공합니다. 어떤 사용 사례든 Amazon FSx ONTAP 과 함께 VMware Cloud on AWS를 선택하면 클라우드의 이점을 빠르게 실현하고,

온프레미스에서 AWS로 일관된 인프라와 운영을 구현하고, 워크로드를 양방향으로 이식하고, 엔터프라이즈급 용량과 성능을 확보할 수 있습니다. 이는 저장소를 연결하는 데 사용되는 익숙한 프로세스 및 절차와 동일합니다. 기억하세요. 새로운 이름과 함께 데이터의 위치만 변경되었을 뿐, 도구와 프로세스는 모두 동일하게 유지되며 Amazon FSx ONTAP 전반적인 배포를 최적화하는 데 도움이 됩니다.

이 과정에 대해 자세히 알아보려면 자세한 안내 영상을 시청하세요.

Amazon FSx ONTAP VMware 클라우드

AWS에서 보충 **NFS** 데이터 저장소 만들기

VMware Cloud가 준비되고 AWS VPC에 연결되면 원래 연결되었거나 기존의 기본 VPC가 아닌 새로 지정된 VPC에 Amazon FSx ONTAP 배포해야 합니다.

시작하려면 SDDC가 있는 동일한 지역 및 가용성 영역에 추가 VPC를 배포한 다음 새 VPC에 Amazon FSx ONTAP 배포합니다. "VMware Cloud에서 SDDC 그룹 구성" 콘솔은 FSx ONTAP 배포될 새로 지정된 VPC에 연결하는 데 필요한 네트워킹 구성 옵션을 활성화합니다.

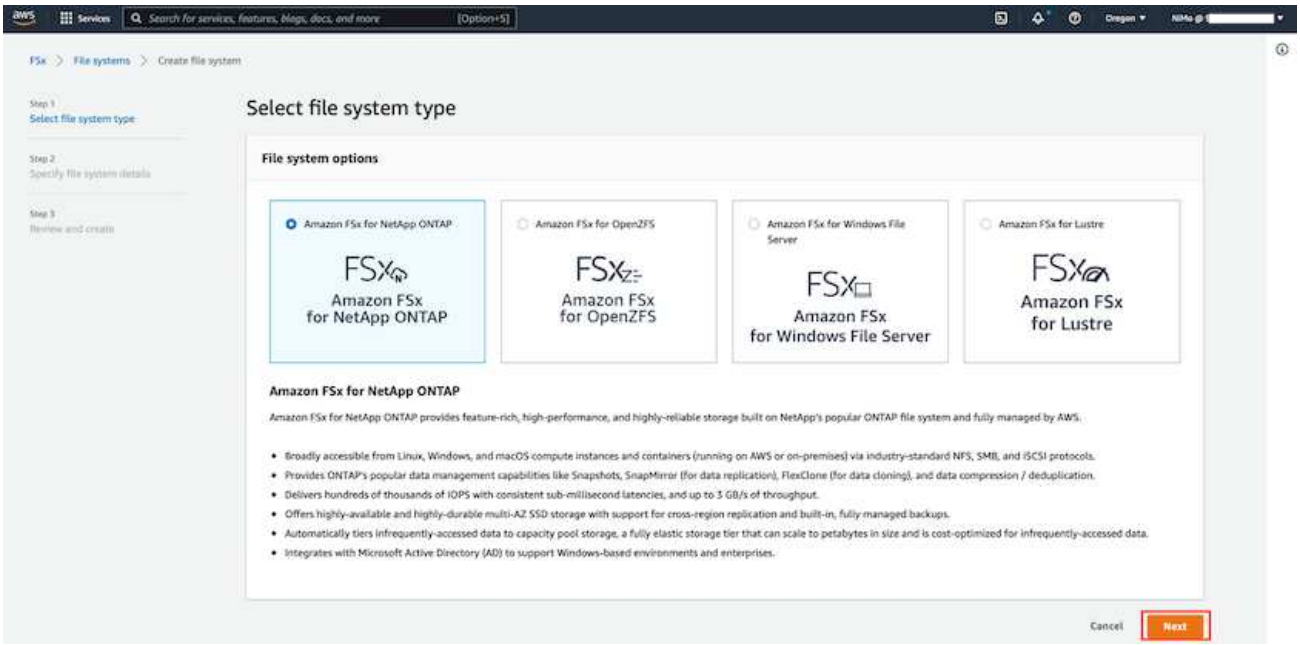
AWS SDDC의 VMware Cloud와 동일한 가용성 영역에 FSx ONTAP 배포합니다.

연결된 VPC에 FSx ONTAP 배포할 수 없습니다. 대신, 새로운 지정된 VPC에 배포한 다음 SDDC 그룹을 통해 VPC를 VMware Managed Transit Gateway(vTGW)에 연결해야 합니다.

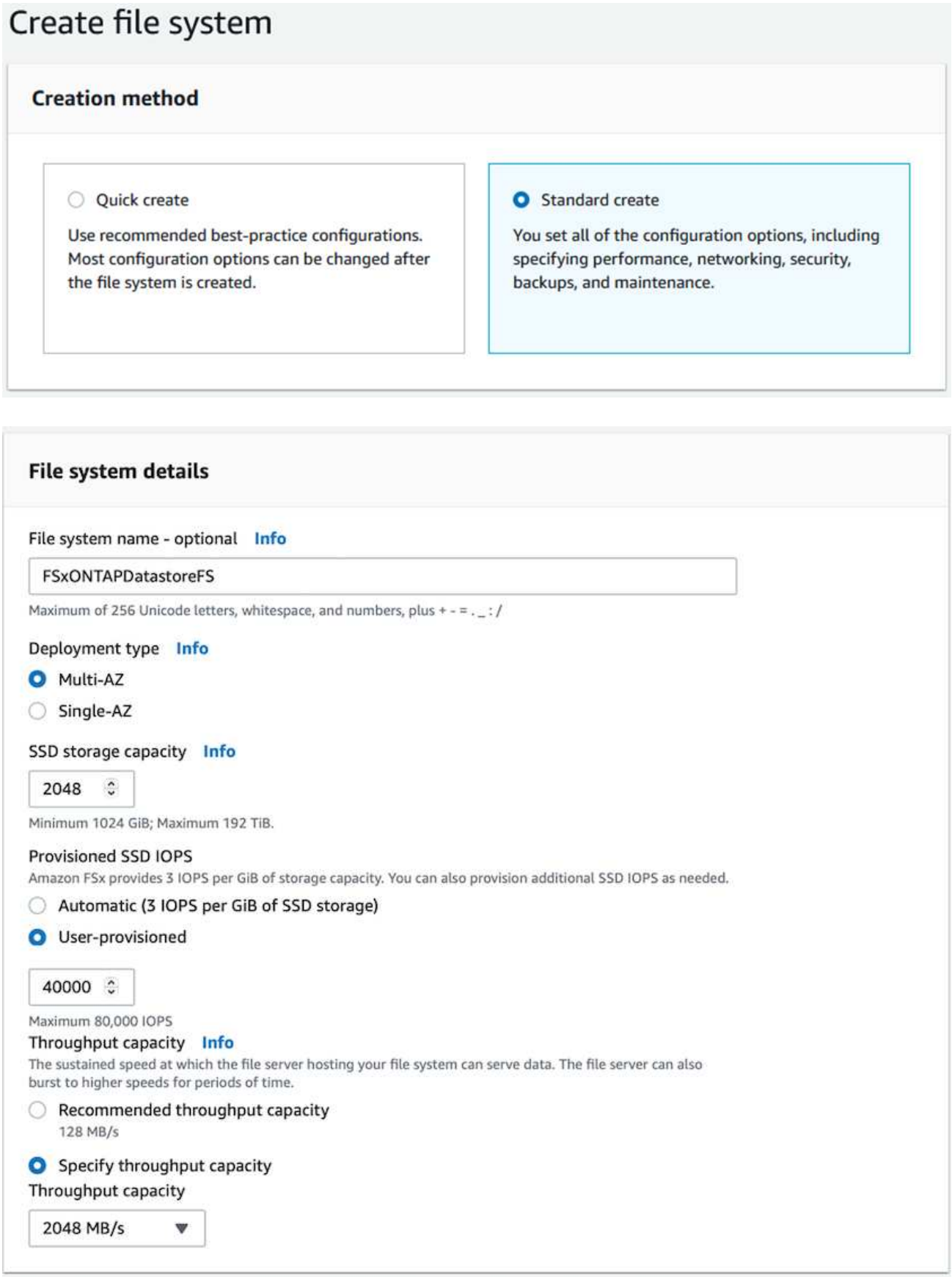
▼ **1**단계**:** 지정된 새 **VPC**에 **Amazon FSx ONTAP** 생성

Amazon FSx ONTAP 파일 시스템을 만들고 마운트하려면 다음 단계를 완료하세요.

1. Amazon FSx 콘솔을 엽니다. `https://console.aws.amazon.com/fsx/` 파일 시스템 생성*을 선택하여 *파일 시스템 생성 마법사를 시작합니다.
2. 파일 시스템 유형 선택 페이지에서 * Amazon FSx ONTAP*을 선택한 후 다음*을 클릭합니다. *파일 시스템 생성 페이지가 나타납니다.



3. 생성 방법으로 *표준 생성*을 선택하세요.

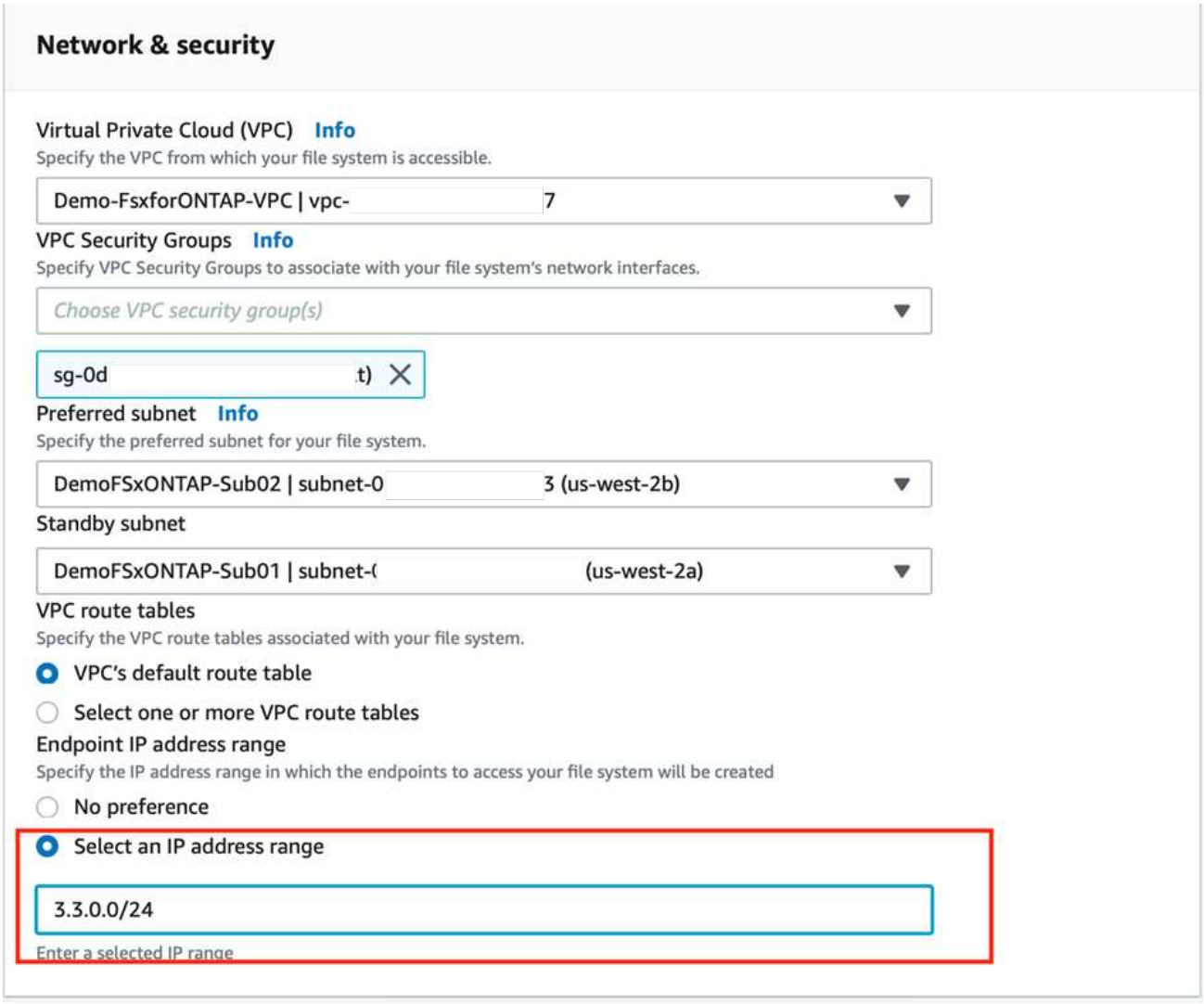


데이터 저장소 크기는 고객마다 상당히 다릅니다. NFS 데이터 저장소당 권장되는 가상 머신 수는 주관적이지만, 각 데이터 저장소에 배치할 수 있는 최적의 VM 수는 여러 요인에 따라 결정됩니다. 대부분의 관리자는 용량만 고려하지만, VMDK로 전송되는 동시 I/O 양은 전반적인 성능에 가장 중요한 요소 중 하나입니다. 온프레미스의 성능 통계를 사용하여 데이터 저장소 볼륨 크기를 적절히 조정합니다.

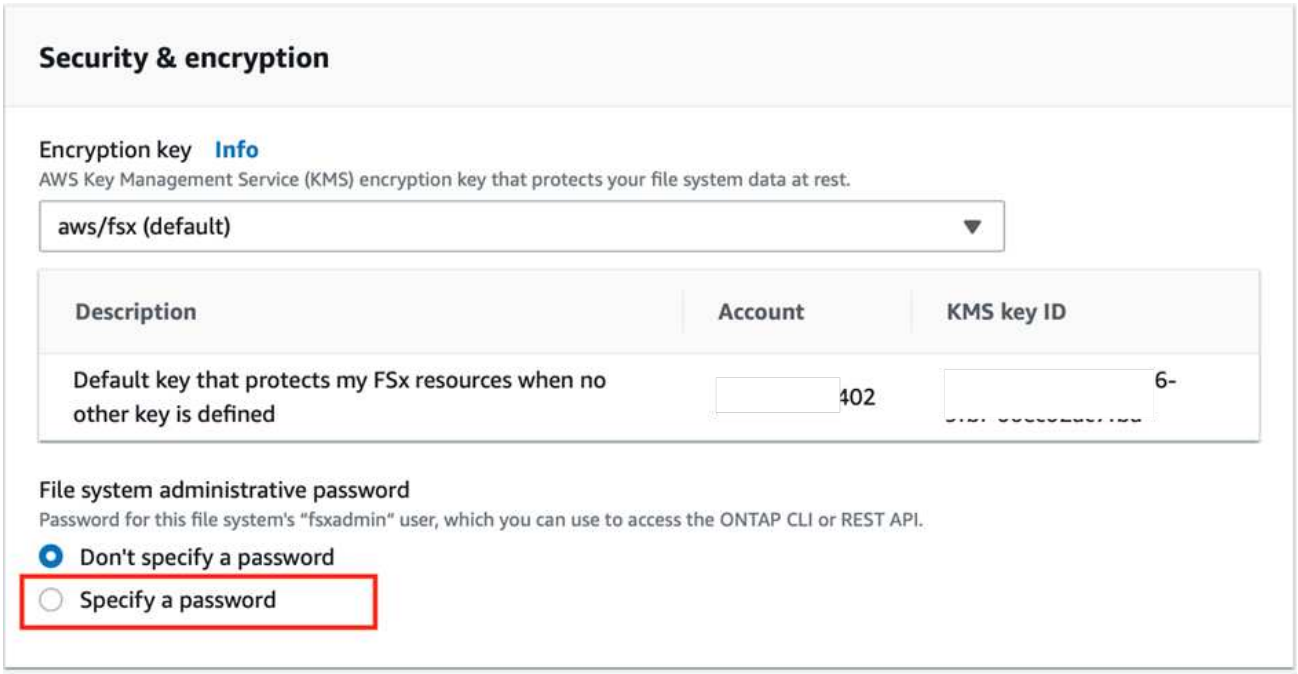
4. Virtual Private Cloud(VPC)의 네트워킹 섹션에서 경로 테이블과 함께 적절한 VPC와 기본 서브넷을 선택합니다. 이 경우 드롭다운 메뉴에서 Demo-FSxforONTAP-VPC가 선택됩니다.

이것이 연결된 VPC가 아닌, 새롭고 지정된 VPC인지 확인하세요.

기본적으로 FSx ONTAP 파일 시스템의 기본 엔드포인트 IP 주소 범위로 198.19.0.0/16을 사용합니다. Endpoint IP 주소 범위가 AWS SDDC, 관련 VPC 서브넷 및 온프레미스 인프라의 VMC와 충돌하지 않는지 확인하세요. 확실하지 않은 경우 충돌이 없는 겹치지 않는 범위를 사용하세요.

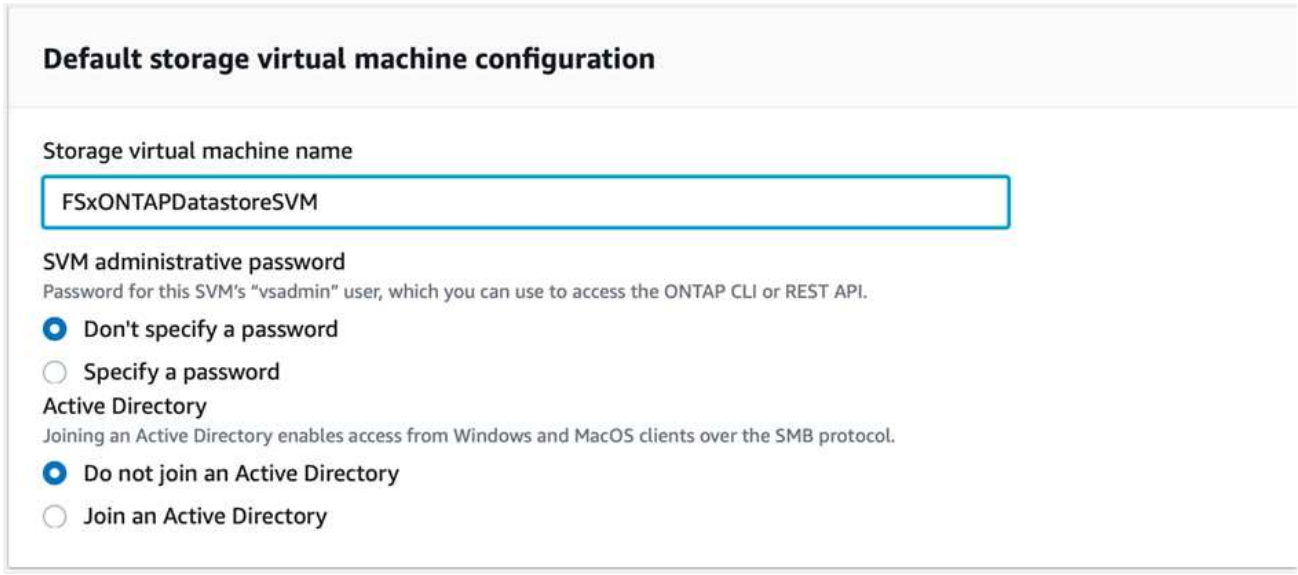


5. 암호화 키의 보안 및 암호화 섹션에서 파일 시스템의 저장 데이터를 보호하는 AWS Key Management Service(AWS KMS) 암호화 키를 선택합니다. *파일 시스템 관리 비밀번호*에 fsxadmin 사용자에 대한 안전한 비밀번호를 입력합니다.



6. 기본 스토리지 가상 머신 구성 섹션에서 SVM의 이름을 지정합니다.

GA 기준으로 4개의 NFS 데이터 저장소가 지원됩니다.



7. 기본 볼륨 구성 섹션에서 데이터 저장소에 필요한 볼륨 이름과 크기를 지정하고 *다음*을 클릭합니다. 이것은 NFSv3 볼륨이어야 합니다. *저장소 효율성*에서 *활성화*를 선택하여 ONTAP 저장소 효율성 기능(압축, 중복 제거, 압축)을 켭니다. 생성 후, 다음과 같이 *_volume modify_*를 사용하여 셸을 사용하여 볼륨 매개변수를 수정합니다.

환경	구성
볼륨 보장(스페이스 보장 스타일)	없음(씬 프로비저닝) - 기본적으로 설정됨
부분적 준비금(부분적 준비금)	0% – 기본적으로 설정됨
snap_reserve(스냅샷 공간 백분율)	0%

환경	구성
자동 크기 조정(autosize-mode)	성장_축소
스토리지 효율성	활성화됨 - 기본적으로 설정됨
자동 삭제	볼륨 / 가장 오래된_첫 번째
볼륨 티어링 정책	스냅샷만 – 기본적으로 설정됨
먼저 시도하세요	자동 성장
스냅샷 정책	None

다음 SSH 명령을 사용하여 볼륨을 만들고 수정하세요.

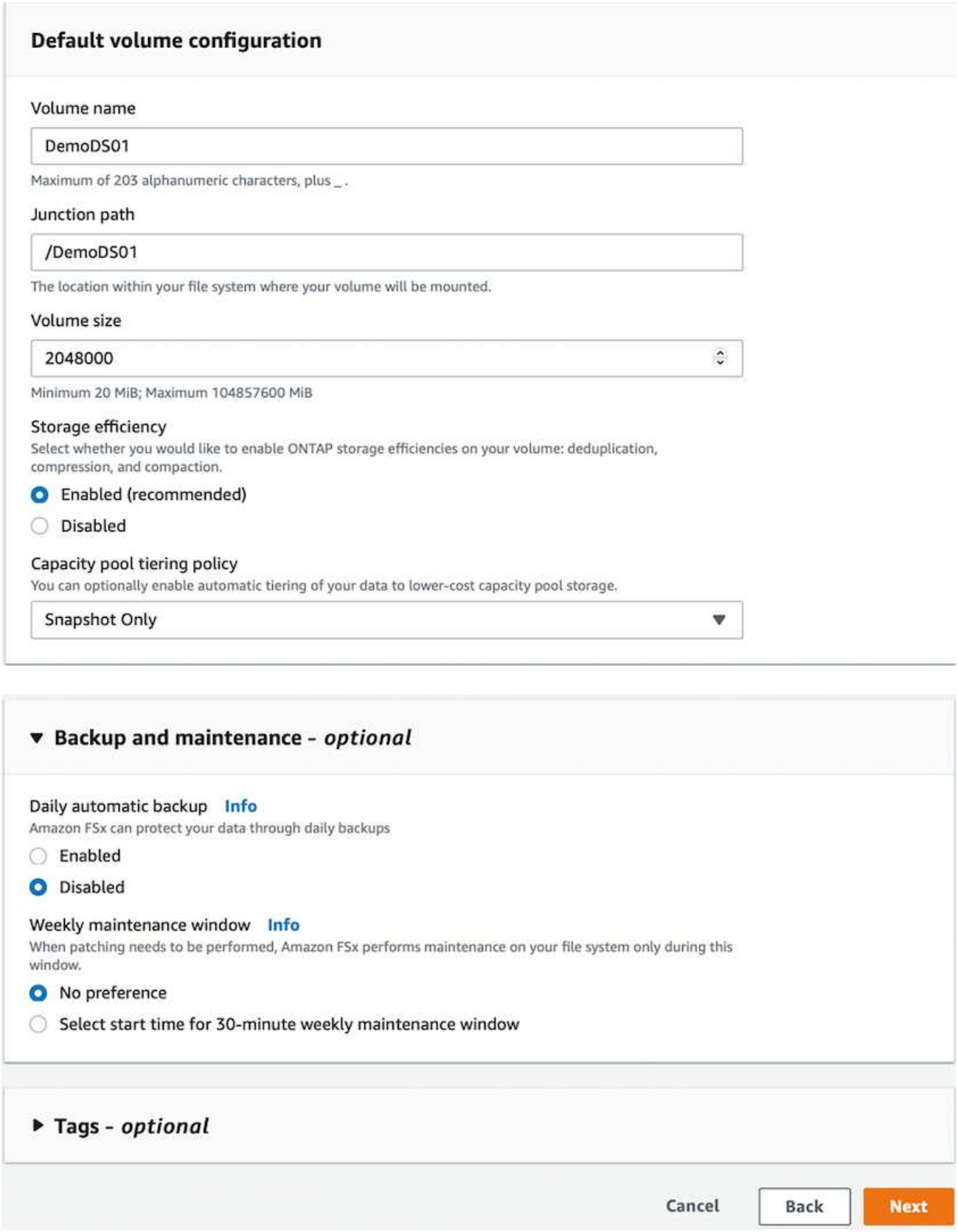
셸에서 새로운 데이터 저장소 볼륨을 생성하는 명령:

```
volume create -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-aggregate aggr1 -size 1024GB -state online -tiering-policy snapshot-
only -percent-snapshot-space 0 -autosize-mode grow -snapshot-policy
none -junction-path /DemoDS002
```

참고: 셸을 통해 생성된 볼륨은 AWS 콘솔에 표시되기까지 몇 분 정도 걸립니다.

기본적으로 설정되지 않은 볼륨 매개변수를 수정하는 명령:

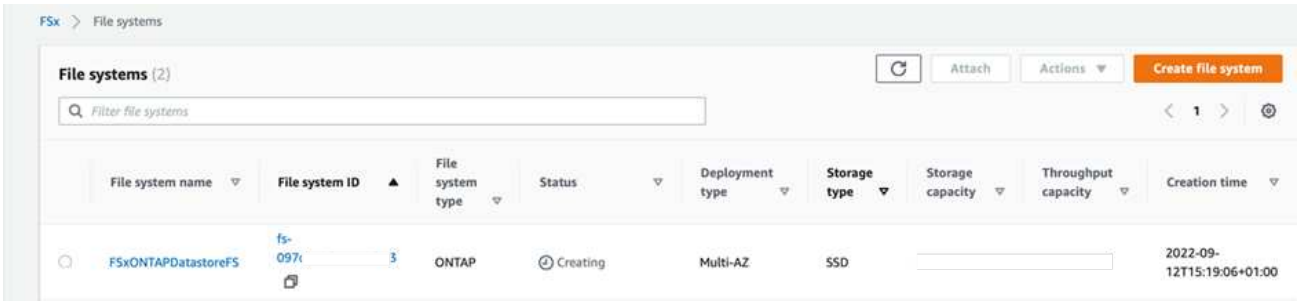
```
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-fractional-reserve 0
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002 -space
-mgmt-try-first vol_grow
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-autosize-mode grow
```

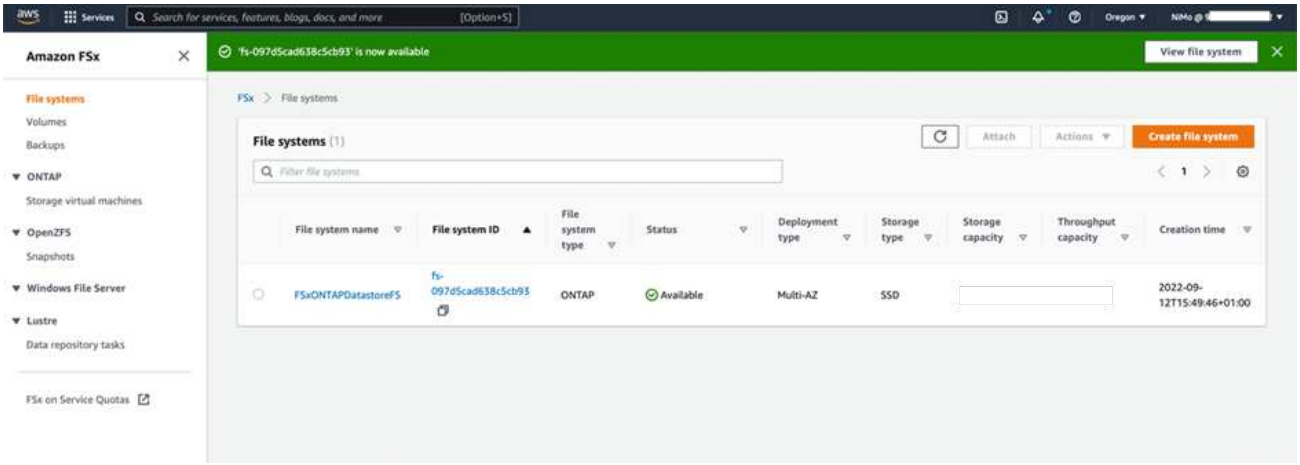


초기 마이그레이션 시나리오에서 기본 스냅샷 정책으로 인해 데이터 저장소 용량이 가득 차는 문제가 발생할 수 있습니다. 이를 극복하려면 필요에 맞게 스냅샷 정책을 수정하세요.

8. 파일 시스템 만들기 페이지에 표시된 파일 시스템 구성을 검토하세요.

9. *파일 시스템 만들기*를 클릭합니다.





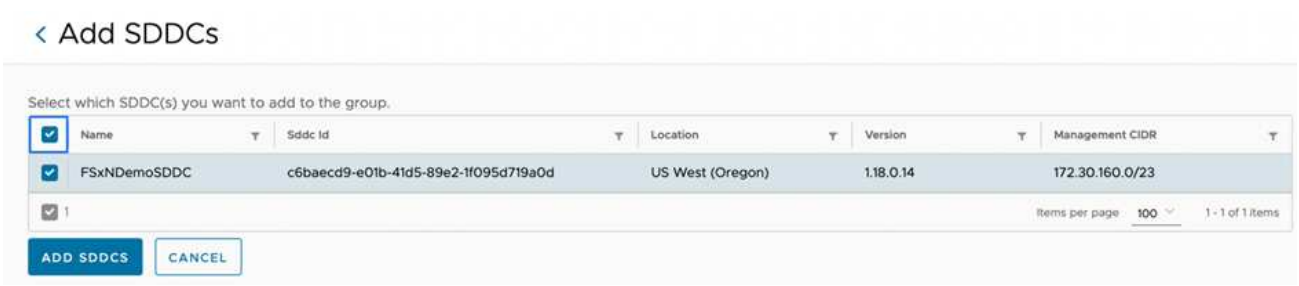
이전 단계를 반복하여 용량 및 성능 요구 사항에 따라 더 많은 스토리지 가상 머신이나 파일 시스템과 데이터 저장소 볼륨을 만듭니다.

Amazon FSx ONTAP 성능에 대해 알아보려면 다음을 참조하세요. "Amazon FSx ONTAP 성능" .

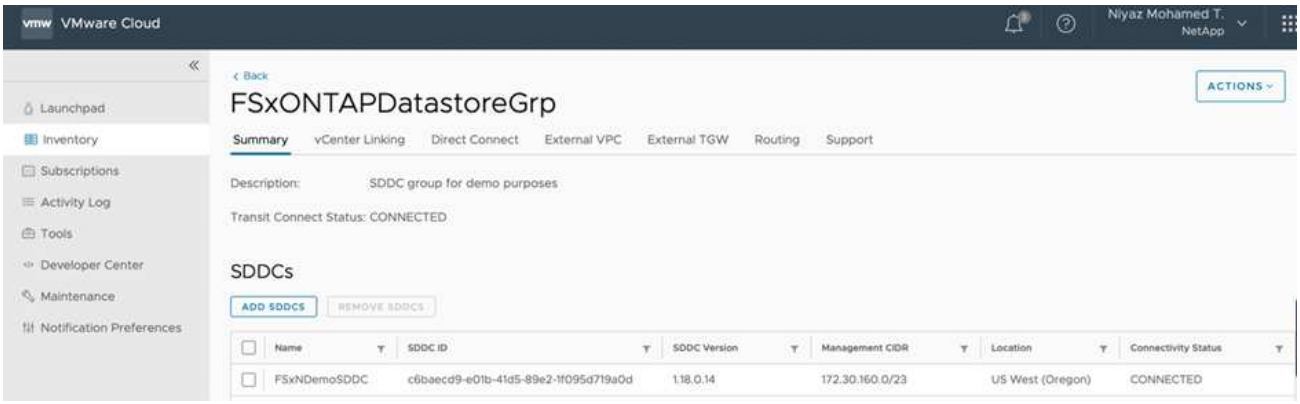
▼ **2**단계**: SDDC** 그룹 만들기

파일 시스템과 SVM을 만든 후 VMware Console을 사용하여 SDDC 그룹을 만들고 VMware Transit Connect를 구성합니다. 그렇게 하려면 다음 단계를 완료하고 VMware Cloud Console과 AWS Console 간을 이동해야 한다는 점을 기억하세요.

1. VMC 콘솔에 로그인하세요 `https://vmc.vmware.com` .
2. 인벤토리 페이지에서 *SDDC 그룹*을 클릭합니다.
3. **SDDC** 그룹 탭에서 *작업*을 클릭하고 *SDDC 그룹 만들기*를 선택합니다. 데모 목적으로 SDDC 그룹을 호출합니다. `FSxONTAPDatastoreGrp` .
4. 멤버십 그리드에서 그룹 멤버로 포함할 SDDC를 선택합니다.

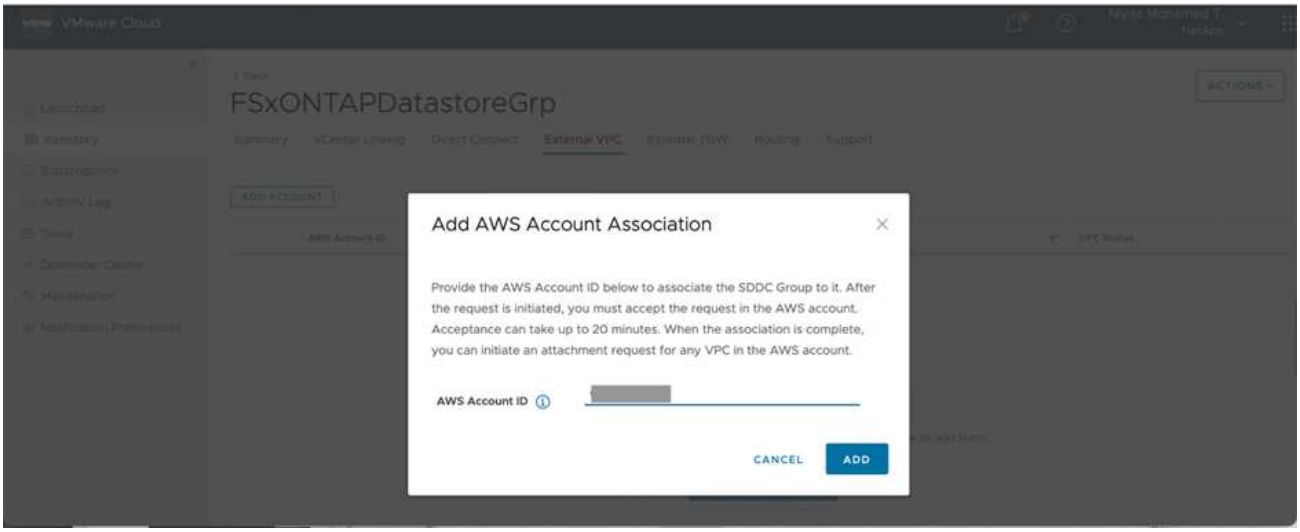


5. "그룹에 VMware Transit Connect를 구성하면 첨부 파일 및 데이터 전송당 요금이 부과됩니다"가 선택되어 있는지 확인한 다음, *그룹 만들기*를 선택합니다. 이 과정을 완료하는 데 몇 분이 걸릴 수 있습니다.

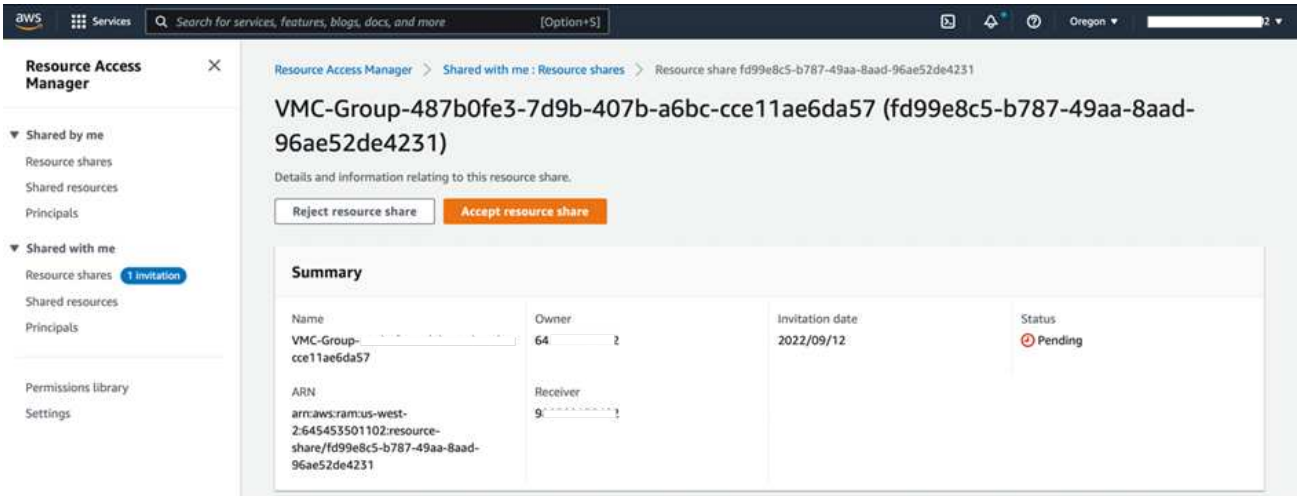


▼ **3**단계**: VMware Transit Connect** 구성

1. 새로 생성된 지정된 VPC를 SDDC 그룹에 연결합니다. 외부 **VPC** 탭을 선택하고 다음을 따르세요. "그룹에 외부 VPC를 연결하기 위한 지침" . 이 과정을 완료하는 데 10~15분이 걸릴 수 있습니다.

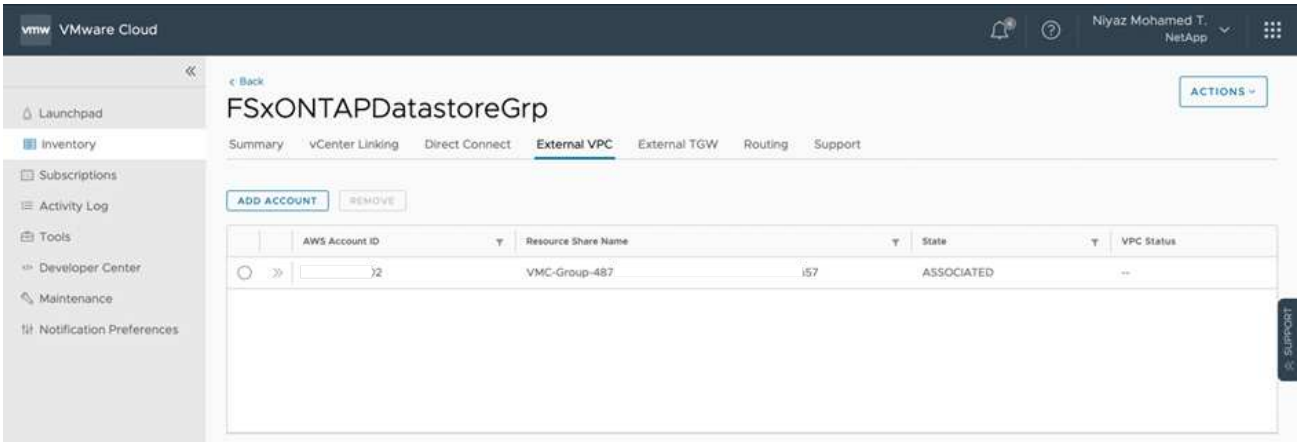


2. *계정 추가*를 클릭하세요.
   a. FSx ONTAP 파일 시스템을 프로비저닝하는 데 사용된 AWS 계정을 제공합니다.
   b. *추가*를 클릭하세요.
3. AWS 콘솔로 돌아와서 동일한 AWS 계정에 로그인하고 **Resource Access Manager** 서비스 페이지로 이동합니다. 리소스 공유를 수락할 수 있는 버튼이 있습니다.



외부 VPC 프로세스의 일부로 AWS 콘솔을 통해 Resource Access Manager를 통해 새로운 공유 리소스에 대한 메시지가 표시됩니다. 공유 리소스는 VMware Transit Connect가 관리하는 AWS Transit Gateway입니다.

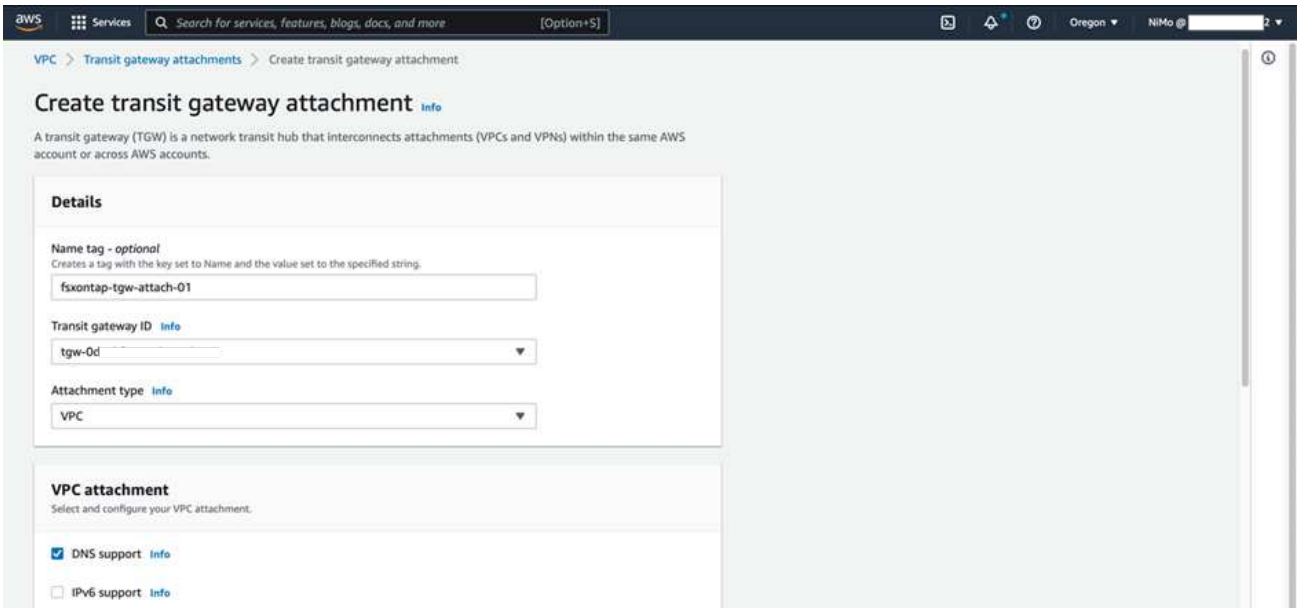
4. *리소스 공유 수락*을 클릭합니다.



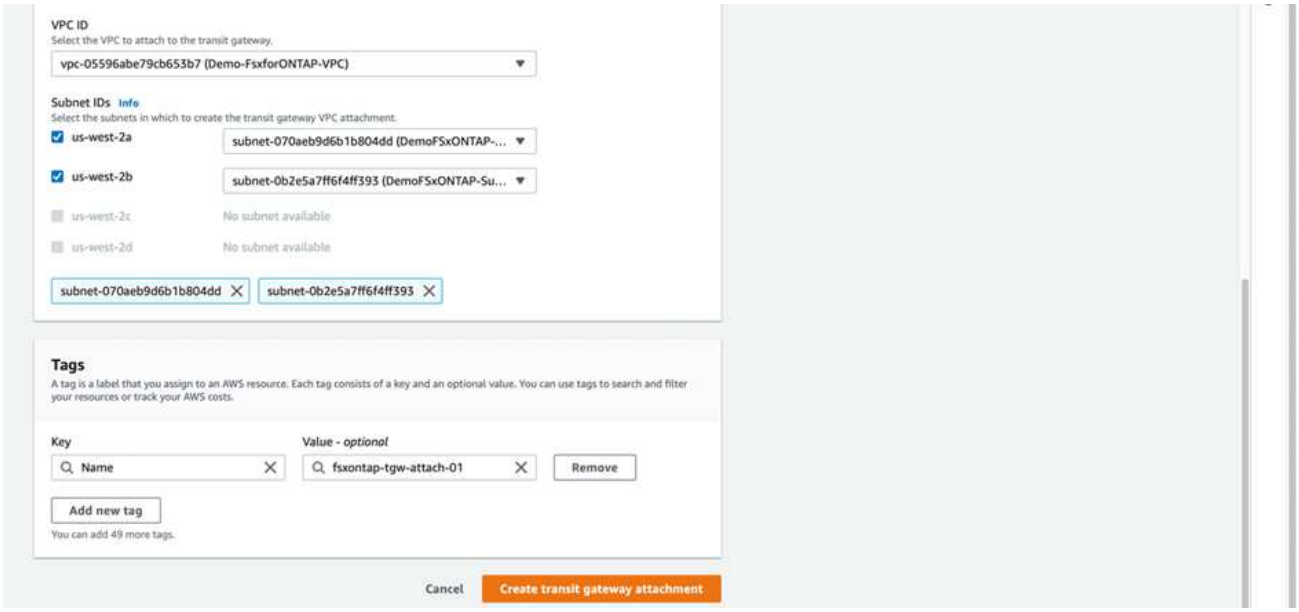
5. VMC 콘솔로 돌아가면 이제 외부 VPC가 연결된 상태임을 확인할 수 있습니다. 나타나기까지 몇 분 정도 걸릴 수 있습니다.

▼ **4**단계**:** 트랜짓 게이트웨이 첨부 파일 만들기

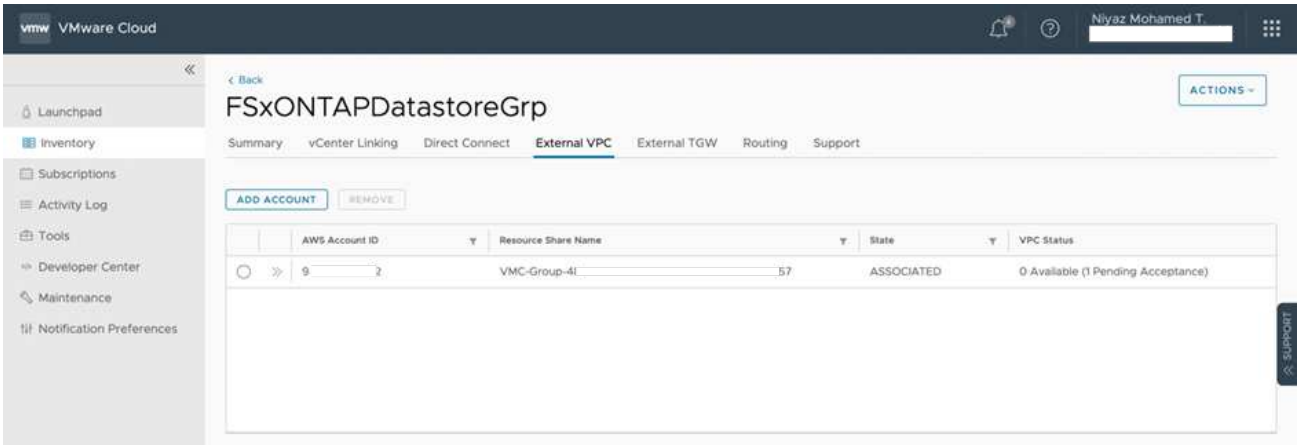
1. AWS 콘솔에서 VPC 서비스 페이지로 이동하여 FSx 파일 시스템 프로비저닝에 사용된 VPC로 이동합니다. 오른쪽 탐색 창에서 *전송 게이트웨이 첨부*를 클릭하여 전송 게이트웨이 첨부를 만듭니다.
2. *VPC 연결*에서 DNS 지원이 선택되어 있는지 확인하고 FSx ONTAP 배포된 VPC를 선택합니다.

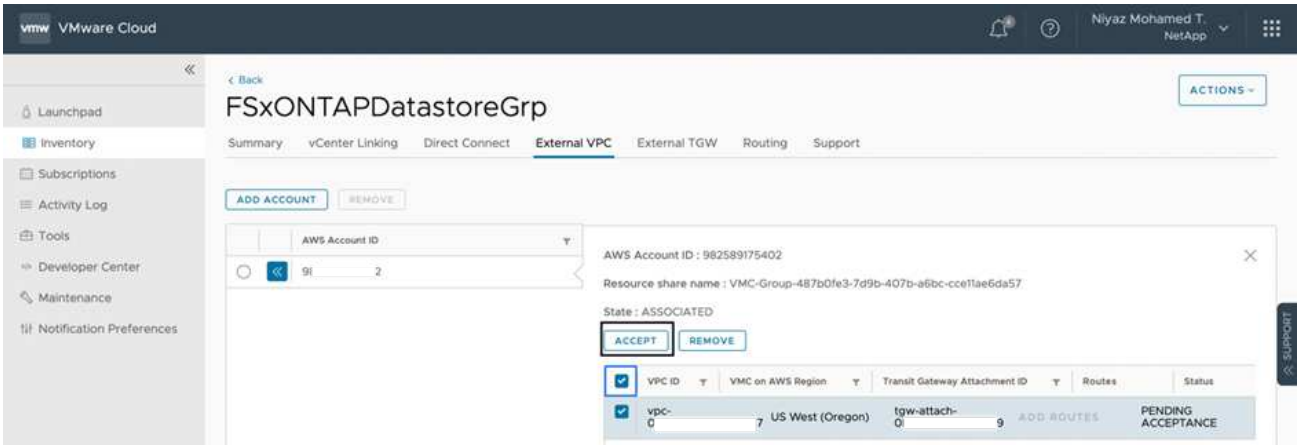


3. *트랜짓 게이트웨이 첨부 파일 만들기*를 클릭합니다.



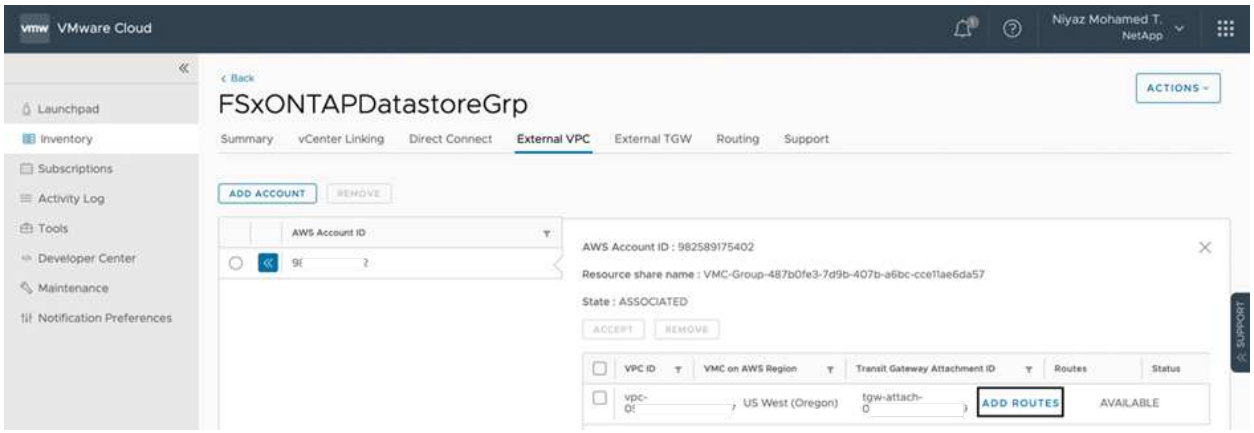
4. VMware Cloud Console로 돌아와 SDDC 그룹 > 외부 VPC 탭으로 돌아갑니다. FSx에 사용된 AWS 계정 ID를 선택하고 VPC를 클릭한 후 *수락*을 클릭합니다.

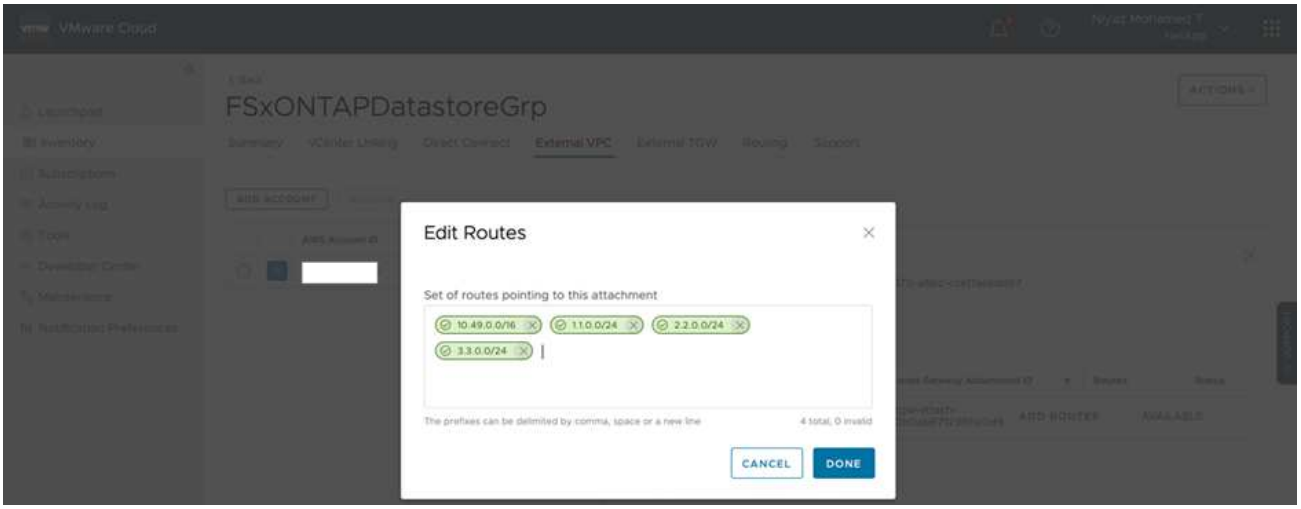




이 옵션이 나타나기까지 몇 분 정도 걸릴 수 있습니다.

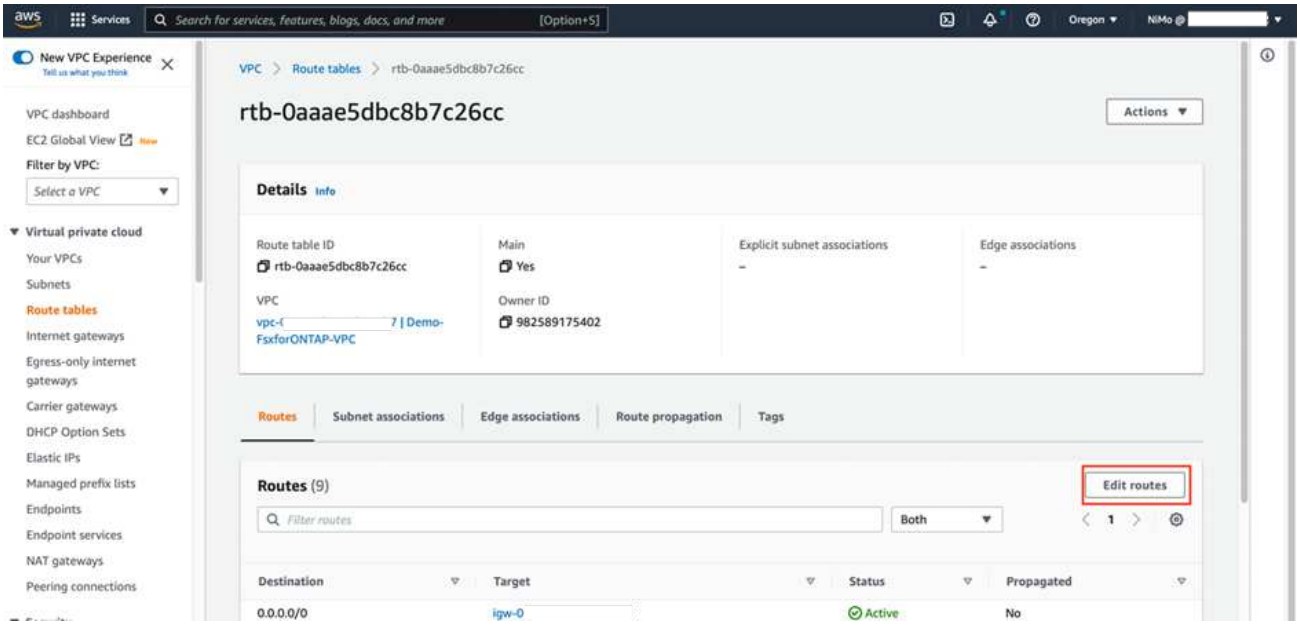
5. 그런 다음 경로 열의 외부 **VPC** 탭에서 경로 추가 옵션을 클릭하고 필요한 경로를 추가합니다.
   - Amazon FSx ONTAP 플로팅 IP에 대한 플로팅 IP 범위에 대한 경로입니다.
   - 새로 생성된 외부 VPC 주소 공간에 대한 경로입니다.



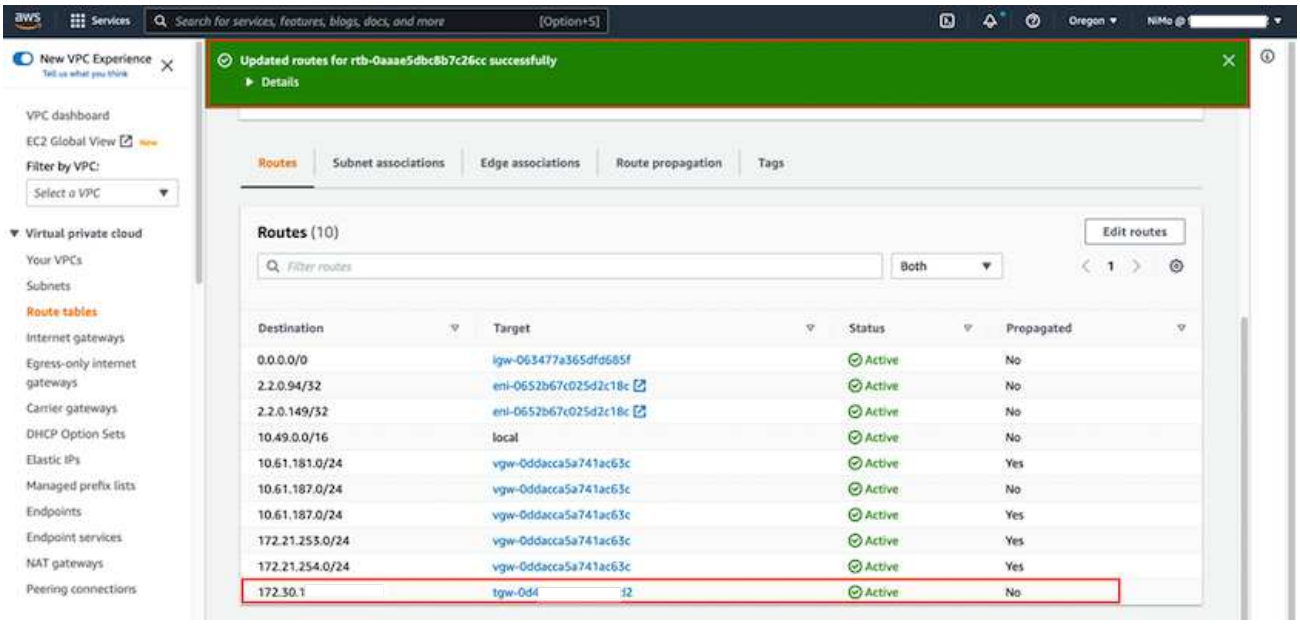


▼ **5**단계**:** 라우팅**(AWS VPC** 및 **SDDC)** 및 보안 그룹 구성

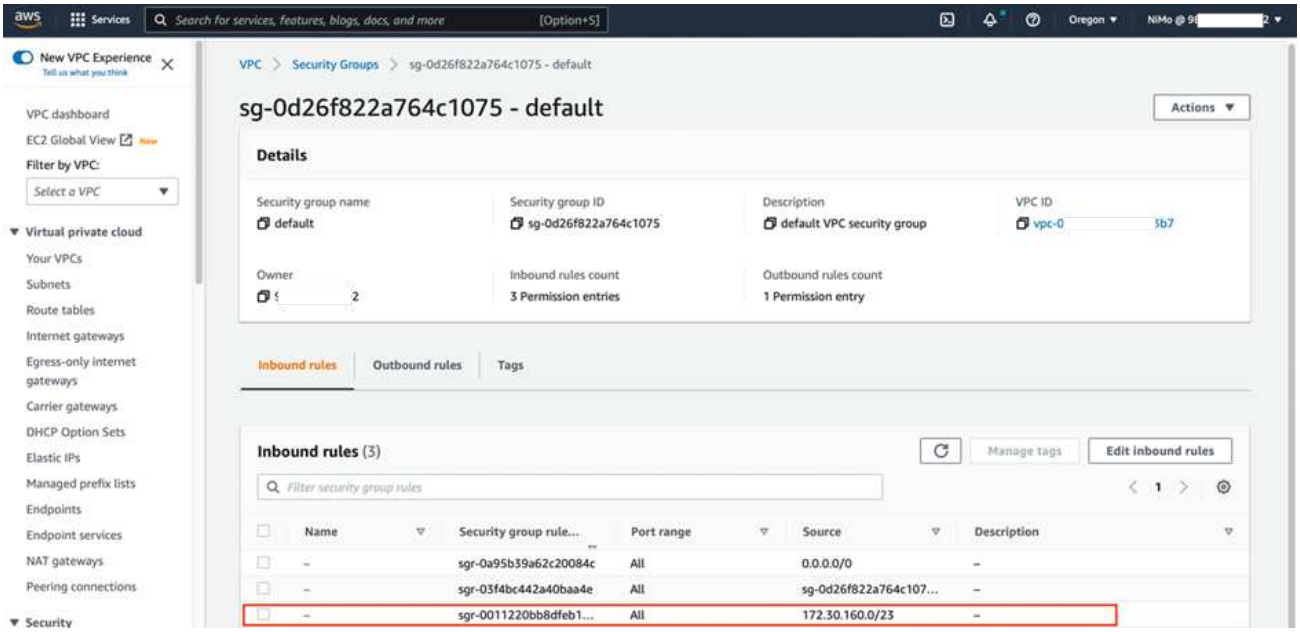
1. AWS 콘솔에서 VPC 서비스 페이지에서 VPC를 찾아 SDDC로 돌아가는 경로를 만들고 VPC에 대한 기본 경로 테이블을 선택합니다.
2. 하단 패널에서 경로 테이블을 찾아 *경로 편집*을 클릭합니다.



3. 경로 편집 패널에서 *경로 추가*를 클릭하고 *전송 게이트웨이*를 선택하여 SDDC 인프라의 CIDR과 관련 TGW ID를 입력합니다. *변경 사항 저장*을 클릭합니다.



4. 다음 단계는 연관된 VPC의 보안 그룹이 SDDC 그룹 CIDR에 대한 올바른 인바운드 규칙으로 업데이트되었는지 확인하는 것입니다.
5. SDDC 인프라의 CIDR 블록으로 인바운드 규칙을 업데이트합니다.



연결 문제를 방지하기 위해 VPC(FSx ONTAP 있는 곳) 경로 테이블이 업데이트되었는지 확인하세요.

NFS 트래픽을 허용하도록 보안 그룹을 업데이트합니다.

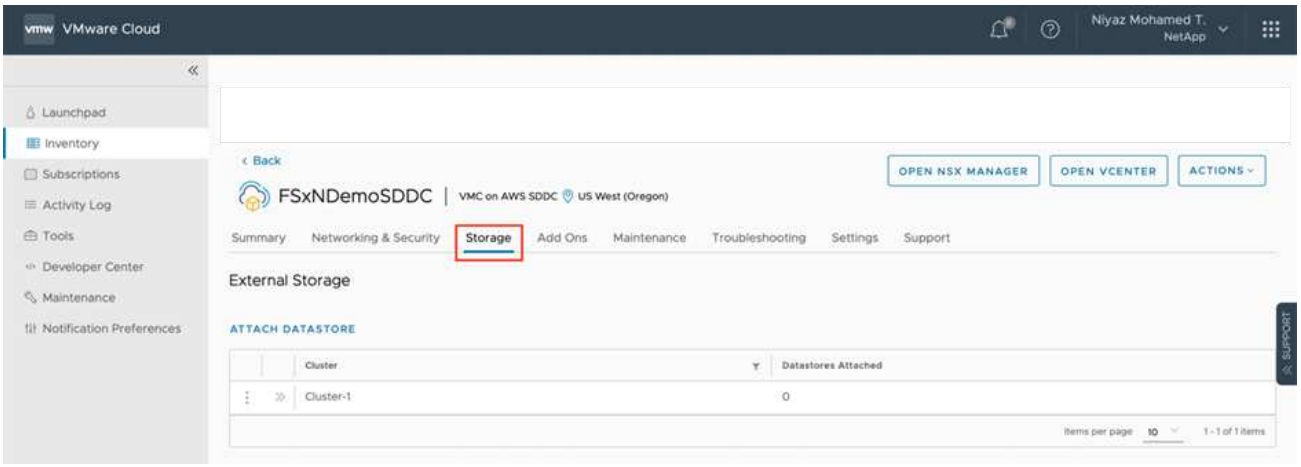
이는 적절한 SDDC에 대한 연결을 준비하는 마지막 단계입니다. 파일 시스템을 구성하고, 경로를 추가하고, 보안 그룹을 업데이트했으므로 이제 데이터 저장소를 마운트할 차례입니다.

▼ 6단계: **NFS** 볼륨을 **SDDC** 클러스터에 데이터 저장소로 연결

파일 시스템이 프로비저닝되고 연결이 설정되면 VMware Cloud Console에 액세스하여 NFS 데이터 저장소를

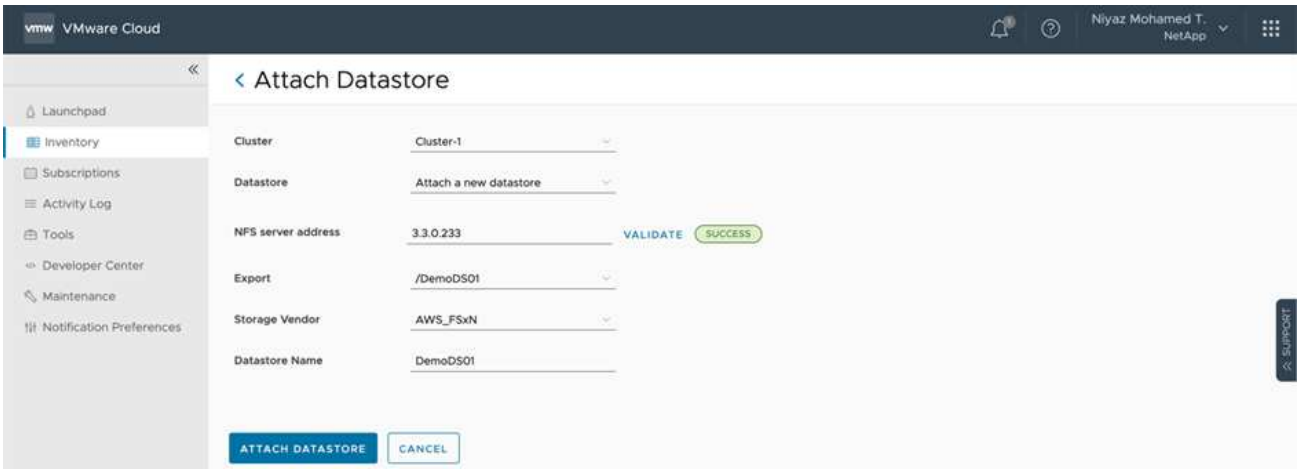
마운트합니다.

1. VMC 콘솔에서 SDDC의 저장소 탭을 엽니다.

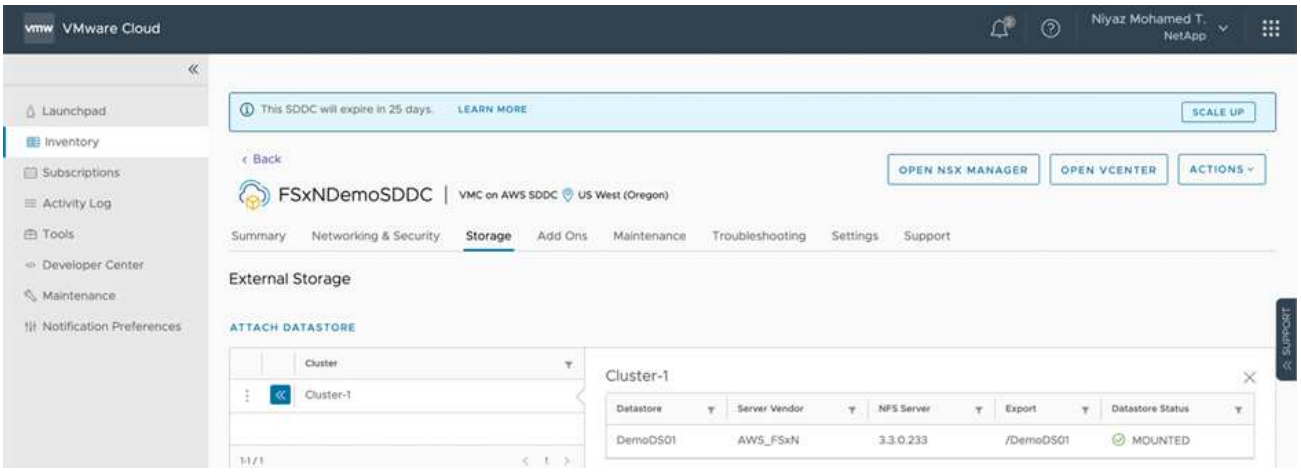


2. *데이터스토어 연결*을 클릭하고 필요한 값을 입력하세요.

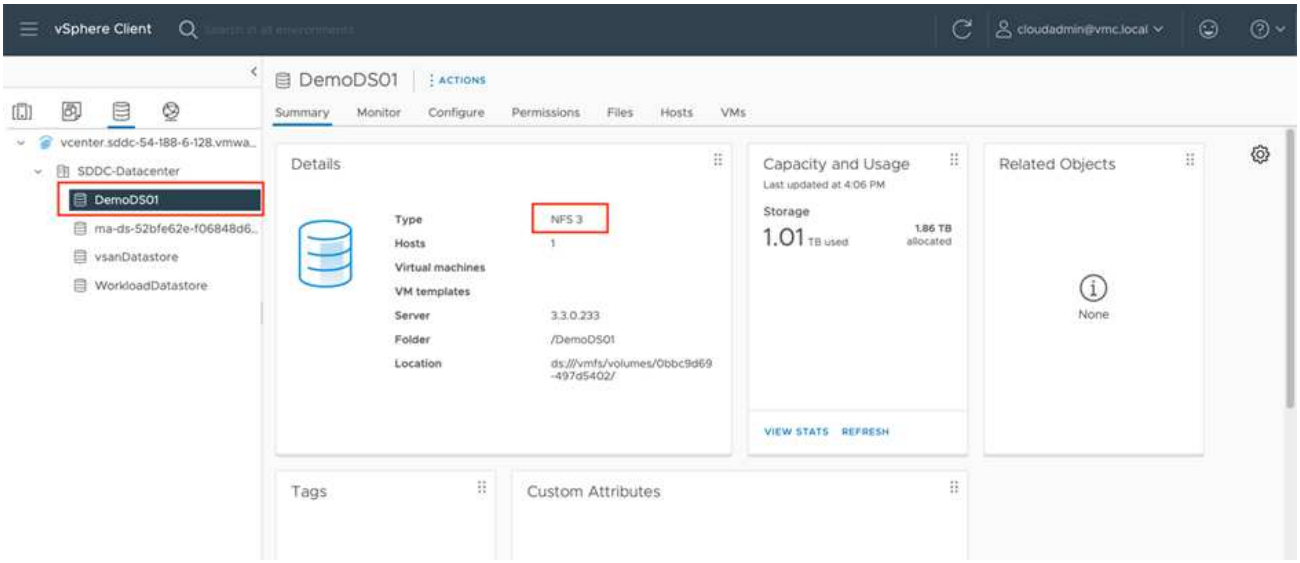
NFS 서버 주소는 AWS 콘솔의 FSx > 스토리지 가상 머신 탭 > 엔드포인트에서 찾을 수 있는 NFS IP 주소입니다.



3. *데이터 저장소 연결*을 클릭하여 클러스터에 데이터 저장소를 연결합니다.



4. 아래와 같이 vCenter에 액세스하여 NFS 데이터 저장소를 검증합니다.



AWS용 **NetApp** 게스트 연결 스토리지 옵션

AWS는 기본 FSx 서비스(FSx ONTAP) 또는 Cloud Volumes ONTAP (CVO)를 통해 게스트에 연결된 NetApp 스토리지를 지원합니다.

FSx ONTAP

Amazon FSx ONTAP NetApp의 인기 있는 ONTAP 파일 시스템을 기반으로 높은 안정성, 확장성, 고성능, 다양한 기능을 갖춘 파일 스토리지를 제공하는 완전 관리형 서비스입니다. FSx ONTAP NetApp 파일 시스템의 친숙한 기능, 성능, 기능 및 API 운영과 완벽하게 관리되는 AWS 서비스의 민첩성, 확장성 및 단순성을 결합합니다.

FSx ONTAP AWS나 온프레미스에서 실행되는 Linux, Windows, macOS 컴퓨팅 인스턴스에서 광범위하게 액세스할 수 있는 기능이 풍부하고 빠르며 유연한 공유 파일 스토리지를 제공합니다. FSx ONTAP 밀리초 미만의 지연 시간을 제공하는 고성능 SSD(Solid State Drive) 스토리지를 제공합니다. FSx ONTAP 사용하면 데이터의 일부에만 SSD 스토리지 비용을 지불하는 동시에 워크로드에 대해 SSD 수준의 성능을 달성할 수 있습니다.

FSx ONTAP 사용하면 버튼을 클릭하기만 하면 파일의 스냅샷을 생성하고, 복제하고, 복제할 수 있으므로 데이터를 관리하는 것이 더 쉬워집니다. 또한 FSx ONTAP 비용이 저렴하고 탄력적인 스토리지에 데이터를 자동으로 계층화하므로 용량을 프로비저닝하거나 관리할 필요성이 줄어듭니다.

FSx ONTAP 완벽하게 관리되는 백업과 지역 간 재해 복구 지원을 통해 가용성과 내구성이 뛰어난 스토리지를 제공합니다. FSx ONTAP 널리 사용되는 데이터 보안 및 바이러스 백신 애플리케이션을 지원하여 데이터를 보다 쉽게 보호하고 보안을 강화합니다.

게스트 연결 스토리지로서의 **FSx ONTAP**

▼ **VMware Cloud on AWS**를 사용하여 **Amazon FSx ONTAP** 구성

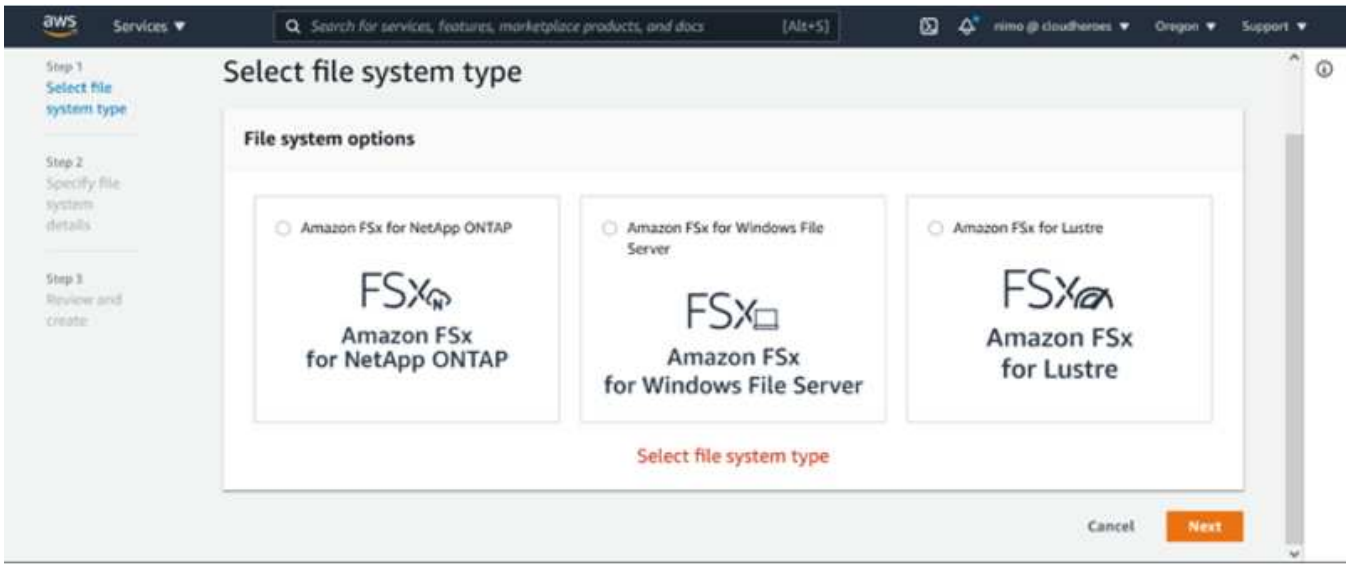
Amazon FSx ONTAP 파일 공유 및 LUN은 AWS의 VMware Cloud에서 VMware SDDC 환경 내에 생성된 VM에서 마운트할 수 있습니다. 볼륨은 Linux 클라이언트에 마운트되고 NFS 또는 SMB 프로토콜을 사용하여 Windows 클라이언트에 매핑될 수 있으며, LUN은 iSCSI를 통해 마운트될 때 블록 장치로 Linux 또는 Windows 클라이언트에 액세스할 수 있습니다. 다음 단계에 따라 NetApp ONTAP 파일 시스템용 Amazon FSx 빠르게 설정할 수 있습니다.

더 나은 성능을 얻고 가용성 영역 간 데이터 전송 요금을 방지하려면 Amazon FSx ONTAP 과 VMware Cloud on AWS가 동일한 가용성 영역에 있어야 합니다.

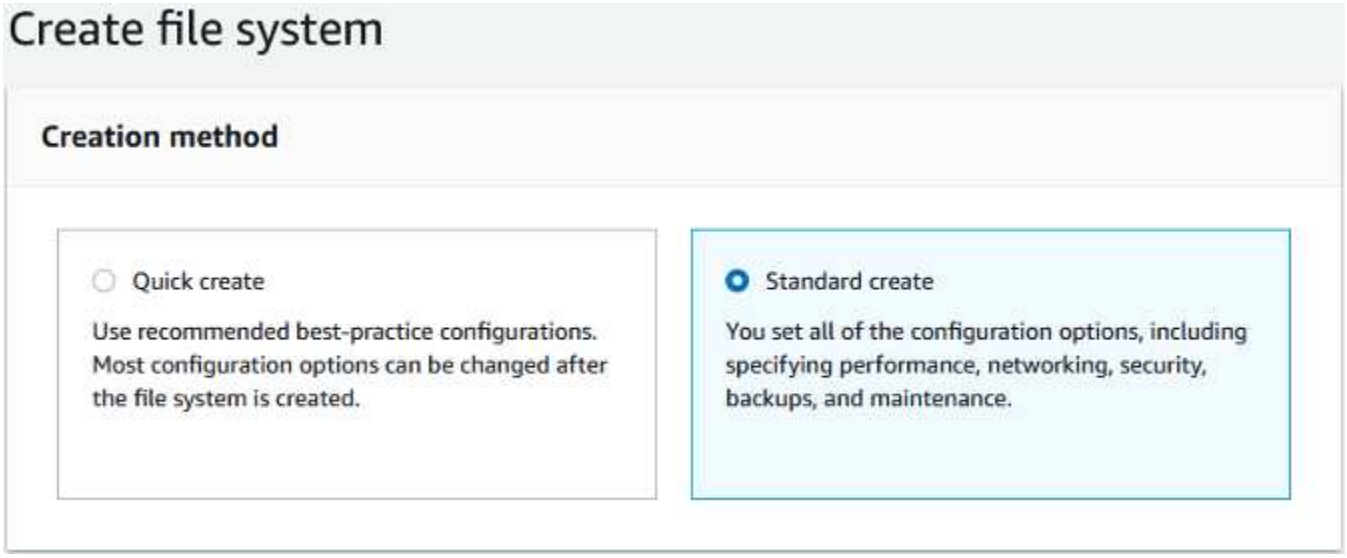
▼ **Amazon FSx ONTAP** 볼륨 생성 및 마운트

Amazon FSx ONTAP 파일 시스템을 만들고 마운트하려면 다음 단계를 완료하세요.

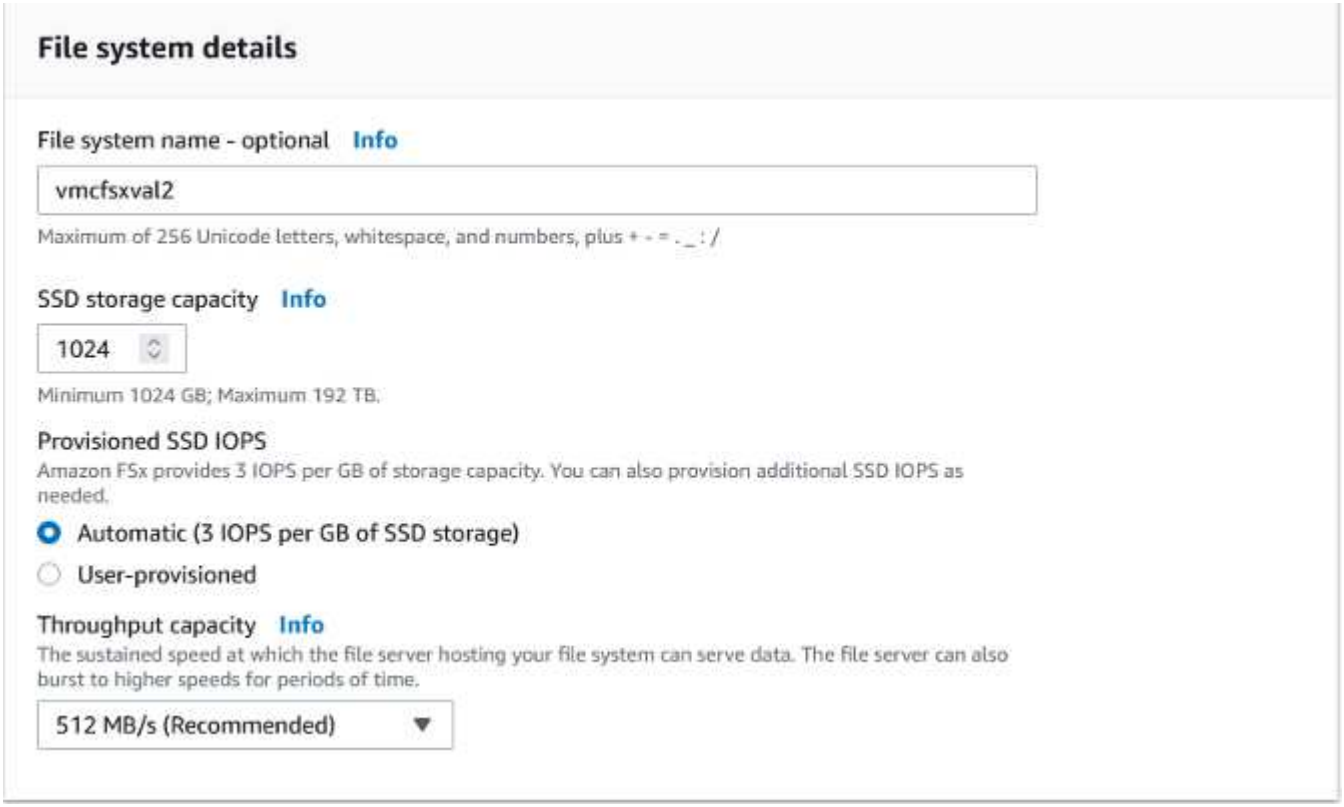
1. 열기"Amazon FSx 콘솔" 파일 시스템 생성 마법사를 시작하려면 파일 시스템 생성을 선택하세요.
2. 파일 시스템 유형 선택 페이지에서 Amazon FSx ONTAP 선택한 후 다음을 선택합니다. 파일 시스템 생성 페이지가 나타납니다.



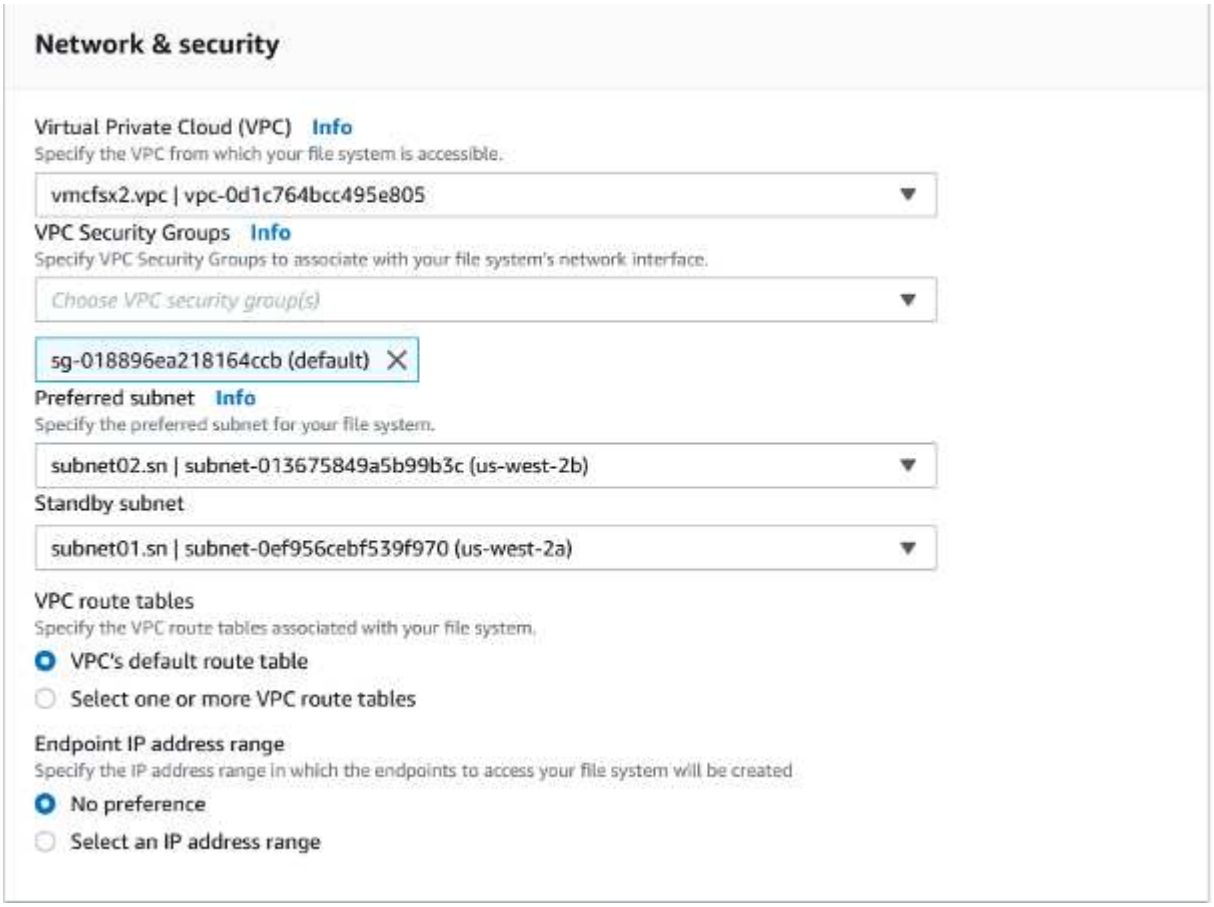
1. 네트워킹 섹션에서 Virtual Private Cloud(VPC)에 대해 경로 테이블과 함께 적절한 VPC와 기본 서브넷을 선택합니다. 이 경우 드롭다운에서 vmcfsx2.vpc가 선택됩니다.



1. 생성 방법으로 표준 생성을 선택하세요. 빠른 생성을 선택할 수도 있지만, 이 문서에서는 표준 생성 옵션을 사용합니다.

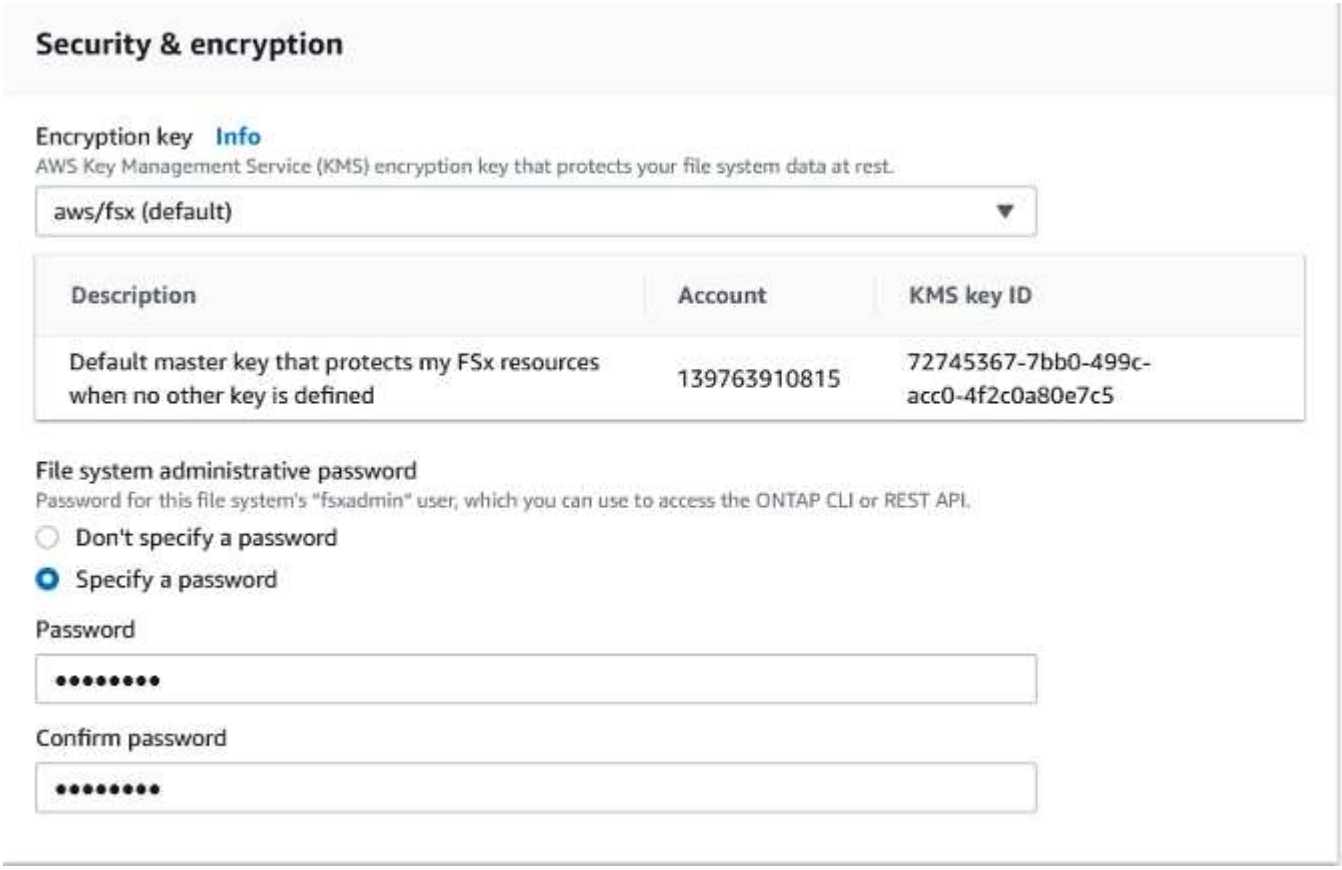


1. 네트워킹 섹션에서 Virtual Private Cloud(VPC)에 대해 경로 테이블과 함께 적절한 VPC와 기본 서브넷을 선택합니다. 이 경우 드롭다운에서 vmcfsx2.vpc가 선택됩니다.

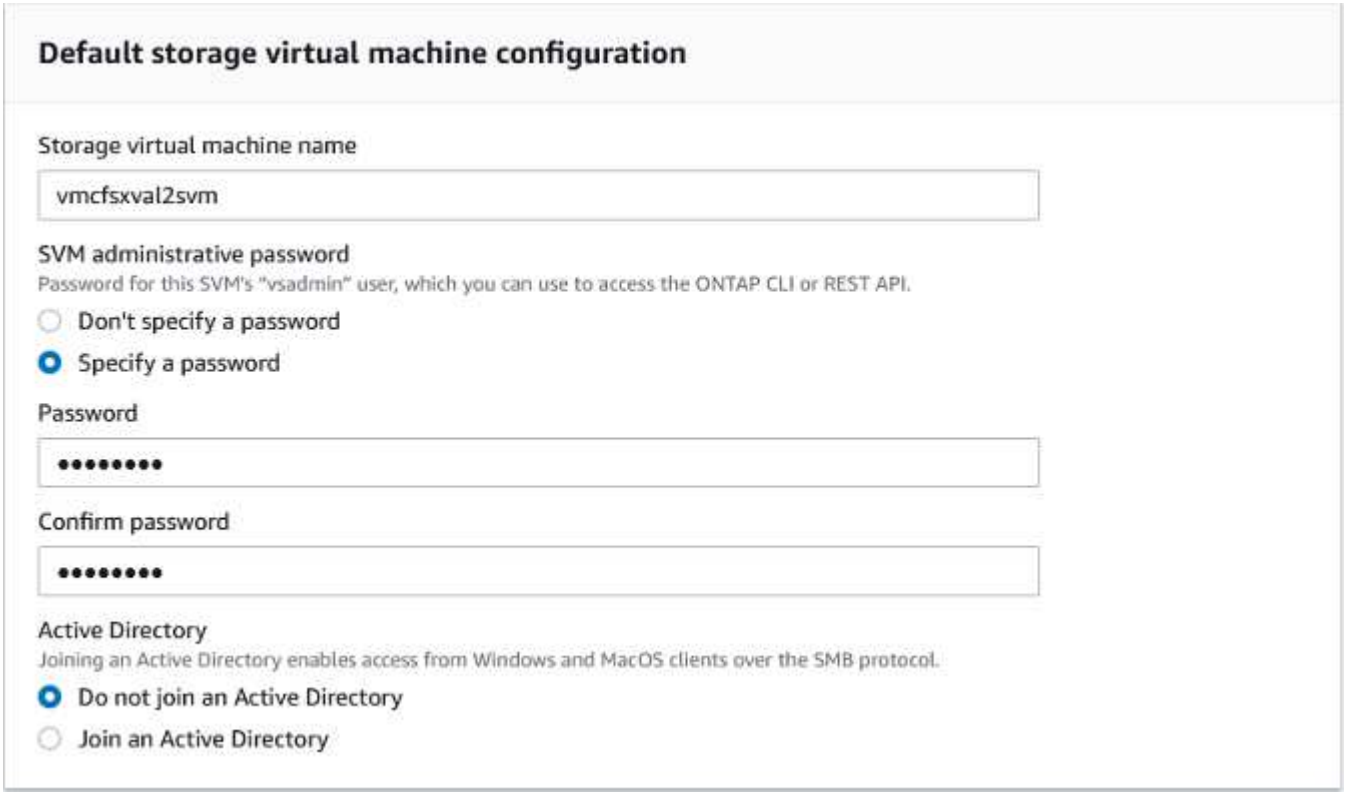


네트워킹 섹션에서 Virtual Private Cloud(VPC)에 대해 경로 테이블과 함께 적절한 VPC와 기본 서브넷을 선택합니다. 이 경우 드롭다운에서 vmcfsx2.vpc가 선택됩니다.

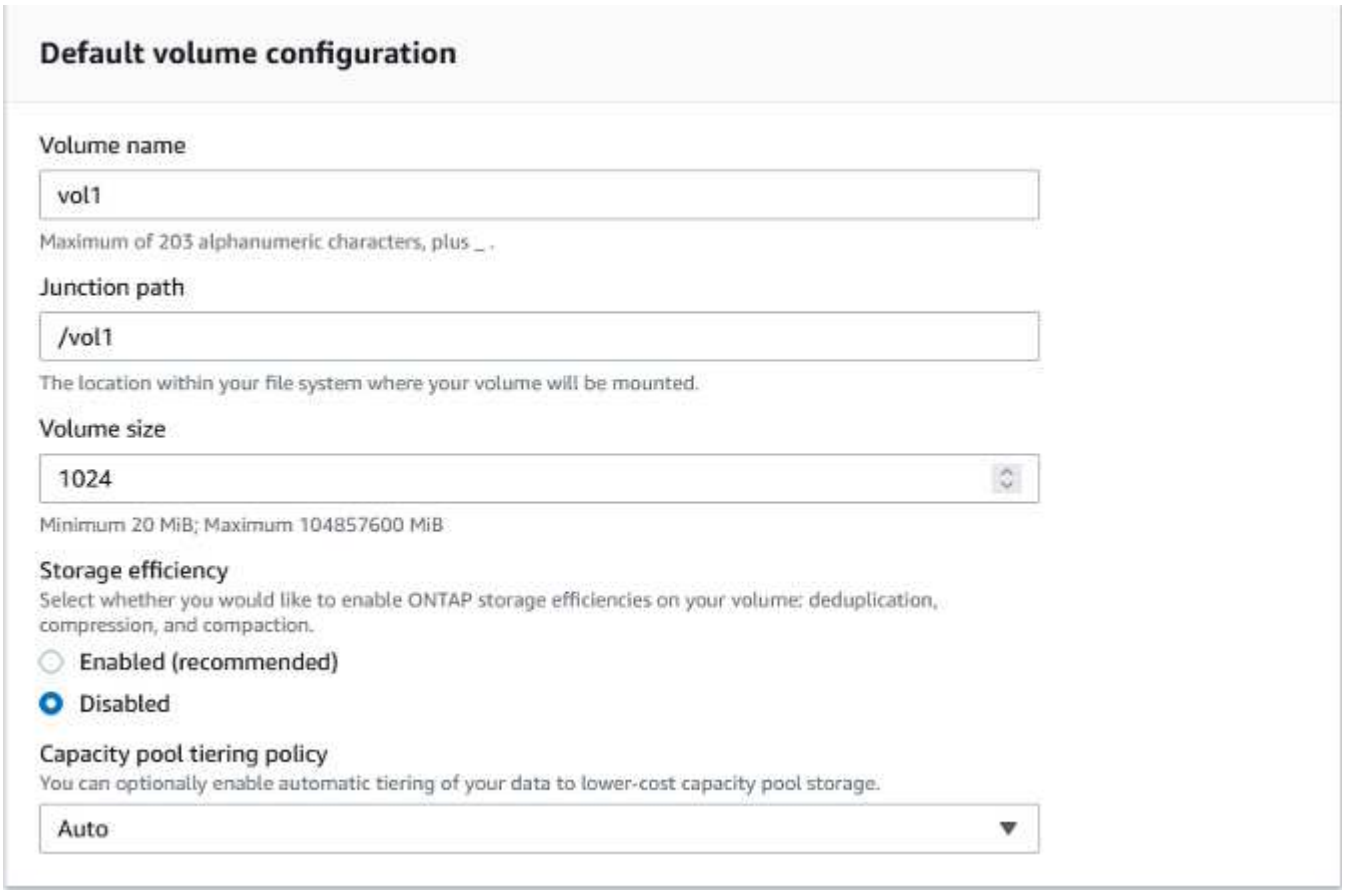
1. 보안 및 암호화 섹션에서 암호화 키에 대해 파일 시스템의 저장 데이터를 보호하는 AWS Key Management Service(AWS KMS) 암호화 키를 선택합니다. 파일 시스템 관리 비밀번호에 fsxadmin 사용자에 대한 안전한 비밀번호를 입력합니다.



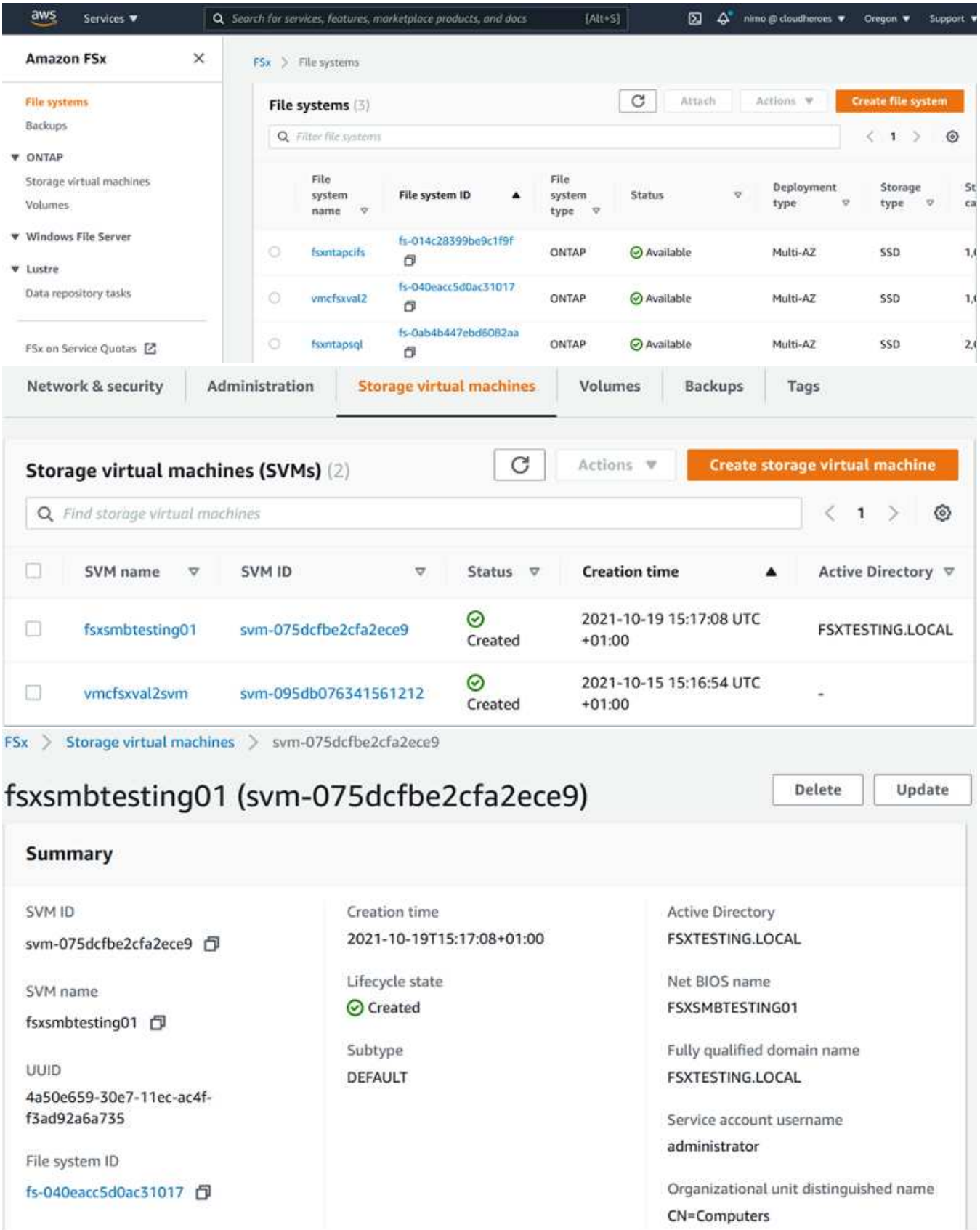
1. 가상 머신에서 REST API나 CLI를 사용하여 ONTAP 관리할 때 vsadmin에 사용할 비밀번호를 지정합니다. 비밀번호가 지정되지 않으면 fsxadmin 사용자를 사용하여 SVM을 관리할 수 있습니다. Active Directory 섹션에서 SMB 공유를 프로비저닝하기 위해 Active Directory를 SVM에 가입해야 합니다. 기본 저장소 가상 머신 구성 섹션에서 이 유효성 검사의 저장소 이름을 제공합니다. SMB 공유는 자체 관리형 Active Directory 도메인을 사용하여 프로비저닝됩니다.



1. 기본 볼륨 구성 섹션에서 볼륨 이름과 크기를 지정합니다. 이것은 NFS 볼륨입니다. 저장소 효율성의 경우 ONTAP 저장소 효율성 기능(압축, 중복 제거, 압축)을 켜려면 '활성화'를 선택하고, 끄려면 '비활성화'를 선택합니다.



1. 파일 시스템 생성 페이지에 표시된 파일 시스템 구성을 검토합니다.
2. 파일 시스템 만들기를 클릭합니다.



더 자세한 정보는 다음을 참조하세요."Amazon FSx ONTAP 시작하기" .

위와 같이 파일 시스템을 생성한 후, 필요한 크기와 프로토콜로 볼륨을 생성합니다.

1. 열기"Amazon FSx 콘솔" .
2. 왼쪽 탐색 창에서 파일 시스템을 선택한 다음 볼륨을 만들려는 ONTAP 파일 시스템을 선택합니다.
3. 볼륨 탭을 선택합니다.
4. 볼륨 생성 탭을 선택합니다.
5. 볼륨 생성 대화 상자가 나타납니다.

데모 목적으로 AWS의 VMware 클라우드에서 실행되는 VM에 쉽게 마운트할 수 있는 NFS 볼륨이 이 섹션에 생성됩니다. nfsdemovol01은 아래와 같이 생성됩니다.



▼ **Linux** 클라이언트에서 **FSx ONTAP** 볼륨 마운트

AWS SDDC의 VMC 내 Linux VM에서 이전 단계에서 만든 FSx ONTAP 볼륨을 마운트하려면 다음 단계를 완료하세요.

1. 지정된 Linux 인스턴스에 연결합니다.
2. SSH(Secure Shell)를 사용하여 인스턴스에서 터미널을 열고 적절한 자격 증명으로 로그인합니다.
3. 다음 명령을 사용하여 볼륨의 마운트 지점에 대한 디렉토리를 만듭니다.

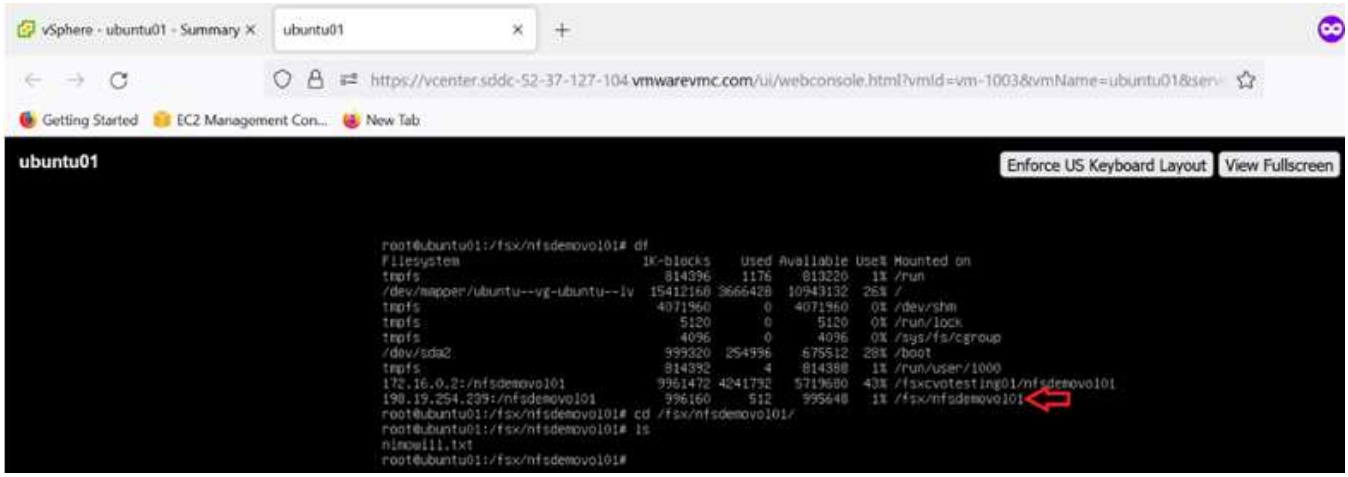
```
$ sudo mkdir /fsx/nfsdemovol01
```

. 이전 단계에서 생성한 디렉토리에 Amazon FSx ONTAP NFS 볼륨을 마운트합니다.

```
sudo mount -t nfs nfsvers=4.1,198.19.254.239:/nfsdemovol01
/fsx/nfsdemovol01
```

```
root@ubuntu01:/fsx/nfsdemovol01# mount -t nfs 198.19.254.239:/nfsdemovol01 /fsx/nfsdemovol01
```

1. 실행 후 df 명령을 실행하여 마운트를 검증합니다.



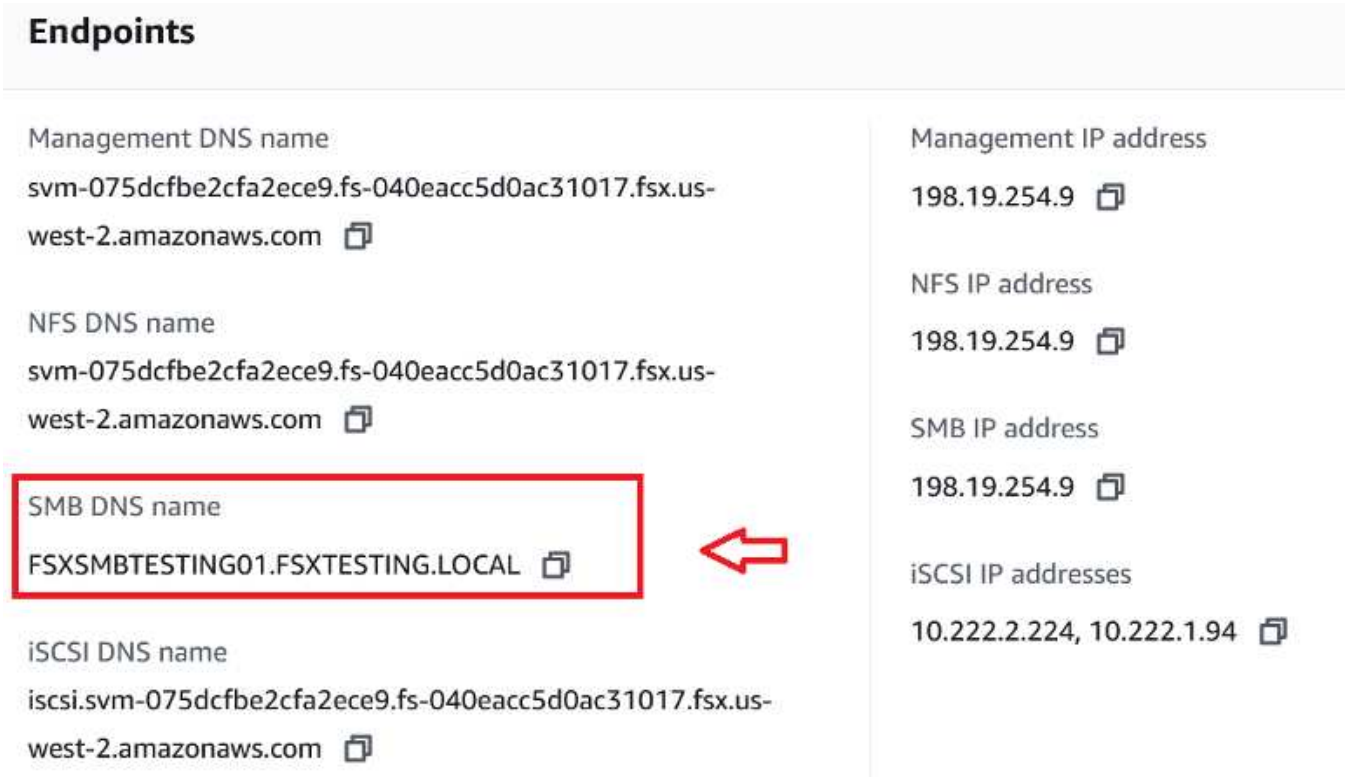
Linux 클라이언트에서 FSx ONTAP 볼륨 마운트

▼ **Microsoft Windows** 클라이언트에 **FSx ONTAP** 볼륨 연결

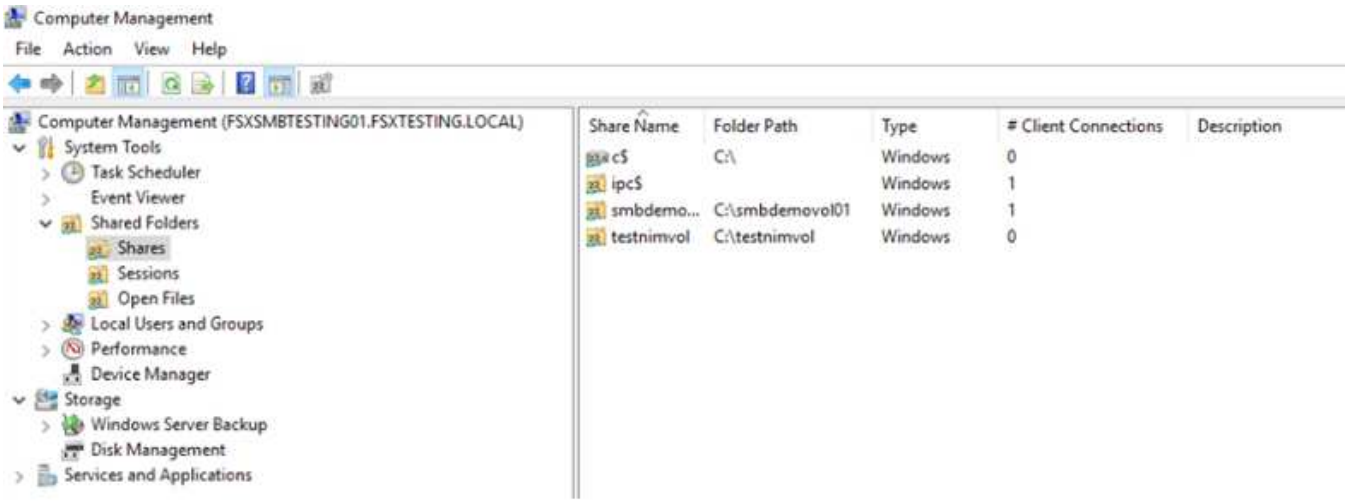
Amazon FSx 파일 시스템에서 파일 공유를 관리하고 매핑하려면 공유 폴더 GUI를 사용해야 합니다.

1. 시작 메뉴를 열고 관리자 권한으로 실행하여 fsmgmt.msc를 실행합니다. 이렇게 하면 공유 폴더 GUI 도구가 열립니다.
2. 작업 > 모든 작업을 클릭하고 다른 컴퓨터에 연결을 선택합니다.
3. 다른 컴퓨터의 경우 스토리지 가상 머신(SVM)의 DNS 이름을 입력합니다. 예를 들어, 이 예에서는 FSXSMBTESTING01.FSXTESTING.LOCAL이 사용됩니다.

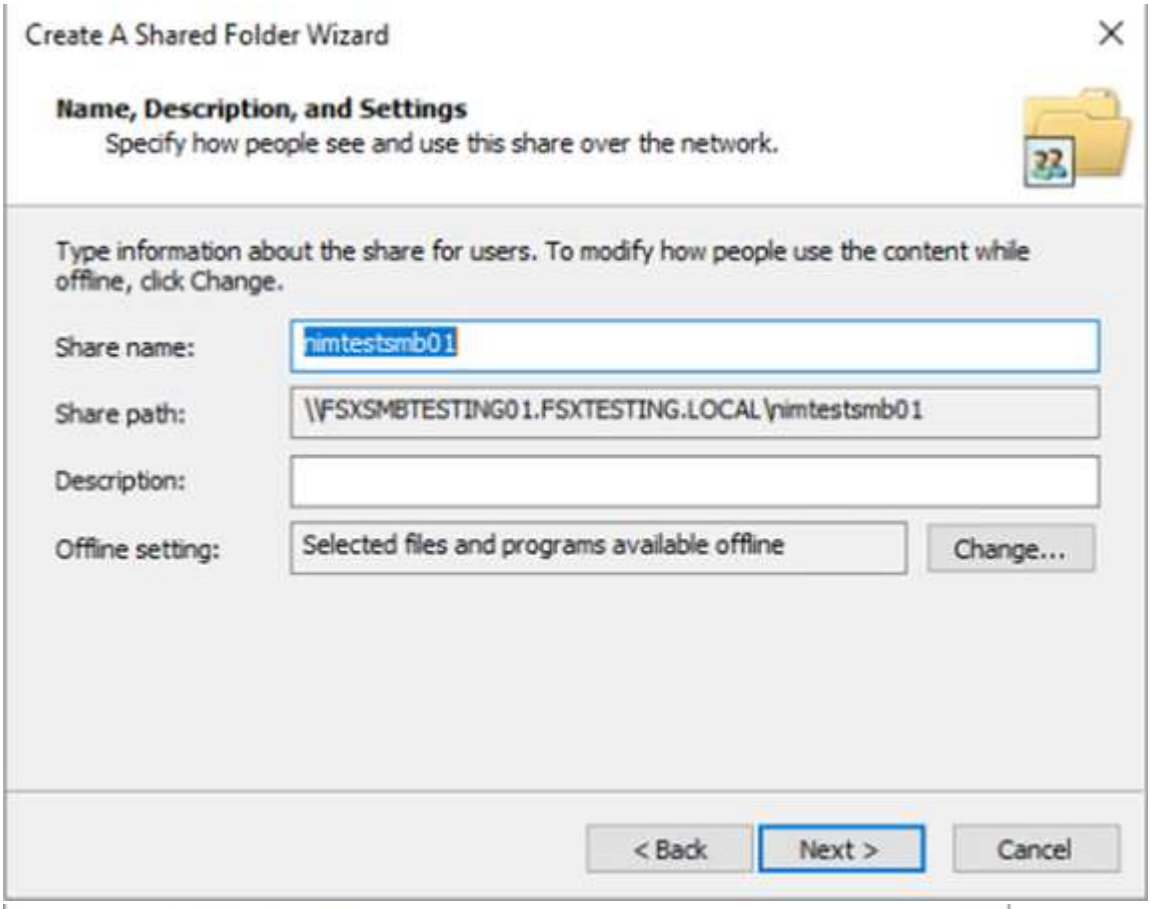
Amazon FSx 콘솔에서 SVM의 DNS 이름을 찾으려면 스토리지 가상 머신을 선택하고 SVM을 선택한 다음 아래로 스크롤하여 엔드포인트로 가서 SMB DNS 이름을 찾으세요. OK를 클릭합니다. 공유 폴더 목록에 Amazon FSx 파일 시스템이 나타납니다.



1. 공유 폴더 도구에서 왼쪽 창에 있는 공유를 선택하면 Amazon FSx 파일 시스템에 대한 활성 공유를 확인할 수 있습니다.



1. 이제 새로운 공유를 선택하고 공유 폴더 만들기 마법사를 완료하세요.

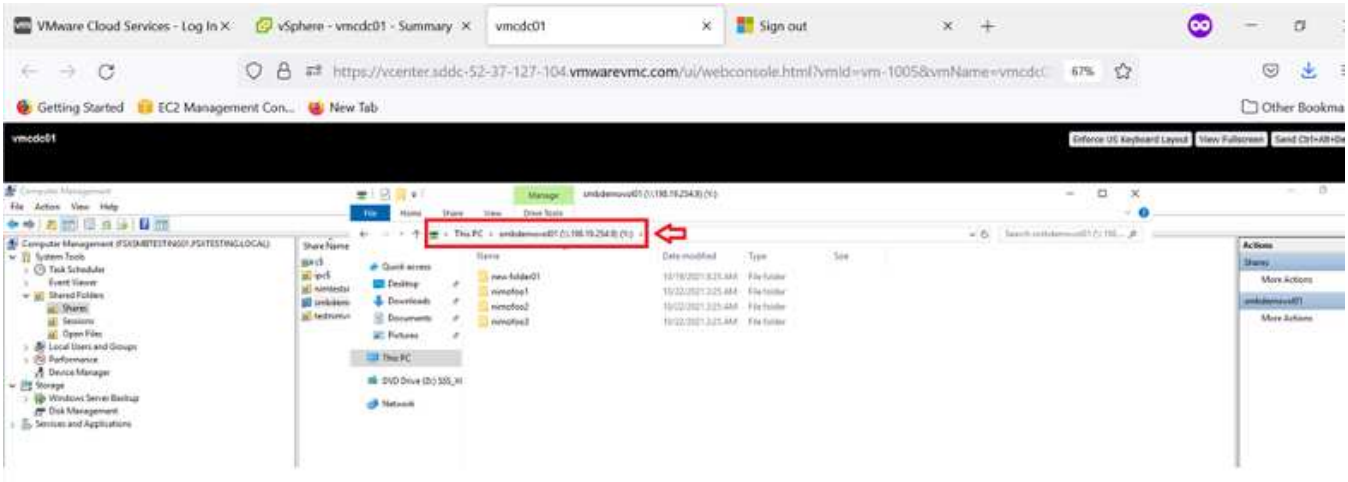




Amazon FSx 파일 시스템에서 SMB 공유를 생성하고 관리하는 방법에 대해 자세히 알아보려면 다음을 참조하세요 ."SMB 공유 생성" .

1. 연결이 설정되면 SMB 공유를 연결하여 애플리케이션 데이터에 사용할 수 있습니다. 이를 달성하려면 공유

경로를 복사하고 네트워크 드라이브 매핑 옵션을 사용하여 AWS SDDC의 VMware Cloud에서 실행되는 VM에 볼륨을 마운트합니다.



▼ **iSCSI**를 사용하여 **FSx ONTAP LUN**을 호스트에 연결합니다.

iSCSI를 사용하여 FSx ONTAP LUN을 호스트에 연결합니다.

FSx의 iSCSI 트래픽은 이전 섹션에서 제공된 경로를 통해 VMware Transit Connect/AWS Transit Gateway를 통과합니다. Amazon FSx ONTAP 에서 LUN을 구성하려면 다음 설명서를 따르세요."여기" .

Linux 클라이언트에서는 iSCSI 데몬이 실행 중인지 확인하세요. LUN이 프로비저닝된 후 Ubuntu를 사용한 iSCSI 구성에 대한 자세한 지침을 참조하세요(예시)."여기" .

이 논문에서는 iSCSI LUN을 Windows 호스트에 연결하는 방법을 설명합니다.

▼ **FSx ONTAP** 에서 **LUN** 프로비저닝:

1. ONTAP 파일 시스템용 FSx의 관리 포트를 사용하여 NetApp ONTAP CLI에 액세스합니다.
2. 크기 조정 출력에 표시된 대로 필요한 크기로 LUN을 만듭니다.

```
FsxId040eacc5d0ac31017::> lun create -vserver vmcfsxval2svm -volume
nimfsxscsivol -lun nimofsxlun01 -size 5gb -ostype windows -space
-reserve enabled
```

이 예에서는 크기가 5g(5368709120)인 LUN을 생성했습니다.

1. 특정 LUN에 액세스할 수 있는 호스트를 제어하기 위해 필요한 igroup을 만듭니다.

```
FsxId040eacc5d0ac31017::> igroup create -vserver vmcfsxval2svm -igroup
winIG -protocol iscsi -ostype windows -initiator iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local

FsxId040eacc5d0ac31017::> igroup show

Vserver   Igroup       Protocol OS Type  Initiators
```

```
--------- ------------ -------- --------
-----------------------------------

vmcfsxval2svm

          ubuntu01     iscsi    linux    iqn.2021-
10.com.ubuntu:01:initiator01

vmcfsxval2svm

          winIG        iscsi    windows  iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local
```

두 개의 항목이 표시되었습니다.

1. 다음 명령을 사용하여 LUN을 igroup에 매핑합니다.

```
FsxId040eacc5d0ac31017::> lun map -vserver vmcfsxval2svm -path
/vol/nimfsxscsivol/nimofsxlun01 -igroup winIG

FsxId040eacc5d0ac31017::> lun show

Vserver   Path                            State   Mapped   Type
Size

--------- ------------------------------ ------- -------- --------
--------

vmcfsxval2svm

          /vol/blocktest01/lun01          online  mapped   linux
5GB

vmcfsxval2svm

          /vol/nimfsxscsivol/nimofsxlun01 online  mapped   windows
5GB
```

두 개의 항목이 표시되었습니다.

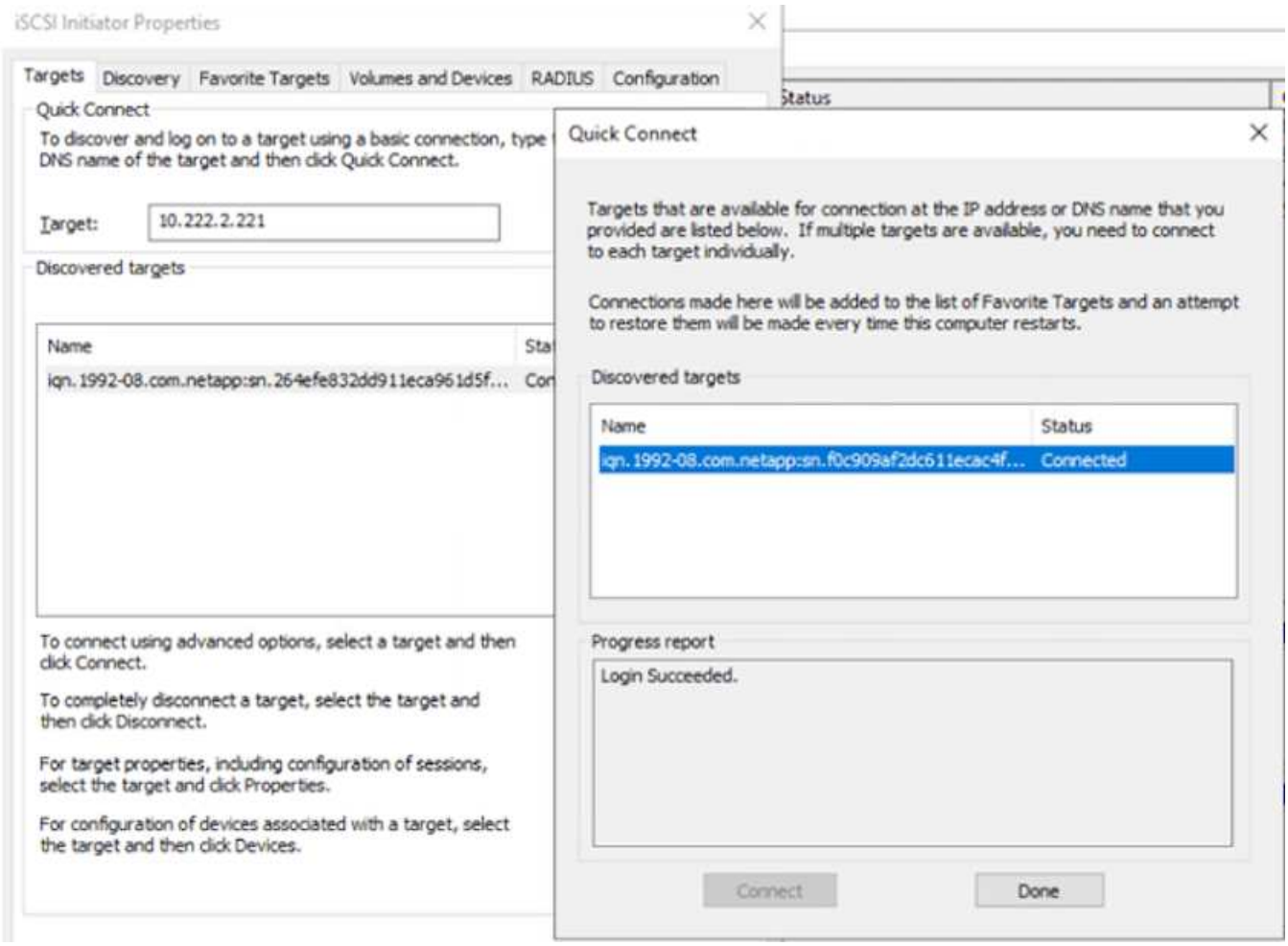
1. 새로 프로비저닝된 LUN을 Windows VM에 연결합니다.

AWS SDDC의 VMware 클라우드에 있는 Windows 호스트에 새 LUN을 연결하려면 다음 단계를 완료하세요.

1. AWS SDDC의 VMware Cloud에 호스팅된 Windows VM에 대한 RDP.

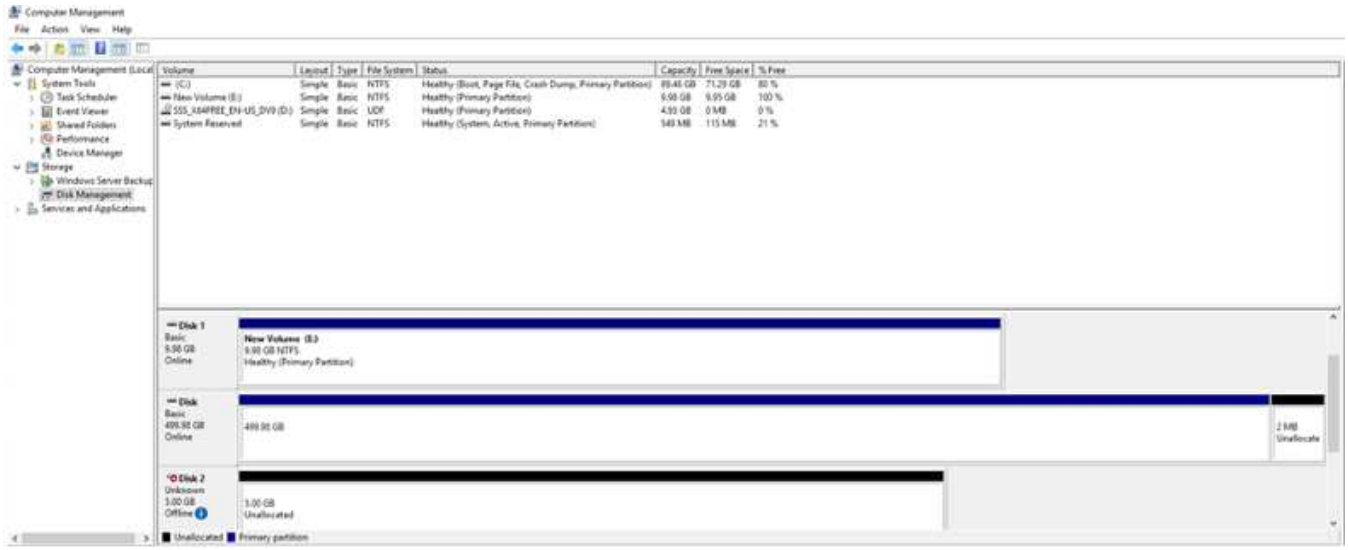
2. 서버 관리자 > 대시보드 > 도구 > iSCSI 초기자로 이동하여 iSCSI 초기자 속성 대화 상자를 엽니다.
3. 검색 탭에서 포털 검색 또는 포털 추가를 클릭한 다음 iSCSI 대상 포트의 IP 주소를 입력합니다.
4. 대상 탭에서 검색된 대상을 선택한 다음 로그온 또는 연결을 클릭합니다.
5. 다중 경로 사용을 선택한 다음 "컴퓨터가 시작될 때 이 연결을 자동으로 복원" 또는 "즐겨찾는 대상 목록에 이 연결 추가"를 선택합니다. 고급을 클릭합니다.

Windows 호스트는 클러스터의 각 노드에 iSCSI 연결이 있어야 합니다. 기본 DSM은 사용할 가장 좋은 경로를 선택합니다.



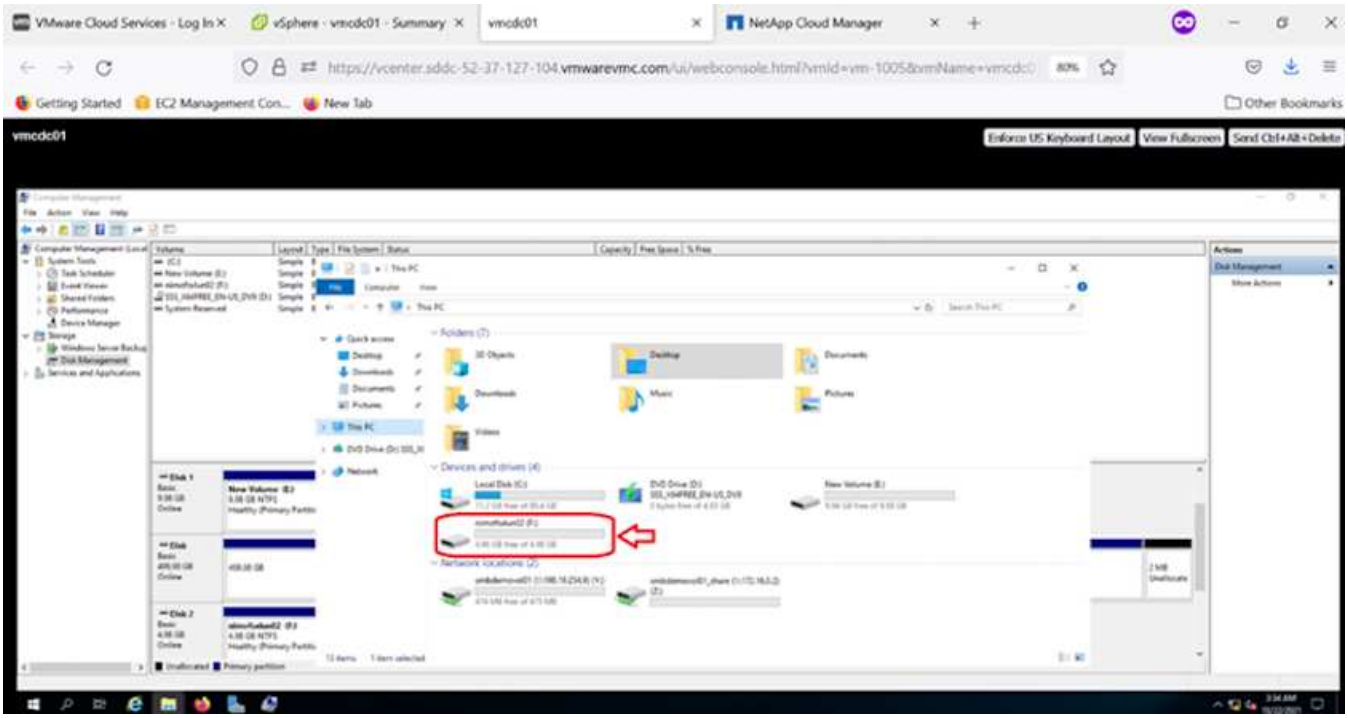
스토리지 가상 머신(SVM)의 LUN은 Windows 호스트에 디스크로 표시됩니다. 새로 추가된 디스크는 호스트에서 자동으로 검색되지 않습니다. 다음 단계를 완료하여 디스크를 검색하기 위한 수동 재검사를 트리거합니다.

1. Windows 컴퓨터 관리 유틸리티를 엽니다: 시작 > 관리 도구 > 컴퓨터 관리.
2. 탐색 트리에서 저장소 노드를 확장합니다.
3. 디스크 관리를 클릭합니다.
4. 작업 > 디스크 다시 검사를 클릭합니다.



Windows 호스트가 새 LUN에 처음 액세스할 때 파티션이나 파일 시스템이 없습니다. 다음 단계를 완료하여 LUN을 초기화하고, 필요한 경우 LUN을 파일 시스템으로 포맷합니다.

1. Windows 디스크 관리를 시작합니다.
2. LUN을 마우스 오른쪽 버튼으로 클릭한 다음 필요한 디스크 또는 파티션 유형을 선택합니다.
3. 마법사의 지시를 따르세요. 이 예에서는 드라이브 F:가 마운트되었습니다.



Cloud Volumes ONTAP (CVO)

클라우드 볼륨 ONTAP 또는 CVO는 NetApp의 ONTAP 스토리지 소프트웨어를 기반으로 구축된 업계 최고의 클라우드 데이터 관리 솔루션으로, Amazon Web Services(AWS), Microsoft Azure 및 Google Cloud Platform(GCP)에서 기본적으로 제공됩니다.

ONTAP 은 클라우드 기반 스토리지를 사용하는 소프트웨어 정의 버전으로, 클라우드와 온프레미스에서 동일한

스토리지 소프트웨어를 사용할 수 있어 데이터를 관리하는 완전히 새로운 방법에 대한 IT 직원의 재교육 필요성이 줄어듭니다.

CVO를 사용하면 고객은 엣지에서 데이터 센터, 클라우드로 원활하게 데이터를 이동할 수 있으며, 하이브리드 클라우드를 하나로 통합할 수 있습니다. 이 모든 기능은 단일 창 관리 콘솔인 NetApp Cloud Manager를 통해 관리할 수 있습니다.

CVO는 설계상 클라우드에서 가장 까다로운 애플리케이션도 만족시킬 수 있는 극한의 성능과 고급 데이터 관리 기능을 제공합니다.

게스트 연결 스토리지로서의 **Cloud Volumes ONTAP (CVO)**

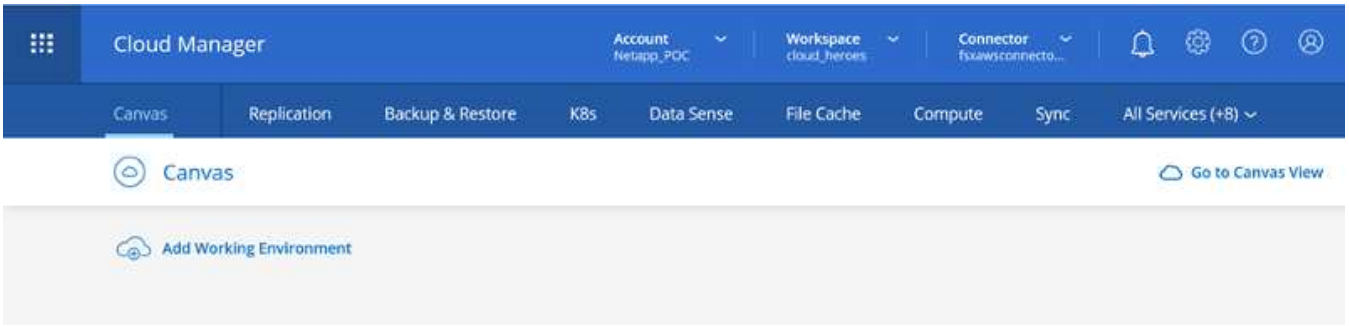
▼ **AWS**에 새로운 **Cloud Volumes ONTAP** 인스턴스 배포(직접 해보기)

Cloud Volumes ONTAP 공유 및 LUN은 AWS SDDC 환경에서 VMware Cloud에서 생성된 VM에서 마운트할 수 있습니다. 볼륨은 기본 AWS VM Linux Windows 클라이언트에도 마운트할 수 있으며, iSCSI를 통해 마운트하면 Cloud Volumes ONTAP iSCSI, SMB 및 NFS 프로토콜을 지원하므로 LUN은 Linux 또는 Windows 클라이언트에서 블록 장치로 액세스할 수 있습니다. Cloud Volumes ONTAP 볼륨은 몇 가지 간단한 단계로 설정할 수 있습니다.

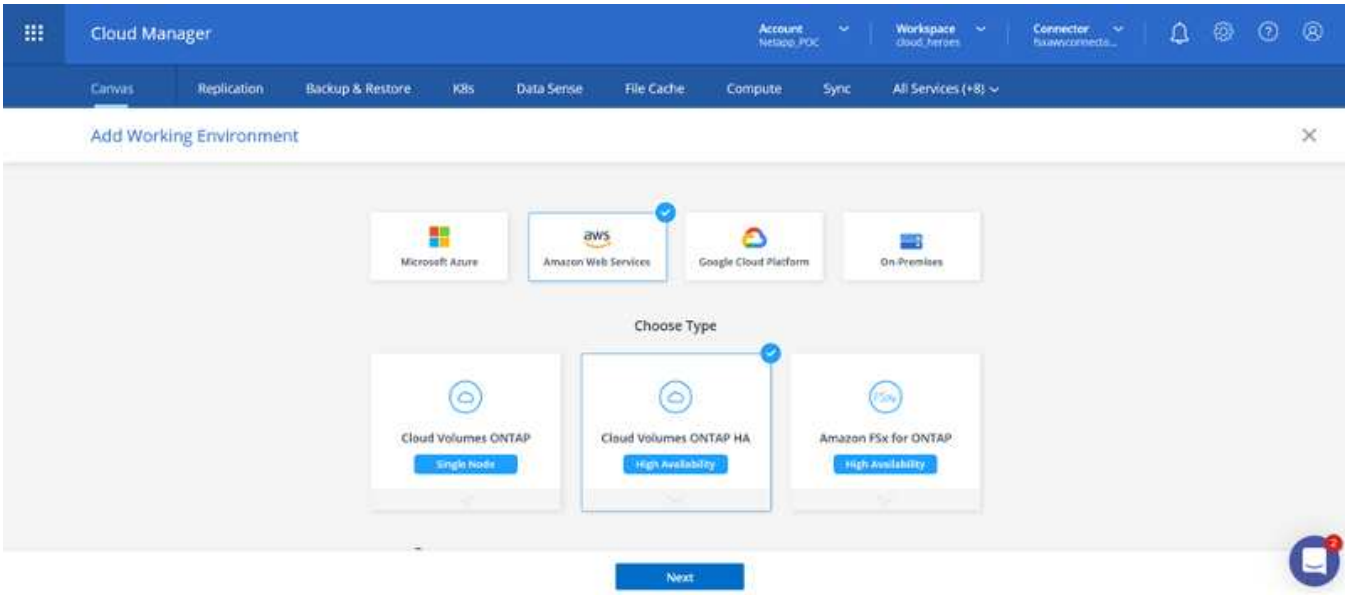
재해 복구나 마이그레이션 목적으로 온프레미스 환경에서 클라우드로 볼륨을 복제하려면 사이트 간 VPN이나 DirectConnect를 사용하여 AWS에 대한 네트워크 연결을 설정합니다. 온프레미스에서 Cloud Volumes ONTAP으로 데이터를 복제하는 내용은 이 문서의 범위를 벗어납니다. 온프레미스와 Cloud Volumes ONTAP 시스템 간에 데이터를 복제하려면 다음을 참조하세요."시스템 간 데이터 복제 설정" .

> "Cloud Volumes ONTAP 사이저"을(를) 사용하여 Cloud Volumes ONTAP 인스턴스의 크기를 정확하게 조정하십시오. 또한 온프레미스 성능을 모니터링하여 Cloud Volumes ONTAP 크기 조정 도구의 입력값으로 활용하십시오.

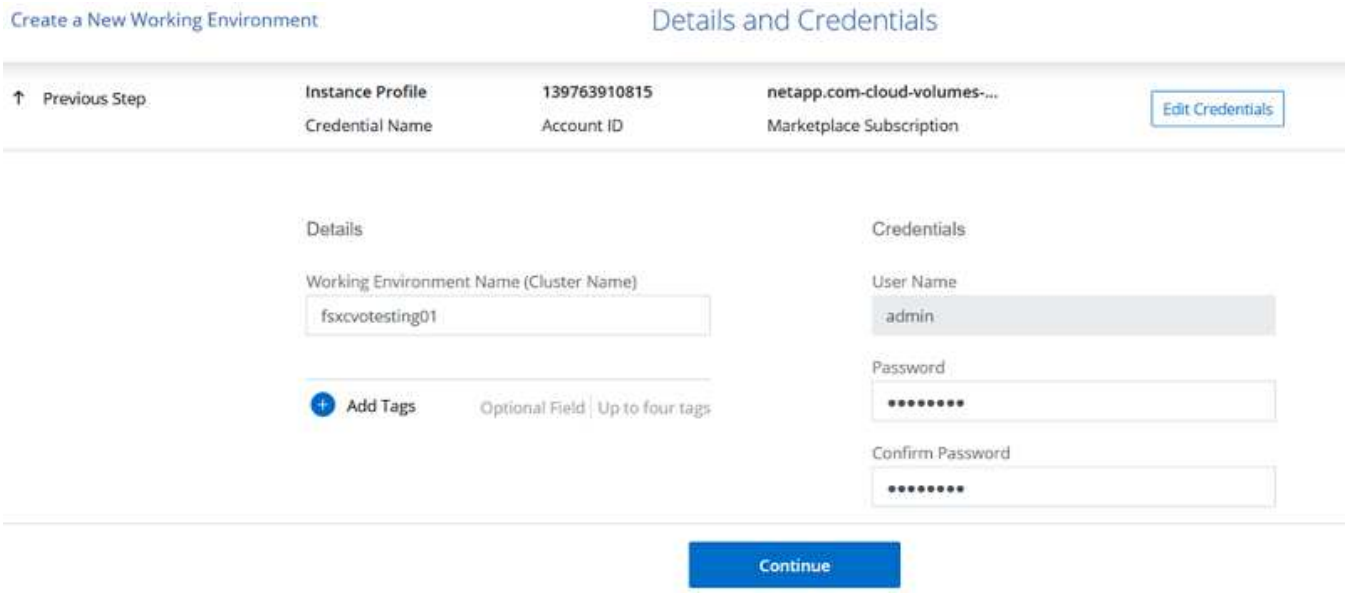
1. NetApp Cloud Central에 로그인하면 Fabric View 화면이 표시됩니다. Cloud Volumes ONTAP 탭을 찾아 Cloud Manager로 이동을 선택합니다. 로그인 후 Canvas 화면이 표시됩니다.



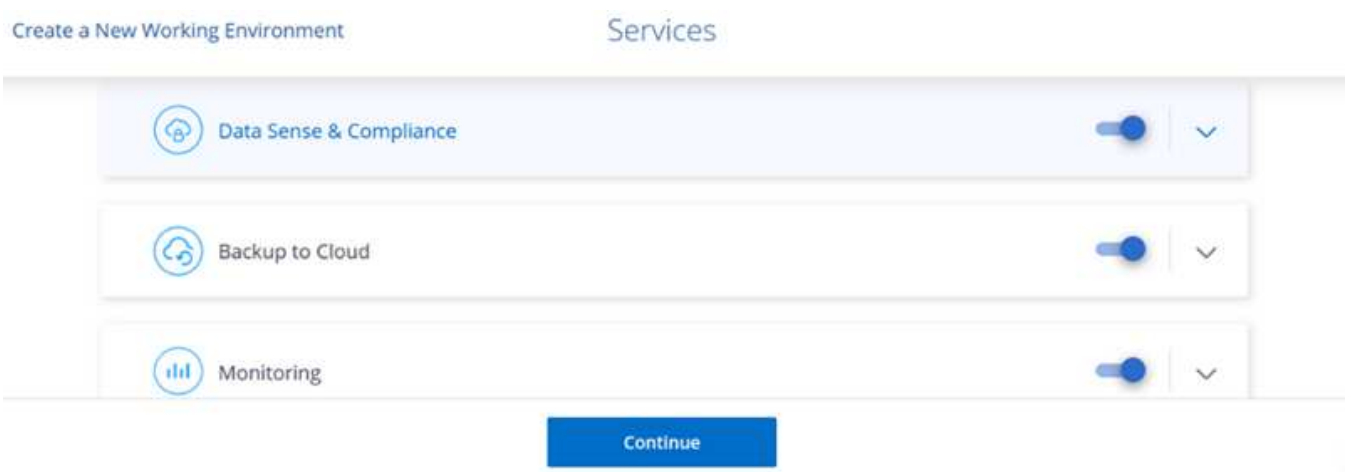
1. 클라우드 관리자 홈페이지에서 작업 환경 추가를 클릭한 다음 클라우드로 AWS를 선택하고 시스템 구성 유형을 선택합니다.



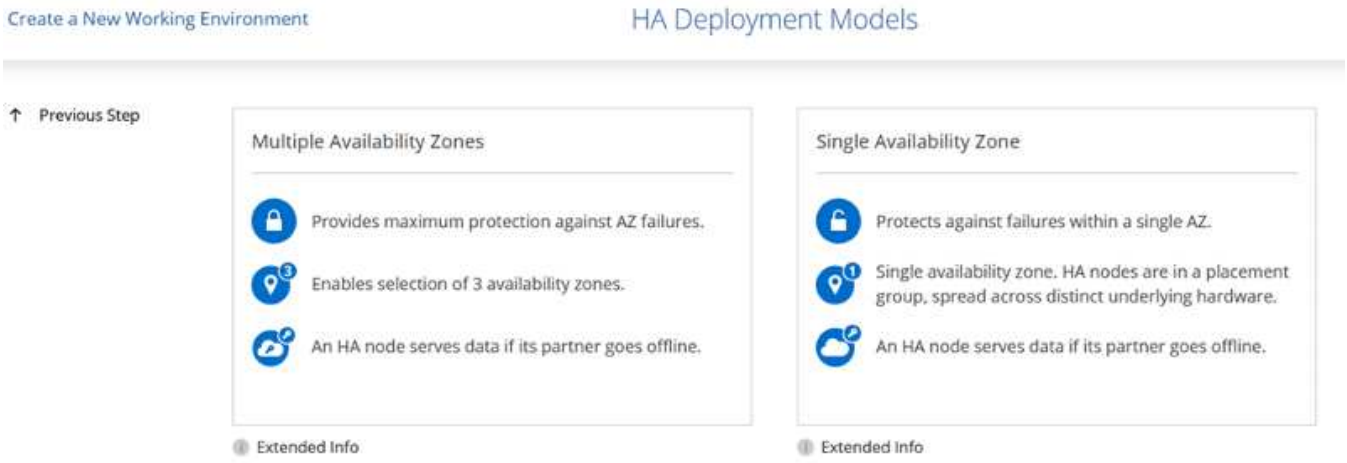
1. 환경 이름과 관리자 자격 증명을 포함하여 생성할 환경에 대한 세부 정보를 제공합니다. 계속을 클릭하세요.



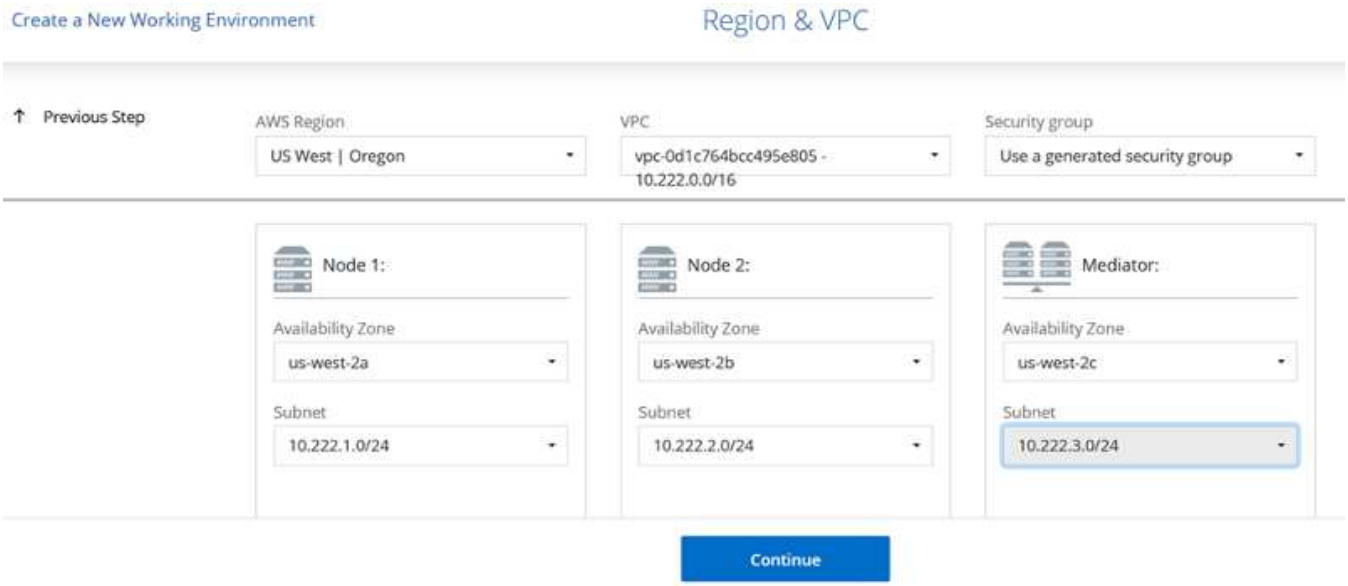
1. NetApp Data Classification, NetApp Backup and Recovery 및 Data Infrastructure Insights를 포함하여 Cloud Volumes ONTAP 배포를 위한 추가 서비스를 선택합니다. 계속을 클릭합니다.



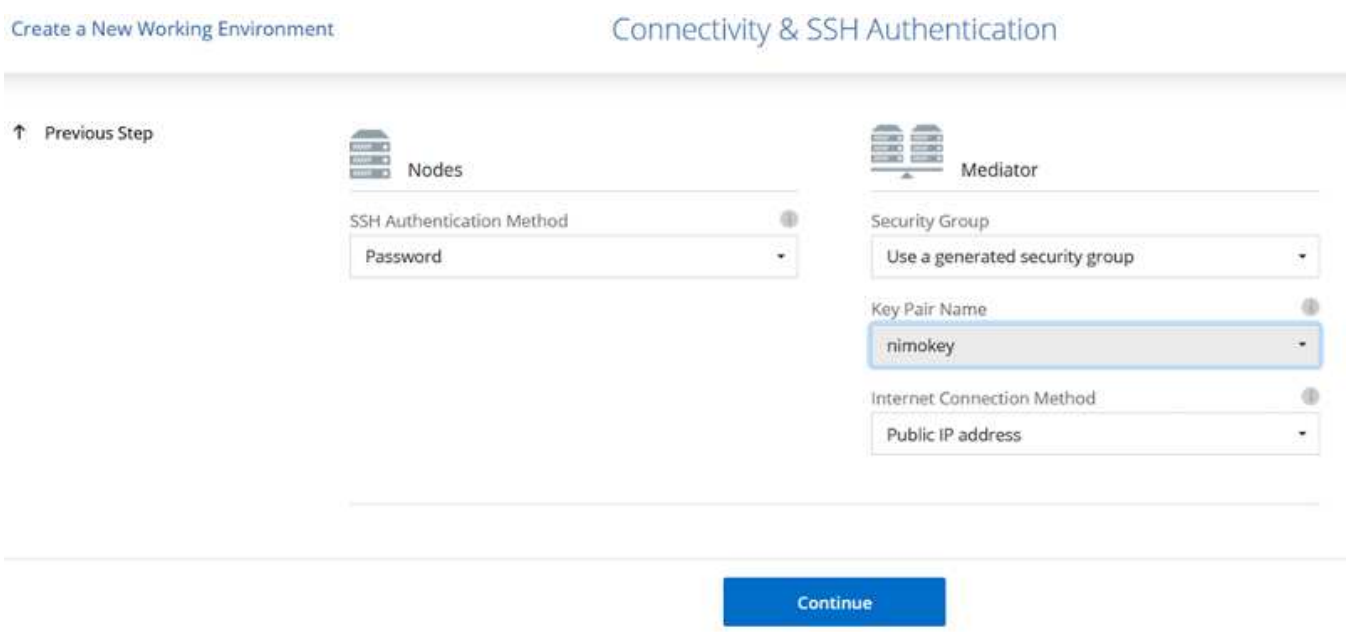
1. HA 배포 모델 페이지에서 다중 가용성 영역 구성을 선택합니다.



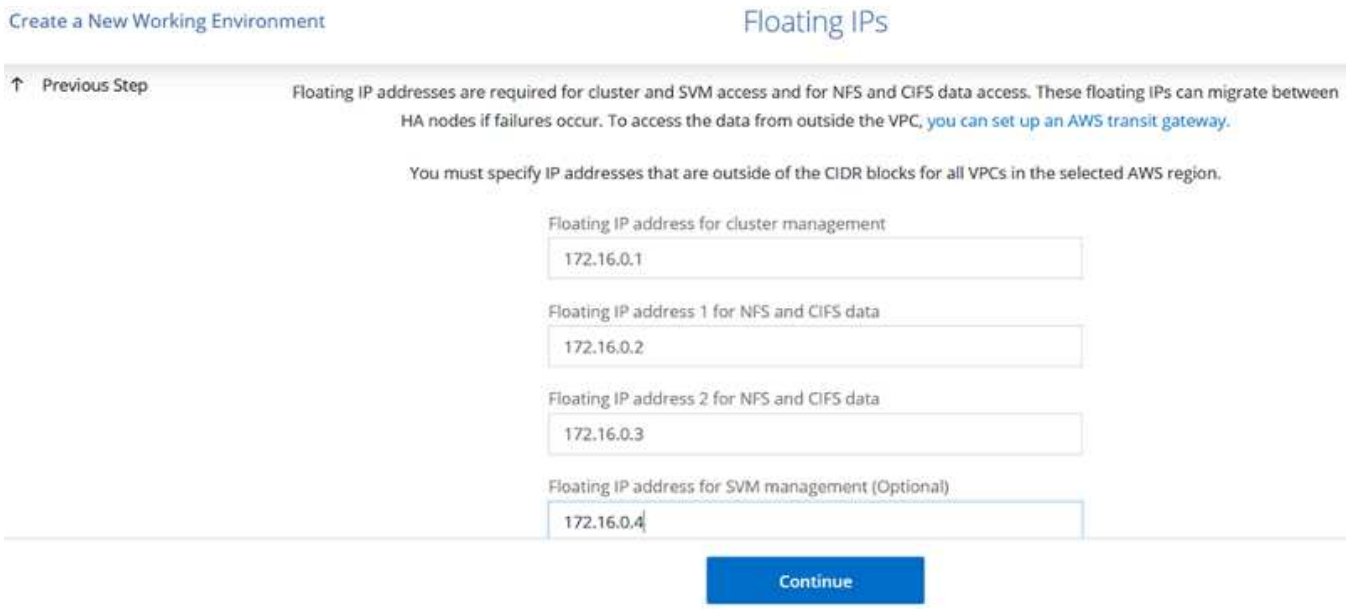
1. 지역 및 VPC 페이지에서 네트워크 정보를 입력한 다음 계속을 클릭합니다.



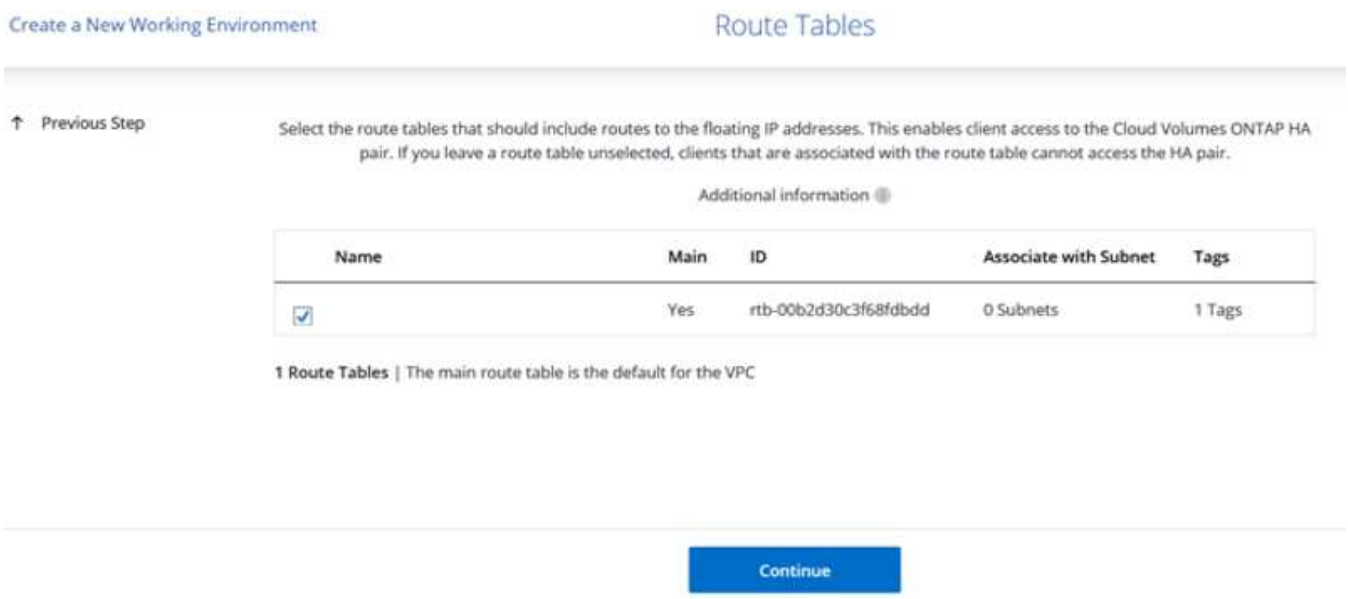
1. 연결 및 SSH 인증 페이지에서 HA 쌍과 중재자에 대한 연결 방법을 선택합니다.



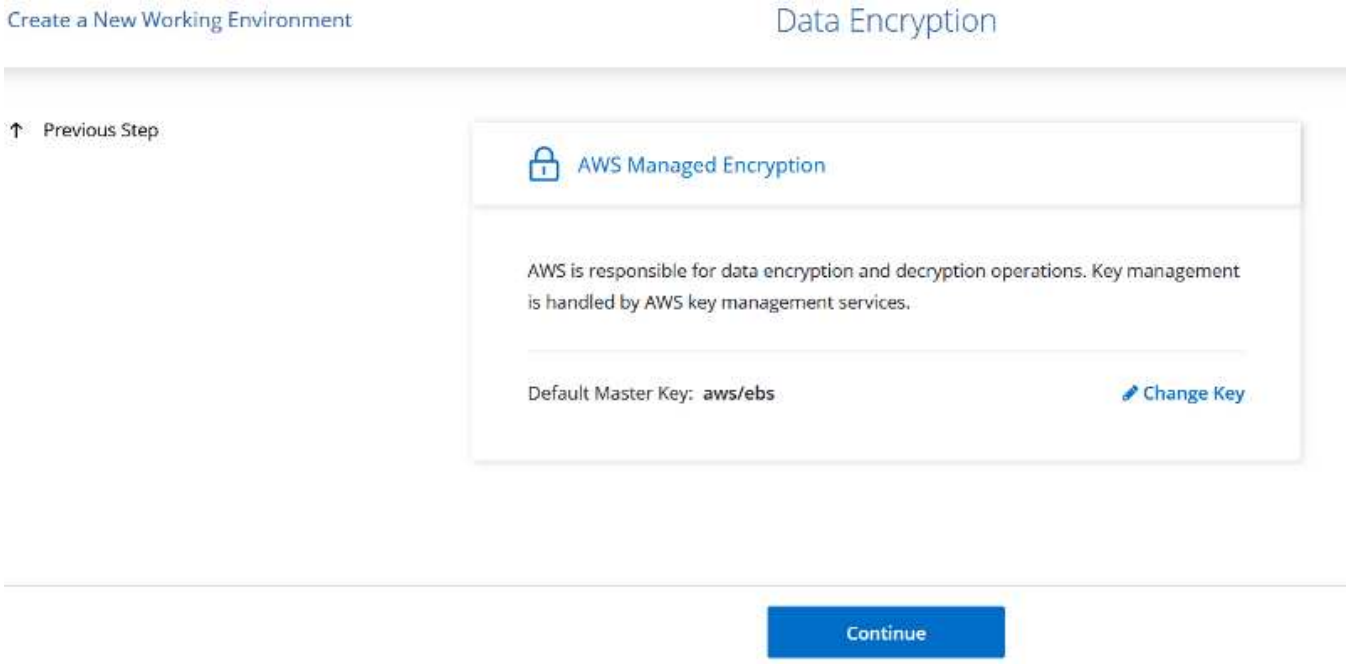
1. 유동 IP 주소를 지정한 후 계속을 클릭합니다.



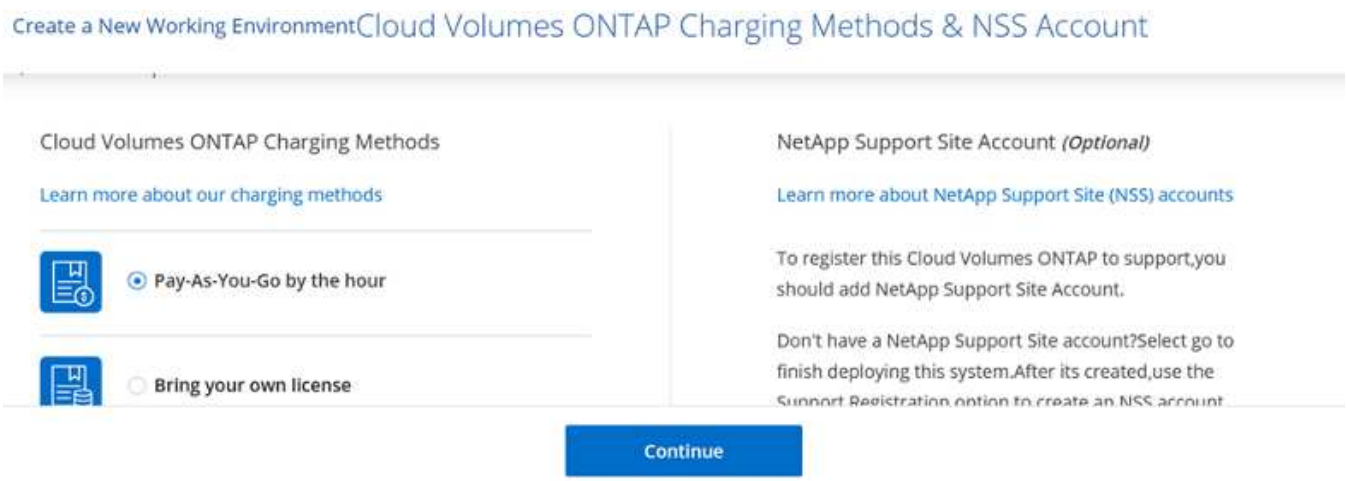
1. 플로팅 IP 주소에 대한 경로를 포함하려면 적절한 경로 테이블을 선택한 다음 계속을 클릭합니다.



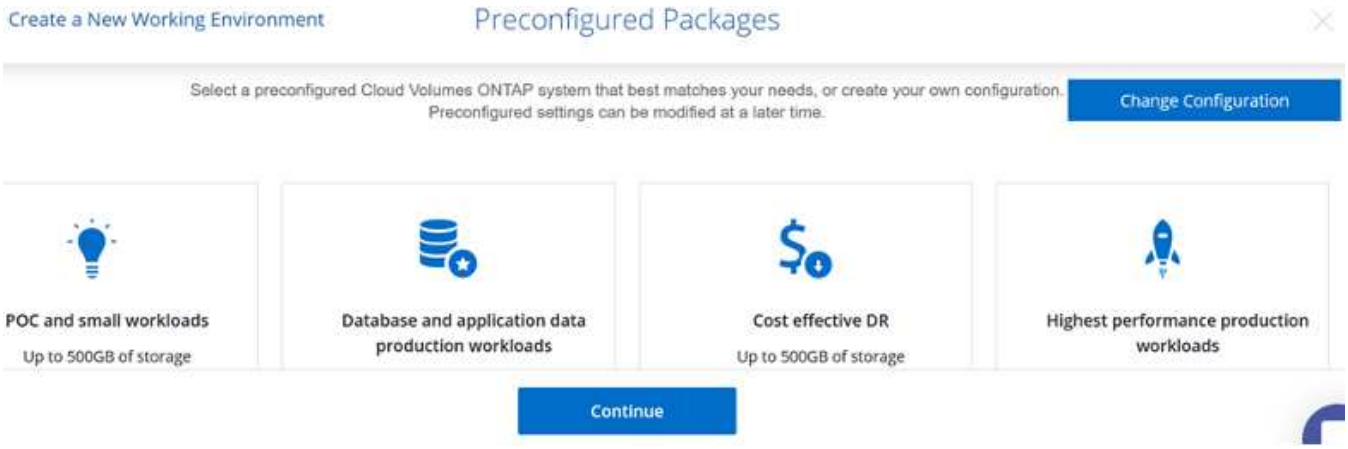
1. 데이터 암호화 페이지에서 AWS 관리 암호화를 선택합니다.



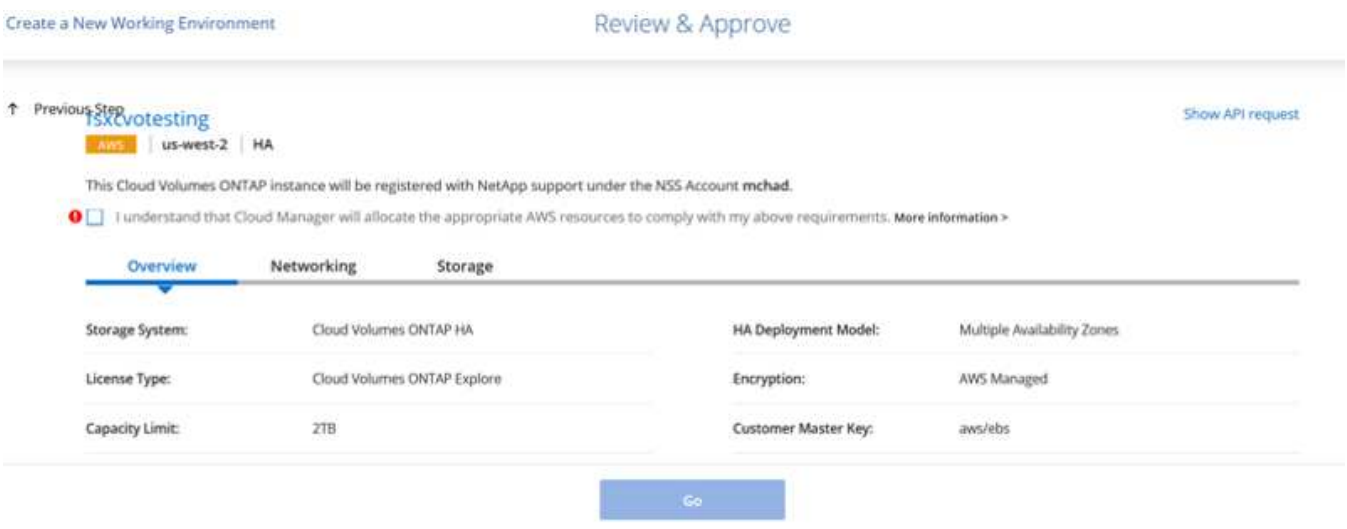
1. 라이선스 옵션을 선택하세요: Pay-As-You-Go 또는 기존 라이선스를 사용하는 BYOL. 이 예에서는 Pay-As-You-Go 옵션이 사용되었습니다.



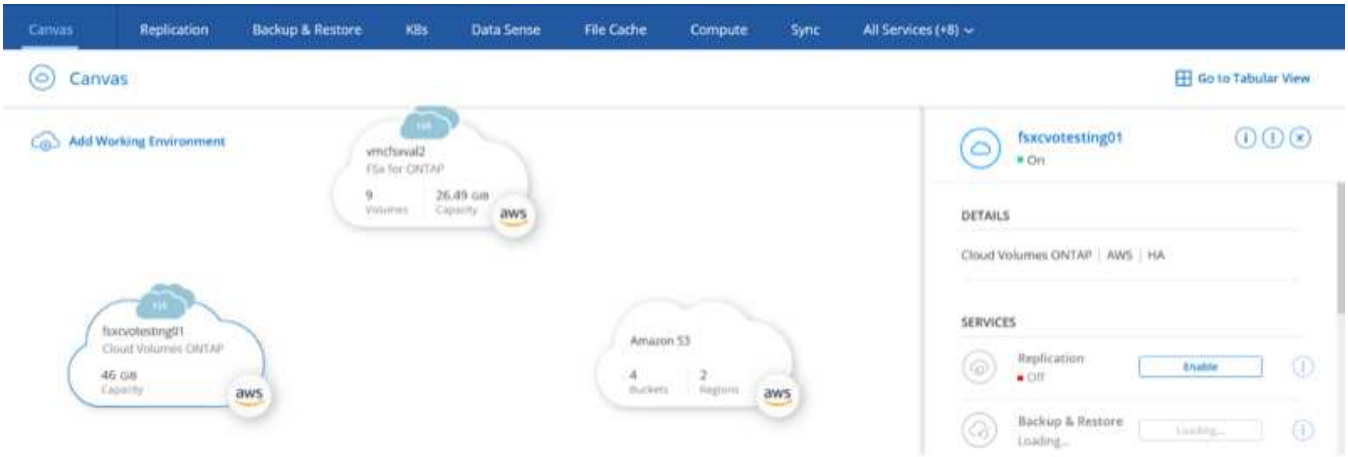
1. AWS SDDC에서 VMware 클라우드를 실행하는 VM에 배포할 워크로드 유형에 따라 미리 구성된 여러 패키지 중에서 선택하세요.



1. 검토 및 승인 페이지에서 선택 사항을 검토하고 확인합니다 . Cloud Volumes ONTAP 인스턴스를 생성하려면 이동을 클릭합니다.

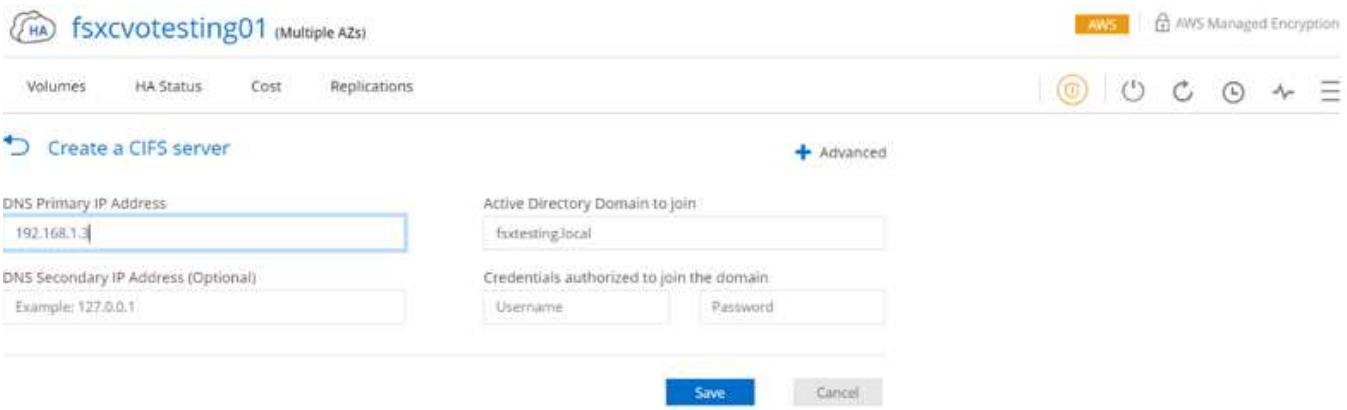


1. Cloud Volumes ONTAP 이 프로비저닝되면 Canvas 페이지의 작업 환경에 나열됩니다.

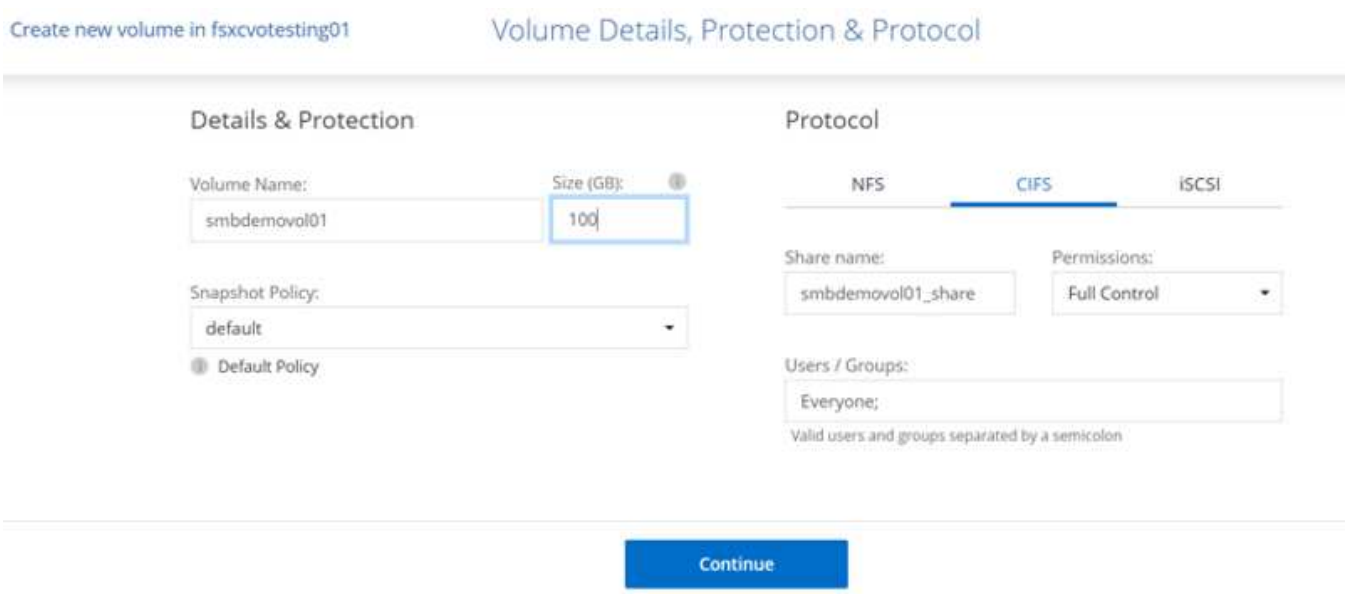


▼ **SMB** 볼륨에 대한 추가 구성

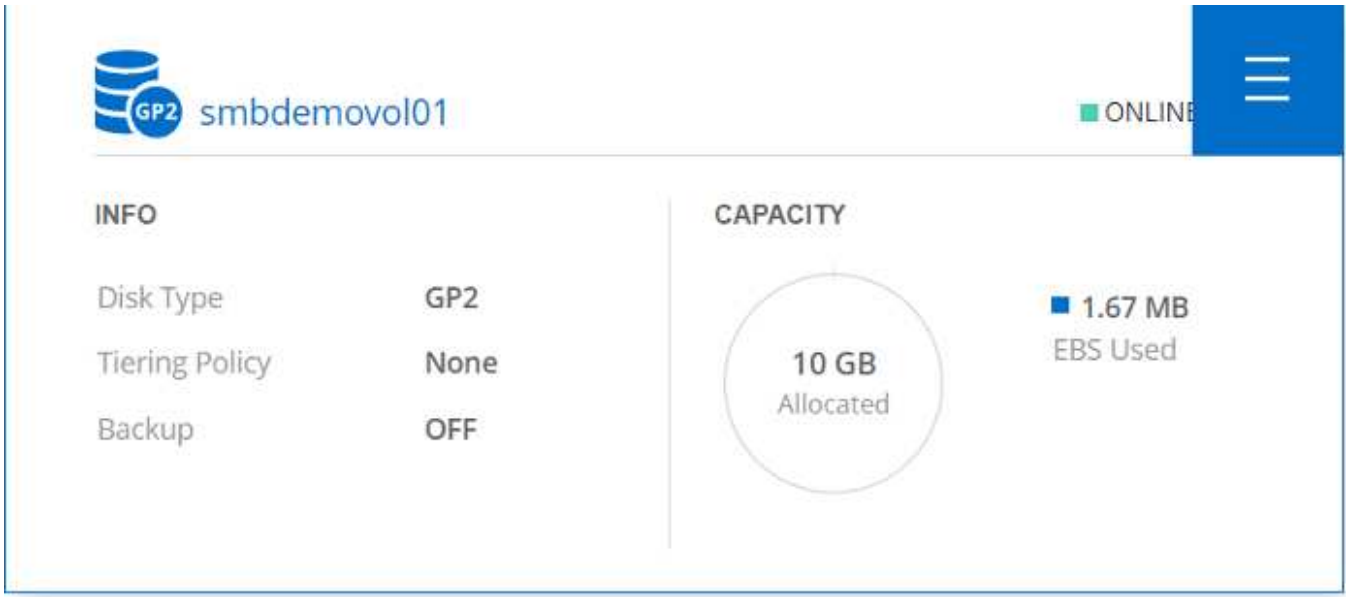
1. 작업 환경이 준비되면 CIFS 서버가 적절한 DNS 및 Active Directory 구성 매개변수로 구성되었는지 확인하세요. SMB 볼륨을 생성하려면 이 단계가 필요합니다.



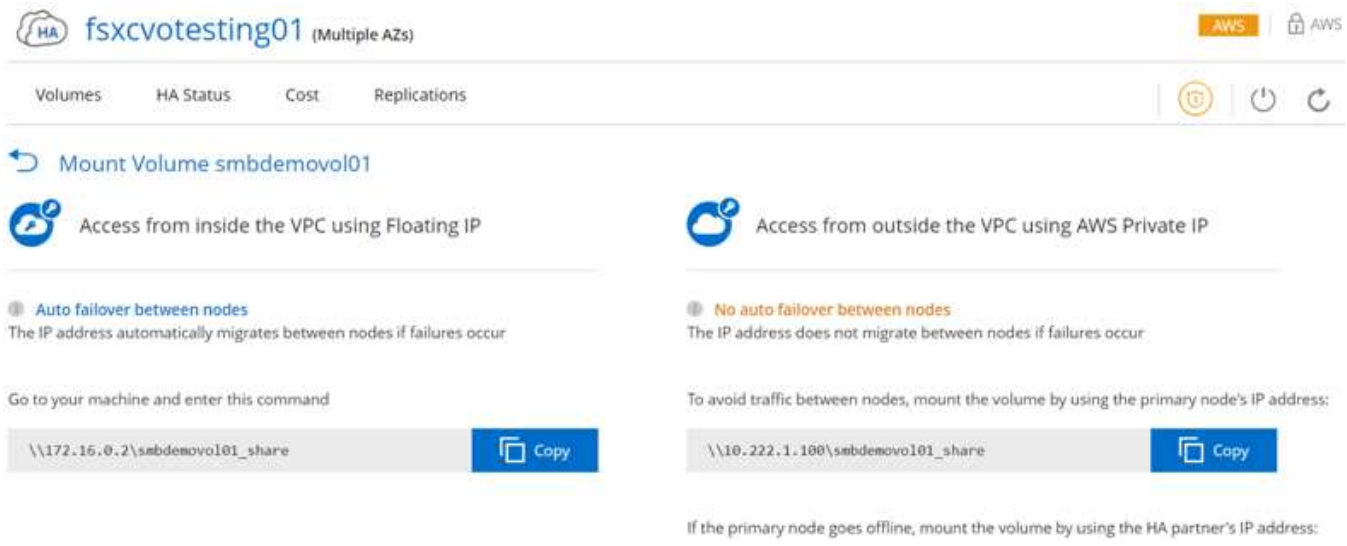
1. 볼륨을 생성할 CVO 인스턴스를 선택하고 볼륨 생성 옵션을 클릭합니다. 적절한 크기를 선택하면 클라우드 관리자가 포함된 집계를 선택하거나 고급 할당 메커니즘을 사용하여 특정 집계에 배치합니다. 이 데모에서는 프로토콜로 SMB가 선택되었습니다.

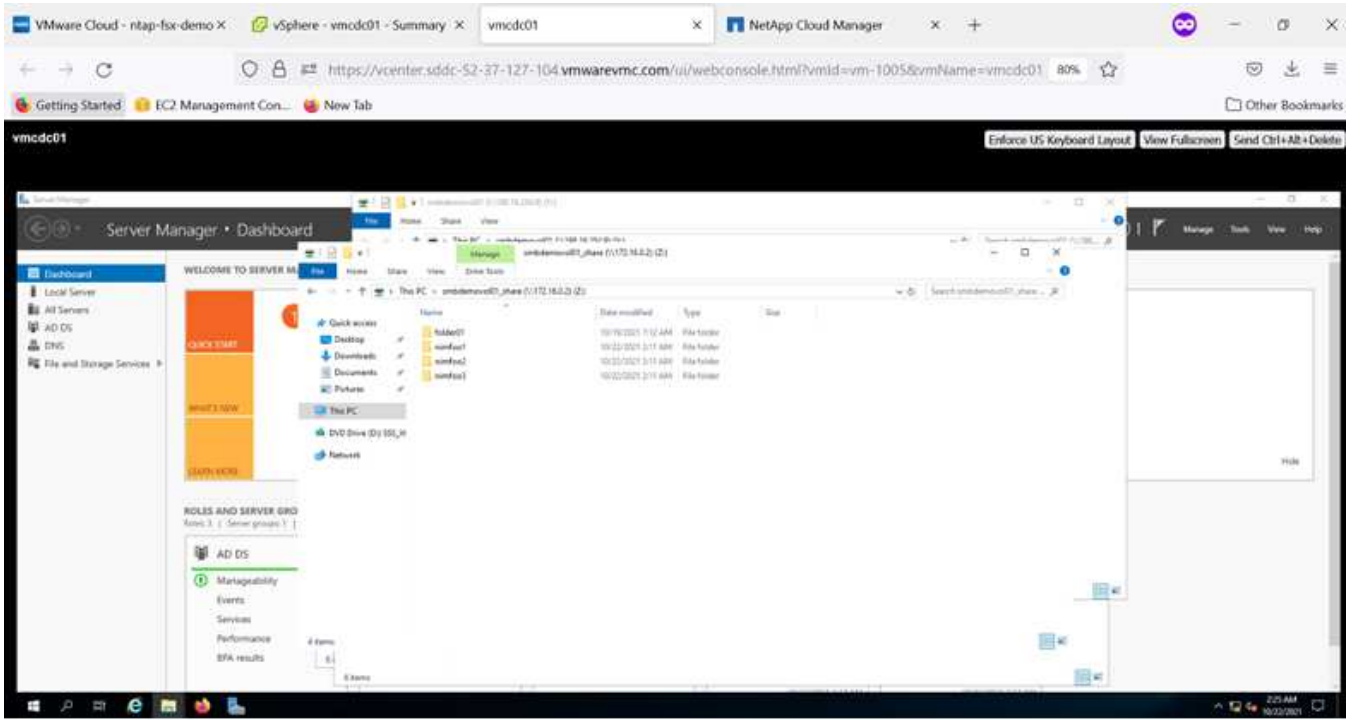


1. 볼륨이 프로비저닝된 후에는 볼륨 창에서 사용할 수 있습니다. CIFS 공유는 프로비저닝되므로 사용자나 그룹에 파일과 폴더에 대한 권한을 부여하고 해당 사용자가 공유에 액세스하여 파일을 만들 수 있는지 확인해야 합니다.



1. 볼륨이 생성된 후 mount 명령을 사용하여 AWS SDDC 호스트의 VMware Cloud에서 실행되는 VM에서 공유에 연결합니다.
2. 다음 경로를 복사하고 네트워크 드라이브 매핑 옵션을 사용하여 AWS SDDC의 VMware Cloud에서 실행되는 VM에 볼륨을 마운트합니다.

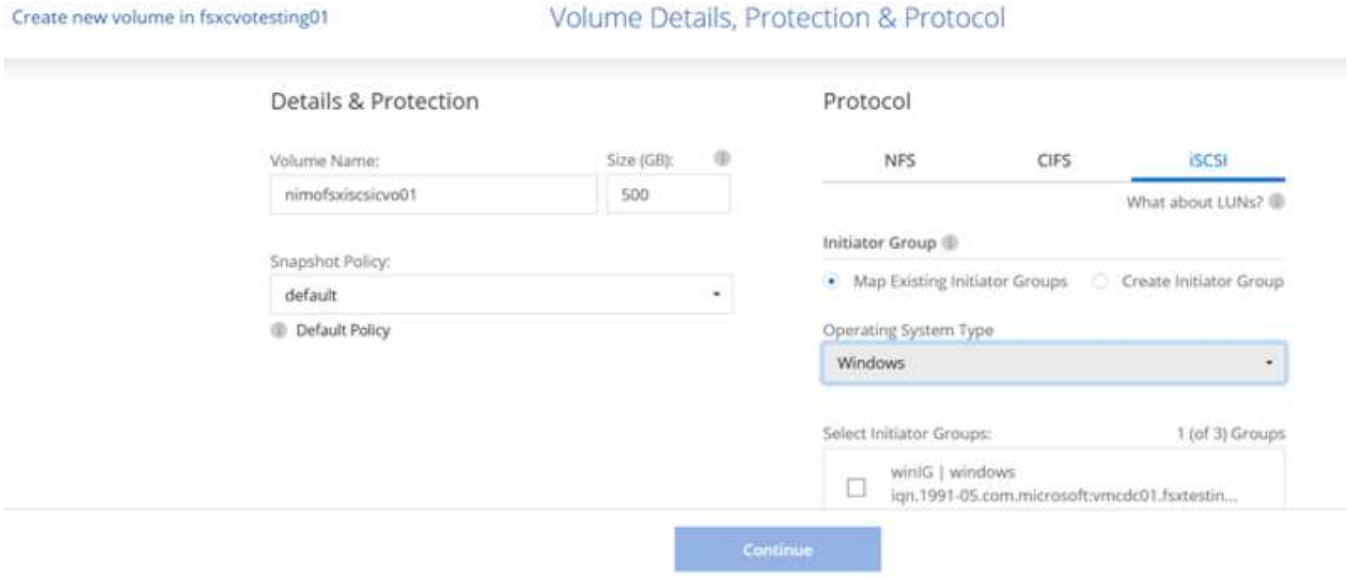


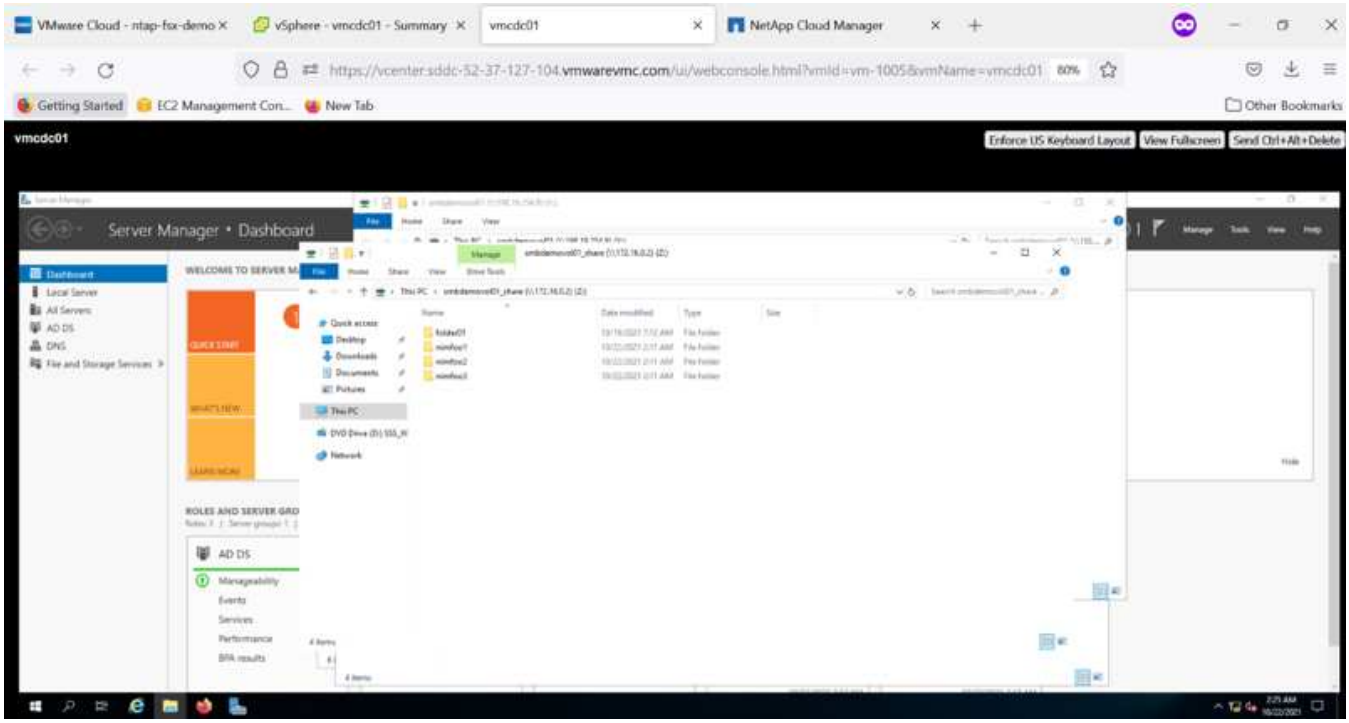


▼ **LUN**을 호스트에 연결합니다

Cloud Volumes ONTAP LUN을 호스트에 연결하려면 다음 단계를 완료하세요.

1. Cloud Manager Canvas 페이지에서 Cloud Volumes ONTAP 작업 환경을 두 번 클릭하여 볼륨을 만들고 관리합니다.
2. 볼륨 추가 > 새 볼륨을 클릭하고 iSCSI를 선택한 다음 초기자 그룹 만들기를 클릭합니다. 계속을 클릭하세요.





1. 볼륨이 프로비저닝된 후 볼륨을 선택한 다음 대상 IQN을 클릭합니다. iSCSI 정규 이름(IQN)을 복사하려면 복사를 클릭합니다. 호스트에서 LUN으로 iSCSI 연결을 설정합니다.

AWS SDDC의 VMware Cloud에 있는 호스트에 대해 동일한 작업을 수행하려면 다음 단계를 완료하세요.

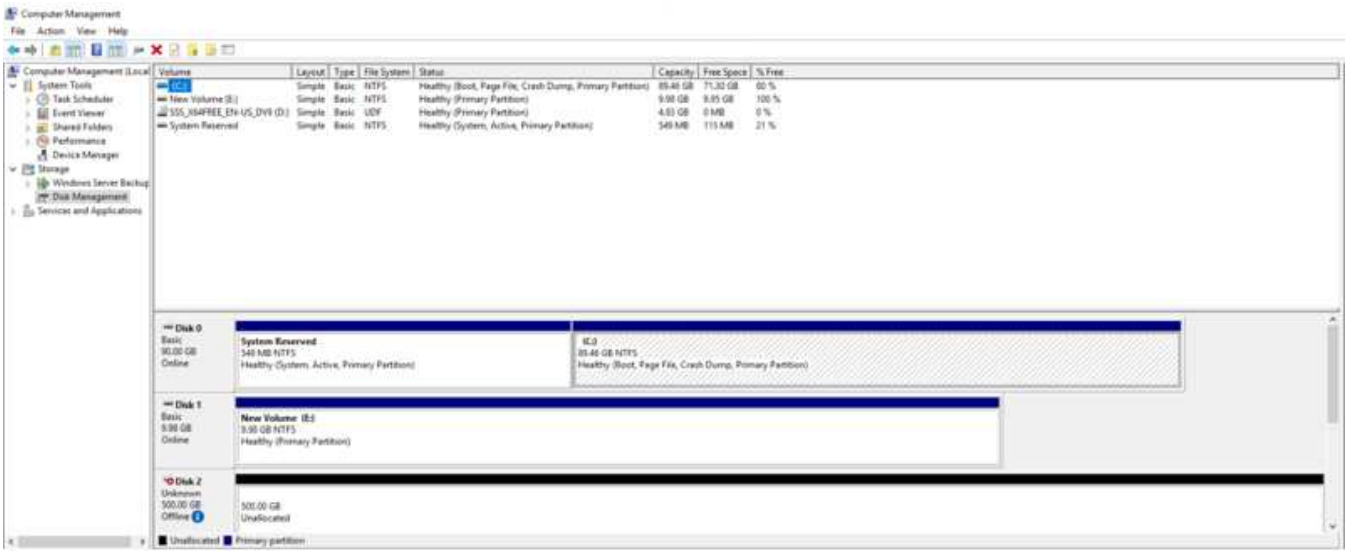
1. AWS의 VMware 클라우드에 호스팅된 VM에 대한 RDP.
2. iSCSI 초기자 속성 대화 상자를 엽니다: 서버 관리자 > 대시보드 > 도구 > iSCSI 초기자.
3. 검색 탭에서 포털 검색 또는 포털 추가를 클릭한 다음 iSCSI 대상 포트의 IP 주소를 입력합니다.
4. 대상 탭에서 검색된 대상을 선택한 다음 로그온 또는 연결을 클릭합니다.
5. 다중 경로 사용을 선택한 다음 컴퓨터가 시작될 때 이 연결을 자동으로 복원하거나 이 연결을 즐겨찾는 대상 목록에 추가를 선택합니다. 고급을 클릭합니다.

Windows 호스트는 클러스터의 각 노드에 iSCSI 연결이 있어야 합니다. 기본 DSM은 사용할 가장 좋은 경로를 선택합니다.



SVM의 LUN은 Windows 호스트에 디스크로 나타납니다. 새로 추가된 디스크는 호스트에서 자동으로 검색되지 않습니다. 다음 단계를 완료하여 디스크를 검색하기 위한 수동 재검사를 트리거합니다.

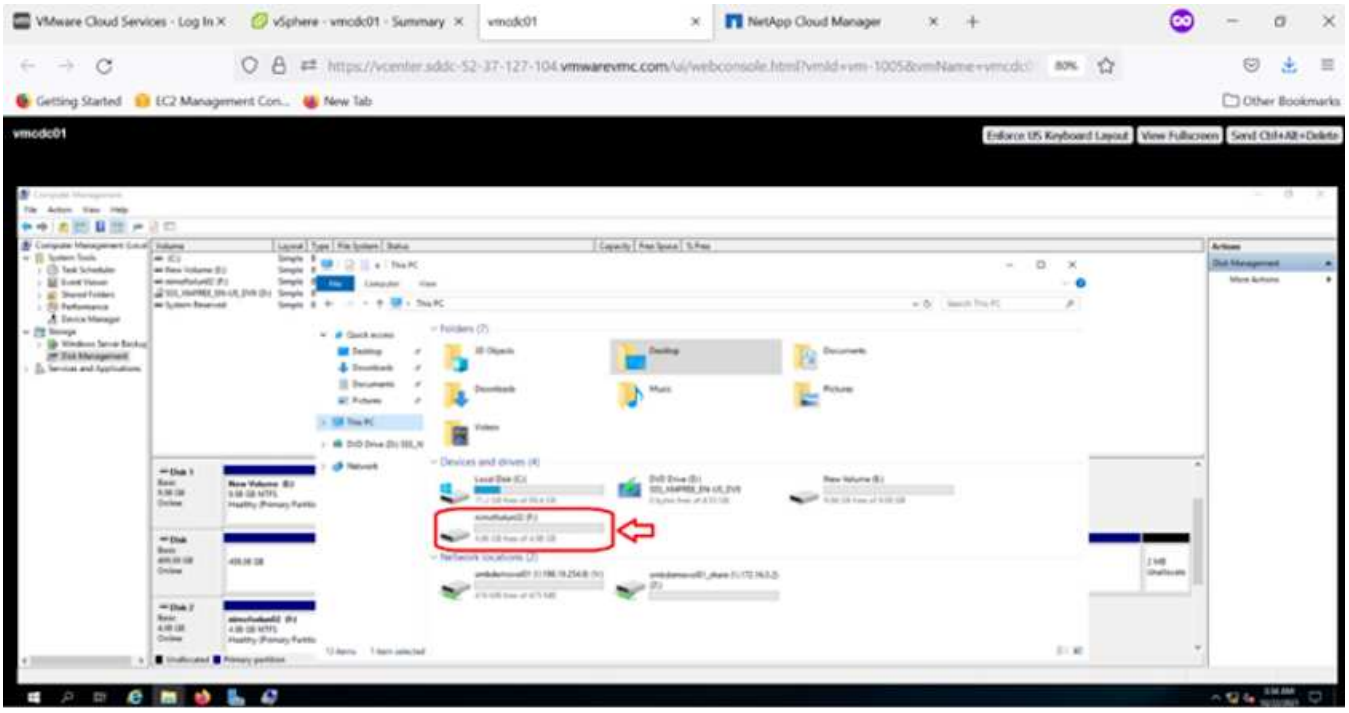
1. Windows 컴퓨터 관리 유틸리티를 엽니다: 시작 > 관리 도구 > 컴퓨터 관리.
2. 탐색 트리에서 저장소 노드를 확장합니다.
3. 디스크 관리를 클릭합니다.
4. 작업 > 디스크 다시 검사를 클릭합니다.



Windows 호스트가 새 LUN에 처음 액세스할 때 파티션이나 파일 시스템이 없습니다. LUN을 초기화하고, 필요한 경우 다음 단계를 완료하여 LUN을 파일 시스템으로 포맷합니다.

1. Windows 디스크 관리를 시작합니다.

2. LUN을 마우스 오른쪽 버튼으로 클릭한 다음 필요한 디스크 또는 파티션 유형을 선택합니다.
3. 마법사의 지시를 따르세요. 이 예에서는 드라이브 F:가 마운트되었습니다.



Linux 클라이언트에서 iSCSI 데몬이 실행 중인지 확인하세요. LUN이 프로비저닝된 후에는 Linux 배포판에 대한 iSCSI 구성에 대한 자세한 지침을 참조하세요. 예를 들어, Ubuntu iSCSI 구성을 찾을 수 있습니다."여기" . 확인하려면 셸에서 lsblk cmd를 실행하세요.

▼ **Linux** 클라이언트에서 **Cloud Volumes ONTAP NFS** 볼륨 마운트

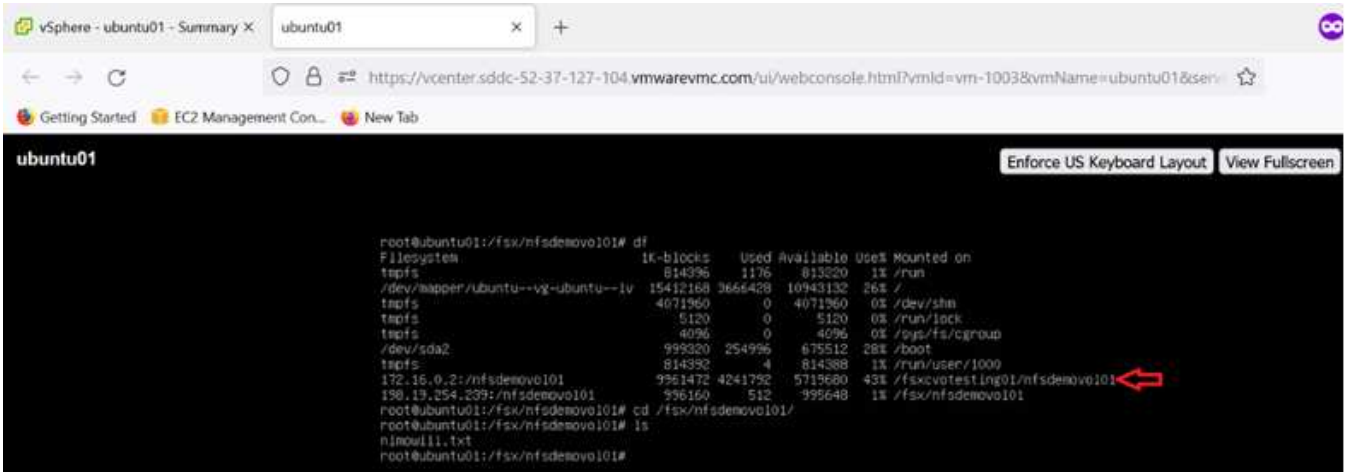
AWS SDDC의 VMC 내 VM에서 Cloud Volumes ONTAP (DIY) 파일 시스템을 마운트하려면 다음 단계를 완료하세요.

1. 지정된 Linux 인스턴스에 연결합니다.
2. 보안 셸(SSH)을 사용하여 인스턴스에서 터미널을 열고 적절한 자격 증명으로 로그인합니다.
3. 다음 명령을 사용하여 볼륨의 마운트 지점에 대한 디렉토리를 만듭니다.

```
 $ sudo mkdir /fsxcvotesting01/nfsdemovol01
. 이전 단계에서 생성한 디렉토리에 Amazon FSx ONTAP NFS 볼륨을 마운트합니다.
```

```
sudo mount -t nfs nfsvers=4.1,172.16.0.2:/nfsdemovol01
/fsxcvotesting01/nfsdemovol01
```

```
root@ubuntu01:/fsx# mount -t nfs 172.16.0.2:/nfsdemovol01 /fsxcvotesting01/nfsdemovol01_
```



Azure 가상화 서비스**: NetApp** 스토리지 사용 옵션

NetApp 스토리지는 게스트 연결 또는 보조 스토리지로 Azure VMware 서비스에 연결될 수 있습니다.

보조 **NFS** 데이터 저장소로서의 **Azure NetApp Files (ANF)**

ESXi 버전 3에서는 온프레미스 배포에 NFS 데이터 저장소 지원이 도입되어 vSphere의 스토리지 기능이 크게 확장되었습니다.

NFS에서 vSphere를 실행하는 것은 강력한 성능과 안정성을 제공하므로 온프레미스 가상화 배포에 널리 채택된 옵션입니다. 온프레미스 데이터 센터에 상당한 NAS(네트워크 연결 스토리지)가 있는 경우 용량 및 성능 문제를 극복하기 위해 Azure NetApp 파일 데이터 저장소와 함께 Azure에 Azure VMware 솔루션 SDDC를 배포하는 것을 고려해야 합니다.

Azure NetApp Files 업계를 선도하는 고가용성 NetApp ONTAP 데이터 관리 소프트웨어를 기반으로 구축되었습니다. Microsoft Azure 서비스는 기초형, 일반형, 특수형의 세 가지 범주로 그룹화됩니다. Azure NetApp Files 특수 범주에 속하며 이미 여러 지역에 배포된 하드웨어에 의해 지원됩니다. Azure NetApp Files 고가용성(HA) 기능이 내장되어 있어 대부분의 중단으로부터 데이터를 보호하고 업계 최고 수준인 99.99%^ 가동 시간 SLA를 제공합니다.

NFS 데이터 저장소로서의 ANF에 대한 자세한 내용은 다음을 방문하세요.

- "보충 NFS 데이터 저장소로서의 ANF: 개요"
- "Azure의 보충 NFS 데이터 저장소 옵션"

게스트 연결 스토리지로서의 **Azure NetApp Files (ANF)**

Azure NetApp Files 엔터프라이즈급 데이터 관리 및 저장 기능을 Azure에 제공하여 워크로드와 애플리케이션을 손쉽게 관리할 수 있도록 해줍니다. 워크로드를 클라우드로 마이그레이션하여 성능 저하 없이 실행하세요.

Azure NetApp Files 장애물을 제거하여 모든 파일 기반 애플리케이션을 클라우드로 옮길 수 있도록 해줍니다. 처음으로 애플리케이션을 다시 설계할 필요가 없고, 복잡하지 않게 애플리케이션을 위한 영구 저장소를 확보할 수 있습니다.

이 서비스는 Microsoft Azure Portal을 통해 제공되므로 사용자는 Microsoft Enterprise Agreement의 일부로 완벽하게 관리되는 서비스를 경험할 수 있습니다. Microsoft가 관리하는 세계적 수준의 지원을 통해 완벽한 안심을 누리세요. 이 단일 솔루션을 사용하면 다중 프로토콜 워크로드를 빠르고 쉽게 추가할 수 있습니다. 레거시 환경에서도 Windows 및 Linux 파일 기반 애플리케이션을 빌드하고 배포할 수 있습니다.

자세한 내용은 다음을 방문하세요."게스트 연결 스토리지로서의 ANF" .

게스트 연결 스토리지로서의 **Cloud Volumes ONTAP (CVO)**

Cloud Volumes ONTAP (CVO)은 NetApp의 ONTAP 스토리지 소프트웨어를 기반으로 구축된 업계 최고의 클라우드 데이터 관리 솔루션으로, Amazon Web Services(AWS), Microsoft Azure 및 Google Cloud Platform(GCP)에서 기본적으로 제공됩니다.

ONTAP 은 클라우드 기반 스토리지를 사용하는 소프트웨어 정의 버전으로, 클라우드와 온프레미스에서 동일한 스토리지 소프트웨어를 사용할 수 있어 데이터를 관리하는 완전히 새로운 방법에 대한 IT 직원의 재교육 필요성이 줄어듭니다.

CVO를 사용하면 고객은 엣지에서 데이터 센터, 클라우드로 원활하게 데이터를 이동할 수 있으며, 하이브리드 클라우드를 하나로 통합할 수 있습니다. 이 모든 기능은 단일 창 관리 콘솔인 NetApp Cloud Manager를 통해 관리할 수 있습니다.

CVO는 설계상 클라우드에서 가장 까다로운 애플리케이션도 만족시킬 수 있는 극한의 성능과 고급 데이터 관리 기능을 제공합니다.

자세한 내용은 다음을 방문하세요."게스트 연결 스토리지로서의 CVO" .

ANF 데이터 저장소 솔루션 개요

모든 성공적인 조직은 변화와 현대화의 길을 걷고 있습니다. 이 과정의 일환으로 기업은 일반적으로 기존 VMware 투자를 활용하면서 클라우드의 이점을 활용하고 마이그레이션, 버스트, 확장 및 재해 복구 프로세스를 최대한 원활하게 만드는 방법을 모색합니다. 클라우드로 마이그레이션하는 고객은 탄력성과 폭발성, 데이터 센터 종료, 데이터 센터 통합, 수명 종료 시나리오, 합병, 인수 등의 문제를 평가해야 합니다. 각 조직이 채택하는 접근 방식은 해당 사업 우선순위에 따라 달라질 수 있습니다. 클라우드 기반 운영을 선택할 때 적절한 성능과 최소한의 방해 요소를 갖춘 저비용 모델을 선택하는 것이 중요한 목표입니다. 올바른 플랫폼을 선택하는 것과 함께 스토리지와 워크플로우 오케스트레이션은 클라우드 배포와 탄력성의 힘을 최대한 활용하는 데 특히 중요합니다.

사용 사례

Azure VMware 솔루션은 고객에게 고유한 하이브리드 기능을 제공하지만, 기본 스토리지 옵션이 제한적이어서 스토리지 사용량이 많은 작업 부하를 가진 조직에서는 유용성이 제한됩니다. 스토리지는 호스트에 직접 연결되므로 스토리지를 확장하는 유일한 방법은 호스트를 추가하는 것인데, 스토리지를 많이 사용하는 작업의 경우 비용이 35~40% 이상 증가할 수 있습니다. 이러한 작업에는 추가 마력이 아닌 추가 저장 용량이 필요한데, 이는 추가 호스트 비용을 지불해야 한다는 것을 의미합니다.

다음 시나리오를 생각해 보겠습니다. 어떤 고객은 성능(vCPU/vMem)을 위해 6개의 호스트가 필요하지만, 저장 용량도 상당히 필요합니다. 평가에 따르면 저장 요구 사항을 충족하려면 12개의 호스트가 필요합니다. 실제로 필요한 것이 저장 공간뿐인데도 추가 마력을 모두 구매해야 하므로 전반적인 TCO가 증가합니다. 이는 마이그레이션, 재해 복구, 버스팅, 개발/테스트 등 모든 사용 사례에 적용할 수 있습니다.

Azure VMware Solution의 또 다른 일반적인 사용 사례는 재해 복구(DR)입니다. 대부분의 조직은 완벽한 재해 복구 전략이 없으며, 재해 복구만을 위해 고스트 데이터 센터를 운영하는 것을 정당화하는 데 어려움을 겪을 수 있습니다. 관리자는 파일럿 라이트 클러스터나 주문형 클러스터를 통해 제로 풋프린트 DR 옵션을 모색할 수 있습니다. 그러면 추가 호스트를 추가하지 않고도 스토리지를 확장할 수 있어 매력적인 옵션이 될 수 있습니다.

따라서 요약하자면, 사용 사례는 두 가지 방법으로 분류할 수 있습니다.

- ANF 데이터 저장소를 사용하여 스토리지 용량 확장
- 온프레미스 또는 Azure 지역 내에서 소프트웨어 정의 데이터 센터(SDDC) 간 비용 최적화된 복구 워크플로를 위한 재해 복구 대상으로 ANF 데이터 저장소를 사용하는 방법. 이 가이드에서는 Azure NetApp Files 사용하여 데이터 저장소에 최적화된 스토리지(현재 공개 미리 보기)와 Azure VMware 솔루션에서 동급 최고의 데이터 보호 및 재해 복구 기능을 제공하는 방법에 대한 통찰력을 제공합니다. 이를 통해 vSAN 스토리지에서 스토리지 용량을 오프로드할 수 있습니다.



ANF 데이터 저장소 사용에 대한 추가 정보는 해당 지역의 NetApp 또는 Microsoft 솔루션 설계자에게 문의하세요.

Azure의 **VMware Cloud** 옵션

Azure VMware 솔루션

Azure VMware 솔루션(AVS)은 Microsoft Azure 퍼블릭 클라우드 내에서 완벽하게 작동하는 VMware SDDC를 제공하는 하이브리드 클라우드 서비스입니다. AVS는 Microsoft에서 완벽하게 관리하고 지원하며 VMware에서 검증한 자체 솔루션으로, Azure 인프라를 사용합니다. 따라서 고객은 컴퓨팅 가상화를 위해 VMware ESXi, 하이퍼 컨버지드 스토리지를 위해 vSAN, 네트워킹 및 보안을 위해 NSX를 얻는 동시에 Microsoft Azure의 글로벌 입지, 동급 최고의 데이터 센터 시설, 풍부한 기본 Azure 서비스 및 솔루션 생태계와의 근접성을 활용할 수 있습니다. Azure VMware Solution SDDC와 Azure NetApp Files 결합하면 최소한의 네트워크 지연으로 최고의 성능을 제공합니다.

사용하는 클라우드에 관계없이 VMware SDDC가 배포되면 초기 클러스터에는 다음 구성 요소가 포함됩니다.

- 관리를 위한 vCenter 서버 어플라이언스와 함께 컴퓨팅 가상화를 위한 VMware ESXi 호스트.
- 각 ESXi 호스트의 물리적 스토리지 자산을 통합한 VMware vSAN 하이퍼 컨버지드 스토리지입니다.
- 가상 네트워킹 및 보안을 위한 VMware NSX와 관리를 위한 NSX Manager 클러스터.

결론

전체 클라우드 또는 하이브리드 클라우드를 타겟으로 삼는지 여부에 관계없이 Azure NetApp 파일은 데이터 요구 사항을 애플리케이션 계층에 원활하게 전달하여 TCO를 줄이는 동시에 파일 서비스와 함께 애플리케이션 워크로드를 배포하고 관리할 수 있는 탁월한 옵션을 제공합니다. 어떤 사용 사례든 Azure NetApp Files 와 함께 Azure VMware 솔루션을 선택하면 클라우드의 이점을 빠르게 실현하고, 온프레미스와 여러 클라우드에서 일관된 인프라와 운영을 구현하고, 워크로드를 양방향으로 이동시키고, 엔터프라이즈급 용량과 성능을 얻을 수 있습니다. 저장소를 연결하는 데 사용되는 익숙한 프로세스와 절차와 동일합니다. 기억하세요. 새로운 이름과 함께 데이터의 위치만 변경되었을 뿐, 도구와 프로세스는 모두 동일하게 유지되며 Azure NetApp Files 전반적인 배포를 최적화하는 데 도움이 됩니다.

테이크아웃

이 문서의 주요 내용은 다음과 같습니다.

- 이제 Azure NetApp Files AVS SDDC의 데이터 저장소로 사용할 수 있습니다.
- 애플리케이션 응답 시간을 단축하고 가용성을 높여 필요할 때 필요한 위치에서 워크로드 데이터에 액세스할 수 있도록 합니다.
- 간단하고 즉각적인 크기 조정 기능으로 vSAN 스토리지의 전반적인 복잡성을 단순화합니다.
- 동적 재구성 기능을 사용하여 미션 크리티컬 워크로드에 대한 성능을 보장합니다.
- Azure VMware Solution Cloud가 대상이라면 Azure NetApp Files 최적화된 배포를 위한 적합한 스토리지

솔루션입니다.

추가 정보를 찾을 수 있는 곳

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 웹사이트 링크를 참조하세요.

- Azure VMware 솔루션 설명서

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

- Azure NetApp Files 설명서

  "https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

- Azure NetApp Files 데이터 저장소를 Azure VMware Solution 호스트에 연결(미리 보기)

  https://docs.microsoft.com/en-us/azure/azure-vmware/attach-azure-netapp-files-to-azure-vmware-solution-hosts?tabs=azure-portal/

Azure에서 보충 **NFS** 데이터 저장소 만들기

ESXi 버전 3에서는 온프레미스 배포에 NFS 데이터 저장소 지원이 도입되어 vSphere의 스토리지 기능이 크게 확장되었습니다.

NFS에서 vSphere를 실행하는 것은 강력한 성능과 안정성을 제공하므로 온프레미스 가상화 배포에 널리 채택된 옵션입니다. 온프레미스 데이터 센터에 상당한 NAS(네트워크 연결 스토리지)가 있는 경우 용량 및 성능 문제를 극복하기 위해 Azure NetApp 파일 데이터 저장소와 함께 Azure에 Azure VMware 솔루션 SDDC를 배포하는 것을 고려해야 합니다.

Azure NetApp Files 업계를 선도하는 고가용성 NetApp ONTAP 데이터 관리 소프트웨어를 기반으로 구축되었습니다. Microsoft Azure 서비스는 기초형, 일반형, 특수형의 세 가지 범주로 그룹화됩니다. Azure NetApp Files 특수 범주에 속하며 이미 여러 지역에 배포된 하드웨어에 의해 지원됩니다. Azure NetApp Files 내장된 고가용성(HA)을 통해 대부분의 중단으로부터 데이터를 보호하고 업계 최고 수준의 SLA를 제공합니다. "99.99%" 가동시간.

Azure NetApp Files 데이터 저장소 기능이 도입되기 전에는 성능과 스토리지 집약적 워크로드를 호스팅하려는 고객을 위한 확장 운영에는 컴퓨팅과 스토리지를 모두 확장해야 했습니다.

다음 사항을 명심하세요.

- SDDC 클러스터에서는 불균형한 클러스터 구성이 권장되지 않습니다. 따라서 스토리지를 확장한다는 것은 더 많은 호스트를 추가하는 것을 의미하며, 이는 TCO(총소유비용) 증가를 의미합니다.
- vSAN 환경은 하나만 가능합니다. 따라서 모든 스토리지 트래픽은 프로덕션 워크로드와 직접적으로 경쟁하게 됩니다.
- 애플리케이션 요구 사항, 성능 및 비용을 조정하기 위해 여러 성능 계층을 제공하는 옵션은 없습니다.
- 클러스터 호스트 위에 구축된 vSAN의 경우 스토리지 용량의 한계에 도달하기 쉽습니다. Azure NetApp Files 와 같은 Azure 기본 PaaS(Platform-as-a-Service) 제품을 데이터 저장소로 통합하면 고객은 스토리지를 개별적으로 독립적으로 확장하고 필요에 따라서만 SDDC 클러스터에 컴퓨팅 노드를 추가할 수 있습니다. 이 기능은 위에서 언급한 과제를 극복합니다.

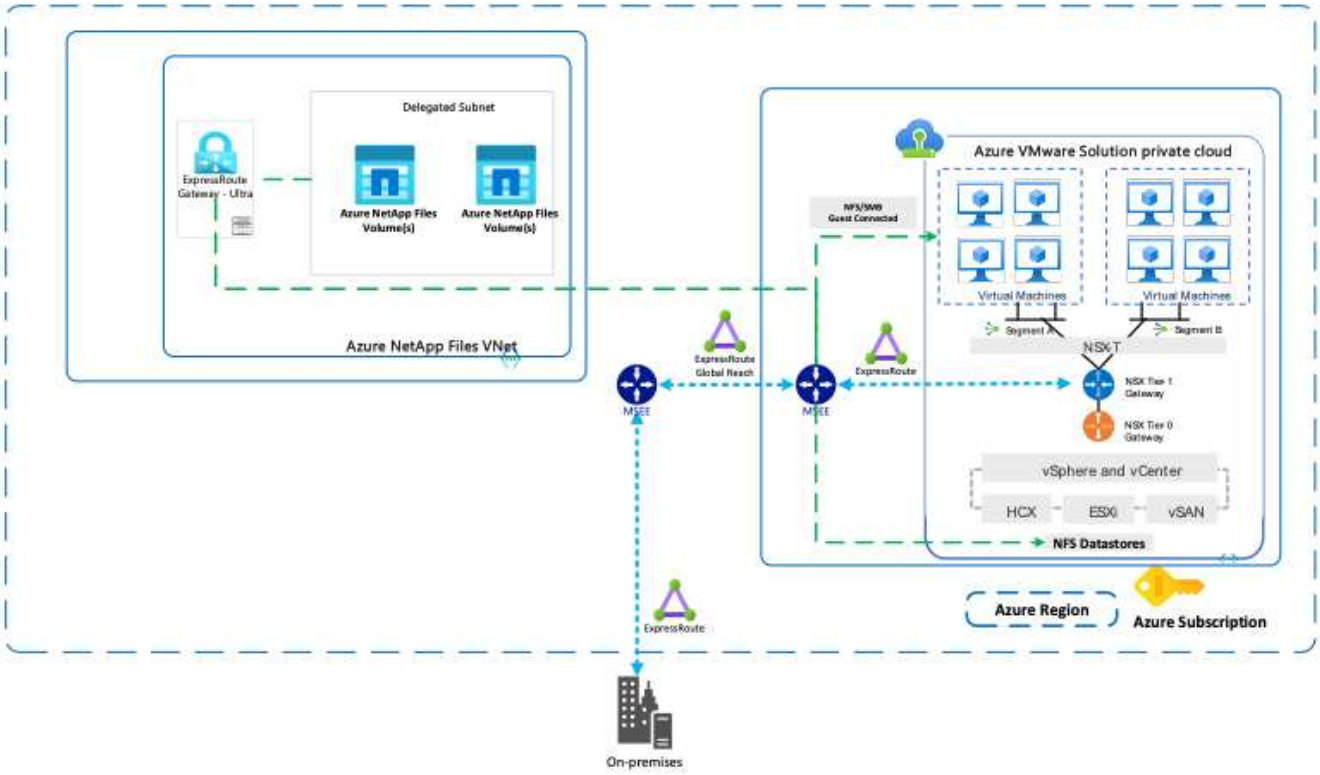
Azure NetApp Files 사용하면 여러 데이터 저장소를 배포할 수도 있습니다. 이를 통해 적절한 데이터 저장소에 가상 머신을 배치하고 워크로드 성능 요구 사항을 충족하는 데 필요한 서비스 수준을 할당하여 온프레미스 배포 모델을

모방하는 데 도움이 됩니다. 다중 프로토콜 지원이라는 고유한 기능을 갖춘 게스트 스토리지는 SQL 및 Oracle과 같은 데이터베이스 워크로드를 위한 추가 옵션이며, 나머지 VMDK를 수용하기 위해 보충적인 NFS 데이터 저장소 기능도 사용합니다. 이 외에도 기본 스냅샷 기능을 사용하면 빠른 백업과 세부적인 복원을 수행할 수 있습니다.

스토리지 계획 및 크기 조정, 필요한 호스트 수 결정을 위해 Azure 및 NetApp 솔루션 아키텍트에 문의하세요. NetApp 테스트, POC 및 프로덕션 배포를 위한 데이터 저장소 레이아웃을 최종 결정하기 전에 스토리지 성능 요구 사항을 파악하는 것이 좋습니다.

세부적인 아키텍처

높은 수준의 관점에서 이 아키텍처는 온-프레미스 환경과 Azure에서 하이브리드 클라우드 연결과 앱 이동성을 달성하는 방법을 설명합니다. 또한 Azure NetApp Files 보조 NFS 데이터 저장소로 사용하고 Azure VMware 솔루션에 호스팅된 게스트 가상 머신의 게스트 내부 저장소 옵션으로 사용하는 방법도 설명합니다.



사이징

마이그레이션이나 재해 복구에서 가장 중요한 측면은 대상 환경에 적합한 크기를 결정하는 것입니다. 온프레미스에서 Azure VMware 솔루션으로 리프트 앤 시프트 작업을 수행하는 데 필요한 노드 수를 이해하는 것은 매우 중요합니다.

크기 조정을 위해 RVTools(권장) 또는 Live Optics나 Azure Migrate와 같은 다른 도구를 사용하여 온-프레미스 환경의 과거 데이터를 사용합니다. RVTools는 대상 환경을 특성화하기 위해 vCPU, vMem, vDisk 및 전원이 켜진 VM과 꺼진 VM을 포함한 모든 필수 정보를 캡처하는 이상적인 도구입니다.

RVtools를 실행하려면 다음 단계를 완료하세요.

1. RVTools를 다운로드하여 설치하세요.
2. RVTools를 실행하고 온-프레미스 vCenter Server에 연결하는 데 필요한 정보를 입력한 다음 로그인을 누릅니다.
3. 재고를 Excel 스프레드시트로 내보냅니다.

4. 스프레드시트를 편집하고 vInfo 탭에서 이상적인 후보가 아닌 모든 VM을 제거합니다. 이 접근 방식은 필요한 수의 호스트로 Azure VMware SDDC 클러스터의 크기를 적절하게 조정하는 데 사용할 수 있는 저장소 요구 사항에 대한 명확한 출력을 제공합니다.

> ⓘ 게스트 내부 저장소와 함께 사용되는 게스트 VM은 별도로 계산해야 합니다. 그러나 Azure NetApp Files 추가 저장소 용량을 쉽게 감당할 수 있으므로 전반적인 TCO를 낮게 유지할 수 있습니다.

Azure VMware 솔루션 배포 및 구성

온프레미스와 마찬가지로 Azure VMware 솔루션을 계획하는 것은 가상 머신을 만들고 마이그레이션하기 위한 성공적인 프로덕션 준비 환경을 조성하는 데 중요합니다.

이 섹션에서는 Azure NetApp Files 와 함께 게스트 내부 저장소를 포함한 데이터 저장소로 사용하도록 AVS를 설정하고 관리하는 방법을 설명합니다.

설정 과정은 세 부분으로 나눌 수 있습니다.

- 리소스 공급자를 등록하고 프라이빗 클라우드를 생성합니다.
- 새 ExpressRoute 가상 네트워크 게이트웨이나 기존 ExpressRoute 가상 네트워크 게이트웨이에 연결합니다.
- 네트워크 연결을 검증하고 프라이빗 클라우드에 액세스합니다. 이것을 참조하세요"링크" Azure VMware 솔루션 SDDC 프로비저닝 프로세스에 대한 단계별 안내입니다.

Azure VMware 솔루션을 사용하여 Azure NetApp Files 구성

Azure NetApp Files 의 새로운 통합을 통해 Azure NetApp Files 볼륨을 사용하여 Azure VMware Solution 리소스 공급자 API/CLI를 통해 NFS 데이터 저장소를 만들고, 프라이빗 클라우드에서 선택한 클러스터에 데이터 저장소를 마운트할 수 있습니다. VM 및 앱 VMDK를 보관하는 것 외에도 Azure NetApp 파일 볼륨은 Azure VMware Solution SDDC 환경에서 생성된 VM에서도 마운트할 수 있습니다. Azure NetApp Files SMB(Server Message Block) 및 NFS(Network File System) 프로토콜을 지원하므로 볼륨을 Linux 클라이언트에 마운트하고 Windows 클라이언트에 매핑할 수 있습니다.

> ⓘ 최적의 성능을 위해 Azure NetApp Files 프라이빗 클라우드와 동일한 가용성 영역에 배포하세요. Express 경로 fastpath와 함께 배치하면 네트워크 지연을 최소화하면서 최상의 성능을 제공합니다.

Azure VMware Solution 프라이빗 클라우드의 VMware 데이터 저장소로 Azure NetApp 파일 볼륨을 연결하려면 다음 필수 구성 요소가 충족되었는지 확인하세요.

▼ 필수 조건

1. az login을 사용하여 구독이 Microsoft.AVS 네임스페이스의 CloudSanExperience 기능에 등록되었는지 확인합니다.

```
az login –tenant xcvxcvxc- vxcv- xcvx- cvxc- vxcvxcvxcv
az feature show --name "CloudSanExperience" --namespace "Microsoft.AVS"
```

1. 등록되어 있지 않으면 등록하세요.

```
az feature register --name "CloudSanExperience" --namespace
```

```
"Microsoft.AVS"
```

등록을 완료하는 데 약 15분이 걸릴 수 있습니다.

1. 등록 상태를 확인하려면 다음 명령을 실행하세요.

```
az feature show --name "CloudSanExperience" --namespace "Microsoft.AVS"
--query properties.state
```

1. 등록이 15분 이상 중간 상태에 갇히면 플래그를 등록 해제한 후 다시 등록하세요.

```
az feature unregister --name "CloudSanExperience" --namespace
"Microsoft.AVS"
az feature register --name "CloudSanExperience" --namespace
"Microsoft.AVS"
```

1. 구독이 Microsoft.AVS 네임스페이스의 AnfDatastoreExperience 기능에 등록되었는지 확인합니다.

```
az feature show --name "AnfDatastoreExperience" --namespace
"Microsoft.AVS" --query properties.state
```

1. vmware 확장 프로그램이 설치되었는지 확인하세요.

```
az extension show --name vmware
```

1. 확장 프로그램이 이미 설치되어 있는 경우 버전이 3.0.0인지 확인하세요. 이전 버전이 설치되어 있는 경우 확장 프로그램을 업데이트하세요.

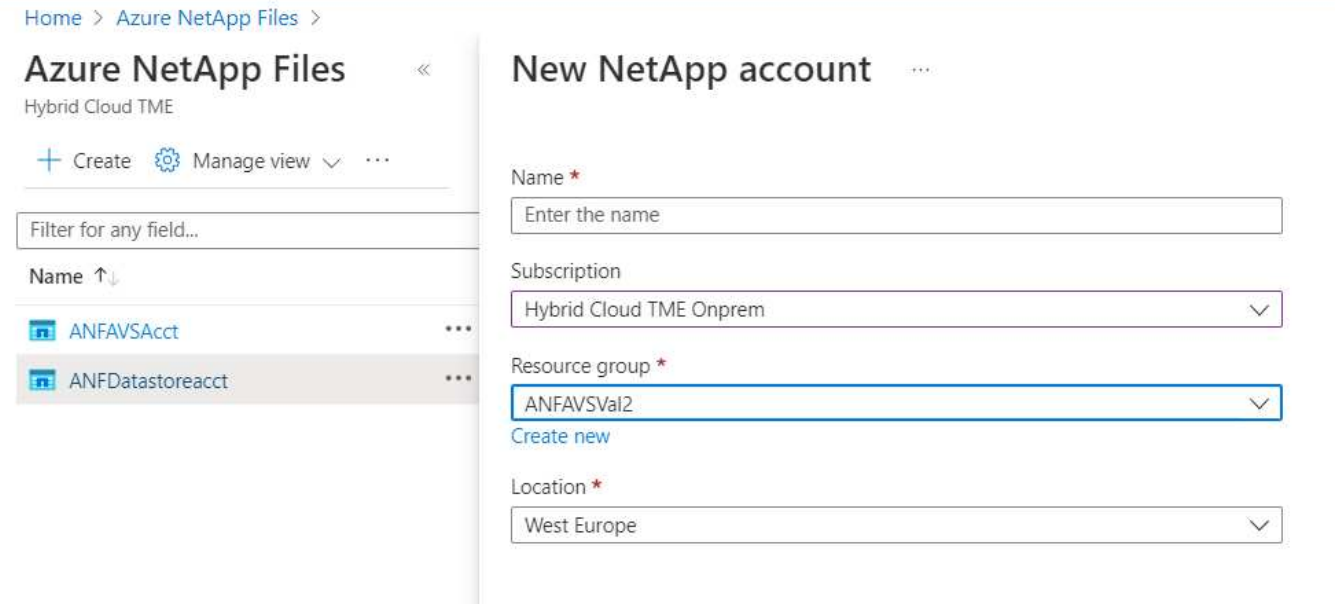
```
az extension update --name vmware
```

1. 확장 프로그램이 아직 설치되지 않았다면 설치하세요.

```
az extension add --name vmware
```

▼ **Azure NetApp Files** 볼륨 만들기 및 마운트

1. Azure Portal에 로그인하여 Azure NetApp Files 액세스합니다. Azure NetApp Files 서비스에 대한 액세스를 확인하고 다음을 사용하여 Azure NetApp Files 리소스 공급자를 등록합니다. `az provider register --namespace Microsoft.NetApp –wait` 명령. 등록 후 NetApp 계정을 만드세요. 이것을 참조하세요 "링크" 자세한 단계는 다음을 참조하세요.

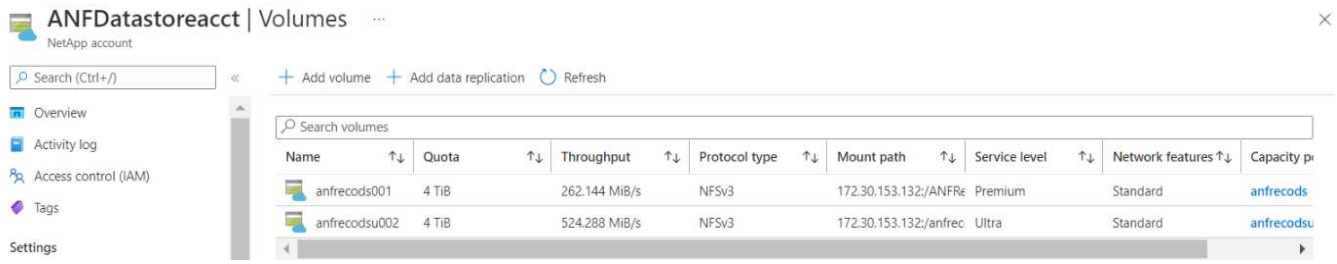


1. NetApp 계정을 만든 후 필요한 서비스 수준과 크기로 용량 풀을 설정합니다. 자세한 내용은 여기를 참조하세요. "링크" .



기억해야 할 점
• NFSv3는 Azure NetApp Files 데이터 저장소에서 지원됩니다. • 기본 vSAN 스토리지를 보완하면서 필요한 경우 용량 제한 워크로드에는 프리미엄 또는 표준 계층을 사용하고 성능 제한 워크로드에는 울트라 계층을 사용하세요.

1. Azure NetApp Files 대한 위임된 서브넷을 구성하고 볼륨을 만들 때 이 서브넷을 지정합니다. 위임된 서브넷을 생성하는 자세한 단계는 다음을 참조하세요. "링크" .
2. 용량 풀 블레이드 아래의 볼륨 블레이드를 사용하여 데이터 저장소에 대한 NFS 볼륨을 추가합니다.



크기 또는 할당량별 Azure NetApp Files 볼륨 성능에 대해 알아보려면 다음을 참조하세요."Azure NetApp Files 에 대한 성능 고려 사항" .

▼ **Azure NetApp** 파일 데이터 저장소를 프라이빗 클라우드에 추가

Azure Portal을 사용하여 Azure NetApp Files 볼륨을 프라이빗 클라우드에 연결할 수 있습니다. 이것을 따르세요"Microsoft의 링크" Azure Portal을 사용하여 Azure NetApp 파일 데이터 저장소를 탑재하는 단계별 접근 방식입니다.

프라이빗 클라우드에 Azure NetApp 파일 데이터 저장소를 추가하려면 다음 단계를 완료하세요.

1. 필요한 기능을 등록한 후 적절한 명령을 실행하여 Azure VMware Solution 프라이빗 클라우드 클러스터에 NFS 데이터 저장소를 연결합니다.
2. Azure VMware Solution 프라이빗 클라우드 클러스터의 기존 ANF 볼륨을 사용하여 데이터 저장소를 만듭니다.

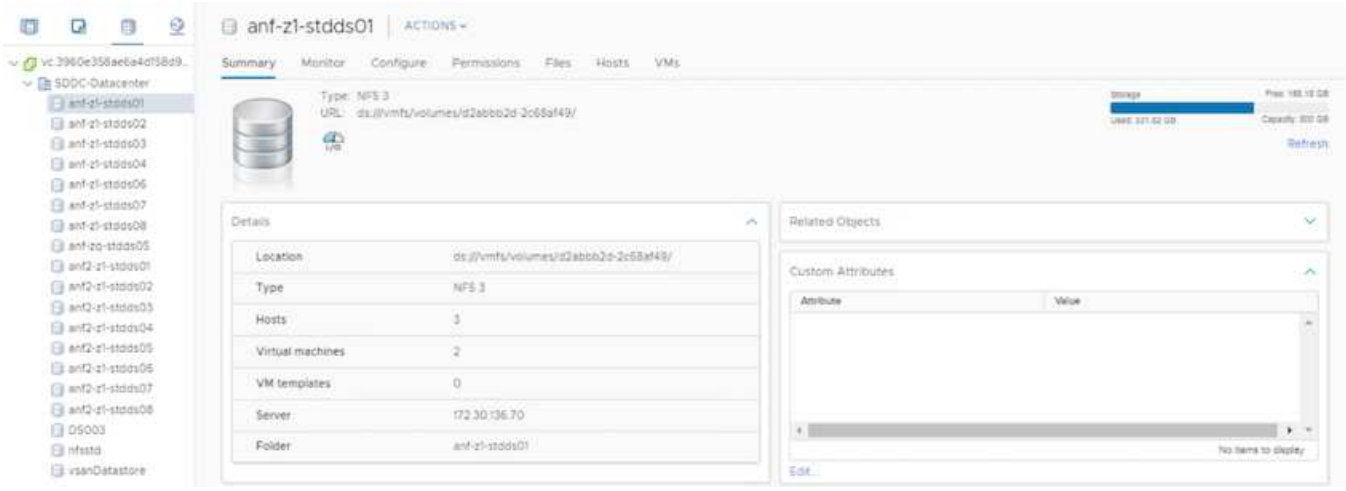
```
C:\Users\niyaz>az vmware datastore netapp-volume create --name
ANFRecoDSU002 --resource-group anfavsval2 --cluster Cluster-1 --private
-cloud ANFDataClus --volume-id /subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002
{
  "diskPoolVolume": null,
  "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateCl
ouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDSU002",
  "name": "ANFRecoDSU002",
  "netAppVolume": {
    "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002
",
    "resourceGroup": "anfavsval2"
  },
  "provisioningState": "Succeeded",
  "resourceGroup": "anfavsval2",
  "type": "Microsoft.AVS/privateClouds/clusters/datastores"
}

. List all the datastores in a private cloud cluster.
```

C:\Users\niyaz>az vmware 데이터 저장소 목록 --리소스 그룹 anfavsval2 --클러스터 클러스터-1 --프라이빗-클라우드 ANFDataClus [{ "디스크 풀 볼륨": null, "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFDataClus/clusters/Cluster-1/데이터 저장소/ANFRecoDS001", "name": "ANFRecoDS001", "netAppVolume": { "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp / NetApp/anfdatastoreacct/capacityPools/anfrecods/volumes/ANFRecoDS001", "resourceGroup": "anfavsval2" }, "provisioningState": "성공", "resourceGroup": "anfavsval2", "type": "Microsoft.AVS/privateClouds/clusters/datastores" }, { "diskPoolVolume": null, "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFDataClus/clusters/Cl

uster-1/datastores/ANFRecoDSU002", "name": "ANFRecoDSU002", "netAppVolume": { "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp / NetApp/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002", "resourceGroup": "anfavsval2" }, "provisioningState": "성공", "resourceGroup": "anfavsval2", "type": "Microsoft.AVS/privateClouds/clusters/datastores" }]

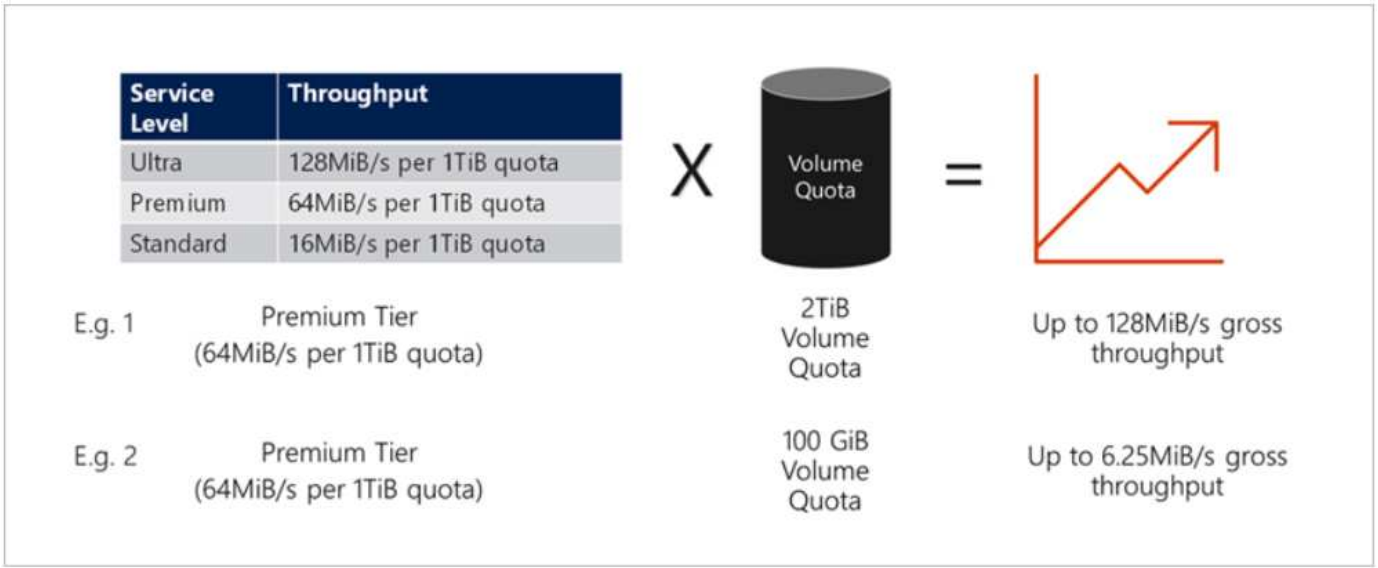
1. 필요한 연결이 구축되면 볼륨이 데이터 저장소로 마운트됩니다.



크기 조정 및 성능 최적화

Azure NetApp Files Standard(테라바이트당 16MBps), Premium(테라바이트당 64MBps), Ultra(테라바이트당 128MBps)의 세 가지 서비스 수준을 지원합니다. 최적의 데이터베이스 작업 부하 성능을 위해서는 적절한 볼륨 크기를 프로비저닝하는 것이 중요합니다. Azure NetApp Files 사용하면 볼륨 성능과 처리량 제한은 다음 요소를 기반으로 결정됩니다.

- 볼륨이 속한 용량 풀의 서비스 수준
- 볼륨에 할당된 할당량
- 용량 풀의 서비스 품질(QoS) 유형(자동 또는 수동)



자세한 내용은 다음을 참조하세요. "Azure NetApp Files 의 서비스 수준" .

이것을 참조하세요"Microsoft의 링크" 크기 조정 과정에서 사용할 수 있는 세부적인 성능 벤치마크입니다.

기억해야 할 점
• 최적의 용량과 성능을 위해 데이터 저장소 볼륨에 프리미엄 또는 표준 계층을 사용하세요. 성능이 필요한 경우 Ultra 등급을 사용할 수 있습니다. • 게스트 마운트 요구 사항에는 프리미엄 또는 울트라 계층을 사용하고, 게스트 VM의 파일 공유 요구 사항에는 표준 또는 프리미엄 계층 볼륨을 사용합니다.

성능 고려 사항

NFS 버전 3에서는 ESXi 호스트와 단일 스토리지 대상 간의 연결을 위한 활성 파이프가 하나뿐이라는 점을 이해하는 것이 중요합니다. 즉, 장애 조치를 위해 대체 연결을 사용할 수 있더라도 단일 데이터 저장소와 기반 저장소의 대역폭은 단일 연결에서 제공할 수 있는 수준으로 제한됩니다.

Azure NetApp Files 볼륨에서 사용 가능한 대역폭을 더 많이 활용하려면 ESXi 호스트에 스토리지 대상에 대한 여러 연결이 있어야 합니다. 이 문제를 해결하려면 여러 개의 데이터 저장소를 구성하고 각 데이터 저장소가 ESXi 호스트와 스토리지 간에 별도의 연결을 사용하도록 할 수 있습니다.

더 높은 대역폭을 위해 모범 사례로 여러 ANF 볼륨을 사용하여 여러 데이터 저장소를 만들고, VMDK를 만들고, VMDK에 걸쳐 논리 볼륨을 스트라이프합니다.

이것을 참조하세요"Microsoft의 링크" 크기 조정 과정에서 사용할 수 있는 세부적인 성능 벤치마크입니다.

기억해야 할 점
• Azure VMware 솔루션은 기본적으로 8개의 NFS 데이터 저장소를 허용합니다. 지원 요청을 통해 증가시킬 수 있습니다. • 더 높은 대역폭과 더 낮은 지연 시간을 위해 Ultra SKU와 함께 ER fastpath를 활용하세요. 더 많은 정보 • Azure NetApp 파일의 "기본" 네트워크 기능을 사용하면 Azure VMware Solution의 연결이 ExpressRoute 회로와 ExpressRoute Gateway의 대역폭에 따라 제한됩니다. • "표준" 네트워크 기능이 있는 Azure NetApp Files 볼륨의 경우 ExpressRoute FastPath가 지원됩니다. FastPath를 활성화하면 게이트웨이를 우회하여 네트워크 트래픽을 Azure NetApp Files 볼륨으로 직접 전송하여 더 높은 대역폭과 더 낮은 대기 시간을 제공합니다.

데이터 저장소 크기 증가

볼륨 재조정 및 동적 서비스 수준 변경은 SDDC에 완전히 투명하게 이루어집니다. Azure NetApp Files 에서 이러한 기능은 지속적인 성능, 용량 및 비용 최적화를 제공합니다. Azure Portal이나 CLI를 사용하여 볼륨 크기를 조정하여 NFS 데이터 저장소의 크기를 늘립니다. 작업이 끝나면 vCenter에 액세스하여 데이터 저장소 탭으로 이동한 다음 해당 데이터 저장소를 마우스 오른쪽 버튼으로 클릭하고 용량 정보 새로 고침을 선택합니다. 이 접근 방식은 다운타임 없이 동적으로 데이터 저장소 용량을 늘리고 데이터 저장소의 성능을 높이는 데 사용할 수 있습니다. 이 프로세스는 애플리케이션에 완전히 투명하게 공개됩니다.

기억해야 할 점
• 볼륨 재구성 및 동적 서비스 수준 기능을 사용하면 안정적인 작업 부하에 맞춰 크기를 조정하여 비용을 최적화하고 과도한 프로비저닝을 방지할 수 있습니다. • VAAI가 활성화되어 있지 않습니다.

작업 부하

▼ 이주

가장 흔한 사용 사례 중 하나는 마이그레이션입니다. VMware HCX 또는 vMotion을 사용하여 온프레미스 VM을 이동합니다. 또는 Rivermeadow를 사용하여 VM을 Azure NetApp Files 데이터 저장소로 마이그레이션할 수 있습니다.

▼ 데이터 보호

ANF 데이터 저장소의 가장 큰 장점 중 하나는 VM을 백업하고 빠르게 복구하는 기능입니다. 스냅샷 복사본을 사용하면 성능에 영향을 주지 않고 VM이나 데이터 저장소의 빠른 복사본을 만든 다음 장기적인 데이터 보호를 위해 Azure 저장소로 보내거나 재해 복구 목적으로 교차 지역 복제를 사용하는 보조 지역으로 보낼 수 있습니다. 이 접근 방식은 변경된 정보만 저장하므로 저장 공간과 네트워크 대역폭을 최소화합니다.

일반적인 보호를 위해 Azure NetApp Files 스냅샷 복사본을 사용하고, 게스트 VM에 있는 SQL Server나 Oracle과 같은 트랜잭션 데이터를 보호하려면 애플리케이션 도구를 사용합니다. 이러한 스냅샷 복사본은 VMware(일관성) 스냅샷과 다르며 장기 보호에 적합합니다.

ANF 데이터 저장소를 사용하면 새 볼륨으로 복원 옵션을 사용하여 전체 데이터 저장소 볼륨을 복제할 수 있으며, 복원된 볼륨을 AVS SDDC 내의 호스트에 다른 데이터 저장소로 마운트할 수 있습니다. 데이터스토어가 마운트된 후에는 해당 데이터스토어 내부의 VM을 개별적으로 복제된 VM처럼 등록, 재구성, 사용자 지정할 수 있습니다.

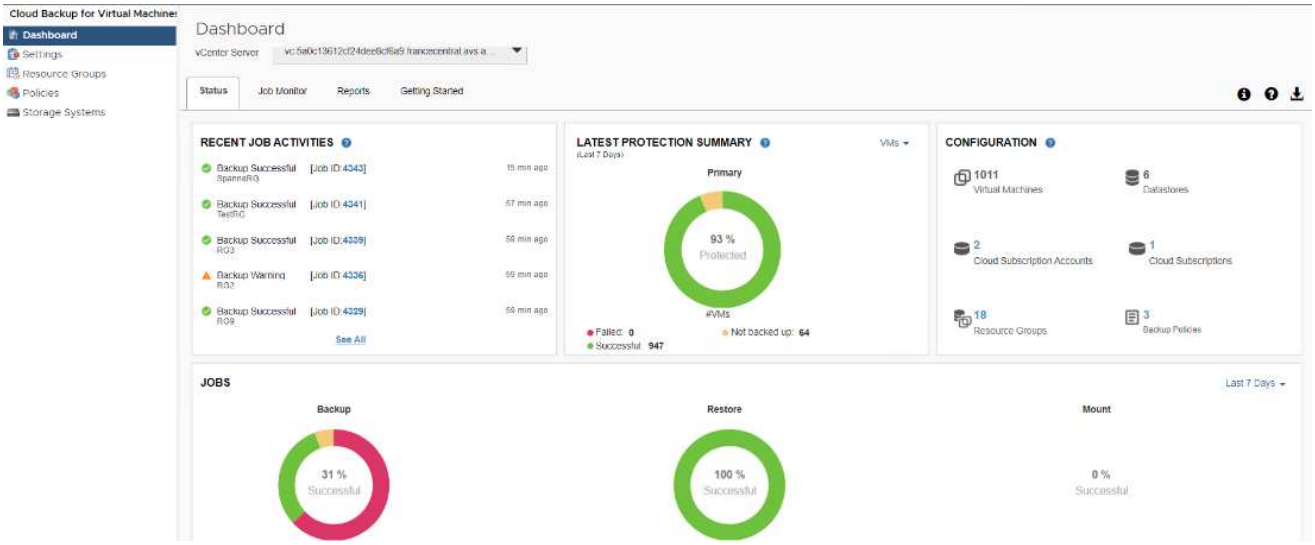
▼ 가상 머신용 **NetApp Backup and Recovery**

NetApp Backup and Recovery for Virtual Machines는 백업 정책을 통해 Azure VMware Solution 가상 머신 및 Azure NetApp Files 데이터스토어를 보호하기 위해 vCenter의 vSphere 웹 클라이언트 GUI를 제공합니다. 이러한 정책은 일정, 보존 기간 및 기타 기능을 정의할 수 있습니다. NetApp Backup and Recovery for Virtual Machine 기능은 Run 명령을 사용하여 배포할 수 있습니다.

다음 단계를 완료하면 설정 및 보호 정책을 설치할 수 있습니다.

1. 실행 명령을 사용하여 Azure VMware Solution 프라이빗 클라우드에 NetApp Backup and Recovery for Virtual Machine을 설치합니다.
2. 클라우드 구독 자격 증명(클라이언트 및 비밀 값)을 추가한 다음, 보호하려는 리소스가 포함된 클라우드 구독 계정(NetApp 계정 및 관련 리소스 그룹)을 추가합니다.
3. 리소스 그룹 백업의 보존, 빈도 및 기타 설정을 관리하는 하나 이상의 백업 정책을 만듭니다.
4. 백업 정책으로 보호해야 하는 하나 이상의 리소스를 추가하기 위해 컨테이너를 만듭니다.
5. 장애가 발생한 경우 전체 VM이나 특정 개별 VMDK를 동일한 위치로 복원합니다.

Azure NetApp Files Snapshot 기술을 사용하면 백업과 복원이 매우 빠르게 진행됩니다.



▼ **Azure NetApp Files, JetStream DR** 및 **Azure VMware** 솔루션을 사용한 재해 복구

클라우드로 재해 복구를 수행하는 것은 사이트 중단 및 데이터 손상 사고(예: 랜섬웨어)로부터 작업 부하를 보호하는 탄력적이고 비용 효율적인 방법입니다. VMware VAIO 프레임워크를 사용하면 온프레미스 VMware 워크로드를 Azure Blob 스토리지에 복제하고 복구할 수 있어 데이터 손실이 최소화되거나 거의 없고 RTO가 거의 0에 가깝습니다. JetStream DR을 사용하면 온프레미스에서 AVS로 복제된 워크로드를 원활하게 복구하고 특히 Azure NetApp Files 로 복구할 수 있습니다. DR 사이트에서 최소한의 리소스와 비용 효율적인 클라우드 스토리지를 사용하여 비용 효율적인 재해 복구를 가능하게 합니다. JetStream DR은 Azure Blob Storage를 통해 ANF 데이터 저장소로의 복구를 자동화합니다. JetStream DR은 네트워크 매핑에 따라 독립적인 VM 또는 관련 VM 그룹을 복구 사이트 인프라로 복구하고 랜섬웨어 보호를 위한 지정 시점 복구를 제공합니다.

"ANF, JetStream 및 AVS를 활용한 DR 솔루션" .

Azure용 **NetApp** 게스트 연결 스토리지 옵션

Azure는 기본 Azure NetApp Files (ANF) 서비스 또는 Cloud Volumes ONTAP (CVO)을 통해 게스트에 연결된 NetApp 스토리지를 지원합니다.

Azure NetApp Files (ANF)

Azure netApp Files는 엔터프라이즈급 데이터 관리 및 저장 기능을 Azure에 제공하여 워크로드와 애플리케이션을 손쉽게 관리할 수 있도록 해줍니다. 워크로드를 클라우드로 마이그레이션하여 성능 저하 없이 실행하세요.

Azure netApp Files는 장애물을 제거하여 모든 파일 기반 애플리케이션을 클라우드로 옮길 수 있도록 해줍니다. 처음으로 애플리케이션을 다시 설계할 필요가 없고, 복잡하지 않게 애플리케이션을 위한 영구 저장소를 확보할 수 있습니다.

이 서비스는 Microsoft Azure Portal을 통해 제공되므로 사용자는 Microsoft Enterprise Agreement의 일부로 완벽하게 관리되는 서비스를 경험할 수 있습니다. Microsoft가 관리하는 세계적 수준의 지원을 통해 완벽한 안심을 누리세요. 이 단일 솔루션을 사용하면 다중 프로토콜 워크로드를 빠르고 쉽게 추가할 수 있습니다. 레거시 환경에서도 Windows 및 Linux 파일 기반 애플리케이션을 빌드하고 배포할 수 있습니다.

게스트 연결 스토리지로서의 **Azure NetApp Files (ANF)**

▼ **Azure VMware** 솔루션**(AVS)**을 사용하여 **Azure NetApp Files** 구성

Azure NetApp Files 공유는 Azure VMware Solution SDDC 환경에서 생성된 VM에서 마운트할 수 있습니다. Azure NetApp Files SMB 및 NFS 프로토콜을 지원하므로 볼륨을 Linux 클라이언트에 마운트하고 Windows

클라이언트에 매핑할 수도 있습니다. Azure NetApp Files 볼륨은 5가지 간단한 단계로 설정할 수 있습니다.

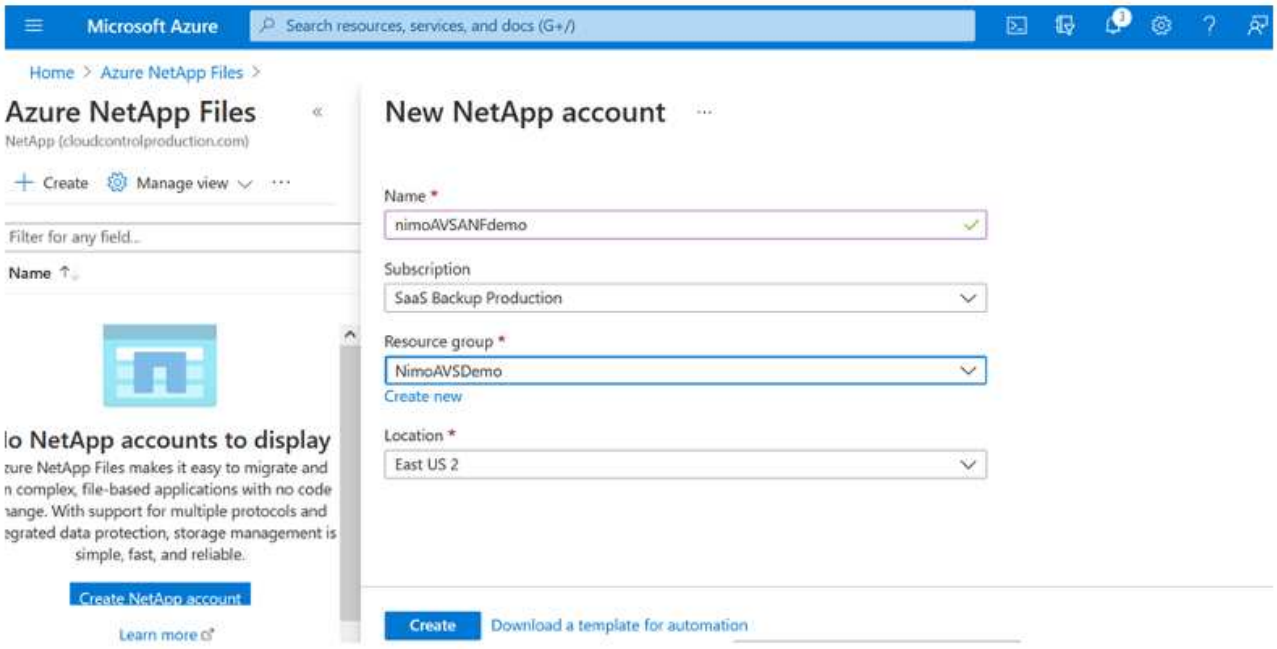
Azure NetApp Files 와 Azure VMware Solution은 동일한 Azure 지역에 있어야 합니다.

▼ **Azure NetApp Files** 볼륨 만들기 및 마운트

Azure NetApp Files 볼륨을 만들고 탑재하려면 다음 단계를 완료하세요.

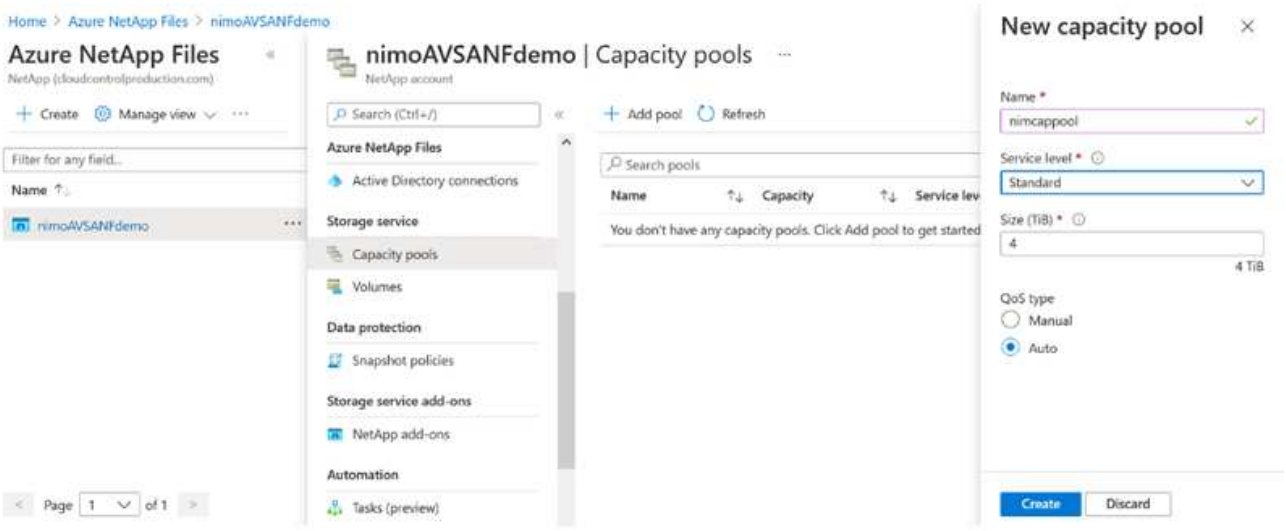
1. Azure Portal에 로그인하여 Azure NetApp Files 액세스합니다. Azure NetApp Files 서비스에 대한 액세스를 확인하고 *az provider register --namespace NetApp –wait* 명령을 사용하여 Azure NetApp Files 리소스 공급자를 등록합니다. 등록이 완료되면 NetApp 계정을 만드세요.

   자세한 단계는 다음을 참조하세요."Azure NetApp Files 공유" . 이 페이지에서는 단계별 과정을 안내해 드립니다.

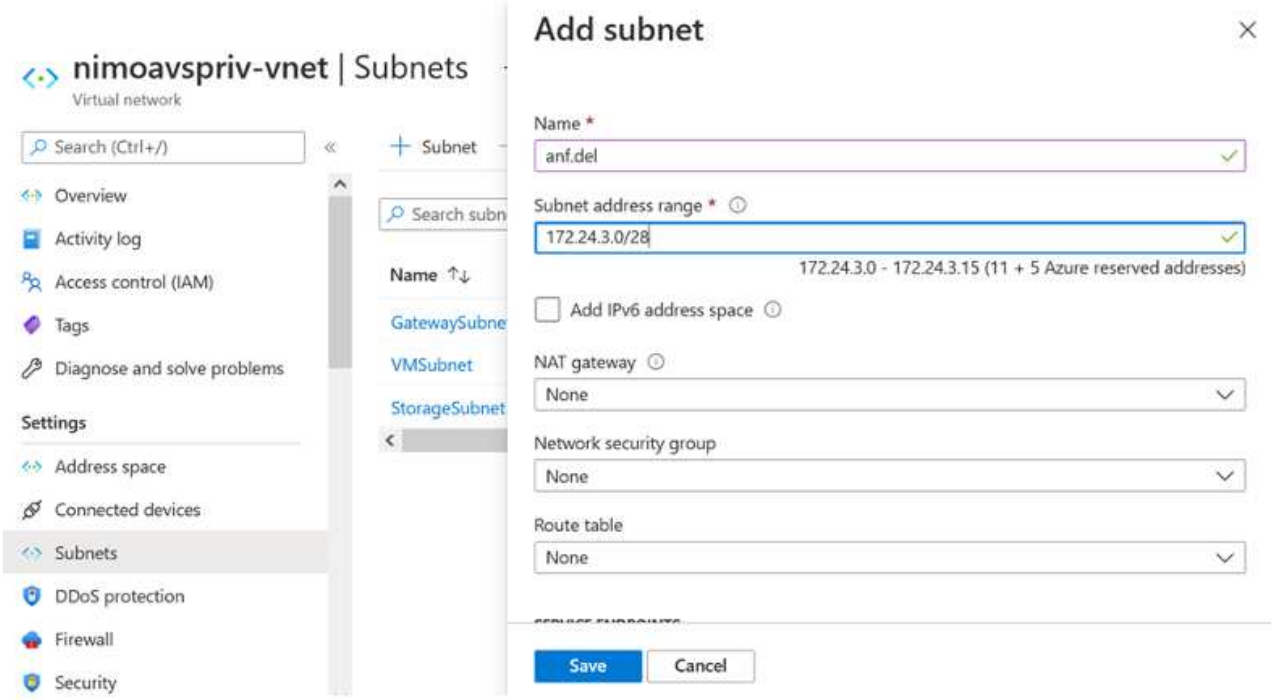


2. NetApp 계정을 만든 후 필요한 서비스 수준과 크기로 용량 풀을 설정합니다.

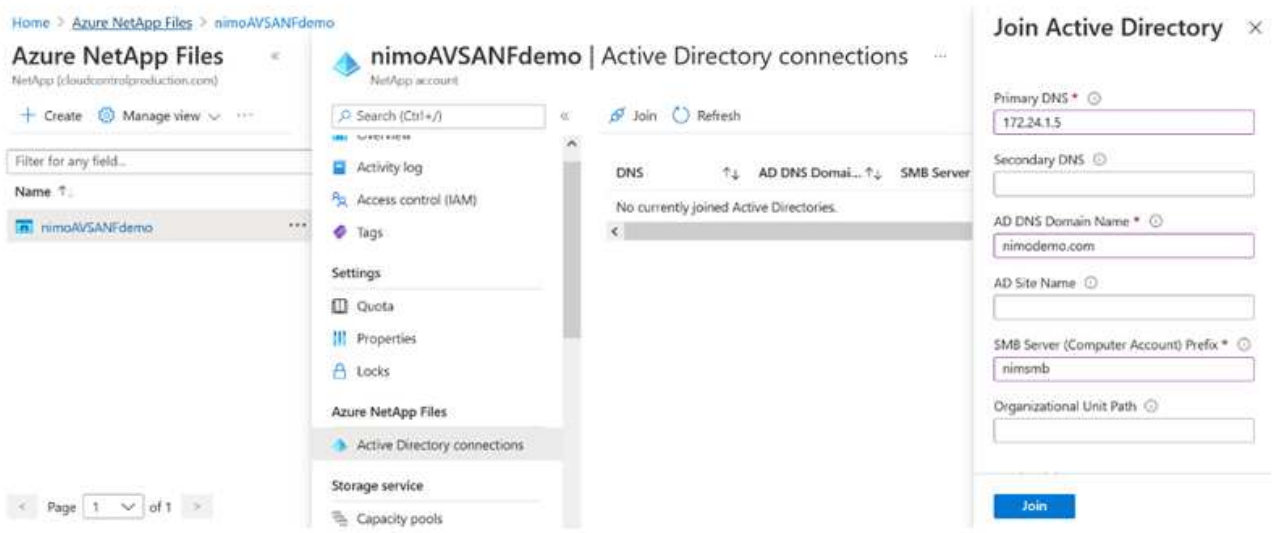
   자세한 내용은 다음을 참조하세요. "용량 풀 설정" .



3. Azure NetApp Files 대한 위임된 서브넷을 구성하고 볼륨을 만드는 동안 이 서브넷을 지정합니다. 위임된 서브넷을 만드는 자세한 단계는 다음을 참조하세요."Azure NetApp Files 에 서브넷 위임" .

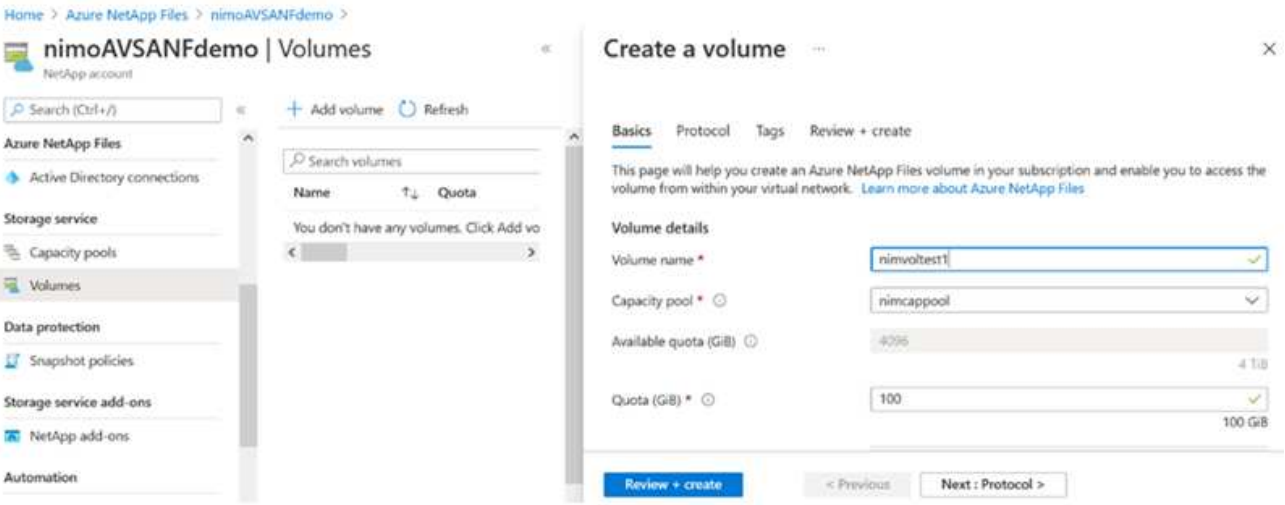


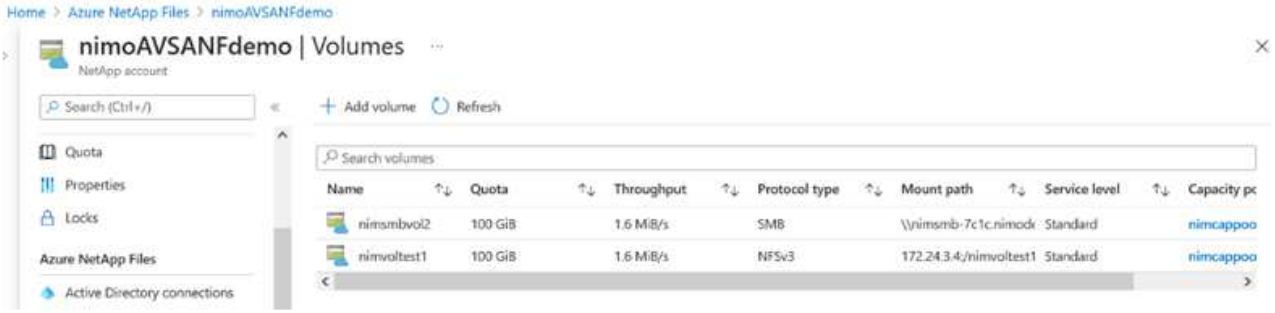
4. 용량 풀 블레이드 아래의 볼륨 블레이드를 사용하여 SMB 볼륨을 추가합니다. SMB 볼륨을 생성하기 전에 Active Directory 커넥터가 구성되어 있는지 확인하세요.



5. 검토 + 생성을 클릭하여 SMB 볼륨을 생성합니다.

   애플리케이션이 SQL Server인 경우 SMB 지속적 가용성을 활성화합니다.

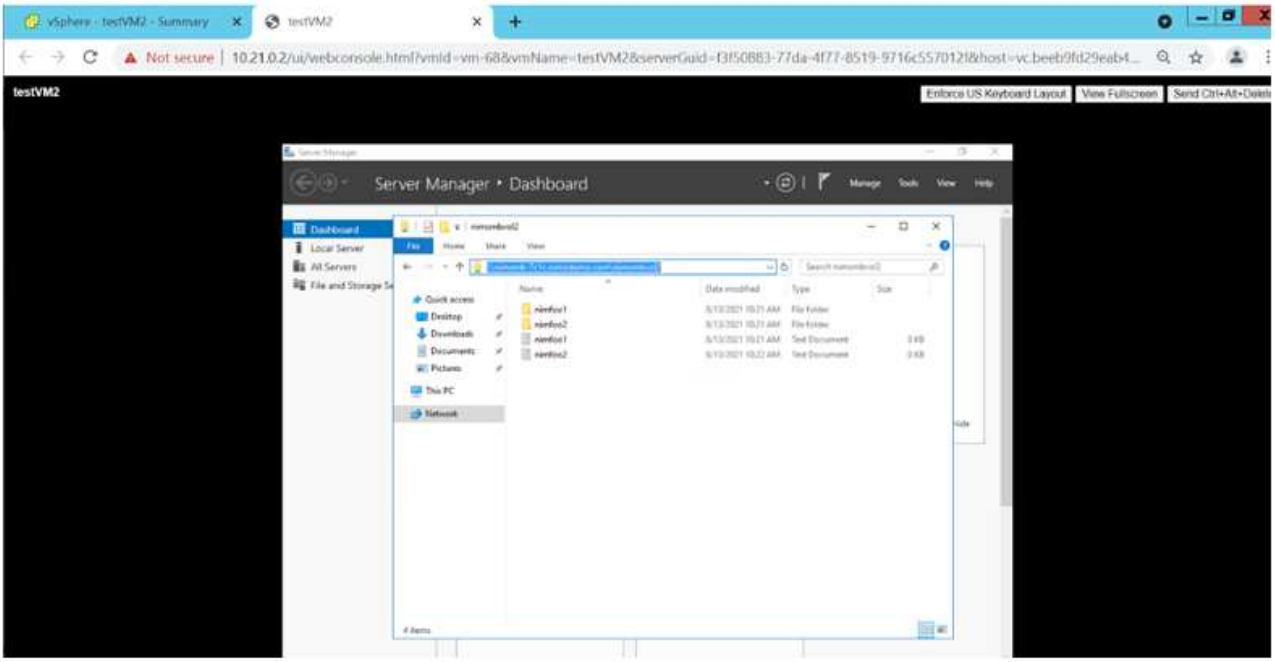


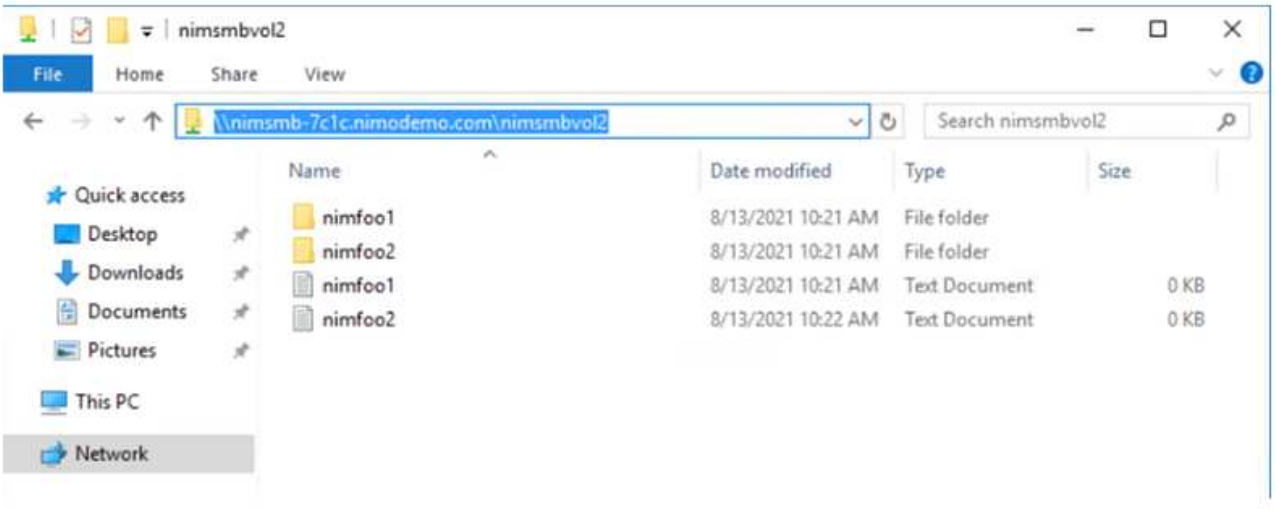


크기 또는 할당량별 Azure NetApp Files 볼륨 성능에 대해 자세히 알아보려면 다음을 참조하세요."Azure NetApp Files 에 대한 성능 고려 사항" .

6. 연결이 설정되면 볼륨을 마운트하여 애플리케이션 데이터에 사용할 수 있습니다.

   이를 수행하려면 Azure Portal에서 볼륨 블레이드를 클릭한 다음, 탑재할 볼륨을 선택하고 탑재 지침에 액세스합니다. 경로를 복사하고 네트워크 드라이브 매핑 옵션을 사용하여 Azure VMware Solution SDDC에서 실행되는 VM에 볼륨을 마운트합니다.





7. Azure VMware Solution SDDC에서 실행되는 Linux VM에 NFS 볼륨을 마운트하려면 동일한 프로세스를 사용합니다. 볼륨 재조정이나 동적 서비스 수준 기능을 사용하여 작업 부하 수요를 충족합니다.

```
nimoadmin@nimoadmin-virtual-machine:~$ sudo mount -t nfs -o rw,hard,tcp 172.24.
3.4:/nimodemonfsv1 /home/nimoadmin/nimodemo11
nimoadmin@nimoadmin-virtual-machine:~$ df
Filesystem                  1K-blocks     Used Available Use% Mounted on
udev                          8168112        0   8168112   0% /dev
tmpfs                         1639548     1488   1638060   1% /run
/dev/sda5                    50824704  7902752  40310496  17% /
tmpfs                         8197728        0   8197728   0% /dev/shm
tmpfs                            5120        0      5120   0% /run/lock
tmpfs                         8197728        0   8197728   0% /sys/fs/cgroup
/dev/loop0                      56832    56832         0 100% /snap/core18/2128
/dev/loop2                      66688    66688         0 100% /snap/gtk-common-the
mes/1515
/dev/loop1                     224256   224256         0 100% /snap/gnome-3-34-188
4/72
/dev/loop3                      52224    52224         0 100% /snap/snap-store/547
/dev/loop4                      33152    33152         0 100% /snap/snapd/12704
/dev/sda1                      523248        4    523244   1% /boot/efi
tmpfs                         1639544       52   1639492   1% /run/user/1000
/dev/sr0                        54738    54738         0 100% /media/nimoadmin/VMw
are Tools
172.24.3.4:/nimodemonfsv1 104857600        0 104857600   0% /home/nimoadmin/nimo
demo11
nimoadmin@nimoadmin-virtual-machine:~$
```

자세한 내용은 다음을 참조하세요. "볼륨의 서비스 수준을 동적으로 변경합니다." .

Cloud Volumes ONTAP (CVO)

클라우드 볼륨 ONTAP 또는 CVO는 NetApp의 ONTAP 스토리지 소프트웨어를 기반으로 구축된 업계 최고의 클라우드 데이터 관리 솔루션으로, Amazon Web Services(AWS), Microsoft Azure 및 Google Cloud Platform(GCP)에서 기본적으로 제공됩니다.

ONTAP 은 클라우드 기반 스토리지를 사용하는 소프트웨어 정의 버전으로, 클라우드와 온프레미스에서 동일한 스토리지 소프트웨어를 사용할 수 있어 데이터를 관리하는 완전히 새로운 방법에 대한 IT 직원의 재교육 필요성이 줄어듭니다.

CVO를 사용하면 고객은 엣지에서 데이터 센터, 클라우드로 원활하게 데이터를 이동할 수 있으며, 하이브리드 클라우드를 하나로 통합할 수 있습니다. 이 모든 기능은 단일 창 관리 콘솔인 NetApp Cloud Manager를 통해 관리할 수 있습니다.

CVO는 설계상 클라우드에서 가장 까다로운 애플리케이션도 만족시킬 수 있는 극한의 성능과 고급 데이터 관리 기능을 제공합니다.

게스트 연결 스토리지로서의 **Cloud Volumes ONTAP (CVO)**

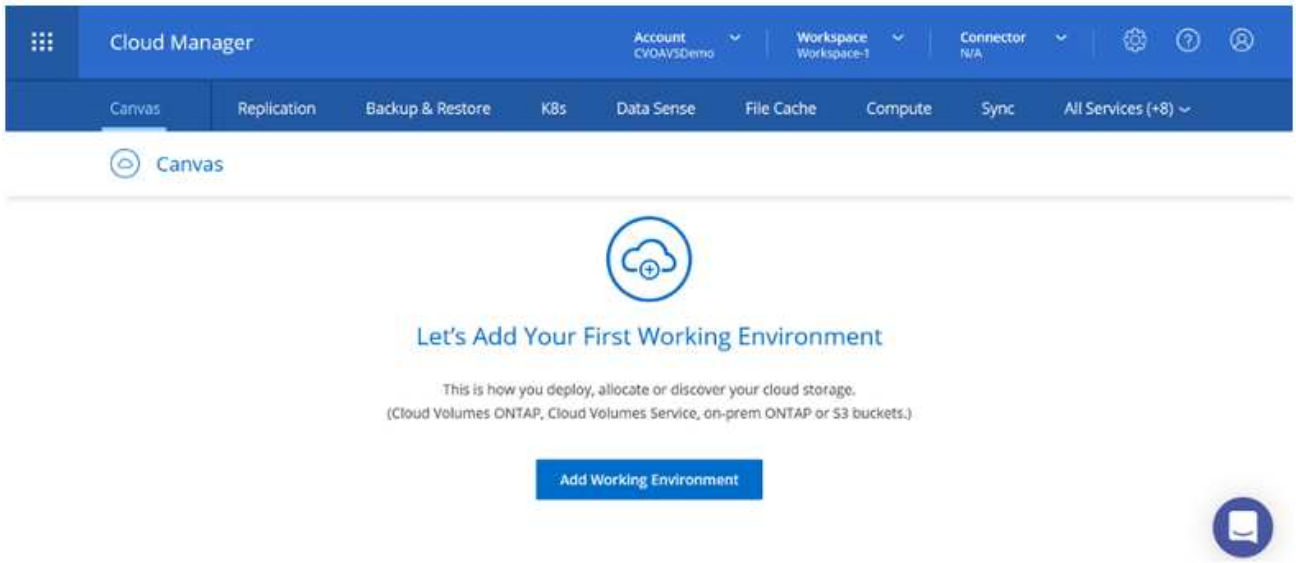
▼ **Azure**에 새로운 **Cloud Volumes ONTAP** 배포

Cloud Volumes ONTAP 공유 및 LUN은 Azure VMware Solution SDDC 환경에서 생성된 VM에서 마운트할 수 있습니다. Cloud Volumes ONTAP iSCSI, SMB, NFS 프로토콜을 지원하므로 볼륨을 Linux 클라이언트와 Windows 클라이언트에도 마운트할 수 있습니다. Cloud Volumes ONTAP 볼륨은 몇 가지 간단한 단계로 설정할 수 있습니다.

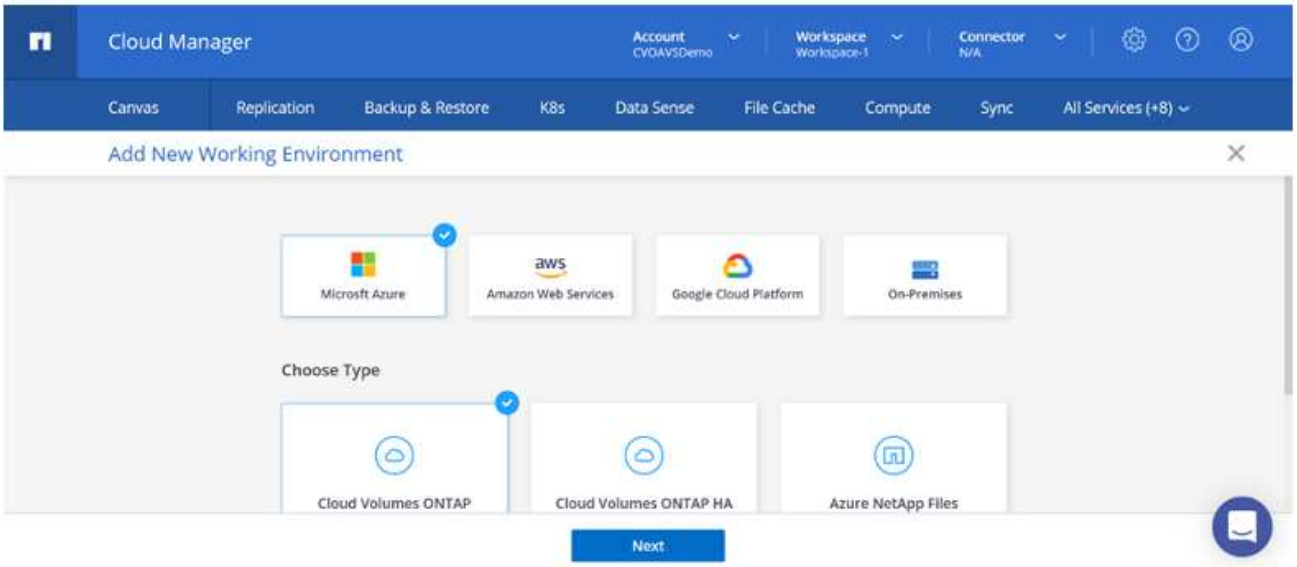
재해 복구나 마이그레이션 목적으로 온프레미스 환경에서 클라우드로 볼륨을 복제하려면 사이트 간 VPN이나 ExpressRoute를 사용하여 Azure에 대한 네트워크 연결을 설정합니다. 온프레미스에서 Cloud Volumes ONTAP으로 데이터를 복제하는 내용은 이 문서의 범위를 벗어납니다. 온프레미스와 Cloud Volumes ONTAP 시스템 간에 데이터를 복제하려면 다음을 참조하세요."시스템 간 데이터 복제 설정" .

"Cloud Volumes ONTAP 사이저"을(를) 사용하여 Cloud Volumes ONTAP 인스턴스의 크기를 정확하게 조정하십시오. 또한 온프레미스 성능을 모니터링하여 Cloud Volumes ONTAP sizer의 입력으로 사용하십시오.

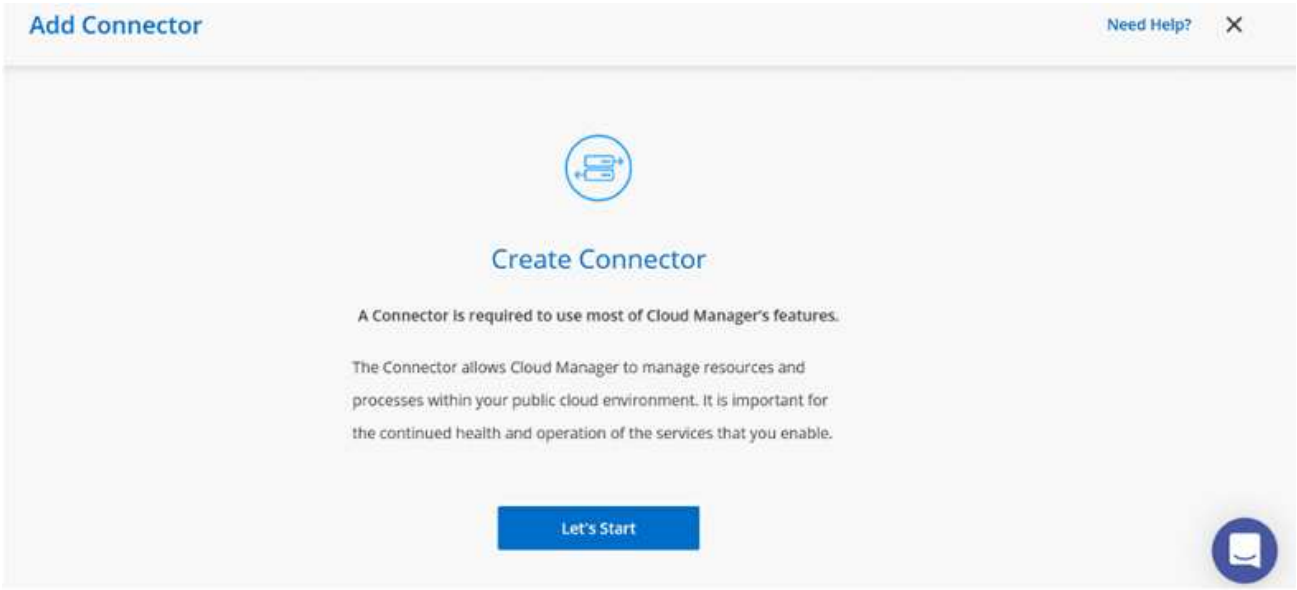
1. NetApp Cloud Central에 로그인하면 Fabric View 화면이 표시됩니다. Cloud Volumes ONTAP 탭을 찾아 Cloud Manager로 이동을 선택합니다. 로그인 후 Canvas 화면이 표시됩니다.



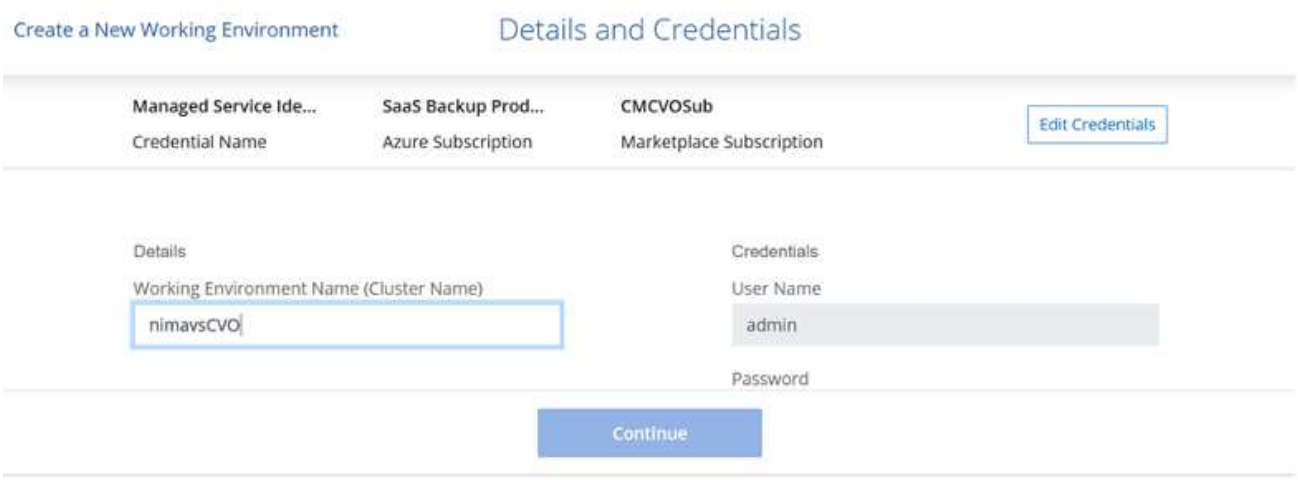
2. 클라우드 관리자 홈페이지에서 작업 환경 추가를 클릭한 다음 클라우드로 Microsoft Azure를 선택하고 시스템 구성 유형을 선택합니다.



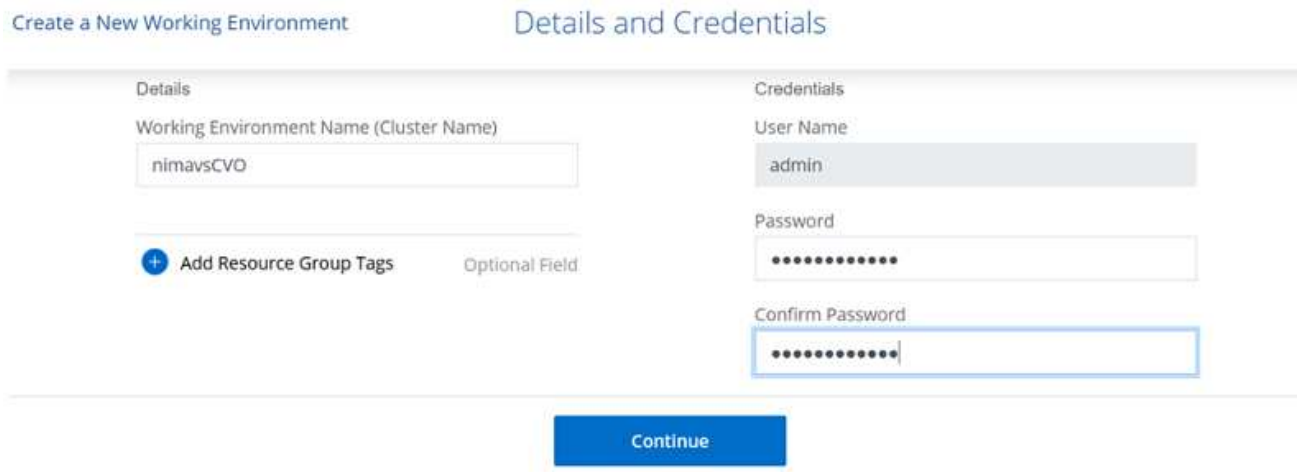
3. 첫 번째 Cloud Volumes ONTAP 작업 환경을 만들 때 Cloud Manager는 커넥터를 배포하라는 메시지를 표시합니다.



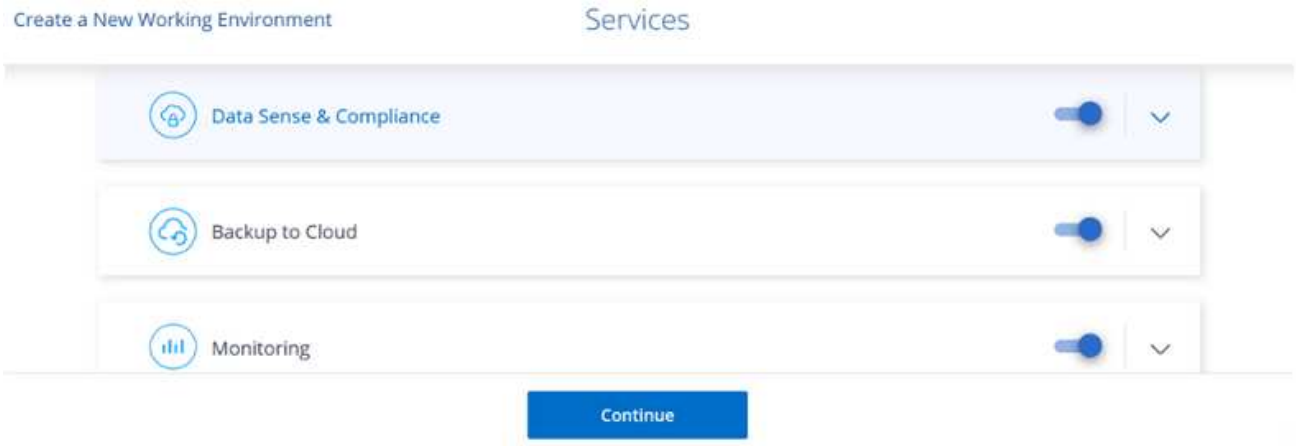
4. 커넥터가 생성된 후 세부 정보 및 자격 증명 필드를 업데이트합니다.



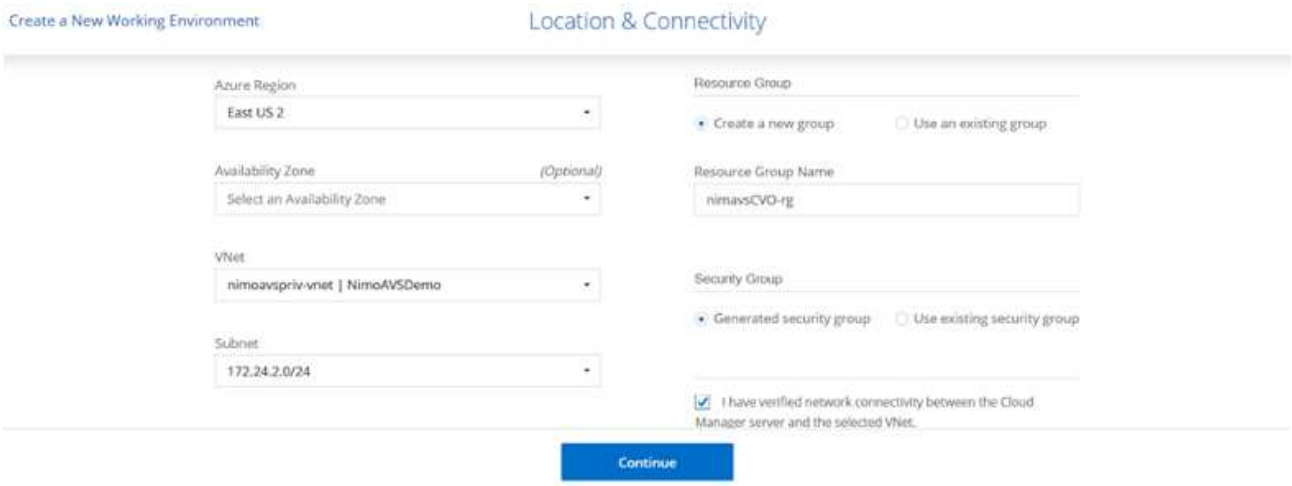
5. 환경 이름과 관리자 자격 증명을 포함하여 생성할 환경에 대한 세부 정보를 제공합니다. Azure 환경에 대한 리소스 그룹 태그를 선택적 매개변수로 추가합니다. 완료되면 계속을 클릭하세요.



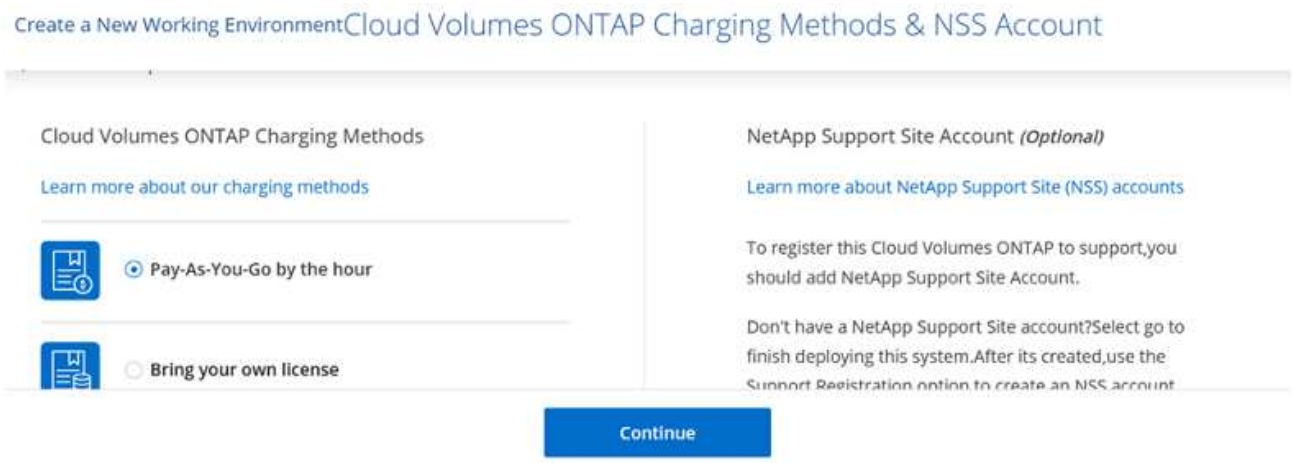
6. NetApp Data Classification, NetApp Backup and Recovery, Data Infrastructure Insights 등 Cloud Volumes ONTAP 배포를 위한 애드온 서비스를 선택합니다. 서비스를 선택한 다음 계속을 클릭합니다.



7. Azure 위치와 연결을 구성합니다. 사용할 Azure 지역, 리소스 그룹, VNet 및 서브넷을 선택합니다.



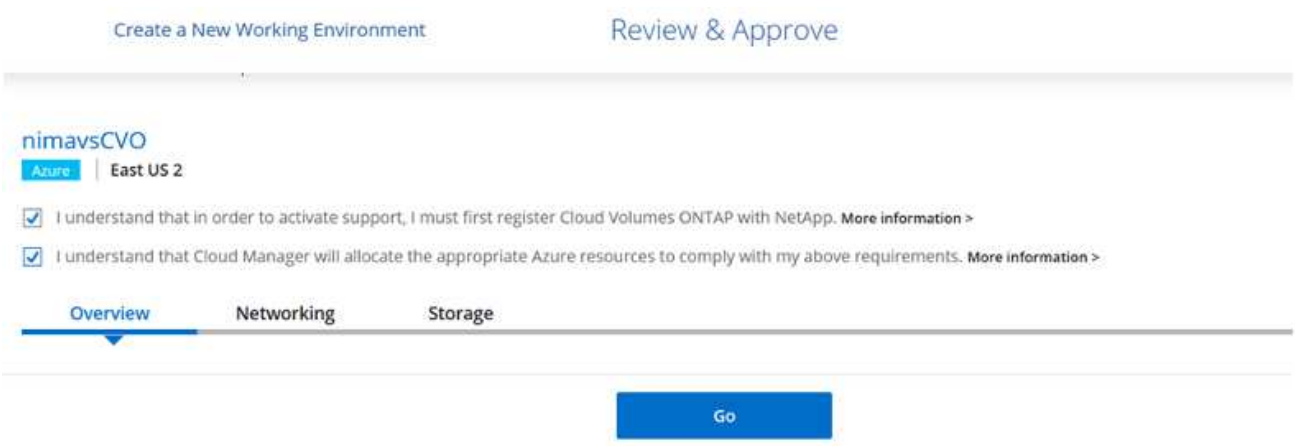
8. 라이선스 옵션을 선택하세요: Pay-As-You-Go 또는 기존 라이선스를 사용하는 BYOL. 이 예에서는 Pay-As-You-Go 옵션이 사용되었습니다.



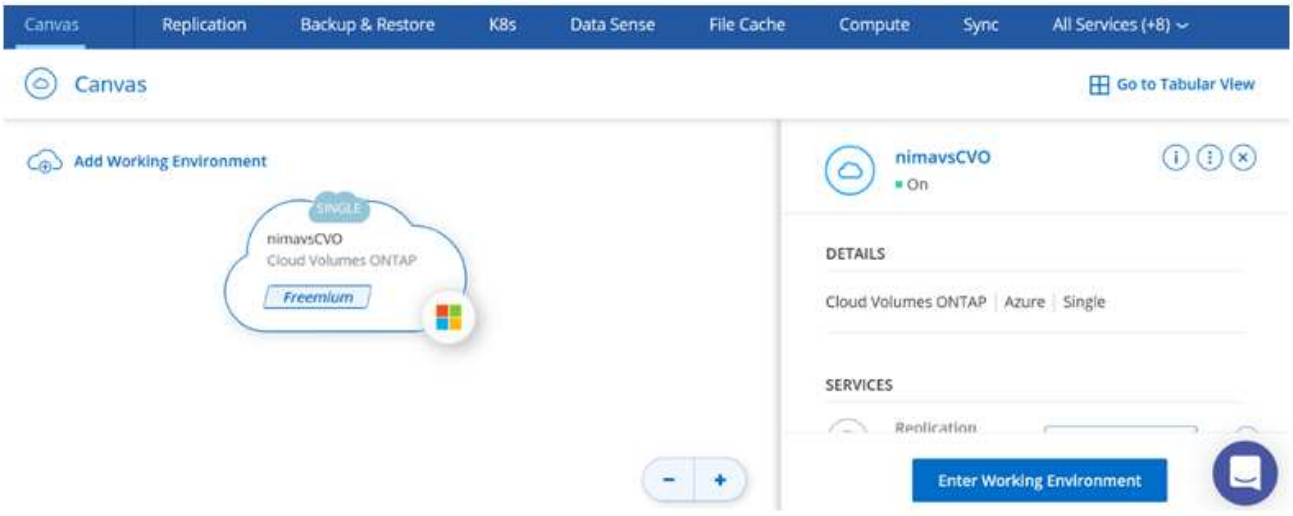
9. 다양한 유형의 워크로드에 맞게 미리 구성된 여러 패키지 중에서 선택하세요.



10. 지원 활성화 및 Azure 리소스 할당과 관련된 두 가지 계약을 수락합니다 . Cloud Volumes ONTAP 인스턴스를 만들려면 이동을 클릭합니다.

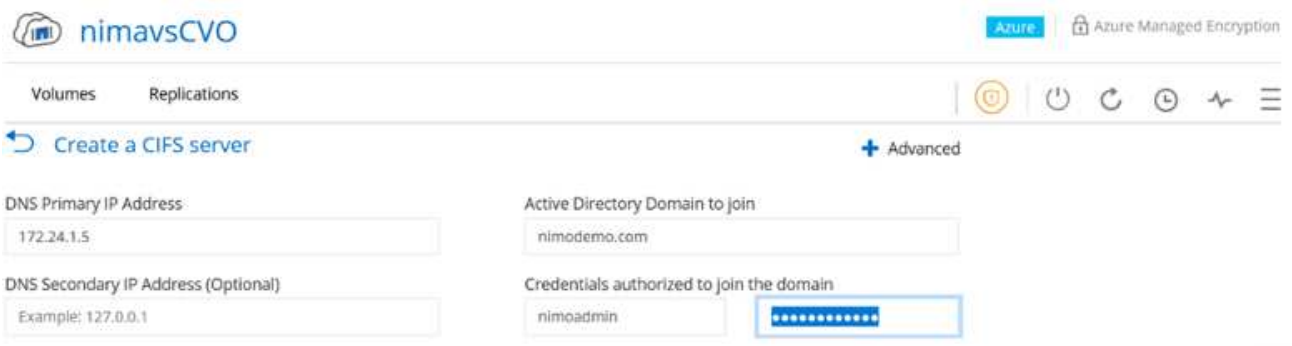


11. Cloud Volumes ONTAP 이 프로비저닝되면 Canvas 페이지의 작업 환경에 나열됩니다.

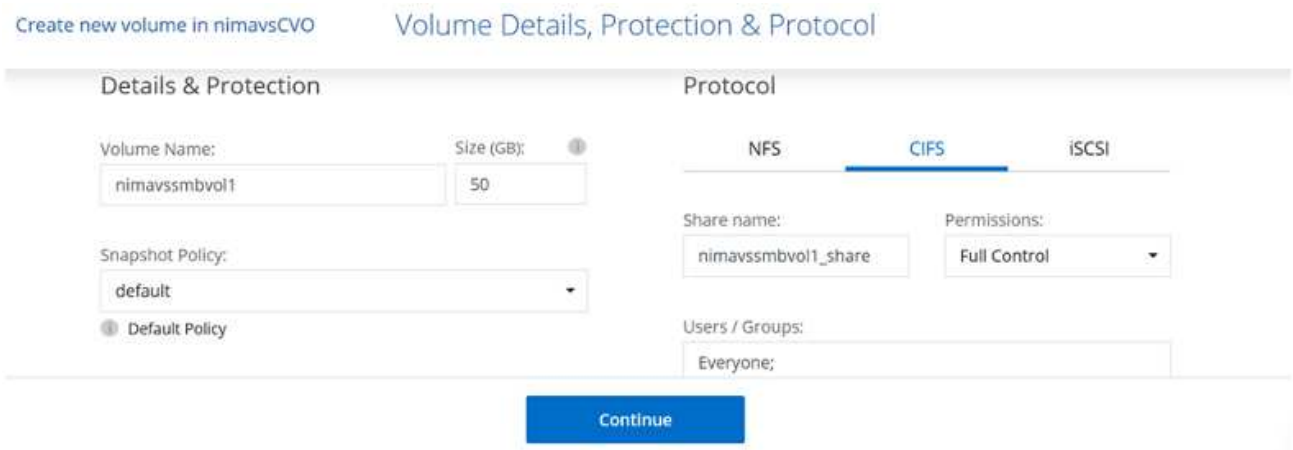


▼ **SMB** 볼륨에 대한 추가 구성

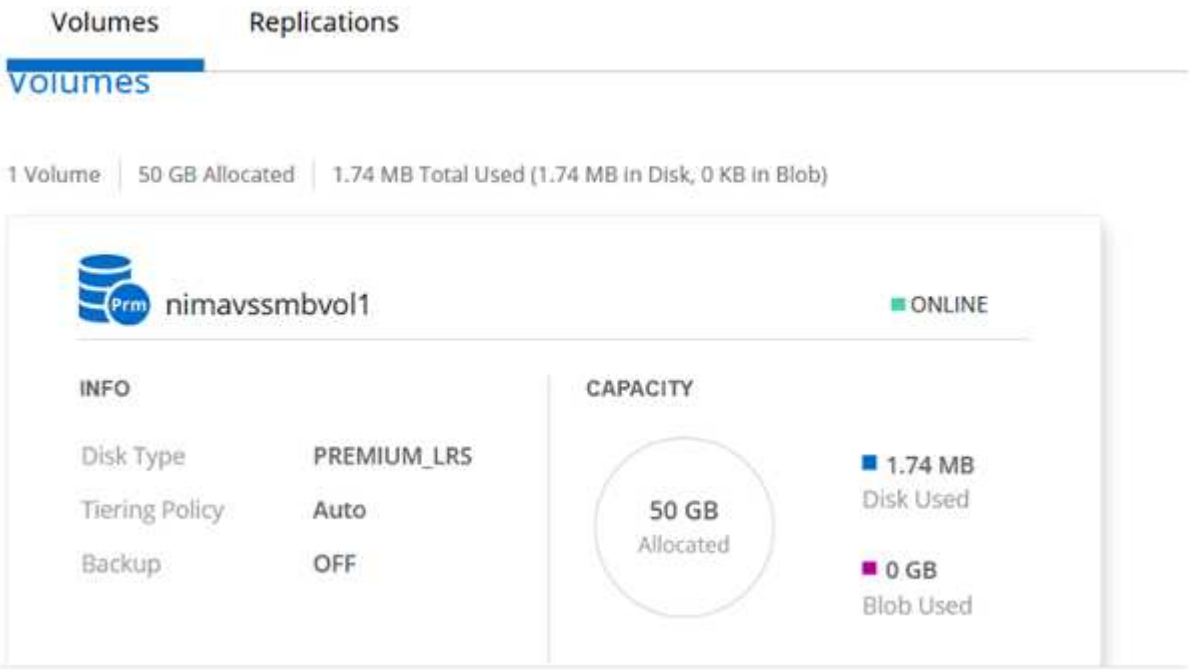
1. 작업 환경이 준비되면 CIFS 서버가 적절한 DNS 및 Active Directory 구성 매개변수로 구성되었는지 확인하세요. SMB 볼륨을 생성하려면 이 단계가 필요합니다.



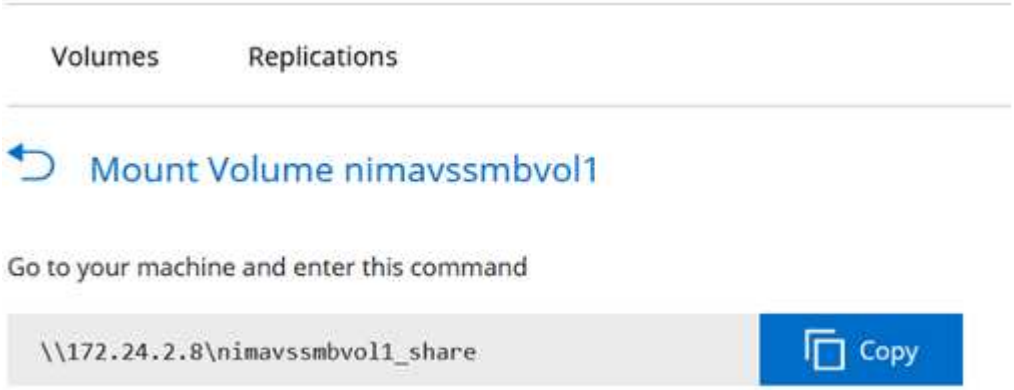
2. SMB 볼륨을 만드는 것은 간단한 과정입니다. 볼륨을 생성할 CVO 인스턴스를 선택하고 볼륨 생성 옵션을 클릭합니다. 적절한 크기를 선택하면 클라우드 관리자가 포함된 집계를 선택하거나 고급 할당 메커니즘을 사용하여 특정 집계에 배치합니다. 이 데모에서는 프로토콜로 SMB가 선택되었습니다.

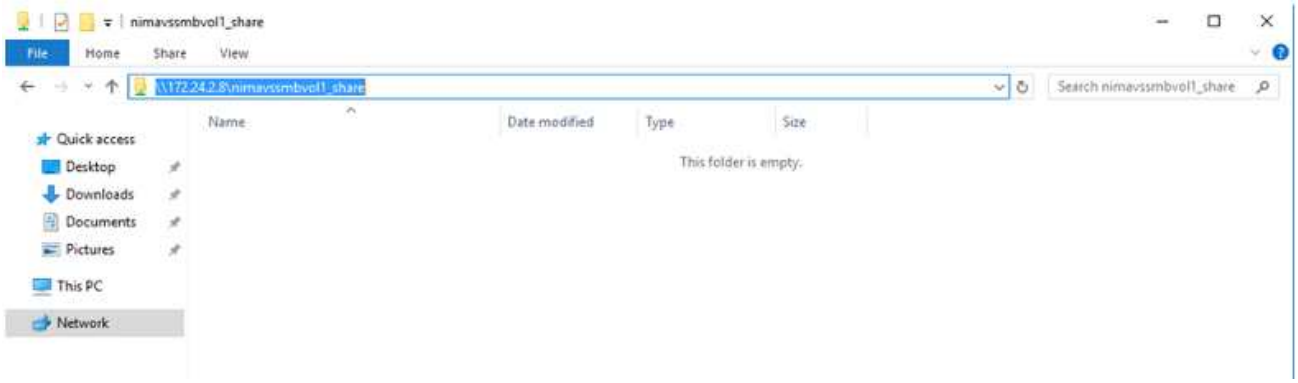


3. 볼륨이 프로비저닝된 후에는 볼륨 창에서 사용할 수 있습니다. CIFS 공유가 프로비저닝되므로 사용자 또는 그룹에 파일과 폴더에 대한 권한을 부여하고 해당 사용자가 공유에 액세스하여 파일을 만들 수 있는지 확인하세요. 볼륨이 온-프레미스 환경에서 복제된 경우 파일 및 폴더 권한이 모두 SnapMirror 복제의 일부로 유지되므로 이 단계는 필요하지 않습니다.



4. 볼륨이 생성된 후 mount 명령을 사용하여 Azure VMware Solution SDDC 호스트에서 실행되는 VM에서 공유에 연결합니다.
5. 다음 경로를 복사하고 네트워크 드라이브 매핑 옵션을 사용하여 Azure VMware Solution SDDC에서 실행되는 VM에 볼륨을 마운트합니다.

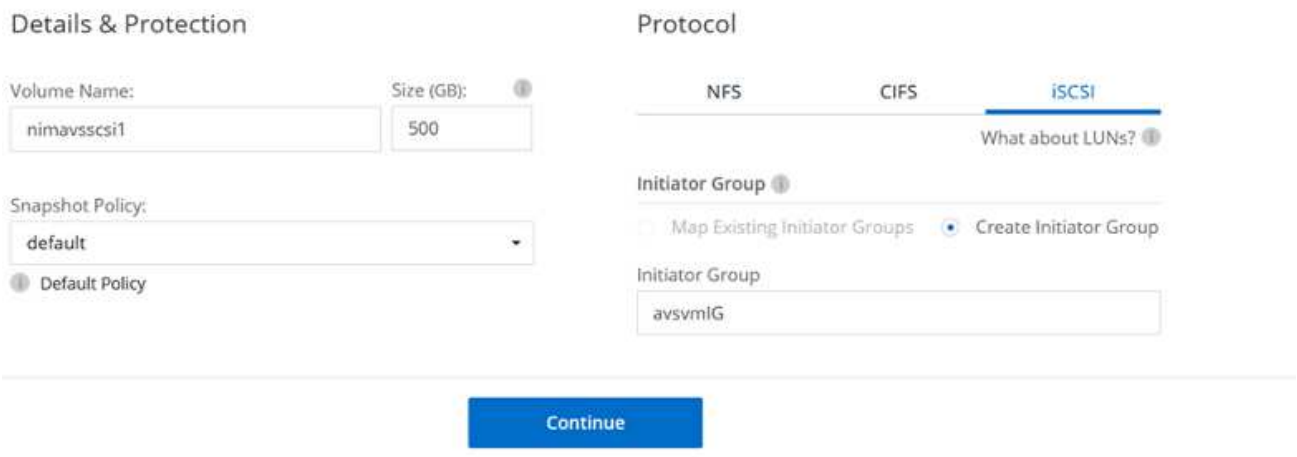




▼ **LUN**을 호스트에 연결합니다

LUN을 호스트에 연결하려면 다음 단계를 완료하세요.

1. Canvas 페이지에서 Cloud Volumes ONTAP 작업 환경을 두 번 클릭하여 볼륨을 만들고 관리합니다.
2. 볼륨 추가 > 새 볼륨을 클릭하고 iSCSI를 선택한 후 초기자 그룹 만들기를 클릭합니다. 계속을 클릭하세요.



3. 볼륨이 프로비저닝된 후 볼륨을 선택한 다음 대상 IQN을 클릭합니다. iSCSI 정규 이름(IQN)을 복사하려면 복사를 클릭합니다. 호스트에서 LUN으로 iSCSI 연결을 설정합니다.

   Azure VMware Solution SDDC에 있는 호스트에 대해 동일한 작업을 수행하려면 다음을 수행합니다.

   a. Azure VMware Solution SDDC에 호스팅된 VM에 대한 RDP.

b. iSCSI 초기자 속성 대화 상자를 엽니다: 서버 관리자 > 대시보드 > 도구 > iSCSI 초기자.

c. 검색 탭에서 포털 검색 또는 포털 추가를 클릭한 다음 iSCSI 대상 포트의 IP 주소를 입력합니다.

d. 대상 탭에서 검색된 대상을 선택한 다음 로그온 또는 연결을 클릭합니다.

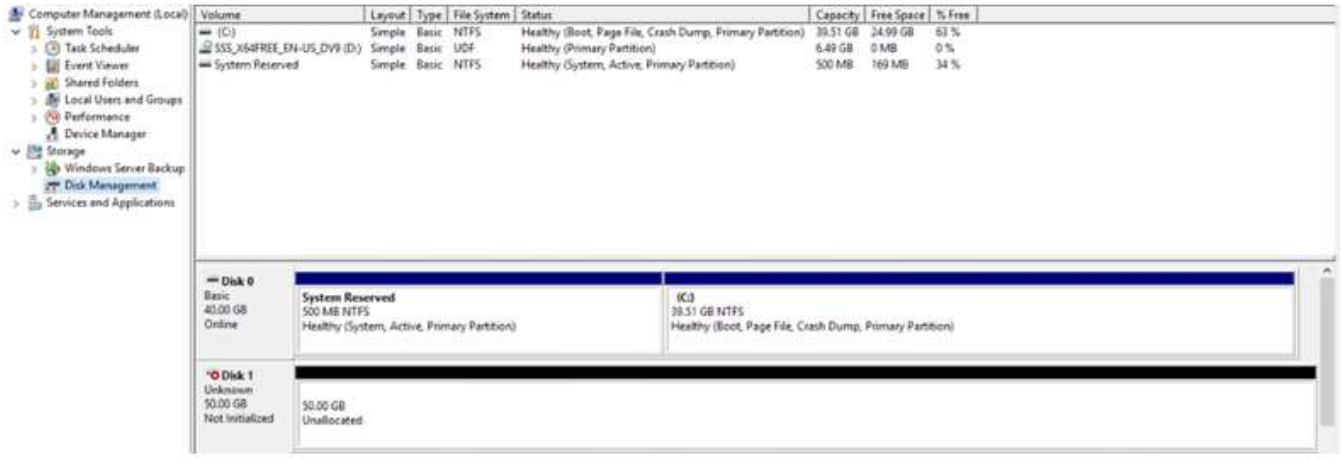
e. 다중 경로 사용을 선택한 다음 컴퓨터 시작 시 이 연결을 자동으로 복원 또는 이 연결을 즐겨찾기 대상 목록에 추가를 선택합니다. 고급을 클릭합니다.

   참고**:** Windows 호스트는 클러스터의 각 노드에 iSCSI 연결이 있어야 합니다. 기본 DSM은 사용할 가장 좋은 경로를 선택합니다.



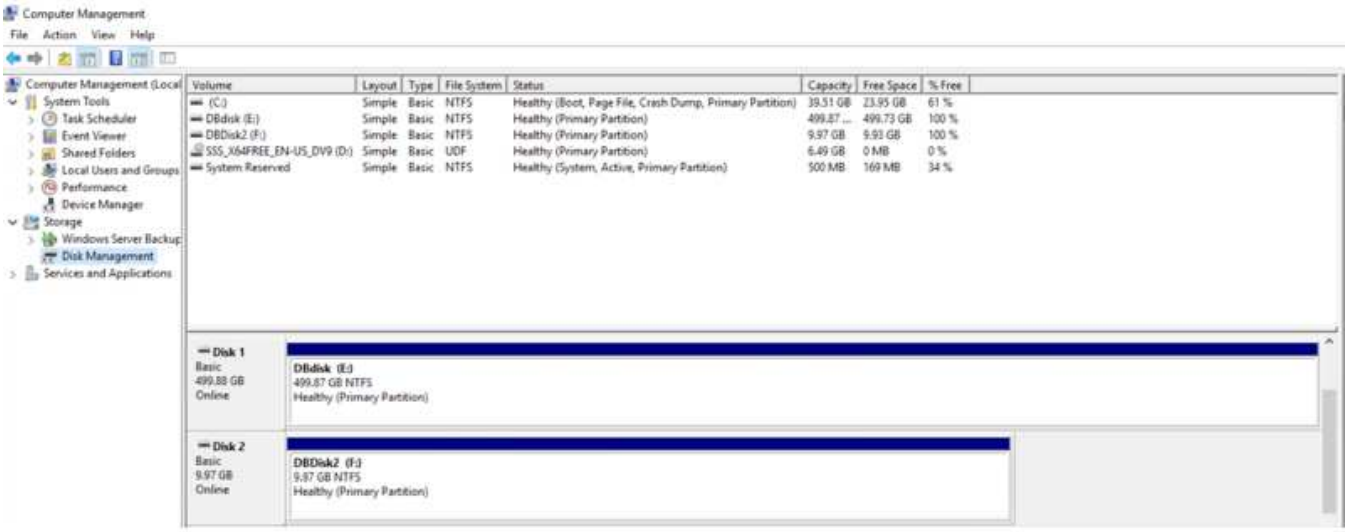
스토리지 가상 머신(SVM)의 LUN은 Windows 호스트에 디스크로 표시됩니다. 새로 추가된 디스크는 호스트에서 자동으로 검색되지 않습니다. 다음 단계를 완료하여 디스크를 검색하기 위한 수동 재검사를 트리거합니다.

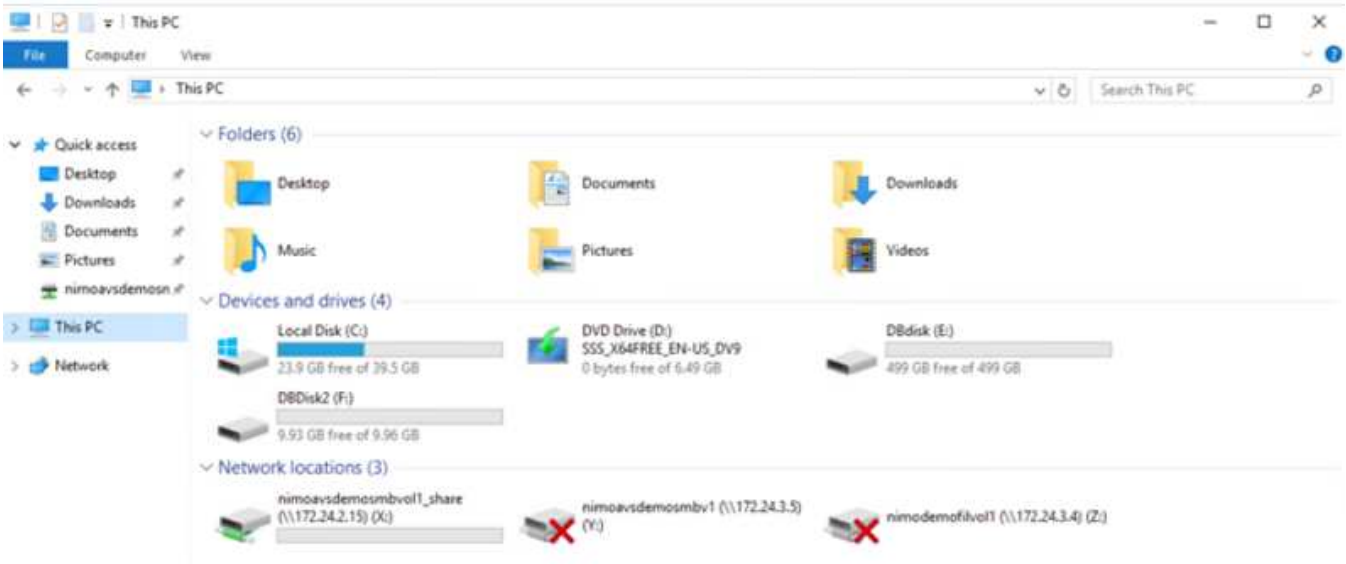
1. Windows 컴퓨터 관리 유틸리티를 엽니다: 시작 > 관리 도구 > 컴퓨터 관리.
2. 탐색 트리에서 저장소 노드를 확장합니다.
3. 디스크 관리를 클릭합니다.
4. 작업 > 디스크 다시 검사를 클릭합니다.



Windows 호스트가 새 LUN에 처음 액세스할 때 파티션이나 파일 시스템이 없습니다. LUN을 초기화하고, 필요한 경우 다음 단계를 완료하여 LUN을 파일 시스템으로 포맷합니다.

1. Windows 디스크 관리를 시작합니다.
2. LUN을 마우스 오른쪽 버튼으로 클릭한 다음 필요한 디스크 또는 파티션 유형을 선택합니다.
3. 마법사의 지시를 따르세요. 이 예에서는 드라이브 E:가 마운트됩니다.





Google Cloud VMware Engine: NetApp 스토리지 사용 옵션

NetApp 스토리지는 게스트 연결 또는 보조 스토리지로 Google Cloud Virtualization Engine에 연결할 수 있습니다.

Google Cloud NetApp Volumes (NetApp Volumes)를 보조 **NFS** 데이터 저장소로 사용

Google Cloud VMware Engine(GCVE) 환경에서 추가 스토리지 용량이 필요한 고객은 Google Cloud NetApp Volumes 활용하여 보조 NFS 데이터 저장소로 마운트할 수 있습니다. Google Cloud NetApp Volumes 에 데이터를 저장하면 고객은 지역 간에 복제하여 재해로부터 보호할 수 있습니다.

자세한 내용은 다음을 방문하세요."Google Cloud NetApp Volumes (NetApp Volumes)를 보조 NFS 데이터 저장소로 사용"

게스트 연결 스토리지로서의 **NetApp CVO**

클라우드 볼륨 ONTAP 또는 CVO는 NetApp의 ONTAP 스토리지 소프트웨어를 기반으로 구축된 업계 최고의 클라우드 데이터 관리 솔루션으로, Amazon Web Services(AWS), Microsoft Azure 및 Google Cloud Platform(GCP)에서 기본적으로 제공됩니다.

ONTAP 은 클라우드 기반 스토리지를 사용하는 소프트웨어 정의 버전으로, 클라우드와 온프레미스에서 동일한 스토리지 소프트웨어를 사용할 수 있어 데이터를 관리하는 완전히 새로운 방법에 대한 IT 직원의 재교육 필요성이 줄어듭니다.

CVO를 사용하면 고객은 엣지에서 데이터 센터, 클라우드로 원활하게 데이터를 이동할 수 있으며, 하이브리드 클라우드를 하나로 통합할 수 있습니다. 이 모든 기능은 단일 창 관리 콘솔인 NetApp Cloud Manager를 통해 관리할 수 있습니다.

CVO는 설계상 클라우드에서 가장 까다로운 애플리케이션도 만족시킬 수 있는 극한의 성능과 고급 데이터 관리 기능을 제공합니다.

자세한 내용은 다음을 방문하세요."게스트 연결 스토리지로서의 NetApp CVO"

게스트 연결 스토리지로서의 **Google Cloud NetApp Volumes (NetApp Volumes)**

Google Cloud NetApp Volumes 공유는 VMware Engine 환경에서 생성된 VM에서 마운트할 수 있습니다. Google Cloud NetApp Volumes SMB 및 NFS 프로토콜을 지원하므로 볼륨을 Linux 클라이언트에 마운트하고 Windows 클라이언트에 매핑할 수도 있습니다. Google Cloud NetApp Volumes 볼륨은 간단한 단계로 설정할 수 있습니다.

Google Cloud NetApp Volumes 와 Google Cloud VMware Engine 프라이빗 클라우드는 동일한 지역에 있어야 합니다.

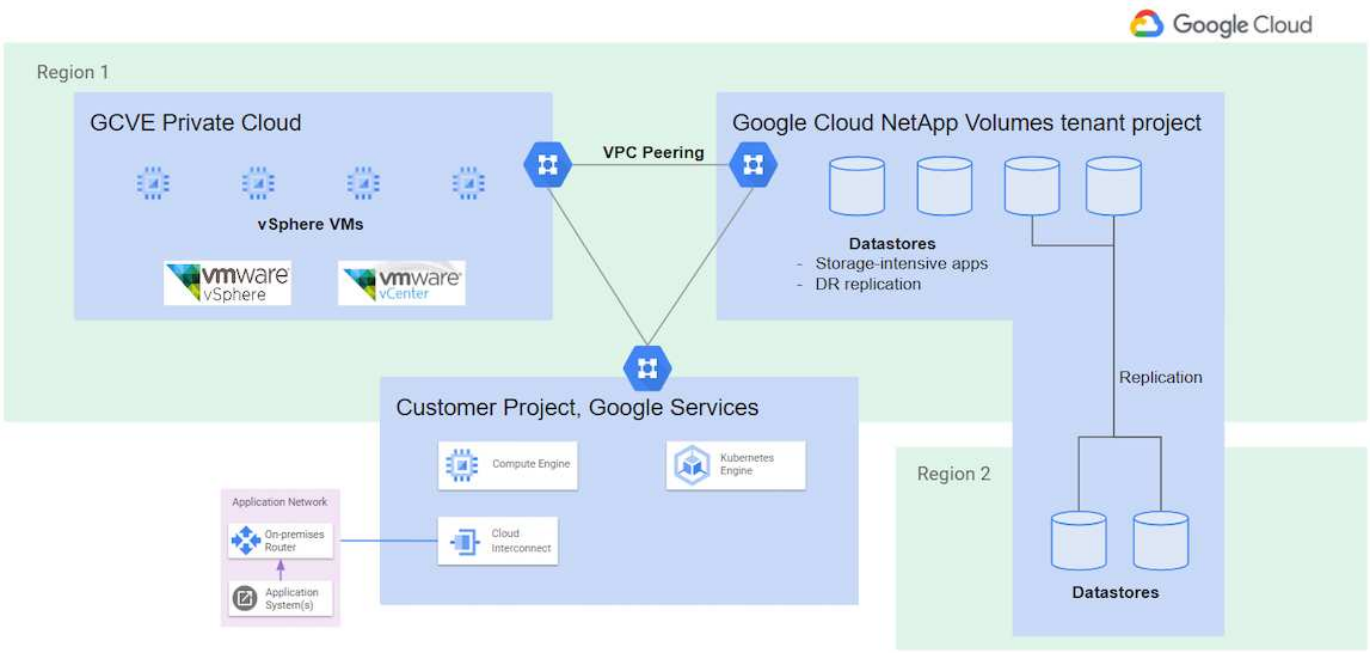
자세한 내용은 다음을 방문하세요."게스트 연결 스토리지로서의 Google Cloud NetApp Volumes (NetApp Volumes)"

Google Cloud NetApp Volumes 사용한 **Google Cloud VMware Engine** 보충 **NFS** 데이터 저장소

고객은 Google Cloud NetApp Volumes 사용하여 NFS 보충 데이터 저장소를 사용하여 Google Cloud VMware Engine의 스토리지 용량을 확장할 수 있습니다.

개요

Google Cloud VMware Engine(GCVE) 환경에서 추가 스토리지 용량이 필요한 고객은 Netapp Cloud Volume Service를 활용하여 보조 NFS 데이터 저장소로 마운트할 수 있습니다. Google Cloud NetApp Volumes 에 데이터를 저장하면 고객은 지역 간에 복제하여 재해로부터 보호할 수 있습니다.



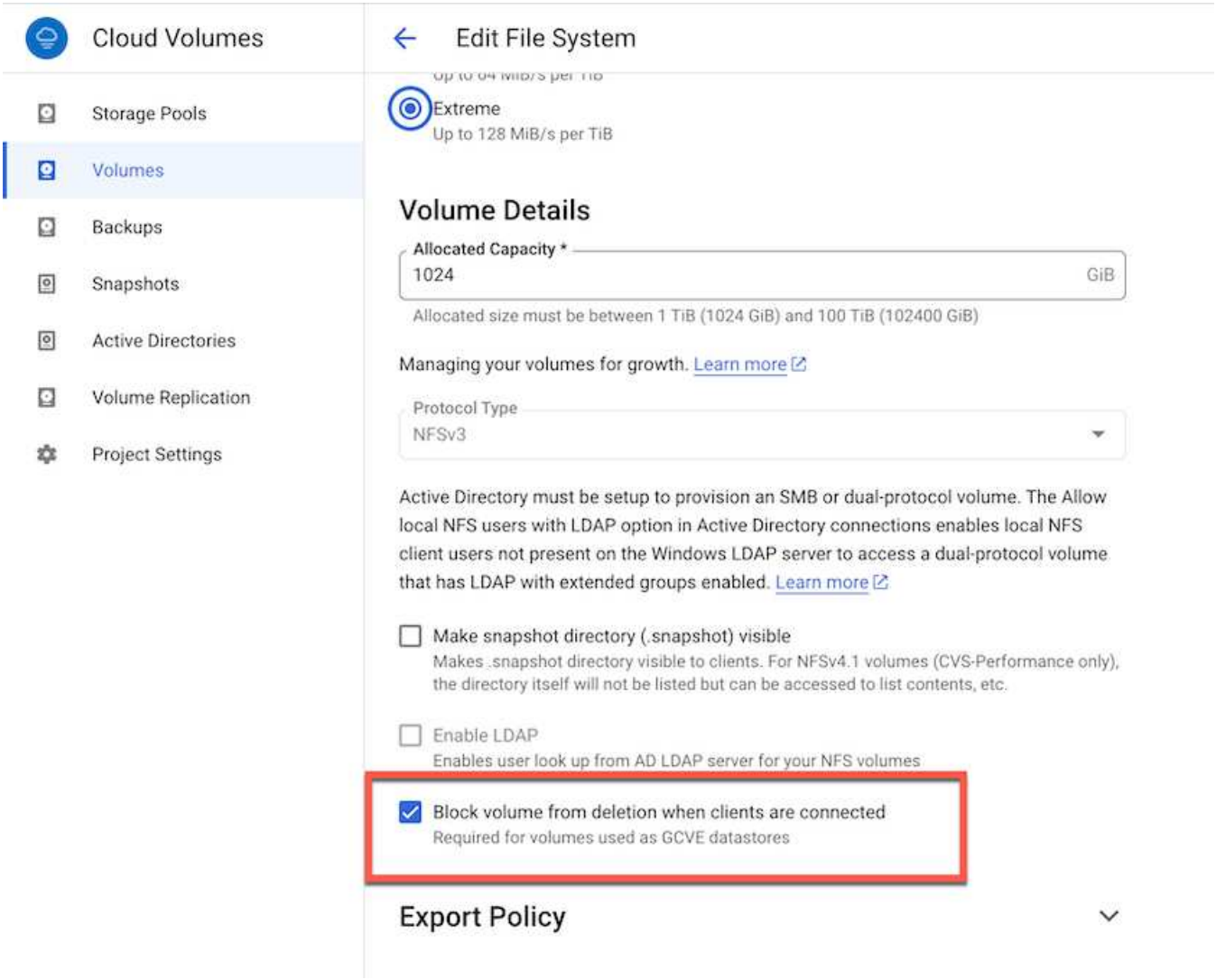
GCVE에서 **Google Cloud NetApp Volumes (NetApp Volumes)**의 **NFS** 데이터 저장소를 마운트하기 위한 배포 단계

▼ **NetApp** 볼륨 프로비저닝-성능 볼륨

Google Cloud NetApp Volumes 볼륨은 "Google Cloud Console 사용" "Google Cloud CLI 또는 API 사용"을(를) 통해 프로비저닝할 수 있습니다.

▼ **NetApp Volumes** 볼륨을 삭제할 수 없음으로 표시

가상 머신이 실행 중인 동안 볼륨이 실수로 삭제되는 것을 방지하려면 아래 스크린샷과 같이 볼륨을 삭제할 수 없도록 표시하십시오.



자세한 내용은 "NFS 볼륨 생성" 설명서를 참조하십시오.

▼ **NetApp Volumes Tenant VPC**에 대한 **GCVE**의 개인 연결이 있는지 확인하세요**.**

NFS 데이터 저장소를 마운트하려면 GCVE와 NetApp 볼륨 프로젝트 사이에 개인 연결이 있어야 합니다. 자세한 내용은 다음을 참조하세요."개인 서비스 액세스를 설정하는 방법"

▼ **NFS** 데이터 저장소 마운트

GCVE에서 NFS 데이터 저장소를 마운트하는 방법에 대한 지침은 다음을 참조하세요."NetApp Volumes를 사용하여 NFS 데이터 저장소를 만드는 방법"

vSphere 호스트는 Google에서 관리되므로 NFS vSphere API for Array Integration(VAAI) vSphere Installation Bundle(VIB)을 설치할 수 없습니다. 가상 볼륨(vVol)에 대한 지원이 필요하면 알려주시기 바랍니다. Jumbo Frames를 사용하고 싶으시다면 다음을 참조하세요."GCP에서 지원되는 최대 MTU 크기"

Google Cloud NetApp Volumes 통한 비용 절감

GCVE 스토리지 요구 사항에 맞춰 Google Cloud NetApp Volumes를 사용하여 얻을 수 있는 잠재적 비용 절감 효과에 대한 자세한 내용은 다음을 확인하십시오. "NetApp ROI 계산기"

참조 링크

- "Google 블로그 - NetApp Volumes를 Google Cloud VMware Engine의 데이터 저장소로 사용하는 방법"
- "NetApp 블로그 - 스토리지가 풍부한 앱을 Google Cloud로 마이그레이션하는 더 나은 방법"

GCP용 **NetApp** 스토리지 옵션

GCP는 Cloud Volumes ONTAP (CVO) 또는 Google Cloud NetApp Volumes (NetApp Volumes)를 통해 게스트에 연결된 NetApp 스토리지를 지원합니다.

Cloud Volumes ONTAP (CVO)

클라우드 볼륨 ONTAP 또는 CVO는 NetApp의 ONTAP 스토리지 소프트웨어를 기반으로 구축된 업계 최고의 클라우드 데이터 관리 솔루션으로, Amazon Web Services(AWS), Microsoft Azure 및 Google Cloud Platform(GCP)에서 기본적으로 제공됩니다.

ONTAP 은 클라우드 기반 스토리지를 사용하는 소프트웨어 정의 버전으로, 클라우드와 온프레미스에서 동일한 스토리지 소프트웨어를 사용할 수 있어 데이터를 관리하는 완전히 새로운 방법에 대한 IT 직원의 재교육 필요성이 줄어듭니다.

CVO를 사용하면 고객은 엣지에서 데이터 센터, 클라우드로 원활하게 데이터를 이동할 수 있으며, 하이브리드 클라우드를 하나로 통합할 수 있습니다. 이 모든 기능은 단일 창 관리 콘솔인 NetApp Cloud Manager를 통해 관리할 수 있습니다.

CVO는 설계상 클라우드에서 가장 까다로운 애플리케이션도 만족시킬 수 있는 극한의 성능과 고급 데이터 관리 기능을 제공합니다.

게스트 연결 스토리지로서의 **Cloud Volumes ONTAP (CVO)**

▼ **Google Cloud**에 **Cloud Volumes ONTAP** 배포(직접 해보기)

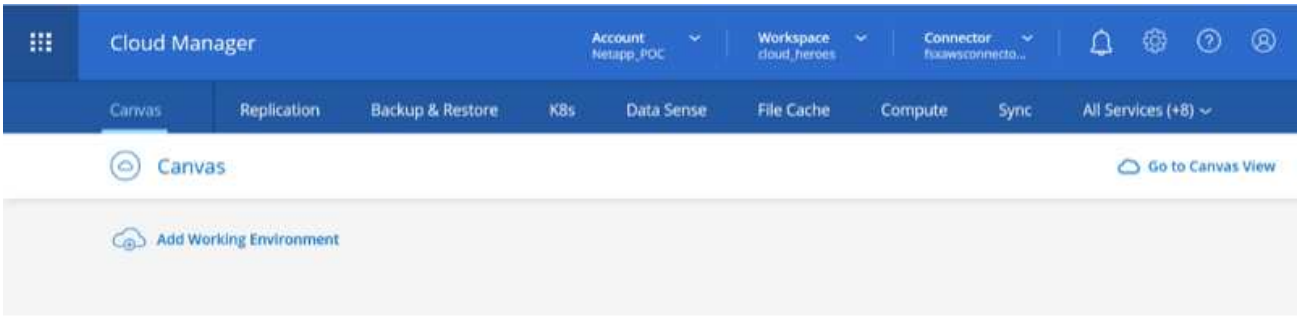
Cloud Volumes ONTAP 공유 및 LUN은 GCVE 프라이빗 클라우드 환경에서 생성된 VM에서 마운트될 수 있습니다. Cloud Volumes ONTAP iSCSI, SMB, NFS 프로토콜을 지원하므로 볼륨은 Linux 클라이언트와 Windows 클라이언트에 마운트할 수 있으며 LUN은 iSCSI를 통해 마운트될 때 블록 장치로 Linux 또는 Windows 클라이언트에 액세스할 수 있습니다. Cloud Volumes ONTAP 볼륨은 몇 가지 간단한 단계로 설정할 수 있습니다.

재해 복구나 마이그레이션 목적으로 온프레미스 환경에서 클라우드로 볼륨을 복제하려면 사이트 간 VPN이나 Cloud Interconnect를 사용하여 Google Cloud에 대한 네트워크 연결을 설정합니다. 온프레미스에서 Cloud Volumes ONTAP 으로 데이터를 복제하는 내용은 이 문서의 범위를 벗어납니다. 온프레미스와 Cloud Volumes ONTAP 시스템 간에 데이터를 복제하려면 다음을 참조하세요."시스템 간 데이터 복제 설정" .

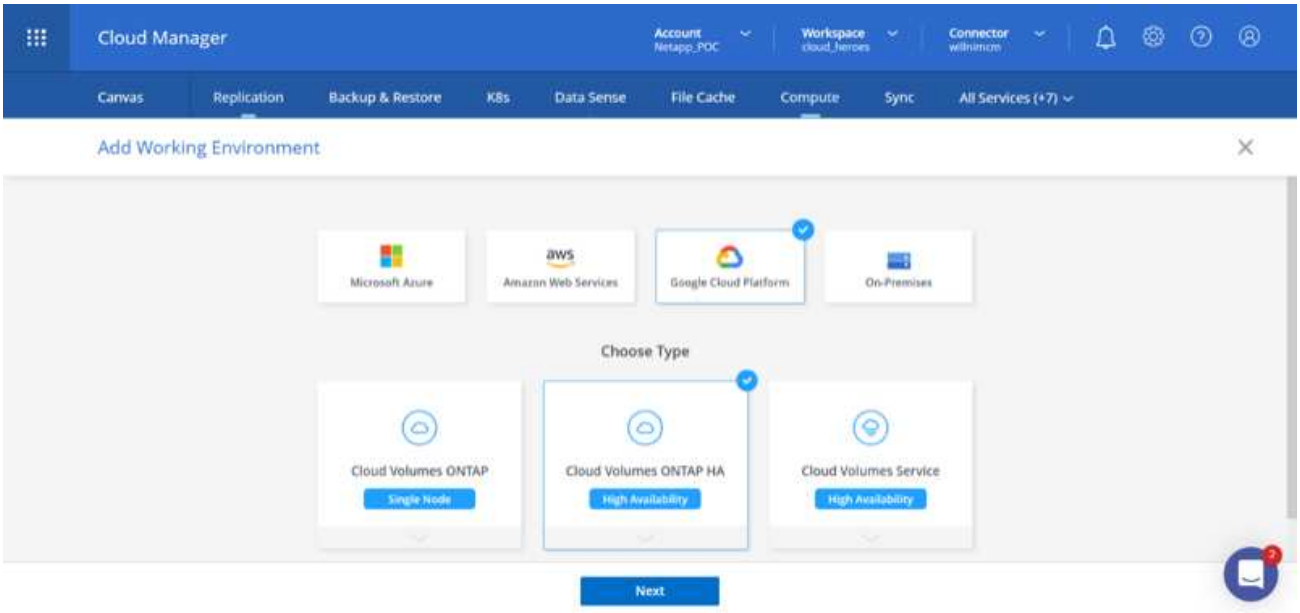


"Cloud Volumes ONTAP 사이저"을(를) 사용하여 Cloud Volumes ONTAP 인스턴스의 크기를 정확하게 조정하십시오. 또한 온프레미스 성능을 모니터링하여 Cloud Volumes ONTAP sizer의 입력으로 사용하십시오.

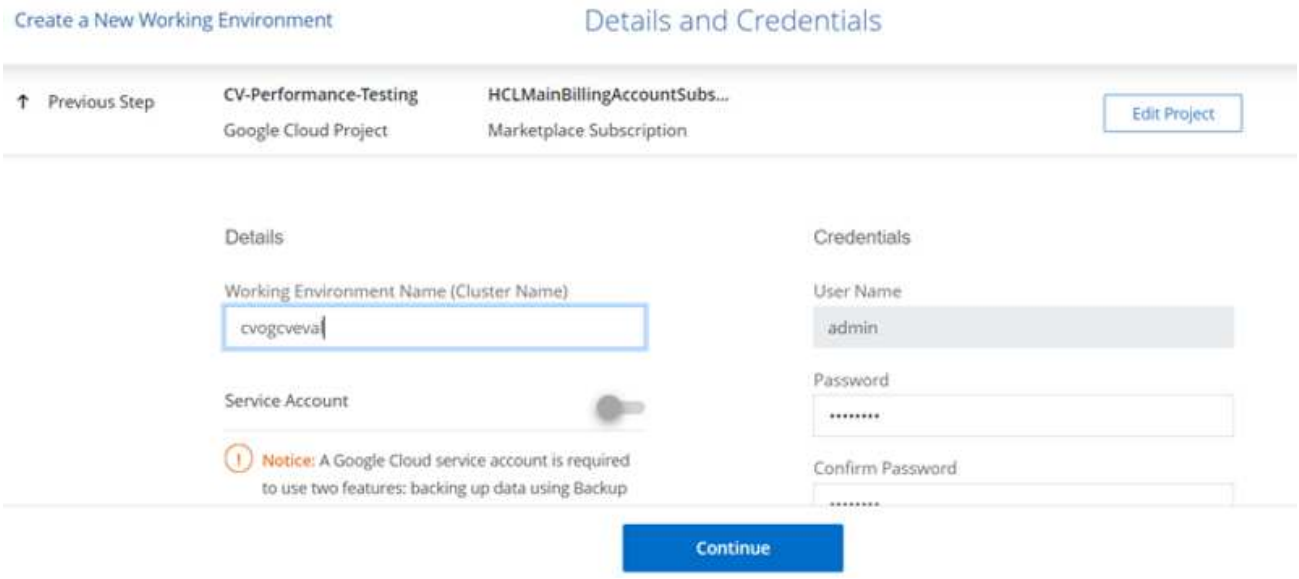
1. NetApp Cloud Central에 로그인하면 Fabric View 화면이 표시됩니다. Cloud Volumes ONTAP 탭을 찾아 Cloud Manager로 이동을 선택합니다. 로그인 후 Canvas 화면이 표시됩니다.



2. 클라우드 관리자 캔버스 탭에서 작업 환경 추가를 클릭한 다음 클라우드로 Google Cloud Platform을 선택하고 시스템 구성 유형을 선택합니다. 그런 다음 다음을 클릭합니다.



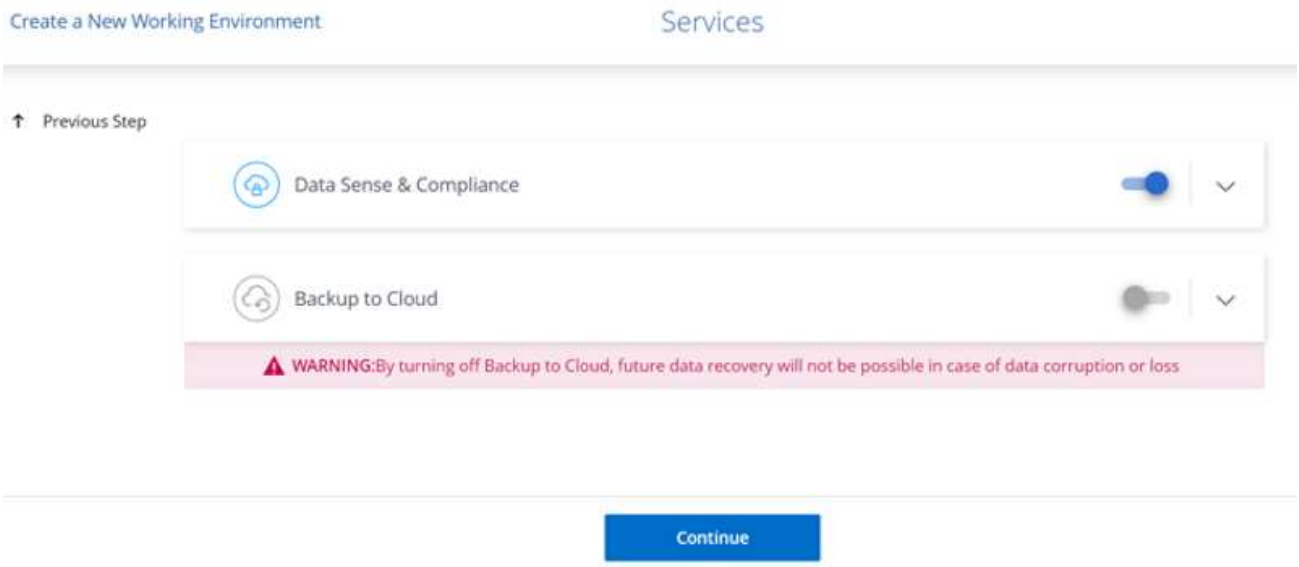
3. 환경 이름과 관리자 자격 증명을 포함하여 생성할 환경에 대한 세부 정보를 제공합니다. 완료되면 계속을 클릭하세요.



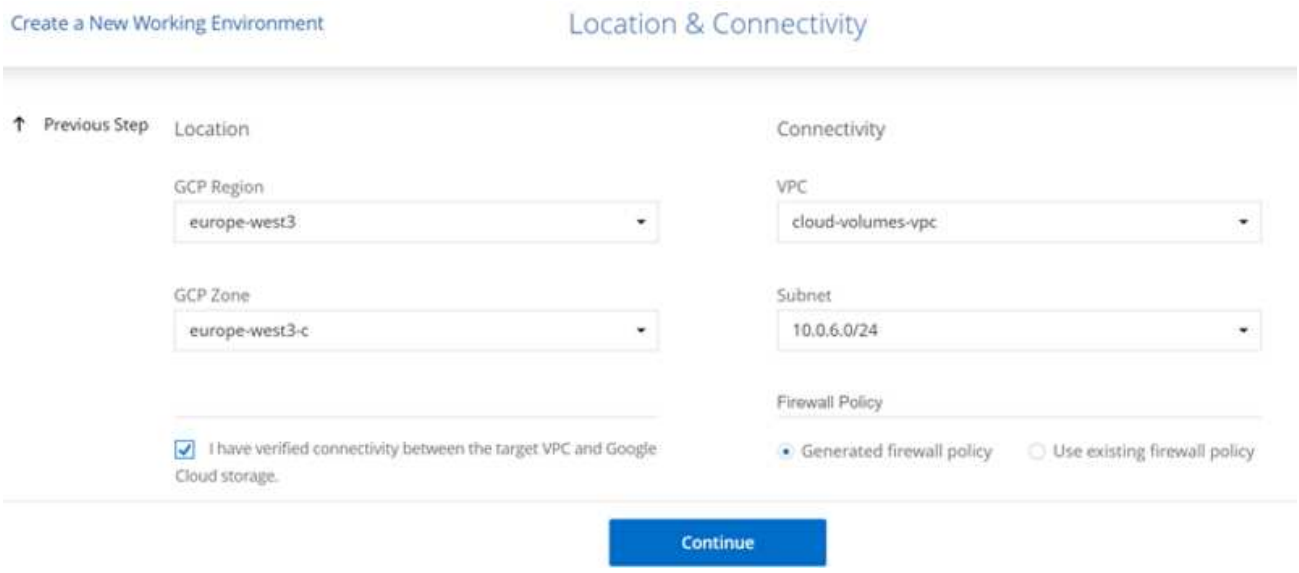
4. 데이터 감지 및 규정 준수 또는 클라우드 백업을 포함하여 Cloud Volumes ONTAP 배포를 위한 추가 서비스를

선택하거나 선택 해제합니다. 그런 다음 계속을 클릭하세요.

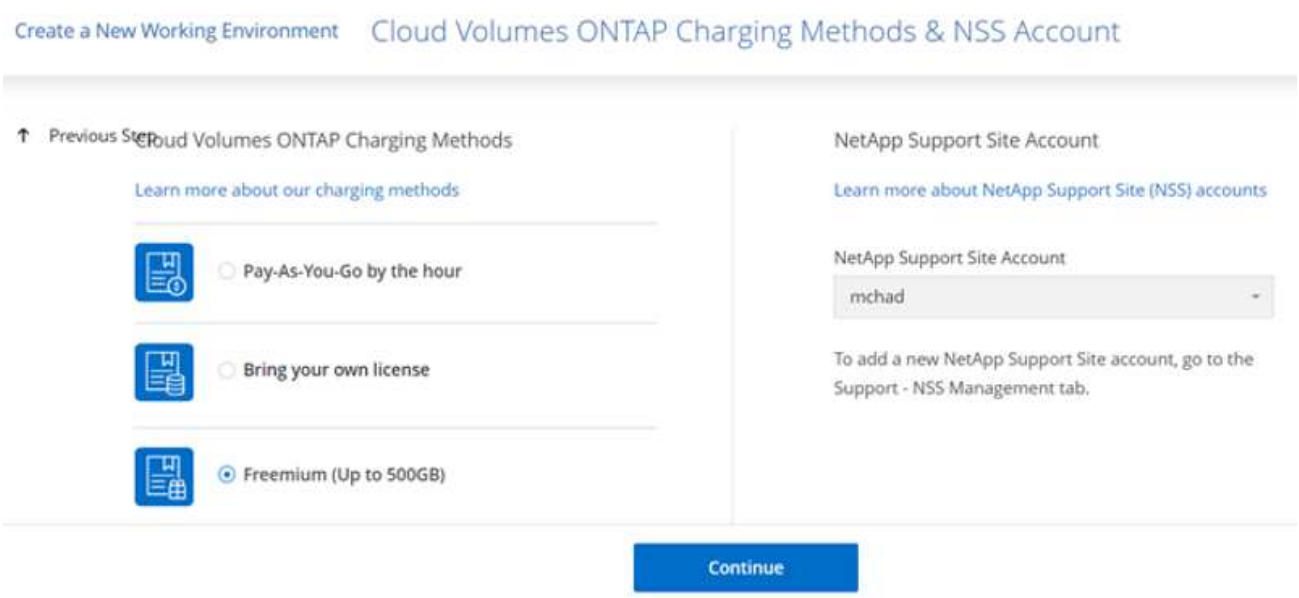
힌트: 추가 서비스를 비활성화하면 확인 팝업 메시지가 표시됩니다. 추가 서비스는 CVO 배포 후에 추가/제거할 수 있습니다. 비용을 피하기 위해 처음부터 필요하지 않은 경우 선택을 해제하는 것이 좋습니다.



5. 위치를 선택하고, 방화벽 정책을 선택한 다음, 확인란을 선택하여 Google Cloud Storage에 대한 네트워크 연결을 확인하세요.

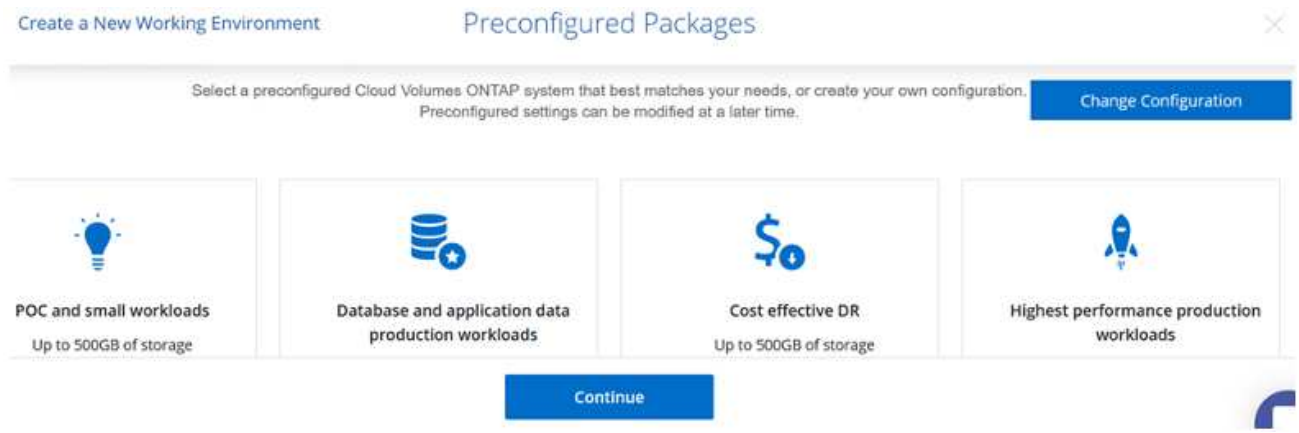


6. 라이선스 옵션을 선택하세요: Pay-As-You-Go 또는 기존 라이선스를 사용하는 BYOL. 이 예에서는 Freemium 옵션이 사용되었습니다. 그런 다음 계속을 클릭하세요.

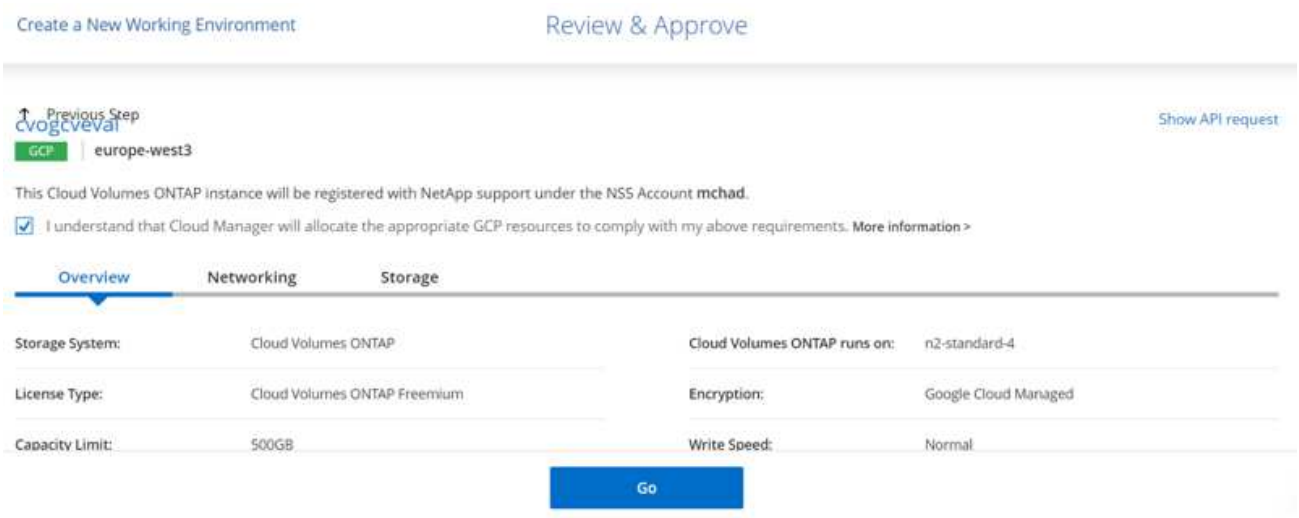


7. AWS SDDC의 VMware 클라우드에서 실행되는 VM에 배포될 워크로드 유형에 따라 미리 구성된 여러 패키지 중에서 선택하세요.

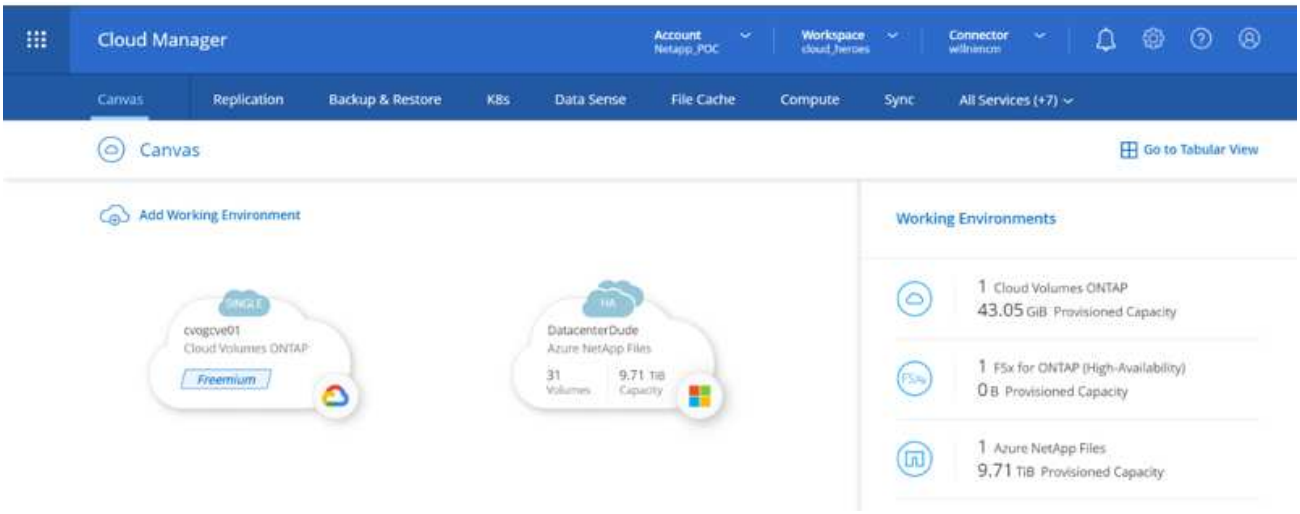
   힌트: 자세한 내용을 보려면 타일 위에 마우스를 올려놓으세요. 또는 구성 변경을 클릭하여 CVO 구성 요소와 ONTAP 버전을 사용자 지정하세요.



8. 검토 및 승인 페이지에서 선택 사항을 검토하고 확인합니다 . Cloud Volumes ONTAP 인스턴스를 생성하려면 이동을 클릭합니다.



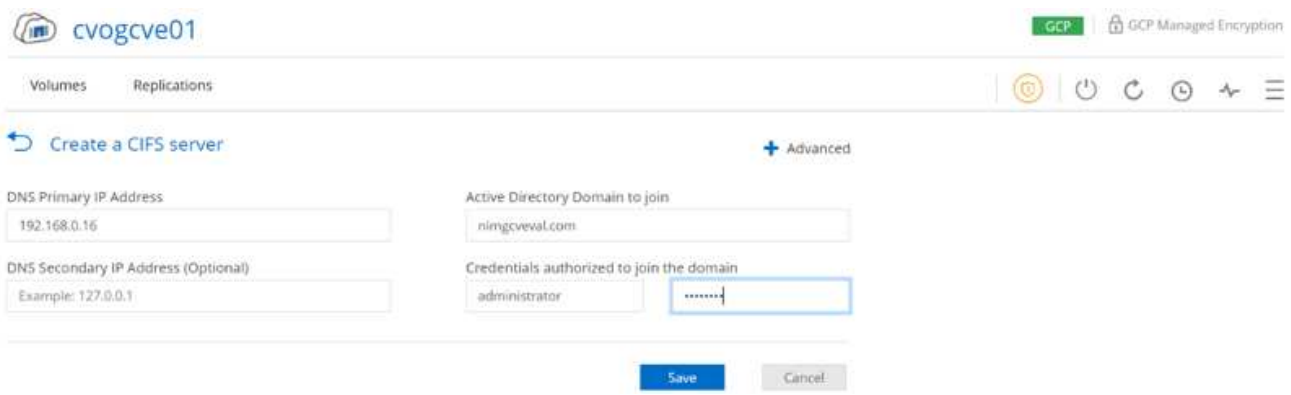
9. Cloud Volumes ONTAP 이 프로비저닝되면 Canvas 페이지의 작업 환경에 나열됩니다.



▼ **SMB** 볼륨에 대한 추가 구성

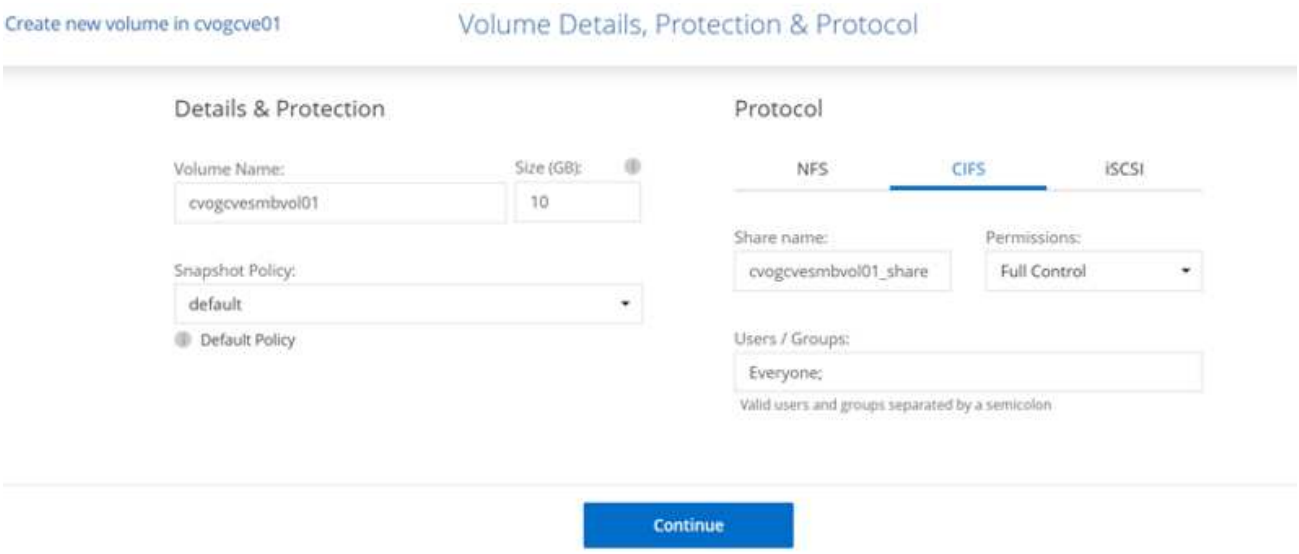
1. 작업 환경이 준비되면 CIFS 서버가 적절한 DNS 및 Active Directory 구성 매개변수로 구성되었는지 확인하세요. SMB 볼륨을 생성하려면 이 단계가 필요합니다.

   힌트: 메뉴 아이콘(⁰)을 클릭하고 고급을 선택하여 더 많은 옵션을 표시하고 CIFS 설정을 선택하세요.



2. SMB 볼륨을 만드는 것은 간단한 과정입니다. Canvas에서 Cloud Volumes ONTAP 작업 환경을 두 번

클릭하여 볼륨을 만들고 관리하고 볼륨 만들기 옵션을 클릭합니다. 적절한 크기를 선택하면 클라우드 관리자가 포함된 집계를 선택하거나 고급 할당 메커니즘을 사용하여 특정 집계에 배치합니다. 이 데모에서는 프로토콜로 CIFS/SMB가 선택되었습니다.



3. 볼륨이 프로비저닝된 후에는 볼륨 창에서 사용할 수 있습니다. CIFS 공유가 프로비저닝되므로 사용자 또는 그룹에 파일과 폴더에 대한 권한을 부여하고 해당 사용자가 공유에 액세스하여 파일을 만들 수 있는지 확인하세요. 볼륨이 온-프레미스 환경에서 복제된 경우 파일 및 폴더 권한이 모두 SnapMirror 복제의 일부로 유지되므로 이 단계는 필요하지 않습니다.

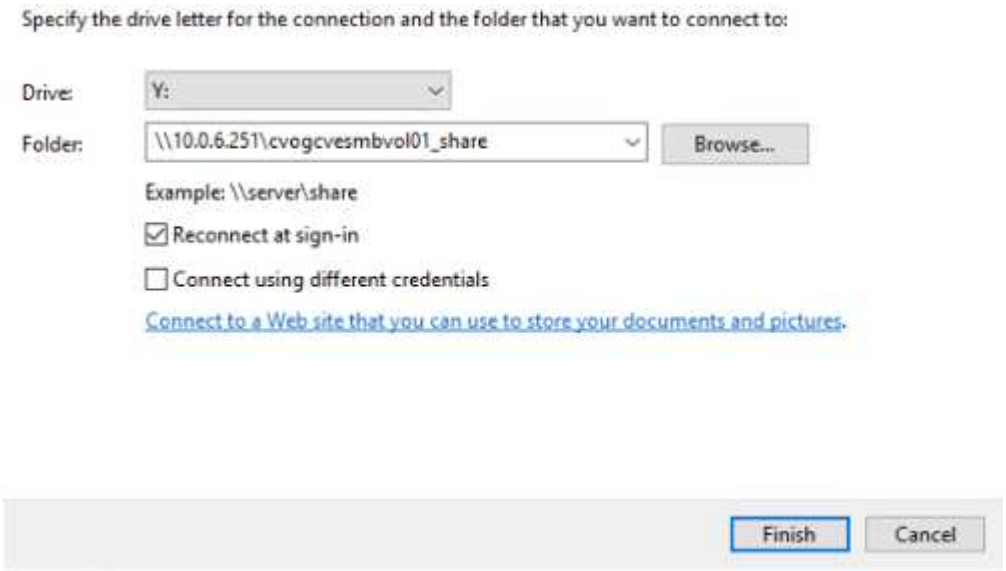
   힌트: 볼륨 메뉴(º)를 클릭하면 옵션이 표시됩니다.



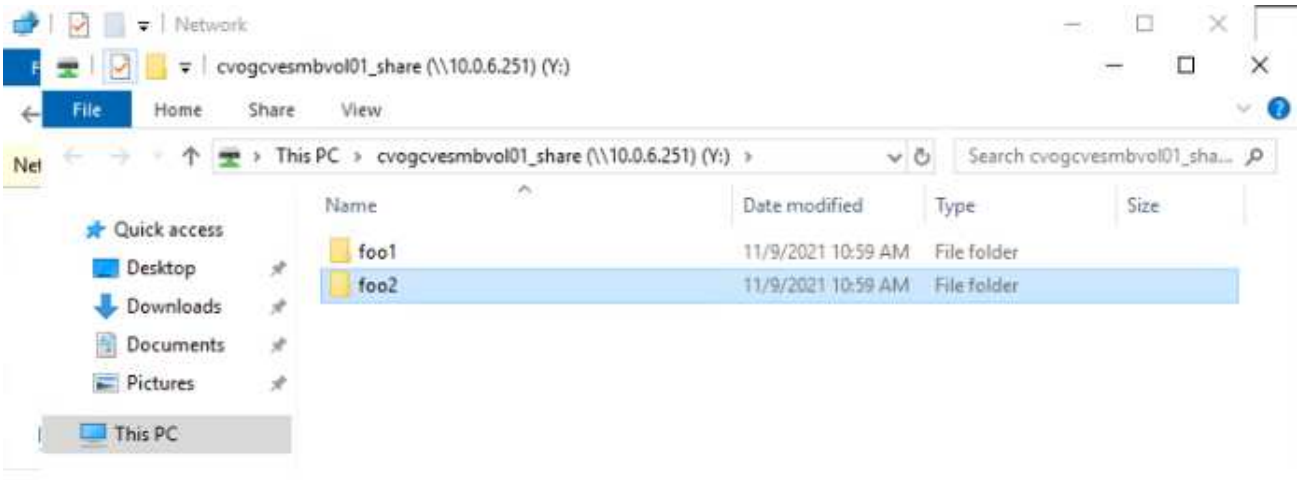
4. 볼륨이 생성된 후 mount 명령을 사용하여 볼륨 연결 지침을 표시한 다음 Google Cloud VMware Engine의 VM에서 공유에 연결합니다.



5. 다음 경로를 복사하고 네트워크 드라이브 매핑 옵션을 사용하여 Google Cloud VMware Engine에서 실행되는 VM에 볼륨을 마운트합니다.



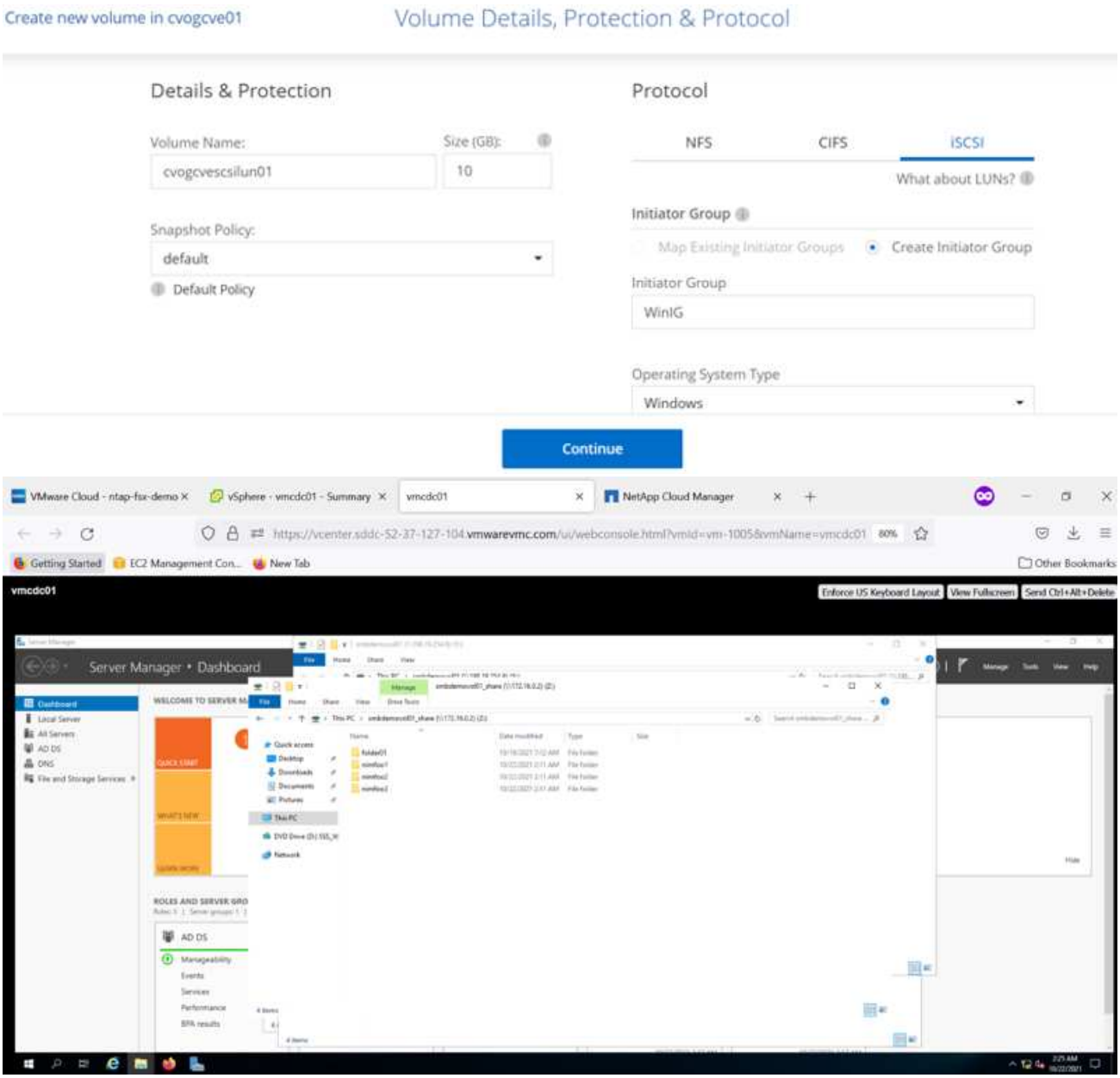
매핑이 완료되면 쉽게 접근할 수 있으며 NTFS 권한도 그에 따라 설정할 수 있습니다.



▼ **Cloud Volumes ONTAP** 의 **LUN**을 호스트에 연결합니다.

클라우드 볼륨 ONTAP LUN을 호스트에 연결하려면 다음 단계를 완료하세요.

1. Canvas 페이지에서 Cloud Volumes ONTAP 작업 환경을 두 번 클릭하여 볼륨을 만들고 관리합니다.
2. 볼륨 추가 > 새 볼륨을 클릭하고 iSCSI를 선택한 후 초기자 그룹 만들기를 클릭합니다. 계속을 클릭하세요.



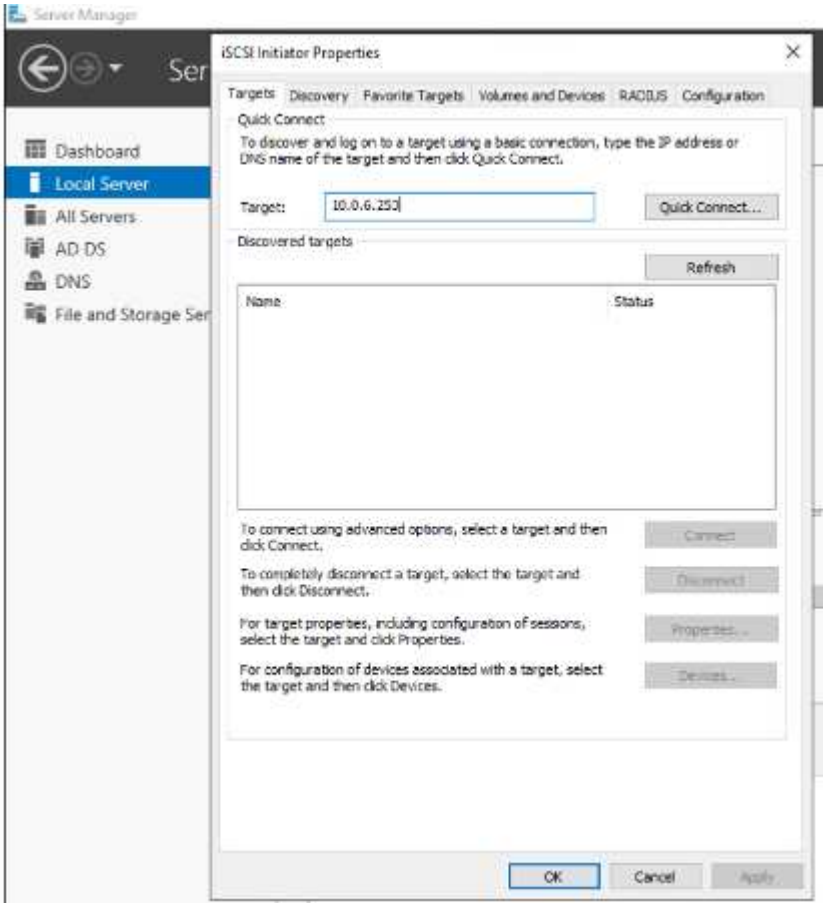
3. 볼륨이 프로비저닝된 후 볼륨 메뉴(⁰)를 선택한 다음 대상 iQN을 클릭합니다. iSCSI 정규 이름(iQN)을 복사하려면 복사를 클릭합니다. 호스트에서 LUN으로 iSCSI 연결을 설정합니다.

Google Cloud VMware Engine에 있는 호스트에 대해서도 동일한 작업을 수행하려면 다음을 수행합니다.

1. Google Cloud VMware Engine에 호스팅된 VM에 대한 RDP.
2. iSCSI 초기자 속성 대화 상자를 엽니다: 서버 관리자 > 대시보드 > 도구 > iSCSI 초기자.
3. 검색 탭에서 포털 검색 또는 포털 추가를 클릭한 다음 iSCSI 대상 포트의 IP 주소를 입력합니다.
4. 대상 탭에서 검색된 대상을 선택한 다음 로그온 또는 연결을 클릭합니다.

5. 다중 경로 사용을 선택한 다음 컴퓨터 시작 시 이 연결을 자동으로 복원 또는 이 연결을 즐겨찾기 대상 목록에 추가를 선택합니다. 고급을 클릭합니다.

> Windows 호스트는 클러스터의 각 노드에 iSCSI 연결이 있어야 합니다. 기본 DSM은 사용할 가장 좋은 경로를 선택합니다.



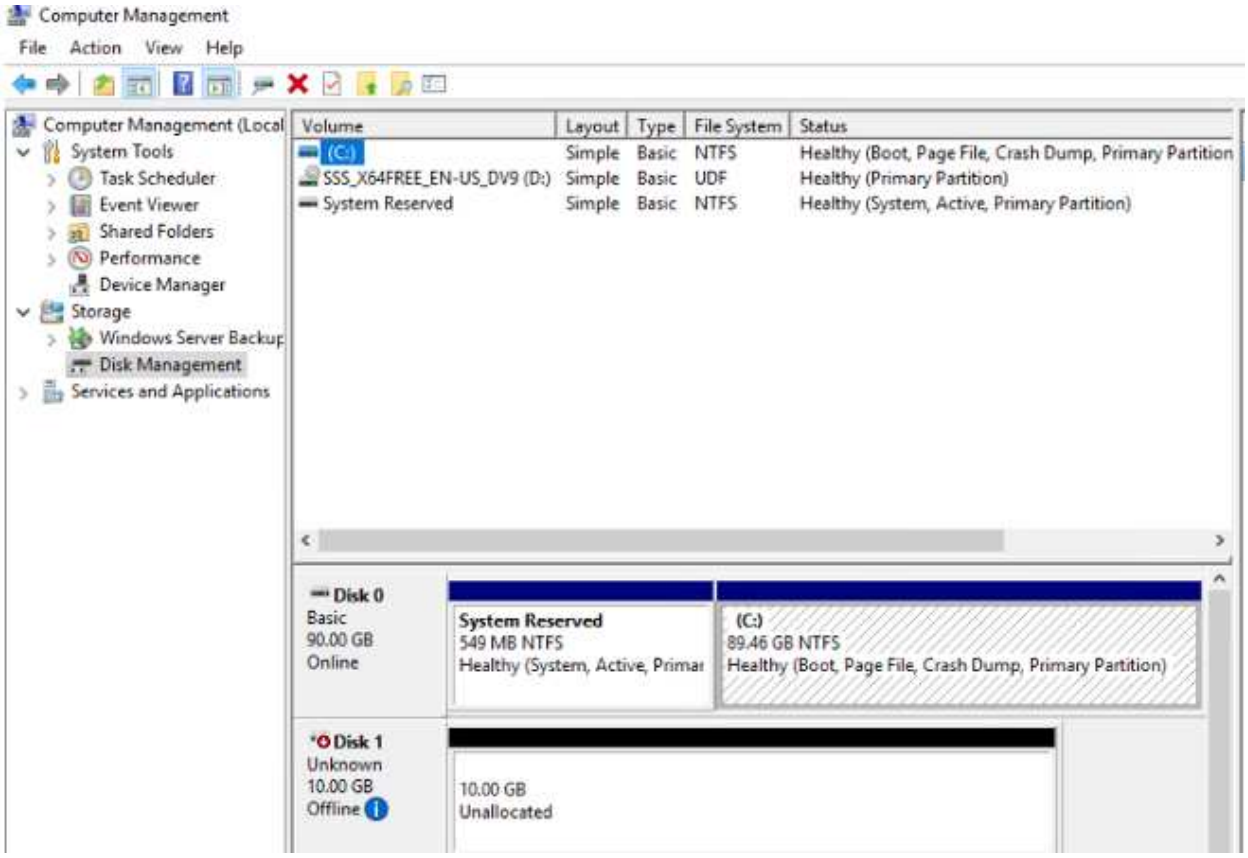
스토리지 가상 머신(SVM)의 LUN은 Windows 호스트에 디스크로 표시됩니다. 새로 추가된 디스크는 호스트에서 자동으로 검색되지 않습니다. 다음 단계를 완료하여 디스크를 검색하기 위한 수동 재검사를 트리거합니다.

a. Windows 컴퓨터 관리 유틸리티를 엽니다: 시작 > 관리 도구 > 컴퓨터 관리.

b. 탐색 트리에서 저장소 노드를 확장합니다.

c. 디스크 관리를 클릭합니다.

d. 작업 > 디스크 다시 검사를 클릭합니다.

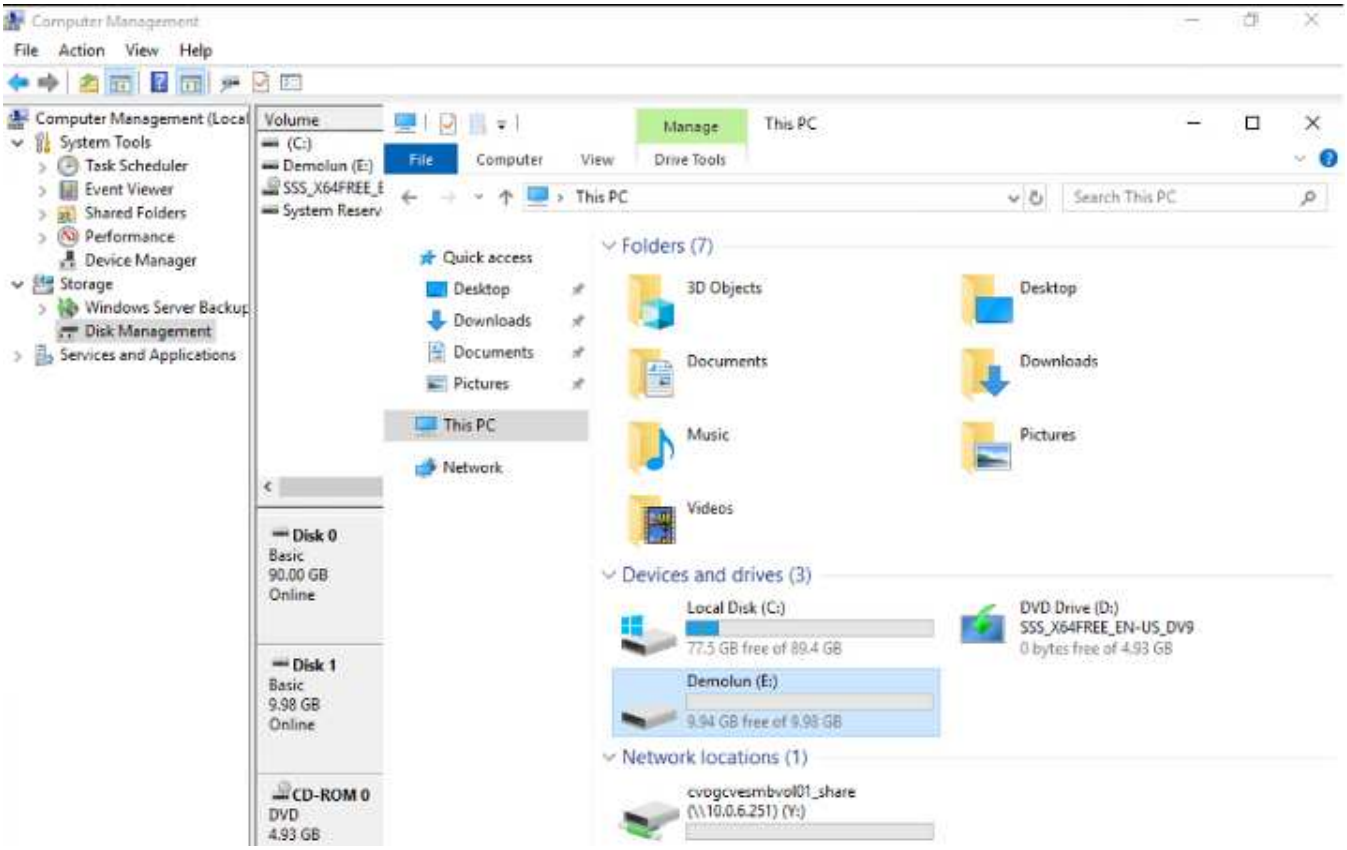


Windows 호스트가 새 LUN에 처음 액세스할 때 파티션이나 파일 시스템이 없습니다. LUN을 초기화하고, 필요한 경우 다음 단계를 완료하여 LUN을 파일 시스템으로 포맷합니다.

a. Windows 디스크 관리를 시작합니다.

b. LUN을 마우스 오른쪽 버튼으로 클릭한 다음 필요한 디스크 또는 파티션 유형을 선택합니다.

c. 마법사의 지시를 따르세요. 이 예에서는 드라이브 F:가 마운트되었습니다.



Linux 클라이언트에서 iSCSI 데몬이 실행 중인지 확인하세요. LUN이 프로비저닝되면 여기에서 Ubuntu를 사용한 iSCSI 구성에 대한 자세한 지침을 참조하세요. 확인하려면 셸에서 lsblk cmd를 실행하세요.

```
niyaz@nimubu01:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0    7:0    0 55.4M  1 loop /snap/core18/2128
loop1    7:1    0  219M  1 loop /snap/gnome-3-34-1804/72
loop2    7:2    0 65.1M  1 loop /snap/gtk-common-themes/1515
loop3    7:3    0   51M  1 loop /snap/snap-store/547
loop4    7:4    0 32.3M  1 loop /snap/snapd/12704
loop5    7:5    0 32.5M  1 loop /snap/snapd/13640
loop6    7:6    0 55.5M  1 loop /snap/core18/2246
loop7    7:7    0    4K  1 loop /snap/bare/5
loop8    7:8    0 65.2M  1 loop /snap/gtk-common-themes/1519
sda      8:0    0   16G  0 disk
├─sda1   8:1    0  512M  0 part /boot/efi
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0 15.5G  0 part /
sdb      8:16   0    1G  0 disk
```

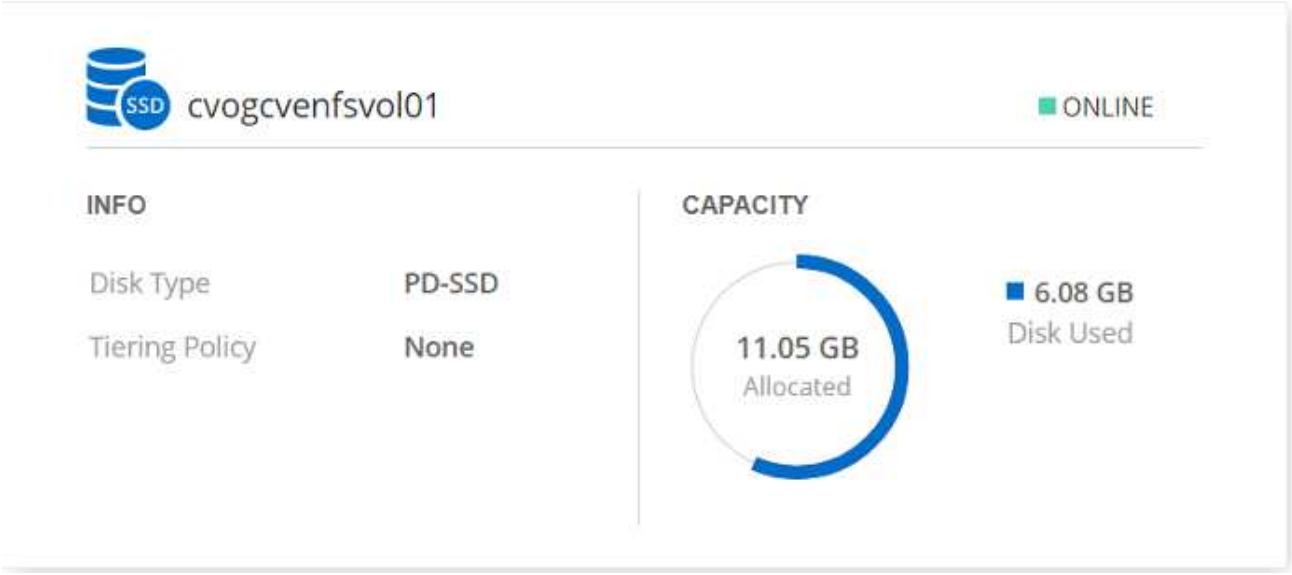
```
nlyaz@nlnubu01:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           394M  1.5M  392M   1% /run
/dev/sda5        16G  7.6G  6.9G  53% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1      219M  219M     0 100% /snap/gnome-3-34-1804/72
/dev/loop2       66M   66M     0 100% /snap/gtk-common-themes/1515
/dev/loop3       51M   51M     0 100% /snap/snap-store/547
/dev/loop0       56M   56M     0 100% /snap/core18/2128
/dev/loop4       33M   33M     0 100% /snap/snapd/12704
/dev/sda1       511M  4.0K  511M   1% /boot/efi
tmpfs           394M   64K  394M   1% /run/user/1000
/dev/loop5       33M   33M     0 100% /snap/snapd/13640
/dev/loop6       56M   56M     0 100% /snap/core18/2246
/dev/loop7      128K  128K     0 100% /snap/bare/5
/dev/loop8       66M   66M     0 100% /snap/gtk-common-themes/1519
/dev/sdb        976M  2.6M  907M   1% /mnt
```

▼ **Linux** 클라이언트에서 **Cloud Volumes ONTAP NFS** 볼륨 마운트

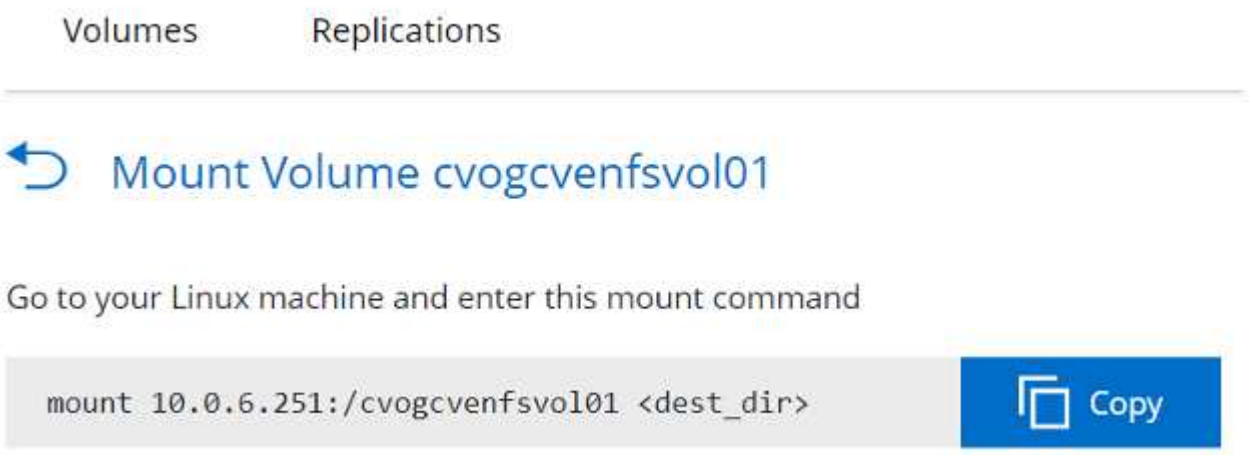
Google Cloud VMware Engine 내의 VM에서 Cloud Volumes ONTAP (DIY) 파일 시스템을 마운트하려면 아래 단계를 따르세요.

아래 단계에 따라 볼륨을 프로비저닝하세요.

1. 볼륨 탭에서 새 볼륨 만들기를 클릭합니다.
2. 새 볼륨 만들기 페이지에서 볼륨 유형을 선택하세요.



3. 볼륨 탭에서 볼륨 위에 마우스 커서를 놓고 메뉴 아이콘(⁰)을 선택한 다음, 마운트 명령을 클릭합니다.



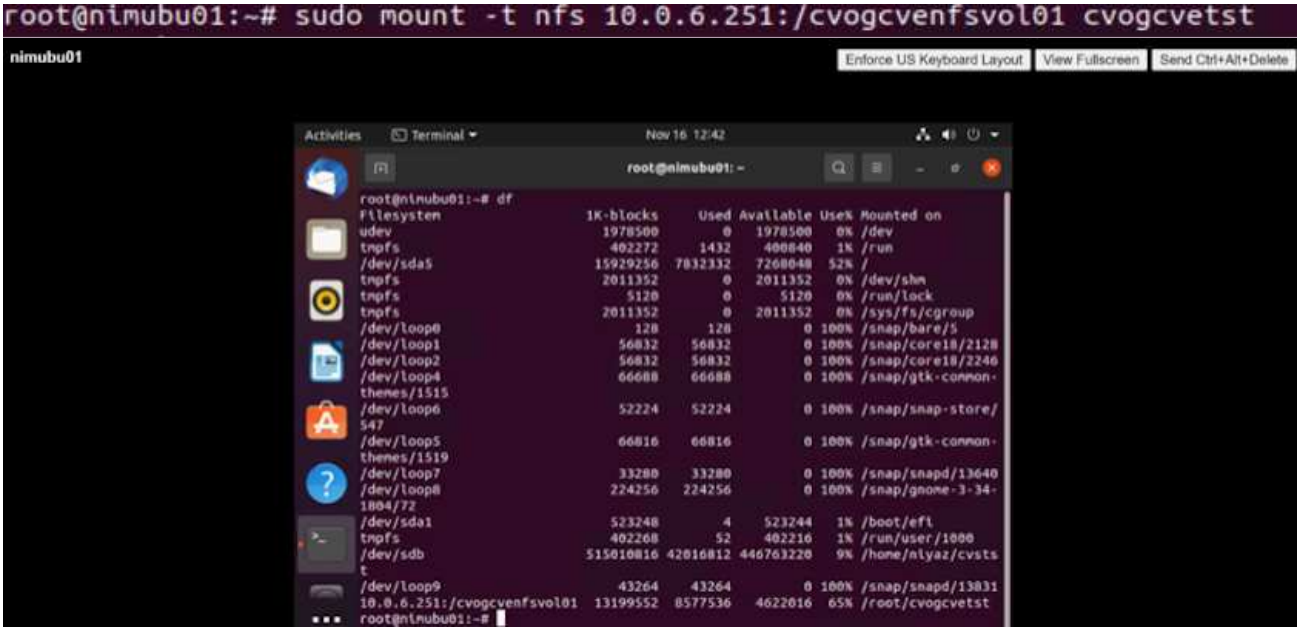
4. 복사를 클릭합니다.
5. 지정된 Linux 인스턴스에 연결합니다.
6. 보안 셸(SSH)을 사용하여 인스턴스에서 터미널을 열고 적절한 자격 증명으로 로그인합니다.
7. 다음 명령을 사용하여 볼륨의 마운트 지점에 대한 디렉토리를 만듭니다.

```
$ sudo mkdir /cvogcvetst
```

```
root@nimubu01:~# sudo mkdir cvogcvetst
```

8. 이전 단계에서 만든 디렉토리에 Cloud Volumes ONTAP NFS 볼륨을 마운트합니다.

```
sudo mount 10.0.6.251:/cvogcvenfsvol01 /cvogcvetst
```



Google Cloud NetApp Volumes (NetApp Volumes)

Google Cloud NetApp Volumes (NetApp Volumes)는 고급 클라우드 솔루션을 제공하는 완벽한 데이터 서비스 포트폴리오입니다. NetApp Volumes는 주요 클라우드 공급업체(NFS 및 SMB 지원)를 위한 여러 파일 액세스 프로토콜을 지원합니다.

기타 이점과 특징은 다음과 같습니다. 스냅샷을 통한 데이터 보호 및 복원, 온프레미스 또는 클라우드에서 데이터 대상을 복제, 동기화 및 마이그레이션하는 특수 기능, 전용 플래시 스토리지 시스템 수준에서 일관된 고성능.

게스트 연결 스토리지로서의 **Google Cloud NetApp Volumes (NetApp Volumes)**

▼ **VMware Engine**을 사용하여 **NetApp** 볼륨 구성

Google Cloud NetApp Volumes 공유는 VMware Engine 환경에서 생성된 VM에서 마운트할 수 있습니다. Google Cloud NetApp Volumes SMB 및 NFS 프로토콜을 지원하므로 볼륨을 Linux 클라이언트에 마운트하고 Windows 클라이언트에 매핑할 수도 있습니다. Google Cloud NetApp Volumes 볼륨은 간단한 단계로 설정할 수 있습니다.

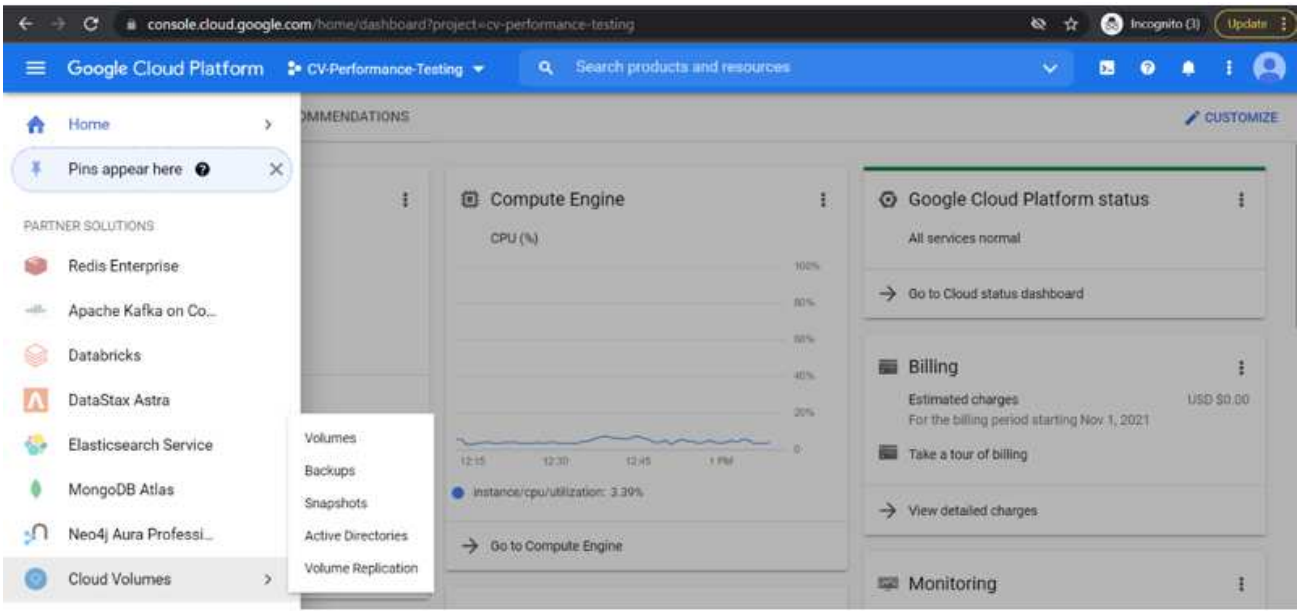
Google Cloud NetApp Volumes 와 Google Cloud VMware Engine 프라이빗 클라우드는 동일한 지역에 있어야 합니다.

Google Cloud Marketplace에서 Google Cloud용 Google Cloud NetApp Volumes 구매, 활성화 및 구성하려면 다음 자세한 내용을 따르세요."가이드" .

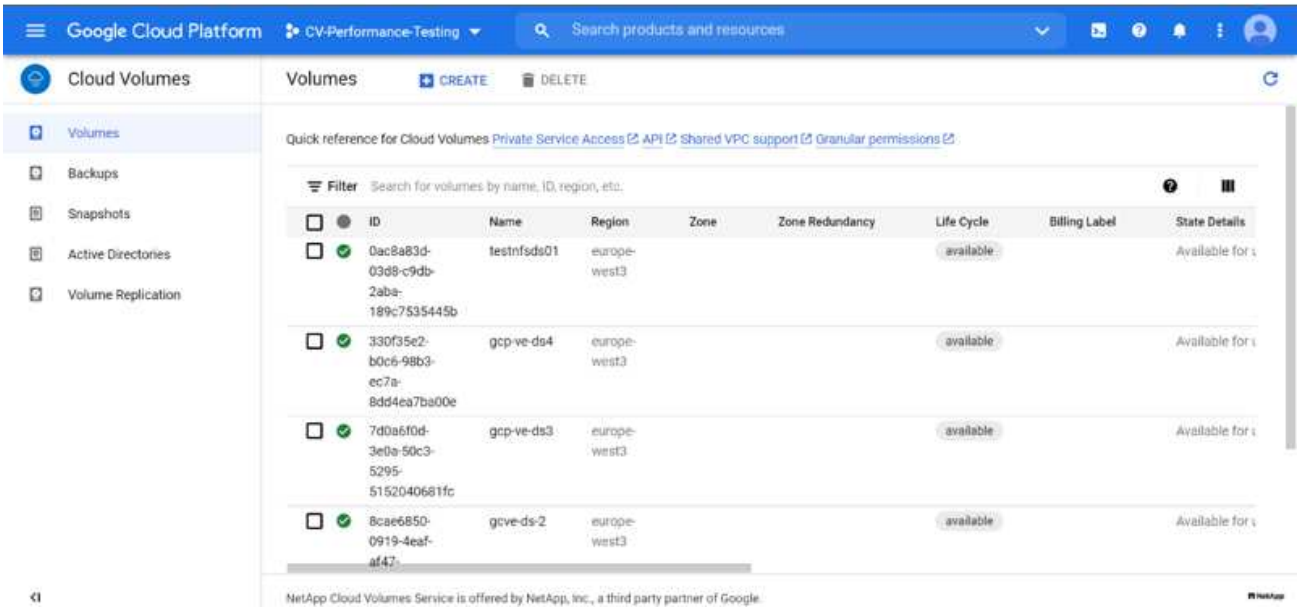
▼ **GCVE** 프라이빗 클라우드에 **NetApp Volumes NFS** 볼륨 생성

NFS 볼륨을 생성하고 마운트하려면 다음 단계를 완료하세요.

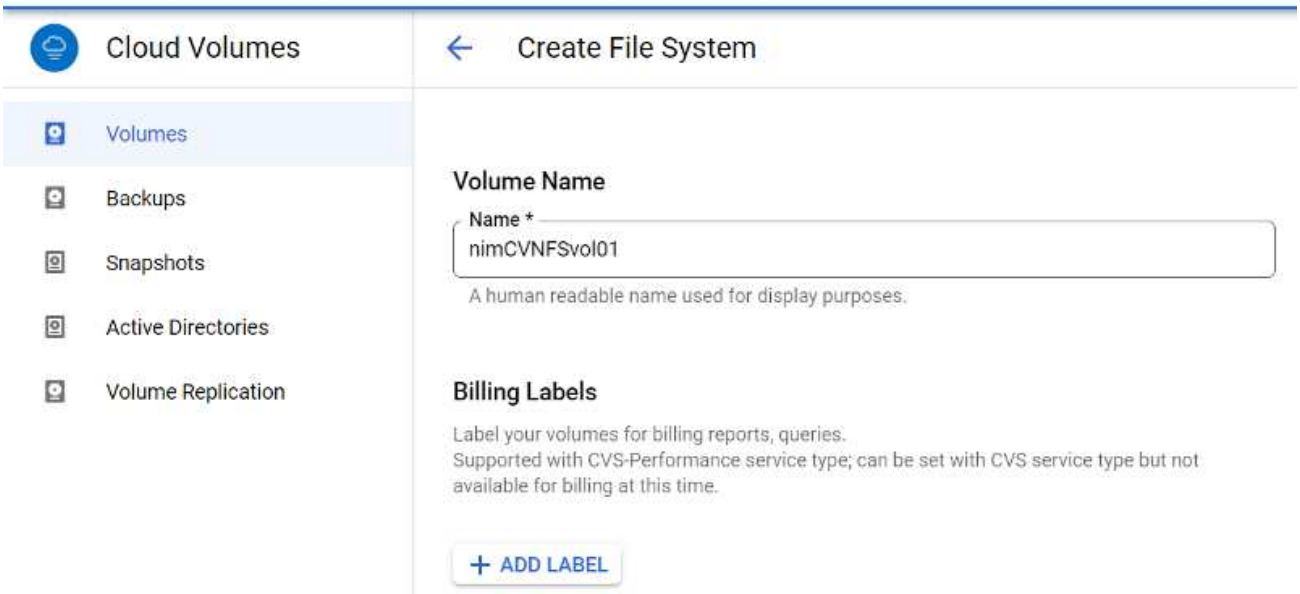
1. Google Cloud Console 내 파트너 솔루션에서 Cloud Volumes에 액세스하세요.



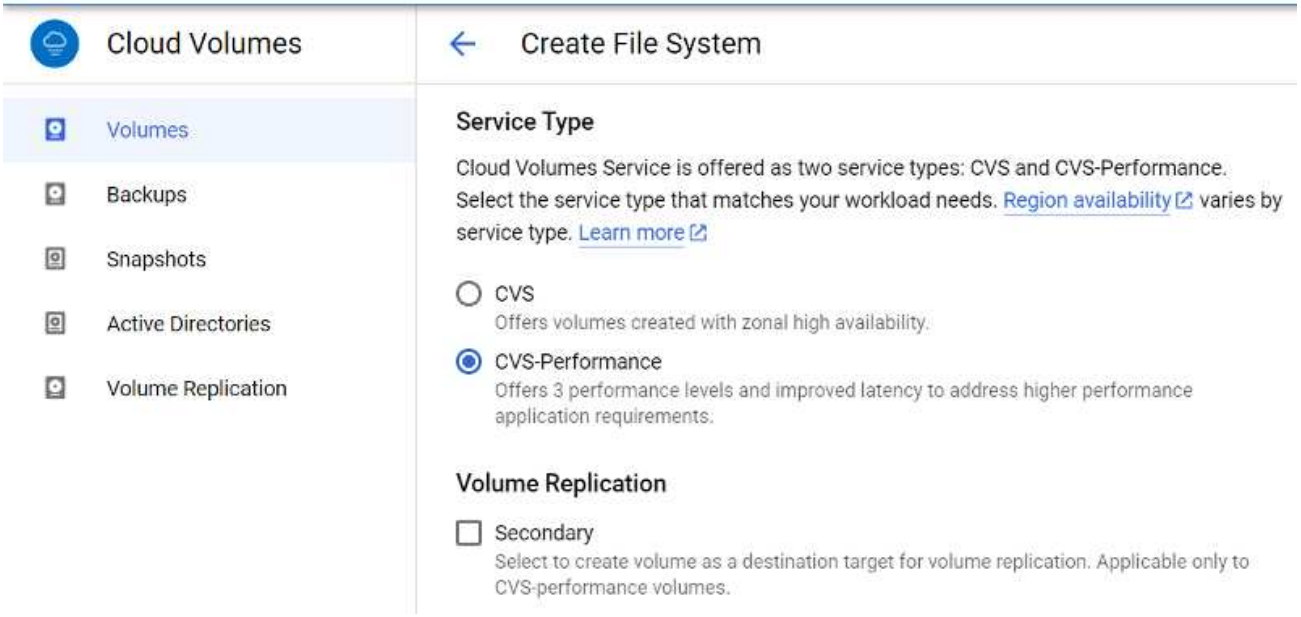
2. Cloud Volumes 콘솔에서 볼륨 페이지로 이동하여 만들기를 클릭합니다.



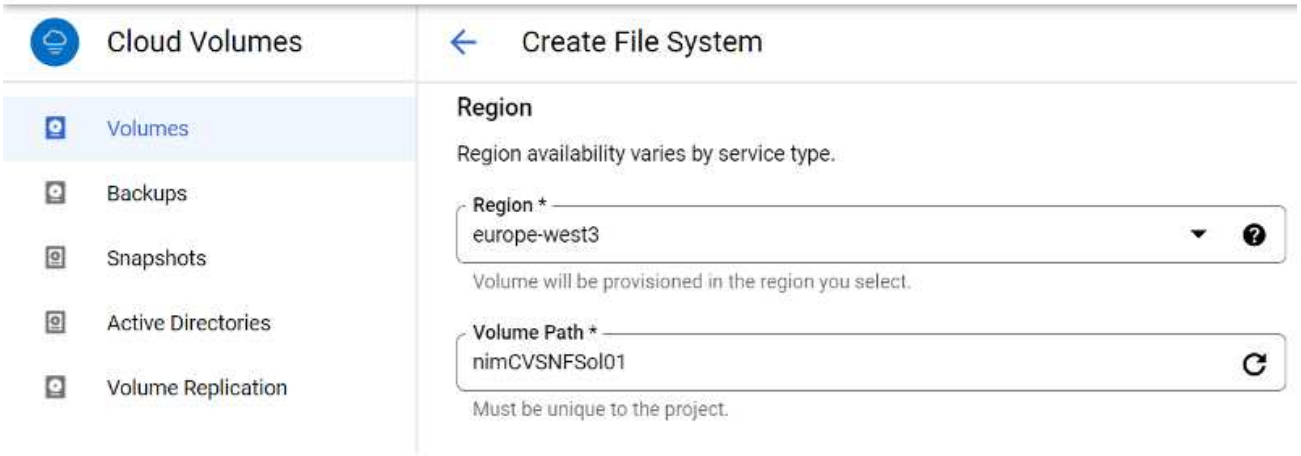
3. 파일 시스템 생성 페이지에서 요금 청구 메커니즘에 필요한 볼륨 이름과 청구 레이블을 지정합니다.



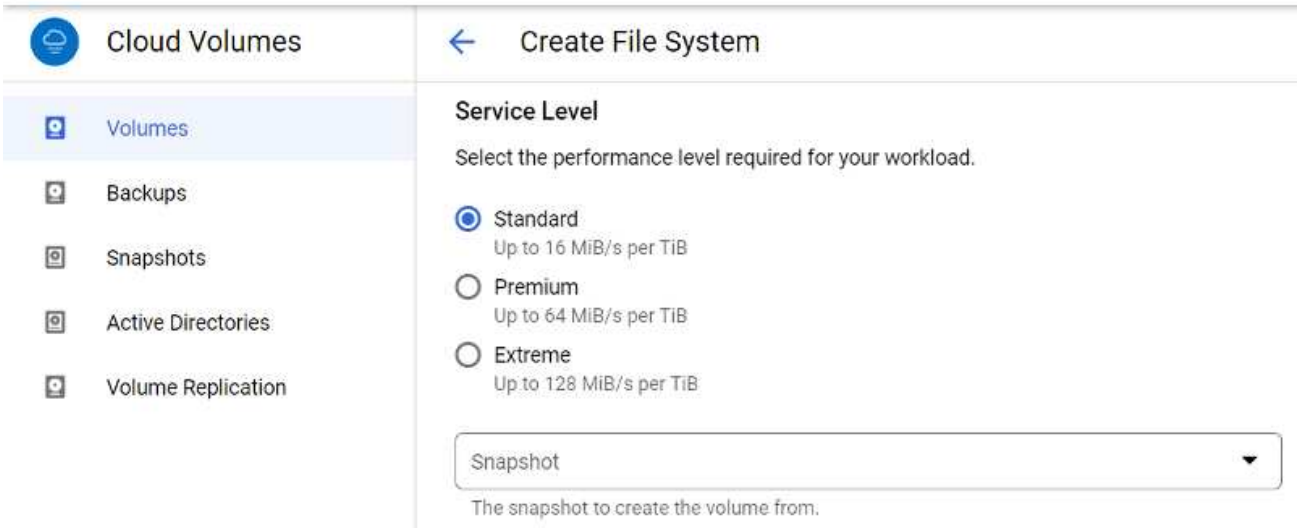
4. 적절한 서비스를 선택하세요. GCVE의 경우, 애플리케이션 작업 부하 요구 사항에 따라 지연 시간을 개선하고 성능을 높이는 NetApp Volumes-Performance 및 원하는 서비스 수준을 선택하세요.



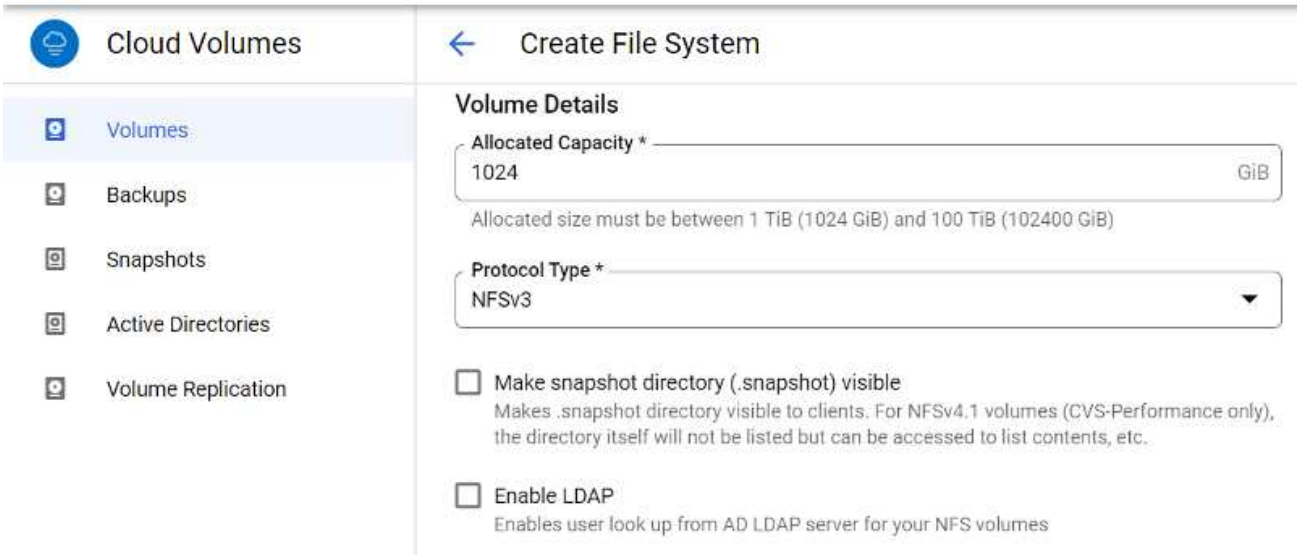
5. 볼륨 및 볼륨 경로에 대한 Google Cloud 지역을 지정합니다(볼륨 경로는 프로젝트의 모든 클라우드 볼륨에서 고유해야 함)



6. 볼륨에 대한 성능 수준을 선택하세요.

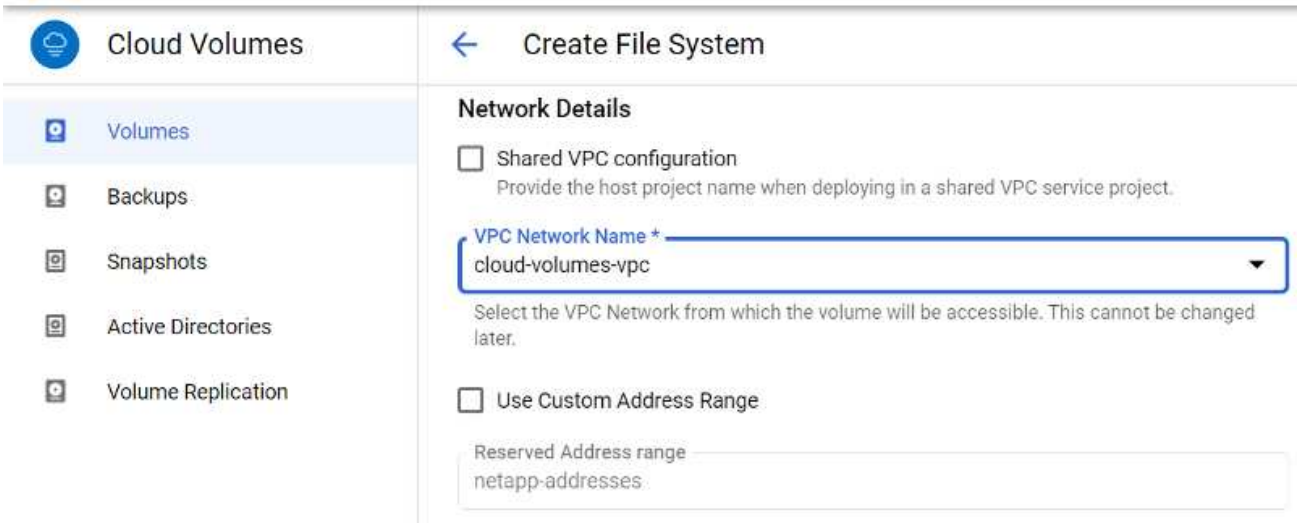


7. 볼륨 크기와 프로토콜 유형을 지정합니다. 이 테스트에서는 NFSv3를 사용했습니다.



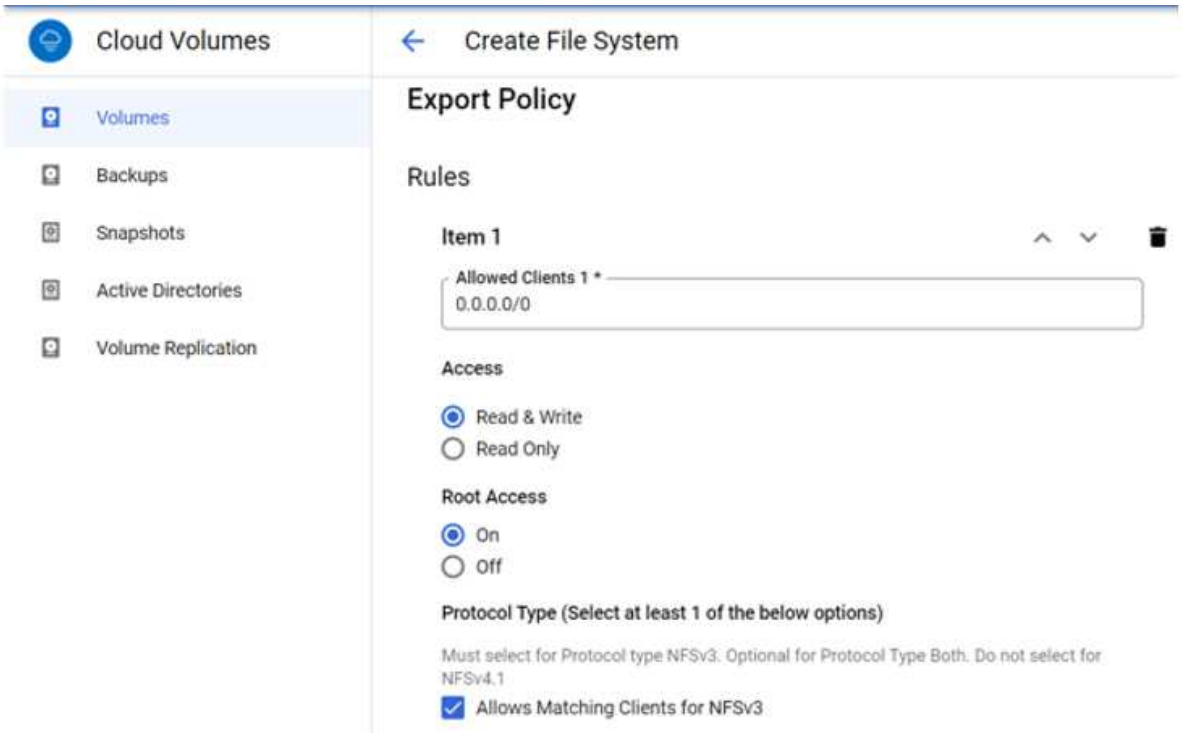
8. 이 단계에서는 볼륨에 액세스할 수 있는 VPC 네트워크를 선택합니다. VPC 피어링이 제대로 되어 있는지 확인하세요.

   힌트: VPC 피어링이 수행되지 않은 경우 팝업 버튼이 표시되어 피어링 명령을 안내합니다. Cloud Shell 세션을 열고 적절한 명령을 실행하여 VPC를 Google Cloud NetApp Volumes 프로듀서와 피어링합니다. 사전에 VPC 피어링을 준비하기로 결정한 경우 이 지침을 참조하세요.



9. 적절한 규칙을 추가하여 내보내기 정책 규칙을 관리하고 해당 NFS 버전에 대한 확인란을 선택합니다.

   참고: 내보내기 정책이 추가되지 않으면 NFS 볼륨에 액세스할 수 없습니다.



10. 저장을 클릭하여 볼륨을 생성합니다.



▼ **VMware Engine**에서 실행되는 **VM**에 **NFS** 내보내기 마운트

NFS 볼륨을 마운트하기 전에 개인 연결의 피어링 상태가 활성으로 나열되어 있는지 확인하세요. 상태가 활성이 되면 mount 명령을 사용합니다.

NFS 볼륨을 마운트하려면 다음을 수행하세요.

1. Cloud Console에서 Cloud Volumes > Volumes로 이동합니다.
2. 볼륨 페이지로 이동
3. NFS 내보내기를 마운트할 NFS 볼륨을 클릭합니다.
4. 오른쪽으로 스크롤하여 자세히 보기에서 마운트 지침을 클릭하세요.

VMware VM의 게스트 OS 내에서 마운트 프로세스를 수행하려면 아래 단계를 따르세요.

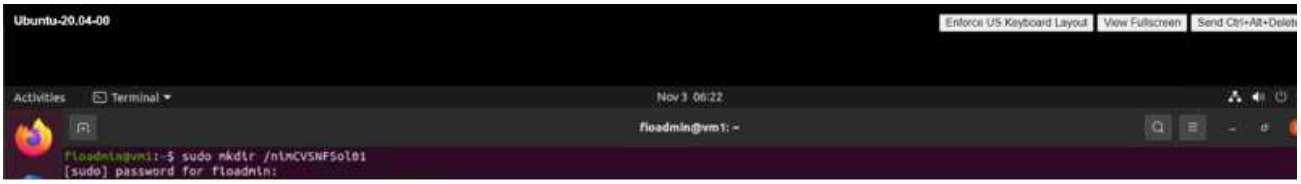
1. SSH 클라이언트를 사용하여 SSH를 통해 가상 머신에 접속합니다.
2. 인스턴스에 nfs 클라이언트를 설치합니다.
   a. Red Hat Enterprise Linux 또는 SuSE Linux 인스턴스에서:

```
 sudo yum install -y nfs-utils
.. Ubuntu 또는 Debian 인스턴스에서:
```

```
sudo apt-get install nfs-common
```

3. 인스턴스에 "/nimCVSNFSol01"과 같은 새 디렉토리를 만듭니다.

```
sudo mkdir /nimCVSNFSol01
```



4. 적절한 명령을 사용하여 볼륨을 마운트합니다. 랩에서 사용된 명령 예는 아래와 같습니다.

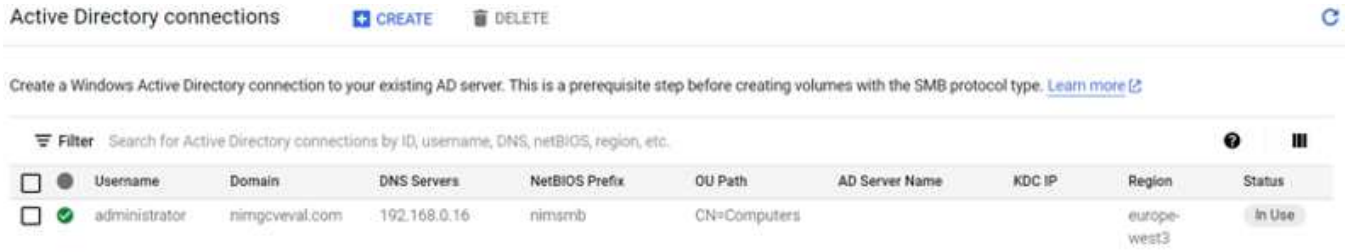
```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp
10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```



```
root@vm1:~# df
Filesystem                     1K-blocks        Used    Available Use% Mounted on
udev                            16409952           0     16409952   0% /dev
tmpfs                            3288328        1580      3286748   1% /run
/dev/sdb5                       61145932    19231356     38778832  34% /
tmpfs                           16441628           0     16441628   0% /dev/shm
tmpfs                               5120           0         5120   0% /run/lock
tmpfs                           16441628           0     16441628   0% /sys/fs/cgroup
/dev/loop0                            128         128            0 100% /snap/bare/5
/dev/loop1                          56832       56832            0 100% /snap/core18/2128
/dev/loop2                          66688       66688            0 100% /snap/gtk-common-themes/1515
/dev/loop4                          66816       66816            0 100% /snap/gtk-common-themes/1519
/dev/loop3                          52224       52224            0 100% /snap/snap-store/547
/dev/loop5                         224256      224256            0 100% /snap/gnome-3-34-1804/72
/dev/sdb1                          523248           4       523244   1% /boot/efi
tmpfs                             3288324          28      3288296   1% /run/user/1000
10.53.0.4:/gcve-ds-1          107374182400 1136086016 106238096384   2% /base
/dev/mapper/nfsprdvg1-prod01    419155968    55384972    363770996  14% /datastore1
/dev/loop8                          33280       33280            0 100% /snap/snapd/13270
/dev/loop6                          33280       33280            0 100% /snap/snapd/13640
/dev/loop7                          56832       56832            0 100% /snap/core18/2246
10.53.0.4:/nimCVSNFSol01      107374182400         256 107374182144   1% /nimCVSNFSol01
root@vm1:~#
```

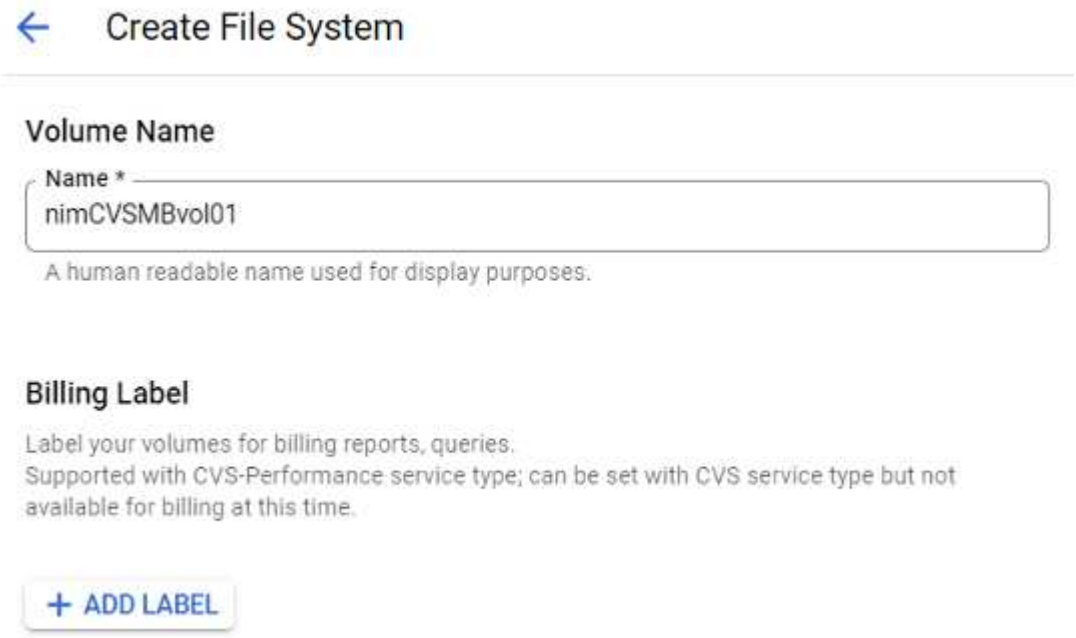
▼ **VMware Engine**에서 실행되는 **VM**에 **SMB** 공유 생성 및 마운트

SMB 볼륨의 경우 SMB 볼륨을 생성하기 전에 Active Directory 연결이 구성되어 있는지 확인하세요.



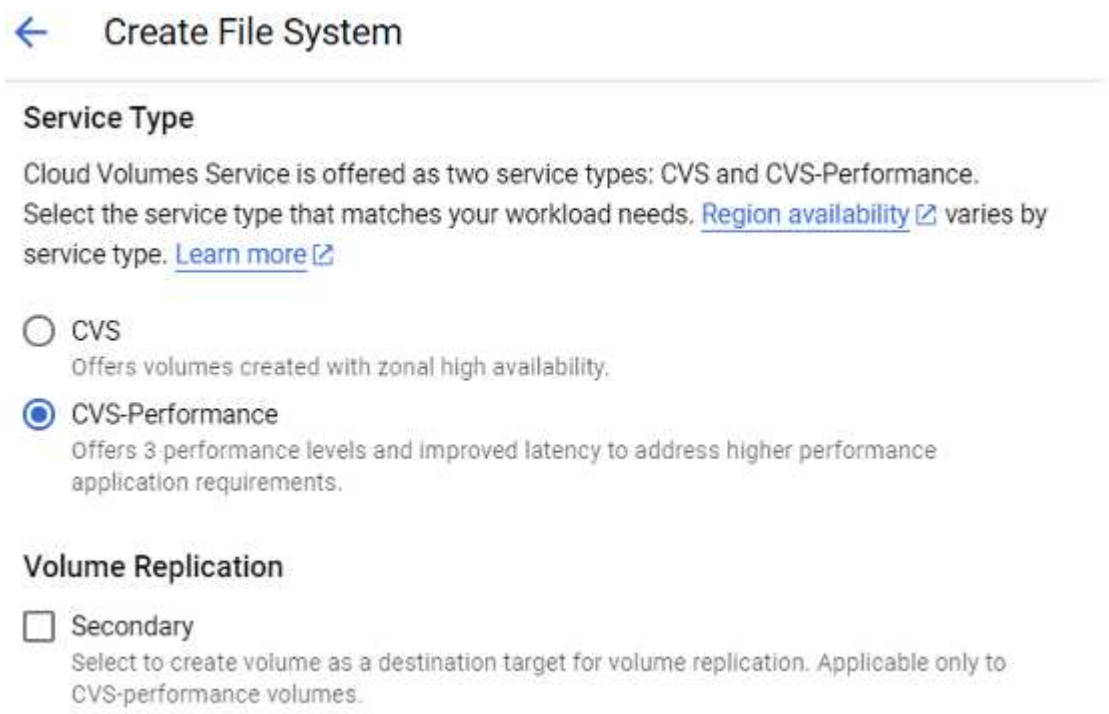
AD 연결이 설정되면 원하는 서비스 수준으로 볼륨을 만듭니다. 단계는 적절한 프로토콜을 선택하는 것을 제외하고는 NFS 볼륨을 만드는 것과 같습니다.

1. Cloud Volumes 콘솔에서 볼륨 페이지로 이동하여 만들기를 클릭합니다.
2. 파일 시스템 생성 페이지에서 요금 청구 메커니즘에 필요한 볼륨 이름과 청구 레이블을 지정합니다.

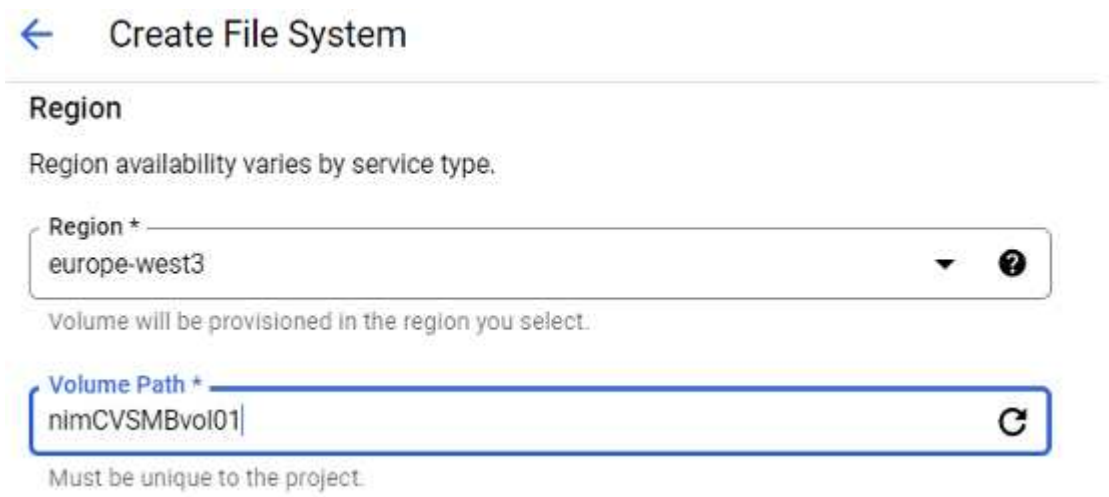


3. 적절한 서비스를 선택하세요. GCVE의 경우 NetApp Volumes-Performance와 원하는 서비스 수준을 선택하여

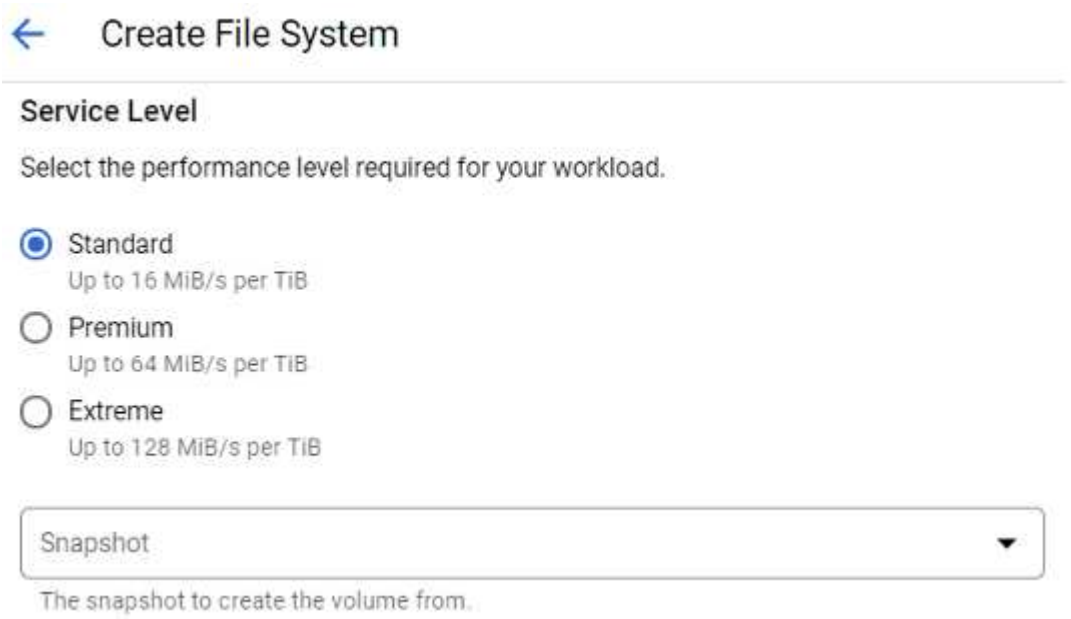
워크로드 요구 사항에 따라 지연 시간을 개선하고 성능을 높이세요.



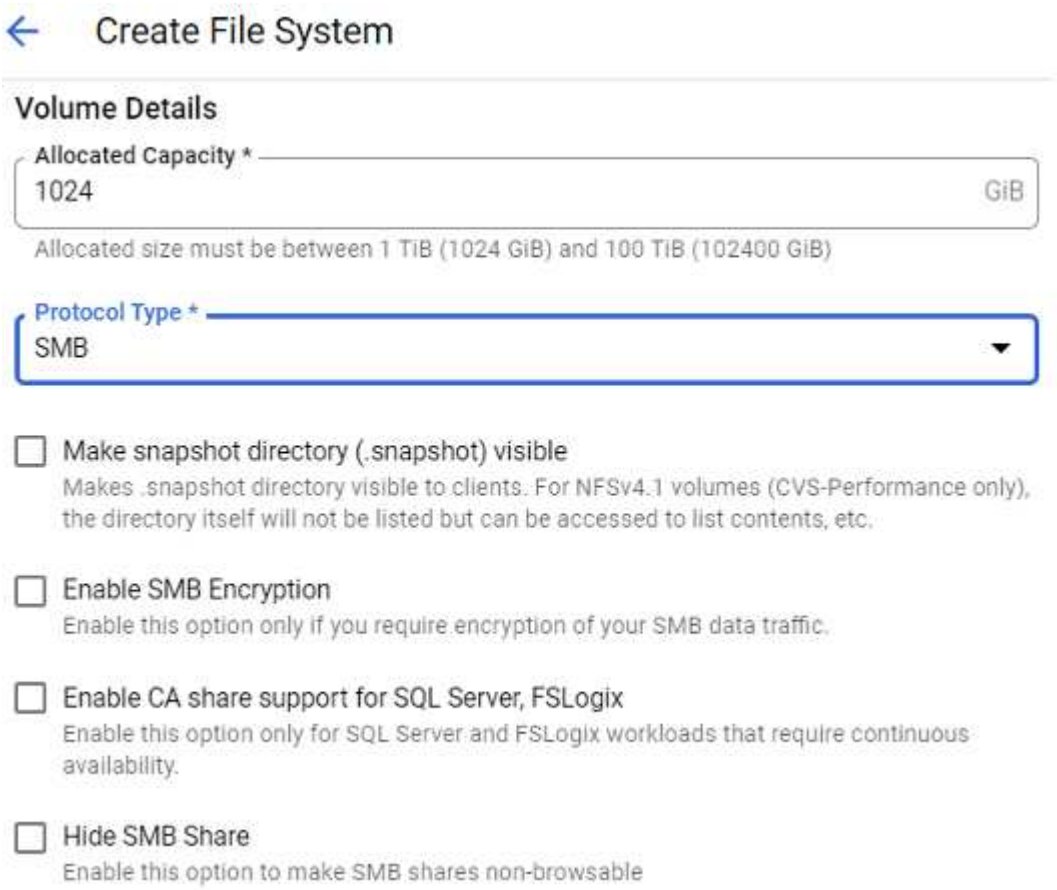
4. 볼륨 및 볼륨 경로에 대한 Google Cloud 지역을 지정합니다(볼륨 경로는 프로젝트의 모든 클라우드 볼륨에서 고유해야 함)



5. 볼륨에 대한 성능 수준을 선택하세요.

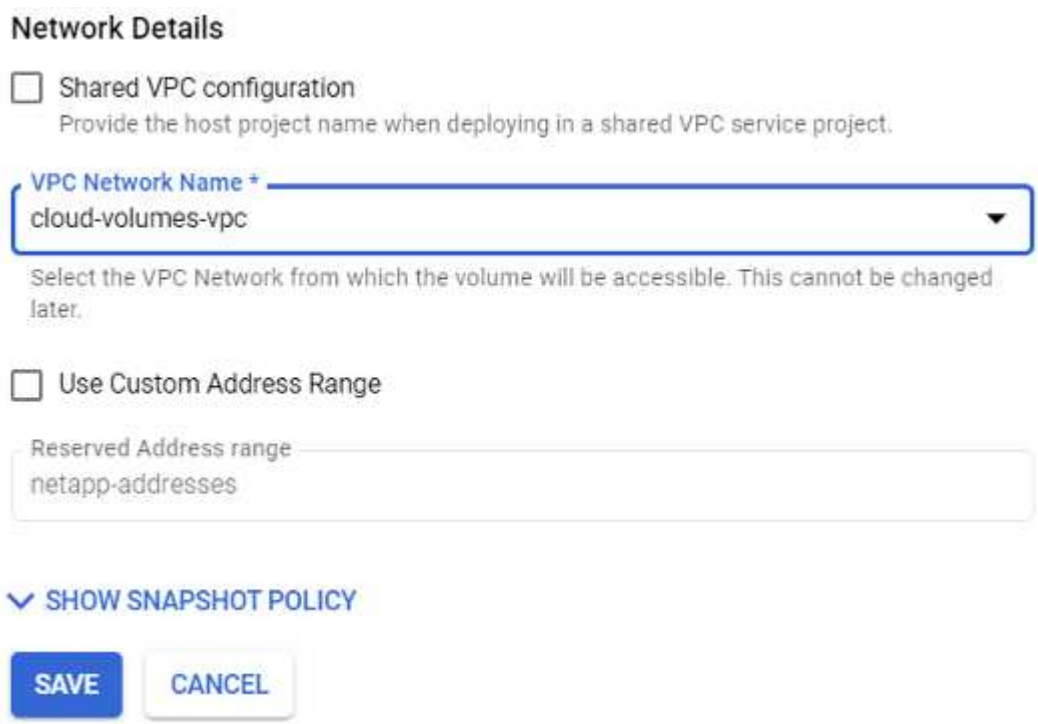


6. 볼륨 크기와 프로토콜 유형을 지정합니다. 이 테스트에서는 SMB가 사용되었습니다.



7. 이 단계에서는 볼륨에 액세스할 수 있는 VPC 네트워크를 선택합니다. VPC 피어링이 제대로 되어 있는지 확인하세요.

   힌트: VPC 피어링이 아직 수행되지 않은 경우, 피어링 명령을 안내하는 팝업 버튼이 표시됩니다. Cloud Shell 세션을 열고 적절한 명령을 실행하여 VPC를 Google Cloud NetApp Volumes producer와 피어링하십시오. VPC 피어링을 미리 준비하기로 결정한 경우, 다음 "지침"을(를) 참조하십시오.



8. 저장을 클릭하여 볼륨을 생성합니다.



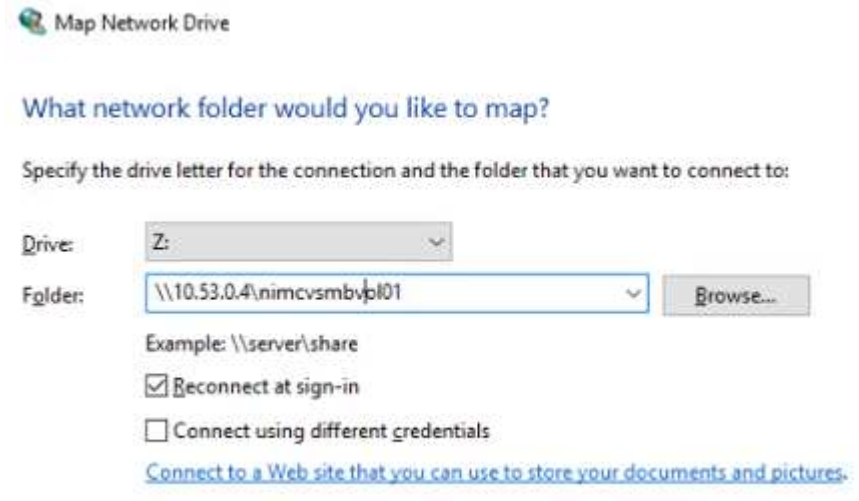
SMB 볼륨을 마운트하려면 다음을 수행하세요.

1. Cloud Console에서 Cloud Volumes > Volumes로 이동합니다.
2. 볼륨 페이지로 이동
3. SMB 공유를 매핑할 SMB 볼륨을 클릭합니다.
4. 오른쪽으로 스크롤하여 자세히 보기에서 마운트 지침을 클릭하세요.

VMware VM의 Windows 게스트 OS 내에서 마운트 프로세스를 수행하려면 아래 단계를 따르세요.

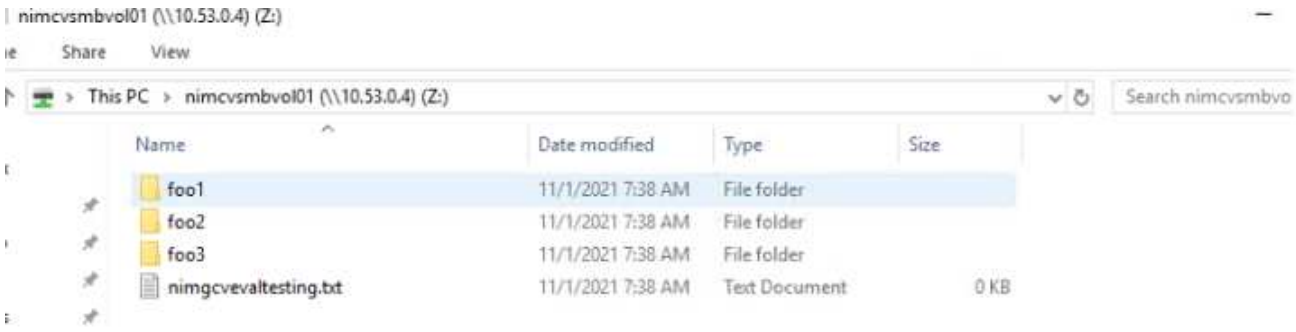
1. 시작 버튼을 클릭한 다음 컴퓨터를 클릭합니다.
2. 네트워크 드라이브 매핑을 클릭합니다.
3. 드라이브 목록에서 사용 가능한 드라이브 문자를 클릭합니다.
4. 폴더 상자에 다음을 입력합니다.

```
\\nimsmb-3830.nimgcveval.com\nimCVSMBvol01
```



컴퓨터에 로그인할 때마다 연결하려면 로그인 시 다시 연결 확인란을 선택하세요.

5. 마침을 클릭합니다.



요약 및 결론**: VMware**와 **NetApp** 하이브리드 멀티클라우드를 함께 사용하는 이유

주요 하이퍼스케일러를 위한 VMware 솔루션과 함께 NetApp Cloud Volumes는 하이브리드 클라우드를 활용하고자 하는 조직에 큰 잠재력을 제공합니다. 이 섹션의 나머지 부분에서는 NetApp Cloud Volumes를 통합하면 진정한 하이브리드 멀티클라우드 기능이 가능해지는 것을 보여주는 사용 사례를 제공합니다.

사용 사례 **#1:** 스토리지 최적화

RVtools 출력을 사용하여 크기 조정 작업을 수행할 때 마력(vCPU/vMem) 규모가 스토리지와 평행하다는 것이 항상 분명합니다. 많은 경우, 조직에서는 클러스터의 크기가 필요한 마력보다 훨씬 큰 저장 공간에 의존하게 됩니다.

NetApp Cloud Volumes를 통합하면 조직은 재플랫폼, IP 변경, 아키텍처 변경 없이 간단한 마이그레이션 방식으로 vSphere 기반 클라우드 솔루션을 실현할 수 있습니다. 또한, 이 최적화를 통해 vSphere에 필요한 최소한의 호스트 수로 유지하면서 스토리지 공간을 확장할 수 있으며, 스토리지 계층 구조, 보안 또는 사용 가능한 파일은 변경되지 않습니다. 이를 통해 배포를 최적화하고 전체 TCO를 35~45% 절감할 수 있습니다. 이러한 통합을 통해 몇 초 만에 웜 스토리지에서 프로덕션 수준의 성능으로 스토리지를 확장할 수도 있습니다.

사용 사례 **#2:** 클라우드 마이그레이션

기업들은 여러 가지 이유로 온프레미스 데이터 센터에서 퍼블릭 클라우드로 애플리케이션을 마이그레이션해야 하는 압박을 받고 있습니다. 임대 만료가 다가오고, 자본 지출(capex)에서 운영 지출(opex)로 전환하라는 재무 지침이 있고, 모든 것을 클라우드로 이전하라는 상향식 명령이 있기 때문입니다.

속도가 중요한 경우 간소화된 마이그레이션 방식만이 실행 가능합니다. 클라우드의 특정 IaaS 플랫폼에 맞게 애플리케이션을 재플랫폼하고 리팩토링하는 작업은 느리고 비용이 많이 들며, 종종 몇 달이 걸리기 때문입니다. 게스트 연결 스토리지를 위한 대역폭 효율적인 SnapMirror 복제(애플리케이션 일관성 있는 스냅샷 복사본 및 HCX와 함께 RDM, 클라우드별 마이그레이션(예: Azure Migrate) 또는 VM 복제를 위한 타사 제품 포함)와 NetApp Cloud Volumes를 결합하면 이러한 전환은 시간이 많이 소요되는 I/O 필터 메커니즘에 의존하는 것보다 훨씬 더 쉽습니다.

사용 사례 **#3:** 데이터 센터 확장

계절적 수요 급증이나 꾸준한 유기적 성장으로 인해 데이터 센터가 용량 한계에 도달하면 NetApp Cloud Volumes와 함께 클라우드 호스팅 VMware로 이전하는 것이 쉬운 솔루션입니다. NetApp Cloud Volumes를 활용하면 가용성 영역 전반에서 높은 가용성과 동적 확장 기능을 제공하여 스토리지를 매우 쉽게 생성, 복제 및 확장할 수 있습니다. NetApp Cloud Volumes를 활용하면 스트레치 클러스터의 필요성을 극복하여 호스트 클러스터 용량을 최소화하는 데 도움이 됩니다.

사용 사례 **#4:** 클라우드로의 재해 복구

기존 방식에서는 재해가 발생하면 클라우드에 복제된 VM을 복원하기 전에 클라우드 자체의 하이퍼바이저 플랫폼으로 변환해야 했습니다. 위기 상황에서 처리할 작업이 아니었습니다.

온프레미스의 SnapCenter 및 SnapMirror 복제와 퍼블릭 클라우드 가상화 솔루션을 함께 사용하여 게스트 연결 스토리지에 NetApp Cloud Volumes를 사용하면 재해 복구를 위한 더 나은 접근 방식을 고안하여 VM 복제본을 클라우드 특정 복구 도구(예: Azure Site Recovery)나 Veeam과 같은 동등한 타사 도구와 함께 완전히 일관된 VMware SDDC 인프라에서 복구할 수 있습니다. 이 접근 방식을 사용하면 재해 복구 훈련을 수행하고 랜섬웨어로부터 신속하게 복구할 수도 있습니다. 이를 통해 필요에 따라 호스트를 추가하여 테스트나 재해 발생 시 전체 운영 환경으로 확장할 수도 있습니다.

사용 사례 **#5:** 애플리케이션 현대화

애플리케이션이 퍼블릭 클라우드에 저장된 후, 조직에서는 수백 개의 강력한 클라우드 서비스를 활용하여 이를 현대화하고 확장하고자 할 것입니다. NetApp Cloud Volumes를 사용하면 애플리케이션 데이터가 vSAN에 갇히지 않고 Kubernetes를 포함한 다양한 사용 사례에서 데이터 이동성이 가능하므로 현대화가 쉽게 진행됩니다.

결론

전체 클라우드 또는 하이브리드 클라우드를 타겟으로 삼는지 여부에 관계없이 NetApp Cloud Volumes는 파일 서비스 및 블록 프로토콜과 함께 애플리케이션 워크로드를 배포하고 관리하는 탁월한 옵션을 제공하며, 데이터 요구 사항을 애플리케이션 계층에 원활하게 전달하여 TCO를 절감합니다.

어떤 사용 사례든 NetApp Cloud Volumes와 함께 원하는 클라우드/하이퍼스케일러를 선택하여 클라우드의 이점을 빠르게 실현하고, 온프레미스와 여러 클라우드에서 일관된 인프라와 운영을 구현하고, 워크로드를 양방향으로 이동시키고, 엔터프라이즈급 용량과 성능을 확보하세요.

이는 저장소를 연결하는 데 사용되는 것과 동일한 익숙한 프로세스 및 절차입니다. 새로운 이름으로 변경된 것은 단지 데이터의 위치일 뿐이며, 도구와 프로세스는 모두 동일하게 유지되며 NetApp Cloud Volumes는 전반적인 배포를 최적화하는 데 도움이 됩니다.

VMware 하이브리드 클라우드 사용 사례

VMware를 활용한 NetApp 하이브리드 멀티클라우드 사용 사례

하이브리드 클라우드 또는 클라우드 우선 배포를 계획할 때 IT 조직에 중요한 사용 사례에 대한 개요입니다.

인기 있는 사용 사례

사용 사례는 다음과 같습니다.

- 재해 복구,
- 데이터 센터 유지 관리 중 호스팅 작업, * 로컬 데이터 센터에 프로비저닝된 것 이상의 추가 리소스가 필요한 급격한 버스트
- VMware 사이트 확장,
- 클라우드로의 빠른 마이그레이션
- 개발/테스트 및
- 클라우드 보완 기술을 활용한 앱의 현대화.

이 문서 전체에서 클라우드 워크로드 참조는 VMware 사용 사례를 사용하여 자세히 설명됩니다. 이러한 사용 사례는 다음과 같습니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 이주하다
- 연장하다

IT 여정 내부

대부분의 조직은 변혁과 현대화를 향한 여정에 나섰습니다. 이러한 과정의 일환으로 기업들은 클라우드의 이점을 활용하고 마이그레이션 프로세스를 가능한 한 원활하게 만드는 방법을 모색하면서 기존 VMware 투자를 활용하려고 노력하고 있습니다. 이러한 접근 방식을 사용하면 데이터가 이미 클라우드에 있으므로 현대화 작업이 매우 수월해집니다.

이 시나리오에 대한 가장 쉬운 답은 각 하이퍼스케일러에서 VMware가 제공하는 제품입니다. NetApp Cloud Volumes와 마찬가지로 VMware는 온프레미스 VMware 환경을 모든 클라우드로 이동하거나 확장하는 방법을 제공하여 클라우드에서 기본적으로 워크로드를 실행하면서 기존 온프레미스 자산, 기술 및 도구를 유지할 수 있습니다. 이렇게 하면 서비스 중단이나 IP 변경이 필요 없기 때문에 위험이 줄어들고, IT 팀은 기존 기술과 도구를 사용하여 사내에서처럼 운영할 수 있습니다. 이를 통해 클라우드 마이그레이션이 가속화되고 하이브리드 멀티클라우드 아키텍처로의 전환이 훨씬 더 원활해질 수 있습니다.

보충 NFS 스토리지 옵션의 중요성 이해

VMware는 모든 클라우드에서 모든 고객에게 고유한 하이브리드 기능을 제공하지만, 제한된 보충 NFS 스토리지 옵션으로 인해 스토리지 사용량이 많은 작업 부하가 있는 조직에서는 유용성이 제한됩니다. 스토리지는 호스트에 직접 연결되므로 스토리지를 확장하는 유일한 방법은 호스트를 추가하는 것입니다. 그러면 스토리지를 많이 사용하는 작업의 경우 비용이 35~40% 이상 증가할 수 있습니다. 이러한 작업에는 추가 마력이 아닌 추가 저장 공간만 필요합니다. 하지만 이는 추가 호스트 비용을 지불해야 한다는 것을 의미합니다.

다음 시나리오를 생각해 보겠습니다.

어떤 고객은 CPU와 메모리에 호스트 5개만 필요하지만 저장 공간이 많이 필요하여 저장 공간 요구 사항을 충족하려면 호스트 12개가 필요합니다. 이러한 요구 사항은 저장 용량만 늘리면 되는데 추가 마력을 구매해야 하므로 결국 재정적 규모가 실제로 커지는 결과를 초래합니다.

클라우드 도입 및 마이그레이션을 계획할 때는 항상 가장 좋은 접근 방식을 평가하고 총 투자를 줄이는 가장 쉬운 경로를 선택하는 것이 중요합니다. 모든 애플리케이션 마이그레이션에 가장 일반적이고 쉬운 방법은 리호스팅(리프트 앤 시프트라고도 함)인데, 이때는 가상 머신(VM)이나 데이터 변환이 없습니다. vSAN을 보완하는 동시에 VMware 소프트웨어 정의 데이터 센터(SDDC)와 함께 NetApp Cloud Volumes를 사용하면 간편한 리프트 앤 시프트 옵션을 제공합니다.

하이퍼스케일러를 위한 **VMware**용 **NetApp** 솔루션

NetApp 각 하이퍼스케일러의 VMware 환경에 제공하는 솔루션에 대해 자세히 알아보세요. 워크플로우 마이그레이션, 클라우드로의 확장/버스팅, 백업/복원 및 재해 복구 등이 포함됩니다.

VMware 환경을 위한 **NetApp** 솔루션

하이브리드 클라우드 모델이나 "클라우드 우선" 모델에서 운영하는 경우, NetApp 클라우드 또는 하이브리드 클라우드 모델에서 워크로드를 관리하는 가장 일반적인 사용 사례를 해결하는 다양한 솔루션을 제공합니다.

NetApp 각 하이퍼스케일러에서 게스트 내부(게스트 연결) 스토리지 또는 보조 NFS 데이터 저장소로 프로비저닝된 스토리지 솔루션도 제공합니다. 모든 솔루션은 클라우드 워크로드에 대한 VMware 분류에 따라 분류됩니다. 해당 분류에는 다음이 포함됩니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 이주하다
- 연장하다

각 하이퍼스케일러에 사용 가능한 솔루션에 대한 자세한 내용은 다음을 방문하세요.

- "AWS/VMC 솔루션"
- "Azure/AVS 솔루션"
- "GCP/GCVE 솔루션"

Amazon VMware Managed Cloud(VMC)를 위한 **NetApp** 솔루션

NetApp AWS에 제공하는 솔루션에 대해 자세히 알아보세요.

VMware는 클라우드 워크로드를 다음 세 가지 범주 중 하나로 정의합니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 이주하다
- 연장하다

다음 섹션에서 사용 가능한 솔루션을 찾아보세요.

보호하다

- "AWS에서 VMC를 사용한 재해 복구(게스트 연결)"
- "FSx ONTAP 사용한 VMC에서의 Veeam 백업 및 복원"
- "FSx ONTAP 및 VMC를 사용한 재해 복구(DRO)"
- "AWS에서 VMware Cloud로의 재해 복구를 위해 Veeam Replication 및 FSx ONTAP 사용"

이주하다

- "VMware HCX를 사용하여 FSx ONTAP 데이터 저장소로 워크로드 마이그레이션"

연장하다

곧 출시됩니다!!

Azure VMware 솔루션(AVS)을 위한 NetApp 솔루션

NetApp 이 Azure에 제공하는 솔루션에 대해 자세히 알아보세요.

VMware는 클라우드 워크로드를 다음 세 가지 범주 중 하나로 정의합니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 이주하다
- 연장하다

다음 섹션에서 사용 가능한 솔루션을 찾아보세요.

보호하다

- "ANF 및 JetStream(보조 NFS 데이터 저장소)을 사용한 재해 복구"
- "ANF 및 CVO(게스트 연결 스토리지)를 사용한 재해 복구"
- "ANF 및 AVS를 사용한 재해 복구(DRO)"
- "Azure VMware 솔루션으로의 재해 복구를 위해 Veeam Replication 및 Azure NetApp Files 데이터 저장소 사용"

이주하다

- "VMware HCX를 사용하여 Azure NetApp Files 데이터 저장소로 워크로드 마이그레이션"

연장하다

곧 출시됩니다!!

Google Cloud VMware Engine(GCVE)을 위한 NetApp 솔루션

NetApp GCP에 제공하는 솔루션에 대해 자세히 알아보세요.

VMware는 클라우드 워크로드를 다음 세 가지 범주 중 하나로 정의합니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 이주하다
- 연장하다

다음 섹션에서 사용 가능한 솔루션을 찾아보세요.

보호하다

- "SnapCenter, Cloud Volumes ONTAP 및 Veeam 복제를 통한 애플리케이션 재해 복구"
- "NetApp SnapCenter 및 Veeam을 통한 GCVE의 NetApp 볼륨에 대한 애플리케이션 일관성 재해 복구"

이주하다

- "VMware HCX를 사용하여 Google Cloud NetApp Volumes NFS 데이터 저장소로 워크로드 마이그레이션"
- "Veeam을 사용하여 Google Cloud NetApp Volumes NFS 데이터 저장소로 VM 복제"

연장하다

곧 출시됩니다!!

AWS/VMC용 NetApp

AWS VMC를 위한 NetApp 기능

NetApp AWS VMware Cloud(VMC)에 제공하는 기능에 대해 자세히 알아보세요. NetApp 게스트 연결 스토리지 장치 또는 보조 NFS 데이터 저장소로 활용하는 것부터 워크플로 마이그레이션, 클라우드로의 확장/버스팅, 백업/복원 및 재해 복구까지 다양한 기능을 제공합니다.

다음 옵션 중에서 선택하여 원하는 콘텐츠 섹션으로 이동하세요.

- "AWS에서 VMC 구성"
- "VMC용 NetApp 스토리지 옵션"
- "NetApp / VMware 클라우드 솔루션"

AWS에서 VMC 구성

온프레미스와 마찬가지로, VM을 만들고 마이그레이션하기 위한 성공적인 프로덕션 준비 환경을 위해서는 클라우드 기반 가상화 환경을 계획하는 것이 중요합니다.

이 섹션에서는 AWS SDDC에서 VMware Cloud를 설정하고 관리하는 방법과 NetApp 스토리지를 연결하는 데 사용 가능한 옵션과 함께 사용하는 방법을 설명합니다.

> ⓘ 게스트 내 스토리지는 Cloud Volumes ONTAP AWS VMC에 연결하는 데 지원되는 유일한 방법입니다.

설정 과정은 다음 단계로 나눌 수 있습니다.

- AWS용 VMware Cloud 배포 및 구성
- VMware Cloud를 FSx ONTAP 에 연결

자세한 내용을 보려면"VMC 구성 단계" .

VMC용 **NetApp** 스토리지 옵션

NetApp 스토리지는 AWS VMC 내에서 추측 연결 또는 보조 NFS 데이터 저장소로 등 여러 가지 방법으로 활용할 수 있습니다.

방문해주세요"지원되는 NetApp 스토리지 옵션" 자세한 내용은.

AWS는 다음 구성에서 NetApp 스토리지를 지원합니다.

- 게스트 연결 스토리지로서의 FSx ONTAP
- 게스트 연결 스토리지로서의 Cloud Volumes ONTAP (CVO)
- 보충 NFS 데이터 저장소로서의 FSx ONTAP

자세한 내용을 보려면"VMC용 게스트 연결 스토리지 옵션" . 자세한 내용을 보려면"VMC에 대한 보충 NFS 데이터 저장소 옵션" .

솔루션 사용 사례

NetApp 및 VMware 클라우드 솔루션을 사용하면 많은 사용 사례를 AWS VMC에 간편하게 배포할 수 있습니다. VMware에서 정의한 각 클라우드 영역에 대한 사용 사례가 정의됩니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 연장하다
- 이주하다

"AWS VMC용 NetApp 솔루션 찾아보기"

AWS/VMC에서 워크로드 보호

TR-4931: Amazon Web Services 및 **Guest Connect**에서 **VMware Cloud**를 사용한 재해 복구

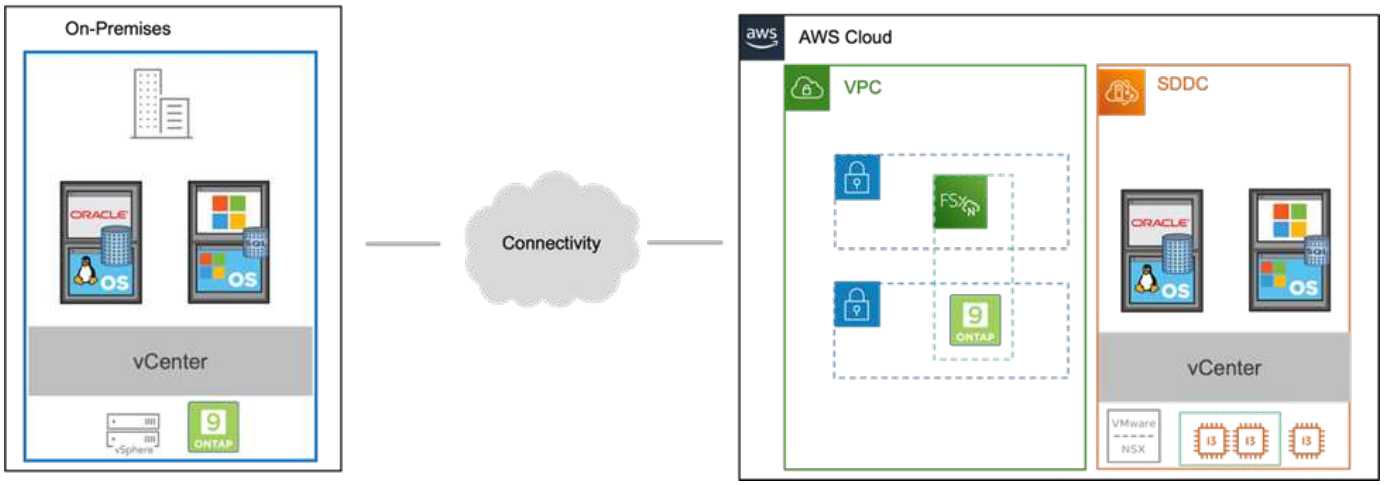
검증된 재해 복구(DR) 환경과 계획은 조직이 주요 비즈니스 중단 발생 시에도 비즈니스에 중요한 애플리케이션을 신속하게 복구할 수 있도록 하는 데 필수적입니다. 이 솔루션은 온프레미스와 AWS의 VMware Cloud를 모두 활용한 VMware 및 NetApp 기술에 초점을 맞춰 DR 사용 사례를 보여주는 데 중점을 둡니다.

개요

NetApp VMware와 오랫동안 통합을 이루어 왔으며, 이는 수만 명의 고객이 가상화 환경을 위한 스토리지 파트너로 NetApp 선택한 것에서 입증됩니다. 이러한 통합은 클라우드의 게스트 연결 옵션과 최근 NFS 데이터 저장소와의 통합에서도 계속됩니다. 이 솔루션은 일반적으로 게스트 연결 스토리지라고 하는 사용 사례에 초점을 맞춥니다.

게스트 연결 스토리지에서는 게스트 VMDK가 VMware에서 제공하는 데이터 저장소에 배포되고, 애플리케이션 데이터는 iSCSI 또는 NFS에 저장되어 VM에 직접 매핑됩니다. 다음 그림에서 볼 수 있듯이 Oracle 및 MS SQL

애플리케이션은 DR 시나리오를 설명하는 데 사용됩니다.



가정, 전제 조건 및 구성 요소 개요

이 솔루션을 배포하기 전에 구성 요소 개요, 솔루션을 배포하는 데 필요한 사전 요구 사항, 이 솔루션을 문서화하는 데 필요한 가정 사항을 검토하세요.

"DR 솔루션 요구 사항, 사전 요구 사항 및 계획"

SnapCenter 사용하여 **DR** 수행

이 솔루션에서 SnapCenter SQL Server 및 Oracle 애플리케이션 데이터에 대한 애플리케이션 일관성 스냅샷을 제공합니다. 이 구성은 SnapMirror 기술과 함께 온프레미스 AFF 와 FSx ONTAP 클러스터 간에 고속 데이터 복제를 제공합니다. 또한, Veeam Backup & Replication은 가상 머신에 대한 백업 및 복원 기능을 제공합니다.

이 섹션에서는 백업과 복원을 위한 SnapCenter, SnapMirror 및 Veeam의 구성에 대해 다룹니다.

다음 섹션에서는 보조 사이트에서 장애 조치를 완료하는 데 필요한 구성과 단계를 다룹니다.

SnapMirror 관계 및 보존 일정 구성

SnapCenter 장기 보관 및 보존 목적으로 기본 스토리지 시스템(기본 > 미러) 및 보조 스토리지 시스템(기본 > 볼트) 내의 SnapMirror 관계를 업데이트할 수 있습니다. 이를 위해 SnapMirror 사용하여 대상 볼륨과 소스 볼륨 간의 데이터 복제 관계를 설정하고 초기화해야 합니다.

소스 및 대상 ONTAP 시스템은 Amazon VPC 피어링, 전송 게이트웨이, AWS Direct Connect 또는 AWS VPN을 사용하여 피어링된 네트워크에 있어야 합니다.

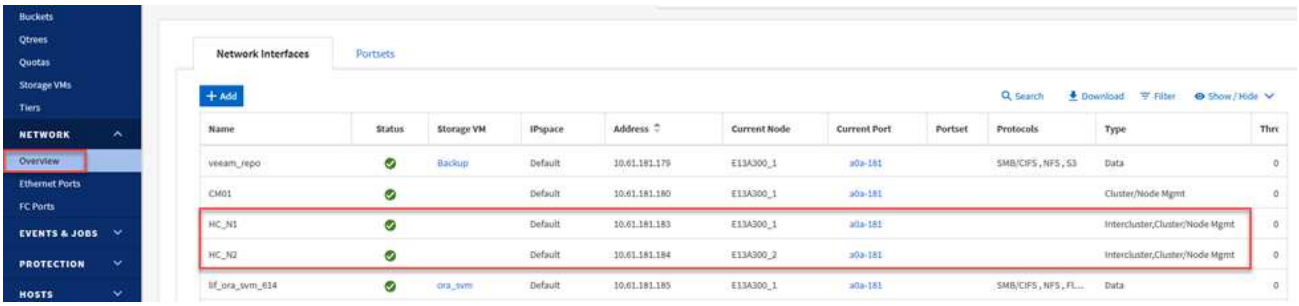
온프레미스 ONTAP 시스템과 FSx ONTAP 간의 SnapMirror 관계를 설정하려면 다음 단계가 필요합니다.

를 참조하세요 "FSx ONTAP – ONTAP 사용자 가이드" FSx를 사용하여 SnapMirror 관계를 만드는 방법에 대한 자세한 내용은 다음을 참조하세요.

▼ 소스 및 대상 **Intercluster** 논리 인터페이스를 기록합니다.

온프레미스에 있는 소스 ONTAP 시스템의 경우 시스템 관리자나 CLI에서 클러스터 간 LIF 정보를 검색할 수 있습니다.

1. ONTAP System Manager에서 네트워크 개요 페이지로 이동하여 FSx가 설치된 AWS VPC와 통신하도록 구성된 유형: 클러스터 간 IP 주소를 검색합니다.



2. FSx의 Intercluster IP 주소를 검색하려면 CLI에 로그인하고 다음 명령을 실행하세요.

```
FSx-Dest::> network interface show -role intercluster
```

```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
FsxId0ae40e08acc0dea67
            inter_1      up/up    172.30.15.42/25    FsxId0ae40e08acc0dea67-01
                                                                   e0e     true
            inter_2      up/up    172.30.14.28/26    FsxId0ae40e08acc0dea67-02
                                                                   e0e     true
2 entries were displayed.
```

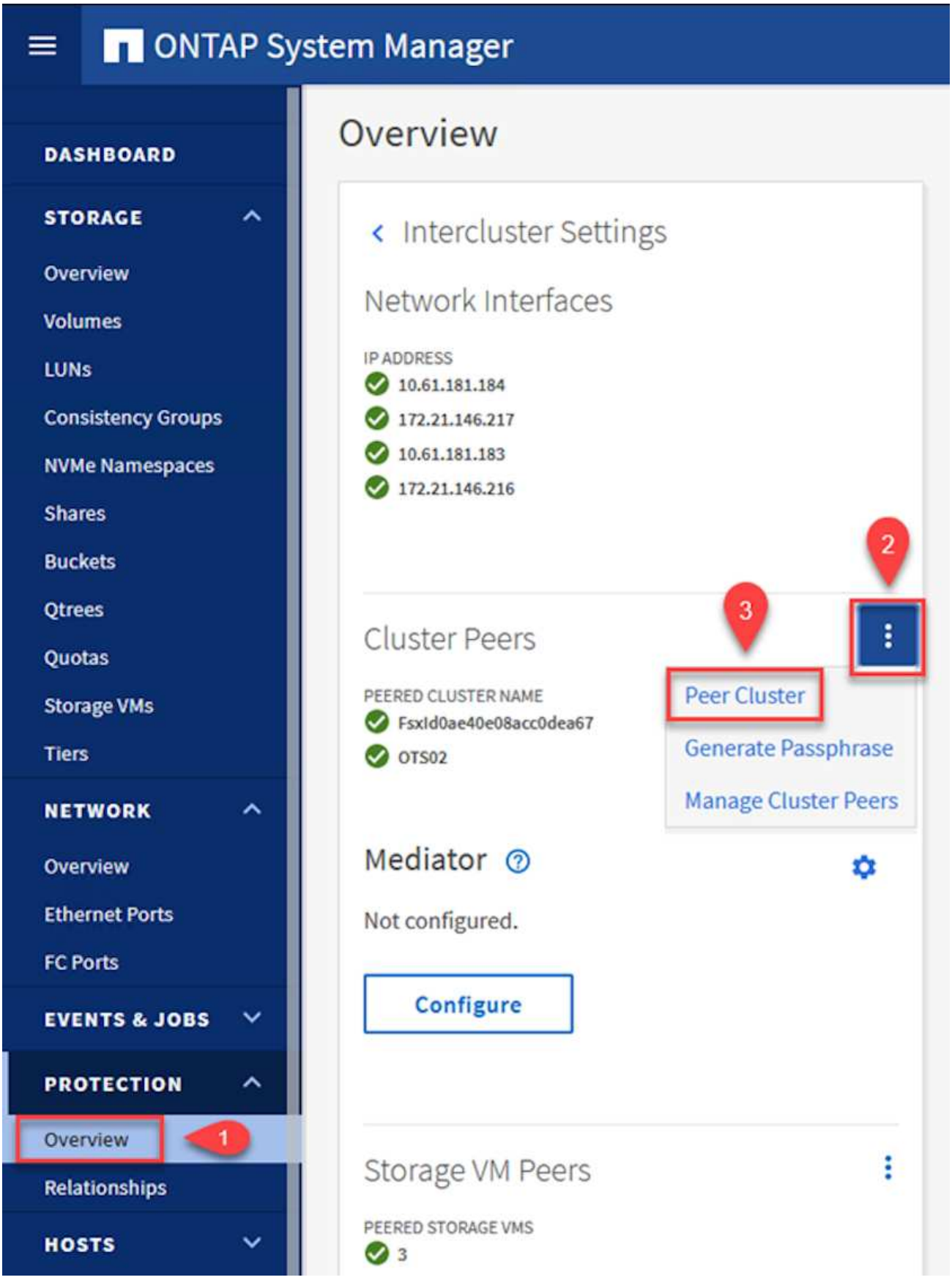
▼ **ONTAP** 과 **FSx** 간 클러스터 피어링 설정

ONTAP 클러스터 간에 클러스터 피어링을 설정하려면 시작 ONTAP 클러스터에서 입력한 고유한 암호문구를 다른 피어 클러스터에서 확인해야 합니다.

1. 다음을 사용하여 대상 FSx 클러스터에서 피어링을 설정합니다. `cluster peer create` 명령. 메시지가 표시되면 나중에 소스 클러스터에서 생성 프로세스를 마무리하는 데 사용되는 고유한 암호구를 입력합니다.

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. 소스 클러스터에서 ONTAP 시스템 관리자나 CLI를 사용하여 클러스터 피어 관계를 설정할 수 있습니다. ONTAP 시스템 관리자에서 보호 > 개요로 이동하여 피어 클러스터를 선택합니다.

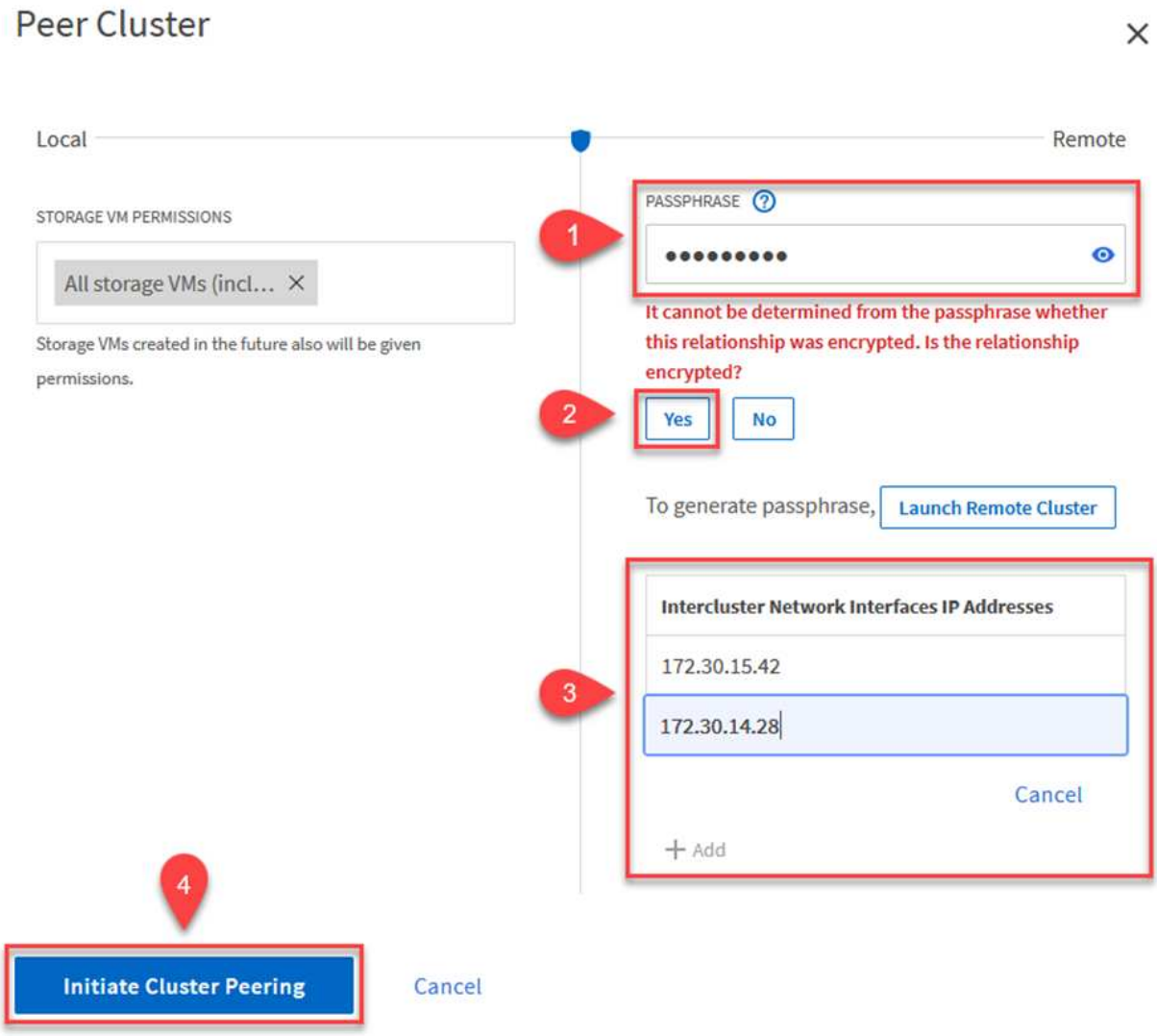


3. 피어 클러스터 대화 상자에서 필요한 정보를 입력합니다.
   a. 대상 FSx 클러스터에서 피어 클러스터 관계를 설정하는 데 사용된 암호를 입력하세요.

b. 선택하다 `Yes` 암호화된 관계를 구축합니다.

c. 대상 FSx 클러스터의 클러스터 간 LIF IP 주소를 입력하세요.

d. 클러스터 피어링 시작을 클릭하여 프로세스를 마무리합니다.



4. 다음 명령을 사용하여 FSx 클러스터에서 클러스터 피어 관계 상태를 확인하세요.

```
FSx-Dest::> cluster peer show
```

```
FsxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability   Authentication
------------------------- --------------------- -------------- --------------
E13A300                   1-80-000011           Available      ok
```

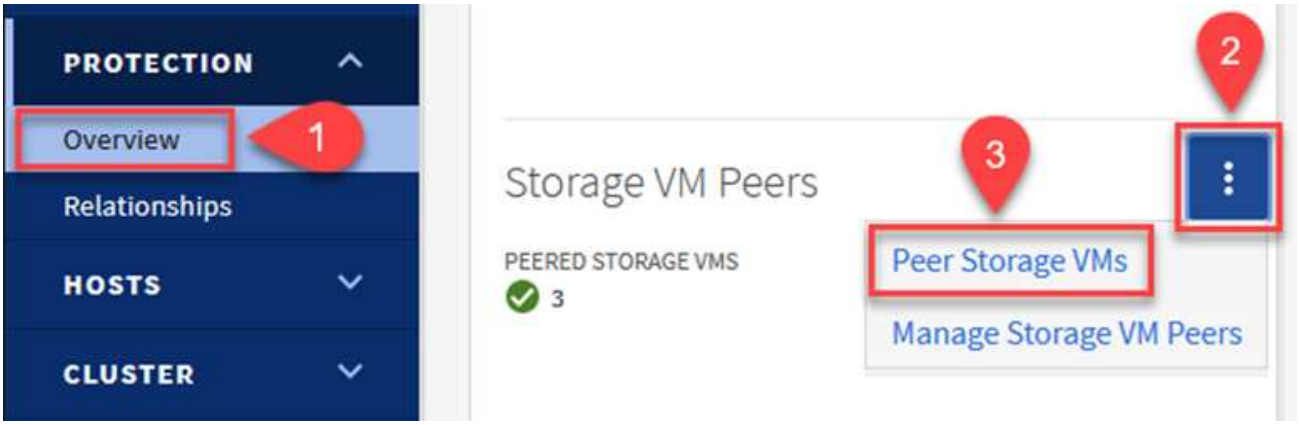
▼ **SVM** 피어링 관계 설정

다음 단계는 SnapMirror 관계에 포함될 볼륨을 포함하는 대상 및 소스 스토리지 가상 머신 간에 SVM 관계를 설정하는 것입니다.

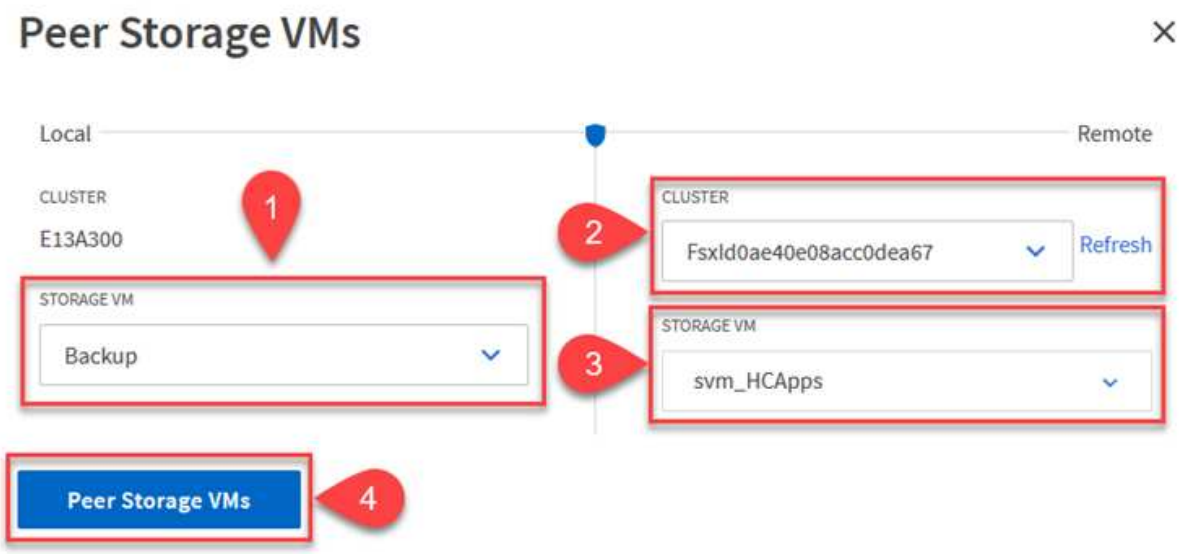
1. 소스 FSx 클러스터에서 CLI에서 다음 명령을 사용하여 SVM 피어 관계를 만듭니다.

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver Backup
-peer-cluster OnPremSourceSVM -applications snapmirror
```

2. 소스 ONTAP 클러스터에서 ONTAP 시스템 관리자나 CLI를 사용하여 피어링 관계를 수락합니다.
3. ONTAP 시스템 관리자에서 보호 > 개요로 이동하여 스토리지 VM 피어 아래에서 피어 스토리지 VM을 선택합니다.



4. Peer Storage VM 대화 상자에서 필수 필드를 작성합니다.
   - 소스 스토리지 VM
   - 대상 클러스터
   - 대상 저장소 VM



5. SVM 피어링 프로세스를 완료하려면 Peer Storage VMs를 클릭하세요.

▼ 스냅샷 보존 정책 생성

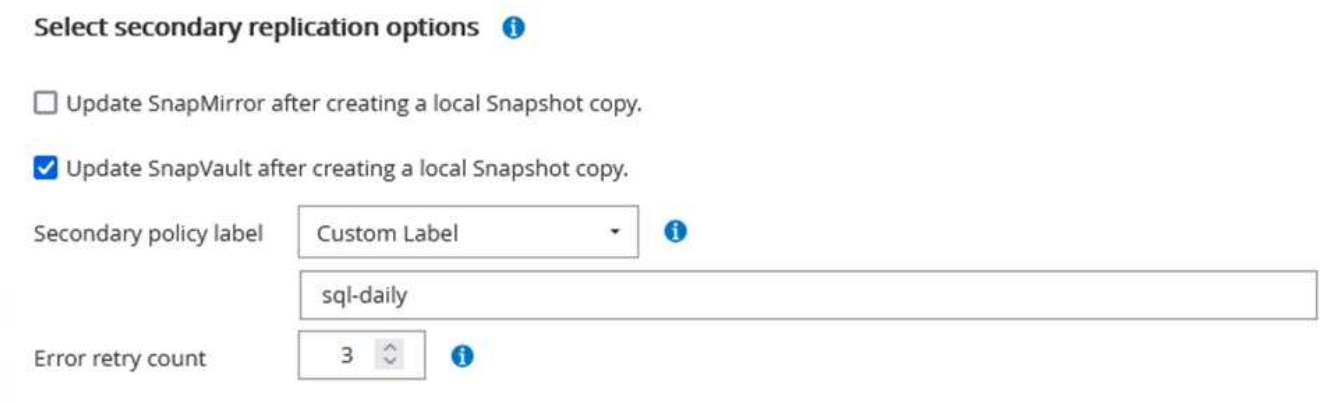
SnapCenter 기본 스토리지 시스템에 스냅샷 복사본으로 존재하는 백업의 보존 일정을 관리합니다. 이는

SnapCenter 에서 정책을 생성할 때 설정됩니다. SnapCenter 보조 스토리지 시스템에 보관된 백업에 대한 보존 정책을 관리하지 않습니다. 이러한 정책은 보조 FSx 클러스터에서 생성되고 소스 볼륨과 SnapMirror 관계에 있는 대상 볼륨과 연관된 SnapMirror 정책을 통해 별도로 관리됩니다.

SnapCenter 정책을 생성할 때 SnapCenter 백업이 수행될 때 생성되는 각 스냅샷의 SnapMirror 레이블에 추가되는 보조 정책 레이블을 지정하는 옵션이 있습니다.

> ⓘ 보조 저장소에서 이러한 레이블은 스냅샷 보존을 강제하기 위해 대상 볼륨과 연관된 정책 규칙과 일치합니다.

다음 예제는 SQL Server 데이터베이스와 로그 볼륨의 일일 백업에 사용되는 정책의 일부로 생성된 모든 스냅샷에 존재하는 SnapMirror 레이블을 보여줍니다.



SQL Server 데이터베이스에 대한 SnapCenter 정책을 만드는 방법에 대한 자세한 내용은 다음을 참조하세요. "SnapCenter 문서" .

먼저 보존할 스냅샷 복사본의 수를 결정하는 규칙이 포함된 SnapMirror 정책을 만들어야 합니다.

1. FSx 클러스터에서 SnapMirror 정책을 만듭니다.

```
FSx-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. SnapCenter 정책에 지정된 보조 정책 레이블과 일치하는 SnapMirror 레이블이 있는 정책에 규칙을 추가합니다.

```
FSx-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

   다음 스크립트는 정책에 추가할 수 있는 규칙의 예를 제공합니다.

```
FSx-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy
Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

각 SnapMirror 레이블과 보관할 스냅샷 수(보관 기간)에 대한 추가 규칙을 만듭니다.

▼ 대상 볼륨 생성

소스 볼륨의 스냅샷 복사본을 수신할 FSx에 대상 볼륨을 생성하려면 FSx ONTAP 에서 다음 명령을 실행합니다.

```
FSx-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

▼ 소스 볼륨과 대상 볼륨 간의 **SnapMirror** 관계 생성

소스 볼륨과 대상 볼륨 사이에 SnapMirror 관계를 생성하려면 FSx ONTAP 에서 다음 명령을 실행합니다.

```
FSx-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

▼ **SnapMirror** 관계 초기화

SnapMirror 관계를 초기화합니다. 이 프로세스는 소스 볼륨에서 생성된 새로운 스냅샷을 시작하고 대상 볼륨에 복사합니다.

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

온프레미스에 **Windows SnapCenter** 서버를 배포하고 구성합니다**.**

▼ 온프레미스에 **Windows SnapCenter** 서버 배포

이 솔루션은 NetApp SnapCenter 사용하여 SQL Server 및 Oracle 데이터베이스의 애플리케이션 일관성 백업을 수행합니다. 가상 머신 VMDK를 백업하기 위한 Veeam Backup & Replication과 함께 사용하면 온프레미스 및 클라우드 기반 데이터 센터를 위한 포괄적인 재해 복구 솔루션을 제공합니다.

SnapCenter software NetApp 지원 사이트에서 구할 수 있으며 도메인이나 작업 그룹에 있는 Microsoft Windows 시스템에 설치할 수 있습니다. 자세한 계획 가이드와 설치 지침은 다음에서 확인할 수 있습니다. "NetApp 문서 센터" .

SnapCenter software 다음에서 구할 수 있습니다. "이 링크" .

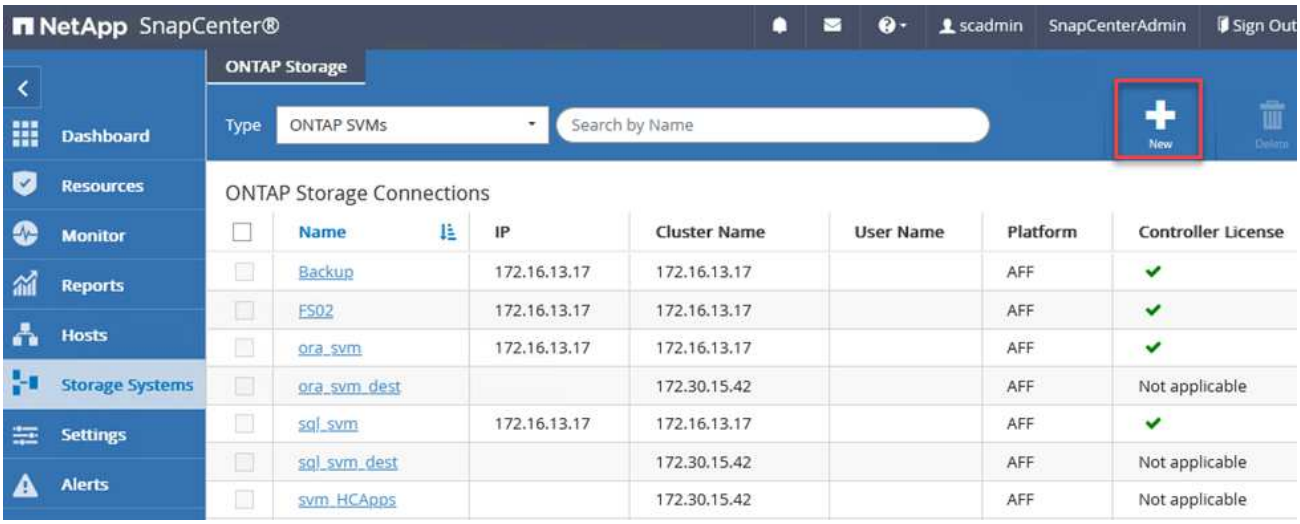
설치가 완료되면 웹 브라우저에서 _\https://Virtual_Cluster_IP_or_FQDN:8146_을 사용하여 SnapCenter 콘솔에 액세스할 수 있습니다.

콘솔에 로그인한 후 SQL Server 및 Oracle 데이터베이스를 백업하기 위해 SnapCenter 구성해야 합니다.

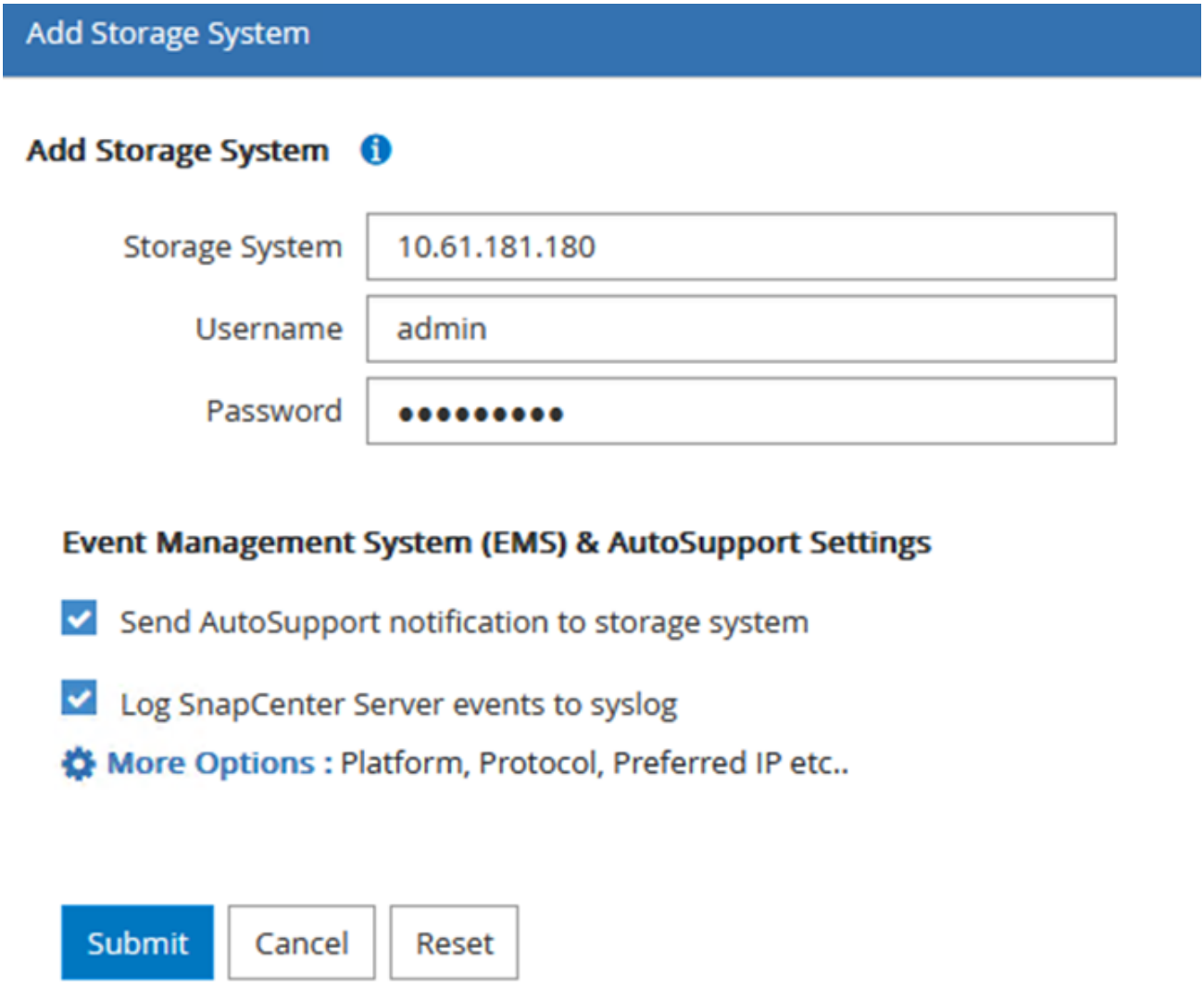
▼ **SnapCenter** 에 스토리지 컨트롤러 추가

SnapCenter 에 스토리지 컨트롤러를 추가하려면 다음 단계를 완료하세요.

1. 왼쪽 메뉴에서 스토리지 시스템을 선택한 다음 새로 만들기를 클릭하여 SnapCenter 에 스토리지 컨트롤러를 추가하는 프로세스를 시작합니다.

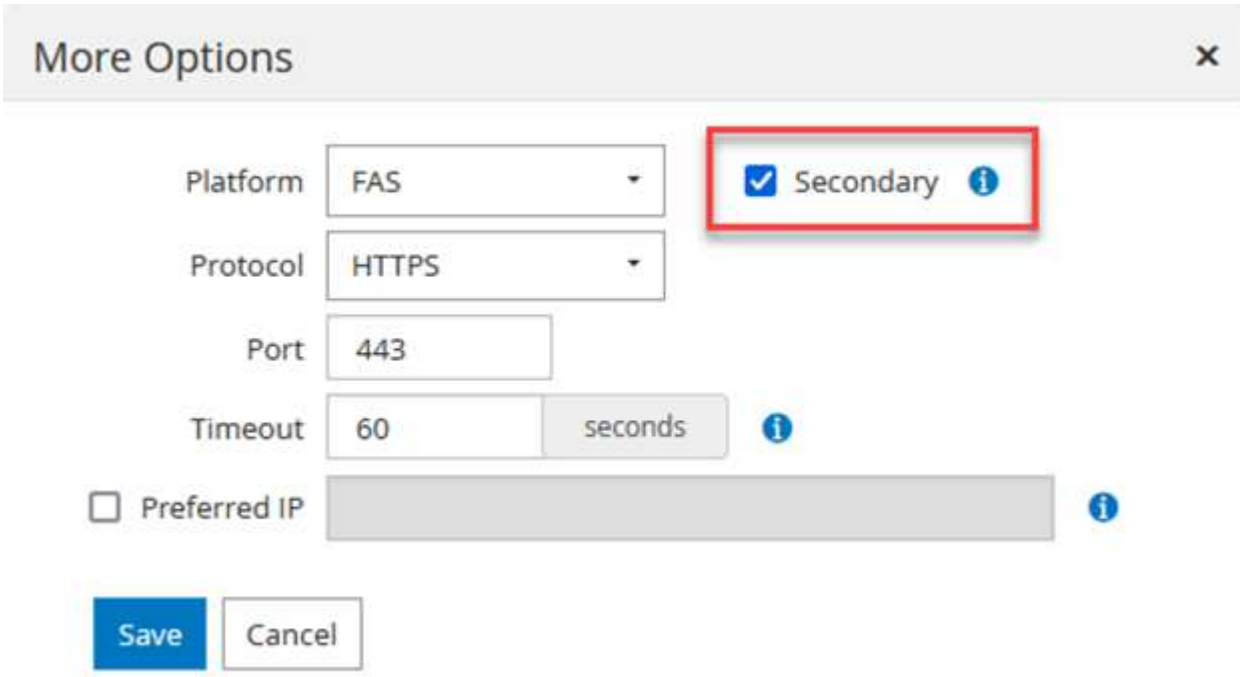


2. 스토리지 시스템 추가 대화 상자에서 로컬 온프레미스 ONTAP 클러스터의 관리 IP 주소와 사용자 이름 및 비밀번호를 추가합니다. 그런 다음 제출을 클릭하여 스토리지 시스템 검색을 시작하세요.



3. SnapCenter 에 FSx ONTAP 시스템을 추가하려면 이 프로세스를 반복합니다. 이 경우, 스토리지 시스템 추가 창 하단에서 추가 옵션을 선택하고 보조 스토리지 시스템의 확인란을 클릭하여 FSx 시스템을 SnapMirror

복사본이나 기본 백업 스냅샷으로 업데이트된 보조 스토리지 시스템으로 지정합니다.

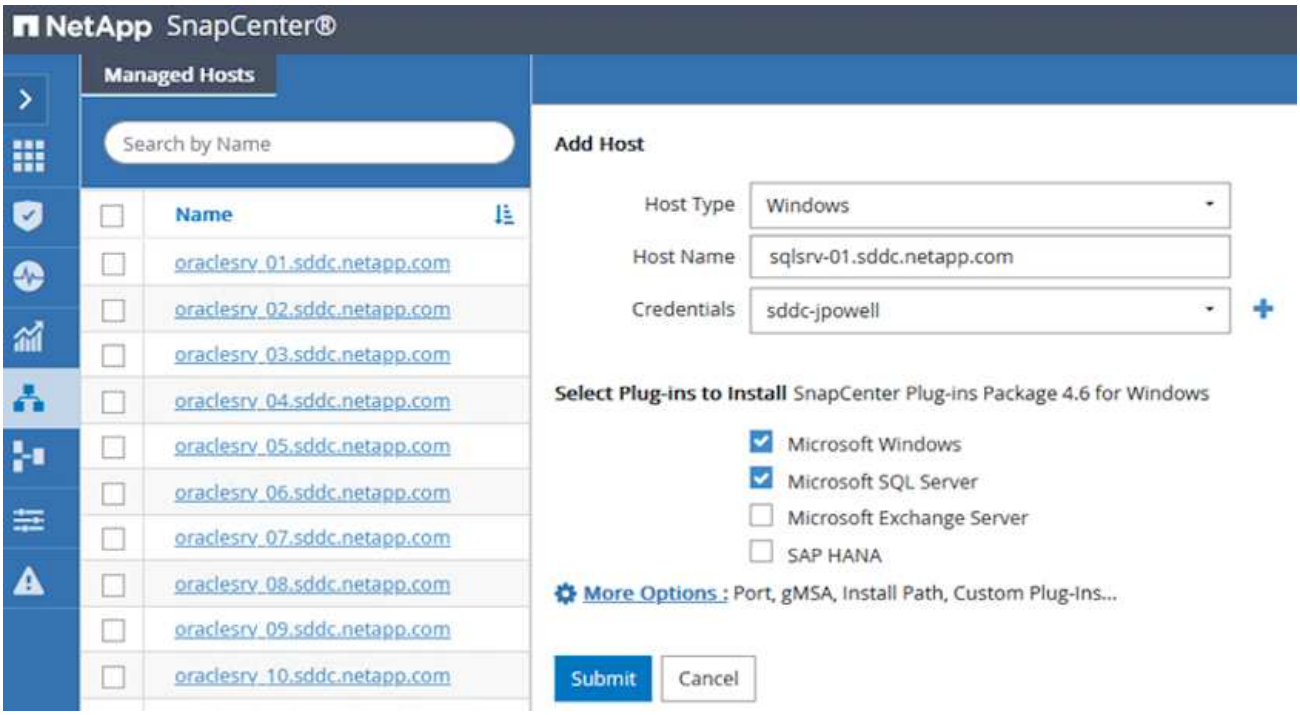


SnapCenter 에 스토리지 시스템을 추가하는 것과 관련된 자세한 내용은 다음 설명서를 참조하세요. "이 링크" .

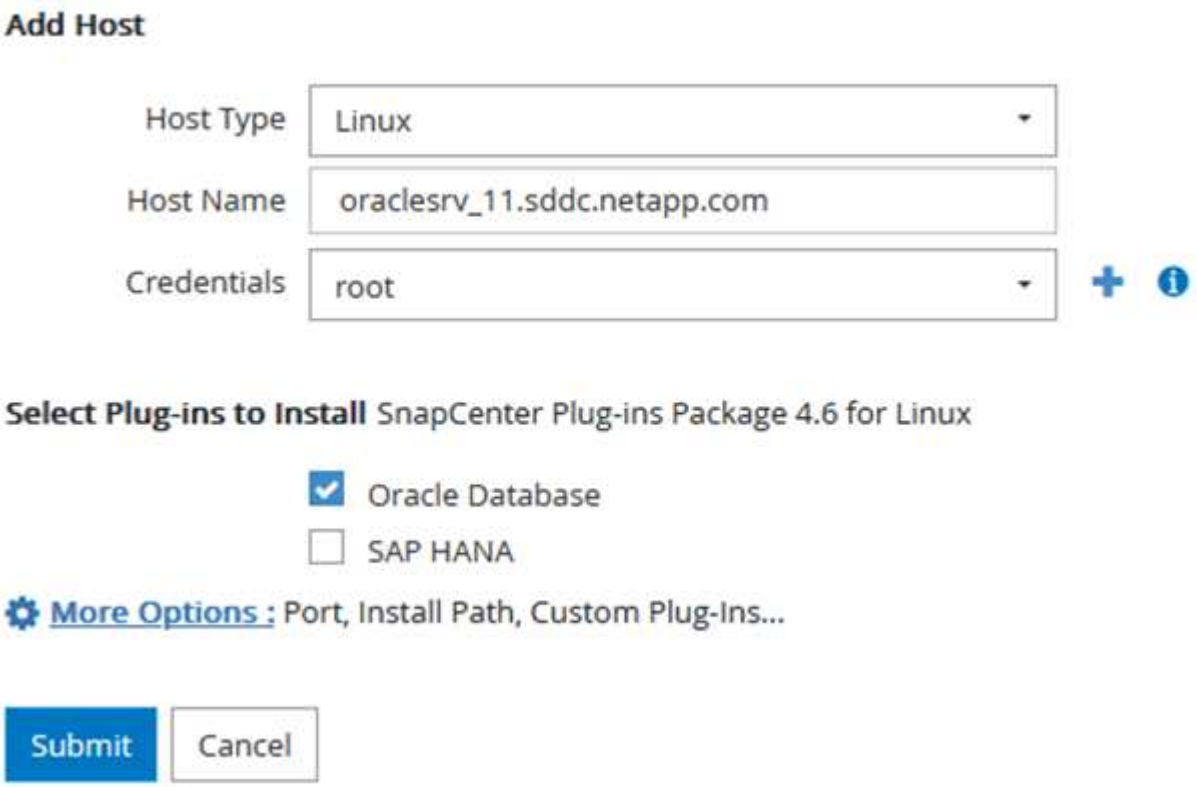
▼ **SnapCenter** 에 호스트 추가

다음 단계는 SnapCenter 에 호스트 애플리케이션 서버를 추가하는 것입니다. SQL Server와 Oracle의 프로세스는 비슷합니다.

1. 왼쪽 메뉴에서 호스트를 선택한 다음 추가를 클릭하여 SnapCenter 에 스토리지 컨트롤러를 추가하는 프로세스를 시작합니다.
2. 호스트 추가 창에서 호스트 유형, 호스트 이름 및 호스트 시스템 자격 증명을 추가합니다. 플러그인 유형을 선택하세요. SQL Server의 경우 Microsoft Windows 및 Microsoft SQL Server 플러그인을 선택하세요.



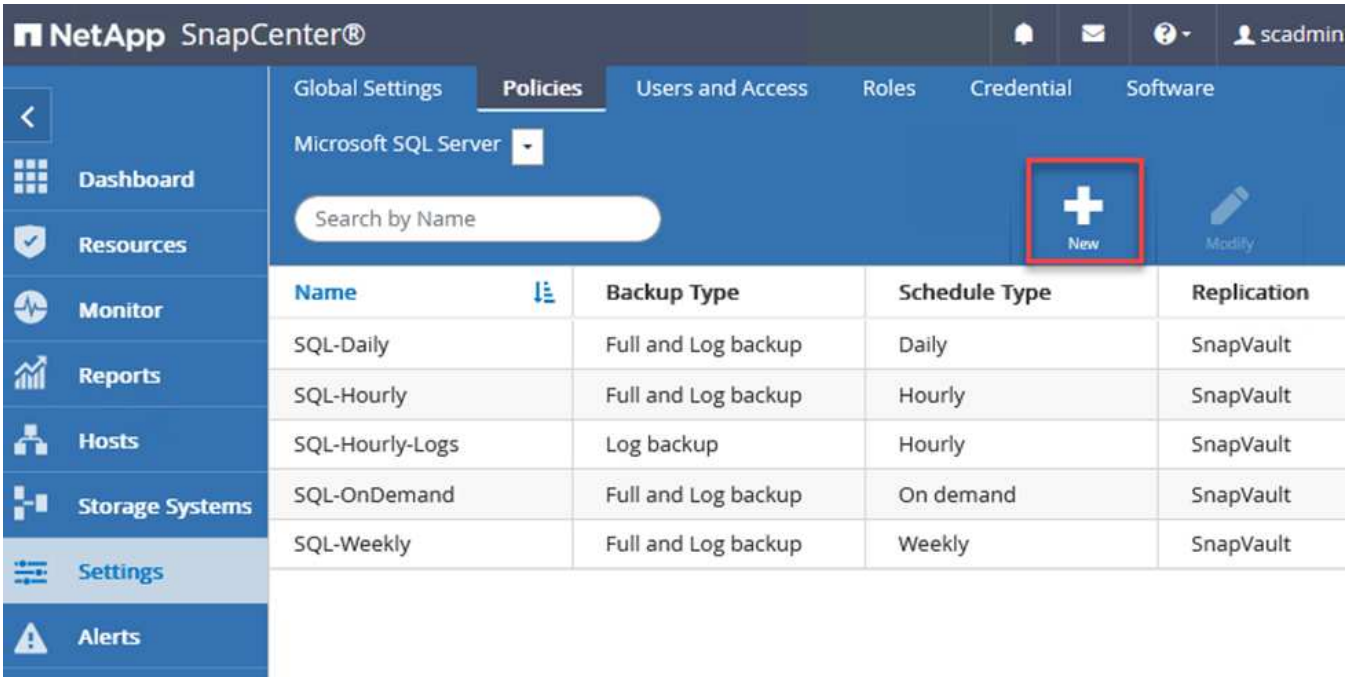
3. Oracle의 경우, "호스트 추가" 대화 상자에서 필수 필드를 입력하고 Oracle 데이터베이스 플러그인 확인란을 선택합니다. 그런 다음 "제출"을 클릭하여 검색 프로세스를 시작하고 SnapCenter 에 호스트를 추가합니다.



▼ **SnapCenter** 정책 만들기

정책은 백업 작업에 따라야 할 구체적인 규칙을 설정합니다. 여기에는 백업 일정, 복제 유형, SnapCenter 트랜잭션 로그 백업 및 잘라내기를 처리하는 방법 등이 포함되지만 이에 국한되지는 않습니다.

SnapCenter 웹 클라이언트의 설정 섹션에서 정책에 액세스할 수 있습니다.



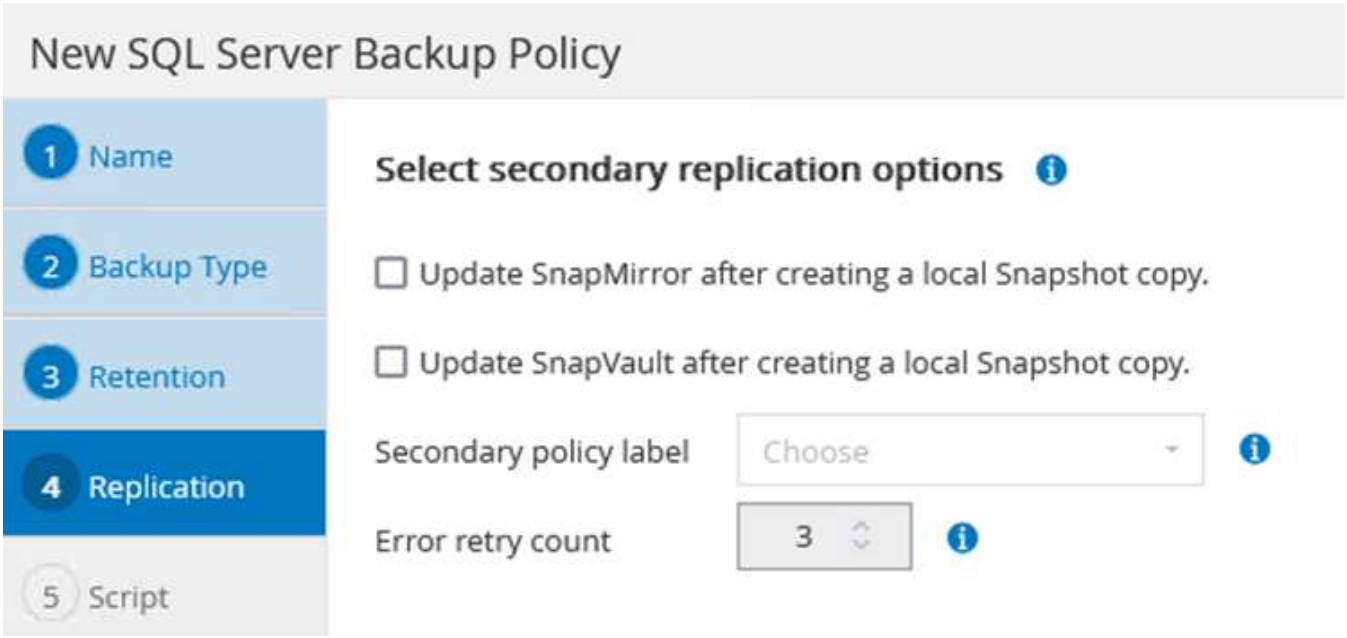
SQL Server 백업에 대한 정책 생성에 대한 전체 정보는 다음을 참조하세요. "SnapCenter 문서" .

Oracle 백업에 대한 정책 생성에 대한 전체 정보는 다음을 참조하세요. "SnapCenter 문서" .

참고사항:

- 정책 생성 마법사를 진행하면서 복제 섹션을 특별히 주의하세요. 이 섹션에서는 백업 프로세스 중에 생성할 보조 SnapMirror 복사본 유형을 지정합니다.
- "로컬 스냅샷 복사본을 만든 후 SnapMirror 업데이트" 설정은 동일한 클러스터에 있는 두 스토리지 가상 머신 간에 SnapMirror 관계가 있는 경우 해당 관계를 업데이트하는 것을 의미합니다.
- "로컬 SnapShot 복사본을 만든 후 SnapVault 업데이트" 설정은 두 개의 별도 클러스터와 온프레미스 ONTAP 시스템과 Cloud Volumes ONTAP 또는 FSx ONTAP 사이에 존재하는 SnapMirror 관계를 업데이트하는 데 사용됩니다.

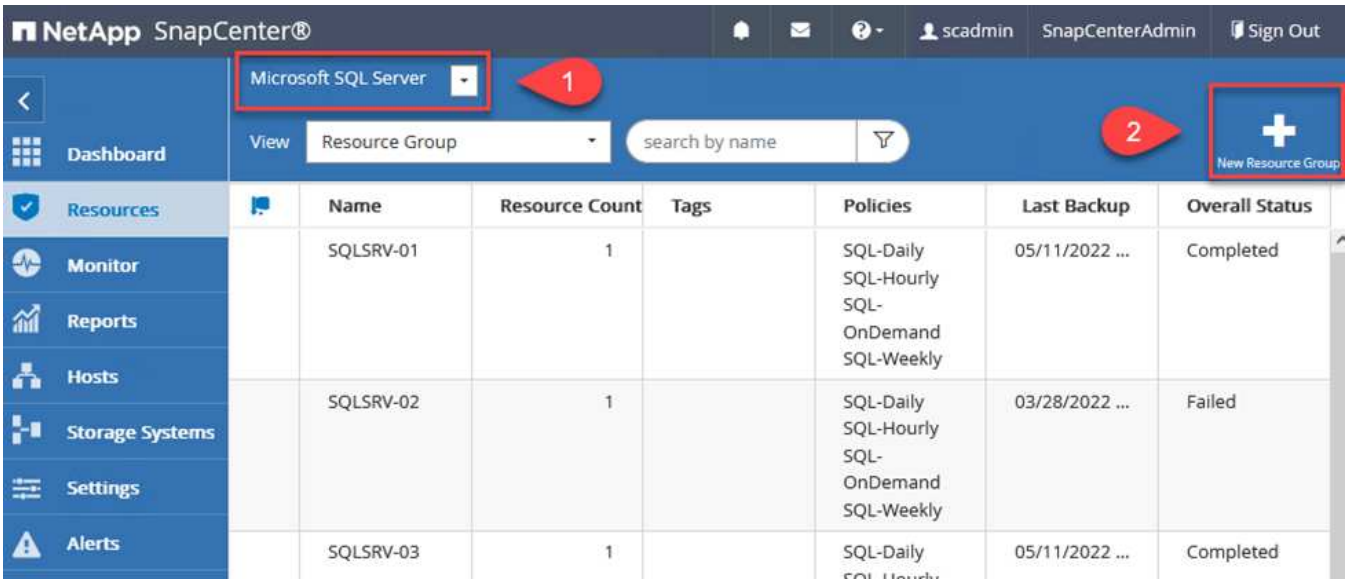
다음 이미지는 이전 옵션과 백업 정책 마법사에서 이 옵션이 어떻게 나타나는지 보여줍니다.



▼ **SnapCenter** 리소스 그룹 만들기

리소스 그룹을 사용하면 백업에 포함할 데이터베이스 리소스와 해당 리소스에 적용할 정책을 선택할 수 있습니다.

1. 왼쪽 메뉴의 리소스 섹션으로 이동하세요.
2. 창 상단에서 작업할 리소스 유형을 선택합니다(이 경우 Microsoft SQL Server). 그런 다음 새 리소스 그룹을 클릭합니다.



SnapCenter 설명서에서는 SQL Server와 Oracle 데이터베이스 모두에 대한 리소스 그룹을 만드는 방법에 대한 단계별 세부 정보를 다룹니다.

SQL 리소스를 백업하려면 다음을 따르세요. "이 링크" .

Oracle 리소스를 백업하려면 다음을 따르세요. "이 링크" .

Veeam 백업 서버 배포 및 구성

Veeam Backup & Replication 소프트웨어는 Veeam 스케일아웃 백업 저장소(SOBR)를 사용하여 애플리케이션 가상 머신을 백업하고 백업 사본을 Amazon S3 버킷에 보관하는 솔루션에 사용됩니다. 이 솔루션에서는 Veeam이 Windows 서버에 배포됩니다. Veeam 배포에 대한 구체적인 지침은 다음을 참조하세요. "Veeam 도움말 센터 기술 문서" .

▼ **Veeam** 스케일아웃 백업 저장소 구성

소프트웨어를 배포하고 라이선스를 취득한 후 백업 작업의 대상 저장소로 SOBR(스케일아웃 백업 저장소)을 생성할 수 있습니다. 재해 복구를 위해 VM 데이터의 백업으로 S3 버킷도 포함해야 합니다.

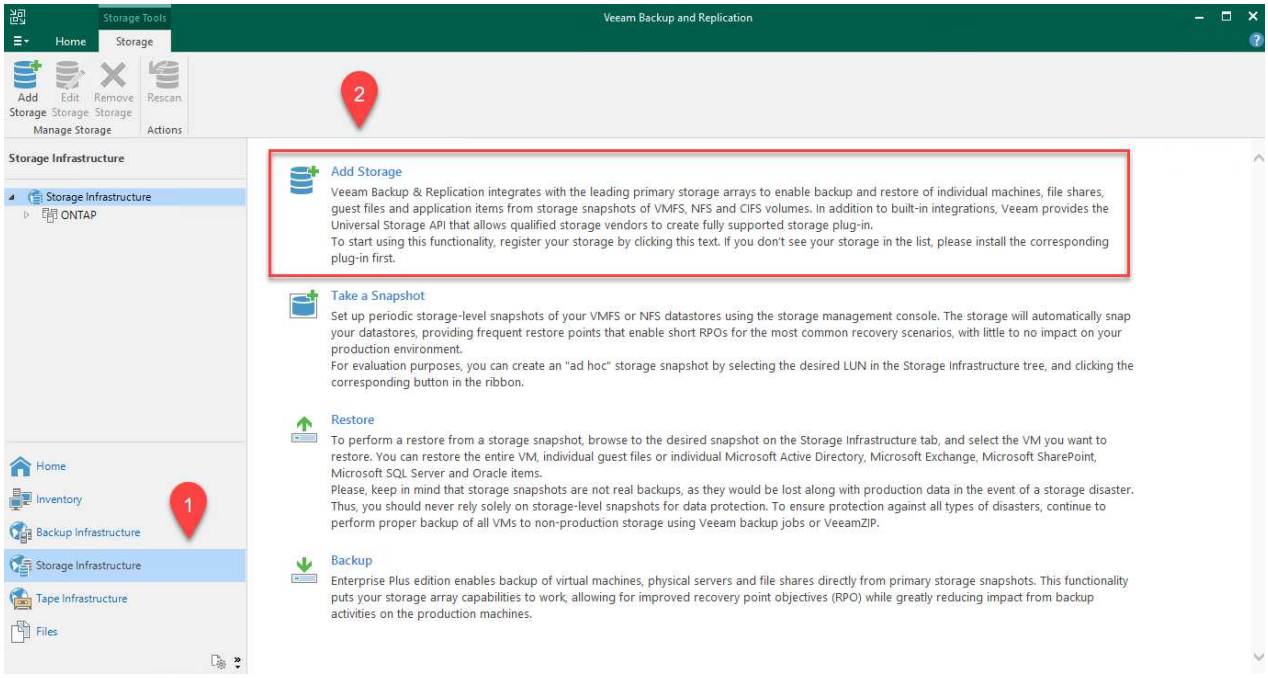
시작하기 전에 다음 전제 조건을 확인하세요.

1. 온프레미스 ONTAP 시스템에 백업 대상 저장소로 SMB 파일 공유를 만듭니다.
2. SOBR에 포함할 Amazon S3 버킷을 만듭니다. 이는 오프사이트 백업을 위한 저장소입니다.

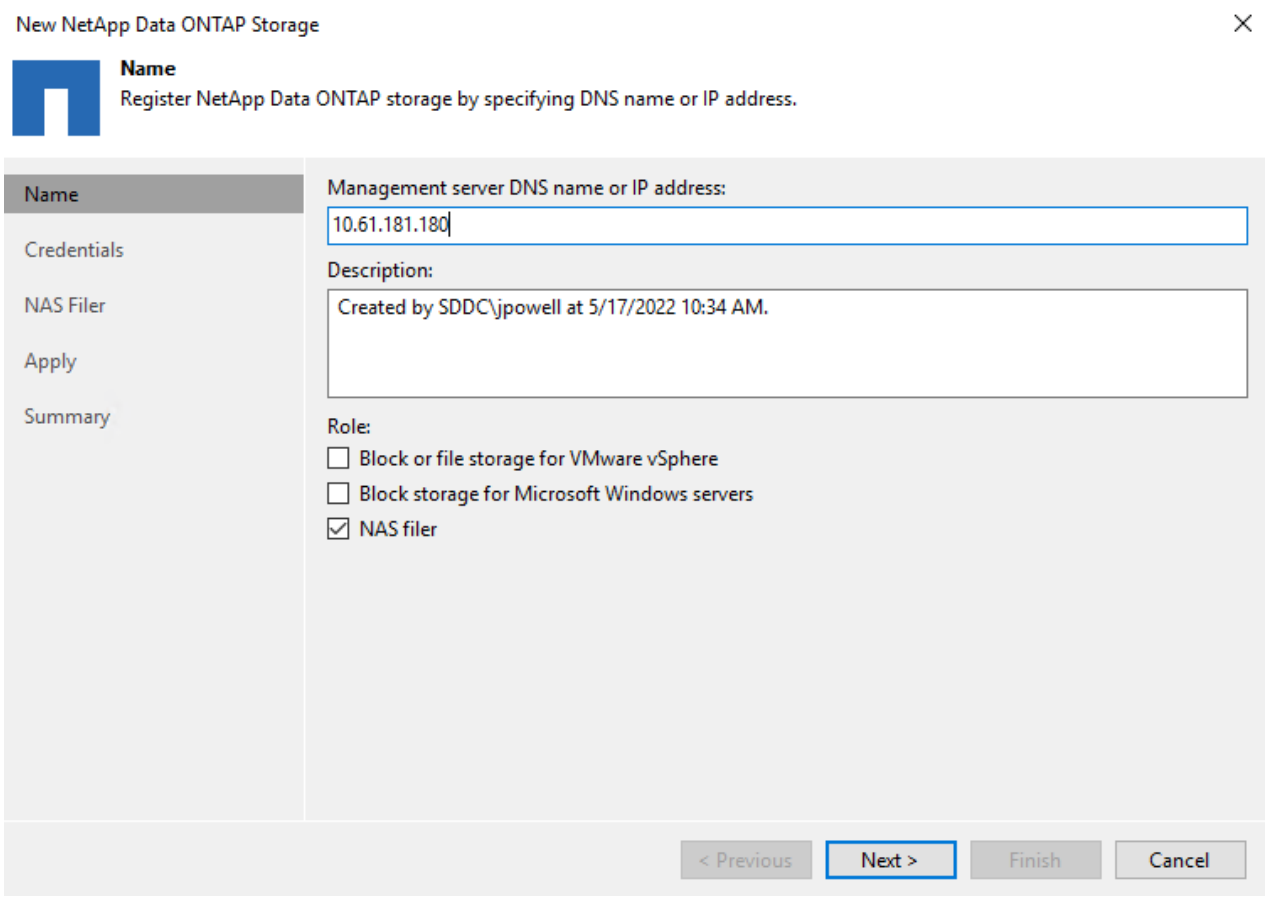
▼ **Veeam**에 **ONTAP** 스토리지 추가

먼저, Veeam에 ONTAP 스토리지 클러스터와 관련 SMB/NFS 파일 시스템을 스토리지 인프라로 추가합니다.

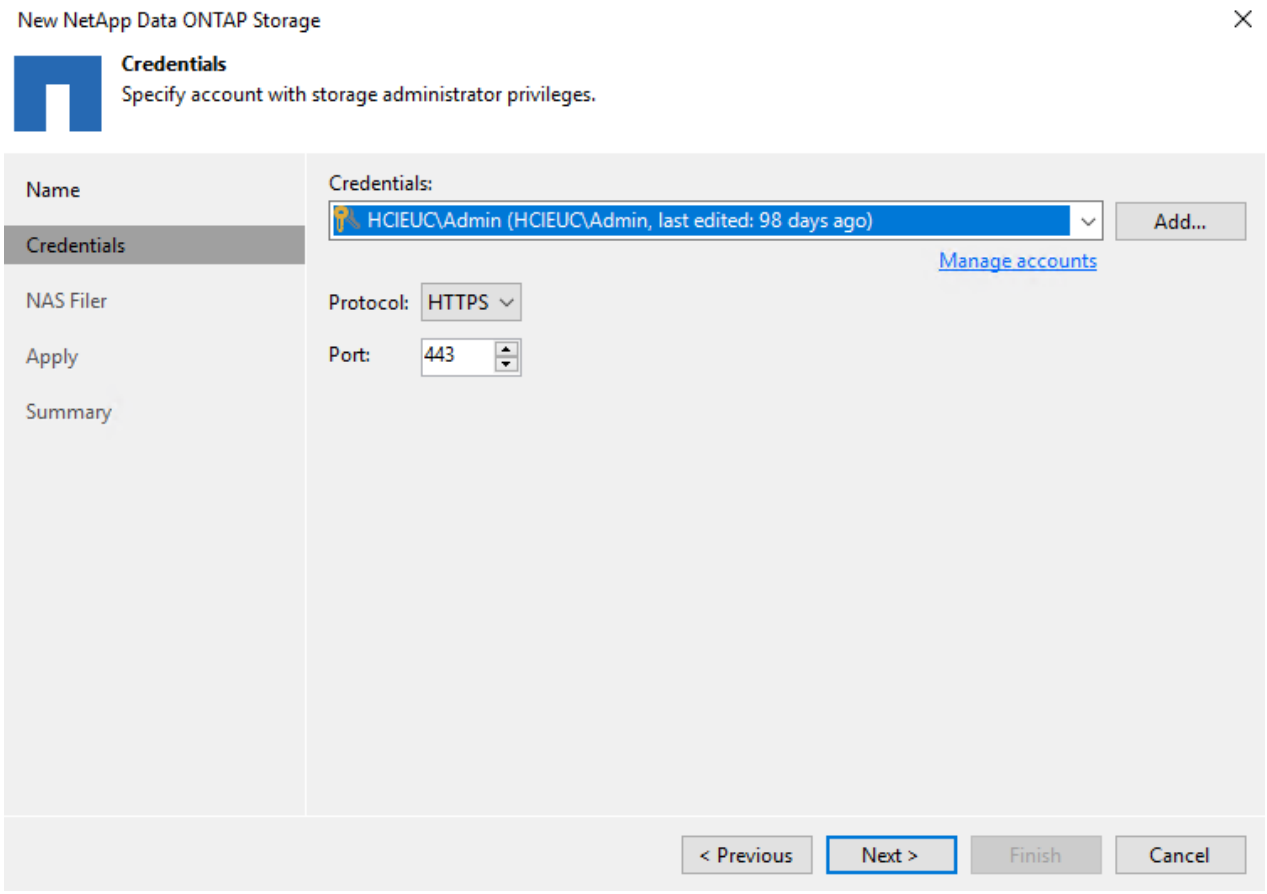
1. Veeam 콘솔을 열고 로그인합니다. 스토리지 인프라로 이동한 다음 스토리지 추가를 선택합니다.



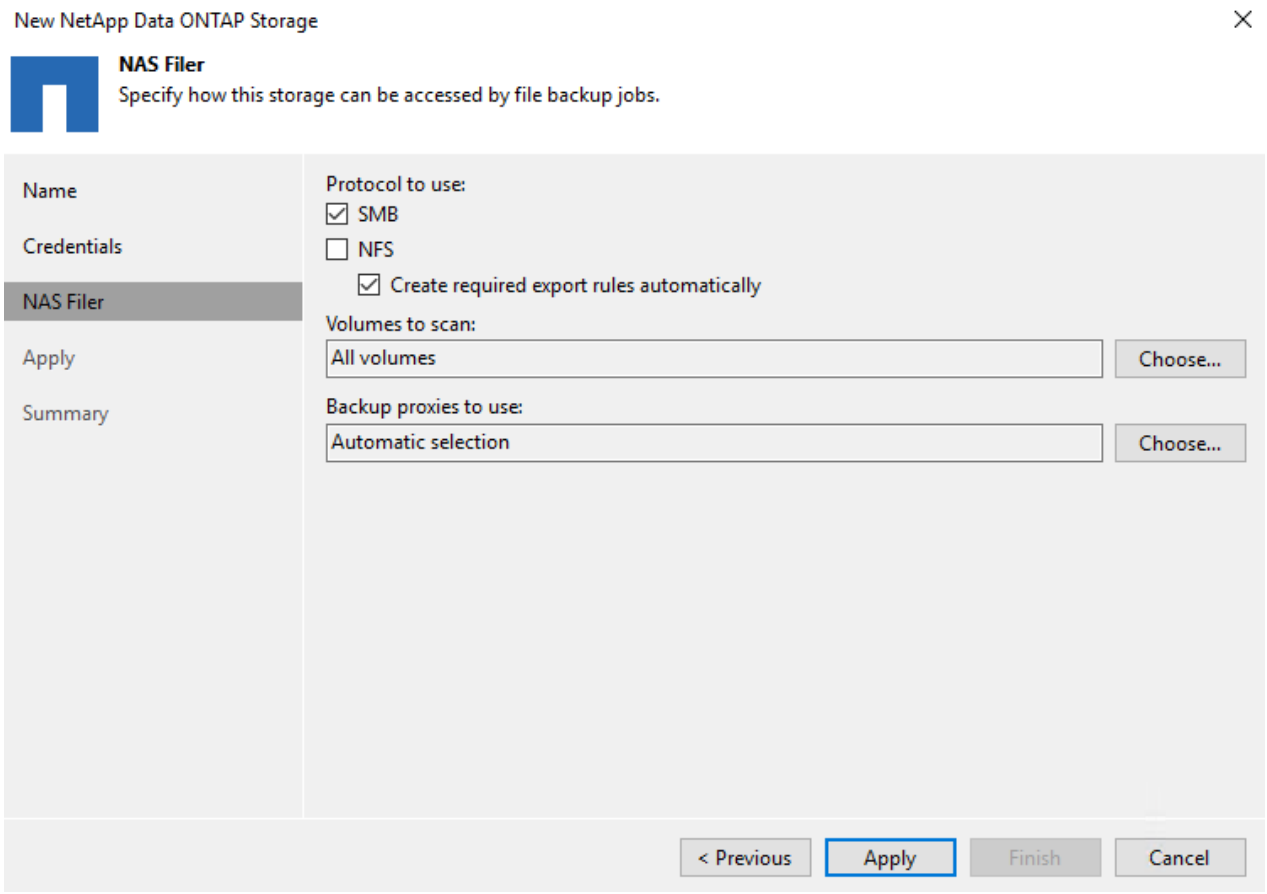
2. 스토리지 추가 마법사에서 스토리지 공급업체로 NetApp 선택한 다음 Data ONTAP 선택합니다.
3. 관리 IP 주소를 입력하고 NAS Filer 상자를 선택하세요. 다음을 클릭하세요.



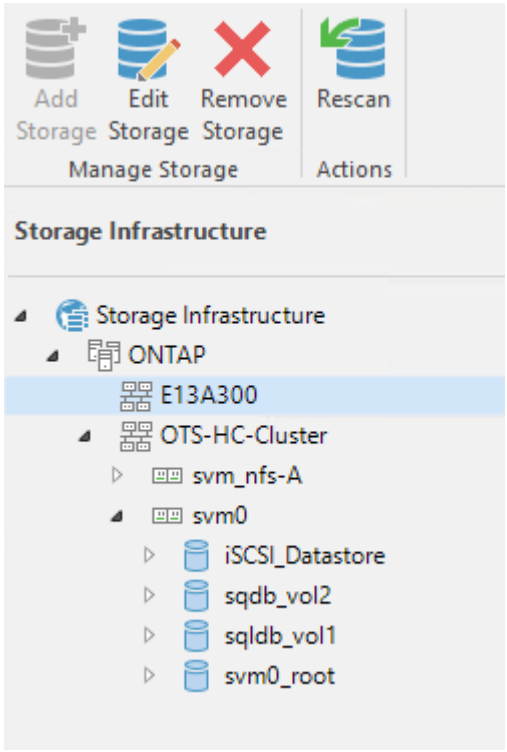
4. ONTAP 클러스터에 액세스하려면 자격 증명을 추가하세요.



5. NAS Filer 페이지에서 스캔할 원하는 프로토콜을 선택하고 다음을 선택합니다.

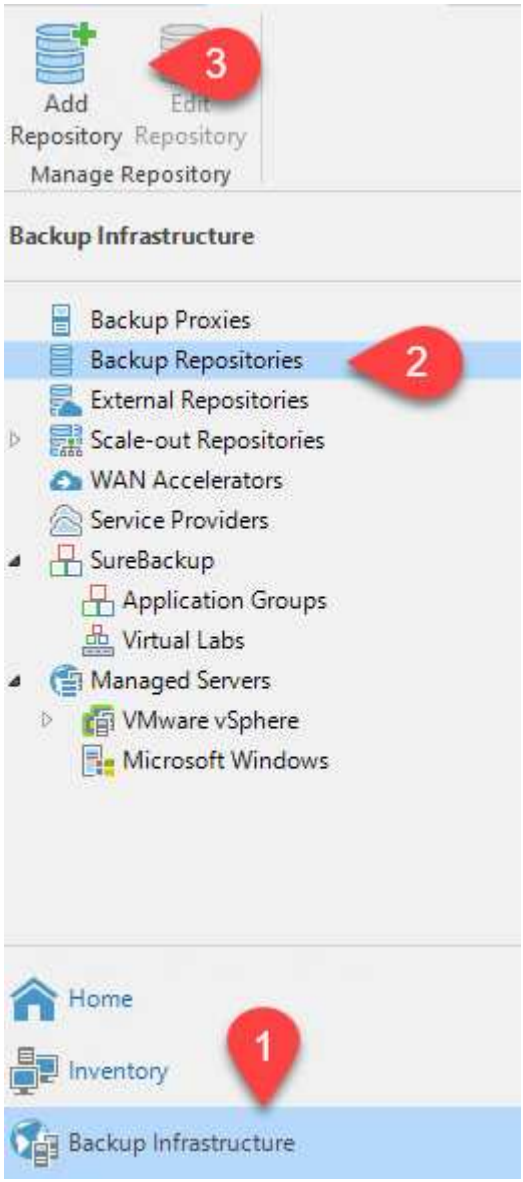


6. 마법사의 적용 및 요약 페이지를 완료하고 마침을 클릭하여 저장소 검색 프로세스를 시작합니다. 검사가 완료되면 ONTAP 클러스터가 NAS 파일러와 함께 사용 가능한 리소스로 추가됩니다.

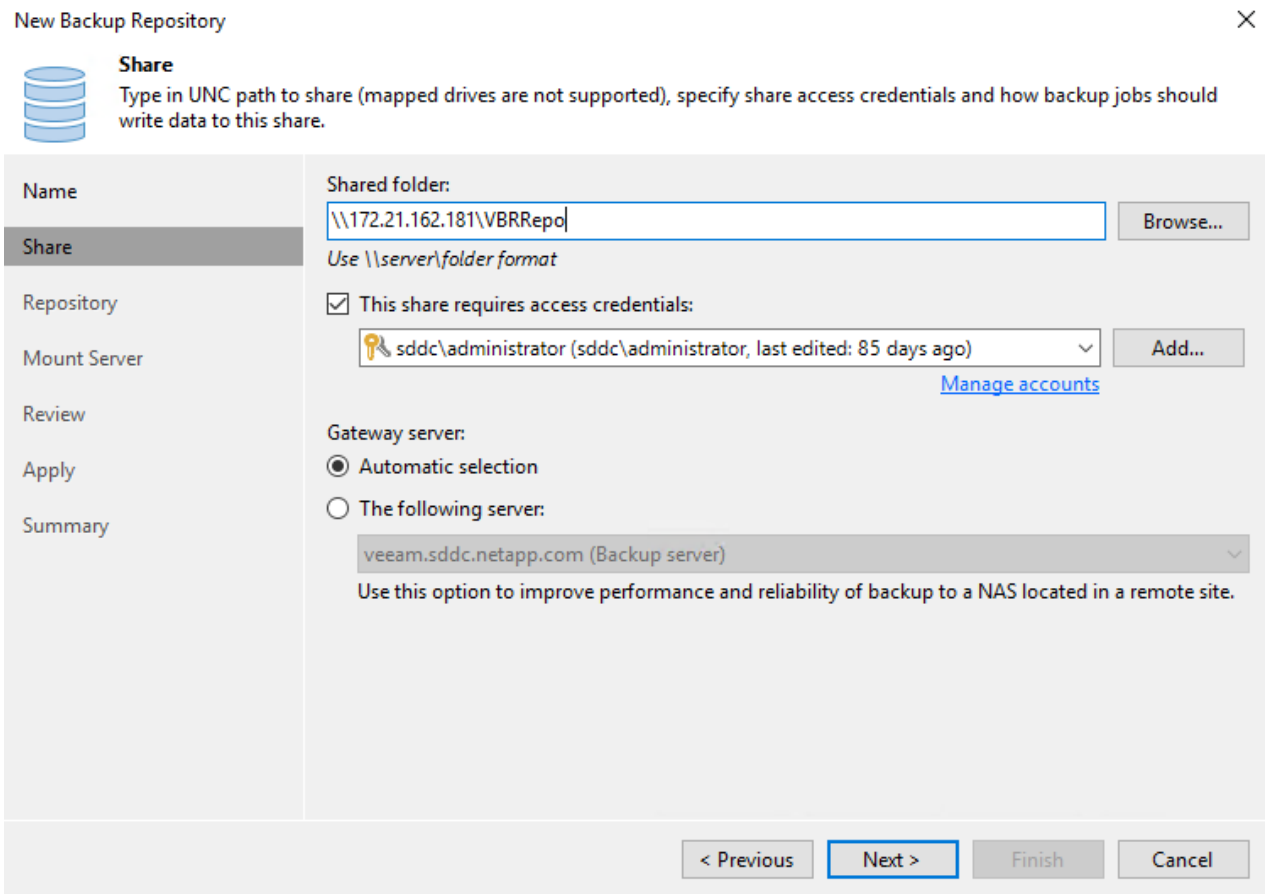


7. 새로 검색된 NAS 공유를 사용하여 백업 저장소를 만듭니다. 백업 인프라에서 백업 저장소를 선택하고 저장소

추가 메뉴 항목을 클릭합니다.



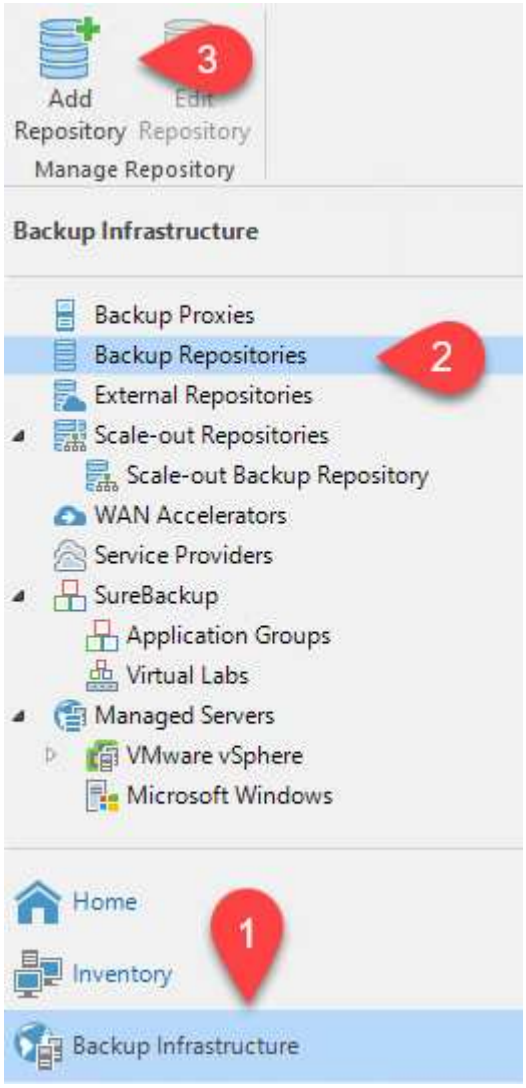
8. 새 백업 저장소 마법사의 모든 단계를 따라 저장소를 만듭니다. Veeam 백업 저장소 생성에 대한 자세한 내용은 다음을 참조하세요. "Veeam 문서" .



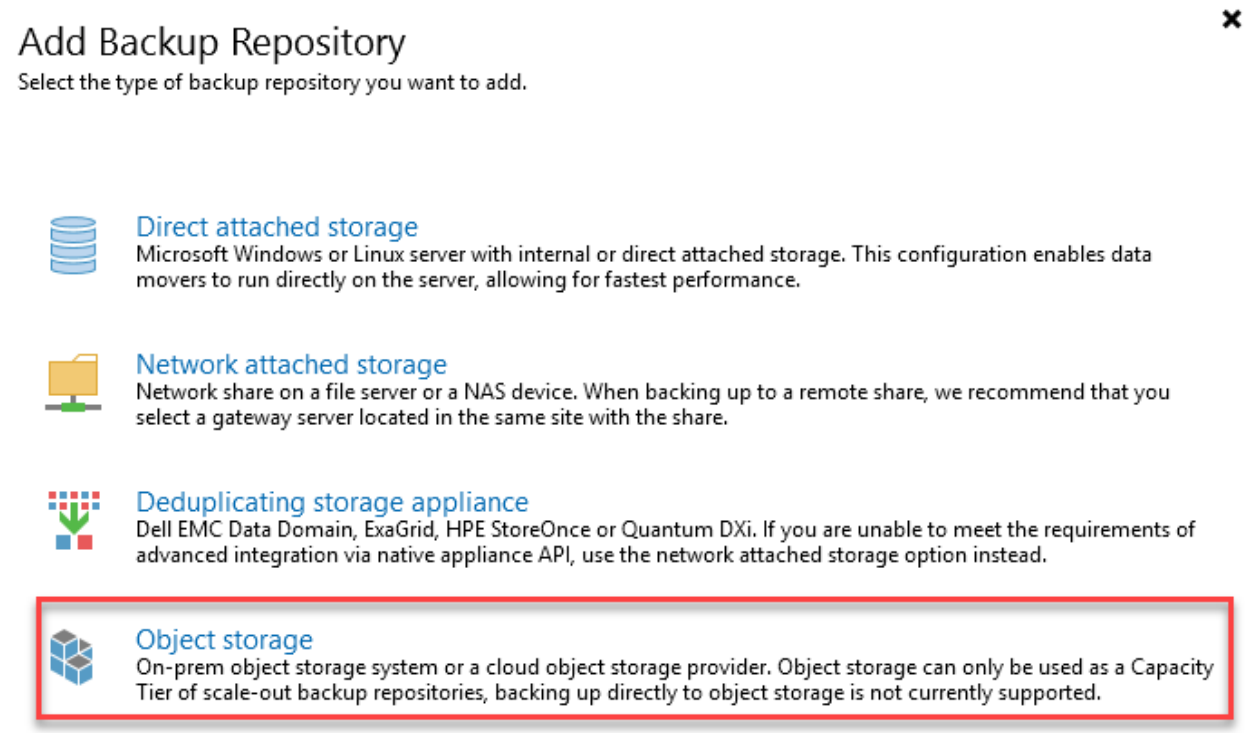
▼ **Amazon S3** 버킷을 백업 저장소로 추가합니다.

다음 단계는 Amazon S3 스토리지를 백업 저장소로 추가하는 것입니다.

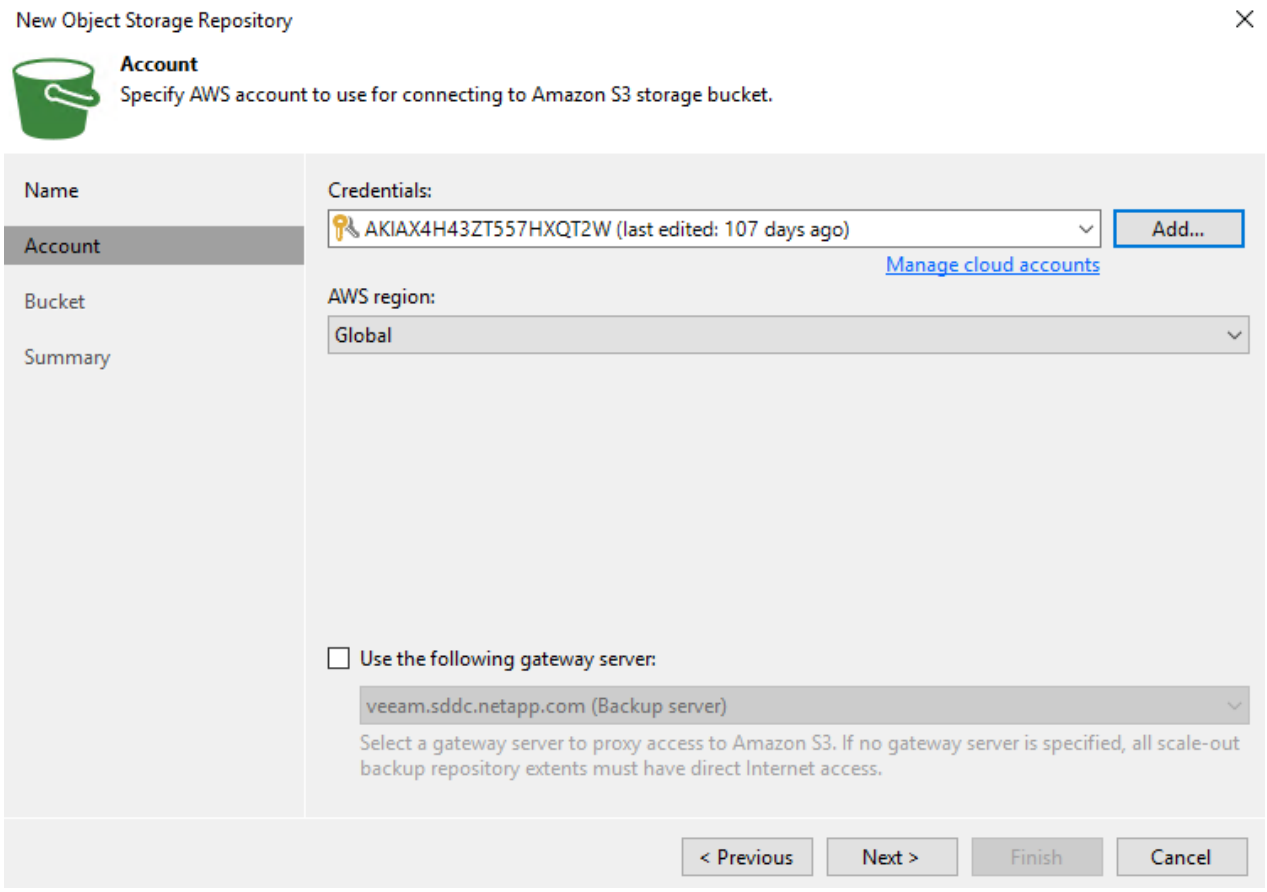
1. 백업 인프라 > 백업 저장소로 이동합니다. 저장소 추가를 클릭합니다.



2. 백업 저장소 추가 마법사에서 개체 스토리지를 선택한 다음 Amazon S3를 선택합니다. 그러면 새 개체 스토리지 리포지토리 마법사가 시작됩니다.



3. 개체 스토리지 저장소의 이름을 입력하고 다음을 클릭합니다.
4. 다음 섹션에서는 신임장을 입력하세요. AWS 액세스 키와 비밀 키가 필요합니다.



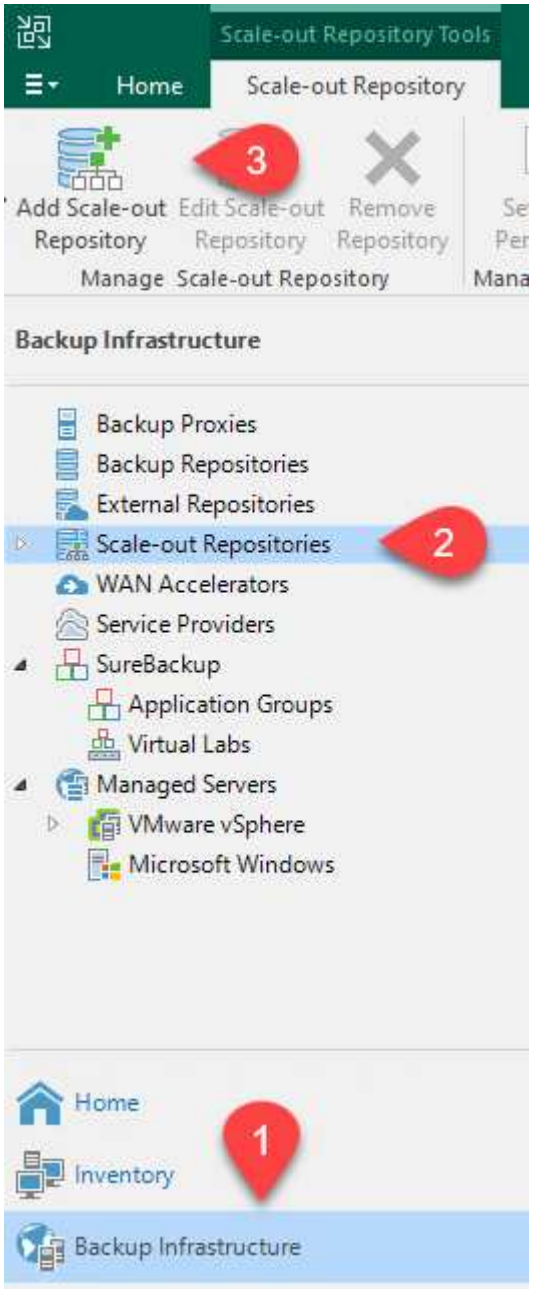
5. Amazon 구성이 로드되면 데이터 센터, 버킷, 폴더를 선택하고 적용을 클릭합니다. 마지막으로 마침을

클릭하여 마법사를 닫습니다.

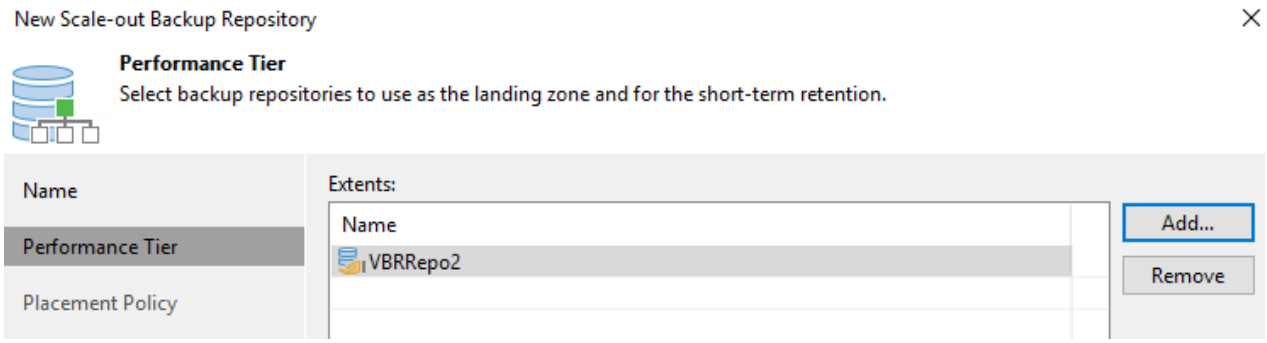
▼ 스케일아웃 백업 저장소 생성

이제 Veeam에 스토리지 저장소를 추가했으므로 재해 복구를 위해 오프사이트 Amazon S3 개체 스토리지에 백업 사본을 자동으로 계층화하는 SOBR을 만들 수 있습니다.

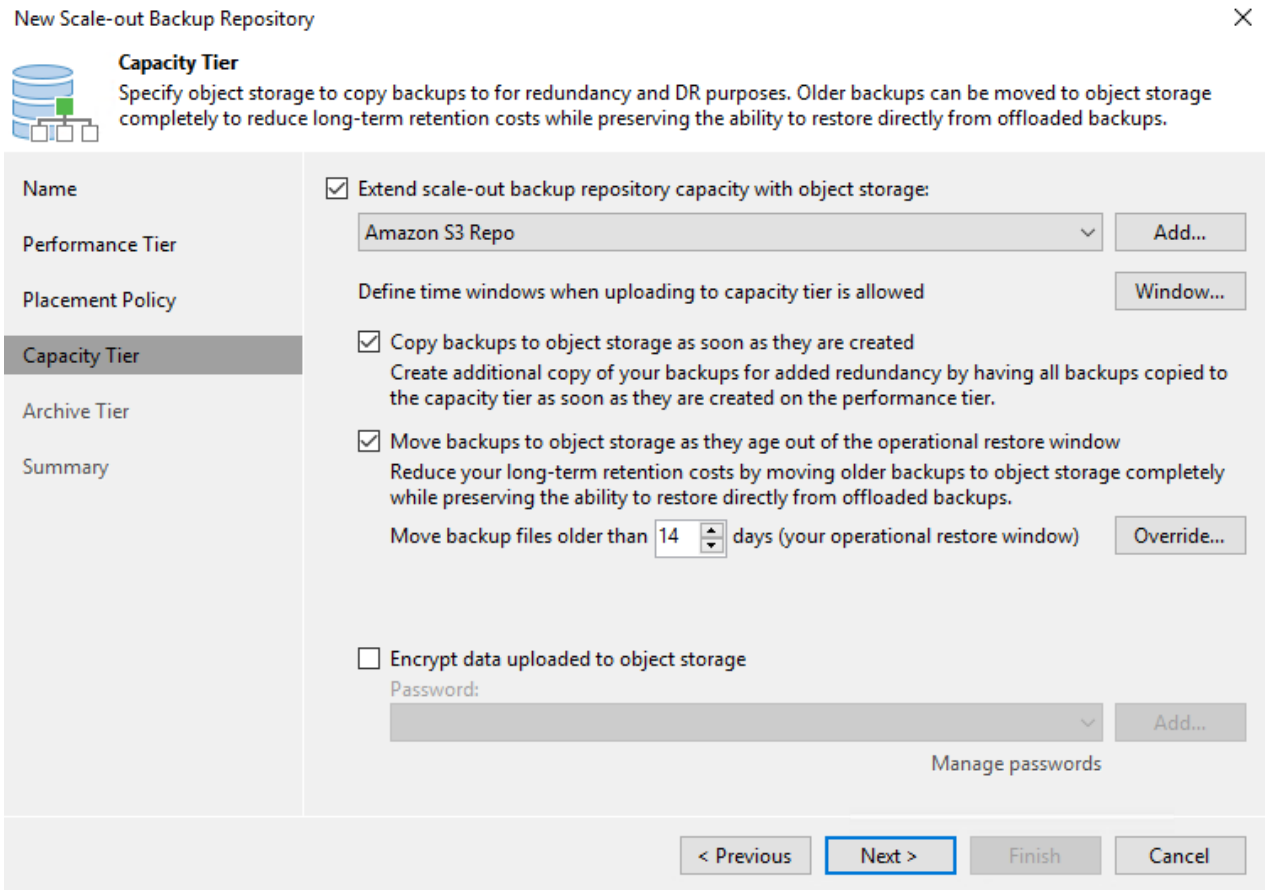
1. 백업 인프라에서 스케일아웃 리포지토리를 선택한 다음 스케일아웃 리포지토리 추가 메뉴 항목을 클릭합니다.



2. 새로운 확장형 백업 저장소에서 SOBR의 이름을 입력하고 다음을 클릭합니다.
3. 성능 계층의 경우 로컬 ONTAP 클러스터에 있는 SMB 공유가 포함된 백업 저장소를 선택합니다.



4. 배치 정책의 경우 요구 사항에 따라 데이터 지역성이나 성능을 선택하세요. 다음을 선택하세요.
5. 용량 계층의 경우 Amazon S3 객체 스토리지로 SOBR을 확장합니다. 재해 복구를 위해 보조 백업을 적시에 전달하려면 백업이 생성되는 즉시 개체 스토리지에 복사를 선택하세요.



6. 마지막으로 '적용' 및 '마침'을 선택하여 SOBR 생성을 완료합니다.

▼ 스케일아웃 백업 저장소 작업 생성

Veeam을 구성하는 마지막 단계는 새로 만든 SOBR을 백업 대상으로 사용하여 백업 작업을 만드는 것입니다. 백업 작업을 만드는 것은 모든 스토리지 관리자의 일반적인 업무이므로 여기서는 자세한 단계를 다루지 않습니다. Veeam에서 백업 작업을 만드는 방법에 대한 자세한 내용은 다음을 참조하세요. "Veeam 도움말 센터 기술 문서" .

NetApp Backup and Recovery 툴 및 구성

AWS에서 실행되는 VMware Cloud Volume 서비스로 애플리케이션 VM 및 데이터베이스 볼륨의 장애 조치를 수행하려면 SnapCenter Server와 Veeam Backup and Replication Server의 실행 인스턴스를 설치하고 구성해야

합니다. 장애 조치가 완료된 후에는 온프레미스 데이터 센터로의 장애 복구를 계획하고 실행할 때까지 정상적인 백업 작업을 재개하도록 이러한 도구를 구성해야 합니다.

▼ 보조 **Windows SnapCenter** 서버 배포

SnapCenter 서버는 VMware Cloud SDDC에 배포되거나 VMware Cloud 환경에 네트워크로 연결된 VPC에 있는 EC2 인스턴스에 설치됩니다.

SnapCenter software NetApp 지원 사이트에서 구할 수 있으며 도메인이나 작업 그룹에 있는 Microsoft Windows 시스템에 설치할 수 있습니다. 자세한 계획 가이드와 설치 지침은 다음에서 확인할 수 있습니다. "NetApp 문서 센터" .

SnapCenter software 다음에서 찾을 수 있습니다. "이 링크" .

▼ 보조 **Windows SnapCenter** 서버 구성

FSx ONTAP 에 미러링된 애플리케이션 데이터를 복원하려면 먼저 온프레미스 SnapCenter 데이터베이스를 전체 복원해야 합니다. 이 프로세스가 완료되면 VM과의 통신이 재설정되고 이제 FSx ONTAP 기본 스토리지로 사용하여 애플리케이션 백업을 재개할 수 있습니다.

이를 달성하려면 SnapCenter 서버에서 다음 항목을 완료해야 합니다.

1. 컴퓨터 이름을 원래 온프레미스 SnapCenter 서버와 동일하게 구성합니다.
2. VMware Cloud 및 FSx ONTAP 인스턴스와 통신하도록 네트워킹을 구성합니다.
3. SnapCenter 데이터베이스를 복원하는 절차를 완료하세요.
4. SnapCenter 재해 복구 모드에 있는지 확인하여 FSx가 이제 백업을 위한 기본 저장소인지 확인하세요.
5. 복구된 가상 머신과 통신이 다시 설정되었는지 확인합니다.

▼ 보조 **Veeam** 백업 및 복제 서버 배포

AWS의 VMware Cloud에 있는 Windows 서버나 EC2 인스턴스에 Veeam Backup & Replication 서버를 설치할 수 있습니다. 자세한 구현 지침은 다음을 참조하세요. "Veeam 도움말 센터 기술 문서" .

▼ 보조 **Veeam** 백업 및 복제 서버 구성

Amazon S3 스토리지에 백업된 가상 머신을 복원하려면 Windows 서버에 Veeam Server를 설치하고 VMware Cloud, FSx ONTAP 및 원본 백업 저장소가 포함된 S3 버킷과 통신하도록 구성해야 합니다. VM이 복원된 후 새로운 백업을 수행하려면 FSx ONTAP 에 새로운 백업 저장소를 구성해야 합니다.

이 프로세스를 수행하려면 다음 항목을 완료해야 합니다.

1. VMware Cloud, FSx ONTAP 및 원본 백업 저장소가 포함된 S3 버킷과 통신하도록 네트워킹을 구성합니다.
2. FSx ONTAP 에서 SMB 공유를 새로운 백업 저장소로 구성합니다.
3. 온프레미스에서 확장형 백업 저장소의 일부로 사용된 원래 S3 버킷을 마운트합니다.
4. VM을 복원한 후 SQL 및 Oracle VM을 보호하기 위해 새로운 백업 작업을 설정합니다.

Veeam을 사용하여 VM을 복원하는 방법에 대한 자세한 내용은 섹션을 참조하세요."Veeam Full Restore를 사용하여 애플리케이션 VM 복원" .

재해 복구를 위한 **SnapCenter** 데이터베이스 백업

SnapCenter 사용하면 재해 발생 시 SnapCenter 서버를 복구할 목적으로 기본 MySQL 데이터베이스와 구성 데이터를 백업하고 복구할 수 있습니다. 우리 솔루션의 경우, VPC에 있는 AWS EC2 인스턴스에서 SnapCenter 데이터베이스와 구성을 복구했습니다. SnapCenter 의 재해 복구에 대한 자세한 내용은 다음을 참조하세요. "이 링크" .

▼ **SnapCenter** 백업 필수 구성 요소

SnapCenter 백업에는 다음과 같은 필수 구성 요소가 필요합니다.

- 백업된 데이터베이스와 구성 파일을 찾기 위해 온프레미스 ONTAP 시스템에 볼륨과 SMB 공유를 생성했습니다.
- 온프레미스 ONTAP 시스템과 AWS 계정의 FSx 또는 CVO 간의 SnapMirror 관계입니다. 이 관계는 백업된 SnapCenter 데이터베이스와 구성 파일이 포함된 스냅샷을 전송하는 데 사용됩니다.
- EC2 인스턴스나 VMware Cloud SDDC의 VM에 있는 클라우드 계정에 Windows Server가 설치되어 있습니다.
- VMware Cloud의 Windows EC2 인스턴스 또는 VM에 SnapCenter 설치되었습니다.

▼ **SnapCenter** 백업 및 복원 프로세스 요약

- 백업 DB 및 구성 파일을 호스팅하기 위해 온프레미스 ONTAP 시스템에 볼륨을 생성합니다.
- 온프레미스와 FSx/CVO 간에 SnapMirror 관계를 설정합니다.
- SMB 공유를 마운트합니다.
- API 작업을 수행하기 위한 Swagger 인증 토큰을 검색합니다.
- DB 복원 프로세스를 시작합니다.
- xcopy 유틸리티를 사용하여 db 및 config 파일 로컬 디렉토리를 SMB 공유로 복사합니다.
- FSx에서 ONTAP 볼륨의 복제본을 만듭니다(온프레미스에서 SnapMirror 통해 복사).
- FSx에서 EC2/VMware Cloud로 SMB 공유를 마운트합니다.
- SMB 공유에서 복원 디렉토리를 로컬 디렉토리로 복사합니다.
- Swagger에서 SQL Server 복원 프로세스를 실행합니다.

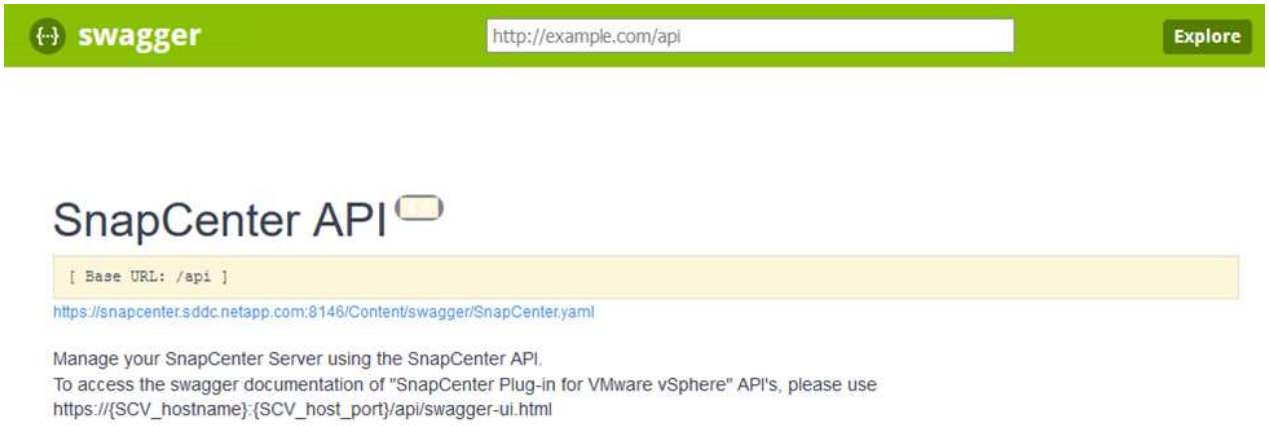
▼ **SnapCenter** 데이터베이스 및 구성 백업

SnapCenter REST API 명령을 실행하기 위한 웹 클라이언트 인터페이스를 제공합니다. Swagger를 통해 REST API에 액세스하는 방법에 대한 정보는 SnapCenter 설명서를 참조하세요. "이 링크" .

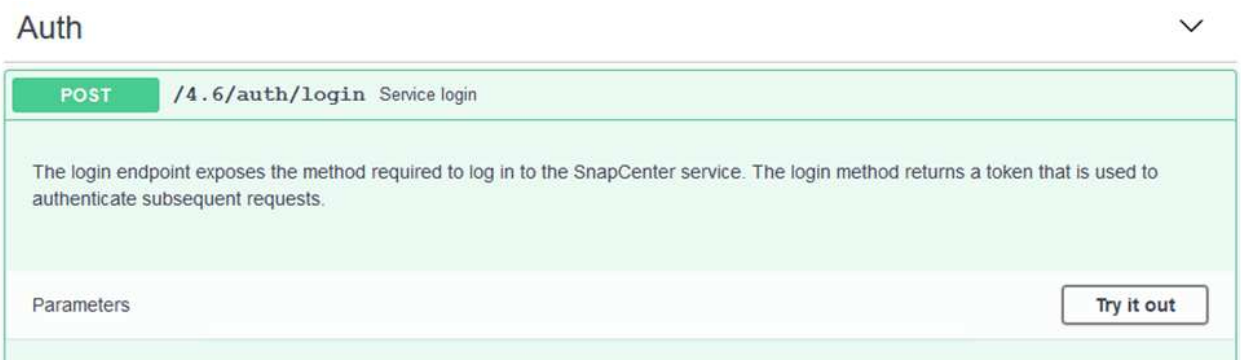
▼ **Swagger**에 로그인하여 승인 토큰을 받으세요

Swagger 페이지로 이동한 후에는 데이터베이스 복원 프로세스를 시작하기 위해 권한 부여 토큰을 검색해야 합니다.

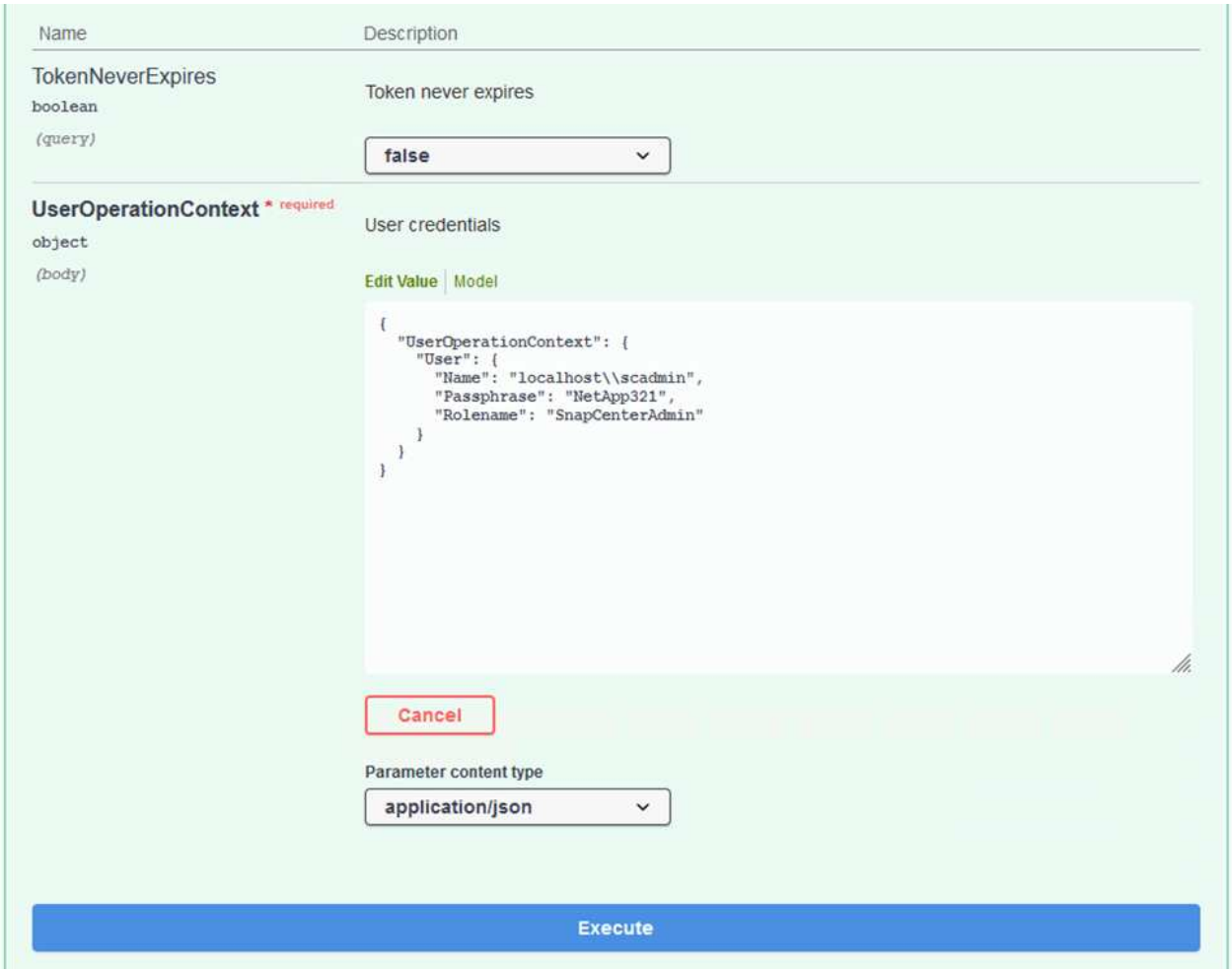
1. _\https://< SnapCenter 서버 IP>:8146/swagger/_에서 SnapCenter Swagger API 웹 페이지에 접속하세요.



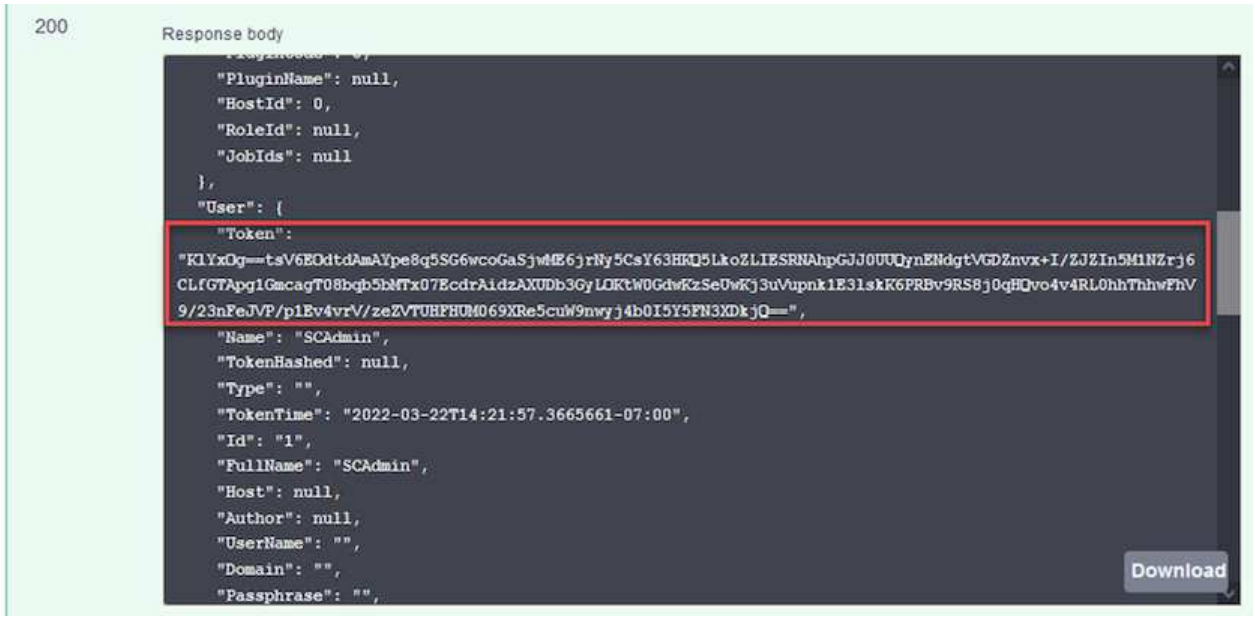
2. 인증 섹션을 확장하고 사용해보기를 클릭하세요.



3. UserOperationContext 영역에서 SnapCenter 자격 증명과 역할을 입력하고 실행을 클릭합니다.



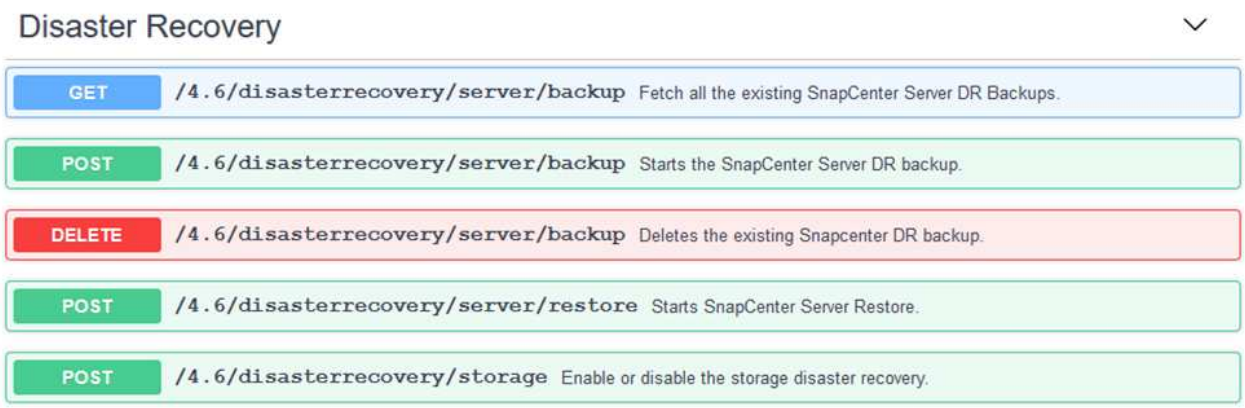
4. 아래의 응답 본문에서 토큰을 확인할 수 있습니다. 백업 프로세스를 실행할 때 인증을 위해 토큰 텍스트를 복사합니다.



▼ **SnapCenter** 데이터베이스 백업 수행

다음으로 Swagger 페이지의 재해 복구 영역으로 이동하여 SnapCenter 백업 프로세스를 시작합니다.

1. 재해 복구 영역을 클릭하여 확장합니다.

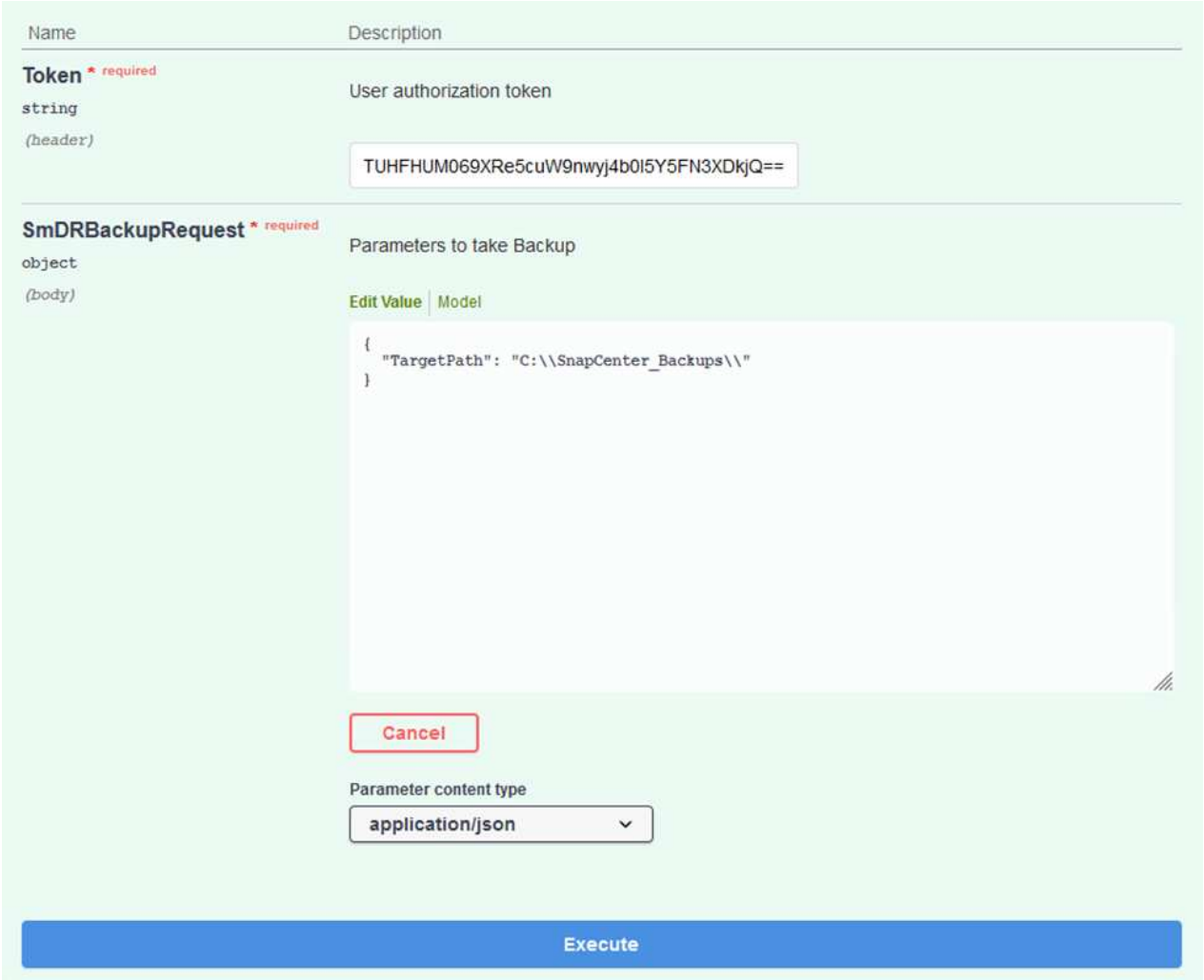


2. 확장하다 `/4.6/disasterrecovery/server/backup` 섹션으로 가서 '시도해보기'를 클릭하세요.



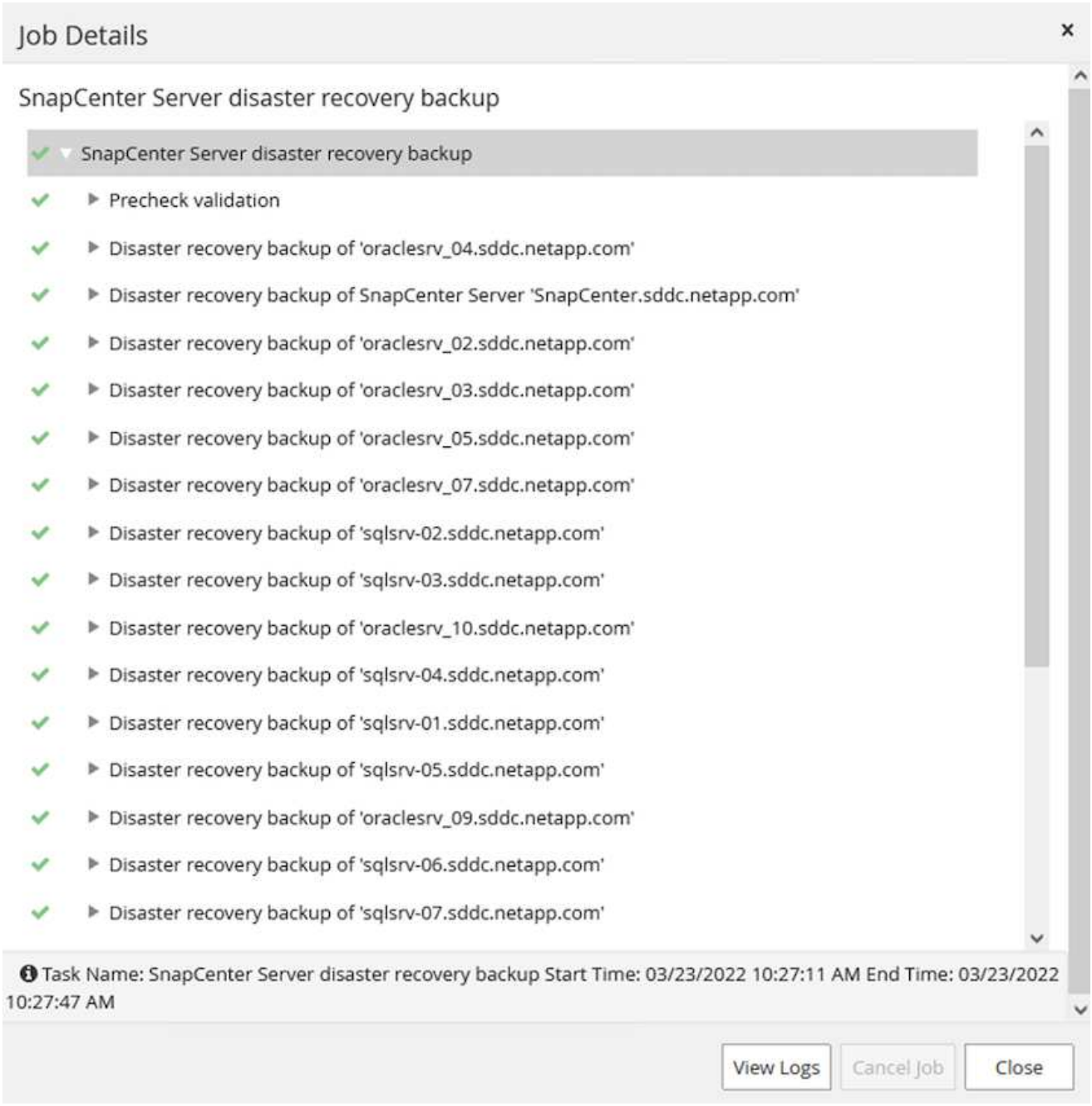
3. SmDRBackupRequest 섹션에서 올바른 로컬 대상 경로를 추가하고 실행을 선택하여 SnapCenter 데이터베이스 및 구성의 백업을 시작합니다.

ⓘ 백업 프로세스에서는 NFS 또는 CIFS 파일 공유에 직접 백업할 수 없습니다.



▼ **SnapCenter** 에서 백업 작업 모니터링

데이터베이스 복구 프로세스를 시작할 때 SnapCenter 에 로그인하여 로그 파일을 검토하세요. 모니터 섹션에서 SnapCenter 서버 재해 복구 백업의 세부 정보를 볼 수 있습니다.



▼ **XCOPY** 유틸리티를 사용하여 데이터베이스 백업 파일을 **SMB** 공유로 복사합니다**.**

다음으로 SnapCenter 서버의 로컬 드라이브에서 CIFS 공유로 백업을 옮겨야 합니다. 이 공유는 SnapMirror 사용하여 AWS의 FSx 인스턴스에 있는 보조 위치로 데이터를 복사하는 데 사용됩니다. 특정 옵션과 함께 xcopy를 사용하여 파일의 권한을 유지합니다.

관리자 권한으로 명령 프롬프트를 엽니다. 명령 프롬프트에서 다음 명령을 입력합니다.

```
xcopy  <Source_Path>  \\<Destination_Server_IP>\<Folder_Path> /O /X /E
/H /K
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O /X
/E /H /K
```

장애 조치

▼ 재해는 **1**차 현장에서 발생합니다**.**

온프레미스 기본 데이터 센터에서 재해가 발생하는 경우, 당사 시나리오에는 AWS의 VMware Cloud를 사용하여 Amazon Web Services 인프라에 있는 보조 사이트로 장애 조치를 취하는 것이 포함됩니다. 가상 머신과 온프레미스 ONTAP 클러스터에 더 이상 액세스할 수 없다고 가정합니다. 또한 SnapCenter 와 Veeam 가상 머신에 더 이상 액세스할 수 없으므로 보조 사이트에서 다시 구축해야 합니다.

이 섹션에서는 인프라를 클라우드로 장애 조치하는 방법을 다루며, 다음과 같은 주제를 다룹니다.

- SnapCenter 데이터베이스를 복구합니다. 새로운 SnapCenter 서버가 구축된 후 MySQL 데이터베이스와 구성 파일을 복원하고 데이터베이스를 재해 복구 모드로 전환하여 보조 FSx 스토리지가 기본 스토리지 장치가 되도록 합니다.
- Veeam Backup & Replication을 사용하여 애플리케이션 가상 머신을 복원합니다. VM 백업이 포함된 S3 스토리지를 연결하고 백업을 가져온 다음 AWS의 VMware Cloud에 복원합니다.
- SnapCenter 사용하여 SQL Server 애플리케이션 데이터를 복원합니다.
- SnapCenter 사용하여 Oracle 애플리케이션 데이터를 복원합니다.

▼ **SnapCenter** 데이터베이스 복원 프로세스

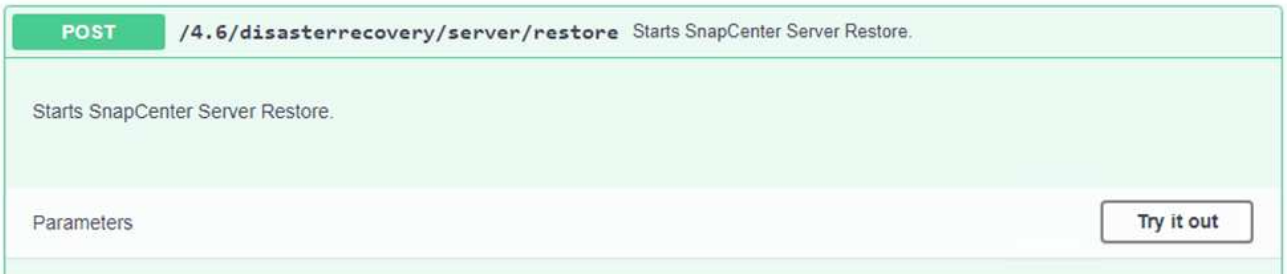
SnapCenter MySQL 데이터베이스와 구성 파일의 백업 및 복원을 허용하여 재해 복구 시나리오를 지원합니다. 이를 통해 관리자는 온프레미스 데이터 센터에서 SnapCenter 데이터베이스를 정기적으로 백업하고 나중에 해당 데이터베이스를 보조 SnapCenter 데이터베이스로 복원할 수 있습니다.

원격 SnapCenter 서버에서 SnapCenter 백업 파일에 액세스하려면 다음 단계를 완료하세요.

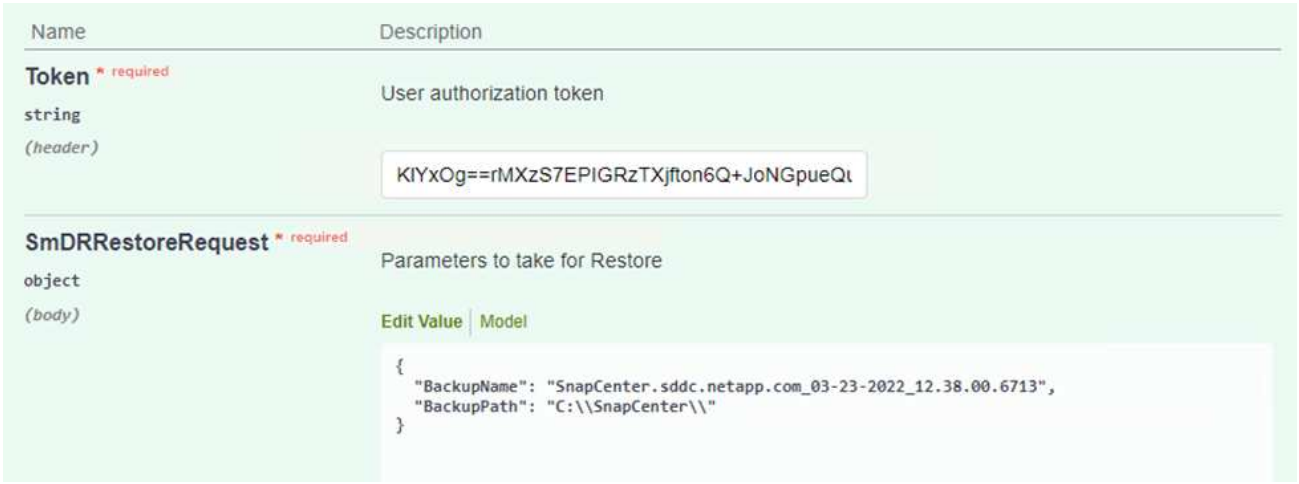
1. FSx 클러스터에서 SnapMirror 관계를 끊어 볼륨을 읽기/쓰기로 설정합니다.
2. 필요한 경우 CIFS 서버를 생성하고 복제된 볼륨의 연결 경로를 가리키는 CIFS 공유를 생성합니다.
3. xcopy를 사용하여 백업 파일을 보조 SnapCenter 시스템의 로컬 디렉토리에 복사합니다.
4. SnapCenter v4.6을 설치하세요.
5. SnapCenter 서버의 FQDN이 원본 서버와 동일한지 확인하세요. 이는 DB 복원이 성공하는 데 필요합니다.

복원 프로세스를 시작하려면 다음 단계를 완료하세요.

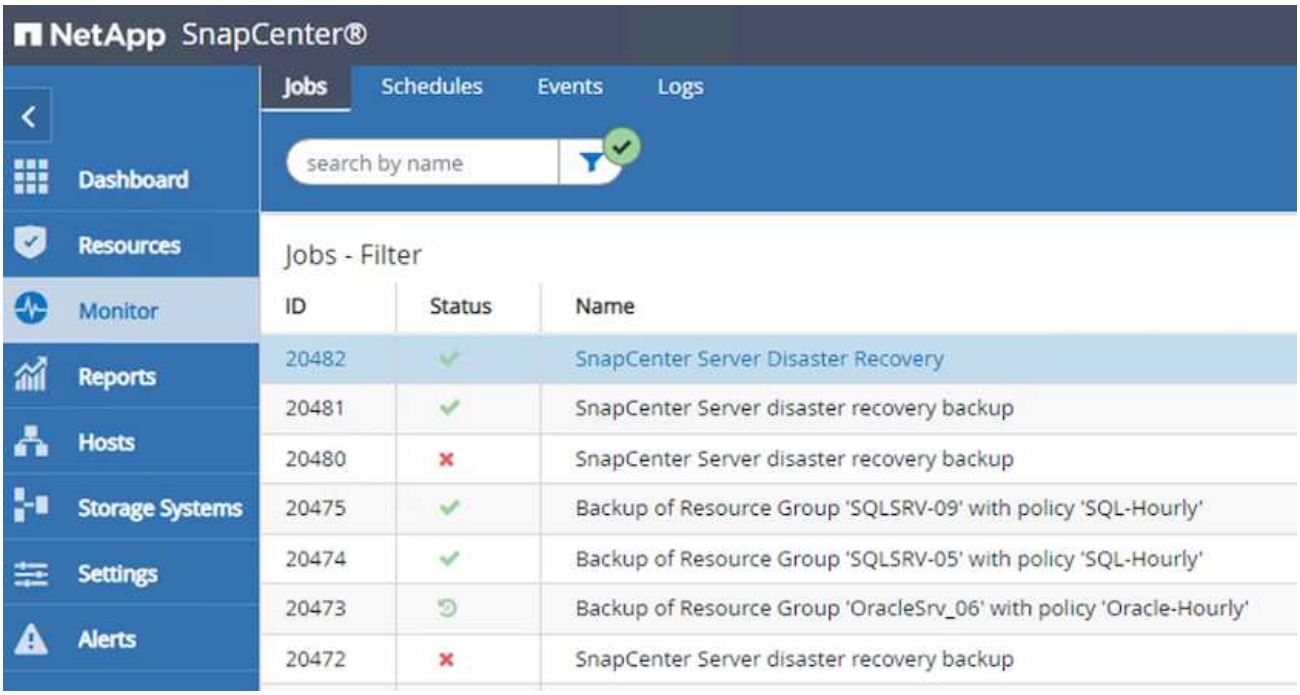
1. 보조 SnapCenter 서버의 Swagger API 웹 페이지로 이동하여 이전 지침에 따라 승인 토큰을 얻습니다.
2. Swagger 페이지의 재해 복구 섹션으로 이동하여 다음을 선택합니다. `/4.6/disasterrecovery/server/restore` 를 클릭하고 '시도해보기'를 클릭하세요.

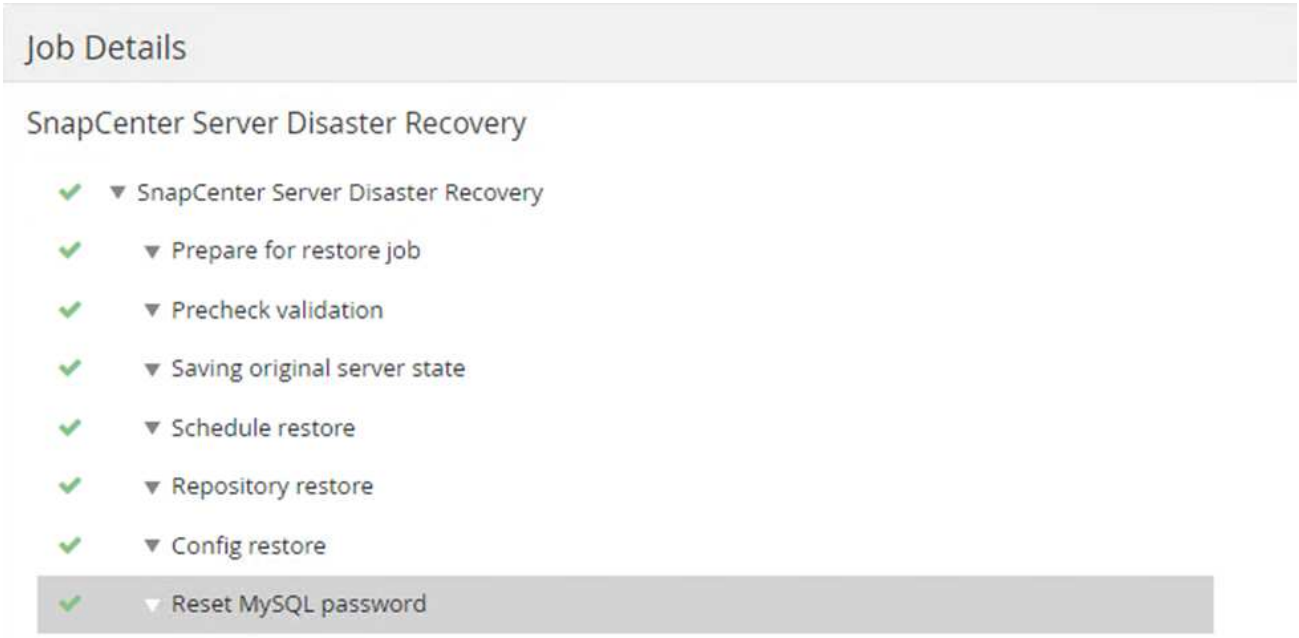


3. 권한 토큰을 붙여넣고, SmDRResterRequest 섹션에 백업 이름과 보조 SnapCenter 서버의 로컬 디렉토리 이름을 붙여넣습니다.



4. 복원 프로세스를 시작하려면 실행 버튼을 선택하세요.
5. SnapCenter 에서 모니터 섹션으로 이동하여 복원 작업의 진행 상황을 확인합니다.





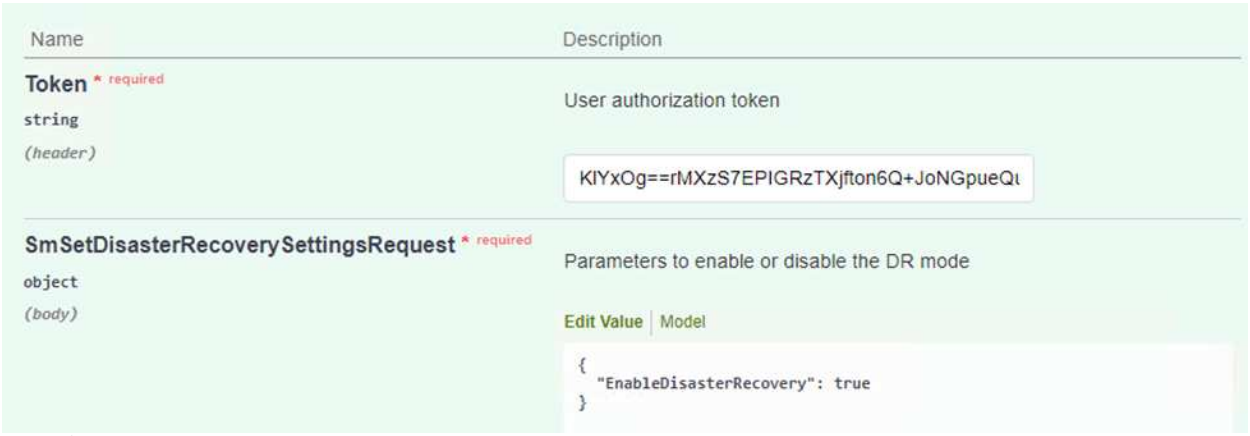
6. 보조 저장소에서 SQL Server 복원을 활성화하려면 SnapCenter 데이터베이스를 재해 복구 모드로 전환해야 합니다. 이 작업은 별도의 작업으로 수행되며 Swagger API 웹 페이지에서 시작됩니다.

   a. 재해 복구 섹션으로 이동하여 클릭하십시오. `/4.6/disasterrecovery/storage` .

   b. 사용자 인증 토큰을 붙여넣습니다.

   c. SmSetDisasterRecoverySettingsRequest 섹션에서 변경하세요. `EnableDisasterRecover` 에게 `true` .

   d. SQL Server에 대한 재해 복구 모드를 활성화하려면 실행을 클릭합니다.



추가 절차에 대한 의견을 참조하세요.

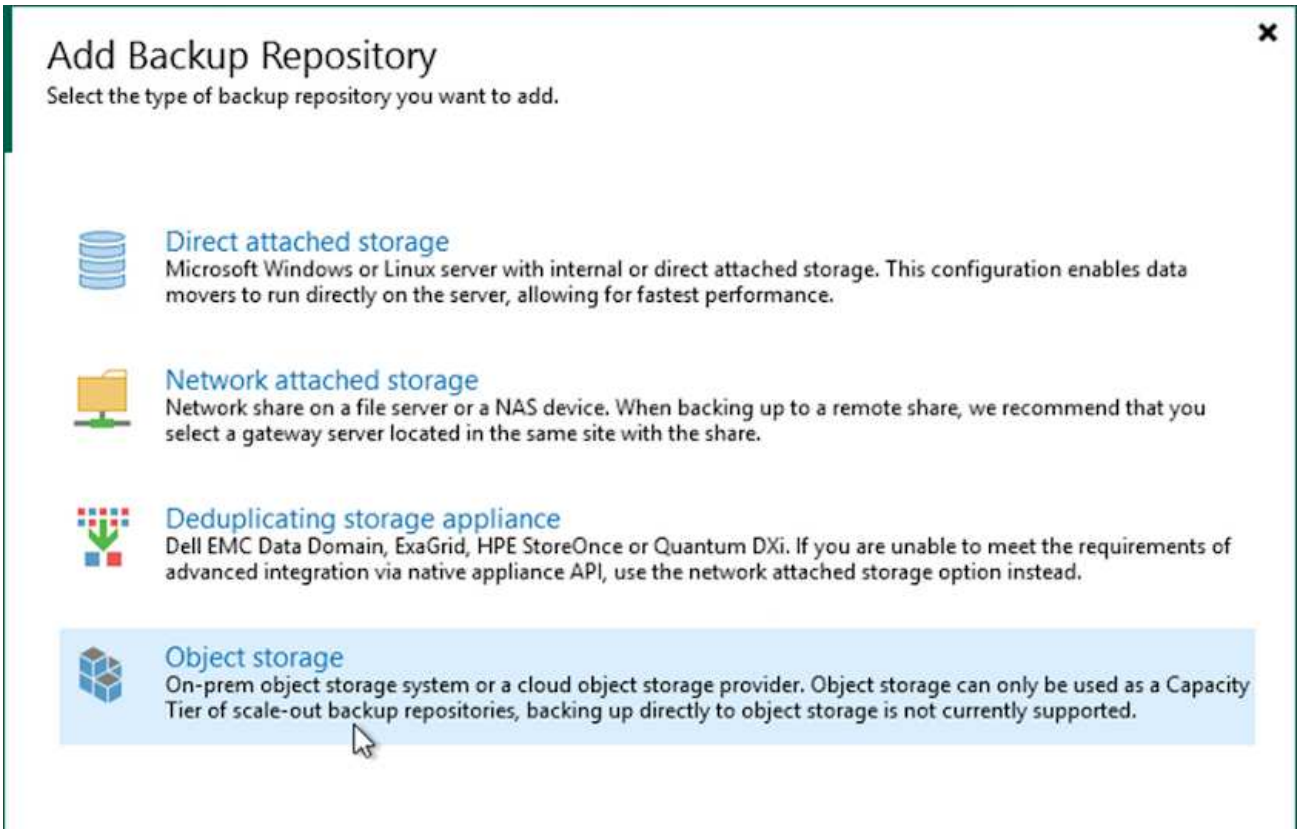
Veeam 전체 복원을 사용하여 애플리케이션 **VM** 복원

▼ 백업 저장소를 만들고 **S3**에서 백업을 가져옵니다**.**

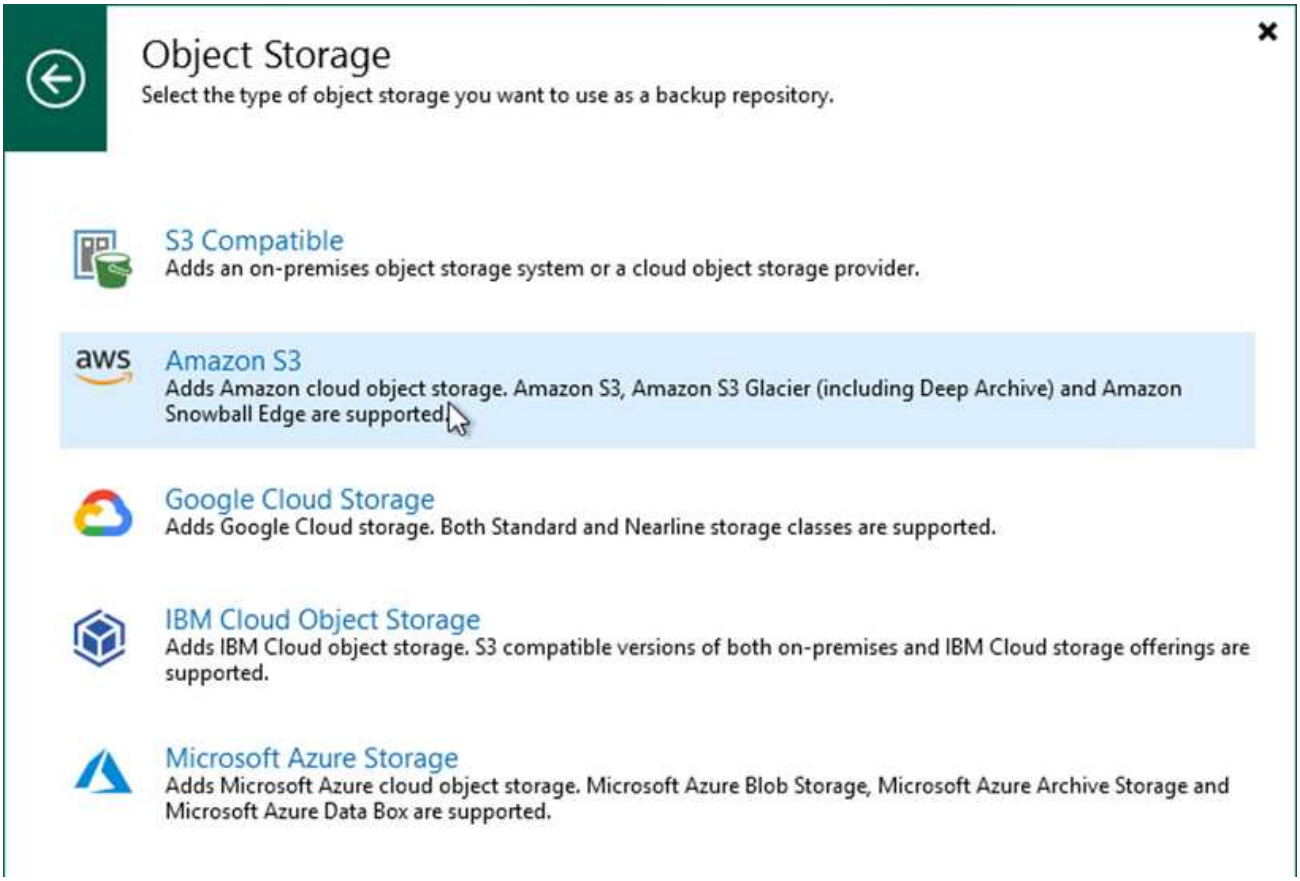
보조 Veeam 서버에서 S3 스토리지의 백업을 가져와 SQL Server 및 Oracle VM을 VMware Cloud 클러스터로 복원합니다.

온프레미스 확장형 백업 저장소에 속한 S3 개체에서 백업을 가져오려면 다음 단계를 완료하세요.

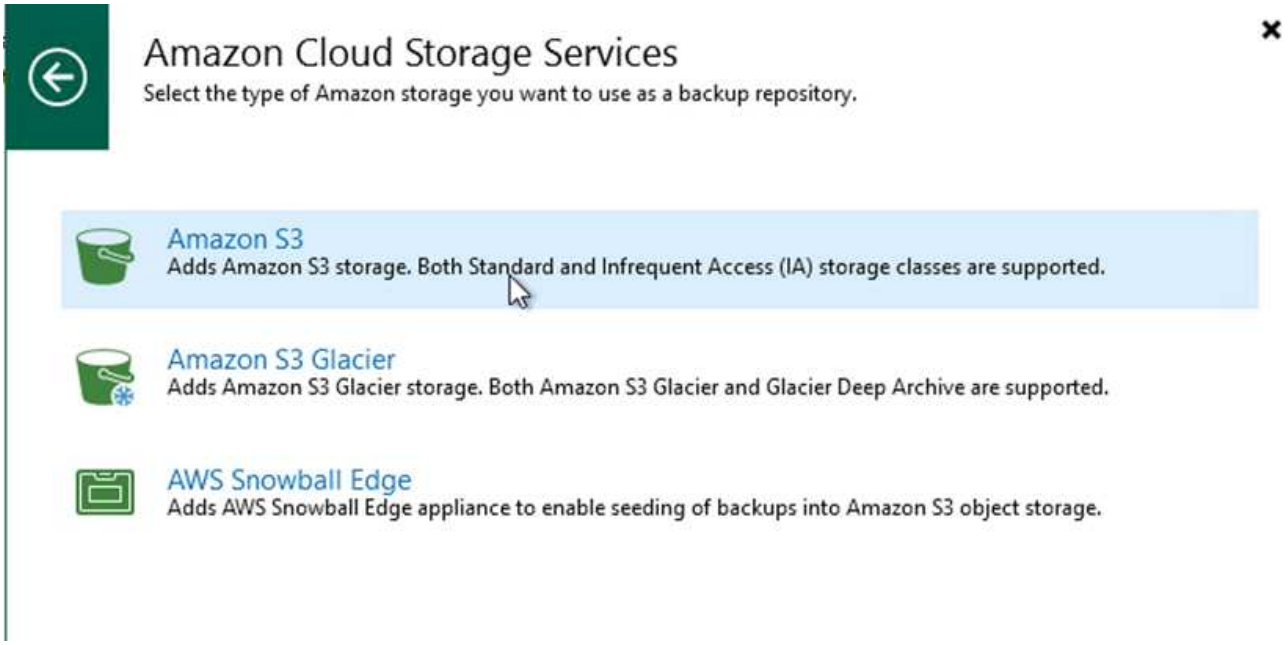
1. 백업 저장소로 가서 상단 메뉴에서 저장소 추가를 클릭하여 백업 저장소 추가 마법사를 시작합니다. 마법사의 첫 번째 페이지에서 백업 저장소 유형으로 개체 스토리지를 선택합니다.



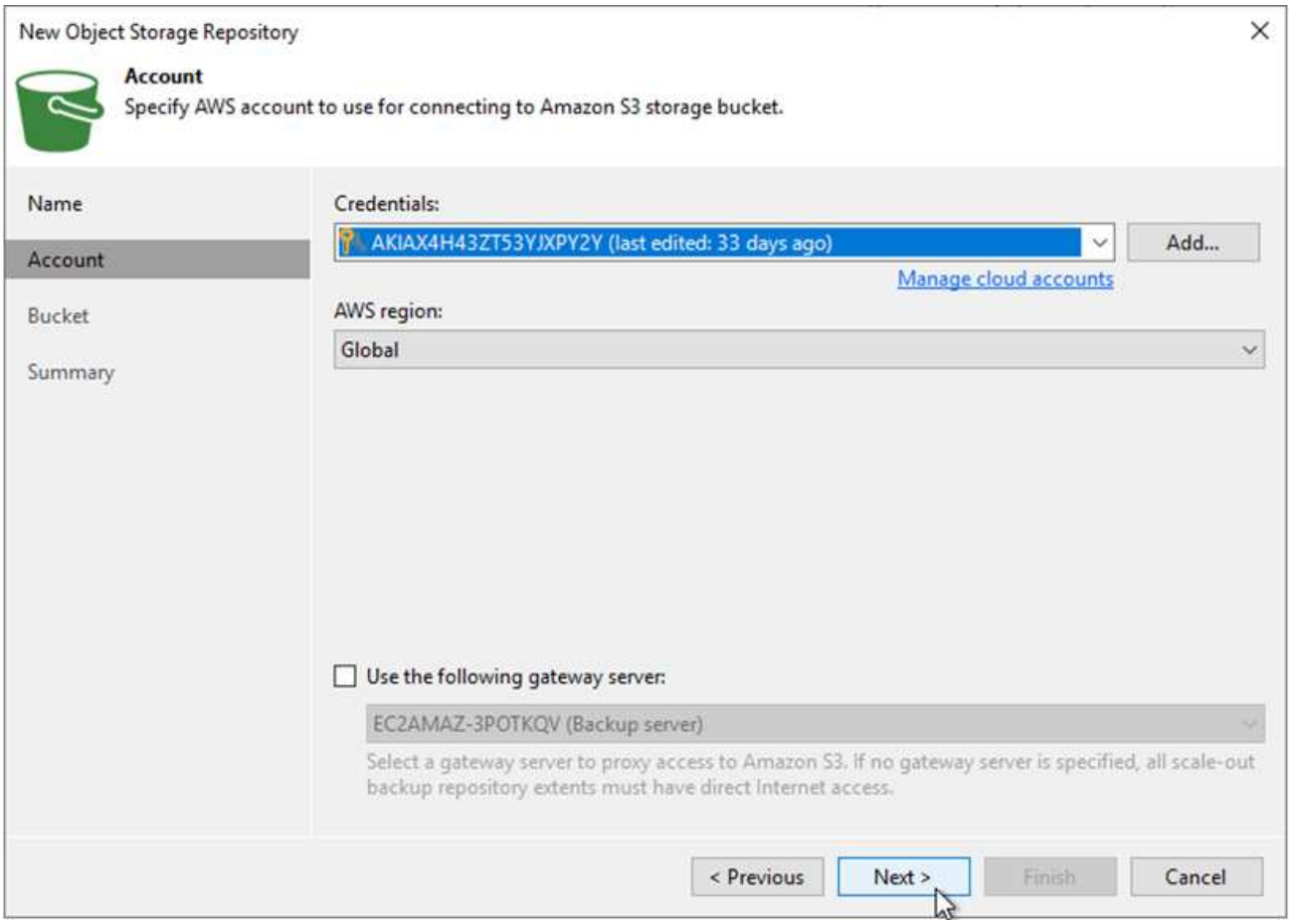
2. 개체 스토리지 유형으로 Amazon S3를 선택합니다.



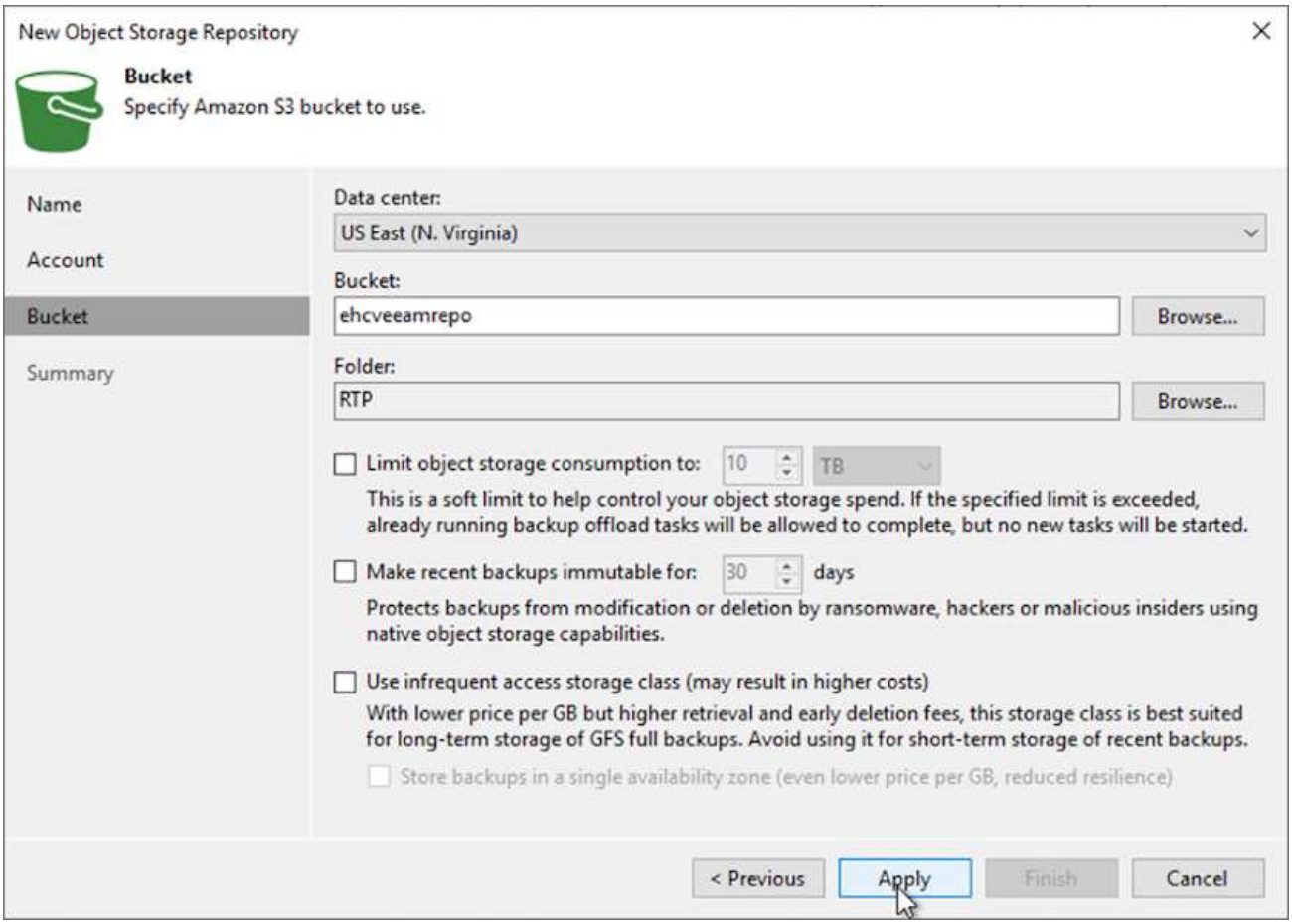
3. Amazon Cloud Storage Services 목록에서 Amazon S3를 선택합니다.



4. 드롭다운 목록에서 미리 입력한 자격 증명을 선택하거나 클라우드 스토리지 리소스에 액세스하기 위한 새 자격 증명을 추가하세요. 계속하려면 '다음'을 클릭하세요.



5. 버킷 페이지에서 데이터 센터, 버킷, 폴더 및 원하는 옵션을 입력합니다. 적용을 클릭하세요.

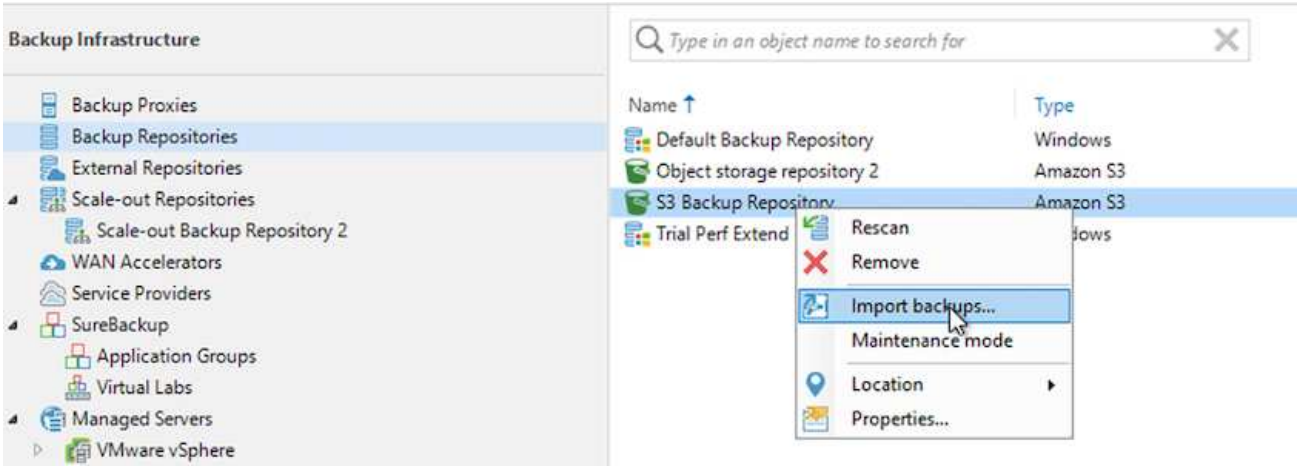


6. 마지막으로, 마침을 선택하여 프로세스를 완료하고 저장소를 추가합니다.

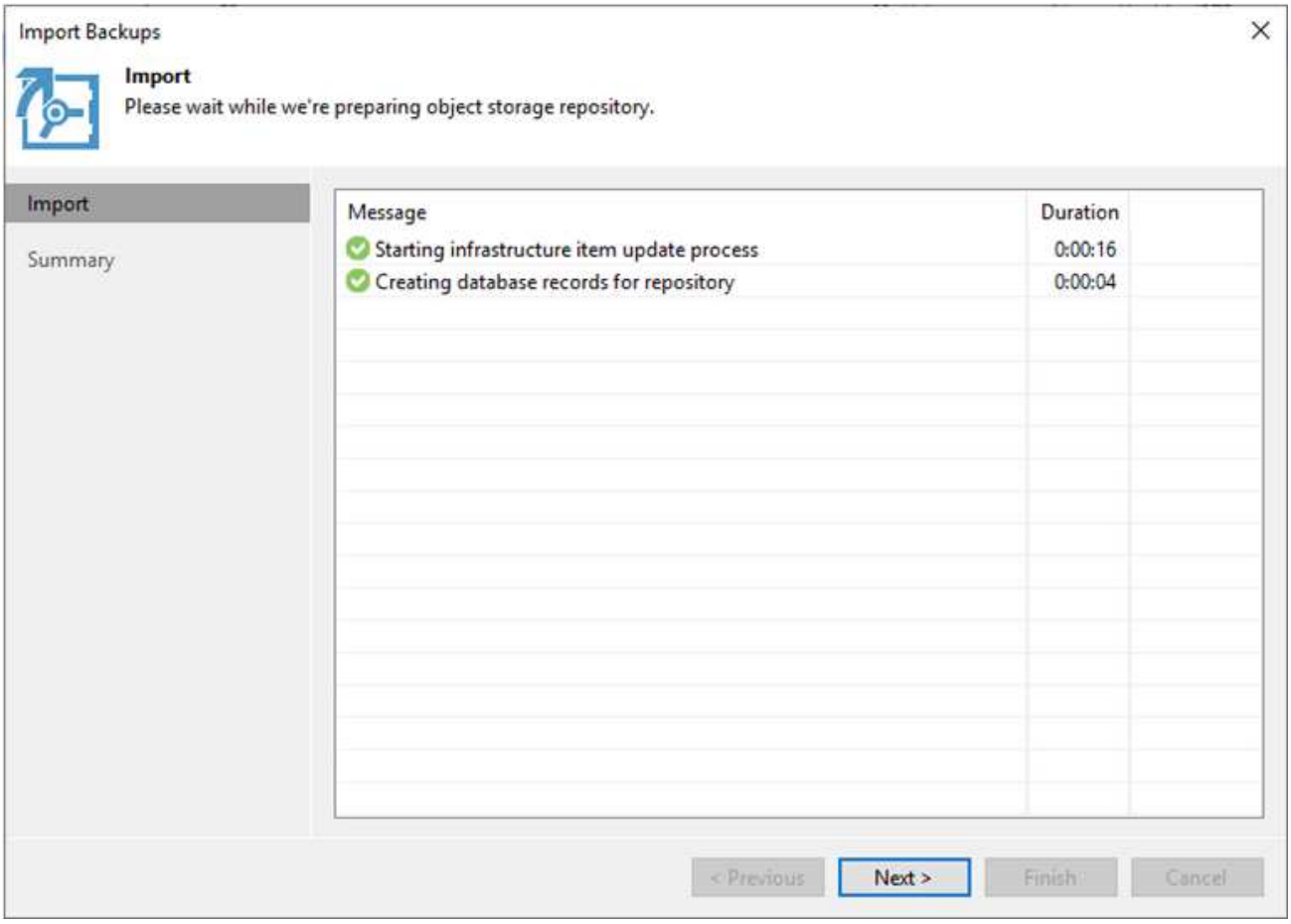
▼ **S3** 개체 스토리지에서 백업 가져오기

이전 섹션에서 추가한 S3 저장소에서 백업을 가져오려면 다음 단계를 완료하세요.

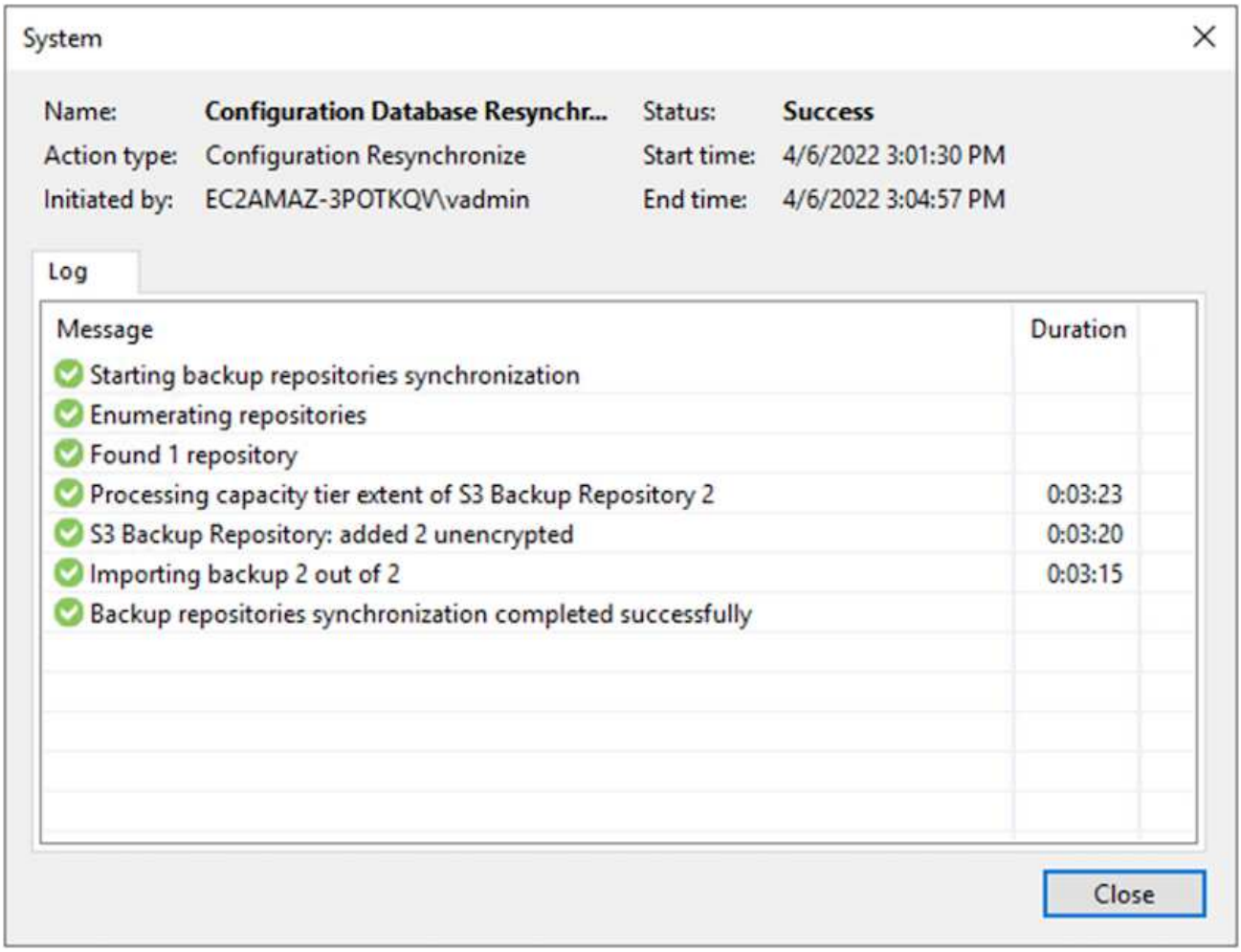
1. S3 백업 저장소에서 백업 가져오기를 선택하여 백업 가져오기 마법사를 시작합니다.



2. 가져오기에 대한 데이터베이스 레코드가 생성된 후 요약 화면에서 다음을 선택한 다음 마침을 선택하여 가져오기 프로세스를 시작합니다.



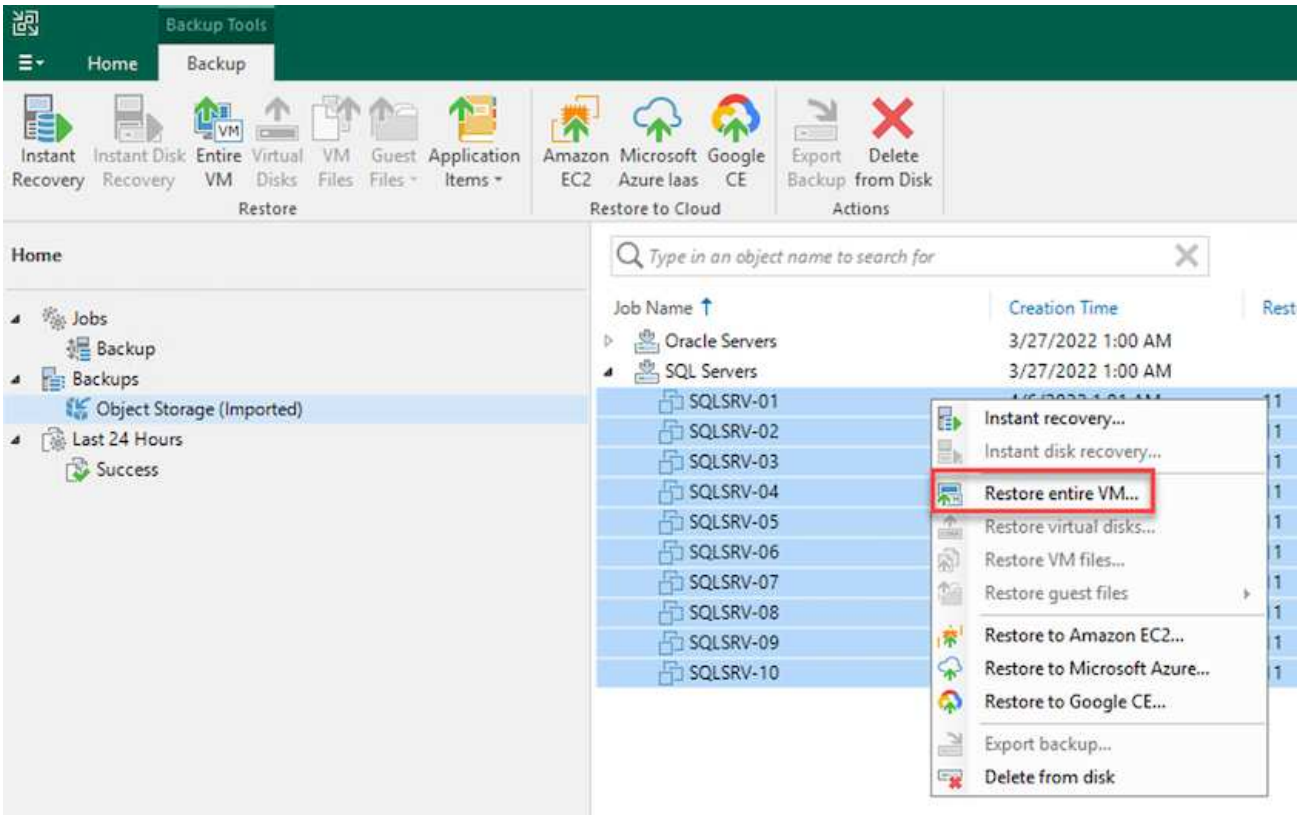
3. 가져오기가 완료되면 VM을 VMware Cloud 클러스터로 복원할 수 있습니다.



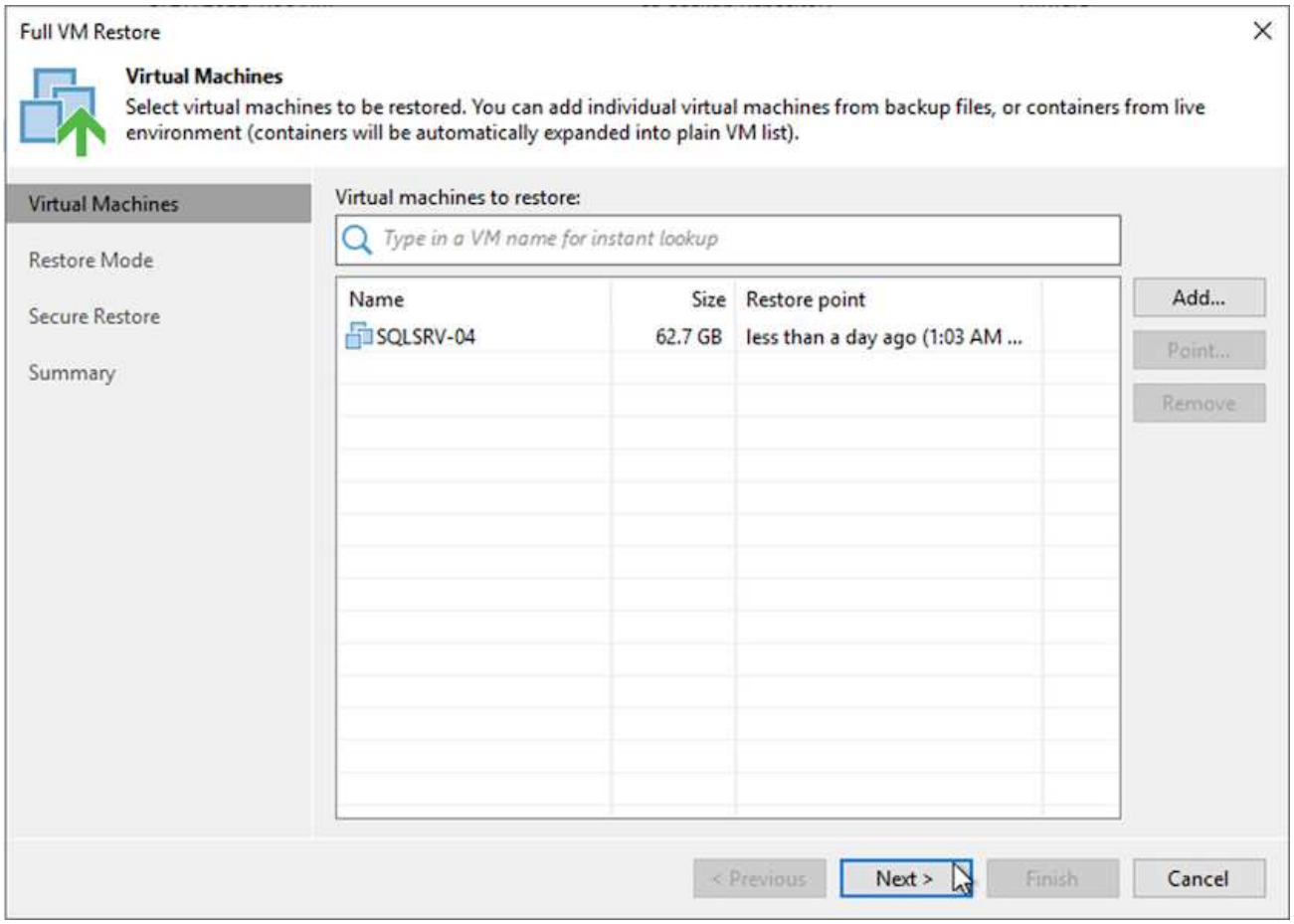
▼ **Veeam** 전체 복원을 사용하여 **VMware Cloud**에 애플리케이션 **VM** 복원

VMware Cloud on AWS 워크로드 도메인/클러스터에 SQL 및 Oracle 가상 머신을 복원하려면 다음 단계를 완료하세요.

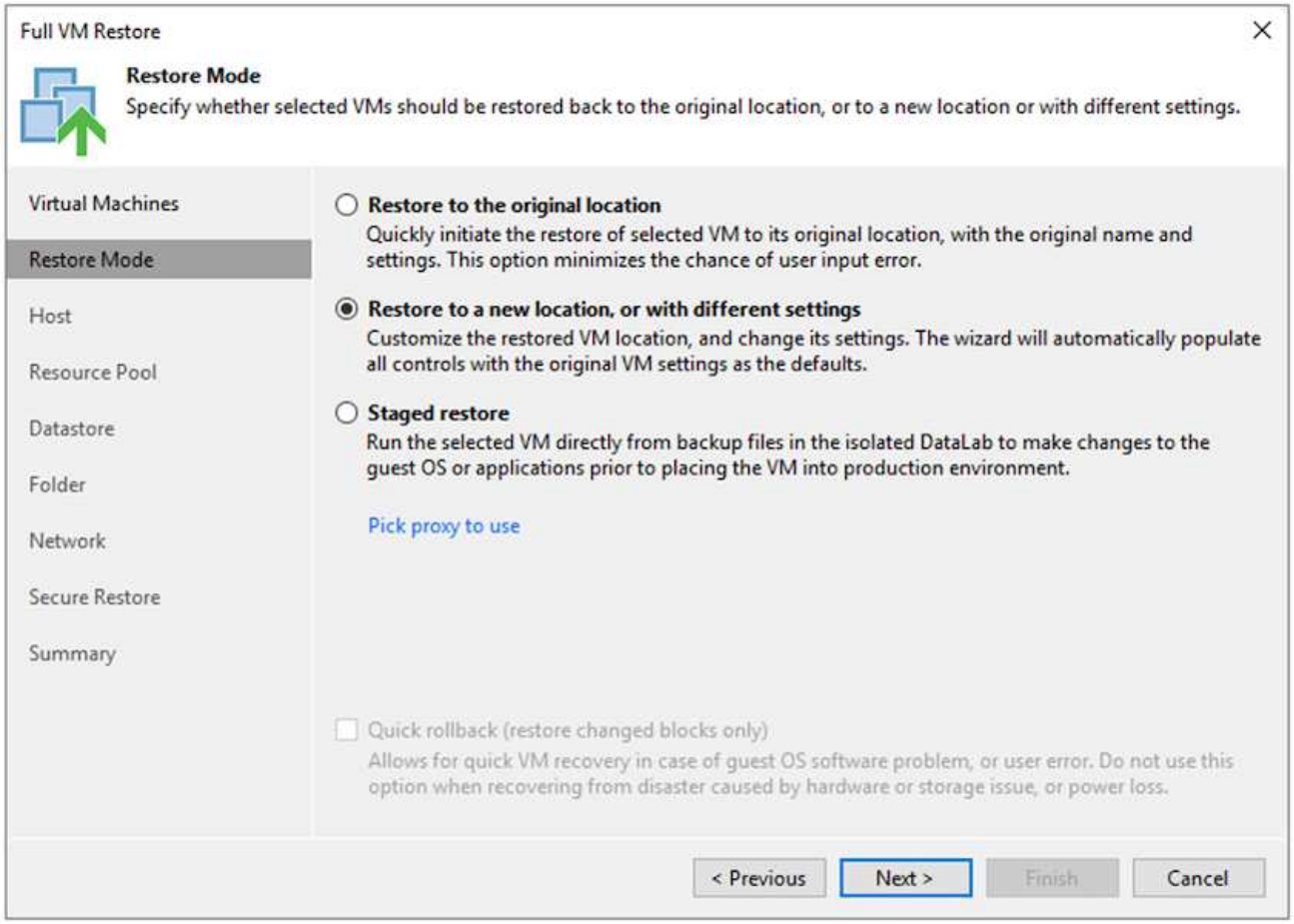
1. Veeam 홈페이지에서 가져온 백업이 포함된 개체 스토리지를 선택하고 복원할 VM을 선택한 다음 마우스 오른쪽 버튼을 클릭하고 전체 VM 복원을 선택합니다.



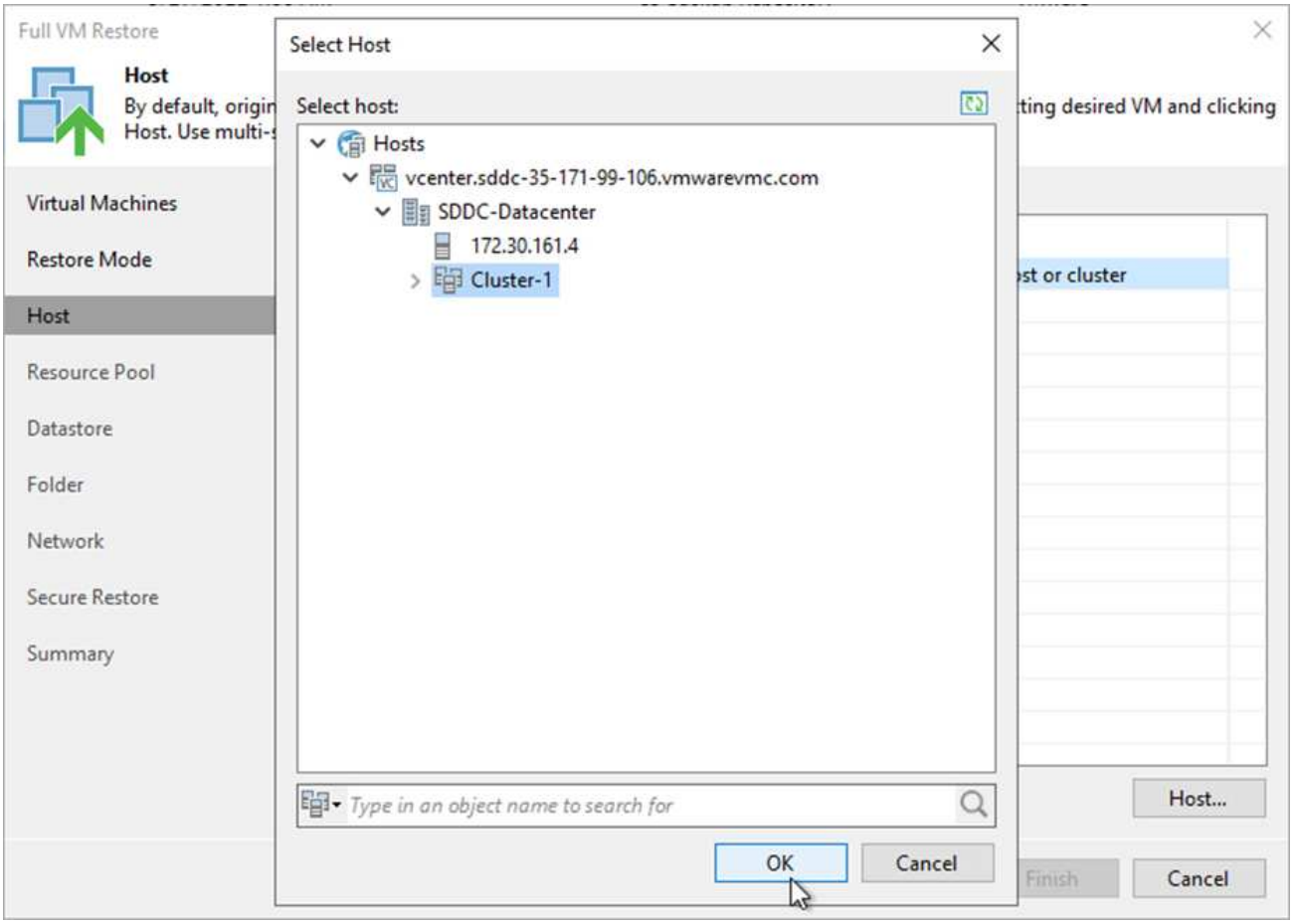
2. 전체 VM 복원 마법사의 첫 번째 페이지에서 원하는 경우 백업할 VM을 수정하고 다음을 선택합니다.



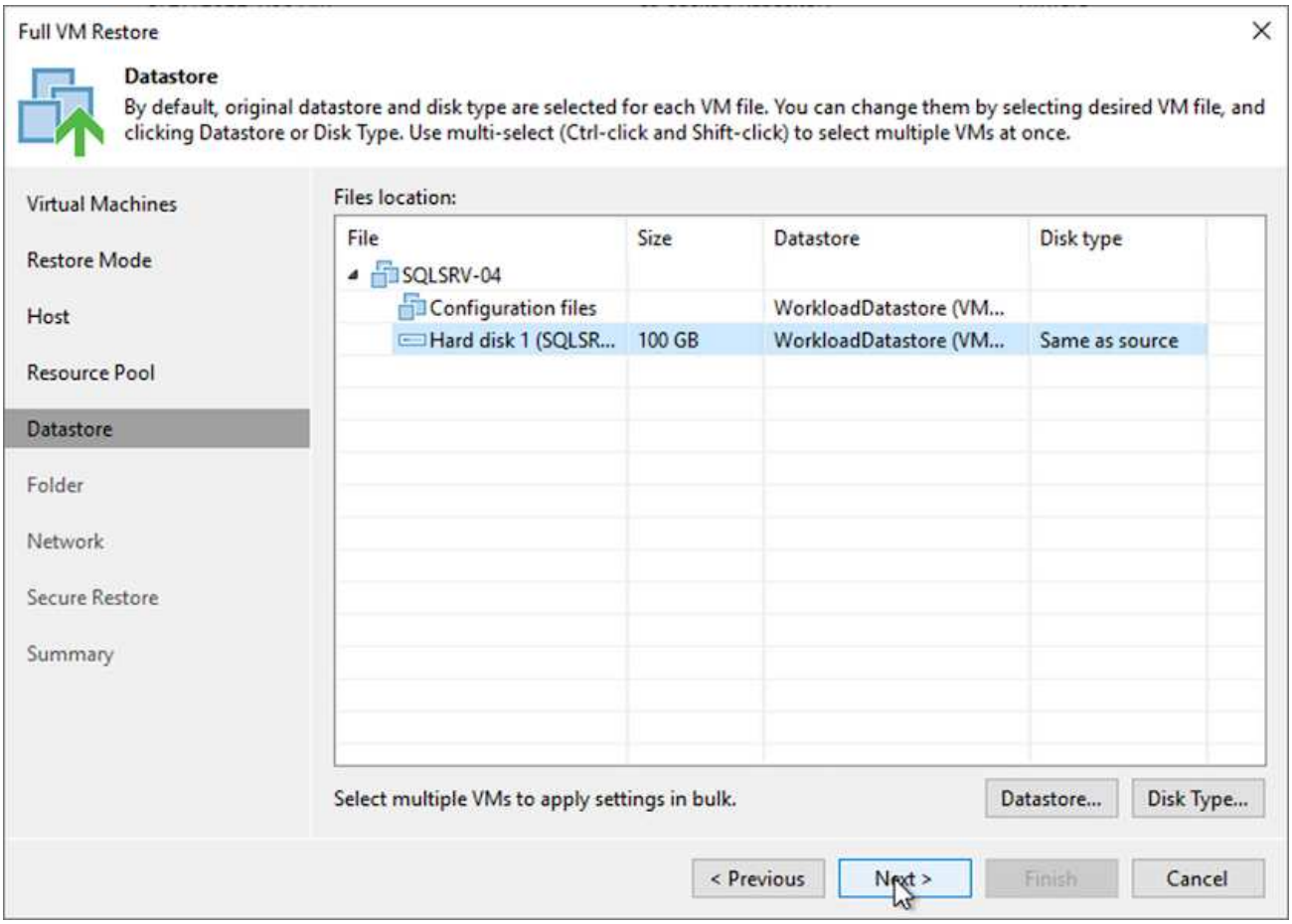
3. 복원 모드 페이지에서 새 위치로 복원 또는 다른 설정으로 복원을 선택합니다.



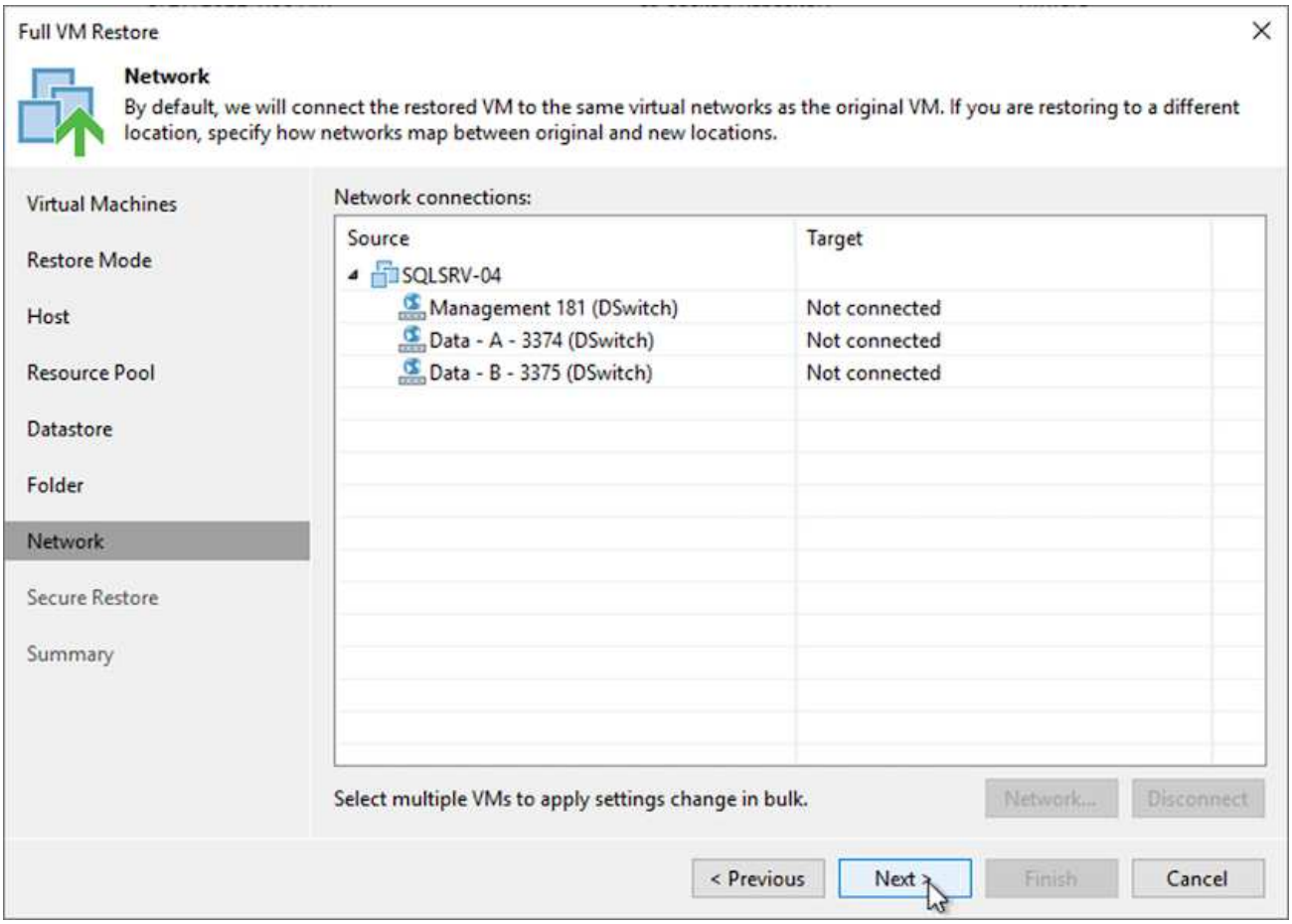
4. 호스트 페이지에서 VM을 복원할 대상 ESXi 호스트 또는 클러스터를 선택합니다.

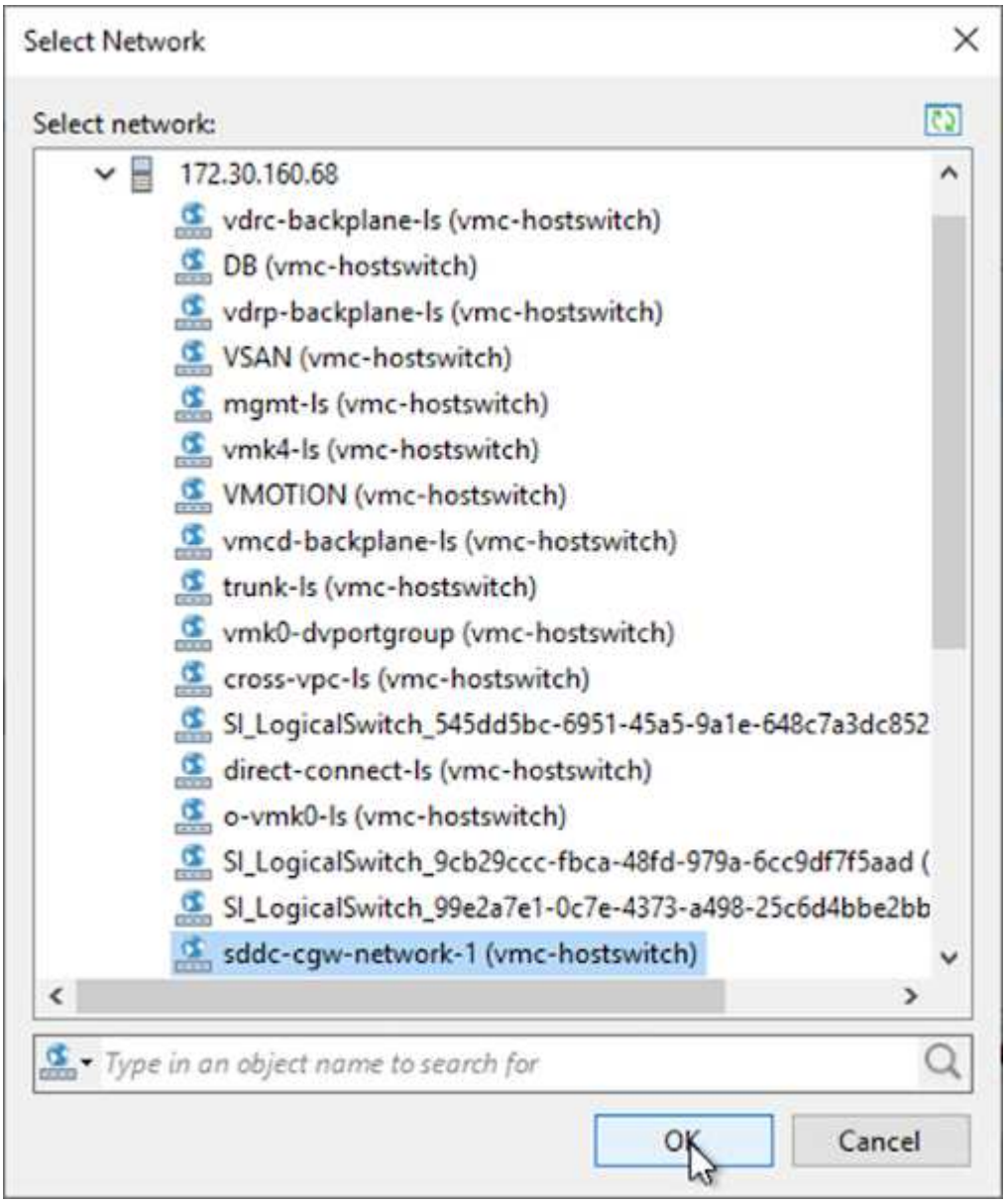


5. 데이터 저장소 페이지에서 구성 파일과 하드 디스크 모두에 대한 대상 데이터 저장소 위치를 선택합니다.



6. 네트워크 페이지에서 VM의 원래 네트워크를 새 대상 위치의 네트워크에 매핑합니다.


Full VM Restore
Network
By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.
Virtual Machines
Restore Mode
Host
Resource Pool
Datastore
Folder
Network
Secure Restore
Summary
Network connections:
Source
Target
SQLSRV-04
Management 181 (DSwitch)
Not connected
Data - A - 3374 (DSwitch)
Not connected
Data - B - 3375 (DSwitch)
Not connected
Select multiple VMs to apply settings change in bulk.
Network...
Disconnect
< Previous
Next >
Finish
Cancel



7. 복구된 VM에서 맬웨어를 검사할지 여부를 선택하고 요약 페이지를 검토한 후 마침을 클릭하여 복원을 시작합니다.

SQL Server 애플리케이션 데이터 복원

다음 프로세스에서는 온프레미스 사이트를 작동 불가능하게 만드는 재해가 발생한 경우 AWS의 VMware Cloud Services에서 SQL Server를 복구하는 방법에 대한 지침을 제공합니다.

복구 단계를 계속 진행하려면 다음 전제 조건이 모두 충족된 것으로 가정합니다.

1. Veeam Full Restore를 사용하여 Windows Server VM이 VMware Cloud SDDC로 복원되었습니다.
2. 보조 SnapCenter 서버가 설정되었고 SnapCenter 데이터베이스 복원 및 구성이 섹션에 설명된 단계를 사용하여 완료되었습니다."SnapCenter 백업 및 복원 프로세스 요약."

▼ **VM: SQL Server VM**에 대한 복원 후 구성

VM 복원이 완료되면 SnapCenter 내에서 호스트 VM을 다시 검색하기 위해 네트워킹 및 기타 항목을 구성해야 합니다.

1. 관리 및 iSCSI 또는 NFS에 대한 새로운 IP 주소를 할당합니다.
2. 호스트를 Windows 도메인에 가입시킵니다.
3. SnapCenter 서버의 DNS 또는 호스트 파일에 호스트 이름을 추가합니다.

SnapCenter 플러그인이 현재 도메인과 다른 도메인 자격 증명을 사용하여 배포된 경우 SQL Server VM에서 Windows 서비스용 플러그인에 대한 로그온 계정을 변경해야 합니다. 로그온 계정을 변경한 후 SnapCenter SMCore, Windows용 플러그인, SQL Server용 플러그인 서비스를 다시 시작합니다.

SnapCenter 에서 복구된 VM을 자동으로 다시 검색하려면 FQDN이 온프레미스 SnapCenter 에 원래 추가된 VM과 동일해야 합니다.

▼ **SQL Server** 복원을 위한 **FSx** 저장소 구성

SQL Server VM에 대한 재해 복구 복원 프로세스를 완료하려면 FSx 클러스터에서 기존 SnapMirror 관계를 해제하고 볼륨에 대한 액세스 권한을 부여해야 합니다. 그렇게 하려면 다음 단계를 완료하세요.

1. SQL Server 데이터베이스와 로그 볼륨에 대한 기존 SnapMirror 관계를 끊으려면 FSx CLI에서 다음 명령을 실행합니다.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

2. SQL Server Windows VM의 iSCSI IQN을 포함하는 이니시에이터 그룹을 만들어 LUN에 대한 액세스 권한을 부여합니다.

```
FSx-Dest::> igroup create -vserver DestSVM -igroup igroupName
-protocol iSCSI -ostype windows -initiator IQN
```

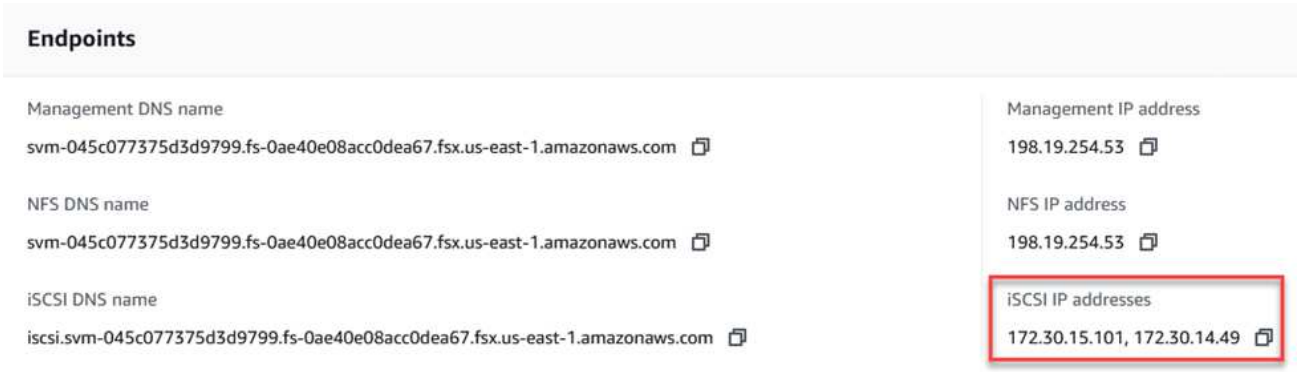
3. 마지막으로 방금 생성한 이니시에이터 그룹에 LUN을 매핑합니다.

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup
igroupName
```

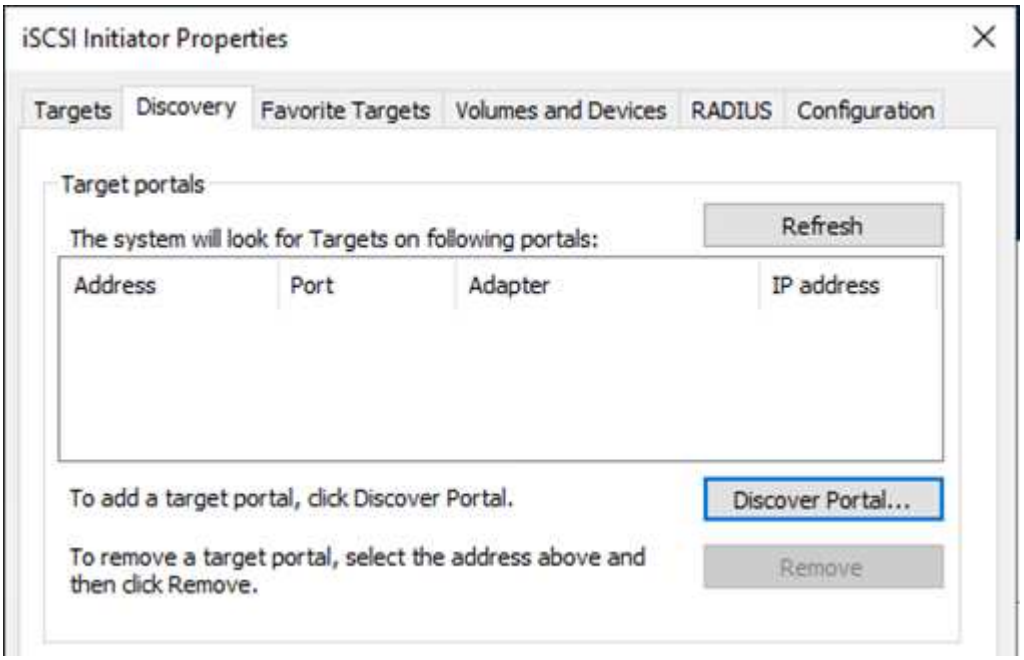
4. 경로 이름을 찾으려면 다음을 실행하세요. `lun show` 명령.

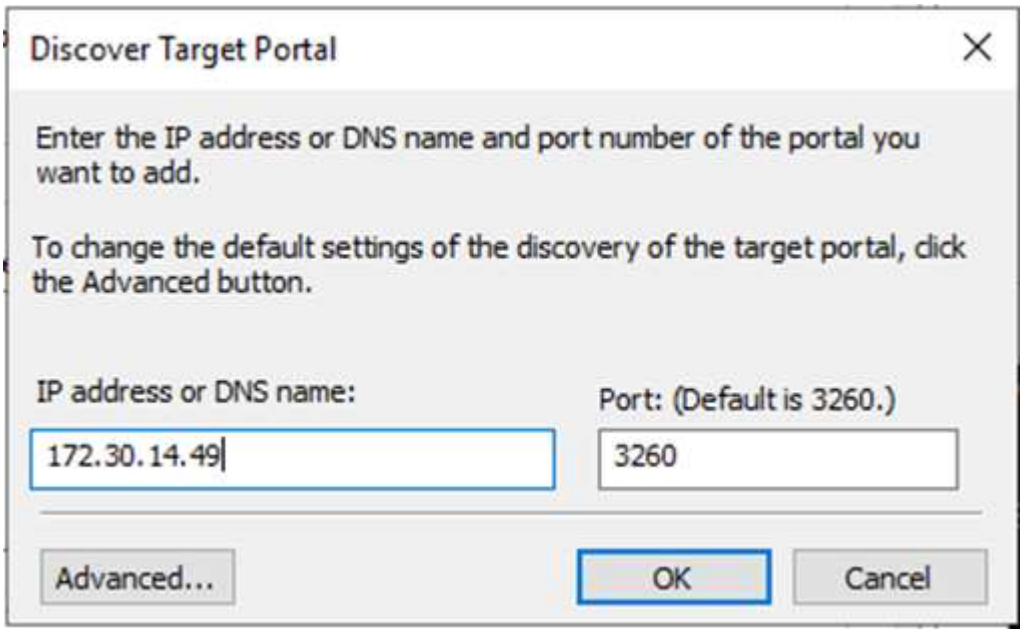
▼ **iSCSI** 액세스를 위해 **Windows VM**을 설정하고 파일 시스템을 검색합니다.

1. SQL Server VM에서 FSx 인스턴스의 iSCSI 대상 인터페이스에 대한 연결이 설정된 VMware 포트 그룹에서 통신하도록 iSCSI 네트워크 어댑터를 설정합니다.
2. iSCSI 초기자 속성 유틸리티를 열고 검색, 즐겨찾는 대상 및 대상 탭에서 이전 연결 설정을 지웁니다.
3. FSx 인스턴스/클러스터에서 iSCSI 논리 인터페이스에 액세스하기 위한 IP 주소를 찾습니다. AWS 콘솔의 Amazon FSx > ONTAP > Storage Virtual Machines에서 해당 내용을 확인할 수 있습니다.



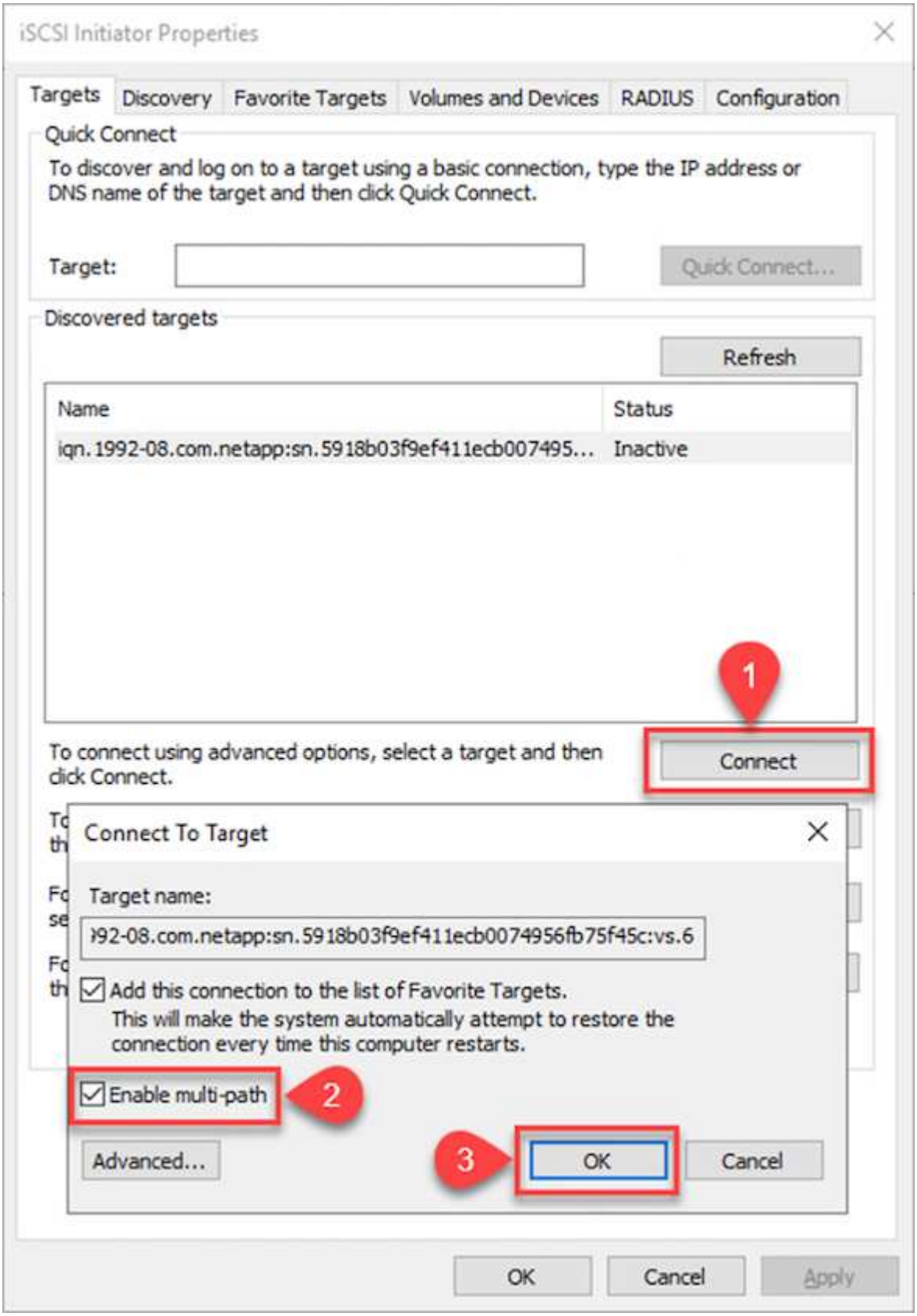
4. 검색 탭에서 검색 포털을 클릭하고 FSx iSCSI 대상의 IP 주소를 입력합니다.



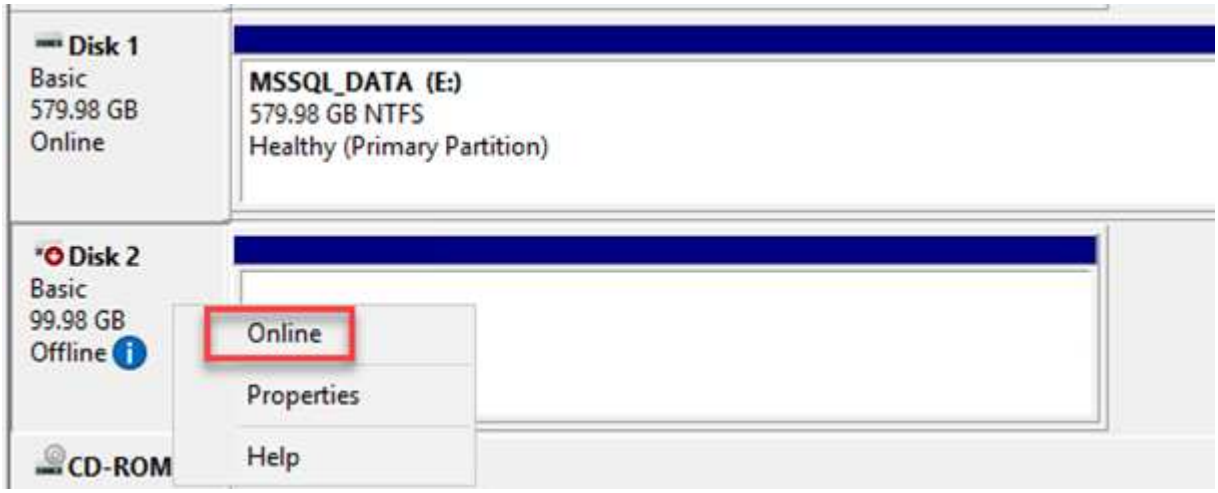


5. 대상 탭에서 연결을 클릭하고 구성에 적합한 경우 다중 경로 사용을 선택한 다음 확인을 클릭하여 대상에

연결합니다.

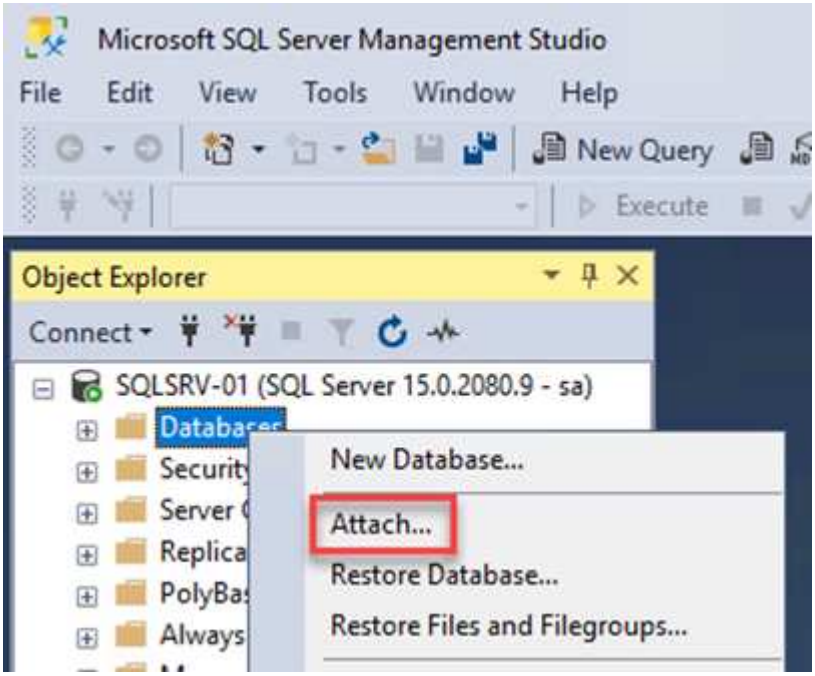


6. 컴퓨터 관리 유틸리티를 열고 디스크를 온라인으로 전환합니다. 이전에 사용하던 것과 동일한 드라이브 문자가 유지되는지 확인하세요.

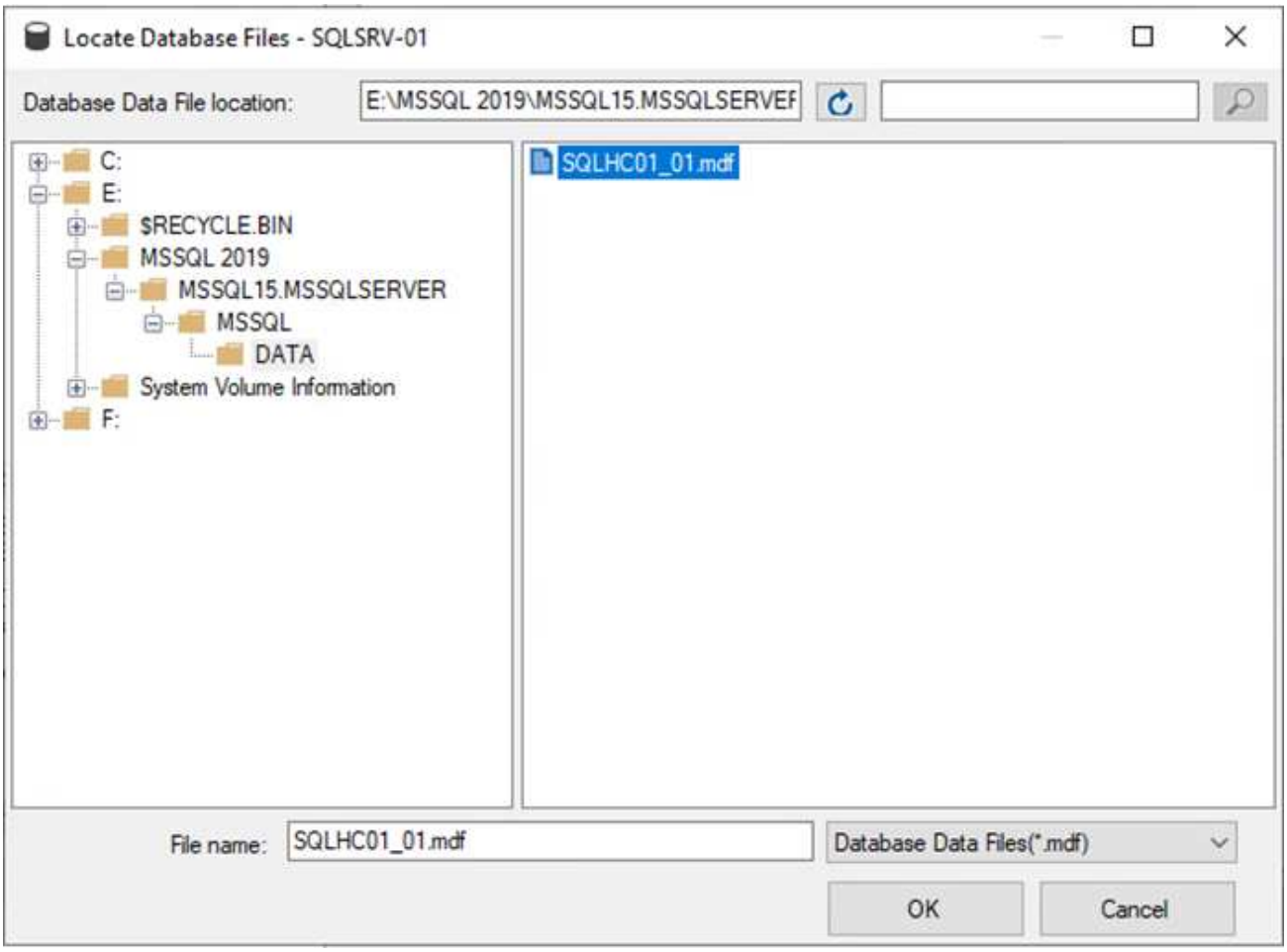


▼ **SQL Server** 데이터베이스 연결

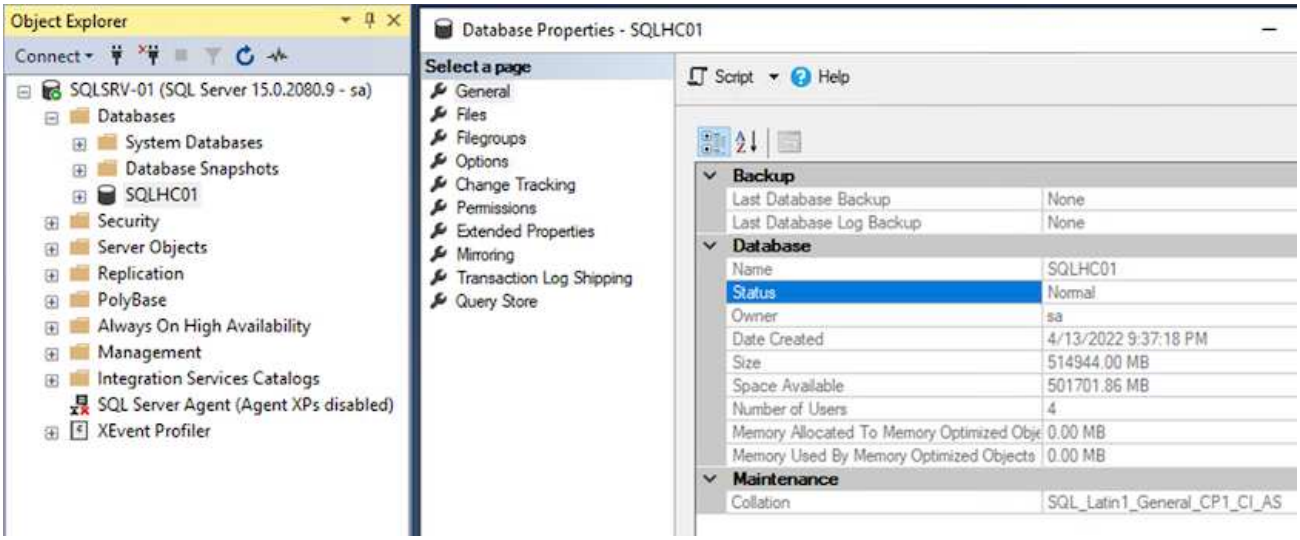
1. SQL Server VM에서 Microsoft SQL Server Management Studio를 열고 연결을 선택하여 데이터베이스에 연결하는 프로세스를 시작합니다.



2. 추가를 클릭하고 SQL Server 기본 데이터베이스 파일이 있는 폴더로 이동하여 해당 파일을 선택한 다음 확인을 클릭합니다.



3. 거래 로그가 별도 드라이브에 있는 경우 거래 로그가 포함된 폴더를 선택하세요.
4. 완료되면 확인을 클릭하여 데이터베이스를 연결합니다.



▼ **SQL Server** 플러그인과 **SnapCenter** 통신 확인

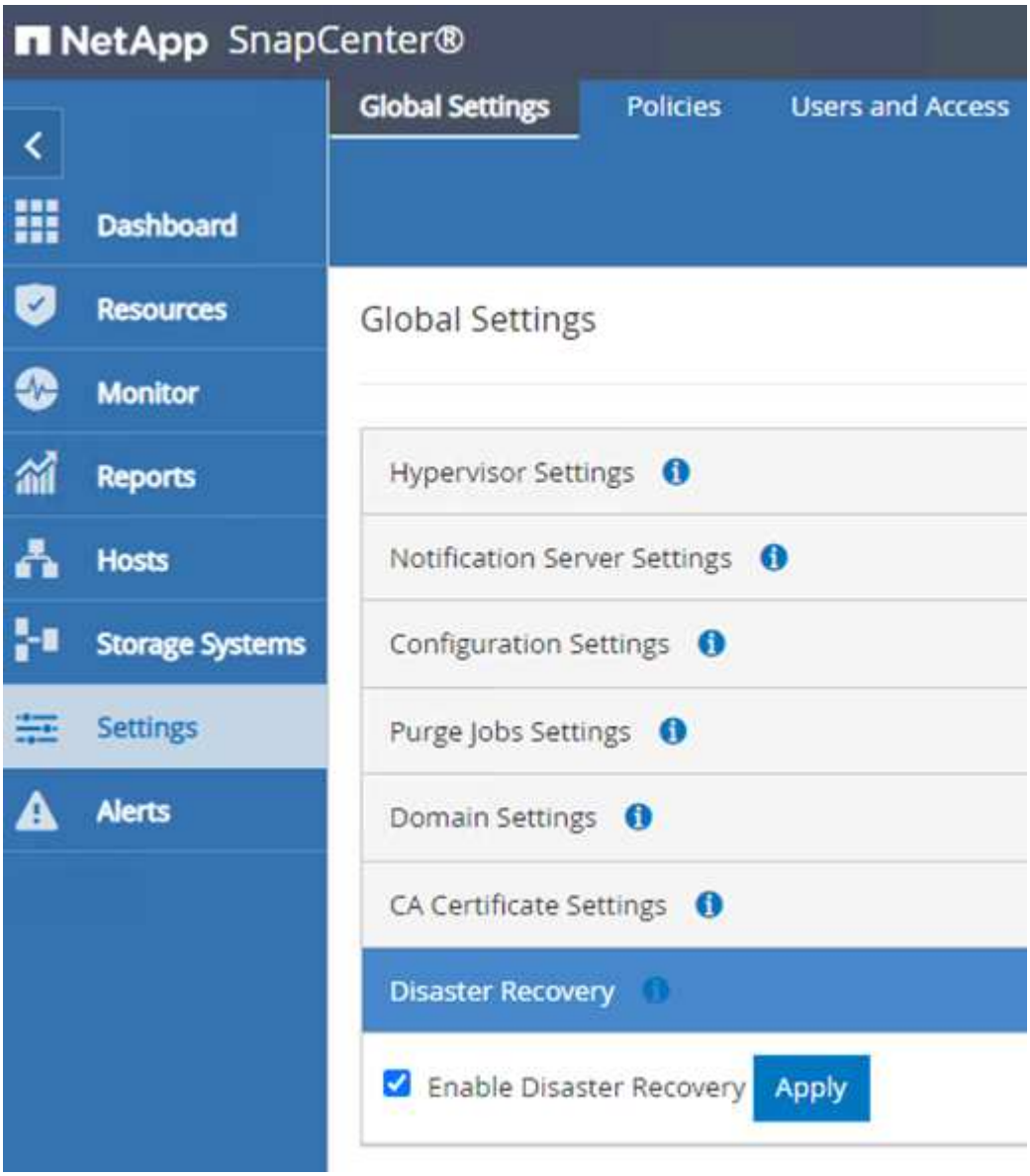
SnapCenter 데이터베이스가 이전 상태로 복원되면 SQL Server 호스트를 자동으로 다시 검색합니다. 이것이 제대로 작동하려면 다음 전제 조건을 염두에 두십시오.

- SnapCenter 재해 복구 모드로 전환해야 합니다. 이 작업은 Swagger API를 통해 수행하거나 재해 복구 아래의

글로벌 설정을 통해 수행할 수 있습니다.

- SQL Server의 FQDN은 온프레미스 데이터 센터에서 실행 중인 인스턴스와 동일해야 합니다.
- 원래의 SnapMirror 관계는 끊어져야 합니다.
- 데이터베이스가 포함된 LUN을 SQL Server 인스턴스에 마운트하고 데이터베이스를 연결해야 합니다.

SnapCenter 재해 복구 모드에 있는지 확인하려면 SnapCenter 웹 클라이언트에서 설정으로 이동하세요. 글로벌 설정 탭으로 이동한 다음 재해 복구를 클릭합니다. 재해 복구 사용 확인란이 활성화되어 있는지 확인하세요.



Oracle 애플리케이션 데이터 복원

다음 프로세스에서는 온프레미스 사이트를 작동 불가능하게 만드는 재해가 발생한 경우 AWS의 VMware Cloud Services에서 Oracle 애플리케이션 데이터를 복구하는 방법에 대한 지침을 제공합니다.

복구 단계를 계속하려면 다음 전제 조건을 완료하세요.

1. Oracle Linux 서버 VM은 Veeam Full Restore를 사용하여 VMware Cloud SDDC로 복원되었습니다.

2. 보조 SnapCenter 서버가 설정되었고 SnapCenter 데이터베이스와 구성 파일이 이 섹션에 설명된 단계를 사용하여 복원되었습니다."SnapCenter 백업 및 복원 프로세스 요약."

▼ **Oracle** 복원을 위한 **FSx** 구성 **– SnapMirror** 관계 끊기

FSx ONTAP 인스턴스에 호스팅된 보조 스토리지 볼륨을 Oracle 서버에서 액세스할 수 있게 하려면 먼저 기존 SnapMirror 관계를 해제해야 합니다.

1. FSx CLI에 로그인한 후 다음 명령을 실행하여 올바른 이름으로 필터링된 볼륨을 확인합니다.

```
FSx-Dest::> volume show -volume VolumeName*
```

```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
ora_svm_dest
          oraclesrv_03_u01_dest
                       aggr1        online     DP        100GB    93.12GB    6%
ora_svm_dest
          oraclesrv_03_u02_dest
                       aggr1        online     DP        200GB    34.98GB   82%
ora_svm_dest
          oraclesrv_03_u03_dest
                       aggr1        online     DP        150GB    33.37GB   77%
3 entries were displayed.

FsxId0ae40e08acc0dea67::>
```

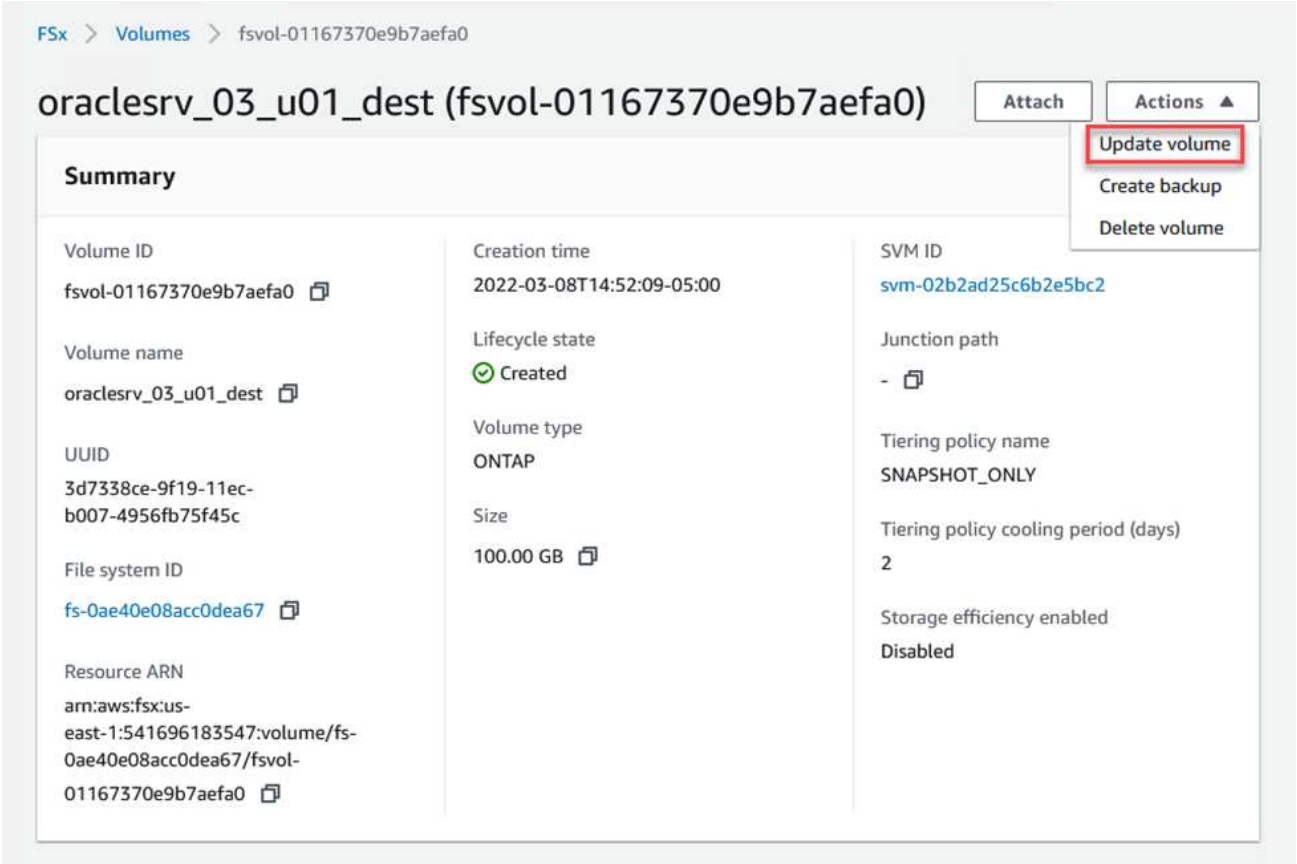
2. 다음 명령을 실행하여 기존 SnapMirror 관계를 해제합니다.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

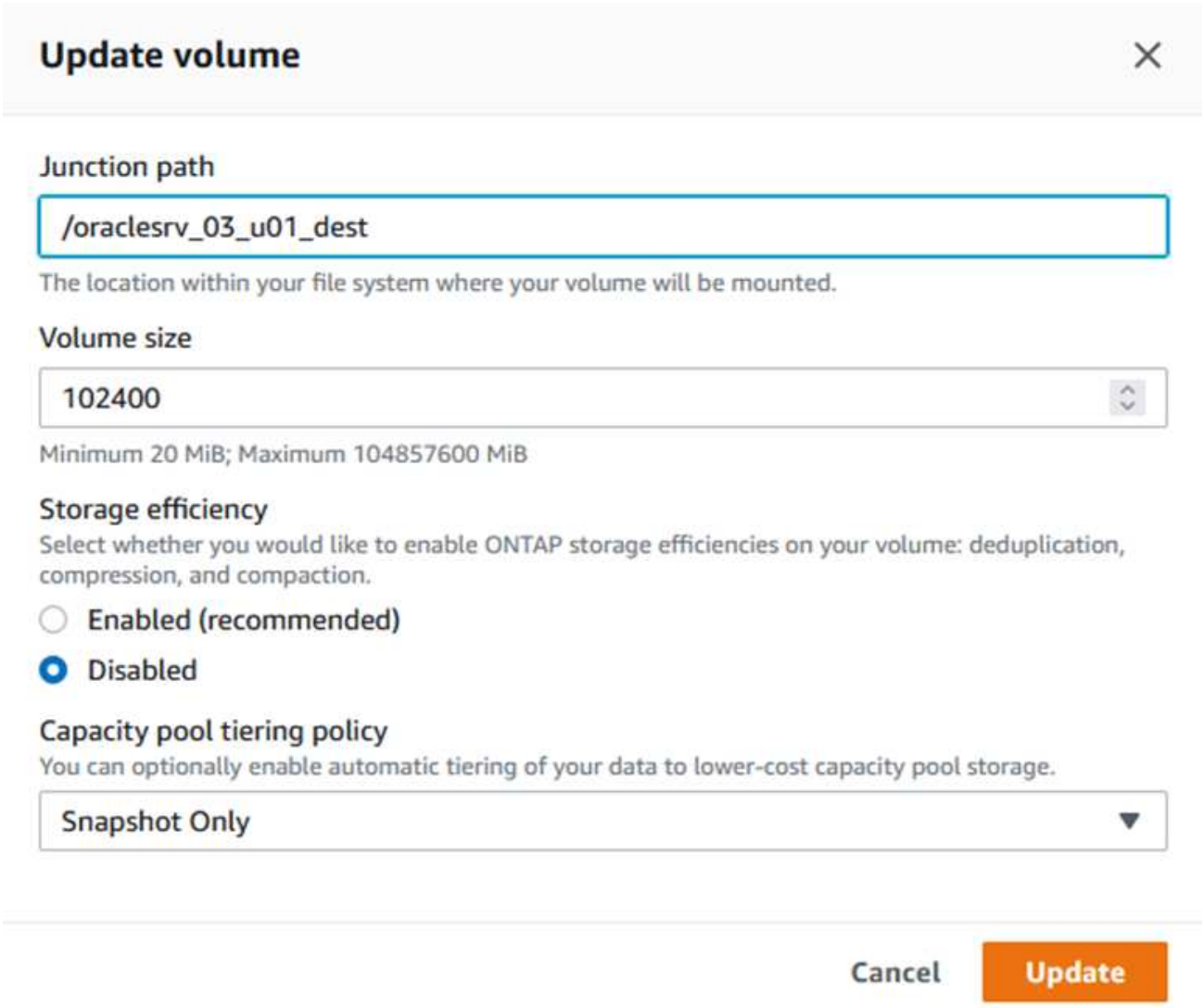
```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".
```

3. Amazon FSx 웹 클라이언트에서 junction-path를 업데이트합니다.



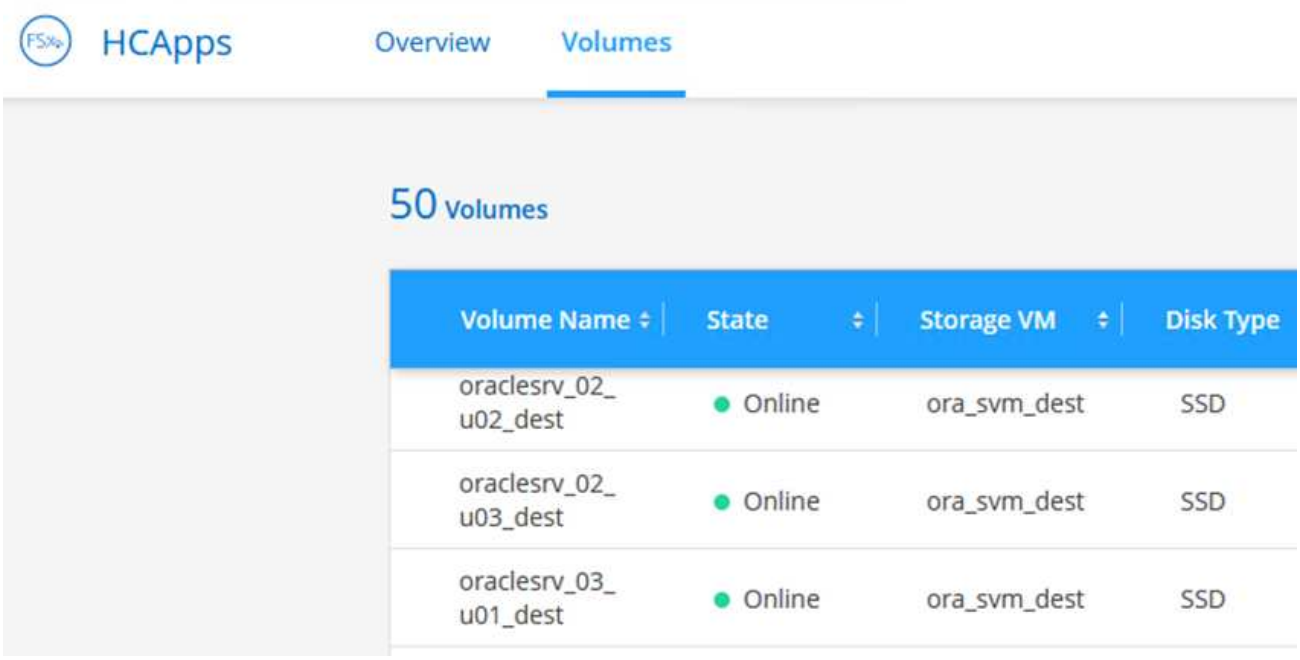
4. 교차로 경로 이름을 추가하고 업데이트를 클릭합니다. Oracle 서버에서 NFS 볼륨을 마운트할 때 이 연결 경로를 지정하세요.



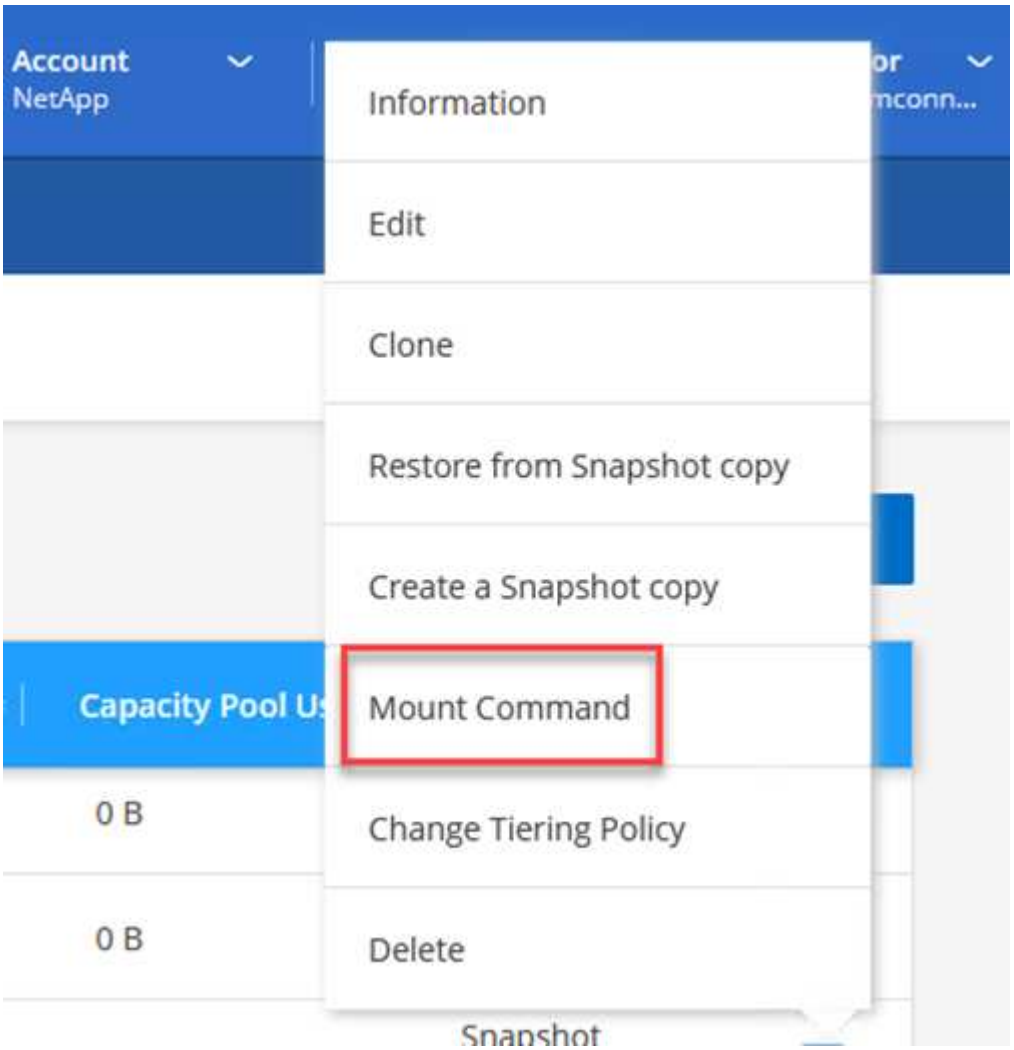
▼ **Oracle Server**에 **NFS** 볼륨 마운트

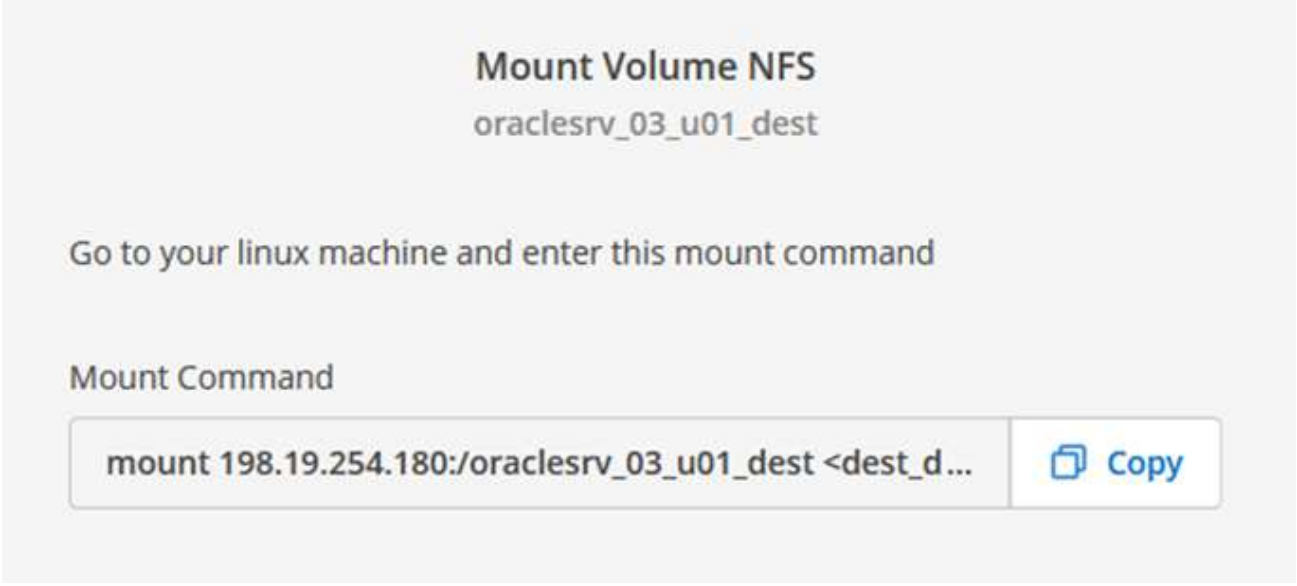
Cloud Manager에서는 Oracle 데이터베이스 파일과 로그가 포함된 NFS 볼륨을 마운트하기 위한 올바른 NFS LIF IP 주소를 사용하여 mount 명령을 얻을 수 있습니다.

1. Cloud Manager에서 FSx 클러스터의 볼륨 목록에 액세스합니다.



2. 작업 메뉴에서 Mount Command를 선택하여 Oracle Linux 서버에서 사용할 mount 명령을 보고 복사합니다.





3. Oracle Linux 서버에 NFS 파일 시스템을 마운트합니다. NFS 공유를 마운트하기 위한 디렉토리가 이미 Oracle Linux 호스트에 있습니다.
4. Oracle Linux 서버에서 mount 명령을 사용하여 NFS 볼륨을 마운트합니다.

```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

Oracle 데이터베이스와 연관된 각 볼륨에 대해 이 단계를 반복합니다.

재부팅 시에도 NFS 마운트를 유지하려면 다음을 편집하세요. `/etc/fstab` 마운트 명령을 포함할 파일입니다.

5. Oracle 서버를 재부팅합니다. Oracle 데이터베이스는 정상적으로 시작되어 사용할 수 있어야 합니다.

장애 복구

이 솔루션에 설명된 장애 조치 프로세스를 성공적으로 완료하면 SnapCenter 와 Veeam은 AWS에서 실행되는 백업 기능을 재개하고 FSx ONTAP 이제 원래 온프레미스 데이터 센터와 기존 SnapMirror 관계가 없는 기본 스토리지로 지정됩니다. 온프레미스에서 정상 기능이 재개된 후에는 이 문서에 설명된 것과 동일한 프로세스를 사용하여 데이터를 온프레미스 ONTAP 스토리지 시스템으로 다시 미러링할 수 있습니다.

이 문서에도 설명되어 있듯이 SnapCenter 구성하여 FSx ONTAP 의 애플리케이션 데이터 볼륨을 온프레미스에 있는 ONTAP 스토리지 시스템으로 미러링할 수 있습니다. 마찬가지로, 스케일아웃 백업 저장소를 사용하여 Veeam이 백업 사본을 Amazon S3에 복제하도록 구성하면 온프레미스 데이터 센터에 있는 Veeam 백업 서버에서 해당 백업에 액세스할 수 있습니다.

이 문서에서는 장애 복구에 대해 다루지 않지만, 장애 복구는 여기에 설명된 자세한 프로세스와 크게 다르지 않습니다.

결론

이 문서에 제시된 사용 사례는 NetApp 과 VMware 간의 통합을 강조하는 검증된 재해 복구 기술에 초점을 맞춥니다. NetApp ONTAP 스토리지 시스템은 검증된 데이터 미러링 기술을 제공하여 조직이 온프레미스와 주요 클라우드 공급업체가 제공하는 ONTAP 기술을 아우르는 재해 복구 솔루션을 설계할 수 있도록 지원합니다.

AWS의 FSx ONTAP SnapCenter 및 SyncMirror 와 원활하게 통합되어 애플리케이션 데이터를 클라우드로 복제할 수 있는 솔루션 중 하나입니다. Veeam Backup & Replication은 NetApp ONTAP 스토리지 시스템과 잘 통합되는 또 다른 잘 알려진 기술이며 vSphere 기본 스토리지로의 장애 조치를 제공할 수 있습니다.

이 솔루션은 SQL Server와 Oracle 애플리케이션 데이터를 호스팅하는 ONTAP 시스템의 게스트 연결 스토리지를 사용하는 재해 복구 솔루션을 제공합니다. SnapMirror 탑재된 SnapCenter ONTAP 시스템의 애플리케이션 볼륨을 보호하고 이를 클라우드에 있는 FSx 또는 CVO로 복제하기 위한 관리하기 쉬운 솔루션을 제공합니다. SnapCenter 모든 애플리케이션 데이터를 AWS의 VMware Cloud로 장애 조치하기 위한 DR 지원 솔루션입니다.

Amazon FSx ONTAP 활용한 **VMware Cloud**의 **Veeam** 백업 및 복원

Veeam Backup & Replication은 VMware Cloud의 데이터를 보호하기 위한 효과적이고 안정적인 솔루션입니다. 이 솔루션은 Veeam Backup and Replication을 사용하여 VMware Cloud의 FSx ONTAP NFS 데이터 저장소에 있는 애플리케이션 VM을 백업하고 복원하기 위한 적절한 설정과 구성을 보여줍니다.

개요

VMware Cloud(AWS 내)는 NFS 데이터 저장소를 보조 스토리지로 사용할 수 있도록 지원하고, FSx ONTAP SDDC 클러스터의 ESXi 호스트 수에 관계없이 확장 가능한 클라우드 애플리케이션용 대량의 데이터를 저장해야 하는 고객을 위한 안전한 솔루션입니다. 이 통합 AWS 스토리지 서비스는 기존의 모든 NetApp ONTAP 기능과 함께 매우 효율적인 스토리지를 제공합니다.

사용 사례

이 솔루션은 다음과 같은 사용 사례를 해결합니다.

- FSx ONTAP 백업 저장소로 사용하여 VMC에 호스팅된 Windows 및 Linux 가상 머신을 백업하고 복원합니다.
- FSx ONTAP 백업 저장소로 사용하여 Microsoft SQL Server 애플리케이션 데이터를 백업하고 복원합니다.
- FSx ONTAP 백업 저장소로 사용하여 Oracle 애플리케이션 데이터를 백업하고 복원합니다.

Amazon FSx ONTAP 사용한 **NFS** 데이터 저장소

이 솔루션의 모든 가상 머신은 FSx ONTAP 보조 NFS 데이터 저장소에 있습니다. FSx ONTAP NFS 데이터 저장소의 보완 수단으로 사용하면 여러 가지 이점이 있습니다. 예를 들어, 다음을 수행할 수 있습니다.

- 복잡한 설정이나 관리 없이도 클라우드에서 확장 가능하고 가용성이 높은 파일 시스템을 만드세요.
- 기존 VMware 환경과 통합하여 익숙한 도구와 프로세스를 사용하여 클라우드 리소스를 관리할 수 있습니다.
- 스냅샷 및 복제와 같은 ONTAP 이 제공하는 고급 데이터 관리 기능을 활용하여 데이터를 보호하고 가용성을 보장하세요.

▼ 솔루션 배포 개요

이 목록은 Veeam Backup & Replication을 구성하고, FSx ONTAP 백업 저장소로 사용하여 백업 및 복원 작업을 실행하고, SQL Server와 Oracle VM 및 데이터베이스를 복원하는 데 필요한 상위 수준의 단계를 제공합니다.

1. Veeam Backup & Replication의 iSCSI 백업 저장소로 사용할 FSx ONTAP 파일 시스템을 만듭니다.
2. Veeam Proxy를 배포하여 백업 워크로드를 분산하고 FSx ONTAP 에 호스팅된 iSCSI 백업 저장소를 마운트합니다.

3. Veeam 백업 작업을 구성하여 SQL Server, Oracle, Linux 및 Windows 가상 머신을 백업합니다.
4. SQL Server 가상 머신과 개별 데이터베이스를 복원합니다.
5. Oracle 가상 머신과 개별 데이터베이스를 복원합니다.

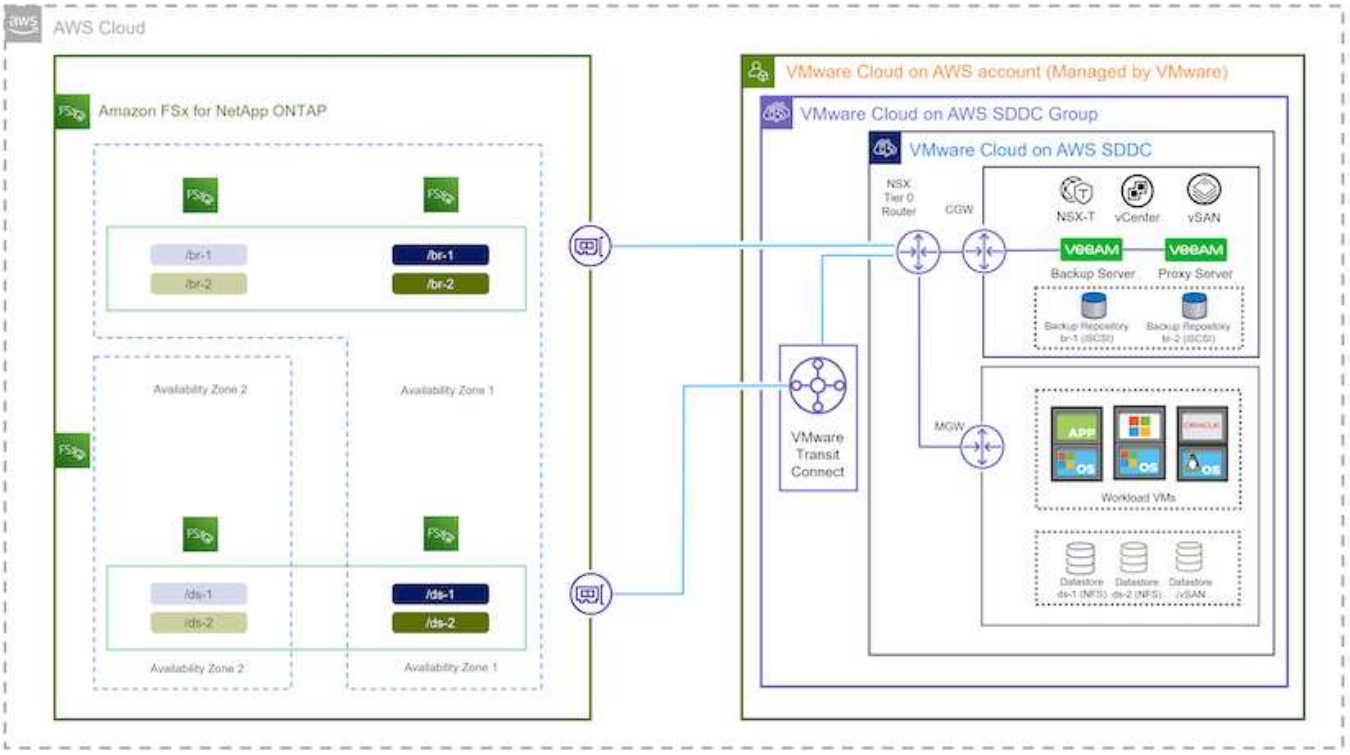
▼ 필수 조건

이 솔루션의 목적은 FSx ONTAP 에서 호스팅되는 NFS 데이터스토어에 위치하고 VMware Cloud에서 실행되는 가상 머신의 데이터 보호를 시연하는 것입니다. 이 솔루션은 다음 구성 요소가 구성되어 사용할 준비가 되었다고 가정합니다.

1. VMware Cloud에 연결된 하나 이상의 NFS 데이터 저장소가 있는 FSx ONTAP 파일 시스템입니다.
2. Veeam Backup & Replication 소프트웨어가 설치된 Microsoft Windows Server VM.
    - Veeam Backup & Replication 서버는 IP 주소나 정규화된 도메인 이름을 사용하여 vCenter 서버를 검색했습니다.
3. 솔루션 배포 중에 Veeam Backup Proxy 구성 요소와 함께 Microsoft Windows Server VM을 설치해야 합니다.
4. FSx ONTAP NFS 데이터 저장소에 VMDK와 애플리케이션 데이터가 있는 Microsoft SQL Server VM. 이 솔루션의 경우 두 개의 별도 VMDK에 두 개의 SQL 데이터베이스가 있었습니다.
    - 참고: 모범 사례로, 데이터베이스와 트랜잭션 로그 파일을 별도의 드라이브에 저장하면 성능과 안정성이 향상됩니다. 이는 트랜잭션 로그가 순차적으로 작성되는 반면, 데이터베이스 파일은 무작위로 작성되기 때문입니다.
5. FSx ONTAP NFS 데이터 저장소에 VMDK와 애플리케이션 데이터가 있는 Oracle Database VM입니다.
6. FSx ONTAP NFS 데이터 저장소에 VMDK가 있는 Linux 및 Windows 파일 서버 VM.
7. Veeam은 백업 환경에서 서버와 구성 요소 간 통신을 위해 특정 TCP 포트가 필요합니다. Veeam 백업 인프라 구성 요소에서는 필요한 방화벽 규칙이 자동으로 생성됩니다. 네트워크 포트 요구 사항의 전체 목록은 포트 섹션을 참조하세요. "VMware vSphere용 Veeam 백업 및 복제 사용자 가이드" .

고수준 아키텍처

이 솔루션의 테스트/검증은 최종 배포 환경과 일치할 수도 있고 일치하지 않을 수도 있는 실험실에서 수행되었습니다. 자세한 내용은 다음 섹션을 참조하세요.



▼ 하드웨어/소프트웨어 구성 요소

이 솔루션의 목적은 FSx ONTAP 에서 호스팅되는 NFS 데이터스토어에 위치하고 VMware Cloud에서 실행되는 가상 머신의 데이터 보호를 시연하는 것입니다. 이 솔루션은 다음 구성 요소가 이미 구성되어 사용할 준비가 되었다고 가정합니다.

- FSx ONTAP NFS 데이터 저장소에 있는 Microsoft Windows VM
- FSx ONTAP NFS 데이터 저장소에 위치한 Linux(CentOS) VM
- FSx ONTAP NFS 데이터 저장소에 있는 Microsoft SQL Server VM
  - 별도의 VMDK에 호스팅된 두 개의 데이터베이스
- FSx ONTAP NFS 데이터 저장소에 있는 Oracle VM

솔루션 배포

이 솔루션에서는 AWS의 VMware Cloud SDDC에서 SQL Server, Oracle, Windows 및 Linux 파일 서버 가상 머신의 백업과 복구를 수행하기 위해 Veeam Backup and Replication 소프트웨어를 활용하는 솔루션을 배포하고 검증하기 위한 자세한 지침을 제공합니다. 이 솔루션의 가상 머신은 FSx ONTAP 에서 호스팅되는 보조 NFS 데이터 저장소에 있습니다. 또한, Veeam 백업 저장소에 사용될 iSCSI 볼륨을 호스팅하기 위해 별도의 FSx ONTAP 파일 시스템이 사용됩니다.

FSx ONTAP 파일 시스템 생성, 백업 저장소로 사용할 iSCSI 볼륨 마운트, 백업 작업 생성 및 실행, VM 및 데이터베이스 복원 수행에 대해 살펴보겠습니다.

FSx ONTAP 에 대한 자세한 내용은 다음을 참조하세요. "FSx ONTAP 사용자 가이드" .

Veeam 백업 및 복제에 대한 자세한 내용은 다음을 참조하세요. "Veeam 도움말 센터 기술 문서" 대지.

AWS에서 VMware Cloud와 함께 Veeam Backup and Replication을 사용할 때의 고려 사항 및 제한 사항은 다음을

참조하세요. "AWS의 VMware Cloud 및 Dell EMC의 VMware Cloud 지원. 고려 사항 및 제한 사항" .

Veeam 프록시 서버 배포

Veeam 프록시 서버는 Veeam Backup & Replication 소프트웨어의 구성 요소로, 소스와 백업 또는 복제 대상 사이의 중개자 역할을 합니다. 프록시 서버는 로컬에서 데이터를 처리하여 백업 작업 중에 데이터 전송을 최적화하고 가속화하는 데 도움이 되며, VMware vStorage API for Data Protection을 사용하거나 직접 스토리지에 액세스하여 다양한 전송 모드를 사용하여 데이터에 액세스할 수 있습니다.

Veeam 프록시 서버 디자인을 선택할 때는 동시 작업 수와 원하는 전송 모드 또는 스토리지 액세스 유형을 고려하는 것이 중요합니다.

프록시 서버 수의 크기 조정 및 시스템 요구 사항은 다음을 참조하세요. "Veeam VMware vSphere 모범 사례 가이드" .

Veeam Data Mover는 Veeam 프록시 서버의 구성 요소이며, 소스에서 VM 데이터를 가져와 타겟으로 전송하는 방법으로 전송 모드를 활용합니다. 전송 모드는 백업 작업을 구성하는 동안 지정됩니다. NFS 데이터 저장소에서 직접 스토리지 액세스를 사용하면 백업 효율성을 높일 수 있습니다.

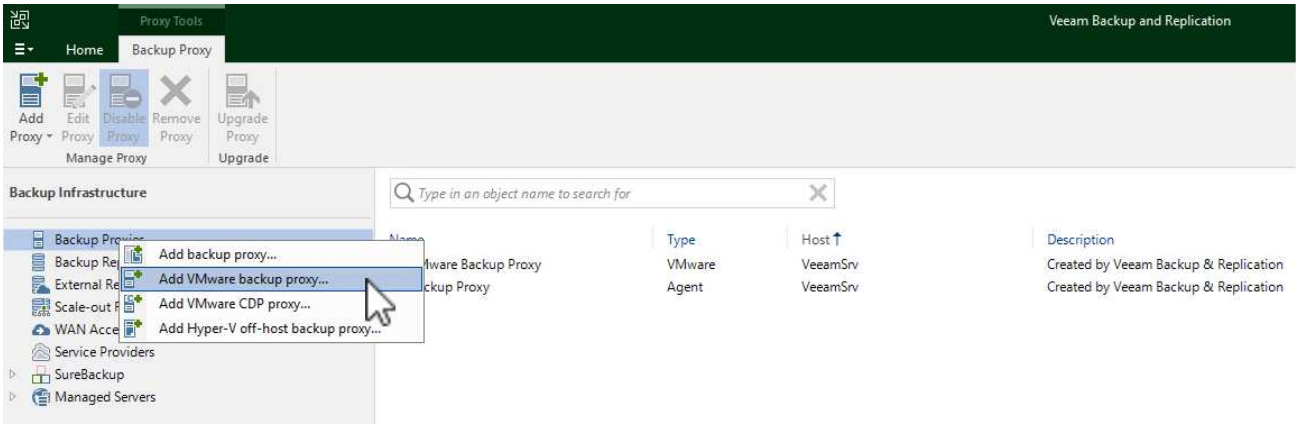
운송 모드에 대한 자세한 내용은 다음을 참조하세요. "VMware vSphere용 Veeam 백업 및 복제 사용자 가이드" .

다음 단계에서는 VMware Cloud SDDC의 Windows VM에 Veeam 프록시 서버를 배포하는 방법을 다룹니다.

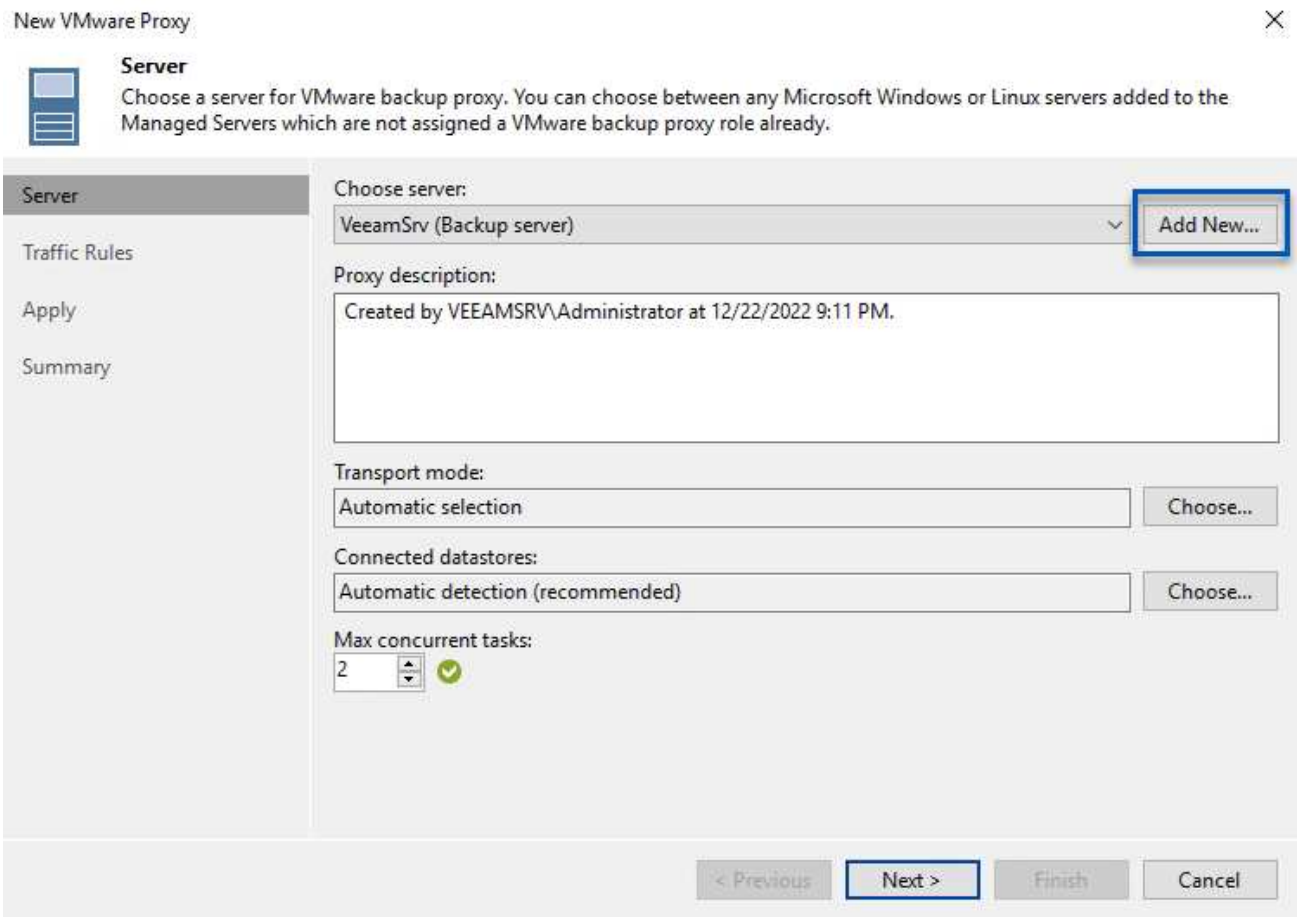
▼ 백업 워크로드를 분산하기 위해 **Veeam Proxy** 배포

이 단계에서는 Veeam 프록시가 기존 Windows VM에 배포됩니다. 이를 통해 백업 작업을 기본 Veeam 백업 서버와 Veeam 프록시 간에 분산할 수 있습니다.

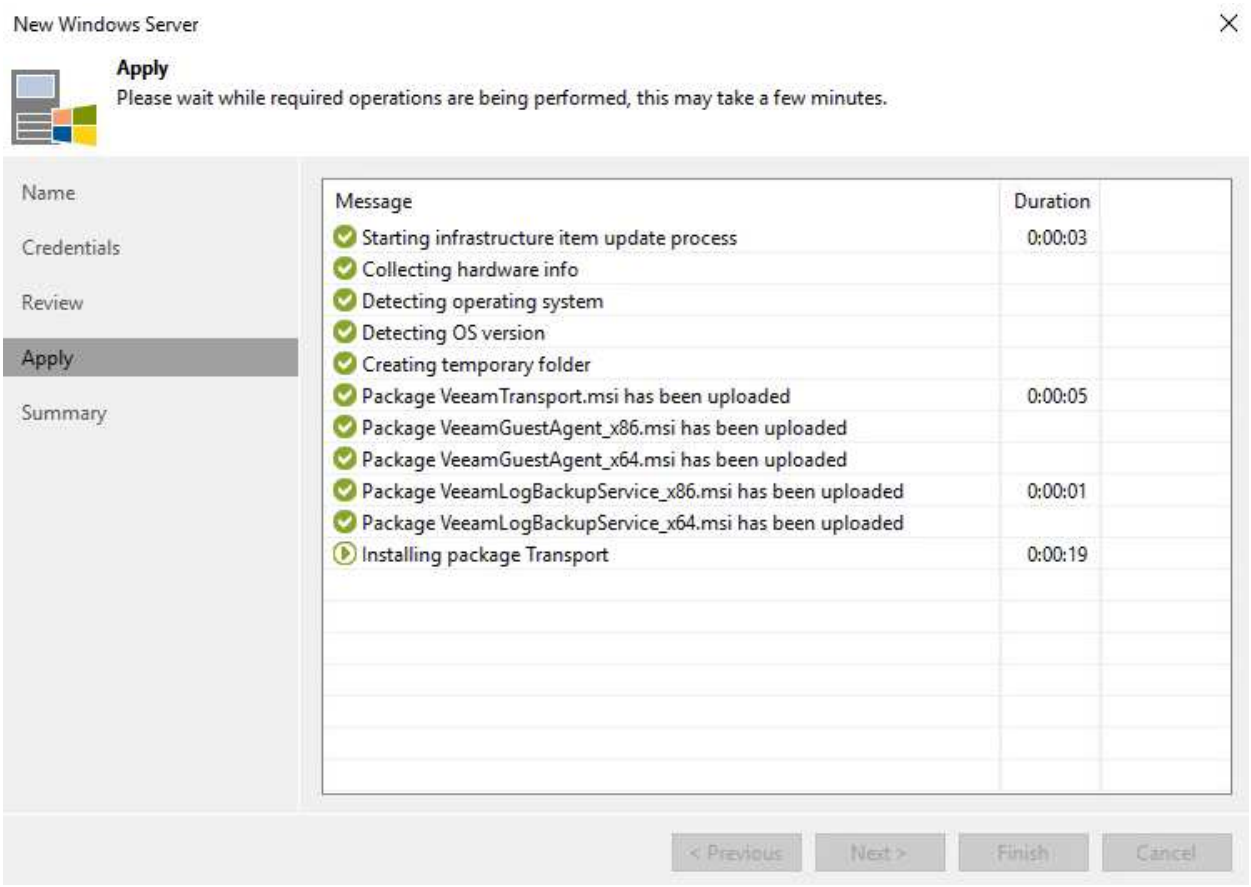
1. Veeam Backup and Replication 서버에서 관리 콘솔을 열고 왼쪽 하단 메뉴에서 *백업 인프라*를 선택합니다.
2. *백업 프록시*를 마우스 오른쪽 버튼으로 클릭하고 *VMware 백업 프록시 추가...*를 클릭하여 마법사를 엽니다.



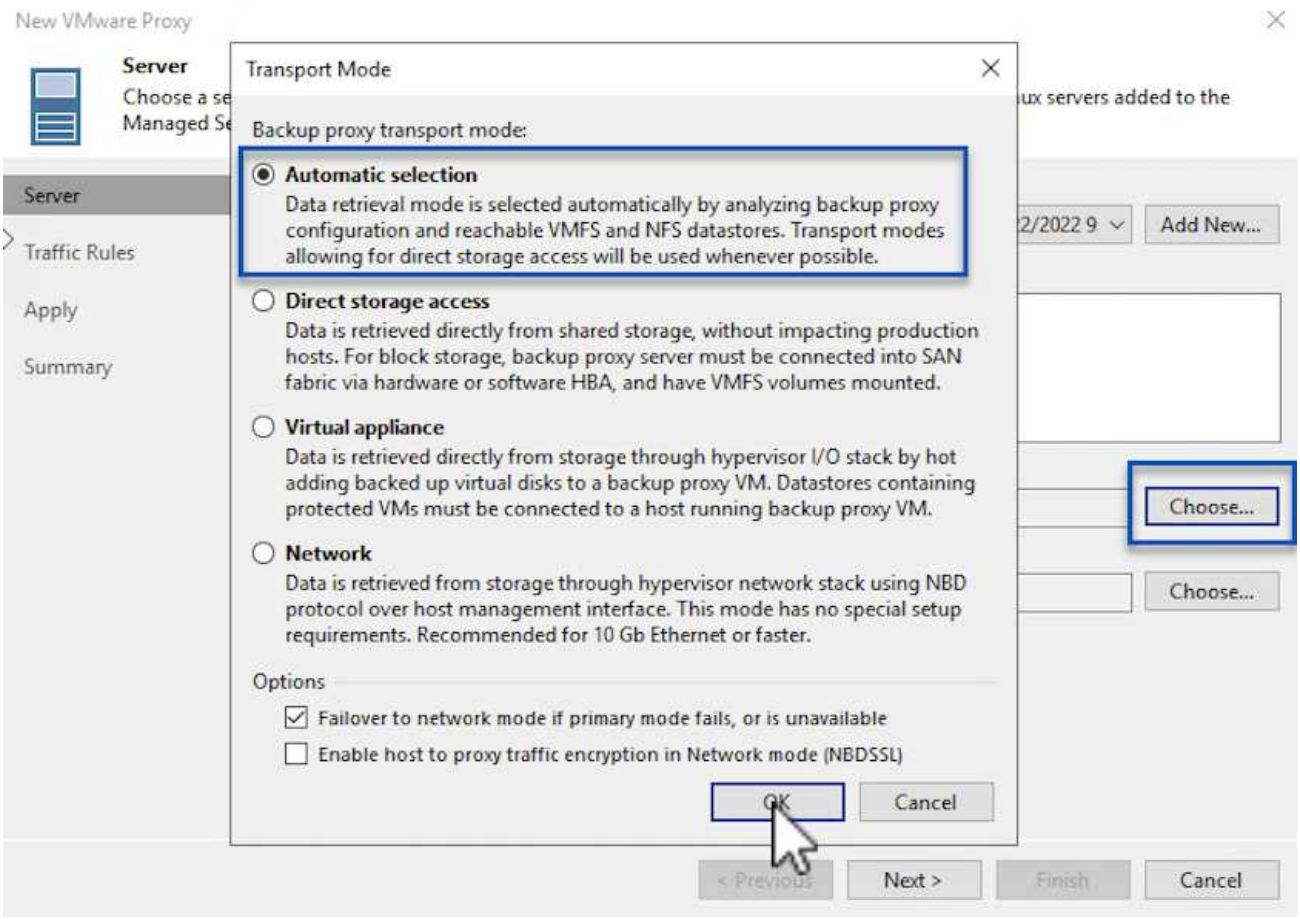
3. **VMware** 프록시 추가 마법사에서 새로 추가**...** 버튼을 클릭하여 새 프록시 서버를 추가합니다.



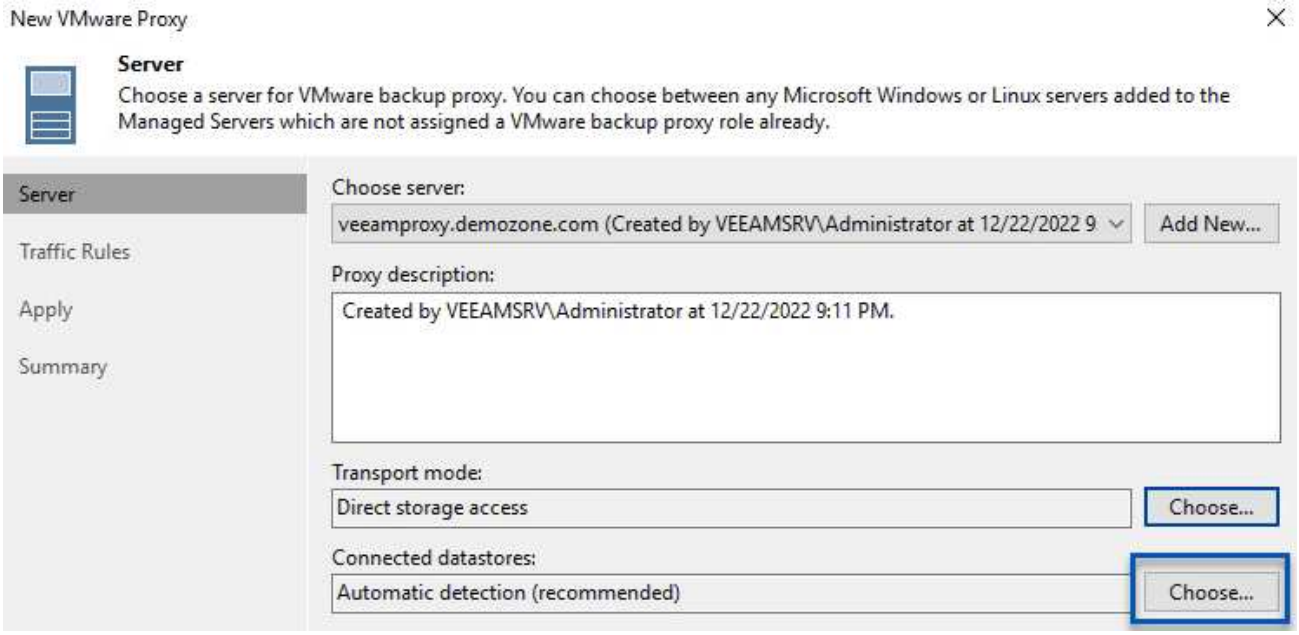
4. Microsoft Windows를 추가하도록 선택하고 메시지를 따라 서버를 추가합니다.
   - DNS 이름 또는 IP 주소를 입력하세요
   - 새 시스템의 자격 증명에 사용할 계정을 선택하거나 새 자격 증명을 추가하세요.
   - 설치할 구성 요소를 검토한 후 *적용*을 클릭하여 배포를 시작하세요.

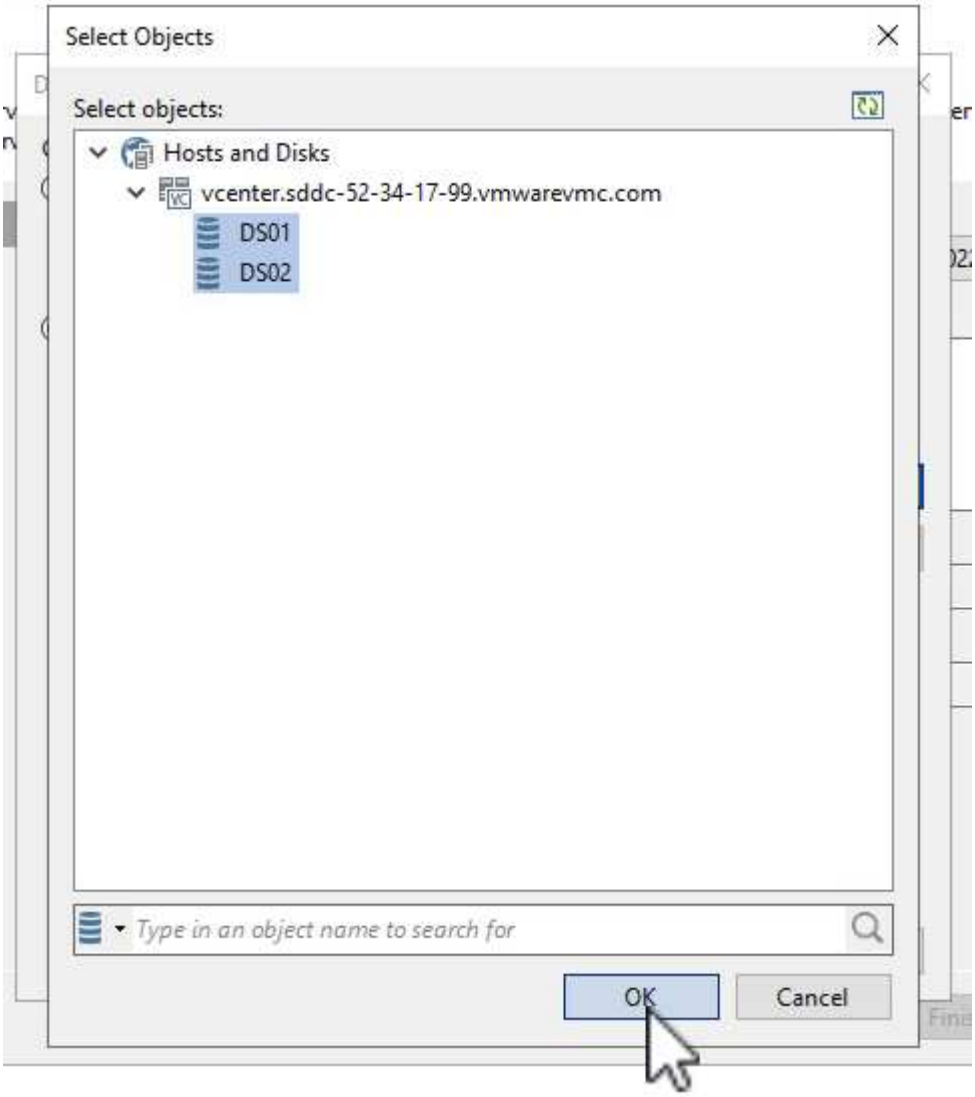


5. 새 **VMware** 프록시 마법사로 돌아가서 전송 모드를 선택합니다. 우리의 경우 *자동 선택*을 선택했습니다.

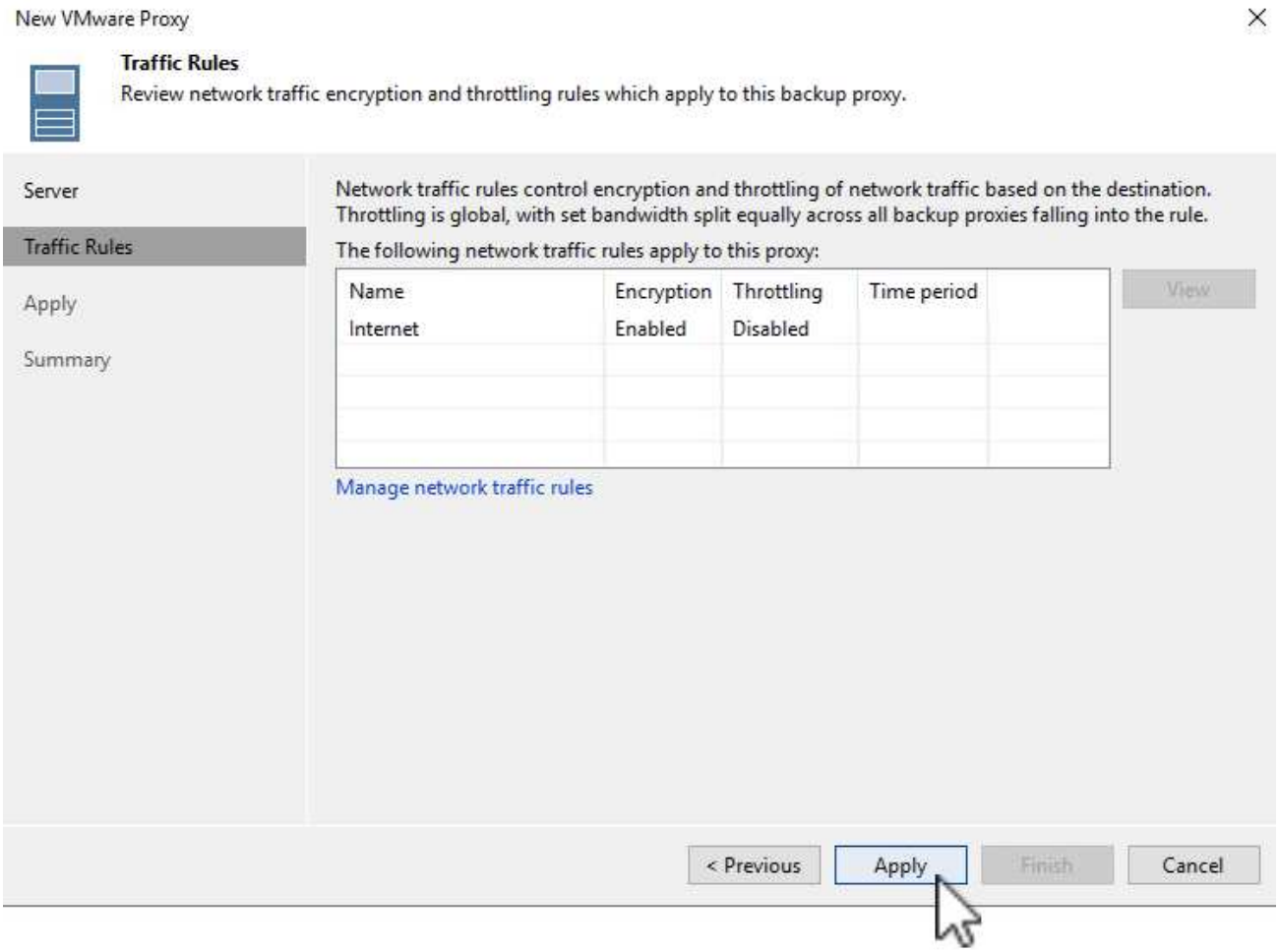


6. VMware 프록시가 직접 액세스할 수 있도록 할 연결된 데이터 저장소를 선택합니다.





7. 암호화나 제한 등 원하는 특정 네트워크 트래픽 규칙을 구성하고 적용합니다. 완료되면 적용 버튼을 클릭하여 배포를 완료하세요.



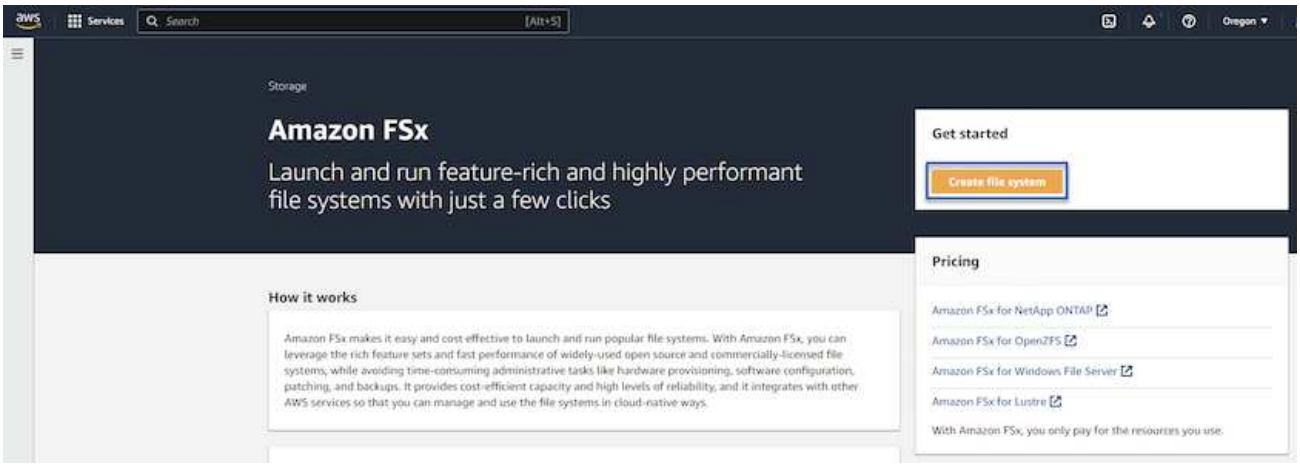
저장소 및 백업 저장소 구성

기본 Veeam 백업 서버와 Veeam 프록시 서버는 직접 연결된 스토리지 형태의 백업 저장소에 액세스할 수 있습니다. 이 섹션에서는 FSx ONTAP 파일 시스템을 만드는 방법, Veeam 서버에 iSCSI LUN을 마운트하는 방법, 백업 저장소를 만드는 방법을 다룹니다.

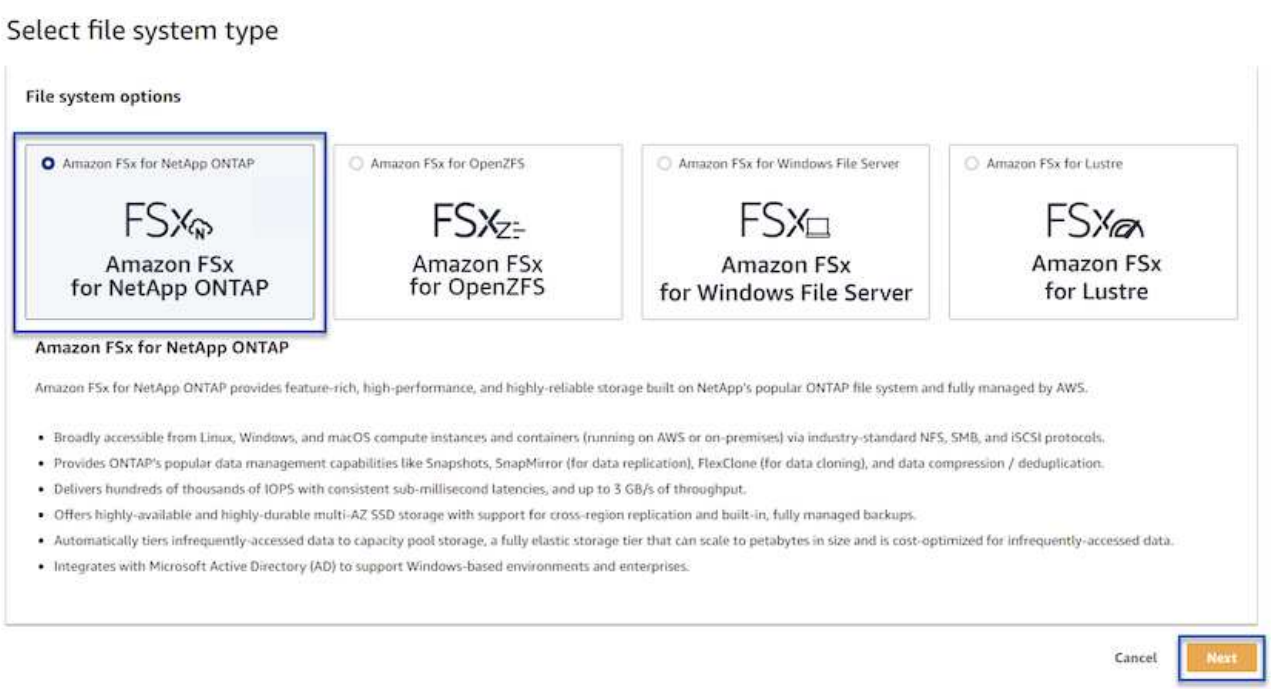
▼ **FSx ONTAP** 파일 시스템 생성

Veeam 백업 저장소의 iSCSI 볼륨을 호스팅하는 데 사용될 FSx ONTAP 파일 시스템을 만듭니다.

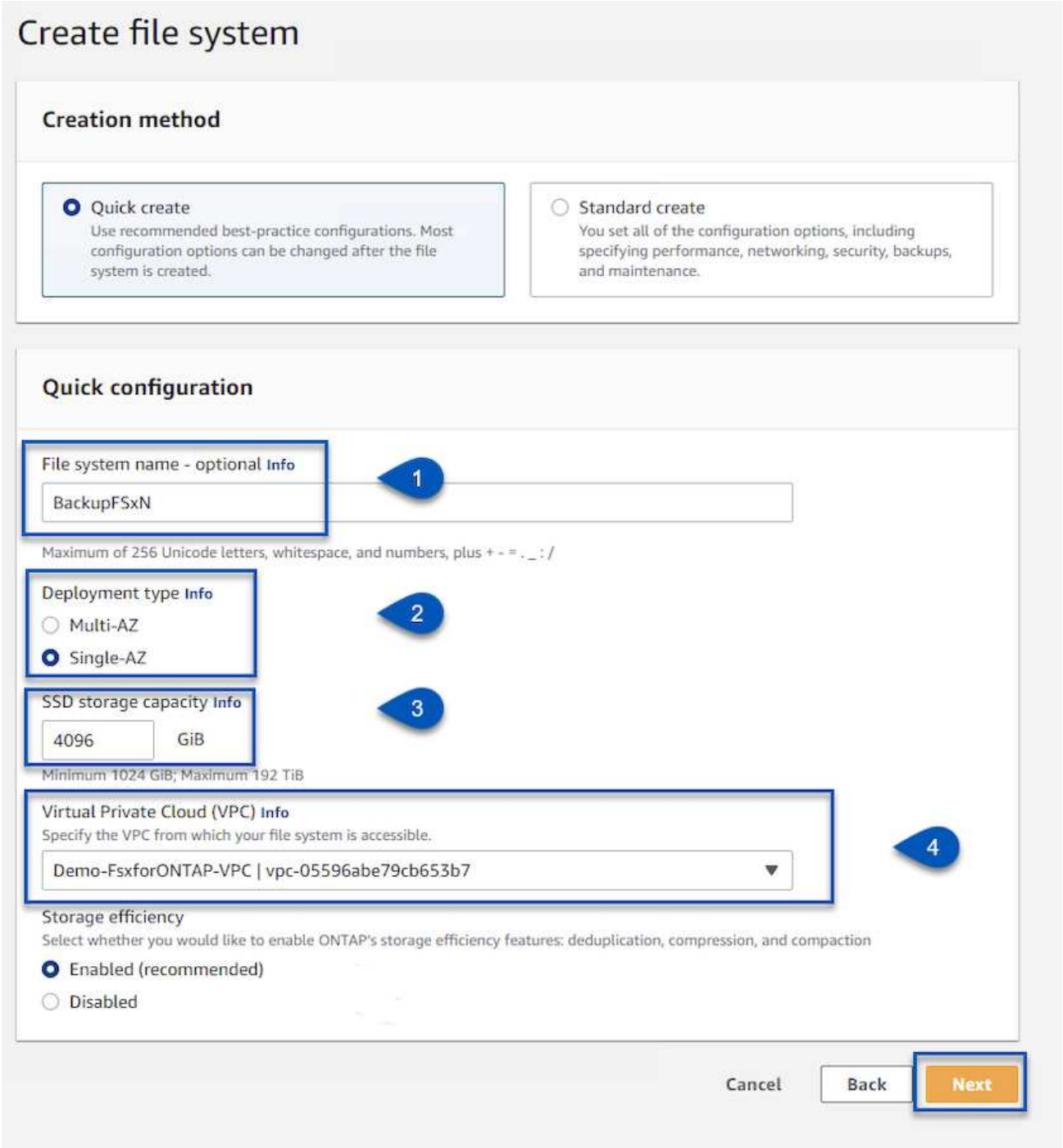
1. AWS 콘솔에서 FSx로 이동한 다음 *파일 시스템 생성*을 선택합니다.



2. 계속하려면 * Amazon FSx ONTAP*을 선택한 후 *다음*을 선택하세요.



3. FSx ONTAP 클러스터가 상주할 파일 시스템 이름, 배포 유형, SSD 스토리지 용량 및 VPC를 입력합니다. 이는 VMware Cloud의 가상 머신 네트워크와 통신하도록 구성된 VPC여야 합니다. *다음*을 클릭하세요.



4. 배포 단계를 검토하고 *파일 시스템 만들기*를 클릭하여 파일 시스템 생성 프로세스를 시작합니다.

▼ **iSCSI LUN** 구성 및 마운트

FSx ONTAP 에서 iSCSI LUN을 생성하고 구성하고 Veeam 백업 및 프록시 서버에 마운트합니다. 이러한 LUN은 나중에 Veeam 백업 저장소를 만드는 데 사용됩니다.

ⓘ FSx ONTAP 에서 iSCSI LUN을 만드는 것은 여러 단계로 구성된 프로세스입니다. 볼륨을 생성하는 첫 번째 단계는 Amazon FSx 콘솔이나 NetApp ONTAP CLI를 사용하여 수행할 수 있습니다.

ⓘ FSx ONTAP 사용에 대한 자세한 내용은 다음을 참조하세요. "FSx ONTAP 사용자 가이드" .

1. NetApp ONTAP CLI에서 다음 명령을 사용하여 초기 볼륨을 생성합니다.

```
FSx-Backup::> volume create -vserver svm_name -volume vol_name
-aggregate aggregate_name -size vol_size -type RW
```

2. 이전 단계에서 만든 볼륨을 사용하여 LUN을 만듭니다.

```
FSx-Backup::> lun create -vserver svm_name -path
/vol/vol_name/lun_name -size size -ostype windows -space-allocation
enabled
```

3. Veeam 백업 및 프록시 서버의 iSCSI IQN을 포함하는 이니시에이터 그룹을 만들어 LUN에 대한 액세스 권한을 부여합니다.

```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

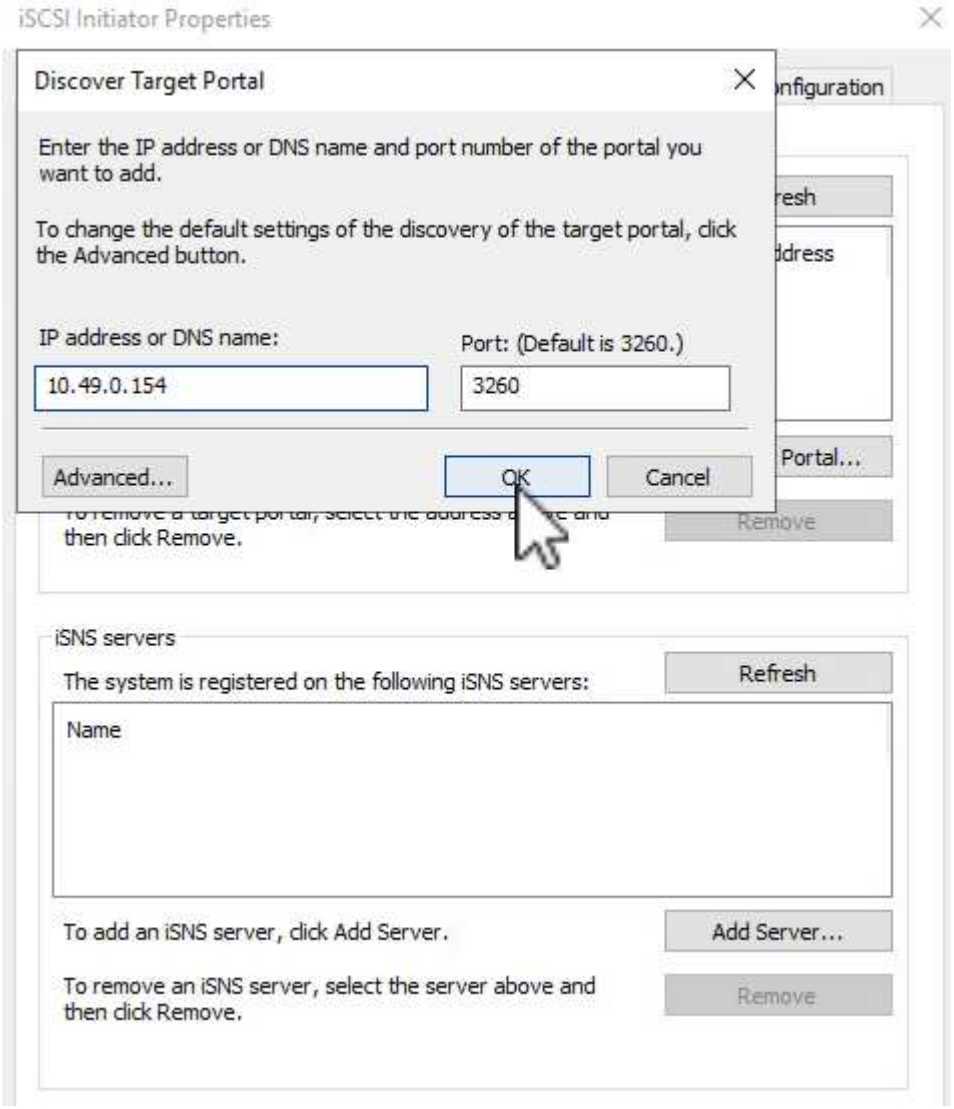


이전 단계를 완료하려면 먼저 Windows 서버의 iSCSI 이니시에이터 속성에서 IQN을 검색해야 합니다.

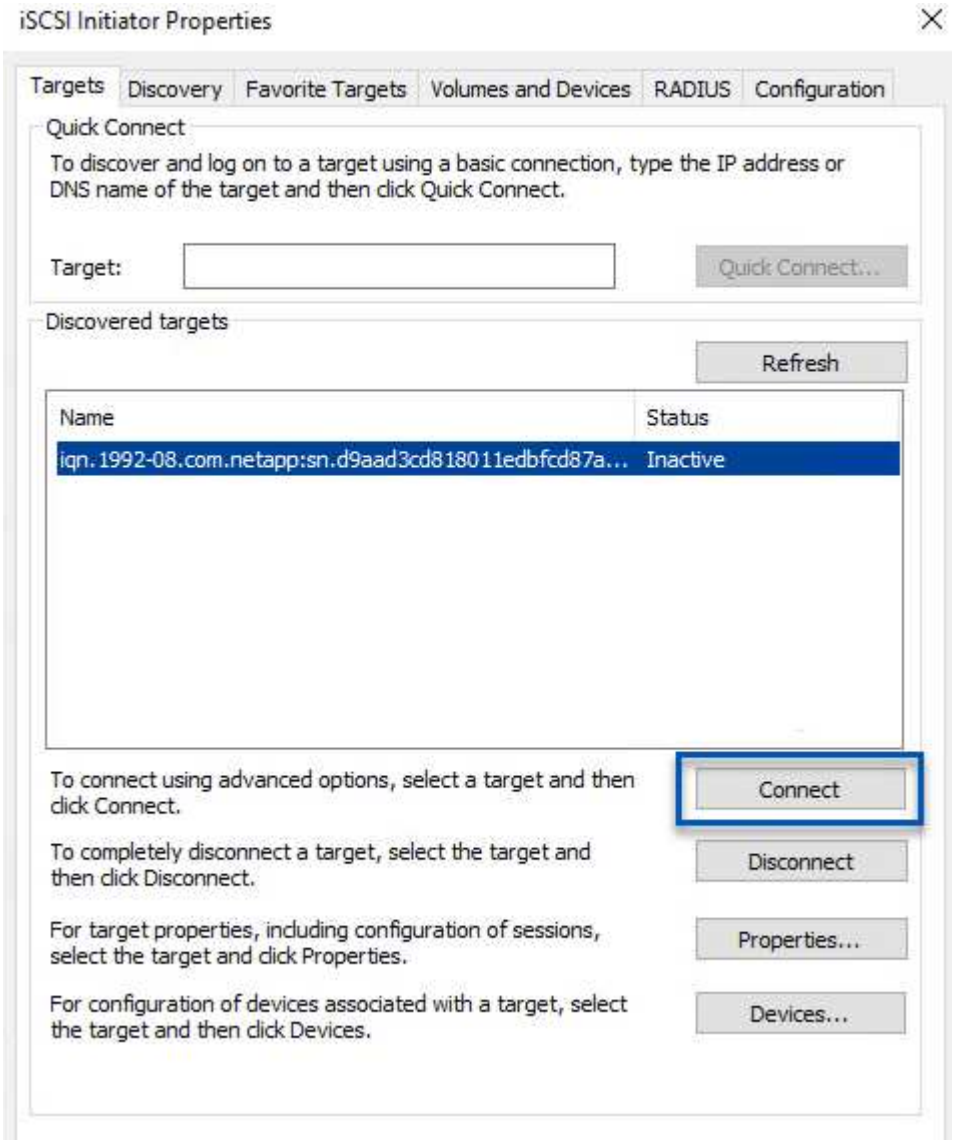
4. 마지막으로 방금 생성한 이니시에이터 그룹에 LUN을 매핑합니다.

```
FSx-Backup::> lun mapping create -vserver svm_name -path
/vol/vol_name/lun_name igroup igroup_name
```

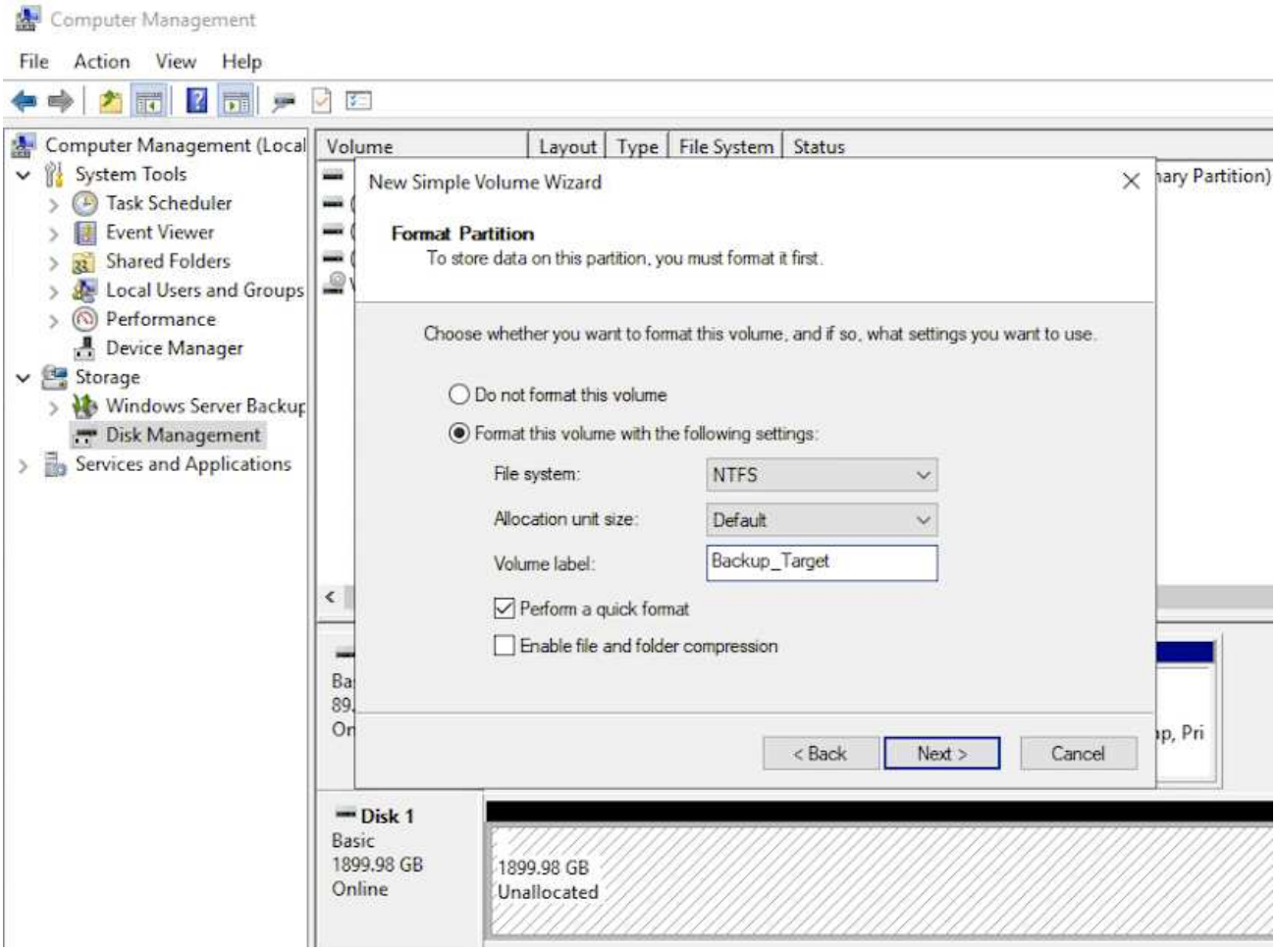
5. iSCSI LUN을 마운트하려면 Veeam Backup & Replication Server에 로그인하고 iSCSI Initiator Properties를 엽니다. 검색 탭으로 이동하여 iSCSI 대상 IP 주소를 입력합니다.



6. 대상 탭에서 비활성 LUN을 강조 표시하고 연결*을 클릭합니다. *다중 경로 사용 상자를 선택하고 *확인*을 클릭하여 LUN에 연결합니다.



7. 디스크 관리 유틸리티에서 새 LUN을 초기화하고 원하는 이름과 드라이브 문자로 볼륨을 만듭니다. 다중 경로 사용 상자를 선택하고 *확인*을 클릭하여 LUN에 연결합니다.

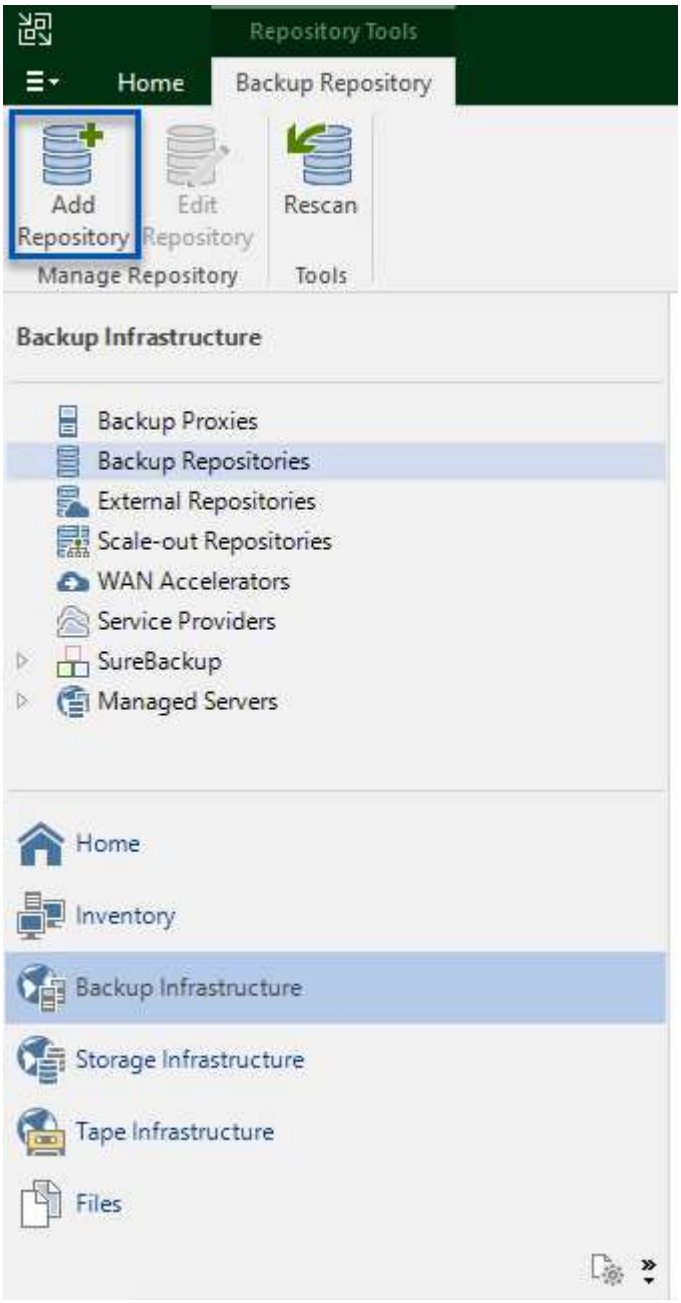


8. Veeam 프록시 서버에 iSCSI 볼륨을 마운트하려면 이 단계를 반복합니다.

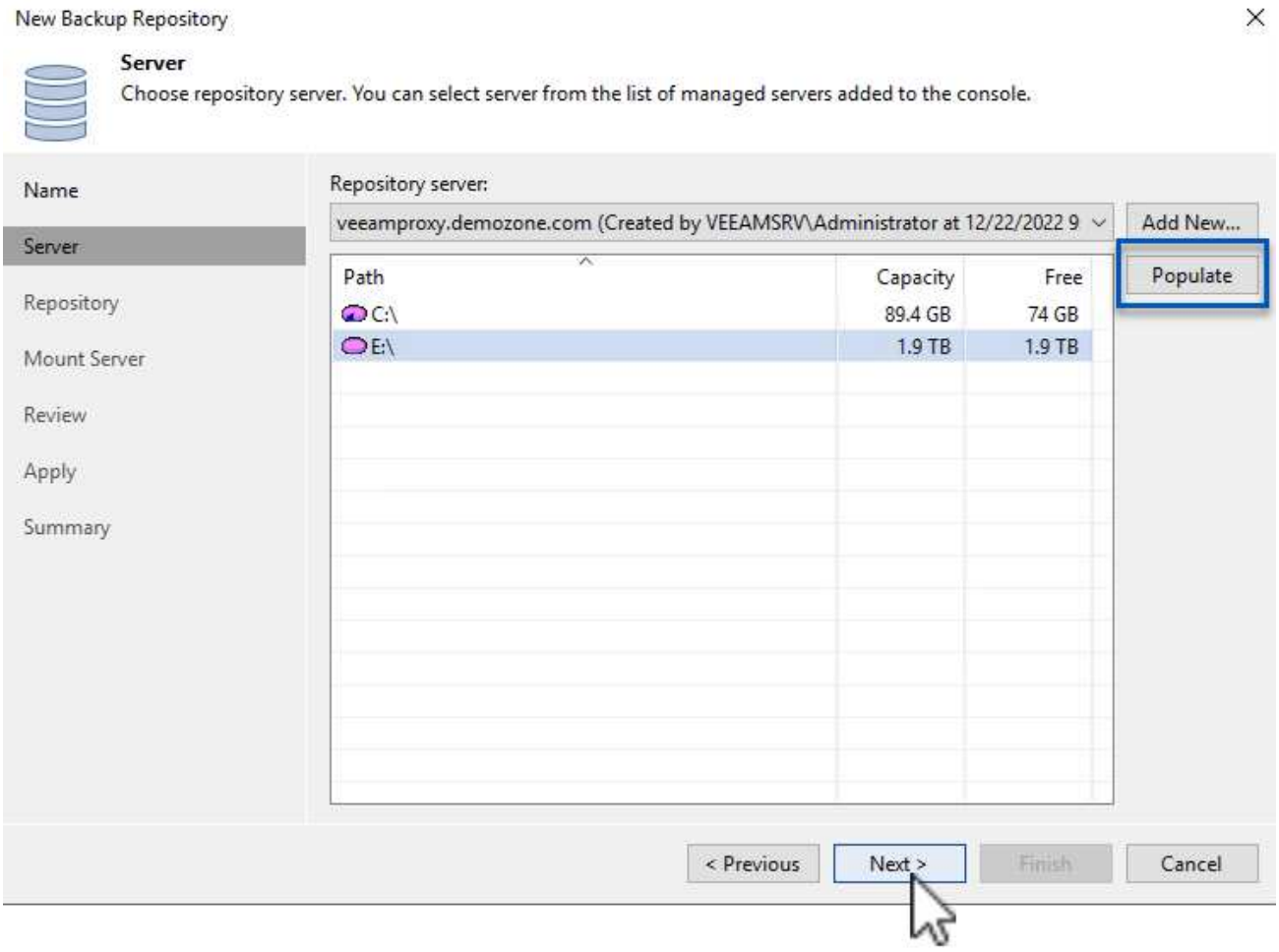
▼ **Veeam** 백업 저장소 만들기

Veeam Backup and Replication 콘솔에서 Veeam Backup 및 Veeam Proxy 서버에 대한 백업 저장소를 만듭니다. 이러한 저장소는 가상 머신 백업을 위한 백업 대상으로 사용됩니다.

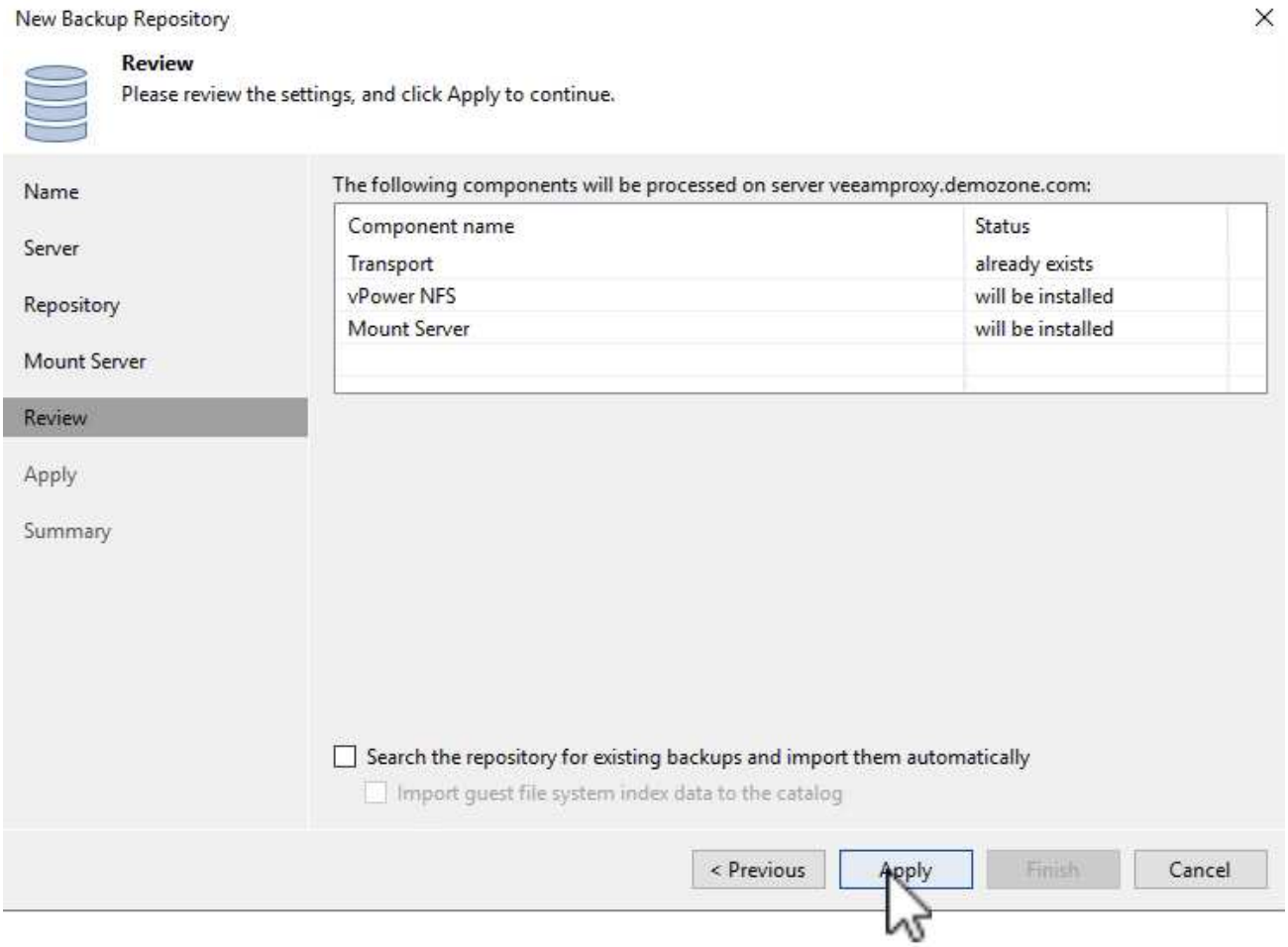
1. Veeam 백업 및 복제 콘솔에서 왼쪽 하단의 *백업 인프라*를 클릭한 다음 *저장소 추가*를 선택합니다.



2. 새 백업 저장소 마법사에서 저장소 이름을 입력한 다음 드롭다운 목록에서 서버를 선택하고 채우기 버튼을 클릭하여 사용할 NTFS 볼륨을 선택합니다.



3. 다음 페이지에서 고급 복원을 수행할 때 백업을 마운트하는 데 사용할 마운트 서버를 선택합니다. 기본적으로 이는 저장소 저장소가 연결된 서버와 동일합니다.
4. 선택 사항을 검토하고 *적용*을 클릭하여 백업 저장소 생성을 시작하세요.



5. 추가 프록시 서버에 대해 이 단계를 반복합니다.

Veeam 백업 작업 구성

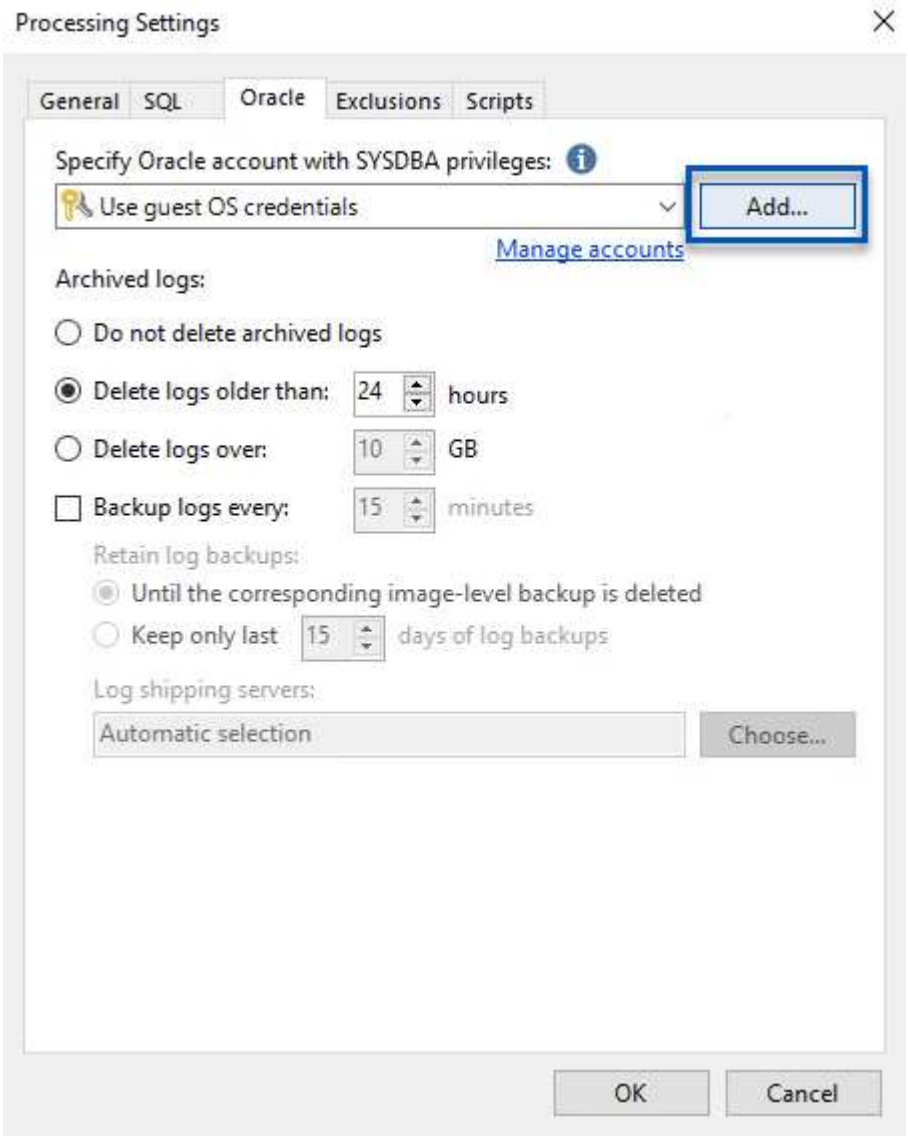
백업 작업은 이전 섹션의 백업 저장소를 활용하여 만들어야 합니다. 백업 작업을 만드는 것은 모든 스토리지 관리자의 일반적인 업무이며, 여기서는 모든 단계를 다루지 않습니다. Veeam에서 백업 작업을 만드는 방법에 대한 자세한 내용은 다음을 참조하세요. "Veeam 도움말 센터 기술 문서" .

이 솔루션에서는 다음에 대한 별도의 백업 작업이 생성되었습니다.

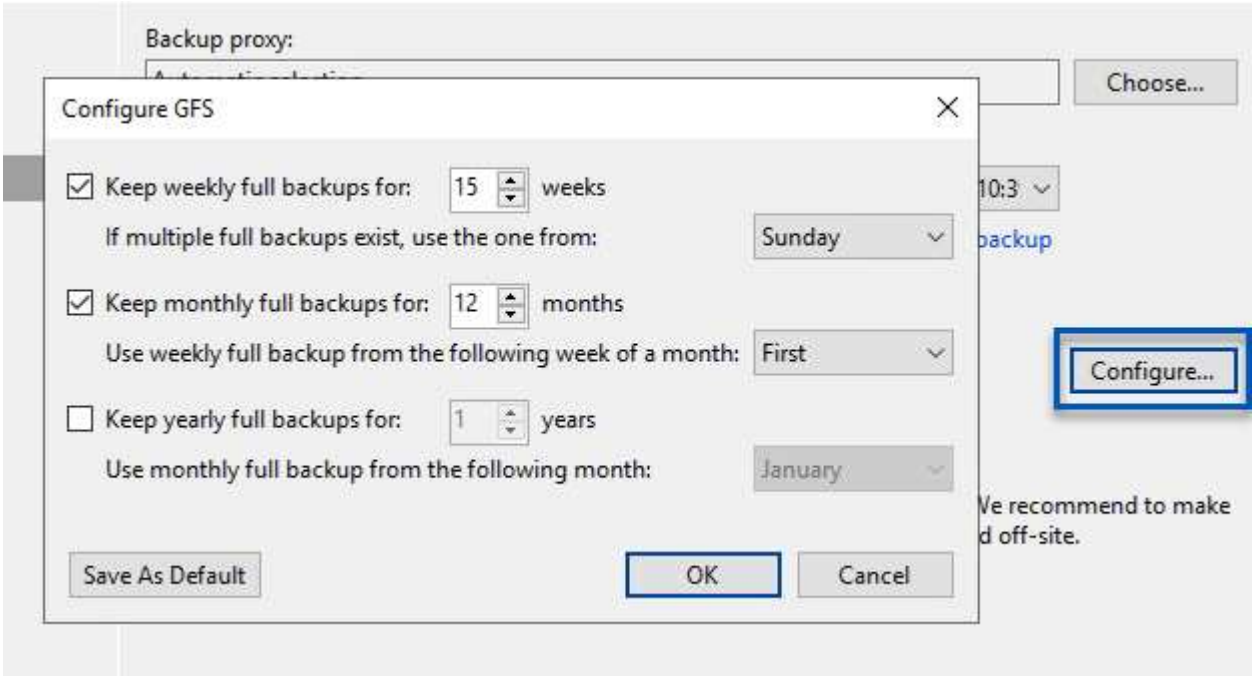
- Microsoft Windows SQL 서버
- Oracle 데이터베이스 서버
- Windows 파일 서버
- 리눅스 파일 서버

▼ **Veeam** 백업 작업 구성 시 일반적인 고려 사항

1. 애플리케이션 인식 처리를 활성화하여 일관된 백업을 만들고 트랜잭션 로그 처리를 수행합니다.
2. 애플리케이션 인식 처리를 활성화한 후, 게스트 OS 자격 증명과 다를 수 있으므로 애플리케이션에 관리자 권한이 있는 올바른 자격 증명을 추가합니다.



3. 백업에 대한 보존 정책을 관리하려면 보관 목적으로 특정 전체 백업을 더 오래 보관*을 선택하고 *구성... 버튼을 클릭하여 정책을 구성합니다.



Veeam 전체 복원을 사용하여 애플리케이션 **VM** 복원

Veeam을 사용하여 전체 복원을 수행하는 것은 애플리케이션 복원을 수행하는 첫 번째 단계입니다. 전원이 켜진 VM이 완전히 복원되었고 모든 서비스가 정상적으로 실행되고 있는지 검증했습니다.

서버 복구는 모든 스토리지 관리자의 일상적인 업무이며, 여기서는 모든 단계를 다루지 않습니다. Veeam에서 전체 복원을 수행하는 것에 대한 보다 자세한 정보는 다음을 참조하세요. "Veeam 도움말 센터 기술 문서" .

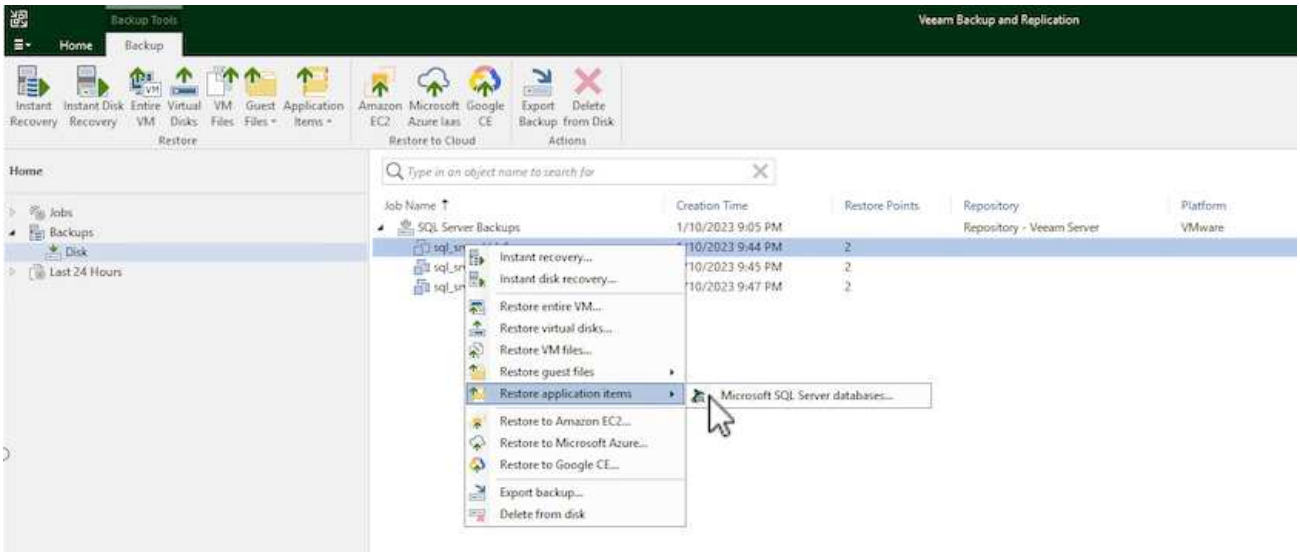
SQL Server 데이터베이스 복원

Veeam Backup & Replication은 SQL Server 데이터베이스를 복원하기 위한 여러 가지 옵션을 제공합니다. 이 검증을 위해 Instant Recovery가 포함된 Veeam Explorer for SQL Server를 사용하여 SQL Server 데이터베이스를 복원했습니다. SQL Server 즉시 복구는 전체 데이터베이스 복원을 기다리지 않고도 SQL Server 데이터베이스를 빠르게 복원할 수 있는 기능입니다. 이러한 신속한 복구 프로세스는 가동 중지 시간을 최소화하고 비즈니스 연속성을 보장합니다. 작동 원리는 다음과 같습니다.

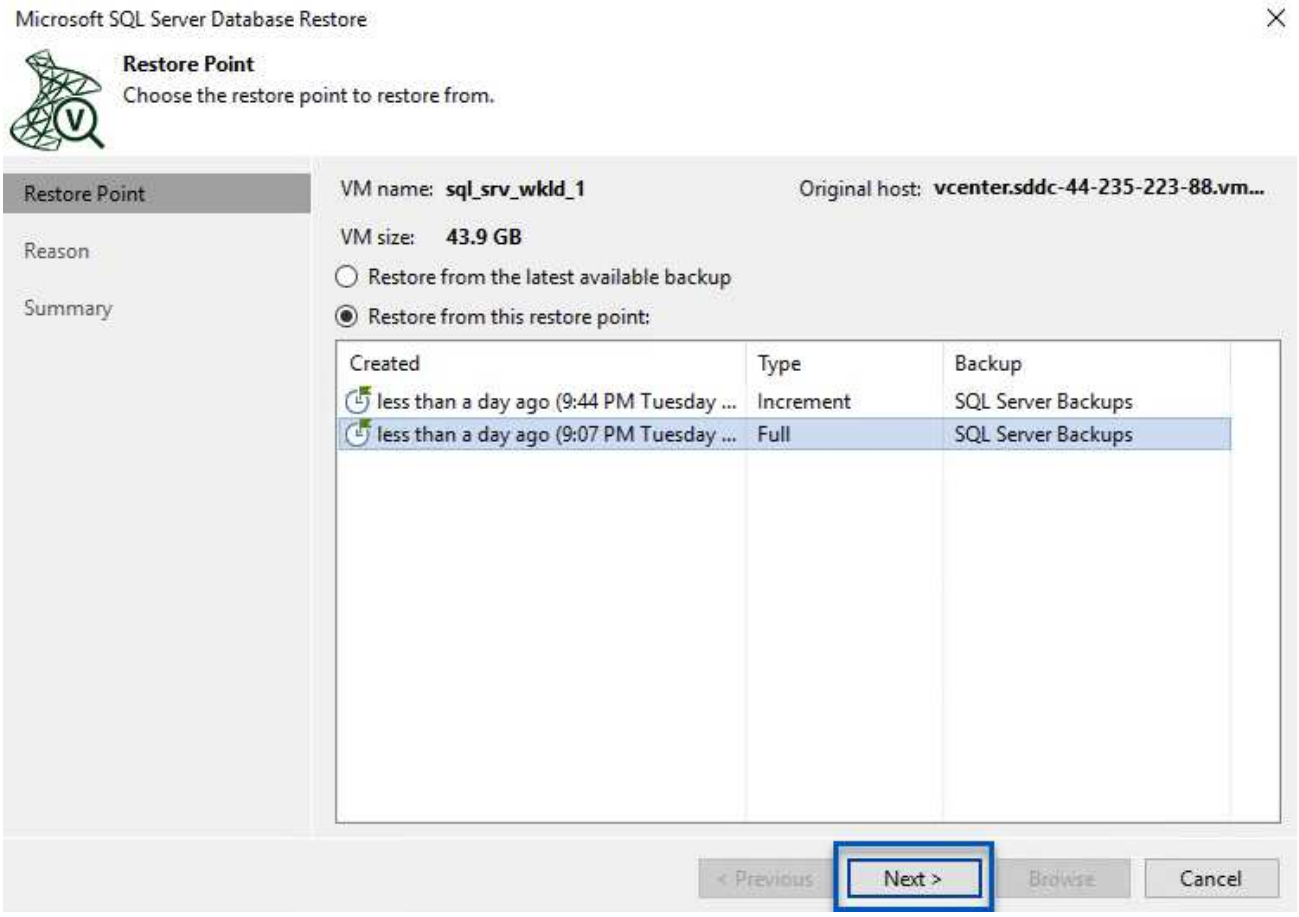
- Veeam Explorer는 복원할 SQL Server 데이터베이스가 포함된 백업을 마운트합니다.
- 이 소프트웨어는 마운트된 파일에서 직접 *데이터베이스를 게시*하여 대상 SQL Server 인스턴스에서 임시 데이터베이스로 액세스할 수 있도록 합니다.
- 임시 데이터베이스가 사용 중인 동안 Veeam Explorer는 *사용자 쿼리를 이 데이터베이스로 리디렉션*하여 사용자가 계속해서 데이터에 액세스하고 작업할 수 있도록 보장합니다.
- 백그라운드에서 Veeam은 *전체 데이터베이스 복원을 수행*하여 임시 데이터베이스에서 원래 데이터베이스 위치로 데이터를 전송합니다.
- 전체 데이터베이스 복원이 완료되면 Veeam Explorer는 *사용자 쿼리를 원래 데이터베이스로 다시 전환*하고 임시 데이터베이스를 제거합니다.

▼ **Veeam Explorer Instant Recovery**를 사용하여 **SQL Server** 데이터베이스 복원

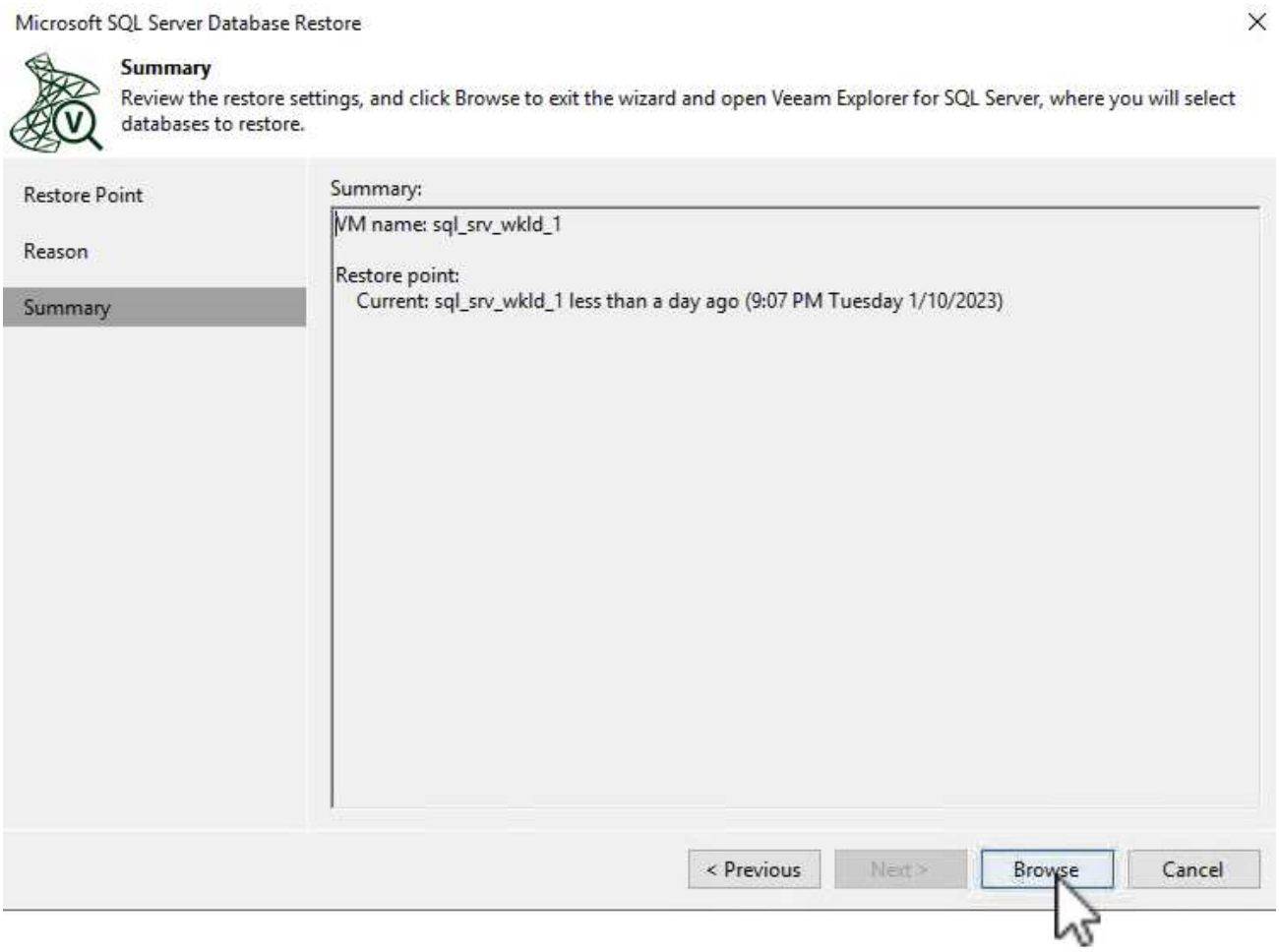
1. Veeam Backup and Replication 콘솔에서 SQL Server 백업 목록으로 이동한 다음 서버를 마우스 오른쪽 버튼으로 클릭하고 *애플리케이션 항목 복원*을 선택한 다음 *Microsoft SQL Server 데이터베이스…*를 선택합니다.



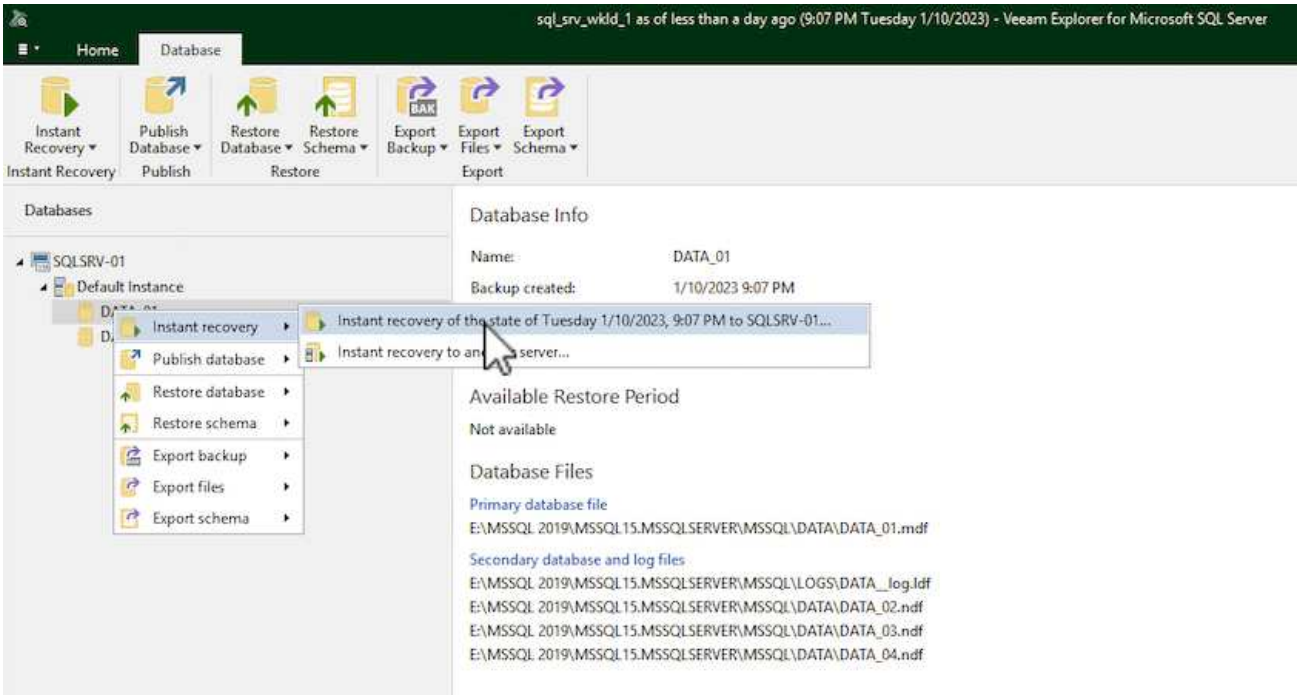
2. Microsoft SQL Server 데이터베이스 복원 마법사에서 목록에서 복원 지점을 선택하고 *다음*을 클릭합니다.



3. 원하는 경우 복원 이유*를 입력한 다음 요약 페이지에서 *찾아보기 버튼을 클릭하여 Microsoft SQL Server용 Veeam Explorer를 시작합니다.

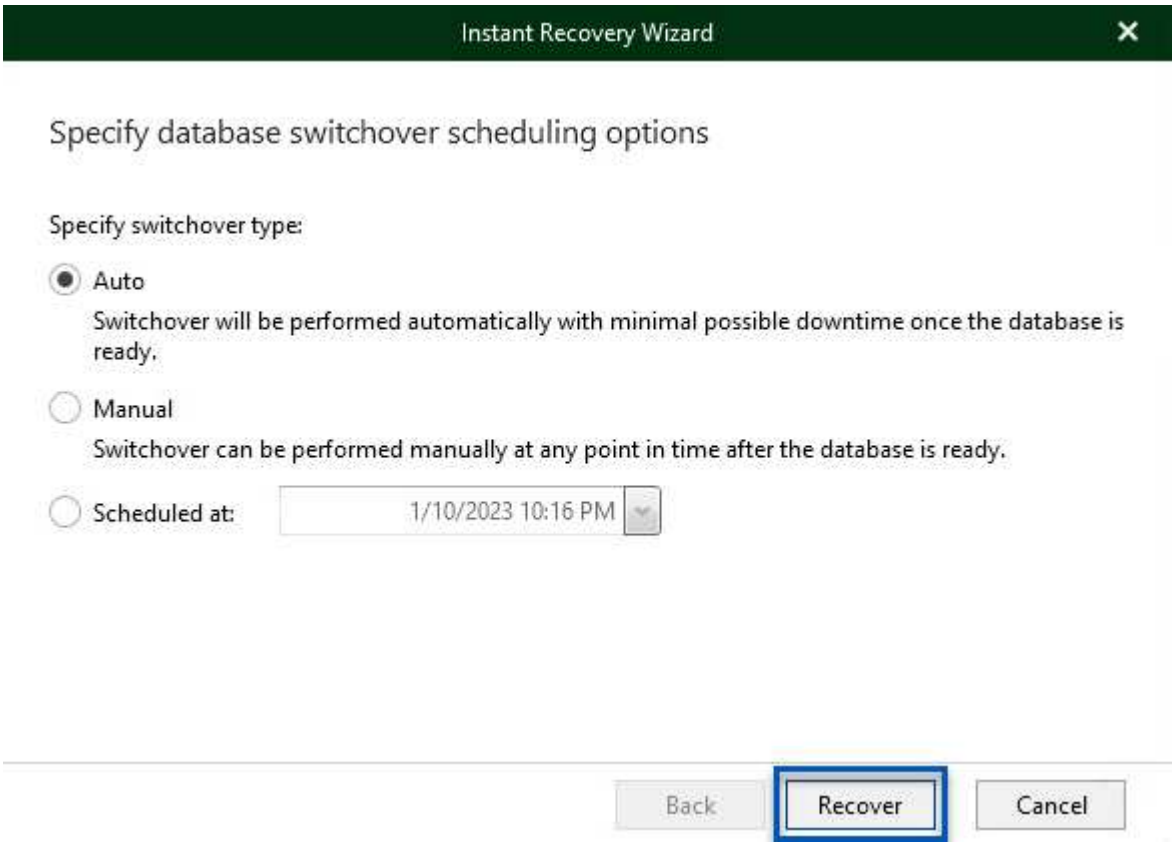


4. Veeam Explorer에서 데이터베이스 인스턴스 목록을 확장하고 마우스 오른쪽 버튼을 클릭하여 *즉시 복구*를 선택한 다음 복구할 특정 복원 지점을 선택합니다.

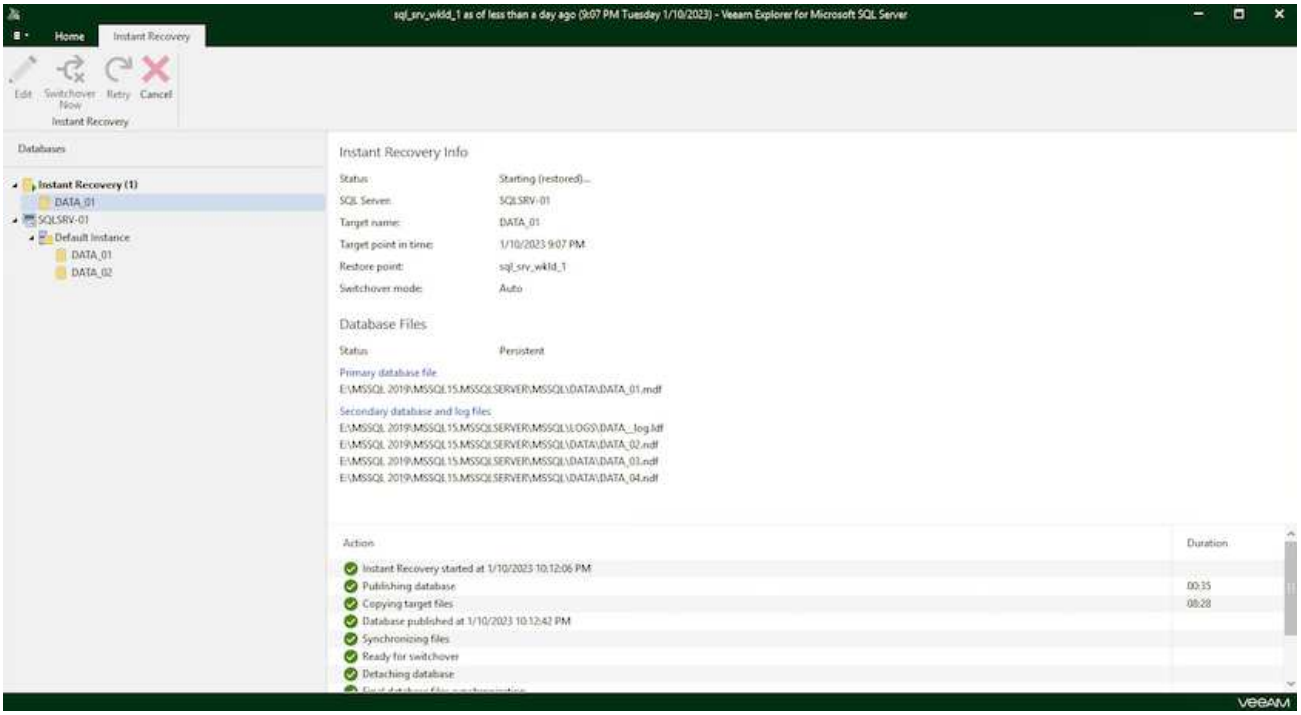


5. 즉시 복구 마법사에서 전환 유형을 지정합니다. 이 작업은 최소한의 가동 중지 시간으로 자동으로 수행될 수도

있고, 수동으로 수행될 수도 있으며, 지정된 시간에 수행될 수도 있습니다. 그런 다음 복구 버튼을 클릭하여 복구 프로세스를 시작하세요.



6. 복구 프로세스는 Veeam Explorer에서 모니터링할 수 있습니다.



Veeam Explorer를 사용하여 SQL Server 복원 작업을 수행하는 방법에 대한 자세한 내용은 Microsoft SQL Server 섹션을 참조하세요. "Veeam Explorers 사용자 가이드" .

Veeam Explorer를 사용하여 **Oracle** 데이터베이스 복원

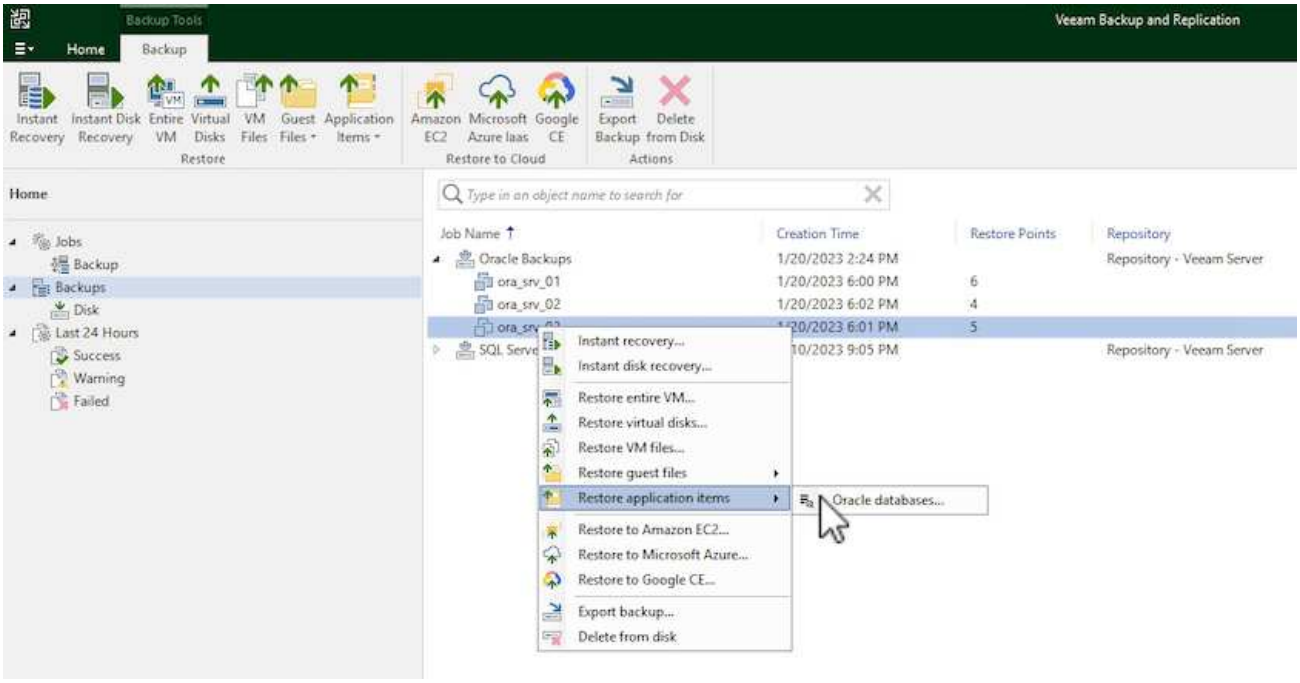
Oracle 데이터베이스용 Veeam Explorer는 표준 Oracle 데이터베이스 복원을 수행하거나 Instant Recovery를 사용하여 중단 없는 복원을 수행하는 기능을 제공합니다. 또한 빠른 액세스를 위한 데이터베이스 게시, Data Guard 데이터베이스 복구 및 RMAN 백업에서의 복원도 지원합니다.

Veeam Explorer를 사용하여 Oracle 데이터베이스 복원 작업을 수행하는 방법에 대한 자세한 내용은 Oracle 섹션을 참조하세요. "Veeam Explorers 사용자 가이드" .

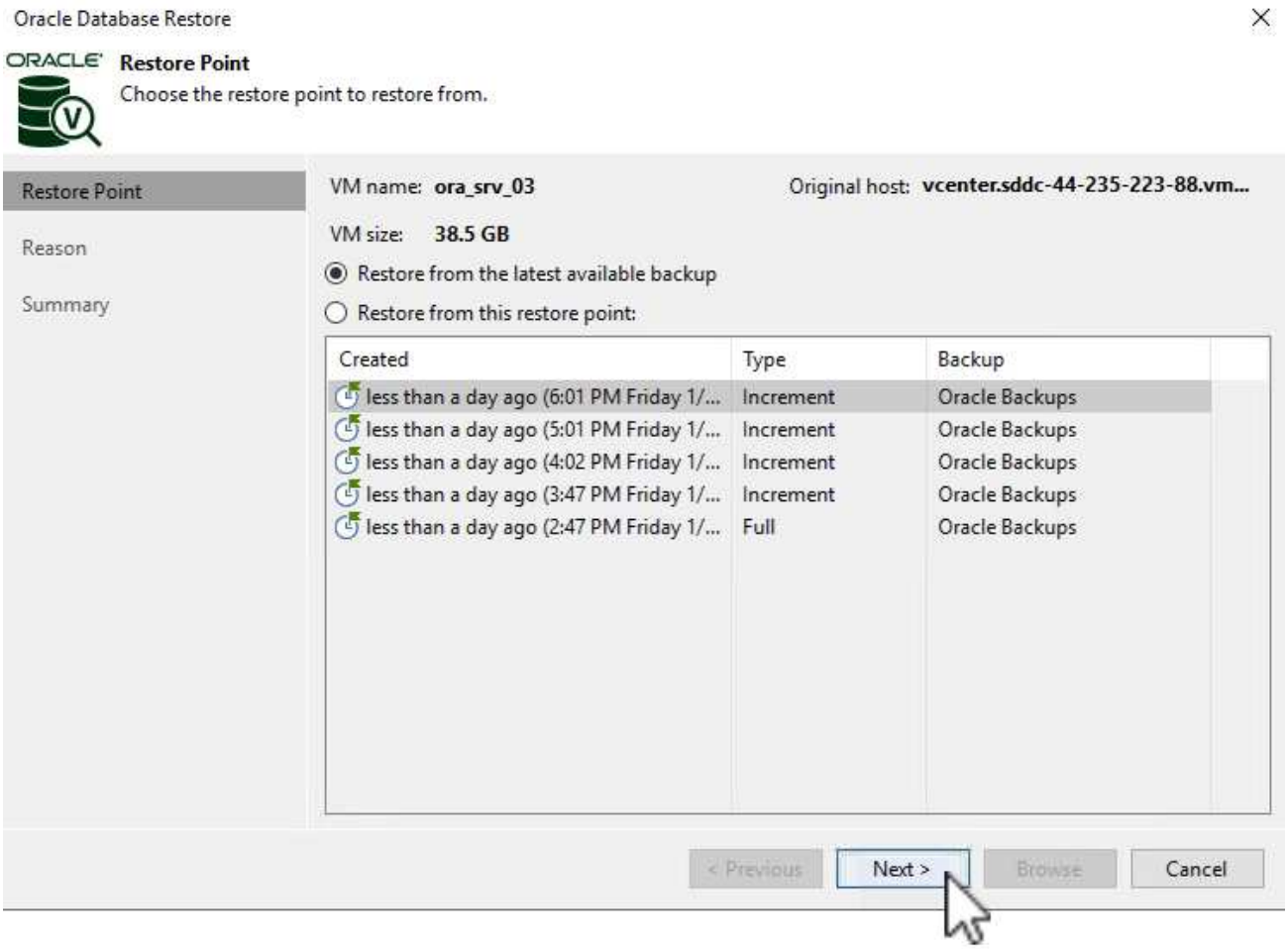
▼ **Veeam Explorer**를 사용하여 **Oracle** 데이터베이스 복원

이 섹션에서는 Veeam Explorer를 사용하여 Oracle 데이터베이스를 다른 서버로 복원하는 방법을 설명합니다.

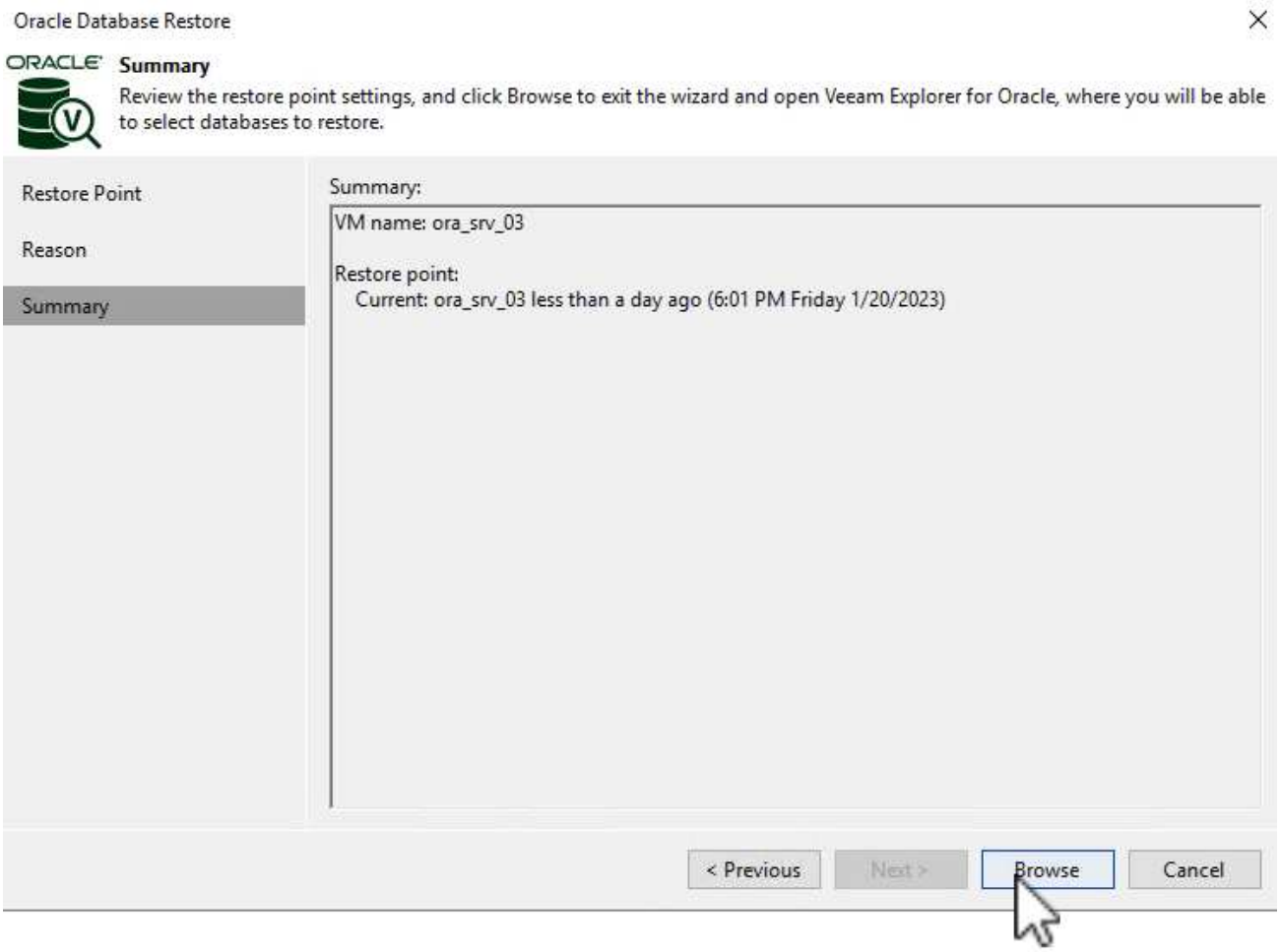
1. Veeam Backup and Replication 콘솔에서 Oracle 백업 목록으로 이동한 다음 서버를 마우스 오른쪽 버튼으로 클릭하고 *애플리케이션 항목 복원*을 선택한 다음 *Oracle 데이터베이스...*를 선택합니다.



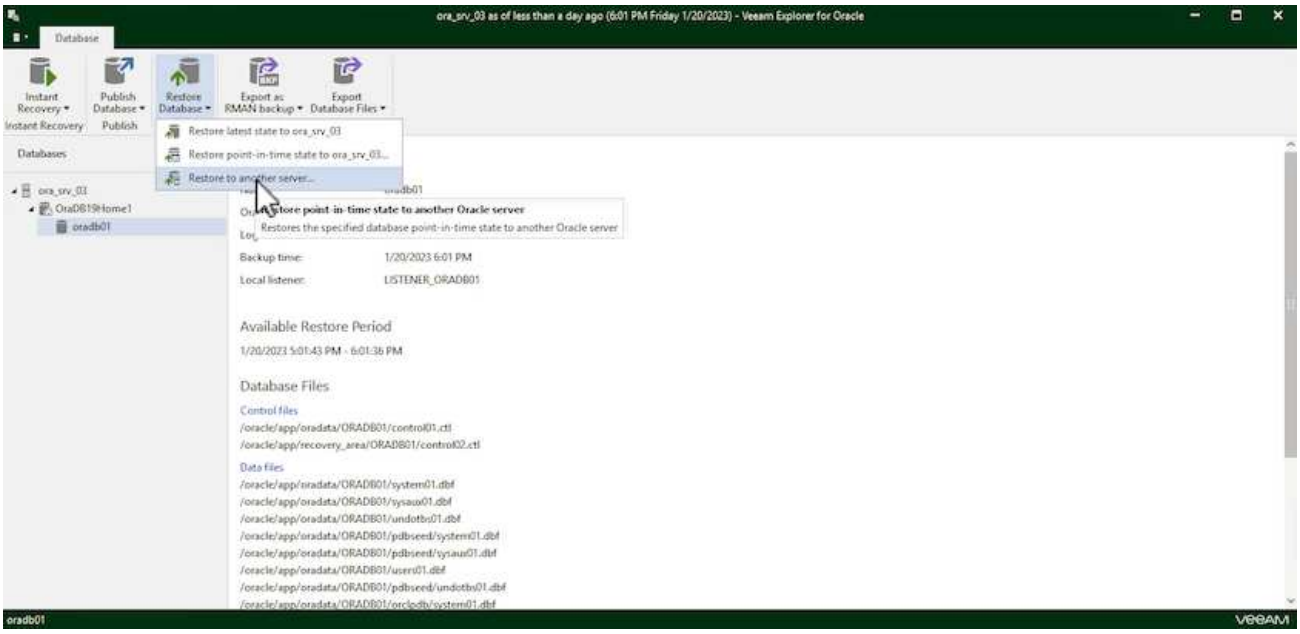
2. Oracle 데이터베이스 복원 마법사에서 목록에서 복원 지점을 선택하고 *다음*을 클릭합니다.



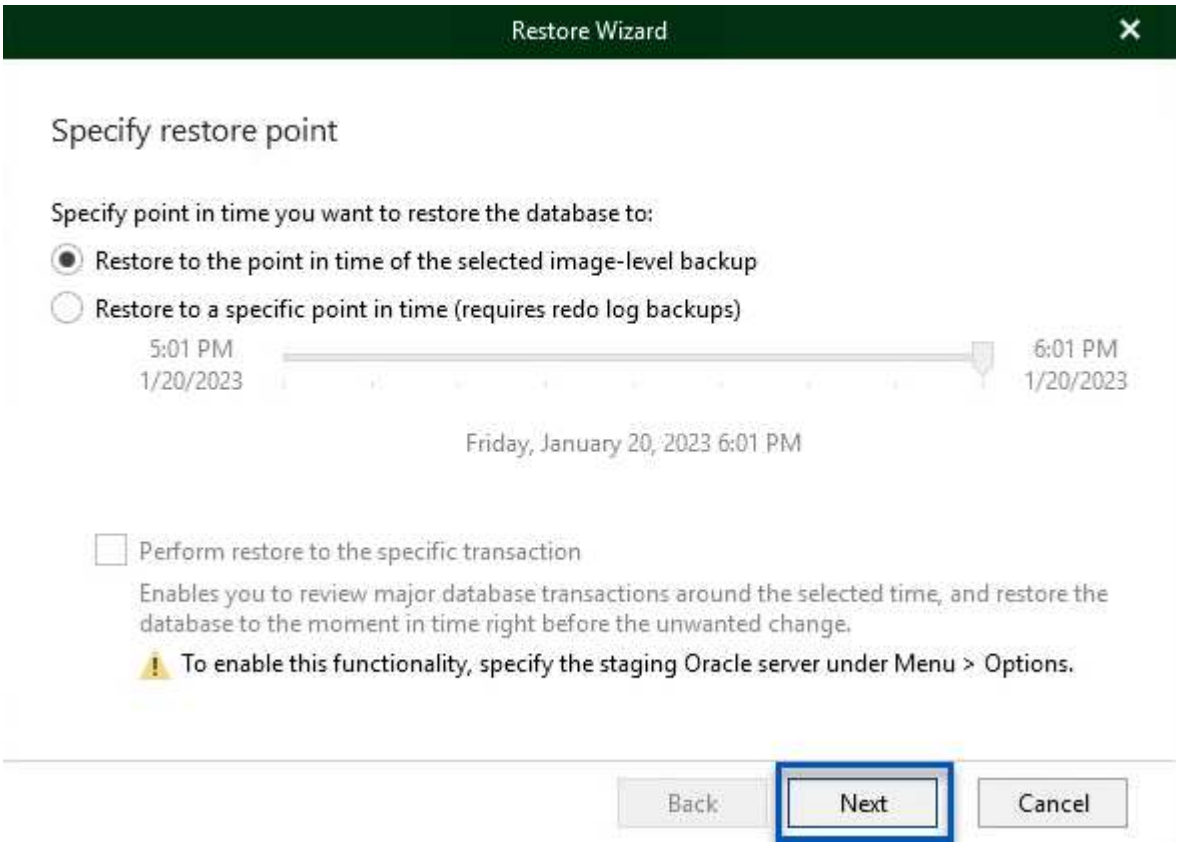
3. 원하는 경우 복원 이유*를 입력한 다음 요약 페이지에서 *찾아보기 버튼을 클릭하여 Oracle용 Veeam Explorer를 시작합니다.



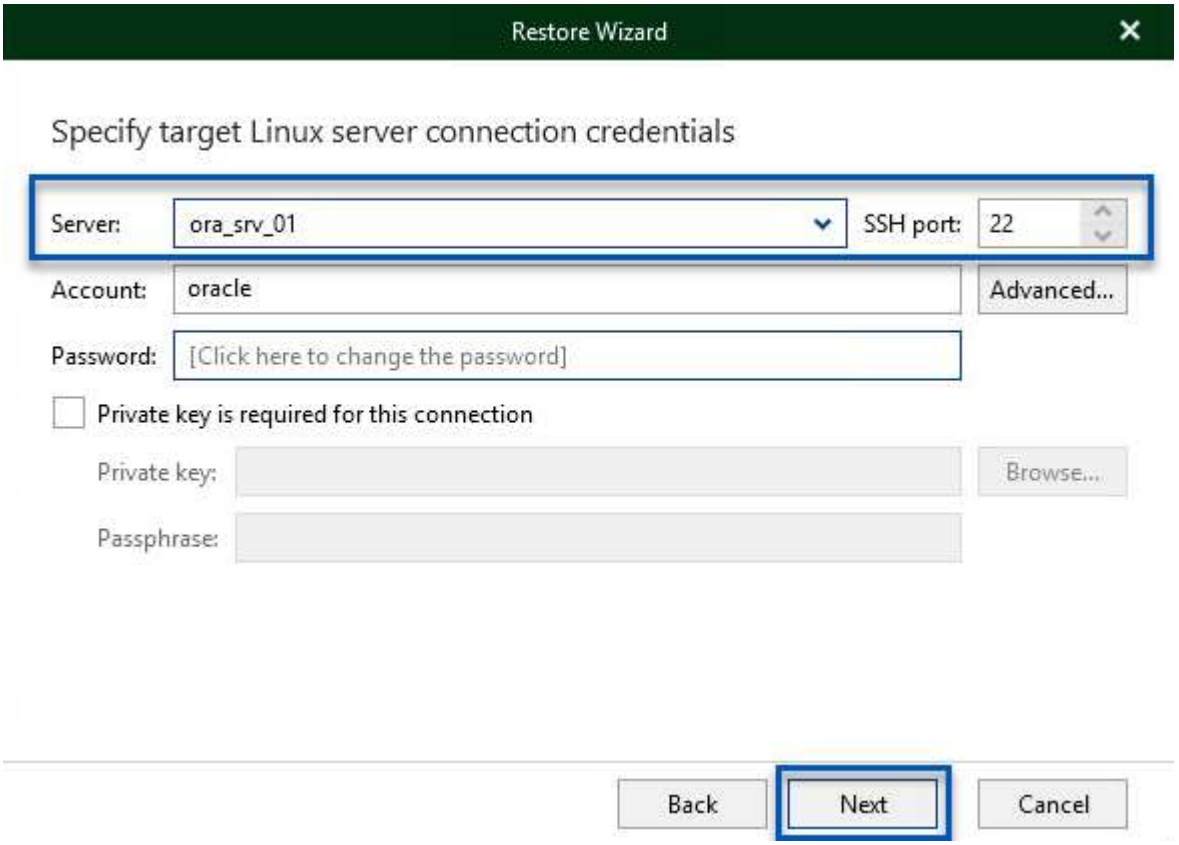
4. Veeam Explorer에서 데이터베이스 인스턴스 목록을 확장하고 복원할 데이터베이스를 클릭한 다음 상단의 데이터베이스 복원 드롭다운 메뉴에서 *다른 서버로 복원...*을 선택합니다.



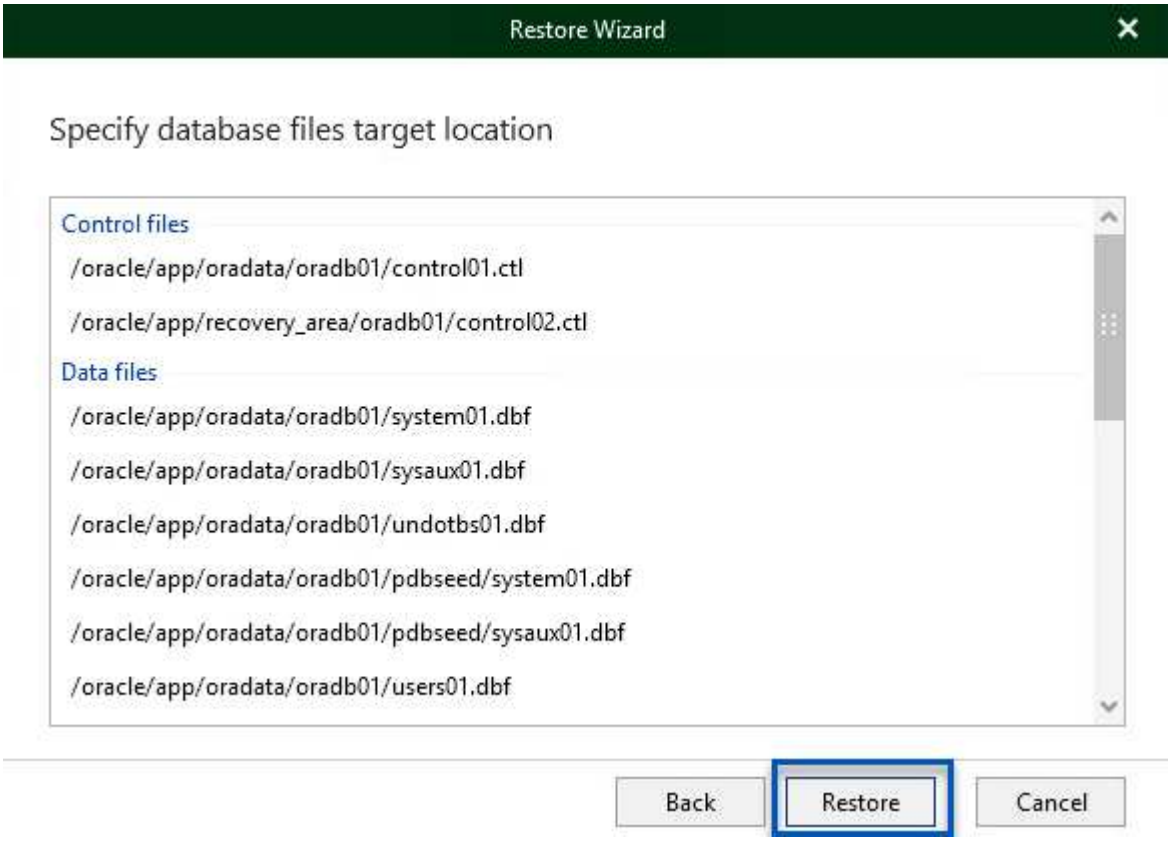
5. 복원 마법사에서 복원할 복원 지점을 지정하고 *다음*을 클릭합니다.



6. 데이터베이스가 복원될 대상 서버와 계정 자격 증명을 지정하고 *다음*을 클릭합니다.



7. 마지막으로, 데이터베이스 파일의 대상 위치를 지정하고 복원 버튼을 클릭하여 복원 프로세스를 시작합니다.

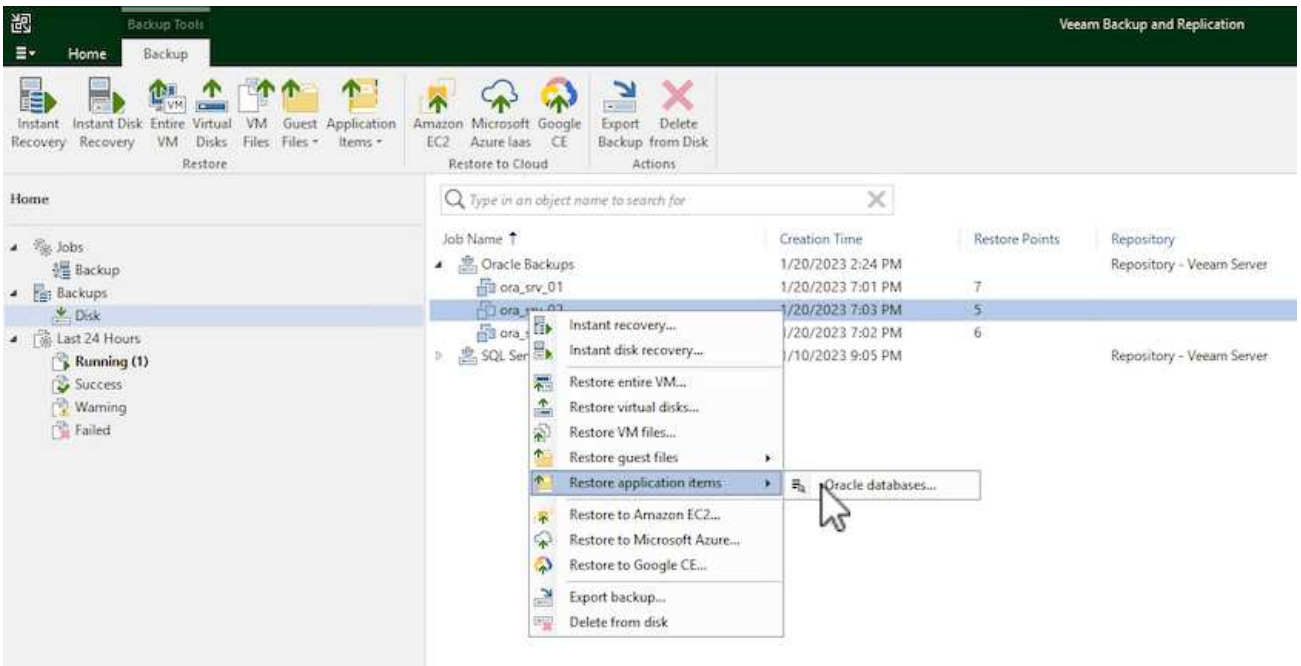


8. 데이터베이스 복구가 완료되면 Oracle 데이터베이스가 서버에서 제대로 시작되는지 확인하세요.

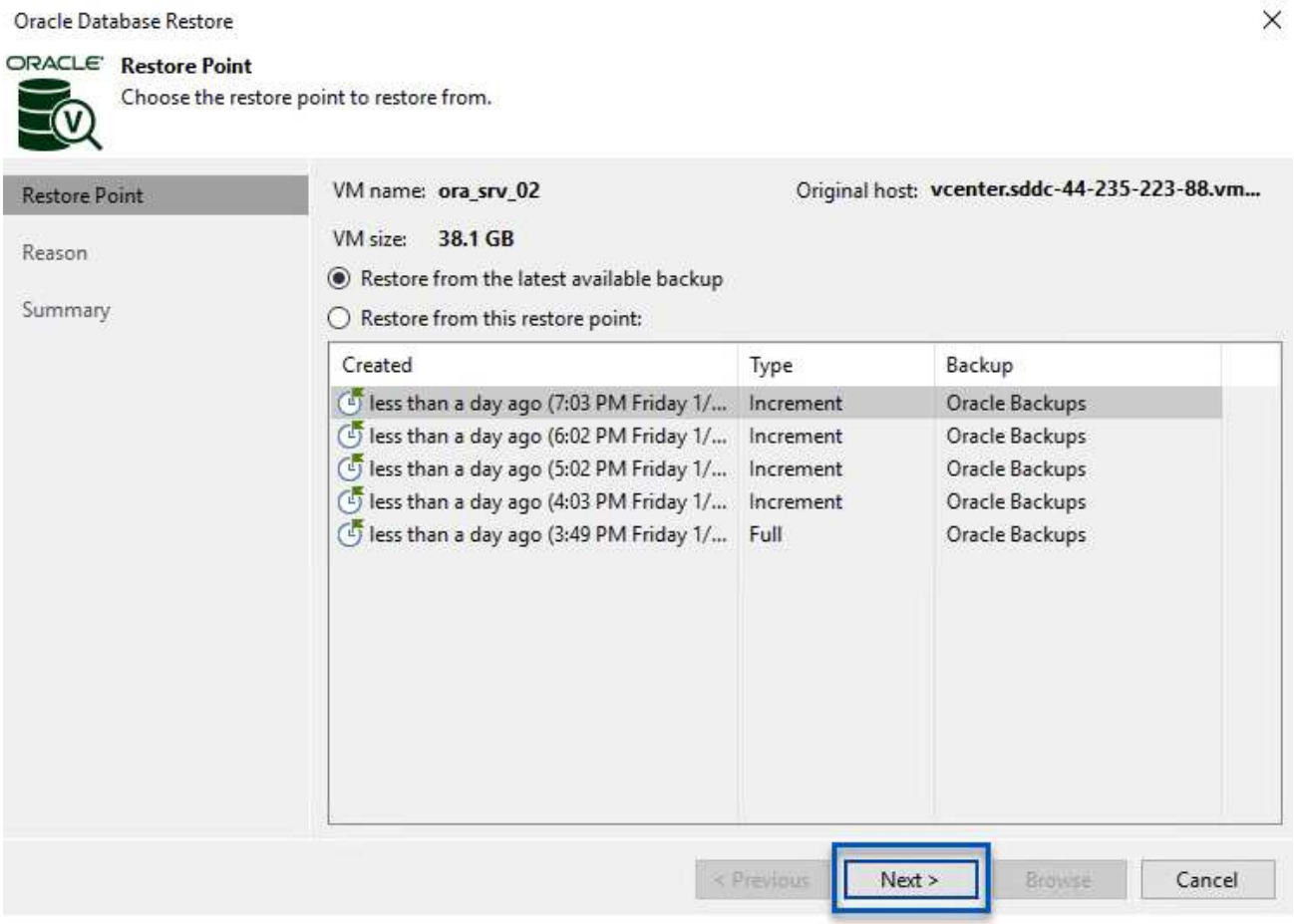
▼ **Oracle** 데이터베이스를 대체 서버에 게시

이 섹션에서는 전체 복원을 실행하지 않고도 빠른 액세스를 위해 대체 서버에 데이터베이스를 게시합니다.

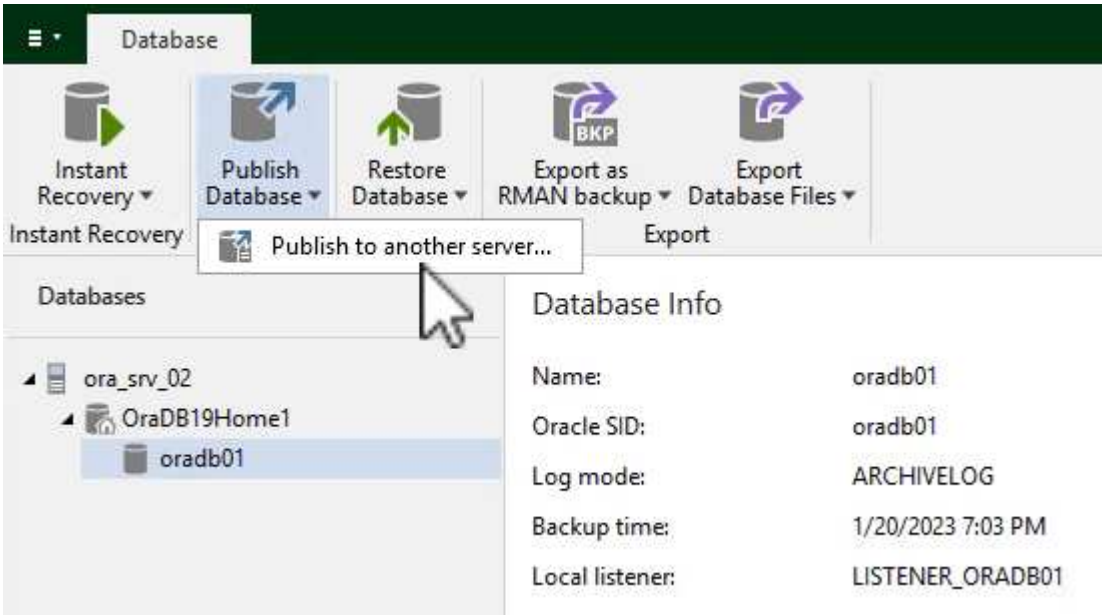
1. Veeam Backup and Replication 콘솔에서 Oracle 백업 목록으로 이동한 다음 서버를 마우스 오른쪽 버튼으로 클릭하고 *애플리케이션 항목 복원*을 선택한 다음 *Oracle 데이터베이스…*를 선택합니다.



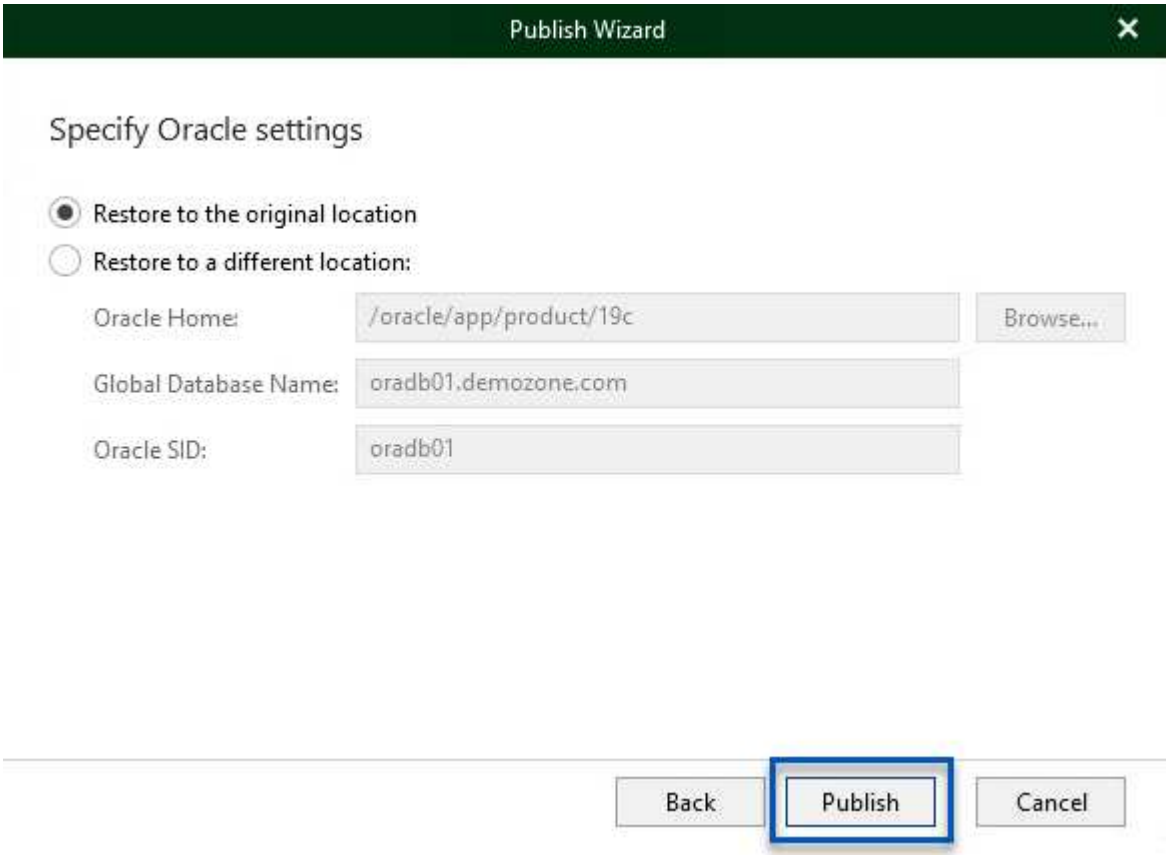
2. Oracle 데이터베이스 복원 마법사에서 목록에서 복원 지점을 선택하고 *다음*을 클릭합니다.



3. 원하는 경우 복원 이유*를 입력한 다음 요약 페이지에서 *찾아보기 버튼을 클릭하여 Oracle용 Veeam Explorer를 시작합니다.
4. Veeam Explorer에서 데이터베이스 인스턴스 목록을 확장하고 복원할 데이터베이스를 클릭한 다음 상단의 데이터베이스 게시 드롭다운 메뉴에서 *다른 서버에 게시…*를 선택합니다.



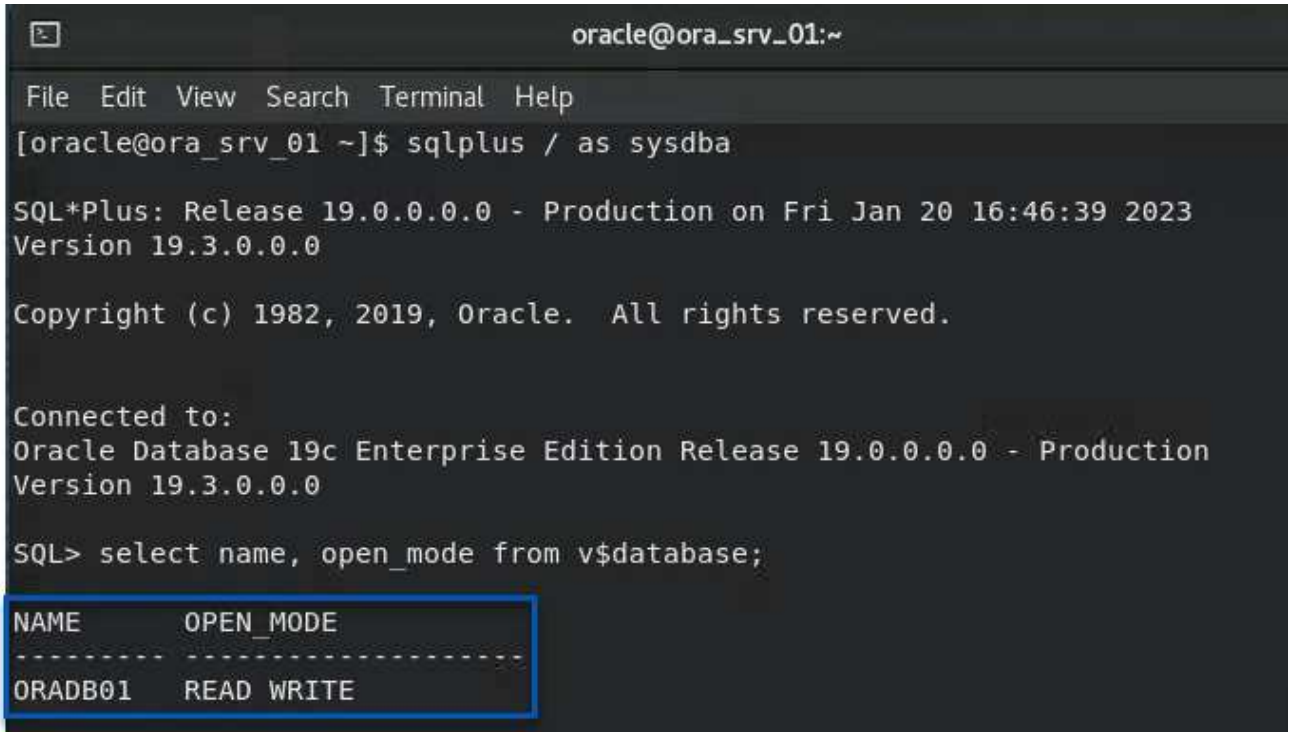
5. 게시 마법사에서 데이터베이스를 게시할 복원 지점을 지정하고 *다음*을 클릭합니다.
6. 마지막으로 대상 Linux 파일 시스템 위치를 지정하고 *게시*를 클릭하여 복원 프로세스를 시작합니다.



7. 게시가 완료되면 대상 서버에 로그인하고 다음 명령을 실행하여 데이터베이스가 실행 중인지 확인하세요.

```
oracle@ora_srv_01> sqlplus / as sysdba
```

```
SQL> select name, open_mode from v$database;
```



결론

VMware Cloud는 비즈니스에 중요한 애플리케이션을 실행하고 중요한 데이터를 저장하기 위한 강력한 플랫폼입니다. 사이버 위협과 데이터 손실로부터 보호하고 비즈니스 연속성을 보장하기 위해 VMware Cloud에 의존하는 기업에게는 안전한 데이터 보호 솔루션이 필수적입니다. 안정적이고 견고한 데이터 보호 솔루션을 선택하면 기업은 무슨 일이 있어도 중요한 데이터가 안전하게 보호된다는 확신을 가질 수 있습니다.

이 문서에 제시된 사용 사례는 NetApp, VMware, Veeam 간의 통합을 강조하는 검증된 데이터 보호 기술에 초점을 맞춥니다. FSx ONTAP 은 AWS의 VMware Cloud에 대한 보충 NFS 데이터 저장소로 지원되며 모든 가상 머신 및 애플리케이션 데이터에 사용됩니다. Veeam Backup & Replication은 기업이 백업 및 복구 프로세스를 개선, 자동화, 간소화하는 데 도움이 되도록 설계된 포괄적인 데이터 보호 솔루션입니다. Veeam은 FSx ONTAP 에 호스팅된 iSCSI 백업 대상 볼륨과 함께 사용되어 VMware Cloud에 있는 애플리케이션 데이터를 위한 안전하고 관리하기 쉬운 데이터 보호 솔루션을 제공합니다.

추가 정보

이 솔루션에 제시된 기술에 대해 자세히 알아보려면 다음 추가 정보를 참조하세요.

- "FSx ONTAP 사용자 가이드"
- "Veeam 도움말 센터 기술 문서"
- "AWS에서 VMware Cloud 지원. 고려 사항 및 제한 사항"

TR-4955: FSx ONTAP 및 **VMC(AWS VMware Cloud)**를 사용한 재해 복구

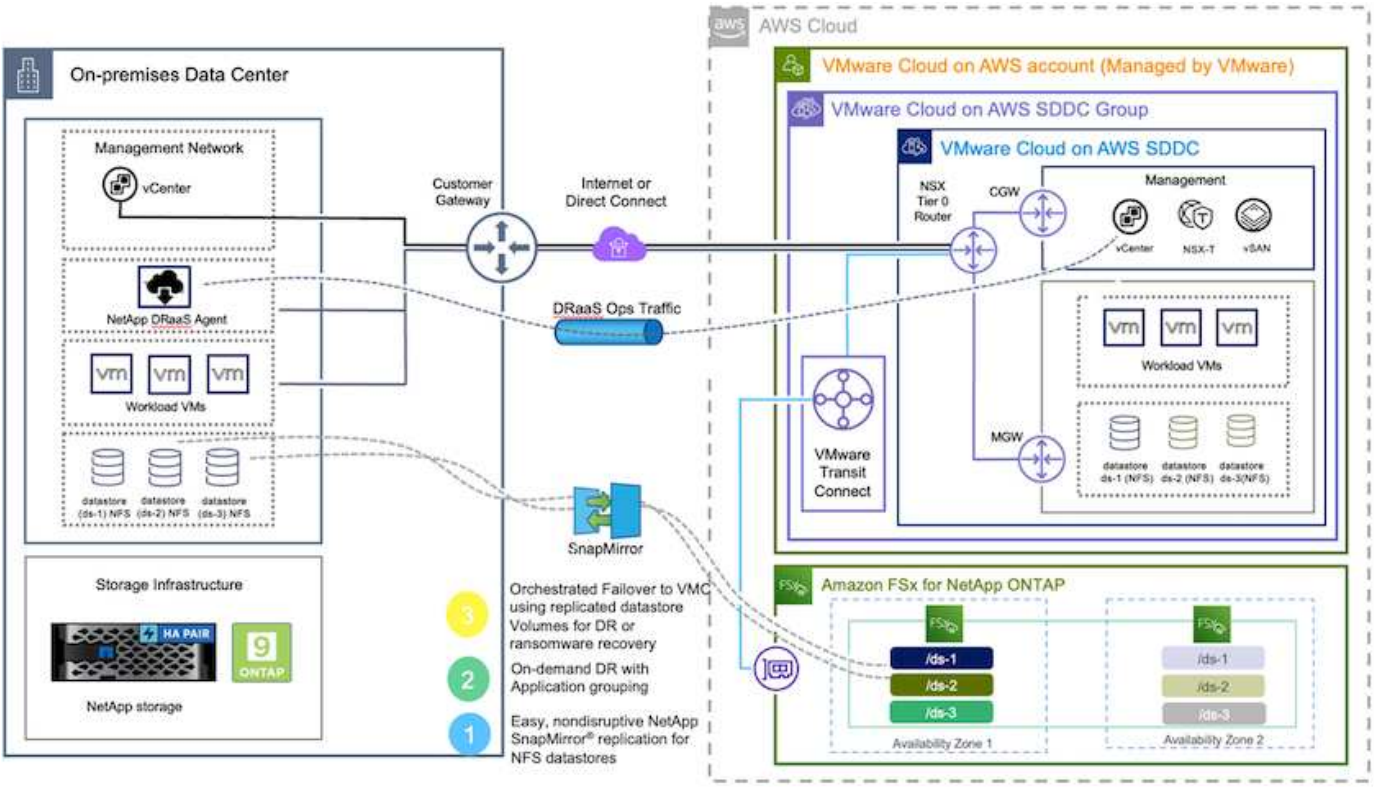
DRO(재해 복구 오케스트레이터, UI가 있는 스크립트 솔루션)를 사용하면 온프레미스에서 FSx ONTAP 으로 복제된 워크로드를 원활하게 복구할 수 있습니다. DRO는 SnapMirror 수준에서 VM 등록을 거쳐 VMC로, 그리고 NSX-T에서 직접 네트워크 매핑까지 복구를 자동화합니다. 이 기능은 모든 VMC 환경에 포함되어 있습니다.

니야즈 모하메드, NetApp

개요

클라우드로 재해 복구를 수행하는 것은 사이트 중단 및 데이터 손상 사고(예: 랜섬웨어)로부터 작업 부하를 보호하는 탄력적이고 비용 효율적인 방법입니다. NetApp SnapMirror 기술을 사용하면 온프레미스 VMware 워크로드를 AWS에서 실행되는 FSx ONTAP 으로 복제할 수 있습니다.

DRO(재해 복구 오케스트레이터, UI가 있는 스크립트 솔루션)를 사용하면 온프레미스에서 FSx ONTAP 으로 복제된 워크로드를 원활하게 복구할 수 있습니다. DRO는 SnapMirror 수준에서 VM 등록을 거쳐 VMC로, 그리고 NSX-T에서 직접 네트워크 매핑까지 복구를 자동화합니다. 이 기능은 모든 VMC 환경에 포함되어 있습니다.



시작하기

AWS에서 **VMware Cloud** 배포 및 구성

"AWS의 VMware 클라우드"AWS 생태계에서 VMware 기반 워크로드에 대한 클라우드 네이티브 환경을 제공합니다. 각 VMware 소프트웨어 정의 데이터 센터(SDDC)는 Amazon Virtual Private Cloud(VPC)에서 실행되며 전체 VMware 스택(vCenter Server 포함), NSX-T 소프트웨어 정의 네트워킹, vSAN 소프트웨어 정의 스토리지, 워크로드에 컴퓨팅 및 스토리지 리소스를 제공하는 하나 이상의 ESXi 호스트를 제공합니다. AWS에서 VMC 환경을 구성하려면 다음 단계를 따르세요."링크" . 조종등 클러스터도 DR 목적으로 사용될 수 있습니다.

초기 릴리스에서는 DRO가 기존 조종등 클러스터를 지원합니다. 온디맨드 SDDC 생성은 향후 릴리스에서 제공될 예정입니다.

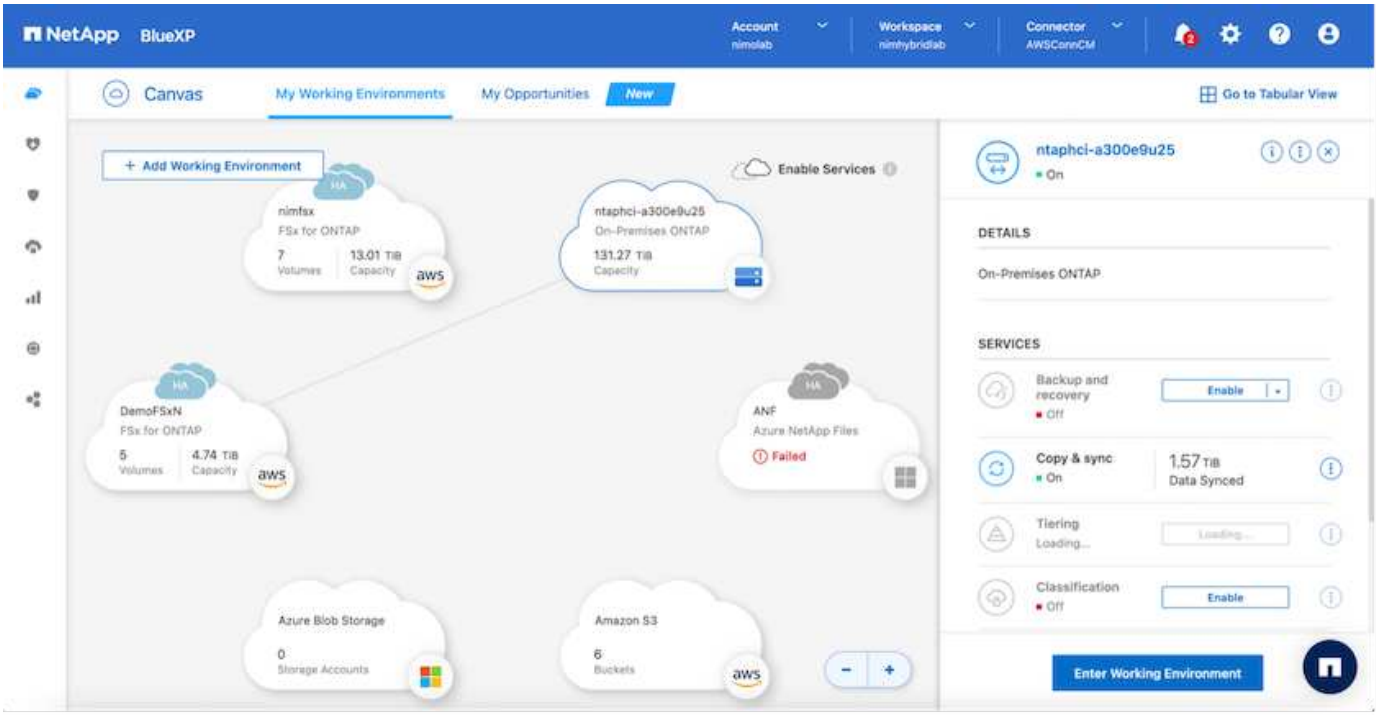
FSx ONTAP 프로비저닝 및 구성

Amazon FSx ONTAP 인기 있는 NetApp ONTAP 파일 시스템을 기반으로 높은 안정성, 확장성, 고성능, 다양한 기능을 갖춘 파일 스토리지를 제공하는 완전 관리형 서비스입니다. 이 단계를 따르세요"링크" FSx ONTAP 프로비저닝하고

구성합니다.

FSx ONTAP 에 SnapMirror 배포 및 구성

다음 단계는 NetApp Console을 사용하여 프로비저닝된 AWS 인스턴스의 FSx ONTAP을 탐색하고, 적절한 빈도 및 NetApp 스냅샷 복사본 보존을 통해 온프레미스 환경에서 FSx ONTAP으로 원하는 데이터스토어 볼륨을 복제하는 것입니다:



DRO를 구성하려면 이 링크의 단계를 따르십시오. 또한 이 링크를 참조하여 NetApp ONTAP CLI를 사용하여 복제 일정을 예약할 수도 있습니다.

SnapMirror 관계는 필수 조건이므로 미리 만들어야 합니다.

DRO 설치

DRO를 시작하려면 지정된 EC2 인스턴스나 가상 머신에서 Ubuntu 운영 체제를 사용하여 필수 구성 요소를 충족하는지 확인하세요. 그런 다음 패키지를 설치하세요.

필수 조건

- 소스 및 대상 vCenter와 스토리지 시스템에 대한 연결이 있는지 확인하세요.
- DNS 이름을 사용하는 경우 DNS 확인이 이루어져야 합니다. 그렇지 않은 경우 vCenter 및 스토리지 시스템에 IP 주소를 사용해야 합니다.
- 루트 권한이 있는 사용자를 만듭니다. EC2 인스턴스에서도 sudo를 사용할 수 있습니다.

OS 요구 사항

- 최소 2GB 및 4개의 vCPU를 갖춘 Ubuntu 20.04(LTS)
- 지정된 에이전트 VM에 다음 패키지를 설치해야 합니다.

- 도커
- Docker-compose
- 제이큐

권한 변경 `docker.sock` : `sudo chmod 666 /var/run/docker.sock` .

그만큼 `deploy.sh` 스크립트는 모든 필수 전제 조건을 실행합니다.

패키지를 설치하세요

1. 지정된 가상 머신에 설치 패키지를 다운로드하세요.

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

에이전트는 온프레미스 또는 AWS VPC 내에 설치할 수 있습니다.

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

```
tar xvf DRO-prereq.tar
```

3. 디렉토리로 이동하여 다음과 같이 배포 스크립트를 실행합니다.

```
sudo sh deploy.sh
```

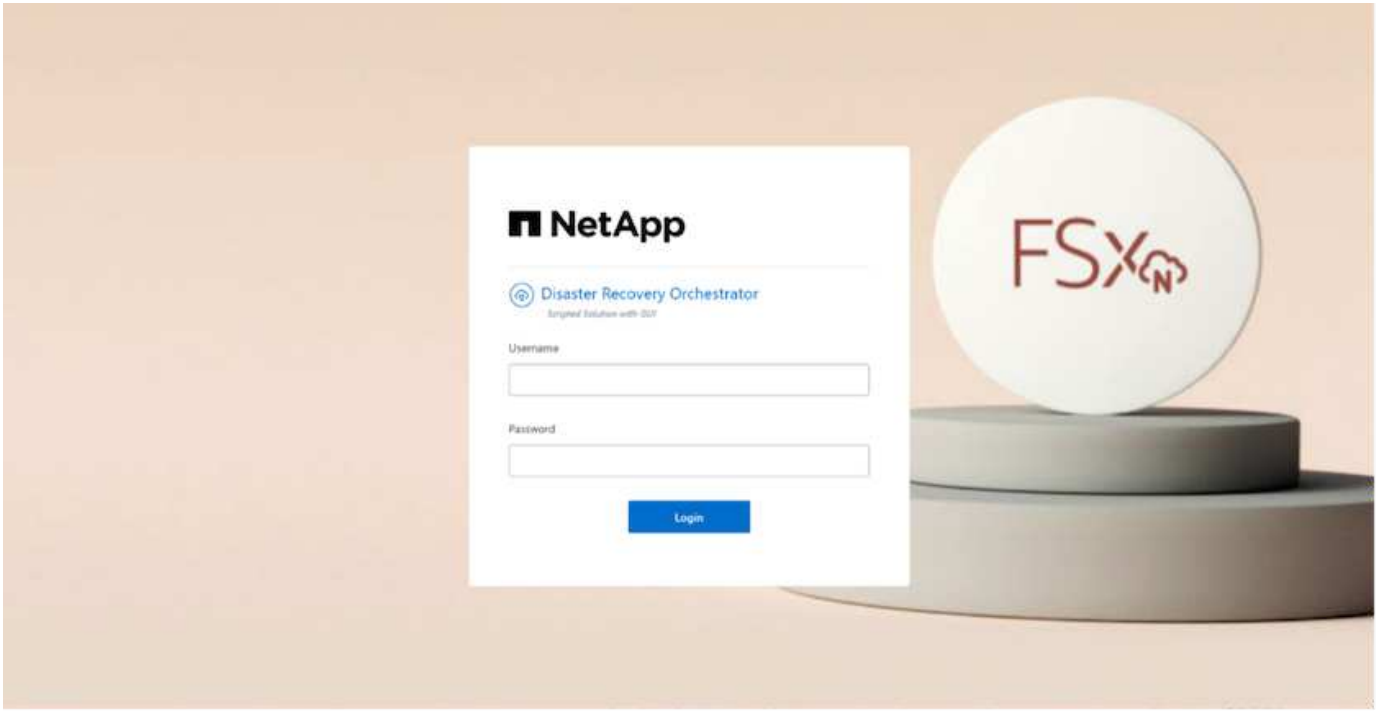
4. UI에 액세스하려면 다음을 사용하세요.

```
https://<host-ip-address>
```

다음 기본 자격 증명을 사용합니다.

```
Username: admin
Password: admin
```

비밀번호는 "비밀번호 변경" 옵션을 사용하여 변경할 수 있습니다.



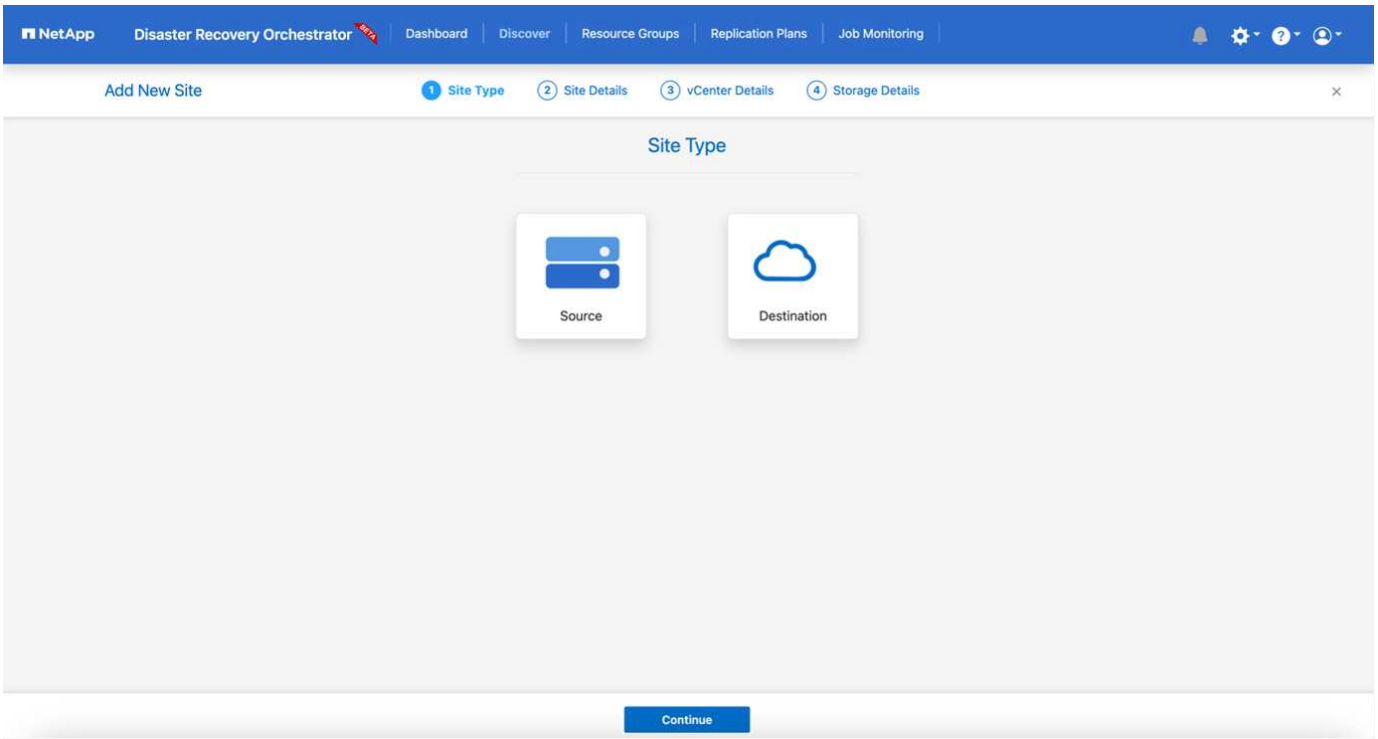
DRO 구성

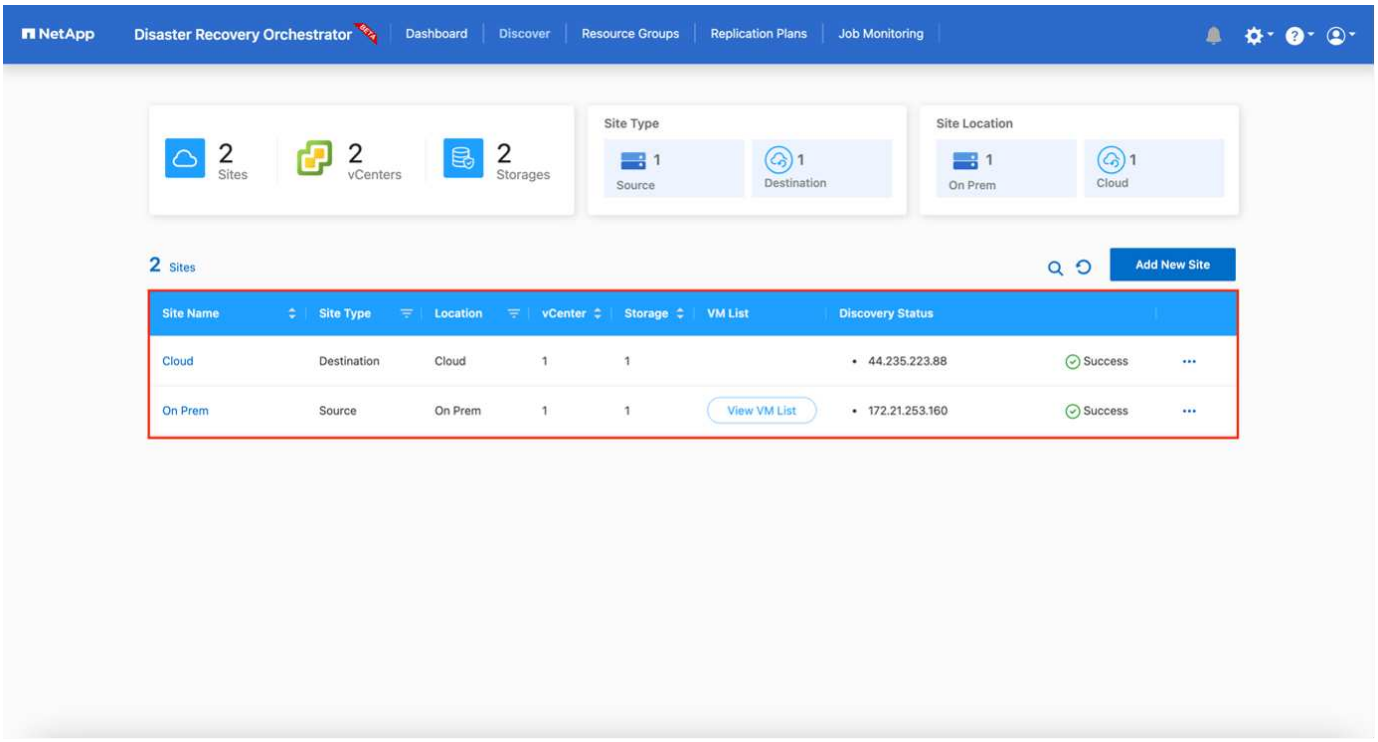
FSx ONTAP 과 VMC가 올바르게 구성된 후 FSx ONTAP 의 읽기 전용 SnapMirror 복사본을 사용하여 온프레미스 워크로드를 VMC로 복구하는 작업을 자동화하도록 DRO를 구성할 수 있습니다.

NetApp DRO 에이전트를 AWS에 배포하고 FSx ONTAP 배포된 동일한 VPC에 배포하는 것을 권장합니다(피어 연결도 가능). 이렇게 하면 DRO 에이전트가 네트워크를 통해 온프레미스 구성 요소뿐 아니라 FSx ONTAP 및 VMC 리소스와도 통신할 수 있습니다.

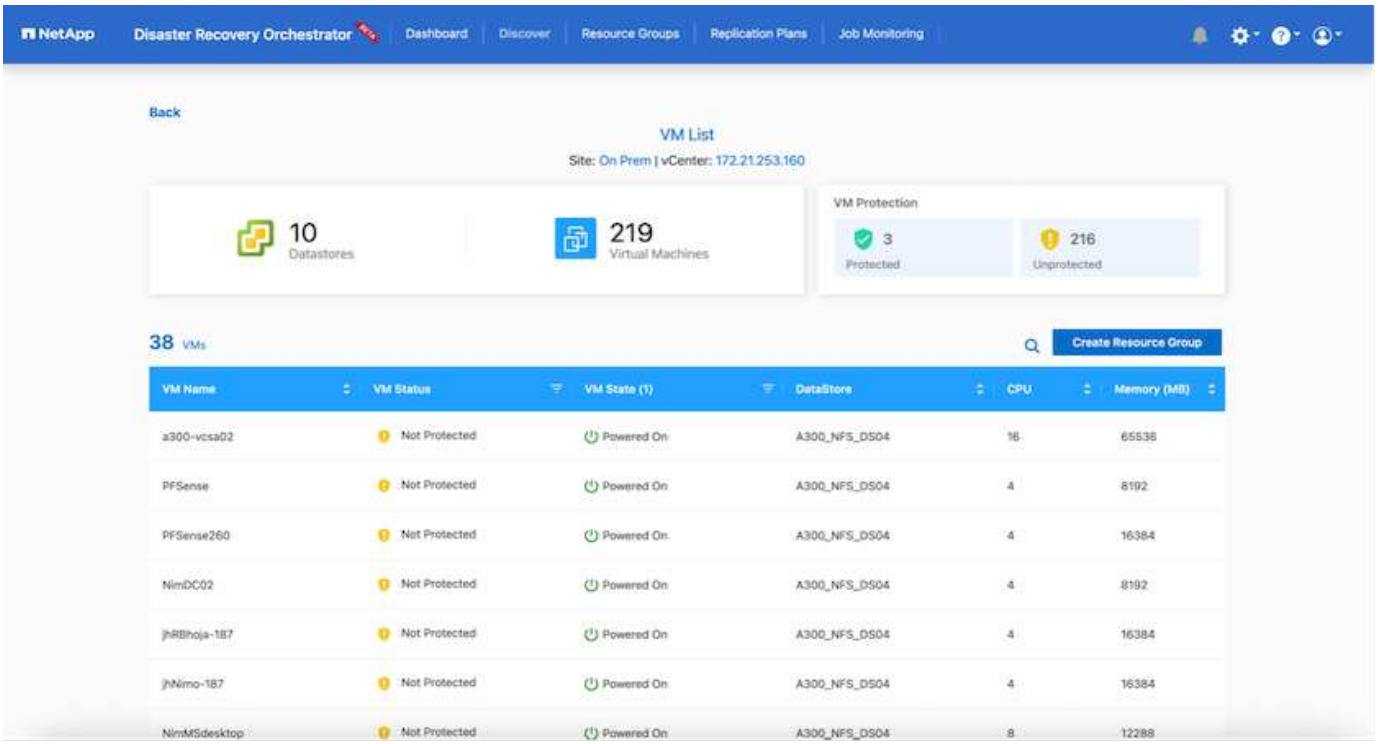
첫 번째 단계는 온프레미스 및 클라우드 리소스(vCenter와 스토리지 모두)를 검색하여 DRO에 추가하는 것입니다. 지원되는 브라우저에서 DRO를 열고 기본 사용자 이름과 비밀번호(admin/admin)를 사용하고 사이트를 추가합니다. Discover 옵션을 사용하여 사이트를 추가할 수도 있습니다. 다음 플랫폼을 추가하세요:

- 온프레미스
  - 온프레미스 vCenter
  - ONTAP 스토리지 시스템
- 클라우드
  - VMC vCenter
  - FSx ONTAP





DRO가 추가되면 자동 검색을 수행하고 소스 스토리지에서 FSx ONTAP 으로의 해당 SnapMirror 복제본이 있는 VM을 표시합니다. DRO는 VM에서 사용하는 네트워크와 포트 그룹을 자동으로 감지하고 이를 채웁니다.



다음 단계는 필요한 VM을 기능 그룹으로 그룹화하여 리소스 그룹으로 사용하는 것입니다.

리소스 그룹화

플랫폼을 추가한 후에는 복구하려는 VM을 리소스 그룹으로 그룹화할 수 있습니다. DRO 리소스 그룹을 사용하면 종속된 VM 세트를 부팅 순서, 부팅 지연, 복구 시 실행할 수 있는 선택적 애플리케이션 유효성 검사가 포함된 논리적 그룹으로 그룹화할 수 있습니다.

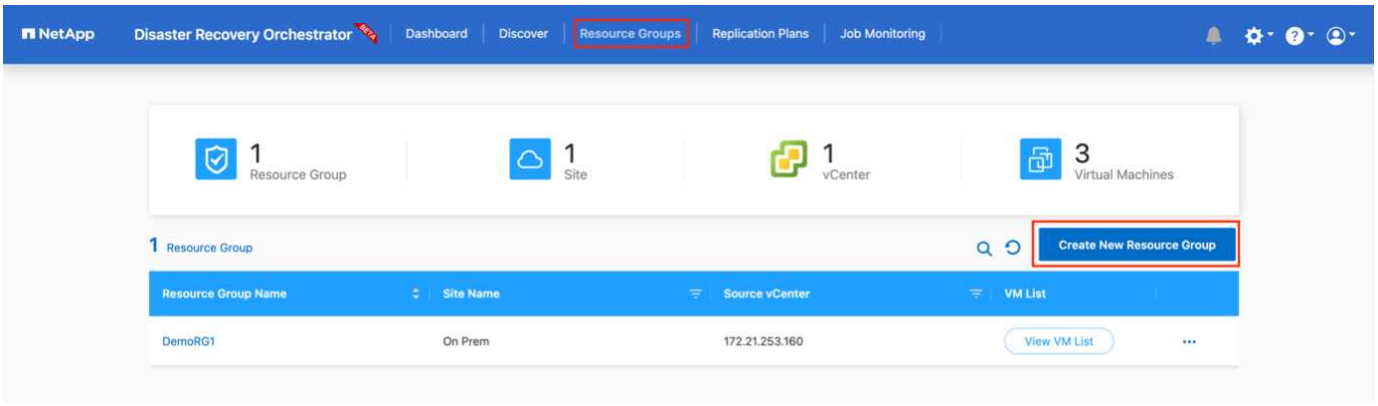
리소스 그룹을 만들려면 다음 단계를 완료하세요.

1. *리소스 그룹*에 액세스하고 *새 리소스 그룹 만들기*를 클릭합니다.
2. *새 리소스 그룹*에서 드롭다운에서 소스 사이트를 선택하고 *만들기*를 클릭합니다.
3. *리소스 그룹 세부 정보*를 제공하고 *계속*을 클릭합니다.
4. 검색 옵션을 사용하여 적절한 VM을 선택하세요.
5. 선택한 VM에 대한 부팅 순서와 부팅 지연(초)을 선택합니다. 각 VM을 선택하고 우선순위를 설정하여 전원 켜기 순서를 설정합니다. 모든 VM의 기본값은 3입니다.

   옵션은 다음과 같습니다.

   1 – 전원을 켜는 첫 번째 가상 머신 3 – 기본값 5 – 전원을 켜는 마지막 가상 머신

6. *리소스 그룹 만들기*를 클릭합니다.

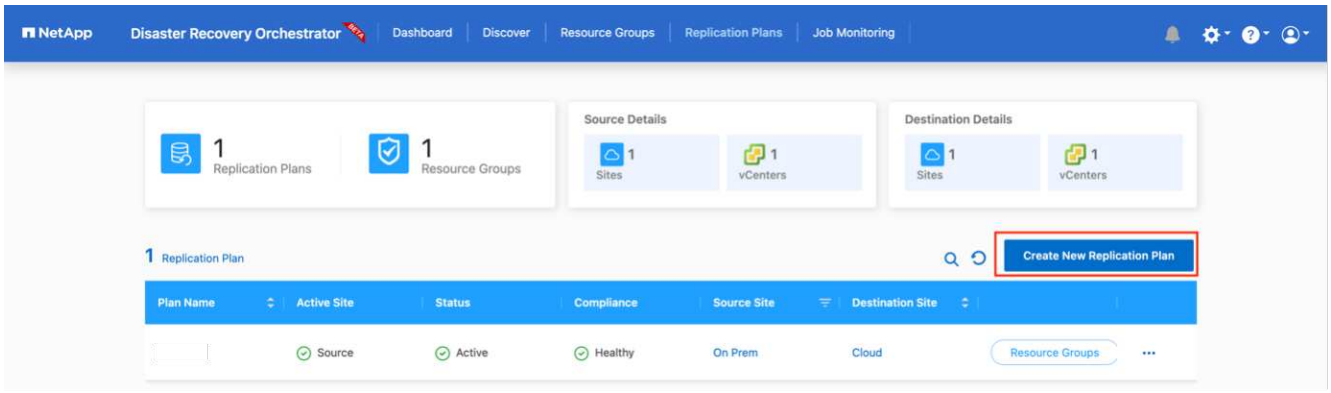


복제 계획

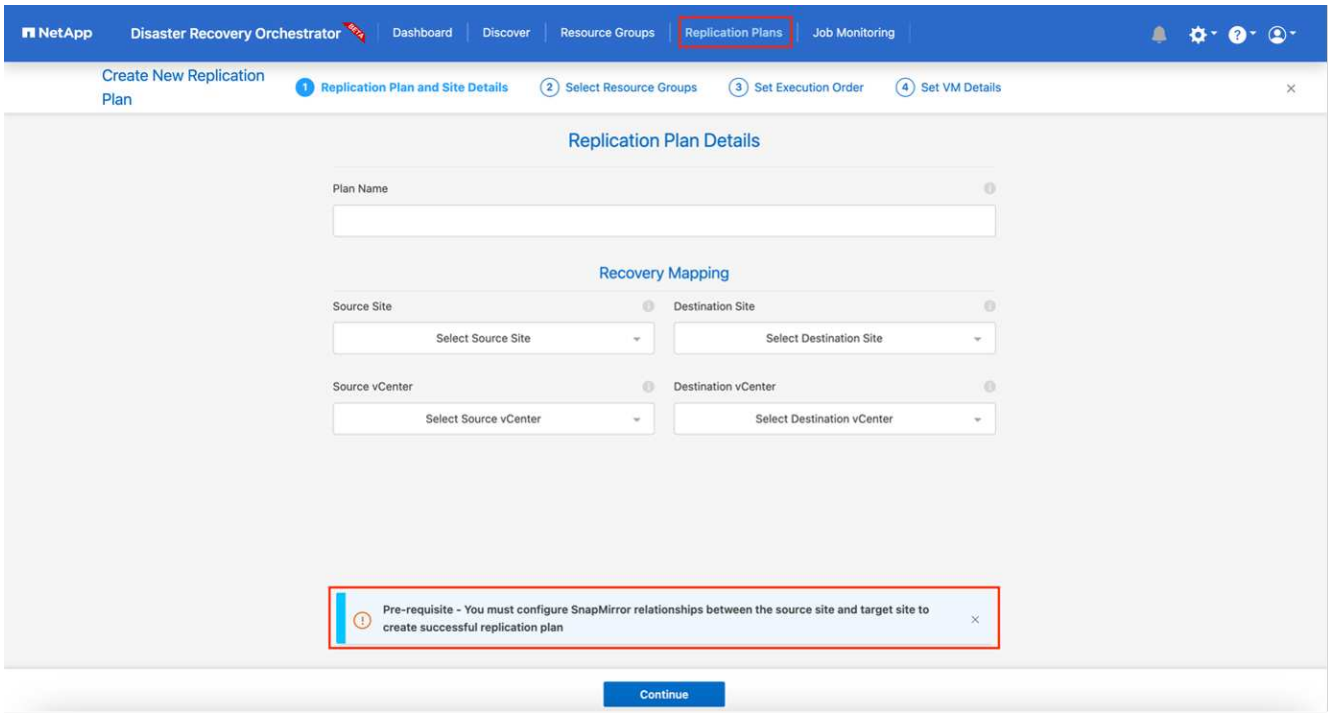
재해 발생 시 애플리케이션을 복구할 계획이 필요합니다. 드롭다운에서 소스 및 대상 vCenter 플랫폼을 선택하고 이 계획에 포함할 리소스 그룹을 선택하고, 애플리케이션을 복원하고 전원을 켜는 방법(예: 도메인 컨트롤러, 그 다음 1계층, 그 다음 2계층 등)을 그룹화합니다. 이러한 계획은 때때로 청사진이라고도 불립니다. 복구 계획을 정의하려면 복제 계획 탭으로 이동하여 *새 복제 계획*을 클릭합니다.

복제 계획을 만들려면 다음 단계를 완료하세요.

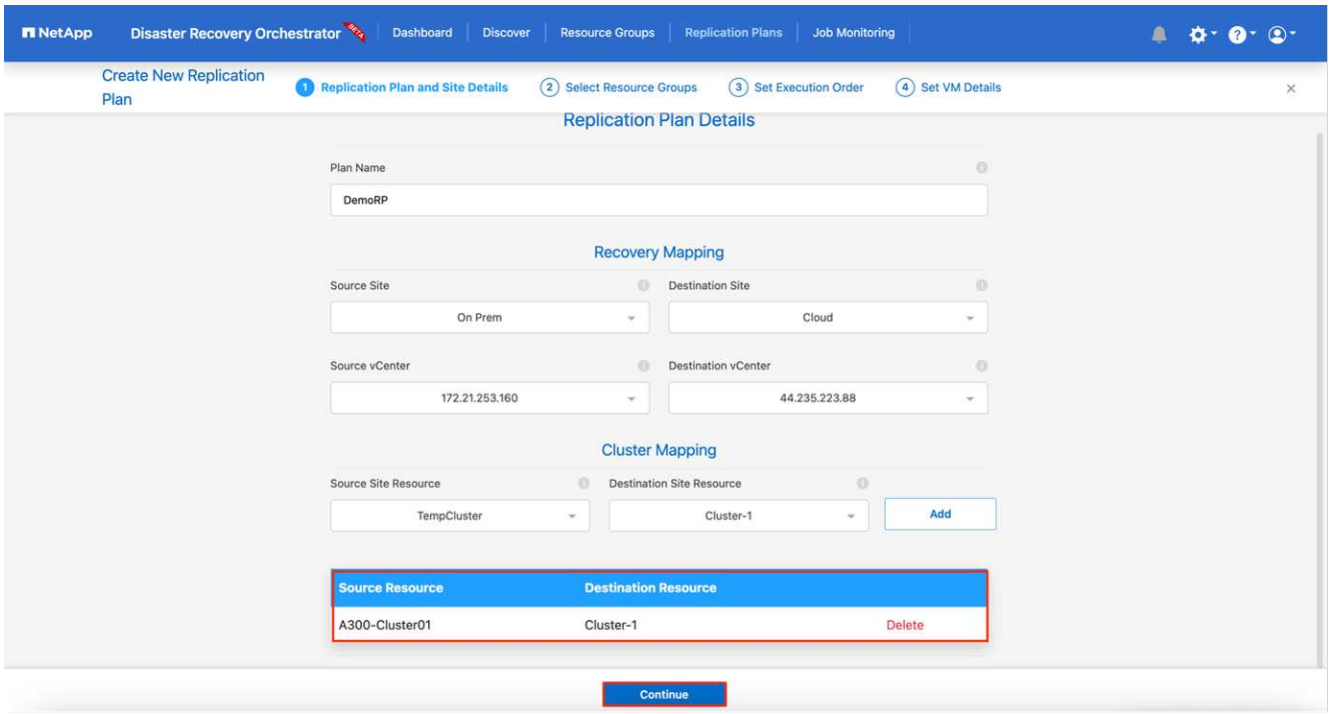
1. *복제 계획*에 액세스하고 *새 복제 계획 만들기*를 클릭합니다.



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

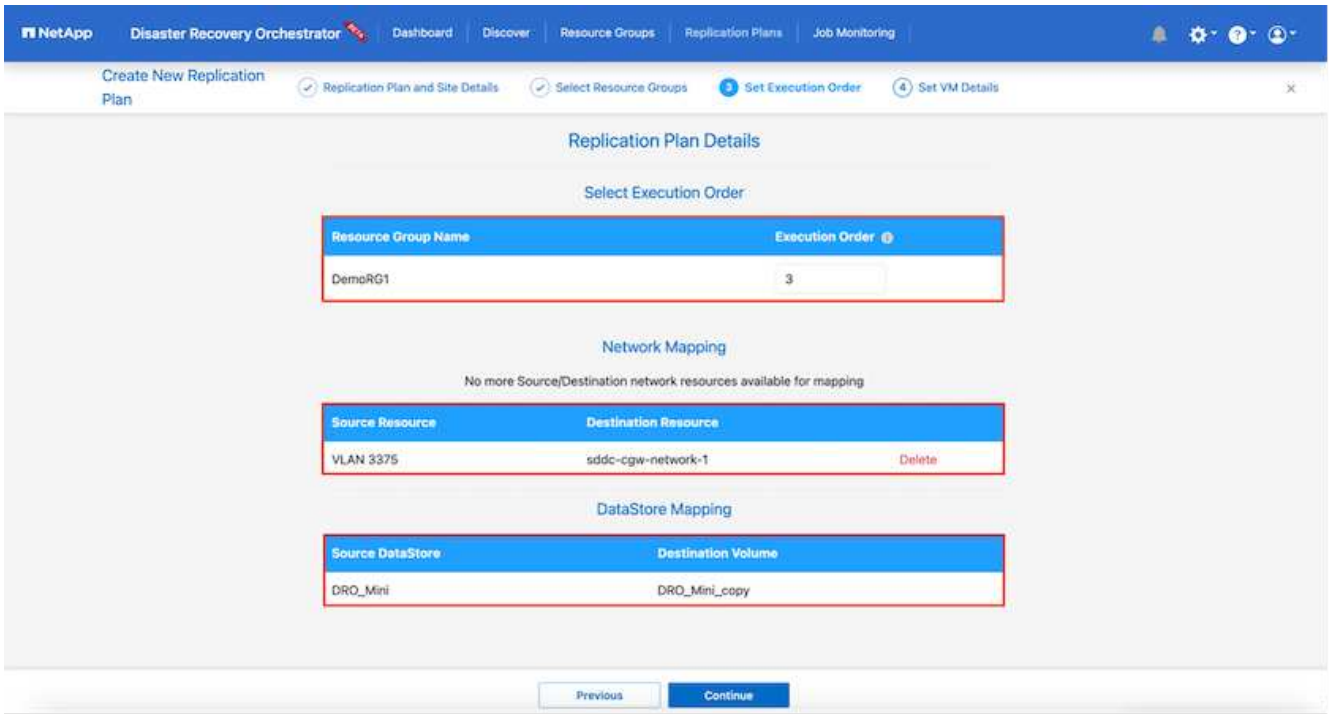


3. 복구 매핑이 완료된 후 클러스터 매핑을 선택합니다.

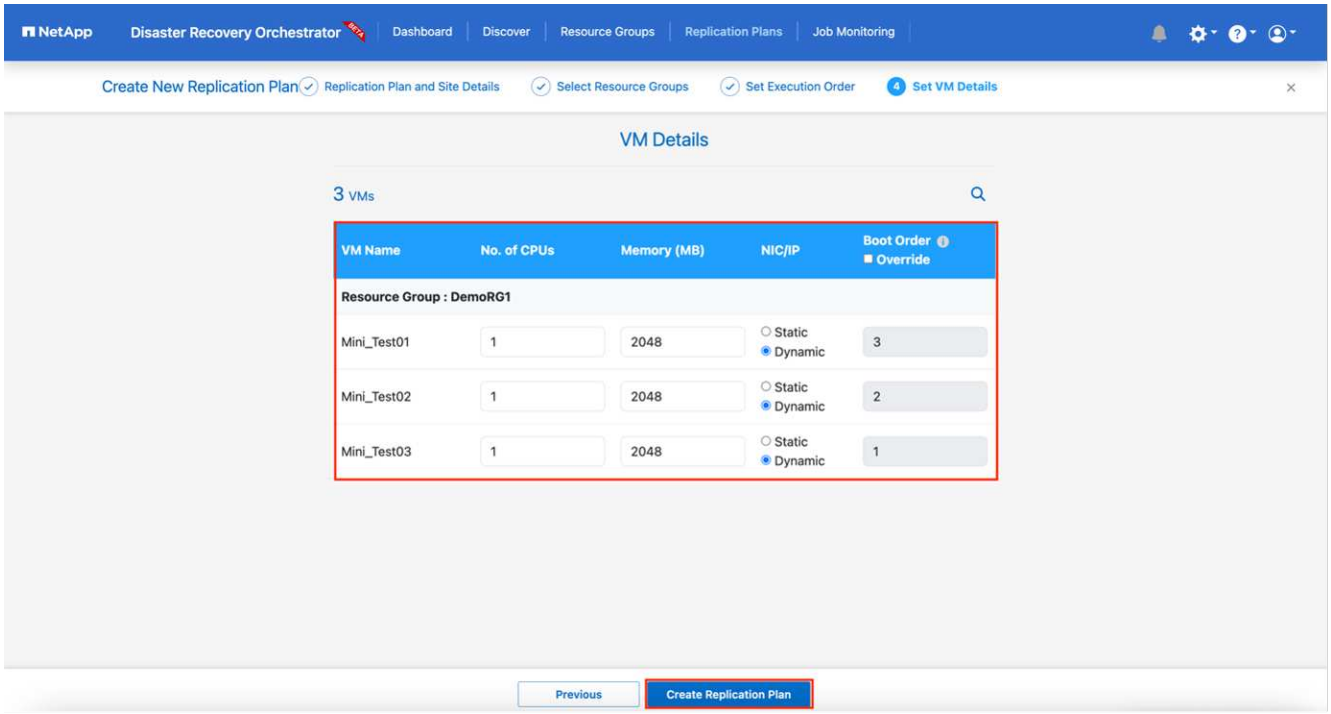


4. *리소스 그룹 세부 정보*를 선택하고 *계속*을 클릭합니다.
5. 리소스 그룹에 대한 실행 순서를 설정합니다. 이 옵션을 사용하면 여러 리소스 그룹이 있는 경우 작업 순서를 선택할 수 있습니다.
6. 작업이 끝나면 적절한 세그먼트에 대한 네트워크 매핑을 선택하세요. 세그먼트는 이미 VMC 내에 프로비저닝되어 있으므로 VM을 매핑할 적절한 세그먼트를 선택하세요.
7. VM 선택에 따라 데이터 저장소 매핑이 자동으로 선택됩니다.

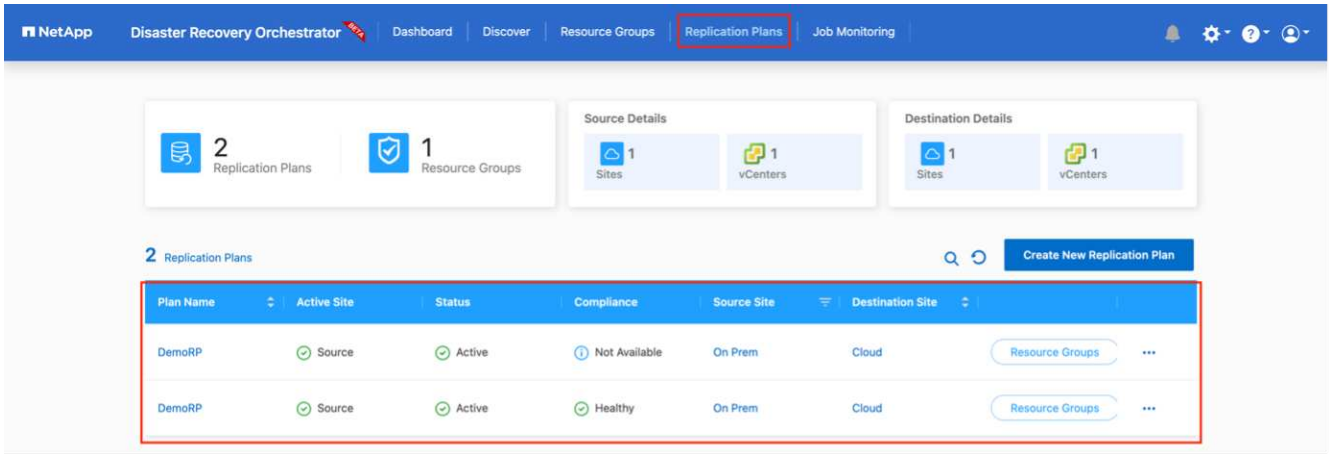
SnapMirror 볼륨 레벨에 있습니다. 따라서 모든 VM은 복제 대상에 복제됩니다. 데이터 저장소에 속한 모든 VM을 선택해야 합니다. 선택하지 않으면 복제 계획에 포함된 VM만 처리됩니다.



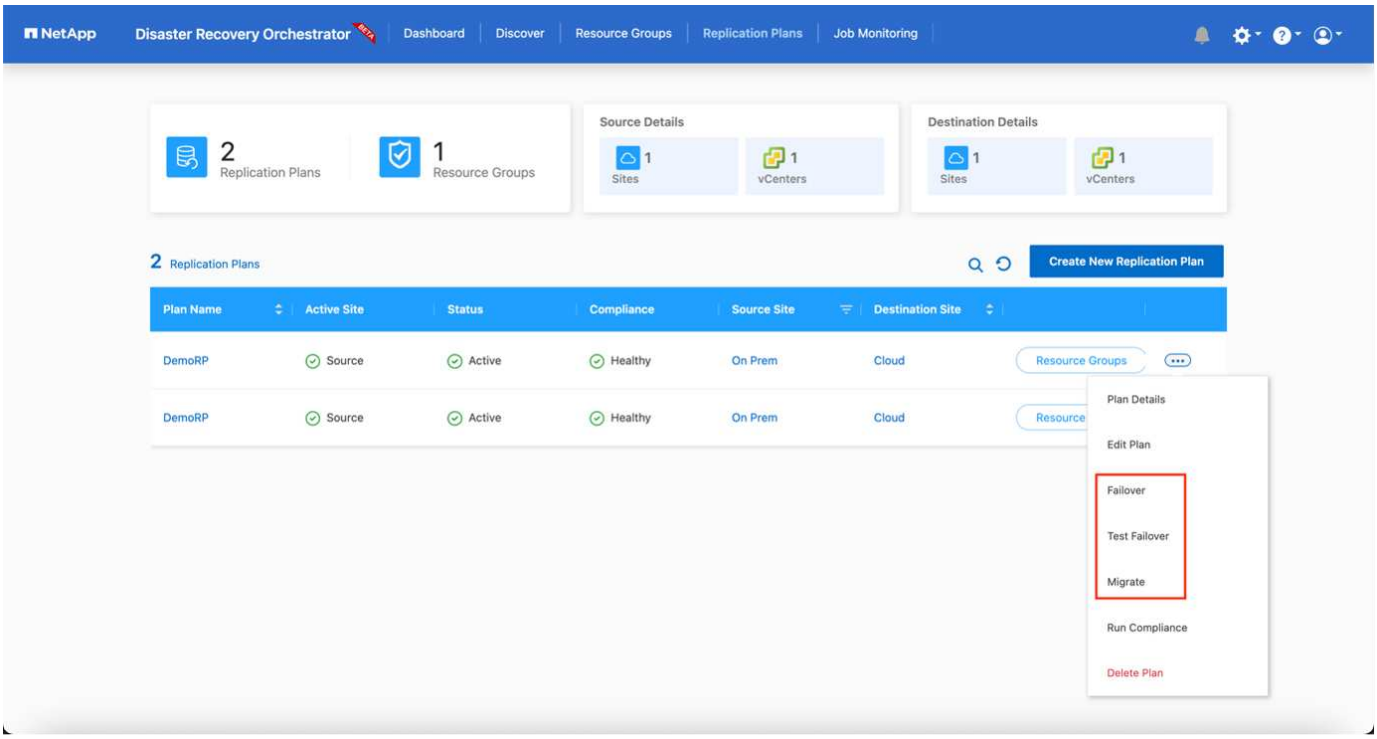
8. VM 세부 정보에서 선택적으로 VM의 CPU 및 RAM 매개변수 크기를 조정할 수 있습니다. 이 기능은 대규모 환경을 더 작은 대상 클러스터로 복구하거나 일대일 물리적 VMware 인프라를 프로비저닝하지 않고도 DR 테스트를 수행할 때 매우 유용합니다. 또한 리소스 그룹 전체에서 선택한 모든 VM의 부팅 순서와 부팅 지연(초)을 수정할 수 있습니다. 리소스 그룹 부팅 순서 선택 중에 선택한 내용에 변경 사항이 있는 경우 부팅 순서를 수정하는 추가 옵션이 있습니다. 기본적으로 리소스 그룹 선택 중에 선택된 부팅 순서가 사용됩니다. 그러나 이 단계에서 모든 수정 작업을 수행할 수 있습니다.

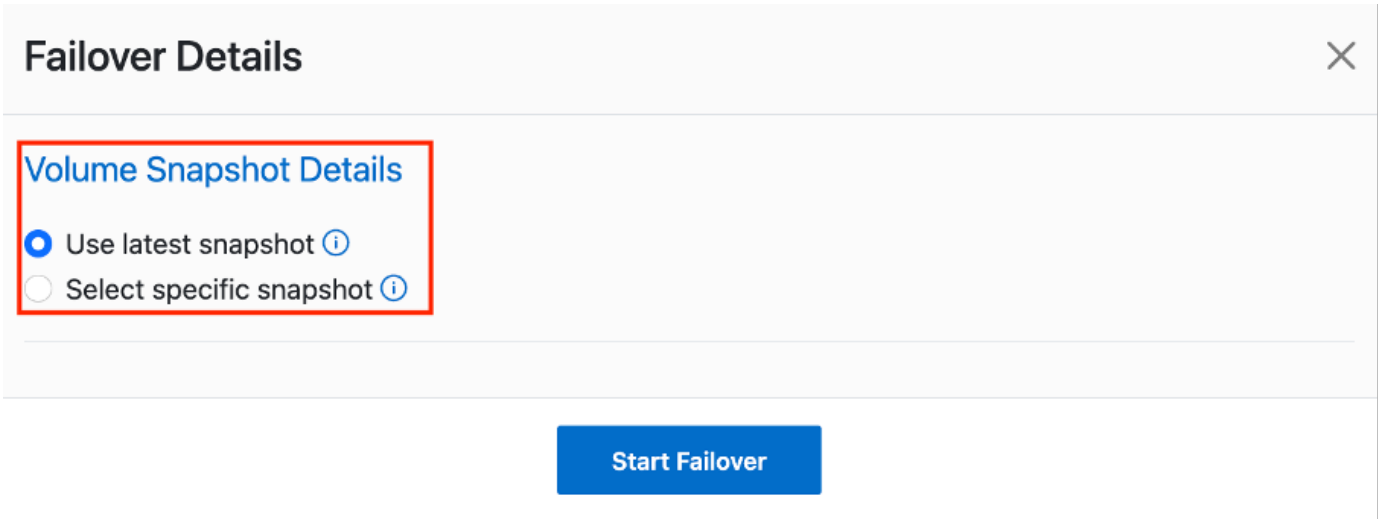


9. *복제 계획 만들기*를 클릭합니다.

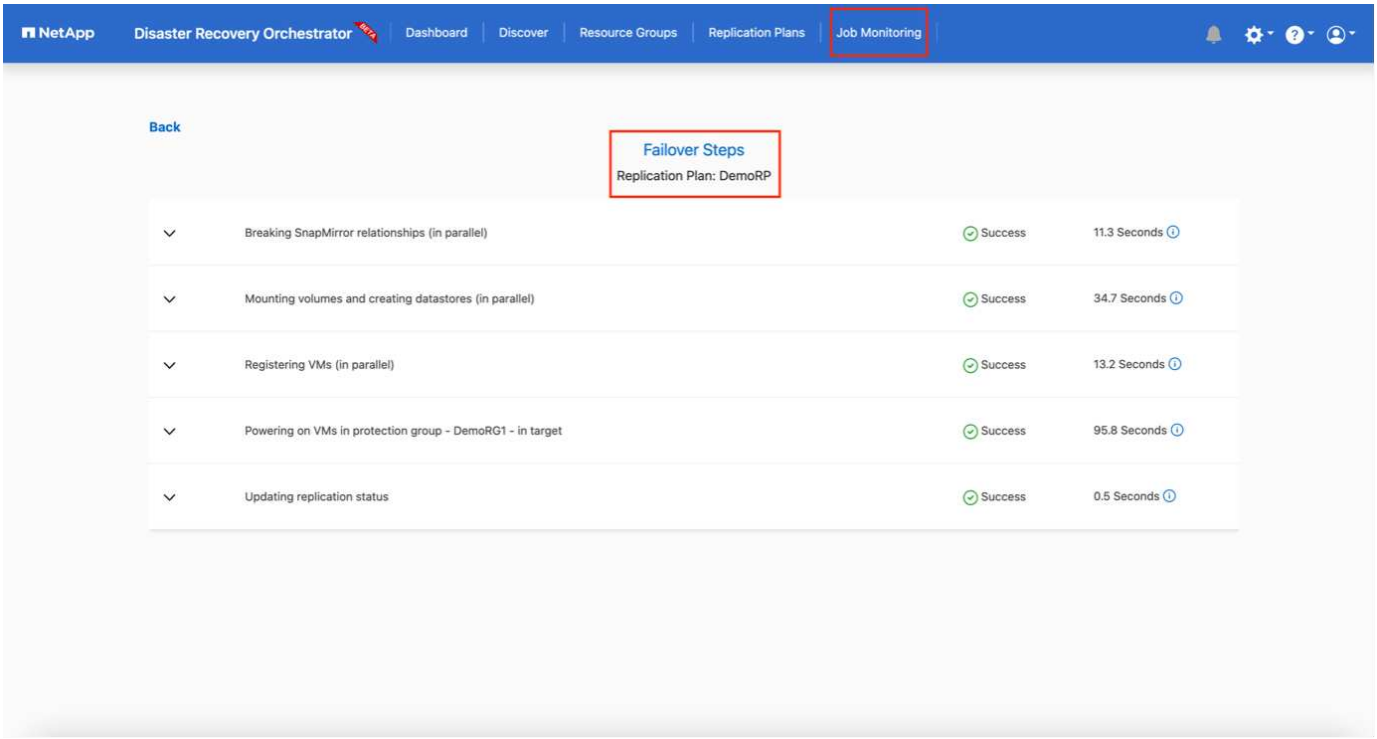


복제 계획이 생성된 후에는 요구 사항에 따라 장애 조치 옵션, 테스트 장애 조치 옵션 또는 마이그레이션 옵션을 실행할 수 있습니다. 장애 조치 및 테스트 장애 조치 옵션 동안 가장 최근의 SnapMirror 스냅샷 복사본이 사용되거나 특정 스냅샷 복사본을 특정 시점 스냅샷 복사본에서 선택할 수 있습니다(SnapMirror 의 보존 정책에 따라). 랜섬웨어와 같이 최신 복제본이 이미 손상되거나 암호화된 경우와 같이 손상 이벤트가 발생하는 경우 특정 시점 옵션이 매우 유용할 수 있습니다. DRO는 이용 가능한 모든 시점을 보여줍니다. 복제 계획에 지정된 구성으로 장애 조치 또는 테스트 장애 조치를 트리거하려면 장애 조치 또는 *테스트 장애 조치*를 클릭하면 됩니다.

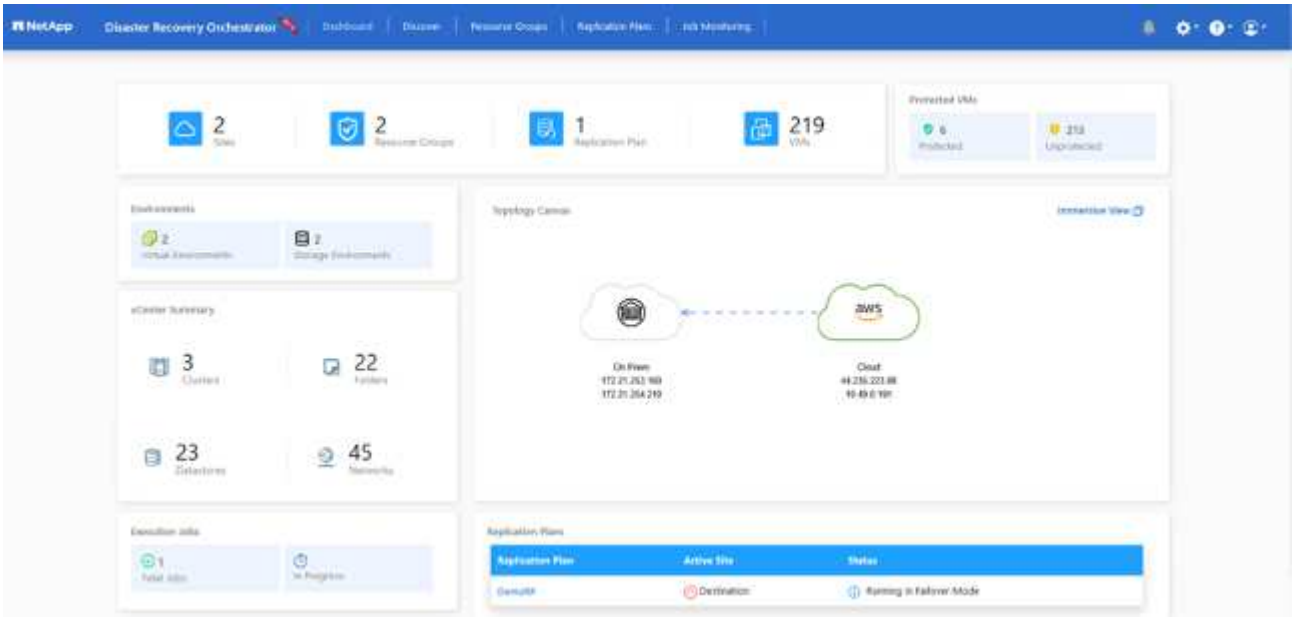




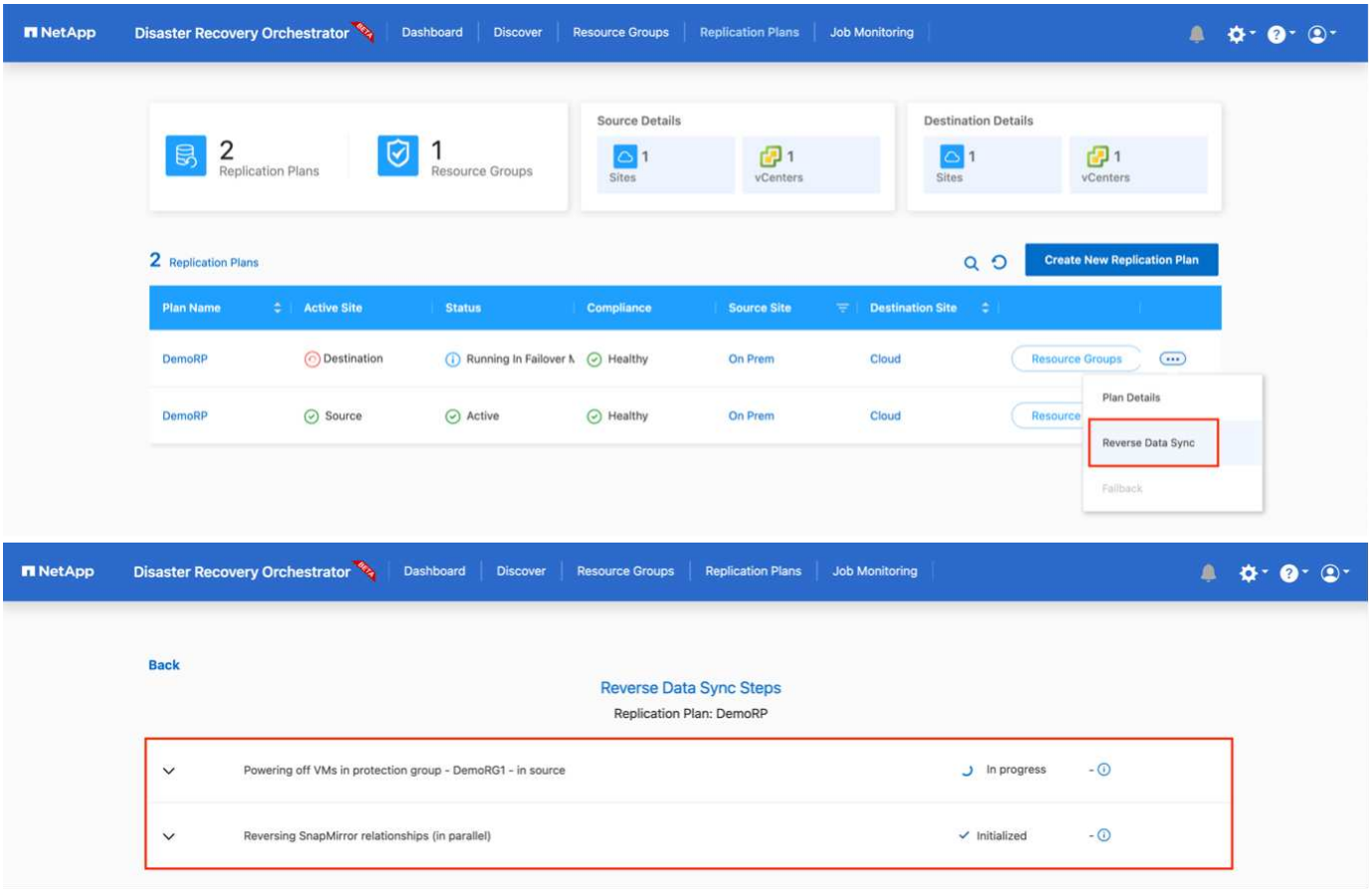
복제 계획은 작업 메뉴에서 모니터링할 수 있습니다.



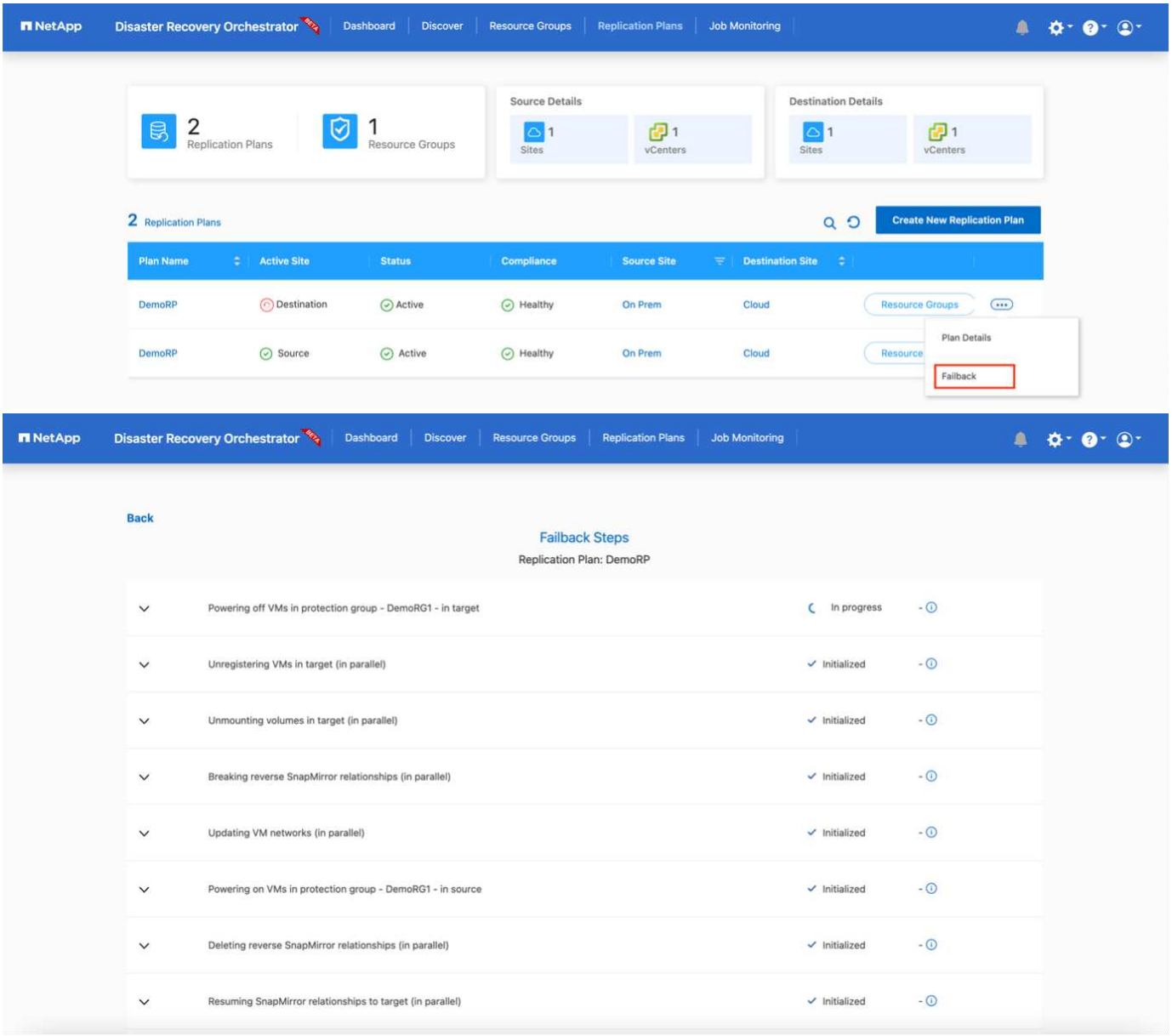
장애 조치가 트리거된 후 복구된 항목은 VMC vCenter(VM, 네트워크, 데이터 저장소)에서 볼 수 있습니다. 기본적으로 VM은 워크로드 폴더로 복구됩니다.



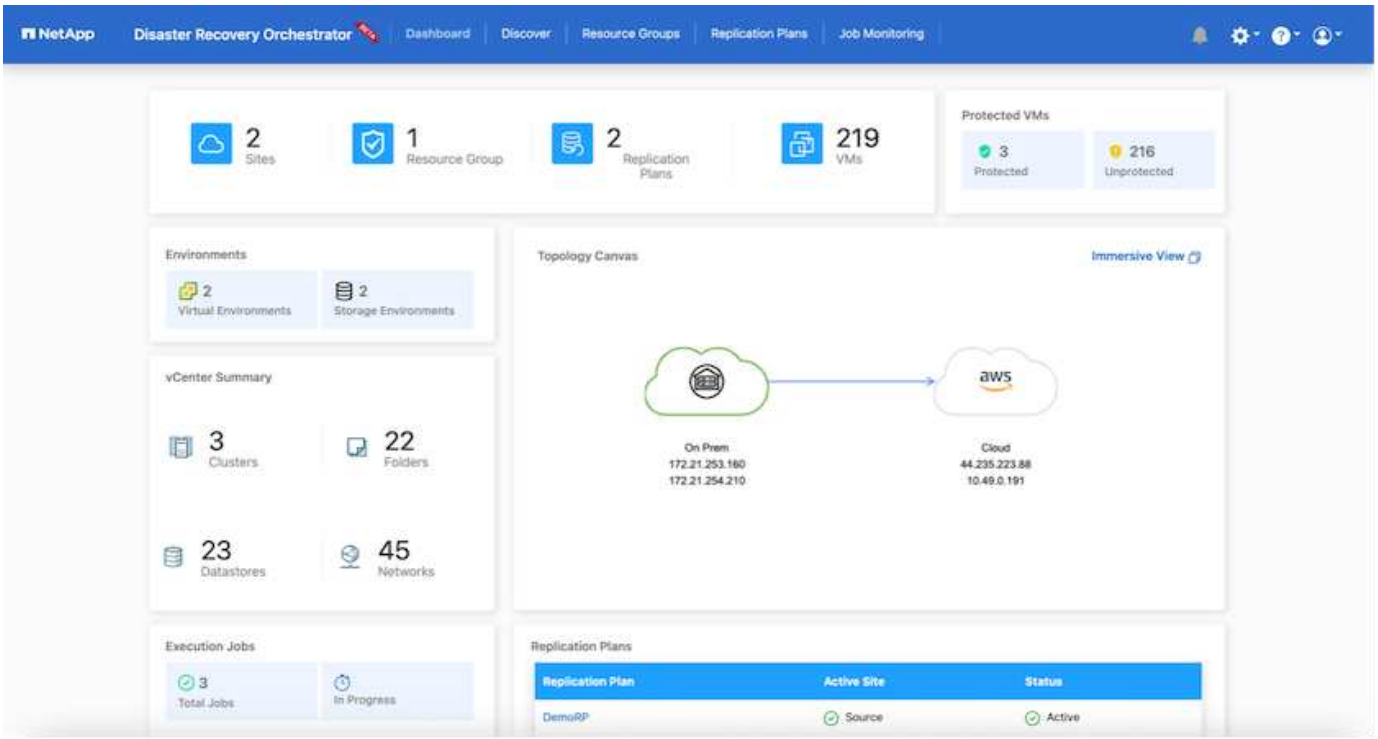
장애 복구는 복제 계획 수준에서 트리거될 수 있습니다. 테스트 장애 조치의 경우, 해체 옵션을 사용하여 변경 사항을 롤백하고 FlexClone 관계를 제거할 수 있습니다. 장애 조치와 관련된 장애 복구는 2단계 프로세스입니다. 복제 계획을 선택하고 *역방향 데이터 동기화*를 선택합니다.



완료되면 장애 복구를 트리거하여 원래 프로덕션 사이트로 돌아갈 수 있습니다.



NetApp Console에서 적절한 볼륨(VMC에 읽기-쓰기 볼륨으로 매핑된 볼륨)의 복제 상태가 중단된 것을 확인할 수 있습니다. 테스트 페일오버 중에는 DRO가 대상 또는 복제본 볼륨을 매핑하지 않습니다. 대신, 필요한 SnapMirror(또는 스냅샷) 인스턴스의 FlexClone 복사본을 만들고 FlexClone 인스턴스를 노출하며, 이는 FSx ONTAP의 추가 물리적 용량을 사용하지 않습니다. 이 프로세스는 볼륨이 수정되지 않도록 보장하며, DR 테스트 또는 분류 워크플로우 중에도 복제 작업이 계속될 수 있도록 합니다. 또한, 이 프로세스는 오류가 발생하거나 손상된 데이터가 복구되는 경우 복제본이 삭제될 위험 없이 복구를 정리할 수 있도록 보장합니다.



랜섬웨어 복구

랜섬웨어로부터 복구하는 것은 힘든 일일 수 있습니다. 특히, IT 조직에서는 안전한 복귀 지점이 어디인지 정확히 파악하기 어려울 수 있으며, 이를 파악한 후에도 잠복해 있는 맬웨어나 취약한 애플리케이션 등의 재발 공격으로부터 복구된 워크로드를 보호하기가 어려울 수 있습니다.

DRO를 사용하면 언제든지 시스템을 복구할 수 있어 이러한 문제를 해결할 수 있습니다. 또한, 남북 트래픽에 노출되지 않은 위치에서 애플리케이션이 작동하고 서로 통신할 수 있도록 작업 부하를 기능적이면서도 격리된 네트워크로 복구할 수도 있습니다. 이를 통해 보안 팀은 법의학 조사를 수행하고 숨겨진 맬웨어나 잠복하고 있는 맬웨어가 없는지 확인할 수 있는 안전한 장소를 확보할 수 있습니다.

이익

- 효율적이고 탄력적인 SnapMirror 복제를 사용합니다.
- 스냅샷 사본 보존을 통해 사용 가능한 어느 시점으로든 복구합니다.
- 저장소, 컴퓨팅, 네트워크 및 애플리케이션 검증 단계에서 수백 개에서 수천 개의 VM을 복구하는 데 필요한 모든 단계를 완전히 자동화합니다.
- 복제된 볼륨을 변경하지 않는 방법을 사용하는 ONTAP FlexClone 기술을 사용하여 워크로드를 복구합니다.
  - 볼륨이나 스냅샷 복사본의 데이터 손상 위험을 방지합니다.
  - DR 테스트 워크플로우 동안 복제 중단을 방지합니다.
  - DR을 넘어 DevTest, 보안 테스트, 패치 또는 업그레이드 테스트, 수정 테스트와 같은 워크플로우를 위해 클라우드 컴퓨팅 리소스를 활용한 DR 데이터의 잠재적 활용.
- CPU 및 RAM을 최적화하여 더 작은 컴퓨팅 클러스터로 복구할 수 있도록 하여 클라우드 비용을 낮추는 데 도움이 됩니다.

AWS의 VMware Cloud와 통합된 Amazon FSx ONTAP SDDC의 클러스터에 연결할 수 있는 NetApp의 ONTAP 파일 시스템을 기반으로 구축된 AWS 관리형 외부 NFS 데이터 저장소입니다. 고객에게 컴퓨팅 리소스에 관계없이 확장 가능한 유연하고 고성능의 가상화된 스토리지 인프라를 제공합니다.

개요

재해 복구 대상으로 VMware Cloud on AWS SDDC를 사용하려는 고객의 경우, FSx ONTAP 데이터 저장소를 사용하면 VM 복제 기능을 제공하는 검증된 타사 솔루션을 사용하여 온프레미스에서 데이터를 복제할 수 있습니다. FSx ONTAP 데이터스토어를 추가하면 스토리지를 수용하기 위해 엄청난 양의 ESXi 호스트를 사용하여 AWS SDDC에 VMware 클라우드를 구축하는 것보다 비용 최적화된 배포가 가능해집니다.

이 접근 방식은 고객이 FSx ONTAP 데이터 저장소와 함께 VMC의 파일럿 라이트 클러스터를 사용하여 VM 복제본을 호스팅하는 데에도 도움이 됩니다. 동일한 프로세스를 VMware Cloud on AWS로 마이그레이션 옵션으로 확장하여 복제 계획을 정상적으로 장애 조치할 수도 있습니다.

문제 진술

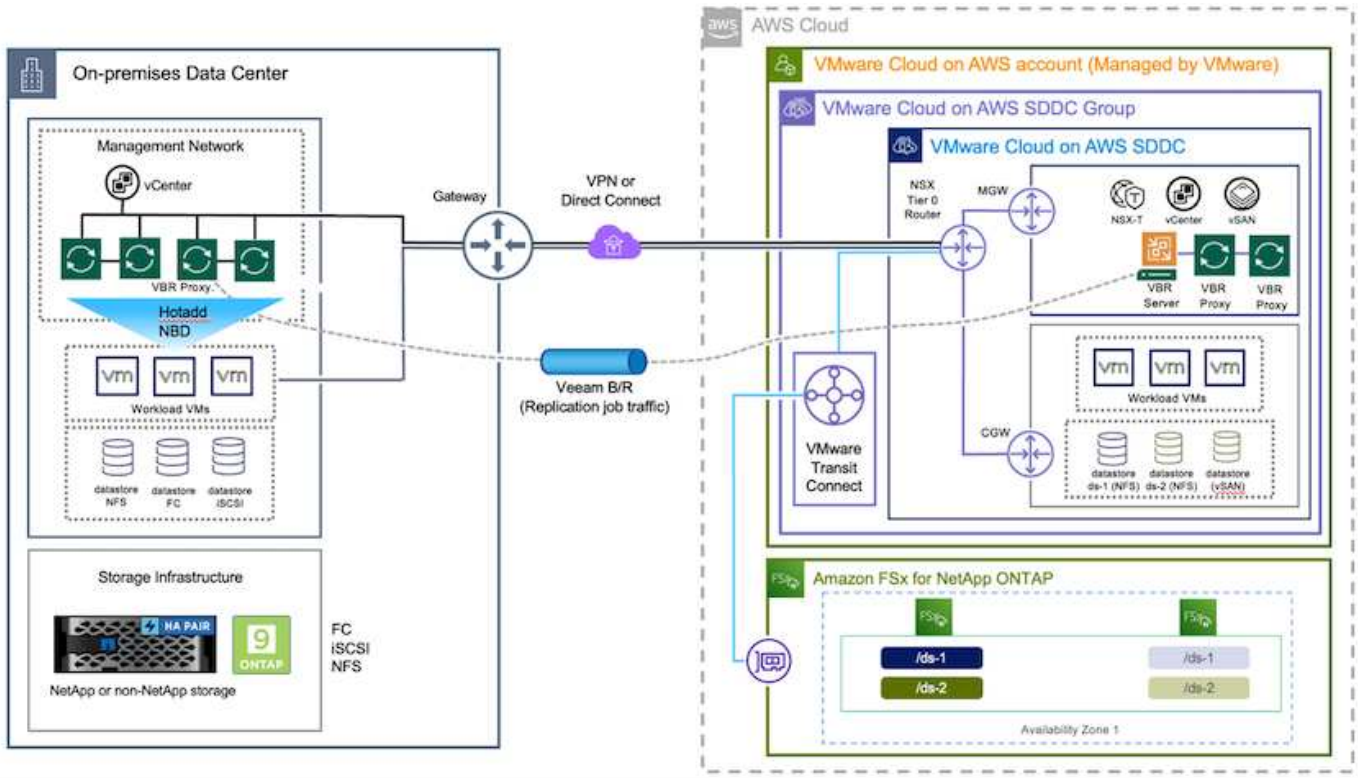
이 문서에서는 FSx ONTAP 데이터 저장소와 Veeam 백업 및 복제를 사용하여 VM 복제 기능을 사용하여 온프레미스 VMware VM을 VMware Cloud on AWS로 재해 복구를 설정하는 방법을 설명합니다.

Veeam Backup & Replication을 사용하면 재해 복구(DR)를 위한 온사이트 및 원격 복제가 가능합니다. 가상 머신이 복제되면 Veeam Backup & Replication은 대상 VMware Cloud on AWS SDDC 클러스터에 기본 VMware vSphere 형식으로 VM의 정확한 복사본을 만들고 복사본을 원본 VM과 동기화된 상태로 유지합니다.

복제는 VM의 복사본이 시작 준비 상태에 있으므로 최상의 복구 시간 목표(RTO) 값을 제공합니다. 이 복제 메커니즘은 재해 발생 시 VMware Cloud on AWS SDDC에서 워크로드를 신속하게 시작할 수 있도록 보장합니다. Veeam Backup & Replication 소프트웨어는 WAN 및 느린 연결을 통한 복제를 위한 트래픽 전송도 최적화합니다. 또한 중복 데이터 블록, 제로 데이터 블록, 스왑 파일 및 제외된 VM 게스트 OS 파일을 필터링하고 복제 트래픽을 압축합니다.

복제 작업이 전체 네트워크 대역폭을 소모하는 것을 방지하려면 WAN 가속기와 네트워크 제한 규칙을 적용할 수 있습니다. Veeam Backup & Replication의 복제 프로세스는 작업 중심입니다. 즉, 복제는 복제 작업을 구성하여 수행됩니다. 재해가 발생하는 경우 복제본으로 장애 조치를 취하여 VM을 복구할 수 있습니다.

장애 조치가 수행되면 복제된 VM이 원래 VM의 역할을 대신하게 됩니다. 장애 조치는 복제본의 최신 상태나 잘 알려진 복원 지점으로 수행할 수 있습니다. 이를 통해 필요에 따라 랜섬웨어 복구나 분리된 테스트가 가능합니다. Veeam Backup & Replication에서 장애 조치(failover)와 장애 복구(failback)는 추후에 마무리되어야 하는 임시적인 중간 단계입니다. Veeam Backup & Replication은 다양한 재해 복구 시나리오를 처리하기 위한 여러 가지 옵션을 제공합니다.



솔루션 배포

높은 수준의 단계

1. Veeam Backup and Replication 소프트웨어는 적절한 네트워크 연결을 갖춘 온프레미스 환경에서 실행됩니다.
2. VMware Cloud on AWS를 구성하려면 VMware Cloud Tech Zone 문서 "Amazon FSx ONTAP 배포 가이드와 VMware Cloud on AWS 통합"를 참조하여 VMware Cloud on AWS SDDC를 배포하고 FSx ONTAP을 NFS 데이터스토어로 구성하십시오. (최소한의 구성으로 설정된 파일럿 라이트 환경을 DR 목적으로 사용할 수 있습니다. 인시던트 발생 시 VM이 이 클러스터로 페일오버되며, 추가 노드를 추가할 수 있습니다.)
3. Veeam Backup and Replication을 사용하여 VM 복제본을 생성하기 위한 복제 작업을 설정합니다.
4. 장애 조치 계획을 수립하고 장애 조치를 수행합니다.
5. 재해 이벤트가 완료되고 기본 사이트가 가동되면 프로덕션 VM으로 다시 전환합니다.

VMC 및 FSx ONTAP 데이터 저장소에 대한 Veeam VM 복제를 위한 필수 구성 요소

1. Veeam Backup & Replication 백업 VM이 AWS SDDC 클러스터의 소스 vCenter와 대상 VMware 클라우드에 연결되어 있는지 확인하세요.
2. 백업 서버는 짧은 이름을 확인하고 소스 및 대상 vCenter에 연결할 수 있어야 합니다.
3. 대상 FSx ONTAP 데이터 저장소에는 복제된 VM의 VMDK를 저장할 수 있는 충분한 여유 공간이 있어야 합니다.

추가 정보는 "고려사항 및 제한사항"을 참조하세요."여기" .

배포 세부 정보

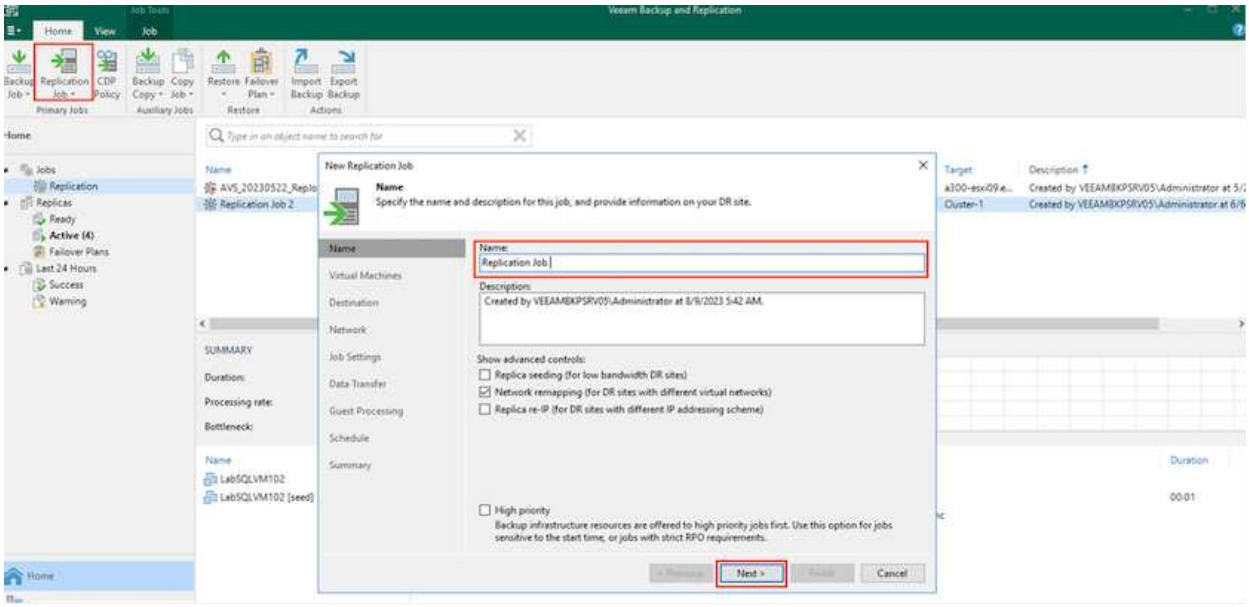
▼ **1**단계**: VM** 복제

Veeam Backup & Replication은 VMware vSphere 스냅샷 기능을 활용하며 복제 중에 Veeam Backup &

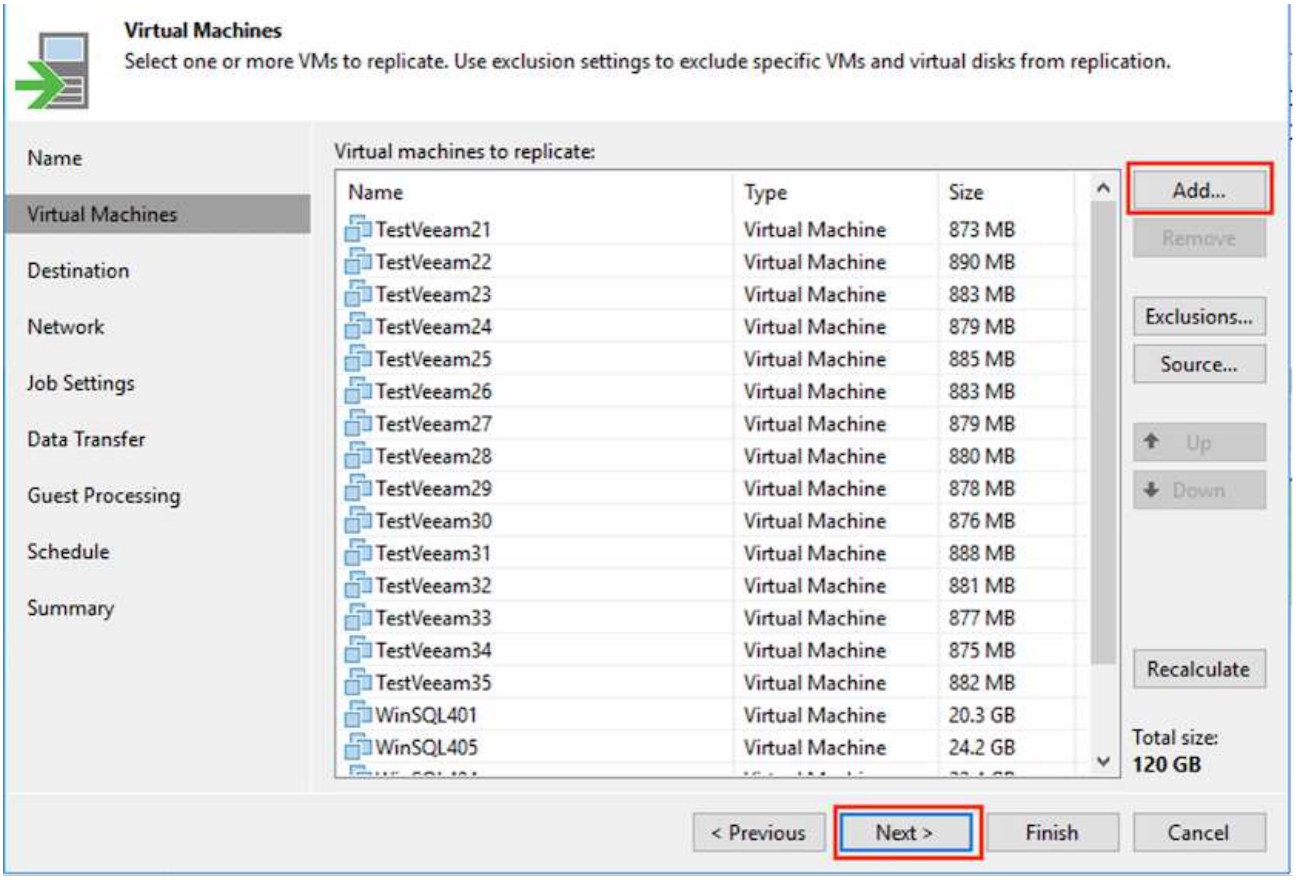
Replication은 VMware vSphere에 VM 스냅샷을 생성하도록 요청합니다. VM 스냅샷은 가상 디스크, 시스템 상태, 구성 등을 포함하는 VM의 특정 시점 복사본입니다. Veeam Backup & Replication은 복제를 위한 데이터 소스로 스냅샷을 사용합니다.

VM을 복제하려면 다음 단계를 따르세요.

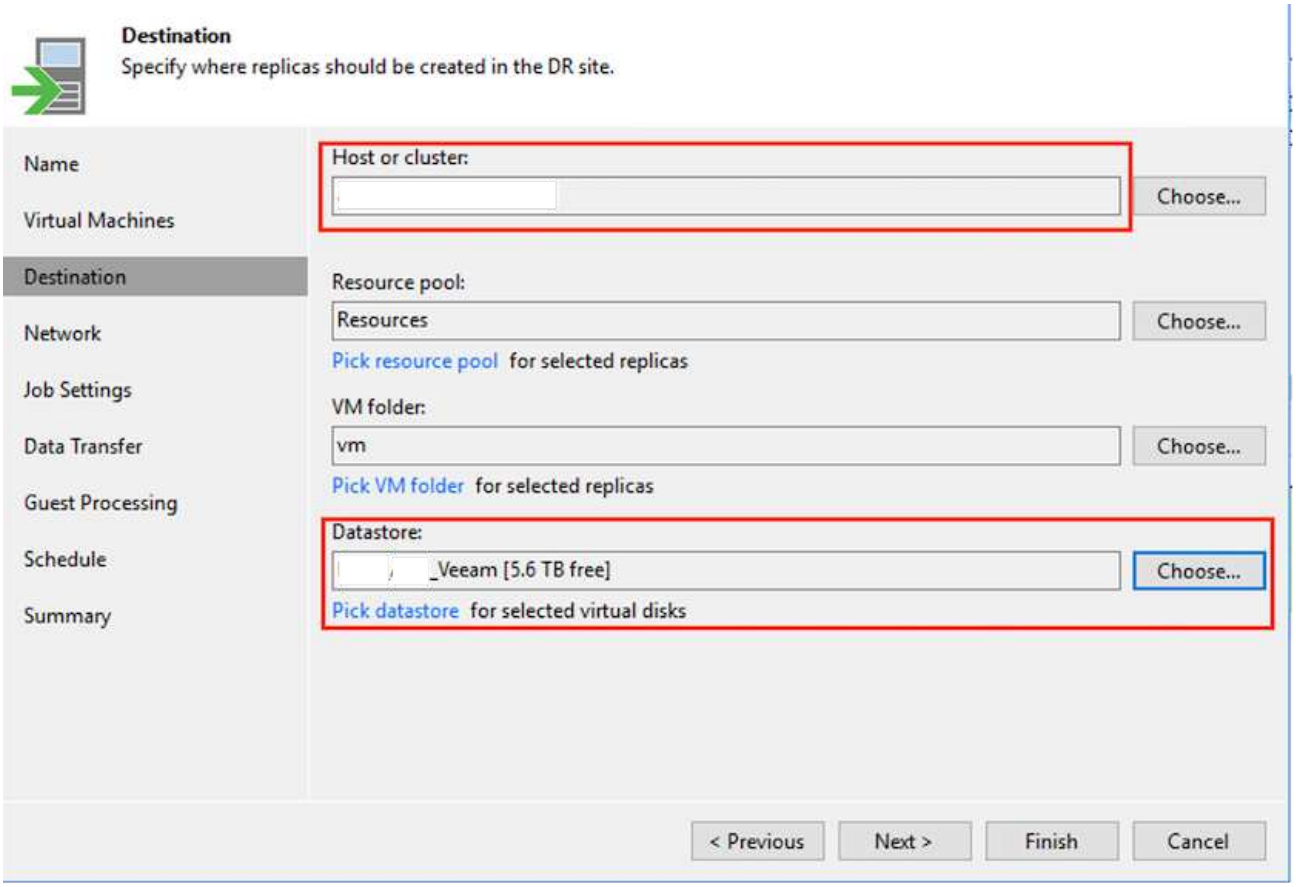
1. Veeam 백업 및 복제 콘솔을 엽니다.
2. 홈 보기에서 복제 작업 > 가상 머신 > VMware vSphere를 선택합니다.
3. 작업 이름을 지정하고 적절한 고급 제어 확인란을 선택합니다. 다음을 클릭하세요.
   - 온프레미스와 AWS 간 연결의 대역폭이 제한된 경우 복제본 시딩 확인란을 선택합니다.
   - VMware Cloud on AWS SDDC의 세그먼트가 온프레미스 사이트 네트워크의 세그먼트와 일치하지 않는 경우 네트워크 재매핑(다른 네트워크를 사용하는 AWS VMC 사이트용) 확인란을 선택합니다.
   - 온프레미스 프로덕션 사이트의 IP 주소 지정 체계가 AWS VMC 사이트의 체계와 다른 경우, 복제본 재IP(IP 주소 지정 체계가 다른 DR 사이트용) 확인란을 선택합니다.



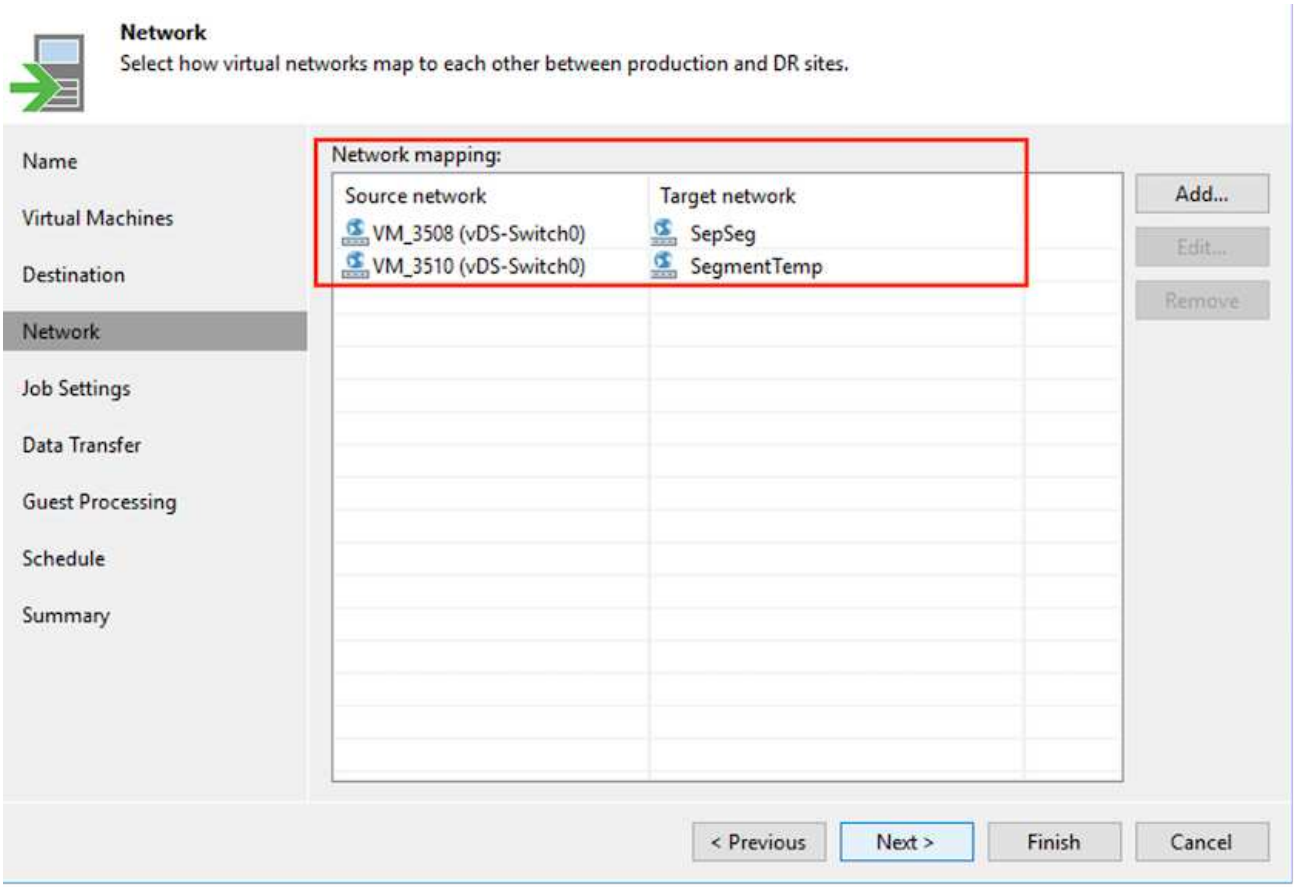
4. 가상 머신 단계에서 VMware Cloud on AWS SDDC에 연결된 FSx ONTAP 데이터 저장소에 복제해야 하는 VM을 선택합니다. 가상 머신을 vSAN에 배치하여 사용 가능한 vSAN 데이터 저장소 용량을 채울 수 있습니다. 파일럿 라이트 클러스터에서는 3노드 클러스터의 사용 가능한 용량이 제한됩니다. 나머지 데이터는 FSx ONTAP 데이터 저장소에 복제될 수 있습니다. 추가*를 클릭한 다음, *개체 추가 창에서 필요한 VM이나 VM 컨테이너를 선택하고 *추가*를 클릭합니다. *다음*을 클릭하세요.



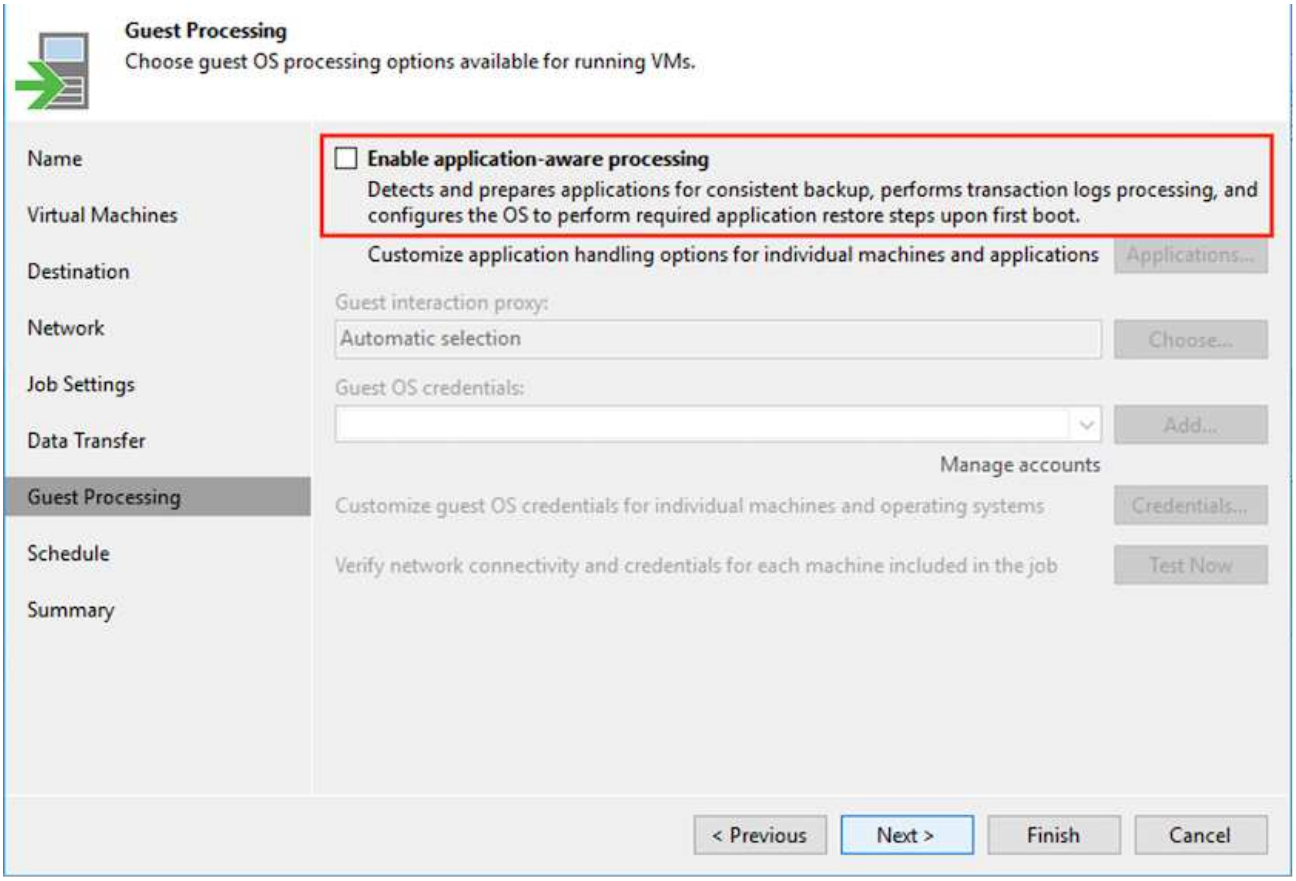
5. 그런 다음 대상을 VMware Cloud on AWS SDDC 클러스터/호스트로 선택하고, VM 복제본에 대한 적절한 리소스 풀, VM 폴더 및 FSx ONTAP 데이터 저장소를 선택합니다. 그런 다음 *다음*을 클릭하세요.



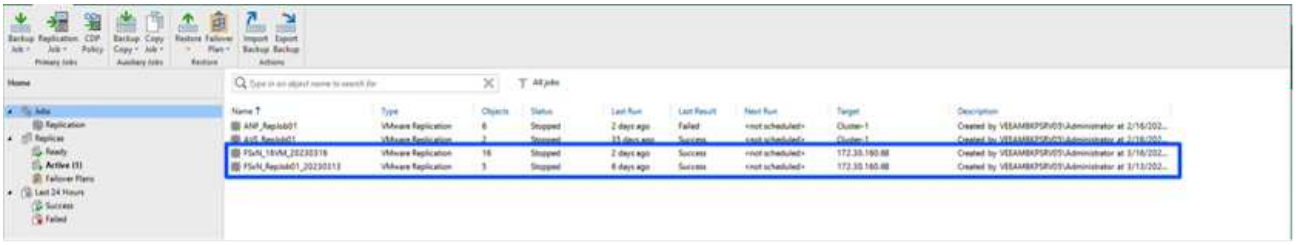
6. 다음 단계에서는 필요에 따라 소스 및 대상 가상 네트워크 간의 매핑을 만듭니다.



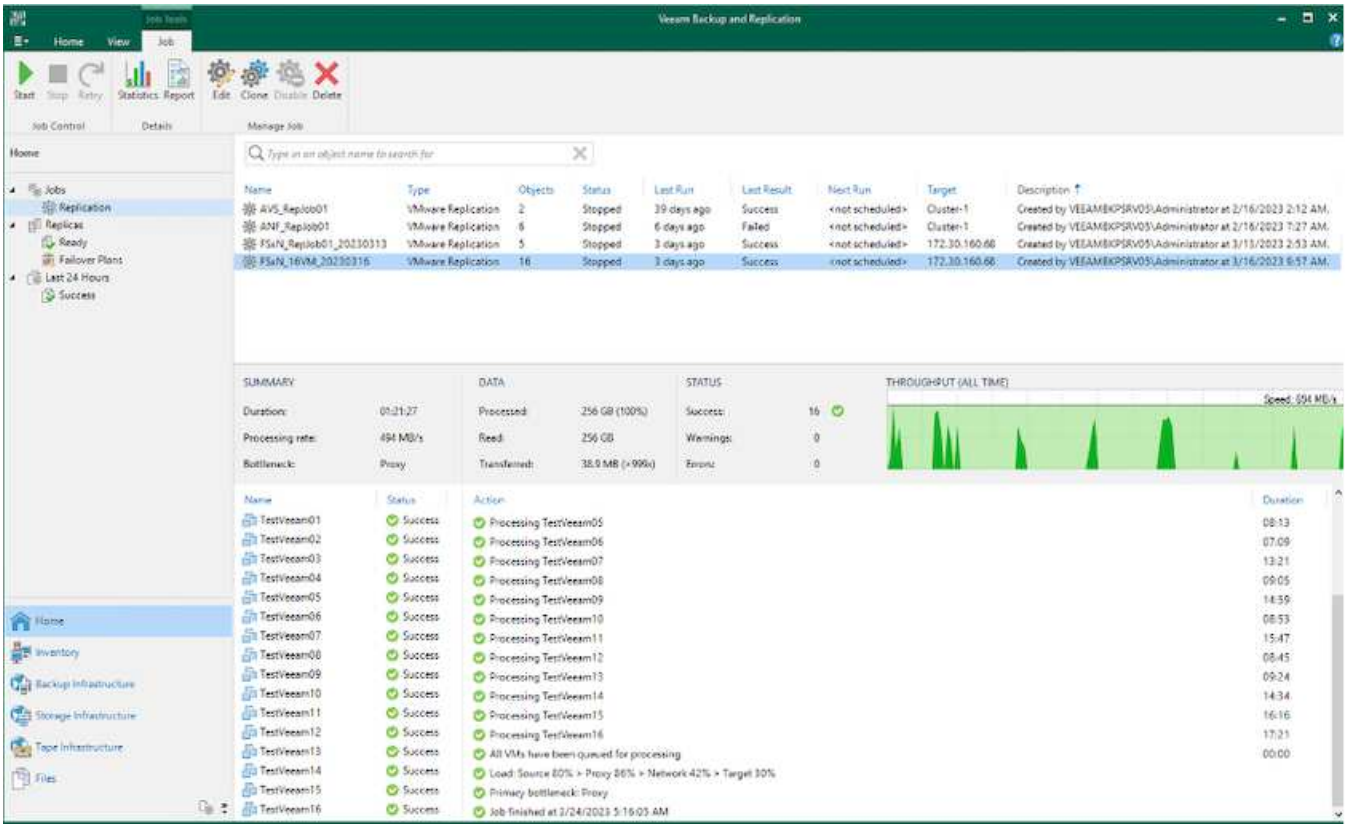
7. 작업 설정 단계에서 VM 복제본, 보존 정책 등의 메타데이터를 저장할 백업 저장소를 지정합니다.
8. 데이터 전송 단계에서 소스 및 대상 프록시 서버를 업데이트하고 자동 선택(기본값)을 그대로 두고 직접 옵션을 선택된 상태로 두고 *다음*을 클릭합니다.
9. 게스트 처리 단계에서 필요에 따라 애플리케이션 인식 처리 사용 옵션을 선택합니다. *다음*을 클릭하세요.



10. 정기적으로 복제 작업을 실행하려면 복제 일정을 선택하세요.
11. 마법사의 요약 단계에서 복제 작업의 세부 정보를 검토합니다. 마법사를 닫은 직후 작업을 시작하려면 마침을 클릭하면 작업 실행 확인란을 선택하고, 그렇지 않으면 확인란을 선택하지 않습니다. 그런 다음 *마침*을 클릭하여 마법사를 닫습니다.



복제 작업이 시작되면 지정된 접미사가 있는 VM이 대상 VMC SDDC 클러스터/호스트에 채워집니다.



Veeam 복제에 대한 추가 정보는 다음을 참조하세요."복제 작동 방식" .

▼ **2**단계**:** 장애 조치 계획 만들기

초기 복제 또는 시딩이 완료되면 장애 조치 계획을 만듭니다. 장애 조치 계획은 종속된 VM에 대해 하나씩 또는 그룹별로 자동으로 장애 조치를 수행하는 데 도움이 됩니다. 장애 조치 계획은 부팅 지연을 포함하여 VM이 처리되는 순서에 대한 청사진입니다. 장애 조치 계획은 또한 중요한 종속 VM이 이미 실행 중인지 확인하는 데 도움이 됩니다.

계획을 생성하려면 복제본이라는 새 하위 섹션으로 이동하여 장애 조치 계획을 선택합니다. 적절한 VM을 선택하세요. Veeam Backup & Replication은 이 시점에 가장 가까운 복원 지점을 찾아 이를 사용하여 VM 복제본을 시작합니다.

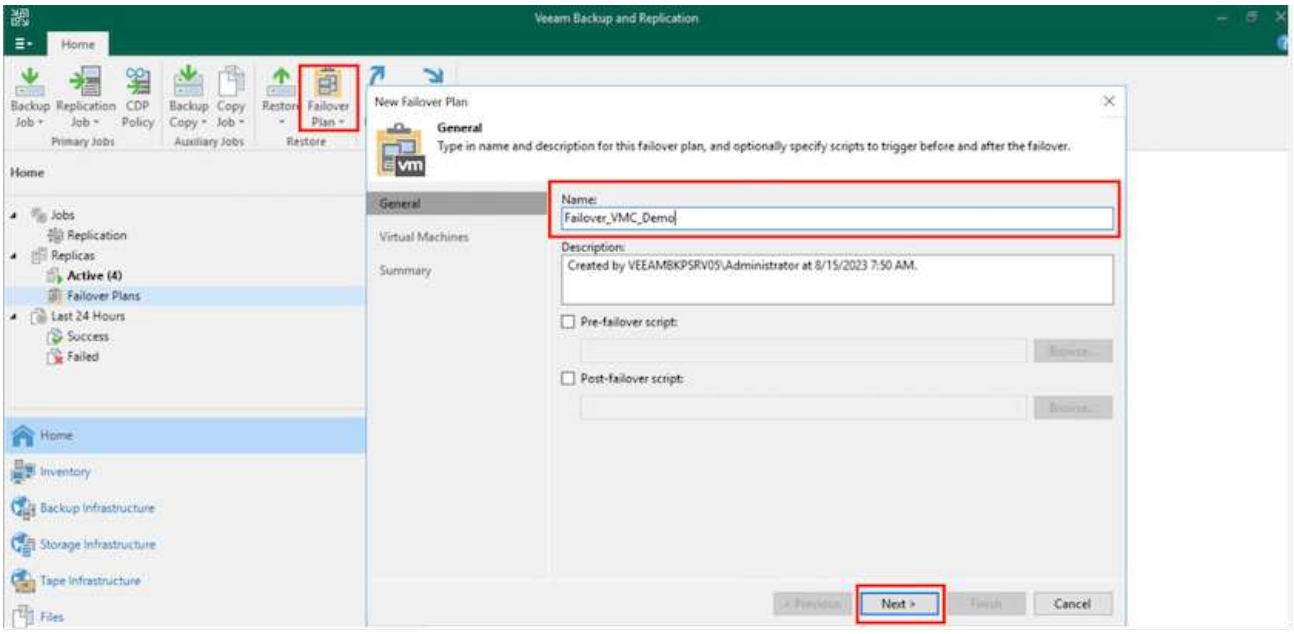
ⓘ 장애 조치 계획은 초기 복제가 완료되고 VM 복제본이 준비 상태가 된 후에만 추가할 수 있습니다.

ⓘ 장애 조치 계획을 실행할 때 동시에 시작할 수 있는 VM의 최대 수는 10개입니다.

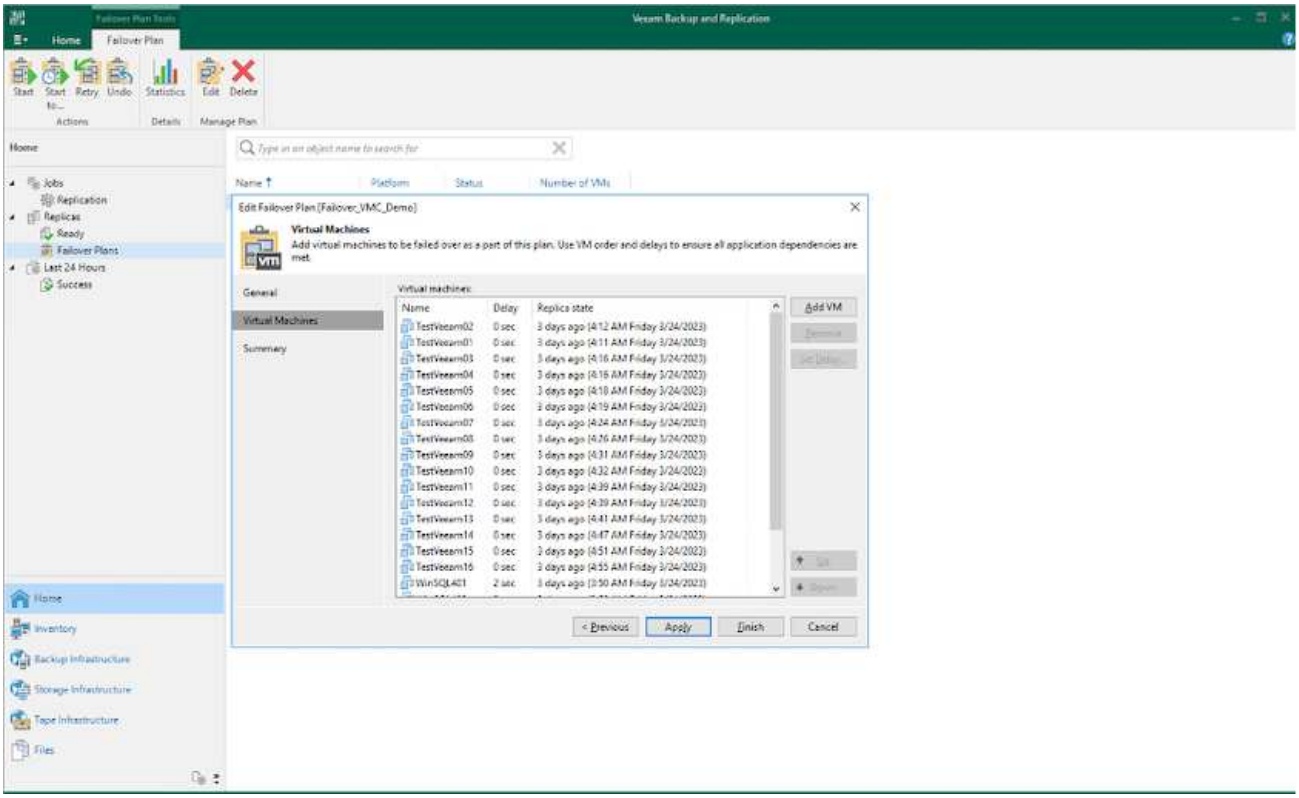
ⓘ 장애 조치 프로세스 동안 소스 VM의 전원은 꺼지지 않습니다.

*장애 조치 계획*을 생성하려면 다음을 수행하세요.

1. 홈 보기에서 *장애 조치 계획 > VMware vSphere*를 선택합니다.
2. 다음으로, 계획의 이름과 설명을 입력하세요. 필요에 따라 사전 및 사후 장애 조치 스크립트를 추가할 수 있습니다. 예를 들어, 복제된 VM을 시작하기 전에 VM을 종료하는 스크립트를 실행합니다.



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



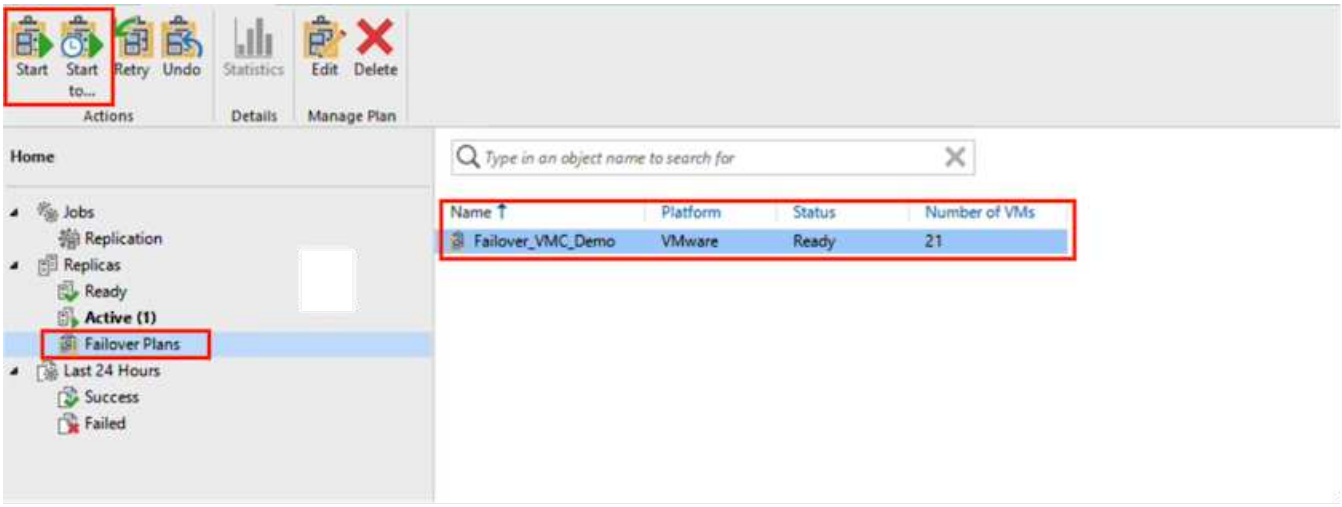
복제 작업 생성에 대한 추가 정보는 다음을 참조하세요."복제 작업 생성" .

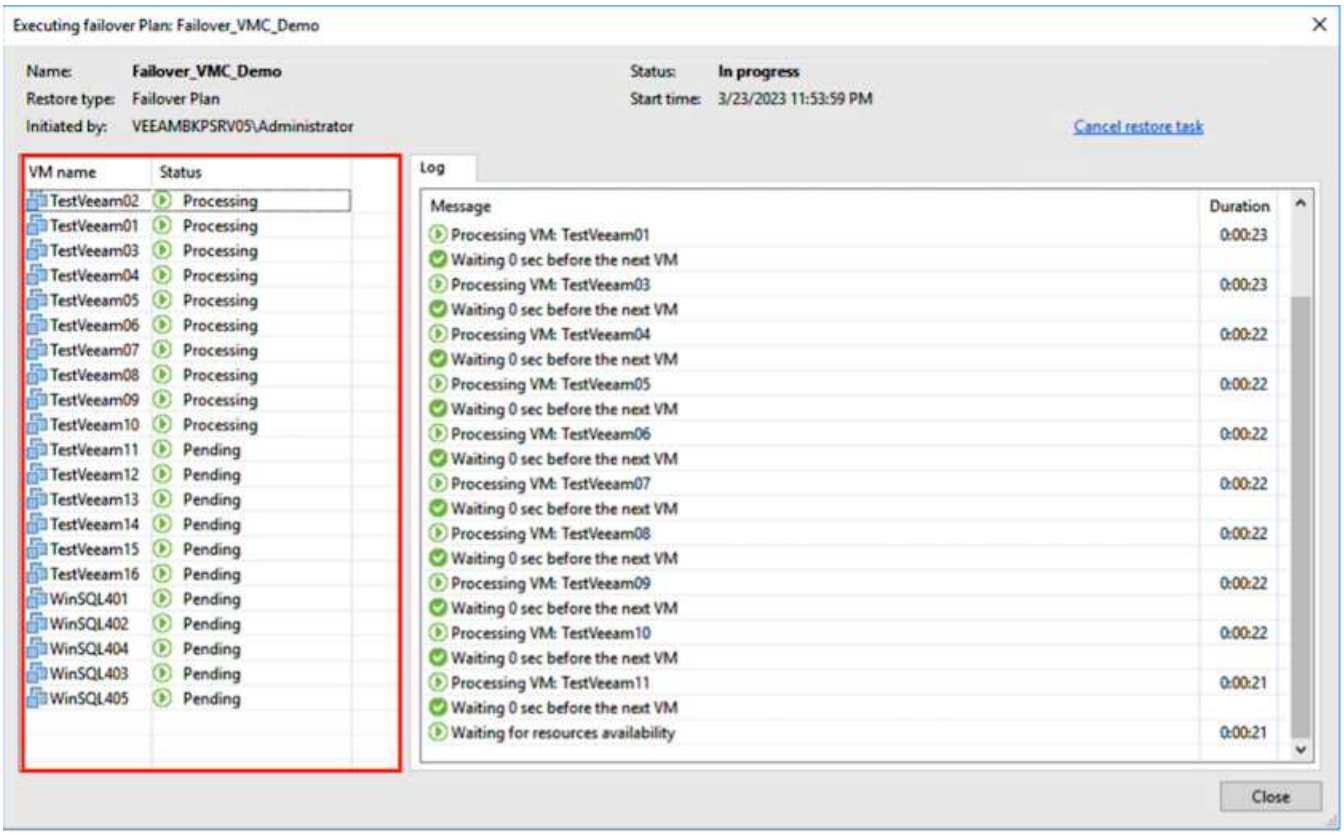
▼ **3**단계**:** 장애 조치 계획 실행

장애 조치(failover) 중에 프로덕션 사이트의 소스 VM은 재해 복구 사이트의 복제본으로 전환됩니다. 장애 조치 프로세스의 일부로 Veeam Backup & Replication은 VM 복제본을 필요한 복구 지점으로 복원하고 모든 I/O 활동을 소스 VM에서 복제본으로 이동합니다. 복제본은 재난 발생 시뿐만 아니라 DR 훈련을 시뮬레이션하는 데에도 사용할 수 있습니다. 장애 조치 시뮬레이션 중에 소스 VM은 계속 실행됩니다. 필요한 모든 테스트가 수행되면 장애 조치를 취소하고 정상적인 작업으로 돌아갈 수 있습니다.

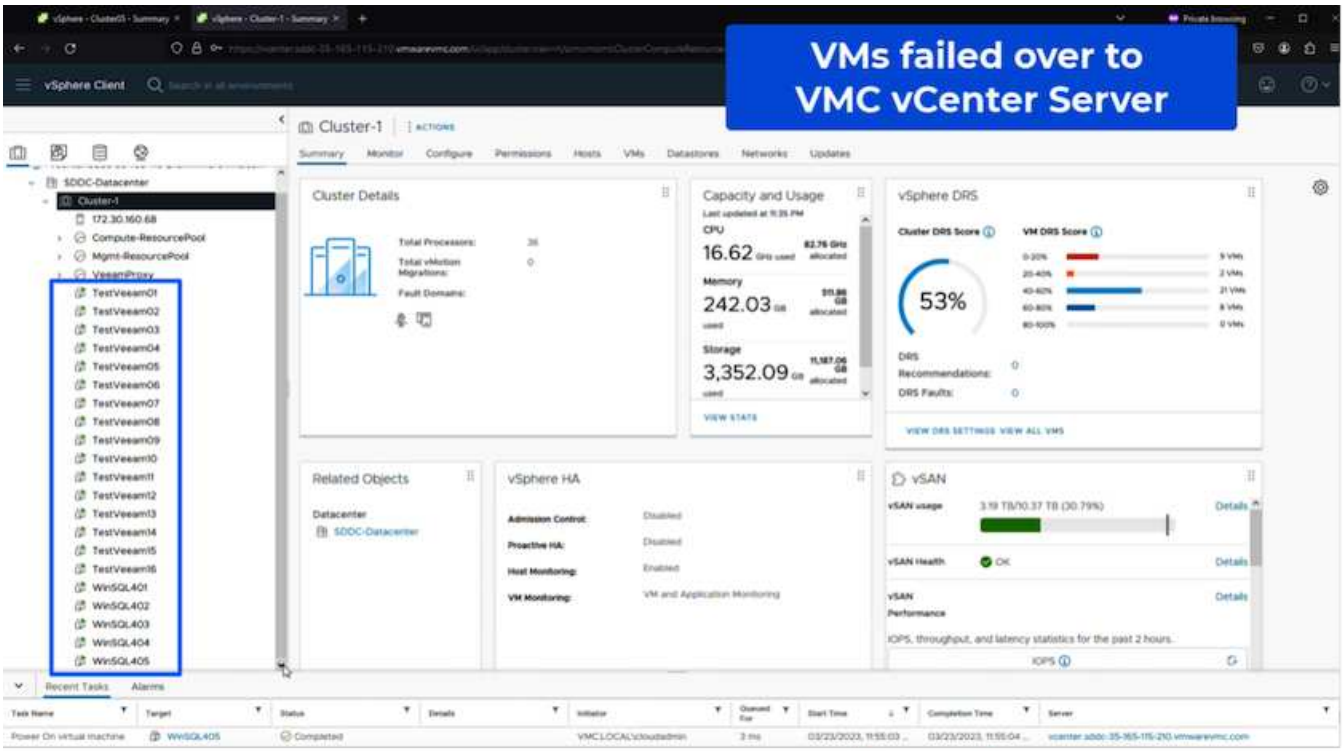
DR 훈련 중 IP 충돌을 피하기 위해 네트워크 분할이 제대로 되어 있는지 확인하세요.

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

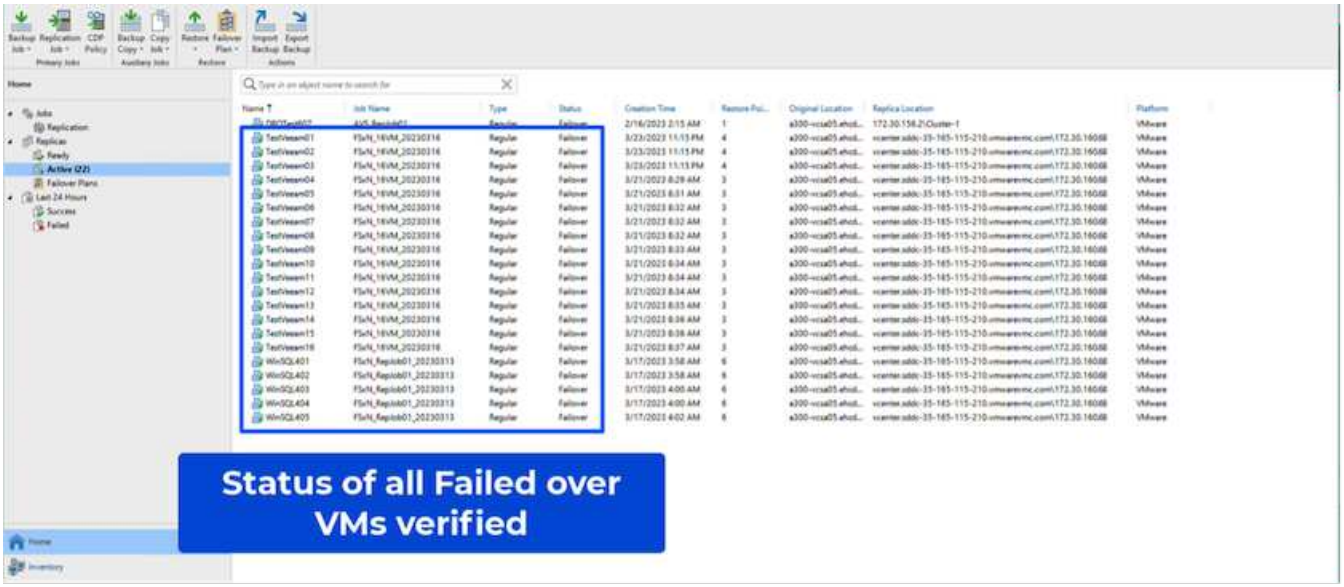




VM 복제본 상태가 준비에서 장애 조치로 변경되고 VM이 대상 VMware Cloud on AWS SDDC 클러스터 /호스트에서 시작됩니다.



장애 조치가 완료되면 VM 상태가 "장애 조치"로 변경됩니다.



Veeam Backup & Replication은 복제본이 준비 상태로 돌아올 때까지 소스 VM에 대한 모든 복제 활동을 중지합니다.

장애 조치 계획에 대한 자세한 내용은 다음을 참조하세요."장애 조치 계획" .

▼ **4**단계**:** 프로덕션 사이트로 장애 복구

장애 조치 계획이 실행 중일 때는 중간 단계로 간주되며 요구 사항에 따라 마무리되어야 합니다. 옵션은 다음과 같습니다.

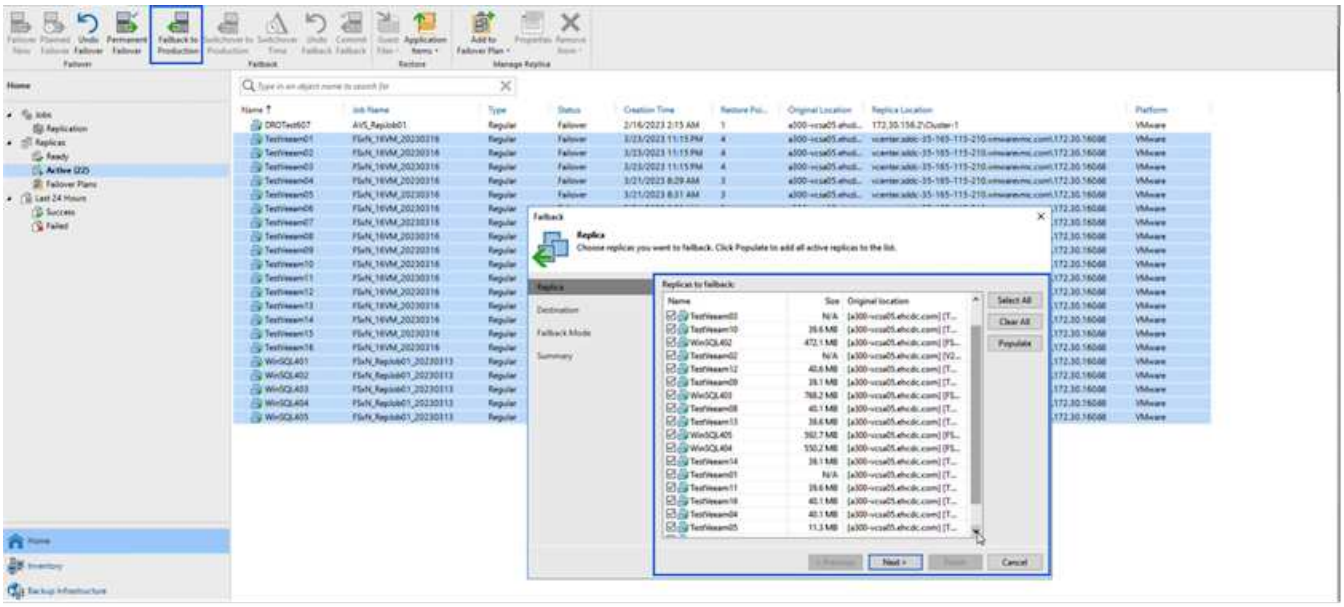
- 운영 환경으로의 장애 복구 - 원래 VM으로 다시 전환하고 VM 복제본이 실행되는 동안 발생한 모든 변경 사항을

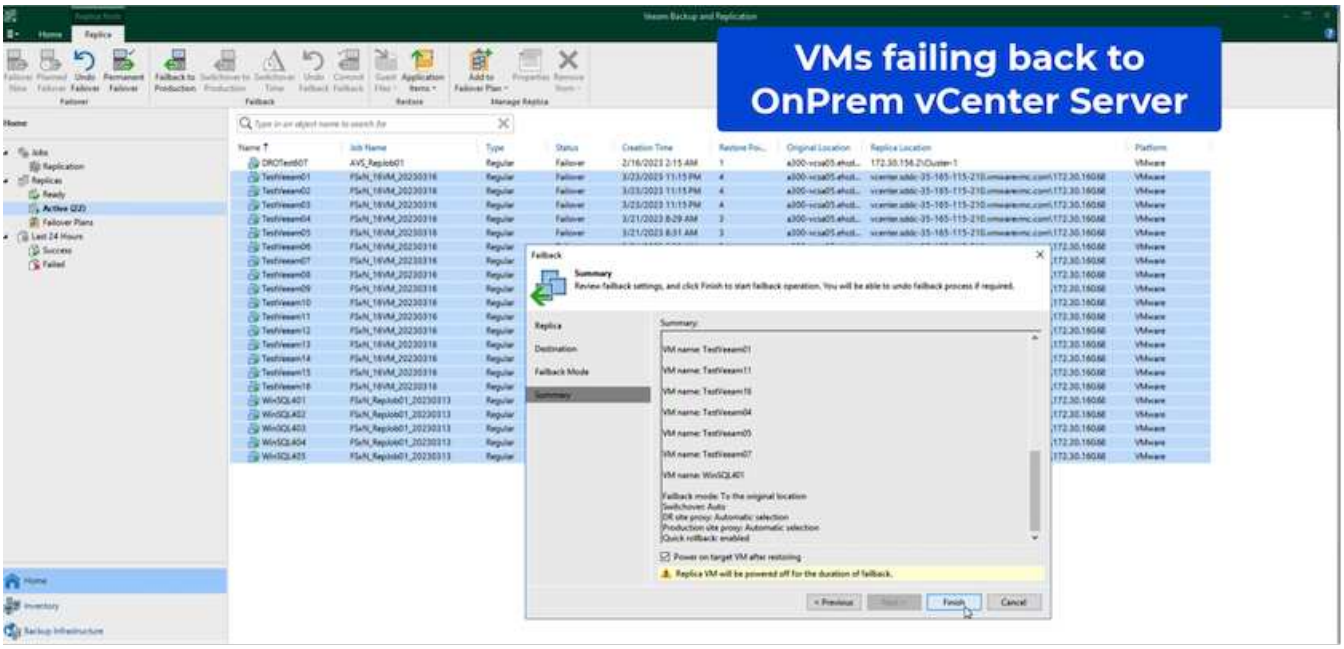
원래 VM으로 전송합니다.

장애 복구를 수행하면 변경 사항은 전송만 되고 게시되지는 않습니다. 원래 VM이 예상대로 작동하는 것이 확인되면 *장애 복구 커밋*을 선택하고, 원래 VM이 예상대로 작동하지 않으면 *장애 복구 실행 취소*를 선택하여 VM 복제본으로 돌아갑니다.

- 장애 조치 취소 - 원래 VM으로 다시 전환하고 실행 중이던 VM 복제본에 적용된 모든 변경 사항을 취소합니다.
- 영구적 장애 조치 - 원본 VM에서 VM 복제본으로 영구적으로 전환하고 이 복제본을 원본 VM으로 사용합니다.

이 데모에서는 프로덕션으로의 장애 복구가 선택되었습니다. 마법사의 대상 단계에서 원래 VM으로의 장애 복구가 선택되었고 "복원 후 VM 전원 켜기" 확인란이 활성화되었습니다.

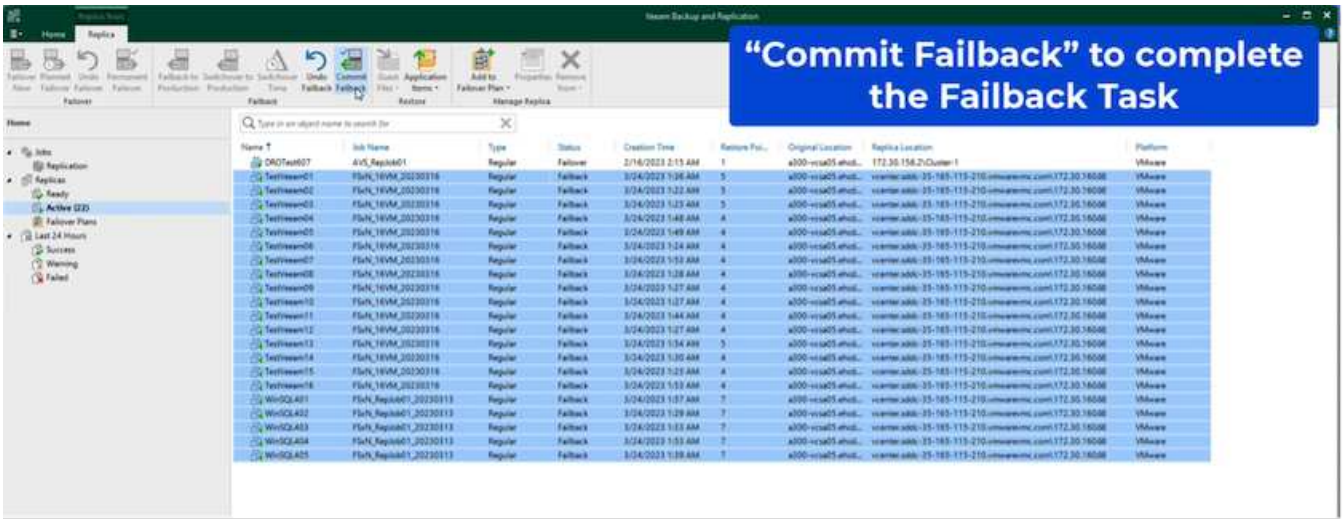


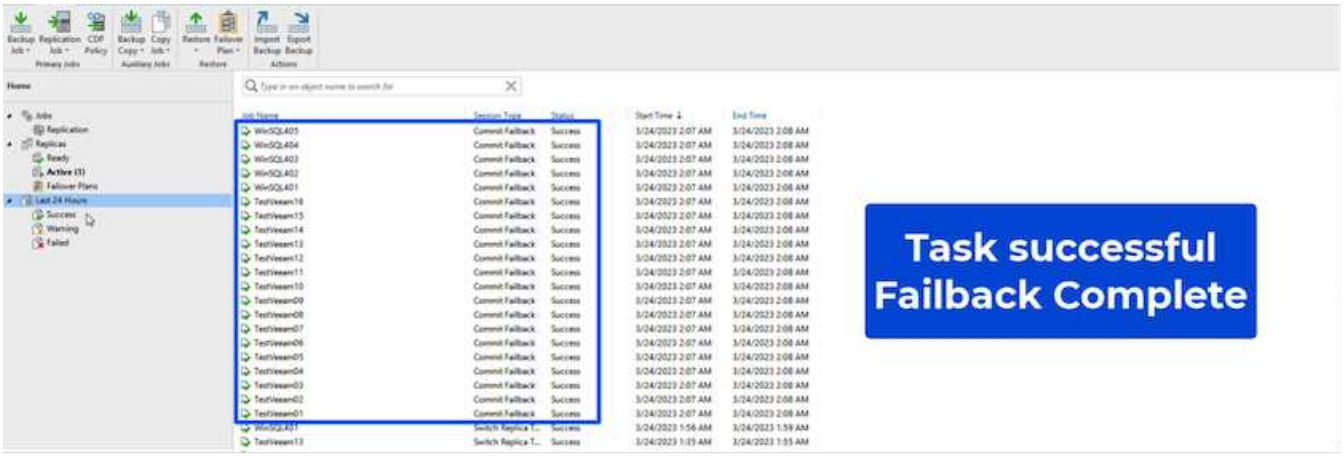


장애 복구 커밋은 장애 복구 작업을 마무리하는 방법 중 하나입니다. 장애 복구가 커밋되면 장애 복구된 VM(프로덕션 VM)에 전송된 변경 사항이 예상대로 작동하는지 확인됩니다. 커밋 작업 후 Veeam Backup & Replication은

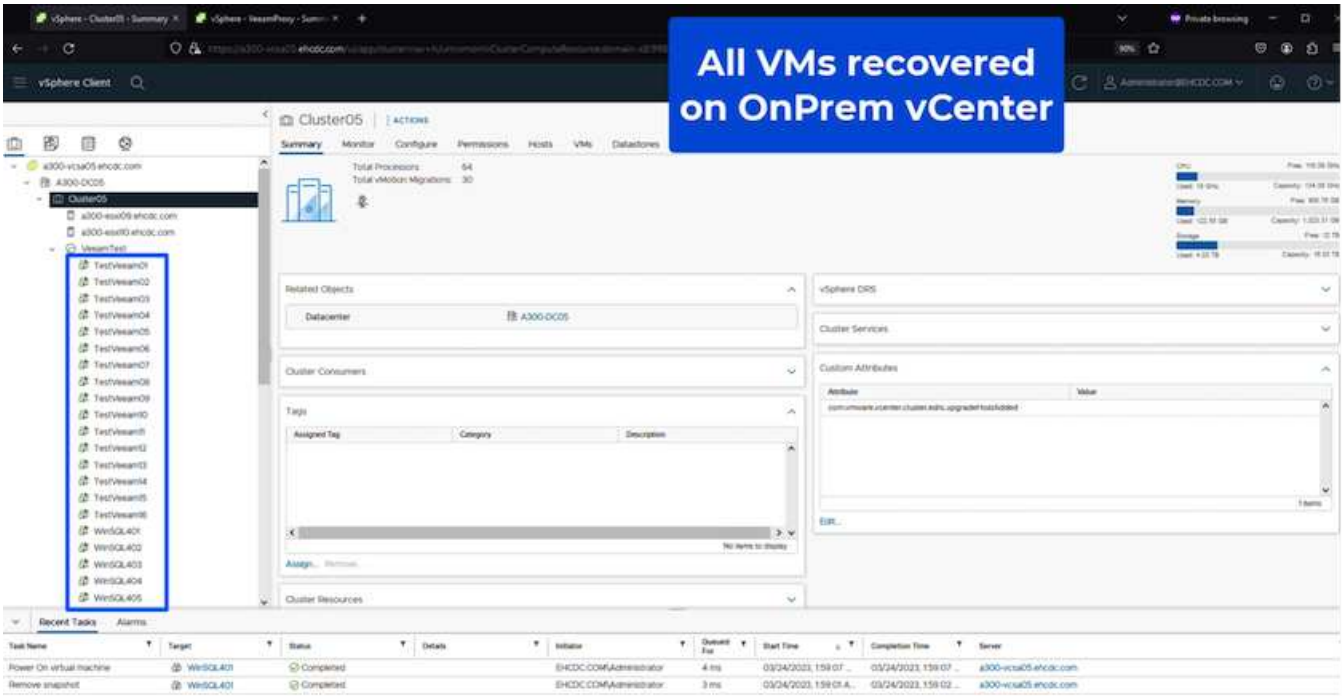
프로덕션 VM에 대한 복제 활동을 재개합니다.

장애 복구 프로세스에 대한 자세한 내용은 Veeam 설명서를 참조하세요."복제를 위한 장애 조치 및 장애 복구" .





운영 환경으로의 장애 복구가 성공적으로 완료되면 모든 VM이 원래 운영 사이트로 복원됩니다.



결론

FSx ONTAP 데이터 저장소 기능을 사용하면 Veeam이나 검증된 타사 도구가 파일럿 라이트 클러스터를 사용하여 저비용 DR 솔루션을 제공할 수 있으며, VM 복제본 사본을 수용하기 위해 클러스터에 많은 수의 호스트를 구축하지 않아도 됩니다. 이를 통해 맞춤형 재해 복구 계획을 처리할 수 있는 강력한 솔루션을 제공하고, 재해 복구 요구 사항을 충족하기 위해 사내 기존 백업 제품을 재사용할 수 있으므로 사내 재해 복구 데이터센터를 종료하고 클라우드 기반 재해 복구가 가능해집니다. 장애 조치는 계획된 장애 조치로 수행할 수도 있고, 재해가 발생하고 DR 사이트를 활성화하기로 결정한 경우 버튼을 클릭하여 장애 조치를 수행할 수도 있습니다.

이 과정에 대해 자세히 알아보려면 자세한 안내 영상을 시청하세요.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a

AWS/VMC에서 워크로드 마이그레이션

TR 4942: VMware HCX를 사용하여 **FSx ONTAP** 데이터 저장소로 워크로드 마이그레이션

Amazon FSx ONTAP 의 보충 NFS 데이터 저장소를 갖춘 Amazon Web Services(AWS)의 VMware Cloud(VMC)에 대한 일반적인 사용 사례는 VMware 워크로드의 마이그레이션입니다. VMware HCX는 선호되는 옵션으로, VMware가 지원하는 모든 데이터 저장소에서 실행되는 온프레미스 가상 머신(VM)과 해당 데이터를 VMC 데이터 저장소로 옮기는 다양한 마이그레이션 방법을 제공합니다. 여기에는 FSx ONTAP 의 보충 NFS 데이터 저장소도 포함됩니다.

개요**: VMware HCX, FSx ONTAP** 추가 데이터 저장소 및 **VMware Cloud**를 사용하여 가상 머신 마이그레이션

VMware HCX는 기본적으로 클라우드 전반의 워크로드 마이그레이션, 워크로드 리밸런싱, 비즈니스 연속성을 간소화하도록 설계된 모빌리티 플랫폼입니다. 이 솔루션은 AWS의 VMware Cloud에 포함되어 있으며, 워크로드를 마이그레이션하는 다양한 방법을 제공하며 재해 복구(DR) 작업에 사용할 수 있습니다.

이 문서에서는 온프레미스와 클라우드 데이터 센터 측에서 모든 주요 구성 요소를 포함하여 VMware HCX를 배포하고 구성하기 위한 단계별 지침을 제공하며, 이를 통해 다양한 VM 마이그레이션 메커니즘을 구현할 수 있습니다.

자세한 내용은 다음을 참조하세요. "VMware HCX 사용자 가이드" 그리고 "설치 체크리스트 B - AWS SDDC 대상 환경에서 VMware Cloud를 사용한 HCX" .

▼ 상위 수준 단계

이 목록은 VMware HCX를 설치하고 구성하는 간단한 단계를 제공합니다.

1. VMware Cloud Services Console을 통해 VMC 소프트웨어 정의 데이터 센터(SDDC)에 대한 HCX를 활성화합니다.
2. 온프레미스 vCenter Server에 HCX Connector OVA 설치 프로그램을 다운로드하여 배포합니다.
3. 라이선스 키로 HCX를 활성화합니다.
4. 온프레미스 VMware HCX Connector를 VMC HCX Cloud Manager와 페어링합니다.
5. 네트워크 프로필, 컴퓨팅 프로필 및 서비스 메시를 구성합니다.
6. (선택 사항) 네트워크 확장을 수행하여 네트워크를 확장하고 재IP를 방지합니다.
7. 기기 상태를 검증하고 마이그레이션이 가능한지 확인하세요.
8. VM 워크로드를 마이그레이션합니다.

▼ 필수 조건

시작하기 전에 다음 전제 조건이 충족되었는지 확인하세요. 자세한 내용은 다음을 참조하세요. "설치 준비" . 연결성을 포함한 전제 조건이 충족되면 VMC의 VMware HCX 콘솔에서 라이선스 키를 생성하여 HCX를 구성하고 활성화합니다. HCX가 활성화되면 vCenter 플러그인이 배포되고 vCenter 콘솔을 사용하여 관리할 수 있습니다.

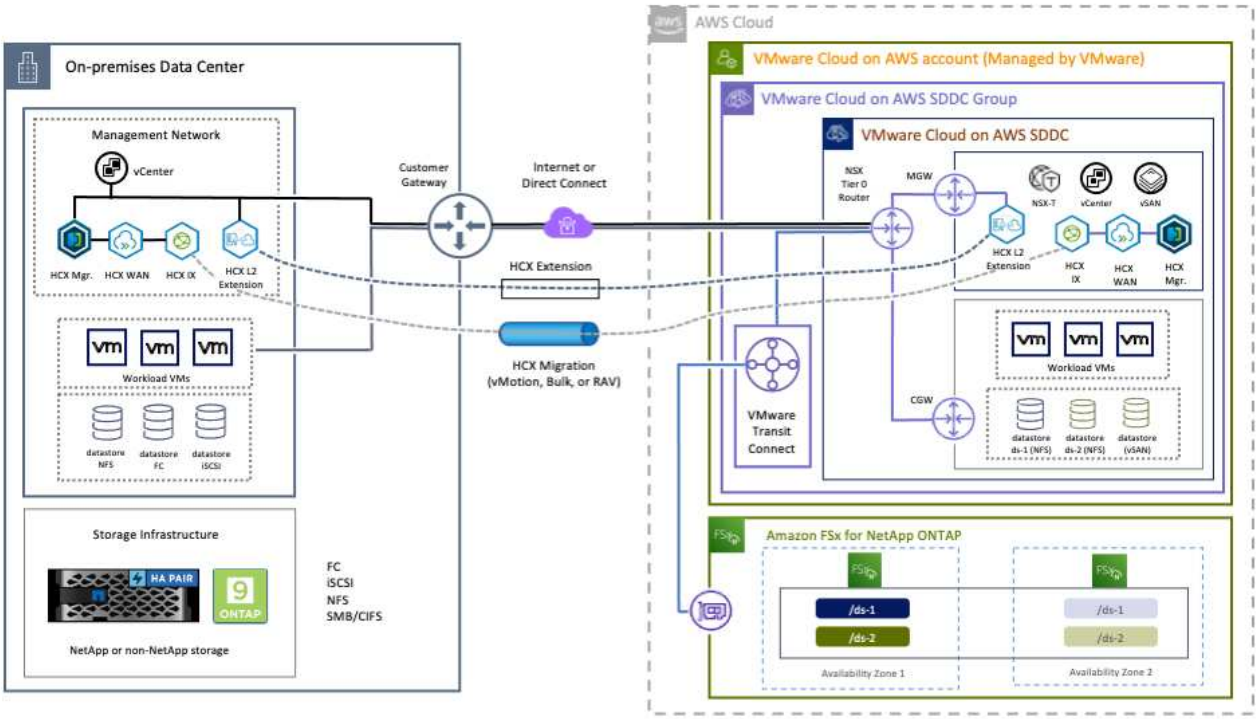
HCX 활성화 및 배포를 진행하기 전에 다음 설치 단계를 완료해야 합니다.

1. 기존 VMC SDDC를 사용하거나 이에 따라 새 SDDC를 만듭니다."NetApp 링크" 아니면 이것 "VMware 링크" .
2. 온프레미스 vCenter 환경에서 VMC SDDC로 가는 네트워크 경로는 vMotion을 사용하여 VM 마이그레이션을 지원해야 합니다.
3. 필수 사항을 확인하세요 "방화벽 규칙 및 포트" 온프레미스 vCenter Server와 SDDC vCenter 간의 vMotion 트래픽에 허용됩니다.
4. FSx ONTAP NFS 볼륨은 VMC SDDC의 보조 데이터 저장소로 마운트되어야 합니다. 적절한 클러스터에 NFS 데이터 저장소를 연결하려면 여기에 설명된 단계를 따르세요."NetApp 링크" 아니면 이것 "VMware 링크" .

▼ 고수준 아키텍처

테스트 목적으로 이 검증에 사용된 온프레미스 랩 환경은 사이트 간 VPN을 통해 AWS VPC에 연결되었으며, 이를 통해 외부 전송 게이트웨이를 통해 온프레미스에서 AWS 및 VMware 클라우드 SDDC로의 연결이 가능해졌습니다. HCX 마이그레이션 및 네트워크 확장 트래픽은 온프레미스와 VMware 클라우드 대상 SDDC 간의 인터넷을 통해 흐릅니다. 이 아키텍처는 Direct Connect 개인 가상 인터페이스를 사용하도록 수정될 수 있습니다.

다음 이미지는 상위 수준의 아키텍처를 보여줍니다.



솔루션 배포

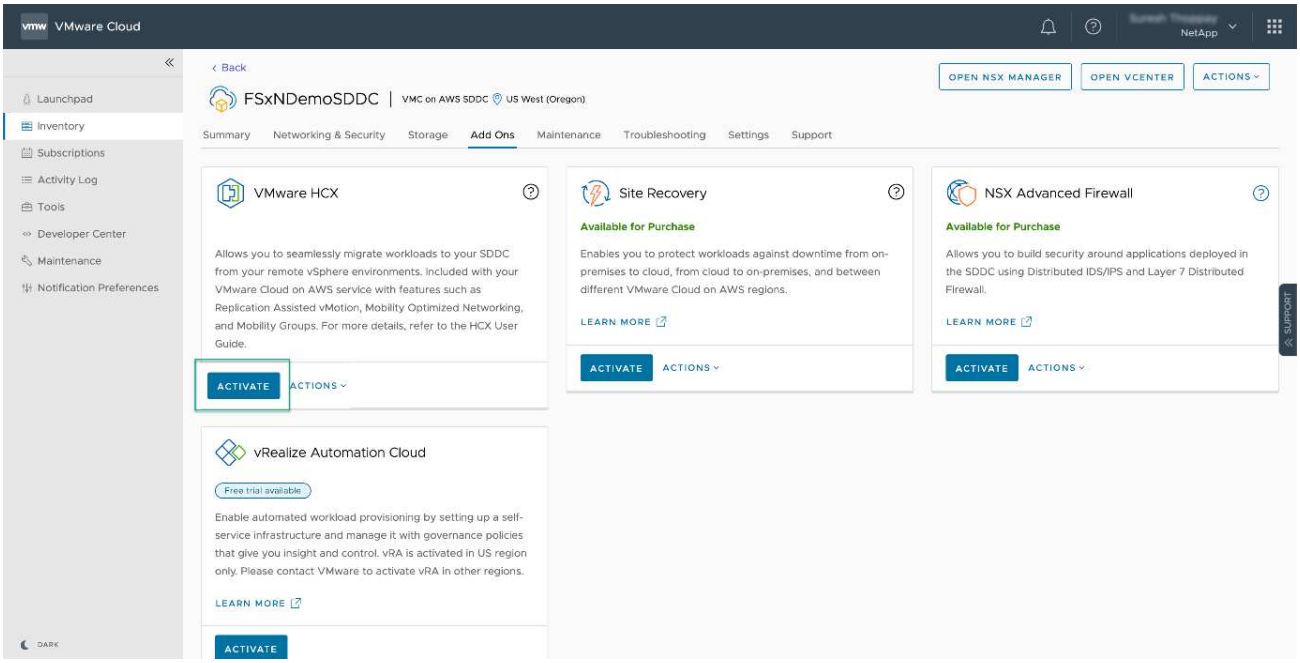
이 솔루션의 배포를 완료하려면 다음 단계를 따르세요.

▼ **1**단계**:** 애드온 옵션을 사용하여 **VMC SDDC**를 통해 **HCX** 활성화

설치를 수행하려면 다음 단계를 완료하세요.

1. VMC 콘솔에 로그인하세요 "vmc.vmware.com" 인벤토리에 액세스하세요.
2. 적절한 SDDC를 선택하고 추가 기능에 액세스하려면 SDDC에서 세부 정보 보기를 클릭하고 추가 기능 탭을 선택하세요.
3. VMware HCX에 대해 활성화를 클릭합니다.

ⓘ 이 단계를 완료하는 데 최대 25분이 걸립니다.

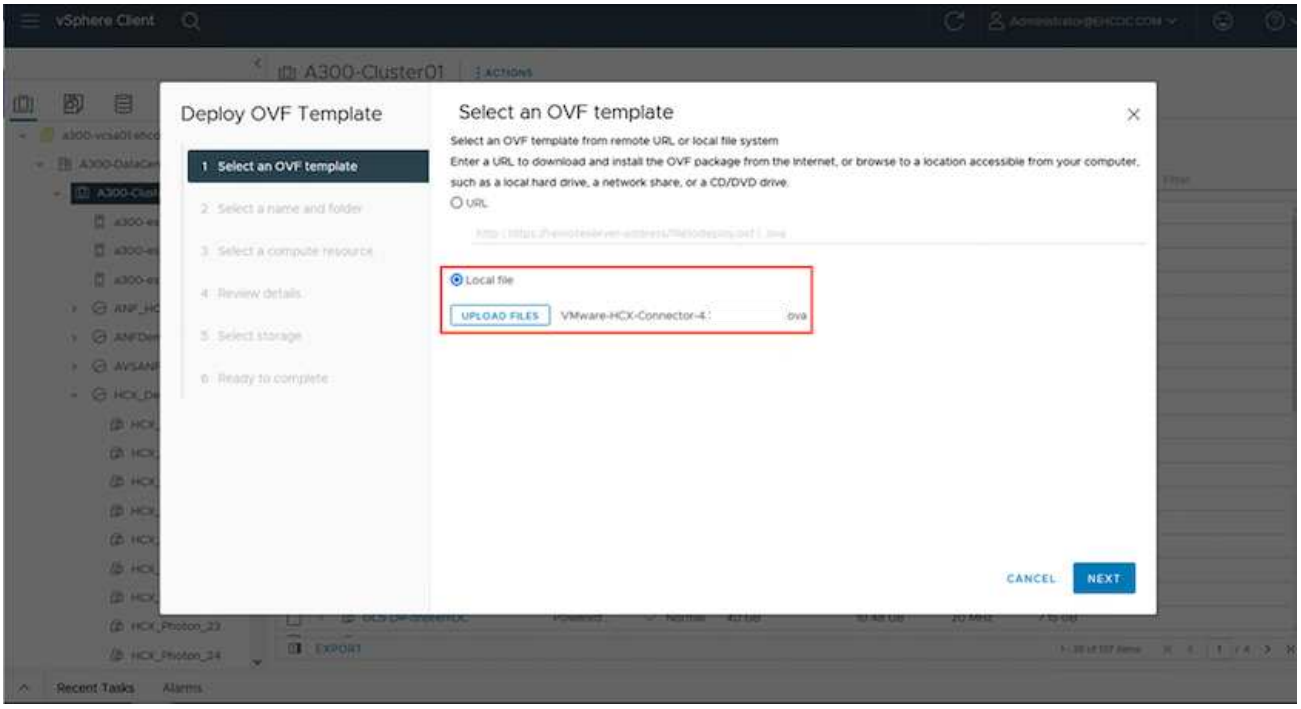


4. 배포가 완료되면 HCX Manager와 관련 플러그인을 vCenter Console에서 사용할 수 있는지 확인하여 배포를 검증합니다.
5. HCX Cloud Manager에 액세스하는 데 필요한 포트를 열려면 적절한 관리 게이트웨이 방화벽을 만듭니다. 이제 HCX Cloud Manager가 HCX 작업을 수행할 준비가 되었습니다.

▼ **2**단계**:** 온프레미스 **vCenter Server**에 설치 프로그램 **OVA** 배포

온프레미스 커넥터가 VMC의 HCX 관리자와 통신하려면 온프레미스 환경에서 적절한 방화벽 포트가 열려 있는지 확인하세요.

1. VMC 콘솔에서 HCX 대시보드로 이동한 후 관리로 가서 시스템 업데이트 탭을 선택합니다. HCX 커넥터 OVA 이미지에 대한 다운로드 링크 요청을 클릭합니다.
2. HCX 커넥터를 다운로드한 후 온프레미스 vCenter Server에 OVA를 배포합니다. vSphere 클러스터를 마우스 오른쪽 버튼으로 클릭하고 OVF 템플릿 배포 옵션을 선택합니다.

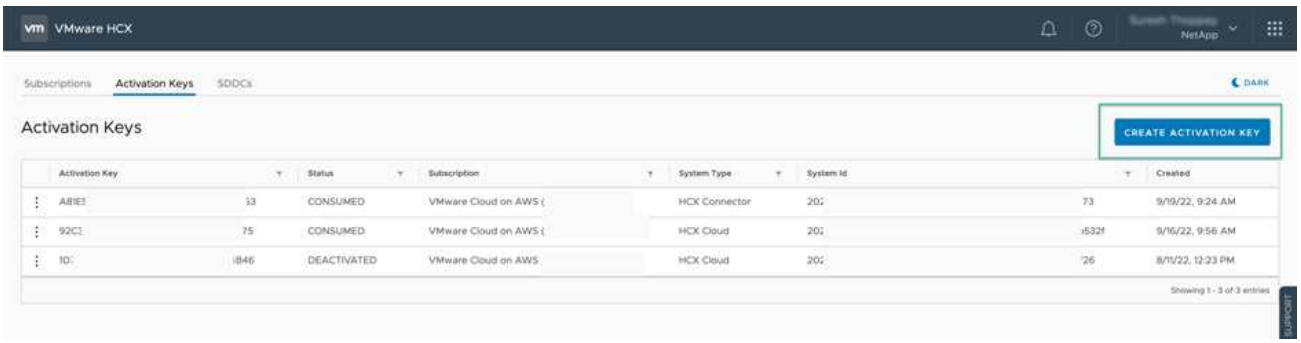


3. OVF 템플릿 배포 마법사에서 필요한 정보를 입력하고 다음을 클릭한 다음 마침을 클릭하여 VMware HCX Connector OVA를 배포합니다.
4. 가상 어플라이언스를 수동으로 켜십시오. 단계별 지침은 다음으로 이동하십시오. "VMware HCX 사용자 가이드" .

▼ **3**단계**:** 라이선스 키로 **HCX** 커넥터 활성화

온프레미스에 VMware HCX Connector OVA를 배포하고 어플라이언스를 시작한 후 다음 단계를 완료하여 HCX Connector를 활성화합니다. VMC의 VMware HCX 콘솔에서 라이선스 키를 생성하고 VMware HCX 커넥터 설정 중에 라이선스를 입력합니다.

1. VMware Cloud Console에서 인벤토리로 이동하여 SDDC를 선택하고 세부 정보 보기를 클릭합니다. VMware HCX 타일의 추가 기능 탭에서 HCX 열기를 클릭합니다.
2. 활성화 키 탭에서 활성화 키 만들기를 클릭합니다. 시스템 유형을 HCX 커넥터로 선택하고 확인을 클릭하면 키가 생성됩니다. 활성화 키를 복사하세요.



온프레미스에 배포된 각 HCX 커넥터에는 별도의 키가 필요합니다.

3. 온프레미스 VMware HCX 커넥터에 로그인하세요. "`https://hcxconnectorIP:9443`" 관리자 자격 증명을 사용합니다.

OVA 배포 중에 정의된 비밀번호를 사용하세요.

4. 라이센스 섹션에서 2단계에서 복사한 활성화 키를 입력하고 활성화를 클릭합니다.

활성화를 성공적으로 완료하려면 온프레미스 HCX 커넥터가 인터넷에 액세스할 수 있어야 합니다.

5. 데이터 센터 위치에서 온프레미스에 VMware HCX Manager를 설치할 위치를 입력합니다. 계속을 클릭하세요.
6. 시스템 이름에서 이름을 업데이트하고 계속을 클릭합니다.
7. 예를 선택한 후 계속을 클릭합니다.
8. 'vCenter 연결'에서 IP 주소나 정규화된 도메인 이름(FQDN)과 vCenter Server의 자격 증명을 입력하고 계속을 클릭합니다.

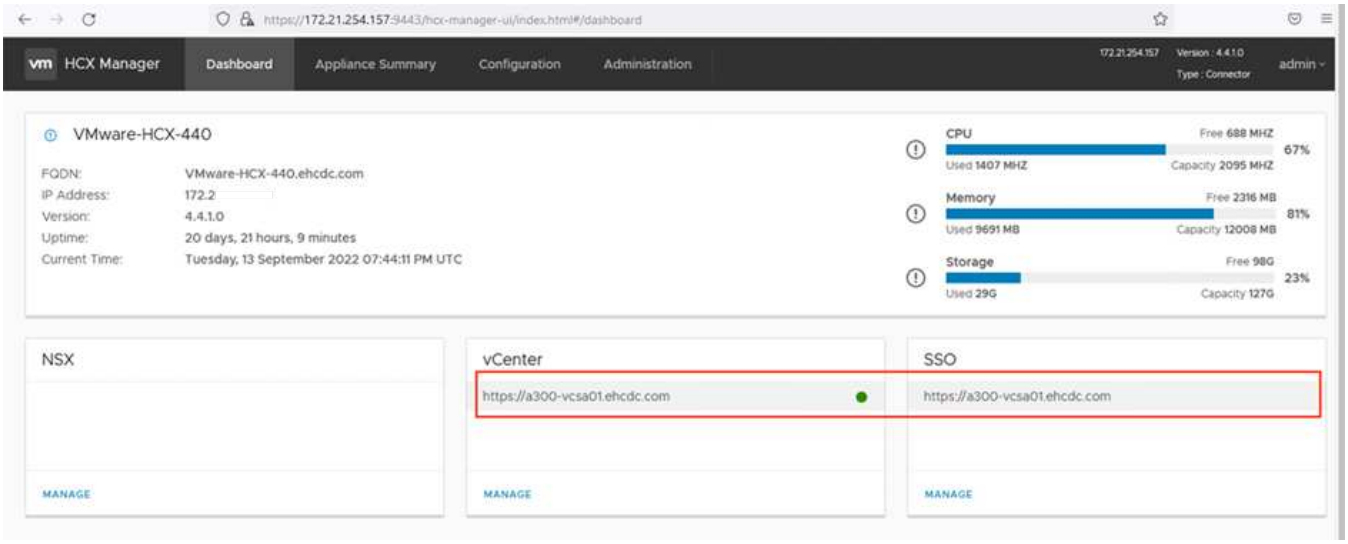
나중에 통신 문제를 피하려면 FQDN을 사용하세요.

9. SSO/PSC 구성에서 Platform Services Controller의 FQDN 또는 IP 주소를 입력하고 계속을 클릭합니다.

vCenter Server의 IP 주소 또는 FQDN을 입력하세요.

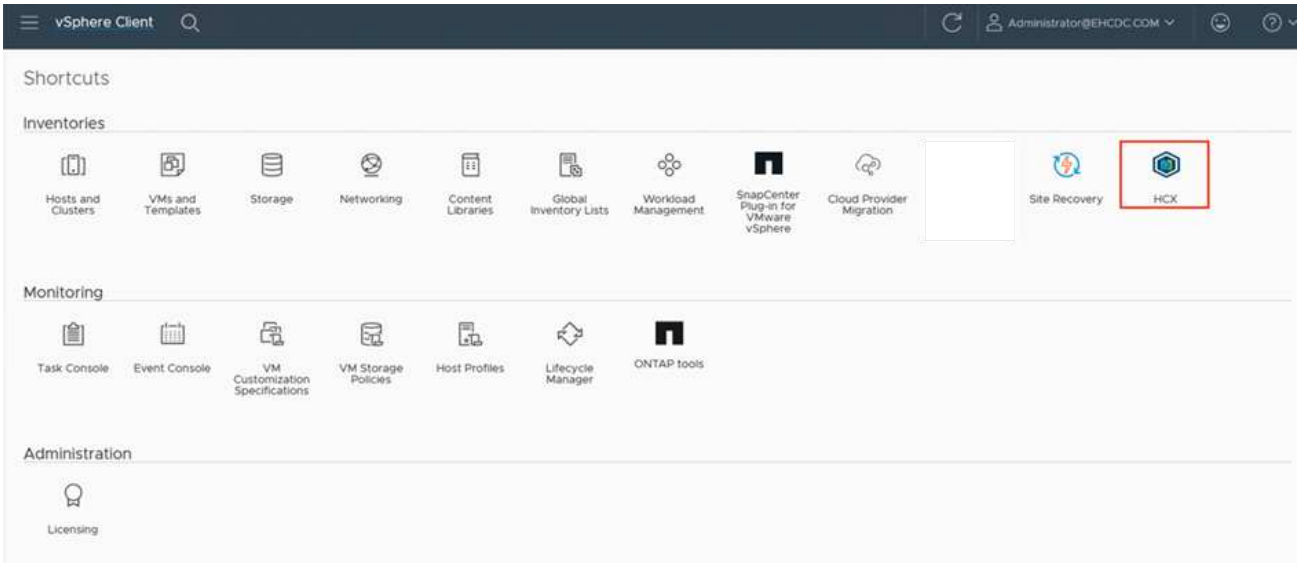
10. 정보가 올바르게 입력되었는지 확인하고 다시 시작을 클릭하세요.
11. 완료되면 vCenter Server가 녹색으로 표시됩니다. vCenter Server와 SSO 모두 올바른 구성 매개변수를 가져야 하며, 이는 이전 페이지와 동일해야 합니다.

이 프로세스는 약 10~20분 정도 걸리며 플러그인이 vCenter Server에 추가됩니다.

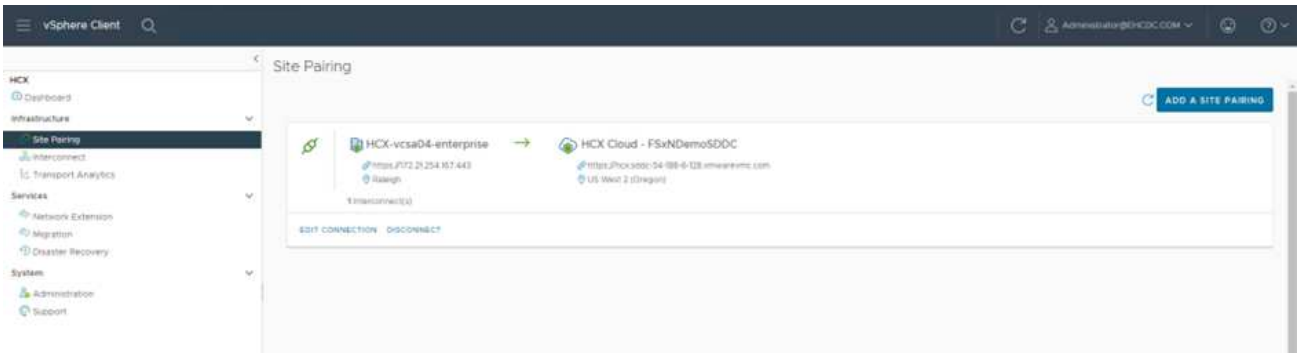


▼ **4**단계**:** 온프레미스 **VMware HCX** 커넥터를 **VMC HCX Cloud Manager**와 페어링

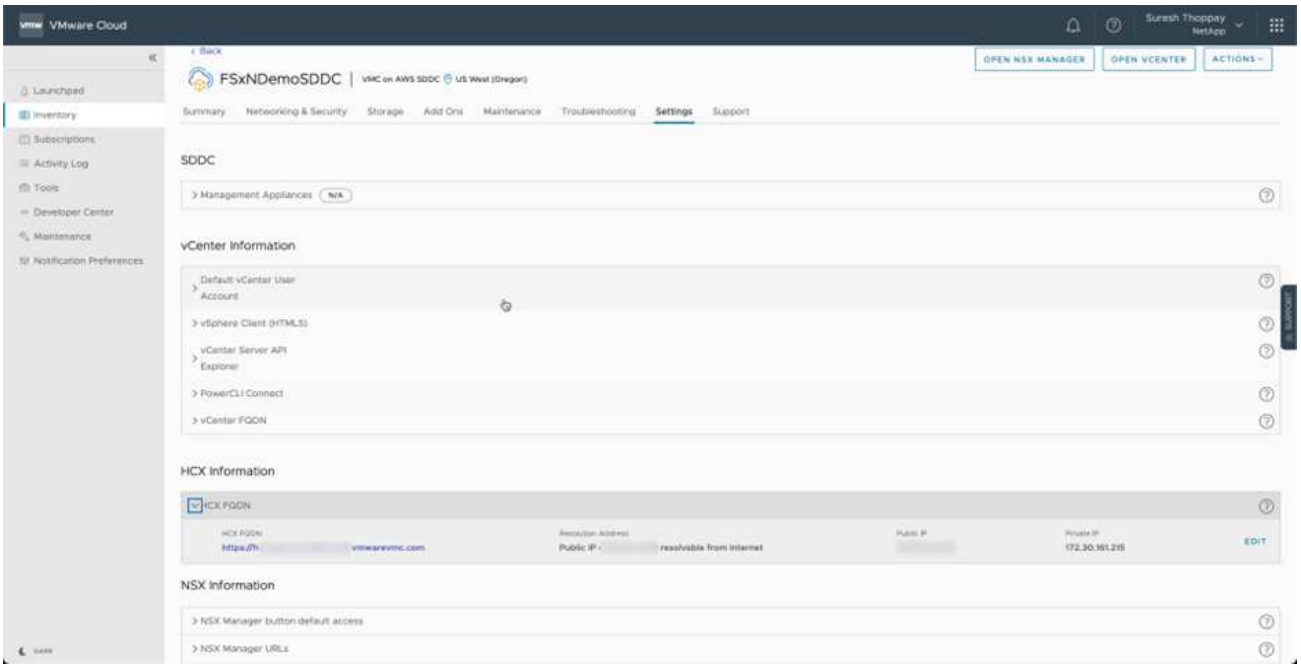
1. 온프레미스 vCenter Server와 VMC SDDC 간에 사이트 쌍을 생성하려면 온프레미스 vCenter Server에 로그인하고 HCX vSphere Web Client 플러그인에 액세스합니다.

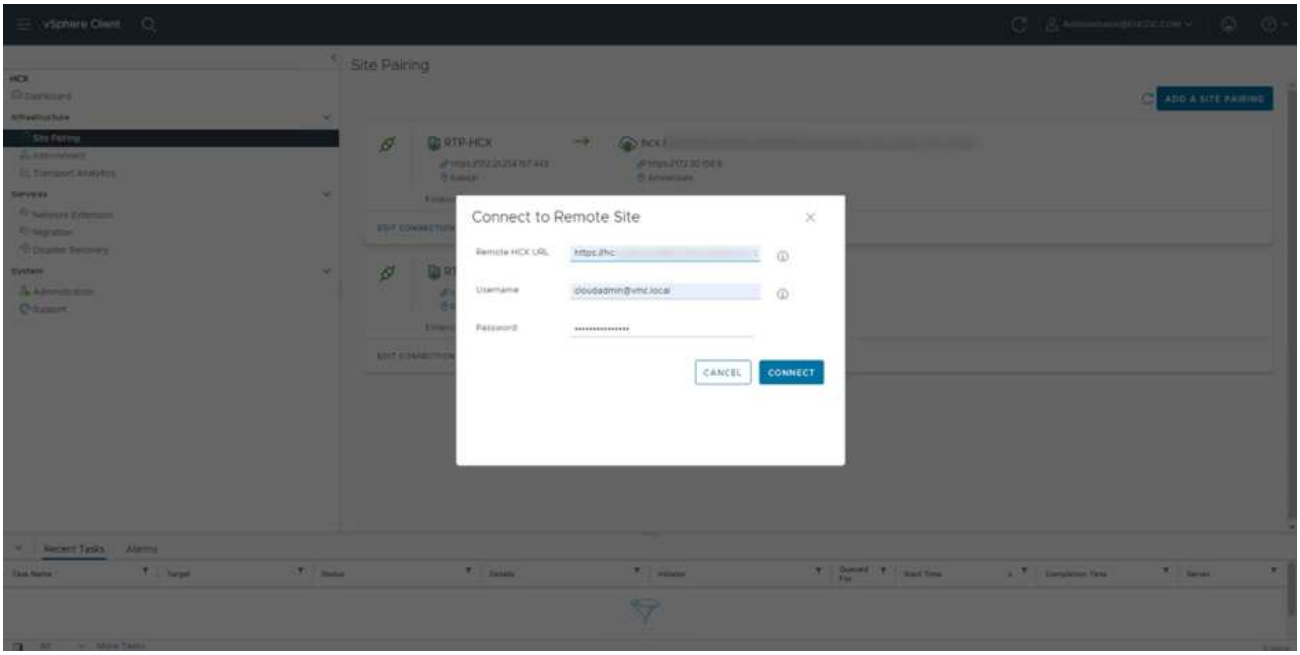


2. 인프라에서 사이트 페어링 추가를 클릭합니다. 원격 사이트를 인증하려면 VMC HCX Cloud Manager URL 또는 IP 주소와 CloudAdmin 역할에 대한 자격 증명을 입력하세요.



HCX 정보는 SDDC 설정 페이지에서 검색할 수 있습니다.





3. 사이트 페어링을 시작하려면 연결을 클릭하세요.

> VMware HCX Connector는 포트 443을 통해 HCX Cloud Manager IP와 통신할 수 있어야 합니다.

4. 페어링이 생성되면 새로 구성된 사이트 페어링을 HCX 대시보드에서 사용할 수 있습니다.

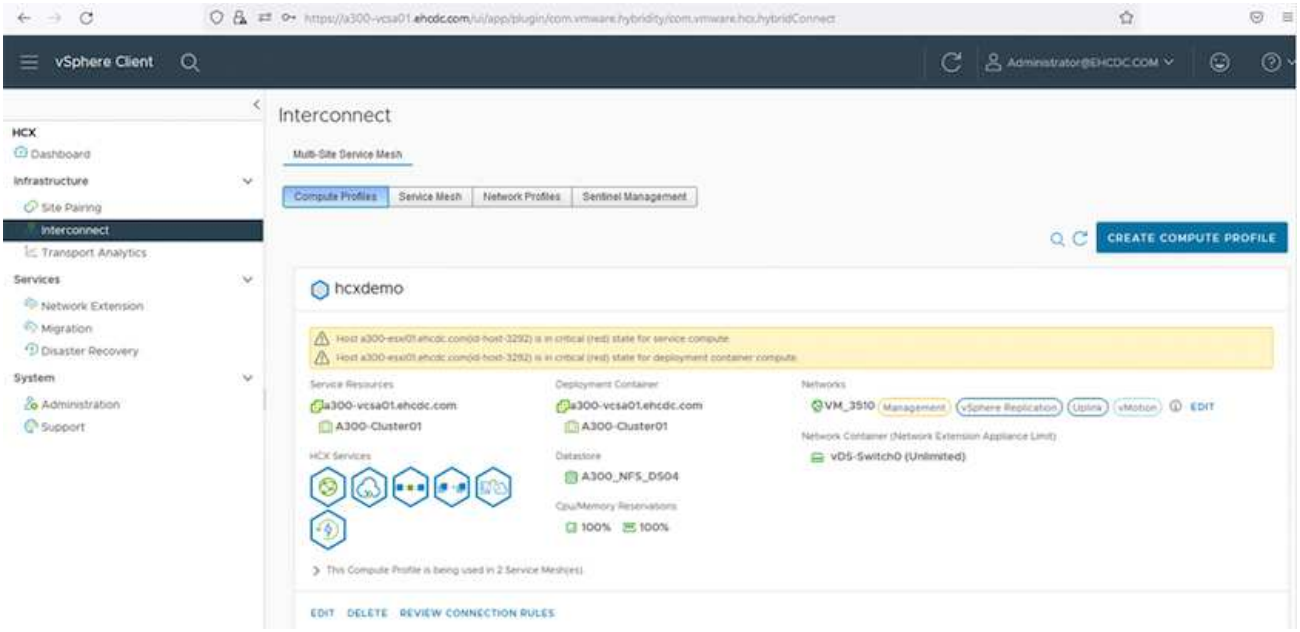
▼ **5**단계**:** 네트워크 프로필**,** 컴퓨팅 프로필 및 서비스 메시 구성

VMware HCX Interconnect(HCX-IX) 어플라이언스는 인터넷을 통한 보안 터널 기능과 대상 사이트에 대한 개인 연결을 제공하여 복제 및 vMotion 기반 기능을 구현합니다. 상호 연결은 암호화, 트래픽 엔지니어링 및 SD-WAN을 제공합니다. HCI-IX Interconnect Appliance를 생성하려면 다음 단계를 완료하세요.

1. 인프라에서 상호 연결 > 다중 사이트 서비스 메시 > 컴퓨팅 프로필 > 컴퓨팅 프로필 만들기를 선택합니다.

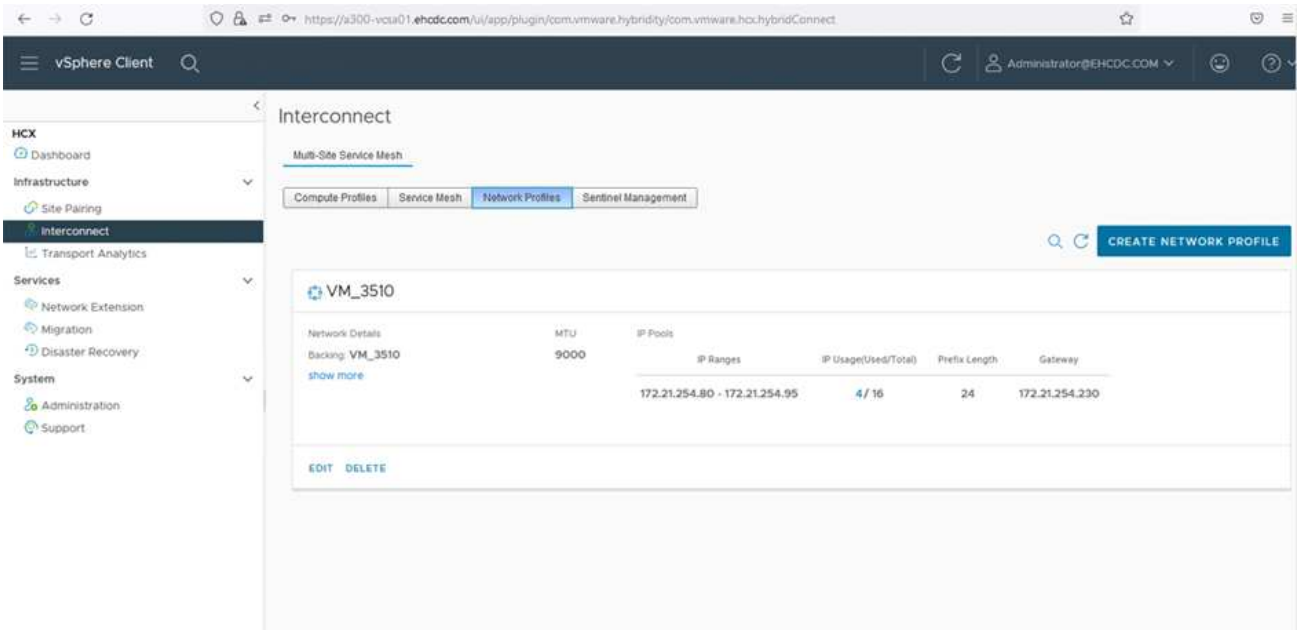
> 컴퓨팅 프로필에는 상호 연결 가상 어플라이언스를 배포하는 데 필요한 컴퓨팅, 스토리지 및 네트워크 배포 매개변수가 포함되어 있습니다. 또한 HCX 서비스에서 VMware 데이터 센터의 어느 부분에 액세스할 수 있는지도 지정합니다.

자세한 지침은 다음을 참조하세요. "컴퓨팅 프로필 생성" .



2. 컴퓨팅 프로필이 생성된 후, 멀티 사이트 서비스 메시 > 네트워크 프로필 > 네트워크 프로필 생성을 선택하여 네트워크 프로필을 생성합니다.
3. 네트워크 프로필은 HCX가 가상 어플라이언스에 사용할 IP 주소와 네트워크 범위를 정의합니다.

> 이렇게 하려면 두 개 이상의 IP 주소가 필요합니다. 이러한 IP 주소는 관리 네트워크에서 가상 어플라이언스에 할당됩니다.

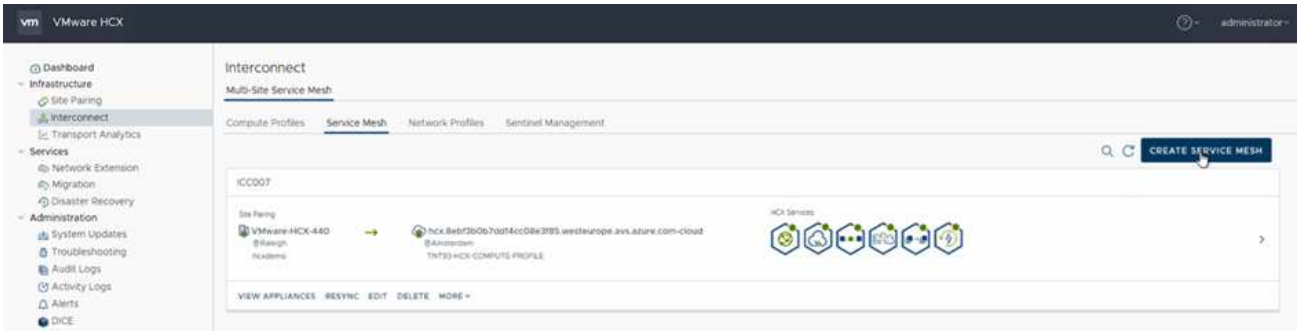


자세한 지침은 다음을 참조하세요. "네트워크 프로필 만들기" .

> 인터넷을 통해 SD-WAN에 연결하는 경우 네트워킹 및 보안 섹션에서 공용 IP를 예약해야 합니다.

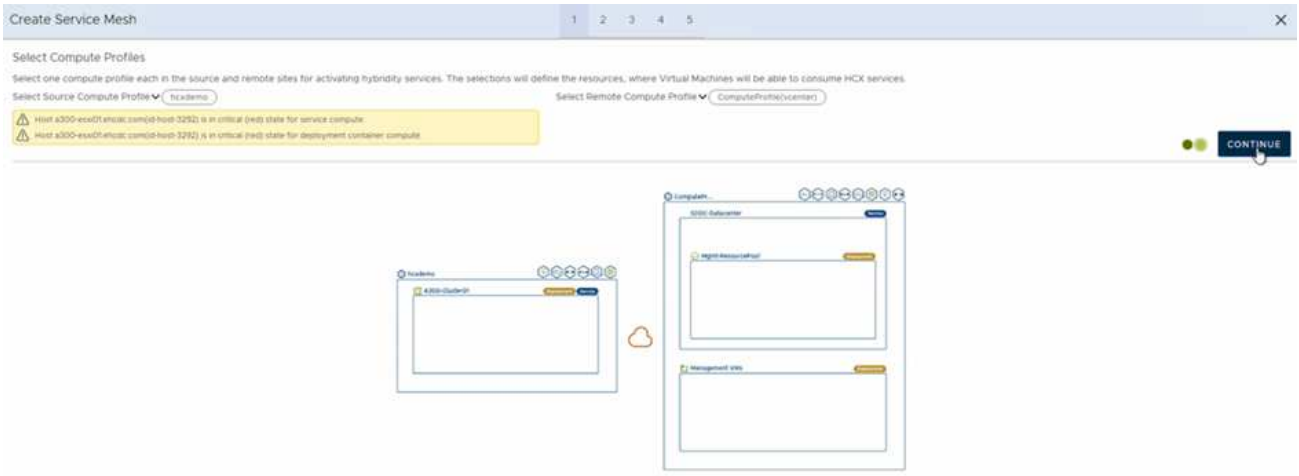
4. 서비스 메시를 생성하려면 Interconnect 옵션 내에서 Service Mesh 탭을 선택하고 온-프레미스 및 VMC SDDC 사이트를 선택합니다.

서비스 메시는 로컬 및 원격 컴퓨팅과 네트워크 프로필 쌍을 설정합니다.

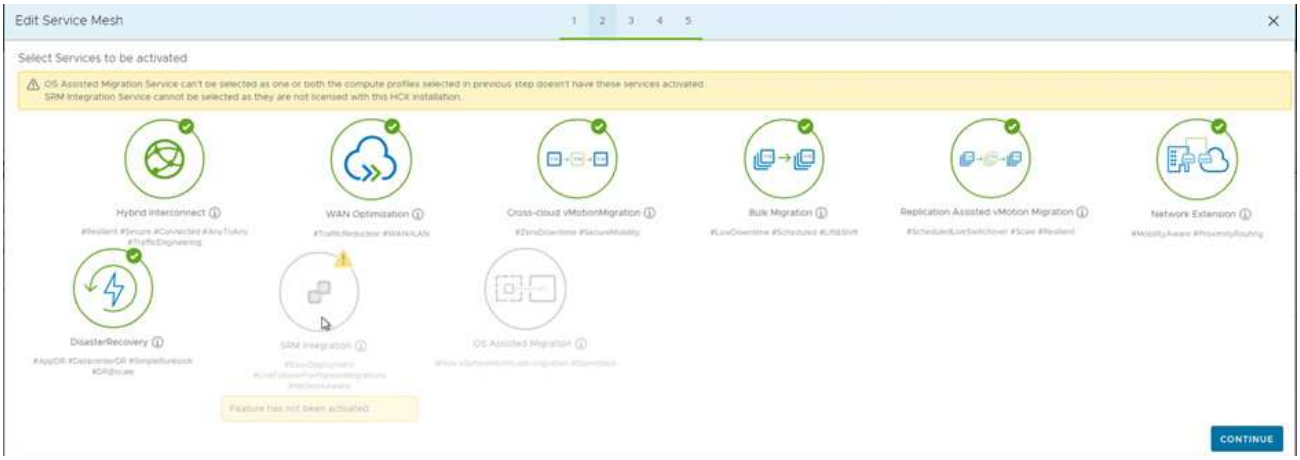


이 프로세스의 일부에는 소스 사이트와 대상 사이트 모두에 자동으로 구성되는 HCX 어플라이언스를 배포하여 안전한 전송 패브릭을 만드는 작업이 포함됩니다.

5. 소스 및 원격 컴퓨팅 프로필을 선택하고 계속을 클릭합니다.



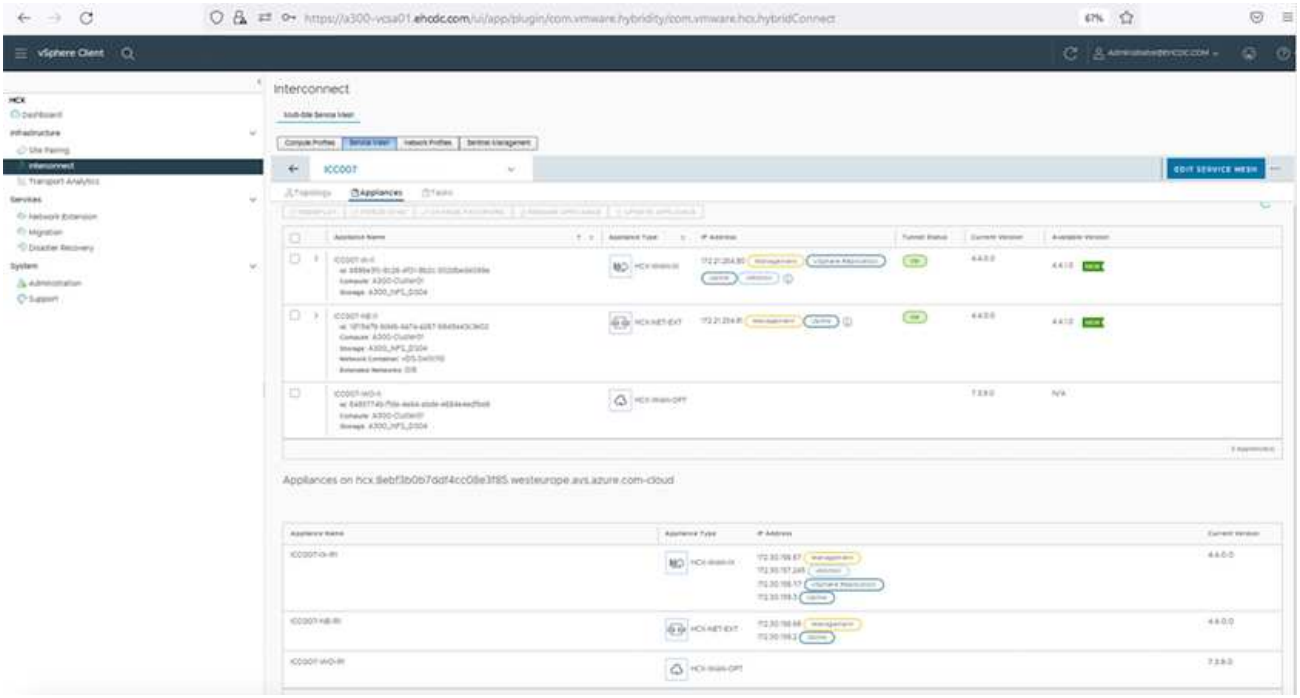
6. 활성화할 서비스를 선택하고 계속을 클릭하세요.



복제 지원 vMotion 마이그레이션, SRM 통합 및 OS 지원 마이그레이션에는 HCX Enterprise 라이선스가 필요합니다.

7. 서비스 메시의 이름을 만들고 마침을 클릭하여 생성 프로세스를 시작합니다. 배포를 완료하는 데 약 30분이

소요됩니다. 서비스 메시가 구성된 후 워크로드 VM을 마이그레이션하는 데 필요한 가상 인프라와 네트워킹이 생성되었습니다.



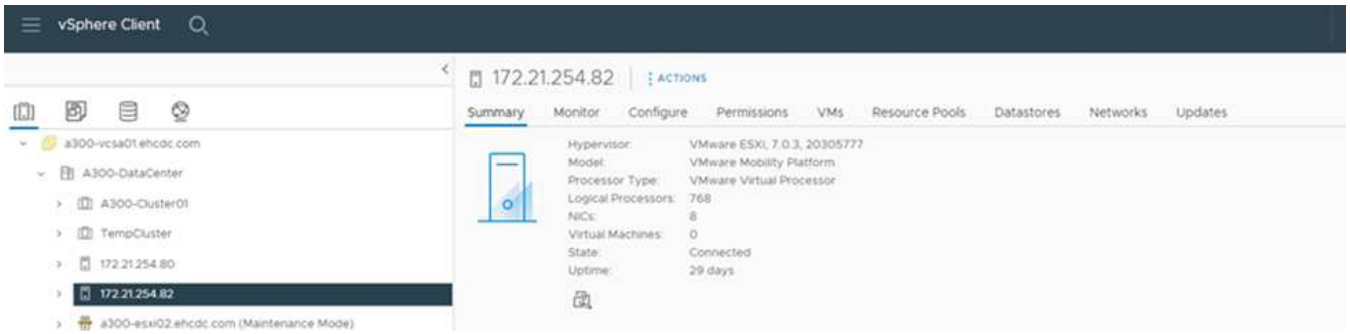
▼ **6**단계**:** 워크로드 마이그레이션

HCX는 온프레미스와 VMC SDDC와 같은 두 개 이상의 서로 다른 환경 간에 양방향 마이그레이션 서비스를 제공합니다. 다양한 마이그레이션 기술을 사용하여 HCX 활성화 사이트 간에 애플리케이션 워크로드를 마이그레이션할 수 있습니다. 이러한 마이그레이션 기술에는 HCX 대량 마이그레이션, HCX vMotion, HCX 콜드 마이그레이션, HCX 복제 지원 vMotion(HCX Enterprise 에디션에서 사용 가능), HCX OS 지원 마이그레이션(HCX Enterprise 에디션에서 사용 가능)이 있습니다.

사용 가능한 HCX 마이그레이션 기술에 대해 자세히 알아보려면 다음을 참조하세요. "VMware HCX 마이그레이션 유형"

HCX-IX 어플라이언스는 Mobility Agent 서비스를 사용하여 vMotion, Cold 및 Replication Assisted vMotion(RAV) 마이그레이션을 수행합니다.

HCX-IX 어플라이언스는 vCenter Server에 Mobility Agent 서비스를 호스트 개체로 추가합니다. 이 개체에 표시되는 프로세서, 메모리, 스토리지 및 네트워킹 리소스는 IX 어플라이언스를 호스팅하는 물리적 하이퍼바이저의 실제 소비량을 나타내지 않습니다.

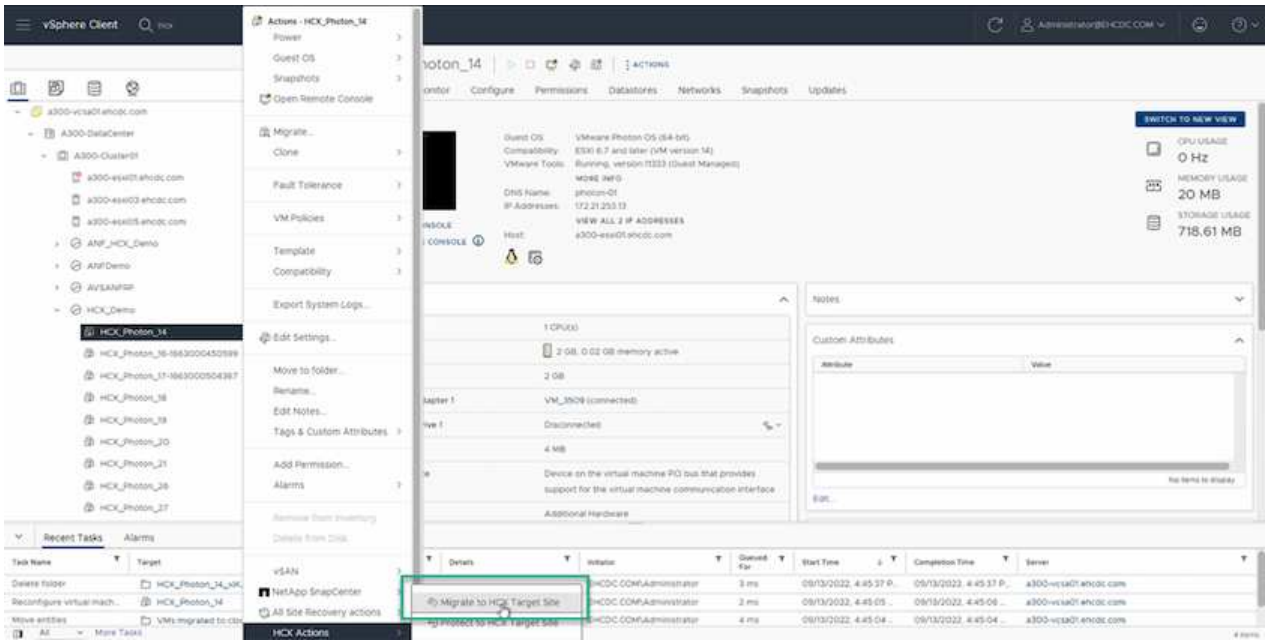


▼ **VMware HCX vMotion**

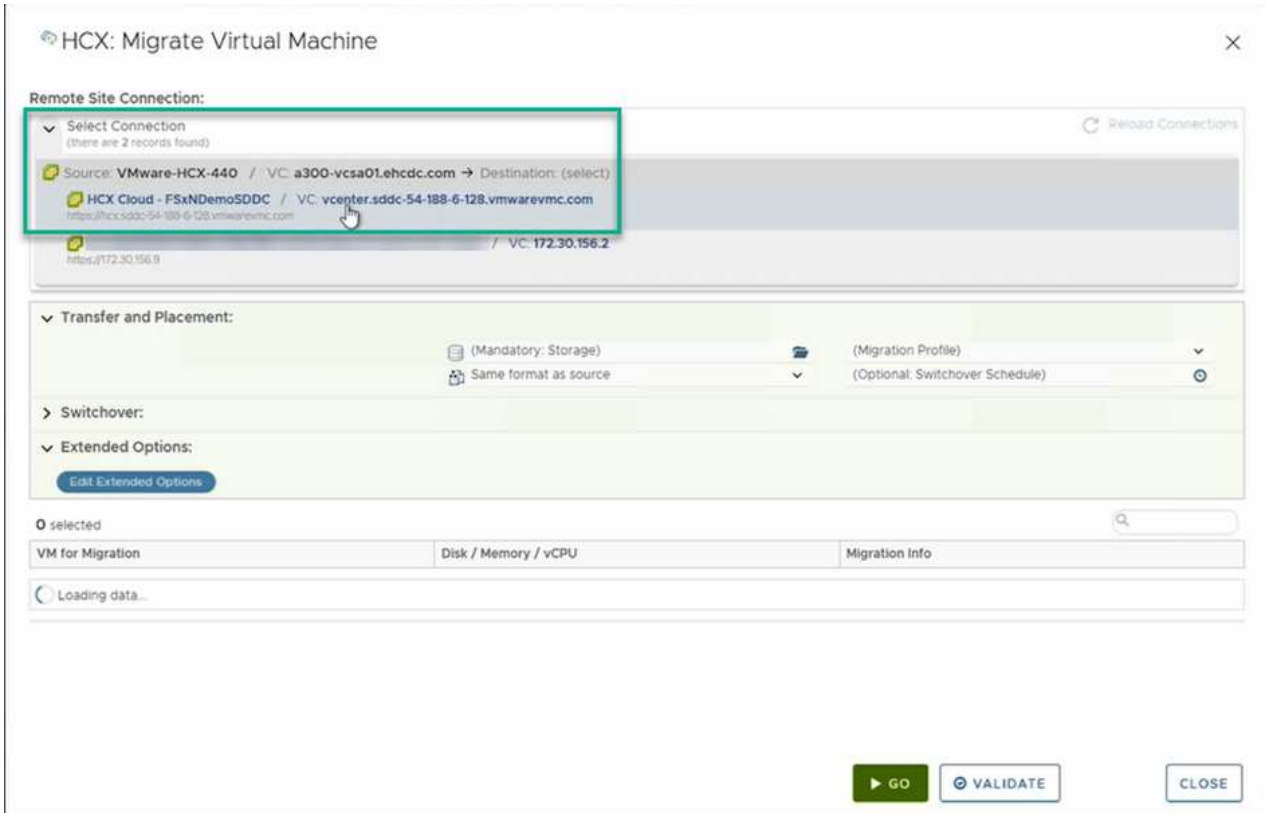
이 섹션에서는 HCX vMotion 메커니즘을 설명합니다. 이 마이그레이션 기술은 VMware vMotion 프로토콜을 사용하여 VM을 VMC SDDC로 마이그레이션합니다. vMotion 마이그레이션 옵션은 한 번에 하나의 VM의 VM 상태를 마이그레이션하는 데 사용됩니다. 이 마이그레이션 방법을 사용하는 동안 서비스 중단은 발생하지 않습니다.

IP 주소를 변경하지 않고도 VM을 마이그레이션하려면 VM이 연결된 포트 그룹에 대해 네트워크 확장이 있어야 합니다.

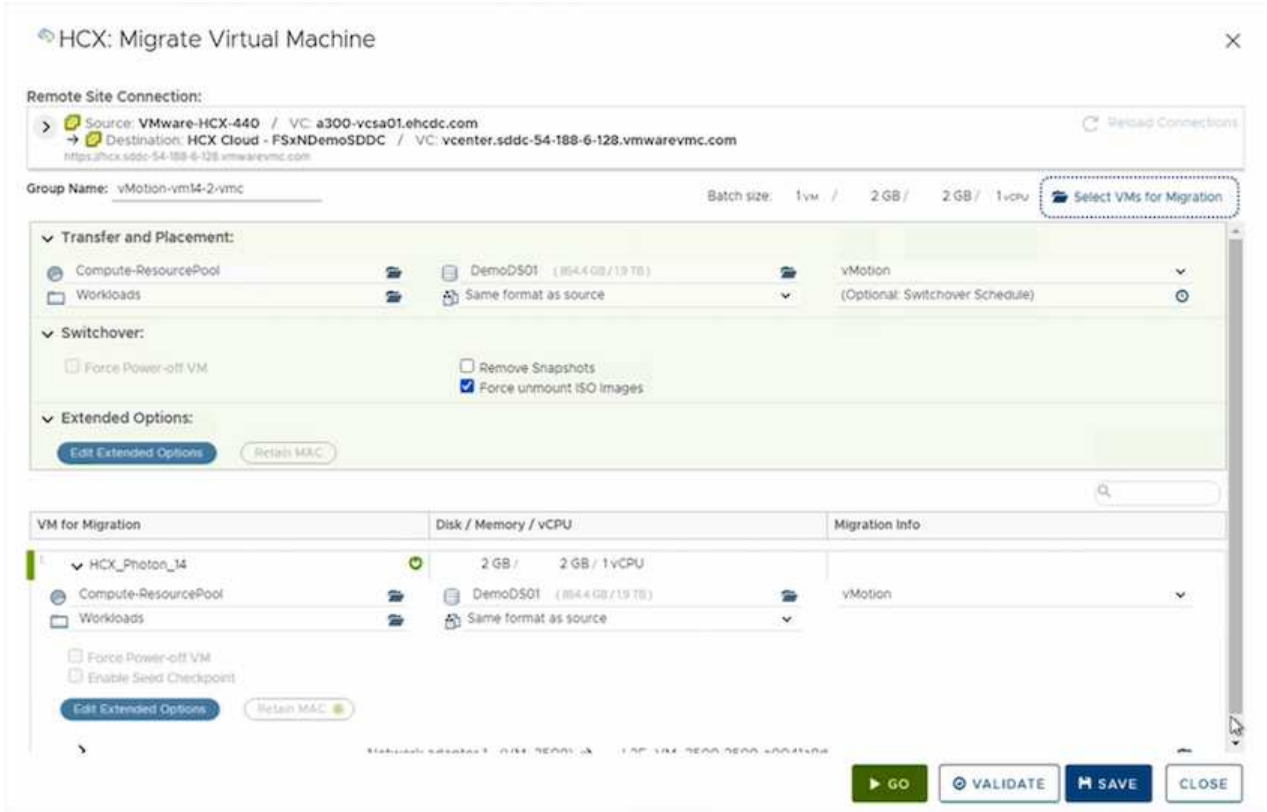
1. 온프레미스 vSphere 클라이언트에서 인벤토리로 이동하여 마이그레이션할 VM을 마우스 오른쪽 버튼으로 클릭하고 HCX 작업 > HCX 대상 사이트로 마이그레이션을 선택합니다.



2. 가상 머신 마이그레이션 마법사에서 원격 사이트 연결(대상 VMC SDDC)을 선택합니다.



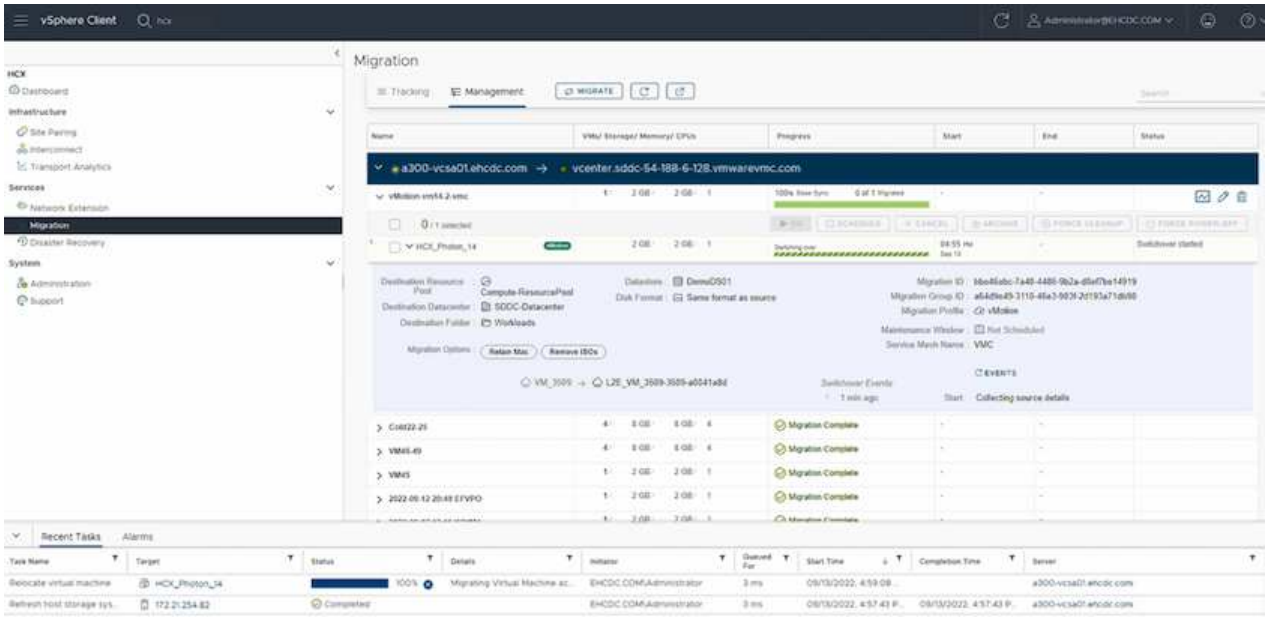
3. 그룹 이름을 추가하고 전송 및 배치에서 필수 필드(클러스터, 저장소, 대상 네트워크)를 업데이트한 후 확인을 클릭합니다.



4. 유효성 검사가 완료되면 '이동'을 클릭하여 마이그레이션을 시작합니다.

vMotion 전송은 VM의 활성 메모리, 실행 상태, IP 주소, MAC 주소를 캡처합니다. HCX vMotion의 요구 사항 및 제한 사항에 대한 자세한 내용은 다음을 참조하세요. "VMware HCX vMotion 및 콜드 마이그레이션 이해" .

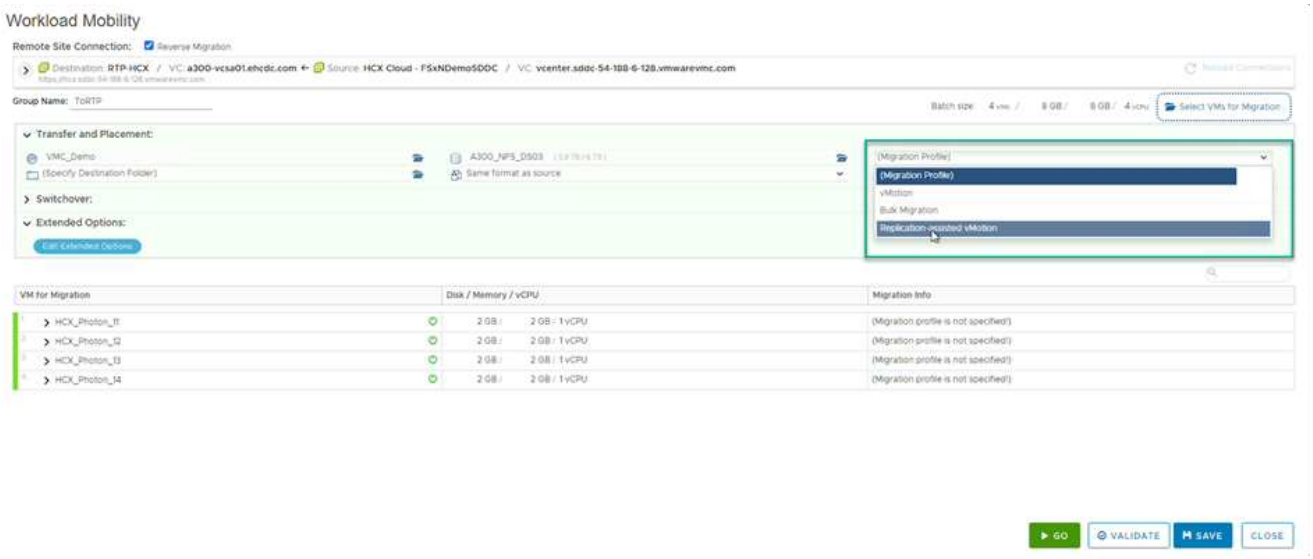
5. HCX > 마이그레이션 대시보드에서 vMotion의 진행 상황과 완료를 모니터링할 수 있습니다.



▼ **VMware** 복제 지원 **vMotion**

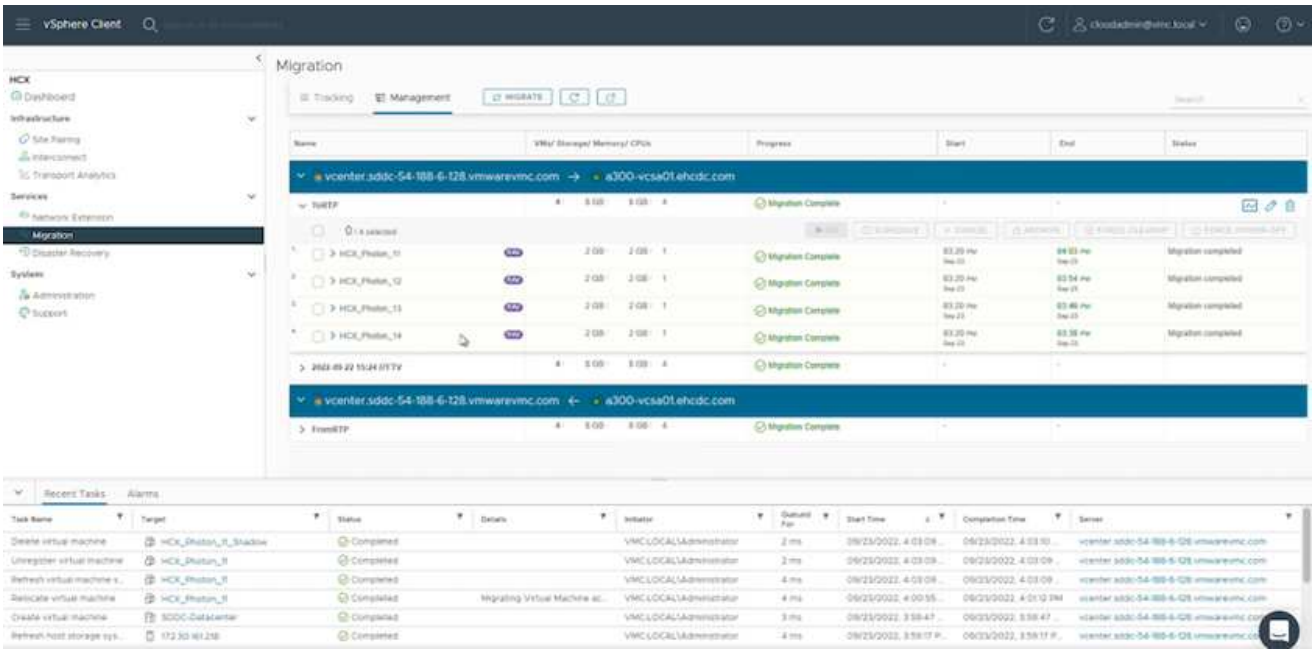
VMware 설명서에서 알 수 있듯이 VMware HCX 복제 지원 vMotion(RAV)은 대량 마이그레이션과 vMotion의 이점을 결합합니다. 대량 마이그레이션은 vSphere Replication을 사용하여 여러 VM을 병렬로 마이그레이션합니다. 전환 중에 VM이 재부팅됩니다. HCX vMotion은 가동 중지 시간 없이 마이그레이션을 수행하지만 복제 그룹에서 한 번에 하나의 VM씩 순차적으로 수행됩니다. RAV는 VM을 병렬로 복제하고 전환 창까지 동기화를 유지합니다. 전환 프로세스 동안 VM 가동 중지 시간 없이 한 번에 하나의 VM만 마이그레이션합니다.

다음 스크린샷은 복제 지원 vMotion으로 마이그레이션 프로필을 보여줍니다.



소수의 VM에 대한 vMotion과 비교했을 때 복제 기간이 더 길어질 수 있습니다. RAV를 사용하면 델타만

동기화하고 메모리 내용을 포함합니다. 다음은 마이그레이션 상태의 스크린샷입니다. 마이그레이션 시작 시간은 같고 종료 시간은 각 VM마다 다릅니다.



HCX 마이그레이션 옵션에 대한 추가 정보와 HCX를 사용하여 온프레미스에서 VMware Cloud on AWS로 워크로드를 마이그레이션하는 방법에 대한 자세한 내용은 다음을 참조하세요. "VMware HCX 사용자 가이드" .

VMware HCX vMotion에는 100Mbps 이상의 처리량 성능이 필요합니다.

대상 VMC FSx ONTAP 데이터 저장소에는 마이그레이션을 수용할 수 있는 충분한 공간이 있어야 합니다.

결론

온프레미스의 모든 유형/공급업체 스토리지에 있는 데이터를 포함하여 모든 클라우드 또는 하이브리드 클라우드를 타겟으로 삼는지 여부에 관계없이 Amazon FSx ONTAP 과 HCX는 데이터 요구 사항을 애플리케이션 계층에 원활하게 전달하여 TCO를 줄이는 동시에 워크로드를 배포하고 마이그레이션할 수 있는 탁월한 옵션을 제공합니다. 어떤 사용 사례에서든 FSx ONTAP 데이터 저장소와 함께 VMC를 선택하면 클라우드의 이점을 빠르게 실현하고, 온프레미스와 여러 클라우드에서 일관된 인프라와 운영을 구현하고, 워크로드를 양방향으로 이동시키고, 엔터프라이즈급 용량과 성능을 확보할 수 있습니다. 이는 VMware vSphere 복제, VMware vMotion 또는 NFC 복사를 사용하여 스토리지를 연결하고 VM을 마이그레이션하는 데 사용되는 익숙한 프로세스 및 절차와 동일합니다.

테이크아웃

이 문서의 주요 내용은 다음과 같습니다.

- 이제 Amazon FSx ONTAP VMC SDDC의 데이터 저장소로 사용할 수 있습니다.
- FSx ONTAP 데이터 저장소를 실행하는 VMC로 온프레미스 데이터 센터의 데이터를 쉽게 마이그레이션할 수 있습니다.
- 마이그레이션 작업 중에 용량 및 성능 요구 사항을 충족하기 위해 FSx ONTAP 데이터 저장소를 쉽게 확장하거나 축소할 수 있습니다.

추가 정보를 찾을 수 있는 곳

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 웹사이트 링크를 참조하세요.

- VMware Cloud 설명서

  "https://docs.vmware.com/en/VMware-Cloud-on-AWS/"

- Amazon FSx ONTAP 설명서

  "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"

  VMware HCX 사용자 가이드

- "https://techdocs.broadcom.com/us/en/vmware-cis/hcx/vmware-hcx/4-10/vmware-hcx-user-guide-4-10.html"

AWS/EVS용 NetApp

EVS의 외부 데이터 저장소로 FSx ONTAP 마운트

Amazon Elastic VMware Service의 외부 데이터 저장소로 **Amazon FSx for NetApp ONTAP** 마운트하는 방법

이 문서에서는 FSx for ONTAP 파일 시스템을 생성하고 이를 Amazon EVS와 함께 사용할 iSCSI(인터넷 소형 컴퓨터 시스템 인터페이스) 또는 NFS(네트워크 파일 시스템) 데이터 저장소로 연결하는 방법에 대한 자세한 단계를 설명합니다.

소개

기존 온프레미스 VMware 투자를 통해 AWS에서 복사본을 마이그레이션, 버스팅, 확장 또는 보호(백업, 재해 복구)하여 배포를 현대화할 수 있는 효율적이고 비용 효율적인 방법을 찾고 있는 조직은 여러 가지 과제에 직면했습니다. Amazon Elastic VMware Service(Amazon EVS)가 출시되면서 이제 Amazon Virtual Private Cloud(VPC)에서 VMware Cloud Foundation(VCF)을 직접 실행할 수 있는 기본 AWS 서비스가 제공됩니다.

Amazon EVS를 사용하면 기존 VCF 배포를 AWS로 확장하고, 최대 사용량 중에 AWS에 접속하여 성능을 확장하고, VCF 워크로드를 AWS에서 완전히 실행하여 현대화, 데이터 센터 종료, 통합 및 기타 사용 사례를 용이하게 할 수 있습니다.

Amazon EVS는 강력한 이점을 제공하지만, 기본 하이퍼 컨버지드 아키텍처는 컴퓨팅과 스토리지를 결합하기 때문에 비즈니스 요구에 따라 둘 중 하나를 독립적으로 확장할 수 없습니다. 오늘날의 데이터 중심 세계에서는 많은 조직의 스토리지 수요가 컴퓨팅 수요보다 높습니다. 하지만 VMware 하이퍼컨버지드 아키텍처에서는 스토리지 리소스가 컴퓨팅 리소스와 결합됩니다. 즉, 저장소 확장은 사용되지 않을 컴퓨팅 호스트를 추가하는 방법으로만 가능합니다. 특히 저장 공간이 많은 작업 부하의 경우 비용이 상당히 증가할 수 있는 상황입니다.

이 문제를 해결하기 위해 AWS와 NetApp Amazon EVS를 위한 외부 스토리지 서비스로 Amazon FSx for NetApp ONTAP (FSx for ONTAP)을 제공합니다. FSx for ONTAP 은 NetApp ONTAP 소프트웨어의 고성능, 데이터 복원력, 비용 효율성 기능을 제공하는 AWS 기반 스토리지 서비스입니다. Amazon EVS 사용자는 FSx for ONTAP 을 외부 스토리지로 사용하여 컴퓨팅 및 스토리지 리소스를 독립적으로 확장할 수 있으므로 총 소유 비용(TCO)을 최적화할 수 있습니다.

개요

이 문서에서는 FSx for ONTAP 파일 시스템을 생성하고 이를 Amazon EVS와 함께 사용할 iSCSI(인터넷 소형 컴퓨터 시스템 인터페이스) 또는 NFS(네트워크 파일 시스템) 데이터 저장소로 연결하는 방법에 대한 자세한 단계를 설명합니다.

이 가이드의 목적

이 가이드에서는 Amazon EVS를 위한 FSx for ONTAP 데이터 저장소를 설정하는 방법에 대한 지침을 제공하며, 모범 사례, 지원 요구 사항, 크기 고려 사항 및 통합을 계획, 설계 및 구현하는 데 도움이 되는 기타 정보를 제공합니다.

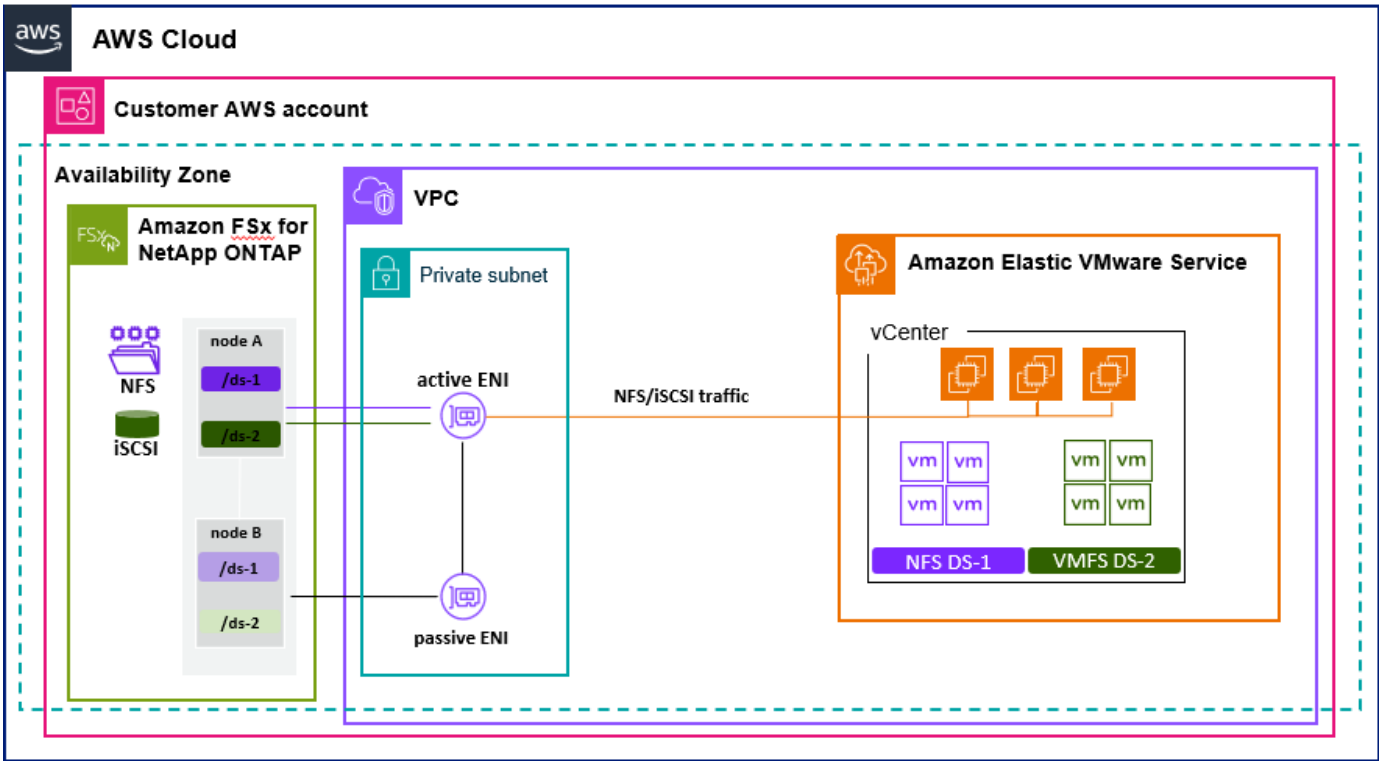
대상

이 튜토리얼은 VMware vSphere, Amazon EVS, AWS 콘솔, FSx for ONTAP 에 익숙한 클라우드 아키텍트와 클라우드 관리자를 대상으로 합니다.

고수준 아키텍처

이 섹션에서는 Amazon EVS의 데이터 저장소로 FSx for ONTAP 사용하기 위한 솔루션 아키텍처에 대한 개요를 설명합니다.

아래에서 AWS VPC 내의 Amazon EVS 환경을 갖춘 FSx for ONTAP 데이터 저장소 아키텍처의 개요를 볼 수 있습니다.



FSx for ONTAP NFS 데이터 저장소로 사용하기 위한 배포 절차

이 섹션에서는 FSx for ONTAP NFS 데이터 저장소로 배포하는 방법에 대한 단계를 보여줍니다. iSCSI 데이터스토어를 배포하는 단계는 다음 섹션에서 자세히 설명합니다.

고수준 배포 단계

Amazon EVS의 NFS 데이터 저장소로 사용하기 위해 FSx for ONTAP 파일 시스템을 배포하고 두 서비스 간의 연결을 설정하는 단계는 다음과 같습니다.

- Amazon EVS VCF 환경이 있는 동일한 VPC에 FSx for ONTAP 파일 시스템을 설정합니다.
- 보안 그룹과 라우팅 테이블을 검증합니다.
- Amazon EVS의 NFS 데이터 저장소로 사용하기 위해 ONTAP 스토리지 볼륨에 FSx를 연결합니다.

필수 조건

Amazon EVS의 NFS 데이터 저장소로 FSx for ONTAP 을 설정하는 프로세스를 시작하기 전에 다음과 같은 전제 조건이 충족되어야 합니다.

- Amazon EVS 가상화 환경. 이를 수행하는 방법에 대한 자세한 내용은 다음 문서를 참조하세요."Amazon EVS 가이드 시작하기" .
- 적절한 SSD 스토리지 용량, 프로비저닝된 IOPS 및 처리량을 갖춘 ONTAP 용 단일 가용성 영역(AZ) FSx를 생성합니다.
- 최적의 성능을 위해 FSx for ONTAP 파일 시스템을 Amazon EVS 인스턴스와 동일한 VPC 내에 배치하세요. FSx for ONTAP 이 다른 VPC에 배포된 경우에도 VPC 피어링이 지원됩니다.
- 성능 요구 사항에 따라 ONTAP 파일 시스템용 Single-AZ FSx에 필요한 올바른 IOPS와 처리량을 선택하세요. 보다"FSx for ONTAP 에 대한 성능 사양 세부 정보" 사용 가능한 각 옵션이 제공하는 처리량과 IOPS를 파악합니다.



이 가이드에서는 서비스 액세스 서브넷과 동일한 서브넷에 FSx for ONTAP 파일 시스템을 배포합니다.

Amazon EVS 가상화 환경이 VPC에 배포되면 NFS 데이터 저장소로 사용될 Single-AZ FSx for ONTAP 파일 시스템을 설정할 수 있습니다.

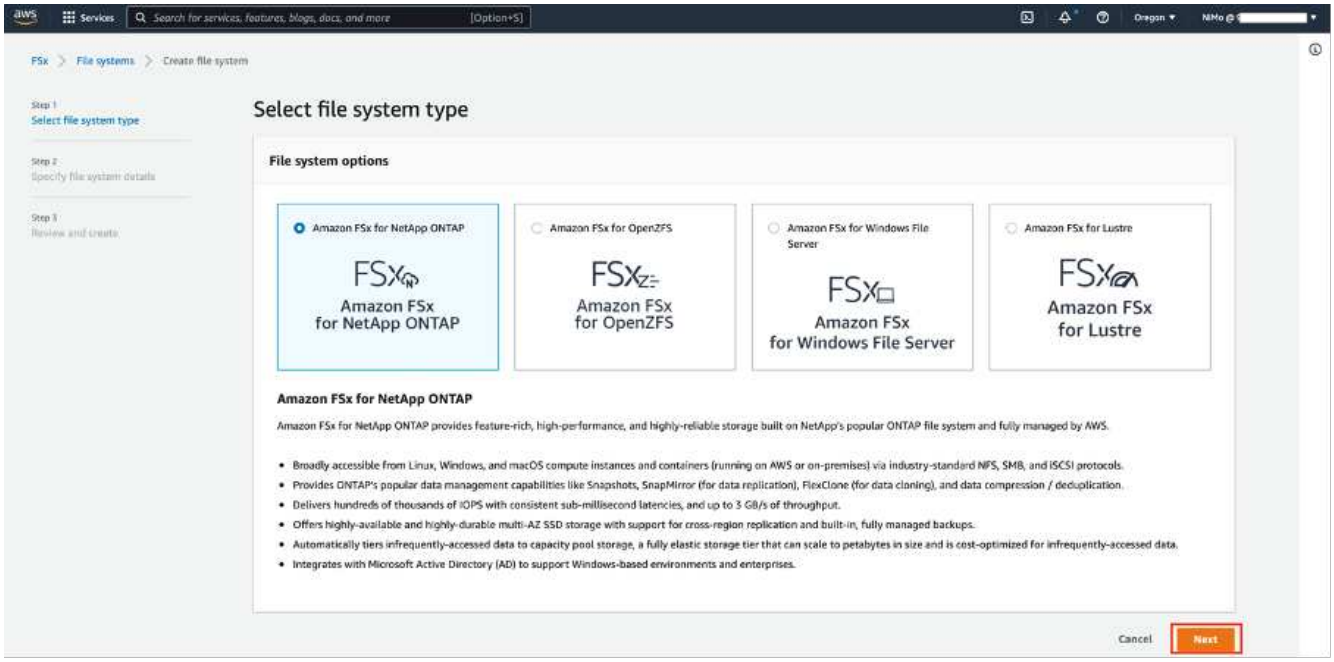


FSx for ONTAP 파일 시스템은 Amazon EVS SDDC와 동일한 AZ에 배포되어야 합니다.

ONTAP 파일 시스템용 **FSx** 생성

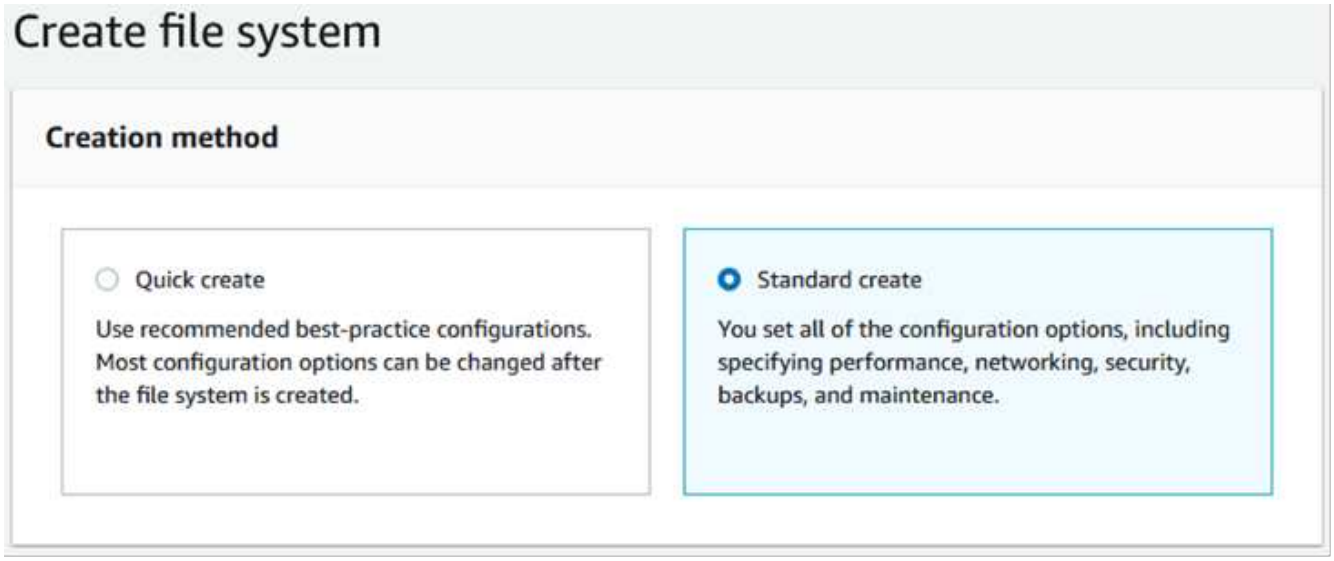
다음 단계에서는 FSx for ONTAP 파일 시스템을 프로비저닝하고 마운트하는 방법을 보여줍니다.

1. Amazon FSx 콘솔로 이동하세요. `https://console.aws.amazon.com/fsx/` 인터넷 브라우저를 사용하여 자격 증명을 사용하여 로그인하세요.
2. 콘솔에서 파일 시스템 만들기를 선택합니다. 이렇게 하면 FSx for ONTAP 파일 시스템을 만드는 설정 마법사가 시작됩니다.
3. 먼저, 파일 시스템 유형을 선택하세요. 사용 가능한 파일 시스템 옵션에서 "Amazon FSx for NetApp ONTAP"을 선택하고 "다음" 버튼을 클릭하여 계속 진행합니다.

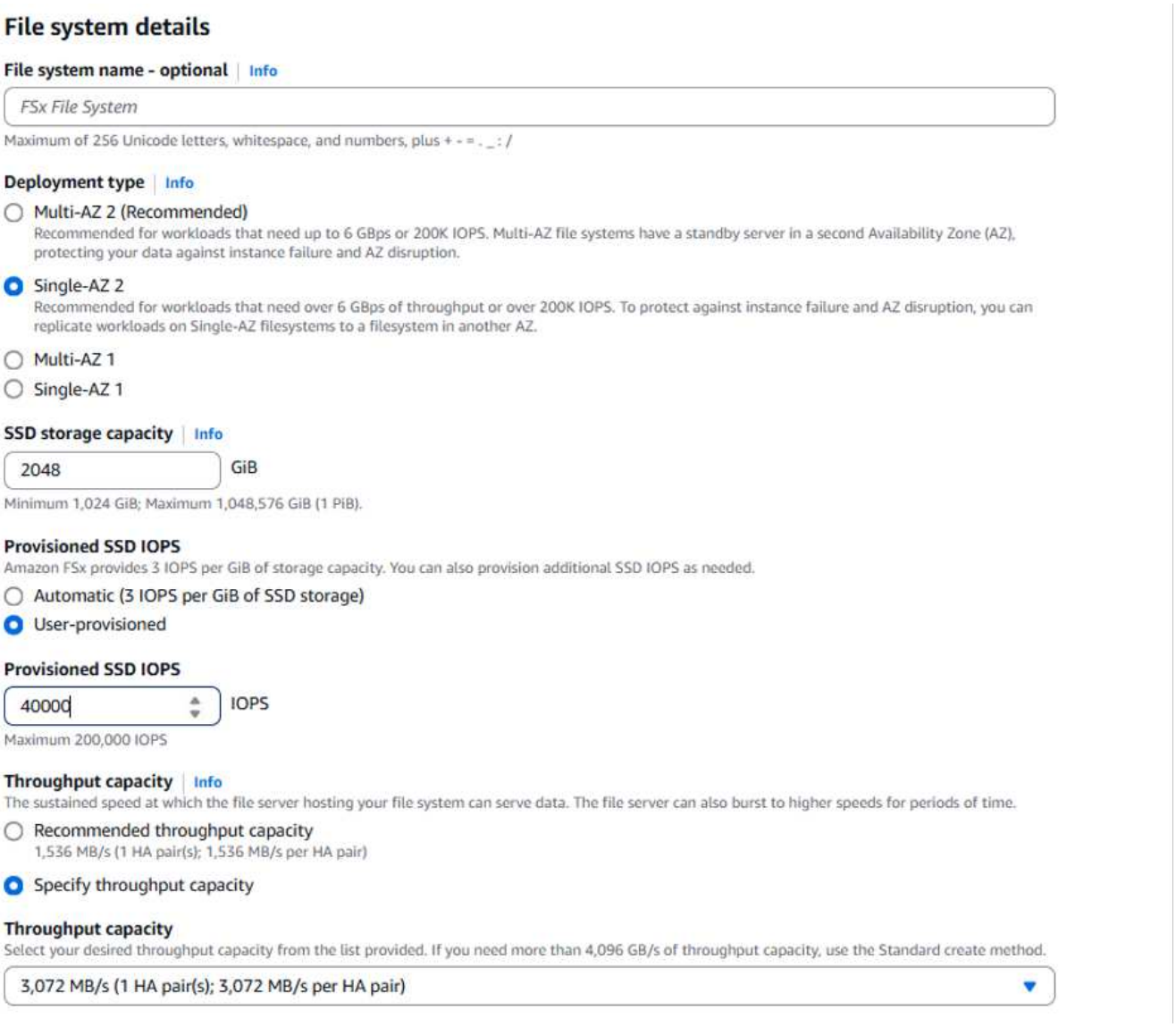


4. 빠른 생성과 표준 생성 옵션 중에서 선택할 수 있습니다. 빠른 생성은 미리 정의된 구성을 제공하고, 표준 생성을 사용하면 사용자가 직접 구성을 정의할 수 있습니다.

   "표준 생성" 옵션을 선택하세요.



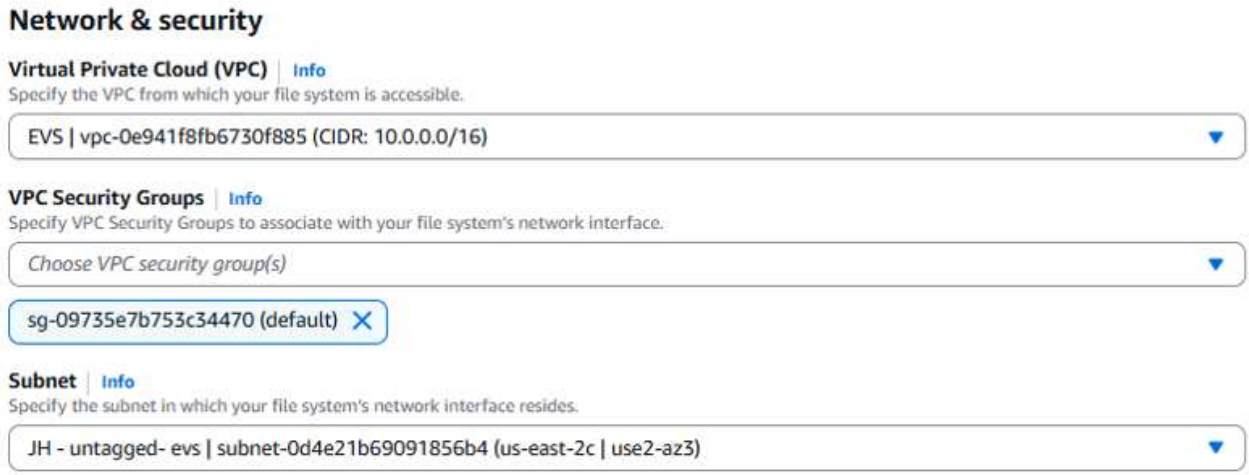
   이제 표준 파일 시스템 설정 마법사가 시작됩니다. 파일 시스템 세부 정보 페이지에서 아래 이미지에 표시된 것과 동일한 정보를 선택하여 입력합니다.



5. 아래로 스크롤하여 "네트워크 및 보안"이라고 표시된 섹션을 찾으세요. 이 섹션에서는 서브넷과 VPC에 대한 세부 정보를 설정합니다. 이 가이드의 목적을 위해 드롭다운 메뉴에서 "EVS-VPC"를 선택하고, EVS 가상 환경의 서브넷으로 서비스 액세스 서브넷(태그 없음 VLAN)을 선택했습니다.

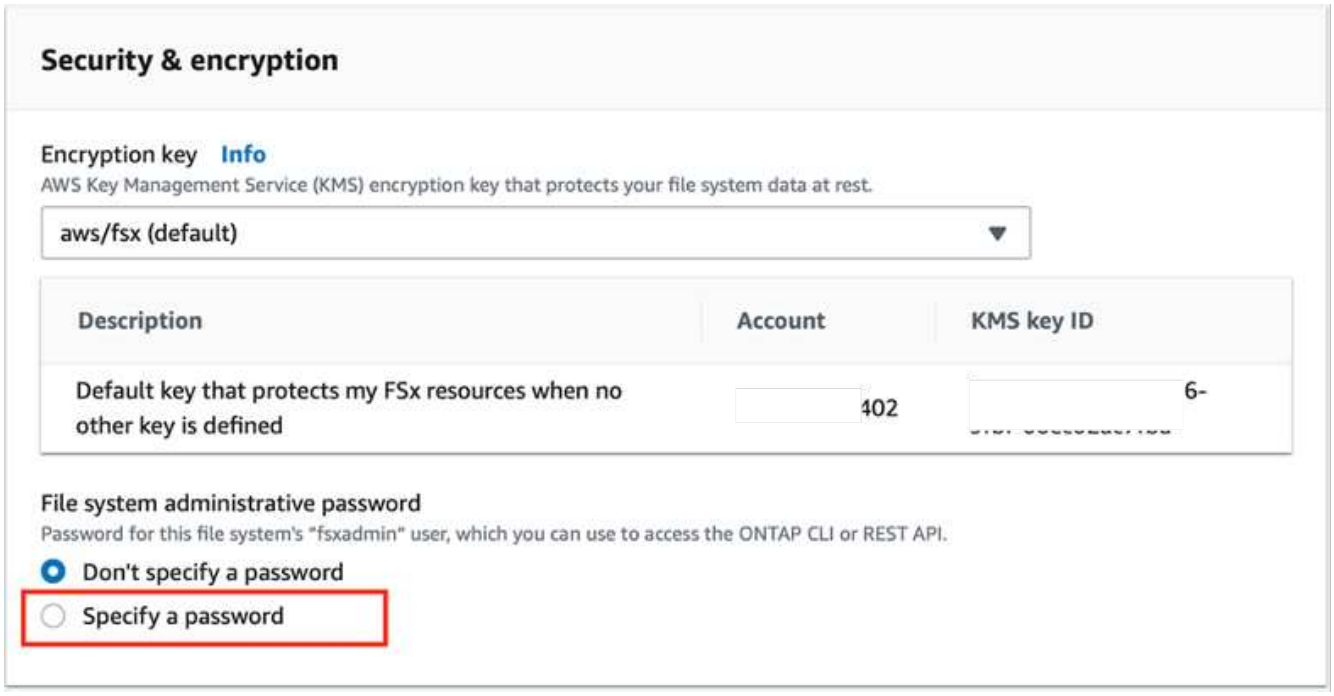


서브넷은 VPC 내의 태그가 지정되지 않은 개인 서브넷일 수 있습니다. 적절한 라우팅이 구성된 경우, VPC 피어링을 통해 연결된 다른 VPC/서브넷에 있을 수도 있습니다.

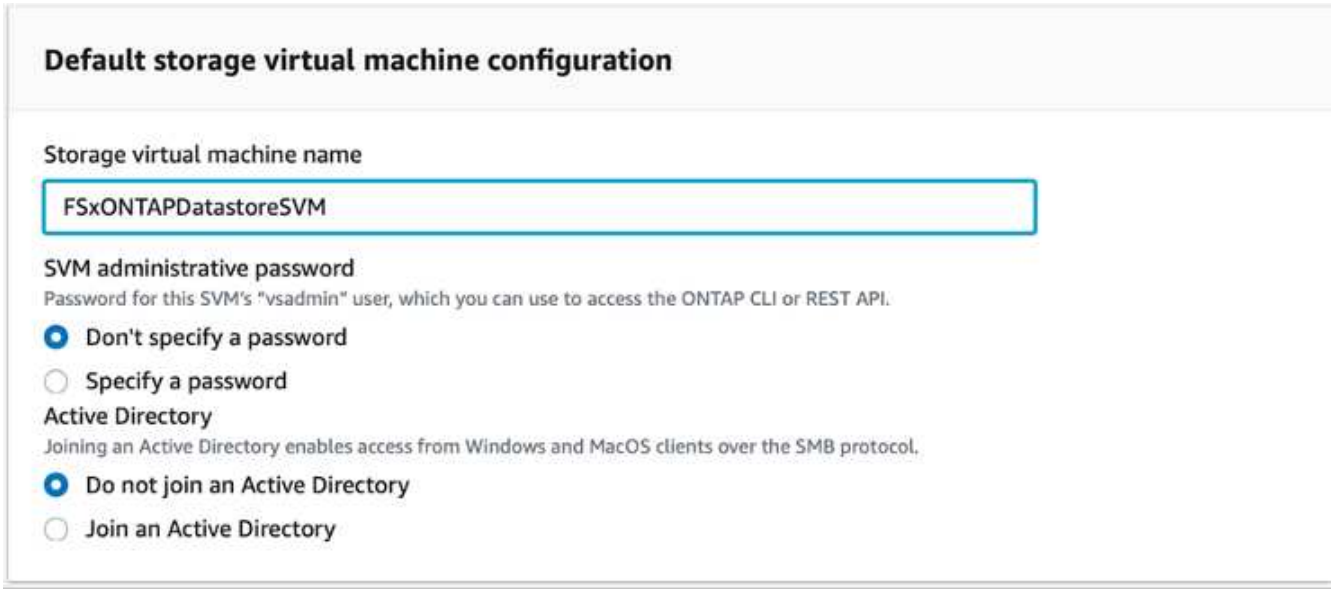


6. 아래로 스크롤하면 "보안 및 암호화" 섹션을 찾을 수 있습니다. 여기에서 드롭다운 메뉴에서 암호화 키를 선택하세요. 이러한 키는 AWS Key Management Service(AWS KMS)에서 제공되며 FSx for ONTAP 파일 시스템에 있는 저장 데이터를 보호합니다.

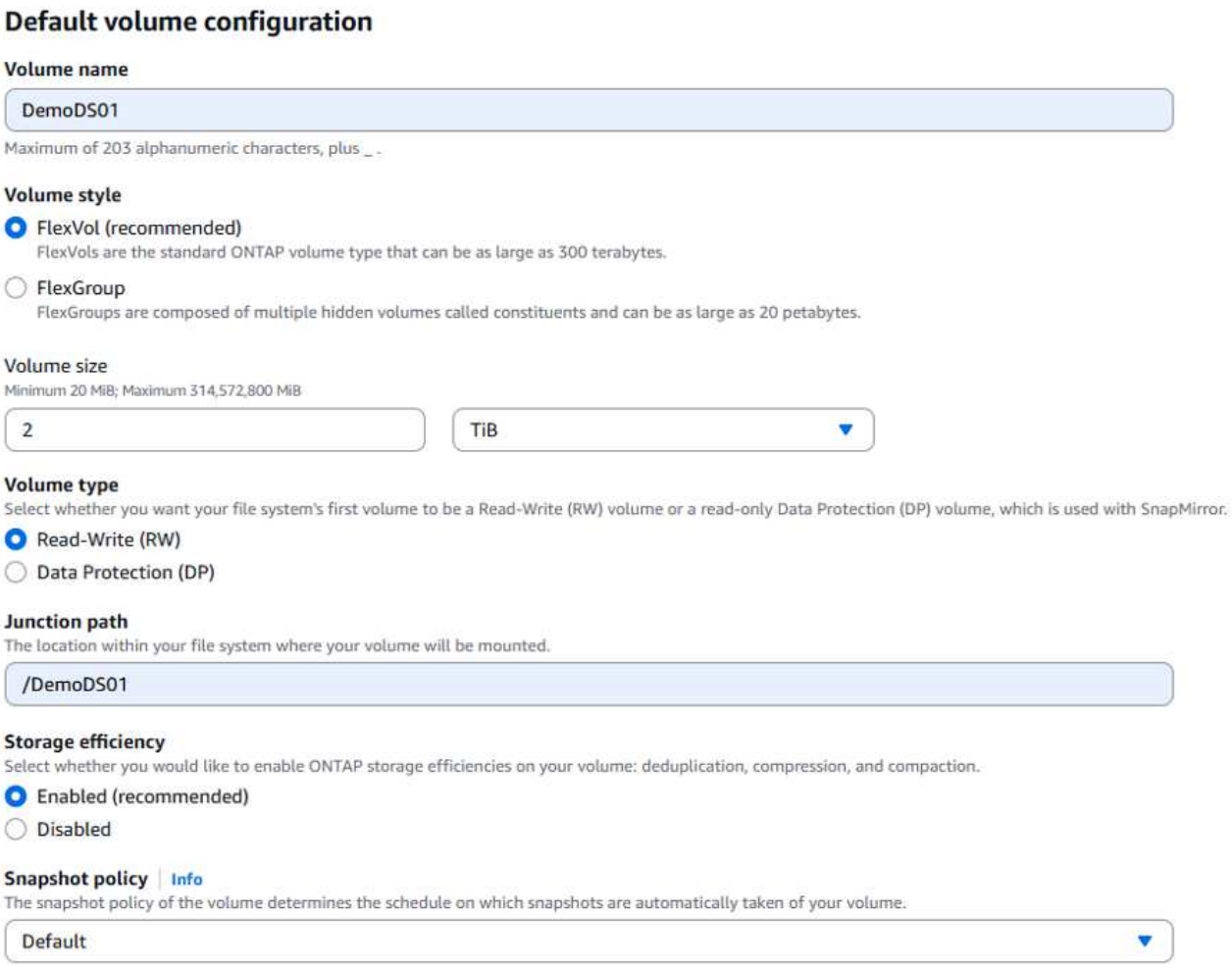
   다음으로, "파일 시스템 관리 비밀번호" 설정에서 파일 시스템을 관리할 fsxadmin 사용자에 대한 고유한 비밀번호를 지정합니다.



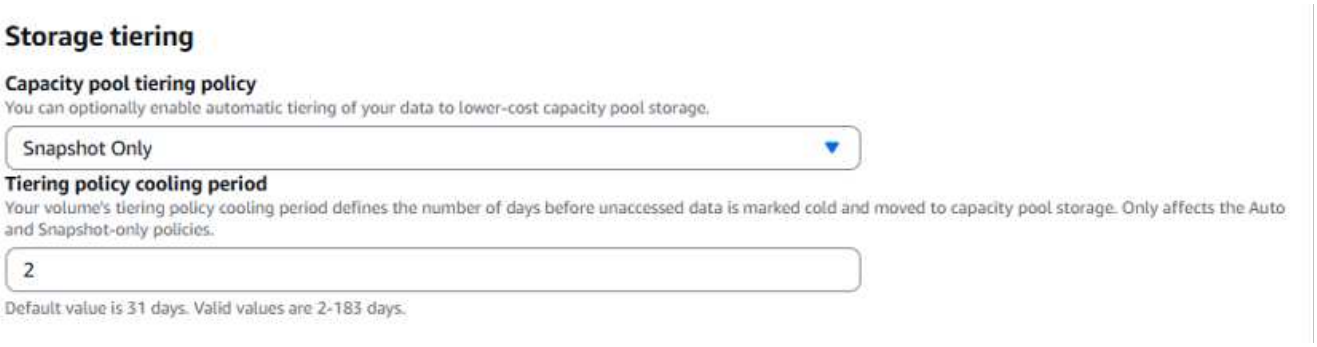
7. 다음으로, "기본 스토리지 가상 머신 구성"이라는 섹션까지 아래로 스크롤합니다. 여기에서는 스토리지 가상 머신(SVM)의 이름을 제공해야 합니다.



8. 다음으로, "기본 볼륨 구성"이라는 섹션까지 아래로 스크롤합니다. 여기서 볼륨의 이름을 지정하고 볼륨 크기를 설정합니다. 볼륨 프로토콜은 NFS v3(기본적으로 활성화됨)이어야 합니다. 전체 저장소 사용량과 비용을 줄이기 위해 저장소 효율성 기능(압축, 중복 제거, 압축)을 활성화하는 옵션을 클릭하세요.



9. 스토리지 계층화 옵션의 경우 드롭다운 메뉴에서 "스냅샷만"을 선택하고 계층화 정책 냉각 기간을 설정합니다. 기본값은 31일이지만, 이 예에서는 2일의 냉각 기간을 설정했습니다.

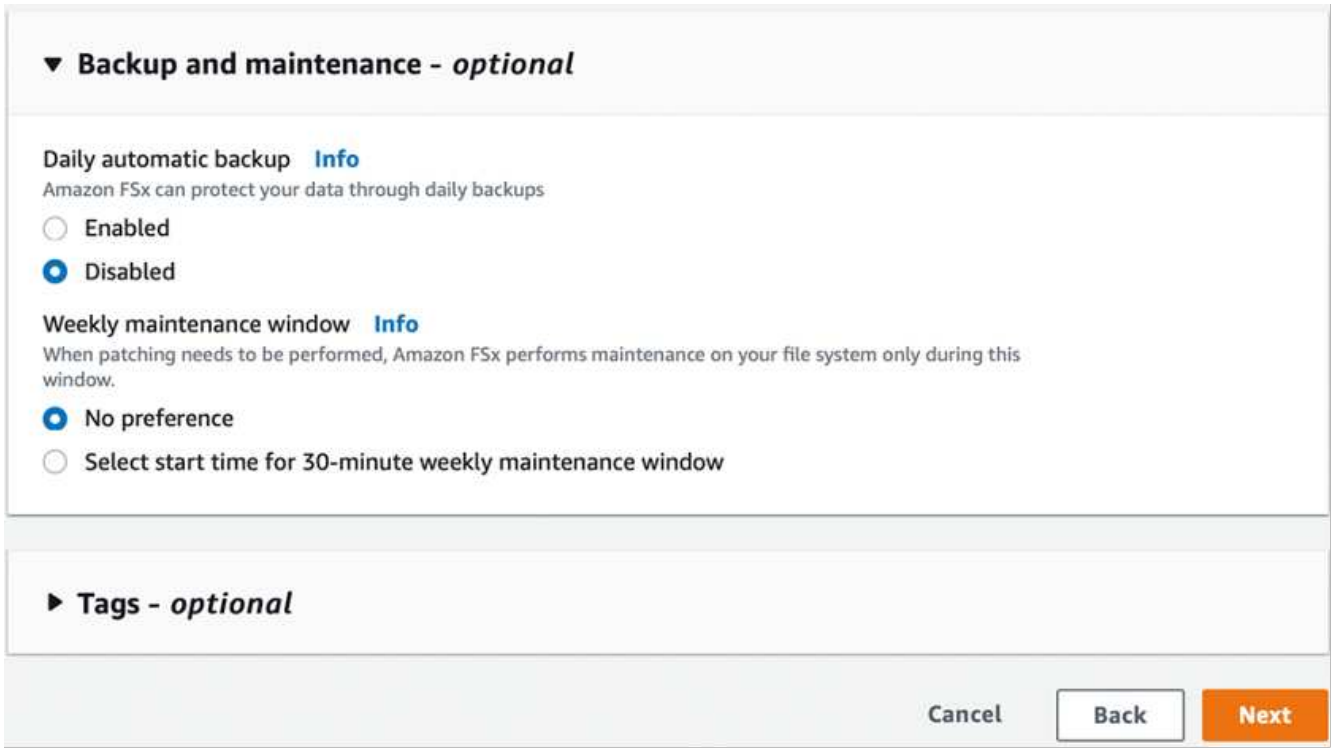


10. 볼륨을 생성한 후 ONTAP 명령줄 인터페이스(ONTAP CLI)를 사용하여 다음 매개변수를 수정합니다.

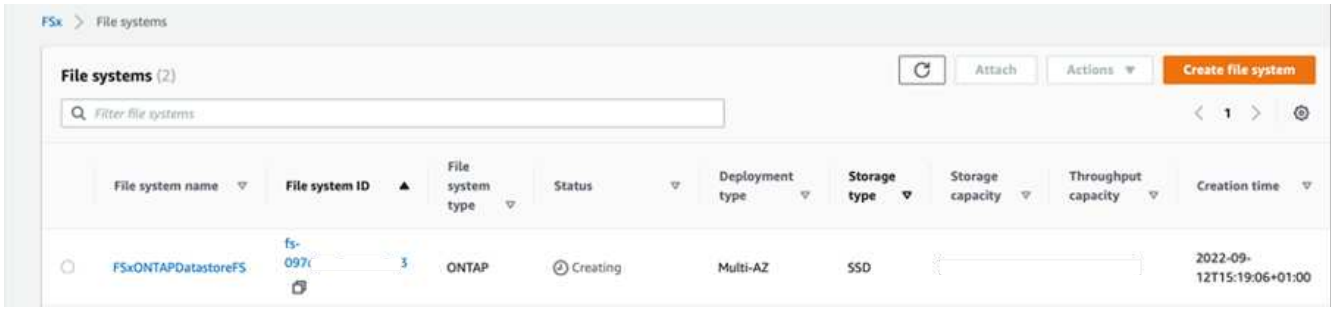
환경	구성
볼륨 보장	없음(씬 프로비저닝됨)
부분적 준비금	0%
스냅_예약	0%
자동 크기 조정	성장_축소
스토리지 효율성	활성화됨
볼륨 티어링 정책	스냅샷만
접근 시간 업데이트(-atime-update)	거짓
최소 미리 읽기(-min-readahead)	거짓
스냅샷 정책	None

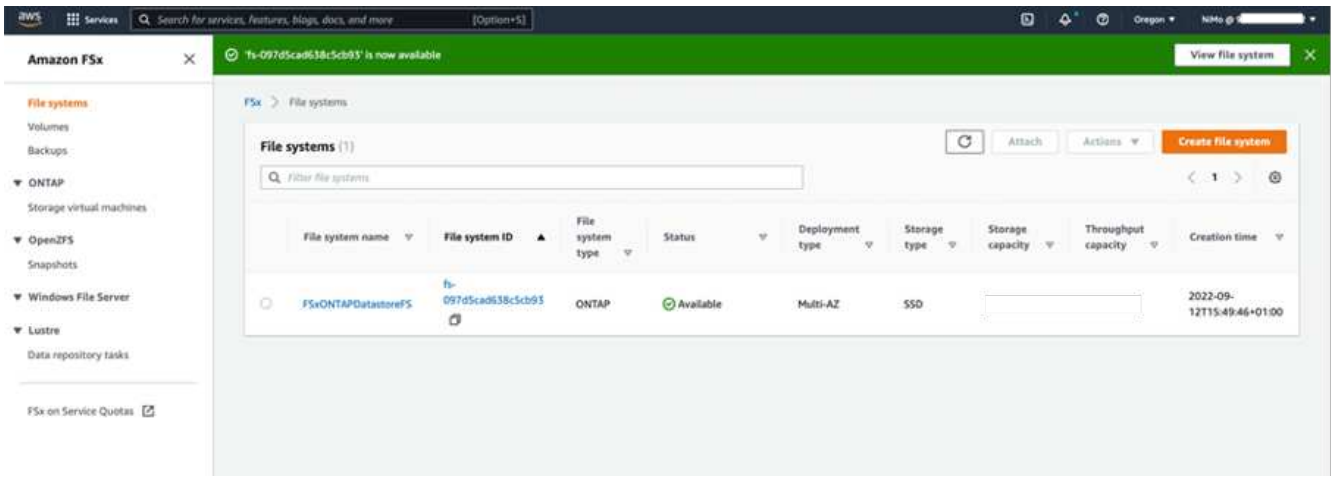
11. 선택 사항인 "백업 및 유지 관리" 단계에서 일일 자동 백업을 비활성화하고 주간 유지 관리 창에 대해 "선호 사항 없음"을 선택합니다.

    완료되면 "다음"을 클릭하세요.



12. 이제 이전 단계에 따라 설정한 전체 파일 시스템 구성을 검토하게 됩니다. 모든 매개변수가 올바른지 확인한 후 "파일 시스템 만들기" 버튼을 클릭하여 설정을 완료합니다.

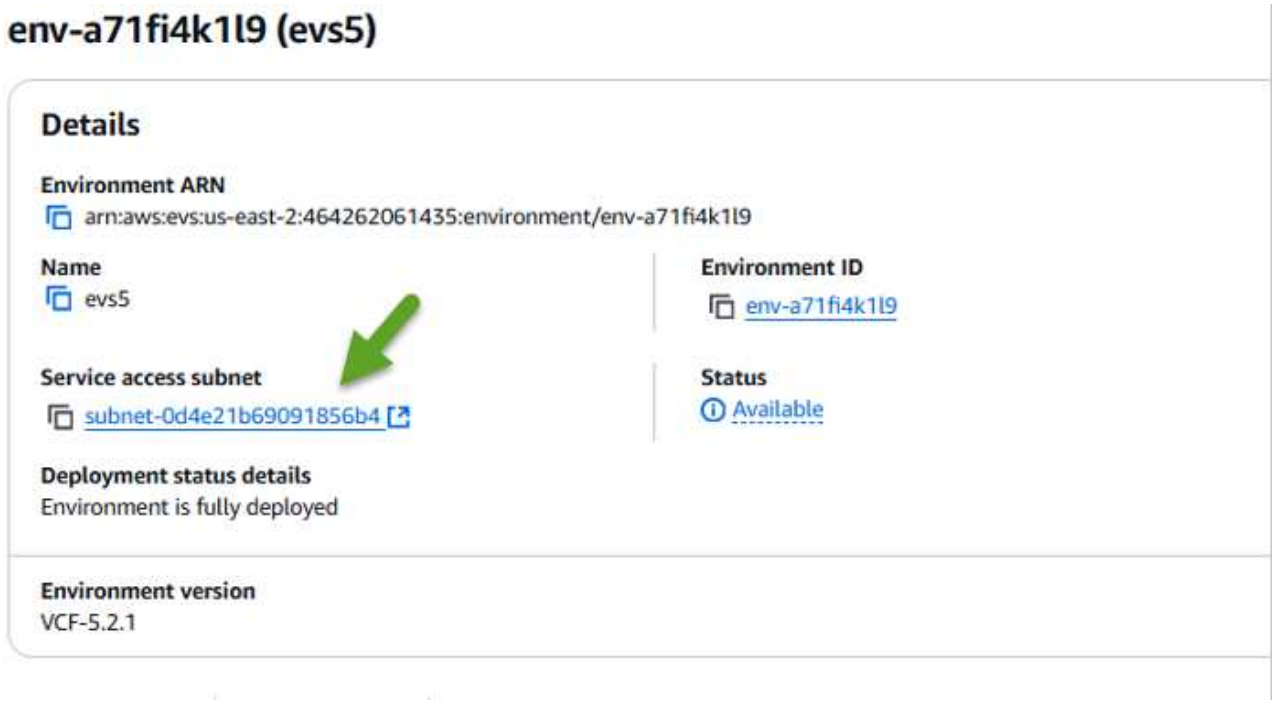




ONTAP 파일 시스템을 위한 추가 FSx를 만들려면 위에 자세히 설명한 단계를 따르고 필요에 따라 성능과 디스크 용량에 영향을 미치는 값을 조정합니다. FSx for ONTAP 의 성능 옵션에 대해 자세히 알아보려면 다음을 참조하세요."이 문서 페이지" .

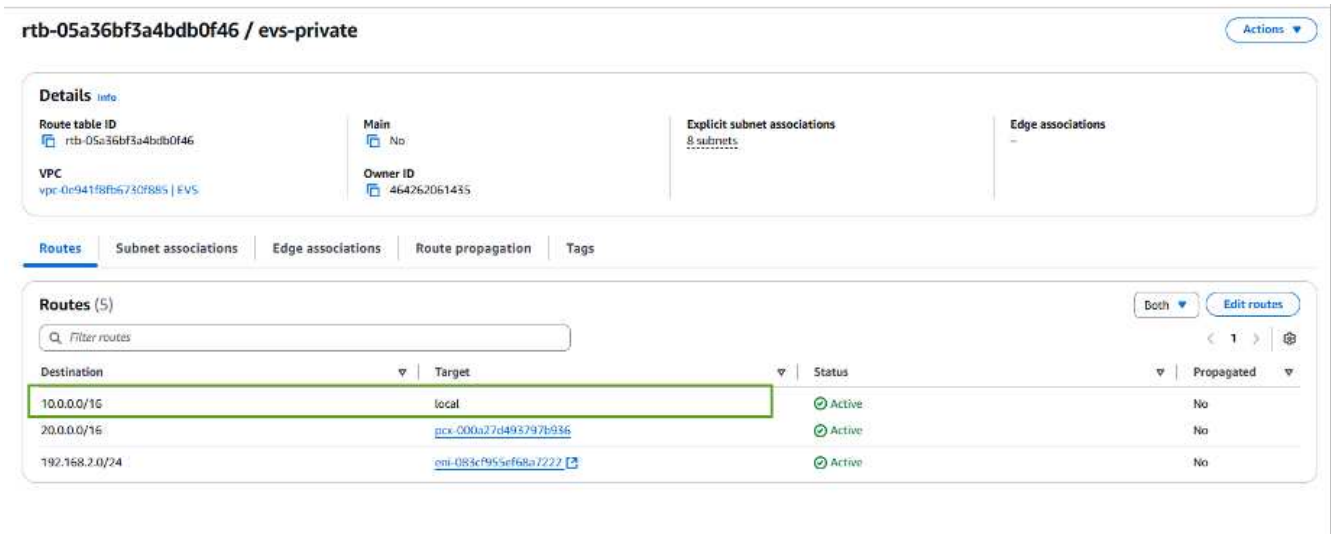
VPC와 SDDC 라우팅 및 보안 그룹을 검증하는 것은 Amazon EVS 가상화 환경과 FSx for ONTAP 파일 시스템 구성 요소가 제대로 함께 작동하는지 확인하는 데 중요합니다.

1. Elastic VMware Service > 가상화 환경 > [Amazon EVS 환경]으로 이동하여 아래의 녹색 화살표에 표시된 대로 서비스 액세스 서브넷을 선택하세요.

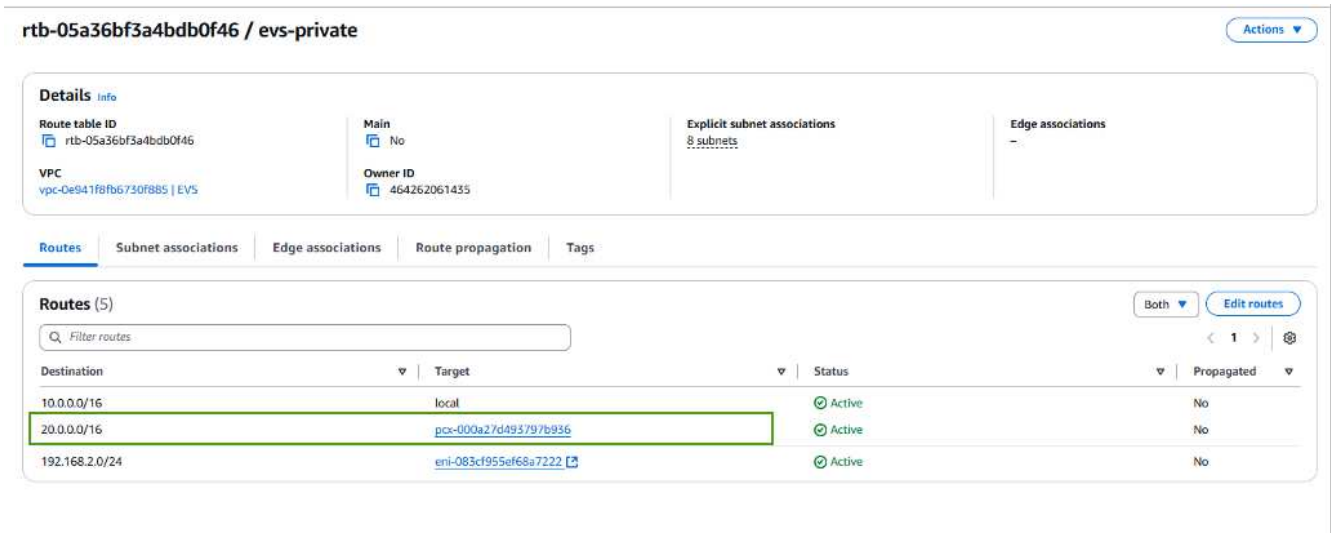


2. 서브넷 패널이 열립니다. 이 패널에서 경로 테이블을 찾아 클릭하세요.

   이 예에서 FSxN ONTAP 파일 시스템은 Amazon EVS VCF 환경과 동일한 VPC에 있으므로 기본 경로가 충분합니다.



   FSx for ONTAP 파일 시스템이 다른 VPC에 있는 경우 해당 VPC에 대한 경로가 추가되었는지 확인하세요. 이 예에서는 FSx for ONTAP 시스템이 있는 VPC에 대한 VPC 피어링을 위한 경로가 추가되었습니다.



3. 다음으로, FSx for ONTAP 파일 시스템에 연결된 보안 그룹(즉, ENI(Elastic Network Interface)에 연결된 보안 그룹, 즉 NFS 포트에 대한 액세스를 허용하는지 확인해야 합니다.)

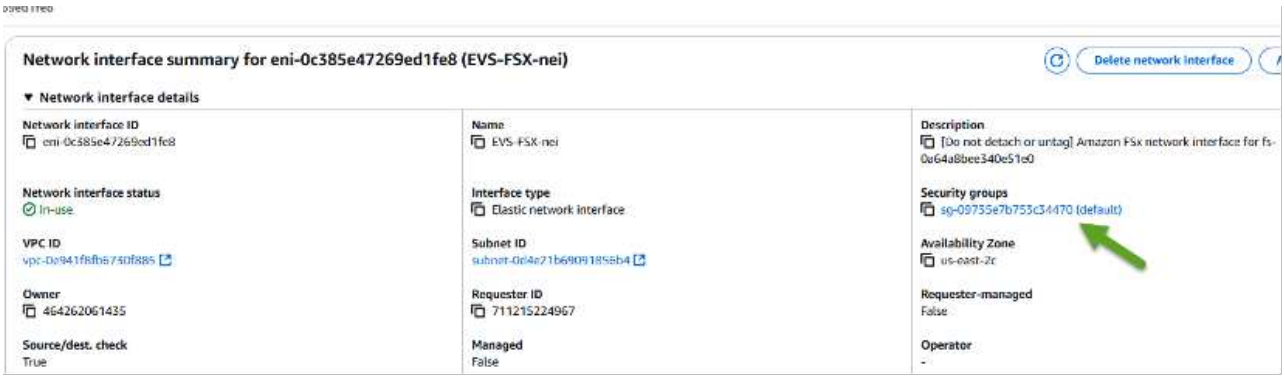
   NFS 및 iSCSI 프로토콜 포트의 전체 목록은 다음 링크를 참조하세요: https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/limit-access-security-groups.html [Amazon VPC를 사용한 파일 시스템 액세스 제어 설명서].

   FSx for ONTAP 파일 시스템이 보안 그룹과 연결되어 있는지 확인하려면:

   a. AWS 콘솔에서 FSx > 파일 시스템 > [FSx for ONTAP 파일 시스템]으로 이동합니다.

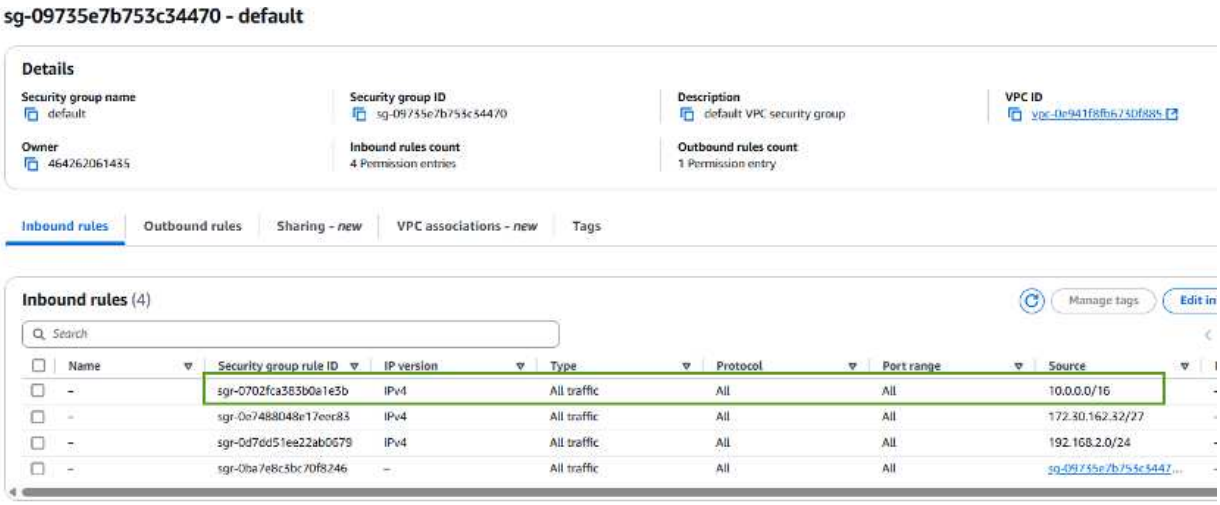
   b. 네트워크 및 보안 탭에서 ENI를 클릭합니다.

   c. 네트워크 인터페이스 세부 정보 아래에 나열된 보안 그룹을 찾으세요. ENI와 연결되어 있습니다(아래 이미지에서 녹색 화살표로 표시).



   d. 포트를 검증합니다. 다음 화면에 표시된 예에서는 모든 트래픽이 허용됩니다. 하지만 NFS 포트로만 제한할 수 있습니다. 포트 목록은 다음과 같습니다.

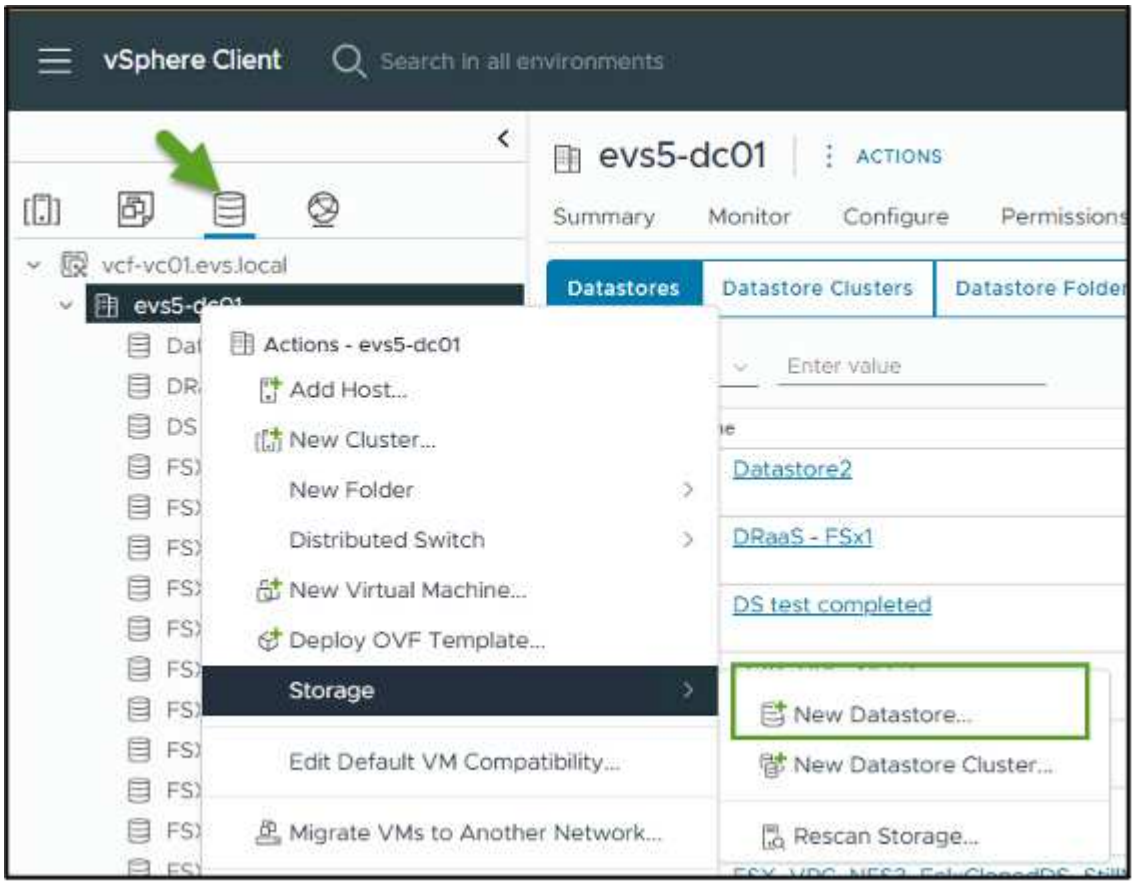
      - 포트 111 TCP: NFS 요청에 사용되는 포트를 협상하는 데 사용되는 포트매퍼입니다.
      - 포트 635 TCP: Mountd는 들어오는 마운트 요청을 수신하기 위한 것입니다.
      - 포트 2049 TCP: NFS 트래픽을 처리하는 NFS.
      - 포트 4045 TCP: 잠금 요청을 처리하는 네트워크 잠금 관리자(NLM)입니다.
      - 포트 4046 TCP: 잠금 관리를 위해 서버가 재부팅될 때 NFS 클라이언트에 알림을 보내는 네트워크 상태 모니터(NSM)입니다.



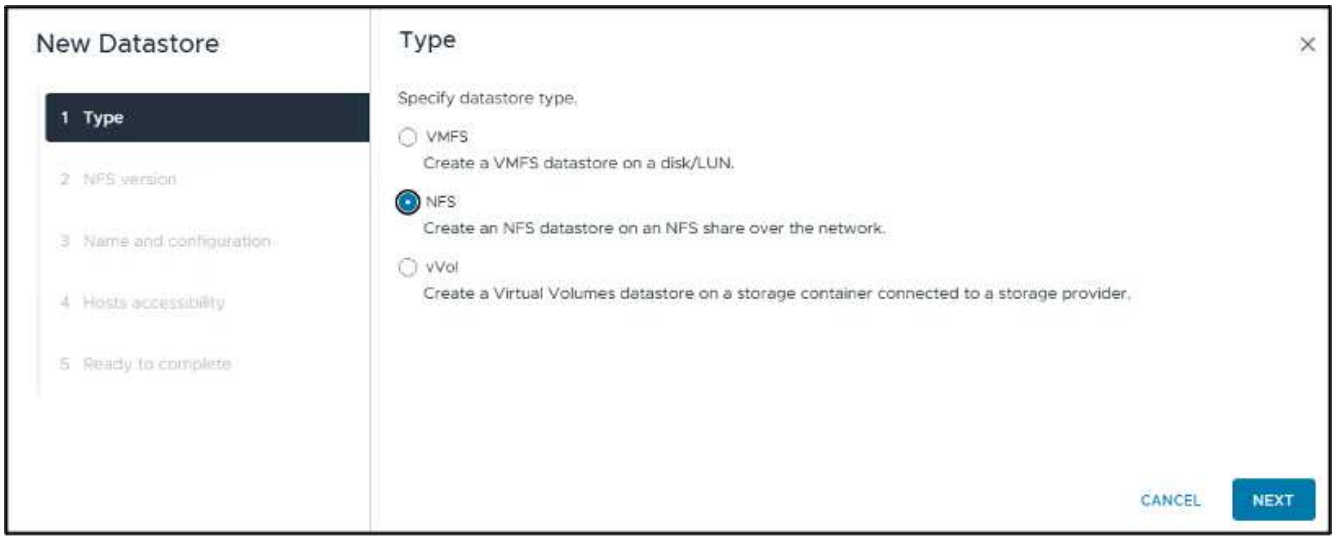
데이터 저장소로 사용하기 위해 **Amazon EVS**에 **ONTAP NFS** 볼륨용 **FSx** 연결

이제 FSx for ONTAP 파일 시스템이 프로비저닝되었고 모든 적절한 연결 매개변수가 검증되었으므로 FSx for ONTAP 스토리지 볼륨을 Amazon EVS에 연결할 차례입니다. 다음 단계에서는 vCenter에 액세스하고 FSx for ONTAP 볼륨을 NFS 데이터 저장소로 마운트하는 방법을 보여줍니다.

1. vSphere 클라이언트에서 "데이터 저장소" 탭으로 이동합니다. 아래에 표시된 대로 데이터 센터를 찾아 저장소 > 새 데이터 저장소로 이동합니다.

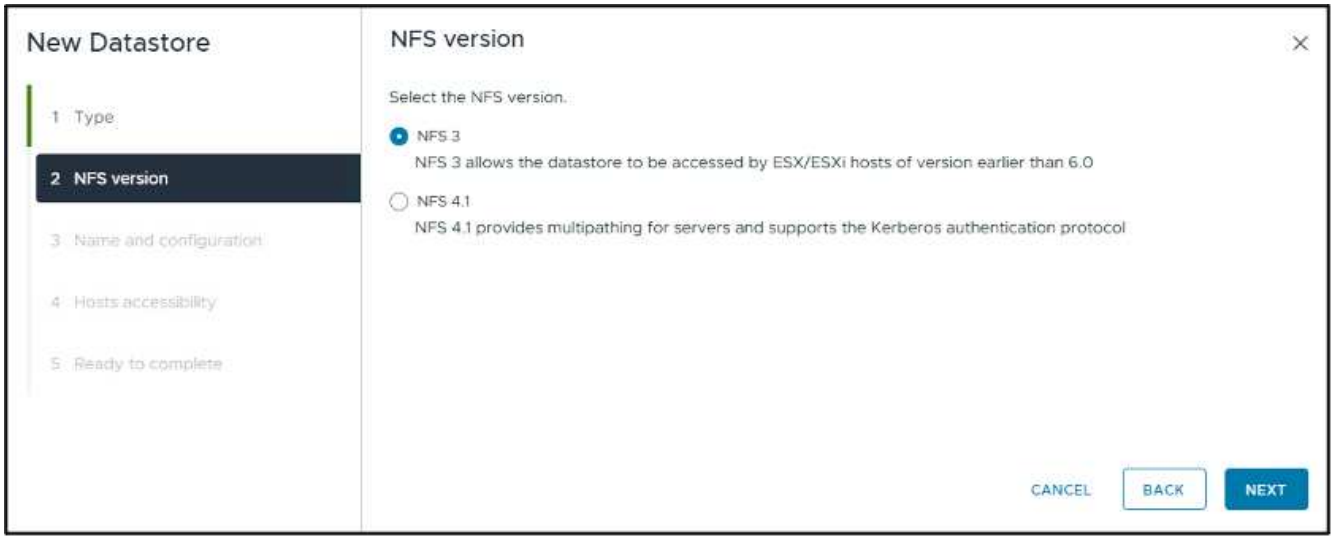


2. 이제 새로운 데이터 저장소 마법사가 시작됩니다. "유형" 단계에서는 데이터 저장소 유형을 선택합니다. "NFS"를 선택하고 "다음"을 클릭하여 계속 진행합니다.



3. "NFS 버전" 단계에서는 NFS 버전을 선택합니다.

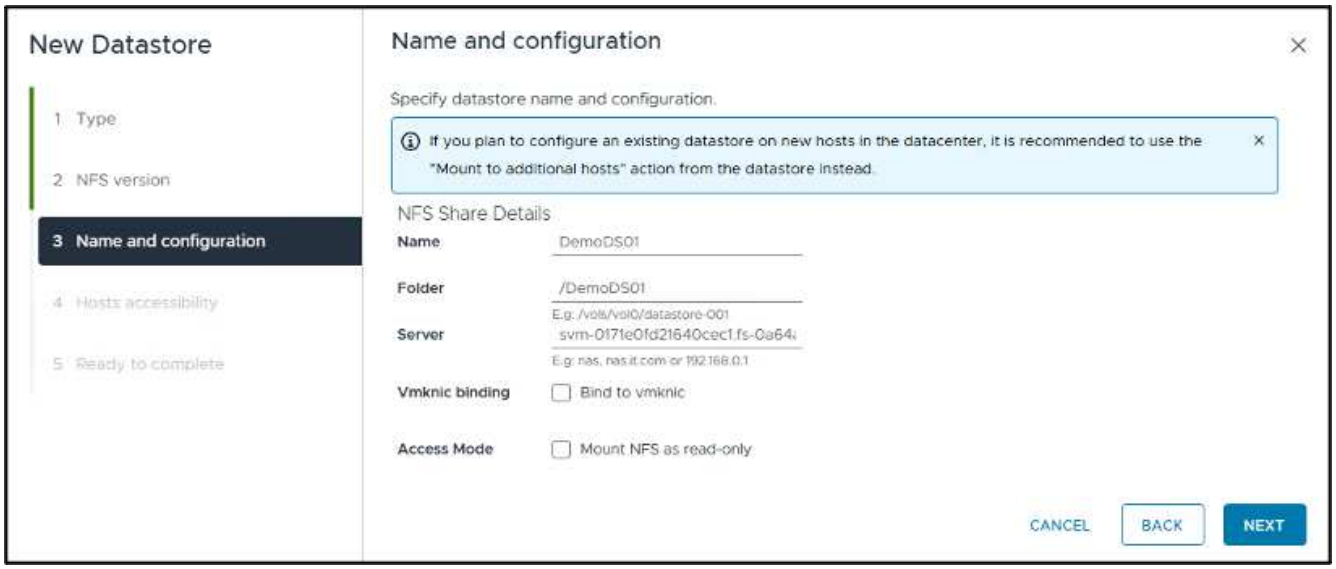
   이 예제에서는 "NFS 3"을 선택하지만 NFS v4.1도 사용할 수 있다는 점에 유의하세요.



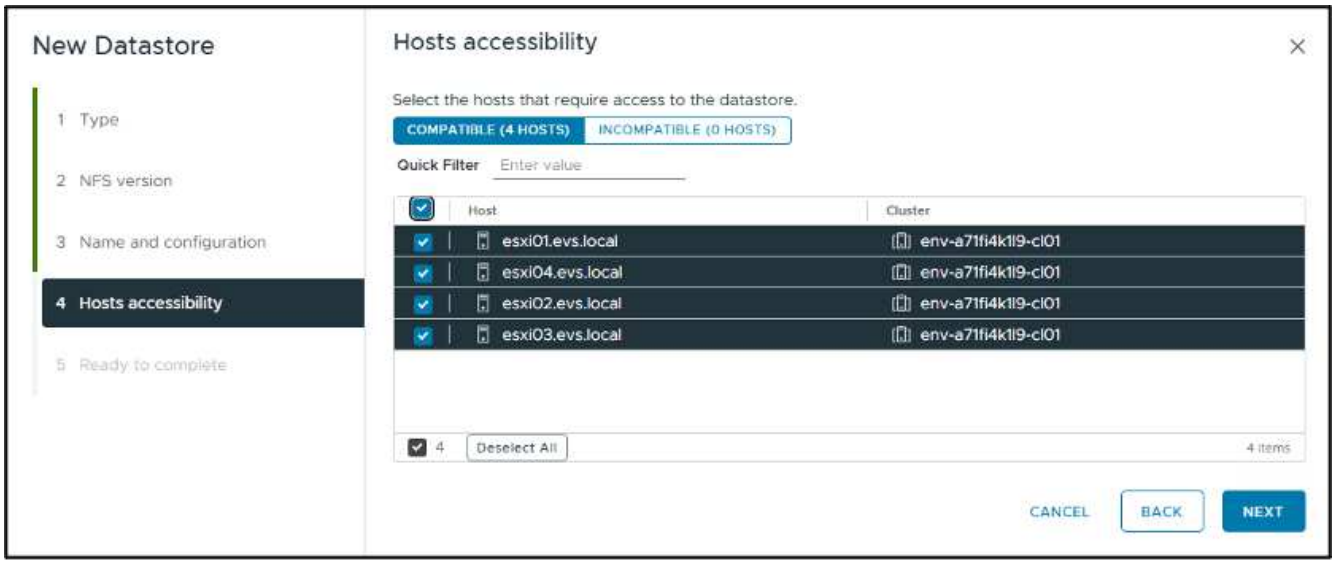
4. "이름 및 구성" 단계에서는 다음을 수행합니다.

   a. 데이터 저장소의 이름을 지정합니다.
   b. 폴더 이름을 지정하세요. NFS 볼륨에 대한 연결 경로를 사용하세요.
   c. 서버의 이름을 지정하세요. SVM의 NFS DNS 이름이나 NFS의 IP 주소를 사용하세요.

      계속하려면 "다음"을 클릭하세요.



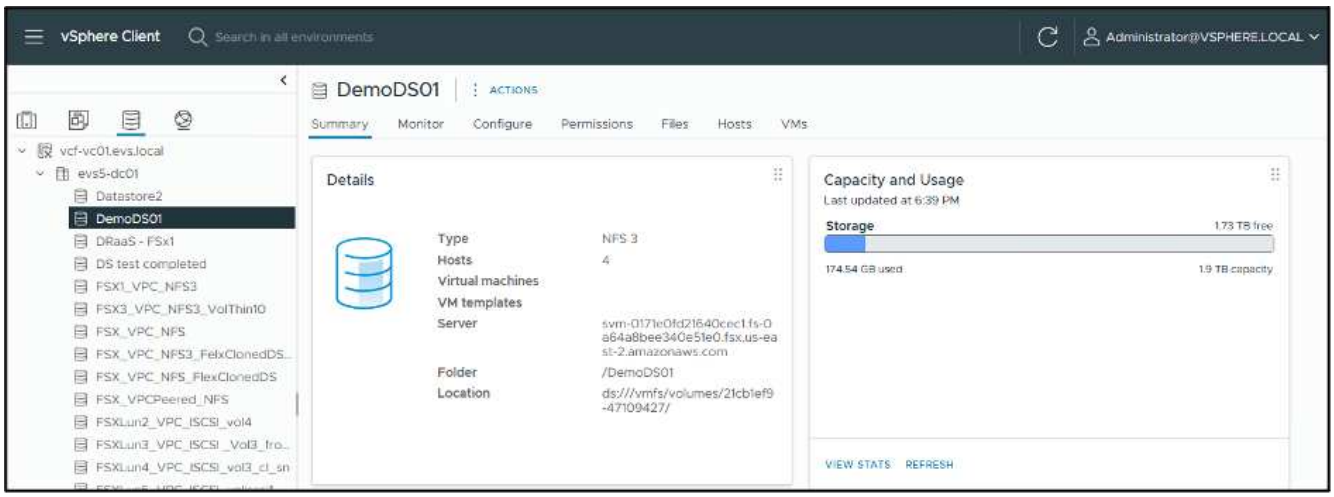
5. "호스트 접근성" 단계에서 데이터 저장소에 액세스해야 하는 모든 호스트를 선택한 다음 "다음"을 클릭하여 계속합니다.



6. "완료 준비" 단계에서 데이터를 검토하고 "완료"를 클릭하여 설정을 완료합니다.



7. 아래와 같이 vCenter에 액세스하여 NFS 데이터 저장소가 연결되었는지 확인합니다.



FSx for ONTAP iSCSI 데이터 저장소로 사용하기 위한 배포 절차

이 섹션에서는 FSx for ONTAP 을 사용하여 iSCSI 데이터 저장소를 구성하는 단계를 다룹니다.

필수 조건

FSx for ONTAP iSCSI 데이터 저장소로 프로비저닝하고 연결하기 전에 먼저 Amazon EVS 가상화 환경을 배포해야 합니다. 자세한 내용은 Amazon EVS 시작하기 가이드 문서를 참조하세요. 이 섹션에서는 FSx for ONTAP 파일 시스템을 배포했다고 가정합니다. 적절한 단계는 위의 자세한 접근 방식 섹션을 참조하세요.

고수준 배포 단계

Amazon EVS의 iSCSI 데이터 저장소로 사용하기 위해 FSx for ONTAP 파일 시스템을 배포하고 두 서비스 간의 연결을 설정하는 데는 다음 단계가 포함됩니다.

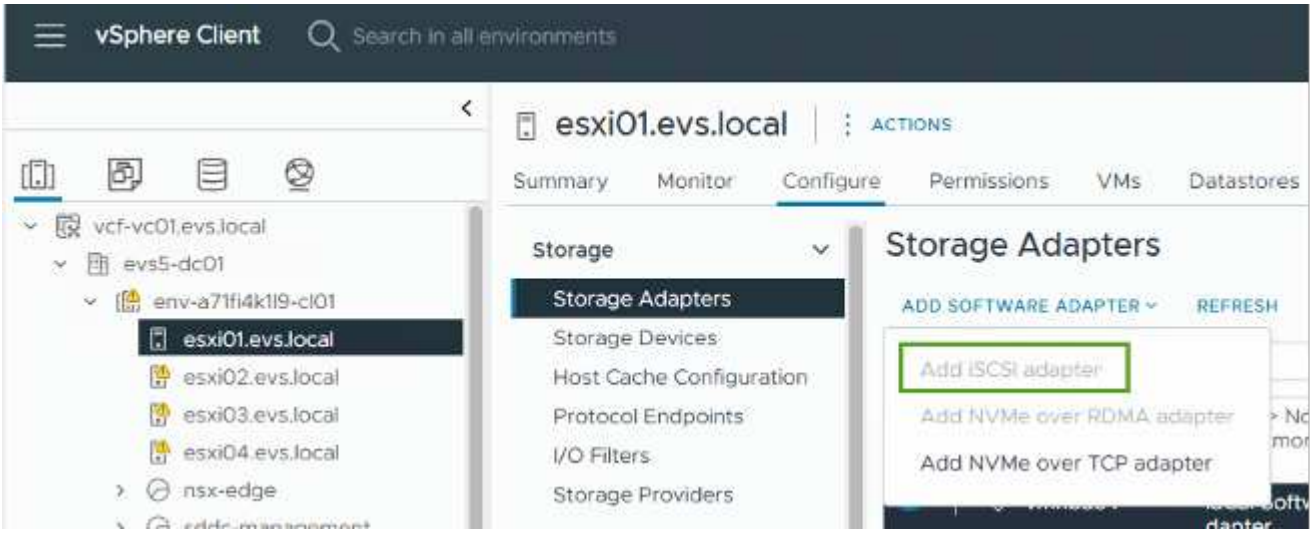
- 각 ESXi 호스트에 대한 iSCSI 네트워크 어댑터 설정.
- FSx for ONTAP 파일 시스템, 볼륨, LUN 등을 만들고 구성합니다.

- ESXi 호스트를 FSx for ONTAP 파일 시스템 서버에 연결합니다.
- iSCSI 데이터스토어 가상 머신 파일 시스템(VMFS)을 생성합니다.

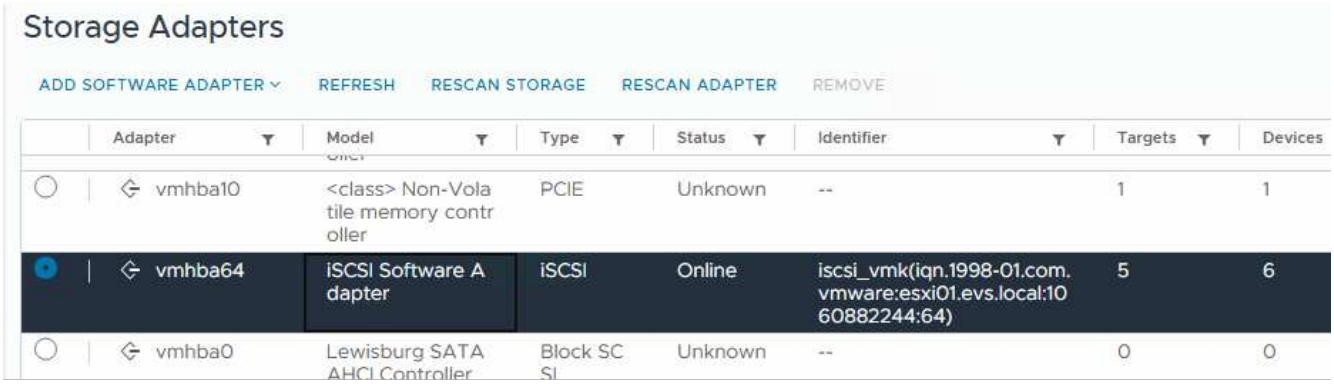
iSCSI 네트워크 어댑터 추가

다음 단계는 사용자 환경의 각 ESXi 호스트에서 수행해야 합니다.

1. vSphere 클라이언트를 입력하고 ESXi 호스트를 선택합니다. 구성 탭에서 "소프트웨어 어댑터 추가"를 선택한 다음, 아래와 같이 드롭다운 메뉴에서 "iSCSI 어댑터 추가"를 선택합니다.

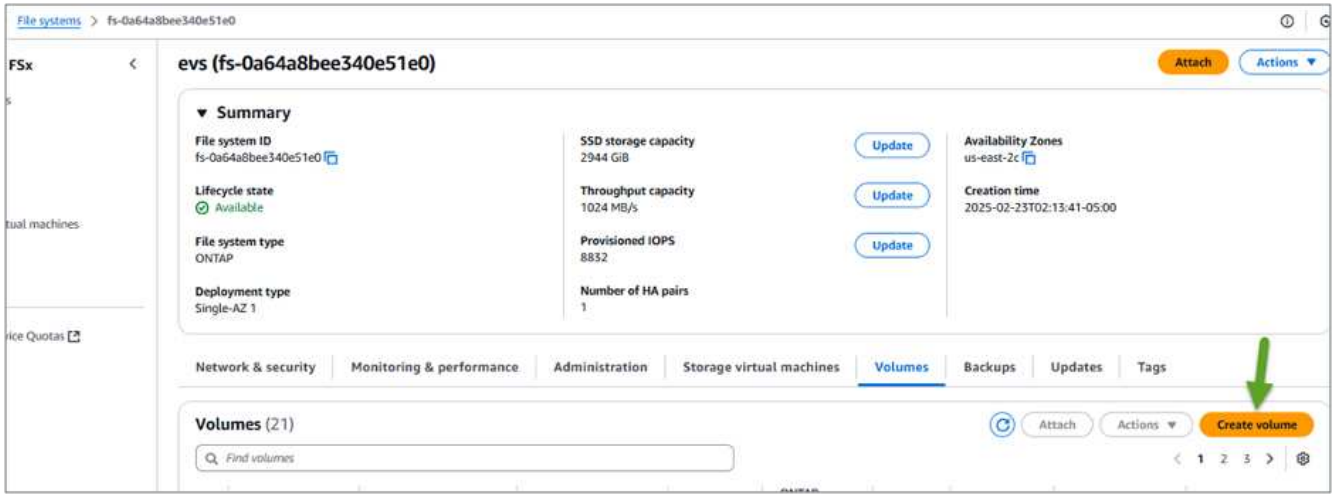


2. 설치가 완료되면 저장소 어댑터 화면이 나타납니다. 메뉴 막대에서 "어댑터 재검사"를 선택합니다. iSCSI 어댑터의 IQN을 기록합니다: iqn.xxxx. 이 값은 나중에 LUN 매핑 단계에서 사용됩니다.



ONTAP 볼륨에 대한 **FSx** 생성

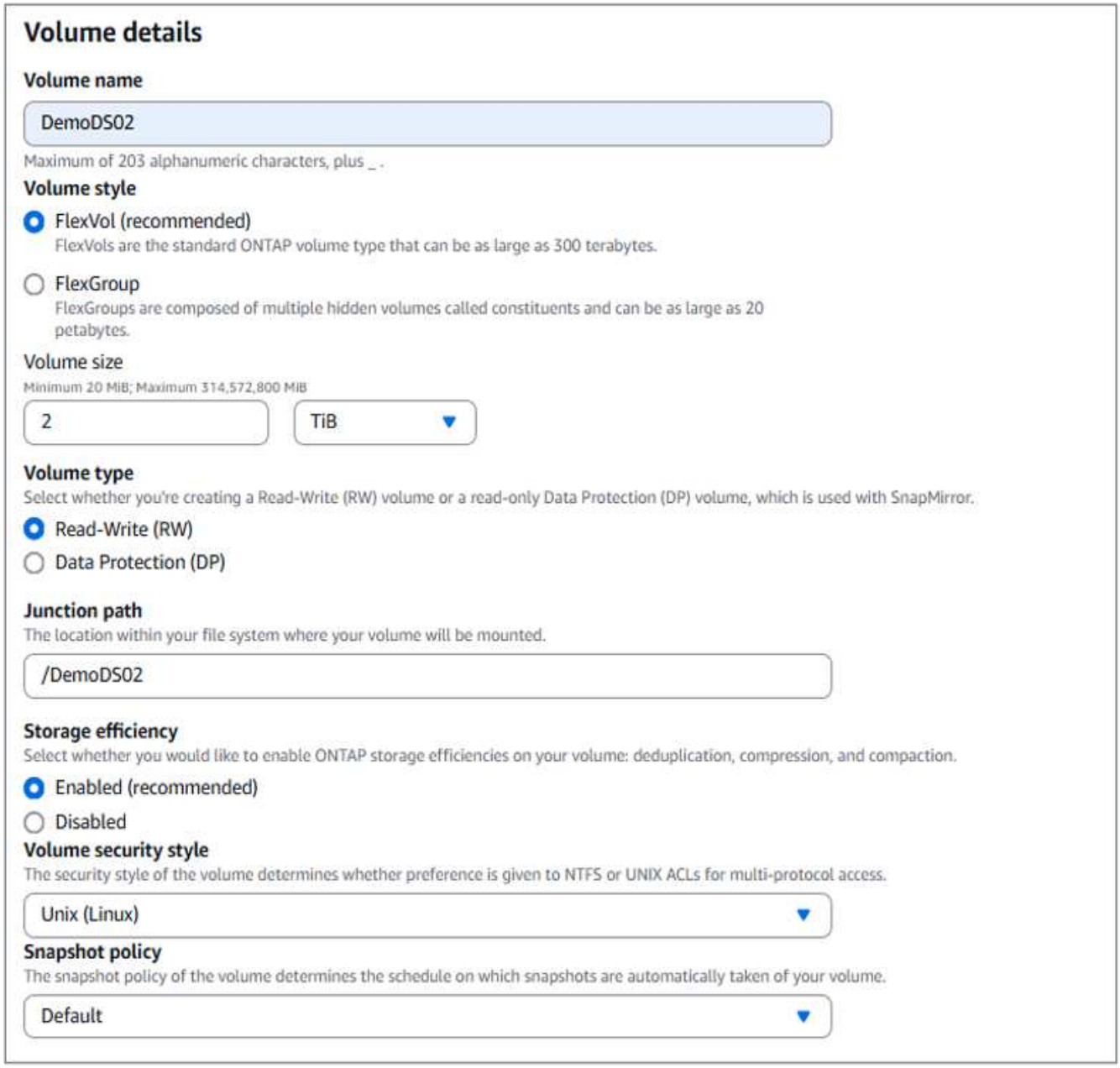
1. AWS 콘솔로 이동하여 FSx for ONTAP 파일 시스템 페이지로 들어가서 "볼륨 생성"을 클릭합니다.



2. 볼륨을 생성할 SVM을 선택합니다.



3. "볼륨 세부 정보" 페이지에서 아래 스크린샷에 표시된 대로 세부 정보를 입력하세요. 완료되면 "만들기"를 클릭하여 볼륨을 설정하세요. ONTAP 스토리지 효율성 기능(압축, 중복 제거, 압축)을 켜려면 "활성화"를 선택합니다.



4. 스토리지 계층화 옵션의 경우 드롭다운 메뉴에서 "스냅샷만"을 선택하고 계층화 정책 냉각 기간을 설정합니다. 기본값은 31일이지만, 이 예에서는 2일의 냉각 기간을 설정했습니다.



5. 볼륨이 생성되면 ONTAP CLI를 사용하여 다음 값을 설정합니다.

환경	구성
볼륨 보장	없음(씬 프로비저닝됨)
부분적 준비금	0%
스냅_예약	0%
자동 크기 조정	성장_축소
스토리지 효율성	활성화됨
볼륨 티어링 정책	스냅샷만
접근 시간 업데이트(-atime-update)	거짓
최소 미리 읽기(-min-readahead)	거짓
스냅샷 정책	None
LUN 공간 예약	장애가 있는
LUN 공간 할당	활성화됨

LUN, igroup 생성 및 LUN 매핑

이 섹션에서는 vSphere에 디스크로 나타날 LUN을 만드는 방법을 보여줍니다. 또한 LUN에 액세스할 수 있는 이니시에이터 목록인 이니시에이터 그룹(igroup)을 만드는 방법도 보여드리겠습니다. igroup은 vSphere ESXi 호스트에서 LUN에 대한 액세스를 허용합니다. 마지막으로 igroup을 LUN에 매핑하는 방법을 보여드리겠습니다.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 FSx for ONTAP 파일 시스템이나 SVM의 관리 포트에서 SSH 세션을 설정합니다.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

2. LUN을 생성합니다. 공간 할당 및 공간 예약을 활성화로 설정하세요. 크기는 볼륨 크기의 최대 90%여야 합니다.

```
Fsxid::> lun create -vserver fsx -path /vol/DemoDS02/lun_name -size 1.8T
-ostype vmware -space-allocation enabled -space-reservation disabled
```

3. igroup을 만들고 클러스터 내의 모든 ESXi 호스트의 IQN을 추가합니다.

```
Fsxid::> lun igroup create -vserver fsx -igroup evs1 -protocol iscsi
-ostype vmware -initiator iqn.1998-
01.com.vmware:esxi01.evs.local:1060882244:64,iqn.1998-
01.com.vmware:esxi02.evs.local:1911302492:64,iqn.1998-
01.com.vmware:esxi03.evs.local:2069609753:64,iqn.1998-
01.com.vmware:esxi04.evs.local:1165297648:64
```

4. 다음 코드로 LUN을 매핑하세요.

```
Fsxid::> lun mapping create -vserver fsx -path /vol/DemoDS02/lun1
-igroup evs1 -lun-id 2
```

5. LUN 매핑을 검토하고 상태가 "매핑됨"으로 변경되었는지 확인합니다. LUN이 매핑된 상태인지 확인하기 위한 필수적인 이중 확인입니다.

```
Fsxid::> lun show
Vserver   Path                            State   Mapped   Type
Size
--------- ------------------------------- ------- -------- --------
--------
fsx       /vol/DemoDS02/lun1              online  mapped   vmware
1.80TB
```

SVM에서 iSCSI 구성 정보 가져오기

1. iSCSI show를 실행하고 대상 이름을 기록합니다. 이는 FSx for ONTAP 디스크의 vSphere 검색에 사용됩니다 (참고: 이 대상 이름은 SVM에 고유합니다).

```
Fsxid::> iscsi show -vserver fsx
                 Vserver: fsx
             Target Name: iqn.1992-
08.com.netapp:sn.c083e374f1b711ef9d9f8123a3ebcf46:vs.3
            Target Alias: fsx
   Administrative Status: up
```

2. iSCSI IP 주소를 기록하세요.

```
Fsxid::> network interface show -vserver fsx -data-protocol iscsi
-fields address
vserver lif       address
------- -------   -----------
fsx     iscsi_1   10.0.10.134
fsx     iscsi_2   10.0.10.227
```

FSx for ONTAP iSCSI 서버를 찾아보세요

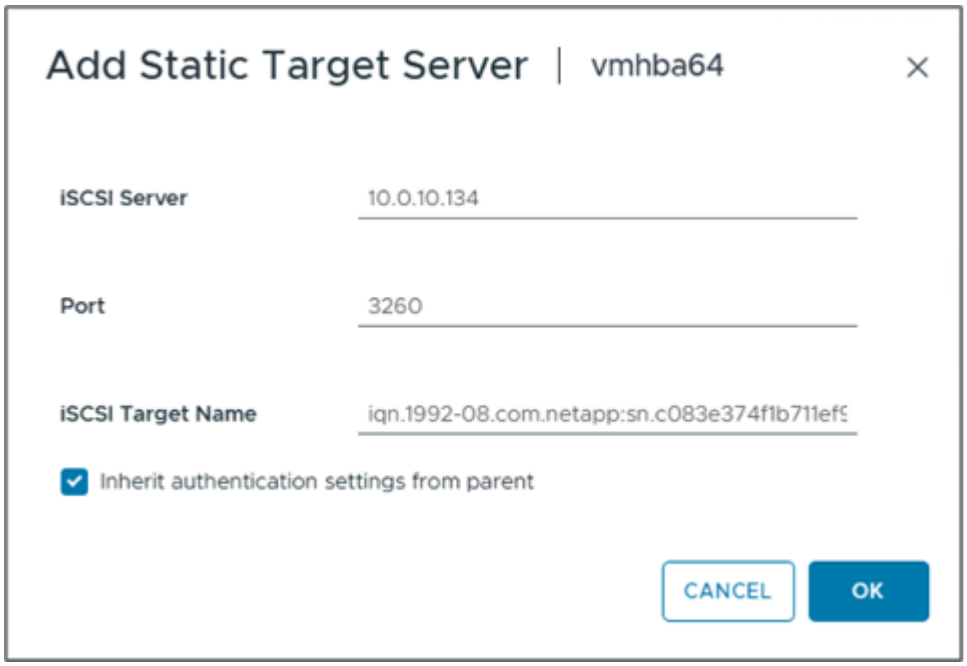
이제 LUN이 매핑되었으므로 SVM의 FSx for ONTAP iSCSI 서버를 검색할 수 있습니다. SDDC에 있는 각 ESXi 호스트에 대해 여기에 나열된 단계를 반복해야 합니다.

1. 먼저, FSx for ONTAP 파일 시스템에 연결된 보안 그룹(즉, ENI에 연결된 그룹)이 iSCSI 포트를 허용하는지 확인하세요.

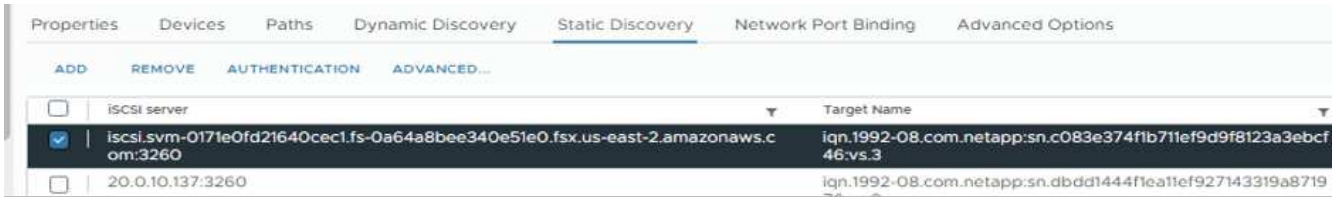
   iSCSI 프로토콜 포트의 전체 목록과 이를 적용하는 방법은 다음을 참조하세요."Amazon VPC를 사용한 파일

시스템 액세스 제어" .

2. vSphere Client에서 ESXi 호스트 > 스토리지 어댑터 > 정적 검색으로 이동한 후 "추가"를 클릭합니다.
3. 위의 iSCSI 서버 IP 주소를 입력하세요(포트는 3260). iSCSI 대상 이름은 iSCSI show 명령의 IQN입니다. 계속하려면 "확인"을 클릭하세요.



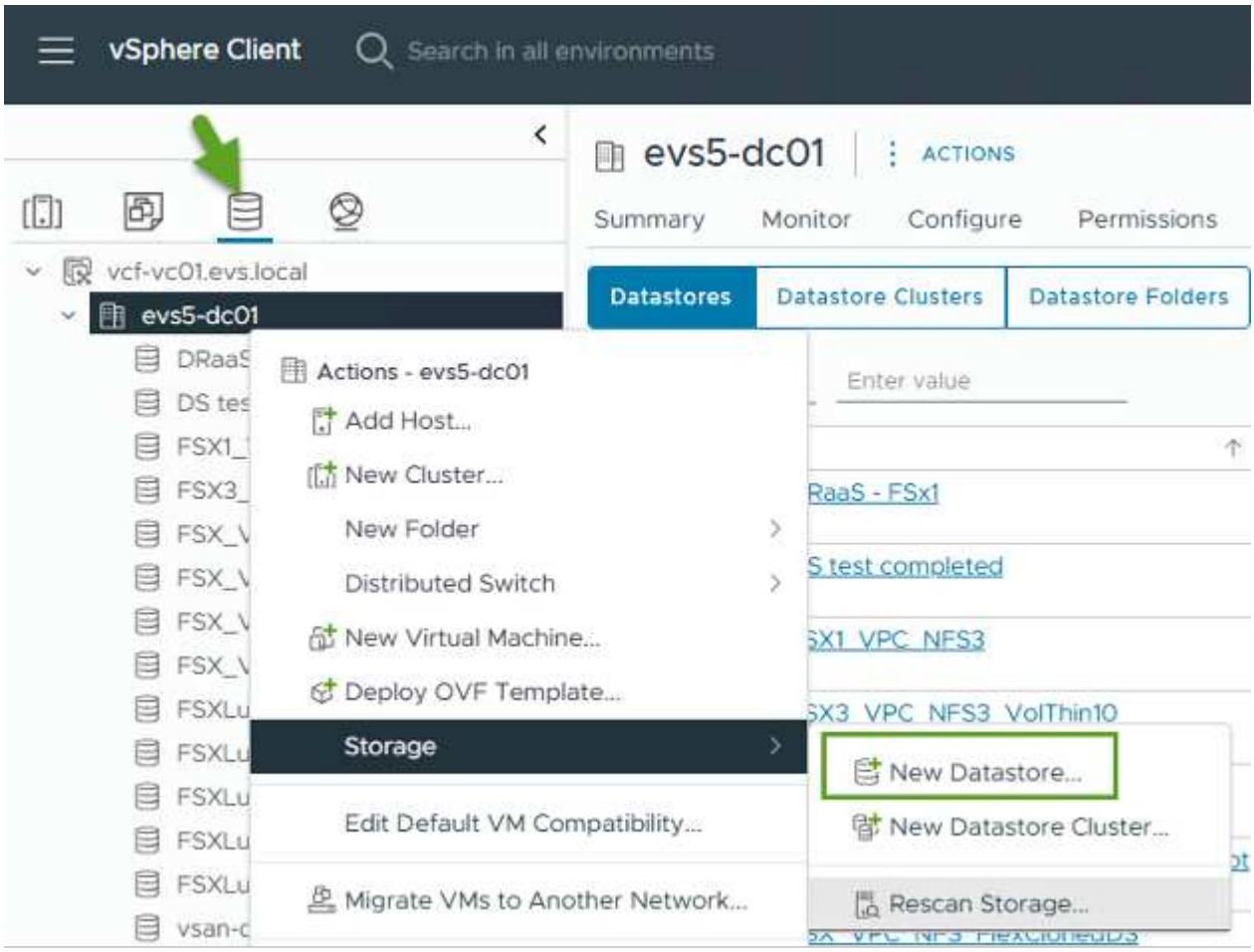
4. 마법사가 닫히고 데이터 저장소 정적 검색 화면이 표시됩니다. 이 페이지의 표에서 대상이 발견되었음을 확인할 수 있습니다.



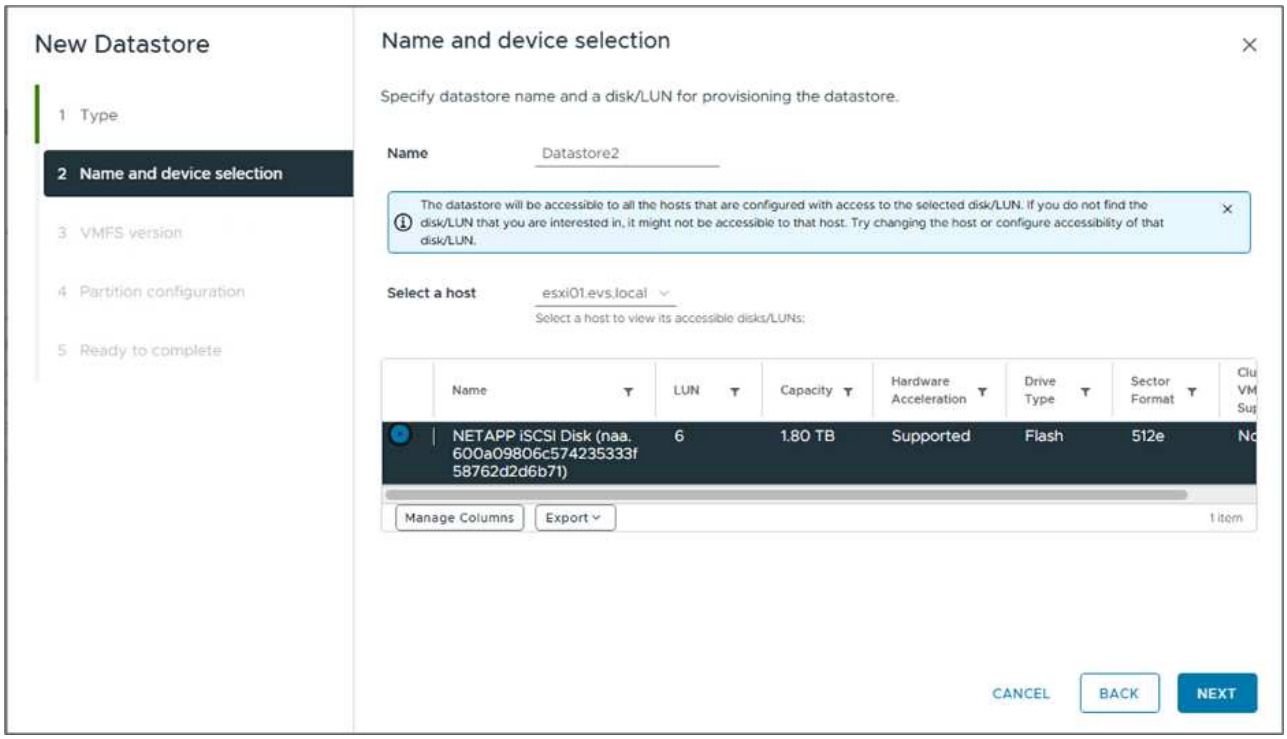
iSCSI 데이터 저장소 만들기

이제 iSCSI 서버를 발견했으므로 iSCSI 데이터 저장소를 만들 수 있습니다.

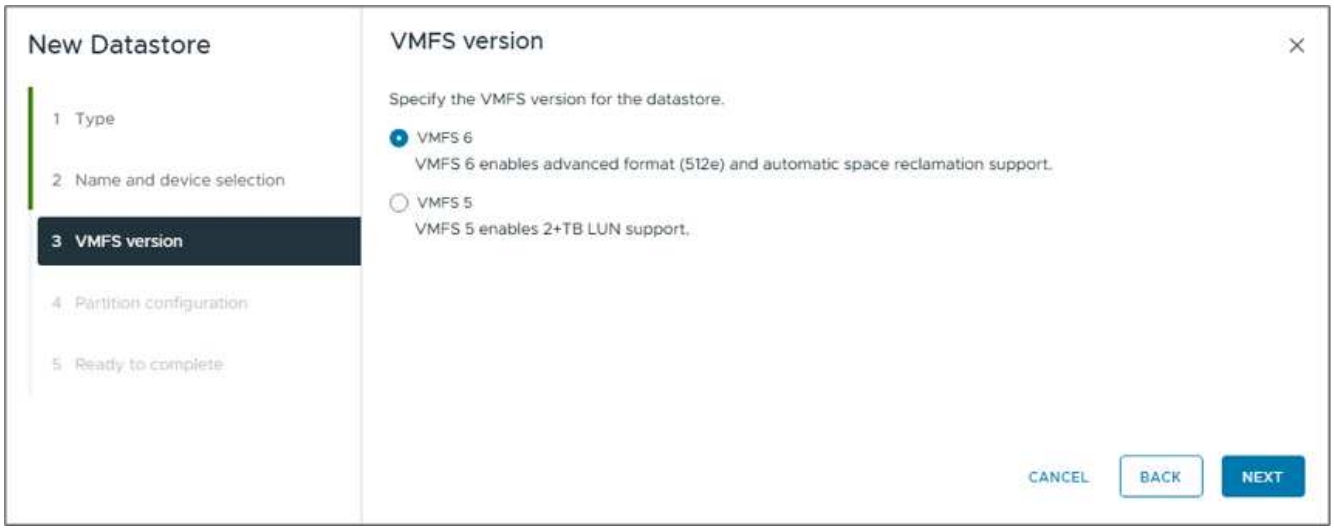
1. vSphere 클라이언트에서 데이터스토어 탭으로 이동하여 데이터스토어를 배포할 SDDC를 선택합니다. 마우스 오른쪽 버튼을 클릭하고 저장소 아이콘(아래 스크린샷에서 녹색 화살표로 표시)을 선택한 다음 드롭다운 메뉴에서 "새 데이터 저장소"를 선택합니다.



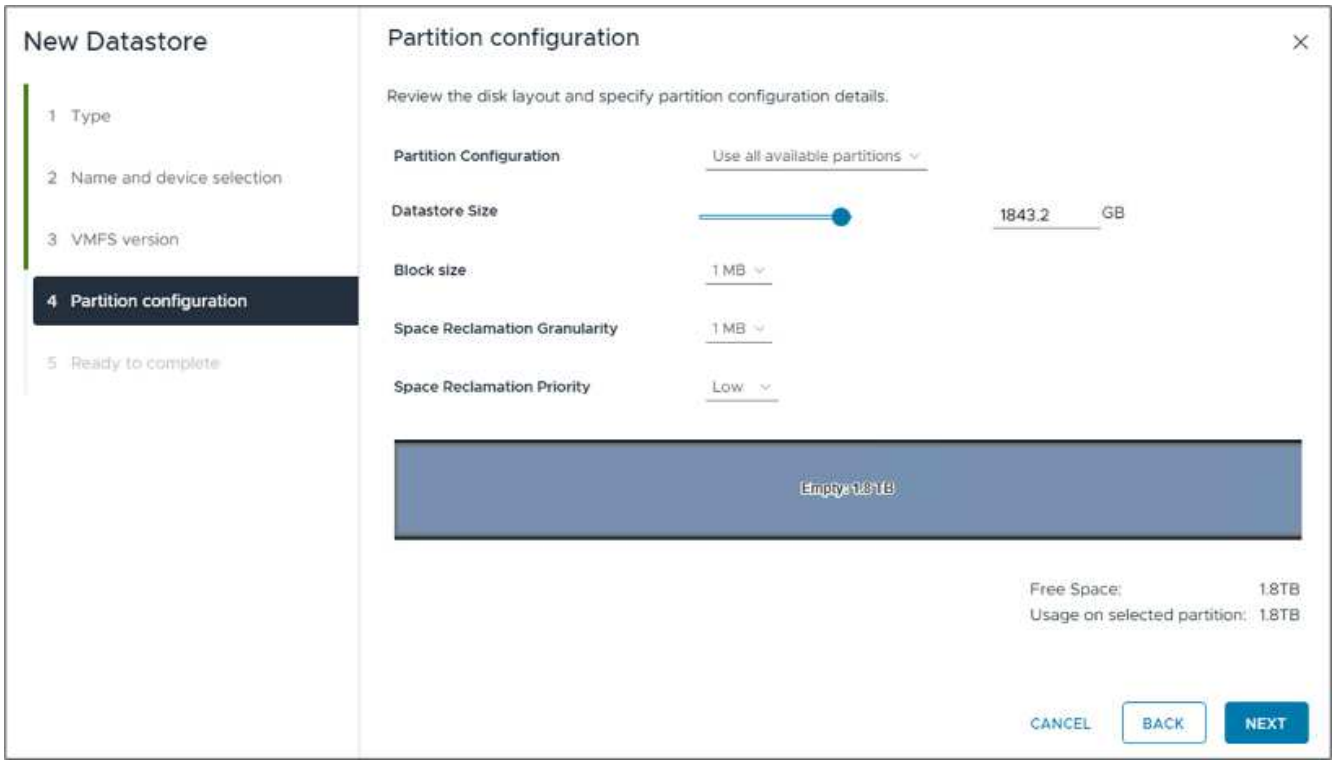
2. 이제 새로운 데이터 저장소 마법사가 시작됩니다. "유형" 단계에서 VMFS 옵션을 선택합니다.
3. "이름 및 장치 선택" 단계에서:
   a. 데이터 저장소의 이름을 입력하세요.
   b. 데이터스토어에 연결할 ESXi 호스트를 선택하세요.
   c. 검색된 디스크(LUN)를 선택하고 "다음"을 클릭합니다.



4. "VMFS 버전" 단계에서 "VMFS 6"을 선택합니다.



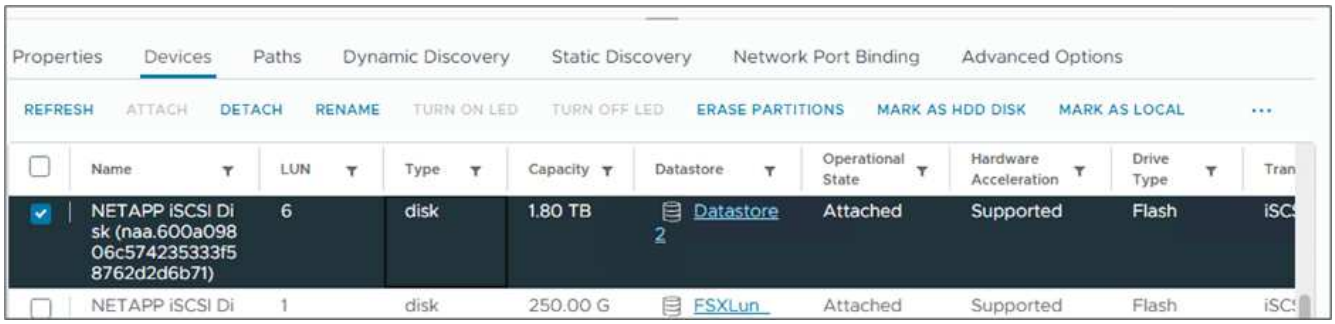
5. "파티션 구성" 단계에서는 "사용 가능한 모든 파티션 사용" 옵션을 포함하여 기본 설정을 그대로 둡니다. 계속하려면 "다음"을 클릭하세요.



6. "완료 준비" 단계에서 설정이 올바른지 확인하세요. 완료되면 "완료"를 클릭하여 설정을 완료하세요.



7. 장치 페이지로 돌아가서 데이터 저장소가 연결되었는지 확인하세요.



결론

이 문서에서는 NFS 및 iSCSI 프로토콜 모두와 함께 사용할 수 있는 Amazon EVS의 외부 스토리지로 FSx for ONTAP 을 설정하는 방법에 대한 지침을 제공합니다.

Amazon EVS의 외부 스토리지로 FSx for ONTAP 을 사용하면 명확한 운영적, 비즈니스적 가치가 제공됩니다. ONTAP 기술을 통해 더 나은 데이터 복원력, 보호, 복제 및 비용 효율성을 제공하고 VMware 하이퍼 컨버지드 아키텍처를 분리하여 TCO를 최적화합니다. FSx for ONTAP 사용하면 Amazon EVS 사용자는 컴퓨팅 리소스를 추가하거나 비용을 늘리지 않고도 스토리지를 확장할 수 있습니다. 이를 통해 AWS 클라우드가 제공하는 탄력성과 확장성의 잠재력이 최대한 발휘됩니다.

자세한 내용을 알아보려면 Amazon의 새로운 소식 공지를 읽어보세요."Amazon EVS가 이제 FSx for ONTAP 과 통합되었습니다." 및 NetApp 블로그:"Amazon EVS, FSx for ONTAP 지원 발표" .

EVS용 FSx ONTAP 데이터 저장소 보호

Amazon Elastic VMware Service를 사용하여 **Amazon FSx for NetApp ONTAP** 데이터스토어를 **NetApp SnapCenter Plug-in for VMware**로 보호하는 방법

이 가이드에서는 NetApp SnapCenter® Plug-in for VMware vSphere(SCV) 백업 및 복구 솔루션을 사용하여 FSx for ONTAP 네트워크 파일 시스템(NFS) 및 iSCSI Amazon EVS 데이터스토어와 관련 VM을 보호하기 위한 간단한 배포 방법을 설명합니다.

소개

Amazon FSx for NetApp ONTAP(FSx for ONTAP) 기반 Amazon Elastic VMware Service(Amazon EVS)용 보조 데이터스토어는 nConnect 활용, Amazon Virtual Private Cloud(Amazon VPC) 피어링, 데이터스토어 마운트당 여러 네트워크 연결 사용과 같은 고성능 워크로드와 스토리지 집약적인 워크로드를 모두 실행하는 데 탁월한 솔루션을 제공합니다.

이 기능을 통해 고객은 vSAN(가상 스토리지 영역 네트워크)에서 제공하는 로컬 인스턴스 스토리지의 한계를 극복하고, 컴퓨팅과 독립적으로 스토리지를 확장하며, 전체 총 소유 비용을 절감할 수 있습니다. 총 소유 비용(TCO) 이점 외에도 FSx for ONTAP은 온프레미스 ONTAP® 고객에게 익숙한 엔터프라이즈급 기능을 갖춘 Amazon EVS를 제공하여 배포를 최적화하고 간소화하는 데 도움을 줍니다. FSx for ONTAP을 사용하면 가상 머신(VM), 데이터스토어 및 가상 머신 디스크(VMDK)의 백업 및 복원 작업을 지원하는 NetApp® Snapshot™, SnapMirror® 및 SnapVault® 기술에 액세스할 수 있습니다. 주요 기능 중 하나는 Snapshot 기반 보호입니다.

개요

조직이 규모를 확장하고 환경을 통합함에 따라 워크로드와 기본 스토리지를 보호해야 할 필요성이 점점 더 중요해집니다. SCV를 사용하면 Amazon EVS vSphere 클라이언트에서 데이터스토어와 가상 머신을 직접 백업할 수 있습니다.

이 가이드의 목적

이 가이드에서는 SCV를 사용하여 Amazon EVS용 FSx for ONTAP 데이터스토어를 보호하는 방법을 안내합니다. VM 및 데이터베이스 보호 시나리오와 복원 방법도 함께 제공됩니다.

대상

이 튜토리얼은 VMware vSphere, Amazon EVS, AWS 콘솔, FSx for ONTAP 에 익숙한 클라우드 아키텍트와 클라우드 관리자를 대상으로 합니다.

배포 및 구성을 위한 고급 단계

다음은 Amazon FSx for NetApp ONTAP에서 VM 및 데이터 저장소를 보호하기 위해 SnapCenter Plug-in for VMware vSphere를 배포하고 구성하는 주요 단계입니다.

1. SCV Open Virtual Appliance(OVA)를 다운로드합니다.
2. vSphere Client 자격 증명을 사용하여 Amazon EVS에 로그인합니다.
3. VMware 배포 마법사를 시작하려면 Open Virtualization Format(OVF) 템플릿을 배포하십시오.
4. 플러그인에 액세스하려면 메뉴에서 SnapCenter Plug-in for VMware를 선택하십시오.
5. 스토리지를 추가합니다.
6. 백업 정책을 생성합니다.
7. 리소스 그룹을 생성합니다.
8. 리소스 그룹을 백업합니다.
9. 전체 가상 머신 또는 특정 가상 디스크나 게스트 파일을 복원합니다.

VMware용 **SnapCenter** 플러그인 설치 절차

이 섹션에서는 VMware용 SnapCenter Plug-in 설정 단계를 설명합니다.

필수 조건

시작하기 전에 다음 사전 요구 사항이 필요합니다.

1. OVA를 배포하는 동안 vCenter 서버를 등록하려면 vCenter의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 지정합니다.
2. vCenter 자격 증명에는 필요한 최소 권한을 가진 계정을 사용하십시오.
3. vCenter Server 액세스를 위한 방화벽 포트를 엽니다.
4. FSx for ONTAP이 실행 중인 Amazon VPC의 보안 그룹을 업데이트하여 SCV가 FSx for ONTAP에 액세스할 수 있도록 합니다.



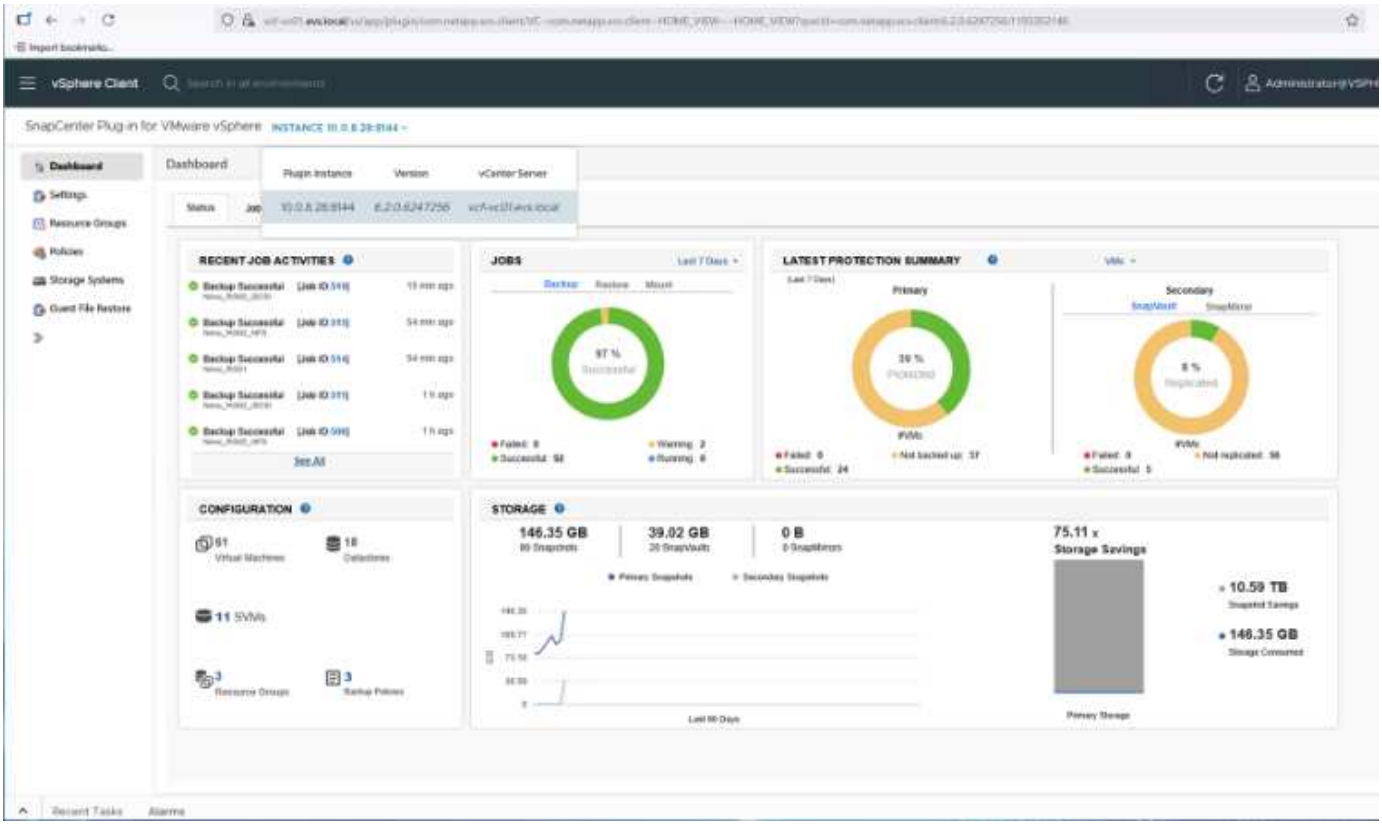
SCV는 무료로 이용할 수 있습니다.

VMware용 **SnapCenter** 플러그인 설정

가상 머신과 이를 호스팅하는 NFS/iSCSI 기반 데이터스토어를 보호하려면 SCV를 배포해야 합니다. 간단한 OVF 가져오기입니다.

배포 단계는 다음과 같습니다.

1. "NetApp 지원 사이트"에서 OVA를 다운로드합니다.
2. Amazon EVS vCenter에 로그인합니다.
3. vCenter 내에서 데이터 센터, 폴더, 클러스터 또는 호스트와 같은 인벤토리 개체를 마우스 오른쪽 버튼으로 클릭하고 "Deploy OVF template"을 선택합니다.
4. 스토리지, 세그먼트 등 올바른 설정을 선택하고 vCenter 및 자격 증명을 업데이트하기 위한 템플릿을 사용자 지정하고, SCV 자격 증명 및 IP 세부 정보를 생성합니다. 검토 후 "완료"를 선택합니다.
5. OVF 가져오기 및 배포 작업이 완료될 때까지 기다립니다.
6. SCV가 성공적으로 배포되면 vCenter 내에 등록됩니다.
7. 플러그인에 액세스하려면 vCenter 웹 클라이언트 페이지의 왼쪽 사이드바로 이동하여 "SnapCenter Plug-in for VMware"를 선택하십시오.



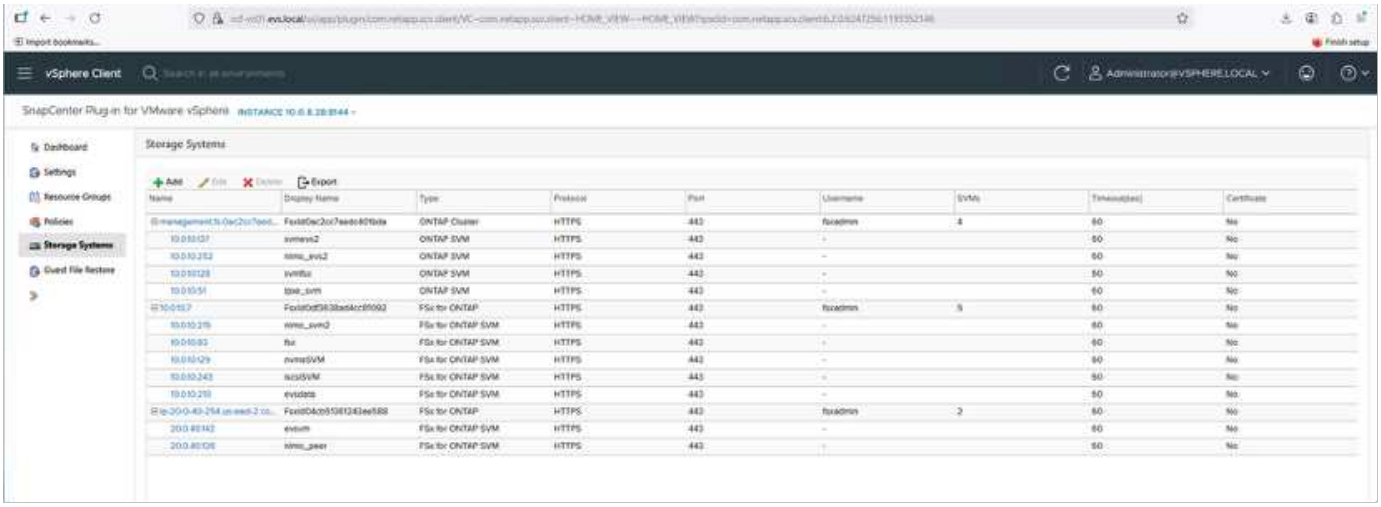
VMware용 **SnapCenter Plug-in** 구성 절차

이 섹션에서는 VMware용 SnapCenter 플러그인을 구성하는 단계를 설명합니다. 다음 섹션에서는 스토리지 추가, 백업 정책 생성 및 리소스 그룹 생성 방법을 자세히 설명합니다.

스토리지 시스템 추가

SVC를 사용하여 워크로드를 보호하는 다음 단계는 "스토리지 시스템"를 추가하는 것입니다. 스토리지를 추가하면 SCV가 vCenter 내에서 백업 및 복원 작업을 감지하고 관리할 수 있습니다. VM 백업 및 복원을 활성화하려면 FSx for NetApp ONTAP 관리 엔드포인트 또는 스토리지 가상 머신(SVM) 관리 엔드포인트 IP를 스토리지 시스템으로 포함하십시오.

1. EVS vCenter의 왼쪽 탐색 메뉴에서 "SnapCenter Plug-in for VMware"를 선택합니다.
2. "스토리지 시스템"을 선택하세요.
3. "추가"를 선택하여 FSx for ONTAP 세부 정보를 추가합니다.
4. "Credentials as the Authentication" 방법을 사용하고 사용자 이름과 암호로 FSxadmin을 입력합니다. 그런 다음 "Add"를 선택하여 설정을 저장합니다.



파일 시스템이 추가되면 모든 SVM이 자동으로 추가됩니다.

SCV 버전이 6.2인 경우 "SCV 지원 페이지"로 이동하여 SCV 6.2P1 릴리스를 다운로드하십시오.

백업 정책을 생성합니다

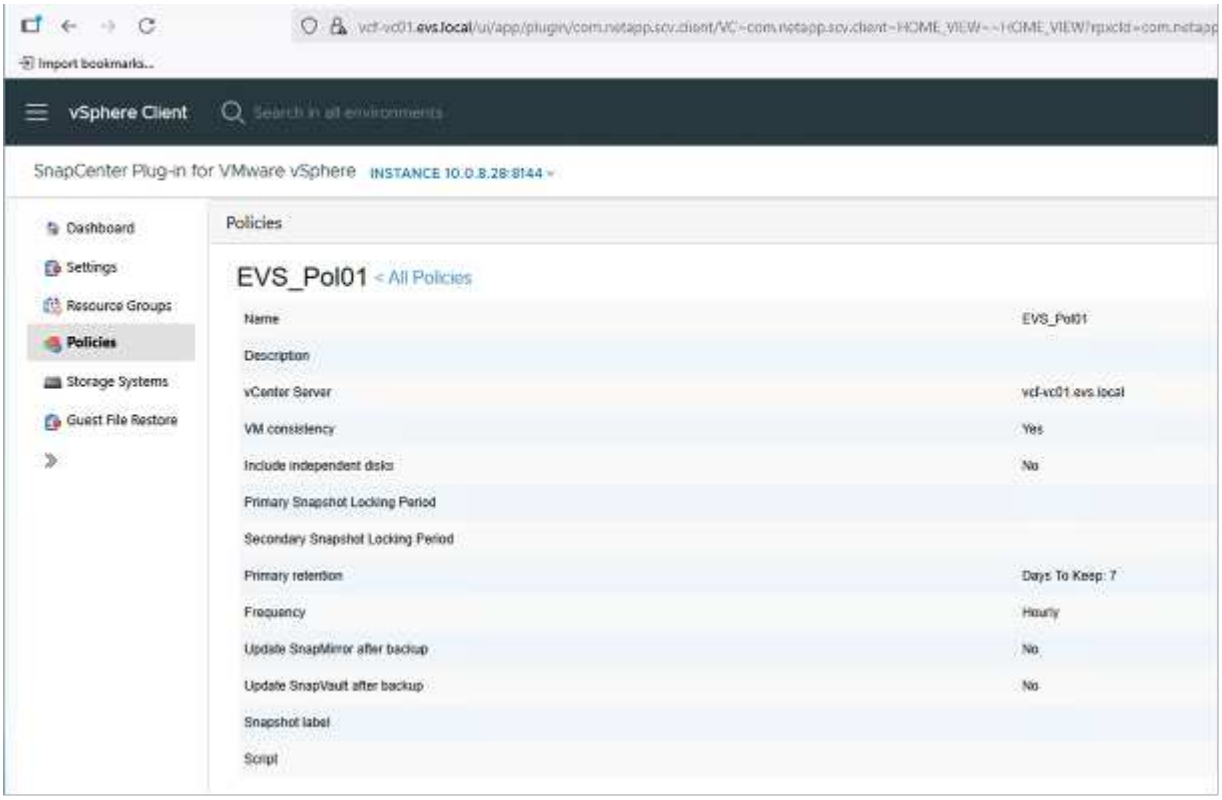
견고한 백업 전략은 백업 일정, 백업 대상 데이터, 백업 보존 기간과 같은 핵심 요소를 정의해야 합니다. 스냅샷 복사본은 전체 데이터 저장소를 보호하기 위해 시간별 또는 일별로 예약할 수 있습니다. 이러한 방식으로 백업을 예약하면 데이터 저장소를 보호할 뿐만 아니라 해당 데이터 저장소에 포함된 VM 및 VMDK에 대한 백업 및 복원 작업도 지원합니다.

가상 머신 및 데이터스토어 백업을 시작하기 전에 "백업 정책"과 리소스 그룹을 생성해야 합니다. 백업 정책은 백업 일정 및 보존 설정과 같은 매개변수를 지정합니다.

다음은 백업 정책을 생성하는 단계입니다.

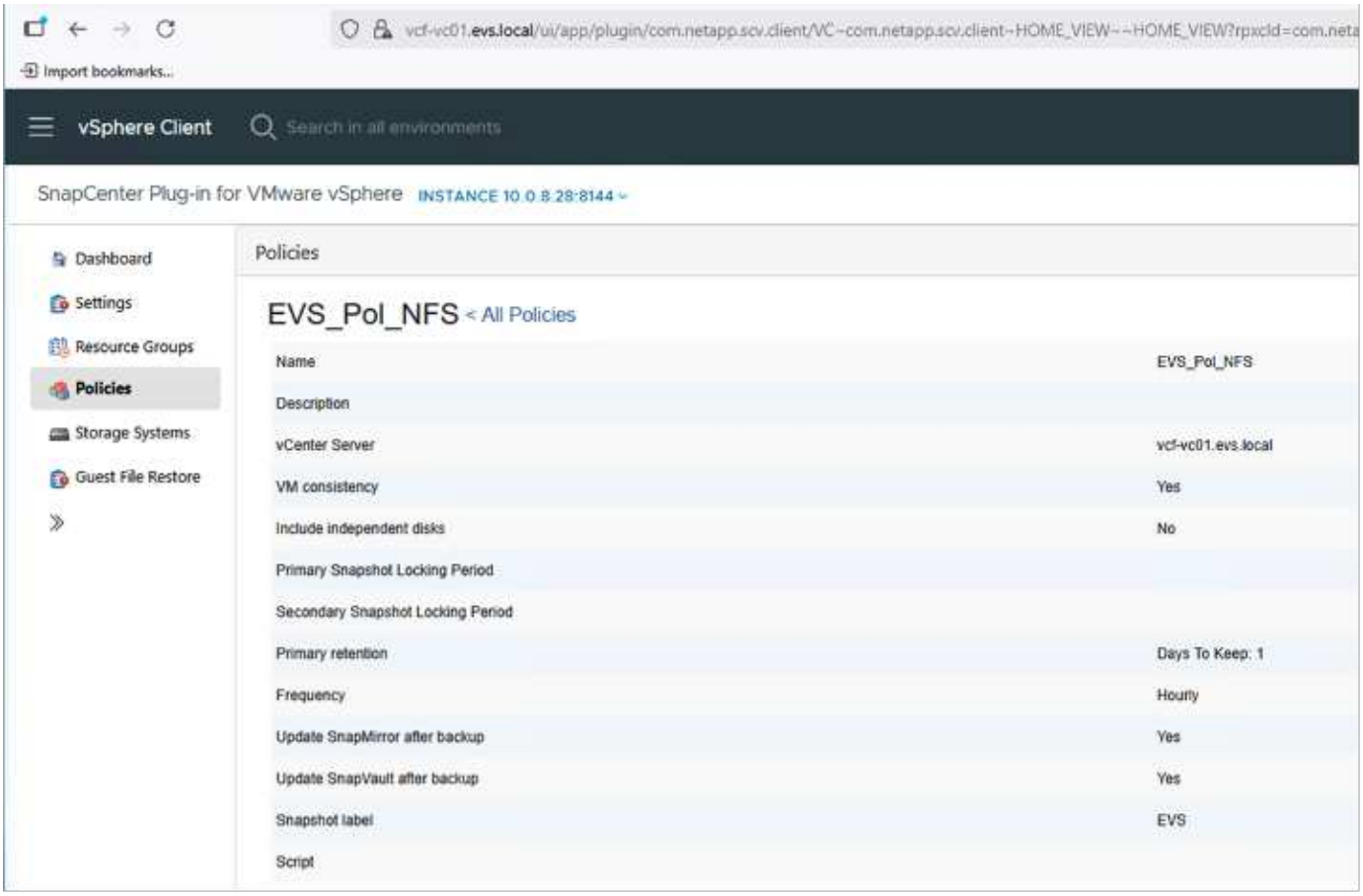
1. SCV의 왼쪽 탐색 메뉴로 이동하여 "정책"을 선택합니다.
2. 정책 페이지에서 "Create"를 선택하여 마법사를 시작하세요.
3. "New Backup Policy page"에서 정책 이름을 입력합니다.
4. 보존 기간, 백업 빈도 및 복제 설정을 지정하십시오.
5. Snapshot 잠금을 활성화하려면 "Locking Period" 확인란을 선택하십시오. 기본 및 보조 Snapshot 잠금 기간을 일/월/년으로 선택할 수 있습니다.

SnapMirror 정책에 정의된 보존 기간과 관계없이, 보조 스냅샷 복사본은 지정된 보조 스냅샷 잠금 기간이 만료될 때까지 그대로 유지됩니다.



VM 일관성 백업을 활성화하려면 VMware Tools가 설치되어 실행 중이어야 합니다. VM 일관성 확인란을 선택하면 VM이 먼저 정지된 다음 VMware가 VM 일관성 스냅샷(메모리 제외)을 수행하고, SnapCenter Plug-in for VMware vSphere가 백업 작업을 수행한 후 VM 작업이 재개됩니다.

스냅샷 복사본을 보조 미러 또는 볼트 파일 시스템으로 복제하려면 관계를 미리 구성해야 합니다.



정책이 생성되면 다음 단계는 백업해야 할 적절한 NFS 또는 iSCSI 데이터 저장소와 VM을 정의하는 리소스 그룹을 생성하는 것입니다.

리소스 그룹을 생성합니다

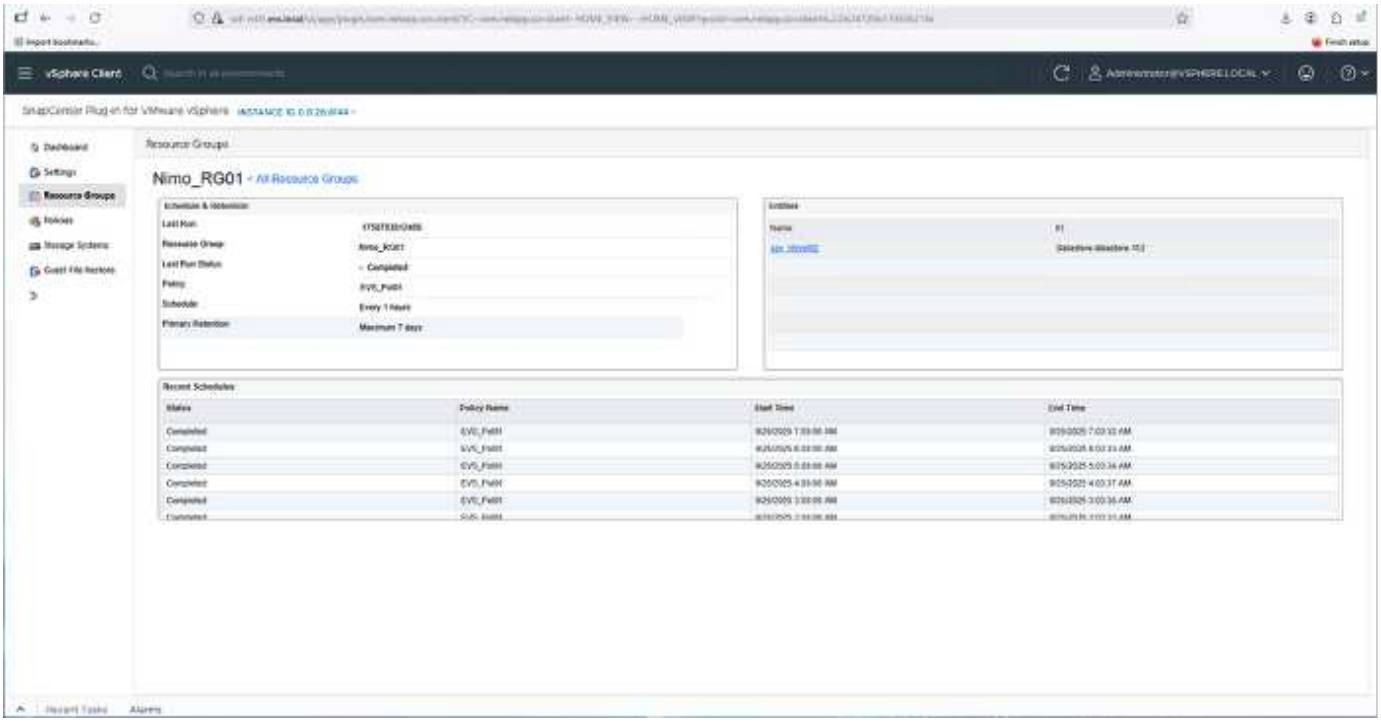
리소스 그룹은 보호가 필요한 VM과 데이터스토어를 담는 컨테이너 역할을 합니다. 리소스는 언제든지 리소스 그룹에 추가하거나 제거할 수 있으므로 백업 구성을 유연하게 관리할 수 있습니다.

다음 단계를 사용하여 "리소스 그룹"을(를) 생성할 수 있습니다.

1. SCV의 왼쪽 탐색 창으로 이동하여 "리소스 그룹"을 선택합니다.
2. 리소스 그룹 페이지에서 "만들기"를 선택하여 리소스 그룹 생성 마법사를 시작합니다.

> ⓘ 리소스 그룹을 생성하는 또 다른 방법은 개별 VM 또는 데이터 저장소를 선택하고 해당 리소스만 포함하는 리소스 그룹을 생성하는 것입니다.

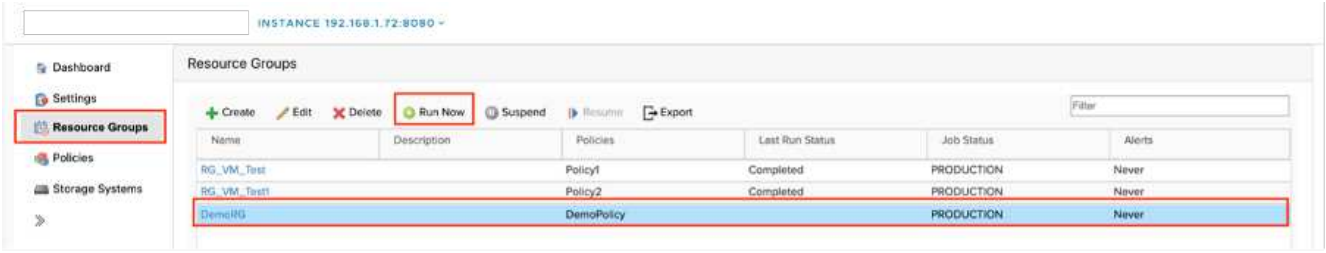
3. "Resources" 페이지에서 범위(VM 또는 데이터 저장소)와 데이터 센터를 선택합니다.
4. "디스크 스패닝" 페이지에서 "여러 데이터스토어에 걸쳐 여러 VMDK를 사용하는 가상 머신" 옵션을 선택합니다.
5. 다음으로 백업 정책을 연결합니다. 기존 정책을 선택하거나 새 백업 정책을 생성합니다.
6. "Schedules" 페이지에서 선택한 각 정책에 대한 백업 일정을 구성합니다.
7. 필요한 항목을 선택했으면 "완료"를 선택하세요. 그러면 새 리소스 그룹이 생성되어 리소스 그룹 목록에 추가됩니다.



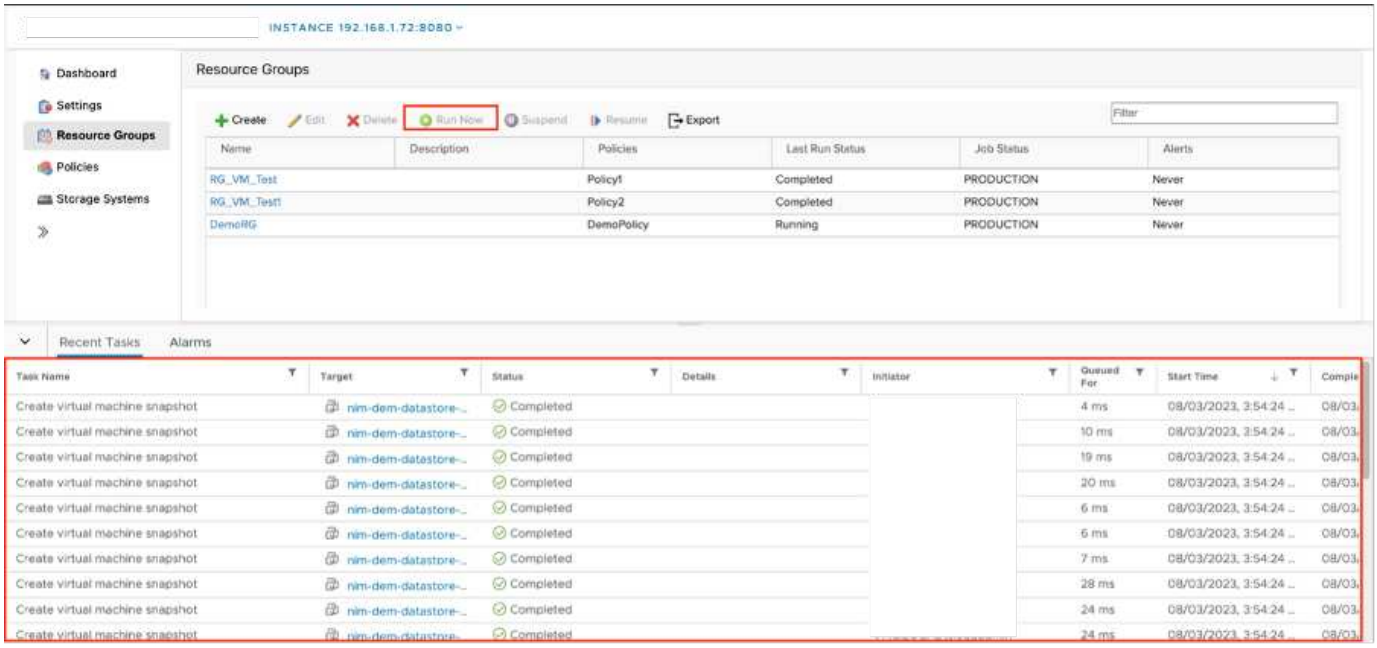
리소스 그룹 백업

백업 작업은 리소스 그룹 내에 정의된 모든 리소스에 대해 실행됩니다. 리소스 그룹에 정책이 연결되어 있고 일정이 구성되어 있는 경우 백업은 해당 일정에 따라 자동으로 수행됩니다.

1. vCenter 웹 클라이언트 페이지의 왼쪽 탐색 창에서 "SnapCenter Plug-in for VMware"를 선택한 다음 "Resource Groups"를 선택합니다.
2. 리소스 그룹 페이지에서 지정된 리소스 그룹을 찾고 "지금 실행"을 선택하여 수동 백업을 시작하십시오.



3. 리소스 그룹에 여러 정책이 구성되어 있는 경우 "지금 백업" 대화 상자에서 백업 작업에 사용할 정책을 선택하십시오.
4. 백업을 시작하려면 "OK"를 선택하십시오.

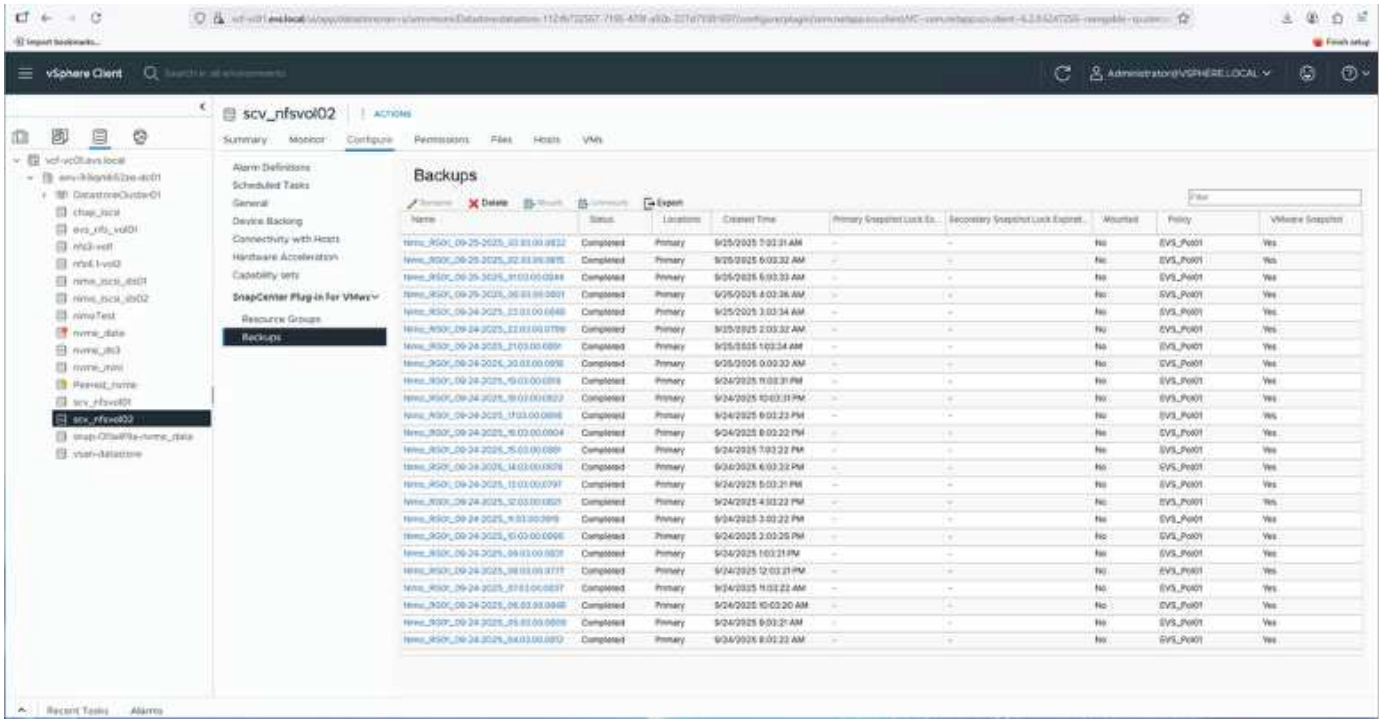


창 하단의 "Recent Tasks"를 선택하거나 대시보드에서 "Job Monitor"를 선택하여 작업 진행 상황을 모니터링합니다.

ⓘ 백업 정책 생성, 리소스 그룹 구성 및 백업 작업 수행 프로세스는 NFS 및 iSCSI를 포함한 다양한 스토리지 프로토콜에서 일관적입니다.

ⓘ 백업은 정책에 정의된 일정에 따라 수행됩니다.

백업이 완료되면 드롭다운 목록에서 "SnapCenter Plug-in for VMware vSphere"를 선택한 다음 "복원"을 선택하여 데이터스토어 수준 또는 개별 VM에 대한 백업을 볼 수 있습니다.



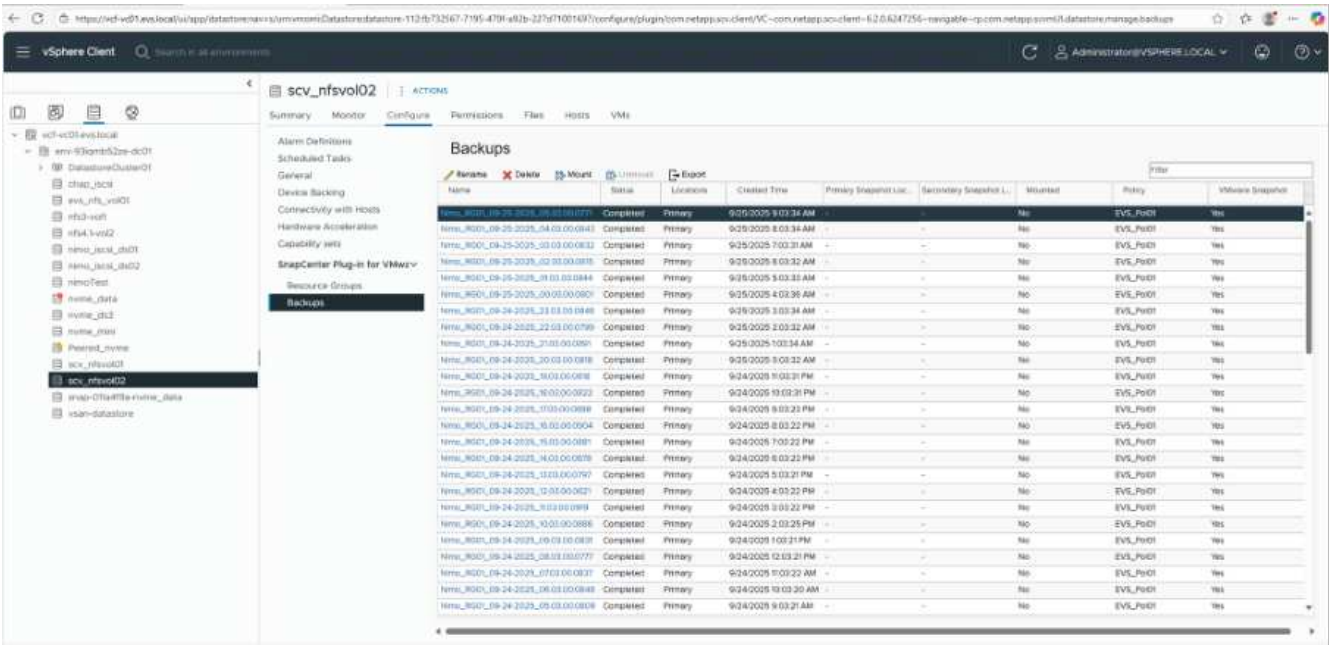
SnapCenter Plug-in for VMware vSphere로 보호되는 **VM**의 복원 절차

이 섹션에서는 백업에서 VM을 복원하는 단계를 설명합니다. SCV를 사용하면 vCenter 내에서 VM을 복원할 수 있으며, 이를 통해 VM을 원래 ESXi 호스트의 원래 데이터스토어로 복구(기존 콘텐츠 덮어쓰기)하거나, 삭제되거나 이름이 변경된 VM을 백업 복사본에서 복원하거나, 원래 ESXi 호스트의 다른 데이터스토어로 복원하거나, 동일한 vCenter에서 관리하는 다른 ESXi 호스트의 원래 데이터스토어로 복원하거나, 동일한 vCenter 환경 내의 다른 ESXi 호스트의 다른 데이터스토어로 복원할 수 있습니다.

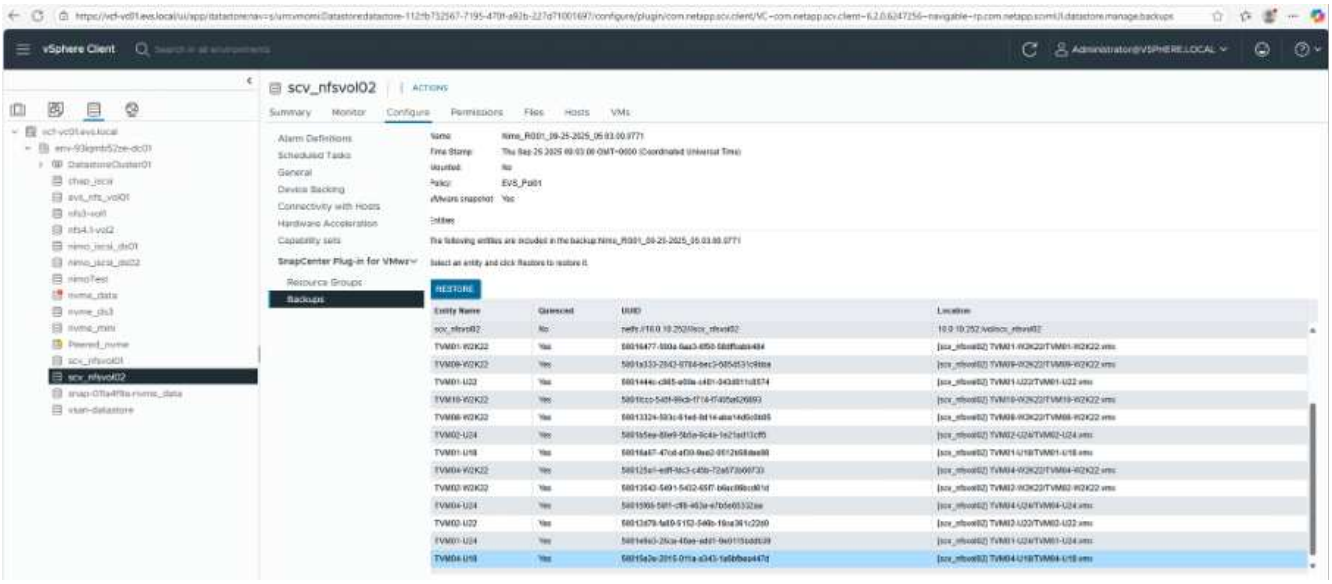
복원 작업 수행 단계

복원 작업을 수행하려면 다음 단계를 수행합니다.

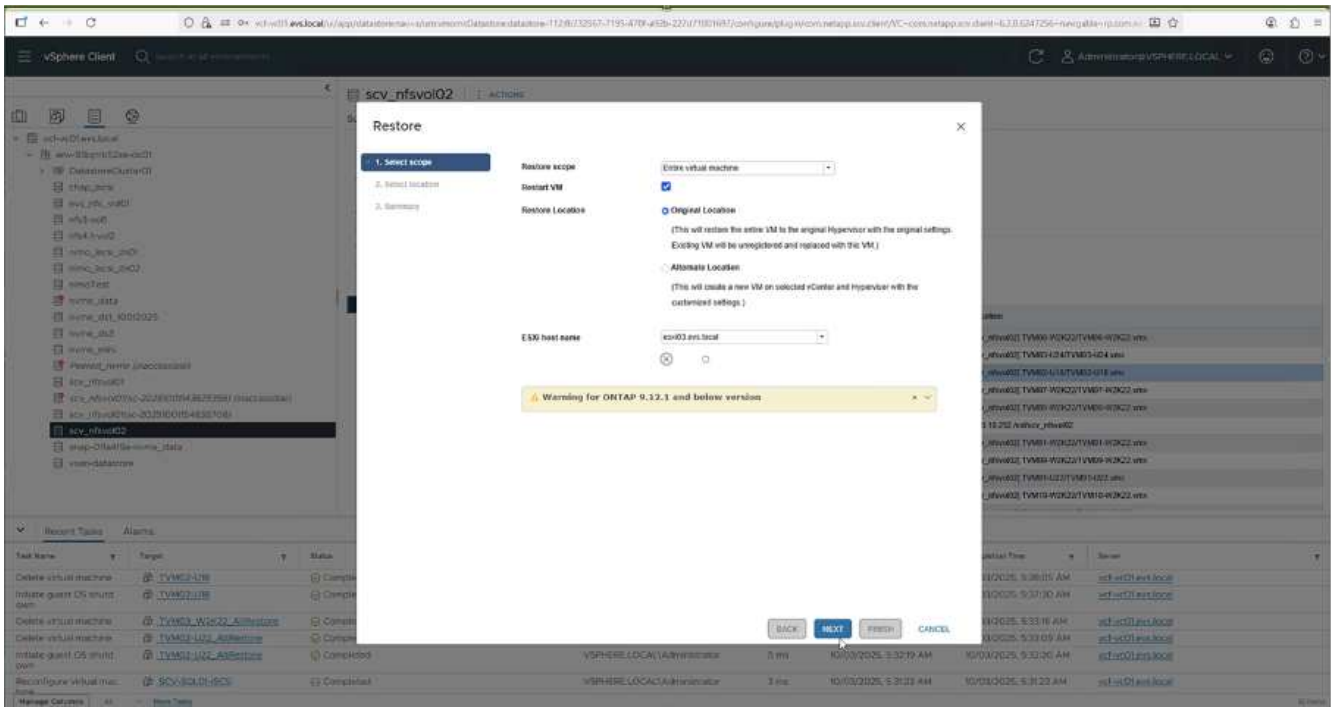
1. EVS vSphere 웹 클라이언트 GUI에서 인벤토리 › 데이터스토어로 이동하여 원하는 데이터스토어를 선택합니다. 그런 다음 "SnapCenter Plug-in for VMware vSphere" 섹션 아래의 구성 › 백업으로 이동합니다.



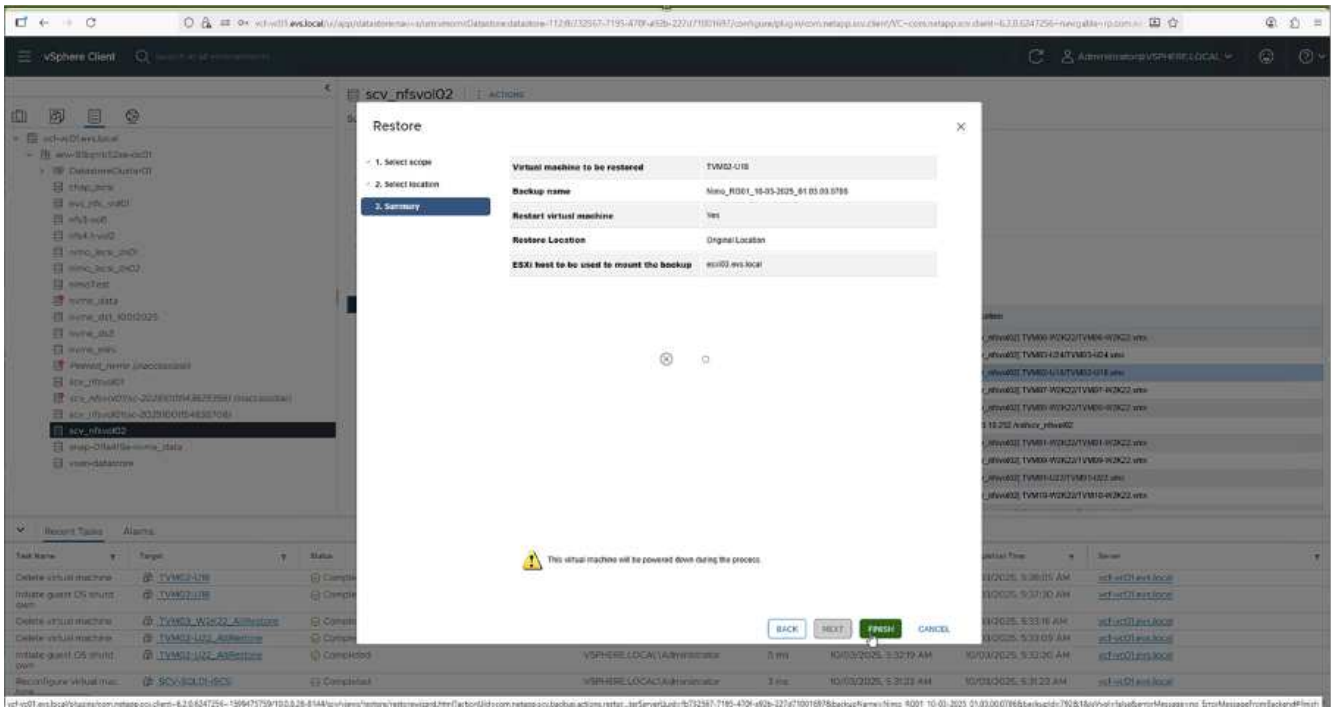
2. 백업을 두 번 클릭하면 해당 백업에 포함된 모든 VM이 표시됩니다. 목록에서 복원할 VM을 찾아 "Restore"를 선택합니다.



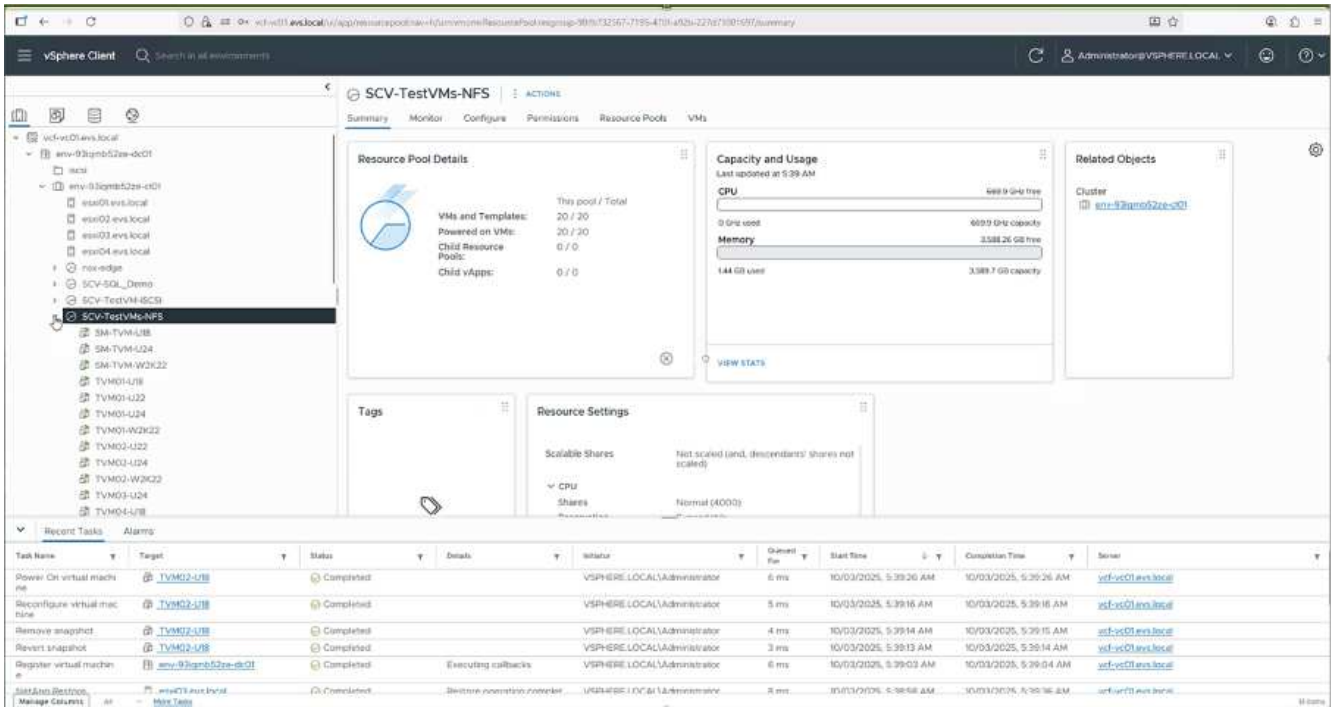
3. "범위 선택 페이지"에서 "복원 범위" 필드의 "전체 가상 머신"을 선택한 다음 "복원 위치"를 선택하고 백업을 마운트할 대상 ESXi 정보를 입력합니다.
4. 복원 작업 후 VM의 전원을 켜야 하는 경우 "VM 다시 시작" 확인란을 활성화합니다.
5. "Select Location page"에서 기본 위치를 선택하십시오.



6. "Summary" 페이지를 검토한 후 "Finish"를 선택하십시오.



7. 화면 하단의 "Recent Tasks"를 선택하여 작업 진행 상황을 모니터링합니다.



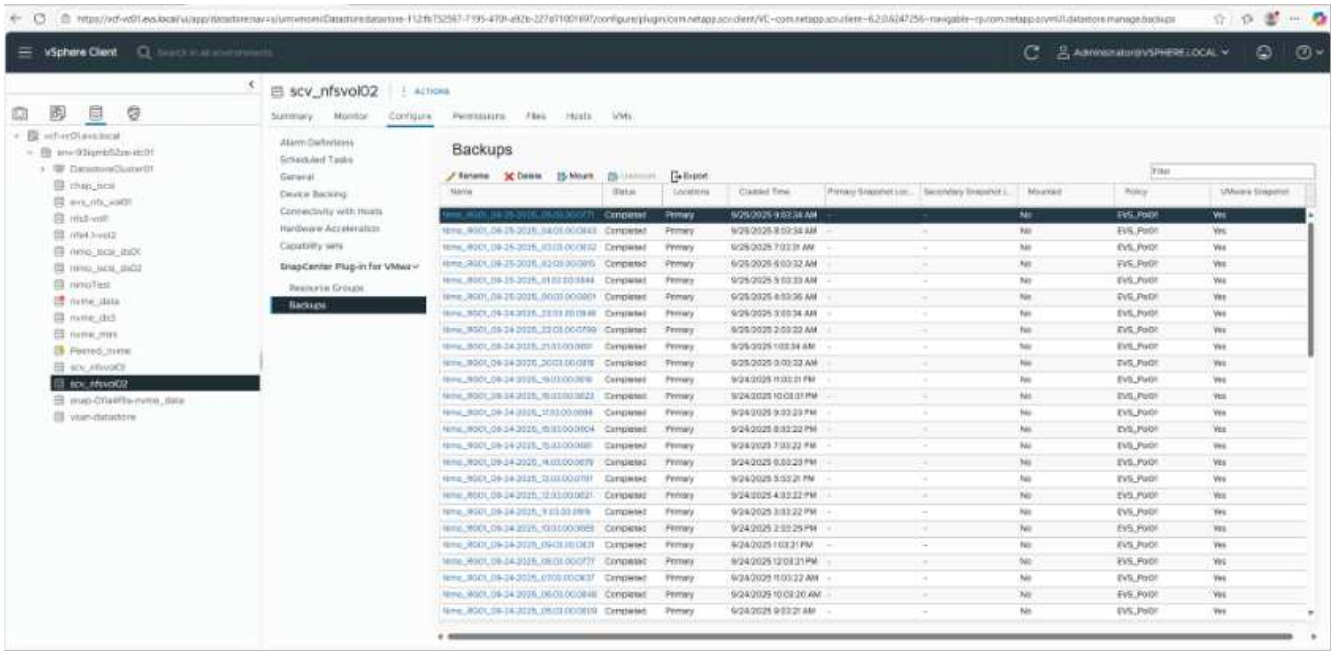
VM이 복원되더라도 이전 리소스 그룹에 자동으로 추가되지는 않습니다. 해당 VM을 보호하려면 수동으로 적절한 리소스 그룹에 추가해야 합니다.

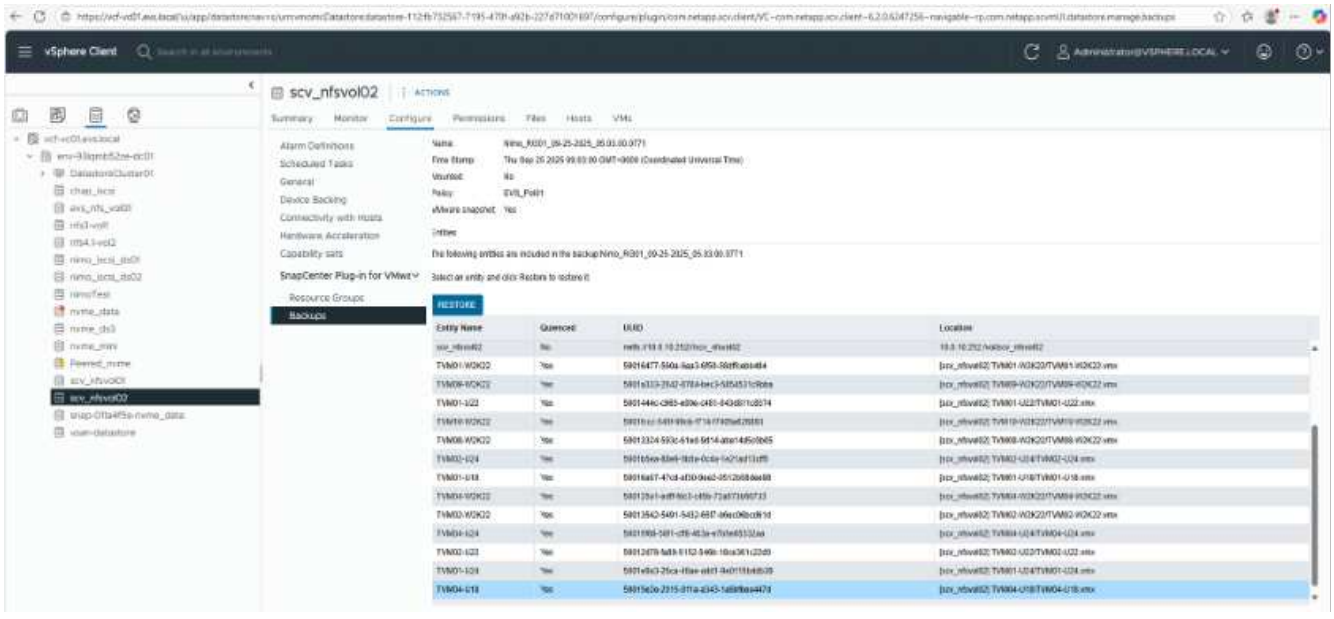
복원 작업은 개별 VM 수준에서도 트리거할 수 있습니다.

삭제된 VM을 복원하는 것은 SCV를 사용하면 간단한 프로세스입니다.

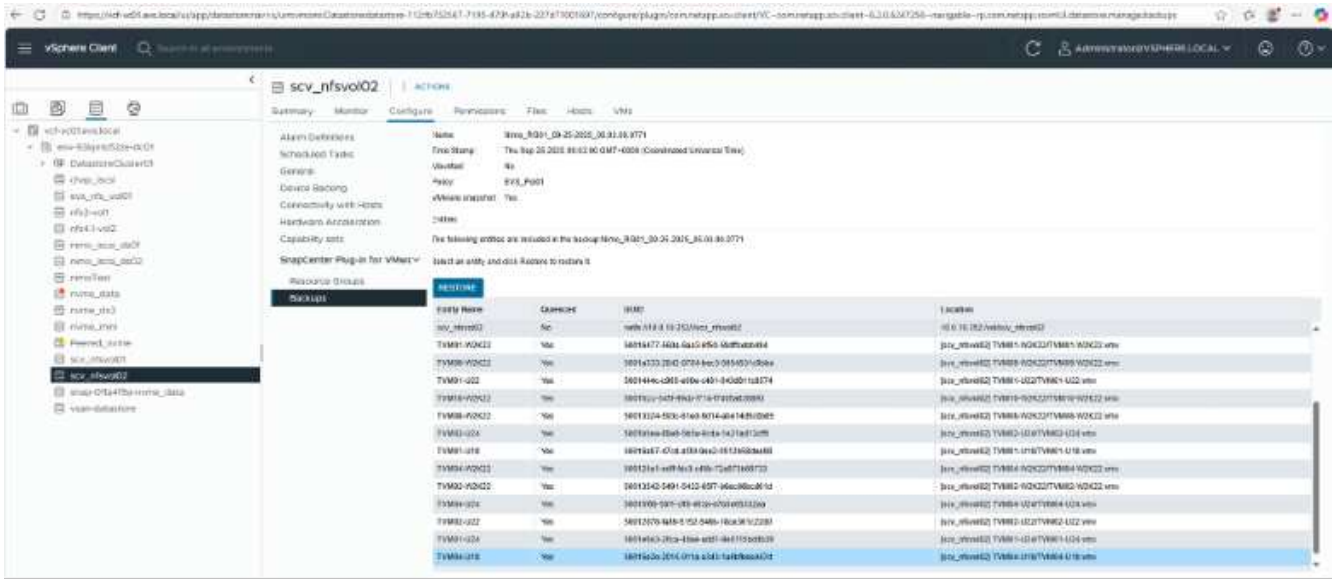
삭제된 VM의 복원 작업은 데이터 저장소 수준에서 수행할 수 있습니다.

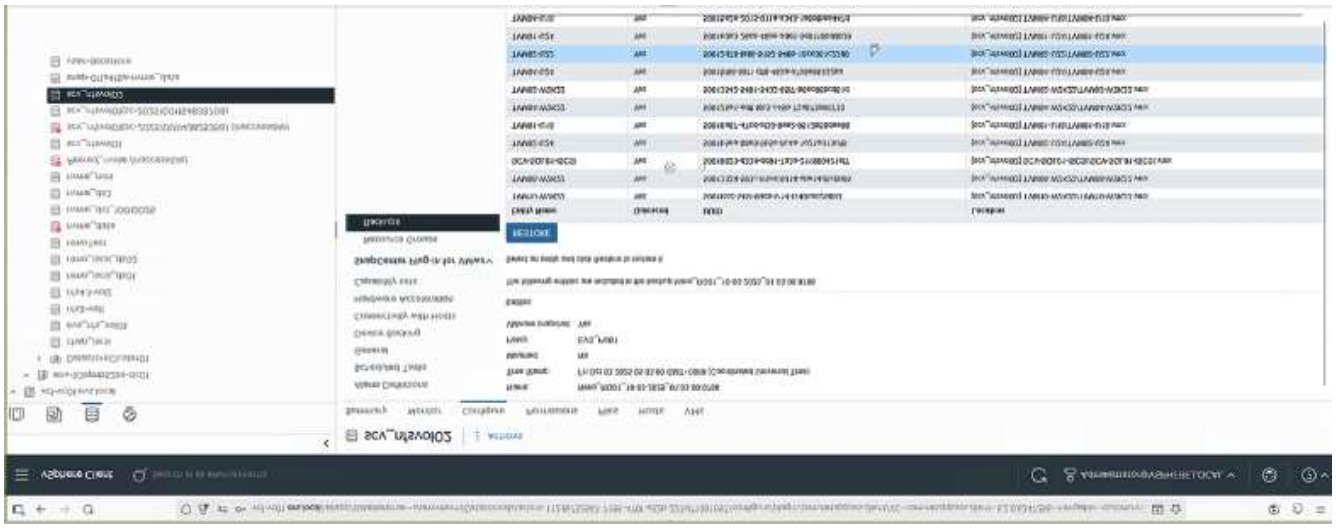
1. 해당 데이터스토어로 이동하여 Configure > Backups를 선택합니다. 거기서 삭제된 VM을 선택하고 "Restore"를 선택합니다.

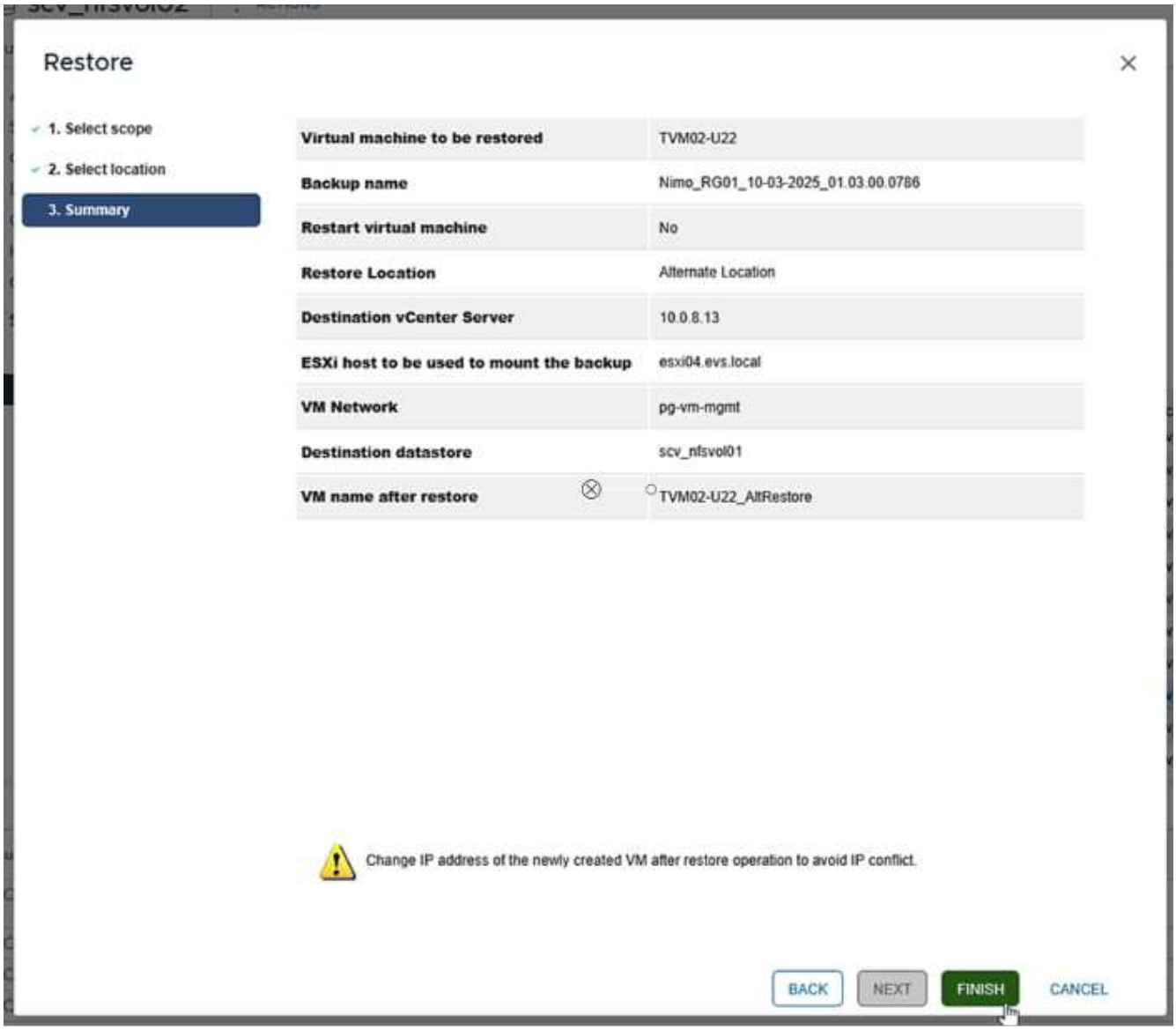


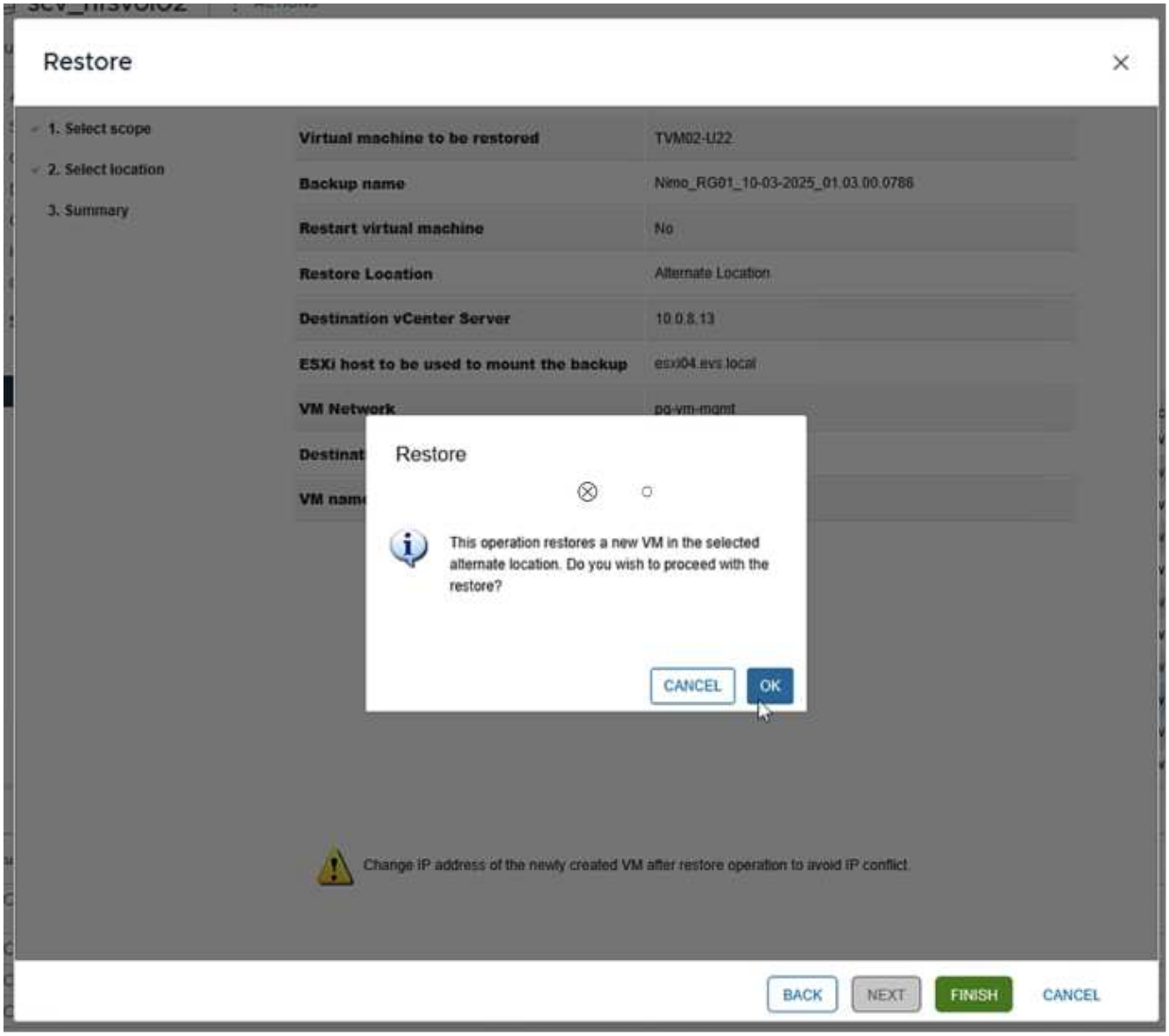


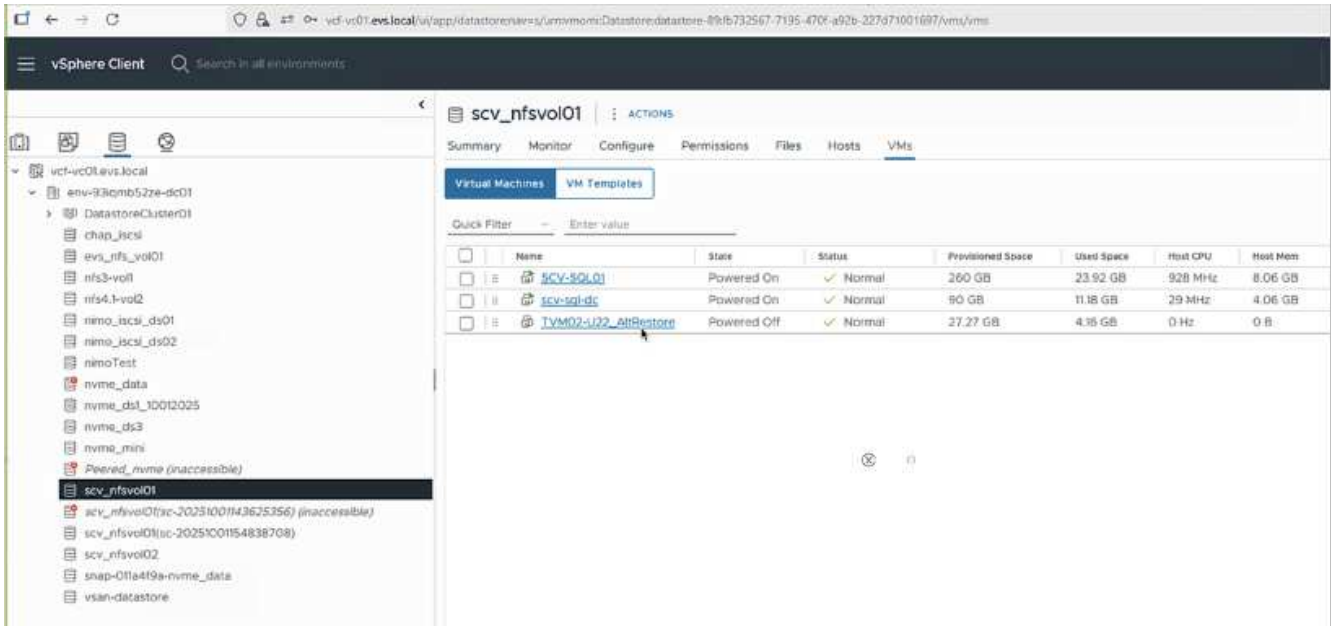
2. 다음 스크린샷 흐름은 VM을 대체 ESXi 호스트 및 다른 데이터 저장소로 복원하는 과정을 다룹니다.


vSphere Client
scv_nfsvol02
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
Alarm Definitions
Scheduled Tasks
General
Device Backing
Connectivity with Hosts
Hardware Acceleration
Capability sets
SnapCenter Plug-in for VMware
Resource Groups
Backups
RESTORE




Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Destination datastore
scv_nfsvol01
VM name after restore
TVM02-U22_AltRestore
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL

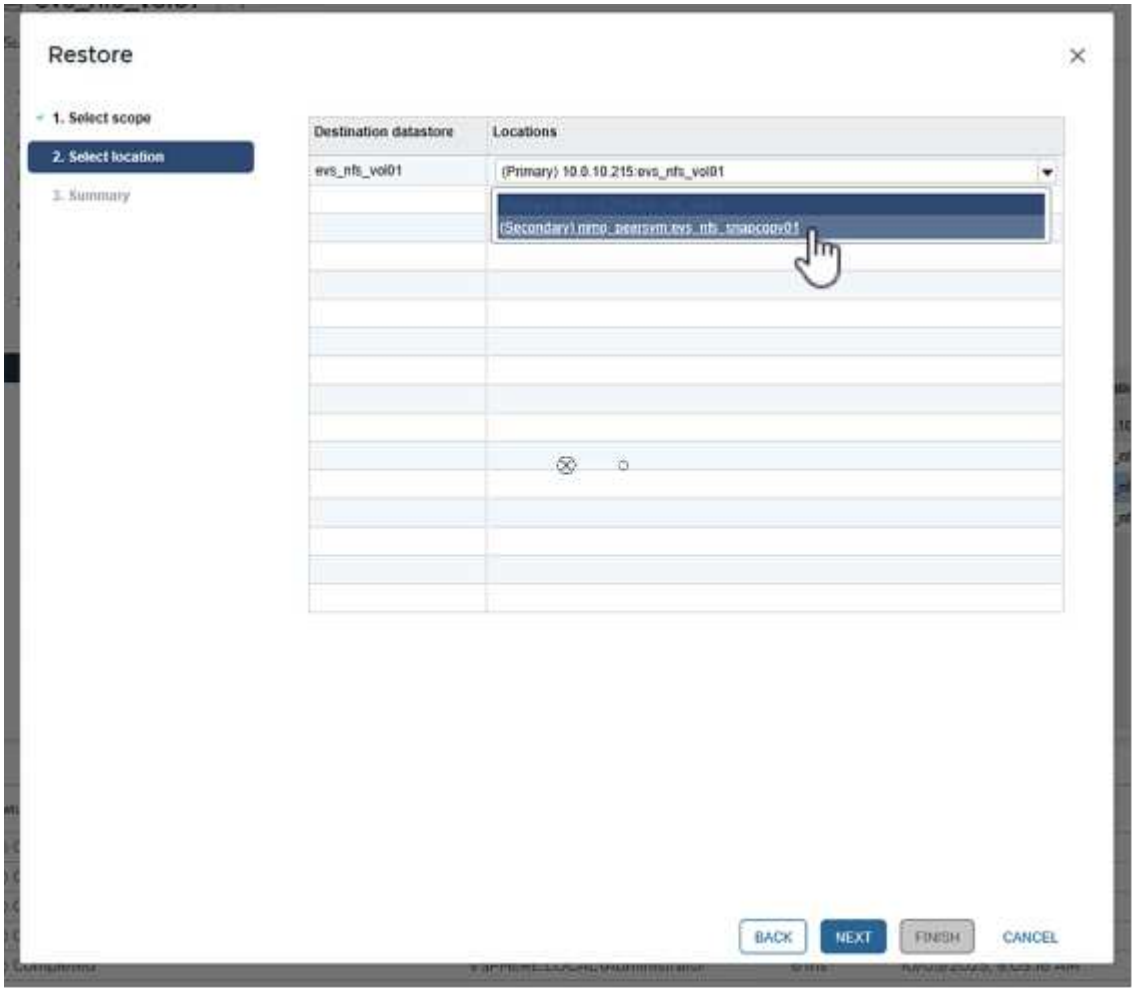

Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Restore
This operation restores a new VM in the selected alternate location. Do you wish to proceed with the restore?
CANCEL
OK
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL


vSphere Client
scv_nfsvol01
ACTIONS
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
Virtual Machines
VM Templates
Quick Filter
Enter value
Name
State
Status
Provisioned Space
Used Space
Host CPU
Host Mem
SCV-SQL01
Powered On
Normal
260 GB
23.92 GB
928 MHz
8.06 GB
scv-sql-dc
Powered On
Normal
90 GB
11.18 GB
29 MHz
4.06 GB
TVM02-U22_AltRestore
Powered Off
Normal
27.27 GB
4.16 GB
0 Hz
0 B
vcf-vc01.evs.local
env-93ojmb52ze-dc01
DatastoreCluster01
chap_iscsi
evs_nfs_vol01
nfs3-vol1
nfs4.1-vol2
nimo_iscsi_ds01
nimo_iscsi_ds02
nimoTest
nvme_data
nvme_ds1_10012025
nvme_ds3
nvme_mini
Peered_nvme (inaccessible)
scv_nfsvol01
scv_nfsvol01(sc-20251001143625356) (inaccessible)
scv_nfsvol01(sc-20251001154838708)
scv_nfsvol02
snap-011a4f9a-nvme_data
vsan-datastore

대상 데이터 저장소에는 충분한 여유 공간이 있어야 하며, "대체 위치로 복원" 필드에 지정된 vCenter는 DNS에서 확인 가능해야 합니다.

NFS 환경에서 복원 효율성을 높이려면 VMware vStorage API for Array Integration(VAAI)을 활성화하십시오.

복원은 SnapMirror 타겟과 같은 보조 위치에서도 수행할 수 있습니다.



+

VMware용 **SnapCenter Plug-in**으로 보호되는 게스트 파일 및 폴더 복원 절차

다음 섹션에서는 VMDK에서 게스트 파일 및 폴더를 복원하는 방법을 보여줍니다.

SnapCenter는 게스트 운영 체제가 Windows인 경우에만 VMDK에서 파일 및 폴더 복원을 지원합니다.

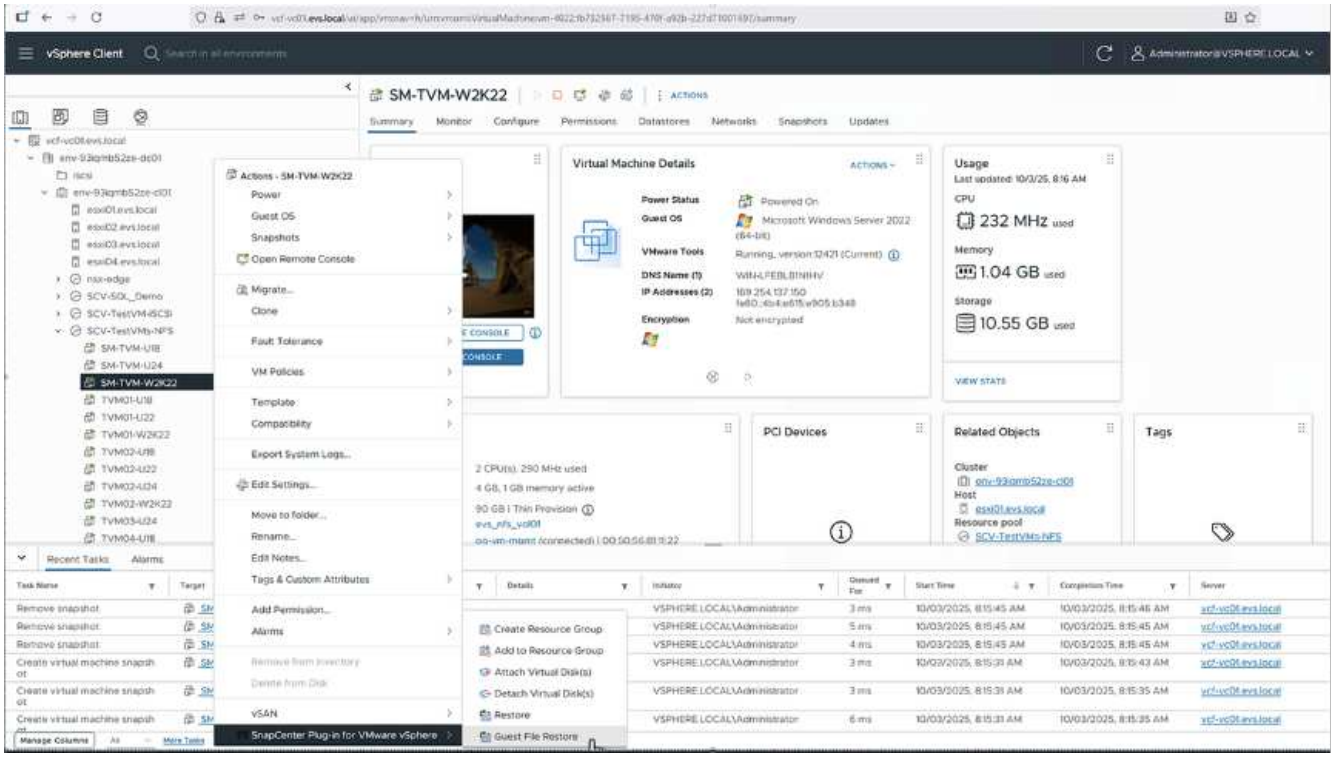
SnapCenter Plug-in for VMware vSphere를 사용한 게스트 파일 및 폴더 복원 시 고려 사항:

- VM에서 VMware Tools가 실행 중이어야 합니다.
- 연결된 VMDK는 기본적으로 24시간 동안 액세스할 수 있습니다.
- 가상 머신에서는 한 번에 하나의 복원 또는 연결 작업만 수행할 수 있습니다.

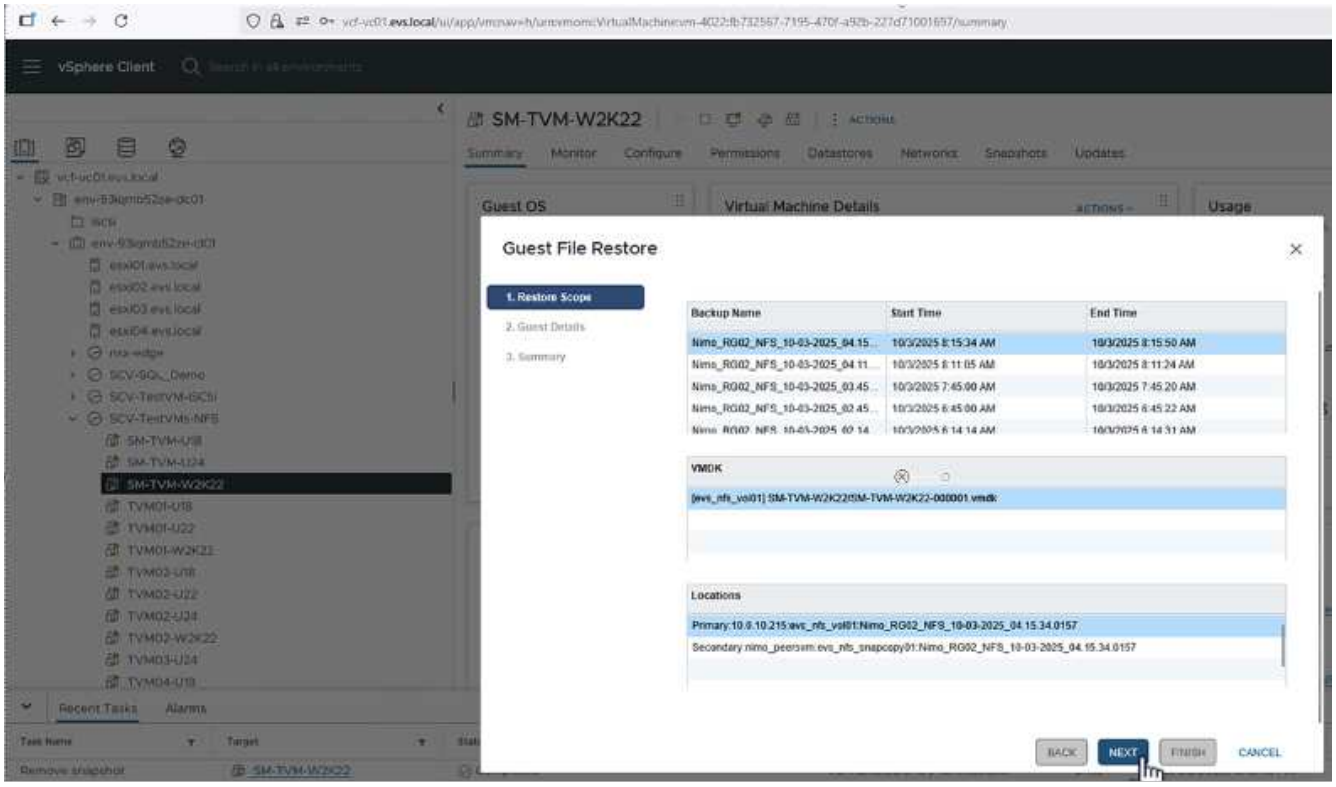
- 시스템 파일, 숨김 파일 및 암호화된 파일은 복원할 수 있지만 원래 속성은 유지되지 않습니다.
- 암호화된 파일을 암호화된 폴더에 복원하거나 시스템 파일을 덮어쓰지 마십시오.

게스트 파일 및 폴더 복원 단계:

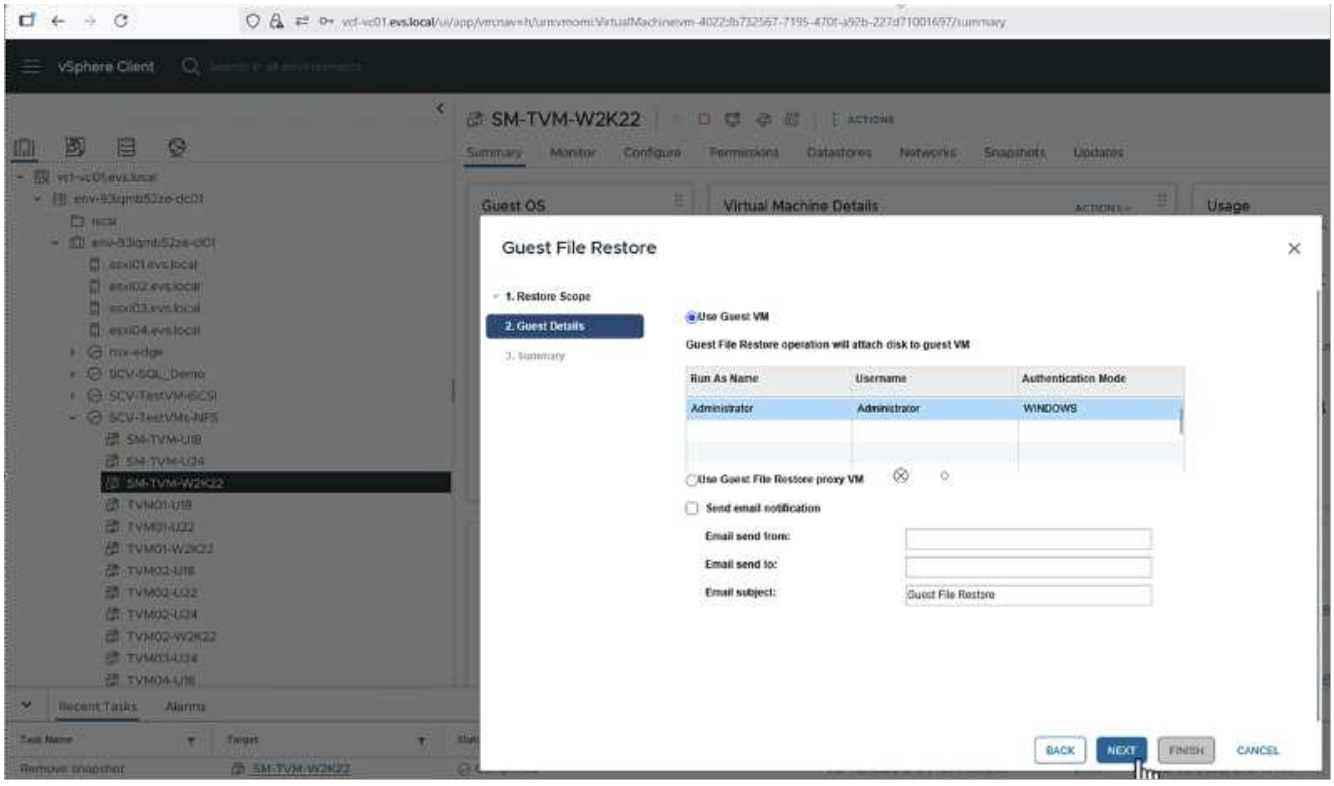
1. 대상 VM을 마우스 오른쪽 버튼으로 클릭하고 **NetApp SnapCenter** › 게스트 파일 복원을 선택합니다.



2. 필요한 VMDK가 포함된 백업을 선택합니다. VMDK와 해당 위치(운영 또는 2차)를 지정합니다.



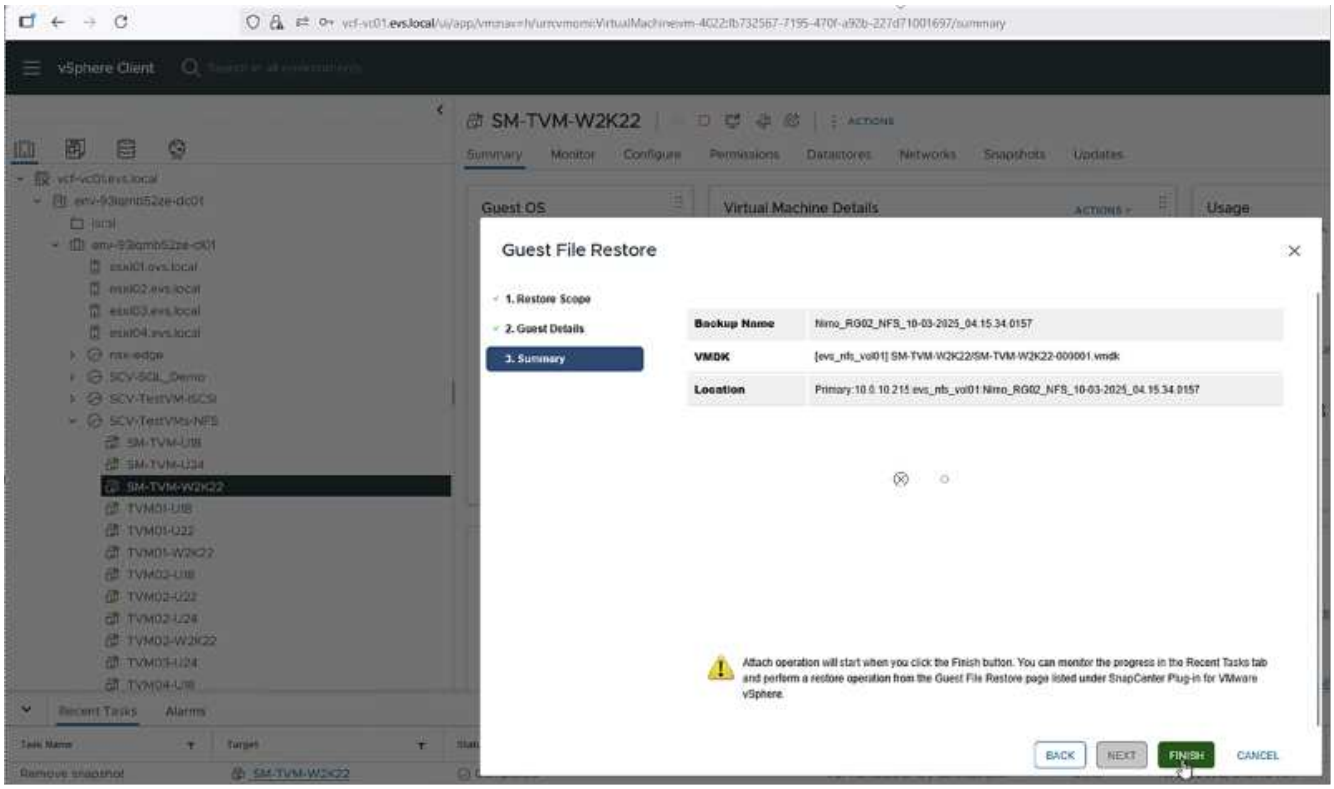
3. "디스크 연결 방법"을 선택하십시오.

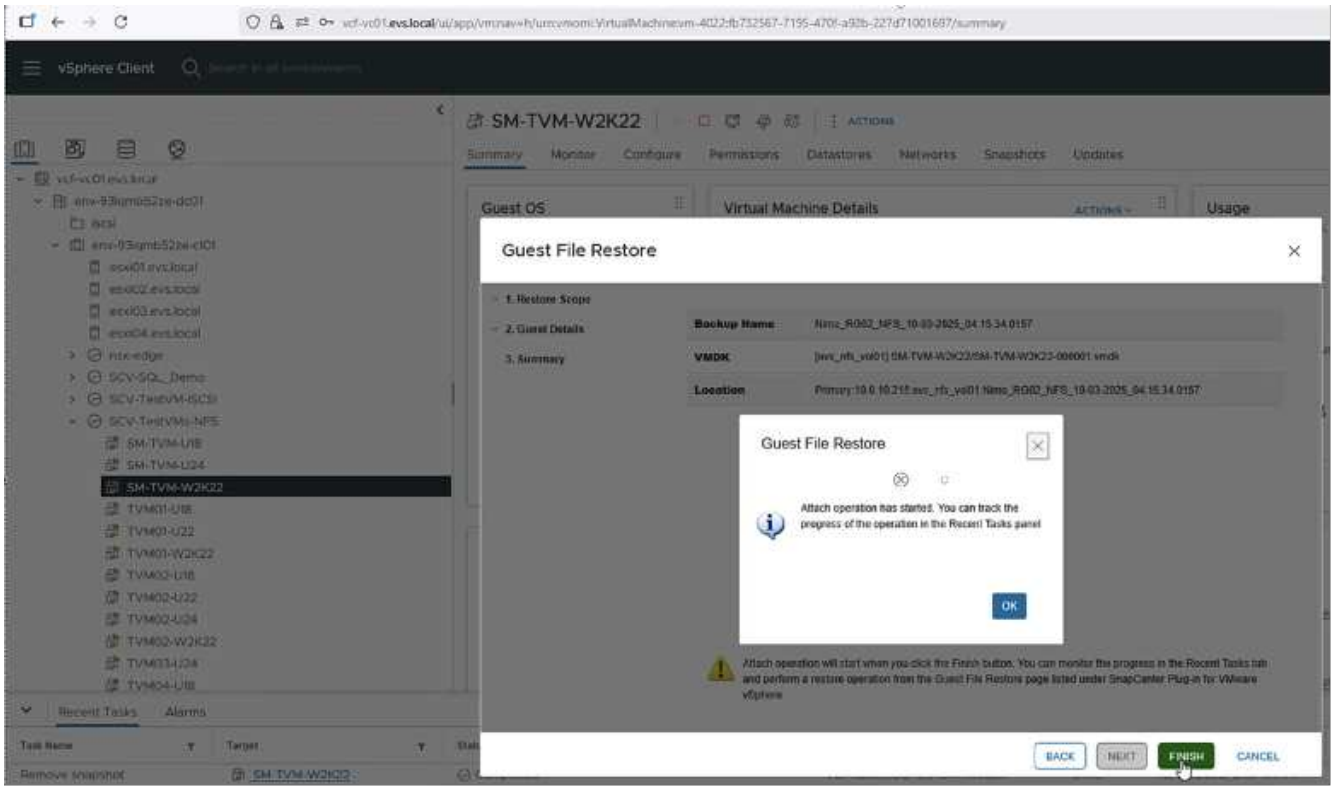


- 게스트 VM 옵션: 디스크를 원래 VM에 연결합니다(사전 구성된 자격 증명 필요). 이 옵션은 이 데모에서 사용됩니다.
- 프록시 VM 옵션: 지정된 프록시 VM에 디스크를 연결합니다(사전에 구성해야 함).

4. 파일을 찾아 복원하기 전에 연결 작업이 완료될 때까지 기다리십시오. 작업이 완료되면 SnapCenter에서 자동으로 게스트 파일 복원 세션을 생성합니다

.





5. 게스트 파일 복원 세션에서 VMDK를 찾아 필요한 파일이나 폴더를 선택한 다음 지정된 위치로 복원합니다.

SnapCenter for SQL(SCSQL)을 사용하는 **VMware VMDK**에서 실행되는 데이터베이스에 대한 보호 절차

다음 섹션에서는 SnapCenter for SQL(SCSQL)을 사용하여 VMware VMDK에서 실행되는 데이터베이스를 보호하는 방법을 보여줍니다.

SCSQL 설정

VMDK의 데이터베이스를 보호하기 위해 SCSQL을 사용하는 설정은 다음과 같습니다.

1. "설치 및 구성" SnapCenter 서버.
2. SnapCenter에 로그인합니다.
3. SnapCenter 환경을 구성합니다.
   - "추가 또는 할당" 스토리지 시스템 연결
   - "생성" 자격 증명.
4. VMware VMDK의 Microsoft SQL Server 데이터베이스:
   - "SCV 구축" (설정 섹션에서 이미 다뤘습니다).
   - SnapCenter에 플러그인을 등록합니다.
5. "SQL Server 호스트 및 플러그인 설치"추가:
   - "SQL 플러그인을 구성합니다".
   - "데이터베이스 및 로그에 대한 보호 계획 및 스케줄을 구성합니다".

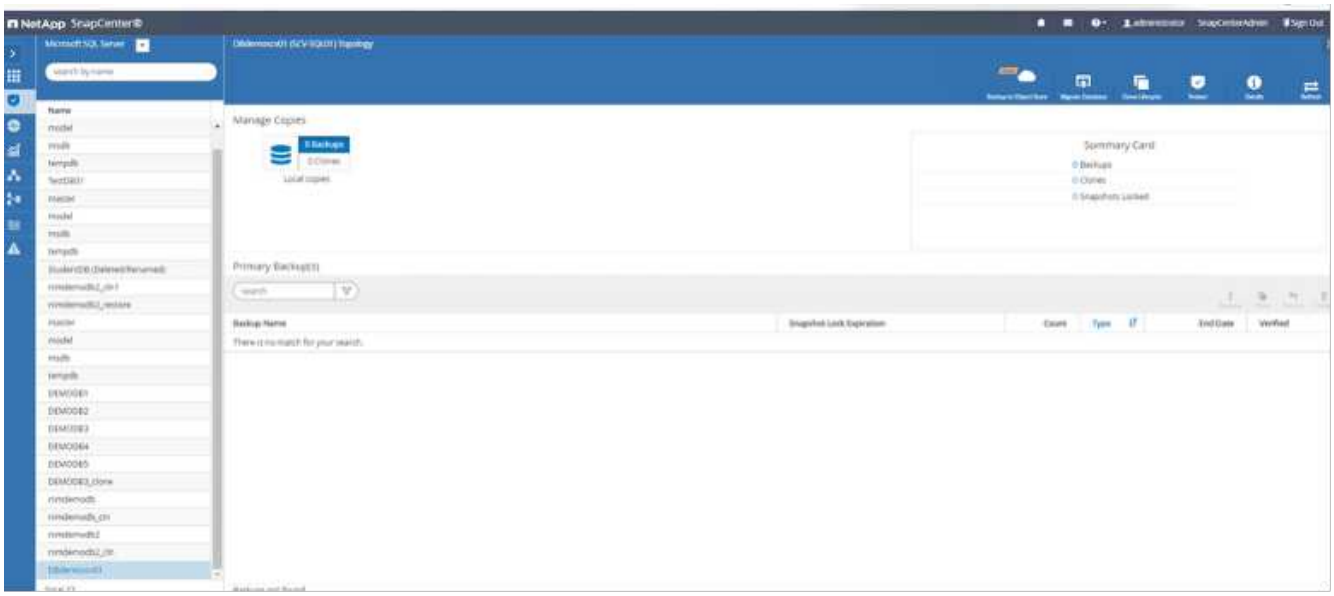


백업 정책 설정

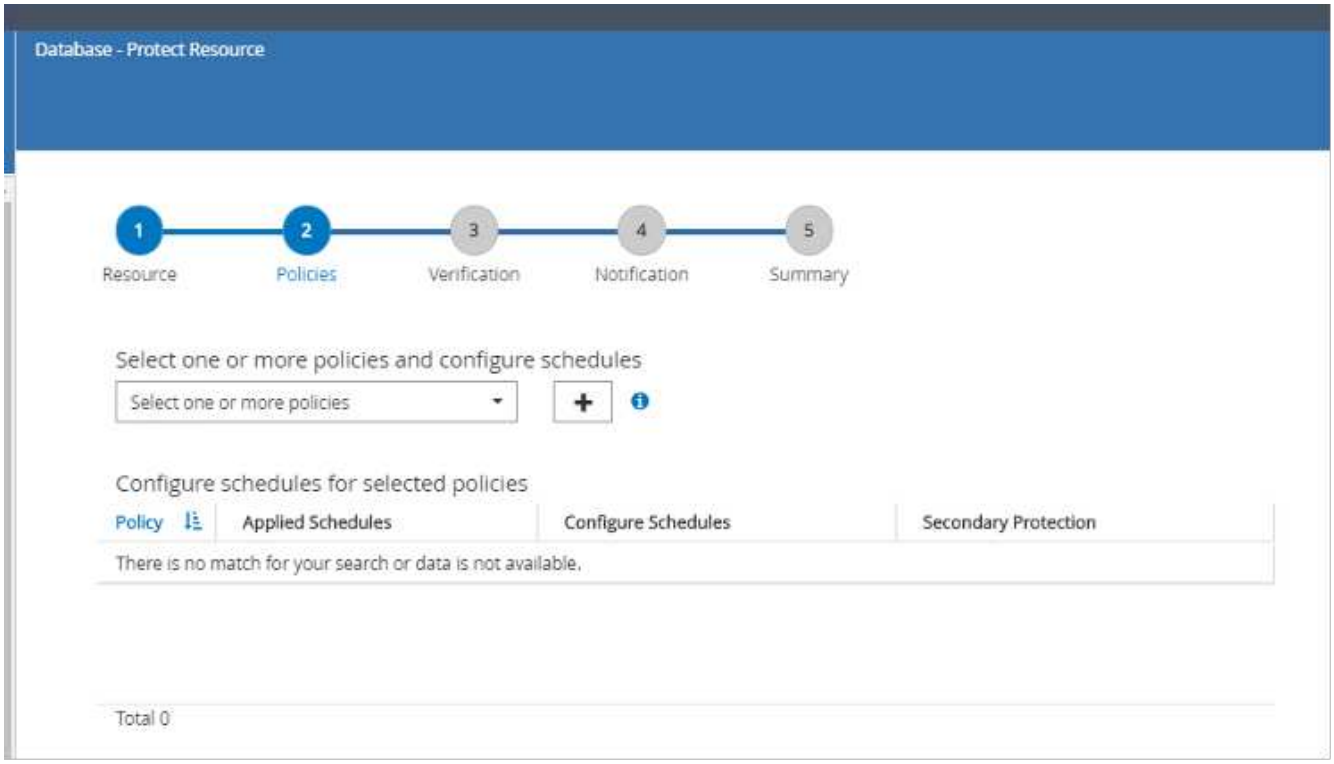
다음 단계에서는 백업 정책을 설정하는 방법을 보여줍니다.

1. 리소스 탭에서 데이터베이스를 선택하고 오른쪽 상단에서 "Protect"를 선택합니다.

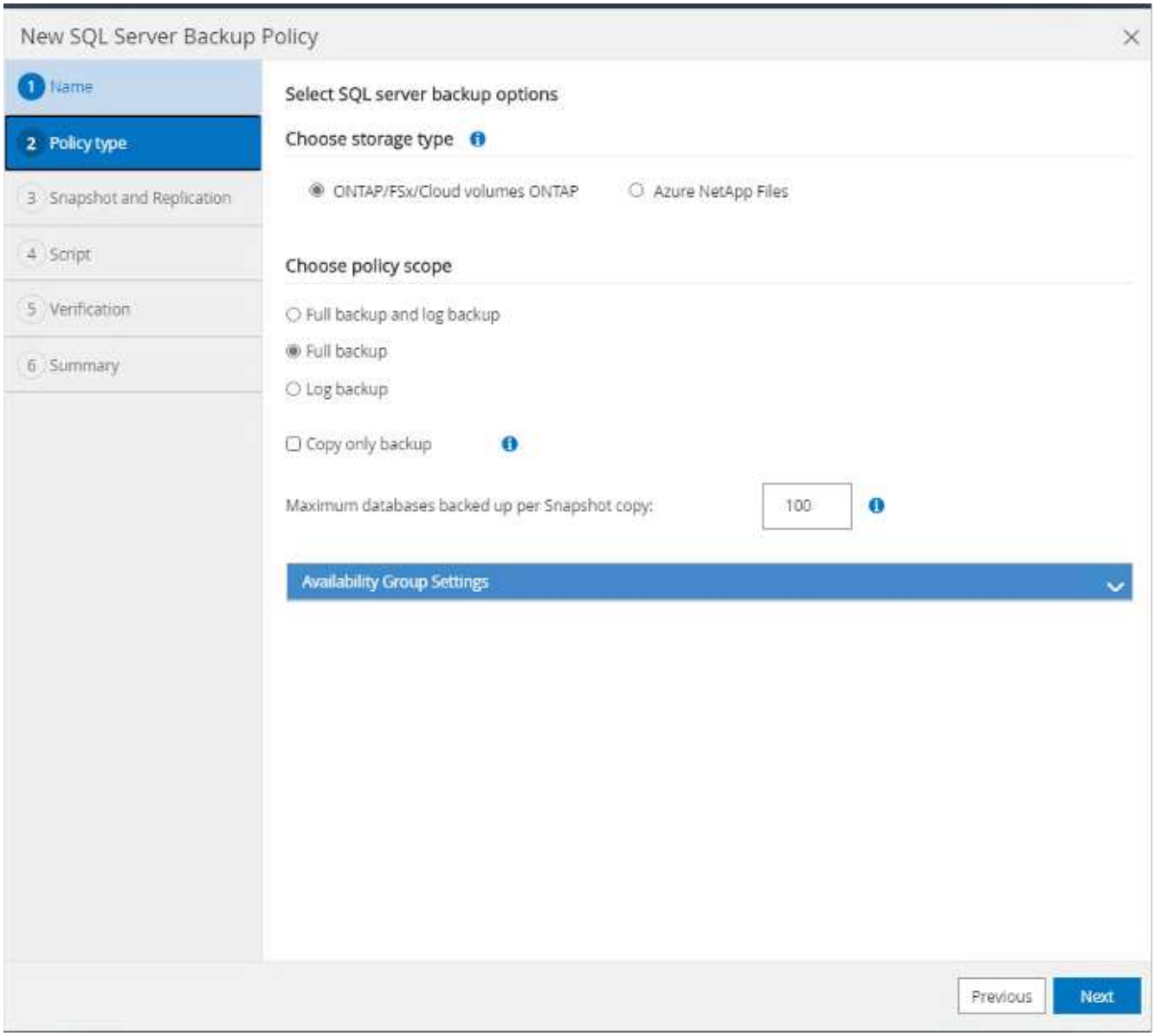
   유효성 검사는 게스트 VM에서 실행 중인 SQL Server 데이터베이스에 대해 수행됩니다.



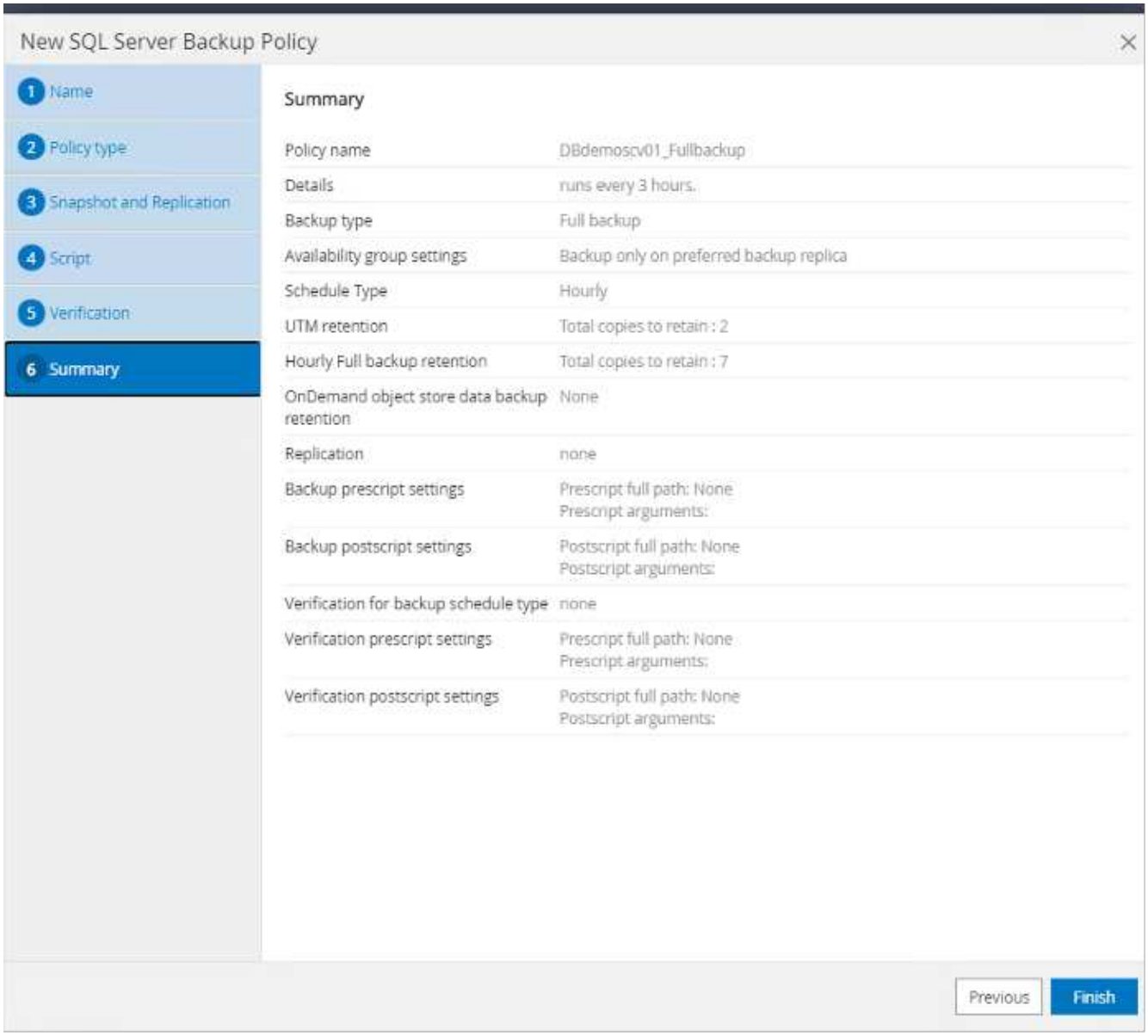
2. 더하기 기호 아이콘을 클릭하여 SQL Server 백업 정책을 구성합니다.



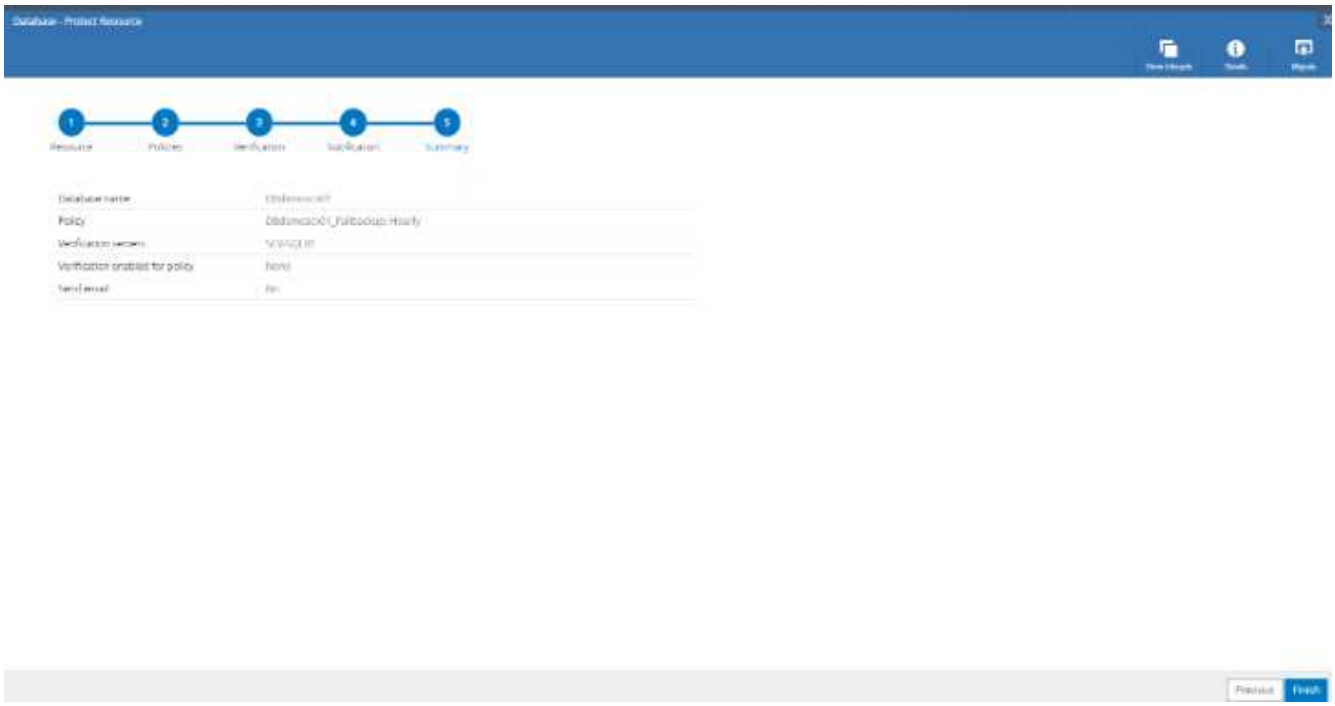
3. 이 데모에서는 "Full backup"이 선택되어 있습니다. 계속하려면 "Next"를 선택하세요.



4. 요약 페이지에서 "Finish"를 선택합니다.


New SQL Server Backup Policy
1 Name
2 Policy type
3 Snapshot and Replication
4 Script
5 Verification
6 Summary
Summary
Policy name
DBdemoscv01_Fullbackup
Details
runs every 3 hours.
Backup type
Full backup
Availability group settings
Backup only on preferred backup replica
Schedule Type
Hourly
UTM retention
Total copies to retain : 2
Hourly Full backup retention
Total copies to retain : 7
OnDemand object store data backup retention
None
Replication
none
Backup prescript settings
Prescript full path: None
Prescript arguments:
Backup postscript settings
Postscript full path: None
Postscript arguments:
Verification for backup schedule type
none
Verification prescript settings
Prescript full path: None
Prescript arguments:
Verification postscript settings
Postscript full path: None
Postscript arguments:
Previous
Finish

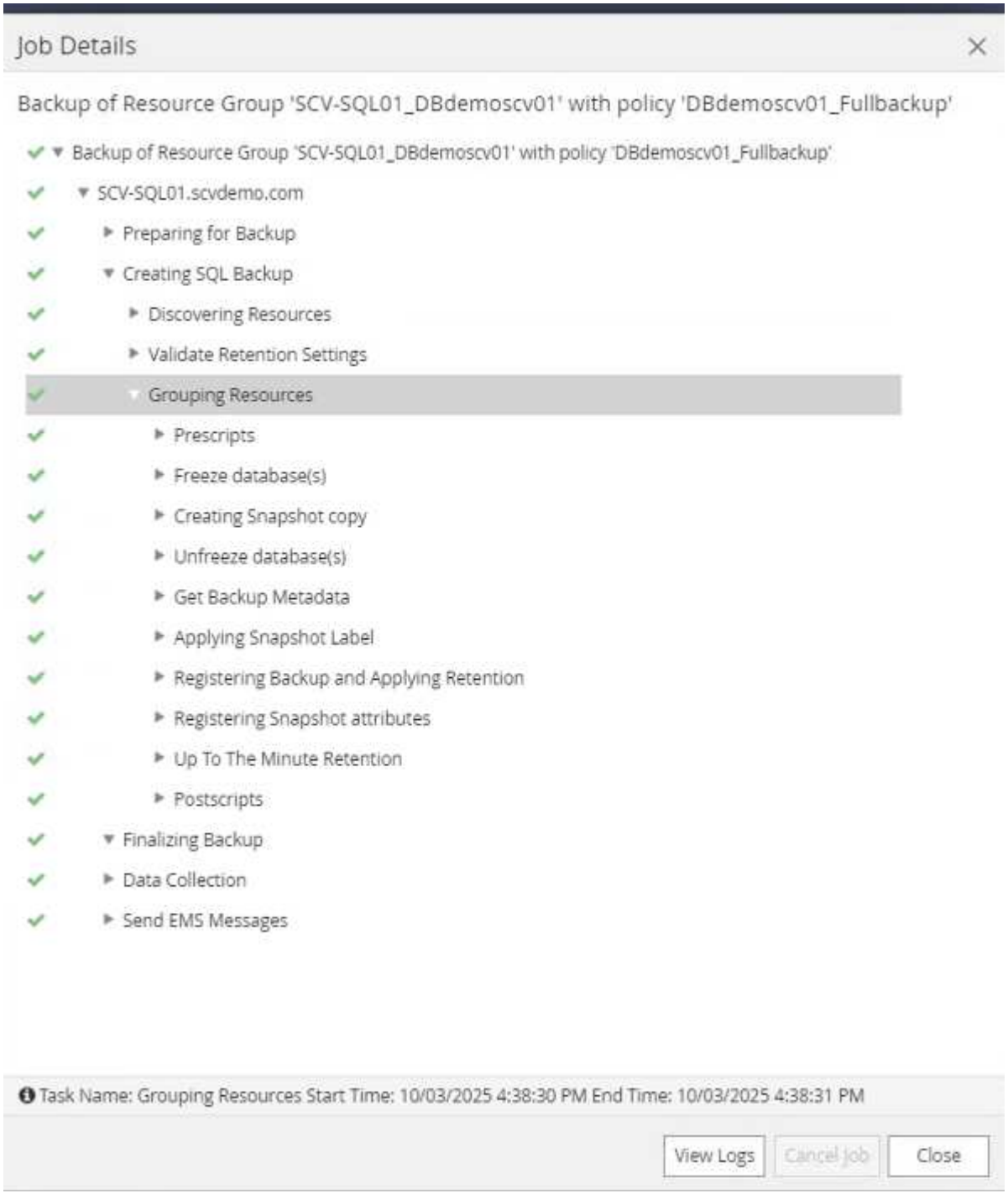
5. "완료"로 진행하십시오.



백업 모니터링

백업 정책을 설정한 후에는 백업 작업이 진행되는 동안 모니터링할 수 있습니다. 지금 백업을 클릭하여 필요에 따라 백업 작업을 실행하거나 예약된 백업 정책이 실행될 때까지 기다리면 됩니다.

1. **Monitor › Jobs**를 사용하여 작업 진행 상황을 모니터링하십시오.
2. 백업 작업을 선택한 다음 "Details"를 클릭하여 아래와 같이 작업 세부 정보를 확인하십시오.

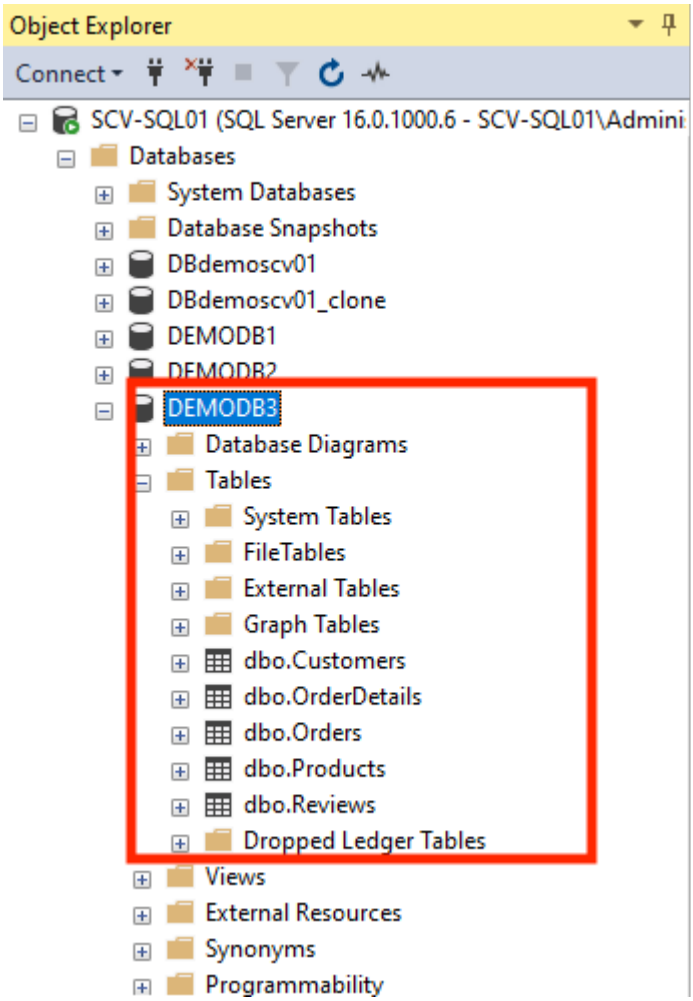


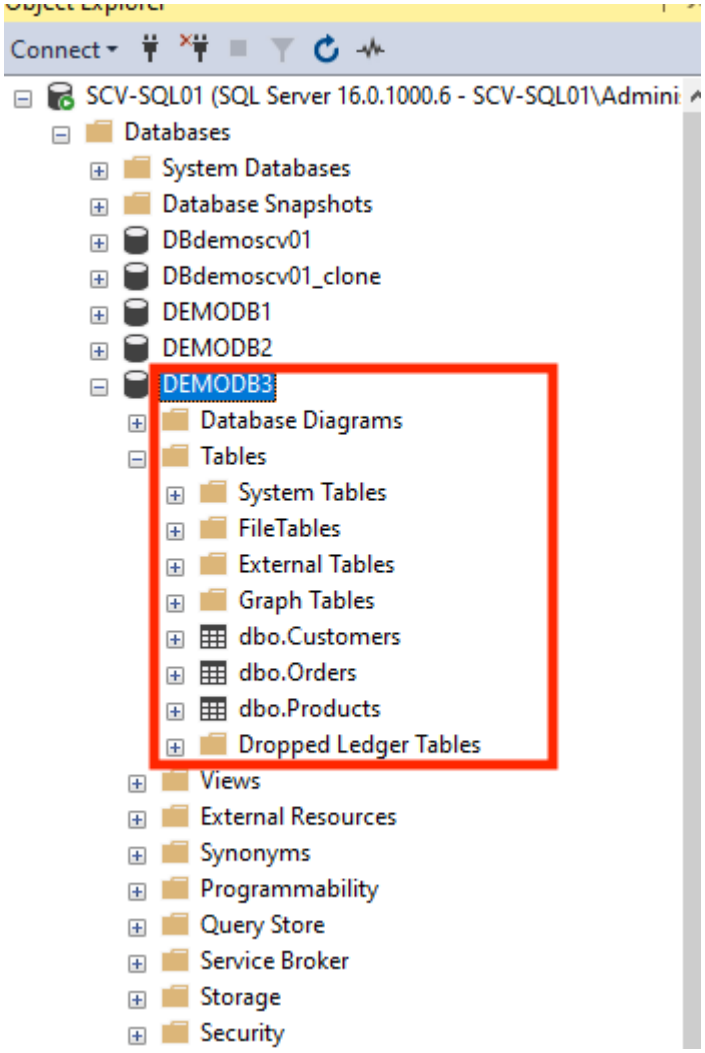
VMDK에 상주하는 데이터베이스 복원

VMDK의 데이터베이스를 특정 시점으로 복원할 수 있습니다.

데이터베이스에서 일부 테이블을 삭제한 다음 시점 복원을 수행하여 수정함으로써 이 작업의 중요성을 시뮬레이션할 수 있습니다.

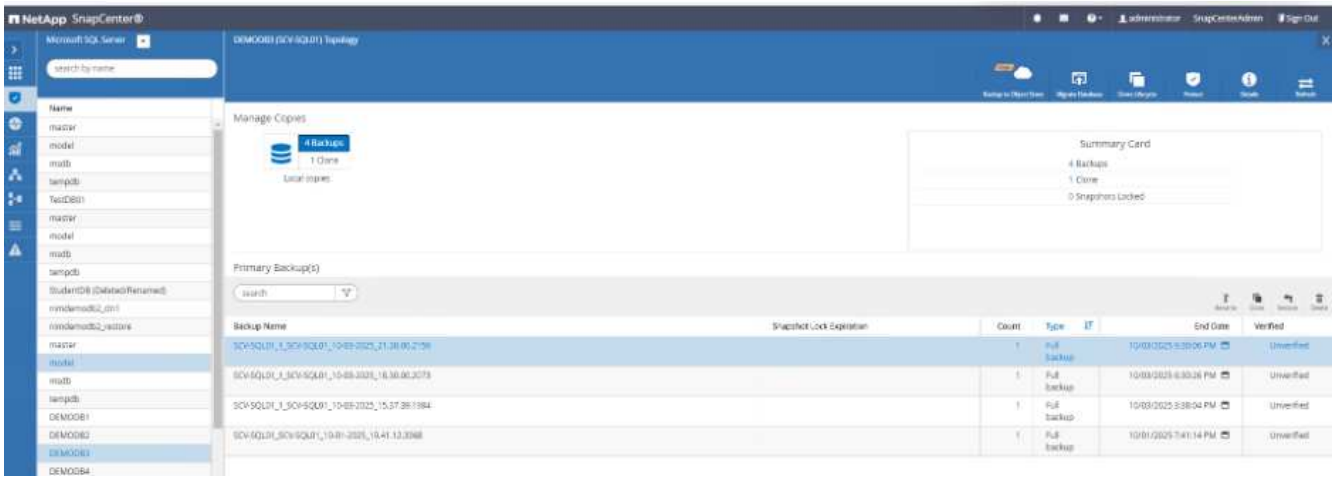
아래에서 첫 번째 스크린샷에 표시된 데이터베이스의 여러 테이블이 두 번째 스크린샷에서 삭제된 것을 확인할 수 있습니다.


Object Explorer
Connect
SCV-SQL01 (SQL Server 16.0.1000.6 - SCV-SQL01\Admini
Databases
System Databases
Database Snapshots
DBdemoscv01
DBdemoscv01_clone
DEMODB1
DEMODB2
DEMODB3
Database Diagrams
Tables
System Tables
FileTables
External Tables
Graph Tables
dbo.Customers
dbo.OrderDetails
dbo.Orders
dbo.Products
dbo.Reviews
Dropped Ledger Tables
Views
External Resources
Synonyms
Programmability

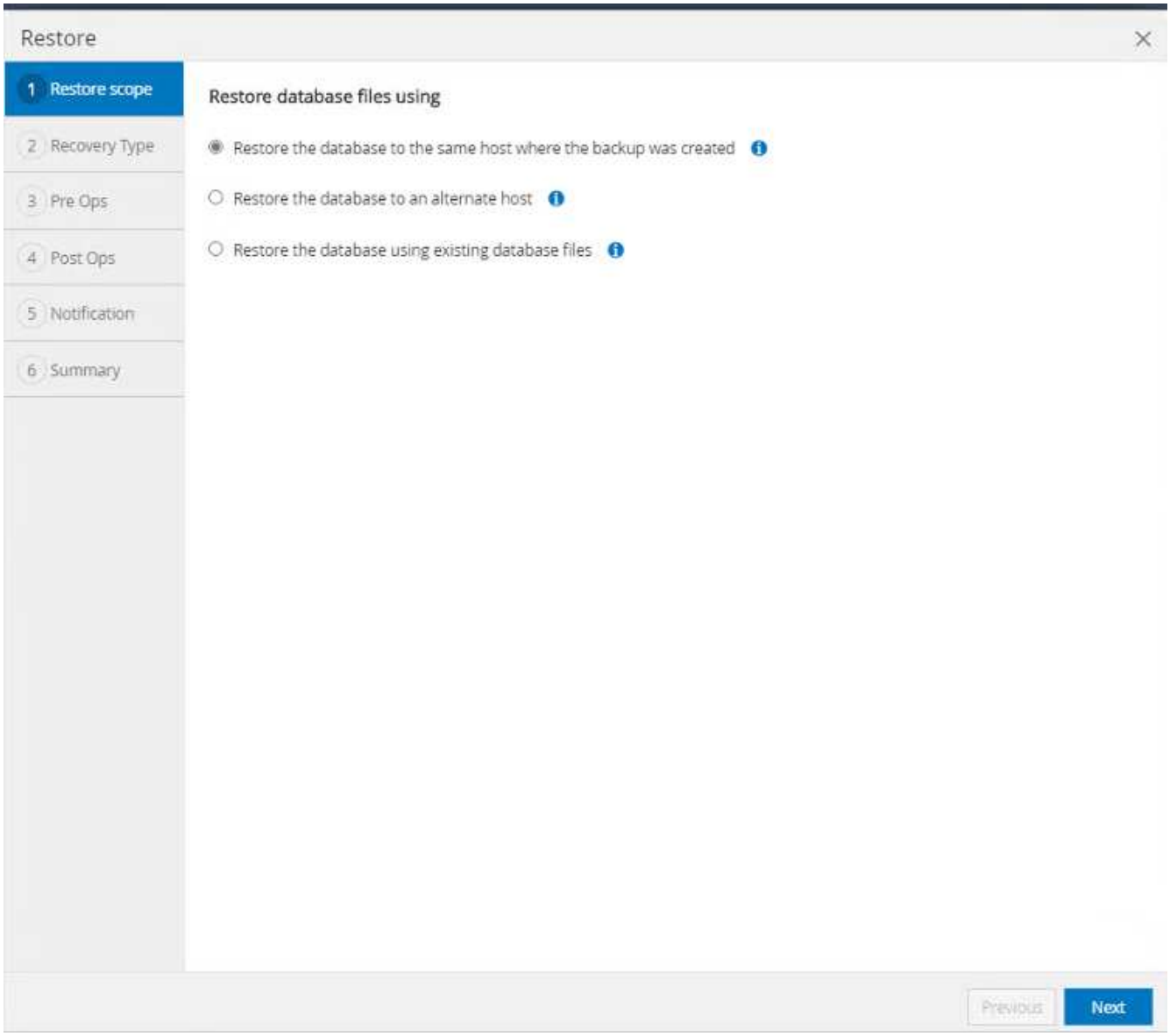


다음 단계는 삭제된 테이블을 복구하기 위해 복원을 수행하는 방법을 보여줍니다.

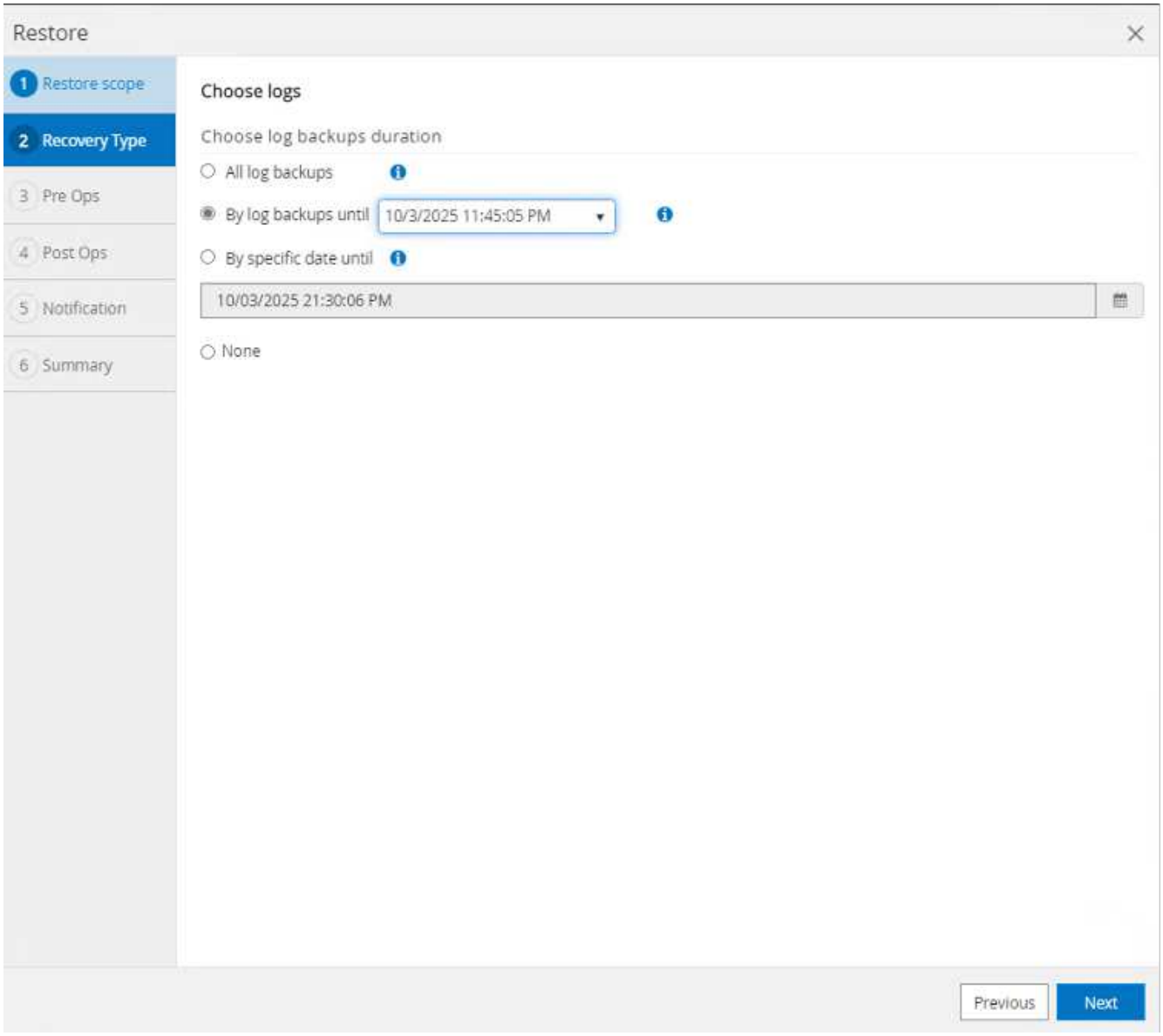
1. 리소스 그룹에서 데이터베이스를 선택합니다.



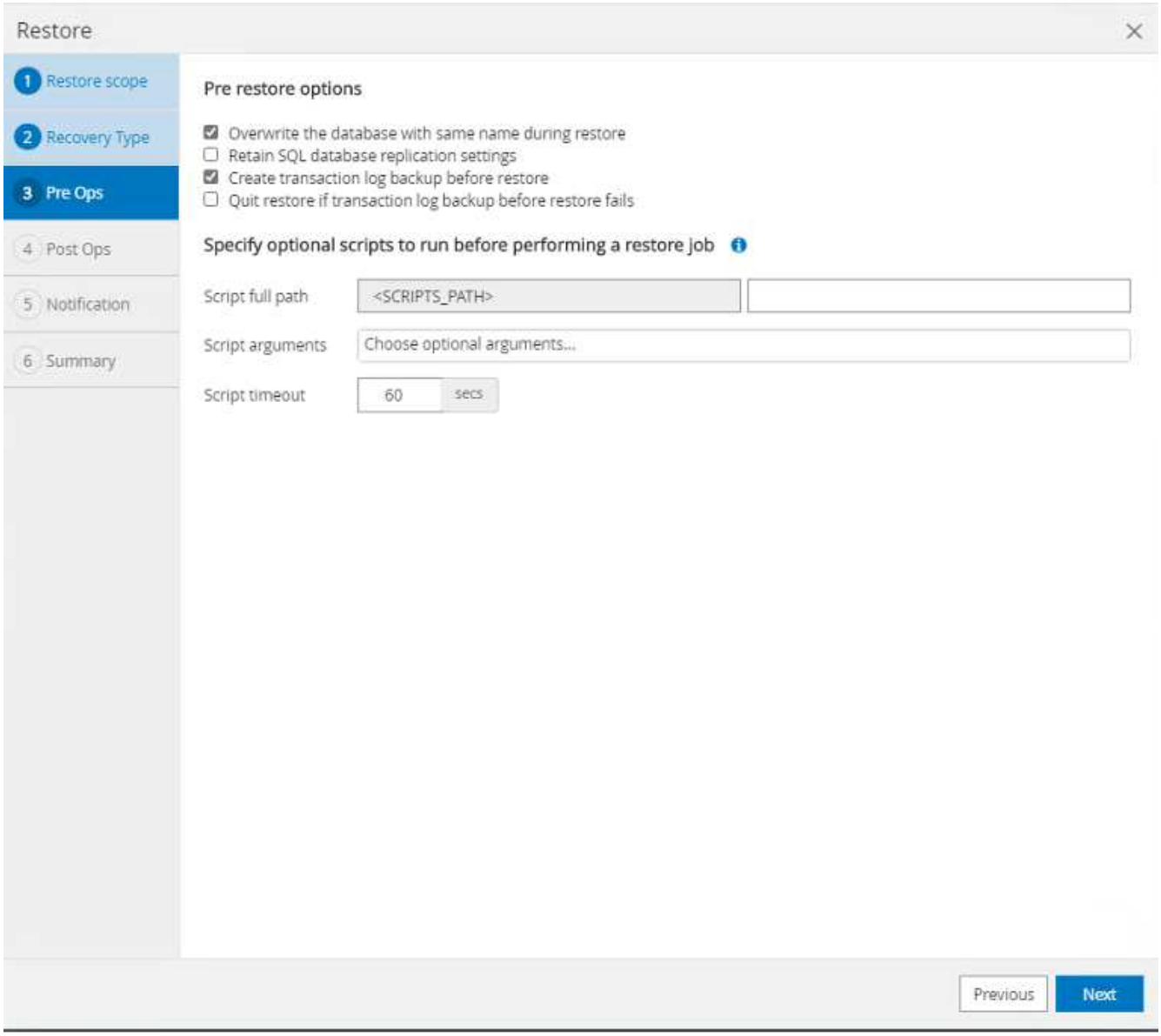
2. 복원 페이지에서 "백업이 생성된 동일한 호스트로 데이터베이스 복원" 옵션을 선택합니다.



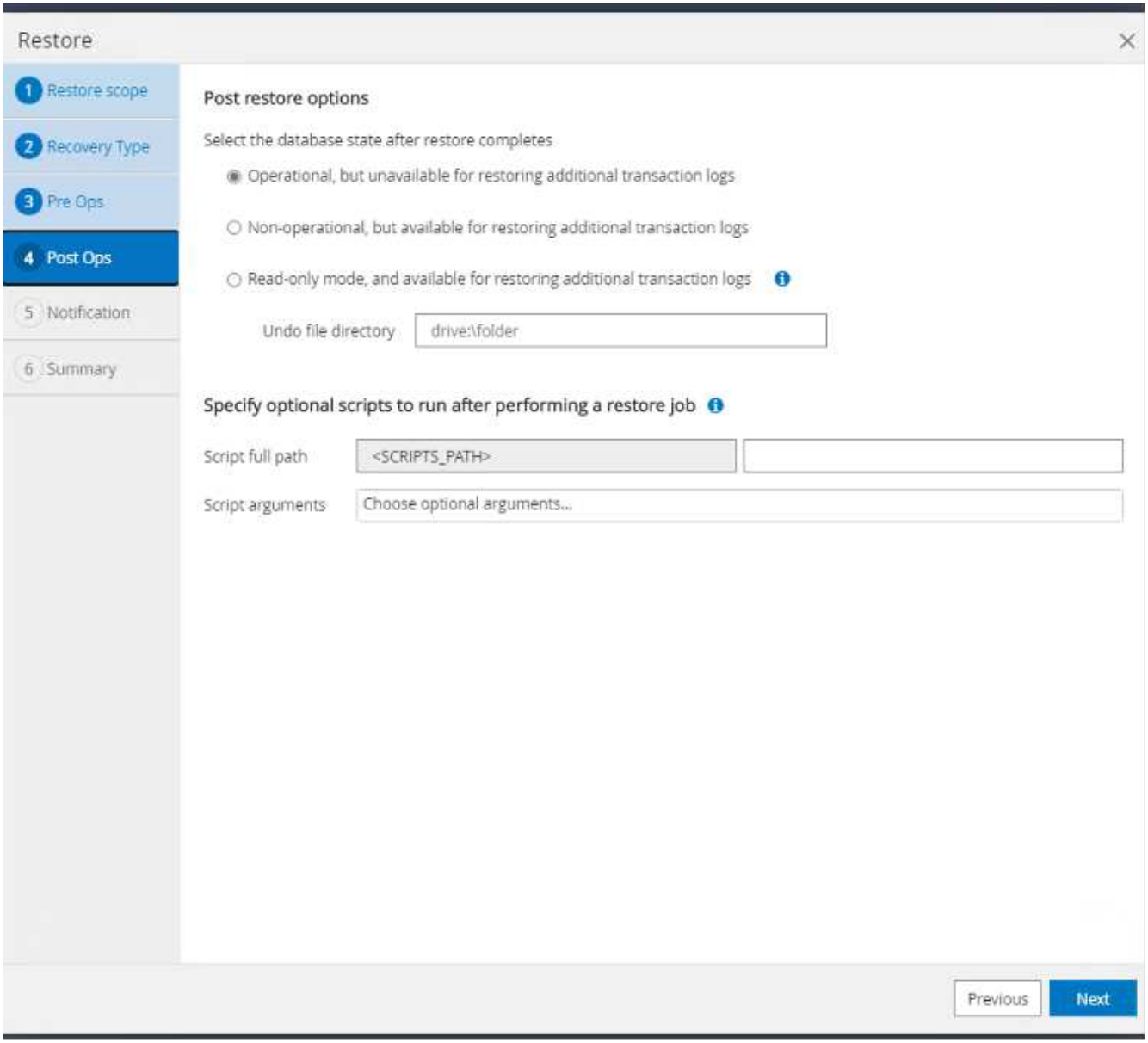
3. 특정 시점의 로그 백업을 사용하려면 해당 옵션을 선택하십시오.



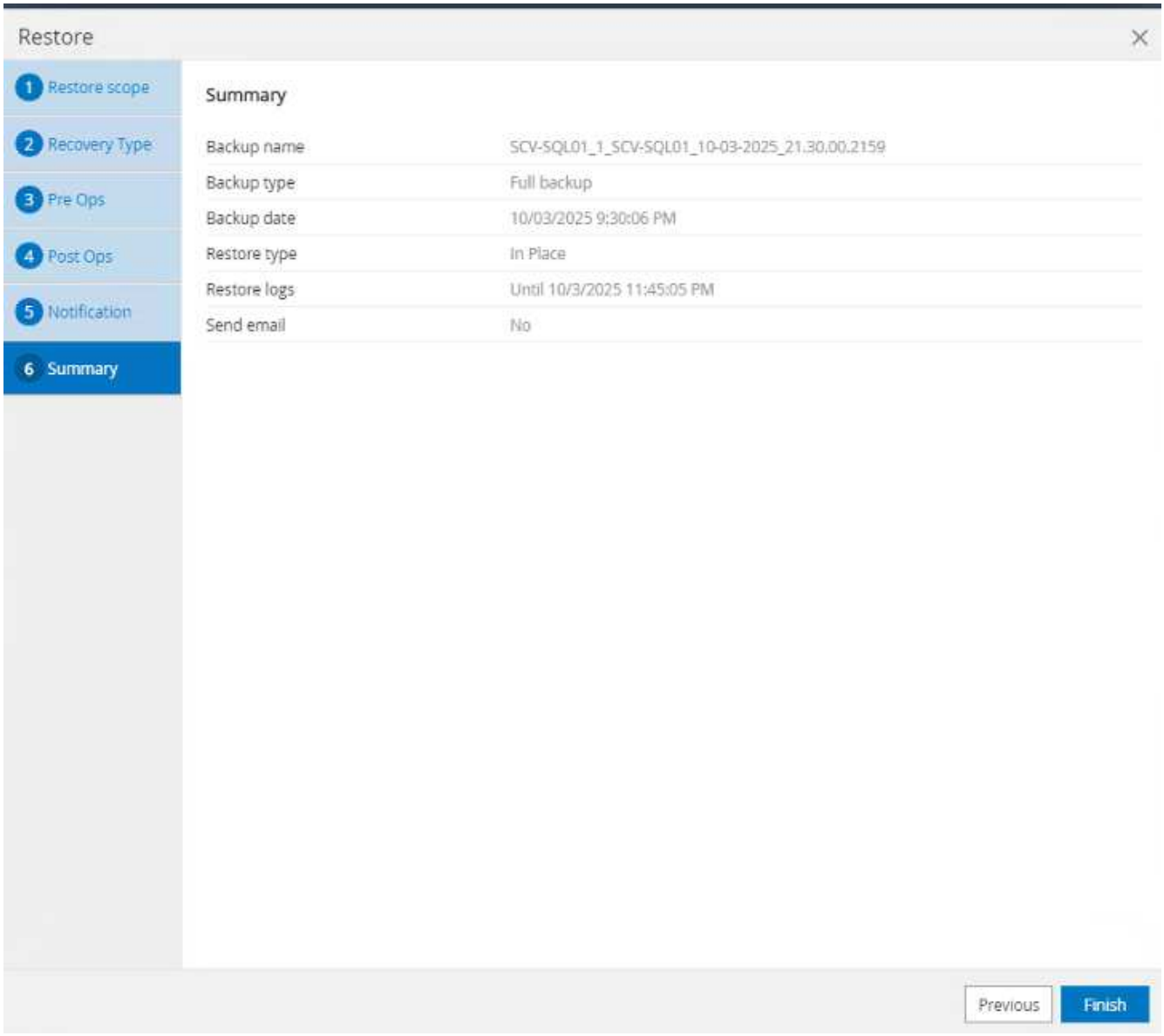
4. "복원 중 동일한 이름의 데이터베이스 덮어쓰기, 복원 전 트랜잭션 로그 백업 생성"을 선택하고 "다음"을 선택합니다.



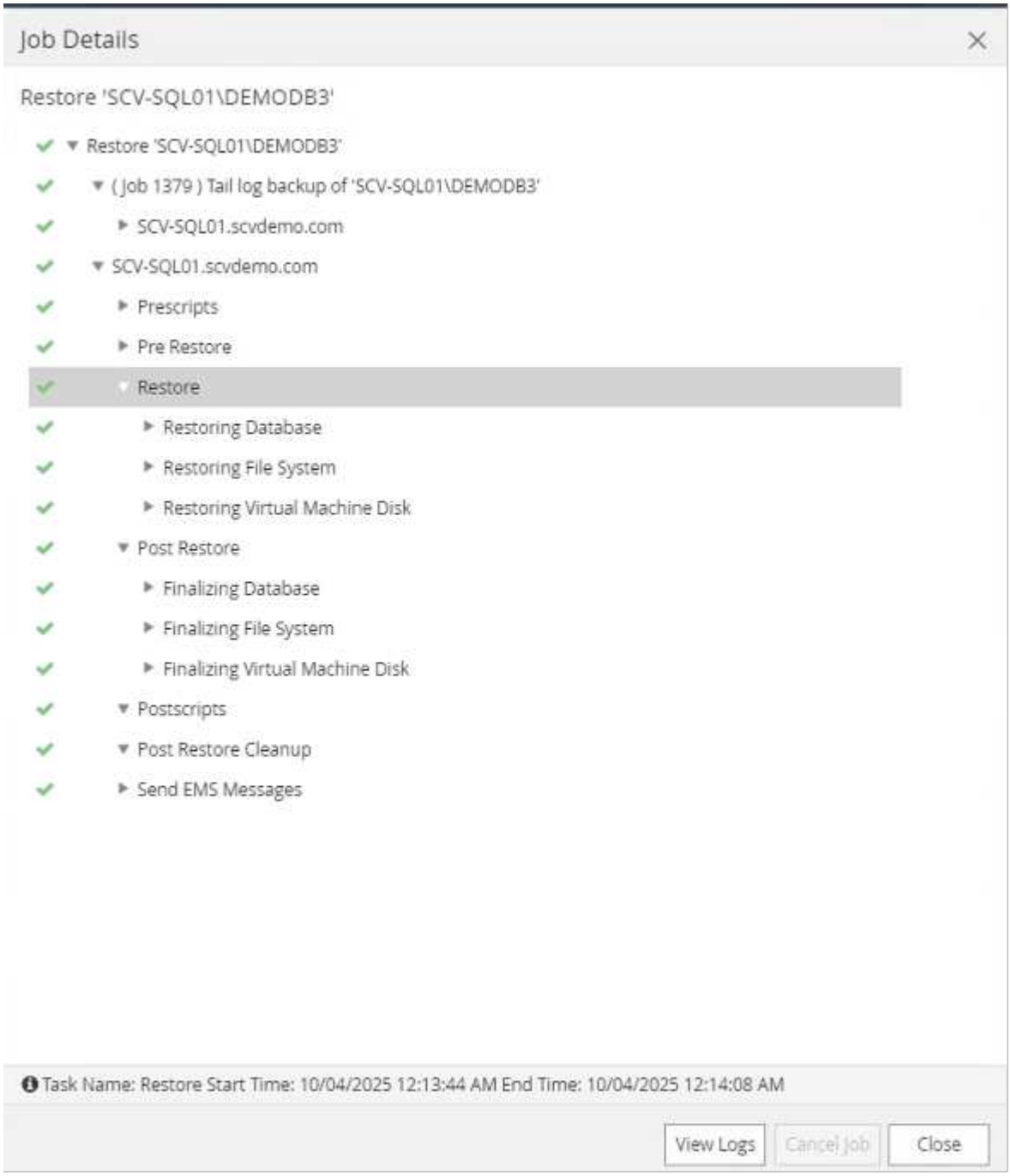
5. 복원 후 데이터베이스가 취할 상태를 목록 옵션에서 선택하고 "Next"를 선택하십시오.



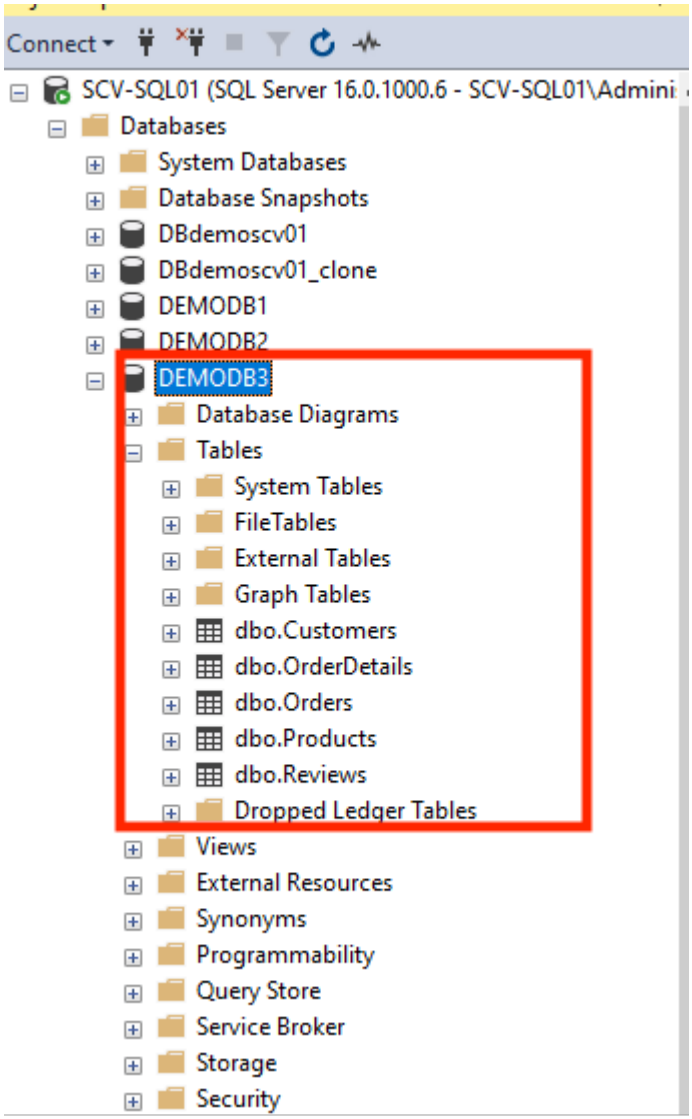
6. 요약 페이지에서 "Finish"를 선택하세요.



7. 작업이 완료될 때까지 모니터링하십시오.



8. 삭제된 테이블이 성공적으로 복원되었는지 확인하십시오.



결론

이 문서에서는 Amazon EVS 클러스터와 함께 FSx for ONTAP을 보조 데이터 저장소로 사용하는 동안 SCV 및 "SnapCenter Plug-in for SQL Server(SCSQL)"를 배포, 구성 및 사용하는 방법에 대한 자세한 단계별 지침을 제공합니다.

결론

요약하자면, Amazon EVS 배포의 총소유비용(TCO)을 최적화하기 위해 FSx for ONTAP을 사용할 때 SCV는 VM 백업을 위한 간단하고 효율적인 방법을 제공합니다. 스냅샷 복사본을 기반으로 하기 때문에 백업 및 복원이 몇 초 만에 완료되어 원활하고 신속하게 VM을 백업하고 복원할 수 있습니다.

"지금 바로 VMware용 SnapCenter 플러그인을 무료로 사용해 보세요".

Azure/AVS용 NetApp

Azure AVS를 위한 NetApp 기능

NetApp Azure VMware Solution(AVS)에 제공하는 기능에 대해 자세히 알아보세요. NetApp 게스트 연결 스토리지 장치 또는 보조 NFS 데이터 저장소로 활용하는 것부터 워크플로 마이그레이션, 클라우드로의 확장/버스팅, 백업/복원 및 재해 복구까지 다양한 기능을 제공합니다.

다음 옵션 중에서 선택하여 원하는 콘텐츠 섹션으로 이동하세요.

- "Azure에서 AVS 구성"
- "AVS용 NetApp 스토리지 옵션"
- "NetApp / VMware 클라우드 솔루션"

Azure에서 AVS 구성

온프레미스와 마찬가지로, VM을 만들고 마이그레이션하기 위한 성공적인 프로덕션 준비 환경을 위해서는 클라우드 기반 가상화 환경을 계획하는 것이 중요합니다.

이 섹션에서는 Azure VMware Solution을 설정하고 관리하는 방법과 NetApp 스토리지를 연결하는 데 사용 가능한 옵션과 함께 사용하는 방법을 설명합니다.

> ⓘ 게스트 내 스토리지는 Cloud Volumes ONTAP Azure VMware Solution에 연결하는 데 지원되는 유일한 방법입니다.

설정 과정은 다음 단계로 나눌 수 있습니다.

- 리소스 공급자를 등록하고 프라이빗 클라우드를 생성하세요
- 새 ExpressRoute 가상 네트워크 게이트웨이 또는 기존 ExpressRoute 가상 네트워크 게이트웨이에 연결
- 네트워크 연결을 검증하고 프라이빗 클라우드에 액세스합니다.

자세한 내용을 보려면"AVS 구성 단계" .

AVS용 NetApp 스토리지 옵션

NetApp 스토리지는 Azure AVS 내에서 추측 연결 또는 보조 NFS 데이터 저장소로 등 여러 가지 방법으로 활용할 수 있습니다.

방문해주세요"지원되는 NetApp 스토리지 옵션" 자세한 내용은.

Azure는 다음 구성에서 NetApp 스토리지를 지원합니다.

- 게스트 연결 스토리지로서의 Azure NetApp Files (ANF)
- 게스트 연결 스토리지로서의 Cloud Volumes ONTAP (CVO)
- 보조 NFS 데이터 저장소로서의 Azure NetApp Files (ANF)

자세한 내용을 보려면"AVS용 게스트 연결 스토리지 옵션" . 자세한 내용을 보려면"AVS를 위한 보충 NFS 데이터 저장소 옵션" .

솔루션 사용 사례

NetApp 및 VMware 클라우드 솔루션을 사용하면 많은 사용 사례를 Azure AVS에 쉽게 배포할 수 있습니다. 각 사용 사례는 VMware에서 정의한 클라우드 영역별로 정의됩니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 연장하다
- 이주하다

"Azure AVS용 NetApp 솔루션 찾아보기"

Azure/AVS에서 워크로드 보호

ANF 및 **JetStream**을 사용한 재해 복구

클라우드로 재해 복구를 수행하는 것은 사이트 중단 및 데이터 손상 사고(예: 랜섬웨어)로부터 작업 부하를 보호하는 탄력적이고 비용 효율적인 방법입니다. VMware VAIO 프레임워크를 사용하면 온프레미스 VMware 워크로드를 Azure Blob 스토리지에 복제하고 복구할 수 있어 데이터 손실이 최소화되거나 거의 없고 RTO가 거의 0에 가깝습니다.

JetStream DR을 사용하면 온프레미스에서 AVS로 복제된 워크로드를 원활하게 복구하고 특히 Azure NetApp Files 로 복구할 수 있습니다. DR 사이트에서 최소한의 리소스와 비용 효율적인 클라우드 스토리지를 사용하여 비용 효율적인 재해 복구를 가능하게 합니다. JetStream DR은 Azure Blob Storage를 통해 ANF 데이터 저장소로의 복구를 자동화합니다. JetStream DR은 네트워크 매핑에 따라 독립적인 VM 또는 관련 VM 그룹을 복구 사이트 인프라로 복구하고 랜섬웨어 보호를 위한 지정 시점 복구를 제공합니다.

이 문서는 JetStream DR의 작동 원리와 주요 구성 요소에 대한 이해를 제공합니다.

▼ 솔루션 배포 개요

1. 온프레미스 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 패키지로 클러스터를 구성합니다(JetStream VIB 설치).
    c. DR AVS 클러스터와 동일한 지역에 Azure Blob(Azure Storage 계정)을 프로비저닝합니다.
    d. DRVA 어플라이언스를 배포하고 복제 로그 볼륨(기존 데이터 저장소 또는 공유 iSCSI 스토리지의 VMDK)을 할당합니다.
    e. 보호된 도메인(관련 VM 그룹)을 만들고 DRVA와 Azure Blob Storage/ANF를 할당합니다.
    f. 보호를 시작합니다.
2. Azure VMware Solution 프라이빗 클라우드에 JetStream DR 소프트웨어를 설치합니다.
    a. 실행 명령을 사용하여 JetStream DR을 설치하고 구성합니다.
    b. 동일한 Azure Blob 컨테이너를 추가하고 도메인 검색 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 RocVA(복구 VA)를 구성하여 VM 배치에 ANF 데이터 저장소를 사용합니다.

f. 적절한 장애 조치(failover) 옵션을 선택하고 RTO가 거의 0에 가까운 도메인이나 VM에 대해 지속적인 복원을 시작합니다.

3. 재해 발생 시 지정된 AVS DR 사이트의 Azure NetApp Files 데이터 저장소로 장애 조치를 트리거합니다.
4. 보호 사이트가 복구된 후 보호 사이트로 장애 복구를 호출합니다. 시작하기 전에 이 문서에 표시된 대로 전제 조건이 충족되었는지 확인하십시오. "링크" 또한 JetStream 소프트웨어에서 제공하는 대역폭 테스트 도구(BWT)를 실행하여 JetStream DR 소프트웨어와 함께 사용할 때 Azure Blob 저장소의 잠재적 성능과 복제 대역폭을 평가합니다. 연결성을 포함한 전제 조건이 갖춰진 후 AVS용 JetStream DR을 설정하고 구독하세요. "Azure 마켓플레이스" . 소프트웨어 번들을 다운로드한 후 위에 설명된 설치 과정을 진행하세요.

많은 수의 VM(예: 100개 이상)에 대한 보호를 계획하고 시작할 때 JetStream DR Automation Toolkit의 용량 계획 도구(CPT)를 사용하세요. 보호할 VM 목록과 RTO 및 복구 그룹 기본 설정을 제공한 다음 CPT를 실행합니다.

CPT는 다음과 같은 기능을 수행합니다.

- RTO에 따라 VM을 보호 도메인으로 결합합니다.
- DRVA의 최적 수와 리소스를 정의합니다.
- 필요한 복제 대역폭을 추정합니다.
- 복제 로그 볼륨 특성(용량, 대역폭 등)을 식별합니다.
- 필요한 객체 스토리지 용량을 추정하는 등의 작업입니다.

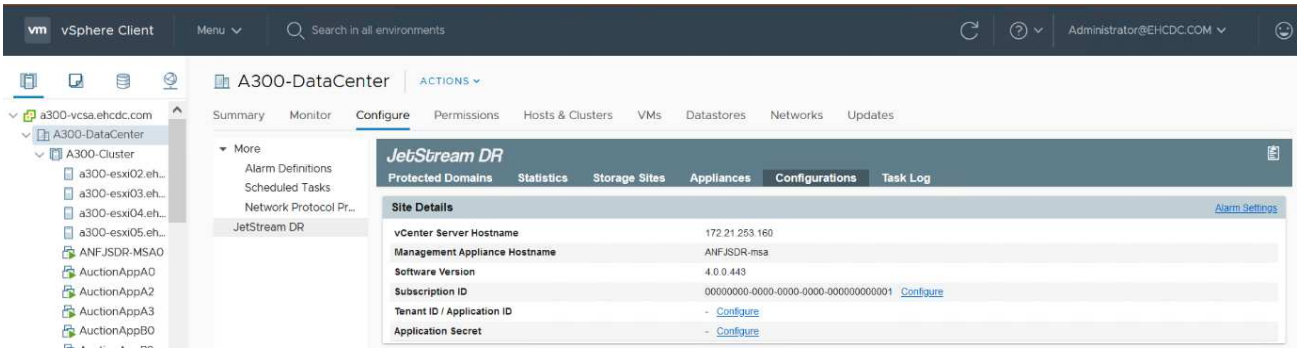
ⓘ 규정된 도메인의 수와 내용은 평균 IOPS, 총 용량, 우선순위(장애 조치 순서를 정의함), RTO 등 다양한 VM 특성에 따라 달라집니다.

온프레미스 데이터 센터에 **JetStream DR** 설치

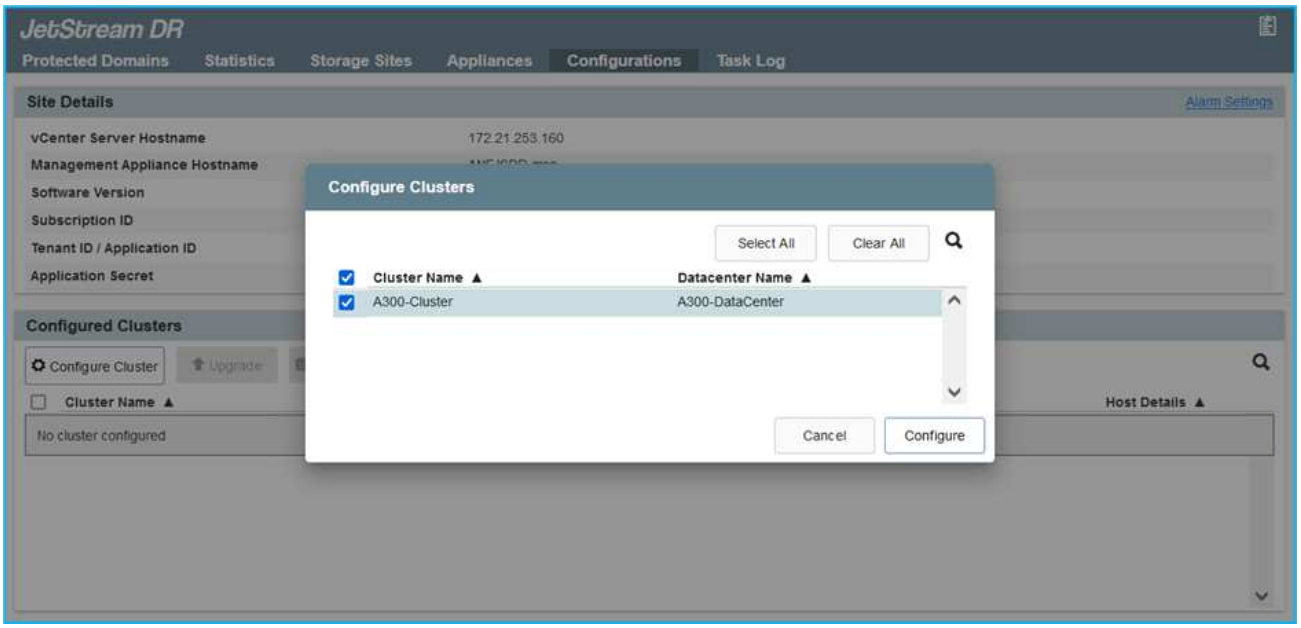
JetStream DR 소프트웨어는 JetStream DR 관리 서버 가상 어플라이언스(MSA), DR 가상 어플라이언스(DRVA), 호스트 구성 요소(I/O 필터 패키지)의 세 가지 주요 구성 요소로 구성됩니다. MSA는 컴퓨팅 클러스터에 호스트 구성 요소를 설치하고 구성한 다음 JetStream DR 소프트웨어를 관리하는 데 사용됩니다. 다음 목록은 설치 과정에 대한 간략한 설명을 제공합니다.

▼ 온프레미스에 **JetStream DR**을 설치하는 방법

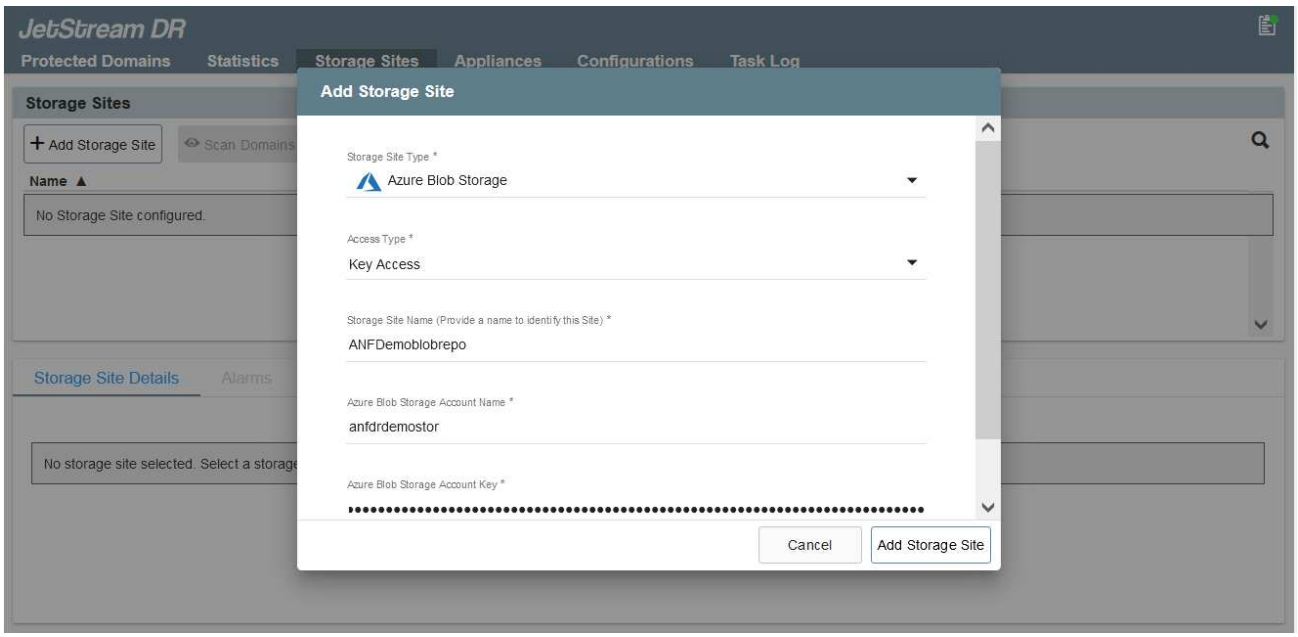
1. 필수 조건을 확인하세요.
2. 리소스 및 구성 권장 사항을 알아보려면 용량 계획 도구를 실행합니다(선택 사항이지만 개념 증명 시험에 권장됨).
3. 지정된 클러스터의 vSphere 호스트에 JetStream DR MSA를 배포합니다.
4. 브라우저에서 DNS 이름을 사용하여 MSA를 시작합니다.
5. MSA에 vCenter 서버를 등록합니다. 설치를 수행하려면 다음의 자세한 단계를 완료하세요.
6. JetStream DR MSA가 배포되고 vCenter Server가 등록된 후 vSphere Web Client를 사용하여 JetStream DR 플러그인에 액세스합니다. 데이터 센터 > 구성 > JetStream DR로 이동하여 이 작업을 수행할 수 있습니다.



7. JetStream DR 인터페이스에서 적절한 클러스터를 선택하세요.



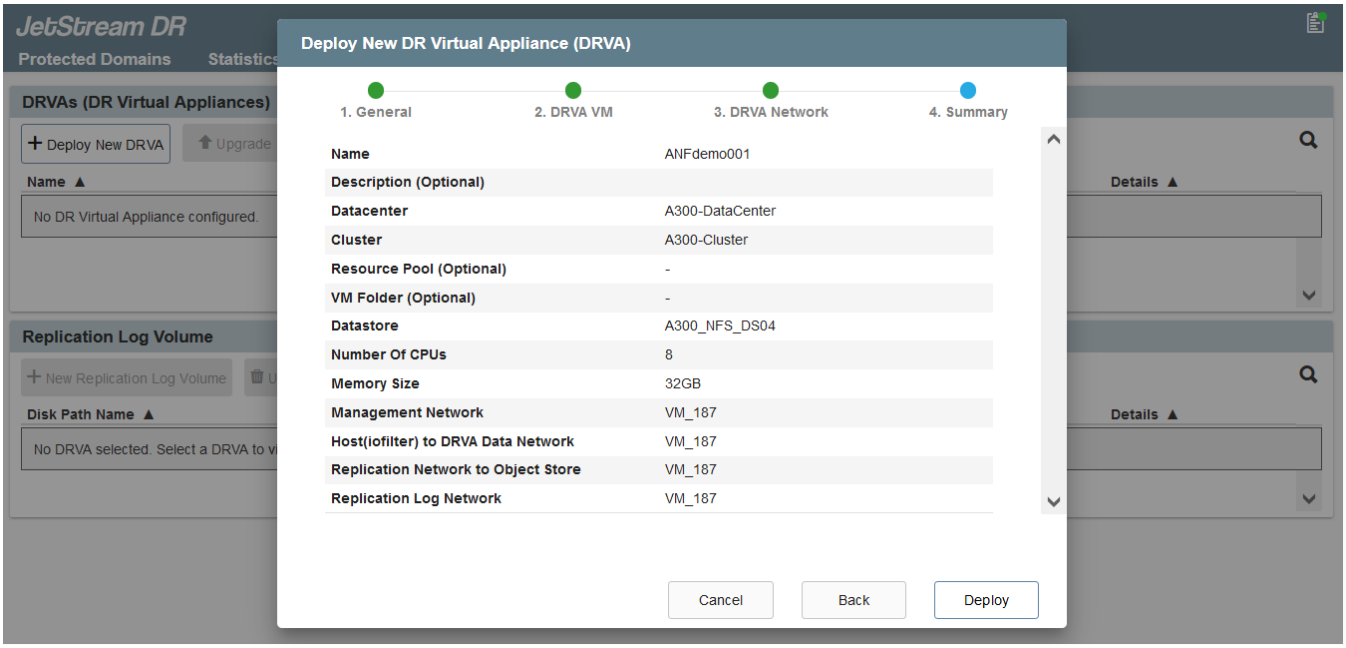
8. I/O 필터 패키지로 클러스터를 구성합니다.



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

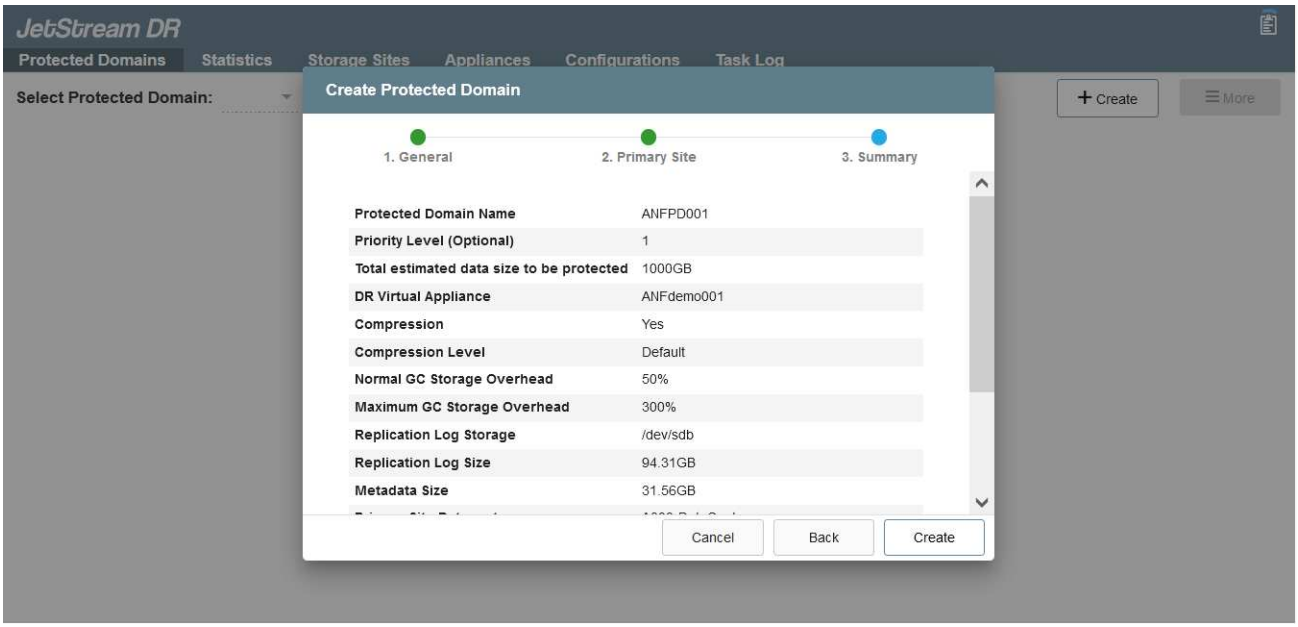
> DRVA는 CPT에서 자동으로 생성할 수 있지만 POC 시험의 경우 DR 주기를 수동으로 구성하고 실행하는 것이 좋습니다(보호 시작 > 장애 조치 > 장애 복구).

JetStream DRVA는 데이터 복제 프로세스의 주요 기능을 용이하게 하는 가상 어플라이언스입니다. 보호된 클러스터에는 최소한 하나의 DRVA가 포함되어야 하며, 일반적으로 호스트당 하나의 DRVA가 구성됩니다. 각 DRVA는 여러 개의 보호된 도메인을 관리할 수 있습니다.



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

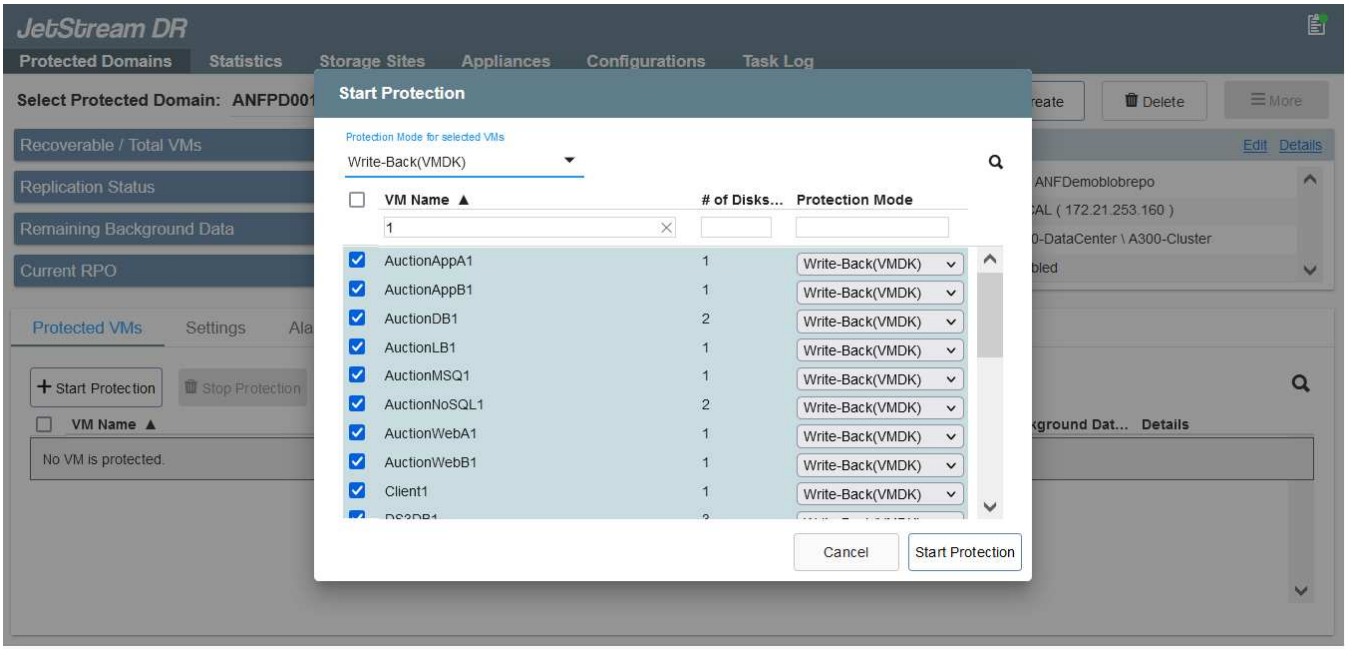
1. 사용 가능한 데이터 저장소나 독립적인 공유 iSCSI 스토리지 풀에서 VMDK를 사용하여 각 DRVA에 대한 복제 로그 볼륨을 생성합니다.
2. 보호된 도메인 탭에서 Azure Blob Storage 사이트, DRVA 인스턴스 및 복제 로그에 대한 정보를 사용하여 필요한 수의 보호된 도메인을 만듭니다. 보호된 도메인은 클러스터 내에서 함께 보호되고 장애 조치/장애 복구 작업에 대한 우선 순위가 지정된 특정 VM 또는 VM 세트를 정의합니다.



3. 보호하려는 VM을 선택하고 보호된 도메인의 VM 보호를 시작합니다. 이렇게 하면 지정된 Blob Store에 데이터 복제가 시작됩니다.

보호된 도메인의 모든 VM에 동일한 보호 모드가 사용되는지 확인합니다.

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



복제 로그 볼륨이 고성능 스토리지에 배치되었는지 확인하세요.

장애 조치 실행 설명서를 구성하여 VM을 그룹화(복구 그룹이라고 함), 부팅 순서 순서를 설정하고 IP 구성과 함께 CPU/메모리 설정을 수정할 수 있습니다.

복구 사이트(AVS)의 모범 사례는 미리 3노드 파일럿 라이트 클러스터를 만드는 것입니다. 이를 통해 다음 항목을 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 저장소로 구성하고 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 가까운 경우, 회복 부위에서 지속적인 수분 보충을 시작해야 합니다.

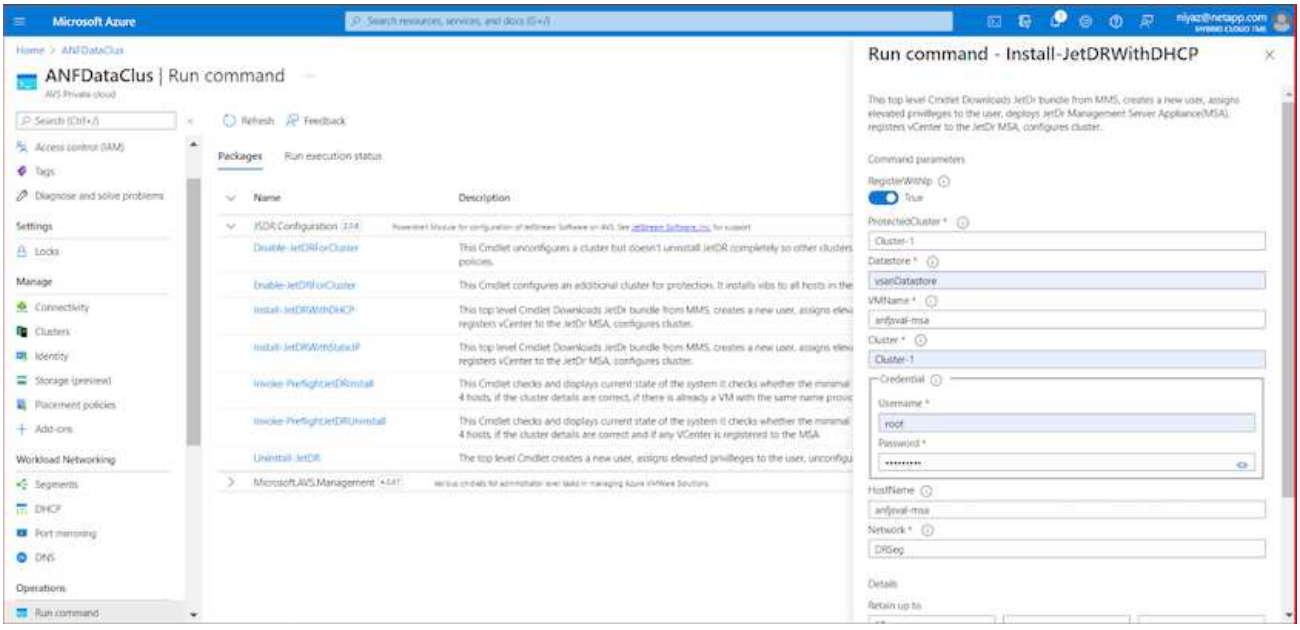
▼ 개인 클라우드에 **AVS**용 **JetStream DR**을 설치하는 방법

Azure VMware Solution 프라이빗 클라우드에 AVS용 JetStream DR을 설치하려면 다음 단계를 완료하세요.

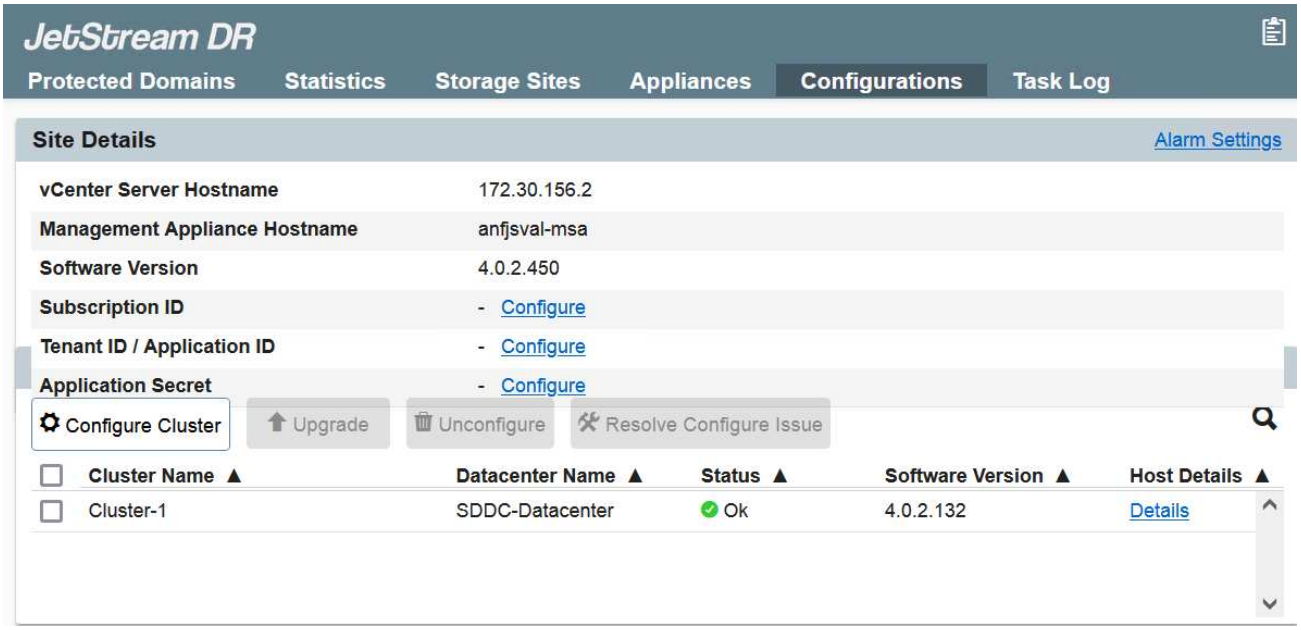
1. Azure Portal에서 Azure VMware 솔루션으로 이동하여 프라이빗 클라우드를 선택하고 명령 실행 > 패키지 > JSDR.Configuration을 선택합니다.

ⓘ 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.

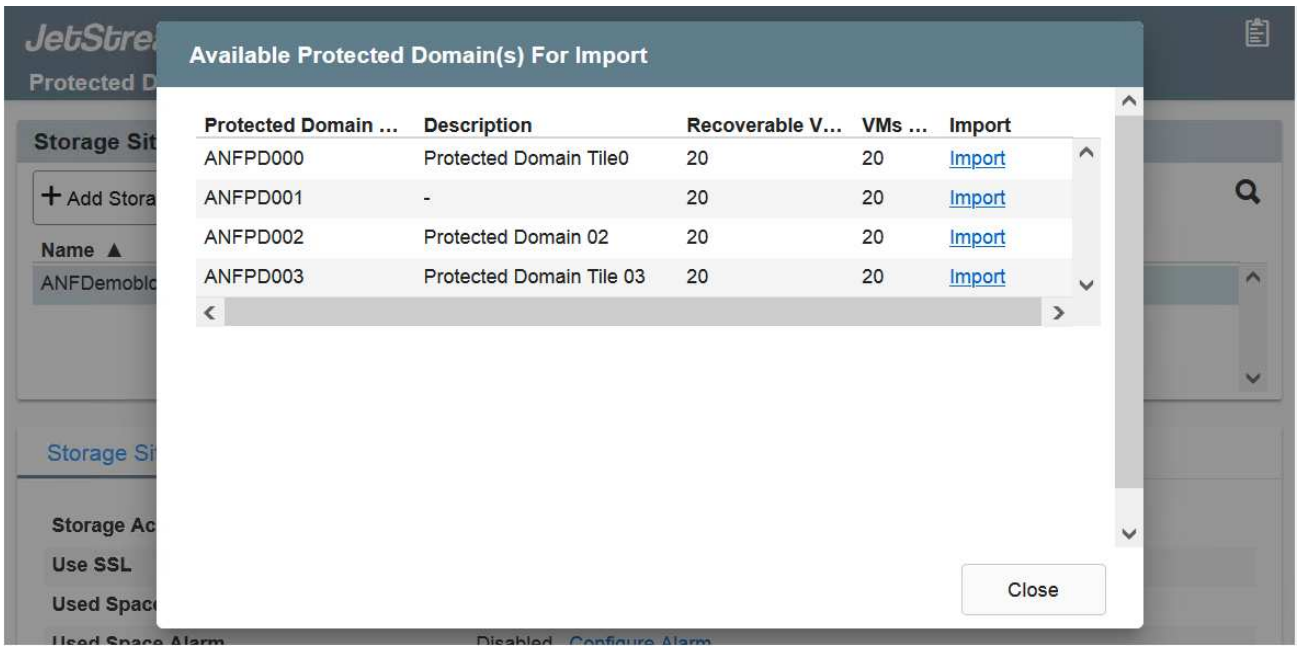
다음 스크린샷은 DHCP 기반 IP 주소를 사용하여 설치하는 방법을 보여줍니다.



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



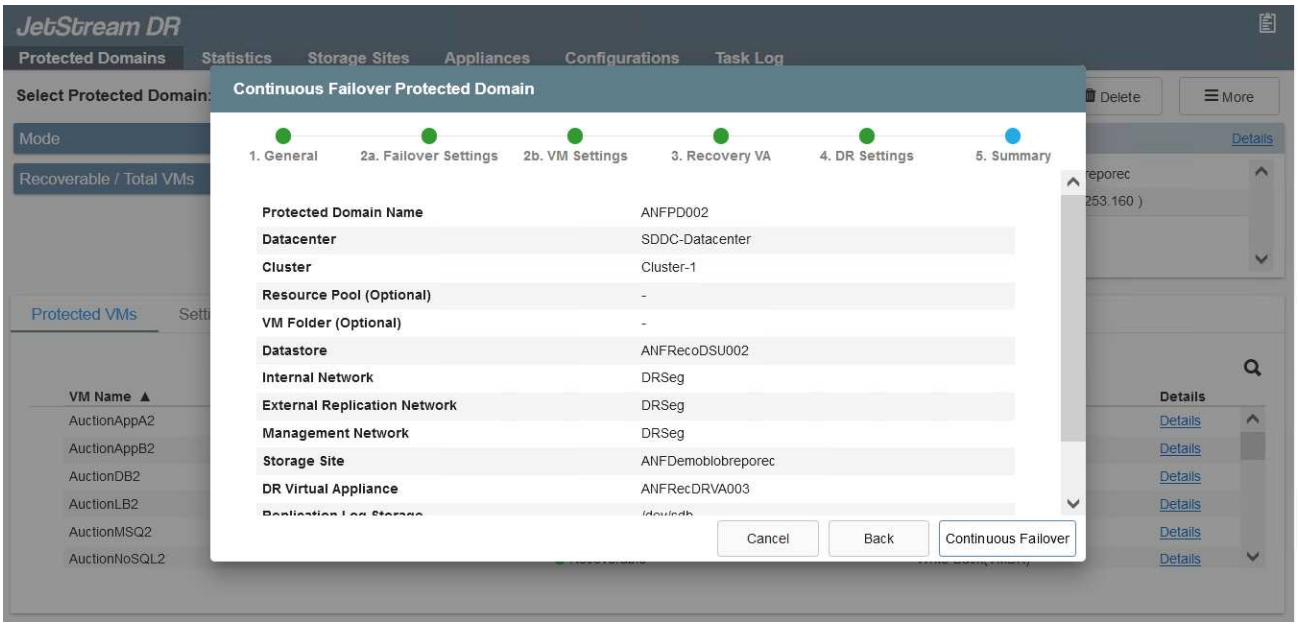
3. JetStream DR 인터페이스에서 온-프레미스 클러스터를 스토리지 사이트로 보호하는 데 사용된 Azure Blob Storage 계정을 추가한 다음 도메인 검사 옵션을 실행합니다.



4. 보호된 도메인을 가져온 후 DRVA 어플라이언스를 배포합니다. 이 예에서는 JetStream DR UI를 사용하여 복구 사이트에서 수동으로 지속적인 수분 공급이 시작됩니다.

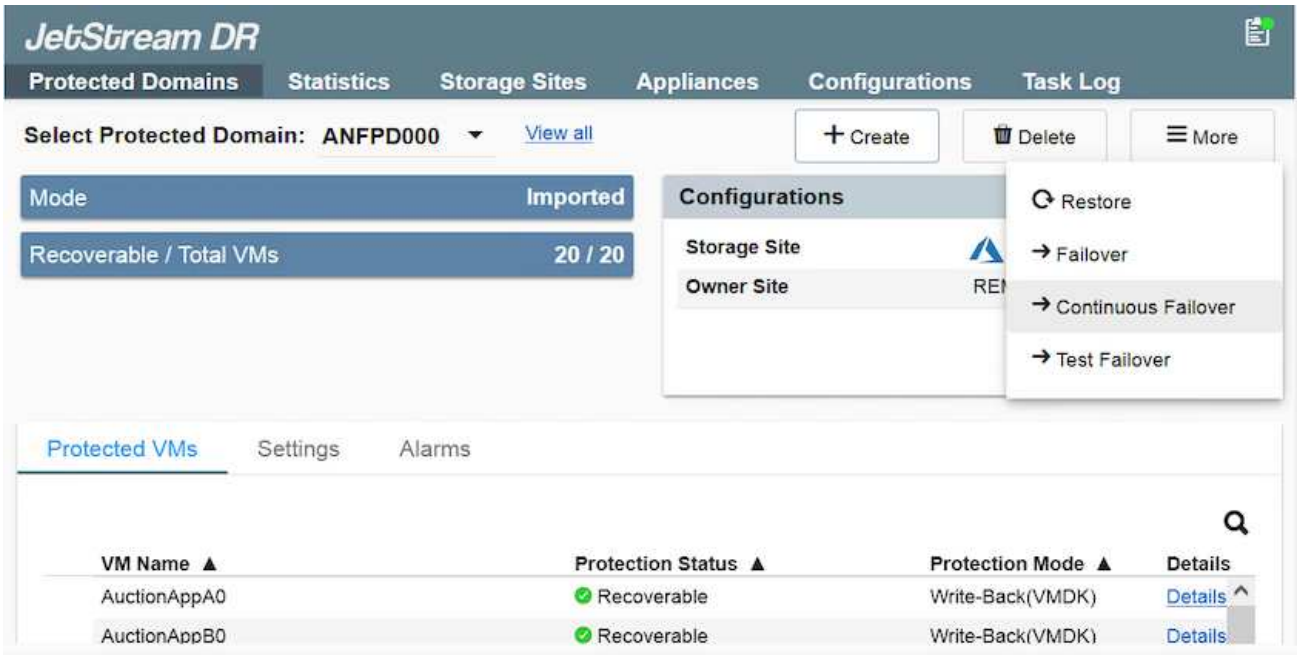
> ⓘ 이러한 단계는 CPT에서 만든 계획을 사용하여 자동화할 수도 있습니다.

5. 사용 가능한 vSAN 또는 ANF 데이터 저장소를 사용하여 복제 로그 볼륨을 생성합니다.
6. 보호된 도메인을 가져오고 VM 배치를 위해 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.

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



장애 조치/장애 복구 수행

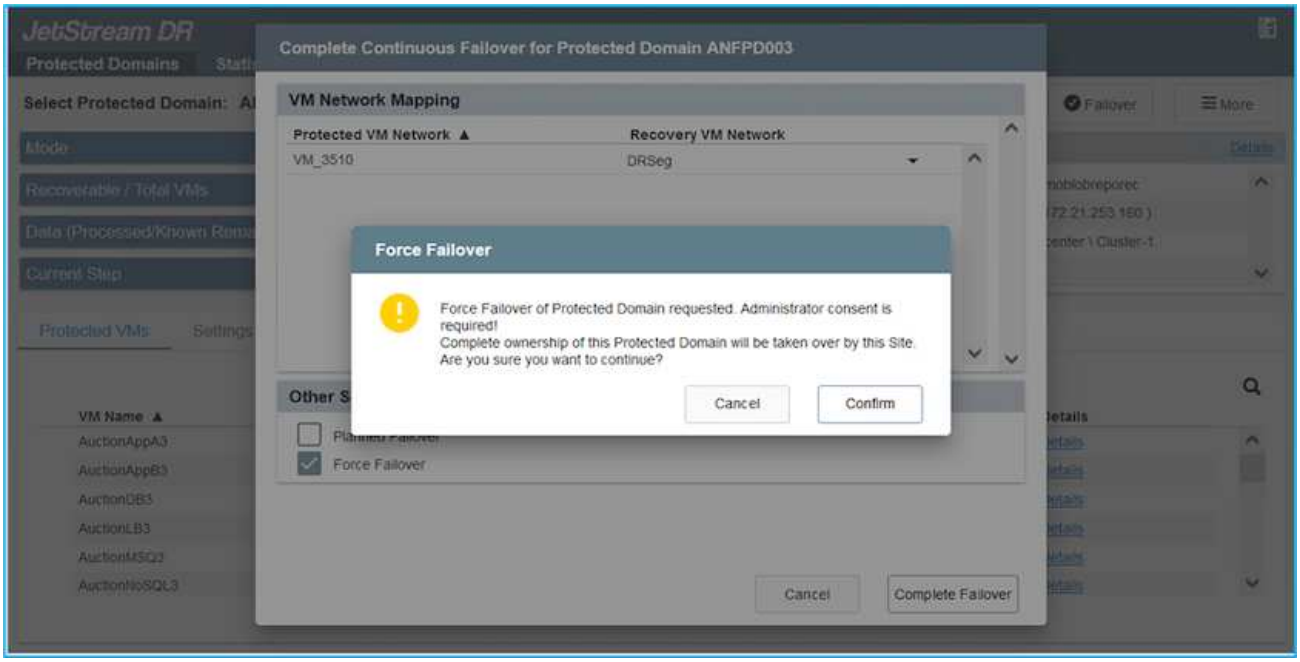
▼ 장애 조치**(Failover)**/장애 복구**(Failback)**를 수행하는 방법

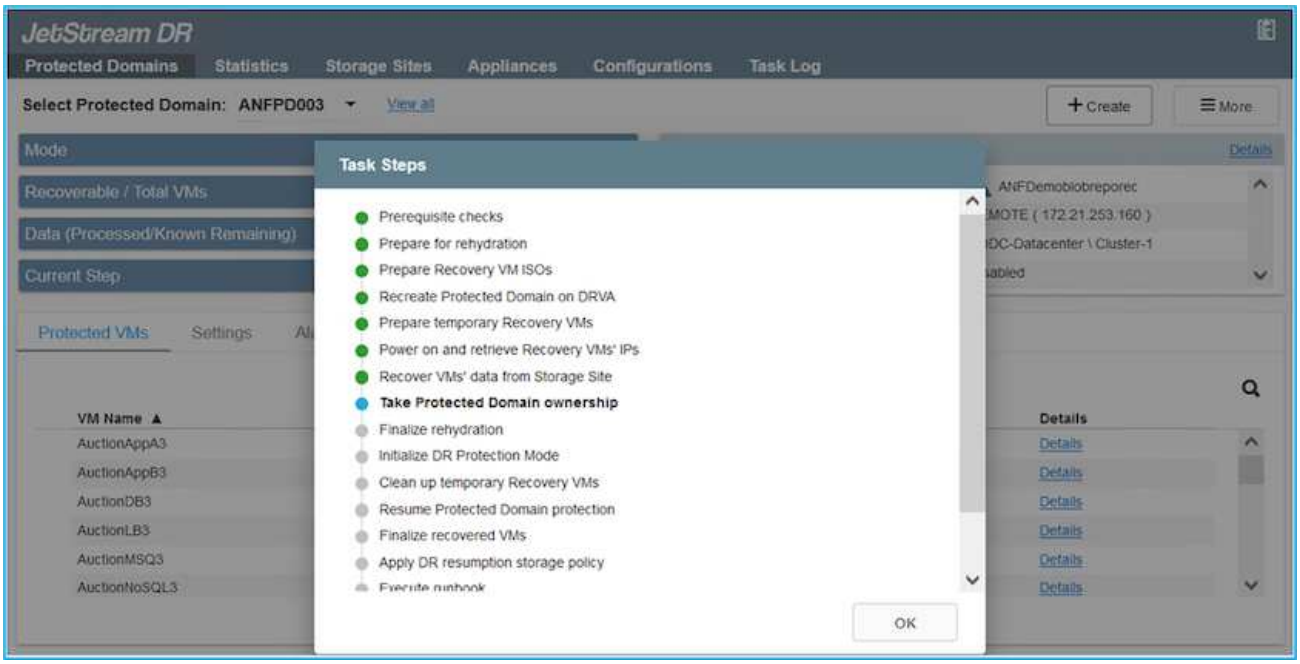
1. 온프레미스 환경의 보호된 클러스터에서 재해(부분적 또는 전체적 장애)가 발생한 후 장애 조치를 트리거합니다.

CPT는 Azure Blob Storage에서 AVS 클러스터 복구 사이트로 VM을 복구하는 장애 조치

계획을 실행하는 데 사용할 수 있습니다.

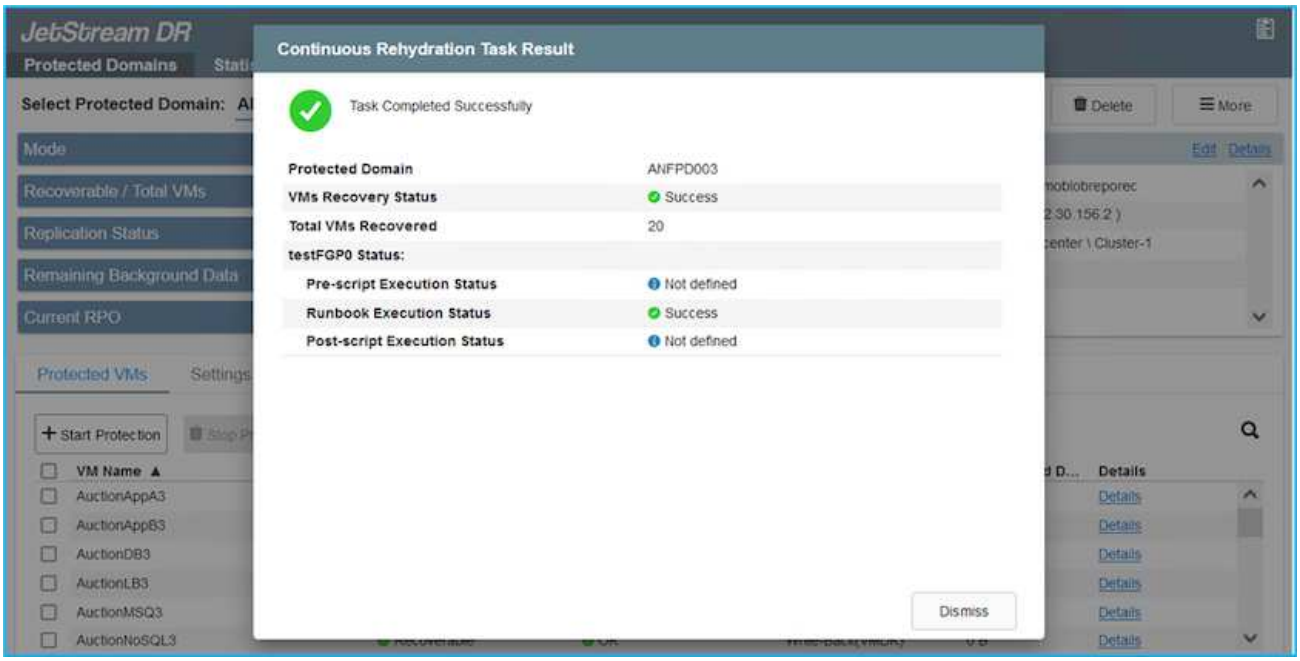
(지속적인 재수화 또는 표준 재수화의) 장애 조치(failover) 후 보호된 VM이 AVS에서 시작되면 보호가 자동으로 재개되고 JetStream DR은 Azure Blob Storage의 적절한/원래 컨테이너로 데이터를 계속 복제합니다.





작업 표시줄에는 장애 조치 활동의 진행 상황이 표시됩니다.

2. 작업이 완료되면 복구된 VM에 액세스하여 정상적으로 업무를 계속 진행합니다.

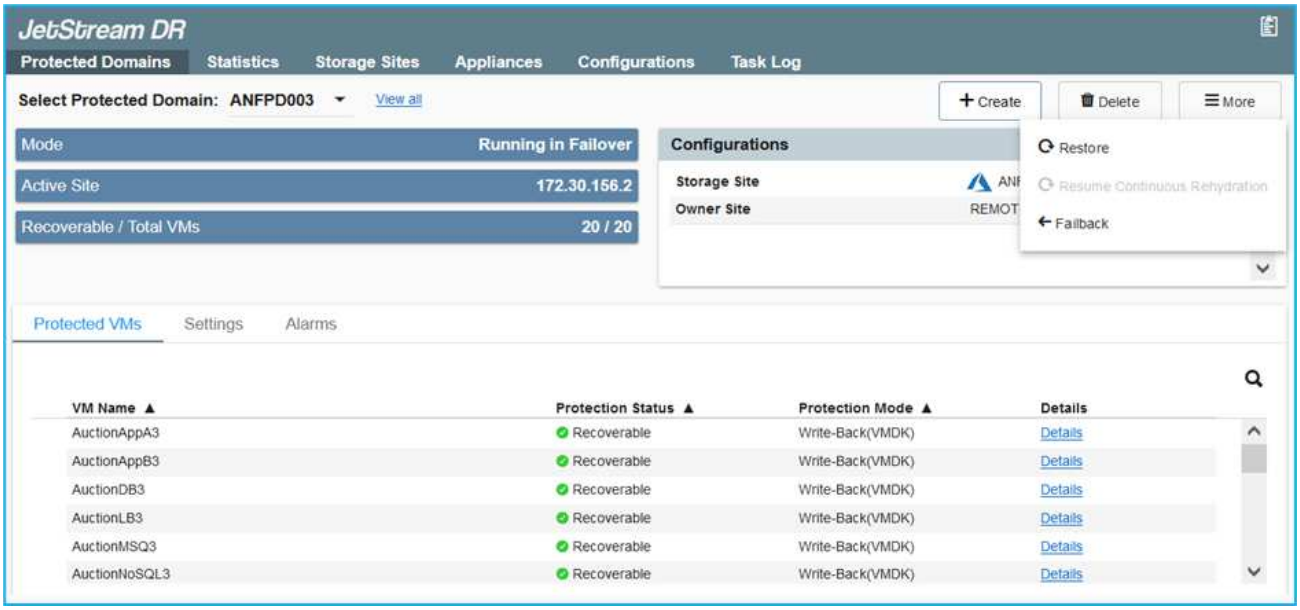


기본 사이트가 다시 가동되면 장애 복구를 수행할 수 있습니다. VM 보호가 재개되었으며 데이터 일관성을 확인해야 합니다.

3. 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.

> 참고사항: `recovery_utility_prepare_failback` Automation Toolkit에서 제공하는 스크립트를 사용하면 원래 보호된 사이트에서 오래된 VM, 도메인 정보 등을 정리하는 데 도움이 될 수 있습니다.

4. 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.

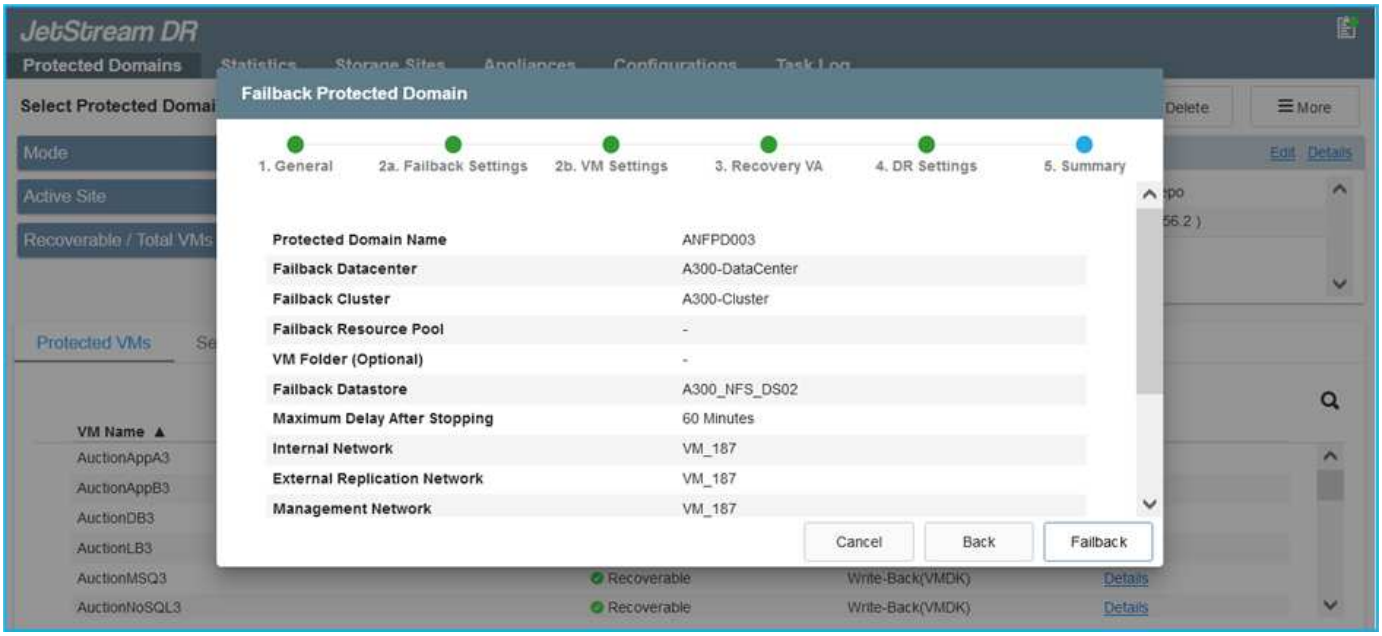
복구 사이트에서 VM을 일시 중지한 후 보호 사이트에서 다시 시작한 후의 최대 지연 시간을 지정합니다. 이 시간에는 장애 조치 VM을 중지한 후 복제를 완료하는 시간, 복구 사이트를 정리하는 시간, 보호된 사이트에서 VM을 다시 만드는 시간이 포함됩니다. NetApp 권장하는 값은 10분입니다.

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

랜섬웨어 복구

랜섬웨어로부터 복구하는 것은 힘든 일일 수 있습니다. 특히, IT 조직에서는 안전한 복귀 지점을 결정하기 어려울 수 있으며, 일단 결정한 후에는 복구된 워크로드가 재발하는 공격(잠복 맬웨어 또는 취약한 애플리케이션을 통한 공격)으로부터 안전하게 보호되는지 확인하는 방법도 어려울 수 있습니다.

AVS용 JetStream DR과 Azure NetApp Files 데이터 저장소를 함께 사용하면 조직이 사용 가능한 시점으로부터 복구할 수 있으므로 필요한 경우 작업 부하를 기능적이고 격리된 네트워크로 복구할 수 있어 이러한 문제를 해결할 수 있습니다. 복구를 통해 애플리케이션은 남북 트래픽에 노출되지 않은 상태에서도 서로 작동하고 통신할 수 있으므로 보안 팀은 법의학 조사 및 기타 필요한 수정 작업을 안전하게 수행할 수 있습니다.



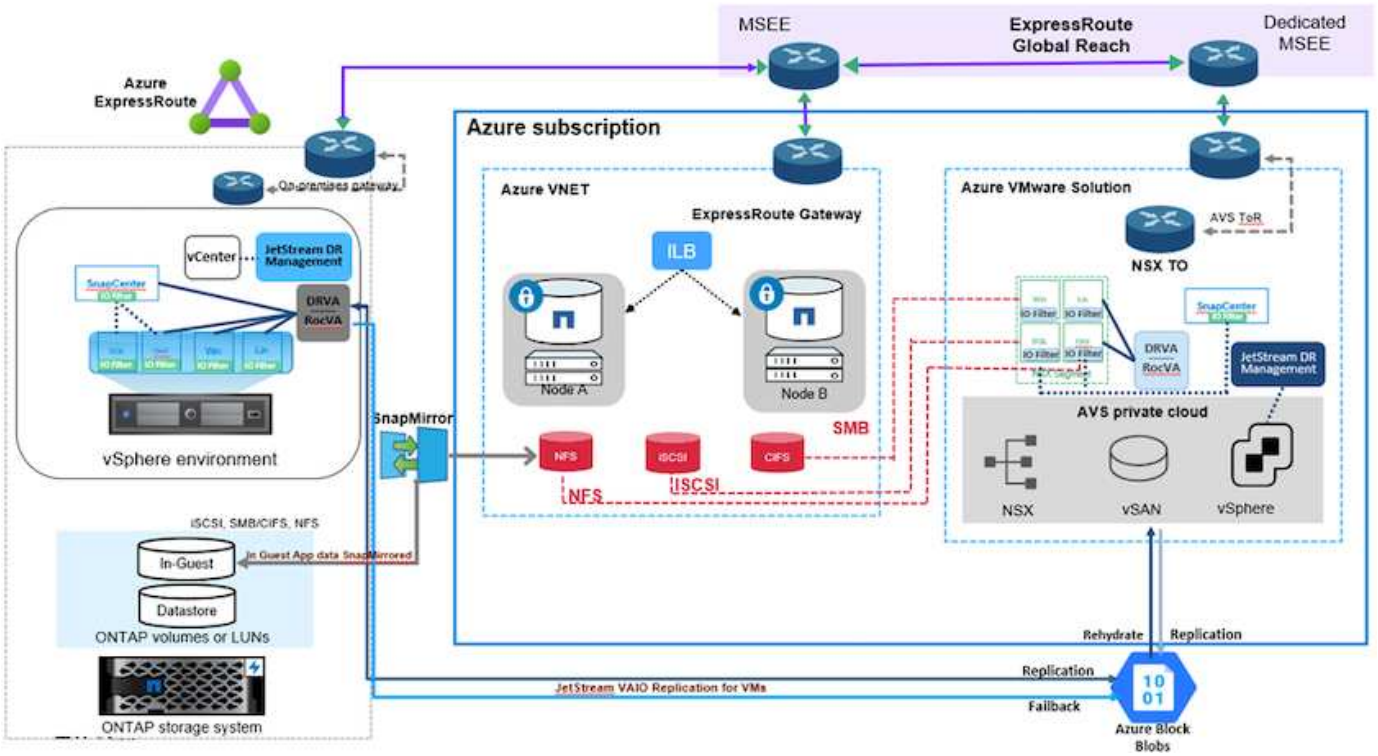
CVO 및 **AVS**(게스트 연결 스토리지)를 사용한 재해 복구

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

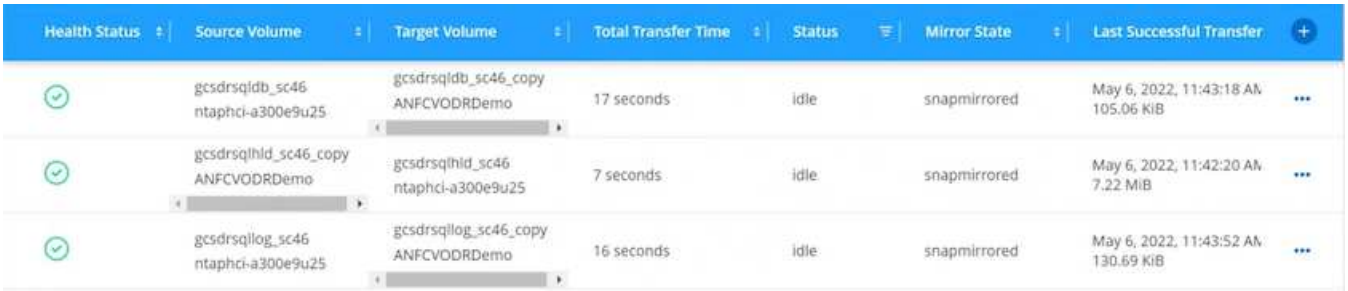
1. SnapCenter 사용하여 필요한 RPO 요구 사항을 충족하는 애플리케이션 데이터를 백업하세요.

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

▼ **Azure**에서 **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.

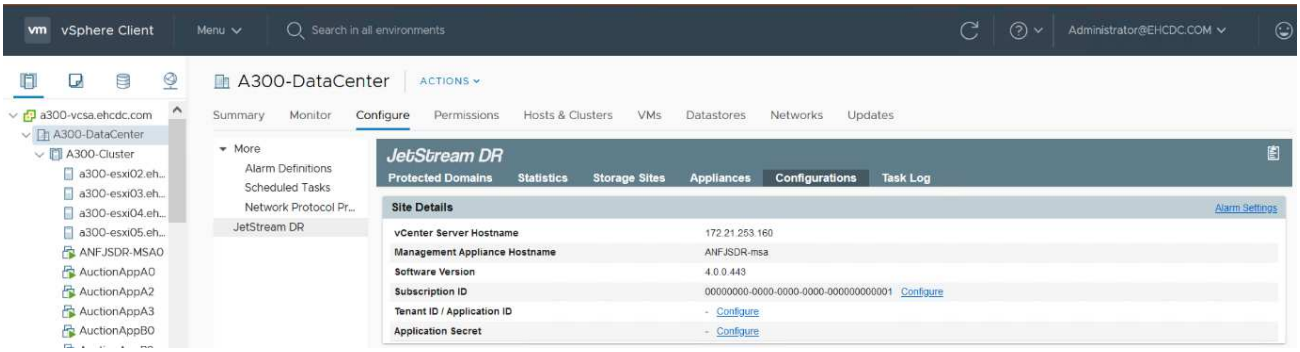
Cloud Volumes ONTAP 과 AVS가 올바르게 구성된 후 VAIO 메커니즘을 사용하고 SnapMirror 활용하여 애플리케이션 볼륨을 Cloud Volumes ONTAP에 복사하여 온프레미스 워크로드를 AVS(애플리케이션 VMDK가

있는 VM 및 게스트 스토리지가 있는 VM)로 복구하는 작업을 자동화하도록 Jetstream을 구성하기 시작 Cloud Volumes ONTAP.

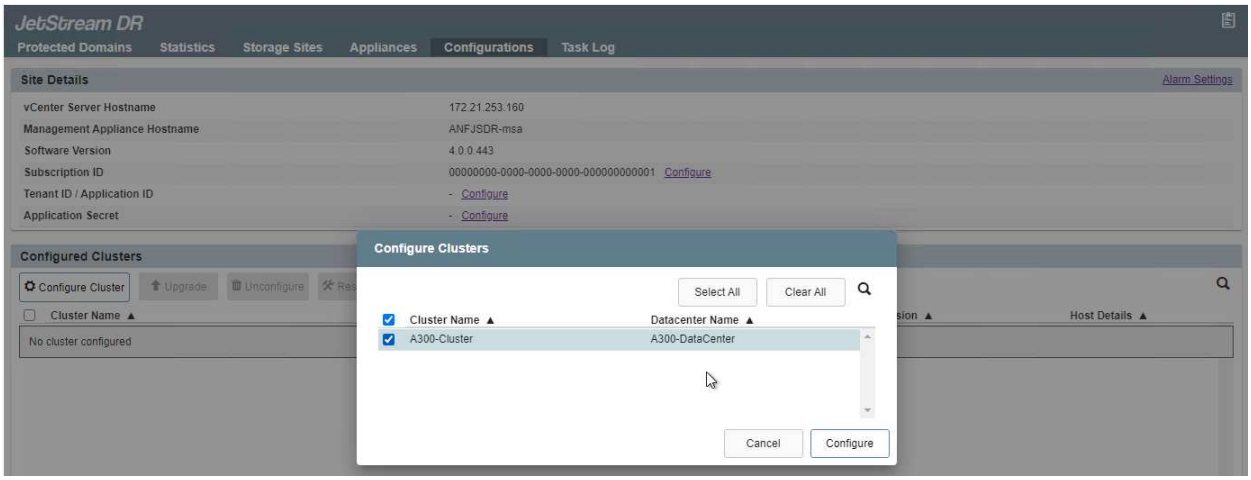
▼ 온프레미스 데이터 센터에 **JetStream DR** 설치

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.

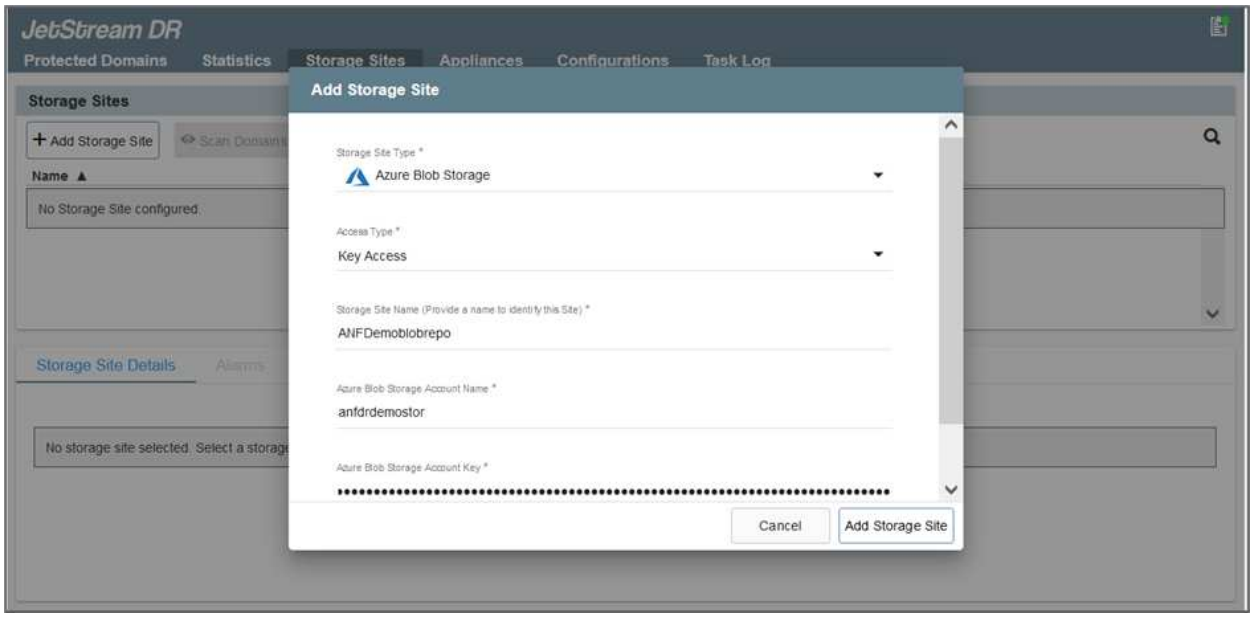
1. 필수 조건을 확인하세요.
2. 리소스 및 구성 권장 사항을 보려면 용량 계획 도구를 실행하세요.
3. 지정된 클러스터의 각 vSphere 호스트에 JetStream DR MSA를 배포합니다.
4. 브라우저에서 DNS 이름을 사용하여 MSA를 시작합니다.
5. MSA에 vCenter 서버를 등록합니다.
6. JetStream DR MSA가 배포되고 vCenter Server가 등록된 후 vSphere Web Client를 사용하여 JetStream DR 플러그인으로 이동합니다. 데이터 센터 > 구성 > JetStream DR로 이동하여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



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

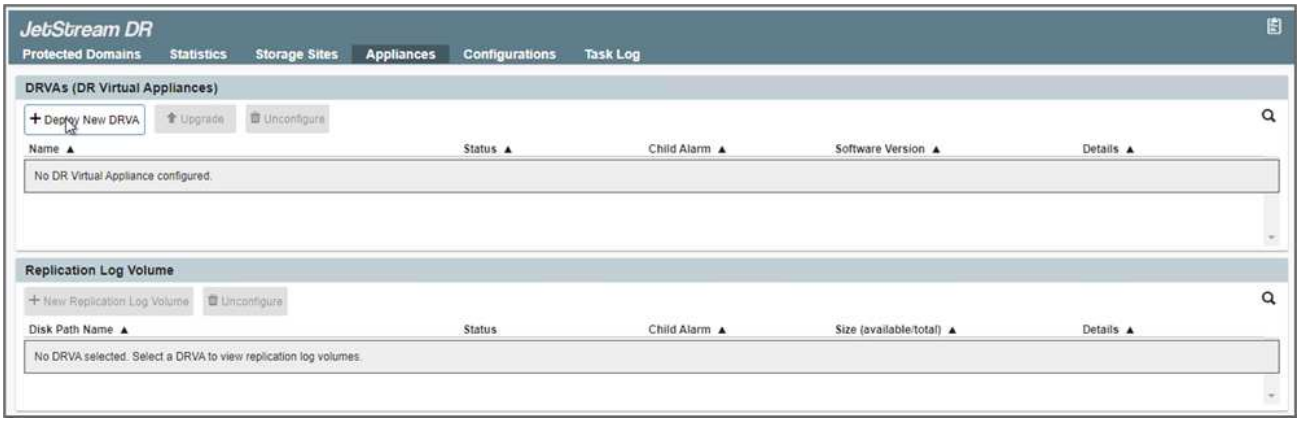


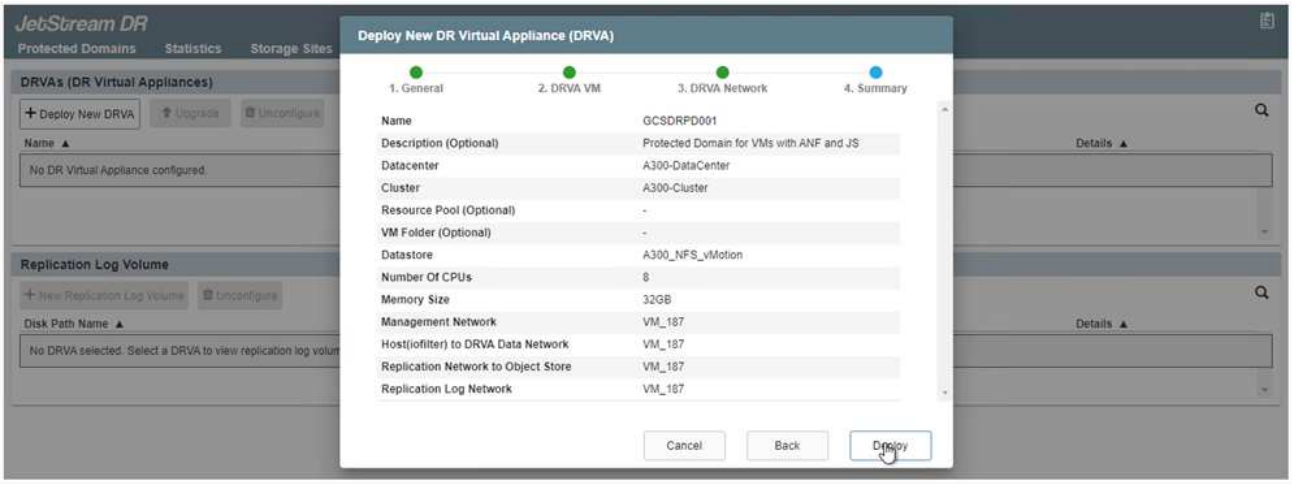
   b. 복구 사이트에 있는 Azure Blob 저장소를 추가합니다.



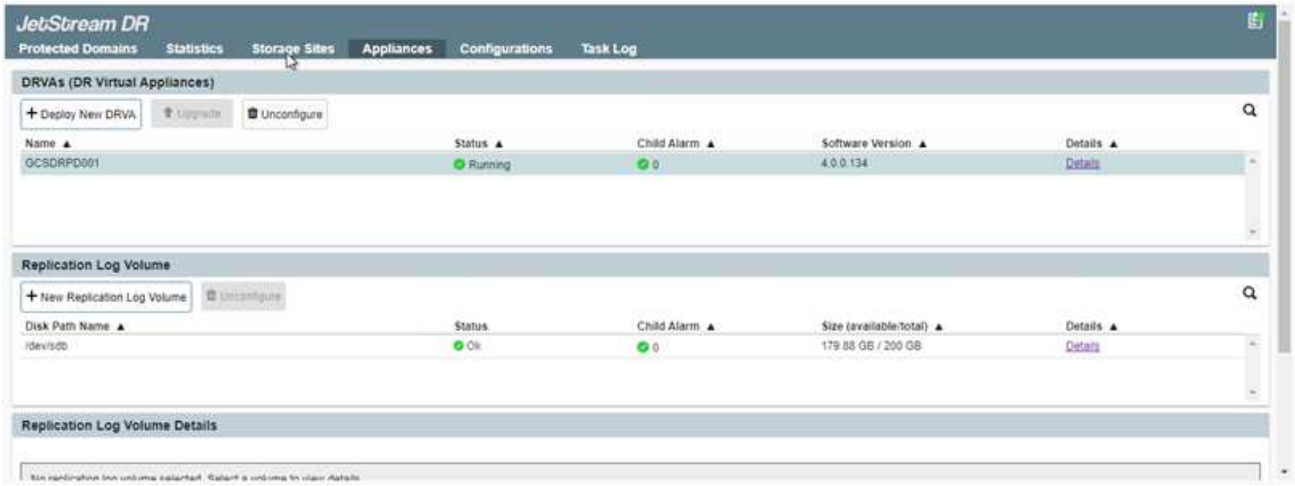
8. 어플라이언스 탭에서 필요한 수의 DR 가상 어플라이언스(DRVA)를 배포합니다.

   용량 계획 도구를 사용하여 필요한 DRVA 수를 추정합니다.

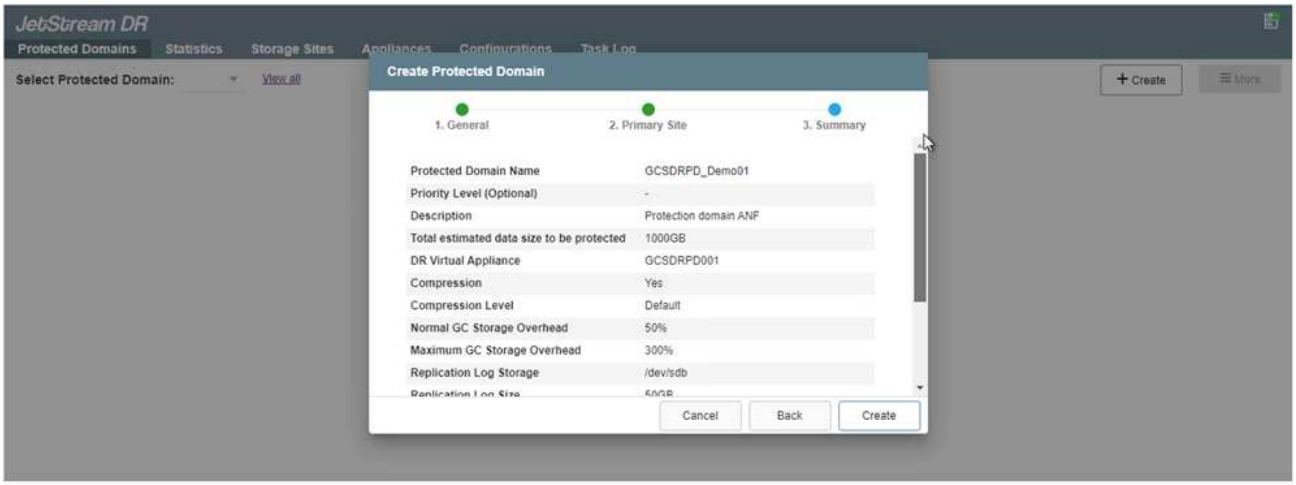


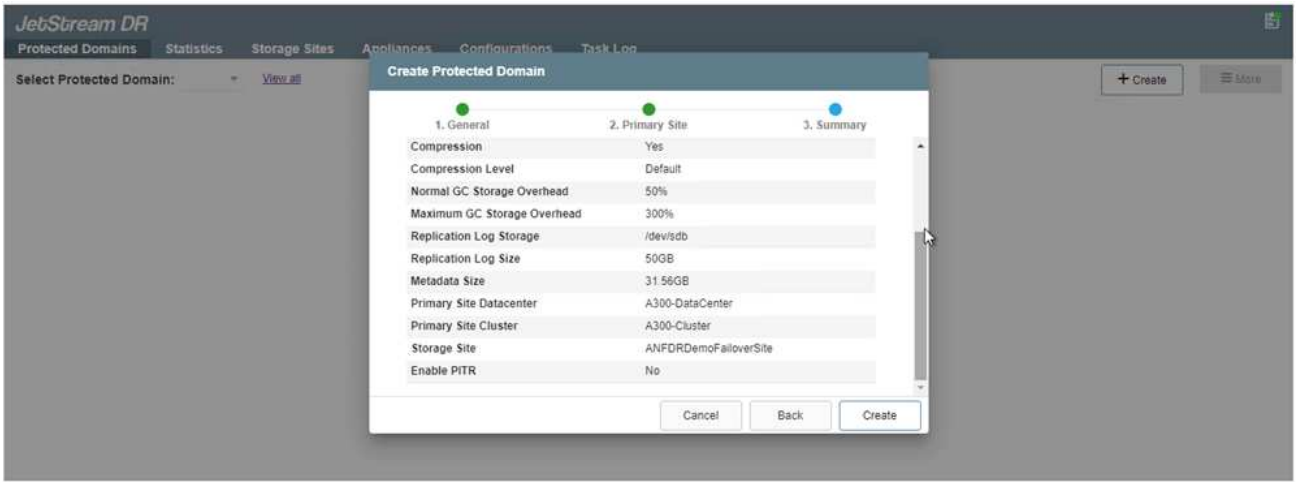


9. 사용 가능한 데이터 저장소나 독립적인 공유 iSCSI 스토리지 풀의 VMDK를 사용하여 각 DRVA에 대한 복제 로그 볼륨을 생성합니다.



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.

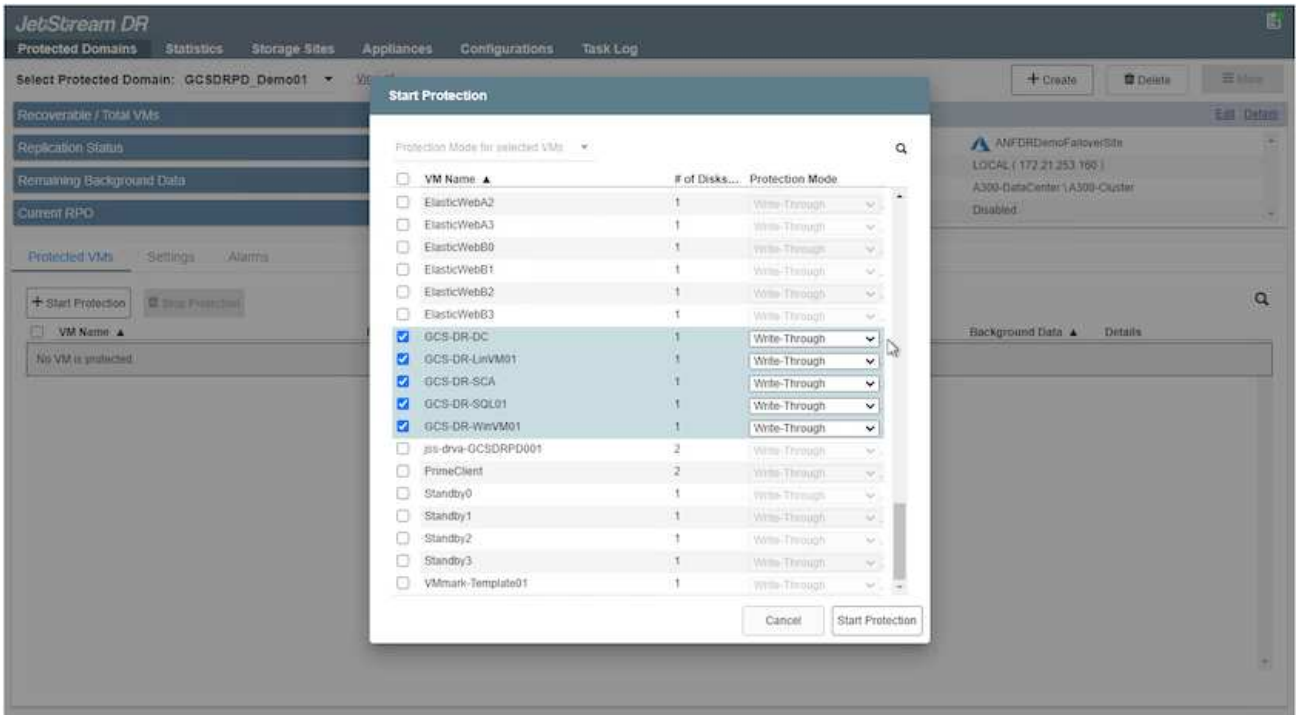




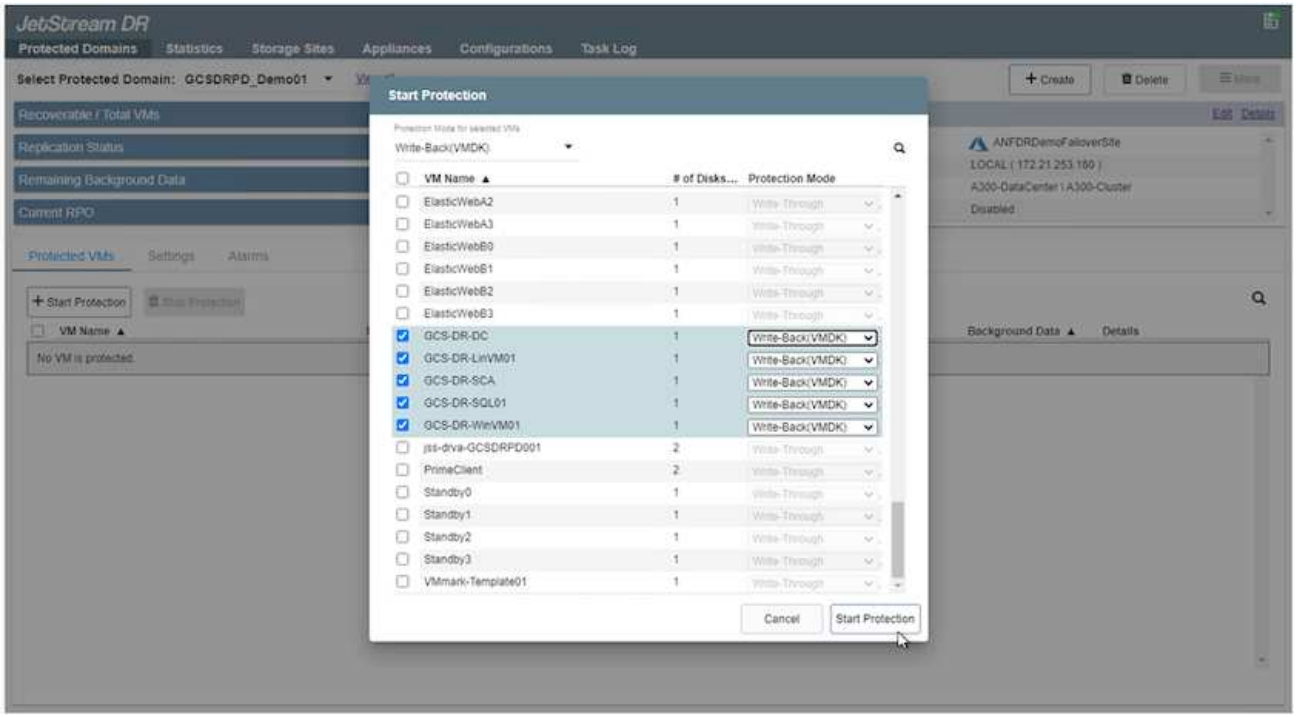
11. 보호할 VM을 선택하고 종속성에 따라 VM을 애플리케이션 그룹으로 그룹화합니다. 애플리케이션 정의를 사용하면 VM 세트를 부팅 순서, 부팅 지연, 복구 시 실행할 수 있는 선택적 애플리케이션 유효성 검사 등을 포함하는 논리적 그룹으로 그룹화할 수 있습니다.

보호된 도메인의 모든 VM에 동일한 보호 모드가 사용되는지 확인하세요.

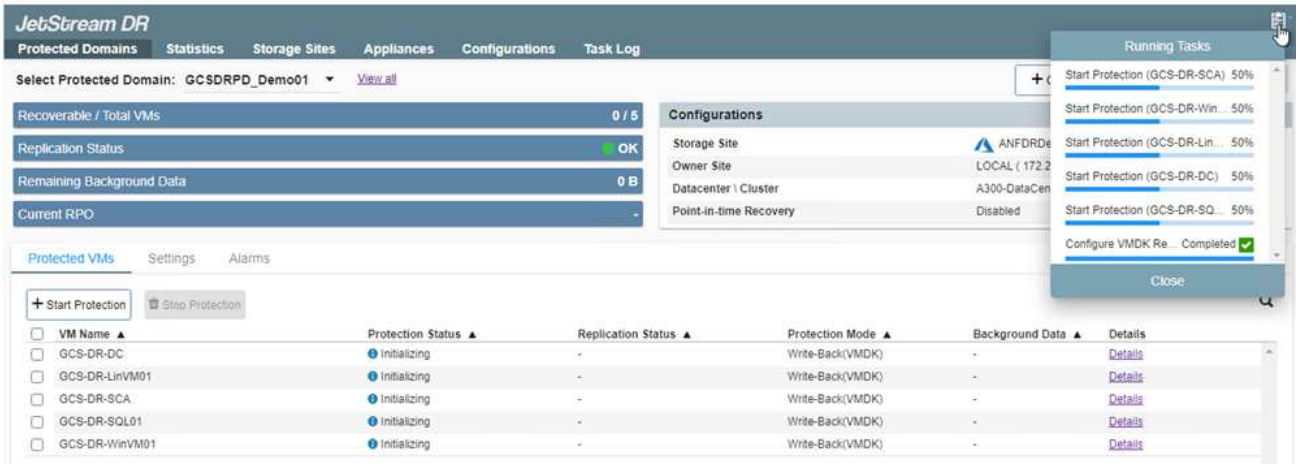
Write-Back(VMDK) 모드는 더 높은 성능을 제공합니다.



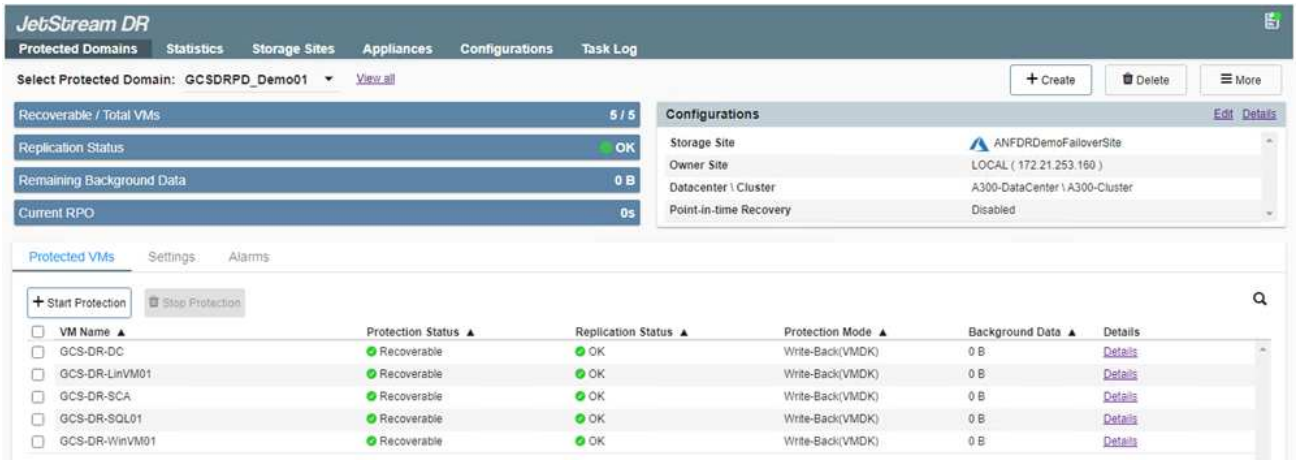
12. 복제 로그 볼륨이 고성능 스토리지에 배치되었는지 확인하세요.



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.

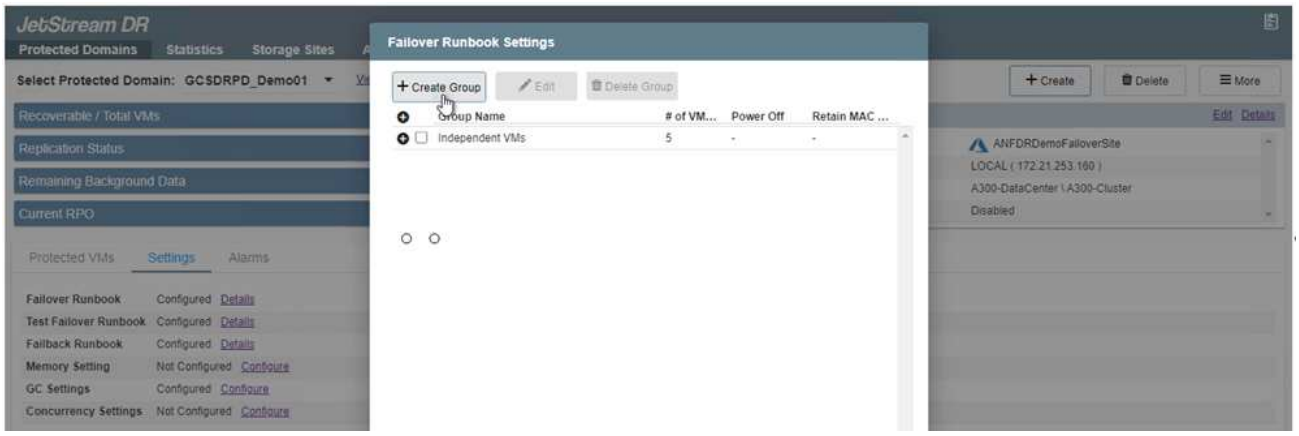
15. 설정을 클릭한 다음 런북 구성 링크를 클릭하여 런북 그룹을 구성합니다.



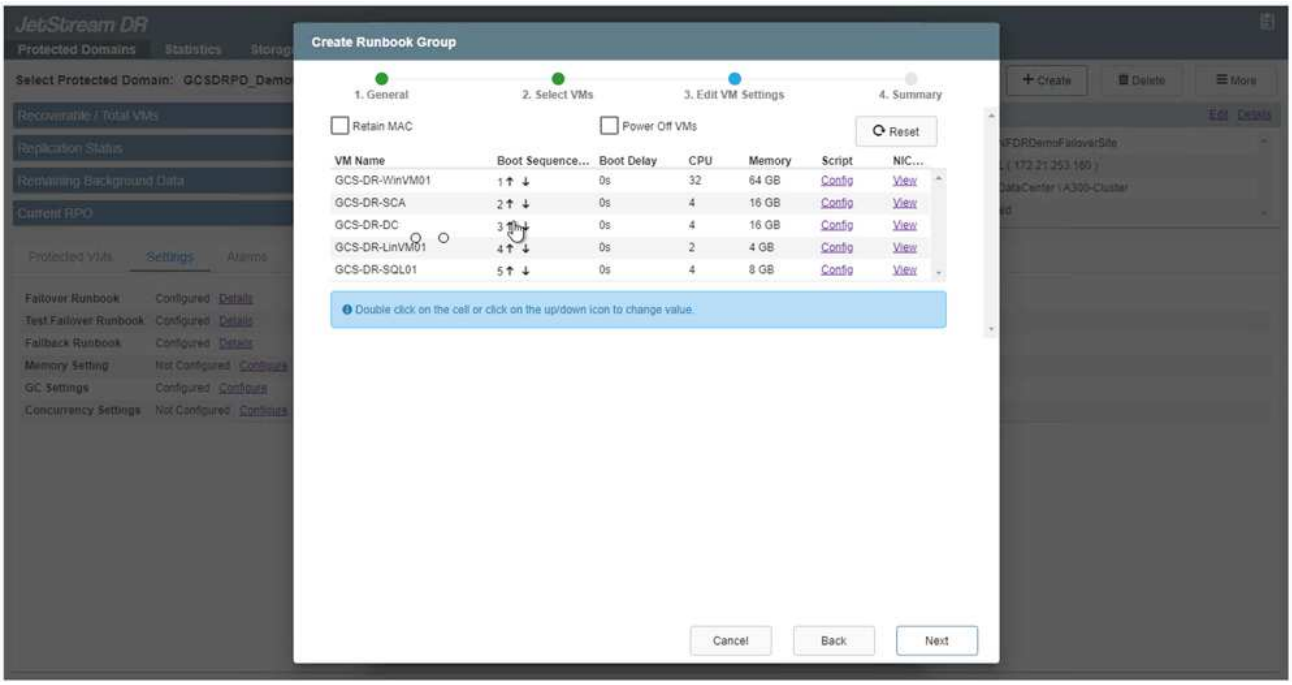
16. 그룹 만들기 버튼을 클릭하여 새로운 런북 그룹을 만듭니다.

필요한 경우 화면 하단에서 사용자 지정 사전 스크립트와 사후 스크립트를 적용하여 런북 그룹의

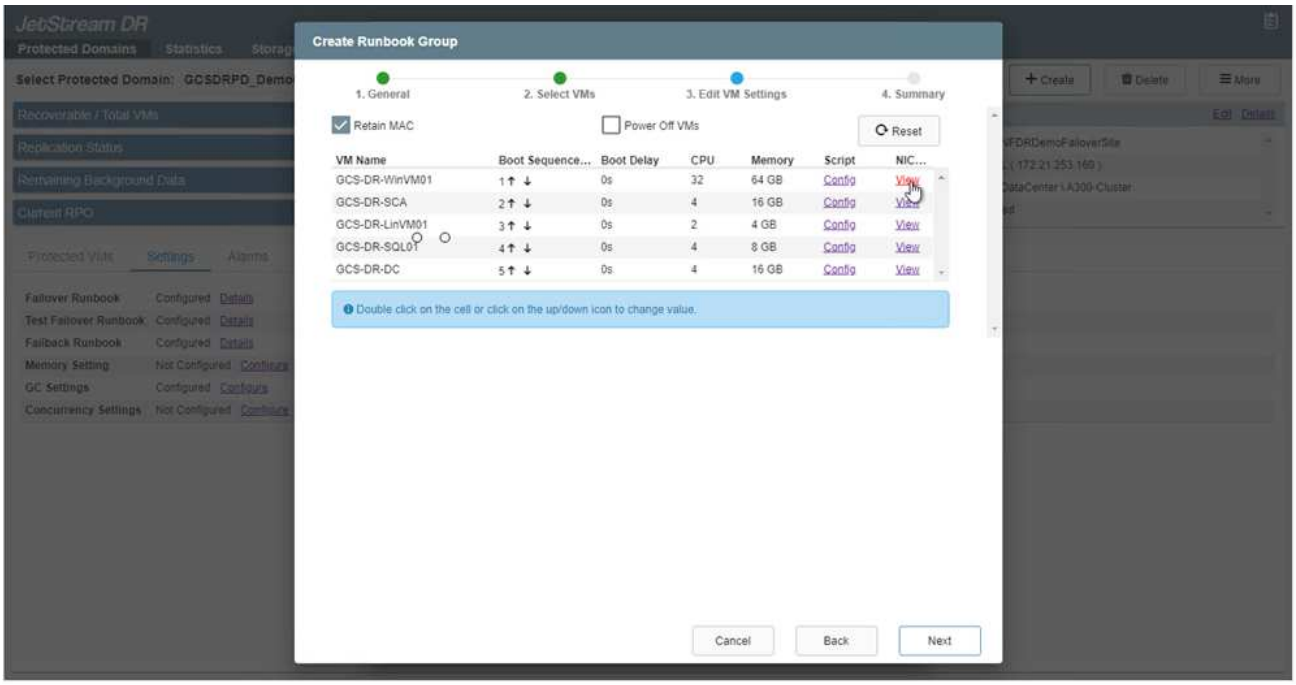
작업 전과 후에 자동으로 실행합니다. Runbook 스크립트가 관리 서버에 있는지 확인하세요.



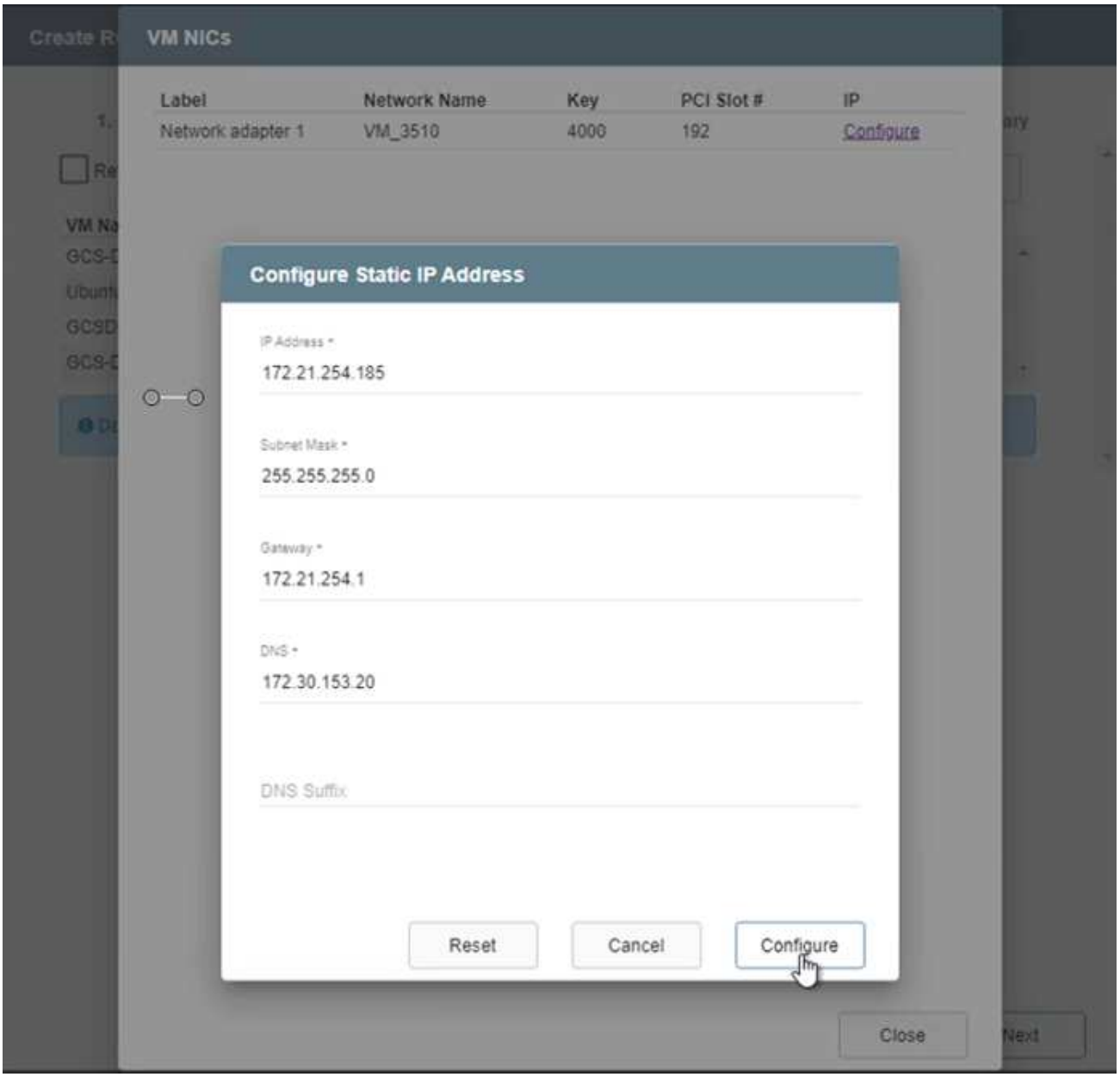
17. 필요에 따라 VM 설정을 편집합니다. 부팅 순서, 부팅 지연(초 단위), CPU 수, 할당할 메모리 양 등 VM 복구에 필요한 매개변수를 지정합니다. 위쪽 또는 아래쪽 화살표를 클릭하여 VM의 부팅 순서를 변경합니다. MAC을 유지하기 위한 옵션도 제공됩니다.

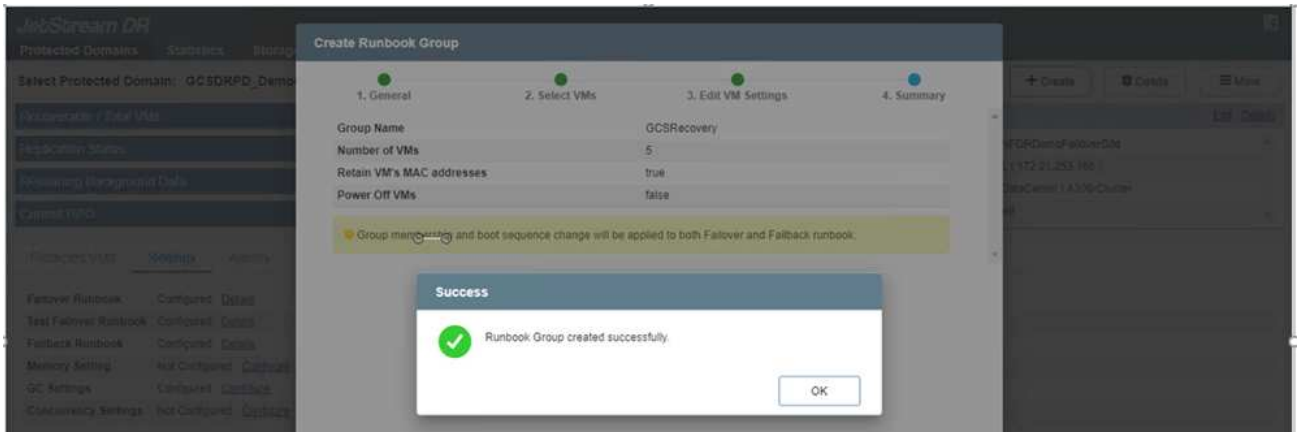


18. 고정 IP 주소는 그룹의 개별 VM에 대해 수동으로 구성할 수 있습니다. VM의 NIC 보기 링크를 클릭하여 IP 주소 설정을 수동으로 구성합니다.



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.

▼ 프라이빗 클라우드에 **AVS**용 **JetStream DR** 설치

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.

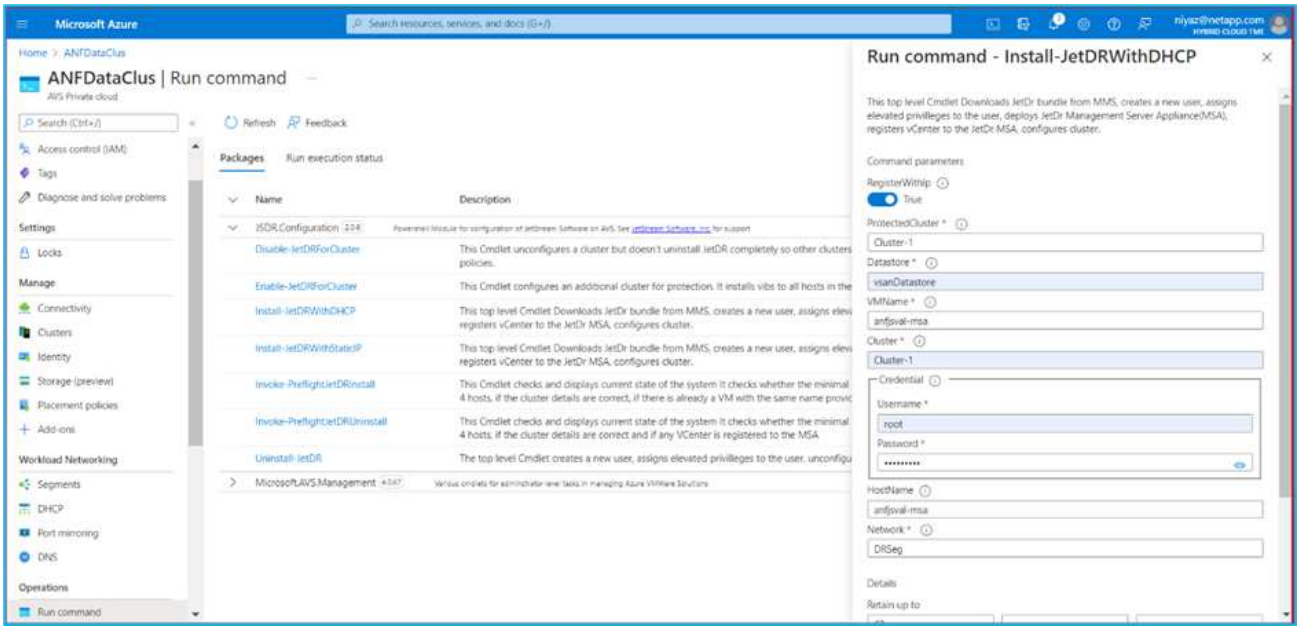
ⓘ 세그먼트 생성을 포함한 네트워크 구성은 온프레미스 요구 사항에 맞게 AVS 클러스터에서 구성되어야 합니다.

ⓘ 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.

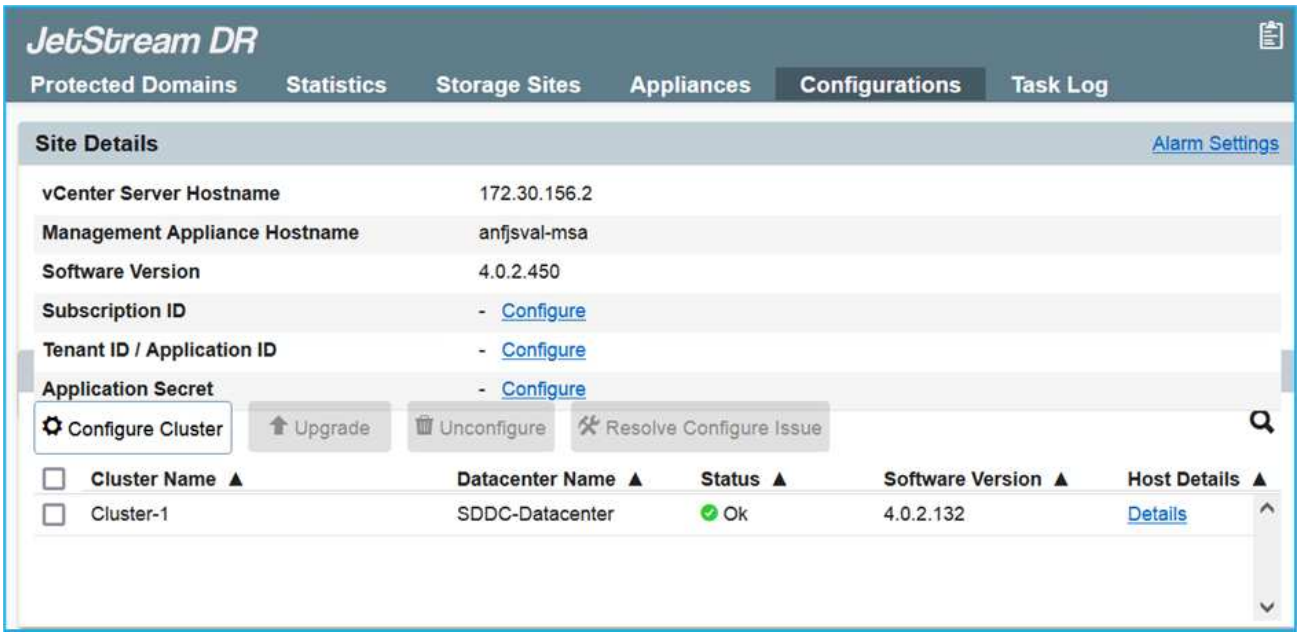
1. Azure VMware Solution 프라이빗 클라우드에 AVS용 JetStream DR을 설치하려면 실행 명령을 사용하세요. Azure Portal에서 Azure VMware 솔루션으로 이동하여 프라이빗 클라우드를 선택하고 명령 실행 > 패키지 > JSDR.Configuration을 선택합니다.

ⓘ 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.

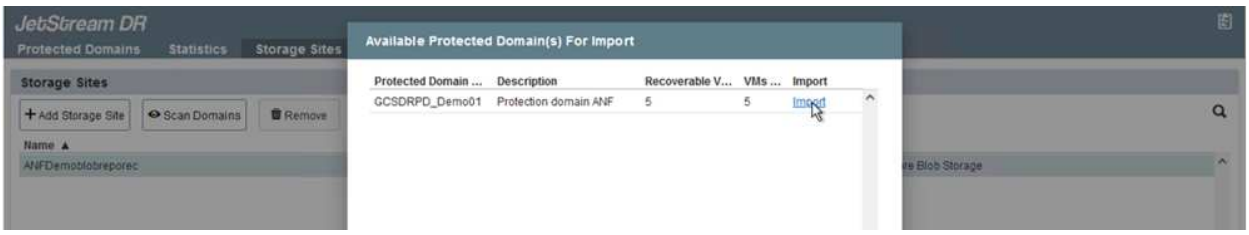
다음 스크린샷은 DHCP 기반 IP 주소를 사용하여 설치하는 방법을 보여줍니다.



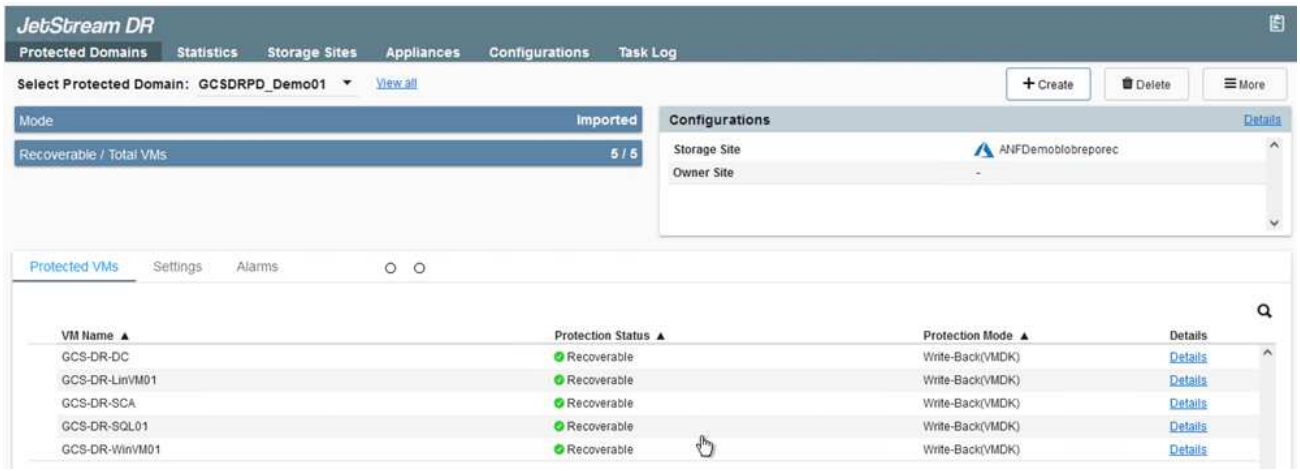
2. AVS용 JetStream DR 설치가 완료되면 브라우저를 새로 고칩니다. JetStream DR UI에 액세스하려면 SDDC 데이터센터 > 구성 > JetStream DR로 이동하세요.



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.



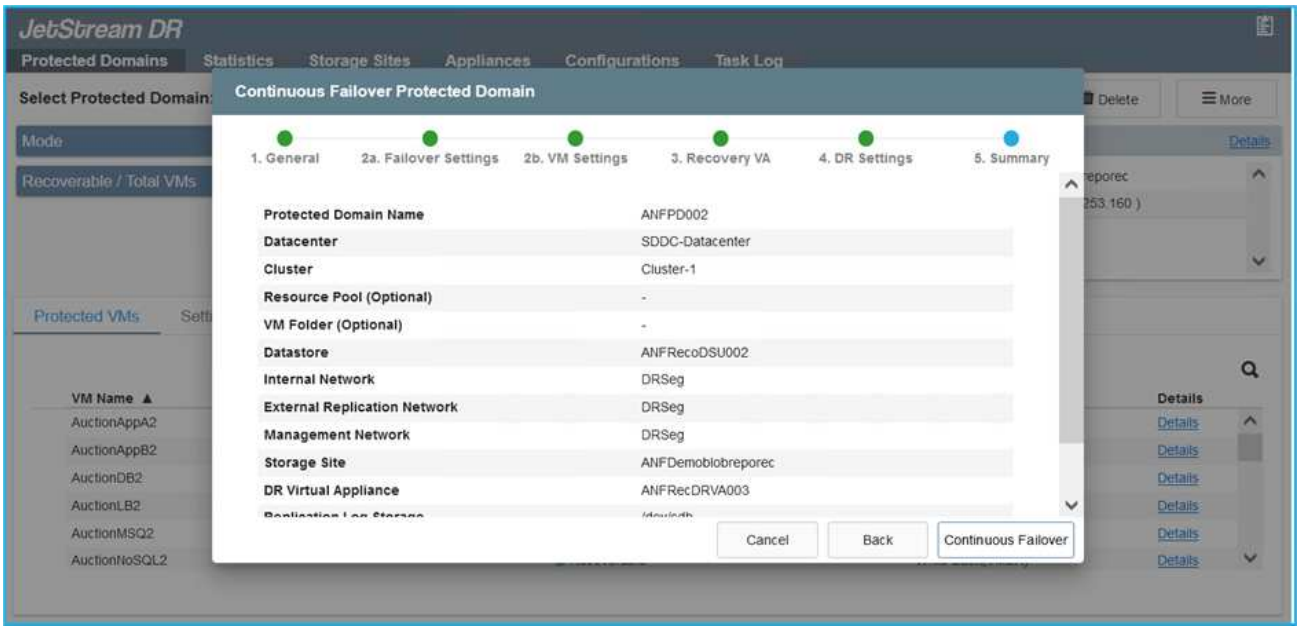
4. 도메인을 복구를 위해 가져왔습니다. 보호된 도메인 탭으로 이동하여 원하는 도메인이 선택되었는지 확인하거나 보호된 도메인 선택 메뉴에서 원하는 도메인을 선택합니다. 보호된 도메인에서 복구 가능한 VM 목록이 표시됩니다.



5. 보호된 도메인을 가져온 후 DRVA 어플라이언스를 배포합니다.

이러한 단계는 CPT에서 만든 계획을 사용하여 자동화할 수도 있습니다.

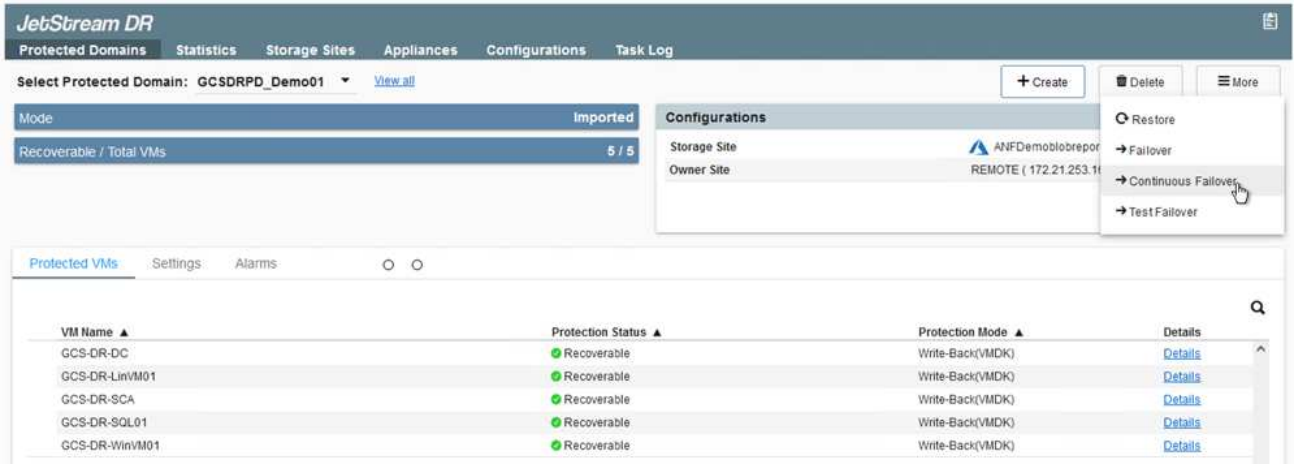
6. 사용 가능한 vSAN 또는 ANF 데이터 저장소를 사용하여 복제 로그 볼륨을 생성합니다.
7. 보호된 도메인을 가져오고 VM 배치에 ANF 데이터 저장소를 사용하도록 복구 VA를 구성합니다.



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.

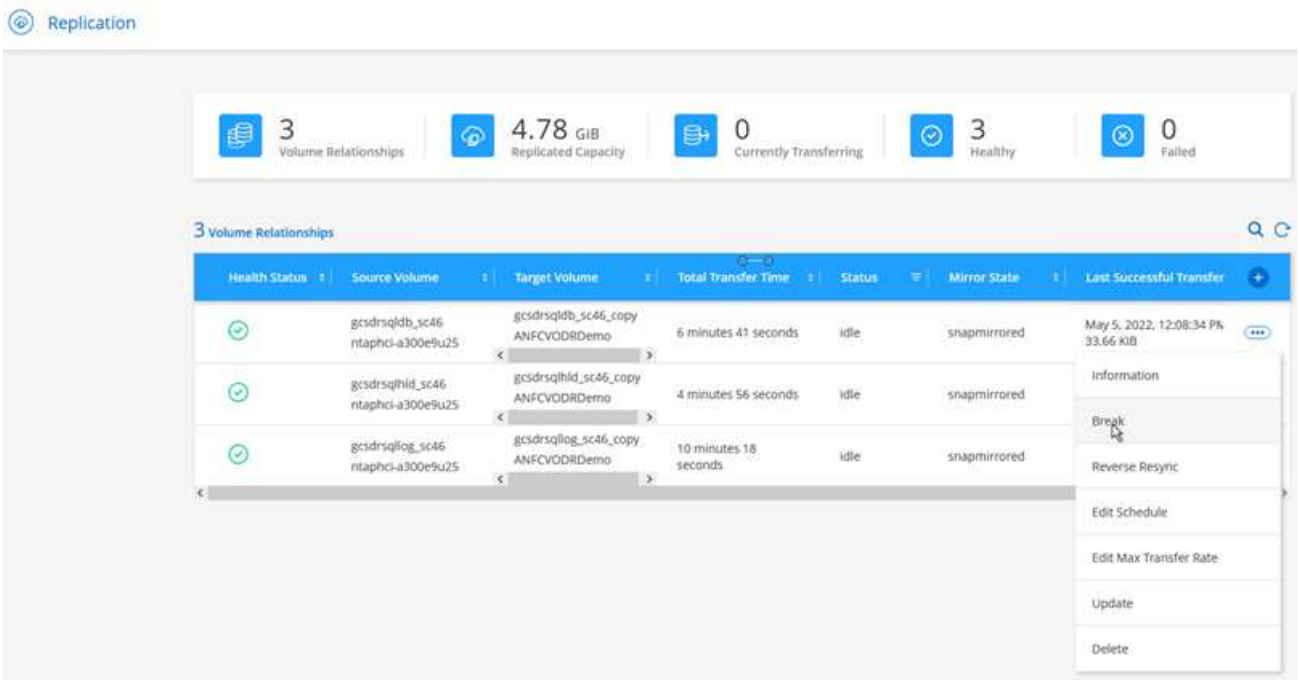
연속 장애 조치와 장애 조치 모드는 구성을 수행하는 시점에 따라 다르지만 두 장애 조치 모드는 모두 동일한 단계를 사용하여 구성됩니다. 재해 발생 시 대응하기 위해 장애 조치 단계가 함께 구성되고 수행됩니다. 지속적인 장애 조치는 언제든지 구성될 수 있으며, 정상적인 시스템 작동 중에 백그라운드에서 실행되도록 허용될 수 있습니다. 재해가 발생한 후에는 지속적인 장애 조치가 완료되어 보호된 VM의 소유권이 즉시 복구 사이트로 이전됩니다(RTO가 거의 0에 가까움).

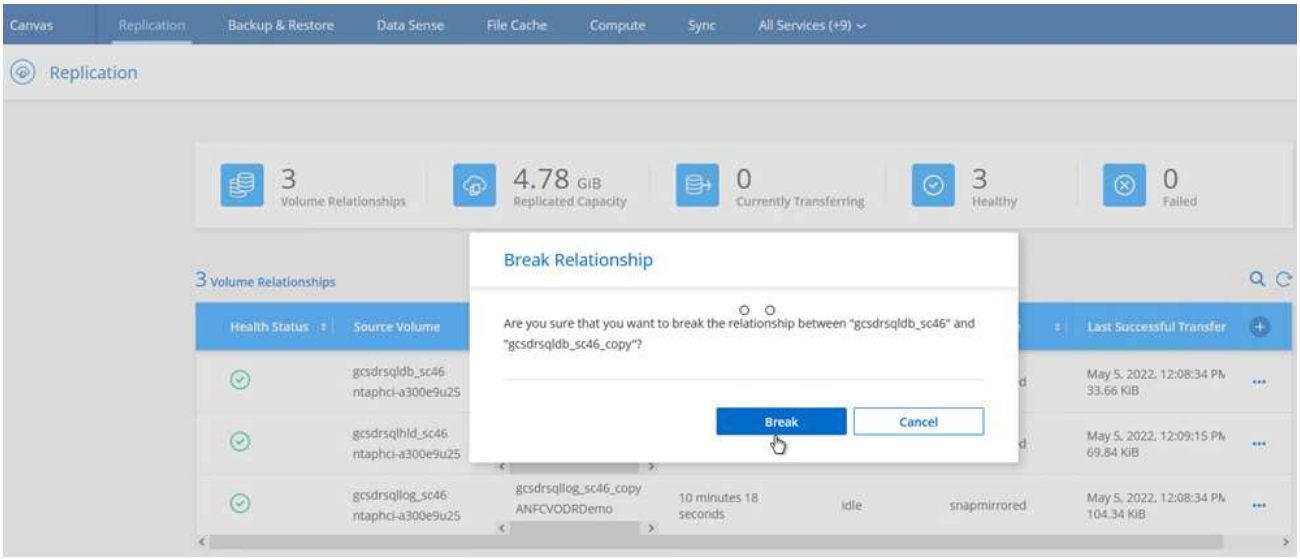


지속적인 장애 조치 프로세스가 시작되고, UI에서 진행 상황을 모니터링할 수 있습니다. 현재 단계 섹션의 파란색 아이콘을 클릭하면 장애 조치 프로세스의 현재 단계에 대한 세부 정보를 보여주는 팝업 창이 나타납니다.

▼ 장애 조치 및 장애 복구

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.

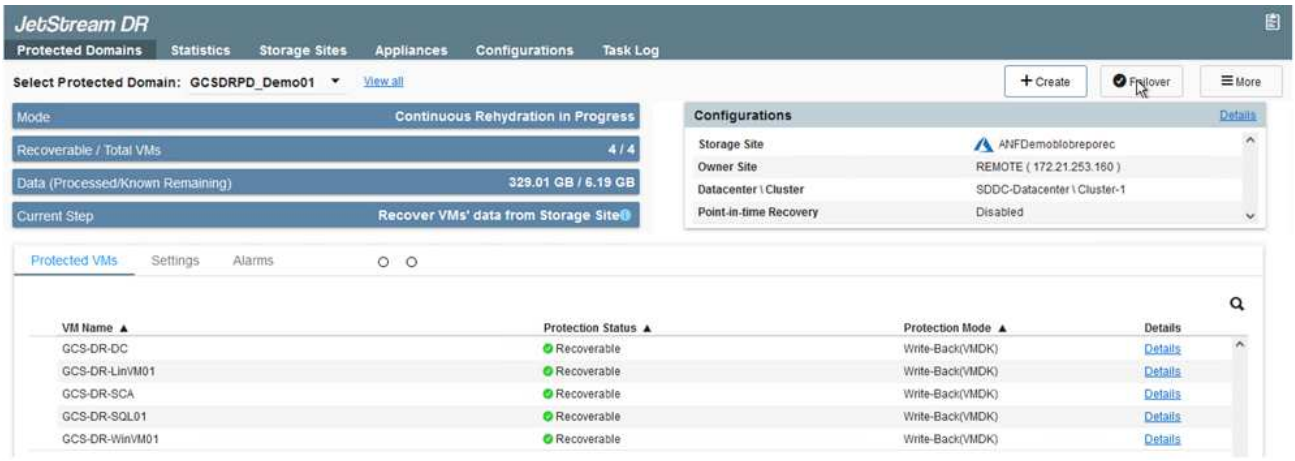


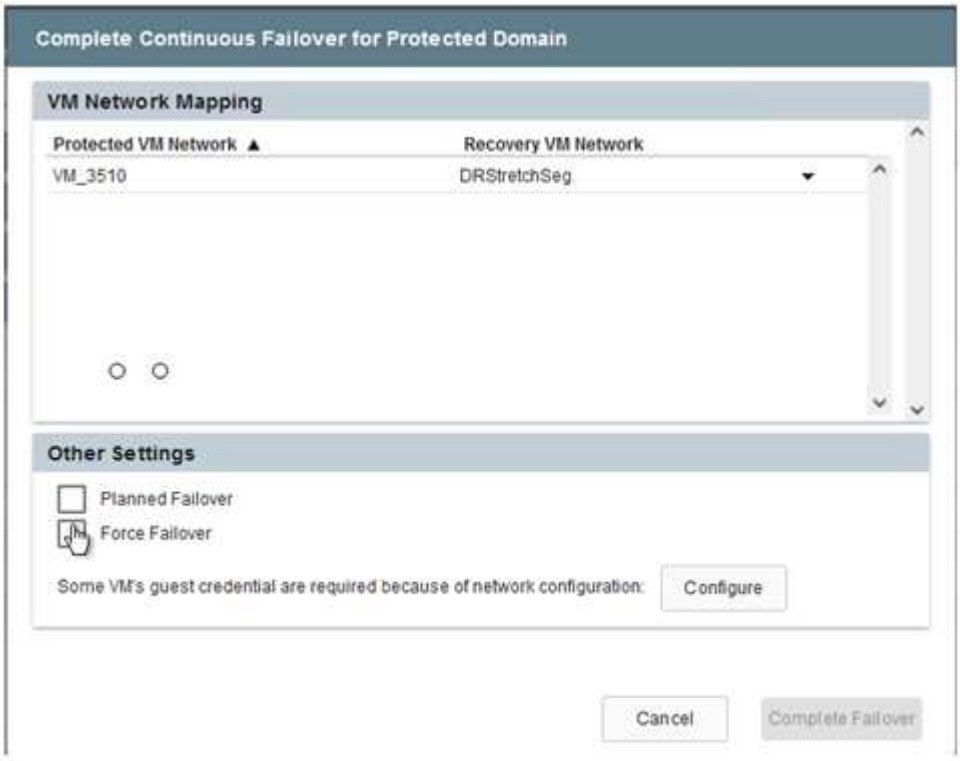


이 단계는 복구 프로세스를 용이하게 하기 위해 쉽게 자동화될 수 있습니다.

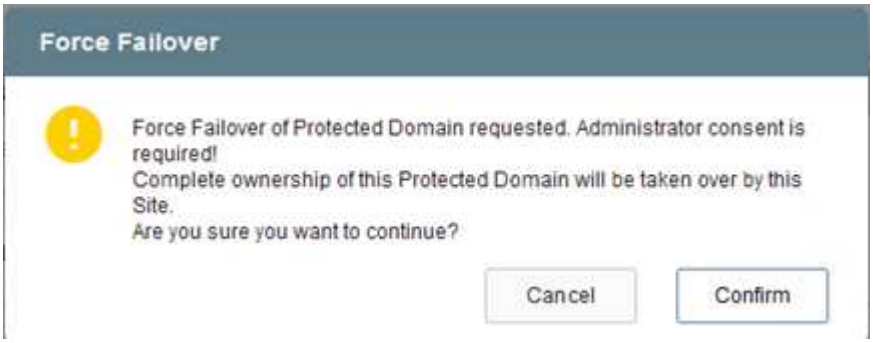
2. AVS SDDC(대상 측)에서 Jetstream UI에 액세스하고 장애 조치 옵션을 트리거하여 장애 조치를 완료합니다. 작업 표시줄에는 장애 조치 활동의 진행 상황이 표시됩니다.

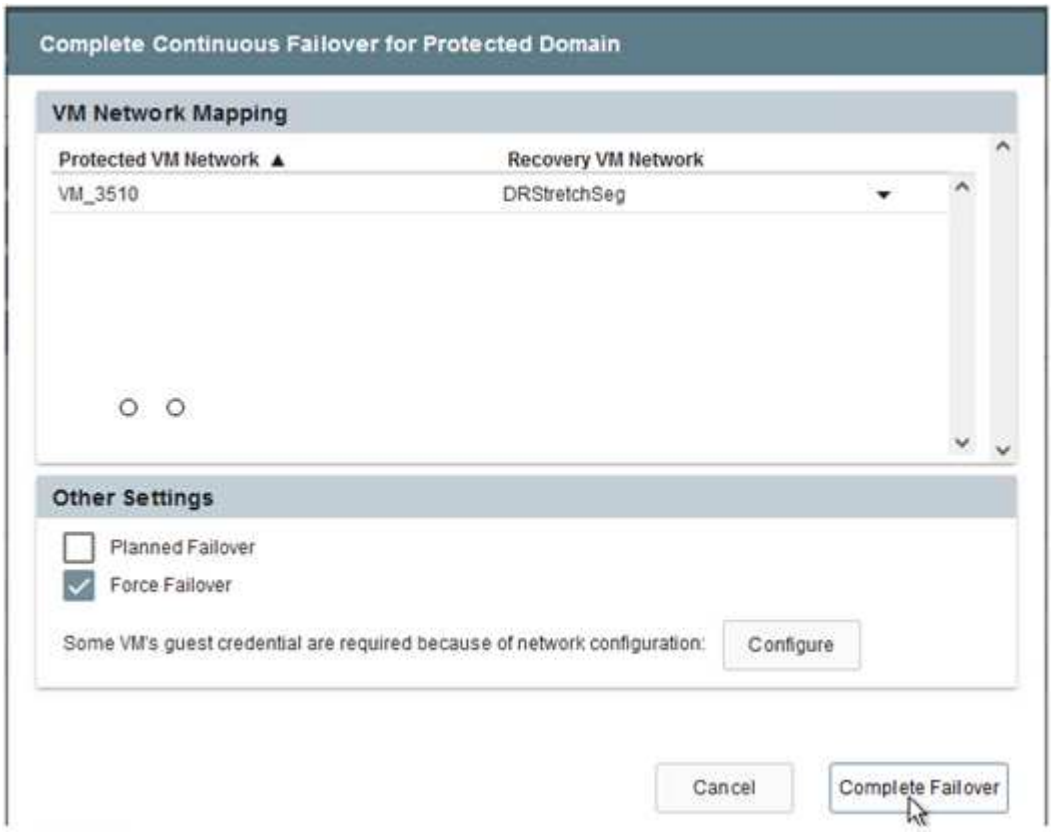
   장애 조치를 완료할 때 나타나는 대화 상자에서 장애 조치 작업을 계획된 대로 지정하거나 강제로 수행된 것으로 가정할 수 있습니다.





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





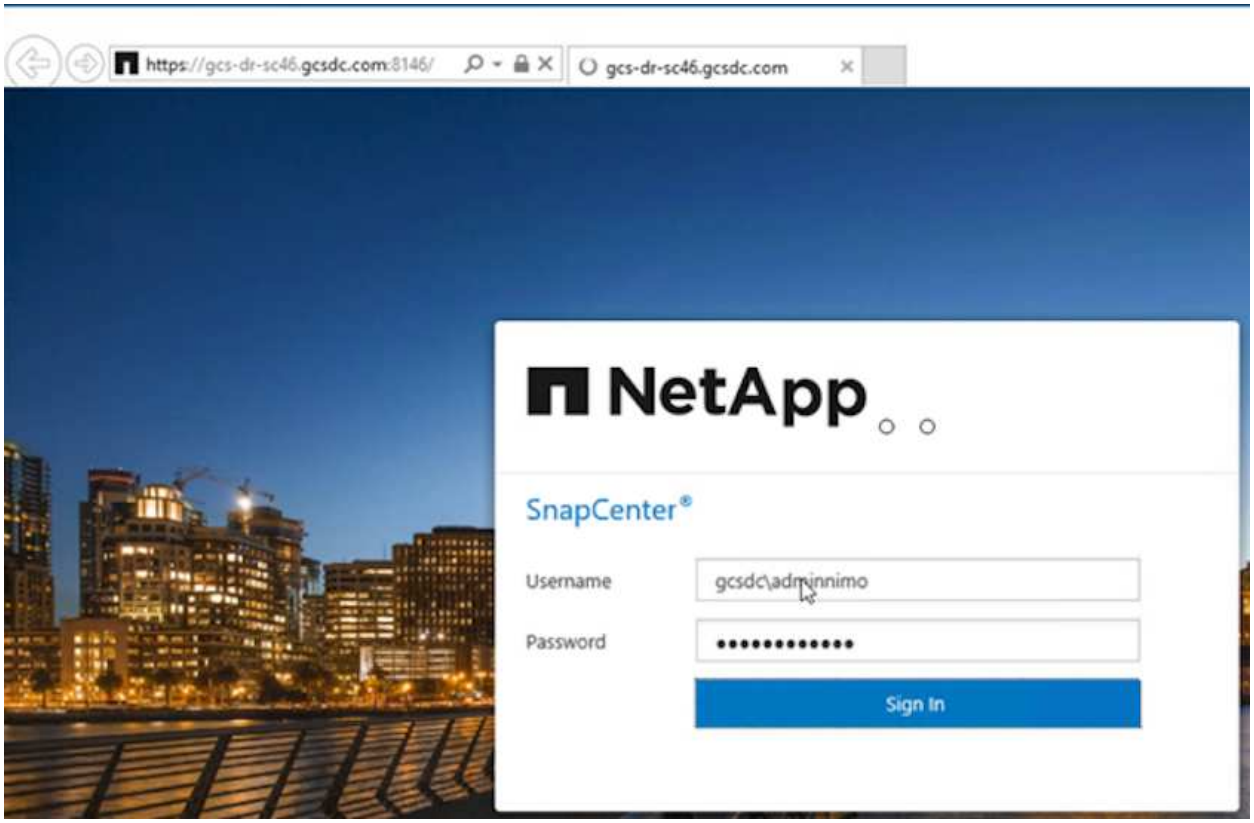
3. 지속적인 장애 조치가 완료되면 작업 완료를 확인하는 메시지가 나타납니다. 작업이 완료되면 복구된 VM에 액세스하여 ISCSI 또는 NFS 세션을 구성합니다.

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.

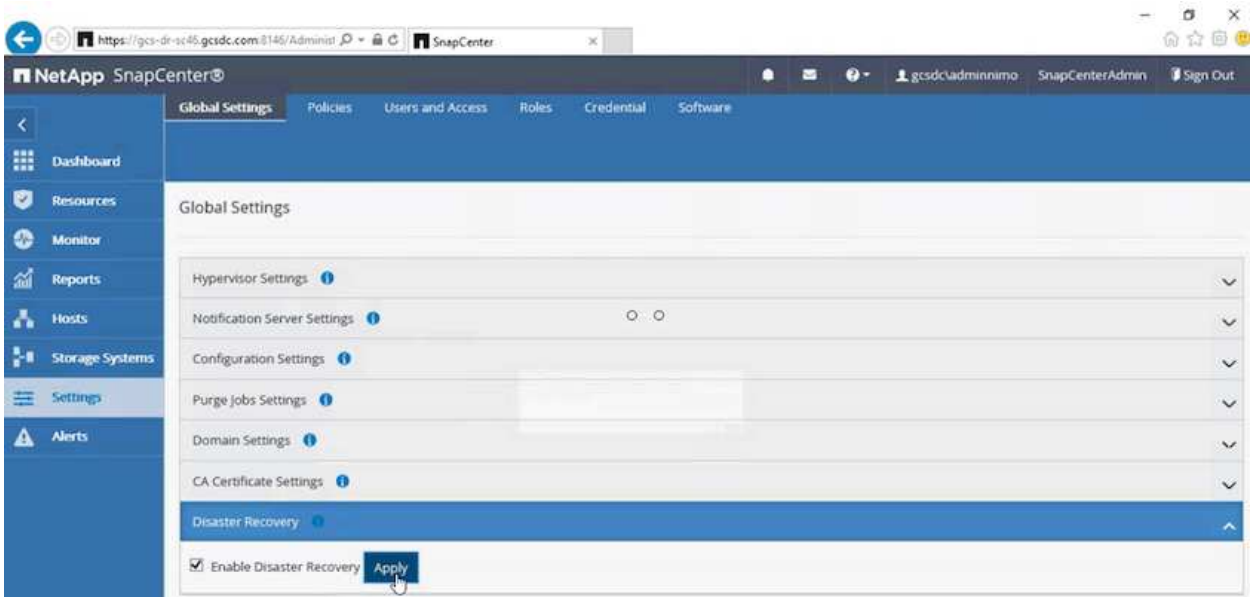
장애 조치 구성 및 인프라를 검증하기 위해 JetStream DR을 테스트 모드(테스트 장애 조치 옵션)로 작동하여 가상 머신과 해당 데이터가 개체 저장소에서 테스트 복구 환경으로 복구되는 과정을 관찰할 수 있습니다. 테스트 모드에서 장애 조치 절차가 실행되면 실제 장애 조치 프로세스와 유사한 작업이 수행됩니다.



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.



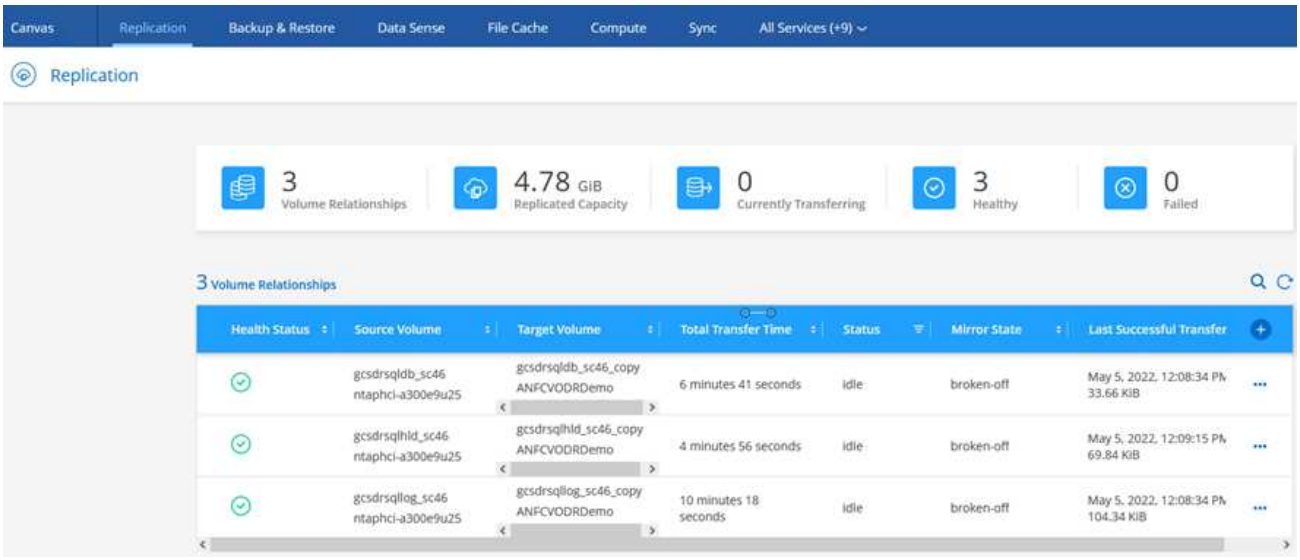
   b. 설정 페이지에서 설정 > 글로벌 설정 > 재해 복구로 이동합니다.
   c. 재해 복구 사용을 선택하세요.
   d. 적용을 클릭하세요.



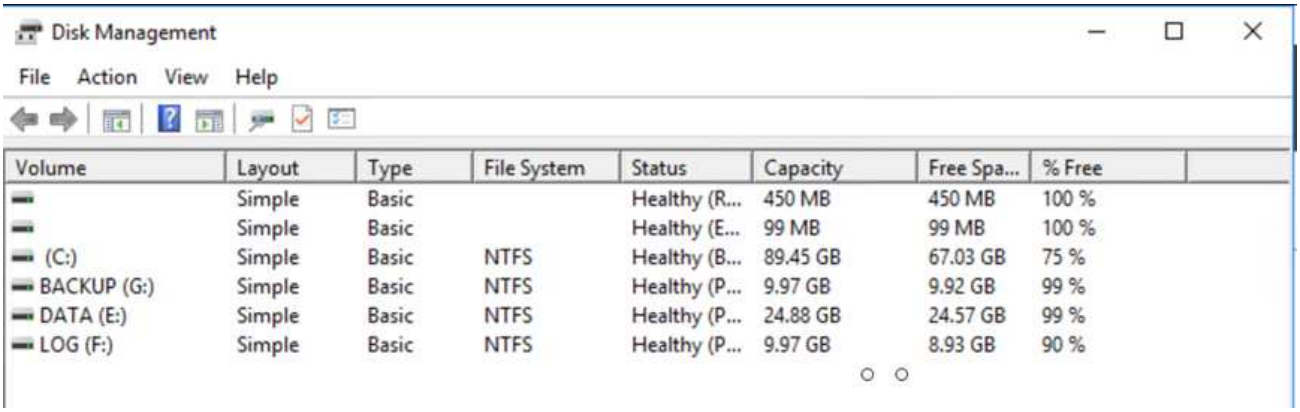
e. 모니터 > 작업을 클릭하여 DR 작업이 활성화되어 있는지 확인하세요.

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.

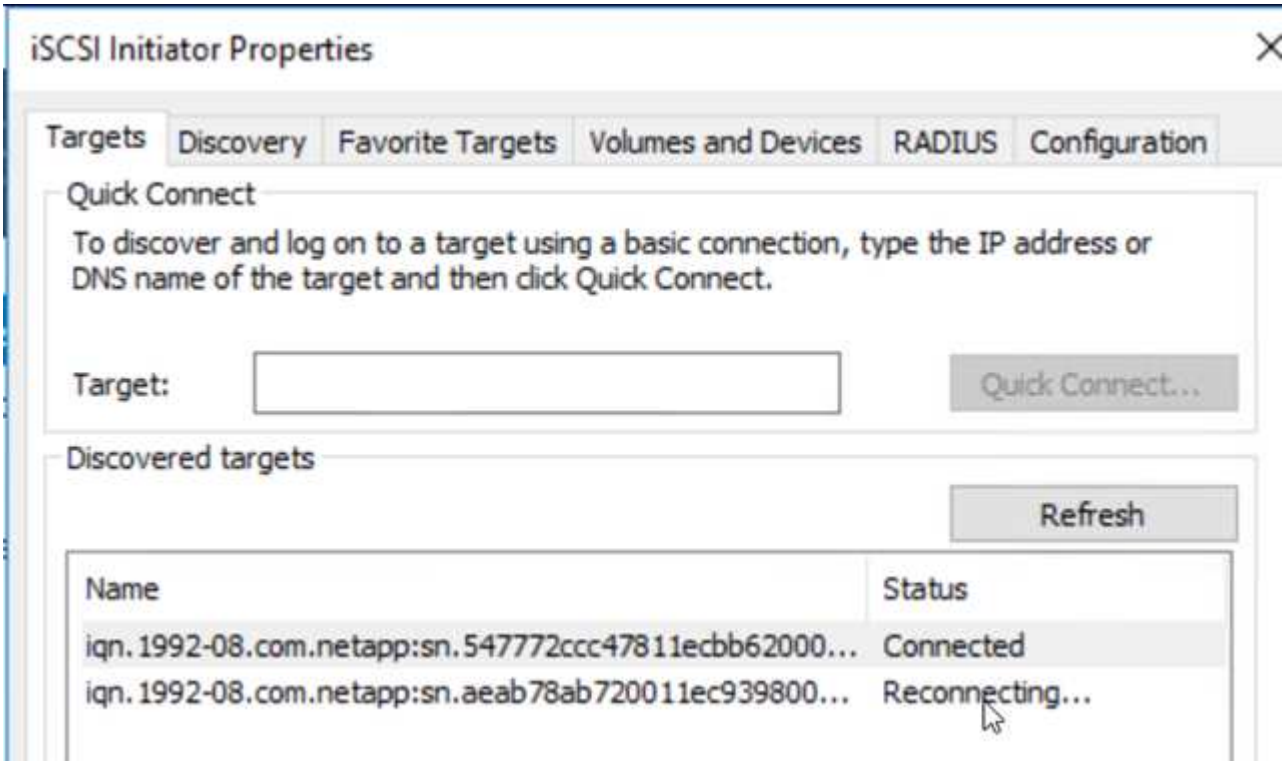
6. SnapMirror 관계가 끊어졌는지 확인하세요.



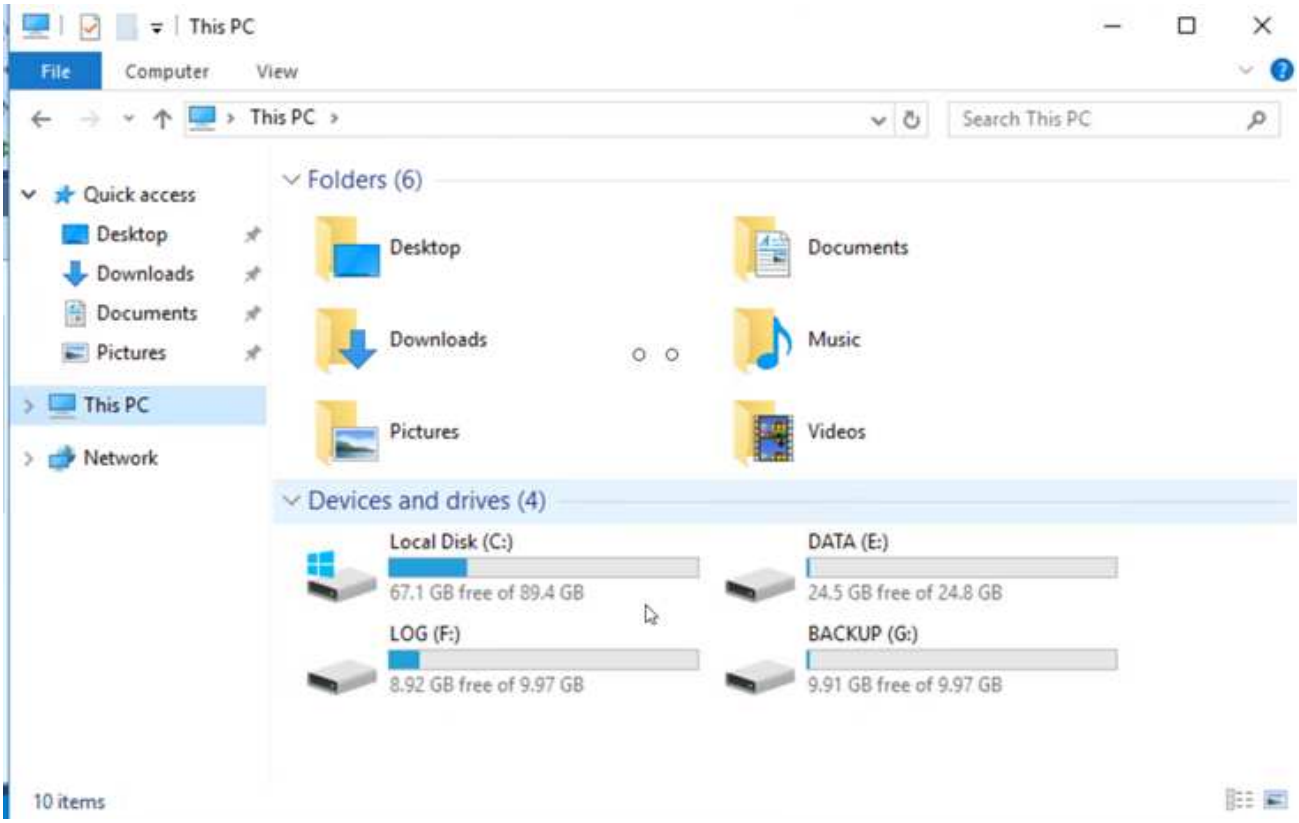
7. Cloud Volumes ONTAP 의 LUN을 동일한 드라이브 문자가 있는 복구된 SQL 게스트 VM에 연결합니다.



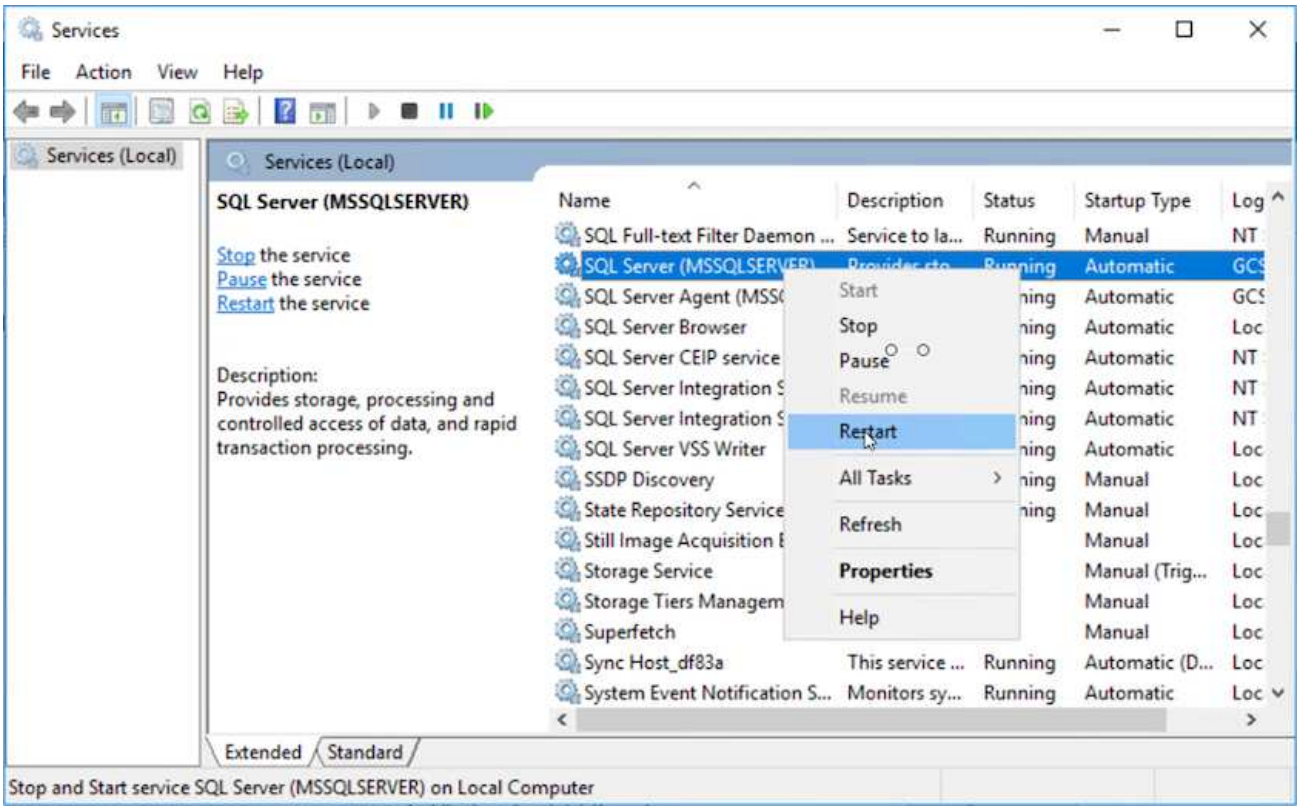
8. iSCSI Initiator를 열고 이전에 연결이 끊긴 세션을 지우고 복제된 Cloud Volumes ONTAP 볼륨에 대한 다중 경로와 함께 새 대상을 추가합니다.



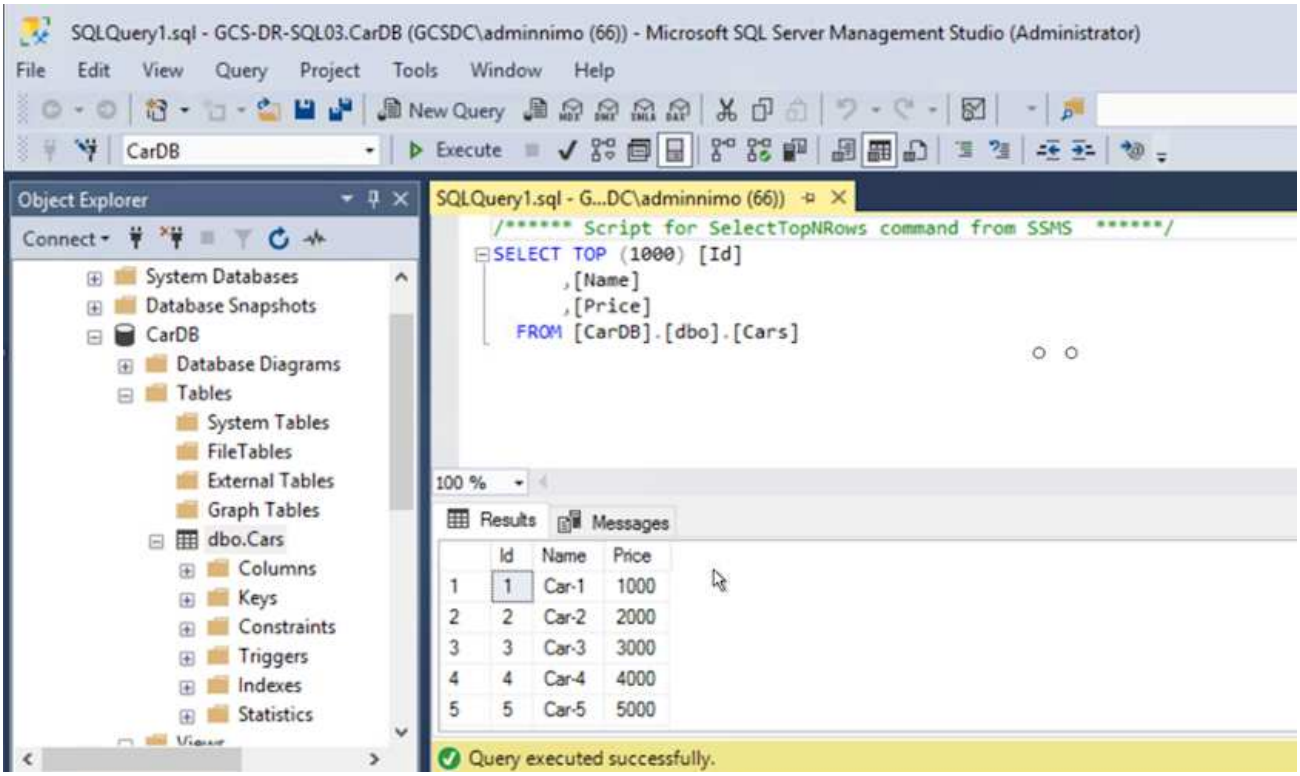
9. 모든 디스크가 DR 이전에 사용된 것과 동일한 드라이브 문자를 사용하여 연결되어 있는지 확인하세요.



10. MSSQL 서버 서비스를 다시 시작합니다.



11. SQL 리소스가 다시 온라인 상태인지 확인하세요.



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

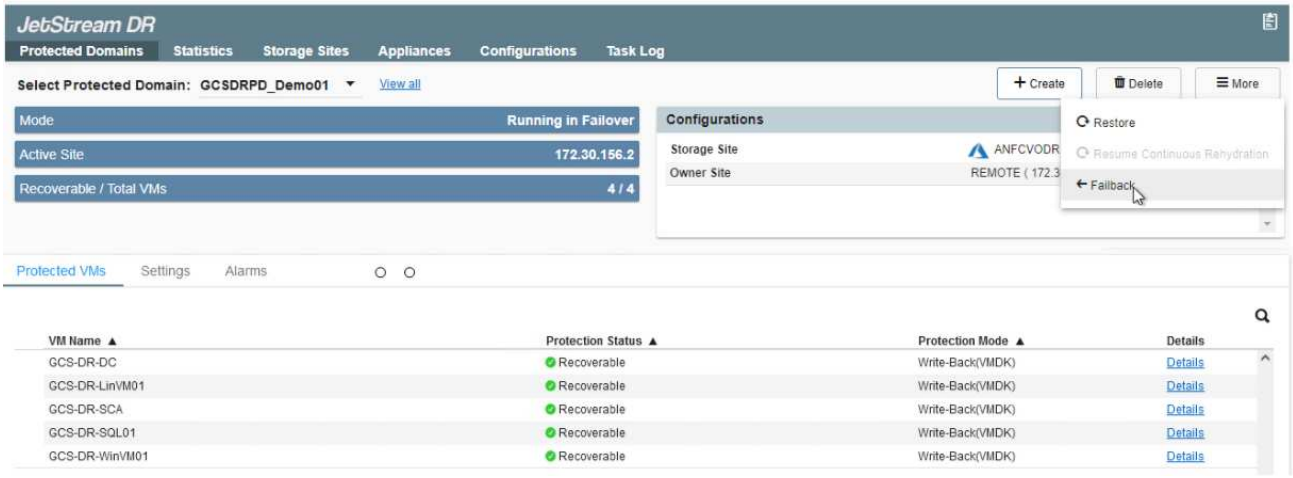
이 시점에서는 운영이 가능하며 사업은 정상적으로 계속됩니다.

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.

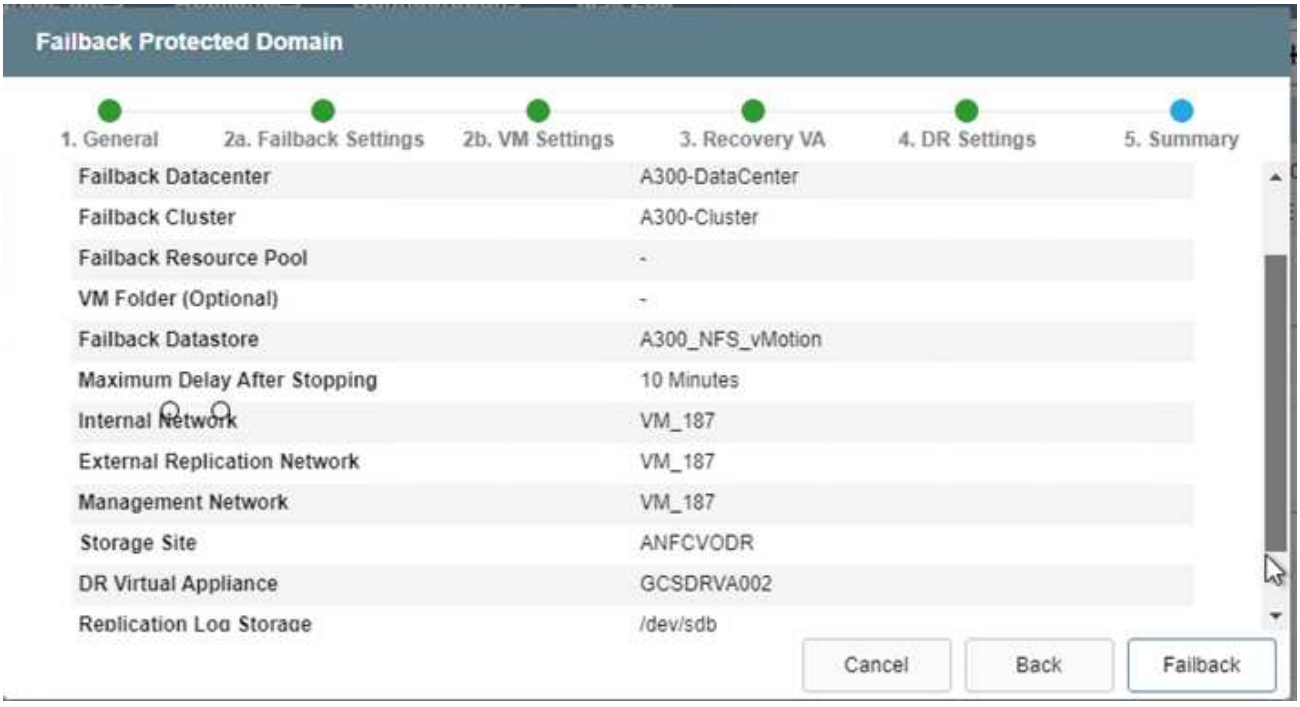
기본 사이트가 다시 가동되면 장애 복구를 수행할 수 있습니다. VM 보호는 Jetstream에 의해 재개되고 SnapMirror 관계는 반전되어야 합니다.

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.

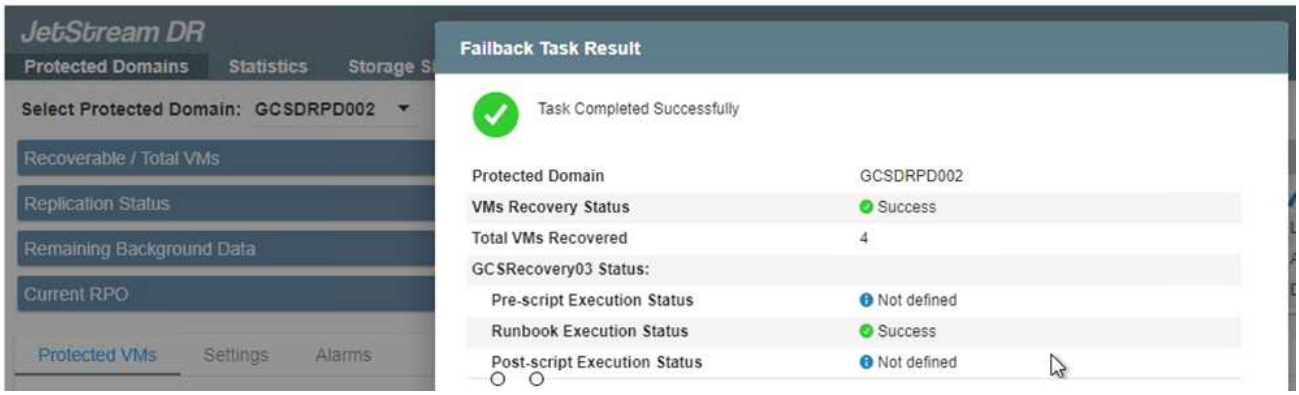
CPT에서 생성된 장애 복구 계획은 VM과 해당 데이터를 개체 저장소에서 원래 VMware 환경으로 반환하는 데에도 사용할 수 있습니다.



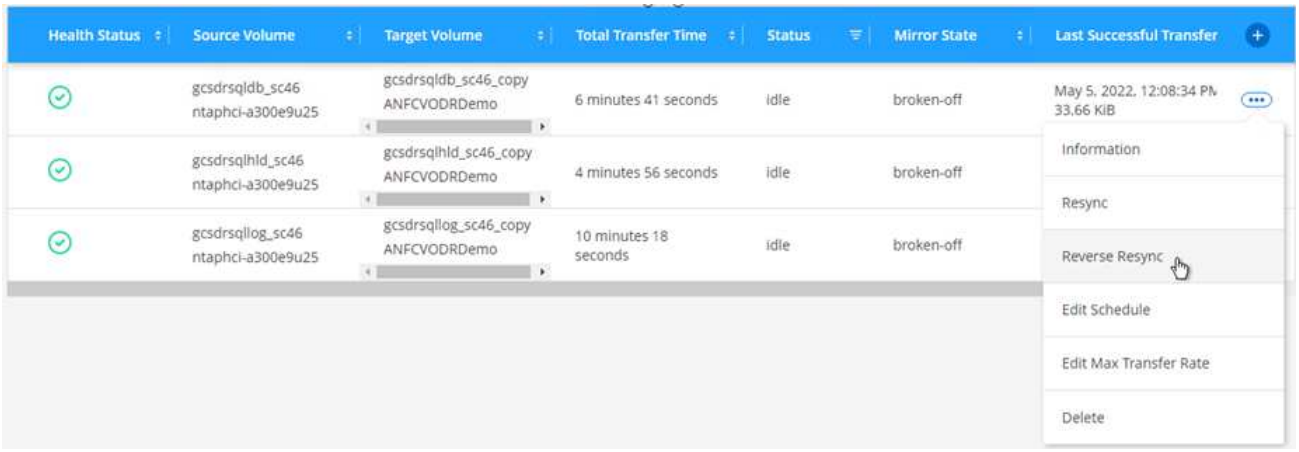
복구 사이트에서 VM을 일시 중지한 후 보호 사이트에서 다시 시작한 후의 최대 지연 시간을 지정합니다. 이 프로세스를 완료하는 데 필요한 시간에는 장애 조치 VM을 중지한 후 복제를 완료하는 데 필요한 시간, 복구 사이트를 정리하는 데 필요한 시간, 보호된 사이트에서 VM을 다시 만드는 데 필요한 시간이 포함됩니다. NetApp 10분을 권장합니다.

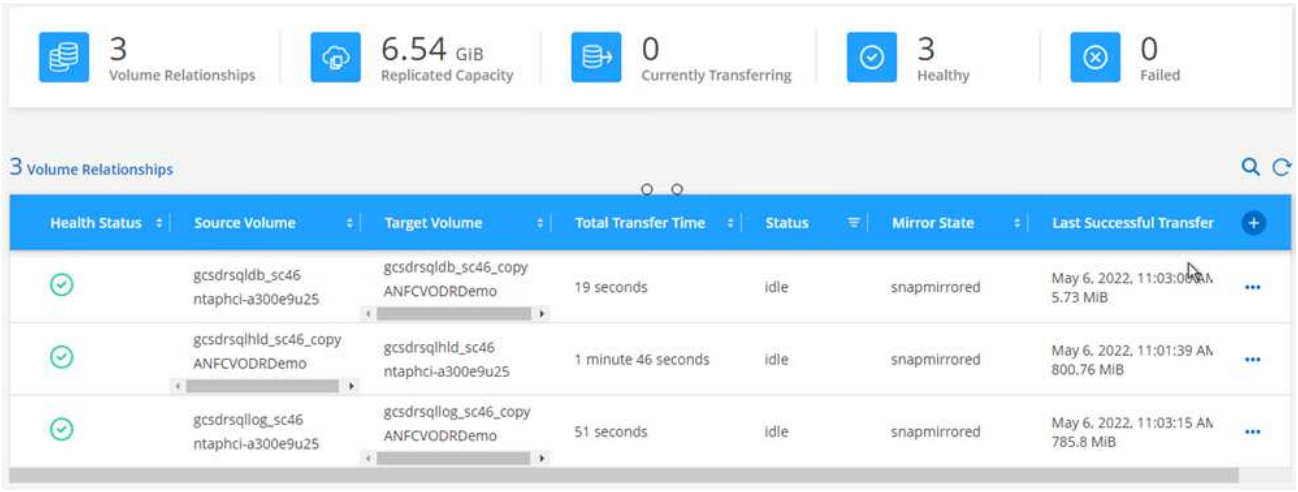


3. 장애 복구 프로세스를 완료한 후 VM 보호 및 데이터 일관성이 재개되었는지 확인합니다.

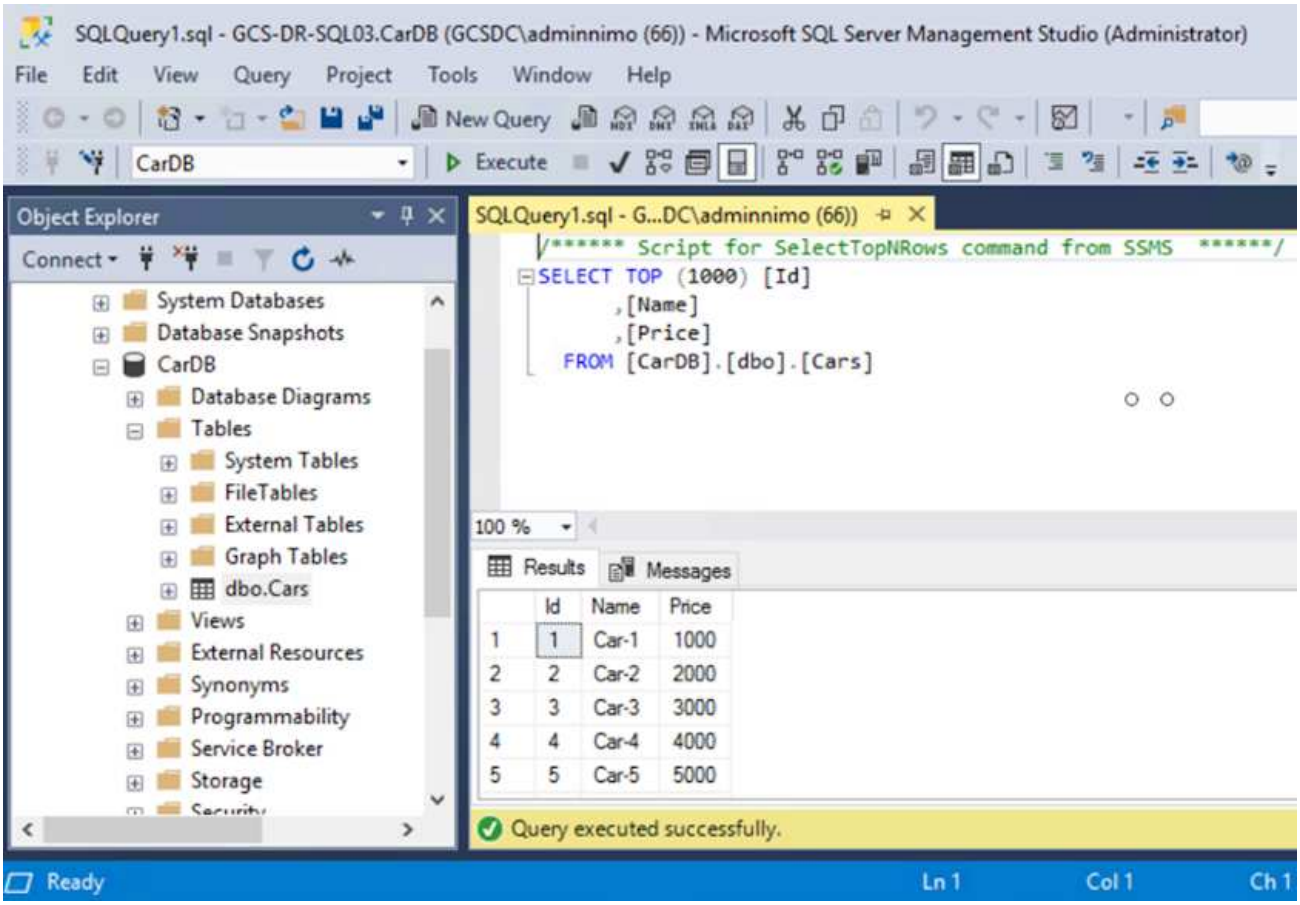


4. VM이 복구된 후 호스트에서 보조 스토리지의 연결을 끊고 기본 스토리지에 연결합니다.





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.

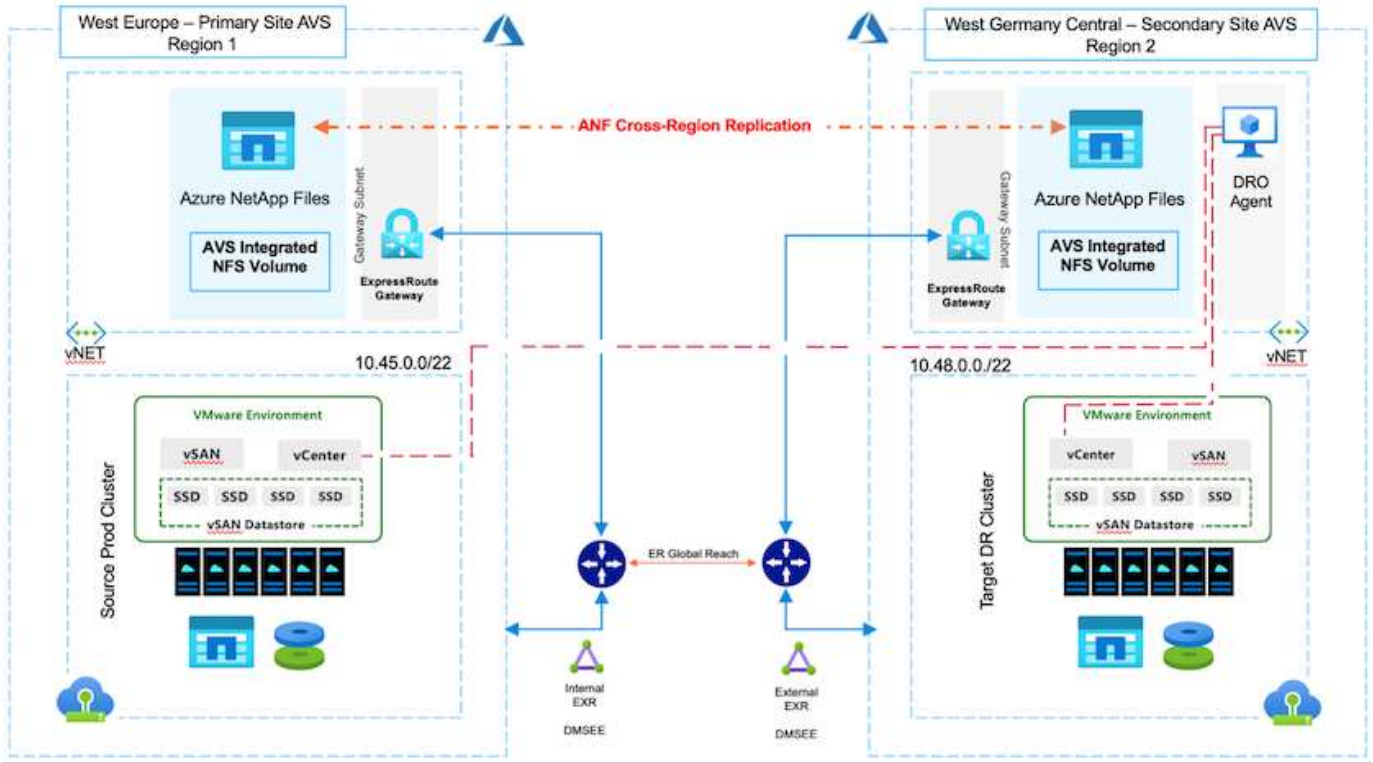
TR-4955: Azure NetApp Files (ANF) 및 **Azure VMware Solution(AVS)**을 사용한 재해 복구

클라우드 내 지역 간 블록 수준 복제를 사용하는 재해 복구는 사이트 중단 및 데이터 손상 이벤트(예: 랜섬웨어)로부터 작업 부하를 보호하는 탄력적이고 비용 효율적인 방법입니다.

개요

Azure NetApp 파일(ANF) 교차 지역 볼륨 복제를 사용하면 기본 AVS 사이트의 NFS 데이터 저장소로 Azure NetApp 파일 볼륨을 사용하여 Azure VMware Solution(AVS) SDDC 사이트에서 실행되는 VMware 워크로드를 대상 복구 지역의 지정된 보조 AVS 사이트로 복제할 수 있습니다.

UI가 있는 스크립트 솔루션인 재해 복구 오케스트레이터(DRO)를 사용하면 하나의 AVS SDDC에서 다른 AVS SDDC로 복제된 워크로드를 원활하게 복구할 수 있습니다. DRO는 복제 피어링을 중단하고 대상 볼륨을 데이터 저장소로 마운트한 다음 AVS에 VM을 등록하고 NSX-T(모든 AVS 프라이빗 클라우드에 포함됨)에서 직접 네트워크 매핑을 수행하여 복구를 자동화합니다.



필수 조건 및 일반 권장 사항

- 복제 피어링을 생성하여 지역 간 복제를 활성화했는지 확인하세요. 보다 "Azure NetApp Files 대한 볼륨 복제 만들기" .
- 소스 및 대상 Azure VMware Solution 프라이빗 클라우드 간에 ExpressRoute Global Reach를 구성해야 합니다.
- 리소스에 액세스할 수 있는 서비스 주체가 있어야 합니다.
- 다음 토폴로지가 지원됩니다: 기본 AVS 사이트에서 보조 AVS 사이트로.
- 구성하다 "복제" 비즈니스 요구 사항과 데이터 변경률에 따라 각 볼륨에 대한 일정을 적절히 조정합니다.

카스케이딩 및 팬인, 팬아웃 토폴로지는 지원되지 않습니다.

시작하기

Azure VMware 솔루션 배포

그만큼 "Azure VMware 솔루션" (AVS)는 Microsoft Azure 퍼블릭 클라우드 내에서 완벽한 기능을 갖춘 VMware SDDC를 제공하는 하이브리드 클라우드 서비스입니다. AVS는 Microsoft에서 완벽하게 관리하고 지원하며 VMware에서 검증한 자체 솔루션으로, Azure 인프라를 사용합니다. 따라서 고객은 컴퓨팅 가상화를 위해 VMware ESXi, 하이퍼 컨버지드 스토리지를 위해 vSAN, 네트워킹 및 보안을 위해 NSX를 얻는 동시에 Microsoft Azure의 글로벌 입지, 동급 최고의 데이터 센터 시설, 풍부한 기본 Azure 서비스 및 솔루션 생태계와의 근접성을 활용할 수 있습니다. Azure VMware Solution SDDC와 Azure NetApp Files 결합하면 최소한의 네트워크 지연으로 최고의 성능을 제공합니다.

Azure에서 AVS 프라이빗 클라우드를 구성하려면 다음 단계를 따르세요."링크" NetApp 문서 및 이 "링크" Microsoft 설명서용. 최소한의 구성으로 설정된 조종등 환경은 DR 목적으로 사용될 수 있습니다. 이 설정에는 중요한 애플리케이션을 지원하는 핵심 구성 요소만 포함되어 있으며, 장애 조치가 발생할 경우 확장하여 더 많은 호스트를 생성하여 대부분의 부하를 처리할 수 있습니다.

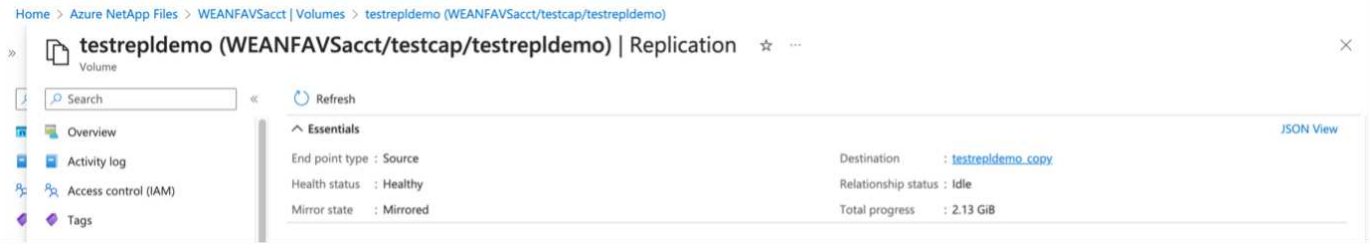
초기 릴리스에서는 DRO가 기존 AVS SDDC 클러스터를 지원합니다. 온디맨드 SDDC 생성은 향후 릴리스에서 제공될 예정입니다.

Azure NetApp Files 프로비저닝 및 구성

"Azure NetApp Files"고성능, 엔터프라이즈급, 계량형 파일 저장 서비스입니다. 이 단계를 따르세요 "링크" AVS 프라이빗 클라우드 배포를 최적화하기 위해 Azure NetApp Files NFS 데이터 저장소로 프로비저닝하고 구성합니다.

Azure NetApp Files 기반 데이터 저장소 볼륨에 대한 볼륨 복제 만들기

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



이 단계를 따르세요 "링크" 복제 피어링을 생성하여 지역 간 복제를 설정합니다. 대상 용량 풀의 서비스 수준은 소스 용량 풀의 서비스 수준과 일치할 수 있습니다. 그러나 이 특정 사용 사례의 경우 표준 서비스 수준을 선택한 다음 "서비스 수준을 수정하다" 실제 재난이나 재해 복구 시뮬레이션이 발생하는 경우.

지역 간 복제 관계는 전제 조건이며 미리 만들어야 합니다.

DRO 설치

DRO를 시작하려면 지정된 Azure 가상 머신에서 Ubuntu 운영 체제를 사용하고 필수 구성 요소를 충족하는지 확인하세요. 그런 다음 패키지를 설치하세요.

필수 조건:

- 리소스에 액세스할 수 있는 서비스 주체입니다.
- 소스 및 대상 SDDC와 Azure NetApp Files 인스턴스에 적절한 연결이 있는지 확인하세요.
- DNS 이름을 사용하는 경우 DNS 확인이 이루어져야 합니다. 그렇지 않은 경우 vCenter에 IP 주소를 사용하세요.

OS 요구 사항:

- Ubuntu Focal 20.04 (LTS) 다음 패키지는 지정된 에이전트 가상 머신에 설치되어야 합니다.
- 도커
- Docker-컴포즈
- JqChange `docker.sock` 이 새로운 허가에 대해: `sudo chmod 666 /var/run/docker.sock` .

그만큼 `deploy.sh` 스크립트는 모든 필수 전제 조건을 실행합니다.

단계는 다음과 같습니다.

1. 지정된 가상 머신에 설치 패키지를 다운로드하세요.

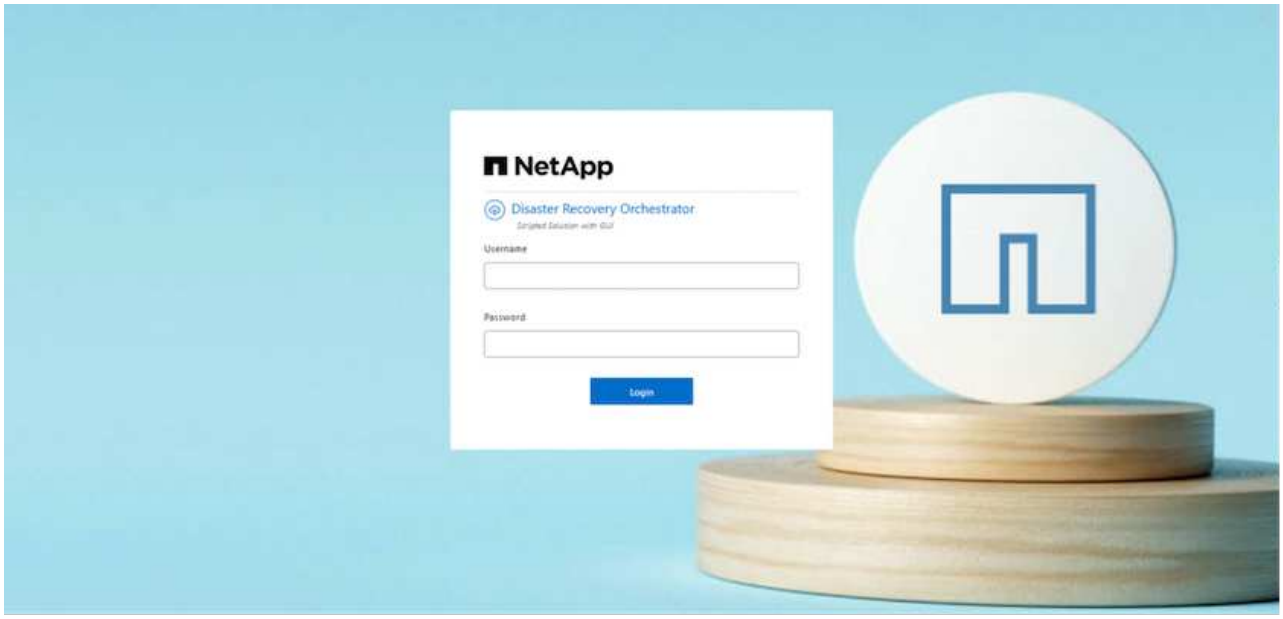
```
git clone https://github.com/NetApp/DRO-Azure.git
```

에이전트는 SDDC와 별도의 AZ에 있는 2차 AVS 사이트 지역이나 1차 AVS 사이트 지역에 설치해야 합니다.

2. 패키지 압축을 풀고 배포 스크립트를 실행한 후 호스트 IP를 입력합니다(예: `10.10.10.10`).

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

3. 다음 자격 증명을 사용하여 UI에 액세스하세요.
   - 사용자 이름: `admin`
   - 비밀번호: `admin`



DRO 구성

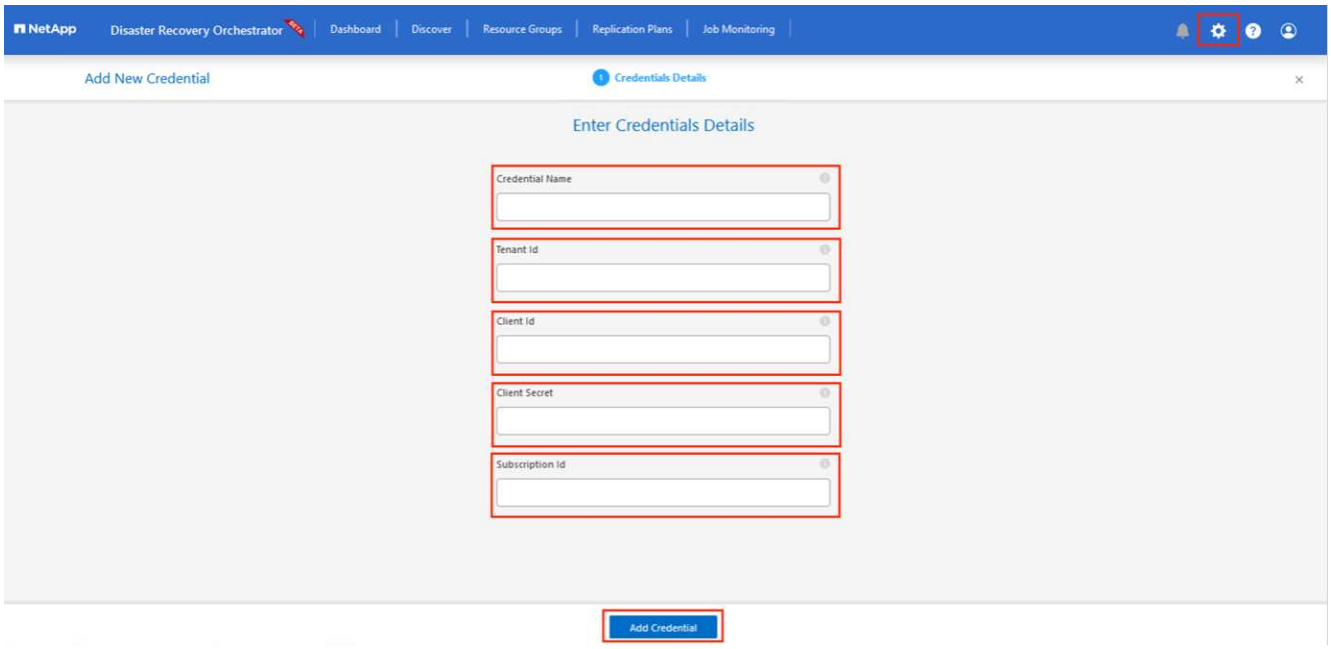
Azure NetApp Files 와 AVS가 올바르게 구성된 후 DRO를 구성하여 기본 AVS 사이트에서 보조 AVS 사이트로 워크로드를 복구하는 작업을 자동화할 수 있습니다. NetApp 보조 AVS 사이트에 DRO 에이전트를 배포하고 ExpressRoute 게이트웨이 연결을 구성하여 DRO 에이전트가 네트워크를 통해 적절한 AVS 및 Azure NetApp Files 구성 요소와 통신할 수 있도록 권장합니다.

첫 번째 단계는 자격 증명을 추가하는 것입니다. DRO에는 Azure NetApp Files 와 Azure VMware Solution을 검색하기 위한 권한이 필요합니다. Azure Active Directory(AD) 애플리케이션을 만들고 설정하고 DRO에 필요한 Azure 자격 증명을 얻어 Azure 계정에 필요한 권한을 부여할 수 있습니다. 서비스 주체를 Azure 구독에 바인딩하고 관련 필수 권한이 있는 사용자 지정 역할을 할당해야 합니다. 소스 및 대상 환경을 추가하면 서비스 주체와 연결된 자격 증명을 선택하라는 메시지가 표시됩니다. 새 사이트 추가를 클릭하기 전에 DRO에 이러한 자격 증명을 추가해야 합니다.

이 작업을 수행하려면 다음 단계를 완료하세요.

1. 지원되는 브라우저에서 DRO를 열고 기본 사용자 이름과 비밀번호를 사용하세요./admin/admin). 첫 번째 로그인 후 비밀번호 변경 옵션을 사용하여 비밀번호를 재설정할 수 있습니다.
2. DRO 콘솔의 오른쪽 상단에서 설정 아이콘을 클릭하고 *자격 증명*을 선택합니다.
3. 새 자격 증명 추가를 클릭하고 마법사의 단계를 따르세요.
4. 자격 증명을 정의하려면 필요한 권한을 부여하는 Azure Active Directory 서비스 주체에 대한 정보를 입력하세요.
   - 자격 증명 이름
   - 세입자 ID
   - 클라이언트 ID
   - 클라이언트 비밀번호
   - 구독 ID

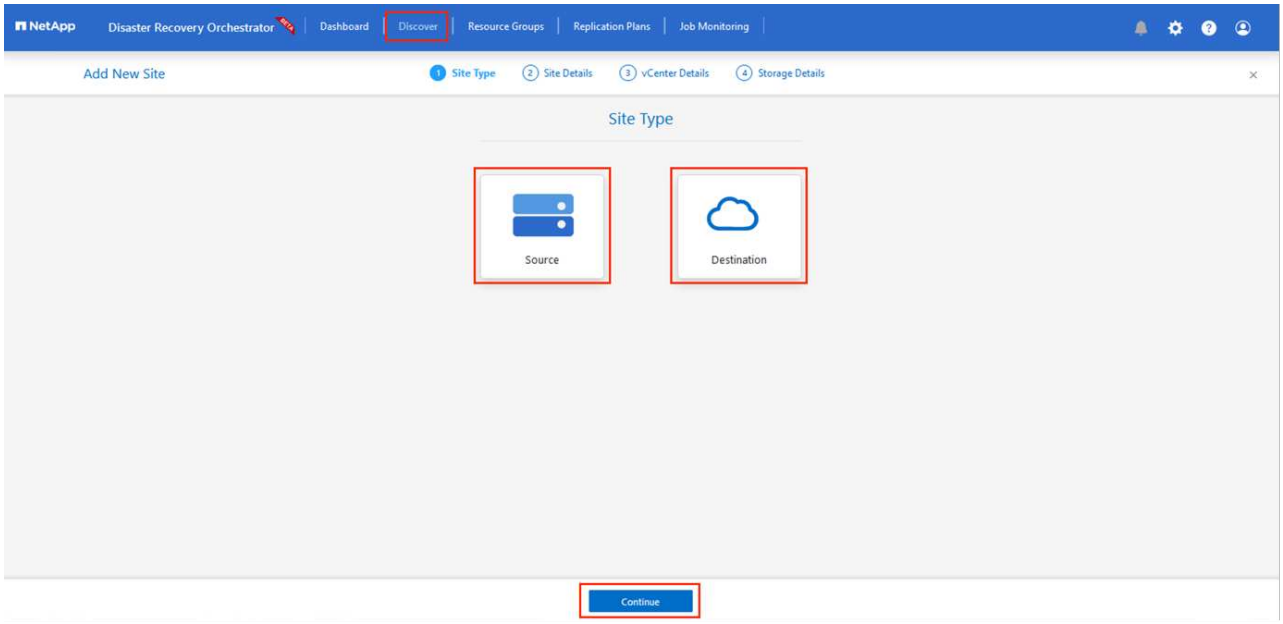
     AD 애플리케이션을 생성할 때 이 정보를 캡처했어야 합니다.
5. 새로운 자격 증명에 대한 세부 정보를 확인하고 자격 증명 추가를 클릭합니다.



   자격 증명을 추가한 후에는 기본 및 보조 AVS 사이트(vCenter와 Azure NetApp 파일 스토리지 계정 모두)를 검색하여 DRO에 추가해야 합니다. 소스 사이트와 대상 사이트를 추가하려면 다음 단계를 완료하세요.

6. 발견 탭으로 이동하세요.
7. *새 사이트 추가*를 클릭하세요.
8. 다음의 기본 AVS 사이트를 추가합니다(콘솔에서 *소스*로 지정).
   - SDDC vCenter
   - Azure NetApp Files 스토리지 계정
9. 다음의 보조 AVS 사이트를 추가합니다(콘솔에서 *대상*으로 지정).

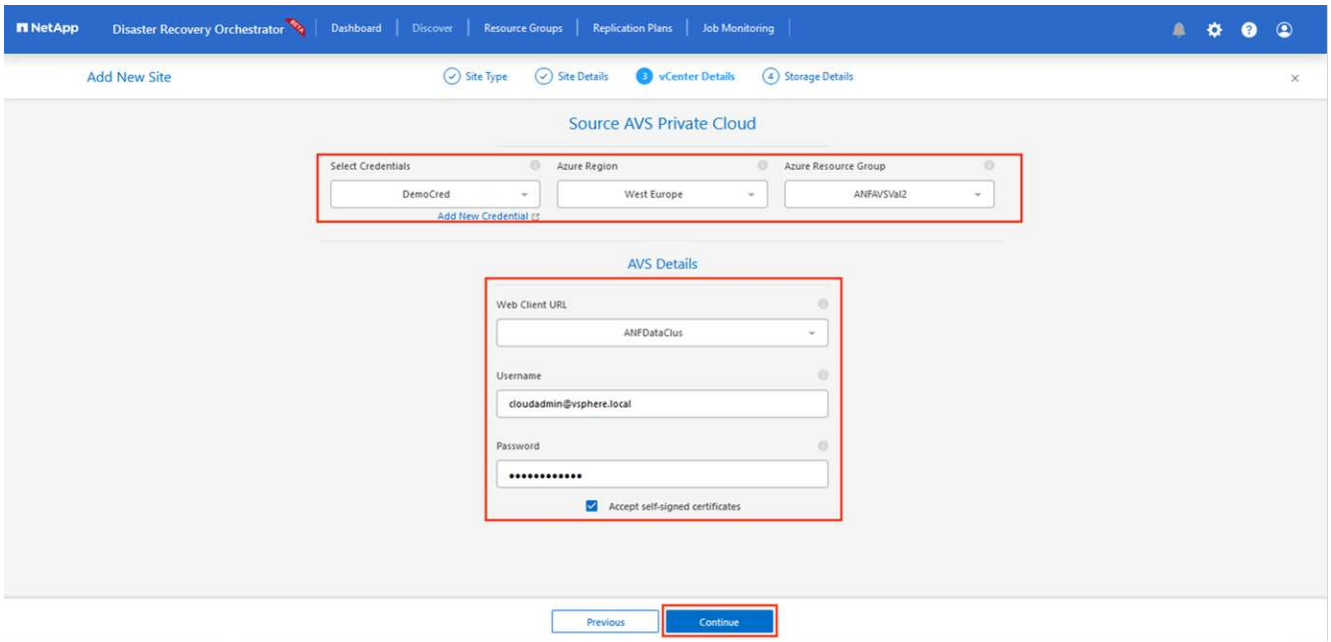
- SDDC vCenter
- Azure NetApp Files 스토리지 계정



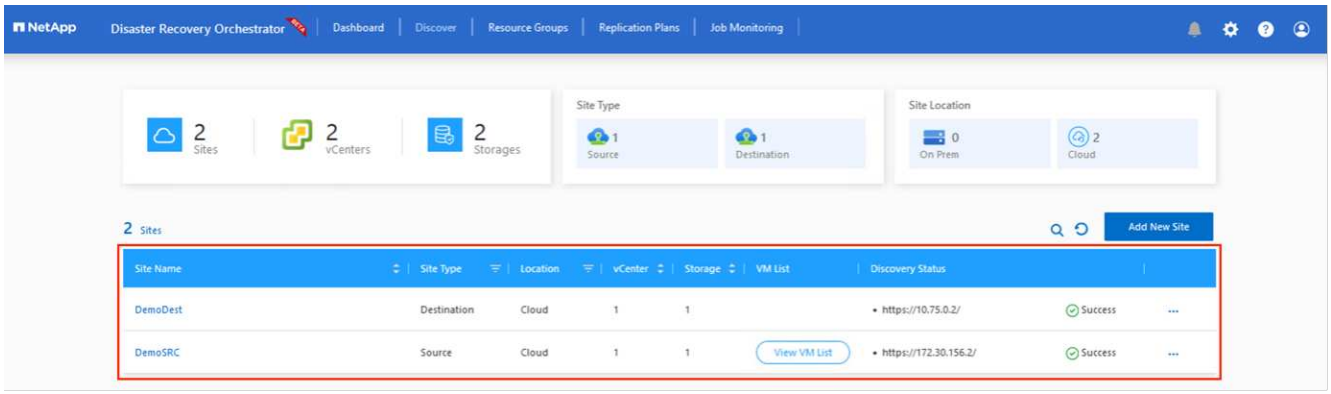
10. *소스*를 클릭하고, 친숙한 사이트 이름을 입력하고, 커넥터를 선택하여 사이트 세부 정보를 추가합니다. 그런 다음 *계속*을 클릭하세요.

   이 문서에서는 시연 목적으로 소스 사이트를 추가하는 방법을 설명합니다.

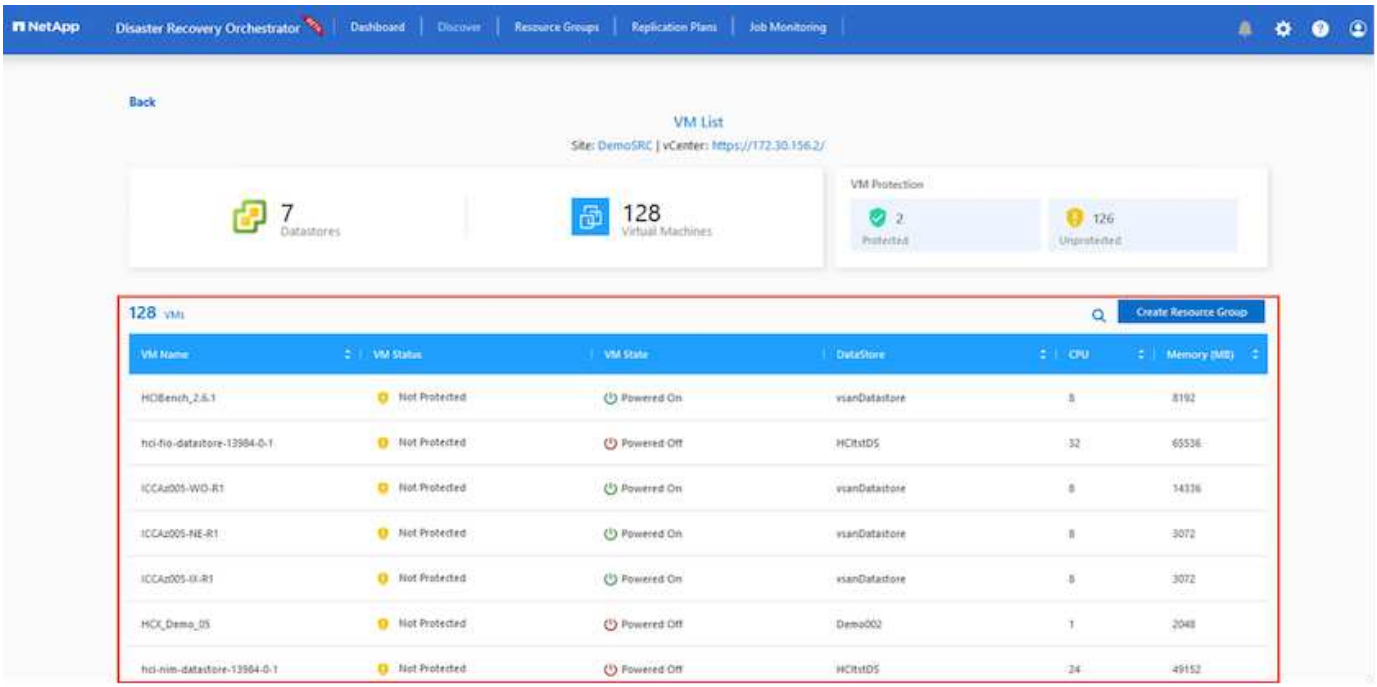
11. vCenter 세부정보를 업데이트합니다. 이렇게 하려면 기본 AVS SDDC의 드롭다운에서 자격 증명, Azure 지역 및 리소스 그룹을 선택합니다.
12. DRO는 해당 지역 내에서 사용 가능한 모든 SDDC를 나열합니다. 드롭다운에서 지정된 개인 클라우드 URL을 선택하세요.
13. 입력하세요 `cloudadmin@vsphere.local` 사용자 자격 증명. Azure Portal에서 액세스할 수 있습니다. 여기에 언급된 단계를 따르세요 "링크" . 완료되면 *계속*을 클릭하세요.



14. Azure 리소스 그룹과 NetApp 계정을 선택하여 원본 저장소 세부 정보(ANF)를 선택합니다.
15. *사이트 만들기*를 클릭하세요.



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



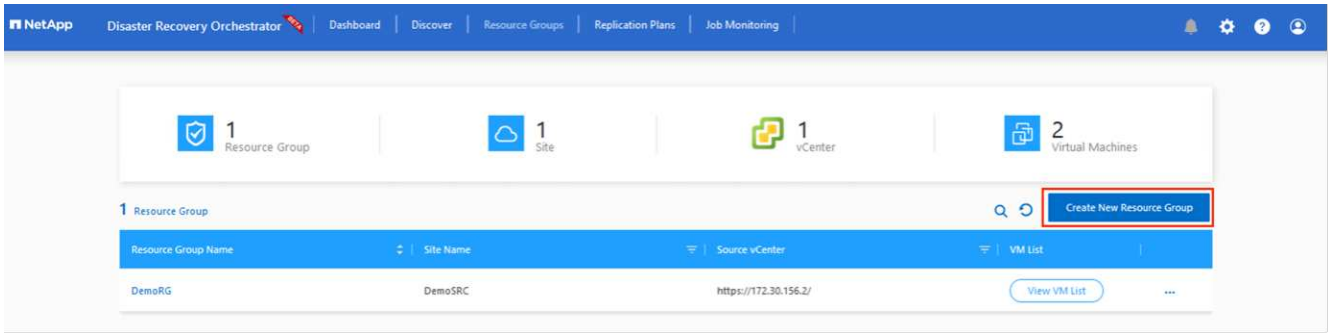
다음 단계는 필요한 VM을 리소스 그룹으로 기능 그룹으로 그룹화하는 것입니다.

리소스 그룹화

플랫폼을 추가한 후 복구하려는 VM을 리소스 그룹으로 그룹화합니다. DRO 리소스 그룹을 사용하면 종속된 VM 세트를 부팅 순서, 부팅 지연, 복구 시 실행할 수 있는 선택적 애플리케이션 유효성 검사가 포함된 논리적 그룹으로 그룹화할 수 있습니다.

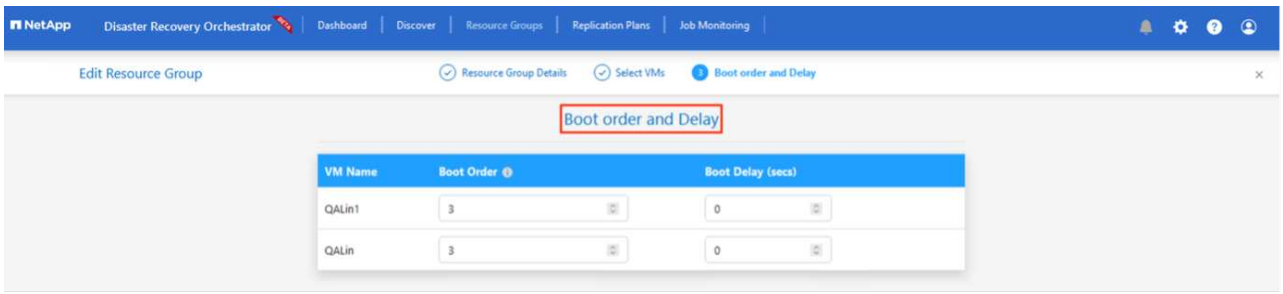
리소스 그룹을 만들려면 새 리소스 그룹 만들기 메뉴 항목을 클릭하세요.

1. *리소스 그룹*에 액세스하고 *새 리소스 그룹 만들기*를 클릭합니다.

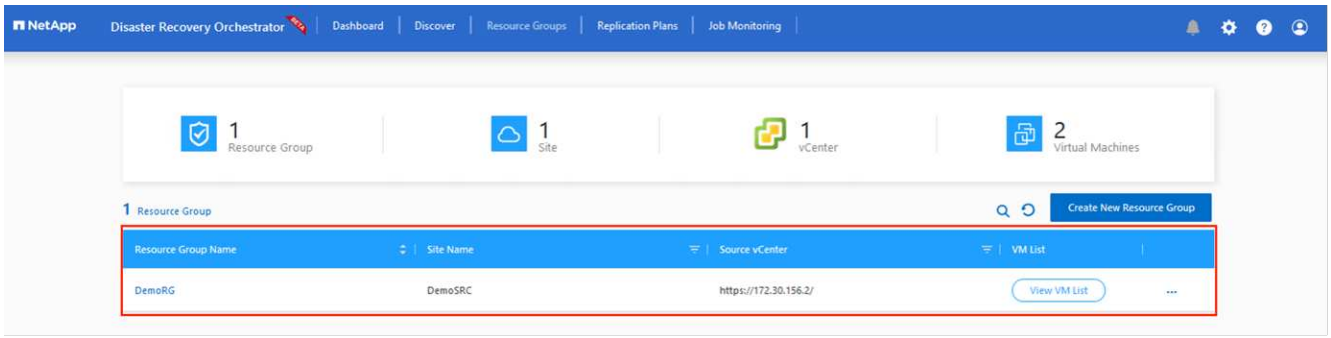


2. 새 리소스 그룹에서 드롭다운에서 소스 사이트를 선택하고 *만들기*를 클릭합니다.
3. 리소스 그룹 세부 정보를 제공하고 *계속*을 클릭합니다.
4. 검색 옵션을 사용하여 적절한 VM을 선택하세요.
5. 선택한 모든 VM에 대해 부팅 순서*와 *부팅 지연(초)을 선택합니다. 각 가상 머신을 선택하고 우선순위를 설정하여 전원 켜기 순서를 정합니다. 모든 가상 머신의 기본값은 3입니다. 옵션은 다음과 같습니다.
   - 전원을 켜는 첫 번째 가상 머신
   - 기본

◦ 마지막으로 전원이 켜진 가상 머신



6. *리소스 그룹 만들기*를 클릭합니다.

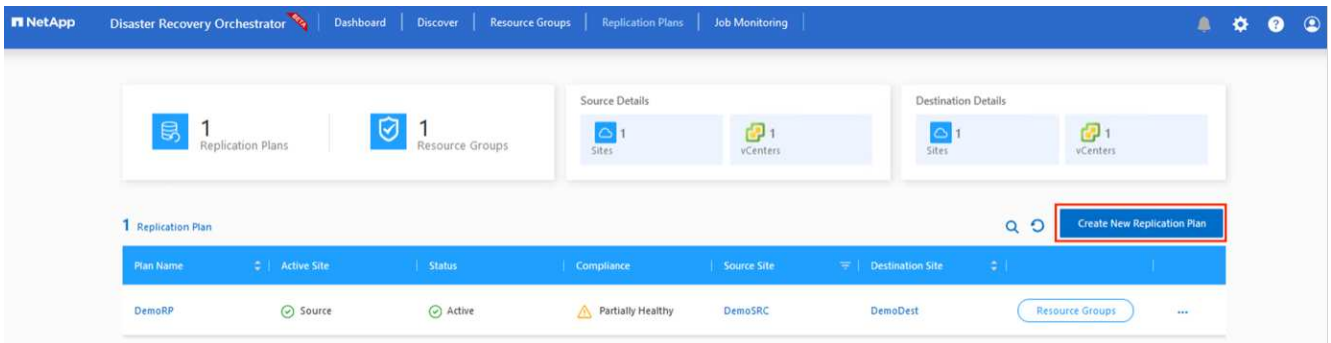


복제 계획

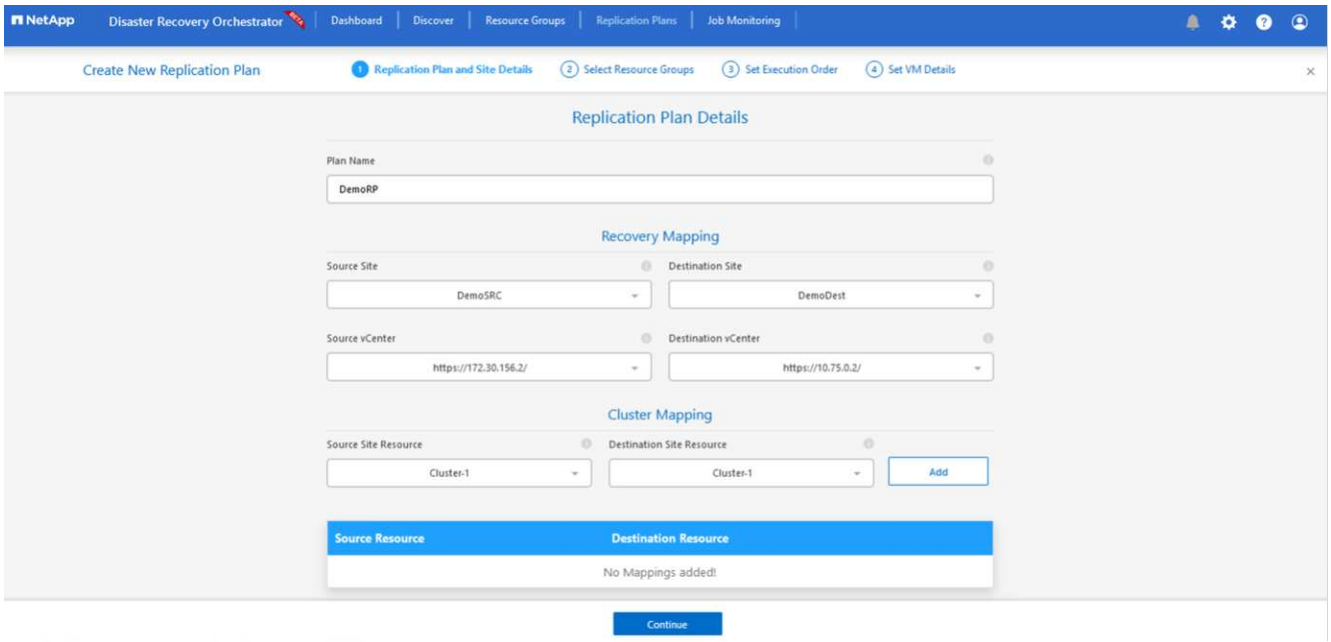
재해 발생 시 애플리케이션을 복구할 계획이 있어야 합니다. 드롭다운에서 소스 및 대상 vCenter 플랫폼을 선택하고, 이 계획에 포함할 리소스 그룹을 선택하고, 애플리케이션을 복원하고 전원을 켜는 방법(예: 도메인 컨트롤러, 1계층, 2계층 등)에 대한 그룹화도 포함합니다. 설계도는 종종 청사진이라고도 불립니다. 복구 계획을 정의하려면 복제 계획 탭으로 이동하여 *새 복제 계획*을 클릭합니다.

복제 계획을 만들려면 다음 단계를 완료하세요.

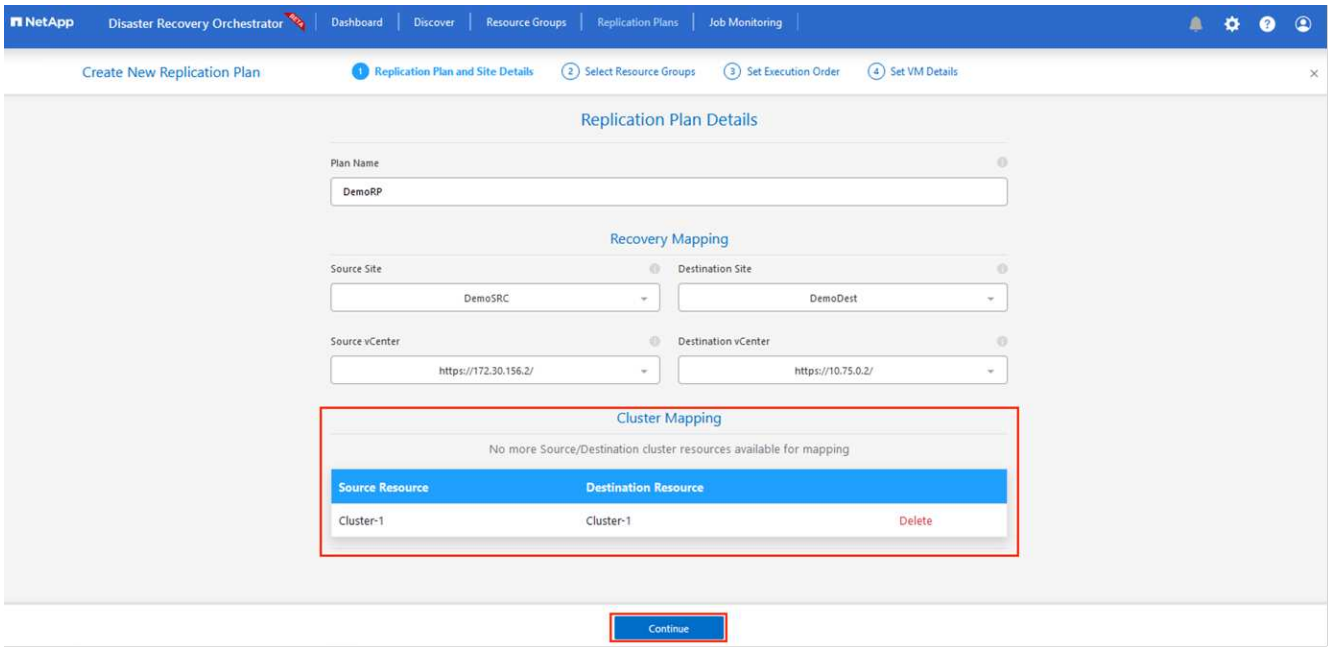
1. *복제 계획*으로 이동하여 *새 복제 계획 만들기*를 클릭합니다.



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

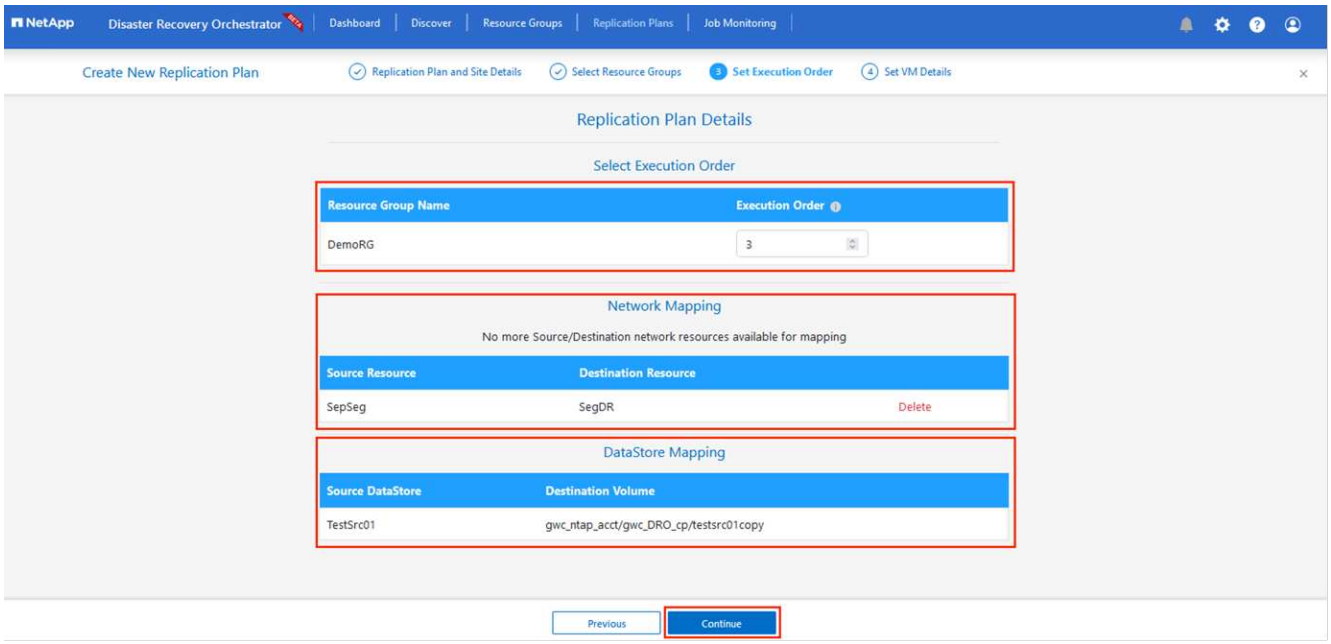


3. 복구 매핑이 완료되면 *클러스터 매핑*을 선택합니다.

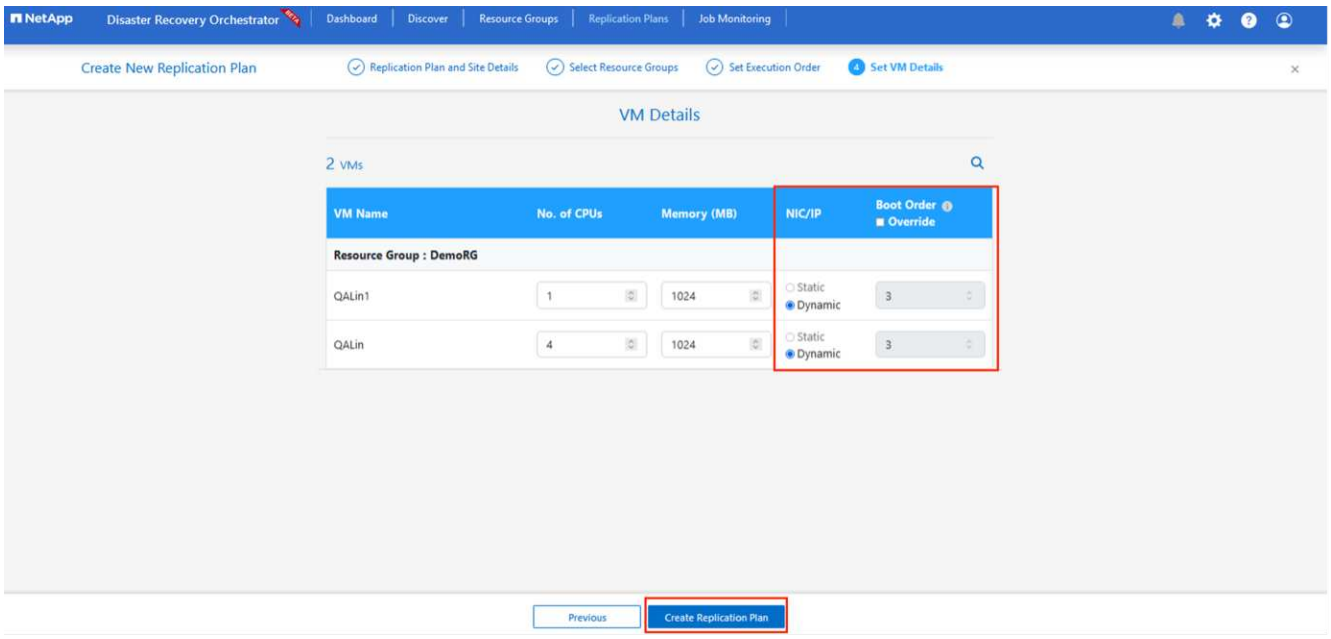


4. *리소스 그룹 세부 정보*를 선택하고 *계속*을 클릭합니다.
5. 리소스 그룹에 대한 실행 순서를 설정합니다. 이 옵션을 사용하면 여러 리소스 그룹이 있는 경우 작업 순서를 선택할 수 있습니다.
6. 완료되면 네트워크 매핑을 적절한 세그먼트로 설정합니다. 세그먼트는 이미 보조 AVS 클러스터에 프로비저닝되어 있어야 하며, 이에 VM을 매핑하려면 적절한 세그먼트를 선택합니다.
7. 데이터 저장소 매핑은 VM 선택에 따라 자동으로 선택됩니다.

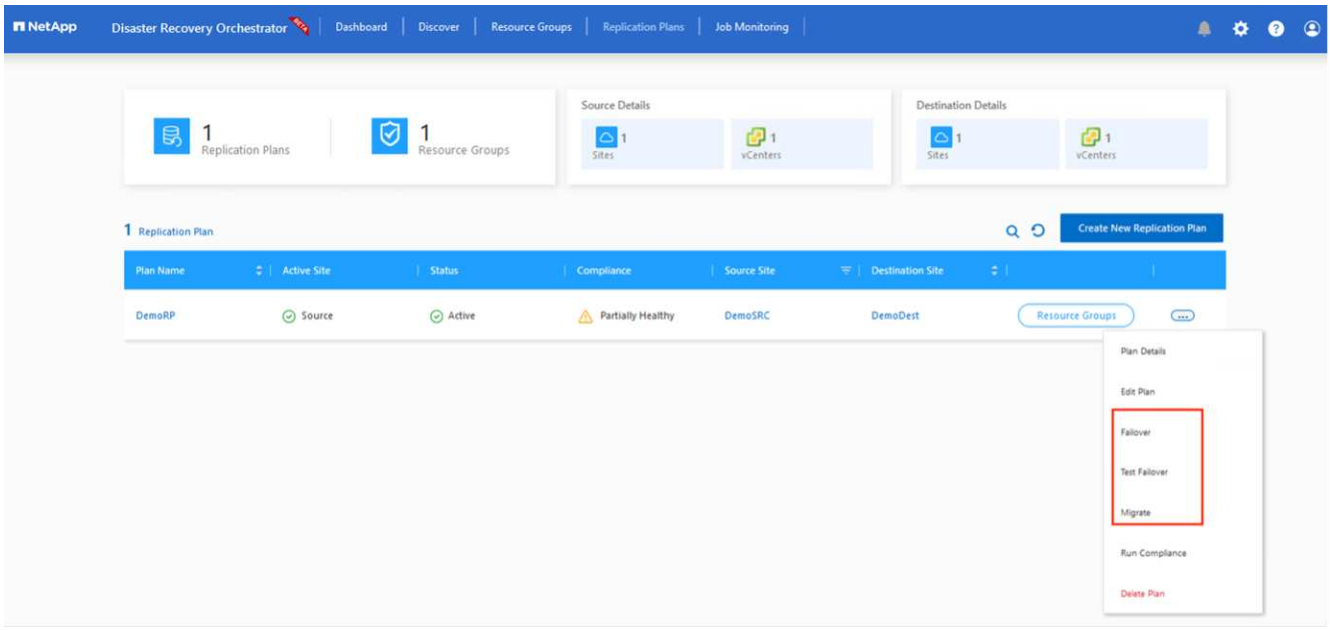
지역 간 복제(CRR)는 볼륨 수준에서 수행됩니다. 따라서 해당 볼륨에 있는 모든 VM은 CRR 대상에 복제됩니다. 복제 계획에 포함된 가상 머신만 처리되므로 데이터 저장소에 포함된 모든 VM을 선택해야 합니다.



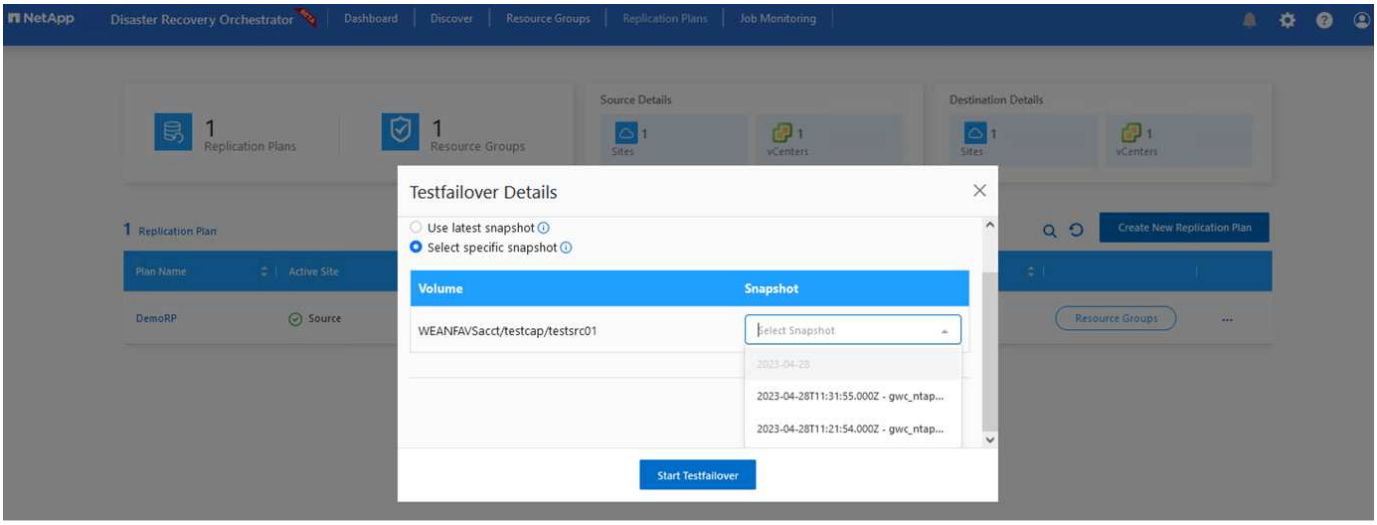
8. VM 세부 정보에서 선택적으로 VM CPU 및 RAM 매개변수의 크기를 조정할 수 있습니다. 이 기능은 대규모 환경을 더 작은 대상 클러스터로 복구하거나 일대일 물리적 VMware 인프라를 프로비저닝하지 않고도 DR 테스트를 수행할 때 매우 유용할 수 있습니다. 또한 리소스 그룹 전체에서 선택한 모든 VM에 대한 부팅 순서와 부팅 지연(초)을 수정합니다. 리소스 그룹 부팅 순서를 선택하는 동안 선택한 내용을 변경해야 하는 경우 부팅 순서를 수정하는 추가 옵션이 있습니다. 기본적으로 리소스 그룹 선택 중에 선택된 부팅 순서가 사용되지만, 이 단계에서 모든 수정 작업을 수행할 수 있습니다.



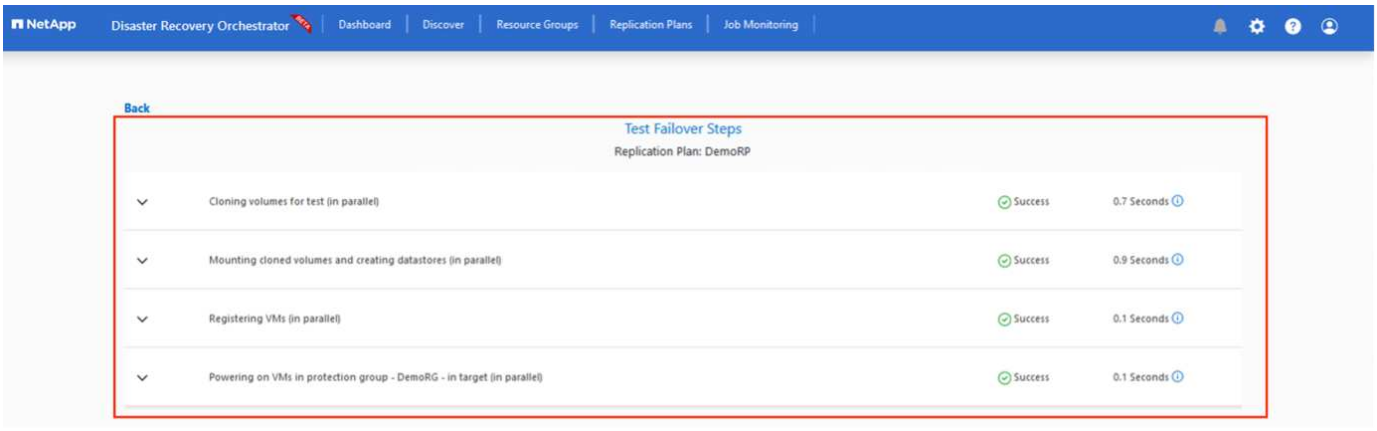
9. *복제 계획 만들기*를 클릭합니다. 복제 계획이 생성된 후 요구 사항에 따라 장애 조치, 테스트 장애 조치 또는 마이그레이션 옵션을 실행할 수 있습니다.



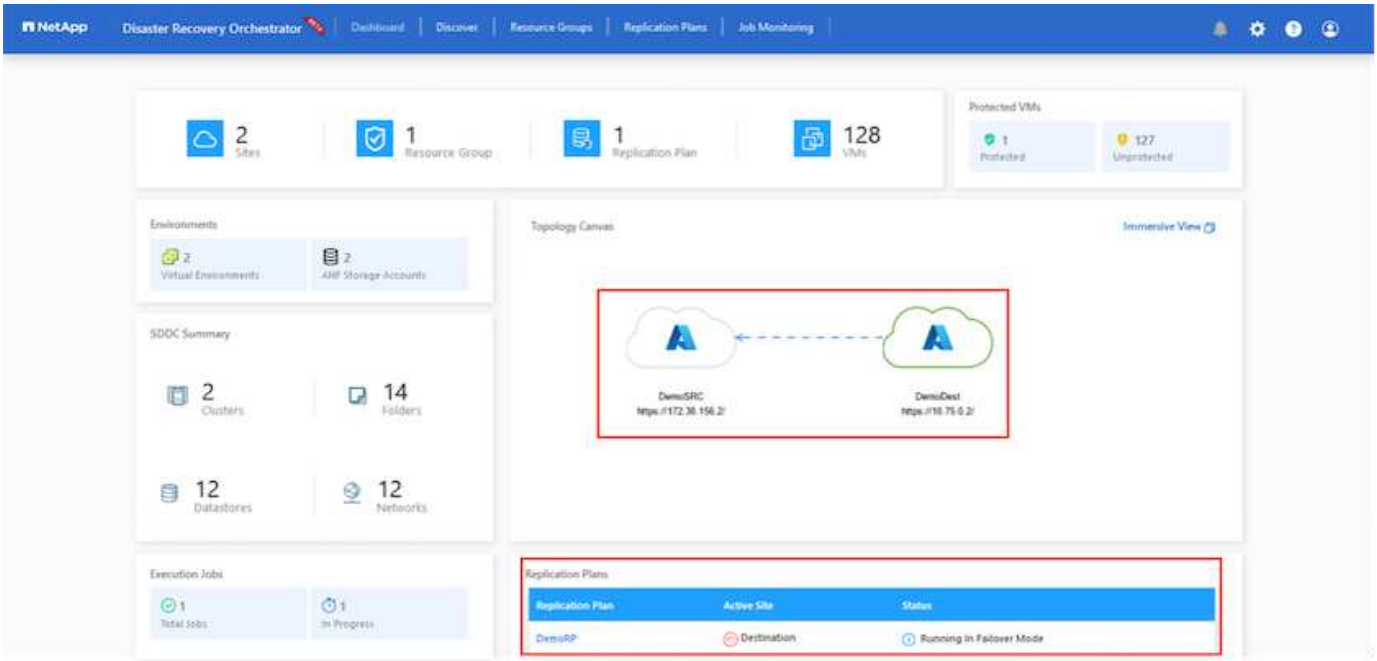
장애 조치 및 테스트 장애 조치 옵션 중에 가장 최근의 스냅샷이 사용되거나 특정 시점 스냅샷에서 특정 스냅샷을 선택할 수 있습니다. 랜섬웨어와 같이 최신 복제본이 이미 손상되거나 암호화된 경우와 같이 손상 이벤트가 발생하는 경우 특정 시점 옵션이 매우 유용할 수 있습니다. DRO는 사용 가능한 모든 시간 지점을 보여줍니다.



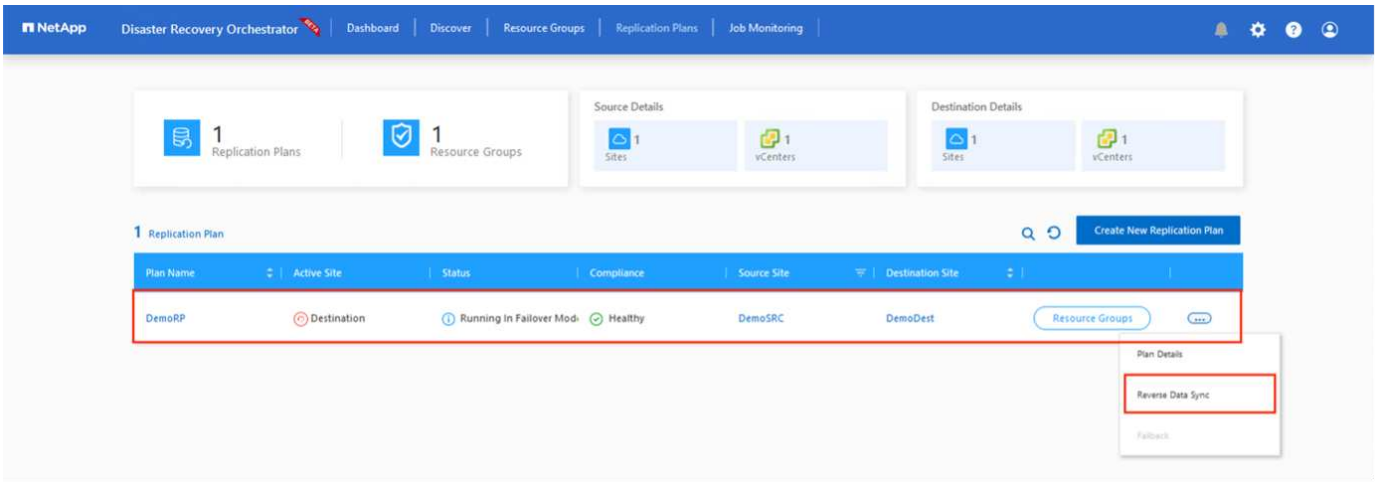
복제 계획에 지정된 구성으로 장애 조치 또는 테스트 장애 조치를 트리거하려면 장애 조치 또는 *테스트 장애 조치*를 클릭하면 됩니다. 작업 메뉴에서 복제 계획을 모니터링할 수 있습니다.



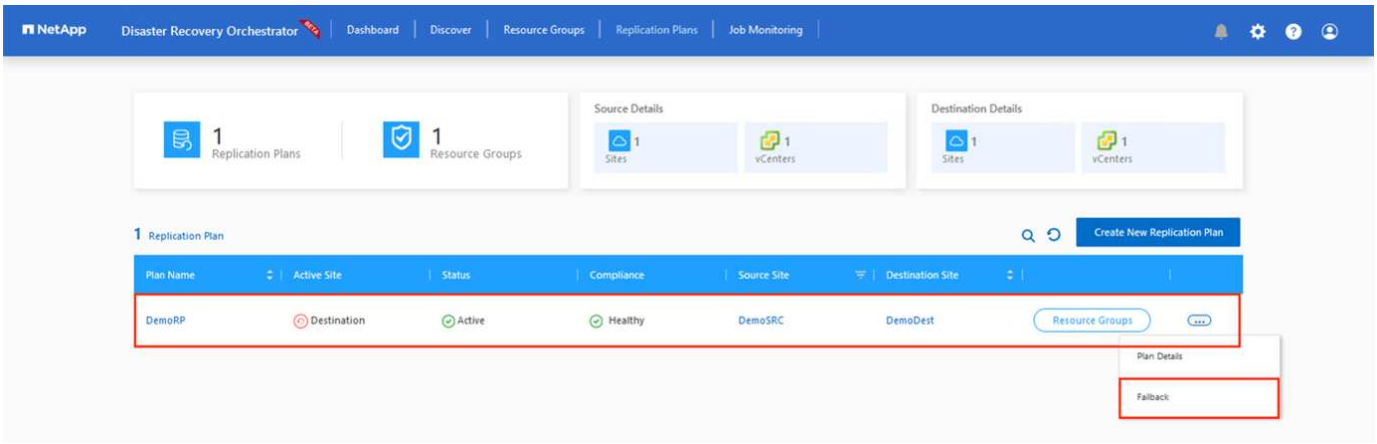
장애 조치가 트리거된 후 복구된 항목은 보조 사이트 AVS SDDC vCenter(VM, 네트워크, 데이터 저장소)에서 볼 수 있습니다. 기본적으로 VM은 워크로드 폴더로 복구됩니다.

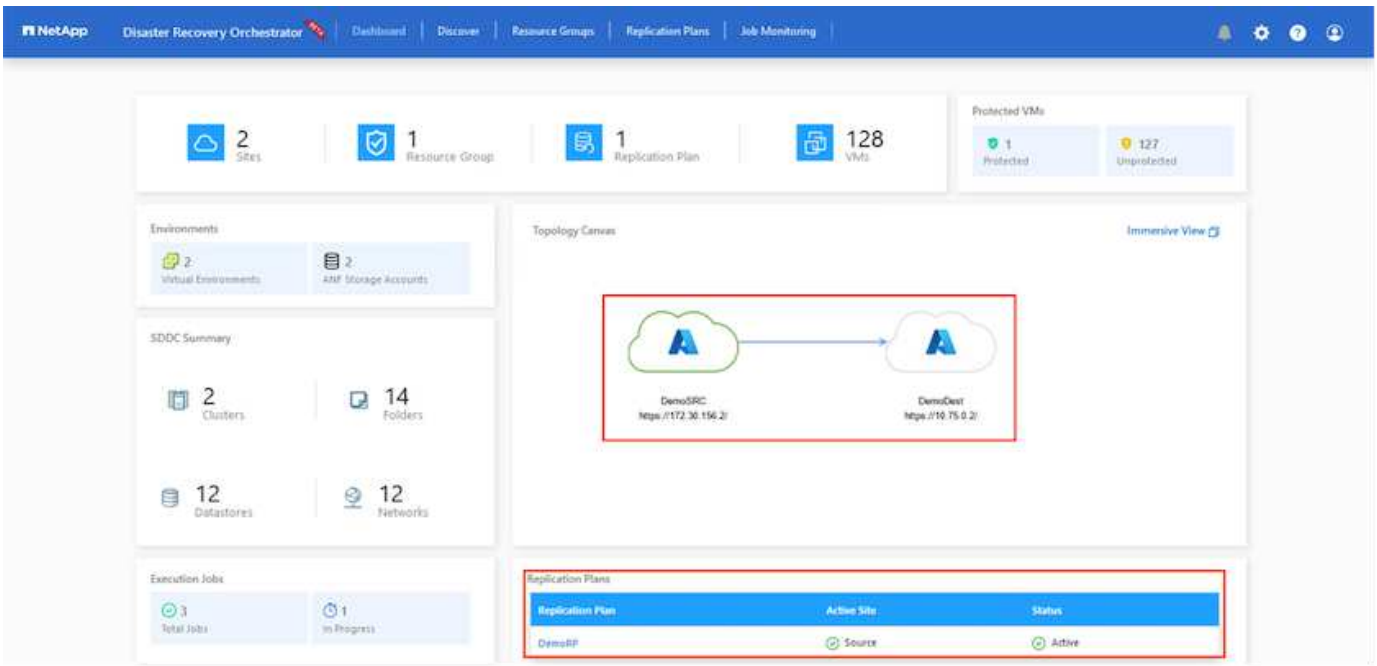


장애 복구는 복제 계획 수준에서 트리거될 수 있습니다. 테스트 장애 조치의 경우, 해체 옵션을 사용하여 변경 사항을 롤백하고 새로 생성된 볼륨을 제거할 수 있습니다. 장애 조치와 관련된 장애 복구는 2단계 프로세스입니다. 복제 계획을 선택하고 *역방향 데이터 동기화*를 선택합니다.



이 단계가 완료되면 장애 복구를 트리거하여 기본 AVS 사이트로 돌아갑니다.





Azure Portal에서 복제 상태가 읽기/쓰기 볼륨으로 보조 사이트 AVS SDDC에 매핑된 해당 볼륨에 대해 중단된 것을 확인할 수 있습니다. 테스트 장애 조치 중에 DRO는 대상 또는 복제 볼륨을 매핑하지 않습니다. 대신, 필요한 지역 간 복제 스냅샷의 새 볼륨을 생성하고 볼륨을 데이터 저장소로 노출하여 용량 풀에서 추가적인 물리적 용량을 사용하고

소스 볼륨이 수정되지 않도록 보장합니다. 특히, DR 테스트나 분류 워크플로우 중에도 복제 작업을 계속할 수 있습니다. 또한, 이 프로세스를 통해 오류가 발생하거나 손상된 데이터가 복구된 경우 복제본이 파괴될 위험 없이 복구를 정리할 수 있습니다.

랜섬웨어 복구

랜섬웨어로부터 복구하는 것은 힘든 일일 수 있습니다. 특히, IT 조직에서는 안전한 복귀 지점이 어디인지 정확히 파악하기 어려울 수 있으며, 이를 파악한 후에도 복구된 워크로드가 재발하는 공격(예: 잠복 맬웨어 또는 취약한 애플리케이션을 통한 공격)으로부터 어떻게 보호될지 확실히 알아내는 것도 어려울 수 있습니다.

DRO는 조직이 사용 가능한 모든 시점에서 복구할 수 있도록 하여 이러한 문제를 해결합니다. 그런 다음 작업 부하를 기능적이면서도 격리된 네트워크로 복구하여 애플리케이션이 서로 작동하고 통신할 수 있지만 남북 트래픽에 노출되지 않도록 합니다. 이 프로세스를 통해 보안팀은 법의학 조사를 수행하고 숨겨져 있거나 잠복해 있는 맬웨어를 식별할 수 있는 안전한 환경을 확보할 수 있습니다.

결론

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

- 효율적이고 탄력적인 Azure NetApp Files 지역 간 복제를 활용하세요.
- 스냅샷 보존을 통해 사용 가능한 모든 시점으로 복구합니다.
- 저장소, 컴퓨팅, 네트워크 및 애플리케이션 검증 단계에서 수백 개에서 수천 개의 VM을 복구하는 데 필요한 모든 단계를 완전히 자동화합니다.
- 워크로드 복구는 복제된 볼륨을 조작하지 않는 "최근 스냅샷에서 새 볼륨 만들기" 프로세스를 활용합니다.
- 볼륨이나 스냅샷에서 데이터 손상 위험을 방지하세요.
- DR 테스트 워크플로우 동안 복제 중단을 방지합니다.
- DR을 넘어 개발/테스트, 보안 테스트, 패치 및 업그레이드 테스트, 수정 테스트 등 워크플로우에 DR 데이터와 클라우드 컴퓨팅 리소스를 활용합니다.
- CPU 및 RAM 최적화는 더 작은 컴퓨팅 클러스터로 복구를 허용하여 클라우드 비용을 낮추는 데 도움이 될 수 있습니다.

추가 정보를 찾을 수 있는 곳

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 문서 및/또는 웹사이트를 검토하세요.

- Azure NetApp Files 대한 볼륨 복제 만들기

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

- Azure NetApp Files 볼륨의 지역 간 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 환경 배포 및 구성

"Azure에 AVS 설정"

- Azure VMware 솔루션 배포 및 구성

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

Azure VMware 솔루션으로의 재해 복구를 위해 **Veeam Replication** 및 **Azure NetApp Files** 데이터 저장소 사용

Azure NetApp Files (ANF) 데이터 저장소는 스토리지를 컴퓨팅에서 분리하고 모든 조직이 워크로드를 클라우드로 이전하는 데 필요한 유연성을 제공합니다. 고객에게 컴퓨팅 리소스에 관계없이 확장 가능한 유연하고 고성능의 스토리지 인프라를 제공합니다. Azure NetApp Files 데이터 저장소는 온프레미스 VMWare 환경을 위한 재해 복구 사이트로 Azure VMware Solution(AVS)과 함께 배포를 간소화하고 최적화합니다.

개요

Azure NetApp Files (ANF) 볼륨 기반 NFS 데이터 저장소는 VM 복제 기능을 제공하는 검증된 타사 솔루션을 사용하여 온프레미스에서 데이터를 복제하는 데 사용할 수 있습니다. Azure NetApp Files 데이터 저장소를 추가하면 저장소를 수용하기 위해 엄청난 양의 ESXi 호스트를 사용하여 Azure VMware Solution SDDC를 구축하는 것보다 비용 최적화된 배포가 가능해집니다. 이런 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 장애 조치를 처리하는 데 필요한 모든 핵심 구성 요소를 갖춘 저비용 인프라를 유지하는 것입니다. 파일럿 라이트 클러스터는 장애 조치가 발생할 경우 확장이 가능하고 더 많은 AVS 호스트를 프로비저닝할 수 있습니다. 그리고 장애 조치가 완료되고 정상적인 운영이 복구되면 파일럿 라이트 클러스터는 저비용 운영 모드로 다시 축소될 수 있습니다.

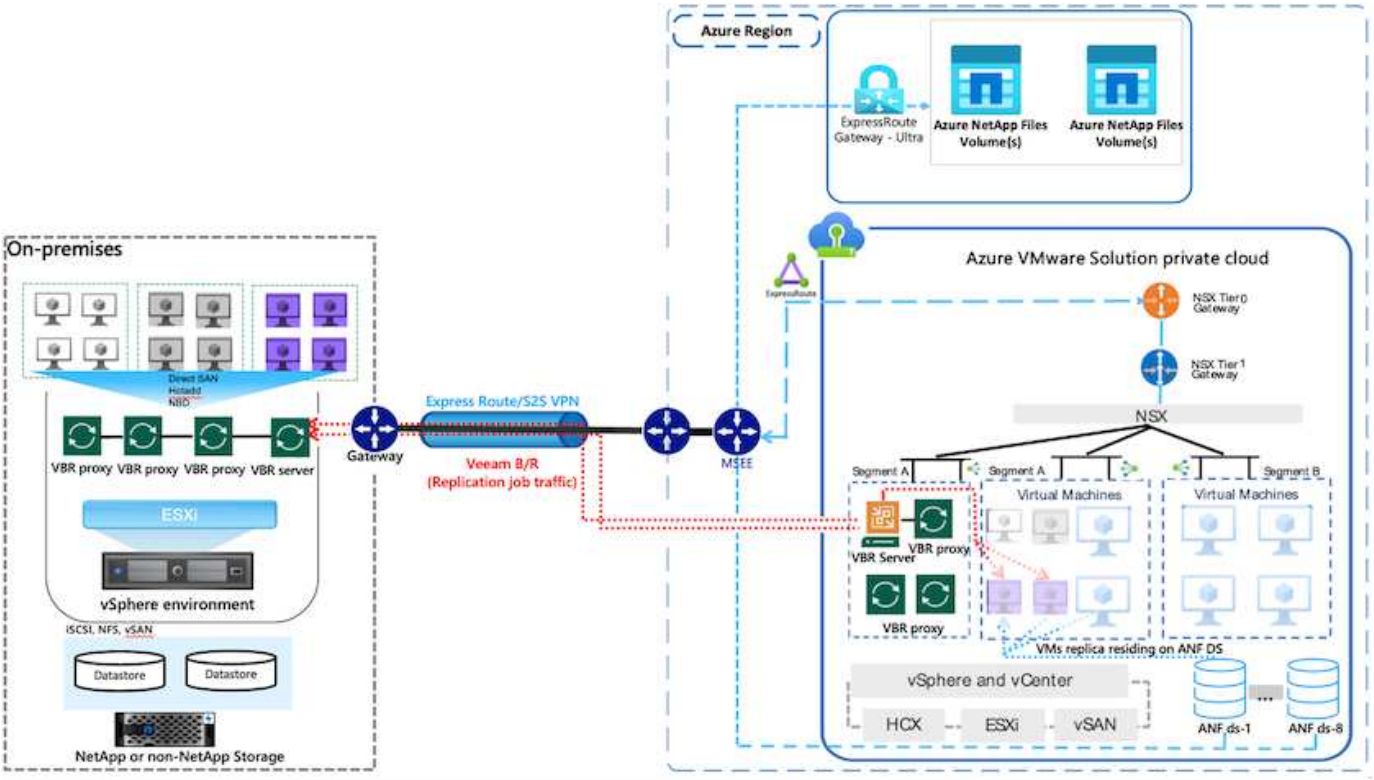
이 문서의 목적

이 문서에서는 Veeam 백업 및 복제와 함께 Azure NetApp Files 데이터 저장소를 사용하여 Veeam VM 복제 소프트웨어 기능을 사용하여 온-프레미스 VMware VM에 대한 재해 복구를 AVS(Virtual Private Network)로 설정하는 방법을 설명합니다.

Veeam Backup & Replication은 가상 환경을 위한 백업 및 복제 애플리케이션입니다. 가상 머신이 복제되면 Veeam Backup & Replication이 AVS에서 복제되고, 소프트웨어는 대상 AVS SDDC 클러스터에서 기본 VMware vSphere 형식으로 VM의 정확한 복사본을 생성합니다. Veeam Backup & Replication은 복사본을 원본 VM과 동기화된 상태로 유지합니다. 복제는 DR 사이트에 VM의 마운트된 복사본이 즉시 시작할 수 있는 상태로 존재하므로 최상의 복구 시간 목표(RTO)를 제공합니다.

이 복제 메커니즘은 재해 발생 시 AVS SDDC에서 워크로드를 신속하게 시작할 수 있도록 보장합니다. Veeam Backup & Replication 소프트웨어는 WAN 및 느린 연결을 통한 복제를 위한 트래픽 전송도 최적화합니다. 또한 중복된 데이터 블록, 0개 데이터 블록, 스왑 파일 및 "제외된 VM 게스트 OS 파일"도 필터링합니다. 해당 소프트웨어는 복제 트래픽도 압축합니다. 복제 작업이 전체 네트워크 대역폭을 소모하는 것을 방지하려면 WAN 가속기와 네트워크 제한 규칙을 활용할 수 있습니다.

Veeam Backup & Replication의 복제 프로세스는 작업 중심입니다. 즉, 복제는 복제 작업을 구성하여 수행됩니다. 재해가 발생하는 경우 복제본으로 장애 조치를 취하여 VM을 복구할 수 있습니다. 장애 조치가 수행되면 복제된 VM이 원래 VM의 역할을 대신하게 됩니다. 장애 조치는 복제본의 최신 상태나 잘 알려진 복원 지점으로 수행할 수 있습니다. 이를 통해 필요에 따라 랜섬웨어 복구나 분리된 테스트가 가능합니다. Veeam Backup & Replication은 다양한 재해 복구 시나리오를 처리하기 위한 여러 가지 옵션을 제공합니다.



솔루션 배포

높은 수준의 단계

1. Veeam Backup and Replication 소프트웨어는 적절한 네트워크 연결을 갖춘 온프레미스 환경에서 실행됩니다.
2. "Azure VMware 솔루션(AVS) 배포"프라이빗 클라우드 및"Azure NetApp Files 데이터 저장소 연결" Azure VMware Solution 호스트로.

   최소한의 구성으로 설정된 조종등 환경은 DR 목적으로 사용될 수 있습니다. 사고 발생 시 VM은 이 클러스터로 장애 조치되며, 추가 노드를 추가할 수 있습니다.

3. Veeam Backup and Replication을 사용하여 VM 복제본을 생성하기 위한 복제 작업을 설정합니다.
4. 장애 조치 계획을 수립하고 장애 조치를 수행합니다.
5. 재해 이벤트가 완료되고 기본 사이트가 가동되면 프로덕션 VM으로 다시 전환합니다.

AVS 및 **ANF** 데이터 저장소에 대한 **Veeam VM** 복제를 위한 필수 구성 요소

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

추가 정보는 "고려사항 및 제한사항"을 참조하세요."여기" .

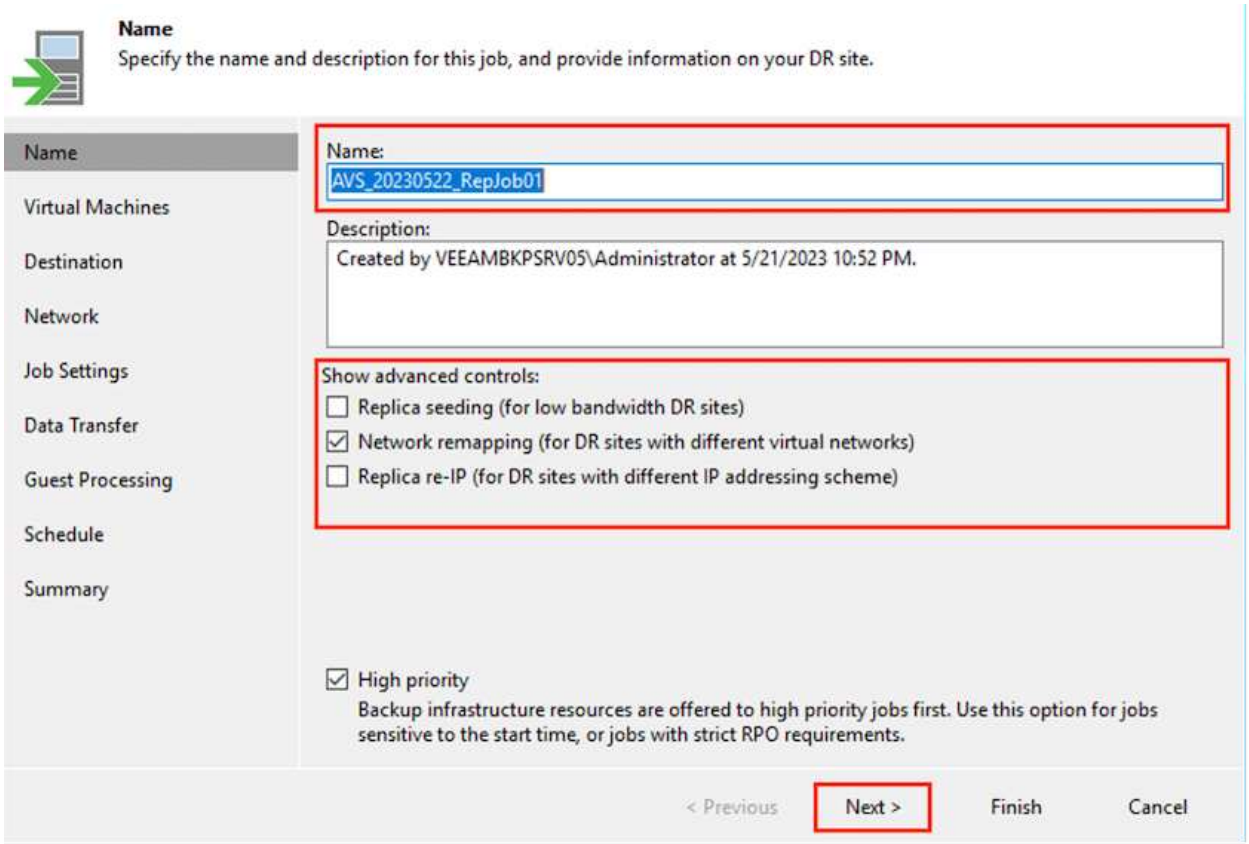
배포 세부 정보

▼ **1**단계**: VM** 복제

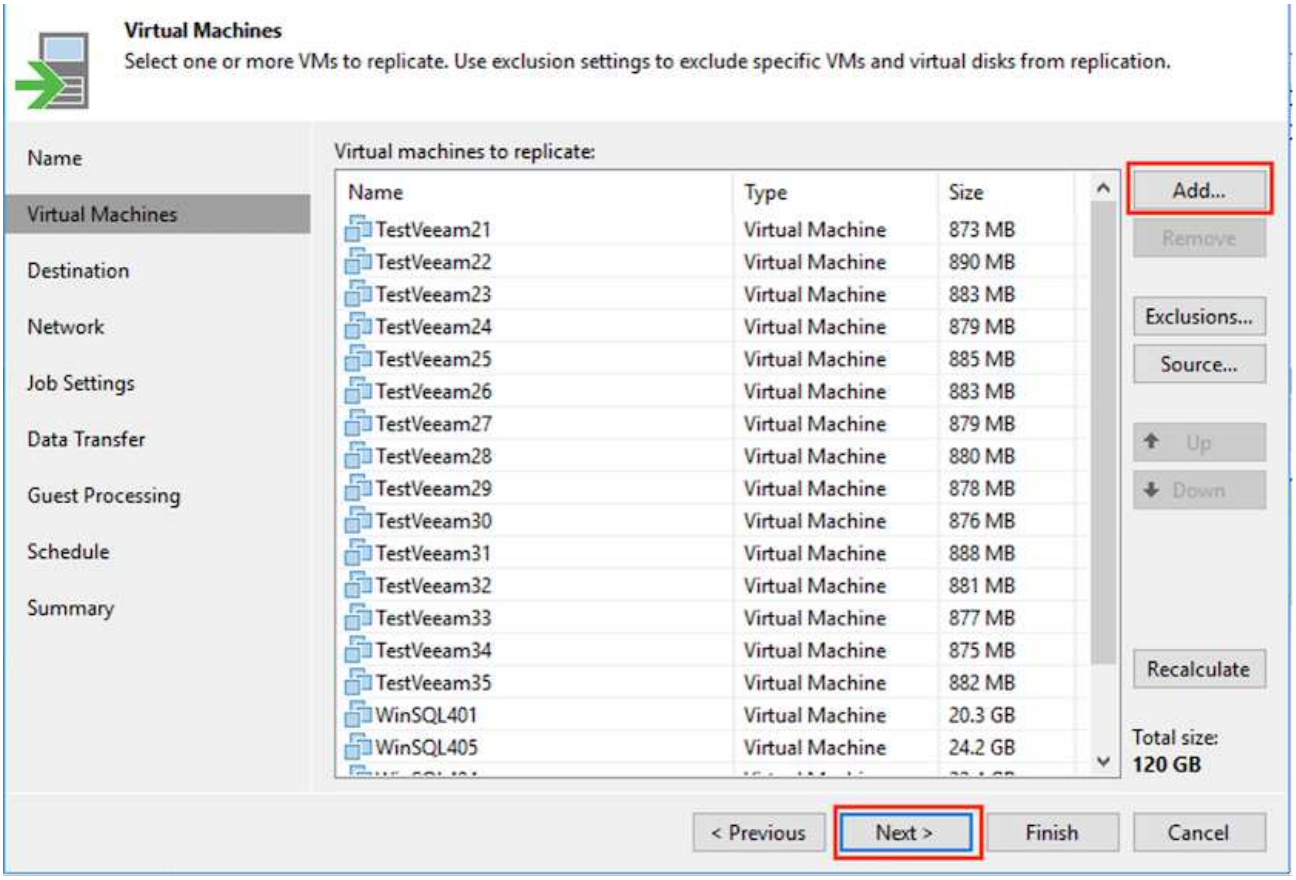
Veeam Backup & Replication은 VMware vSphere 스냅샷 기능을 활용합니다. 복제 중에 Veeam Backup & Replication은 VMware vSphere에 VM 스냅샷을 생성하도록 요청합니다. VM 스냅샷은 가상 디스크, 시스템 상태, 구성 및 메타데이터를 포함하는 VM의 특정 시점 복사본입니다. Veeam Backup & Replication은 복제를 위한 데이터 소스로 스냅샷을 사용합니다.

VM을 복제하려면 다음 단계를 따르세요.

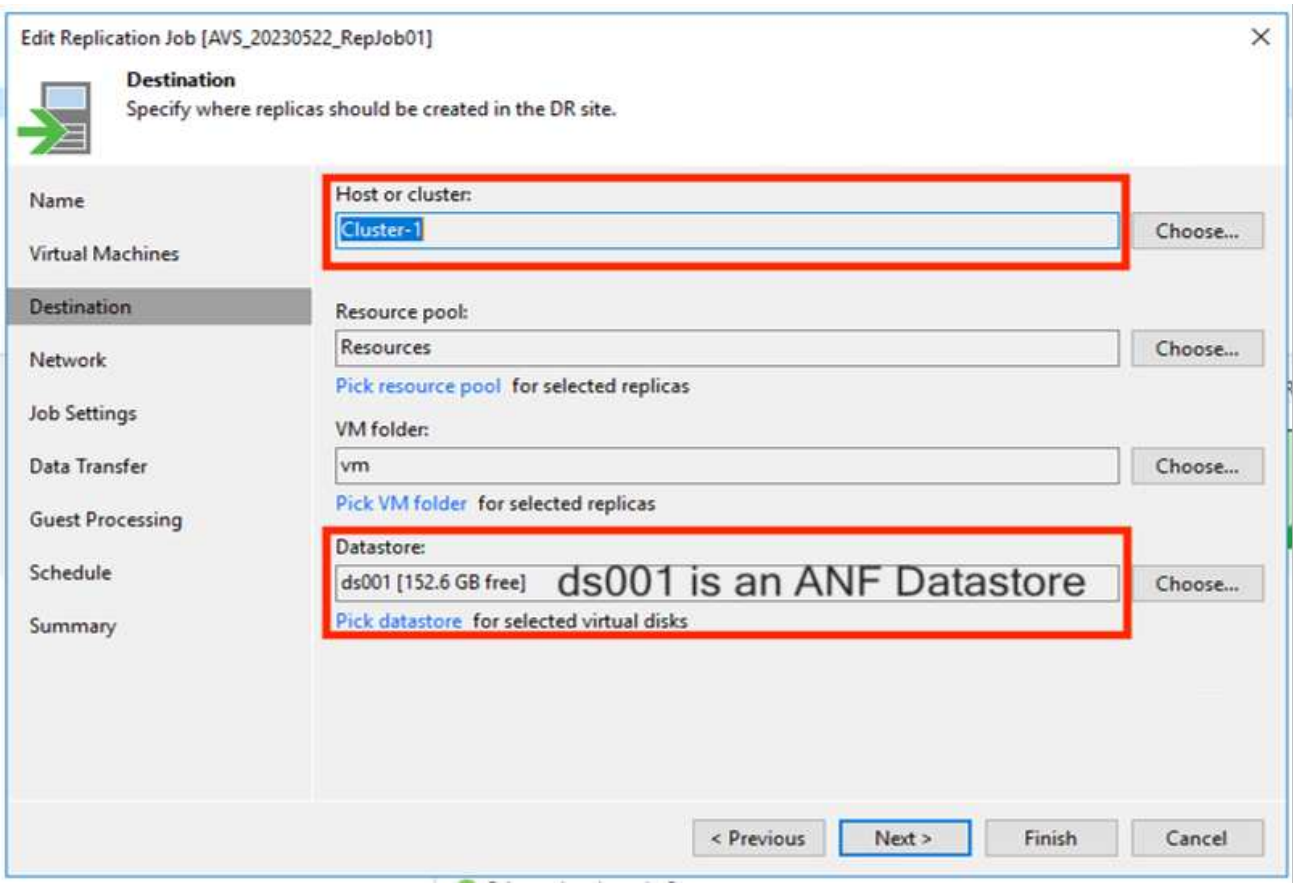
1. Veeam 백업 및 복제 콘솔을 엽니다.
2. 홈 보기에서. 작업 노드를 마우스 오른쪽 버튼으로 클릭하고 복제 작업 > 가상 머신을 선택합니다.
3. 작업 이름을 지정하고 적절한 고급 제어 확인란을 선택합니다. 다음을 클릭하세요.
   - 온-프레미스와 Azure 간 연결의 대역폭이 제한된 경우 복제본 시딩 확인란을 선택합니다. Azure VMware Solution SDDC의 세그먼트가 온-프레미스 사이트 네트워크의 세그먼트와 일치하지 않는 경우 네트워크 재매핑(다른 네트워크를 사용하는 AVS SDDC 사이트용) 확인란을 선택합니다.
   - 온프레미스 프로덕션 사이트의 IP 주소 지정 체계가 대상 AVS 사이트의 체계와 다른 경우, 복제본 재IP(IP 주소 지정 체계가 다른 DR 사이트용) 확인란을 선택합니다.



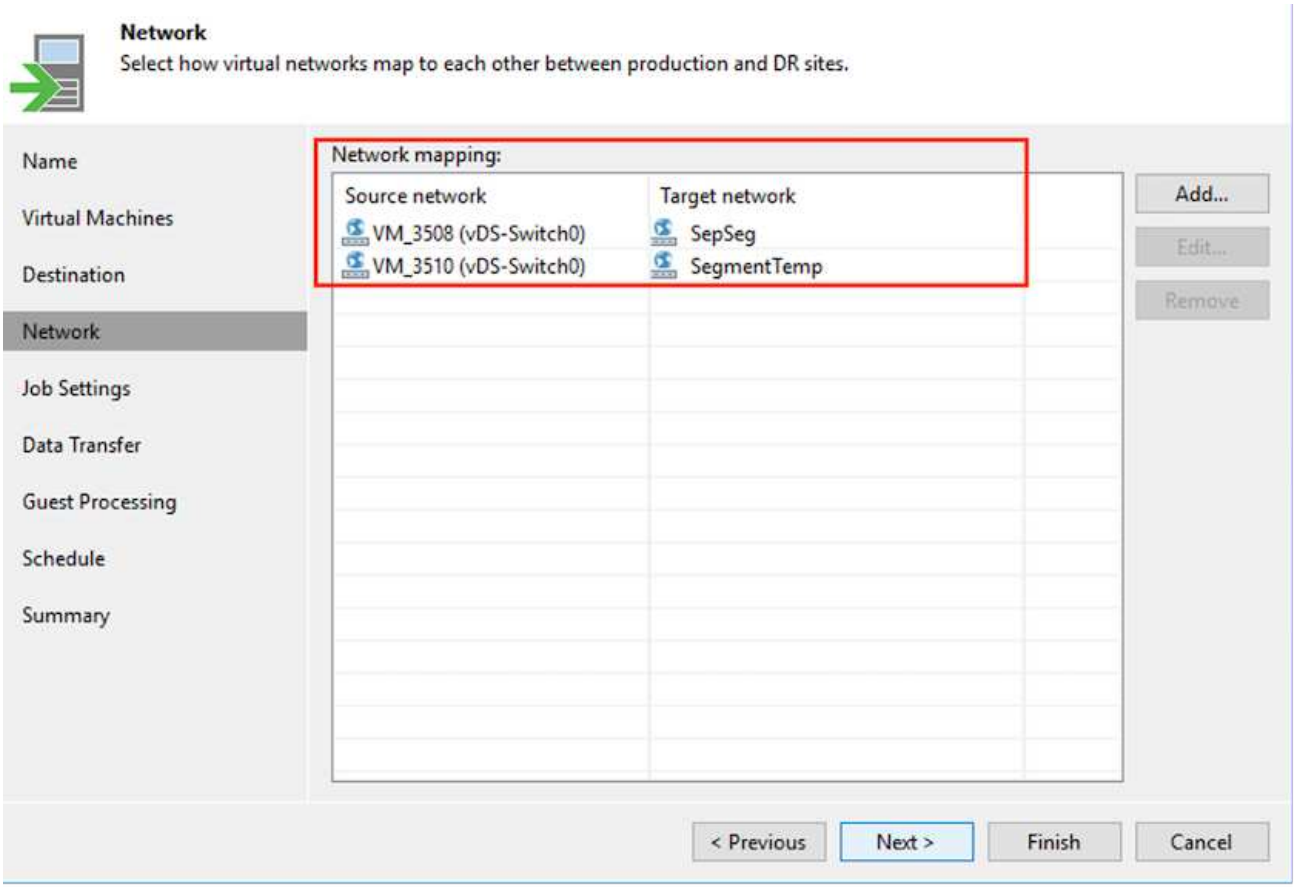
4. 가상 머신 단계에서 Azure VMware Solution SDDC에 연결된 Azure NetApp Files 데이터 저장소에 복제할 VM을 선택합니다. 가상 머신을 vSAN에 배치하여 사용 가능한 vSAN 데이터 저장소 용량을 채울 수 있습니다. 파일럿 라이트 클러스터에서는 3노드 클러스터의 사용 가능한 용량이 제한됩니다. 나머지 데이터는 Azure NetApp Files 데이터 저장소에 쉽게 저장하여 VM을 복구하고, CPU/메모리 요구 사항을 충족하도록 클러스터를 확장할 수 있습니다. 추가*를 클릭한 다음, *개체 추가 창에서 필요한 VM이나 VM 컨테이너를 선택하고 *추가*를 클릭합니다. *다음*을 클릭하세요.



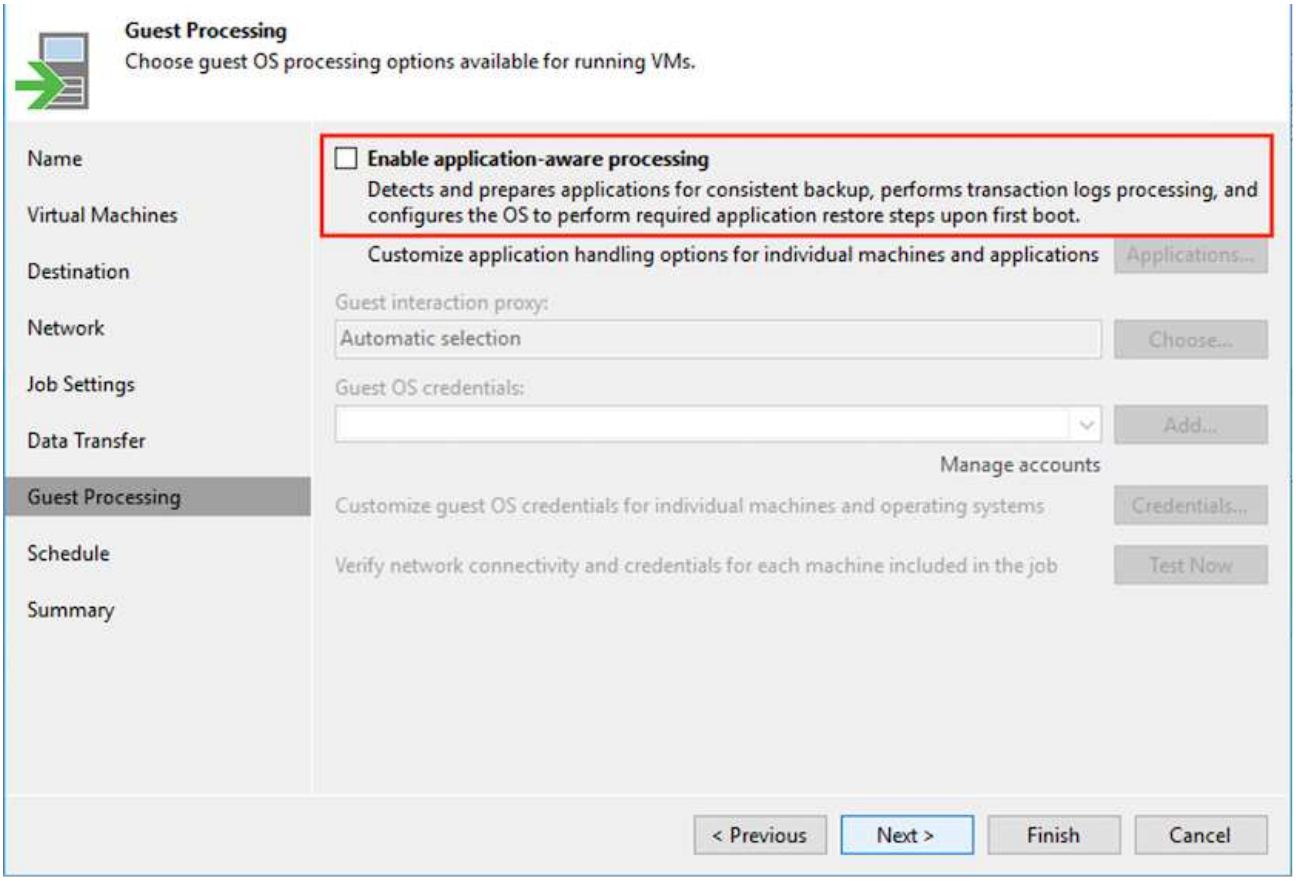
5. 그런 다음 대상을 Azure VMware Solution SDDC 클러스터/호스트로 선택하고 VM 복제본에 대한 적절한 리소스 풀, VM 폴더 및 FSx ONTAP 데이터 저장소를 선택합니다. 그런 다음 *다음*을 클릭합니다.



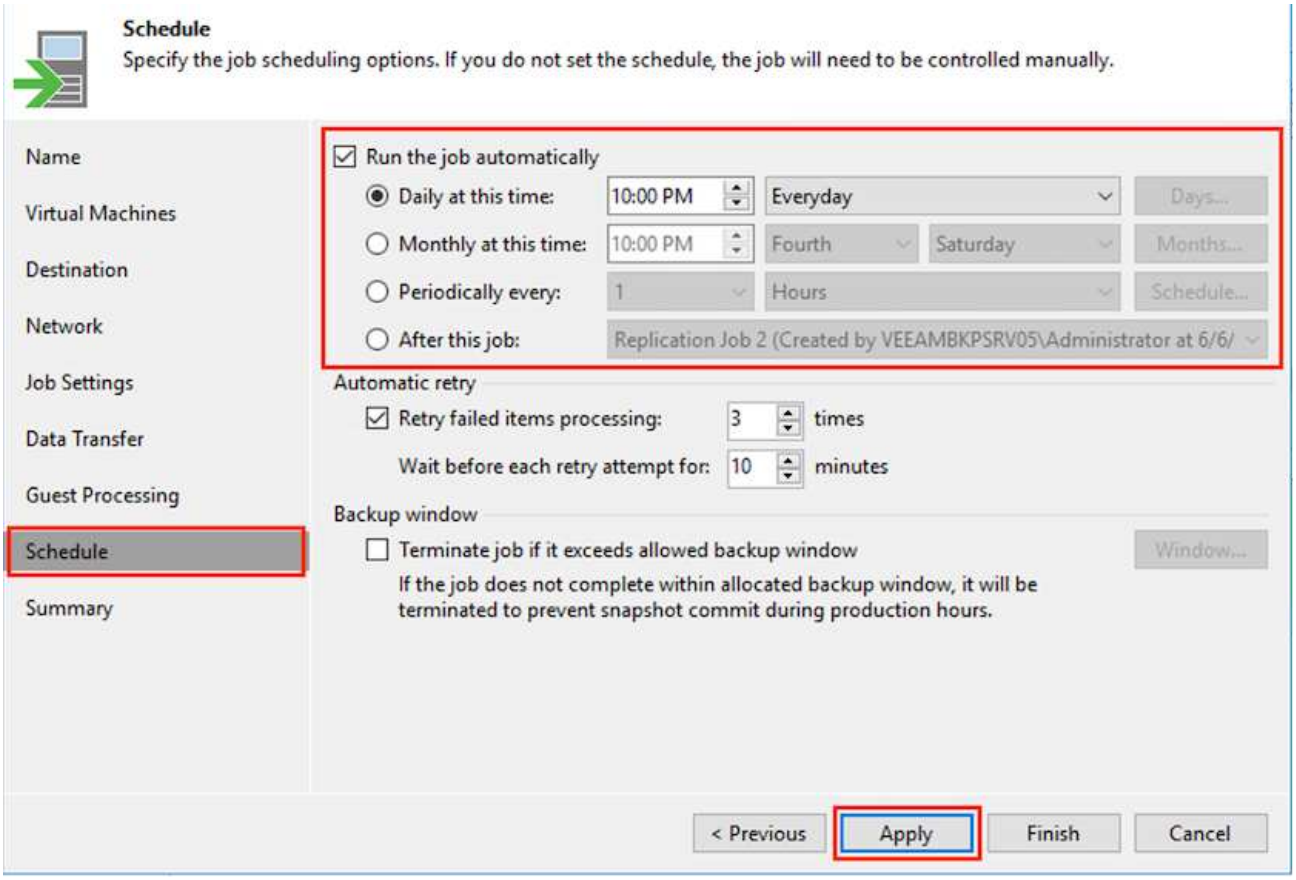
6. 다음 단계에서는 필요에 따라 소스 및 대상 가상 네트워크 간의 매핑을 만듭니다.



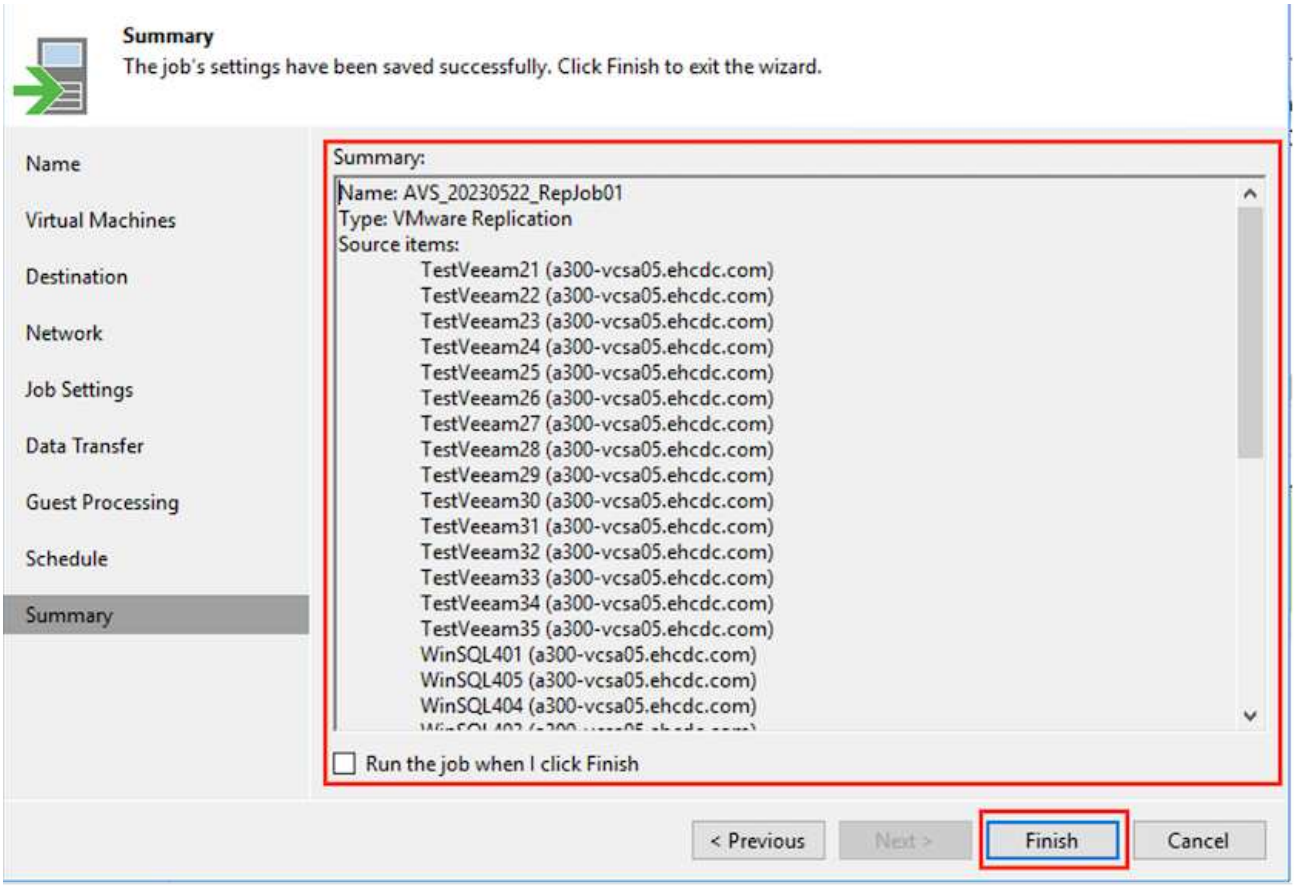
7. 작업 설정 단계에서 VM 복제본, 보존 정책 등의 메타데이터를 저장할 백업 저장소를 지정합니다.
8. 데이터 전송 단계에서 소스 및 대상 프록시 서버를 업데이트하고 자동 선택(기본값)을 그대로 두고 직접 옵션을 선택된 상태로 두고 *다음*을 클릭합니다.
9. 게스트 처리 단계에서 필요에 따라 애플리케이션 인식 처리 사용 옵션을 선택합니다. *다음*을 클릭하세요.



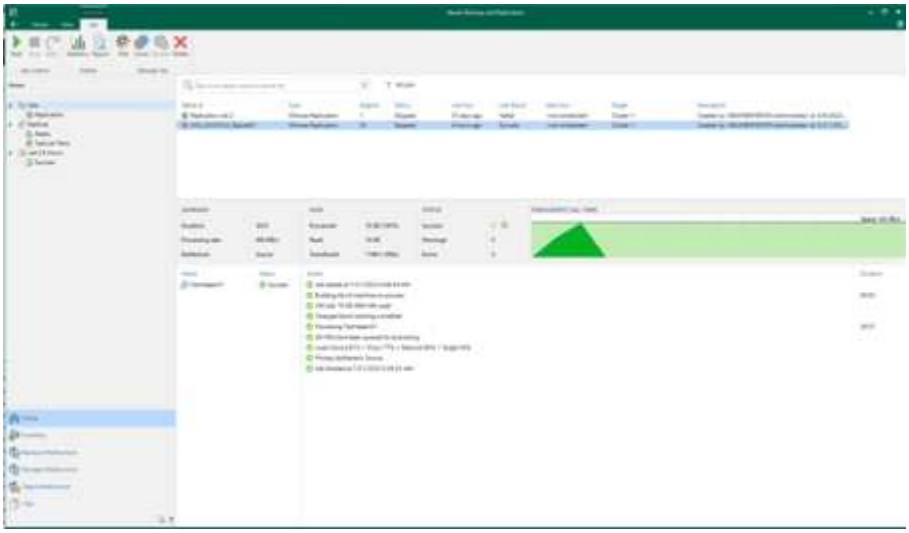
10. 정기적으로 복제 작업을 실행하려면 복제 일정을 선택하세요.



11. 마법사의 요약 단계에서 복제 작업의 세부 정보를 검토합니다. 마법사를 닫은 직후 작업을 시작하려면 마침을 클릭하면 작업 실행 확인란을 선택하고, 그렇지 않으면 확인란을 선택하지 않습니다. 그런 다음 *마침*을 클릭하여 마법사를 닫습니다.



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



Veeam 복제에 대한 추가 정보는 다음을 참조하세요."복제 작동 방식"

▼ **2**단계**:** 장애 조치 계획 만들기

초기 복제 또는 시딩이 완료되면 장애 조치 계획을 만듭니다. 장애 조치 계획은 종속된 VM에 대해 하나씩 또는 그룹별로 자동으로 장애 조치를 수행하는 데 도움이 됩니다. 장애 조치 계획은 부팅 지연을 포함하여 VM이 처리되는 순서에 대한 청사진입니다. 장애 조치 계획은 또한 중요한 종속 VM이 이미 실행 중인지 확인하는 데 도움이 됩니다.

계획을 생성하려면 *복제본*이라는 새 하위 섹션으로 이동하여 *장애 조치 계획*을 선택합니다. 적절한 VM을 선택하세요. Veeam Backup & Replication은 이 시점에 가장 가까운 복원 지점을 찾아 이를 사용하여 VM 복제본을

시작합니다.

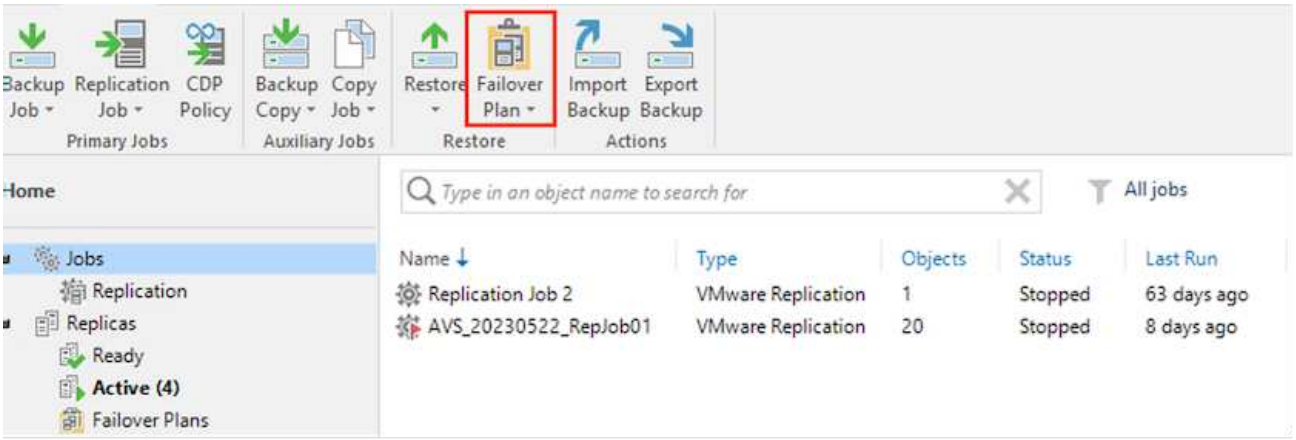
장애 조치 계획은 초기 복제가 완료되고 VM 복제본이 준비 상태가 된 후에만 추가할 수 있습니다.

장애 조치 계획을 실행할 때 동시에 시작할 수 있는 최대 VM 수는 10개입니다.

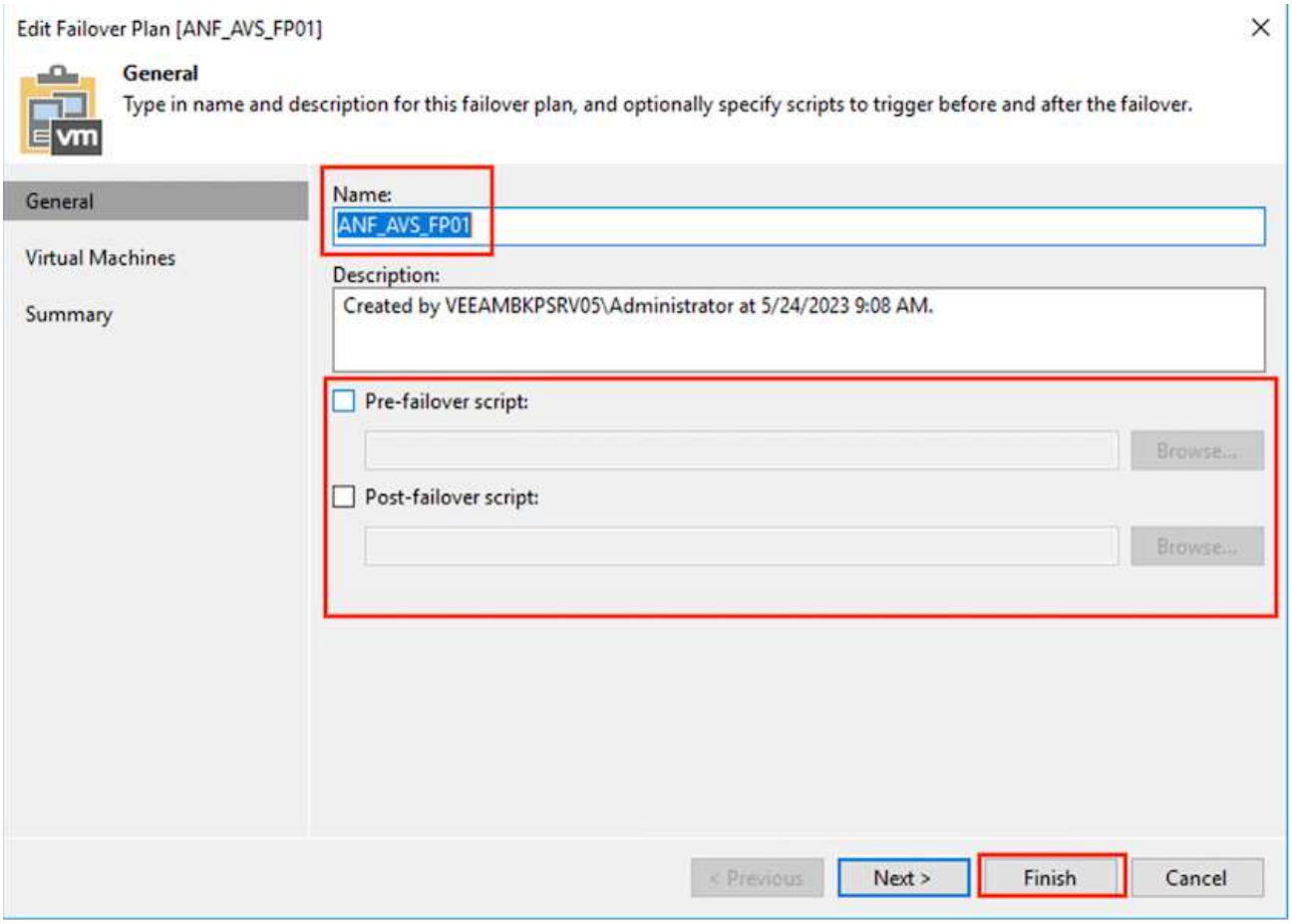
장애 조치 프로세스 동안 소스 VM의 전원이 꺼지지 않습니다.

*장애 조치 계획*을 생성하려면 다음을 수행하세요.

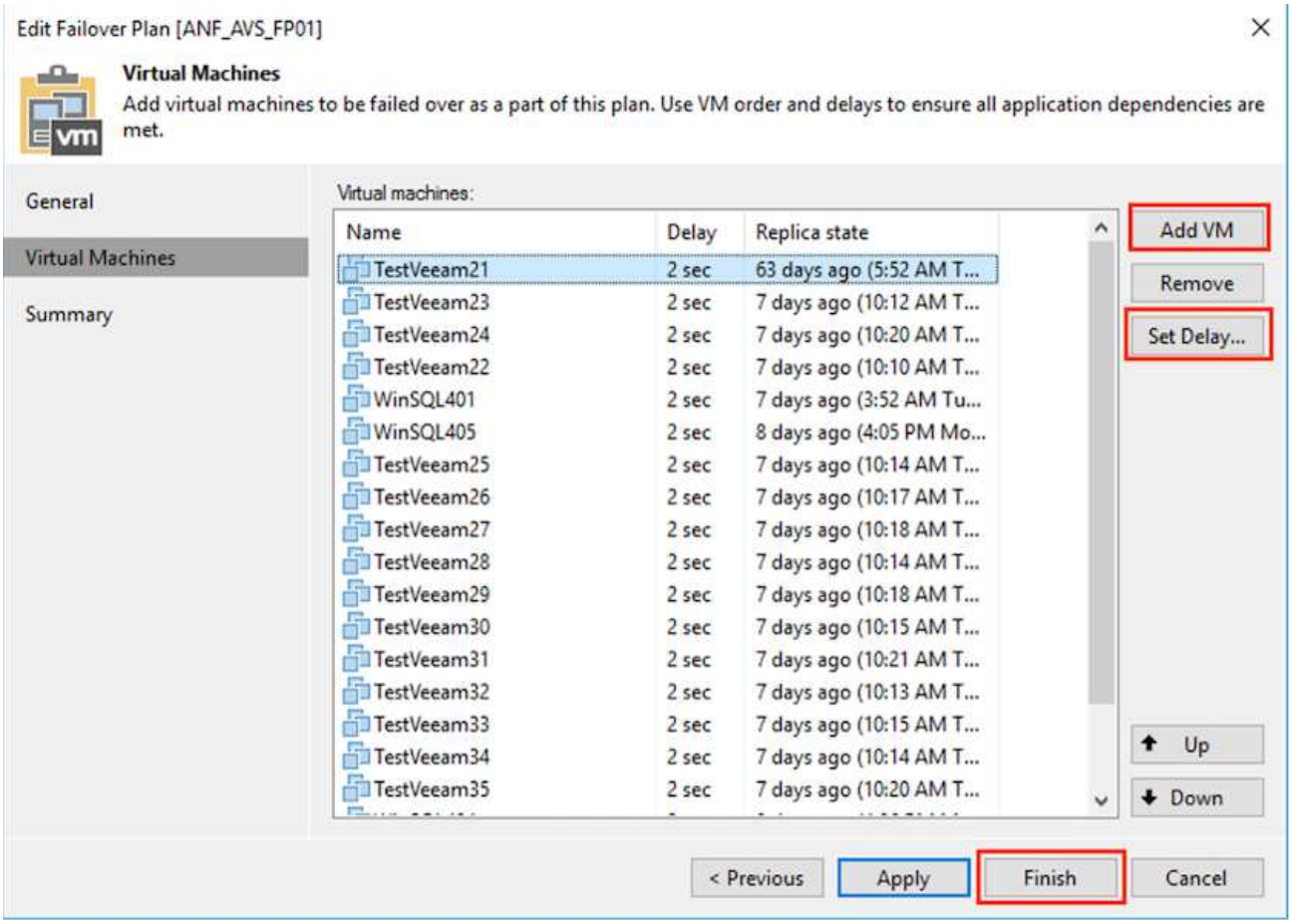
1. 홈 보기에서. 복제본 노드를 마우스 오른쪽 버튼으로 클릭하고 장애 조치 계획 > 장애 조치 계획 > VMware vSphere를 선택합니다.



2. 다음으로 계획의 이름과 설명을 입력하세요. 필요에 따라 사전 및 사후 장애 조치 스크립트를 추가할 수 있습니다. 예를 들어, 복제된 VM을 시작하기 전에 VM을 종료하는 스크립트를 실행합니다.



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



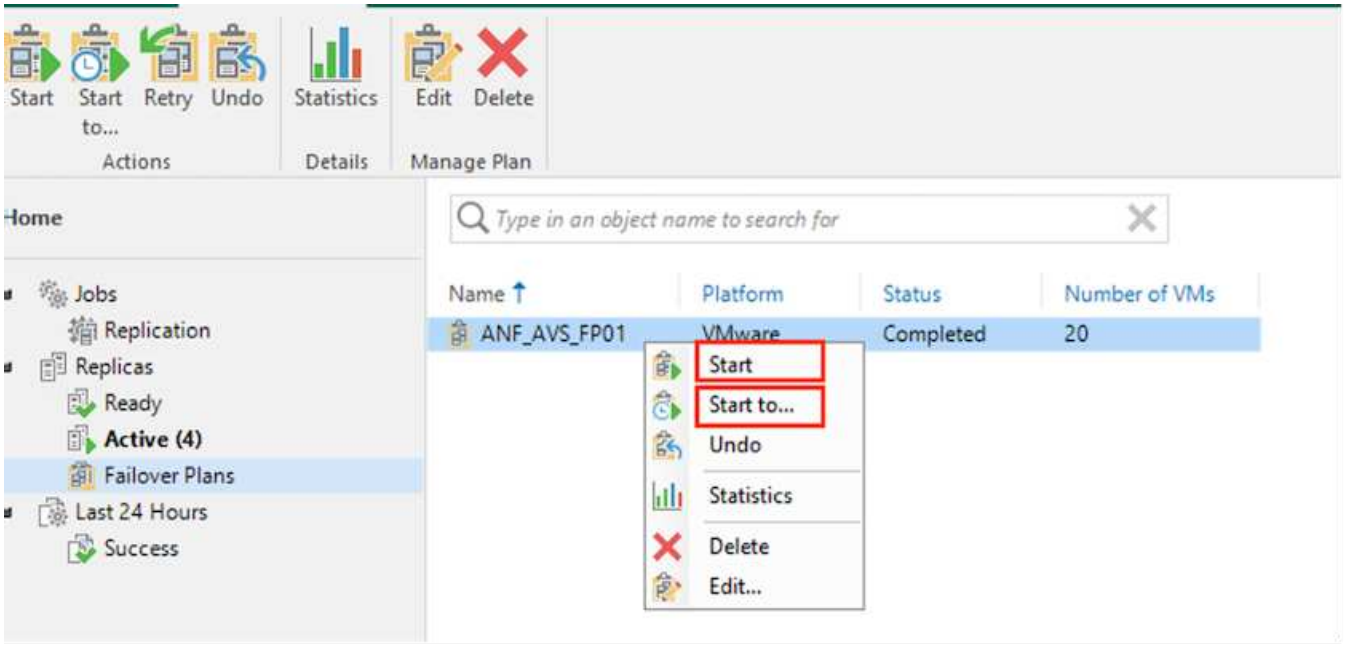
복제 작업 생성에 대한 추가 정보는 다음을 참조하세요."복제 작업 생성" .

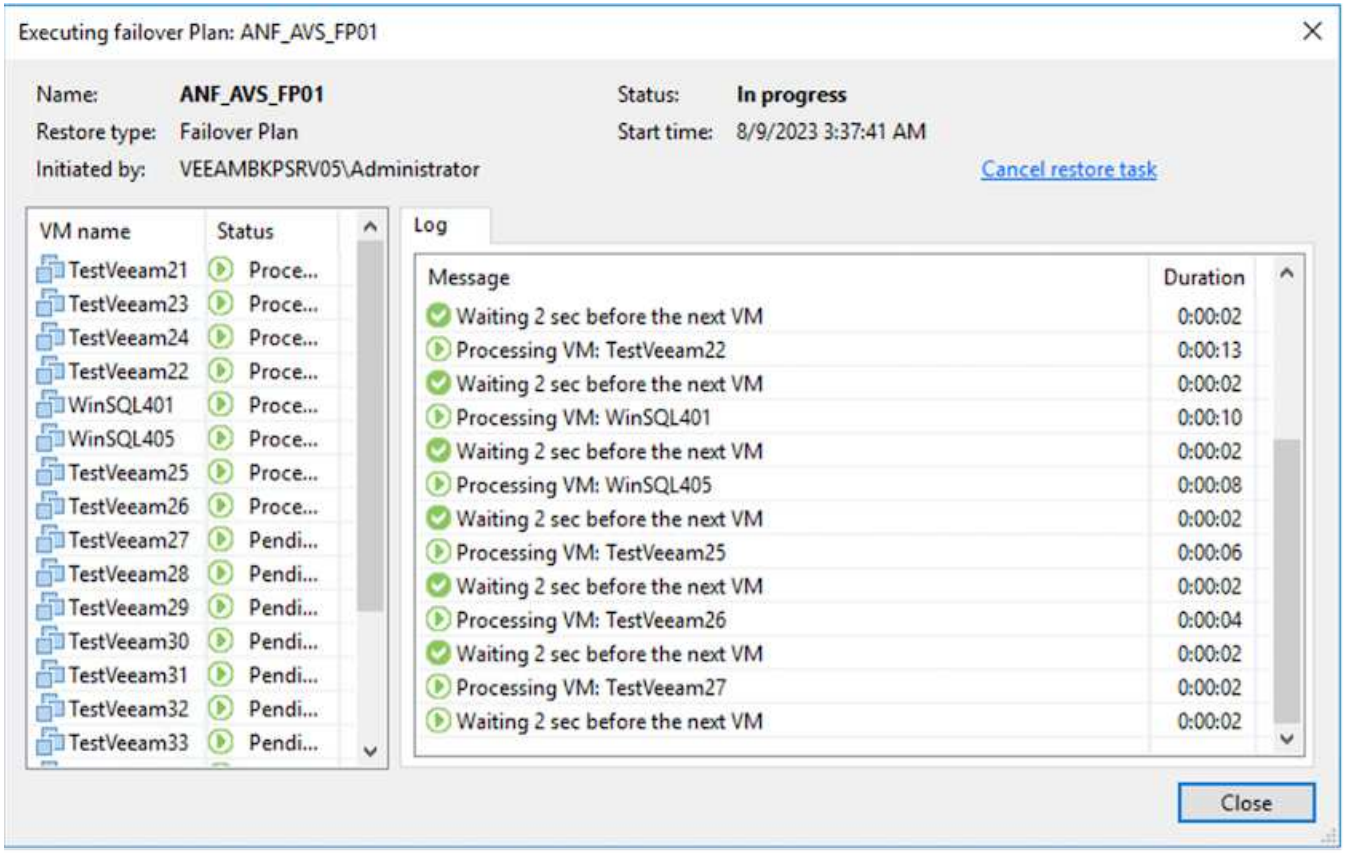
▼ **3**단계**:** 장애 조치 계획 실행

장애 조치(failover) 중에 프로덕션 사이트의 소스 VM은 재해 복구 사이트의 복제본으로 전환됩니다. 장애 조치 프로세스의 일부로 Veeam Backup & Replication은 VM 복제본을 필요한 복구 지점으로 복원하고 모든 I/O 활동을 소스 VM에서 복제본으로 이동합니다. 복제본은 재난 발생 시뿐만 아니라 DR 훈련을 시뮬레이션하는 데에도 사용할 수 있습니다. 장애 조치 시뮬레이션 중에 소스 VM은 계속 실행됩니다. 필요한 모든 테스트가 수행되면 장애 조치를 취소하고 정상적인 작업으로 돌아갈 수 있습니다.

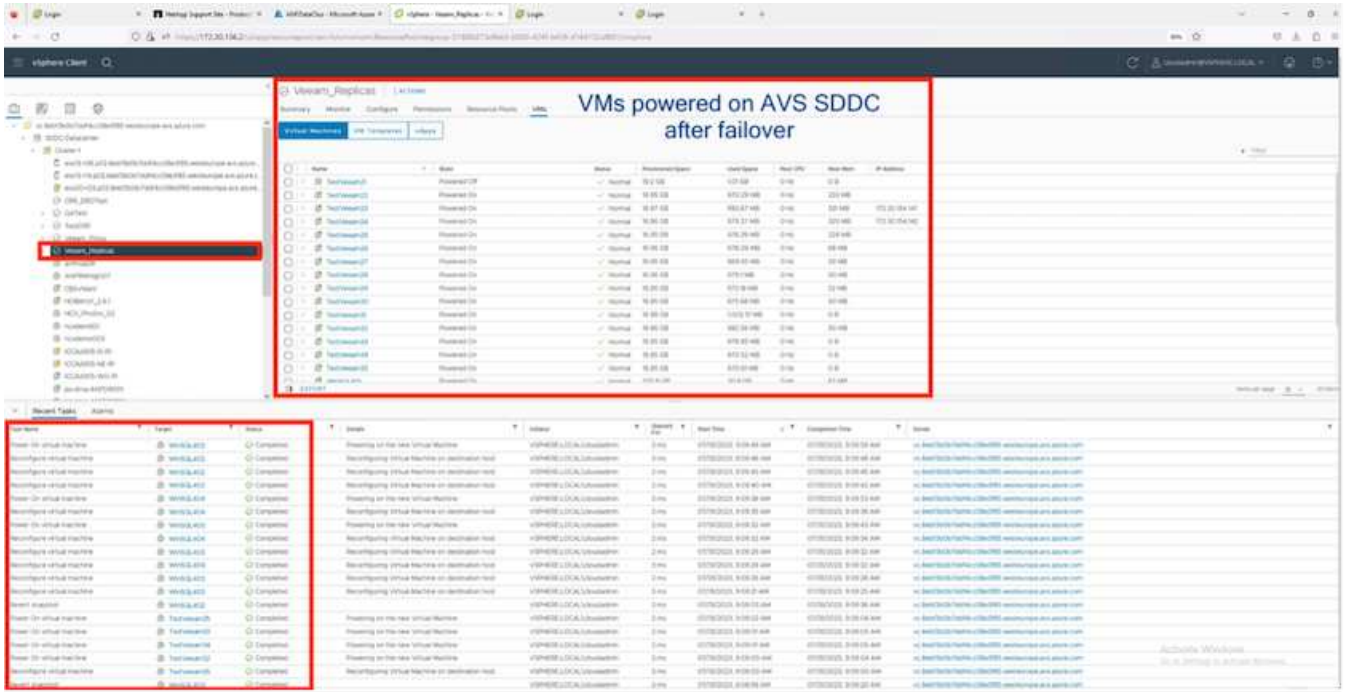
장애 조치 중 IP 충돌을 피하기 위해 네트워크 분할이 제대로 되어 있는지 확인하세요.

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

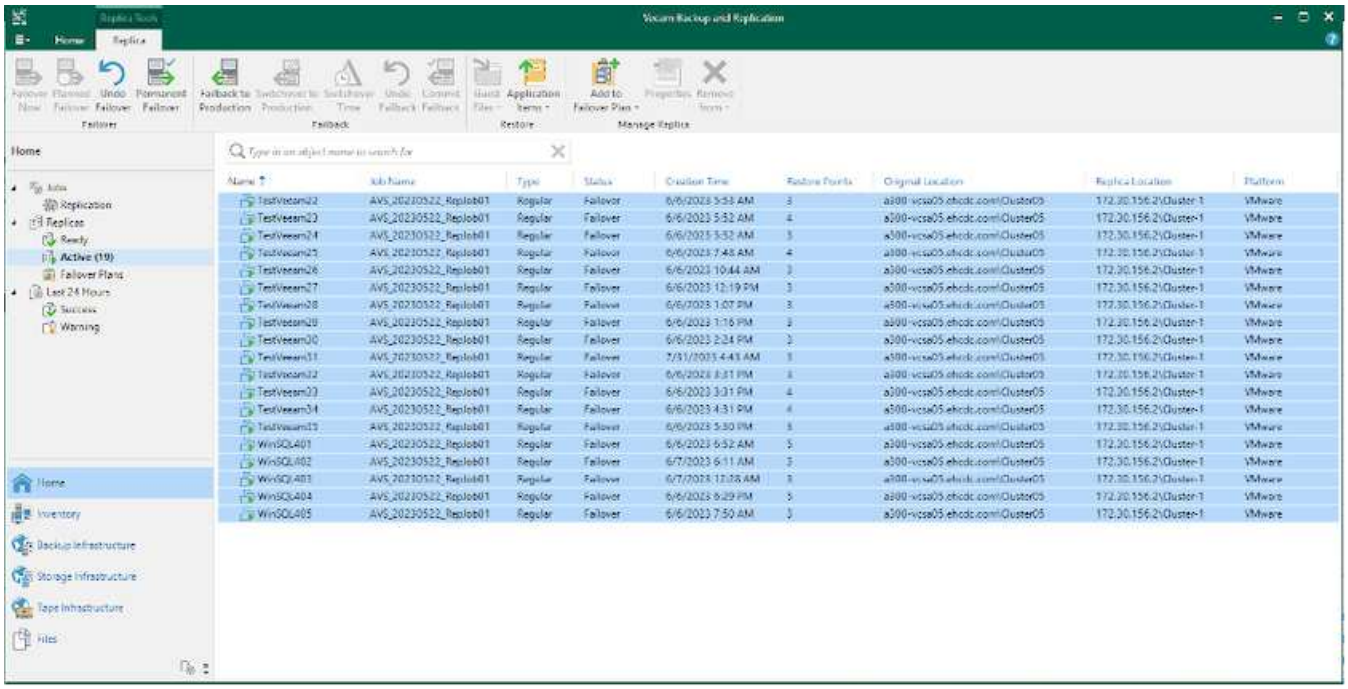




VM 복제본 상태가 준비에서 장애 조치로 변경되고 VM이 대상 Azure VMware Solution(AVS) SDDC 클러스터 /호스트에서 시작됩니다.



장애 조치가 완료되면 VM 상태가 "장애 조치"로 변경됩니다.



Veeam Backup & Replication은 복제본이 준비 상태로 돌아올 때까지 소스 VM에 대한 모든 복제 활동을 중지합니다.

장애 조치 계획에 대한 자세한 내용은 다음을 참조하세요."장애 조치 계획" .

▼ **4**단계**:** 프로덕션 사이트로 장애 복구

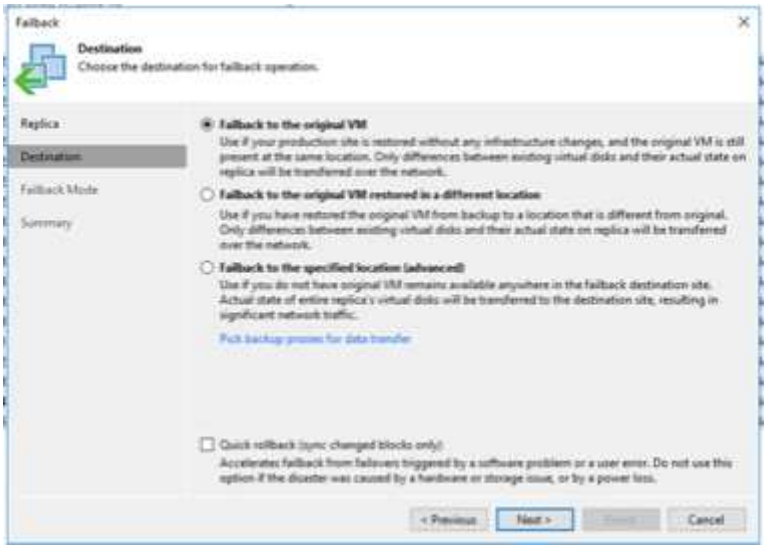
장애 조치 계획이 실행 중일 때는 중간 단계로 간주되며 요구 사항에 따라 마무리되어야 합니다. 옵션은 다음과 같습니다.

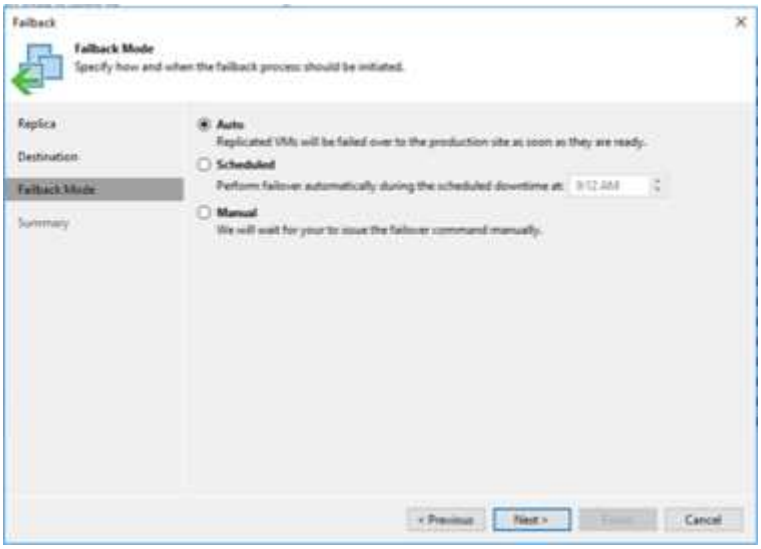
- 운영 환경으로의 장애 복구 - 원래 VM으로 다시 전환하고 VM 복제본이 실행되는 동안 발생한 모든 변경 사항을 원래 VM으로 전송합니다.

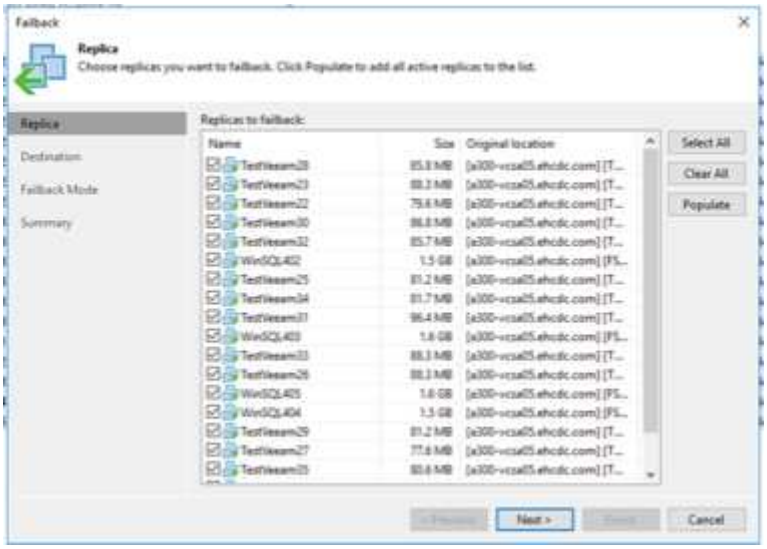
> 장애 복구를 수행하면 변경 사항은 전송만 되고 게시되지는 않습니다. 원래 VM이 예상대로 작동하는 것이 확인되면 *페일백 커밋*을 선택하고, 원래 VM이 예상대로 작동하지 않는 경우 VM 복제본으로 돌아가려면 페일백 실행 취소를 선택합니다.

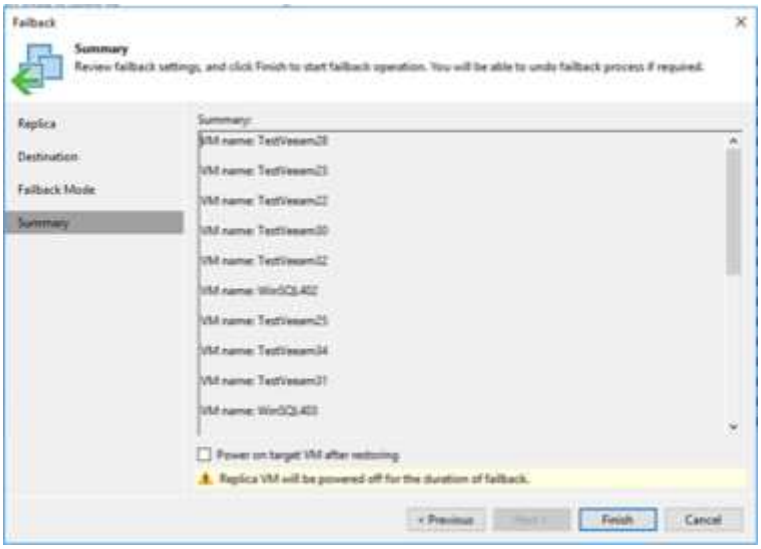
- 장애 조치 취소 - 원래 VM으로 다시 전환하고 실행 중이던 VM 복제본에 적용된 모든 변경 사항을 취소합니다.
- 영구적 장애 조치 - 원본 VM에서 VM 복제본으로 영구적으로 전환하고 이 복제본을 원본 VM으로 사용합니다.

이 데모에서는 프로덕션으로의 장애 복구가 선택되었습니다. 마법사의 대상 단계에서 원래 VM으로의 장애 복구가 선택되었고 "복원 후 VM 전원 켜기" 확인란이 활성화되었습니다.



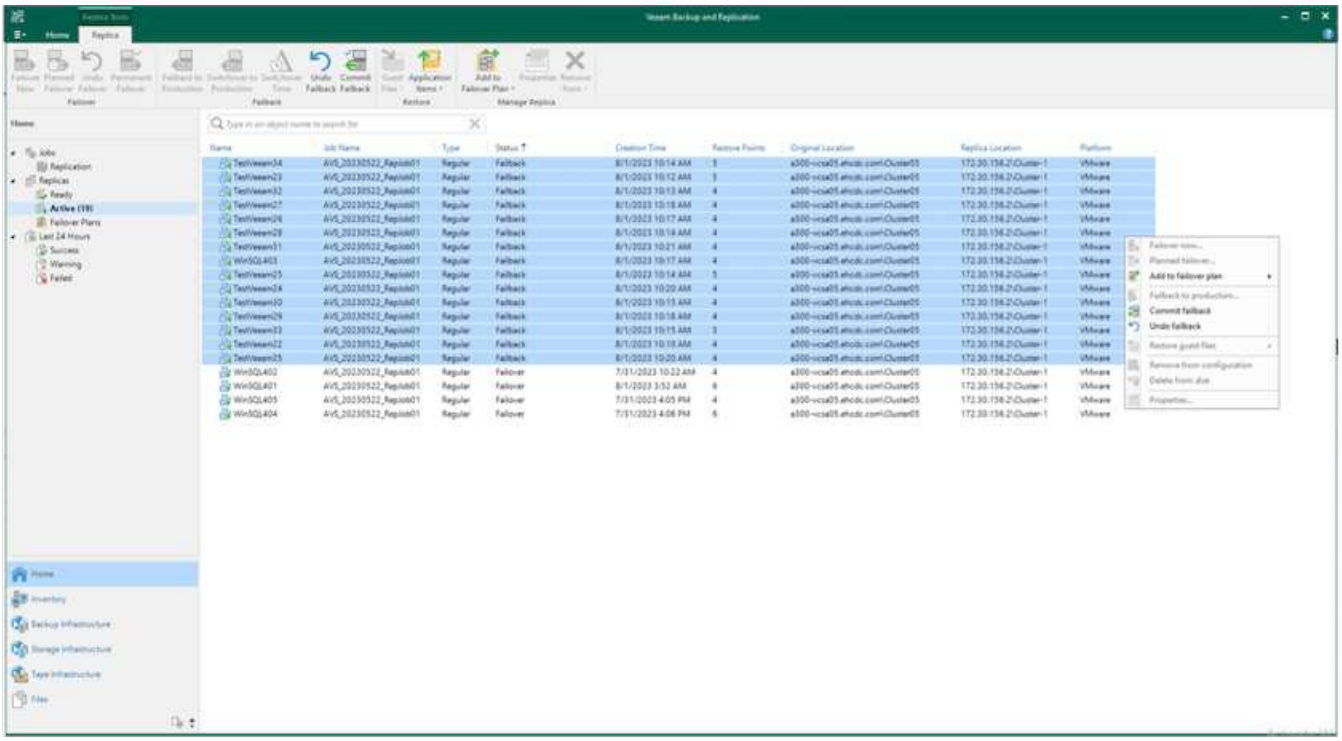




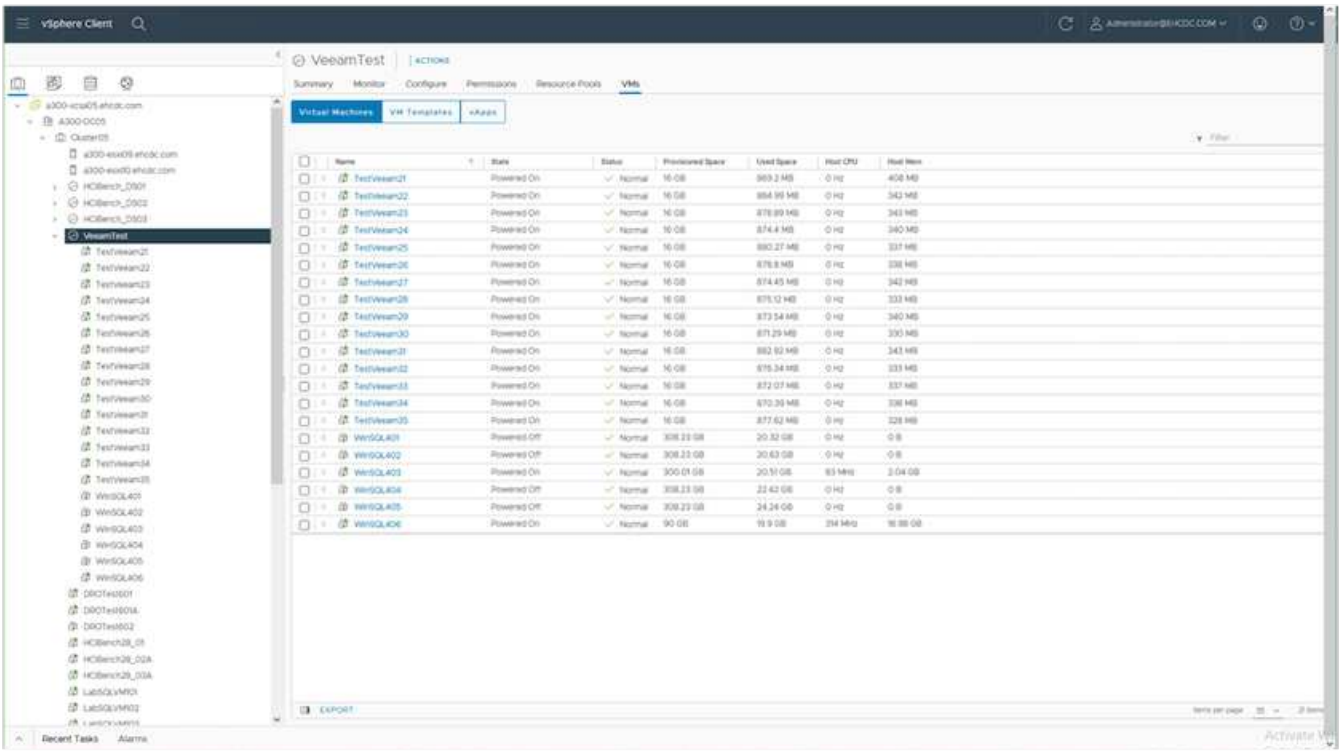


장애 복구 커밋은 장애 복구 작업을 마무리하는 방법 중 하나입니다. 장애 복구가 커밋되면 장애 복구된 VM(프로덕션 VM)에 전송된 변경 사항이 예상대로 작동하는지 확인됩니다. 커밋 작업 후 Veeam Backup & Replication은 프로덕션 VM에 대한 복제 활동을 재개합니다.

장애 복구 프로세스에 대한 자세한 내용은 Veeam 설명서를 참조하세요."복제를 위한 장애 조치 및 장애 복구" .



운영 환경으로의 장애 복구가 성공적으로 완료되면 모든 VM이 원래 운영 사이트로 복원됩니다.



결론

Azure NetApp Files 데이터 저장소 기능을 사용하면 Veeam이나 검증된 타사 도구가 VM 복제본만을 수용하기 위해 대규모 클러스터를 구축하는 대신 파일럿 라이트 클러스터를 활용하여 저비용 DR 솔루션을 제공할 수 있습니다. 이를 통해 맞춤형 재해 복구 계획을 효과적으로 처리하고 사내 기존 백업 제품을 재해 복구에 재사용하여 사내 재해 복구 데이터 센터를 종료하고 클라우드 기반 재해 복구를 구현할 수 있습니다. 재해 발생 시 버튼을 클릭하여 장애 조치를 취하거나 재해가 발생하면 자동으로 장애 조치를 취할 수 있습니다.

이 과정에 대해 자세히 알아보려면 자세한 안내 영상을 시청하세요.

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

Azure/AVS에서 워크로드 마이그레이션

TR-4940: VMware HCX를 사용하여 워크로드를 Azure NetApp Files 데이터 저장소로 마이그레이션 - 빠른 시작 가이드

Azure VMware Solution 및 Azure NetApp Files 데이터 저장소의 가장 일반적인 사용 사례 중 하나는 VMware 워크로드의 마이그레이션입니다. VMware HCX는 선호되는 옵션으로, 온-프레미스 가상 머신(VM)과 해당 데이터를 Azure NetApp Files 데이터 저장소로 옮기는 다양한 마이그레이션 메커니즘을 제공합니다.

개요: VMware HCX, Azure NetApp Files 데이터 저장소 및 Azure VMware 솔루션을 사용하여 가상 머신 마이그레이션

VMware HCX는 기본적으로 애플리케이션 마이그레이션, 워크로드 리밸런싱, 심지어 클라우드 전반의 비즈니스 연속성을 단순화하도록 설계된 마이그레이션 플랫폼입니다. Azure VMware Solution Private Cloud의 일부로 포함되어 있으며 워크로드를 마이그레이션하는 다양한 방법을 제공하며 재해 복구(DR) 작업에 사용할 수 있습니다.

이 문서에서는 Azure NetApp Files 데이터 저장소를 프로비저닝하고, 온프레미스와 Azure VMware 솔루션 측의 모든 주요 구성 요소를 포함하여 VMware HCX를 다운로드, 배포 및 구성하는 방법에 대한 단계별 지침을 제공합니다. 여기에는 다양한 VM 마이그레이션 메커니즘을 활성화하기 위한 상호 연결, 네트워크 확장 및 WAN 최적화가 포함됩니다.



VMware HCX는 마이그레이션이 VM 수준에서 진행되므로 모든 데이터 저장소 유형과 호환됩니다. 따라서 이 문서는 기존 NetApp 고객과 비용 효율적인 VMware 클라우드 배포를 위해 Azure VMware Solution과 함께 Azure NetApp Files 배포할 계획인 비 NetApp 고객에게 적용됩니다.

▼ 상위 수준 단계

이 목록은 Azure 클라우드 측에 HCX Cloud Manager를 설치 및 구성하고 온프레미스에 HCX Connector를 설치하는 데 필요한 개략적인 단계를 제공합니다.

1. Azure Portal을 통해 HCX를 설치합니다.
2. 온프레미스 VMware vCenter Server에 HCX Connector Open Virtualization Appliance(OVA) 설치 프로그램을 다운로드하여 배포합니다.
3. 라이선스 키로 HCX를 활성화하세요.
4. 온프레미스 VMware HCX Connector를 Azure VMware Solution HCX Cloud Manager와 연결합니다.
5. 네트워크 프로필, 컴퓨팅 프로필 및 서비스 메시를 구성합니다.
6. (선택 사항) 마이그레이션 중에 재IP를 방지하기 위해 네트워크 확장을 수행합니다.
7. 기기 상태를 검증하고 마이그레이션이 가능한지 확인하세요.
8. VM 워크로드를 마이그레이션합니다.

▼ 필수 조건

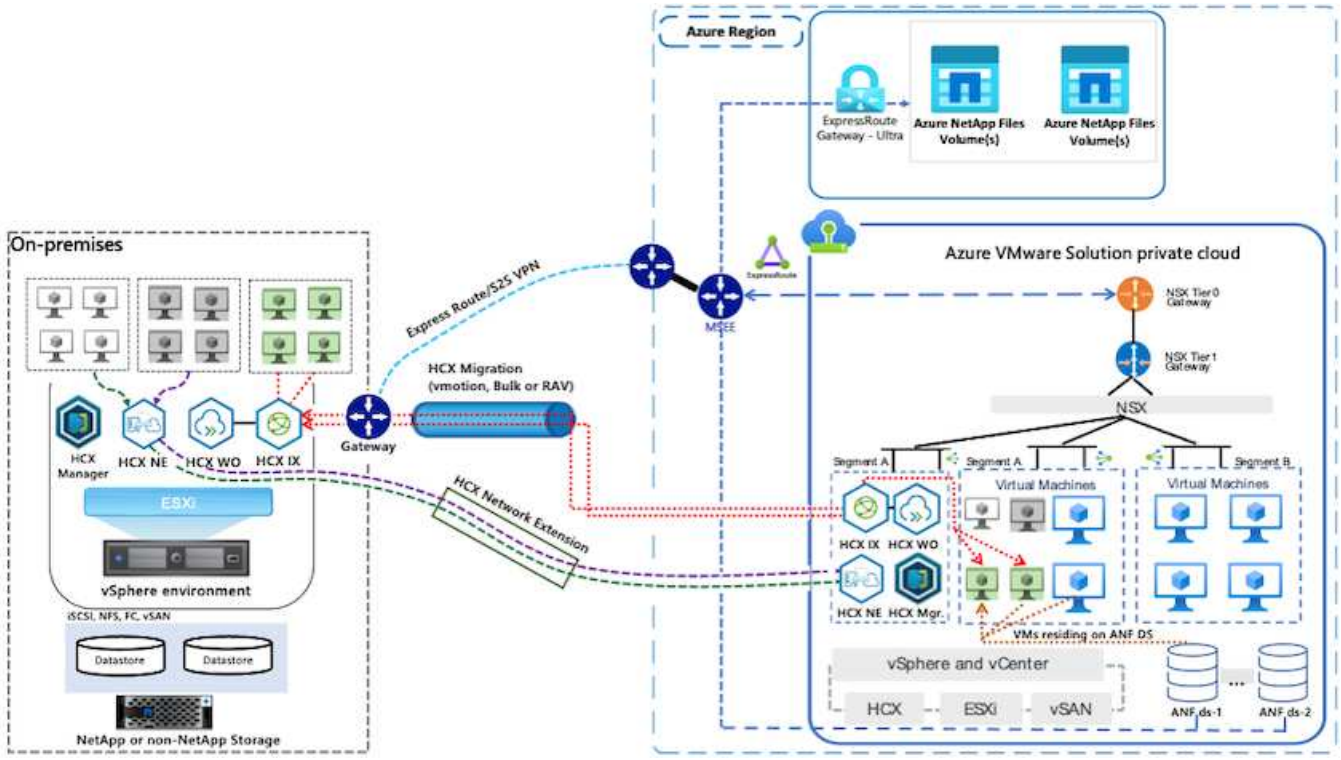
시작하기 전에 다음 전제 조건이 충족되었는지 확인하세요. 자세한 내용은 다음을 참조하세요. "링크" . 연결성을 포함한 필수 구성 요소가 준비되면 Azure VMware Solution 포털에서 라이선스 키를 생성하여 HCX를 구성하고 활성화합니다. OVA 설치 프로그램을 다운로드한 후 아래 설명된 대로 설치 과정을 진행하세요.

HCX Advanced가 기본 옵션이며, VMware HCX Enterprise Edition도 지원 티켓을 통해 이용 가능하며 추가 비용 없이 지원됩니다.

- 기존 Azure VMware 솔루션 소프트웨어 정의 데이터 센터(SDDC)를 사용하거나 이를 사용하여 프라이빗 클라우드를 만듭니다."NetApp 링크" 아니면 이것 "마이크로소프트 링크" .
- 온프레미스 VMware vSphere 지원 데이터 센터에서 VM 및 관련 데이터를 마이그레이션하려면 데이터 센터에서 SDDC 환경으로의 네트워크 연결이 필요합니다. 워크로드를 마이그레이션하기 전에 "사이트 간 VPN 또는 Express Route Global Reach 연결을 설정하세요" 온프레미스 환경과 해당 프라이빗 클라우드 간.
- 온프레미스 VMware vCenter Server 환경에서 Azure VMware Solution 프라이빗 클라우드로의 네트워크 경로는 vMotion을 사용하여 VM 마이그레이션을 지원해야 합니다.
- 필수 사항을 확인하세요 "방화벽 규칙 및 포트" 온프레미스 vCenter Server와 SDDC vCenter 간의 vMotion 트래픽이 허용됩니다. 프라이빗 클라우드에서는 vMotion 네트워크의 라우팅이 기본적으로 구성됩니다.
- Azure NetApp Files NFS 볼륨은 Azure VMware Solution의 데이터 저장소로 마운트되어야 합니다. 여기에 자세히 설명된 단계를 따르세요. "링크" Azure NetApp Files 데이터 저장소를 Azure VMware Solutions 호스트에 연결합니다.

▼ 고수준 아키텍처

테스트 목적으로, 이 검증에 사용된 온프레미스 랩 환경은 사이트 간 VPN을 통해 연결되었으며, 이를 통해 온프레미스에서 Azure VMware Solution으로 연결할 수 있습니다.



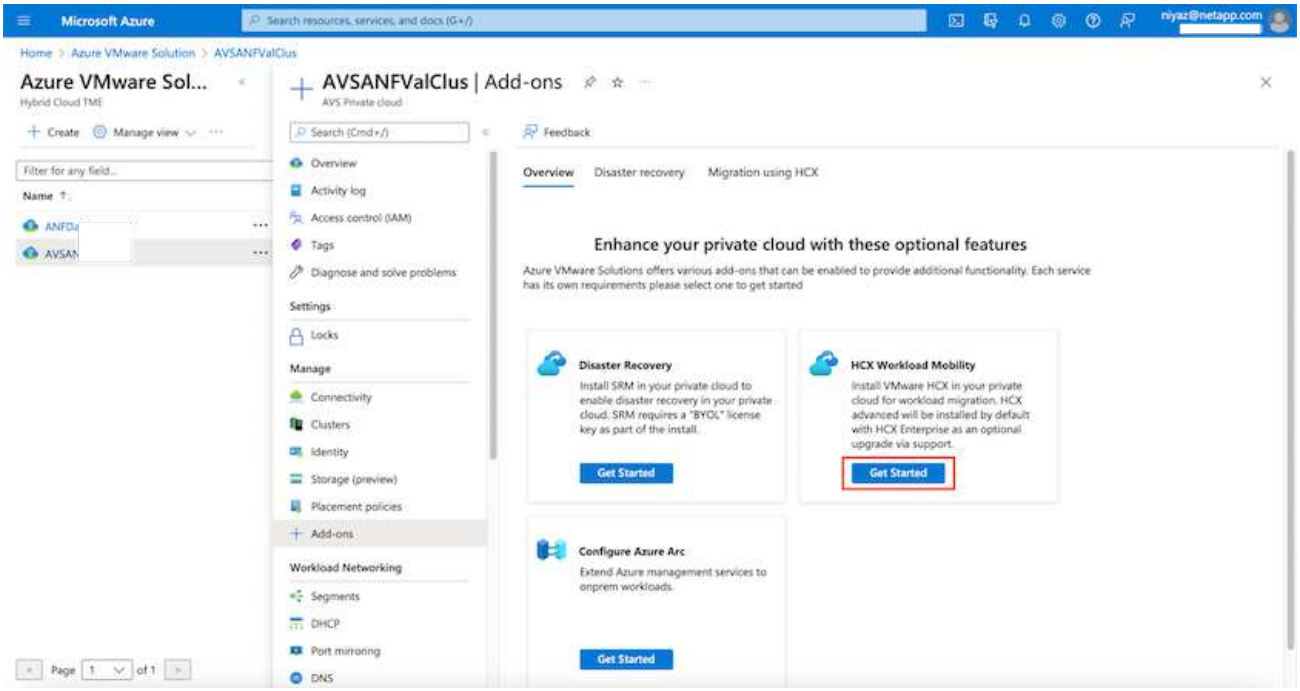
솔루션 배포

이 솔루션의 배포를 완료하려면 다음 단계를 따르세요.

▼ **1**단계**:** 추가 기능 옵션을 사용하여 **Azure Portal**을 통해 **HCX** 설치

설치를 수행하려면 다음 단계를 완료하세요.

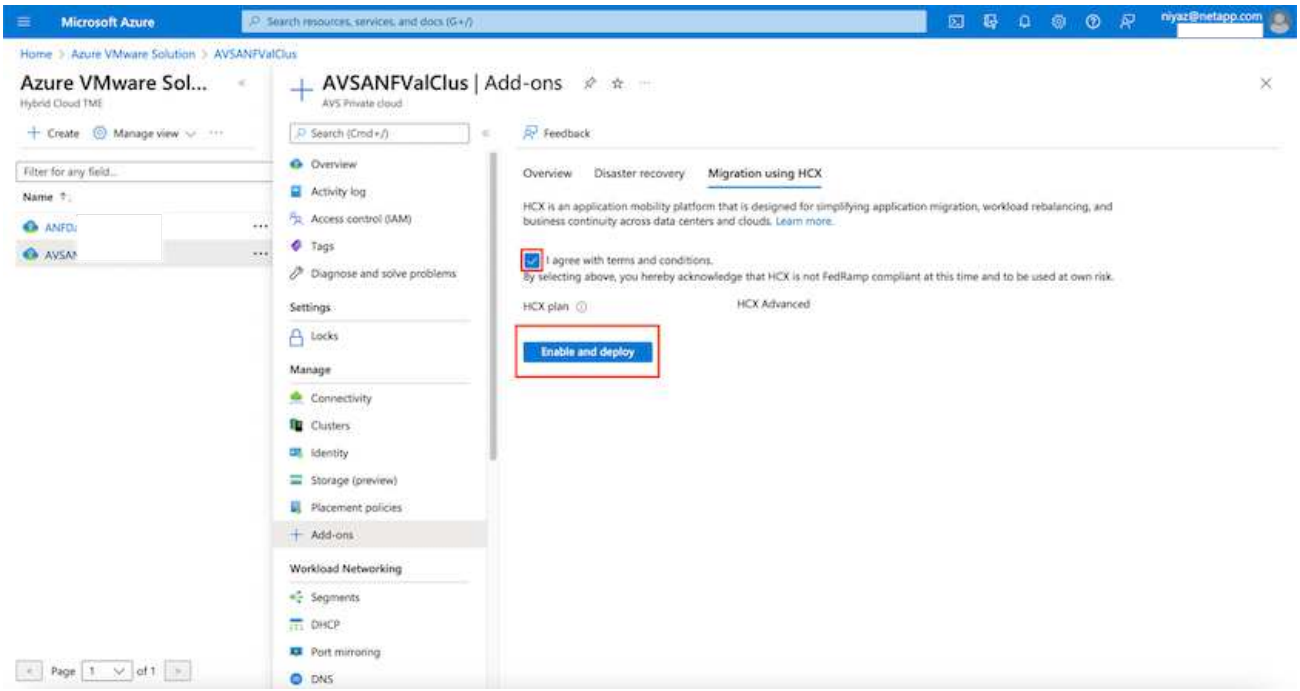
1. Azure Portal에 로그인하여 Azure VMware Solution 프라이빗 클라우드에 액세스하세요.
2. 적절한 프라이빗 클라우드를 선택하고 애드온에 액세스하세요. *관리 > 추가 기능*으로 이동하면 됩니다.
3. HCX 워크로드 모빌리티 섹션에서 *시작하기*를 클릭합니다.



4. 이용 약관에 동의합니다 옵션을 선택하고 *활성화 및 배포*를 클릭합니다.

> 기본 배포는 HCX Advanced입니다. Enterprise Edition을 활성화하려면 지원 요청을 열어주세요.

> 배포에는 약 25~30분이 소요됩니다.



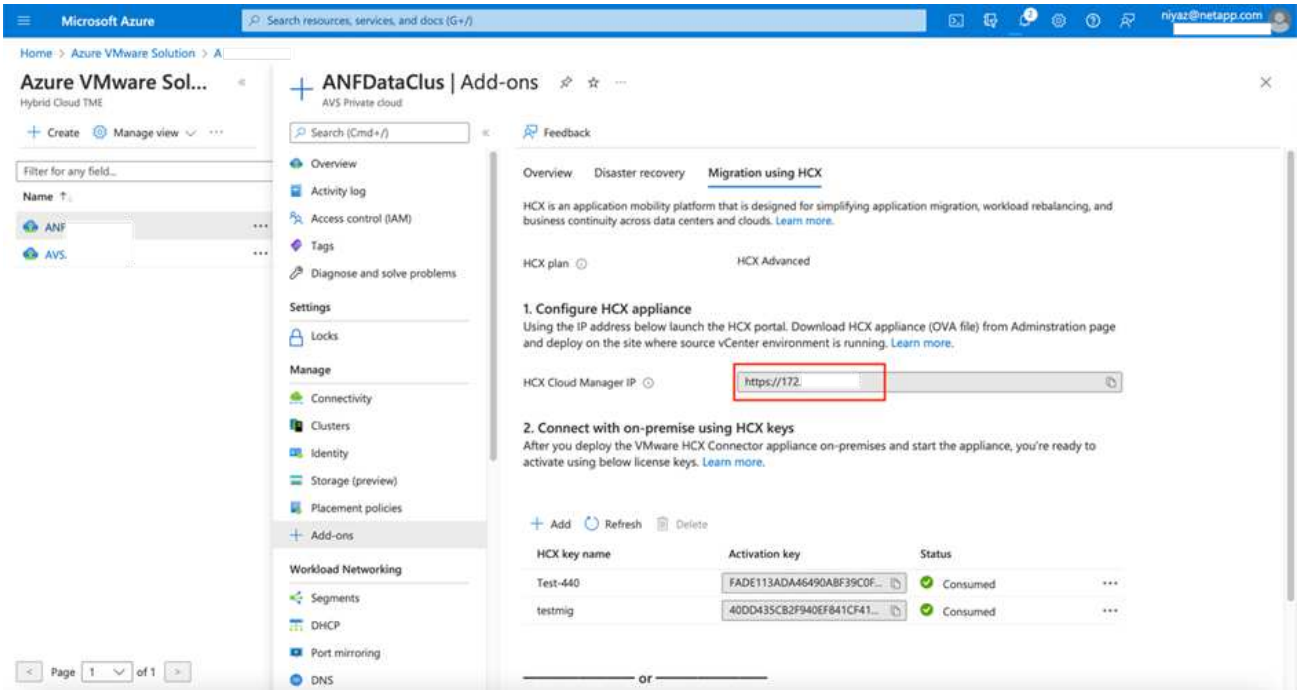
▼ **2**단계**:** 온프레미스 **vCenter Server**에 설치 프로그램 **OVA** 배포

온-프레미스 커넥터가 Azure VMware Solution의 HCX Manager에 연결하려면 온-프레미스 환경에서 적절한 방화벽 포트가 열려 있는지 확인하세요.

온프레미스 vCenter Server에 HCX 커넥터를 다운로드하고 설치하려면 다음 단계를 완료하세요.

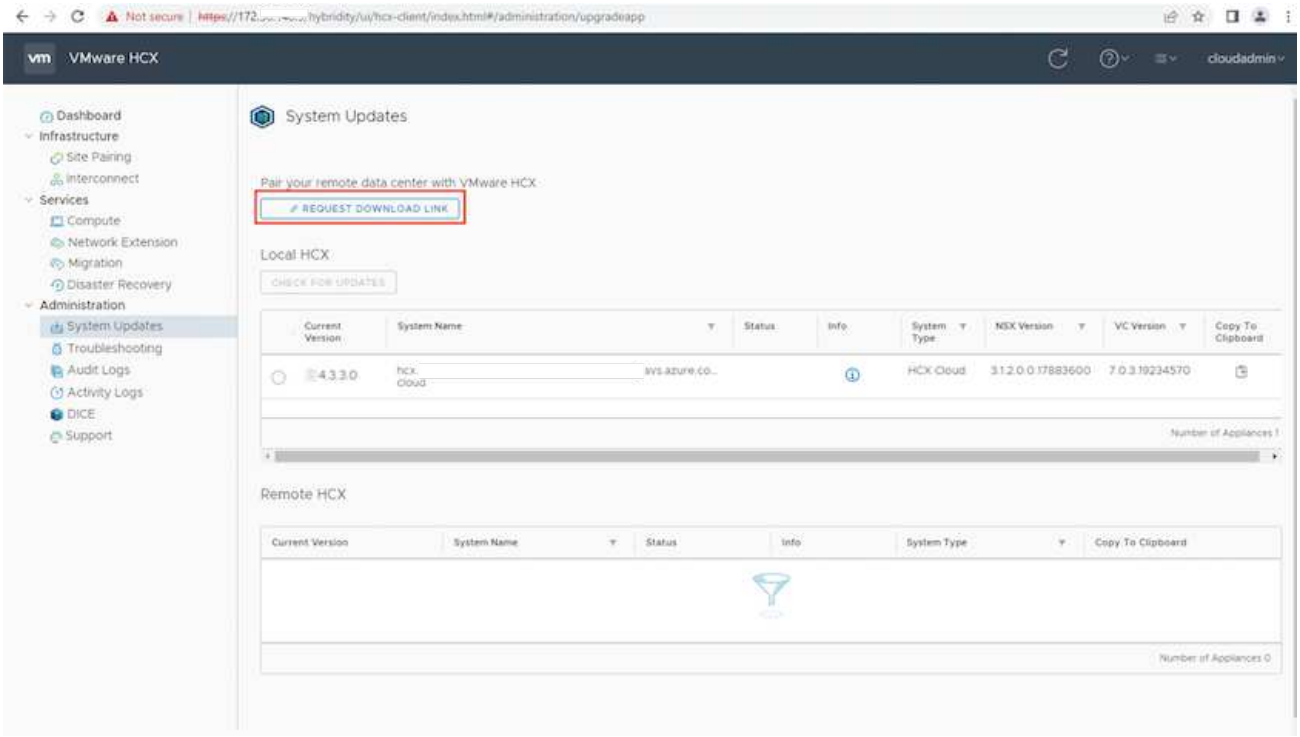
1. Azure Portal에서 Azure VMware Solution으로 이동하여 프라이빗 클라우드를 선택하고 *관리 > 추가 기능 > HCX를 사용한 마이그레이션*을 선택한 다음 HCX Cloud Manager 포털을 복사하여 OVA 파일을 다운로드합니다.

   HCX 포털에 액세스하려면 기본 CloudAdmin 사용자 자격 증명을 사용하세요.

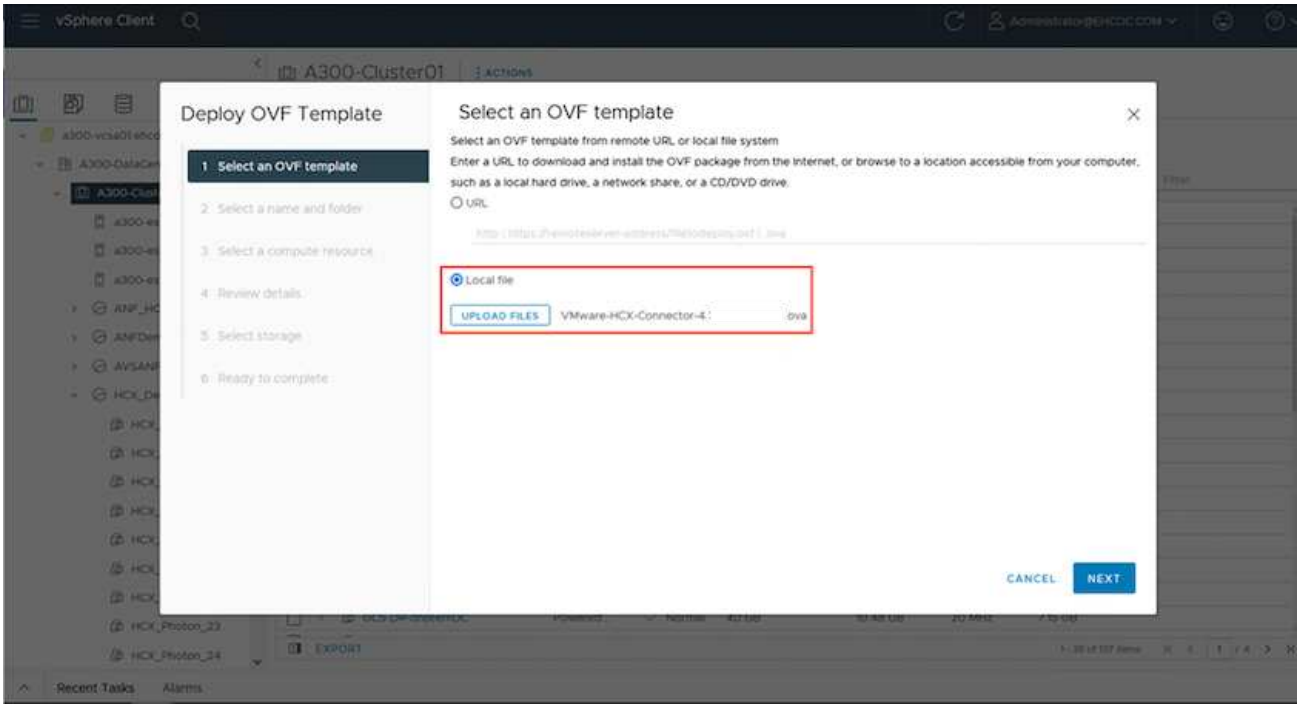


2. jumphost를 사용하여 cloudadmin@vsphere.local로 HCX 포털에 액세스한 후 *관리 > 시스템 업데이트*로 이동하여 *다운로드 링크 요청*을 클릭합니다.

   OVA 링크를 다운로드하거나 복사하여 브라우저에 붙여넣어 온프레미스 vCenter Server에 배포할 VMware HCX Connector OVA 파일의 다운로드 프로세스를 시작합니다.



3. OVA를 다운로드한 후 **OVF** 템플릿 배포 옵션을 사용하여 온프레미스 VMware vSphere 환경에 배포합니다.



4. OVA 배포에 필요한 모든 정보를 입력하고, *다음*을 클릭한 다음, *마침*을 클릭하여 VMware HCX 커넥터 OVA를 배포합니다.

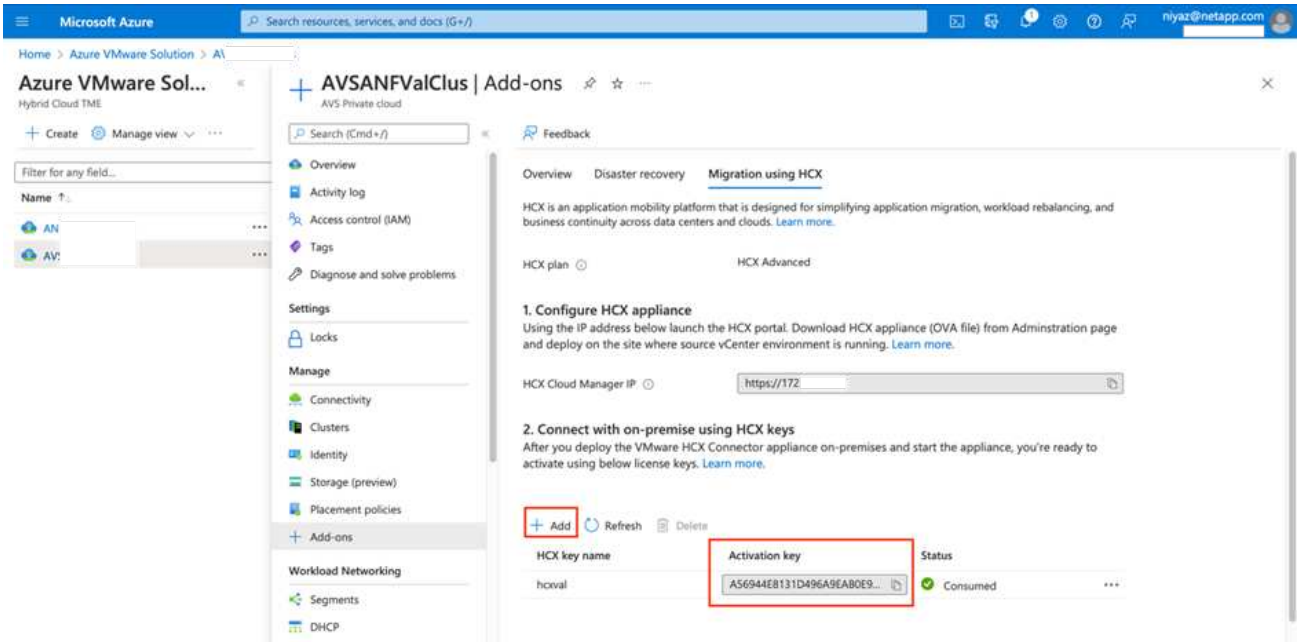
ⓘ 가상 어플라이언스의 전원을 수동으로 켭니다.

단계별 지침은 다음을 참조하세요. "VMware HCX 사용자 가이드" .

▼ **3**단계**:** 라이선스 키로 **HCX** 커넥터 활성화

온프레미스에 VMware HCX Connector OVA를 배포하고 어플라이언스를 시작한 후 다음 단계를 완료하여 HCX Connector를 활성화합니다. Azure VMware Solution 포털에서 라이선스 키를 생성하고 VMware HCX Manager에서 활성화합니다.

1. Azure Portal에서 Azure VMware Solution으로 이동하여 프라이빗 클라우드를 선택하고 *관리 > 추가 기능 > HCX를 사용한 마이그레이션*을 선택합니다.
2. *HCX 키를 사용하여 온프레미스와 연결*에서 *추가*를 클릭하고 활성화 키를 복사합니다.



> 배포된 각 온프레미스 HCX 커넥터에는 별도의 키가 필요합니다.

3. 온프레미스 VMware HCX Manager에 로그인하세요. "`https://hcxmanagerIP:9443`" 관리자 자격 증명을 사용합니다.

> OVA 배포 중에 정의된 비밀번호를 사용하세요.

4. 라이센스에서 3단계에서 복사한 키를 입력하고 *활성화*를 클릭합니다.

> 온프레미스 HCX 커넥터는 인터넷에 접속할 수 있어야 합니다.

5. *데이터 센터 위치*에서 온프레미스에서 VMware HCX Manager를 설치할 수 있는 가장 가까운 위치를 제공합니다. *계속*을 클릭하세요.
6. *시스템 이름*에서 이름을 업데이트하고 *계속*을 클릭합니다.
7. *예, 계속*을 클릭합니다.
8. *vCenter 연결*에서 vCenter Server의 정규화된 도메인 이름(FQDN) 또는 IP 주소와 해당 자격 증명을 제공하고 *계속*을 클릭합니다.

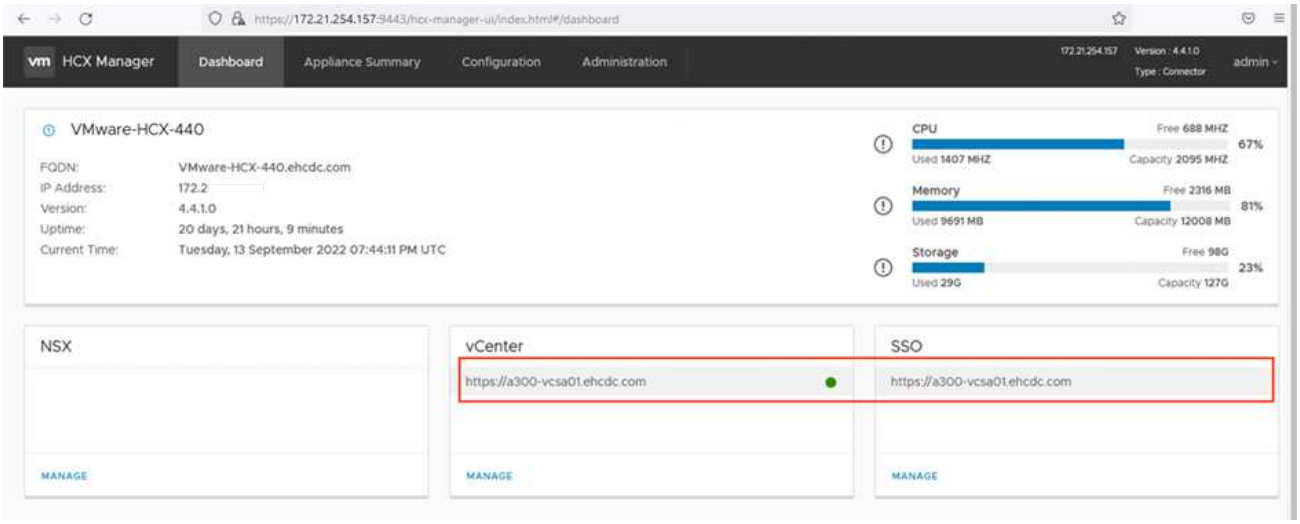
> 나중에 연결 문제를 방지하려면 FQDN을 사용하세요.

9. *SSO/PSC 구성*에서 Platform Services Controller의 FQDN 또는 IP 주소를 입력하고 *계속*을 클릭합니다.

VMware vCenter Server FQDN 또는 IP 주소를 입력하세요.

10. 입력한 정보가 정확한지 확인하고 *다시 시작*을 클릭하세요.
11. 서비스가 다시 시작된 후 나타나는 페이지에서 vCenter Server가 녹색으로 표시됩니다. vCenter Server와 SSO 모두 적절한 구성 매개변수를 가져야 하며, 이는 이전 페이지와 동일해야 합니다.

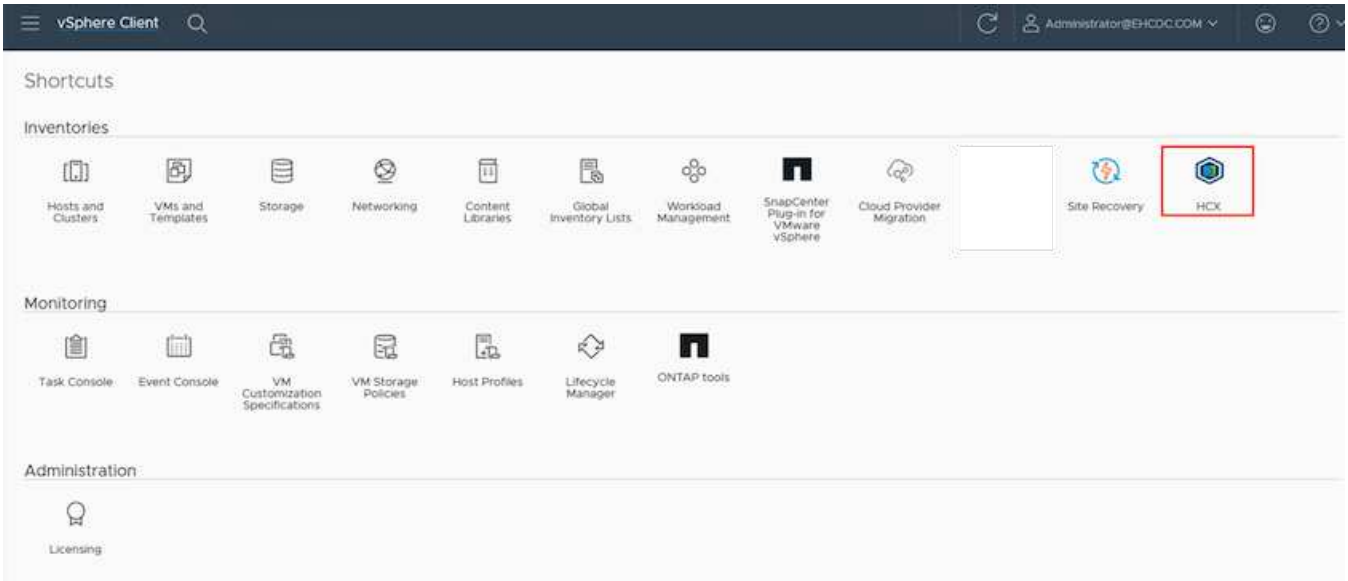
이 프로세스는 약 10~20분 정도 걸리며 플러그인이 vCenter Server에 추가됩니다.



▼ **4**단계: 온-프레미스 **VMware HCX** 커넥터를 **Azure VMware Solution HCX Cloud Manager**와 페어링

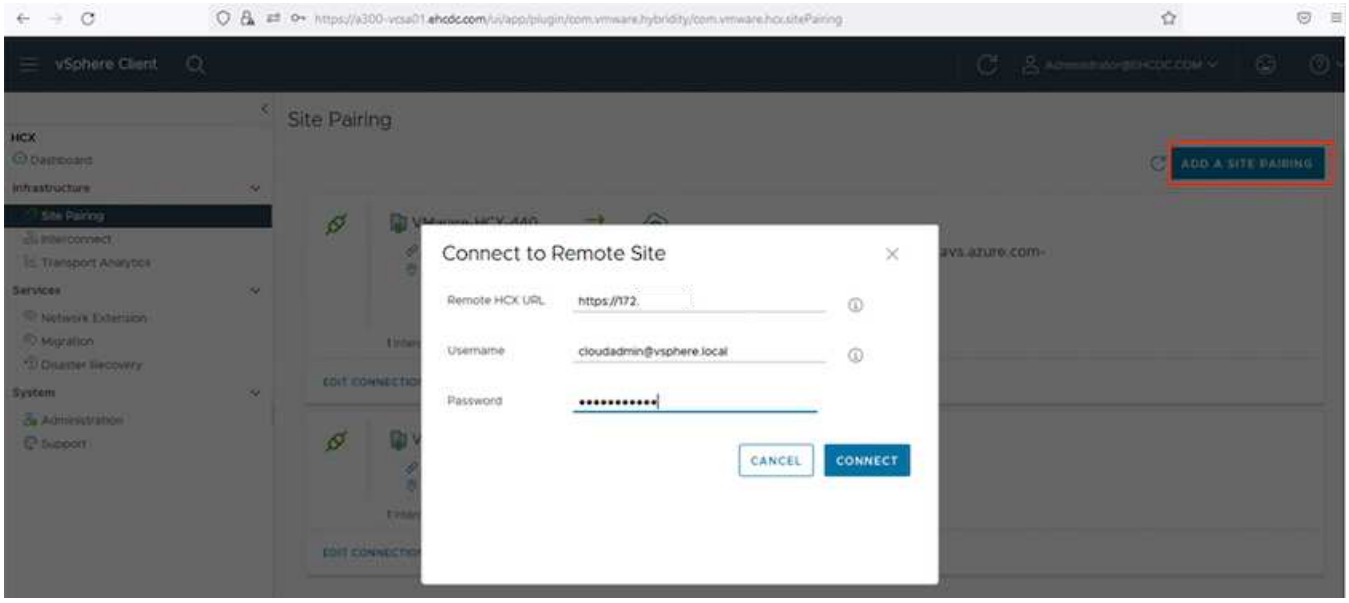
온-프레미스와 Azure VMware Solution에 HCX 커넥터를 설치한 후, 페어링을 추가하여 Azure VMware Solution 프라이빗 클라우드에 대한 온-프레미스 VMware HCX 커넥터를 구성합니다. 사이트 페어링을 구성하려면 다음 단계를 완료하세요.

1. 온-프레미스 vCenter 환경과 Azure VMware Solution SDDC 간에 사이트 쌍을 만들려면 온-프레미스 vCenter Server에 로그인하고 새 HCX vSphere Web Client 플러그인에 액세스합니다.



1. 인프라에서 *사이트 페어링 추가*를 클릭합니다.

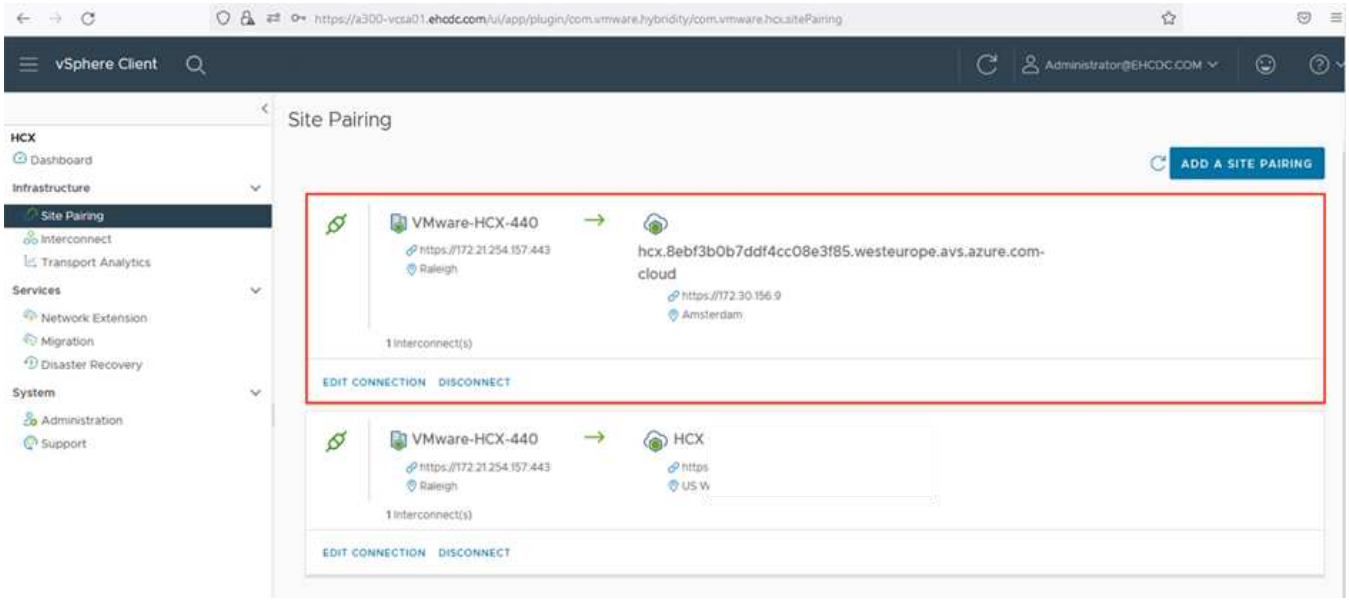
Azure VMware Solution HCX Cloud Manager URL 또는 IP 주소와 프라이빗 클라우드에 액세스하기 위한 CloudAdmin 역할의 자격 증명을 입력하세요.



1. *연결*을 클릭하세요.

VMware HCX Connector는 포트 443을 통해 HCX Cloud Manager IP로 라우팅할 수 있어야 합니다.

1. 페어링이 생성되면 새로 구성된 사이트 페어링을 HCX 대시보드에서 사용할 수 있습니다.

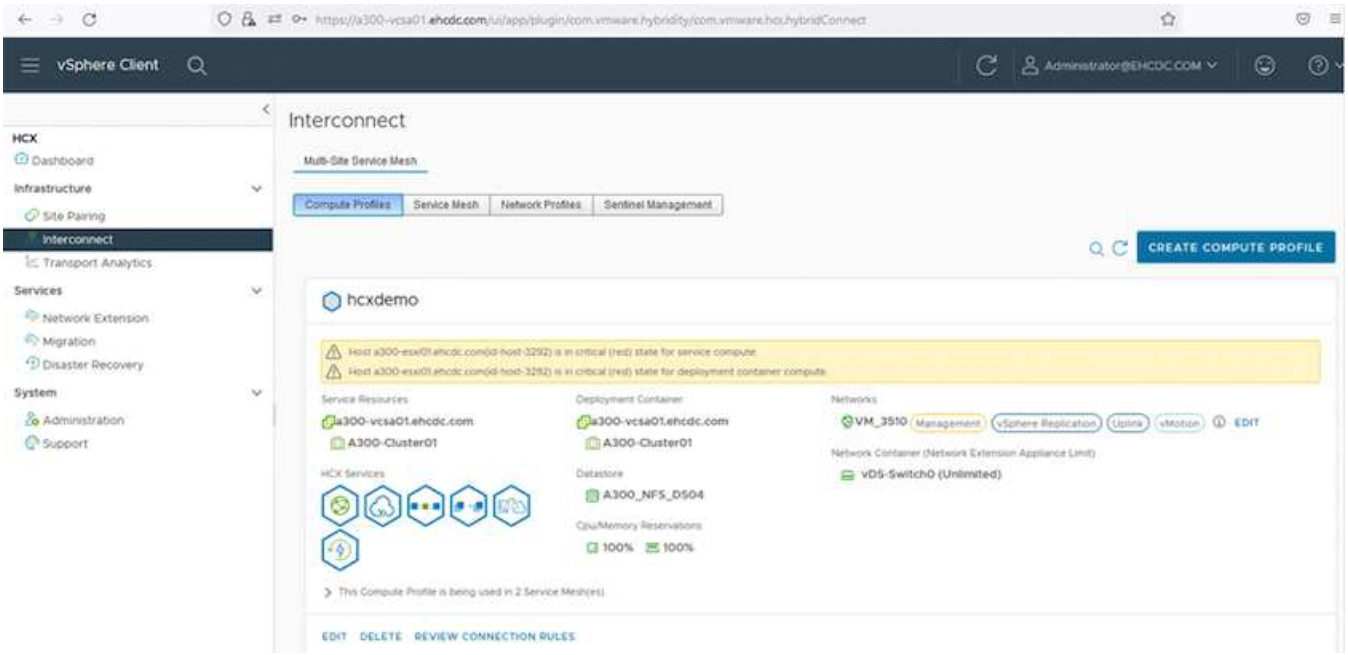


▼ **5**단계**:** 네트워크 프로필**,** 컴퓨팅 프로필 및 서비스 메시 구성

VMware HCX Interconnect 서비스 어플라이언스는 인터넷과 대상 사이트에 대한 개인 연결을 통해 복제 및 vMotion 기반 마이그레이션 기능을 제공합니다. 상호 연결은 암호화, 트래픽 엔지니어링, VM 이동성을 제공합니다. Interconnect 서비스 어플라이언스를 생성하려면 다음 단계를 완료하세요.

1. 인프라에서 *상호 연결 > 다중 사이트 서비스 메시 > 컴퓨팅 프로필 > 컴퓨팅 프로필 만들기*를 선택합니다.

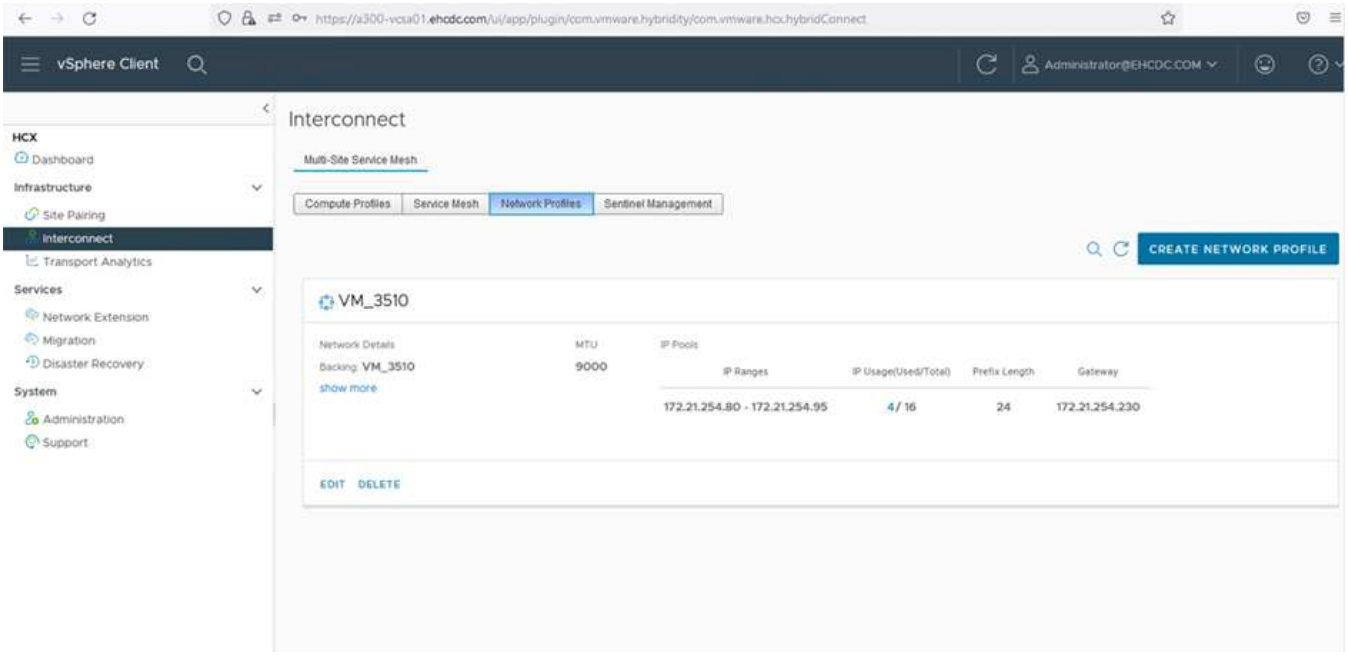
컴퓨팅 프로필은 배포되는 어플라이언스와 HCX 서비스가 액세스할 수 있는 VMware 데이터 센터 부분을 포함한 배포 매개변수를 정의합니다.



1. 컴퓨팅 프로필을 만든 후 *멀티 사이트 서비스 메시 > 네트워크 프로필 > 네트워크 프로필 만들기*를 선택하여 네트워크 프로필을 만듭니다.

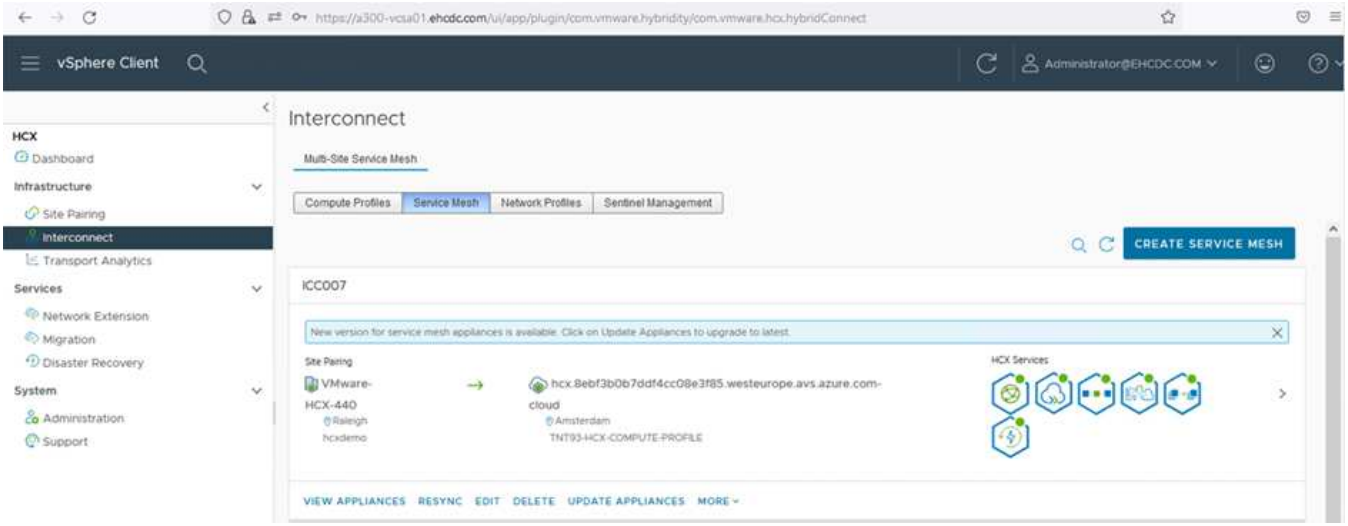
네트워크 프로필은 HCX가 가상 어플라이언스에 사용하는 IP 주소와 네트워크 범위를 정의합니다.

이 단계에는 두 개 이상의 IP 주소가 필요합니다. 이러한 IP 주소는 관리 네트워크에서 Interconnect Appliance에 할당됩니다.

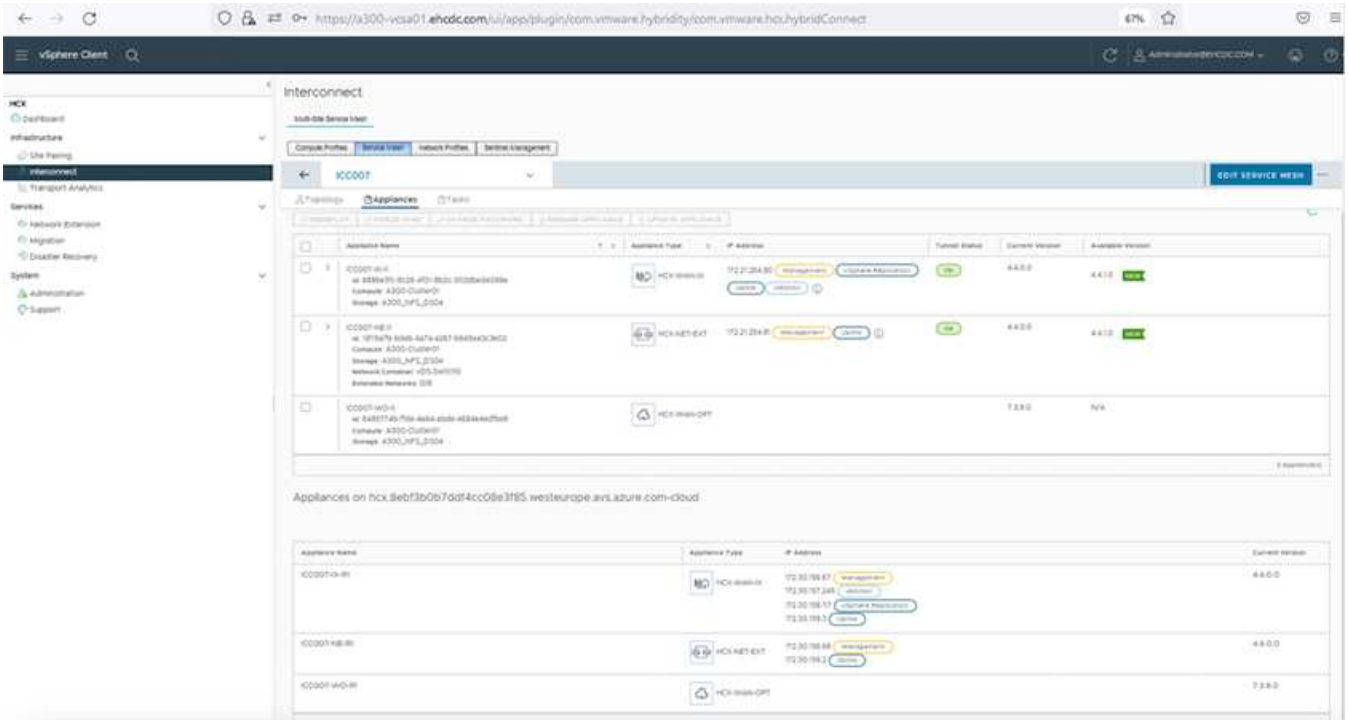


1. 이제 컴퓨팅 및 네트워크 프로필이 성공적으로 생성되었습니다.
2. 상호 연결 옵션 내에서 서비스 메시 탭을 선택하여 서비스 메시를 만들고 온-프레미스 및 Azure SDDC 사이트를 선택합니다.
3. 서비스 메시는 로컬 및 원격 컴퓨팅과 네트워크 프로필 쌍을 지정합니다.

이 프로세스의 일환으로 HCX 어플라이언스는 소스 사이트와 대상 사이트 모두에 배포되고 자동으로 구성되어 안전한 전송 패브릭을 생성합니다.



1. 이것은 구성의 마지막 단계입니다. 배포를 완료하는 데 약 30분이 소요됩니다. 서비스 메시가 구성되면 워크로드 VM을 마이그레이션하기 위한 IPsec 터널이 성공적으로 생성되어 환경이 준비됩니다.



▼ **6**단계**:** 워크로드 마이그레이션

다양한 VMware HCX 마이그레이션 기술을 사용하여 온-프레미스와 Azure SDDC 간에 워크로드를 양방향으로 마이그레이션할 수 있습니다. HCX 대량 마이그레이션, HCX vMotion, HCX 콜드 마이그레이션, HCX 복제 지원

vMotion(HCX Enterprise 에디션에서 사용 가능), HCX OS 지원 마이그레이션(HCX Enterprise 에디션에서 사용 가능) 등 다양한 마이그레이션 기술을 사용하여 VMware HCX 활성화 엔터티 간에 VM을 이동할 수 있습니다.

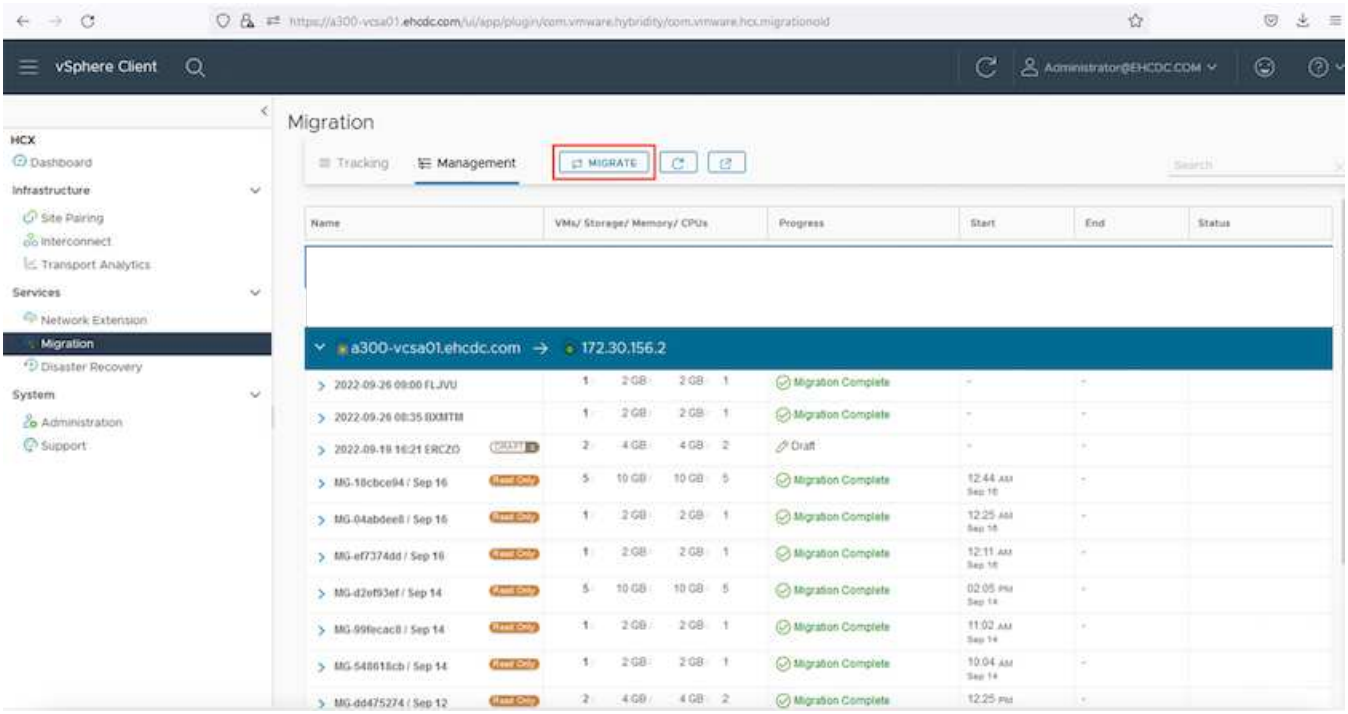
다양한 HCX 마이그레이션 메커니즘에 대해 자세히 알아보려면 다음을 참조하세요. "VMware HCX 마이그레이션 유형" .

대량 마이그레이션

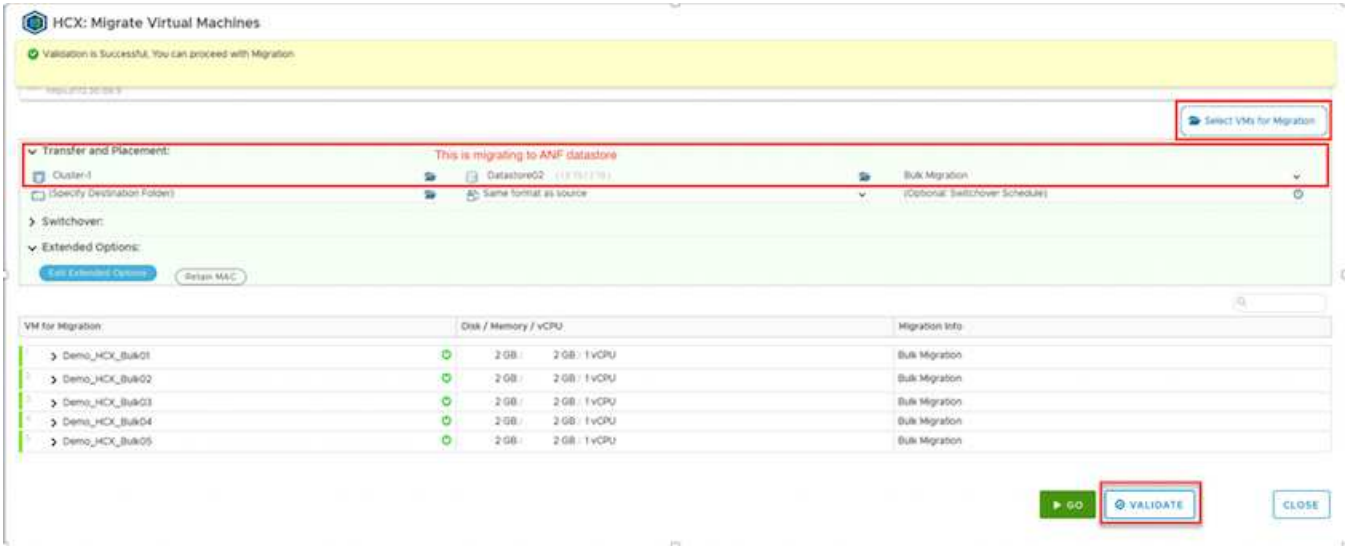
이 섹션에서는 대량 마이그레이션 메커니즘에 대해 자세히 설명합니다. 대량 마이그레이션 중에 HCX의 대량 마이그레이션 기능은 vSphere Replication을 사용하여 디스크 파일을 마이그레이션하고 대상 vSphere HCX 인스턴스에서 VM을 다시 생성합니다.

대량 VM 마이그레이션을 시작하려면 다음 단계를 완료하세요.

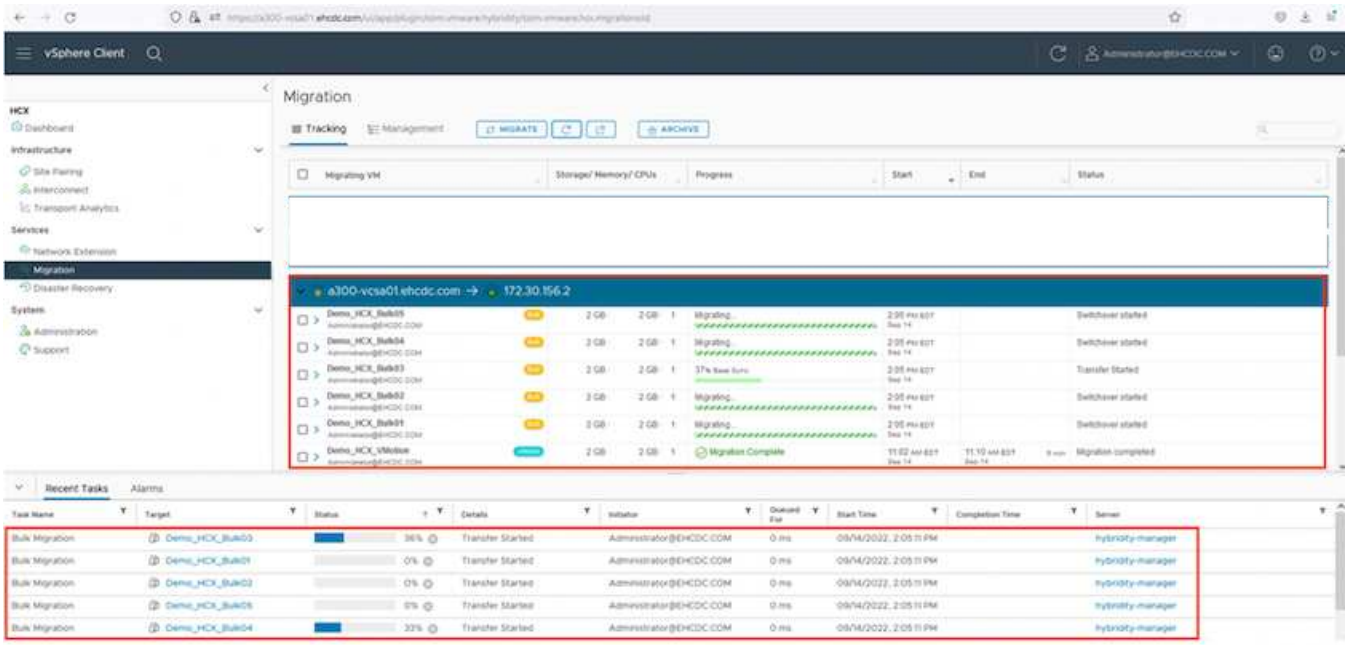
1. 서비스 > 마이그레이션*에서 *마이그레이션 탭에 액세스합니다.



1. *원격 사이트 연결*에서 원격 사이트 연결을 선택하고 소스와 대상을 선택합니다. 이 예에서 대상은 Azure VMware Solution SDDC HCX 엔드포인트입니다.
2. *마이그레이션을 위한 VM 선택*을 클릭합니다. 이는 온프레미스 VM의 모든 목록을 제공합니다. 일치:값 표현식을 기준으로 VM을 선택하고 *추가*를 클릭합니다.
3. 전송 및 배치 섹션에서 마이그레이션 프로필을 포함하여 필수 필드(클러스터, 저장소, 대상 및 네트워크)를 업데이트하고 *검증*을 클릭합니다.

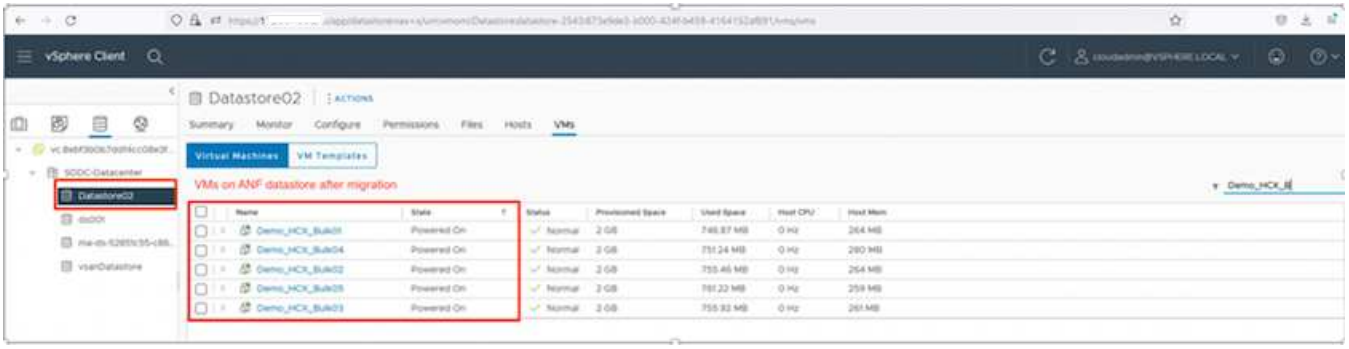


1. 유효성 검사가 완료되면 *이동*을 클릭하여 마이그레이션을 시작합니다.



이 마이그레이션 중에 대상 vCenter 내의 지정된 Azure NetApp Files 데이터 저장소에 플레이스홀더 디스크가 생성되어 소스 VM 디스크의 데이터를 플레이스홀더 디스크로 복제할 수 있습니다. HBR은 대상에 대한 전체 동기화를 위해 트리거되고, 기준이 완료된 후 RPO(복구 지점 목표) 주기를 기반으로 증분 동기화가 수행됩니다. 전체/증분 동기화가 완료된 후 특정 일정을 설정하지 않으면 자동으로 전환이 실행됩니다.

1. 마이그레이션이 완료되면 대상 SDDC vCenter에 액세스하여 해당 내용을 검증합니다.

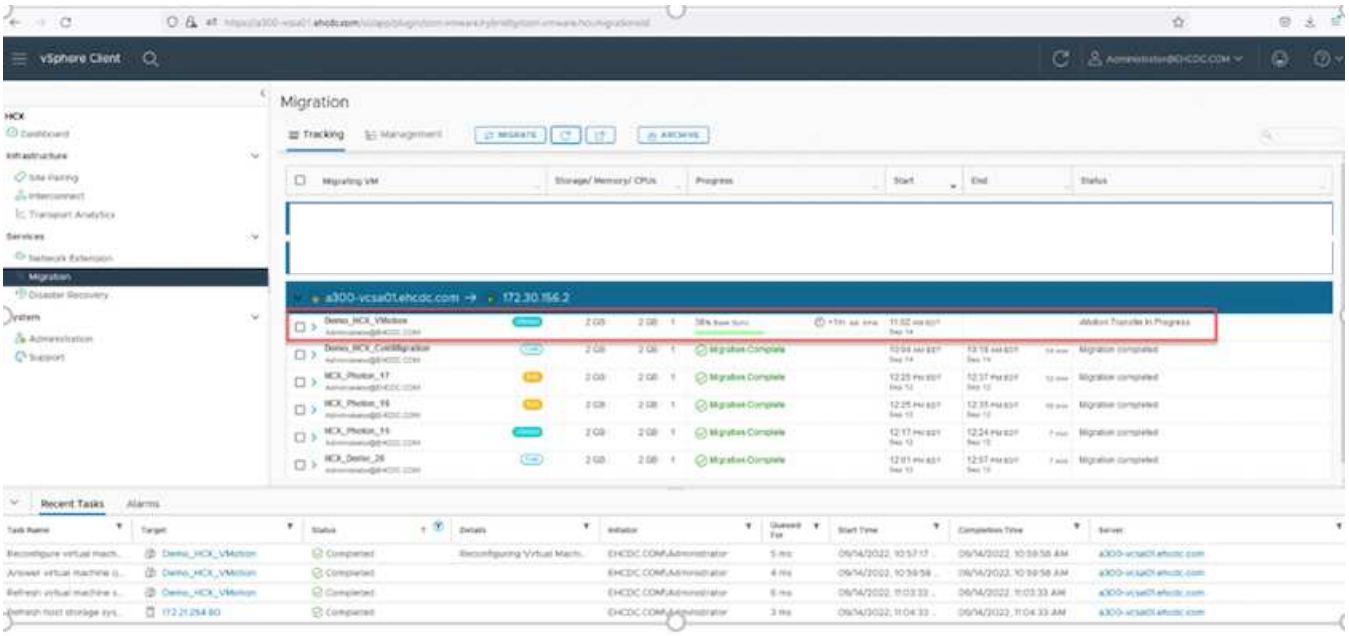


HCX를 사용하여 온프레미스에서 Azure VMware 솔루션으로 워크로드를 마이그레이션하는 방법과 다양한 마이그레이션 옵션에 대한 추가 및 자세한 정보는 다음을 참조하세요. "VMware HCX 마이그레이션 고려 사항" .

이 과정에 대해 자세히 알아보려면 다음 영상을 시청하세요.

HCX를 사용한 워크로드 마이그레이션

HCX vMotion 옵션의 스크린샷은 다음과 같습니다.



이 과정에 대해 자세히 알아보려면 다음 영상을 시청하세요.

HCX v모션

마이그레이션을 처리하는 데 충분한 대역폭이 있는지 확인하세요.

대상 ANF 데이터 저장소에는 마이그레이션을 처리할 수 있는 충분한 공간이 있어야 합니다.

결론

온프레미스의 모든 유형/공급업체 스토리지에 있는 데이터를 대상으로 전체 클라우드 또는 하이브리드 클라우드를 사용하든, Azure NetApp Files 와 HCX는 데이터 요구 사항을 애플리케이션 계층에 원활하게 전달하여 TCO를 줄이는

동시에 애플리케이션 워크로드를 배포하고 마이그레이션할 수 있는 탁월한 옵션을 제공합니다. 어떤 사용 사례든 Azure NetApp Files 와 함께 Azure VMware 솔루션을 선택하면 클라우드의 이점을 빠르게 실현하고, 온프레미스와 여러 클라우드에서 일관된 인프라와 운영을 구현하고, 워크로드를 양방향으로 이식하고, 엔터프라이즈급 용량과 성능을 얻을 수 있습니다. VMware vSphere Replication, VMware vMotion 또는 NFC(네트워크 파일 복사)를 사용하여 스토리지를 연결하고 VM을 마이그레이션하는 데 사용되는 익숙한 프로세스 및 절차와 동일합니다.

테이크아웃

이 문서의 주요 내용은 다음과 같습니다.

- 이제 Azure VMware Solution SDDC에서 Azure NetApp Files 데이터 저장소로 사용할 수 있습니다.
- 온-프레미스에서 Azure NetApp Files 저장소로 데이터를 쉽게 마이그레이션할 수 있습니다.
- 마이그레이션 작업 중에 용량 및 성능 요구 사항을 충족하기 위해 Azure NetApp Files 데이터 저장소를 쉽게 확장하거나 축소할 수 있습니다.

추가 정보를 찾을 수 있는 곳

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 웹사이트 링크를 참조하세요.

- Azure VMware 솔루션 설명서

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

- Azure NetApp Files 설명서

"https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

- VMware HCX 마이그레이션 고려 사항

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

GCP/GCVE용 NetApp

Google Cloud Platform GCVE를 위한 NetApp 기능

NetApp Google Cloud Platform(GCP) Google Cloud VMware Engine(GCVE)에 제공하는 기능에 대해 자세히 알아보세요. NetApp 게스트 연결 스토리지 장치 또는 보조 NFS 데이터 저장소로 활용하는 것부터 워크플로 마이그레이션, 클라우드로의 확장/버스팅, 백업/복원 및 재해 복구까지 다양한 기능을 제공합니다.

다음 옵션 중에서 선택하여 원하는 콘텐츠 섹션으로 이동하세요.

- "GCP에서 GCVE 구성"
- "GCVE를 위한 NetApp 스토리지 옵션"
- "NetApp / VMware 클라우드 솔루션"

GCP에서 GCVE 구성

온프레미스와 마찬가지로, VM을 만들고 마이그레이션하기 위한 성공적인 프로덕션 준비 환경을 위해서는 클라우드

기반 가상화 환경을 계획하는 것이 중요합니다.

이 섹션에서는 GCVE를 설정하고 관리하는 방법과 NetApp 스토리지 연결에 사용 가능한 옵션과 함께 사용하는 방법을 설명합니다.

> 게스트 내 스토리지는 Cloud Volumes ONTAP 및 Google Cloud NetApp Volumes GCVE에 연결하는 데 지원되는 유일한 방법입니다.

설정 과정은 다음 단계로 나눌 수 있습니다.

- GCVE 배포 및 구성
- GCVE에 대한 개인 액세스 활성화

자세한 내용을 보려면"GCVE 구성 단계" .

GCVE를 위한 **NetApp** 스토리지 옵션

NetApp 스토리지는 GCP GCVE 내에서 추측 연결 또는 보조 NFS 데이터 저장소로 등 여러 가지 방법으로 활용할 수 있습니다.

방문해주세요"지원되는 NetApp 스토리지 옵션" 자세한 내용은.

Google Cloud는 다음 구성에서 NetApp 스토리지를 지원합니다.

- 게스트 연결 스토리지로서의 Cloud Volumes ONTAP (CVO)
- 게스트 연결 스토리지로서의 Google Cloud NetApp Volumes (NetApp Volumes)
- Google Cloud NetApp Volumes (NetApp Volumes)를 보조 NFS 데이터 저장소로 사용

자세한 내용을 보려면"GCVE를 위한 게스트 연결 스토리지 옵션" . 자세한 내용을 보려면"GCVE에 대한 보충 NFS 데이터 저장소 옵션" .

더 자세히 알아보세요"Google Cloud NetApp Volumes 데이터 저장소 지원(NetApp 블로그)" 또는"Google Cloud NetApp Volumes Google Cloud VMware Engine의 데이터 저장소로 사용하는 방법(Google 블로그)"

솔루션 사용 사례

NetApp 및 VMware 클라우드 솔루션을 사용하면 많은 사용 사례를 Azure AVS에 쉽게 배포할 수 있습니다. 각 사용 사례는 VMware에서 정의한 클라우드 영역별로 정의됩니다.

- 보호(재해 복구 및 백업/복원 모두 포함)
- 연장하다
- 이주하다

"Google Cloud GCVE를 위한 NetApp 솔루션을 찾아보세요"

GCP/GCVE에서 워크로드 보호

NetApp SnapCenter 및 **Veeam** 복제를 통한 애플리케이션 일관성 재해 복구

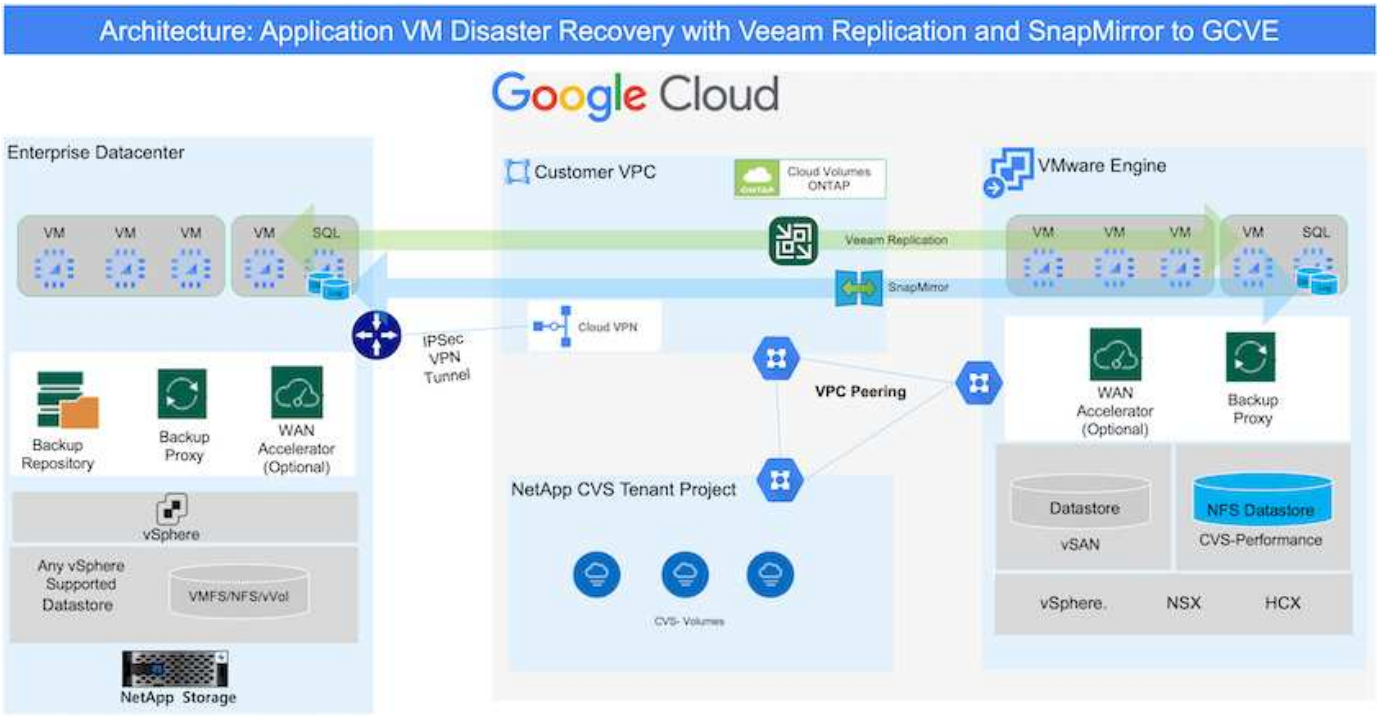
클라우드로 재해 복구를 수행하는 것은 랜섬웨어와 같은 사이트 중단 및 데이터 손상 사건으로부터 워크로드를 보호하는 탄력적이고 비용 효율적인 방법입니다. NetApp SnapMirror 사용하면 게스트 연결 스토리지를 사용하는 온프레미스 VMware 워크로드를 Google Cloud에서 실행되는 NetApp Cloud Volumes ONTAP 으로 복제할 수 있습니다.

개요

많은 고객이 VMware vSphere에 호스팅된 애플리케이션 VM에 대한 효과적인 재해 복구 솔루션을 찾고 있습니다. 많은 기업이 재난 발생 시 복구를 위해 기존 백업 솔루션을 사용합니다. 이런 솔루션은 종종 RTO를 늘리고 기대에 부응하지 못합니다. RPO와 RTO를 줄이기 위해, 적절한 권한이 있는 네트워크 연결과 환경이 제공되는 한 온프레미스에서 GCVE로의 Veeam VM 복제도 활용할 수 있습니다. 참고: Veeam VM 복제는 게스트 VM 내부의 iSCSI 또는 NFS 마운트와 같은 VM 게스트에 연결된 스토리지 장치를 보호하지 않습니다. 따로 보호해야 합니다.

SQL VM에 대한 애플리케이션 일관성 복제를 위해 그리고 RTO를 줄이기 위해 SnapCenter 사용하여 SQL 데이터베이스와 로그 볼륨의 스냅미러 작업을 조율했습니다.

이 문서에서는 NetApp SnapMirror, Veeam 및 Google Cloud VMware Engine(GCVE)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.

온프레미스 환경과 Google Cloud 네트워크를 연결하려면 전용 상호 연결이나 Cloud VPN과 같은 연결 옵션을 사용하세요. 세그먼트는 온프레미스 VLAN 설계를 기반으로 생성되어야 합니다.

온프레미스 데이터 센터를 Google Cloud에 연결하는 데에는 여러 가지 옵션이 있으므로 이 문서에서는 구체적인 워크플로를 설명할 수 없습니다. 온프레미스와 Google 간의 적절한 연결 방법에 대해서는 Google Cloud 문서를 참조하세요.

DR 솔루션 배포

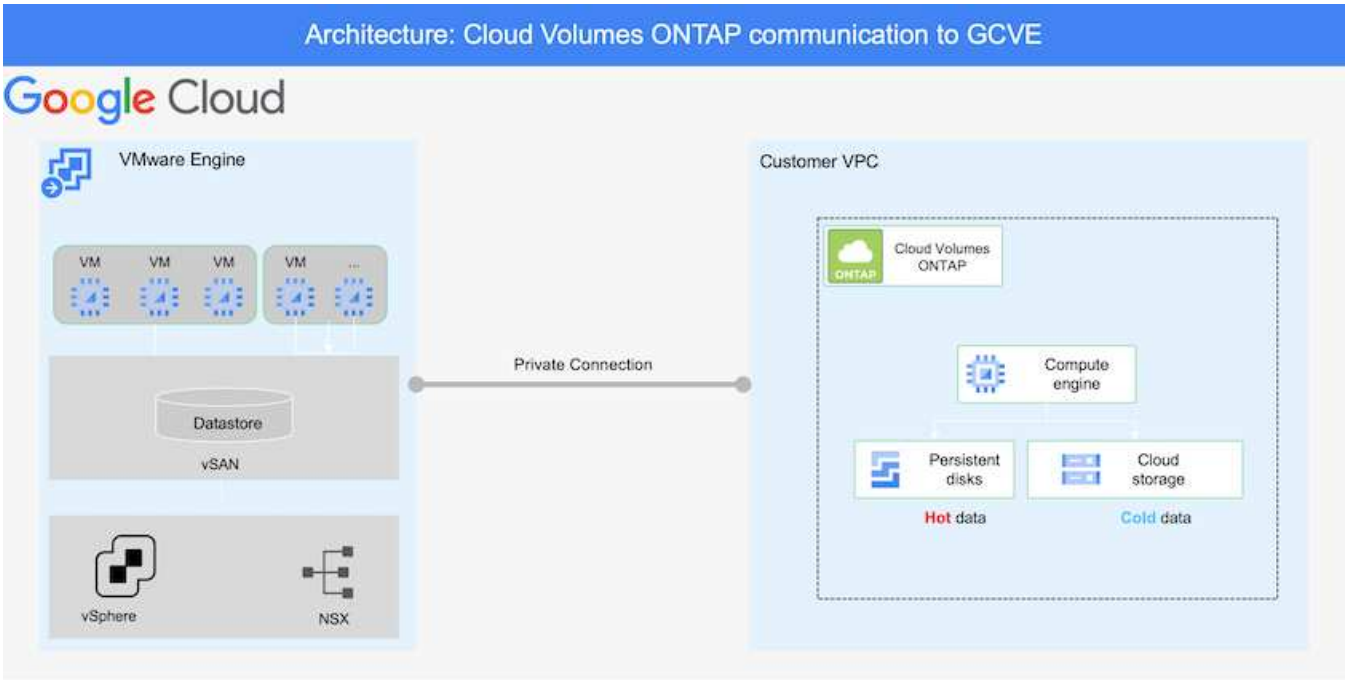
솔루션 배포 개요

1. SnapCenter 사용하여 필요한 RPO 요구 사항을 충족하는 애플리케이션 데이터를 백업하세요.
2. 적절한 구독 및 가상 네트워크 내에서 NetApp Console을 사용하여 올바른 인스턴스 크기로 Cloud Volumes ONTAP을 프로비저닝합니다.
   a. 해당 애플리케이션 볼륨에 맞게 SnapMirror 구성합니다.
   b. 예약된 작업 후 SnapMirror 업데이트를 트리거하도록 SnapCenter 의 백업 정책을 업데이트합니다.
3. Veeam 소프트웨어를 설치하고 가상 머신을 Google Cloud VMware Engine 인스턴스로 복제하기 시작합니다.
4. 재해 발생 시 NetApp Console을 사용하여 SnapMirror 관계를 중단하고 Veeam을 통해 가상 머신의 페일오버를 트리거합니다.
   a. 애플리케이션 VM에 대한 ISCSI LUN과 NFS 마운트를 다시 연결합니다.
   b. 온라인으로 신청하세요.
5. 기본 사이트가 복구된 후 SnapMirror 역방향으로 재동기화하여 보호된 사이트로 장애 복구를 호출합니다.

배포 세부 정보

▼ **Google Cloud**에서 **CVO**를 구성하고 볼륨을 **CVO**에 복제합니다**.**

첫 번째 단계는 Google Cloud에서 Cloud Volumes ONTAP 구성하는 것입니다("씨보") 원하는 빈도와 스냅샷 보존 기간을 설정하여 원하는 볼륨을 Cloud Volumes ONTAP 에 복제합니다.



SnapCenter 설정 및 데이터 복제에 대한 단계별 샘플 지침은 다음을 참조하세요."SnapCenter 사용하여 복제 설정"

SnapCenter 사용한 SQL VM 보호 검토

▼ **GCVE** 호스트 및 **CVO** 데이터 액세스 구성

SDDC를 배포할 때 고려해야 할 두 가지 중요한 요소는 GCVE 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.

NFS 데이터 저장소용 Google Cloud NetApp Volumes 와 SQL 데이터베이스 및 로그용 Cloud Volumes ONTAP 모든 VPC에 배포할 수 있으며, GCVE는 NFS 데이터 저장소를 마운트하고 VM을 iSCSI LUN에 연결하기 위해 해당 VPC에 대한 개인 연결이 있어야 합니다.

GCVE SDDC를 구성하려면 다음을 참조하세요."Google Cloud Platform(GCP)에서 가상화 환경 배포 및 구성" . 전제 조건으로, 연결이 설정된 후 GCVE 호스트에 있는 게스트 VM이 Cloud Volumes ONTAP 의 데이터를 사용할 수 있는지 확인합니다.

Cloud Volumes ONTAP 과 GCVE가 올바르게 구성된 후 Veeam Replication 기능을 사용하고 SnapMirror 활용하여 애플리케이션 볼륨을 Cloud Volumes ONTAP에 복사하여 온프레미스 워크로드를 GCVE(애플리케이션 VMDK가 있는 VM 및 게스트 스토리지가 있는 VM)로 복구하는 작업을 자동화하도록 Veeam을 구성하기 Cloud Volumes ONTAP.

▼ **Veeam** 구성 요소 설치

배포 시나리오에 따라 배포해야 할 Veeam 백업 서버, 백업 저장소 및 백업 프록시입니다. 이 사용 사례에서는 Veeam에 대한 개체 저장소를 배포할 필요가 없으며, Scale-out 저장소도 필요하지 않습니다. "설치 절차는 Veeam 설명서를 참조하세요." 추가 정보는 다음을 참조하세요."Veeam 복제를 통한 마이그레이션"

▼ **Veeam**을 사용하여 **VM** 복제 설정

온프레미스 vCenter와 GCVE vCenter 모두 Veeam에 등록해야 합니다. "vSphere VM 복제 작업 설정" 마법사의 게스트 처리 단계에서 애플리케이션 인식 백업 및 복구에 SnapCenter 활용하므로 애플리케이션 처리 비활성화를 선택합니다.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

▼ **Microsoft SQL Server VM**의 장애 조치

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

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.

- Veeam Replication을 사용하면 DR 사이트에서 VM IP 주소를 변경할 수 있습니다.

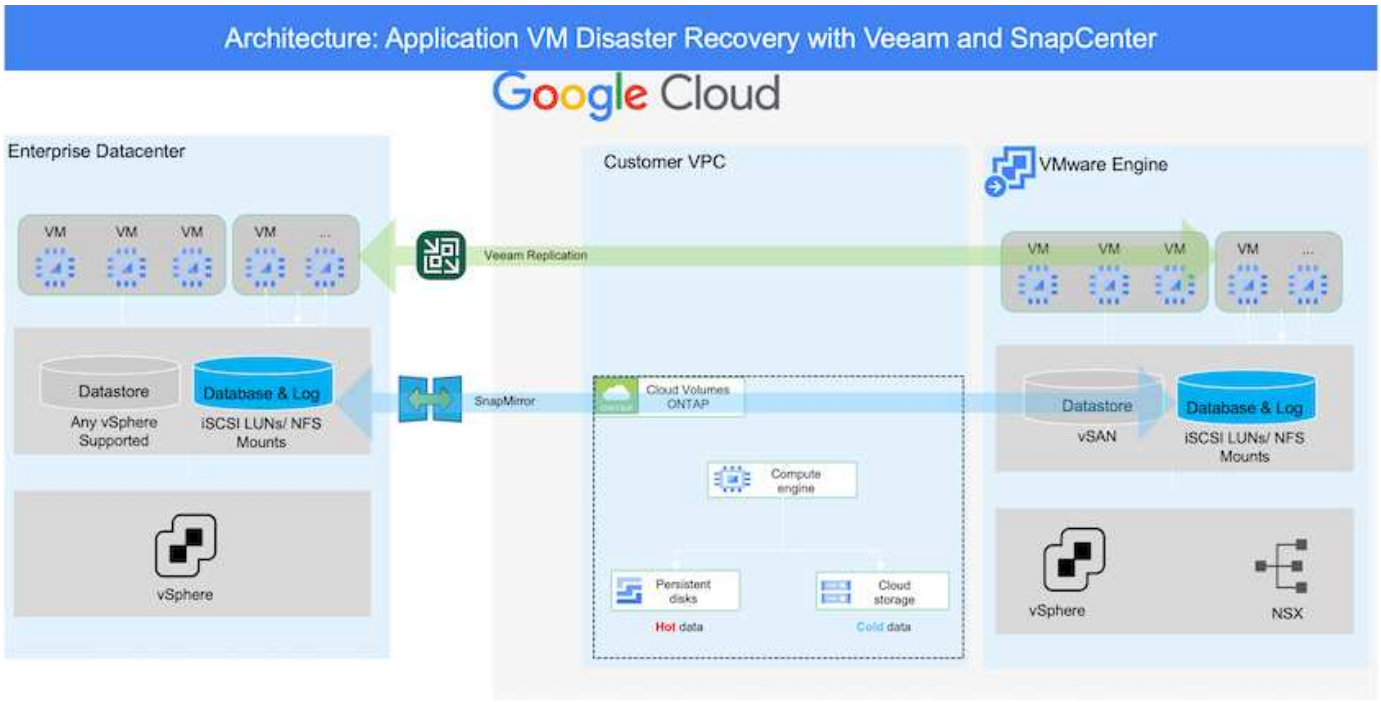
SnapCenter, Cloud Volumes ONTAP 및 **Veeam** 복제를 통한 애플리케이션 재해 복구

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 Google Cloud에서 실행되는 NetApp Cloud Volumes ONTAP 으로 복제할 수 있습니다.

개요

여기에는 애플리케이션 데이터가 포함됩니다. 하지만 실제 VM 자체는 어떻습니까? 재해 복구는 가상 머신, VMDK, 애플리케이션 데이터 등 모든 종속 구성 요소를 포괄해야 합니다. 이를 달성하기 위해 SnapMirror 와 Veeam을 함께 사용하면 VM VMDK에 vSAN 스토리지를 사용하면서 온프레미스에서 Cloud Volumes ONTAP 으로 복제된 워크로드를 원활하게 복구할 수 있습니다.

이 문서에서는 NetApp SnapMirror, Veeam 및 Google Cloud VMware Engine(GCVE)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.

온프레미스 환경과 Google Cloud 네트워크를 연결하려면 전용 상호 연결이나 Cloud VPN과 같은 연결 옵션을 사용하세요. 세그먼트는 온프레미스 VLAN 설계를 기반으로 생성되어야 합니다.

온프레미스 데이터 센터를 Google Cloud에 연결하는 데에는 여러 가지 옵션이 있으므로 이 문서에서는 구체적인 워크플로를 설명할 수 없습니다. 온프레미스와 Google 간의 적절한 연결 방법에 대해서는 Google Cloud 문서를 참조하세요.

DR 솔루션 배포

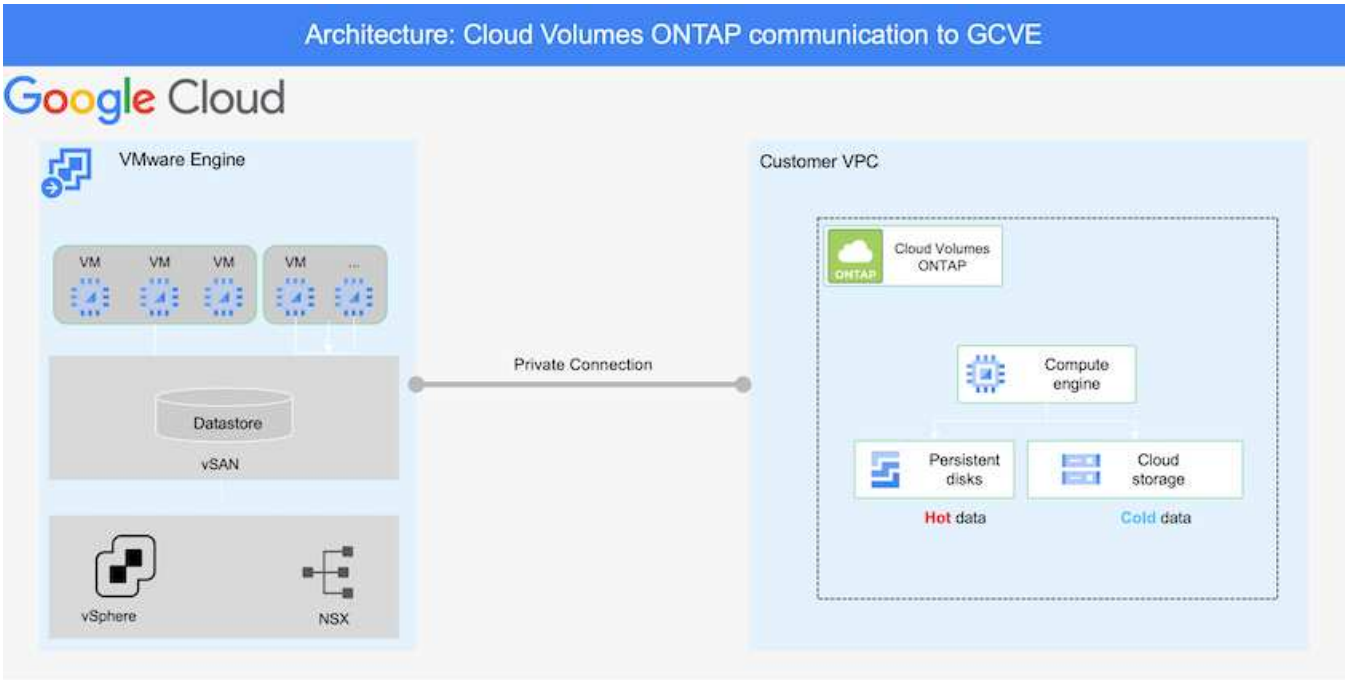
솔루션 배포 개요

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. Veeam 소프트웨어를 설치하고 가상 머신을 Google Cloud VMware Engine 인스턴스로 복제하기 시작합니다.
4. 재해 발생 시 Cloud Manager를 사용하여 SnapMirror 관계를 끊고 Veeam을 사용하여 가상 머신의 장애 조치를 트리거합니다.
   a. 애플리케이션 VM에 대한 ISCSI LUN과 NFS 마운트를 다시 연결합니다.
   b. 온라인으로 신청하세요.
5. 기본 사이트가 복구된 후 SnapMirror 역방향으로 재동기화하여 보호된 사이트로 장애 복구를 호출합니다.

배포 세부 정보

▼ **Google Cloud**에서 **CVO**를 구성하고 볼륨을 **CVO**에 복제합니다**.**

첫 번째 단계는 Google Cloud에서 Cloud Volumes ONTAP 구성하는 것입니다("씨보") 원하는 빈도와 스냅샷 보존 기간을 설정하여 원하는 볼륨을 Cloud Volumes ONTAP 에 복제합니다.



SnapCenter 설정 및 데이터 복제에 대한 단계별 샘플 지침은 다음을 참조하세요."SnapCenter 사용하여 복제 설정"

SnapCenter 사용하여 복제 설정

▼ **GCVE** 호스트 및 **CVO** 데이터 액세스 구성

SDDC를 배포할 때 고려해야 할 두 가지 중요한 요소는 GCVE 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.

Cloud Volumes ONTAP 모든 VPC에 배포할 수 있으며 GCVE는 VM을 iSCSI LUN에 연결하기 위해 해당 VPC에 대한 개인 연결이 있어야 합니다.

GCVE SDDC를 구성하려면 다음을 참조하세요."Google Cloud Platform(GCP)에서 가상화 환경 배포 및 구성" . 전제 조건으로, 연결이 설정된 후 GCVE 호스트에 있는 게스트 VM이 Cloud Volumes ONTAP 의 데이터를 사용할 수 있는지 확인합니다.

Cloud Volumes ONTAP 과 GCVE가 올바르게 구성된 후 Veeam Replication 기능을 사용하고 SnapMirror 활용하여 애플리케이션 볼륨을 Cloud Volumes ONTAP에 복사하여 온프레미스 워크로드를 GCVE(애플리케이션 VMDK가 있는 VM 및 게스트 스토리지가 있는 VM)로 복구하는 작업을 자동화하도록 Veeam을 구성하기 Cloud Volumes ONTAP.

▼ **Veeam** 구성 요소 설치

배포 시나리오에 따라 배포해야 할 Veeam 백업 서버, 백업 저장소 및 백업 프록시입니다. 이 사용 사례에서는 Veeam에 대한 개체 저장소를 배포할 필요가 없으며, Scale-out 저장소도 필요하지 않습니다.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["설치 절차는 Veeam 설명서를 참조하세요."]

▼ **Veeam**을 사용하여 **VM** 복제 설정

온프레미스 vCenter와 GCVE vCenter 모두 Veeam에 등록해야 합니다. "vSphere VM 복제 작업 설정" 마법사의 게스트 처리 단계에서 애플리케이션 인식 백업 및 복구에 SnapCenter 활용하므로 애플리케이션 처리 비활성화를 선택합니다.

vSphere VM 복제 작업 설정

▼ **Microsoft SQL Server VM**의 장애 조치

Microsoft SQL Server VM의 장애 조치

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.
- Veeam Replication을 사용하면 DR 사이트에서 VM IP 주소를 변경할 수 있습니다.

Google Cloud VMware Engine으로의 재해 복구를 위해 Veeam Replication 및 Google Cloud NetApp Volumes 데이터 저장소 사용

위기 상황에서는 포괄적인 재해 복구 계획이 기업에게 매우 중요합니다. 많은 조직이 일상 업무와 재해 복구를 위해 클라우드 컴퓨팅을 활용합니다. 이러한 사전 예방적 접근 방식을 통해 비용이 많이 드는 비즈니스 중단을 줄이거나 없앨 수 있습니다.

이 문서에서는 Veeam Backup & Replication을 사용하여 온프레미스 VMware VM에 대한 재해 복구를 Google Cloud Google Cloud NetApp Volumes (NetApp Volumes)를 사용하여 Google Cloud VMware Engine(GCVE)으로 설정하는 방법을 설명합니다.

개요

Google Cloud NetApp Volumes Google Cloud에서 사용할 수 있는 Google과 NetApp 의 스토리지 서비스입니다. NetApp Volumes 서비스는 고성능 NFS/SMB 스토리지를 제공합니다. VMware 인증 NetApp Volumes NFS 스토리지는 GCVE에서 ESXi 호스트의 외부 데이터 저장소로 사용할 수 있습니다. 사용자는 GCVE 프라이빗 클라우드와 NetApp Volumes 프로젝트 간에 피어링 연결을 만들어야 합니다. 지역 내 저장소 접근으로 인해 발생하는 네트워크 요금은 없습니다. 사용자는 Google Cloud 콘솔에서 NetApp Volumes 볼륨을 생성하고 ESXi 호스트에 볼륨을 데이터 저장소로 마운트하기 전에 삭제 보호를 활성화할 수 있습니다.

NetApp Volumes 기반 NFS 데이터 저장소는 VM 복제 기능을 제공하는 검증된 타사 솔루션을 사용하여 온프레미스에서 데이터를 복제하는 데 사용할 수 있습니다. NetApp Volumes 데이터 저장소를 추가하면 스토리지를 수용하기 위해 많은 수의 ESXi 호스트를 사용하여 Google Cloud VMware Engine(GCVE) 기반 SDDC를 구축하는 대신 비용 최적화된 배포가 가능합니다. 이런 접근 방식을 "파일럿 라이트 클러스터"라고 합니다. 파일럿 라이트 클러스터는 NetApp Volumes 데이터 저장소 용량과 함께 최소 GCVE 호스트 구성(3개의 GCVE ESXi 호스트)으로, 용량 요구 사항을 충족하기 위해 독립적인 확장을 허용합니다.

목표는 장애 조치를 관리하는 데 필요한 핵심 구성 요소만으로 비용 효율적인 인프라를 유지하는 것입니다. 파일럿 라이트 클러스터는 장애 조치 시 확장되어 더 많은 GCVE 호스트를 추가할 수 있습니다. 장애 조치가 해결되고 정상적인 운영이 재개되면 파일럿 라이트 클러스터는 규모를 줄여 저비용 운영 모드로 돌아갈 수 있습니다.

이 문서의 목적

이 문서에서는 Veeam Backup & Replication과 함께 Google Cloud NetApp Volumes 데이터스토어를 사용하여 Veeam VM 복제 소프트웨어 기능을 사용하여 온프레미스 VMware VM에 대한 재해 복구를 GCVE로 설정하는 방법을 설명합니다.

Veeam Backup & Replication은 가상 환경을 위한 백업 및 복제 애플리케이션입니다. 가상 머신이 복제되면 Veeam Backup & Replication은 대상 GCVE SDDC 클러스터에 기본 VMware vSphere 형식으로 VM의 정확한 복사본을 생성합니다. Veeam Backup & Replication은 복사본을 원본 VM과 동기화된 상태로 유지합니다. 복제는 DR 사이트에 VM의 마운트된 복사본이 즉시 시작할 수 있는 상태로 존재하므로 최상의 복구 시간 목표(RTO)를 제공합니다.

이 복제 메커니즘은 재해 발생 시 워크로드가 GCVE에서 빠르게 시작될 수 있도록 보장합니다. Veeam Backup & Replication 소프트웨어는 WAN 및 느린 연결을 통한 복제를 위한 트래픽 전송도 최적화합니다. 또한 중복된 데이터 블록, 0개 데이터 블록, 스왑 파일 및 "제외된 VM 게스트 OS 파일"도 필터링합니다. 해당 소프트웨어는 복제 트래픽도 압축합니다. 복제 작업이 전체 네트워크 대역폭을 소모하는 것을 방지하려면 WAN 가속기와 네트워크 제한 규칙을 활용할 수 있습니다.

Veeam Backup & Replication의 복제 프로세스는 작업 중심입니다. 즉, 복제는 복제 작업을 구성하여 수행됩니다. 재해가 발생하는 경우 복제본으로 장애 조치를 취하여 VM을 복구할 수 있습니다. 장애 조치가 수행되면 복제된 VM이 원래 VM의 역할을 대신하게 됩니다. 장애 조치는 복제본의 최신 상태나 알려진 양호한 복원 지점으로 수행할 수 있습니다. 이를 통해 필요에 따라 랜섬웨어 복구나 분리된 테스트가 가능합니다. Veeam Backup & Replication은 다양한 재해 복구 시나리오를 처리하기 위한 여러 가지 옵션을 제공합니다.

솔루션 개요

이 솔루션은 다음과 같은 상위 수준 단계를 포함합니다.

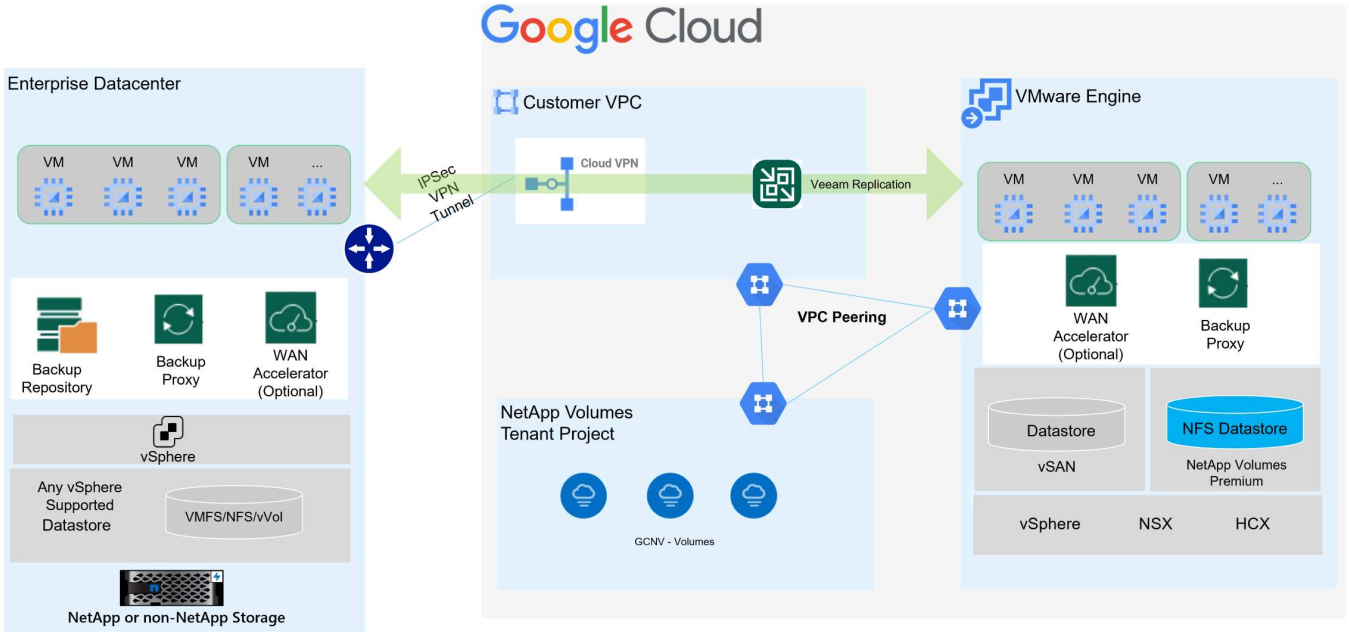
1. Google Cloud NetApp Volumes 사용하여 NFS 볼륨 만들기
2. NetApp Volumes NFS 볼륨에서 GCVE 데이터 저장소를 생성하려면 GCP 프로세스를 따르세요.
3. Veeam Backup & Replication을 사용하여 VM 복제본을 생성하는 복제 작업을 설정합니다.
4. 장애 조치 계획을 만들고 장애 조치를 수행합니다.
5. 재해 이벤트가 완료되고 기본 사이트가 가동되면 프로덕션 VM으로 다시 전환합니다.

NetApp Volumes에서 GCVE 데이터 저장소로 사용할 볼륨을 생성하는 경우 NFS v3만 지원됩니다.

GCVE의 데이터 저장소로 NetApp Volumes NFS 볼륨을 사용하는 방법에 대한 자세한 내용은 다음을 확인하세요. "Google Cloud NetApp Volumes 에서 호스팅하는 vSphere 데이터 저장소로 NFS 볼륨 사용" .

아키텍처

다음 다이어그램은 이 문서에 제시된 솔루션의 아키텍처를 보여줍니다. 권장되는 모범 사례는 온-프레미스 사이트와 GCVE SDDC 모두에 Veeam Backup & Replication 서버를 두는 것입니다. 백업 및 복구는 온프레미스의 Veeam 서버에서 수행 및 관리되고, 복제는 GCVE SDDC의 Veeam 서버에서 관리됩니다. 이 아키텍처는 기본 데이터 센터에 장애가 발생할 때 가장 높은 가용성을 제공합니다.



GCVE 및 **NetApp** 볼륨 데이터 저장소에 대한 **Veeam** 복제를 위한 필수 구성 요소

이 솔루션에는 다음과 같은 구성 요소와 구성이 필요합니다.

1. NetApp Volumes에는 NFS 볼륨을 생성할 수 있는 충분한 여유 용량을 갖춘 스토리지 풀이 있습니다.
2. Veeam Backup and Replication 소프트웨어는 적절한 네트워크 연결을 갖춘 온프레미스 환경에서 실행됩니다.
3. Veeam Backup & Replication 백업 VM이 소스와 대상 GCVE SDDC 클러스터에 연결되어 있는지 확인하세요.

4. Veeam Backup & Replication 백업 VM이 소스 및 대상 GCVE 클러스터 모두에서 Veeam Proxy 서버 VM에 연결되어 있는지 확인하세요.
5. 백업 서버는 짧은 이름을 확인하고 소스 및 대상 vCenter에 연결할 수 있어야 합니다.

사용자는 VMware Engine Cloud 콘솔 UI 내의 VPC 네트워크 피어링 또는 개인 연결 페이지를 사용하여 GCVE 프라이빗 클라우드와 NetApp Volumes 프로젝트 간에 피어링 연결을 만들어야 합니다.

> Veeam Backup and Replication 인벤토리에 GCVE vCenter 서버를 추가하려면 Veeam에 상승된 권한이 있는 GCVE 솔루션 사용자 계정이 필요합니다. 자세한 내용은 Google Cloud Platform(GCP) 설명서를 참조하십시오 "VMware Engine 권한 상승".

추가 정보는 다음을 참조하세요. "고려 사항 및 제한 사항" Veeam Backup & Replication 설명서에서.

배포 단계

다음 섹션에서는 Google Cloud NetApp Volumes 사용하여 NFS 데이터 저장소를 만들고 마운트하는 배포 단계와 Veeam Backup and Replication을 사용하여 온프레미스 데이터 센터와 Google Cloud VMware Engine 간에 전체 재해 복구 솔루션을 구현하는 방법을 간략하게 설명합니다.

GCVE를 위한 NetApp Volumes NFS 볼륨 및 데이터 저장소 생성

참조하다 "Google Cloud NetApp Volumes 에서 호스팅하는 vSphere 데이터 저장소로 NFS 볼륨 사용" GCVE를 위한 데이터 저장소로 Google Cloud NetApp Volumes 사용하는 방법에 대한 개요를 알아보세요.

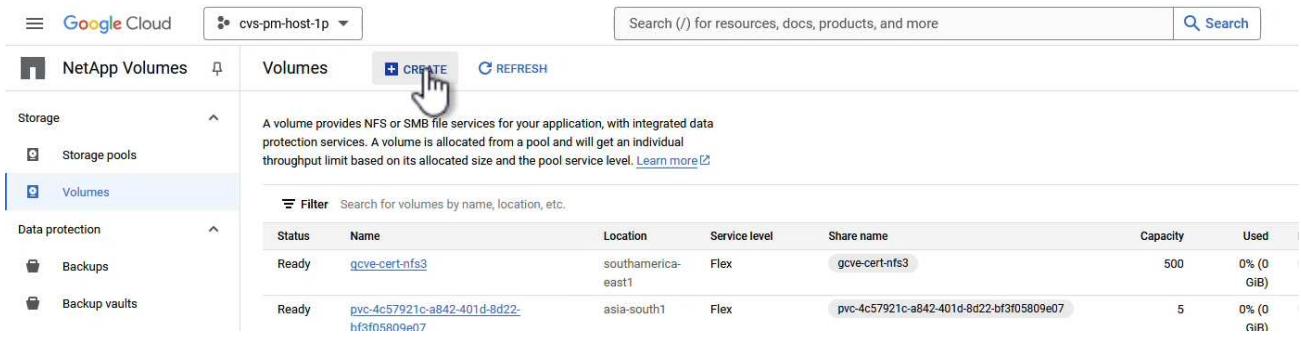
NetApp Volumes를 사용하여 GCVE용 NFS 데이터 저장소를 만들고 사용하려면 다음 단계를 완료하세요.

▼ **NetApp** 볼륨 **NFS** 볼륨 생성

Google Cloud NetApp Volumes Google Cloud Platform(GCP) 콘솔에서 액세스합니다.

참조하다 "볼륨을 생성합니다" 이 단계에 대한 자세한 내용은 Google Cloud NetApp Volumes 설명서를 참조하세요.

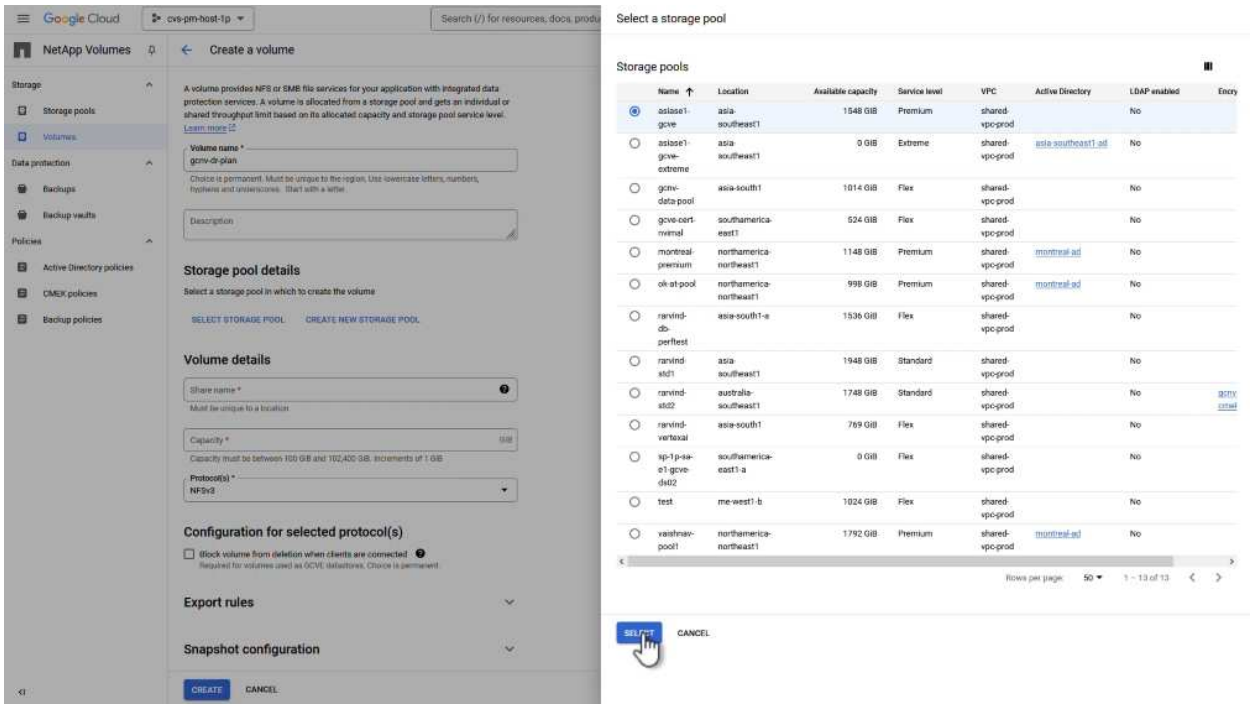
1. 웹 브라우저에서 다음으로 이동합니다. https://console.cloud.google.com/ GCP 콘솔에 로그인하세요. 시작하려면 * NetApp Volumes*를 검색하세요.
2. * NetApp Volumes* 관리 인터페이스에서 *만들기*를 클릭하여 NFS 볼륨을 만듭니다.

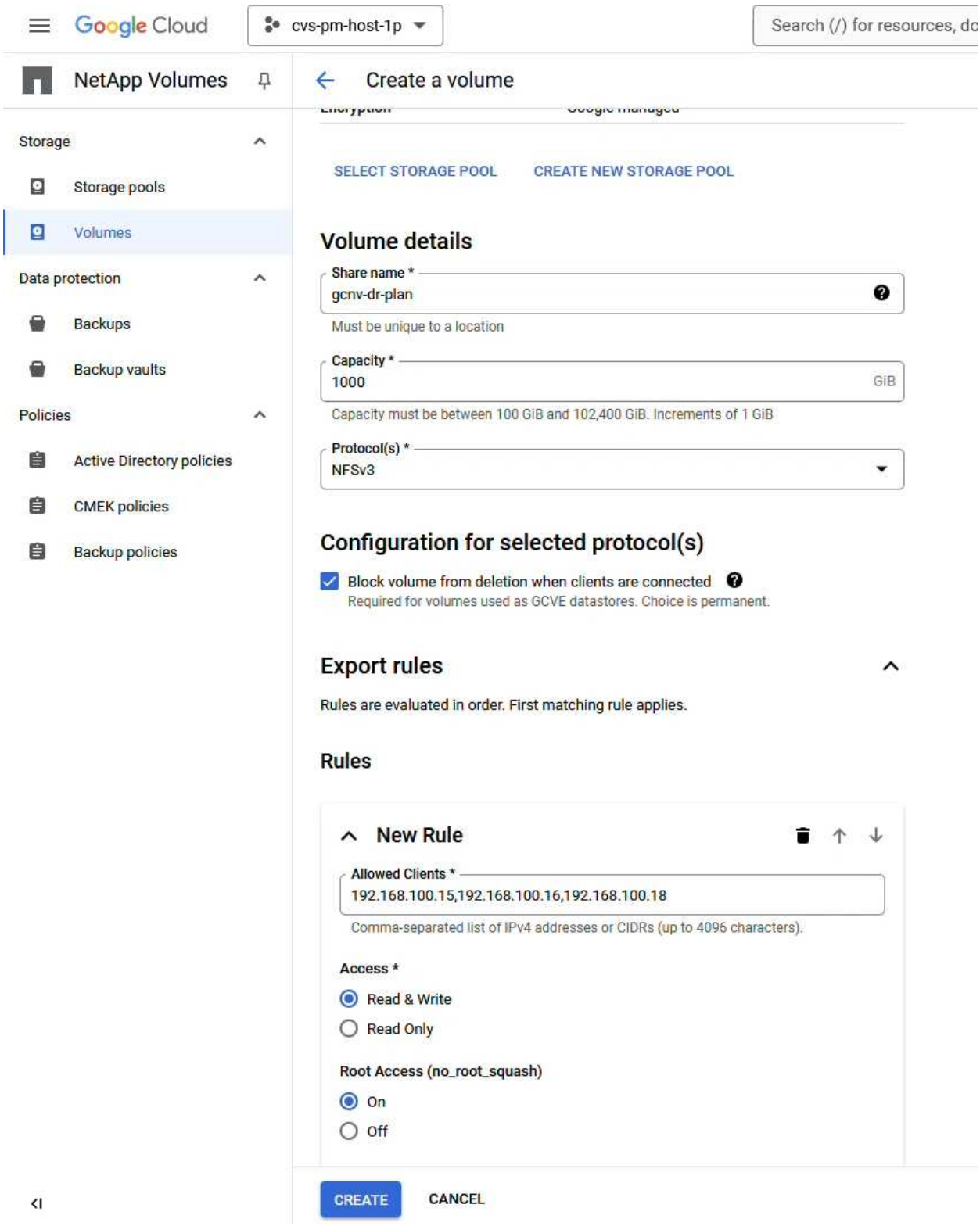


3. 볼륨 생성 마법사에서 필요한 모든 정보를 입력합니다.
   - 볼륨의 이름입니다.

- 볼륨을 생성할 스토리지 풀입니다.
- NFS 볼륨을 마운트할 때 사용되는 공유 이름입니다.
- 볼륨의 용량(GiB)입니다.
- 사용할 저장 프로토콜입니다.
- 클라이언트가 연결되면 볼륨 삭제 차단 확인란을 선택합니다(데이터 저장소로 마운트할 때 GCVE에서 필요).
- 볼륨에 접근하기 위한 내보내기 규칙입니다. 이는 NFS 네트워크에 있는 ESXi 어댑터의 IP 주소입니다.
- 로컬 스냅샷을 사용하여 볼륨을 보호하는 데 사용되는 스냅샷 일정입니다.
- 선택적으로 볼륨을 백업하거나 볼륨에 대한 레이블을 만들 수 있습니다.

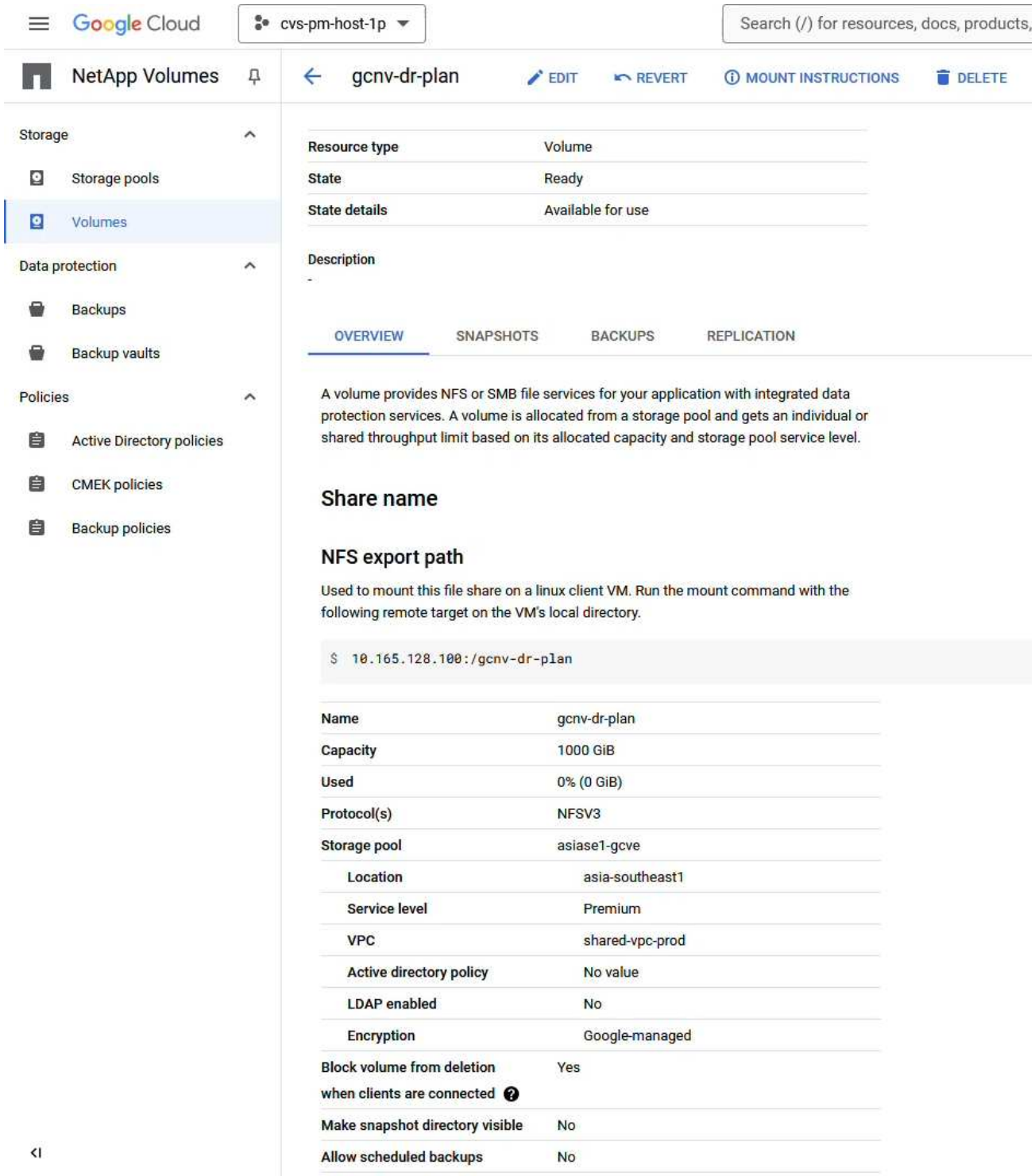
NetApp Volumes에서 GCVE 데이터 저장소로 사용할 볼륨을 생성하는 경우 NFS v3만 지원됩니다.





볼륨 생성을 완료하려면 *만들기*를 클릭하세요.

4. 볼륨이 생성되면 볼륨을 마운트하는 데 필요한 NFS 내보내기 경로를 볼륨의 속성 페이지에서 볼 수 있습니다.



▼ **GCVE**에서 **NFS** 데이터 저장소 마운트

이 글을 쓰는 시점에서 GCVE에 데이터 저장소를 마운트하는 프로세스에는 볼륨을 NFS 데이터 저장소로 마운트하기 위해 GCP 지원 티켓을 열어야 합니다.

참조하다 "Google Cloud NetApp Volumes 에서 호스팅하는 vSphere 데이터 저장소로 NFS 볼륨 사용" 자세한 내용은.

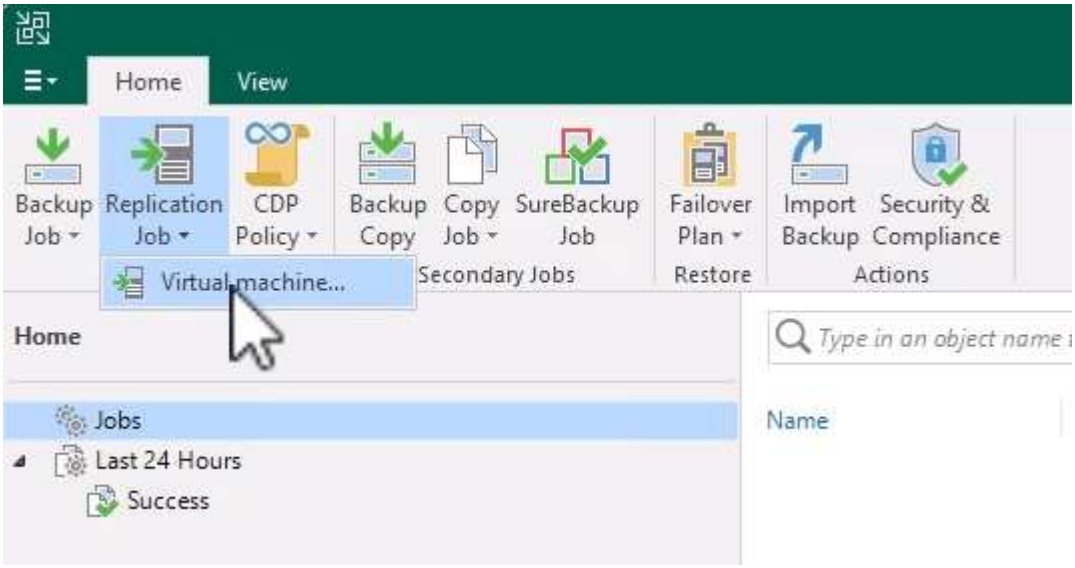
VM을 **GCVE**로 복제하고 장애 조치 계획을 실행하고 장애 복구합니다**.**

▼ **GCVE**에서 **NFS** 데이터 저장소에 **VM** 복제

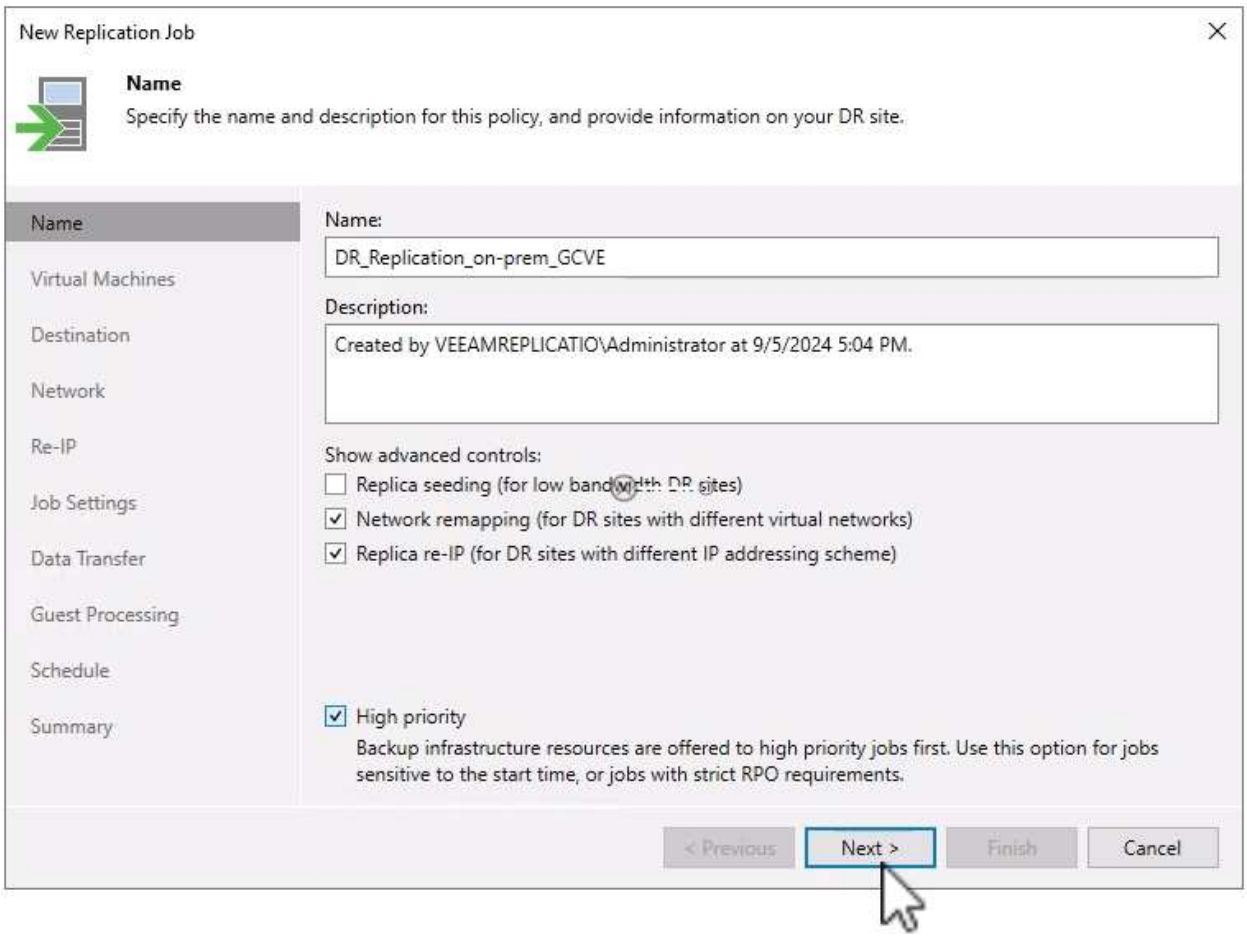
Veeam Backup & Replication은 복제 중에 VMware vSphere 스냅샷 기능을 활용하고, Veeam Backup & Replication은 VMware vSphere에 VM 스냅샷을 생성하도록 요청합니다. VM 스냅샷은 가상 디스크, 시스템 상태, 구성 및 메타데이터를 포함하는 VM의 특정 시점 복사본입니다. Veeam Backup & Replication은 복제를 위한 데이터 소스로 스냅샷을 사용합니다.

VM을 복제하려면 다음 단계를 완료하세요.

1. Veeam 백업 및 복제 콘솔을 엽니다.
2. 홈 탭에서 *복제 작업 > 가상 머신...*을 클릭합니다.

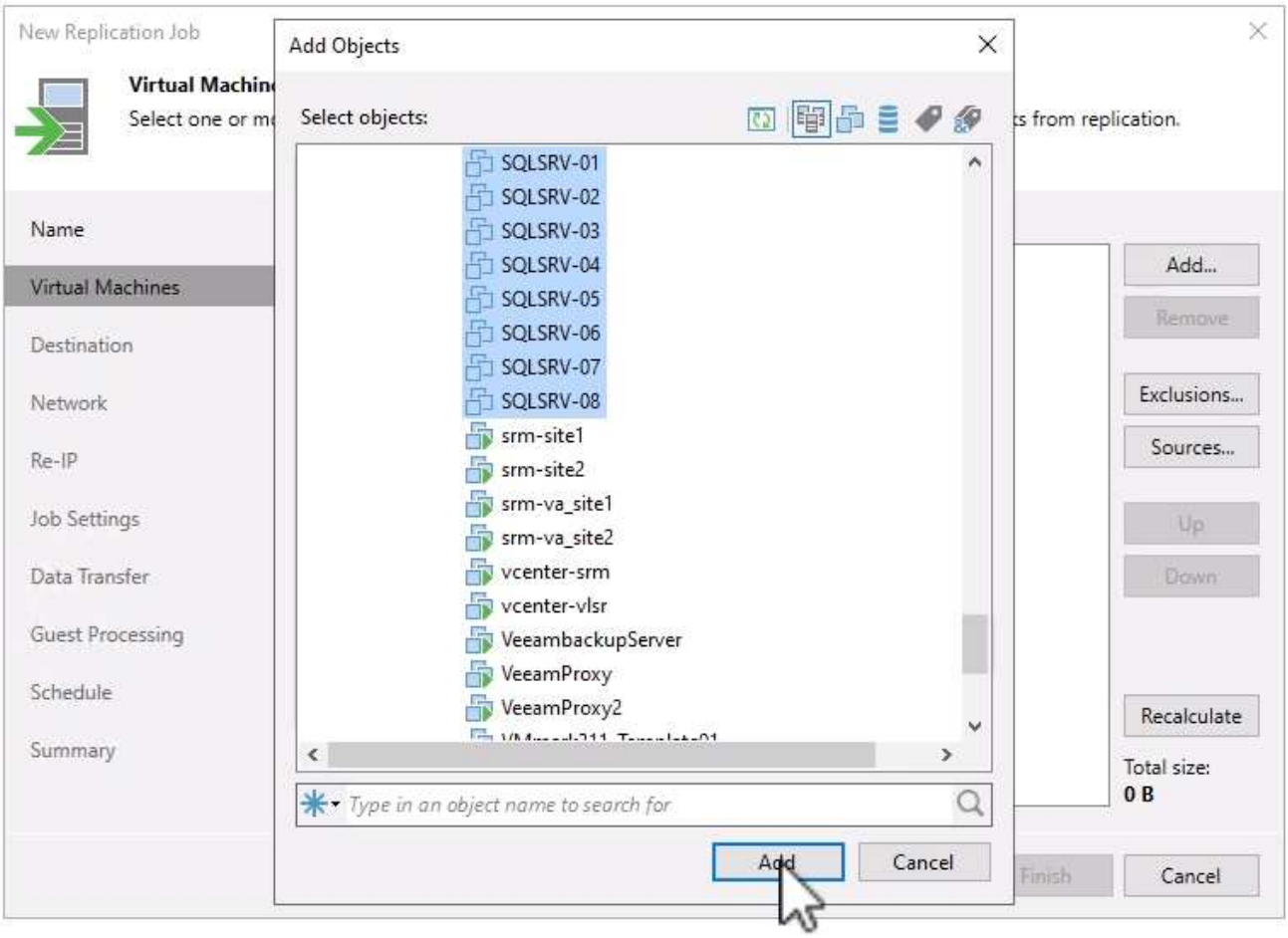


3. 새 복제 작업 마법사의 이름 페이지에서 작업 이름을 지정하고 적절한 고급 제어 확인란을 선택합니다.
   - 온프레미스와 GCP 간 연결의 대역폭이 제한된 경우 복제본 시딩 확인란을 선택합니다.
   - GCVE SDDC의 세그먼트가 온프레미스 사이트 네트워크의 세그먼트와 일치하지 않는 경우 네트워크 리매핑(다른 네트워크를 사용하는 GCVE SDDC 사이트의 경우) 확인란을 선택합니다.
   - 온프레미스 프로덕션 사이트의 IP 주소 지정 방식이 대상 GCVE 사이트의 방식과 다른 경우, 복제본 재 IP(다른 IP 주소 지정 방식을 사용하는 DR 사이트용) 확인란을 선택합니다.

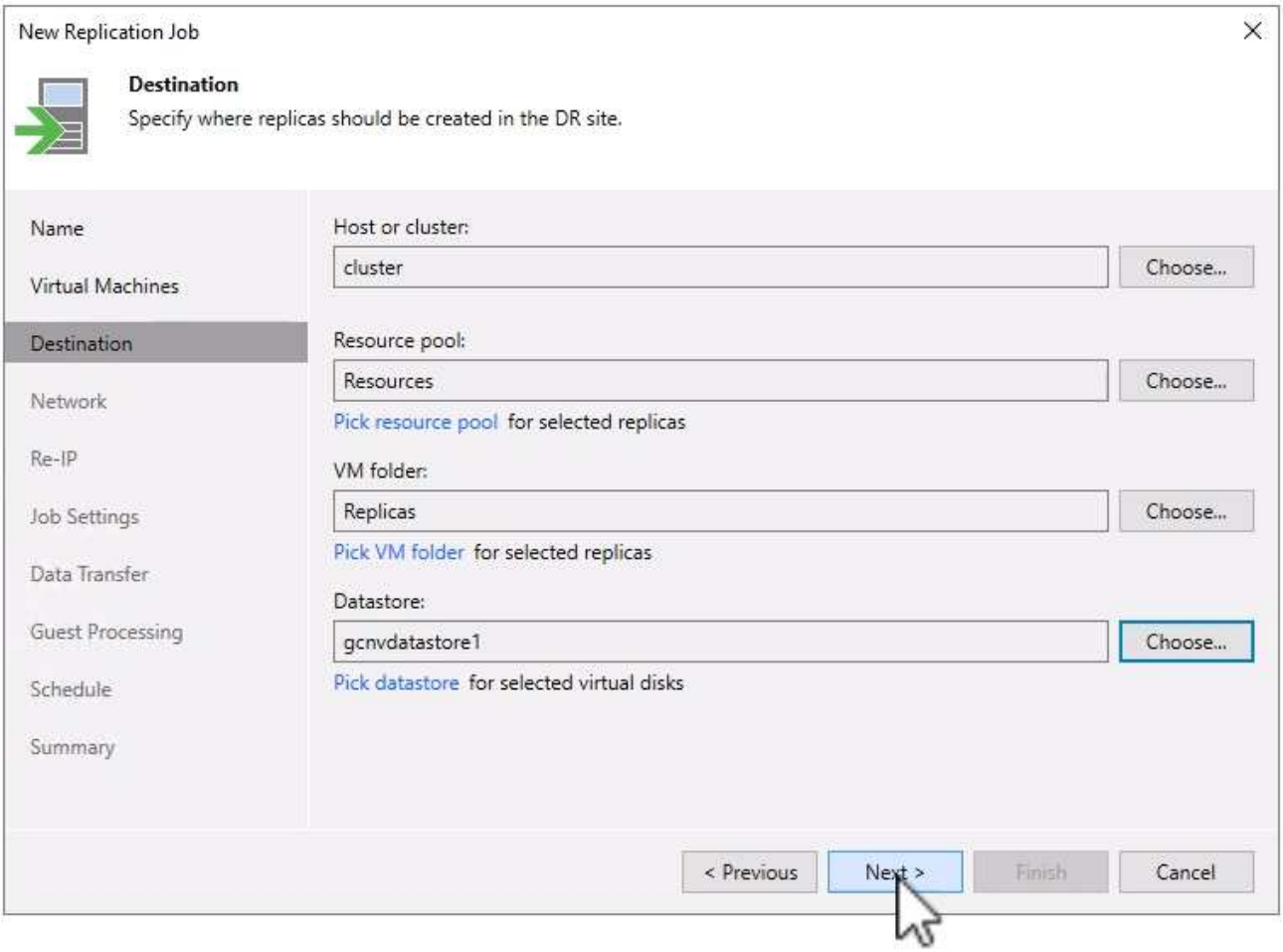


4. 가상 머신 페이지에서 GCVE SDDC에 연결된 NetApp Volumes 데이터 저장소에 복제할 VM을 선택합니다. 추가*를 클릭한 다음, *개체 추가 창에서 필요한 VM이나 VM 컨테이너를 선택하고 *추가*를 클릭합니다. *다음*을 클릭하세요.

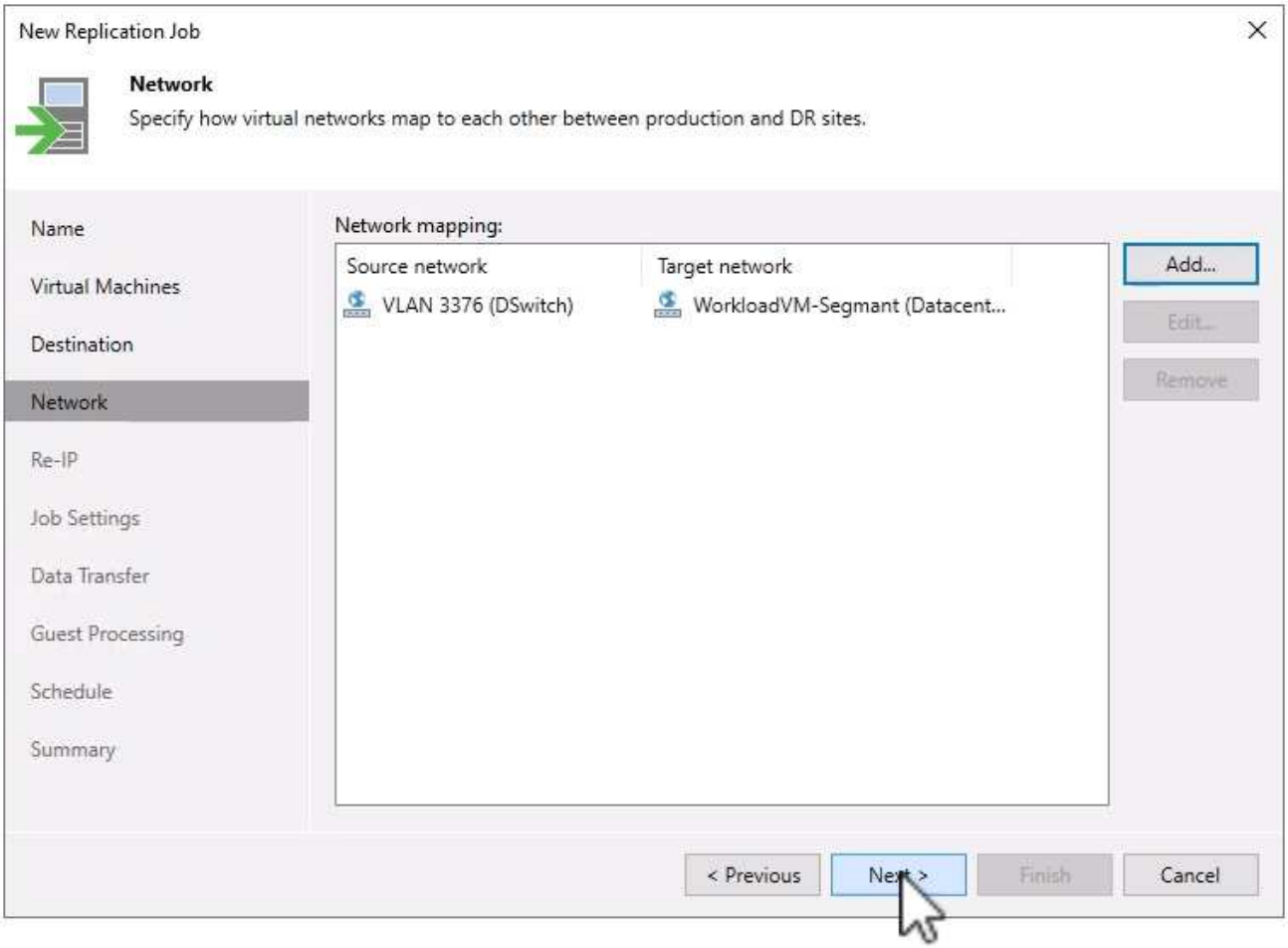
> 가상 머신을 vSAN에 배치하여 사용 가능한 vSAN 데이터 저장소 용량을 채울 수 있습니다. 파일럿 라이트 클러스터에서는 3노드 vSAN 클러스터의 사용 가능한 용량이 제한됩니다. 나머지 데이터는 Google Cloud NetApp Volumes 데이터 저장소에 쉽게 저장하여 VM을 복구할 수 있으며, 나중에 CPU/메모리 요구 사항을 충족하도록 클러스터를 확장할 수 있습니다.



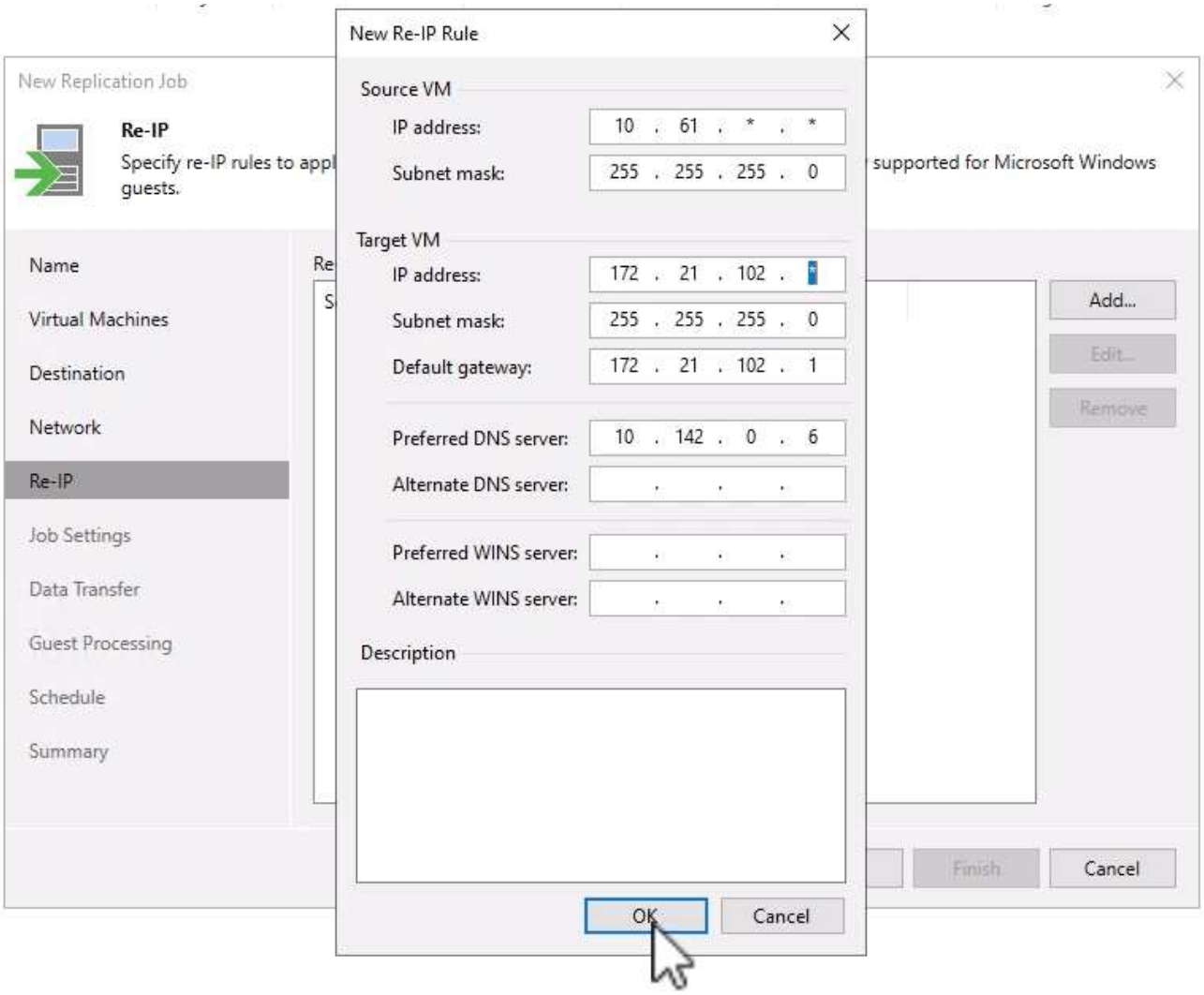
5. 대상 페이지에서 대상을 GCVE SDDC 클러스터/호스트, VM 복제본에 대한 적절한 리소스 풀, VM 폴더 및 NetApp Volumes 데이터 저장소로 선택합니다. 계속하려면 *다음*을 클릭하세요.



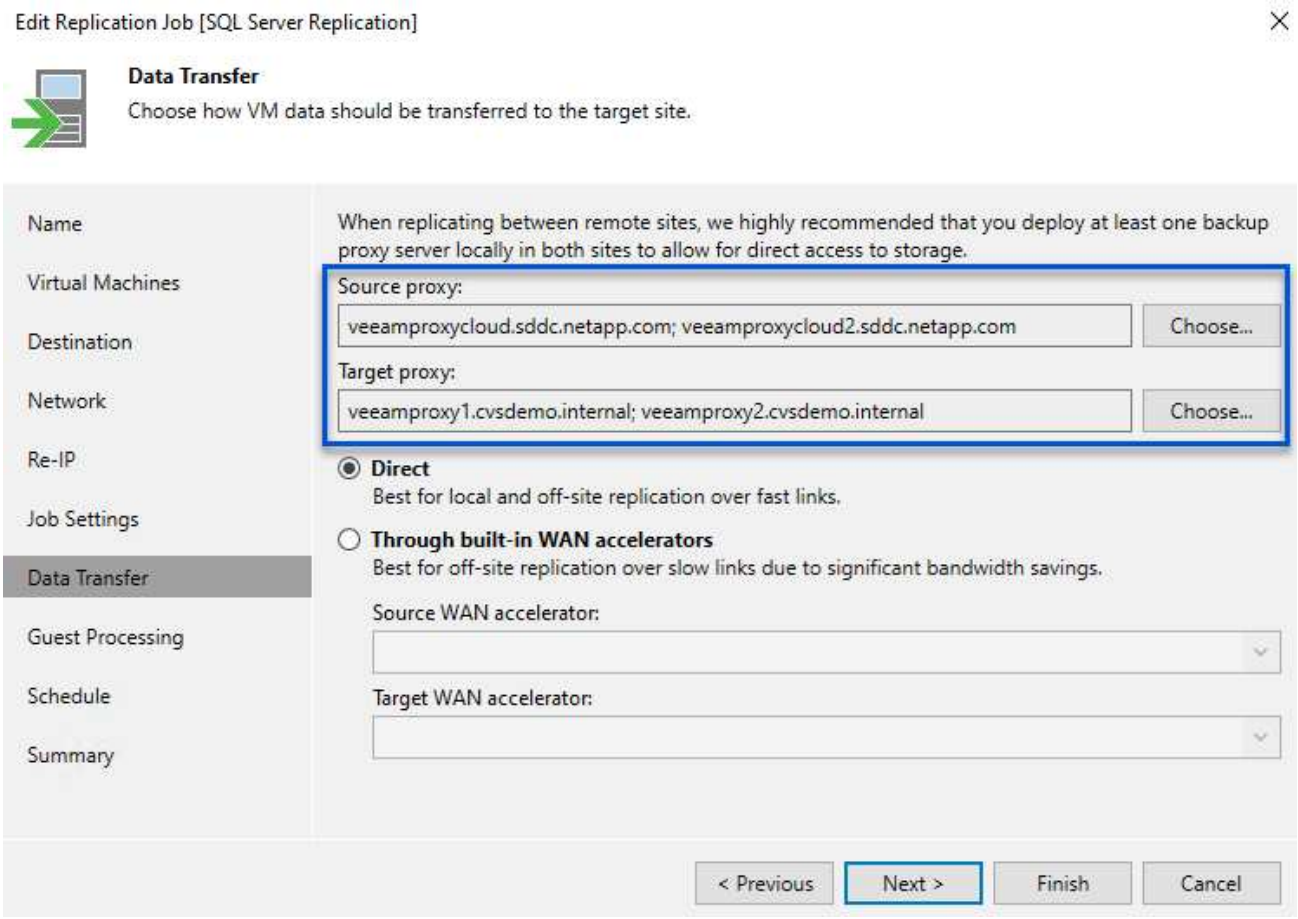
6. 네트워크 페이지에서 필요에 따라 소스 및 대상 가상 네트워크 간의 매핑을 만듭니다. 계속하려면 *다음*을 클릭하세요.



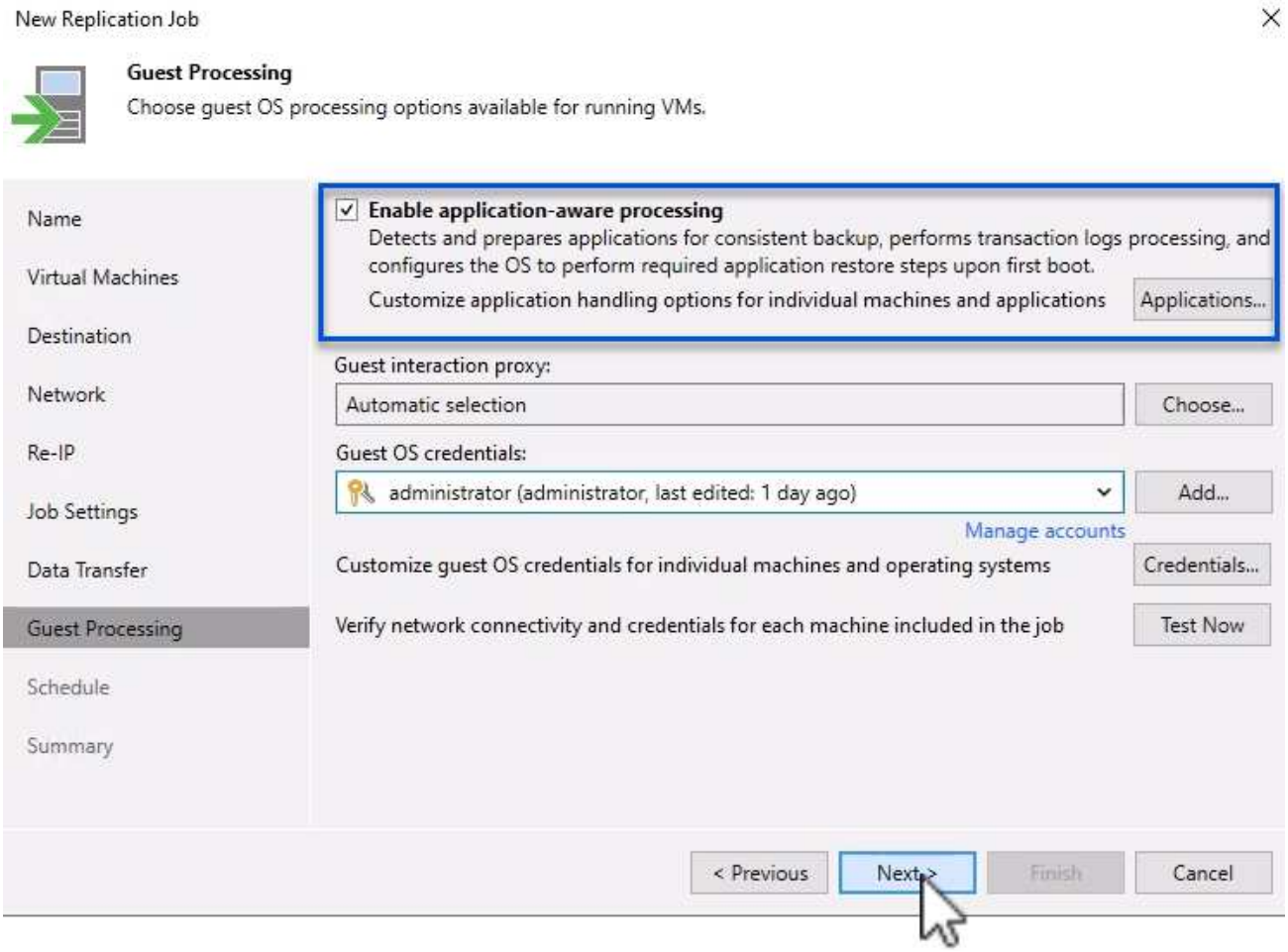
7. **Re-IP** 페이지에서 추가... 버튼을 클릭하여 새로운 re-ip 규칙을 추가합니다. 장애 조치 시 소스 VM에 적용될 네트워킹을 지정하려면 소스 및 대상 VM IP 범위를 입력합니다. 별표를 사용하여 해당 옥텟에 대한 주소 범위를 지정합니다. 계속하려면 *다음*을 클릭하세요.



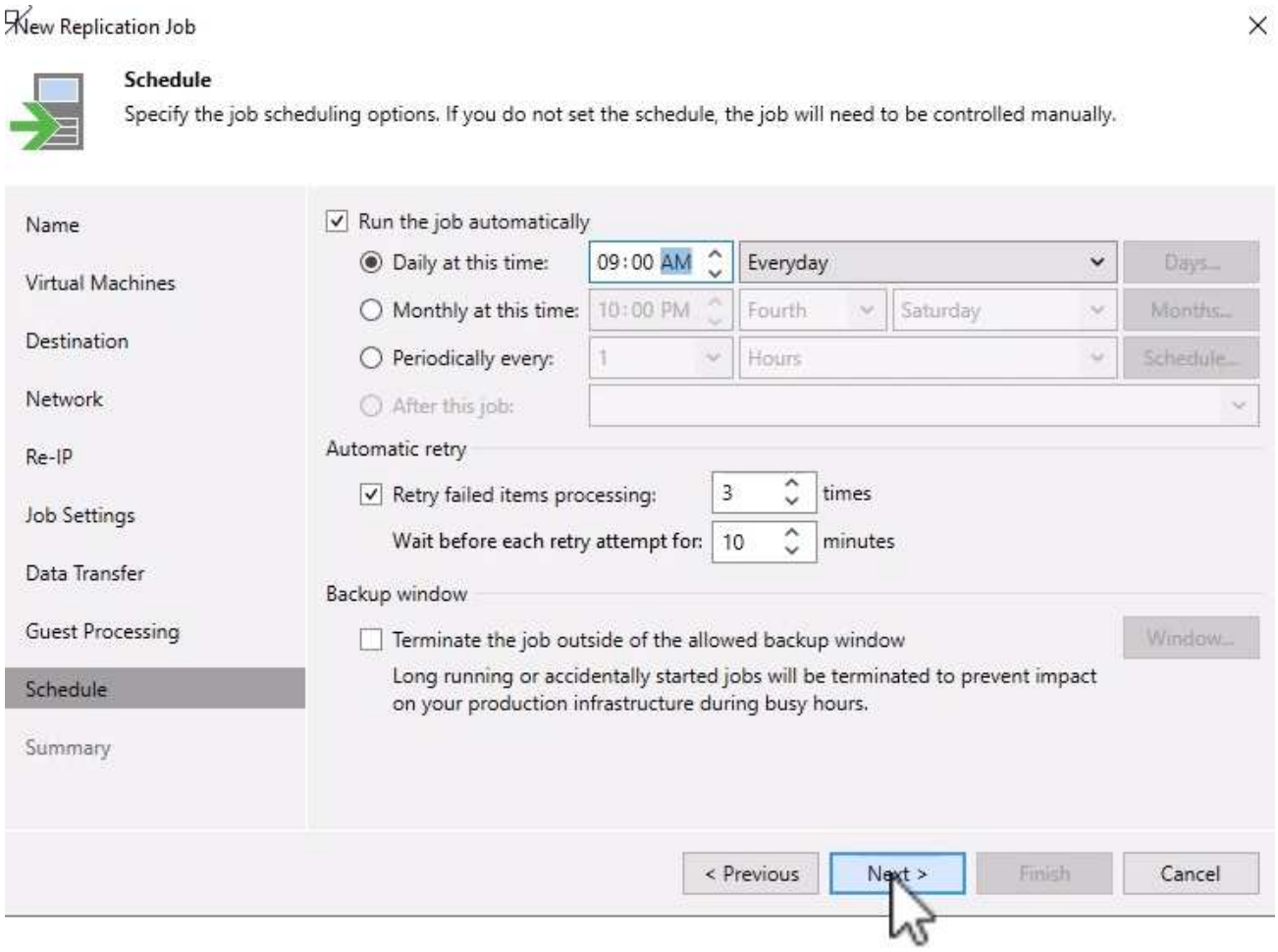
8. 작업 설정 페이지에서 VM 복제본의 메타데이터를 저장할 백업 저장소와 보존 정책을 지정하고, 추가 작업 설정을 위해 하단에 있는 고급... 버튼을 선택합니다. 계속하려면 *다음*을 클릭하세요.
9. *데이터 전송*에서 소스 및 대상 사이트에 있는 프록시 서버를 선택하고 직접 옵션을 선택된 상태로 유지합니다. WAN 가속기도 구성된 경우 여기에서 선택할 수 있습니다. 계속하려면 *다음*을 클릭하세요.



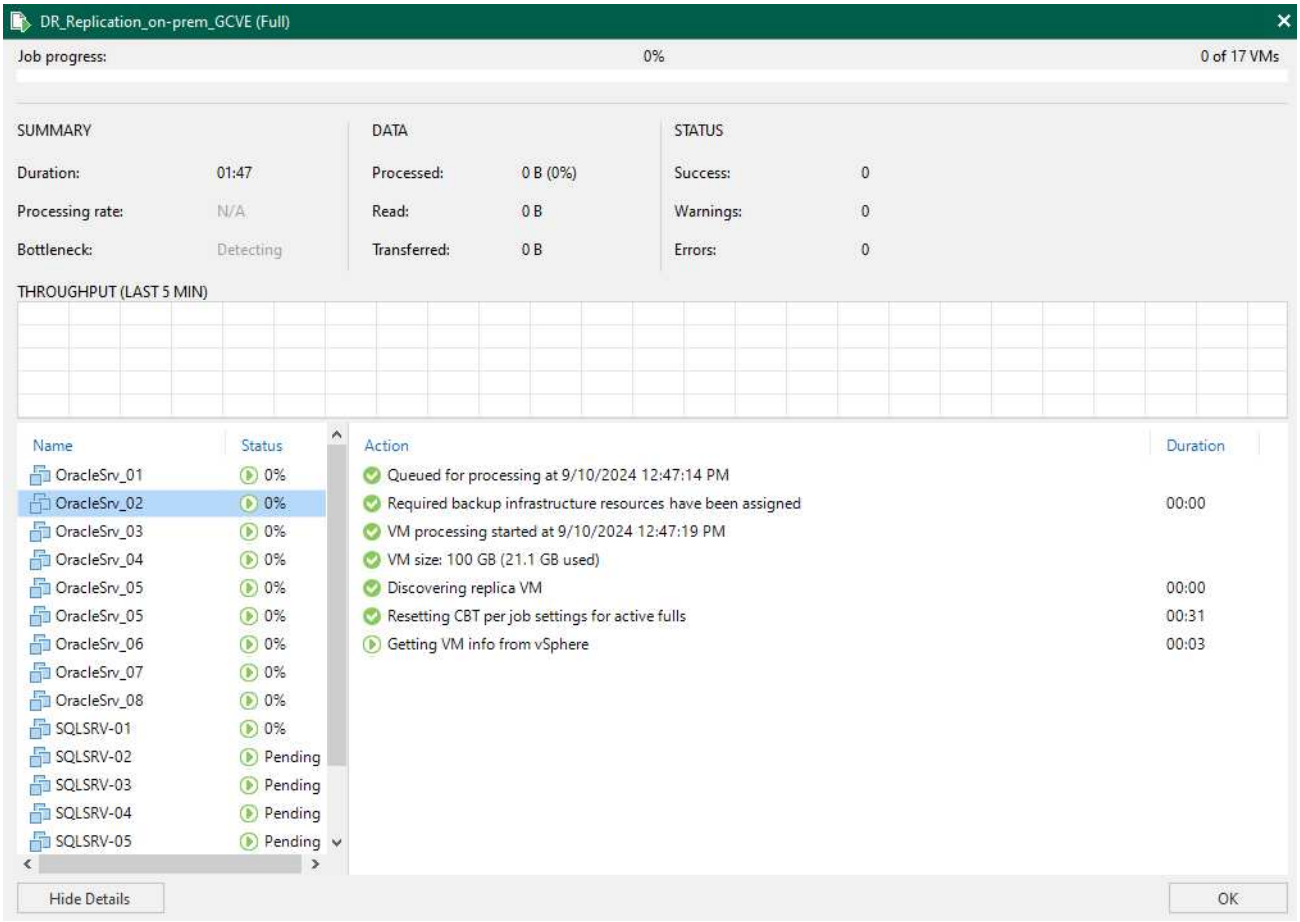
10. 게스트 처리 페이지에서 필요에 따라 애플리케이션 인식 처리 사용 상자를 선택하고 *게스트 OS 자격 증명*을 선택합니다. 계속하려면 *다음*을 클릭하세요.



11. 일정 페이지에서 복제 작업이 실행되는 시간과 빈도를 정의합니다. 계속하려면 *다음*을 클릭하세요.



12. 마지막으로, 요약 페이지에서 작업 설정을 검토하세요. 마침을 클릭하면 작업 실행 확인란을 선택하고 *마침*을 클릭하여 복제 작업 생성을 완료합니다.
13. 복제 작업을 실행하면 작업 상태 창에서 해당 작업을 볼 수 있습니다.



Veeam 복제에 대한 추가 정보는 다음을 참조하세요."복제 작동 방식"

▼ 장애 조치 계획 만들기

초기 복제 또는 시딩이 완료되면 장애 조치 계획을 만듭니다. 장애 조치 계획은 종속된 VM에 대해 하나씩 또는 그룹별로 자동으로 장애 조치를 수행하는 데 도움이 됩니다. 장애 조치 계획은 부팅 지연을 포함하여 VM이 처리되는 순서에 대한 청사진입니다. 장애 조치 계획은 또한 중요한 종속 VM이 이미 실행 중인지 확인하는 데 도움이 됩니다.

초기 복제 또는 시딩을 완료한 후 장애 조치 계획을 수립합니다. 이 계획은 개별적으로 또는 그룹으로 종속된 VM의 장애 조치를 조율하기 위한 전략적 청사진 역할을 합니다. VM의 처리 순서를 정의하고, 필요한 부팅 지연을 통합하며, 중요한 종속 VM이 다른 VM보다 먼저 작동하도록 보장합니다. 잘 구성된 장애 조치 계획을 구현함으로써 조직은 재해 복구 프로세스를 간소화하고, 가동 중지 시간을 최소화하며, 장애 조치 이벤트 중에 상호 종속된 시스템의 무결성을 유지할 수 있습니다.

Veeam Backup & Replication은 계획을 생성할 때 가장 최근의 복원 지점을 자동으로 식별하고 이를 사용하여 VM 복제본을 시작합니다.

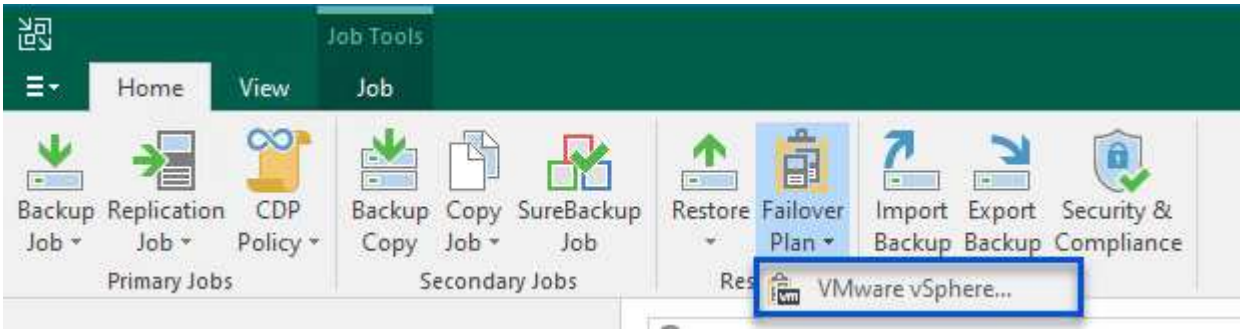
ⓘ 장애 조치 계획은 초기 복제가 완료되고 VM 복제본이 준비 상태가 된 후에만 생성할 수 있습니다.

ⓘ 장애 조치 계획을 실행할 때 동시에 시작할 수 있는 VM의 최대 수는 10개입니다.

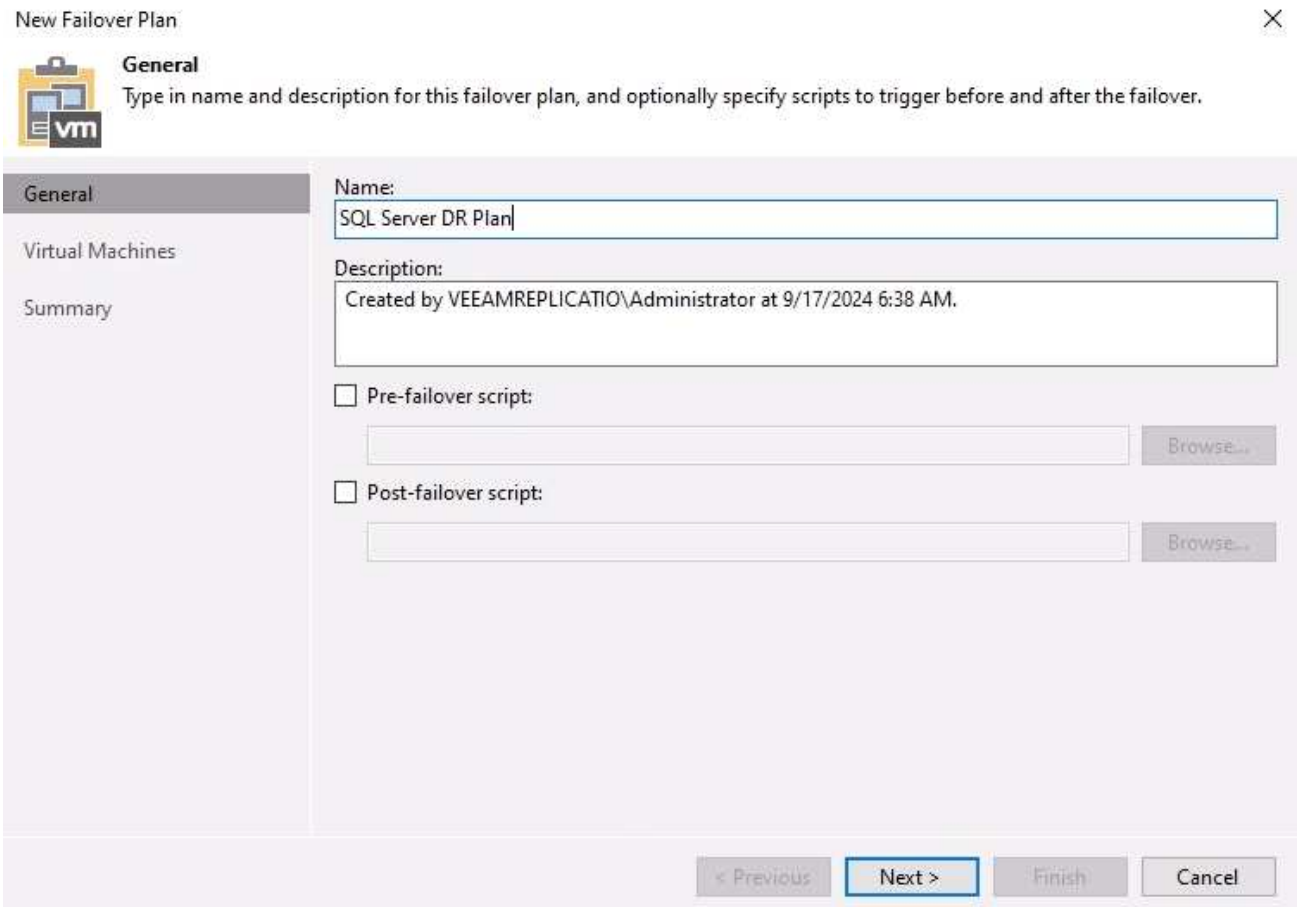
ⓘ 장애 조치 프로세스 동안 소스 VM의 전원은 꺼지지 않습니다.

*장애 조치 계획*을 생성하려면 다음 단계를 완료하세요.

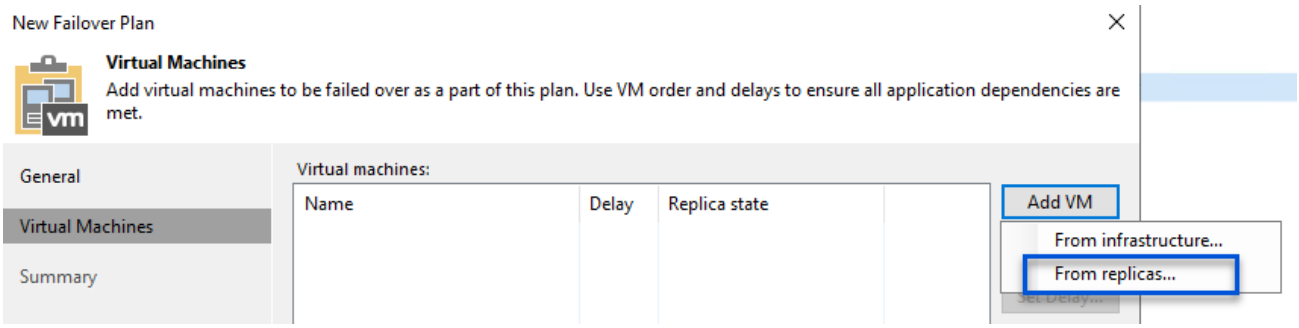
1. 홈 보기에서 복원 섹션의 장애 조치 계획 버튼을 클릭합니다. 드롭다운에서 *VMware vSphere…*를 선택하세요.

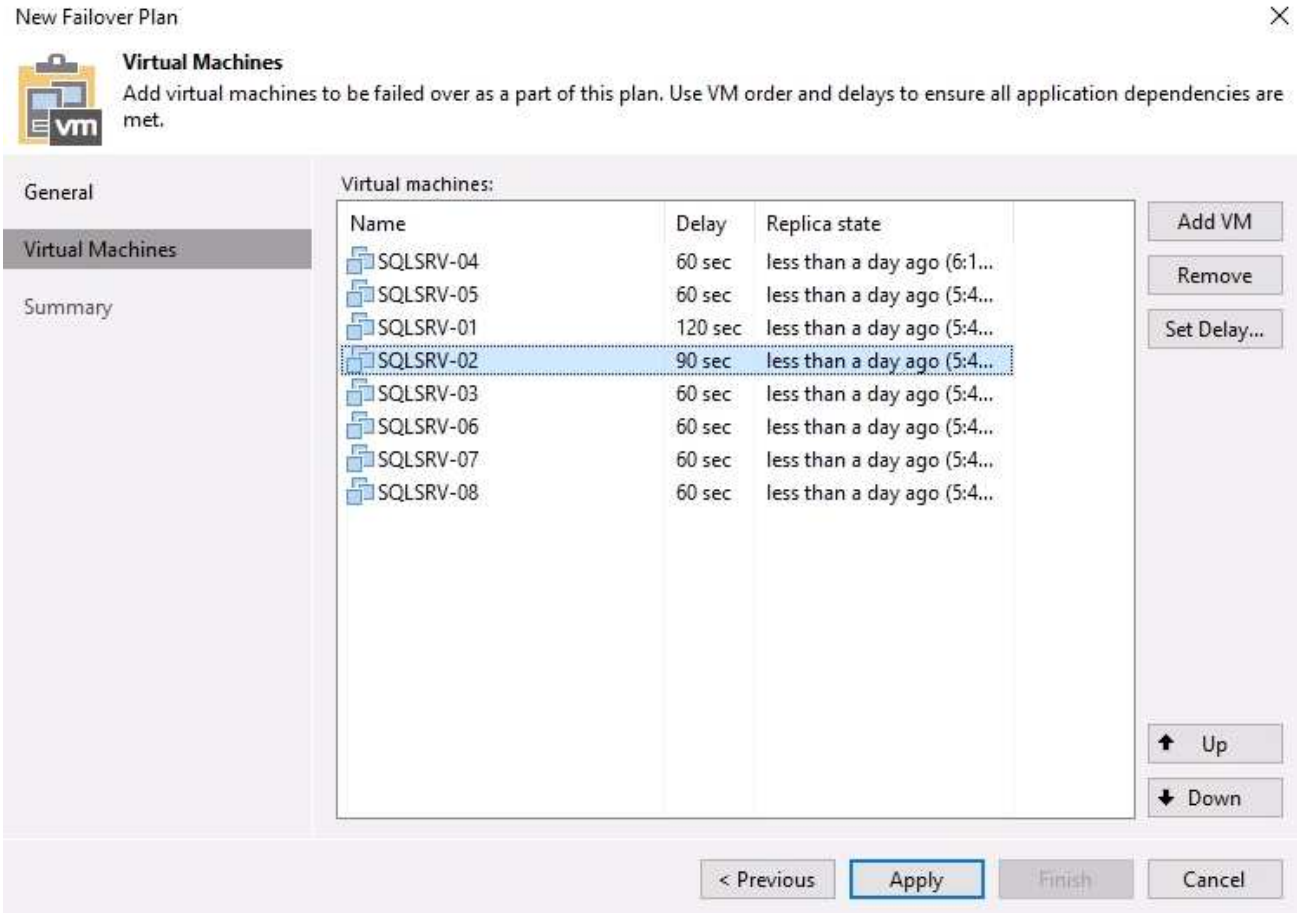


2. 새로운 장애 조치 계획 마법사의 일반 페이지에서 계획의 이름과 설명을 입력합니다. 필요에 따라 사전 및 사후 장애 조치 스크립트를 추가할 수 있습니다. 예를 들어, 복제된 VM을 시작하기 전에 VM을 종료하는 스크립트를 실행합니다.



3. 가상 머신 페이지에서 **VM** 추가 버튼을 클릭하고 *복제본에서…*를 선택합니다. 장애 조치 계획에 포함할 VM을 선택한 다음, 애플리케이션 종속성을 충족하도록 VM 부팅 순서와 필요한 부팅 지연을 수정합니다.





계속하려면 *적용*을 클릭하세요.

4. 마지막으로 모든 장애 조치 계획 설정을 검토하고 *마침*을 클릭하여 장애 조치 계획을 만듭니다.

복제 작업 생성에 대한 추가 정보는 다음을 참조하세요."복제 작업 생성" .

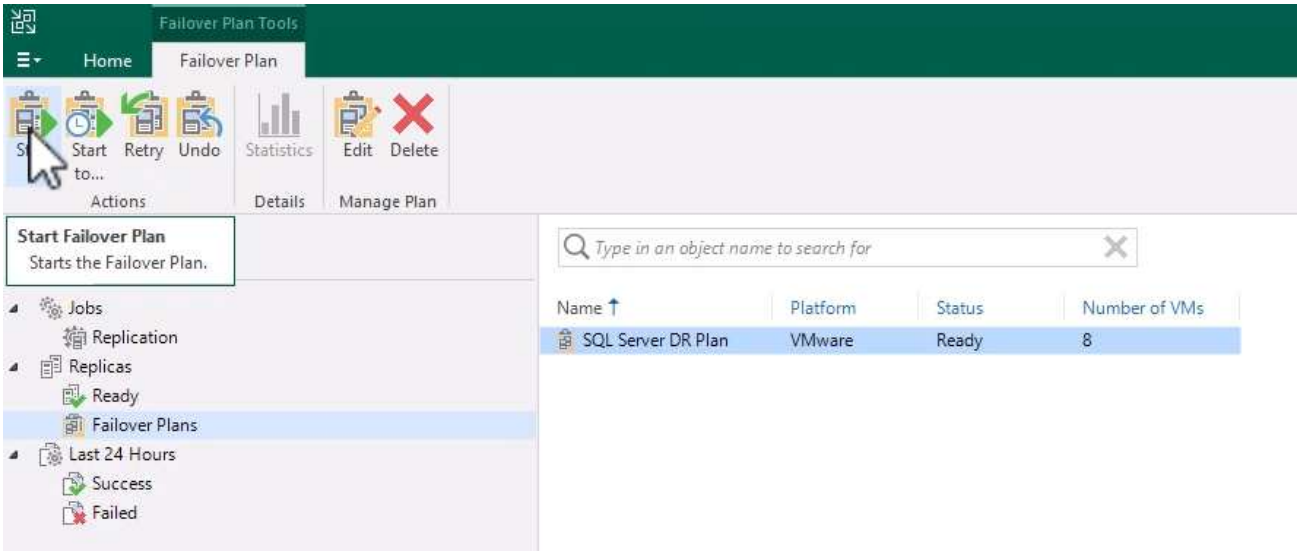
▼ 장애 조치 계획 실행

장애 조치(failover) 중에 프로덕션 사이트의 소스 VM은 재해 복구 사이트의 복제본으로 전환됩니다. 이 프로세스의 일부로 Veeam Backup & Replication은 VM 복제본을 필요한 복원 지점으로 복원하고 소스 VM의 모든 I/O 활동을 복제본으로 전송합니다. 복제품은 실제 재난 상황에서만 활용되는 것이 아니라 재해 복구 훈련을 시뮬레이션하는 데에도 활용됩니다. 장애 조치 시뮬레이션에서는 소스 VM이 계속 실행됩니다. 필요한 테스트가 완료되면 장애 조치를 취소하고 작업을 정상으로 되돌릴 수 있습니다.

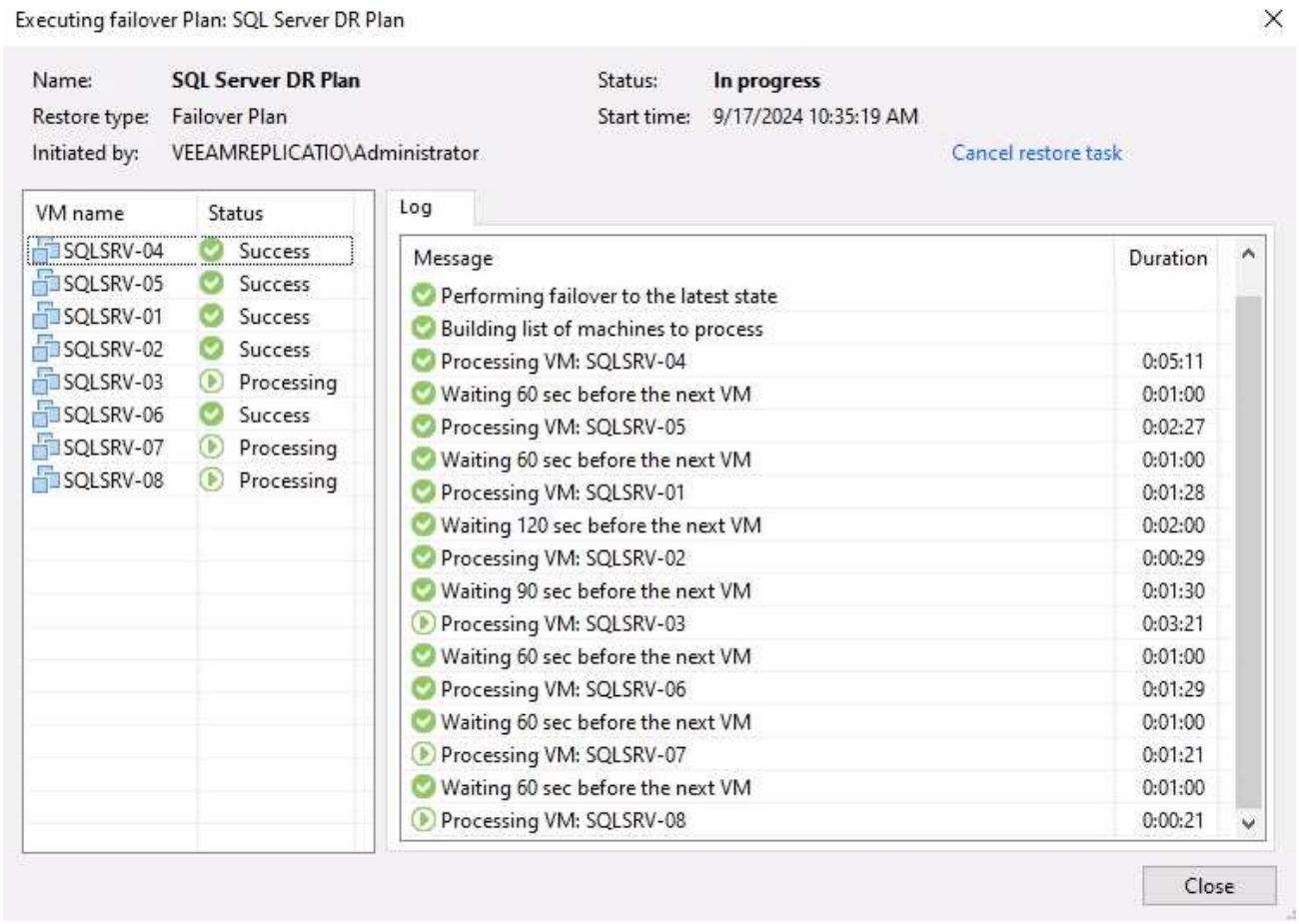
장애 조치 중 IP 충돌을 피하기 위해 네트워크 분할이 제대로 되어 있는지 확인하세요.

장애 조치 계획을 시작하려면 다음 단계를 완료하세요.

1. 시작하려면 홈 보기에서 왼쪽 메뉴의 복제본 > 장애 조치 계획*을 클릭한 다음 *시작 버튼을 클릭합니다. 또는 시작... 버튼을 사용하여 이전 복원 지점으로 장애 조치를 수행할 수 있습니다.



2. 장애 조치 계획 실행 창에서 장애 조치 진행 상황을 모니터링합니다.



Veeam Backup & Replication은 복제본이 준비 상태로 돌아올 때까지 소스 VM에 대한 모든 복제 활동을 중지합니다.

장애 조치 계획에 대한 자세한 내용은 다음을 참조하세요."장애 조치 계획" .

▼ 프로덕션 사이트로의 장애 복구

장애 조치를 수행하는 것은 중간 단계로 간주되며 요구 사항에 따라 마무리되어야 합니다. 옵션은 다음과 같습니다.

- 운영 환경으로의 장애 복구 - 원본 VM으로 되돌리고 복제본의 활성 기간 동안 변경된 모든 내용을 소스 VM과 동기화합니다.

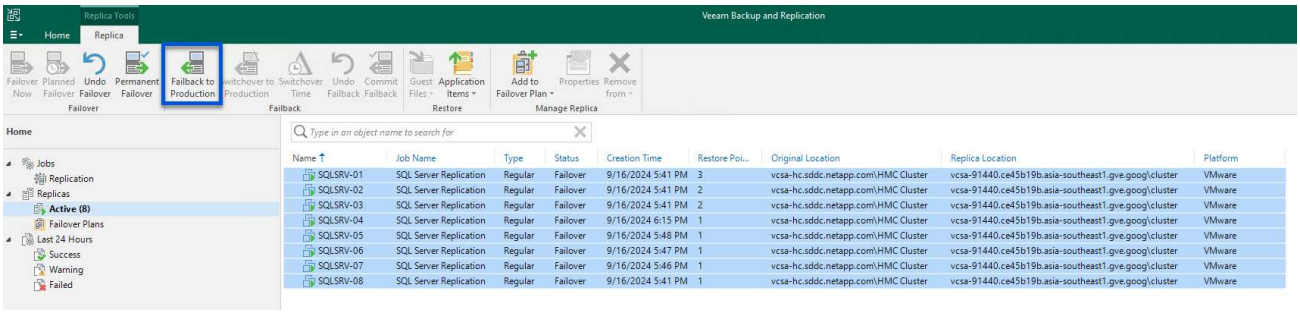
장애 복구 중에 변경 사항은 전송되지만 즉시 적용되지는 않습니다. 원래 VM의 기능이 검증되면 *페일백 커밋*을 선택합니다. 또는 원래 VM에서 예상치 못한 동작이 나타나는 경우 *장애 복구 취소*를 선택하여 VM 복제본으로 되돌립니다.

- 장애 조치 취소 - 운영 기간 동안 VM 복제본에 적용된 모든 변경 사항을 삭제하고 원래 VM으로 되돌립니다.
- 영구 장애 조치 - 원본 VM에서 복제본으로 영구적으로 전환하여 진행 중인 작업을 위한 새로운 기본 VM으로 복제본을 설정합니다.

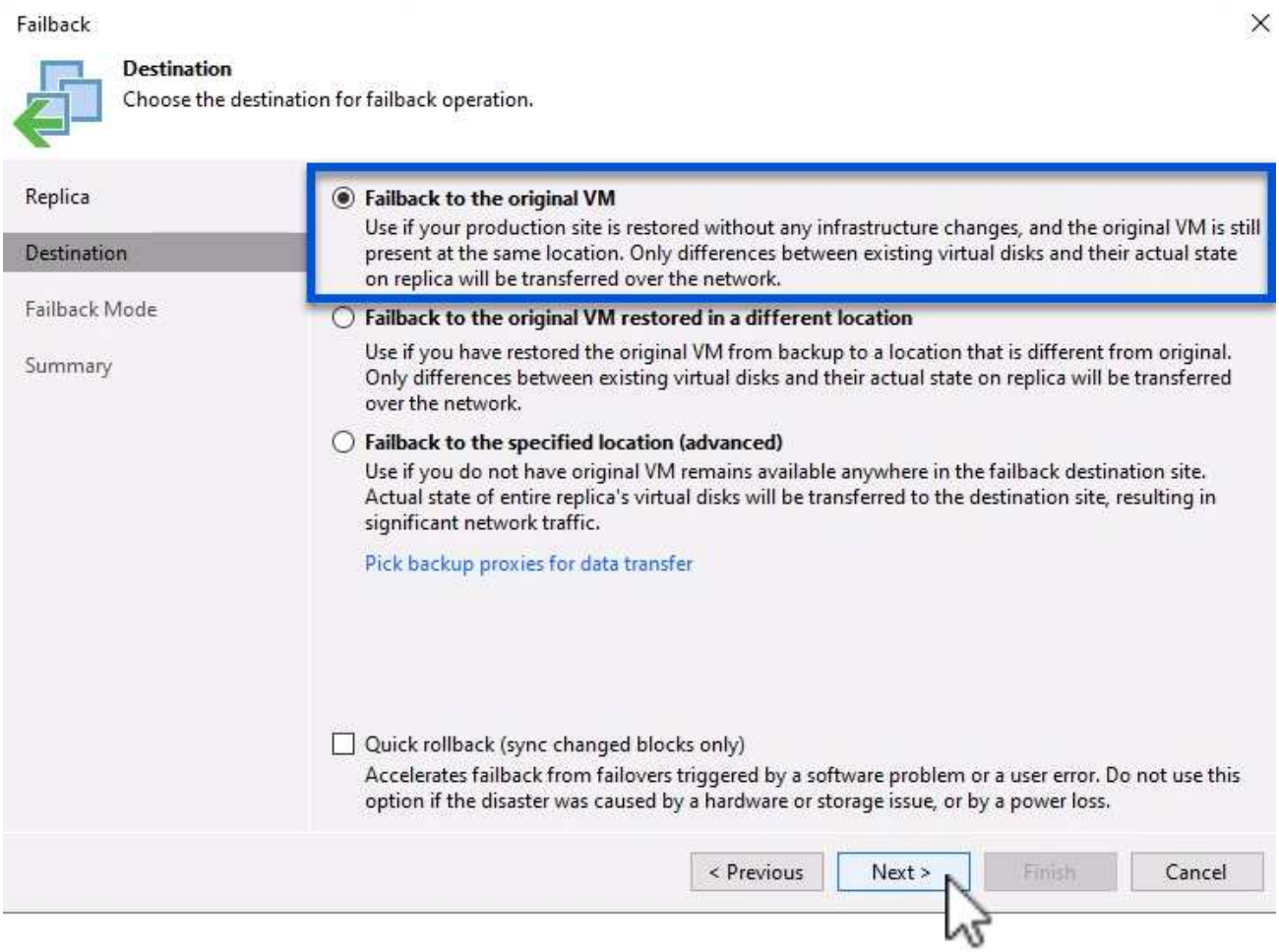
이 시나리오에서는 "프로덕션으로의 장애 복구" 옵션이 선택되었습니다.

프로덕션 사이트로 장애 복구를 수행하려면 다음 단계를 완료하세요.

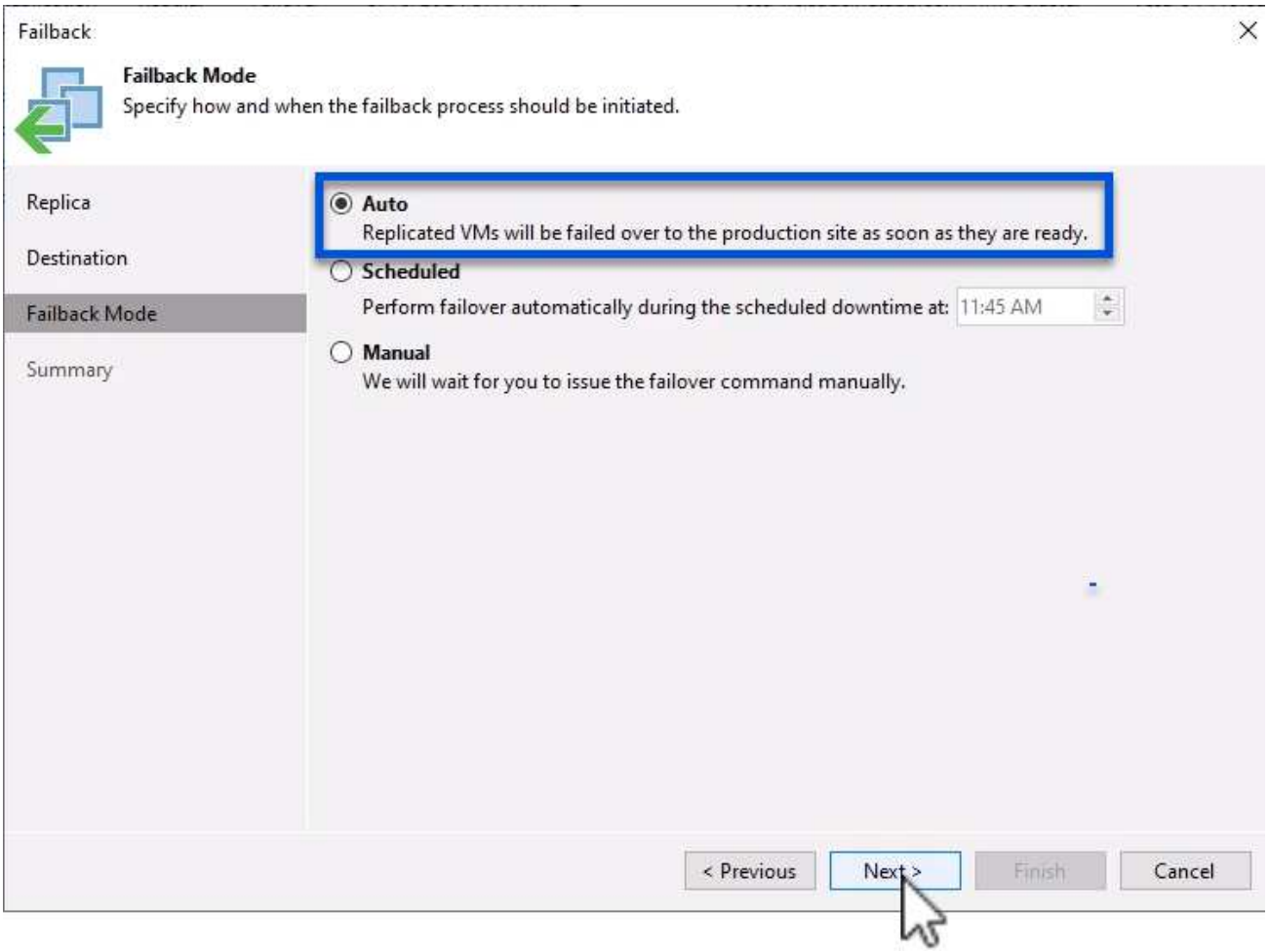
1. 홈 보기에서 왼쪽 메뉴의 복제본 **>** 활성*을 클릭합니다. 포함할 **VM**을 선택하고 상단 메뉴에서 *프로덕션으로 장애 복구 버튼을 클릭합니다.



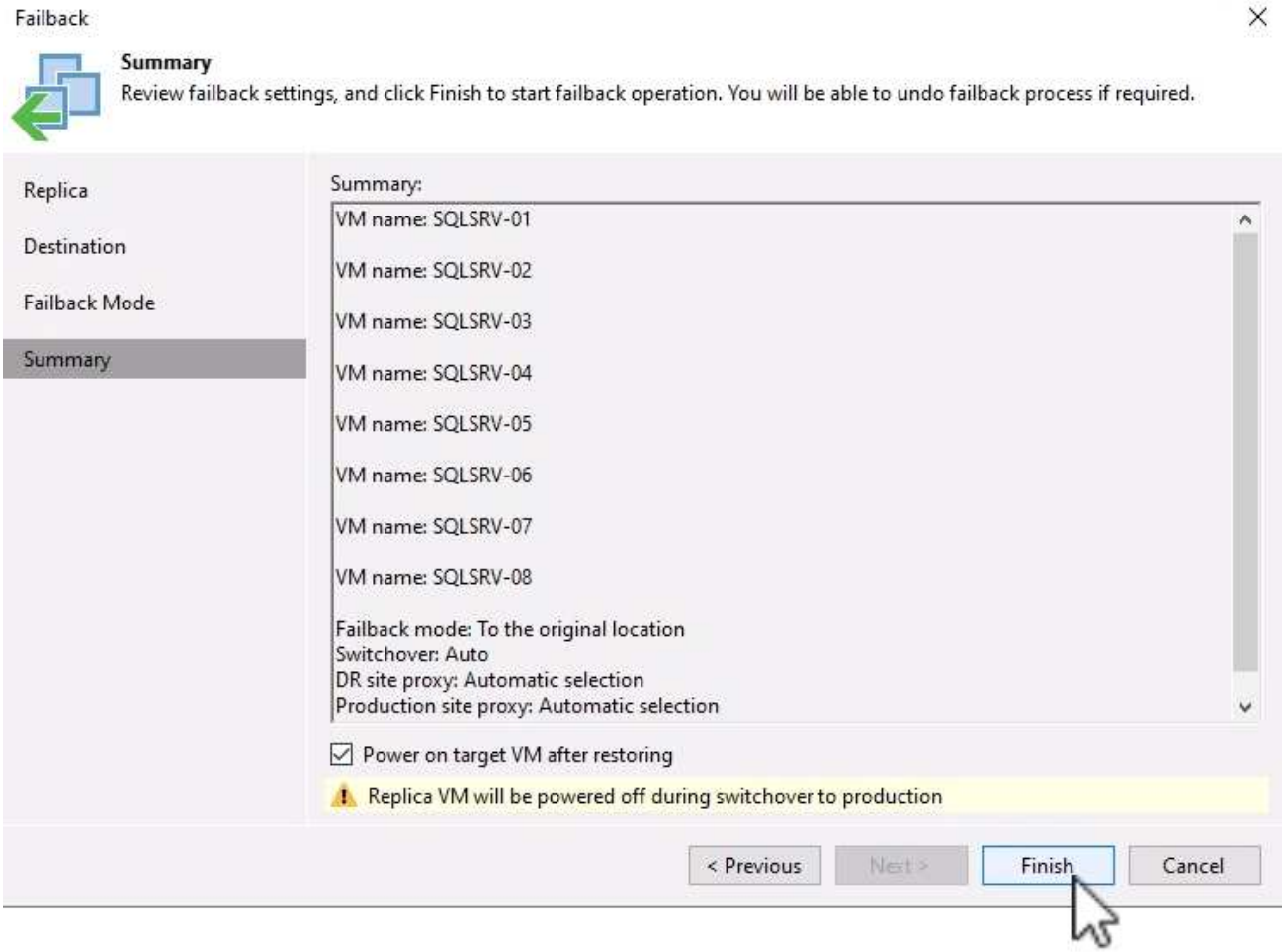
2. 장애 복구 마법사의 복제본 페이지에서 장애 복구 작업에 포함할 복제본을 선택합니다.
3. 대상 페이지에서 *원래 VM으로 장애 복구*를 선택하고 *다음*을 클릭하여 계속합니다.



4. 장애 복구 모드 페이지에서 *자동*을 선택하면 가능한 한 빨리 장애 복구가 시작됩니다.

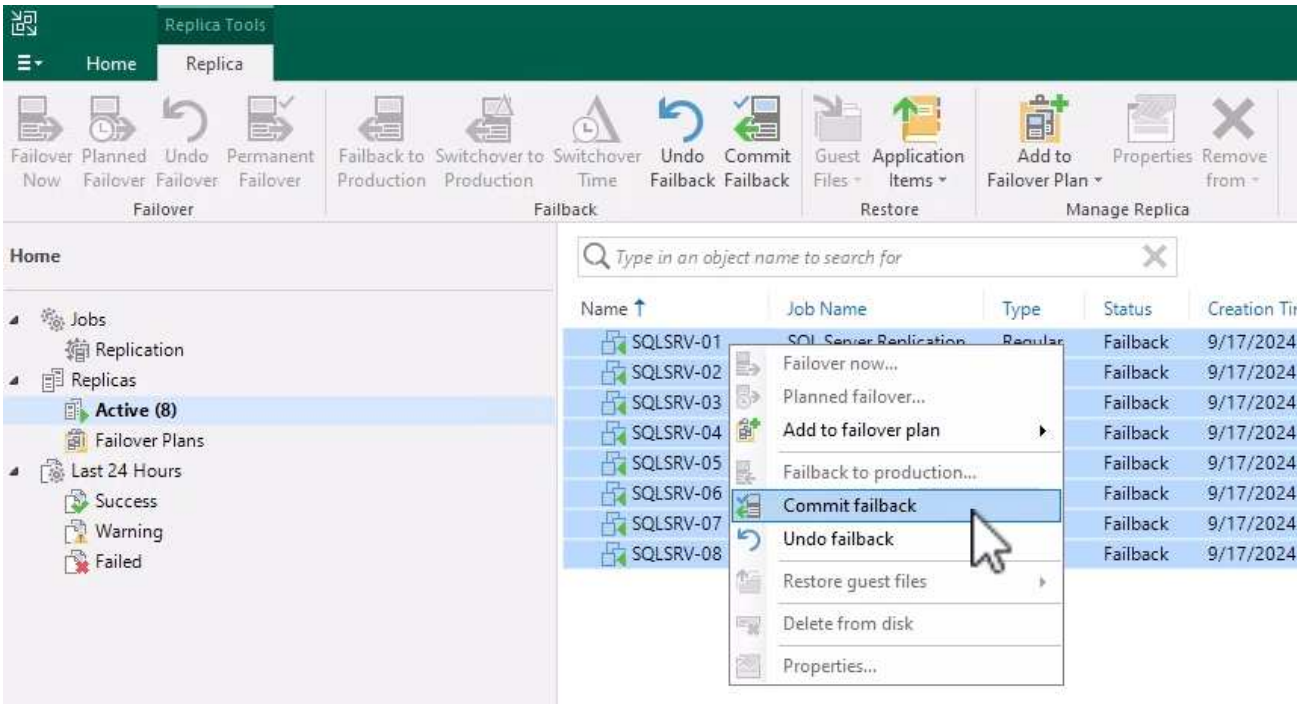


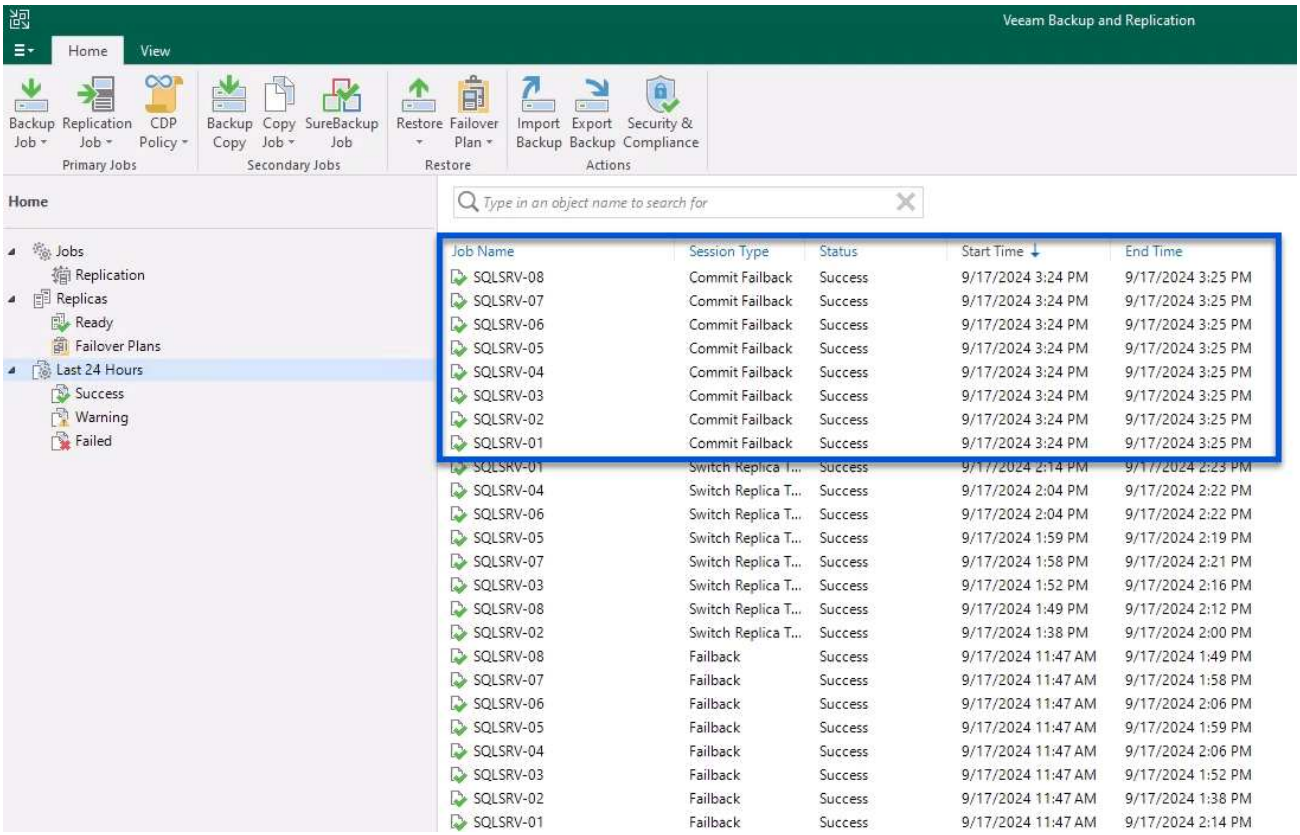
5. 요약 페이지에서 복원 후 대상 **VM** 전원 켜기 여부를 선택한 다음, 마침을 클릭하여 장애 복구 작업을 시작합니다.



장애 복구 커밋은 장애 복구 작업을 마무리하고 프로덕션 VM에 대한 변경 사항의 성공적인 통합을 확인합니다. 커밋 시, Veeam Backup & Replication은 복원된 프로덕션 VM에 대한 정기적인 복제 활동을 재개합니다. 이렇게 하면 복구된 복제본의 상태가 _Failback_에서 _Ready_로 변경됩니다.

1. 장애 복구를 커밋하려면 *복제본 > 활성*으로 이동하여 커밋할 VM을 선택하고 마우스 오른쪽 버튼을 클릭한 다음 *장애 복구 커밋*을 선택합니다.





프로덕션으로의 장애 복구가 성공하면 모든 VM이 원래 프로덕션 사이트로 복원됩니다.

장애 복구 프로세스에 대한 자세한 내용은 Veeam 설명서를 참조하세요."복제를 위한 장애 조치 및 장애 복구" .

결론

Google Cloud NetApp Volumes 데이터 저장소 기능은 Veeam과 다른 검증된 타사 도구를 사용하여 비용 효율적인 재해 복구(DR) 솔루션을 제공할 수 있도록 지원합니다. VM 복제본에 대규모 전용 클러스터 대신 파일럿 라이트 클러스터를 활용하면 조직에서 비용을 크게 줄일 수 있습니다. 이러한 접근 방식을 통해 클라우드 기반 재해 복구를 위한 기존 사내 백업 솔루션을 활용하는 맞춤형 재해 복구 전략이 가능해져 온프레미스 데이터 센터가 추가로 필요 없게 됩니다. 재해 발생 시, 단 한 번의 클릭으로 장애 조치를 시작하거나 자동으로 발생하도록 구성하여 최소한의 가동 중지 시간으로 비즈니스 연속성을 보장할 수 있습니다.

이 과정에 대해 자세히 알아보려면 자세한 안내 영상을 시청하세요.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=b2fb8597-c3fe-49e2-8a84-b1f10118db6d

GCP/GCVE에서 워크로드 마이그레이션

VMware HCX를 사용하여 Google Cloud NetApp Volumes 데이터 저장소로 워크로드 마이그레이션 - 빠른 시작 가이드

Google Cloud VMware Engine 및 Cloud Volume Service 데이터 저장소의 가장 일반적인 사용 사례 중 하나는 VMware 워크로드의 마이그레이션입니다. VMware HCX는 선호되는 옵션으로, 온프레미스 가상 머신(VM)과 해당 데이터를 Cloud Volume Service NFS 데이터 저장소로 옮기는 다양한 마이그레이션 메커니즘을 제공합니다.

개요: VMware HCX, Google Cloud NetApp Volumes 데이터 저장소 및 Google Cloud VMware Engine(GCVE)을 사용하여 가상 머신 마이그레이션

VMware HCX는 기본적으로 애플리케이션 마이그레이션, 워크로드 리밸런싱, 심지어 클라우드 전반의 비즈니스 연속성을 단순화하도록 설계된 마이그레이션 플랫폼입니다. Google Cloud VMware Engine Private Cloud의 일부로 포함되어 있으며, 워크로드를 마이그레이션하는 다양한 방법을 제공하며 재해 복구(DR) 작업에 사용할 수 있습니다.

이 문서에서는 Cloud Volume Service 데이터스토어를 프로비저닝하고, 온프레미스와 Google Cloud VMware Engine 측의 모든 주요 구성 요소를 포함하여 VMware HCX를 다운로드, 배포, 구성하는 방법에 대한 단계별 지침을 제공합니다. 여기에는 다양한 VM 마이그레이션 메커니즘을 활성화하기 위한 Interconnect, 네트워크 확장, WAN 최적화가 포함됩니다.

> VMware HCX는 마이그레이션이 VM 수준에서 진행되므로 모든 데이터 저장소 유형과 호환됩니다. 따라서 이 문서는 기존 NetApp 고객과 비용 효율적인 VMware 클라우드 구축을 위해 Google Cloud VMware Engine과 함께 Cloud Volume Service를 배포할 계획인 비 NetApp 고객에게 적용됩니다.

▼ 상위 수준 단계

이 목록은 온프레미스의 HCX Connector에서 Google Cloud VMware Engine 측의 HCX Cloud Manager로 VM을 페어링하고 마이그레이션하는 데 필요한 상위 수준의 단계를 제공합니다.

1. Google VMware Engine 포털을 통해 HCX를 준비합니다.
2. 온프레미스 VMware vCenter Server에 HCX Connector Open Virtualization Appliance(OVA) 설치 프로그램을 다운로드하여 배포합니다.
3. 라이선스 키로 HCX를 활성화하세요.
4. 온프레미스 VMware HCX Connector를 Google Cloud VMware Engine HCX Cloud Manager와 페어링합니다.
5. 네트워크 프로필, 컴퓨팅 프로필 및 서비스 메시를 구성합니다.

6. (선택 사항) 마이그레이션 중에 재IP를 방지하기 위해 네트워크 확장을 수행합니다.
7. 기기 상태를 검증하고 마이그레이션이 가능한지 확인하세요.
8. VM 워크로드를 마이그레이션합니다.

▼ 필수 조건

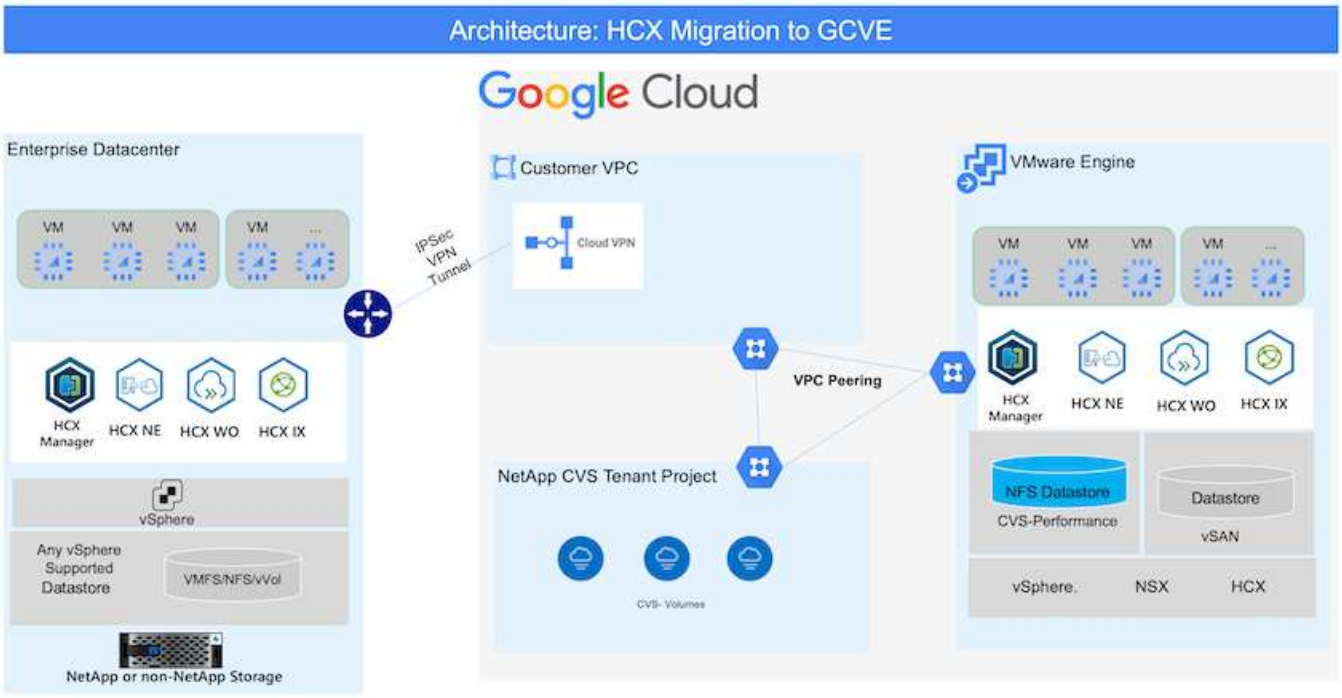
시작하기 전에 다음 전제 조건이 충족되었는지 확인하세요. 자세한 내용은 다음을 참조하세요. "링크" . 연결성을 포함한 필수 구성 요소를 갖추면 Google Cloud VMware Engine 포털에서 HCX 라이선스 키를 다운로드합니다. OVA 설치 프로그램을 다운로드한 후 아래 설명된 대로 설치 과정을 진행하세요.

> HCX Advanced가 기본 옵션이며, VMware HCX Enterprise Edition도 지원 티켓을 통해 이용 가능하며 추가 비용 없이 지원됩니다. 나타내다 "이 링크"

- 기존 Google Cloud VMware Engine 소프트웨어 정의 데이터 센터(SDDC)를 사용하거나 이를 사용하여 프라이빗 클라우드를 만드십시오."NetApp 링크" 아니면 이것 "구글 링크" .
- 온프레미스 VMware vSphere 지원 데이터 센터에서 VM 및 관련 데이터를 마이그레이션하려면 데이터 센터에서 SDDC 환경으로의 네트워크 연결이 필요합니다. 워크로드를 마이그레이션하기 전에 "클라우드 VPN 또는 클라우드 상호 연결 설정" 온프레미스 환경과 해당 프라이빗 클라우드 간.
- 온프레미스 VMware vCenter Server 환경에서 Google Cloud VMware Engine 프라이빗 클라우드로의 네트워크 경로는 vMotion을 사용하여 VM 마이그레이션을 지원해야 합니다.
- 필수 사항을 확인하세요 "방화벽 규칙 및 포트" 온프레미스 vCenter Server와 SDDC vCenter 간의 vMotion 트래픽이 허용됩니다.
- Cloud Volume Service NFS 볼륨은 Google Cloud VMware Engine의 데이터 저장소로 마운트되어야 합니다. 여기에 자세히 설명된 단계를 따르세요. "링크" Cloud Volume Service 데이터스토어를 Google Cloud VMware Engines 호스트에 연결합니다.

▼ 고수준 아키텍처

테스트 목적으로, 이 검증에 사용된 온프레미스 랩 환경은 Cloud VPN을 통해 연결되었으며, 이를 통해 온프레미스에서 Google Cloud VPC로 연결할 수 있습니다.



Google에서 VMware HCX를 사용하는 것에 대한 자세한 내용은 다음을 참조하세요. "VMware 링크"

솔루션 배포

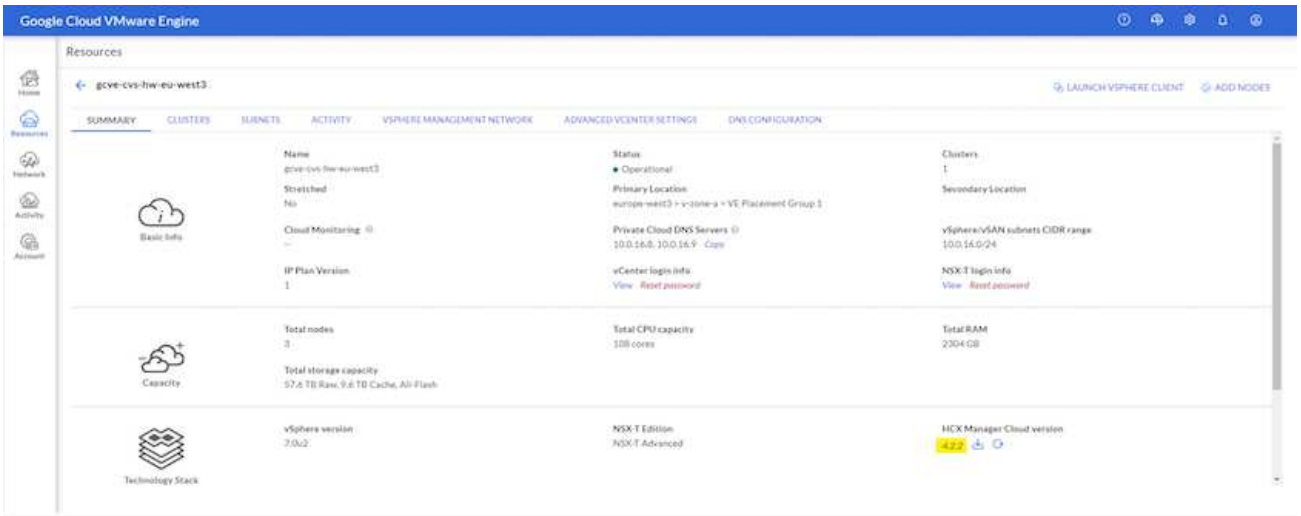
이 솔루션의 배포를 완료하려면 다음 단계를 따르세요.

▼ 1단계: **Google VMware Engine Portal**을 통해 **HCX** 준비

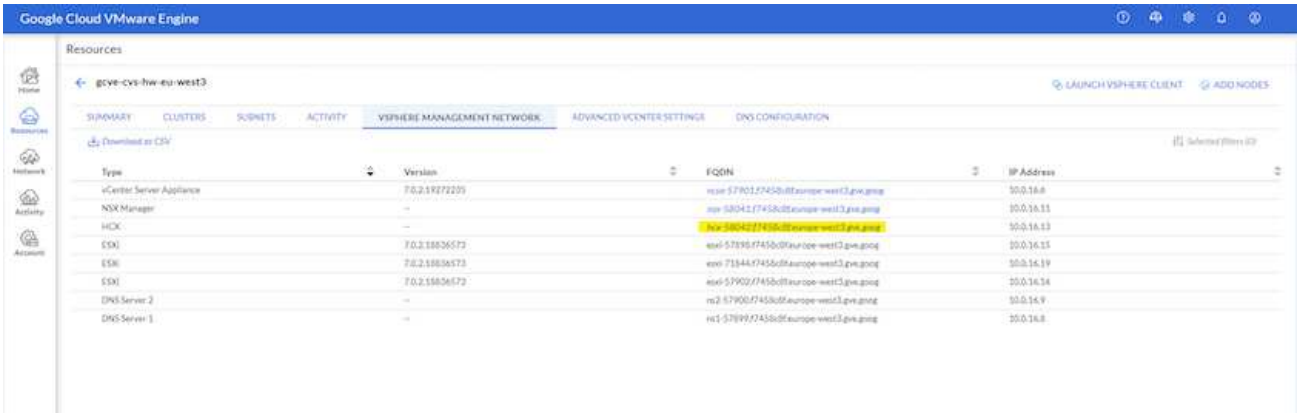
HCX Cloud Manager 구성 요소는 VMware Engine으로 프라이빗 클라우드를 프로비저닝할 때 자동으로 설치됩니다. 사이트 페어링을 준비하려면 다음 단계를 완료하세요.

1. Google VMware Engine Portal에 로그인하고 HCX Cloud Manager에 로그인합니다.

   HCX 버전 링크를 클릭하여 HCX 콘솔에 로그인할 수 있습니다
   .

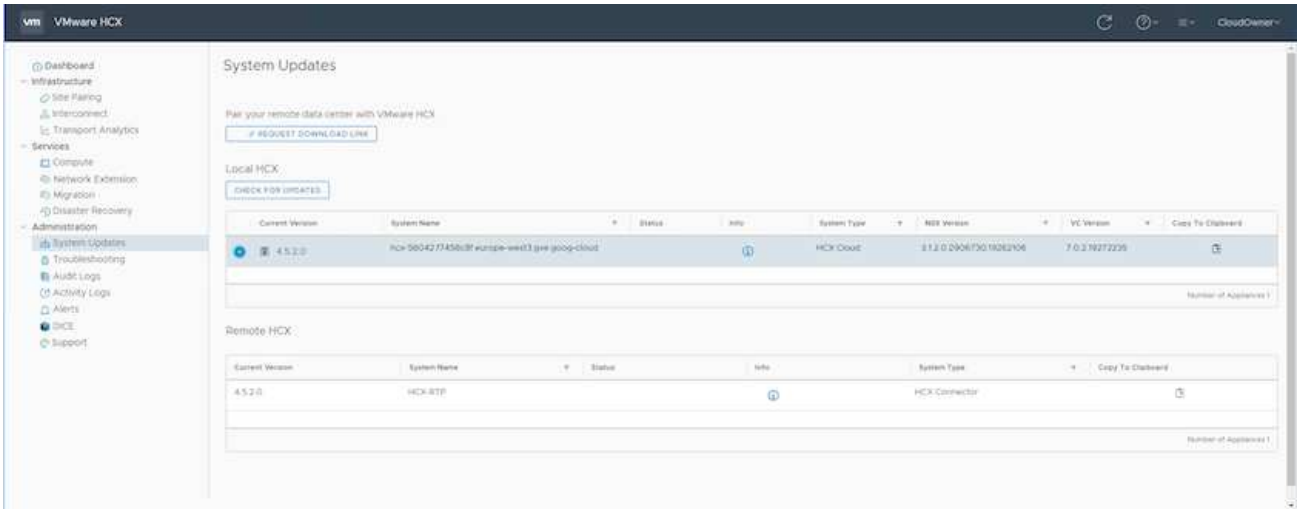


   또는 vSphere 관리 네트워크 탭에서 HCX FQDN을 클릭합니다
   .



2. HCX Cloud Manager에서 *관리 > 시스템 업데이트*로 이동합니다.
3. *다운로드 링크 요청*을 클릭하여 OVA 파일을 다운로드하세요

.



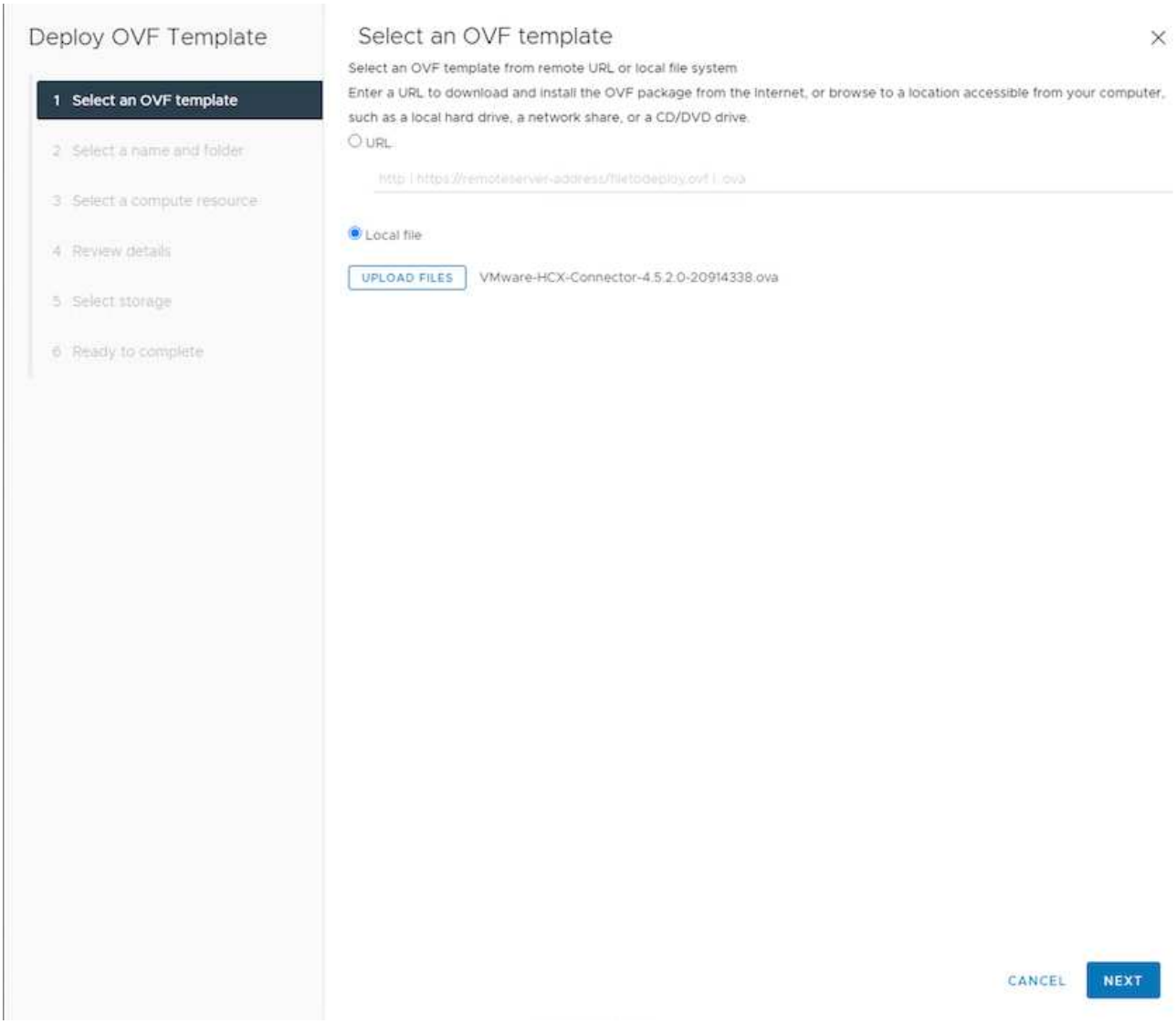
4. HCX Cloud Manager UI에서 사용 가능한 최신 버전으로 HCX Cloud Manager를 업데이트하세요.

▼ **2**단계**:** 온프레미스 **vCenter Server**에 설치 프로그램 **OVA** 배포

온프레미스 커넥터가 Google Cloud VMware Engine의 HCX Manager에 연결하려면 온프레미스 환경에서 적절한 방화벽 포트가 열려 있는지 확인하세요.

온프레미스 vCenter Server에 HCX 커넥터를 다운로드하고 설치하려면 다음 단계를 완료하세요.

1. 이전 단계에서 설명한 대로 Google Cloud VMware Engine의 HCX 콘솔에서 OVA를 다운로드합니다.
2. OVA를 다운로드한 후 **OVF** 템플릿 배포 옵션을 사용하여 온프레미스 VMware vSphere 환경에 배포합니다.



3. OVA 배포에 필요한 모든 정보를 입력하고, *다음*을 클릭한 다음, *마침*을 클릭하여 VMware HCX 커넥터 OVA를 배포합니다.

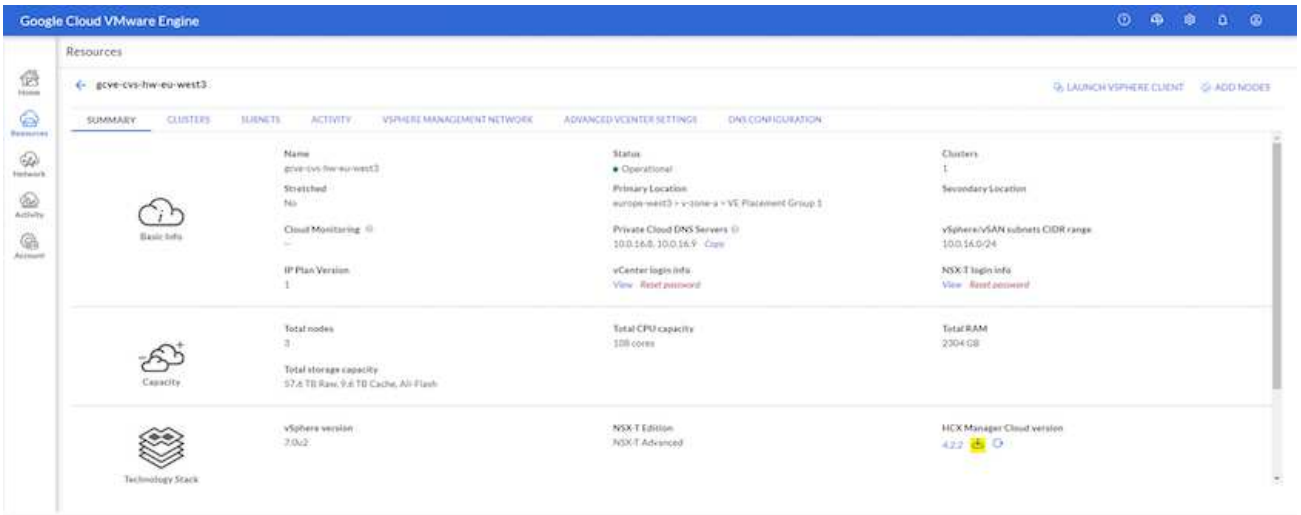
   가상 어플라이언스의 전원을 수동으로 켭니다.

단계별 지침은 다음을 참조하세요. "Google HCX 문서" .

▼ **3**단계**:** 라이선스 키로 **HCX** 커넥터 활성화

온프레미스에 VMware HCX Connector OVA를 배포하고 어플라이언스를 시작한 후 다음 단계를 완료하여 HCX Connector를 활성화합니다. Google Cloud VMware Engine 포털에서 라이선스 키를 생성하고 VMware HCX Manager에서 활성화합니다.

1. VMware Engine 포털에서 리소스를 클릭하고, 프라이빗 클라우드를 선택한 다음, **HCX Manager Cloud** 버전 아래에 있는 다운로드 아이콘을 클릭합니다.



다운로드한 파일을 열고 라이센스 키 문자열을 복사합니다.

2. 온프레미스 VMware HCX Manager에 로그인하세요. "`https://hcxmanagerIP:9443`" 관리자 자격 증명을 사용합니다.

   OVA 배포 중에 정의된 hcxmanagerIP와 비밀번호를 사용합니다.

3. 라이센스에서 3단계에서 복사한 키를 입력하고 *활성화*를 클릭합니다.

   온프레미스 HCX 커넥터는 인터넷에 접속할 수 있어야 합니다.

4. *데이터 센터 위치*에서 온프레미스에서 VMware HCX Manager를 설치할 수 있는 가장 가까운 위치를 제공합니다. *계속*을 클릭하세요.
5. *시스템 이름*에서 이름을 업데이트하고 *계속*을 클릭합니다.
6. *예, 계속*을 클릭합니다.
7. *vCenter 연결*에서 vCenter Server의 정규화된 도메인 이름(FQDN) 또는 IP 주소와 해당 자격 증명을 제공하고 *계속*을 클릭합니다.

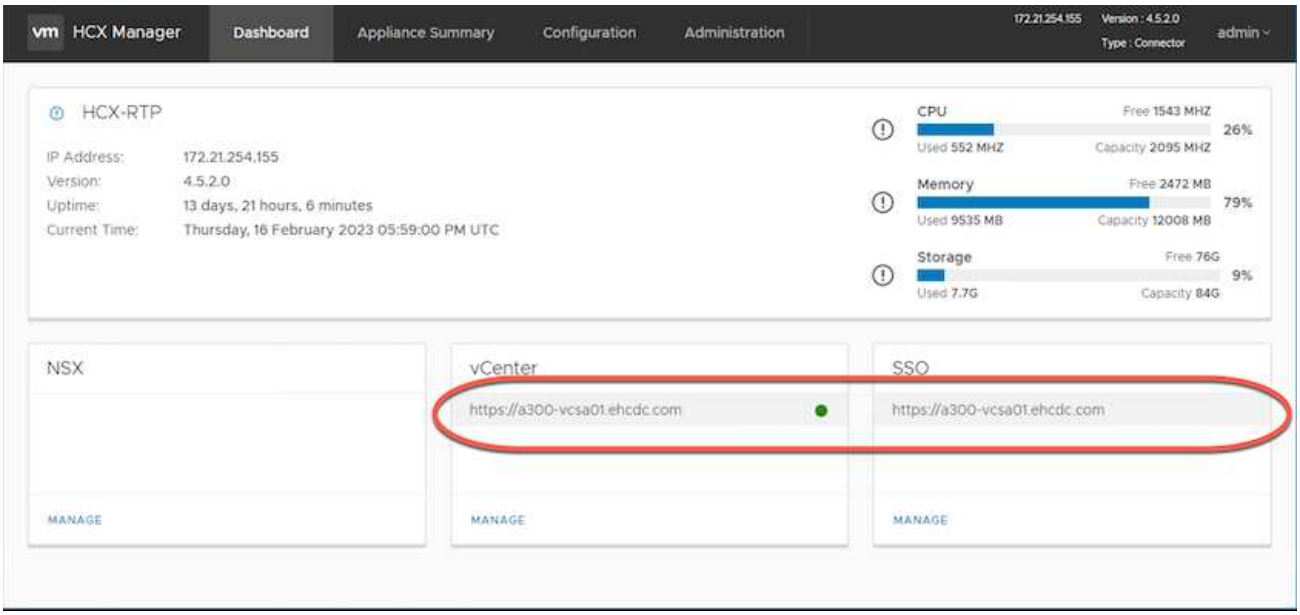
   나중에 연결 문제를 방지하려면 FQDN을 사용하세요.

8. *SSO/PSC 구성*에서 Platform Services Controller(PSC)의 FQDN 또는 IP 주소를 입력하고 *계속*을 클릭합니다.

   내장형 PSC의 경우 VMware vCenter Server FQDN 또는 IP 주소를 입력하세요.

9. 입력한 정보가 정확한지 확인하고 *다시 시작*을 클릭하세요.
10. 서비스가 다시 시작된 후 나타나는 페이지에서 vCenter Server가 녹색으로 표시됩니다. vCenter Server와 SSO 모두 적절한 구성 매개변수를 가져야 하며, 이는 이전 페이지와 동일해야 합니다.

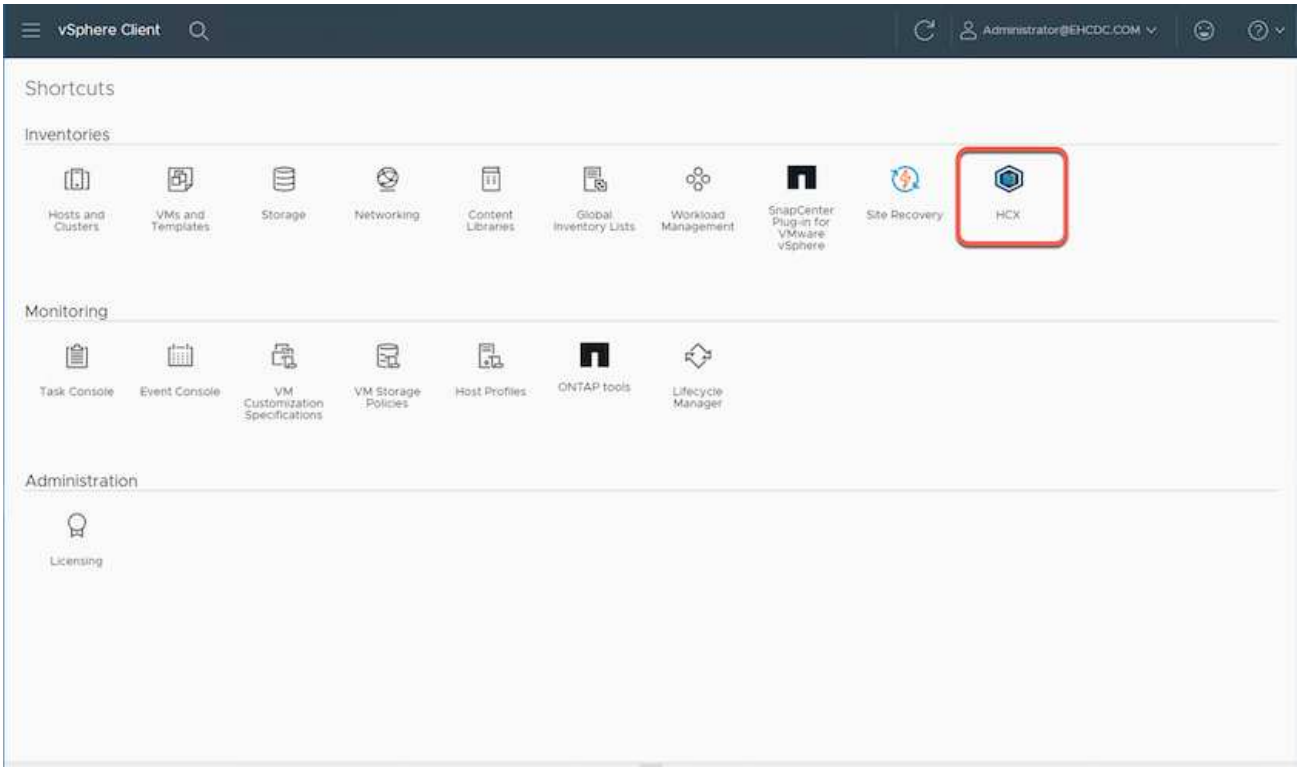
    이 프로세스는 약 10~20분 정도 걸리며 플러그인이 vCenter Server에 추가됩니다.



▼ **4**단계: 온프레미스 **VMware HCX** 커넥터를 **Google Cloud VMware Engine HCX Cloud Manager**와 페어링

HCX 커넥터가 온프레미스 vCenter에 배포되고 구성된 후 페어링을 추가하여 Cloud Manager에 대한 연결을 설정합니다. 사이트 페어링을 구성하려면 다음 단계를 완료하세요.

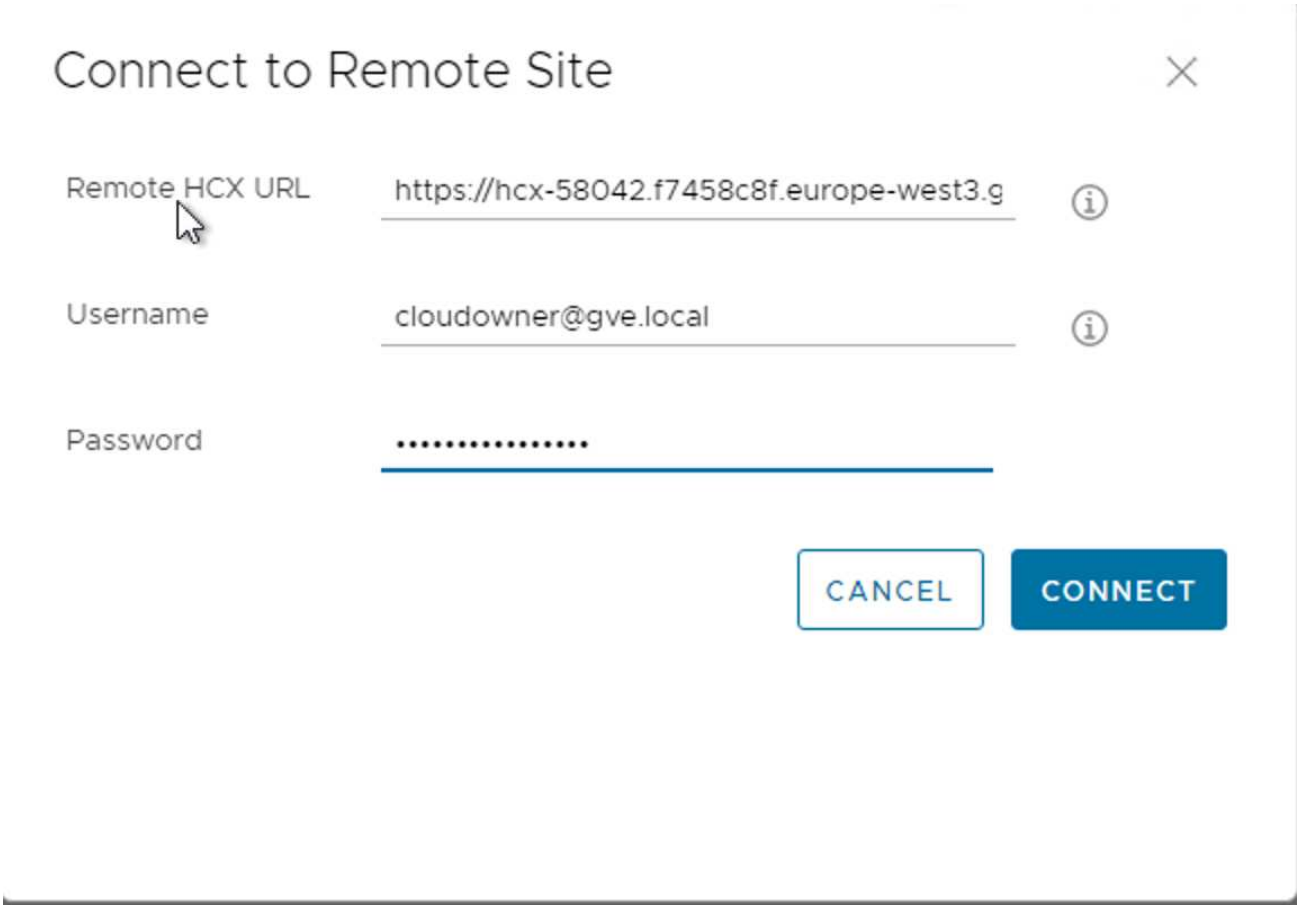
1. 온프레미스 vCenter 환경과 Google Cloud VMware Engine SDDC 간에 사이트 쌍을 생성하려면 온프레미스 vCenter Server에 로그인하고 새로운 HCX vSphere Web Client 플러그인에 액세스합니다.



2. 인프라에서 *사이트 페어링 추가*를 클릭합니다.

Google Cloud VMware Engine HCX Cloud Manager URL 또는 IP 주소와 프라이빗 클라우드에 액세스하기 위한 클라우드 소유자 역할 권한이 있는 사용자의 자격 증명을

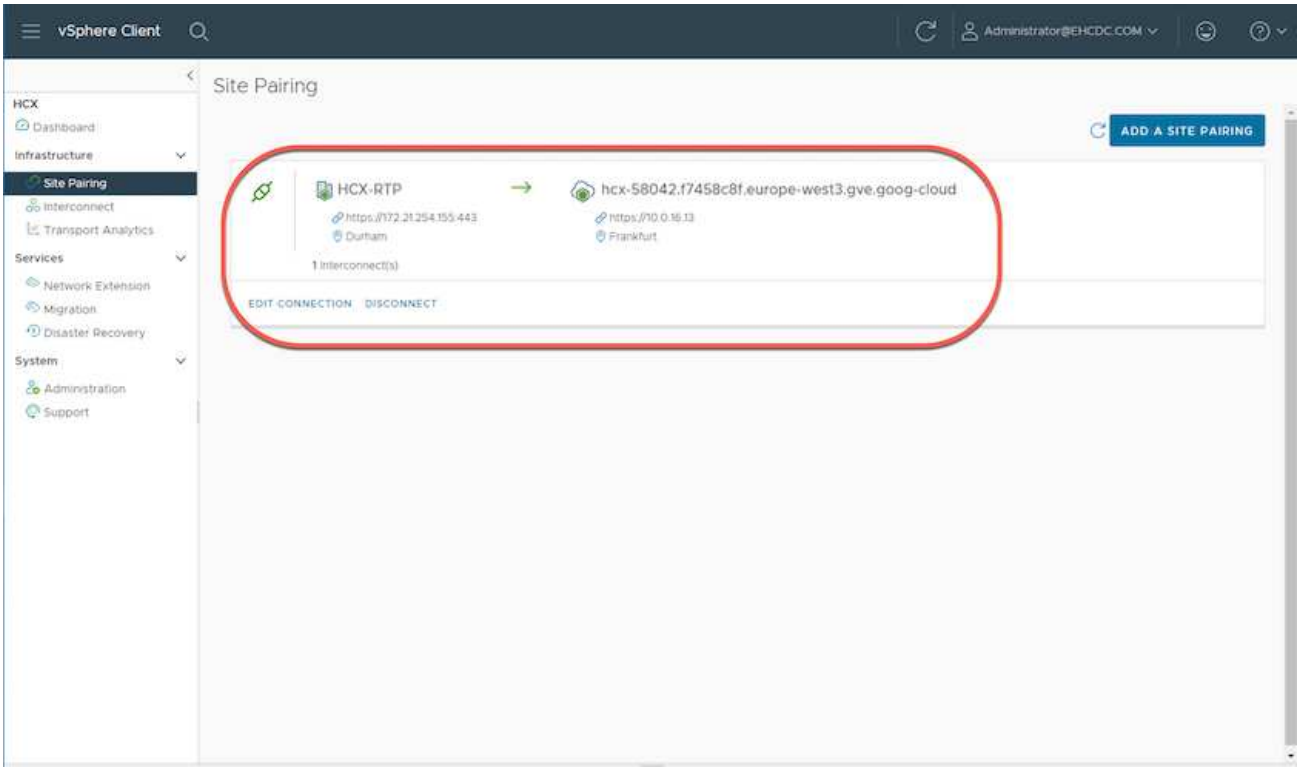
입력합니다.



3. *연결*을 클릭하세요.

VMware HCX Connector는 포트 443을 통해 HCX Cloud Manager IP로 라우팅할 수 있어야 합니다.

4. 페어링이 생성되면 새로 구성된 사이트 페어링을 HCX 대시보드에서 사용할 수 있습니다.

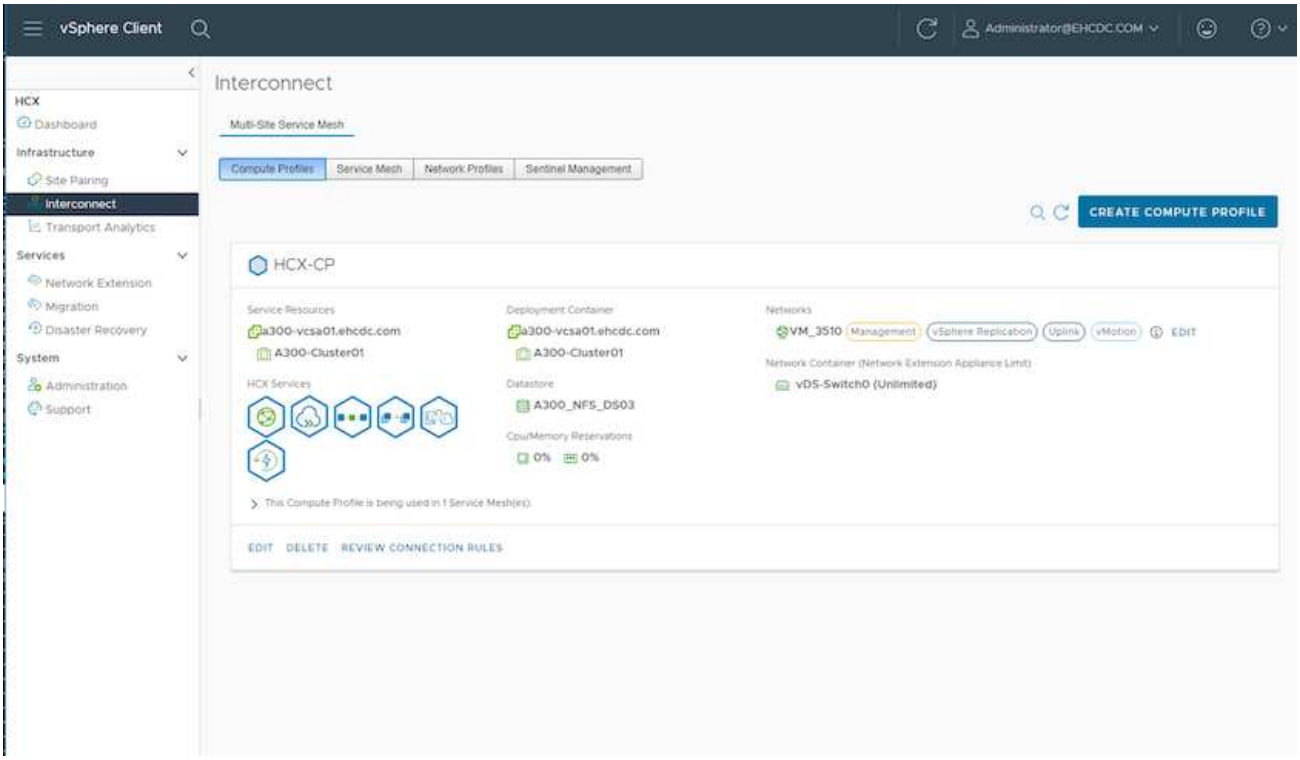


▼ **5**단계**:** 네트워크 프로필**,** 컴퓨팅 프로필 및 서비스 메시 구성

VMware HCX Interconnect 서비스 어플라이언스는 인터넷과 대상 사이트에 대한 개인 연결을 통해 복제 및 vMotion 기반 마이그레이션 기능을 제공합니다. 상호 연결은 암호화, 트래픽 엔지니어링, VM 이동성을 제공합니다. Interconnect 서비스 어플라이언스를 생성하려면 다음 단계를 완료하세요.

1. 인프라에서 *상호 연결 > 다중 사이트 서비스 메시 > 컴퓨팅 프로필 > 컴퓨팅 프로필 만들기*를 선택합니다.

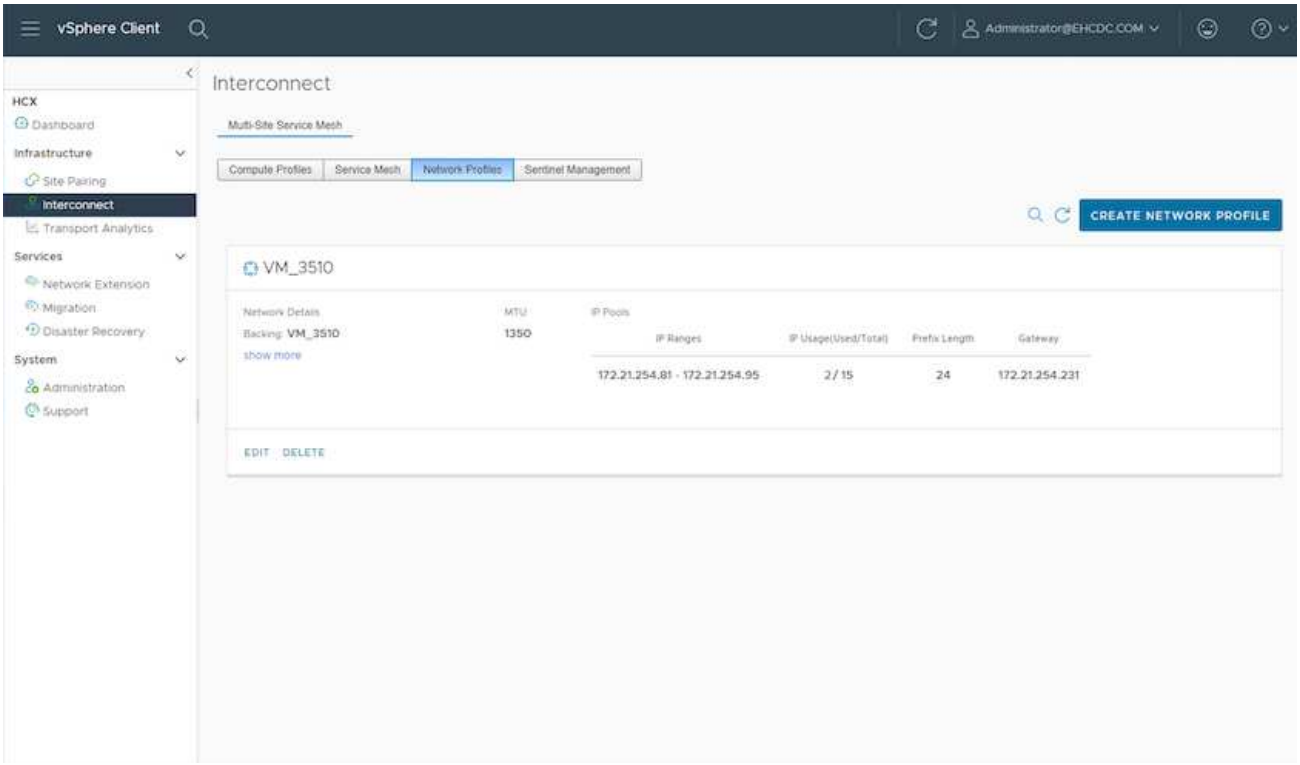
ⓘ 컴퓨팅 프로필은 배포되는 어플라이언스와 HCX 서비스가 액세스할 수 있는 VMware 데이터 센터 부분을 포함한 배포 매개변수를 정의합니다.



2. 컴퓨팅 프로필을 만든 후 *멀티 사이트 서비스 메시 > 네트워크 프로필 > 네트워크 프로필 만들기*를 선택하여 네트워크 프로필을 만듭니다.

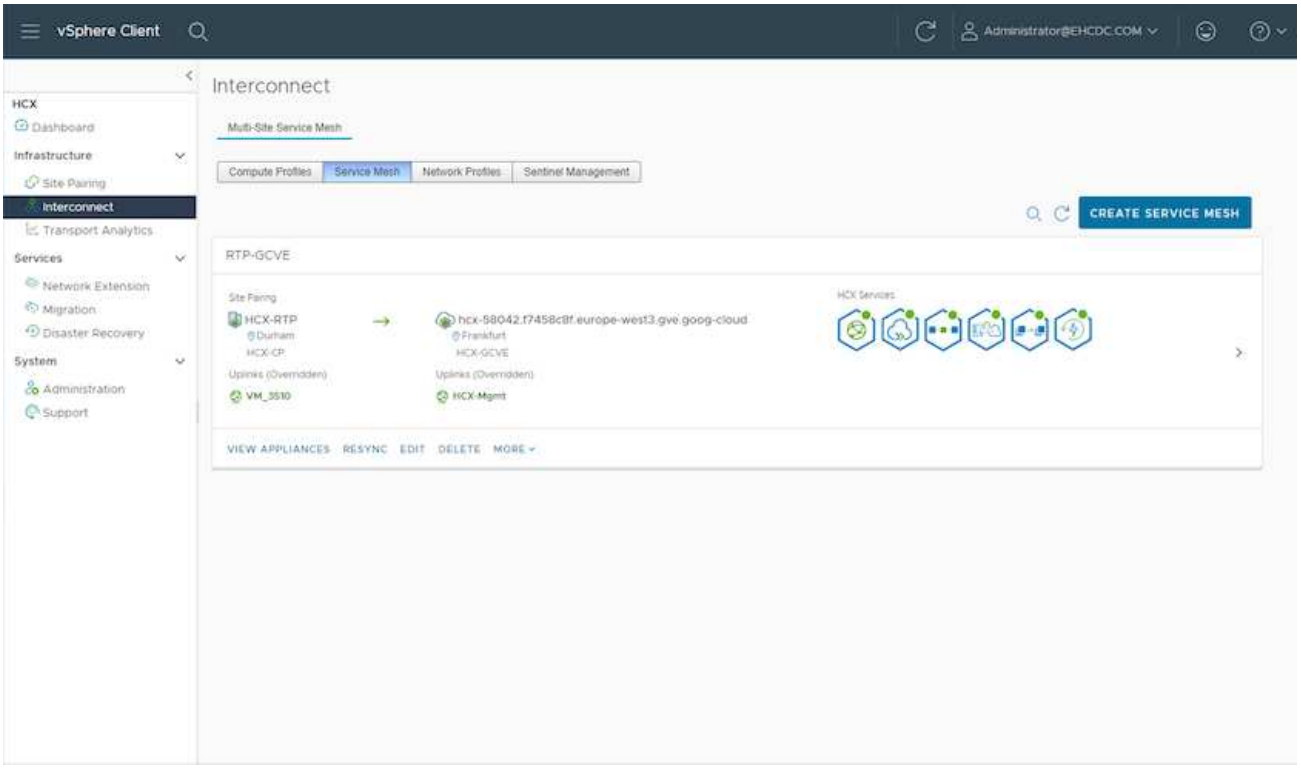
   네트워크 프로필은 HCX가 가상 어플라이언스에 사용하는 IP 주소와 네트워크 범위를 정의합니다.

   이 단계에는 두 개 이상의 IP 주소가 필요합니다. 이러한 IP 주소는 관리 네트워크에서 Interconnect Appliance에 할당됩니다.

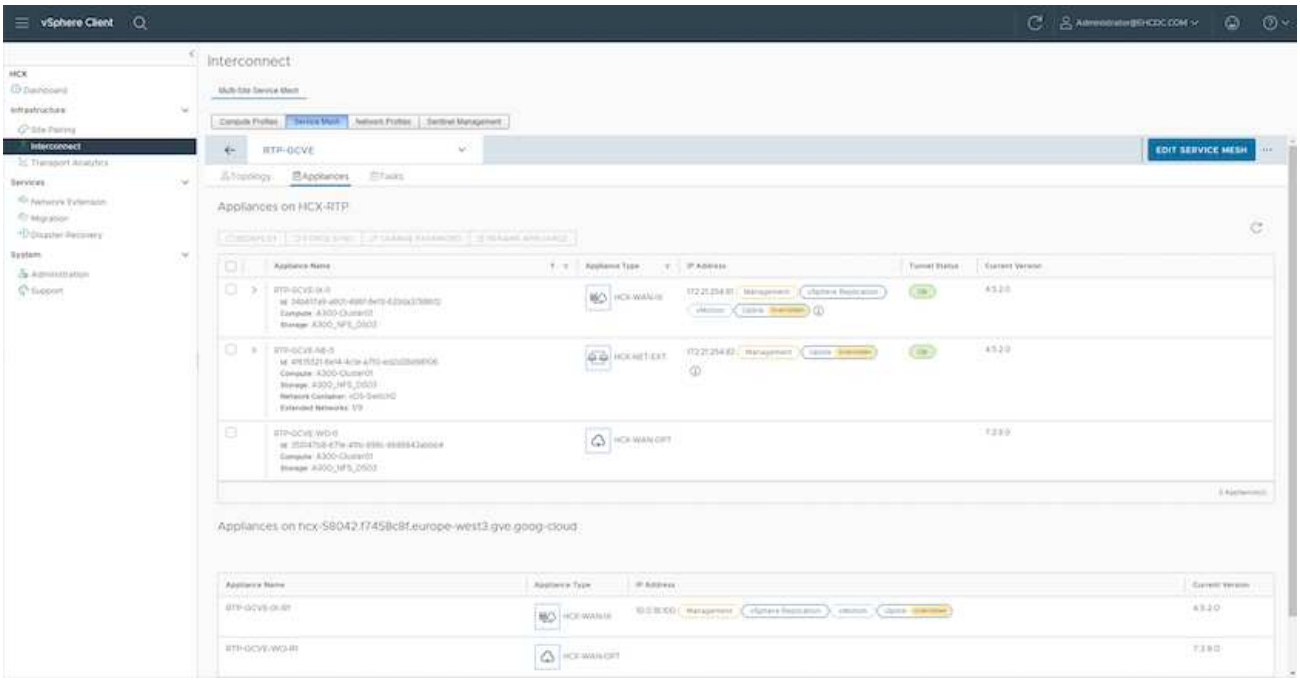


3. 이제 컴퓨팅 및 네트워크 프로필이 성공적으로 생성되었습니다.
4. 상호 연결 옵션 내에서 서비스 메시 탭을 선택하여 서비스 메시를 만들고 온-프레미스 및 GCVE SDDC 사이트를 선택합니다.
5. 서비스 메시는 로컬 및 원격 컴퓨팅과 네트워크 프로필 쌍을 지정합니다.

> 이 프로세스의 일환으로 HCX 어플라이언스는 소스 사이트와 대상 사이트 모두에 배포되고 자동으로 구성되어 안전한 전송 패브릭을 생성합니다.



6. 이것은 구성의 마지막 단계입니다. 배포를 완료하는 데 약 30분이 소요됩니다. 서비스 메시가 구성되면 워크로드 VM을 마이그레이션하기 위한 IPsec 터널이 성공적으로 생성되어 환경이 준비됩니다.



▼ **6**단계**:** 워크로드 마이그레이션

다양한 VMware HCX 마이그레이션 기술을 사용하여 온프레미스와 GCVE SDDC 간에 워크로드를 양방향으로 마이그레이션할 수 있습니다. HCX 대량 마이그레이션, HCX vMotion, HCX 콜드 마이그레이션, HCX 복제 지원 vMotion(HCX Enterprise 에디션에서 사용 가능), HCX OS 지원 마이그레이션(HCX Enterprise 에디션에서 사용 가능) 등 다양한 마이그레이션 기술을 사용하여 VMware HCX 활성화 엔터티 간에 VM을 이동할 수 있습니다.

다양한 HCX 마이그레이션 메커니즘에 대해 자세히 알아보려면 다음을 참조하세요. "VMware HCX 설명서를 사용하여 VMware VM 마이그레이션" .

HCX-IX 어플라이언스는 Mobility Agent 서비스를 사용하여 vMotion, Cold 및 Replication Assisted vMotion(RAV) 마이그레이션을 수행합니다.

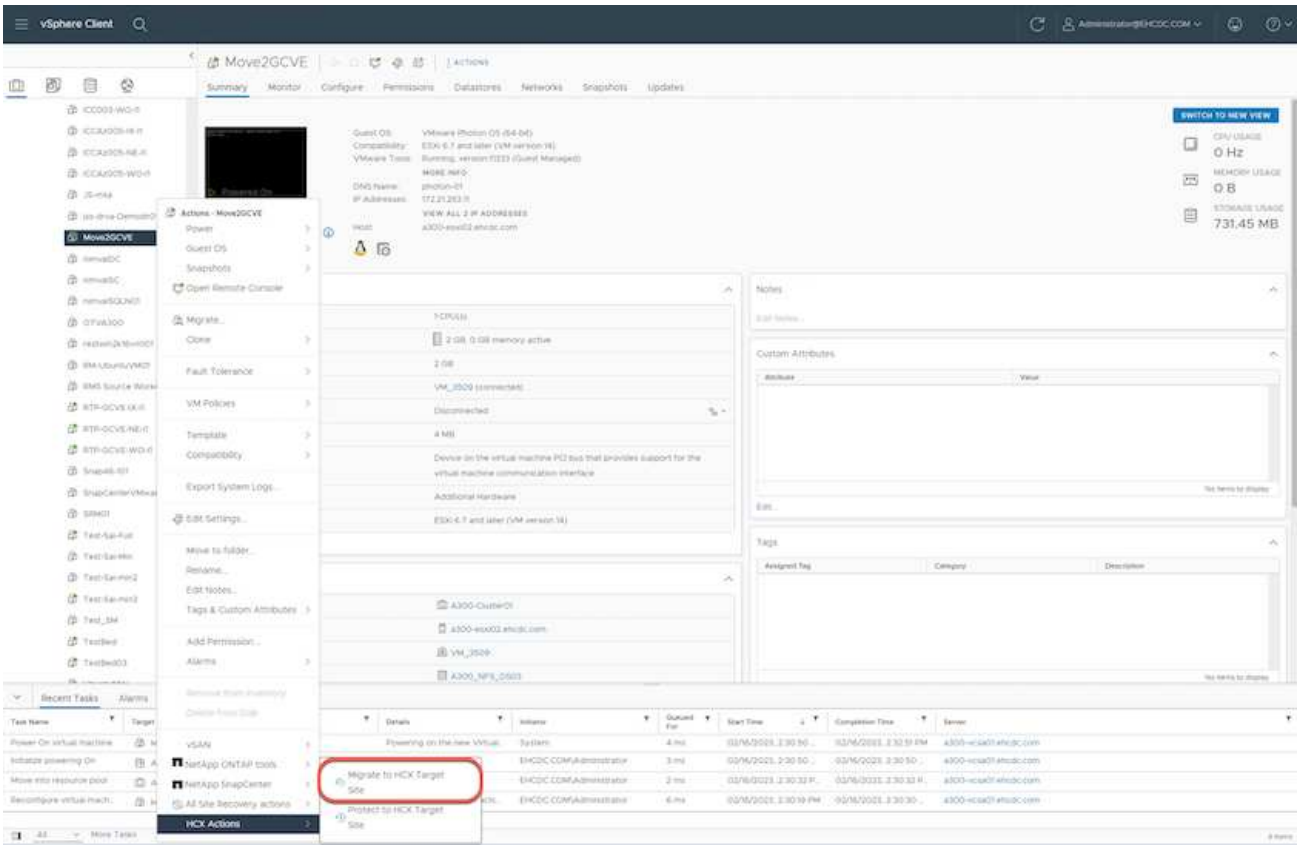
ⓘ HCX-IX 어플라이언스는 vCenter Server에 Mobility Agent 서비스를 호스트 개체로 추가합니다. 이 개체에 표시되는 프로세서, 메모리, 스토리지 및 네트워킹 리소스는 IX 어플라이언스를 호스팅하는 물리적 하이퍼바이저의 실제 소비량을 나타내지 않습니다.

HCX v모션

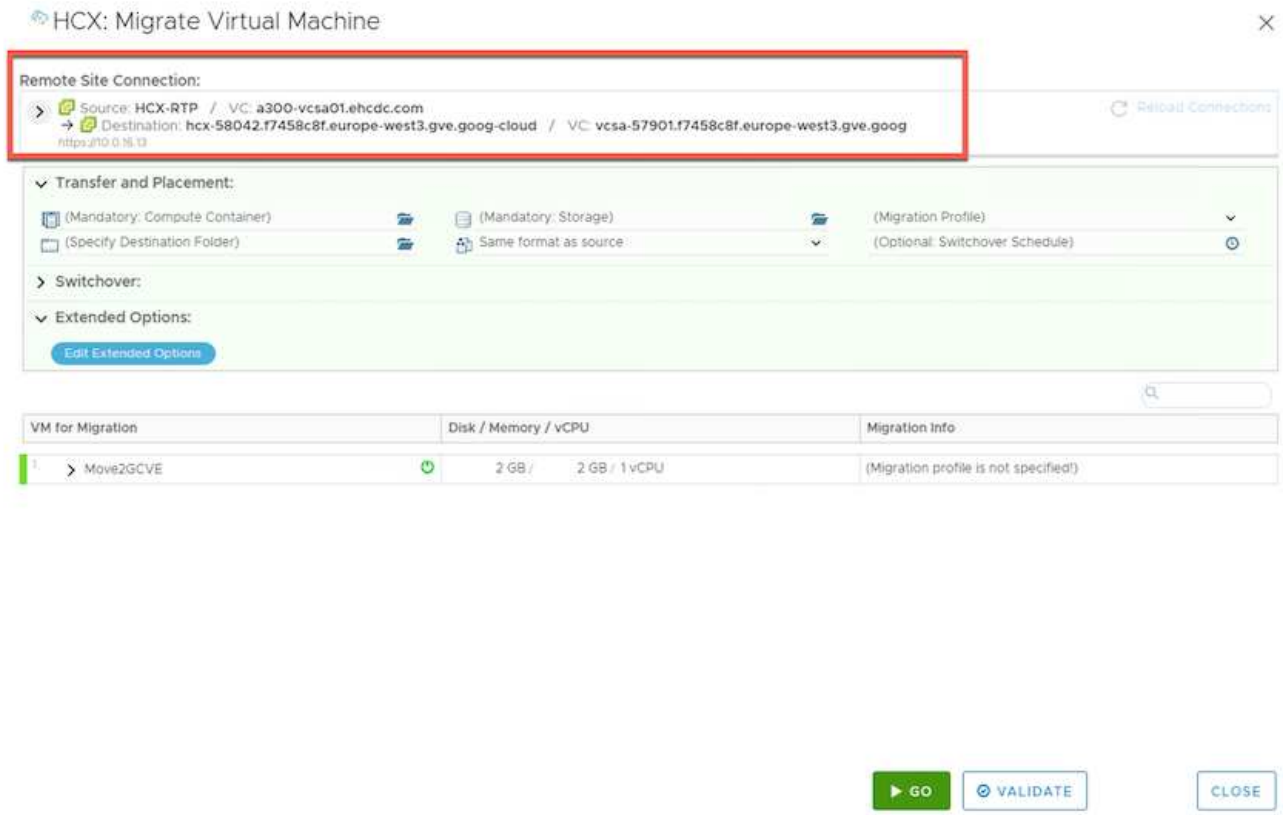
이 섹션에서는 HCX vMotion 메커니즘을 설명합니다. 이 마이그레이션 기술은 VMware vMotion 프로토콜을 사용하여 VM을 GCVE로 마이그레이션합니다. vMotion 마이그레이션 옵션은 한 번에 하나의 VM의 VM 상태를 마이그레이션하는 데 사용됩니다. 이 마이그레이션 방법을 사용하는 동안 서비스 중단은 발생하지 않습니다.

ⓘ IP 주소를 변경하지 않고도 VM을 마이그레이션하려면 VM이 연결된 포트 그룹에 대해 네트워크 확장이 있어야 합니다.

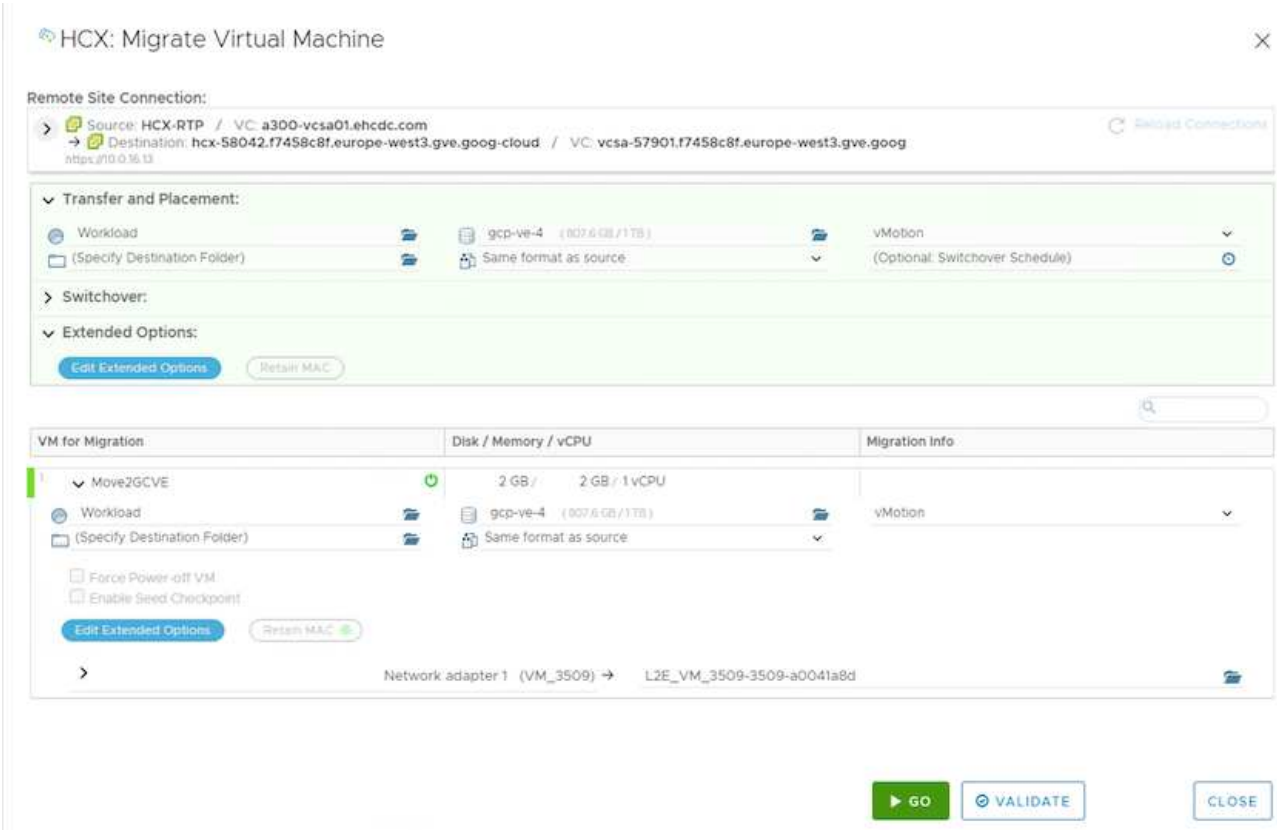
1. 온프레미스 vSphere 클라이언트에서 인벤토리로 이동하여 마이그레이션할 VM을 마우스 오른쪽 버튼으로 클릭하고 HCX 작업 > HCX 대상 사이트로 마이그레이션을 선택합니다.



2. 가상 머신 마이그레이션 마법사에서 원격 사이트 연결(대상 GCVE)을 선택합니다.



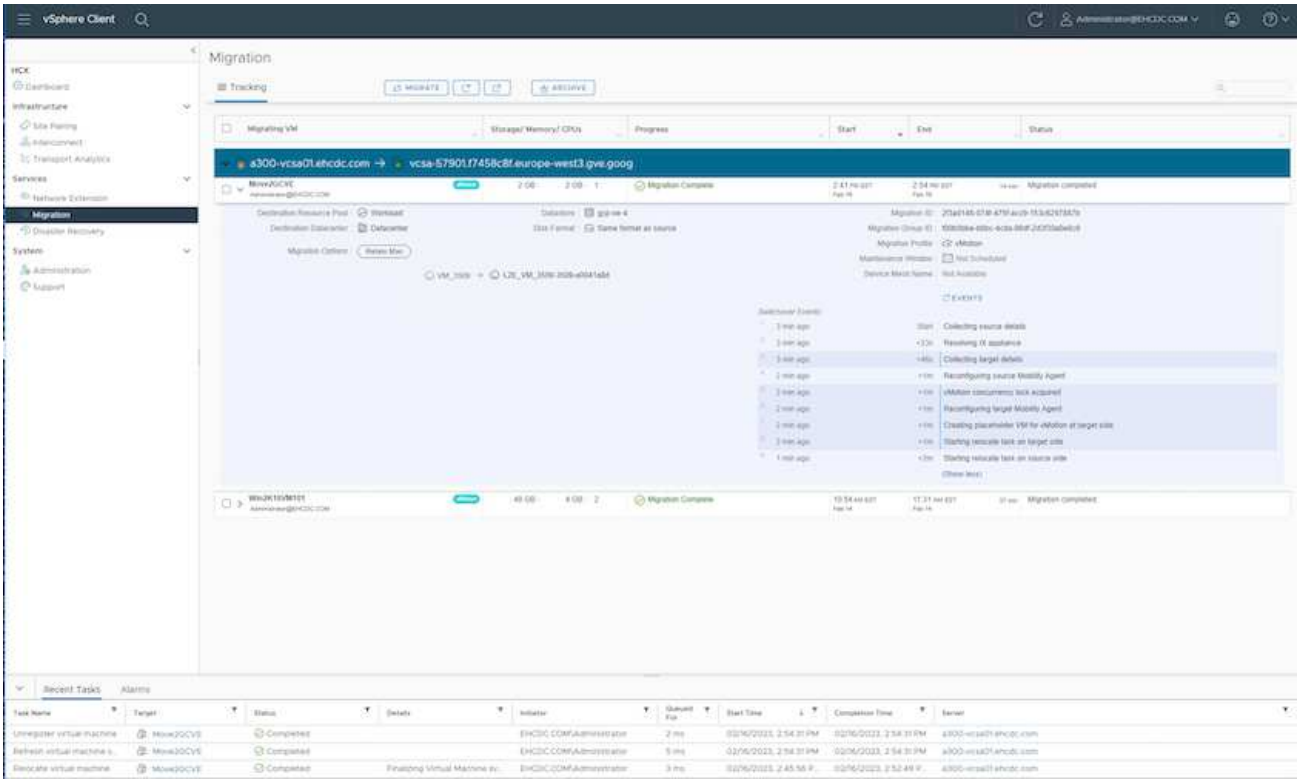
3. 필수 필드(클러스터, 저장소, 대상 네트워크)를 업데이트하고 확인을 클릭합니다.



4. 유효성 검사가 완료되면 '이동'을 클릭하여 마이그레이션을 시작합니다.

> vMotion 전송은 VM의 활성 메모리, 실행 상태, IP 주소, MAC 주소를 캡처합니다. HCX vMotion의 요구 사항 및 제한 사항에 대한 자세한 내용은 다음을 참조하세요. "VMware HCX vMotion 및 콜드 마이그레이션 이해" .

5. HCX > 마이그레이션 대시보드에서 vMotion의 진행 상황과 완료를 모니터링할 수 있습니다.



대상 Google Cloud NetApp Volumes (NetApp Volumes) NFS 데이터 저장소에는 마이그레이션을 처리할 수 있는 충분한 공간이 있어야 합니다.

결론

온프레미스의 모든 유형/공급업체 스토리지에 있는 데이터를 대상으로 전체 클라우드 또는 하이브리드 클라우드를 타겟팅하든, Cloud Volume Service와 HCX는 데이터 요구 사항을 애플리케이션 계층에 원활하게 전달하여 TCO를 줄이는 동시에 애플리케이션 워크로드를 배포하고 마이그레이션할 수 있는 탁월한 옵션을 제공합니다. 어떤 사용 사례에서든 클라우드의 이점을 빠르게 실현하고, 온프레미스와 여러 클라우드에서 일관된 인프라와 운영을 구현하고, 워크로드를 양방향으로 이동시키고, 엔터프라이즈급 용량과 성능을 얻으려면 Cloud Volume Service와 함께 Google Cloud VMware Engine을 선택하세요. VMware vSphere Replication, VMware vMotion 또는 NFC(네트워크 파일 복사)를 사용하여 스토리지를 연결하고 VM을 마이그레이션하는 데 사용되는 익숙한 프로세스 및 절차와 동일합니다.

테이크아웃

이 문서의 주요 내용은 다음과 같습니다.

- 이제 Google Cloud VMware Engine SDDC에서 Cloud Volume Service를 데이터 저장소로 사용할 수 있습니다.
- 온프레미스에서 Cloud Volume Service 데이터 저장소로 데이터를 쉽게 마이그레이션할 수 있습니다.
- 마이그레이션 작업 중에 용량 및 성능 요구 사항을 충족하기 위해 Cloud Volume Service 데이터 저장소를 쉽게 확장하거나 축소할 수 있습니다.

참고용 **Google** 및 **VMware**의 비디오

▼ 구글에서

- "GCVE를 사용하여 HCX 커넥터 배포"
- "GCVE를 사용하여 HCX ServiceMesh 구성"

- "HCX를 사용하여 VM을 GCVE로 마이그레이션"

▼ **VMware**에서

- "GCVE를 위한 HCX 커넥터 배포"
- "GCVE를 위한 HCX ServiceMesh 구성"
- "HCX 워크로드를 GCVE로 마이그레이션"

추가 정보를 찾을 수 있는 곳

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 웹사이트 링크를 참조하세요.

- Google Cloud VMware Engine 문서

  "https://cloud.google.com/vmware-engine/docs/overview"

- Cloud Volume Service 설명서

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- VMware HCX 사용자 가이드

  "https://docs.vmware.com/en/VMware-HCX/index.html"

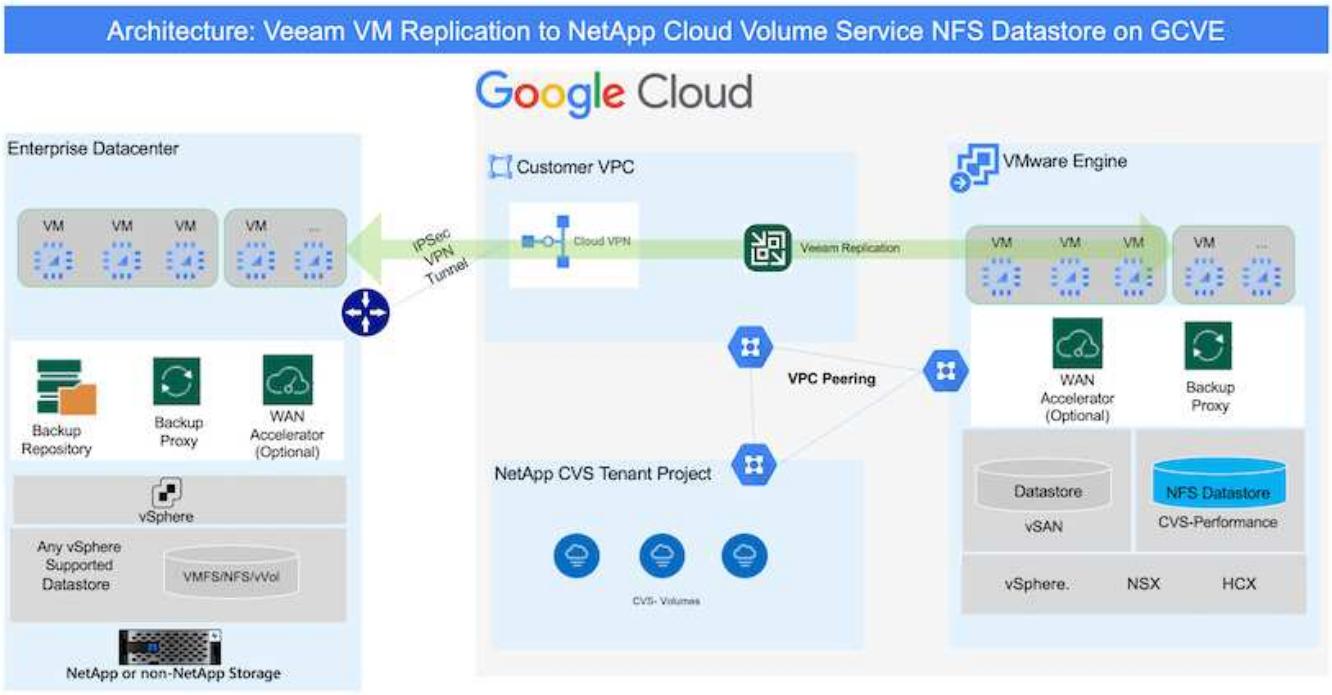
Veeam 복제 기능을 사용하여 **Google Cloud NetApp Volumes NFS** 데이터 저장소로 **VM** 마이그레이션

현재 데이터 보호 요구 사항을 위해 Veeam을 사용하고 있는 고객은 해당 솔루션을 계속 사용하여 워크로드를 GCVE로 마이그레이션하고 Google Cloud NetApp Volumes NFS 데이터 저장소의 이점을 누리고 있습니다.

개요

VMware vSphere에서 실행되는 VM 워크로드는 Veeam 복제 기능을 활용하여 Google Cloud VMware Engine(GCVE)으로 마이그레이션할 수 있습니다.

이 문서에서는 Google Cloud NetApp Volumes, Veeam 및 Google Cloud VMware Engine(GCVE)을 사용하여 VM 마이그레이션을 설정하고 수행하기 위한 단계별 접근 방식을 제공합니다.



가정

이 문서에서는 기존 vSphere 서버에서 Google Cloud VMware Engine으로 네트워크 연결을 설정하기 위해 Google Cloud VPN이나 Cloud Interconnect 또는 기타 네트워킹 옵션이 있다고 가정합니다.

온프레미스 데이터 센터를 Google Cloud에 연결하는 데에는 여러 가지 옵션이 있으므로 이 문서에서는 구체적인 워크플로를 설명할 수 없습니다. 를 참조하세요"Google Cloud 문서" 온프레미스와 Google 간의 적절한 연결 방법에 대해 알아보세요.

마이그레이션 솔루션 배포

솔루션 배포 개요

1. Google Cloud NetApp Volumes 의 NFS 데이터 저장소가 GCVE vCenter에 마운트되었는지 확인하세요.
2. Veeam Backup Recovery가 기존 VMware vSphere 환경에 배포되었는지 확인하세요.
3. Google Cloud VMware Engine 인스턴스에 가상 머신 복제를 시작하려면 복제 작업을 만듭니다.
4. Veeam 복제 작업의 장애 조치를 수행합니다.
5. Veeam에서 영구 장애 조치를 수행합니다.

배포 세부 정보

Google Cloud NetApp Volumes 의 **NFS** 데이터 저장소가 **GCVE vCenter**에 마운트되었는지 확인하세요**.**

GCVE vCenter에 로그인하여 충분한 공간이 있는 NFS 데이터 저장소가 있는지 확인하세요. 그렇지 않은 경우 다음을 참조하세요."GCVE에서 NetApp 볼륨을 NFS 데이터 저장소로 마운트"

Veeam Backup Recovery가 기존 **VMware vSphere** 환경에 배포되었는지 확인하세요.

참고해주세요"Veeam 복제 구성 요소" 필수 구성 요소를 설치하기 위한 설명서입니다.

Google Cloud VMware Engine 인스턴스에 가상 머신 복제를 시작하려면 복제 작업을 만듭니다.

온프레미스 vCenter와 GCVE vCenter 모두 Veeam에 등록해야 합니다. "vSphere VM 복제 작업 설정" 다음은 방법을 설명하는 비디오입니다."복제 작업 구성" .

> 복제 VM은 소스 VM과 다른 IP를 가질 수 있으며, 다른 포트 그룹에 연결될 수도 있습니다. 자세한 내용은 위의 영상을 확인하세요.

Veeam 복제 작업의 장애 조치 수행

VM을 마이그레이션하려면 다음을 수행하십시오."장애 조치 수행"

Veeam에서 영구 장애 조치를 수행합니다.

GCVE를 새로운 소스 환경으로 처리하려면 다음을 수행하십시오."영구 장애 조치"

이 솔루션의 이점

- 기존 Veeam 백업 인프라를 마이그레이션에 활용할 수 있습니다.
- Veeam Replication을 사용하면 대상 사이트의 VM IP 주소를 변경할 수 있습니다.
- Veeam 외부에서 복제된 기존 데이터(예: NetApp 시스템에서 복제된 데이터)를 다시 매핑할 수 있는 기능이 있습니다.
- 대상 사이트에서 다양한 네트워크 포트 그룹을 지정할 수 있는 기능이 있습니다.
- VM의 전원 켜기 순서를 지정할 수 있습니다.
- WAN을 통해 전송하는 데이터 양을 최소화하기 위해 VMware 변경 블록 추적을 활용합니다.
- 복제를 위한 사전 및 사후 스크립트를 실행할 수 있는 기능.
- 스냅샷에 대한 사전 및 사후 스크립트를 실행하는 기능.

Google Cloud의 Google Cloud NetApp Volumes 로 데이터 보호

TR-4918: 보안 개요 **- Google Cloud**의 **Google Cloud NetApp Volumes**

올리버 크라우스, 저스틴 파리시, NetApp

특히 스토리지 관리자가 인프라를 제어할 수 없는 클라우드 환경에서 보안은 클라우드 제공업체가 제공하는 서비스에 데이터를 안심하고 맡기기 위해 가장 중요합니다. 이 문서는 "Google Cloud NetApp Volumes Google Cloud에서 제공됩니다."에서 제공하는 보안 서비스에 대한 개요입니다.

대상 청중

이 문서의 대상 독자는 다음과 같은 역할을 포함하되 이에 국한되지 않습니다.

- 클라우드 제공업체
- 스토리지 관리자
- 스토리지 아키텍트
- 현장 자원
- 비즈니스 의사 결정권자

이 기술 보고서의 내용에 대해 질문이 있는 경우 다음 섹션을 참조하세요."문의하세요."

약어	정의
NetApp 볼륨-SW	Google Cloud NetApp Volumes, 서비스 유형 NetApp Volumes
NetApp 볼륨-성능	클라우드 볼륨 서비스, 서비스 유형 NetApp 볼륨-성능
공익광고	

Google Cloud의 **Google Cloud NetApp Volumes** 데이터를 보호하는 방법

Google Cloud의 Google Cloud NetApp Volumes 기본적으로 데이터를 보호하는 다양한 방법을 제공합니다.

보안 아키텍처 및 테넌시 모델

Google Cloud NetApp Volumes 서비스 관리(제어 평면)와 데이터 액세스(데이터 평면)를 여러 엔드포인트에 분할하여 어느 쪽도 다른 쪽에 영향을 미치지 않도록 하여 Google Cloud에서 안전한 아키텍처를 제공합니다(섹션 참조)."Google Cloud NetApp Volumes 아키텍처"). Google을 사용합니다 "개인 서비스 접근" (PSA) 프레임워크를 통해 서비스를 제공합니다. 이 프레임워크는 NetApp 에서 제공하고 운영하는 서비스 생산자와 고객 프로젝트의 가상 사설 클라우드(VPC)인 서비스 소비자를 구분합니다. 이 소비자는 Google Cloud NetApp Volumes 파일 공유에 액세스하려는 클라이언트를 호스팅합니다.

이 아키텍처에서는 세입자(섹션 참조)"임대 모델")은 사용자가 명시적으로 연결하지 않는 한 서로 완전히 분리된 Google Cloud 프로젝트로 정의됩니다. 테넌트는 Google Cloud NetApp Volumes 볼륨 플랫폼을 사용하여 다른 테넌트로부터 데이터 볼륨, 외부 이름 서비스 및 기타 필수 솔루션 부분을 완전히 격리할 수 있습니다. Google Cloud NetApp Volumes 플랫폼은 VPC 피어링을 통해 연결되므로 해당 격리가 여기에도 적용됩니다. 공유 VPC를 사용하여 여러 프로젝트 간에 Google Cloud NetApp Volumes 볼륨 공유를 활성화할 수 있습니다(섹션 참조)"공유 VPC"). SMB 공유 및 NFS 내보내기에 액세스 제어를 적용하여 데이터 세트를 보거나 수정할 수 있는 사람이나 항목을 제한할 수 있습니다.

제어 평면에 대한 강력한 **ID** 관리

Google Cloud NetApp Volumes 구성이 이루어지는 제어 평면에서 ID 관리는 다음을 사용하여 관리됩니다. "ID 액세스 관리(IAM)" . IAM은 Google Cloud 프로젝트 인스턴스에 대한 인증(로그인) 및 권한 부여(사용 권한)를 제어할 수 있는 표준 서비스입니다. 모든 구성은 TLS 1.2 암호화를 사용하는 안전한 HTTPS 전송을 통해 Google Cloud NetApp Volumes API를 통해 수행되며, 추가 보안을 위해 JWT 토큰을 사용하여 인증이 수행됩니다. Google Cloud NetApp Volumes 용 Google 콘솔 UI는 사용자 입력을 Google Cloud NetApp Volumes API 호출로 변환합니다.

보안 강화 **-** 공격 표면 제한

효과적인 보안의 일부는 서비스에서 사용 가능한 공격 표면의 수를 제한하는 것입니다. 공격 표면에는 저장 데이터, 전송 중인 데이터, 로그인, 데이터 세트 자체 등 다양한 요소가 포함될 수 있습니다.

관리형 서비스는 설계상 본질적으로 일부 공격 영역을 제거합니다. 섹션에 설명된 대로 인프라 관리"서비스 운영," 전담팀이 처리하고 자동화하여 실제로 사람이 구성을 만지는 횟수를 줄임으로써 의도적이든 의도치 않은 오류든 발생하는 횟수를 줄이는 데 도움이 됩니다. 네트워크는 반드시 필요한 서비스만 서로 접근할 수 있도록 울타리로 둘러싸여 있습니다. 암호화는 데이터 저장소에 내장되어 있으며 데이터 평면에만 Google Cloud NetApp Volumes 관리자가 보안에 주의를 기울여야 합니다. 대부분의 관리를 API 인터페이스 뒤에 숨기면 공격 표면을 제한하여 보안을 확보할 수 있습니다.

제로 트러스트 모델

역사적으로 IT 보안 철학은 신뢰하되 확인하는 것이었으며, 위협을 완화하기 위해 외부 메커니즘(예: 방화벽 및 침입 탐지 시스템)에만 의존하는 것으로 나타났습니다. 그러나 공격과 침해는 피싱, 소셜 엔지니어링, 내부자 위협 및 네트워크에 침입하여 파괴를 일으키는 검증 방법을 제공하는 기타 방법을 통해 검증을 우회하는 방식으로 발전했습니다.

Zero Trust는 보안의 새로운 방법론이 되었으며, 현재의 모토는 "모든 것을 검증하면서도 아무것도 믿지 마라"입니다. 따라서 기본적으로 아무것도 접근이 허용되지 않습니다. 이 만트라는 표준 방화벽과 침입 탐지 시스템(IDS)을 포함한 다양한 방법으로 시행되며 다음과 같은 방법을 통해서도 시행됩니다.

- 강력한 인증 방법(AES 암호화 Kerberos 또는 JWT 토큰 등)
- 단일 강력한 ID 소스(예: Windows Active Directory, LDAP(Lightweight Directory Access Protocol), Google IAM)
- 네트워크 분할 및 보안 멀티테넌시(기본적으로 테넌트만 액세스 허용)
- 최소 권한 액세스 정책을 통한 세분화된 액세스 제어
- 디지털 감사 및 서류 추적 기능을 갖춘 전담 및 신뢰할 수 있는 관리자의 소규모 독점 목록

Google Cloud에서 실행되는 Google Google Cloud NetApp Volumes "아무것도 믿지 않고, 모든 것을 검증한다"는 입장을 구현하여 Zero Trust 모델을 고수합니다.

암호화

정지 상태의 데이터 암호화(섹션 참조)"저장 중 데이터 암호화") NetApp Volume Encryption(NVE)과 함께 XTS-AES-256 암호를 사용하고 비행 중에"SMB 암호화" 또는 NFS Kerberos 5p 지원. 지역 간 복제 전송은 TLS 1.2 암호화로 보호되므로 안심할 수 있습니다(섹션 링크:gcp-gcnv-security-considerations.html#랜섬웨어, 맬웨어 및 바이러스의 탐지, 예방 및 완화#cross-region-replication["지역 간 복제"] 참조). 또한 Google 네트워킹은 암호화된 통신도 제공합니다(섹션 참조)"전송 중 데이터 암호화") 공격에 대한 보호 계층을 추가했습니다. 전송 암호화에 대한 자세한 내용은 섹션을 참조하세요."구글 클라우드 네트워크" .

데이터 보호 및 백업

보안은 단순히 공격을 예방하는 것만이 아닙니다. 또한 공격이 발생할 경우 어떻게 공격을 복구할 것인가에 대한 내용도 있습니다. 이 전략에는 데이터 보호와 백업이 포함됩니다. Google Cloud NetApp Volumes 중단 발생 시 다른 지역으로 복제하는 방법을 제공합니다(섹션 참조)."지역 간 복제") 또는 데이터 세트가 랜섬웨어 공격의 영향을 받는 경우. 또한 다음을 사용하여 Google Cloud NetApp Volumes 인스턴스 외부 위치에 대한 비동기 데이터 백업을 수행할 수도 있습니다."Google Cloud NetApp Volumes 백업" . 정기적으로 백업하면 보안 사고를 완화하는 데 걸리는 시간을 줄이고 관리자의 비용과 걱정을 줄일 수 있습니다.

업계 최고의 스냅샷 복사본을 통한 빠른 랜섬웨어 완화

데이터 보호 및 백업 외에도 Google Cloud NetApp Volumes 변경 불가능한 스냅샷 복사본에 대한 지원을 제공합니다(섹션 참조)."변경 불가능한 스냅샷 복사본") 랜섬웨어 공격으로부터 복구를 허용하는 볼륨(섹션 참조)"서비스 운영" 문제를 발견한 후 몇 초 이내에 최소한의 방해로 해결합니다. 복구 시간과 효과는 스냅샷 일정에 따라 다르지만, 랜섬웨어 공격 시 최소 1시간 간격의 델타를 제공하는 스냅샷 사본을 만들 수 있습니다. 스냅샷 복사는 성능과 용량

사용에 미치는 영향이 미미하며 데이터 세트를 보호하는 데 있어 위험은 적고 보상은 높은 접근 방식입니다.

보안 고려 사항 및 공격 표면

데이터 보안 방법을 이해하기 위한 첫 번째 단계는 위험과 잠재적인 공격 영역을 파악하는 것입니다.

여기에는 다음이 포함됩니다(이에 국한되지 않음):

- 관리 및 로그인
- 정지 상태의 데이터
- 비행 중 데이터
- 네트워크 및 방화벽
- 랜섬웨어, 맬웨어 및 바이러스

공격 표면을 이해하면 환경의 보안을 강화하는 데 도움이 됩니다. Google Cloud의 Google Cloud NetApp Volumes 이미 이러한 주제 중 많은 부분을 고려하고 있으며, 어떠한 관리자 상호 작용 없이도 기본적으로 보안 기능을 구현합니다.

안전한 로그인 보장

중요한 인프라 구성 요소를 보호할 때 승인된 사용자만 로그인하여 환경을 관리할 수 있도록 하는 것이 중요합니다. 악의적인 행위자가 관리자 자격 증명을 침해하면 성에 접근할 수 있는 열쇠를 손에 넣고 구성 변경, 볼륨 및 백업 삭제, 백도어 생성 또는 스냅샷 일정 비활성화 등 원하는 작업을 모두 수행할 수 있습니다.

Google Cloud용 Google Cloud NetApp Volumes StaaS(Storage as a Service)의 난독화를 통해 승인되지 않은 관리자 로그인으로부터 보호합니다. Google Cloud NetApp Volumes 외부 로그인 없이 클라우드 제공업체에서 전적으로 유지 관리합니다. 모든 설정 및 구성 작업은 완전히 자동화되어 있어, 매우 드문 상황을 제외하고는 인간 관리자가 시스템과 상호 작용할 필요가 전혀 없습니다.

로그인이 필요한 경우, Google Cloud의 Google Cloud NetApp Volumes 시스템에 로그인할 수 있는 신뢰할 수 있는 관리자의 매우 짧은 목록을 유지하여 로그인을 보호합니다. 이러한 게이트키핑은 잠재적으로 악의적인 행위자가 접근하는 횟수를 줄이는 데 도움이 됩니다. 또한, Google Cloud 네트워킹은 여러 계층의 네트워크 보안 뒤에 시스템을 숨기고 외부 세계에 필요한 것만 노출합니다. Google Cloud, Google Cloud NetApp Volumes 아키텍처에 대한 정보는 다음 섹션을 참조하세요."Google Cloud NetApp Volumes 아키텍처."

클러스터 관리 및 업그레이드

잠재적인 보안 위험이 있는 두 가지 영역으로는 클러스터 관리(악의적인 행위자가 관리자 액세스 권한을 갖는 경우 발생)와 업그레이드(소프트웨어 이미지가 손상된 경우 발생)가 있습니다.

스토리지 관리 보호

서비스로 제공되는 스토리지는 클라우드 데이터 센터 외부의 최종 사용자가 액세스할 수 없도록 하여 관리자가 노출될 수 있는 추가적인 위험을 제거합니다. 대신, 고객이 데이터 액세스 플레인에 대해서만 구성이 수행됩니다. 각 테넌트는 자체 볼륨을 관리하며, 어떤 테넌트도 다른 Google Cloud NetApp Volumes 인스턴스에 접속할 수 없습니다. 서비스는 자동화로 관리되며, 섹션에 설명된 프로세스를 통해 시스템에 대한 액세스 권한이 부여된 매우 소수의 신뢰할 수 있는 관리자 목록이 있습니다."서비스 운영."

NetApp Volumes-Performance 서비스 유형은 지역에 장애가 발생할 경우 다른 지역에 대한 데이터 보호를 제공하기

위한 옵션으로 지역 간 복제를 제공합니다. 이러한 경우, Google Cloud NetApp Volumes 영향을 받지 않는 지역으로 장애 조치되어 데이터 액세스를 유지할 수 있습니다.

서비스 업그레이드

업데이트는 취약한 시스템을 보호하는 데 도움이 됩니다. 각 업데이트에는 공격 표면을 최소화하는 보안 강화 및 버그 수정이 제공됩니다. 소프트웨어 업데이트는 중앙 저장소에서 다운로드되고, 업데이트가 허용되기 전에 검증을 거쳐 공식 이미지가 사용되었는지, 그리고 악의적인 행위자에 의해 업그레이드가 손상되지 않았는지 확인합니다.

Google Cloud NetApp Volumes 사용하면 클라우드 제공업체 팀이 업데이트를 처리하므로 구성 및 업그레이드에 정통하고 프로세스를 자동화하고 완벽하게 테스트한 전문가를 제공함으로써 관리자 팀의 위험 노출이 제거됩니다. 업그레이드는 중단 없이 이루어지며, Google Cloud NetApp Volumes 최상의 전반적인 결과를 위해 최신 업데이트를 유지합니다.

이러한 서비스 업그레이드를 수행하는 관리자 팀에 대한 정보는 다음 섹션을 참조하세요."서비스 운영."

저장 중인 데이터 보안

디스크가 도난당하거나 반환되거나 다른 용도로 사용되는 경우를 대비해 저장 데이터 암호화는 중요한 역할을 합니다. Google Cloud NetApp Volumes 의 데이터는 소프트웨어 기반 암호화를 사용하여 저장 상태에서 보호됩니다.

- Google에서 생성한 키는 NetApp Volumes-SW에 사용됩니다.
- NetApp Volumes-Performance의 경우 볼륨별 키는 Google Cloud NetApp Volumes 에 내장된 키 관리자에 저장되며, 이 키 관리자는 NetApp ONTAP CryptoMod를 사용하여 AES-256 암호화 키를 생성합니다. CryptoMod는 CMVP FIPS 140-2 검증 모듈 목록에 등재되어 있습니다. 보다 "FIPS 140-2 인증 #4144" .

2021년 11월부터 NetApp Volumes-Performance에 대한 고객 관리 암호화(CMEK) 기능 미리보기가 제공되었습니다. 이 기능을 사용하면 Google 키 관리 서비스(KMS)에 호스팅된 프로젝트별, 지역별 마스터 키로 볼륨별 키를 암호화할 수 있습니다. KMS를 사용하면 외부 키 관리자를 연결할 수 있습니다.

NetApp Volumes-Performance용 KMS 구성 방법에 대한 자세한 내용은 다음을 참조하십시오 "Google Cloud NetApp Volumes 문서를 참조하세요.".

아키텍처에 대한 자세한 내용은 섹션을 참조하세요."Google Cloud NetApp Volumes 아키텍처."

비행 중 데이터 보안

저장 중인 데이터를 보호하는 것 외에도 Google Cloud NetApp Volumes 인스턴스와 클라이언트 또는 복제 대상 간에 데이터가 전송되는 동안에도 데이터를 보호할 수 있어야 합니다. Google Cloud NetApp Volumes Kerberos를 사용한 SMB 암호화, 패킷 서명/봉인, 데이터 전송의 종단 간 암호화를 위한 NFS Kerberos 5p와 같은 암호화 방법을 사용하여 NAS 프로토콜을 통해 전송 중인 데이터에 대한 암호화를 제공합니다.

Google Cloud NetApp Volumes 볼륨 복제에는 AES-GCM 암호화 방법을 활용하는 TLS 1.2가 사용됩니다.

Telnet, NDMP 등의 대부분의 안전하지 않은 기내 프로토콜은 기본적으로 비활성화되어 있습니다. 하지만 DNS는 Google Cloud NetApp Volumes 에서 암호화되지 않으므로(DNS Sec 지원 없음) 가능한 경우 외부 네트워크 암호화를 사용하여 암호화해야 합니다. 섹션을 참조하세요"전송 중 데이터 암호화" 전송 중 데이터 보안에 대한 자세한 내용은 여기를 참조하세요.

NAS 프로토콜 암호화에 대한 정보는 다음 섹션을 참조하세요."NAS 프로토콜."

NAS 권한에 대한 사용자 및 그룹

클라우드에서 데이터를 보호하는 데는 적절한 사용자 및 그룹 인증이 필요합니다. 즉, 데이터에 액세스하는 사용자가 해당 환경에서 실제 사용자인지 확인하고 그룹에 유효한 사용자가 포함되어 있는지 확인해야 합니다. 이러한 사용자와 그룹은 저장 시스템의 파일과 폴더에 대한 초기 공유 및 내보내기 액세스 권한과 권한 검증을 제공합니다.

Google Cloud NetApp Volumes SMB 공유 및 Windows 스타일 권한에 대해 표준 Active Directory 기반 Windows 사용자 및 그룹 인증을 사용합니다. 이 서비스는 NFS 내보내기, NFSv4 ID 유효성 검사, Kerberos 인증 및 NFSv4 ACL을 위한 UNIX 사용자 및 그룹을 위한 LDAP와 같은 UNIX ID 공급자를 활용할 수도 있습니다.

> 현재 Google Cloud NetApp Volumes 에서는 LDAP 기능을 위해 Active Directory LDAP만 지원됩니다.

랜섬웨어, 맬웨어 및 바이러스의 탐지, 예방 및 완화

랜섬웨어, 맬웨어, 바이러스는 관리자에게 지속적인 위협이며, 이러한 위협을 탐지, 예방, 완화하는 것이 기업 조직의 최우선 과제입니다. 중요한 데이터 세트에 대한 단일 랜섬웨어 공격은 잠재적으로 수백만 달러의 손실을 초래할 수 있으므로 위험을 최소화하기 위해 할 수 있는 모든 조치를 취하는 것이 좋습니다.

Google Cloud NetApp Volumes는 현재 바이러스 백신 보호 "자동 랜섬웨어 감지" 등 기본 탐지 또는 예방 조치를 포함하고 있지 않지만, 정기적인 스냅샷 일정을 활성화하여 랜섬웨어 이벤트로부터 신속하게 복구할 수 있습니다. 스냅샷 복사본은 변경 불가능하며 파일 시스템의 변경된 블록을 가리키는 읽기 전용 포인터로, 거의 즉각적으로 생성되고 성능에 미치는 영향이 최소화되며 데이터가 변경되거나 삭제될 때만 공간을 사용합니다. 원하는 복구 시점 목표(RPO)/복구 시간 목표(RTO)에 맞춰 스냅샷 복사본 일정을 설정할 수 있으며, 볼륨당 최대 1,024개의 스냅샷 복사본을 유지할 수 있습니다.

Google Cloud NetApp Volumes 에서는 스냅샷 지원이 추가 비용(스냅샷 복사본에 보관된 변경된 블록/데이터에 대한 데이터 저장 비용 제외) 없이 제공되며, 랜섬웨어 공격이 발생하는 경우 공격이 발생하기 전의 스냅샷 복사본으로 롤백하는 데 사용할 수 있습니다. 스냅샷 복원은 몇 초 만에 완료되며, 복원 후에는 평소처럼 데이터를 제공할 수 있습니다. 자세한 내용은 다음을 참조하세요. "랜섬웨어에 대한 NetApp 솔루션" .

랜섬웨어가 비즈니스에 영향을 미치지 않도록 방지하려면 다음 중 하나 이상을 포함하는 다층적 접근 방식이 필요합니다.

- 엔드포인트 보호
- 네트워크 방화벽을 통한 외부 위협으로부터 보호
- 데이터 이상 감지
- 중요 데이터 세트의 다중 백업(온사이트 및 오프사이트)
- 백업의 정기적인 복원 테스트
- 변경 불가능한 읽기 전용 NetApp 스냅샷 복사본
- 중요 인프라를 위한 다중 인증
- 시스템 로그인에 대한 보안 감사

이 목록은 모든 내용을 담고 있지는 않지만 랜섬웨어 공격의 가능성에 대처할 때 참고할 만한 좋은 청사진입니다. Google Cloud의 Google Cloud NetApp Volumes 랜섬웨어 이벤트로부터 보호하고 그 영향을 줄이는 여러 가지 방법을 제공합니다.

변경 불가능한 스냅샷 복사본

Google Cloud NetApp Volumes 기본적으로 사용자 지정 일정에 따라 생성되는 변경 불가능한 읽기 전용 스냅샷 복사본을 제공하여 데이터가 삭제되거나 전체 볼륨이 랜섬웨어 공격을 받은 경우 신속한 특정 시점 복구가 가능합니다. 스냅샷은 이전의 좋은 스냅샷 사본으로 빠르게 복원되며 스냅샷 일정과 RTO/RPO의 보존 기간을 기반으로 데이터 손실을 최소화합니다. 스냅샷 기술을 사용하면 성능에 미치는 영향이 미미합니다.

Google Cloud NetApp Volumes 의 스냅샷 복사본은 읽기 전용이므로 랜섬웨어가 눈에 띄지 않게 데이터 세트에 확산되고 랜섬웨어에 감염된 데이터의 스냅샷 복사본이 생성되지 않는 한 랜섬웨어에 감염될 수 없습니다. 따라서 데이터 이상을 기반으로 한 랜섬웨어 감지도 고려해야 합니다. Google Cloud NetApp Volumes 현재 기본적으로 감지 기능을 제공하지 않지만 외부 모니터링 소프트웨어를 사용할 수 있습니다.

백업 및 복원

Google Cloud NetApp Volumes 표준 NAS 클라이언트 백업 기능(NFS 또는 SMB를 통한 백업 등)을 제공합니다.

- NetApp Volumes-Performance는 다른 NetApp Volumes-Performance 볼륨으로의 리전 간 볼륨 복제를 제공합니다. 자세한 내용은 Google Cloud NetApp Volumes 설명서에서 "볼륨 복제"을(를) 참조하십시오.
- NetApp Volumes-SW는 서비스에서 기본적으로 볼륨 백업/복원 기능을 제공합니다. 자세한 내용은 Google Cloud NetApp Volumes 설명서의 "클라우드 백업"을(를) 참조하십시오.

볼륨 복제는 랜섬웨어 이벤트를 포함한 재해 발생 시 빠른 장애 조치를 위해 소스 볼륨의 정확한 사본을 제공합니다.

지역 간 복제

NetApp Volumes-Performance를 사용하면 Google 네트워크에서 실행되는 복제에 사용되는 특정 인터페이스를 사용하여 NetApp 에서 제어하는 백엔드 서비스 네트워크에서 TLS1.2 AES 256 GCM 암호화를 사용하여 데이터 보호 및 보관 사용 사례를 위해 Google Cloud 지역 전체에서 볼륨을 안전하게 복제할 수 있습니다. 기본(소스) 볼륨에는 활성 프로덕션 데이터가 포함되어 있으며 보조(대상) 볼륨에 복제되어 기본 데이터 세트의 정확한 복제본을 제공합니다.

초기 복제는 모든 블록을 전송하지만 업데이트는 기본 볼륨에서 변경된 블록만 전송합니다. 예를 들어, 기본 볼륨에 있는 1TB 데이터베이스를 보조 볼륨으로 복제하는 경우, 초기 복제 시 1TB의 공간이 전송됩니다. 해당 데이터베이스에 초기화와 다음 업데이트 사이에 변경되는 수백 개의 행(가정적으로 수 MB)이 있는 경우, 변경된 행이 있는 블록만 보조(수 MB)에 복제됩니다. 이를 통해 전송 시간을 짧게 유지하고 복제 비용을 낮추는 데 도움이 됩니다.

파일과 폴더에 대한 모든 권한은 보조 볼륨에 복제되지만 공유 액세스 권한(예: 내보내기 정책 및 규칙 또는 SMB 공유 및 공유 ACL)은 별도로 처리해야 합니다. 사이트 장애 조치(failover)의 경우 대상 사이트는 동일한 이름 서비스와 Active Directory 도메인 연결을 활용하여 사용자 및 그룹 ID와 권한을 일관되게 처리해야 합니다. 재해 발생 시 복제 관계를 끊고 보조 볼륨을 읽기-쓰기로 변환하여 보조 볼륨을 장애 조치 대상으로 사용할 수 있습니다.

볼륨 복제본은 읽기 전용이므로 바이러스에 의해 데이터가 감염되거나 랜섬웨어에 의해 기본 데이터 세트가 암호화된 경우 데이터를 빠르게 복구할 수 있도록 데이터의 변경 불가능한 복사본을 오프사이트에 제공합니다. 읽기 전용 데이터는 암호화되지 않지만, 기본 볼륨이 영향을 받고 복제가 발생하면 감염된 블록도 복제됩니다. 영향을 받지 않은 이전 스냅샷 복사본을 사용하여 복구할 수 있지만, 공격이 얼마나 빨리 감지되는지에 따라 SLA가 약속된 RTO/RPO 범위를 벗어날 수 있습니다.

또한 Google Cloud의 교차 리전 복제(CRR) 관리를 통해 볼륨 삭제, 스냅샷 삭제 또는 스냅샷 일정 변경 등 악의적인 관리 작업을 방지할 수 있습니다. 이를 위해 소스 볼륨은 삭제할 수 있지만 미러를 끊을 수 없어 대상 볼륨을 삭제할 수 없는 볼륨 관리자와 볼륨 작업을 전혀 수행할 수 없는 CRR 관리자를 분리하는 사용자 지정 역할을 생성합니다. 각 관리자 그룹에 허용되는 권한에 대해서는 Google Cloud NetApp Volumes 설명서의 "보안 고려 사항"을(를) 참조하십시오.

Google Cloud NetApp Volumes 백업

Google Cloud NetApp Volumes 높은 데이터 내구성을 제공하지만 외부 이벤트로 인해 데이터가 손실될 수 있습니다. 바이러스나 랜섬웨어와 같은 보안 이벤트가 발생하는 경우, 적절한 시기에 데이터 액세스를 재개하기 위해 백업과 복원이 매우 중요합니다. 관리자가 실수로 Google Cloud NetApp Volumes 볼륨을 삭제할 수 있습니다. 또는 사용자가 단순히 여러 달 동안 데이터의 백업 버전을 보관하고 싶어하고 볼륨 내부에 추가 스냅샷 복사 공간을 유지하는 것이 비용 문제가 될 수도 있습니다. 최근 몇 주 동안의 백업 버전을 보관하여 손실된 데이터를 복원하는 가장 좋은 방법은 스냅샷 복사본이지만, 해당 복사본은 볼륨 내부에 저장되어 있으며 볼륨이 사라지면 손실됩니다.

이러한 모든 이유로 Google Cloud NetApp Volumes는 "Google Cloud NetApp Volumes 백업"을(를) 통해 백업 서비스를 제공합니다.

Google Cloud NetApp Volumes 백업은 Google Cloud Storage(GCS)에 볼륨 사본을 생성합니다. 볼륨 내에 저장된 실제 데이터만 백업하며, 여유 공간은 백업하지 않습니다. 이 백업은 영구적으로 증분적으로 작동합니다. 즉, 볼륨 콘텐츠를 한 번 전송한 후 변경된 데이터만 계속 백업합니다. 여러 개의 전체 백업을 거치는 기존 백업 개념과 비교했을 때, 이 방식은 백업 스토리지 용량을 대폭 절약하여 비용을 절감합니다. 백업 공간의 월별 가격은 볼륨에 비해 낮으므로 백업 버전을 더 오랫동안 보관하기에 이상적인 곳입니다.

사용자는 Google Cloud NetApp Volumes 백업을 사용하여 동일한 지역 내의 동일 볼륨이나 다른 볼륨에 모든 백업 버전을 복원할 수 있습니다. 소스 볼륨이 삭제되더라도 백업 데이터는 보존되며 독립적으로 관리(예: 삭제)해야 합니다.

Google Cloud NetApp Volumes 백업은 옵션으로 Google Cloud NetApp Volumes에 기본 제공됩니다. 사용자는 볼륨별로 Google Cloud NetApp Volumes 백업을 활성화하여 보호할 볼륨을 결정할 수 있습니다. 백업, "지원되는 최대 백업 버전 수", 예약 및 "가격"에 대한 자세한 내용은 "Google Cloud NetApp Volumes 백업 설명서"을 참조하십시오.

프로젝트의 모든 백업 데이터는 GCS 버킷에 저장됩니다. 이 버킷은 서비스에서 관리하며 사용자에게는 보이지 않습니다. 각 프로젝트는 다른 버킷을 사용합니다. 현재 버킷은 Google Cloud NetApp Volumes 볼륨과 동일한 지역에 있지만 더 많은 옵션에 대해 논의 중입니다. 최신 상태를 확인하려면 설명서를 참조하세요.

Google Cloud NetApp Volumes 버킷에서 GCS로 데이터를 전송하는 데는 HTTPS 및 TLS1.2를 사용하는 서비스 내부 Google 네트워크가 사용됩니다. 저장된 데이터는 Google에서 관리하는 키를 사용하여 암호화됩니다.

Google Cloud NetApp Volumes 백업을 관리(백업 생성, 삭제 및 복원)하려면 사용자에게 "roles/netapp.admin" 역할이 있어야 합니다.

개요

클라우드 솔루션을 신뢰하려면 아키텍처와 보안 방식을 이해해야 합니다. 이 섹션에서는 Google의 Google Cloud NetApp Volumes 아키텍처의 다양한 측면을 설명하여 데이터 보안에 대한 잠재적 우려를 완화하는 데 도움을 주고, 가장 안전한 배포를 위해 추가 구성 단계가 필요할 수 있는 영역을 설명합니다.

Google Cloud NetApp Volumes 의 일반 아키텍처는 제어 평면과 데이터 평면이라는 두 가지 주요 구성 요소로 나눌 수 있습니다.

제어 평면

Google Cloud NetApp Volumes 의 제어 평면은 Google Cloud NetApp Volumes 관리자와 NetApp 기본 자동화 소프트웨어가 관리하는 백엔드 인프라입니다. 이 플레인은 최종 사용자에게 완전히 투명하며 네트워킹, 스토리지 하드웨어, 소프트웨어 업데이트 등을 포함하여 Google Cloud NetApp Volumes 와 같은 클라우드 상주 솔루션에 가치를 제공하는 데 도움이 됩니다.

데이터 플레인

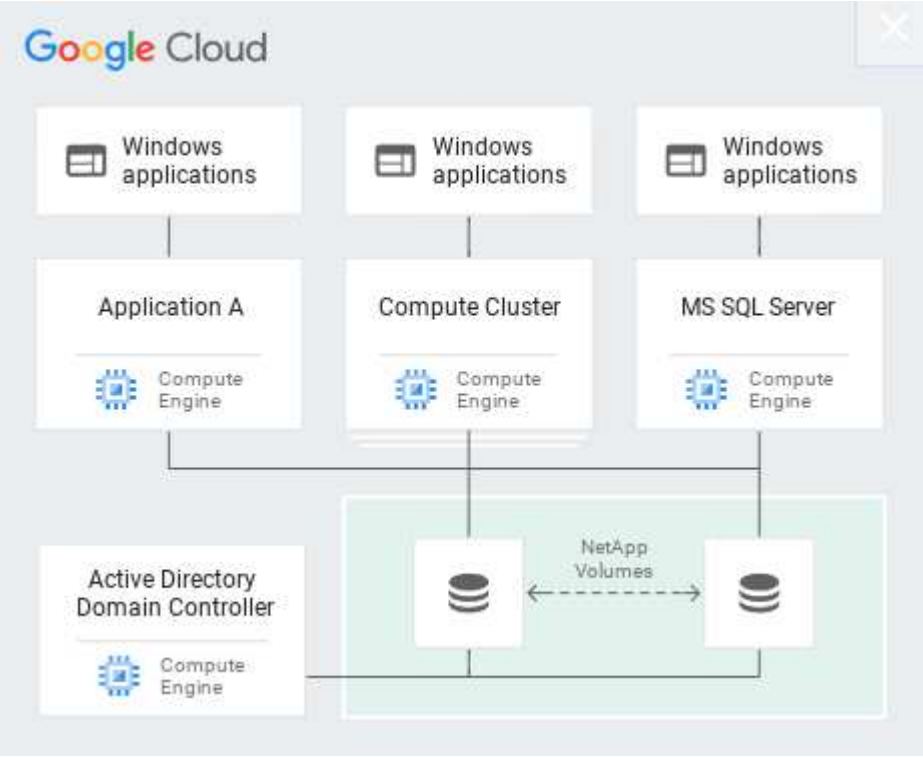
Google Cloud NetApp Volumes 의 데이터 플레인에는 실제 데이터 볼륨과 전반적인 Google Cloud NetApp Volumes 구성(액세스 제어, Kerberos 인증 등)이 포함됩니다. 데이터 플레인은 전적으로 Google Cloud NetApp Volumes 플랫폼의 최종 사용자와 소비자의 제어를 받습니다.

각 항공기의 보안 및 관리 방법에는 뚜렷한 차이가 있습니다. 다음 섹션에서는 Google Cloud NetApp Volumes 아키텍처 개요부터 시작하여 이러한 차이점에 대해 설명합니다.

Google Cloud NetApp Volumes 아키텍처

CloudSQL, Google Cloud VMware Engine(GCVE), FileStore와 같은 다른 Google Cloud 기본 서비스와 유사한 방식으로 Google Cloud NetApp Volumes 사용합니다. "구글 공익광고" 서비스를 제공하기 위해. PSA에서는 서비스가 서비스 생산자 프로젝트 내부에 구축됩니다. "VPC 네트워크 피어링" 서비스 소비자와 연결합니다. 서비스 제작자는 NetApp 에서 제공하고 운영하며, 서비스 소비자는 고객 프로젝트의 VPC로, Google Cloud NetApp Volumes 파일 공유에 액세스하려는 클라이언트를 호스팅합니다.

다음 그림은 "Google Cloud NetApp Volumes 설명서"에서 참조한 것으로 전체적인 개요를 보여줍니다.



점선 위의 부분은 볼륨 수명 주기를 제어하는 서비스의 제어 평면을 보여줍니다. 점선 아래 부분은 데이터 평면을 보여줍니다. 왼쪽 파란색 상자는 사용자 VPC(서비스 소비자)를 나타내고, 오른쪽 파란색 상자는 NetApp 에서 제공하는 서비스 생산자를 나타냅니다. 둘 다 VPC 피어링을 통해 연결됩니다.

임대 모델

Google Cloud NetApp Volumes 에서는 개별 프로젝트가 고유한 테넌트로 간주됩니다. 즉, 볼륨 조작, 스냅샷 복사본 등이 프로젝트별로 수행된다는 의미입니다. 즉, 모든 볼륨은 해당 볼륨이 생성된 프로젝트의 소유이며, 기본적으로 해당 프로젝트에서만 볼륨 내부의 데이터를 관리하고 액세스할 수 있습니다. 이는 서비스의 제어 평면 뷰로 간주됩니다.

공유 **VPC**

데이터 평면 보기에서 Google Cloud NetApp Volumes 공유 VPC에 연결할 수 있습니다. 호스팅 프로젝트나 공유 VPC에 연결된 서비스 프로젝트 중 하나에서 볼륨을 생성할 수 있습니다. 해당 공유 VPC에 연결된 모든 프로젝트(호스트 또는 서비스)는 네트워크 계층(TCP/IP)에서 볼륨에 도달할 수 있습니다. 공유 VPC에서 네트워크로 연결된 모든 클라이언트는 NAS 프로토콜을 통해 데이터에 액세스할 가능성이 있으므로 개별 볼륨에 대한 액세스 제어(예: 사용자/그룹 액세스 제어 목록(ACL) 및 NFS 내보내기용 호스트 이름/IP 주소)를 사용하여 누가 데이터에 액세스할 수 있는지 제어해야 합니다.

고객 프로젝트당 최대 5개의 VPC에 Google Cloud NetApp Volumes 연결할 수 있습니다. 제어 평면에서 이 프로젝트를 사용하면 연결된 VPC에 관계없이 생성된 모든 볼륨을 관리할 수 있습니다. 데이터 플레인에서 VPC는 서로 분리되어 있으며, 각 볼륨은 하나의 VPC에만 연결될 수 있습니다.

개별 볼륨에 대한 액세스는 프로토콜별(NFS/SMB) 액세스 제어 메커니즘을 통해 제어됩니다.

즉, 네트워크 계층에서는 공유 VPC에 연결된 모든 프로젝트가 볼륨을 볼 수 있는 반면, 관리 측면에서는 제어 평면을 통해 소유자 프로젝트만 볼륨을 볼 수 있습니다.

VPC 서비스 제어

VPC 서비스 제어는 인터넷에 연결되어 전 세계에서 접근 가능한 Google Cloud 서비스 주변에 액세스 제어 경계를 설정합니다. 이러한 서비스는 사용자 ID를 통해 액세스 제어를 제공하지만 어떤 네트워크 위치 요청이 발생하는지 제한할 수는 없습니다. VPC 서비스 제어는 정의된 네트워크에 대한 액세스를 제한하는 기능을 도입하여 이러한 격차를 해소합니다.

Google Cloud NetApp Volumes 데이터 플레인은 외부 인터넷에 연결되지 않고 명확하게 정의된 네트워크 경계(경계)가 있는 개인 VPC에 연결됩니다. 해당 네트워크 내에서 각 볼륨은 프로토콜별 액세스 제어를 사용합니다. 모든 외부 네트워크 연결은 Google Cloud 프로젝트 관리자가 명시적으로 생성합니다. 그러나 제어 평면은 데이터 평면과 동일한 보호 기능을 제공하지 않으며 유효한 자격 증명을 가진 모든 사람이 어디서나 액세스할 수 있습니다. "JWT 토큰").

간단히 말해, Google Cloud NetApp Volumes 데이터 플레인은 VPC 서비스 제어를 지원할 필요 없이 네트워크 액세스 제어 기능을 제공하며 VPC 서비스 제어를 명시적으로 사용하지 않습니다.

패킷 스니핑/추적 고려 사항

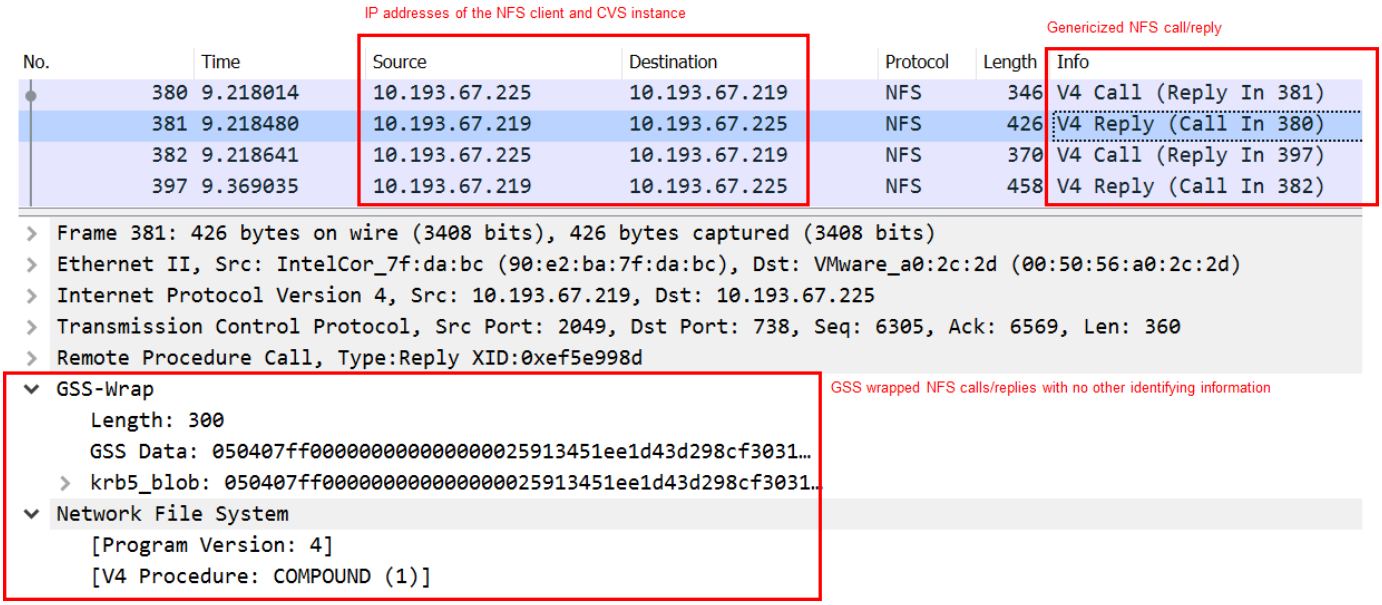
패킷 캡처는 네트워크 문제나 기타 문제(예: NAS 권한, LDAP 연결 등)를 해결하는 데 유용할 수 있지만, 네트워크 IP 주소, MAC 주소, 사용자 및 그룹 이름, 엔드포인트에서 사용되는 보안 수준에 대한 정보를 얻기 위해 악의적으로 사용될 수도 있습니다. Google Cloud 네트워킹, VPC 및 방화벽 규칙이 구성된 방식 때문에 사용자 로그인 자격 증명 없이는 원치 않는 네트워크 패킷 액세스를 얻기 어렵습니다."JWT 토큰" 클라우드 인스턴스로. 패킷 캡처는 엔드포인트(예: 가상 머신(VM))에서만 가능하며, 공유 VPC 및/또는 외부 네트워크 터널/IP 전달을 사용하여 엔드포인트로의 외부 트래픽을 명시적으로 허용하지 않는 한 VPC 내부의 엔드포인트에서만 가능합니다. 클라이언트 외부의 트래픽을 탐지할 방법이 없습니다.

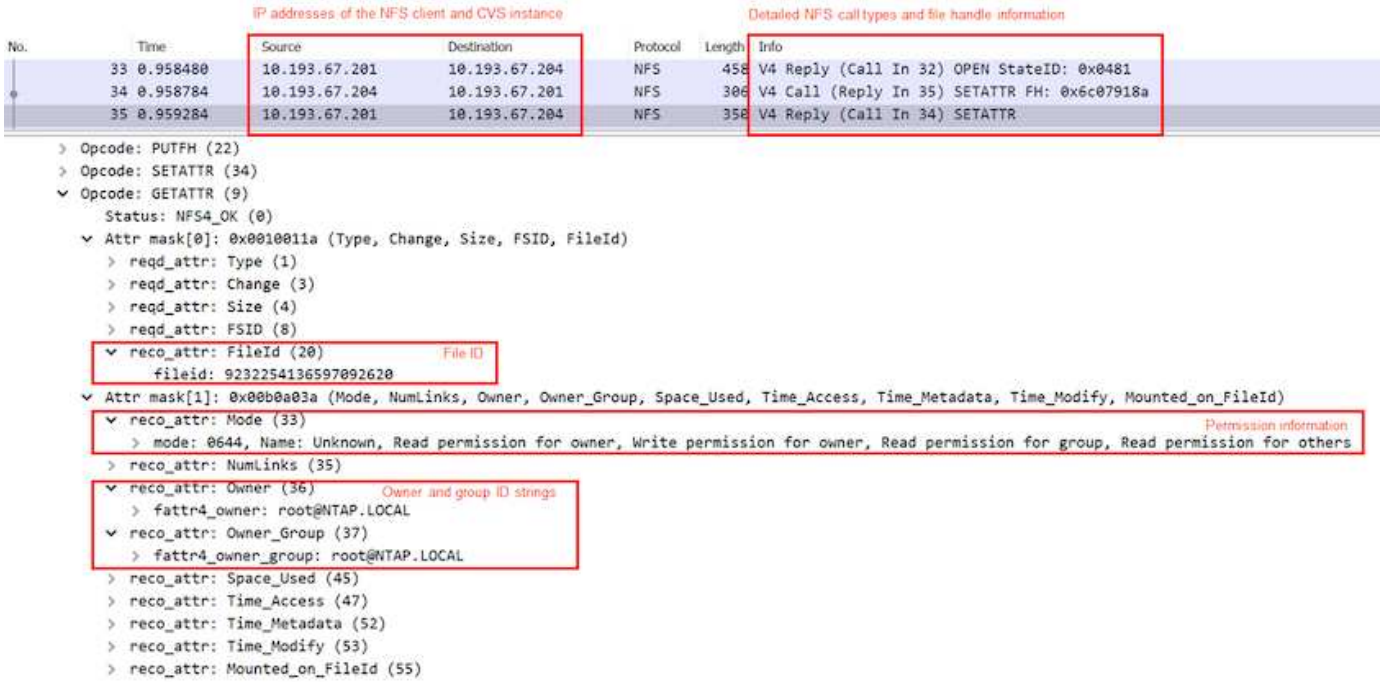
공유 VPC를 사용하는 경우 NFS Kerberos 및/또는"SMB 암호화" 흔적에서 얻은 정보의 대부분을 가릴 수 있습니다. 그러나 일부 트래픽은 여전히 일반 텍스트로 전송됩니다."DNS" 그리고"LDAP 쿼리" . 다음 그림은 Google Cloud NetApp Volumes 에서 발생한 일반 텍스트 LDAP 쿼리의 패킷 캡처와 노출된 잠재적 식별 정보를 보여줍니다. 현재 Google Cloud NetApp Volumes 의 LDAP 쿼리는 암호화나 SSL을 통한 LDAP를 지원하지 않습니다. NetApp Volumes-Performance는 Active Directory에서 요청하는 경우 LDAP 서명을 지원합니다. NetApp Volumes-SW는 LDAP 서명을 지원하지 않습니다.



unixUserPassword는 LDAP에 의해 쿼리되며 일반 텍스트로 전송되지 않고 대신 솔트 해시 형태로 전송됩니다. 기본적으로 Windows LDAP는 unixUserPassword 필드를 채우지 않습니다. 이 필드는 LDAP를 통해 클라이언트에 대한 대화형 로그인을 위해 Windows LDAP를 활용해야 하는 경우에만 필요합니다. Google Cloud NetApp Volumes 인스턴스에 대한 대화형 LDAP 로그인을 지원하지 않습니다.

다음 그림은 AUTH_SYS를 통한 NFS 캡처 옆에 있는 NFS Kerberos 대화의 패킷 캡처를 보여줍니다. 두 가지 추적에서 제공되는 정보가 어떻게 다른지, 그리고 전송 중 암호화를 활성화하면 NAS 트래픽에 대한 전반적인 보안이 어떻게 강화되는지 살펴보세요.





VM 네트워크 인터페이스

공격자가 시도할 수 있는 한 가지 방법은 VM에 새 네트워크 인터페이스 카드(NIC)를 추가하는 것입니다. "난잡한 모드" (포트 미러링) 또는 기존 NIC에서 무차별 모드를 활성화하여 모든 트래픽을 탐지합니다. Google Cloud에서 새로운 NIC를 추가하려면 VM을 완전히 종료해야 하며, 이를 통해 알림이 생성되므로 공격자가 이를 눈치채지 못하게 수행할 수 없습니다.

또한 NIC는 전혀 무차별 모드로 설정할 수 없으며 Google Cloud에서 경고가 발생합니다.

제어 평면 아키텍처

Google Cloud NetApp Volumes 에 대한 모든 관리 작업은 API를 통해 수행됩니다. GCP Cloud Console에 통합된 Google Cloud NetApp Volumes 관리도 Google Cloud NetApp Volumes API를 사용합니다.

ID 및 액세스 관리

ID 및 액세스 관리("그래요")은 Google Cloud 프로젝트 인스턴스에 대한 인증(로그인) 및 권한 부여(사용 권한)를 제어할 수 있는 표준 서비스입니다. Google IAM은 권한 부여 및 해제에 대한 전체 감사 추적을 제공합니다. 현재 Google Cloud NetApp Volumes 제어 평면 감사를 제공하지 않습니다.

권한/허가 개요

IAM은 Google Cloud NetApp Volumes에 대한 세분화된 기본 권한을 제공합니다. 다음을 확인할 수 있습니다 "여기에서 세부적인 권한의 전체 목록을 확인하세요.".

IAM은 또한 다음과 같은 두 가지 미리 정의된 역할을 제공합니다. `netappcloudvolumes.admin` 그리고 `netappcloudvolumes.viewer` . 이러한 역할은 특정 사용자나 서비스 계정에 할당될 수 있습니다.

IAM 사용자가 Google Cloud NetApp Volumes 관리할 수 있도록 적절한 역할과 권한을 할당합니다.

세분화된 권한을 사용하는 예는 다음과 같습니다.

- 사용자가 볼륨을 삭제할 수 없도록 get/list/create/update 권한만 있는 사용자 지정 역할을 빌드합니다.
- 사용자 정의 역할만 사용하세요. `snapshot.*` 애플리케이션과 일관된 스냅샷 통합을 구축하는 데 사용되는 서비스 계정을 생성할 수 있는 권한입니다.
- 위임할 사용자 정의 역할 작성 `volumereplication.*` 특정 사용자에게.

서비스 계정

스크립트를 통해 Google Cloud NetApp Volumes API 호출을 수행하려면 "테라폼" , 서비스 계정을 생성해야 합니다. `roles/netappcloudvolumes.admin` 역할. 이 서비스 계정을 사용하면 두 가지 방법으로 Google Cloud NetApp Volumes API 요청을 인증하는 데 필요한 JWT 토큰을 생성할 수 있습니다.

- JSON 키를 생성하고 Google API를 사용하여 이를 통해 JWT 토큰을 파생합니다. 가장 간단한 방법이지만, 수동으로 비밀(JSON 키)을 관리해야 합니다.
- 사용 "서비스 계정 사칭" ~와 함께 `roles/iam.serviceAccountTokenCreator` . 코드(스크립트, Terraform 등)는 다음과 같이 실행됩니다. "애플리케이션 기본 자격 증명" 서비스 계정을 가장하여 권한을 얻습니다. 이러한 접근 방식은 Google의 보안 모범 사례를 반영합니다.

자세한 내용은 Google 클라우드 문서에서 "서비스 계정 및 개인 키 생성"을(를) 참조하십시오.

Google Cloud NetApp Volumes API

Google Cloud NetApp Volumes API는 HTTPS(TLSv1.2)를 기본 네트워크 전송으로 사용하여 REST 기반 API를 사용합니다. 최신 API 정의 및 API 사용 방법에 대한 정보는 "Google 클라우드 문서의 Cloud Volumes API"에서 확인할 수 있습니다.

API 엔드포인트는 NetApp 에서 표준 HTTPS(TLSv1.2) 기능을 사용하여 운영 및 보안됩니다.

JWT 토큰

API에 대한 인증은 JWT 베어러 토큰을 사용하여 수행됩니다.("RFC-7519"). 유효한 JWT 토큰은 Google Cloud IAM 인증을 사용하여 얻어야 합니다. 이 작업은 서비스 계정 JSON 키를 제공하여 IAM에서 토큰을 가져와서 수행해야 합니다.

감사 로깅

현재 사용자가 접근할 수 있는 제어 평면 감사 로그가 없습니다.

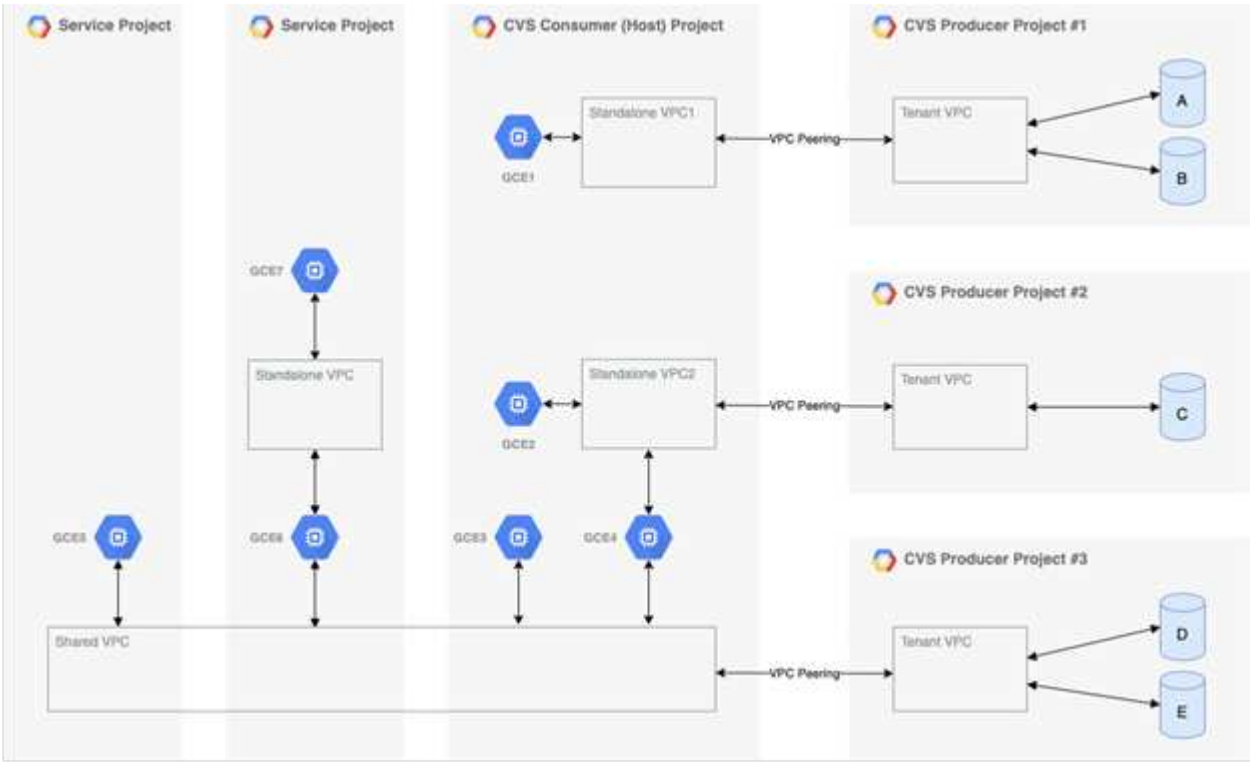
데이터 플레인 아키텍처

Google Cloud NetApp Volumes Google Cloud를 활용합니다. "개인 서비스 접근" 뼈대. 이 프레임워크에서 사용자는 Google Cloud NetApp Volumes 에 연결할 수 있습니다. 이 프레임워크는 다른 Google Cloud 서비스와 마찬가지로 서비스 네트워킹 및 VPC 피어링 구조를 사용하여 테넌트 간의 완전한 격리를 보장합니다.

Google Cloud용 Google Cloud NetApp Volumes의 아키텍처 개요는 다음을 참조하십시오 "Google Cloud NetApp Volumes 아키텍처".

사용자 VPC(독립형 또는 공유)는 볼륨을 호스팅하는 Google Cloud NetApp Volumes 관리 테넌트 프로젝트 내의

VPC에 피어링됩니다.



위 그림은 세 개의 VPC 네트워크가 Google Cloud NetApp Volumes 에 연결되고 여러 Compute Engine VM(GCE1-7)이 볼륨을 공유하는 프로젝트(가운데에 있는 NetApp Volumes 소비자 프로젝트)를 보여줍니다.

- VPC1을 통해 GCE1은 볼륨 A와 B에 액세스할 수 있습니다.
- VPC2를 사용하면 GCE2와 GCE4가 볼륨 C에 액세스할 수 있습니다.
- 세 번째 VPC 네트워크는 두 개의 서비스 프로젝트와 공유되는 공유 VPC입니다. 이를 통해 GCE3, GCE4, GCE5, GCE6이 볼륨 D와 E에 액세스할 수 있습니다. 공유 VPC 네트워크는 NetApp Volumes-Performance 서비스 유형의 볼륨에서만 지원됩니다.

GCE7은 어떤 볼륨에도 액세스할 수 없습니다.

데이터는 전송 중(Kerberos 및/또는 SMB 암호화 사용)과 Google Cloud NetApp Volumes 에 저장된 상태 모두에서 암호화될 수 있습니다.

전송 중 데이터 암호화

전송 중인 데이터는 NAS 프로토콜 계층에서 암호화될 수 있으며, Google Cloud 네트워크 자체도 다음 섹션에서 설명하는 대로 암호화됩니다.

구글 클라우드 네트워크

Google Cloud는 네트워크 수준에서 트래픽을 암호화합니다. "전송 중 암호화" Google 문서에서. "Google Cloud NetApp Volumes 아키텍처" 섹션에서 언급한 대로, Google Cloud NetApp Volumes NetApp 제어하는 PSA 제작자 프로젝트에서 제공됩니다.

NetApp Volumes-SW의 경우, 프로듀서 테넌트는 Google VM을 실행하여 서비스를 제공합니다. 사용자 VM과

Google Cloud NetApp Volumes VM 간의 트래픽은 Google에서 자동으로 암호화됩니다.

NetApp Volumes-Performance의 데이터 경로는 네트워크 계층에서 완전히 암호화되지 않았지만 NetApp 과 Google은 다음과 같은 조합을 사용합니다. "IEEE 802.1AE 암호화(MACSec)" , "캡슐화" (데이터 암호화) 및 물리적으로 제한된 네트워크를 통해 Google Cloud NetApp Volumes NetApp Volumes-Performance 서비스 유형과 Google Cloud 간에 전송되는 데이터를 보호합니다.

NAS 프로토콜

NFS 및 SMB NAS 프로토콜은 프로토콜 계층에서 선택적 전송 암호화를 제공합니다.

SMB 암호화

"SMB 암호화"SMB 데이터의 종단 간 암호화를 제공하고 신뢰할 수 없는 네트워크에서 발생하는 도청으로부터 데이터를 보호합니다. 클라이언트/서버 데이터 연결(SMB3.x 지원 클라이언트에서만 사용 가능)과 서버/도메인 컨트롤러 인증 모두에 대해 암호화를 활성화할 수 있습니다.

SMB 암호화가 활성화된 경우 암호화를 지원하지 않는 클라이언트는 공유에 액세스할 수 없습니다.

Google Cloud NetApp Volumes SMB 암호화를 위해 RC4-HMAC, AES-128-CTS-HMAC-SHA1 및 AES-256-CTS-HMAC-SHA1 보안 암호를 지원합니다. SMB는 서버에서 지원하는 가장 높은 암호화 유형으로 협상합니다.

NFSv4.1 케르베로스

NFSv4.1의 경우 NetApp Volumes-Performance는 다음에 설명된 대로 Kerberos 인증을 제공합니다. "RFC7530" 볼륨별로 Kerberos를 활성화할 수 있습니다.

현재 Kerberos에 사용할 수 있는 가장 강력한 암호화 유형은 AES-256-CTS-HMAC-SHA1입니다. Google Cloud NetApp Volumes AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3 및 NFS용 DES를 지원합니다. 또한 CIFS/SMB 트래픽의 경우 ARCFOUR-HMAC(RC4)를 지원하지만 NFS의 경우 지원하지 않습니다.

Kerberos는 NFS 마운트에 대해 세 가지 보안 수준을 제공하며, 이를 통해 Kerberos 보안의 강도를 선택할 수 있습니다.

RedHat의 경우 "일반적인 마운트 옵션" 선적 서류 비치:

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

일반적으로 Kerberos 보안 수준이 높아질수록 클라이언트와 서버가 전송하는 각 패킷에 대한 NFS 작업을 암호화하고 암호 해독하는 데 시간을 소비하므로 성능이 저하됩니다. 많은 클라이언트와 NFS 서버는 더 나은 전반적인 경험을 위해 CPU에 AES-NI 오프로드를 지원하지만, Kerberos 5p(전체 엔드투엔드 암호화)가 성능에 미치는 영향은 Kerberos 5(사용자 인증)가 미치는 영향보다 훨씬 큽니다.

다음 표는 각 수준이 보안과 성능에 미치는 영향의 차이점을 보여줍니다.

보안 수준	보안	성능
NFSv3—시스템	• 보안성이 가장 낮음; 숫자 사용자 ID/그룹 ID가 포함된 일반 텍스트 • 패킷 캡처에서 UID, GID, 클라이언트 IP 주소, 내보내기 경로, 파일 이름, 권한을 볼 수 있습니다.	• 대부분의 경우에 가장 좋습니다
NFSv4.x—시스템	• NFSv3보다 보안성이 더 높음(클라이언트 ID, 이름 문자열/도메인 문자열 일치) 그러나 여전히 일반 텍스트 • 패킷 캡처에서 UID, GID, 클라이언트 IP 주소, 이름 문자열, 도메인 ID, 내보내기 경로, 파일 이름, 권한을 볼 수 있습니다.	• 순차적 작업(예: VM, 데이터베이스, 대용량 파일)에 적합합니다. • 파일 수가 많고 메타데이터가 많으면 나쁩니다(30-50% 더 나쁨)
NFS—krb5	• 모든 NFS 패킷의 자격 증명에 대한 Kerberos 암호화 - GSS 래퍼의 RPC 호출에서 사용자/그룹의 UID/GID를 래핑합니다. • 마운트에 대한 액세스를 요청하는 사용자는 유효한 Kerberos 티켓(사용자 이름/암호 또는 수동 키 탭 교환을 통해)이 필요합니다. 티켓은 지정된 기간 후에 만료되며 사용자는 액세스를 위해 다시 인증해야 합니다. • NFS 작업이나 mount/portmapper/nlm과 같은 보조 프로토콜에 대한 암호화 없음(패킷 캡처에서 내보내기 경로, IP 주소, 파일 핸들, 권한, 파일 이름, atime/mtime을 볼 수 있음)	• 대부분의 경우 Kerberos에 가장 좋지만 AUTH_SYS보다 나쁩니다.

보안 수준	보안	성능
NFS—krb5i	• 모든 NFS 패킷의 자격 증명에 대한 Kerberos 암호화 - GSS 래퍼의 RPC 호출에서 사용자 /그룹의 UID/GID를 래핑합니다. • 마운트에 대한 액세스를 요청하는 사용자는 유효한 Kerberos 티켓(사용자 이름/암호 또는 수동 키 탭 교환을 통해)이 필요합니다. 티켓은 지정된 기간 후에 만료되며 사용자는 액세스를 위해 다시 인증해야 합니다. • NFS 작업이나 mount/portmapper/nlm과 같은 보조 프로토콜에 대한 암호화 없음(패킷 캡처에서 내보내기 경로, IP 주소, 파일 핸들, 권한, 파일 이름, atime/mtime을 볼 수 있음) • 모든 패킷에 Kerberos GSS 체크섬을 추가하여 아무것도 패킷을 가로채지 못하도록 보장합니다. 체크섬이 일치하면 대화가 허용됩니다.	• NFS 페이로드가 암호화되지 않기 때문에 krb5p보다 낫습니다. krb5에 비해 추가된 오버헤드는 무결성 검사합계뿐입니다. krb5i의 성능은 krb5보다 크게 나쁘지는 않지만 약간 저하될 것입니다.
NFS – krb5p	• 모든 NFS 패킷의 자격 증명에 대한 Kerberos 암호화 - GSS 래퍼의 RPC 호출에서 사용자 /그룹의 UID/GID를 래핑합니다. • 마운트에 대한 액세스를 요청하는 사용자는 유효한 Kerberos 티켓(사용자 이름/암호 또는 수동 키탭 교환을 통해)이 필요합니다. 티켓은 지정된 기간이 지나면 만료되며 사용자는 액세스를 위해 다시 인증해야 합니다. • 모든 NFS 패킷 페이로드는 GSS 래퍼로 암호화됩니다(패킷 캡처에서 파일 핸들, 권한, 파일 이름, atime/mtime을 볼 수 없음). • 무결성 검사가 포함되어 있습니다. • NFS 작업 유형이 표시됩니다(FSINFO, ACCESS, GETATTR 등). • 보조 프로토콜(마운트, 포트맵, nlm 등)은 암호화되지 않습니다. (내보내기 경로, IP 주소를 볼 수 있음)	• 보안 수준의 성능이 최악입니다. krb5p는 더 많은 암호화/복호화를 수행해야 합니다. • 파일 수가 많은 작업 부하의 경우 NFSv4.x를 사용하는 krb5p보다 성능이 더 뛰어납니다.

Google Cloud NetApp Volumes 에서는 구성된 Active Directory 서버가 Kerberos 서버 및 LDAP 서버로 사용됩니다(RFC2307 호환 스키마에서 사용자 ID를 조회하기 위해). 다른 Kerberos 또는 LDAP 서버는 지원되지 않습니다. NetApp Google Cloud NetApp Volumes 에서 ID 관리를 위해 LDAP를 사용할 것을 적극 권장합니다. 패킷 캡처에서 NFS Kerberos가 어떻게 표시되는지에 대한 자세한 내용은 섹션 "Packet sniffing/trace considerations."를 참조하세요.

저장 중 데이터 암호화

Google Cloud NetApp Volumes 의 모든 볼륨은 AES-256 암호화를 사용하여 저장 상태에서 암호화됩니다. 즉, 미디어에 기록된 모든 사용자 데이터는 암호화되며 볼륨별 키로만 암호를 해독할 수 있습니다.

- NetApp Volumes-SW의 경우 Google에서 생성한 키가 사용됩니다.
- NetApp Volumes-Performance의 경우 볼륨별 키는 Google Cloud NetApp Volumes 에 내장된 키 관리자에 저장됩니다.

2021년 11월부터 고객 관리 암호화 키(CMEK) 기능 미리보기가 제공되었습니다. 이를 통해 볼륨별 키를 호스팅되는 프로젝트별, 지역별 마스터 키로 암호화할 수 있습니다. "Google 키 관리 서비스(KMS)." KMS를 사용하면 외부 키 관리자를 연결할 수 있습니다.

NetApp Volumes-Performance용 KMS 구성에 대한 자세한 내용은 "고객 관리 암호화 키 설정"을(를) 참조하십시오.

방화벽

Google Cloud NetApp Volumes NFS 및 SMB 공유를 제공하기 위해 여러 TCP 포트를 노출합니다.

- "NFS 액세스에 필요한 포트"
- "SMB 접속에 필요한 포트"

또한 SMB, Kerberos를 포함한 LDAP를 사용하는 NFS 및 이중 프로토콜 구성에는 Windows Active Directory 도메인에 대한 액세스가 필요합니다. Active Directory 연결은 "구성됨"지역별로 설정해야 합니다. Active Directory 도메인 컨트롤러(DC)는 "DNS 기반 DC 검색"지정된 DNS 서버를 사용하여 식별됩니다. 반환된 DC 중 하나가 사용됩니다. Active Directory 사이트를 지정하여 사용 가능한 DC 목록을 제한할 수 있습니다.

Google Cloud NetApp Volumes는 "Google Cloud NetApp Volumes 온보딩" 동안 `gcloud compute address` 명령으로 할당된 CIDR 범위의 IP 주소를 사용하여 연결합니다. 이 CIDR을 소스 주소로 사용하여 Active Directory 도메인 컨트롤러에 대한 인바운드 방화벽을 구성할 수 있습니다.

Active Directory 도메인 컨트롤러는 다음 조건을 충족해야 합니다 "여기에 언급된 대로 Google Cloud NetApp Volumes CIDR에 포트를 노출합니다.".

NAS 프로토콜 개요

NAS 프로토콜에는 NFS(v3 및 v4.1)와 SMB/CIFS(2.x 및 3.x)가 포함됩니다. 이러한 프로토콜을 통해 NetApp Volumes는 여러 NAS 클라이언트에서 데이터에 대한 공유 액세스를 허용합니다. 또한 Google Cloud NetApp Volumes NAS 공유에 있는 파일과 폴더에 대한 모든 ID 및 권한 설정을 존중하면서 NFS 및 SMB/CIFS 클라이언트에 대한 액세스를 동시에(듀얼 프로토콜) 제공할 수 있습니다. 가능한 가장 높은 수준의 데이터 전송 보안을 유지하기 위해

Google Cloud NetApp Volumes SMB 암호화 및 NFS Kerberos 5p를 사용하여 전송 중 프로토콜 암호화를 지원합니다.

듀얼 프로토콜은 NetApp Volumes-Performance에서만 사용할 수 있습니다.

NAS 프로토콜의 기본

NAS 프로토콜은 네트워크의 여러 클라이언트가 GCP의 Google Cloud NetApp Volumes 와 같은 스토리지 시스템의 동일한 데이터에 액세스할 수 있는 방법입니다. NFS와 SMB는 정의된 NAS 프로토콜이며 클라이언트/서버 기반으로 작동하는 반면 Google Cloud NetApp Volumes 서버 역할을 합니다. 클라이언트는 서버에 액세스, 읽기, 쓰기 요청을 보내고, 서버는 파일 잠금 메커니즘을 조정하고, 권한을 저장하고, ID 및 인증 요청을 처리하는 역할을 합니다.

예를 들어, NAS 클라이언트가 폴더에 새 파일을 만들려면 다음과 같은 일반적인 프로세스를 따릅니다.

1. 클라이언트는 서버에 디렉토리에 대한 정보(권한, 소유자, 그룹, 파일 ID, 사용 가능한 공간 등)를 요청합니다. 서버는 요청한 클라이언트와 사용자가 상위 폴더에 대한 필요한 권한을 가지고 있는 경우 해당 정보를 응답합니다.
2. 디렉토리에 대한 권한이 액세스를 허용하는 경우, 클라이언트는 서버에 생성하려는 파일 이름이 파일 시스템에 이미 있는지 묻습니다. 파일 이름이 이미 사용 중이면 생성이 실패합니다. 파일 이름이 존재하지 않으면 서버는 클라이언트에게 계속 진행할 수 있음을 알립니다.
3. 클라이언트는 서버에 호출을 보내 디렉토리 핸들과 파일 이름으로 파일을 생성하고 액세스 및 수정 시간을 설정합니다. 서버는 다른 파일이 동일한 파일 ID로 생성되지 않도록 파일에 고유한 파일 ID를 발급합니다.
4. 클라이언트는 WRITE 작업 전에 파일 속성을 확인하기 위해 호출을 보냅니다. 권한이 허락한다면 클라이언트는 새 파일을 작성합니다. 프로토콜/애플리케이션에서 잠금을 사용하는 경우, 클라이언트는 서버에 잠금을 요청하여 다른 클라이언트가 잠긴 파일에 액세스하는 것을 방지하고 데이터 손상을 방지합니다.

NFS

NFS는 RFC(Request for Comments)에 정의된 개방형 IETF 표준인 분산 파일 시스템 프로토콜로, 누구나 프로토콜을 구현할 수 있도록 해줍니다.

Google Cloud NetApp Volumes 은 클라이언트 또는 클라이언트 세트에서 액세스할 수 있는 경로를 내보내어 NFS 클라이언트와 공유됩니다. 이러한 내보내기를 마운트하기 위한 권한은 Google Cloud NetApp Volumes 관리자가 구성할 수 있는 내보내기 정책 및 규칙에 의해 정의됩니다.

NetApp NFS 구현은 프로토콜에 대한 황금 표준으로 간주되며 수많은 기업 NAS 환경에서 사용됩니다. 다음 섹션에서는 NFS와 Google Cloud NetApp Volumes 에서 사용할 수 있는 특정 보안 기능과 이러한 기능이 구현되는 방법에 대해 설명합니다.

기본 로컬 UNIX 사용자 및 그룹

Google Cloud NetApp Volumes 다양한 기본 기능을 위한 여러 개의 기본 UNIX 사용자와 그룹이 포함되어 있습니다. 현재 이러한 사용자와 그룹은 수정하거나 삭제할 수 없습니다. 현재 Google Cloud NetApp Volumes 에 새로운 로컬 사용자와 그룹을 추가할 수 없습니다. 기본 사용자 및 그룹 이외의 UNIX 사용자 및 그룹은 외부 LDAP 이름 서비스를 통해 제공되어야 합니다.

다음 표는 기본 사용자 및 그룹과 해당 숫자 ID를 보여줍니다. NetApp 에서는 LDAP나 로컬 클라이언트에서 숫자 ID를 재사용하는 새로운 사용자나 그룹을 만들지 않는 것을 권장합니다.

기본 사용자: 숫자 ID	기본 그룹: 숫자 ID
• 루트:0 • pcuser:65534 • 아무도:65535	• 루트:0 • 데몬:1 • pcuser:65534 • 아무도:65535

NFSv4.1을 사용하는 경우 NFS 클라이언트에서 디렉토리 나열 명령을 실행하면 루트 사용자가 nobody로 표시될 수 있습니다. 이는 클라이언트의 ID 도메인 매핑 구성으로 인해 발생합니다. 라는 섹션을 참조하세요.NFSv4.1 및 nobody 사용자/그룹 이 문제에 대한 자세한 내용과 해결 방법은 다음을 참조하세요.

루트 사용자

Linux에서 루트 계정은 Linux 기반 파일 시스템의 모든 명령, 파일, 폴더에 액세스할 수 있습니다. 이 계정의 강력한 기능 때문에 보안 모범 사례에서는 종종 루트 사용자를 비활성화하거나 어떤 방식으로든 제한해야 합니다. NFS 내보내기에서 루트 사용자가 파일과 폴더에 대해 가지는 권한은 내보내기 정책 및 규칙과 루트 스쿼시라는 개념을 통해 Google Cloud NetApp Volumes 에서 제어할 수 있습니다.

루트 스쿼싱은 NFS 마운트에 액세스하는 루트 사용자가 익명 숫자 사용자 65534로 스쿼싱되도록 보장합니다(섹션 참조)익명의 사용자 ")이며 현재는 내보내기 정책 규칙 생성 중에 루트 액세스에 대해 끄기를 선택하여 NetApp Volumes-Performance를 사용하는 경우에만 사용할 수 있습니다. 루트 사용자가 익명 사용자로 압축되면 더 이상 chown을 실행할 수 있는 권한이 없습니다. "setuid/setgid 명령(스티키 비트)" NFS 마운트의 파일이나 폴더, 그리고 루트 사용자가 생성한 파일이나 폴더의 소유자/그룹으로 익명 UID가 표시됩니다. 또한 NFSv4 ACL은 루트 사용자가 수정할 수 없습니다. 하지만 루트 사용자는 여전히 chmod에 접근할 수 있으며 명시적인 권한이 없는 파일을 삭제할 수도 있습니다. 루트 사용자의 파일 및 폴더 권한에 대한 액세스를 제한하려면 NTFS ACL이 있는 볼륨을 사용하고 이름이 지정된 Windows 사용자를 만드는 것을 고려하십시오. `root` , 원하는 권한을 파일이나 폴더에 적용합니다.

익명의 사용자

익명(anon) 사용자 ID는 유효한 NFS 자격 증명 없이 도착한 클라이언트 요청에 매핑되는 UNIX 사용자 ID 또는 사용자 이름을 지정합니다. 루트 스쿼싱이 사용되는 경우 루트 사용자가 포함될 수 있습니다. Google Cloud NetApp Volumes 의 익명 사용자는 65534입니다.

이 UID는 일반적으로 사용자 이름과 연결됩니다. `nobody` 또는 `nfsnobody` Linux 환경에서. Google Cloud NetApp Volumes 또한 로컬 UNIX 사용자 `pcuser`로 65534를 사용합니다(섹션 참조)기본 로컬 UNIX 사용자 및 그룹 "), LDAP에서 유효한 일치하는 UNIX 사용자를 찾을 수 없을 때 Windows에서 UNIX 이름 매핑을 위한 기본 대체 사용자이기도 합니다.

UID 65534에 대한 Linux 및 Google Cloud NetApp Volumes 사용자 이름이 다르기 때문에 NFSv4.1을 사용할 때 65534에 매핑된 사용자의 이름 문자열이 일치하지 않을 수 있습니다. 결과적으로, 당신은 볼 수 있습니다 `nobody` 일부 파일과 폴더에 대한 사용자 권한. "섹션을 참조하세요.NFSv4.1 및 nobody 사용자/그룹 " 이 문제와 해결 방법에 대한 정보는 여기를 참조하세요.

접근 제어/수출

NFS 마운트에 대한 초기 내보내기/공유 액세스는 내보내기 정책에 포함된 호스트 기반 내보내기 정책 규칙을 통해 제어됩니다. NFS 공유를 마운트하기 위한 액세스와 호스트에 허용되는 액세스 수준을 허용하기 위해 호스트 IP, 호스트 이름, 서브넷, 넷그룹 또는 도메인이 정의됩니다. 내보내기 정책 규칙 구성 옵션은 Google Cloud NetApp Volumes 수준에 따라 달라집니다.

NetApp Volumes-SW의 경우 다음 옵션을 사용하여 내보내기 정책 구성을 수행할 수 있습니다.

- 클라이언트 매칭**.** IP 주소를 쉼표로 구분한 목록, 호스트 이름, 서브넷, 넷그룹, 도메인 이름을 쉼표로 구분한 목록입니다.
- **RO/RW** 접근 규칙**.** 내보내기에 대한 액세스 수준을 제어하려면 읽기/쓰기 또는 읽기 전용을 선택하세요. NetApp Volumes-Performance는 다음과 같은 옵션을 제공합니다.
- 클라이언트 매칭**.** IP 주소를 쉼표로 구분한 목록, 호스트 이름, 서브넷, 넷그룹, 도메인 이름을 쉼표로 구분한 목록입니다.
- **RO/RW** 접근 규칙**.** 내보내기에 대한 액세스 수준을 제어하려면 읽기/쓰기 또는 읽기 전용을 선택하세요.
- 루트 접근**(**켜기**/**끄기**).** 루트 스쿼시를 구성합니다(섹션 참조)루트 사용자 (자세한 내용은 "을 참조하세요).
- 프로토콜 유형**.** 이렇게 하면 NFS 마운트에 대한 액세스가 특정 프로토콜 버전으로 제한됩니다. 볼륨에 대해 NFSv3와 NFSv4.1을 모두 지정하는 경우 둘 다 비워두거나 두 상자를 모두 선택하세요.
- **Kerberos** 보안 수준**(Kerberos** 사용이 선택된 경우**).** 읽기 전용 또는 읽기-쓰기 액세스를 위한 krb5, krb5i 및/또는 krb5p 옵션을 제공합니다.

소유권 변경**(chown)** 및 그룹 변경**(chgrp)**

Google Cloud NetApp Volumes 의 NFS에서는 루트 사용자만 파일 및 폴더에서 chown/chgrp를 실행할 수 있습니다. 다른 사용자는 다음을 봅니다. `Operation not permitted` 오류가 발생합니다. 자신이 소유한 파일에도 오류가 발생합니다. 뿌리 호박을 사용하는 경우(섹션 "루트 사용자 "), 루트는 루트가 아닌 사용자에게 압류되고 chown 및 chgrp에 액세스할 수 없습니다. 현재 Google Cloud NetApp Volumes 에는 루트가 아닌 사용자에게 chown 및 chgrp를 허용하는 해결 방법이 없습니다. 소유권 변경이 필요한 경우 이중 프로토콜 볼륨을 사용하고 보안 스타일을 NTFS로 설정하여 Windows 측에서 권한을 제어하는 것을 고려하세요.

권한 관리

Google Cloud NetApp Volumes UNIX 보안 스타일을 사용하는 볼륨에 대한 NFS 클라이언트의 권한을 제어하기 위해 두 가지 모드 비트(rwx의 경우 644, 777 등)와 NFSv4.1 ACL을 모두 지원합니다. 이러한 권한 관리에는 표준 권한 관리(예: chmod, chown 또는 nfs4_setfacl)가 사용되며 이를 지원하는 모든 Linux 클라이언트에서 작동합니다.

또한 NTFS로 설정된 이중 프로토콜 볼륨을 사용하는 경우 NFS 클라이언트는 Windows 사용자에 대한 Google Cloud NetApp Volumes 이름 매핑을 활용할 수 있으며, 이는 NTFS 권한을 확인하는 데 사용됩니다. Google Cloud NetApp Volumes 에서 숫자 ID를 사용자 이름으로 변환하려면 LDAP 연결이 필요합니다. Google Cloud NetApp Volumes 유효한 UNIX 사용자 이름을 Windows 사용자 이름에 올바르게 매핑해야 하기 때문입니다.

NFSv3에 대한 세분화된 **ACL** 제공

모드 비트 권한은 의미론상 소유자, 그룹 및 기타 모든 사람에게만 적용됩니다. 즉, 기본 NFSv3에 대한 세부적인 사용자 액세스 제어가 없습니다. Google Cloud NetApp Volumes POSIX ACL이나 확장된 속성(예: chattr)을 지원하지 않으므로 세분화된 ACL은 NFSv3를 사용하는 다음 시나리오에서만 가능합니다.

- 유효한 UNIX-Windows 사용자 매핑이 포함된 NTFS 보안 스타일 볼륨(CIFS 서버 필요).
- NFSv4.1 ACL은 ACL을 적용하기 위해 NFSv4.1을 마운트한 관리자 클라이언트를 사용하여 적용됩니다.

두 방법 모두 UNIX ID 관리를 위한 LDAP 연결과 유효한 UNIX 사용자 및 그룹 정보가 채워져야 합니다(섹션 참조)."LDAP")이며 NetApp Volumes-Performance 인스턴스에서만 사용할 수 있습니다. NFS와 함께 NTFS 보안 스타일 볼륨을 사용하려면 SMB 연결이 설정되지 않은 경우에도 이중 프로토콜(SMB 및 NFSv3) 또는 이중 프로토콜(SMB 및 NFSv4.1)을 사용해야 합니다. NFSv3 마운트와 함께 NFSv4.1 ACL을 사용하려면 다음을 선택해야 합니다. `Both (NFSv3/NFSv4.1)` 프로토콜 유형으로.

일반 UNIX 모드 비트는 NTFS 또는 NFSv4.x ACL이 제공하는 것과 동일한 수준의 권한 세분성을 제공하지 않습니다. 다음 표는 NFSv3 모드 비트와 NFSv4.1 ACL 간의 권한 세분성을 비교합니다. NFSv4.1 ACL에 대한 정보는 다음을 참조하세요. "nfs4_acl - NFSv4 액세스 제어 목록" .

NFSv3 모드 비트	**NFSv4.1 ACL**
• 실행 시 사용자 ID 설정 • 실행 시 그룹 ID 설정 • 교체된 텍스트 저장(POSIX에 정의되지 않음) • 소유자에 대한 읽기 권한 • 소유자에 대한 쓰기 권한 • 파일에 대한 소유자의 실행 권한 또는 디렉토리에서 소유자의 권한 조회(검색) • 그룹에 대한 읽기 권한 • 그룹에 대한 쓰기 권한 • 파일에 대한 그룹의 실행 권한 또는 디렉토리에서 그룹의 권한 조회(검색) • 다른 사람을 위한 읽기 권한 • 다른 사람에게 쓰기 권한 부여 • 파일에 대한 다른 사용자의 실행 권한 또는 디렉토리에서 다른 사용자의 권한 조회(검색)	액세스 제어 항목(ACE) 유형(허용/거부/감사) * 상속 플래그 * 디렉터리 상속 * 파일 상속 * 전파 금지 상속 * 상속 전용 권한 * 읽기-데이터(파일) / 목록-디렉토리(디렉토리) * 쓰기-데이터(파일) / 파일 생성(디렉토리) * 추가-데이터(파일) / 하위 디렉토리 생성(디렉토리) * 실행(파일) / 디렉토리 변경(디렉토리) * 삭제 * 자식 삭제 * 읽기-속성 * 쓰기-속성 * 읽기-지정된-속성 * 쓰기-지정된-속성 * 읽기-ACL * 쓰기-ACL * 쓰기-소유자 * 동기화

마지막으로, NFS 그룹 멤버십(NFSv3 및 NFSV4.x 모두)은 RPC 패킷 제한에 따라 AUTH_SYS의 기본 최대값인 16으로 제한됩니다. NFS Kerberos는 최대 32개의 그룹을 제공하고 NFSv4 ACL은 세분화된 사용자 및 그룹 ACL(ACE당 최대 1024개 항목)을 통해 이러한 제한을 제거합니다.

또한 Google Cloud NetApp Volumes는 최대 지원 그룹을 32개까지 확장할 수 있는 확장된 그룹 지원을 제공합니다. 이를 위해서는 유효한 UNIX 사용자 및 그룹 ID가 포함된 LDAP 서버에 대한 LDAP 연결이 필요합니다. 이를 구성하는 방법에 대한 자세한 내용은 Google 설명서에서 "NFS 볼륨 생성 및 관리"을(를) 참조하십시오.

NFSv3 사용자 및 그룹 **ID**

NFSv3 사용자 및 그룹 ID는 이름이 아닌 숫자 ID로 전송됩니다. Google Cloud NetApp Volumes NFSv3에서 이러한 숫자 ID에 대한 사용자 이름을 확인하지 않으며, UNIX 보안 스타일 볼륨은 모드 비트만 사용합니다. NFSv4.1 ACL이 있는 경우 ACL을 제대로 확인하려면 숫자 ID 조회 및/또는 이름 문자열 조회가 필요합니다. 이는 NFSv3를 사용하는 경우에도 마찬가지입니다. NTFS 보안 스타일 볼륨을 사용하는 경우 Google Cloud NetApp Volumes 숫자 ID를 유효한 UNIX 사용자로 확인한 다음 유효한 Windows 사용자에 매핑하여 액세스 권한을 협상해야 합니다.

NFSv3 사용자 및 그룹 **ID**의 보안 제한 사항

NFSv3를 사용하면 클라이언트와 서버는 숫자 ID로 읽기 또는 쓰기를 시도하는 사용자가 유효한 사용자인지 확인할 필요가 없습니다. 그저 암묵적으로 신뢰될 뿐입니다. 숫자 ID를 스푸핑하는 것만으로도 파일 시스템이 잠재적인 침해 위험에 노출됩니다. 이러한 보안 취약점을 방지하기 위해 Google Cloud NetApp Volumes 에는 몇 가지 옵션이 있습니다.

- NFS에 Kerberos를 구현하려면 사용자가 사용자 이름과 비밀번호 또는 키탭 파일로 인증하여 마운트에 액세스할 수 있는 Kerberos 티켓을 받아야 합니다. Kerberos는 NetApp Volumes-Performance 인스턴스와 NFSv4.1에서만

사용할 수 있습니다.

- 내보내기 정책 규칙에서 호스트 목록을 제한하면 어떤 NFSv3 클라이언트가 Google Cloud NetApp Volumes 볼륨에 액세스할 수 있는지가 제한됩니다.
- 듀얼 프로토콜 볼륨을 사용하고 볼륨에 NTFS ACL을 적용하면 NFSv3 클라이언트가 숫자 ID를 유효한 UNIX 사용자 이름으로 확인하여 마운트에 액세스하기 위한 적절한 인증을 받아야 합니다. 이렇게 하려면 LDAP를 활성화하고 UNIX 사용자 및 그룹 ID를 구성해야 합니다.
- 루트 사용자를 제한하면 루트 사용자가 NFS 마운트에 입힐 수 있는 피해는 제한되지만 위험이 완전히 없어지는 것은 아닙니다. 자세한 내용은 "섹션"을 참조하세요.루트 사용자 ."

궁극적으로 NFS 보안은 사용하는 프로토콜 버전이 제공하는 것에 따라 제한됩니다. NFSv3는 전반적으로 NFSv4.1보다 성능이 뛰어나지만 동일한 수준의 보안을 제공하지는 않습니다.

NFSv4.1

NFSv4.1은 다음과 같은 이유로 NFSv3에 비해 더 높은 보안과 안정성을 제공합니다.

- 임대 기반 메커니즘을 통한 통합 잠금
- 상태 저장 세션
- 단일 포트(2049)를 통한 모든 NFS 기능
- TCP만
- ID 도메인 매핑
- Kerberos 통합(NFSv3는 Kerberos를 사용할 수 있지만 NFS에만 사용할 수 있으며 NLM과 같은 보조 프로토콜에는 사용할 수 없습니다)

NFSv4.1 종속성

NFSv4.1에는 추가 보안 기능이 있기 때문에 NFSv3를 사용하는 데 필요하지 않은 일부 외부 종속성이 있습니다 (SMB가 Active Directory와 같은 종속성을 요구하는 것과 유사).

NFSv4.1 ACL

Google Cloud NetApp Volumes NFSv4.x ACL에 대한 지원을 제공하며, 이는 다음과 같은 일반 POSIX 스타일 권한에 비해 뚜렷한 이점을 제공합니다.

- 파일 및 디렉토리에 대한 사용자 액세스를 세부적으로 제어
- 더 나은 NFS 보안
- CIFS/SMB와의 상호 운용성 향상
- AUTH_SYS 보안을 사용하여 사용자당 16개 그룹의 NFS 제한 제거
- ACL은 그룹 ID(GID) 확인의 필요성을 우회하여 GID 제한을 효과적으로 제거합니다. NFSv4.1 ACL은 Google Cloud NetApp Volumes 아닌 NFS 클라이언트에서 제어됩니다. NFSv4.1 ACL을 사용하려면 클라이언트의 소프트웨어 버전이 이를 지원하고 적절한 NFS 유틸리티가 설치되어 있는지 확인하세요.

NFSv4.1 ACL과 **SMB** 클라이언트 간 호환성

NFSv4 ACL은 Windows 파일 수준 ACL(NTFS ACL)과 다르지만 기능은 비슷합니다. 그러나 다중 프로토콜 NAS 환경에서 NFSv4.1 ACL이 있고 이중 프로토콜 액세스(동일한 데이터 세트에서 NFS와 SMB)를 사용하는 경우 SMB2.0

이상을 사용하는 클라이언트는 Windows 보안 탭에서 ACL을 보거나 관리할 수 없습니다.

NFSv4.1 ACL 작동 방식

참고로, 다음 용어가 정의되어 있습니다.

- 접근 제어 목록**(ACL).** 권한 항목 목록입니다.
- 접근 통제 항목**(ACE).** 목록에 있는 권한 항목입니다.

SETATTR 작업 중에 클라이언트가 파일에 NFSv4.1 ACL을 설정하면 Google Cloud NetApp Volumes 해당 ACL을 개체에 설정하여 기존 ACL을 대체합니다. 파일에 ACL이 없으면 파일의 모드 권한은 OWNER@, GROUP@, EVERYONE@으로부터 계산됩니다. 파일에 기존 SUID/SGID/STICKY 비트가 있는 경우 영향을 받지 않습니다.

GETATTR 작업 중에 클라이언트가 파일에 대한 NFSv4.1 ACL을 받으면 Google Cloud NetApp Volumes 해당 개체와 연결된 NFSv4.1 ACL을 읽고, ACE 목록을 구성한 다음 해당 목록을 클라이언트에 반환합니다. 파일에 NT ACL이나 모드 비트가 있는 경우, 모드 비트에서 ACL이 구성되고 클라이언트로 반환됩니다.

ACL에 DENY ACE가 있으면 액세스가 거부되고, ALLOW ACE가 있으면 액세스가 허용됩니다. 그러나 ACL에 두 ACE가 모두 없는 경우에도 액세스가 거부됩니다.

보안 설명자는 보안 ACL(SACL)과 임의 ACL(DACL)로 구성됩니다. NFSv4.1이 CIFS/SMB와 상호 운용되는 경우 DACL은 NFSv4와 CIFS에 일대일로 매핑됩니다. DACL은 ALLOW와 DENY ACE로 구성됩니다.

기본적인 경우 `chmod` NFSv4.1 ACL이 설정된 파일이나 폴더에서 실행되면 기존 사용자 및 그룹 ACL은 유지되지만 기본 OWNER@, GROUP@, EVERYONE@ ACL이 수정됩니다.

NFSv4.1 ACL을 사용하는 클라이언트는 시스템의 파일과 디렉토리에 대한 ACL을 설정하고 볼 수 있습니다. ACL이 있는 디렉토리에 새 파일이나 하위 디렉토리가 생성되면 해당 개체는 해당 태그가 지정된 ACL의 모든 ACE를 상속합니다. "상속 플래그" .

파일이나 디렉토리에 NFSv4.1 ACL이 있는 경우, 해당 ACL은 파일이나 디렉토리에 액세스하는 데 사용된 프로토콜에 관계없이 액세스를 제어하는 데 사용됩니다.

파일과 디렉토리는 부모 디렉토리의 NFSv4 ACL에서 ACE를 상속받습니다(적절한 수정이 필요할 수 있음). 단, ACE에 올바른 상속 플래그가 지정되어 있어야 합니다.

NFSv4 요청의 결과로 파일이나 디렉토리가 생성되는 경우, 결과 파일이나 디렉토리의 ACL은 파일 생성 요청에 ACL이 포함되어 있는지 아니면 표준 UNIX 파일 액세스 권한만 포함되어 있는지에 따라 달라집니다. ACL은 상위 디렉토리에 ACL이 있는지 여부에 따라 달라집니다.

- 요청에 ACL이 포함되어 있으면 해당 ACL이 사용됩니다.
- 요청에 표준 UNIX 파일 액세스 권한만 포함되어 있고 상위 디렉토리에 ACL이 없는 경우 클라이언트 파일 모드를 사용하여 표준 UNIX 파일 액세스 권한을 설정합니다.
- 요청에 표준 UNIX 파일 액세스 권한만 포함되어 있고 상위 디렉토리에 상속 불가능한 ACL이 있는 경우, 요청에 전달된 모드 비트를 기반으로 하는 기본 ACL이 새 개체에 설정됩니다.
- 요청에 표준 UNIX 파일 접근 권한만 포함되어 있지만 상위 디렉토리에 ACL이 있는 경우, 해당 ACE에 적절한 상속 플래그가 지정되어 있는 한 상위 디렉토리의 ACL에 있는 ACE가 새 파일이나 디렉토리에 상속됩니다.

ACE 권한

NFSv4.1 ACL 권한은 대문자와 소문자로 구성된 일련의 문자 값을 사용합니다(예: `rxtncy`) 접근을 제어합니다. 이러한 문자 값에 대한 자세한 내용은 다음을 참조하세요. "방법: NFSv4 ACL 사용" .

umask 및 ACL 상속을 사용한 NFSv4.1 ACL 동작

"NFSv4 ACL은 ACL 상속을 제공하는 기능을 제공합니다." . ACL 상속은 NFSv4.1 ACL이 설정된 개체 아래에 생성된 파일이나 폴더가 해당 구성에 따라 ACL을 상속할 수 있음을 의미합니다. "ACL 상속 플래그" .

"우마스크"관리자 상호 작용 없이 디렉토리에 파일과 폴더가 생성되는 권한 수준을 제어하는 데 사용됩니다. 기본적으로 Google Cloud NetApp Volumes umask가 상속된 ACL을 재정의할 수 있도록 허용합니다. 이는 예상되는 동작입니다. "RFC 5661" .

ACL 포맷팅

NFSv4.1 ACL에는 특정 형식이 있습니다. 다음 예는 파일에 설정된 ACE입니다.

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

위의 예는 다음의 ACL 형식 지침을 따릅니다.

```
type:flags:principal:permissions
```

의 유형 `A` 허용하다라는 뜻입니다. 이 경우에는 주체가 그룹이 아니고 상속을 포함하지 않기 때문에 상속 플래그가 설정되지 않습니다. 또한 ACE는 AUDIT 항목이 아니므로 감사 플래그를 설정할 필요가 없습니다. NFSv4.1 ACL에 대한 자세한 내용은 다음을 참조하세요. "http://linux.die.net/man/5/nfs4_acl" .

NFSv4.1 ACL이 제대로 설정되지 않은 경우(또는 클라이언트와 서버에서 이름 문자열을 확인할 수 없는 경우) ACL이 예상대로 작동하지 않거나 ACL 변경 사항이 적용되지 않고 오류가 발생할 수 있습니다.

오류의 예는 다음과 같습니다.

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

명시적 거부

NFSv4.1 권한에는 OWNER, GROUP, EVERYONE에 대한 명시적 DENY 속성이 포함될 수 있습니다. 그 이유는 NFSv4.1 ACL이 기본적으로 거부되기 때문입니다. 즉, ACE에서 ACL을 명시적으로 허가하지 않으면 거부됩니다. 명시적 DENY 속성은 명시적이든 아니든 모든 ACCESS ACE보다 우선합니다.

DENY ACE는 속성 태그로 설정됩니다. `D` .

아래 예에서 GROUP@은 모든 읽기 및 실행 권한이 허용되지만 모든 쓰기 액세스 권한은 거부됩니다.

```
sh-4.1$ nfs4_getfacl /mixed
```

```
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

가능하면 DENY ACE는 피해야 합니다. 혼란스럽고 복잡할 수 있기 때문입니다. 명시적으로 정의되지 않은 ALLOW ACL은 암묵적으로 거부됩니다. DENY ACE가 설정된 경우, 사용자는 액세스 권한이 부여되어야 할 때 액세스가 거부될 수 있습니다.

이전 ACE 세트는 모드 비트에서 755와 동일하며 다음을 의미합니다.

- 소유자는 모든 권리를 갖습니다.
- 그룹은 읽기 전용입니다.
- 다른 사람들은 읽기만 했습니다.

그러나 권한을 775와 동일하게 조정하더라도 EVERYONE에 대한 명시적인 DENY 설정으로 인해 액세스가 거부될 수 있습니다.

NFSv4.1 ID 도메인 매핑 종속성

NFSv4.1은 ID 도메인 매핑 논리를 보안 계층으로 활용하여 NFSv4.1 마운트에 액세스하려는 사용자가 주장한 사람인지 확인하는 데 도움을 줍니다. 이러한 경우 NFSv4.1 클라이언트에서 제공되는 사용자 이름과 그룹 이름은 이름 문자열을 추가하여 Google Cloud NetApp Volumes 인스턴스로 전송됩니다. 해당 사용자 이름/그룹 이름과 ID 문자열 조합이 일치하지 않으면 사용자 및/또는 그룹은 지정된 기본 nobody 사용자로 압축됩니다. `/etc/idmapd.conf` 클라이언트의 파일.

이 ID 문자열은 적절한 권한 준수를 위해 필요하며, 특히 NFSv4.1 ACL 및/또는 Kerberos를 사용하는 경우에 필요합니다. 따라서 클라이언트와 Google Cloud NetApp Volumes 간의 일관성을 보장하고 적절한 사용자 및 그룹 이름 ID 확인을 위해 LDAP 서버와 같은 이름 서비스 서버 종속성이 필요합니다.

Google Cloud NetApp Volumes 정적 기본 ID 도메인 이름 값을 사용합니다. `defaultv4iddomain.com` . NFS 클라이언트는 ID 도메인 이름 설정에 대해 기본적으로 DNS 도메인 이름을 사용하지만 수동으로 ID 도메인 이름을 조정할 수 있습니다. `/etc/idmapd.conf` .

Google Cloud NetApp Volumes 에서 LDAP가 활성화된 경우, Google Cloud NetApp Volumes NFS ID 도메인을 DNS의 검색 도메인에 구성된 내용으로 자동으로 변경하며, 다른 DNS 도메인 검색 이름을 사용하지 않는 한 클라이언트는 수정할 필요가 없습니다.

Google Cloud NetApp Volumes 로컬 파일이나 LDAP에서 사용자 이름이나 그룹 이름을 확인할 수 있는 경우, 도메인 문자열이 사용되고 일치하지 않는 도메인 ID는 none으로 처리됩니다. Google Cloud NetApp Volumes 로컬 파일이나 LDAP에서 사용자 이름이나 그룹 이름을 찾을 수 없는 경우 숫자 ID 값이 사용되고 NFS 클라이언트가 이름을 올바르게 확인합니다(이는 NFSv3 동작과 유사함).

Google Cloud NetApp Volumes 볼륨이 사용하는 것과 일치하도록 클라이언트의 NFSv4.1 ID 도메인을 변경하지 않으면 다음과 같은 동작이 나타납니다.

- Google Cloud NetApp Volumes 의 로컬 항목이 있는 UNIX 사용자 및 그룹(예: 로컬 UNIX 사용자 및 그룹에

정의된 root)은 nobody 값으로 압축됩니다.

- Google Cloud NetApp Volumes LDAP를 사용하도록 구성된 경우 LDAP에 항목이 있는 UNIX 사용자 및 그룹은 NFS 클라이언트와 Google Cloud NetApp Volumes 간의 DNS 도메인이 다르면 none으로 축소됩니다.
- 로컬 항목이나 LDAP 항목이 없는 UNIX 사용자와 그룹은 숫자 ID 값을 사용하고 NFS 클라이언트에 지정된 이름으로 확인됩니다. 클라이언트에 이름이 없으면 숫자 ID만 표시됩니다.

다음은 이전 시나리오의 결과를 보여줍니다.

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

클라이언트와 서버 ID 도메인이 일치하면 동일한 파일 목록이 다음과 같이 표시됩니다.

```
# ls -la
total 8
drwxr-xr-x 2 root   root          4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root          4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835          9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

이 문제와 해결 방법에 대한 자세한 내용은 "섹션"을 참조하세요.NFSv4.1 및 nobody 사용자/그룹 ."

Kerberos 종속성

NFS와 함께 Kerberos를 사용하려면 Google Cloud NetApp Volumes 에 다음이 있어야 합니다.

- Kerberos Distribution Center 서비스(KDC)를 위한 Active Directory 도메인
- LDAP 기능을 위한 UNIX 정보로 채워진 사용자 및 그룹 속성이 있는 Active Directory 도메인(Google Cloud NetApp Volumes 의 NFS Kerberos는 적절한 기능을 위해 사용자 SPN과 UNIX 사용자 매핑이 필요합니다.)
- Google Cloud NetApp Volumes 인스턴스에서 LDAP가 활성화됨
- DNS 서비스를 위한 Active Directory 도메인

NFSv4.1 및 **nobody** 사용자/그룹

NFSv4.1 구성에서 가장 흔히 나타나는 문제 중 하나는 파일이나 폴더가 목록에 표시되는 경우입니다. `ls` 소유한 것으로서 `user:group` 의 조합 `nobody:nobody` .

예를 들어:

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

그리고 숫자형 ID는 `99` .

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

어떤 경우에는 파일에 올바른 소유자가 표시될 수 있지만 `nobody` 그룹으로서.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

아무도 아닌 사람은 누구인가?

그만큼 `nobody` NFSv4.1의 사용자는 다음과 다릅니다. `nfsnobody` 사용자. NFS 클라이언트가 각 사용자를 어떻게 보는지 보려면 다음을 실행하세요. `id` 명령:

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

NFSv4.1을 사용하면 `nobody` 사용자는 다음에 의해 정의된 기본 사용자입니다. `idmapd.conf` 파일이며 원하는 사용자로 정의할 수 있습니다.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

왜 이런 일이 일어날까요?

이름 문자열 매핑을 통한 보안은 NFSv4.1 작업의 핵심 원칙이므로 이름 문자열이 제대로 일치하지 않을 때의 기본 동작은 해당 사용자를 일반적으로 사용자 및 그룹이 소유한 파일과 폴더에 액세스할 수 없는 사용자에게로 밀어넣는 것입니다.

당신이 볼 때 `nobody` 파일 목록에 있는 사용자 및/또는 그룹의 경우 이는 일반적으로 NFSv4.1에 잘못 구성된 부분이 있음을 의미합니다. 여기서는 대소문자를 구분하는 것이 중요합니다.

예를 들어, user1@CVSDEMO.LOCAL(uid 1234, gid 1234)이 내보내기에 액세스하는 경우 Google Cloud NetApp Volumes user1@CVSDEMO.LOCAL(uid 1234, gid 1234)을 찾을 수 있어야 합니다. Google Cloud NetApp Volumes 의 사용자가 USER1@CVSDEMO.LOCAL인 경우, 일치하지 않습니다(대문자 USER1 대 소문자 user1). 많은 경우 클라이언트의 메시지 파일에서 다음 내용을 볼 수 있습니다.

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

클라이언트와 서버는 모두 사용자가 주장하는 사람인지에 동의해야 하므로 클라이언트가 보는 사용자가 Google Cloud NetApp Volumes 보는 사용자와 동일한 정보를 가지고 있는지 확인하려면 다음 사항을 확인해야 합니다.

- **NFSv4.x ID** 도메인**.** 고객: `idmapd.conf` 파일; Google Cloud NetApp Volumes 사용 `defaultv4iddomain.com` 수동으로 변경할 수 없습니다. NFSv4.1과 함께 LDAP를 사용하는 경우 Google Cloud NetApp Volumes ID 도메인을 DNS 검색 도메인이 사용하는 도메인으로 변경하는데, 이는 AD 도메인과 동일합니다.
- 사용자 이름과 숫자 **ID.** 이는 클라이언트가 사용자 이름을 어디에서 찾고 있는지 확인하고 이름 서비스 스위치 구성을 활용합니다. 클라이언트: `nsswitch.conf` 및/또는 로컬 비밀번호 및 그룹 파일. Google Cloud NetApp Volumes 이를 수정할 수 없지만 LDAP가 활성화되면 자동으로 구성에 LDAP를 추가합니다.
- 그룹 이름과 숫자 **ID.** 이는 클라이언트가 그룹 이름을 어디에서 찾고 있는지 확인하고 이름 서비스 스위치 구성을 활용합니다. 클라이언트: `nsswitch.conf` 및/또는 로컬 비밀번호 및 그룹 파일. Google Cloud NetApp Volumes 이를 수정할 수 없지만 LDAP가 활성화되면 자동으로 구성에 LDAP를 추가합니다.

거의 모든 경우에, 당신이 본다면 `nobody` 클라이언트의 사용자 및 그룹 목록에서 문제는 Google Cloud NetApp Volumes 와 NFS 클라이언트 간의 사용자 또는 그룹 이름 도메인 ID 변환입니다. 이러한 시나리오를 방지하려면 LDAP를 사용하여 클라이언트와 Google Cloud NetApp Volumes 간의 사용자 및 그룹 정보를 확인하세요.

클라이언트에서 **NFSv4.1**에 대한 이름 **ID** 문자열 보기

NFSv4.1을 사용하는 경우 이전에 설명한 대로 NFS 작업 중에 이름-문자열 매핑이 수행됩니다.

사용하는 것 외에도 `/var/log/messages` NFSv4 ID 문제를 찾으려면 다음을 사용할 수 있습니다. "nfsidmap -l" NFS 클라이언트에서 명령을 실행하여 NFSv4 도메인에 올바르게 매핑된 사용자 이름을 확인합니다.

예를 들어, 이는 클라이언트에서 찾을 수 있는 사용자와 Google Cloud NetApp Volumes NFSv4.x 마운트에 액세스한 후의 명령 출력입니다.

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

NFSv4.1 ID 도메인에 제대로 매핑되지 않은 사용자(이 경우, `netapp-user`) 동일한 마운트에 접근하려고 시도하고 파일을 터치하면 할당됩니다. `nobody:nobody` 예상대로.

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
```

```
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

그만큼 `nfsidmap -l` 출력은 사용자를 보여줍니다 `pcuser` 디스플레이에는 있지만 `netapp-user` ; 이것은 우리의 수출 정책 규칙에 있는 익명 사용자입니다.(`65534`).

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

중소기업

"중소기업"는 Microsoft에서 개발한 네트워크 파일 공유 프로토콜로, 이더넷 네트워크를 통해 여러 SMB 클라이언트에 중앙 집중식 사용자/그룹 인증, 권한, 잠금 및 파일 공유를 제공합니다. 파일과 폴더는 공유를 통해 클라이언트에 제공되며, 이는 다양한 공유 속성으로 구성할 수 있고 공유 수준 권한을 통해 액세스 제어를 제공합니다. SMB는 Windows, Apple, Linux 클라이언트 등 프로토콜 지원을 제공하는 모든 클라이언트에 제공될 수 있습니다.

Google Cloud NetApp Volumes 프로토콜의 SMB 2.1 및 3.x 버전을 지원합니다.

접근 제어/SMB 공유

- Windows 사용자 이름이 Google Cloud NetApp Volumes 볼륨에 대한 액세스를 요청하면 Google Cloud NetApp Volumes Google Cloud NetApp Volumes 관리자가 구성한 방법을 사용하여 UNIX 사용자 이름을 찾습니다.
- 외부 UNIX ID 공급자(LDAP)가 구성되어 있고 Windows/UNIX 사용자 이름이 동일한 경우, 추가 구성 없이 Windows 사용자 이름이 UNIX 사용자 이름과 1:1로 매핑됩니다. LDAP가 활성화되면 Active Directory가 사용자 및 그룹 개체의 UNIX 특성을 호스팅하는 데 사용됩니다.
- Windows 이름과 UNIX 이름이 완전히 일치하지 않으면 Google Cloud NetApp Volumes LDAP 이름 매핑 구성을 사용할 수 있도록 LDAP를 구성해야 합니다(섹션 참조)."비대칭 이름 매핑을 위한 LDAP 사용").
- LDAP가 사용되지 않으면 Windows SMB 사용자는 기본 로컬 UNIX 사용자로 매핑됩니다. `pcuser` Google Cloud NetApp Volumes 에서. 이는 사용자가 Windows에서 작성한 파일을 의미합니다. `pcuser` UNIX 소유권을 다음과 같이 표시합니다. `pcuser` 다중 프로토콜 NAS 환경에서. `pcuser` 여기가 사실상 `nobody` Linux 환경의

사용자(UID 65534).

SMB만 사용하는 배포에서는 `pcuser` 매핑은 계속 발생하지만 Windows 사용자 및 그룹 소유권이 올바르게 표시되고 SMB 전용 볼륨에 대한 NFS 액세스가 허용되지 않으므로 문제가 되지 않습니다. 또한 SMB 전용 볼륨은 생성된 후 NFS 또는 이중 프로토콜 볼륨으로의 변환을 지원하지 않습니다.

Windows는 Active Directory 도메인 컨트롤러와의 사용자 이름 인증을 위해 Kerberos를 활용하는데, 이를 위해서는 Google Cloud NetApp Volumes 인스턴스 외부에 있는 AD DC와 사용자 이름/비밀번호를 교환해야 합니다. Kerberos 인증은 다음과 같은 경우에 사용됩니다. `\\SERVERNAME` UNC 경로는 SMB 클라이언트에서 사용되며 다음 사항이 적용됩니다.

- SERVERNAME에 대한 DNS A/AAAA 항목이 있습니다.
- SERVERNAME에 대한 SMB/CIFS 액세스를 위한 유효한 SPN이 있습니다.

Google Cloud NetApp Volumes SMB 볼륨이 생성되면 머신 계정 이름은 섹션에 정의된 대로 생성됩니다."Google Cloud NetApp Volumes Active Directory에 표시되는 방식입니다." Google Cloud NetApp Volumes 동적 DNS(DDNS)를 활용하여 DNS에 필요한 A/AAAA 및 PTR 항목을 생성하고 머신 계정 주체에 필요한 SPN 항목을 생성하기 때문에 해당 머신 계정 이름은 SMB 공유 액세스 경로가 됩니다.

> PTR 항목을 생성하려면 Google Cloud NetApp Volumes 인스턴스 IP 주소에 대한 역방향 조회 영역이 DNS 서버에 있어야 합니다.

예를 들어, 이 Google Cloud NetApp Volumes 볼륨은 다음 UNC 공유 경로를 사용합니다. `\\cvs-east-433d.cvsdemo.local` .

Active Directory에서 Google Cloud NetApp Volumes 에서 생성된 SPN 항목은 다음과 같습니다.

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

DNS 정방향/역방향 조회 결과입니다.

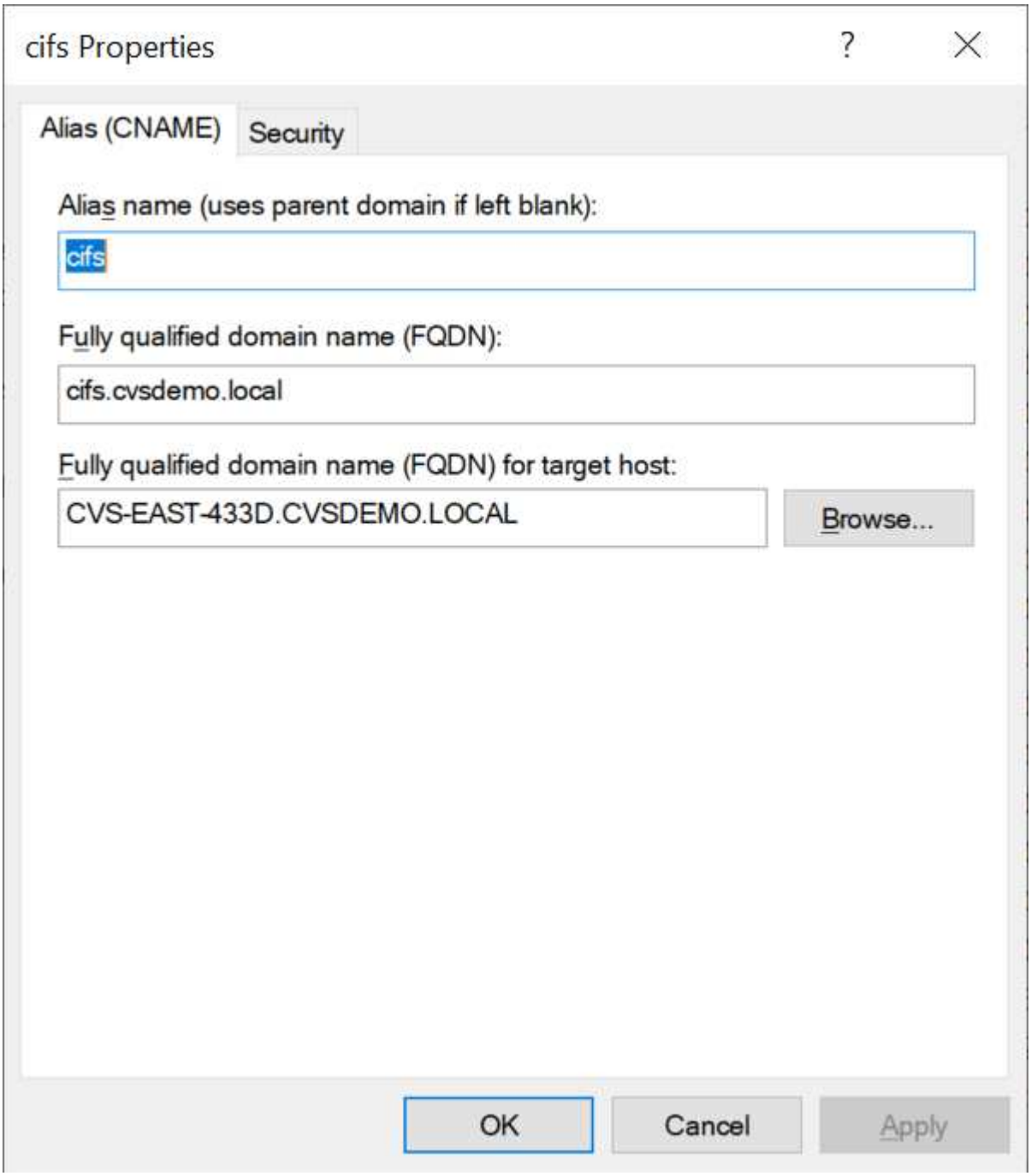
```
PS C:\> nslookup NetApp Volumes-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    NetApp Volumes-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    NetApp Volumes-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

선택적으로 Google Cloud NetApp Volumes 에서 SMB 공유에 대한 SMB 암호화를 활성화/요구하여 더 많은 액세스 제어를 적용할 수 있습니다. 엔드포인트 중 하나에서 SMB 암호화가 지원되지 않으면 액세스가 허용되지 않습니다.

SMB 이름 별칭 사용

어떤 경우에는 최종 사용자가 Google Cloud NetApp Volumes 에 사용 중인 머신 계정 이름을 아는 것이 보안 문제가 될 수 있습니다. 다른 경우에는 최종 사용자에게 더 간단한 액세스 경로를 제공하고 싶을 수도 있습니다. 이런 경우 SMB 별칭을 만들 수 있습니다.

SMB 공유 경로에 대한 별칭을 만들려면 DNS의 CNAME 레코드를 활용할 수 있습니다. 예를 들어, 이름을 사용하려면 `\\CIFS` 대신 공유에 액세스하려면 `\\cvs-east- 433d.cvsdemo.local` 하지만 여전히 Kerberos 인증을 사용하고, 기존 A/AAAA 레코드를 가리키는 DNS의 CNAME과 기존 머신 계정에 추가된 SPN을 통해 Kerberos 액세스를 제공하려고 합니다.



CNAME을 추가한 후의 DNS 정방향 조회 결과는 다음과 같습니다.

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    NetApp Volumes-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

새로운 SPN을 추가한 후의 SPN 쿼리 결과는 다음과 같습니다.

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

패킷 캡처에서는 CNAME에 연결된 SPN을 사용하여 세션 설정 요청을 볼 수 있습니다.

```
431 4.156722                                    SMB2     308 Negotiate Protocol Response
432 4.156785                                    SMB2     232 Negotiate Protocol Request
434 4.158108                                    SMB2     374 Negotiate Protocol Response
435 4.160977                                    SMB2    1978 Session Setup Request
437 4.166224                                    SMB2     322 Session Setup Response
438 4.166891                                    SMB2     152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063                                    SMB2     138 Tree Connect Response
```

```
realm: CVSDEMO.LOCAL
sname
   name-type: kRB5-NT-SRV-INST (2)
   sname-string: 2 items
      SNameString: cifs
      SNameString: cifs
enc-part
   etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

SMB 인증 방언

Google Cloud NetApp Volumes 다음을 지원합니다. "방언" SMB 인증의 경우:

- 엘엠
- NTLM
- NTLMv2
- 케르베로스

SMB 공유 액세스를 위한 Kerberos 인증은 사용할 수 있는 가장 안전한 인증 수준입니다. AES 및 SMB 암호화를 활성화하면 보안 수준이 더욱 높아집니다.

Google Cloud NetApp Volumes LM 및 NTLM 인증에 대한 이전 버전과의 호환성도 지원합니다. Kerberos가 잘못 구성된 경우(예: SMB 별칭을 만드는 경우) 공유 액세스는 더 약한 인증 방법(예: NTLMv2)을 사용합니다. 이러한 메커니즘은 보안성이 낮기 때문에 일부 Active Directory 환경에서는 비활성화됩니다. 약한 인증 방법이 비활성화되고 Kerberos가 제대로 구성되지 않으면 대체할 수 있는 유효한 인증 방법이 없기 때문에 공유 액세스가 실패합니다.

Active Directory에서 지원되는 인증 수준을 구성/보기 위한 정보는 다음을 참조하세요. "네트워크 보안: LAN Manager 인증 수준" .

권한 모델

NTFS/파일 권한

NTFS 권한은 NTFS 논리를 따르는 파일 시스템의 파일과 폴더에 적용되는 권한입니다. NTFS 권한을 적용할 수 있습니다. `Basic` 또는 `Advanced` 그리고 설정할 수 있습니다 `Allow` 또는 `Deny` 접근 제어를 위해.

기본 권한에는 다음이 포함됩니다.

- 전체 제어
- 수정하다
- 읽기 및 실행
- 읽다
- 쓰다

사용자나 그룹에 대한 권한을 설정하는 경우 ACE라고 하며 ACL에 저장됩니다. NTFS 권한은 UNIX 모드 비트와 동일한 읽기/쓰기/실행 기본 기능을 사용하지만, 소유권 가져오기, 폴더 만들기/데이터 추가, 속성 쓰기 등과 같이 보다 세부적이고 확장된 액세스 제어(특수 권한이라고도 함)로 확장될 수도 있습니다.

표준 UNIX 모드 비트는 NTFS 권한과 동일한 수준의 세분성을 제공하지 않습니다(예: ACL에서 개별 사용자 및 그룹 개체에 대한 권한을 설정하거나 확장된 특성을 설정하는 기능). 그러나 NFSv4.1 ACL은 NTFS ACL과 동일한 기능을 제공합니다.

NTFS 권한은 공유 권한보다 더 구체적이며 공유 권한과 함께 사용할 수 있습니다. NTFS 권한 구조에서는 가장 제한적인 것이 적용됩니다. 따라서 액세스 권한을 정의할 때 사용자 또는 그룹에 대한 명시적 거부는 전체 제어 권한보다 우선합니다.

NTFS 권한은 Windows SMB 클라이언트에서 제어됩니다.

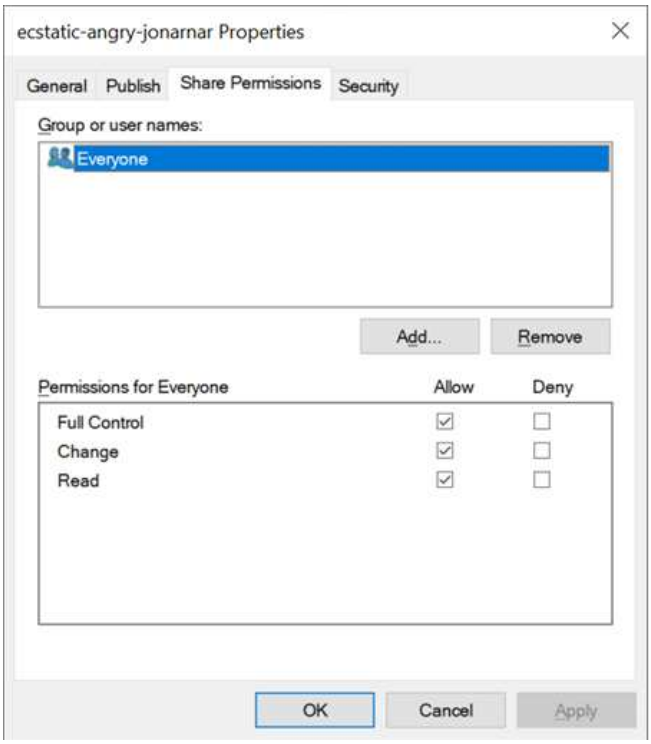
공유 권한

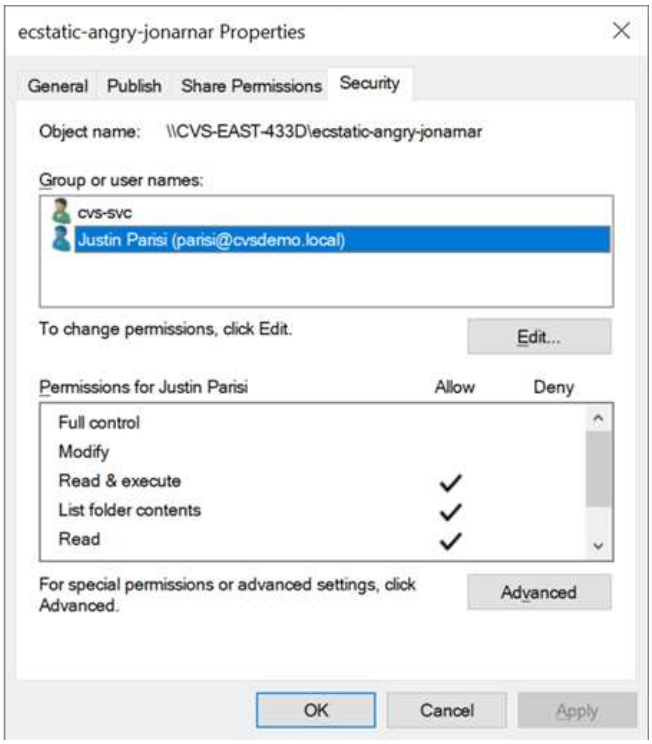
공유 권한은 NTFS 권한(읽기/변경/모든 권한만 해당)보다 일반적이며 SMB 공유에 대한 초기 항목을 제어합니다. 이는 NFS 내보내기 정책 규칙의 작동 방식과 유사합니다.

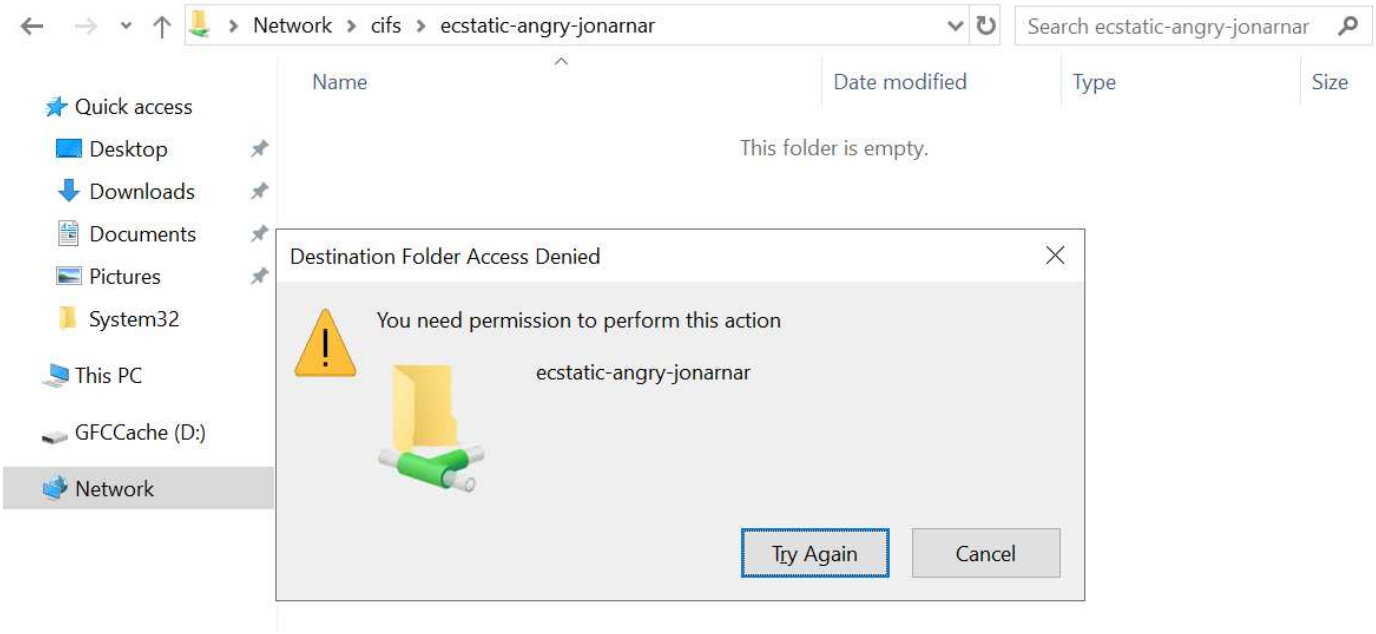
NFS 내보내기 정책 규칙은 IP 주소나 호스트 이름과 같은 호스트 기반 정보를 통해 액세스를 제어하지만, SMB 공유 권한은 공유 ACL의 사용자 및 그룹 ACE를 사용하여 액세스를 제어할 수 있습니다. Windows 클라이언트나 Google Cloud NetApp Volumes 관리 UI에서 공유 ACL을 설정할 수 있습니다.

기본적으로 공유 ACL과 초기 볼륨 ACL에는 모든 사람에게 전체 제어 권한이 포함됩니다. 파일 ACL은 변경해야 하지만 공유 권한은 공유 내 개체의 파일 권한에 의해 무시됩니다.

예를 들어, 사용자에게 Google Cloud NetApp Volumes 볼륨 파일 ACL에 대한 읽기 액세스 권한만 허용된 경우, 다음 그림에서 볼 수 있듯이 공유 ACL이 모든 사람에게 모든 권한이 부여되어 있더라도 파일 및 폴더를 만드는 액세스는 거부됩니다.







최상의 보안 결과를 얻으려면 다음을 수행하세요.

- 공유 및 파일 ACL에서 모든 사람을 제거하고 대신 사용자 또는 그룹에 대한 공유 액세스를 설정합니다.
- 관리의 편의성과 그룹 관리를 통해 공유 ACL에 사용자를 더 빠르게 추가/삭제하고 제거할 수 있도록 개별 사용자 대신 그룹을 사용하여 액세스를 제어합니다.
- 공유 권한에 대한 ACE에 덜 제한적이고 보다 일반적인 공유 액세스를 허용하고 파일 권한이 있는 사용자 및 그룹의 액세스를 잠가 보다 세부적인 액세스 제어를 제공합니다.
- 명시적으로 거부 ACL을 일반적으로 사용하지 마세요. 거부 ACL은 허용 ACL을 무시합니다. 파일 시스템에 대한 액세스를 신속하게 제한해야 하는 사용자나 그룹에 대해 명시적 거부 ACL 사용을 제한합니다.
- 다음 사항에 주의를 기울이십시오. "ACL 상속" 권한을 수정할 때의 설정; 파일 수가 많은 디렉토리나 볼륨의

최상위에 상속 플래그를 설정하면 해당 디렉토리나 볼륨 아래의 각 파일에 상속된 권한이 추가되어, 각 파일을 조정할 때 의도치 않은 액세스/거부 및 권한 수정의 장기적 반복과 같은 원치 않는 동작이 발생할 수 있습니다.

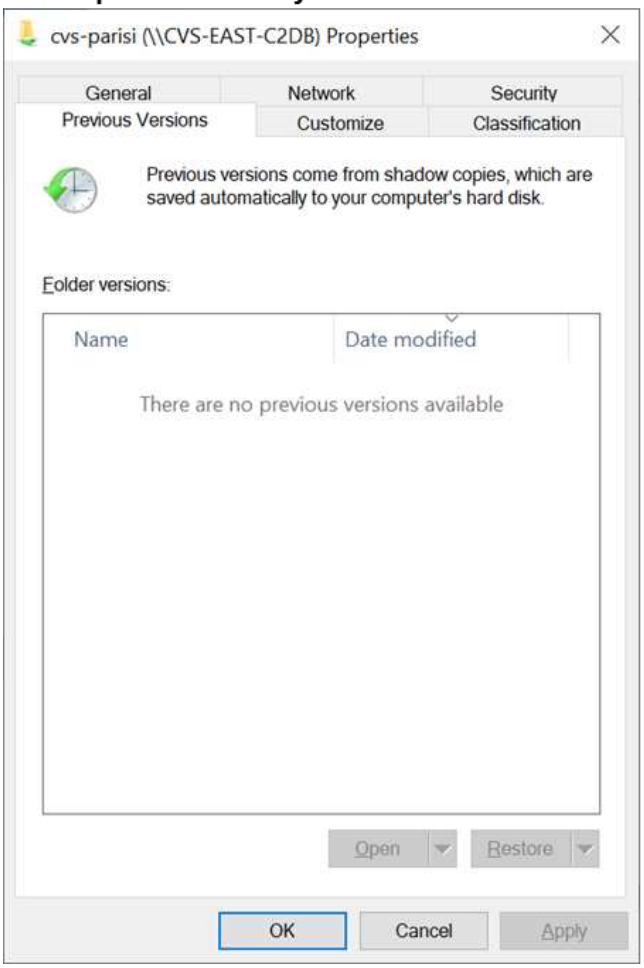
SMB 공유 보안 기능

Google Cloud NetApp Volumes 에서 SMB 액세스 권한이 있는 볼륨을 처음 만들면 해당 볼륨을 보호하기 위한 일련의 선택 사항이 제공됩니다.

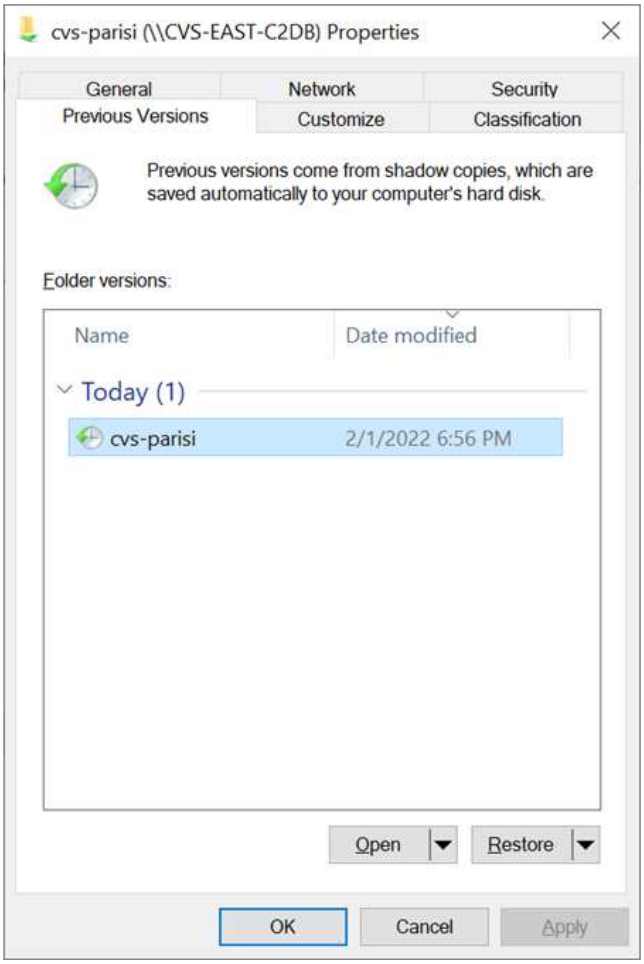
이러한 선택 사항 중 일부는 Google Cloud NetApp Volumes 수준(성능 또는 소프트웨어)에 따라 달라지며 선택 사항은 다음과 같습니다.

- 스냅샷 디렉토리를 표시합니다**(NetApp Volumes-Performance**와 **NetApp Volumes-SW** 모두에서 사용 가능**).** 이 옵션은 SMB 클라이언트가 SMB 공유의 스냅샷 디렉토리에 액세스할 수 있는지 여부를 제어합니다 .(`\\server\share\~snapshot` 및/또는 이전 버전 탭). 기본 설정은 선택 안 함입니다. 즉, 볼륨이 기본적으로 숨겨지고 액세스가 허용되지 않음을 의미합니다. `~snapshot` 디렉토리에 있고 볼륨의 이전 버전 탭에 스냅샷 복사본이 나타나지 않습니다.

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



보안상의 이유, 성능상의 이유(AV 검사에서 이러한 폴더를 숨김) 또는 기본 설정상의 이유로 최종 사용자에게서 스냅샷 사본을 숨기는 것이 바람직할 수 있습니다. Google Cloud NetApp Volumes 스냅샷은 읽기 전용이므로 이러한 스냅샷이 표시되더라도 최종 사용자는 스냅샷 디렉터리에 있는 파일을 삭제하거나 수정할 수 없습니다. 스냅샷 복사본이 생성될 당시의 파일이나 폴더에 대한 파일 권한이 적용됩니다. 스냅샷 복사본 사이에서 파일이나 폴더의 권한이 변경되면 해당 변경 사항은 스냅샷 디렉터리의 파일이나 폴더에도 적용됩니다. 사용자와 그룹은 권한에 따라 이러한 파일이나 폴더에 액세스할 수 있습니다. 스냅샷 디렉토리에 있는 파일을 삭제하거나 수정하는 것은 불가능하지만,

스냅샷 디렉토리 외부로 파일이나 폴더를 복사하는 것은 가능합니다.

- **SMB** 암호화를 활성화합니다**(NetApp Volumes-Performance** 및 **NetApp Volumes-SW** 모두에서 사용 가능**).** 기본적으로 SMB 공유에서는 SMB 암호화가 비활성화되어 있습니다(체크 안 함). 상자를 선택하면 SMB 암호화가 활성화되어 SMB 클라이언트와 서버 간 트래픽이 지원되는 가장 높은 암호화 수준으로 전송 중에 암호화됩니다. Google Cloud NetApp Volumes SMB에 대해 최대 AES-256 암호화를 지원합니다. SMB 암호화를 활성화하면 SMB 클라이언트가 알아차릴 수도 있고 알아차리지 못할 수도 있는 성능 저하가 발생합니다. 대략 10~20% 정도입니다. NetApp 성능 저하가 허용 가능한 수준인지 확인하기 위해 테스트를 강력히 권장합니다.
- **SMB** 공유 숨기기**(NetApp Volumes-Performance** 및 **NetApp Volumes-SW** 모두에서 사용 가능**).** 이 옵션을 설정하면 일반 탐색 시 SMB 공유 경로가 숨겨집니다. 이는 공유 경로를 모르는 클라이언트가 기본 UNC 경로에 액세스할 때 공유를 볼 수 없음을 의미합니다(예: `\\NetApp Volumes-SMB`). 확인란을 선택하면 SMB 공유 경로를 명시적으로 알고 있는 클라이언트나 그룹 정책 개체에 의해 정의된 공유 경로를 가진 클라이언트만 액세스할 수 있습니다(난독화를 통한 보안).
- 액세스 기반 열거**(ABE)**를 활성화합니다**(NetApp Volumes-SW**에만 해당**).** 이는 SMB 공유를 숨기는 것과 비슷하지만, 공유나 파일은 해당 개체에 대한 액세스 권한이 없는 사용자나 그룹에게만 숨겨집니다. 예를 들어, Windows 사용자인 경우 `joe` 최소한 읽기 권한이 허용되지 않으면 Windows 사용자는 권한을 통해 `joe` SMB 공유나 파일을 전혀 볼 수 없습니다. 이 기능은 기본적으로 비활성화되어 있으며, 확인란을 선택하면 활성화할 수 있습니다. ABE에 대한 자세한 내용은 NetApp 기술 자료 문서를 참조하세요. "액세스 기반 열거(ABE)는 어떻게 작동합니까?"
- **CA(Continuously Available)** 공유 지원을 활성화합니다**(NetApp Volumes-Performance**에만 해당**).** "지속적으로 이용 가능한 SMB 주식" Google Cloud NetApp Volumes 백엔드 시스템의 노드 전체에 잠금 상태를 복제하여 장애 조치 이벤트 중에 애플리케이션 중단을 최소화하는 방법을 제공합니다. 이는 보안 기능은 아니지만 전반적인 복원력을 향상시킵니다. 현재 이 기능은 SQL Server 및 FSLogix 애플리케이션에서만 지원됩니다.

기본 숨겨진 공유

Google Cloud NetApp Volumes 에서 SMB 서버가 생성되면 "숨겨진 관리 공유" ($ 명명 규칙을 사용하여) 데이터 볼륨 SMB 공유에 추가로 생성됩니다. 여기에는 C$(네임스페이스 액세스)와 IPC$(프로그램 간 통신을 위한 명명된 파이프 공유, 예: Microsoft Management Console(MMC) 액세스에 사용되는 원격 프로시저 호출(RPC))가 포함됩니다.

IPC$ 공유에는 공유 ACL이 포함되어 있지 않으며 수정할 수 없습니다. 이는 RPC 호출에만 엄격하게 사용됩니다. "Windows는 기본적으로 이러한 공유에 대한 익명 액세스를 허용하지 않습니다." .

C$ 공유는 기본적으로 BUILTIN/Administrators 액세스를 허용하지만 Google Cloud NetApp Volumes 자동화는 공유 ACL을 제거하고 누구에게도 액세스를 허용하지 않습니다. C$ 공유에 액세스하면 Google Cloud NetApp Volumes 파일 시스템에 마운트된 모든 볼륨을 볼 수 있기 때문입니다. 결과적으로, 탐색을 시도합니다. `\\SERVER\C$` 실패하다.

로컬**/BUILTIN** 관리자**/**백업 권한이 있는 계정

Google Cloud NetApp Volumes SMB 서버는 특정 도메인 사용자 및 그룹에 액세스 권한을 적용하는 로컬 그룹(예: BUILTIN\Administrators)이 있다는 점에서 일반 Windows SMB 서버와 비슷한 기능을 유지합니다.

백업 사용자에 추가할 사용자를 지정하면 해당 Active Directory 연결을 사용하는 Google Cloud NetApp Volumes 인스턴스의 BUILTIN\Backup Operators 그룹에 사용자가 추가되어 다음을 가져옵니다. "SeBackupPrivilege 및 SeRestorePrivilege" .

보안 권한 사용자에 사용자를 추가하면 사용자에게 SeSecurityPrivilege가 부여됩니다. 이는 다음과 같은 일부 애플리케이션 사용 사례에 유용합니다. "SMB 공유의 SQL Server" .

Backup Users

Provide a comma separated list of domain users or a domain group name that require elevated privileges to access volumes created by Cloud Volumes Service.

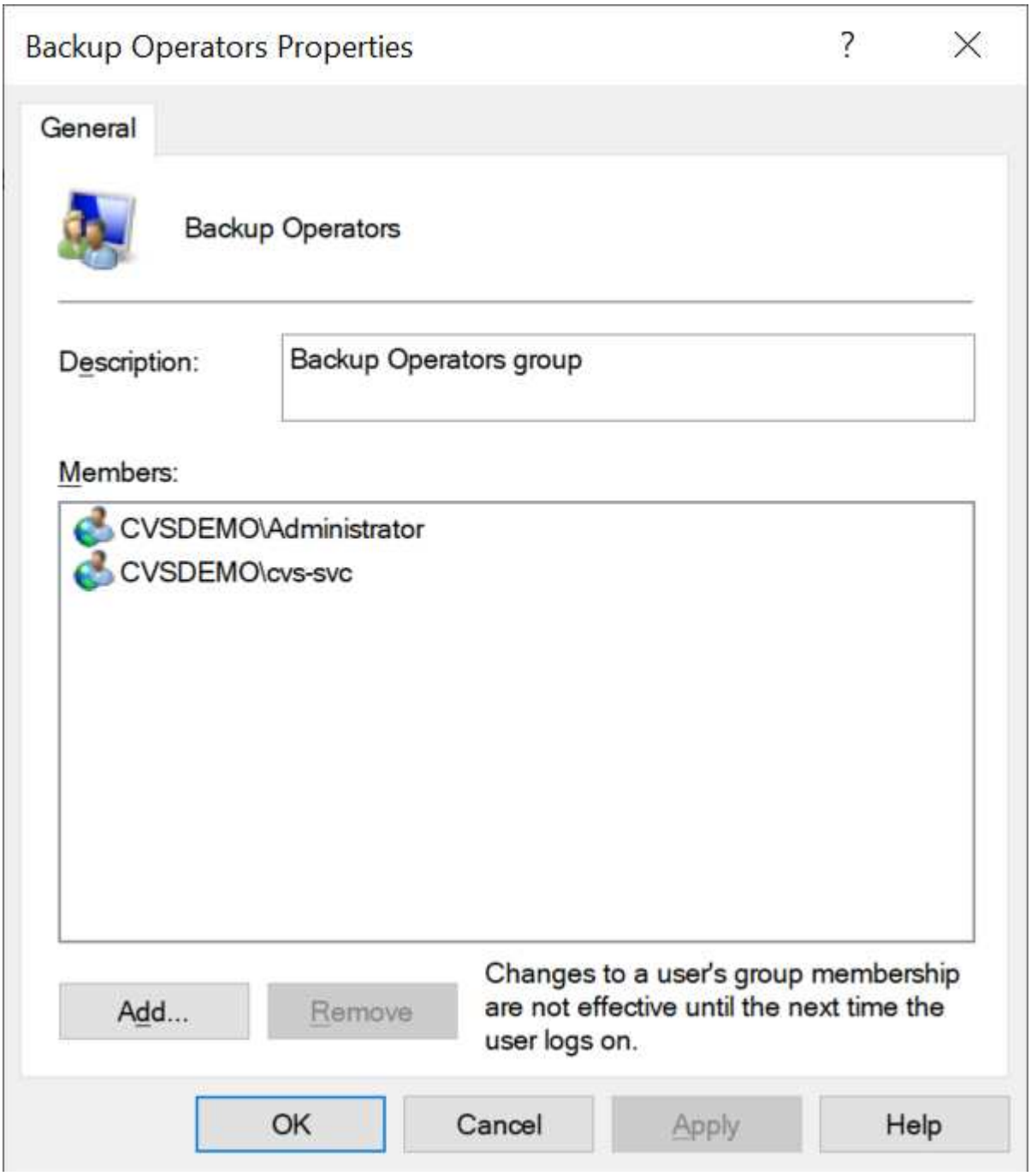
Accountnames
administrator,cvs-svc

Security Privilege Users

Provide a list of comma separated domain user accounts that require elevated privileges to manage security log for the Active Directory associated with Cloud Volumes Service.

Accountnames
administrator,cvs-svc

적절한 권한이 있으면 MMC를 통해 Google Cloud NetApp Volumes 로컬 그룹 멤버십을 볼 수 있습니다. 다음 그림은 Google Cloud NetApp Volumes 콘솔을 사용하여 추가된 사용자를 보여줍니다.

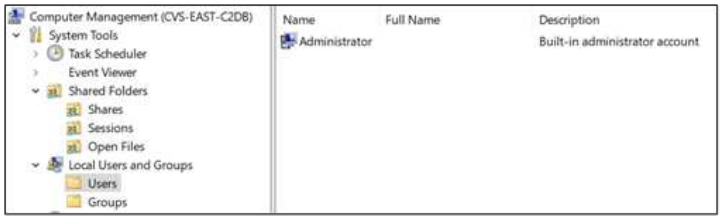


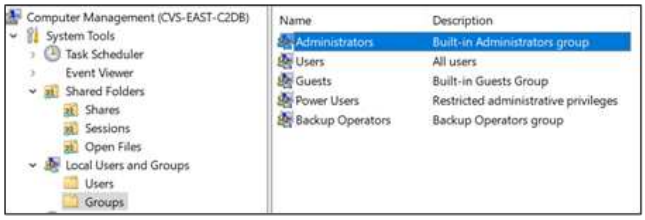
다음 표는 기본 BUILTIN 그룹 목록과 기본적으로 추가되는 사용자/그룹을 보여줍니다.

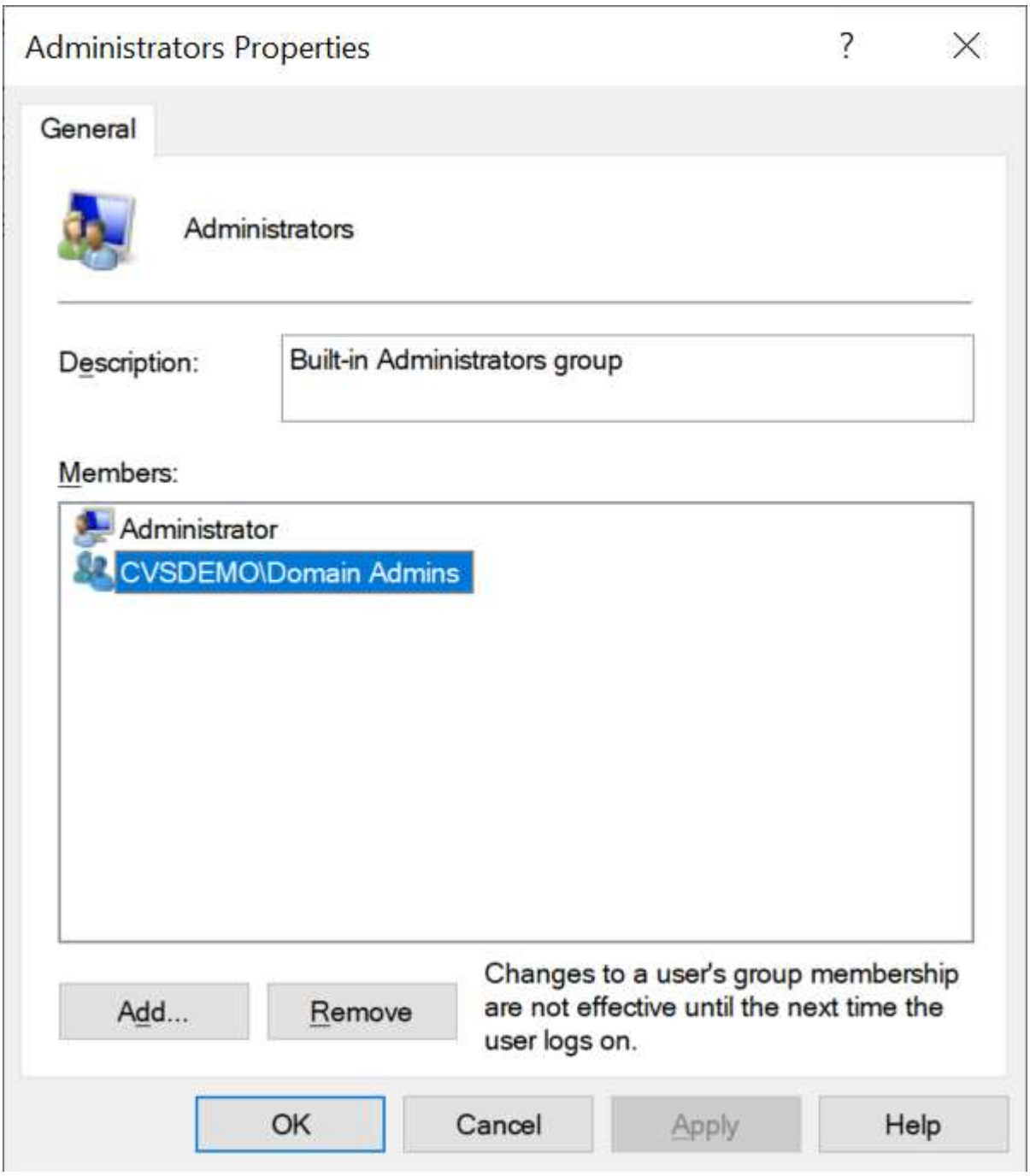
로컬/**BUILTIN** 그룹	기본 멤버
BUILTIN\관리자*	도메인\도메인 관리자
BUILTIN\백업 운영자*	None
건물\게스트	도메인\도메인 게스트
BUILTIN\파워 유저	None
BUILTIN\도메인 사용자	도메인\도메인 사용자

*그룹 멤버십은 Google Cloud NetApp Volumes Active Directory 연결 구성에서 제어됩니다.

MMC 창에서 로컬 사용자와 그룹(및 그룹 구성원)을 볼 수 있지만, 이 콘솔에서 개체를 추가하거나 삭제하거나 그룹 구성원 자격을 변경할 수는 없습니다. 기본적으로 Google Cloud NetApp Volumes 의 BUILTIN\Administrators 그룹에는 Domain Admins 그룹과 Administrator만 추가됩니다. 현재로서는 이를 수정할 수 없습니다.







MMC/컴퓨터 관리 액세스

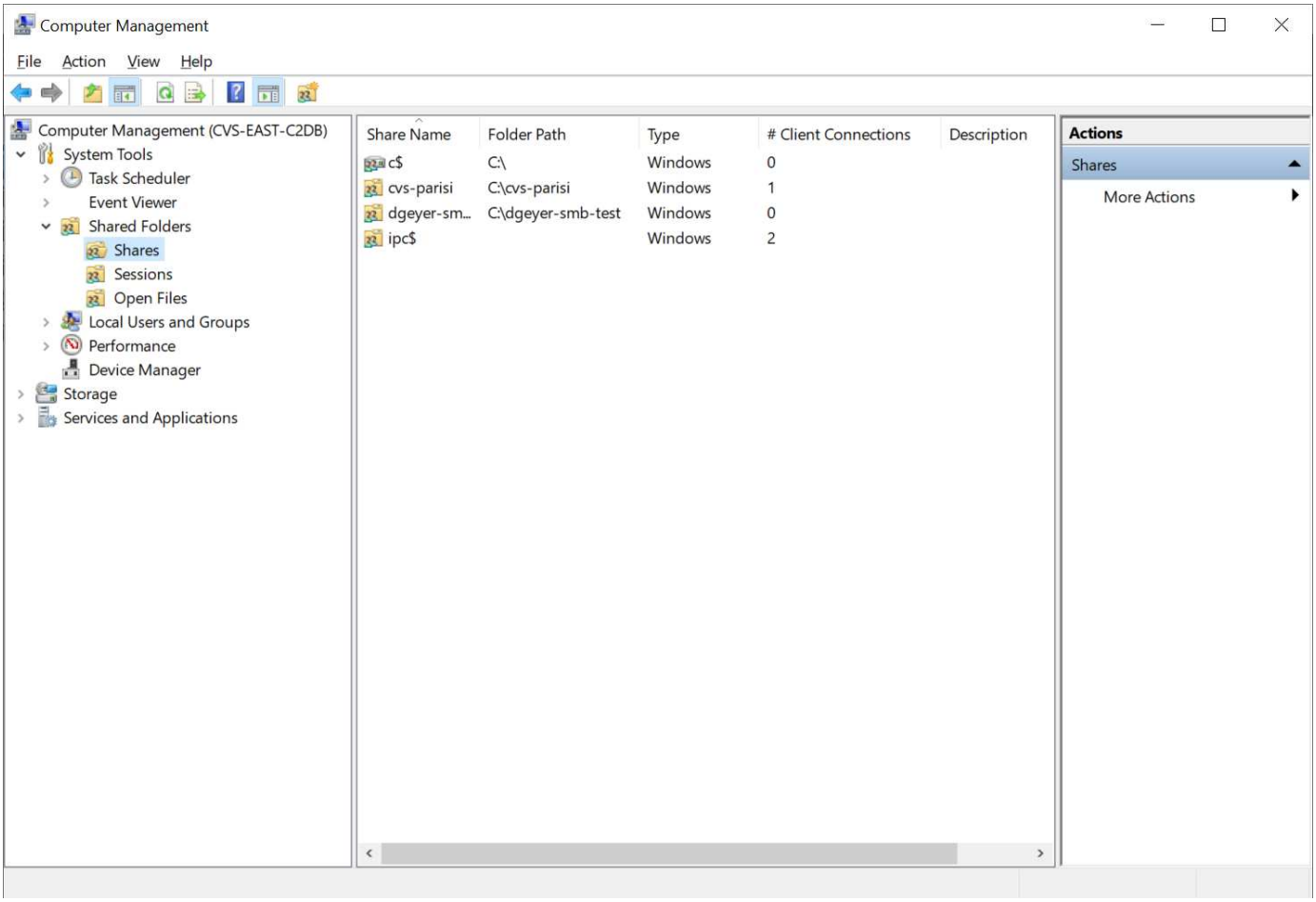
Google Cloud NetApp Volumes 의 SMB 액세스는 컴퓨터 관리 MMC에 대한 연결을 제공하여 공유 항목을 보고, 공유 ACL을 관리하고, SMB 세션을 보고 관리하고 파일을 열 수 있도록 해줍니다.

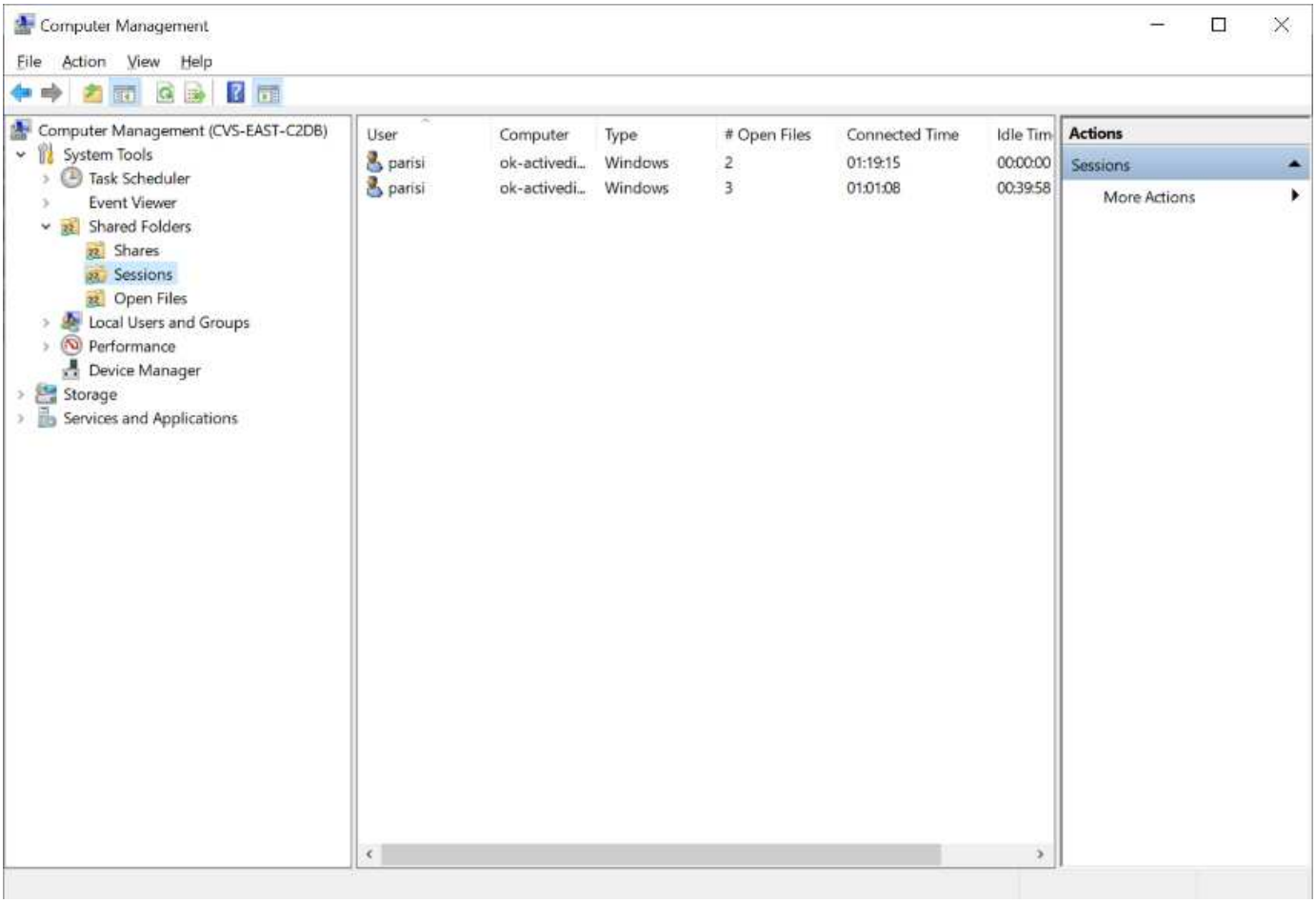
Google Cloud NetApp Volumes 에서 SMB 공유 및 세션을 보려면 MMC를 사용하려면 현재 로그인한 사용자가 도메인 관리자여야 합니다. 다른 사용자는 MMC에서 SMB 서버를 보거나 관리할 수 있는 권한이 있으며, Google Cloud NetApp Volumes SMB 인스턴스에서 공유 또는 세션을 보려고 하면 권한이 없습니다 대화 상자가 표시됩니다.

SMB 서버에 연결하려면 컴퓨터 관리를 열고 컴퓨터 관리를 마우스 오른쪽 버튼으로 클릭한 다음 다른 컴퓨터에 연결을 선택하세요. 그러면 SMB 서버 이름(Google Cloud NetApp Volumes 볼륨 정보에서 확인 가능)을 입력할 수 있는 컴퓨터 선택 대화 상자가 열립니다.

적절한 권한으로 SMB 공유를 보면 Active Directory 연결을 공유하는 Google Cloud NetApp Volumes 인스턴스의 모든 사용 가능한 공유를 볼 수 있습니다. 이 동작을 제어하려면 Google Cloud NetApp Volumes 볼륨 인스턴스에서 SMB 공유 숨기기 옵션을 설정합니다.

지역당 하나의 Active Directory 연결만 허용됩니다.





다음 표는 MMC에서 지원/지원되지 않는 기능 목록을 보여줍니다.

지원되는 기능	지원되지 않는 기능
• 공유 보기 • 활성 SMB 세션 보기 • 열린 파일 보기 • 로컬 사용자 및 그룹 보기 • 지역 그룹 멤버십 보기 • 시스템의 세션, 파일 및 트리 연결 목록을 열거합니다. • 시스템에서 열려 있는 파일을 닫습니다 • 열려 있는 세션을 닫습니다 • 공유 만들기/관리	• 새로운 로컬 사용자/그룹 생성 • 기존 로컬 사용자/그룹 관리/보기 • 이벤트 또는 성능 로그 보기 • 스토리지 관리 • 서비스 및 애플리케이션 관리

SMB 서버 보안 정보

Google Cloud NetApp Volumes 의 SMB 서버는 Kerberos 클록 오차, 티켓 수명, 암호화 등을 포함하여 SMB 연결에 대한 보안 정책을 정의하는 일련의 옵션을 사용합니다.

다음 표에는 해당 옵션의 목록, 기능, 기본 구성, Google Cloud NetApp Volumes 에서 수정할 수 있는지 여부가 나와 있습니다. 일부 옵션은 Google Cloud NetApp Volumes 에 적용되지 않습니다.

보안 옵션	그것이 하는 일	기본값	바꿀 수 있나요?
최대 Kerberos 클록 오차(분)	Google Cloud NetApp Volumes 와 도메인 컨트롤러 간의 최대 시간 차이. 시간 오차가 5분을 초과하면 Kerberos 인증이 실패합니다. 이는 Active Directory 기본값으로 설정됩니다.	5	아니요
Kerberos 티켓 수명(시간)	갱신이 필요하기 전까지 Kerberos 티켓이 유효한 최대 시간입니다. 10시간 이내에 갱신이 이루어지지 않을 경우 새로운 티켓을 구매해야 합니다. Google Cloud NetApp Volumes 이러한 갱신을 자동으로 수행합니다. Active Directory의 기본값은 10시간입니다.	10	아니요
최대 Kerberos 티켓 갱신(일)	새로운 승인 요청이 필요하기 전에 Kerberos 티켓을 갱신할 수 있는 최대 일수입니다. Google Cloud NetApp Volumes SMB 연결에 대한 티켓을 자동으로 갱신합니다. Active Directory의 기본값은 7일입니다.	7	아니요
Kerberos KDC 연결 시간 초과(초)	KDC 연결이 시간 초과되기 전까지의 시간(초)입니다.	3	아니요
수신 SMB 트래픽에 대한 서명 필요	SMB 트래픽에 대한 서명이 필요하도록 설정합니다. true로 설정하면 서명을 지원하지 않는 클라이언트는 연결에 실패합니다.	거짓	
로컬 사용자 계정에 대한 암호 복잡성 요구	로컬 SMB 사용자의 비밀번호에 사용됩니다. Google Cloud NetApp Volumes 로컬 사용자 생성을 지원하지 않으므로 이 옵션은 Google Cloud NetApp Volumes 에 적용되지 않습니다.	진실	아니요
Active Directory LDAP 연결에 start_tls 사용	Active Directory LDAP에 대한 TLS 연결을 시작하는 데 사용됩니다. Google Cloud NetApp Volumes 현재 이 기능을 활성화할 수 없습니다.	거짓	아니요

보안 옵션	그것이 하는 일	기본값	바꿀 수 있나요?
Kerberos에 AES-128 및 AES-256 암호화가 활성화되어 있습니까?	이는 Active Directory 연결에 AES 암호화를 사용할지 여부를 제어하며, Active Directory 연결을 만들거나 수정할 때 Active Directory 인증에 AES 암호화 사용 옵션을 통해 제어됩니다.	거짓	예
LM 호환성 수준	Active Directory 연결에 지원되는 인증 언어 수준입니다. "섹션을 참조하세요.SMB 인증 방언 " 자세한 내용은.	ntlmv2-krb	아니요
수신 CIFS 트래픽에 SMB 암호화 요구	모든 공유에 SMB 암호화가 필요합니다. 이것은 Google Cloud NetApp Volumes 에서는 사용되지 않습니다. 대신 볼륨별로 암호화를 설정합니다(섹션 참조).SMB 공유 보안 기능 ").	거짓	아니요
클라이언트 세션 보안	LDAP 통신에 대한 서명 및/또는 봉인을 설정합니다. 이 문제는 현재 Google Cloud NetApp Volumes 에 설정되어 있지 않지만 향후 릴리스에서는 이 문제를 해결하는 데 필요할 수 있습니다. Windows 패치로 인한 LDAP 인증 문제에 대한 수정 사항은 다음 섹션에서 다룹니다."LDAP 채널 바인딩." .	None	아니요
DC 연결을 위한 SMB2 활성화	DC 연결에는 SMB2를 사용합니다. 기본적으로 활성화되어 있습니다.	시스템 기본값	아니요
LDAP 추천 추적	여러 LDAP 서버를 사용하는 경우, 참조 추적을 통해 클라이언트는 첫 번째 서버에서 항목을 찾을 수 없을 때 목록에 있는 다른 LDAP 서버를 참조할 수 있습니다. 현재 Google Cloud NetApp Volumes 에서는 지원되지 않습니다.	거짓	아니요
보안 Active Directory 연결을 위해 LDAPS 사용	SSL을 통한 LDAP 사용을 활성화합니다. 현재 Google Cloud NetApp Volumes 에서는 지원되지 않습니다.	거짓	아니요

보안 옵션	그것이 하는 일	기본값	바꿀 수 있나요?
DC 연결에는 암호화가 필요합니다.	성공적인 DC 연결을 위해서는 암호화가 필요합니다. Google Cloud NetApp Volumes 에서는 기본적으로 비활성화되어 있습니다.	거짓	아니요

듀얼 프로토콜/멀티 프로토콜

Google Cloud NetApp Volumes는 적절한 액세스 권한을 유지하면서 SMB 및 NFS 클라이언트 모두에 동일한 데이터 세트를 공유할 수 있는 기능을 제공합니다 ("듀얼 프로토콜"). 이는 프로토콜 간의 ID 매핑을 조정하고 중앙 집중식 백엔드 LDAP 서버를 사용하여 Google Cloud NetApp Volumes에 UNIX ID를 제공함으로써 수행됩니다. 사용 편의성을 위해 Windows Active Directory를 사용하여 Windows 및 UNIX 사용자를 모두 제공할 수 있습니다.

접근 제어

- 공유 접근 제어. 어떤 클라이언트 및/또는 사용자와 그룹이 NAS 공유에 액세스할 수 있는지 확인합니다. NFS의 경우, 내보내기 정책과 규칙은 클라이언트의 내보내기 액세스를 제어합니다. NFS 내보내기는 Google Cloud NetApp Volumes 인스턴스에서 관리됩니다. SMB는 CIFS/SMB 공유와 공유 ACL을 활용하여 사용자 및 그룹 수준에서 보다 세부적인 제어를 제공합니다. https://library.netapp.com/ecmdocs/ECMP1401220/html/GUID-C1772CDF-8AEE-422B-AB87-CFCB7E50FF94.html [MMC/Computer Management^]를 사용하여 SMB 클라이언트에서 공유 수준 ACL을 구성할 수 있습니다. Google Cloud NetApp Volumes 인스턴스에 대한 관리자 권한이 있는 계정이 필요합니다(링크:gcp-gcnv-smb.html#로컬/BUILTIN 관리자/백업 권한이 있는 계정[" 로컬/BUILTIN 관리자/백업 권한이 있는 계정"] 섹션 참조).
- 파일 접근 제어. 파일 또는 폴더 수준에서 권한을 제어하며 항상 NAS 클라이언트에서 관리합니다. NFS 클라이언트는 기존 모드 비트(rwx) 또는 NFSv4 ACL을 활용할 수 있습니다. SMB 클라이언트는 NTFS 권한을 활용합니다.

NFS와 SMB 모두에 데이터를 제공하는 볼륨에 대한 액세스 제어는 사용 중인 프로토콜에 따라 달라집니다. 이중 프로토콜을 사용한 권한에 대한 정보는 "섹션"을 참조하세요.권한 모델 ."

사용자 매핑

클라이언트가 볼륨에 액세스하면 Google Cloud NetApp Volumes 들어오는 사용자를 반대 방향의 유효한 사용자에 매핑하려고 시도합니다. 이는 프로토콜 전반에 걸쳐 적절한 액세스가 이루어졌는지 확인하고 액세스를 요청한 사용자가 실제로 주장하는 사람인지 확인하는 데 필요합니다.

예를 들어, Windows 사용자가 다음과 같은 경우 `joe` SMB를 통해 UNIX 권한이 있는 볼륨에 액세스를 시도하면 Google Cloud NetApp Volumes 검색을 수행하여 해당 UNIX 사용자를 찾습니다. `joe` . 만약 존재한다면 Windows 사용자로 SMB 공유에 쓰여진 파일 `joe` UNIX 사용자로 나타납니다 `joe` NFS 클라이언트에서.

또는 UNIX 사용자가 다음과 같은 경우 `joe` Windows 권한으로 Google Cloud NetApp Volumes 볼륨에 액세스를 시도하는 경우 UNIX 사용자는 유효한 Windows 사용자에 매핑할 수 있어야 합니다. 그렇지 않으면 볼륨에 대한 액세스가 거부됩니다.

현재 LDAP를 사용한 외부 UNIX ID 관리에는 Active Directory만 지원됩니다. 이 서비스에 대한 액세스 구성에 대한 자세한 내용은 "AD 연결 생성"을 참조하십시오.

이중 프로토콜 설정을 사용하는 경우 Google Cloud NetApp Volumes 볼륨의 보안 스타일을 활용하여 ACL 유형을 결정합니다. 이러한 보안 스타일은 지정된 NAS 프로토콜에 따라 설정되며, 이중 프로토콜의 경우 Google Cloud NetApp Volumes 볼륨을 생성할 때 선택합니다.

- NFS만 사용하는 경우 Google Cloud NetApp Volumes 볼륨은 UNIX 권한을 사용합니다.
- SMB만 사용하는 경우 Google Cloud NetApp Volumes 볼륨은 NTFS 권한을 사용합니다.

듀얼 프로토콜 볼륨을 생성하는 경우 볼륨 생성 시 ACL 스타일을 선택할 수 있습니다. 이러한 결정은 원하는 권한 관리에 따라 내려져야 합니다. 사용자가 Windows/SMB 클라이언트에서 권한을 관리하는 경우 NTFS를 선택하세요. 사용자가 NFS 클라이언트와 chmod/chown을 선호하는 경우 UNIX 보안 스타일을 사용하세요.

Active Directory 연결을 만드는 데 대한 고려 사항

Google Cloud NetApp Volumes 사용하면 SMB 및 UNIX 사용자 모두의 ID 관리를 위해 Google Cloud NetApp Volumes 인스턴스를 외부 Active Directory 서버에 연결할 수 있습니다. Google Cloud NetApp Volumes 에서 SMB를 사용하려면 Active Directory 연결을 만들어야 합니다.

이를 위한 구성에는 보안을 위해 고려해야 할 몇 가지 옵션이 제공됩니다. 외부 Active Directory 서버는 온프레미스 인스턴스이거나 클라우드 네이티브일 수 있습니다. 온프레미스 Active Directory 서버를 사용하는 경우 도메인을 외부 네트워크(DMZ 또는 외부 IP 주소 등)에 노출하지 마세요. 대신, 안전한 개인 터널이나 VPN, 단방향 포리스트 트러스트 또는 온프레미스 네트워크에 대한 전용 네트워크 연결을 사용하십시오. "비공개 Google 액세스" . 자세한 내용은 Google Cloud 문서를 참조하세요. "Google Cloud에서 Active Directory를 사용하는 모범 사례" .

> NetApp Volumes-SW를 사용하려면 Active Directory 서버가 동일한 지역에 있어야 합니다. NetApp Volumes-SW에서 다른 지역에 DC 연결을 시도하면 시도가 실패합니다. NetApp Volumes-SW를 사용하는 경우 Active Directory DC를 포함하는 Active Directory 사이트를 만든 다음 Google Cloud NetApp Volumes 에서 사이트를 지정하여 지역 간 DC 연결 시도를 방지하세요.

Active Directory 자격 증명

NFS용 SMB 또는 LDAP가 활성화된 경우 Google Cloud NetApp Volumes Active Directory 컨트롤러와 상호 작용하여 인증에 사용할 머신 계정 개체를 생성합니다. 이는 Windows SMB 클라이언트가 도메인에 가입하고 Active Directory의 조직 단위(OU)에 대한 동일한 액세스 권한을 요구하는 방식과 다르지 않습니다.

많은 경우 보안 그룹은 Google Cloud NetApp Volumes 와 같은 외부 서버에서 Windows 관리자 계정을 사용하는 것을 허용하지 않습니다. 어떤 경우에는 보안 모범 사례에 따라 Windows 관리자 사용자가 완전히 비활성화됩니다.

SMB 머신 계정을 생성하는 데 필요한 권한

Active Directory에 Google Cloud NetApp Volumes 머신 객체를 추가하려면 도메인에 대한 관리 권한이 있거나 "머신 계정 객체를 생성하고 수정하기 위한 위임된 권한" 지정된 OU에 대한 것이 필요합니다. Active Directory의 제어 위임 마법사를 사용하여 다음 액세스 권한이 제공되는 컴퓨터 개체의 생성/삭제에 대한 사용자 액세스 권한을 제공하는 사용자 지정 작업을 만들어 이 작업을 수행할 수 있습니다.

- 읽기/쓰기
- 모든 자식 개체 생성/삭제
- 모든 속성 읽기/쓰기

- 비밀번호 변경/재설정

이렇게 하면 정의된 사용자에 대한 보안 ACL이 Active Directory의 OU에 자동으로 추가되고 Active Directory 환경에 대한 액세스가 최소화됩니다. 사용자가 위임된 후에는 이 창에서 해당 사용자 이름과 비밀번호를 Active Directory 자격 증명으로 제공할 수 있습니다.

Active Directory 도메인에 전달되는 사용자 이름과 비밀번호는 보안을 강화하기 위해 머신 계정 개체 쿼리 및 생성 중에 Kerberos 암호화를 활용합니다.

Active Directory 연결 세부 정보

`https://docs.cloud.google.com/netapp/volumes/docs/configure-and-use/active-directory/about-ad["Active Directory 연결 세부 정보"^]`는 관리자가 다음과 같은 컴퓨터 계정 배치를 위한 특정 `Active Directory` 스키마 정보를 제공할 수 있도록 지침을 제공합니다.

- **Active Directory** 연결 유형**.** 지역의 Active Directory 연결이 Google Cloud NetApp Volumes 또는 NetApp Volumes-Performance 서비스 유형의 볼륨에 사용되는지 여부를 지정하는 데 사용됩니다. 기존 연결에서 이것이 잘못 설정되면, 사용 또는 편집 시 제대로 작동하지 않을 수 있습니다.
- 도메인**.** Active Directory 도메인 이름.
- 사이트**.** 보안 및 성능 향상을 위해 Active Directory 서버를 특정 사이트로 제한합니다 "고려 사항". 여러 Active Directory 서버가 여러 지역에 걸쳐 있는 경우 이 설정이 필요합니다. Google Cloud NetApp Volumes는 현재 Google Cloud NetApp Volumes 인스턴스와 다른 지역에 있는 Active Directory 서버에 대한 Active Directory 인증 요청을 허용하지 않기 때문입니다. (예를 들어, Active Directory 도메인 컨트롤러가 NetApp Volumes-Performance만 지원하는 지역에 있지만 NetApp Volumes-SW 인스턴스에 SMB 공유를 사용하려는 경우입니다.)
- **DNS** 서버**.** 이름 조회에 사용할 DNS 서버입니다.
- **NetBIOS** 이름**(**선택 사항**).** 원하는 경우 서버의 NetBIOS 이름을 입력합니다. 이는 Active Directory 연결을 사용하여 새로운 컴퓨터 계정을 생성할 때 사용됩니다. 예를 들어 NetBIOS 이름이 NetApp Volumes-EAST로 설정된 경우 머신 계정 이름은 NetApp Volumes-EAST-{1234}가 됩니다. 섹션을 참조하세요"Google Cloud NetApp Volumes Active Directory에 표시되는 방식" 자세한 내용은.
- 조직 단위**(OU).** 컴퓨터 계정을 만드는 특정 OU입니다. 이 기능은 특정 OU에 대한 머신 계정의 제어권을 사용자에게 위임하는 경우에 유용합니다.
- **AES** 암호화**.** AD 인증에 AES 암호화 사용 확인란을 선택하거나 선택 취소할 수도 있습니다. Active Directory 인증에 AES 암호화를 사용하면 사용자 및 그룹 조회 중에 Google Cloud NetApp Volumes 와 Active Directory 간 통신에 대한 보안이 강화됩니다. 이 옵션을 활성화하기 전에 도메인 관리자에게 문의하여 Active Directory 도메인 컨트롤러가 AES 인증을 지원하는지 확인하세요.

기본적으로 대부분의 Windows 서버는 약한 암호(예: DES 또는 RC4-HMAC)를 비활성화하지 않지만 약한 암호를 비활성화하도록 선택한 경우 Google Cloud NetApp Volumes Active Directory 연결이 AES를 활성화하도록 구성되었는지 확인하세요. 그렇지 않으면 인증 실패가 발생합니다. AES 암호화를 활성화해도 약한 암호가 비활성화되는 것은 아니지만, 대신 Google Cloud NetApp Volumes SMB 머신 계정에 AES 암호에 대한 지원이 추가됩니다.

Kerberos 영역 세부 정보

이 옵션은 SMB 서버에는 적용되지 않습니다. 오히려 Google Cloud NetApp Volumes 시스템에 대한 NFS Kerberos를 구성할 때 사용됩니다. 이러한 세부 정보가 채워지면 NFS Kerberos 영역이 구성되고(Linux의 krb5.conf

파일과 유사) Google Cloud NetApp Volumes 볼륨 생성 시 NFS Kerberos가 지정되면 Active Directory 연결이 NFS Kerberos 배포 센터(KDC) 역할을 하므로 이 영역이 사용됩니다.

현재 Windows가 아닌 KDC는 Google Cloud NetApp Volumes 와 함께 사용할 수 없습니다.

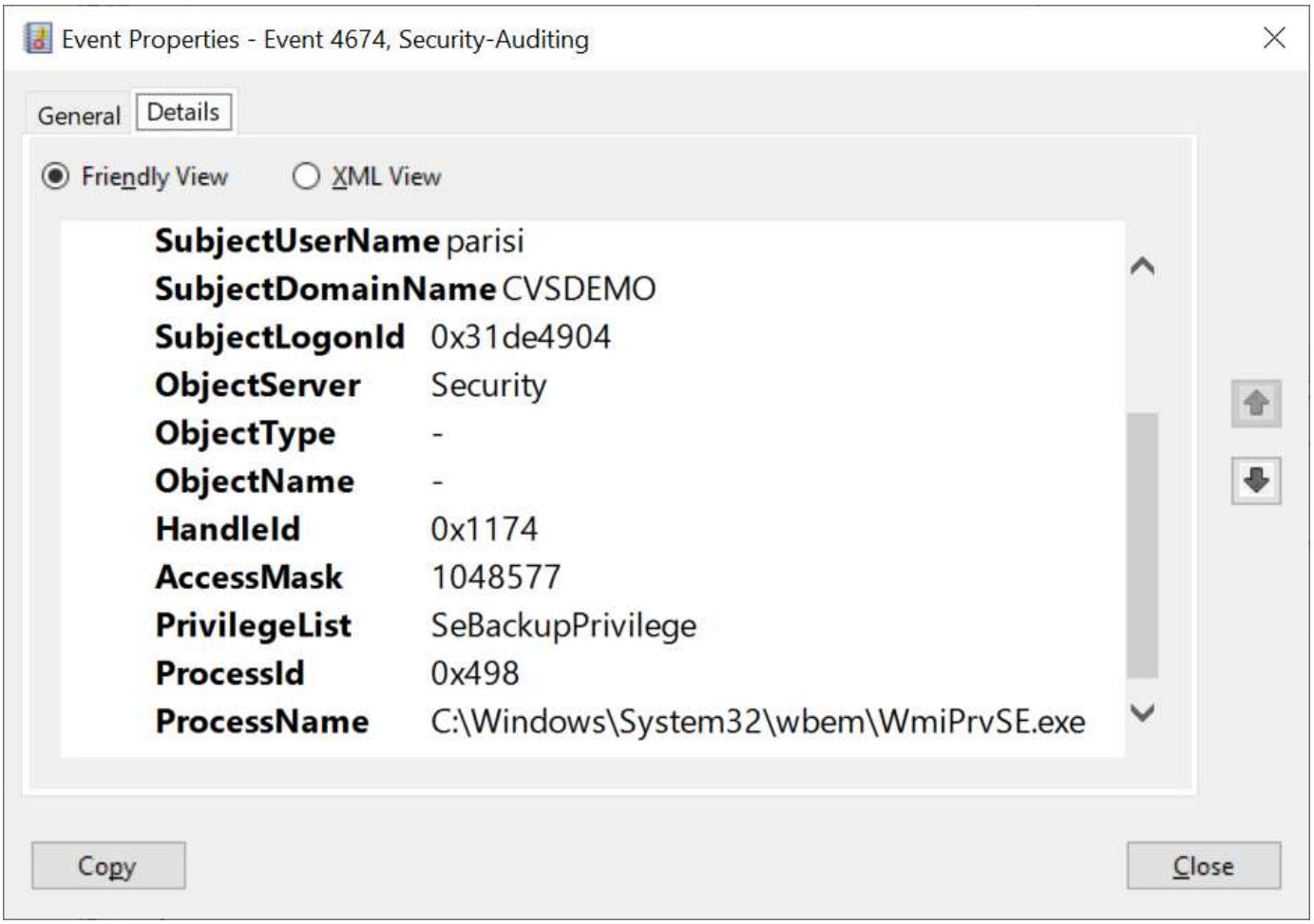
지역

지역을 사용하면 Active Directory 연결이 있는 위치를 지정할 수 있습니다. 이 지역은 Google Cloud NetApp Volumes 볼륨과 동일한 지역이어야 합니다.

- **LDAP**를 사용하는 로컬 **NFS** 사용자**.** 이 섹션에는 LDAP를 사용하여 로컬 NFS 사용자를 허용하는 옵션도 있습니다. NFS(확장 그룹)의 16개 그룹 제한을 넘어 UNIX 사용자 그룹 멤버십 지원을 확장하려면 이 옵션을 선택하지 않아야 합니다. 그러나 확장 그룹을 사용하려면 UNIX ID에 대한 LDAP 서버를 구성해야 합니다. LDAP 서버가 없으면 이 옵션을 선택하지 마세요. LDAP 서버가 있고 로컬 UNIX 사용자(예: root)도 사용하려는 경우 이 옵션을 선택하세요.

백업 사용자

이 옵션을 사용하면 Google Cloud NetApp Volumes 볼륨에 대한 백업 권한이 있는 Windows 사용자를 지정할 수 있습니다. 일부 애플리케이션이 NAS 볼륨의 데이터를 올바르게 백업하고 복원하려면 백업 권한(SeBackupPrivilege)이 필요합니다. 이 사용자는 볼륨의 데이터에 대한 높은 수준의 액세스 권한을 가지고 있으므로 다음을 고려해야 합니다. "해당 사용자 액세스에 대한 감사 활성화" . 이 기능을 활성화하면 감사 이벤트가 이벤트 뷰어 > Windows 로그 > 보안에 표시됩니다.



보안 권한 사용자

이 옵션을 사용하면 Google Cloud NetApp Volumes 볼륨에 대한 보안 수정 권한이 있는 Windows 사용자를 지정할 수 있습니다. 일부 애플리케이션에는 보안 권한(SeSecurityPrivilege)이 필요합니다.("SQL Server와 같은") 설치 중에 권한을 올바르게 설정하세요. 보안 로그를 관리하려면 이 권한이 필요합니다. 이 권한은 SeBackupPrivilege만큼 강력하지는 않지만 NetApp 다음을 권장합니다. "사용자의 사용자 액세스 감사" 필요한 경우 이 권한 수준을 사용합니다.

자세한 내용은 다음을 참조하세요. "새 로그온에 할당된 특별 권한" .

Google Cloud NetApp Volumes Active Directory에 표시되는 방식

Google Cloud NetApp Volumes Active Directory에 일반 머신 계정 개체로 표시됩니다. 명명 규칙은 다음과 같습니다.

- CIFS/SMB와 NFS Kerberos는 별도의 머신 계정 객체를 생성합니다.
- LDAP가 활성화된 NFS는 Kerberos LDAP 바인딩을 위해 Active Directory에 머신 계정을 생성합니다.
- LDAP가 있는 이중 프로토콜 볼륨은 LDAP 및 SMB에 대한 CIFS/SMB 머신 계정을 공유합니다.
- CIFS/SMB 머신 계정은 머신 계정에 NAME-1234(<10자 이름에 하이픈이 붙은 무작위 4자리 ID)라는 명명 규칙을 사용합니다. Active Directory 연결에서 NetBIOS 이름 설정을 통해 NAME을 정의할 수 있습니다(섹션 참조)Active Directory 연결 세부 정보 ").
- NFS Kerberos는 NFS-NAME-1234를 명명 규칙으로 사용합니다(최대 15자). 15자 이상을 사용하면 이름은 NFS-TRUNCATED-NAME-1234가 됩니다.
- LDAP가 활성화된 NFS 전용 NetApp Volumes-Performance 인스턴스는 CIFS/SMB 인스턴스와 동일한 명명 규칙을 사용하여 LDAP 서버에 바인딩하기 위한 SMB 머신 계정을 생성합니다.
- SMB 머신 계정이 생성되면 기본적으로 숨겨진 관리자 공유가 생성됩니다(섹션 참조)"기본 숨겨진 공유")도 생성되지만(c$, admin$, ipc$) 해당 공유에는 ACL이 할당되지 않아 액세스할 수 없습니다.
- 기본적으로 머신 계정 개체는 CN=Computers에 배치되지만 필요한 경우 다른 OU를 지정할 수 있습니다. "섹션을 참조하세요.SMB 머신 계정을 생성하는 데 필요한 권한 Google Cloud NetApp Volumes 에 대한 머신 계정 객체를 추가/제거하는 데 필요한 액세스 권한에 대한 정보는 "를 참조하세요.

Google Cloud NetApp Volumes SMB 머신 계정을 Active Directory에 추가하면 다음 필드가 채워집니다.

- cn (지정된 SMB 서버 이름 사용)
- dNSHostName(SMBserver.domain.com 포함)
- msDS-SupportedEncryptionTypes(AES 암호화가 활성화되지 않은 경우 DES_CBC_MD5, RC4_HMAC_MD5 허용, AES 암호화가 활성화된 경우 SMB용 머신 계정과 Kerberos 티켓 교환을 위해 DES_CBC_MD5, RC4_HMAC_MD5, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96 허용)
- 이름(SMB 서버 이름 포함)
- sAMAccountName(SMBserver$ 포함)
- servicePrincipalName(Kerberos용 host/smbserver.domain.com 및 host/smbserver SPN 포함)

머신 계정에서 약한 Kerberos 암호화 유형(enctype)을 비활성화하려면 머신 계정의 msDS-SupportedEncryptionTypes 값을 다음 표에 있는 값 중 하나로 변경하여 AES만 허용하면 됩니다.

msDS-SupportedEncryptionTypes 값	**Enctype** 활성화됨
2	DES_CBC_MD5

msDS-SupportedEncryptionTypes 값	**Enctype** 활성화됨
4	RC4_HMAC
8	AES128_CTS_HMAC_SHA1_96만
16	AES256_CTS_HMAC_SHA1_96만
24	AES128_CTS_HMAC_SHA1_96 및 AES256_CTS_HMAC_SHA1_96
30	DES_CBC_MD5, RC4_HMAC, AES128_CTS_HMAC_SHA1_96 및 AES256_CTS_HMAC_SHA1_96

SMB 머신 계정에 AES 암호화를 활성화하려면 Active Directory 연결을 생성할 때 AD 인증에 AES 암호화 사용을 클릭합니다.

NFS Kerberos에 대한 AES 암호화를 활성화하려면 "Google Cloud NetApp Volumes 문서를 참조하세요.".

기타 **NAS** 인프라 서비스 종속성**(KDC, LDAP** 및 **DNS)**

NAS 공유에 Google Cloud NetApp Volumes 사용하는 경우, 적절한 기능을 위해 외부 종속성이 필요할 수 있습니다. 이러한 종속성은 특정 상황에서 작용합니다. 다음 표에서는 다양한 구성 옵션과 필요한 종속성(있는 경우)을 보여줍니다.

구성	종속성이 필요합니다
NFSv3만	None
NFSv3 Kerberos만	Windows Active Directory: * KDC * DNS * LDAP
NFSv4.1만	클라이언트 ID 매핑 구성(/etc/idmap.conf)
NFSv4.1 Kerberos만	• 클라이언트 ID 매핑 구성(/etc/idmap.conf) • Windows Active Directory: KDC DNS LDAP
SMB만 해당	액티브 디렉토리: * KDC * DNS
멀티프로토콜 NAS(NFS 및 SMB)	• 클라이언트 ID 매핑 구성(NFSv4.1만 해당; /etc/idmap.conf) • Windows Active Directory: KDC DNS LDAP

머신 계정 개체에 대한 **Kerberos** 키탭 회전/암호 재설정

SMB 머신 계정을 사용하면 Google Cloud NetApp Volumes SMB 머신 계정에 대한 주기적 비밀번호 재설정을 예약합니다. 이러한 비밀번호 재설정은 Kerberos 암호화를 사용하여 이루어지며, 매주 넷째 일요일 오후 11시와 오전 1시 사이의 무작위 시간에 작동합니다. 이러한 비밀번호 재설정은 Kerberos 키 버전을 변경하고, Google Cloud NetApp Volumes 시스템에 저장된 키탭을 순환시키며, Google Cloud NetApp Volumes 에서 실행되는 SMB 서버의 보안 수준을 더 높게 유지하는 데 도움이 됩니다. 머신 계정 비밀번호는 무작위로 지정되며 관리자는 이를 알 수 없습니다.

NFS Kerberos 머신 계정의 경우, 암호 재설정은 KDC와 새로운 키탭이 생성되거나 교환될 때만 이루어집니다. 현재 Google Cloud NetApp Volumes 에서는 이 작업을 수행할 수 없습니다.

LDAP 및 **Kerberos**와 함께 사용할 네트워크 포트

LDAP 및 Kerberos를 사용할 때는 이러한 서비스에서 사용하는 네트워크 포트를 확인해야 합니다. Google Cloud NetApp Volumes에서 사용하는 포트의 전체 목록은 "보안 고려 사항에 대한 Google Cloud NetApp Volumes 문서 "에서 확인할 수 있습니다.

LDAP

Google Cloud NetApp Volumes LDAP 클라이언트 역할을 하며 UNIX ID에 대한 사용자 및 그룹 조회를 위해 표준 LDAP 검색 쿼리를 사용합니다. Google Cloud NetApp Volumes 에서 제공하는 표준 기본 사용자 이외의 사용자와 그룹을 사용하려면 LDAP가 필요합니다. 사용자 주체(예: user1@domain.com)와 함께 NFS Kerberos를 사용하려는 경우에도 LDAP가 필요합니다. 현재는 Microsoft Active Directory를 사용하는 LDAP만 지원됩니다.

Active Directory를 UNIX LDAP 서버로 사용하려면 UNIX ID에 사용하려는 사용자와 그룹에 필요한 UNIX 특성을 채워야 합니다. Google Cloud NetApp Volumes 속성을 기반으로 쿼리하는 기본 LDAP 스키마 템플릿을 사용합니다. "RFC-2307-비스" . 결과적으로, 다음 표는 사용자 및 그룹에 대해 채워야 하는 최소한의 필수 Active Directory 특성과 각 특성의 용도를 보여줍니다.

Active Directory에서 LDAP 속성을 설정하는 방법에 대한 자세한 내용은 다음을 참조하십시오. "이중 프로토콜 액세스 관리."

기인하다	그것이 하는 일
UID*	UNIX 사용자 이름을 지정합니다
uid번호*	UNIX 사용자의 숫자 ID를 지정합니다.
gidNumber*	UNIX 사용자의 기본 그룹 숫자 ID를 지정합니다.
객체클래스*	사용되는 객체 유형을 지정합니다. Google Cloud NetApp Volumes 객체 클래스 목록에 "사용자"가 포함되어야 합니다(대부분의 Active Directory 배포에 기본적으로 포함됨).
이름	계정에 대한 일반 정보(실명, 전화번호 등 - gecos라고도 함)
unixUserPassword	이 항목은 설정할 필요가 없습니다. NAS 인증을 위한 UNIX ID 조회에는 사용되지 않습니다. 이것을 설정하면 구성된 unixUserPassword 값이 일반 텍스트로 저장됩니다.
unixHomeDirectory	Linux 클라이언트에서 사용자가 LDAP로 인증할 때 UNIX 홈 디렉토리에 대한 경로를 정의합니다. UNIX 홈 디렉토리 기능에 LDAP를 사용하려면 이것을 설정합니다.
로그인셸	사용자가 LDAP에 대해 인증할 때 Linux 클라이언트의 bash/profile 셸에 대한 경로를 정의합니다.

- Google Cloud NetApp Volumes 에서 제대로 작동하려면 속성이 필요함을 나타냅니다. 나머지 속성은 클라이언트 측에서만 사용됩니다.

기인하다	그것이 하는 일
씨엔*	UNIX 그룹 이름을 지정합니다. LDAP에 Active Directory를 사용하는 경우 이는 개체가 처음 생성될 때 설정되지만 나중에 변경할 수 있습니다. 이 이름은 다른 객체와 동일할 수 없습니다. 예를 들어, UNIX 사용자 user1이 Linux 클라이언트에서 user1이라는 그룹에 속해 있는 경우 Windows에서는 동일한 cn 속성을 가진 두 개의 객체를 허용하지 않습니다. 이 문제를 해결하려면 Windows 사용자의 이름을 고유한 이름(예: user1-UNIX)으로 바꾸세요. Google Cloud NetApp Volumes 의 LDAP는 UNIX 사용자 이름에 uid 속성을 사용합니다.
gidNumber*	UNIX 그룹 숫자 ID를 지정합니다.
객체클래스*	사용되는 객체 유형을 지정합니다. Google Cloud NetApp Volumes 그룹이 객체 클래스 목록에 포함되어야 합니다(이 속성은 대부분의 Active Directory 배포에 기본적으로 포함되어 있습니다).
멤버Uid	어떤 UNIX 사용자가 UNIX 그룹의 구성원인지 지정합니다. Google Cloud NetApp Volumes 의 Active Directory LDAP를 사용하면 이 필드가 필요하지 않습니다. Google Cloud NetApp Volumes LDAP 스키마는 그룹 멤버십에 Member 필드를 사용합니다.
회원*	그룹 멤버십/보조 UNIX 그룹에 필요합니다. 이 필드는 Windows 사용자를 Windows 그룹에 추가하여 채워집니다. 그러나 Windows 그룹에 UNIX 속성이 채워지지 않으면 UNIX 사용자의 그룹 멤버십 목록에 포함되지 않습니다. NFS에서 사용할 수 있어야 하는 모든 그룹은 이 표에 나열된 필수 UNIX 그룹 속성을 채워야 합니다.

- Google Cloud NetApp Volumes 에서 제대로 작동하려면 속성이 필요함을 나타냅니다. 나머지 속성은 클라이언트 측에서만 사용됩니다.

LDAP 바인딩 정보

LDAP에서 사용자를 쿼리하려면 Google Cloud NetApp Volumes LDAP 서비스에 바인딩(로그인)해야 합니다. 이 로그인은 읽기 전용 권한을 가지며 디렉토리 조회를 위해 LDAP UNIX 속성을 쿼리하는 데 사용됩니다. 현재 LDAP 바인딩은 SMB 머신 계정을 사용해서만 가능합니다.

LDAP는 다음에 대해서만 활성화할 수 있습니다. `NetApp Volumes-Performance` 인스턴스로 사용하고 NFSv3, NFSv4.1 또는 이중 프로토콜 볼륨에 사용합니다. LDAP 지원 볼륨을 성공적으로 배포하려면 Google Cloud NetApp Volumes 볼륨과 동일한 지역에서 Active Directory 연결을 설정해야 합니다.

LDAP가 활성화되면 특정 시나리오에서 다음이 발생합니다.

- Google Cloud NetApp Volumes 프로젝트에 NFSv3 또는 NFSv4.1만 사용하는 경우 Active Directory 도메인 컨트롤러에 새 머신 계정이 생성되고 Google Cloud NetApp Volumes 의 LDAP 클라이언트는 머신 계정 자격 증명을 사용하여 Active Directory에 바인딩됩니다. NFS 볼륨과 기본 숨겨진 관리 공유에 대해 SMB 공유가 생성되지 않습니다(섹션 참조)"기본 숨겨진 공유") 공유 ACL을 제거했습니다.
- Google Cloud NetApp Volumes 프로젝트에 이중 프로토콜 볼륨을 사용하는 경우 SMB 액세스를 위해 생성된 단일 머신 계정만 사용하여 Google Cloud NetApp Volumes 의 LDAP 클라이언트를 Active Directory에

바인딩합니다. 추가적인 머신 계정이 생성되지 않습니다.

- 전용 SMB 볼륨이 별도로 생성된 경우(LDAP가 있는 NFS 볼륨이 활성화되기 전이나 후에), LDAP 바인딩을 위한 머신 계정은 SMB 머신 계정과 공유됩니다.
- NFS Kerberos도 활성화된 경우 두 개의 머신 계정이 생성됩니다. 하나는 SMB 공유 및/또는 LDAP 바인딩을 위한 것이고 다른 하나는 NFS Kerberos 인증을 위한 것입니다.

LDAP 쿼리

LDAP 바인딩은 암호화되지만 LDAP 쿼리는 일반 LDAP 포트 389를 사용하여 일반 텍스트로 전송됩니다. 이 잘 알려진 포트는 현재 Google Cloud NetApp Volumes 에서 변경할 수 없습니다. 결과적으로 네트워크에서 패킷 스니핑에 액세스할 수 있는 사람은 사용자 및 그룹 이름, 숫자 ID, 그룹 멤버십을 볼 수 있습니다.

하지만 Google Cloud VM은 다른 VM의 유니캐스트 트래픽을 감지할 수 없습니다. LDAP 트래픽에 적극적으로 참여하는 VM(바인딩이 가능한 VM)만 LDAP 서버의 트래픽을 볼 수 있습니다. Google Cloud NetApp Volumes 의 패킷 스니핑에 대한 자세한 내용은 다음 섹션을 참조하세요."패킷 스니핑/추적 고려사항."

LDAP 클라이언트 구성 기본값

Google Cloud NetApp Volumes 인스턴스에서 LDAP가 활성화된 경우 기본적으로 특정 구성 세부 정보가 포함된 LDAP 클라이언트 구성이 생성됩니다. 어떤 경우에는 옵션이 Google Cloud NetApp Volumes 에 적용되지 않거나 (지원되지 않음) 구성할 수 없습니다.

LDAP 클라이언트 옵션	그것이 하는 일	기본값	바꿀 수 있나요?
LDAP 서버 목록	쿼리에 사용할 LDAP 서버 이름이나 IP 주소를 설정합니다. 이는 Google Cloud NetApp Volumes 에는 사용되지 않습니다. 대신 Active Directory 도메인을 사용하여 LDAP 서버를 정의합니다.	설정되지 않음	아니요
Active Directory 도메인	LDAP 쿼리에 사용할 Active Directory 도메인을 설정합니다. Google Cloud NetApp Volumes DNS의 LDAP에 대한 SRV 레코드를 활용하여 도메인의 LDAP 서버를 찾습니다.	Active Directory 연결에 지정된 Active Directory 도메인으로 설정합니다.	아니요
선호하는 Active Directory 서버	LDAP에 사용할 기본 Active Directory 서버를 설정합니다. Google Cloud NetApp Volumes 에서는 지원되지 않습니다. 대신 Active Directory 사이트를 사용하여 LDAP 서버 선택을 제어하세요.	설정되지 않음.	아니요

LDAP 클라이언트 옵션	그것이 하는 일	기본값	바꿀 수 있나요**?**
SMB 서버 자격 증명을 사용하여 바인딩	SMB 머신 계정을 사용하여 LDAP에 바인딩합니다. 현재 Google Cloud NetApp Volumes 에서 지원되는 유일한 LDAP 바인딩 방법입니다.	진실	아니요
스키마 템플릿	LDAP 쿼리에 사용되는 스키마 템플릿입니다.	MS-AD-BIS	아니요
LDAP 서버 포트	LDAP 쿼리에 사용되는 포트 번호입니다. Google Cloud NetApp Volumes 현재 표준 LDAP 포트 389만 사용합니다. LDAPS/포트 636은 현재 지원되지 않습니다.	389	아니요
LDAPS가 활성화되어 있습니까?	쿼리 및 바인딩에 SSL(Secure Sockets Layer)을 통한 LDAP를 사용할지 여부를 제어합니다. 현재 Google Cloud NetApp Volumes 에서는 지원되지 않습니다.	거짓	아니요
쿼리 시간 초과(초)	쿼리 시간 초과. 쿼리가 지정된 값보다 오래 걸리면 쿼리가 실패합니다.	3	아니요
최소 바인드 인증 수준	지원되는 최소 바인드 수준입니다. Google Cloud NetApp Volumes LDAP 바인딩에 머신 계정을 사용하고 Active Directory는 기본적으로 익명 바인딩을 지원하지 않으므로 이 옵션은 보안에 적용되지 않습니다.	익명의	아니요
DN 바인딩	간단한 바인드를 사용할 때 바인드에 사용되는 사용자/고유 이름(DN)입니다. Google Cloud NetApp Volumes LDAP 바인딩에 머신 계정을 사용하며 현재 간단한 바인딩 인증을 지원하지 않습니다.	설정되지 않음	아니요
기본 DN	LDAP 검색에 사용되는 기본 DN입니다.	DN 형식(즉, DC=도메인, DC=로컬)으로 Active Directory 연결에 사용되는 Windows 도메인입니다.	아니요

LDAP 클라이언트 옵션	그것이 하는 일	기본값	바꿀 수 있나요**?**
기본 검색 범위	기본 DN 검색의 검색 범위입니다. 값에는 base, onelevel 또는 subtree가 포함될 수 있습니다. Google Cloud NetApp Volumes 서브트리 검색만 지원합니다.	서브트리	아니요
사용자 DN	LDAP 쿼리에 대한 사용자 검색이 시작되는 DN을 정의합니다. 현재 Google Cloud NetApp Volumes 에서는 지원되지 않으므로 모든 사용자 검색은 기본 DN에서 시작됩니다.	설정되지 않음	아니요
사용자 검색 범위	사용자 DN 검색의 검색 범위입니다. 값에는 base, onelevel 또는 subtree가 포함될 수 있습니다. Google Cloud NetApp Volumes 사용자 검색 범위 설정을 지원하지 않습니다.	서브트리	아니요
그룹 DN	LDAP 쿼리에 대한 그룹 검색이 시작되는 DN을 정의합니다. 현재 Google Cloud NetApp Volumes 에서는 지원되지 않으므로 모든 그룹 검색은 기본 DN에서 시작됩니다.	설정되지 않음	아니요
그룹 검색 범위	그룹 DN 검색의 검색 범위입니다. 값에는 base, onelevel 또는 subtree가 포함될 수 있습니다. Google Cloud NetApp Volumes 그룹 검색 범위 설정을 지원하지 않습니다.	서브트리	아니요
넷그룹 DN	LDAP 쿼리에 대한 netgroup 검색이 시작되는 DN을 정의합니다. 현재 Google Cloud NetApp Volumes 에서는 지원되지 않으므로 모든 netgroup 검색은 기본 DN에서 시작됩니다.	설정되지 않음	아니요

LDAP 클라이언트 옵션	그것이 하는 일	기본값	바꿀 수 있나요**?**
Netgroup 검색 범위	netgroup DN 검색의 검색 범위입니다. 값에는 base, onelevel 또는 subtree가 포함될 수 있습니다. Google Cloud NetApp Volumes netgroup 검색 범위 설정을 지원하지 않습니다.	서브트리	아니요
LDAP를 통해 start_tls 사용	포트 389를 통한 인증서 기반 LDAP 연결을 위해 Start TLS를 활용합니다. 현재 Google Cloud NetApp Volumes 에서는 지원되지 않습니다.	거짓	아니요
호스트별 netgroup 조회 활성화	모든 멤버를 나열하기 위해 넷그룹을 확장하는 대신 호스트 이름으로 넷그룹 조회를 활성화합니다. 현재 Google Cloud NetApp Volumes 에서는 지원되지 않습니다.	거짓	아니요
호스트별 넷그룹 DN	LDAP 쿼리에 대한 netgroup-by-host 검색이 시작되는 DN을 정의합니다. 현재 Google Cloud NetApp Volumes 에서는 Netgroup-by-host가 지원되지 않습니다.	설정되지 않음	아니요
호스트별 넷그룹 검색 범위	netgroup-by-host DN 검색의 검색 범위입니다. 값에는 base, onelevel 또는 subtree가 포함될 수 있습니다. 현재 Google Cloud NetApp Volumes 에서는 Netgroup-by-host가 지원되지 않습니다.	서브트리	아니요
클라이언트 세션 보안	LDAP에서 사용되는 세션 보안 수준(서명, 봉인 또는 없음)을 정의합니다. LDAP 서명은 Active Directory에서 요청하는 경우 NetApp Volumes-Performance에서 지원됩니다. NetApp Volumes-SW는 LDAP 서명을 지원하지 않습니다. 두 서비스 유형 모두 현재 봉인은 지원되지 않습니다.	None	아니요

LDAP 클라이언트 옵션	그것이 하는 일	기본값	바꿀 수 있나요**?**
LDAP 참조 추적	여러 LDAP 서버를 사용하는 경우, 참조 추적을 통해 클라이언트는 첫 번째 서버에서 항목을 찾을 수 없을 때 목록에 있는 다른 LDAP 서버를 참조할 수 있습니다. 현재 Google Cloud NetApp Volumes 에서는 지원되지 않습니다.	거짓	아니요
그룹 멤버십 필터	LDAP 서버에서 그룹 멤버십을 조회할 때 사용할 사용자 지정 LDAP 검색 필터를 제공합니다. 현재 Google Cloud NetApp Volumes 에서는 지원되지 않습니다.	설정되지 않음	아니요

비대칭 이름 매핑을 위한 **LDAP** 사용

Google Cloud NetApp Volumes 기본적으로 특별한 구성 없이 동일한 사용자 이름을 가진 Windows 사용자와 UNIX 사용자를 양방향으로 매핑합니다. Google Cloud NetApp Volumes 유효한 UNIX 사용자(LDAP 사용)를 찾을 수 있는 한 1:1 이름 매핑이 수행됩니다. 예를 들어, Windows 사용자인 경우 `johnsmith` 사용되면 Google Cloud NetApp Volumes UNIX 사용자를 찾을 수 있습니다. `johnsmith` LDAP에서 해당 사용자에 대한 이름 매핑이 성공하면 해당 사용자가 만든 모든 파일/폴더가 `johnsmith` 올바른 사용자 소유권과 영향을 미치는 모든 ACL을 표시합니다. `johnsmith` NAS 프로토콜에 관계없이 적용됩니다. 이것을 대칭적 이름 매핑이라고 합니다.

비대칭 이름 매핑은 Windows 사용자와 UNIX 사용자 ID가 일치하지 않는 경우입니다. 예를 들어, Windows 사용자인 경우 `johnsmith` UNIX ID를 가지고 있습니다 `jsmith` Google Cloud NetApp Volumes 변화에 대해 알릴 방법이 필요합니다. 현재 Google Cloud NetApp Volumes 정적 이름 매핑 규칙 생성을 지원하지 않으므로 파일 및 폴더의 적절한 소유권과 예상 권한을 보장하기 위해 Windows 및 UNIX ID 모두에 대한 사용자 ID를 조회하는 데 LDAP를 사용해야 합니다.

기본적으로 Google Cloud NetApp Volumes 포함됩니다. `LDAP` 비대칭 이름에 대해 LDAP를 사용하여 이름 매핑 기능을 제공하기 위해 인스턴스의 ns-switch에서 이름 맵 데이터베이스를 Google Cloud NetApp Volumes 찾는 내용을 반영하도록 일부 사용자/그룹 속성만 수정하면 됩니다.

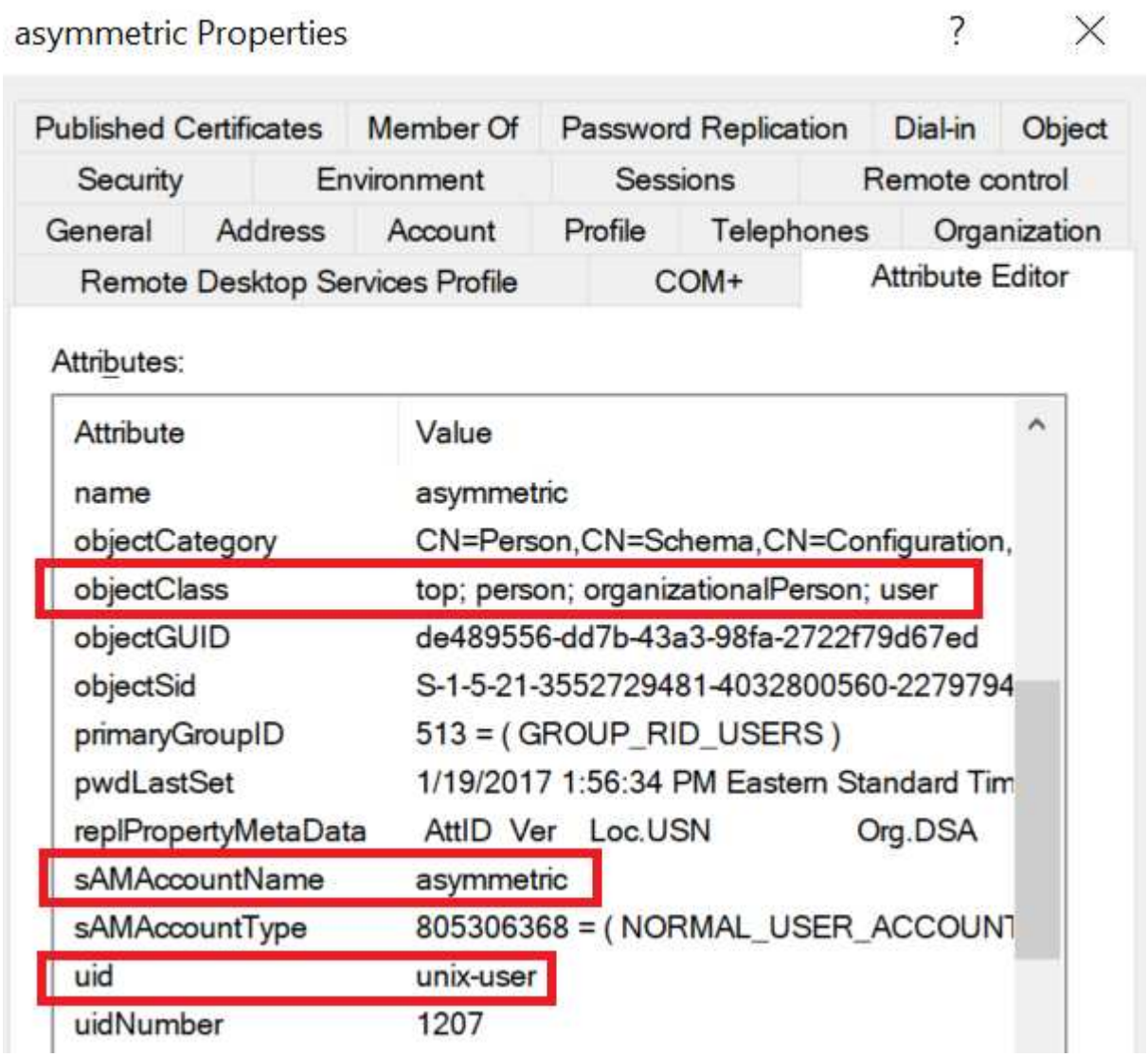
다음 표는 비대칭 이름 매핑 기능을 위해 LDAP에 어떤 속성을 채워야 하는지 보여줍니다. 대부분의 경우 Active Directory는 이미 이 작업을 수행하도록 구성되어 있습니다.

Google Cloud NetApp Volumes 속성	그것이 하는 일	**Google Cloud NetApp Volumes** 에서 이름 매핑에 사용하는 값
Windows에서 UNIX로의 objectClass	사용되는 객체의 유형을 지정합니다. (즉, 사용자, 그룹, posixAccount 등)	사용자를 포함해야 합니다(원하는 경우 여러 다른 값을 포함할 수 있음).
Windows에서 UNIX로의 속성	생성 시 Windows 사용자 이름을 정의합니다. Google Cloud NetApp Volumes Windows에서 UNIX로의 조회에 이를 사용합니다.	여기서는 변경할 필요가 없습니다. sAMAccountName은 Windows 로그인 이름과 동일합니다.
UID	UNIX 사용자 이름을 정의합니다.	원하는 UNIX 사용자 이름입니다.

Google Cloud NetApp Volumes 현재 LDAP 조회에서 도메인 접두사를 사용하지 않으므로 여러 도메인 LDAP 환경은 LDAP 네임맵 조회에서 제대로 작동하지 않습니다.

다음 예에서는 Windows 이름을 가진 사용자를 보여줍니다. `asymmetric` , UNIX 이름 `unix-user` 그리고 SMB와 NFS 모두에서 파일을 쓸 때의 동작입니다.

다음 그림은 Windows 서버에서 LDAP 속성이 어떻게 보이는지 보여줍니다.



NFS 클라이언트에서 UNIX 이름은 쿼리할 수 있지만 Windows 이름은 쿼리할 수 없습니다.

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

NFS에서 파일이 작성될 때 `unix-user` 다음은 NFS 클라이언트의 결과입니다.

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

Windows 클라이언트에서 파일 소유자가 적절한 Windows 사용자로 설정되어 있는 것을 확인할 수 있습니다.

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

반대로 Windows 사용자가 생성한 파일 `asymmetric` 다음 텍스트에 표시된 것처럼 SMB 클라이언트에서 적절한 UNIX 소유자가 표시됩니다.

중소기업(SMB):

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS:

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

LDAP 채널 바인딩

Windows Active Directory 도메인 컨트롤러의 취약점으로 인해 "Microsoft 보안 권고 ADV190023" DC가 LDAP 바인딩을 허용하는 방식을 변경합니다.

Google Cloud NetApp Volumes 에 미치는 영향은 모든 LDAP 클라이언트에 미치는 영향과 동일합니다. Google Cloud NetApp Volumes 현재 채널 바인딩을 지원하지 않습니다. Google Cloud NetApp Volumes 기본적으로 협상을 통해 LDAP 서명을 지원하므로 LDAP 채널 바인딩은 문제가 되지 않습니다. 채널 바인딩이 활성화된 상태에서 LDAP에 바인딩하는 데 문제가 있는 경우 ADV190023의 수정 단계에 따라 Google Cloud NetApp Volumes 에서 LDAP 바인딩이 성공하도록 하세요.

DNS

Active Directory와 Kerberos는 모두 호스트 이름에서 IP로, IP에서 호스트 이름으로의 확인을 위해 DNS에 종속됩니다. DNS를 사용하려면 포트 53이 열려 있어야 합니다. Google Cloud NetApp Volumes DNS 레코드를

수정하지 않으며 현재 사용을 지원하지 않습니다. "동적 DNS" 네트워크 인터페이스에서.

Active Directory DNS를 구성하여 DNS 레코드를 업데이트할 수 있는 서버를 제한할 수 있습니다. 자세한 내용은 다음을 참조하세요. "보안 Windows DNS" .

Google 프로젝트 내의 리소스는 기본적으로 Google Cloud DNS를 사용하며, 이는 Active Directory DNS와 연결되지 않습니다. Cloud DNS를 사용하는 클라이언트는 Google Cloud NetApp Volumes 에서 반환된 UNC 경로를 확인할 수 없습니다. Active Directory 도메인에 가입된 Windows 클라이언트는 Active Directory DNS를 사용하도록 구성되며 이러한 UNC 경로를 확인할 수 있습니다.

클라이언트를 Active Directory에 연결하려면 Active Directory DNS를 사용하도록 클라이언트의 DNS 구성을 설정해야 합니다. 선택적으로 Cloud DNS가 요청을 Active Directory DNS로 전달하도록 구성할 수 있습니다. 자세한 내용은 "내 클라이언트가 SMB NetBIOS 이름을 확인할 수 없는 이유는 무엇입니까?"을(를) 참조하십시오.

Google Cloud NetApp Volumes 현재 DNSSEC를 지원하지 않으며 DNS 쿼리는 일반 텍스트로 수행됩니다.

파일 접근 감사

현재 Google Cloud NetApp Volumes 에서는 지원되지 않습니다.

바이러스 백신 보호

클라이언트에서 NAS 공유에 대한 Google Cloud NetApp Volumes 에서 바이러스 백신 검사를 수행해야 합니다. 현재 Google Cloud NetApp Volumes 에는 기본 바이러스 백신 통합이 없습니다.

서비스 운영

Google Cloud NetApp Volumes 팀은 Google Cloud의 백엔드 서비스를 관리하고 다양한 전략을 사용하여 플랫폼을 보호하고 원치 않는 액세스를 방지합니다.

각 고객은 기본적으로 다른 고객으로부터 접근이 차단된 고유한 서브넷을 갖고, Google Cloud NetApp Volumes 의 모든 테넌트는 완전한 데이터 격리를 위해 자체 네임스페이스와 VLAN을 갖습니다. 사용자가 인증된 후, 서비스 제공 엔진(SDE)은 해당 테넌트에 대한 구성 데이터만 읽을 수 있습니다.

물리적 보안

적절한 사전 승인을 받은 경우, 현장 엔지니어와 NetApp 인증 현장 지원 엔지니어(FSE)만이 실제 작업을 위해 케이지와 랙에 접근할 수 있습니다. 저장 및 네트워크 관리가 허용되지 않습니다. 이러한 현장 리소스만이 하드웨어 유지 관리 작업을 수행할 수 있습니다.

현장 엔지니어의 경우 랙 ID와 장치 위치(RU)를 포함하는 작업 명세서(SOW)에 대한 티켓이 제출되고, 티켓에는 다른 모든 세부 정보가 포함됩니다. NetApp FSE의 경우 COLO에 현장 방문 티켓을 제출해야 하며, 티켓에는 감사 목적으로 방문자의 세부 정보, 날짜 및 시간이 포함되어야 합니다. FSE의 SOW는 NetApp 에 내부적으로 전달됩니다.

운영팀

Google Cloud NetApp Volumes 의 운영 팀은 Google Cloud NetApp Volumes 의 프로덕션 엔지니어링 및 사이트 안정성 엔지니어(SRE)와 하드웨어의 NetApp 현장 지원 엔지니어 및 파트너로 구성됩니다. 모든 운영팀 구성원은 Google Cloud에서의 업무에 대한 인증을 받았으며, 제기된 모든 티켓에 대한 자세한 업무 기록이 보관됩니다. 또한, 각 결정이 적절하게 검토되도록 엄격한 변경 관리 및 승인 절차가 마련되어 있습니다.

SRE 팀은 제어 평면을 관리하고, Google Cloud NetApp Volumes 에서 UI 요청에서 백엔드 하드웨어 및 소프트웨어로 데이터가 라우팅되는 방식을 관리합니다. SRE 팀은 볼륨과 inode 최대값과 같은 시스템 리소스도 관리합니다. SRE는 고객 데이터와 상호 작용하거나 고객 데이터에 액세스할 수 없습니다. SRE는 백엔드 하드웨어에 대한 새로운 디스크나 메모리 교체 요청과 같은 반품 물품 승인(RMA)에 대한 조정도 제공합니다.

고객의 책임

Google Cloud NetApp Volumes 고객은 조직의 Active Directory 및 사용자 역할 관리와 볼륨 및 데이터 작업도 관리합니다. 고객은 관리 역할을 가질 수 있으며 NetApp 과 Google Cloud에서 제공하는 두 가지 사전 정의된 역할(관리자 및 뷰어)을 사용하여 동일한 Google Cloud 프로젝트 내의 다른 최종 사용자에게 권한을 위임할 수 있습니다.

관리자는 고객 프로젝트 내의 모든 VPC를 고객이 적절하다고 판단하는 Google Cloud NetApp Volumes 에 피어링할 수 있습니다. Google Cloud 마켓플레이스 구독에 대한 액세스를 관리하고 데이터 플레인에 액세스할 수 있는 VPC를 관리하는 것은 고객의 책임입니다.

악성 **SRE** 보호

발생할 수 있는 우려 사항 중 하나는 Google Cloud NetApp Volumes 악의적인 SRE가 있거나 SRE 자격 증명이 손상된 경우를 어떻게 보호하는가입니다.

프로덕션 환경에 접근할 수 있는 사람은 제한된 수의 SRE 직원뿐입니다. 관리자 권한은 소수의 숙련된 관리자에게만 제한됩니다. Google Cloud NetApp Volumes 프로덕션 환경에서 모든 사람이 수행하는 모든 작업은 기록되며, 기준에 대한 이상이나 의심스러운 활동은 보안 정보 및 이벤트 관리(SIEM) 위협 인텔리전스 플랫폼을 통해 감지됩니다. 그 결과, Google Cloud NetApp Volumes 백엔드에 너무 큰 피해가 발생하기 전에 악의적인 활동을 추적하고 완화할 수 있습니다.

볼륨 수명 주기

Google Cloud NetApp Volumes 볼륨 내의 데이터가 아닌 서비스 내의 객체만 관리합니다. 볼륨에 액세스하는 클라이언트만 데이터, ACL, 파일 소유자 등을 관리할 수 있습니다. 이러한 볼륨의 데이터는 저장 시 암호화되며 액세스는 Google Cloud NetApp Volumes 인스턴스의 테넌트로 제한됩니다.

Google Cloud NetApp Volumes 의 볼륨 수명 주기는 생성-업데이트-삭제입니다. 볼륨은 볼륨이 삭제될 때까지 볼륨의 스냅샷 사본을 보관하며, 검증된 Google Cloud NetApp Volumes 관리자만이 Google Cloud NetApp Volumes 에서 볼륨을 삭제할 수 있습니다. 관리자가 볼륨 삭제를 요청하면 삭제를 확인하기 위해 볼륨 이름을 입력하는 추가 단계가 필요합니다. 볼륨을 삭제하면 해당 볼륨은 사라지고 복구할 수 없습니다.

Google Cloud NetApp Volumes 계약이 종료되는 경우 NetApp 특정 기간이 지난 후 볼륨을 삭제하도록 표시합니다. 해당 기간이 만료되기 전에 고객의 요청에 따라 볼륨을 복구할 수 있습니다.

인증

Google Cloud용 Google Cloud NetApp Volumes 현재 ISO/IEC 27001:2013 및 ISO/IEC 27018:2019 표준에 따라 인증을 받았습니다. 이 서비스는 최근 SOC2 유형 I 인증 보고서도 받았습니다. NetApp 데이터 보안 및 개인 정보 보호에 대한 약속에 대한 자세한 내용은 다음을 참조하세요. "규정 준수: 데이터 보안 및 데이터 개인 정보 보호" .

GDPR

개인 정보 보호 및 GDPR 준수에 대한 당사의 약속은 유럽 위원회가 제공하는 "표준 계약 조항"이 포함된 당사 "고객 Data Processing 추가 조항" 등 여러 "고객 계약"에서 확인하실 수 있습니다. 당사는 또한 기업 행동 강령에 명시된 핵심 가치를 바탕으로 개인 정보 보호 정책에서도 이러한 약속을 이행합니다.

추가 정보 및 연락처 정보

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 문서 및/또는 웹사이트를 검토하세요.

- Google Cloud Google Cloud NetApp Volumes Cloud 설명서

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- Google 개인 서비스 액세스

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- NetApp 제품 설명서

  "https://www.netapp.com/support-and-training/documentation/"

- 암호화 검증 모듈 프로그램 NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- 랜섬웨어에 대한 NetApp 솔루션

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- TR-4616: ONTAP 의 NFS Kerberos

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

문의하기

이 기술 보고서를 개선할 수 있는 방법을 알려주시기 바랍니다.

doccomments@netapp.com으로 문의하세요. 제목에 기술 보고서 4918을 포함하세요.

NetApp Disaster Recovery

VMware 워크로드를 보호하기 위한 SnapCenter 플러그인 및 NetApp Backup and Recovery를 활용한 VMware용 3-2-1 데이터 보호

3-2-1 백업 전략은 업계에서 인정된 데이터 보호 방법으로, 귀중한 데이터를 보호하기 위한 포괄적인 접근 방식을 제공합니다. 이러한 전략은 신뢰할 수 있으며 예상치 못한 재해가 발생하더라도 여전히 사용 가능한 데이터 사본이 유지된다는 점을 보장합니다.

개요

이 전략은 세 가지 기본 규칙으로 구성됩니다.

1. 최소한 3개의 데이터 사본을 보관하세요. 이렇게 하면 사본 하나가 손실되거나 손상되더라도 최소한 두 개의 사본이 남아 있어 대체할 수 있습니다.
2. 두 개의 백업 사본을 서로 다른 저장 매체나 장치에 저장하세요. 저장 매체를 다양화하면 장치별 또는 매체별 오류로부터 보호하는 데 도움이 됩니다. 한 장치가 손상되거나 한 유형의 미디어가 실패하더라도 다른 백업 사본은

영향을 받지 않습니다.

3. 마지막으로, 최소한 하나의 백업 사본이 오프사이트에 있는지 확인하세요. 원격지 보관은 화재나 홍수와 같은 국지적 재해에 대비한 안전장치 역할을 하며, 이로 인해 현장 사본을 사용할 수 없게 될 수 있습니다.

이 솔루션 문서에서는 온프레미스 가상 머신의 기본 및 보조 백업을 생성하기 위해 SnapCenter Plug-in for VMware vSphere (SCV)를 사용하고, 데이터의 복사본을 클라우드 스토리지 또는 StorageGRID에 백업하기 위해 가상 머신용 NetApp Backup and Recovery를 사용하는 3-2-1 백업 솔루션을 다룹니다.

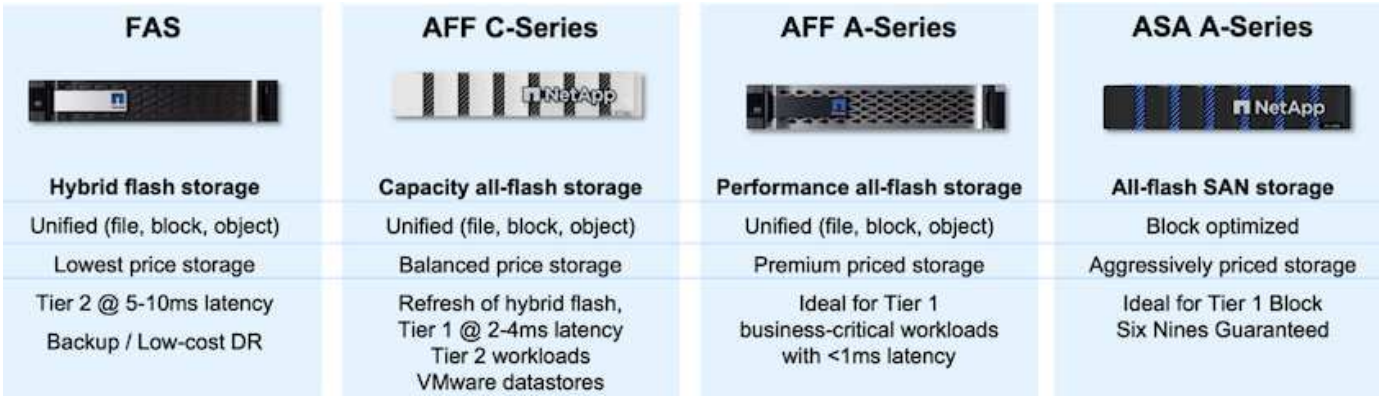
사용 사례

이 솔루션은 다음과 같은 사용 사례를 해결합니다.

- SnapCenter Plug-in for VMware vSphere 사용하여 온프레미스 가상 머신과 데이터 저장소를 백업하고 복원합니다.
- 가상 머신용 NetApp Backup and Recovery를 사용하여 ONTAP 클러스터에서 호스팅되고 오브젝트 스토리지에 백업되는 온프레미스 가상 머신 및 데이터스토어의 백업 및 복원.

NetApp ONTAP 데이터 스토리지

ONTAP 은 SAN이나 NAS 프로토콜을 통해 액세스하든 통합 스토리지를 제공하는 NetApp의 업계 최고 스토리지 솔루션입니다. 3-2-1 백업 전략은 온프레미스 데이터가 여러 미디어 유형에서 보호되도록 보장하며 NetApp 고속 플래시부터 저렴한 미디어까지 다양한 플랫폼을 제공합니다.



NetApp의 모든 하드웨어 플랫폼에 대한 자세한 내용은 다음을 확인하세요. "NetApp 데이터 스토리지" .

SnapCenter Plug-in for VMware vSphere

VMware vSphere용 SnapCenter 플러그인은 VMware vSphere와 긴밀하게 통합된 데이터 보호 제품으로, 가상 머신의 백업과 복원을 쉽게 관리할 수 있도록 해줍니다. 해당 솔루션의 일부로 SnapMirror 보조 ONTAP 스토리지 클러스터에 가상 머신 데이터의 두 번째 변경 불가능한 백업 사본을 생성하는 빠르고 안정적인 방법을 제공합니다. 이 아키텍처를 구현하면 가상 머신 복원 작업을 기본 또는 보조 백업 위치에서 쉽게 시작할 수 있습니다.

SCV는 OVA 파일을 사용하여 Linux 가상 어플라이언스로 배포됩니다. 이 플러그인은 이제 원격 플러그인 아키텍처를 사용합니다. 원격 플러그인은 vCenter 서버 외부에서 실행되며 SCV 가상 어플라이언스에서 호스팅됩니다.

SCV에 대한 자세한 내용은 다음을 참조하세요. "SnapCenter Plug-in for VMware vSphere 설명서" .

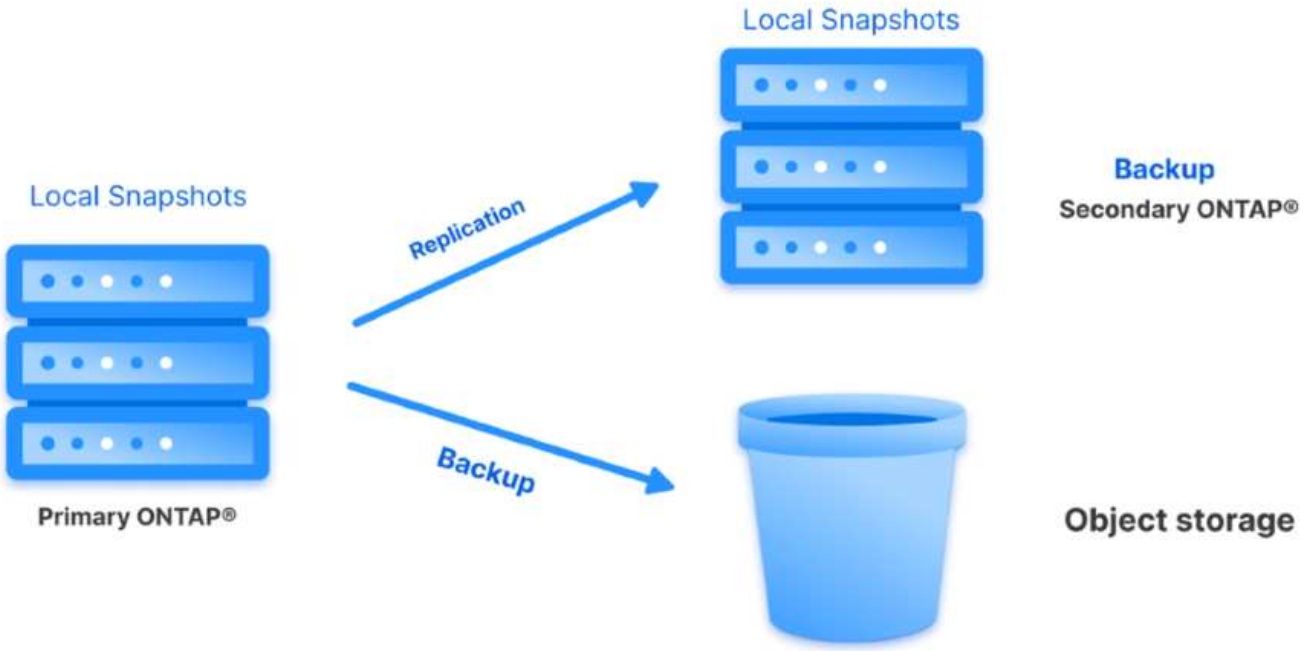
VMware 워크로드를 보호하기 위한 NetApp Backup and Recovery

NetApp Backup and Recovery는 클라우드 기반 데이터 관리 툴로, 온프레미스 및 클라우드 환경 전반에 걸쳐 다양한

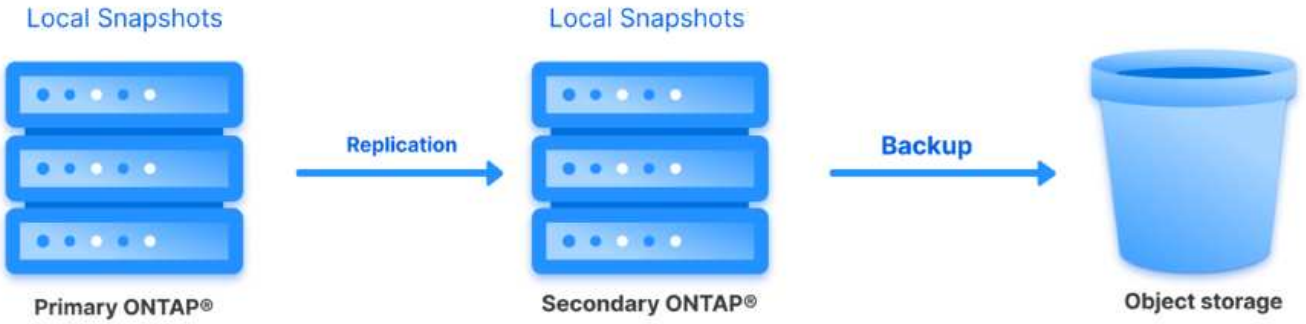
백업 및 복구 작업을 위한 단일 컨트롤 플레인을 제공합니다. NetApp Backup and Recovery for VM 제품군의 일부로, SnapCenter Plugin for VMware vSphere(온프레미스)와 통합하여 데이터 사본을 클라우드의 오브젝트 스토리지로 확장하는 기능이 있습니다. 이를 통해 기본 또는 2차 스토리지 백업을 소스로 하는 오프사이트 데이터의 세 번째 사본이 생성됩니다. NetApp Backup and Recovery for VMs를 사용하면 이 두 온프레미스 위치 중 하나에서 데이터 사본을 전송하는 스토리지 정책을 손쉽게 설정할 수 있습니다.

NetApp Backup and Recovery에서 기본 백업과 보조 백업 중 하나를 소스로 선택하면 다음 두 가지 토폴로지 중 하나가 구현됩니다:

팬아웃 토폴로지 – SnapCenter Plug-in for VMware vSphere에서 백업을 시작하면 로컬 스냅샷이 즉시 생성됩니다. 그런 다음 SCV는 SnapMirror 작업을 시작하여 가장 최근 스냅샷을 보조 ONTAP 클러스터로 복제합니다. NetApp Backup and Recovery에서 정책은 선택한 클라우드 공급자의 오브젝트 스토리지로 전송할 데이터의 스냅샷 복사본 소스로 기본 ONTAP 클러스터를 지정합니다.

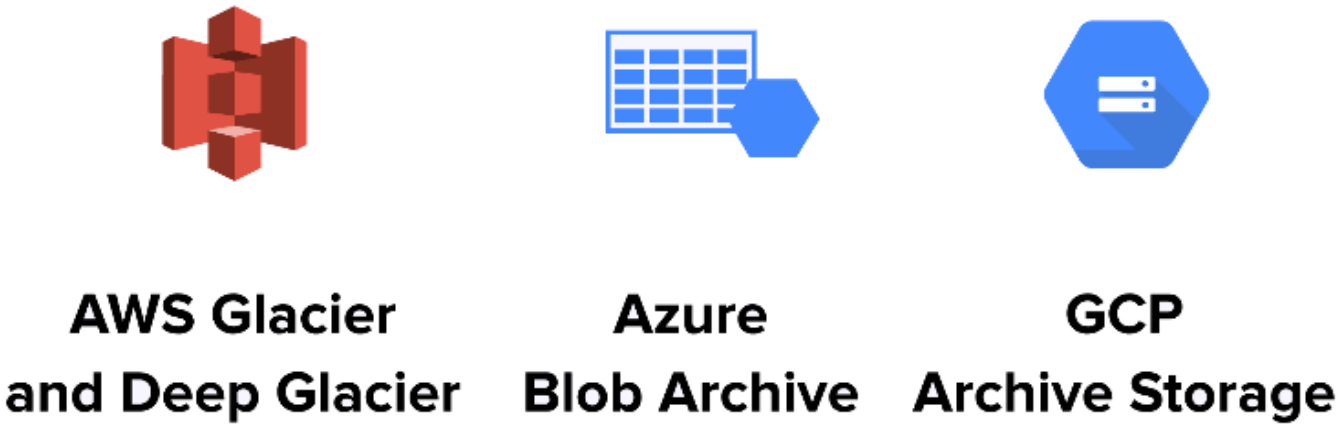


계단식 토폴로지 – SCV를 사용하여 기본 및 보조 데이터 복사본을 생성하는 방법은 위에서 언급한 팬아웃 토폴로지와 동일합니다. 단, 이번에는 NetApp Backup and Recovery에서 오브젝트 스토리지에 대한 백업이 보조 ONTAP 클러스터에서 시작되도록 지정하는 정책을 생성합니다.



NetApp Backup and Recovery는 온프레미스 ONTAP 스냅샷의 백업 복사본을 AWS Glacier, Azure Blob 및 GCP

Archive 스토리지에 생성할 수 있습니다.



또한 NetApp StorageGRID 개체 스토리지 백업 대상으로 사용할 수 있습니다. StorageGRID 에 대한 자세한 내용은 다음을 참조하세요. "StorageGRID 랜딩 페이지" .

▼ 솔루션 배포 개요

이 목록은 SCV 및 NetApp Console에서 이 솔루션을 구성하고 백업 및 복원 작업을 실행하는 데 필요한 주요 단계를 제공합니다:

1. 기본 및 보조 데이터 복사에 사용할 ONTAP 클러스터 간의 SnapMirror 관계를 구성합니다.
2. VMware vSphere에 대한 SnapCenter 플러그인을 구성합니다.
   a. 스토리지 시스템 추가
   b. 백업 정책 생성
   c. 리소스 그룹 생성
   d. 백업을 먼저 실행하여 백업 작업을 시작합니다.
3. 가상 머신용 NetApp Backup and Recovery 구성
   a. 작업 환경 추가
   b. SCV 및 vCenter 어플라이언스 알아보기
   c. 백업 정책 생성
   d. 백업 활성화
4. SCV를 사용하여 기본 및 보조 저장소에서 가상 머신을 복원합니다.
5. NetApp 콘솔을 사용하여 오브젝트 스토리지에서 가상 머신을 복원합니다.

▼ 필수 조건

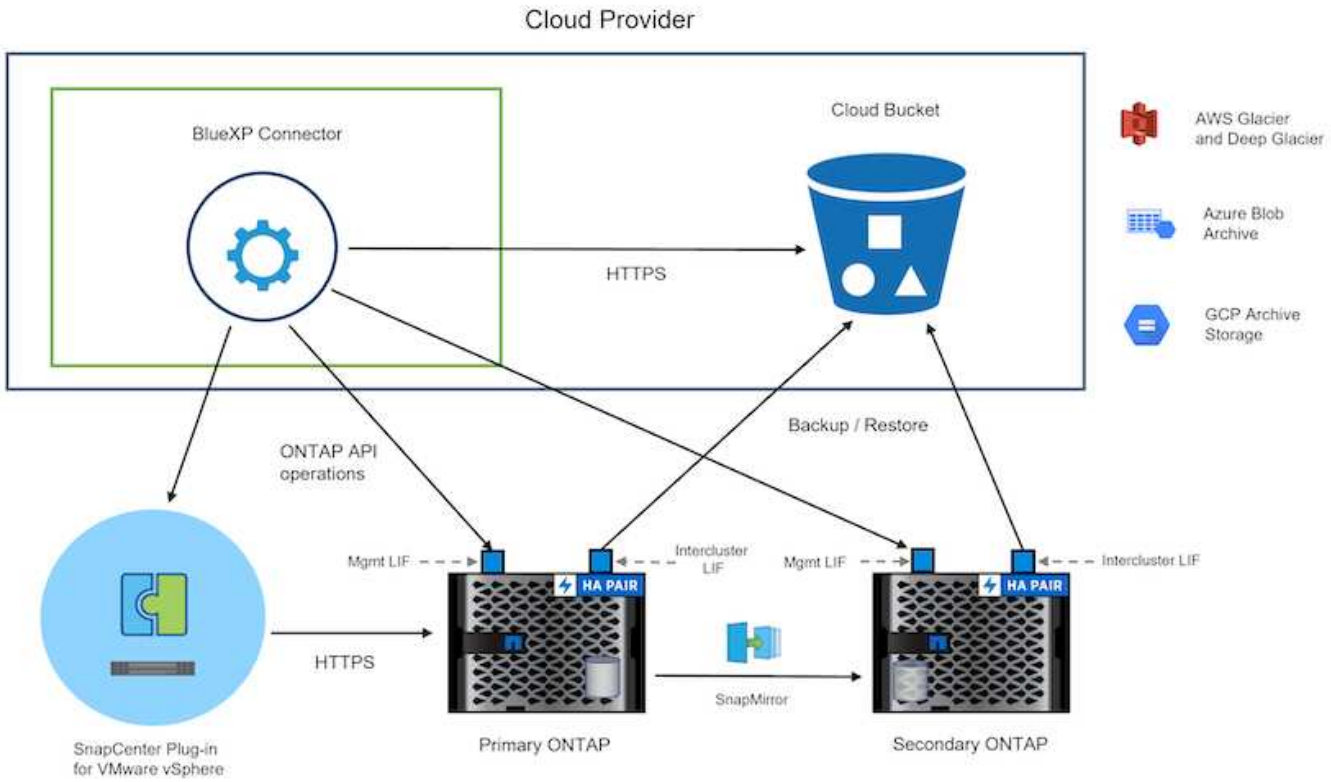
이 솔루션의 목적은 NetApp ONTAP 에서 호스팅되는 NFS 데이터스토어에 위치하고 VMware vSphere에서 실행되는 가상 머신의 데이터 보호를 시연하는 것입니다. 이 솔루션은 다음 구성 요소가 구성되어 사용할 준비가 되었다고 가정합니다.

1. VMware vSphere에 연결된 NFS 또는 VMFS 데이터 저장소가 있는 ONTAP 스토리지 클러스터입니다. NFS와 VMFS 데이터 저장소가 모두 지원됩니다. 이 솔루션에는 NFS 데이터 저장소가 활용되었습니다.
2. NFS 데이터 저장소에 사용되는 볼륨에 대해 SnapMirror 관계가 설정된 보조 ONTAP 스토리지 클러스터입니다.

3. 오브젝트 스토리지 백업에 사용되는 클라우드 공급자용 콘솔 에이전트가 설치되었습니다.
4. 백업할 가상 머신은 기본 ONTAP 스토리지 클러스터에 있는 NFS 데이터 저장소에 있습니다.
5. 콘솔 에이전트와 온프레미스 ONTAP 스토리지 클러스터 관리 인터페이스 간의 네트워크 연결.
6. 콘솔 에이전트와 온프레미스 SCV 어플라이언스 VM 간, 그리고 콘솔 에이전트와 vCenter 간의 네트워크 연결.
7. 온프레미스 ONTAP 클러스터 간 LIF와 개체 스토리지 서비스 간의 네트워크 연결입니다.
8. 기본 및 보조 ONTAP 스토리지 클러스터에서 관리 SVM에 대한 DNS가 구성되었습니다. 자세한 내용은 다음을 참조하세요. "호스트 이름 확인을 위한 DNS 구성" .

고수준 아키텍처

이 솔루션의 테스트/검증은 최종 배포 환경과 일치할 수도 있고 일치하지 않을 수도 있는 실험실에서 수행되었습니다.



솔루션 배포

본 솔루션에서는 SnapCenter Plug-in for VMware vSphere와 Backup and Recovery를 활용하여 온프레미스 데이터 센터에 위치한 VMware vSphere 클러스터 내의 Windows 및 Linux 가상 머신을 백업 및 복구하는 솔루션을 배포하고 검증하는 방법에 대한 자세한 지침을 제공합니다. 이 구성에서 가상 머신은 ONTAP A300 스토리지 클러스터에서 호스팅되는 NFS 데이터스토어에 저장됩니다. 또한, 별도의 ONTAP A300 스토리지 클러스터는 SnapMirror를 사용하여 복제된 볼륨의 2차 대상 역할을 합니다. 또한, Amazon Web Services 및 Azure Blob에서 호스팅되는 오브젝트 스토리지가 데이터의 세 번째 복사본을 위한 대상으로 사용되었습니다.

SCV에서 관리하는 백업의 보조 복사본에 대한 SnapMirror 관계 생성과 SCV 및 NetApp Console 모두에서의 백업 작업 구성에 대해 살펴보겠습니다.

SnapCenter Plug-in for VMware vSphere 에 대한 자세한 내용은 다음을 참조하세요. "SnapCenter Plug-in for VMware vSphere 설명서" .

백업 및 복구에 대한 자세한 내용은 "백업 및 복구 문서"를 참조하십시오.

ONTAP 클러스터 간 SnapMirror 관계 설정

SnapCenter Plug-in for VMware vSphere ONTAP SnapMirror 기술을 사용하여 보조 SnapMirror 및/또는 SnapVault 복사본을 보조 ONTAP 클러스터로 전송하는 것을 관리합니다.

SCV 백업 정책에는 SnapMirror 또는 SnapVault 관계를 사용하는 옵션이 있습니다. 가장 큰 차이점은 SnapMirror 옵션을 사용할 경우 정책에서 백업을 위해 구성된 보존 일정이 기본 및 보조 위치에서 동일하다는 것입니다. SnapVault 보관을 위해 설계되었으며, 이 옵션을 사용하면 보조 ONTAP 스토리지 클러스터의 스냅샷 복사본에 대해 SnapMirror 관계와 별도의 보존 일정을 설정할 수 있습니다.

SnapMirror 관계 설정은 많은 단계가 자동화되는 NetApp Console에서 수행하거나, System Manager 및 ONTAP CLI를 사용하여 수행할 수 있습니다. 이러한 모든 방법은 아래에서 설명합니다.

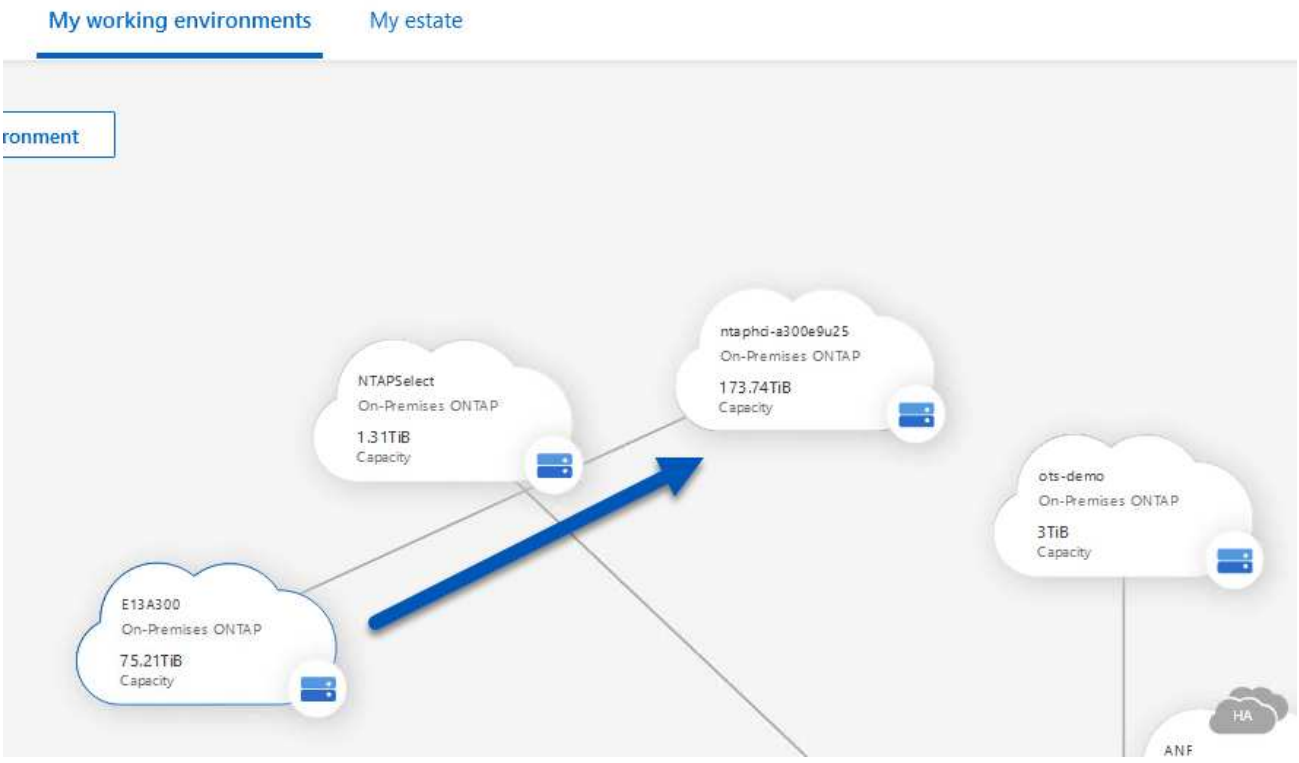
NetApp Console을 사용하여 SnapMirror 관계 설정

NetApp Console에서 다음 단계를 완료해야 합니다:

▼ 1차 및 2차 ONTAP 스토리지 시스템에 대한 복제 설정

먼저 NetApp Console에 로그인하고 시스템으로 이동하십시오.

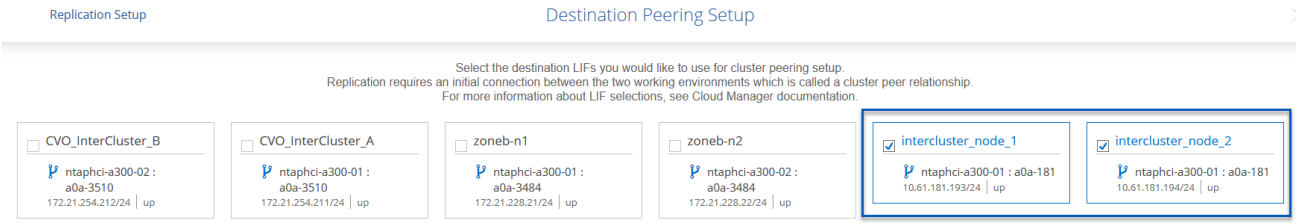
1. 소스(기본) ONTAP 스토리지 시스템을 대상(보조) ONTAP 스토리지 시스템으로 끌어서 놓습니다.



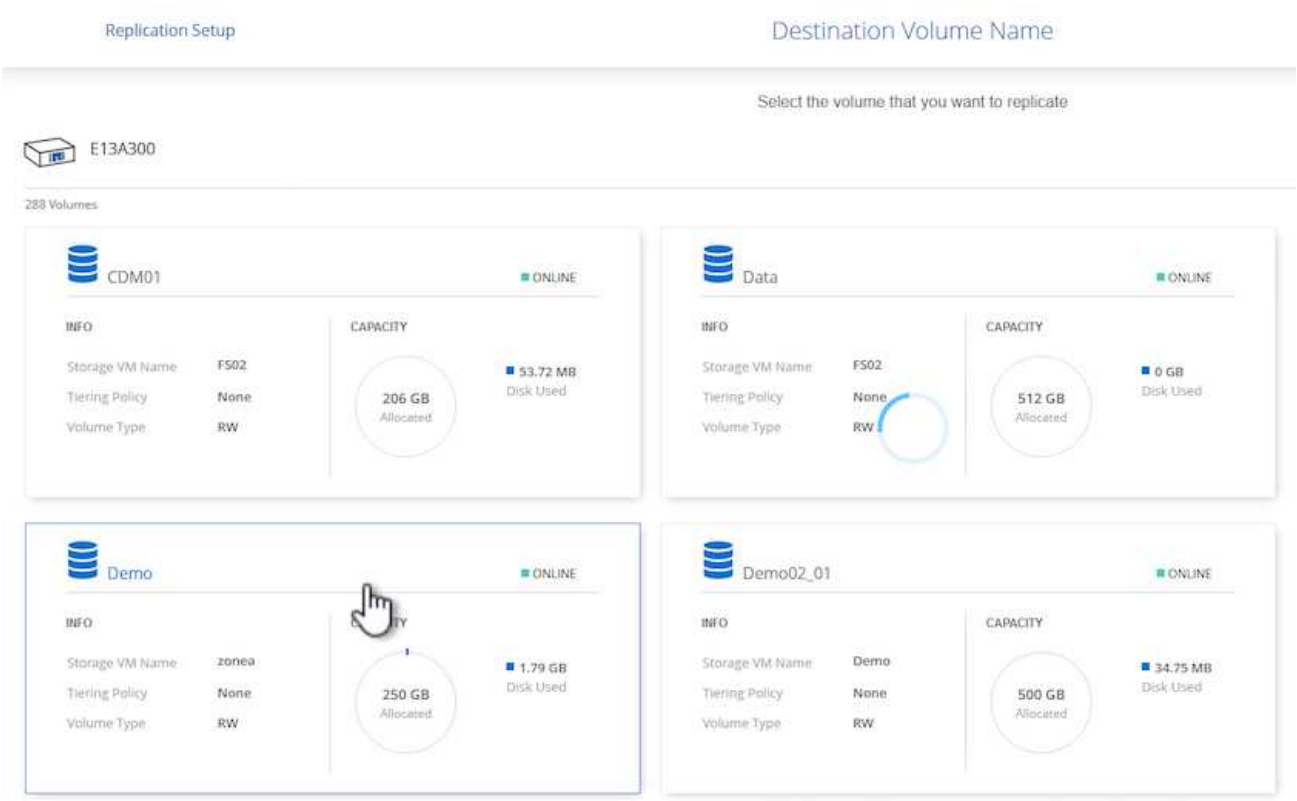
2. 나타나는 메뉴에서 *복제*를 선택합니다.



3. 대상 피어링 설정 페이지에서 스토리지 시스템 간 연결에 사용할 대상 Intercluster LIF를 선택합니다.

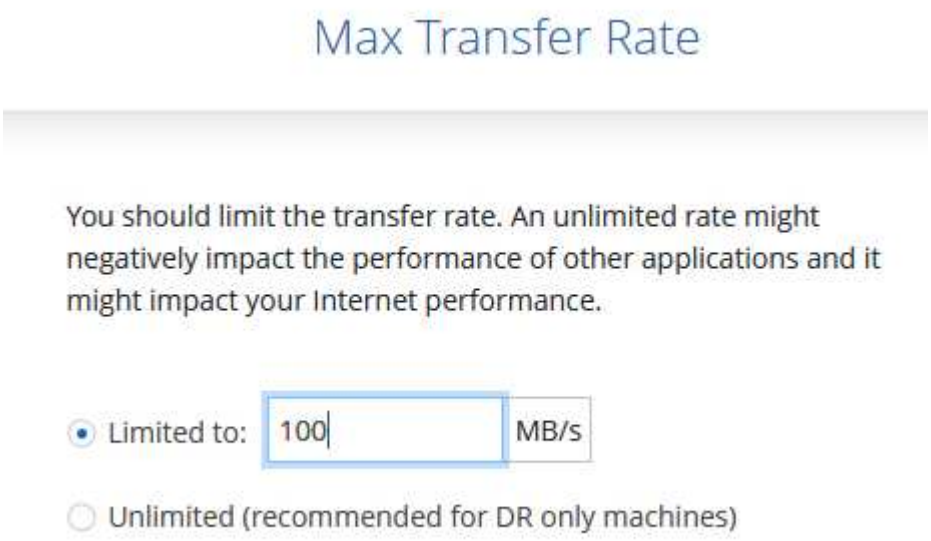


4. 대상 볼륨 이름 페이지에서 먼저 소스 볼륨을 선택한 다음 대상 볼륨 이름을 입력하고 대상 SVM과 집계를 선택합니다. 계속하려면 *다음*을 클릭하세요.

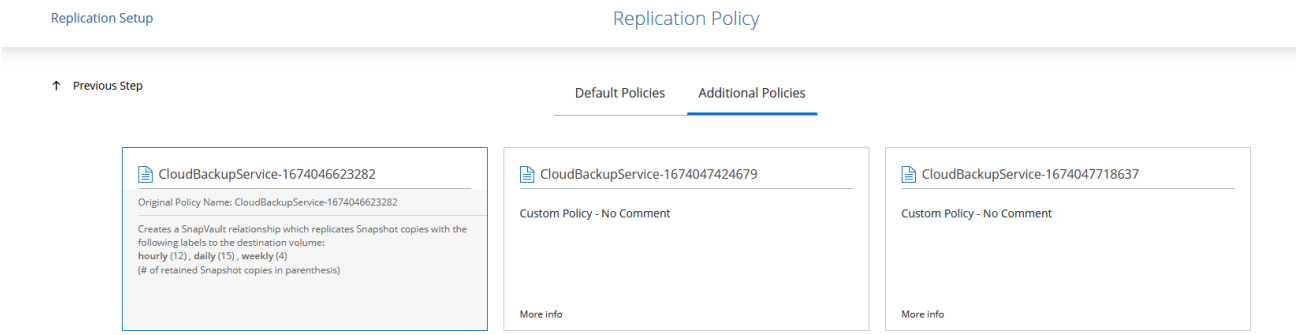




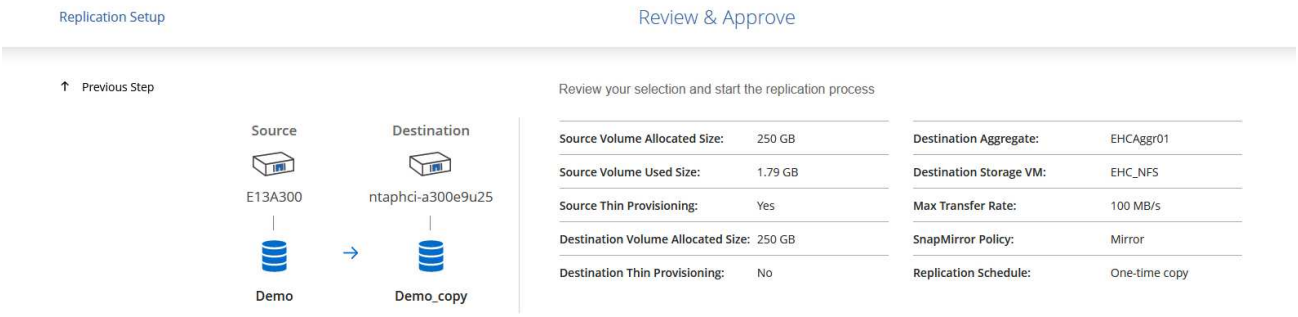
5. 복제가 발생할 최대 전송 속도를 선택합니다.



6. 보조 백업의 보존 일정을 결정할 정책을 선택하세요. 이 정책은 사전에 만들 수 있습니다(아래의 스냅샷 보존 정책 만들기 단계의 수동 프로세스 참조) 또는 원하는 경우 사후에 변경할 수 있습니다.



7. 마지막으로 모든 정보를 검토하고 시작 버튼을 클릭하여 복제 설정 프로세스를 시작합니다.



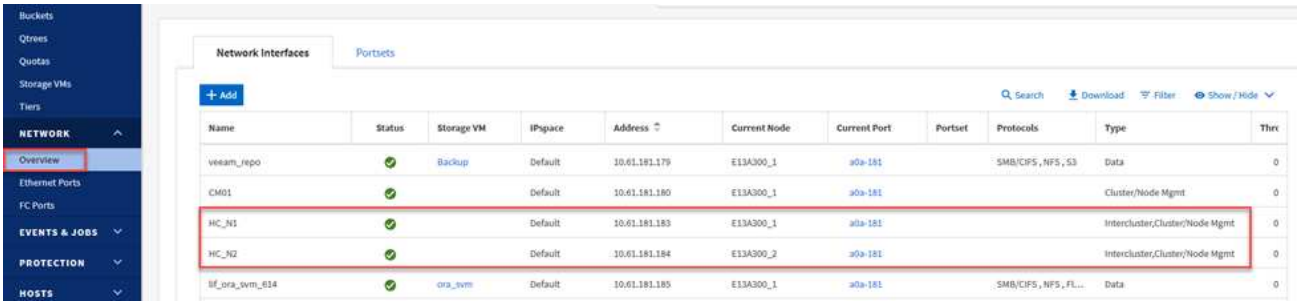
System Manager 및 ONTAP CLI를 사용하여 SnapMirror 관계 설정

SnapMirror 관계를 설정하는 데 필요한 모든 단계는 System Manager나 ONTAP CLI를 사용하여 수행할 수 있습니다. 다음 섹션에서는 두 가지 방법에 대한 자세한 정보를 제공합니다.

▼ 소스 및 대상 **Intercluster** 논리 인터페이스를 기록합니다.

소스 및 대상 ONTAP 클러스터의 경우 System Manager나 CLI에서 클러스터 간 LIF 정보를 검색할 수 있습니다.

1. ONTAP System Manager에서 네트워크 개요 페이지로 이동하여 FSx가 설치된 AWS VPC와 통신하도록 구성된 유형: 클러스터 간 IP 주소를 검색합니다.



2. CLI를 사용하여 Intercluster IP 주소를 검색하려면 다음 명령을 실행하세요.

```
ONTAP-Dest::> network interface show -role intercluster
```

▼ **ONTAP** 클러스터 간 클러스터 피어링 설정

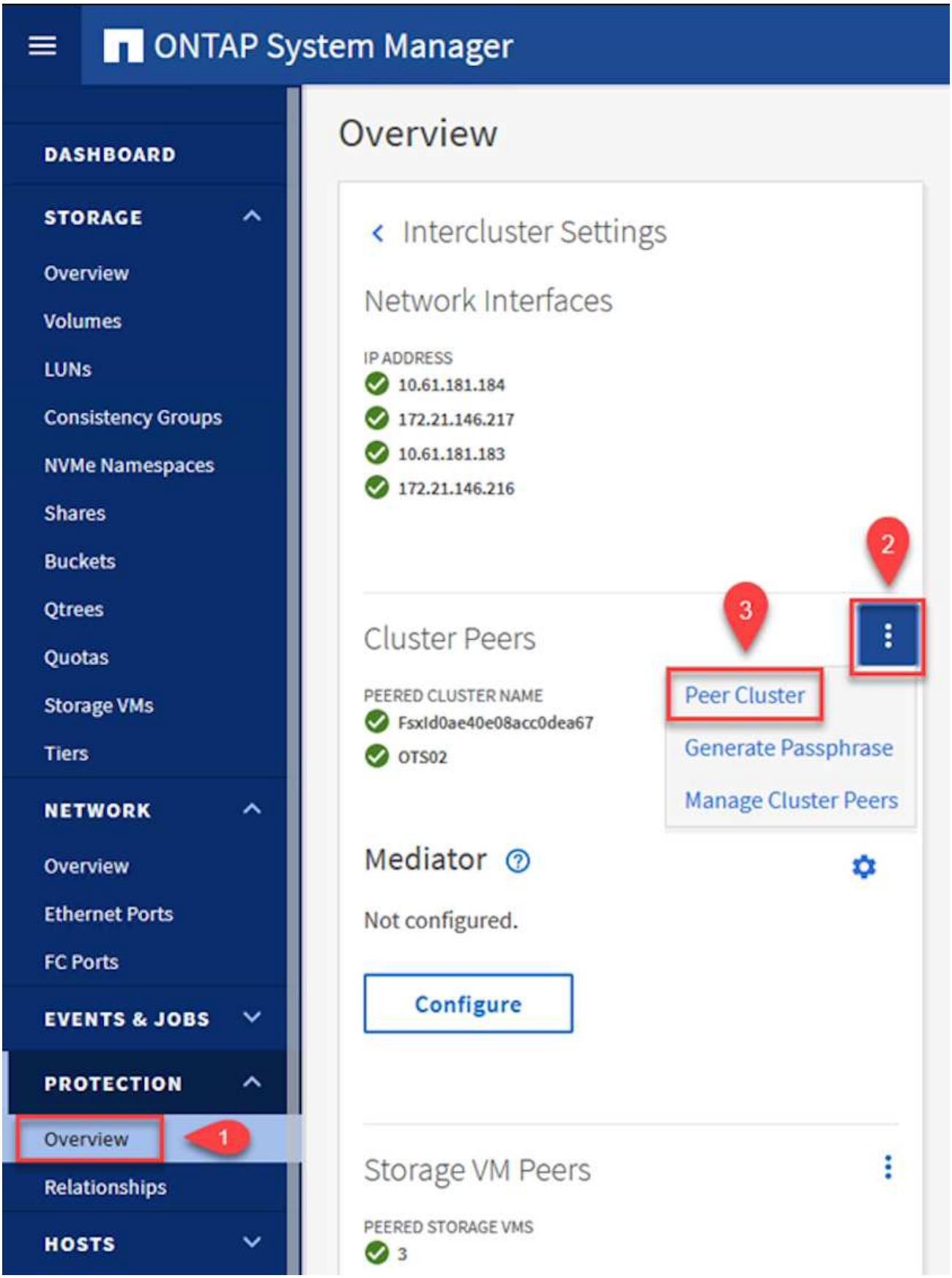
ONTAP 클러스터 간에 클러스터 피어링을 설정하려면 시작 ONTAP 클러스터에서 입력한 고유한 암호문구를 다른

피어 클러스터에서 확인해야 합니다.

1. 다음을 사용하여 대상 ONTAP 클러스터에서 피어링을 설정합니다. `cluster peer create` 명령. 메시지가 표시되면 나중에 소스 클러스터에서 생성 프로세스를 마무리하는 데 사용되는 고유한 암호구를 입력합니다.

```
ONTAP-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. 소스 클러스터에서 ONTAP 시스템 관리자나 CLI를 사용하여 클러스터 피어 관계를 설정할 수 있습니다. ONTAP 시스템 관리자에서 보호 > 개요로 이동하여 피어 클러스터를 선택합니다.

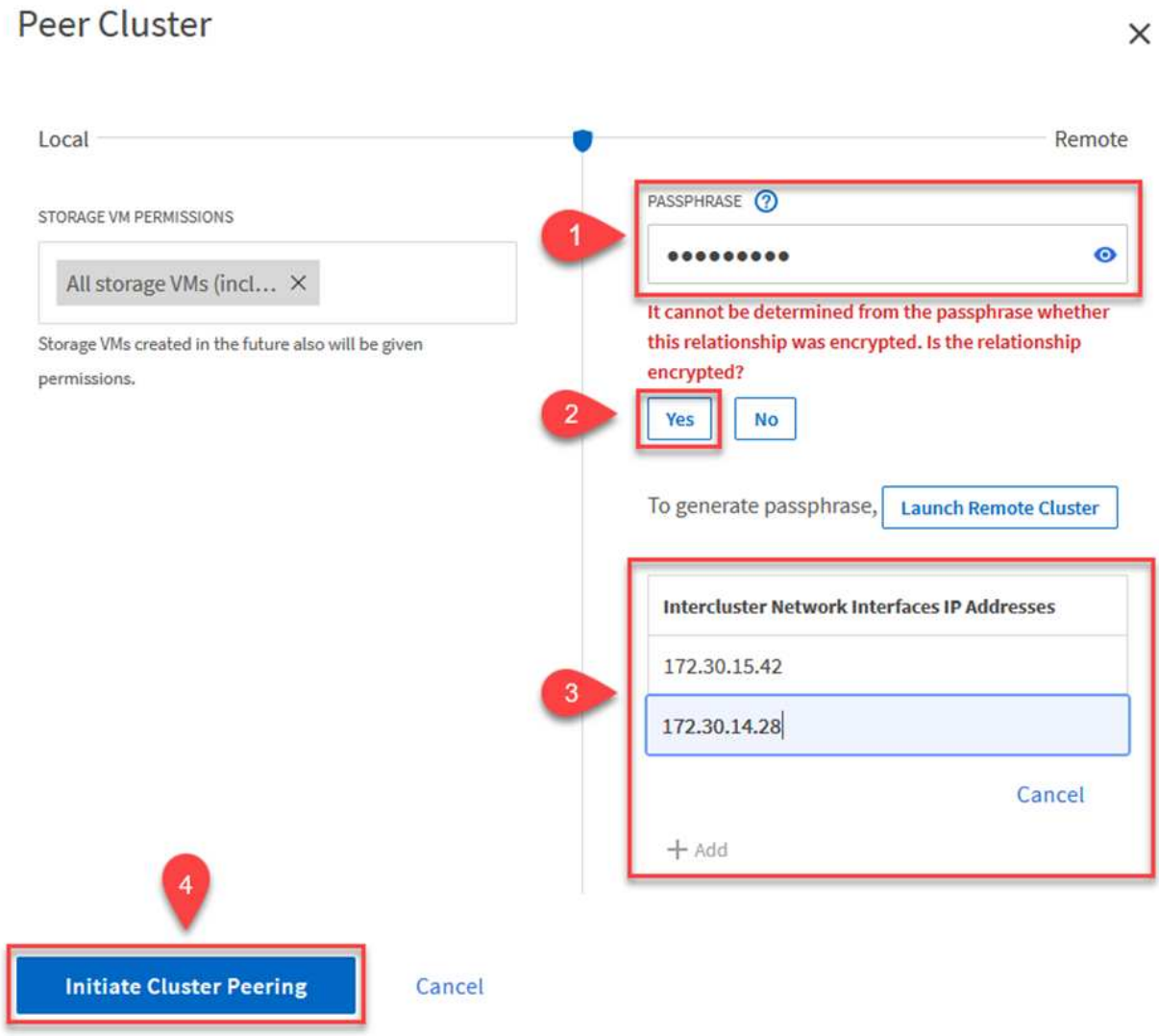


3. 피어 클러스터 대화 상자에서 필요한 정보를 입력합니다.
   a. 대상 ONTAP 클러스터에서 피어 클러스터 관계를 설정하는 데 사용된 암호를 입력하세요.

b. 선택하다 `Yes` 암호화된 관계를 구축합니다.

c. 대상 ONTAP 클러스터의 클러스터 간 LIF IP 주소를 입력하세요.

d. 클러스터 피어링 시작을 클릭하여 프로세스를 마무리합니다.



4. 다음 명령을 사용하여 대상 ONTAP 클러스터에서 클러스터 피어 관계 상태를 확인합니다.

```
ONTAP-Dest::> cluster peer show
```

▼ **SVM** 피어링 관계 설정

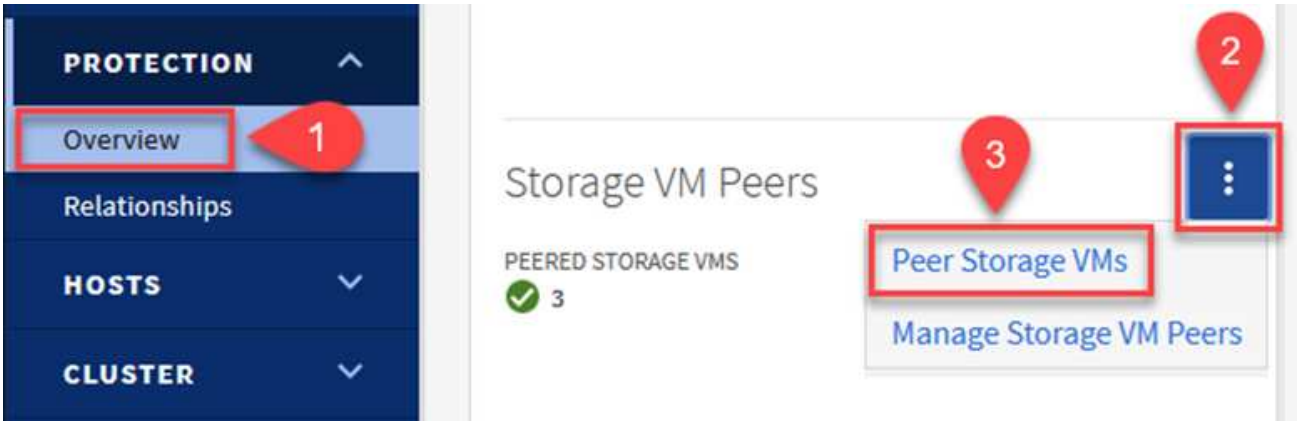
다음 단계는 SnapMirror 관계에 포함될 볼륨을 포함하는 대상 및 소스 스토리지 가상 머신 간에 SVM 관계를 설정하는 것입니다.

1. 대상 ONTAP 클러스터에서 CLI에서 다음 명령을 사용하여 SVM 피어 관계를 만듭니다.

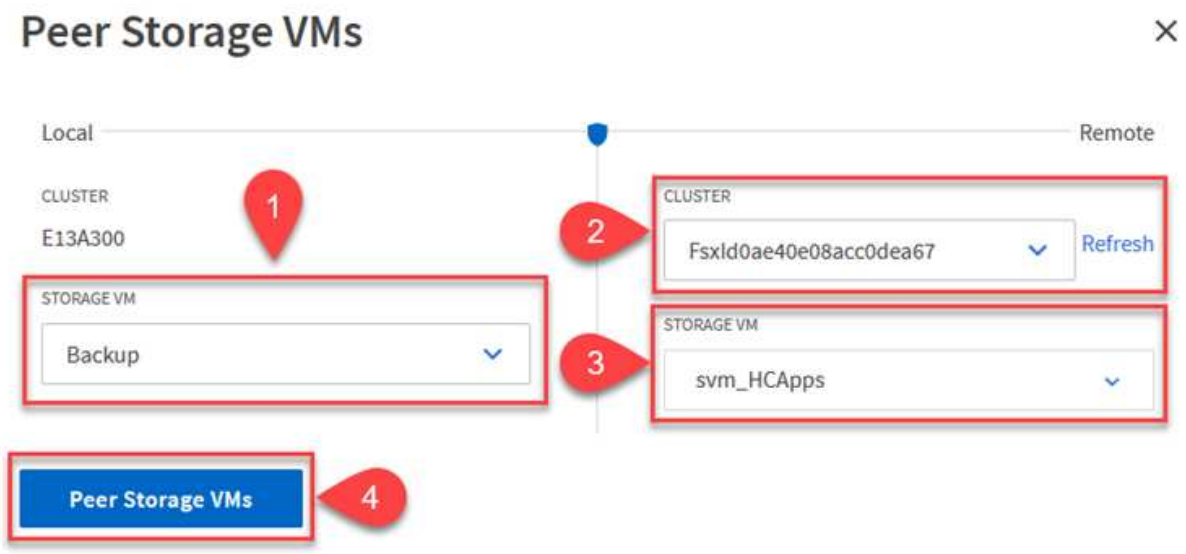
```
ONTAP-Dest::> vserver peer create -vserver DestSVM -peer-vserver
```

```
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. 소스 ONTAP 클러스터에서 ONTAP 시스템 관리자나 CLI를 사용하여 피어링 관계를 수락합니다.
3. ONTAP 시스템 관리자에서 보호 > 개요로 이동하여 스토리지 VM 피어 아래에서 피어 스토리지 VM을 선택합니다.



4. Peer Storage VM 대화 상자에서 필수 필드를 작성합니다.
   - 소스 스토리지 VM
   - 대상 클러스터
   - 대상 저장소 VM



5. SVM 피어링 프로세스를 완료하려면 Peer Storage VMs를 클릭하세요.

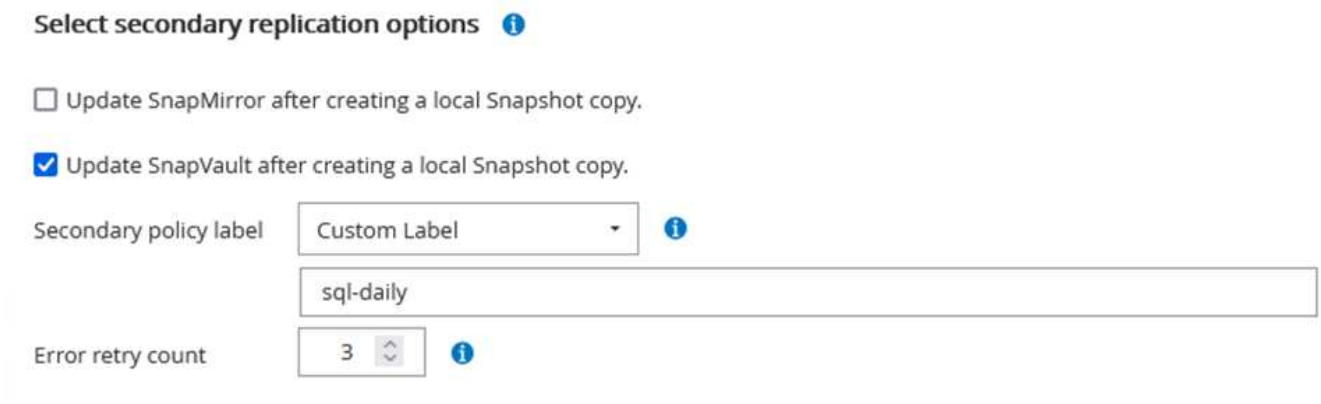
▼ 스냅샷 보존 정책 생성

SnapCenter 기본 스토리지 시스템에 스냅샷 복사본으로 존재하는 백업의 보존 일정을 관리합니다. 이는 SnapCenter 에서 정책을 생성할 때 설정됩니다. SnapCenter 보조 스토리지 시스템에 보관된 백업에 대한 보존 정책을 관리하지 않습니다. 이러한 정책은 보조 FSx 클러스터에서 생성되고 소스 볼륨과 SnapMirror 관계에 있는 대상 볼륨과 연관된 SnapMirror 정책을 통해 별도로 관리됩니다.

SnapCenter 정책을 생성할 때 SnapCenter 백업이 수행될 때 생성되는 각 스냅샷의 SnapMirror 레이블에 추가되는 보조 정책 레이블을 지정하는 옵션이 있습니다.

보조 저장소에서 이러한 레이블은 스냅샷 보존을 강제하기 위해 대상 볼륨과 연관된 정책 규칙과 일치합니다.

다음 예제는 SQL Server 데이터베이스와 로그 볼륨의 일일 백업에 사용되는 정책의 일부로 생성된 모든 스냅샷에 존재하는 SnapMirror 레이블을 보여줍니다.



SQL Server 데이터베이스에 대한 SnapCenter 정책을 만드는 방법에 대한 자세한 내용은 다음을 참조하세요. "SnapCenter 문서" .

먼저 보존할 스냅샷 복사본의 수를 결정하는 규칙이 포함된 SnapMirror 정책을 만들어야 합니다.

1. FSx 클러스터에서 SnapMirror 정책을 만듭니다.

```
ONTAP-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. SnapCenter 정책에 지정된 보조 정책 레이블과 일치하는 SnapMirror 레이블이 있는 정책에 규칙을 추가합니다.

```
ONTAP-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

다음 스크립트는 정책에 추가할 수 있는 규칙의 예를 제공합니다.

```
ONTAP-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy
Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

각 SnapMirror 레이블과 보관할 스냅샷 수(보관 기간)에 대한 추가 규칙을 만듭니다.

▼ 대상 볼륨 생성

소스 볼륨의 스냅샷 복사본을 수신할 대상 볼륨을 ONTAP 에 생성하려면 대상 ONTAP 클러스터에서 다음 명령을 실행합니다.

```
ONTAP-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

▼ 소스 볼륨과 대상 볼륨 간의 **SnapMirror** 관계 생성

소스 볼륨과 대상 볼륨 간에 SnapMirror 관계를 생성하려면 대상 ONTAP 클러스터에서 다음 명령을 실행합니다.

```
ONTAP-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

▼ **SnapMirror** 관계 초기화

SnapMirror 관계를 초기화합니다. 이 프로세스는 소스 볼륨에서 생성된 새로운 스냅샷을 시작하고 대상 볼륨에 복사합니다.

볼륨을 생성하려면 대상 ONTAP 클러스터에서 다음 명령을 실행합니다.

```
ONTAP-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

SnapCenter Plug-in for VMware vSphere 구성

SnapCenter Plug-in for VMware vSphere 설치하면 vCenter Server Appliance 관리 인터페이스에서 액세스할 수 있습니다. SCV는 ESXi 호스트에 마운트된 NFS 데이터 저장소에 대한 백업을 관리하며, 여기에는 Windows 및 Linux VM이 포함됩니다.

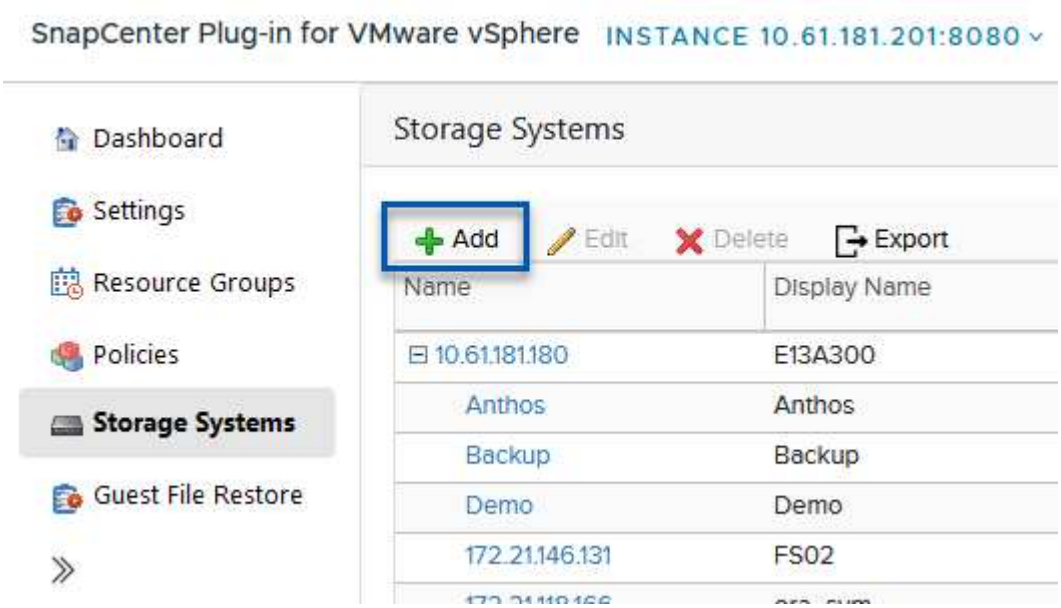
검토하다 "데이터 보호 워크플로" 백업 구성 단계에 대한 자세한 내용은 SCV 설명서 섹션을 참조하세요.

가상 머신과 데이터 저장소의 백업을 구성하려면 플러그인 인터페이스에서 다음 단계를 완료해야 합니다.

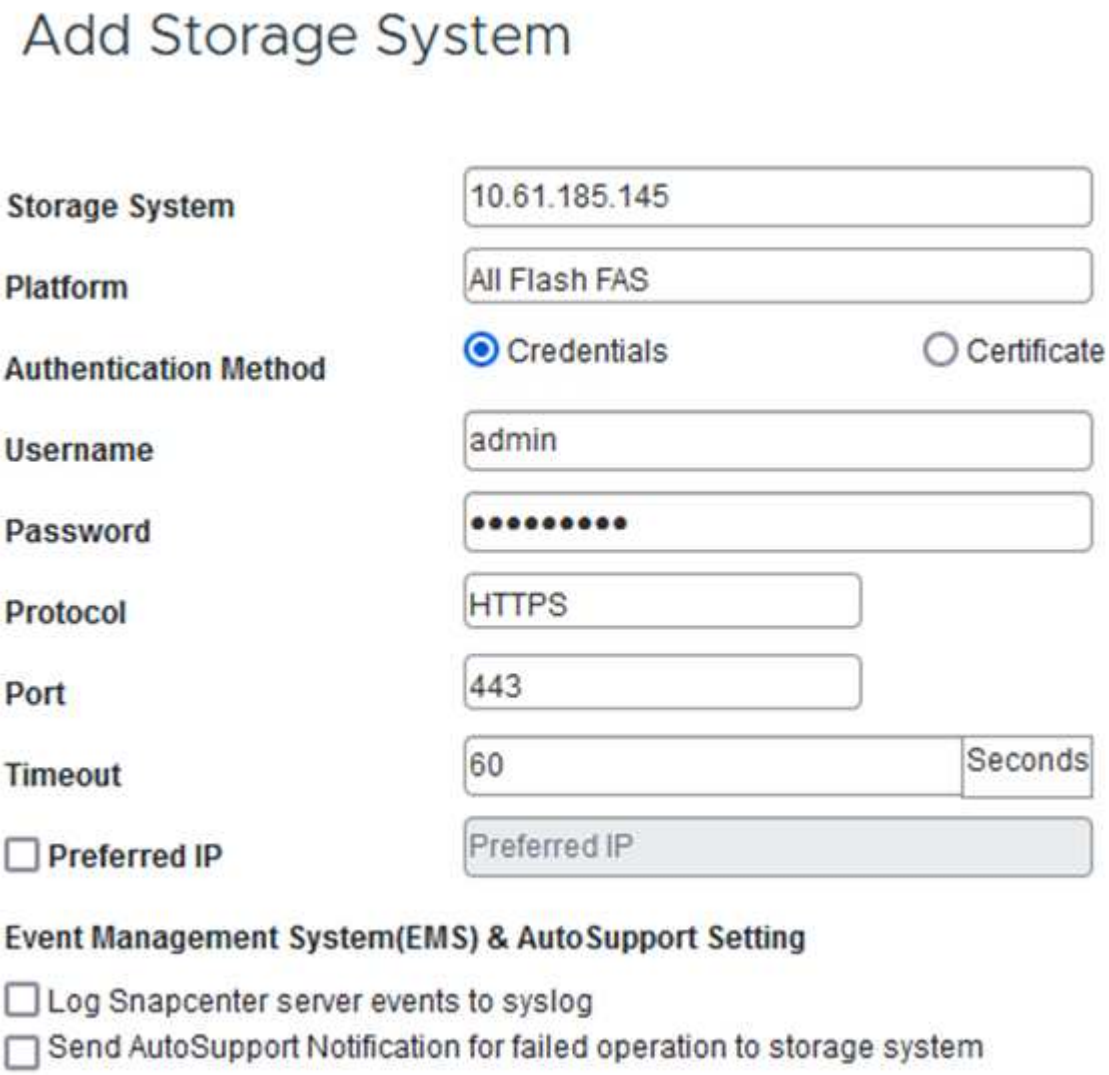
▼ **Discovery ONTAP** 스토리지 시스템

기본 및 보조 백업에 사용할 ONTAP 스토리지 클러스터를 알아보세요.

1. SnapCenter Plug-in for VMware vSphere 에서 왼쪽 메뉴의 스토리지 시스템*으로 이동한 후 *추가 버튼을 클릭합니다.



2. 기본 ONTAP 스토리지 시스템에 대한 자격 증명과 플랫폼 유형을 입력하고 *추가*를 클릭합니다.



3. 보조 ONTAP 스토리지 시스템에 대해서도 이 절차를 반복합니다.

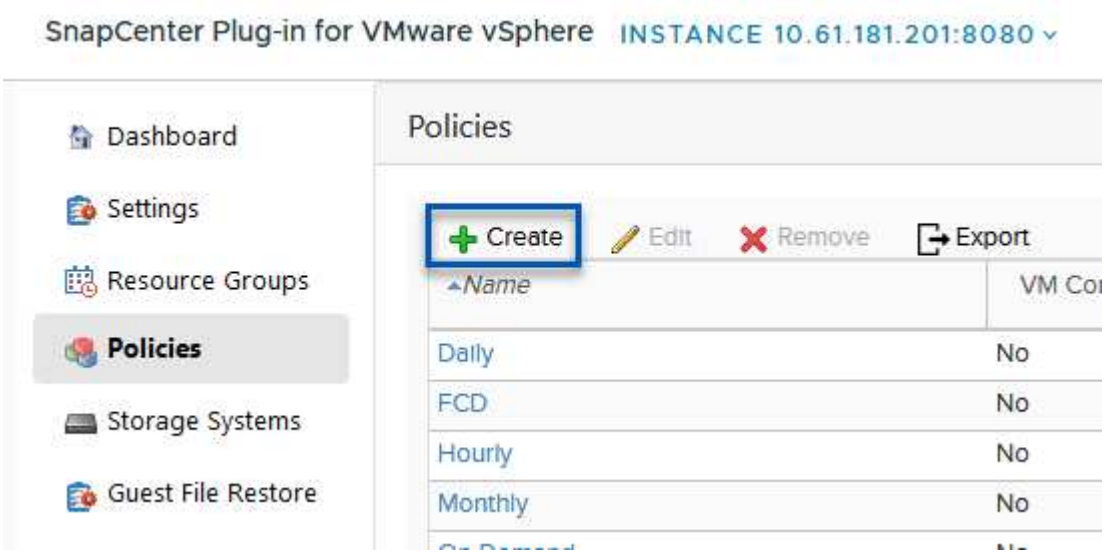
▼ **SCV** 백업 정책 생성

정책은 SCV가 관리하는 백업에 대한 보존 기간, 빈도 및 복제 옵션을 지정합니다.

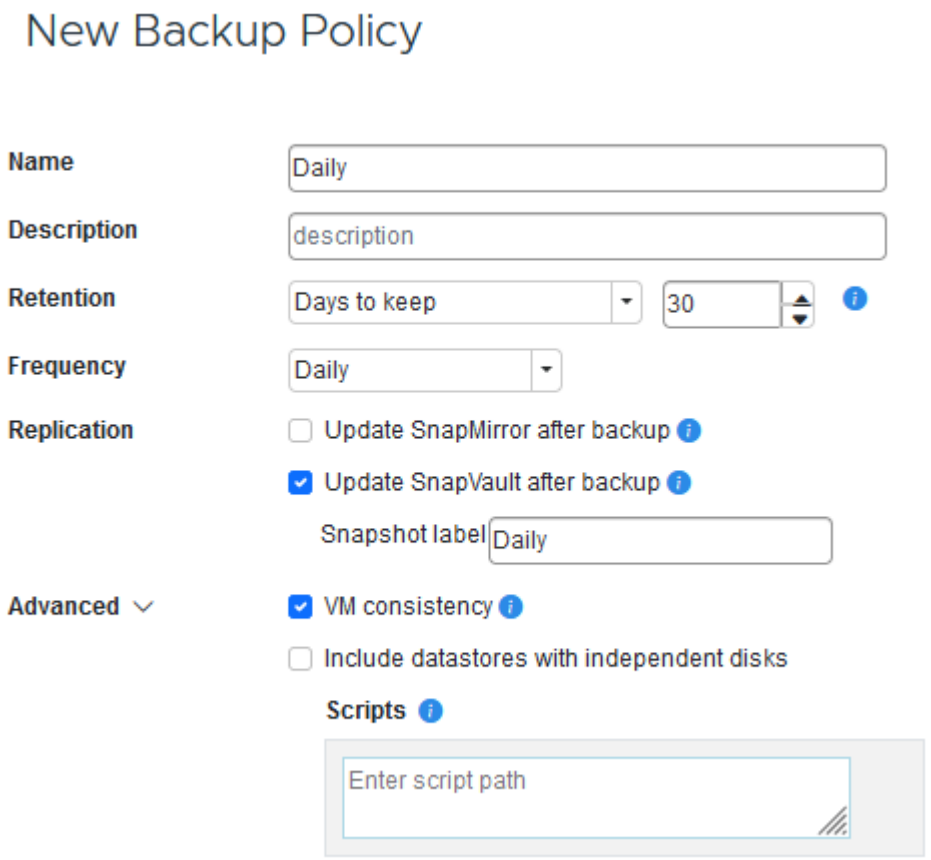
검토하다 "VM 및 데이터 저장소에 대한 백업 정책 생성" 자세한 내용은 설명서 섹션을 참조하세요.

백업 정책을 만들려면 다음 단계를 완료하세요.

1. SnapCenter Plug-in for VMware vSphere 에서 왼쪽 메뉴의 정책*으로 이동하고 *만들기 버튼을 클릭합니다.



2. 정책 이름, 보존 기간, 빈도 및 복제 옵션, 스냅샷 레이블을 지정합니다.



SnapCenter 플러그인에서 정책을 생성할 때 SnapMirror 및 SnapVault 에 대한 옵션이 표시됩니다. SnapMirror 선택하면 정책에 지정된 보존 일정이 기본 스냅샷과 보조 스냅샷 모두에 동일하게 적용됩니다. SnapVault 선택하면 보조 스냅샷의 보존 일정은 SnapMirror 관계로 구현된 별도의 일정을 기반으로 합니다. 이 기능은 2차 백업의 보존 기간을 늘리고 싶을 때 유용합니다.

스냅샷 레이블은 보조 ONTAP 클러스터로 복제된 SnapVault 복사본에 대해 특정 보존 기간을 가진 정책을 시행하는 데 사용할 수 있다는 점에서 유용합니다. SCV를 NetApp Data Services와 함께 사용하는 경우, 스냅샷 레이블 필드는 비어 있거나 백업 정책에 지정된 레이블과 [underline]#일치#해야 합니다.

3. 필요한 각 정책에 대해 이 절차를 반복합니다. 예를 들어, 일일, 주간, 월간 백업에 대해 별도의 정책을 적용합니다.

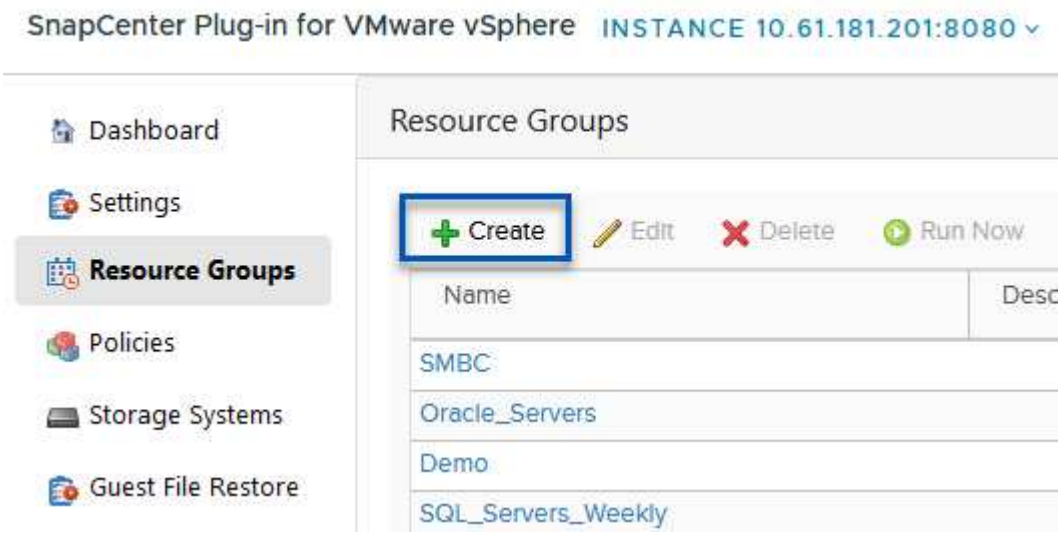
▼ 리소스 그룹 생성

리소스 그룹에는 백업 작업에 포함될 데이터 저장소와 가상 머신, 관련 정책 및 백업 일정이 포함되어 있습니다.

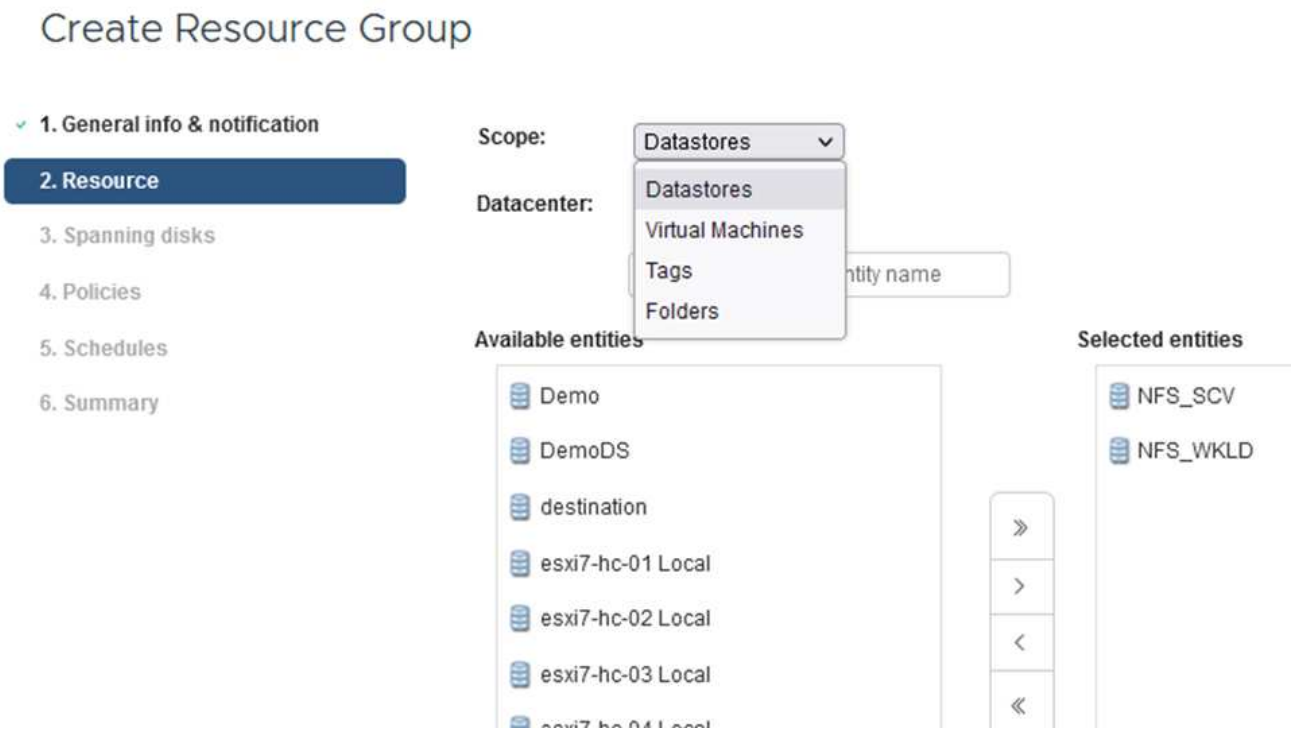
검토하다 "리소스 그룹 생성" 자세한 내용은 설명서 섹션을 참조하세요.

리소스 그룹을 만들려면 다음 단계를 완료하세요.

1. SnapCenter Plug-in for VMware vSphere 에서 왼쪽 메뉴의 리소스 그룹*으로 이동하여 *만들기 버튼을 클릭합니다.

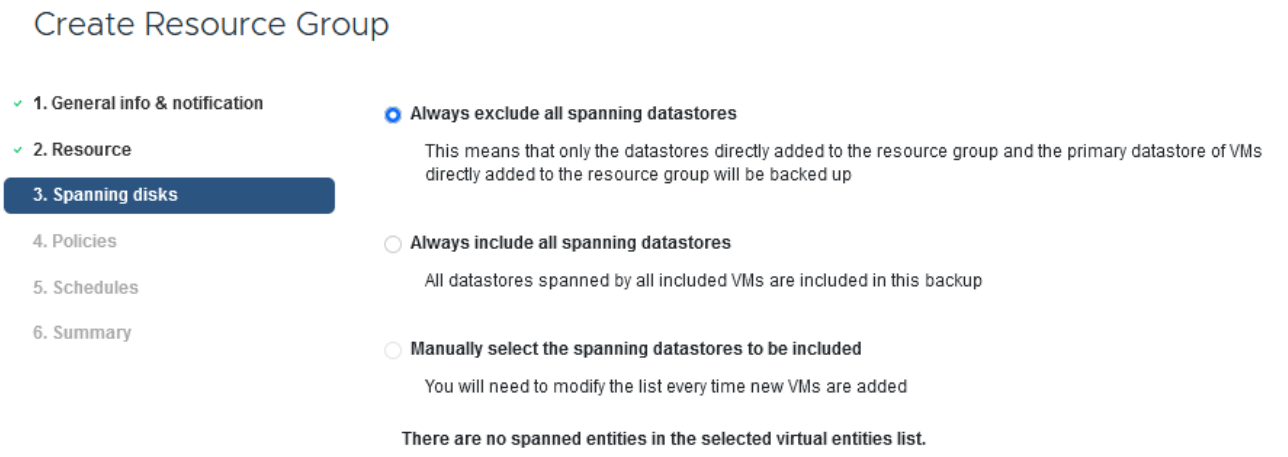


2. 리소스 그룹 만들기 마법사에서 그룹의 이름과 설명을 입력하고, 알림을 받는 데 필요한 정보도 입력합니다. *다음*을 클릭하세요
3. 다음 페이지에서 백업 작업에 포함할 데이터 저장소와 가상 머신을 선택한 후 *다음*을 클릭합니다.



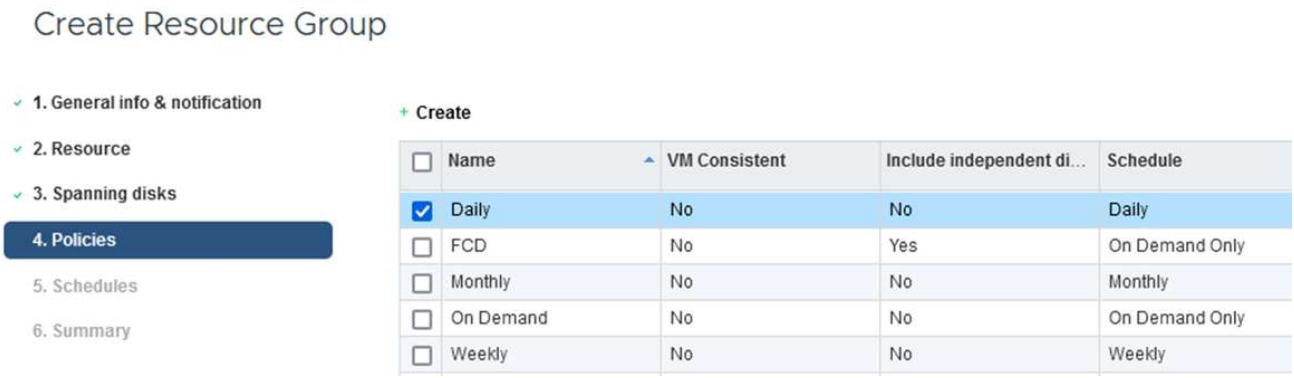
특정 VM이나 전체 데이터 저장소를 선택할 수 있습니다. 어떤 것을 선택하든 기본 볼륨의 스냅샷을 찍은 결과이므로 전체 볼륨(및 데이터 저장소)이 백업됩니다. 대부분의 경우 전체 데이터 저장소를 선택하는 것이 가장 쉽습니다. 하지만 복원 시 사용 가능한 VM 목록을 제한하려는 경우 백업할 VM의 하위 집합만 선택할 수 있습니다.

4. 여러 데이터스토어에 있는 VMDK가 있는 VM의 데이터스토어를 확장하기 위한 옵션을 선택한 후 *다음*을 클릭합니다.



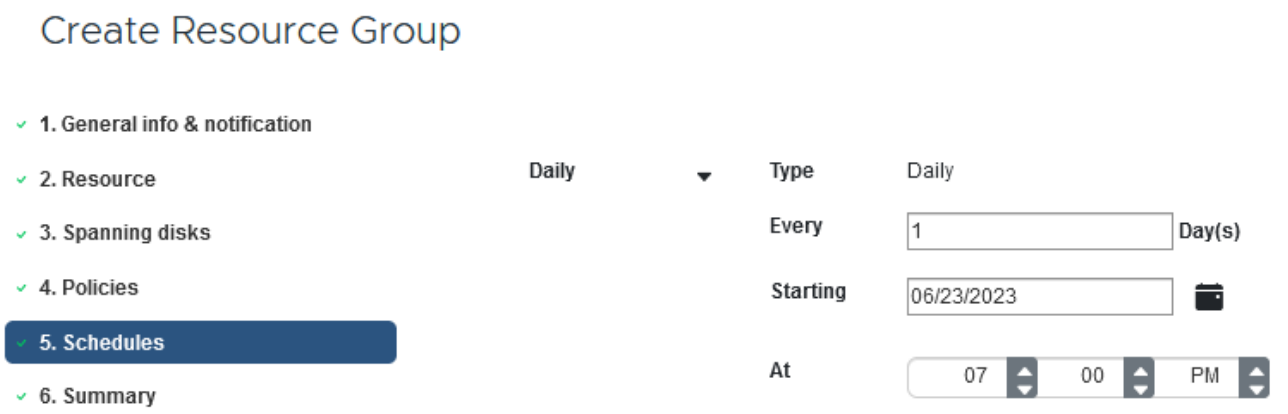
VMware 워크로드를 보호하기 위한 백업 및 복구 기능은 현재 여러 데이터스토어에 걸쳐 있는 VMDK를 사용하는 VM 백업을 지원하지 않습니다.

5. 다음 페이지에서 리소스 그룹과 연관될 정책을 선택하고 *다음*을 클릭합니다.



Backup and Recovery를 사용하여 SCV 관리 스냅샷을 오브젝트 스토리지에 백업할 때 각 리소스 그룹은 하나의 정책에만 연결될 수 있습니다.

6. 백업이 실행될 시간을 결정하는 일정을 선택하세요. *다음*을 클릭하세요.

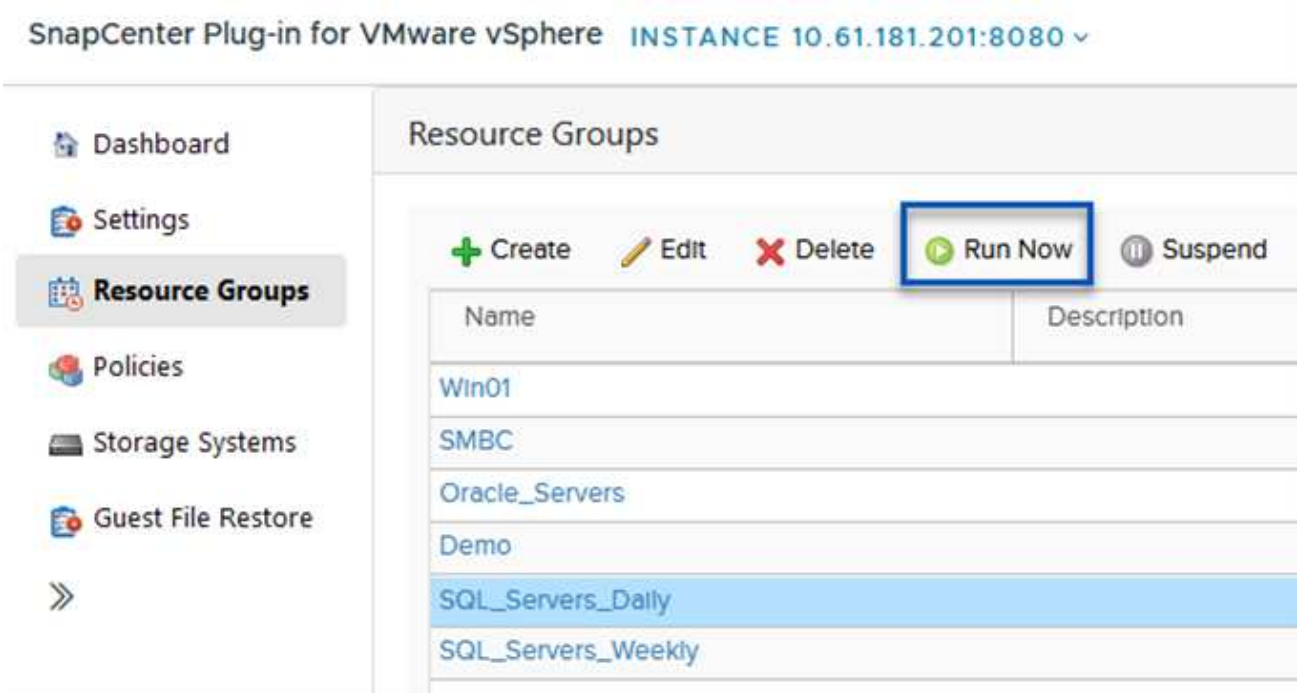


7. 마지막으로 요약 페이지를 검토한 후 *마침*을 클릭하여 리소스 그룹 생성을 완료합니다.

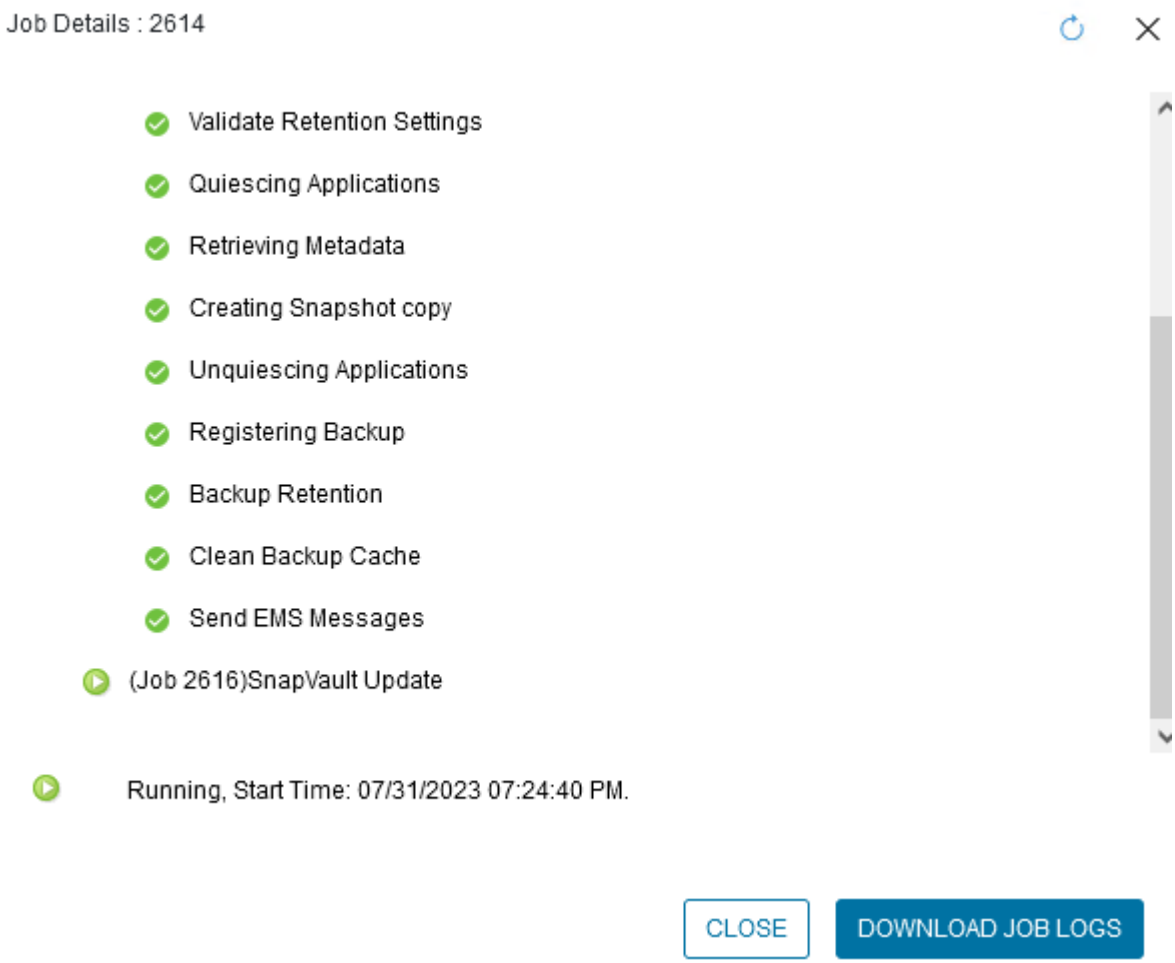
▼ 백업 작업 실행

이 마지막 단계에서는 백업 작업을 실행하고 진행 상황을 모니터링합니다. NetApp Console에서 리소스를 탐색하려면 먼저 SCV에서 하나 이상의 백업 작업이 성공적으로 완료되어야 합니다.

1. SnapCenter Plug-in for VMware vSphere 에서 왼쪽 메뉴의 *리소스 그룹*으로 이동합니다.
2. 백업 작업을 시작하려면 원하는 리소스 그룹을 선택하고 지금 실행 버튼을 클릭하세요.



3. 백업 작업을 모니터링하려면 왼쪽 메뉴의 *대시보드*로 이동하세요. *최근 작업 활동*에서 작업 ID 번호를 클릭하여 작업 진행 상황을 모니터링하세요.



NetApp Console에서 오브젝트 스토리지로 백업 구성

NetApp Console이 데이터 인프라를 효과적으로 관리하려면 콘솔 에이전트를 먼저 설치해야 합니다. 콘솔 에이전트는 리소스 탐색 및 데이터 운영 관리와 관련된 작업을 수행합니다.

콘솔 에이전트에 대한 자세한 내용은 NetApp Console 설명서에서 "콘솔 에이전트에 대해 알아보십시오"을(를) 참조하십시오.

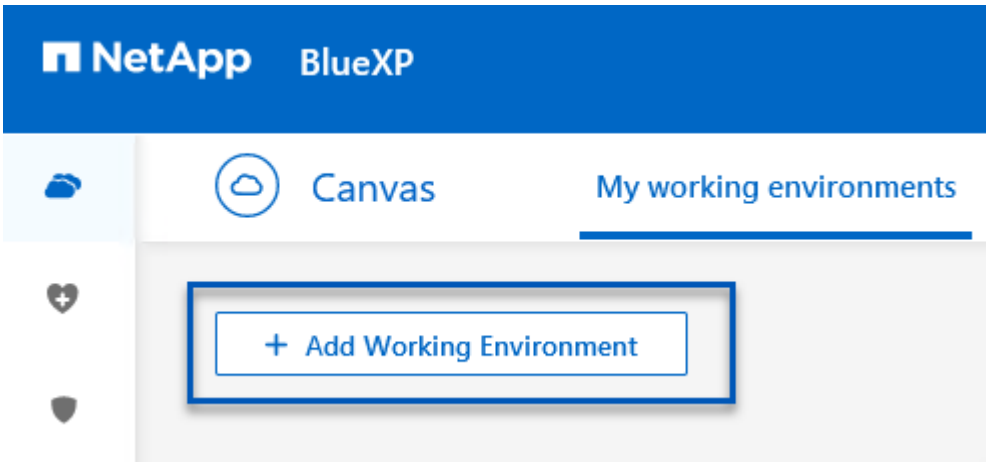
사용 중인 클라우드 공급자용 에이전트가 설치되면 시스템에서 오브젝트 스토리지의 그래픽 표현을 볼 수 있습니다.

온프레미스에서 SCV가 관리하는 데이터를 백업하도록 Backup and Recovery를 구성하려면 다음 단계를 완료하십시오.

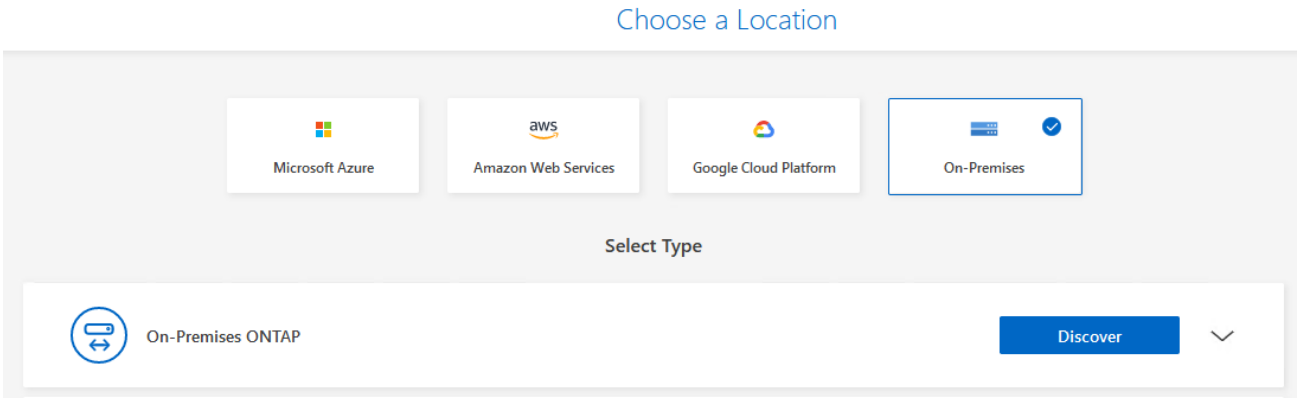
▼ 시스템에 **ONTAP** 스토리지 시스템 추가

첫 번째 단계는 온프레미스 ONTAP 스토리지 시스템을 NetApp Console에 추가하는 것입니다.

1. 시스템에서 *+ 추가*를 클릭하여 시작하십시오.



2. 위치 선택에서 사내*를 선택한 다음 *검색 버튼을 클릭합니다.



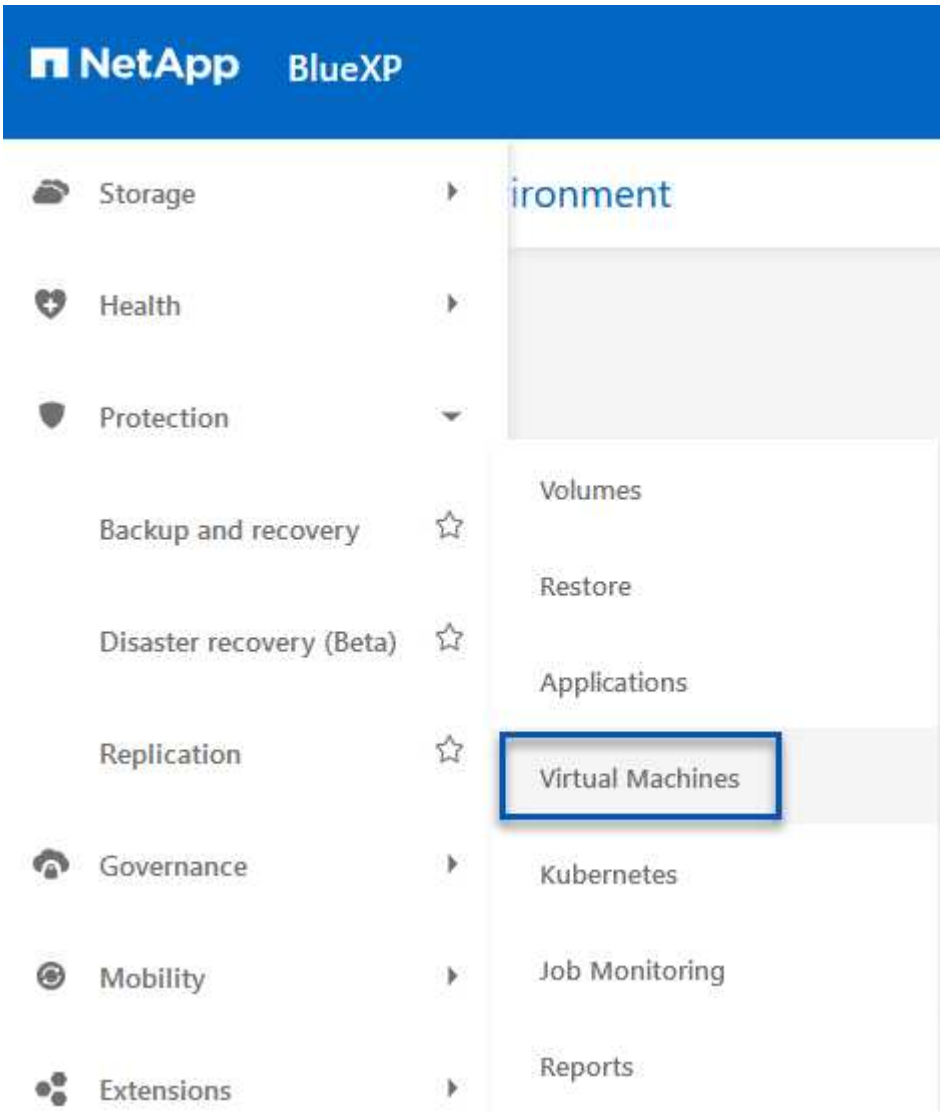
3. ONTAP 스토리지 시스템의 자격 증명을 입력하고 검색 버튼을 클릭하여 작업 환경을 추가합니다.



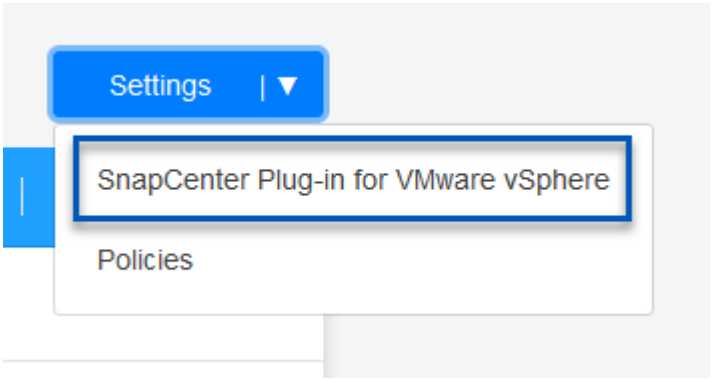
▼ 온프레미스 **SCV** 어플라이언스 및 **vCenter**를 검색하세요

온프레미스 데이터스토어와 가상 머신 리소스를 검색하려면 SCV 데이터 브로커에 대한 정보와 vCenter 관리 어플라이언스에 대한 자격 증명을 추가합니다.

1. NetApp Console 왼쪽 메뉴에서 *보호 > 백업 및 복구 > 워크로드 > VMware*를 선택하십시오.

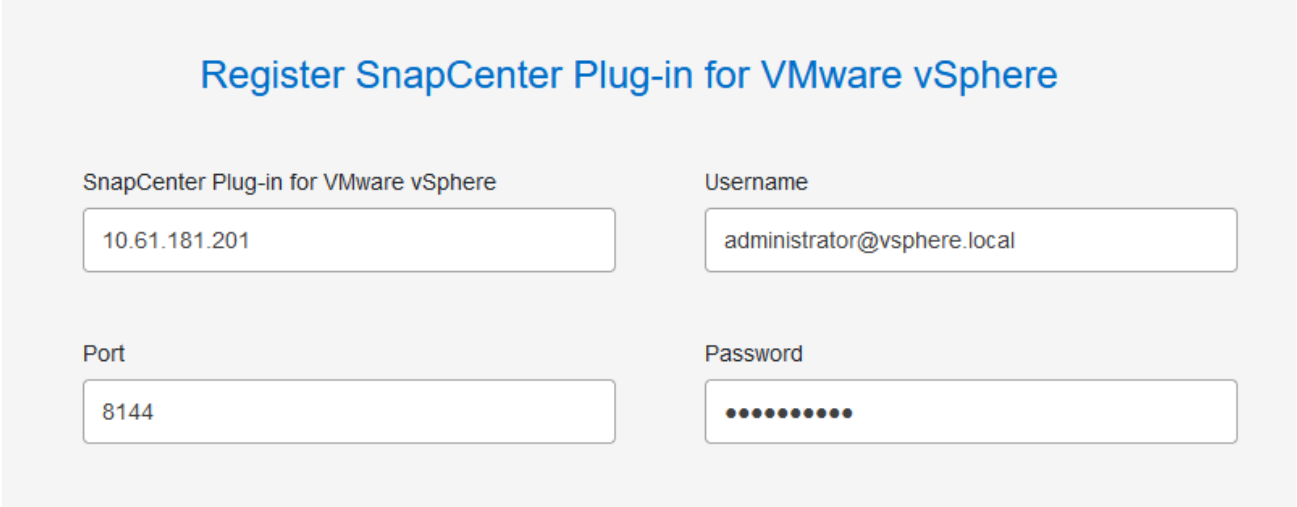


2. 가상 머신 메인 화면에서 설정 드롭다운 메뉴에 액세스하고 * SnapCenter Plug-in for VMware vSphere*을 선택합니다.

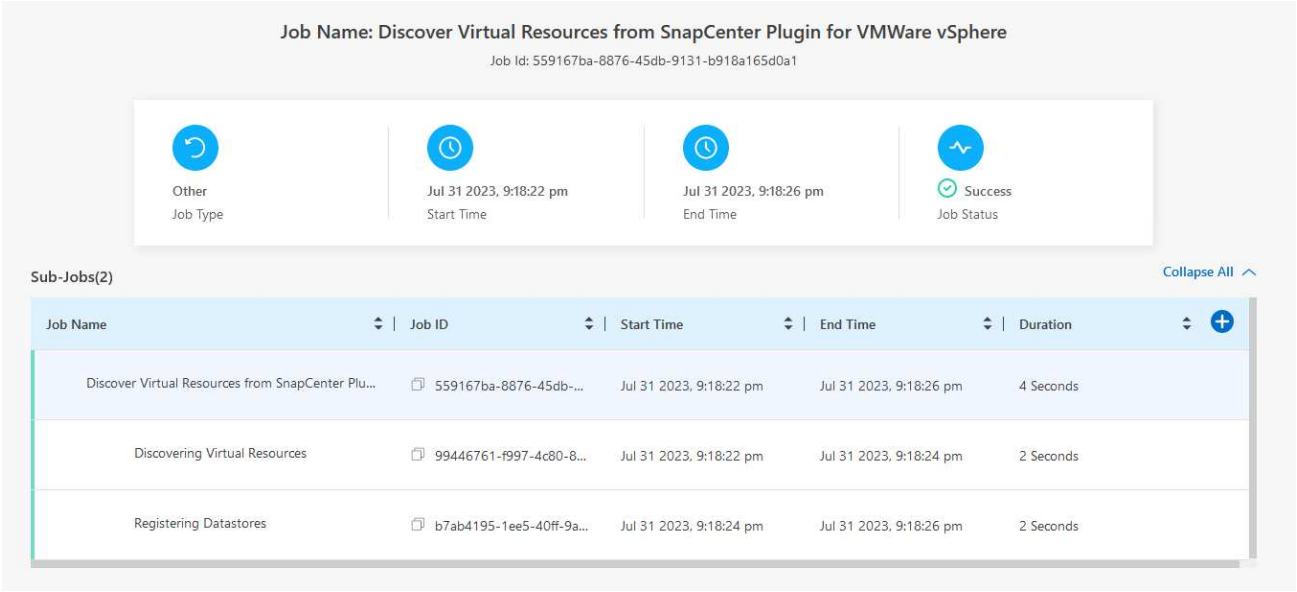


3. 등록 버튼을 클릭한 다음 SnapCenter 플러그인 어플라이언스의 IP 주소와 포트 번호, vCenter 관리

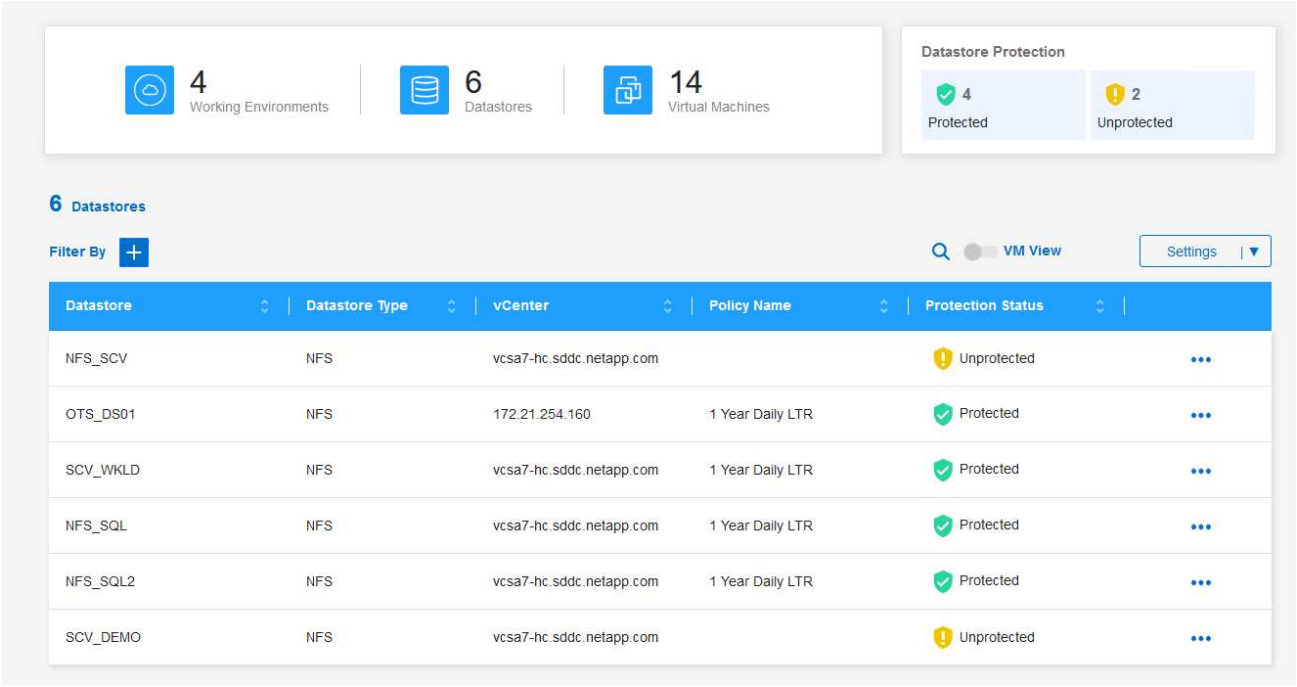
어플라이언스의 사용자 이름과 비밀번호를 입력합니다. 등록 버튼을 클릭하여 검색 과정을 시작하세요.



4. 작업 모니터링 탭에서 작업 진행 상황을 모니터링할 수 있습니다.



5. 검색이 완료되면 검색된 모든 SCV 어플라이언스의 데이터 저장소와 가상 머신을 볼 수 있습니다.

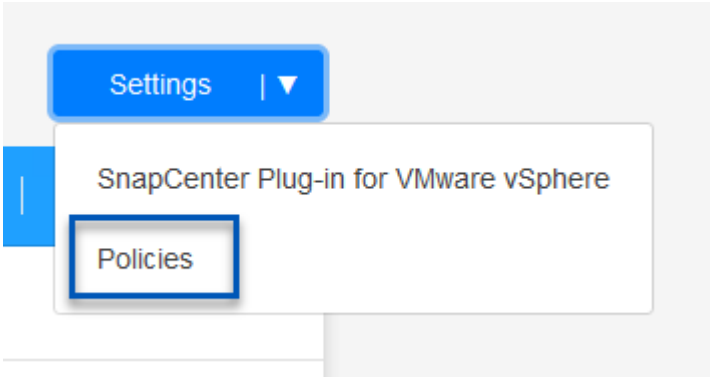


▼ 백업 정책 생성

가상 머신용 NetApp Backup and Recovery에서 보존 기간, 백업 소스 및 아카이빙 정책을 지정하는 정책을 생성합니다.

보호 그룹 생성에 대한 자세한 내용은 "보호 그룹 생성"을(를) 참조하십시오.

1. 가상 머신용 NetApp Backup and Recovery 기본 페이지에서 설정 드롭다운 메뉴에 액세스하여 *정책*을 선택합니다.



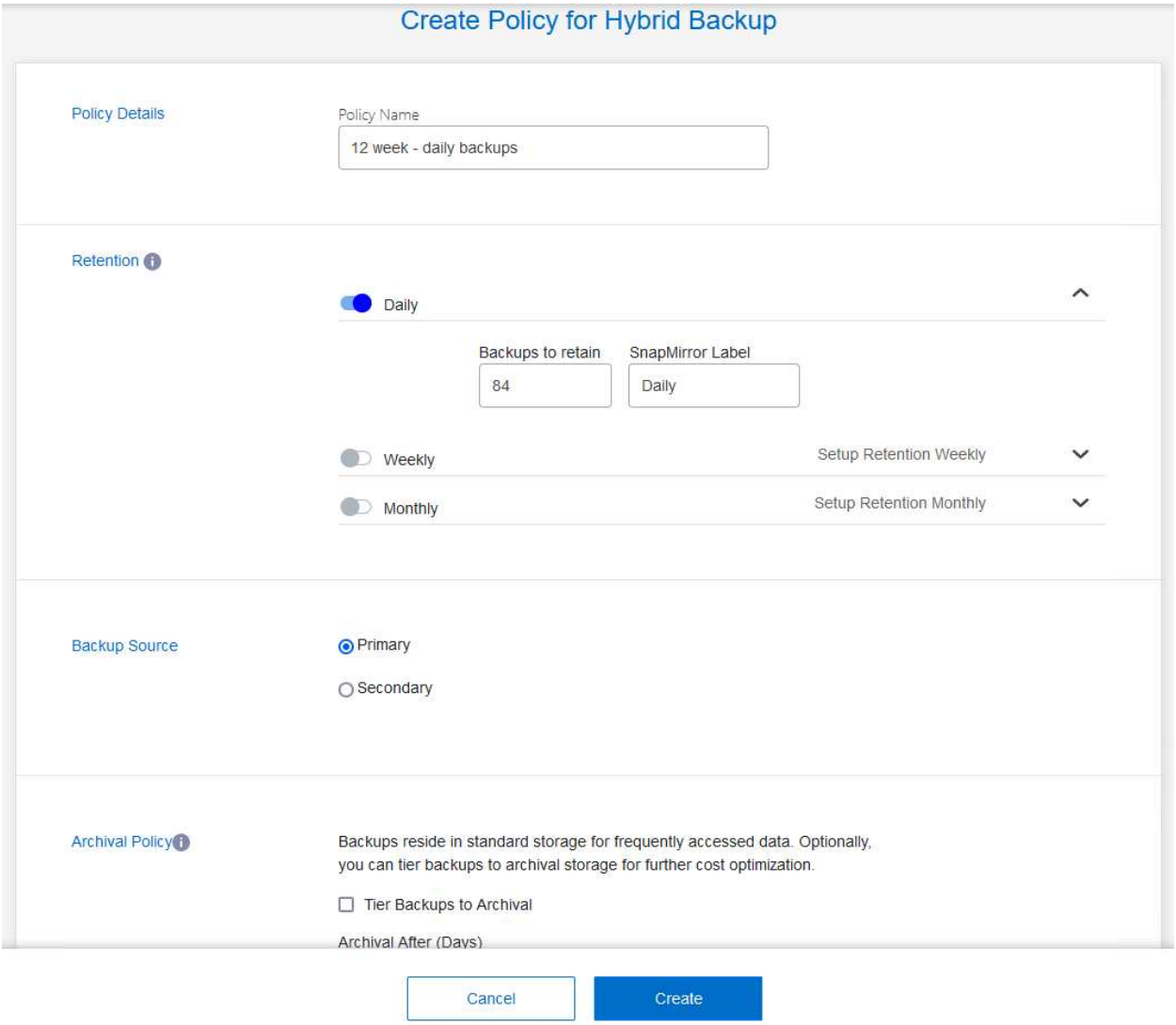
2. 정책 만들기*를 클릭하여 *하이브리드 백업 정책 만들기 창에 액세스합니다.

   a. 정책에 대한 이름을 추가합니다.

   b. 원하는 보존 기간을 선택하세요

   c. 백업이 기본 온프레미스 ONTAP 스토리지 시스템 또는 보조 온프레미스 ONTAP 스토리지 시스템에서 제공될지 여부를 선택합니다.

   d. 선택적으로, 추가 비용 절감을 위해 백업을 보관 저장소에 얼마 동안 저장할지 기간을 지정합니다.



여기에 입력된 SnapMirror 레이블은 어떤 백업에 정책을 적용할지 식별하는 데 사용됩니다. 레이블 이름은 해당 온프레미스 SCV 정책의 레이블 이름과 일치해야 합니다.

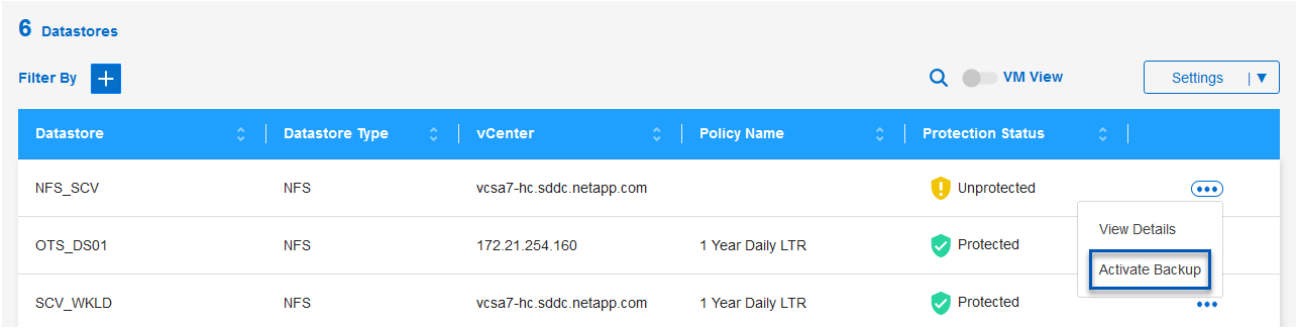
3. *만들기*를 클릭하여 정책 생성을 완료하세요.

▼ **Amazon Web Services**에 데이터 저장소 백업

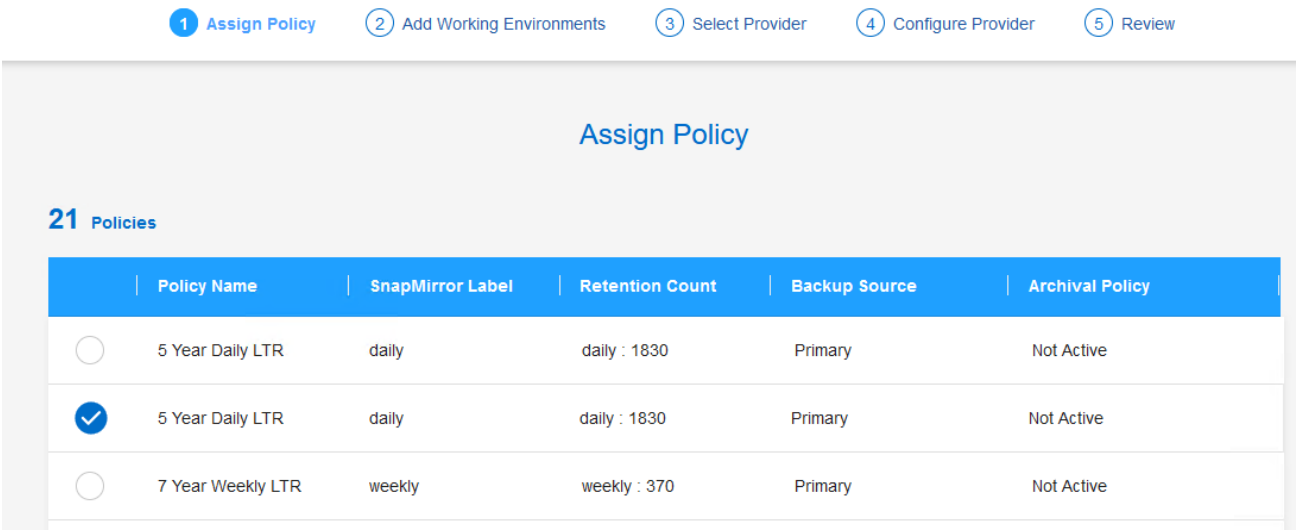
마지막 단계는 개별 데이터 저장소와 가상 머신에 대한 데이터 보호를 활성화하는 것입니다. 다음 단계에서는 AWS에 대한 백업을 활성화하는 방법을 설명합니다.

자세한 내용은 다음을 참조하십시오 "VMware 워크로드 백업".

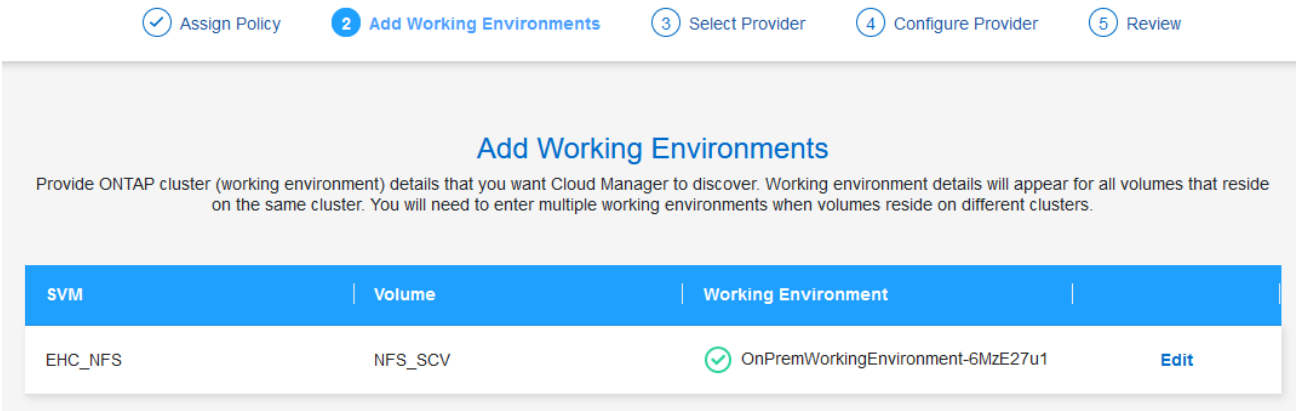
1. 가상 머신용 NetApp Backup and Recovery 기본 페이지에서 백업할 데이터스토어의 설정 드롭다운에 액세스하여 *백업 활성화*를 선택합니다.



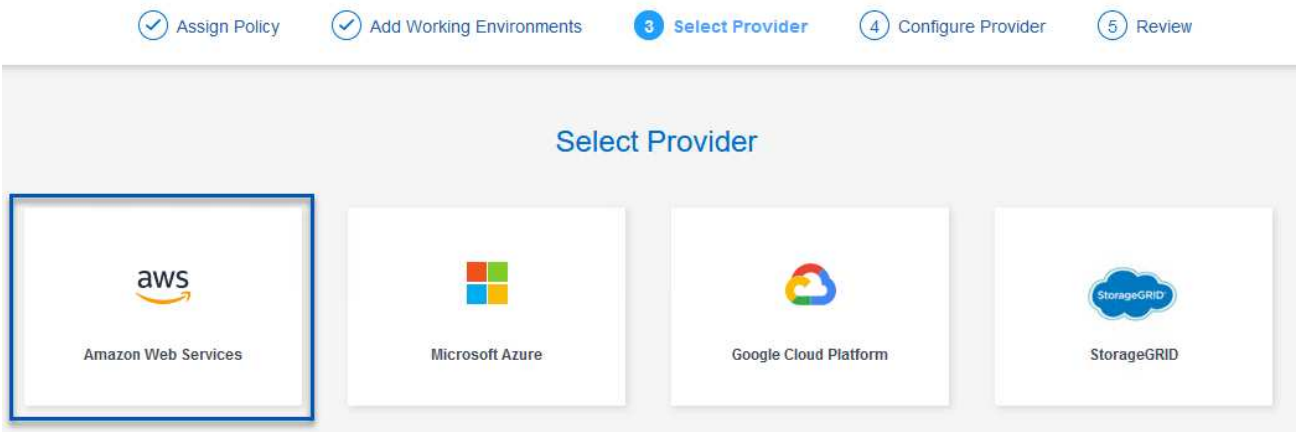
2. 데이터 보호 작업에 사용할 정책을 할당하고 *다음*을 클릭합니다.



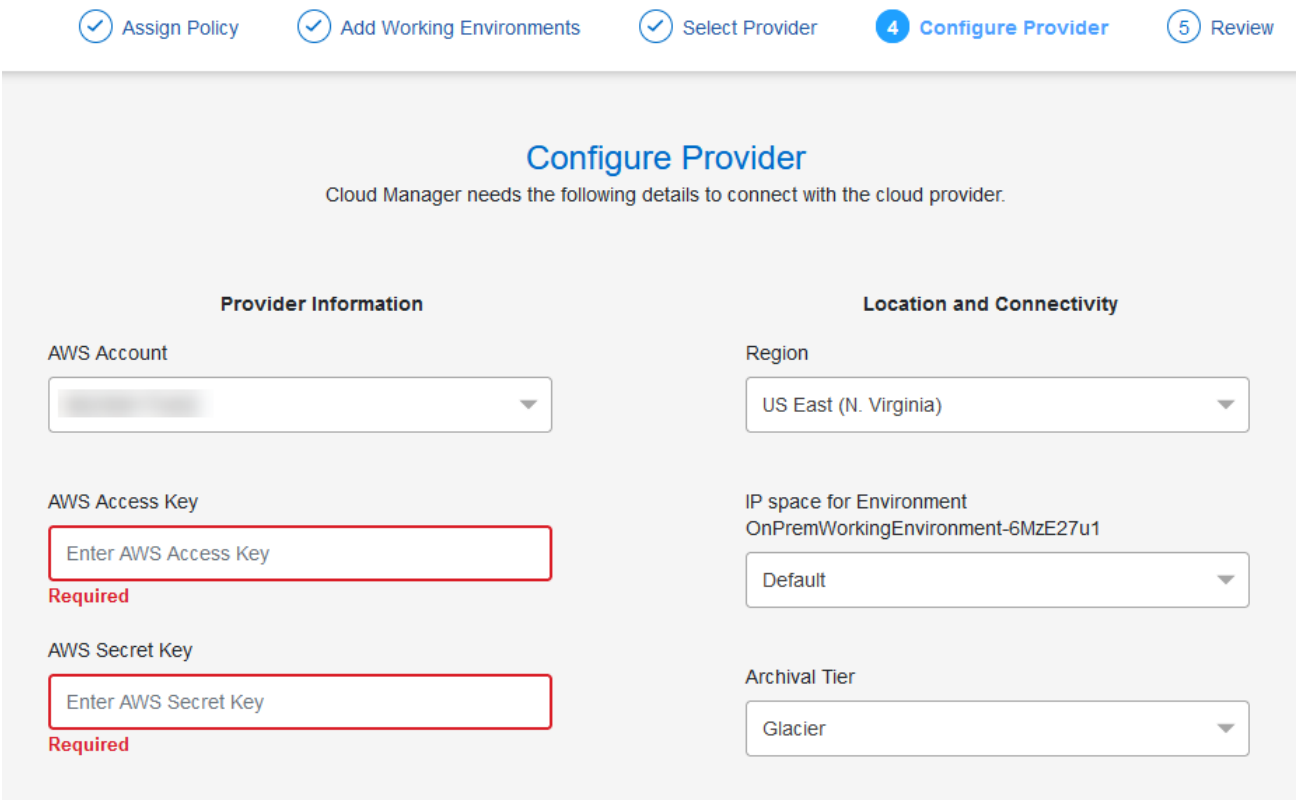
3. 작업 환경 추가 페이지에는 작업 환경이 이전에 검색된 경우 체크 표시가 있는 데이터 저장소와 작업 환경이 나타나야 합니다. 작업 환경을 이전에 발견하지 못한 경우 여기에 추가할 수 있습니다. 계속하려면 *다음*을 클릭하세요.



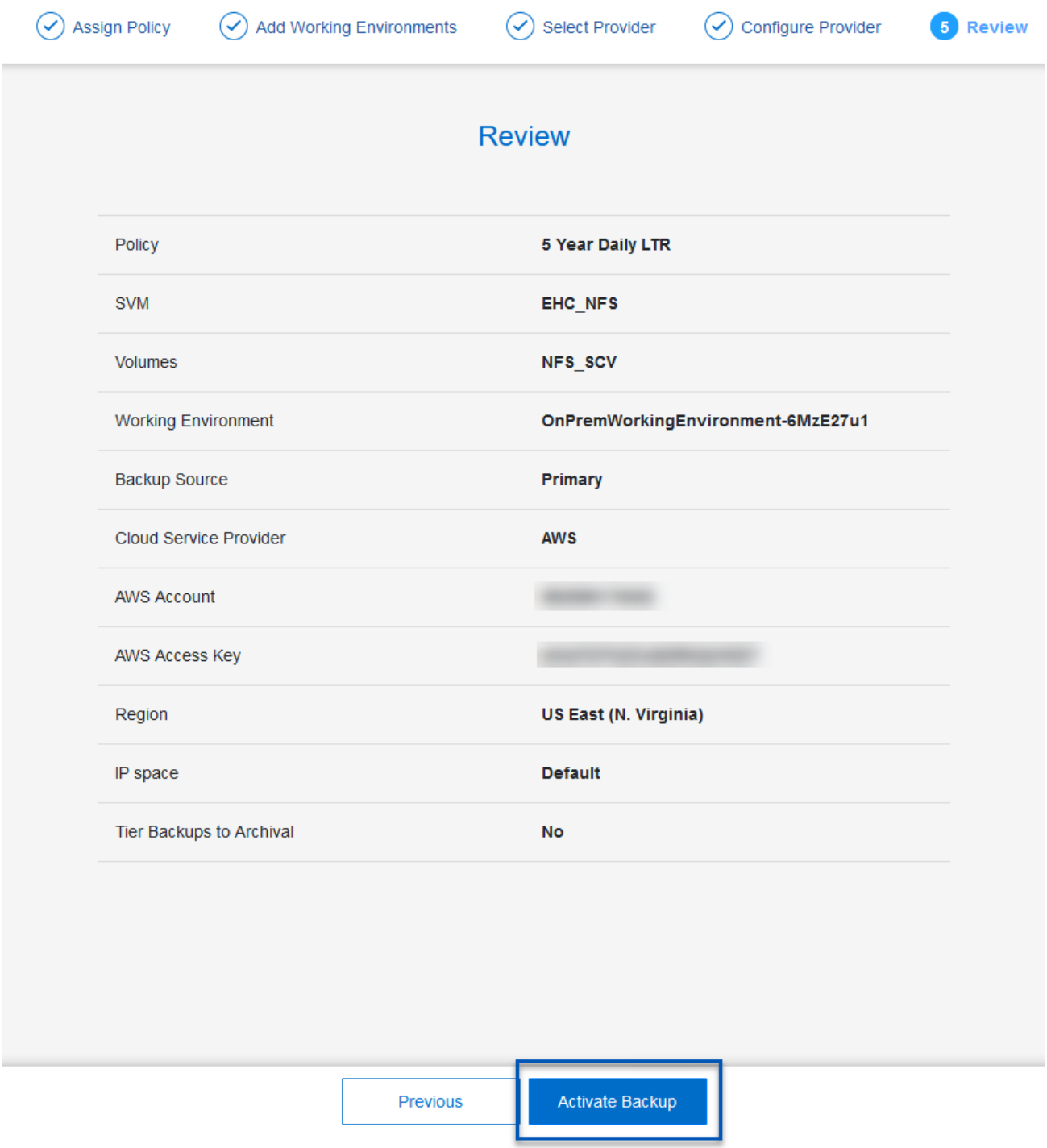
4. 공급자 선택 페이지에서 AWS를 클릭한 다음 다음 버튼을 클릭하여 계속합니다.



5. AWS 액세스 키와 비밀 키, 지역, 사용할 보관 계층을 포함하여 AWS에 대한 공급자별 자격 증명 정보를 작성합니다. 또한 온프레미스 ONTAP 스토리지 시스템에 대한 ONTAP IP 공간을 선택합니다. *다음*을 클릭하세요.



6. 마지막으로 백업 작업 세부 정보를 검토하고 백업 활성화 버튼을 클릭하여 데이터 저장소의 데이터 보호를 시작합니다.



이 시점에서는 데이터 전송이 즉시 시작되지 않을 수 있습니다. NetApp Backup and Recovery는 매시간 미처리된 스냅샷을 검색한 후 오브젝트 스토리지로 전송합니다.

데이터 손실 시 가상 머신 복원

귀하의 데이터를 안전하게 보호하는 것은 포괄적인 데이터 보호의 한 측면일 뿐입니다. 데이터 손실이나 랜섬웨어 공격이 발생한 경우 어느 위치에서나 데이터를 신속하게 복원할 수 있는 능력도 마찬가지로 중요합니다. 이러한 기능은 원활한 비즈니스 운영을 유지하고 복구 지점 목표를 달성하는 데 필수적입니다.

NetApp 높은 적응성을 갖춘 3-2-1 전략을 제공하여 기본, 보조 및 개체 스토리지 위치에서 보존 일정을 사용자 정의하여 제어할 수 있습니다. 이 전략은 특정 요구 사항에 맞게 데이터 보호 접근 방식을 조정할 수 있는 유연성을 제공합니다.

이 섹션에서는 SnapCenter Plug-in for VMware vSphere 및 가상 머신용 NetApp Backup and Recovery의 데이터 복원 프로세스에 대한 개요를 제공합니다.

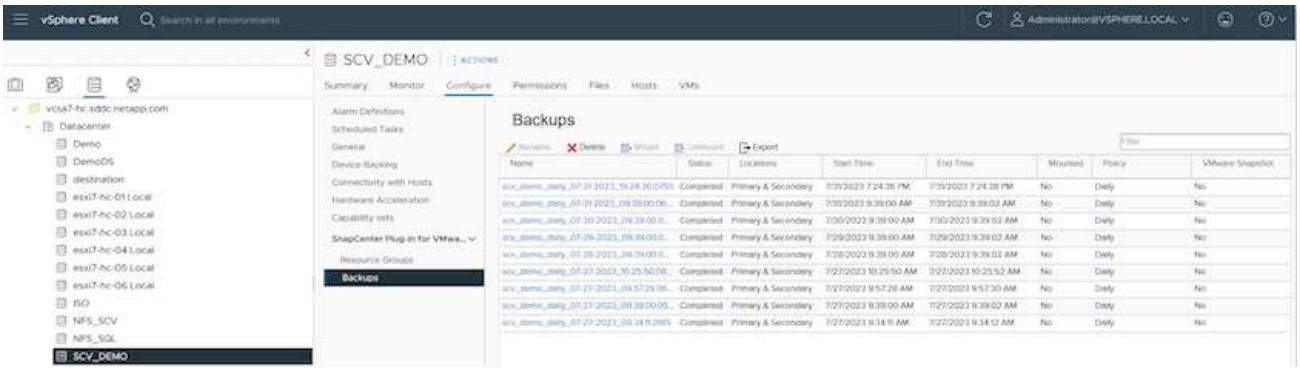
SnapCenter Plug-in for VMware vSphere 에서 가상 머신 복원

이 솔루션을 사용하면 가상 머신이 원래 위치와 대체 위치로 복원되었습니다. 이 솔루션에서는 SCV의 데이터 복구 기능의 모든 측면을 다루지는 않습니다. SCV가 제공하는 모든 것에 대한 자세한 정보는 다음을 참조하세요. "백업에서 VM 복원" 제품 설명서에서.

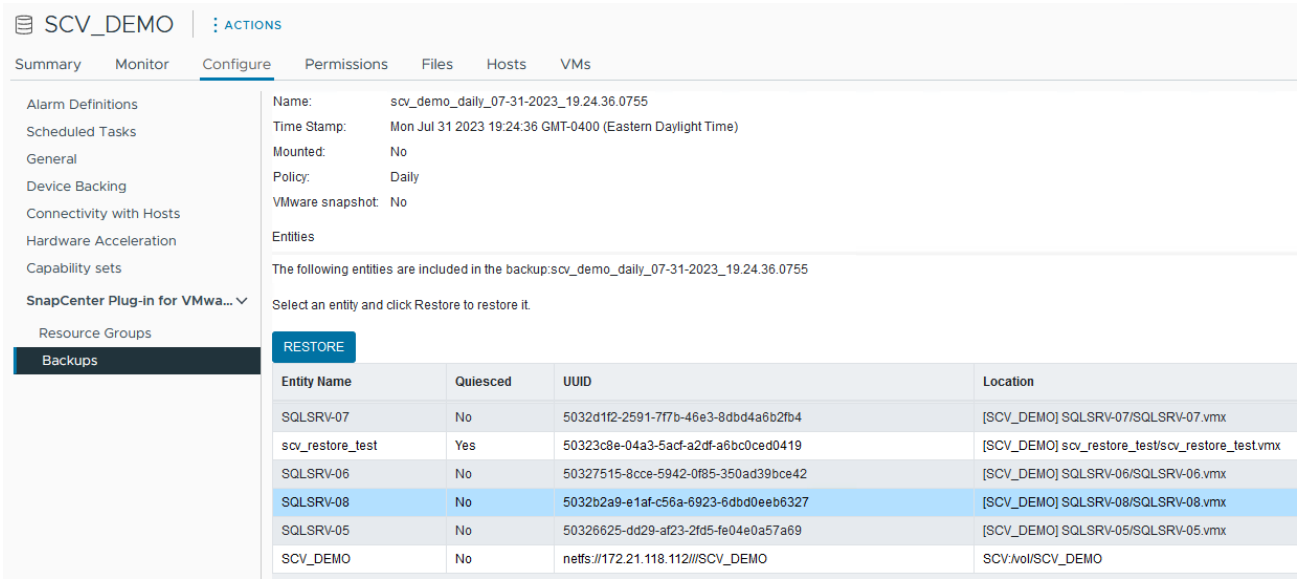
▼ **SCV**에서 가상 머신 복원

기본 또는 보조 저장소에서 가상 머신을 복원하려면 다음 단계를 완료하세요.

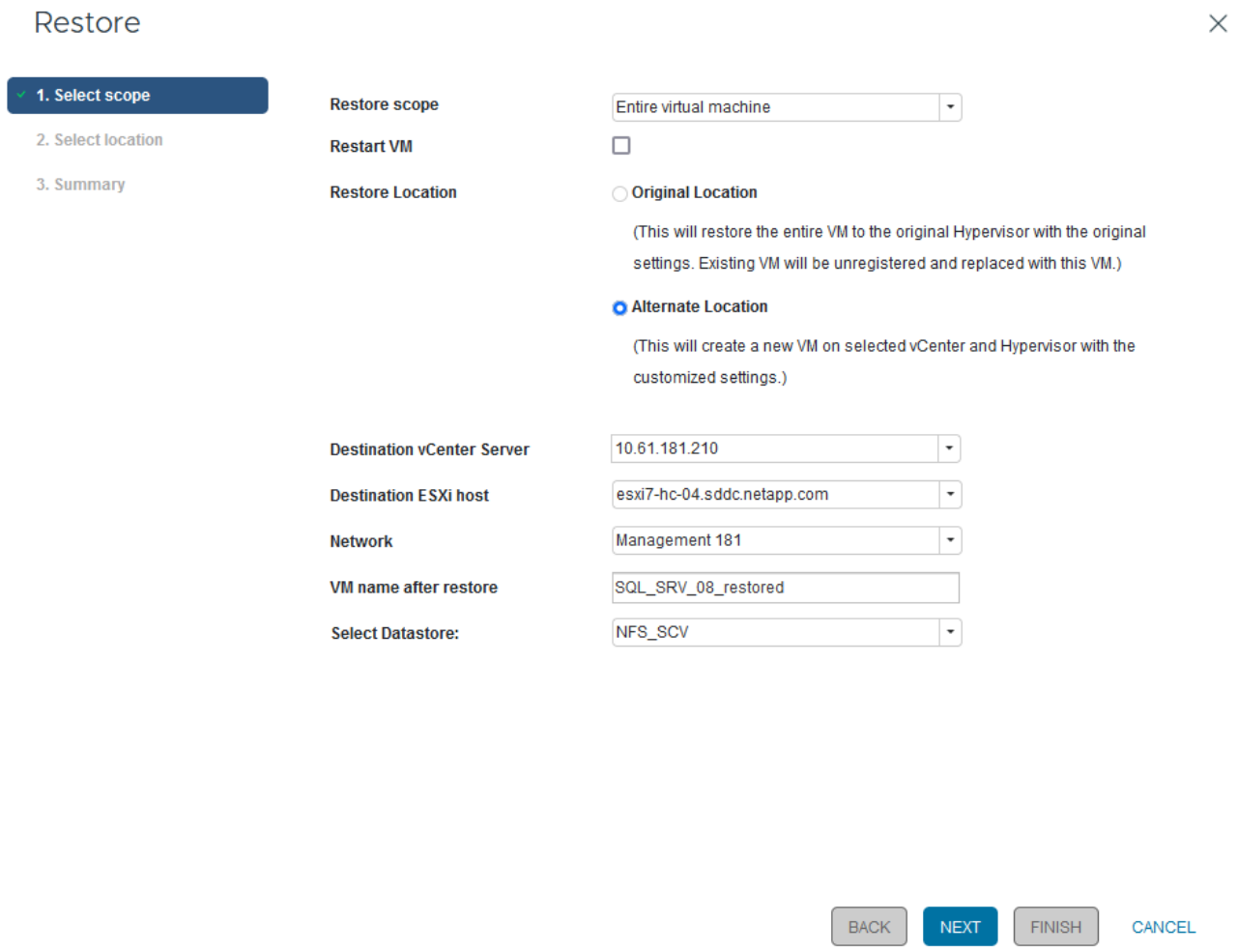
1. vCenter 클라이언트에서 *인벤토리 > 스토리지*로 이동한 다음 복원하려는 가상 머신이 포함된 데이터 저장소를 클릭합니다.
2. 구성 탭에서 *백업*을 클릭하면 사용 가능한 백업 목록에 액세스할 수 있습니다.



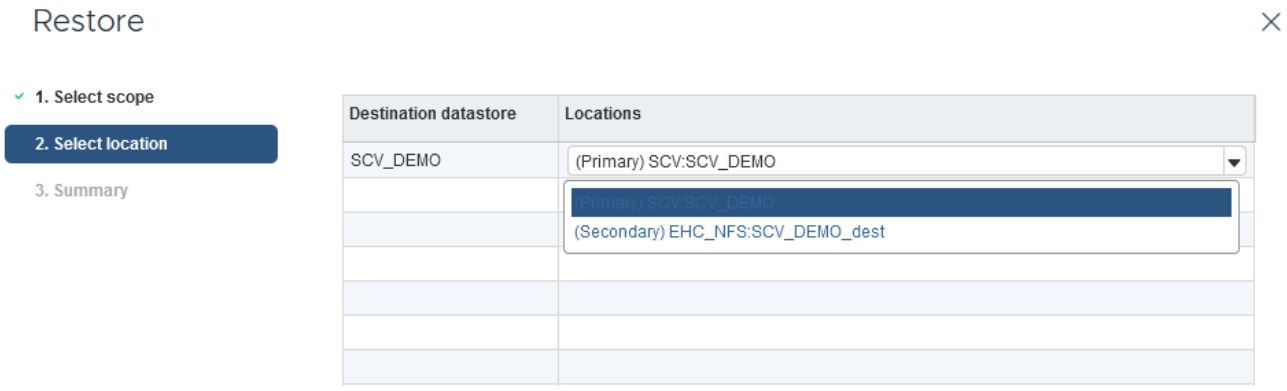
3. 백업을 클릭하여 VM 목록에 액세스한 다음 복원할 VM을 선택합니다. *복원*을 클릭하세요.



4. 복원 마법사에서 전체 가상 머신이나 특정 VMDK를 복원하도록 선택합니다. 원래 위치나 대체 위치에 설치할지 선택하고, 복원 후 VM 이름과 대상 데이터 저장소를 제공합니다. *다음*을 클릭하세요.



5. 기본 또는 보조 저장 위치에서 백업을 선택합니다.



6. 마지막으로 백업 작업 요약을 검토하고 마침을 클릭하여 복원 프로세스를 시작합니다.

가상 머신용 **NetApp Backup and Recovery**에서 가상 머신 복원

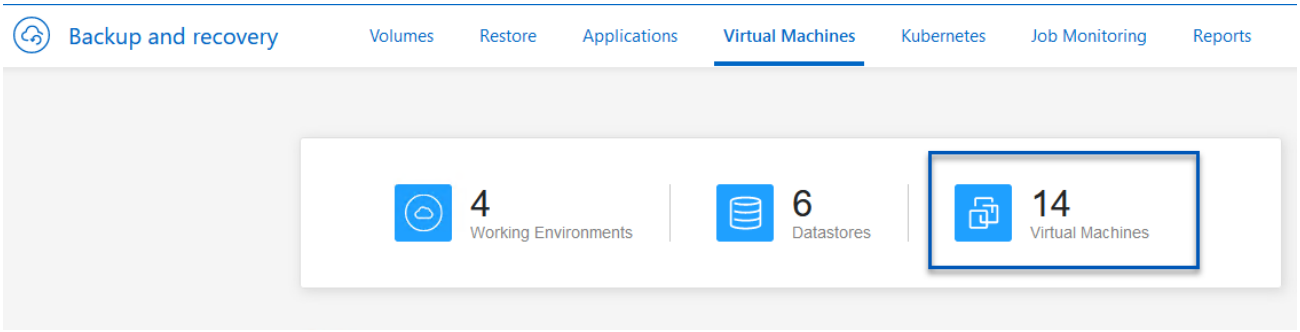
NetApp Backup and Recovery for Virtual Machines는 가상 머신을 원래 위치로 복원할 수 있도록 지원합니다. 복원 기능은 NetApp Backup and Recovery 웹 콘솔을 통해 액세스할 수 있습니다.

자세한 내용은 "클라우드에서 가상 머신 데이터 복원"을(를) 참조하십시오.

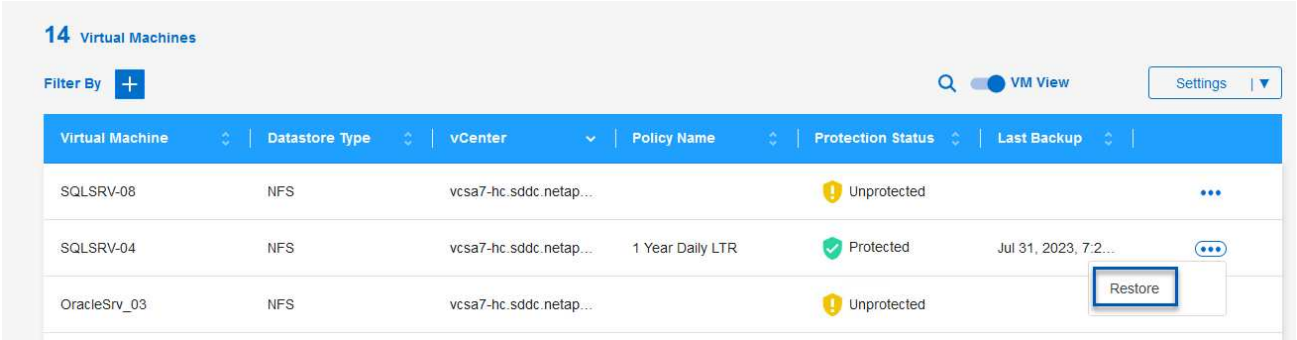
▼ **NetApp Backup and Recovery**에서 가상 머신 복원

NetApp Backup and Recovery에서 가상 머신을 복원하려면 다음 단계를 완료하십시오.

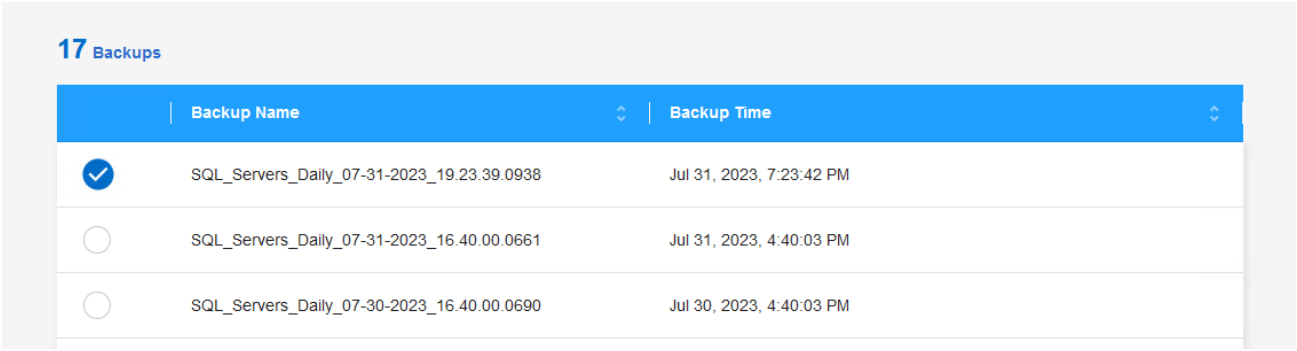
1. *보호 > 백업 및 복구 > 가상 머신*으로 이동한 후 가상 머신을 클릭하면 복원 가능한 가상 머신 목록을 볼 수 있습니다.



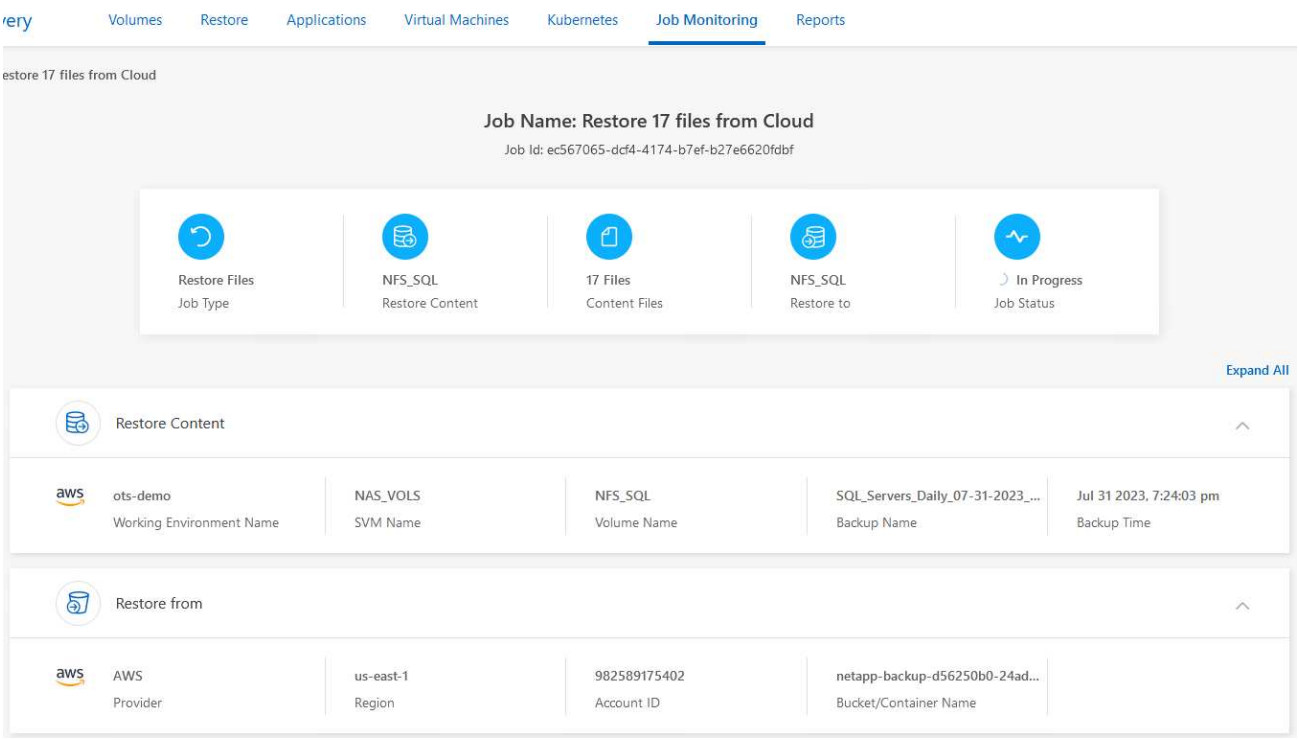
2. 복원할 VM의 설정 드롭다운 메뉴에 액세스하여 다음을 선택합니다.



3. 복원할 백업을 선택하고 *다음*을 클릭합니다.



4. 백업 작업 요약을 검토하고 *복원*을 클릭하여 복원 프로세스를 시작합니다.
5. 작업 모니터링 탭에서 복원 작업의 진행 상황을 모니터링합니다.



결론

가상 머신용 SnapCenter Plug-in for VMware vSphere 및 NetApp Backup and Recovery와 함께 구현된 3-2-1 백업 전략은 강력하고 안정적이며 비용 효율적인 데이터 보호 솔루션을 제공합니다. 이 전략은 데이터 중복성과 접근성을 보장할 뿐만 아니라, 온프레미스 ONTAP 스토리지 시스템과 클라우드 기반 오브젝트 스토리지 등 모든 위치에서 데이터를 복원할 수 있는 유연성을 제공합니다.

본 문서에 제시된 사용 사례는 NetApp, VMware 및 주요 클라우드 제공업체 간의 통합을 강조하는 검증된 데이터 보호 기술에 중점을 둡니다. SnapCenter Plug-in for VMware vSphere는 VMware vSphere와 원활하게 통합되어 데이터 보호 작업을 효율적이고 중앙 집중식으로 관리할 수 있도록 지원합니다. 이러한 통합을 통해 가상 머신의 백업 및 복구 프로세스가 간소화되어 VMware 에코시스템 내에서 손쉬운 예약, 모니터링 및 유연한 복원 작업이 가능해집니다. 가상 머신용 NetApp Backup and Recovery는 가상 머신 데이터를 클라우드 기반 오브젝트 스토리지에 안전하게 에어갭 백업으로 제공하여 3-2-1의 1을 구현합니다. 직관적인 인터페이스와 논리적인 워크플로는 중요 데이터의 장기 보관을 위한 안전한 플랫폼을 제공합니다.

추가 정보

이 솔루션에 제시된 기술에 대해 자세히 알아보려면 다음 추가 정보를 참조하세요.

- "SnapCenter Plug-in for VMware vSphere 설명서"
- "NetApp Console 설명서"

NetApp Disaster Recovery

개요

재해 복구는 모든 VMware 관리자의 최우선 관심사입니다. VMware는 전체 서버를 가상 머신을 구성하는 일련의 파일로 캡슐화하기 때문에 관리자는 클론, 스냅샷, 복제본 등 블록 스토리지 기반 기술을 활용하여 이러한 가상 머신을 보호합니다. ONTAP 어레이는 볼륨 데이터, 즉 지정된

데이터스토어 LUN에 있는 가상 머신을 한 사이트에서 다른 사이트로 전송하는 내장 복제 기능을 제공합니다. NetApp Disaster Recovery는 vSphere와 통합되어 재해 발생 시 원활한 페일오버 및 페일백을 위한 전체 워크플로를 자동화합니다. 스토리지 복제와 지능형 자동화를 결합함으로써 관리자는 이제 재해 복구 계획을 구성, 자동화 및 테스트할 뿐만 아니라 재해 발생 시 손쉽게 실행할 수 있는 관리 가능한 방법을 확보하게 되었습니다.

VMware vSphere 환경에서 DR 장애 조치에 가장 많은 시간이 소요되는 부분은 DR 사이트에서 VM의 인벤토리를 작성하고, 등록하고, 재구성하고, 전원을 켜는 데 필요한 단계를 실행하는 것입니다. 이상적인 솔루션은 RPO(분 단위)와 RTO(분 단위에서 시간 단위)가 모두 낮습니다. DR 솔루션에서 종종 간과되는 요소 중 하나는 주기적으로 DR 솔루션을 효율적으로 테스트하는 능력입니다.

DR 솔루션을 설계하려면 다음 요소를 염두에 두십시오.

- 복구 시간 목표(RTO). RTO는 기업이 재해로부터 얼마나 빨리 복구할 수 있는지를 나타내는 지표로, 더 구체적으로는 비즈니스 서비스를 다시 사용할 수 있도록 복구 프로세스를 실행하는 데 걸리는 시간을 나타냅니다.
- 복구 지점 목표(RPO) RPO는 재해가 발생한 시간을 기준으로 복구된 데이터가 사용 가능해진 이후의 경과 시간을 말합니다.
- 확장성과 적응성. 이 요소에는 수요가 증가함에 따라 저장 리소스를 점진적으로 늘릴 수 있는 능력이 포함됩니다.

사용 가능한 솔루션에 대한 자세한 기술 정보는 다음을 참조하세요.

- "NFS 데이터스토어용 NetApp Disaster Recovery"
- "VMFS 데이터스토어용 NetApp Disaster Recovery"

NFS 데이터스토어용 NetApp Disaster Recovery

NFS 데이터스토어용 NetApp Disaster Recovery

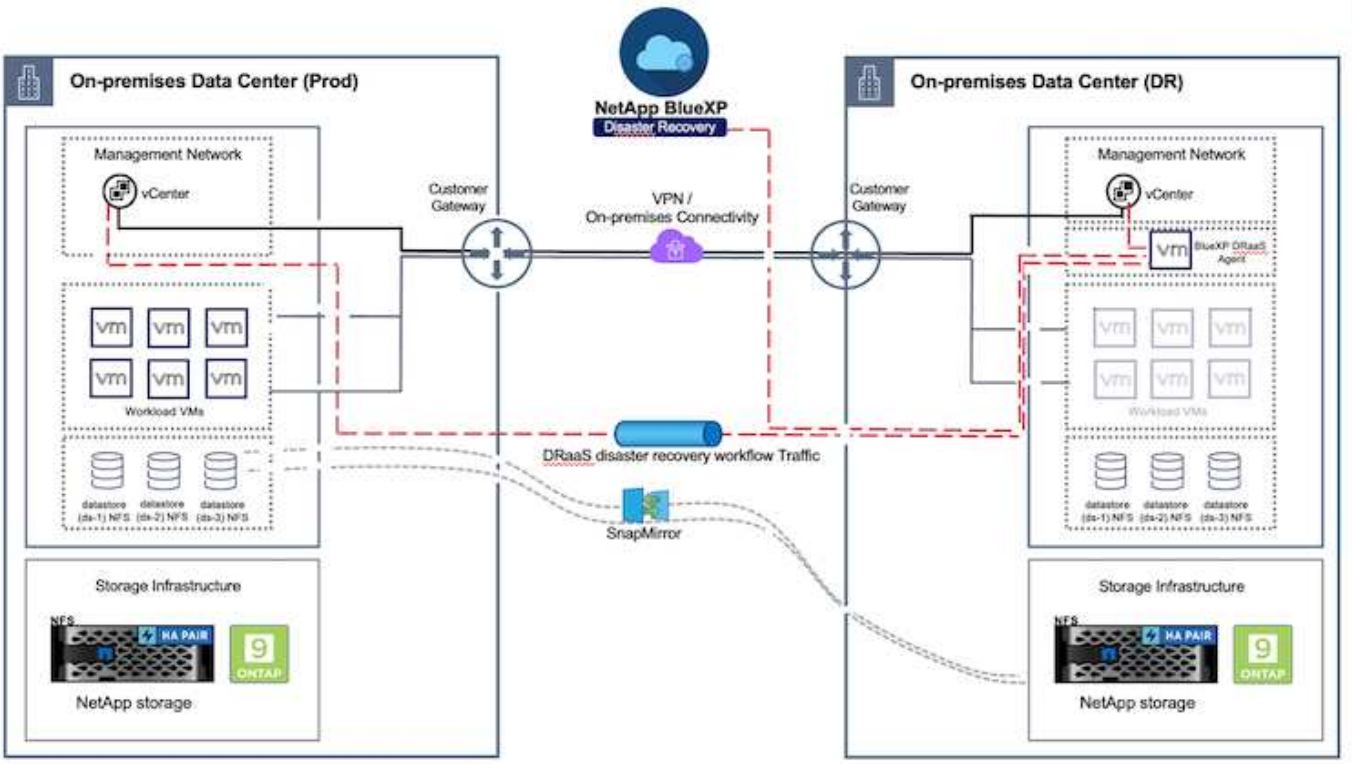
운영 사이트에서 재해 복구 사이트로 블록 수준 복제를 통해 재해 복구를 구현하는 것은 랜섬웨어 공격과 같은 사이트 중단 및 데이터 손상 이벤트로부터 작업 부하를 보호하는 탄력적이고 비용 효율적인 방법입니다. NetApp SnapMirror 복제를 사용하면 NFS 데이터 저장소가 있는 온프레미스 ONTAP 시스템에서 실행되는 VMware 워크로드를 VMware가 배포된 지정된 복구 데이터 센터에 있는 다른 ONTAP 스토리지 시스템으로 복제할 수 있습니다.

이 문서의 이 섹션에서는 온프레미스 VMware VM을 지정된 다른 사이트로 재해 복구하도록 NetApp Disaster Recovery를 구성하는 방법을 설명합니다. 이 설정의 일부로 콘솔 에이전트, ONTAP 어레이 온보딩, 사이트 정의 및 VMware vCenter 연결이 포함됩니다. 또한 이 문서에서는 사이트 간 복제를 구성하는 방법과 복구 계획을 설정하고 테스트하는 방법을 자세히 설명합니다. 마지막 섹션에서는 전체 사이트 페일오버 수행 방법과 기본 사이트가 복구되어 온라인 상태가 되었을 때 페일백하는 방법에 대한 지침을 제공합니다.

NetApp Data Services의 일부인 재해 복구를 활용하여 기업은 온프레미스 VMware vCenters 및 ONTAP 스토리지를 쉽게 탐색할 수 있습니다. 그런 다음 조직은 리소스 그룹을 생성하고, 재해 복구 계획을 생성하여 리소스 그룹과 연결한 후, 페일오버 및 페일백을 테스트하거나 실행할 수 있습니다. SnapMirror는 스토리지 수준의 블록 복제를 제공하여 두 사이트를 증분 변경 사항으로 최신 상태로 유지함으로써 최대 5분의 RPO(복구 시점 목표)를 달성합니다. 또한 프로덕션 환경에 영향을 주거나 추가 스토리지 비용을 발생시키지 않고 재해 복구 절차를 시뮬레이션할 수 있습니다.

재해 복구는 ONTAP의 FlexClone 기술을 활용하여 재해 복구 사이트에 마지막으로 복제된 스냅샷에서 NFS 데이터 저장소의 공간 효율적인 복사본을 생성합니다. 재해 복구 테스트를 완료한 후, 고객은 실제 복제된 프로덕션 리소스에 영향을 주지 않고 테스트 환경을 쉽게 삭제할 수 있습니다. 실제 페일오버가 발생할 경우, 재해 복구는 몇 번의

클릭만으로 지정된 재해 복구 사이트에서 보호된 가상 머신을 자동으로 시작하는 데 필요한 모든 단계를 오케스트레이션합니다. 또한 이 서비스는 필요한 경우 페일백 작업을 위해 SnapMirror 관계를 기본 사이트로 반전시키고 보조 사이트의 변경 사항을 기본 사이트로 복제합니다. 이러한 모든 기능은 다른 유명 대안에 비해 훨씬 저렴한 비용으로 제공됩니다.

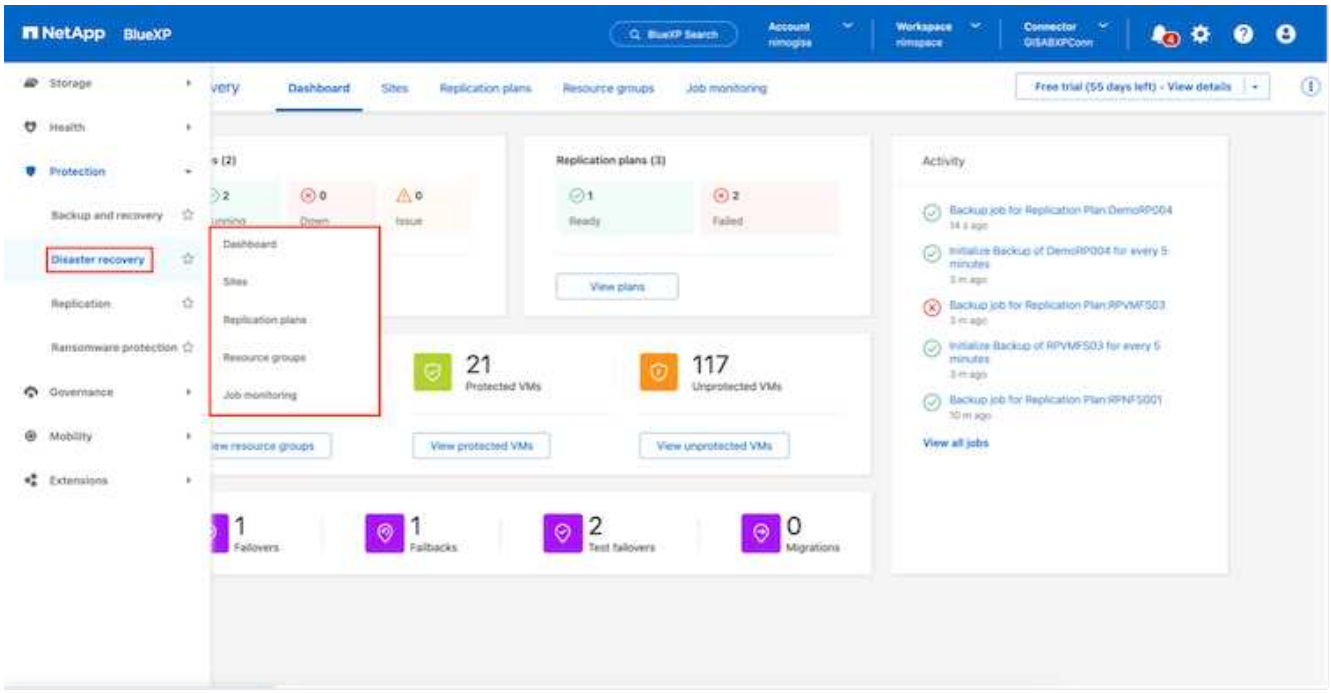


재해 복구용 vCenter Server, ESXi 및 ONTAP의 최신 정보 및 지원되는 버전에 대해서는 "재해 복구 지원 구성"을(를) 참조하십시오.

시작하기

NetApp Disaster Recovery를 시작하려면 NetApp 콘솔을 사용한 다음 서비스에 액세스하십시오.

1. 콘솔에 로그인하십시오.
2. 콘솔 왼쪽 탐색 메뉴에서 보호 > 재해 복구를 선택합니다.
3. 재해 복구 대시보드가 나타납니다.

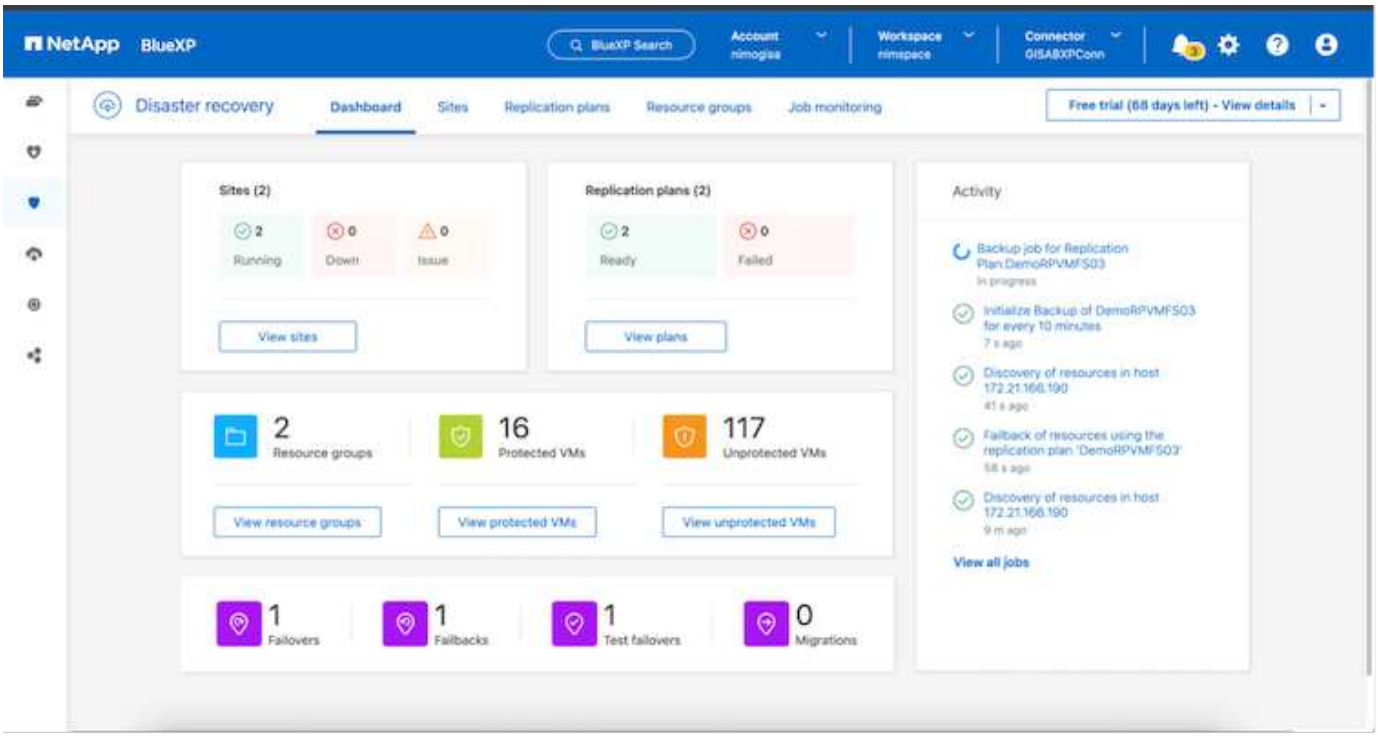


재해 복구 계획을 구성하기 전에 다음 사전 요구 사항이 충족되었는지 확인하십시오.

- 콘솔 에이전트가 배포되었습니다.
- 에이전트는 소스 및 대상 vCenter 및 스토리지 시스템에 대한 연결성을 갖습니다.
- NFS 서비스가 활성화된 SVM이 포함된 ONTAP 클러스터를 사용할 수 있습니다.
- VMware용 NFS 데이터스토어를 호스팅하는 온프레미스 NetApp 스토리지 시스템이 콘솔에 추가됩니다.
- DNS 이름을 사용하는 경우 DNS 확인이 이루어져야 합니다. 그렇지 않은 경우 vCenter에 IP 주소를 사용하세요.
- SnapMirror 복제는 지정된 NFS 기반 데이터 저장소 볼륨에 대해 구성됩니다.
- 해당 환경에 지원되는 vCenter Server 및 ESXi 서버 버전이 있는지 확인하세요.

소스 사이트와 대상 사이트 간의 연결이 설정되면 구성 단계를 진행하세요. 이 작업은 몇 번의 클릭과 약 3~5분 정도 소요됩니다.

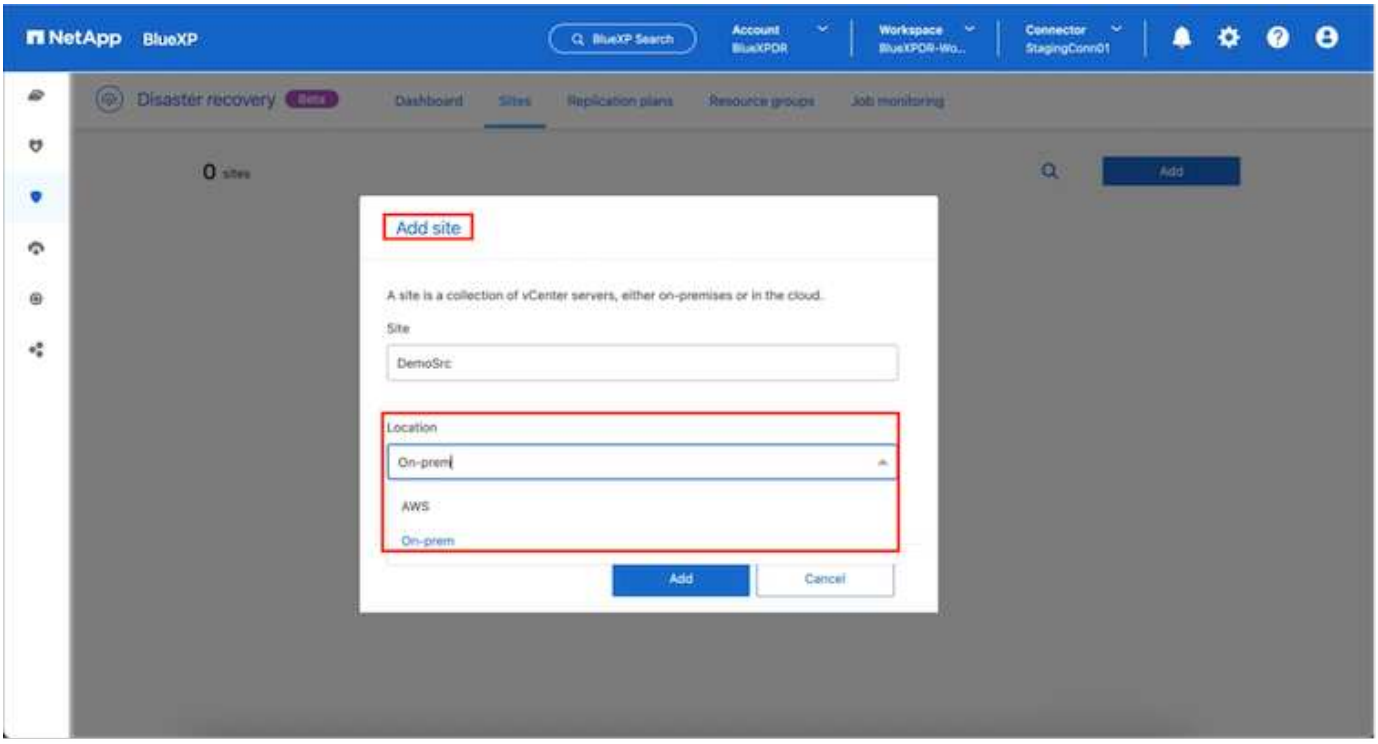
NetApp은 콘솔 에이전트가 네트워크를 통해 소스 및 대상 리소스와 통신할 수 있도록 콘솔 에이전트를 대상 사이트 또는 제3의 사이트에 배포하는 것을 권장합니다.



NetApp Disaster Recovery 구성

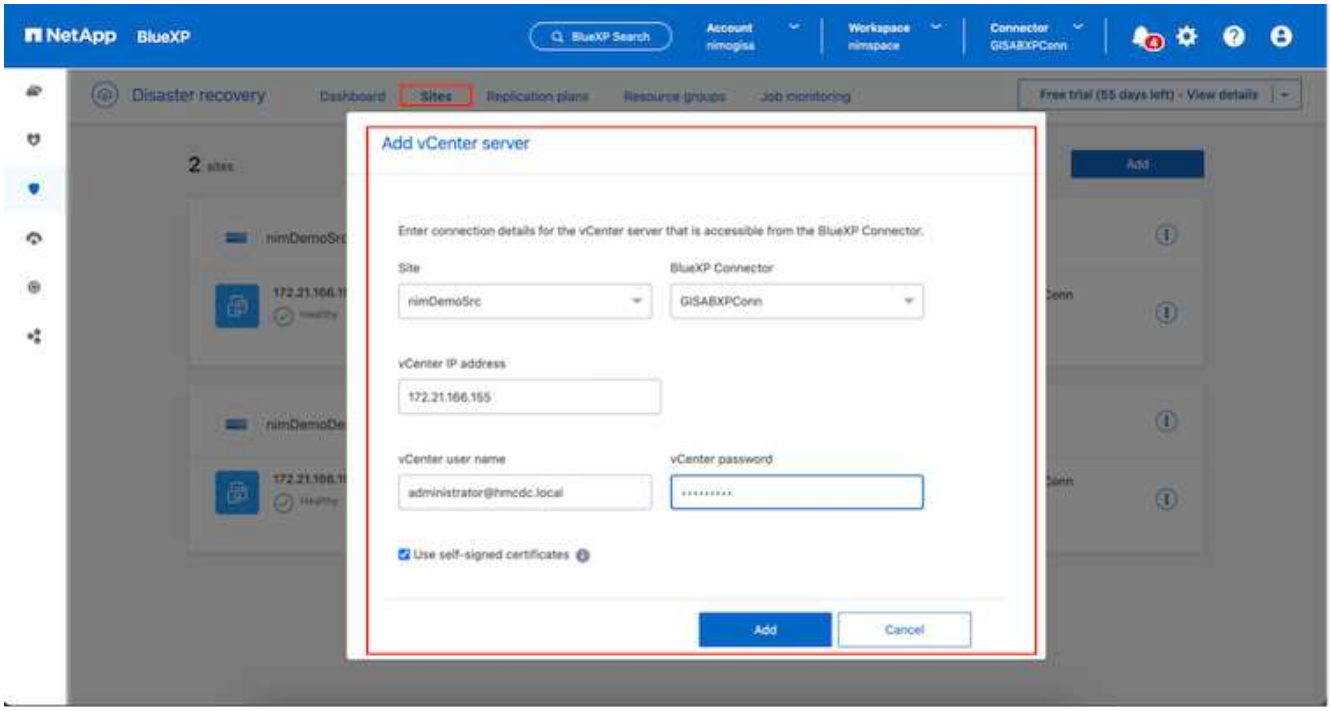
재해 복구를 준비하는 첫 번째 단계는 온프레미스 vCenter 및 스토리지 리소스를 탐색하고 NetApp Disaster Recovery에 추가하는 것입니다.

콘솔을 열고 왼쪽 탐색 메뉴에서 보호 **>** 재해 복구*를 선택합니다**.** *사이트*를 클릭하고 이름을 입력한 다음 위치 유형을 선택합니다**.** 그런 다음 ***vCenter** 추가 버튼을 클릭합니다.

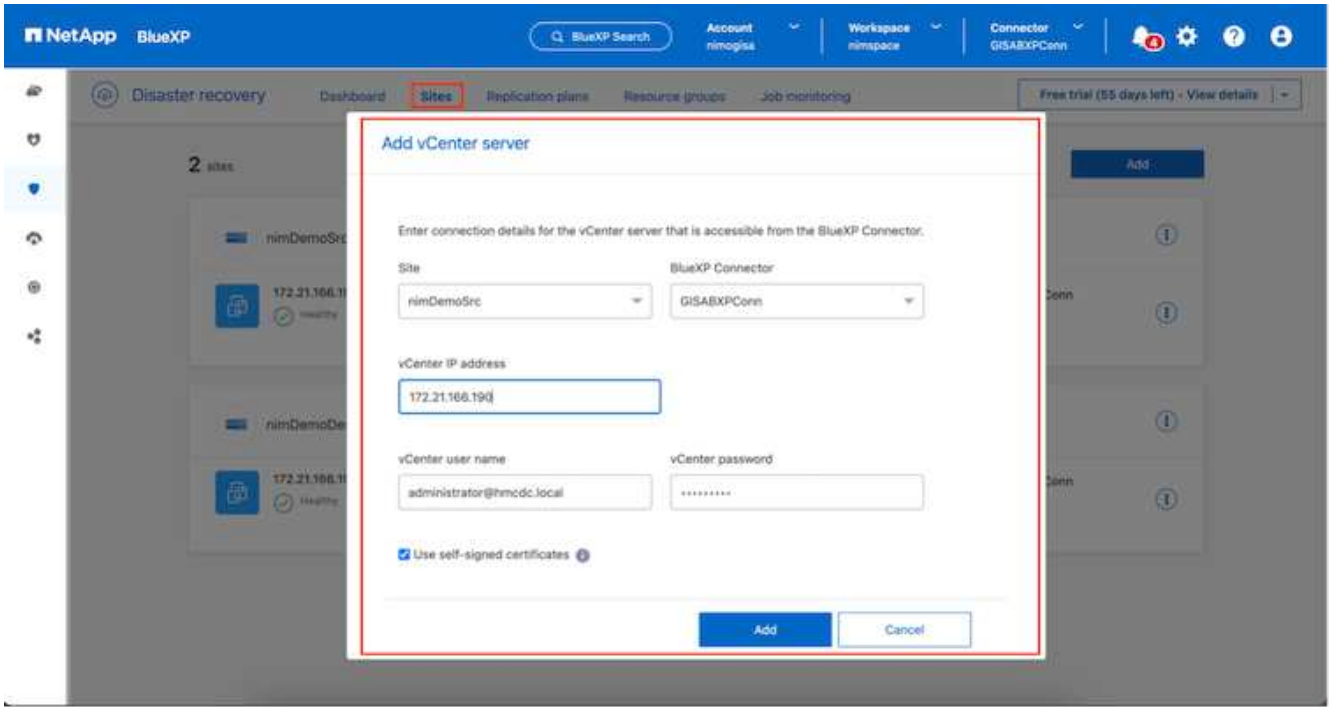


다음 플랫폼을 추가하세요:

- 원천. 온프레미스 vCenter.



- 목적지. VMC SDDC vCenter.



vCenter가 추가되면 자동 검색이 실행됩니다.

소스 사이트 배열과 대상 사이트 배열 간 스토리지 복제 구성

SnapMirror는 NetApp 환경에서 데이터 복제를 제공합니다. NetApp 스냅샷 기술을 기반으로 구축된 SnapMirror 복제는 이전 업데이트 이후 변경되거나 추가된 블록만 복제하므로 매우 효율적입니다. SnapMirror는 NetApp OnCommand System Manager 또는 ONTAP CLI를 사용하여 쉽게 구성할 수 있습니다. NetApp Data Services 또한

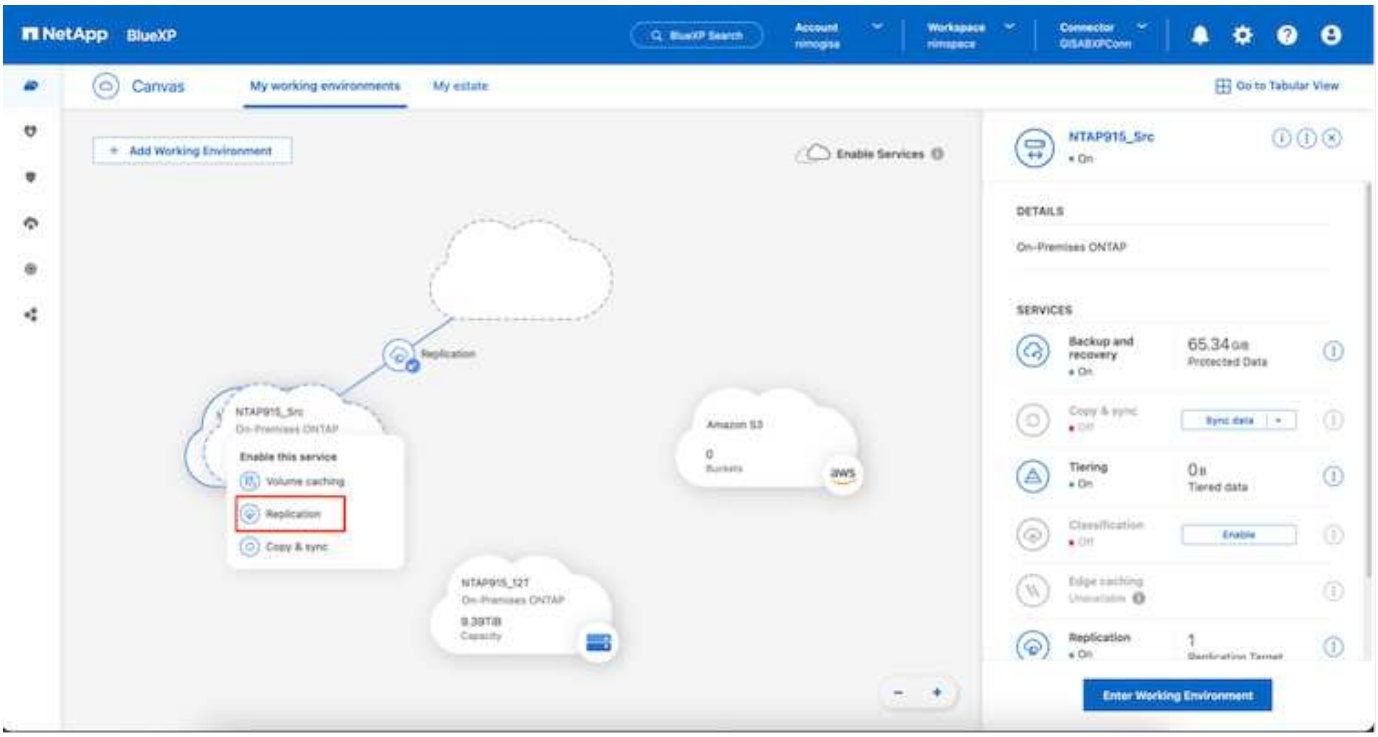
클러스터 및 SVM 피어링이 사전에 구성된 경우 SnapMirror 관계를 생성합니다.

기본 스토리지가 완전히 손실되지 않은 경우, SnapMirror는 기본 사이트와 DR 사이트를 효율적으로 재동기화하는 방법을 제공합니다. SnapMirror는 단순히 SnapMirror 관계를 반전시키는 것만으로 DR 사이트에서 기본 사이트로 변경되거나 새로 추가된 데이터만 전송하여 두 사이트를 재동기화할 수 있습니다. 즉, 재해 복구의 복제 계획은 장애 조치 후 전체 볼륨을 다시 복사하지 않고도 양방향으로 재동기화할 수 있습니다. 관계를 역방향으로 재동기화하는 경우, 스냅샷 복사본의 마지막 성공적인 동기화 이후 기록된 새로운 데이터만 대상으로 다시 전송됩니다.

CLI 또는 System Manager를 통해 볼륨에 대해 SnapMirror 관계가 이미 구성된 경우, NetApp Data Services는 해당 관계를 가져와 나머지 워크플로 작업을 계속 진행합니다.

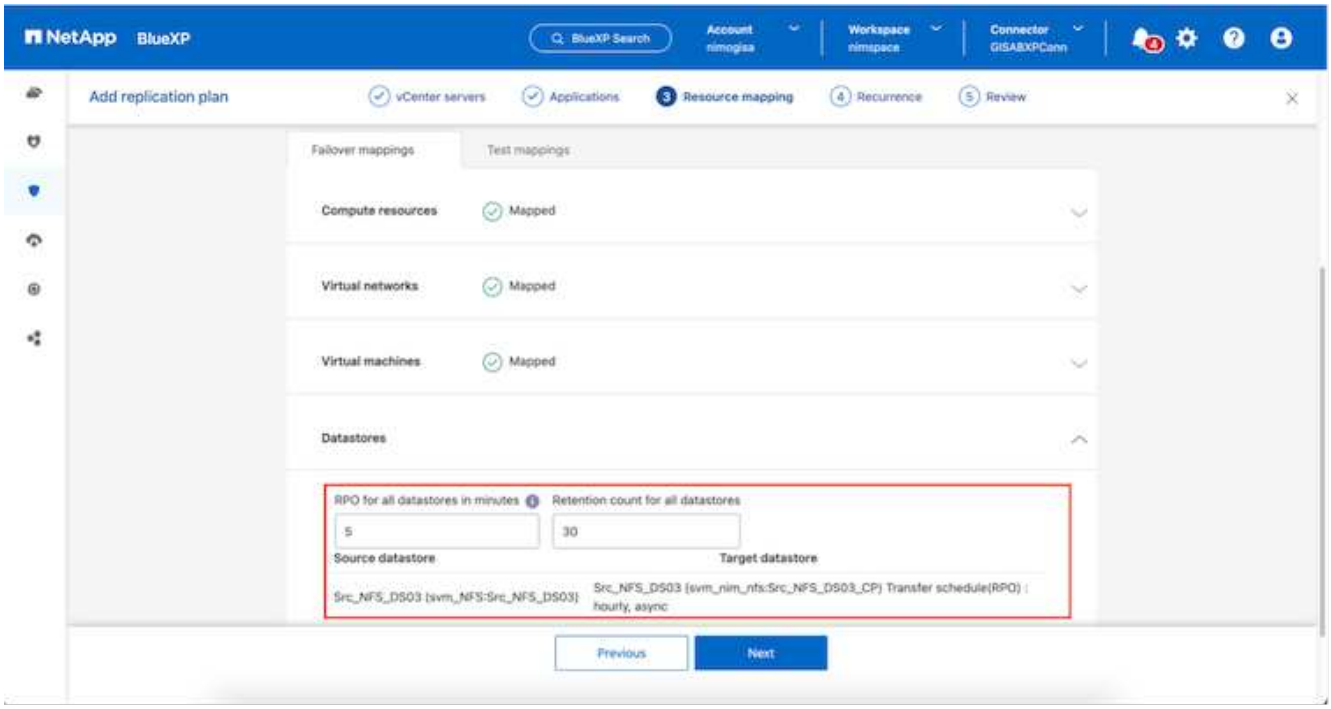
VMware 재해 복구를 설정하는 방법

SnapMirror 복제를 생성하는 프로세스는 모든 애플리케이션에 대해 동일합니다. 이 프로세스는 수동 또는 자동화 방식으로 진행할 수 있습니다. 가장 쉬운 방법은 NetApp Console을 활용하여 환경 내의 소스 ONTAP 시스템을 대상으로 간단히 드래그 앤 드롭하는 방식으로 SnapMirror 복제를 구성하는 것입니다. 그러면 마법사가 실행되어 나머지 프로세스를 안내합니다.



재해 복구는 다음 두 가지 기준이 충족될 경우 이를 자동화할 수도 있습니다:

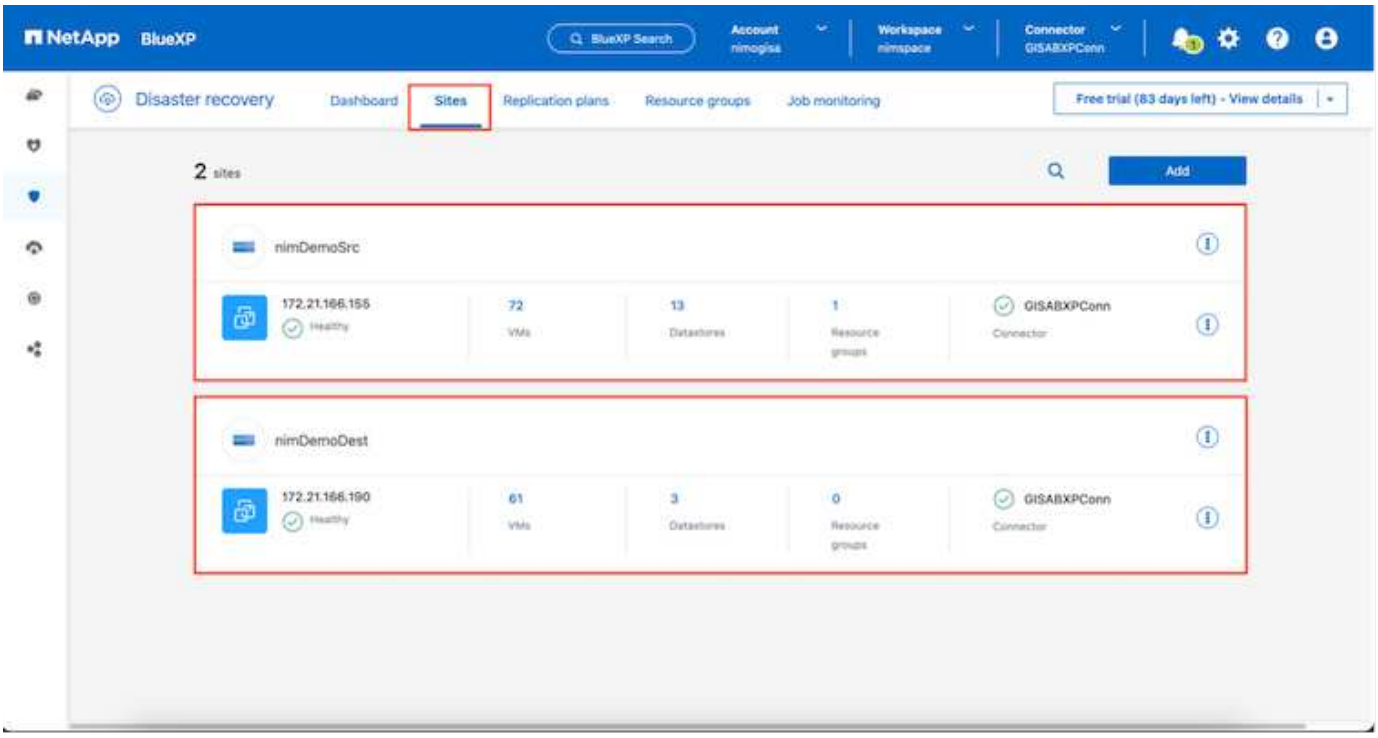
- 소스 클러스터와 대상 클러스터는 피어 관계를 갖습니다.
- 소스 SVM과 대상 SVM은 피어 관계를 갖습니다.



CLI를 통해 볼륨에 대해 SnapMirror 관계가 이미 구성된 경우, 재해 복구는 해당 관계를 가져와 나머지 워크플로 작업을 계속 진행합니다.

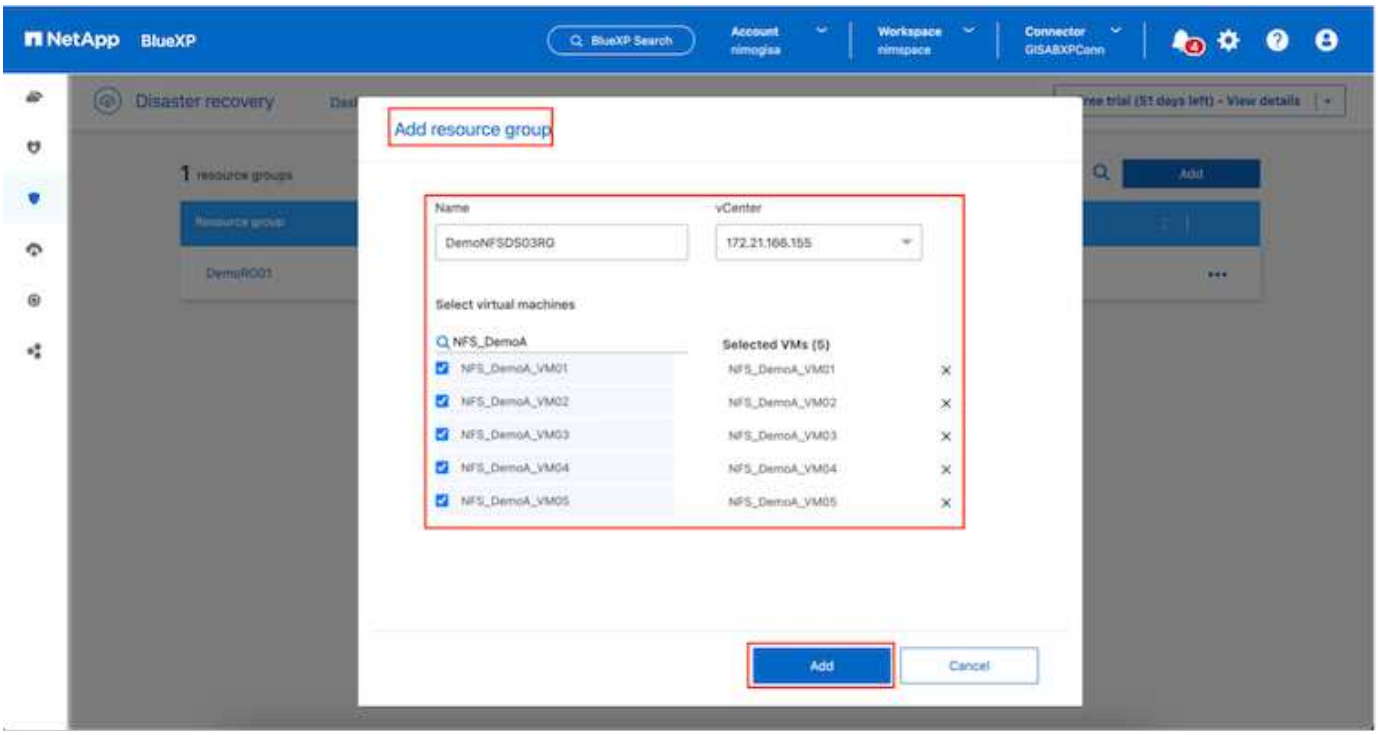
재해 복구는 어떤 도움을 줄 수 있습니까**?**

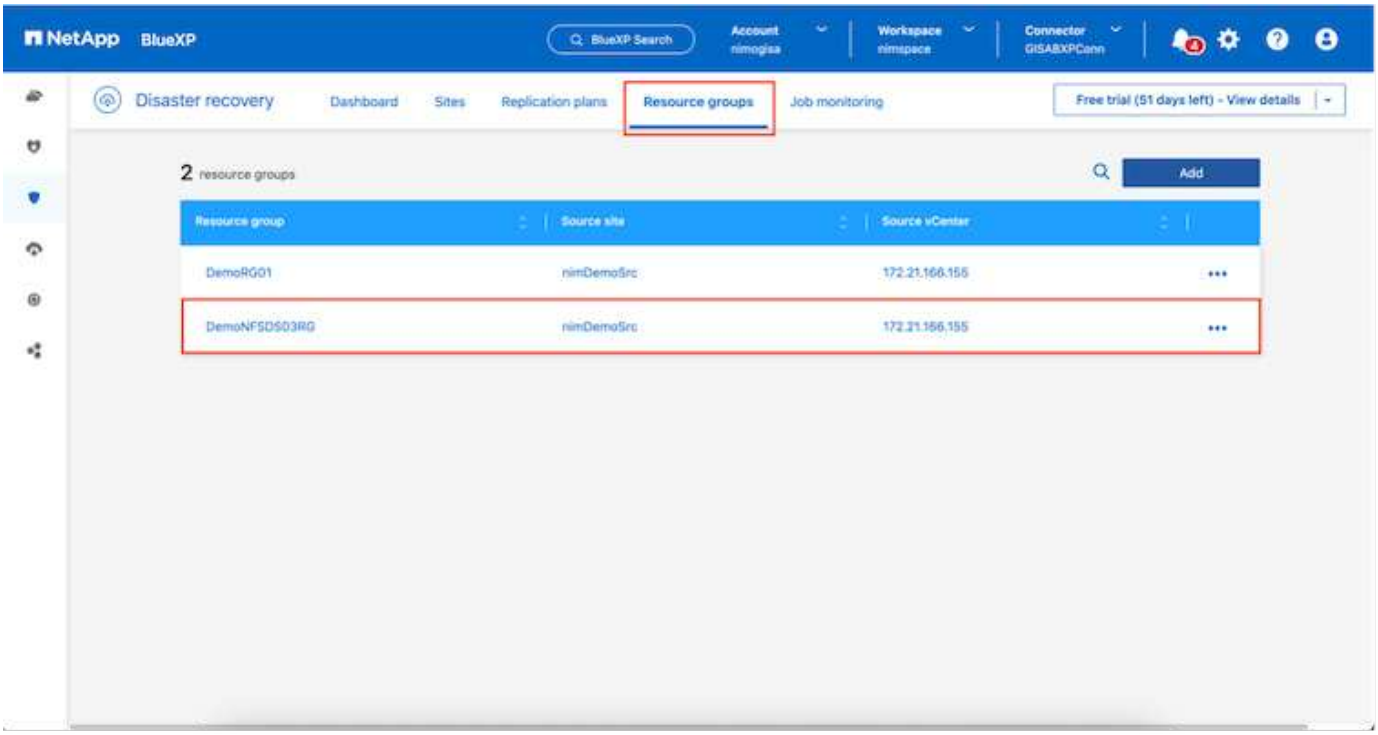
소스 및 대상 사이트가 추가되면 Disaster Recovery는 자동 심층 탐색을 수행하여 관련 메타데이터와 함께 VM을 표시합니다. 또한 Disaster Recovery는 VM에서 사용하는 네트워크 및 포트 그룹을 자동으로 감지하여 채웁니다.



사이트를 추가한 후에는 VM을 리소스 그룹으로 묶을 수 있습니다. 재해 복구 리소스 그룹을 사용하면 종속 VM들을

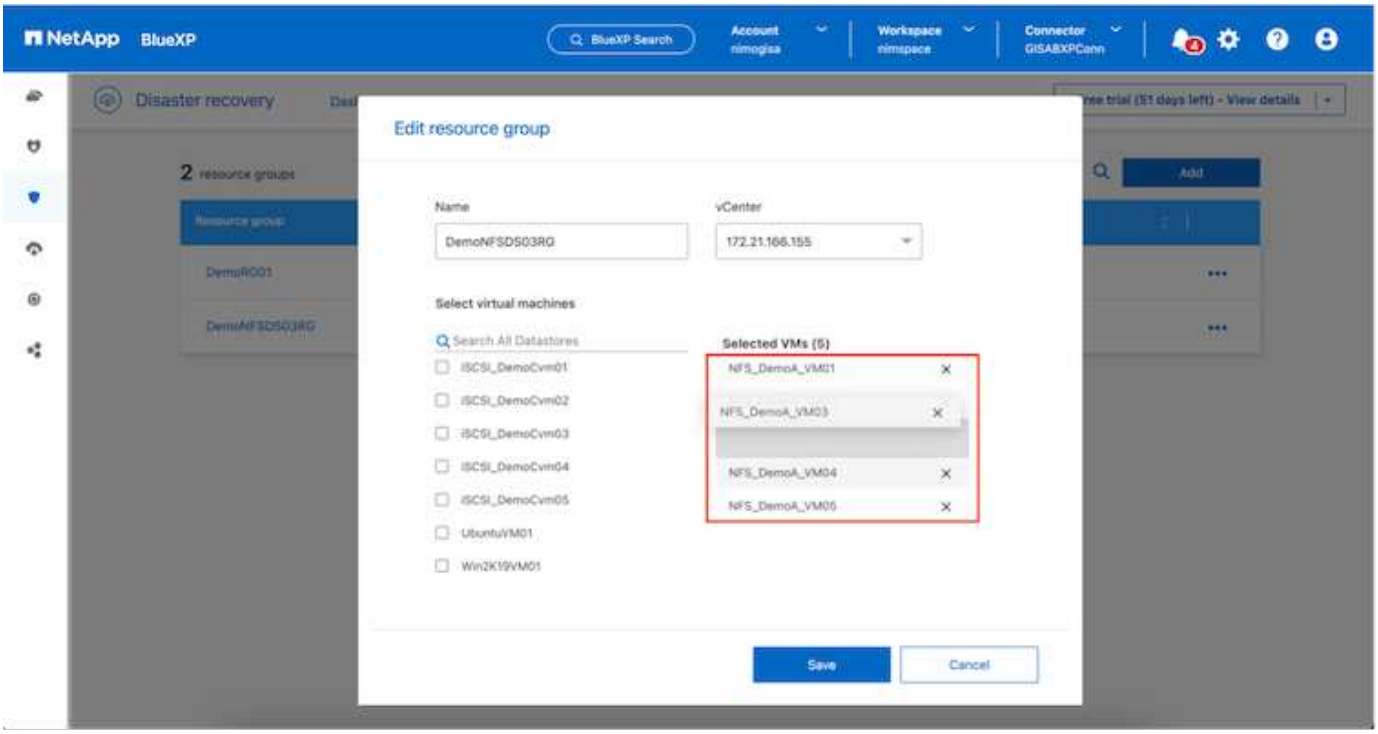
논리적 그룹으로 묶고, 복구 시 실행될 부팅 순서와 부팅 지연 시간을 지정할 수 있습니다. 리소스 그룹 생성을 시작하려면 *리소스 그룹*으로 이동하여 *새 리소스 그룹 만들기*를 클릭하십시오.



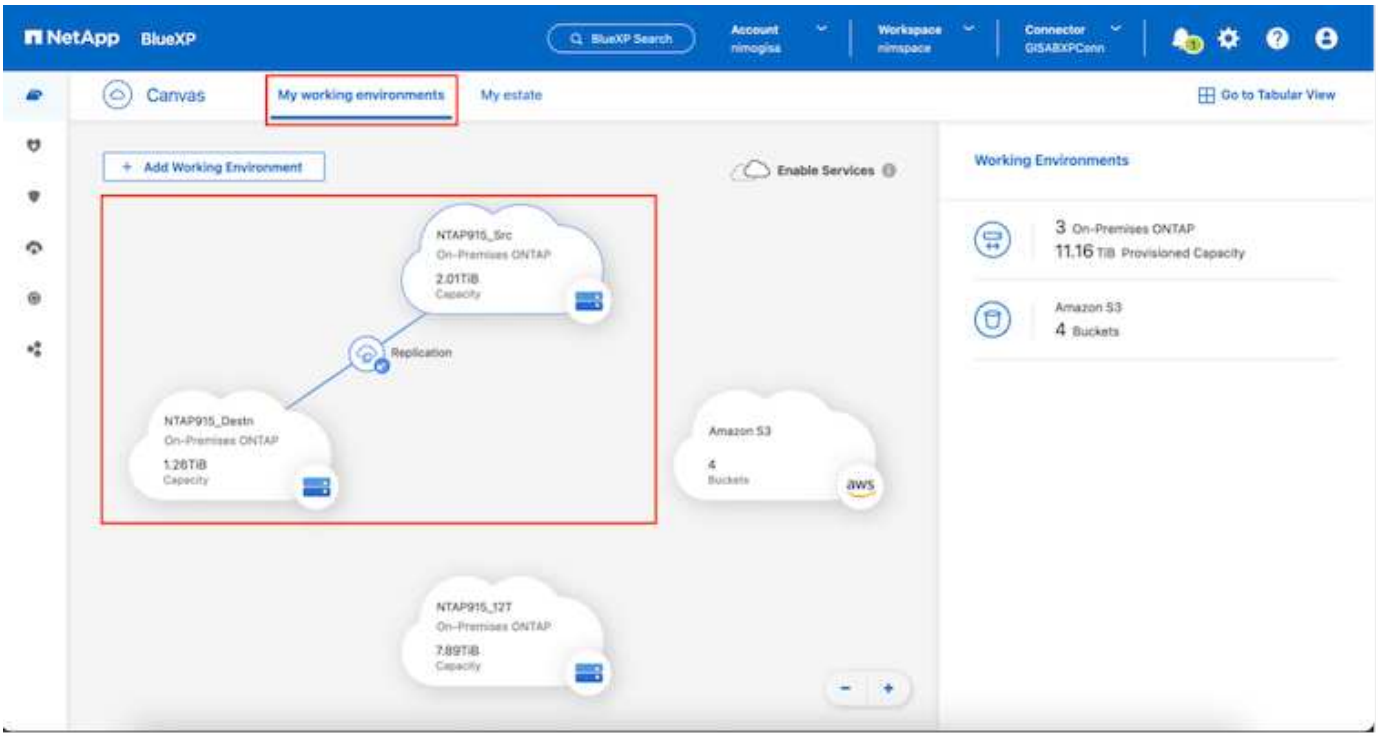


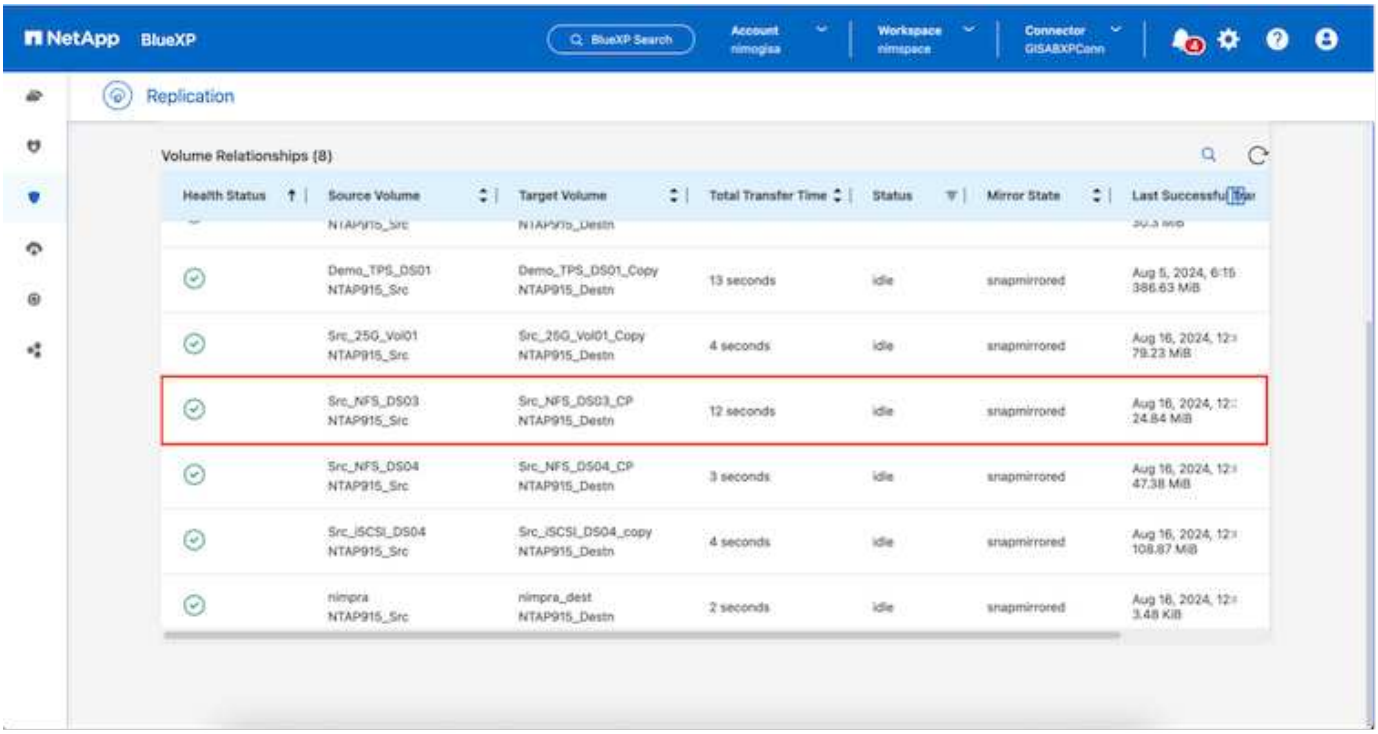
리소스 그룹은 복제 계획을 생성하는 동안에도 생성될 수 있습니다.

리소스 그룹을 만드는 동안 간단한 드래그 앤 드롭 메커니즘을 사용하여 VM의 부팅 순서를 정의하거나 수정할 수 있습니다.



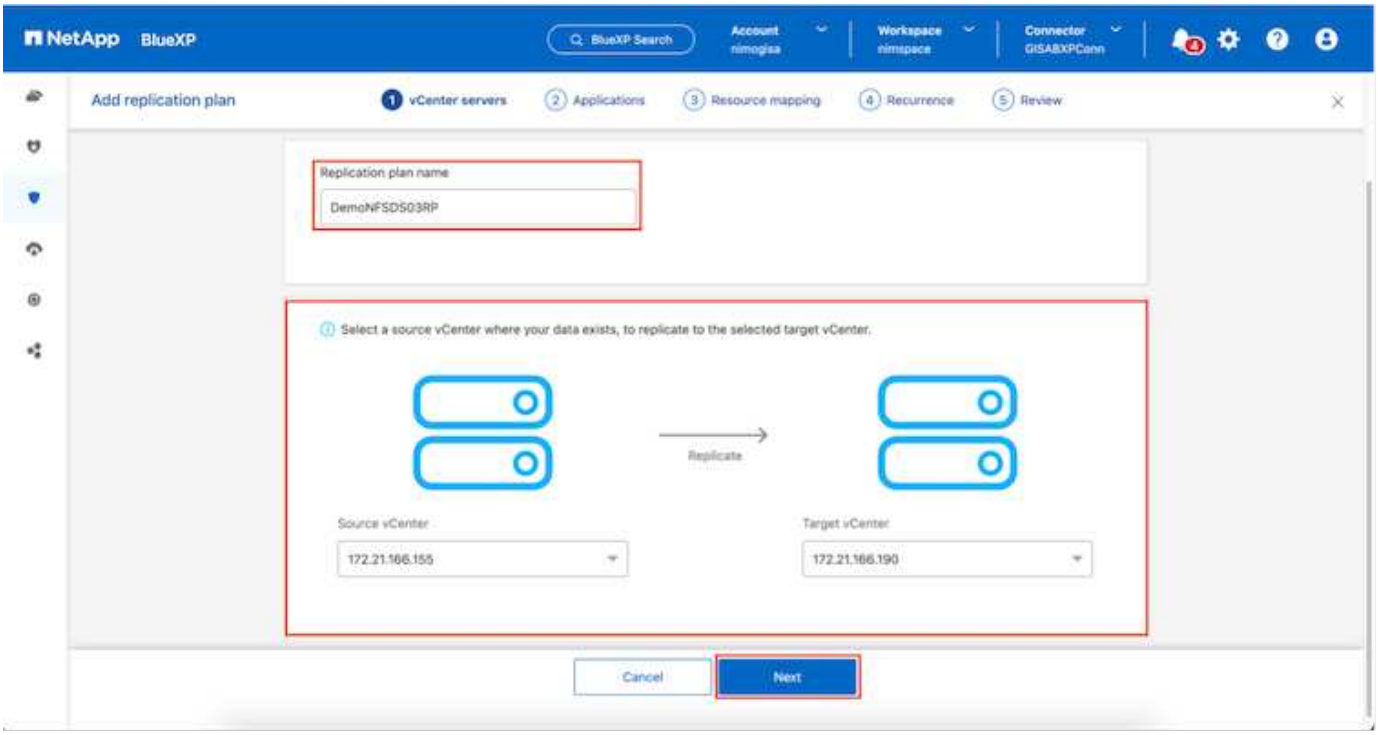
리소스 그룹을 만든 후 다음 단계는 재해 발생 시 가상 머신과 애플리케이션을 복구하기 위한 실행 청사진 또는 계획을 만드는 것입니다. 필수 구성 요소에서 언급했듯이 SnapMirror 복제는 사전에 구성할 수 있으며, DRaaS는 복제 계획을 만드는 동안 지정된 RPO 및 보존 횟수를 사용하여 구성할 수 있습니다.



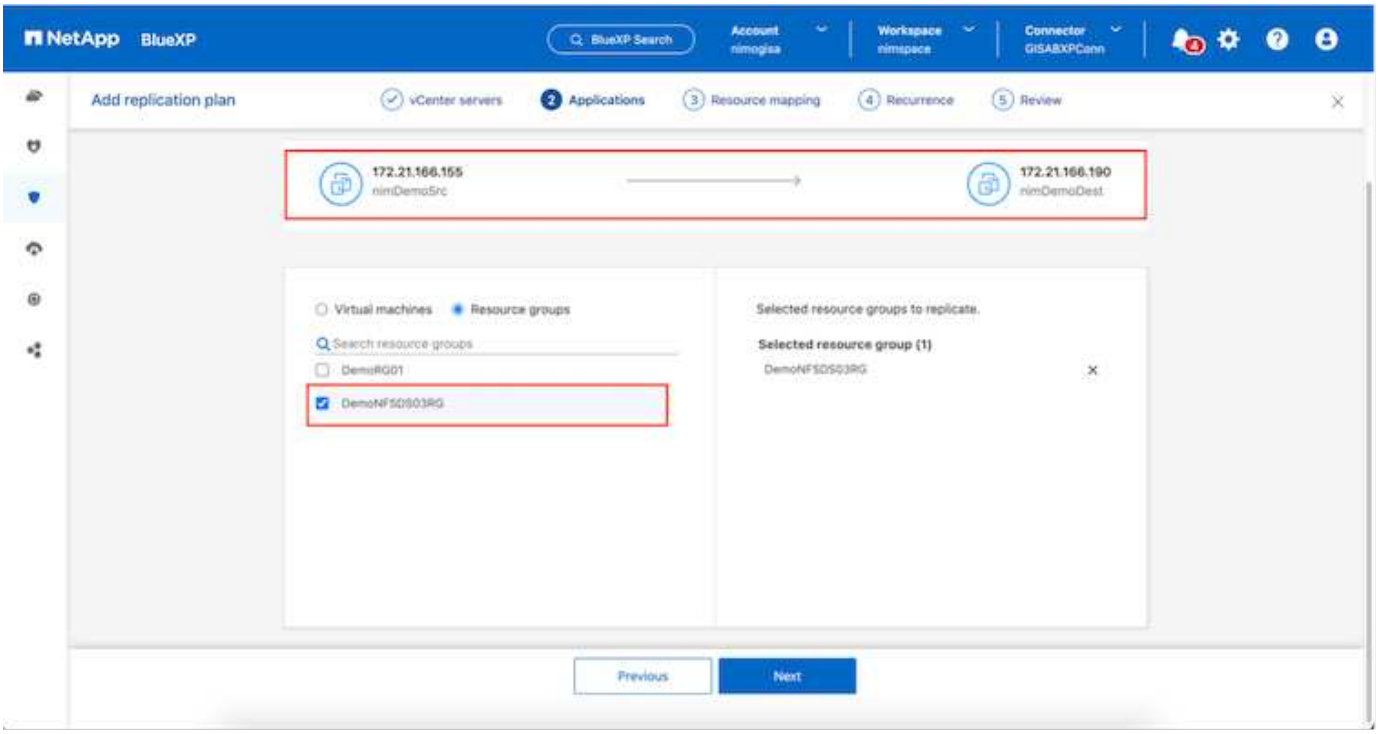


드롭다운에서 소스 및 대상 vCenter 플랫폼을 선택하여 복제 계획을 구성하고, 계획에 포함할 리소스 그룹을 선택하고, 애플리케이션을 복원하고 전원을 켜는 방법, 클러스터 및 네트워크 매핑을 그룹화합니다. 복구 계획을 정의하려면 복제 계획 탭으로 이동하여 *계획 추가*를 클릭합니다.

먼저 소스 vCenter를 선택한 다음 대상 vCenter를 선택합니다.



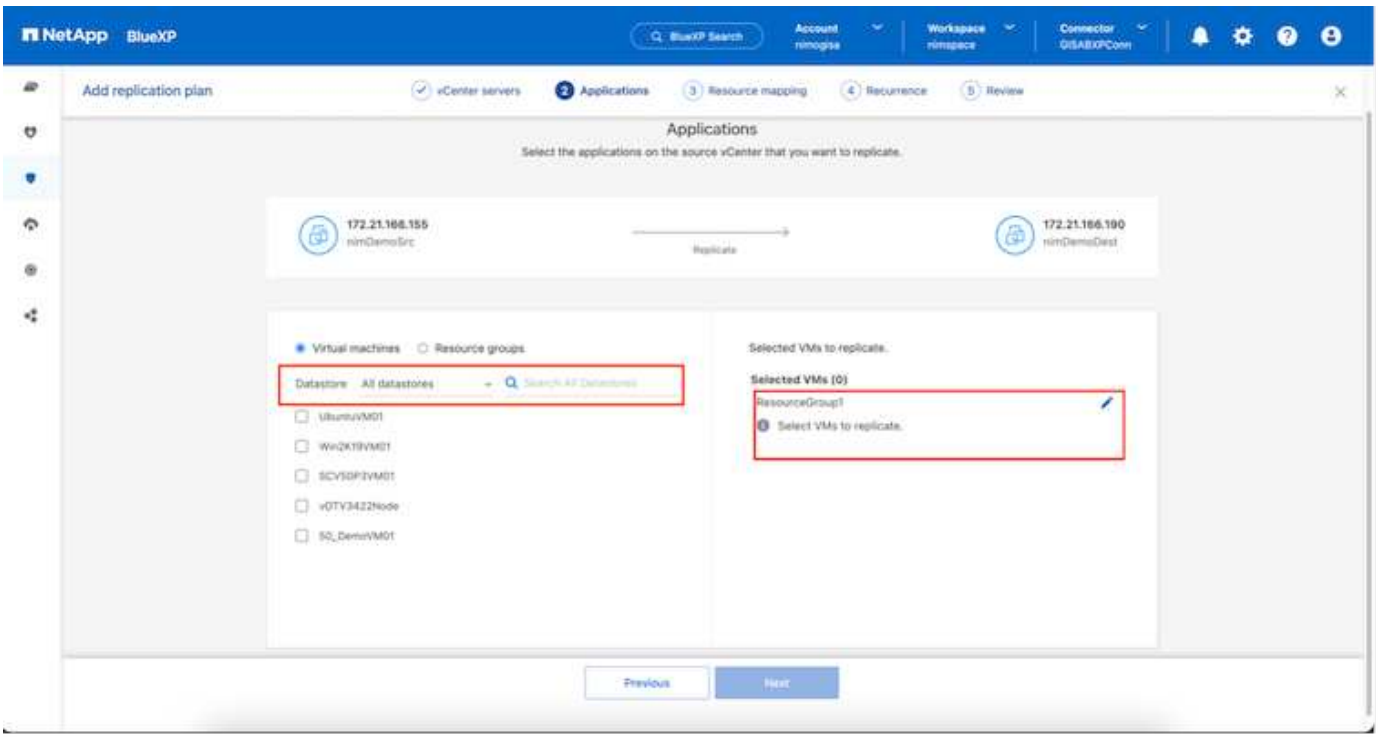
다음 단계는 기존 리소스 그룹을 선택하는 것입니다. 리소스 그룹이 생성되지 않은 경우 마법사는 복구 목표에 따라 필요한 가상 머신을 그룹화(기본적으로 기능적 리소스 그룹 생성)하는 데 도움을 줍니다. 이는 또한 애플리케이션 가상 머신을 복원하는 방법에 대한 작업 순서를 정의하는 데 도움이 됩니다.



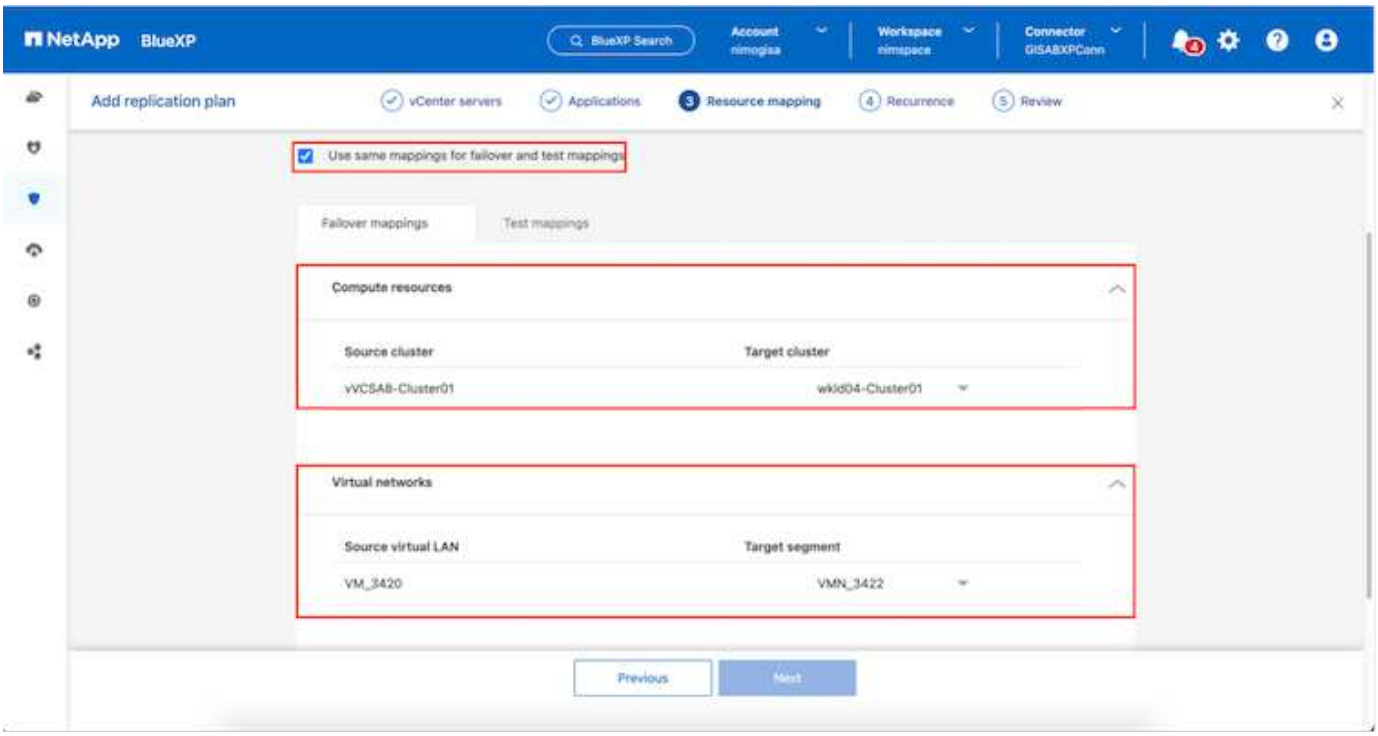
리소스 그룹을 사용하면 드래그 앤 드롭 기능을 사용하여 부팅 순서를 설정할 수 있습니다. 이를 사용하면 복구 프로세스 중에 VM의 전원이 켜지는 순서를 쉽게 수정할 수 있습니다.

리소스 그룹 내의 각 가상 머신은 순서에 따라 순차적으로 시작됩니다. 두 개의 리소스 그룹이 병렬로 시작됩니다.

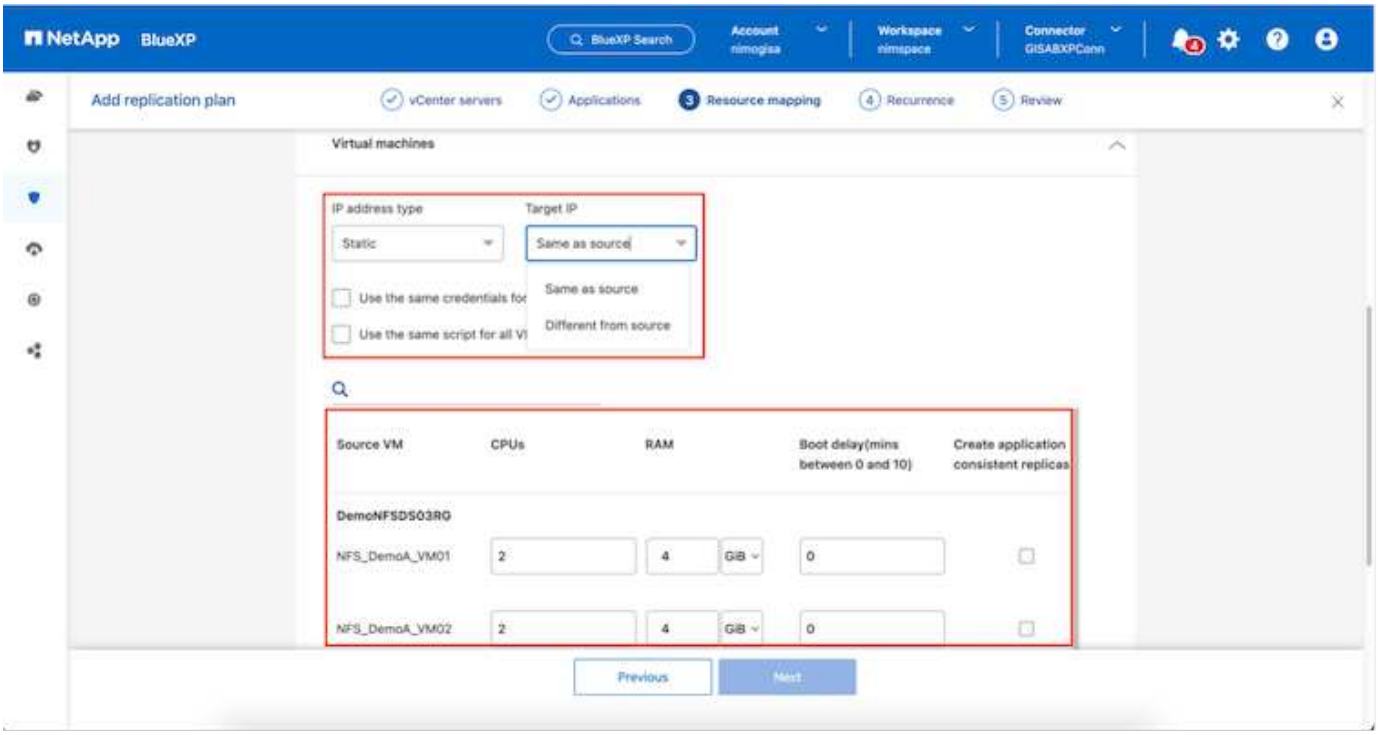
아래 스크린샷은 리소스 그룹이 사전에 생성되지 않은 경우 조직의 요구 사항에 따라 가상 머신이나 특정 데이터 저장소를 필터링하는 옵션을 보여줍니다.



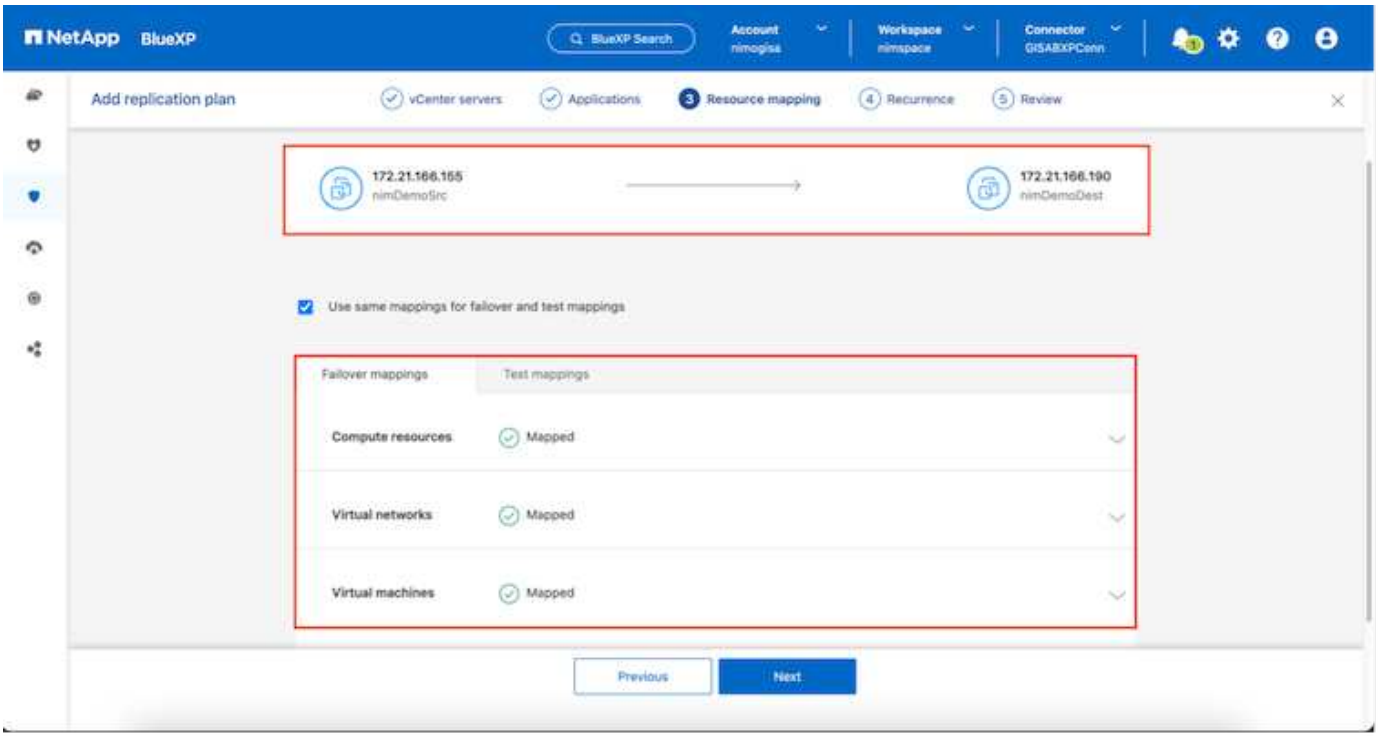
리소스 그룹을 선택한 후에는 장애 조치 매핑을 생성합니다. 이 단계에서는 소스 환경의 리소스가 대상에 어떻게 매핑되는지 지정합니다. 여기에는 컴퓨팅 리소스, 가상 네트워크, IP 사용자 지정, 사전 및 사후 스크립트, 부팅 지연, 애플리케이션 일관성 등이 포함됩니다. 자세한 내용은 "복제 계획 만들기"을(를) 참조하십시오.



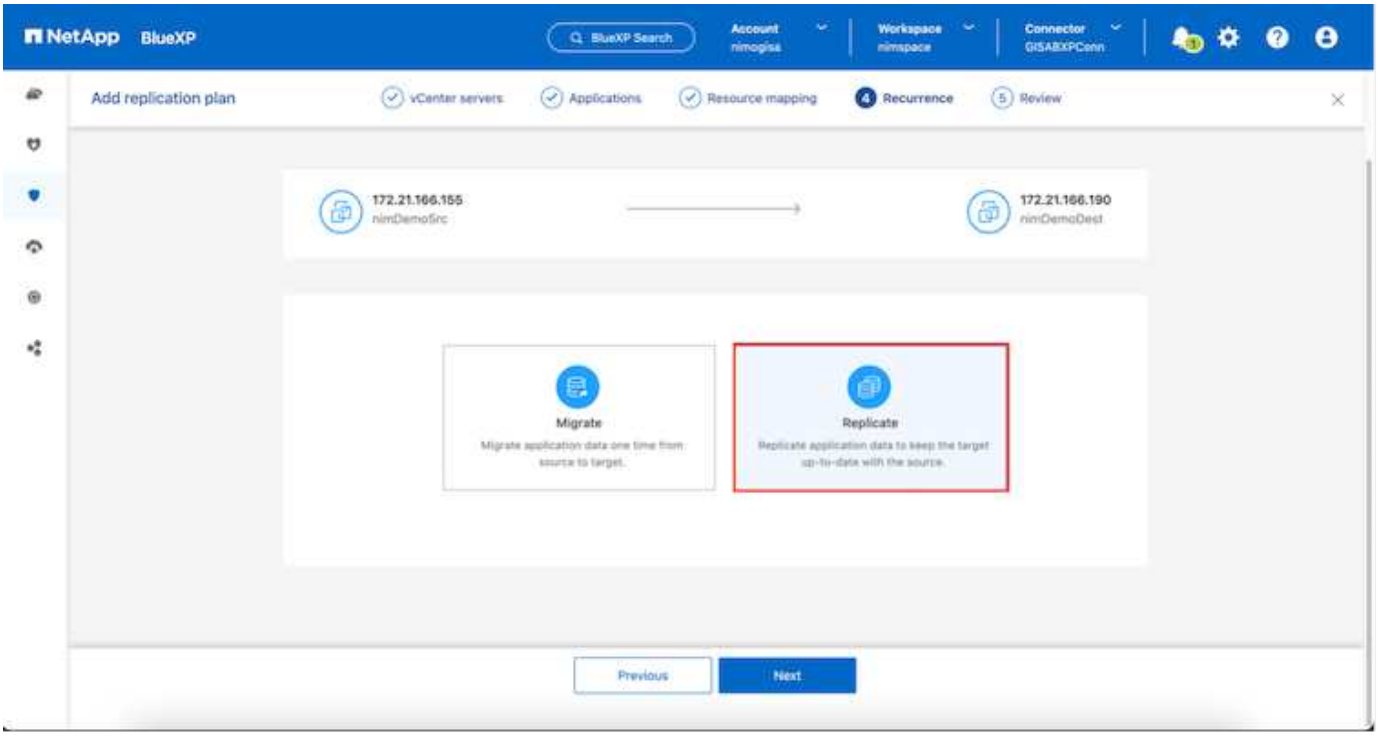
기본적으로 테스트 작업과 장애 조치 작업 모두에 동일한 매핑 매개변수가 사용됩니다. 테스트 환경에 대해 다른 매핑을 설정하려면 아래와 같이 체크박스 선택을 해제한 후 테스트 매핑 옵션을 선택하세요.



리소스 매핑이 완료되면 다음을 클릭합니다.

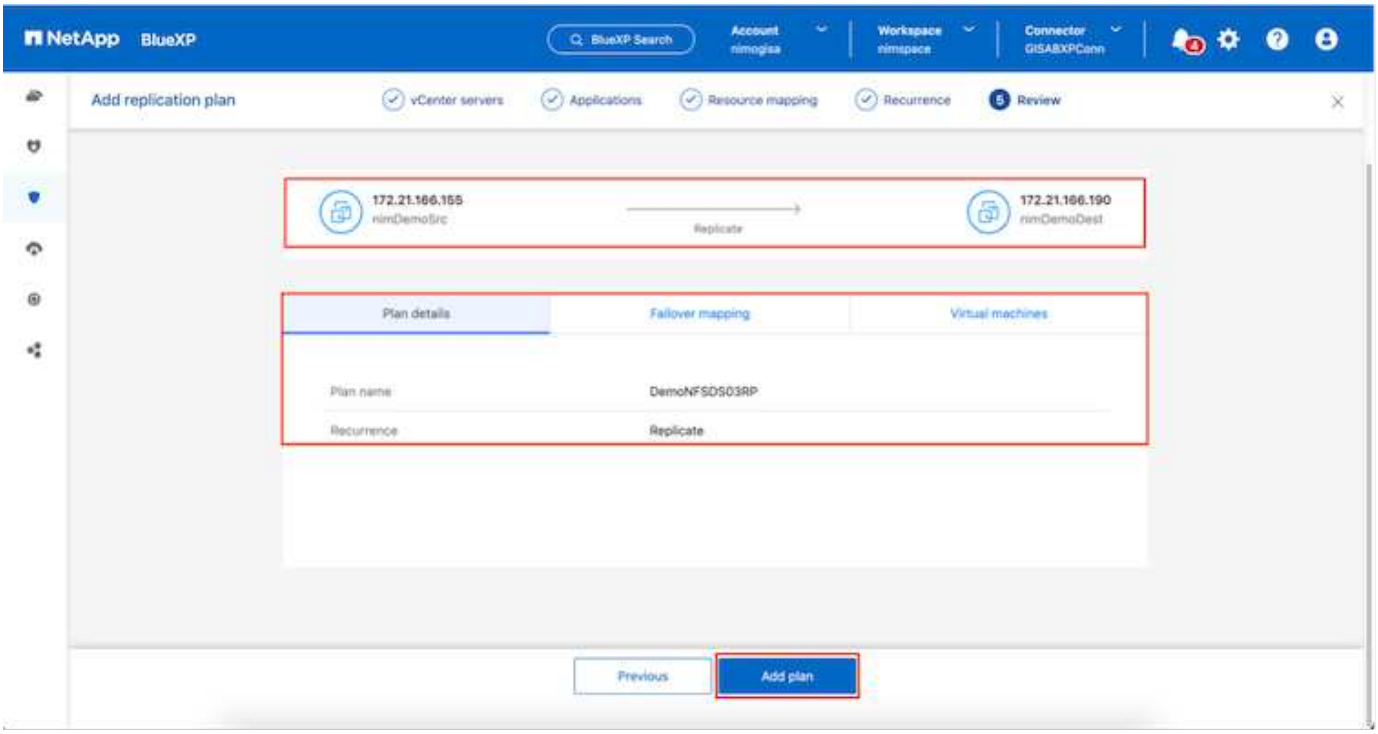


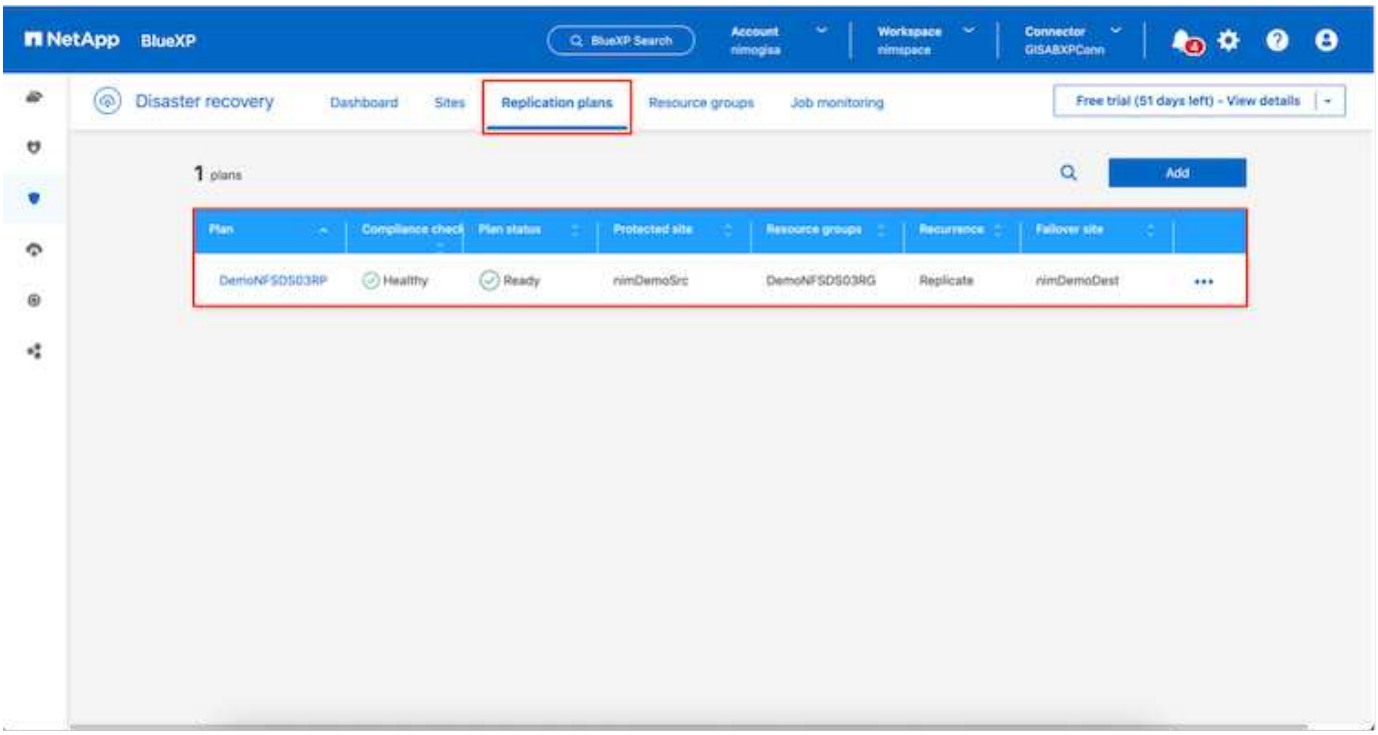
반복 유형을 선택하세요. 간단히 말해서, 마이그레이션(장애 조치를 사용한 일회성 마이그레이션) 또는 반복적 지속적 복제 옵션을 선택합니다. 이 연습에서는 복제 옵션이 선택되었습니다.



완료되면 생성된 매핑을 검토한 후 *계획 추가*를 클릭합니다.

서로 다른 볼륨 및 SVM에 있는 VM도 복제 계획에 포함될 수 있습니다. VM 배치 위치(동일한 볼륨 또는 동일한 SVM 내의 별도 볼륨, 서로 다른 SVM의 별도 볼륨)에 따라 재해 복구는 일관성 그룹 스냅샷을 생성합니다.



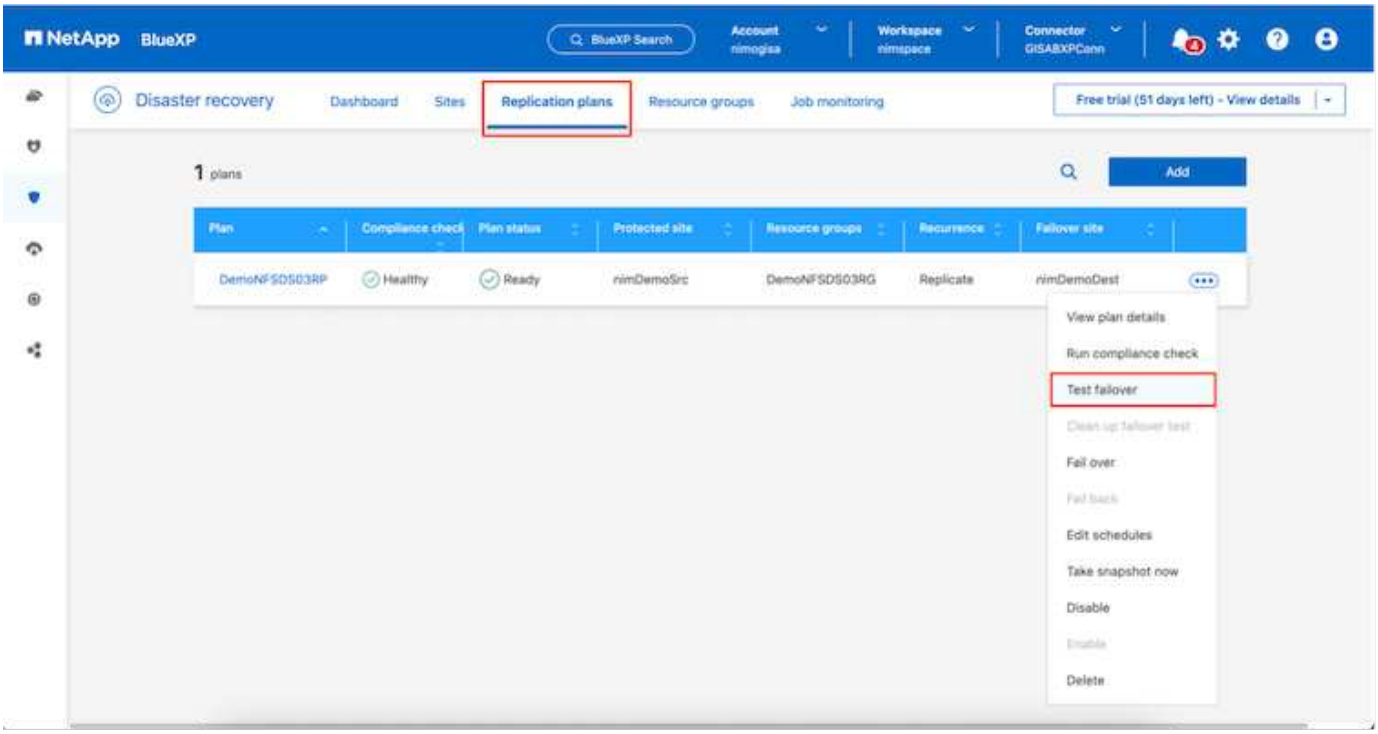


재해 복구는 다음과 같은 워크플로로 구성됩니다.

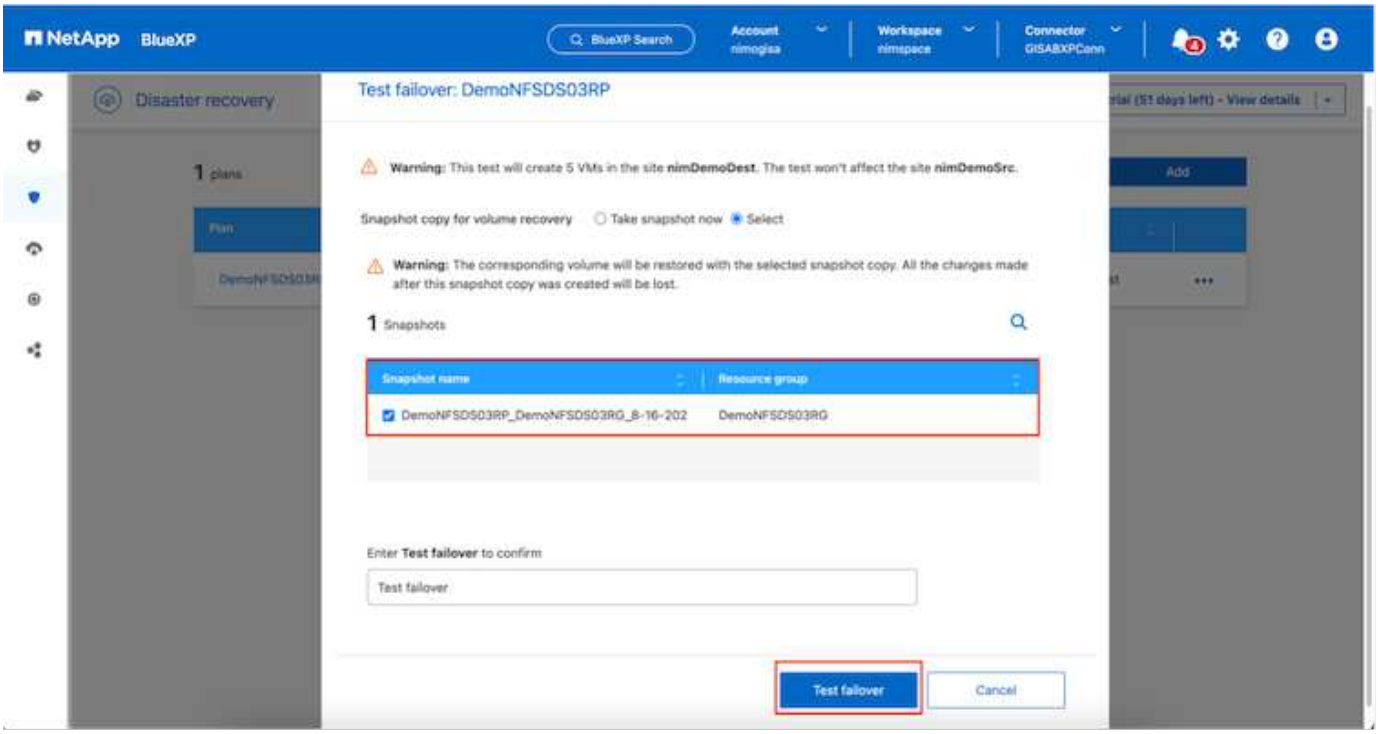
- 테스트 장애 조치(주기적 자동 시뮬레이션 포함)
- 클린업 페일오버 테스트
- 장애 조치
- 장애 복구

테스트 장애 조치

Disaster Recovery의 테스트 페일오버는 VMware 관리자가 프로덕션 환경에 영향을 주지 않고 복구 계획을 완벽하게 검증할 수 있도록 하는 운영 절차입니다. 테스트 페일오버 동안 Disaster Recovery는 DR 스토리지 시스템에 복제된 NFS 데이터스토어 볼륨의 공간 효율적인 NetApp FlexClone 복사본을 생성합니다. 그런 다음 이러한 FlexClone 볼륨을 DR 사이트의 ESXi 호스트에 마운트하고 격리된 테스트 네트워크에서 VM의 전원을 켭니다. 이 프로세스를 통해 관리자는 실제 재해 발생 시 재해 복구 계획이 의도한 대로 작동하는지 확인할 수 있습니다.

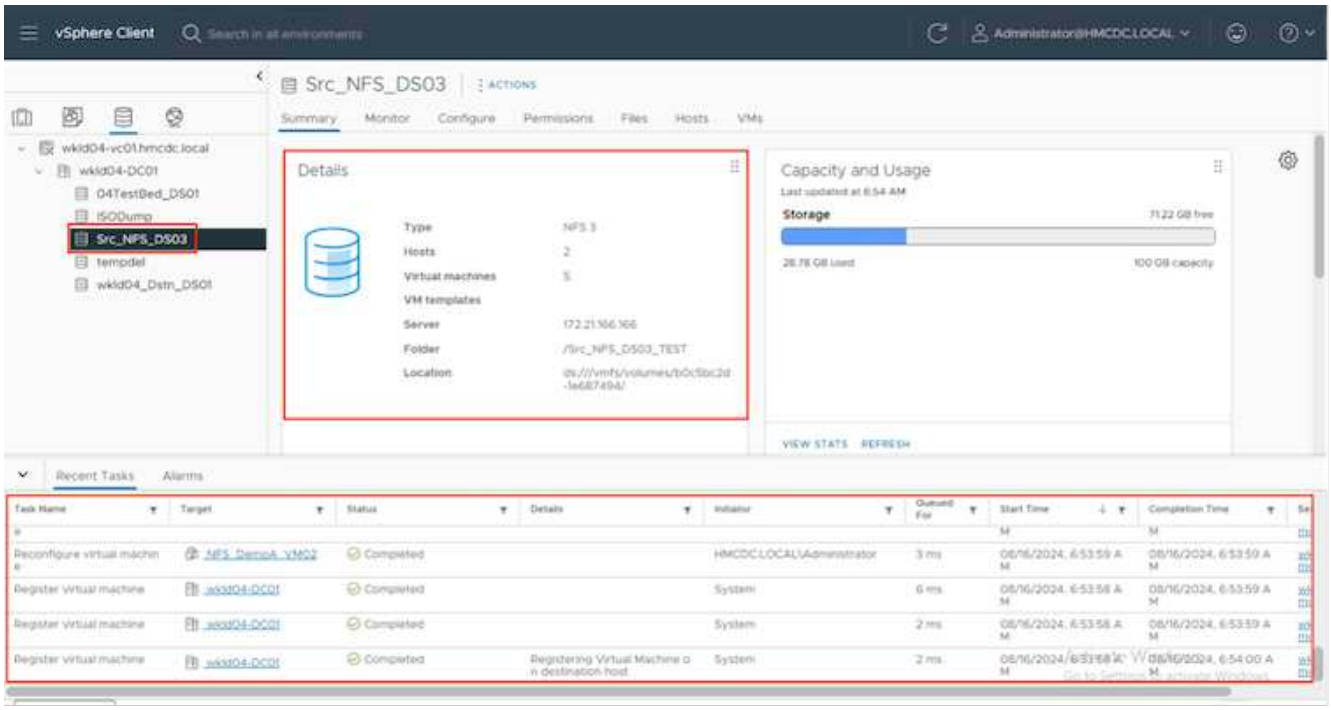


재해 복구는 테스트 페일오버 작업에서 스냅샷을 선택적 기능으로 선택할 수 있는 기능을 포함합니다. 이 기능을 통해 VMware 관리자는 환경에 최근 적용된 변경 사항이 대상 사이트에 복제되어 테스트 중에 존재하는지 확인할 수 있습니다. 이러한 변경 사항에는 VM 게스트 운영 체제에 대한 패치가 포함됩니다



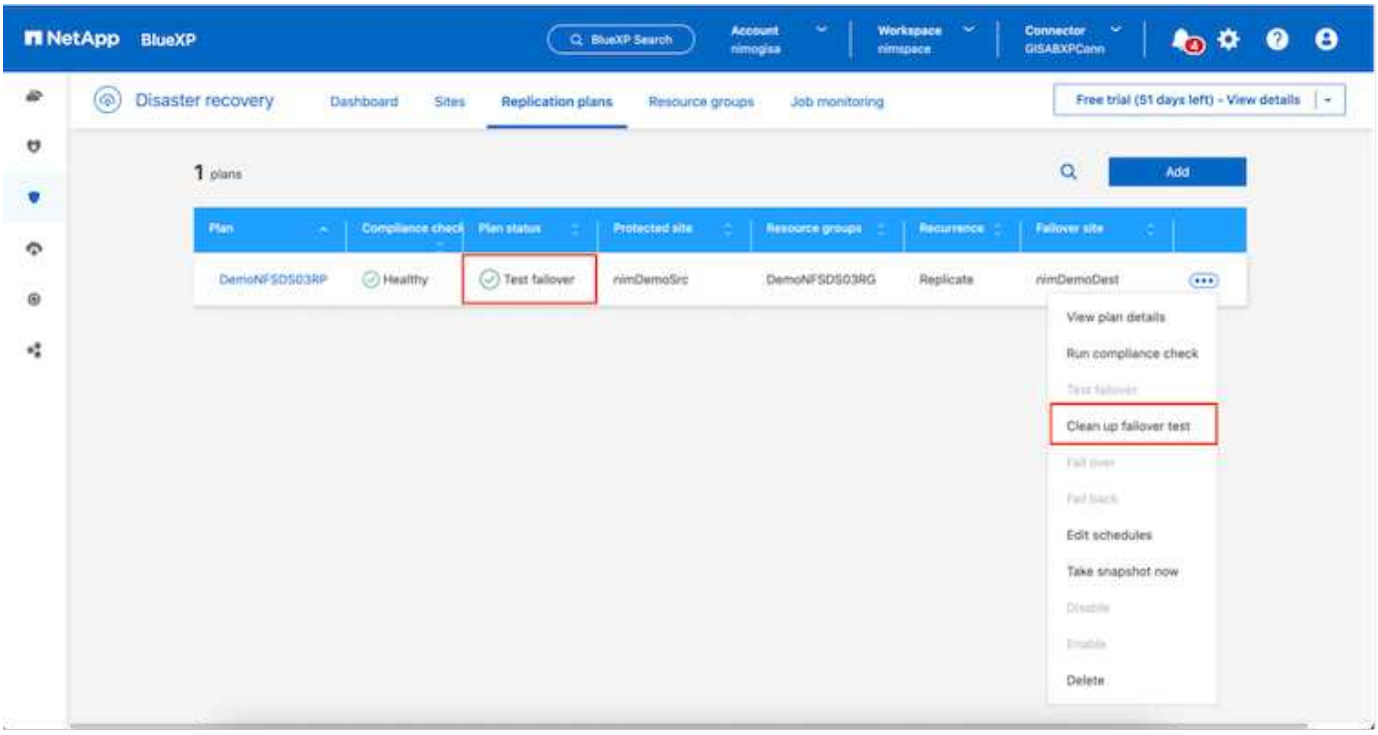
VMware 관리자가 테스트 페일오버 작업을 실행하면 Disaster Recovery가 다음 작업을 자동화합니다:

- 최근 프로덕션 사이트에서 변경된 내용을 대상 사이트의 스토리지에 업데이트하기 위해 SnapMirror 관계를 트리거합니다.
- DR 스토리지 어레이에서 FlexVol 볼륨의 NetApp FlexClone 볼륨을 생성합니다.
- FlexClone 볼륨의 NFS 데이터 저장소를 DR 사이트의 ESXi 호스트에 연결합니다.
- 매핑 중에 지정된 테스트 네트워크에 VM 네트워크 어댑터를 연결합니다.
- DR 사이트의 네트워크에 대해 정의된 대로 VM 게스트 운영 체제 네트워크 설정을 재구성합니다.
- 복제 계획에 저장된 사용자 정의 명령을 실행합니다.
- 복제 계획에 정의된 순서대로 VM의 전원을 켭니다.



클린업 페일오버 테스트 작업

정리 장애 조치 테스트 작업은 복제 계획 테스트가 완료되고 VMware 관리자가 정리 프롬프트에 응답한 후에 발생합니다.



이 작업을 수행하면 가상 머신(VM)과 복제 계획 상태가 준비 상태로 재설정됩니다.

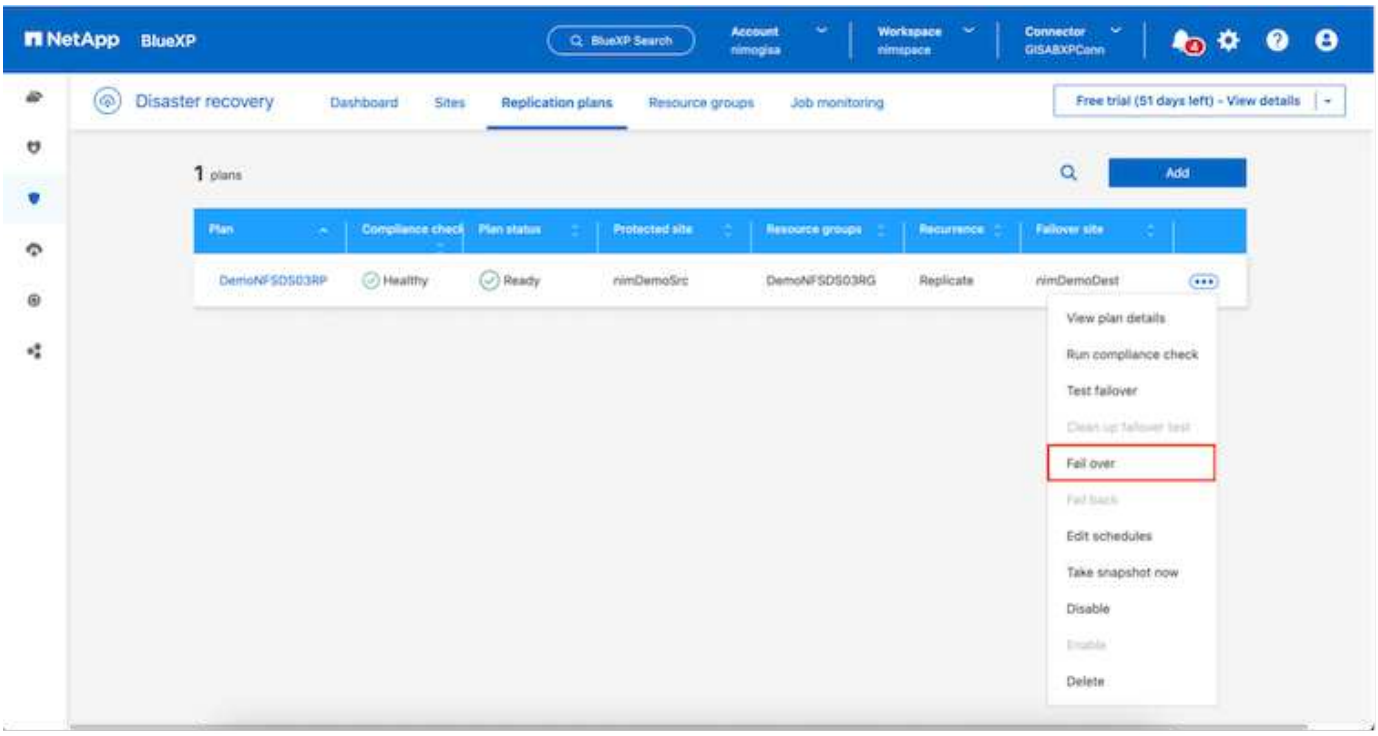
VMware 관리자가 복구 작업을 수행하면 재해 복구는 다음 프로세스를 완료합니다.

1. 테스트에 사용된 FlexClone 복사본에서 복구된 각 VM의 전원을 끕니다.

2. 테스트 중 복구된 VM을 표시하는 데 사용된 FlexClone 볼륨을 삭제합니다.

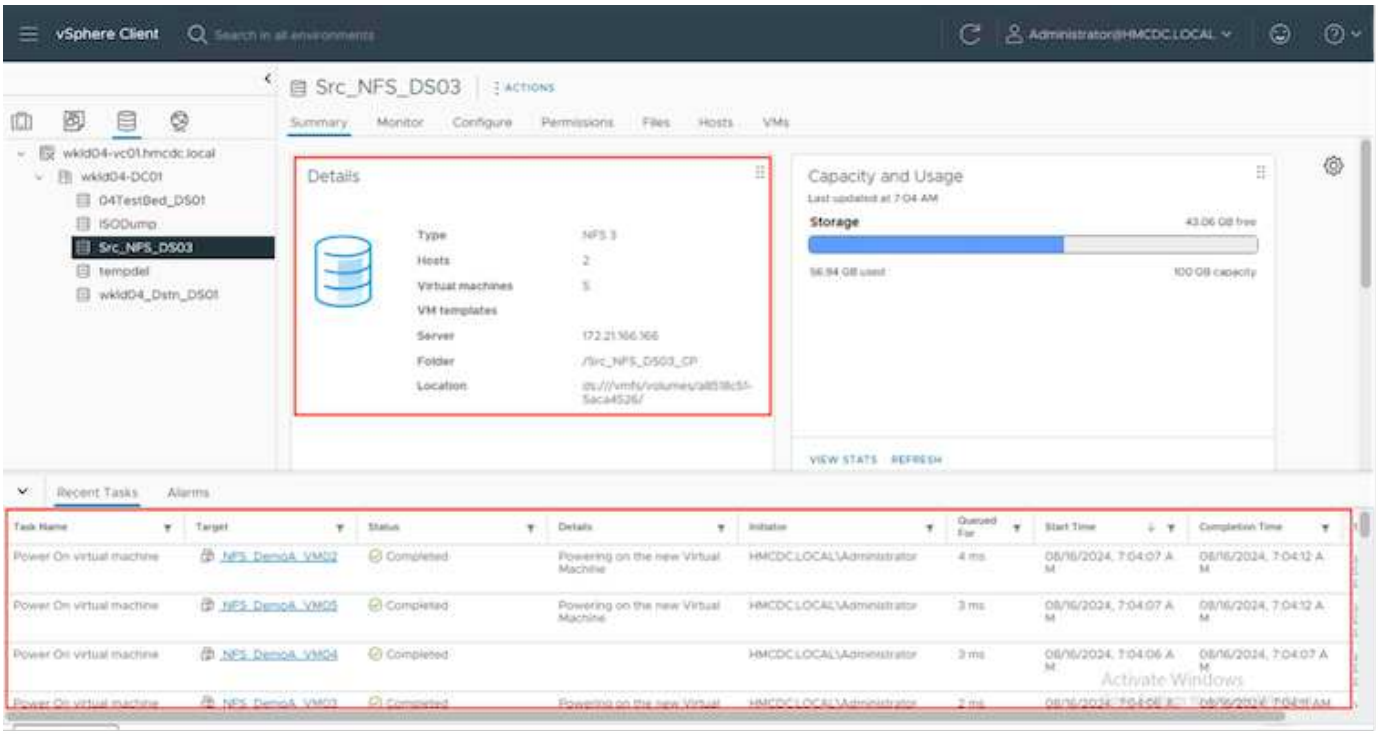
계획된 마이그레이션 및 장애 조치

재해 복구에는 실제 페일오버를 수행하는 두 가지 방법이 있습니다. 바로 계획된 마이그레이션과 페일오버입니다. 첫 번째 방법인 계획된 마이그레이션은 VM 종료 및 스토리지 복제 동기화를 프로세스에 포함하여 VM을 복구하거나 대상 사이트로 효과적으로 이동하는 방식입니다. 계획된 마이그레이션을 위해서는 소스 사이트에 대한 액세스가 필요합니다. 두 번째 방법인 페일오버는 계획되거나 계획되지 않은 페일오버로, 완료할 수 있었던 마지막 스토리지 복제 간격으로부터 대상 사이트에서 VM을 복구하는 방식입니다. 솔루션에 설계된 RPO에 따라 DR 시나리오에서는 일정량의 데이터 손실이 예상될 수 있습니다.



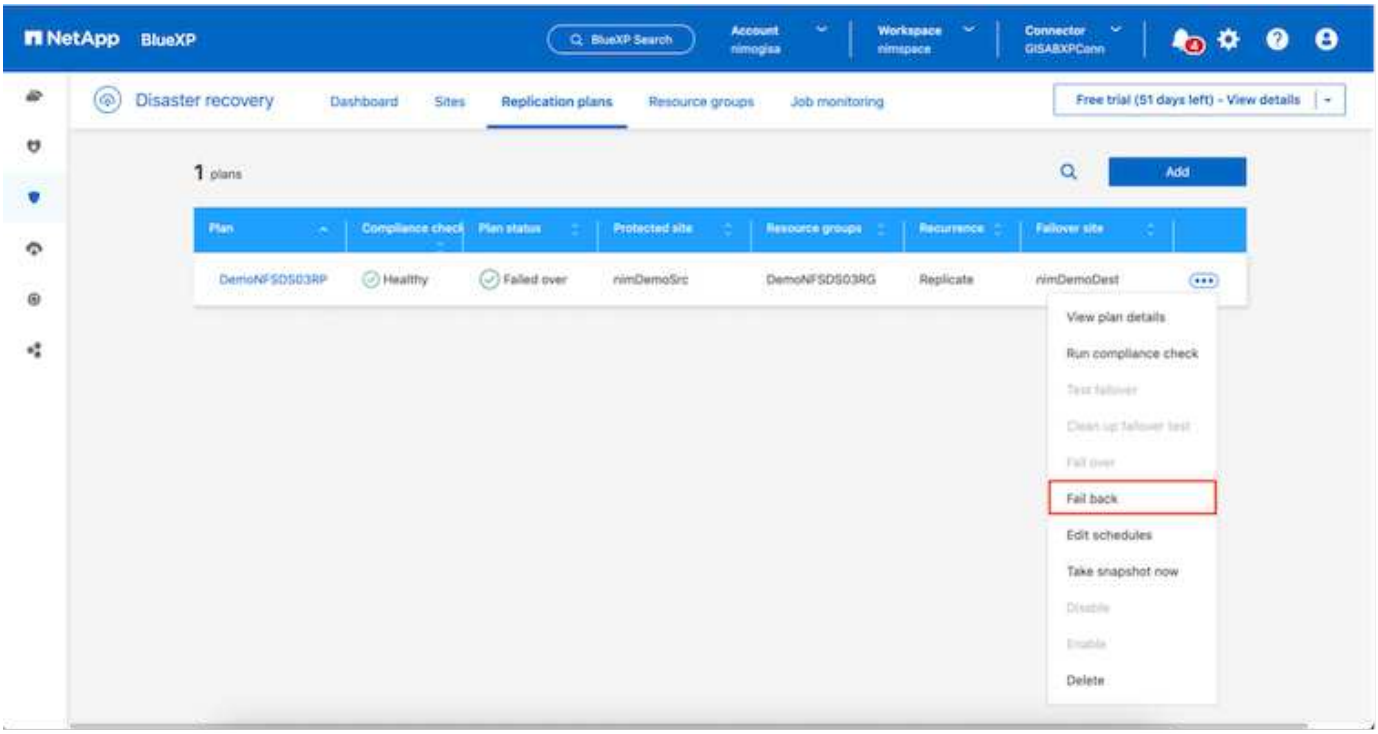
VMware 관리자가 장애 조치 작업을 수행하면 Disaster Recovery가 다음 작업을 자동화합니다.

- NetApp SnapMirror 관계를 끊고 장애 조치합니다.
- 복제된 NFS 데이터 저장소를 DR 사이트의 ESXi 호스트에 연결합니다.
- VM 네트워크 어댑터를 적절한 대상 사이트 네트워크에 연결합니다.
- 대상 사이트의 네트워크에 대해 정의된 대로 VM 게스트 운영 체제 네트워크 설정을 재구성합니다.
- 복제 계획에 저장된 사용자 정의 명령(있는 경우)을 실행합니다.
- 복제 계획에 정의된 순서대로 VM의 전원을 켭니다.



장애 복구

장애 복구는 복구 후 소스 및 대상 사이트의 원래 구성을 복원하는 선택적 절차입니다.



VMware 관리자는 서비스를 원래 소스 사이트로 복원할 준비가 되면 장애 복구 절차를 구성하고 실행할 수 있습니다.

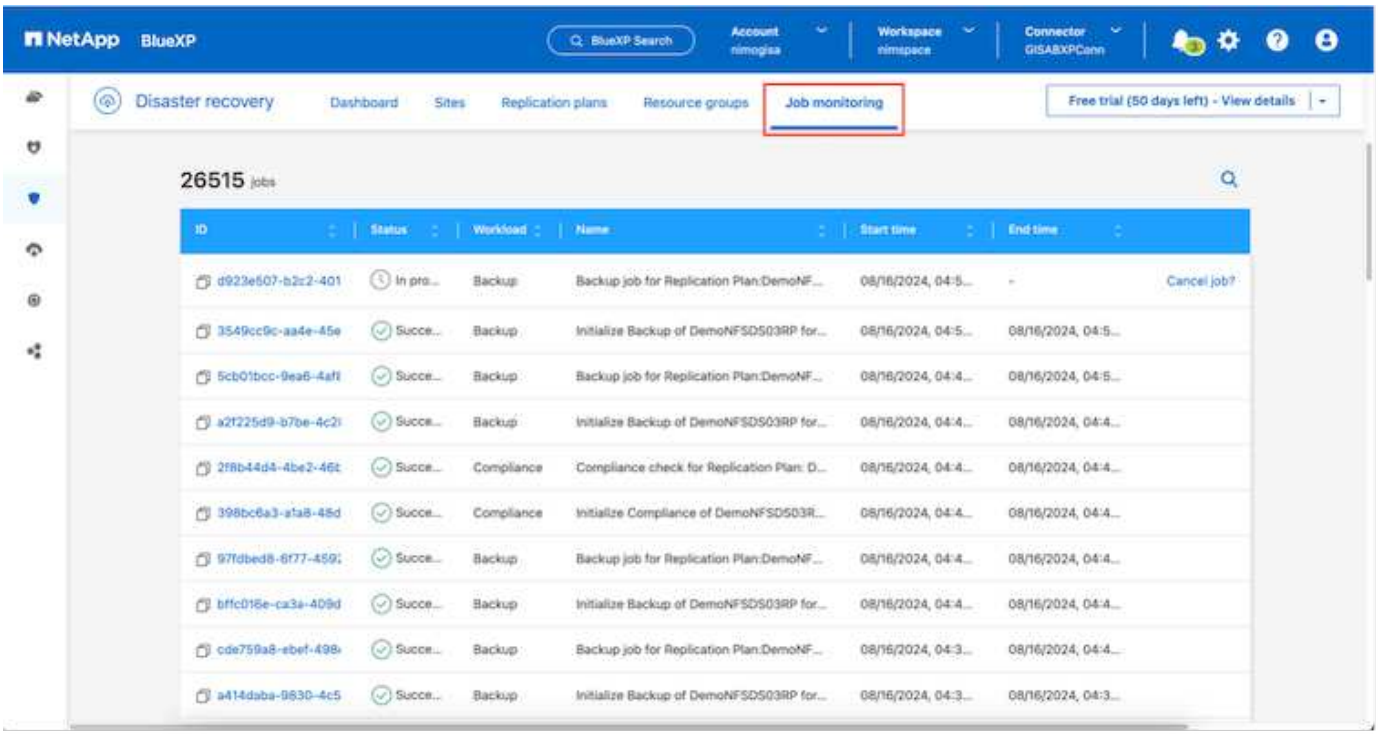
참고: 재해 복구는 복제 방향을 바꾸기 전에 모든 변경 사항을 원래 소스 가상 머신으로 복제(재동기화)합니다. 이 프로세스는 타겟으로 장애 조치가 완료된 관계에서 시작되며 다음 단계를 포함합니다.

- 대상 사이트의 가상 머신과 볼륨의 전원을 끄고 등록을 취소합니다.
- 원본 소스의 SnapMirror 관계를 끊어서 읽기/쓰기가 가능하도록 합니다.
- 복제를 되돌리려면 SnapMirror 관계를 다시 동기화합니다.
- 소스에 볼륨을 마운트하고, 소스 가상 머신의 전원을 켜서 등록합니다.

재해 복구 액세스 및 구성에 대한 자세한 내용은 "VMware용 NetApp Disaster Recovery에 대해 알아보십시오."을(를) 참조하십시오.

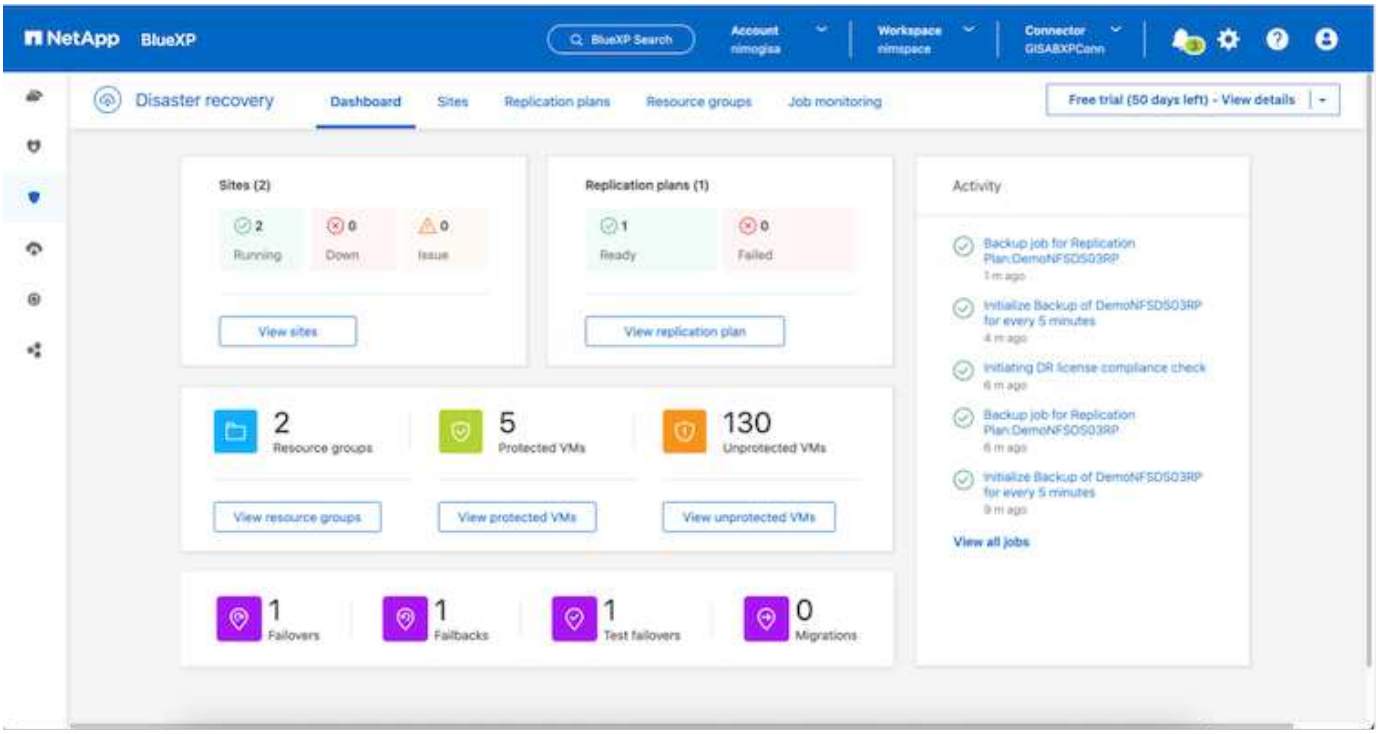
모니터링 및 대시보드

콘솔 또는 ONTAP CLI에서 해당 데이터스토어 볼륨의 복제 상태를 모니터링할 수 있으며, 작업 모니터링을 통해 장애 조치 또는 테스트 장애 조치의 상태를 추적할 수 있습니다.



작업이 현재 진행 중이거나 대기 중이고 이를 중지하고 싶은 경우, 취소 옵션이 있습니다.

재해 복구 대시보드를 통해 재해 복구 사이트 및 복제 계획의 상태를 확실하게 평가할 수 있습니다. 이를 통해 관리자는 정상, 연결 끊김 또는 성능 저하 상태의 사이트 및 계획을 신속하게 파악할 수 있습니다.



이는 맞춤형 재해 복구 계획을 처리하는 강력한 솔루션을 제공합니다. 장애 조치는 계획된 장애 조치로 수행할 수도 있고, 재해가 발생하고 DR 사이트를 활성화하기로 결정한 경우 버튼을 클릭하여 장애 조치를 수행할 수도 있습니다.

이 프로세스에 대해 자세히 알아보려면 자세한 연습 비디오를 따르거나 다음을 사용하십시오."솔루션 시뮬레이터" .

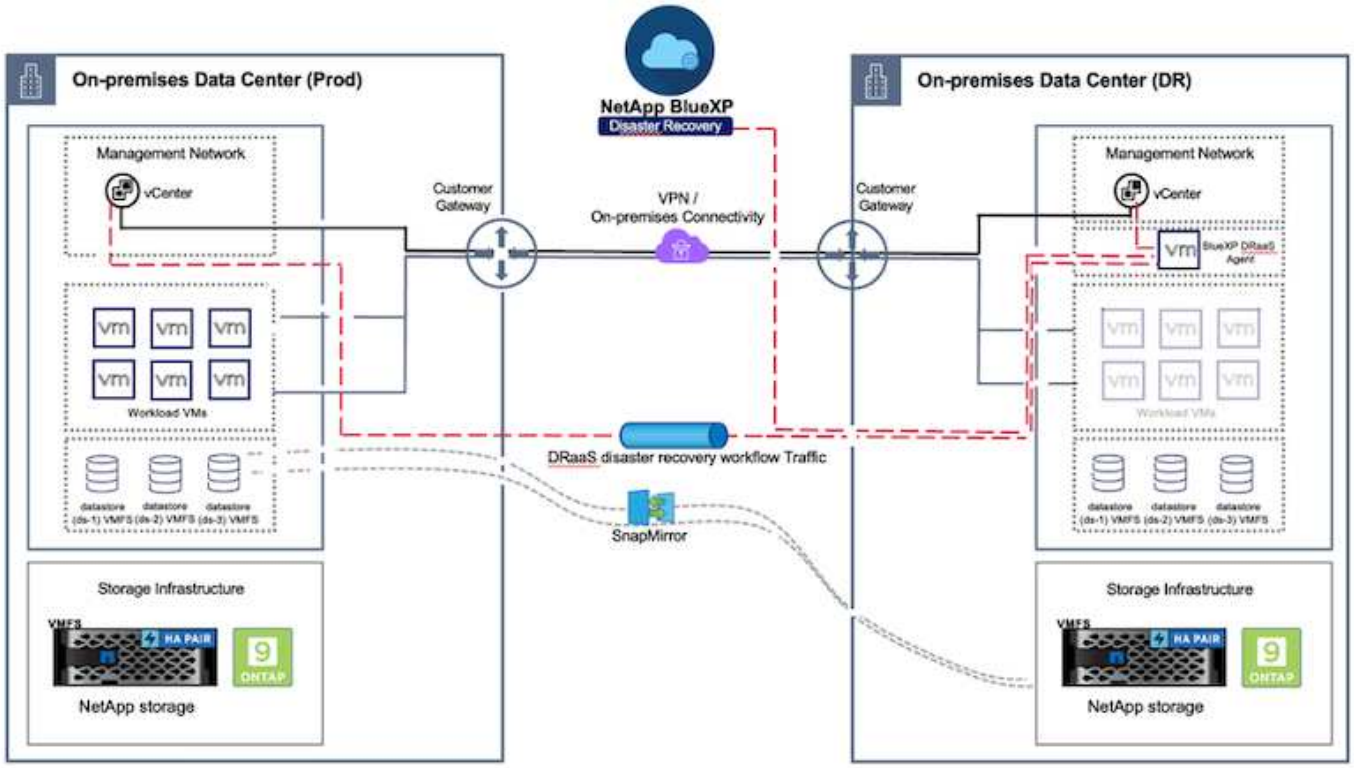
VMFS 데이터스토어용 NetApp Disaster Recovery

운영 사이트에서 재해 복구 사이트로 블록 수준 복제를 사용하는 재해 복구는 랜섬웨어 공격과 같은 사이트 중단 및 데이터 손상 이벤트로부터 작업 부하를 보호하는 탄력적이고 비용 효율적인 방법입니다. NetApp SnapMirror 복제를 사용하면 VMFS 데이터 저장소를 사용하는 온프레미스 ONTAP 시스템을 실행하는 VMware 워크로드를 VMware가 상주하는 지정된 복구 데이터 센터의 다른 ONTAP 스토리지 시스템으로 복제할 수 있습니다.

이 문서의 이 섹션에서는 온프레미스 VMware VM을 지정된 다른 사이트로 재해 복구하도록 설정하기 위한 NetApp Disaster Recovery 구성에 대해 설명합니다. 이 설정의 일부로 Console 에이전트, ONTAP 어레이 온보딩, 사이트 정의 및 VMware vCenter 연결이 포함됩니다. 또한 이 문서에서는 사이트 간 복제를 구성하는 방법과 복구 계획을 설정하고 테스트하는 방법에 대해 자세히 설명합니다. 마지막 섹션에서는 전체 사이트 페일오버를 수행하는 방법과 기본 사이트가 복구되어 온라인 상태가 되었을 때 페일백하는 방법에 대한 지침을 제공합니다.

NetApp Data Services의 일부인 Disaster Recovery를 사용하면 고객이 온프레미스 VMware vCenters와 ONTAP 스토리지를 탐색하고, 리소스 그룹을 생성하고, 재해 복구 계획을 생성하고, 이를 리소스 그룹과 연결하고, 페일오버 및 페일백을 테스트하거나 실행할 수 있습니다. SnapMirror는 스토리지 수준의 블록 복제를 제공하여 두 사이트가 증분 변경 사항으로 최신 상태를 유지하도록 하며, 최대 5분의 RPO를 달성합니다. 프로덕션 및 복제된 데이터스토어에 영향을 주거나 추가 스토리지 비용을 발생시키지 않고 정기적인 훈련으로 DR 절차를 시뮬레이션하는 것도 가능합니다. NetApp Data Services는 ONTAP의 FlexClone 기술을 활용하여 DR 사이트의 마지막 복제된 스니샷에서 VMFS 데이터스토어의 공간 효율적인 복사본을 생성합니다. DR 테스트가 완료되면 고객은 테스트 환경을 간단히 삭제할 수 있으며, 이 경우에도 실제 복제된 프로덕션 리소스에는 아무런 영향이 없습니다. 실제 페일오버가 필요한 경우(계획된 경우든 계획되지 않은 경우든) 몇 번의 클릭만으로 Disaster Recovery가 지정된 재해 복구 사이트에서 보호된 가상 머신을 자동으로 가동하는 데 필요한 모든 단계를 오케스트레이션합니다. 서비스는 필요할 때 페일백 작업을 위해 기본 사이트에 대한 SnapMirror 관계를 역방향으로 전환하고 보조에서 기본으로 변경 사항을 복제합니다. 이 모든 것은 잘

알려진 다른 대안에 비해 훨씬 낮은 비용으로 달성할 수 있습니다.

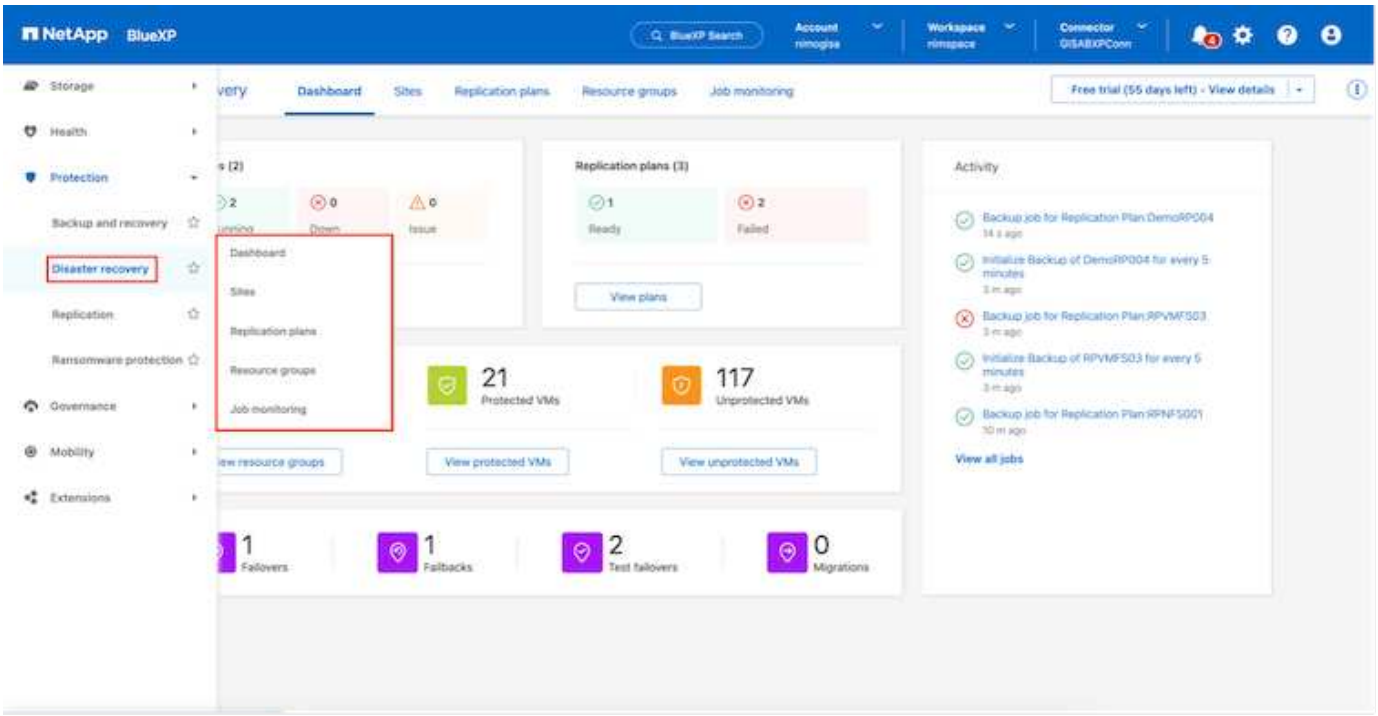


재해 복구용 vCenter Server, ESXi 및 ONTAP의 최신 정보 및 지원되는 버전에 대해서는 "재해 복구 지원 구성"을(를) 참조하십시오.

시작하기

재해 복구를 시작하려면 NetApp Console을 사용한 다음 서비스에 액세스하십시오.

1. 콘솔에 로그인하십시오.
2. 콘솔 왼쪽 탐색 메뉴에서 보호 > 재해 복구를 선택합니다.
3. 재해 복구 대시보드가 나타납니다.

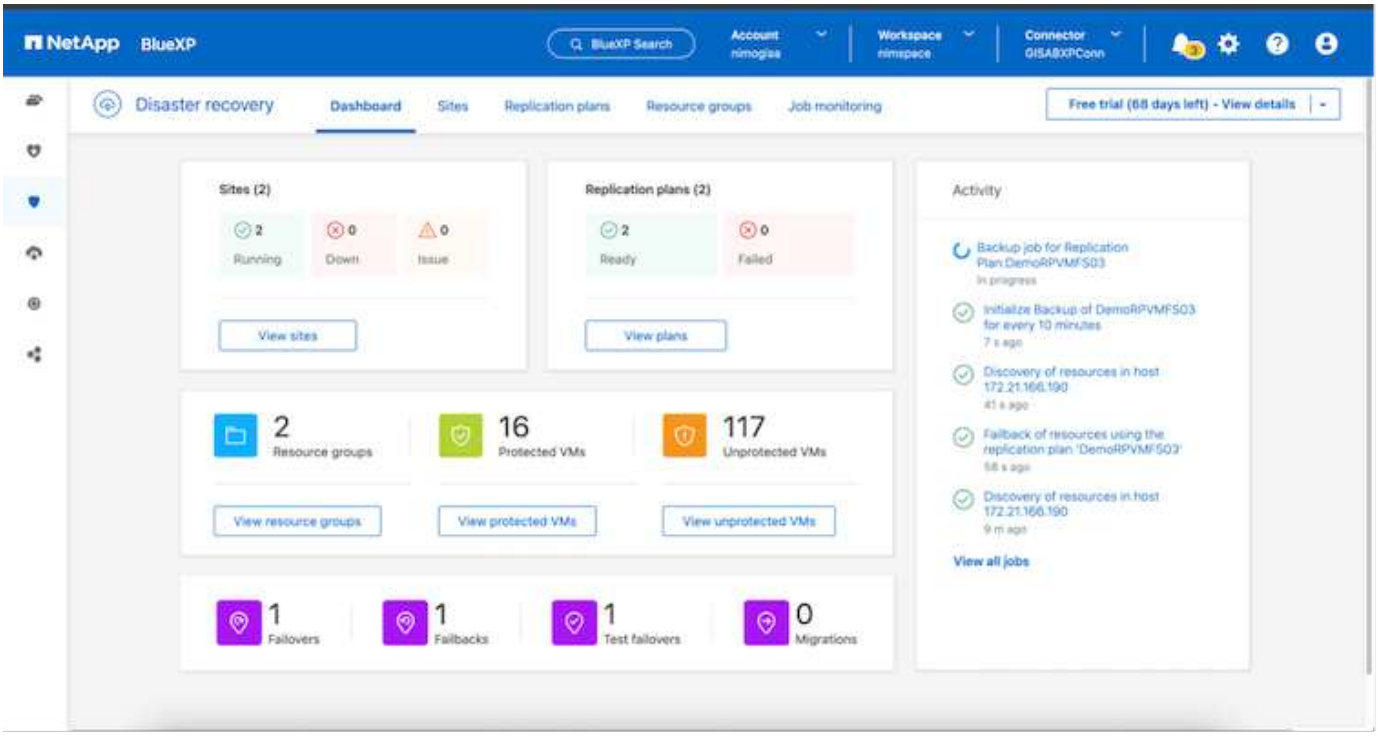


재해 복구 계획을 구성하기 전에 다음 전제 조건이 충족되었는지 확인하세요.

- 콘솔 에이전트는 AWS VPC에 배포됩니다.
- 콘솔 에이전트 인스턴스는 소스 및 대상 vCenter 및 스토리지 시스템에 연결됩니다.
- VMware용 VMFS 데이터스토어를 호스팅하는 온프레미스 NetApp 스토리지 시스템이 콘솔에 추가됩니다.
- DNS 이름을 사용하는 경우 DNS 확인이 이루어져야 합니다. 그렇지 않은 경우 vCenter에 IP 주소를 사용하세요.
- SnapMirror 복제는 지정된 VMFS 기반 데이터 저장소 볼륨에 대해 구성됩니다.

소스 사이트와 대상 사이트 간의 연결이 설정되면 구성 단계를 진행하세요. 이 작업에는 약 3~5분 정도 소요됩니다.

NetApp은 콘솔 에이전트를 재해 복구 사이트 또는 제3의 사이트에 배포하여 실제 장애 또는 자연재해 발생 시 콘솔 에이전트가 네트워크를 통해 소스 및 대상 리소스와 통신할 수 있도록 하는 것을 권장합니다.

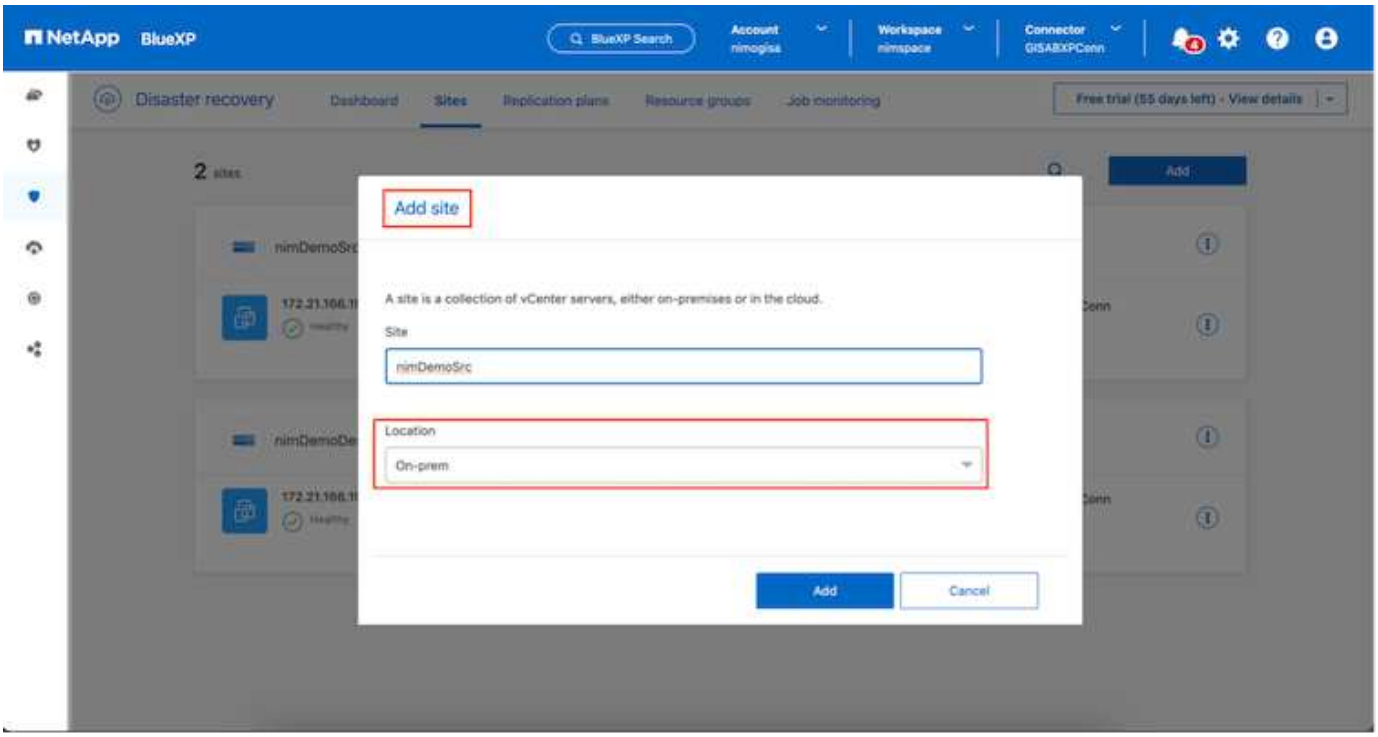


이 문서를 작성하는 시점에는 온프레미스 간 VMFS 데이터 저장소에 대한 지원이 기술 미리보기 단계에 있습니다. 이 기능은 FC 및 ISCSI 프로토콜 기반 VMFS 데이터 저장소에서 모두 지원됩니다.

재해 복구 구성

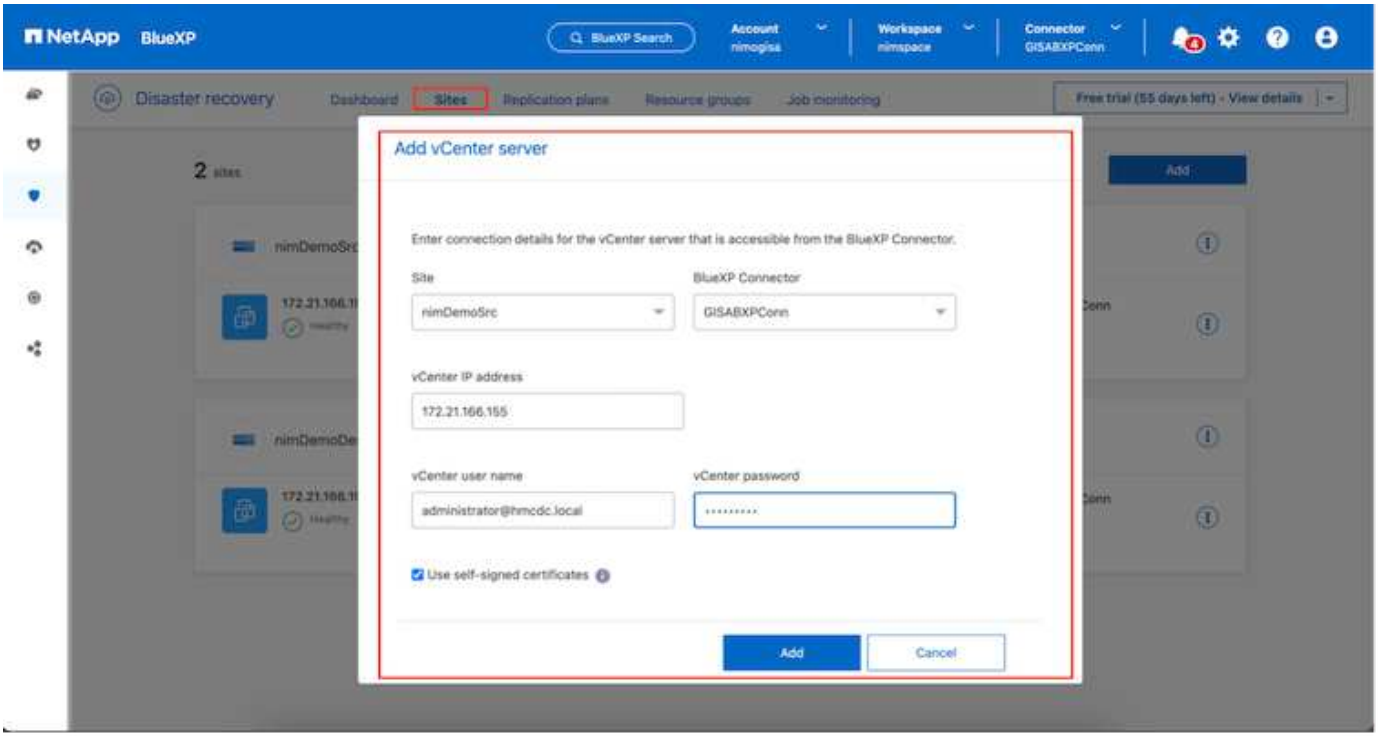
재해 복구를 준비하는 첫 번째 단계는 온프레미스 vCenter 및 스토리지 리소스를 탐색하고 재해 복구에 추가하는 것입니다.

캔버스 내 작업 환경에 ONTAP 스토리지 시스템이 추가되었는지 확인하십시오. 콘솔을 열고 왼쪽 탐색 메뉴에서 *보호 > 재해 복구*를 선택합니다. *vCenter 서버 탐색*을 선택하거나 상단 메뉴를 사용하여 *사이트 > 추가 > vCenter 추가*를 선택합니다.

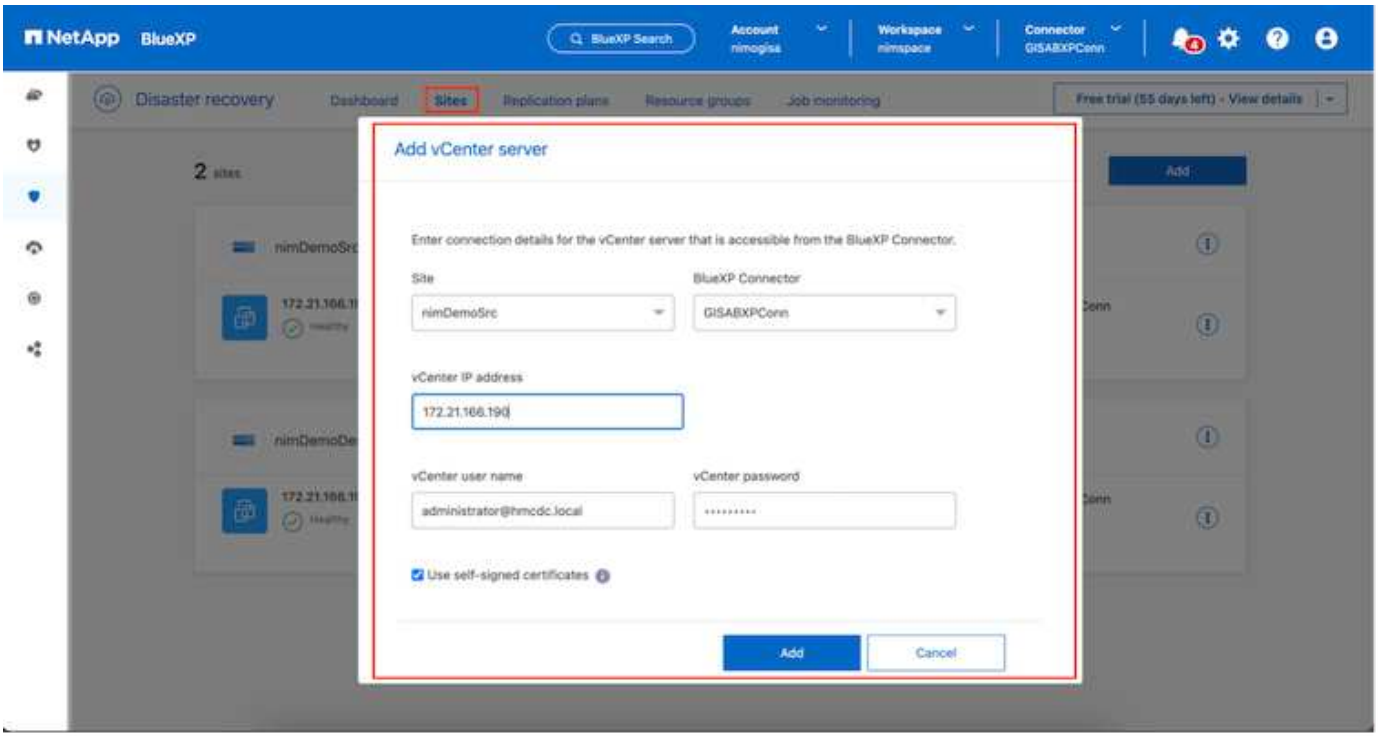


다음 플랫폼을 추가하세요:

- 원천. 온프레미스 vCenter.



- 목적지. VMC SDDC vCenter.



vCenter가 추가되면 자동 검색이 실행됩니다.

소스 사이트와 대상 사이트 간 스토리지 복제 구성

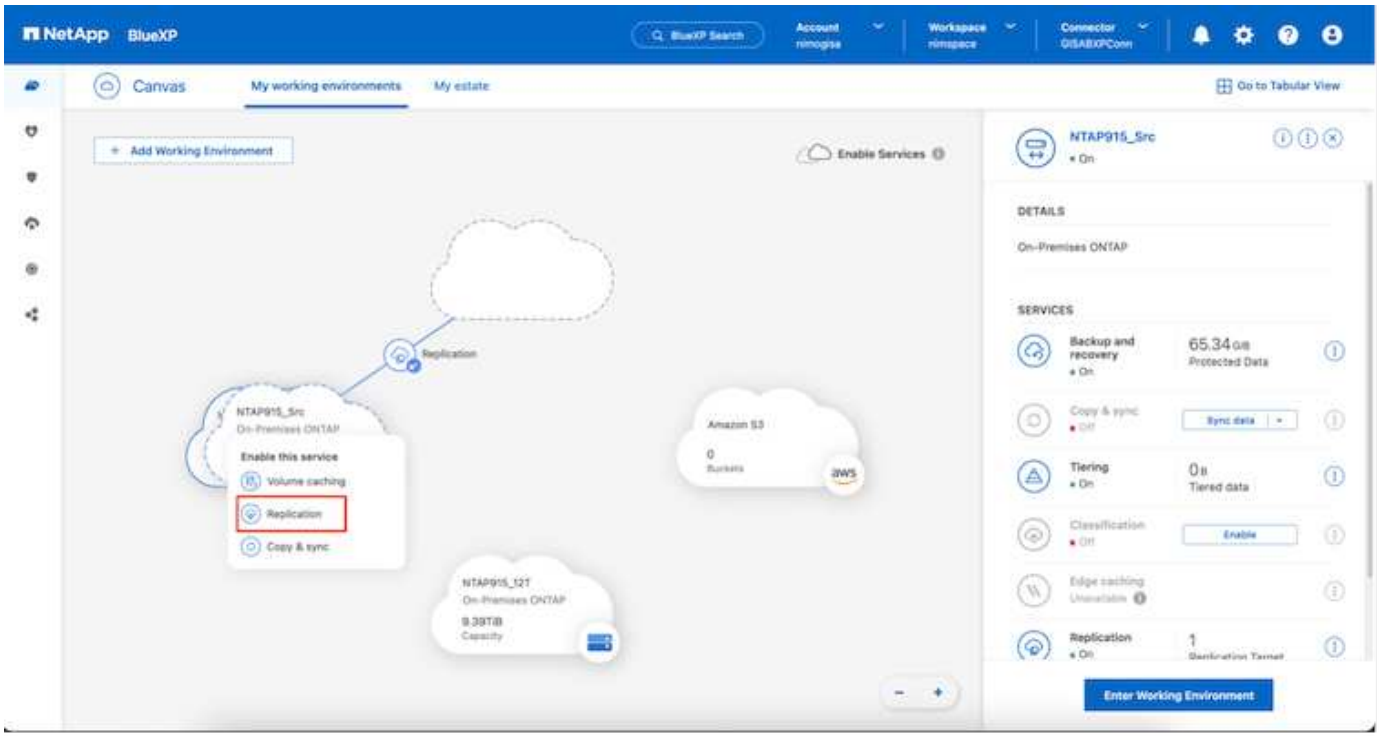
SnapMirror ONTAP 스냅샷을 활용하여 한 위치에서 다른 위치로의 데이터 전송을 관리합니다. 처음에는 소스 볼륨의 스냅샷을 기반으로 한 전체 복사본이 대상에 복사되어 기준 동기화를 수행합니다. 소스에서 데이터가 변경되면 새로운 스냅샷이 생성되어 기준 스냅샷과 비교됩니다. 변경된 것으로 확인된 블록은 대상에 복제되고, 최신 스냅샷이 현재 기준선 또는 최신 공통 스냅샷이 됩니다. 이를 통해 프로세스를 반복하고 증분 업데이트를 대상에 전송할 수 있습니다.

SnapMirror 관계가 설정되면 대상 볼륨은 온라인 읽기 전용 상태가 되므로 계속 액세스할 수 있습니다. SnapMirror 파일이나 다른 논리적 수준이 아닌 물리적 저장 블록으로 작동합니다. 즉, 대상 볼륨은 스냅샷, 볼륨 설정 등을 포함하여 소스의 동일한 복제본입니다. 데이터 압축 및 데이터 중복 제거와 같은 ONTAP 공간 효율성 기능이 소스 볼륨에서 사용되는 경우 복제된 볼륨은 이러한 최적화를 유지합니다.

SnapMirror 관계를 끊으면 대상 볼륨을 쓸 수 있게 되며 일반적으로 SnapMirror 사용하여 DR 환경에 데이터를 동기화할 때 장애 조치를 수행하는 데 사용됩니다. SnapMirror 는 장애 조치 사이트에서 변경된 데이터를 나중에 다시 온라인 상태가 되면 효율적으로 기본 시스템으로 다시 동기화하고 원래 SnapMirror 관계를 재설정할 수 있을 만큼 정교합니다.

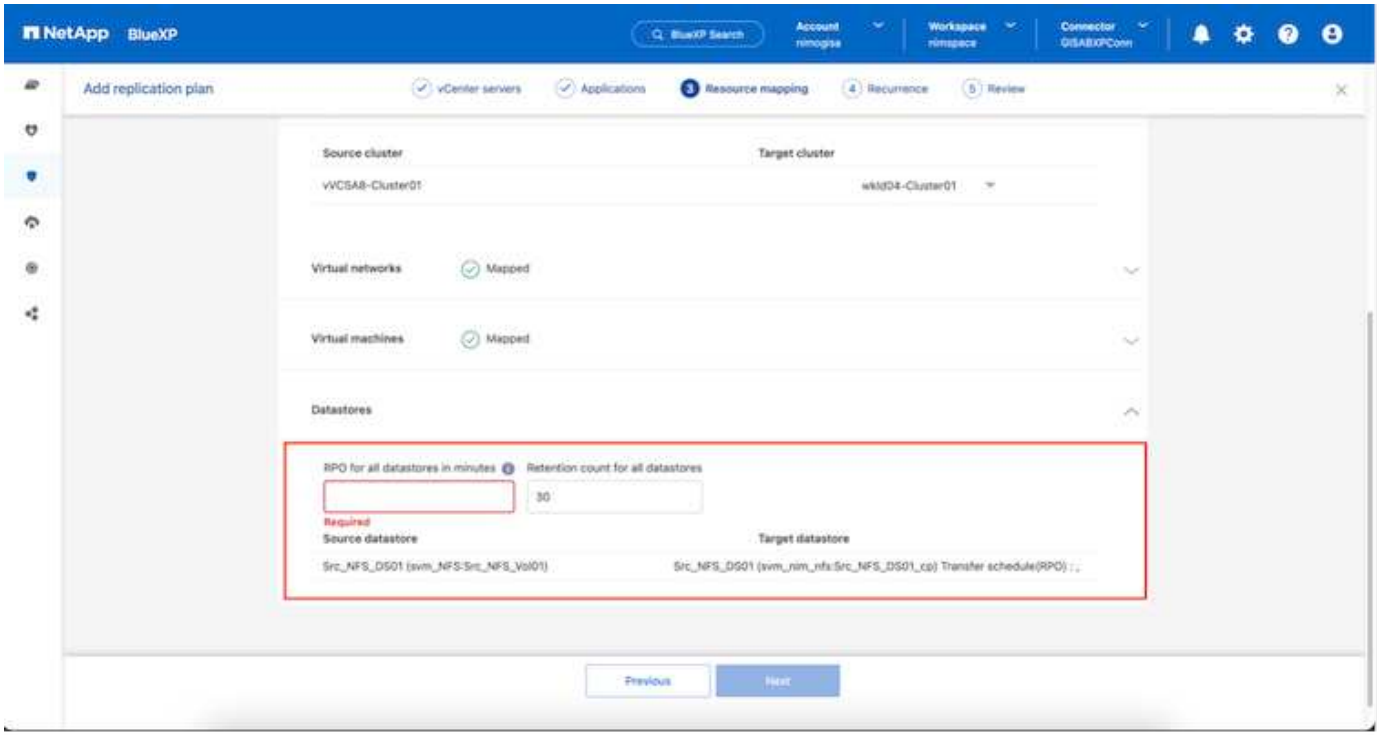
VMware 재해 복구를 설정하는 방법

어떤 애플리케이션이든 SnapMirror 복제를 생성하는 프로세스는 동일합니다. 이 프로세스는 수동 또는 자동으로 진행할 수 있습니다. 가장 쉬운 방법은 콘솔을 활용하여 환경의 소스 ONTAP 시스템을 대상으로 간단히 드래그 앤 드롭하여 SnapMirror 복제를 구성하는 것입니다. 그러면 마법사가 실행되어 나머지 프로세스를 안내합니다.



NetApp Data Services는 다음 두 가지 조건을 충족하는 경우 동일한 작업을 자동화할 수도 있습니다:

- 소스 클러스터와 대상 클러스터는 피어 관계를 갖습니다.
- 소스 SVM과 대상 SVM은 피어 관계를 갖습니다.

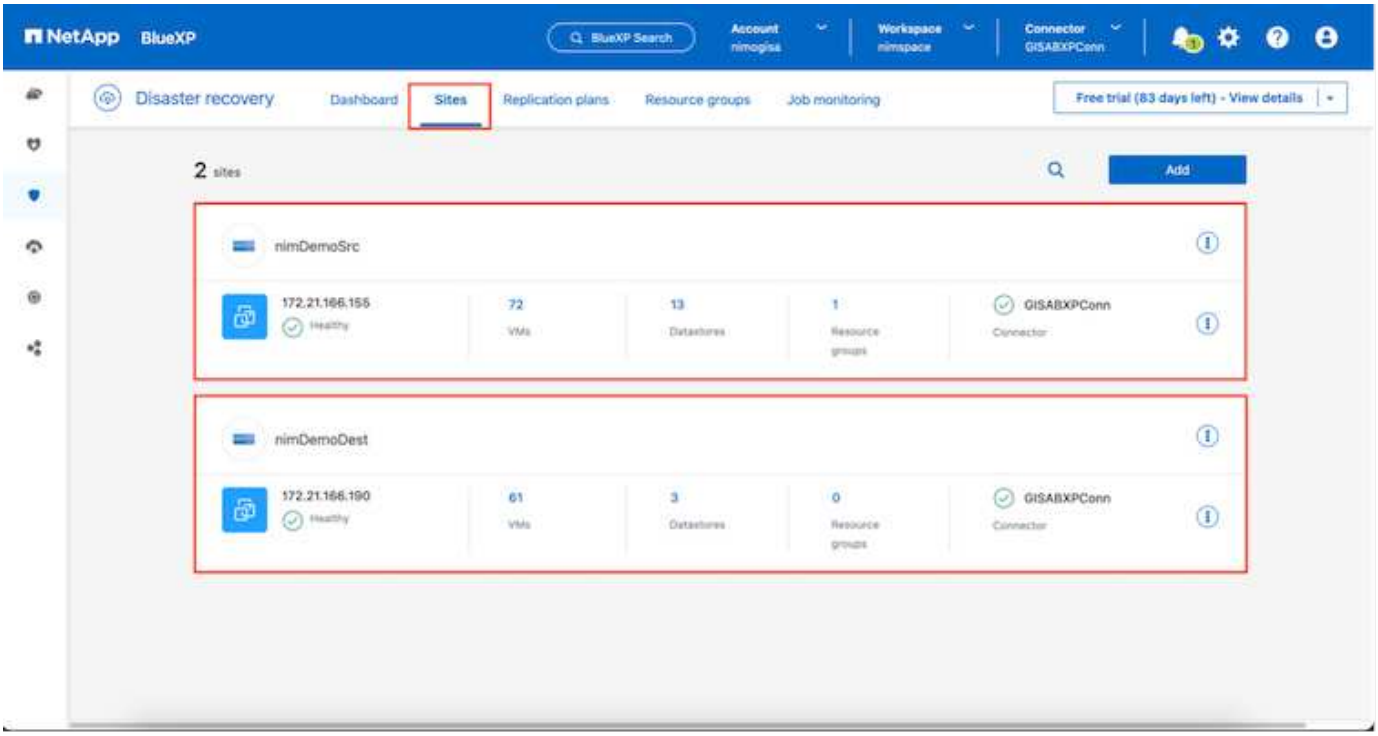


CLI를 통해 볼륨에 대해 SnapMirror 관계가 이미 구성된 경우, Console은 해당 관계를 가져와 나머지 워크플로 작업을 계속 진행합니다.

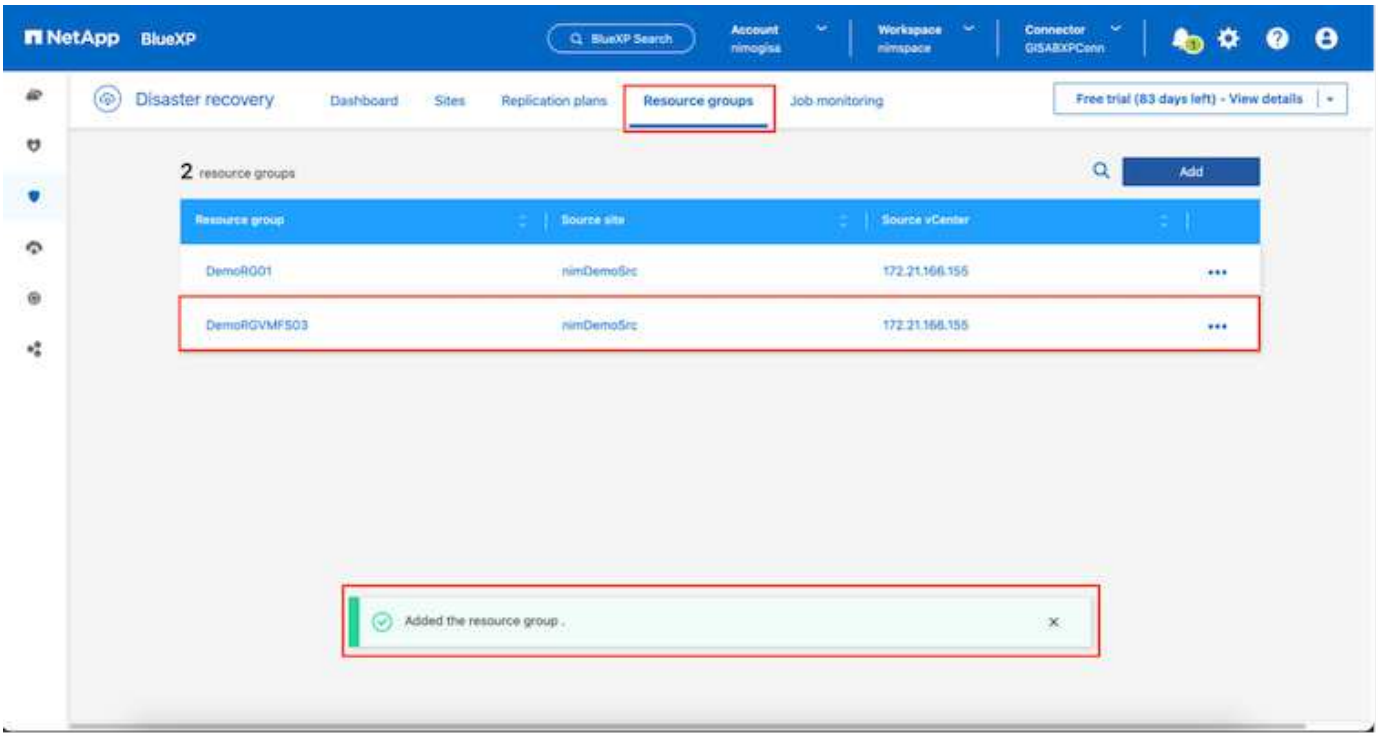
위의 방법 외에도 ONTAP CLI 또는 System Manager를 통해 SnapMirror 복제를 생성할 수도 있습니다. SnapMirror를 사용하여 데이터를 동기화하는 데 사용되는 방식과 관계없이, Disaster Recovery는 원활하고 효율적인 재해 복구 작업을 위해 워크플로를 오케스트레이션합니다.

재해 복구는 어떤 도움을 줄 수 있습니까?

소스 및 대상 사이트가 추가되면 Disaster Recovery는 자동 심층 탐색을 수행하여 관련 메타데이터와 함께 VM을 표시합니다. 또한 Disaster Recovery는 VM에서 사용하는 네트워크 및 포트 그룹을 자동으로 감지하여 채웁니다.

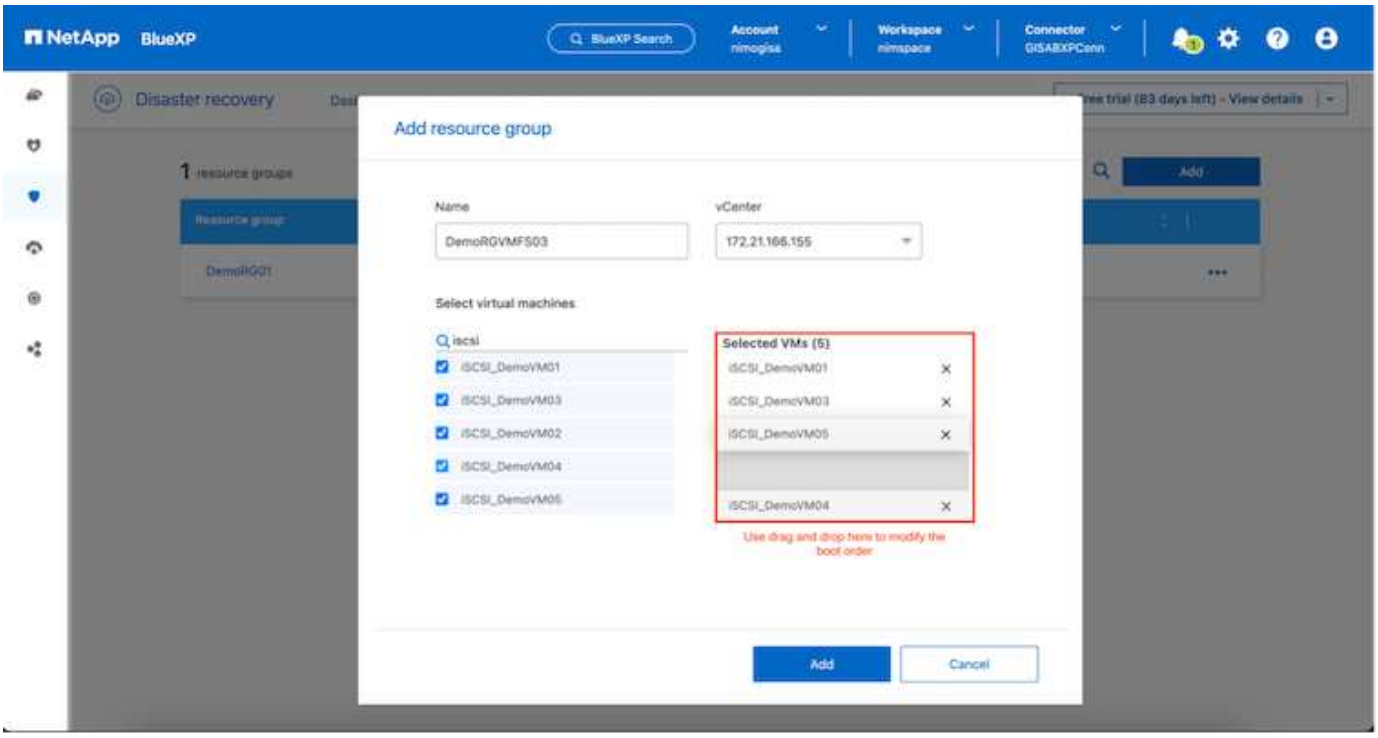


사이트를 추가한 후에는 VM을 리소스 그룹으로 묶을 수 있습니다. 재해 복구 리소스 그룹을 사용하면 종속 VM들을 논리적 그룹으로 묶고, 복구 시 실행될 부팅 순서와 부팅 지연 시간을 지정할 수 있습니다. 리소스 그룹 생성을 시작하려면 *리소스 그룹*으로 이동하여 *새 리소스 그룹 만들기*를 클릭하십시오.

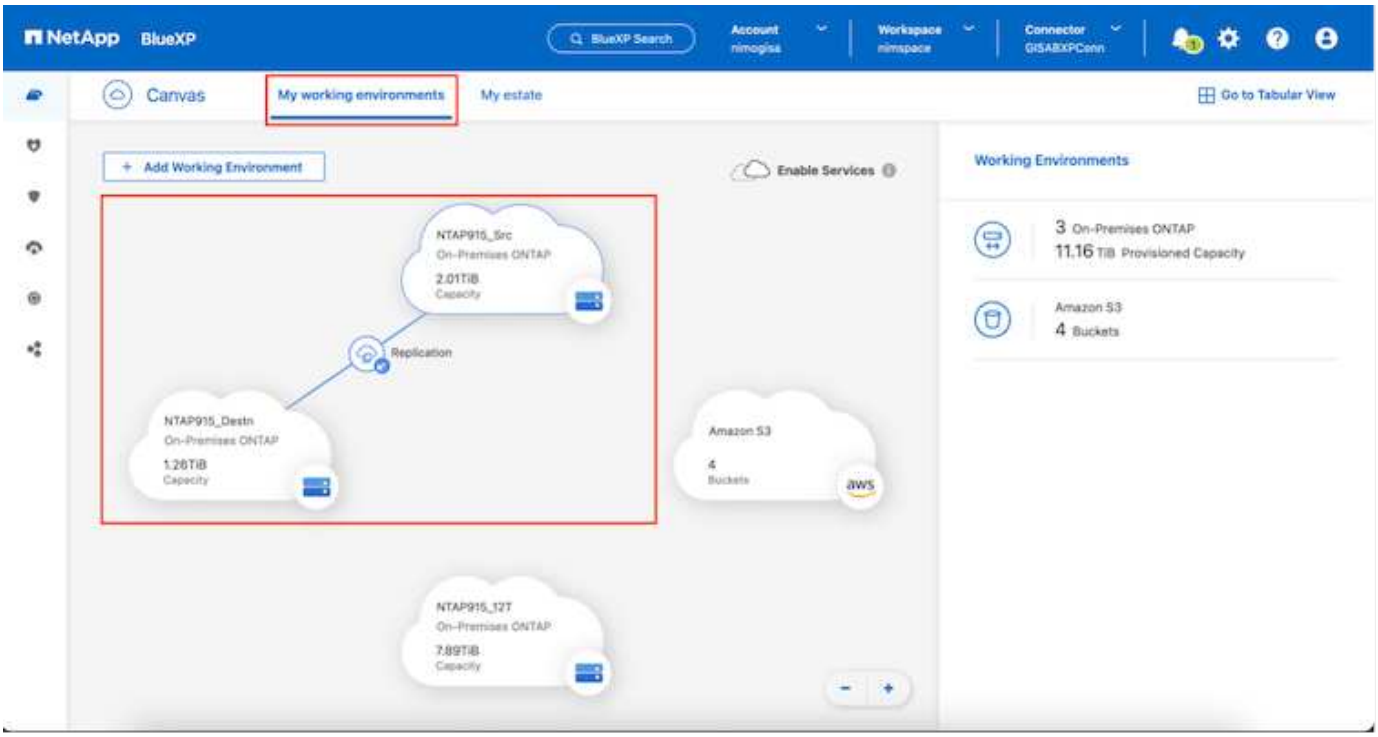


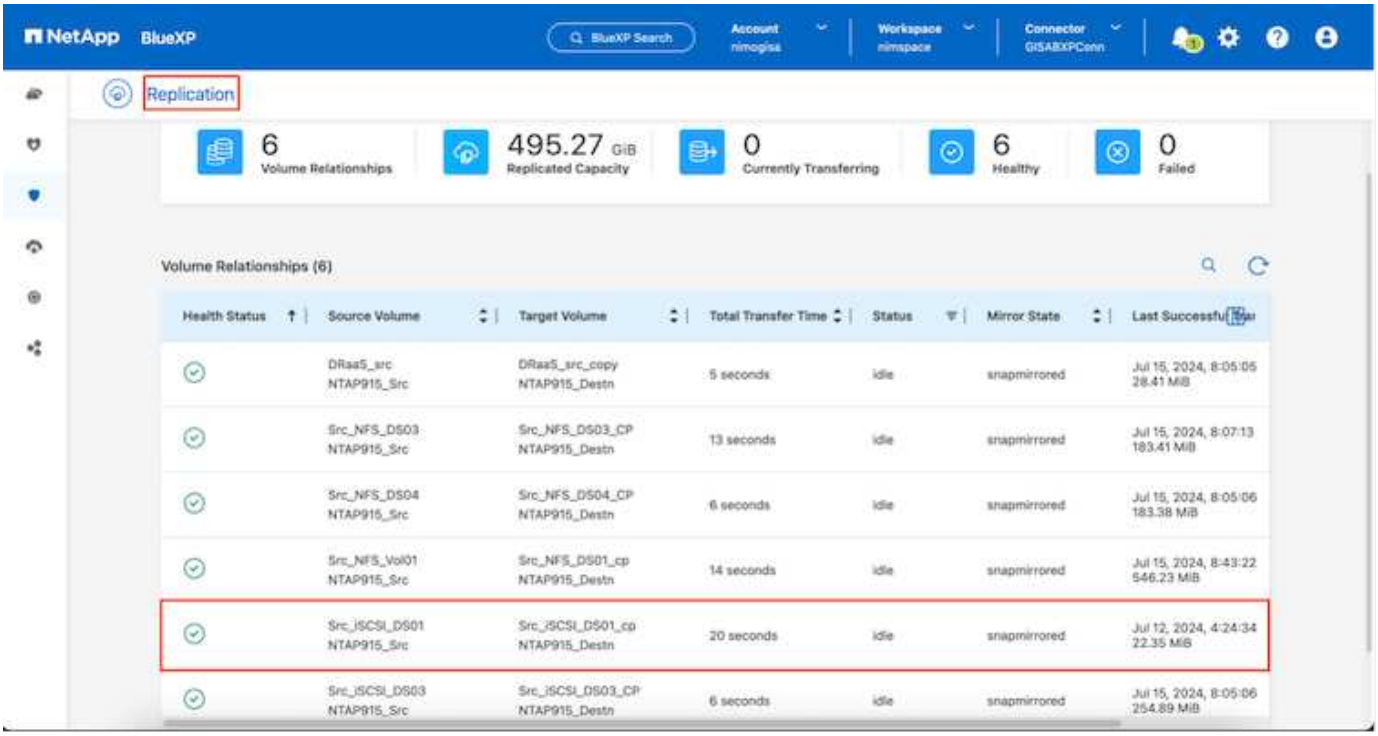
리소스 그룹은 복제 계획을 생성하는 동안에도 생성될 수 있습니다.

리소스 그룹을 만드는 동안 간단한 드래그 앤 드롭 메커니즘을 사용하여 VM의 부팅 순서를 정의하거나 수정할 수 있습니다.



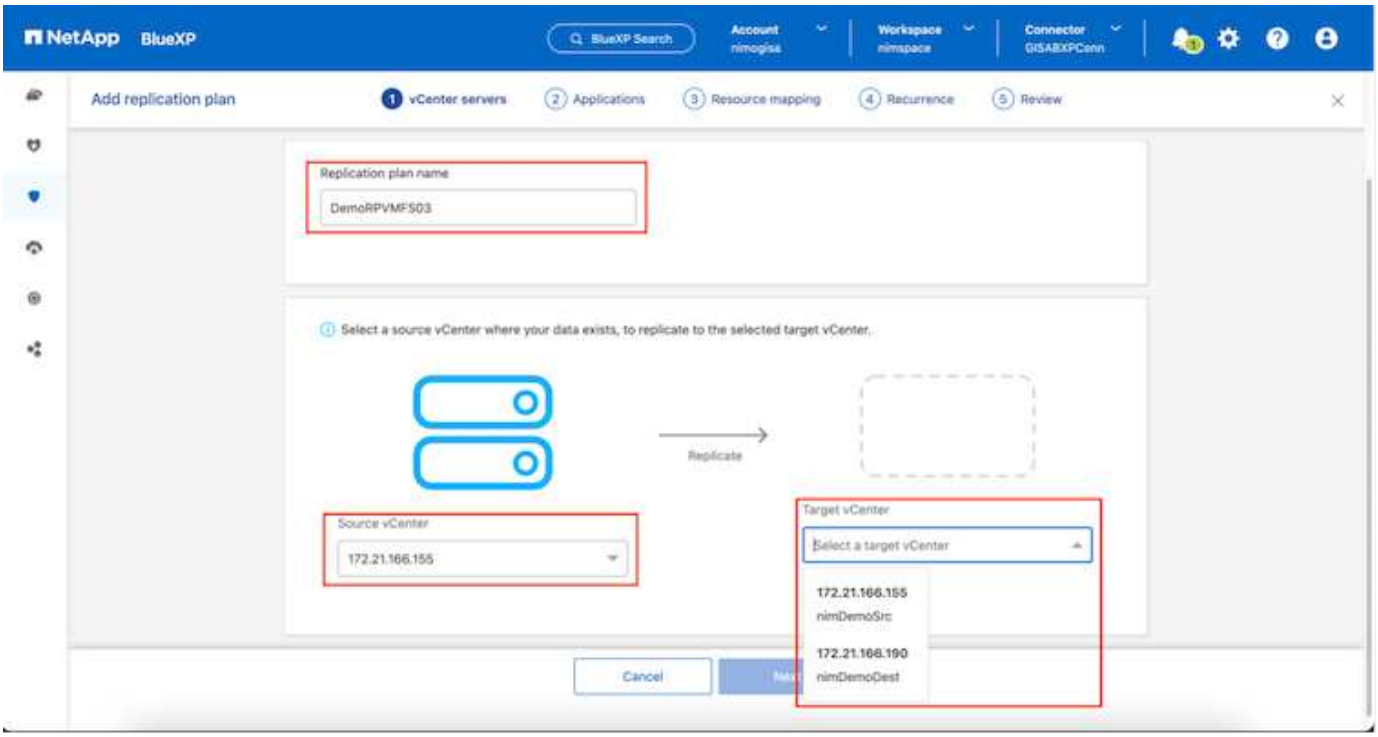
리소스 그룹을 만든 후 다음 단계는 재해 발생 시 가상 머신과 애플리케이션을 복구하기 위한 실행 청사진 또는 계획을 만드는 것입니다. 필수 구성 요소에서 언급했듯이 SnapMirror 복제는 사전에 구성할 수 있으며, DRaaS는 복제 계획을 만드는 동안 지정된 RPO 및 보존 횟수를 사용하여 구성할 수 있습니다.



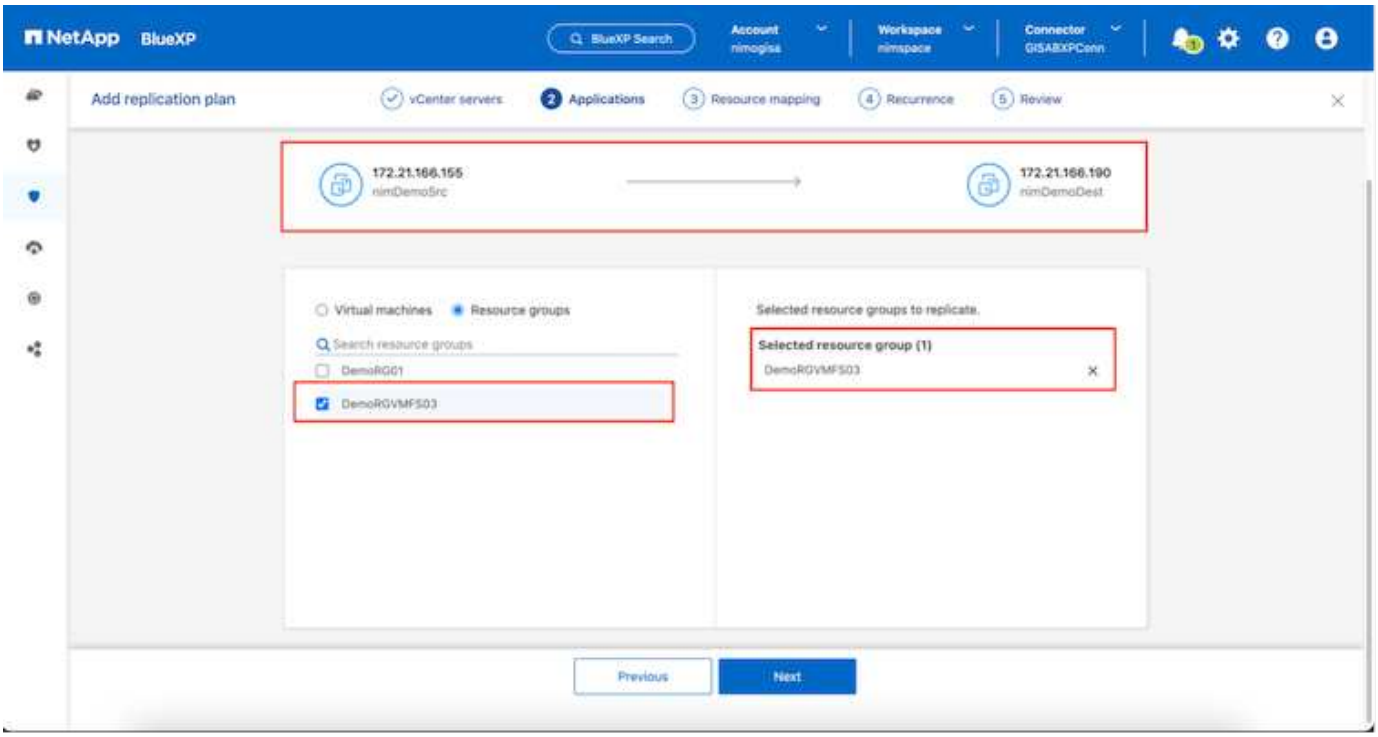


드롭다운에서 소스 및 대상 vCenter 플랫폼을 선택하여 복제 계획을 구성하고, 계획에 포함할 리소스 그룹을 선택하고, 애플리케이션을 복원하고 전원을 켜는 방법, 클러스터 및 네트워크 매핑을 그룹화합니다. 복구 계획을 정의하려면 복제 계획 탭으로 이동하여 *계획 추가*를 클릭합니다.

먼저 소스 vCenter를 선택한 다음 대상 vCenter를 선택합니다.



다음 단계는 기존 리소스 그룹을 선택하는 것입니다. 리소스 그룹이 생성되지 않은 경우 마법사는 복구 목표에 따라 필요한 가상 머신을 그룹화(기본적으로 기능적 리소스 그룹 생성)하는 데 도움을 줍니다. 이는 또한 애플리케이션 가상 머신을 복원하는 방법에 대한 작업 순서를 정의하는 데 도움이 됩니다.

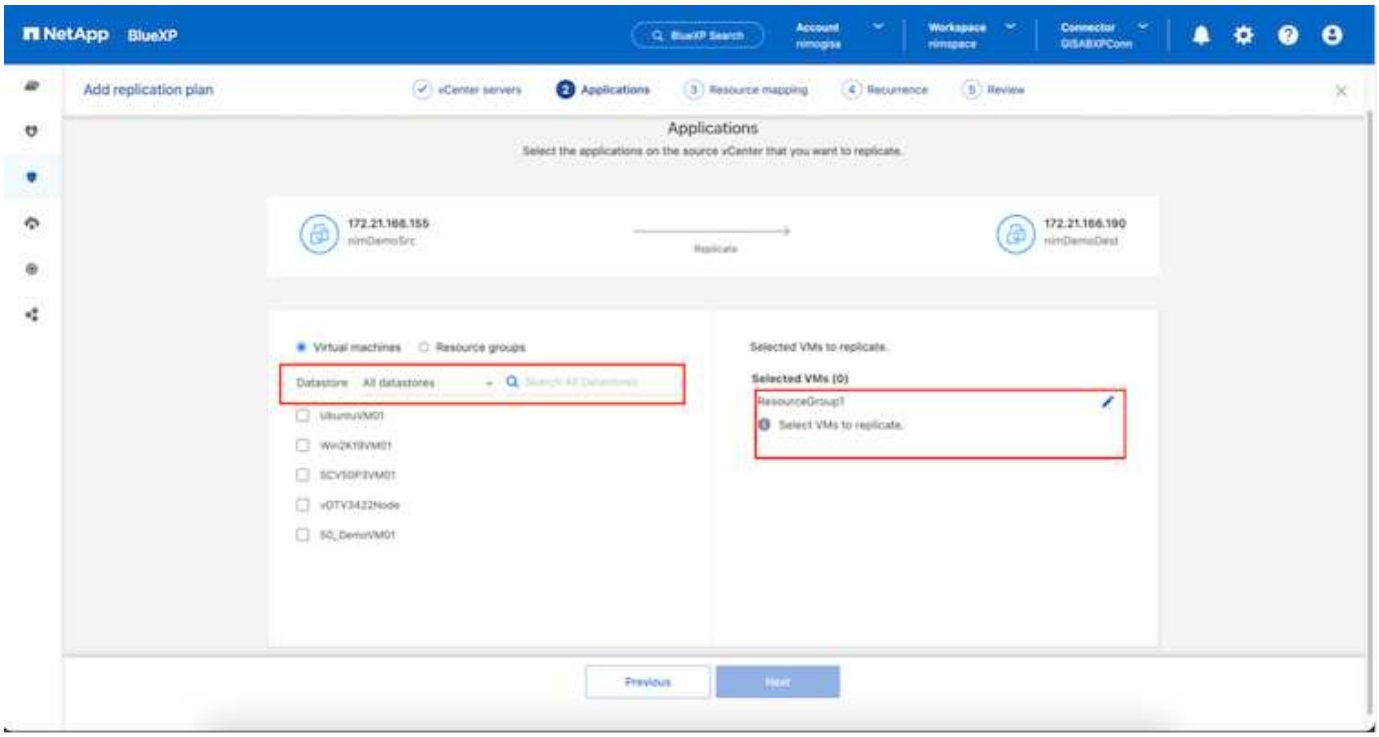


리소스 그룹을 사용하면 드래그 앤 드롭 기능을 사용하여 부팅 순서를 설정할 수 있습니다. 이를 사용하면 복구 프로세스 중에 VM의 전원이 켜지는 순서를 쉽게 수정할 수 있습니다.

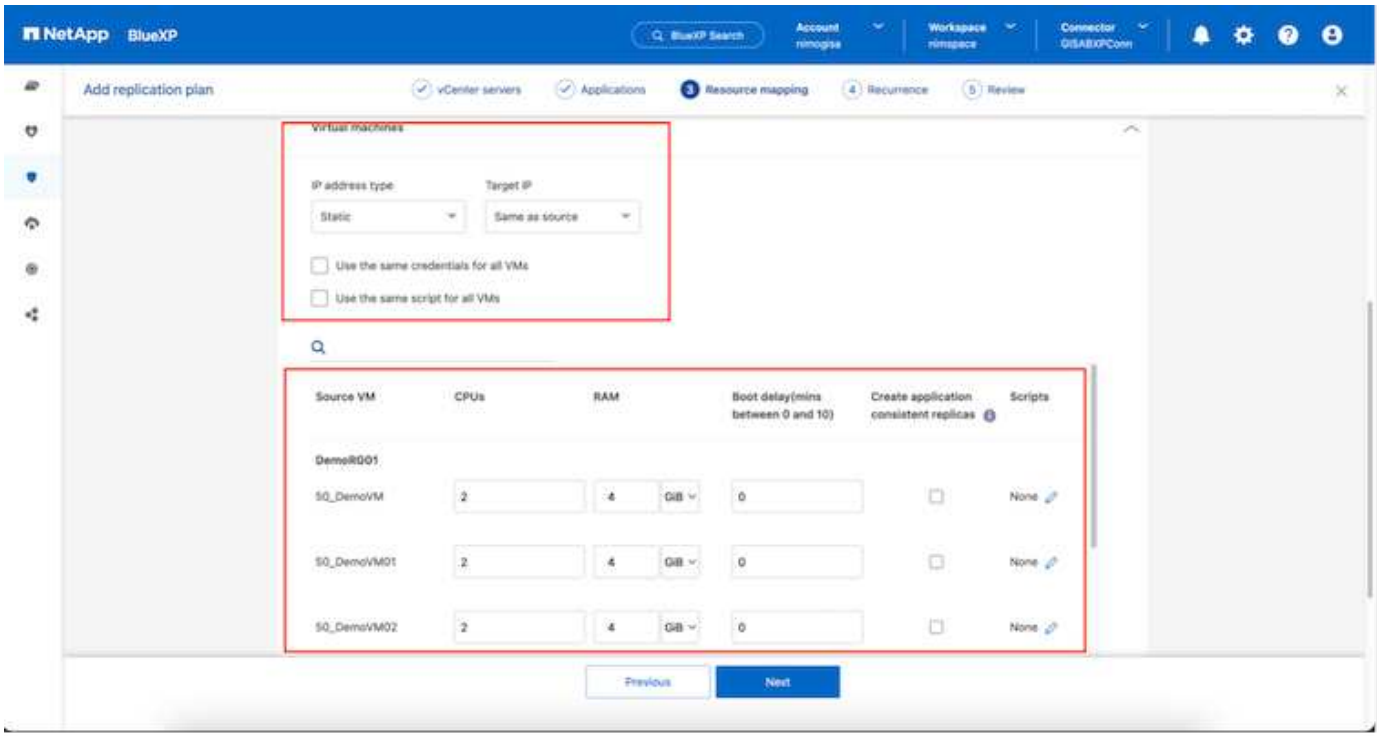
리소스 그룹 내의 각 가상 머신은 순서에 따라 순차적으로 시작됩니다. 두 개의 리소스 그룹이 병렬로

시작됩니다.

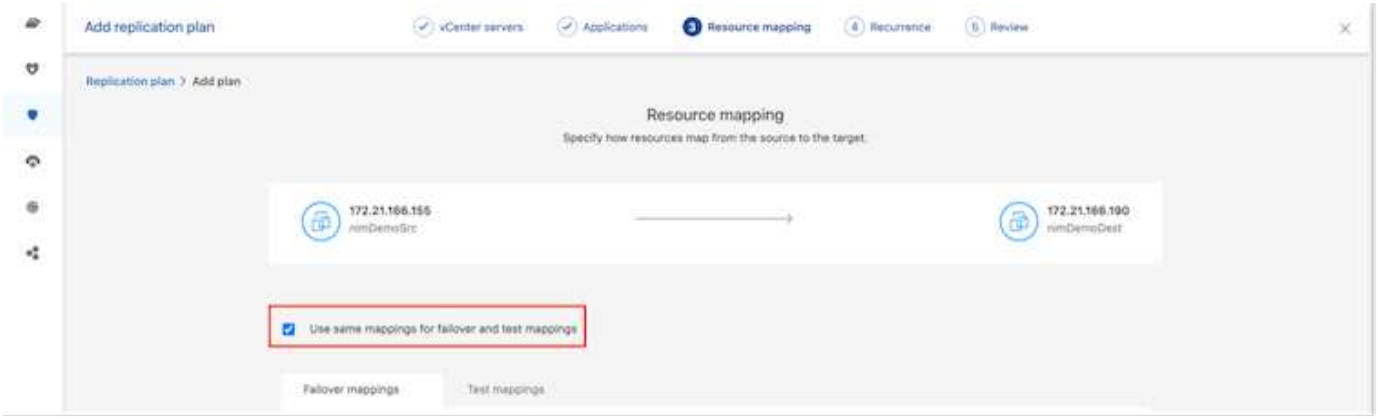
아래 스크린샷은 리소스 그룹이 사전에 생성되지 않은 경우 조직의 요구 사항에 따라 가상 머신이나 특정 데이터 저장소를 필터링하는 옵션을 보여줍니다.



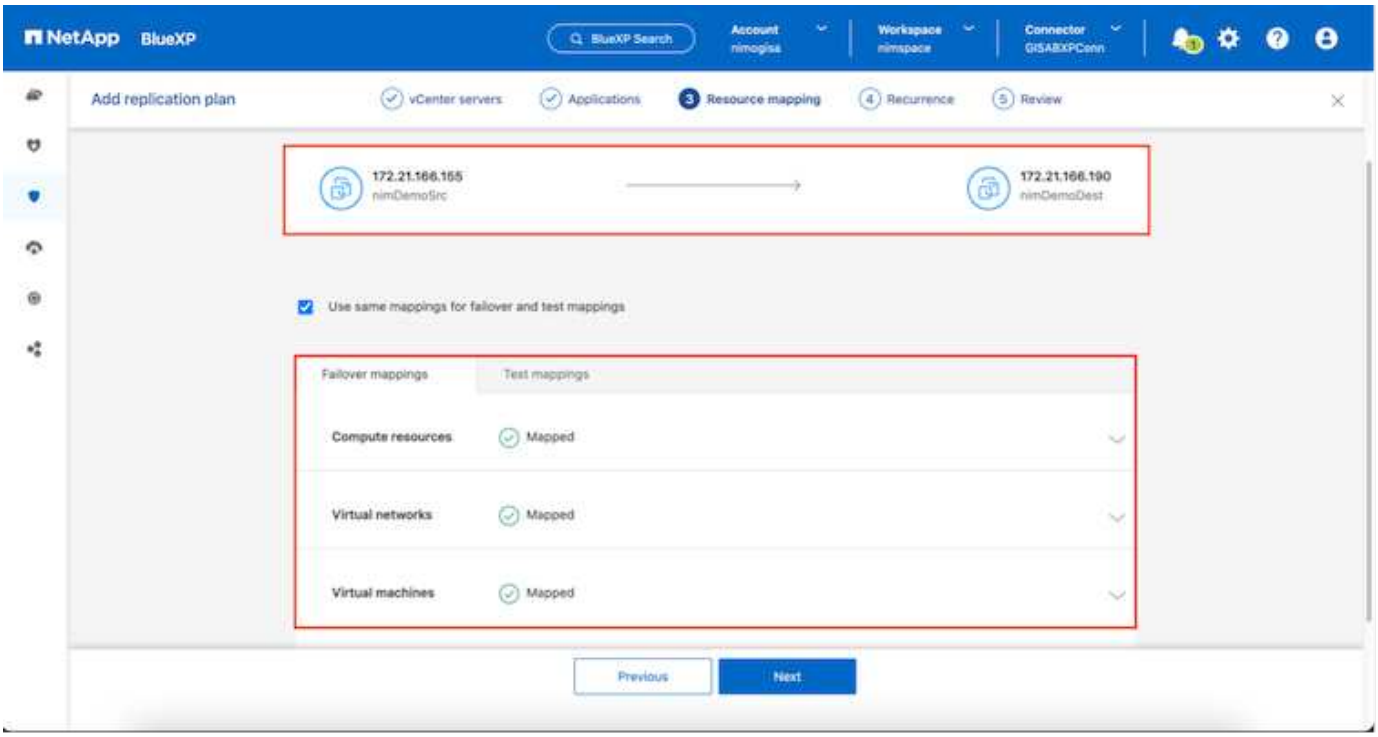
리소스 그룹을 선택한 후에는 장애 조치 매핑을 생성합니다. 이 단계에서는 소스 환경의 리소스가 대상 환경으로 어떻게 매핑되는지 지정합니다. 여기에는 컴퓨팅 리소스, 가상 네트워크가 포함됩니다. IP 사용자 지정, 사전 및 사후 스크립트, 부팅 지연, 애플리케이션 일관성 등입니다. 자세한 내용은 "복제 계획 만들기"을(를) 참조하십시오.



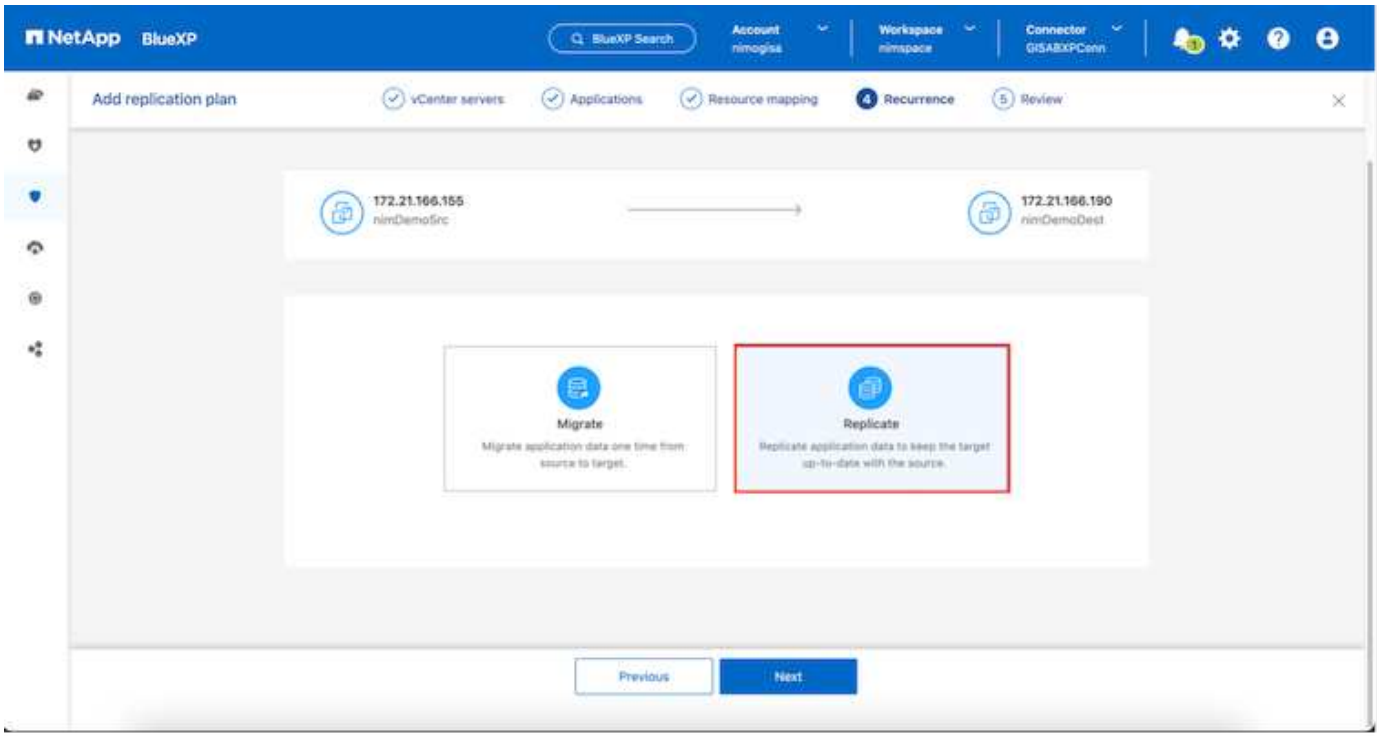
기본적으로 테스트 작업과 장애 조치 작업 모두에 동일한 매핑 매개변수가 사용됩니다. 테스트 환경에 다른 매핑을 적용하려면 아래와 같이 체크박스 선택을 해제한 후 테스트 매핑 옵션을 선택하세요.



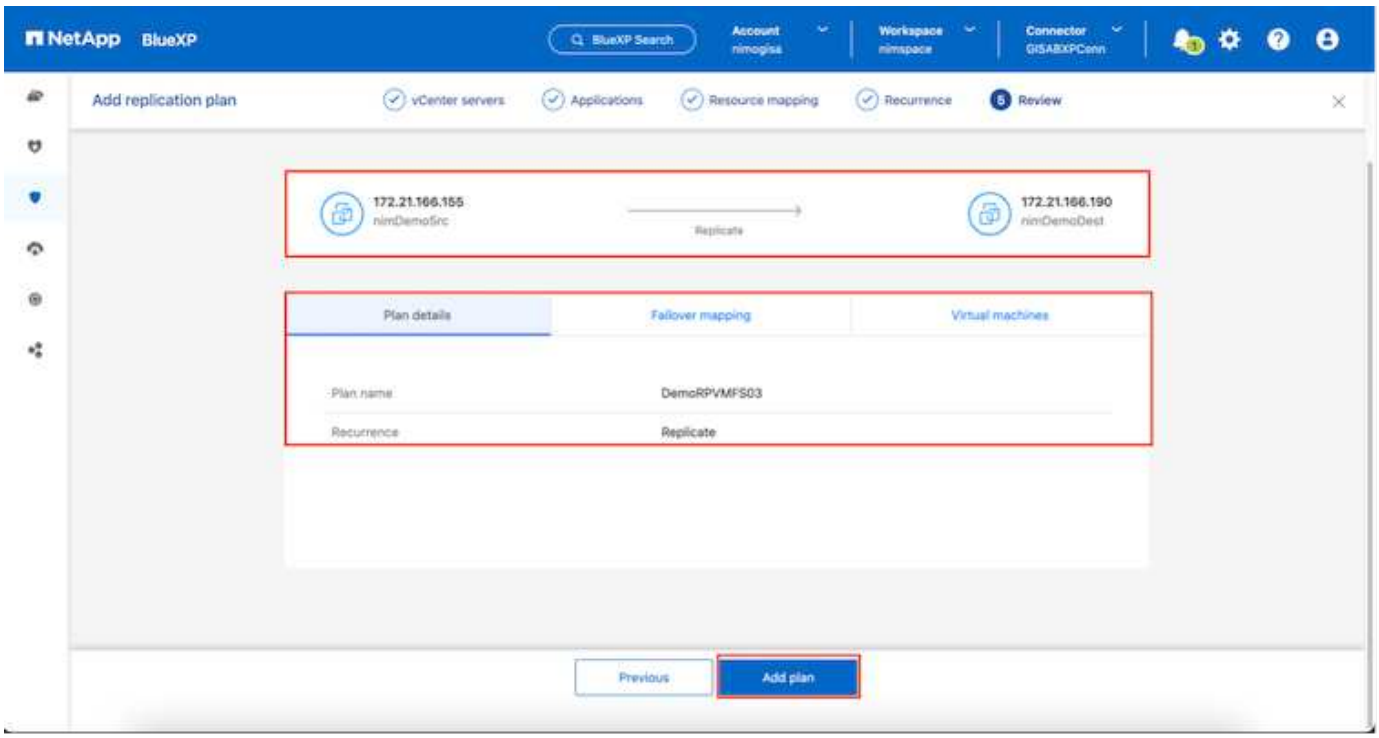
리소스 매핑이 완료되면 다음을 클릭합니다.

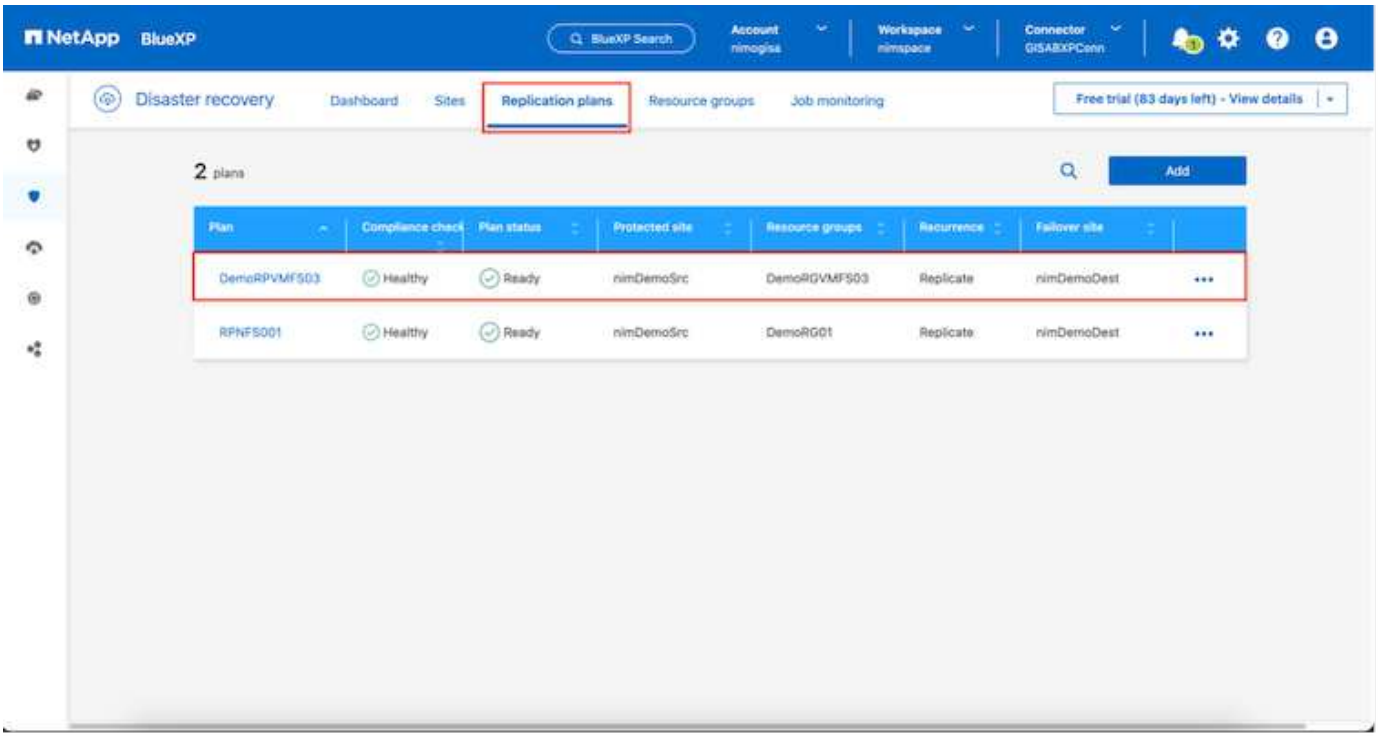


반복 유형을 선택하세요. 간단히 말해서, 마이그레이션(장애 조치를 사용한 일회성 마이그레이션) 또는 반복적 지속적 복제 옵션을 선택합니다. 이 연습에서는 복제 옵션이 선택되었습니다.

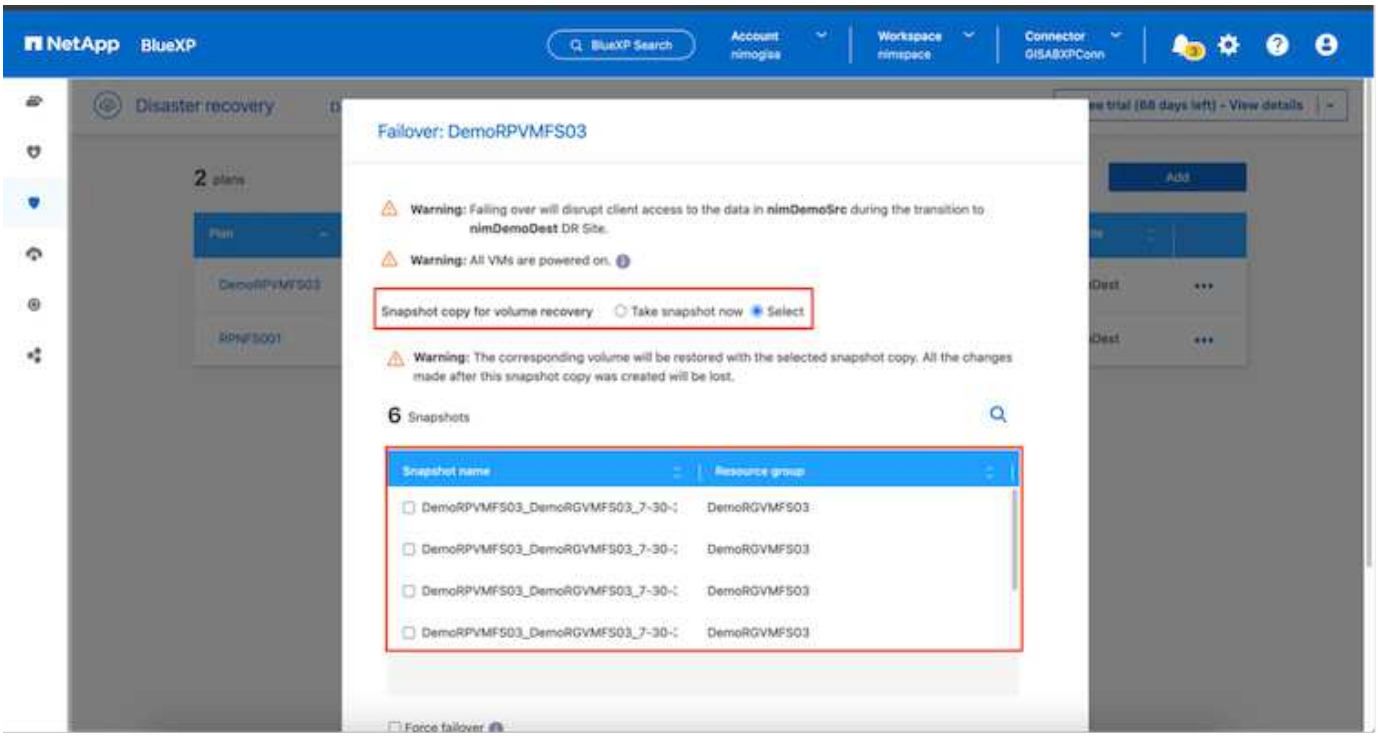


완료되면 생성된 매핑을 검토한 후 계획 추가를 클릭합니다.

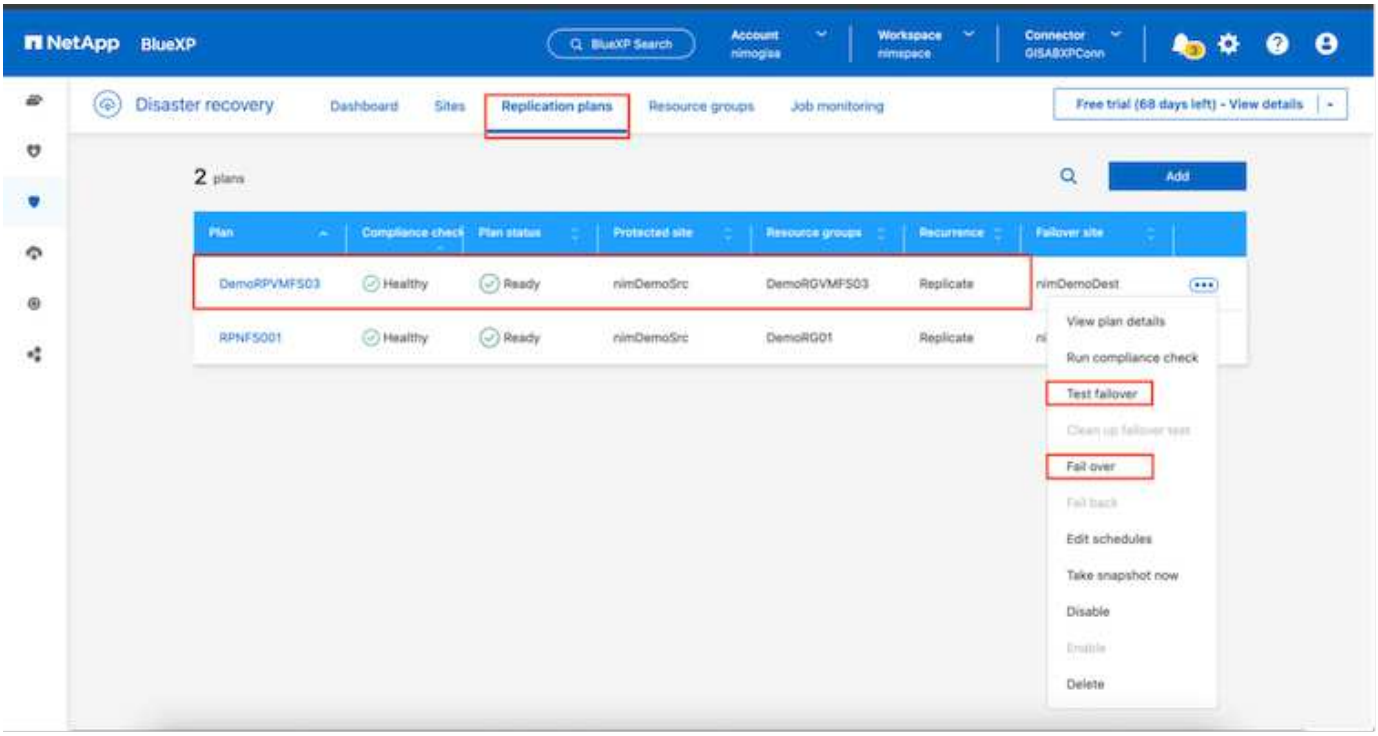




복제 계획이 생성되면 요구 사항에 따라 페일오버 옵션, 테스트 페일오버 옵션 또는 마이그레이션 옵션을 선택하여 페일오버를 수행할 수 있습니다. 재해 복구는 30분마다 계획에 따라 복제 프로세스가 실행되도록 보장합니다. 페일오버 및 테스트 페일오버 옵션 중에는 가장 최근의 SnapMirror 스냅샷 복사본을 사용하거나 특정 시점 스냅샷 복사본에서 특정 스냅샷 복사본을 선택할 수 있습니다(SnapMirror의 보존 정책에 따라). 특정 시점 옵션은 랜섬웨어와 같은 손상 이벤트가 발생하여 가장 최근의 복제본이 이미 손상되었거나 암호화된 경우에 매우 유용할 수 있습니다. 재해 복구는 사용 가능한 모든 복구 지점을 표시합니다.



복제 계획에 지정된 구성으로 장애 조치 또는 테스트 장애 조치를 트리거하려면 장애 조치 또는 *테스트 장애 조치*를 클릭합니다.

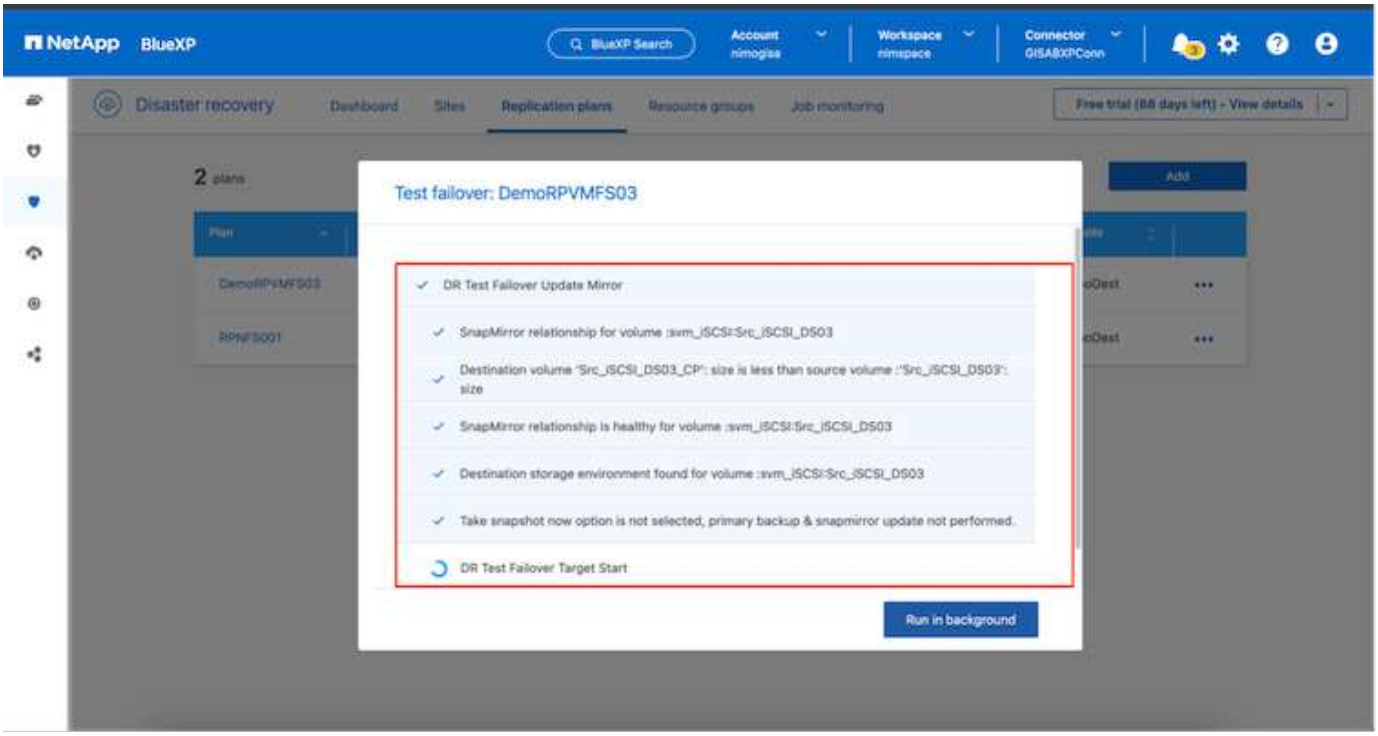


장애 조치 또는 테스트 장애 조치 작업 중에는 무슨 일이 일어나나요?

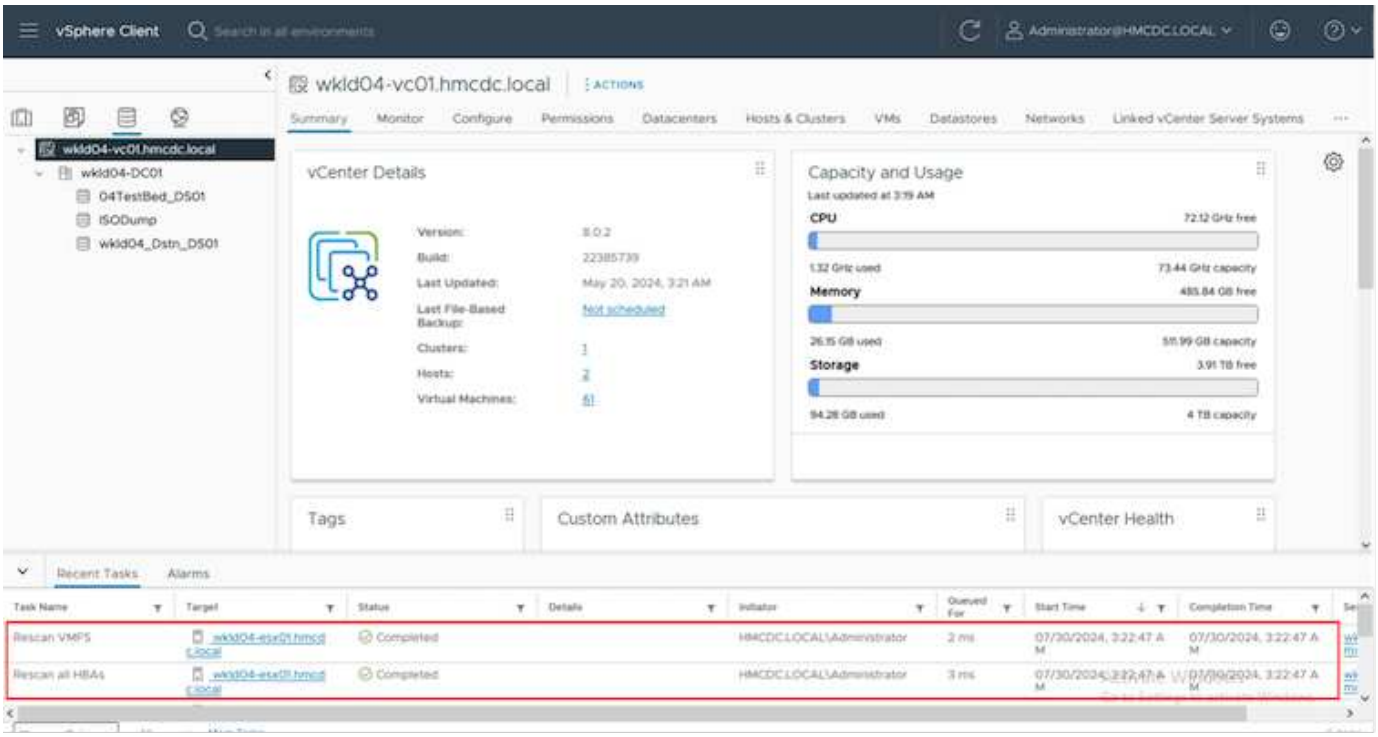
테스트 페일오버 작업 중에 재해 복구는 대상 볼륨의 최신 스냅샷 복사본 또는 선택한 스냅샷을 사용하여 대상 ONTAP 스토리지 시스템에 FlexClone 볼륨을 생성합니다.

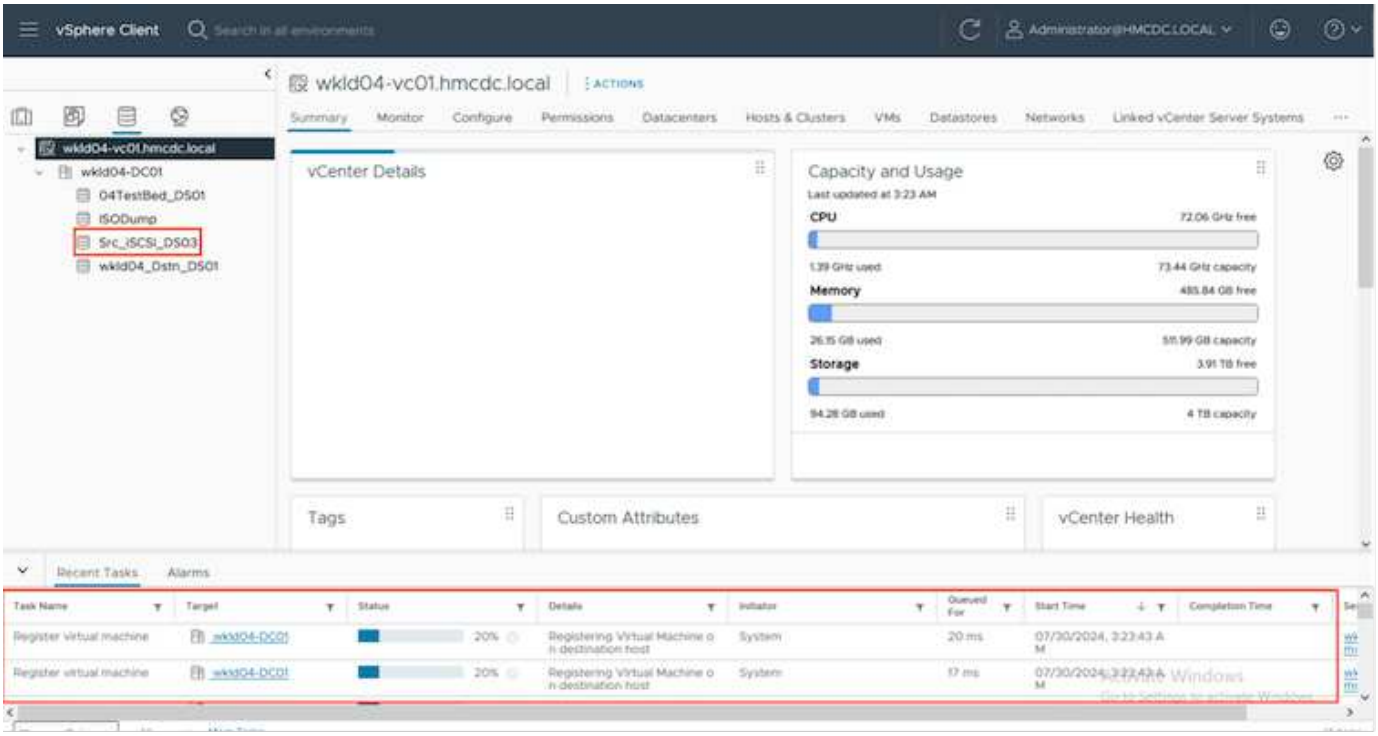
테스트 장애 조치 작업은 대상 ONTAP 스토리지 시스템에 복제된 볼륨을 생성합니다.

테스트 복구 작업을 실행해도 SnapMirror 복제에는 영향을 미치지 않습니다.



이 프로세스 동안 Disaster Recovery는 원래 타겟 볼륨을 매핑하지 않습니다. 대신 선택한 스냅샷에서 새로운 FlexClone 볼륨을 생성하고, FlexClone 볼륨을 지원하는 임시 데이터 저장소가 ESXi 호스트에 매핑됩니다.



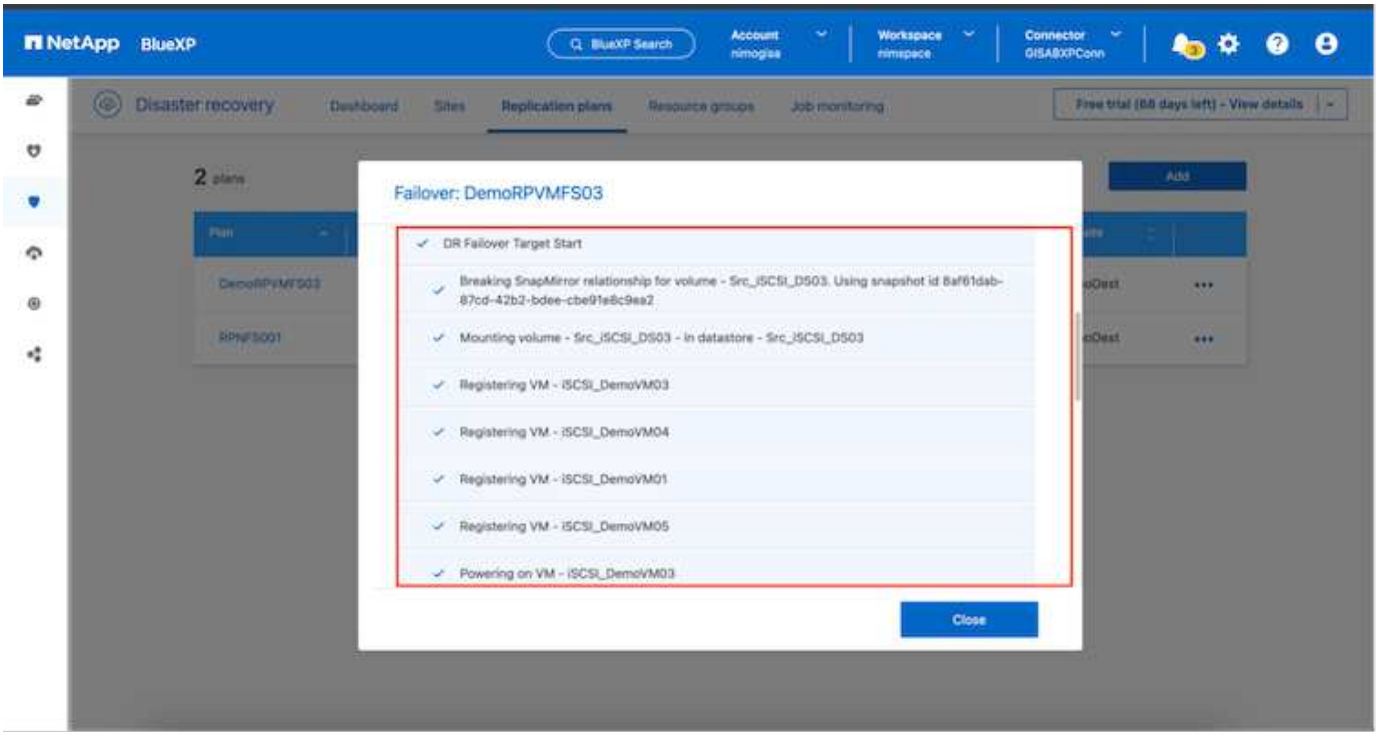


테스트 페일오버 작업이 완료되면 *"Clean Up failover test"*를 사용하여 정리 작업을 시작할 수 있습니다. 이 작업 중에 재해 복구는 작업에 사용된 FlexClone 볼륨을 삭제합니다.

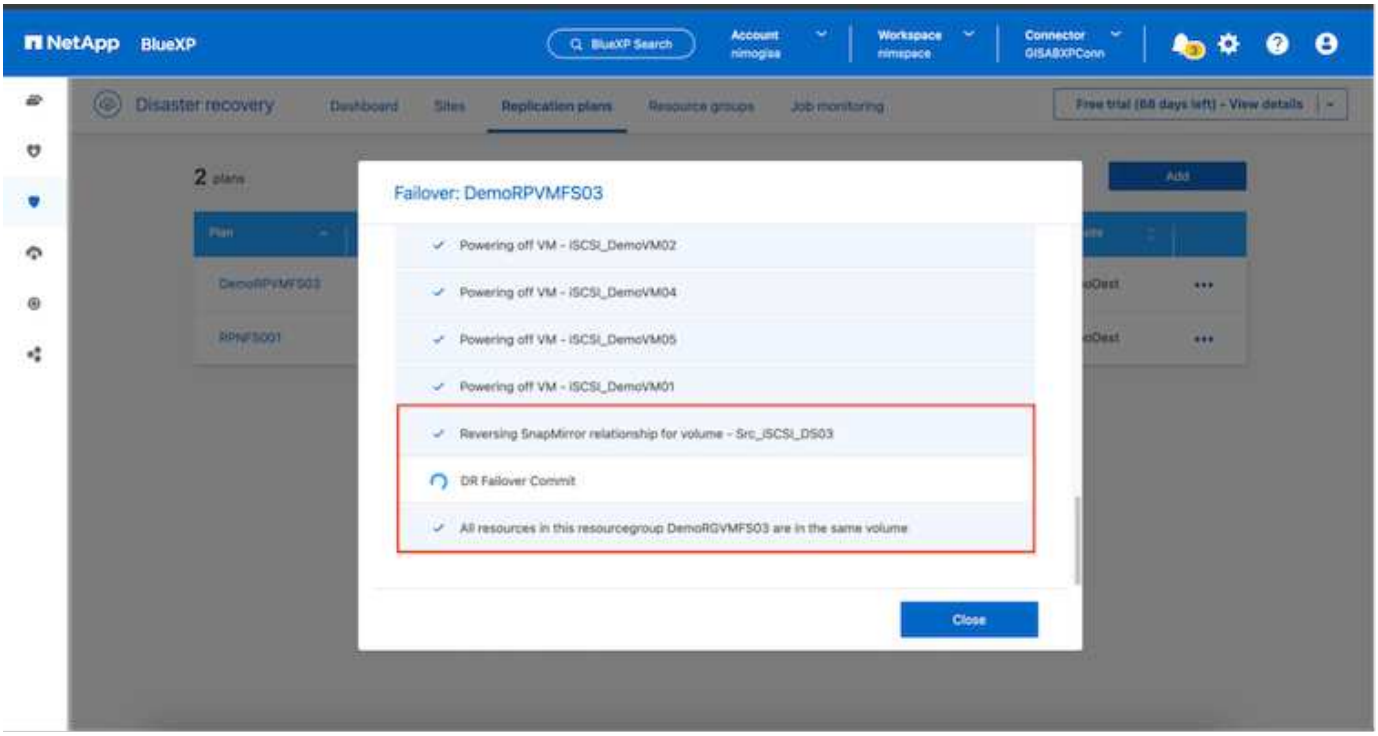
실제 재해 발생 시, 재해 복구는 다음과 같은 단계를 수행합니다:

1. 사이트 간의 SnapMirror 관계를 끊습니다.

2. 재서명 후 VMFS 데이터 저장소 볼륨을 마운트하여 즉시 사용할 수 있습니다.
3. VM 등록
4. VM 전원 켜기



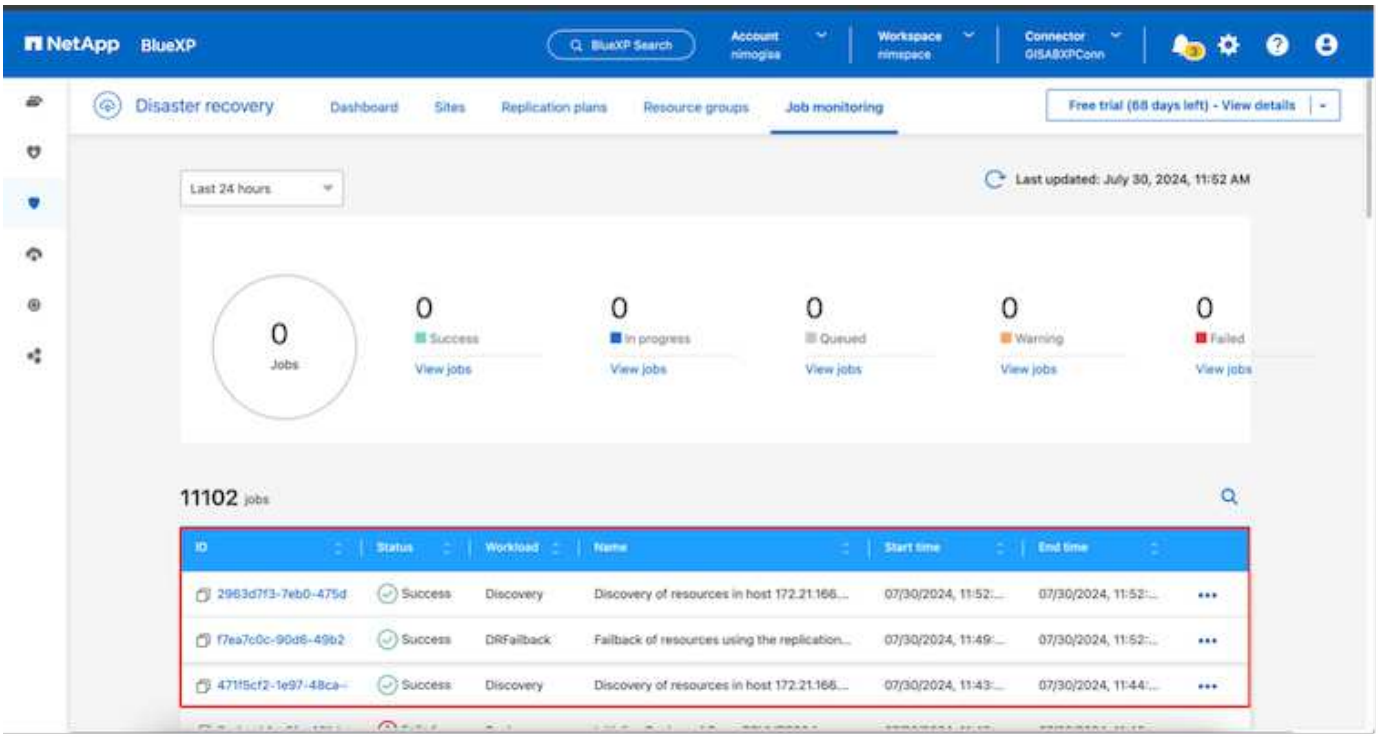
기본 사이트가 가동되면 재해 복구 기능을 통해 SnapMirror에 대한 역방향 재동기화 및 페일백을 활성화할 수 있으며, 이 또한 버튼 클릭 한 번으로 수행할 수 있습니다.



그리고 마이그레이션 옵션을 선택하면 계획된 장애 조치 이벤트로 간주됩니다. 이 경우 소스 사이트의 가상 머신을

종료하는 추가 단계가 실행됩니다. 나머지 단계는 장애 조치 이벤트와 동일합니다.

콘솔 또는 ONTAP CLI에서 해당 데이터스토어 볼륨의 복제 상태를 모니터링할 수 있으며, 작업 모니터링을 통해 장애 조치 또는 테스트 장애 조치의 상태를 추적할 수 있습니다.



이는 맞춤형 재해 복구 계획을 처리하는 강력한 솔루션을 제공합니다. 장애 조치는 계획된 장애 조치로 수행할 수도 있고, 재해가 발생하고 DR 사이트를 활성화하기로 결정한 경우 버튼을 클릭하여 장애 조치를 수행할 수도 있습니다.

이 프로세스에 대해 자세히 알아보려면 자세한 연습 비디오를 따르거나 다음을 사용하십시오."솔루션 시뮬레이터" .

Red Hat OpenShift 컨테이너 워크로드를 활용한 NetApp 하이브리드 멀티클라우드

시작하기

Red Hat OpenShift 컨테이너 워크로드를 위한 NetApp 하이브리드 멀티클라우드 솔루션

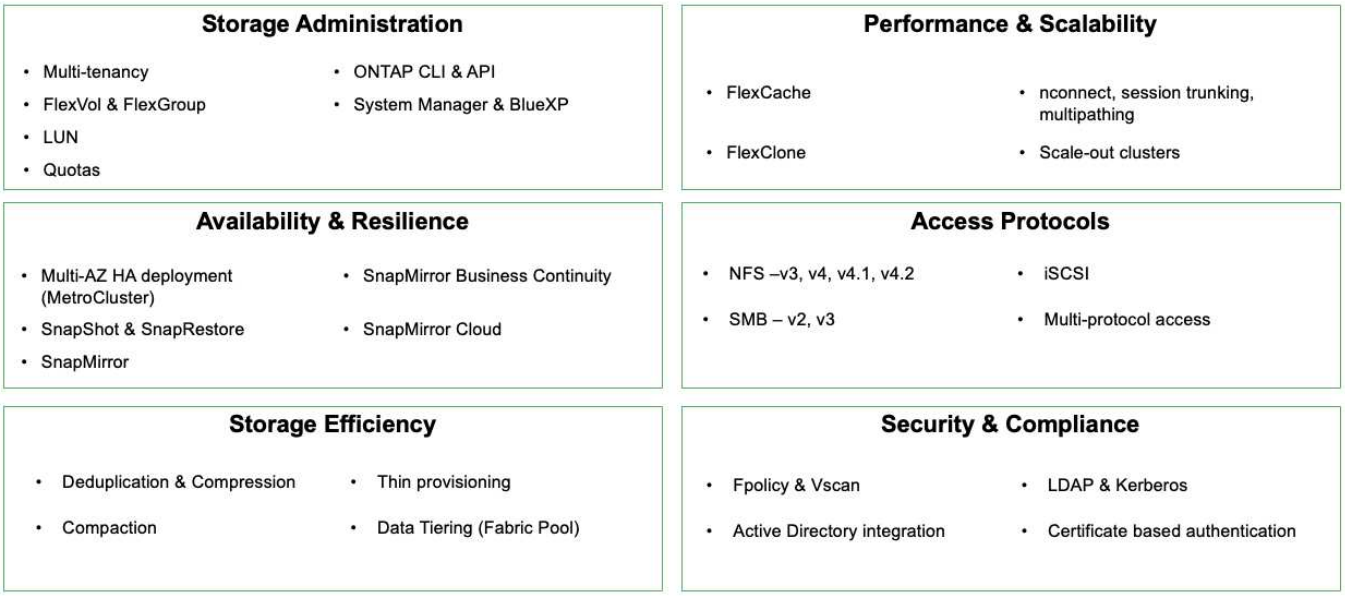
NetApp 기존 엔터프라이즈 애플리케이션을 현대화하고 Kubernetes를 기반으로 구축된 컨테이너와 오케스트레이션 플랫폼을 사용하여 새로운 애플리케이션을 구축하는 고객이 크게 늘어나는 것을 보고 있습니다. Red Hat OpenShift Container Platform은 많은 고객이 도입한 사례 중 하나입니다.

개요

점점 더 많은 고객이 기업 내에서 컨테이너를 도입함에 따라 NetApp 상태 저장 애플리케이션의 지속적인 스토리지 요구 사항과 데이터 보호, 데이터 보안, 데이터 마이그레이션과 같은 기존 데이터 관리 요구 사항을 충족하는 데 완벽한 위치에 있습니다. 하지만 이러한 요구 사항은 다양한 전략, 도구, 방법을 통해 충족됩니다.

- NetApp ONTAP** 기반 스토리지 옵션은 아래 나열되어 있으며 컨테이너와 Kubernetes 배포에 보안, 데이터 보호, 안정성 및 유연성을 제공합니다.
  - 온프레미스의 자체 관리형 스토리지:
- NetApp Fabric Attached Storage(FAS), NetApp All Flash FAS Array(AFF), NetApp All SAN Array(ASA) 및 ONTAP Select
  - 온프레미스의 공급자 관리 스토리지:
- NetApp Keystone STaaS(Storage as a Service)를 제공합니다.
  - 클라우드의 자체 관리형 스토리지:
- NetApp Cloud Volumes ONTAP(CVO)은 하이퍼스케일러에서 자체 관리형 스토리지를 제공합니다.
  - 클라우드의 공급자 관리 스토리지:
- Amazon FSx for NetApp ONTAP, Azure NetApp Files 및 Google Cloud NetApp Volumes 클라우드에서 파일 기반 스토리지를 제공합니다.

ONTAP feature highlights

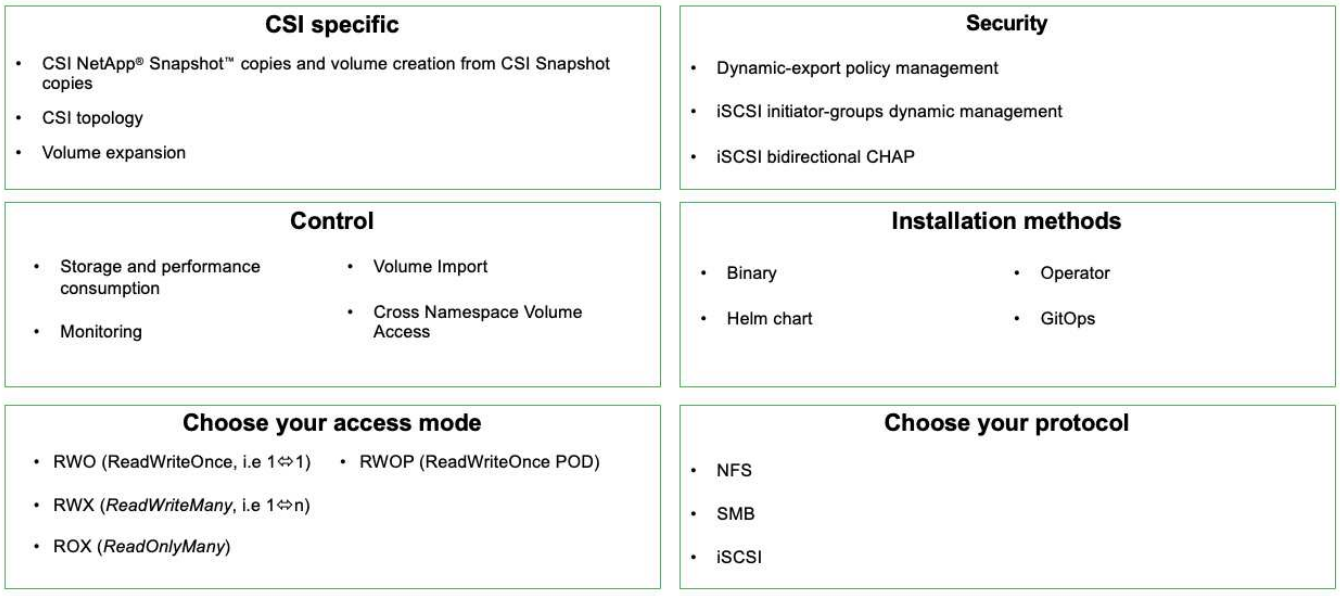


NetApp Console을 사용하면 단일 컨트롤 플레인/인터페이스에서 모든 스토리지 및 데이터 자산을 관리할 수 있습니다.

NetApp Console을 사용하면 클라우드 스토리지(예: Cloud Volumes ONTAP 및 Azure NetApp Files)를 생성 및 관리하고, 데이터를 이동, 보호 및 분석하며, 다양한 온프레미스 및 엣지 스토리지 장치를 제어할 수 있습니다.

- NetApp Trident**는 다양한 NetApp 스토리지 옵션에 의해 지원되는 영구 스토리지를 빠르고 쉽게 사용할 수 있도록 하는 CSI 호환 스토리지 오케스트레이터입니다. NetApp 에서 유지 관리하고 지원하는 오픈 소스 소프트웨어입니다.

Astra Trident CSI feature highlights



비즈니스에 중요한 컨테이너 작업에는 지속적인 볼륨 이상이 필요합니다. 데이터 관리 요구 사항에는 애플리케이션 쿠버네티스 객체의 보호 및 마이그레이션도 필요합니다.

애플리케이션 데이터에는 사용자 데이터 외에도 Kubernetes 객체가 포함됩니다. 다음은 몇 가지 예입니다. - Pod 사양, PVC, 배포, 서비스와 같은 Kubernetes 객체 - 구성 맵 및 비밀과 같은 사용자 지정 구성 객체 - 스냅샷 복사본, 백업, 복제본과 같은 영구 데이터 - CR 및 CRD와 같은 사용자 지정 리소스

NetApp Trident Protect는 NetApp Trident에 무료 애드온으로 제공되며, NetApp ONTAP 스토리지 시스템을 기반으로 하는 스테이트풀 Kubernetes 애플리케이션의 기능과 가용성을 향상시키는 고급 애플리케이션 데이터 관리 기능을 제공합니다. Trident Protect는 퍼블릭 클라우드와 온프레미스 환경 모두에서 컨테이너화된 워크로드의 관리, 보호 및 이동을 간소화합니다. 또한 API 및 CLI를 통해 강력한 자동화 기능을 제공합니다.

이 참조 문서는 Trident Protect를 사용하여 RedHat OpenShift 플랫폼에 배포된 컨테이너 기반 애플리케이션의 데이터 보호에 대한 검증을 제공합니다. 또한 이 솔루션은 컨테이너 플랫폼을 관리하기 위한 Red Hat Advanced Cluster Management(ACM)의 배포 및 사용에 대한 높은 수준의 세부 정보를 제공합니다. 또한 이 문서에서는 Trident CSI 프로비저너를 사용하여 NetApp 스토리지를 Red Hat OpenShift 컨테이너 플랫폼과 통합하는 방법에 대한 세부 정보를 강조합니다.

Red Hat OpenShift 컨테이너 워크로드를 위한 **NetApp** 하이브리드 멀티클라우드 솔루션의 가치 제안

대부분의 고객은 기존 인프라 없이 Kubernetes 기반 환경을 구축하는 것으로 시작하지 않습니다. 아마도 그들은 대부분의 엔터프라이즈 애플리케이션을 가상 머신(예: 대규모 VMware 환경)에서 실행하는 전통적인 IT 부서일 것입니다. 그런 다음 그들은 현대적 애플리케이션 개발팀의 요구를 충족시키기 위해 작은 컨테이너 기반 환경을 구축하기 시작했습니다. 이러한 이니셔티브는 보통 작게 시작하지만, 팀이 새로운 기술과 능력을 배우고 이를 도입함으로써 얻을 수 있는 많은 이점을 인식하기 시작하면서 점점 더 보편화되기 시작합니다. 고객에게 좋은 소식은 NetApp 두 환경의 요구 사항을 모두 충족할 수 있다는 것입니다. Red Hat OpenShift를 활용한 하이브리드 멀티클라우드 솔루션 세트를 통해 NetApp 고객은 전체 인프라와 조직을 개편하지 않고도 최신 클라우드 기술과 서비스를 도입할 수 있습니다. 고객 애플리케이션과 데이터가 온프레미스, 클라우드, 가상 머신 또는 컨테이너에서 호스팅되는지 여부에 관계없이 NetApp 일관된 데이터 관리, 보호, 보안 및 이동성을 제공할 수 있습니다. 이러한 새로운 솔루션을 사용하면 NetApp 수십 년 동안 온프레미스 데이터 센터 환경에서 제공해 온 동일한 가치를 기업의 전체 데이터 수평선에서 사용할 수 있으며, 새로운 기술을 습득하거나 새로운 팀을 구성하기 위해 상당한 투자를 할 필요가 없습니다. NetApp 고객이 클라우드 여정의 어떤 단계에 있든 이러한 비즈니스 과제를 해결하는 데 도움을 줄 수 있는 좋은 위치에 있습니다.

Red Hat Openshift를 활용한 NetApp 하이브리드 멀티 클라우드:

- NetApp 기반 스토리지 솔루션과 함께 Red Hat OpenShift를 사용할 때 고객이 데이터와 애플리케이션을 관리, 보호, 보안 및 마이그레이션하는 가장 좋은 방법을 보여주는 검증된 설계와 사례를 고객에게 제공합니다.
- VMware 환경, 베어 메탈 인프라 또는 이 두 가지의 조합에서 NetApp 스토리지와 함께 Red Hat OpenShift를 실행하는 고객을 위한 모범 사례를 제시합니다.
- 온프레미스와 클라우드 환경, 그리고 두 가지를 모두 사용하는 하이브리드 환경에 대한 전략과 옵션을 설명합니다.

Red Hat OpenShift 컨테이너 워크로드를 위한 NetApp Hybrid Multicloud 지원 솔루션

이 솔루션은 OpenShift Container Platform(OCP), OpenShift Advanced Cluster Manager(ACM), NetApp ONTAP, NetApp Console 및 NetApp Trident Protect를 사용한 마이그레이션 및 중앙 집중식 데이터 보호 기능을 테스트하고 검증합니다.

이 솔루션의 경우 다음 시나리오가 NetApp 에서 테스트되어 검증되었습니다. 솔루션은 다음과 같은 특성에 따라 여러 시나리오로 구분됩니다.

- 온프레미스
- 구름
  - 자체 관리형 OpenShift 클러스터 및 자체 관리형 NetApp 스토리지
  - 공급자 관리 OpenShift 클러스터 및 공급자 관리 NetApp 스토리지

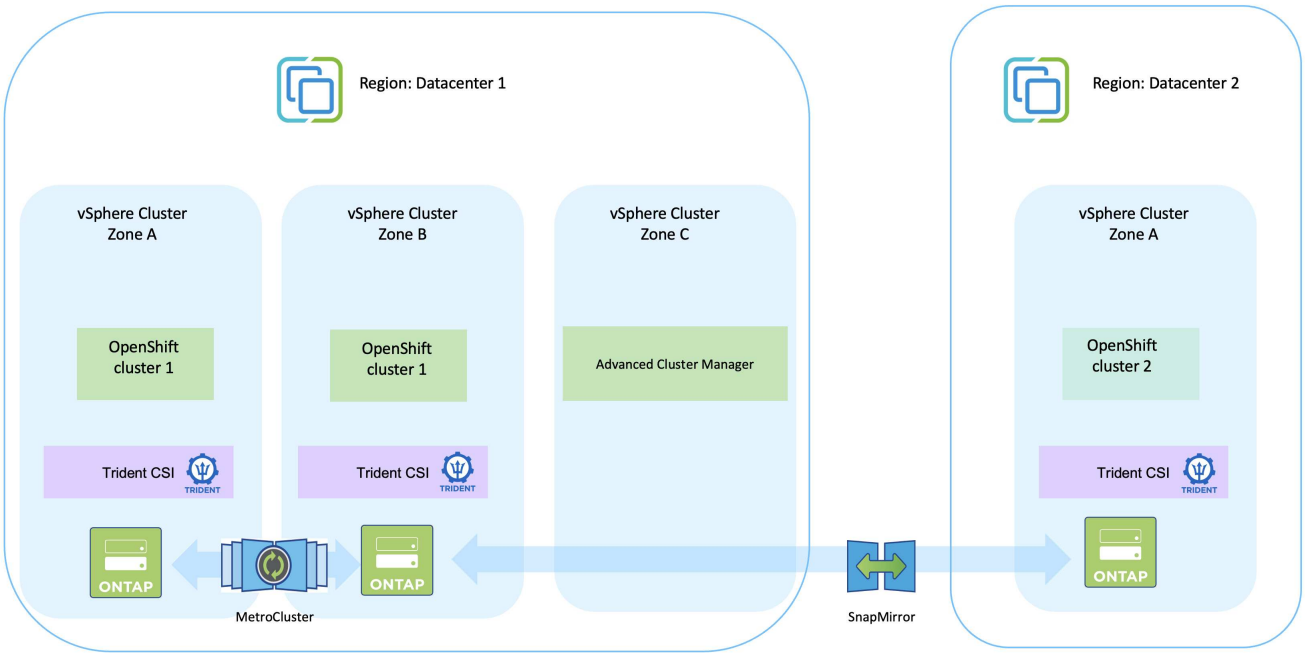
향후 추가적인 솔루션과 사용 사례를 구축할 예정입니다.

시나리오 **1: Trident Protect**를 사용한 온프레미스 환경 내 데이터 보호 및 마이그레이션

온프레미스: 자체 관리형 **OpenShift** 클러스터 및 자체 관리형 **NetApp** 스토리지

- Trident Protect를 사용하여 애플리케이션을 보호하고 온프레미스 클러스터 간의 마이그레이션을 지원하십시오.

시나리오 **1**

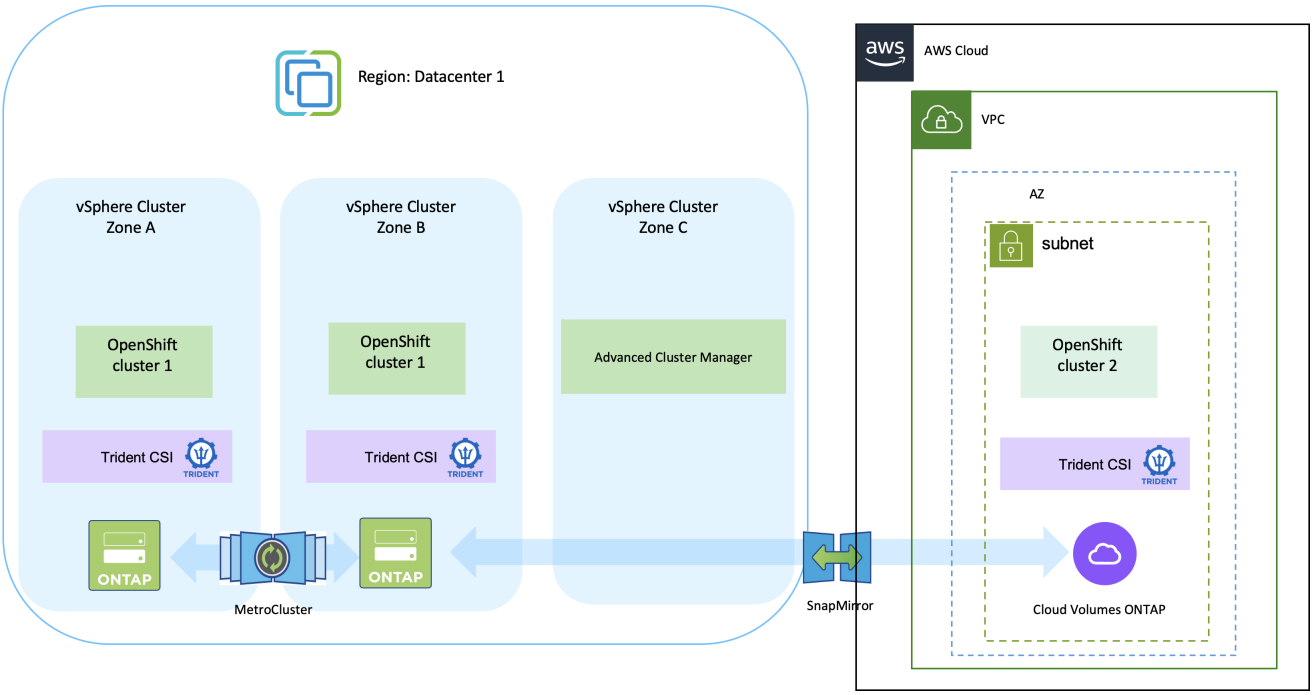


시나리오 **2: Trident Protect**를 사용하여 온프레미스 환경에서 **AWS** 환경으로의 데이터 보호 및 마이그레이션

온프레미스: 자체 관리형 **OpenShift** 클러스터 및 자체 관리형 스토리지 **AWS** 클라우드: 자체 관리형 **OpenShift** 클러스터 및 자체 관리형 스토리지

- Trident Protect를 사용하여 애플리케이션을 보호하고 온프레미스 클러스터와 AWS의 자체 관리형 OpenShift 클러스터 간의 마이그레이션을 지원하세요.

시나리오 **2**

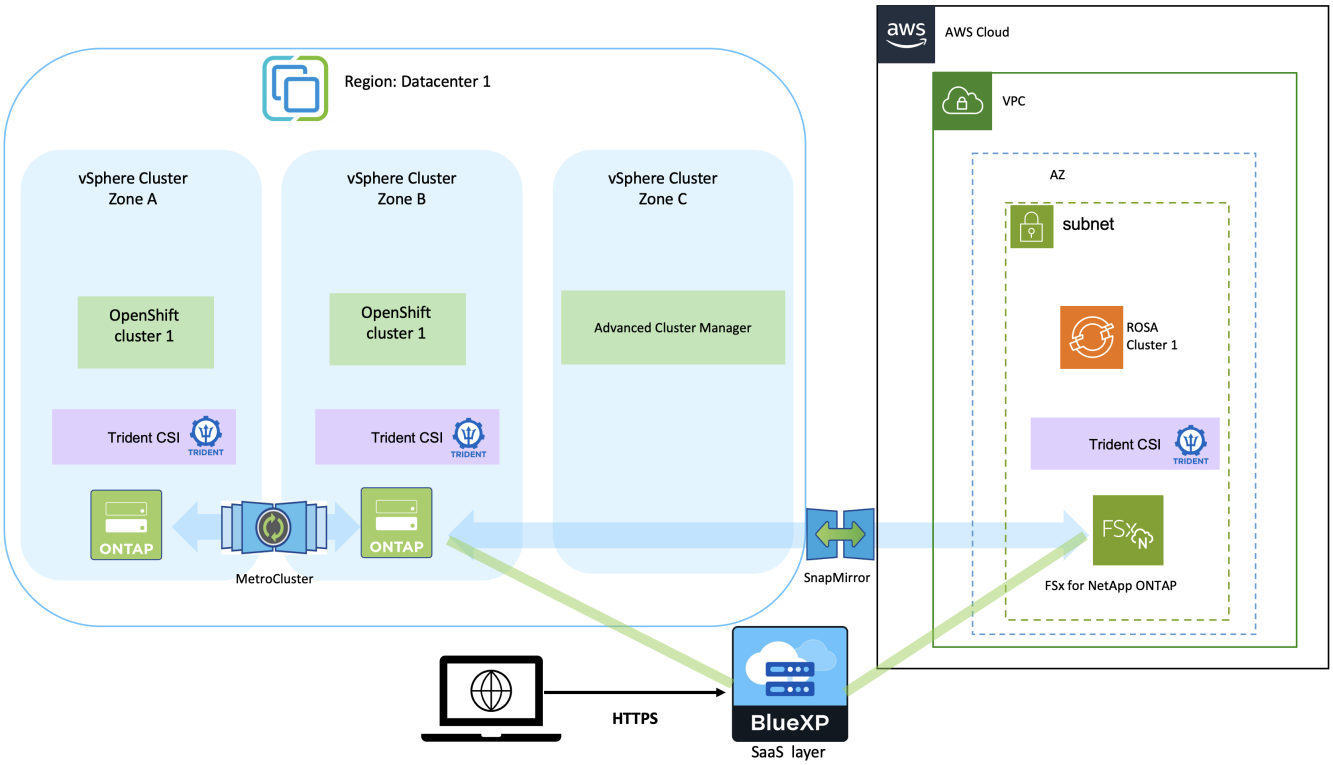


시나리오 **3:** 온프레미스 환경에서 **AWS** 환경으로의 데이터 보호 및 마이그레이션

온프레미스**:** 자체 관리형 **OpenShift** 클러스터 및 자체 관리형 스토리지 **AWS** 클라우드**:** 공급자 관리형 **OpenShift** 클러스터**(ROSA)** 및 공급자 관리형 스토리지**(FSx ONTAP)**

- NetApp Console을 사용하여 영구 볼륨(FSx ONTAP)의 복제를 수행합니다.
- OpenShift GitOps를 사용하여 애플리케이션 메타데이터를 다시 생성합니다.

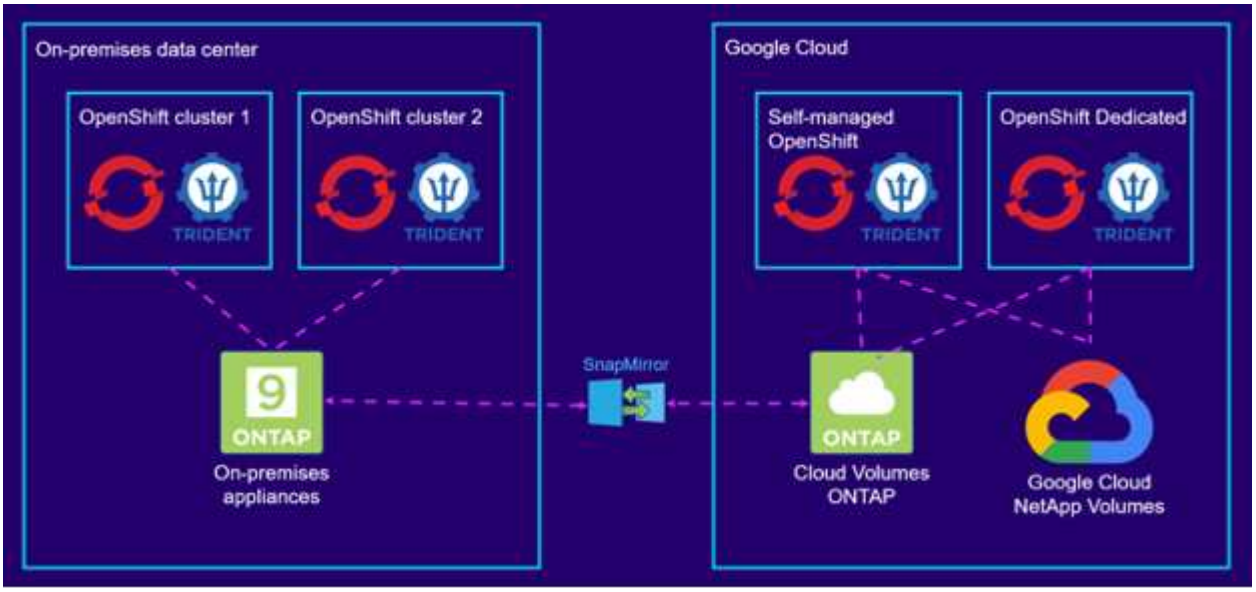
시나리오 **3**



시나리오 **4: Trident Protect**를 사용하여 온프레미스 환경에서 **GCP** 환경으로의 데이터 보호 및 마이그레이션

온프레미스: 자체 관리형 **OpenShift** 클러스터 및 자체 관리형 스토리지 **Google Cloud:** 자체 관리형 **OpenShift** 클러스터 및 자체 관리형 스토리지

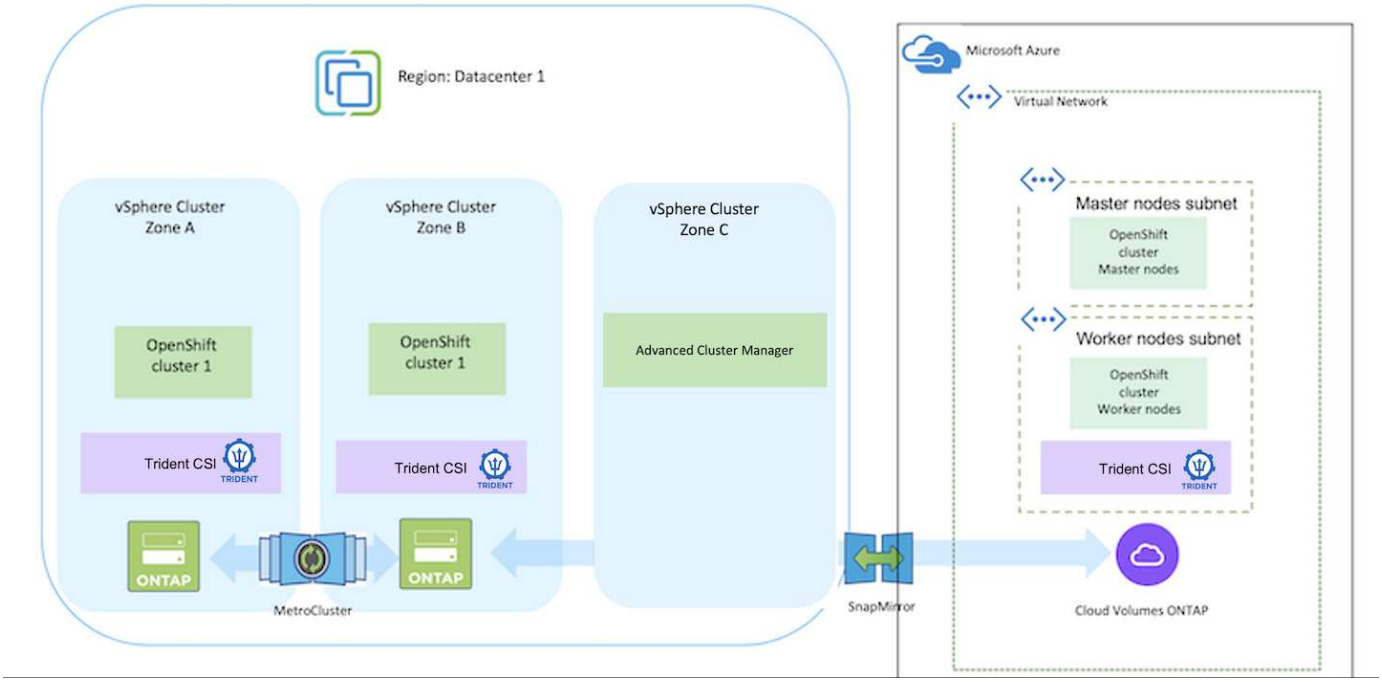
- Trident Protect를 사용하여 애플리케이션을 보호하고 온프레미스와 Google Cloud OpenShift 클러스터 간의 마이그레이션을 지원하세요.



MetroCluster 구성에서 ONTAP 사용할 때의 고려 사항은 다음을 참조하세요."여기" .

온프레미스**:** 자체 관리형 **OpenShift** 클러스터 및 자체 관리형 스토리지 **Azure Cloud:** 자체 관리형 **OpenShift** 클러스터 및 자체 관리형 스토리지

- Trident Protect를 사용하여 애플리케이션을 보호하고 온프레미스와 Azure의 OpenShift 클러스터 간의 마이그레이션을 지원하세요.



MetroCluster 구성에서 ONTAP 사용할 때의 고려 사항은 다음을 참조하세요."여기" .

솔루션 검증에 사용된 다양한 구성 요소의 버전

이 솔루션은 OpenShift 컨테이너 플랫폼, OpenShift Advanced Cluster Manager, NetApp ONTAP 및 NetApp Trident Protect를 사용하여 마이그레이션 및 중앙 집중식 데이터 보호를 테스트하고 검증합니다.

솔루션의 시나리오 1, 2, 3은 아래 표에 표시된 버전을 사용하여 검증되었습니다.

요소	버전
VM웨어	vSphere Client 버전 8.0.0.10200 VMware ESXi, 8.0.0, 20842819
허브 클러스터	오픈시프트 4.11.34
소스 및 대상 클러스터	온프레미스 및 AWS에서 OpenShift 4.12.9
* NetApp Trident*	Trident 서버 및 클라이언트 23.04.0
* NetApp Trident 프로텍트*	Trident 프로텍트 22.11.0-82
* NetApp ONTAP*	ONTAP 9.12.1
AWS FSx ONTAP	싱글 AZ

솔루션의 시나리오 4는 아래 표에 표시된 버전을 사용하여 검증되었습니다.

요소	버전
VM웨어	vSphere Client 버전 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
허브 클러스터	오픈시프트 4.13.13
소스 및 대상 클러스터	온프레미스 및 Google Cloud의 OpenShift 4.13.12
* NetApp Trident*	Trident 서버 및 클라이언트 23.07.0
* NetApp ONTAP*	ONTAP 9.12.1
* Cloud Volumes ONTAP*	단일 AZ, 단일 노드, 9.14.0

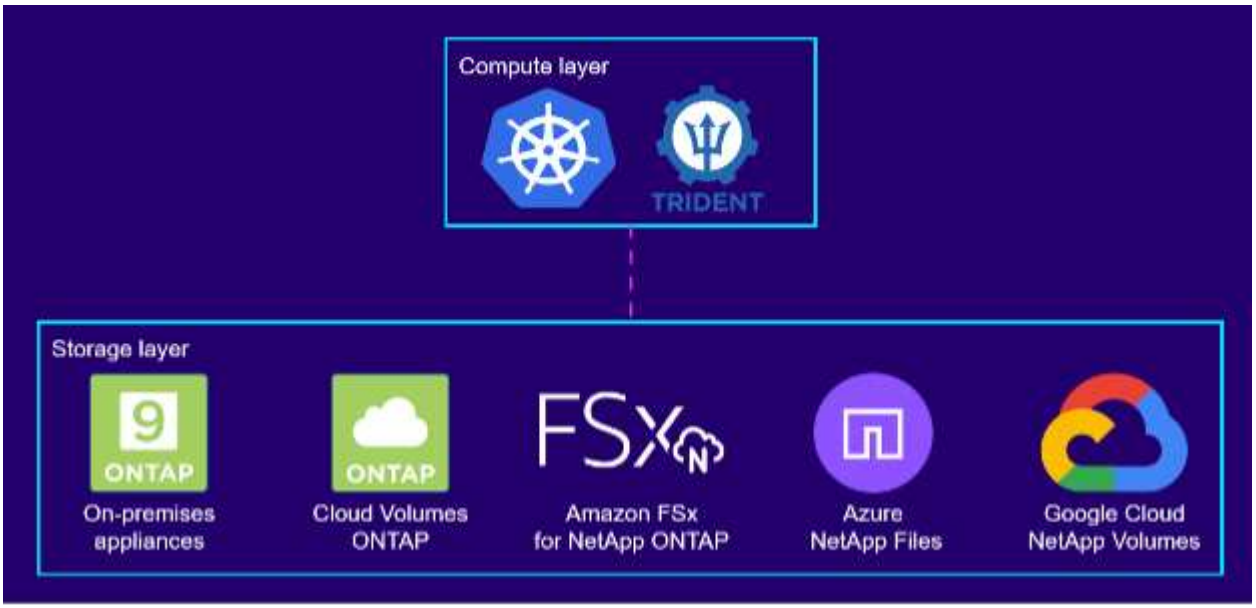
솔루션의 시나리오 5는 아래 표에 표시된 버전을 사용하여 검증되었습니다.

요소	버전
VM웨어	vSphere Client 버전 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
소스 및 대상 클러스터	온프레미스 및 Azure의 OpenShift 4.13.25
* NetApp Trident*	Trident Server 및 Client 23.10.0
* NetApp Trident 프로텍트*	Trident 프로텍트 23.10
* NetApp ONTAP*	ONTAP 9.12.1
* Cloud Volumes ONTAP*	단일 AZ, 단일 노드, 9.14.0

Red Hat OpenShift 컨테이너와 지원되는 **NetApp** 스토리지 통합

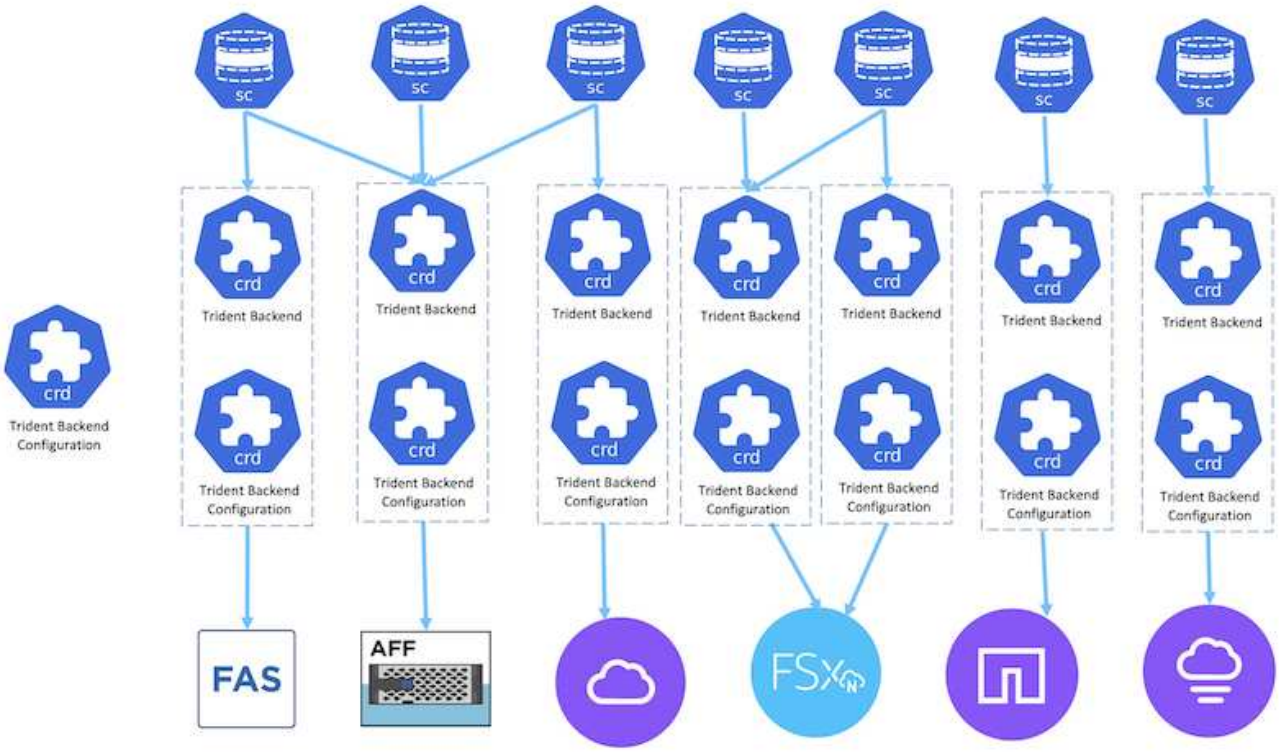
Red Hat OpenShift 컨테이너가 VMware에서 실행되든 하이퍼스케일러에서 실행되든 NetApp Trident 지원하는 다양한 유형의 백엔드 NetApp 스토리지에 대한 CSI 프로비저너로 사용될 수 있습니다.

다음 다이어그램은 NetApp Trident 사용하여 OpenShift 클러스터와 통합할 수 있는 다양한 백엔드 NetApp 스토리지를 보여줍니다.



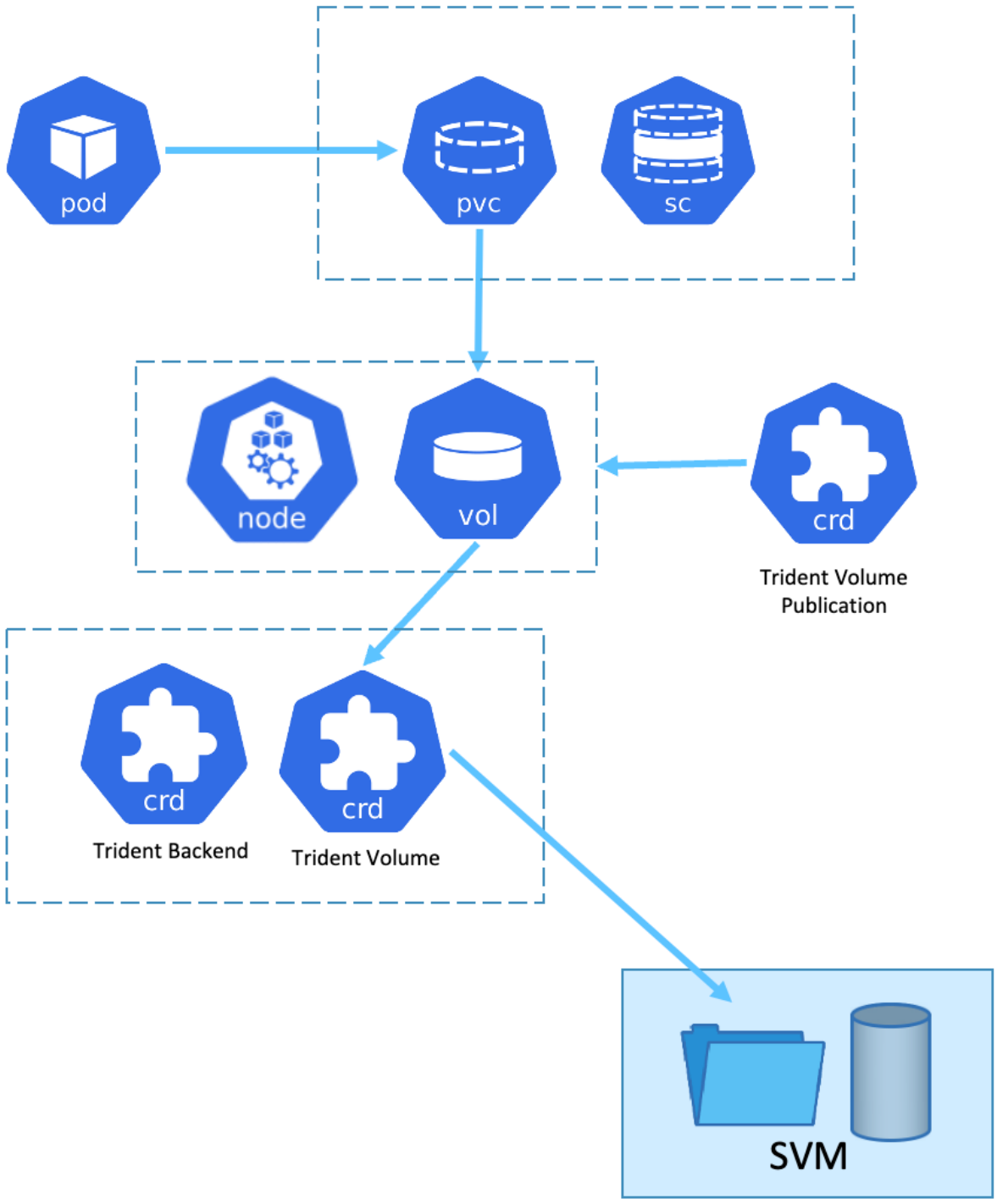
ONTAP 스토리지 가상 머신(SVM)은 안전한 멀티 테넌시를 제공합니다. 단일 OpenShift 클러스터는 단일 SVM이나 여러 SVM, 심지어 여러 ONTAP 클러스터에 연결할 수 있습니다. 저장소 클래스는 매개변수 또는 레이블을 기준으로 백엔드 저장소를 필터링합니다. 스토리지 관리자는 Trident 백엔드 구성을 사용하여 스토리지 시스템에 연결하기 위한 매개변수를 정의합니다. 연결이 성공적으로 설정되면 트라이던트 백엔드를 생성하고 스토리지 클래스가 필터링할 수 있는 정보를 채웁니다.

스토리지 클래스와 백엔드 간의 관계는 아래와 같습니다.



애플리케이션 소유자가 스토리지 클래스를 사용하여 영구 볼륨을 요청합니다. 스토리지 클래스는 백엔드 스토리지를 필터링합니다.

Pod와 백엔드 스토리지 간의 관계는 아래와 같습니다.



컨테이너 스토리지 인터페이스**(CSI)** 옵션

vSphere 환경에서 고객은 ONTAP 과 통합할 VMware CSI 드라이버 및/또는 Trident CSI를 선택할 수 있습니다. VMware CSI를 사용하면 영구 볼륨이 로컬 SCSI 디스크로 사용되는 반면, Trident 사용하면 네트워크로 사용됩니다.

VMware CSI는 ONTAP 에서 RWX 액세스 모드를 지원하지 않으므로, RWX 모드가 필요한 경우 애플리케이션은 Trident CSI를 사용해야 합니다. FC 기반 배포의 경우 VMware CSI가 선호되고 SnapMirror Business Continuity(SMBC)는 영역 수준의 고가용성을 제공합니다.

VMware CSI 지원

- 코어 블록 기반 데이터 저장소(FC, FCoE, iSCSI, NVMeoF)
- 코어 파일 기반 데이터 저장소(NFS v3, v4)
- vVol 데이터 저장소(블록 및 파일)

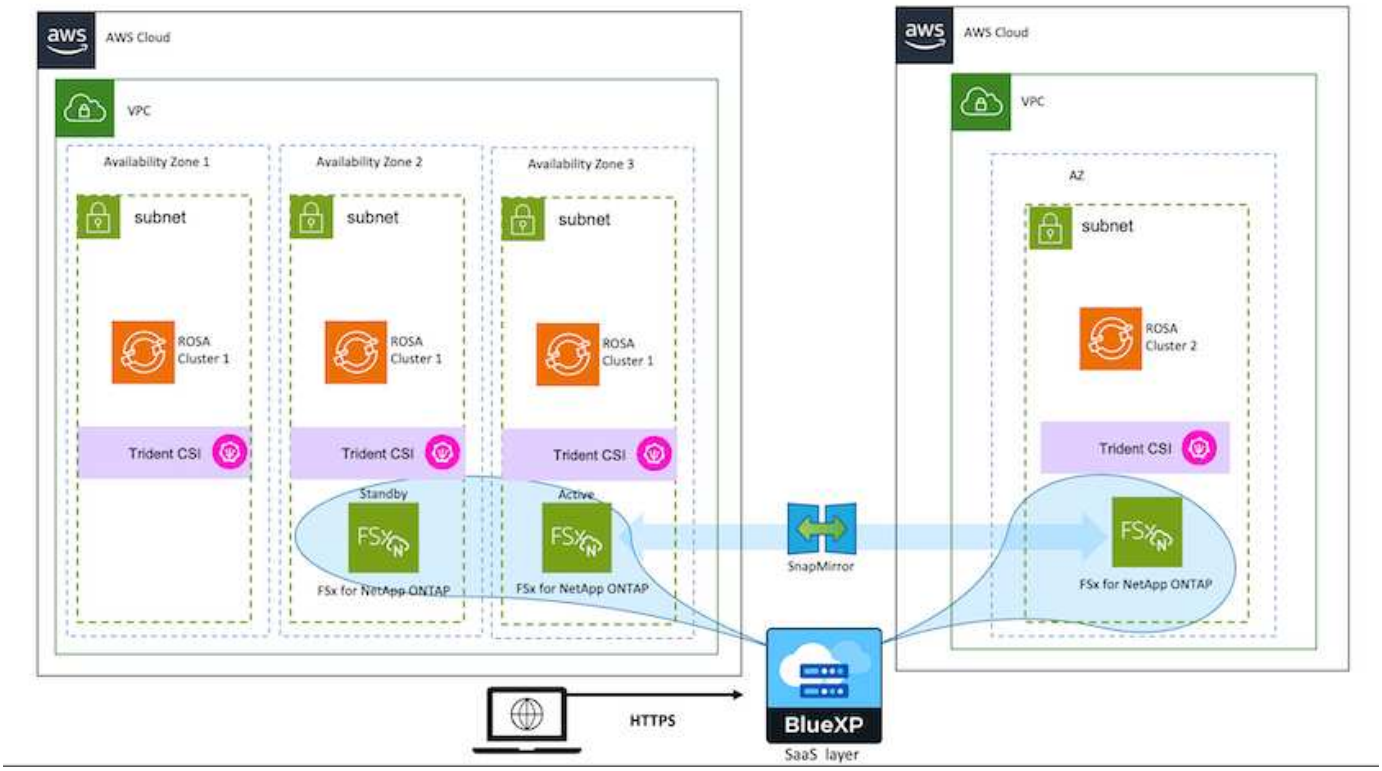
Trident ONTAP 지원하기 위해 다음과 같은 드라이버를 보유하고 있습니다.

- 온탑산(전용권)
- 온탭-샌-이코노미(공유 볼륨)
- ontap-nas(전용 볼륨)
- ontap-nas-economy(공유 볼륨)
- ontap-nas-flexgroup(전용 대규모 볼륨)

VMware CSI와 Trident CSI 모두에 대해 ONTAP NFS의 경우 nconnect, 세션 트렁킹, Kerberos 등을 지원하고 블록 프로토콜의 경우 다중 경로, CHAP 인증 등을 지원합니다.

AWS에서 Amazon FSx for NetApp ONTAP (FSx ONTAP)은 단일 가용 영역(AZ) 또는 다중 AZ에 배포될 수 있습니다. 높은 가용성이 필요한 프로덕션 워크로드의 경우, 다중 AZ는 영역 수준의 장애 허용성을 제공하고 단일 AZ에 비해 NVMe 읽기 캐시가 더 뛰어납니다. 자세한 내용은 다음을 확인하세요."AWS 성능 가이드라인" .

재해 복구 사이트의 비용을 절감하기 위해 단일 AZ FSx ONTAP 활용할 수 있습니다
.



FSx ONTAP 에서 지원하는 SVM 수에 대해서는 다음을 참조하세요."FSx ONTAP 스토리지 가상 머신 관리"

추가 문서

참고할 수 있는 추가 문서는 다음과 같습니다.

1. "VMware vSphere"
2. "OpenShift 컨테이너 플랫폼 제품 문서"
3. "OpenShift 컨테이너 플랫폼 클러스터 설치"
4. "고급 클러스터 관리 제품 설명서"
5. "ACM을 사용하여 클러스터 만들기"
6. "OpenShift에 Red Hat Quay 배포"
7. "Trident"
8. "ONTAP 9"
9. "NetApp 베르다" - Verda(오픈 소스)는 인기 있는 클라우드 네이티브 데이터 집약적 애플리케이션을 위한 참조 실행 후크 모음을 제공합니다
10. "NetApp 데이터 서비스"
11. "AWS 클래식 아키텍처 기반 Red Hat OpenShift 서비스"
12. "Amazon FSx ONTAP"
13. "GCP에 OpenShift 클러스터 설치"
14. "Azure에 OpenShift 클러스터 설치"

온프레미스용 **OpenShift**

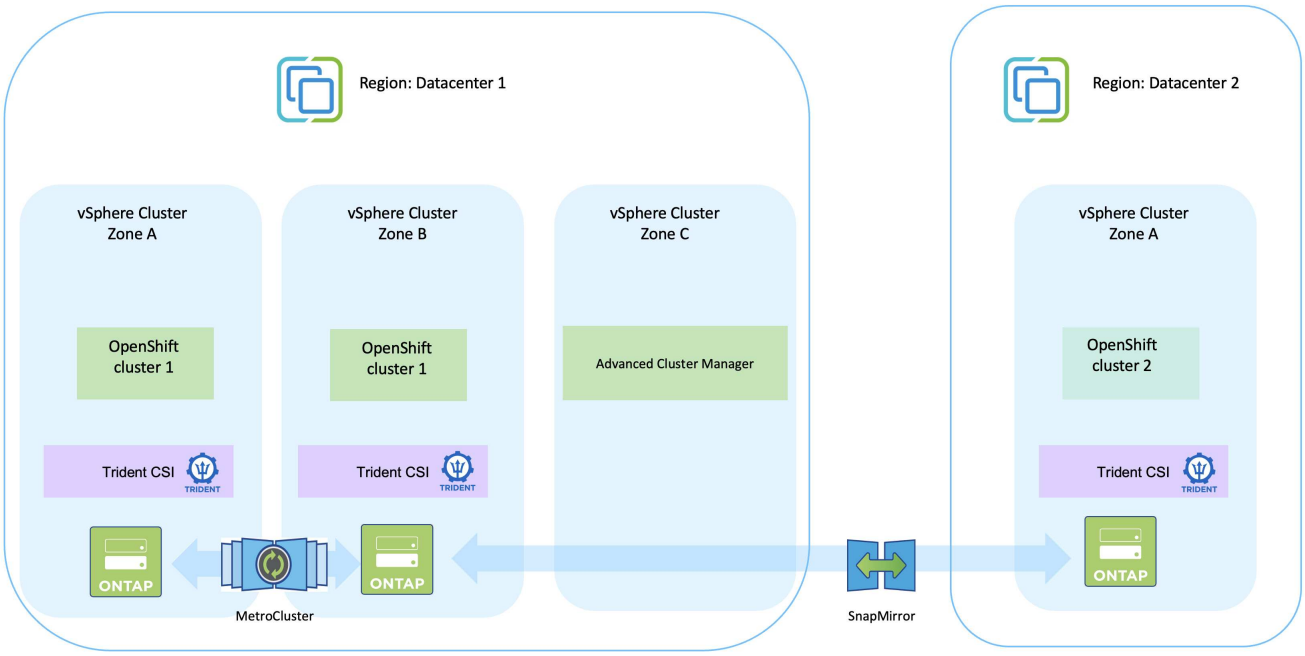
VMware에서 **Red Hat OpenShift Container** 플랫폼 워크로드를 지원하는 **NetApp** 솔루션

고객이 개인 데이터 센터의 인프라에서 최신 컨테이너화된 애플리케이션을 실행해야 하는 경우, 그렇게 할 수 있습니다. 컨테이너 워크로드를 배포하기 위한 성공적인 프로덕션 준비 환경을 조성하려면 Red Hat OpenShift 컨테이너 플랫폼(OCP)을 계획하고 배포해야 합니다. OCP 클러스터는 VMware나 베어 메탈에 배포할 수 있습니다.

NetApp ONTAP 스토리지는 컨테이너 배포에 필요한 데이터 보호, 안정성, 유연성을 제공합니다. Trident 고객의 상태 저장 애플리케이션을 위한 지속적인 ONTAP 스토리지를 사용하는 동적 스토리지 프로비저너 역할을 합니다. NetApp Trident Protect는 데이터 보호, 마이그레이션, 비즈니스 연속성 등 상태 저장 애플리케이션의 다양한 데이터 관리 요구 사항을 충족하는 데 사용할 수 있습니다.

VMware vSphere를 사용하면 NetApp ONTAP 도구에서 데이터 저장소를 프로비저닝하는 데 활용할 수 있는 vCenter 플러그인을 제공합니다. 태그를 적용하고 이를 OpenShift와 함께 사용하여 노드 구성과 데이터를 저장합니다. NVMe 기반 스토리지는 낮은 지연 시간과 높은 성능을 제공합니다.

Trident Protect를 사용한 **OpenShift Container** 워크로드를 위한 데이터 보호 및 마이그레이션 솔루션

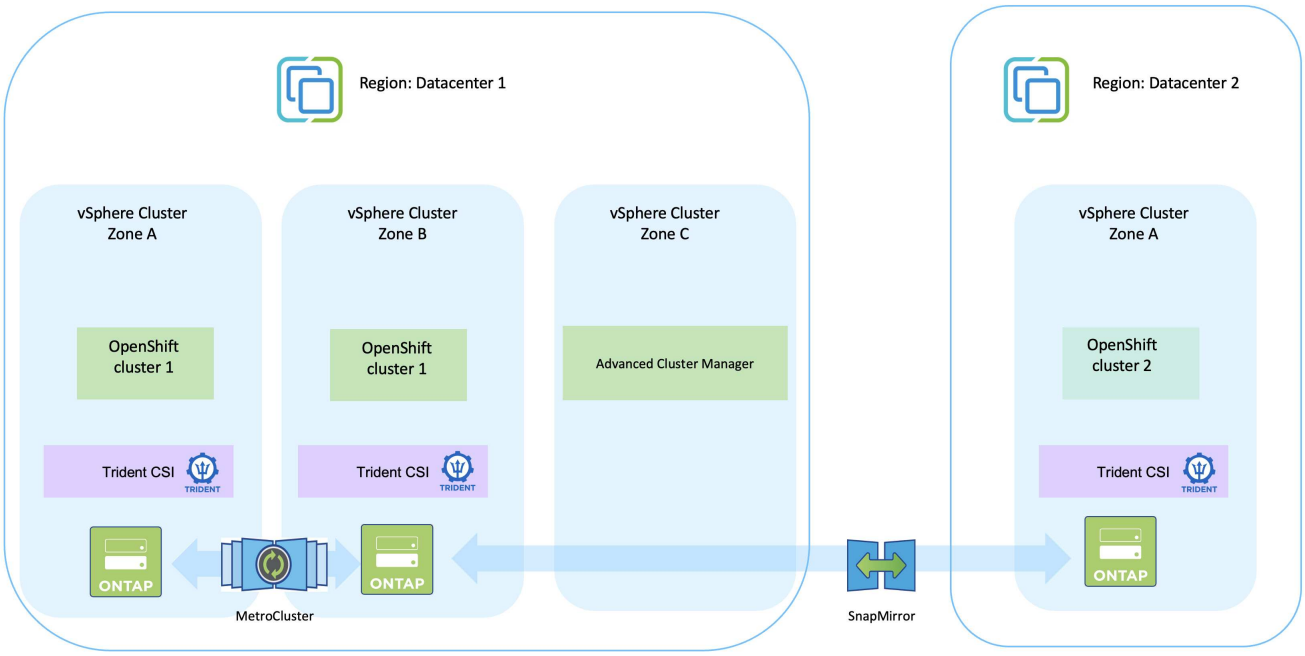


VMware에서 Red Hat OpenShift Container 플랫폼 배포 및 구성

이 섹션에서는 OpenShift 클러스터를 설정 및 관리하고 클러스터에서 상태 저장 애플리케이션을 관리하는 방법에 대한 고급 워크플로를 설명합니다. Trident 의 도움으로 NetApp ONTAP 스토리지 어레이를 사용하여 영구 볼륨을 제공하는 방법을 보여줍니다.

Red Hat OpenShift Container 플랫폼 클러스터를 배포하는 방법에는 여러 가지가 있습니다. 설정에 대한 이러한 간략한 설명은 사용된 특정 방법에 대한 문서 링크를 제공합니다. 제공된 관련 링크에서 다른 방법을 참조할 수 있습니다."리소스 섹션" .

다음은 데이터 센터의 VMware에 배포된 클러스터를 나타내는 다이어그램입니다.



설정 과정은 다음 단계로 나눌 수 있습니다.

▼ **CentOS VM** 배포 및 구성

- VMware vSphere 환경에 배포됩니다.
- 이 VM은 솔루션의 NetApp Trident 및 NetApp Trident Protect와 같은 일부 구성 요소를 배포하는 데 사용됩니다.
- 이 VM에는 설치 중에 루트 사용자가 구성됩니다.

▼ **VMware vSphere(Hub** 클러스터)에 **OpenShift Container Platform** 클러스터 배포 및 구성

OCP 클러스터를 배포하는 "지원 배치" 방법에 대한 지침을 참조하십시오.

다음 사항을 기억하세요. - 설치 프로그램에 제공할 ssh 공개 키와 개인 키를 생성하세요. 이러한 키는 필요한 경우 마스터 및 워커 노드에 로그인하는 데 사용됩니다. - 지원 설치 프로그램에서 설치 프로그램을 다운로드하세요. 이 프로그램은 마스터 및 워커 노드에 대해 VMware vSphere 환경에서 생성한 VM을 부팅하는 데 사용됩니다. - VM은 최소한의 CPU, 메모리, 하드 디스크 요구 사항을 가져야 합니다. (vm create 명령을 참조하세요."이것" (이 정보를 제공하는 마스터 및 워커 노드에 대한 페이지) - 모든 VM에서 diskUUID를 활성화해야 합니다. - 마스터용으로 최소 3개의 노드와 워커용으로 3개의 노드를 만듭니다. - 설치 프로그램에서 발견되면 VMware vSphere 통합 토글 버튼을 켭니다.

▼ 허브 클러스터에 고급 클러스터 관리 설치

이는 허브 클러스터의 고급 클러스터 관리 운영자를 사용하여 설치됩니다. 지침을 참조하세요"여기" .

▼ 두 개의 추가 **OCP** 클러스터(소스 및 대상)를 설치합니다.

- 추가 클러스터는 허브 클러스터의 ACM을 사용하여 배포할 수 있습니다.
- 지침을 참조하십시오 "여기".

▼ **NetApp ONTAP** 스토리지 구성

- VMWare 환경에서 OCP VM에 연결할 수 있는 ONTAP 클러스터를 설치합니다.
- SVM을 생성합니다.
- SVM의 저장소에 액세스하기 위해 NAS 데이터 lif를 구성합니다.

▼ **OCP** 클러스터에 **NetApp Trident** 설치

- 허브, 소스 및 대상 클러스터의 세 클러스터 모두에 NetApp Trident 설치합니다.
- 지침을 참조하십시오 "여기".
- ontap-nas에 대한 스토리지 백엔드를 만듭니다.
- ontap-nas에 대한 스토리지 클래스를 생성합니다.
- 지침을 참조하세요"여기" .

▼ 소스 클러스터에 애플리케이션 배포

OpenShift GitOps를 사용하여 애플리케이션을 배포합니다. (예: Postgres, Ghost)

다음 단계는 Trident Protect를 사용하여 데이터를 보호하고 소스 클러스터에서 대상 클러스터로 데이터를 마이그레이션하는 것입니다. 나타내다"여기" 지침을 보려면 클릭하세요.

Trident Protect를 사용한 데이터 보호

이 페이지는 Trident Protect를 사용하여 VMware vSphere에서 실행되는 Red Hat OpenShift 컨테이너 기반 애플리케이션의 데이터 보호 옵션을 보여줍니다.

사용자가 Red Hat OpenShift를 사용하여 애플리케이션을 현대화하는 과정에서 실수로 인한 삭제나 기타 인적 오류로부터 보호하기 위한 데이터 보호 전략을 수립해야 합니다. 또한 재해로부터 데이터를 보호하기 위해 규제 또는 규정 준수 목적상 보호 전략이 필요한 경우도 많습니다.

데이터 보호에 대한 요구 사항은 특정 시점의 복사본으로 되돌리는 것부터 인간의 개입 없이 다른 오류 도메인으로 자동으로 장애 조치하는 것까지 다양합니다. 많은 고객이 ONTAP Kubernetes 애플리케이션용 기본 스토리지 플랫폼으로 선택하는 이유는 멀티테넌시, 멀티 프로토콜, 고성능 및 대용량 제공, 다중 사이트 위치에 대한 복제 및 캐싱, 보안 및 유연성과 같은 풍부한 기능 때문입니다.

Trident Protect를 사용하여 컨테이너 워크로드를 보호하고 마이그레이션하는 방법에 대한 자세한 내용은 다음 섹션을 참조하십시오. - "Trident Protect를 사용하여 컨테이너 앱을 보호하고 마이그레이션하세요."

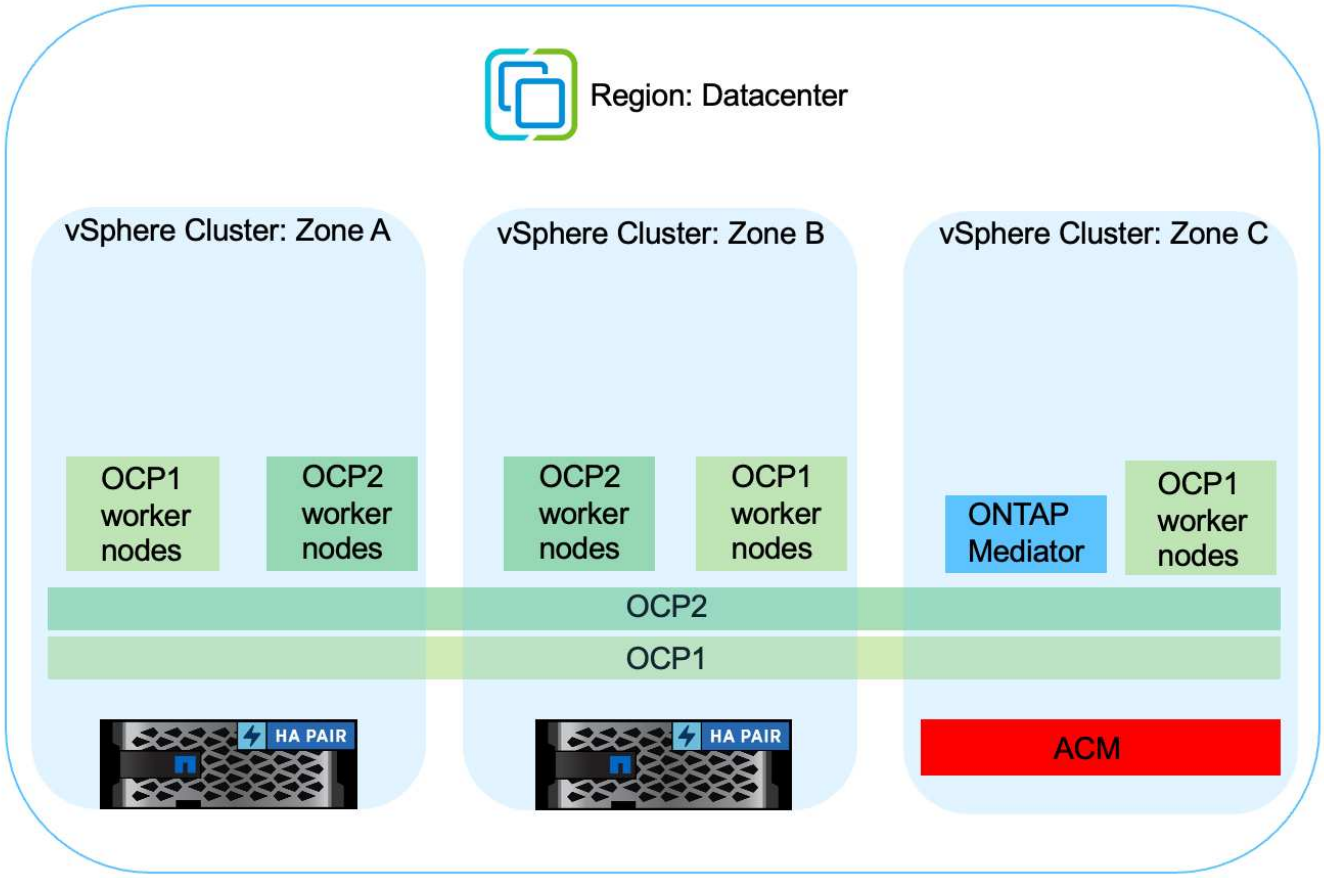
MetroCluster 통한 비즈니스 연속성

ONTAP 용 하드웨어 플랫폼의 대부분은 장치 장애로부터 보호하는 고가용성 기능을 갖추고 있어 재해 복구를 수행할 필요가 없습니다. 하지만 화재나 기타 재해로부터 보호하고 RPO가 0이고 RTO가 낮은 상태로 사업을 계속하려면 종종 MetroCluster 솔루션이 사용됩니다.

현재 ONTAP 시스템을 보유하고 있는 고객은 거리 제한 내에서 지원되는 ONTAP 시스템을 추가하여 MetroCluster 로 확장하여 영역 수준 재해 복구를 제공할 수 있습니다. CSI(컨테이너 스토리지 인터페이스)인 Trident MetroCluster 구성을 포함한 NetApp ONTAP 과 Cloud Volumes ONTAP, Azure NetApp Files, AWS FSx ONTAP 등의 다른 옵션을 지원합니다. Trident ONTAP 에 대한 5가지 스토리지 드라이버 옵션을 제공하며 모두 MetroCluster 구성에서 지원됩니다. 나타내다"여기" Trident 가 지원하는 ONTAP 스토리지 드라이버에 대한 추가 세부 정보를 확인하세요.

MetroCluster 솔루션에는 두 오류 도메인에서 동일한 네트워크 주소에 액세스할 수 있는 2계층 네트워크 확장 또는

기능이 필요합니다. MetroCluster 구성이 완료되면 MetroCluster SVM의 모든 볼륨이 보호되고 SyncMirror (RPO 0)의 이점을 얻을 수 있으므로 솔루션은 애플리케이션 소유자에게 투명하게 공개됩니다.



Trident 백엔드 구성(TBC)의 경우 MetroCluster 구성을 사용할 때 dataLIF 및 SVM을 지정하지 마세요. managementLIF에 대한 SVM 관리 IP를 지정하고 vsadmin 역할 자격 증명을 사용합니다.

Trident Protect 데이터 보호 기능에 대한 자세한 내용은 "여기"에서 확인할 수 있습니다.

자체 관리 구성 요소를 갖춘 하이브리드 클라우드

하이브리드 클라우드에서 **Red Hat OpenShift** 컨테이너 플랫폼 워크로드를 지원하는 **NetApp** 솔루션

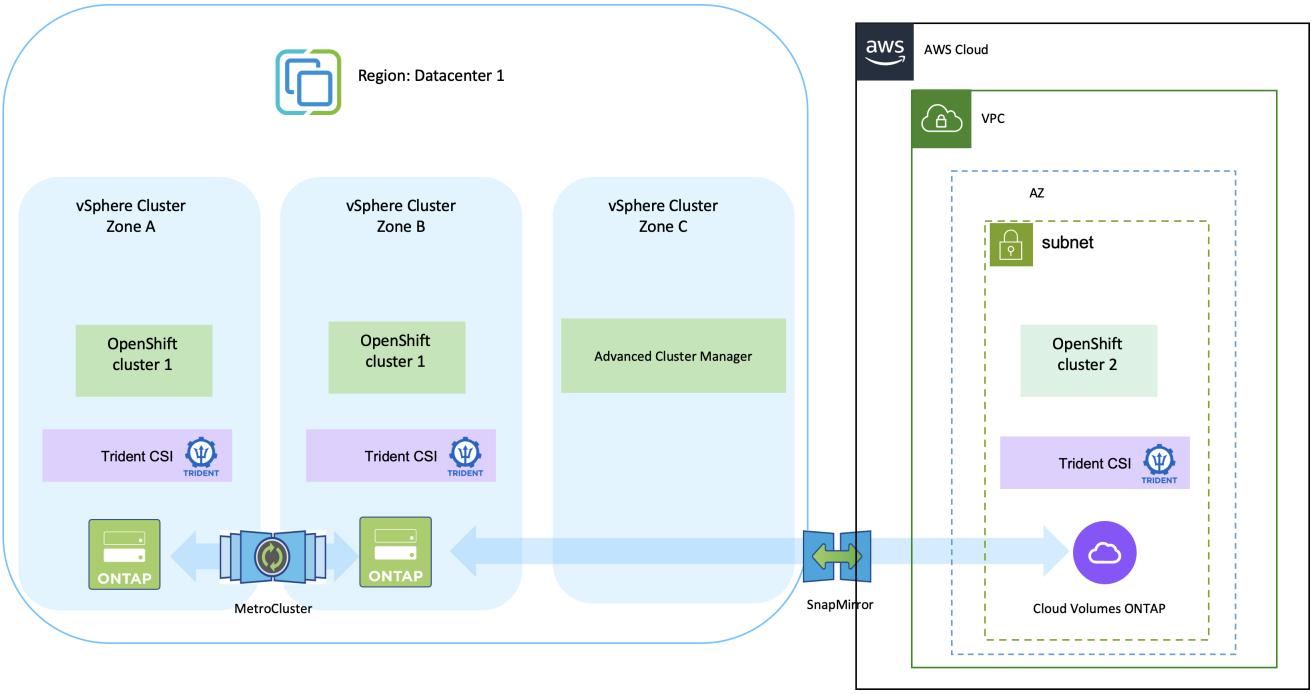
고객은 현대화 여정의 어느 시점에 이르러 일부 선택된 워크로드나 모든 워크로드를 데이터 센터에서 클라우드로 이전해야 할 수도 있습니다. 기업은 다양한 이유로 클라우드에서 자체 관리형 OpenShift 컨테이너와 자체 관리형 NetApp 스토리지를 사용하기로 선택할 수 있습니다. 데이터 센터에서 컨테이너 워크로드를 마이그레이션하기 위한 성공적인 프로덕션 준비 환경을 구축하려면 클라우드에서 Red Hat OpenShift 컨테이너 플랫폼(OCP)을 계획하고 배포해야 합니다. OCP 클러스터는 데이터 센터의 VMware 또는 Bare Metal에 배포할 수 있으며, 클라우드 환경의 AWS, Azure 또는 Google Cloud에 배포할 수 있습니다.

NetApp Cloud Volumes ONTAP 스토리지는 AWS, Azure 및 Google Cloud의 컨테이너 배포 환경에 데이터 보호, 안정성 및 유연성을 제공합니다. Trident는 고객의 상태 저장 애플리케이션에 필요한 영구 Cloud Volumes ONTAP

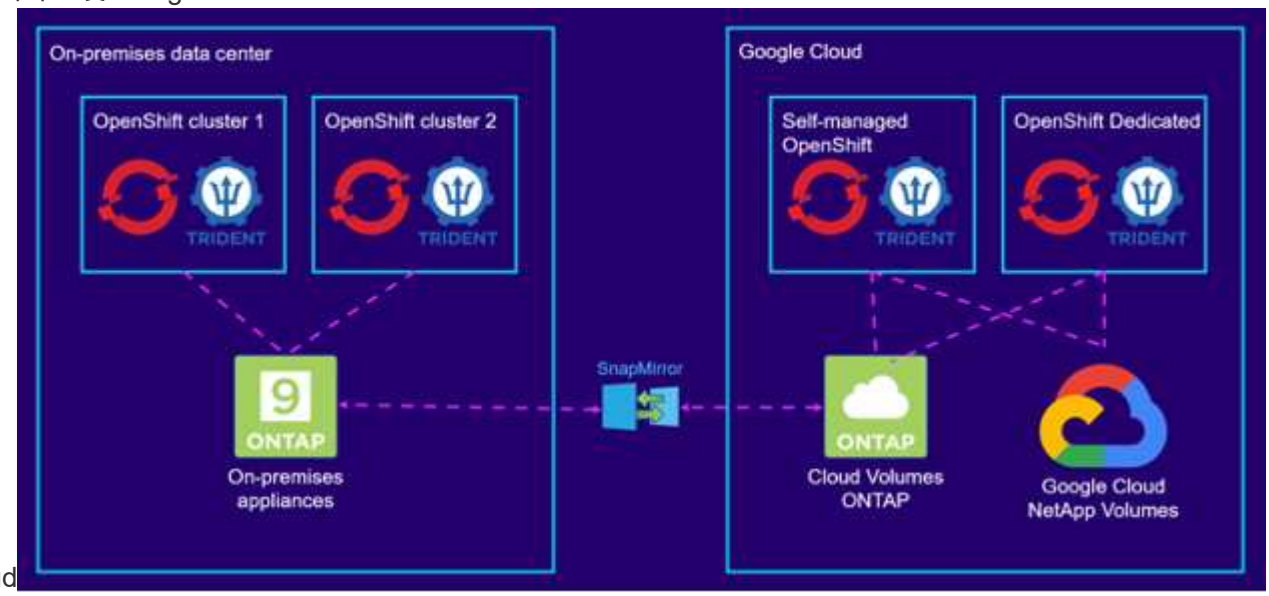
스토리지를 활용하는 동적 스토리지 프로비저너 역할을 합니다. Trident Protect는 데이터 보호, 마이그레이션 및 비즈니스 연속성과 같은 상태 저장 애플리케이션의 데이터 관리 요구 사항에 사용할 수 있습니다.

Trident Protect를 사용하여 하이브리드 클라우드에서 **OpenShift Container** 워크로드를 위한 데이터 보호 및 마이그레이션 솔루션

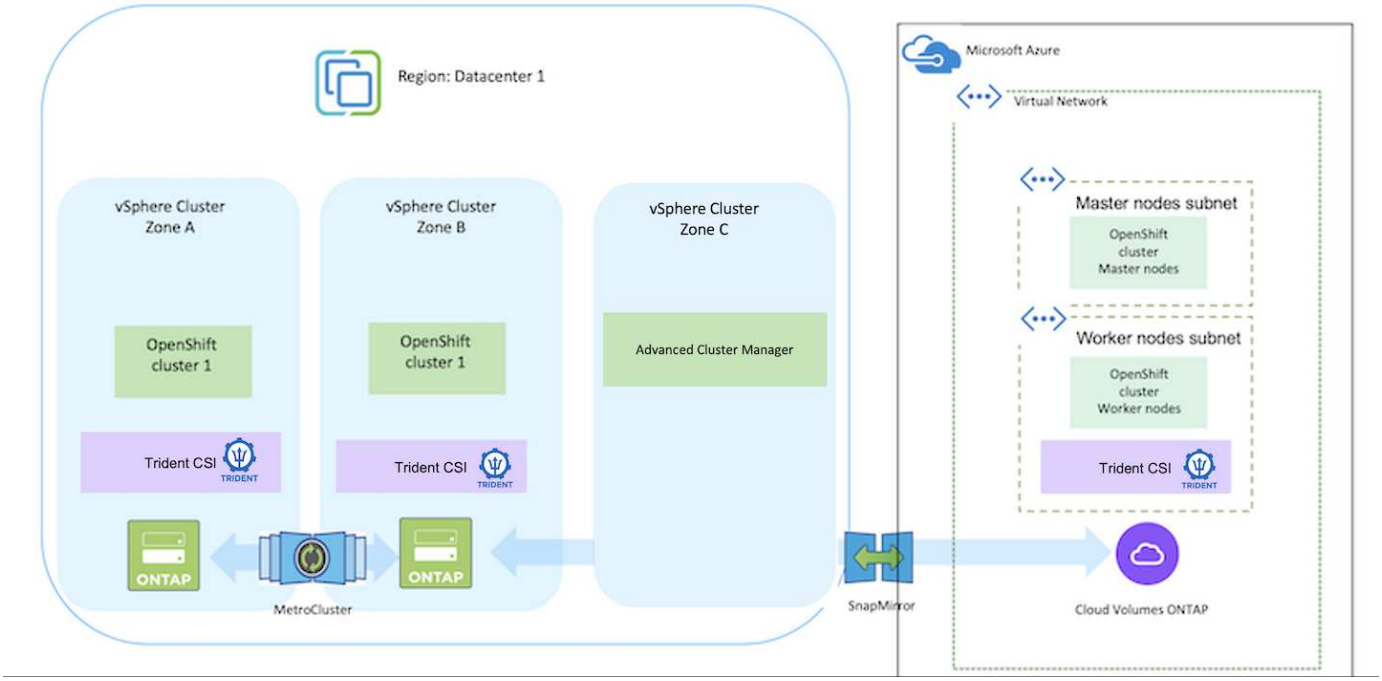
온프레미스 및
AWS



온프레미스 및 Google
Cloud



온프레미스 및 Azure
클라우드

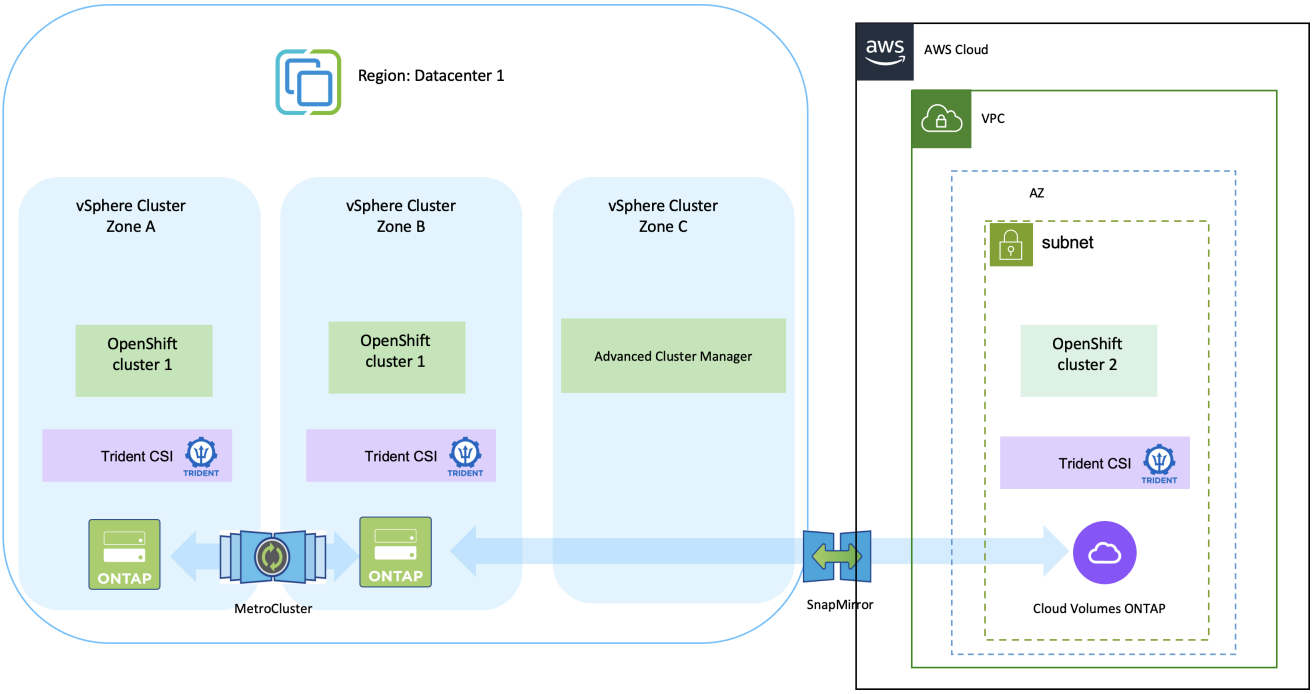


AWS에서 Red Hat OpenShift 컨테이너 플랫폼 배포 및 구성

이 섹션에서는 AWS에서 OpenShift 클러스터를 설정 및 관리하고, 여기에 상태 저장 애플리케이션을 배포하는 방법에 대한 개략적인 워크플로를 설명합니다. Trident 의 도움으로 NetApp Cloud Volumes ONTAP 스토리지를 사용하여 영구 볼륨을 제공하는 방법을 보여줍니다. 상태 저장 애플리케이션의 데이터 보호 및 마이그레이션 활동을 수행하기 위해 Trident Protect를 사용하는 방법에 대한 세부 정보가 제공됩니다.

AWS에 Red Hat OpenShift Container 플랫폼 클러스터를 배포하는 방법에는 여러 가지가 있습니다. 설정에 대한 이러한 간략한 설명은 사용된 특정 방법에 대한 문서 링크를 제공합니다. 제공된 관련 링크에서 다른 방법을 참조할 수 있습니다."리소스 섹션" .

다음은 VPN을 사용하여 AWS에 배포되고 데이터 센터에 연결된 클러스터를 나타내는 다이어그램입니다.



설정 과정은 다음 단계로 나눌 수 있습니다.

▼ **Advanced Cluster Management**에서 **AWS**에 **OCP** 클러스터를 설치합니다.

- 온프레미스 네트워크에 연결하기 위해 사이트 간 VPN 연결(pfsense 사용)이 있는 VPC를 만듭니다.
- 사내 네트워크에 인터넷 연결이 있습니다.
- 3개의 다른 AZ에 3개의 개인 서브넷을 만듭니다.
- VPC에 대한 Route 53 개인 호스팅 영역과 DNS 확인자를 만듭니다.

Advanced Cluster Management(ACM) 마법사에서 AWS에 OpenShift 클러스터를 생성하십시오. 지침 "여기"을 참조하십시오.

OpenShift 하이브리드 클라우드 콘솔에서 AWS에 클러스터를 생성할 수도 있습니다. 자세한 지침은 "여기"을(를) 참조하십시오.

ACM을 사용하여 클러스터를 생성할 때, 양식 보기에서 세부 정보를 입력한 후 yaml 파일을 편집하여 설치를 사용자 정의할 수 있습니다. 클러스터가 생성된 후에는 문제 해결이나 추가적인 수동 구성을 위해 클러스터 노드에 ssh 로그인할 수 있습니다. 설치 중에 제공한 ssh 키와 사용자 이름 core를 사용하여 로그인합니다.

▼ **NetApp Console**을 사용하여 **AWS**에 **Cloud Volumes ONTAP**을 배포합니다.

- 온프레미스 VMware 환경에 커넥터를 설치합니다. 지침을 참조하세요"여기" .
- 커넥터를 사용하여 AWS에 CVO 인스턴스를 배포합니다. 지침을 참조하세요"여기" .

커넥터는 클라우드 환경에도 설치될 수 있습니다. 나타내다"여기" 추가 정보를 원하시면.

▼ **OCP** 클러스터에 **Trident** 설치

- Helm을 사용하여 Trident Operator를 배포하십시오. 지침을 참조하십시오 "여기"
- 백엔드와 스토리지 클래스를 만듭니다. 지침을 참조하세요"여기" .

다중 구역 아키텍처를 위한 **Trident** 의 **CSI** 토폴로지 기능 사용

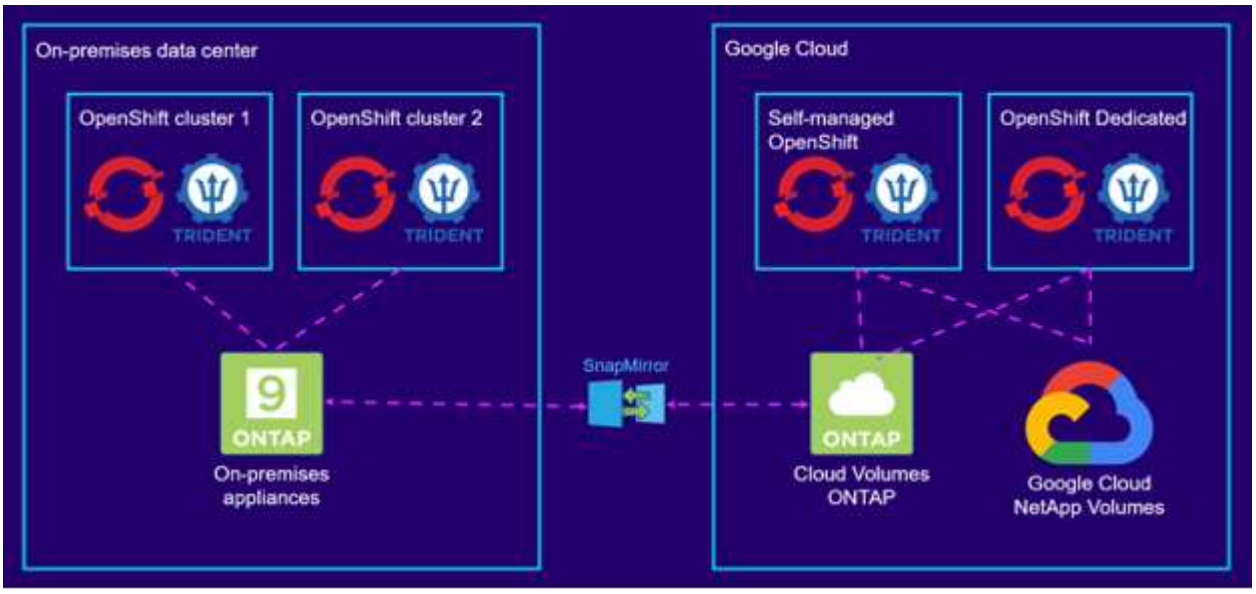
오늘날 클라우드 공급업체는 Kubernetes/OpenShift 클러스터 관리자가 영역 기반 클러스터 노드를 생성할 수 있도록 합니다. 노드는 한 지역 내의 여러 가용성 영역에 위치할 수도 있고, 여러 지역에 걸쳐 위치할 수도 있습니다. 다중 구역 아키텍처의 워크로드에 대한 볼륨 프로비저닝을 용이하게 하기 위해 Trident CSI 토폴로지를 사용합니다. CSI 토폴로지 기능을 사용하면 지역 및 가용성 영역을 기반으로 볼륨에 대한 액세스를 노드 하위 집합으로 제한할 수 있습니다. 나타내다"여기" 추가 세부 사항은 다음을 참조하세요.

Kubernetes는 두 가지 볼륨 바인딩 모드를 지원합니다. - ***VolumeBindingMode***_가 ***_Immediate*** (기본값)로 설정된 경우 Trident 토폴로지 인식 없이 볼륨을 생성합니다. 영구 볼륨은 요청하는 포드의 스케줄링 요구 사항에 대한 종속성 없이 생성됩니다. - ***VolumeBindingMode***_가 ***_WaitForFirstConsumer***로 설정된 경우 PVC에 대한 영구 볼륨의 생성 및 바인딩은 PVC를 사용하는 포드가 예약되고 생성될 때까지 지연됩니다. 이런 방식으로 토폴로지 요구 사항에 의해 적용되는 스케줄링 제약 조건을 충족하는 볼륨이 생성됩니다. Trident 스토리지 백엔드는 가용성 영역(토폴로지 인식 백엔드)을 기반으로 볼륨을 선택적으로 프로비저닝하도록 설계될 수 있습니다. 이러한 백엔드를 사용하는 StorageClass의 경우, 지원되는 지역/영역에서 예약된 애플리케이션에서 요청하는 경우에만 볼륨이 생성됩니다. (토폴로지 인식 StorageClass) 참조"여기" 추가 세부 사항은 다음을 참조하세요.

Google Cloud에서 Red Hat OpenShift Container Platform 배포 및 구성

이 섹션에서는 GCP에서 OpenShift 클러스터를 설정 및 관리하고 여기에 상태 저장 애플리케이션을 배포하는 방법에 대한 개략적인 워크플로를 설명합니다. Trident 의 도움을 받아 Google Cloud NetApp Volumes 및 NetApp Cloud Volumes ONTAP 스토리지를 사용하여 영구 볼륨을 제공하는 방법을 보여줍니다.

다음은 GCP에 배포되고 VPN을 사용하여 데이터 센터에 연결된 클러스터를 보여주는 다이어그램입니다.



GCP에 Red Hat OpenShift Container 플랫폼 클러스터를 배포하는 방법에는 여러 가지가 있습니다. 설정에 대한 이러한 간략한 설명은 사용된 특정 방법에 대한 문서 링크를 제공합니다. 제공된 관련 링크에서 다른 방법을 참조할 수 있습니다."리소스 섹션" .

설정 과정은 다음 단계로 나눌 수 있습니다.

CLI에서 **GCP**에 **OCP** 클러스터 설치

- "여기"에 명시된 모든 필수 조건을 충족했는지 확인하십시오.
- 온프레미스와 GCP 간의 VPN 연결을 위해 pfsense VM을 생성하고 구성했습니다. 지침은 다음을 참조하세요. "여기" .
  - pfsense의 원격 게이트웨이 주소는 Google Cloud Platform에서 VPN 게이트웨이를 생성한 후에만 구성할 수 있습니다.
  - 2단계의 원격 네트워크 IP 주소는 OpenShift 클러스터 설치 프로그램을 실행하고 클러스터의 인프라 구성 요소를 만든 후에만 구성할 수 있습니다.
  - Google Cloud의 VPN은 설치 프로그램을 통해 클러스터의 인프라 구성 요소가 생성된 후에만 구성할 수 있습니다.
- 이제 GCP에 OpenShift 클러스터를 설치합니다.
  - 설치 프로그램과 풀 시크릿을 얻은 후, 설명서에 제공된 단계에 따라 클러스터를 배포하십시오 "여기".
  - 설치하면 Google Cloud Platform에 VPC 네트워크가 생성됩니다. 또한 Cloud DNS에 개인 영역을 만들고 A 레코드를 추가합니다.
    - VPC 네트워크의 CIDR 블록 주소를 사용하여 pfsense를 구성하고 VPN 연결을 설정합니다. 방화벽이 올바르게 설정되었는지 확인하세요.
    - Google Cloud DNS의 A 레코드에 있는 IP 주소를 사용하여 온프레미스 환경의 DNS에 A 레코드를 추가합니다.
  - 클러스터 설치가 완료되고 kubeconfig 파일과 클러스터 콘솔에 로그인할 수 있는 사용자 이름과 비밀번호가 제공됩니다.

Google Cloud NetApp Volumes 배포

- Google Cloud NetApp Volumes 설명된 대로 프로젝트에 추가할 수 있습니다."여기" .

NetApp Console을 사용하여 **GCP**에 **Cloud Volumes ONTAP** 배포

- Google Cloud에 콘솔 에이전트를 설치하십시오. 지침을 참조하십시오 "여기".
- 에이전트를 사용하여 Google Cloud에 CVO 인스턴스를 배포합니다. 지침을 참조하십시오 "여기".

GCP의 **OCP** 클러스터에 **Trident** 설치

- 그림과 같이 Trident를 배포하는 방법은 여러 가지가 있습니다 "여기".
- 이 프로젝트에서는 지침 "여기"을 사용하여 Trident Operator를 수동으로 배포함으로써 Trident를 설치했습니다.
- 백엔드와 스토리지 클래스를 생성합니다. 지침을 참조하세요"여기" .

다중 구역 아키텍처를 위한 **Trident** 의 **CSI** 토폴로지 기능 사용

오늘날 클라우드 공급업체는 Kubernetes/OpenShift 클러스터 관리자가 영역 기반 클러스터 노드를 생성할 수 있도록 합니다. 노드는 한 지역 내의 여러 가용성 영역에 위치할 수도 있고, 여러 지역에 걸쳐 위치할 수도 있습니다. 다중 구역 아키텍처의 워크로드에 대한 볼륨 프로비저닝을 용이하게 하기 위해 Trident CSI 토폴로지를 사용합니다. CSI 토폴로지 기능을 사용하면 지역 및 가용성 영역을 기반으로 볼륨에 대한 액세스를 노드 하위 집합으로 제한할 수 있습니다. 나타내다"여기" 추가 세부 사항은 다음을 참조하세요.

Kubernetes는 두 가지 볼륨 바인딩 모드를 지원합니다. - ***VolumeBindingMode***_가 ***_Immediate*** (기본값)로 설정된 경우 Trident 토폴로지 인식 없이 볼륨을 생성합니다. 영구 볼륨은 요청하는 포드의

스케줄링 요구 사항에 대한 종속성 없이 생성됩니다. - ***VolumeBindingMode***_가 ***_WaitForFirstConsumer***로 설정된 경우 PVC에 대한 영구 볼륨의 생성 및 바인딩은 PVC를 사용하는 포드가 예약되고 생성될 때까지 지연됩니다. 이런 방식으로 토폴로지 요구 사항에 의해 적용되는 스케줄링 제약 조건을 충족하는 볼륨이 생성됩니다. Trident 스토리지 백엔드는 가용성 영역(토폴로지 인식 백엔드)을 기반으로 볼륨을 선택적으로 프로비저닝하도록 설계될 수 있습니다. 이러한 백엔드를 사용하는 StorageClass의 경우, 지원되는 지역/영역에서 예약된 애플리케이션에서 요청하는 경우에만 볼륨이 생성됩니다. (토폴로지 인식 StorageClass) 참조"여기" 추가 세부 사항은 다음을 참조하세요.

데모 영상

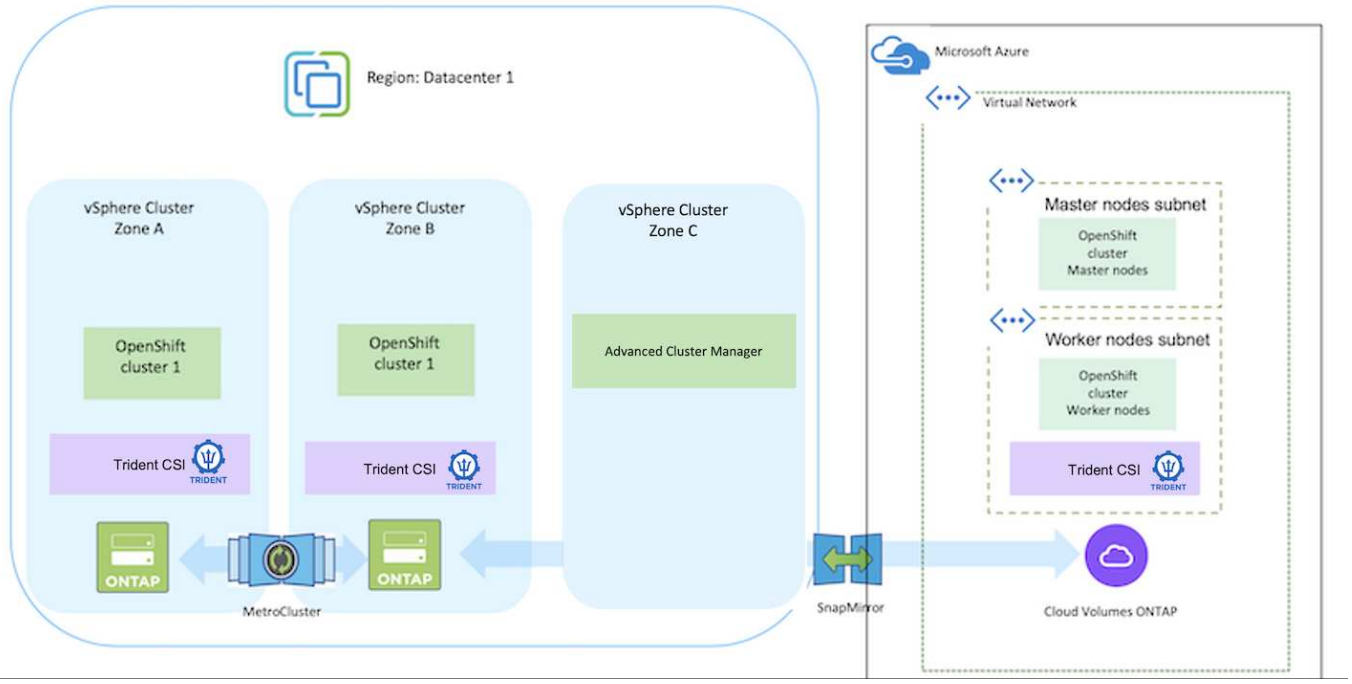
Google Cloud Platform에 OpenShift 클러스터 설치

Trident Protect로 OpenShift 클러스터 가져오기

Azure에서 Red Hat OpenShift 컨테이너 플랫폼 배포 및 구성

이 섹션에서는 Azure에서 OpenShift 클러스터를 설정 및 관리하고 여기에 상태 저장 애플리케이션을 배포하는 방법에 대한 개략적인 워크플로를 설명합니다. Trident 의 도움으로 NetApp Cloud Volumes ONTAP 스토리지를 사용하여 영구 볼륨을 제공하는 방법을 보여줍니다. 상태 저장 애플리케이션의 데이터 보호 및 마이그레이션 활동을 수행하기 위해 Trident Protect를 사용하는 방법에 대한 세부 정보가 제공됩니다.

다음은 VPN을 사용하여 Azure에 배포되고 데이터 센터에 연결된 클러스터를 보여주는 다이어그램입니다.



Azure에 Red Hat OpenShift Container 플랫폼 클러스터를 배포하는 방법에는 여러 가지가 있습니다. 설정에 대한 이러한 간략한 설명은 사용된 특정 방법에 대한 문서 링크를 제공합니다. 제공된 관련 링크에서 다른 방법을 참조할 수 있습니다."리소스 섹션" .

설정 과정은 다음 단계로 나눌 수 있습니다.

▼ **CLI**에서 **Azure**에 **OCP** 클러스터를 설치합니다.

- "여기"에 명시된 모든 필수 조건을 충족했는지 확인하십시오.
- VPN, 서브넷, 네트워크 보안 그룹, 개인 DNS 영역을 만듭니다. VPN 게이트웨이와 사이트 간 VPN 연결을 생성합니다.
- 온프레미스와 Azure 간의 VPN 연결을 위해 pfsense VM을 생성하고 구성했습니다. 지침은 다음을 참조하세요. "여기" .
- 설치 프로그램과 풀 시크릿을 확보하고 설명서에 제공된 단계에 따라 클러스터를 배포하십시오 "여기".
- 클러스터 설치가 완료되고 kubeconfig 파일과 클러스터 콘솔에 로그인할 수 있는 사용자 이름과 비밀번호가 제공됩니다.

install-config.yaml 파일의 샘플은 아래와 같습니다.

```
apiVersion: v1
baseDomain: sddc.netapp.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 512
        diskType: "StandardSSD_LRS"
      type: Standard_D2s_v3
      ultraSSDCapability: Disabled
      #zones:
      #- "1"
      #- "2"
      #- "3"
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 1024
        diskType: Premium_LRS
      type: Standard_D8s_v3
      ultraSSDCapability: Disabled
  replicas: 3
metadata:
```

```
  creationTimestamp: null
  name: azure-cluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    baseDomainResourceGroupName: ocp-base-domain-rg
    cloudName: AzurePublicCloud
    computeSubnet: ocp-subnet2
    controlPlaneSubnet: ocp-subnet1
    defaultMachinePlatform:
      osDisk:
        diskSizeGB: 1024
        diskType: "StandardSSD_LRS"
      ultraSSDCapability: Disabled
    networkResourceGroupName: ocp-nc-us-rg
    #outboundType: UserDefinedRouting
    region: northcentralus
    resourceGroupName: ocp-cluster-ncusrg
    virtualNetwork: ocp_vnet_ncus
publish: Internal
pullSecret:
```

▼ **NetApp** 콘솔을 사용하여 **Azure**에 **Cloud Volumes ONTAP**을 배포합니다**.**

- Azure에 NetApp Console 에이전트를 설치합니다. 지침을 참조하십시오 "여기".
- 에이전트를 사용하여 Azure에 CVO 인스턴스를 배포합니다. 지침을 참조하십시오"여기".

다중 구역 아키텍처를 위한 **Trident** 의 **CSI** 토폴로지 기능 사용

오늘날 클라우드 공급업체는 Kubernetes/OpenShift 클러스터 관리자가 영역 기반 클러스터 노드를 생성할 수 있도록 합니다. 노드는 한 지역 내의 여러 가용성 영역에 위치할 수도 있고, 여러 지역에 걸쳐 위치할 수도 있습니다. 다중 구역 아키텍처의 워크로드에 대한 볼륨 프로비저닝을 용이하게 하기 위해 Trident CSI 토폴로지를 사용합니다. CSI 토폴로지 기능을 사용하면 지역 및 가용성 영역을 기반으로 볼륨에 대한 액세스를 노드 하위 집합으로 제한할 수 있습니다. 나타내다"여기" 추가 세부 사항은 다음을 참조하세요.

Kubernetes는 두 가지 볼륨 바인딩 모드를 지원합니다. - ***VolumeBindingMode***_가 ***_Immediate*** (기본값)로 설정된 경우 Trident 토폴로지 인식 없이 볼륨을 생성합니다. 영구 볼륨은 요청하는 포드의 스케줄링 요구 사항에 대한 종속성 없이 생성됩니다. - ***VolumeBindingMode***_가 ***_WaitForFirstConsumer***로 설정된 경우 PVC에 대한 영구 볼륨의 생성 및 바인딩은 PVC를 사용하는 포드가 예약되고 생성될 때까지 지연됩니다. 이런 방식으로 토폴로지 요구 사항에 의해 적용되는 스케줄링 제약 조건을 충족하는 볼륨이 생성됩니다. Trident 스토리지 백엔드는 가용성 영역(토폴로지

인식 백엔드)을 기반으로 볼륨을 선택적으로 프로비저닝하도록 설계될 수 있습니다. 이러한 백엔드를 사용하는 StorageClass의 경우, 지원되는 지역/영역에서 예약된 애플리케이션에서 요청하는 경우에만 볼륨이 생성됩니다. (토폴로지 인식 StorageClass) 참조"여기" 추가 세부 사항은 다음을 참조하세요.

Trident Protect를 사용한 데이터 보호

Trident Protect를 사용하여 컨테이너 워크로드를 보호하고 마이그레이션하는 방법에 대한 자세한 내용은 다음 섹션을 참조하십시오. - "Trident Protect를 사용하여 컨테이너 앱을 보호하고 마이그레이션하세요."

공급자 관리 구성 요소를 갖춘 하이브리드 클라우드

관리형 **Red Hat OpenShift** 컨테이너 플랫폼 워크로드를 갖춘 **NetApp** 솔루션

고객은 "클라우드에서 태어났을 수도 있고", 현대화 여정의 어느 시점에 데이터 센터에서 일부 선택된 워크로드나 모든 워크로드를 클라우드로 옮길 준비가 되었을 수도 있습니다. 이들은 워크로드를 실행하기 위해 클라우드에서 공급자가 관리하는 OpenShift 컨테이너와 공급자가 관리하는 NetApp 스토리지를 사용하기로 선택할 수 있습니다. 컨테이너 워크로드를 위한 성공적인 프로덕션 준비 환경을 구축하려면 클라우드에서 관리형 Red Hat OpenShift 컨테이너 클러스터를 계획하고 배포해야 합니다. NetApp 3대 퍼블릭 클라우드에서 관리형 Red Hat 솔루션을 위한 완전 관리형 스토리지 제품을 제공합니다.

- Amazon FSx for NetApp ONTAP (FSx ONTAP)*

FSx ONTAP AWS에서 컨테이너를 배포할 때 데이터 보호, 안정성, 유연성을 제공합니다. Trident 고객의 상태 저장 애플리케이션을 위한 영구 FSx ONTAP 스토리지를 사용하는 동적 스토리지 프로비저너 역할을 합니다.

ROSA는 여러 가용성 영역에 걸쳐 제어 평면 노드를 분산하여 HA 모드로 배포할 수 있는 반면, FSx ONTAP 도 다중 AZ 옵션으로 프로비저닝하여 높은 가용성을 제공하고 AZ 장애로부터 보호할 수 있습니다.

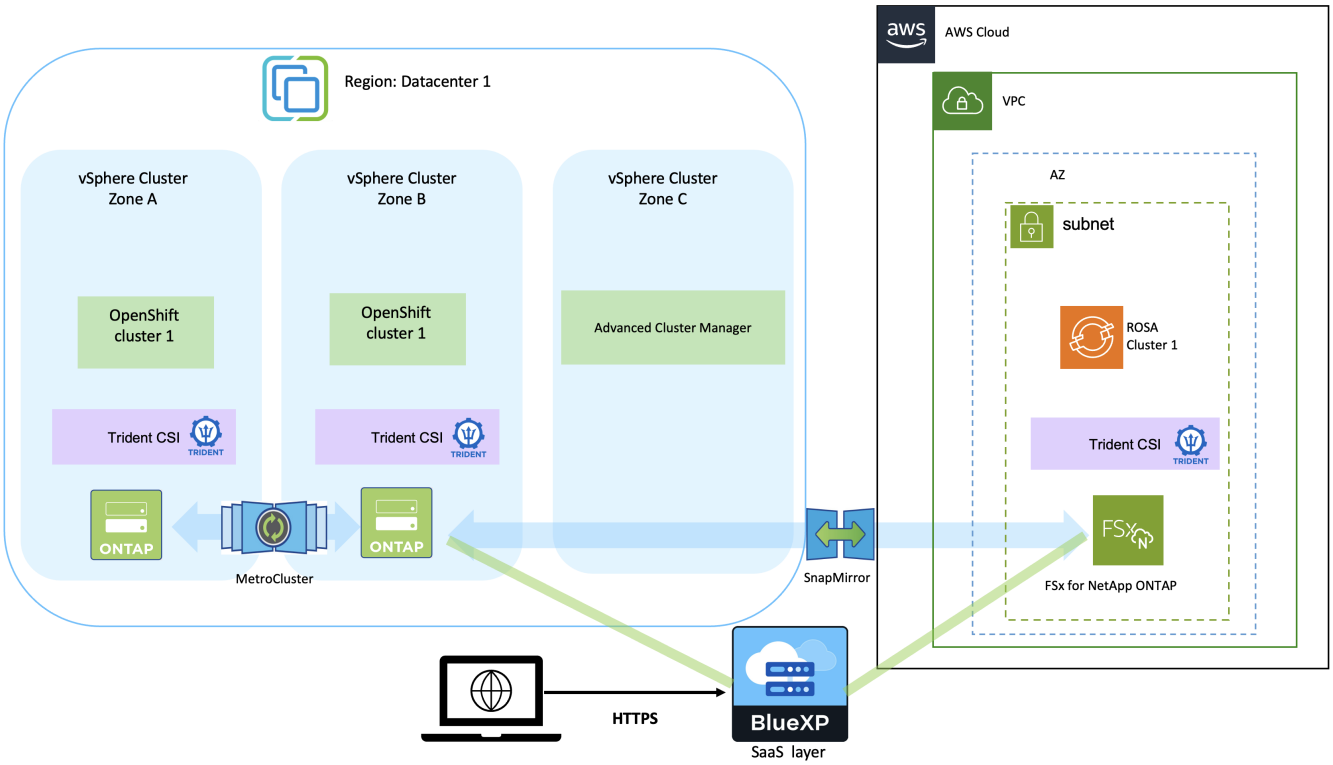
- Google Cloud NetApp Volumes*

Red Hat OpenShift Dedicated는 하이브리드 클라우드 전반에서 애플리케이션을 신속하게 구축, 배포 및 확장할 수 있는 완전 관리형 애플리케이션 플랫폼입니다. Google Cloud NetApp Volumes ONTAP의 엔터프라이즈 데이터 관리 기능 전체를 Google Cloud의 OpenShift 배포에 적용하는 영구 볼륨을 제공합니다.

AWS에서 관리형 **Red Hat OpenShift** 컨테이너 플랫폼 배포 및 구성

이 섹션에서는 AWS(ROSA)에서 관리형 Red Hat OpenShift 클러스터를 설정하는 개략적인 워크플로를 설명합니다. 이 섹션은 영구 볼륨을 제공하기 위해 Trident가 관리형 Amazon FSx for NetApp ONTAP(FSx ONTAP)을 스토리지 백엔드로 사용하는 방법을 보여줍니다. NetApp Console을 사용하여 AWS에 FSx ONTAP을 배포하는 방법에 대한 자세한 내용이 제공됩니다. 또한 NetApp Console 및 OpenShift GitOps(Argo CD)를 사용하여 ROSA 클러스터의 상태 저장 애플리케이션에 대한 데이터 보호 및 마이그레이션 작업을 수행하는 방법에 대한 자세한 내용도 제공됩니다.

다음은 AWS에 배포되고 FSx ONTAP 백엔드 스토리지로 사용하는 ROSA 클러스터를 보여주는 다이어그램입니다.



이 솔루션은 AWS의 두 VPC에 있는 두 개의 ROSA 클러스터를 사용하여 검증되었습니다. 각 ROSA 클러스터는 Trident 사용하여 FSx ONTAP 과 통합되었습니다. AWS에 ROSA 클러스터와 FSx ONTAP 배포하는 방법에는 여러 가지가 있습니다. 설정에 대한 이러한 간략한 설명은 사용된 특정 방법에 대한 문서 링크를 제공합니다. 제공된 관련 링크에서 다른 방법을 참조할 수 있습니다."리소스 섹션" .

설정 과정은 다음 단계로 나눌 수 있습니다.

ROSA 클러스터 설치

- 두 개의 VPC를 만들고 VPC 간에 VPC 피어링 연결을 설정합니다.
- ROSA 클러스터 설치 지침은 "여기"을(를) 참조하십시오.

FSx ONTAP 설치

- NetApp Console에서 VPC에 FSx ONTAP을 설치합니다. NetApp Console 계정 생성 및 시작에 대해서는 "여기"를 참조하십시오. FSx ONTAP 설치에 대해서는 "여기"를 참조하십시오. FSx ONTAP을 관리하기 위해 AWS에 커넥터를 생성하는 방법에 대해서는 "여기"를 참조하십시오.
- AWS를 사용하여 FSx ONTAP 배포합니다. 나타내다"여기" AWS 콘솔을 사용하여 배포합니다.

ROSA 클러스터에 **Trident** 설치**(Helm** 차트 사용**)**

- Helm 차트를 사용하여 ROSA 클러스터에 Trident를 설치합니다. 문서 링크 참조: 여기.

ROSA 클러스터를 위한 Trident 와 FSx ONTAP 통합

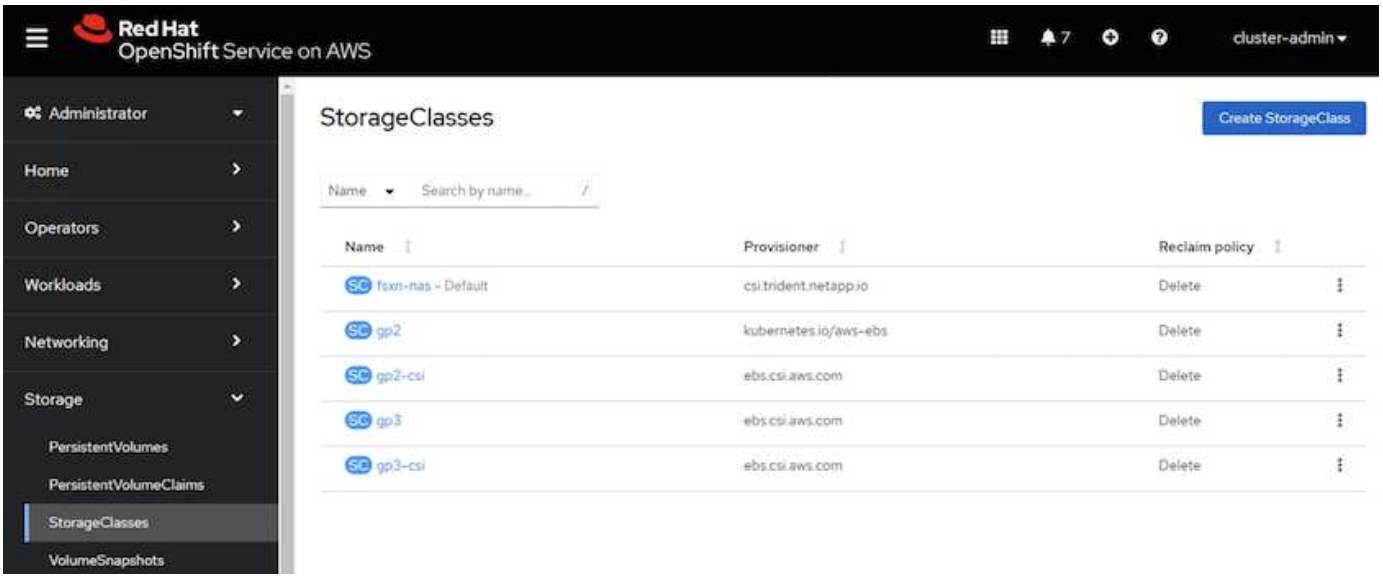
OpenShift GitOps를 사용하면 ApplicationSet을 사용하여 ArgoCD에 등록되는 모든 관리형 클러스터에 Trident CSI를 배포할 수 있습니다.

```yaml
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: trident-operator
spec:
  generators:
  - clusters: {}
    # selector:
    #   matchLabels:
    #     tridentversion: '23.04.0'
  template:
    metadata:
      name: '{{nameNormalized}}-trident'
    spec:
      destination:
        namespace: trident
        server: '{{server}}'
      source:
        repoURL: 'https://netapp.github.io/trident-helm-chart'
        targetRevision: 23.04.0
        chart: trident-operator
      project: default
      syncPolicy:
        syncOptions:
          - CreateNamespace=true
```



Trident (FSx ONTAP 용)를 사용하여 백엔드 및 스토리지 클래스 생성

- 나타내다"여기" 백엔드와 스토리지 클래스 생성에 대한 자세한 내용은 다음을 참조하세요.
- OpenShift 콘솔에서 Trident CSI를 기본값으로 사용하여 FsxN에 대해 생성된 스토리지 클래스를 만듭니다. 아래의 스크린샷을 참조하세요.



OpenShift GitOps(Argo CD)를 사용하여 애플리케이션 배포

- 클러스터에 OpenShift GitOps 오퍼레이터를 설치하십시오. 지침 "여기"을 참조하십시오.
- SetUp 클러스터용 새 Argo CD 인스턴스를 설정하십시오. 지침 "여기"을 참조하십시오.

Argo CD 콘솔을 열고 애플리케이션을 배포합니다. 예를 들어, Helm 차트를 사용하여 Jenkins 애플리케이션을 Argo

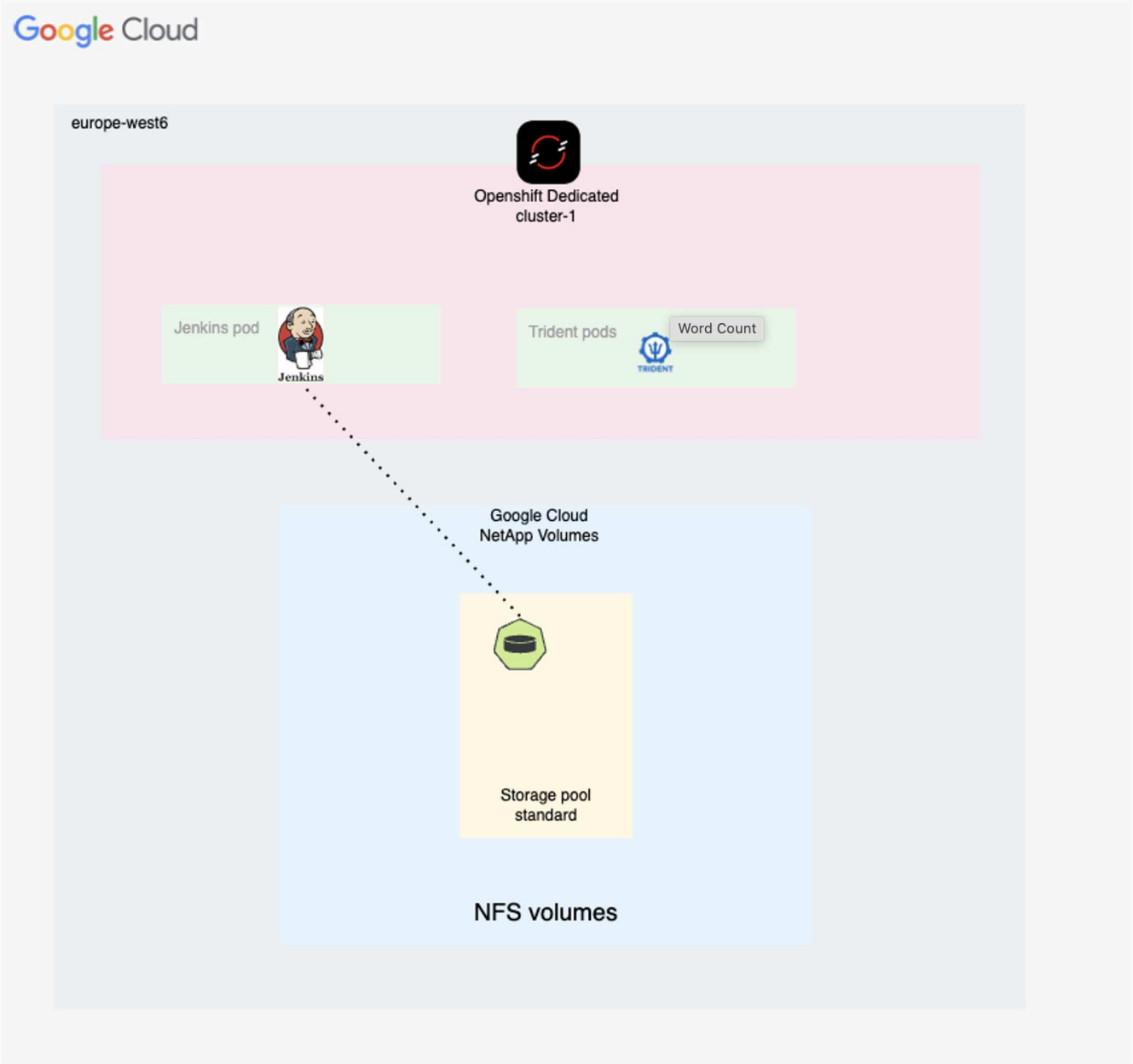
CD로 배포할 수 있습니다. 애플리케이션을 생성할 때 다음과 같은 세부 정보가 제공됩니다. 프로젝트: default 클러스터: 'https://kubernetes.default.svc'[](따옴표 제외) 네임스페이스: Jenkins Helm 차트 URL: 'https://charts.bitnami.com/bitnami'[](따옴표 제외)

Helm 매개변수: global.storageClass: fsxn-nas

Google Cloud NetApp Volumes 사용하여 **Google Cloud**에 **OpenShift Dedicated** 배포 및 구성

이 섹션에서는 Google Cloud 플랫폼에서 OpenShift Dedicated(OSD) 클러스터를 설정하는 개략적인 워크플로를 설명합니다. NetApp Trident Kubernetes로 실행되는 상태 저장 애플리케이션에 영구 볼륨을 제공하기 위해 스토리지 백엔드로 Google Cloud NetApp Volumes 사용하는 것을 보여줍니다.

다음은 Google Cloud에 배포되고 NetApp Volumes를 백엔드 스토리지로 사용하는 OSD 클러스터를 보여주는 다이어그램입니다.



설정 과정은 다음 단계로 나눌 수 있습니다.

Google Cloud에 **OSD** 클러스터 설치

- 클러스터에 기존 VPC를 사용하려면 OSD 클러스터에 대한 VPC, 두 개의 서브넷, 클라우드 라우터, 두 개의 GCP 클라우드 NAT를 만들어야 합니다. 나타내다"여기" 지침을 보려면 클릭하세요.
- Customer Cloud Subscription(CCS) 결제 모델을 사용하여 GCP에 OSD 클러스터를 설치하는 방법에 대한 지침은 "여기"을(를) 참조하십시오. OSD는 Google Cloud Marketplace에서도 제공됩니다. Google Cloud Marketplace 솔루션을 사용하여 OSD를 설치하는 방법을 보여주는 동영상은 "여기"에 있습니다.

Google Cloud NetApp Volumes 활성화

- 나타내다"여기" Google Cloud NetApp Volumes 에 대한 액세스 설정에 대한 정보는 다음을 참조하세요. 다음 단계를 모두 따르세요.
- 스토리지 풀을 생성합니다. 나타내다"여기" Google Cloud NetApp Volumes 에서 스토리지 풀을 설정하는 방법에 대한 정보입니다. OSD에서 실행되는 상태 저장 Kubernetes 애플리케이션의 볼륨은 스토리지 풀 내에 생성됩니다.

OSD 클러스터에 **Trident** 설치**(Helm** 차트 사용**)**

- Helm 차트를 사용하여 OSD 클러스터에 Trident를 설치하십시오. Helm 차트 설치 방법에 대한 지침은 "여기"을 참조하십시오.

OSD 클러스터를 위한 **NetApp Trident** 와 **NetApp Volumes** 통합

Trident 사용하여 백엔드 및 스토리지 클래스 생성(Google Cloud NetApp Volumes 용)

- 백엔드 생성에 대한 자세한 내용은 여기를 참조하세요.
- 현재 쿠버네티스의 스토리지 클래스 중에 기본값으로 표시된 것이 있다면, 스토리지 클래스를 편집하여 해당 주석을 제거하세요.
- Trident CSI 프로비저너를 사용하여 NetApp 볼륨에 대한 스토리지 클래스를 하나 이상 만듭니다. 주석을 사용하여 저장 클래스 중 하나만 기본값으로 지정합니다. 이를 통해 PVC는 PVC 매니페스트에서 명시적으로 호출되지 않은 경우에도 이 저장 클래스를 사용할 수 있습니다. 주석이 포함된 예는 아래와 같습니다.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-standard-k8s
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: true
```

OpenShift GitOps(Argo CD)를 사용하여 애플리케이션 배포

- 클러스터에 OpenShift GitOps 오퍼레이터를 설치하십시오. 지침을 참조하십시오 "여기".
- SetUp 클러스터용 새 Argo CD 인스턴스를 설정하십시오. 지침 "여기"을 참조하십시오.

Argo CD 콘솔을 열고 애플리케이션을 배포합니다. 예를 들어, Helm 차트를 사용하여 Jenkins 애플리케이션을 Argo CD로 배포할 수 있습니다. 애플리케이션을 생성할 때 다음과 같은 세부 정보가 제공됩니다. 프로젝트: default 클러스터: 'https://kubernetes.default.svc'[](따옴표 제외) 네임스페이스: Jenkins Helm 차트 URL: 'https://charts.bitnami.com/bitnami'[](따옴표 제외)

데이터 보호

Trident Protect를 사용하여 컨테이너 워크로드를 보호하고 마이그레이션하는 방법에 대한 자세한 내용은 다음 섹션을 참조하십시오. - "Trident Protect를 사용하여 컨테이너 앱을 보호하고 마이그레이션하세요."

Red Hat OpenShift 워크로드를 위한 추가 **NetApp** 하이브리드 멀티클라우드 솔루션

다음 추가 해결 방법을 참조하십시오.

- "온프레미스 Red Hat OpenShift 컨테이너 솔루션"
- "Red Hat OpenShift Service on AWS 컨테이너 솔루션"
- "온프레미스 Red Hat OpenShift 가상화 솔루션"
- "Red Hat OpenShift Service on AWS 가상화 솔루션"

Trident Protect를 사용하여 데이터 보호

Trident Protect를 사용하여 OpenShift Container Platform의 컨테이너 앱 데이터 보호

참조 문서의 이 섹션에서는 Trident Protect를 사용하여 Container Apps의 스냅샷 및 백업을 생성하는 방법에 대한 자세한 내용을 제공합니다. NetApp Trident Protect는 NetApp ONTAP 스토리지 시스템과 NetApp Trident CSI 스토리지 프로비저너를 기반으로 하는 스테이트풀 Kubernetes 애플리케이션의 기능과 가용성을 향상시키는 고급 애플리케이션 데이터 관리 기능을 제공합니다. Trident Protect는 애플리케이션 스냅샷 및 백업을 생성합니다. 즉, 영구 볼륨의 애플리케이션 데이터뿐만 아니라 애플리케이션 메타데이터에 대한 스냅샷 및 백업이 생성됩니다. Trident Protect에서 생성된 스냅샷 및 백업은 다음 객체 스토리지 중 하나에 저장하고 나중에 복원할 수 있습니다.

- AWS S3
- Azure Blob 저장소
- 구글 클라우드 스토리지
- ONTAP S3
- 스토리지그리드
- 기타 S3 호환 스토리지

Trident Protect는 Kubernetes 모델의 역할 기반 액세스 제어(RBAC)를 사용합니다. 기본적으로 Trident Protect는 trident-protect라는 단일 시스템 네임스페이스와 해당 기본 서비스 계정을 제공합니다. 사용자 수가 많거나 특정 보안 요구 사항이 있는 조직의 경우 Trident Protect의 RBAC 기능을 활용하여 리소스 및 네임스페이스에 대한 액세스 제어를 더욱 세밀하게 제어할 수 있습니다.

Trident Protect의 RBAC에 대한 추가 정보는 "Trident Protect 문서"에서 확인할 수 있습니다.

> 클러스터 관리자는 기본 trident-protect 네임스페이스의 리소스에 액세스할 수 있으며 다른 모든 네임스페이스의 리소스에도 액세스할 수 있습니다. 사용자는 trident-protect 네임스페이스에서 스냅샷 및 백업 CR과 같은 애플리케이션 데이터 관리 사용자 정의 리소스(CR)를 생성할 수 없습니다. 가장 좋은 방법은 사용자가 애플리케이션 네임스페이스에서 해당 CR을 만드는 것입니다.

Trident Protect는 설명서"여기"에 제공된 지침을 사용하여 설치할 수 있습니다. 이 섹션에서는 Trident Protect를 사용한 컨테이너 애플리케이션의 데이터 보호 및 애플리케이션 복원 워크플로를 보여줍니다. 1. 스냅샷 생성(필요 시 또는 예약) 2. 스냅샷에서 복원(동일 및 다른 네임스페이스로 복원) 3. 백업 생성 4. 백업에서 복원

▼ 필수 조건

애플리케이션의 스냅샷 및 백업을 생성하기 전에 Trident Protect에서 스냅샷과 백업을 저장할 오브젝트 스토리지를 구성해야 합니다. 이는 버킷 CR을 사용하여 수행됩니다. 관리자만 버킷 CR을 생성하고 구성할 수 있습니다. Trident Protect에서 버킷 CR은 AppVault라고 합니다. AppVault 오브젝트는 스토리지 버킷을 Kubernetes 워크플로에서

선언적으로 표현한 것입니다. AppVault CR에는 백업, 스냅샷, 복원 작업 및 SnapMirror 복제와 같은 보호 작업에 버킷을 사용하는 데 필요한 구성이 포함되어 있습니다.

이 예제에서는 ONTAP S3를 객체 스토리지로 사용하는 방법을 보여드리겠습니다. ONTAP S3용 AppVault CR을 생성하는 워크플로는 다음과 같습니다. 1. ONTAP 클러스터의 SVM에 S3 객체 스토어 서버를 생성합니다. 2. 객체 스토어 서버에 버킷을 생성합니다. 3. SVM에 S3 사용자를 생성합니다. 액세스 키와 시크릿 키는 안전한 곳에 보관하십시오. 4. OpenShift에서 ONTAP S3 자격 증명을 저장할 시크릿을 생성합니다. 5. ONTAP S3용 AppVault 객체를 생성합니다.

ONTAP S3용 Trident Protect AppVault 구성

ONTAP S3를 AppVault로 사용하여 Trident Protect를 구성하기 위한 샘플 YAML 파일

```
# alias tp='tridentctl-protect'

appvault-secret.yaml

apiVersion: v1
stringData:
  accessKeyID: "<access key id created for a user to access ONTAP S3
bucket>"
  secretAccessKey: "corresponding Secret Access Key"
#data:
# base 64 encoded values
#  accessKeyID: <base64 access key id created for a user to access ONTAP
S3 bucket>
#  secretAccessKey: <base 64  Secret Access Key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque

appvault.yaml

apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
```

```
      bucketName: ""
      projectID: ""
    s3:
      bucketName: <bucket-name for storing the snapshots and backups>
      endpoint: <endpoint IP for S3>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost openshift-benchmark]#
[root@localhost openshift-benchmark]# tp get appvault -n trident-protect
+-------------------+----------+-----------+------+-------+
|       NAME        | PROVIDER |   STATE   | AGE  | ERROR |
+-------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 2d2h |       |
+-------------------+----------+-----------+------+-------+
[root@localhost openshift-benchmark]#
```

postgresql 앱 설치를 위한 샘플 **yaml** 파일

```
postgres.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: postgres
spec:
  replicas: 1
  selector:
    matchLabels:
      app: postgres
  template:
    metadata:
      labels:
```

```
        app: postgres
    spec:
      containers:
      - name: postgres
        image: postgres:14
        env:
        - name: POSTGRES_USER
          #value: "myuser"
          value: "admin"
        - name: POSTGRES_PASSWORD
          #value: "mypassword"
          value: "adminpass"
        - name: POSTGRES_DB
          value: "mydb"
        - name: PGDATA
          value: "/var/lib/postgresql/data/pgdata"
        ports:
        - containerPort: 5432
        volumeMounts:
        - name: postgres-storage
          mountPath: /var/lib/postgresql/data
      volumes:
      - name: postgres-storage
        persistentVolumeClaim:
          claimName: postgres-pvc
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: postgres-pvc
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 5Gi
---
apiVersion: v1
kind: Service
metadata:
  name: postgres
spec:
  selector:
    app: postgres
  ports:
  - protocol: TCP
```

```
    port: 5432
    targetPort: 5432
  type: ClusterIP

Now create the Trident Protect application CR for the postgres app.
Include the objects in the namespace postgres and create it in the
postgres namespace.
# tp create app postgres-app --namespaces postgres -n postgres
```

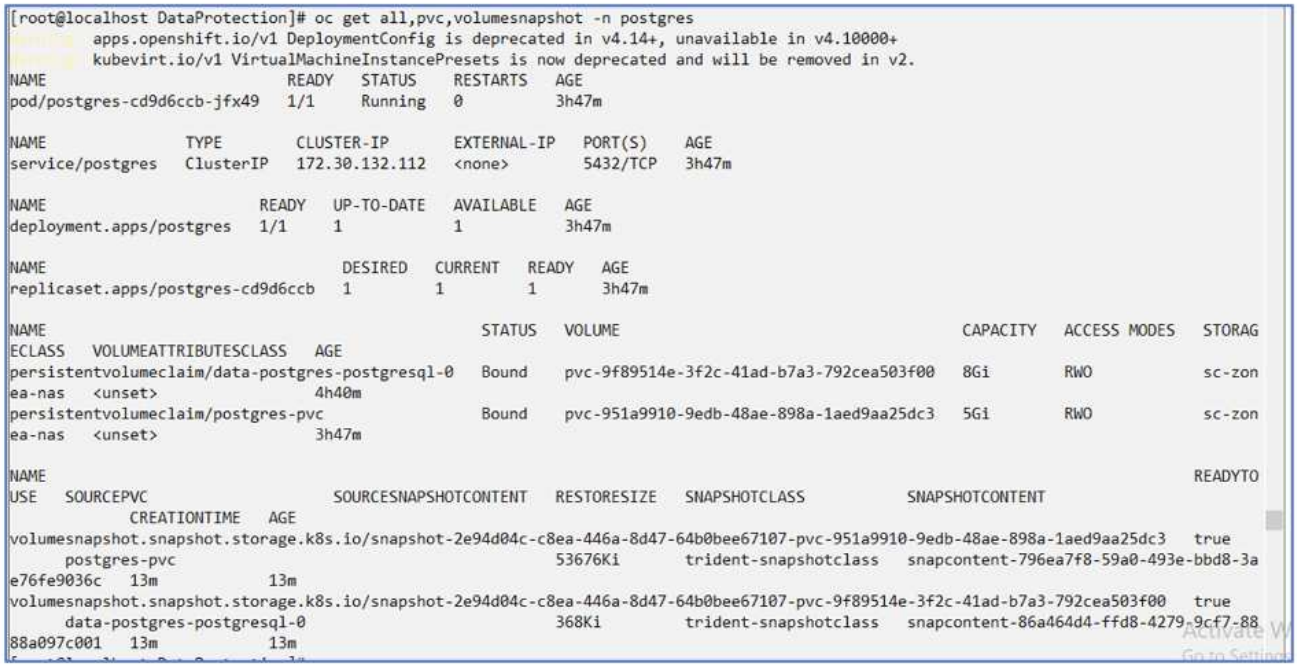
```
[root@localhost RedHat]# tp get app -n postgres
+--------------+------------+-------+-----+
|     NAME     | NAMESPACES | STATE | AGE |
+--------------+------------+-------+-----+
| postgres-app | postgres   | Ready | 24s |
+--------------+------------+-------+-----+
[root@localhost RedHat]#
```

▼ 스냅샷 만들기

주문형 스냅샷 만들기

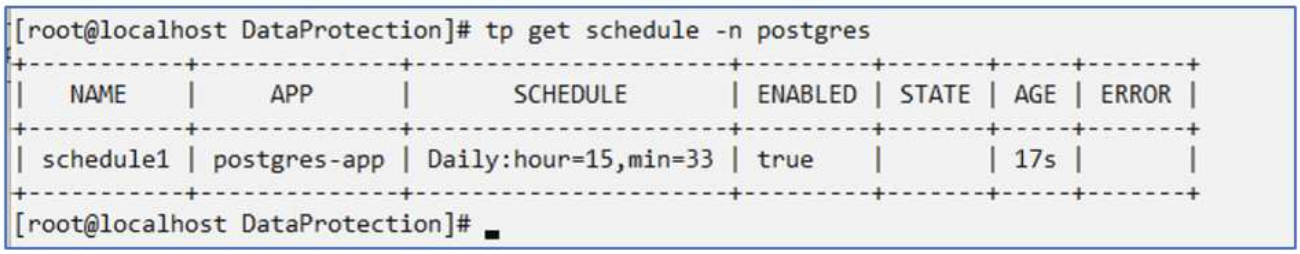
```
# tp create snapshot postgres-snap1 --app postgres-app --appvault ontap-
s3-appvault -n postgres
Snapshot "postgres-snap1" created.
```

```
[root@localhost RedHat]# tp get snapshot -n postgres
+----------------+--------------+-----------+-----+-------+
|      NAME      |   APP REF    |   STATE   | AGE | ERROR |
+----------------+--------------+-----------+-----+-------+
| postgres-snap1 | postgres-app | Completed | 19s |       |
+----------------+--------------+-----------+-----+-------+
[root@localhost RedHat]#
```



일정 만들기 다음 명령을 사용하면 매일 15:33에 스냅샷이 생성되고 두 개의 스냅샷과 백업이 보관됩니다.

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```



yaml을 사용하여 일정 만들기

```
# tp create schedule schedule2 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres --dry-run >
hourly-snapshotschedule.yaml

cat hourly-snapshotschedule.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Schedule
```

```
metadata:
  creationTimestamp: null
  name: schedule2
  namespace: postgres
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: postgres-app
  backupRetention: "2"
  dataMover: Restic
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  #hour: "15"
  minute: "33"
  recurrenceRule: ""
  snapshotRetention: "2"
status: {}
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+--------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 8d7h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 8d7h |       |
+-----------+--------------+----------------------+---------+-------+------+-------+
[root@localhost DataProtection]#
```

이 일정에 따라 생성된 스냅샷을 볼 수 있습니다.

```
[root@localhost DataProtection]# tp get snap -n postgres
+-----------------------------+--------------+-----------+-------+-------+
|            NAME             |   APP REF    |   STATE   |  AGE  | ERROR |
+-----------------------------+--------------+-----------+-------+-------+
| hourly-3f1ee-20250214183300 | postgres-app | Completed | 19s   |       |
| postgres-snap1              | postgres-app | Completed | 1h25m |       |
+-----------------------------+--------------+-----------+-------+-------+
[root@localhost DataProtection]#
```

볼륨 스냅샷도 생성됩니다.

```
[root@localhost DataProtection]# oc get volumesnapshots -n postgres
NAME                                                                                                  READYTOUSE   SOURCEPVC
                                CREATIONTIME   AGE
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-59a0-493e-bbd8-3ae76fe9036c   114m           114m
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-ffd8-4279-9cf7-8888a097c001   114m           114m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-7adc-4042-a8c9-7606d1103ead   30m            30m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-3a82-43f6-9868-dcadd2cc04e2   30m            30m
```

▼ 애플리케이션 손실을 시뮬레이션하기 위해 애플리케이션을 삭제합니다.

```
# oc delete deployment/postgres -n postgres
# oc get pod,pvc -n postgres
No resources found in postgres namespace.
```

▼ 스냅샷에서 동일한 네임스페이스로 복원

```
# tp create sir postgres-sir --snapshot postgres/hourly-3f1ee-
20250214183300 -n postgres
SnapshotInplaceRestore "postgres-sir" created.
```

```
[root@localhost DataProtection]# tp get sir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-sir | ontap-s3-appvault | Completed | 2m39s |       |
+--------------+--------------------+-----------+-------+-------+
```

애플리케이션과 해당 PVC가 동일한 네임스페이스로 복원됩니다.

```
[root@localhost DataProtection]# oc get pods,pvc -n postgres
NAME                     READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-x85tg   1/1     Running   0          98s

NAME                                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/data-postgres-postgresql-0   Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>                 105s
persistentvolumeclaim/postgres-pvc                 Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>                 105s
[root@localhost DataProtection]#
```

▼ 스냅샷에서 다른 네임스페이스로 복원

```
# tp create snapshotrestore postgres-restore --snapshot postgres/hourly-
3f1ee-20250214183300 --namespace-mapping postgres:postgres-restore -n
postgres-restore
SnapshotRestore "postgres-restore" created.
```

```
[root@localhost DataProtection]# tp get snapshotrestore -n postgres-restore
+------------------+--------------------+-----------+-------+-------+
|       NAME       |      APPVAULT      |   STATE   |  AGE  | ERROR |
+------------------+--------------------+-----------+-------+-------+
| postgres-restore | ontap-s3-appvault | Completed | 1m15s |       |
+------------------+--------------------+-----------+-------+-------+
```

애플리케이션이 새로운 네임스페이스로 복원된 것을 볼 수 있습니다.

```
[root@localhost DataProtection]#
[root@localhost DataProtection]# oc get pods,pvc -n postgres-restore
NAME                          READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-pfxw9   1/1     Running   0          8d

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/data-postgres-postgresql-0    Bound    pvc-3dff4e42-828d-49f9-84e9-4daf75479292   8Gi        RWO            sc-zonea-nas
persistentvolumeclaim/postgres-pvc                  Bound    pvc-f57321b2-f21f-4eb7-8f86-4a17f915318b   5Gi        RWO            sc-zonea-nas
[root@localhost DataProtection]#
```

▼ 백업 만들기

주문형 백업 생성

```
# tp create backup postgres-backup1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup1" created.
```

```
[root@localhost DataProtection]# tp get backup -n postgres
+-----------------------------+--------------+-----------+--------+-------+
|            NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+-----------------------------+--------------+-----------+--------+-------+
| backup1                     | postgres-app | Completed | 5d12h  |       |
| daily-feac1-20250222153300  | postgres-app | Completed | 1d10h  |       |
| daily-feac1-20250223153300  | postgres-app | Completed | 10h36m |       |
| hourly-3f1ee-20250224003300 | postgres-app | Completed | 1h36m  |       |
| hourly-3f1ee-20250224013300 | postgres-app | Completed | 36m27s |       |
| postgres-backup1            | postgres-app | Completed | 6m19s  |       |
+-----------------------------+--------------+-----------+--------+-------+
```

백업 일정 생성

위 목록의 일일 백업과 매시간 백업은 이전에 설정한 일정에 따라 생성됩니다.

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily --hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+--------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 9d8h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 9d8h |       |
+-----------+--------------+----------------------+---------+-------+------+-------+
```

▼ 백업에서 복원

데이터 손실을 시뮬레이션하려면 애플리케이션과 **PVC**를 삭제하세요.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-dftkt     1/1     Running   0          11s
[root@localhost DataProtection]# oc get deployment -n postgres
NAME       READY   UP-TO-DATE   AVAILABLE   AGE
postgres   1/1     1            1           20s
[root@localhost DataProtection]# oc delete deployment/postgres -n postgres
deployment.apps "postgres" deleted
[root@localhost DataProtection]# oc get pods -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTE
SCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>
         5d13h
postgres-pvc                  Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>
         5d13h
[root@localhost DataProtection]# oc delete pvc/data-postgres-postgresql-0  -n postgres
persistentvolumeclaim "data-postgres-postgresql-0" deleted
[root@localhost DataProtection]# oc delete pvc/postgres-pvc -n postgres
persistentvolumeclaim "postgres-pvc" deleted
[root@localhost DataProtection]# oc get pvc -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

동일한 네임스페이스로 복원 #tp create bir postgres-bir --backup postgres/hourly-3f1ee-20250224023300 -n postgres BackupInplaceRestore "postgres-bir"이 생성되었습니다.

```
[root@localhost DataProtection]# tp get bir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-bir | ontap-s3-appvault | Completed | 2m19s |       |
+--------------+--------------------+-----------+-------+-------+
```

애플리케이션과 PVC는 동일한 네임스페이스에 복원됩니다.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-t857w     1/1     Running   0          10m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-0a849c19-16fe-466f-9733-85e82a8b1677   8Gi        RWO            sc-zonea-nas   <unset>
          10m
postgres-pvc                  Bound    pvc-ded304ea-02d4-4225-b606-63007666ad66   5Gi        RWO            sc-zonea-nas   <unset>
          10m
```

다른 네임스페이스로 복원 새로운 네임스페이스를 만듭니다. 백업에서 새 네임스페이스로 복원합니다.

```
[root@localhost DataProtection]# oc create ns postgres-restore-from-backup
namespace/postgres-restore-from-backup created
[root@localhost DataProtection]# tp create backuprestore postgres-restore-from-backup --backup postgres/postgres-backup1 --namespace-map
ping postgres:postgres-restore-from-backup -n postgres-restore-from-backup
BackupRestore "postgres-restore-from-backup" created.
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                          STATE     ERROR   AGE
postgres-restore-from-backup   Running           37s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                          STATE     ERROR   AGE
postgres-restore-from-backup   Running           56s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                          STATE       ERROR   AGE
postgres-restore-from-backup   Completed           2m52s
[root@localhost DataProtection]# oc get pods -n postgres-restore-from-backup
NAME                       READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-p659p   1/1     Running   0          2m9s
[root@localhost DataProtection]# oc get pvc -n postgres-restore-from-backup
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-36df7399-95da-4c67-a621-af9434015bdb   8Gi        RWO            sc-zonea-nas   <unset>
          2m18s
postgres-pvc                 Bound    pvc-633de3aa-a4f9-4f3b-93cc-e91afbd4fe02   5Gi        RWO            sc-zonea-nas   <unset>
          2m18s
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

▼ 애플리케이션 마이그레이션

애플리케이션을 다른 클러스터로 복제하거나 마이그레이션하려면(클러스터 간 복제 수행) 소스 클러스터에서 백업을 생성한 다음 다른 클러스터에 백업을 복원하십시오. 타겟 클러스터에 Trident Protect가 설치되어 있는지 확인하십시오.

소스 클러스터에서 아래 이미지에 표시된 단계를 수행합니다.

```
[root@localhost DataProtection]# tp create backup postgres-backup-cluster1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup-cluster1" created.
[root@localhost DataProtection]# tp get backup -n postgres
+-----------------------------+--------------+-----------+--------+-------+
|            NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+-----------------------------+--------------+-----------+--------+-------+
| backup1                     | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300  | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300  | postgres-app | Completed | 12h18m |       |
| hourly-3f1ee-20250224023300 | postgres-app | Completed | 1h18m  |       |
| hourly-3f1ee-20250224033300 | postgres-app | Completed | 18m26s |       |
| postgres-backup-cluster1    | postgres-app | Running   | 35s    |       |
| postgres-backup1            | postgres-app | Completed | 1h48m  |       |
+-----------------------------+--------------+-----------+--------+-------+
[root@localhost DataProtection]# tp get backup -n postgres
+-----------------------------+--------------+-----------+--------+-------+
|            NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+-----------------------------+--------------+-----------+--------+-------+
| backup1                     | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300  | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300  | postgres-app | Completed | 12h19m |       |
| hourly-3f1ee-20250224023300 | postgres-app | Completed | 1h19m  |       |
| hourly-3f1ee-20250224033300 | postgres-app | Completed | 19m41s |       |
| postgres-backup-cluster1    | postgres-app | Completed | 1m50s  |       |
| postgres-backup1            | postgres-app | Completed | 1h49m  |       |
+-----------------------------+--------------+-----------+--------+-------+
```

Activate Windows
Go to Settings to activate Windows.

소스 클러스터에서 대상 클러스터로 컨텍스트를 전환합니다. 그런 다음 대상 클러스터 컨텍스트에서 AppVault에 액세스할 수 있는지 확인하고 대상 클러스터에서 AppVault 콘텐츠를 가져옵니다.

```
[root@localhost DataProtection]# kubectl config use-context default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin
Switched to context "default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin".
[root@localhost DataProtection]# tp get appvault -n trident-protect
+-------------------+----------+-----------+------+-------+
|       NAME        | PROVIDER |   STATE   | AGE  | ERROR |
+-------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 3d6h |       |
+-------------------+----------+-----------+------+-------+
[root@localhost DataProtection]# tp get appvaultcontent ontap-s3-appvault --show-resources backup --show-paths
+---------------+--------------+--------+----------------------------+--------------------------+-----------------------------------
-----------------------------------------------------------------------------------+
|    CLUSTER    |     APP      |  TYPE  |            NAME            |        TIMESTAMP         |
                      PATH                                                                                                  |
+---------------+--------------+--------+----------------------------+--------------------------+-----------------------------------
-----------------------------------------------------------------------------------+
| ocp-cluster11 | bbox         | backup | bboxbackup1                | 2025-01-17 15:57:49 (UTC) | bbox_68b4f05f-d5f1-4304-8c69-ad67514
fe393/backups/bboxbackup1_3960c945-8ee0-42fe-945c-c57bb0a3af6f                                                             |
| ocp-cluster11 | postgres-app | backup | backup1                    | 2025-02-18 13:31:50 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/backup1_28e1bd9a-9b04-4412-8b96-811f9b62e2e3                                                         |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250222153300 | 2025-02-22 15:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250222153300_23d1386b-09f0-456f-aa49-a5865fd48abd                                      |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250223153300 | 2025-02-23 15:34:42 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250223153300_c492a4d1-38a9-4472-9684-4705c12a206d                                      |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224033300 | 2025-02-24 03:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224033300_3d09ab81-f6fe-47fa-a699-28006160cdbc                                     |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224043300 | 2025-02-24 04:34:47 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224043300_66805e4f-7631-48a6-98f7-d34bb8626031                                     |
| ocp-cluster11 | postgres-app | backup | postgres-backup-cluster1   | 2025-02-24 03:52:36 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/postgres-backup-cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3                                        |
```

목록에서 백업 경로를 사용하고 아래 명령에 표시된 대로 backuprestore CR 객체를 만듭니다.

```
# tp create backuprestore backup-restore-cluster2 --namespace-mapping
postgres:postgres --appvault ontap-s3-appvault --path postgres-
app_4d798ed5-cfa8-49ff-a5b6-c5e2d89aeb89/backups/postgres-backup-
cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3 -n postgres
BackupRestore "backup-restore-cluster2" created.
```

```
[root@localhost DataProtection]# tp get backuprestore -n postgres
+--------------------------+--------------------+-----------+--------+-------+
|           NAME           |      APPVAULT      |   STATE   |  AGE   | ERROR |
+--------------------------+--------------------+-----------+--------+-------+
| backup-restore-cluster2 | ontap-s3-appvault | Completed | 12m41s |       |
+--------------------------+--------------------+-----------+--------+-------+
```

이제 대상 클러스터에 애플리케이션 포드와 PVC가 생성된 것을 볼 수 있습니다.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-2lvcq   1/1     Running   0          13m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-872a5182-601b-4848-b410-fef368337d07   8Gi        RWO            sc-zoneb-san   <unset>
          13m
postgres-pvc                 Bound    pvc-caf9fa71-76a8-4645-9bb5-2ed72e72948b   5Gi        RWO            sc-zoneb-san   <unset>
          13m
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

Trident Protect를 사용하여 Red Hat OpenShift Virtualization의 VM 보호

OpenShift Virtualization에서 스냅샷 및 백업을 사용하여 VM을 보호합니다. 이 절차에는

ONTAP S3 객체 스토리지를 사용하여 AppVault를 생성하고, Kubernetes 리소스 객체, 영구 볼륨 및 내부 이미지를 포함한 VM 데이터를 캡처하도록 Trident Protect를 구성하고, 필요할 때 데이터를 복원하는 과정이 포함됩니다.

OpenShift 가상화 환경의 가상 머신은 OpenShift 컨테이너 플랫폼의 워커 노드에서 실행되는 컨테이너화된 애플리케이션입니다. VM 메타데이터와 VM의 영구 디스크를 보호하는 것은 손실되거나 손상될 경우 복구할 수 있도록 하는 데 중요합니다.

OpenShift Virtualization VM의 영구 디스크는 "Trident CSI"을 사용하여 OpenShift 클러스터에 통합된 ONTAP 스토리지로 백업할 수 있습니다. 이 섹션에서는 "Trident Protect"를 사용하여 데이터 볼륨을 포함한 VM의 스냅샷 및 백업을 ONTAP 객체 스토리지에 생성합니다.

필요한 경우 스냅샷이나 백업에서 복원합니다.

Trident Protect는 OpenShift 클러스터의 애플리케이션 및 VM에 대한 스냅샷, 백업, 복원 및 재해 복구를 지원합니다. OpenShift Virtualization VM의 경우, Trident Protect로 보호할 수 있는 데이터에는 VM과 연결된 Kubernetes 리소스 객체, 영구 볼륨 및 내부 이미지가 포함됩니다.

다음은 이 섹션의 예제에 사용된 다양한 구성 요소의 버전입니다.

- "오픈시프트 클러스터 4.17"
- "Red Hat에서 제공하는 OpenShift Virtualization Operator를 통해 설치된 OpenShift Virtualization"
- "Trident 25.02"
- "Trident Protect 25.02"
- "ONTAP 9.16"

객체 스토리지를 위한 **AppVault** 생성

▼ **AppVault** 만들기

애플리케이션 또는 VM의 스냅샷 및 백업을 생성하기 전에 Trident Protect에서 스냅샷 및 백업을 저장할 오브젝트 스토리지를 구성해야 합니다. 이는 버킷 CR을 사용하여 수행됩니다. 버킷 CR은 관리자만 생성하고 구성할 수 있습니다. Trident Protect에서 버킷 CR은 AppVault라고 합니다. AppVault 오브젝트는 스토리지 버킷을 Kubernetes 워크플로에서 선언적으로 표현한 것입니다. AppVault CR에는 백업, 스냅샷, 복원 작업 및 SnapMirror 복제와 같은 보호 작업에 버킷을 사용하는 데 필요한 구성이 포함되어 있습니다.

이 예제에서는 ONTAP S3를 객체 스토리지로 사용하는 방법을 보여드리겠습니다. ONTAP S3용 AppVault CR을 생성하는 워크플로는 다음과 같습니다. 1. ONTAP 클러스터의 SVM에 S3 객체 스토어 서버를 생성합니다. 2. 객체 스토어 서버에 버킷을 생성합니다. 3. SVM에 S3 사용자를 생성합니다. 액세스 키와 시크릿 키는 안전한 곳에 보관하십시오. 4. OpenShift에서 ONTAP S3 자격 증명을 저장할 시크릿을 생성합니다. 5. ONTAP S3용 AppVault 객체를 생성합니다.

ONTAP S3용 **Trident Protect AppVault** 구성

```
# alias tp='tridentctl-protect'

# cat appvault-secret.yaml
apiVersion: v1
stringData:
  accessKeyID: "<access key of S3>"
```

```
  secretAccessKey: "<secret access key of S3>"
# you can also provide base 64 encoded values instead of string values
#data:
# base 64 encoded values
#  accessKeyID: < base 64 encoded access key>
#  secretAccessKey: <base 64 encoded secretAccess key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque

# cat appvault.yaml
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: trident-protect
      endpoint: <lif for S3 access>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost VM-DataProtection]# tp get appvault
+-------------------+----------+-----------+-------+---------+-------+
|       NAME        | PROVIDER |   STATE   | ERROR | MESSAGE |  AGE  |
+-------------------+----------+-----------+-------+---------+-------+
| ontap-s3-appvault | OntapS3  | Available |       |         | 8d17h |
+-------------------+----------+-----------+-------+---------+-------+
[root@localhost VM-DataProtection]#
```

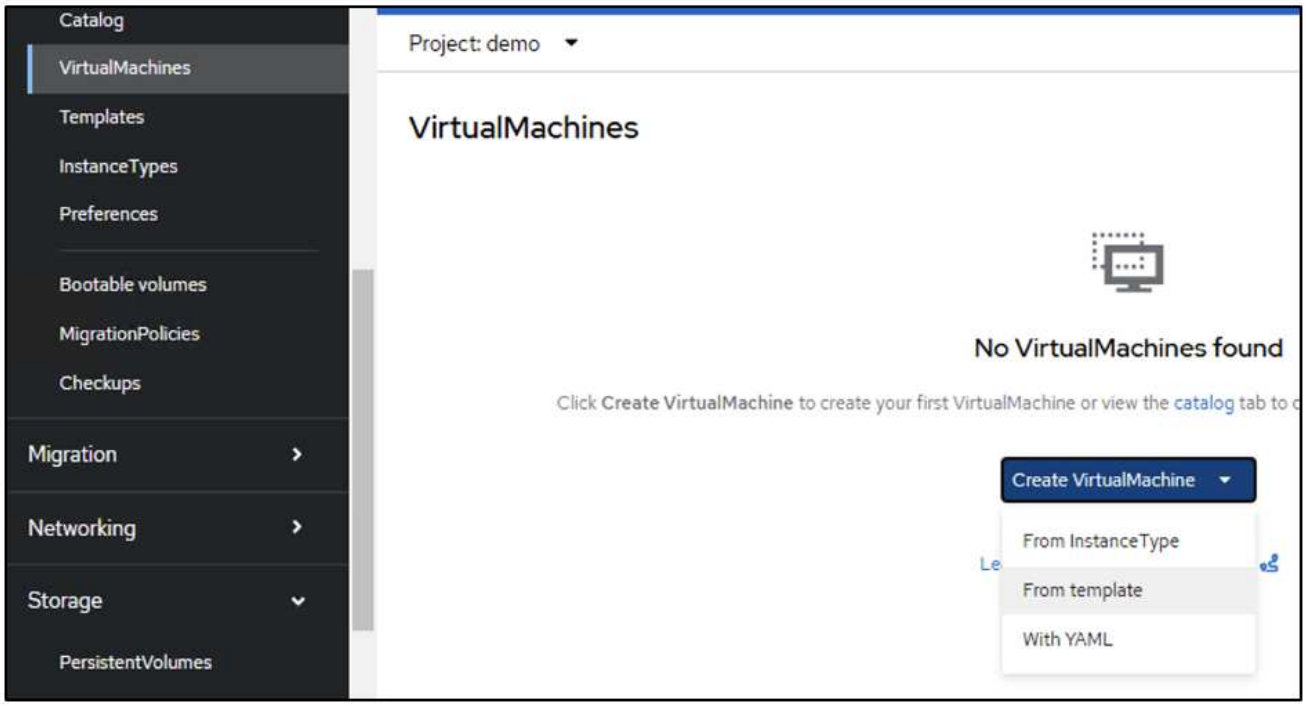
OpenShift Virtualization에서 **VM** 만들기

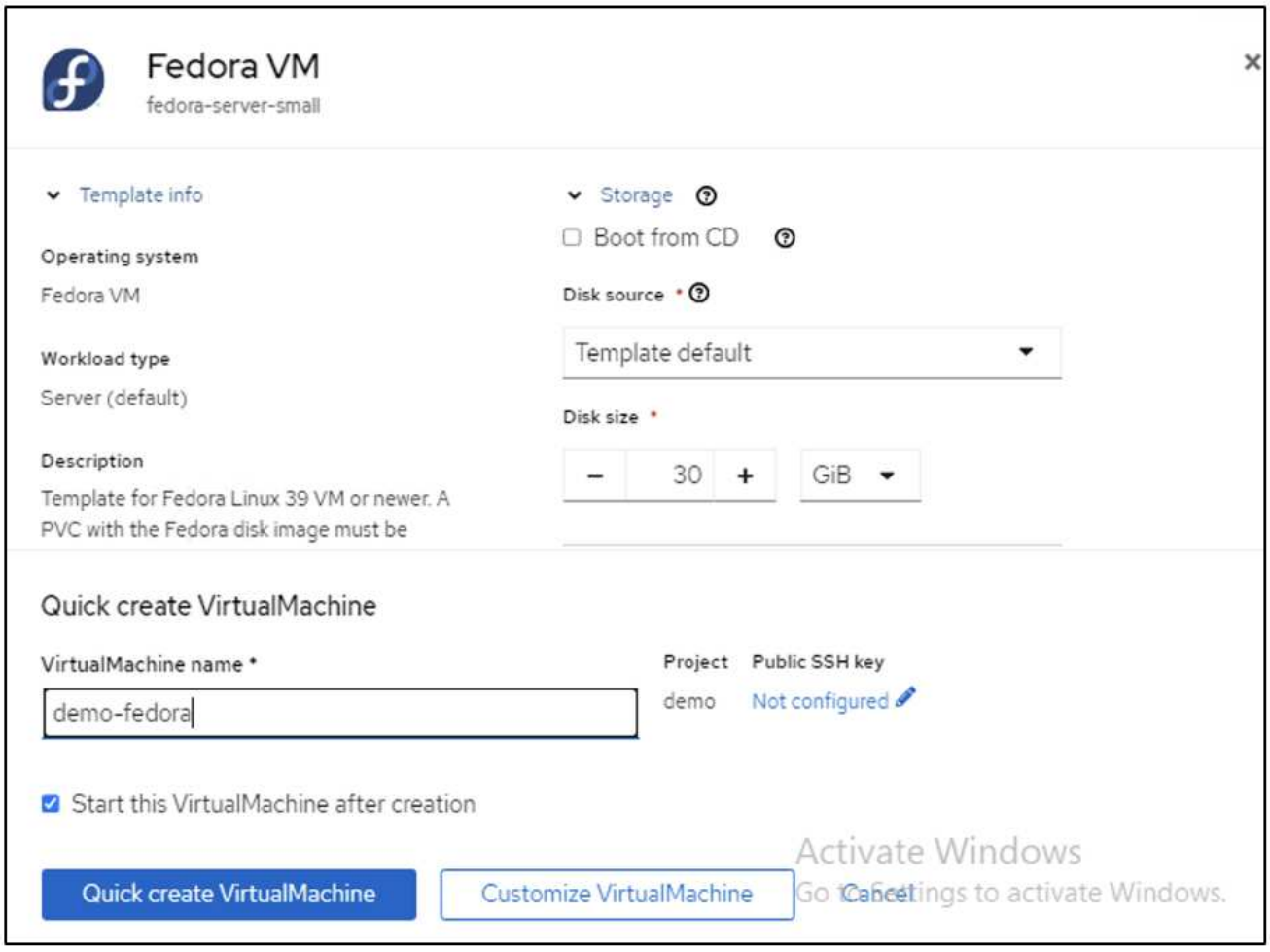
▼ **OpenShift Virtualization**에서 **VM** 만들기

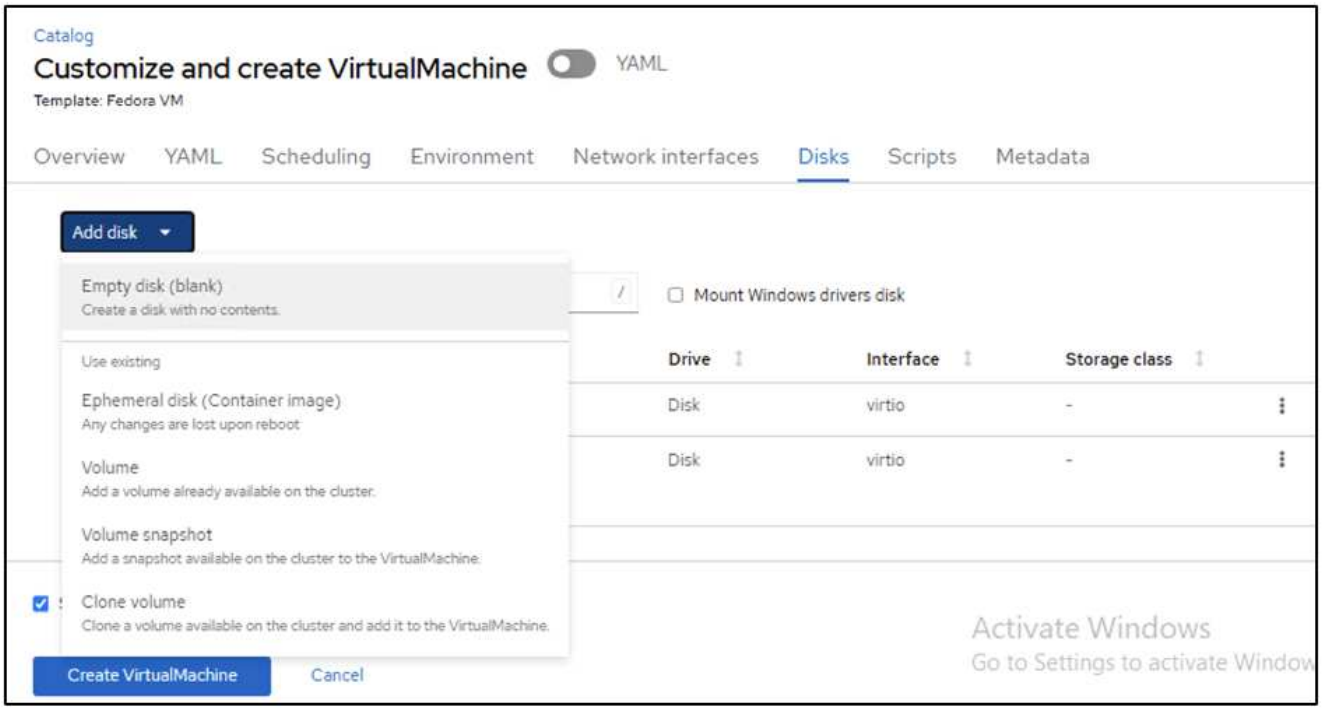
다음 스크린샷은 템플릿을 사용하여 콘솔에서 VM(네임스페이스 demo의 demo-fedora)을 만드는 방법을 보여줍니다. 루트 디스크는 기본 저장소 클래스를 자동으로 선택하므로 기본 저장소 클래스가 적절하게 설정되었는지 확인하세요. 이 설정에서 기본 저장소 클래스는 **sc-zonea-san**입니다. 추가 디스크를 생성할 때 스토리지 클래스 sc-zonea-san을 선택하고 "최적화된 스토리지 설정 적용" 확인란을 선택하세요. 이렇게 하면 액세스 모드가 RWX로 설정되고 볼륨 모드가 차단으로 설정됩니다.

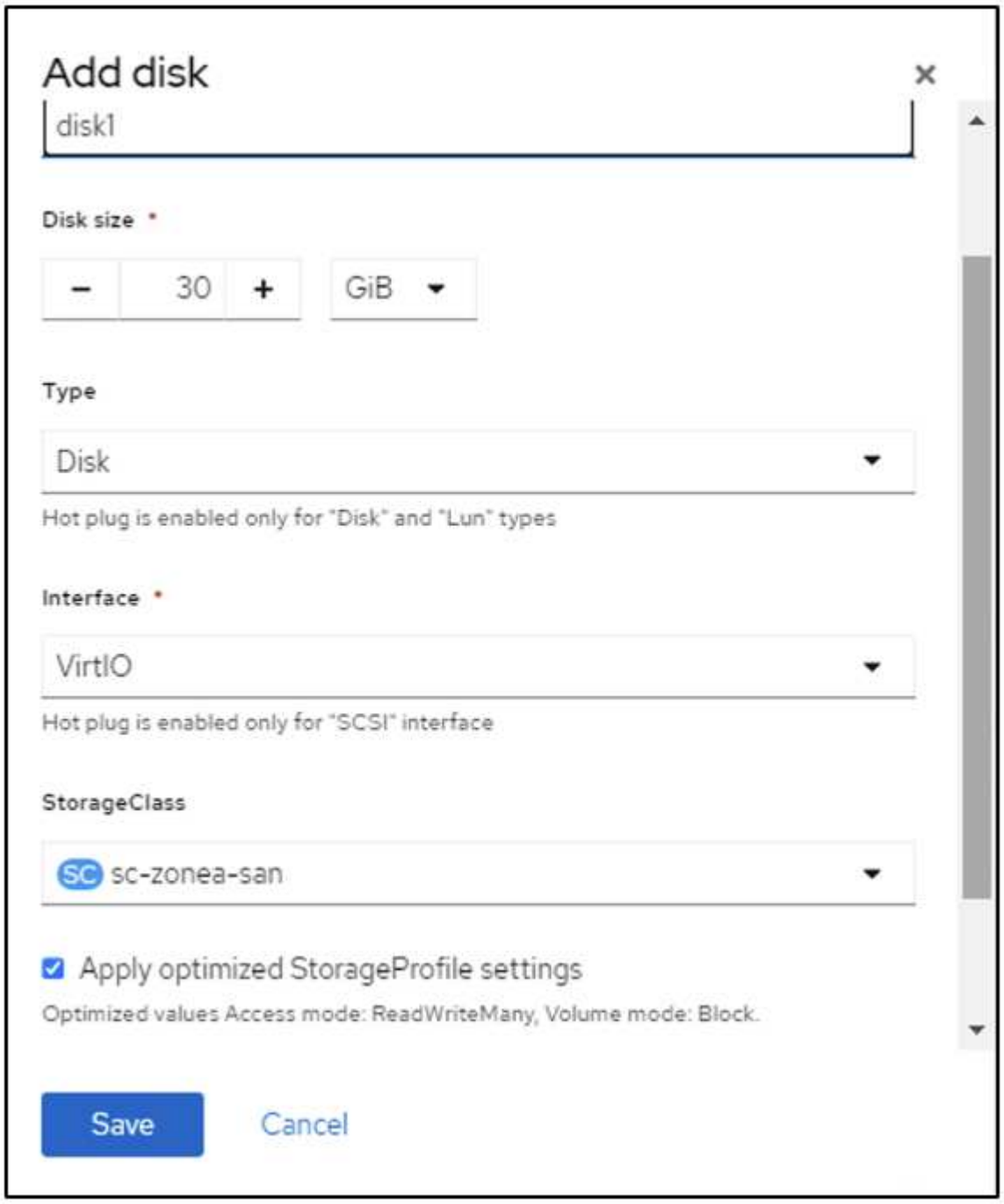
ⓘ Trident SAN(iSCSI, NVMe/TCP 및 FC)의 블록 볼륨 모드에서 RWX 액세스 모드를 지원합니다. (NAS의 기본 접속 모드입니다.) 나중에 VM의 라이브 마이그레이션을 수행해야 하는 경우 RWX 액세스 모드가 필요합니다.

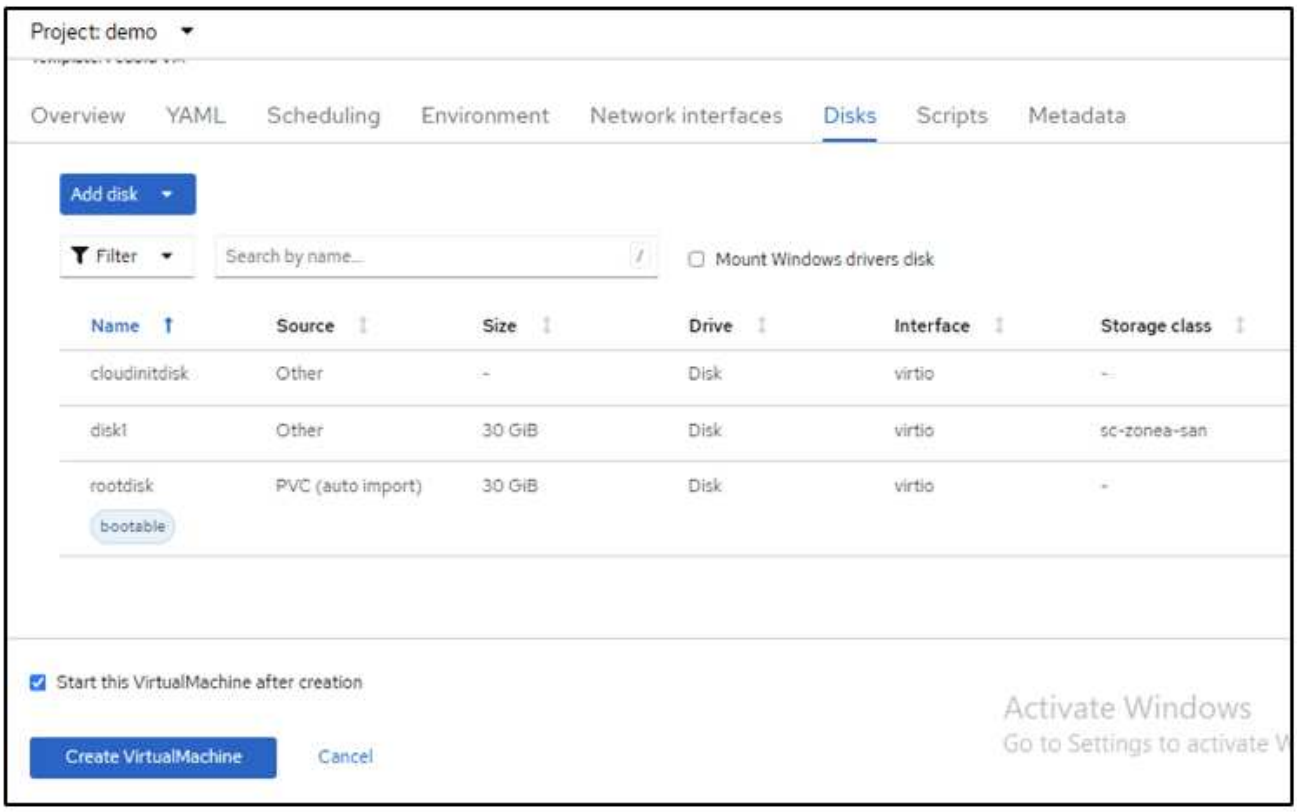



Catalog
VirtualMachines
Templates
InstanceTypes
Preferences
Bootable volumes
MigrationPolicies
Checkups
Migration
Networking
Storage
PersistentVolumes
Project: demo
VirtualMachines
No VirtualMachines found
Click Create VirtualMachine to create your first VirtualMachine or view the catalog tab to
Create VirtualMachine
From InstanceType
From template
With YAML


Fedora VM
fedora-server-small
Template info
Operating system
Fedora VM
Workload type
Server (default)
Description
Template for Fedora Linux 39 VM or newer. A PVC with the Fedora disk image must be
Storage
Boot from CD
Disk source *
Template default
Disk size *
30
GiB
Quick create VirtualMachine
VirtualMachine name *
demo-fedora
Project
demo
Public SSH key
Not configured
Start this VirtualMachine after creation
Quick create VirtualMachine
Customize VirtualMachine
Cancel
Activate Windows
Go to Settings to activate Windows.


Catalog
Customize and create VirtualMachine
YAML
Template: Fedora VM
Overview
YAML
Scheduling
Environment
Network interfaces
Disks
Scripts
Metadata
Add disk
Empty disk (blank)
Create a disk with no contents.
Use existing
Ephemeral disk (Container image)
Any changes are lost upon reboot
Volume
Add a volume already available on the cluster.
Volume snapshot
Add a snapshot available on the cluster to the VirtualMachine.
Clone volume
Clone a volume available on the cluster and add it to the VirtualMachine.
Mount Windows drivers disk
Drive
Interface
Storage class
Disk
virtio
-
Disk
virtio
-
Create VirtualMachine
Cancel
Activate Windows
Go to Settings to activate Window


Add disk
disk1
Disk size *
30
GiB
Type
Disk
Hot plug is enabled only for "Disk" and "Lun" types
Interface *
VirtIO
Hot plug is enabled only for "SCSI" interface
StorageClass
SC sc-zonea-san
Apply optimized StorageProfile settings
Optimized values Access mode: ReadWriteMany, Volume mode: Block.
Save
Cancel




```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   2m54s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          110s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

앱 만들기

▼ 앱 만들기

VM용 Trident Protect 앱을 생성하세요

이 예에서 demo 네임스페이스에는 하나의 VM이 있으며 앱을 생성할 때 네임스페이스의 모든 리소스가 포함됩니다.

```
# alias tp='tridentctl-protect'
# tp create app demo-vm --namespaces demo -n demo --dry-run > app.yaml

# cat app.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-vm
  namespace: demo
```

```
spec:
  includedNamespaces:
  - namespace: demo
# oc create -f app.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+---------+------------+-------+-----+
|  NAME   | NAMESPACES | STATE | AGE |
+---------+------------+-------+-----+
| demo-vm | demo       | Ready | 45s |
+---------+------------+-------+-----+
[root@localhost VM-DataProtection]#
```

백업을 만들어 앱을 보호하세요

▼ 백업 만들기

주문형 백업 만들기

이전에 만든 앱(demo-vm)에 대한 백업을 만들고, 이 백업에는 demo 네임스페이스의 모든 리소스가 포함됩니다. 백업이 저장될 AppVault 이름을 입력하세요.

```
# tp create backup demo-vm-backup-on-demand --app demo-vm --appvault
ontap-s3-appvault -n demo
Backup "demo-vm-backup-on-demand" created.
```

```
[root@localhost VM-DataProtection]# tp get backup -n demo
+--------------------------+---------+----------------+-----------+-------+--------+
|           NAME           |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+--------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand | demo-vm | Retain         | Completed |       | 12m53s |
+--------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

일정에 따라 백업 만들기

보존할 백업의 세분성과 개수를 지정하여 백업 일정을 만듭니다.

```
# tp create schedule backup-schedule1 --app demo-vm --appvault ontap-s3-
appvault --granularity Hourly --minute 45 --backup-retention 1 -n demo
--dry-run>backup-schedule-demo-vm.yaml
schedule.protect.trident.netapp.io/backup-schedule1 created
```

```
#cat backup-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: backup-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "1"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "45"
  recurrenceRule: ""
  snapshotRetention: "0"
status: {}
# oc create -f backup-schedule-demo-vm.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+------------------+---------+---------------+---------+-------+-------+-----+
|       NAME       |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR | AGE |
+------------------+---------+---------------+---------+-------+-------+-----+
| backup-schedule1 | demo-vm | Hourly:min=45 | true    |       |       | 9s  |
+------------------+---------+---------------+---------+-------+-------+-----+
```

```
[root@localhost VM-DataProtection]# tp get backups -n demo
+-----------------------------+---------+----------------+-----------+-------+--------+
|            NAME             |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-----------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand    | demo-vm | Retain         | Completed |       | 44m4s  |
| hourly-4c094-20250312144500 | demo-vm | Retain         | Completed |       | 20m34s |
+-----------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

백업에서 복원

▼ 백업에서 복원

VM을 동일한 네임스페이스로 복원

예시에서 백업 demo-vm-backup-on-demand에는 Fedora VM용 demo-app을 사용한 백업이 포함되어 있습니다.

먼저 VM을 삭제하고 PVC, Pod 및 VM 개체가 "demo" 네임스페이스에서 삭제되었는지 확인하세요.

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   59m   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          58m

NAME                                                  STATUS   VOLUME                                     CAPACITY
CLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                     Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi
a-san   <unset>                 59m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi
a-san   <unset>                 59m
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc delete vm demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
No resources found in demo namespace.
[root@localhost VM-DataProtection]#
```

이제 백업-인-플레이스 복원 개체를 만듭니다.

```
# tp create bir demo-fedora-restore --backup demo/demo-vm-backup-on-
demand -n demo --dry-run>vm-demo-bir.yaml

# cat vm-demo-bir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo-fedora-restore
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/demo-vm-backup-on-demand_f6af3513-9739-480e-88c7-
4cca45808a80
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-bir.yaml -n demo
backupinplacerestore.protect.trident.netapp.io/demo-fedora-restore
created
```

```
[root@localhost VM-DataProtection]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo-fedora-restore | ontap-s3-appvault | Completed |       | 28m17s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

VM, Pod 및 PVC가 복구되었는지 확인하세요.

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   116s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-9kfxh   1/1     Running   0          116s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

VM을 다른 네임스페이스로 복원

먼저 앱을 복원할 새 네임스페이스를 만듭니다. 이 예에서는 demo2입니다. 그런 다음 백업 복원 개체를 만듭니다.

```
# tp create br demo2-fedora-restore --backup demo/hourly-4c094-
20250312154500 --namespace-mapping demo:demo2 -n demo2 --dry-run>vm
-demo2-br.yaml

# cat vm-demo2-br.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo2-fedora-restore
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/hourly-4c094-20250312154500_aaa14543-a3fa-41f1-
a04c-44b1664d0f81
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
  conditions: null
```

```
  postRestoreExecHooksRunResults: null
  state: ""
# oc create -f vm-demo2-br.yaml -n demo2
```

```
[root@localhost VM-DataProtection]# tp get br -n demo2
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-fedora-restore | ontap-s3-appvault | Completed |       | 38m52s |
+----------------------+--------------------+-----------+-------+--------+
```

VM, Pod, PVC가 새 네임스페이스 demo2에 생성되었는지 확인합니다.

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                   AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

스냅샷을 사용하여 앱 보호

▼ 스냅샷 만들기

주문형 스냅샷 만들기 앱에 대한 스냅샷을 만들고 저장해야 하는 AppVault를 지정합니다.

```
# tp create snapshot demo-vm-snapshot-ondemand --app demo-vm --appvault
ontap-s3-appvault -n demo --dry-run
# cat demo-vm-snapshot-on-demand.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  creationTimestamp: null
  name: demo-vm-snapshot-ondemand
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  completionTimeout: 0s
  volumeSnapshotsCreatedTimeout: 0s
  volumeSnapshotsReadyToUseTimeout: 0s
status:
  conditions: null
  postSnapshotExecHooksRunResults: null
  preSnapshotExecHooksRunResults: null
```

```
  state: ""

# oc create -f demo-vm-snapshot-on-demand.yaml
snapshot.protect.trident.netapp.io/demo-vm-snapshot-ondemand created
```

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

스냅샷 일정 만들기 스냅샷 일정을 만듭니다. 보존할 스냅샷의 세분성과 개수를 지정합니다.

```
# tp create Schedule snapshot-schedule1 --app demo-vm --appvault ontap-s3-appvault --granularity Hourly --minute 50 --snapshot-retention 1 -n demo --dry-run>snapshot-schedule-demo-vm.yaml

# cat snapshot-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: snapshot-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "0"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "50"
  recurrenceRule: ""
  snapshotRetention: "1"
status: {}

# oc create -f snapshot-schedule-demo-vm.yaml
schedule.protect.trident.netapp.io/snapshot-schedule1 created
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+--------------------+---------+---------------+---------+-------+-------+-------+
|        NAME        |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR |  AGE  |
+--------------------+---------+---------------+---------+-------+-------+-------+
| backup-schedule1   | demo-vm | Hourly:min=45 | true    |       |       | 5d23h |
| snapshot-schedule1 | demo-vm | Hourly:min=50 | true    |       |       | 12s   |
+--------------------+---------+---------------+---------+-------+-------+-------+
[root@localhost VM-DataProtection]#
```

```
[root@localhost VM-DataProtection]# tp get snapshots -n demo
+-------------------------------------------+---------+----------------+-----------+-------+--------+
|                   NAME                    |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-------------------------------------------+---------+----------------+-----------+-------+--------+
| backup-39b67e1c-f875-4045-93df-78634bae9dfb | demo-vm | Delete         | Completed |       | 6m29s  |
| demo-vm-snapshot-ondemand                 | demo-vm | Delete         | Completed |       | 21m30s |
| hourly-51839-20250318135000               | demo-vm | Delete         | Completed |       | 1m29s  |
+-------------------------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

스냅샷에서 복원

▼ 스냅샷에서 복원

스냅샷에서 동일한 네임스페이스로 **VM** 복원 demo2 네임스페이스에서 VM demo-fedora를 삭제합니다.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   28h   Running   True

NAME                                                    STATUS   VOLUME
ORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                       Bound    pvc-e0d5f79d-dff9-450d-be0e-90ab6880b7af
-zonea-san   <unset>                 28h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-e6f7890a-70c7-4538-9035-5e2e9379511d
-zonea-san   <unset>                 28h
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost RedHat]#
```

VM의 스냅샷에서 스냅샷-인-플레이스-복원 개체를 만듭니다.

```
# tp create sir demo-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand -n demo --dry-run>vm-demo-sir.yaml

# cat vm-demo-sir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  creationTimestamp: null
  name: demo-fedora-restore-from-snapshot
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
```

```
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  conditions: null
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-sir.yaml
snapshotinplacerestore.protect.trident.netapp.io/demo-fedora-restore-
from-snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sir -n demo
+-----------------------------------+-------------------+-----------+-------+--------+
|               NAME                |     APPVAULT      |   STATE   | ERROR |  AGE   |
+-----------------------------------+-------------------+-----------+-------+--------+
| demo-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 58m17s |
+-----------------------------------+-------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

VM과 해당 PVC가 데모 네임스페이스에 생성되었는지 확인합니다.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m17s   Running   True

NAME                                                  STATUS   VOLUME
persistentvolumeclaim/demo-fedora                     Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
[root@localhost RedHat]#
```

스냅샷에서 다른 네임스페이스로 **VM** 복원

이전에 백업에서 복원한 demo2 네임스페이스의 VM을 삭제합니다.

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   3m12s   Running   True
virtualmachine.kubevirt.io/demo-fedora   3m11s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-w77rr   1/1     Running   0          3m11s
pod/virt-launcher-demo-fedora-wwdtc   1/1     Running   0          3m11s

NAME                                                  STATUS   VOLUME                                     CAPACITY   ACCESS MODES
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                     Bound    pvc-7aafd5e2-d4cf-4af6-a259-c68e016ec6cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m26s
persistentvolumeclaim/demo-fedora                     Bound    pvc-c1f8145a-56ea-42c5-abb4-6457b6853e1c   30Gi       RWX
  sc-zonea-san   <unset>                 3m25s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-e82b6d98-6762-4473-9bb8-7e98efcb7987   30Gi       RWX
  sc-zonea-san   <unset>                 3m20s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-ee13cfbc-2921-4129-a214-a0f6b10335cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m16s
[root@localhost VM-DataProtection]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo2
virtualmachine.kubevirt.io "demo-fedora" deleted
```

스냅샷에서 스냅샷 복원 개체를 만들고 네임스페이스 매핑을 제공합니다.

```
# tp create sr demo2-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand --namespace-mapping demo:demo2 -n demo2 --dry
-run>vm-demo2-sr.yaml

# cat vm-demo2-sr.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  creationTimestamp: null
  name: demo2-fedora-restore-from-snapshot
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo2-sr.yaml
snapshotrestore.protect.trident.netapp.io/demo2-fedora-restore-from-
snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sr -n demo2
+-----------------------------------+-------------------+-----------+-------+--------+
|                NAME               |     APPVAULT      |   STATE   | ERROR |  AGE   |
+-----------------------------------+-------------------+-----------+-------+--------+
| demo2-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 15m22s |
+-----------------------------------+-------------------+-----------+-------+--------+
```

VM과 해당 PVC가 새 네임스페이스 demo2에 복원되었는지 확인합니다.

```
[root@localhost RedHat]# oc get vm,pvc -n demo2
NAME                                      AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora    29h   Running   True

NAME                                                          STATUS   VOLUME
STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                             Bound    pvc-35dcd9b2-4fca-486c-af9e-596bc5b4dc15
-zonea-san     <unset>                 29h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87         Bound    pvc-575a3111-382f-4933-a778-0089fa1ea2af
-zonea-san     <unset>                 29h
[root@localhost RedHat]#
```

특정 **VM** 복원

▼ 네임스페이스에서 특정 **VM**을 선택하여 스냅샷/백업을 생성하고 복원합니다.

이전 예에서는 네임스페이스 내에 단일 VM이 있었습니다. 백업에 전체 네임스페이스를 포함함으로써 해당 VM과 연관된 모든 리소스가 캡처되었습니다. 다음 예제에서는 동일한 네임스페이스에 다른 VM을 추가하고 레이블 선택기를 사용하여 이 새로운 VM에 대한 앱을 만듭니다.

demo 네임스페이스에 새 **VM(demo-centos vm)**을 만듭니다.

```
[root@localhost VM-DataProtection]# oc get vm,pod,pvc -n demo
NAME                                      AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos    2m47s   Running   True
virtualmachine.kubevirt.io/demo-fedora    81m     Running   True

NAME                                  READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-2nq6g   1/1     Running   0          113s
pod/virt-launcher-demo-fedora-9kfxh   1/1     Running   0          81m

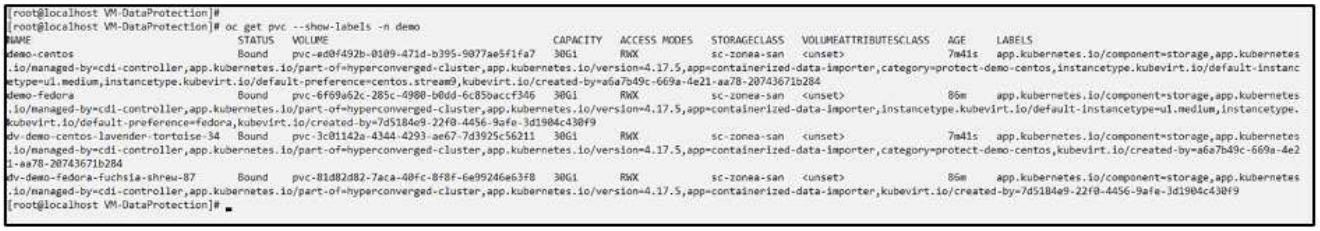
NAME                                                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-centos                             Bound    pvc-ed0f492b-0109-471d-b395-9077ae5f1fa7   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/demo-fedora                             Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34     Bound    pvc-3c01142a-4344-4293-ae67-7d3925c56211   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87         Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

demo-centos vm 및 관련 리소스에 레이블을 지정합니다.

```
[root@localhost VM-DataProtection]# oc label vm demo-centos category=protect-demo-centos -n demo
virtualmachine.kubevirt.io/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc demo-centos category=protect-demo-centos -n demo
persistentvolumeclaim/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc dv-demo-centos-lavender-tortoise-34 category=protect-demo-centos -n demo
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34 labeled
[root@localhost VM-DataProtection]#
```

demo-centos vm 및 **pvcs**에 레이블이 지정되었는지 확인하세요.

```
[root@localhost VM-DataProtection]# oc get vm --show-labels -n demo
NAME          AGE     STATUS    READY   LABELS
demo-centos   6m31s   Running   True    app=demo-centos,category=protect-demo-centos,kubevirt.io/dynamic-credentials-support=true,vm.kubevirt.io/template.namespace=openshift,vm.kubevirt.io/template.revision=1,vm.kubevirt.io/template.version=v0.31.1,vm.kubevirt.io/template=centos-stream9-server-small
demo-fedora   85m     Running   True    app=demo-fedora,vm.kubevirt.io/template.namespace=openshift,vm.kubevirt.io/template.revision=1,vm.kubevirt.io/template.version=v0.31.1,vm.kubevirt.io/template=fedora-server-small
[root@localhost VM-DataProtection]#
```



레이블 선택기를 사용하여 특정 **VM(demo-centos)**에 대한 앱만 만들기

```
# tp create app demo-centos-app --namespaces 'demo(category=protect-
demo-centos)' -n demo --dry-run>demo-centos-app.yaml

# cat demo-centos-app.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-centos-app
  namespace: demo
spec:
  includedNamespaces:
  - labelSelector:
      matchLabels:
        category: protect-demo-centos
    namespace: demo
status:
  conditions: null

# oc create -f demo-centos-app.yaml -n demo
application.protect.trident.netapp.io/demo-centos-app created
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+-----------------+------------+-------+------+
|      NAME       | NAMESPACES | STATE | AGE  |
+-----------------+------------+-------+------+
| demo-centos-app | demo       | Ready | 56s  |
| demo-vm         | demo       | Ready | 4h6m |
+-----------------+------------+-------+------+
```

필요에 따라 일정에 따라 백업과 스냅샷을 만드는 방법은 이전에 보여준 것과 동일합니다. 스냅샷이나 백업을 생성하는 데 사용되는 trident-protect 앱에는 네임스페이스의 특정 VM만 포함되어 있으므로, 이를 복원하면 특정 VM만 복원됩니다. 아래는 백업/복원 작업의 예를 보여줍니다.

해당 앱을 사용하여 네임스페이스의 특정 **VM** 백업을 만듭니다.

이전 단계에서는 레이블 선택기를 사용하여 demo 네임스페이스에 centos vm만 포함하도록 앱을 만들었습니다. 이 앱에 대한 백업(이 예에서는 주문형 백업)을 만듭니다.

```
# tp create backup demo-centos-backup-on-demand --app demo-centos-app
--appvault ontap-s3-appvault -n demo
Backup "demo-centos-backup-on-demand" created.
```

```
+-------------------------------+-----------------+----------------+-----------+-------+--------+
|             NAME              |       APP       | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-------------------------------+-----------------+----------------+-----------+-------+--------+
| demo-centos-backup-on-demand | demo-centos-app | Retain         | Completed |       | 13m22s |
| demo-vm-backup-on-demand     | demo-vm         | Retain         | Completed |       | 4h19m  |
| hourly-4c094-20250312174500  | demo-vm         | Retain         | Completed |       | 56m17s |
+-------------------------------+-----------------+----------------+-----------+-------+--------+
```

특정 **VM**을 동일한 네임스페이스로 복원 특정 VM(centos)의 백업은 해당 앱을 사용하여 생성되었습니다. 여기에서 백업-인-플레이스-복원이나 백업-복원이 생성되면 해당 VM만 복원됩니다. Centos VM을 삭제합니다.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                      AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos    4m27s   Running   True
virtualmachine.kubevirt.io/demo-fedora    4m27s   Running   True

NAME                                                                STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                                   Bound    pvc-e8faeaf8-fc0c-4d92-96de-c83a335a7a17
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/demo-fedora                                   Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34           Bound    pvc-66eb7996-1420-4513-a67c-2824f08534da
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87               Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
  sc-zonea-san   <unset>                 4m32s
```

```
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-centos -n demo
virtualmachine.kubevirt.io "demo-centos" deleted
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                      AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora    5m17s   Running   True

NAME                                                        STATUS   VOLUME
persistentvolumeclaim/demo-fedora                           Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
```

demo-centos-backup-on-demand에서 백업 인플레이스 복원을 생성하고 CentOS VM이 다시 생성되었는지 확인합니다.

```
#tp create bir demo-centos-restore --backup demo/demo-centos-backup-on-
demand -n demo
BackupInplaceRestore "demo-centos-restore" created.
```

```
[root@localhost RedHat]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+-------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE  |
+----------------------+--------------------+-----------+-------+-------+
| demo-centos-restore  | ontap-s3-appvault  | Completed |       | 57m9s |
| demo-fedora-restore  | ontap-s3-appvault  | Completed |       | 7d5h  |
+----------------------+--------------------+-----------+-------+-------+
```

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   29m   Running   True
virtualmachine.kubevirt.io/demo-fedora   85m   Running   True

NAME                                                    STATUS   VOLUME                                     C
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-82954bf7-4a7e-4e0c-9a04-4fa152e1b0ef   1
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc   1
  sc-zonea-san   <unset>                 85m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-2a8d4eb5-ed6d-4408-b85d-e218e9a5d4b0   1
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c   1
  sc-zonea-san   <unset>                 85m
[root@localhost RedHat]#
```

특정 **VM**을 다른 네임스페이스로 복원 demo-centos-backup-on-demand에서 다른 네임스페이스(demo3)로 백업 복원을 만들고 centos VM이 다시 생성되었는지 확인합니다.

```
# tp create br demo2-centos-restore --backup demo/demo-centos-backup-on-demand --namespace-mapping demo:demo3 -n demo3
BackupRestore "demo2-centos-restore" created.
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# tp get br -n demo3
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-centos-restore | ontap-s3-appvault  | Completed |       | 52m57s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost RedHat]#
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# oc get vm,pvc -n demo3
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   19m   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-0a14e38f-07de-4e09-8f88-14a9a8bb45c2
  sc-zonea-san   <unset>                 19m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-d4f9cf2f-264c-4d02-94bf-0db28b427acc
  sc-zonea-san   <unset>                 19m
[root@localhost RedHat]#
```

비디오 데모

다음 비디오는 스냅샷을 사용하여 VM을 보호하는 방법을 보여줍니다.

VM 보호

타사 도구를 사용하여 컨테이너 앱 보호

OpenShift API for Data Protection(OADP)을 사용하여 **OpenShift Container Platform**의 컨테이너 앱에 대한 데이터 보호

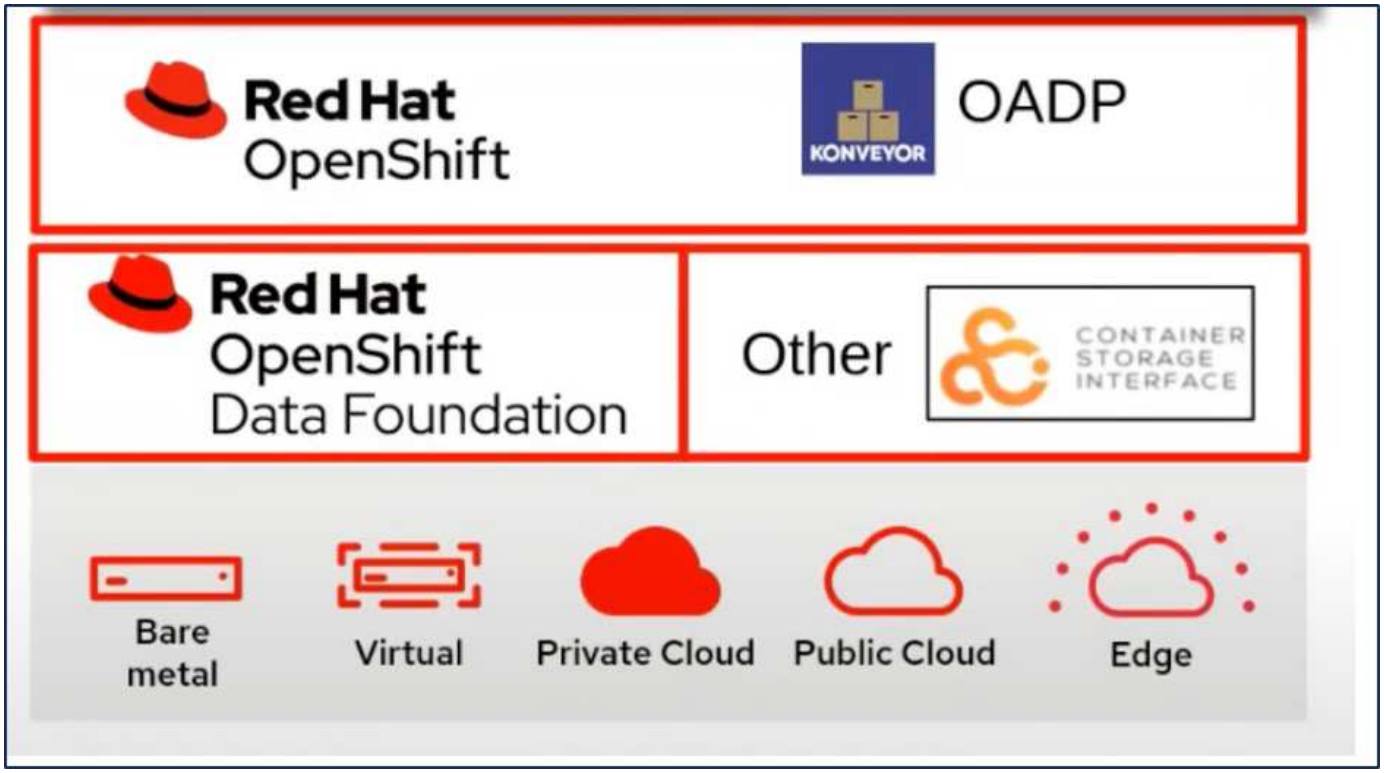
이 참조 문서 섹션에서는 NetApp ONTAP S3 또는 NetApp StorageGRID S3에서 Velero와 함께 OpenShift API for Data Protection(OADP)을 사용하여 컨테이너 앱의 백업을 만드는 방법에 대한 세부 정보를 제공합니다. 앱의 영구 볼륨(PV)을 포함한 네임스페이스 범위 리소스의 백업은 CSI Trident Snapshots를 사용하여 생성됩니다.

컨테이너 앱을 위한 영구 스토리지는 "Trident CSI"를 사용하여 OpenShift 클러스터에 통합된 ONTAP 스토리지로 지원될 수 있습니다. 이 섹션에서는 "데이터 보호를 위한 OpenShift API(OADP)"를 사용하여 데이터 볼륨을 포함한 앱의 백업을 다음으로 수행합니다.

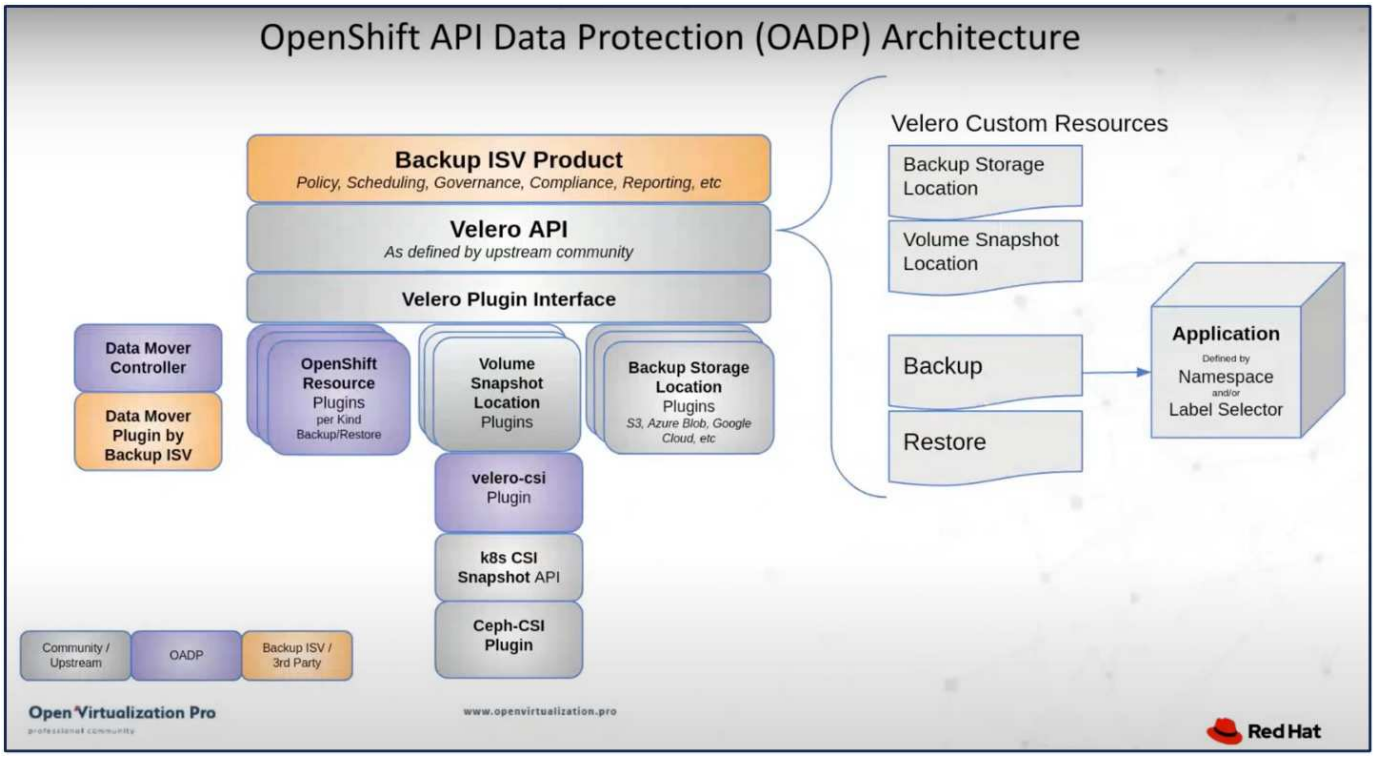
- ONTAP 객체 스토리지
- 스토리지그리드

필요할 때 백업에서 복원합니다. 백업이 생성된 클러스터에만 앱을 복원할 수 있습니다.

OADP를 사용하면 OpenShift 클러스터에서 애플리케이션의 백업, 복원 및 재해 복구가 가능합니다. OADP로 보호할 수 있는 데이터에는 Kubernetes 리소스 개체, 영구 볼륨 및 내부 이미지가 포함됩니다.



Red Hat OpenShift는 오픈소스 커뮤니티에서 개발한 솔루션을 활용하여 데이터 보호를 구현했습니다. "벨레로" Kubernetes 클러스터 리소스와 영구 볼륨을 안전하게 백업하고 복원하고, 재해 복구를 수행하고, 마이그레이션하는 오픈 소스 도구입니다. Velero를 쉽게 사용할 수 있도록 OpenShift는 OADP 연산자와 Velero 플러그인을 개발하여 CSI 스토리지 드라이버와 통합했습니다. 공개된 OADP API의 핵심은 Velero API를 기반으로 합니다. OADP 운영자를 설치하고 구성한 후에는 Velero API에서 제공하는 작업에 따라 백업/복원 작업을 수행할 수 있습니다.



OADP 1.3은 OpenShift 클러스터 4.12 이상의 운영자 허브에서 사용할 수 있습니다. CSI 볼륨 스냅샷을 원격 개체 저장소로 옮길 수 있는 내장형 Data Mover가 있습니다. 이렇게 하면 백업하는 동안 스냅샷을 개체 스토리지 위치로 이동하여 이동성과 내구성을 제공합니다. 재난 발생 후 스냅샷을 복원하는 데 사용할 수 있습니다.

다음은 이 섹션의 예제에 사용된 다양한 구성 요소의 버전입니다.

- 오픈시프트 클러스터 4.14
- Red Hat에서 제공하는 OADP Operator 1.13
- Linux용 Velero CLI 1.13
- Trident 24.02
- ONTAP 9.12
- helm을 사용하여 postgresql을 설치했습니다.

"Trident CSI" "데이터 보호를 위한 OpenShift API(OADP)" "벨레로"

데이터 보호를 위한 **OpenShift API(OADP)** 운영자 설치

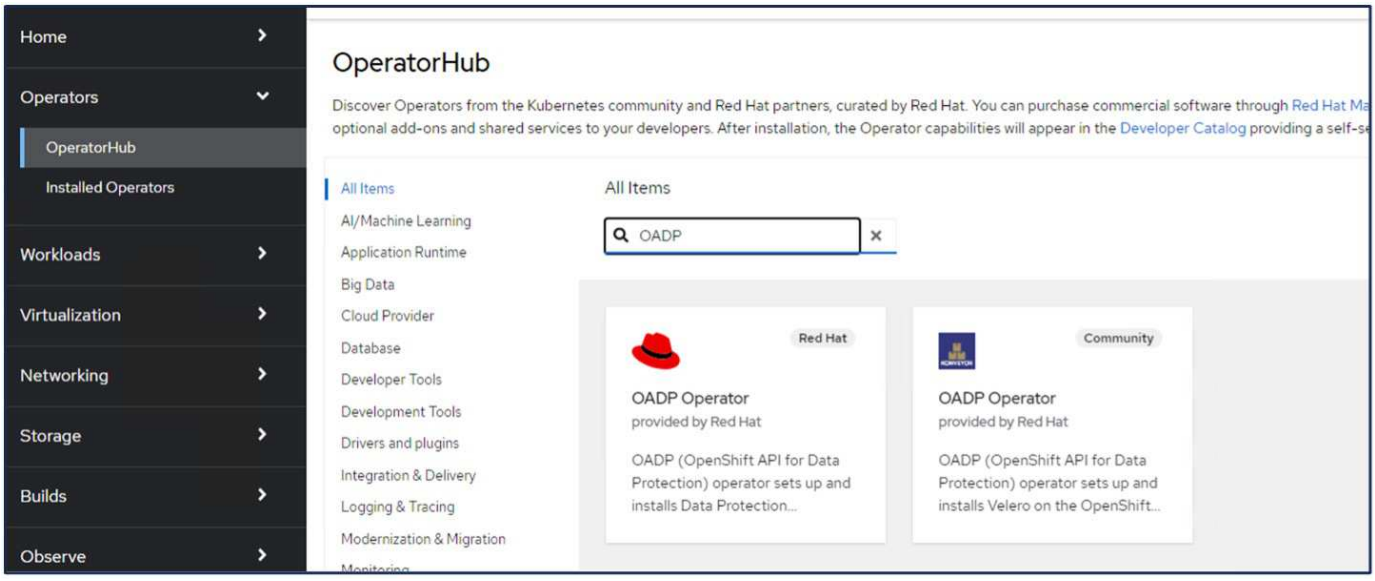
이 섹션에서는 OADP(OpenShift API for Data Protection) Operator를 설치하는 방법을 간략하게 설명합니다.

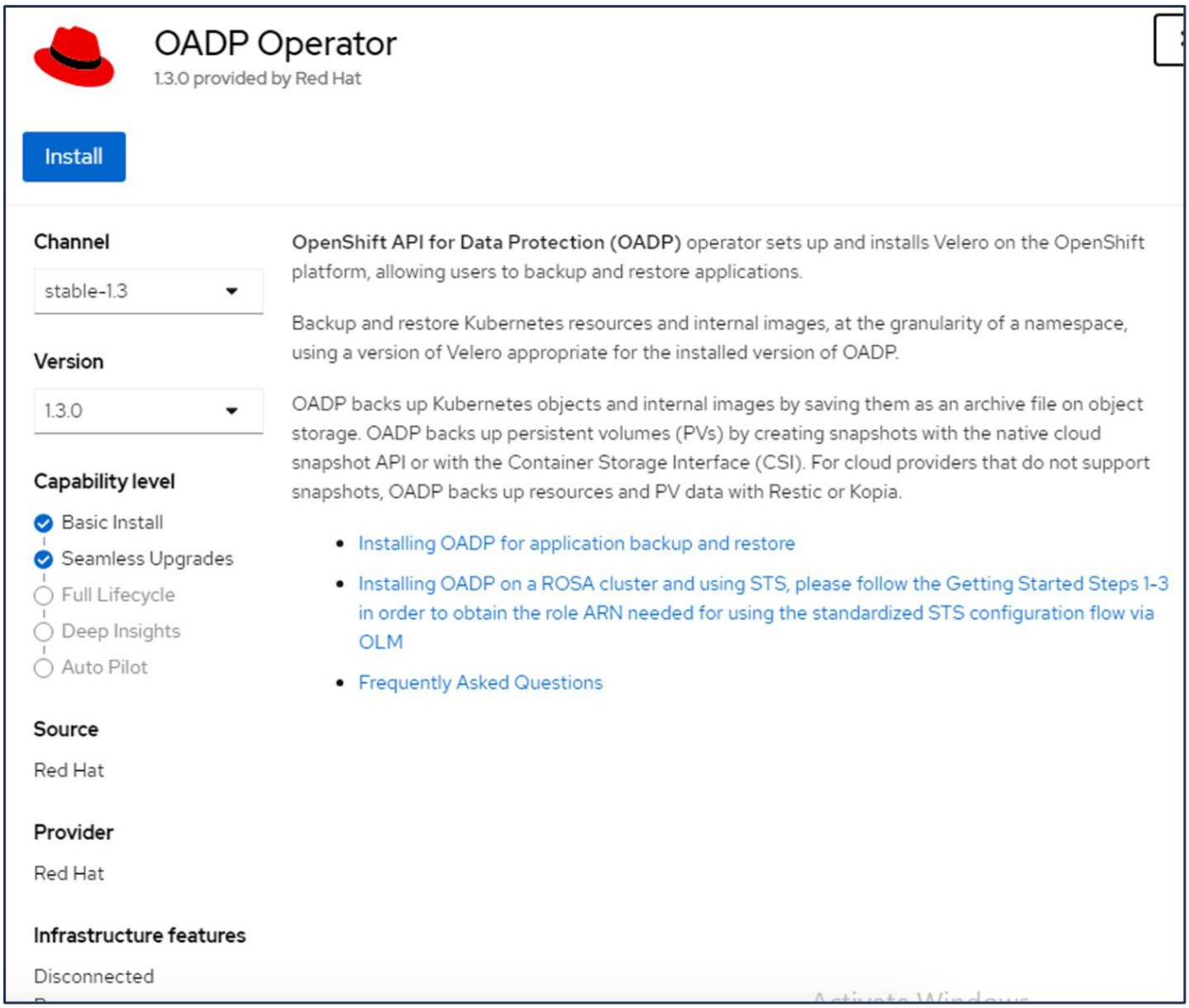
필수 조건

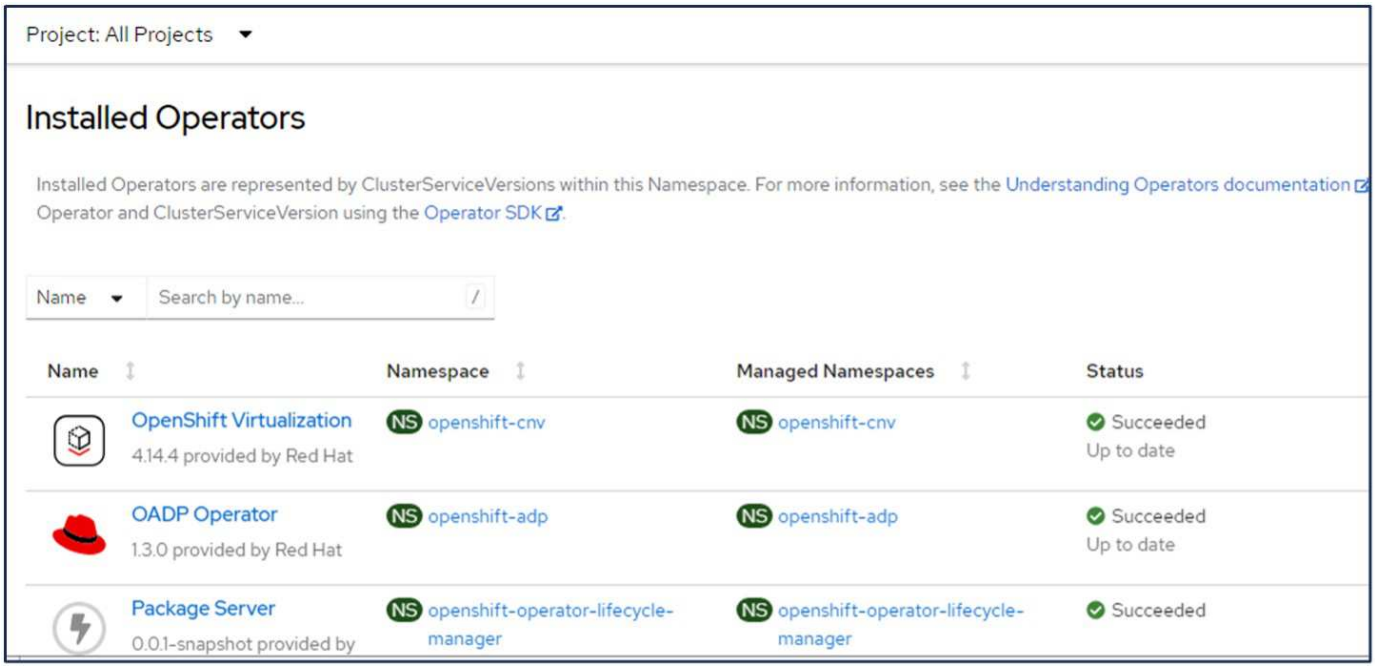
- RHCOS 작업자 노드가 있는 베어 메탈 인프라에 설치된 Red Hat OpenShift 클러스터(버전 4.12 이상)
- Trident 사용하여 클러스터와 통합된 NetApp ONTAP 클러스터
- ONTAP 클러스터의 SVM으로 구성된 Trident 백엔드
- Trident 프로비저너로 사용하여 OpenShift 클러스터에 구성된 StorageClass
- 클러스터에 생성된 Trident Snapshot 클래스
- Red Hat OpenShift 클러스터에 대한 클러스터 관리자 액세스
- NetApp ONTAP 클러스터에 대한 관리자 액세스
- 클러스터에 배포된 postgresql과 같은 애플리케이션
- $PATH에 tridentctl 및 oc 도구가 설치되고 추가된 관리자 워크스테이션

OADP Operator 설치 단계

1. 클러스터의 운영자 허브로 이동하여 Red Hat OADP 운영자를 선택합니다. 설치 페이지에서 모든 기본 선택 사항을 사용하고 설치를 클릭합니다. 다음 페이지에서도 기본값을 모두 사용하고 설치를 클릭합니다. OADP 운영자는 openshift-adp 네임스페이스에 설치됩니다.




OADP Operator
1.3.0 provided by Red Hat
Install
Channel
stable-1.3
Version
1.3.0
Capability level
Basic Install
Seamless Upgrades
Full Lifecycle
Deep Insights
Auto Pilot
Source
Red Hat
Provider
Red Hat
Infrastructure features
Disconnected
OpenShift API for Data Protection (OADP) operator sets up and installs Velero on the OpenShift platform, allowing users to backup and restore applications.
Backup and restore Kubernetes resources and internal images, at the granularity of a namespace, using a version of Velero appropriate for the installed version of OADP.
OADP backs up Kubernetes objects and internal images by saving them as an archive file on object storage. OADP backs up persistent volumes (PVs) by creating snapshots with the native cloud snapshot API or with the Container Storage Interface (CSI). For cloud providers that do not support snapshots, OADP backs up resources and PV data with Restic or Kopia.
Installing OADP for application backup and restore
Installing OADP on a ROSA cluster and using STS, please follow the Getting Started Steps 1-3 in order to obtain the role ARN needed for using the standardized STS configuration flow via OLM
Frequently Asked Questions


Project: All Projects
Installed Operators
Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the Understanding Operators documentation
Operator and ClusterServiceVersion using the Operator SDK
Name
Search by name...
Name
Namespace
Managed Namespaces
Status
OpenShift Virtualization
4.14.4 provided by Red Hat
openshift-cnv
openshift-cnv
Succeeded
Up to date
OADP Operator
1.3.0 provided by Red Hat
openshift-adp
openshift-adp
Succeeded
Up to date
Package Server
0.0.1-snapshot provided by
openshift-operator-lifecycle-manager
openshift-operator-lifecycle-manager
Succeeded

Ontap S3 세부 정보를 사용한 Velero 구성을 위한 전제 조건

운영자 설치가 성공적으로 완료되면 Velero 인스턴스를 구성합니다. Velero는 S3 호환 개체 스토리지를 사용하도록 구성할 수 있습니다. 다음 절차를 사용하여 ONTAP S3를 구성합니다."ONTAP 설명서의 개체 스토리지 관리 섹션" . Velero와 통합하려면 ONTAP S3 구성에서 다음 정보가 필요합니다.

- S3에 액세스하는 데 사용할 수 있는 논리 인터페이스(LIF)
- 액세스 키와 비밀 액세스 키가 포함된 S3에 액세스하기 위한 사용자 자격 증명
- 사용자에 대한 액세스 권한이 있는 백업을 위한 S3의 버킷 이름
- Object Storage에 안전하게 액세스하려면 Object Storage 서버에 TLS 인증서를 설치해야 합니다.

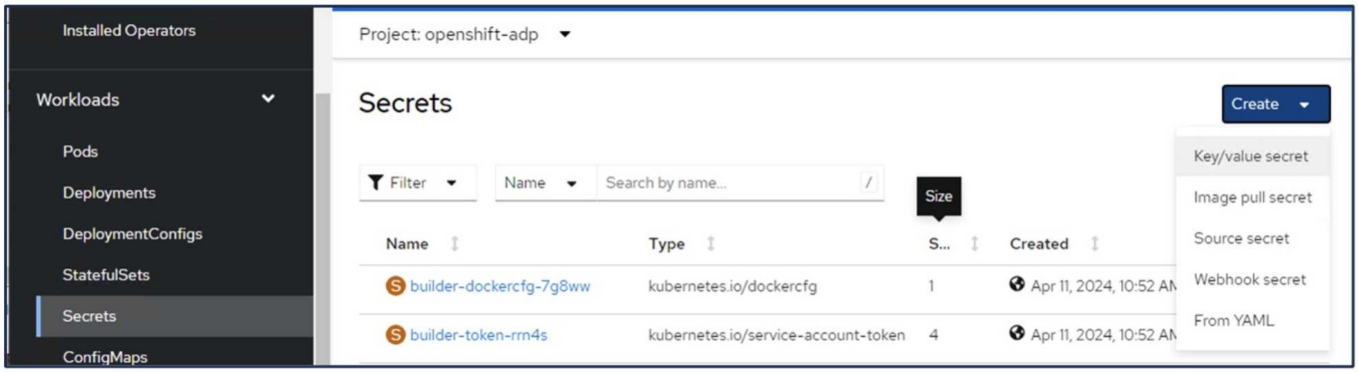
StorageGrid S3 세부 정보를 사용한 Velero 구성을 위한 필수 구성 요소

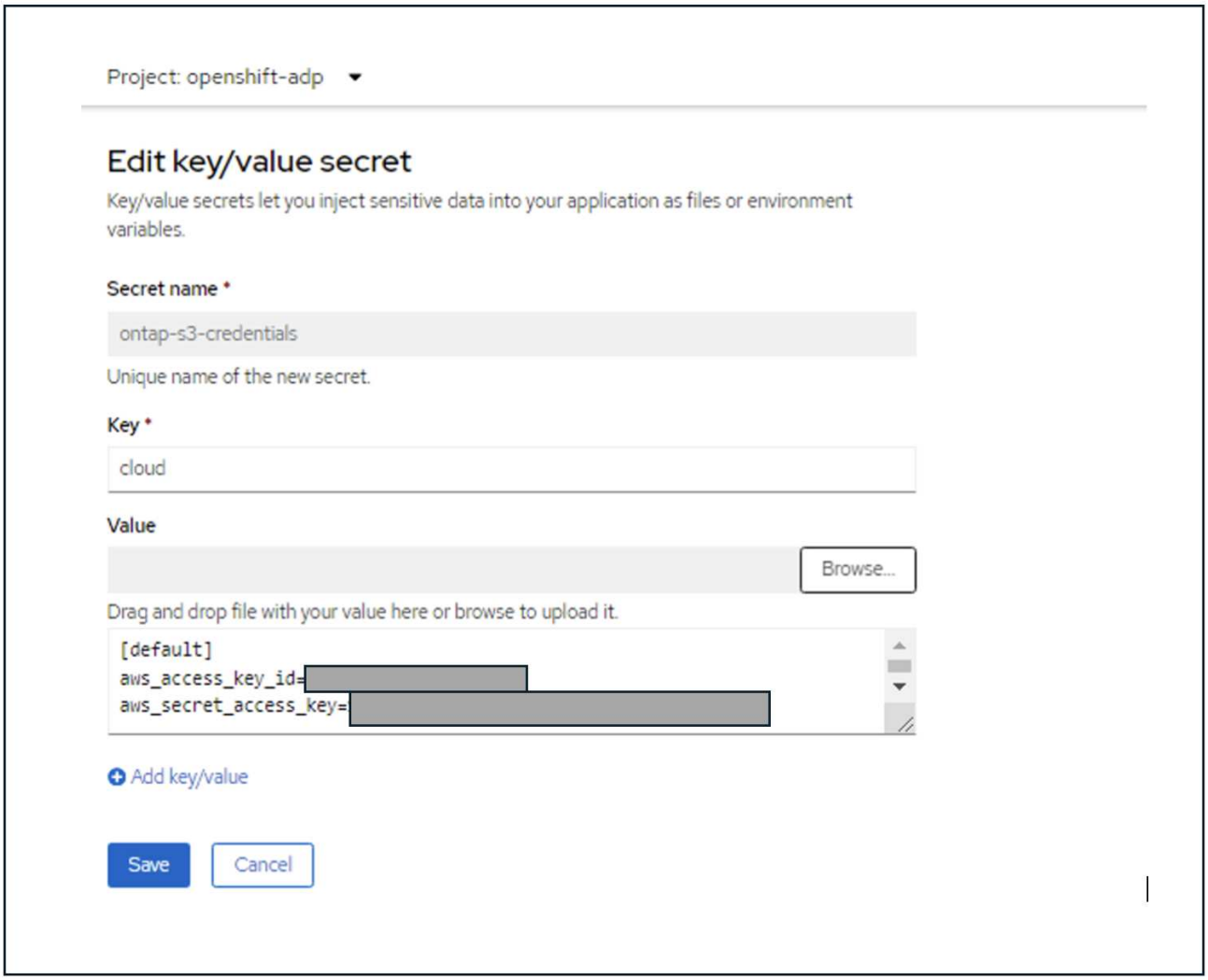
Velero는 S3 호환 개체 스토리지를 사용하도록 구성할 수 있습니다. 다음 절차에 따라 StorageGrid S3를 구성할 수 있습니다."StorageGrid 문서" . Velero와 통합하려면 StorageGrid S3 구성에서 다음 정보가 필요합니다.

- S3에 접속할 수 있는 엔드포인트
- 액세스 키와 비밀 액세스 키가 포함된 S3에 액세스하기 위한 사용자 자격 증명
- 사용자에 대한 액세스 권한이 있는 백업을 위한 S3의 버킷 이름
- Object Storage에 안전하게 액세스하려면 Object Storage 서버에 TLS 인증서를 설치해야 합니다.

Velero 구성 단계

- 먼저 ONTAP S3 사용자 자격 증명이나 StorageGrid 테넌트 사용자 자격 증명에 대한 비밀을 만듭니다. 이는 나중에 Velero를 구성하는 데 사용됩니다. CLI나 웹 콘솔에서 비밀을 생성할 수 있습니다. 웹 콘솔에서 비밀을 생성하려면 비밀을 선택한 다음 키/값 비밀을 클릭합니다. 표시된 대로 자격 증명 이름, 키 및 값에 대한 값을 제공합니다. 반드시 S3 사용자의 액세스 키 ID와 비밀 액세스 키를 사용하세요. 비밀에 적절한 이름을 붙이세요. 아래 샘플에서는 ontap-s3-credentials라는 이름의 ONTAP S3 사용자 자격 증명이 포함된 비밀이 생성됩니다.





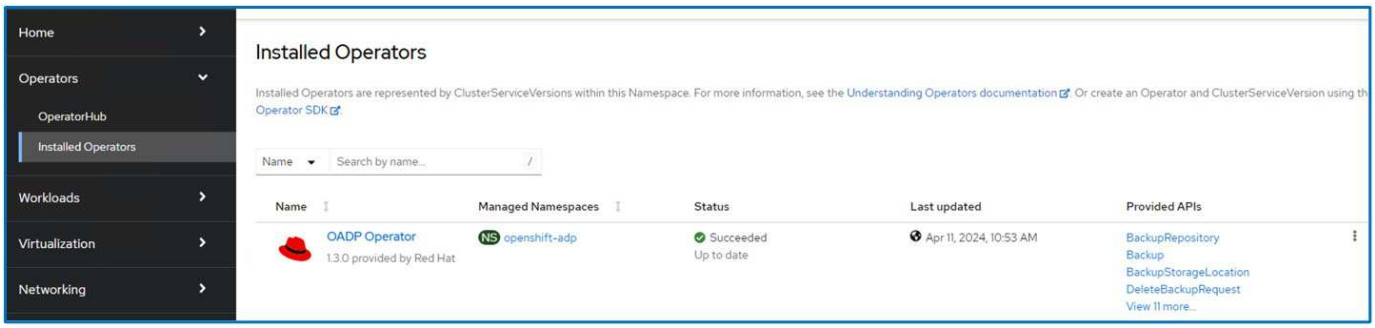
CLI에서 sg-s3-credentials라는 이름의 비밀을 생성하려면 다음 명령을 사용할 수 있습니다.

```
# oc create secret generic sg-s3-credentials --namespace openshift-adp --from-file
cloud=cloud-credentials.txt

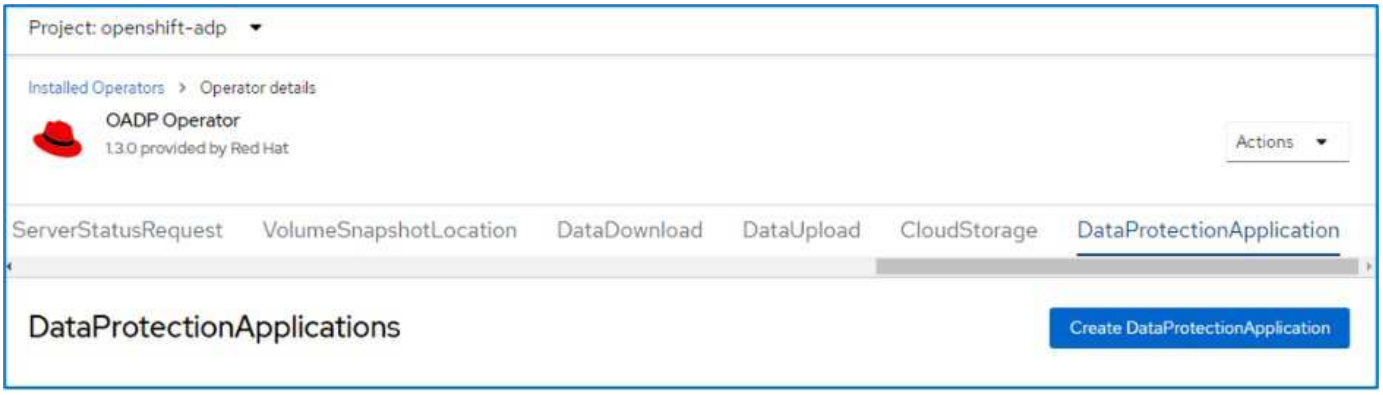
Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3
user in the following format:

[default]
aws_access_key_id=< Access Key ID of S3 user>
aws_secret_access_key=<Secret Access key of S3 user>
```

- 다음으로, Velero를 구성하려면 운영자 아래의 메뉴 항목에서 설치된 운영자를 선택하고, OADP 운영자를 클릭한 다음, **DataProtectionApplication** 탭을 선택합니다.



DataProtectionApplication 만들기를 클릭합니다. 양식 보기에서 DataProtection 애플리케이션의 이름을 제공하거나 기본 이름을 사용합니다.



이제 YAML 뷰로 가서 아래 yaml 파일 예시에 표시된 대로 사양 정보를 바꾸세요.

- ONTAP S3를 backupLocation으로 사용하여 Velero를 구성하기 위한 샘플 yaml 파일**

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false' ->use this for https
communication with ONTAP S3
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'  ->This allows use of IP in s3URL
          s3Url: 'https://10.61.181.161' ->Ensure TLS certificate for S3
is configured
        credential:
          key: cloud
          name: ontap-s3-credentials -> previously created secret
        default: true
        objectStorage:
          bucket: velero -> Your bucket name previously created in S3 for
backups
          prefix: container-demo-backup ->The folder that will be created
in the bucket
```

```
          caCert: <base64 encoded CA Certificate installed on ONTAP
Cluster with the SVM Scope where the bucker exists>
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
      #default Data Mover uses Kopia to move snapshots to Object Storage
    velero:
      defaultPlugins:
        - csi ->This plugin to use CSI snapshots
        - openshift
        - aws
        - kubevirt -> This plugin to use Velero with OIpenShift
Virtualization
```

StorageGrid S3를 **backupLocation**으로 사용하여 **Velero**를 구성하기 위한 샘플 **yaml** 파일

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true'
          profile: default
          region: us-east-1 ->region of your StorageGrid system
          s3ForcePathStyle: 'True'
          s3Url: 'https://172.21.254.25:10443' ->the IP used to access S3
        credential:
          key: cloud
          name: sg-s3-credentials ->secret created earlier
        default: true
        objectStorage:
          bucket: velero
          prefix: demobackup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
```

```
        - kubevirt
```

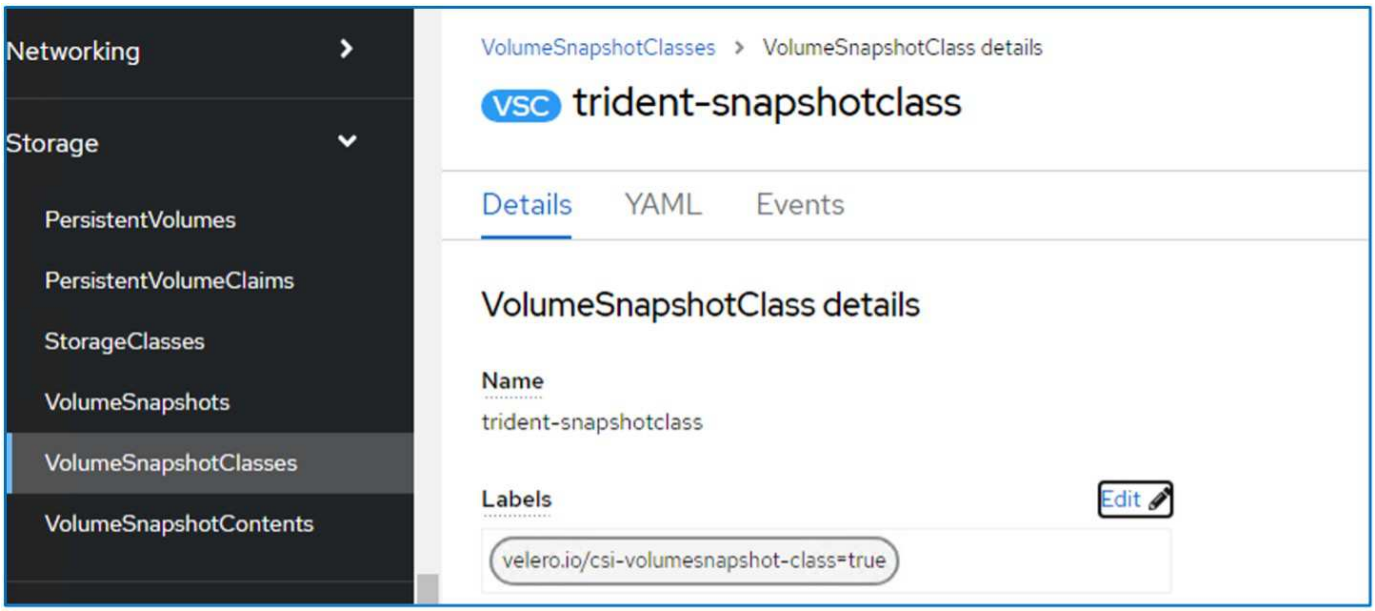
yaml 파일의 spec 섹션은 위의 예와 유사하게 다음 매개변수에 대해 적절하게 구성되어야 합니다.

backupLocations ONTAP S3 또는 StorageGrid S3(yaml에 표시된 자격 증명 및 기타 정보 포함)가 velero의 기본 BackupLocation으로 구성됩니다.

snapshotLocations CSI(Container Storage Interface) 스냅샷을 사용하는 경우 CSI 드라이버를 등록하기 위해 VolumeSnapshotClass CR을 생성하므로 스냅샷 위치를 지정할 필요가 없습니다. 우리의 예에서, 여러분은 Trident CSI를 사용하고 있으며, 이전에 Trident CSI 드라이버를 사용하여 VolumeSnapShotClass CR을 생성했습니다.

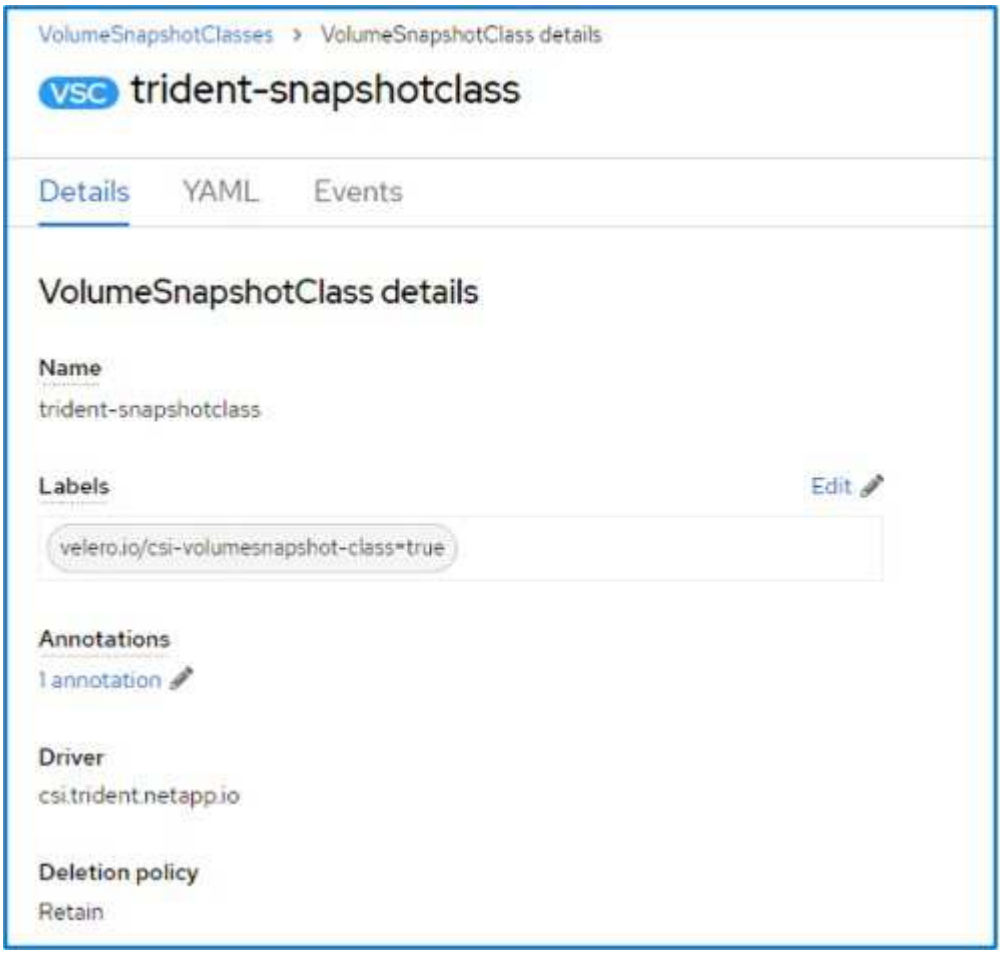
CSI 플러그인 활성화 Velero의 defaultPlugins에 csi를 추가하여 CSI 스냅샷으로 영구 볼륨을 백업합니다. CSI 지원 PVC를 백업하는 Velero CSI 플러그인은 **velero.io/csi-volumesnapshot-class** 레이블이 설정된 클러스터에서 VolumeSnapshotClass를 선택합니다. 이를 위해

- 트라이던트 VolumeSnapshotClass를 생성해야 합니다.
- 아래와 같이 trident-snapshotclass의 라벨을 편집하여 **velero.io/csi-volumesnapshot-class=true**로 설정합니다.

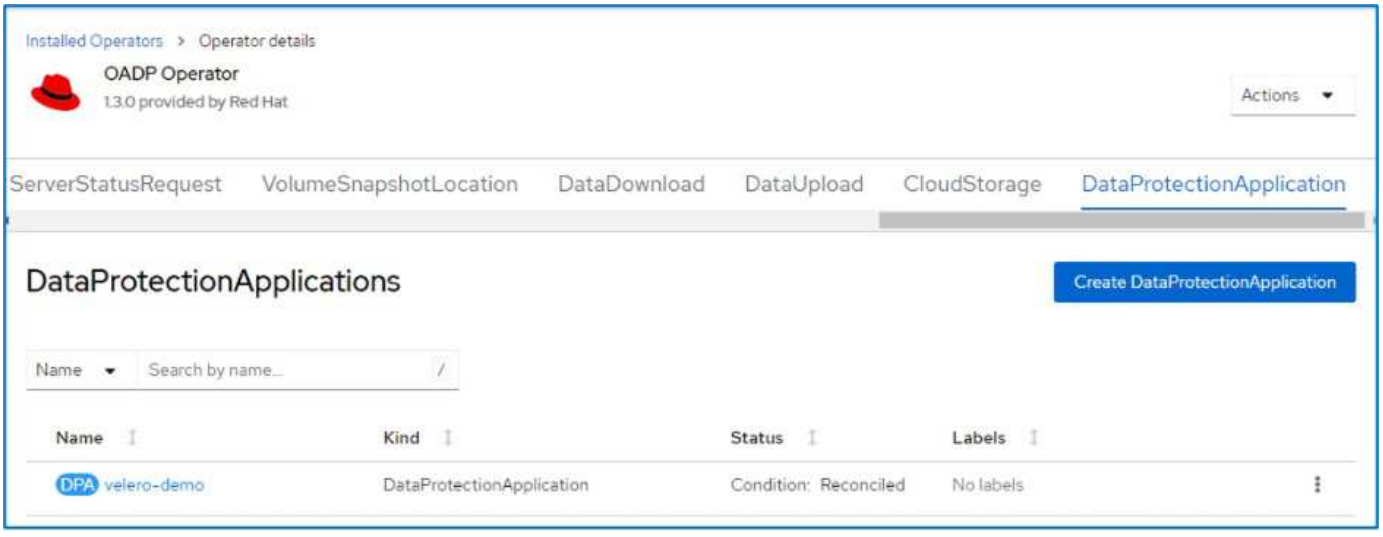


VolumeSnapshot 개체가 삭제된 경우에도 스냅샷이 유지되는지 확인하세요. *deletionPolicy*를 Retain으로 설정하면 됩니다. 그렇지 않은 경우 네임스페이스를 삭제하면 해당 네임스페이스에 백업된 모든 PVC가 완전히 손실됩니다.

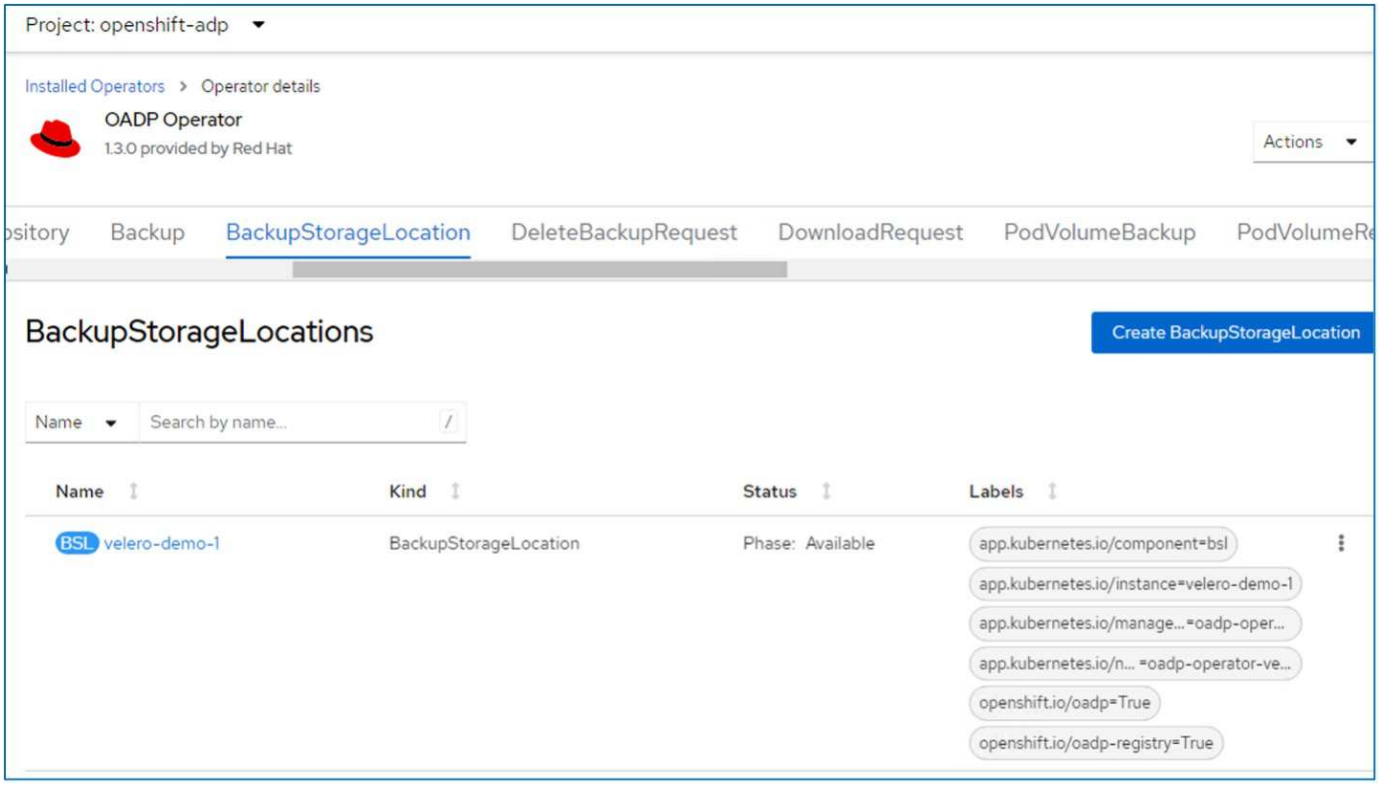
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



DataProtectionApplication이 생성되었고 조건이 Reconciled인지 확인하세요.



OADP 운영자는 해당 BackupStorageLocation을 생성합니다. 이는 백업을 생성할 때 사용됩니다.



OpenShift 컨테이너 플랫폼에서 앱에 대한 주문형 백업 생성

이 섹션에서는 OpenShift Virtualization에서 VM에 대한 주문형 백업을 생성하는 방법을 설명합니다.

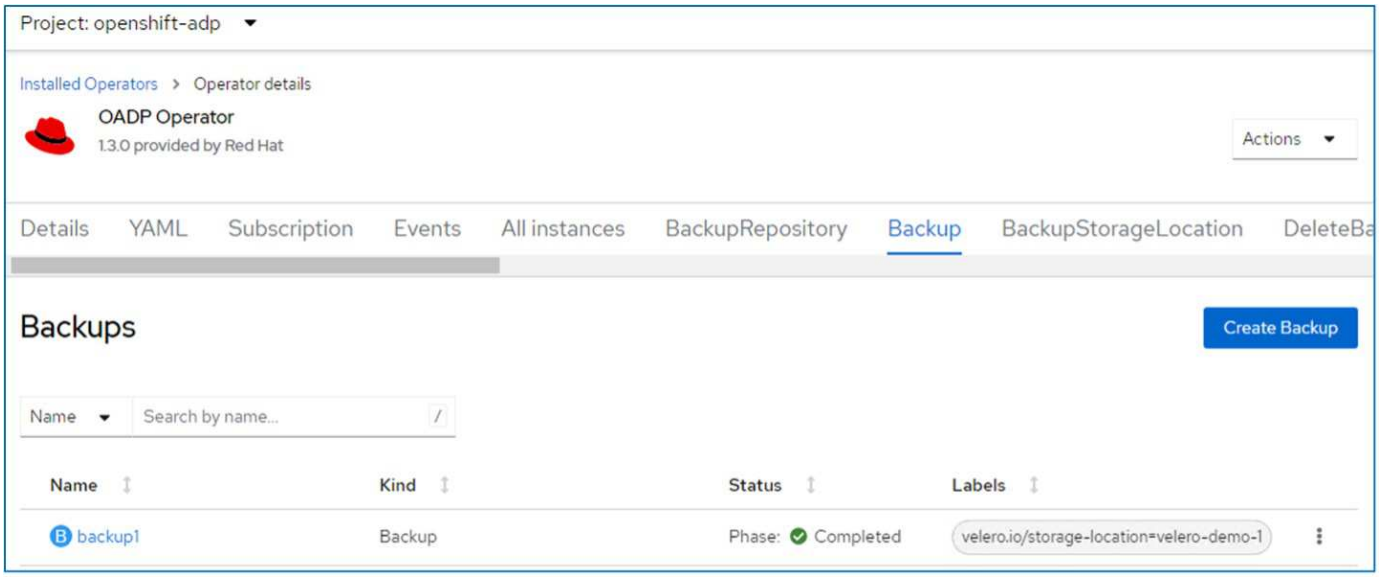
앱 백업을 만드는 단계

앱(앱 메타데이터 및 앱의 영구 볼륨)의 온디맨드 백업을 생성하려면 **Backup** 탭을 클릭하여 백업 사용자 지정 리소스(CR)를 생성하십시오. 백업 CR을 생성하기 위한 샘플 yaml이 제공됩니다. 이 yaml을 사용하면 지정된 네임스페이스의 앱과 해당 영구 스토리지가 백업됩니다. "선적 서류 비치"에 표시된 대로 추가 매개변수를 설정할 수 있습니다.

CSI는 지정된 네임스페이스의 영구 볼륨과 앱 리소스의 스냅샷을 생성합니다. 이 스냅샷은 yaml에 지정된 백업 위치에 저장됩니다. 백업은 TTL에 지정된 대로 30일 동안 시스템에 보관됩니다.

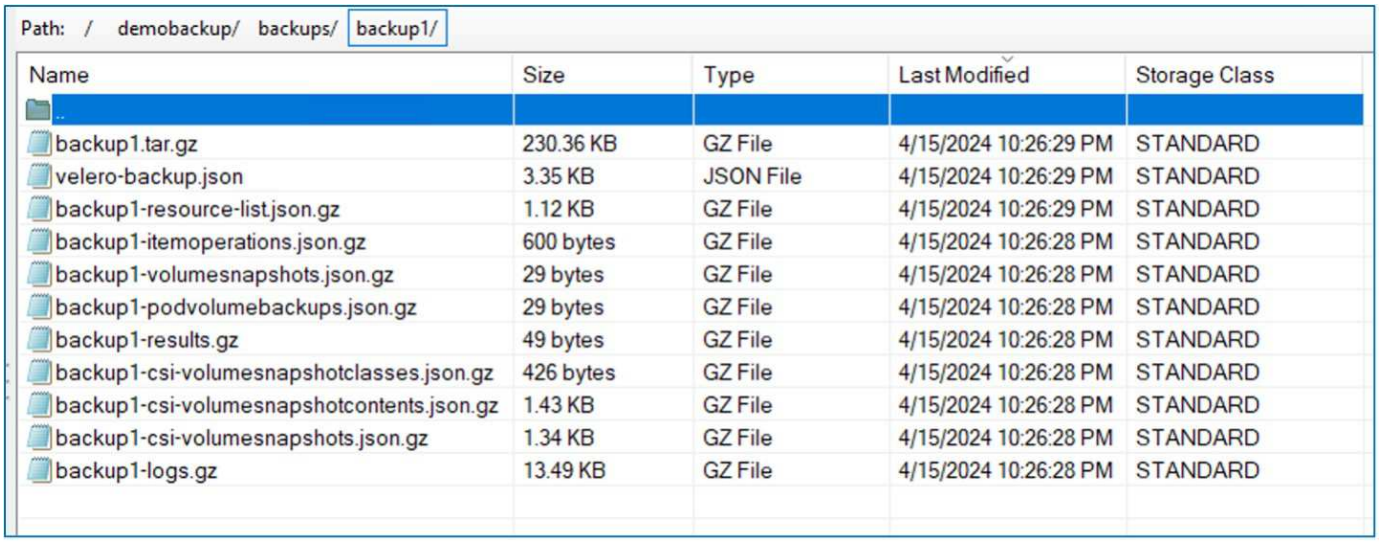
```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql ->namespace of the app
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: false
  storageLocation: velero-container-backup-ontap-1 -->this is the
backupStorageLocation previously created when Velero is configured.
  ttl: 720h0m0s
```

백업이 완료되면 해당 단계가 완료로 표시됩니다.



S3 브라우저 애플리케이션을 사용하면 Object Storage에서 백업을 검사할 수 있습니다. 백업 경로는 구성된 버킷에 접두사 이름(velero/container-demo-backup)과 함께 표시됩니다. 백업 내용에는 볼륨 스냅샷, 로그 및 애플리케이션의 기타 메타데이터가 포함되어 있음을 확인할 수 있습니다.

StorageGrid에서는 테넌트 관리자에서 제공하는 S3 콘솔을 사용하여 백업 객체를 볼 수도 있습니다.



앱에 대한 예약된 백업 생성

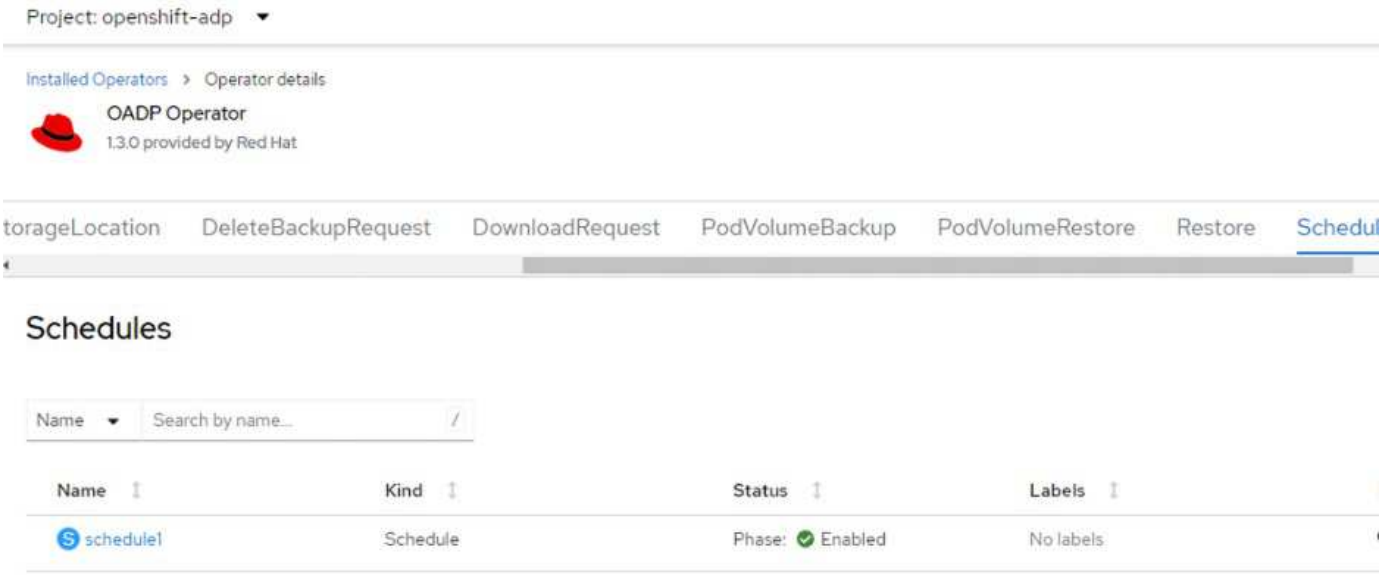
일정에 따라 백업을 만들려면 일정 CR을 만들어야 합니다. 일정은 백업을 만들고 싶은 시간을 지정할 수 있게 해주는 Cron 표현식입니다. 일정 CR을 만드는 샘플 YAML은 아래와 같습니다.

```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: schedule1
```

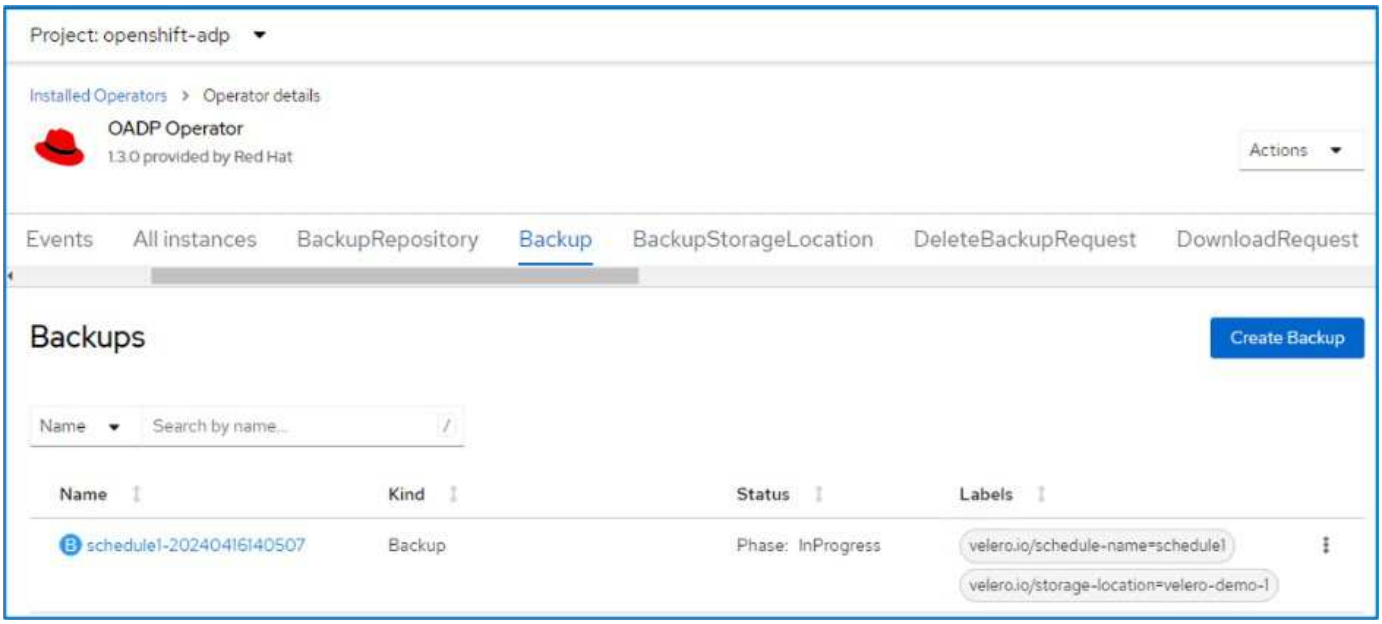
```
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    includedNamespaces:
      - postgresql
    storageLocation: velero-container-backup-ontap-1
```

Cron 표현식 0 7 * * *는 매일 7시에 백업이 생성됨을 의미합니다. 백업에 포함될 네임스페이스와 백업의 저장 위치도 지정됩니다. 따라서 백업 CR 대신 일정 CR을 사용하여 지정된 시간과 빈도로 백업을 생성합니다.

일정이 생성되면 활성화됩니다.



백업은 이 일정에 따라 생성되며, 백업 탭에서 볼 수 있습니다.



한 클러스터에서 다른 클러스터로 앱 마이그레이션

Velero의 백업 및 복원 기능은 클러스터 간에 데이터를 마이그레이션하는 데 유용한 도구입니다. 이 섹션에서는 한 클러스터의 개체 스토리지에 앱 백업을 만든 다음, 동일한 개체 스토리지에서 다른 클러스터로 앱을 복원하여 한 클러스터에서 다른 클러스터로 앱을 마이그레이션하는 방법을 설명합니다. .

▼ 첫 번째 클러스터에서 백업

클러스터 **1**의 전제 조건

- 클러스터에 Trident 설치해야 합니다.
- 트라이던트 백엔드와 스토리지 클래스를 만들어야 합니다.
- 클러스터에 OADP 운영자가 설치되어 있어야 합니다.
- DataProtectionApplication을 구성해야 합니다.

다음 사양을 사용하여 DataProtectionApplication 객체를 구성합니다.

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false'
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'
          s3Url: 'https://10.61.181.161'
        credential:
          key: cloud
          name: ontap-s3-credentials
        default: true
        objectStorage:
          bucket: velero
          caCert: <base-64 encoded tls certificate>
          prefix: container-backup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
```

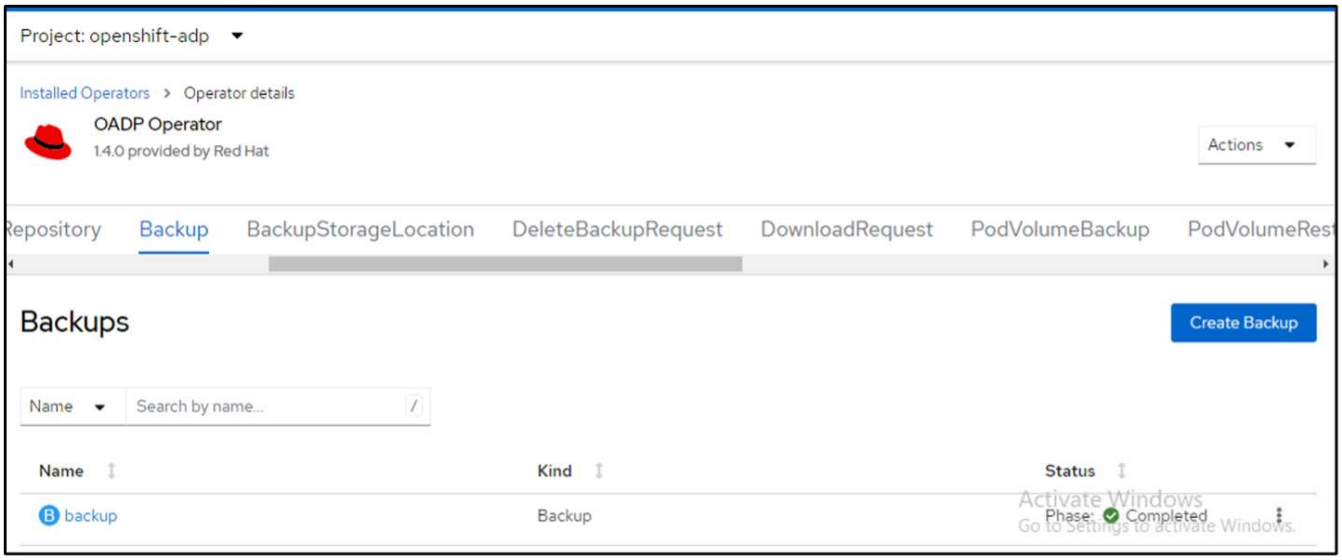
```
        - kubevirt
```

- 클러스터에서 애플리케이션을 만들고 이 애플리케이션을 백업합니다. 예를 들어, postgres 애플리케이션을 설치합니다.

```
[root@localhost ~]# oc get nodes
NAME           STATUS   ROLES                  AGE     VERSION
ocp6-master1   Ready    control-plane,master   3d13h   v1.27.15+6147456
ocp6-master2   Ready    worker                 3d12h   v1.27.15+6147456
ocp6-master3   Ready    control-plane,master   3d13h   v1.27.15+6147456
ocp6-worker1   Ready    worker                 3d12h   v1.27.15+6147456
ocp6-worker2   Ready    worker                 3d12h   v1.27.15+6147456
ocp6-worker3   Ready    control-plane,master   3d12h   v1.27.15+6147456
[root@localhost ~]# helm install postgresql bitnami/postgresql -n postgresql --create namespace^C
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          4h53m
[root@localhost ~]# oc get pvc -n postgresql
NAME              STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-f7a3c772-0e61-49cb-a3d0-7c7b2ec87dc6   8Gi        RWO            ontap-nas      4h53m
[root@localhost ~]# oc get pv -n postgresql
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                     STORAGECLASS
REASON   AGE
pvc-2e9e982f-54a4-4e7b-8eae-a589e0d9d819   1Gi        RWO            Delete           Bound    trident/basic             ontap-nas
         4h55m
pvc-f7a3c772-0e61-49cb-a3d0-7c7b2ec87dc6   8Gi        RWO            Delete           Bound    postgresql/data-postgresql-0   ontap-nas
         4h53m
[root@localhost ~]#
```

- 백업 CR에 다음 사양을 사용하세요.

```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: true
  storageLocation: velero-sample-1
  ttl: 720h0m0s
```



모든 인스턴스 탭을 클릭하면 다양한 객체가 생성되고 여러 단계를 거쳐 최종적으로 백업 완료 단계에 도달하는 것을 볼 수 있습니다.

네임스페이스 postgresql의 리소스 백업은 OADP 사양의 backupLocation에 지정된 개체 스토리지 위치(ONTAP S3)에 저장됩니다.

▼ 두 번째 클러스터로 복원

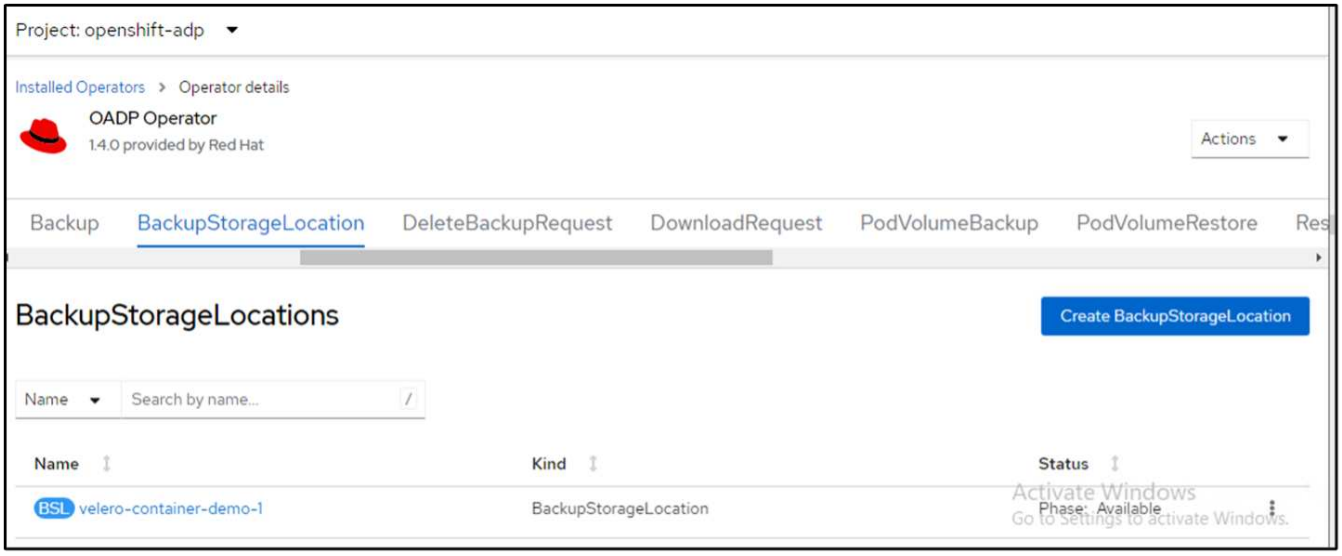
클러스터 **2**의 전제 조건

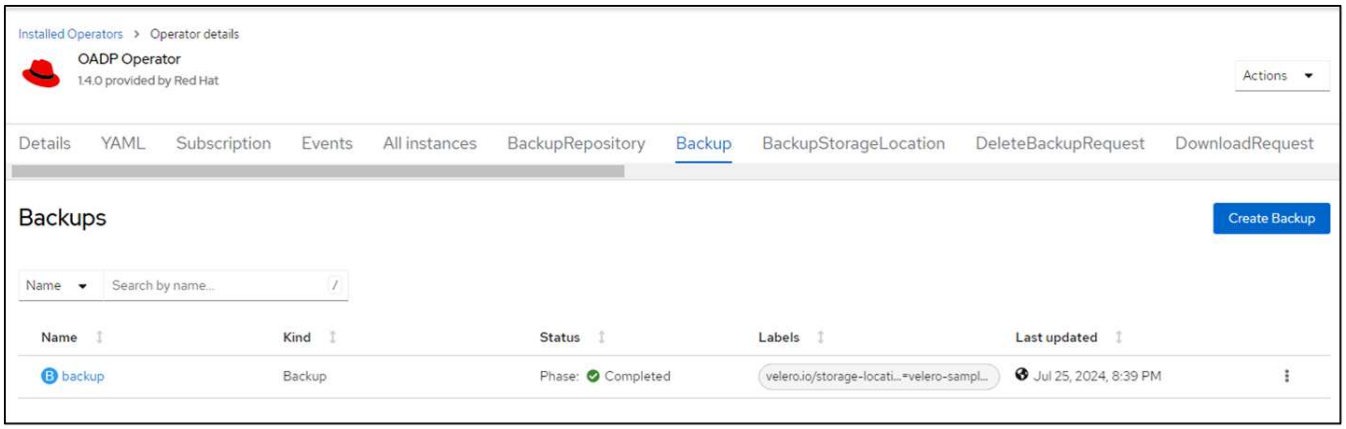
- 클러스터 2에 Trident 설치해야 합니다.
- postgresql 앱은 postgresql 네임스페이스에 이미 설치되어 있어서는 안 됩니다.
- OADP 운영자는 클러스터 2에 설치해야 하며, BackupStorage 위치는 첫 번째 클러스터에서 백업이 저장된 동일한 개체 저장소 위치를 가리켜야 합니다.
- 백업 CR은 두 번째 클러스터에서 볼 수 있어야 합니다.

```
[root@localhost ~]# oc get pods -n trident
NAME                                READY   STATUS    RESTARTS   AGE
trident-controller-6799cfb77f-8rzvk   6/6     Running   6          2d7h
trident-node-linux-7wvjz            2/2     Running   2          2d7h
trident-node-linux-8vvm2            2/2     Running   0          2d7h
trident-node-linux-bgs6f            2/2     Running   2          2d7h
trident-node-linux-njwb8            2/2     Running   0          2d7h
trident-node-linux-scqjl            2/2     Running   0          2d7h
trident-node-linux-swr69            2/2     Running   2          2d7h
trident-operator-b88b86fc8-7fk68    1/1     Running   1          2d7h
[root@localhost ~]#
```

```
[root@localhost ~]# oc get nodes
NAME           STATUS   ROLES                  AGE   VERSION
ocp7-master1   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master2   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master3   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-worker1   Ready    worker                 3d    v1.27.15+6147456
ocp7-worker2   Ready    worker                 3d    v1.27.15+6147456
ocp7-worker3   Ready    worker                 3d    v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pvc -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pv -n postgresql
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                 STORAGECLASS   REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic         ontap-nas               11m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc      vsphere-sc              2d7
h
[root@localhost ~]#
```

Activate Windows
Go to Settings to activate Windows.

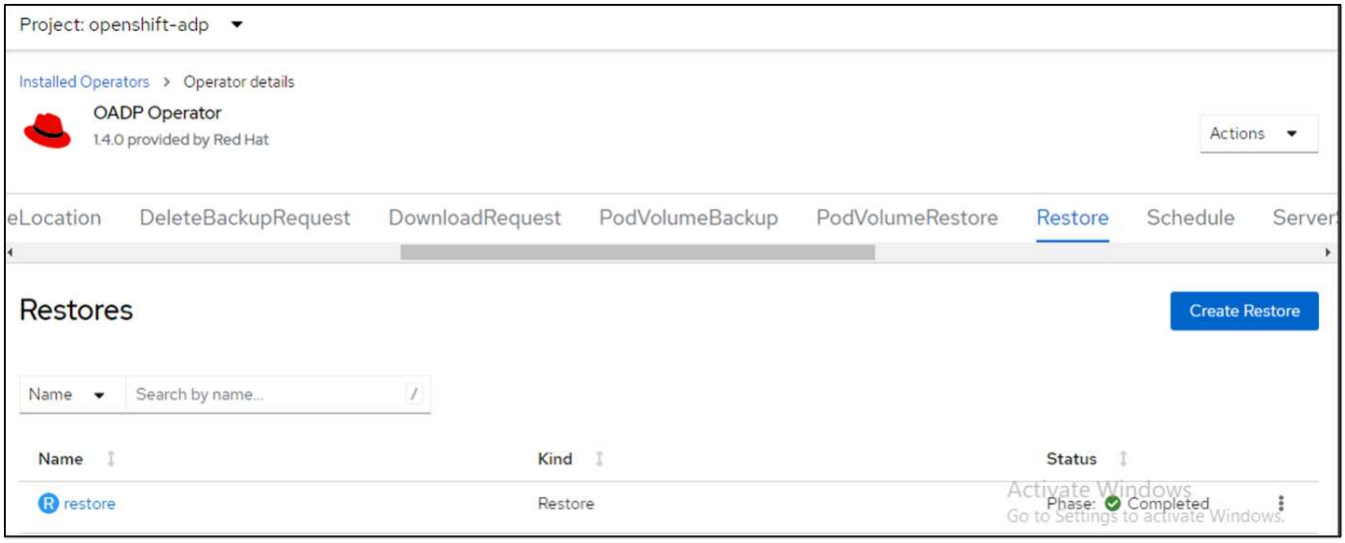




백업에서 이 클러스터의 앱을 복원합니다. 다음 yaml을 사용하여 Restore CR을 만듭니다.

```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
  backupName: backup
  restorePVs: true
```

복원이 완료되면 postgresql 앱이 이 클러스터에서 실행 중이고 pvc 및 해당 pv와 연결되어 있는 것을 확인할 수 있습니다. 앱의 상태는 백업이 수행된 시점과 동일합니다.




```
[root@localhost ~]# export KUBECONFIG=ocp-cluster7/kubeconfig-ocp-cluster7
[root@localhost ~]# oc get nodes
NAME           STATUS   ROLES                  AGE    VERSION
ocp7-master1   Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-master2   Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-master3   Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-worker1   Ready    worker                 3d3h   v1.27.15+6147456
ocp7-worker2   Ready    worker                 3d3h   v1.27.15+6147456
ocp7-worker3   Ready    worker                 3d3h   v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          31m
[root@localhost ~]# oc get pvc -n postgresql
NAME              STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-ce7044e3-2ba5-4934-8bad-553fa7d35128   8Gi        RWO            ontap-nas      31m
[root@localhost ~]# oc get pv
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                          STORAGECLASS
REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic                  ontap-nas
         3h27m
pvc-ce7044e3-2ba5-4934-8bad-553fa7d35128   8Gi        RWO            Delete           Bound    postgresql/data-postgresql-0   ontap-nas
         31m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc               vsphere-sc
         2d10h
[root@localhost ~]#
```

Activate Windows
Go to Settings to activate Windows.

백업에서 앱 복원

이 섹션에서는 백업에서 앱을 복원하는 방법을 설명합니다.

필수 조건

백업에서 복원하려면 앱이 있던 네임스페이스가 실수로 삭제되었다고 가정해 보겠습니다.

```
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          102s
[root@localhost ~]# oc delete ns postgresql
namespace "postgresql" deleted

[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]#
```

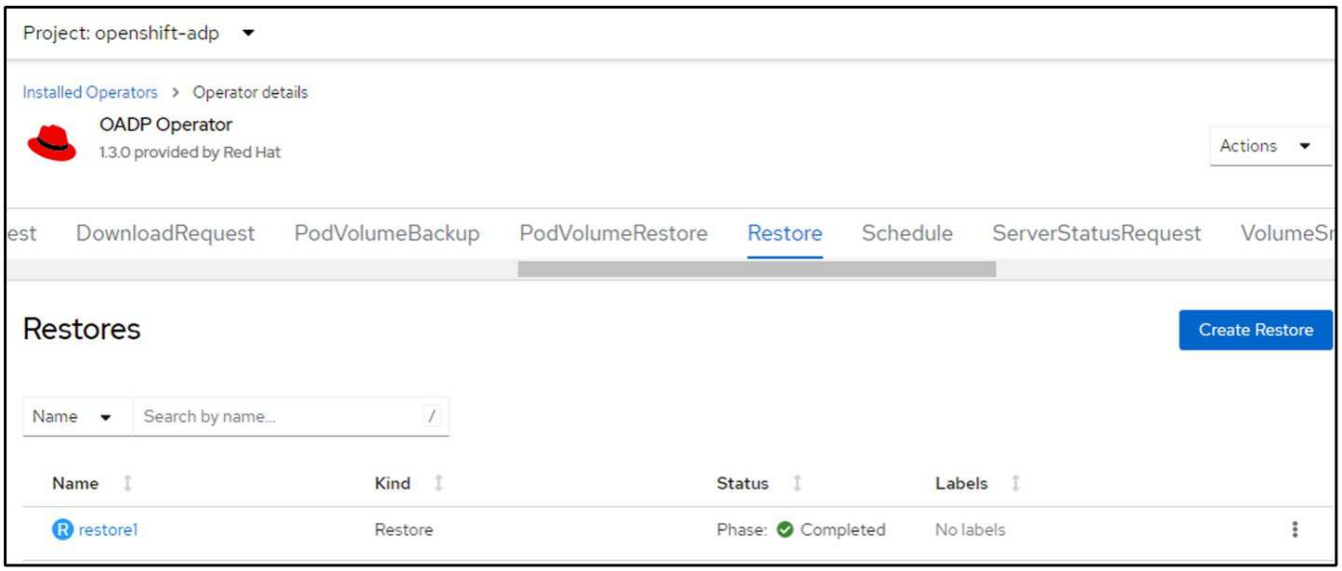
▼ 동일한 네임스페이스로 복원

방금 생성한 백업에서 복원하려면 Restore Custom Resource(CR)를 생성해야 합니다. 이름을 지정하고, 복원할 백업의 이름을 지정한 다음, restorePVs를 true로 설정해야 합니다. 추가 매개변수는 "선적 서류 비치"에 표시된 대로 설정할 수 있습니다. Create 버튼을 클릭합니다.




```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
```

단계가 완료로 표시되면 스냅샷을 찍었을 때의 상태로 앱이 복원된 것을 확인할 수 있습니다. 앱이 동일한 네임스페이스로 복원됩니다.




```
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS              RESTARTS   AGE
postgresql-0   0/1     ContainerCreating   0          16s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   0/1     Running   0          22s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   0/1     Running   0          29s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          37s
[root@localhost ~]#
```

▼ 다른 네임스페이스로 복원

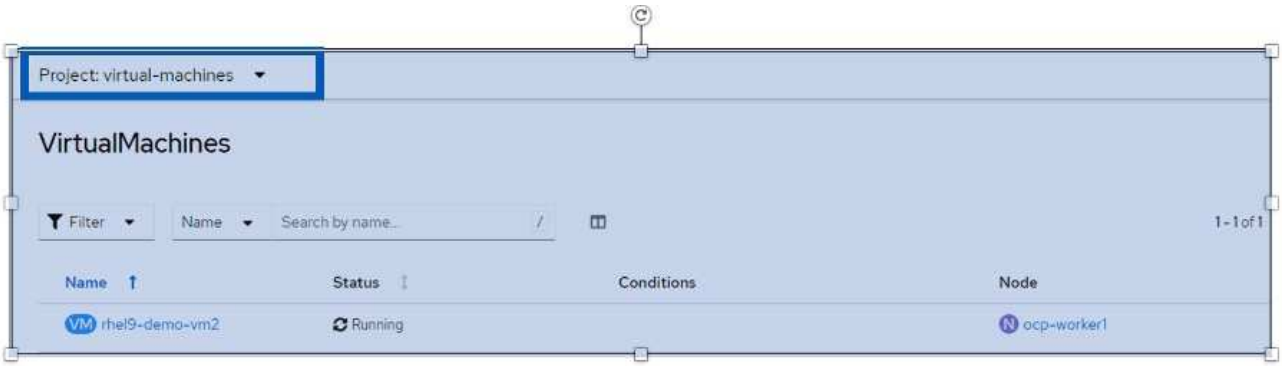
앱을 다른 네임스페이스로 복원하려면 Restore CR의 YAML 정의에 네임스페이스 매핑을 제공하면 됩니다.

다음 샘플 yaml 파일은 postgresql 네임스페이스에서 앱과 해당 영구 저장소를 새 네임스페이스인 postgresql-restored로 복원하는 Restore CR을 만듭니다.

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
```

```
  includedNamespaces:
  - postgresql
  namespaceMapping:
    postgresql: postgresql-restored
```

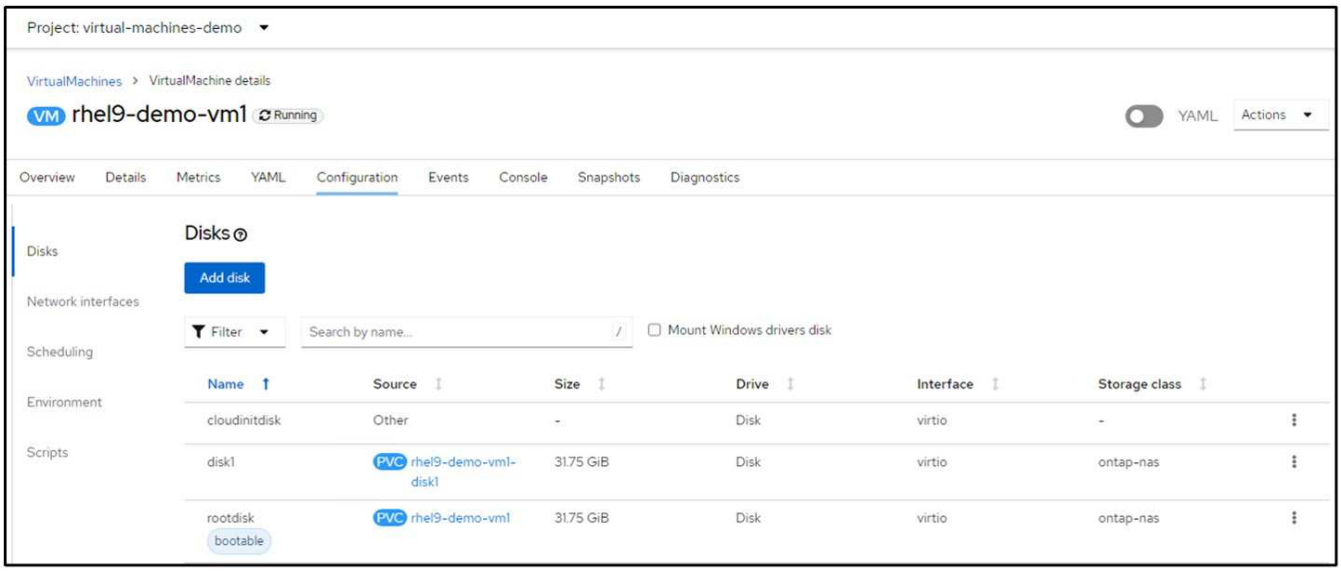
단계가 완료로 표시되면 스냅샷을 찍었을 때의 상태로 앱이 복원된 것을 확인할 수 있습니다. 앱은 yaml에 지정된 다른 네임스페이스로 복원됩니다.

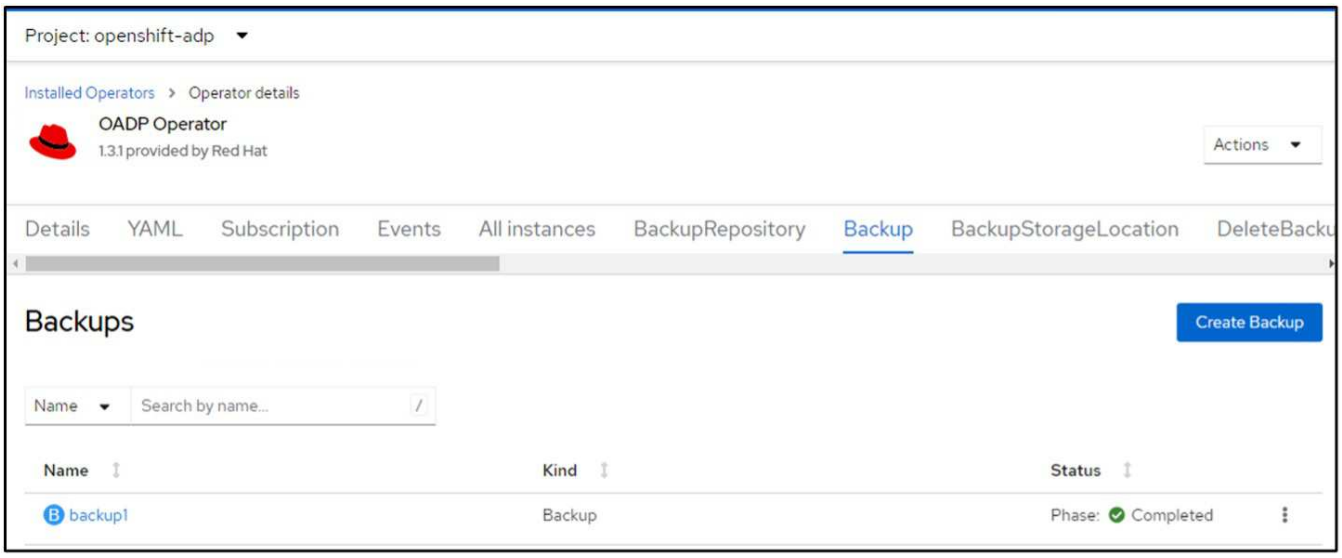


▼ 다른 스토리지 클래스로 복원

Velero는 JSON 패치를 지정하여 복원 중에 리소스를 수정하는 일반적인 기능을 제공합니다. JSON 패치는 리소스가 복원되기 전에 리소스에 적용됩니다. JSON 패치는 configmap에 지정되고 configmap은 restore 명령에서 참조됩니다. 이 기능을 사용하면 다양한 저장 클래스를 사용하여 복원할 수 있습니다.

아래 예에서 앱은 배포 중에 영구 볼륨의 스토리지 클래스로 ontap-nas를 사용합니다. backup-postgresql-ontaps3라는 앱의 백업이 생성됩니다.





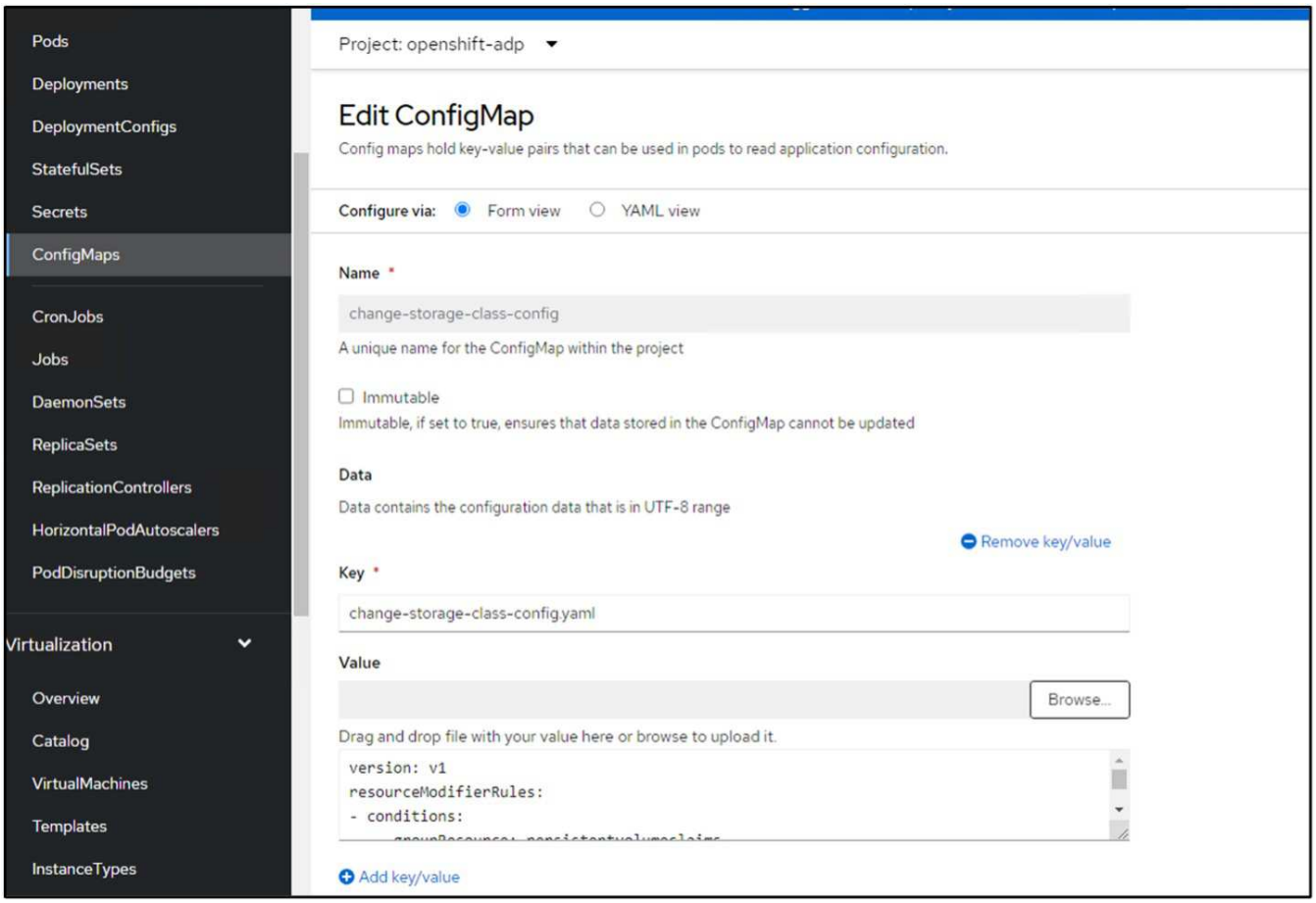
앱을 제거하여 앱이 사라진 것처럼 가장합니다.

예를 들어 ontap-nas-eco 스토리지 클래스와 같이 다른 스토리지 클래스를 사용하여 VM을 복원하려면 다음 두 단계를 수행해야 합니다.

1단계

다음과 같이 openshift-adp 네임스페이스에 구성 맵(콘솔)을 만듭니다. 스크린샷에 표시된 대로 세부 정보를 입력합니다. 네임스페이스 선택: openshift-adp 이름: change-ontap-sc(원하는 이름 사용 가능) 키: change-ontap-sc-config.yaml: 값:

```
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "data-postgresql*"
     namespaces:
     - postgresql
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"
```



결과적으로 생성되는 구성 맵 객체는 다음과 같습니다(CLI):

```
# kubectl describe cm/change-storage-class-config -n openshift-
adp
Name:         change-storage-class-config
Namespace:    openshift-adp
Labels:       velero.io/change-storage-class=RestoreItemAction
              velero.io/plugin-config=
Annotations:  <none>

Data
====
change-storage-class-config.yaml:
----
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "^rhel*"
     namespaces:
     - virtual-machines-demo
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"



BinaryData
====

Events:  <none>
```

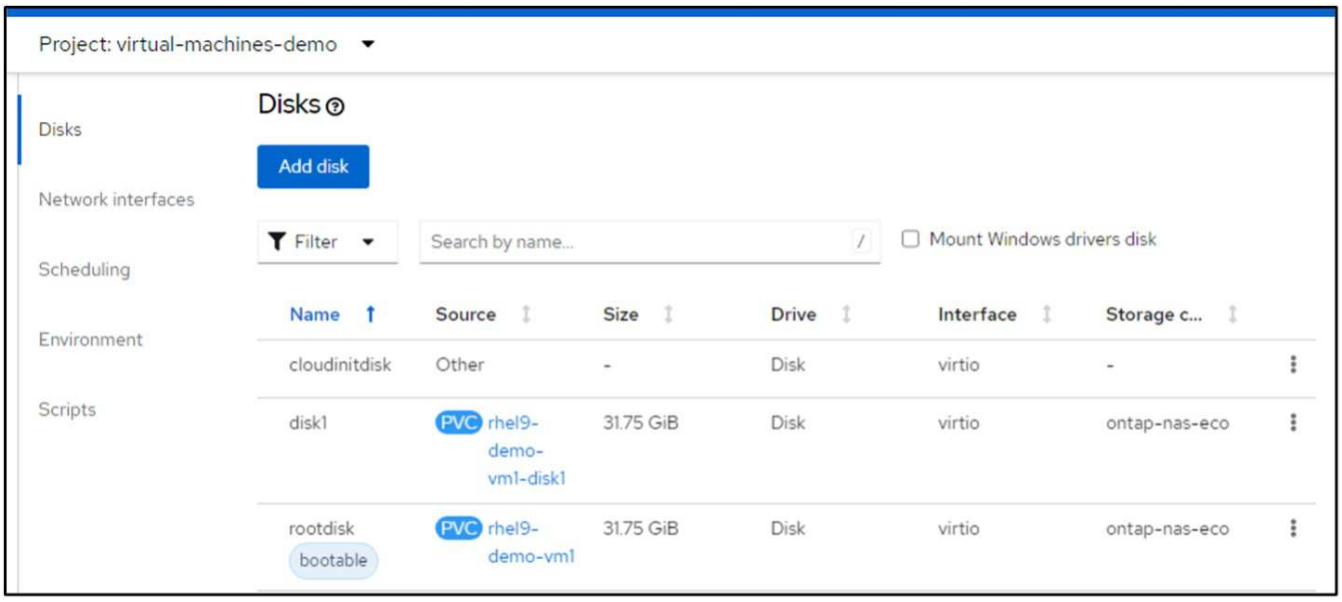
이 구성 맵은 복원이 생성될 때 리소스 수정자 규칙을 적용합니다. rhel로 시작하는 모든 영구 볼륨 클레임에 대해 스토리지 클래스 이름을 ontap-nas-eco로 바꾸는 패치가 적용됩니다.

2단계

VM을 복원하려면 Velero CLI에서 다음 명령을 사용하세요.

```
#velero restore create restore1 --from-backup backup1 --resource
-modifier-configmap change-storage-class-config -n openshift-adp
```

앱은 ontap-nas-eco 스토리지 클래스를 사용하여 생성된 영구 볼륨 클레임과 동일한 네임스페이스에 복원됩니다.



Velero를 사용하여 백업 및 복원 삭제

이 섹션에서는 Velero를 사용하여 OpenShift 컨테이너 플랫폼에서 앱의 백업과 복원을 삭제하는 방법을 설명합니다.

모든 백업 나열

OC CLI 도구나 Velero CLI 도구를 사용하여 모든 백업 CR을 나열할 수 있습니다. Velero CLI를 지침에 따라 다운로드하세요."Velero 문서" .

```
[root@localhost ~]# oc get backups -n openshift-adp
NAME                        AGE
backup-postgresql-ontaps3   23h
backup2                     26s
schedule1-20240717070005    6h42m
[root@localhost ~]# velero get backups -n openshift-adp
NAME                        STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                  SELECTOR
backup-postgresql-ontaps3   Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                     Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005    Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

백업 삭제

OC CLI 도구를 사용하면 개체 스토리지 데이터를 삭제하지 않고도 백업 CR을 삭제할 수 있습니다. 백업은 CLI/콘솔 출력에서 제거됩니다. 하지만 해당 백업은 개체 스토리지에서 제거되지 않으므로 CLI/콘솔 출력에 다시 나타납니다.

```
[root@localhost ~]# oc delete backup backup2 -n openshift-adp
backup.velero.io "backup2" deleted
[root@localhost ~]# oc get backups -n openshift-adp
NAME                          AGE
backup-postgresql-ontaps3     23h
schedule1-20240717070005      6h49m
[root@localhost ~]# oc get backups -n openshift-adp
NAME                          AGE
backup-postgresql-ontaps3     23h
backup2                       24s
schedule1-20240717070005      6h50m
[root@localhost ~]#
```

백업 **CR**과 관련된 개체 스토리지 데이터를 삭제하려면 **Velero CLI** 도구를 사용하면 됩니다**.**

```
[root@localhost ~]# velero get backups -n openshift-adp
NAME                          STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                SELECTOR
backup-postgresql-ontaps3     Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                       Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005      Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]# velero delete backup backup2 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete backup "backup2" submitted successfully.
The backup will be fully deleted after all associated data (disk snapshots, backup files, restores) are removed.
[root@localhost ~]# velero get backups -n openshift-adp
NAME                          STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                SELECTOR
backup-postgresql-ontaps3     Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005      Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

복원 삭제

OC CLI 또는 Velero CLI를 사용하여 CR 개체 복원을 삭제할 수 있습니다.

```
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                        STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3     Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
restore1   backup-postgresql-ontaps3     Completed   2024-07-16 16:36:37 -0400 EDT   2024-07-16 16:36:59 -0400 EDT   0        9          2024-07-16 16:36:37 -0400 EDT   <none>
[root@localhost ~]# velero restore delete restore1 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete restore "restore1" submitted successfully.
The restore will be fully deleted after all associated data (restore files in object storage) are removed.
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                        STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3     Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
[root@localhost ~]#
[root@localhost ~]# oc delete restore restore -n openshift-adp
restore.velero.io "restore" deleted
[root@localhost ~]# oc get restore -n openshift-adp
No resources found in openshift-adp namespace.
[root@localhost ~]# velero get restore -n openshift-adp
[root@localhost ~]#
```

Activate Windows

NetApp 사용한 하이브리드 멀티클라우드 솔루션에 대한 비디오와 데모를 시청하세요

NetApp 사용한 Amazon Web Services용 하이브리드 멀티클라우드 솔루션에 대한 비디오를 시청하세요

NetApp 의 AWS용 하이브리드 멀티클라우드 솔루션을 소개하는 NetApp의 포괄적인 비디오 라이브러리를 살펴보세요. Windows 및 Linux 시나리오를 포함하여 VMware Cloud on AWS와 Amazon FSx for ONTAP 의 게스트 연결 스토리지, TCO 절감, 보충 데이터 저장소 및 마이그레이션 워크플로에 대한 비디오를 시청하세요.

게스트 연결 스토리지

iSCSI를 사용하는 FSx ONTAP 사용한 Windows 게스트 연결 스토리지

NFS를 사용하는 FSx ONTAP 사용한 Linux 게스트 연결 스토리지

TCO 및 보충 데이터 저장소

Amazon FSx ONTAP 통한 VMware Cloud on AWS TCO 절감

Amazon FSx ONTAP 사용한 AWS 보충 데이터 저장소의 VMware Cloud

마이그레이션 워크플로(HCX)

VMC를 위한 VMware HCX 배포 및 구성 설정

VMC 및 FSx ONTAP 용 VMware HCX를 사용한 vMotion 마이그레이션 데모

VMC 및 FSx ONTAP 용 VMware HCX를 사용한 콜드 마이그레이션 데모

NetApp 사용한 Azure VMware 클라우드를 위한 하이브리드 멀티클라우드 솔루션에 대한 비디오를 시청하세요

NetApp 의 Azure VMware Solution(AVS)을 위한 하이브리드 멀티클라우드 솔루션을 소개하는 NetApp의 포괄적인 비디오 라이브러리를 살펴보세요. 이 컬렉션에는 보충 데이터 저장소, 재해 복구, 마이그레이션 워크플로에 대한 비디오가 포함되어 있습니다.

보충 데이터 저장소

Azure NetApp Files 사용한 Azure VMware 솔루션 보충 데이터 저장소 개요

재해 복구

Cloud Volumes ONTAP, SnapCenter 및 JetStream을 사용한 Azure VMware 솔루션 DR

마이그레이션 워크플로(HCX)

AVS 및 ANF를 위한 VMware HCX를 사용한 콜드 마이그레이션 데모

AVS 및 ANF를 위한 VMware HCX를 사용한 vMotion 데모

AVS 및 ANF를 위한 VMware HCX를 사용한 대량 마이그레이션 데모

NetApp 과 Red Hat OpenShift를 위한 하이브리드 멀티클라우드 솔루션에 대한 비디오를 시청하세요

NetApp 과 Red Hat OpenShift를 위한 하이브리드 멀티클라우드 솔루션을 소개하는 NetApp의 포괄적인 비디오 라이브러리를 살펴보세요. 이 컬렉션에는 FSx ONTAP 사용한 AWS(ROSA)의 OpenShift에 대한 스냅샷 및 복원, Trident 와의 통합, 앱에 대한 장애 조치 및 장애 복구, Ansible을 사용한 FlexPod 에서의 자동화된 Oracle RAC 배포에 대한 데모가 포함되어 있습니다.

스냅샷 및 복원

Amazon FSx ONTAP 스토리지를 사용하는 AWS(ROSA) 클러스터의 Red Hat OpenShift Service에 대한 애플리케이션 스냅샷/복원

스토리지 통합

FSx ONTAP 과 Trident 의 통합

장애 조치 및 장애 복구

FSx ONTAP 사용한 ROSA의 앱 장애 조치 및 장애 복구

솔루션 자동화



Ansible을 사용하여 **FlexPod** 에 **Oracle 19c RAC** 자동 배포

NetApp 전문가의 클라우드 솔루션 블로그를 읽어보세요

ONTAP 스토리지를 NetApp 클라우드 솔루션과 통합하기 위한 실용적인 지침과 모범 사례를 제공하는 블로그를 읽어보세요.

AWS 및 Amazon FSx for ONTAP 과 VMware 통합

- "Amazon EC2 및 Amazon FSx ONTAP iSCSI 프로토콜을 사용하여 VMware VM을 AWS로 마이그레이션"
- "Amazon EVS가 이제 FSx for ONTAP 과 통합되었습니다."
- "Amazon EVS, FSx for ONTAP 지원 발표"
- "VMware HCX를 사용하여 AWS SDDC에서 FSx ONTAP 및 VMware Cloud로 하이브리드 클라우드 구성"

Azure VMware 솔루션

- "모든 클라우드에서 스토리지 및 데이터 집약적인 VMware 워크로드 최적화"
- "VMware 워크로드를 Azure VMware Solution으로 이전하시겠습니까? 먼저 이 글을 읽어보세요."

구글 클라우드 VMware 엔진

- "Google Cloud VMware Engine(NetApp)에 대한 Google Cloud Google Cloud NetApp Volumes 데이터 저장소 지원"
- "Google Cloud VMware Engine(Google)의 데이터 저장소로 NetApp Volumes를 사용하는 방법"
- "NetApp 블로그 - 스토리지가 풍부한 앱을 Google Cloud로 마이그레이션하는 더 나은 방법"

데이터 보호 및 관리

- "SnapCenter 플러그인 및 NetApp Backup and Recovery for VMs를 사용한 VMware용 3-2-1 데이터 보호"
- "NetApp Cloud Insights 통한 최신 데이터 센터의 관찰성"

OpenShift 컨테이너 워크로드를 위한 NetApp

- "NetApp ONTAP Red Hat OpenShift 컨테이너 플랫폼의 로그 저장소로도 사용됩니다."

VMware Sovereign Cloud

- "새로운 Sovereign Cloud 이니셔티브 소개"

법적 고지 사항

법적 고지사항은 저작권 표시, 상표, 특허 등에 대한 정보를 제공합니다.

저작권

"https://www.netapp.com/company/legal/copyright/"

상표

NETAPP, NETAPP 로고 및 NetApp 상표 페이지에 나열된 마크는 NetApp, Inc.의 상표입니다. 다른 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

"https://www.netapp.com/company/legal/trademarks/"

특허

NetApp 이 소유한 현재 특허 목록은 다음에서 확인할 수 있습니다.

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

개인정보 보호정책

"https://www.netapp.com/company/legal/privacy-policy/"

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 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.