NetApp 의 VMware Cloud Foundation

NetApp virtualization solutions

NetApp
August 24, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/netapp-solutions-virtualization/vmware/vmw-vcf-overview.html on August 24, 2025. Always check docs.netapp.com for the latest.

목차

NetApp 의 VMware Cloud Foundation . . . 1
VMware Cloud Foundation 및 ONTAP 통해 하이브리드 클라우드 경험을 간소화하세요 . . . 1
소개 . . . 1
NetApp ONTAP 소개 . . . 1
VMware Cloud Foundation 소개 . . . 1
VCF 도메인 . . . 1
VCF를 사용한 저장 . . . 2
VCF에 ONTAP 이유 . . . 3
추가 정보: . . . 4
요약 . . . 5
문서 리소스 . . . 5
VMware Cloud Foundation 및 ONTAP 사용한 디자인 옵션 . . . 6
저장 옵션 . . . 6
청사진 . . . 6
VMware Cloud Foundation 및 ONTAP 사용하여 프라이빗 클라우드 환경 설정 . . . 11
새로운 VCF 9 인스턴스 배포 . . . 11
기존 구성 요소를 VCF 9로 수렴 . . . 13
기존 VCF 환경을 VCF 9로 업그레이드 . . . 14
NetApp SnapMirror 및 BlueXP DRaaS를 사용한 재해 복구 구현 . . . 14
시작하기 . . . 15
BlueXP disaster recovery 구성 . . . 17
소스 사이트 배열과 대상 사이트 배열 간 스토리지 복제 구성 . . . 17
VMware 재해 복구를 설정하는 방법 . . . 18
BlueXP disaster recovery 귀사를 위해 무엇을 해드릴 수 있나요? . . . 18
테스트 장애 조치 . . . 23
클린업 페일오버 테스트 작업 . . . 25
계획된 마이그레이션 및 장애 조치 . . . 25
장애 복구 . . . 27
모니터링 및 대시보드 . . . 28
기존 vSphere 클러스터를 VCF로 변환 . . . 29
기존 데이터 저장소가 있는 vSphere 환경을 VCF로 변환하는 방법에 대해 알아보세요. . . . 29
vCenter 서버 인스턴스를 VCF 관리 도메인(NFS 데이터 저장소)으로 변환 . . . 30
vCenter 서버 인스턴스를 VCF 관리 도메인(FC 데이터 저장소)으로 변환 . . . 44
주요 저장소를 사용하여 VCF 제공 . . . 58
ONTAP 주요 스토리지 솔루션으로 사용하여 VCF 환경 제공 . . . 58
ONTAP 에서 FC 기반 VMFS 데이터 저장소를 VCF 관리 도메인의 주 저장소로 사용합니다. . . . 58
ONTAP 에서 VCF 관리 도메인의 주 저장소로 NFS 데이터 저장소 사용 . . . 59
ONTAP 에서 FC 기반 VMFS 데이터 저장소를 VI 워크로드 도메인의 주요 스토리지로 사용 . . . 61
VI 워크로드 도메인의 주요 스토리지로 ONTAP 의 NFS 데이터 저장소 사용 . . . 63

보충 스토리지로 VCF 확장 . . . 83
보조 스토리지를 사용하여 VCF 환경의 스토리지 확장에 대해 알아보세요. . . . 83
ONTAP tools for VMware vSphere 사용하여 관리 도메인의 보조 스토리지로 iSCSI 데이터 저장소 추가 . . . 83
ONTAP tools for VMware vSphere 사용하여 관리 도메인의 보조 스토리지로 FC 기반 VMFS 데이터 저장소 추가 . . . 107
ONTAP tools for VMware vSphere 사용하여 VI 워크로드 도메인에 보조 스토리지로 vVols 추가 . . . 108
ONTAP tools for VMware vSphere 사용하여 VI 워크로드 도메인에 보충 스토리지로 NFS 및 vVols 추가 . . . 134
VI 워크로드 도메인에 보조 스토리지로 NVMe over TCP 추가 . . . 158
VI 워크로드 도메인에 보조 스토리지로 FC 기반 VMFS 데이터 저장소 추가 . . . 182
SnapCenter 로 VCF 보호 . . . 183
VMware vSphere용 SnapCenter 플러그인을 사용하여 VCF 워크로드 도메인을 보호하는 방법에 대해 알아보세요. . . . 183
VMware vSphere용 SnapCenter 플러그인을 사용하여 VCF 워크로드 도메인 보호 . . . 184
VMware vSphere용 SnapCenter 플러그인을 사용하여 VCF 관리 및 워크로드 도메인 보호 . . . 219
VMware vSphere용 NVMe over TCP 스토리지 및 SnapCenter 플러그인을 사용하여 VCF 워크로드 도메인을 보호합니다. . . . 232
BlueXP 로 VMware 데이터 저장소 보호 . . . 239
BlueXP disaster recovery 사용하여 VMware 데이터 저장소를 보호하는 방법에 대해 알아보세요. . . . 239
VMware vSphere 및 BlueXP backup and recovery 위한 SnapCenter 플러그인을 사용하여 VMware에 대한 3-2-1 데이터 보호 구성 . . . 239
BlueXP disaster recovery 사용하여 VMFS 데이터 저장소에 대한 재해 복구 설정 . . . 280
BlueXP disaster recovery 사용하여 NFS 데이터 저장소에 대한 재해 복구 설정 . . . 298
vSphere Metro Storage Cluster로 워크로드 보호 . . . 318
ONTAP 고가용성을 VMware vSphere Metro Storage Cluster(vMSC)와 통합하는 방법에 대해 알아보세요. 318
MetroCluster 사용하여 VCF 관리 도메인에 대한 스트레치 클러스터 구성 . . . 319
MetroCluster 사용하여 VI 워크로드 도메인에 대한 스트레치 클러스터 구성 . . . 330
SnapMirror Active Sync를 사용하여 VCF 관리 도메인에 대한 스트레치 클러스터 구성 . . . 342
SnapMirror Active Sync를 사용하여 VI 워크로드 도메인에 대한 스트레치 클러스터 구성 . . . 344
VMware vSphere에서 ONTAP 데이터 저장소로 VM 마이그레이션 . . . 346
네트워크 요구 사항 . . . 346
VM 마이그레이션 시나리오 . . . 348
VM 템플릿 마이그레이션 시나리오 . . . 373
사용 사례 . . . 380
추가 자료 . . . 381
NFS 스토리지를 위한 자율형 랜섬웨어 보호 . . . 381
Data Infrastructure Insights 사용하여 온프레미스 스토리지 모니터링 . . . 391
Data Infrastructure Insights 통한 온프레미스 스토리지 모니터링 . . . 391
솔루션 배포 개요 . . . 391
필수 조건 . . . 392
솔루션 배포 . . . 392
결론 . . . 409

추가 정보 409

NetApp 의 VMware Cloud Foundation

VMware Cloud Foundation 및 ONTAP 통해 하이브리드 클라우드 경험을 간소화하세요

NetApp ONTAP VMware Cloud Foundation(VCF)과 통합되어 블록 및 파일 프로토콜을 모두 지원하는 통합 스토리지 솔루션을 제공합니다. 이러한 통합을 통해 하이브리드 클라우드 배포가 간소화되고, 데이터 관리와 성능이 개선되며, 온프레미스와 클라우드 환경에서 일관된 데이터 서비스가 보장됩니다.

소개

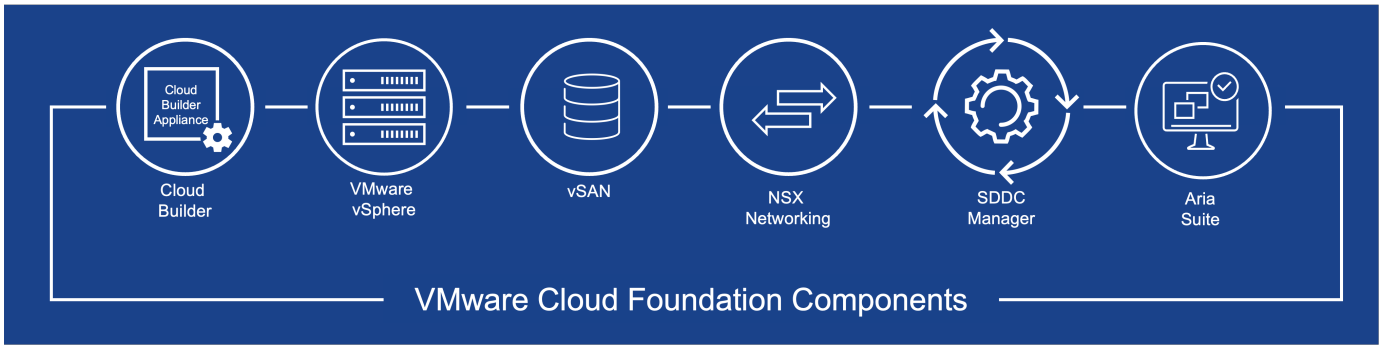
VCF와 함께 NetApp 사용하면 중복 제거, 압축, 스냅샷과 같은 NetApp의 고급 기능을 통해 데이터 관리 및 스토리지 효율성이 향상됩니다. 이러한 조합은 가상화된 환경에 원활한 통합, 높은 성능, 확장성을 제공합니다. 또한, 온프레미스와 클라우드 인프라 전반에서 일관된 데이터 서비스와 관리를 지원하여 하이브리드 클라우드 배포를 간소화합니다.

NetApp ONTAP 소개

NetApp ONTAP 은 광범위한 제품군에 걸쳐 고급 스토리지 기능을 제공하는 포괄적인 데이터 관리 소프트웨어입니다. ONTAP 소프트웨어 정의 스토리지, 주요 클라우드 공급업체를 통한 퍼스트 파티 서비스, NetApp ASA (All San Array), AFF (All-flash FAS), FAS (Fabric-Attached Storage) 플랫폼용 스토리지 OS로 제공됩니다. ONTAP 사일로를 만들지 않고도 VMware 가상화를 포함한 다양한 사용 사례에 대해 높은 성능과 낮은 대기 시간을 제공합니다.

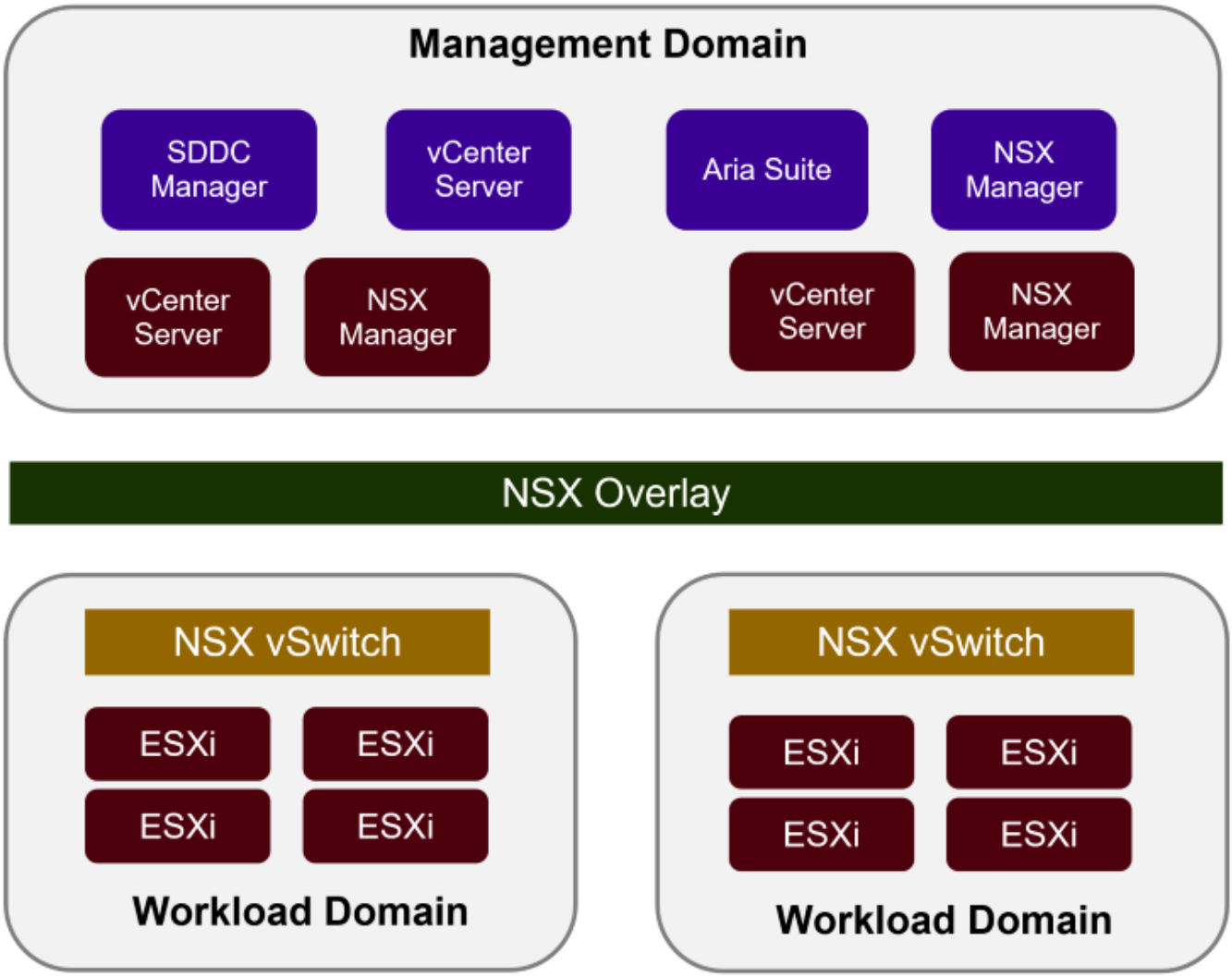
VMware Cloud Foundation 소개

VCF는 컴퓨팅, 네트워크 및 스토리지 서비스를 VMware 제품 및 타사 통합과 통합하여 기본 Kubernetes와 가상 머신 기반 워크로드를 모두 용이하게 해줍니다. 이 소프트웨어 플랫폼에는 VMware vSphere, NSX, Aria Suite Enterprise, Tanzu Kubernetes Grid, HCX Enterprise, SDDC Manager 및 vSAN을 통해 호스트 CPU 코어에 연결된 스토리지 용량과 같은 주요 구성 요소가 포함되어 있습니다. NetApp ONTAP 온프레미스와 퍼블릭 클라우드 모두에서 다양한 VCF 배포 모델과 원활하게 통합됩니다.



VCF 도메인

도메인은 VCF 내의 기반이 되는 구성 요소로, 리소스를 별개의 독립적인 그룹으로 구성할 수 있도록 합니다. 도메인은 인프라를 보다 효과적으로 구성하여 리소스가 효율적으로 활용되도록 보장합니다. 각 도메인은 자체 컴퓨팅, 네트워크 및 스토리지 요소와 함께 배포됩니다.



VCF에는 두 가지 주요 도메인 유형이 있습니다.

- 관리 도메인 – 관리 도메인에는 VCF 환경의 핵심 기능을 담당하는 구성 요소가 포함됩니다. 이러한 구성 요소는 리소스 프로비저닝, 모니터링, 유지 관리와 같은 필수 작업을 처리하며 VMware용 NetApp ONTAP 도구와 같은 타사 플러그인 통합을 포함합니다. 모범 사례가 준수되도록 Cloud Builder Appliance를 사용하여 관리 도메인을 배포하거나 기존 vCenter 환경을 VCF 관리 도메인으로 변환할 수 있습니다.
- 가상 인프라 워크로드 도메인 – 가상 인프라 워크로드 도메인은 특정 운영적 요구 사항, 워크로드 또는 조직에 전담된 리소스 풀로 설계되었습니다. SDDC 관리자를 통해 워크로드 도메인을 쉽게 배포하여 일련의 복잡한 작업을 자동화하는 데 도움이 됩니다. VCF 환경 내에서 최대 24개의 워크로드 도메인을 프로비저닝할 수 있으며, 각 도메인은 애플리케이션에 적합한 인프라의 단위를 나타냅니다.

VCF를 사용한 저장

도메인의 기능에서 가장 중요한 것은 도메인이 사용하는 저장 공간입니다. VCF는 하이퍼 컨버지드 사용 사례를 위한 CPU 코어 기반 vSAN 용량을 포함하는 동시에 광범위한 외부 스토리지 솔루션도 지원합니다. 이러한 유연성은 기존 스토리지 어레이에 상당한 투자를 했거나 vSAN에서 제공하는 것 이상의 프로토콜을 지원해야 하는 기업에 매우 중요합니다. VMware는 VCF를 통해 다양한 스토리지 유형을 지원합니다.

VCF에는 두 가지 주요 저장 유형이 있습니다.

- 주요 저장소 – 이 저장소 유형은 도메인을 처음 생성할 때 할당됩니다. 관리 도메인의 경우 이 저장소는 VCF 관리 및 운영 구성 요소를 보관합니다. 워크로드 도메인의 경우, 이 스토리지는 도메인이 배포된 워크로드, VM 또는 컨테이너를 지원하도록 설계되었습니다.
- 보조 스토리지 – 배포 후 모든 워크로드 도메인에 보조 스토리지를 추가할 수 있습니다. 이 스토리지 유형은 조직이 스토리지 인프라에 대한 기존 투자를 활용하고 다양한 스토리지 기술을 통합하여 성능, 확장성, 비용 효율성을 최적화하는 데 도움이 됩니다.

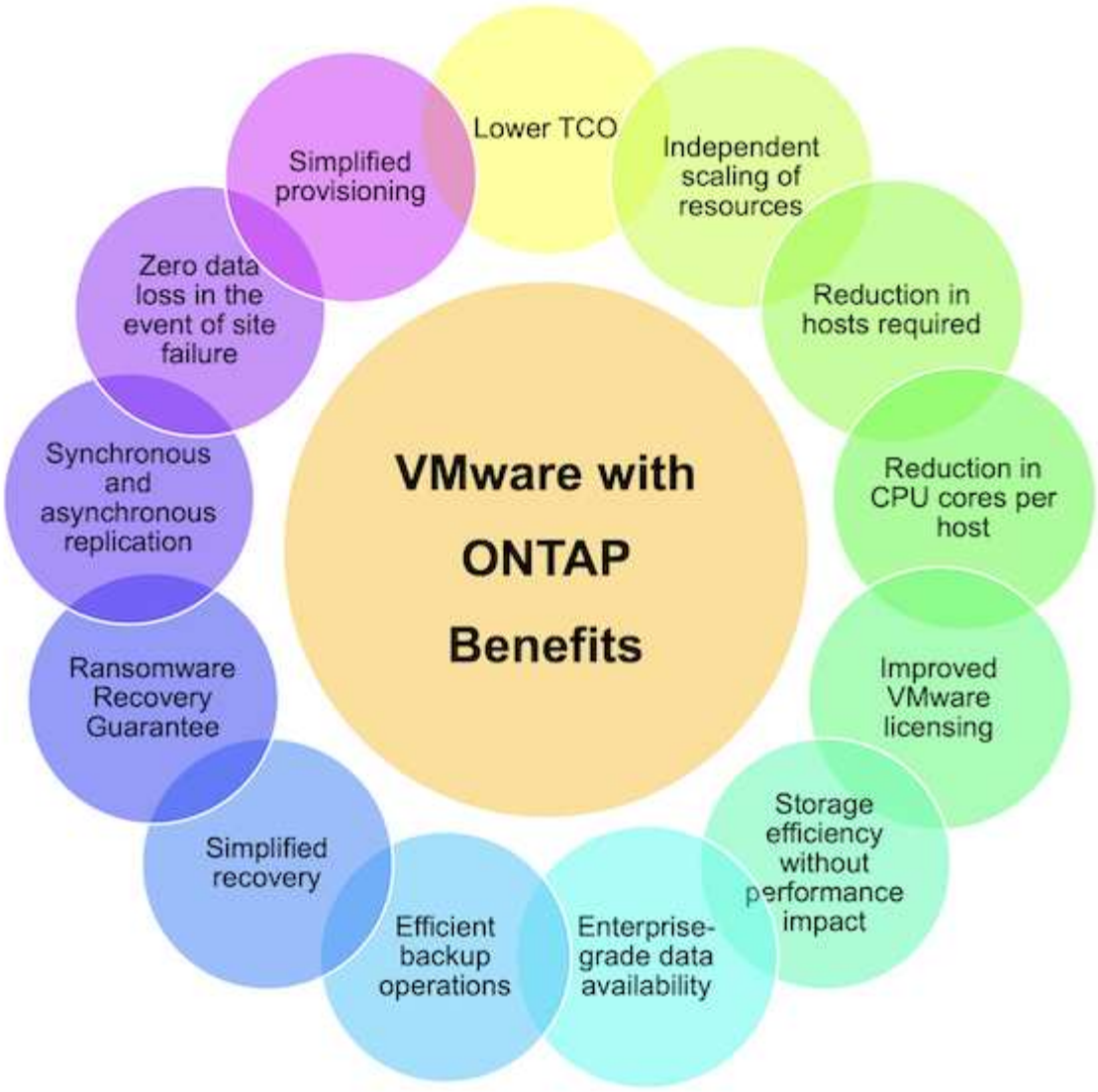
VCF 스토리지 유형 지원

도메인 유형	주요 저장소	보충 저장
관리 도메인	vSAN FC* NFS*	vVols (FC, iSCSI 또는 NFS) FC NFS iSCSI NVMe/TCP NVMe/FC NVMe/RDMA
가상 인프라 워크로드 도메인	vSAN vVols (FC, iSCSI 또는 NFS) FC NFS	vVols (FC, iSCSI 또는 NFS) FC NFS iSCSI NVMe/TCP NVMe/FC NVMe/RDMA

참고: * 기존 vSphere 환경에서 VCF 가져오기 도구를 사용할 경우 특정 프로토콜 지원이 제공됩니다.

VCF에 ONTAP 이유

투자 보호 및 다중 프로토콜 지원과 관련된 사용 사례 외에도 VCF 워크로드 도메인 내에서 외부 공유 스토리지를 활용해야 하는 데에는 여러 가지 이유가 있습니다. 워크로드 도메인에 프로비저닝된 스토리지는 단순히 VM과 컨테이너를 호스팅하는 저장소일 뿐이라고 가정할 수 있습니다. 그러나 조직의 요구가 라이선스 용량을 초과하여 엔터프라이즈급 스토리지가 필요한 경우가 많습니다. VCF 내의 도메인에 할당된 ONTAP 이 제공하는 스토리지는 배포가 쉽고 미래에도 사용할 수 있는 공유 스토리지 솔루션을 제공합니다.



아래에 식별된 VMware VCF의 주요 ONTAP 이점에 대한 자세한 내용은 다음을 참조하세요."VMware에 ONTAP 해야 하는 이유" .

- 1일차부터 확장에 따른 유연성
- ONTAP 에 스토리지 작업 오프로드
- 동급 최고의 저장 효율성
- 엔터프라이즈급 데이터 가용성
- 효율적인 백업 및 복구 작업
- 전체적인 비즈니스 연속성 기능

추가 정보:

- "NetApp 스토리지 옵션"
- "vSphere Metro Storage Cluster(vMSC) 지원"
- "VMware vSphere용 ONTAP 도구"

- "ONTAP 사용한 VMware 자동화"
- "NetApp SnapCenter"
- "VMware와 NetApp 활용한 하이브리드 멀티클라우드"
- "보안 및 랜섬웨어 보호"
- "VMware 워크로드를 NetApp 으로 쉽게 마이그레이션"
- "BlueXP 재해 복구"
- "데이터 인프라 통찰력"
- "VM 데이터 수집기"

요약

ONTAP 모든 작업 부하 요구 사항을 처리하는 플랫폼을 제공하며, 맞춤형 블록 스토리지 솔루션과 통합 제품을 제공하여 안정적이고 보안된 방식으로 VM과 애플리케이션에서 더 빠른 결과를 얻을 수 있도록 지원합니다. ONTAP 고급 데이터 감소 및 이동 기술을 통합하여 데이터 센터의 설치 공간을 최소화하는 동시에 중요한 워크로드를 온라인 상태로 유지하기 위해 엔터프라이즈 수준의 가용성을 보장합니다. 또한 AWS, Azure 및 Google은 VMware-in-the-Cloud 제품의 일부로 VMware 클라우드 기반 클러스터의 vSAN 스토리지를 향상시키기 위해 NetApp 기반 외부 스토리지를 지원합니다. 전반적으로 NetApp의 뛰어난 기능으로 인해 VMware Cloud Foundation 배포에 더 효과적인 선택이 됩니다.

문서 리소스

VMware Cloud Foundation에 대한 NetApp 제품에 대한 자세한 내용은 다음을 참조하세요.

VMware Cloud Foundation 문서

- "VMware Cloud Foundation 문서"
- NetApp 사용한 VCF에 대한 4부(4) 블로그 시리즈*
- "NetApp 과 VMware Cloud Foundation을 더욱 간편하게 1부: 시작하기"
- "NetApp 과 VMware Cloud Foundation을 더욱 간편하게 2부: VCF 및 ONTAP 주요 스토리지"
- "NetApp 과 VMware Cloud Foundation을 더욱 간편하게 3부: VCF와 Element 주요 스토리지"
- "NetApp 및 VMware Cloud Foundation을 더욱 간편하게 - 4부: VMware 및 보조 스토리지용 ONTAP 도구"
- NetApp All-Flash SAN 어레이를 갖춘 VMware Cloud Foundation*
- "NetApp ASA 어레이를 사용한 VCF, 소개 및 기술 개요"
- "FC와 함께 ONTAP 관리 도메인의 주요 스토리지로 사용"
- "VI 워크로드 도메인의 주요 스토리지로 FC와 함께 ONTAP 사용"
- "Ontap Tools를 사용하여 VCF 관리 도메인에 iSCSI 데이터 저장소를 배포합니다."
- "Ontap Tools를 사용하여 VCF 관리 도메인에 FC 데이터 저장소를 배포합니다."
- "Ontap Tools를 사용하여 VI 워크로드 도메인에 vVols (iSCSI) 데이터 저장소를 배포합니다."
- "VI 워크로드 도메인에서 사용할 NVMe over TCP 데이터 저장소 구성"
- "VI 워크로드 도메인에서 VM을 보호하고 복원하기 위해 SnapCenter Plug-in for VMware vSphere 배포하고 사용합니다."

- "VI 워크로드 도메인(NVMe/TCP 데이터 저장소)에서 VM을 보호하고 복원하기 위해 SnapCenter Plug-in for VMware vSphere 배포하고 사용합니다."
- NetApp All-Flash AFF 어레이를 갖춘 VMware Cloud Foundation*
- "NetApp AFF 어레이를 사용한 VCF, 소개 및 기술 개요"
- "관리 도메인의 주 저장소로 NFS와 함께 ONTAP 사용"
- "VI 워크로드 도메인의 주요 스토리지로 NFS와 함께 ONTAP 사용"
- "ONTAP 도구를 사용하여 VI 워크로드 도메인에 vVols (NFS) 데이터 저장소를 배포합니다."
- VMware Cloud Foundation을 위한 NetApp FlexPod 솔루션*
- "VMware Cloud Foundation을 통한 FlexPod 하이브리드 클라우드 확장"
- "VMware Cloud Foundation의 워크로드 도메인으로서의 FlexPod"
- "VMware Cloud Foundation 설계 가이드를 위한 워크로드 도메인으로서의 FlexPod"

VMware Cloud Foundation 및 ONTAP 사용한 디자인 옵션

VCF 9로 새로 시작하거나 기존 배포를 재사용하여 VCF 9와 ONTAP 사용하여 프라이빗 클라우드 환경을 만들 수 있습니다. VCF 9의 인기 있는 디자인 청사진과 NetApp 제품이 어떻게 가치를 더하는지 알아보세요.

저장 옵션

ONTAP 포함된 VMware Cloud Foundation은 다양한 성능, 확장성 및 가용성 요구 사항을 충족하기 위해 다양한 스토리지 구성을 지원합니다. 다음 표는 사용자 환경에서 사용할 수 있는 주요 저장소 옵션과 보조 저장소 옵션을 요약한 것입니다.

제품군	**FC의 VMFS**	**NFSv3**
ASA A-시리즈 및 C-시리즈	예	아니요
AFF A-시리즈 및 C-시리즈	예	예
FAS	예	예

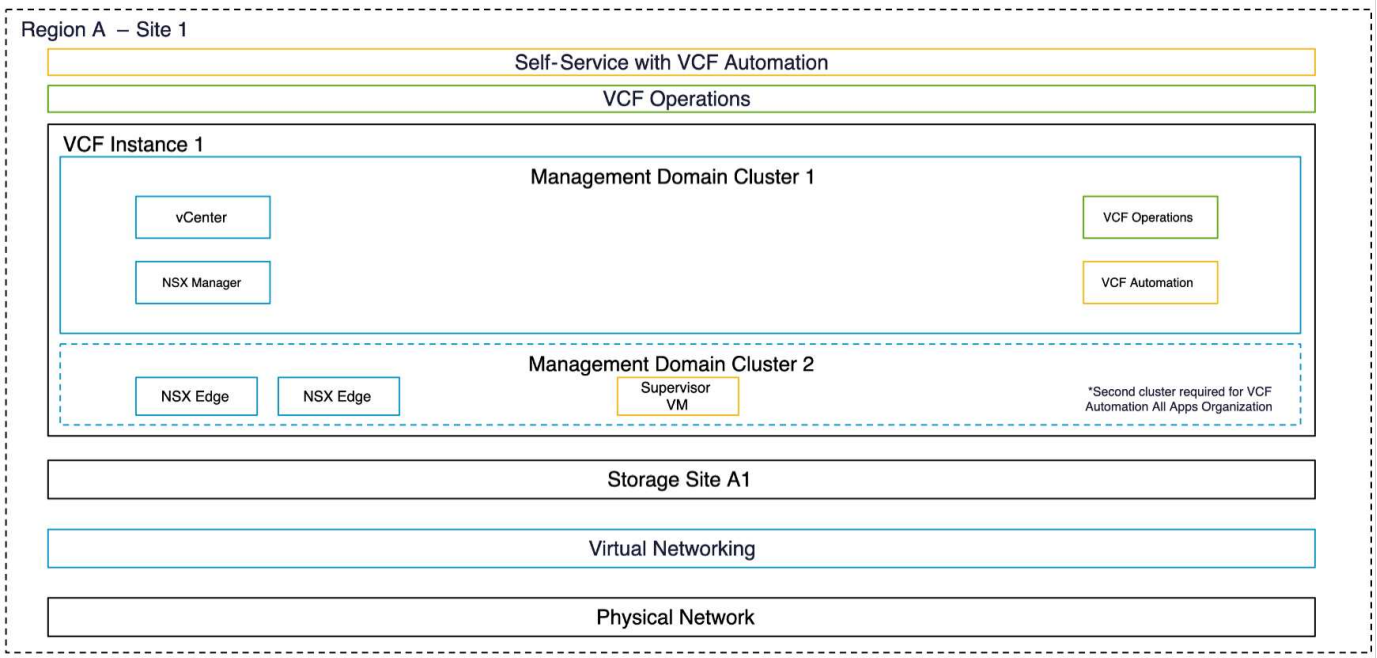
제품군	**FC의 VMFS**	**iSCSI의 VMFS**	**NVMe-oF의 VMFS**	**NFSv3**	**NFSv4.1**
ASA A-시리즈 및 C-시리즈	예	예	예	아니요	아니요
AFF A-시리즈 및 C-시리즈	예	예	예	예	예
FAS	예	예	예	예	예

청사진

다음 청사진은 다양한 사이트 및 리소스 시나리오에서 VMware Cloud Foundation과 ONTAP 에 대한 일반적인 배포 모델을 보여줍니다.

최소 설치 면적을 갖춘 단일 사이트의 **VCF** 함대

이 디자인 블루프린트는 최소한의 리소스로 단일 vSphere 클러스터에 관리 및 워크로드 구성 요소를 배포하기 위한 것입니다. VMFS 및 NFSv3 주요 데이터 저장소를 지원하고 2노드 구성을 통한 간단한 배포 옵션을 제공합니다. 모든 앱 조직 모델과 함께 VCF 자동화를 사용하려는 경우 vSphere Supervisor와 NSX Edge 노드를 배포할 두 번째 클러스터가 필요합니다.



리소스 소비를 최소화하려면 가능하면 기존 ONTAP 도구 인스턴스를 사용하세요. 사용할 수 없는 경우 작은 프로필을 갖춘 단일 노드가 적합합니다. SnapCenter Plug-in for VMware vSphere 기본 스냅샷과 다른 ONTAP 스토리지 어레이로의 복제를 사용하여 가상 머신과 데이터스토어를 보호합니다.

> VCF를 탐색할 리소스가 부족하다면 많은 클라우드 공급업체가 VCF를 서비스로 제공하고, ONTAP 클라우드 공급업체의 자체 서비스로 제공됩니다.

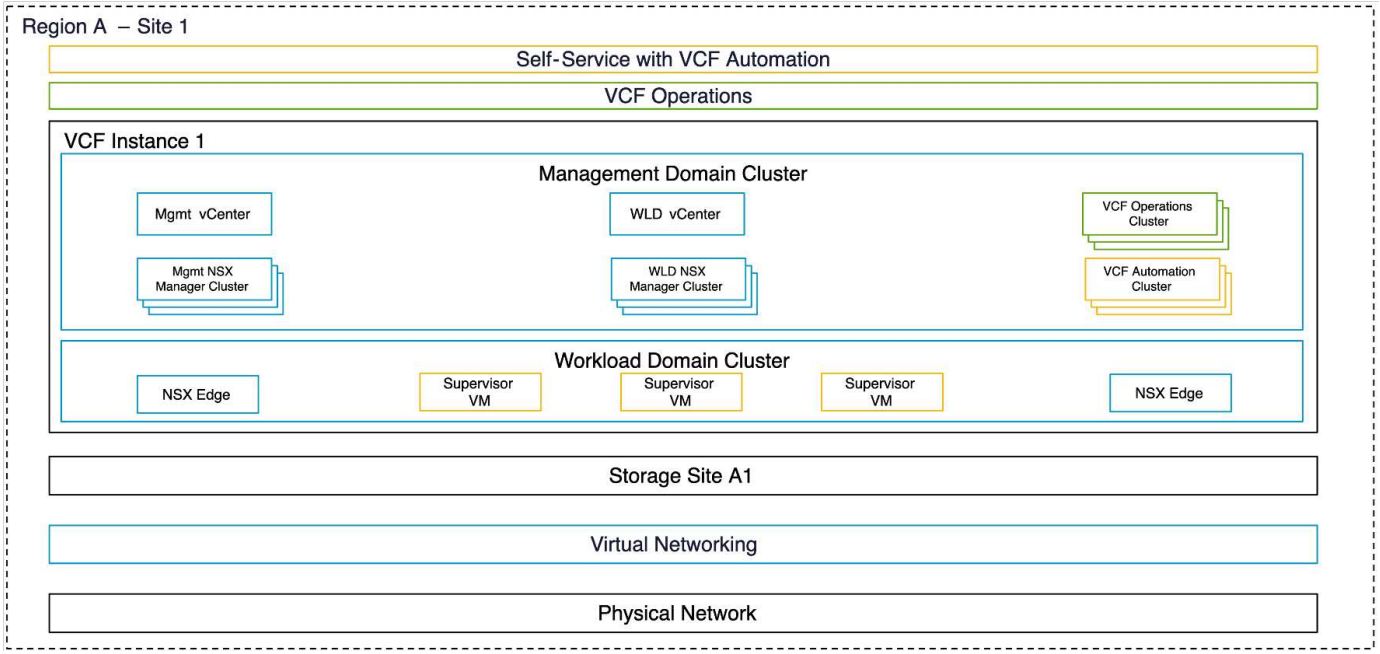
이 디자인에 대한 자세한 내용은 다음을 참조하세요."단일 사이트에서 최소한의 설치 공간으로 VCF 함대에 대한 Broadcom 기술 문서 제공" .

단일 사이트의 **VCF** 함대

이 설계 청사진은 애플리케이션 고가용성에 의존하는 단일 기본 데이터 센터를 사용하는 고객을 대상으로 합니다. 일반적으로 단일 VCF 환경이 관련됩니다. 블록 워크로드에는 ASA 사용하고 파일/통합 워크로드에는 AFF 사용할 수 있습니다.

콘텐츠 저장소는 VCF 도메인에서 VM 템플릿과 컨테이너 레지스트리를 공유합니다. FlexGroup Volume에 호스팅되는 경우 FlexCache 기능을 구독 데이터 저장소로 사용할 수 있습니다.

> FlexCache Datastore에서 VM을 호스팅하는 것은 지원되지 않습니다.



HA 모드에서 ONTAP 도구의 단일 인스턴스는 VCF 제품군의 모든 vCenter를 관리할 수 있습니다. 를 참조하세요"ONTAP 도구의 구성 제한" 자세한 내용은. ONTAP 도구는 VCF SSO 및 VCF OPS 스마트 그룹화와 통합되어 동일한 UI에서 여러 vCenter에 액세스할 수 있습니다.

ONTAP 도구를 사용한 VCF 보충 데이터 저장소

VM 및 데이터 저장소를 보호하려면 각 vCenter 인스턴스에 SnapCenter 플러그인을 배포해야 합니다.

스토리지 정책 기반 관리 기능은 vSphere Supervisor와 함께 사용되어 VKS의 제어 VM을 호스팅합니다. 태그는 VCF Ops에서 중앙 관리됩니다. NetApp Trident CSI는 VKS와 함께 사용되어 네이티브 어레이 기능을 활용한 애플리케이션 백업 보호를 구현합니다. vSphere CSI를 사용하면 영구 볼륨 세부 정보가 VCF Automation에 표시됩니다.

이 청사진에 대한 자세한 내용은 다음을 참조하세요."단일 사이트에서 VCF 제품군에 대한 Broadcom 기술 문서" .

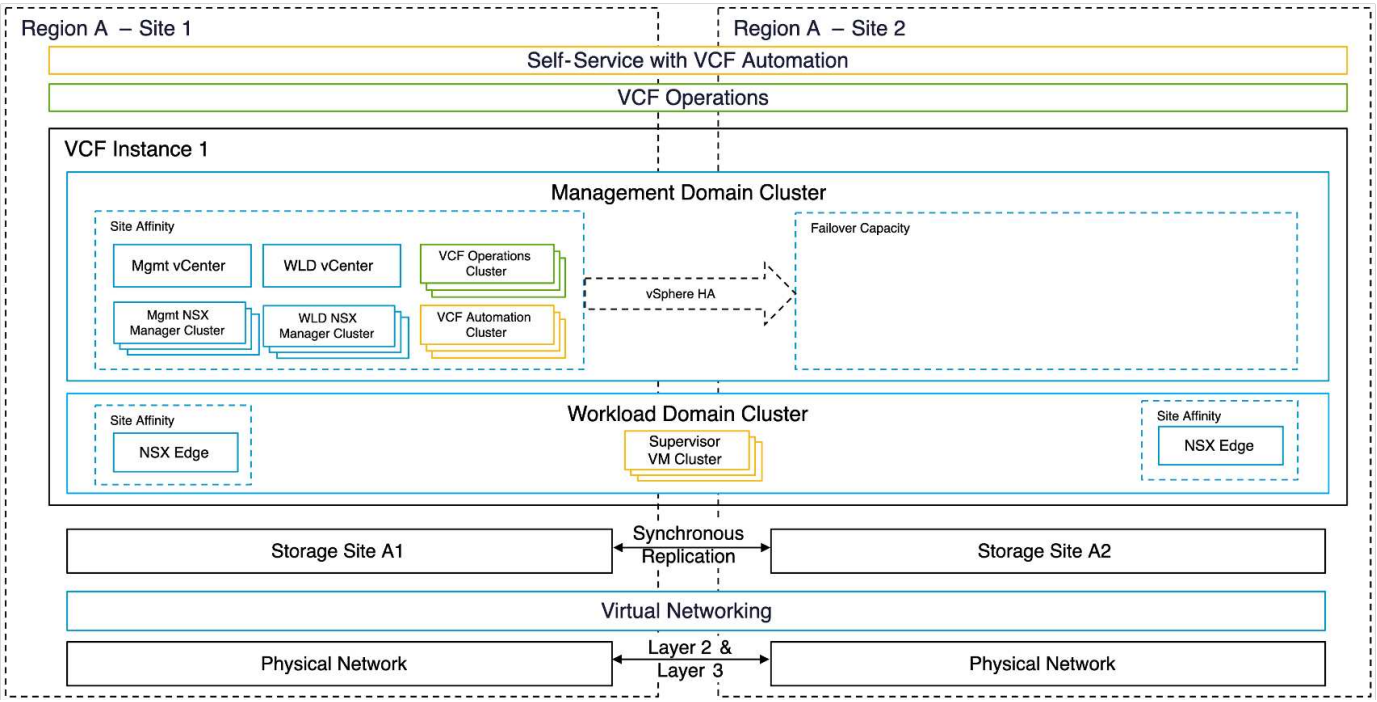
단일 지역에 여러 사이트가 있는 **VCF** 함대

이 디자인은 다양한 장애 도메인에 작업 부하를 분산하여 더 높은 가용성을 갖춘 클라우드형 서비스를 제공하는 고객을 위한 것입니다.

VMFS 데이터 저장소의 경우 SnapMirror Active Sync는 vSphere Metro Storage Cluster와 함께 사용할 수 있는 액티브-액티브 스토리지 유닛을 제공합니다. 균일 액세스 모드는 투명한 스토리지 장애 조치를 제공하는 반면, 비균일 액세스 모드는 장애 도메인 장애 발생 시 VM을 다시 시작해야 합니다.

NFS 데이터 저장소의 경우, vSphere Metro Storage Cluster를 탑재한 ONTAP MetroCluster 높은 가용성을 보장합니다. 중재자는 분할 두뇌 시나리오를 피하고 이제 BlueXP 에서 호스팅될 수 있습니다.

VM 배치 규칙은 관리 도메인 구성 요소에 대해 동일한 장애 도메인 내의 VM을 제어합니다.



ONTAP 도구는 SnapMirror 활성 동기화 관계를 설정하는 UI를 제공합니다. 두 장애 도메인의 스토리지 시스템은 ONTAP 도구와 SnapCenter Plug-in for VMware vSphere 에 등록되어야 합니다.

SnapMirror 및 SnapMirror to Cloud를 통해 VM용 BlueXP Backup and Recovery를 사용하여 3-2-1 백업 정책을 구현할 수 있습니다. 세 위치 중 어느 곳에서나 복원을 수행할 수 있습니다.

Kubernetes용 Trident Protect 또는 BlueXP Backup and Recovery는 VKS 클러스터 애플리케이션을 보호합니다.

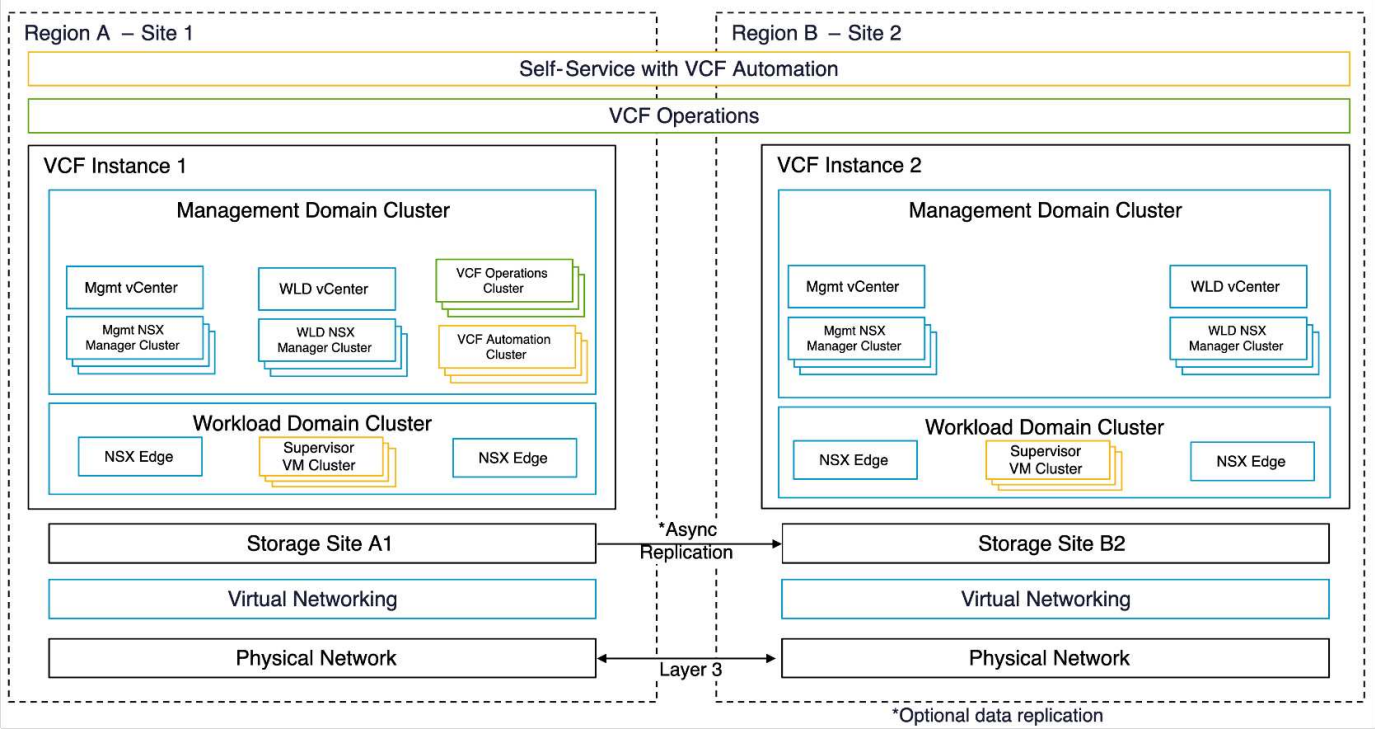
자세한 내용은 다음을 확인하세요."단일 지역에 여러 사이트가 있는 VCF 함대에 대한 Broadcom 기술 문서" .

여러 지역에 걸쳐 여러 사이트를 보유한 **VCF** 함대

이 디자인은 전 세계에 퍼져 있는 고객을 대상으로 하며, 근접 서비스와 재해 복구 솔루션을 제공합니다.

VMware Live Site Recovery 또는 BlueXP Disaster Recovery as a Service를 사용하여 VM의 재해 복구를 관리할 수 있습니다. ONTAP 도구는 ONTAP 사용하여 스토리지 작업을 조율하기 위한 SRA(스토리지 복제 어댑터)를 제공합니다.

제품군	**SnapMirror** 액티브 싱크	**MetroCluster**
ASA A-시리즈 및 C-시리즈	예	예
AFF A-시리즈 및 C-시리즈	예	예
FAS	아니요	예



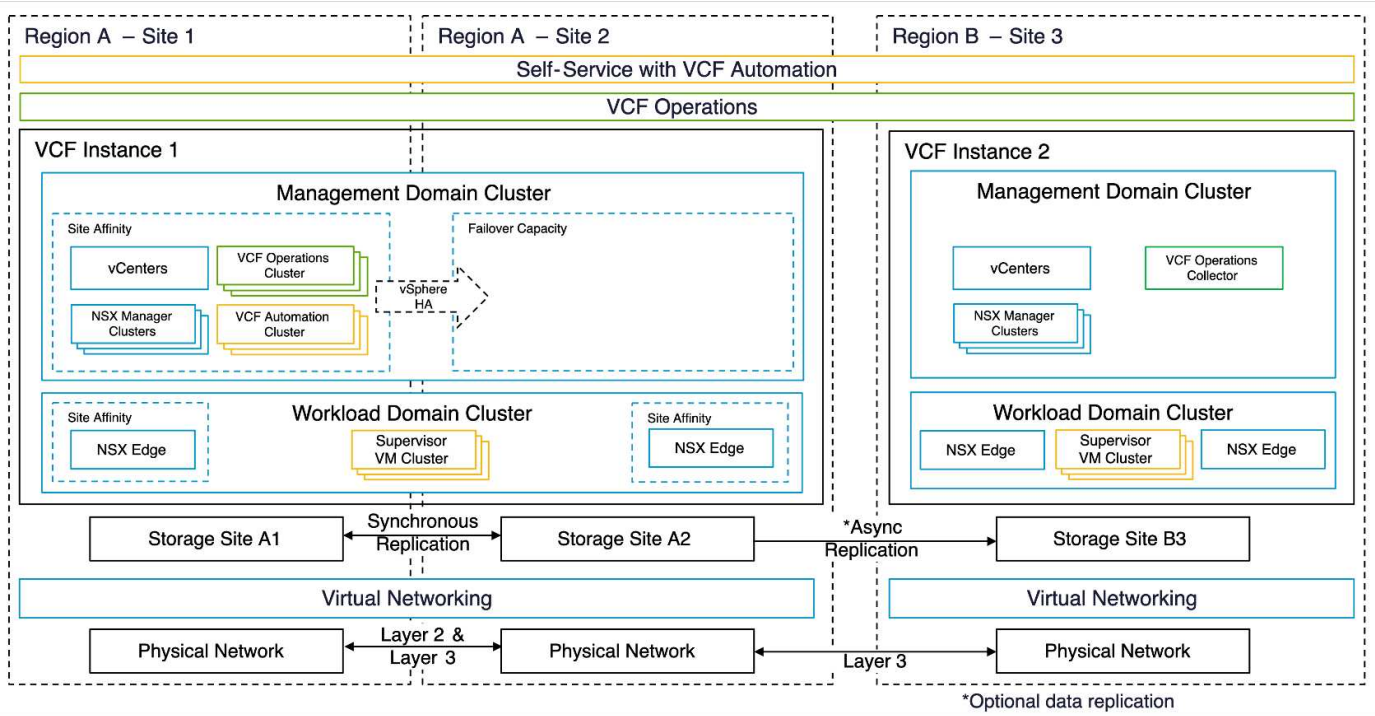
ONTAP 도구는 데이터 저장소 복제 설정을 위한 UI를 제공합니다. BlueXP 스토리지 어레이 간 복제에도 사용할 수 있습니다. SnapCenter Plug-in for VMware vSphere SnapShots에 대한 기존 SnapMirror 관계를 활용합니다.

자세한 내용은 다음을 확인하세요."여러 지역에 걸쳐 여러 사이트를 보유한 VCF 함대에 대한 Broadcom 기술 문서" .

단일 지역에 여러 사이트가 있는 **VCF** 함대와 추가 지역

이 설계는 VM과 VKS 애플리케이션의 가용성과 재해 복구를 모두 다룹니다.

ASA, AFF, FAS 이 디자인 옵션을 지원합니다.



ONTAP 도구나 BlueXP 사용하여 복제 관계를 설정할 수 있습니다.

자세한 내용은 다음을 참조하십시오. "단일 지역 내 여러 사이트와 추가 지역이 있는 VCF 함대에 대한 Broadcom 기술 문서" .

VMware Cloud Foundation 및 ONTAP 사용하여 프라이빗 클라우드 환경 설정

ONTAP 사용하여 VMware Cloud Foundation 9 환경을 배포, 융합 또는 업그레이드합니다. 새로운 VCF 9.0 환경을 설정하고, 기존 vCenter 인스턴스와 ONTAP 데이터 저장소를 통합하고, 이전 VCF 배포를 업그레이드하는 방법을 알아보세요.

새로운 VCF 9 인스턴스 배포

이 워크플로를 사용하여 깨끗한 VMware Cloud Foundation(VCF) 9.0 환경을 배포합니다. 배포 후에는 워크로드를 마이그레이션하거나 애플리케이션 프로비저닝을 시작하고 인프라 서비스를 제공할 수 있습니다.

상위 레벨 단계는 다음을 참조하세요."빌드 여정 – 새로운 VMware Cloud Foundation 배포 설치" .

단계

1. 를 따르세요"Broadcom VCF 9 배포 단계" .
2. 배포 준비 단계에서는 주요 스토리지 옵션에 대한 작업을 완료합니다.

FC의 VMFS

1. 모든 ESXi 호스트의 WWPN을 수집합니다. 당신은 실행할 수 있습니다 `esxcli storage san fc list` , ESXi 호스트 클라이언트를 사용하거나 PowerCLI를 사용하세요.
2. 구역 지정을 구성합니다. 보다 "ONTAP 시스템에 권장되는 FC 구역 구성" .

   ⓘ 물리적 어댑터 WWPN이 아닌 SVM 논리 인터페이스(LIF)의 WWPN을 사용하세요.

3. System Manager, ONTAP CLI 또는 API를 사용하여 LUN을 생성하고 WWPN을 통해 호스트에 매핑합니다.
4. ESXi에서 스토리지 어댑터를 다시 스캔하고 VMFS 데이터 저장소를 생성합니다.

NFSv3

1. 하나의 ESXi 호스트에 VMkernel 인터페이스를 만듭니다.
2. 확인하십시오"SVM에는 NFS가 활성화되어 있습니다." 그리고"NFS를 통한 vStorage가 활성화되었습니다." .
3. 볼륨을 생성하고 ESXi 호스트를 허용하는 정책과 함께 내보냅니다.
4. 필요에 따라 권한을 조정하세요.
5. ONTAP NFS VAAI VIB를 배포하고 vLCM 이미지에 포함합니다. 예를 들어: `esxcli software vib install -d /NetAppNasPlugin2.0.1.zip` . (NetApp 지원 사이트에서 ZIP을 다운로드하세요.)
6. VMkernel 인터페이스를 생성한 호스트에 NFS 볼륨을 마운트합니다. 예를 들어: `esxcli storage nfs add -c 4 -H 192.168.122.210 -s /use1_m01_nfs01 -v use1-m01-cl01-nfs01` .

   ⓘ 그만큼 `nConnect` 세션 수는 호스트당입니다. 필요에 따라 배포 후 다른 호스트를 업데이트합니다.

1. **VCF** 함대 배포 단계의 *배포 요약 확인 및 다음 단계 검토*가 끝나면 다음을 완료하세요.
   a. ONTAP 도구 배포
      - "ONTAP 도구 10.x 다운로드"NetApp 지원 사이트에서.
      - ONTAP 도구 관리자, 노드 및 내부 통신에 사용되는 가상 IP에 대한 DNS 레코드를 만듭니다.
      - OVA를 관리 vCenter Server에 배포합니다.
      - "관리 도메인 vCenter 등록"ONTAP 도구 관리자를 사용하여.
      - "저장소 백엔드 추가"vSphere Client UI를 사용합니다.
      - "보충 데이터 저장소 만들기"(콘텐츠 레지스트리를 하나 포함).
      - HA 배포를 계획하는 경우 콘텐츠 레지스트리를 만듭니다.
      - "HA 활성화"ONTAP 도구 관리자에서.
   b. SnapCenter 플러그인 배포
      - "SnapCenter Plug-in for VMware vSphere 배포" .
      - "저장소 백엔드 추가" .
      - "백업 정책 생성" .

        - "리소스 그룹 생성" .
    c. BlueXP 커넥터 배포
        - "커넥터 없이 할 수 있는 일을 검토하세요" .
        - "커넥터 배포" .
    d. 백업 및 복구에 BlueXP 사용하세요
        - "VM 워크로드 보호" .
        - "VKS 워크로드 보호" .
2. VCF 인스턴스에서 vCenter를 워크로드 도메인으로 가져온 후 다음을 완료하세요.
    a. ONTAP 도구 등록
        - "워크로드 도메인 vCenter 등록"ONTAP 도구 관리자를 사용하여.
        - "저장소 백엔드 추가"vSphere Client UI를 사용합니다.
        - "보충 데이터 저장소 만들기" .
    b. SnapCenter Plug-in for VMware vSphere 배포
        - "SnapCenter Plug-in for VMware vSphere 배포" .
        - "저장소 백엔드 추가" .
        - "백업 정책 생성" .
        - "리소스 그룹 생성" .
    c. 백업 및 복구에 BlueXP 사용하세요
        - "VM 워크로드 보호" .
        - "VKS 워크로드 보호" .

새로운 워크로드 도메인을 생성할 때마다 이러한 단계를 재사용할 수 있습니다.

기존 구성 요소를 **VCF 9**로 수렴

이미 VCF 차량의 일부 구성 요소를 보유하고 있고 이를 재사용하는 것을 선호할 수도 있습니다. vCenter 인스턴스를 재사용하는 경우 데이터 저장소는 ONTAP 도구로 프로비저닝되는 경우가 많으며, 이는 VCF의 주요 저장소 역할을 할 수 있습니다.

필수 조건

- 기존 vCenter 인스턴스가 작동하는지 확인합니다.
- ONTAP 에서 제공하는 데이터 저장소를 사용할 수 있는지 확인하세요.
- 에 대한 액세스를 보장합니다"상호 운용성 매트릭스" .

단계

1. 검토하다"VCF로 수렴하기 위한 지원 시나리오" .
2. ONTAP 에서 프로비저닝한 데이터 저장소를 주 저장소로 사용하여 vCenter 인스턴스를 수렴합니다.
3. 다음을 사용하여 지원되는 버전을 확인하세요."상호 운용성 매트릭스" .
4. 치받이"ONTAP 도구" 필요한 경우.

5. 업그레이드"VMware vSphere용 SnapCenter 플러그인" 필요한 경우.

기존 VCF 환경을 VCF 9로 업그레이드

표준 업그레이드 프로세스를 사용하여 이전 VCF 배포를 버전 9.0으로 업그레이드합니다. 그 결과, 업그레이드된 관리 및 워크로드 도메인을 갖춘 버전 9.0을 실행하는 VCF 환경이 탄생했습니다.

필수 조건

- 관리 도메인과 워크로드 도메인을 백업합니다.
- ONTAP 도구와 SnapCenter 플러그인이 VCF 9.0과 호환되는지 확인하세요. 를 따르세요"상호 운용성 매트릭스" 에게"ONTAP 도구 업그레이드" 그리고"VMware vSphere용 SnapCenter 플러그인" VCF 9에서 지원되는

단계

1. VCF 관리 도메인을 업그레이드합니다. 보다"VCF 관리 도메인을 VCF 9로 업그레이드" 지침을 보려면.
2. 모든 VCF 5.x 워크로드 도메인을 업그레이드합니다. 보다"VCF 5.x 워크로드 도메인을 VCF 9로 업그레이드" 지침을 보려면.

NetApp SnapMirror 및 BlueXP DRaaS를 사용한 재해 복구 구현

NetApp SnapMirror 및 BlueXP DRaaS를 사용한 NFS 데이터 저장소를 위한 VCF 재해 복구 솔루션

운영 사이트에서 재해 복구(DR) 사이트로 블록 수준 복제를 수행하면 랜섬웨어 공격을 포함한 사이트 중단 및 데이터 손상 사건으로부터 워크로드를 보호하는 탄력적이고 비용 효율적인 전략을 제공합니다. NetApp SnapMirror 복제를 사용하면 NFS 또는 VMFS 데이터 저장소를 사용하여 온프레미스 ONTAP 시스템에서 실행되는 VMware VCF 9 워크로드 도메인을 VMware가 배포된 지정된 복구 데이터 센터에 있는 보조 ONTAP 시스템으로 복제할 수 있습니다.

이 섹션에서는 온프레미스 VMware 가상 머신에 대한 재해 복구를 구축하기 위해 BlueXP 재해 복구 서비스(DRaaS)를 구성하는 방법을 간략하게 설명합니다.

설정에는 다음이 포함됩니다.

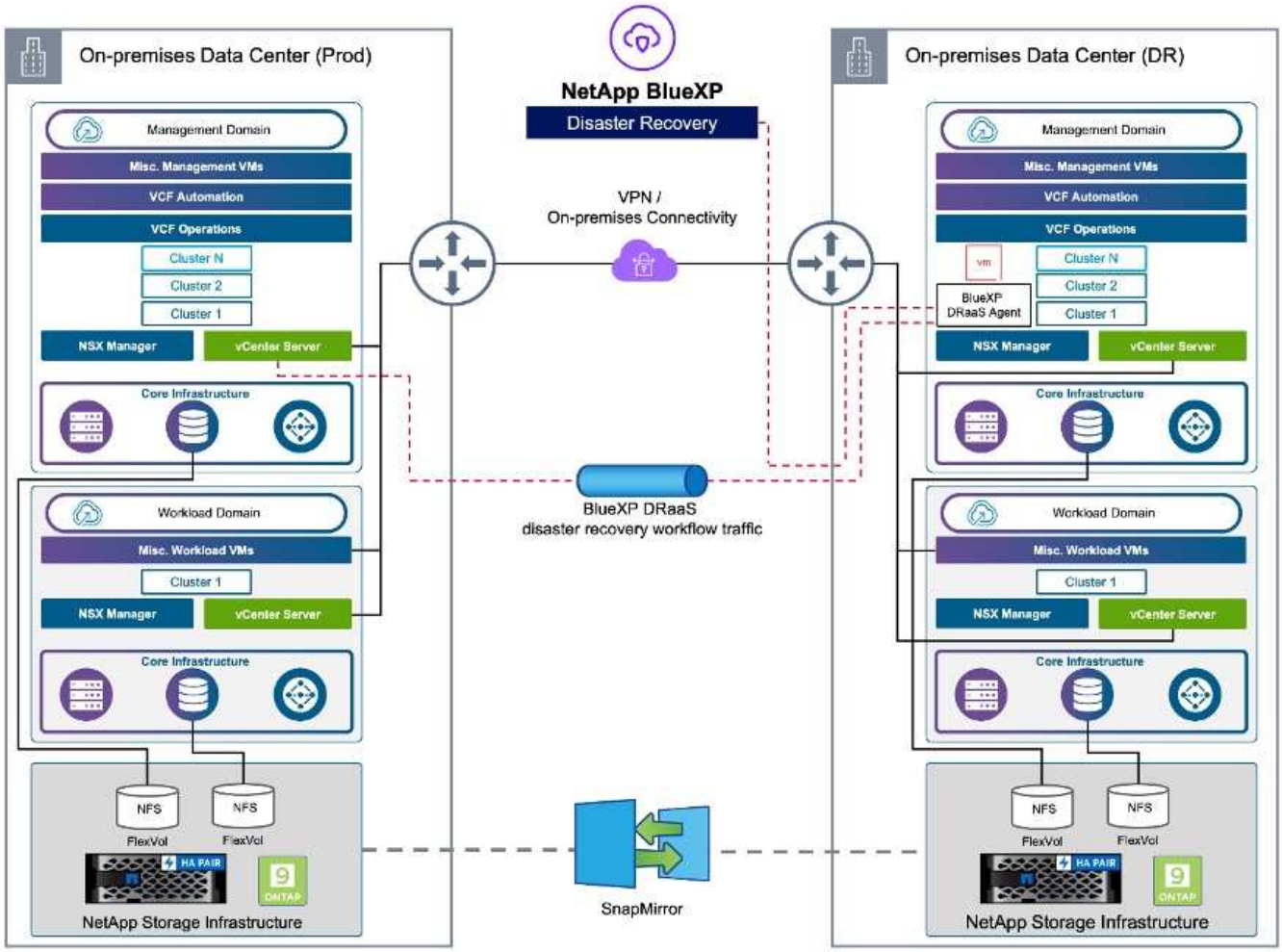
- BlueXP 계정을 만들고 BlueXP 커넥터를 배포합니다.
- BlueXP 캔버스에 ONTAP 어레이를 추가하여 VMware vCenter와 ONTAP 스토리지 간 통신을 원활하게 합니다.
- SnapMirror 사용하여 사이트 간 복제를 구성합니다.
- 장애 조치 준비 상태를 검증하기 위한 복구 계획을 설정하고 테스트합니다.

NetApp BlueXP 콘솔에 통합된 BlueXP disaster recovery 서비스를 통해 조직은 온프레미스 VMware vCenter 및 ONTAP 스토리지 시스템을 원활하게 검색할 수 있습니다. 문제가 발견되면 관리자는 리소스 그룹을 정의하고, 재해 복구 계획을 만들고, 이를 적절한 리소스와 연결하고, 장애 조치 및 장애 복구 작업을 시작하거나 테스트할 수 있습니다. NetApp SnapMirror 효율적인 블록 수준 복제를 제공하여 DR 사이트가 증분 업데이트를 통해 프로덕션 환경과 동기화 상태를 유지하도록 보장합니다. 이를 통해 복구 지점 목표(RPO)를 최소 5분으로 단축할 수 있습니다.

BlueXP DRaaS는 중단 없는 재해 복구 테스트도 지원합니다. ONTAP의 FlexClone 기술을 활용하여 프로덕션 작업 부하에 영향을 주거나 추가 스토리지 비용을 발생시키지 않고 가장 최근에 복제된 스냅샷에서 NFS 데이터 저장소의 공간 효율적인 임시 복사본을 생성합니다. 테스트 후에는 환경을 쉽게 해체하여 복제된 데이터의 무결성을 보존할 수 있습니다.

실제로 장애 조치가 발생하는 경우 BlueXP 복구 프로세스를 조율하여 최소한의 사용자 개입으로 지정된 DR 사이트에서 보호된 가상 머신을 자동으로 실행합니다. 기본 사이트가 복구되면 서비스는 SnapMirror 관계를 역전시키고 모든 변경 사항을 원래 사이트로 복제하여 원활하고 제어된 장애 복구를 가능하게 합니다.

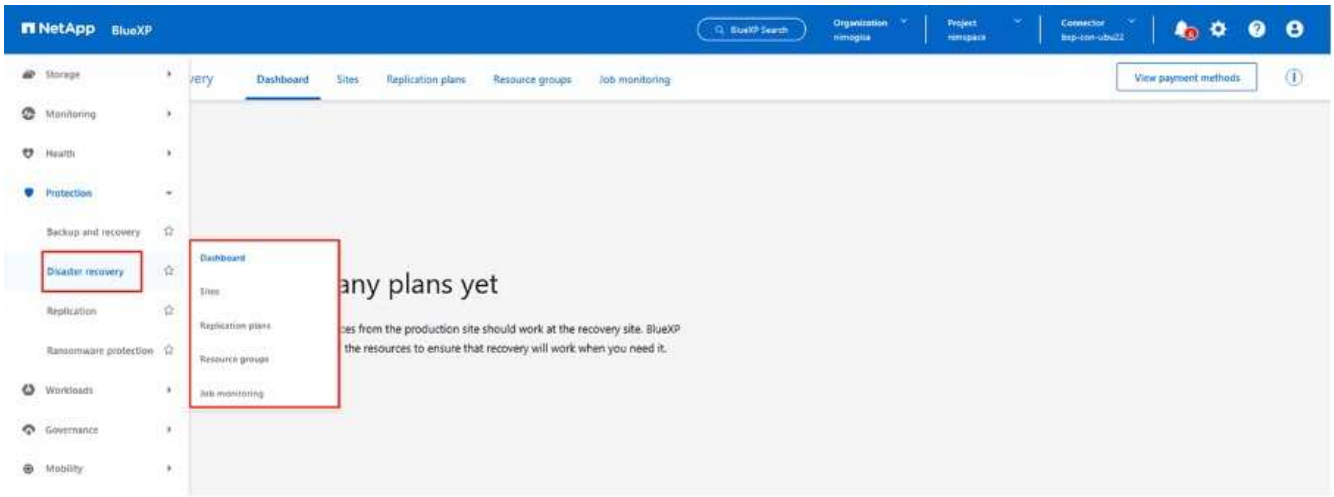
이러한 모든 기능은 기존 재해 복구 솔루션에 비해 상당히 낮은 비용으로 제공됩니다.



시작하기

BlueXP disaster recovery 시작하려면 BlueXP 콘솔을 사용한 다음 서비스에 액세스하세요.

1. BlueXP 에 로그인하세요.
2. BlueXP 왼쪽 탐색 창에서 보호 > 재해 복구를 선택합니다.
3. BlueXP disaster recovery 보드가 나타납니다.



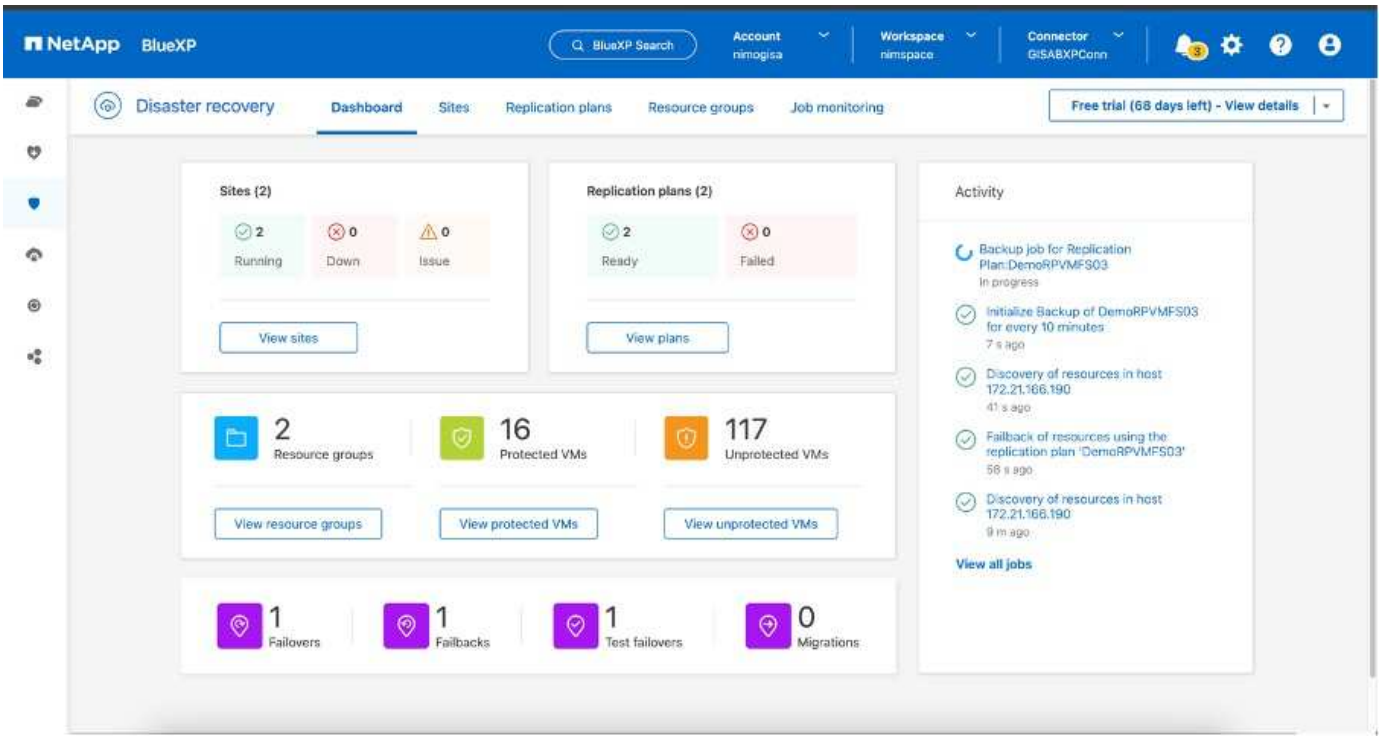
재해 복구 계획을 구성하기 전에 다음 사항을 확인하십시오."필수 조건" 충족됩니다:

- BlueXP Connector는 NetApp BlueXP 에 설정되어 있습니다.
- BlueXP 커넥터 인스턴스는 소스 및 대상 워크로드 도메인 vCenter와 스토리지 시스템에 연결할 수 있습니다.
- NetApp Data ONTAP 클러스터는 NFS 또는 VMFS 데이터 저장소를 제공합니다.
- VMware용 NFS 또는 VMFS 데이터 저장소를 호스팅하는 온프레미스 NetApp 스토리지 시스템이 BlueXP 에 추가되었습니다.
- DNS 이름을 사용하는 경우 DNS 확인이 이루어져야 합니다. 그렇지 않은 경우 vCenter에 IP 주소를 사용하세요.
- SnapMirror 복제는 지정된 NFS 또는 VMFS 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.

참고: NetApp BlueXP 커넥터가 네트워크를 통해 소스 및 대상 리소스와 통신할 수 있도록 대상 사이트나 제3의 사이트에 BlueXP 커넥터를 배포하는 것을 권장합니다.

이 데모에서는 워크로드 도메인이 ONTAP NFS 스토리지로 구성됩니다. VMFS 기반 데이터 저장소의 워크플로 단계는 동일하게 유지됩니다.



BlueXP disaster recovery 구성

재해 복구를 준비하는 첫 번째 단계는 소스 vCenter 및 스토리지 리소스를 검색하여 BlueXP disaster recovery 에 추가하는 것입니다.

BlueXP 콘솔을 열고 왼쪽 탐색에서 보호 > 재해 복구를 선택합니다. vCenter 서버 검색을 선택하거나 상단 메뉴에서 사이트 > 추가 > vCenter 추가를 선택합니다.

다음 플랫폼을 추가하세요:

- 소스 워크로드 도메인 vCenter
- 대상 워크로드 도메인 vCenter.

vCenter가 추가되면 자동 검색이 실행됩니다.

소스 사이트 배열과 대상 사이트 배열 간 스토리지 복제 구성

SnapMirror NetApp 환경에서 데이터 복제를 제공합니다. NetApp Snapshot® 기술을 기반으로 구축된 SnapMirror 복제는 이전 업데이트 이후 변경되거나 추가된 블록만 복제하므로 매우 효율적입니다. SnapMirror NetApp OnCommand® System Manager나 ONTAP CLI를 사용하여 쉽게 구성할 수 있습니다. BlueXP DRaaS는 클러스터와 SVM 피어링이 사전에 구성된 경우 SnapMirror 관계도 생성합니다.

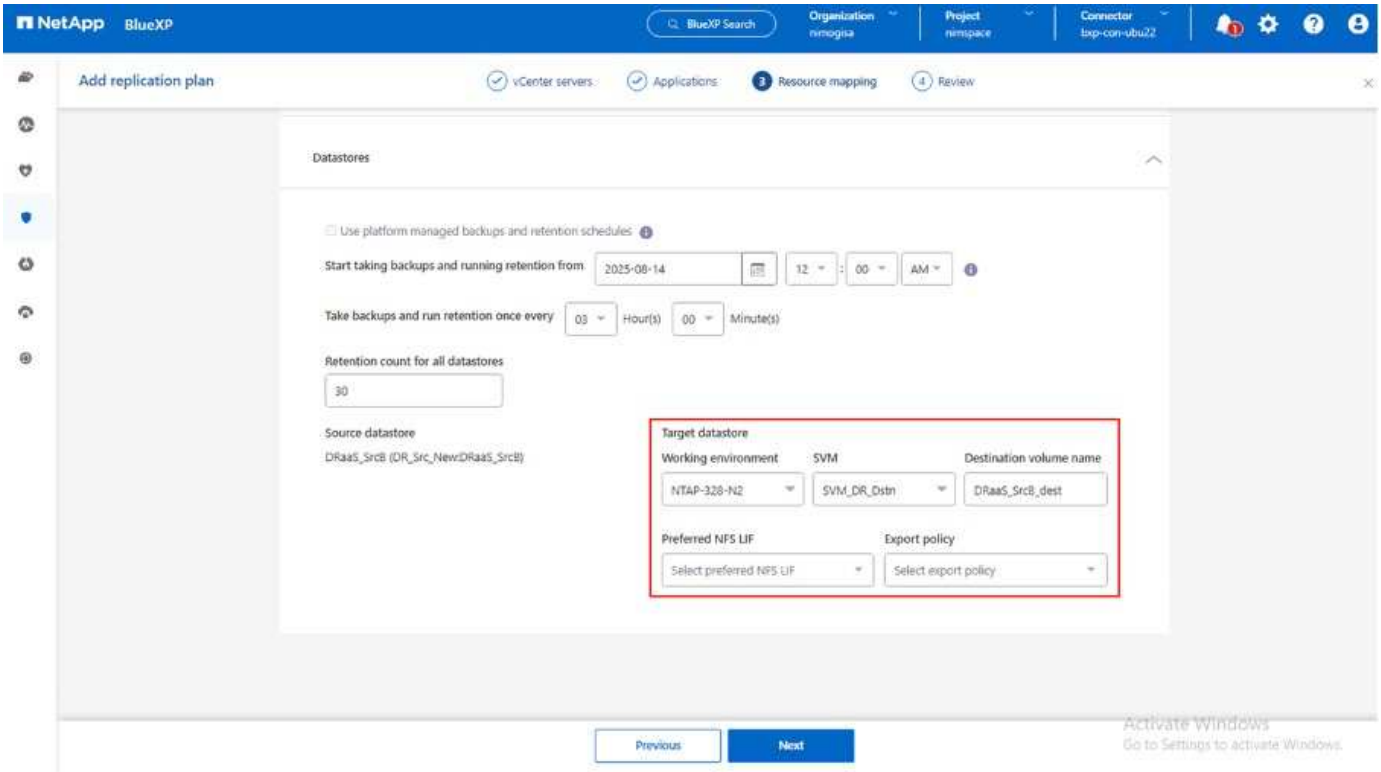
기본 스토리지가 완전히 손실되지 않은 경우 SnapMirror 기본 사이트와 DR 사이트를 다시 동기화하는 효율적인 수단을 제공합니다. SnapMirror 두 사이트를 다시 동기화하여 SnapMirror 관계를 간단히 반대로 하여 DR 사이트에서 기본 사이트로 변경된 데이터나 새 데이터만 전송할 수 있습니다. 즉, BlueXP DRaaS의 복제 계획은 장애 조치 후 전체 볼륨을 다시 복사하지 않고도 어느 방향으로든 다시 동기화될 수 있습니다. 관계가 역방향으로 재동기화되는 경우 스냅샷 복사본의 마지막 성공적인 동기화 이후에 작성된 새 데이터만 대상으로 다시 전송됩니다.

> CLI 또는 시스템 관리자를 통해 볼륨에 대한 SnapMirror 관계가 이미 구성된 경우 BlueXP DRaaS는 해당 관계를 선택하고 나머지 워크플로 작업을 계속 진행합니다.

VMware 재해 복구를 설정하는 방법

SnapMirror 복제를 생성하는 프로세스는 모든 애플리케이션에서 동일하게 유지됩니다. 이 과정은 수동이거나 자동화될 수 있습니다. 가장 쉬운 방법은 BlueXP DRaaS를 활용하는 것입니다. 다음 두 가지 기준이 충족되면 이 서비스를 자동화할 수 있습니다.

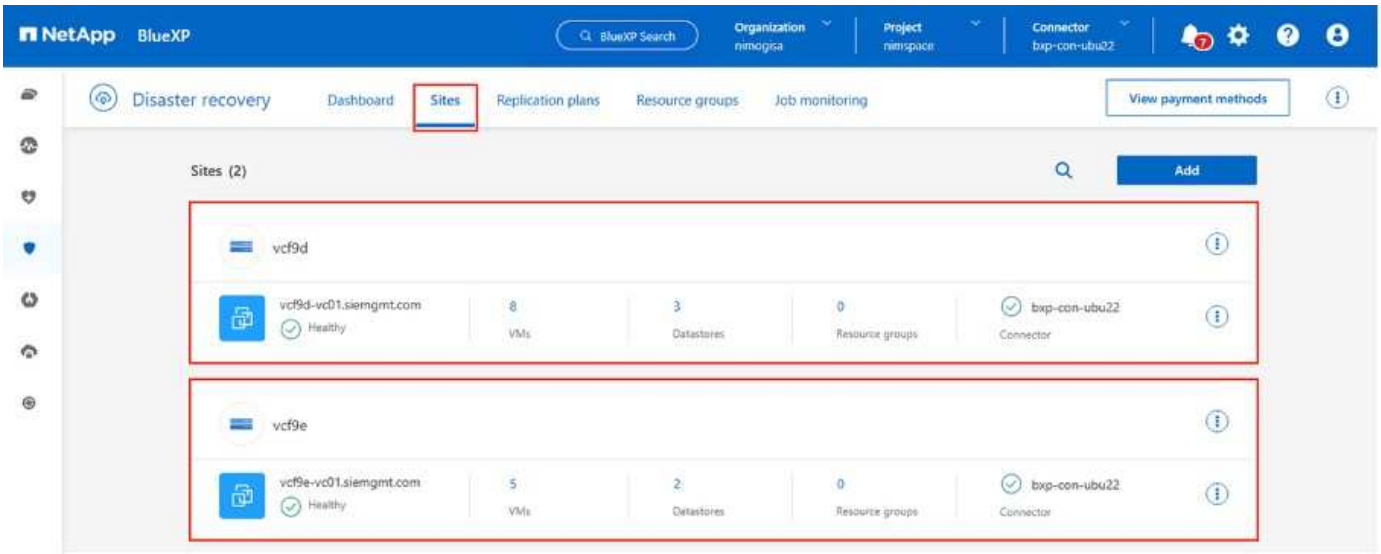
- 소스 클러스터와 대상 클러스터는 피어 관계를 갖습니다.
- 소스 SVM과 대상 SVM은 피어 관계를 갖습니다.



BlueXP 또한 환경의 소스 ONTAP 시스템을 대상 환경으로 간단히 끌어서 놓아 나머지 프로세스를 안내하는 마법사를 실행함으로써 SnapMirror 복제를 구성하는 대체 옵션을 제공합니다.

BlueXP disaster recovery 귀사를 위해 무엇을 해드릴 수 있나요?

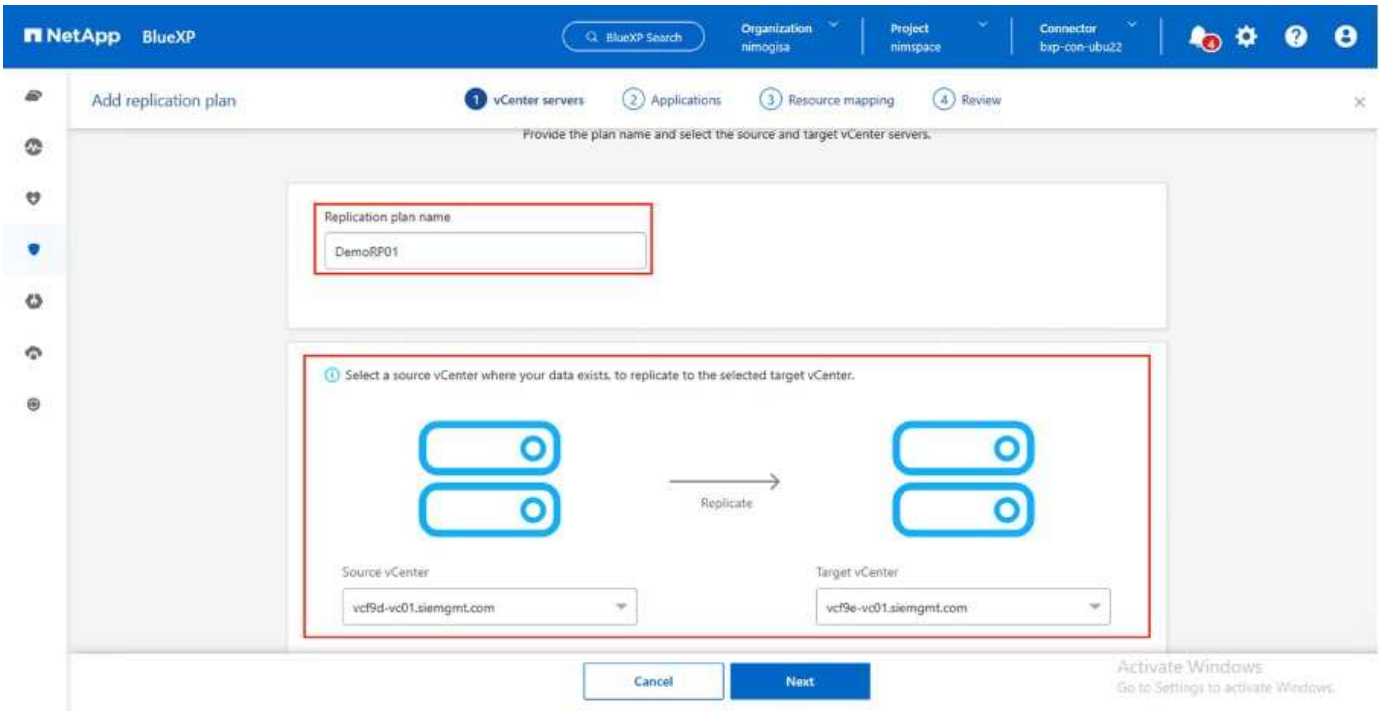
소스 사이트와 대상 사이트가 추가되면 BlueXP disaster recovery 자동으로 심층 검색을 수행하고 관련 메타데이터와 함께 VM을 표시합니다. BlueXP disaster recovery 은 VM에서 사용하는 네트워크와 포트 그룹을 자동으로 감지하여 채웁니다.



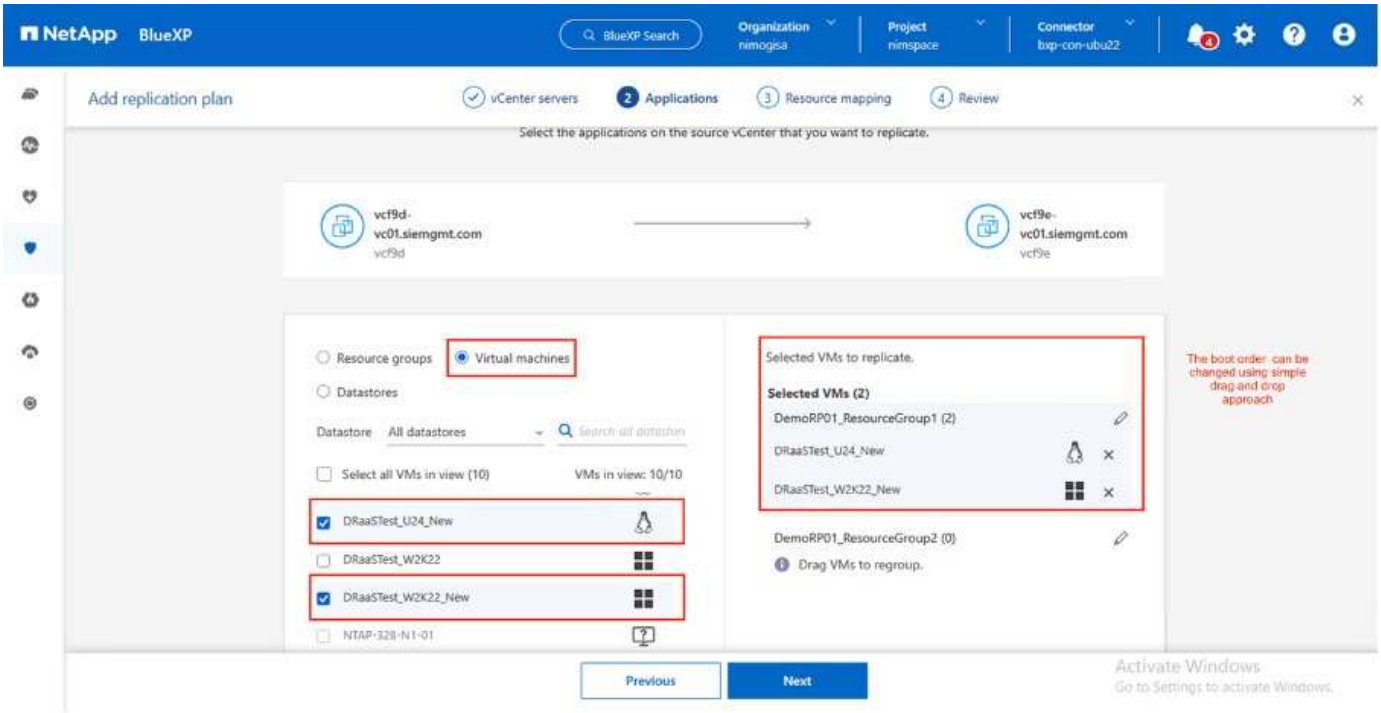
사이트를 추가한 후 드롭다운에서 소스 및 대상 vCenter 플랫폼을 선택하여 복제 계획을 구성하고 계획에 포함할 리소스 그룹을 선택하고, 애플리케이션을 복원하고 전원을 켜는 방법, 클러스터 및 네트워크 매핑을 그룹화합니다. 복구 계획을 정의하려면 복제 계획 탭으로 이동하여 *계획 추가*를 클릭합니다.

이 단계에서는 VM을 리소스 그룹으로 그룹화할 수 있습니다. BlueXP disaster recovery 리소스 그룹을 사용하면 종속된 VM 세트를 논리적 그룹으로 그룹화할 수 있으며, 이 그룹에는 복구 시 실행될 수 있는 부팅 순서와 부팅 지연이 포함됩니다. 리소스 그룹은 리소스 그룹 탭을 사용해서 만들 수도 있습니다.

먼저 소스 vCenter를 선택한 다음 대상 vCenter를 선택합니다.



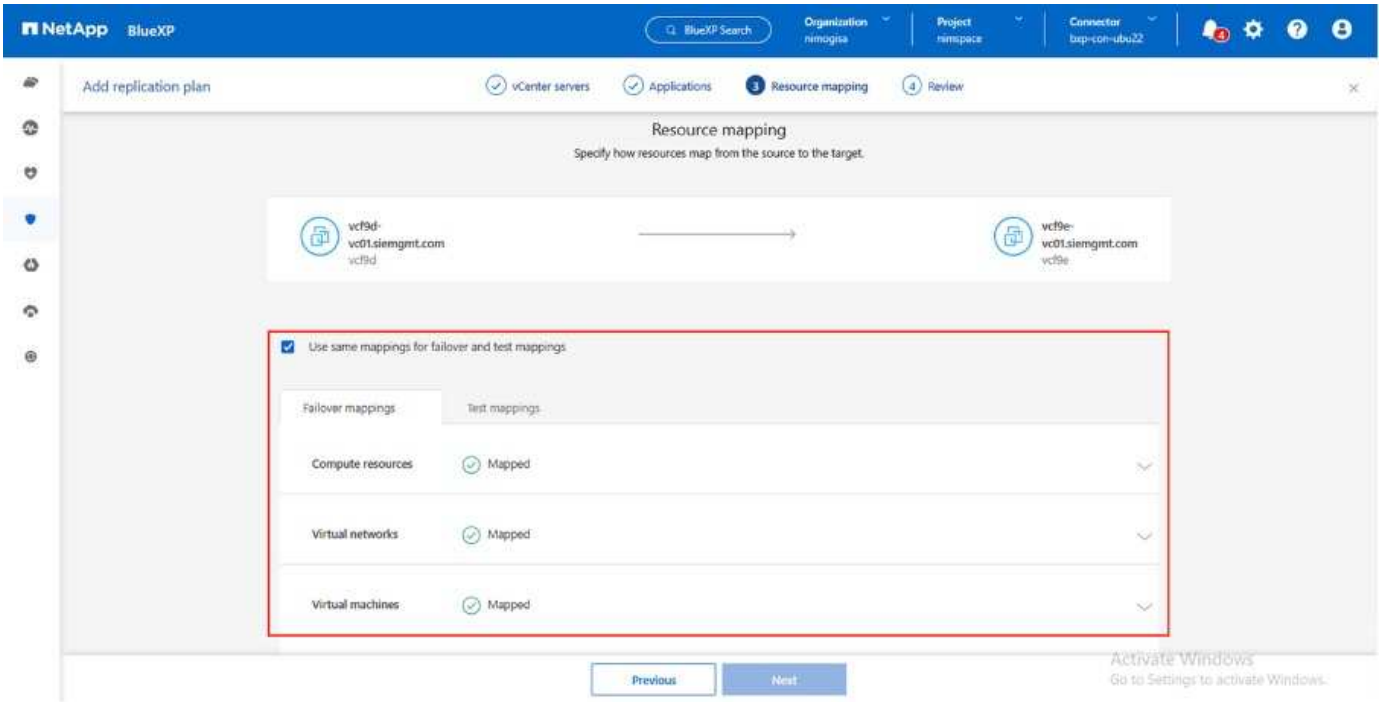
다음 단계는 기존 리소스 그룹을 선택하는 것입니다. 리소스 그룹이 생성되지 않은 경우 마법사는 복구 목표에 따라 필요한 가상 머신을 그룹화(기본적으로 기능적 리소스 그룹 생성)하는 데 도움을 줍니다. 이는 또한 애플리케이션 가상 머신을 복원하는 방법에 대한 작업 순서를 정의하는 데 도움이 됩니다.



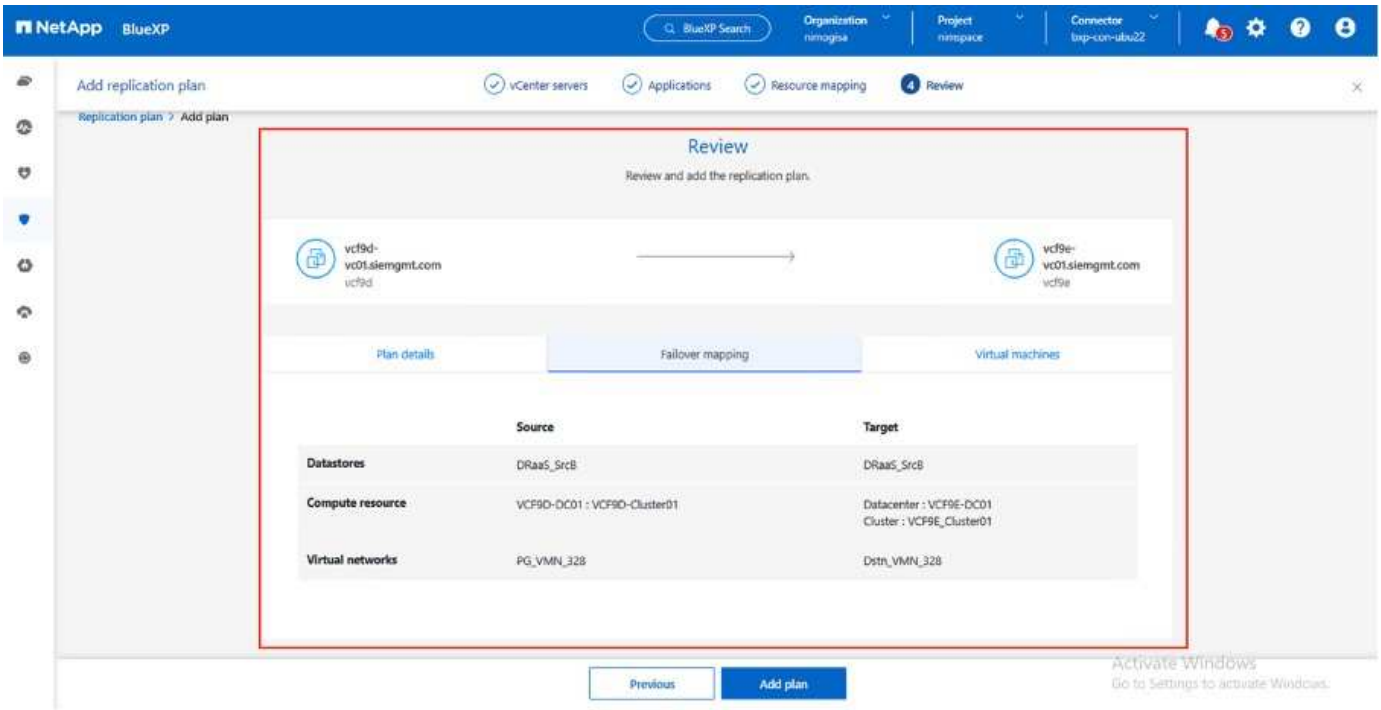
리소스 그룹을 사용하면 드래그 앤 드롭 기능을 사용하여 부팅 순서를 설정할 수 있습니다. 이를 사용하면 복구 프로세스 중에 VM의 전원이 켜지는 순서를 쉽게 수정할 수 있습니다.

복제 계획을 통해 리소스 그룹이 생성되면 다음 단계는 재해 발생 시 가상 머신과 애플리케이션을 복구하기 위한 청사진이나 매핑을 선택하는 것입니다. 이 단계에서는 소스 환경의 리소스가 대상 환경에 어떻게 매핑되는지 지정합니다. 여기에는 컴퓨팅 리소스, 가상 네트워크, IP 사용자 정의, 사전 및 사후 스크립트, 부팅 지연, 애플리케이션 일관성 등이 포함됩니다. 자세한 내용은 다음을 참조하세요."복제 계획 만들기" . 필수 구성 요소에서 언급했듯이 SnapMirror 복제는 사전에 구성할 수 있으며, DRaaS는 복제 계획을 만드는 동안 지정된 RPO 및 보존 횟수를 사용하여 구성할 수 있습니다.

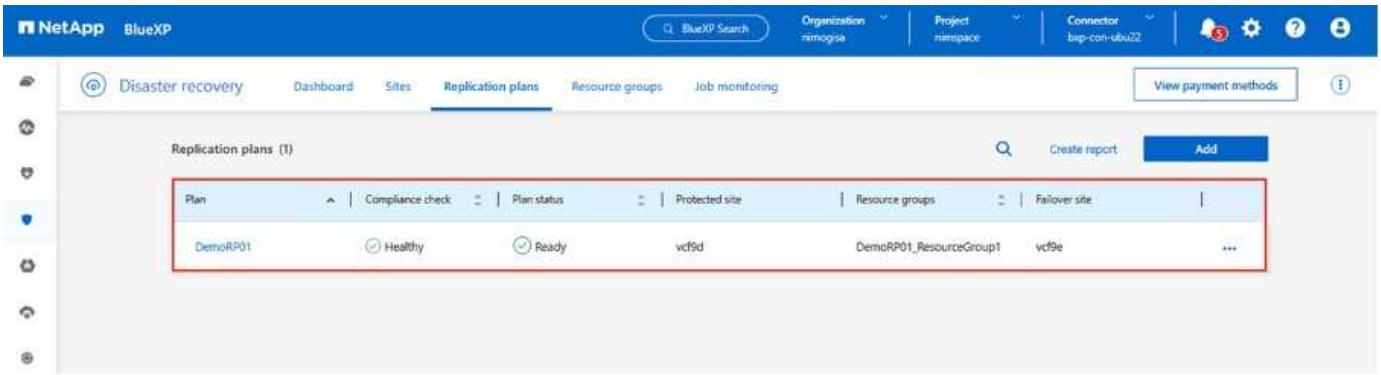
참고: 기본적으로 테스트 작업과 장애 조치 작업 모두에 동일한 매핑 매개변수가 사용됩니다. 테스트 환경에 대해 다른 매핑을 설정하려면 "장애 조치 및 테스트 매핑에 동일한 매핑 사용" 체크 상자의 선택을 취소한 후 테스트 매핑 옵션을 선택합니다. 리소스 매핑이 완료되면 다음을 클릭합니다.



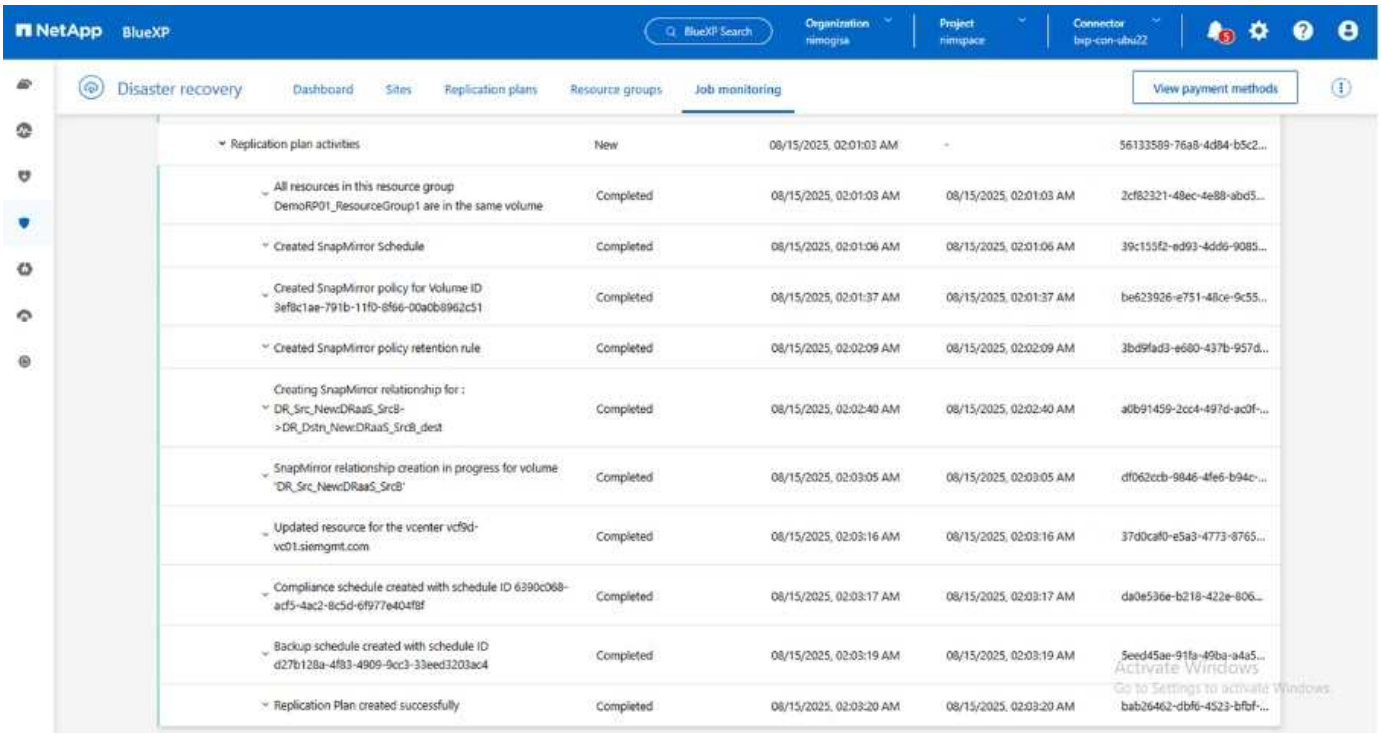
완료되면 생성된 매핑을 검토한 후 계획 추가를 클릭합니다.



다양한 볼륨과 SVM의 VM을 복제 계획에 포함할 수 있습니다. VM 배치(동일한 볼륨에 있는지, 동일한 SVM 내의 별도 볼륨인지, 서로 다른 SVM의 별도 볼륨인지)에 따라 BlueXP disaster recovery 일관성 그룹 스냅샷을 생성합니다.

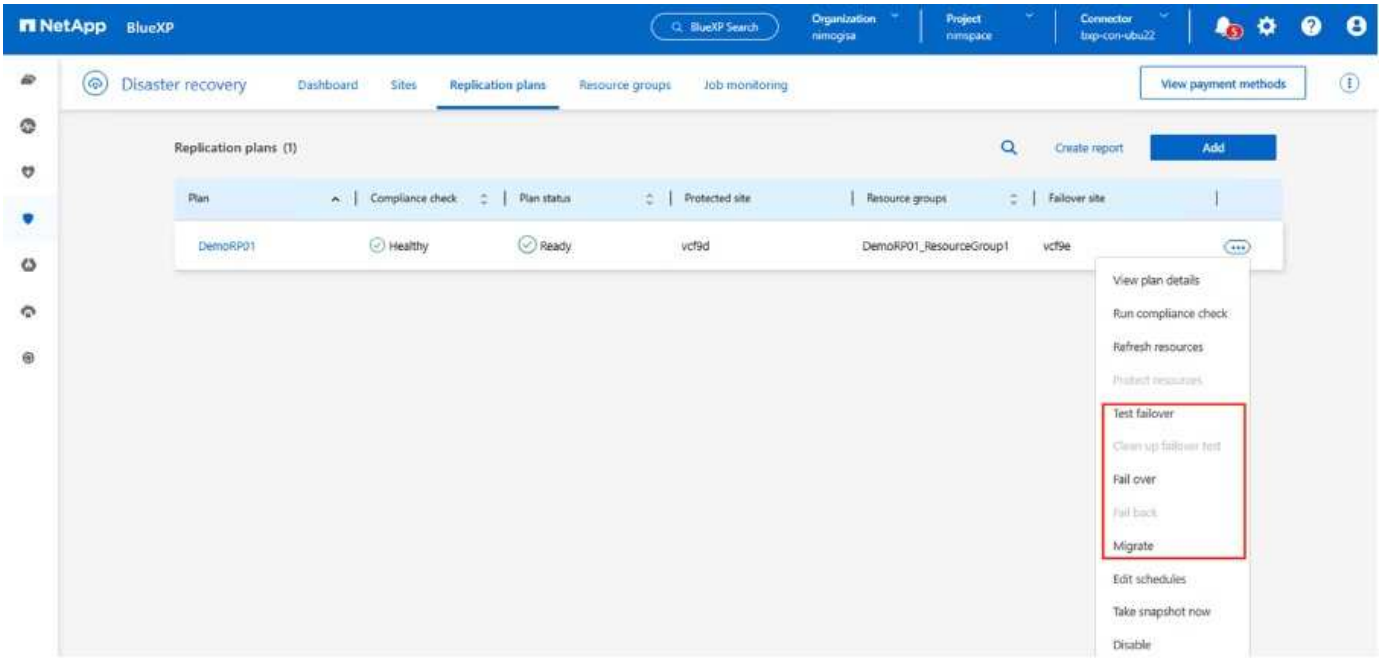


계획이 생성되자마자 일련의 검증이 실행되고 SnapMirror 복제 및 일정이 선택 사항에 따라 구성됩니다.



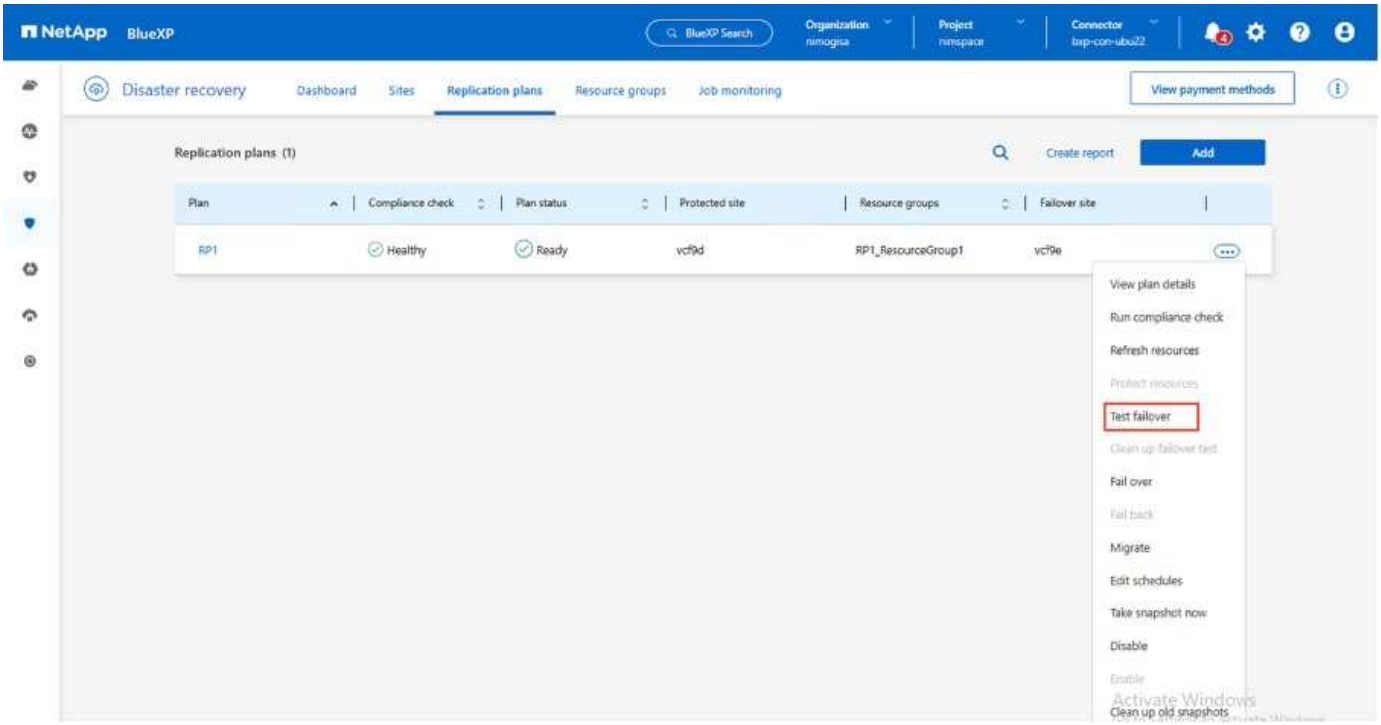
BlueXP DRaaS는 다음 워크플로로 구성됩니다.

- 테스트 장애 조치(주기적 자동 시뮬레이션 포함)
- 클린업 페일오버 테스트
- 장애 조치:
  - 계획된 마이그레이션(일회성 장애 조치를 위한 사용 사례 확장)
  - 재해 복구
- 장애 복구

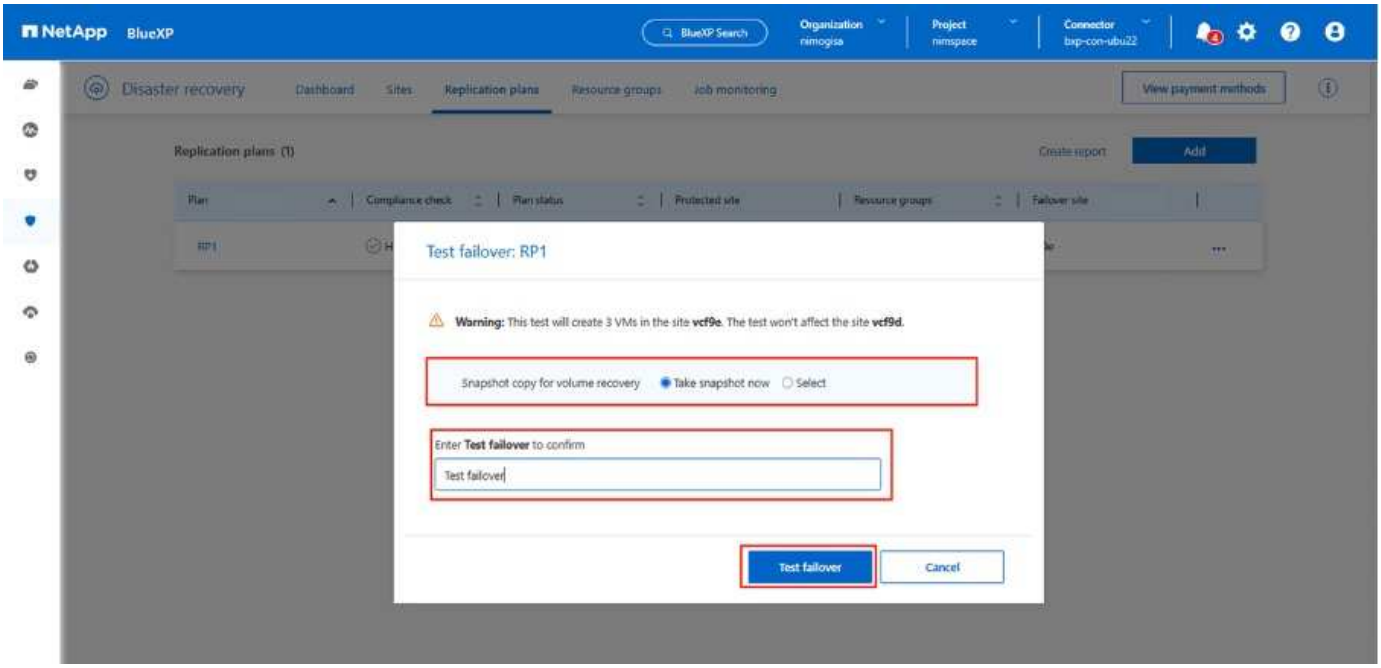


테스트 장애 조치

BlueXP DRaaS의 테스트 페일오버는 VMware 관리자가 프로덕션 환경을 방해하지 않고 복구 계획을 완전히 검증할 수 있도록 하는 운영 절차입니다.

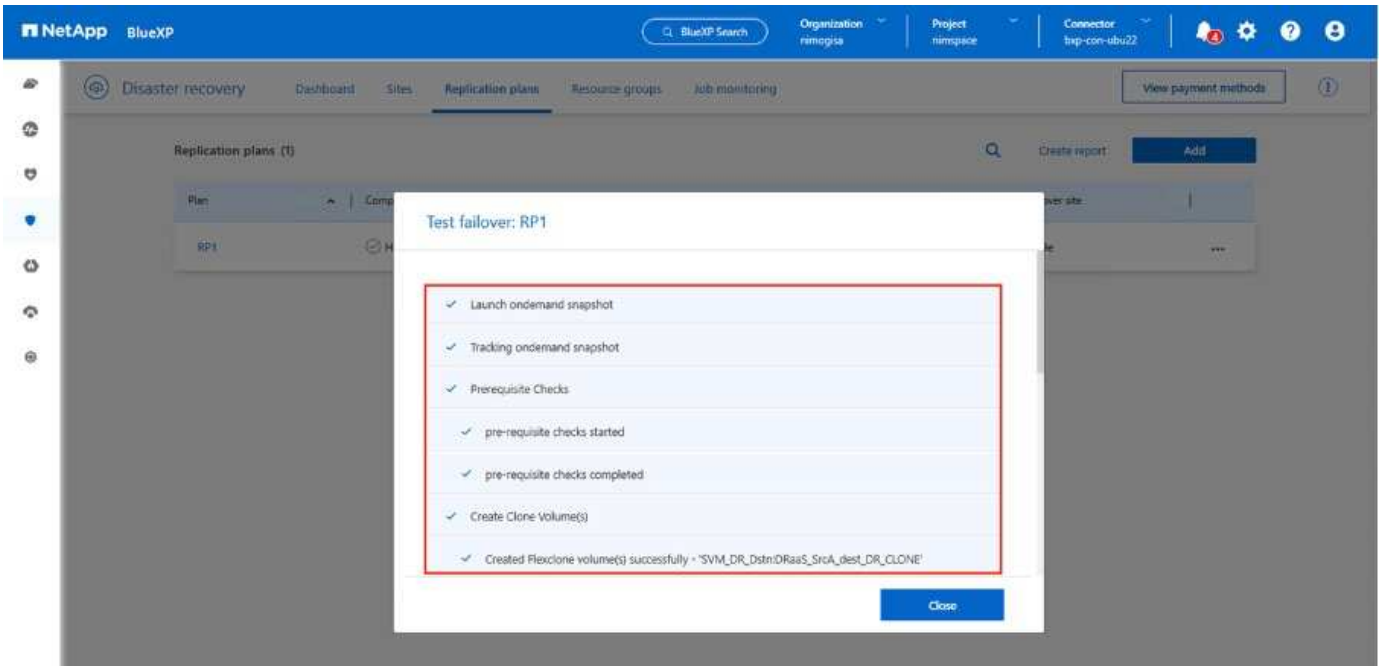


BlueXP DRaaS는 테스트 장애 조치 작업에서 스냅샷을 선택적 기능으로 선택하는 기능을 통합합니다. 이 기능을 사용하면 VMware 관리자는 최근 환경에서 변경된 사항이 대상 사이트에 복제되어 테스트 중에도 그대로 유지되는지 확인할 수 있습니다. 이러한 변경 사항에는 VM 게스트 운영 체제에 대한 패치가 포함됩니다.



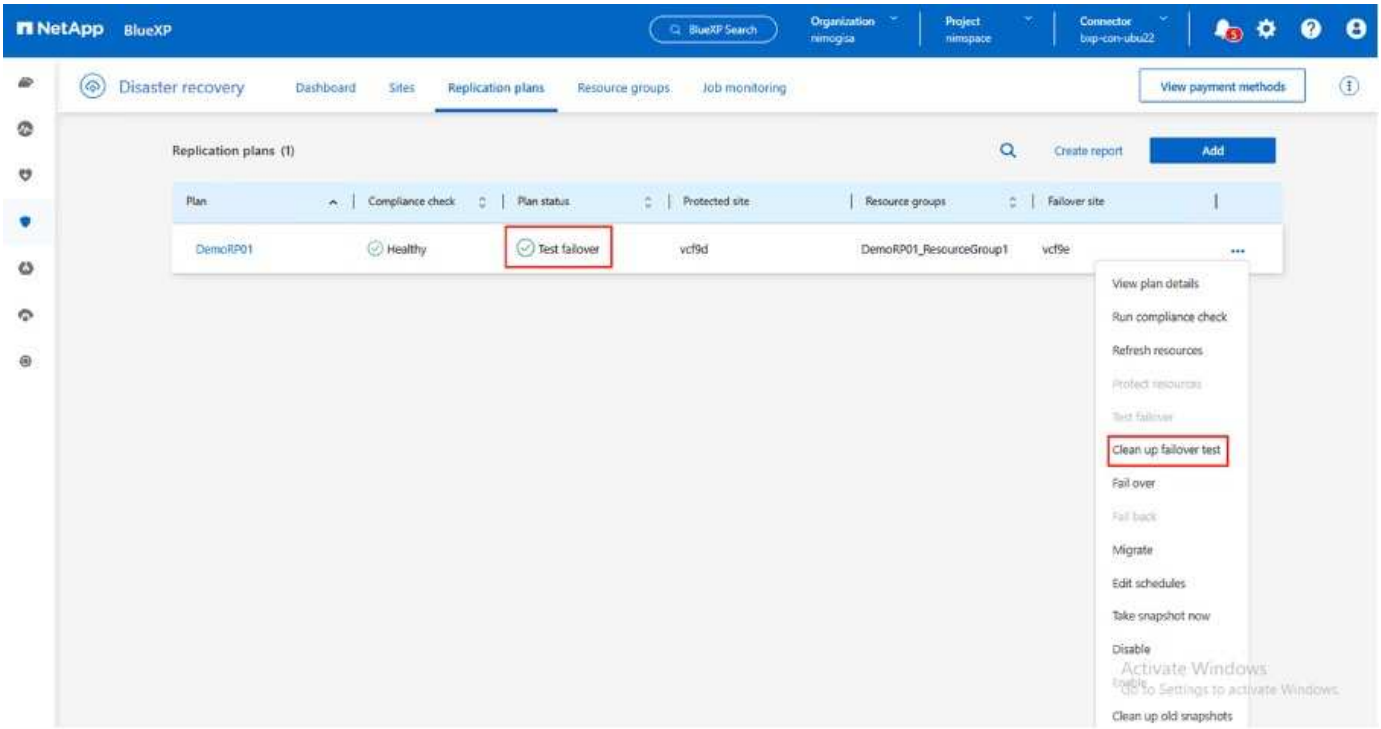
VMware 관리자가 테스트 장애 조치 작업을 실행하면 BlueXP DRaaS는 다음 작업을 자동화합니다.

- 최근 프로덕션 사이트에서 변경된 내용을 대상 사이트의 스토리지에 업데이트하기 위해 SnapMirror 관계를 트리거합니다.
- DR 스토리지 어레이에서 FlexVol 볼륨의 NetApp FlexClone 볼륨을 생성합니다.
- FlexClone 볼륨의 데이터스토어를 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.

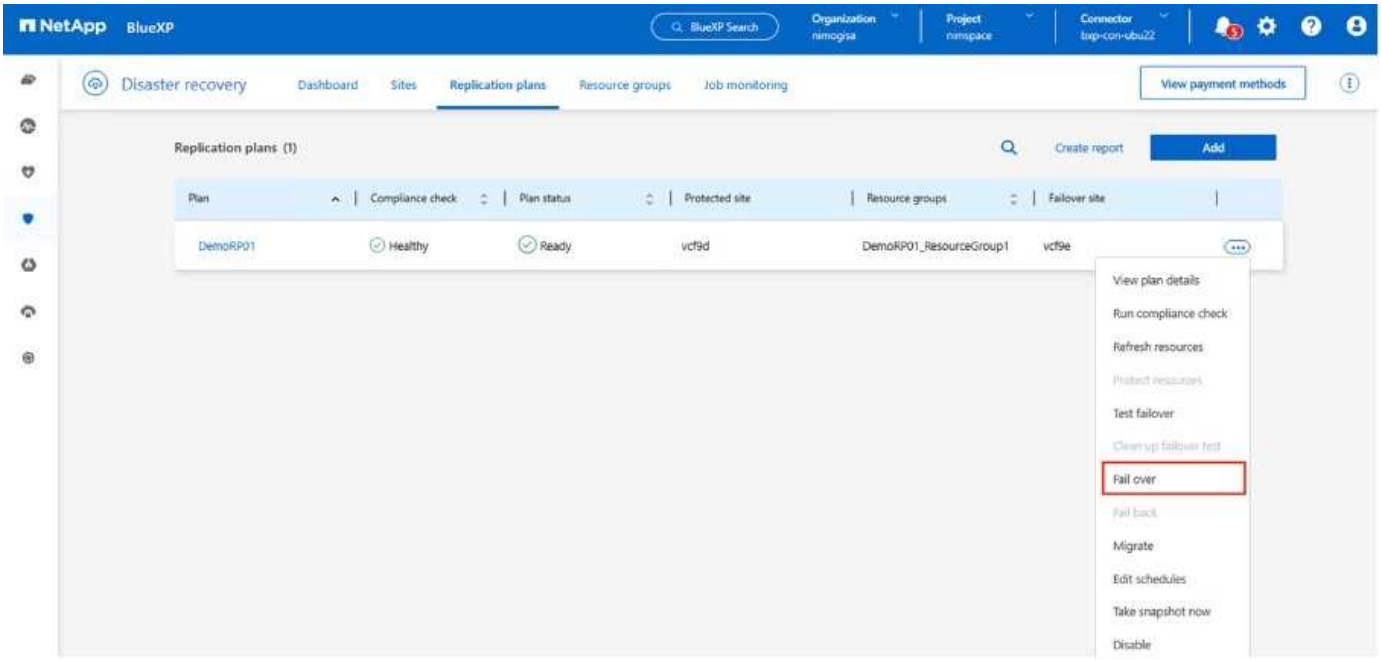


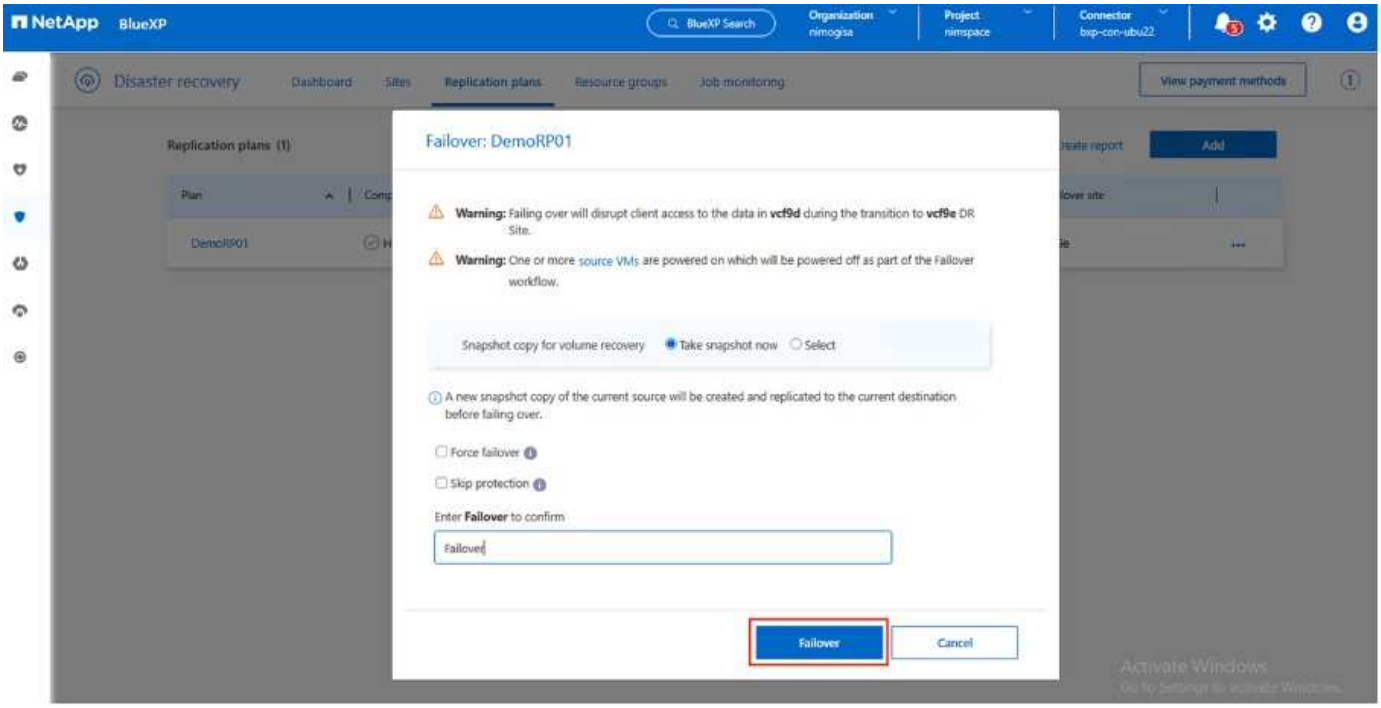
이 작업을 수행하면 가상 머신(VM)과 복제 계획 상태가 준비 상태로 재설정됩니다. VMware 관리자가 복구 작업을 수행하면 BlueXP DRaaS는 다음 프로세스를 완료합니다.

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

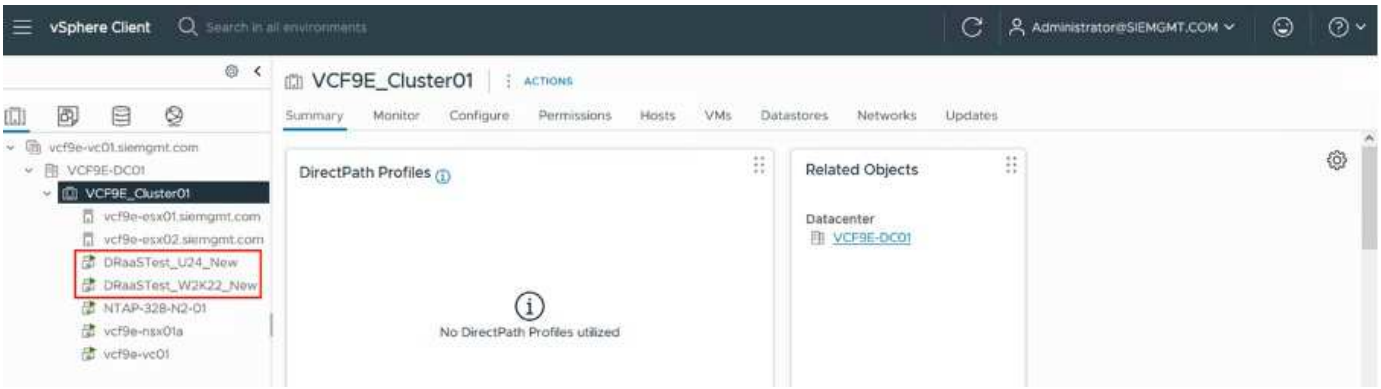
BlueXP DRaaS는 실제 장애 조치를 수행하는 데 계획된 마이그레이션과 장애 조치라는 두 가지 방법을 제공합니다. 첫 번째 방법인 계획된 마이그레이션은 VM 종료 및 스토리지 복제 동기화를 프로세스에 통합하여 VM을 대상 사이트로 복구하거나 효과적으로 이동합니다. 계획된 마이그레이션에는 소스 사이트에 대한 액세스가 필요합니다. 두 번째 방법인 장애 조치(failover)는 계획된/계획되지 않은 장애 조치로, VM이 마지막 저장소 복제 간격에서 완료될 수 있었던 대상 사이트에서 복구됩니다. 솔루션에 설계된 RPO에 따라 DR 시나리오에서 어느 정도의 데이터 손실이 예상될 수 있습니다.





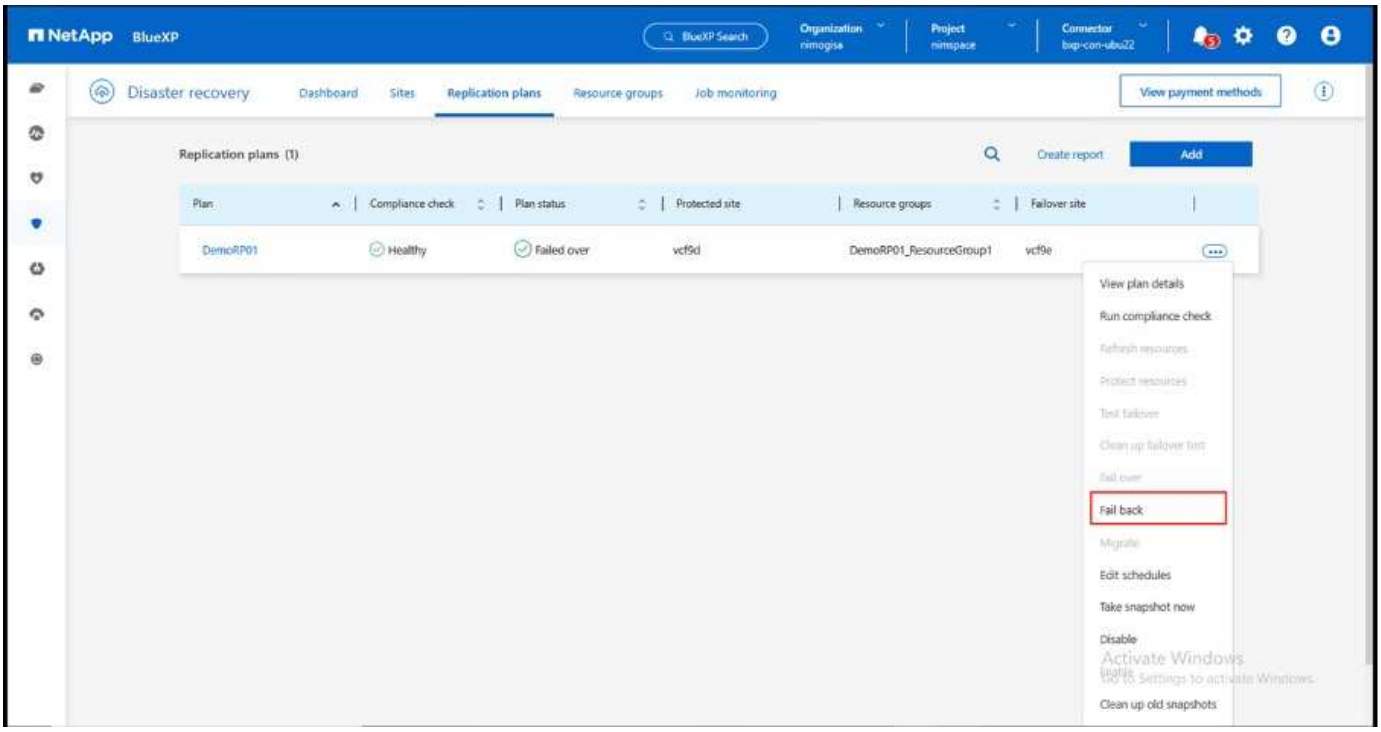
VMware 관리자가 장애 조치 작업을 수행하면 BlueXP DRaaS는 다음 작업을 자동화합니다.

- NetApp SnapMirror 관계를 끊고 장애 조치합니다.
- 복제된 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.

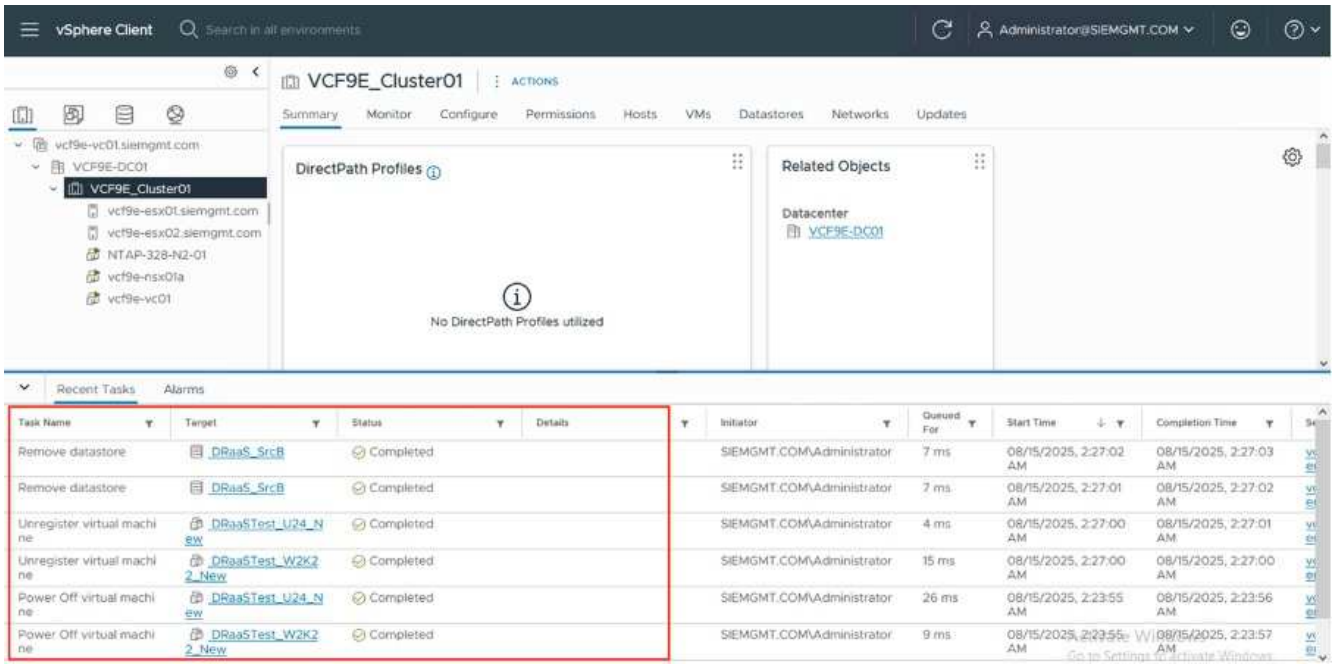


VMware 관리자는 서비스를 원래 소스 사이트로 복원할 준비가 되면 장애 복구 절차를 구성하고 실행할 수 있습니다.

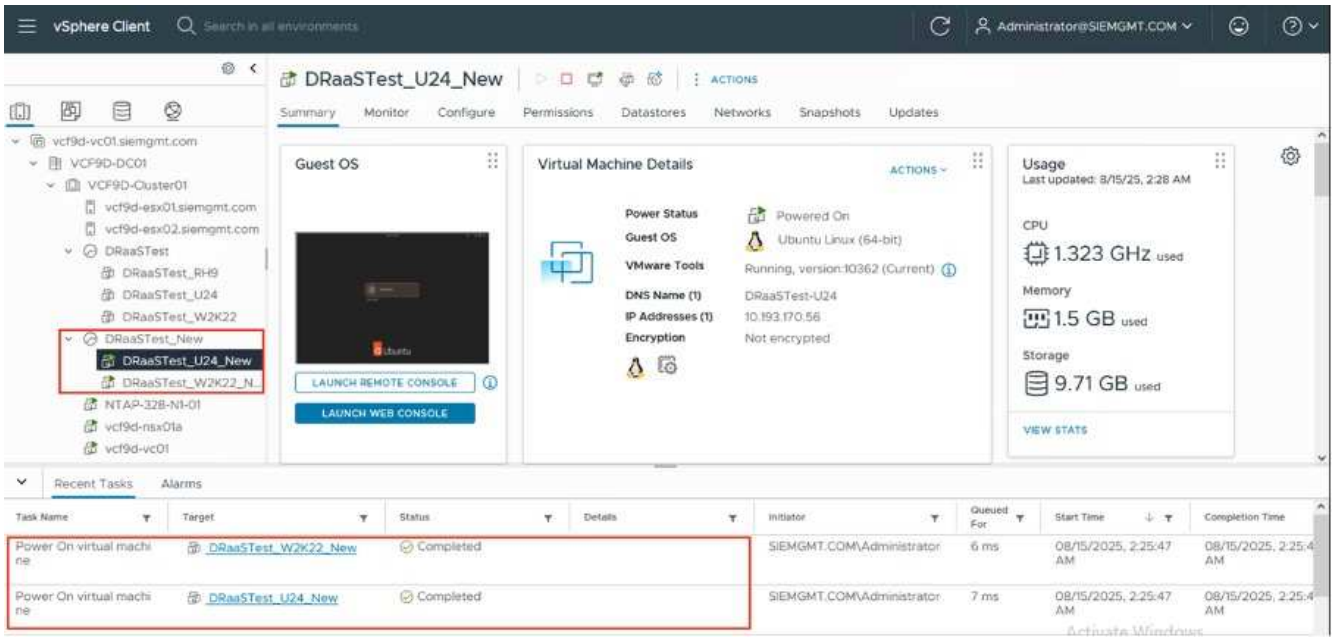
> BlueXP DRaaS는 복제 방향을 바꾸기 전에 모든 변경 사항을 원본 소스 가상 머신으로 복제(재동기화)합니다.

이 프로세스는 대상으로의 장애 조치를 완료한 관계에서 시작되며 다음 단계를 포함합니다.

- 대상 사이트의 가상 머신과 볼륨의 전원을 끄고 등록을 취소합니다.



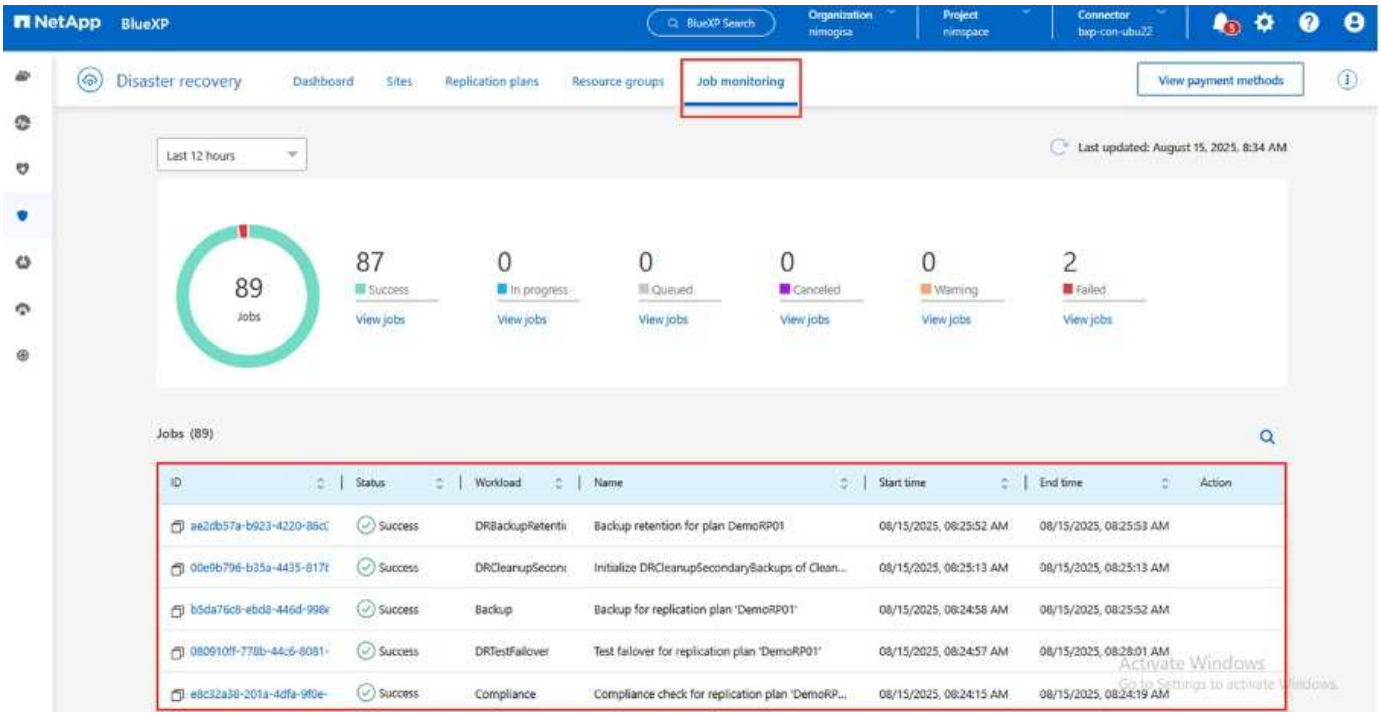
- 원본 소스의 SnapMirror 관계를 끊어서 읽기/쓰기가 가능하도록 합니다.
- 복제를 되돌리려면 SnapMirror 관계를 다시 동기화합니다.
- 소스에 볼륨을 마운트하고, 소스 가상 머신의 전원을 켜서 등록합니다.



BlueXP DRaaS에 액세스하고 구성하는 방법에 대한 자세한 내용은 다음을 참조하세요."VMware용 BlueXP 재해 복구에 대해 알아보세요" .

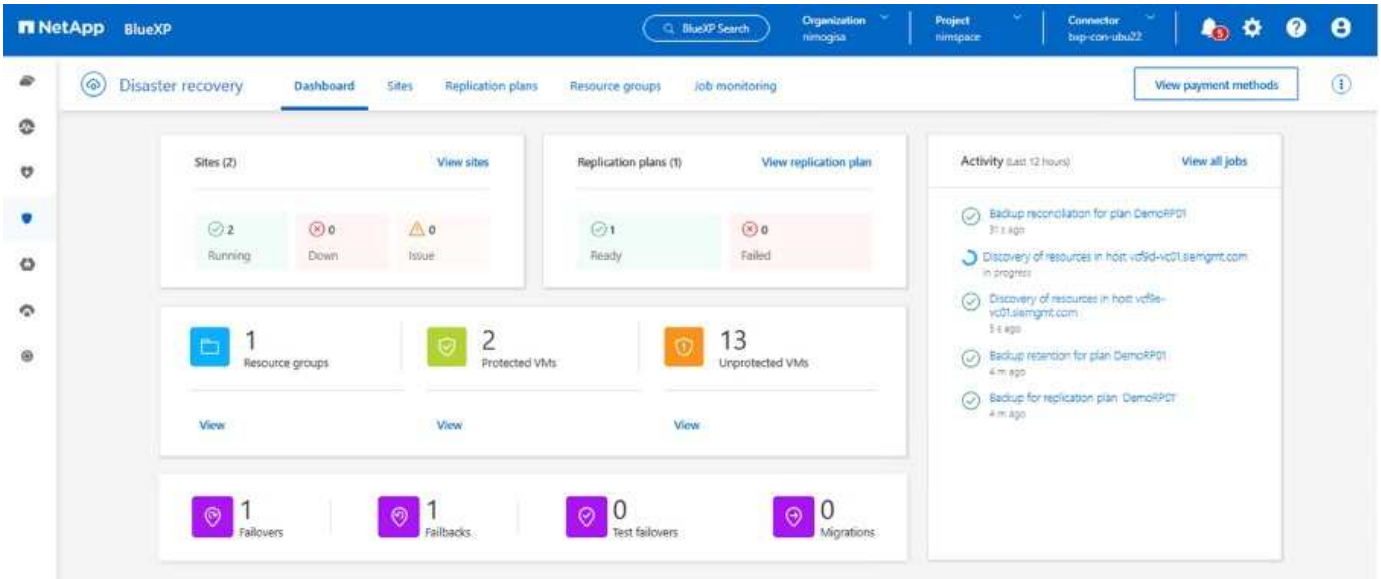
모니터링 및 대시보드

BlueXP 또는 ONTAP CLI에서 해당 데이터 저장소 볼륨에 대한 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.

BlueXP disaster recovery 보드를 사용하면 재해 복구 사이트와 복제 계획의 상태를 확실하게 평가할 수 있습니다. 이를 통해 관리자는 정상, 연결이 끊긴 또는 성능이 저하된 사이트와 계획을 신속하게 식별할 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.

기존 **vSphere** 클러스터를 **VCF**로 변환

기존 데이터 저장소가 있는 **vSphere** 환경을 **VCF**로 변환하는 방법에 대해 알아보세요**.**

ONTAP 에서 실행되는 기존 데이터 저장소가 있는 vSphere 환경을 VMware Cloud

Foundation(VCF) 환경으로 변환하려면 현재 인프라를 최신 프라이빗 클라우드 아키텍처에 통합해야 합니다.

이 프로세스는 ONTAP 스토리지의 유연성을 활용하여 원활한 데이터 액세스와 관리를 제공합니다. VCF 관리 도메인이 설정되면 관리자는 효율적으로 추가 vSphere 환경을 VCF 생태계로 가져올 수 있습니다. 이러한 통합은 리소스 활용도를 높이고, 프라이빗 클라우드 관리를 간소화하며, 기존 작업 부하를 최소화하면서 원활한 전환을 보장합니다.

vCenter 인스턴스를 변환하는 데 대한 기술적 세부 사항은 다음 솔루션을 참조하세요.

- "기존 vCenter 인스턴스를 VCF 관리 도메인(NFS)으로 변환"
- "vCenter 인스턴스(FC 데이터스토어)를 VCF 관리 도메인으로 변환"

vCenter 서버 인스턴스를 **VCF** 관리 도메인**(NFS** 데이터 저장소**)**으로 변환

NetApp ONTAP NFS 데이터 저장소가 있는 기존 vSphere 8 클러스터를 VMware Cloud Foundation(VCF) 관리 도메인으로 변환합니다. 이 절차에는 NFS 스토리지 프로비저닝, VMware용 ONTAP 도구 배포, VCF 가져오기 도구를 사용하여 VCF 내에서 효율적인 관리와 최적화된 리소스 활용을 위해 클러스터를 변환하는 작업이 포함됩니다.

소개

ONTAP 에서 실행되는 기존 NFS 데이터 저장소가 있는 클러스터를 변환하려면 기존 인프라를 최신 프라이빗 클라우드 아키텍처로 통합해야 합니다. 이 프로세스는 NFS 스토리지의 유연성을 활용하여 원활한 데이터 액세스와 관리를 보장합니다. 변환 프로세스를 통해 VCF 관리 도메인이 설정되면 관리자는 NFS 데이터 저장소를 사용하는 클러스터를 포함하여 추가 vSphere 클러스터를 VCF 생태계로 효율적으로 가져올 수 있습니다. 이러한 통합은 리소스 활용도를 높일 뿐만 아니라 프라이빗 클라우드 인프라 관리를 간소화하여 기존 작업 부하를 최소화하면서 원활한 전환을 보장합니다.

이 솔루션에서는 클러스터가 VCF 관리 도메인으로 변환될 때 vSphere 8의 NFS 데이터스토어가 주 스토리지가 되는 방식을 보여드리겠습니다.

시나리오 개요

이 시나리오에서는 다음과 같은 상위 수준 단계를 다룹니다.

- ONTAP tools for VMware vSphere 배포합니다.
- ONTAP 도구를 사용하여 NFS 데이터 저장소를 프로비저닝합니다.
- VCF 가져오기 도구를 사용하여 vSphere 클러스터를 검증합니다.
- vSphere 클러스터에 SDDC Manager를 배포합니다.
- VCF 변환 중에 NSX를 생성하기 위해 JSON 파일을 구성합니다.
- VCF 가져오기 도구를 사용하여 vSphere 8 클러스터를 VCF 5.2로 변환합니다.

필수 조건

이 시나리오에는 다음과 같은 구성 요소와 구성이 필요합니다.

- NFS 트래픽을 허용하도록 구성된 스토리지 가상 머신(SVM)이 있는 NetApp AFF 스토리지 시스템입니다.

- NFS 트래픽을 전달하고 SVM과 연관되는 논리적 인터페이스(LIF)가 IP 네트워크에 생성되었습니다.
- 4개의 ESXi 호스트와 클러스터에 함께 배치된 vCenter 어플라이언스를 갖춘 vSphere 8 클러스터입니다.
- 이 목적으로 설정된 VLAN 또는 네트워크 세그먼트에서 vMotion 및 NFS 스토리지 트래픽을 위해 구성된 분산 포트 그룹입니다.
- VCF 변환에 필요한 소프트웨어를 다운로드하세요.

ONTAP tools for VMware vSphere HA 또는 비 HA 구성으로 설치할 수 있습니다. ONTAP 도구의 전제 조건에 대한 전체 정보는 다음을 참조하세요. "ONTAP tools for VMware vSphere 의 필수 구성 요소" .

vSphere를 VCF 5.2로 변환하거나 가져오기 위해 지원되는 저장소 및 기타 고려 사항은 다음을 참조하세요. "기존 vSphere 환경을 VMware Cloud Foundation으로 변환하거나 가져오기 전 고려 사항" .

필수 소프트웨어는 다음으로 이동하세요. "Broadcom 지원 포털" .

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

배포 단계

이 솔루션은 ONTAP tools for VMware vSphere 사용하여 NFS 데이터 저장소를 프로비저닝하고 기존 vSphere 8 클러스터를 VCF 관리 도메인으로 변환하는 프로세스를 다룹니다.

다음 단계를 완료하세요.

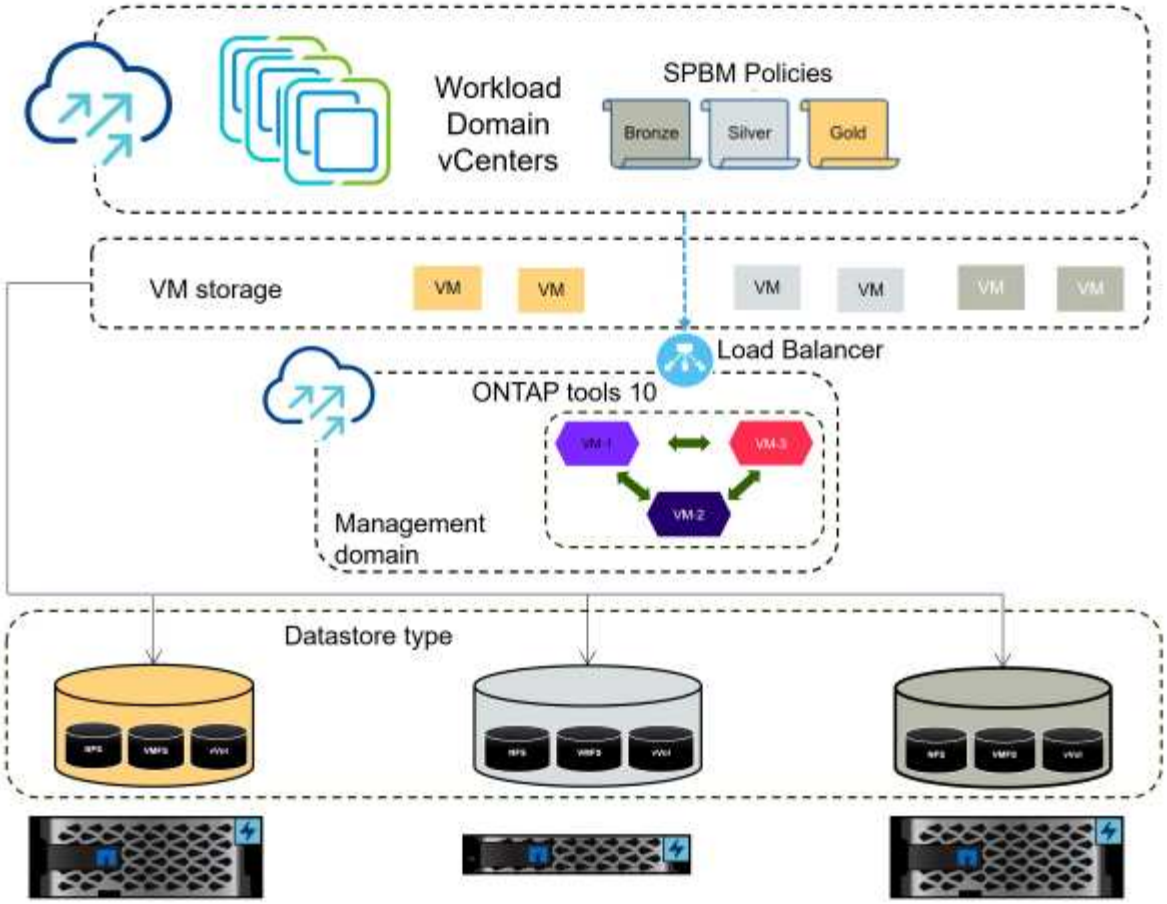
- ONTAP tools for VMware vSphere 배포합니다.
- ONTAP 도구를 사용하여 NFS 데이터 저장소를 프로비저닝합니다.
- VCF 가져오기 도구를 vCenter 어플라이언스에 복사합니다.
- VCF 가져오기 도구를 사용하여 vCenter 어플라이언스에 대한 사전 검사를 실행합니다.
- vCenter 클러스터에 SDDC 관리자 VM을 배포합니다.
- 변환 프로세스 중에 배포할 NSX 클러스터에 대한 JSON 파일을 만듭니다.
- 필요한 소프트웨어를 SDDC 관리자에 업로드합니다.
- vSphere 클러스터를 SDDC 관리자 인벤토리로 변환합니다.

변환 프로세스 개요는 다음을 참조하세요. "VMware Cloud Foundation에서 vSphere 환경을 관리 도메인으로 변환하거나 vSphere 환경을 VI 워크로드 도메인으로 가져오기" .

ONTAP 도구 배포 및 **NFS** 데이터 저장소 프로비저닝

ONTAP 도구 10의 아키텍처는 ONTAP 도구 서비스, vSphere 플러그인, REST API를 포함하는 모듈식 확장 가능 프레임워크를 활용하여 VMware 환경과 원활하게 통합되도록 설계되었으며, 이를 통해 효율적인 스토리지 관리, 자동화 및 데이터 보호가 가능합니다.

ONTAP tools for VMware vSphere HA 또는 비 HA 구성으로 설치할 수 있습니다.

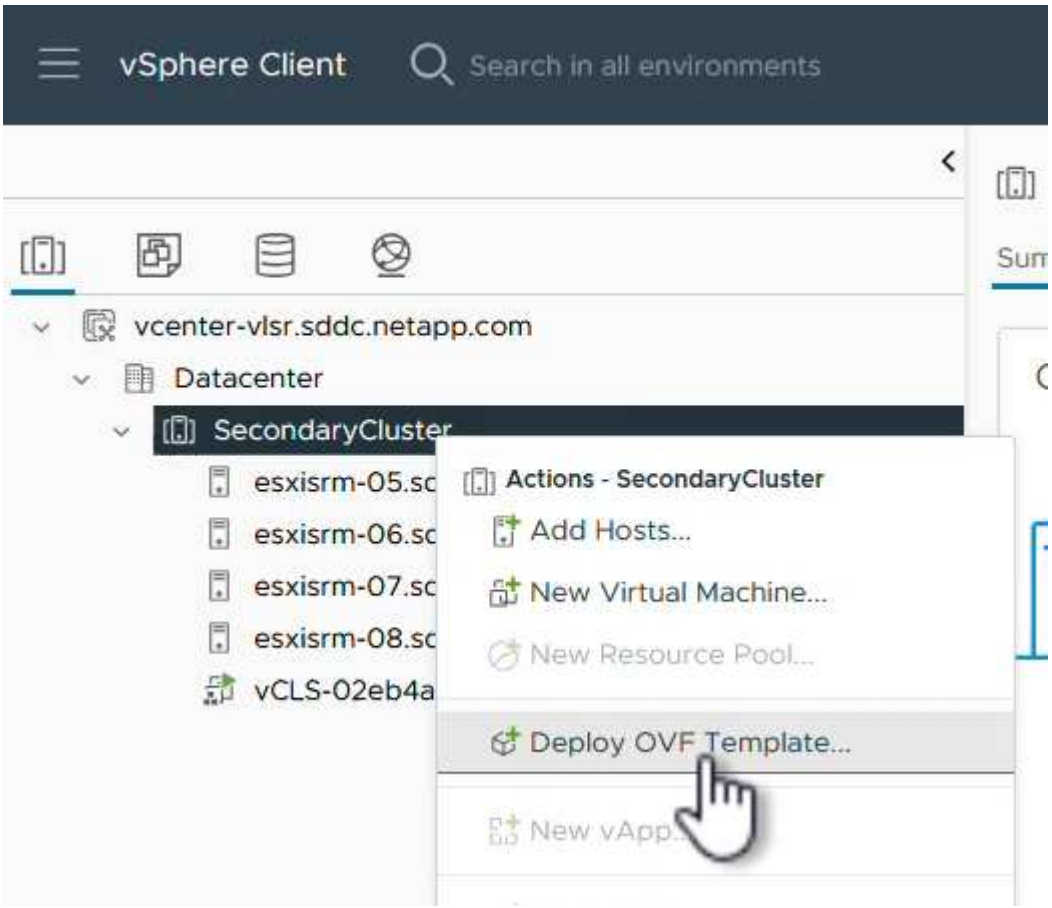

Workload
Domain
vCenters
SPBM Policies
Bronze
Silver
Gold
VM storage
VM
VM
VM
VM
VM
VM
Load Balancer
ONTAP tools 10
VM-1
VM-3
VM-2
Management
domain
Datastore type

ONTAP tools for VMware vSphere 배포

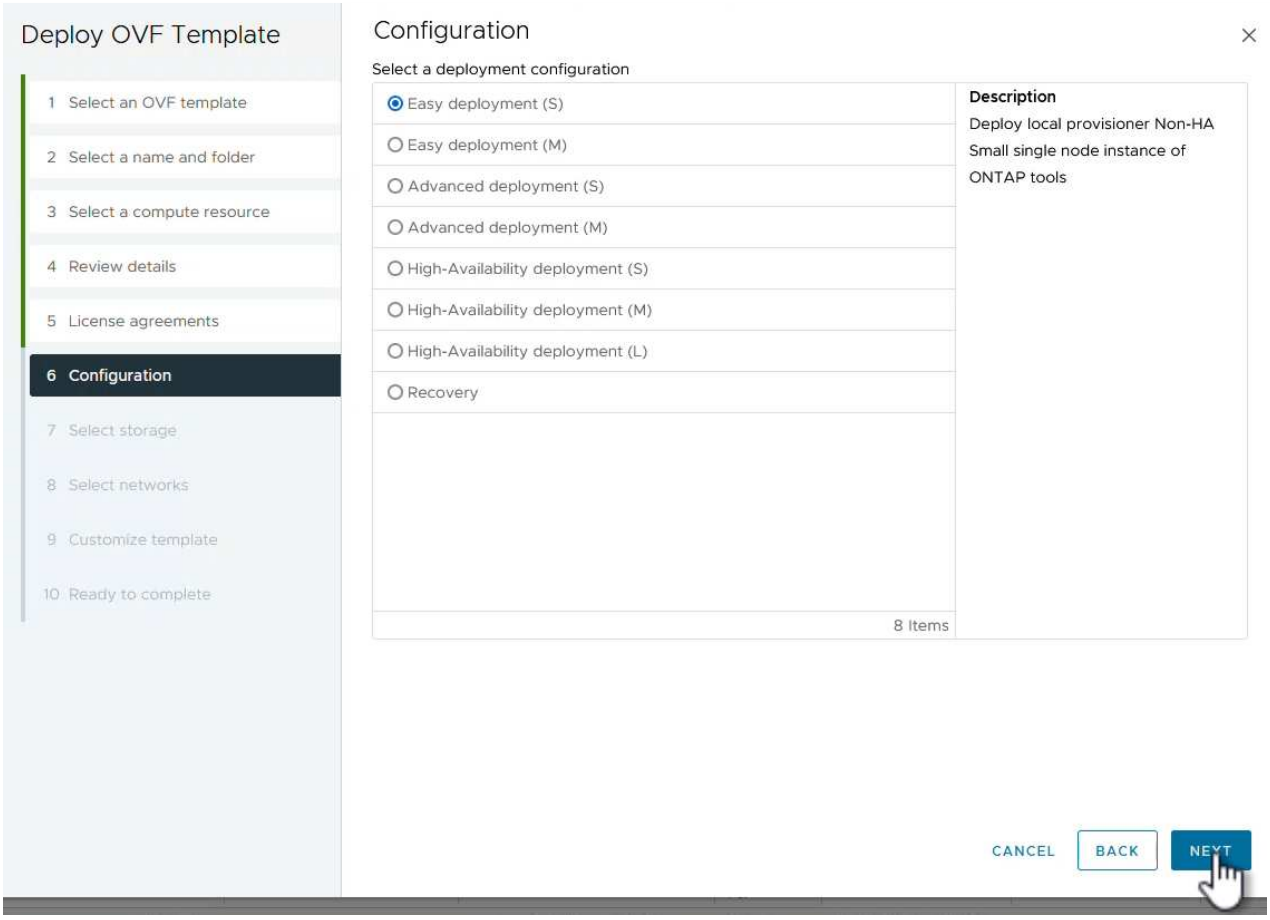
이 단계에서는 ONTAP 도구 10이 비 HA 구성으로 배포됩니다.

HA 및 비 HA 구성에 대한 추가 배포 세부 정보는 다음을 참조하세요. "ONTAP tools for VMware vSphere 배포" .

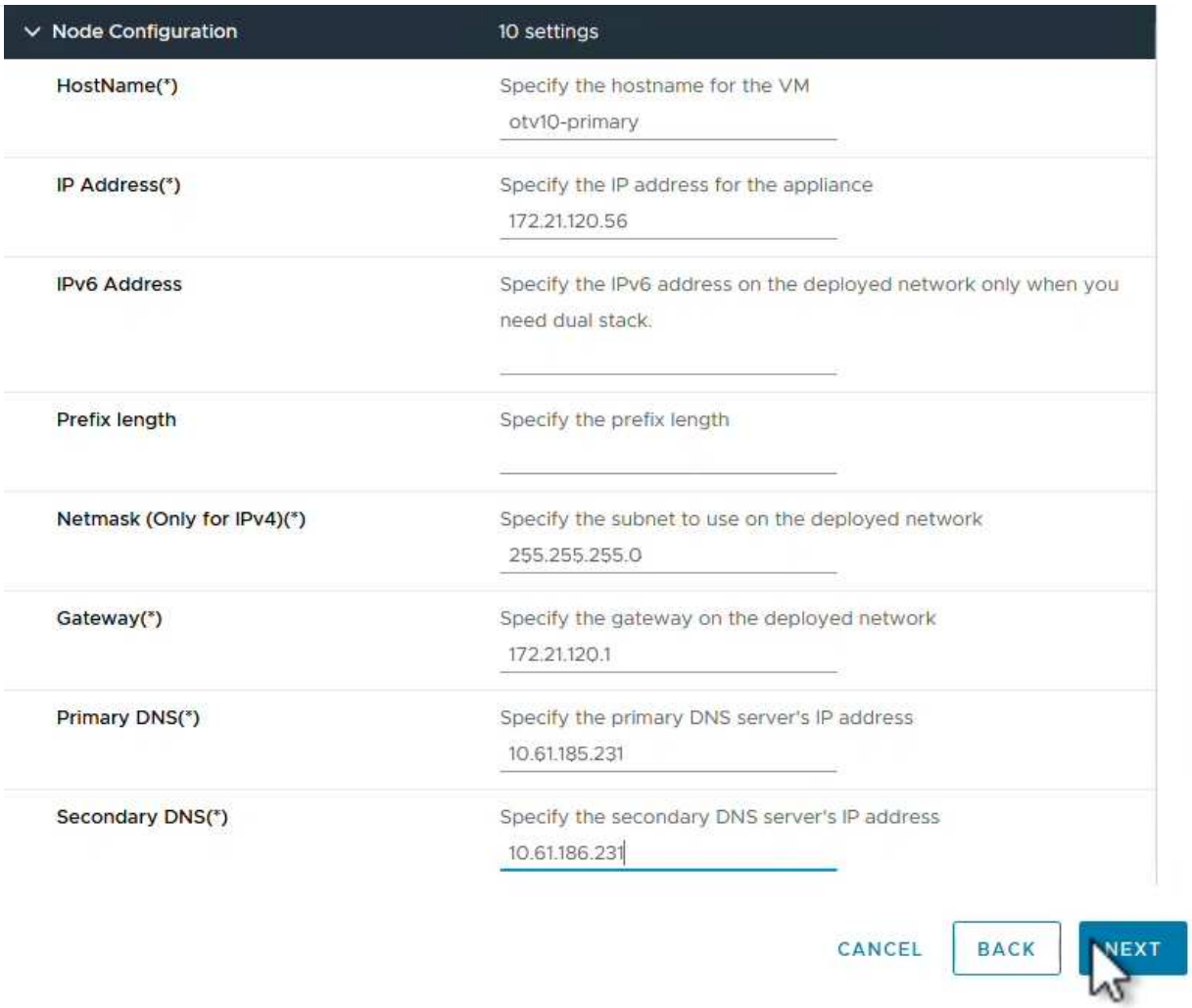
1. ONTAP 도구 10 OVA 템플릿을 다운로드하세요. "NetApp 지원 사이트" .
2. vSphere 클라이언트에서 클러스터를 마우스 오른쪽 버튼으로 클릭하고 *OVF 템플릿 배포*를 클릭합니다.



3. *OVF 템플릿 배포*에서 다음 단계를 완료하세요.
   - OVF 템플릿을 선택하세요.
   - 이름과 폴더를 선택하세요.
   - 컴퓨팅 리소스를 선택하세요.
   - 리뷰 세부 정보.
   - 라이센스 계약에 동의합니다.
4. 템플릿의 구성 페이지에서 HA 구성에 ONTAP 도구를 배포할지 여부를 포함한 배포 유형을 선택합니다. 계속하려면 *다음*을 클릭하세요.



5. 저장소 선택 페이지에서 VM을 설치할 데이터 저장소를 선택하고 *다음*을 클릭합니다.
6. ONTAP 도구 VM이 통신할 네트워크를 선택합니다. 계속하려면 *다음*을 클릭하세요.
7. "템플릿 사용자 지정" 창에서 필요한 모든 정보를 입력합니다.
    - 애플리케이션 사용자 이름 및 비밀번호
    - 프록시 URL을 포함한 ASUP(자동 지원)를 활성화할지 여부를 선택합니다.
    - 관리자 사용자 이름과 비밀번호.
    - NTP 서버.
    - 유지 관리 사용자 이름과 비밀번호(콘솔에서 사용되는 유지 관리 계정).
    - 배포 구성에 필요한 IP 주소를 제공합니다.
    - 노드 구성에 필요한 모든 네트워킹 정보를 제공합니다.

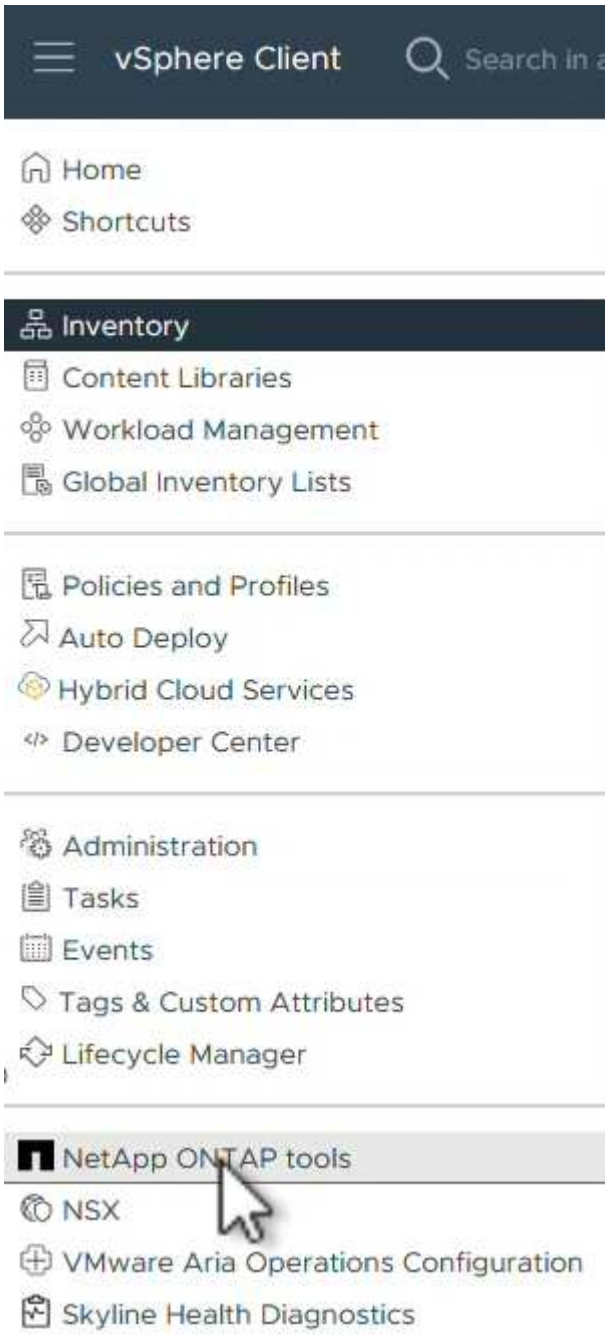


8. 마지막으로, 계속하려면 *다음*을 클릭하고, 배포를 시작하려면 *마침*을 클릭합니다.

ONTAP 도구 구성

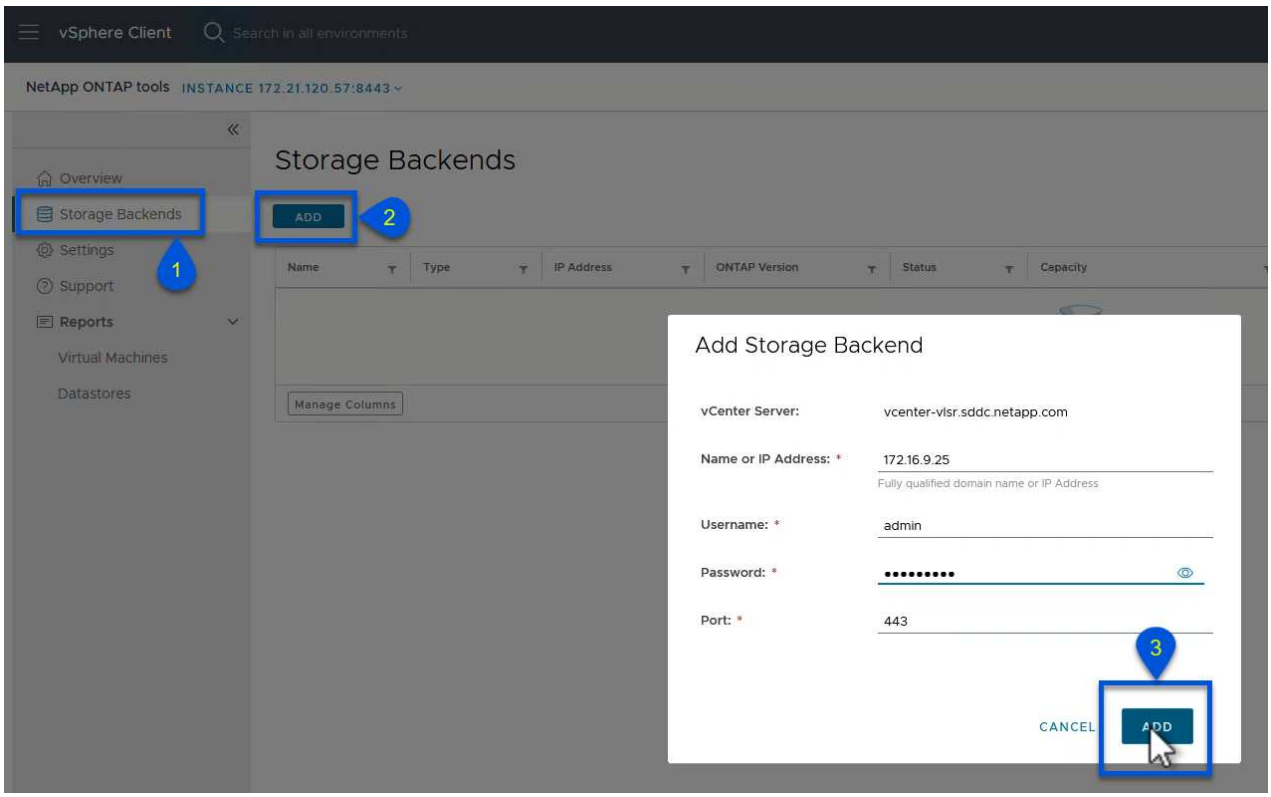
ONTAP 도구 VM이 설치되고 전원이 켜지면 vCenter 서버와 ONTAP 스토리지 시스템을 추가하는 등 몇 가지 기본 구성이 필요합니다. 설명서를 참조하세요 "ONTAP tools for VMware vSphere" 자세한 내용은.

1. 참조하다 "vCenter 인스턴스 추가" ONTAP 도구로 관리되도록 vCenter 인스턴스를 구성합니다.
2. ONTAP 스토리지 시스템을 추가하려면 vSphere 클라이언트에 로그인하고 왼쪽의 주 메뉴로 이동하세요. * NetApp ONTAP 도구*를 클릭하여 사용자 인터페이스를 시작합니다.



3. 왼쪽 메뉴에서 스토리지 백엔드*로 이동한 후 *추가*를 클릭하여 *스토리지 백엔드 추가 창에 액세스합니다.

4. 관리할 ONTAP 스토리지 시스템에 대한 IP 주소와 자격 증명을 입력하세요. *추가*를 클릭하여 완료하세요.

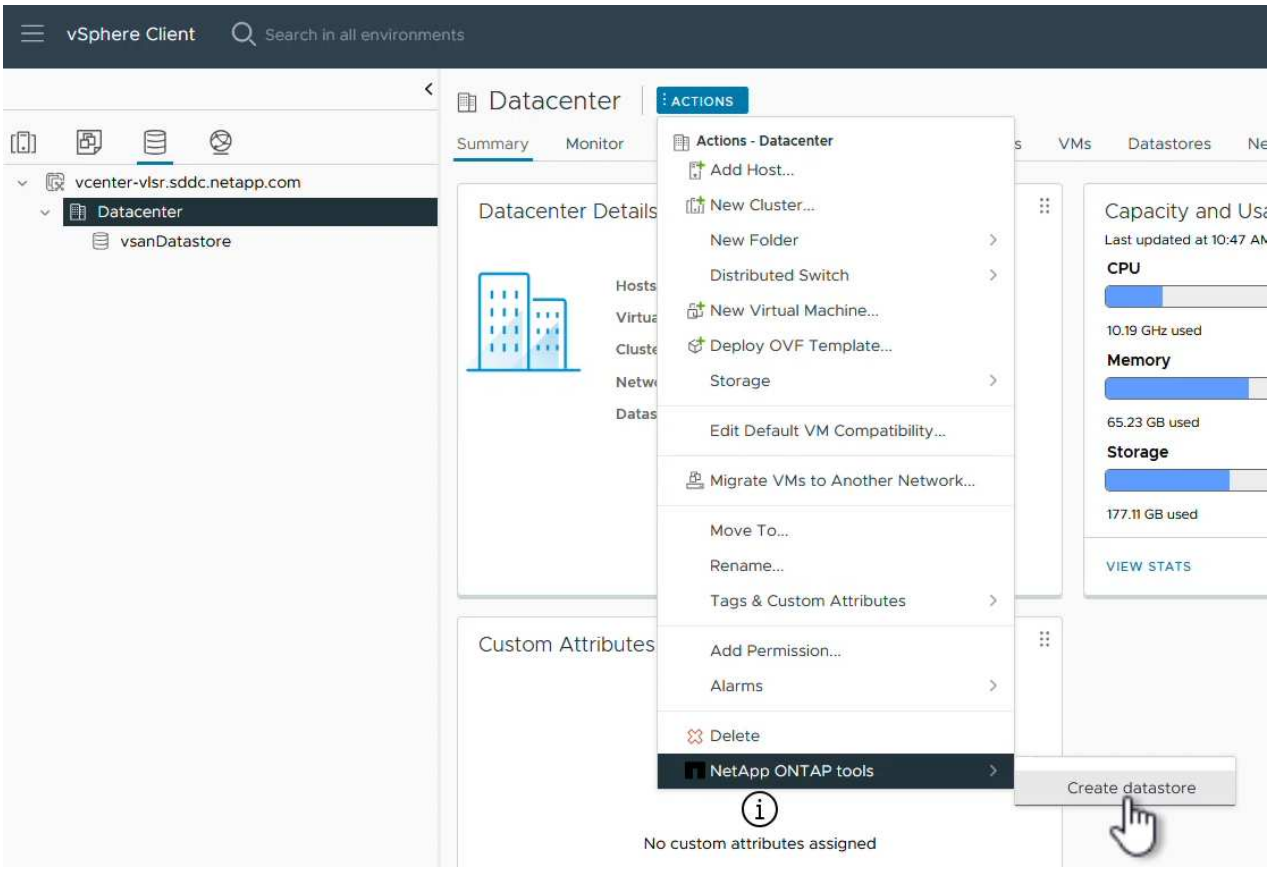


여기에서는 클러스터 IP 주소를 사용하여 vSphere 클라이언트 UI에 스토리지 백엔드가 추가됩니다. 이를 통해 스토리지 시스템의 모든 SVM을 완벽하게 관리할 수 있습니다. 또는 ONTAP 도구 관리자를 사용하여 스토리지 백엔드를 추가하고 vCenter 인스턴스와 연결할 수 있습니다. `https://loadBalanceIP:8443/virtualization/ui/` . 이 방법을 사용하면 vSphere 클라이언트 UI에서 SVM 자격 증명만 추가할 수 있으므로 스토리지 액세스를 보다 세부적으로 제어할 수 있습니다.

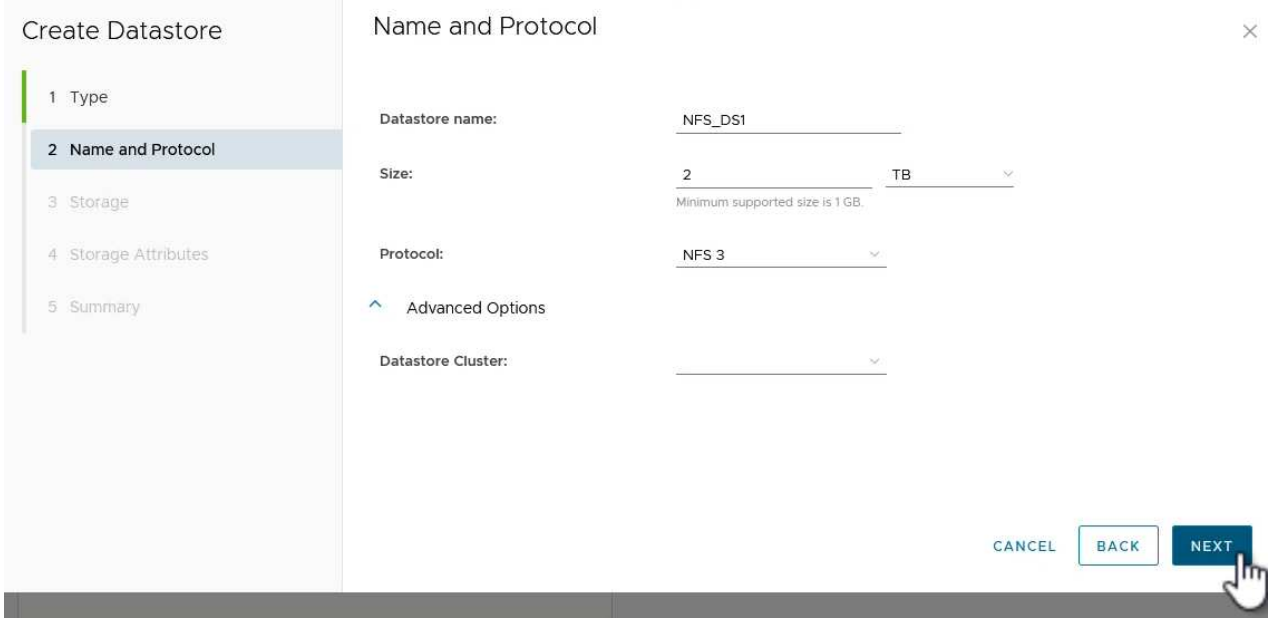
ONTAP 도구를 사용하여 **NFS** 데이터 저장소 프로비저닝

ONTAP 도구는 vSphere 클라이언트 UI 전체의 기능을 통합합니다. 이 단계에서는 스토리지 인벤토리 페이지에서 NFS 데이터 저장소가 프로비저닝됩니다.

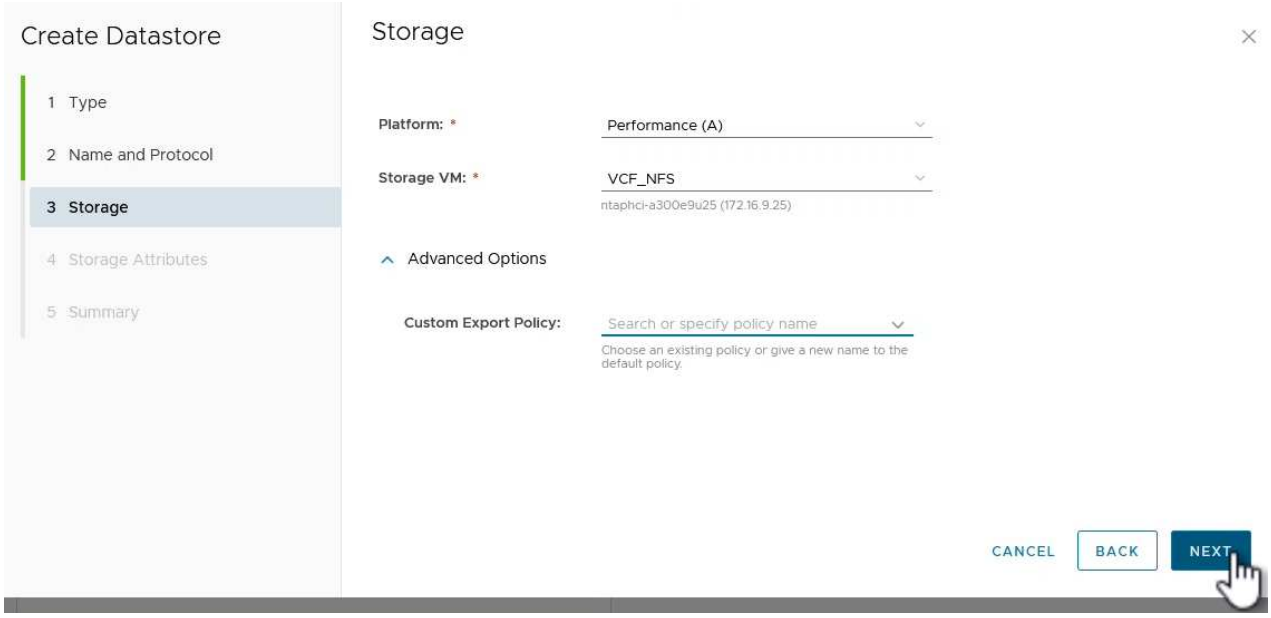
1. vSphere 클라이언트에서 스토리지 인벤토리로 이동합니다.
2. *작업 > NetApp ONTAP 도구 > 데이터 저장소 만들기*로 이동합니다.



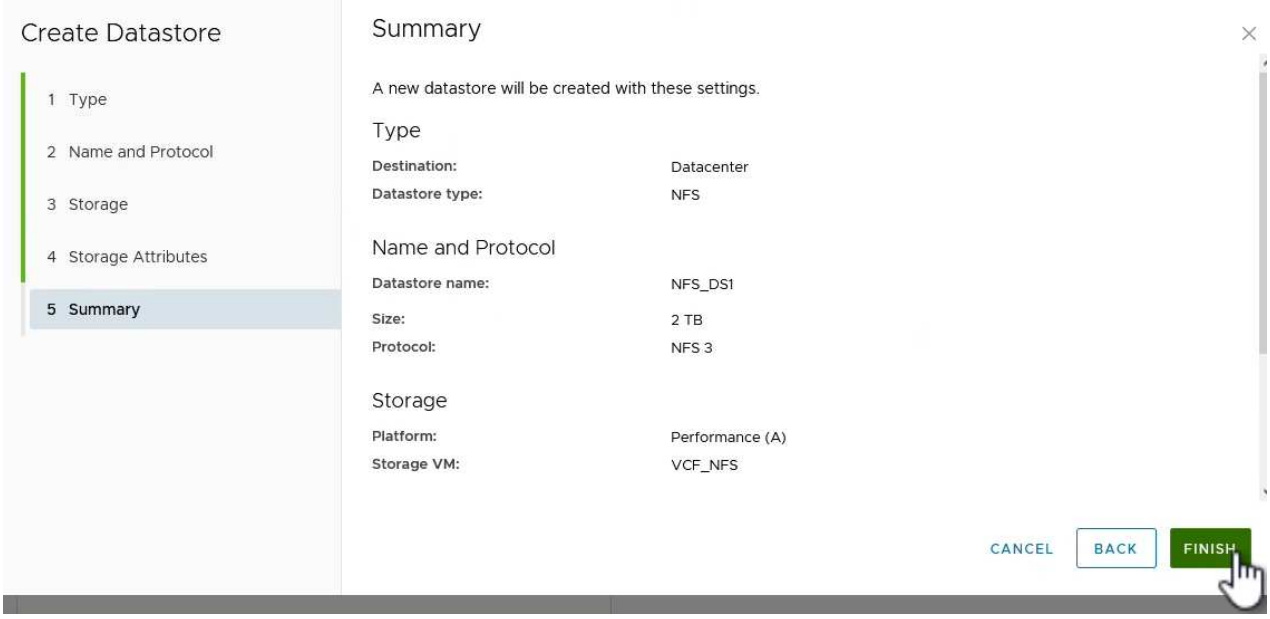
3. 데이터스토어 생성 마법사에서 생성할 데이터스토어 유형을 선택합니다. 옵션은 NFS 또는 VMFS입니다.
4. 이름 및 프로토콜 페이지에서 데이터 저장소의 이름, 크기, 사용할 NFS 프로토콜을 입력합니다.



5. 저장소 페이지에서 ONTAP 스토리지 플랫폼과 스토리지 가상 머신(SVM)을 선택합니다. 여기에서 사용 가능한 사용자 정의 내보내기 정책을 선택할 수도 있습니다. 계속하려면 *다음*을 클릭하세요.



6. 저장소 속성 페이지에서 사용할 저장소 집계를 선택합니다. 계속하려면 *다음*을 클릭하세요.
7. 요약 페이지에서 정보를 검토하고 *마침*을 클릭하여 프로비저닝 프로세스를 시작합니다. ONTAP 도구는 ONTAP 스토리지 시스템에 볼륨을 생성하고 이를 클러스터의 모든 ESXi 호스트에 NFS 데이터 저장소로 마운트합니다.



vSphere 클러스터를 **VCF 5.2**로 변환

다음 섹션에서는 SDDC 관리자를 배포하고 vSphere 8 클러스터를 VCF 5.2 관리 도메인으로 변환하는 단계를 설명합니다. 필요한 경우, 추가 세부 정보는 VMware 문서를 참조하세요.

Broadcom의 VMware에서 제공하는 VCF 가져오기 도구는 vCenter 어플라이언스와 SDDC 관리자 모두에서 구성을 검증하고 vSphere 및 VCF 환경에 대한 변환 및 가져오기 서비스를 제공하는 유틸리티입니다.

자세한 내용은 다음을 참조하세요. "VCF 가져오기 도구 옵션 및 매개변수" .

VCF 가져오기 도구 복사 및 추출

VCF 가져오기 도구는 vCenter 어플라이언스에서 vSphere 클러스터가 VCF 변환 또는 가져오기 프로세스에 적합한지 확인하는 데 사용됩니다.

다음 단계를 완료하세요.

1. 다음 단계를 따르세요 "VCF 가져오기 도구를 대상 vCenter Appliance에 복사합니다." VMware Docs에서 VCF 가져오기 도구를 올바른 위치로 복사하세요.
2. 다음 명령을 사용하여 번들을 추출합니다.

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

vCenter 어플라이언스 검증

변환하기 전에 VCF 가져오기 도구를 사용하여 vCenter 어플라이언스를 검증합니다.

1. 다음 단계를 따르세요 "변환 전 대상 vCenter에서 사전 검사 실행" 검증을 실행하려면.
2. 다음 출력은 vCenter 어플라이언스가 사전 검사를 통과했음을 보여줍니다.

```
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter 172.21.166.57 --sso-user administrator@vsphere.local
[2024-10-23 19:03:23,609] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.0-24307788
Enter vCenter SSO password:
[2024-10-23 19:03:28,825] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2024-10-23 19:03:28,938] [INFO] vc_precheck: Connected to vCenter 172.21.166.57 in 0.11 seconds
[2024-10-23 19:03:28,939] [INFO] vc_precheck: Running pre-checks for vCenter 172.21.166.57...
[2024-10-23 19:03:28,939] [INFO] vc_precheck: [1/10] VC BOM version check...                    PASS
[2024-10-23 19:03:28,975] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...            PASS
[2024-10-23 19:03:28,999] [INFO] vc_precheck: [3/10] Supported storage available check...       PASS
[2024-10-23 19:03:29,020] [INFO] vc_precheck: [4/10] vCenter VM location check...               PASS
[2024-10-23 19:03:29,233] [INFO] vc_precheck: [5/10] VxRail registration check...               PASS
[2024-10-23 19:03:29,414] [INFO] vc_precheck: [6/10] NSX-T registration check...                PASS
[2024-10-23 19:03:29,437] [INFO] vc_precheck: [7/10] Standalone host check...                   PASS
[2024-10-23 19:03:31,870] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...  PASS
[2024-10-23 19:03:32,962] [INFO] vc_precheck: [9/10] ELM ring topology check...                 PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: [10/10] WCP import check...                       PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: All pre-checks passed!
[2024-10-23 19:03:33,383] [INFO] vc_precheck: Pre-checks for vCenter 172.21.166.57 completed in 4.44 seconds
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]#
```

SDDC 관리자 배포

SDDC 관리자는 VCF 관리 도메인으로 변환될 vSphere 클러스터에 함께 배치되어야 합니다.

VMware Docs의 배포 지침에 따라 배포를 완료하세요.

참조하다 "대상 vCenter에 SDDC Manager Appliance 배포" .

자세한 내용은 다음을 참조하세요."위원회 호스트" VCF 관리 가이드에서.

NSX 배포를 위한 JSON 파일 생성

vSphere 환경을 VMware Cloud Foundation으로 가져오거나 변환하는 동안 NSX Manager를 배포하려면 NSX 배포 사양을 만듭니다. NSX 배포에는 최소 3개의 호스트가 필요합니다.

> 변환 또는 가져오기 작업에서 NSX Manager 클러스터를 배포하는 경우 NSX-VLAN 네트워킹이 활용됩니다. NSX-VLAN 네트워킹의 제한 사항에 대한 자세한 내용은 "기존 vSphere 환경을 VMware Cloud Foundation으로 변환하거나 가져오기 전 고려 사항" 섹션을 참조하세요. NSX-VLAN 네트워킹 제한 사항에 대한 정보는 다음을 참조하세요. "기존 vSphere 환경을 VMware Cloud Foundation으로 변환하거나 가져오기 전 고려 사항" .

다음은 NSX 배포를 위한 JSON 파일의 예입니다.

```
{
  "license_key": "xxxxx-xxxxx-xxxxx-xxxxx-xxxxx",
  "form_factor": "medium",
  "admin_password": "NetApp!23456789",
  "install_bundle_path": "/tmp/vcfimport/bundle-133764.zip",
  "cluster_ip": "172.21.166.72",
  "cluster_fqdn": "vcf-m02-nsx01.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "vcf-m02-nsx01a.sddc.netapp.com",
    "name": "vcf-m02-nsx01a",
    "ip_address": "172.21.166.73",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01b.sddc.netapp.com",
    "name": "vcf-m02-nsx01b",
    "ip_address": "172.21.166.74",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01c.sddc.netapp.com",
    "name": "vcf-m02-nsx01c",
    "ip_address": "172.21.166.75",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

JSON 파일을 SDDC 관리자의 디렉토리에 복사합니다.

SDDC 관리자에 소프트웨어 업로드

VCF 가져오기 도구와 NSX 배포 번들을 SDDC 관리자의 /home/vcf/vcfimport 디렉토리에 복사합니다.

보다 "SDDC 관리자 어플라이언스에 필요한 소프트웨어 업로드" 자세한 지침은 여기를 참조하세요.

vSphere 클러스터를 VCF 관리 도메인으로 변환

VCF 가져오기 도구는 변환 과정을 수행하는 데 사용됩니다. VCF 가져오기 도구 기능의 인쇄물을 검토하려면 /home/vcf/vcf-import-package/vcf-brownfield-import-<version>/vcf-brownfield-toolset 디렉토리에서 다음 명령을 실행하세요.

```
python3 vcf_brownfield.py --help
```

다음 명령은 vSphere 클러스터를 VCF 관리 도메인으로 변환하고 NSX 클러스터를 배포하기 위해 실행됩니다.

```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --domain-name '<wld-domain-name>' --nsx-deployment-spec
-path '<nsx-deployment-json-spec-path>'
```

전체 지침은 다음을 참조하세요. "vSphere 환경을 SDDC 관리자 인벤토리로 변환하거나 가져오기" .

VCF에 라이선싱 추가

변환을 완료한 후에는 환경에 라이선스를 추가해야 합니다.

1. SDDC 관리자 UI에 로그인합니다.
2. 탐색 창에서 *관리 > 라이선싱*으로 이동합니다.
3. *+ 라이선스 키*를 클릭하세요.
4. 드롭다운 메뉴에서 제품을 선택하세요.
5. 라이센스 키를 입력하세요.
6. 라이센스에 대한 설명을 제공하세요.
7. *추가*를 클릭하세요.
8. 각 라이선스에 대해 이 단계를 반복합니다.

ONTAP tools for VMware vSphere 에 대한 비디오 데모

ONTAP tools for VMware vSphere 사용한 NFS 데이터 저장소

vCenter 서버 인스턴스를 VCF 관리 도메인(FC 데이터 저장소)으로 변환

ONTAP Fibre Channel 데이터스토어를 사용하여 vSphere 8 클러스터를 VMware Cloud Foundation 관리 도메인으로 변환합니다. 이 절차에는 FC 스토리지 프로비저닝, VMware용 ONTAP 도구 배포, VCF 가져오기 도구를 사용하여 VCF 환경 내에서 클러스터를 마이그레이션하고 관리하는 작업이 포함됩니다.

소개

ONTAP 에서 실행되는 기존 파이버 채널(FC) 데이터 저장소가 있는 vSphere 환경을 변환하려면 기존 인프라를 최신 프라이빗 클라우드 아키텍처로 통합해야 합니다. 이 프로세스는 FC 스토리지의 견고성을 활용하여 원활한 데이터 액세스와 관리를 보장합니다. 변환 프로세스를 통해 VCF 관리 도메인이 설정되면 관리자는 FC 데이터 저장소를 사용하는 환경을 포함하여 추가 vSphere 환경을 VCF 생태계로 효율적으로 가져올 수 있습니다. 이러한 통합은 리소스 활용도를 높일 뿐만 아니라 프라이빗 클라우드 인프라 관리를 간소화하여 기존 작업 부하를 최소화하면서 원활한 전환을 보장합니다.

이 솔루션에서는 클러스터가 VCF 관리 도메인으로 변환될 때 vSphere 8의 FC 데이터스토어가 주 스토리지가 되는 방식을 보여드리겠습니다.

시나리오 개요

이 시나리오에서는 다음과 같은 상위 수준 단계를 다룹니다.

- ONTAP tools for VMware vSphere 배포합니다.
- ONTAP 도구를 사용하여 FC 데이터 저장소를 프로비저닝합니다.
- VCF 가져오기 도구를 사용하여 vSphere 클러스터를 검증합니다.
- vSphere 클러스터에 SDDC Manager를 배포합니다.
- VCF 변환 중에 NSX를 생성하기 위해 JSON 파일을 구성합니다.
- VCF 가져오기 도구를 사용하여 vSphere 8 클러스터를 VCF 5.2.1로 변환합니다.

필수 조건

이 시나리오에는 다음과 같은 구성 요소와 구성이 필요합니다.

- FC(Fibre Channel) 트래픽을 허용하도록 구성된 스토리지 가상 머신(SVM)이 있는 NetApp ASA R2/ ASA/ AFF 스토리지 시스템입니다.
- 논리 인터페이스(LIF)는 FC 트래픽을 전송하기 위해 만들어졌으며 SVM과 연관됩니다.
- FC 트래픽을 전송하도록 지정된 스위치에 FC 구역 설정이 구성되었습니다.
- 4개의 ESXi 호스트와 클러스터에 함께 배치된 vCenter 어플라이언스를 갖춘 vSphere 8 클러스터입니다.
- 이 목적으로 설정된 VLAN 또는 네트워크 세그먼트에서 vMotion을 위해 구성된 분산 포트 그룹입니다.
- VCF 변환에 필요한 소프트웨어를 다운로드하세요.

ONTAP tools for VMware vSphere HA 또는 비 HA 구성으로 설치할 수 있습니다. ONTAP 도구의 필수 구성 요소에 대한 전체 정보는 다음을 참조하세요. "ONTAP tools for VMware vSphere 의 필수 구성 요소" .

vSphere를 VCF 5.2로 변환하거나 가져오기 위해 지원되는 저장소 및 기타 고려 사항은 다음을 참조하세요. "기존

vSphere 환경을 VMware Cloud Foundation으로 변환하거나 가져오기 전 고려 사항" .

필수 소프트웨어는 다음을 참조하세요. "기존 vSphere 환경을 변환하거나 가져오기 위한 소프트웨어 다운로드" .

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 5.2 설명서" .

배포 단계

이 솔루션은 ONTAP tools for VMware vSphere 사용하여 FC 데이터스토어를 프로비저닝하고 기존 vSphere 8 클러스터를 VCF 관리 도메인으로 변환하는 프로세스를 다룹니다.

다음 단계를 완료하세요.

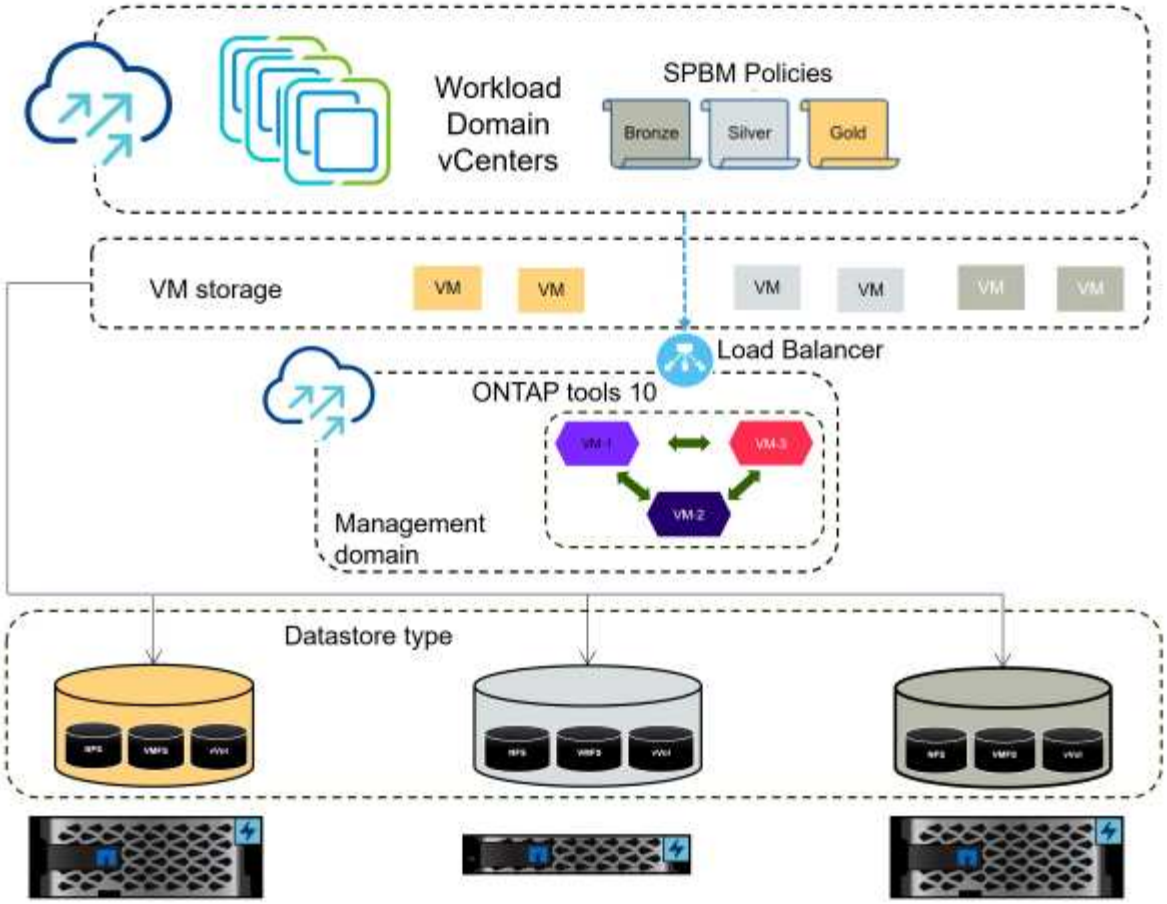
- ONTAP tools for VMware vSphere 배포합니다.
- ONTAP 도구를 사용하여 FC 데이터 저장소를 프로비저닝합니다.
- VCF 가져오기 도구를 vCenter 어플라이언스에 복사합니다.
- VCF 가져오기 도구를 사용하여 vCenter 어플라이언스에 대한 사전 검사를 실행합니다.
- vCenter 클러스터에 SDDC 관리자 VM을 배포합니다.
- 변환 프로세스 중에 배포할 NSX 클러스터에 대한 JSON 파일을 만듭니다.
- 필요한 소프트웨어를 SDDC 관리자에 업로드합니다.
- vSphere 클러스터를 SDDC 관리자 인벤토리로 변환합니다.

변환 프로세스 개요는 다음을 참조하세요. "VMware Cloud Foundation에서 vSphere 환경을 관리 도메인으로 변환하거나 vSphere 환경을 VI 워크로드 도메인으로 가져오기" .

ONTAP 도구 배포 및 **FC** 데이터 저장소 프로비저닝

ONTAP 도구 10의 아키텍처는 ONTAP 도구 서비스, vSphere 플러그인, REST API를 포함하는 모듈식 확장 가능 프레임워크를 활용하여 VMware 환경과 원활하게 통합되도록 설계되었으며, 이를 통해 효율적인 스토리지 관리, 자동화 및 데이터 보호가 가능합니다.

ONTAP tools for VMware vSphere HA 또는 비 HA 구성으로 설치할 수 있습니다.

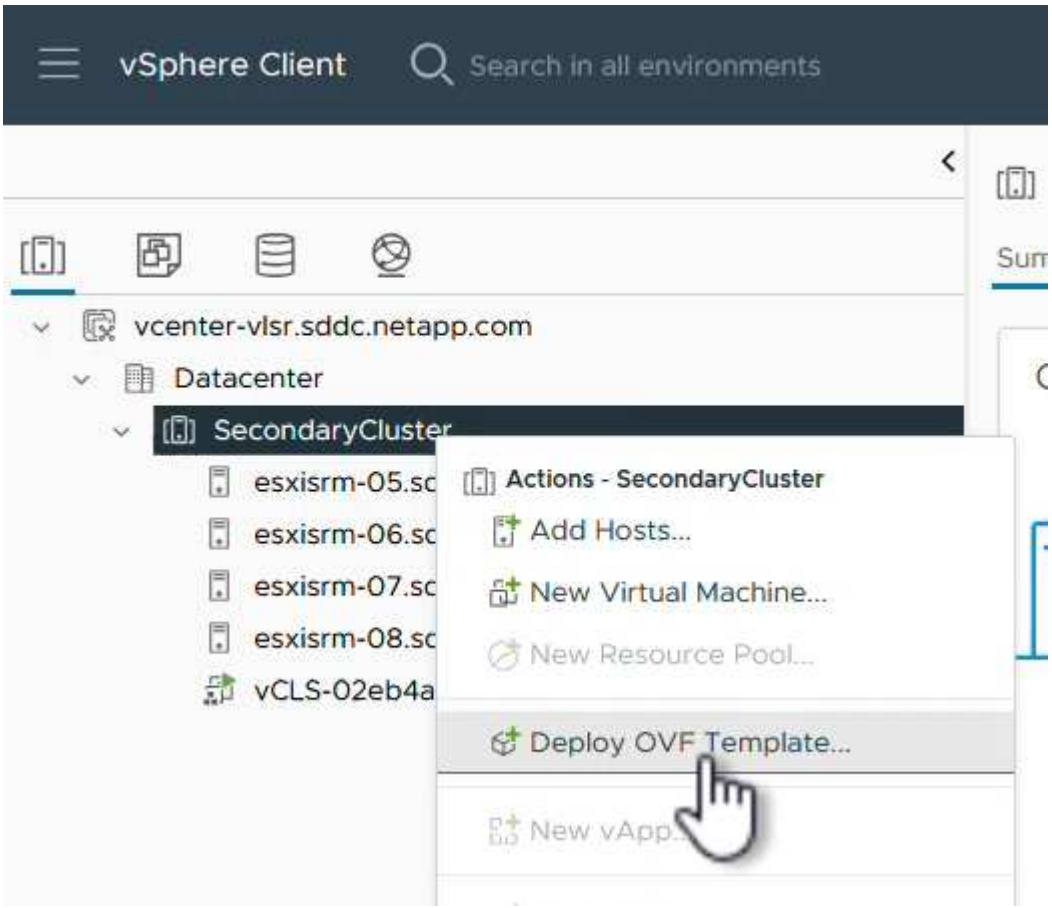

Workload
Domain
vCenters
SPBM Policies
Bronze
Silver
Gold
VM storage
VM
VM
VM
VM
VM
VM
Load Balancer
ONTAP tools 10
VM-1
VM-3
VM-2
Management
domain
Datastore type

ONTAP tools for VMware vSphere 배포

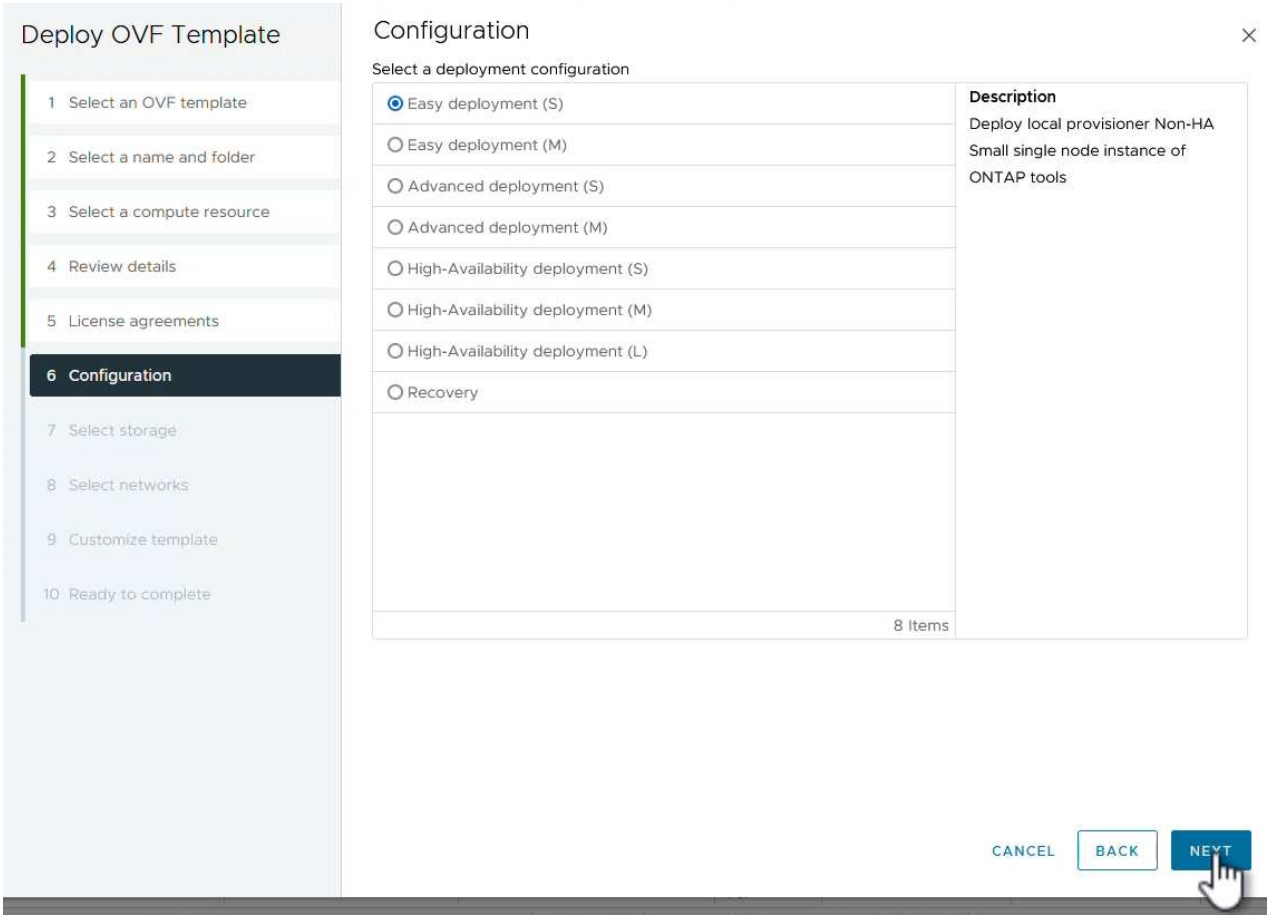
이 단계에서는 ONTAP 도구 10이 비 HA 구성으로 배포됩니다.

HA 및 비 HA 구성에 대한 추가 배포 세부 정보는 다음을 참조하세요. "ONTAP tools for VMware vSphere 배포" .

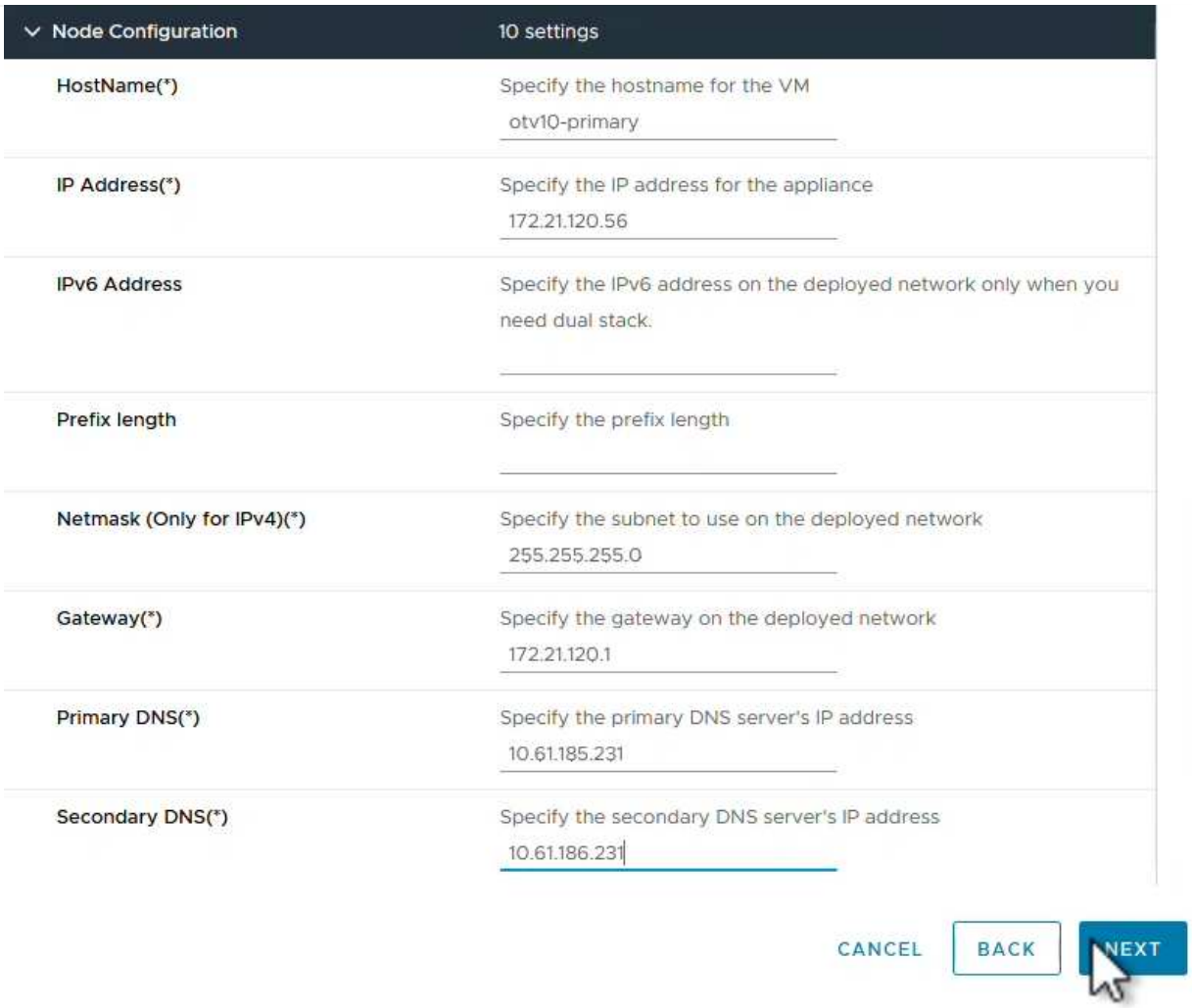
1. ONTAP 도구 10 OVA 템플릿을 다운로드하세요. "NetApp 지원 사이트" .
2. vSphere 클라이언트에서 클러스터를 마우스 오른쪽 버튼으로 클릭하고 *OVF 템플릿 배포*를 클릭합니다.



3. *OVF 템플릿 배포*에서 다음 단계를 완료하세요.
   - OVF 템플릿을 선택하세요.
   - 이름과 폴더를 선택하세요.
   - 컴퓨팅 리소스를 선택하세요.
   - 리뷰 세부 정보.
   - 라이센스 계약에 동의합니다.
4. 템플릿의 구성 페이지에서 HA 구성에 ONTAP 도구를 배포할지 여부를 포함한 배포 유형을 선택합니다. 계속하려면 *다음*을 클릭하세요.



5. 저장소 선택 페이지에서 VM을 설치할 데이터 저장소를 선택하고 *다음*을 클릭합니다.
6. ONTAP 도구 VM이 통신할 네트워크를 선택합니다. 계속하려면 *다음*을 클릭하세요.
7. "템플릿 사용자 지정" 창에서 필요한 모든 정보를 입력합니다.
    - 애플리케이션 사용자 이름 및 비밀번호
    - 프록시 URL을 포함한 ASUP(자동 지원)를 활성화할지 여부를 선택합니다.
    - 관리자 사용자 이름과 비밀번호.
    - NTP 서버.
    - 유지 관리 사용자 이름과 비밀번호(콘솔에서 사용되는 유지 관리 계정).
    - 배포 구성에 필요한 IP 주소를 제공합니다.
    - 노드 구성에 필요한 모든 네트워킹 정보를 제공합니다.

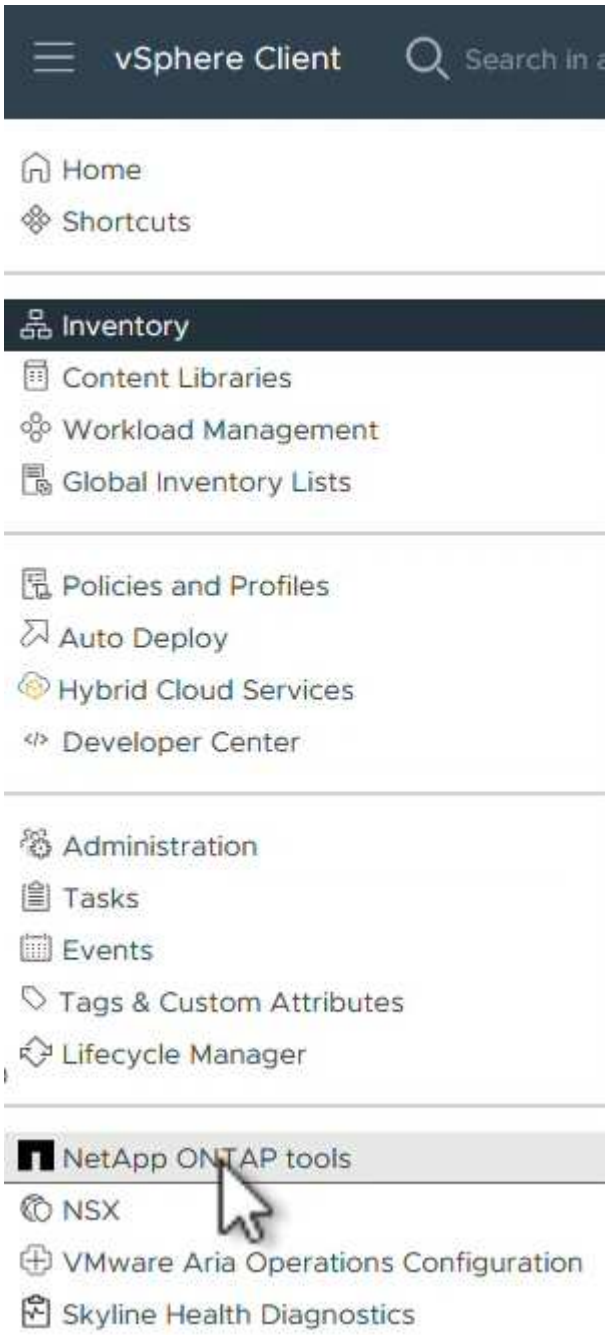


8. 마지막으로, 계속하려면 *다음*을 클릭하고, 배포를 시작하려면 *마침*을 클릭합니다.

ONTAP 도구 구성

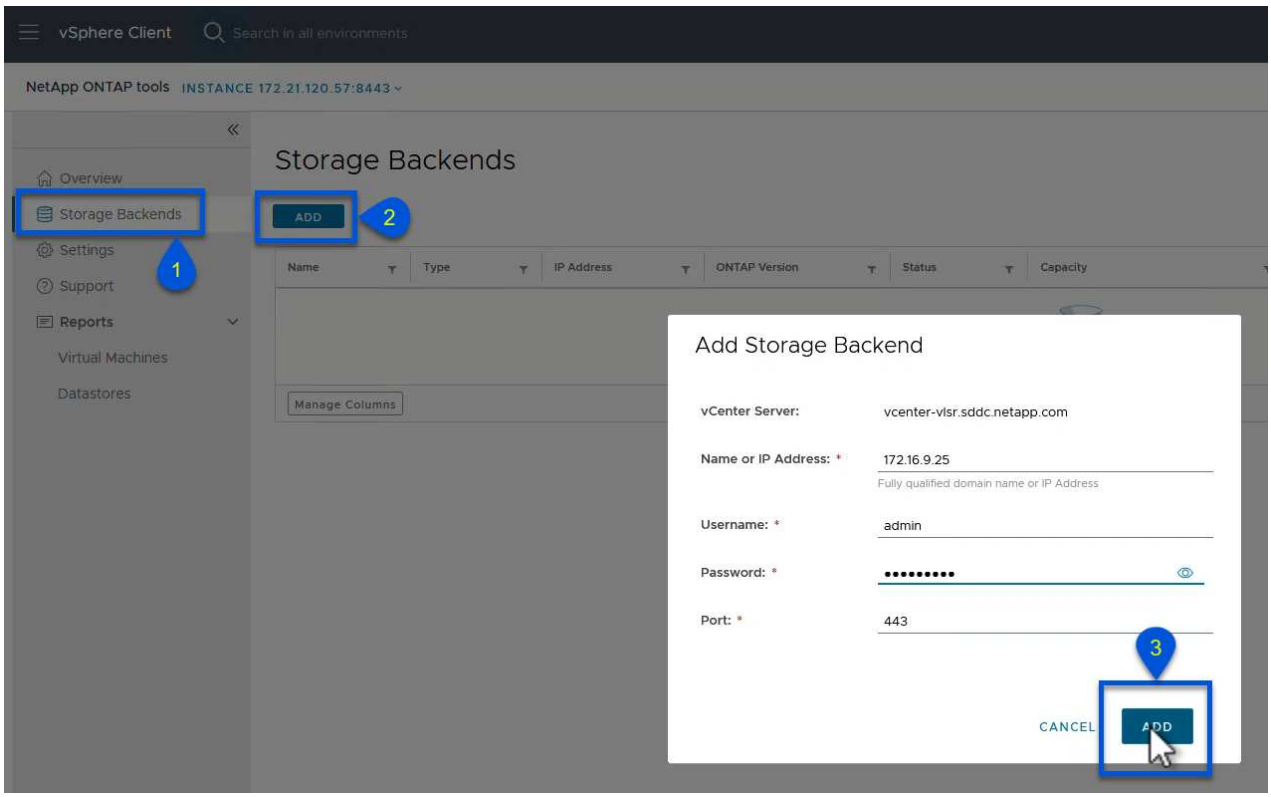
ONTAP 도구 VM이 설치되고 전원이 켜지면 vCenter 서버와 ONTAP 스토리지 시스템을 추가하는 등 몇 가지 기본 구성이 필요합니다. 설명서를 참조하세요 "ONTAP tools for VMware vSphere" 자세한 내용은.

1. 참조하다 "vCenter 인스턴스 추가" ONTAP 도구로 관리되도록 vCenter 인스턴스를 구성합니다.
2. ONTAP 스토리지 시스템을 추가하려면 vSphere 클라이언트에 로그인하고 왼쪽의 주 메뉴로 이동하세요. * NetApp ONTAP 도구*를 클릭하여 사용자 인터페이스를 시작합니다.



3. 왼쪽 메뉴에서 스토리지 백엔드*로 이동한 후 *추가*를 클릭하여 *스토리지 백엔드 추가 창에 액세스합니다.

4. 관리할 ONTAP 스토리지 시스템에 대한 IP 주소와 자격 증명을 입력하세요. *추가*를 클릭하여 완료하세요.

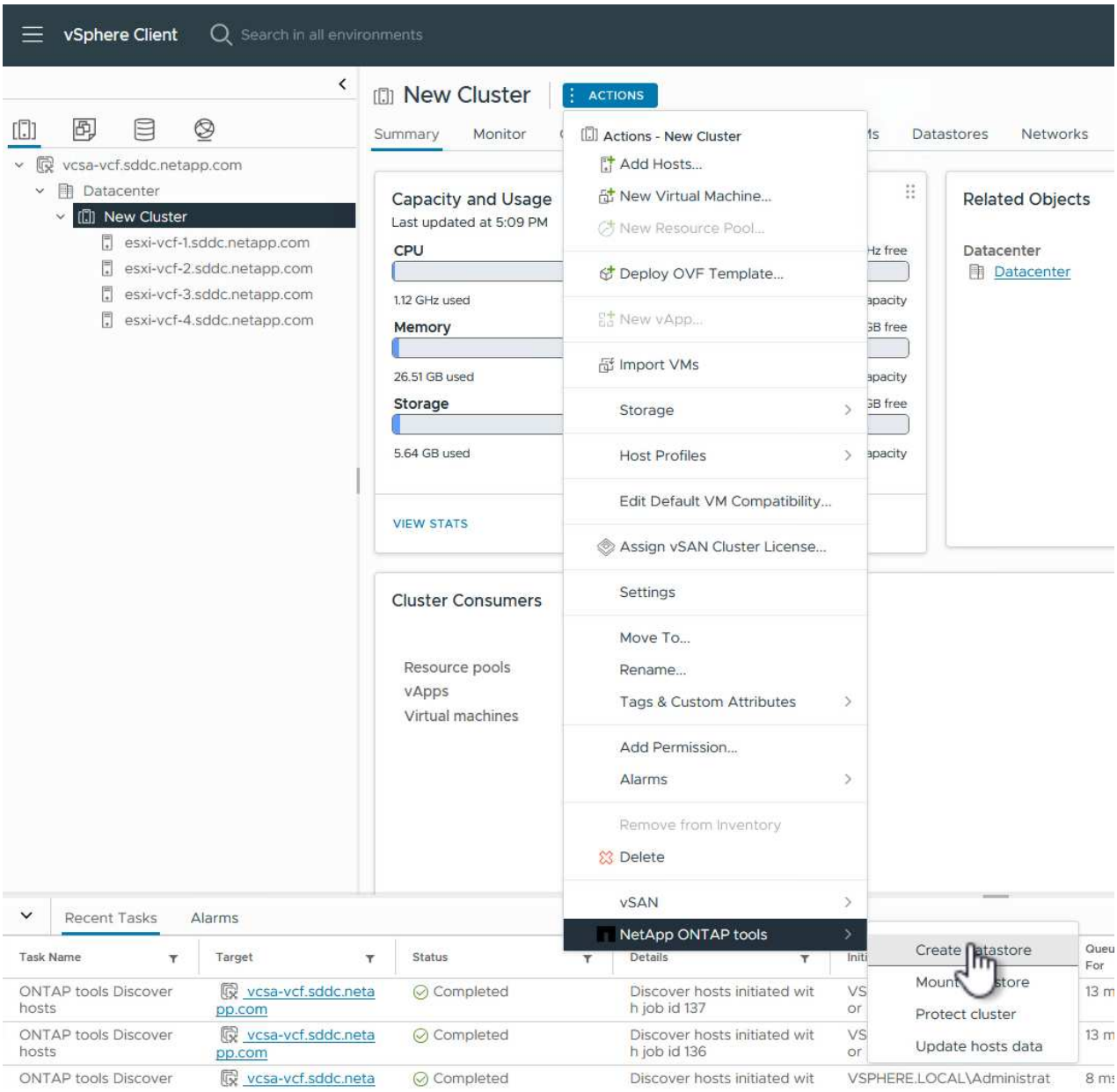


여기에서는 클러스터 IP 주소를 사용하여 vSphere 클라이언트 UI에 스토리지 백엔드가 추가됩니다. 이를 통해 스토리지 시스템의 모든 SVM을 완벽하게 관리할 수 있습니다. 또는 ONTAP 도구 관리자를 사용하여 스토리지 백엔드를 추가하고 vCenter 인스턴스와 연결할 수 있습니다. `https://loadBalanceIP:8443/virtualization/ui/` . 이 방법을 사용하면 vSphere 클라이언트 UI에서 SVM 자격 증명만 추가할 수 있으므로 스토리지 액세스를 보다 세부적으로 제어할 수 있습니다.

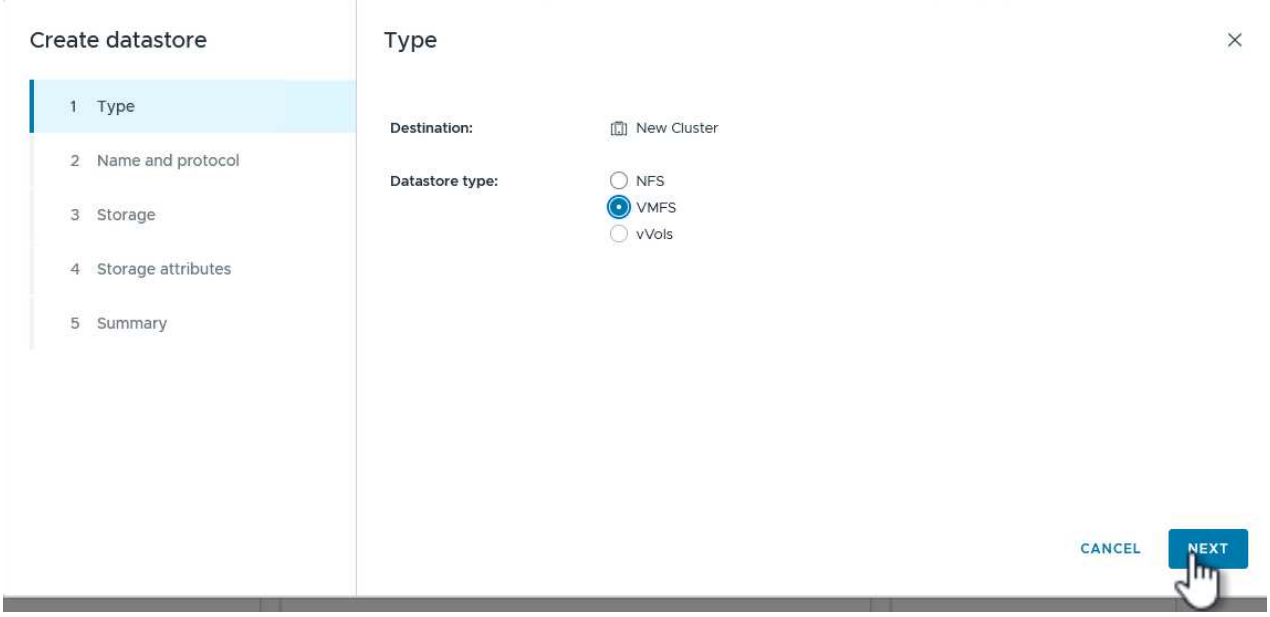
ONTAP 도구를 사용하여 **FC** 데이터 저장소 프로비저닝

ONTAP 도구는 vSphere 클라이언트 UI 전체의 기능을 통합합니다. 이 단계에서는 호스트 인벤토리 페이지에서 FC 데이터 저장소가 프로비저닝됩니다.

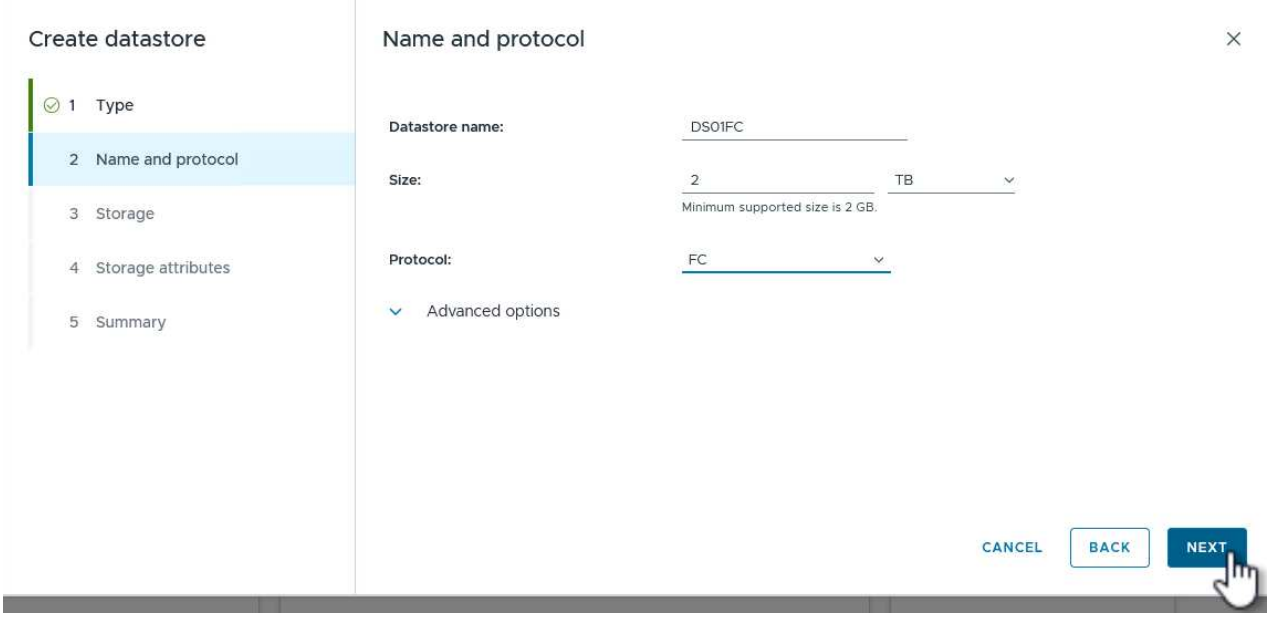
1. vSphere 클라이언트에서 호스트(또는 스토리지) 인벤토리로 이동합니다.
2. *작업 > NetApp ONTAP 도구 > 데이터 저장소 만들기*로 이동합니다.



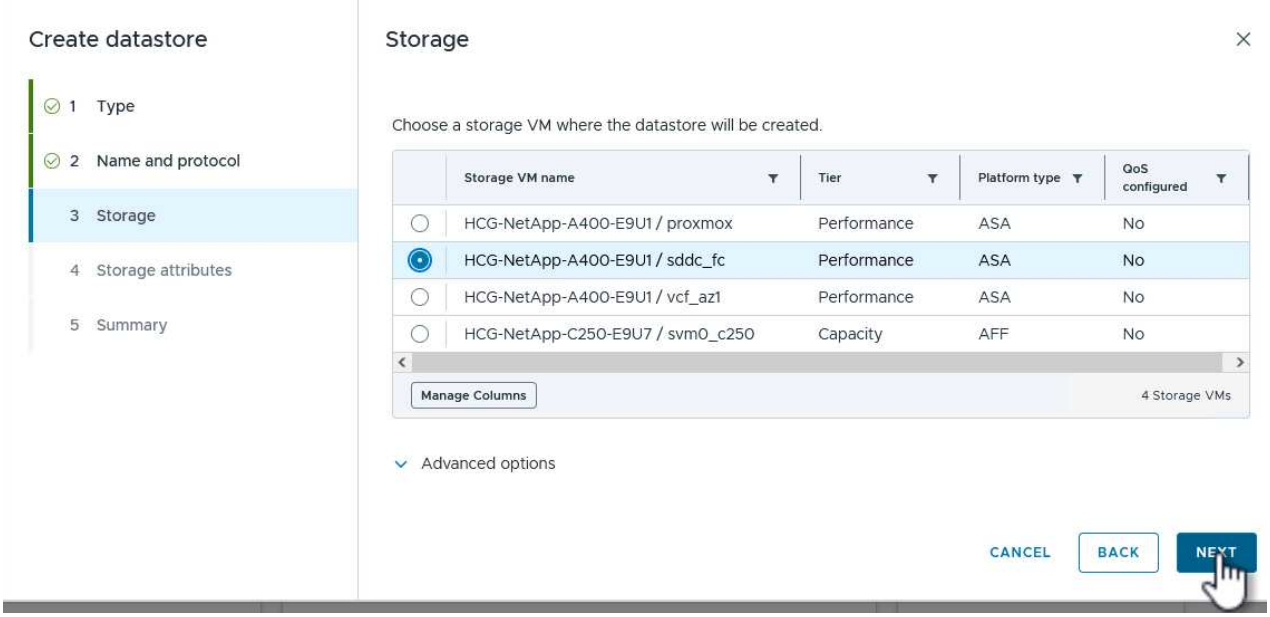
3. 데이터 저장소 만들기 마법사에서 만들 데이터 저장소 유형으로 VMFS를 선택합니다.



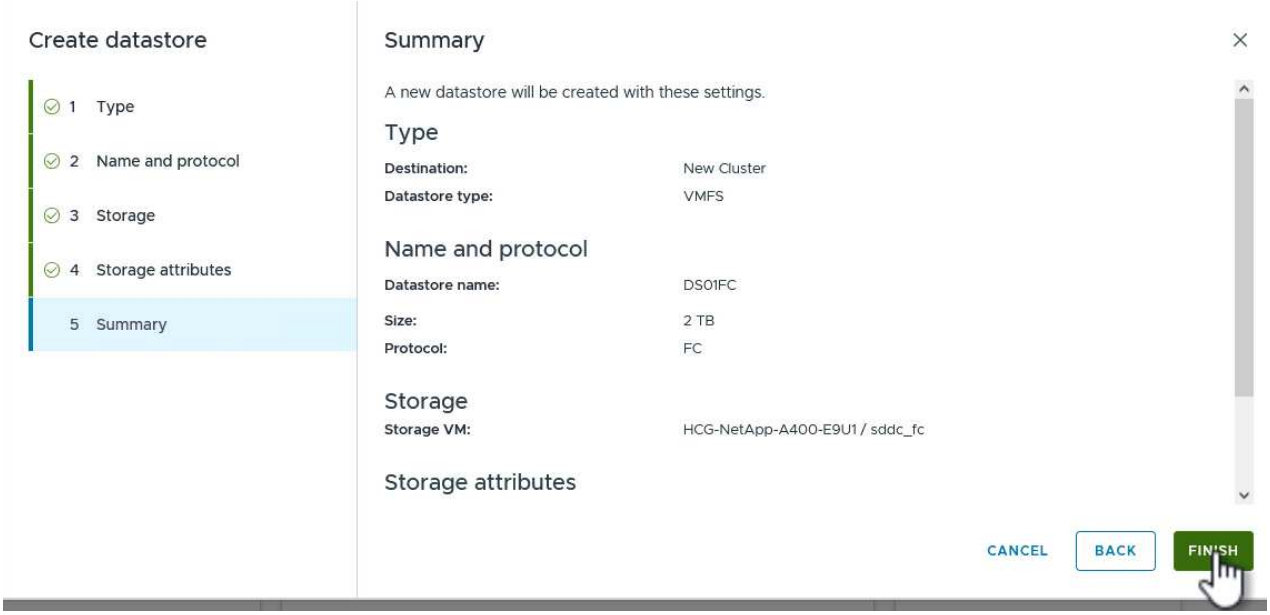
4. 이름 및 프로토콜 페이지에서 데이터 저장소의 이름, 크기, 사용할 FC 프로토콜을 입력합니다.



5. 저장소 페이지에서 ONTAP 스토리지 플랫폼과 스토리지 가상 머신(SVM)을 선택합니다. 여기에서 사용 가능한 사용자 정의 내보내기 정책을 선택할 수도 있습니다. 계속하려면 *다음*을 클릭하세요.



6. 저장소 속성 페이지에서 사용할 저장소 집계를 선택합니다. 계속하려면 *다음*을 클릭하세요.
7. 요약 페이지에서 정보를 검토하고 *마침*을 클릭하여 프로비저닝 프로세스를 시작합니다. ONTAP 도구는 ONTAP 스토리지 시스템에 볼륨을 생성하고 이를 클러스터의 모든 ESXi 호스트에 대한 FC 데이터 저장소로 마운트합니다.



vSphere 환경을 **VCF 5.2**로 변환

다음 섹션에서는 SDDC 관리자를 배포하고 vSphere 8 클러스터를 VCF 5.2 관리 도메인으로 변환하는 단계를 설명합니다. 필요한 경우, 추가 세부 정보는 VMware 문서를 참조하세요.

Broadcom의 VMware에서 제공하는 VCF 가져오기 도구는 vCenter 어플라이언스와 SDDC 관리자 모두에서 구성을 검증하고 vSphere 및 VCF 환경에 대한 변환 및 가져오기 서비스를 제공하는 유틸리티입니다.

자세한 내용은 다음을 참조하세요. "VCF 가져오기 도구 옵션 및 매개변수" .

VCF 가져오기 도구 복사 및 추출

VCF 가져오기 도구는 vCenter 어플라이언스에서 vSphere 클러스터가 VCF 변환 또는 가져오기 프로세스에 적합한지 확인하는 데 사용됩니다.

다음 단계를 완료하세요.

1. 다음 단계를 따르세요 "VCF 가져오기 도구를 대상 vCenter Appliance에 복사합니다." VMware Docs에서 VCF 가져오기 도구를 올바른 위치로 복사하세요.
2. 다음 명령을 사용하여 번들을 추출합니다.

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

vCenter 어플라이언스 검증

변환하기 전에 VCF 가져오기 도구를 사용하여 vCenter 어플라이언스를 검증합니다.

1. 다음 단계를 따르세요 "변환 전 대상 vCenter에서 사전 검사 실행" 검증을 실행하려면.
2. 다음 출력은 vCenter 어플라이언스가 사전 검사를 통과했음을 보여줍니다.

```
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter 172.21.166.57 --sso-user administrator@vsphere.local
[2024-10-23 19:03:23,609] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.0-24307788
Enter vCenter SSO password:
[2024-10-23 19:03:28,825] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2024-10-23 19:03:28,938] [INFO] vc_precheck: Connected to vCenter 172.21.166.57 in 0.11 seconds
[2024-10-23 19:03:28,939] [INFO] vc_precheck: Running pre-checks for vCenter 172.21.166.57...
[2024-10-23 19:03:28,939] [INFO] vc_precheck: [1/10] VC BOM version check...                    PASS
[2024-10-23 19:03:28,975] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...            PASS
[2024-10-23 19:03:28,999] [INFO] vc_precheck: [3/10] Supported storage available check...       PASS
[2024-10-23 19:03:29,020] [INFO] vc_precheck: [4/10] vCenter VM location check...               PASS
[2024-10-23 19:03:29,233] [INFO] vc_precheck: [5/10] VxRail registration check...               PASS
[2024-10-23 19:03:29,414] [INFO] vc_precheck: [6/10] NSX-T registration check...                PASS
[2024-10-23 19:03:29,437] [INFO] vc_precheck: [7/10] Standalone host check...                   PASS
[2024-10-23 19:03:31,870] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...  PASS
[2024-10-23 19:03:32,962] [INFO] vc_precheck: [9/10] ELM ring topology check...                 PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: [10/10] WCP import check...                       PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: All pre-checks passed!
[2024-10-23 19:03:33,383] [INFO] vc_precheck: Pre-checks for vCenter 172.21.166.57 completed in 4.44 seconds
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]#
```

SDDC 관리자 배포

SDDC 관리자는 VCF 관리 도메인으로 변환될 vSphere 클러스터에 함께 배치되어야 합니다.

VMware Docs의 배포 지침에 따라 배포를 완료하세요.

참조하다 "대상 vCenter에 SDDC Manager Appliance 배포" .

자세한 내용은 다음을 참조하세요."위원회 호스트" VCF 관리 가이드에서.

NSX 배포를 위한 JSON 파일 생성

vSphere 환경을 VMware Cloud Foundation으로 가져오거나 변환하는 동안 NSX Manager를 배포하려면 NSX 배포 사양을 만듭니다. NSX 배포에는 최소 3개의 호스트가 필요합니다.

자세한 내용은 다음을 참조하세요. "기존 vSphere 환경을 변환하거나 가져오기 위한 NSX 배포 사양 생성" .

> 변환 또는 가져오기 작업에서 NSX Manager 클러스터를 배포하는 경우 NSX-VLAN 네트워킹이 활용됩니다. NSX-VLAN 네트워킹의 제한 사항에 대한 자세한 내용은 "기존 vSphere 환경을 VMware Cloud Foundation으로 변환하거나 가져오기 전 고려 사항" 섹션을 참조하세요. NSX-VLAN 네트워킹 제한 사항에 대한 정보는 다음을 참조하세요. "기존 vSphere 환경을 VMware Cloud Foundation으로 변환하거나 가져오기 전 고려 사항" .

다음은 NSX 배포를 위한 JSON 파일의 예입니다.

```
{
  "license_key": "xxxxx-xxxxx-xxxxx-xxxxx-xxxxx",
  "form_factor": "medium",
  "admin_password": "************************",
  "install_bundle_path": "/tmp/vcfimport/bundle-133764.zip",
  "cluster_ip": "172.21.166.72",
  "cluster_fqdn": "vcf-m02-nsx01.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "vcf-m02-nsx01a.sddc.netapp.com",
    "name": "vcf-m02-nsx01a",
    "ip_address": "172.21.166.73",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01b.sddc.netapp.com",
    "name": "vcf-m02-nsx01b",
    "ip_address": "172.21.166.74",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01c.sddc.netapp.com",
    "name": "vcf-m02-nsx01c",
    "ip_address": "172.21.166.75",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

JSON 파일을 SDDC 관리자의 디렉토리에 복사합니다.

SDDC 관리자에 소프트웨어 업로드

VCF 가져오기 도구와 NSX 배포 번들을 SDDC 관리자의 /home/vcf/vcfimport 디렉토리에 복사합니다.

보다 "SDDC 관리자 어플라이언스에 필요한 소프트웨어 업로드" 자세한 지침은 여기를 참조하세요.

vSphere 클러스터를 **VCF** 관리 도메인으로 변환

VCF 가져오기 도구는 변환 과정을 수행하는 데 사용됩니다. VCF 가져오기 도구 기능의 인쇄물을 검토하려면 /home/vcf/vcf-import-package/vcf-brownfield-import-<version>/vcf-brownfield-toolset 디렉토리에서 다음 명령을 실행하세요.

```
python3 vcf_brownfield.py --help
```

다음 명령은 vSphere 클러스터를 VCF 관리 도메인으로 변환하고 NSX 클러스터를 배포하기 위해 실행됩니다.

```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --domain-name '<wld-domain-name>' --nsx-deployment-spec
-path '<nsx-deployment-json-spec-path>'
```

전체 지침은 다음을 참조하세요. "vSphere 환경을 SDDC 관리자 인벤토리로 변환하거나 가져오기" .

VCF에 라이선싱 추가

변환을 완료한 후에는 환경에 라이선스를 추가해야 합니다.

1. SDDC 관리자 UI에 로그인합니다.
2. 탐색 창에서 *관리 > 라이선싱*으로 이동합니다.
3. *+ 라이선스 키*를 클릭하세요.
4. 드롭다운 메뉴에서 제품을 선택하세요.
5. 라이센스 키를 입력하세요.
6. 라이센스에 대한 설명을 제공하세요.
7. *추가*를 클릭하세요.
8. 각 라이선스에 대해 이 단계를 반복합니다.

ONTAP tools for VMware vSphere 에 대한 비디오 데모

ONTAP tools for VMware vSphere 사용한 NFS 데이터 저장소

주요 저장소를 사용하여 VCF 제공

ONTAP 주요 스토리지 솔루션으로 사용하여 VCF 환경 제공

NetApp ONTAP 스토리지는 VMware Cloud Foundation(VCF) 관리 및 Virtual Infrastructure(VI) 워크로드 도메인을 위한 이상적인 기본 스토리지 솔루션입니다. ONTAP 높은 성능, 확장성, 고급 데이터 관리 및 원활한 통합을 제공하여 운영 효율성과 데이터 보호를 개선합니다.

적절한 도메인과 적절한 프로토콜에서 VCF 환경을 프로비저닝하는 데 대한 기술적 세부 사항은 다음 솔루션을 참조하세요.

- "FC를 사용한 관리 도메인"
- "NFS를 사용한 관리 도메인"
- "FC를 사용한 가상 인프라 워크로드 도메인"
- "NFS를 사용한 가상 인프라 워크로드 도메인"

ONTAP 에서 FC 기반 VMFS 데이터 저장소를 VCF 관리 도메인의 주 저장소로 사용합니다.

이 사용 사례에서는 ONTAP 의 기존 FC 기반 VMFS 데이터 저장소를 VMware Cloud Foundation(VCF) 관리 도메인의 기본 스토리지로 사용하는 절차를 설명합니다. 이 절차에서는 필요한 구성 요소, 구성 및 배포 단계를 요약합니다.

소개

적절한 경우 VCF의 SDDC 관리자에서 수행해야 하는 단계에 대한 외부 문서를 참조하고, 스토리지 구성 부분에만 해당하는 단계를 참조합니다.

기존 FC 기반 vSphere 환경을 ONTAP 으로 변환하는 방법에 대한 정보는 다음을 참조하세요."vSphere 환경(FC 데이터 저장소)을 VCF 관리 도메인으로 변환" .

> VCF 릴리스 5.2에서는 기존 vSphere 8 환경을 VCF 관리 도메인으로 변환하거나 VCF VI 워크로드 도메인으로 가져오는 기능이 도입되었습니다. 이 릴리스 이전에는 VMware vSAN이 VCF 관리 도메인의 주 스토리지에 대한 유일한 옵션이었습니다.

> 이 솔루션은 NetApp ASA, AFF , FAS 포함한 FC 스토리지를 지원하는 ONTAP 플랫폼에 적용할 수 있습니다.

필수 조건

이 시나리오에서는 다음 구성 요소와 구성이 사용됩니다.

- FC 트래픽을 허용하도록 구성된 스토리지 가상 머신(SVM)이 있는 NetApp 스토리지 시스템입니다.
- FC 트래픽을 전달하고 SVM과 연관되는 FC 패브릭에 논리 인터페이스(LIF)가 생성되었습니다.
- FC 스위치에서 호스트 HBA 및 스토리지 대상에 대한 단일 이니시에이터-대상 구역 설정을 사용하도록 구역 설정이 구성되었습니다.

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

배포 단계

관리 도메인 - 기본 클러스터

초기 클러스터의 FC 주 저장소는 VCF 브라운필드 가져오기 도구에서만 지원됩니다. VCF가 Cloud Builder 도구(릴리스 버전 5.2.x 이전)를 사용하여 배포된 경우 vSAN만 지원됩니다.

기존 vSphere 환경 사용에 대한 자세한 내용은 다음을 참조하세요. "기존 vSphere 환경을 관리 도메인으로 변환" 자세한 내용은.

관리 도메인 - 추가 클러스터

관리 도메인의 추가 vSphere 클러스터는 다음 옵션을 사용하여 배포할 수 있습니다.

- vSphere 환경에 추가 클러스터를 두고 VCF 브라운필드 가져오기 도구를 사용하여 vSphere 환경을 관리 도메인으로 변환합니다. "ONTAP tools for VMware vSphere" "시스템 관리자 또는 ONTAP API" VMFS 데이터스토어를 vSphere 클러스터에 배포하는 데 사용할 수 있습니다.
- SDDC API를 사용하여 추가 클러스터를 배포합니다. vSphere 호스트에는 VMFS 데이터 저장소가 구성되어 있어야 합니다. 사용 "시스템 관리자 또는 ONTAP API" LUN을 vSphere 호스트에 배포합니다.
- SDDC 관리자 UI를 사용하여 추가 클러스터를 배포합니다. 하지만 이 옵션은 버전 5.2.x까지만 VSAN 데이터 저장소를 생성합니다.

추가 정보

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

ONTAP 에서 VCF 관리 도메인의 주 저장소로 NFS 데이터 저장소 사용

이 사용 사례에서는 ONTAP 의 기존 NFS 데이터 저장소를 VMware Cloud Foundation(VCF) 관리 도메인의 기본 저장소로 사용하는 절차를 설명합니다. 이 절차에서는 필요한 구성 요소, 구성 단계 및 배포 프로세스를 요약합니다.

소개

적절한 경우 VCF의 SDDC 관리자에서 수행해야 하는 단계에 대한 외부 문서를 참조하고, 스토리지 구성 부분에만 해당하는 단계를 참조합니다.

기존 NFS 기반 vSphere 환경을 ONTAP 으로 변환하는 방법에 대한 정보는 다음을 참조하세요."vSphere 환경(NFS 데이터 저장소)을 VCF 관리 도메인으로 변환" .

> VCF 릴리스 5.2에서는 기존 vSphere 8 환경을 VCF 관리 도메인으로 변환하거나 VCF VI 워크로드 도메인으로 가져오는 기능이 도입되었습니다. 이 릴리스 이전에는 VMware vSAN이 VCF 관리 도메인의 주 스토리지에 대한 유일한 옵션이었습니다.

이 솔루션은 NetApp AFF 및 FAS 포함한 NFS 스토리지를 지원하는 ONTAP 플랫폼에 적용할 수 있습니다.

필수 조건

이 시나리오에서는 다음 구성 요소와 구성이 사용됩니다.

- NFS 트래픽을 허용하도록 구성된 스토리지 가상 머신(SVM)이 있는 NetApp 스토리지 시스템입니다.
- NFS 트래픽을 전달하고 SVM과 연관되는 논리적 인터페이스(LIF)가 IP 네트워크에 생성되었습니다.
- 4개의 ESXi 호스트와 클러스터에 함께 배치된 vCenter 어플라이언스를 갖춘 vSphere 8 클러스터입니다.
- 이 목적으로 설정된 VLAN 또는 네트워크 세그먼트에서 vMotion 및 NFS 스토리지 트래픽을 위해 구성된 분산 포트 그룹입니다.
- VCF 변환에 필요한 소프트웨어를 다운로드하세요.

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

배포 단계

관리 도메인 - 기본 클러스터

초기 클러스터의 NFS 주 저장소는 VCF 브라운필드 가져오기 도구에서만 지원됩니다. VCF가 Cloud Builder 도구(버전 5.2.x까지)로 배포된 경우 VSAN만 지원됩니다.

기존 vSphere 환경 사용에 대한 자세한 내용은 다음을 참조하세요. "기존 vSphere 환경을 관리 도메인으로 변환" 자세한 내용은.

관리 도메인 - 추가 클러스터

관리 도메인의 추가 vSphere 클러스터는 다음 옵션을 사용하여 배포할 수 있습니다.

- vSphere 환경에 추가 클러스터를 두고 VCF 브라운필드 가져오기 도구를 사용하여 vSphere 환경을 관리 도메인으로 변환합니다. "ONTAP tools for VMware vSphere" "시스템 관리자 또는 ONTAP API" NFS 데이터스토어를 vSphere 클러스터에 배포하는 데 사용할 수 있습니다.
- SDDC API를 사용하여 추가 클러스터를 배포합니다. vSphere 호스트에는 NFS 데이터 저장소가 구성되어 있어야 합니다. 사용 "시스템 관리자 또는 ONTAP API" LUN을 vSphere 호스트에 배포합니다.
- SDDC 관리자 UI를 사용하여 추가 클러스터를 배포합니다. 하지만 이 옵션은 5.2.x 이전 릴리스에서만 vSAN 데이터 저장소를 생성합니다.

추가 정보

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

ONTAP 에서 FC 기반 VMFS 데이터 저장소를 VI 워크로드 도메인의 주요 스토리지로 사용

이 사용 사례에서는 VMware Cloud Foundation(VCF) Virtual Infrastructure(VI) 워크로드 도메인에 대한 기본 스토리지 솔루션으로 ONTAP 에 파이버 채널(FC) VMFS 데이터 저장소를 설정하는 절차를 설명합니다. 이 절차에서는 필요한 구성 요소, 구성 단계 및 배포 프로세스를 요약합니다.

파이버 채널의 이점

고성능: FC는 고속 데이터 전송률을 제공하므로 대량의 데이터에 빠르고 안정적으로 액세스해야 하는 애플리케이션에 이상적입니다.

낮은 지연 시간: 매우 낮은 지연 시간은 데이터베이스 및 가상화 환경과 같은 성능에 민감한 애플리케이션에 매우 중요합니다.

신뢰성: FC 네트워크는 내장된 중복성 및 오류 수정과 같은 기능을 갖추고 있어 견고성과 안정성이 뛰어난 것으로 알려져 있습니다.

전용 대역폭: FC는 스토리지 트래픽에 전용 대역폭을 제공하여 네트워크 혼잡 위험을 줄입니다.

NetApp 스토리지 시스템에서 파이버 채널을 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요. "FC를 사용한 SAN 프로비저닝" .

시나리오 개요

이 시나리오에서는 다음과 같은 상위 수준 단계를 다룹니다.

- FC 트래픽을 위한 논리 인터페이스(LIF)가 있는 스토리지 가상 머신(SVM)을 만듭니다.
- 배포될 호스트의 WWPN 정보를 수집하고 ONTAP 스토리지 시스템에 해당 이니시에이터 그룹을 생성합니다.
- ONTAP 스토리지 시스템에 FC 볼륨을 생성합니다.
- FC 볼륨을 생성하기 위해 맵 개시자 그룹
- FC 스위치에서 단일 이니시에이터-타겟 구역 설정을 활용합니다. 각 개시자마다 하나의 영역을 만듭니다(단일 개시자 영역).
  - 각 영역에 대해 SVM에 대한 ONTAP FC 논리 인터페이스(WWPN)인 대상을 포함합니다. SVM당 노드당 최소 2개의 논리적 인터페이스가 있어야 합니다. 물리적 포트의 WWPN을 사용하지 마세요.
- SDDC Manager에서 vMotion 트래픽을 위한 네트워크 풀을 생성합니다.
- VI 워크로드 도메인에서 사용할 VCF의 커미션 호스트입니다.
- FC 데이터스토어를 주 스토리지로 사용하여 VCF에 VI 워크로드 도메인을 배포합니다.

> 이 솔루션은 NetApp AFF 및 FAS 포함한 NFS 스토리지를 지원하는 ONTAP 플랫폼에 적용할 수 있습니다.

필수 조건

이 시나리오에서는 다음 구성 요소와 구성이 사용됩니다.

- FC 스위치에 연결된 FC 포트가 있는 ONTAP AFF 또는 ASA 스토리지 시스템.

- FC lifes로 생성된 SVM입니다.
- FC 스위치에 연결된 FC HBA가 있는 vSphere.
- FC 스위치에는 단일 이니시에이터-타겟 구역 설정이 구성됩니다.

NetApp FC LUN에 대해 다중 경로를 권장합니다.

배포 단계

관리 도메인 - 기본 클러스터

초기 클러스터의 FC 주 저장소는 VCF 브라운필드 가져오기 도구에서만 지원됩니다. VCF가 CloudBuilder 도구(버전 5.2.x까지)로 배포된 경우 VSAN만 지원됩니다. 나타내다 "기존 vSphere 환경을 관리 도메인으로 변환" 자세한 내용은.

관리 도메인 - 추가 클러스터

관리 도메인의 추가 vSphere 클러스터는 다음 옵션을 사용하여 배포할 수 있습니다. * vSphere 환경에 추가 클러스터를 두고 VCF 브라운필드 가져오기 도구를 사용하여 vSphere 환경을 관리 도메인으로 변환합니다. "ONTAP tools for VMware vSphere" , "시스템 관리자 또는 ONTAP API" VMFS 데이터스토어를 vSphere 클러스터에 배포하는 데 사용할 수 있습니다. * SDDC API를 사용하여 추가 클러스터를 배포합니다. vSphere 호스트에는 VMFS 데이터 저장소가 구성되어 있어야 합니다. 사용 "시스템 관리자 또는 ONTAP API" LUN을 vSphere 호스트에 배포합니다. * SDDC 관리자 UI를 사용하여 추가 클러스터를 배포합니다. 하지만 이 옵션은 버전 5.2.x까지만 VSAN 데이터 저장소를 생성합니다.

VI 워크로드 도메인 - 기본 클러스터

관리 도메인이 실행되면 VI 워크로드 도메인을 생성할 수 있습니다.

- SDDC 관리자 UI 사용. vSphere 호스트에는 VMFS 데이터 저장소가 구성되어 있어야 합니다. System Manager 또는 ONTAP API를 사용하여 LUN을 vSphere 호스트에 배포합니다.
- 기존 vSphere 환경을 새로운 VI 워크로드 도메인으로 가져옵니다. ONTAP tools for VMware vSphere, System Manager 또는 ONTAP API를 사용하여 VMFS 데이터스토어를 vSphere 클러스터에 배포할 수 있습니다.

VI 워크로드 도메인 - 추가 클러스터

VI 워크로드가 실행되면 다음 옵션을 사용하여 FC LUN의 VMFS에 추가 클러스터를 배포할 수 있습니다.

- VCF 브라운필드 가져오기 도구를 사용하여 vSphere 환경의 추가 클러스터를 가져왔습니다. ONTAP tools for VMware vSphere, System Manager 또는 ONTAP API를 사용하여 VMFS 데이터스토어를 vSphere 클러스터에 배포할 수 있습니다.
- SDDC 관리자 UI 또는 API를 사용하여 추가 클러스터를 배포합니다. vSphere 호스트에는 VMFS 데이터 저장소가 구성되어 있어야 합니다. System Manager 또는 ONTAP API를 사용하여 LUN을 vSphere 호스트에 배포합니다.

추가 정보

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

VI 워크로드 도메인의 주요 스토리지로 ONTAP 의 NFS 데이터 저장소 사용

이 사용 사례에서는 VMware Cloud Foundation(VCF) Virtual Infrastructure(VI) 워크로드 도메인에 대한 기본 스토리지 솔루션으로 ONTAP 에서 NFS 데이터 저장소를 구성하는 절차를 설명합니다. 이 절차에서는 필요한 구성 요소, 구성 단계 및 배포 프로세스를 요약합니다.

NFS의 이점

간단하고 사용 용이성**:** NFS는 설정과 관리가 간단하므로 빠르고 쉽게 파일을 공유해야 하는 환경에 매우 적합한 선택입니다.

확장성**:** ONTAP의 아키텍처는 NFS가 효율적으로 확장되어 인프라를 크게 변경하지 않고도 증가하는 데이터 요구 사항을 지원할 수 있도록 해줍니다.

유연성**:** NFS는 광범위한 애플리케이션과 작업 부하를 지원하므로 가상화된 환경을 포함한 다양한 사용 사례에 다양하게 활용할 수 있습니다.

자세한 내용은 vSphere 8에 대한 NFS v3 참조 가이드를 참조하세요.

NetApp 스토리지 시스템에서 파이버 채널을 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요."vSphere 8용 NFS v3 참조 가이드" .

시나리오 개요

이 시나리오에서는 다음과 같은 상위 수준 단계를 다룹니다.

- NFS 트래픽을 위한 논리적 인터페이스(LIF)를 갖춘 스토리지 가상 머신(SVM)을 생성합니다.
- ONTAP 스토리지 가상 머신(SVM)에 대한 네트워킹을 확인하고 NFS 트래픽을 전송하는 논리적 인터페이스(LIF)가 있는지 확인합니다.
- ESXi 호스트가 NFS 볼륨에 액세스할 수 있도록 내보내기 정책을 만듭니다.
- ONTAP 스토리지 시스템에 NFS 볼륨을 생성합니다.
- SDDC Manager에서 NFS 및 vMotion 트래픽을 위한 네트워크 풀을 만듭니다.
- VI 워크로드 도메인에서 사용할 VCF의 커미션 호스트입니다.
- NFS 데이터 저장소를 주 저장소로 사용하여 VCF에 VI 워크로드 도메인을 배포합니다.
- VMware VAAI용 NetApp NFS 플러그인 설치

> 이 솔루션은 NetApp AFF 및 FAS 포함한 NFS 스토리지를 지원하는 ONTAP 플랫폼에 적용할 수 있습니다.

필수 조건

이 시나리오에서는 다음 구성 요소와 구성이 사용됩니다.

- NFS 트래픽을 허용하도록 구성된 스토리지 가상 머신(SVM)이 있는 NetApp AFF 스토리지 시스템입니다.
- NFS 트래픽을 전달하고 SVM과 연관되는 논리적 인터페이스(LIF)가 IP 네트워크에 생성되었습니다.
- VCF 관리 도메인 배포가 완료되었으며 SDDC 관리자 인터페이스에 액세스할 수 있습니다.

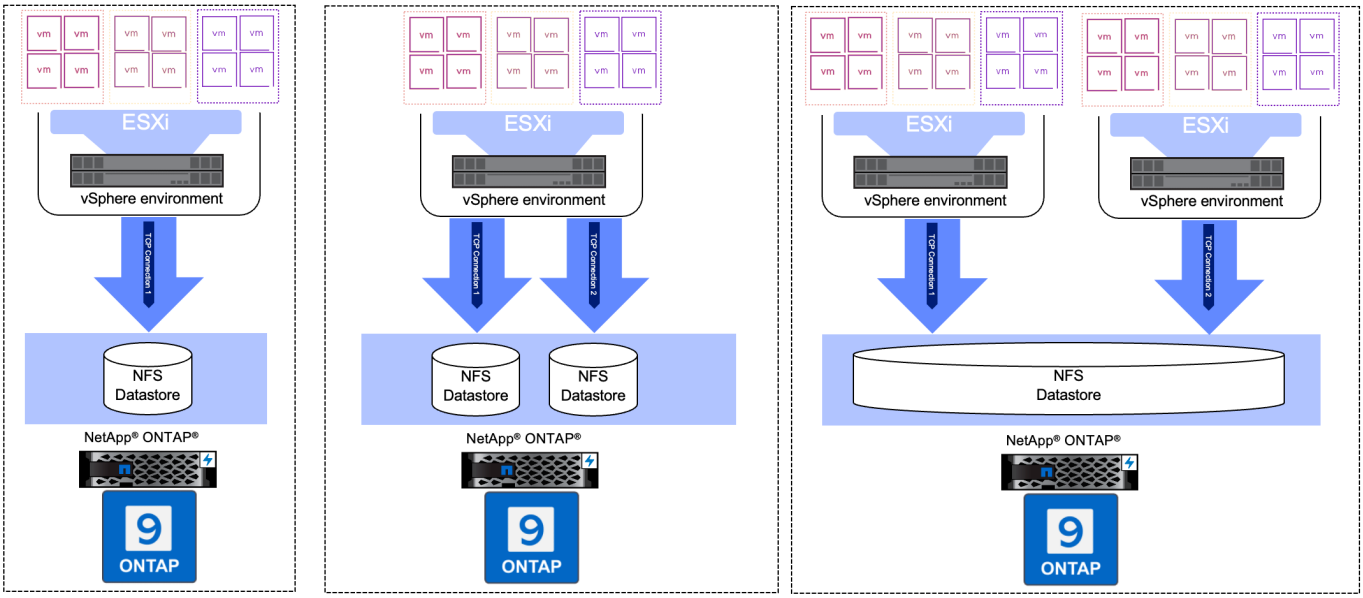
- VCF 관리 네트워크에서 통신을 위해 구성된 4개의 ESXi 호스트.
- 이 목적으로 설정된 VLAN 또는 네트워크 세그먼트의 vMotion 및 NFS 스토리지 트래픽을 위해 예약된 IP 주소입니다.

> VI 워크로드 도메인을 배포할 때 VCF는 NFS 서버에 대한 연결을 검증합니다. 이 작업은 NFS IP 주소와 함께 추가 vmkernel 어댑터를 추가하기 전에 ESXi 호스트의 관리 어댑터를 사용하여 수행됩니다. 따라서 검증을 진행할 수 있도록 1) 관리 네트워크가 NFS 서버로 라우팅 가능한지, 2) 관리 네트워크의 LIF가 NFS 데이터 저장소 볼륨을 호스팅하는 SVM에 추가되었는지 확인해야 합니다.

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

vSphere 클러스터에서 NFS를 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요."vSphere 8용 NFS v3 참조 가이드" .



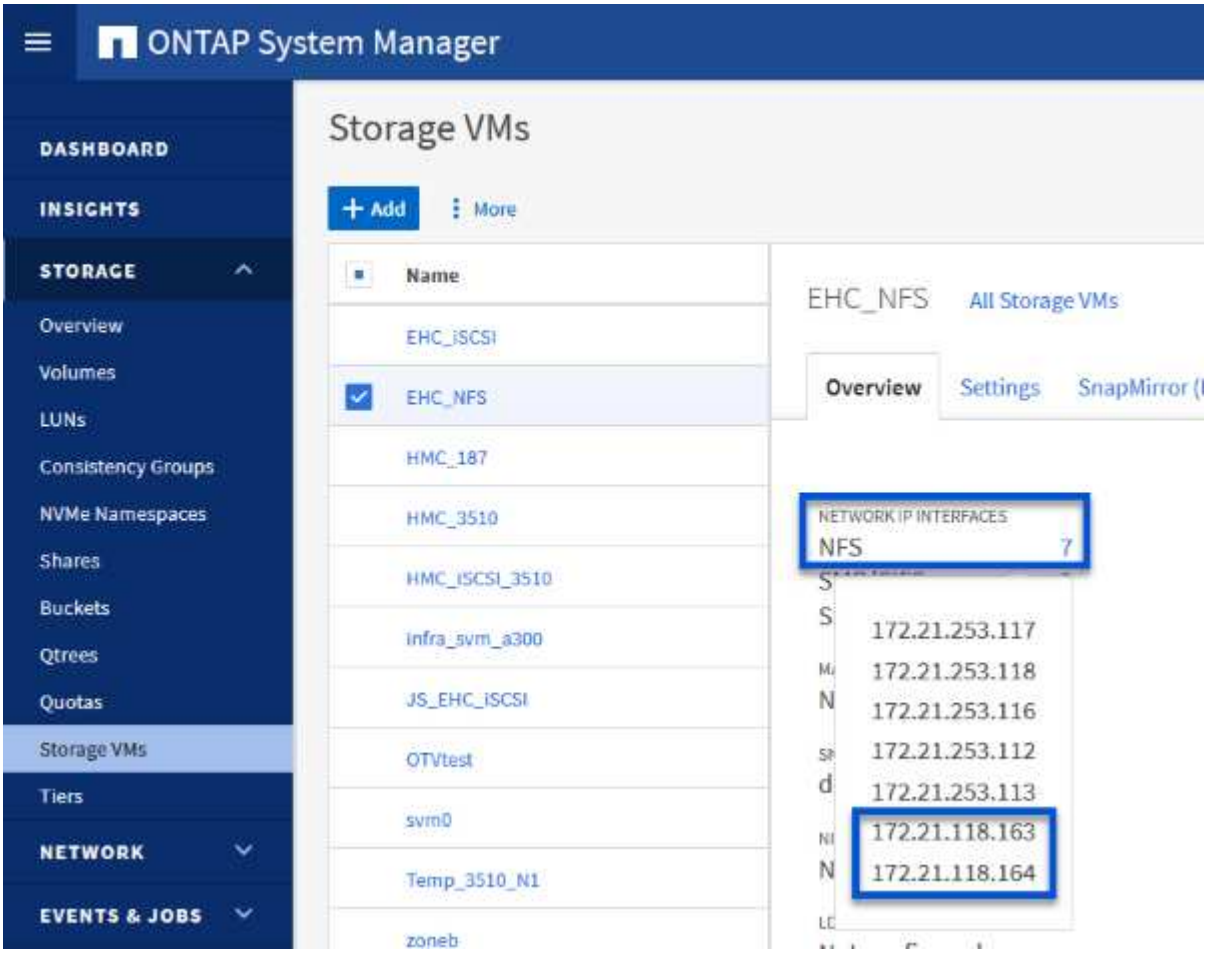
배포 단계

NFS 데이터 저장소를 주 저장소로 사용하여 VI 워크로드 도메인을 배포하려면 다음 단계를 완료하세요.

ONTAP SVM에 대한 네트워킹 확인

ONTAP 스토리지 클러스터와 VI 워크로드 도메인 간 NFS 트래픽을 전송할 네트워크에 필요한 논리적 인터페이스가 설정되었는지 확인합니다.

1. ONTAP 시스템 관리자의 왼쪽 메뉴에서 저장소 **VM***으로 이동한 다음 **NFS** 트래픽에 사용할 **SVM**을 클릭합니다**.** *개요 탭의 네트워크 **IP** 인터페이스*에서 ***NFS** 오른쪽에 있는 숫자를 클릭합니다. 목록에서 필요한 LIF IP 주소가 나열되어 있는지 확인하세요.



또는 다음 명령을 사용하여 ONTAP CLI에서 SVM과 연관된 LIF를 확인하세요.

```
network interface show -vserver <SVM_NAME>
```

1. ESXi 호스트가 ONTAP NFS 서버와 통신할 수 있는지 확인합니다. SSH를 통해 ESXi 호스트에 로그인하고 SVM LIF에 ping을 보냅니다.

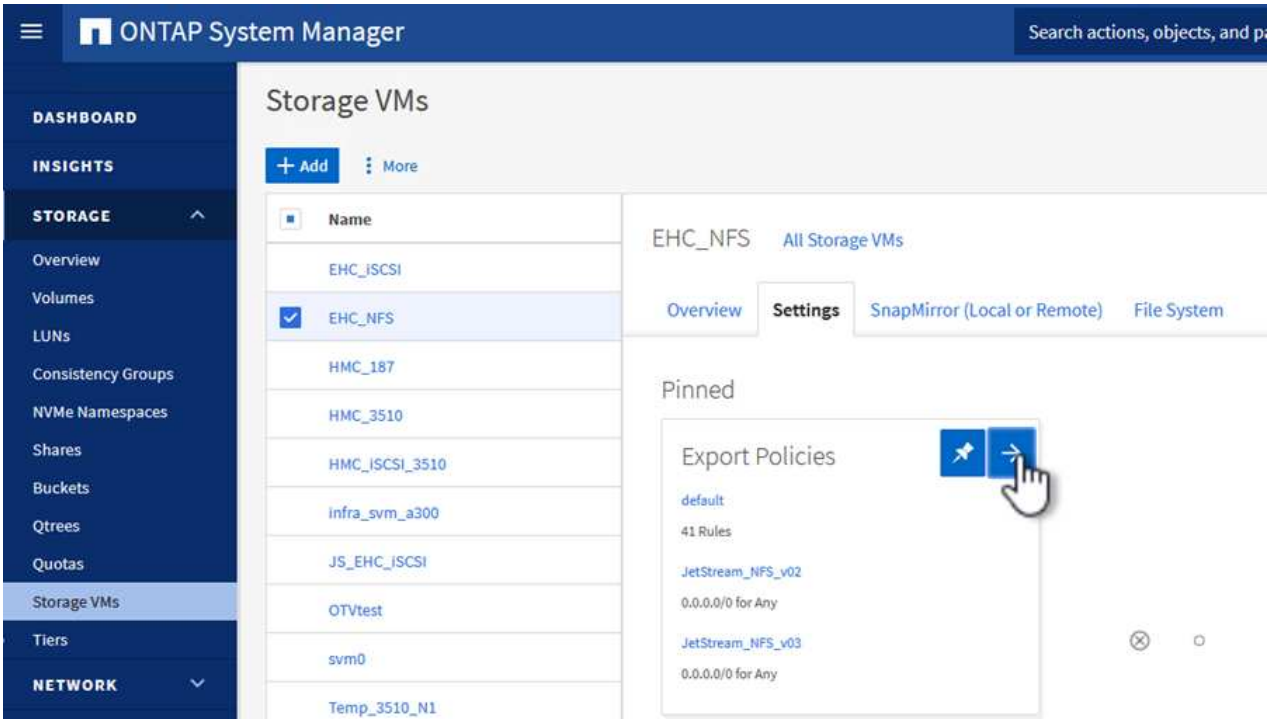
```
vmkping <IP Address>
```

VI 워크로드 도메인을 배포할 때 VCF는 NFS 서버에 대한 연결을 검증합니다. 이 작업은 NFS IP 주소와 함께 추가 vmkernel 어댑터를 추가하기 전에 ESXi 호스트의 관리 어댑터를 사용하여 수행됩니다. 따라서 검증을 진행할 수 있도록 1) 관리 네트워크가 NFS 서버로 라우팅 가능한지, 2) 관리 네트워크의 LIF가 NFS 데이터 저장소 볼륨을 호스팅하는 SVM에 추가되었는지 확인해야 합니다.

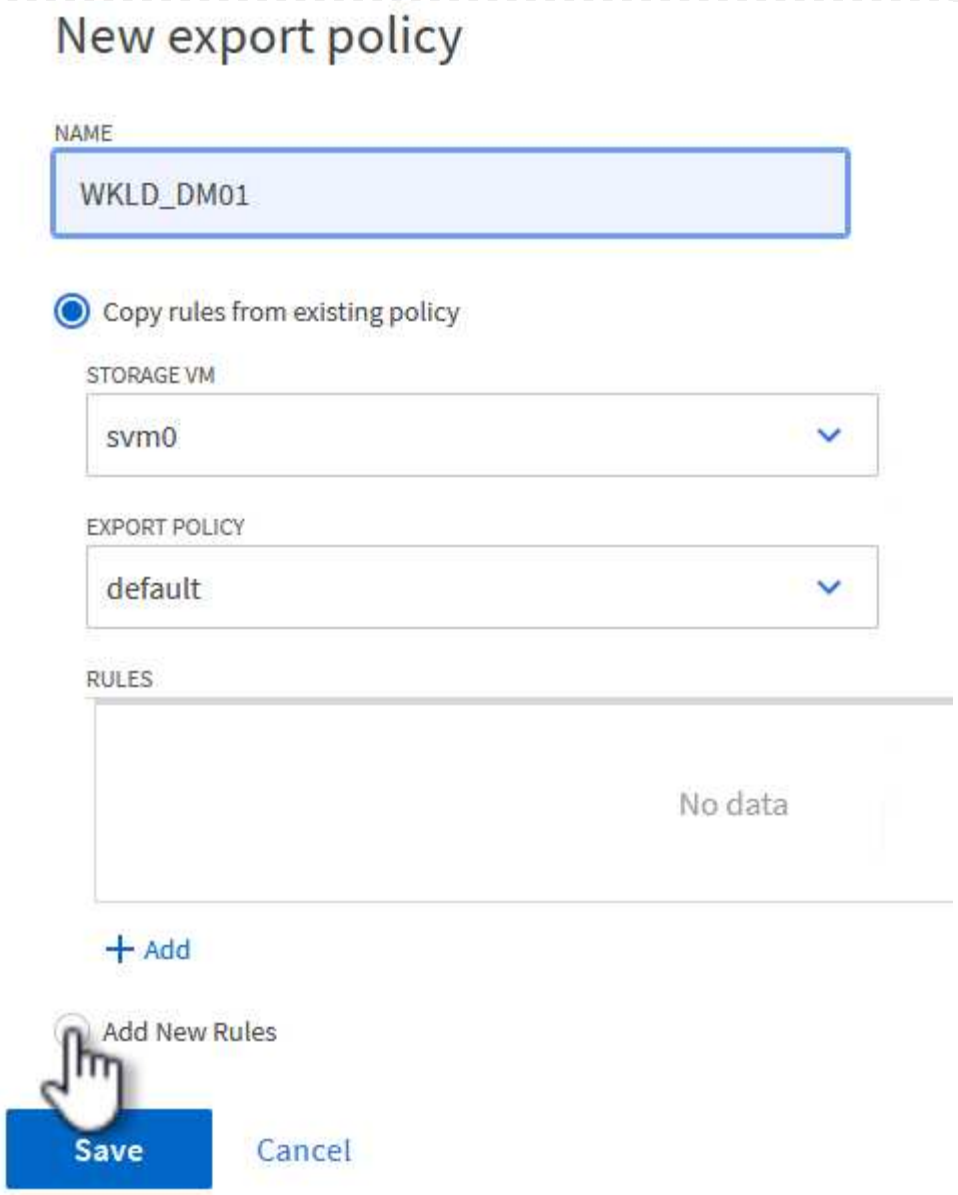
NFS 볼륨 공유를 위한 내보내기 정책 생성

ONTAP System Manager에서 내보내기 정책을 만들어 NFS 볼륨에 대한 액세스 제어를 정의합니다.

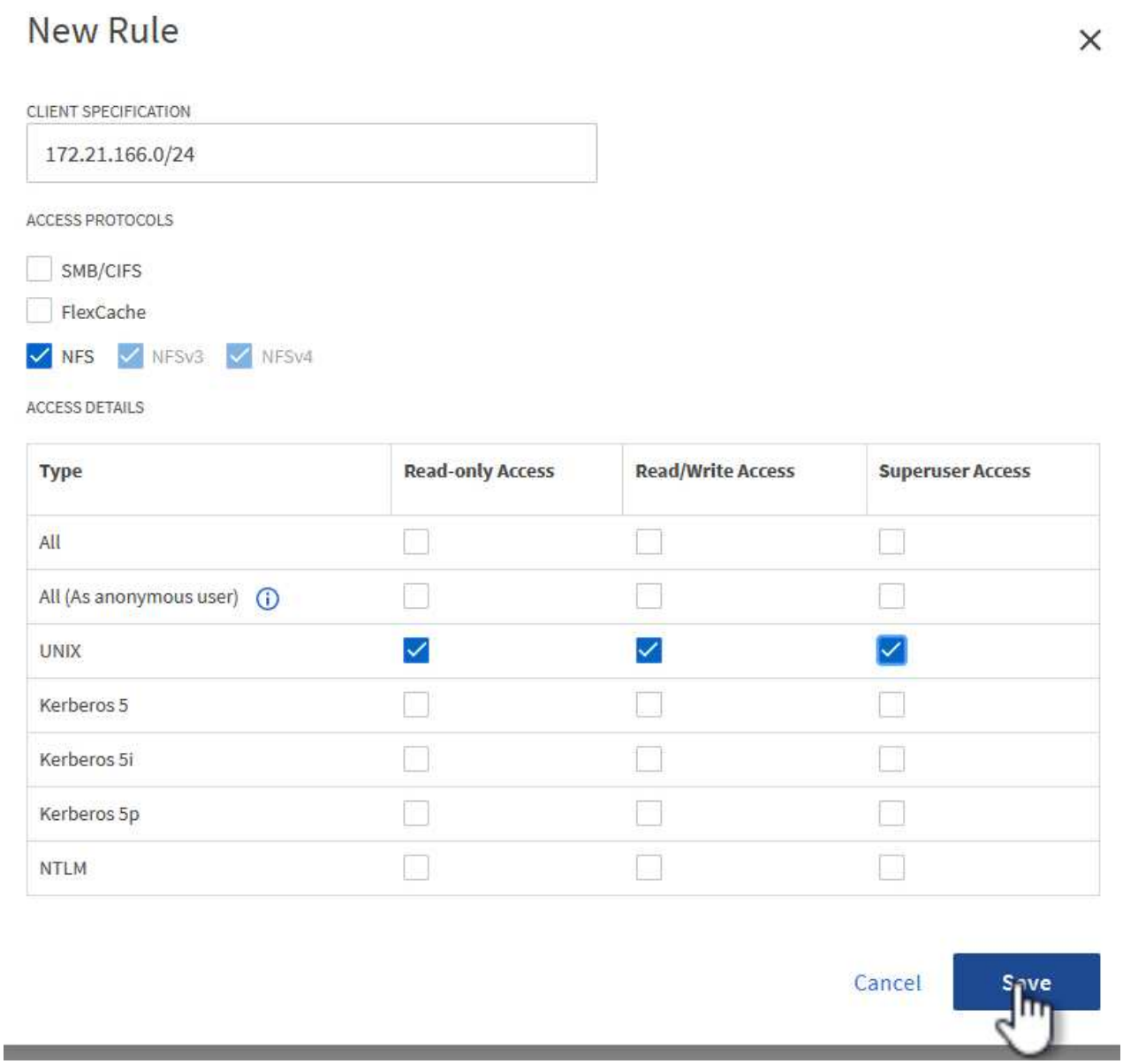
1. ONTAP 시스템 관리자에서 왼쪽 메뉴의 *스토리지 VM*을 클릭하고 목록에서 SVM을 선택합니다.
2. 설정 탭에서 *내보내기 정책*을 찾아 화살표를 클릭하여 액세스합니다.



3. 새 내보내기 정책 창에서 정책 이름을 추가하고, 새 규칙 추가 버튼을 클릭한 다음, **+**추가 버튼을 클릭하여 새 규칙을 추가합니다.



4. 규칙에 포함할 IP 주소, IP 주소 범위 또는 네트워크를 입력하세요. **SMB/Cifs** 및 * FlexCache* 상자의 선택을 해제하고 아래의 액세스 세부 정보를 선택하세요. ESXi 호스트에 액세스하려면 UNIX 상자를 선택하는 것으로 충분합니다.



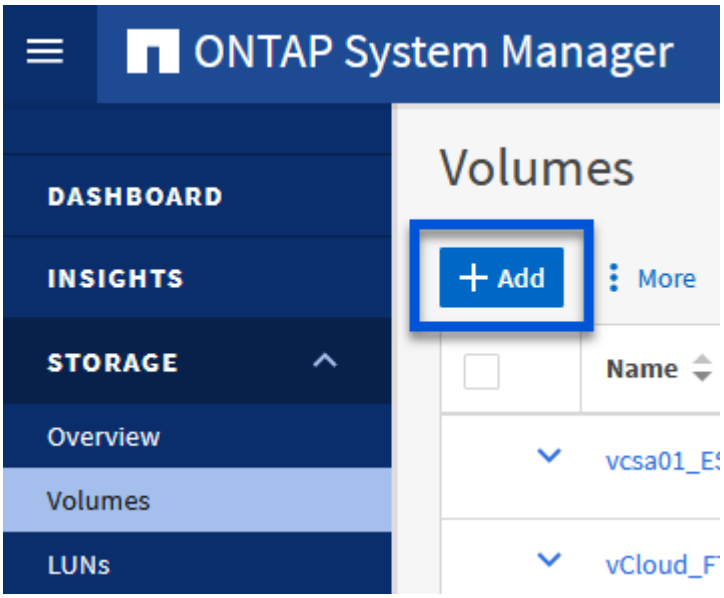
VI 워크로드 도메인을 배포할 때 VCF는 NFS 서버에 대한 연결을 검증합니다. 이 작업은 NFS IP 주소와 함께 추가 vmkernel 어댑터를 추가하기 전에 ESXi 호스트의 관리 어댑터를 사용하여 수행됩니다. 따라서 검증을 진행하기 위해서는 VCF 관리 네트워크가 수출 정책에 포함되어야 합니다.

5. 모든 규칙을 입력한 후 저장 버튼을 클릭하여 새 내보내기 정책을 저장합니다.
6. 또는 ONTAP CLI에서 내보내기 정책과 규칙을 만들 수 있습니다. ONTAP 설명서에서 내보내기 정책을 만들고 규칙을 추가하는 단계를 참조하세요.
   - ONTAP CLI를 사용하여"수출 정책 만들기" .
   - ONTAP CLI를 사용하여"내보내기 정책에 규칙 추가" .

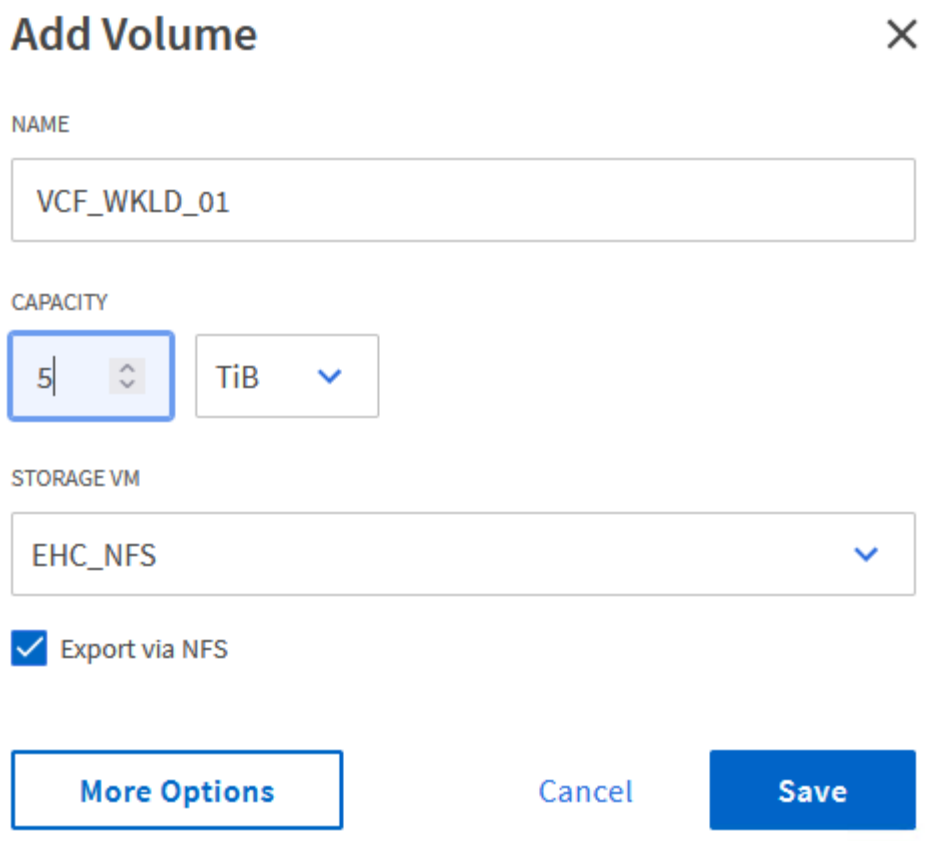
NFS 볼륨 생성

워크로드 도메인 배포에서 데이터 저장소로 사용할 ONTAP 스토리지 시스템에 NFS 볼륨을 만듭니다.

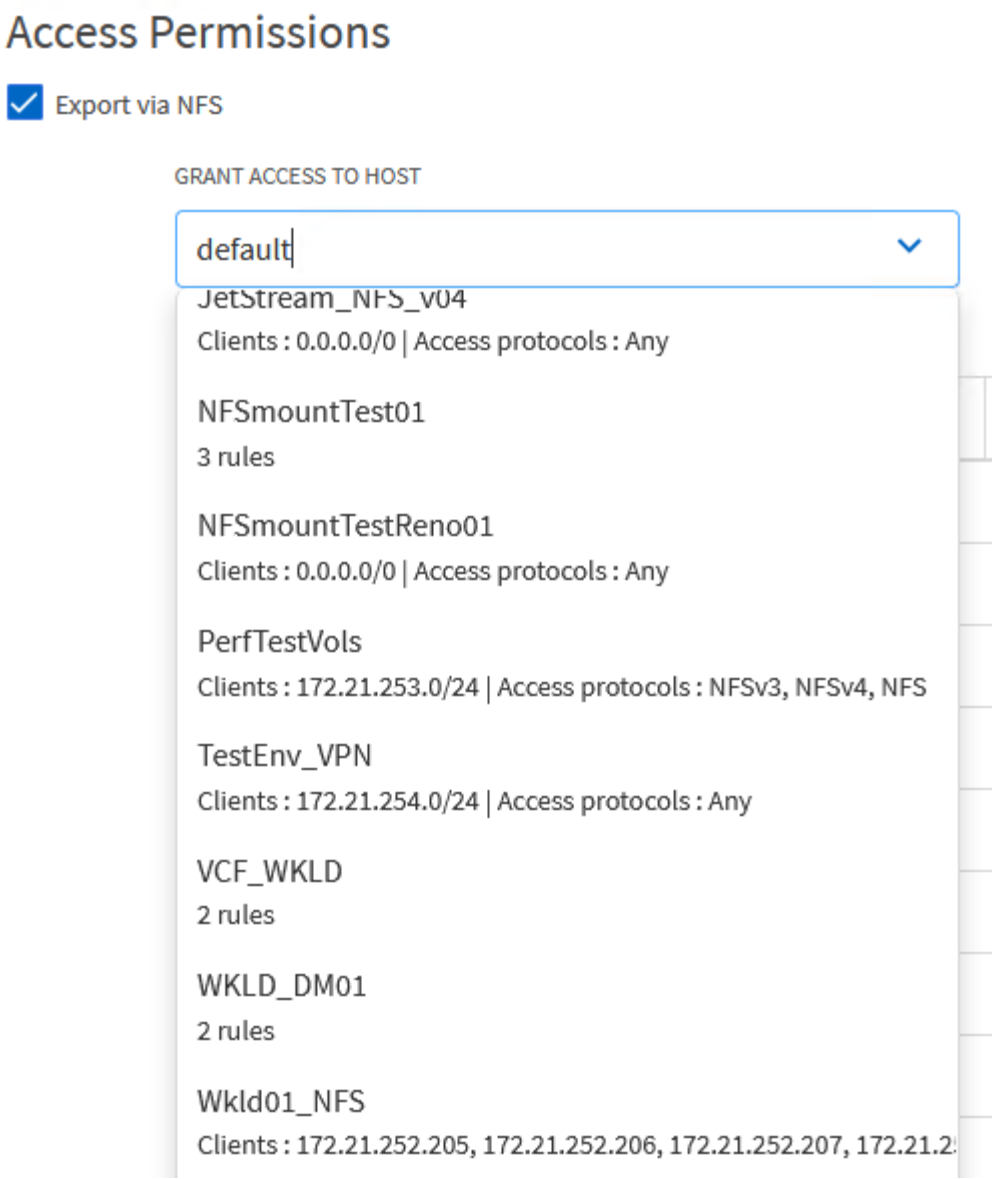
1. ONTAP 시스템 관리자의 왼쪽 메뉴에서 *저장소 > 볼륨*으로 이동한 다음 *+추가*를 클릭하여 새 볼륨을 만듭니다.



2. 볼륨의 이름을 추가하고, 원하는 용량을 입력하고, 볼륨을 호스팅할 스토리지 VM을 선택합니다. 계속하려면 *추가 옵션*을 클릭하세요.



3. 액세스 권한에서 VCF 관리 네트워크 또는 IP 주소와 NFS 서버와 NFS 트래픽의 검증에 사용될 NFS 네트워크 IP 주소가 포함된 내보내기 정책을 선택합니다.



+

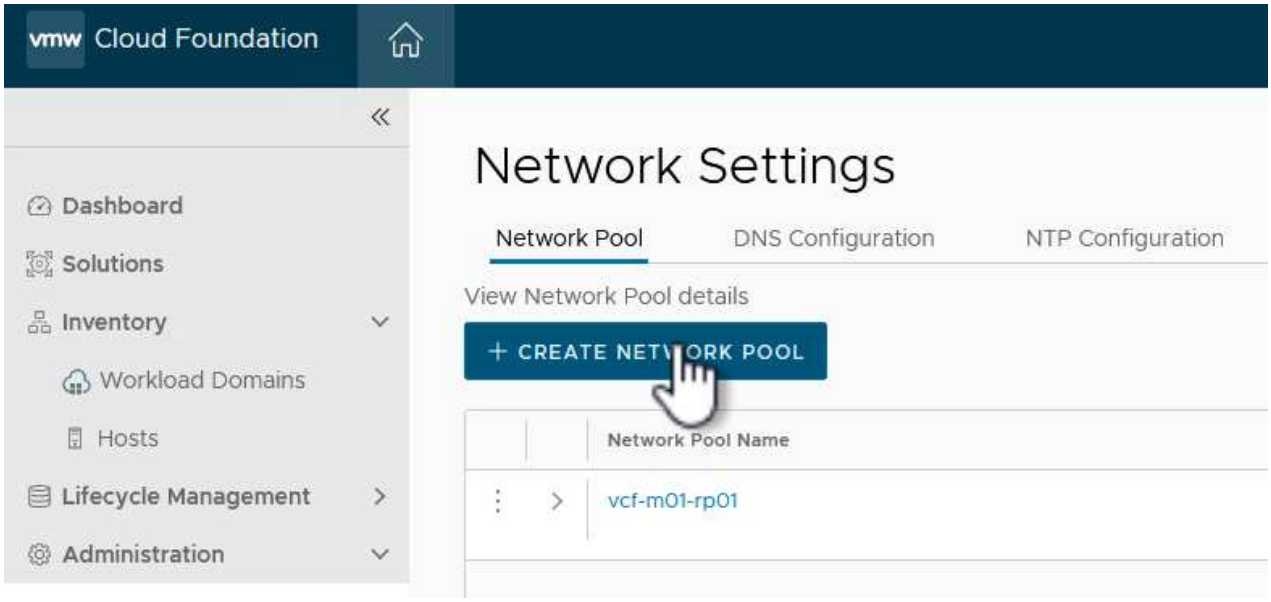
> VI 워크로드 도메인을 배포할 때 VCF는 NFS 서버에 대한 연결을 검증합니다. 이 작업은 NFS IP 주소와 함께 추가 vmkernel 어댑터를 추가하기 전에 ESXi 호스트의 관리 어댑터를 사용하여 수행됩니다. 따라서 검증을 진행할 수 있도록 1) 관리 네트워크가 NFS 서버로 라우팅 가능한지, 2) 관리 네트워크의 LIF가 NFS 데이터 저장소 볼륨을 호스팅하는 SVM에 추가되었는지 확인해야 합니다.

4. 또는 ONTAP 볼륨은 ONTAP CLI에서 생성할 수 있습니다. 자세한 내용은 다음을 참조하세요."lun 생성" ONTAP 명령 설명서의 명령입니다.

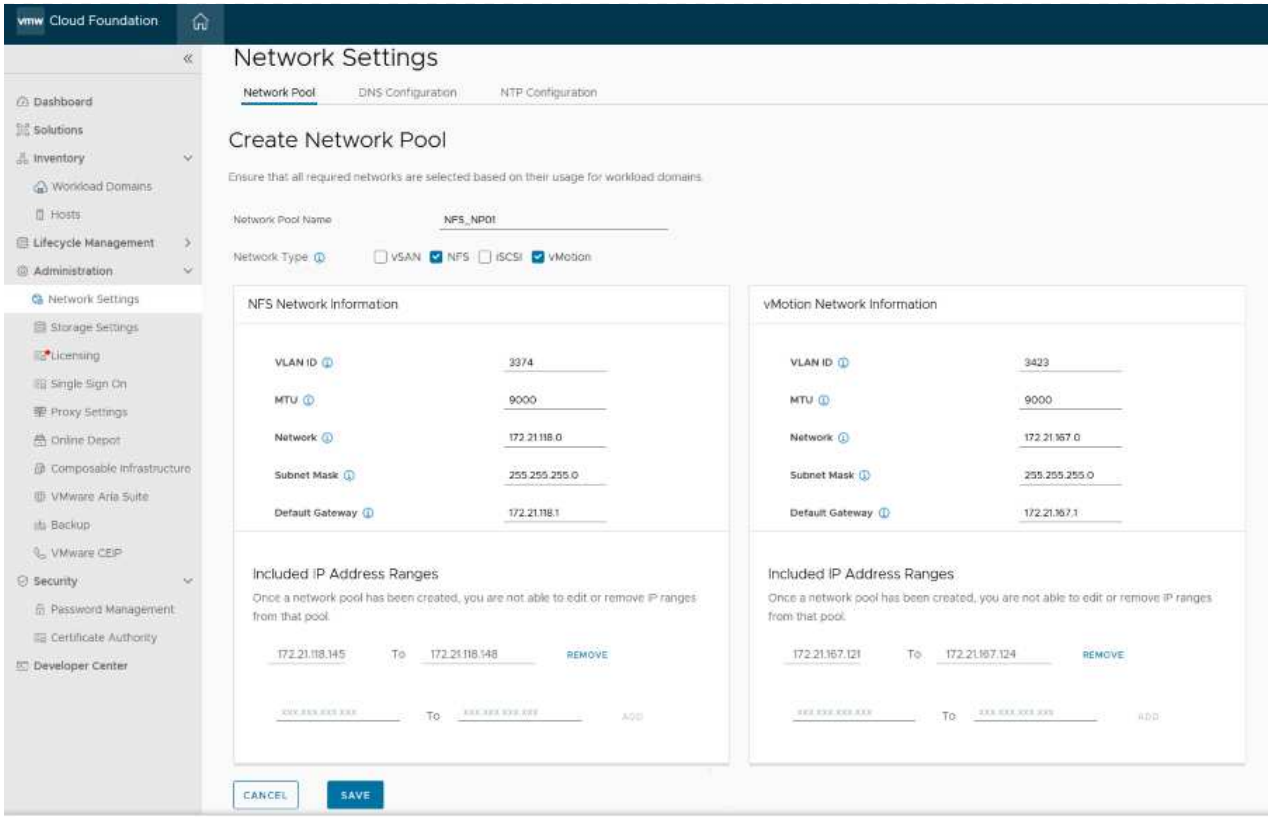
SDDC 관리자에서 네트워크 풀 생성

ESXi 호스트를 시운전하기 전에 SDDC 관리자에서 네트워크 풀을 생성해야 VI 워크로드 도메인에 배포할 준비가 됩니다. 네트워크 풀에는 NFS 서버와 통신하는 데 사용되는 VMkernel 어댑터에 대한 네트워크 정보와 IP 주소 범위가 포함되어야 합니다.

1. SDDC 관리자 웹 인터페이스에서 왼쪽 메뉴의 네트워크 설정*으로 이동한 다음 *+ 네트워크 풀 만들기 버튼을 클릭합니다.



2. 네트워크 풀의 이름을 입력하고, NFS에 대한 확인란을 선택한 다음 모든 네트워킹 세부 정보를 입력합니다. vMotion 네트워크 정보에 대해서도 이 과정을 반복합니다.



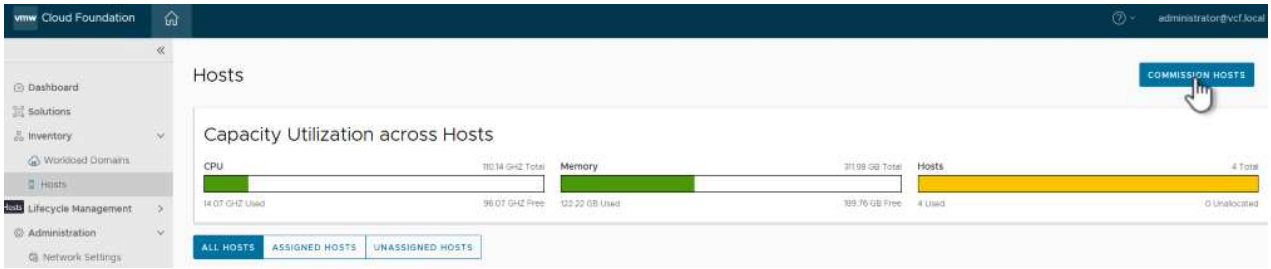
3. 저장 버튼을 클릭하면 네트워크 풀 생성이 완료됩니다.

위원회 호스트

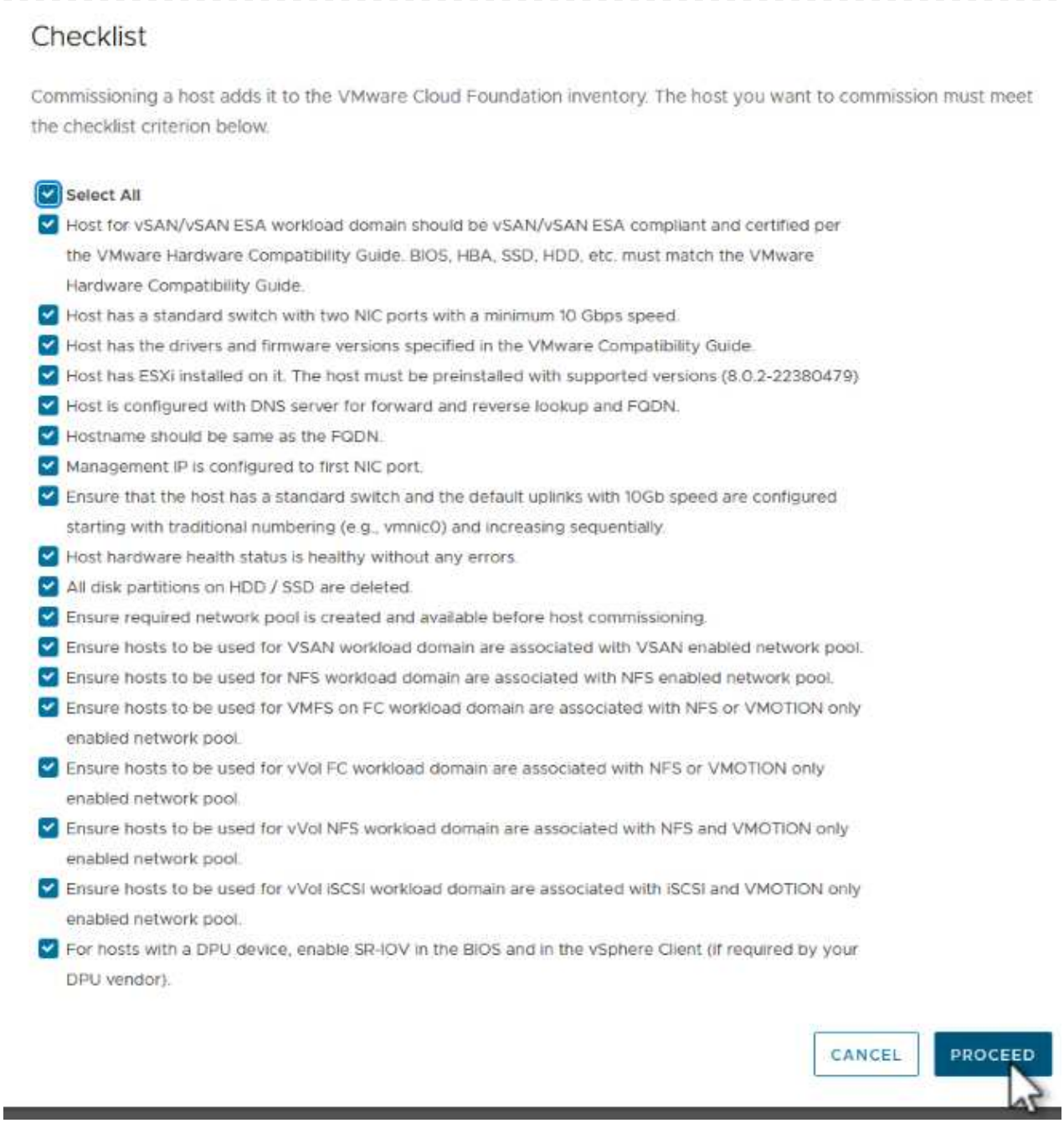
ESXi 호스트를 워크로드 도메인으로 배포하려면 먼저 SDDC 관리자 인벤토리에 추가해야 합니다. 여기에는 필요한 정보를 제공하고, 검증을 통과하고, 시운전 절차를 시작하는 것이 포함됩니다.

자세한 내용은 다음을 참조하세요."위원회 호스트" VCF 관리 가이드에서.

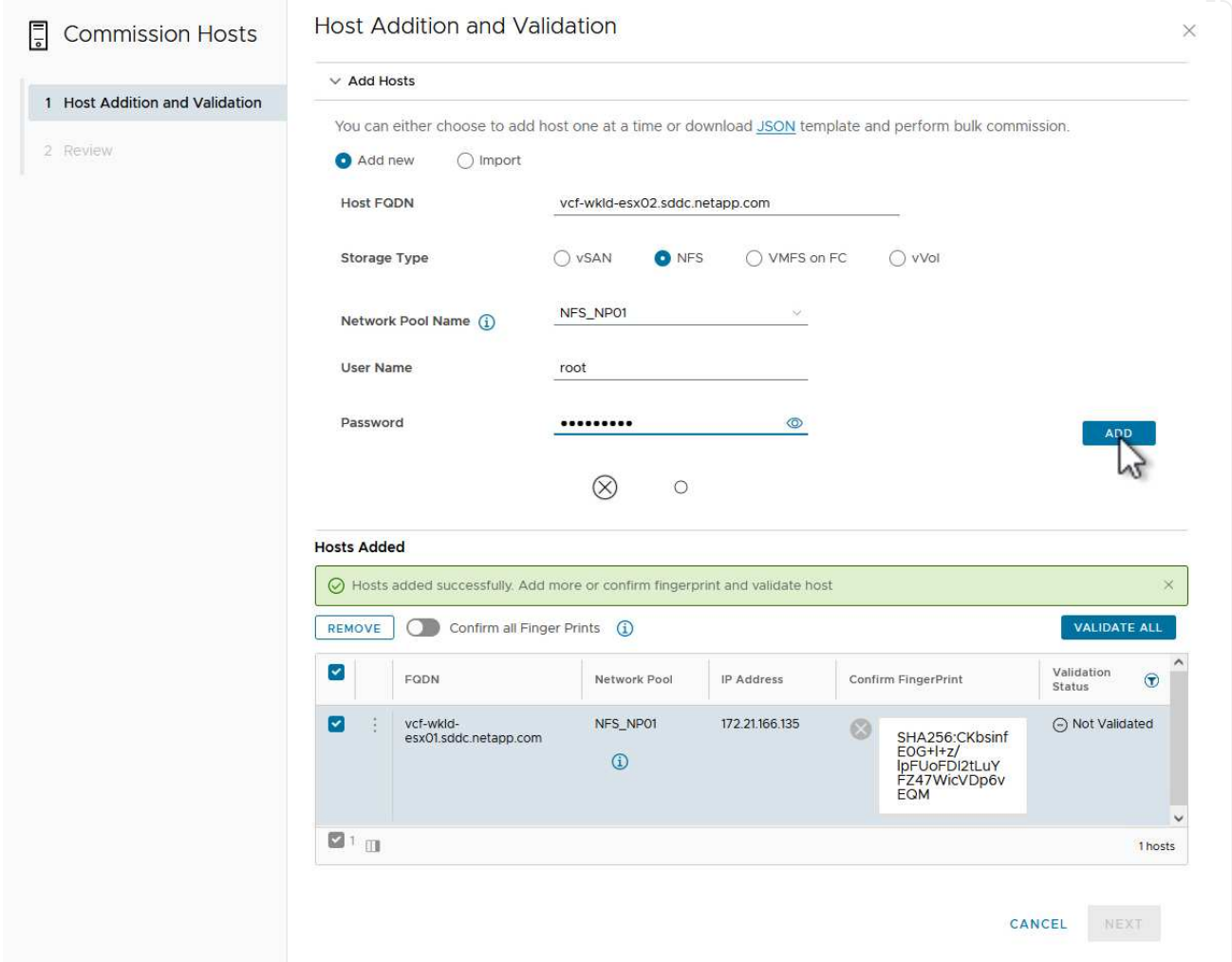
1. SDDC 관리자 인터페이스에서 왼쪽 메뉴의 호스트*로 이동한 다음 *호스트 위임 버튼을 클릭합니다.



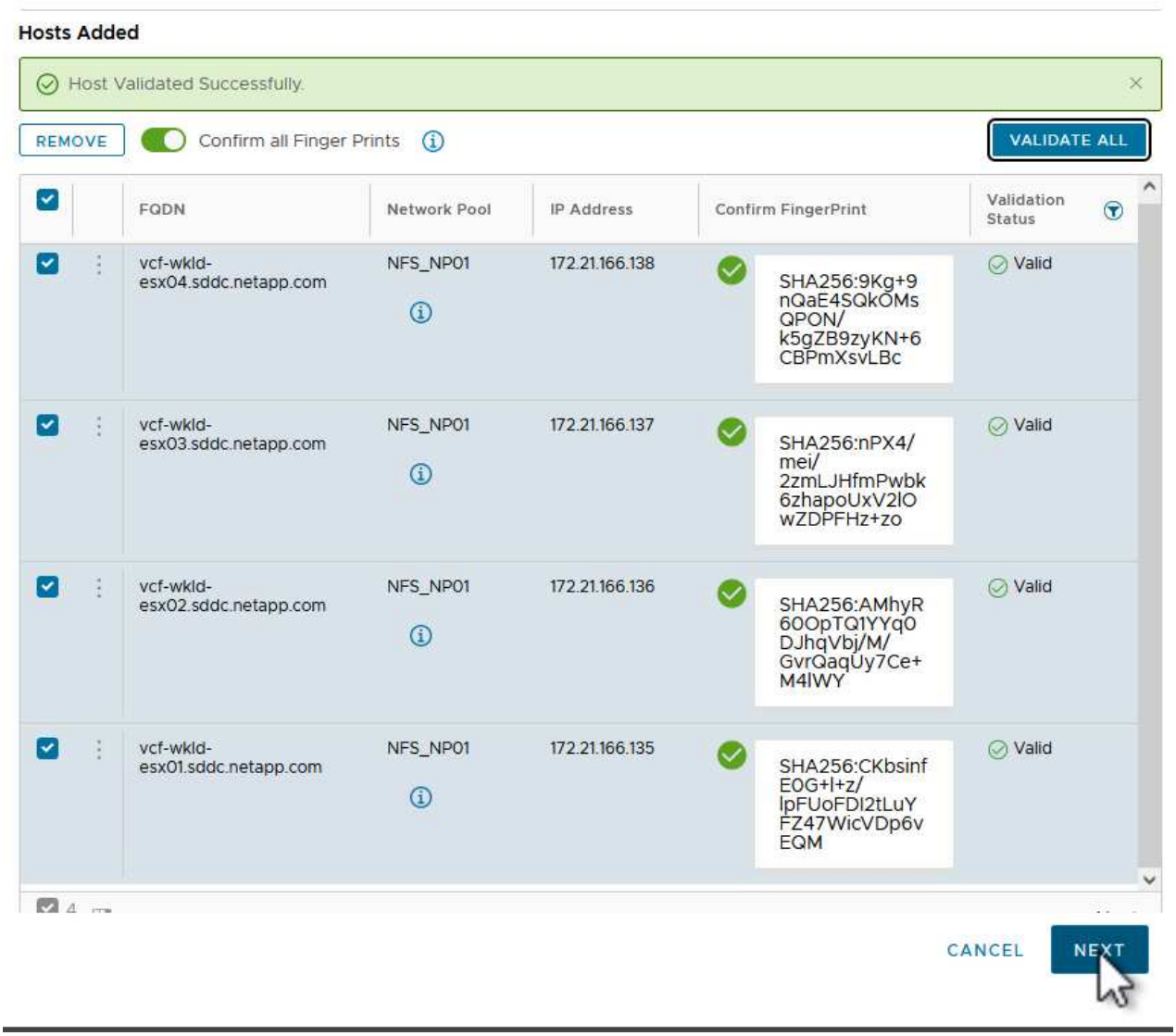
2. 첫 번째 페이지는 필수 체크리스트입니다. 모든 필수 조건을 다시 한 번 확인하고 모든 확인란을 선택하여 계속 진행하세요.



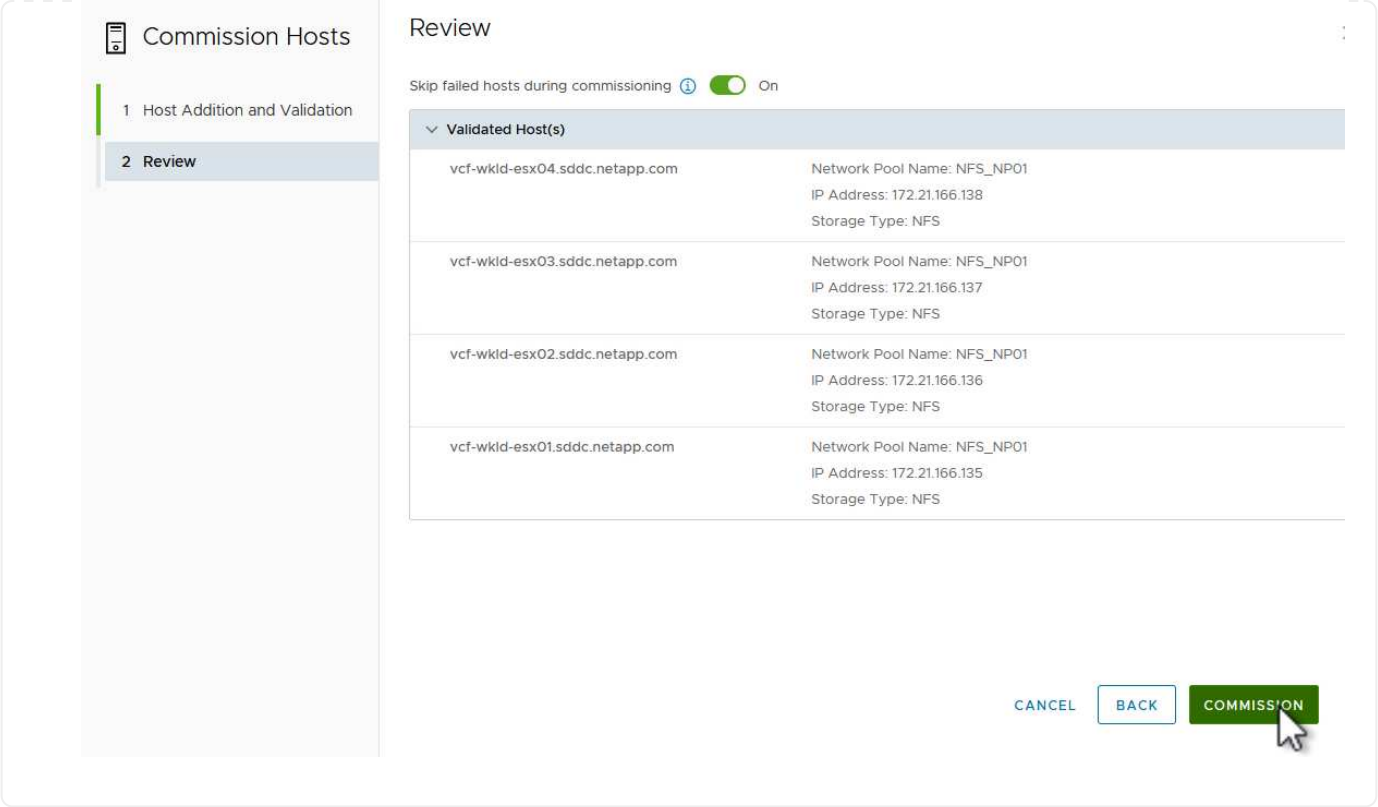
3. 호스트 추가 및 검증 창에서 호스트 **FQDN**, 스토리지 유형, 워크로드 도메인에 사용될 vMotion 및 NFS 스토리지 IP 주소가 포함된 네트워크 풀 이름, ESXi 호스트에 액세스하기 위한 자격 증명을 입력합니다. * 추가*를 클릭하여 검증할 호스트 그룹에 호스트를 추가합니다.



4. 검증할 모든 호스트를 추가한 후, 모두 검증 버튼을 클릭하여 계속 진행하세요.
5. 모든 호스트가 검증되었다고 가정하고 계속하려면 *다음*을 클릭하세요.



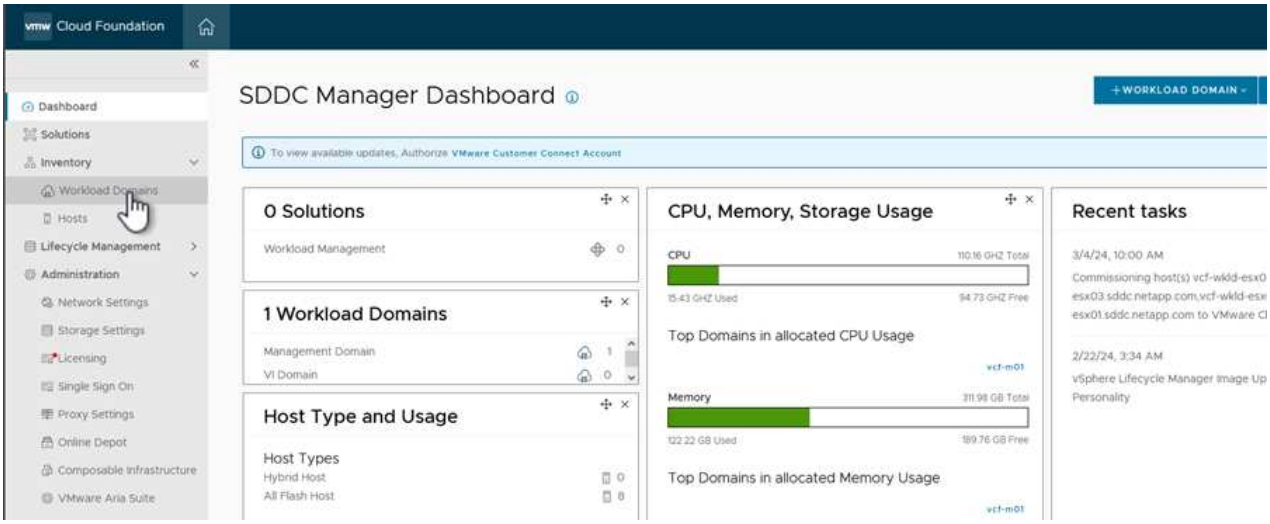
6. 위임할 호스트 목록을 검토하고 위임 버튼을 클릭하여 프로세스를 시작하세요. SDDC 관리자의 작업 창에서 시운전 프로세스를 모니터링합니다.


Commission Hosts
1 Host Addition and Validation
2 Review
Review
Skip failed hosts during commissioning
On
Validated Host(s)
vcf-wkld-esx04.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.138
Storage Type: NFS
vcf-wkld-esx03.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.137
Storage Type: NFS
vcf-wkld-esx02.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.136
Storage Type: NFS
vcf-wkld-esx01.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.135
Storage Type: NFS
CANCEL
BACK
COMMISSION

VI 워크로드 도메인 배포는 VCF 클라우드 관리자 인터페이스를 사용하여 수행됩니다. 여기에서는 저장소 구성과 관련된 단계만 설명합니다.

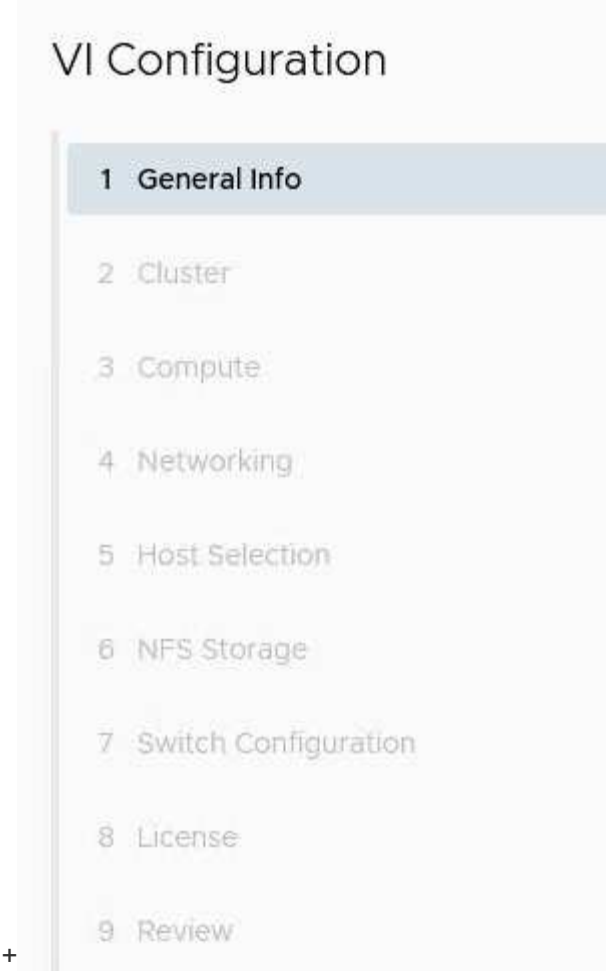
VI 워크로드 도메인 배포에 대한 단계별 지침은 다음을 참조하세요."SDDC 관리자 UI를 사용하여 VI 워크로드 도메인 배포" .

1. SDDC 관리자 대시보드에서 오른쪽 상단 모서리에 있는 *+ 워크로드 도메인*을 클릭하여 새로운 워크로드 도메인을 만듭니다.



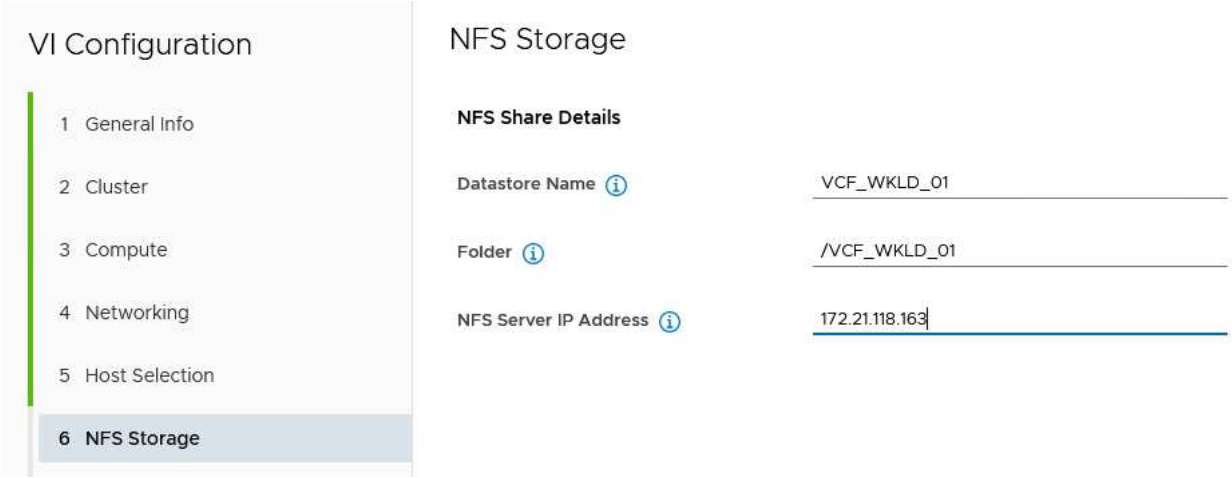
2. VI 구성 마법사에서 필요에 따라 일반 정보, 클러스터, 컴퓨팅, 네트워킹* 및 호스트 선택 섹션을 작성합니다.

VI 구성 마법사에 필요한 정보를 채우는 방법에 대한 정보는 다음을 참조하세요."SDDC 관리자 UI를 사용하여 VI 워크로드 도메인 배포" .

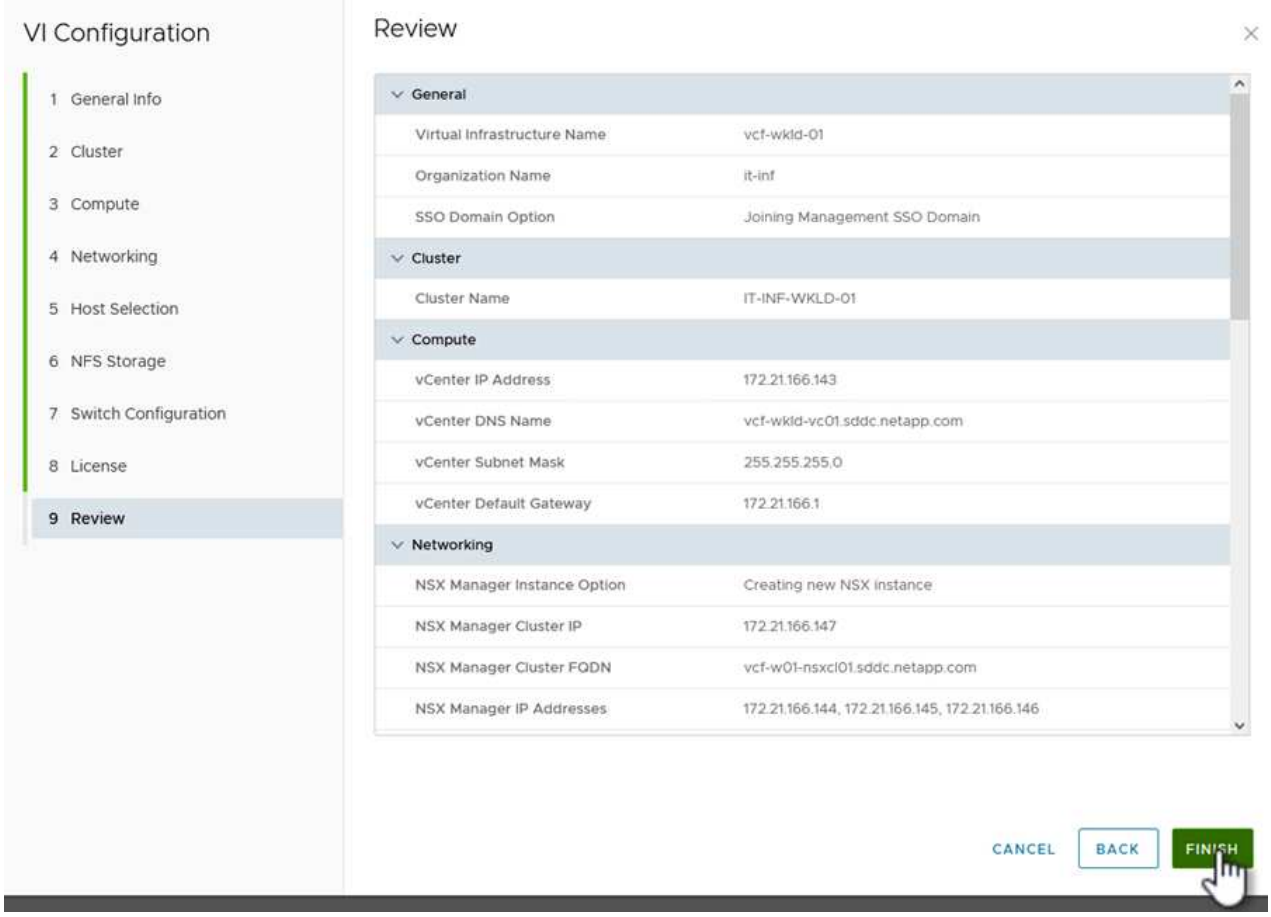


+

1. NFS 저장소 섹션에서 데이터 저장소 이름, NFS 볼륨의 폴더 마운트 지점, ONTAP NFS 저장소 VM LIF의 IP 주소를 입력합니다.



2. VI 구성 마법사에서 스위치 구성 및 라이선스 단계를 완료한 다음 *마침*을 클릭하여 워크로드 도메인 생성 프로세스를 시작합니다.



3. 프로세스를 모니터링하고 프로세스 중에 발생하는 모든 검증 문제를 해결합니다.

VMware VAAI용 NetApp NFS 플러그인 설치

VMware VAAI용 NetApp NFS 플러그인은 ESXi 호스트에 설치된 VMware Virtual Disk Libraries를 통합하고 더 빠르게 완료되는 고성능 복제 작업을 제공합니다. 이는 VMware vSphere와 함께 ONTAP 스토리지 시스템을 사용할 때 권장되는 절차입니다.

VMware VAAI용 NetApp NFS 플러그인을 배포하는 방법에 대한 단계별 지침은 다음 지침을 참조하세요 ."VMware VAAI용 NetApp NFS 플러그인 설치" .

이 솔루션에 대한 비디오 데모

VCF 워크로드 도메인의 주 스토리지로서의 NFS 데이터 저장소

추가 정보

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

보충 스토리지로 VCF 확장

보조 스토리지를 사용하여 VCF 환경의 스토리지 확장에 대해 알아보세요.

VMware Cloud Foundation(VCF)은 VCF 관리 도메인과 가상 인프라(VI) 워크로드 도메인의 스토리지를 확장하기 위한 광범위한 보조 스토리지 옵션을 지원합니다.

VMware vSphere용 NetApp ONTAP 도구는 NetApp 스토리지를 VCF 환경에 원활하게 통합하여 이러한 확장을 위한 효율적인 솔루션을 제공합니다. ONTAP 도구는 데이터스토어의 설정 및 관리를 간소화하여 관리자가 vSphere Client에서 직접 스토리지를 프로비저닝하고 관리할 수 있도록 합니다. ONTAP은 스냅샷, 복제, 데이터 보호와 같은 고급 기능을 제공하여 VCF 환경 내에서 스토리지 성능, 효율성, 확장성을 향상시킵니다.

VCF 환경을 확장하기 위한 기술적 세부 사항은 다음 솔루션을 참조하세요.

- "iSCSI를 사용한 관리 도메인"
- "FC를 사용한 관리 도메인"
- "vVols 를 사용한 가상 인프라 워크로드 도메인(iSCSI)"
- "vVols (NFS)를 사용한 가상 인프라 워크로드 도메인"
- "NVMe/TCP를 사용한 가상 인프라 워크로드 도메인"
- "FC를 사용한 가상 인프라 워크로드 도메인"

ONTAP tools for VMware vSphere 사용하여 관리 도메인의 보조 스토리지로 iSCSI 데이터 저장소 추가

이 사용 사례에서는 VMware Cloud Foundation(VCF) 관리 도메인의 보조 스토리지로 iSCSI 데이터스토어를 추가하는 절차를 설명합니다. 이 절차에서는 iSCSI를 위한 논리적 인터페이스(LIF)를 갖춘 스토리지 가상 머신(SVM) 설정, ESXi 호스트에서 iSCSI 네트워킹 구성, VMware vSphere용 ONTAP 도구 배포, VMFS 데이터 저장소 생성에 대한 내용을 요약합니다.

iSCSI의 이점

고성능: 빠르고 효율적인 데이터 전송 속도와 낮은 지연 시간을 제공하는 고성능을 제공합니다. 까다로운 엔터프라이즈 애플리케이션과 가상화 환경에 이상적입니다.

관리 용이성: 익숙한 IP 기반 도구와 프로토콜을 사용하여 스토리지 관리를 간소화합니다.

비용 효율성: 기존 이더넷 인프라를 활용하여 특수 하드웨어의 필요성을 줄이고 조직이 안정적이고 확장 가능한 스토리지 솔루션을 구축할 수 있도록 합니다.

NetApp 스토리지 시스템에서 iSCSI를 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요. "iSCSI를 사용한 SAN 프로비저닝" .

시나리오 개요

이 시나리오에서는 다음과 같은 상위 수준 단계를 다룹니다.

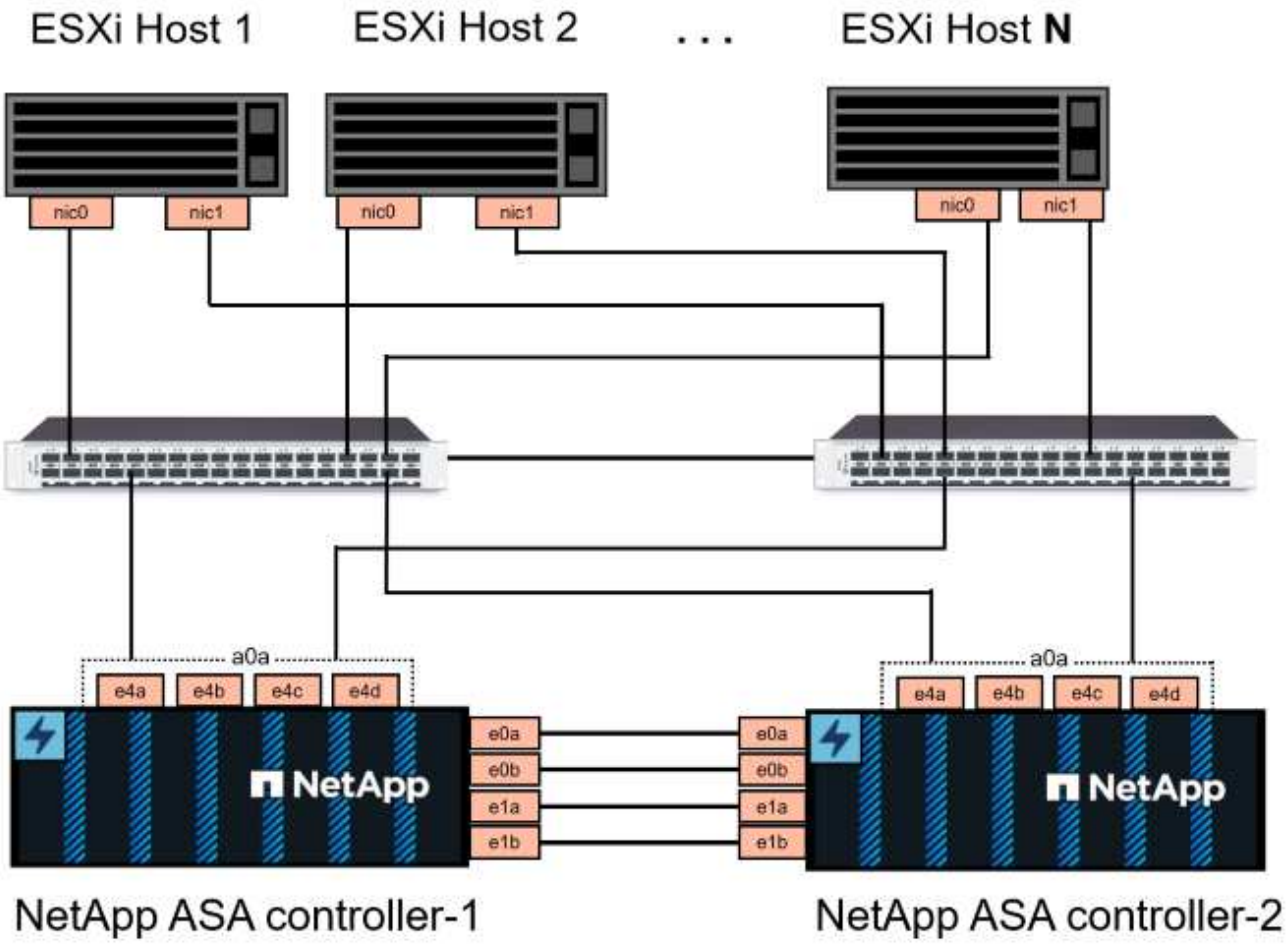
- iSCSI 트래픽을 위한 논리 인터페이스(LIF)가 있는 스토리지 가상 머신(SVM)을 만듭니다.
- VCF 관리 도메인에서 iSCSI 네트워크에 대한 분산 포트 그룹을 만듭니다.
- VCF 관리 도메인의 ESXi 호스트에서 iSCSI용 vmkernel 어댑터를 생성합니다.
- VCF 관리 도메인에 ONTAP 도구를 배포합니다.
- VCF 관리 도메인에 새로운 VMFS 데이터 저장소를 만듭니다.

필수 조건

이 시나리오에는 다음과 같은 구성 요소와 구성이 필요합니다.

- 스토리지 트래픽에 전용된 이더넷 스위치의 물리적 데이터 포트가 있는 ONTAP AFF 또는 ASA 스토리지 시스템입니다.
- VCF 관리 도메인 배포가 완료되었으며 vSphere 클라이언트에 액세스할 수 있습니다.

NetApp iSCSI에 대해 완전 중복 네트워크 설계를 권장합니다. 다음 다이어그램은 스토리지 시스템, 스위치, 네트워크 어댑터 및 호스트 시스템에 대한 장애 내구성을 제공하는 중복 구성의 예를 보여줍니다. NetApp 을 참조하세요"SAN 구성 참조" 추가 정보를 원하시면.



다중 경로 지정 및 여러 경로에 걸친 장애 조치의 경우 NetApp iSCSI 구성의 모든 SVM에 대해 별도의 이더넷 네트워크에 스토리지 노드당 최소 두 개의 LIF를 두는 것을 권장합니다.

이 문서에서는 새로운 SVM을 생성하고 iSCSI 트래픽에 대한 여러 LIF를 생성하기 위해 IP 주소 정보를 지정하는 프로세스를 보여줍니다. 기존 SVM에 새로운 LIF를 추가하려면 다음을 참조하세요."LIF(네트워크 인터페이스) 생성" .

VMware에서 VMFS iSCSI 데이터 저장소를 사용하는 것에 대한 추가 정보는 다음을 참조하세요."vSphere VMFS 데이터스토어 - ONTAP 사용한 iSCSI 스토리지 백엔드" .

> 동일한 IP 네트워크에 여러 VMkernel 어댑터가 구성된 상황에서는 ESXi 호스트에서 소프트웨어 iSCSI 포트 바인딩을 사용하여 어댑터 전체에 걸친 부하 분산이 이루어지도록 하는 것이 좋습니다. KB 문서를 참조하세요"ESX/ESXi에서 소프트웨어 iSCSI 포트 바인딩을 사용하기 위한 고려 사항(2038869)" .

배포 단계

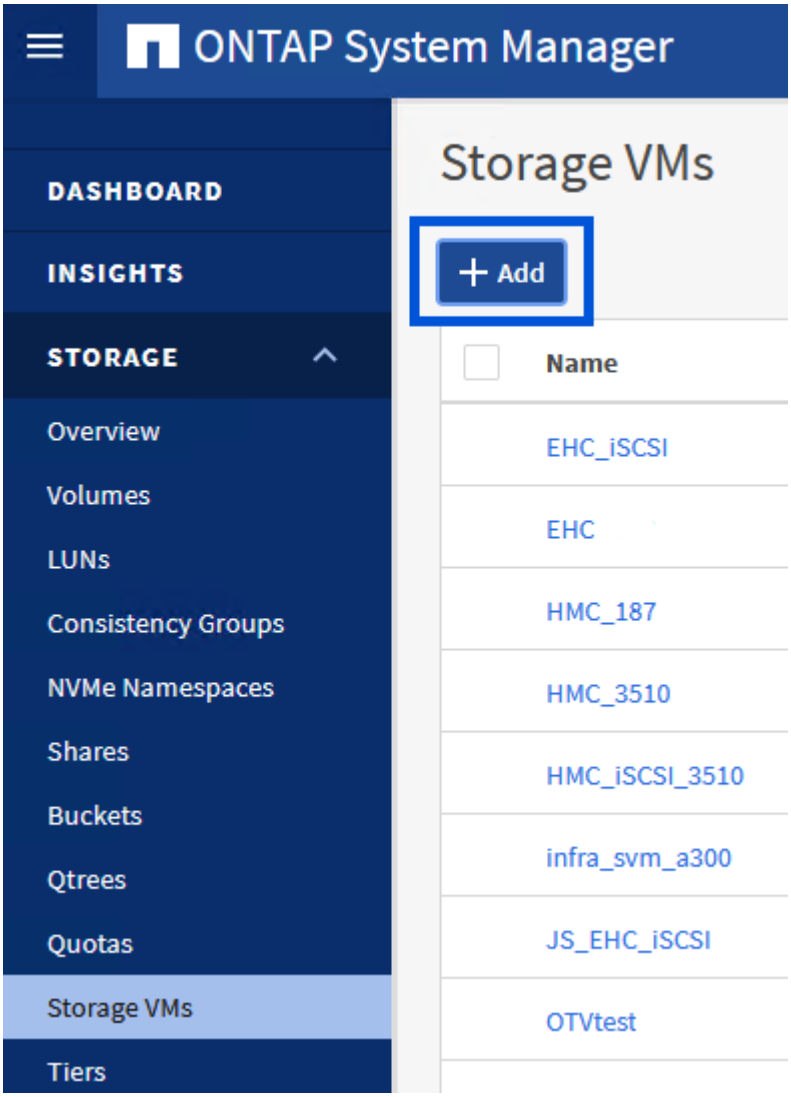
ONTAP 도구를 배포하고 이를 사용하여 VCF 관리 도메인에 VMFS 데이터 저장소를 생성하려면 다음 단계를 완료하세요.

ONTAP 스토리지 시스템에 **SVM** 및 **LIF** 생성

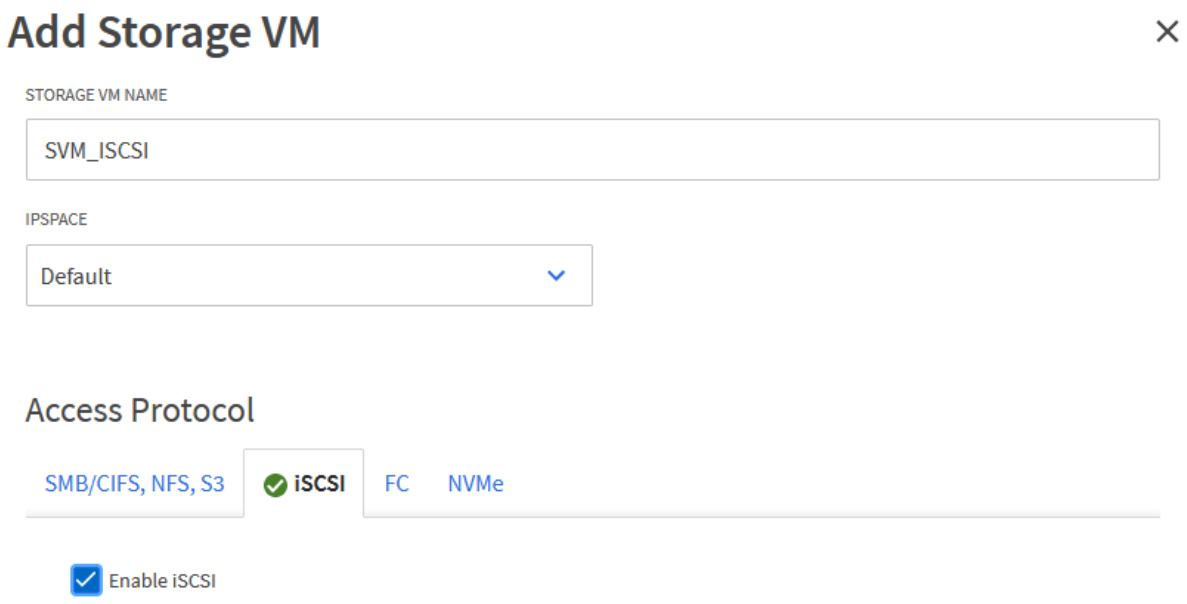
다음 단계는 ONTAP 시스템 관리자에서 수행됩니다.

iSCSI 트래픽을 위한 여러 LIF와 함께 SVM을 생성하려면 다음 단계를 완료하세요.

1. ONTAP System Manager에서 왼쪽 메뉴의 *Storage VMs*로 이동한 다음 *+ 추가*를 클릭하여 시작합니다.

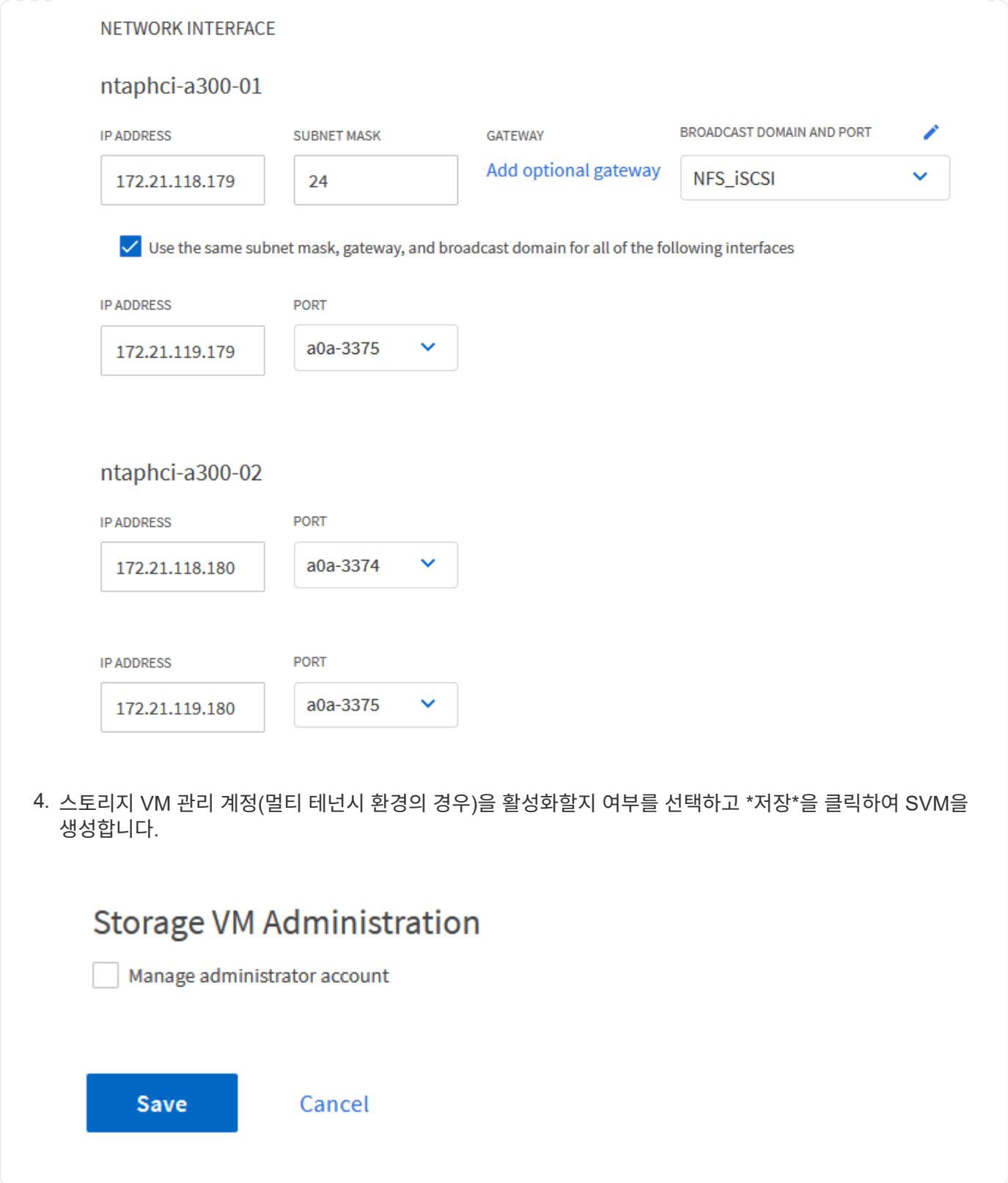


2. 스토리지 **VM** 추가 마법사에서 SVM의 이름*을 입력하고, ***IP** 공간*을 선택한 다음, *액세스 프로토콜*에서 ***iSCSI** 탭을 클릭하고 **iSCSI** 사용 확인란을 선택합니다.



3. 네트워크 인터페이스 섹션에 첫 번째 LIF에 대한 **IP** 주소, 서브넷 마스크, *브로드캐스트 도메인 및 포트*를 입력합니다. 이후 LIF의 경우 확인란을 활성화하여 나머지 모든 LIF에서 공통 설정을 사용하거나 별도의 설정을 사용할 수 있습니다.

> 다중 경로 지정 및 여러 경로에 걸친 장애 조치의 경우 NetApp iSCSI 구성의 모든 SVM에 대해 별도의 이더넷 네트워크에 스토리지 노드당 최소 두 개의 LIF를 두는 것을 권장합니다.



4. 스토리지 VM 관리 계정(멀티 테넌시 환경의 경우)을 활성화할지 여부를 선택하고 *저장*을 클릭하여 SVM을 생성합니다.

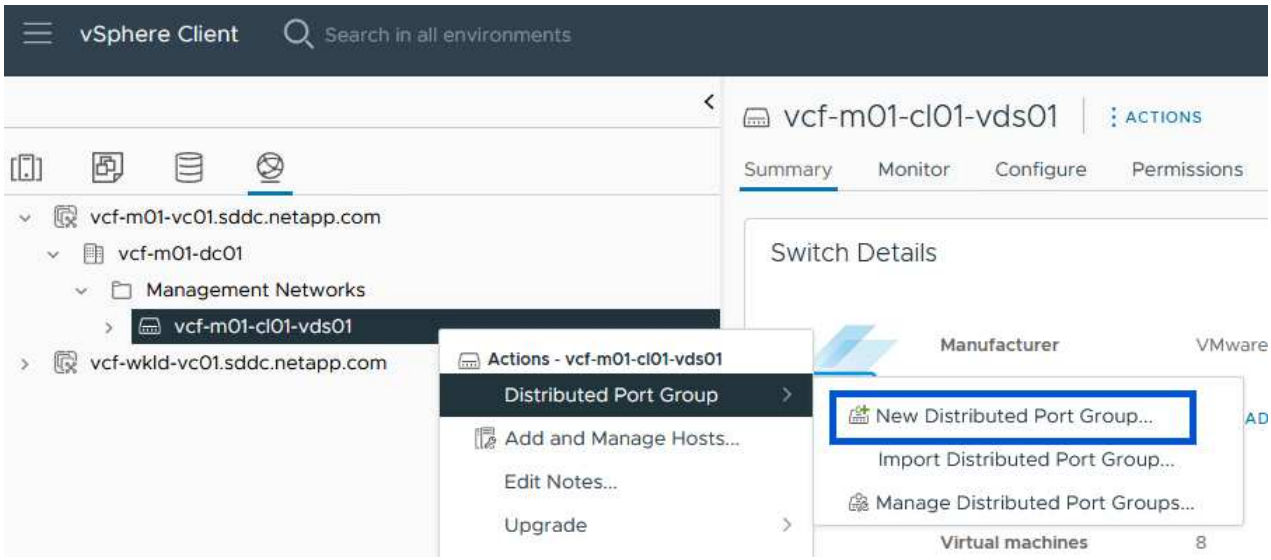
ESXi 호스트에서 **iSCSI**에 대한 네트워킹 설정

다음 단계는 vSphere 클라이언트를 사용하여 VCF 관리 도메인 클러스터에서 수행됩니다.

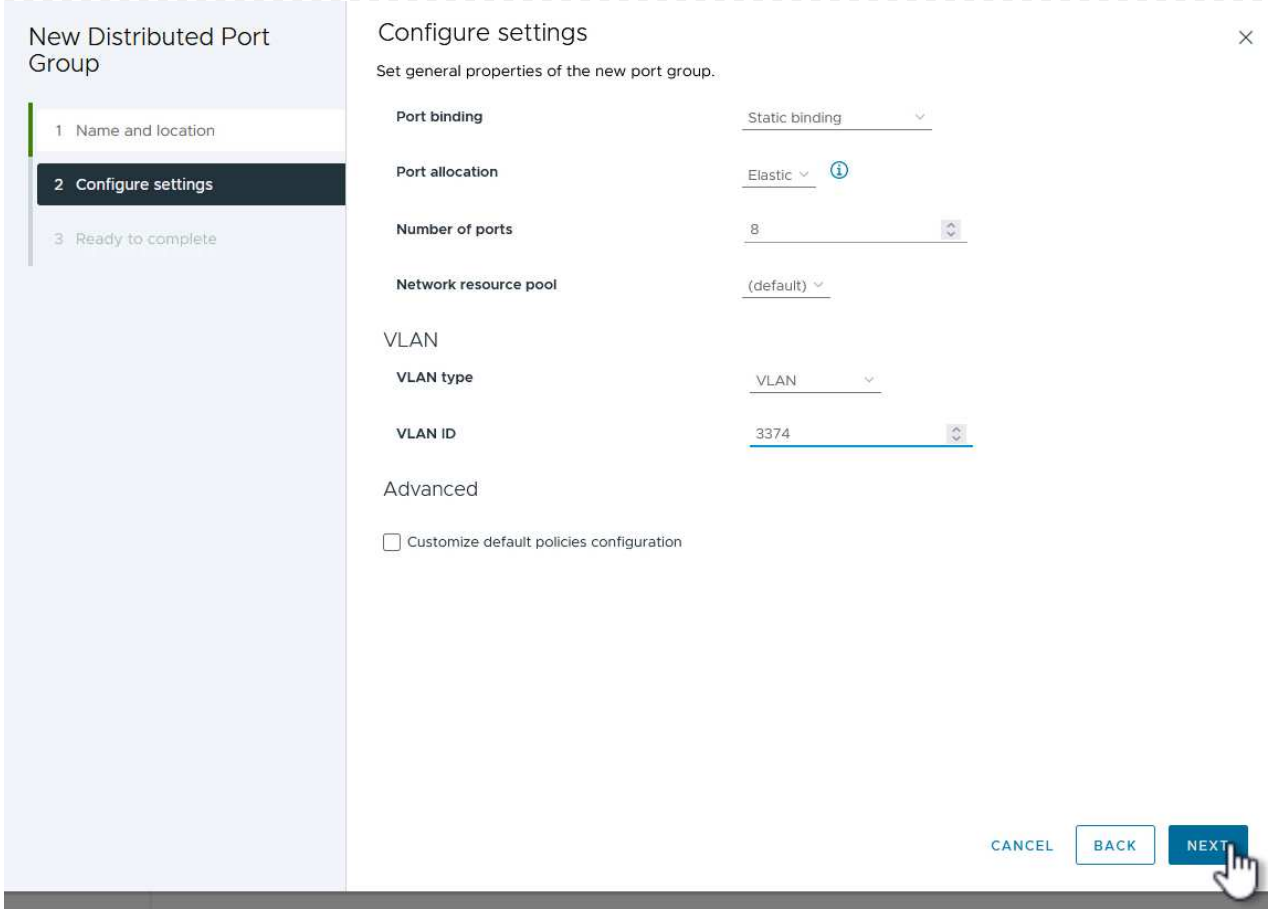
iSCSI 트래픽을 위한 분산 포트 그룹 생성

각 iSCSI 네트워크에 대한 새로운 분산 포트 그룹을 생성하려면 다음을 완료하세요.

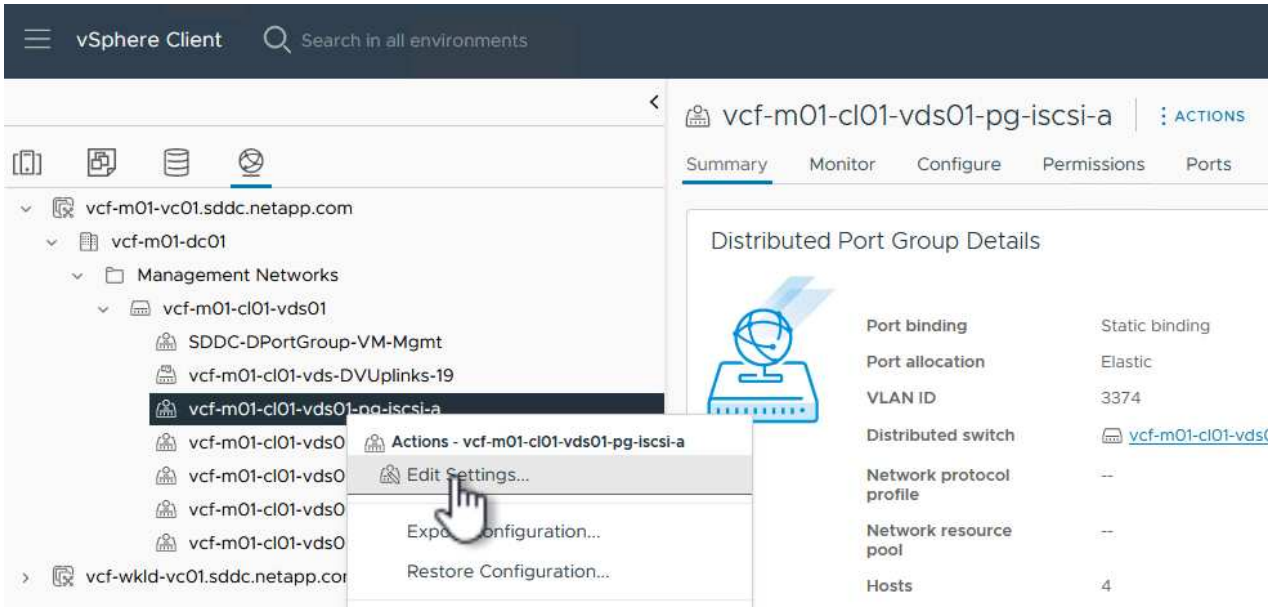
1. 관리 도메인 클러스터의 vSphere 클라이언트에서 *인벤토리 > 네트워킹*으로 이동합니다. 기존 분산 스위치로 이동하여 *새 분산 포트 그룹…*을 만드는 작업을 선택합니다.



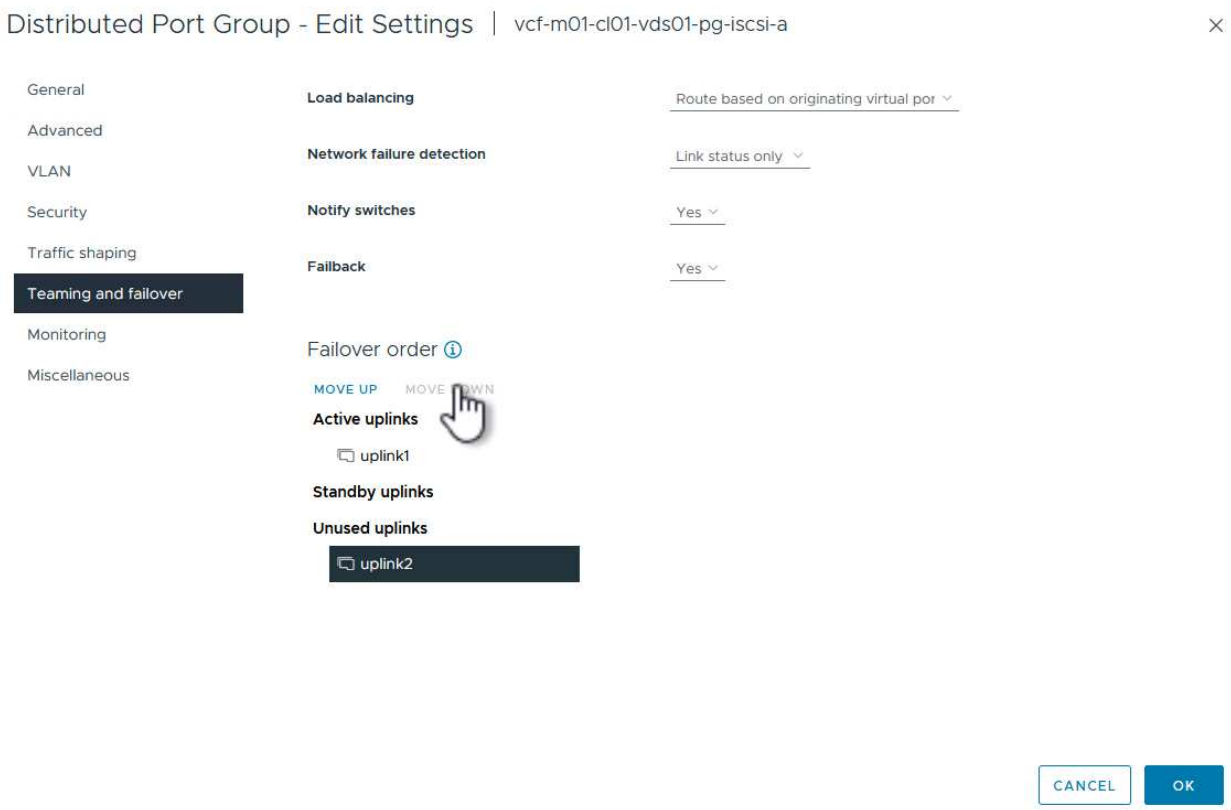
2. 새 분산 포트 그룹 마법사에서 새 포트 그룹의 이름을 입력하고 *다음*을 클릭하여 계속합니다.
3. 설정 구성 페이지에서 모든 설정을 작성하세요. VLAN을 사용하는 경우 올바른 VLAN ID를 제공해야 합니다. 계속하려면 *다음*을 클릭하세요.



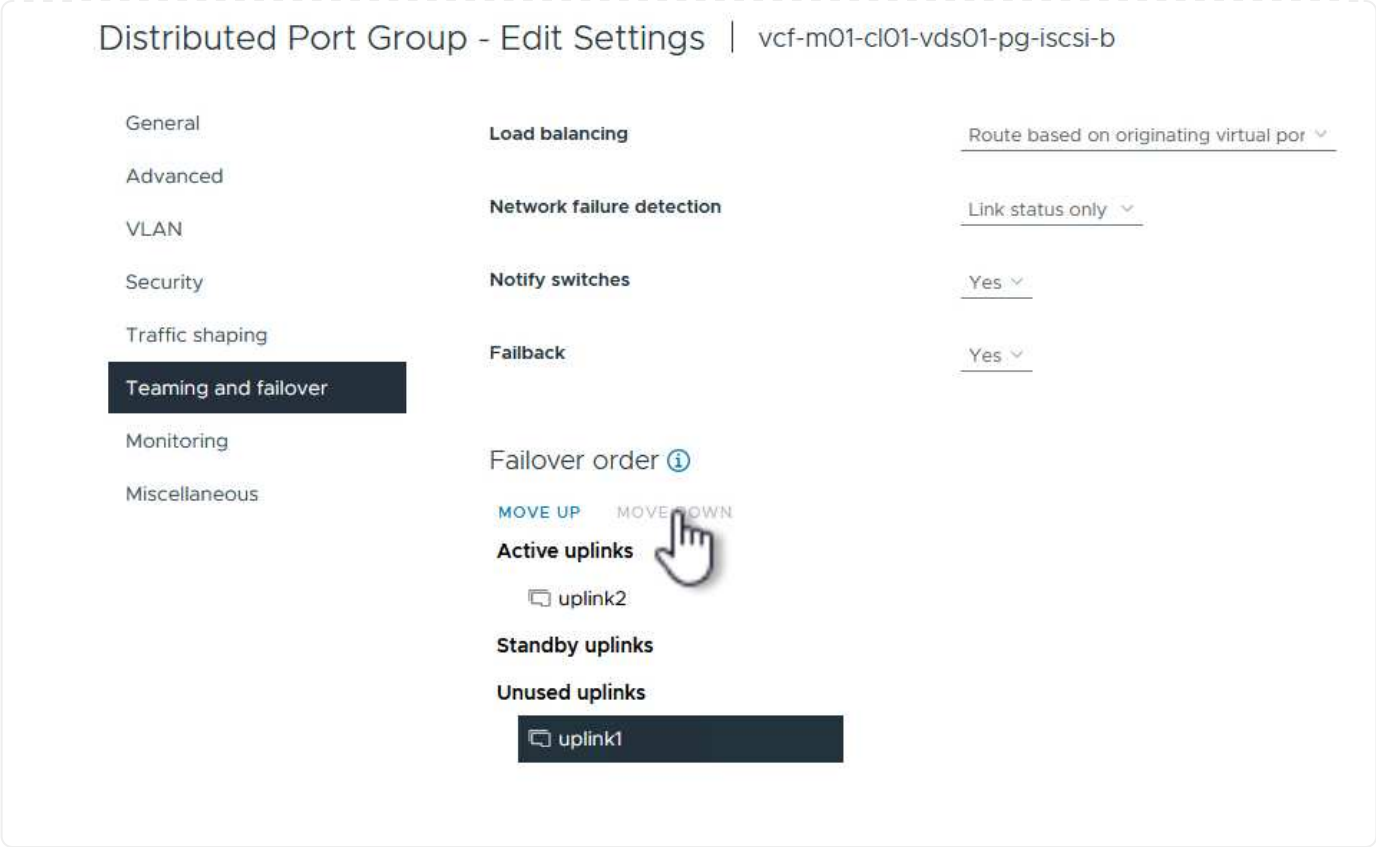
4. 완료 준비 페이지에서 변경 사항을 검토하고 *마침*을 클릭하여 새 분산 포트 그룹을 만듭니다.
5. 두 번째 iSCSI 네트워크에 사용되는 분산 포트 그룹을 생성하려면 이 프로세스를 반복하고 올바른 *VLAN ID*를 입력했는지 확인하세요.
6. 두 포트 그룹이 모두 생성되면 첫 번째 포트 그룹으로 이동하여 설정 편집... 작업을 선택합니다.



7. 분산 포트 그룹 - 설정 편집 페이지에서 왼쪽 메뉴의 *팀 구성 및 장애 조치*로 이동한 다음 *업링크2*를 클릭하여 *사용하지 않는 업링크*로 이동합니다.



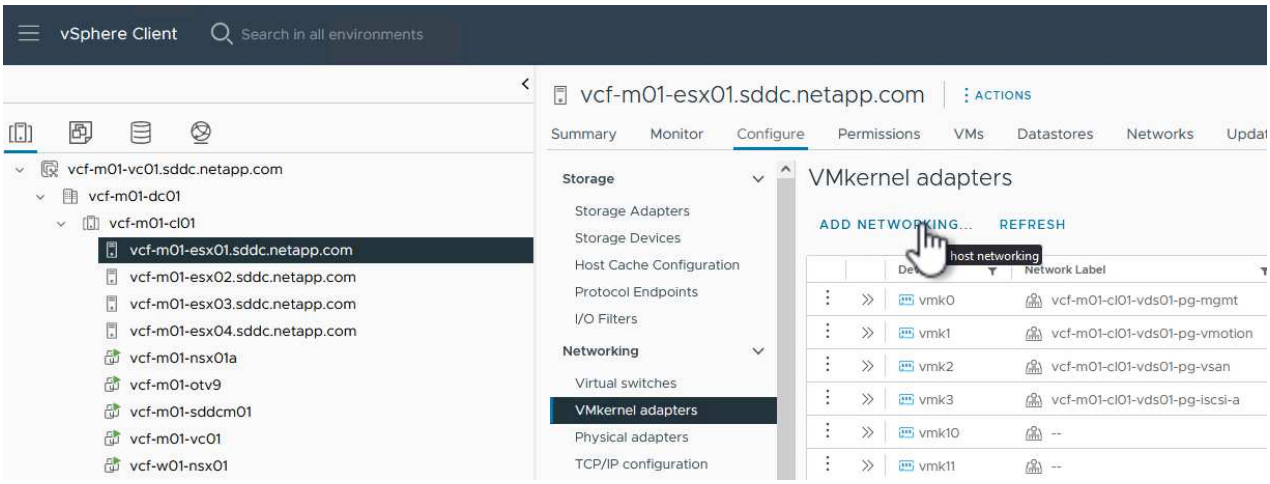
8. 두 번째 iSCSI 포트 그룹에 대해서도 이 단계를 반복합니다. 하지만 이번에는 *uplink1*을 *사용하지 않는 업링크*로 옮깁니다.


Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-b
General
Advanced
VLAN
Security
Traffic shaping
Teaming and failover
Monitoring
Miscellaneous
Load balancing
Route based on originating virtual por
Network failure detection
Link status only
Notify switches
Yes
Failback
Yes
Failover order
MOVE UP
MOVE DOWN
Active uplinks
uplink2
Standby uplinks
Unused uplinks
uplink1

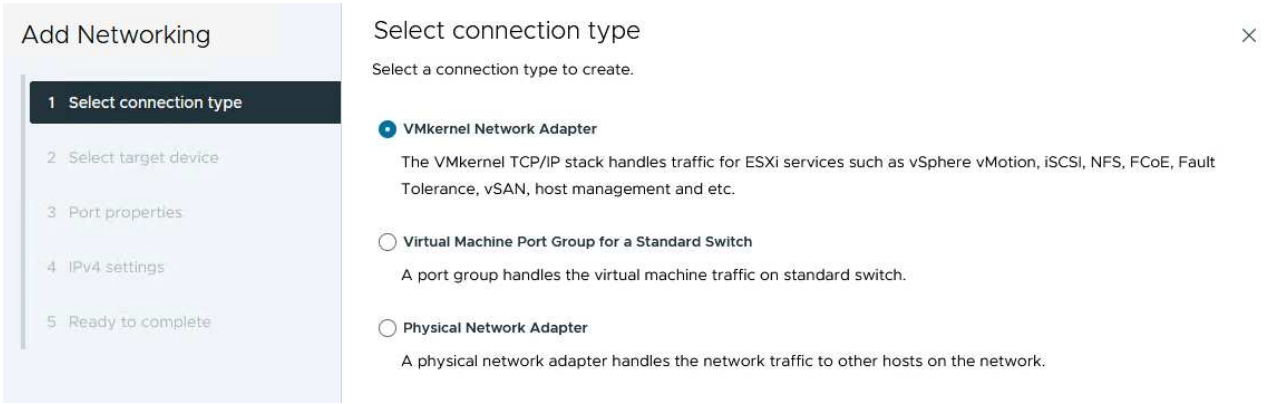
각 **ESXi** 호스트에 **VMkernel** 어댑터를 만듭니다.

관리 도메인의 각 ESXi 호스트에서 이 프로세스를 반복합니다.

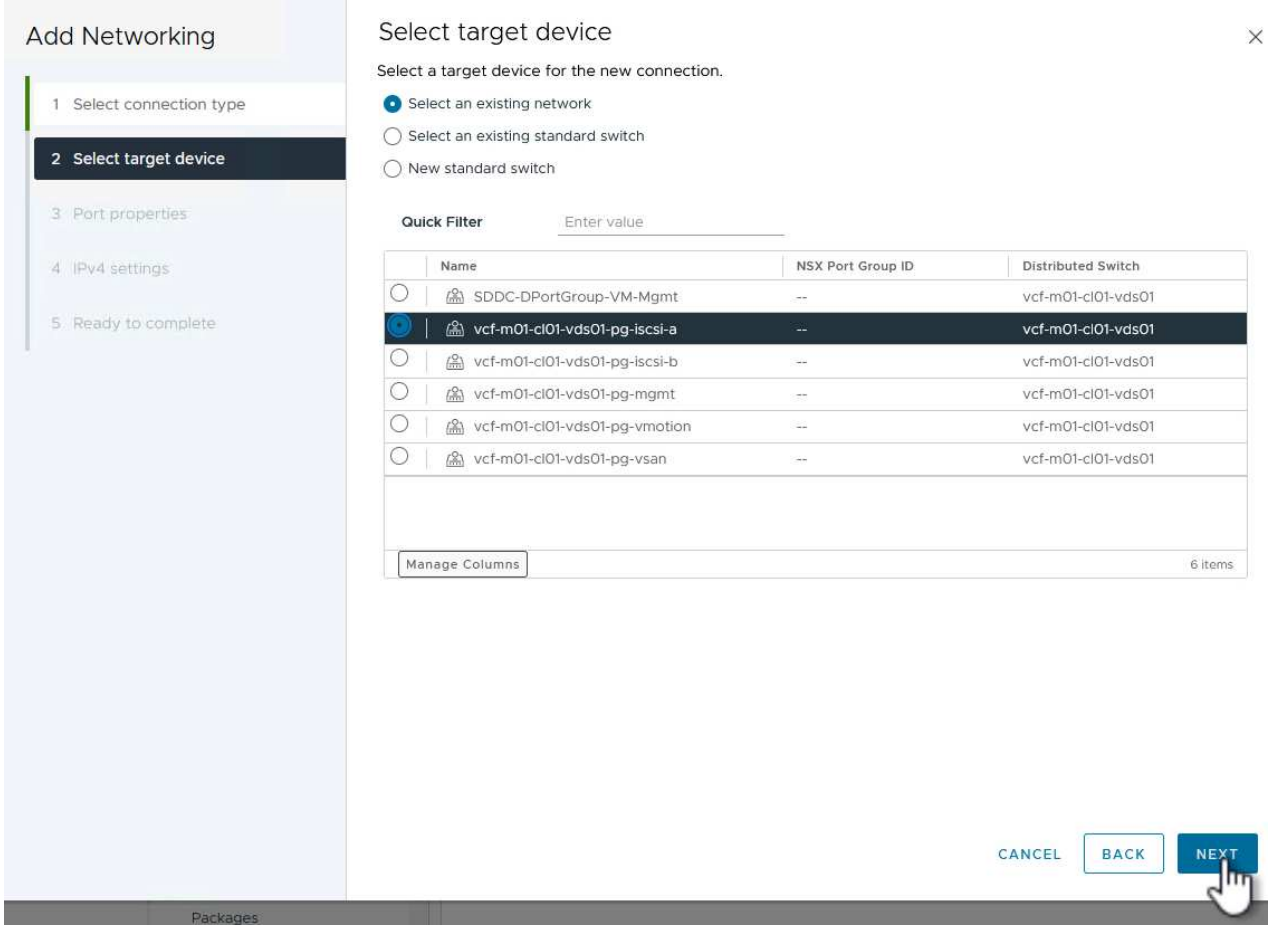
1. vSphere 클라이언트에서 관리 도메인 인벤토리에 있는 ESXi 호스트 중 하나로 이동합니다. 구성 탭에서 *VMkernel 어댑터*를 선택하고 *네트워킹 추가...*를 클릭하여 시작합니다.



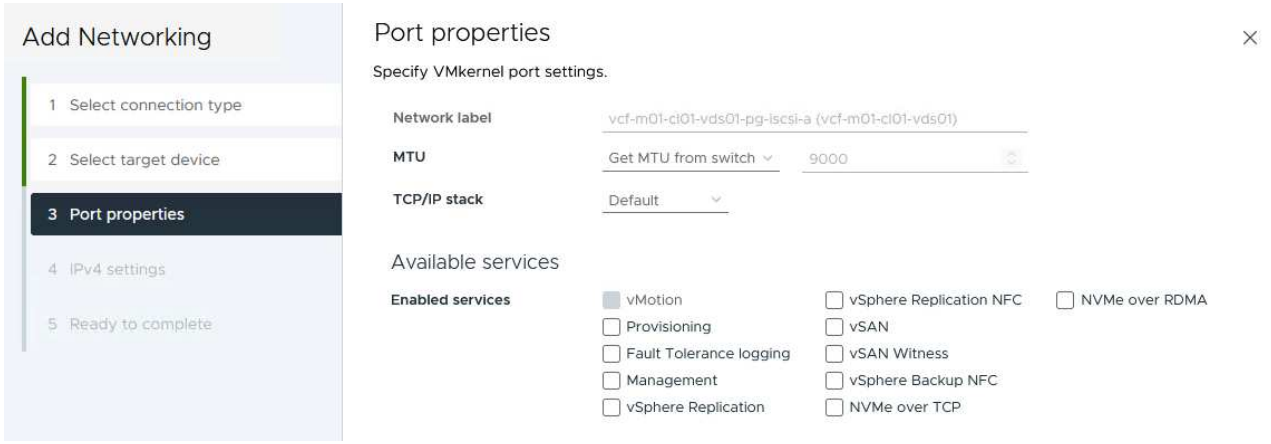
2. 연결 유형 선택 창에서 *VMkernel 네트워크 어댑터*를 선택하고 *다음*을 클릭하여 계속합니다.



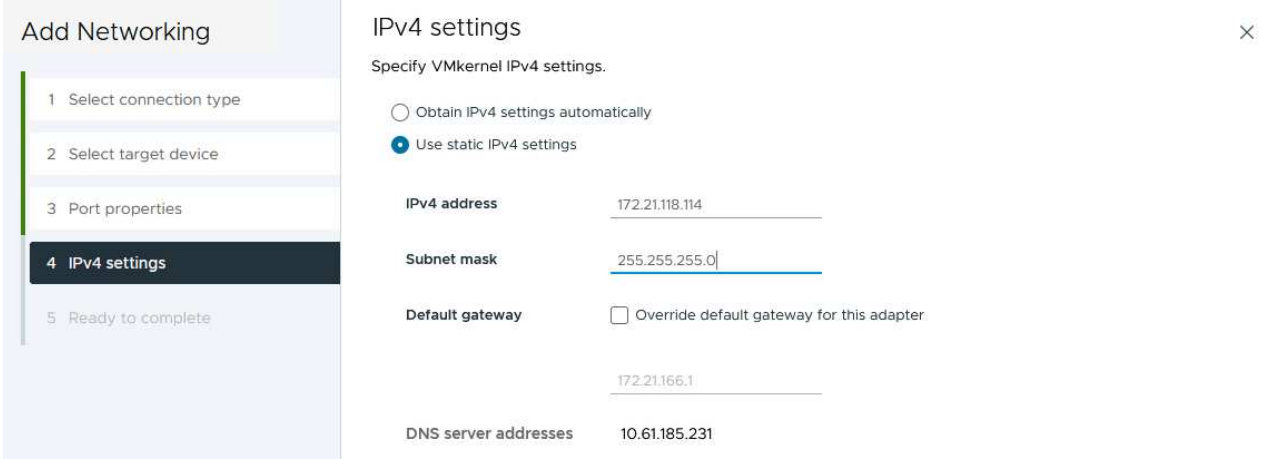
3. 대상 장치 선택 페이지에서 이전에 생성한 iSCSI용 분산 포트 그룹 중 하나를 선택합니다.



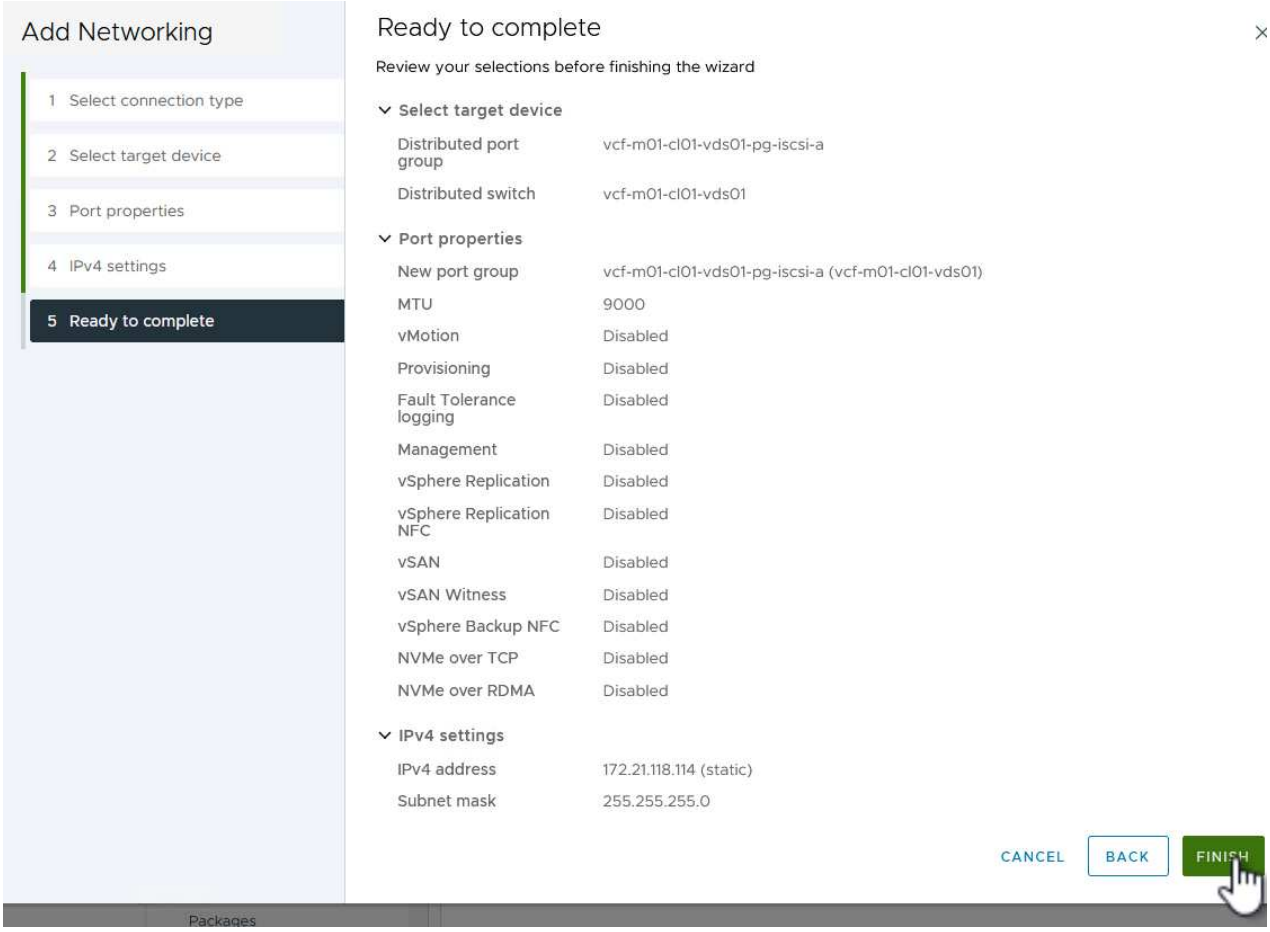
4. 포트 속성 페이지에서 기본값을 유지하고 *다음*을 클릭하여 계속합니다.



5. **IPv4** 설정 페이지에서 **IP** 주소, *서브넷 마스크*를 입력하고 새로운 게이트웨이 IP 주소를 입력합니다(필요한 경우에만). 계속하려면 *다음*을 클릭하세요.



6. 완료 준비 페이지에서 선택 사항을 검토하고 *마침*을 클릭하여 VMkernel 어댑터를 만듭니다.



7. 두 번째 iSCSI 네트워크에 대한 VMkernel 어댑터를 생성하려면 이 과정을 반복합니다.

ONTAP 도구를 배포하고 사용하여 스토리지 구성

다음 단계는 vSphere 클라이언트를 사용하여 VCF 관리 도메인 클러스터에서 수행되며 여기에는 OTV 배포, VMFS

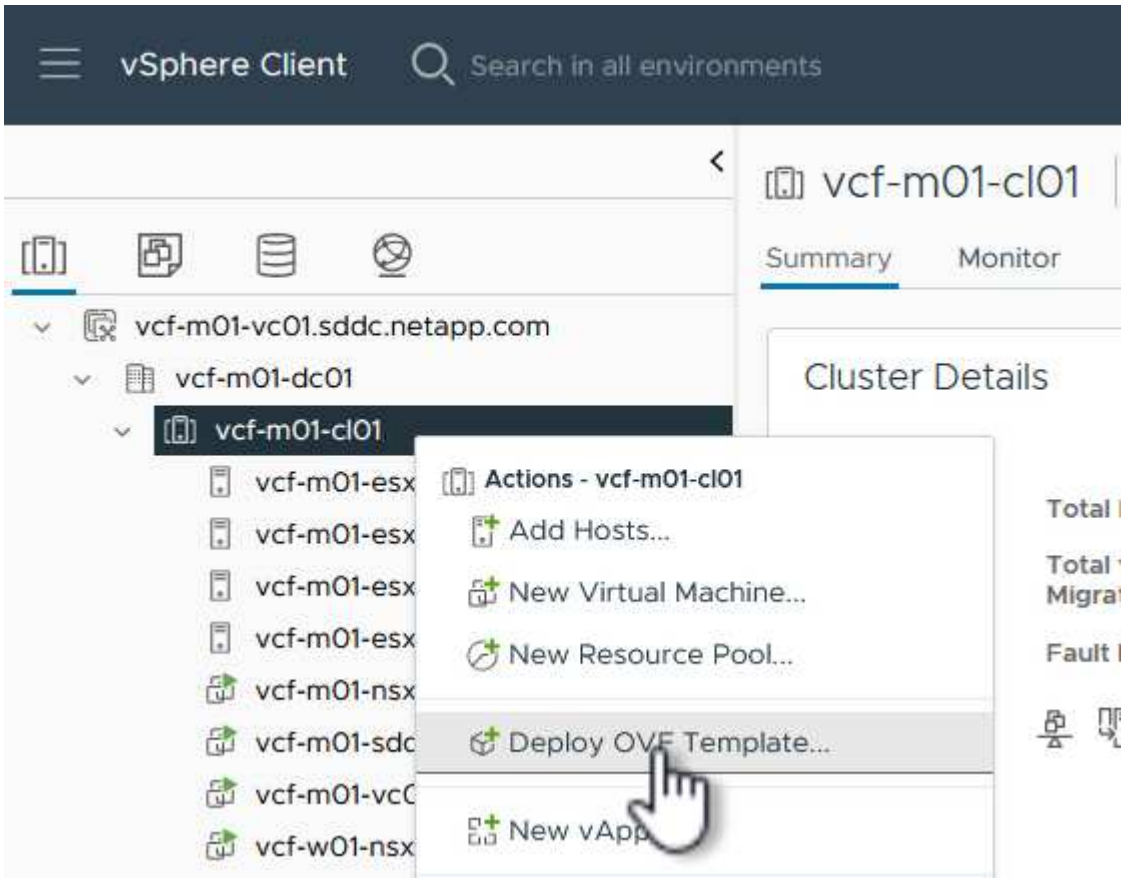
iSCSI 데이터 저장소 생성, 관리 VM을 새 데이터 저장소로 마이그레이션하는 작업이 포함됩니다.

ONTAP tools for VMware vSphere 배포

ONTAP tools for VMware vSphere VM 어플라이언스로 배포되며 ONTAP 스토리지를 관리하기 위한 통합 vCenter UI를 제공합니다.

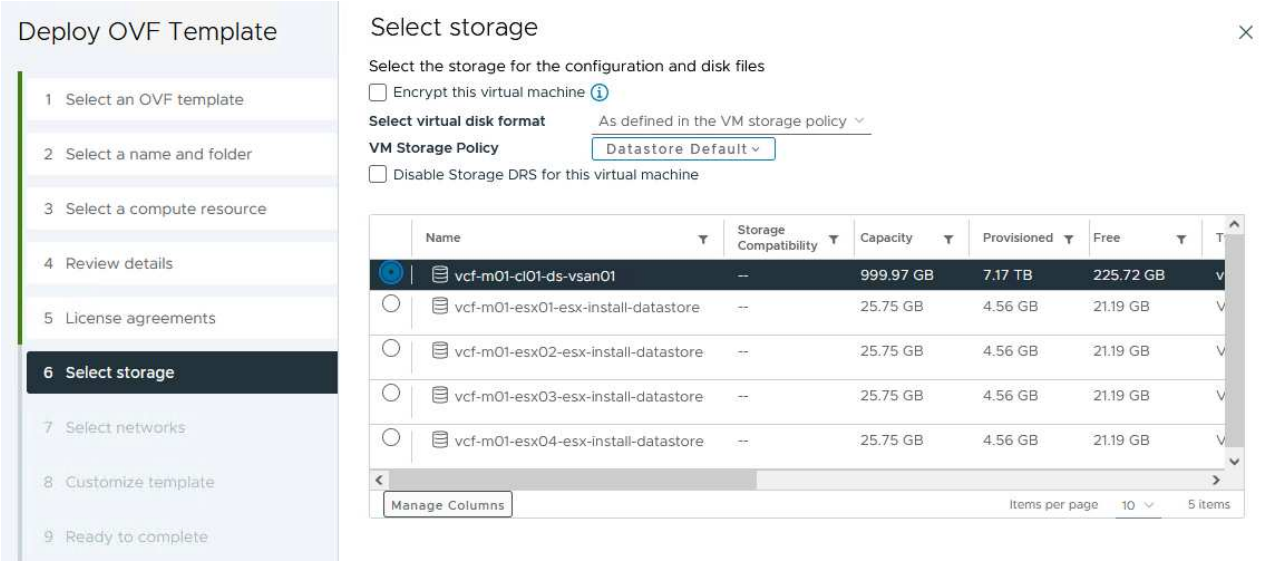
ONTAP tools for VMware vSphere 배포하려면 다음을 완료하세요.

1. ONTAP 도구 OVA 이미지를 가져옵니다."NetApp 지원 사이트" 로컬 폴더로 다운로드합니다.
2. VCF 관리 도메인의 vCenter 어플라이언스에 로그인합니다.
3. vCenter 어플라이언스 인터페이스에서 관리 클러스터를 마우스 오른쪽 버튼으로 클릭하고 *OVF 템플릿 배포…*를 선택합니다.

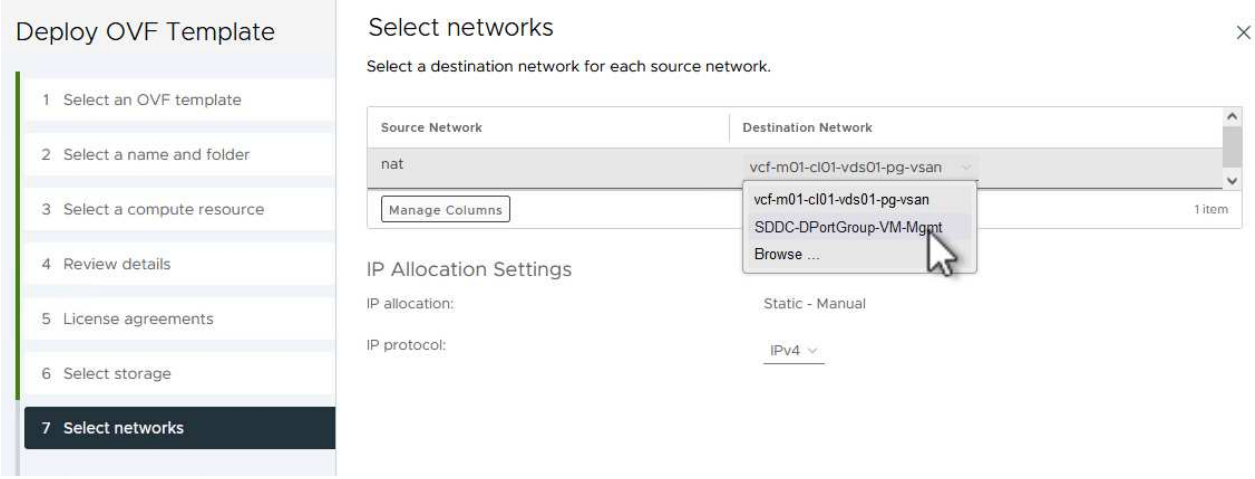


4. **OVF** 템플릿 배포 마법사에서 로컬 파일 라디오 버튼을 클릭하고 이전 단계에서 다운로드한 ONTAP 도구 OVA 파일을 선택합니다.

5. 마법사의 2~5단계에서는 VM의 이름과 폴더를 선택하고, 컴퓨팅 리소스를 선택하고, 세부 정보를 검토한 다음 라이선스 계약에 동의합니다.
6. 구성 및 디스크 파일의 저장 위치로 VCF 관리 도메인 클러스터의 vSAN 데이터 저장소를 선택합니다.

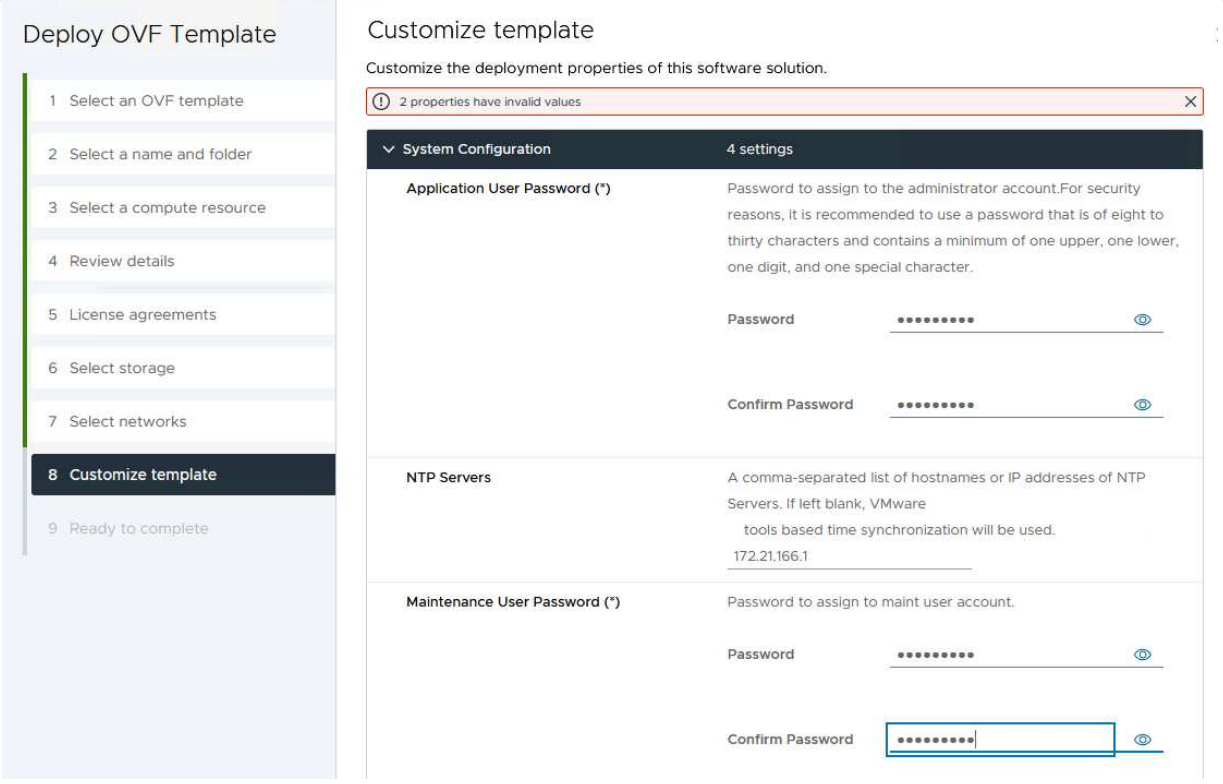


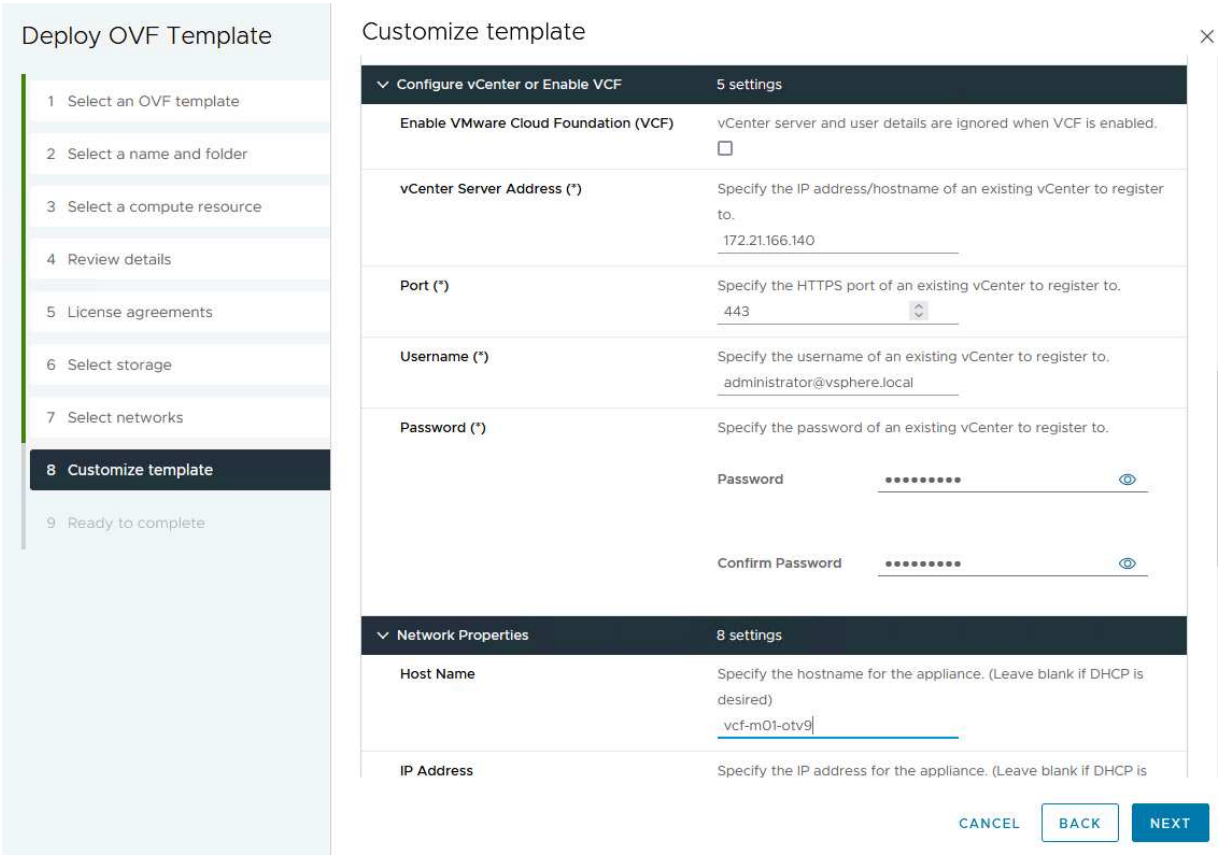
7. 네트워크 선택 페이지에서 관리 트래픽에 사용되는 네트워크를 선택합니다.



8. 사용자 정의 템플릿 페이지에서 필요한 모든 정보를 입력하세요.
   - OTV에 대한 관리 액세스에 사용되는 비밀번호입니다.
   - NTP 서버 IP 주소.
   - OTV 유지관리 계정 비밀번호.
   - OTV 더비 DB 비밀번호.
   - **VMware Cloud Foundation(VCF)** 활성화 상자를 선택하지 마세요. 보조 저장 장치를 배포하는 데 VCF 모드는 필요하지 않습니다.
   - vCenter 어플라이언스의 FQDN 또는 IP 주소를 입력하고 vCenter에 대한 자격 증명을 제공합니다.
   - 필수 네트워크 속성 필드를 제공하세요.

     계속하려면 *다음*을 클릭하세요.



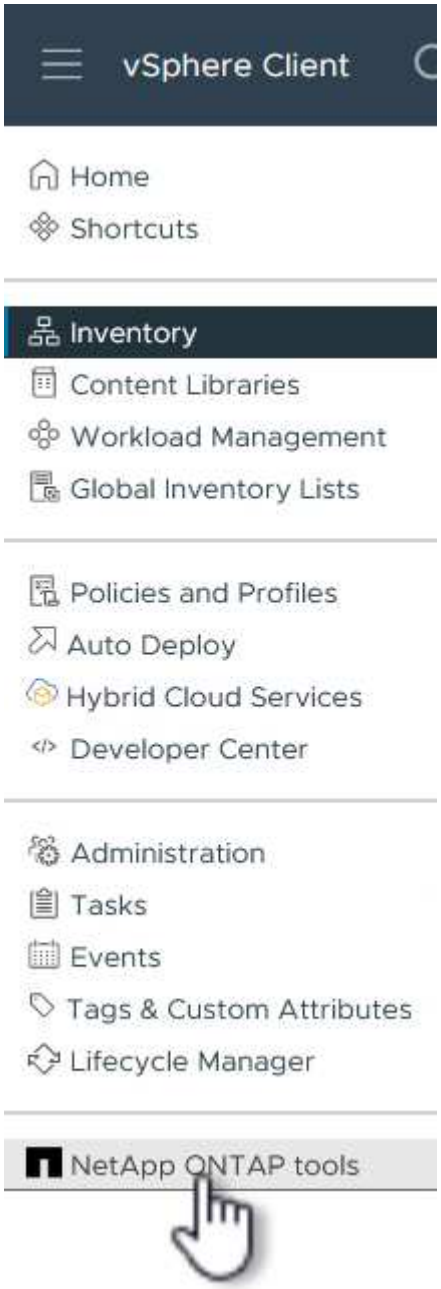


9. 완료 준비 페이지에서 모든 정보를 검토하고 마침을 클릭하여 OTV 어플라이언스 배포를 시작합니다.

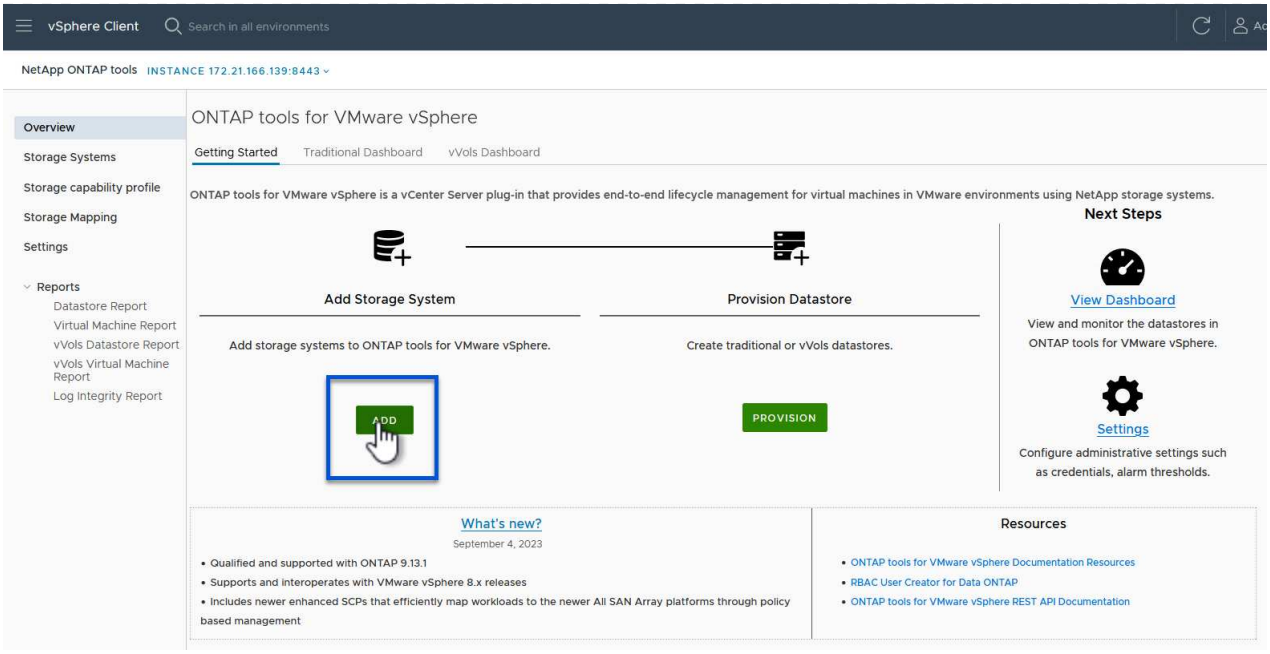
OTV를 사용하여 관리 도메인에 **VMFS iSCSI** 데이터 저장소 구성

OTV를 사용하여 관리 도메인의 보조 저장소로 VMFS iSCSI 데이터 저장소를 구성하려면 다음을 완료하세요.

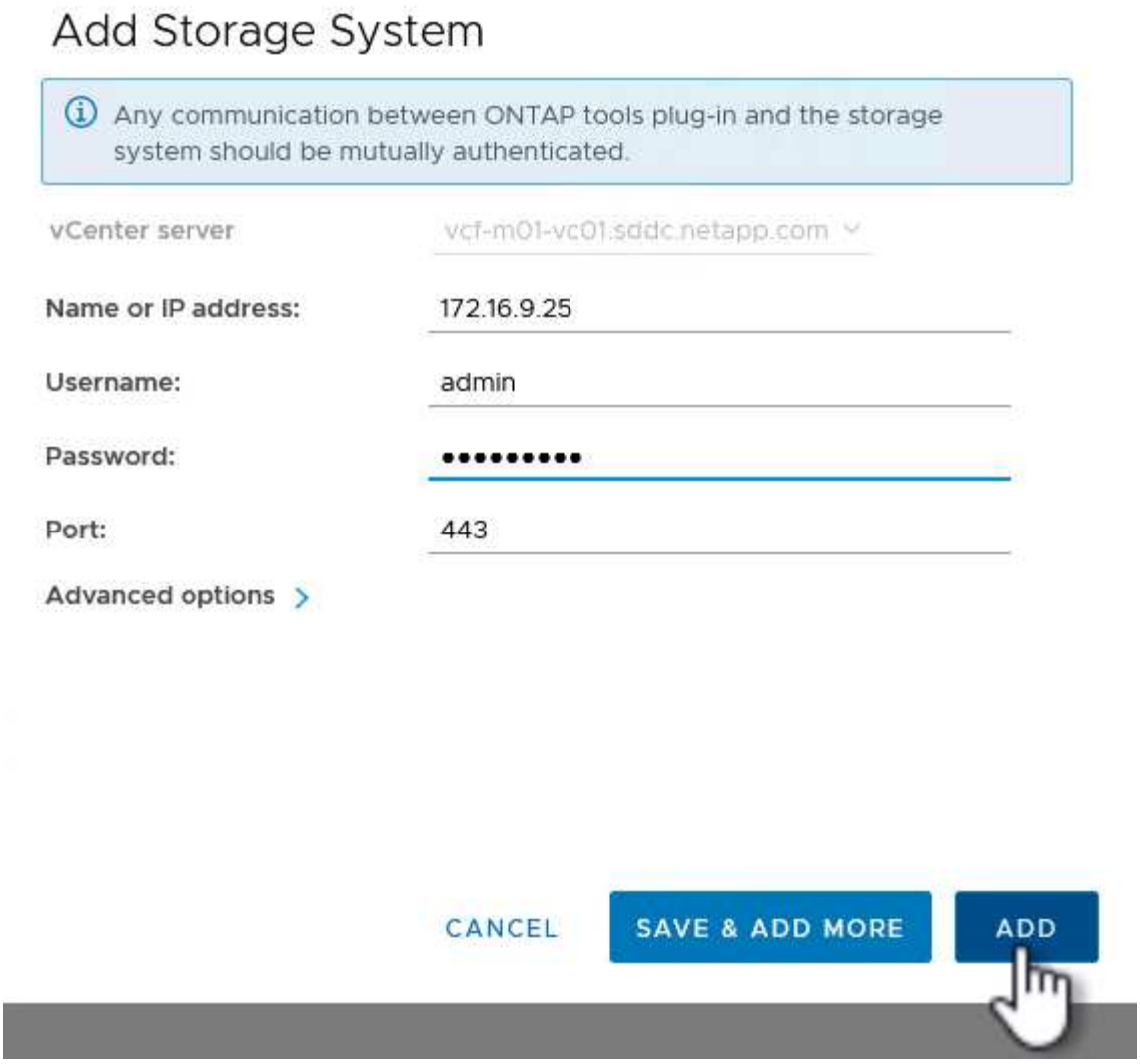
1. vSphere 클라이언트에서 주 메뉴로 이동하여 * NetApp ONTAP 도구*를 선택합니다.



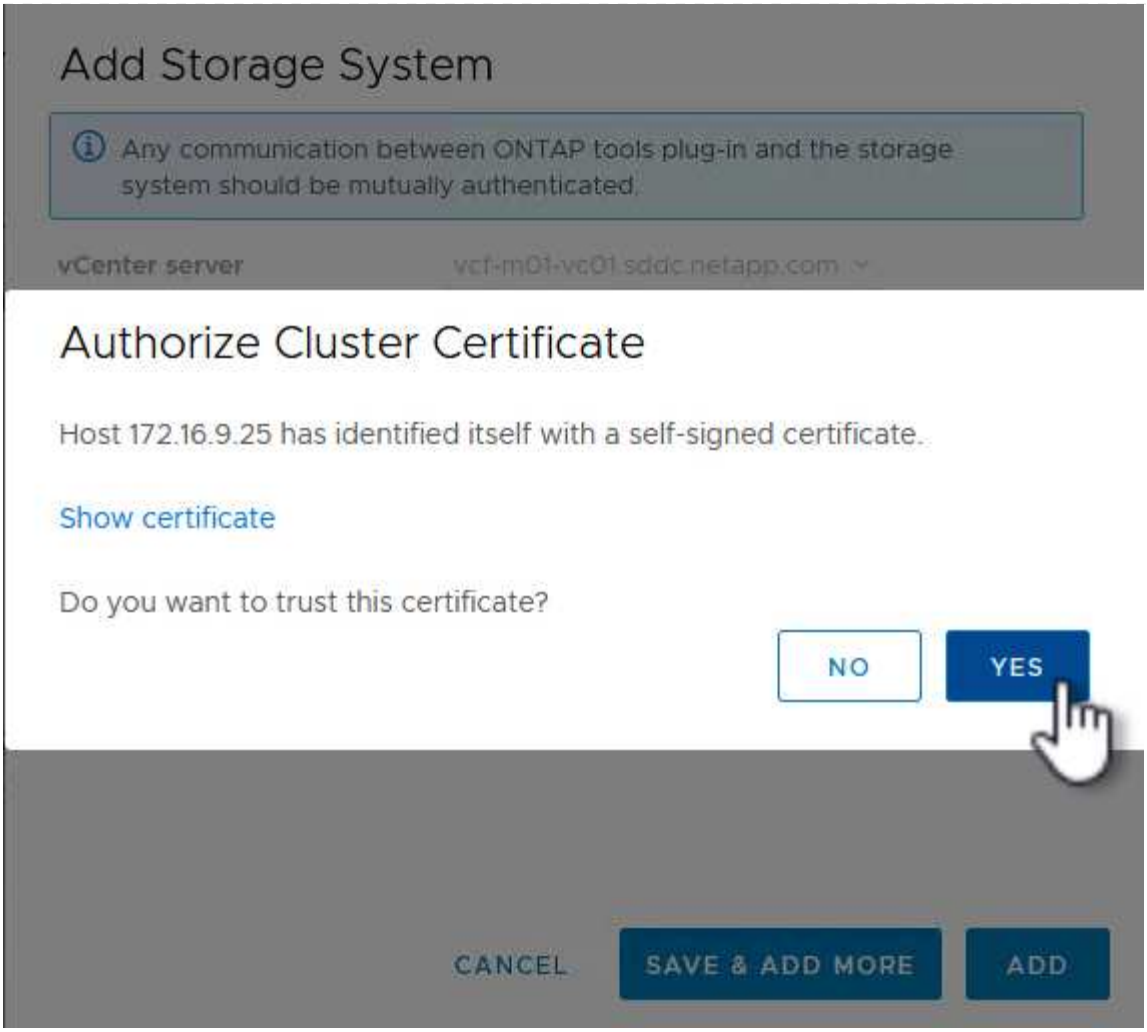
2. * ONTAP 도구*의 시작 페이지(또는 스토리지 시스템)에서 *추가*를 클릭하여 새 스토리지 시스템을 추가합니다.



3. ONTAP 스토리지 시스템의 IP 주소와 자격 증명을 제공하고 *추가*를 클릭합니다.



4. *예*를 클릭하여 클러스터 인증서를 인증하고 스토리지 시스템을 추가합니다.

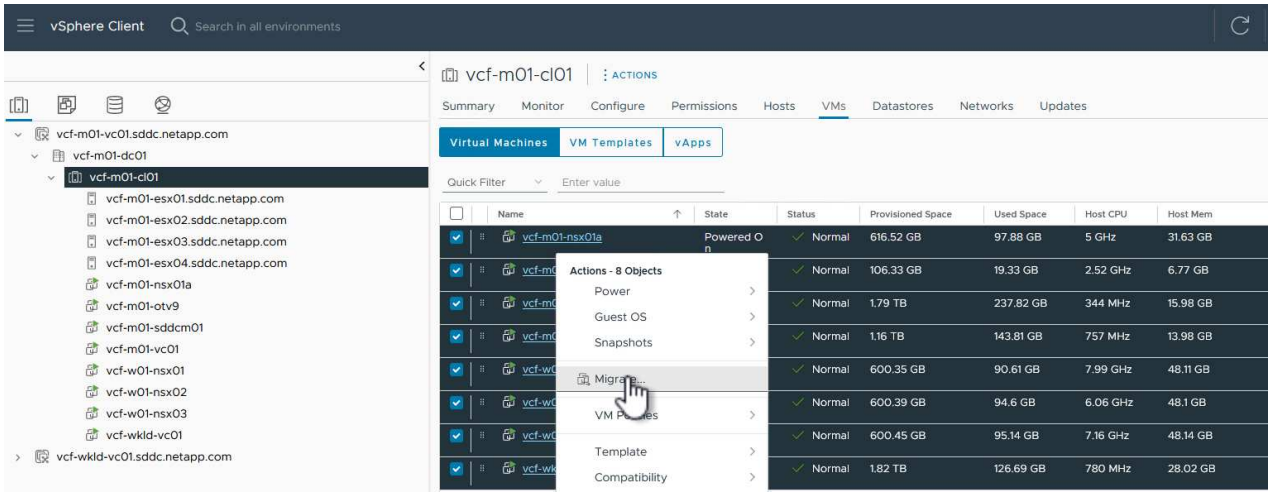

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Authorize Cluster Certificate
Host 172.16.9.25 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES
CANCEL
SAVE & ADD MORE
ADD

관리 **VM**을 **iSCSI** 데이터 저장소로 마이그레이션

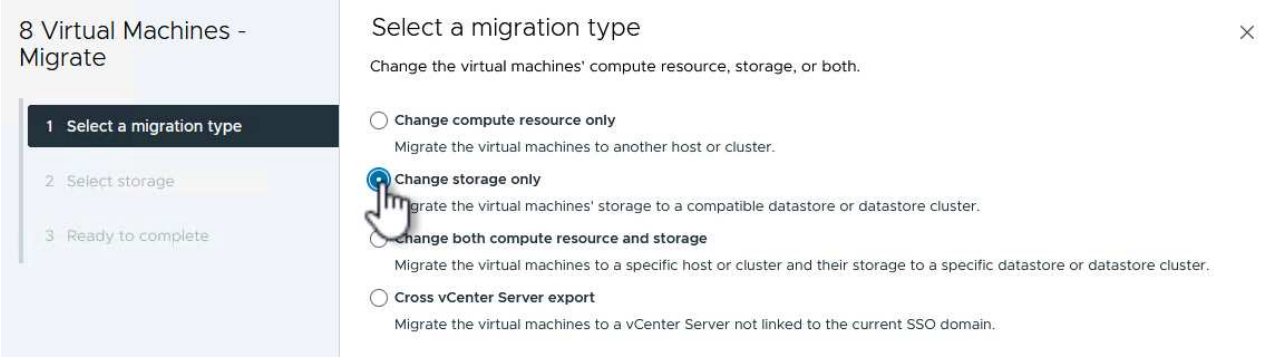
VCF 관리 VM을 보호하기 위해 ONTAP 스토리지를 사용하는 것이 선호되는 경우 vMotion을 사용하여 VM을 새로 생성된 iSCSI 데이터스토어로 마이그레이션할 수 있습니다.

VCF 관리 VM을 iSCSI 데이터 저장소로 마이그레이션하려면 다음 단계를 완료하세요.

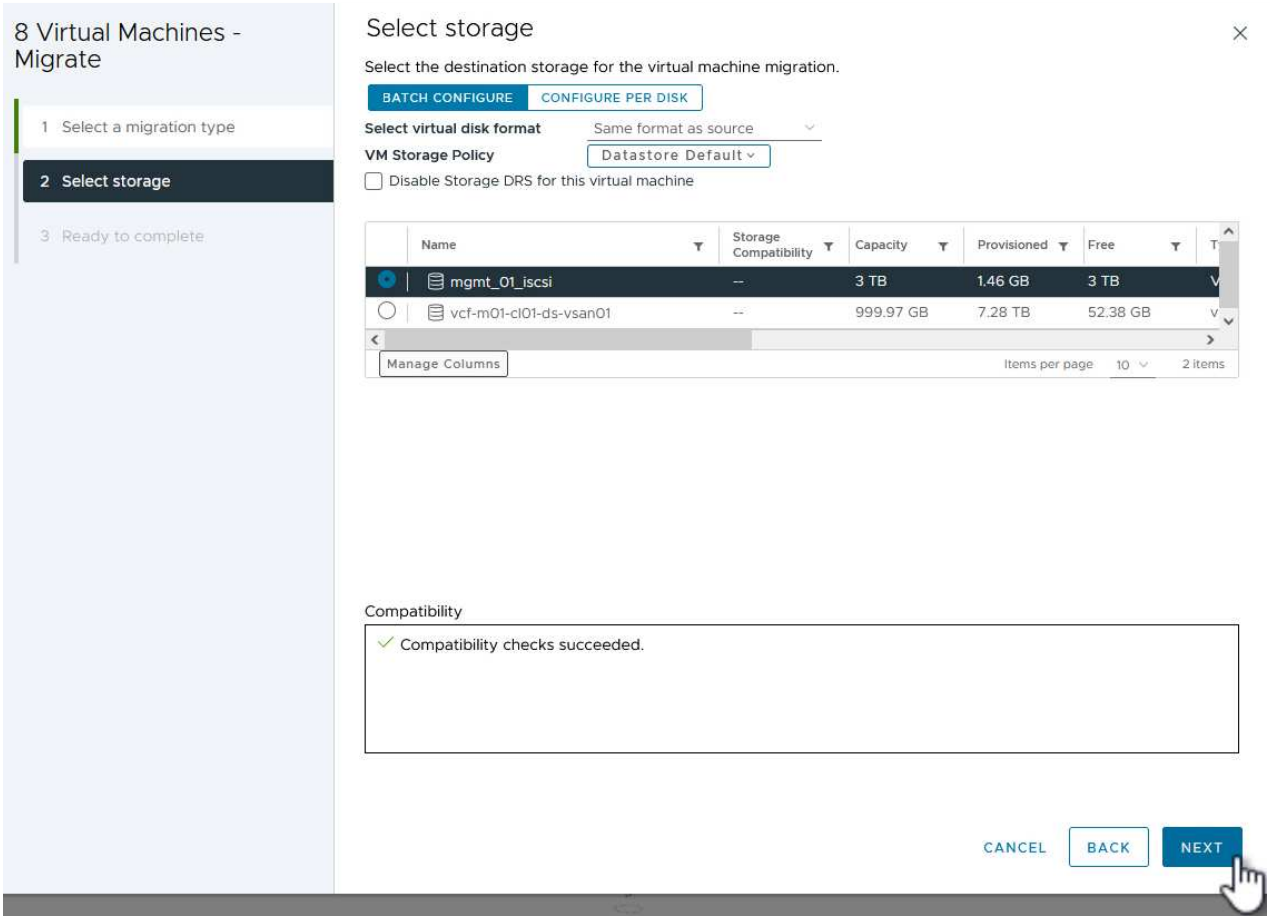
1. vSphere Client에서 관리 도메인 클러스터로 이동하여 **VM** 탭을 클릭합니다.
2. iSCSI 데이터 저장소로 마이그레이션할 VM을 선택하고 마우스 오른쪽 버튼을 클릭한 후 *마이그레이션..*을 선택합니다.



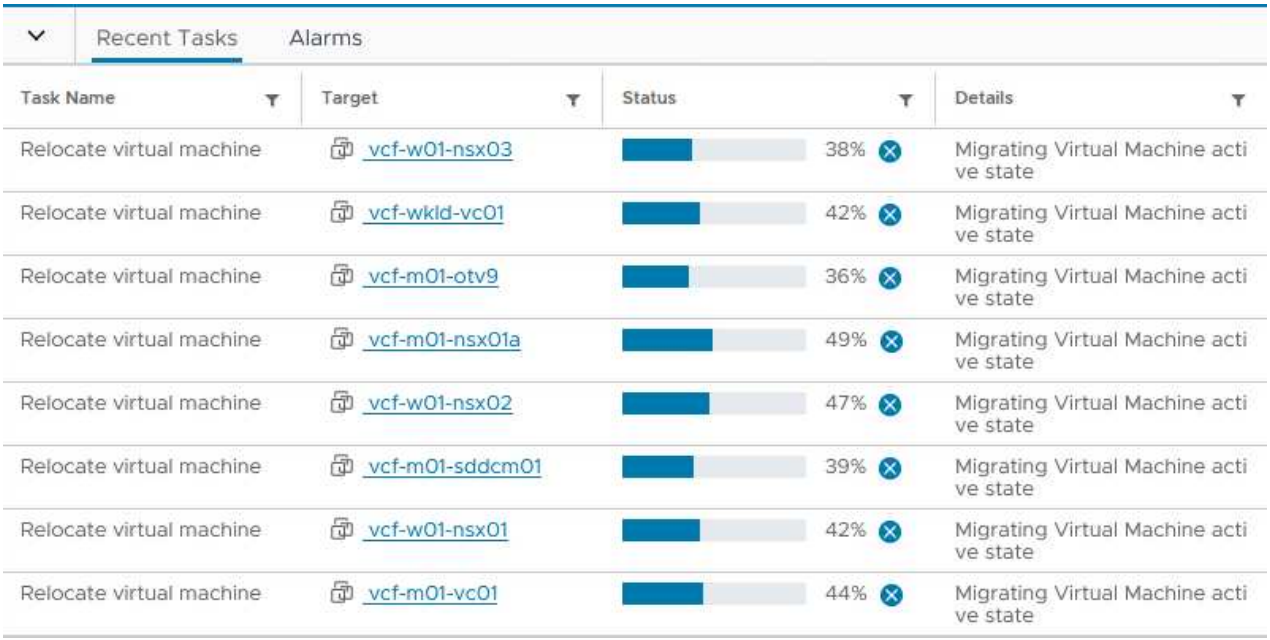
3. 가상 머신 - 마이그레이션 마법사에서 마이그레이션 유형으로 *저장소만 변경*을 선택하고 *다음*을 클릭하여 계속합니다.



4. 저장소 선택 페이지에서 iSCSi 데이터 저장소를 선택하고 *다음*을 선택하여 계속합니다.



5. 선택 사항을 검토하고 *마침*을 클릭하여 마이그레이션을 시작합니다.
6. 이전 상태는 최근 작업 창에서 볼 수 있습니다.



추가 정보

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

이 솔루션에 대한 비디오 데모

VCF 관리 도메인을 위한 보조 스토리지로서의 iSCSI 데이터 저장소

ONTAP tools for VMware vSphere 사용하여 관리 도메인의 보조 스토리지로 FC 기반 VMFS 데이터 저장소 추가

이 사용 사례에서는 ONTAP Tools for VMware를 사용하여 VMware Cloud Foundation(VCF) 관리 도메인의 보조 스토리지로 파이버 채널(FC)을 통해 VMFS 데이터 저장소를 구성하는 절차를 설명합니다. 이 절차에서는 VMware vSphere용 ONTAP 도구 배포, vCenter 서버 등록, 스토리지 백엔드 정의, FC 데이터스토어 프로비저닝을 요약합니다.

파이버 채널의 이점

고성능: FC는 고속 데이터 전송률을 제공하므로 대량의 데이터에 빠르고 안정적으로 액세스해야 하는 애플리케이션에 이상적입니다.

낮은 지연 시간: 매우 낮은 지연 시간은 데이터베이스 및 가상화 환경과 같은 성능에 민감한 애플리케이션에 매우 중요합니다.

신뢰성: FC 네트워크는 내장된 중복성 및 오류 수정과 같은 기능을 갖추고 있어 견고성과 안정성이 뛰어난 것으로 알려져 있습니다.

전용 대역폭: FC는 스토리지 트래픽에 전용 대역폭을 제공하여 네트워크 혼잡 위험을 줄입니다.

NetApp 스토리지 시스템에서 파이버 채널을 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요. "FC를 사용한 SAN 프로비저닝" .

시나리오 개요

VCF 보충 데이터 저장소는 vCenter를 사용한 2일차 작업의 일부로 제공됩니다. 이 시나리오에서는 다음과 같은 상위 수준 단계를 다룹니다.

- 관리 도메인에 ONTAP 도구 배포
- ONTAP 도구에 VI 워크로드 vCenter 서버 등록
- VMware vSphere용 ONTAP 도구 플러그인에서 스토리지 백엔드 정의
- FC 전송에 VMFS 프로비저닝

필수 조건

이 시나리오에는 다음과 같은 구성 요소와 구성이 필요합니다.

- FC 스위치에 연결된 FC 포트가 있는 ONTAP 스토리지 시스템입니다.

- FC lifes로 생성된 SVM입니다.
- FC 스위치에 연결된 FC HBA가 있는 vSphere.
- FC 스위치에는 단일 이니시에이터-타겟 구역 설정이 구성됩니다.

> ONTAP 시스템의 물리적 FC 포트 대신 영역 구성에서 SVM FC 논리적 인터페이스를 사용합니다.

NetApp FC LUN에 대해 다중 경로를 권장합니다.

ONTAP 스토리지 시스템에서 파이버 채널을 구성하는 방법에 대한 자세한 내용은 다음을 참조하세요. "SAN 스토리지 관리" ONTAP 9 문서에서.

ONTAP 스토리지 시스템과 함께 VMFS를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오."VMFS 배포 가이드" .

관리 도메인에 대한 배포 단계

ONTAP 도구를 배포하고 이를 사용하여 VCF 관리 도메인에 VMFS 데이터 저장소를 생성하려면 다음 단계를 완료하세요.

- "관리 도메인에 ONTAP 도구 배포"
- "vSphere 클라이언트 인터페이스를 사용하여 스토리지 백엔드 정의"
- "FC에 VMFS 프로비저닝"

추가 정보

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

이 솔루션에 대한 비디오 데모

VCF 관리 도메인을 위한 보조 저장소로서의 VMFS(FC) 데이터 저장소

ONTAP tools for VMware vSphere 사용하여 **VI** 워크로드 도메인에 보조 스토리지로 **vVols** 추가

이 사용 사례에서는 VMware Cloud Foundation(VCF) Virtual Infrastructure(VI) 워크로드 도메인의 보조 스토리지를 위해 iSCSI를 사용하여 vVols 데이터 저장소를 구성하는 절차를 설명합니다. 이 절차에서는 iSCSI 네트워킹 설정, VMware vSphere용 ONTAP 도구 배포, vVols 데이터 저장소 프로비저닝을 요약합니다.

*iSCSI*는 vVols 데이터 저장소의 저장 프로토콜로 사용됩니다.

iSCSI의 이점

고성능**:** 빠르고 효율적인 데이터 전송 속도와 낮은 지연 시간을 제공하는 고성능을 제공합니다. 까다로운 엔터프라이즈 애플리케이션과 가상화 환경에 이상적입니다.

관리 용이성: 익숙한 IP 기반 도구와 프로토콜을 사용하여 스토리지 관리를 간소화합니다.

비용 효율성: 기존 이더넷 인프라를 활용하여 특수 하드웨어의 필요성을 줄이고 조직이 안정적이고 확장 가능한 스토리지 솔루션을 구축할 수 있도록 합니다.

NetApp 스토리지 시스템에서 iSCSI를 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요. "iSCSI를 사용한 SAN 프로비저닝" .

시나리오 개요

이 시나리오에서는 다음과 같은 상위 수준 단계를 다룹니다.

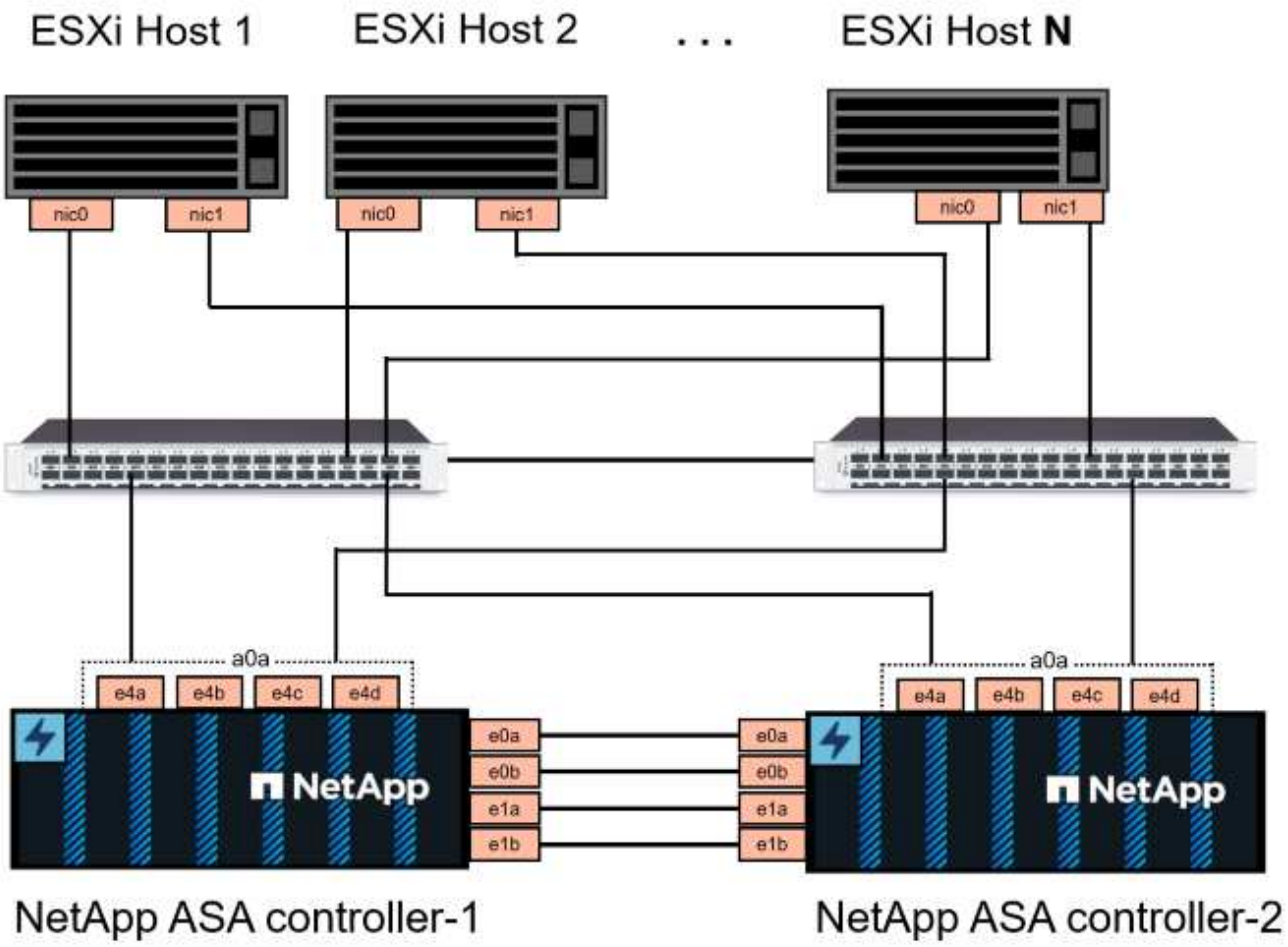
- iSCSI 트래픽을 위한 논리 인터페이스(LIF)가 있는 스토리지 가상 머신(SVM)을 만듭니다.
- VI 워크로드 도메인에서 iSCSI 네트워크에 대한 분산 포트 그룹을 생성합니다.
- VI 워크로드 도메인의 ESXi 호스트에서 iSCSI용 vmkernel 어댑터를 생성합니다.
- VI 워크로드 도메인에 ONTAP 도구를 배포합니다.
- VI 워크로드 도메인에 새로운 vVols 데이터 저장소를 만듭니다.

필수 조건

이 시나리오에는 다음과 같은 구성 요소와 구성이 필요합니다.

- 스토리지 트래픽에 전용된 이더넷 스위치의 물리적 데이터 포트가 있는 ONTAP AFF 또는 ASA 스토리지 시스템입니다.
- VCF 관리 도메인 배포가 완료되었으며 vSphere 클라이언트에 액세스할 수 있습니다.
- VI 워크로드 도메인이 이전에 배포되었습니다.

NetApp iSCSI에 대해 완전 중복 네트워크 설계를 권장합니다. 다음 다이어그램은 스토리지 시스템, 스위치, 네트워크 어댑터 및 호스트 시스템에 대한 장애 내구성을 제공하는 중복 구성의 예를 보여줍니다. NetApp 을 참조하세요"SAN 구성 참조" 추가 정보를 원하시면.



다중 경로 지정 및 여러 경로에 걸친 장애 조치의 경우 NetApp iSCSI 구성의 모든 SVM에 대해 별도의 이더넷 네트워크에 스토리지 노드당 최소 두 개의 LIF를 두는 것을 권장합니다.

이 문서에서는 새로운 SVM을 생성하고 iSCSI 트래픽에 대한 여러 LIF를 생성하기 위해 IP 주소 정보를 지정하는 프로세스를 보여줍니다. 기존 SVM에 새로운 LIF를 추가하려면 다음을 참조하세요."LIF(네트워크 인터페이스) 생성" .

> 동일한 IP 네트워크에 여러 VMkernel 어댑터가 구성된 상황에서는 ESXi 호스트에서 소프트웨어 iSCSI 포트 바인딩을 사용하여 어댑터 전체에 걸친 부하 분산이 이루어지도록 하는 것이 좋습니다. KB 문서를 참조하세요"ESX/ESXi에서 소프트웨어 iSCSI 포트 바인딩을 사용하기 위한 고려 사항(2038869)" .

VMware에서 VMFS iSCSI 데이터 저장소를 사용하는 것에 대한 추가 정보는 다음을 참조하세요."vSphere VMFS 데이터스토어 - ONTAP 사용한 iSCSI 스토리지 백엔드" .

배포 단계

ONTAP 도구를 배포하고 이를 사용하여 VCF 관리 도메인에 vVols 데이터 저장소를 생성하려면 다음 단계를 완료하세요.

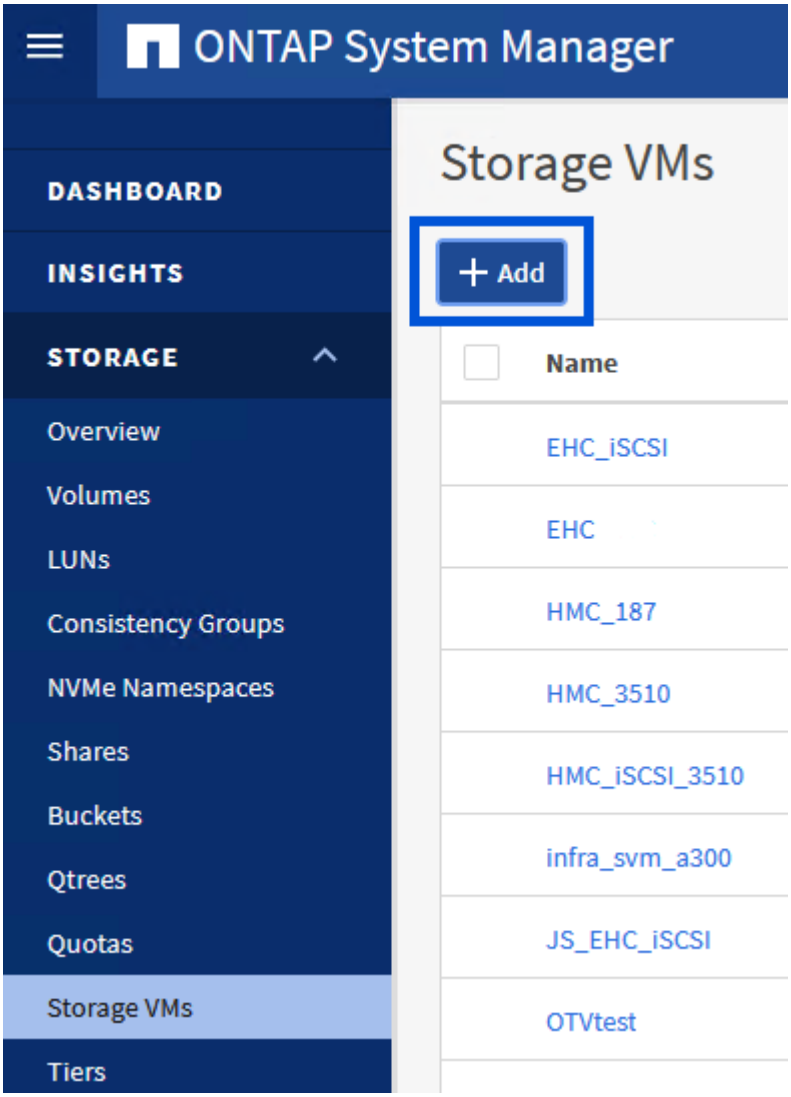
ONTAP 스토리지 시스템에 **SVM** 및 **LIF** 생성

다음 단계는 ONTAP 시스템 관리자에서 수행됩니다.

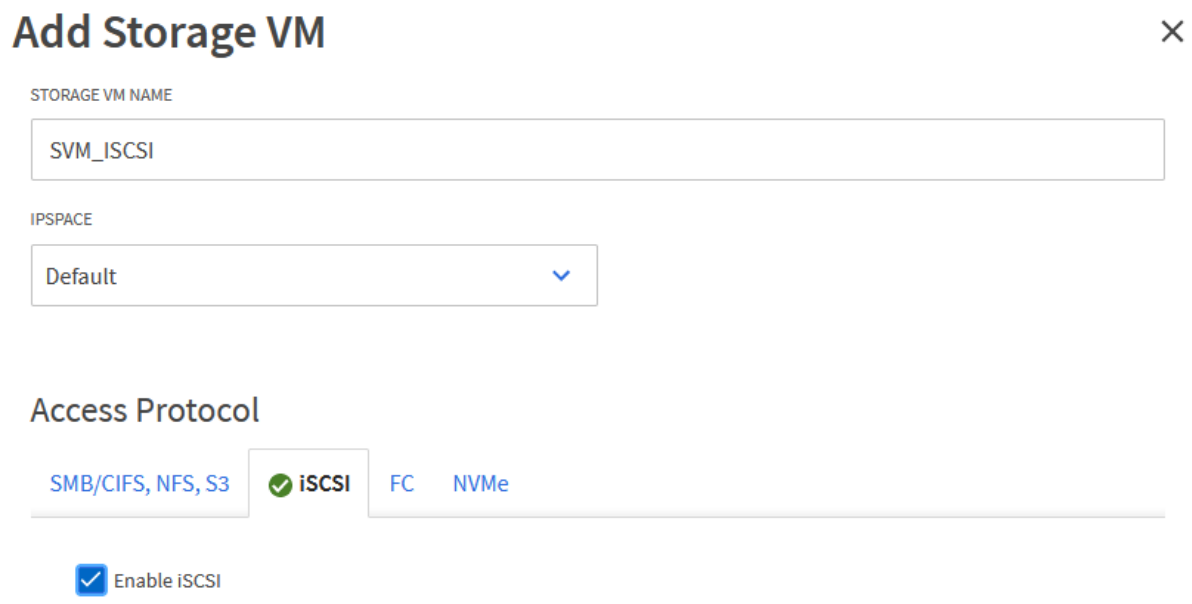
스토리지 **VM** 및 **LIF** 생성

iSCSI 트래픽을 위한 여러 LIF와 함께 SVM을 생성하려면 다음 단계를 완료하세요.

1. ONTAP System Manager에서 왼쪽 메뉴의 *Storage VMs*로 이동한 다음 *+ 추가*를 클릭하여 시작합니다.

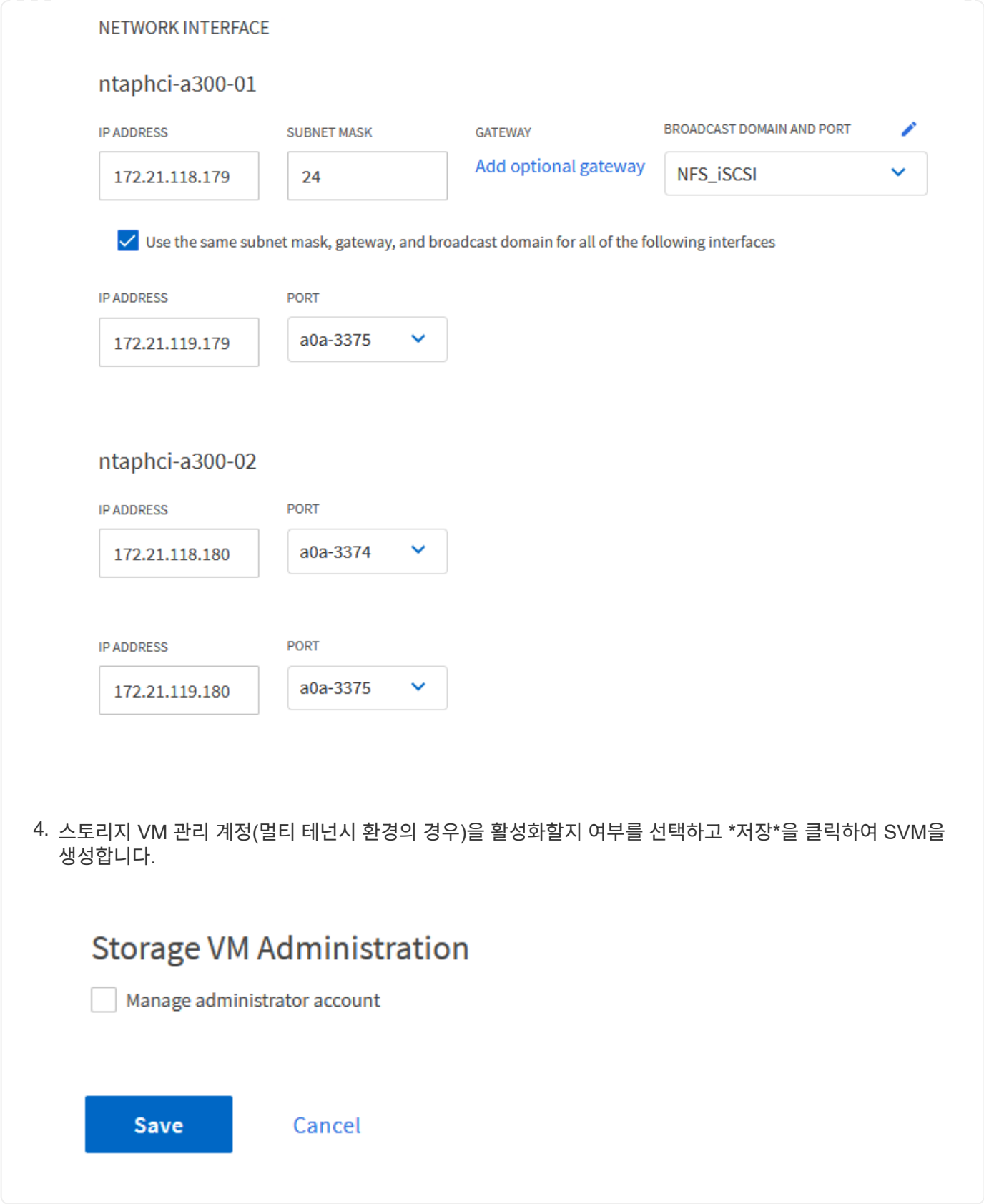


2. 스토리지 **VM** 추가 마법사에서 SVM의 이름*을 입력하고, ***IP** 공간*을 선택한 다음, *액세스 프로토콜*에서 ***iSCSI** 탭을 클릭하고 **iSCSI** 사용 확인란을 선택합니다.



3. 네트워크 인터페이스 섹션에 첫 번째 LIF에 대한 **IP** 주소, 서브넷 마스크, *브로드캐스트 도메인 및 포트*를 입력합니다. 이후 LIF의 경우 확인란을 활성화하여 나머지 모든 LIF에서 공통 설정을 사용하거나 별도의 설정을 사용할 수 있습니다.

> ⓘ 다중 경로 지정 및 여러 경로에 걸친 장애 조치의 경우 NetApp iSCSI 구성의 모든 SVM에 대해 별도의 이더넷 네트워크에 스토리지 노드당 최소 두 개의 LIF를 두는 것을 권장합니다.



4. 스토리지 VM 관리 계정(멀티 테넌시 환경의 경우)을 활성화할지 여부를 선택하고 *저장*을 클릭하여 SVM을 생성합니다.

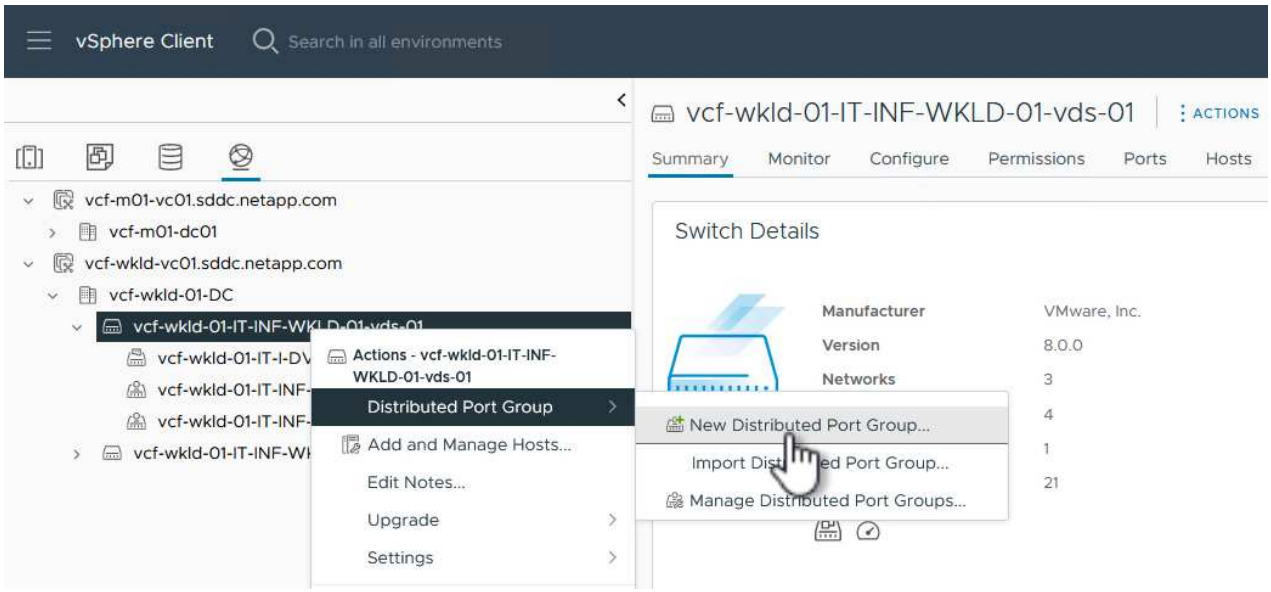
ESXi 호스트에서 **iSCSI**에 대한 네트워킹 설정

다음 단계는 vSphere 클라이언트를 사용하여 VI 워크로드 도메인 클러스터에서 수행됩니다. 이 경우 vCenter Single Sign-On이 사용되므로 vSphere 클라이언트는 관리 및 워크로드 도메인에서 공통적입니다.

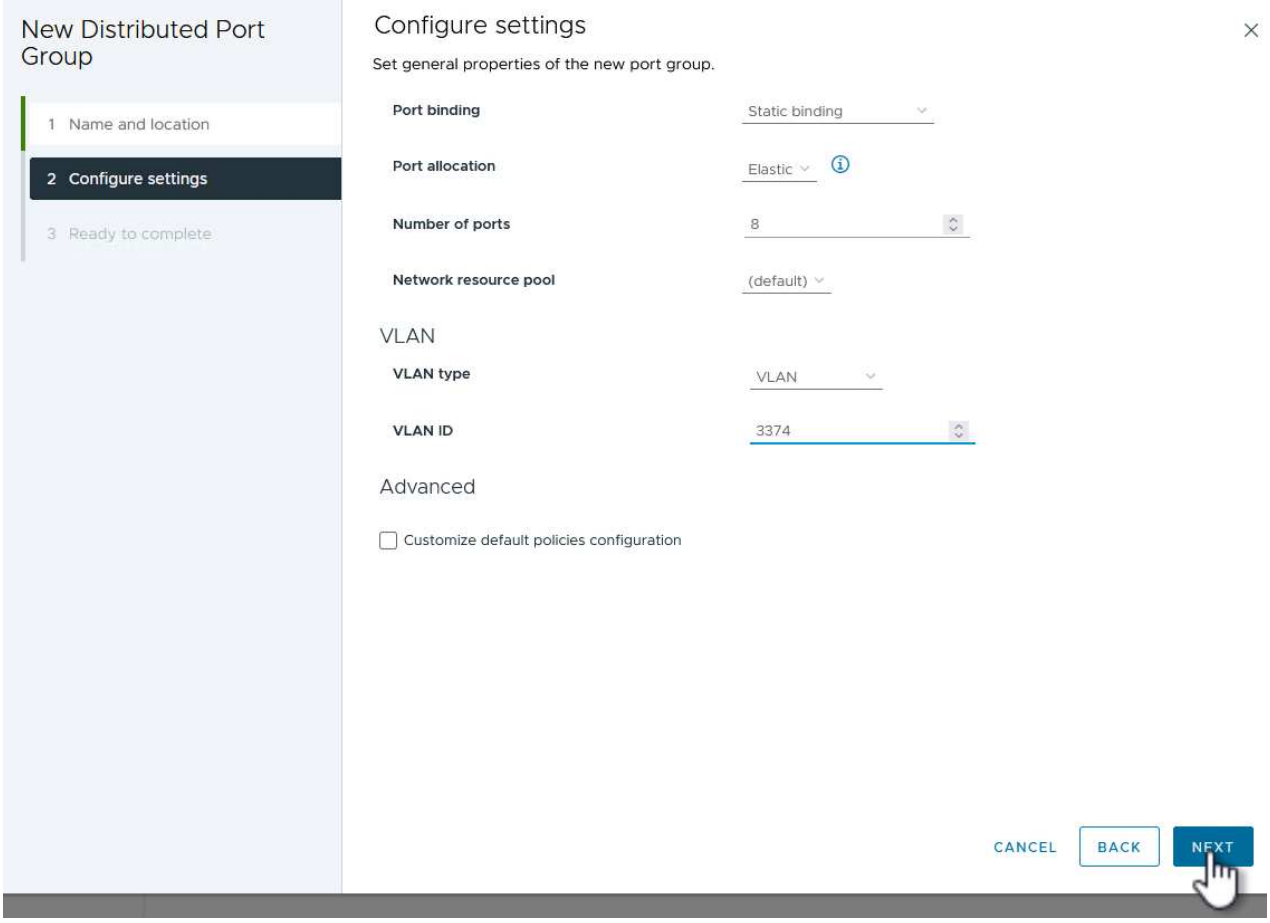
iSCSI 트래픽을 위한 분산 포트 그룹 생성

각 iSCSI 네트워크에 대한 새로운 분산 포트 그룹을 생성하려면 다음을 완료하세요.

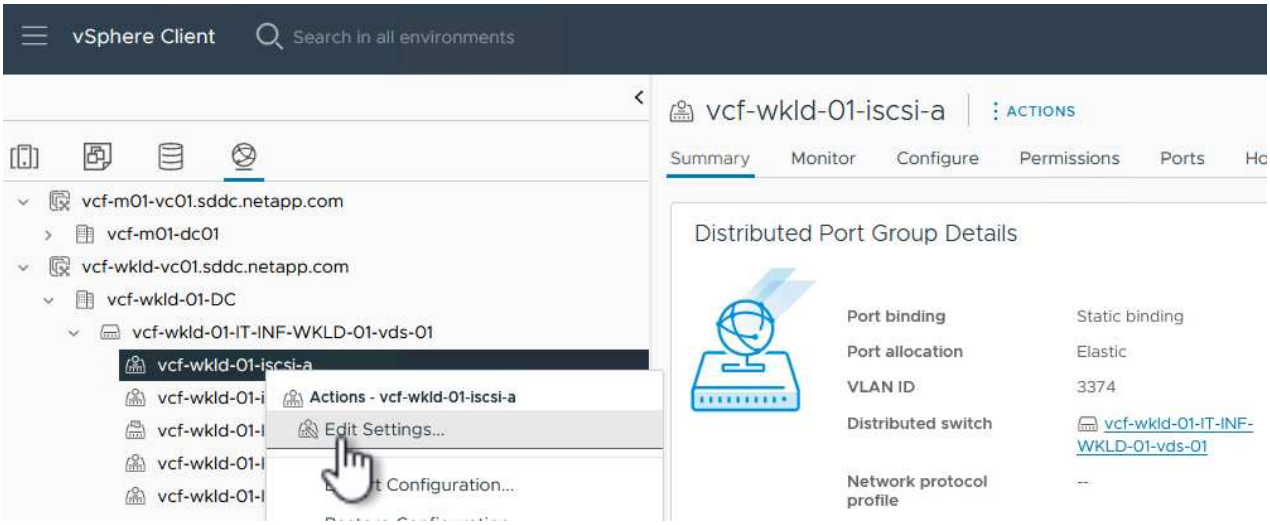
1. vSphere 클라이언트에서 워크로드 도메인에 대한 *인벤토리 > 네트워킹*으로 이동합니다. 기존 분산 스위치로 이동하여 *새 분산 포트 그룹...*을 만드는 작업을 선택합니다.



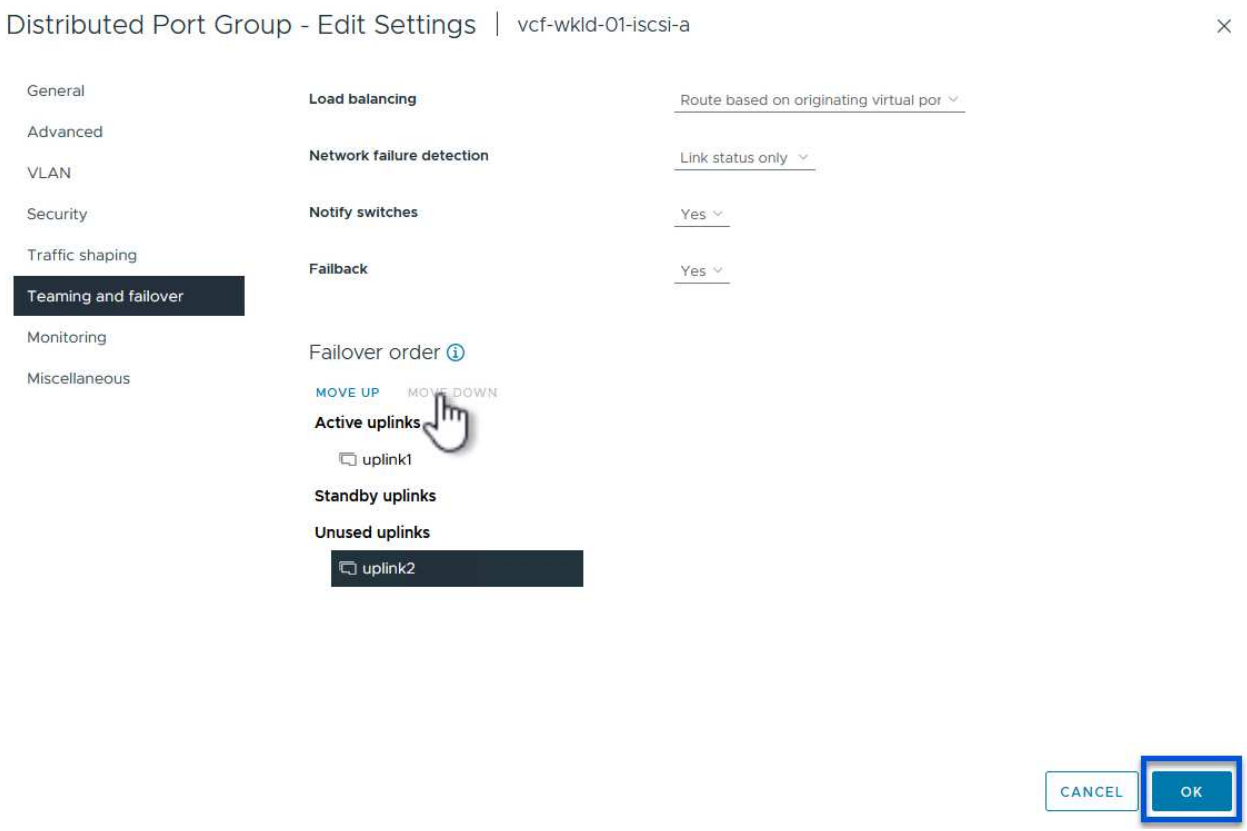
2. 새 분산 포트 그룹 마법사에서 새 포트 그룹의 이름을 입력하고 *다음*을 클릭하여 계속합니다.
3. 설정 구성 페이지에서 모든 설정을 작성하세요. VLAN을 사용하는 경우 올바른 VLAN ID를 제공해야 합니다. 계속하려면 *다음*을 클릭하세요.



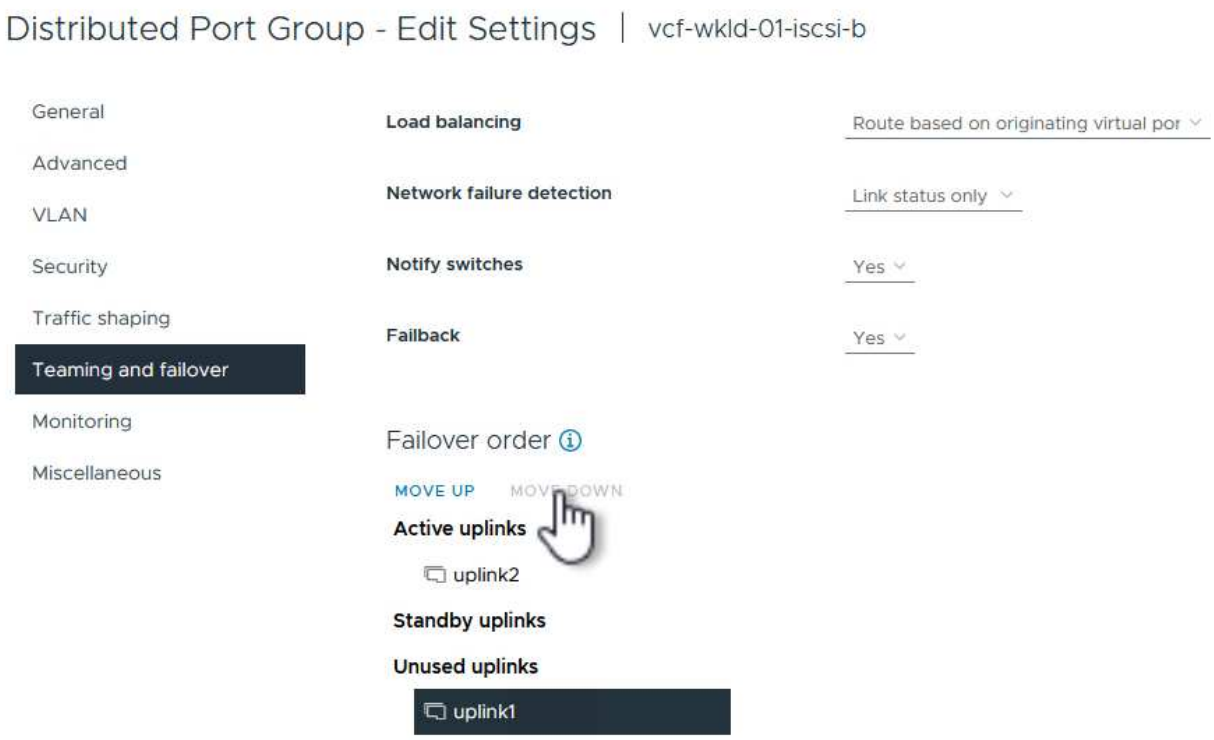
4. 완료 준비 페이지에서 변경 사항을 검토하고 *마침*을 클릭하여 새 분산 포트 그룹을 만듭니다.
5. 두 번째 iSCSI 네트워크에 사용되는 분산 포트 그룹을 생성하려면 이 프로세스를 반복하고 올바른 *VLAN ID*를 입력했는지 확인하세요.
6. 두 포트 그룹이 모두 생성되면 첫 번째 포트 그룹으로 이동하여 설정 편집... 작업을 선택합니다.



7. 분산 포트 그룹 - 설정 편집 페이지에서 왼쪽 메뉴의 *팀 구성 및 장애 조치*로 이동한 다음 *업링크2*를 클릭하여 *사용하지 않는 업링크*로 이동합니다.



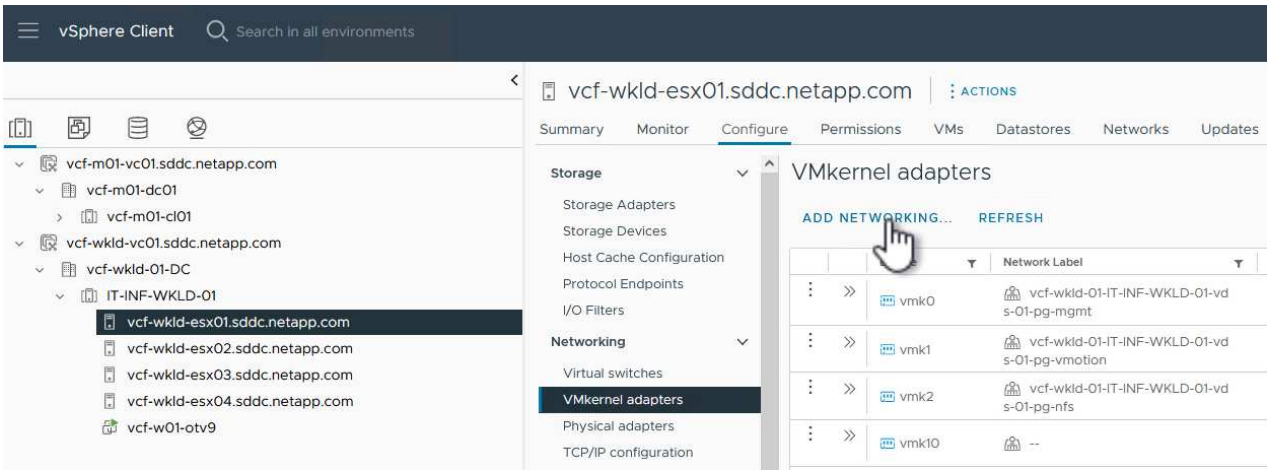
8. 두 번째 iSCSI 포트 그룹에 대해서도 이 단계를 반복합니다. 하지만 이번에는 *uplink1*을 *사용하지 않는 업링크*로 옮깁니다.



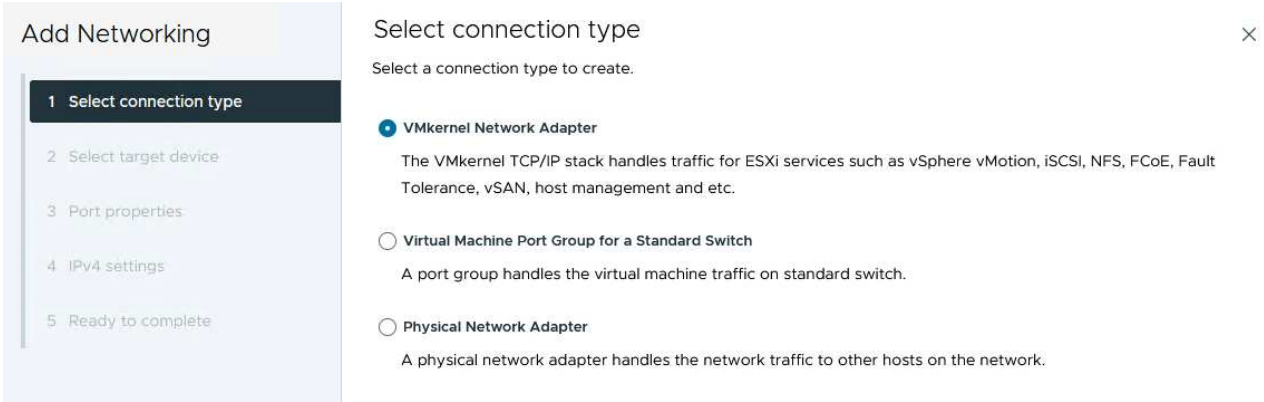
각 **ESXi** 호스트에 **VMkernel** 어댑터를 만듭니다.

워크로드 도메인의 각 ESXi 호스트에서 이 프로세스를 반복합니다.

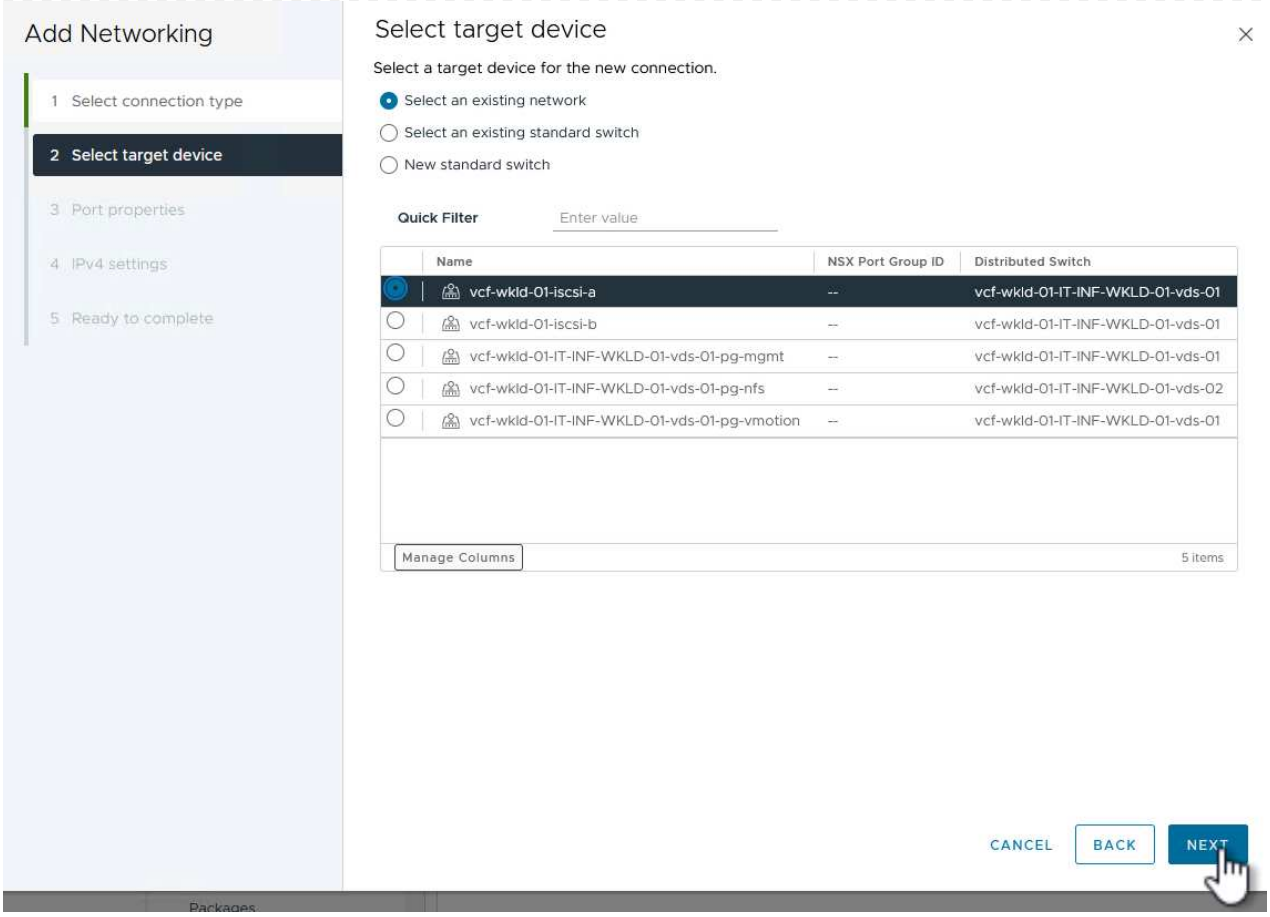
1. vSphere 클라이언트에서 워크로드 도메인 인벤토리의 ESXi 호스트 중 하나로 이동합니다. 구성 탭에서 *VMkernel 어댑터*를 선택하고 *네트워킹 추가...*를 클릭하여 시작합니다.



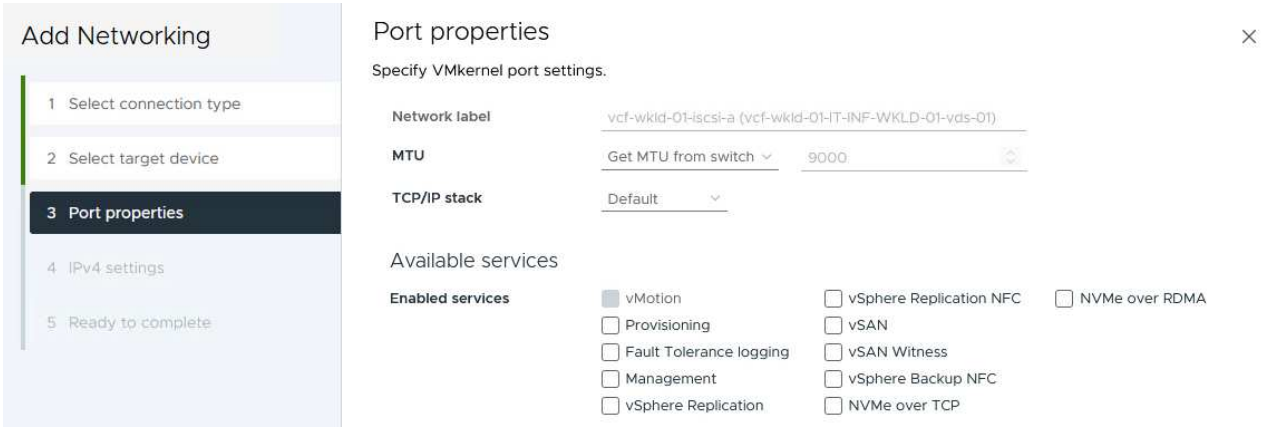
2. 연결 유형 선택 창에서 *VMkernel 네트워크 어댑터*를 선택하고 *다음*을 클릭하여 계속합니다.



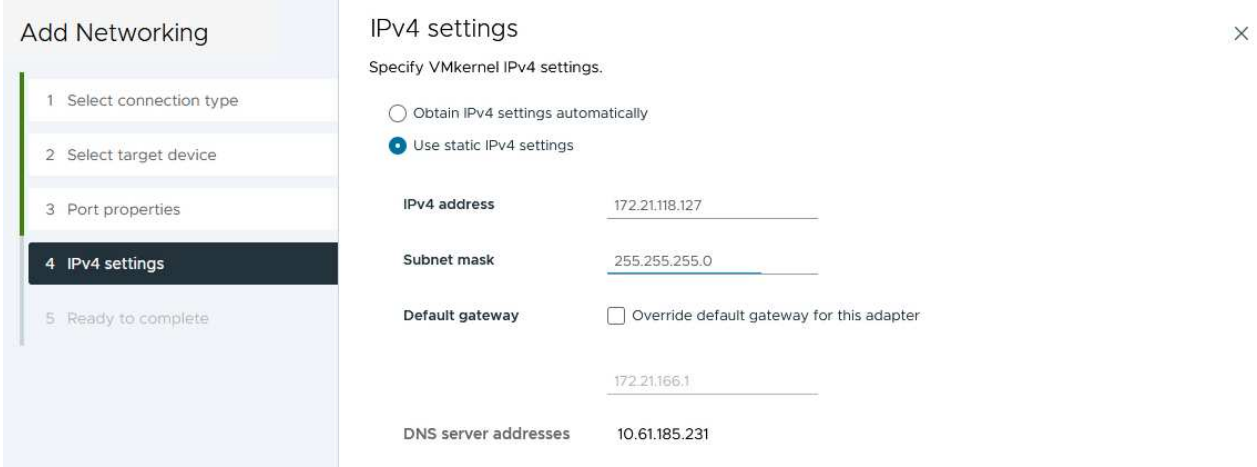
3. 대상 장치 선택 페이지에서 이전에 생성한 iSCSI용 분산 포트 그룹 중 하나를 선택합니다.



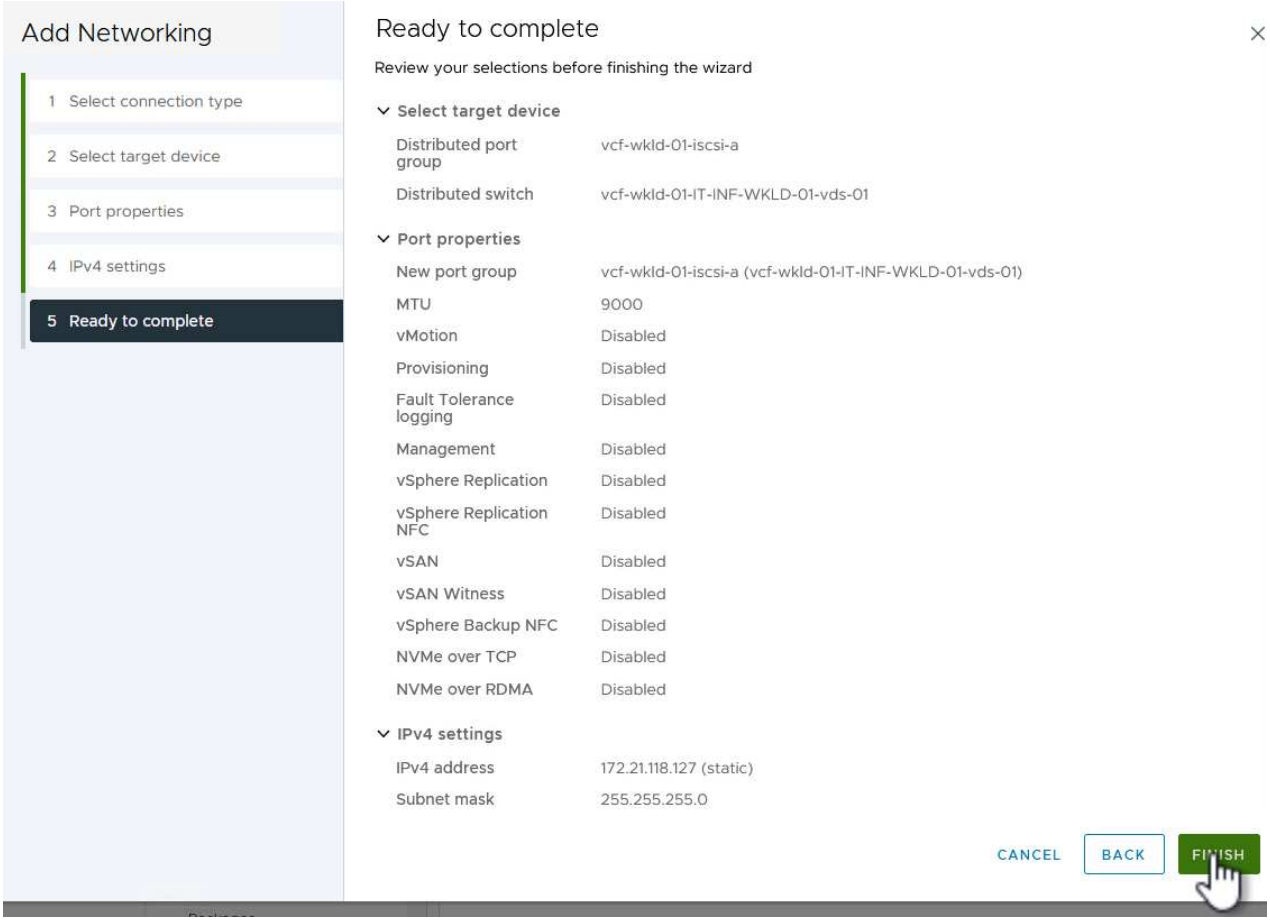
4. 포트 속성 페이지에서 기본값을 유지하고 *다음*을 클릭하여 계속합니다.



5. **IPv4** 설정 페이지에서 **IP** 주소, *서브넷 마스크*를 입력하고 새로운 게이트웨이 IP 주소를 입력합니다(필요한 경우에만). 계속하려면 *다음*을 클릭하세요.



6. 완료 준비 페이지에서 선택 사항을 검토하고 *마침*을 클릭하여 VMkernel 어댑터를 만듭니다.



7. 두 번째 iSCSI 네트워크에 대한 VMkernel 어댑터를 생성하려면 이 과정을 반복합니다.

ONTAP 도구를 배포하고 사용하여 스토리지 구성

다음 단계는 vSphere 클라이언트를 사용하여 VCF 관리 도메인 클러스터에서 수행되며 ONTAP 도구 배포, vVols

iSCSI 데이터 저장소 생성, 관리 VM을 새 데이터 저장소로 마이그레이션하는 작업을 포함합니다.

VI 워크로드 도메인의 경우 ONTAP 도구는 VCF 관리 클러스터에 설치되지만 VI 워크로드 도메인과 연결된 vCenter에 등록됩니다.

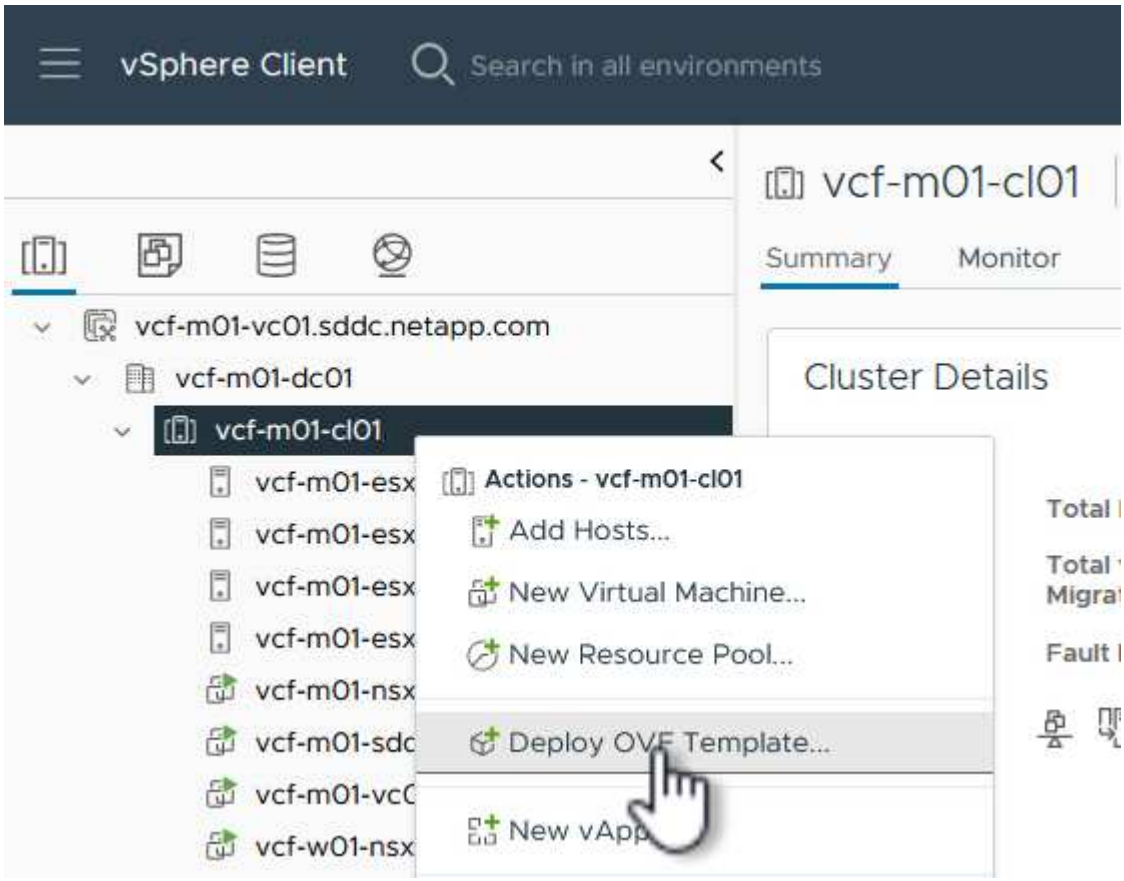
여러 vCenter 환경에서 ONTAP 도구를 배포하고 사용하는 것에 대한 추가 정보는 다음을 참조하세요."여러 vCenter Server 환경에서 ONTAP 도구를 등록하기 위한 요구 사항" .

ONTAP tools for VMware vSphere 배포

ONTAP tools for VMware vSphere VM 어플라이언스로 배포되며 ONTAP 스토리지를 관리하기 위한 통합 vCenter UI를 제공합니다.

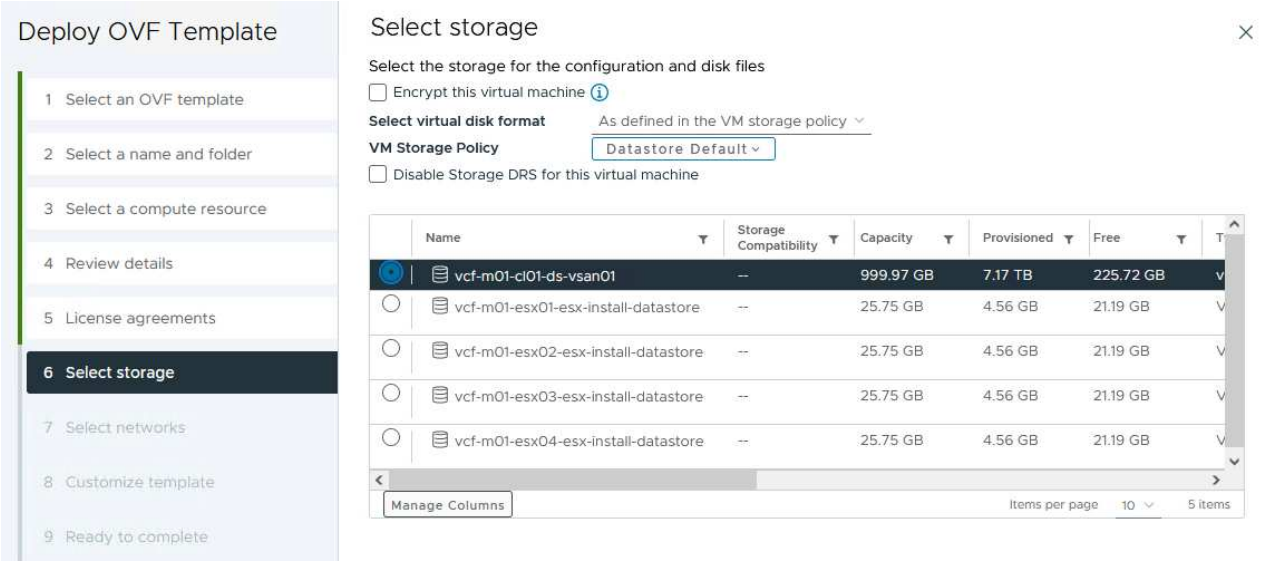
ONTAP tools for VMware vSphere 배포하려면 다음을 완료하세요.

1. ONTAP 도구 OVA 이미지를 가져옵니다."NetApp 지원 사이트" 로컬 폴더로 다운로드합니다.
2. VCF 관리 도메인의 vCenter 어플라이언스에 로그인합니다.
3. vCenter 어플라이언스 인터페이스에서 관리 클러스터를 마우스 오른쪽 버튼으로 클릭하고 *OVF 템플릿 배포…*를 선택합니다.

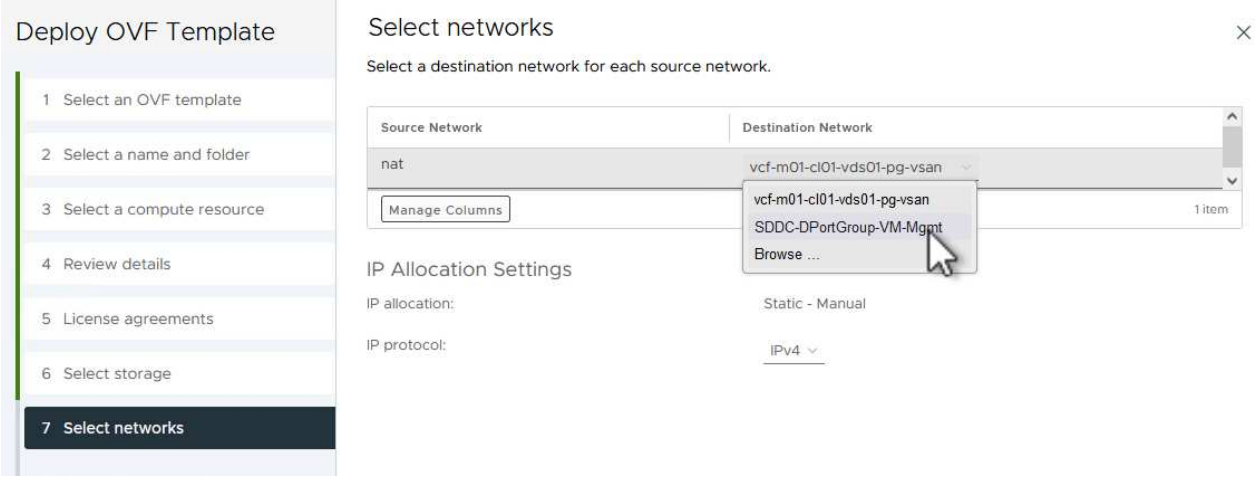


4. **OVF** 템플릿 배포 마법사에서 로컬 파일 라디오 버튼을 클릭하고 이전 단계에서 다운로드한 ONTAP 도구 OVA 파일을 선택합니다.

5. 마법사의 2~5단계에서는 VM의 이름과 폴더를 선택하고, 컴퓨팅 리소스를 선택하고, 세부 정보를 검토한 다음 라이선스 계약에 동의합니다.
6. 구성 및 디스크 파일의 저장 위치로 VCF 관리 도메인 클러스터의 vSAN 데이터 저장소를 선택합니다.

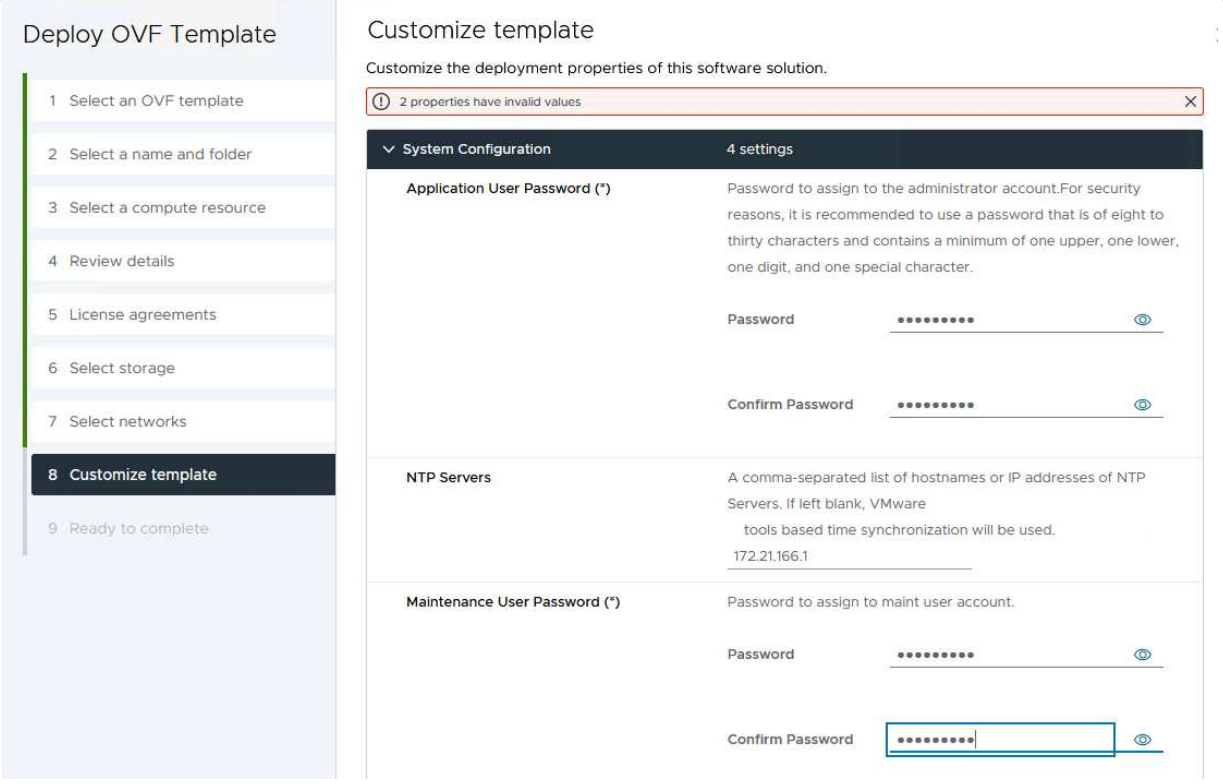


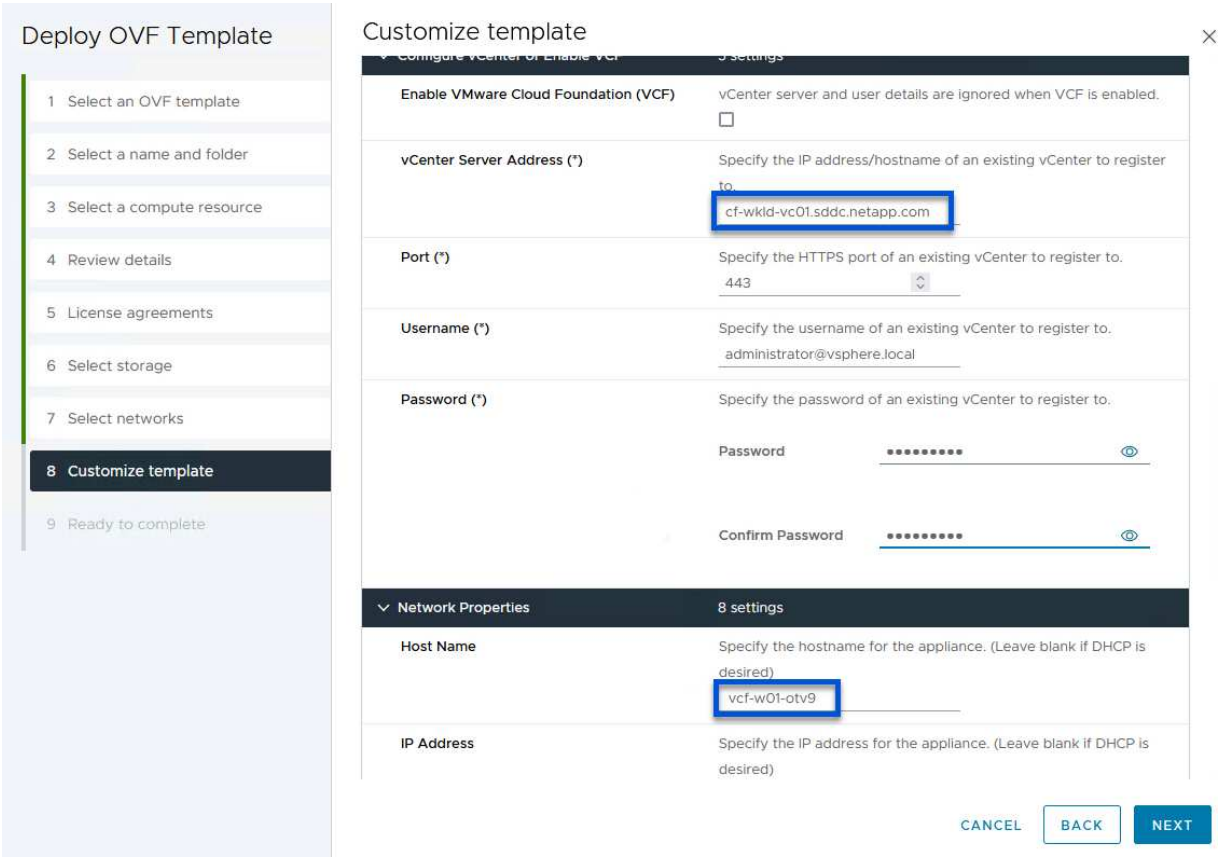
7. 네트워크 선택 페이지에서 관리 트래픽에 사용되는 네트워크를 선택합니다.



8. 사용자 정의 템플릿 페이지에서 필요한 모든 정보를 입력하세요.
   - ONTAP 도구에 대한 관리 액세스에 사용되는 비밀번호입니다.
   - NTP 서버 IP 주소.
   - ONTAP 도구 유지 관리 계정 비밀번호.
   - ONTAP 도구 Derby DB 비밀번호.
   - **VMware Cloud Foundation(VCF)** 활성화 상자를 선택하지 마세요. 보조 저장 장치를 배포하는 데 VCF 모드는 필요하지 않습니다.
   - *VI 워크로드 도메인*에 대한 vCenter 어플라이언스의 FQDN 또는 IP 주소
   - *VI 워크로드 도메인*의 vCenter 어플라이언스에 대한 자격 증명
   - 필수 네트워크 속성 필드를 제공하세요.

     계속하려면 *다음*을 클릭하세요.

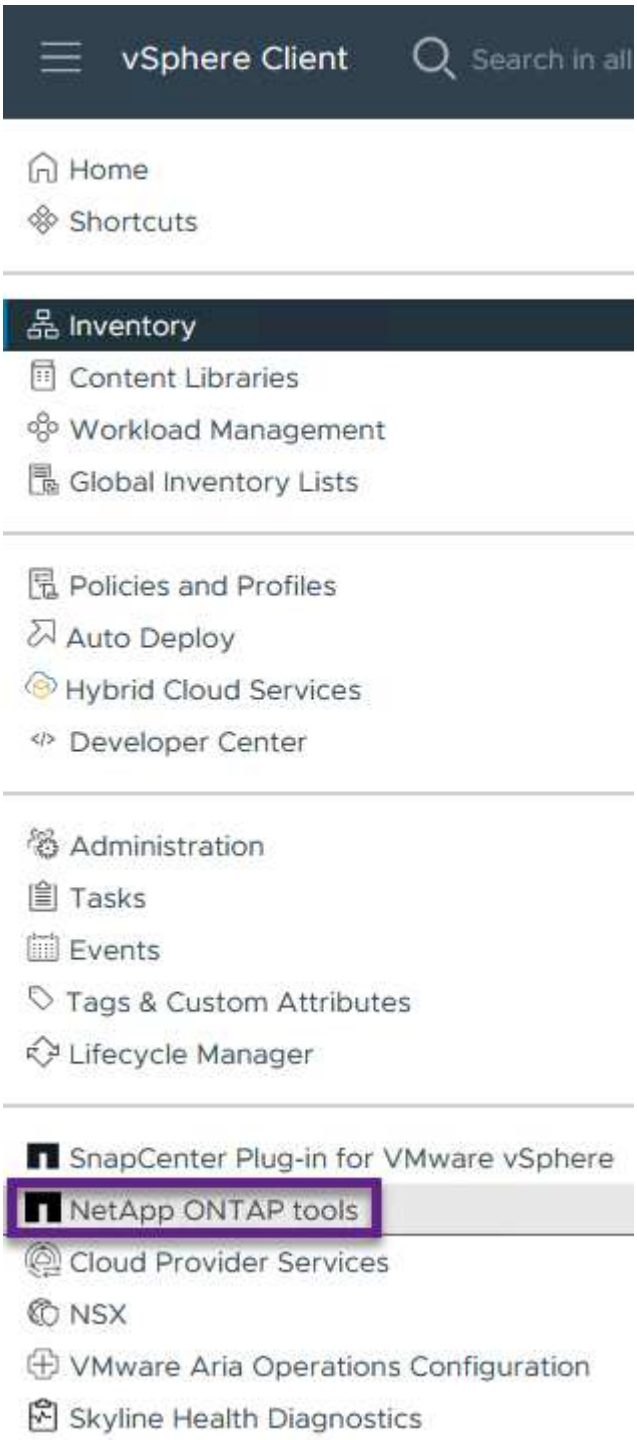




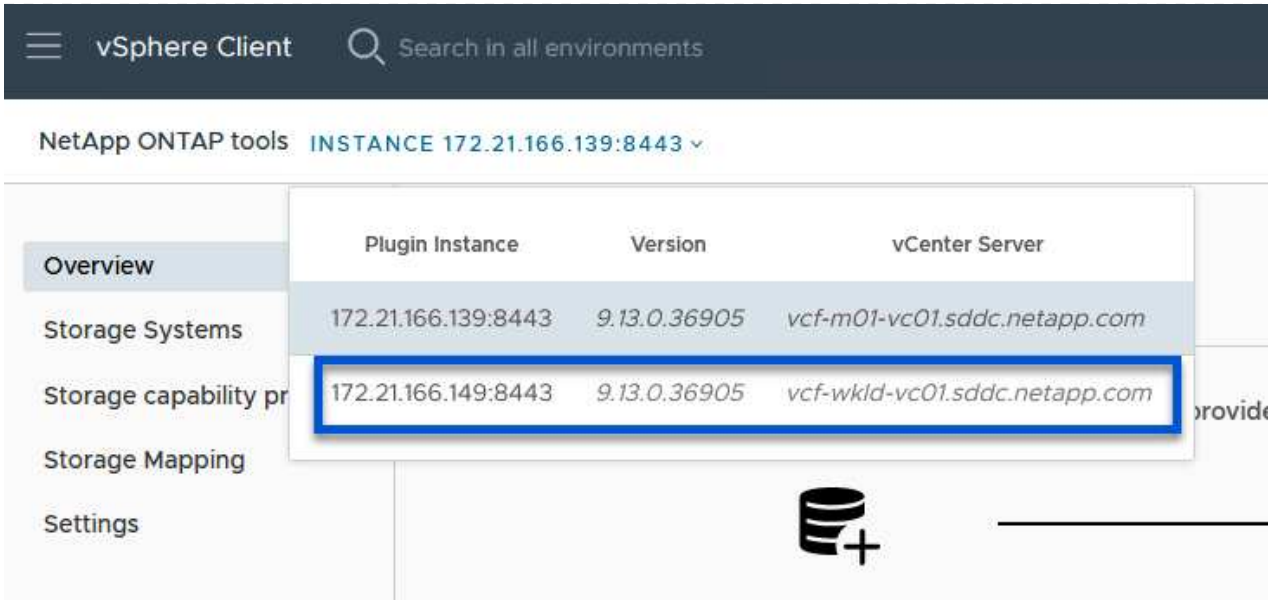
9. 완료 준비 페이지에서 모든 정보를 검토하고 마침을 클릭하여 ONTAP 도구 어플라이언스 배포를 시작합니다.

ONTAP 도구에 스토리지 시스템을 추가합니다.

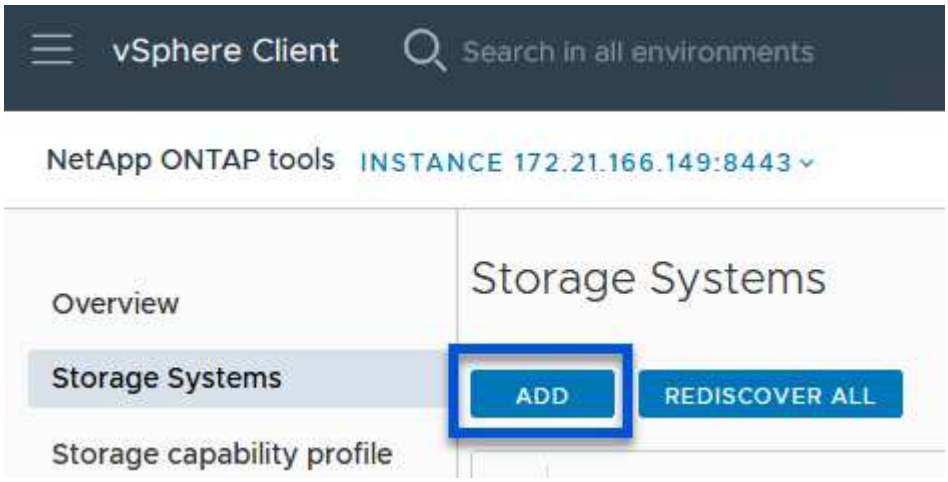
1. vSphere 클라이언트의 기본 메뉴에서 NetApp ONTAP 도구를 선택하여 액세스합니다.



2. ONTAP 도구 인터페이스의 인스턴스 드롭다운 메뉴에서 관리할 워크로드 도메인과 연결된 ONTAP 도구 인스턴스를 선택합니다.

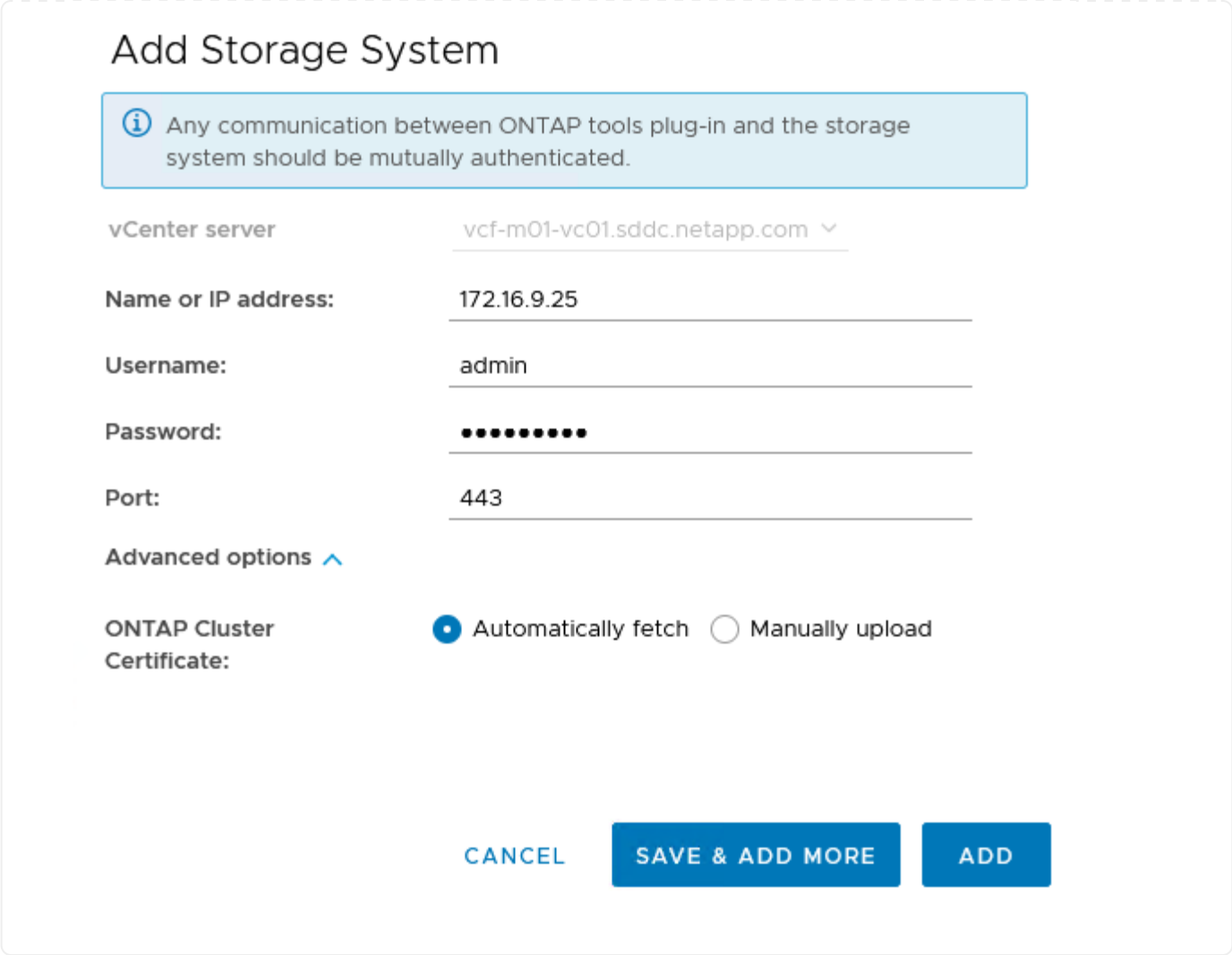


3. ONTAP 도구의 왼쪽 메뉴에서 *스토리지 시스템*을 선택한 다음 *추가*를 누릅니다.



4. IP 주소, 저장 시스템의 자격 증명, 포트 번호를 입력하세요. *추가*를 클릭하여 검색 프로세스를 시작하세요.

> vVol에는 SVM 자격 증명이 아닌 ONTAP 클러스터 자격 증명이 필요합니다. 자세한 내용은 다음을 참조하세요. "스토리지 시스템 추가" ONTAP 도구 설명서에서.

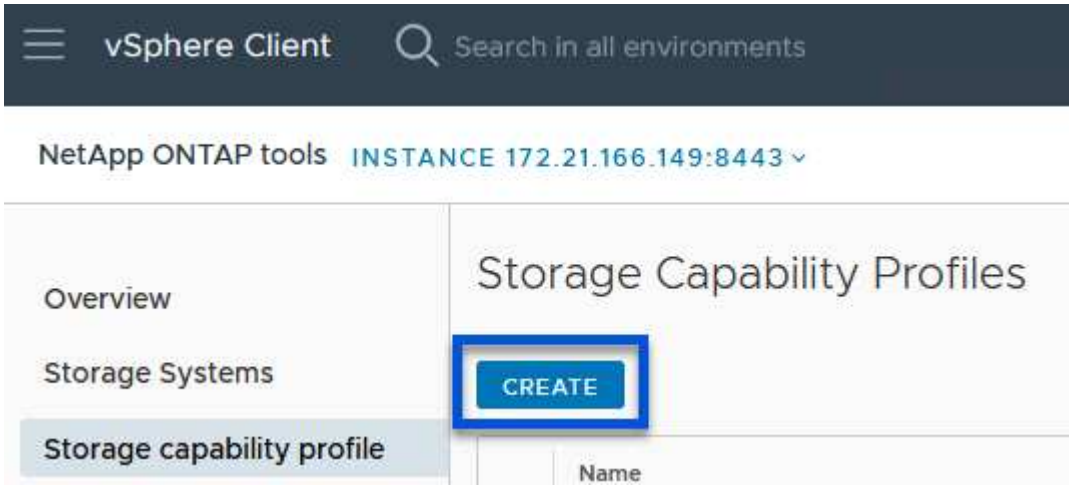

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Name or IP address:
172.16.9.25
Username:
admin
Password:
Port:
443
Advanced options
ONTAP Cluster Certificate:
Automatically fetch
Manually upload
CANCEL
SAVE & ADD MORE
ADD

ONTAP 도구에서 스토리지 기능 프로필 만들기

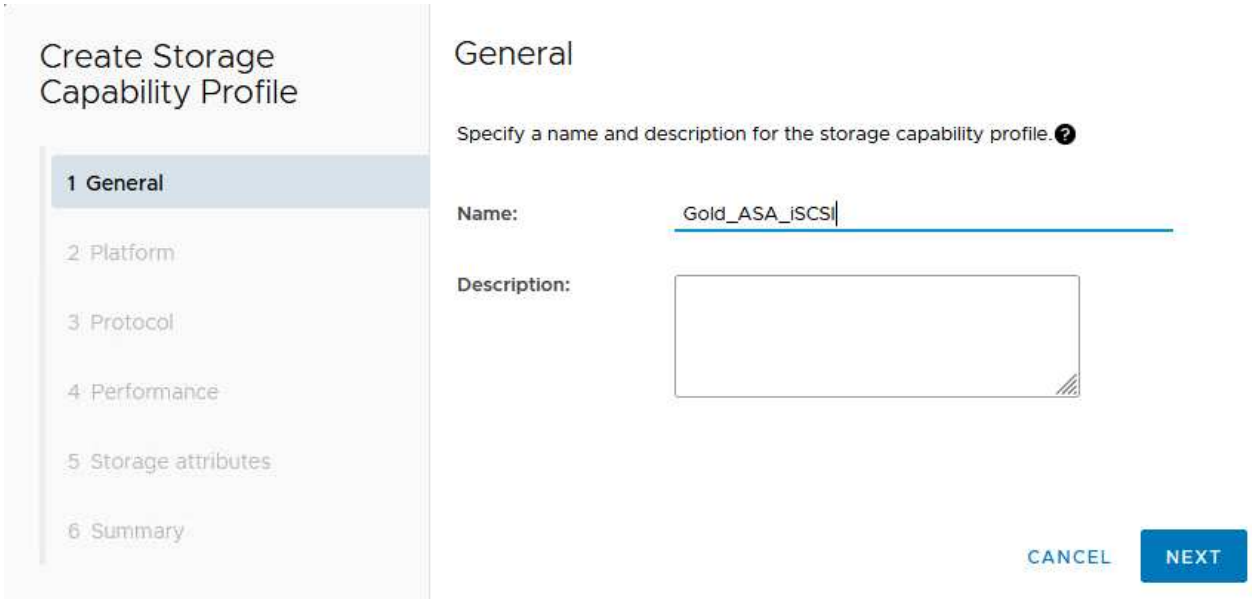
저장 기능 프로필은 저장 어레이 또는 저장 시스템이 제공하는 기능을 설명합니다. 여기에는 서비스 품질 정의가 포함되며 프로필에 정의된 매개변수를 충족하는 스토리지 시스템을 선택하는 데 사용됩니다. 제공된 프로필 중 하나를 사용하거나 새로운 프로필을 만들 수 있습니다.

ONTAP 도구에서 저장 기능 프로필을 생성하려면 다음 단계를 완료하세요.

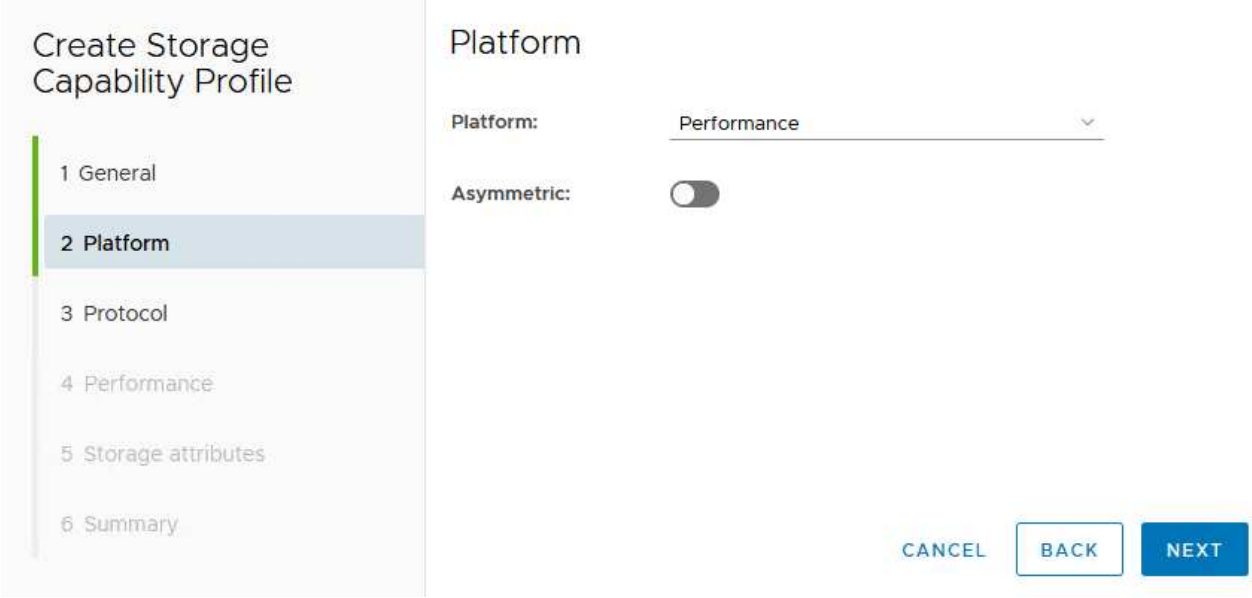
1. ONTAP 도구의 왼쪽 메뉴에서 *저장 기능 프로필*을 선택한 다음 *만들기*를 누릅니다.



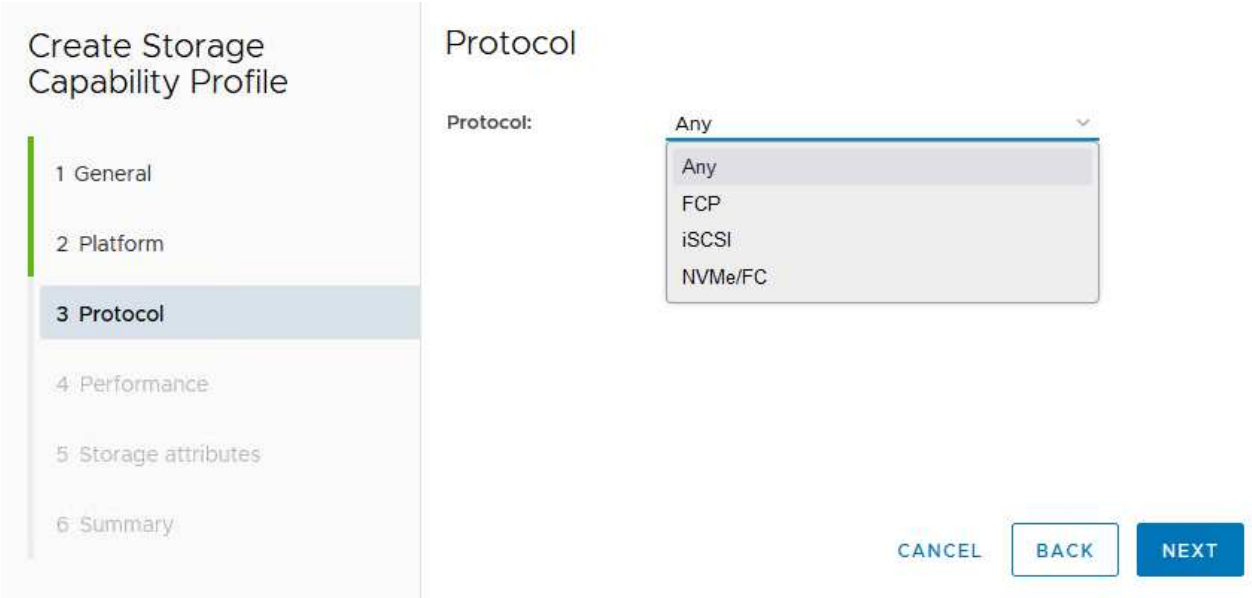
2. 저장소 기능 프로필 만들기 마법사에서 프로필의 이름과 설명을 입력하고 *다음*을 클릭합니다.



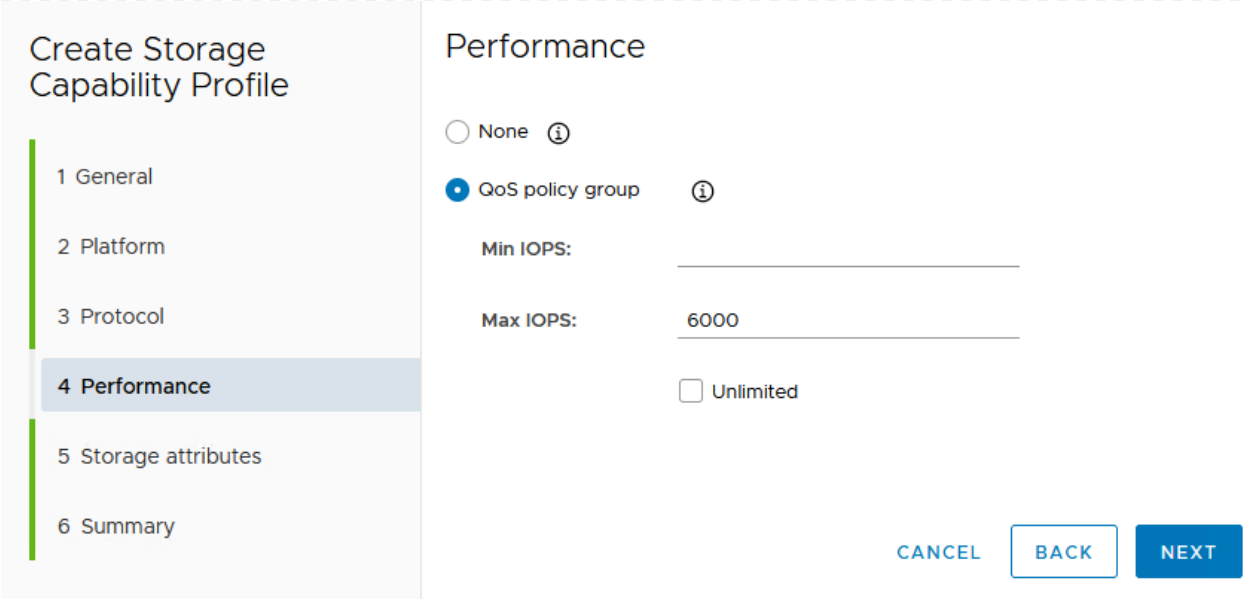
3. 플랫폼 유형을 선택하고 스토리지 시스템이 All-Flash SAN 어레이가 되도록 지정하려면 *비대칭*을 false로 설정합니다.



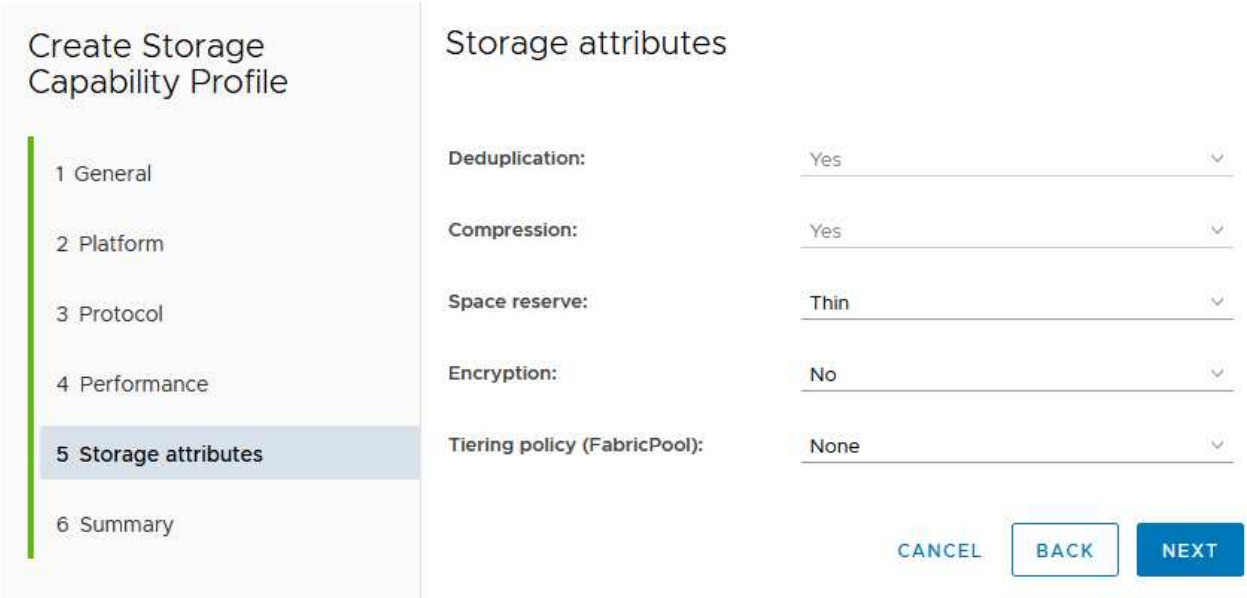
4. 다음으로, 프로토콜을 선택하거나 모든 프로토콜을 허용합니다. 계속하려면 *다음*을 클릭하세요.



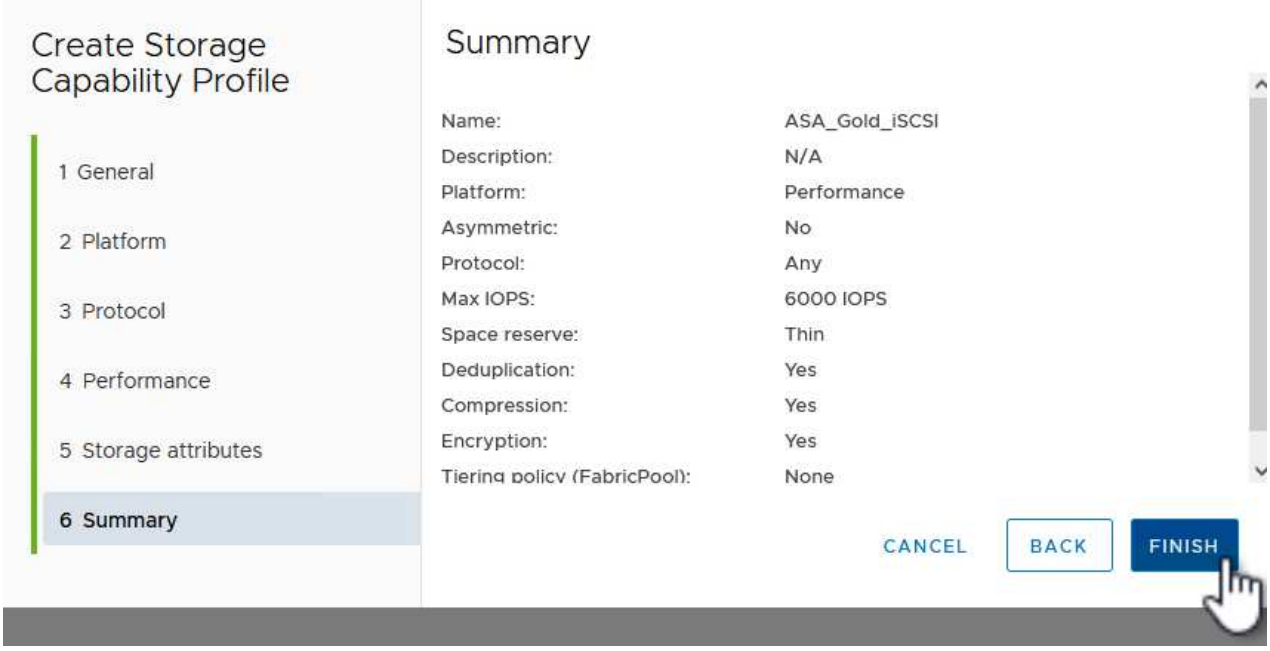
5. 성능 페이지에서는 허용되는 최소 및 최대 IOP 형태로 서비스 품질을 설정할 수 있습니다.



6. 필요에 따라 스토리지 효율성, 공간 예약, 암호화 및 계층화 정책을 선택하여 스토리지 속성 페이지를 완성합니다.



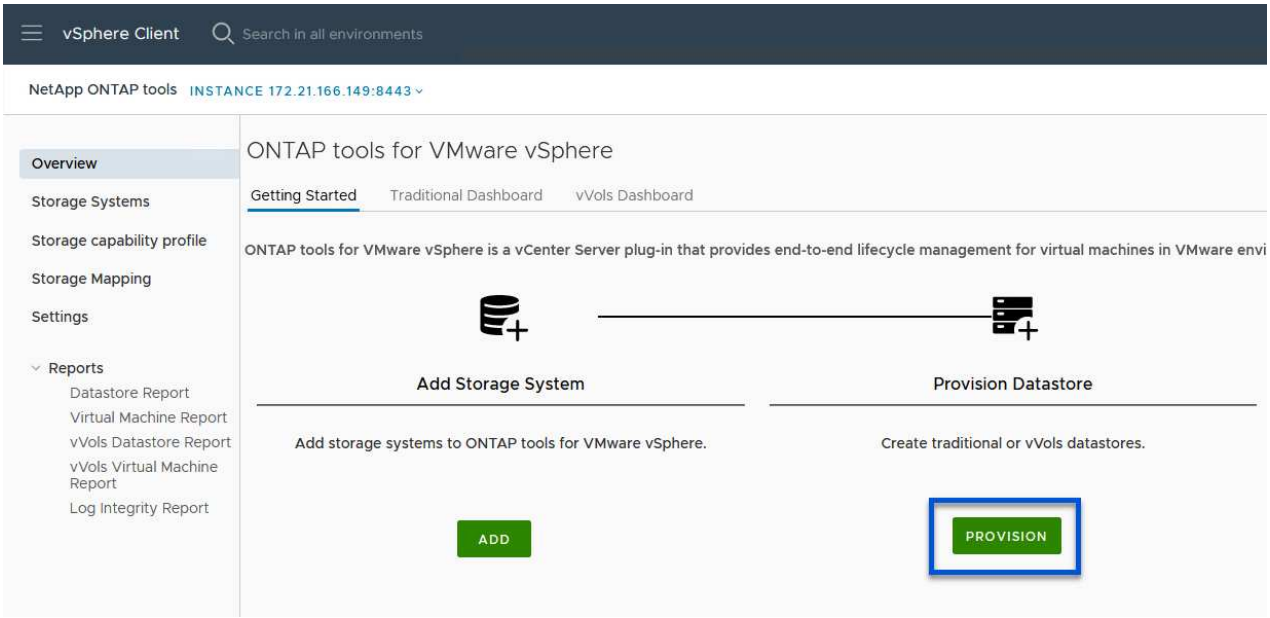
7. 마지막으로 요약을 검토하고 '마침'을 클릭하여 프로필을 만듭니다.


Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Summary
Name: ASA_Gold_iSCSI
Description: N/A
Platform: Performance
Asymmetric: No
Protocol: Any
Max IOPS: 6000 IOPS
Space reserve: Thin
Deduplication: Yes
Compression: Yes
Encryption: Yes
Tiering policy (FabricPool): None
CANCEL
BACK
FINISH

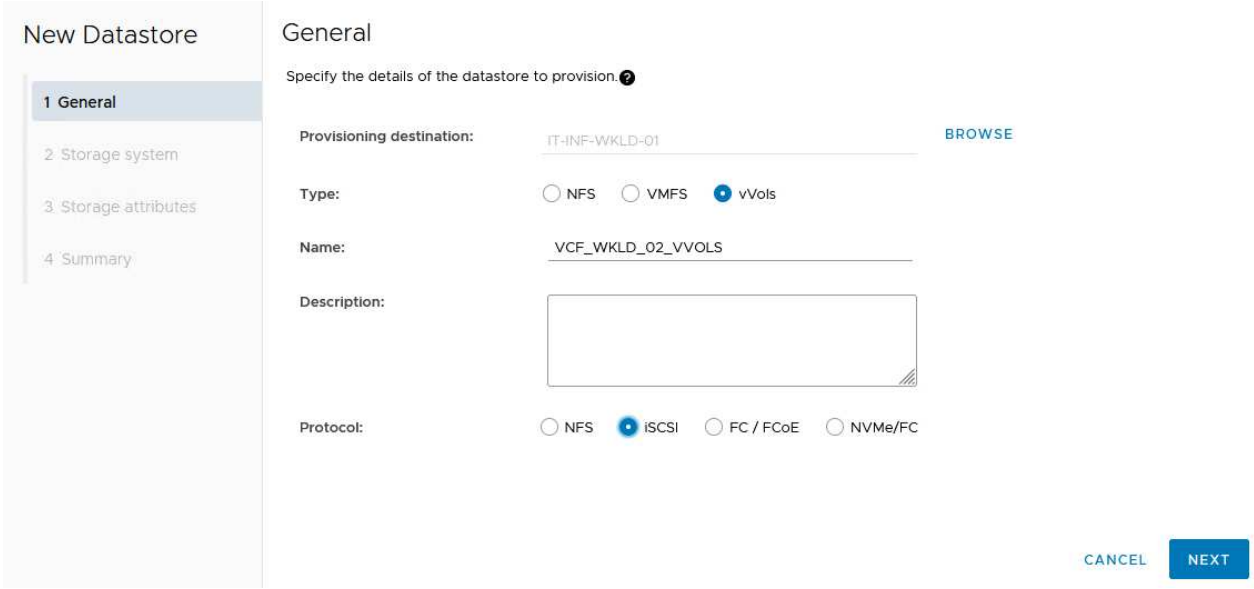
ONTAP 도구에서 **vVols** 데이터 저장소 만들기

ONTAP 도구에서 vVols 데이터 저장소를 생성하려면 다음 단계를 완료하세요.

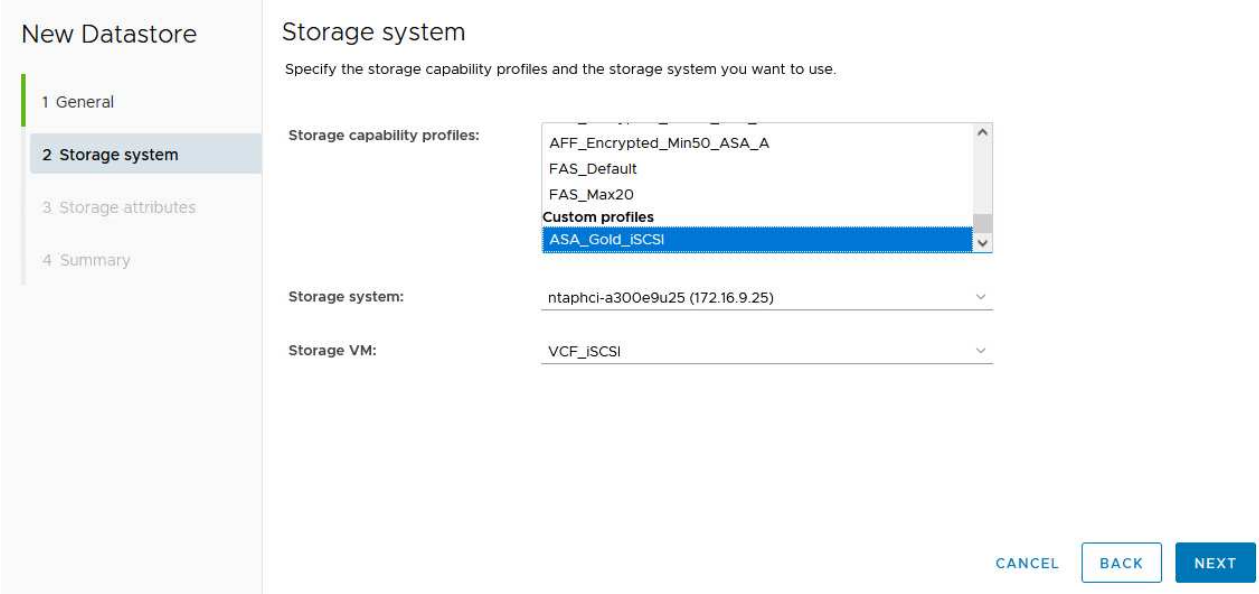
1. ONTAP 도구에서 개요*를 선택하고 *시작하기 탭에서 *프로비저닝*을 클릭하여 마법사를 시작합니다.



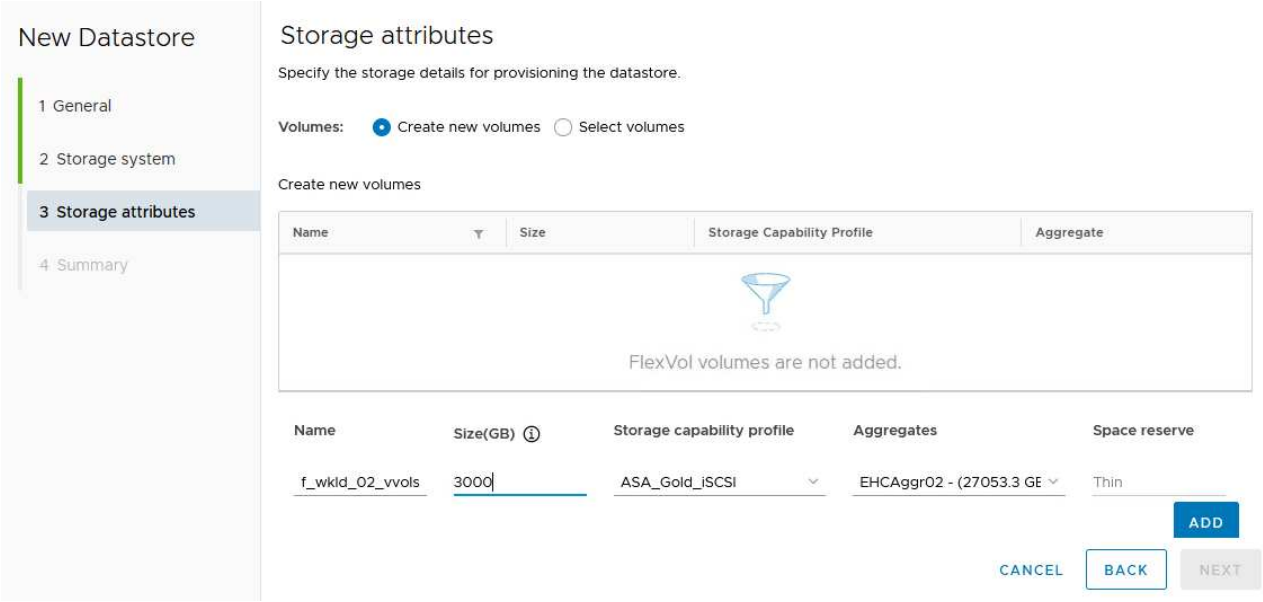
2. 새 데이터 저장소 마법사의 일반 페이지에서 vSphere 데이터 센터 또는 클러스터 대상을 선택합니다. 데이터 저장소 유형으로 * vVols*를 선택하고, 데이터 저장소의 이름을 입력하고, 프로토콜로 *iSCSI*를 선택합니다. 계속하려면 *다음*을 클릭하세요.



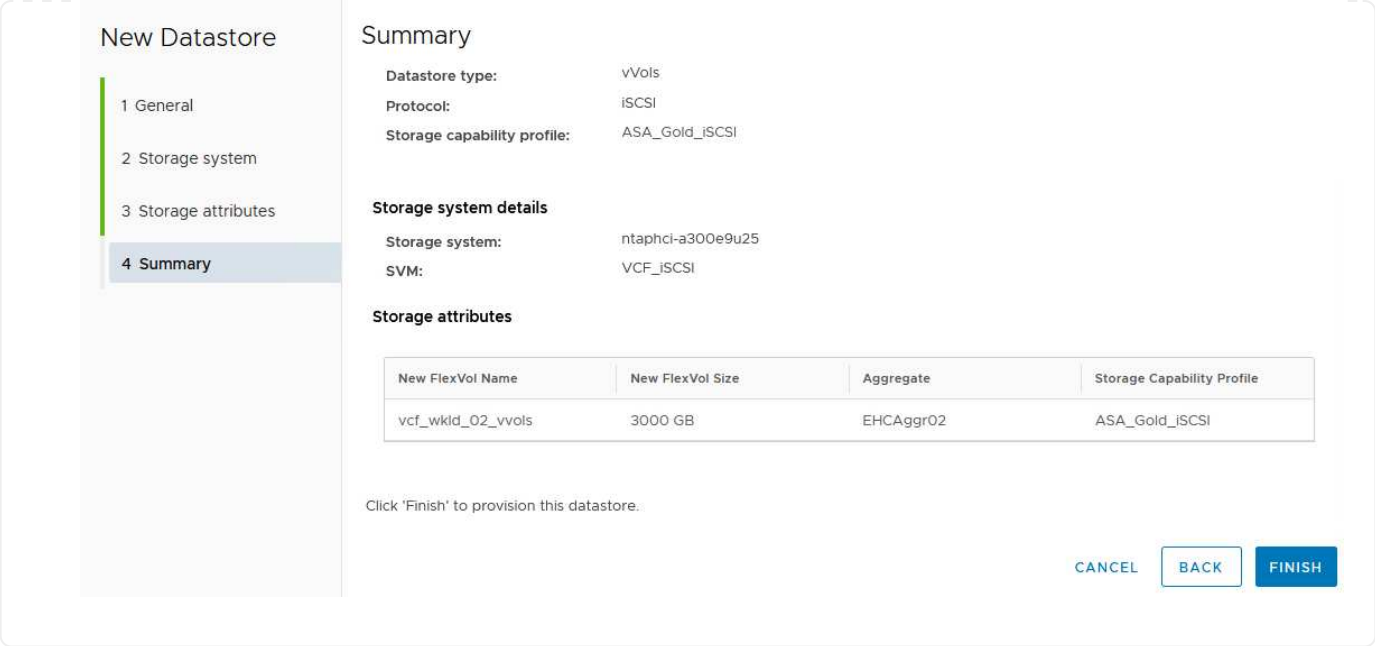
3. 스토리지 시스템 페이지에서 스토리지 용량 프로필, 스토리지 시스템 및 SVM을 선택합니다. 계속하려면 * 다음*을 클릭하세요.



4. 저장소 속성 페이지에서 데이터 저장소에 대한 새 볼륨을 생성하도록 선택하고 생성할 볼륨의 저장소 속성을 입력합니다. *추가*를 클릭하여 볼륨을 생성한 다음 *다음*을 클릭하여 계속합니다.



5. 마지막으로 요약을 검토하고 *마침*을 클릭하여 vVol 데이터 저장소 생성 프로세스를 시작합니다.



추가 정보

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

ONTAP tools for VMware vSphere 사용하여 VI 워크로드 도메인에 보충 스토리지로 NFS 및 vVols 추가

이 사용 사례에서는 ONTAP Tools for VMware를 사용하여 VMware Cloud Foundation(VCF) Virtual Infrastructure(VI) 워크로드 도메인에 대한 보조 스토리지로 NFS 및 vVols 데이터 저장소를 추가하는 절차를 설명합니다. 이 절차에서는 VMware vSphere에 ONTAP 도구를 배포하고, NFS 논리 인터페이스를 사용하여 SVM(스토리지 가상 머신)을 구성하고, NFS 및 vVols 데이터 저장소를 프로비저닝하는 방법을 요약합니다.

*NFS*는 vVols 데이터 저장소의 저장 프로토콜로 사용됩니다.

NFS의 이점

간단하고 사용 용이성**:** NFS는 설정과 관리가 간단하므로 빠르고 쉽게 파일을 공유해야 하는 환경에 매우 적합한 선택입니다.

확장성**:** ONTAP의 아키텍처는 NFS가 효율적으로 확장되어 인프라를 크게 변경하지 않고도 증가하는 데이터 요구 사항을 지원할 수 있도록 해줍니다.

유연성**:** NFS는 광범위한 애플리케이션과 작업 부하를 지원하므로 가상화된 환경을 포함한 다양한 사용 사례에 다양하게 활용할 수 있습니다.

자세한 내용은 다음을 참조하세요. "vSphere 8용 NFS v3 참조 가이드" .

시나리오 개요

이 시나리오에서는 다음과 같은 상위 수준 단계를 다룹니다.

- NFS 트래픽을 위한 논리 인터페이스(LIF)가 있는 스토리지 가상 머신(SVM)을 만듭니다.
- VI 워크로드 도메인에서 NFS 네트워크에 대한 분산 포트 그룹을 만듭니다.
- VI 워크로드 도메인의 ESXi 호스트에서 NFS용 vmkernel 어댑터를 생성합니다.
- VI 워크로드 도메인에 ONTAP 도구를 배포합니다.
- VI 워크로드 도메인에 새로운 NFS 데이터 저장소를 만듭니다.
- VI 워크로드 도메인에 새로운 vVols 데이터 저장소를 만듭니다.

필수 조건

이 시나리오에는 다음과 같은 구성 요소와 구성이 필요합니다.

- 스토리지 트래픽에 전용된 이더넷 스위치의 물리적 데이터 포트를 갖춘 ONTAP AFF 또는 FAS 스토리지 시스템입니다.
- VCF 관리 도메인 배포가 완료되었으며 vSphere 클라이언트에 액세스할 수 있습니다.
- VI 워크로드 도메인이 이전에 배포되었습니다.

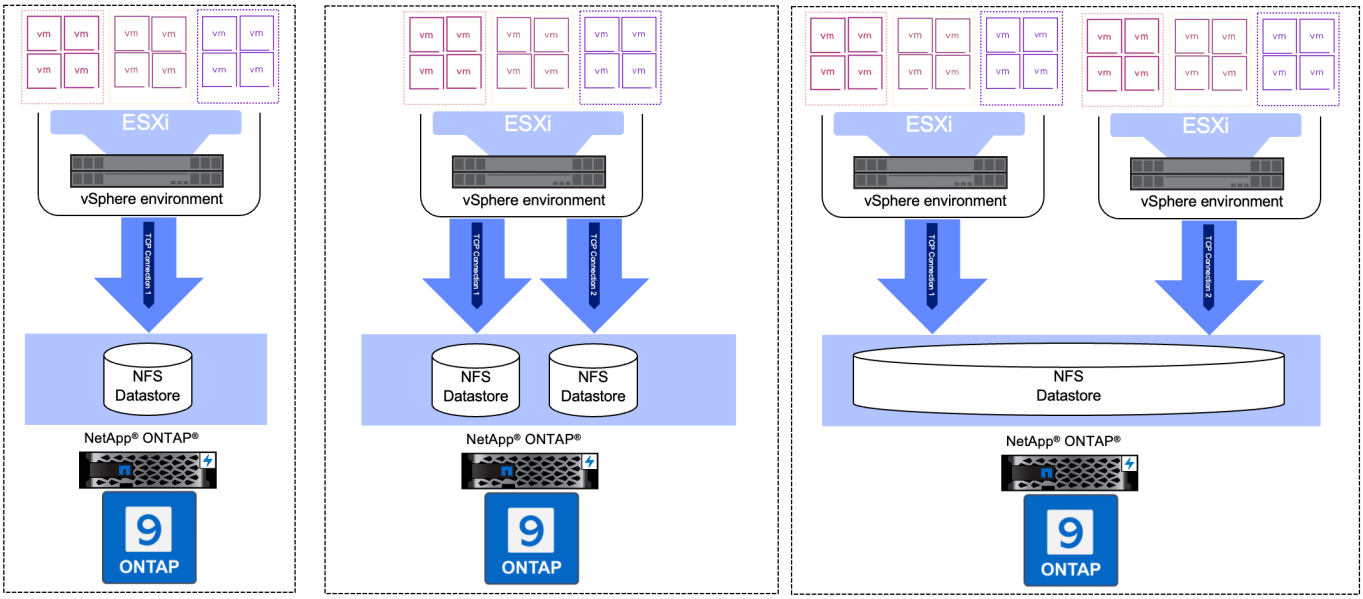
NetApp 스토리지 시스템, 스위치, 네트워크 어댑터 및 호스트 시스템에 대한 내결함성을 제공하는 NFS에 대한 중복 네트워크 설계를 권장합니다. 아키텍처 요구 사항에 따라 단일 서브넷이나 여러 서브넷으로 NFS를 배포하는 것이 일반적입니다.

참조하다 "VMware vSphere를 사용하여 NFS를 실행하기 위한 모범 사례" VMware vSphere에 대한 자세한 정보는 다음을 참조하세요.

VMware vSphere와 함께 ONTAP 사용하는 것에 대한 네트워크 지침은 다음을 참조하세요. "네트워크 구성 - NFS" NetApp 엔터프라이즈 애플리케이션 설명서의 섹션입니다.

이 문서에서는 새로운 SVM을 생성하고 NFS 트래픽에 대한 여러 LIF를 생성하기 위해 IP 주소 정보를 지정하는 프로세스를 보여줍니다. 기존 SVM에 새로운 LIF를 추가하려면 다음을 참조하세요."LIF(네트워크 인터페이스) 생성" .

vSphere 클러스터에서 NFS를 사용하는 것에 대한 전체 정보는 다음을 참조하십시오."vSphere 8용 NFS v3 참조 가이드" .



배포 단계

ONTAP 도구를 배포하고 이를 사용하여 VCF 관리 도메인에 vVols 및 NFS 데이터 저장소를 생성하려면 다음 단계를 완료하세요.

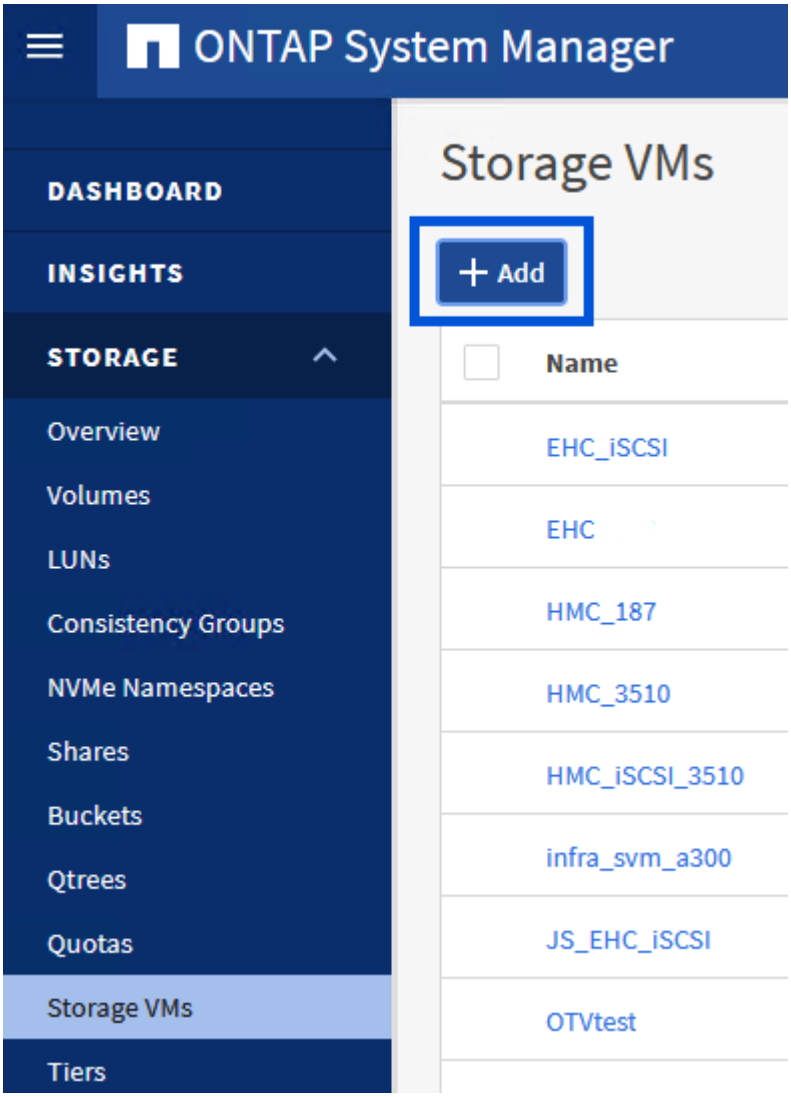
ONTAP 스토리지 시스템에 **SVM** 및 **LIF** 생성

다음 단계는 ONTAP 시스템 관리자에서 수행됩니다.

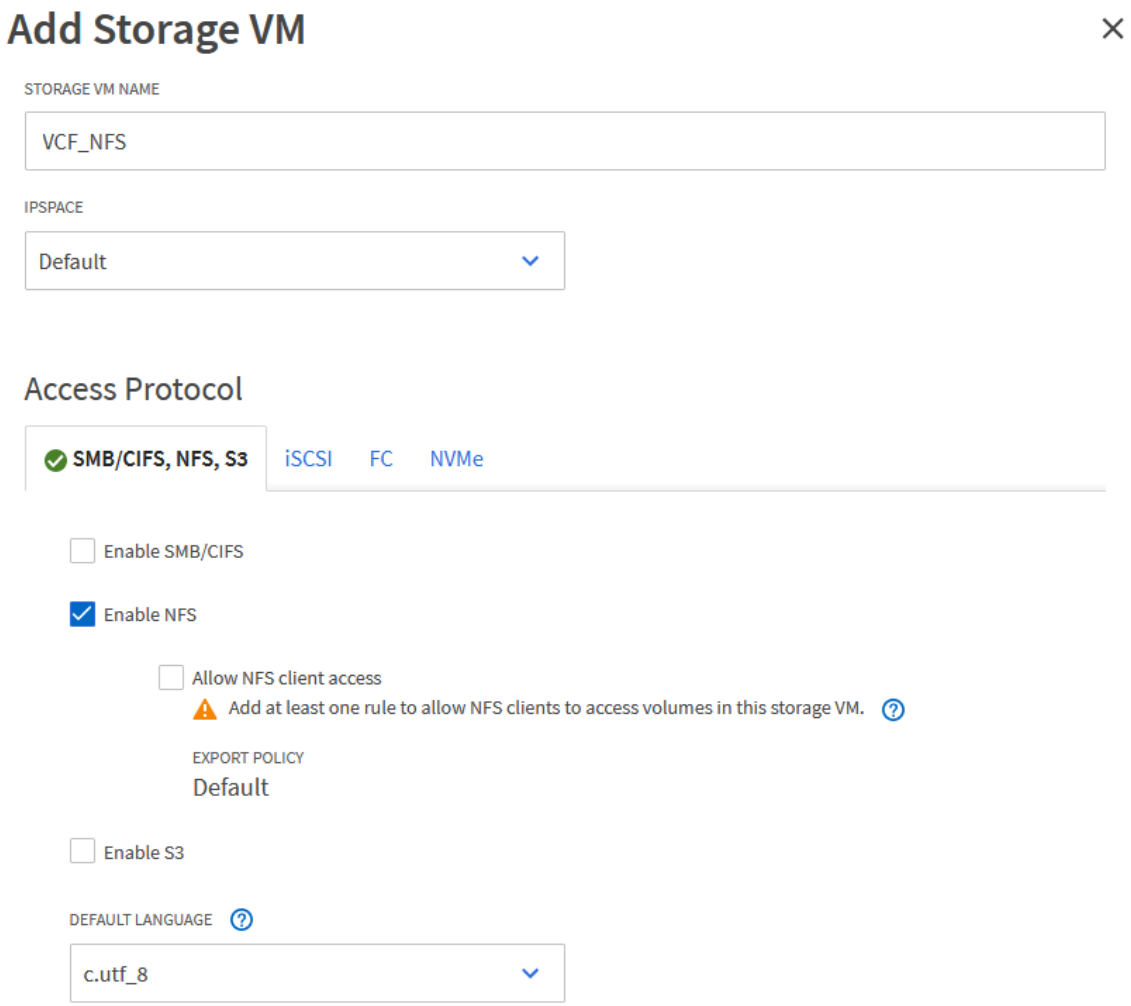
스토리지 **VM** 및 **LIF** 생성

NFS 트래픽을 위한 여러 LIF와 함께 SVM을 생성하려면 다음 단계를 완료하세요.

1. ONTAP System Manager에서 왼쪽 메뉴의 *Storage VMs*로 이동한 다음 *+ 추가*를 클릭하여 시작합니다.

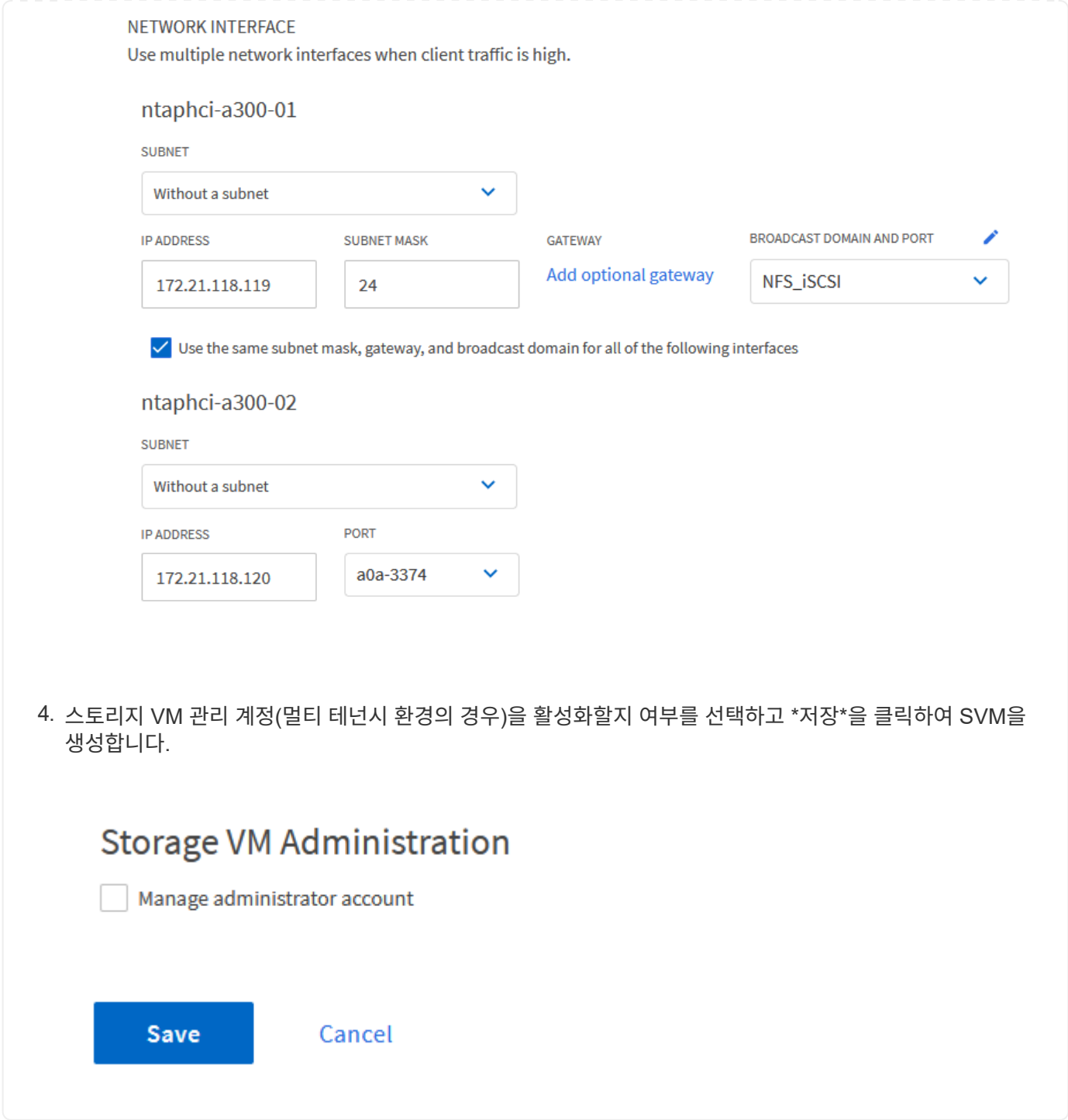


2. 스토리지 **VM** 추가 마법사에서 SVM의 이름*을 입력하고, ***IP** 공간*을 선택한 다음, *액세스 프로토콜*에서 ***SMB/CIFS, NFS, S3** 탭을 클릭하고 **NFS** 사용 확인란을 선택합니다.



여기에서는 **NFS** 클라이언트 액세스 허용 버튼을 선택할 필요가 없습니다. VMware vSphere용 Ontap Tools를 사용하여 데이터 저장소 배포 프로세스를 자동화합니다. 여기에는 ESXi 호스트에 대한 클라이언트 액세스를 제공하는 것이 포함됩니다.

3. 네트워크 인터페이스 섹션에 첫 번째 LIF에 대한 **IP** 주소, 서브넷 마스크, *브로드캐스트 도메인 및 포트*를 입력합니다. 이후 LIF의 경우 확인란을 활성화하여 나머지 모든 LIF에서 공통 설정을 사용하거나 별도의 설정을 사용할 수 있습니다.



4. 스토리지 VM 관리 계정(멀티 테넌시 환경의 경우)을 활성화할지 여부를 선택하고 *저장*을 클릭하여 SVM을 생성합니다.

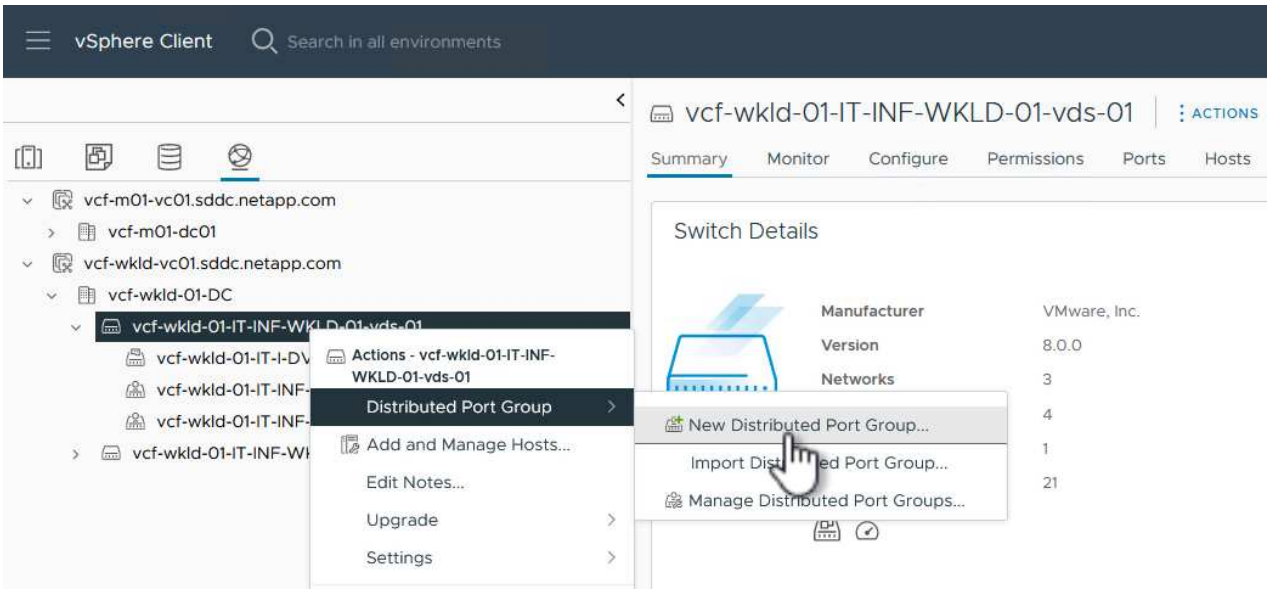
ESXi 호스트에서 **NFS**에 대한 네트워킹 설정

다음 단계는 vSphere 클라이언트를 사용하여 VI 워크로드 도메인 클러스터에서 수행됩니다. 이 경우 vCenter Single Sign-On이 사용되므로 vSphere 클라이언트는 관리 및 워크로드 도메인에서 공통적입니다.

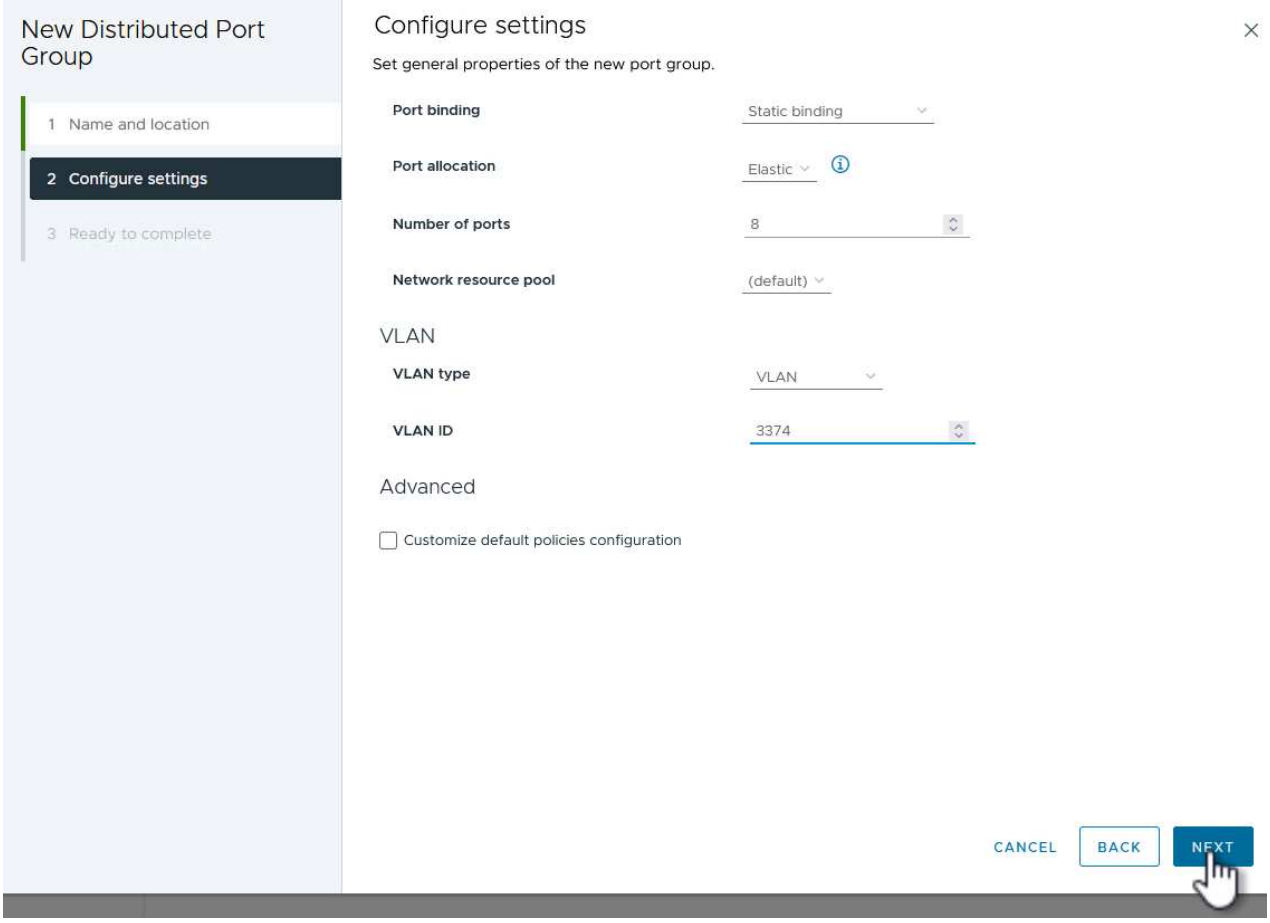
NFS 트래픽을 위한 분산 포트 그룹 생성

네트워크에서 NFS 트래픽을 전송할 새로운 분산 포트 그룹을 만들려면 다음을 완료하세요.

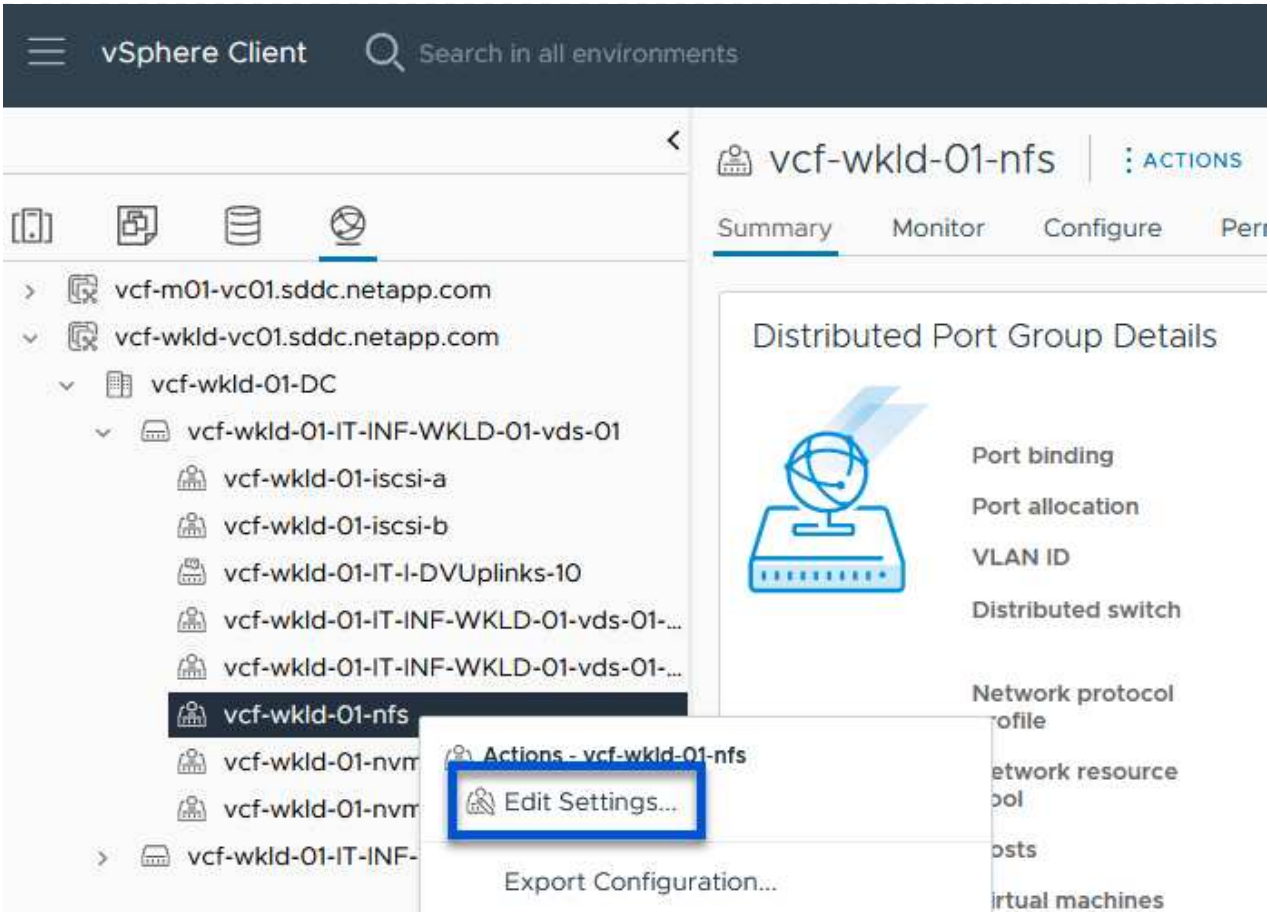
1. vSphere 클라이언트에서 워크로드 도메인에 대한 *인벤토리 > 네트워킹*으로 이동합니다. 기존 분산 스위치로 이동하여 *새 분산 포트 그룹...*을 만드는 작업을 선택합니다.



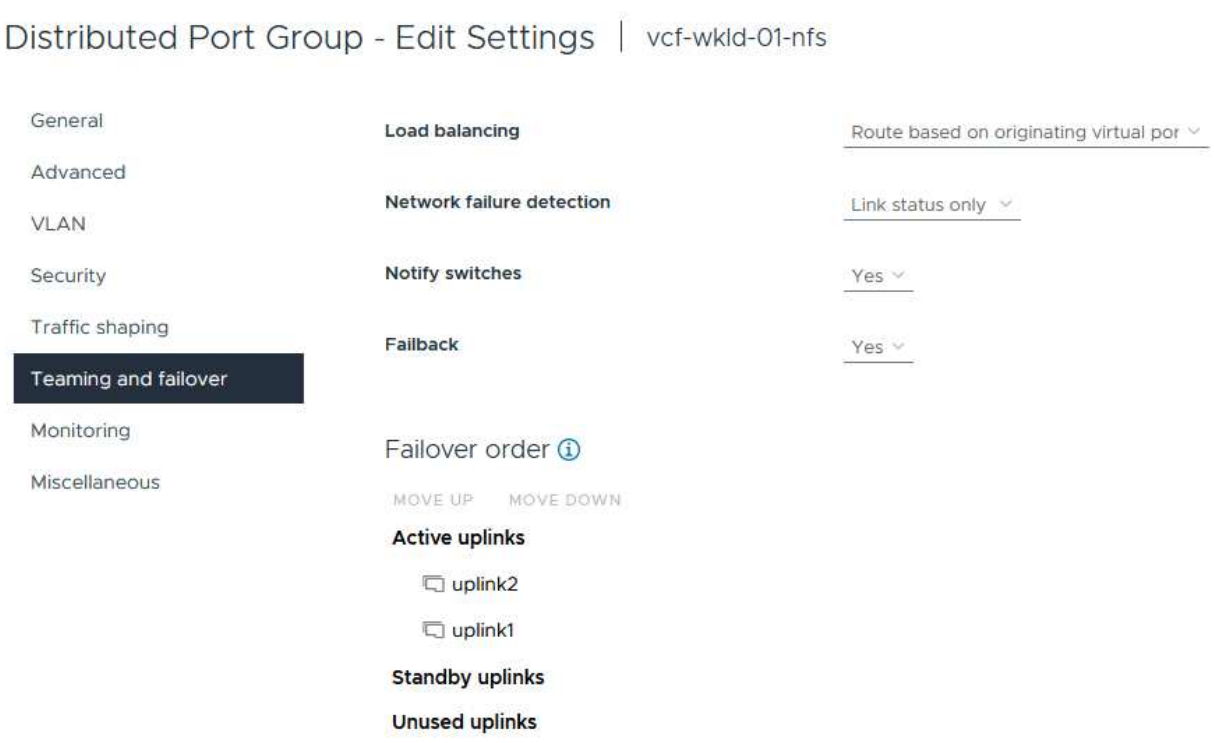
2. 새 분산 포트 그룹 마법사에서 새 포트 그룹의 이름을 입력하고 *다음*을 클릭하여 계속합니다.
3. 설정 구성 페이지에서 모든 설정을 작성하세요. VLAN을 사용하는 경우 올바른 VLAN ID를 제공해야 합니다. 계속하려면 *다음*을 클릭하세요.



4. 완료 준비 페이지에서 변경 사항을 검토하고 *마침*을 클릭하여 새 분산 포트 그룹을 만듭니다.
5. 포트 그룹이 생성되면 포트 그룹으로 이동하여 설정 편집... 작업을 선택합니다.



6. 분산 포트 그룹 - 설정 편집 페이지에서 왼쪽 메뉴의 팀 구성 및 장애 조치*로 이동합니다. **NFS** 트래픽에 사용할 업링크의 티밍을 활성화하려면 *활성 업링크 영역에 함께 있어야 합니다. 사용하지 않는 업링크를 *사용하지 않는 업링크*로 옮깁니다.

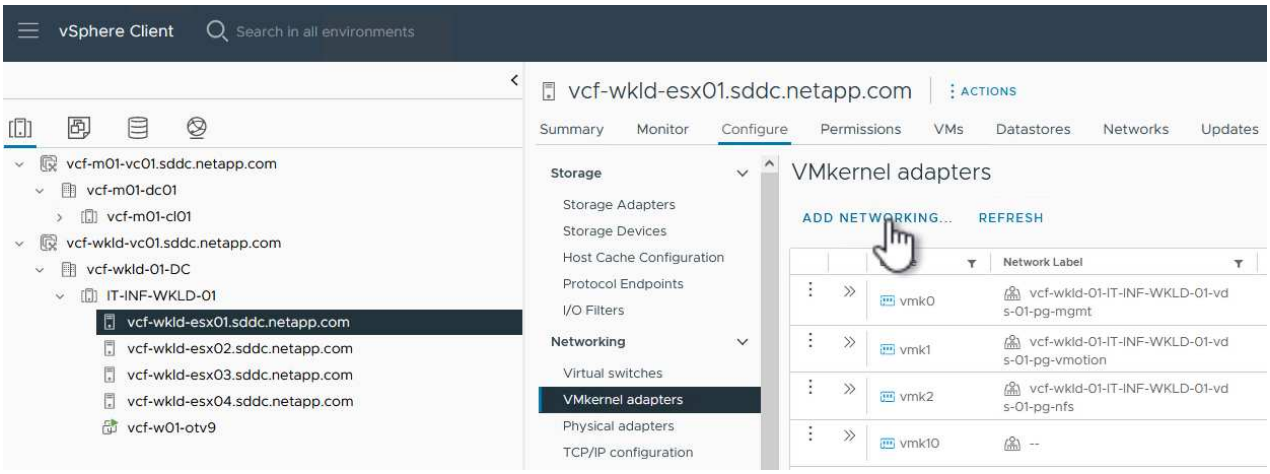


7. 클러스터의 각 ESXi 호스트에 대해 이 프로세스를 반복합니다.

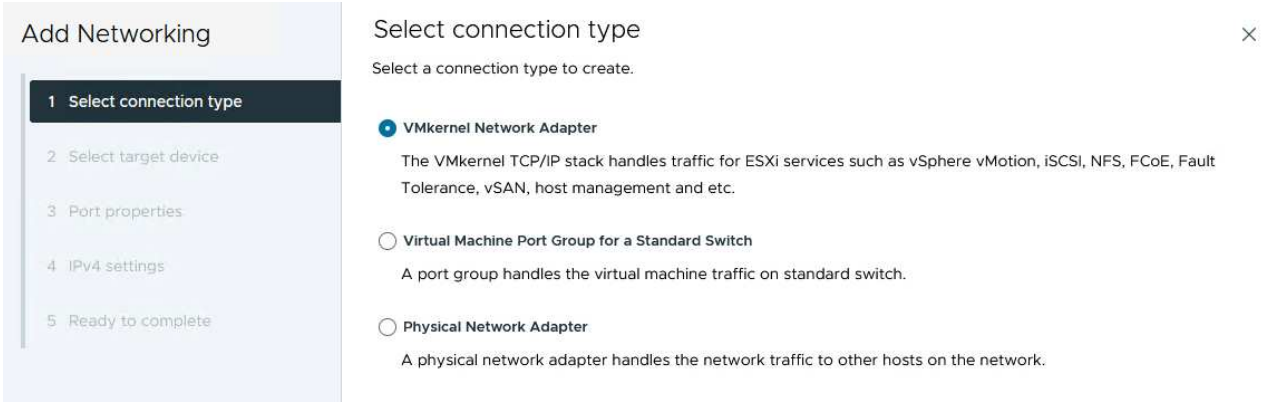
각 **ESXi** 호스트에 **VMkernel** 어댑터를 만듭니다.

워크로드 도메인의 각 ESXi 호스트에서 이 프로세스를 반복합니다.

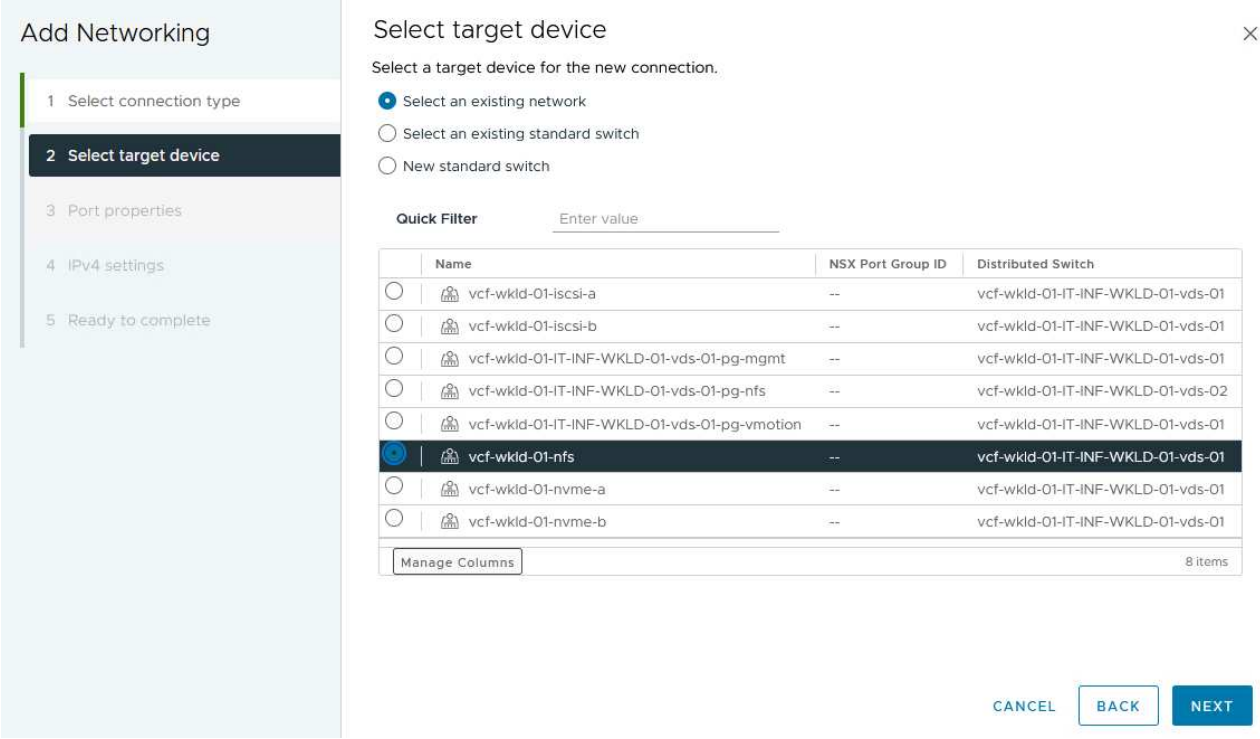
1. vSphere 클라이언트에서 워크로드 도메인 인벤토리의 ESXi 호스트 중 하나로 이동합니다. 구성 탭에서 *VMkernel 어댑터*를 선택하고 *네트워킹 추가...*를 클릭하여 시작합니다.



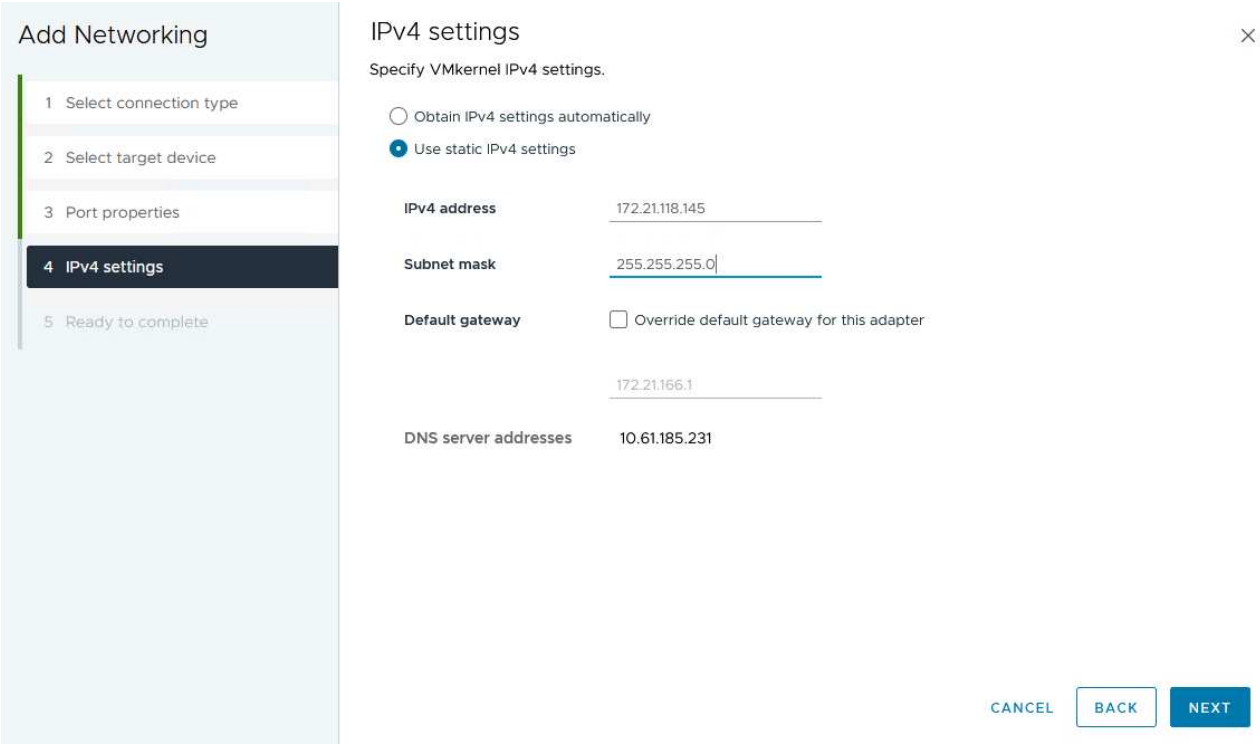
2. 연결 유형 선택 창에서 *VMkernel 네트워크 어댑터*를 선택하고 *다음*을 클릭하여 계속합니다.



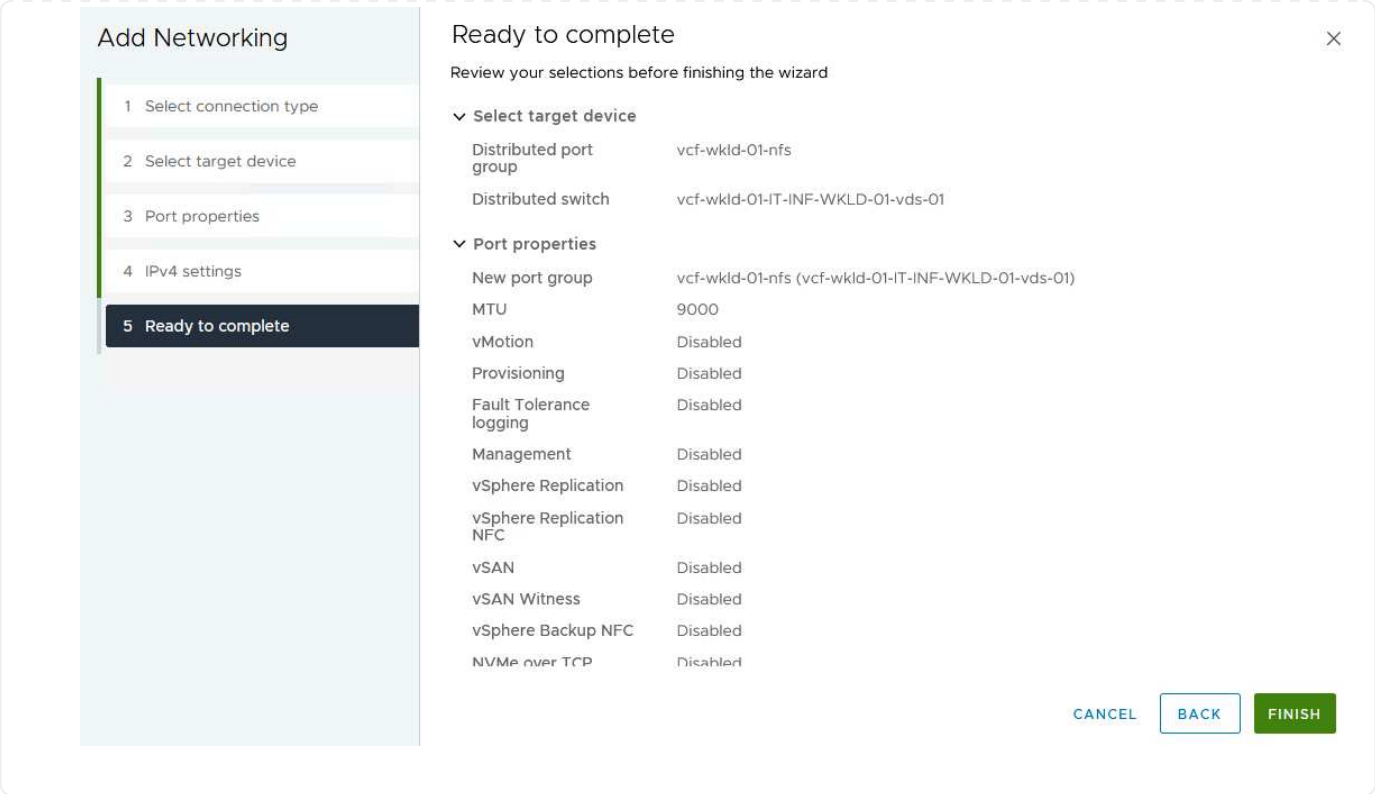
3. 대상 장치 선택 페이지에서 이전에 생성한 NFS용 분산 포트 그룹 중 하나를 선택합니다.



4. 포트 속성 페이지에서 기본값(활성화된 서비스 없음)을 유지하고 *다음*을 클릭하여 계속합니다.
5. **IPv4** 설정 페이지에서 **IP** 주소, *서브넷 마스크*를 입력하고 새로운 게이트웨이 IP 주소를 입력합니다(필요한 경우에만). 계속하려면 *다음*을 클릭하세요.



6. 완료 준비 페이지에서 선택 사항을 검토하고 *마침*을 클릭하여 VMkernel 어댑터를 만듭니다.



ONTAP 도구를 배포하고 사용하여 스토리지 구성

다음 단계는 vSphere 클라이언트를 사용하여 VCF 관리 도메인 클러스터에서 수행되며 여기에는 OTV 배포, vVols NFS 데이터 저장소 생성, 관리 VM을 새 데이터 저장소로 마이그레이션하는 작업이 포함됩니다.

VI 워크로드 도메인의 경우 OTV는 VCF 관리 클러스터에 설치되지만 VI 워크로드 도메인과 연결된 vCenter에 등록됩니다.

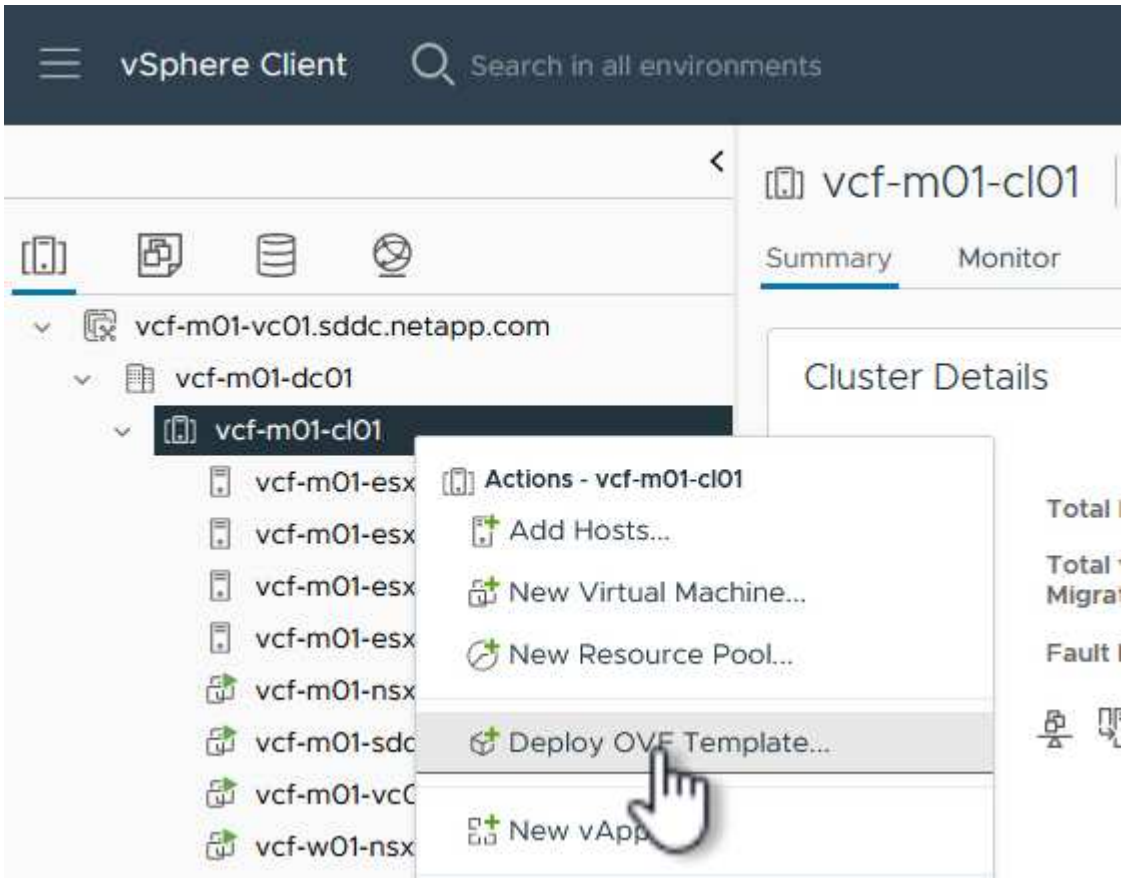
여러 vCenter 환경에서 ONTAP 도구를 배포하고 사용하는 것에 대한 추가 정보는 다음을 참조하세요."여러 vCenter Server 환경에서 ONTAP 도구를 등록하기 위한 요구 사항" .

ONTAP tools for VMware vSphere 배포

ONTAP tools for VMware vSphere VM 어플라이언스로 배포되며 ONTAP 스토리지를 관리하기 위한 통합 vCenter UI를 제공합니다.

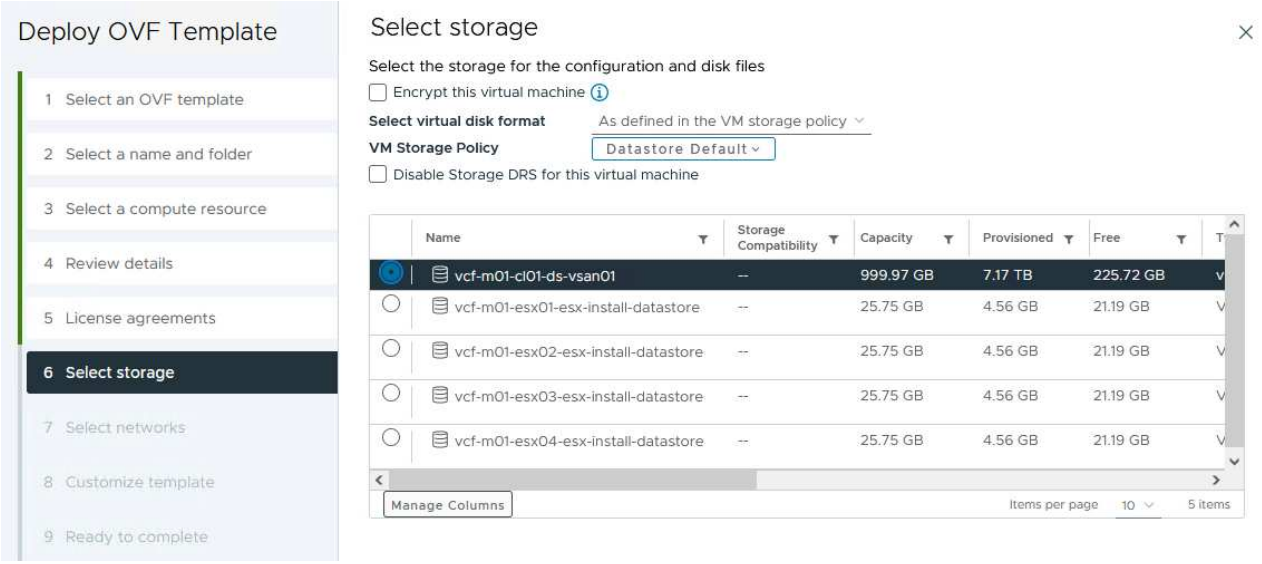
ONTAP tools for VMware vSphere 배포하려면 다음을 완료하세요.

1. ONTAP 도구 OVA 이미지를 가져옵니다."NetApp 지원 사이트" 로컬 폴더로 다운로드합니다.
2. VCF 관리 도메인의 vCenter 어플라이언스에 로그인합니다.
3. vCenter 어플라이언스 인터페이스에서 관리 클러스터를 마우스 오른쪽 버튼으로 클릭하고 *OVF 템플릿 배포…*를 선택합니다.

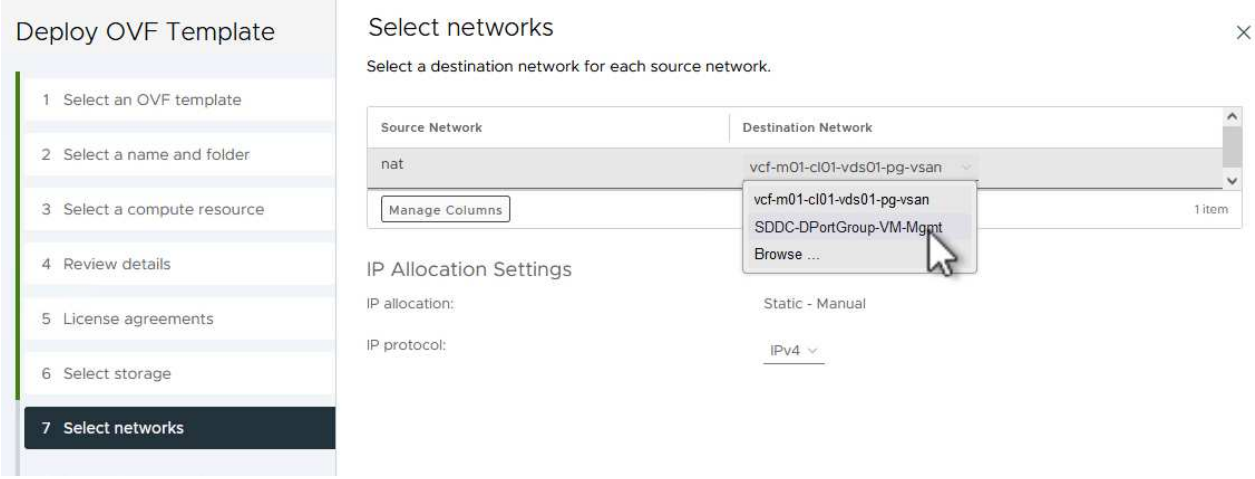


4. **OVF** 템플릿 배포 마법사에서 로컬 파일 라디오 버튼을 클릭하고 이전 단계에서 다운로드한 ONTAP 도구 OVA 파일을 선택합니다.

5. 마법사의 2~5단계에서는 VM의 이름과 폴더를 선택하고, 컴퓨팅 리소스를 선택하고, 세부 정보를 검토한 다음 라이선스 계약에 동의합니다.
6. 구성 및 디스크 파일의 저장 위치로 VCF 관리 도메인 클러스터의 vSAN 데이터 저장소를 선택합니다.

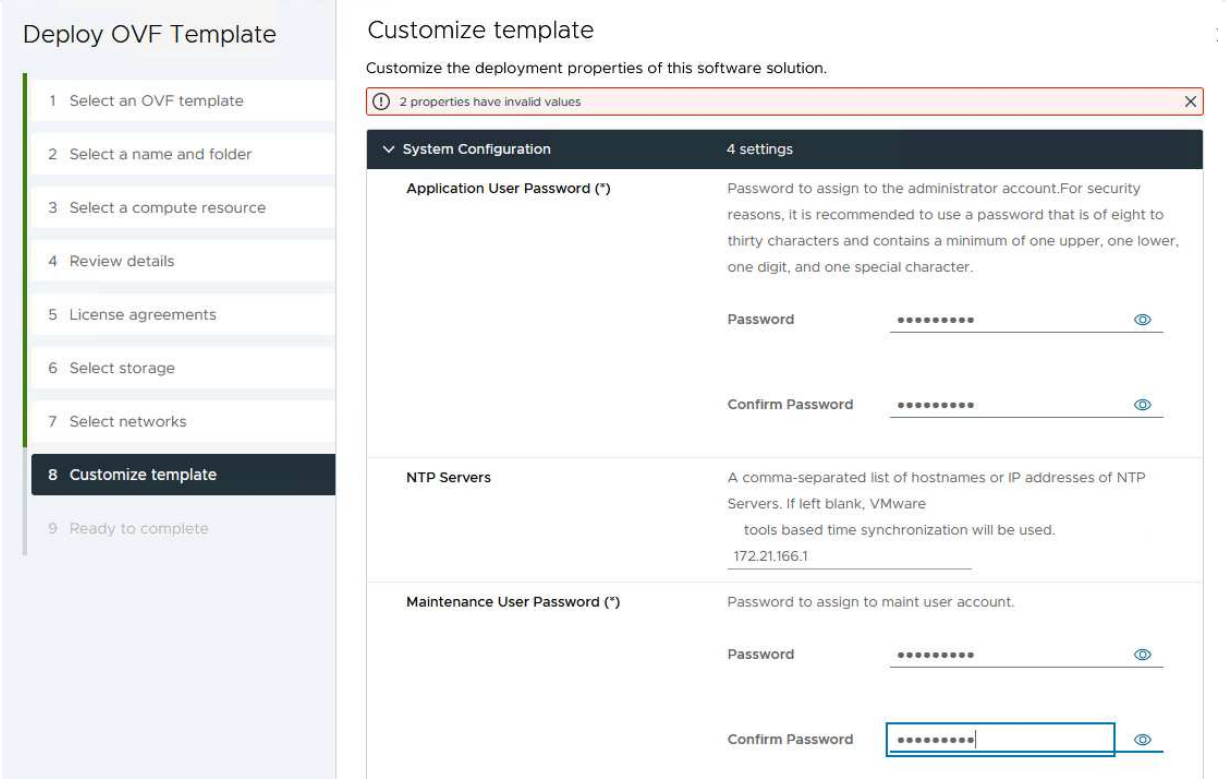


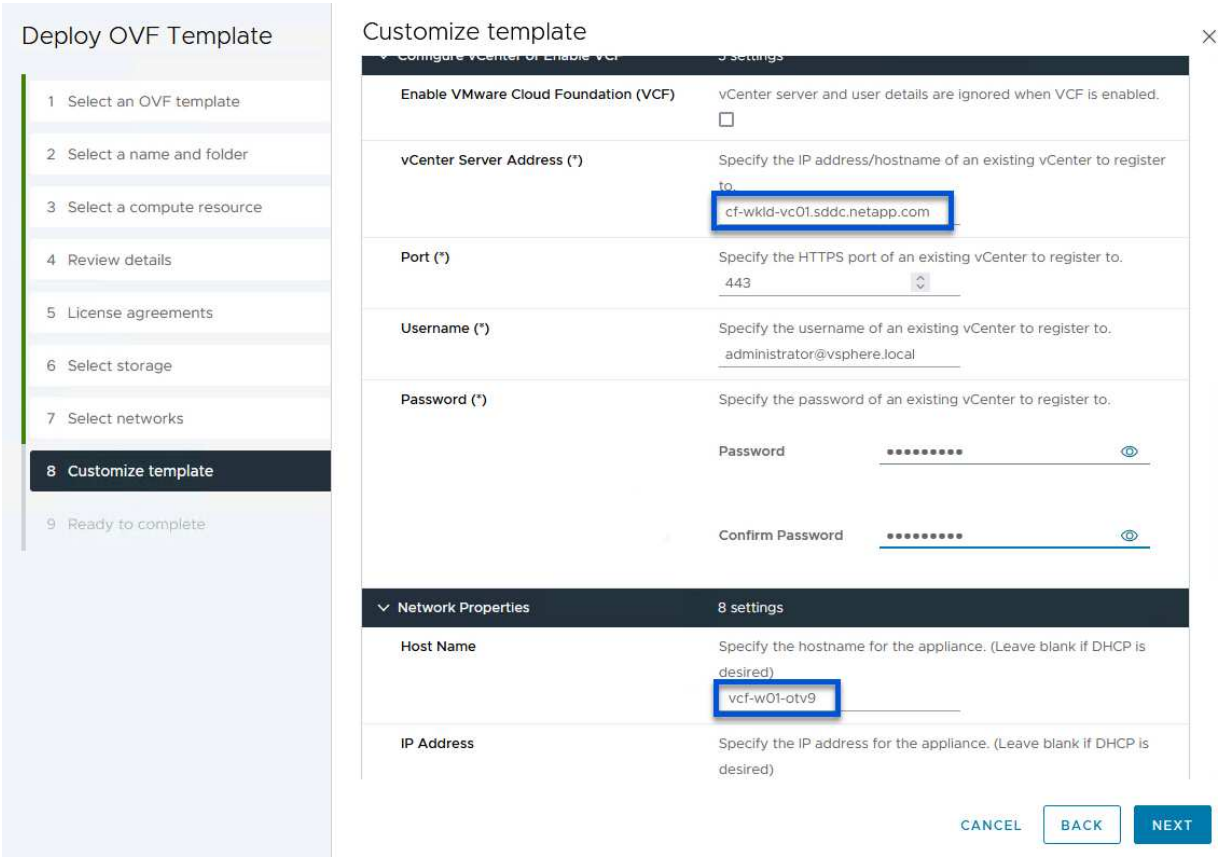
7. 네트워크 선택 페이지에서 관리 트래픽에 사용되는 네트워크를 선택합니다.



8. 사용자 정의 템플릿 페이지에서 필요한 모든 정보를 입력하세요.
   - OTV에 대한 관리 액세스에 사용되는 비밀번호입니다.
   - NTP 서버 IP 주소.
   - OTV 유지관리 계정 비밀번호.
   - OTV 더비 DB 비밀번호.
   - **VMware Cloud Foundation(VCF)** 활성화 상자를 선택하지 마세요. 보조 저장 장치를 배포하는 데 VCF 모드는 필요하지 않습니다.
   - *VI 워크로드 도메인*에 대한 vCenter 어플라이언스의 FQDN 또는 IP 주소
   - *VI 워크로드 도메인*의 vCenter 어플라이언스에 대한 자격 증명
   - 필수 네트워크 속성 필드를 제공하세요.

     계속하려면 *다음*을 클릭하세요.

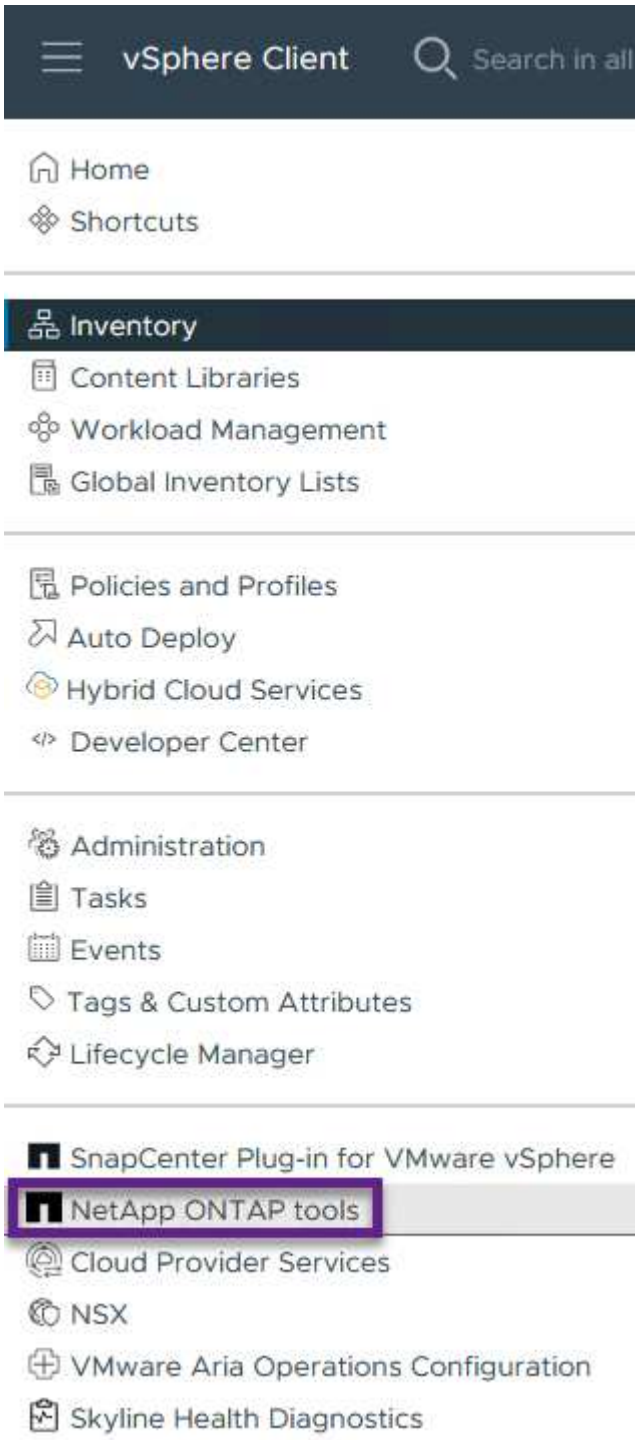




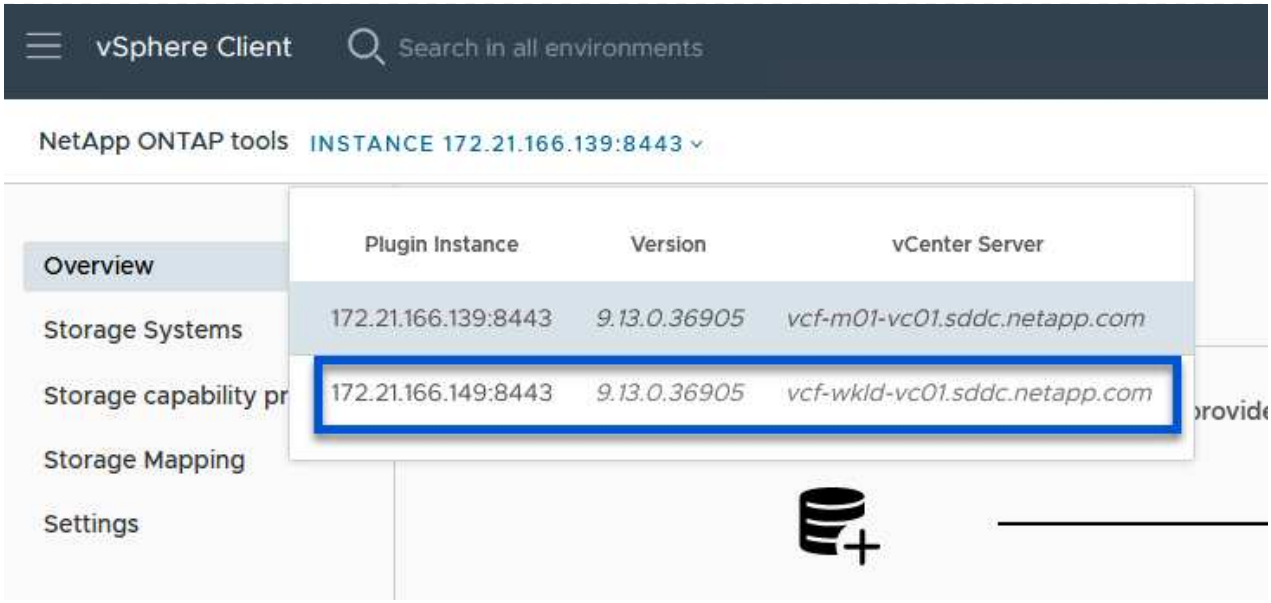
9. 완료 준비 페이지에서 모든 정보를 검토하고 마침을 클릭하여 OTV 어플라이언스 배포를 시작합니다.

ONTAP 도구에 스토리지 시스템을 추가합니다.

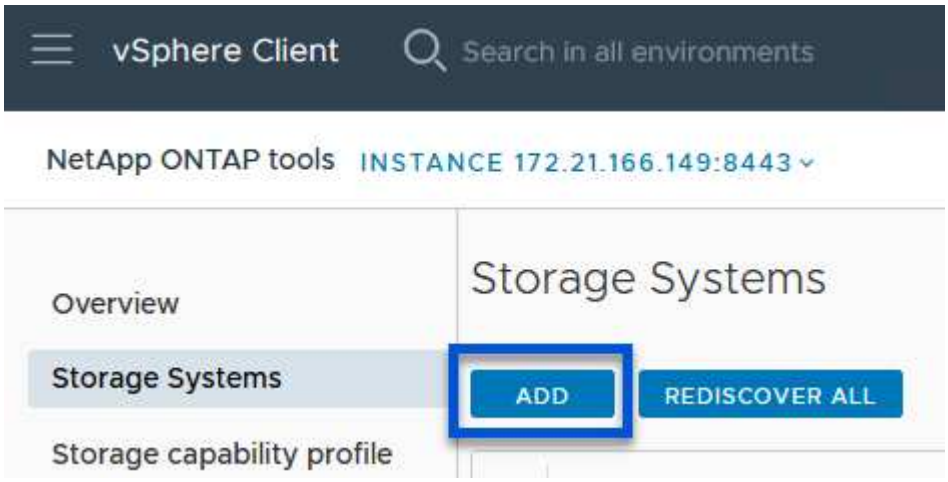
1. vSphere 클라이언트의 기본 메뉴에서 NetApp ONTAP 도구를 선택하여 액세스합니다.



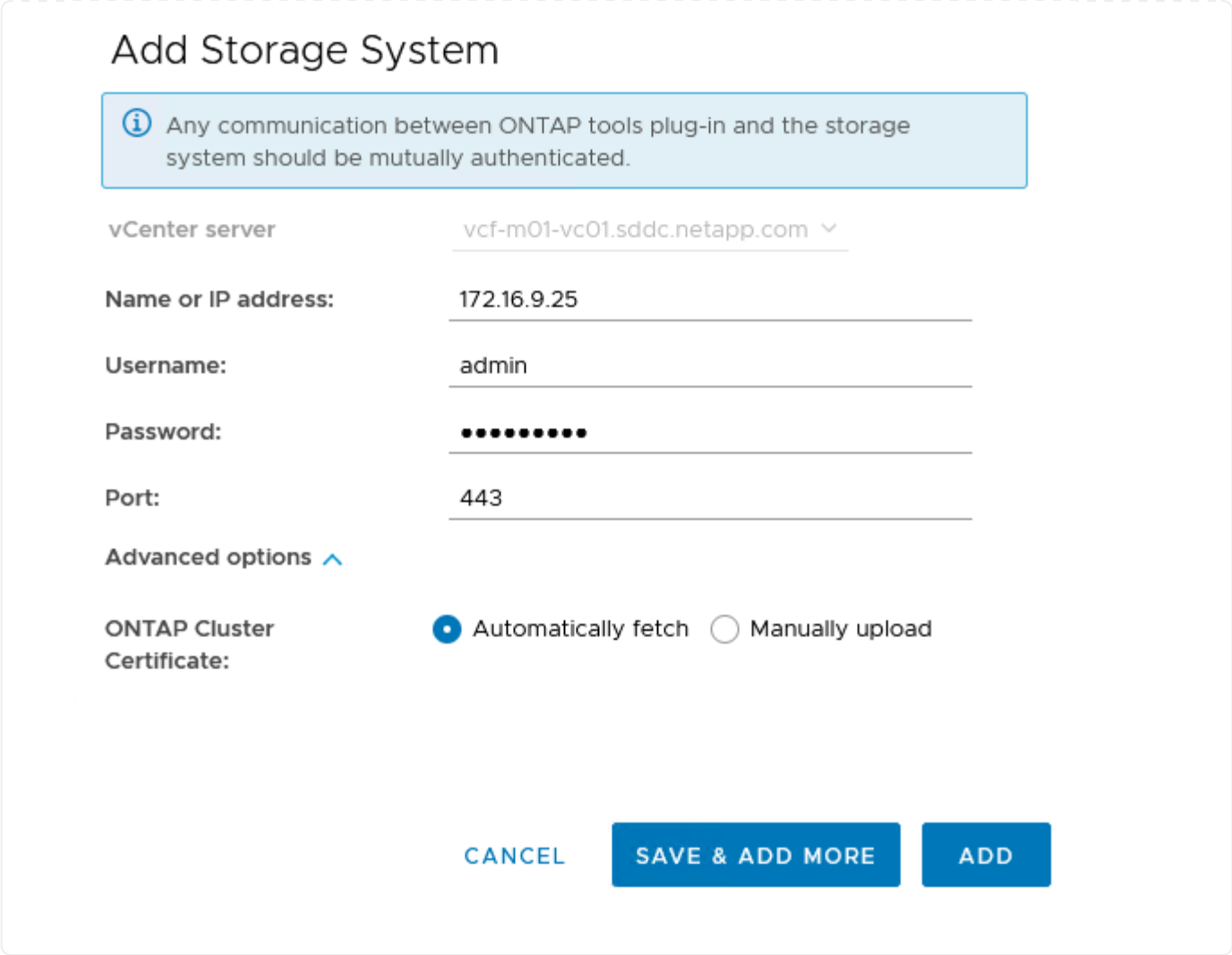
2. ONTAP 도구 인터페이스의 인스턴스 드롭다운 메뉴에서 관리할 워크로드 도메인과 연결된 OTV 인스턴스를 선택합니다.



3. ONTAP 도구의 왼쪽 메뉴에서 *스토리지 시스템*을 선택한 다음 *추가*를 누릅니다.



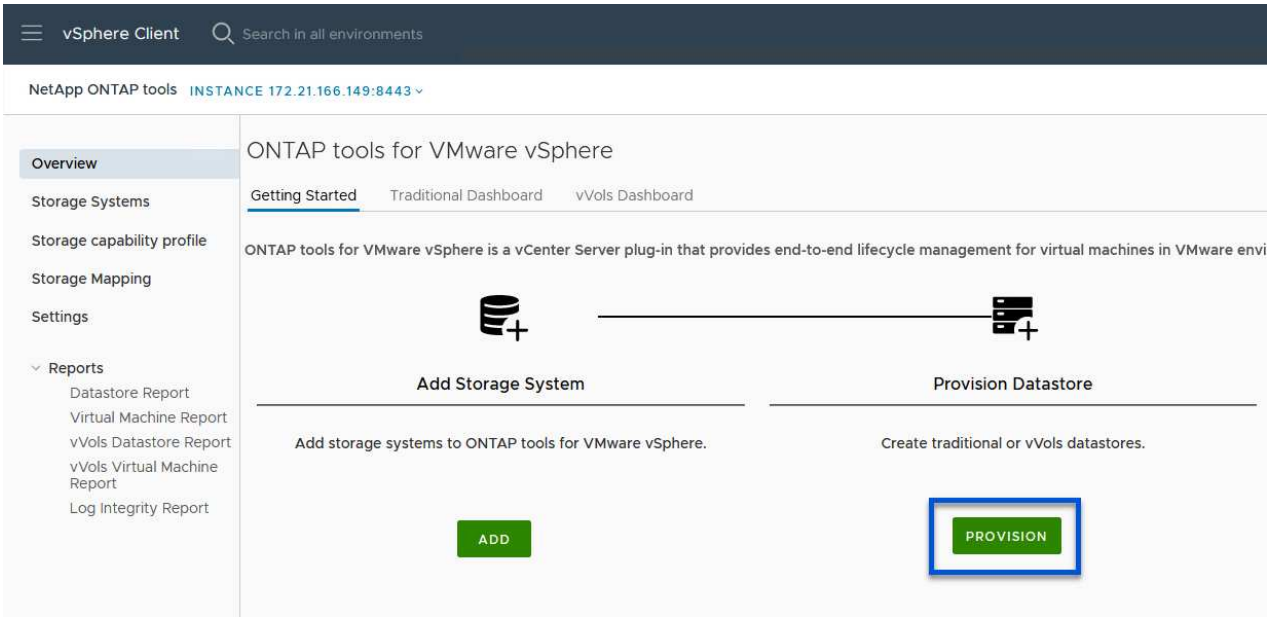
4. IP 주소, 저장 시스템의 자격 증명, 포트 번호를 입력하세요. *추가*를 클릭하여 검색 프로세스를 시작하세요.


Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Name or IP address:
172.16.9.25
Username:
admin
Password:
Port:
443
Advanced options
ONTAP Cluster Certificate:
Automatically fetch
Manually upload
CANCEL
SAVE & ADD MORE
ADD

ONTAP 도구에서 **NFS** 데이터 저장소 만들기

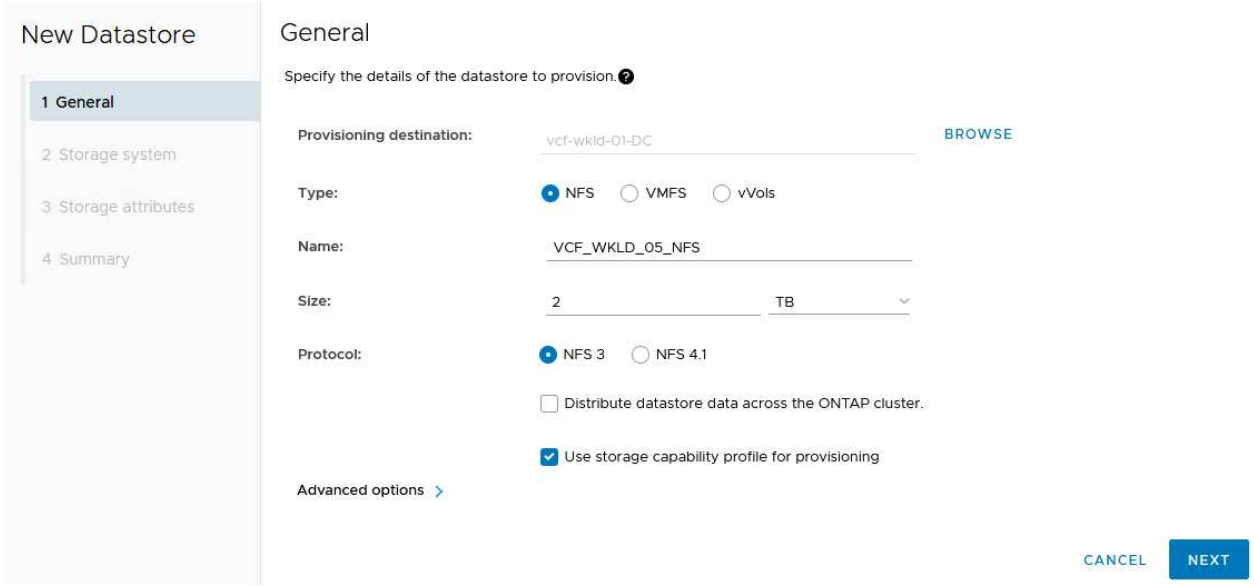
ONTAP 도구를 사용하여 NFS에서 실행되는 ONTAP 데이터 저장소를 배포하려면 다음 단계를 완료하세요.

1. ONTAP 도구에서 개요*를 선택하고 *시작하기 탭에서 *프로비저닝*을 클릭하여 마법사를 시작합니다.

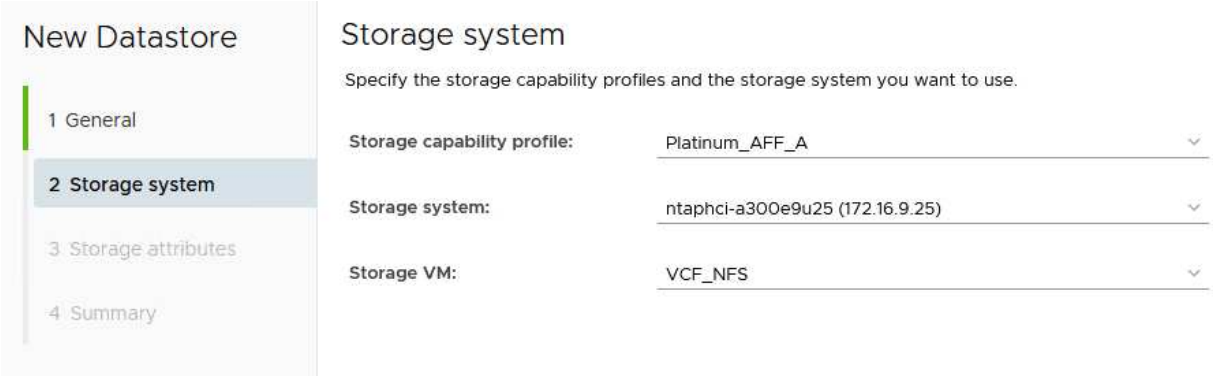


2. 새 데이터 저장소 마법사의 일반 페이지에서 vSphere 데이터 센터 또는 클러스터 대상을 선택합니다. 데이터 저장소 유형으로 *NFS*를 선택하고, 데이터 저장소의 이름을 입력하고, 프로토콜을 선택합니다. FlexGroup 볼륨을 사용할지 여부와 프로비저닝을 위해 스토리지 기능 파일을 사용할지 여부를 선택합니다. 계속하려면 *다음*을 클릭하세요.

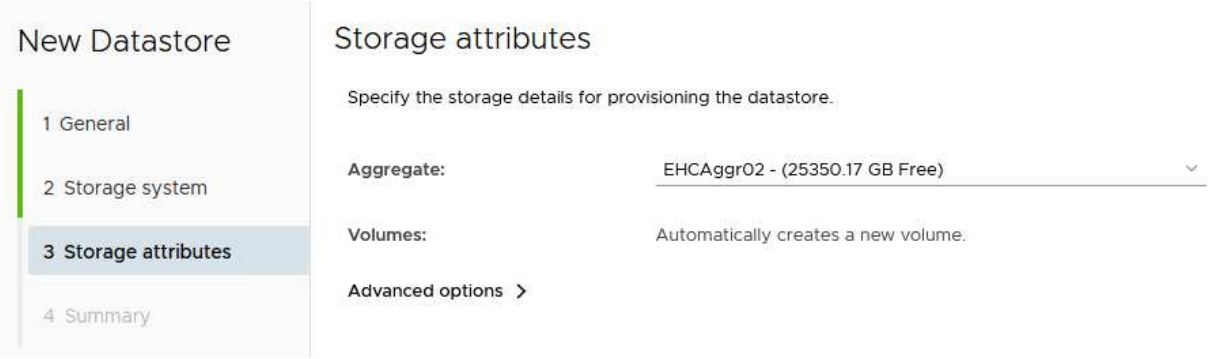
   참고: *클러스터 전체에 데이터 저장소 데이터 분산*을 선택하면 기본 볼륨이 FlexGroup 볼륨으로 생성되어 스토리지 기능 프로필을 사용할 수 없습니다. 참조하다 "FlexGroup 볼륨에 대해 지원되는 구성 및 지원되지 않는 구성" FlexGroup Volumes 사용에 대한 자세한 내용은 다음을 참조하세요.



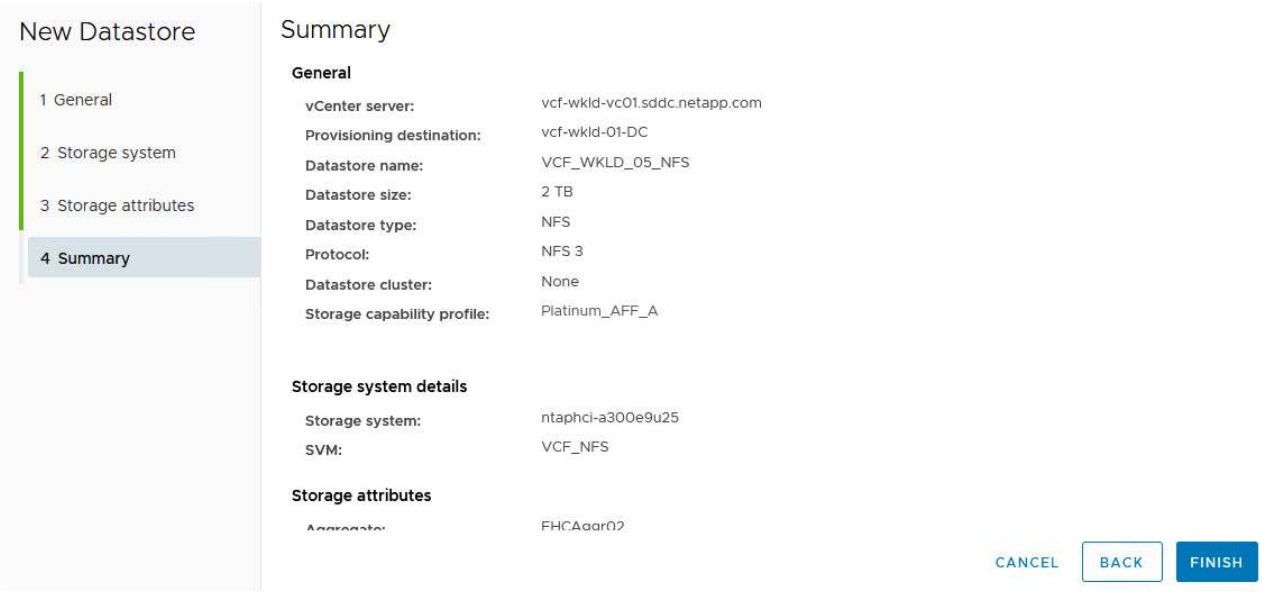
3. 스토리지 시스템 페이지에서 스토리지 용량 프로필, 스토리지 시스템 및 SVM을 선택합니다. 계속하려면 *다음*을 클릭하세요.



4. 저장소 속성 페이지에서 사용할 집계를 선택한 후 *다음*을 클릭하여 계속합니다.



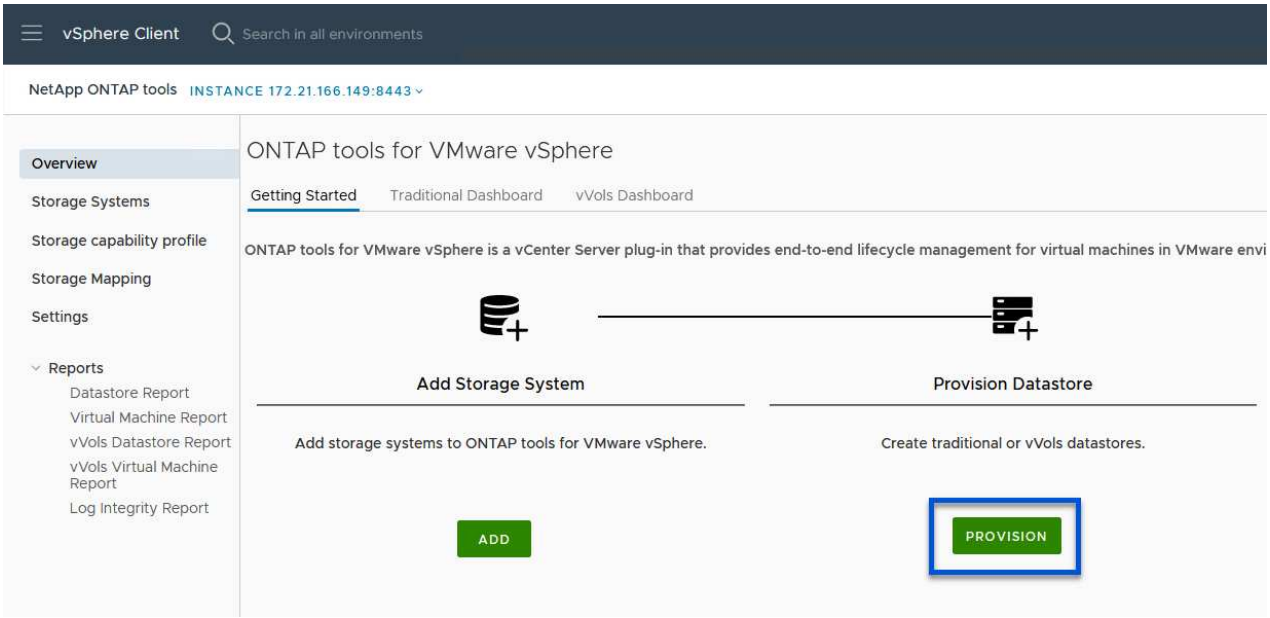
5. 마지막으로 *요약*을 검토하고 마침을 클릭하여 NFS 데이터 저장소 생성을 시작합니다.



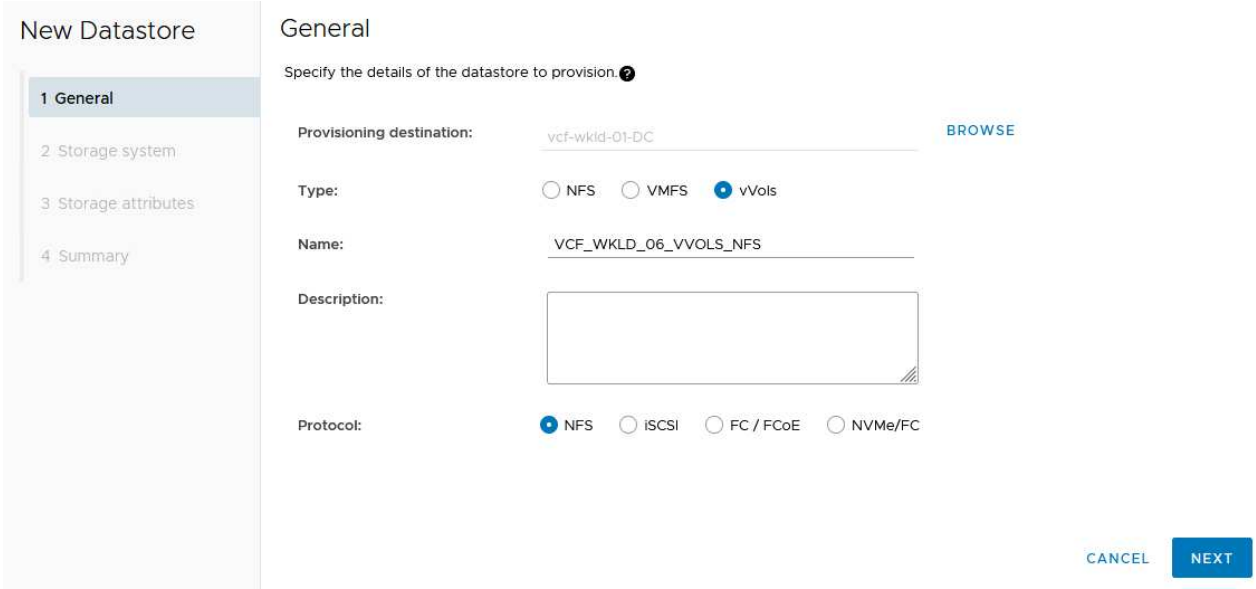
ONTAP 도구에서 **vVols** 데이터 저장소 만들기

ONTAP 도구에서 vVols 데이터 저장소를 생성하려면 다음 단계를 완료하세요.

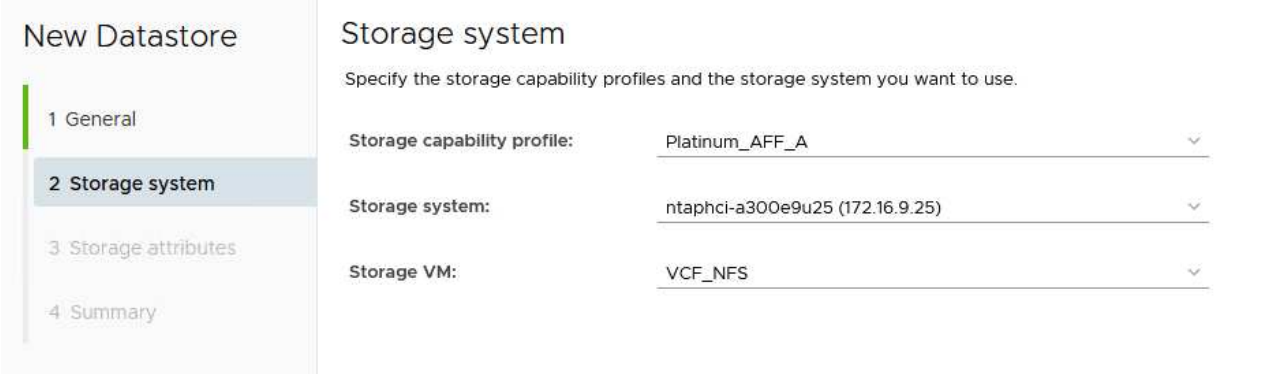
1. ONTAP 도구에서 개요*를 선택하고 *시작하기 탭에서 *프로비저닝*을 클릭하여 마법사를 시작합니다.



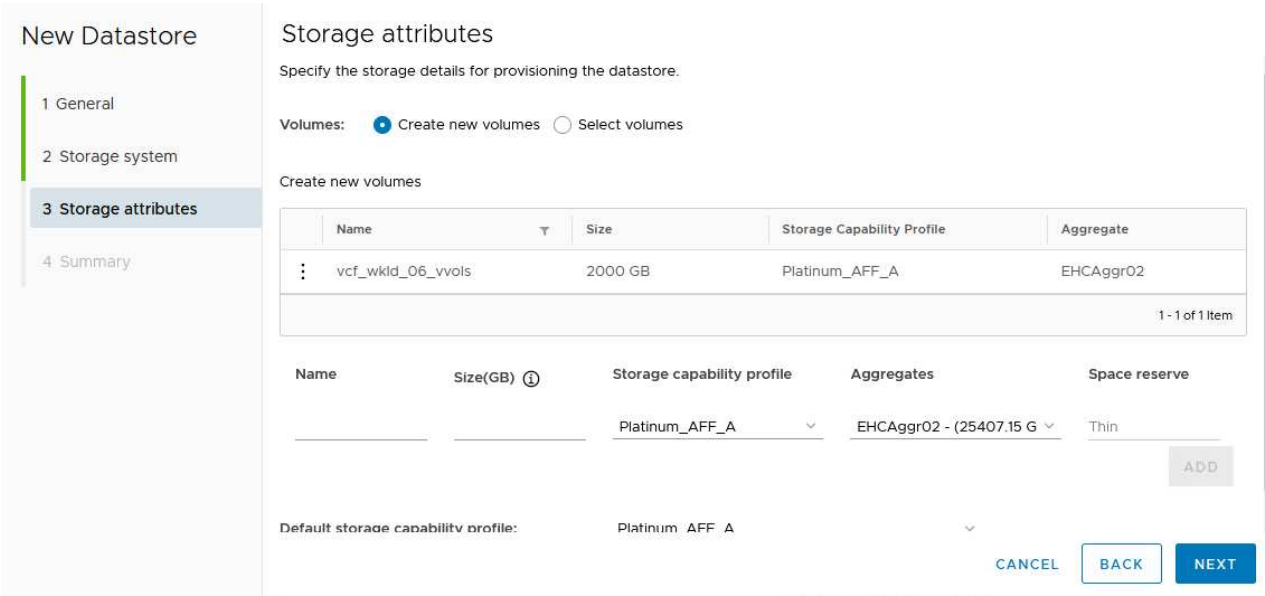
2. 새 데이터 저장소 마법사의 일반 페이지에서 vSphere 데이터 센터 또는 클러스터 대상을 선택합니다. 데이터 저장소 유형으로 * vVols*를 선택하고, 데이터 저장소의 이름을 입력하고, 프로토콜로 *NFS*를 선택합니다. 계속하려면 *다음*을 클릭하세요.



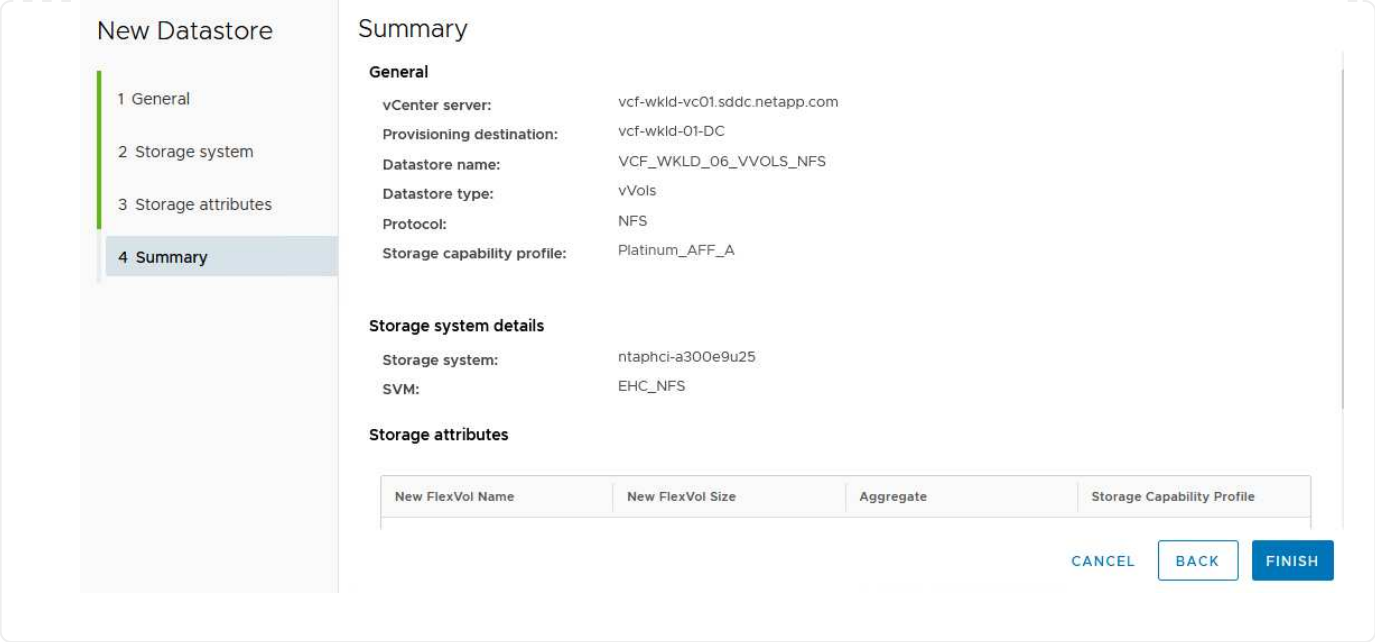
3. 스토리지 시스템 페이지에서 스토리지 용량 프로필, 스토리지 시스템 및 SVM을 선택합니다. 계속하려면 *다음*을 클릭하세요.



4. 저장소 속성 페이지에서 데이터 저장소에 대한 새 볼륨을 생성하도록 선택하고 생성할 볼륨의 저장소 속성을 입력합니다. *추가*를 클릭하여 볼륨을 생성한 다음 *다음*을 클릭하여 계속합니다.



5. 마지막으로 *요약*을 검토하고 *마침*을 클릭하여 vVol 데이터 저장소 생성 프로세스를 시작합니다.



추가 정보

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

VI 워크로드 도메인에 보조 스토리지로 NVMe over TCP 추가

이 사용 사례에서는 ONTAP Tools for VMware를 사용하여 VMware Cloud Foundation(VCF) Virtual Infrastructure(VI) 워크로드 도메인에 대한 보조 스토리지로 NVMe over TCP(NVMe/TCP)를 구성하는 절차를 설명합니다. 이 절차에서는 NVMe/TCP 지원 스토리지 가상 머신(SVM) 설정, NVMe 네임스페이스 생성, ESXi 호스트 네트워킹 구성, VMFS 데이터스토어 배포에 대한 내용을 요약합니다.

TCP를 통한 NVMe의 이점

고성능: 낮은 지연 시간과 높은 데이터 전송 속도로 뛰어난 성능을 제공합니다. 이는 까다로운 애플리케이션과 대규모 데이터 작업에 매우 중요합니다.

확장성: 확장 가능한 구성을 지원하여 IT 관리자가 데이터 요구 사항이 증가함에 따라 인프라를 원활하게 확장할 수 있습니다.

비용 효율성: 표준 이더넷 스위치에서 실행되며 TCP 데이터그램 내부에 캡슐화됩니다. 구현에 특별한 장비가 필요하지 않습니다.

NVMe의 이점에 대한 자세한 내용은 다음을 참조하세요. "NVME란 무엇인가요?"

시나리오 개요

이 시나리오에서는 다음과 같은 상위 수준 단계를 다룹니다.

- NVMe/TCP 트래픽을 위한 논리 인터페이스(LIF)가 있는 스토리지 가상 머신(SVM)을 생성합니다.

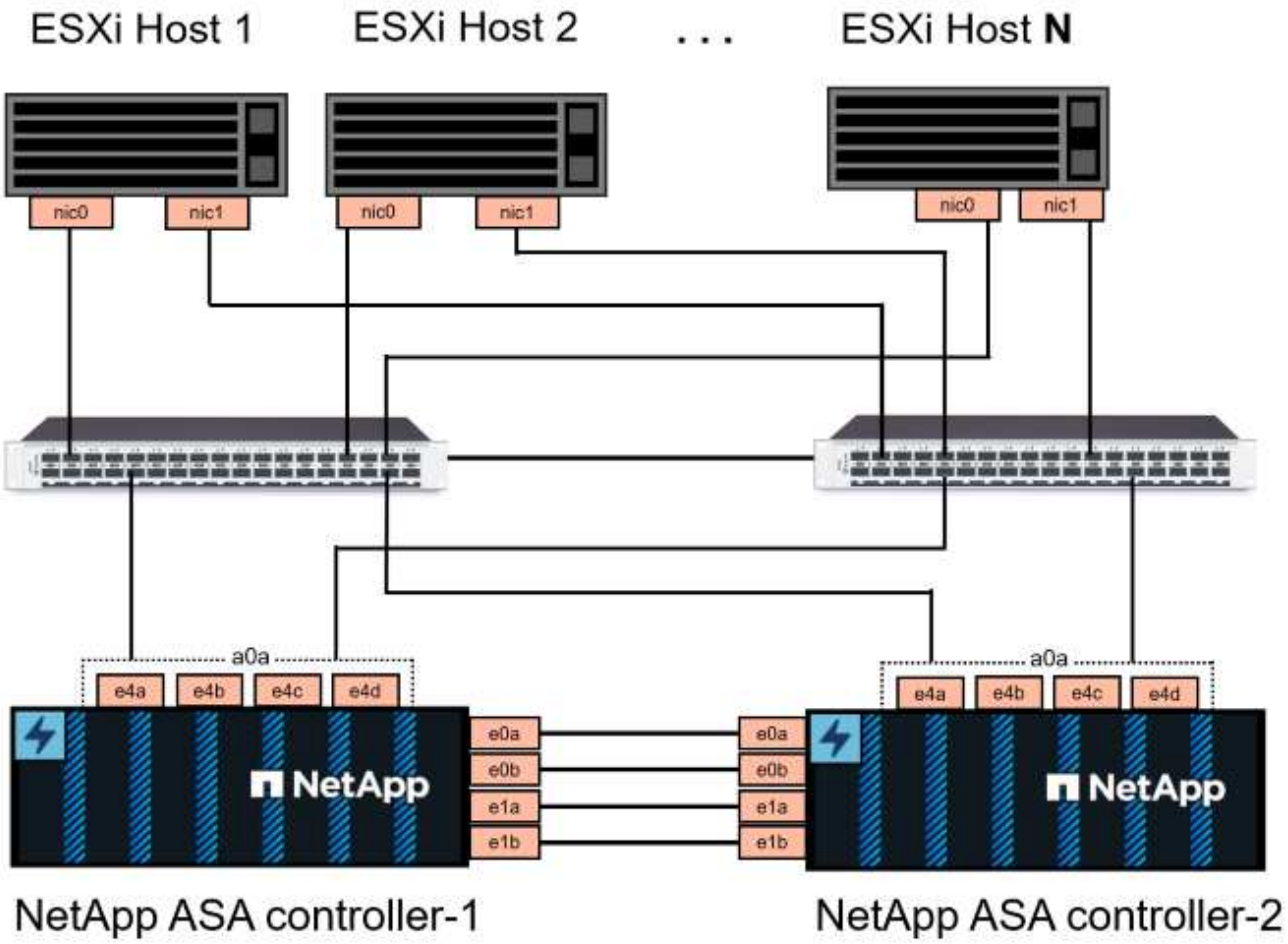
- VI 워크로드 도메인에서 iSCSI 네트워크에 대한 분산 포트 그룹을 생성합니다.
- VI 워크로드 도메인의 ESXi 호스트에서 iSCSI용 vmkernel 어댑터를 생성합니다.
- ESXi 호스트에 NVMe/TCP 어댑터를 추가합니다.
- NVMe/TCP 데이터 저장소를 배포합니다.

필수 조건

이 시나리오에는 다음과 같은 구성 요소와 구성이 필요합니다.

- 스토리지 트래픽에 전용된 이더넷 스위치의 물리적 데이터 포트가 있는 ONTAP AFF 또는 ASA 스토리지 시스템입니다.
- VCF 관리 도메인 배포가 완료되었으며 vSphere 클라이언트에 액세스할 수 있습니다.
- VI 워크로드 도메인이 이전에 배포되었습니다.

NetApp NVMe/TCP에 대해 완전 중복 네트워크 설계를 권장합니다. 다음 다이어그램은 스토리지 시스템, 스위치, 네트워크 어댑터 및 호스트 시스템에 대한 장애 내구성을 제공하는 중복 구성의 예를 보여줍니다. NetApp 을 참조하세요"SAN 구성 참조" 추가 정보를 원하시면.



다중 경로 지정 및 여러 경로에 걸친 장애 조치의 경우 NetApp NVMe/TCP 구성의 모든 SVM에 대해 별도의 이더넷 네트워크에 스토리지 노드당 최소 두 개의 LIF를 두는 것을 권장합니다.

이 문서에서는 새로운 SVM을 생성하고 NVMe/TCP 트래픽에 대한 여러 LIF를 생성하기 위해 IP 주소 정보를 지정하는 프로세스를 보여줍니다. 기존 SVM에 새로운 LIF를 추가하려면 다음을 참조하세요."LIF(네트워크 인터페이스) 생성" .

ONTAP 스토리지 시스템에 대한 NVMe 설계 고려 사항에 대한 추가 정보는 다음을 참조하세요."NVMe 구성, 지원 및 제한 사항" .

배포 단계

NVMe/TCP를 사용하여 VCF 워크로드 도메인에 VMFS 데이터 저장소를 생성하려면 다음 단계를 완료하세요.

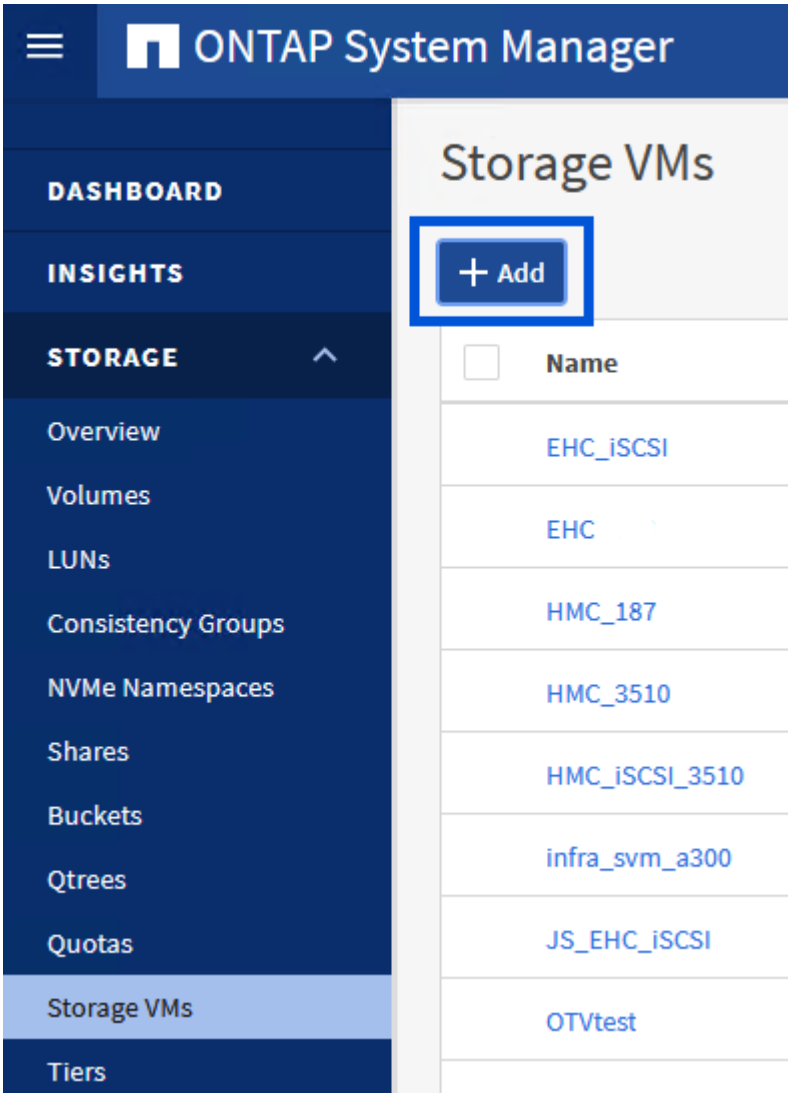
ONTAP 스토리지 시스템에 **SVM, LIF** 및 **NVMe** 네임스페이스 생성

다음 단계는 ONTAP 시스템 관리자에서 수행됩니다.

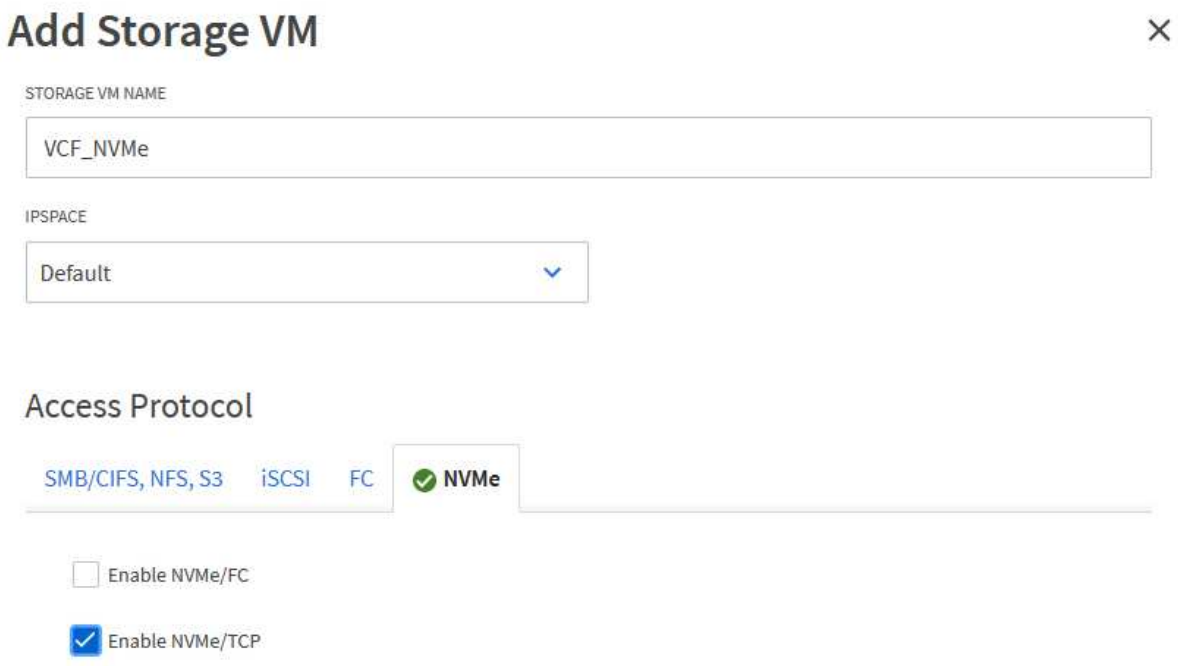
스토리지 **VM** 및 **LIF** 생성

NVMe/TCP 트래픽을 위한 여러 LIF와 함께 SVM을 생성하려면 다음 단계를 완료하세요.

1. ONTAP System Manager에서 왼쪽 메뉴의 *Storage VMs*로 이동한 다음 *+ 추가*를 클릭하여 시작합니다.

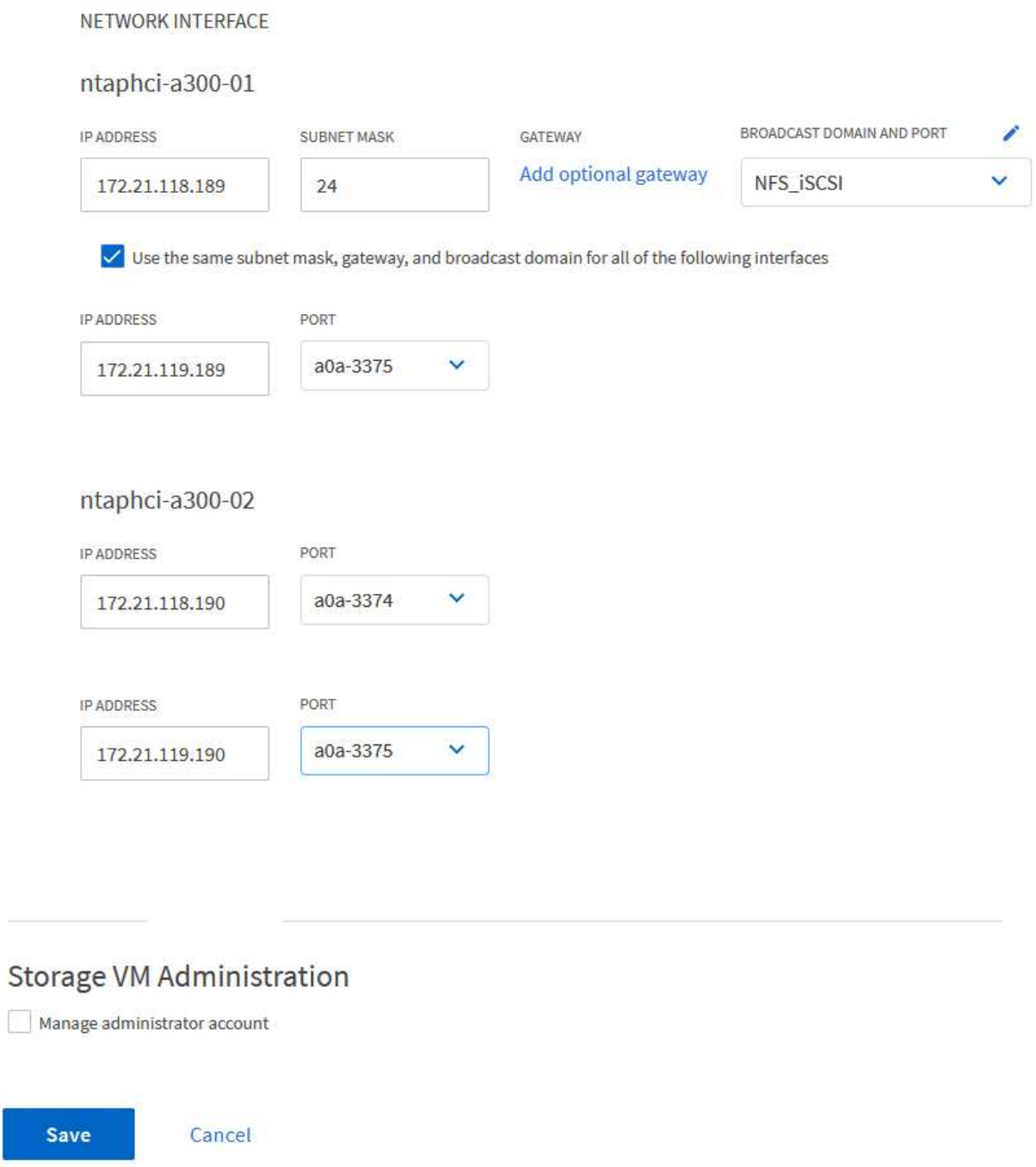


2. 스토리지 **VM** 추가 마법사에서 SVM의 이름*을 입력하고, ***IP** 공간*을 선택한 다음, *액세스 프로토콜*에서 ***NVMe** 탭을 클릭하고 **NVMe/TCP** 사용 확인란을 선택합니다.

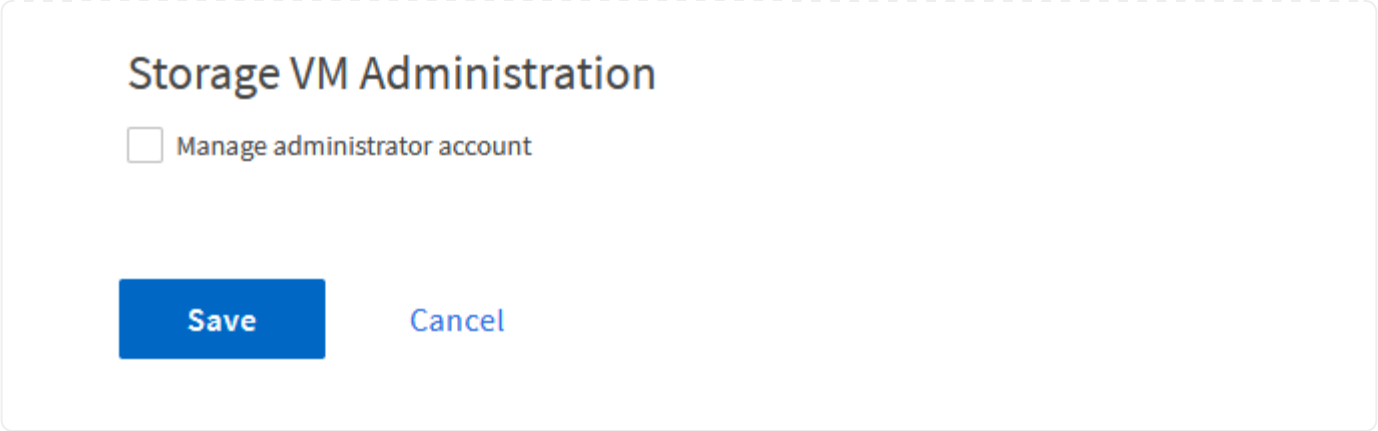


3. 네트워크 인터페이스 섹션에 첫 번째 LIF에 대한 **IP** 주소, 서브넷 마스크, *브로드캐스트 도메인 및 포트*를 입력합니다. 이후 LIF의 경우 확인란을 활성화하여 나머지 모든 LIF에서 공통 설정을 사용하거나 별도의 설정을 사용할 수 있습니다.

> ⓘ 다중 경로 지정 및 여러 경로에 걸친 장애 조치의 경우 NetApp NVMe/TCP 구성의 모든 SVM에 대해 별도의 이더넷 네트워크에 스토리지 노드당 최소 두 개의 LIF를 두는 것을 권장합니다.



4. 스토리지 VM 관리 계정(멀티 테넌시 환경의 경우)을 활성화할지 여부를 선택하고 *저장*을 클릭하여 SVM을 생성합니다.


Storage VM Administration
Manage administrator account
Save
Cancel

NVMe 네임스페이스 생성

NVMe 네임스페이스는 iSCSI 또는 FC의 LUN과 유사합니다. vSphere Client에서 VMFS 데이터스토어를 배포하려면 먼저 NVMe 네임스페이스를 만들어야 합니다. NVMe 네임스페이스를 생성하려면 먼저 클러스터의 각 ESXi 호스트에서 NVMe 정규 이름(NQN)을 얻어야 합니다. ONTAP 은 NQN을 사용하여 네임스페이스에 대한 액세스 제어를 제공합니다.

NVMe 네임스페이스를 생성하려면 다음 단계를 완료하세요.

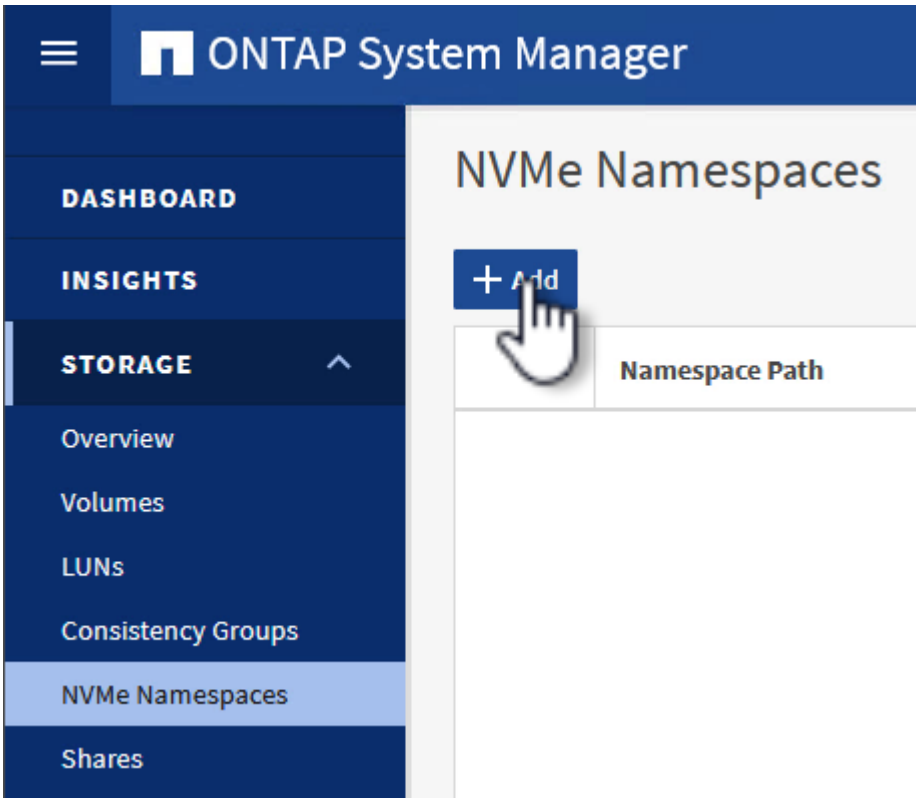
1. 클러스터 내 ESXi 호스트에서 SSH 세션을 열어 NQN을 얻습니다. CLI에서 다음 명령을 사용하세요.

   ```
   esxcli nvme info get
   ```

   다음과 유사한 출력이 표시되어야 합니다.

   ```
   Host NQN: nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-esx01
   ```

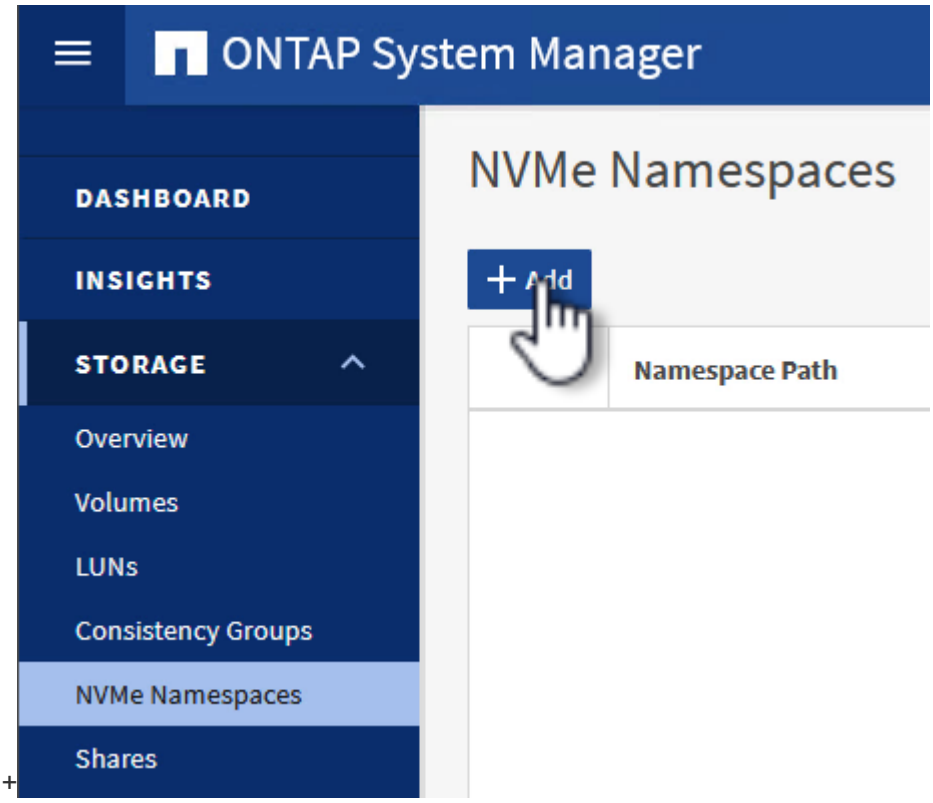
2. 클러스터의 각 ESXi 호스트에 대한 NQN을 기록합니다.
3. ONTAP 시스템 관리자의 왼쪽 메뉴에서 *NVMe 네임스페이스*로 이동한 다음 *+ 추가*를 클릭하여 시작합니다.



4. **NVMe** 네임스페이스 추가 페이지에서 이름 접두사, 생성할 네임스페이스 수, 네임스페이스 크기, 네임스페이스에 액세스할 호스트 운영 체제를 입력합니다. 호스트 **NQN** 섹션에서 네임스페이스에 액세스할

ESXi 호스트에서 이전에 수집한 NQN의 쉼표로 구분된 목록을 만듭니다.

스냅샷 보호 정책과 같은 추가 항목을 구성하려면 *추가 옵션*을 클릭하세요. 마지막으로 *저장*을 클릭하여 NVMe 네임스페이스를 생성합니다.



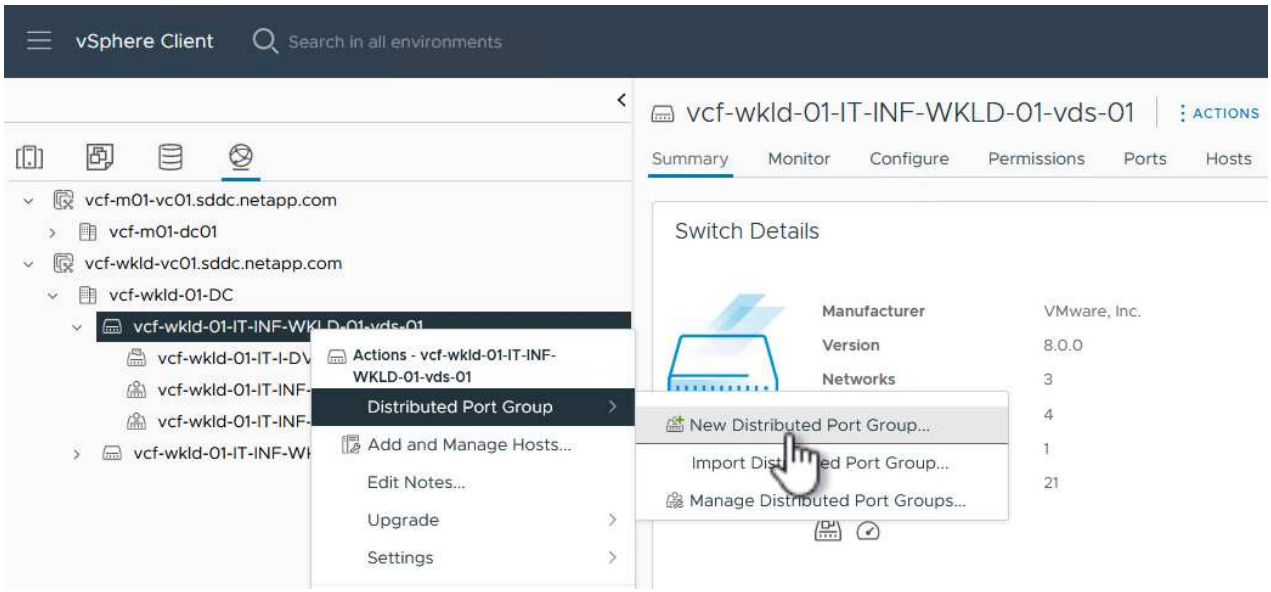
ESXi 호스트에 네트워킹 및 **NVMe** 소프트웨어 어댑터 설정

다음 단계는 vSphere 클라이언트를 사용하여 VI 워크로드 도메인 클러스터에서 수행됩니다. 이 경우 vCenter Single Sign-On이 사용되므로 vSphere 클라이언트는 관리 도메인과 워크로드 도메인 모두에서 공통적입니다.

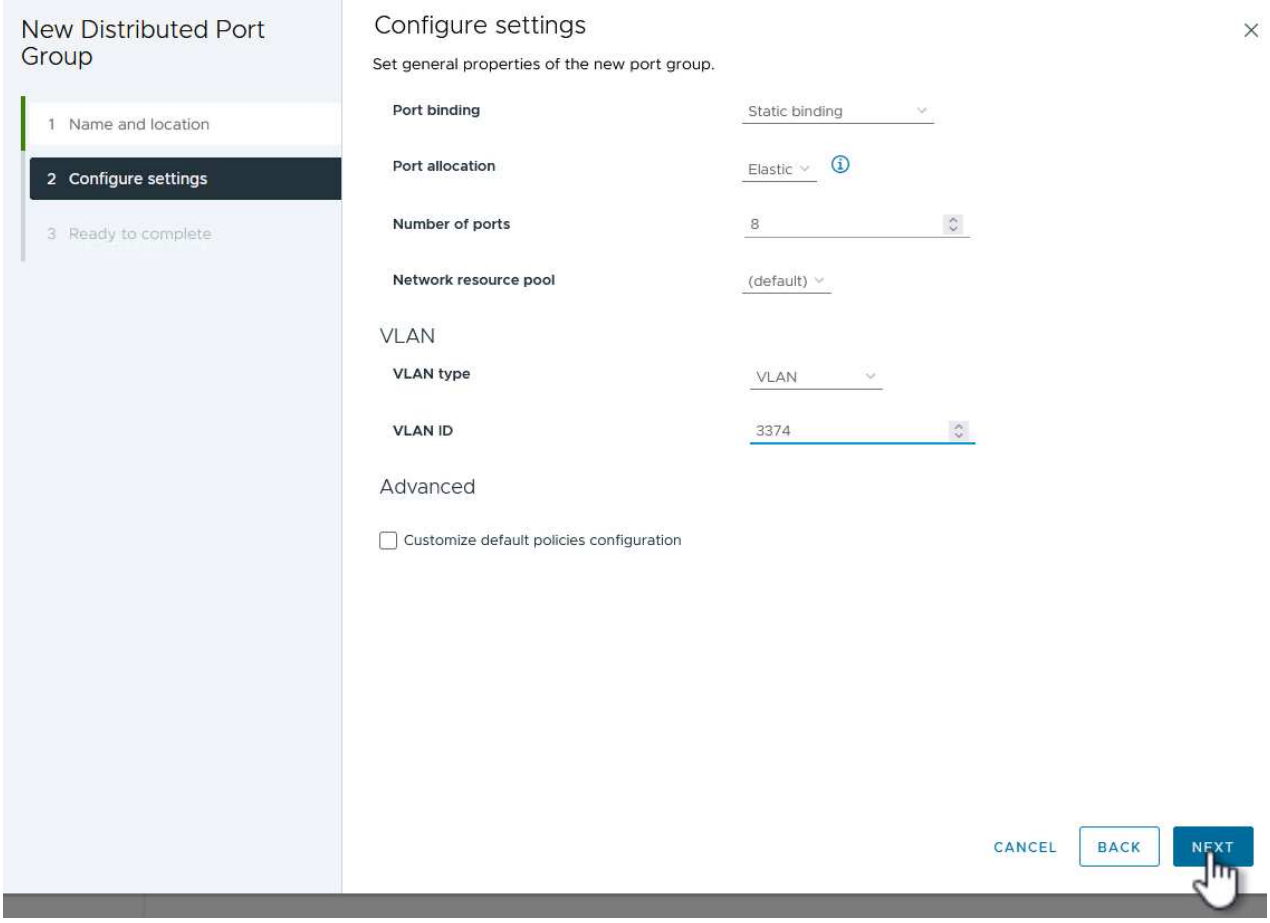
NVME/TCP 트래픽을 위한 분산 포트 그룹 생성

각 NVMe/TCP 네트워크에 대한 새로운 분산 포트 그룹을 생성하려면 다음을 완료하세요.

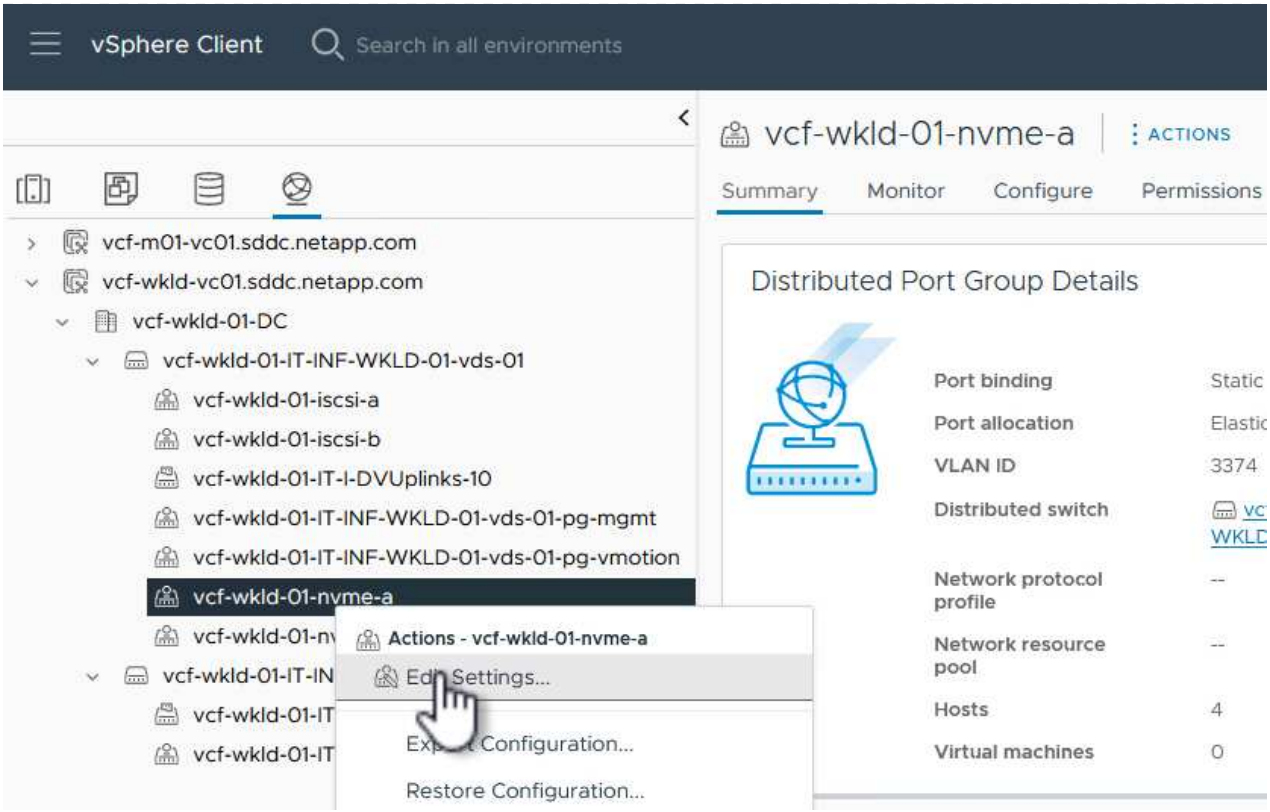
1. vSphere 클라이언트에서 워크로드 도메인에 대한 *인벤토리 > 네트워킹*으로 이동합니다. 기존 분산 스위치로 이동하여 *새 분산 포트 그룹...*을 만드는 작업을 선택합니다.



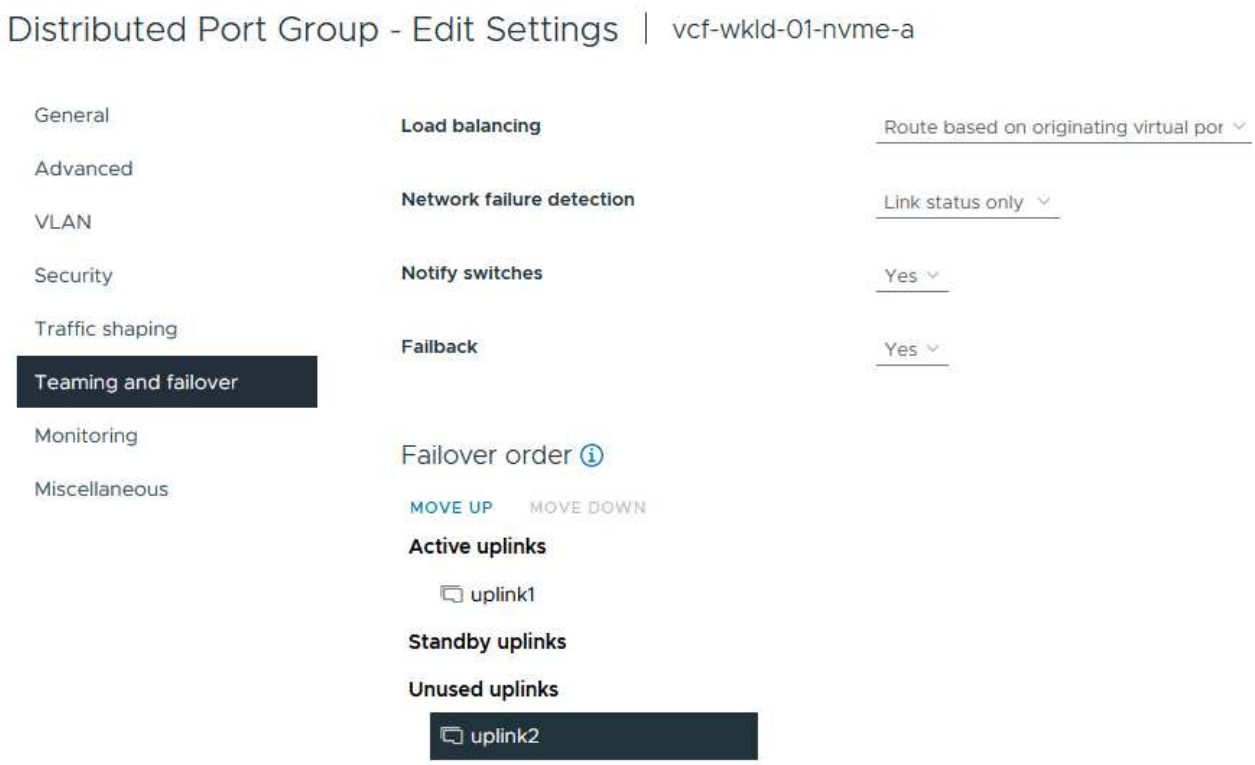
2. 새 분산 포트 그룹 마법사에서 새 포트 그룹의 이름을 입력하고 *다음*을 클릭하여 계속합니다.
3. 설정 구성 페이지에서 모든 설정을 작성하세요. VLAN을 사용하는 경우 올바른 VLAN ID를 제공해야 합니다. 계속하려면 *다음*을 클릭하세요.



4. 완료 준비 페이지에서 변경 사항을 검토하고 *마침*을 클릭하여 새 분산 포트 그룹을 만듭니다.
5. 두 번째 NVMe/TCP 네트워크에 대한 분산 포트 그룹을 생성하려면 이 프로세스를 반복하고 올바른 *VLAN ID*를 입력했는지 확인하세요.
6. 두 포트 그룹이 모두 생성되면 첫 번째 포트 그룹으로 이동하여 설정 편집... 작업을 선택합니다.

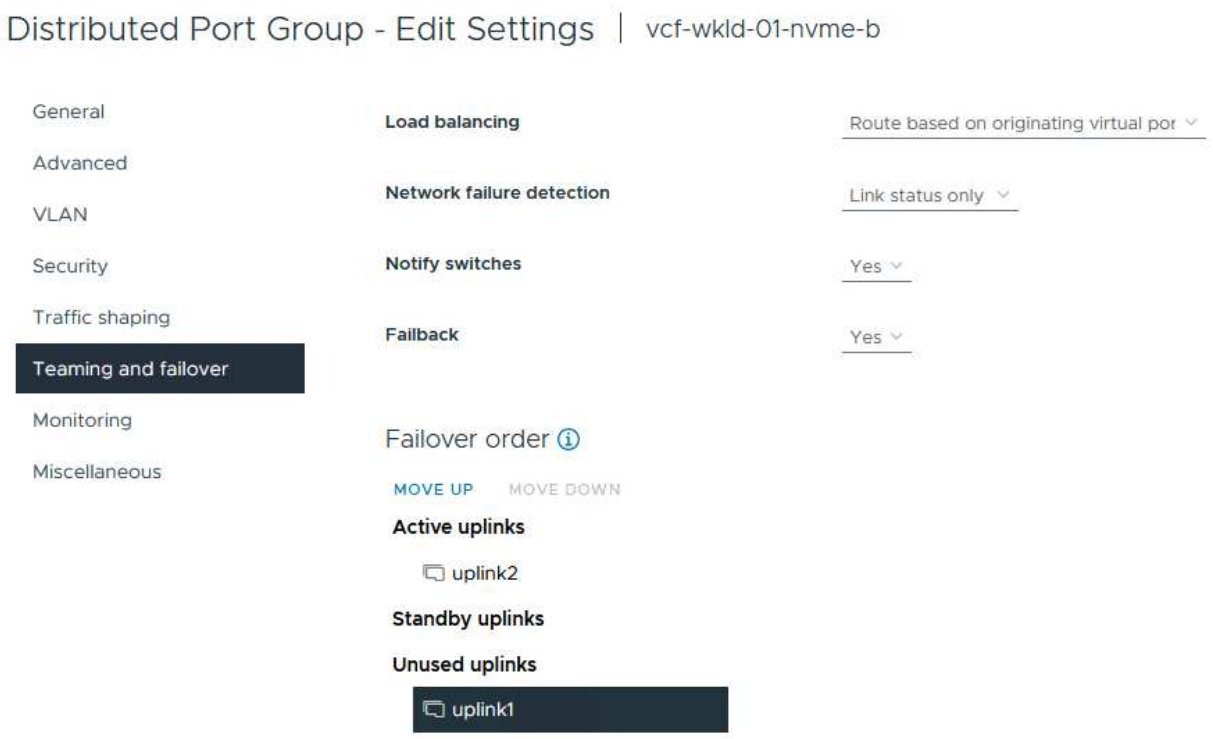


7. 분산 포트 그룹 - 설정 편집 페이지에서 왼쪽 메뉴의 *팀 구성 및 장애 조치*로 이동한 다음 *업링크2*를 클릭하여 *사용하지 않는 업링크*로 이동합니다.



8. 두 번째 NVMe/TCP 포트 그룹에 대해서도 이 단계를 반복합니다. 하지만 이번에는 *uplink1*을 *사용하지

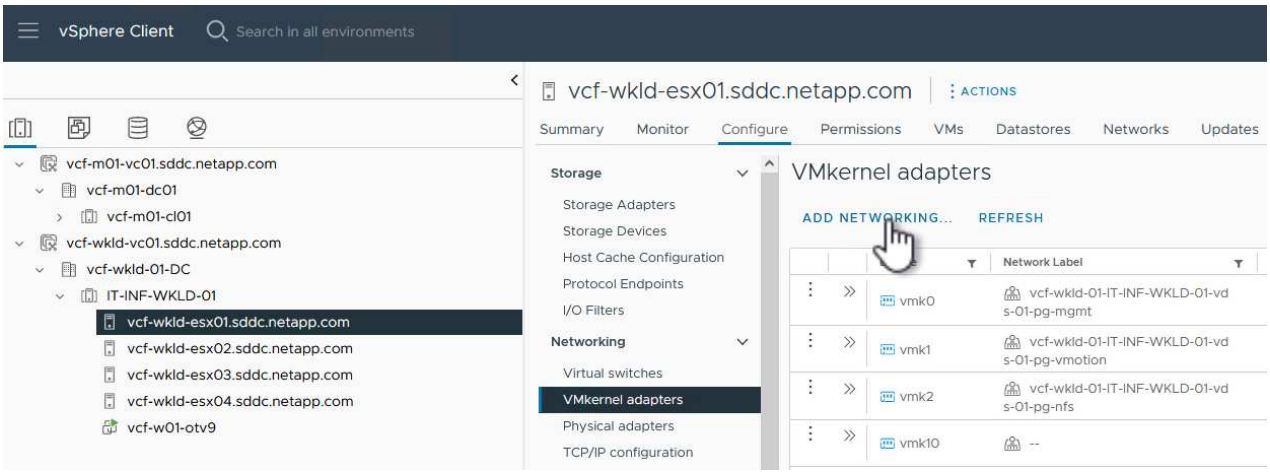
않는 업링크*로 옮깁니다.


Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-b
General
Advanced
VLAN
Security
Traffic shaping
Teaming and failover
Monitoring
Miscellaneous
Load balancing
Route based on originating virtual por
Network failure detection
Link status only
Notify switches
Yes
Failback
Yes
Failover order
MOVE UP
MOVE DOWN
Active uplinks
uplink2
Standby uplinks
Unused uplinks
uplink1

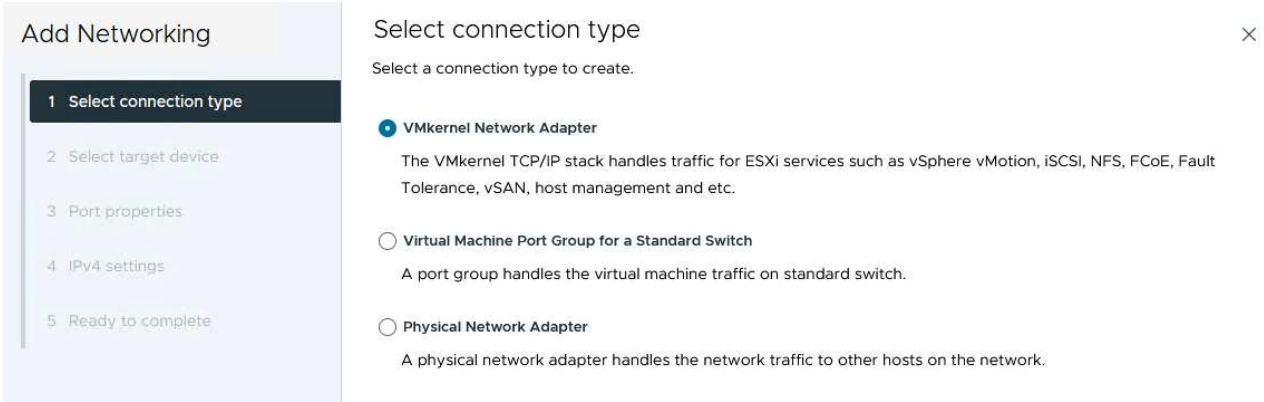
각 **ESXi** 호스트에 **VMkernel** 어댑터를 만듭니다.

워크로드 도메인의 각 ESXi 호스트에서 이 프로세스를 반복합니다.

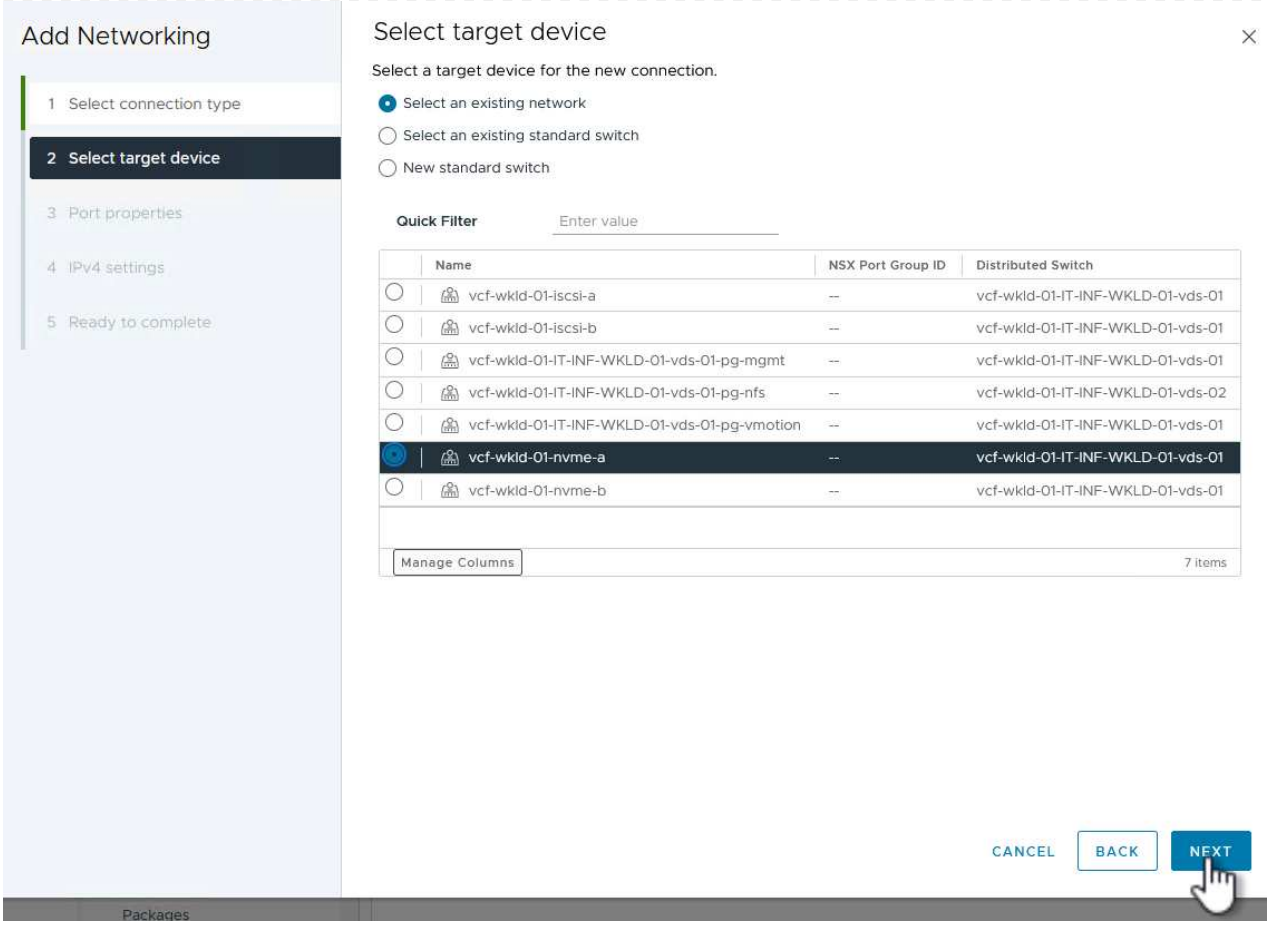
1. vSphere 클라이언트에서 워크로드 도메인 인벤토리의 ESXi 호스트 중 하나로 이동합니다. 구성 탭에서 *VMkernel 어댑터*를 선택하고 *네트워킹 추가...*를 클릭하여 시작합니다.



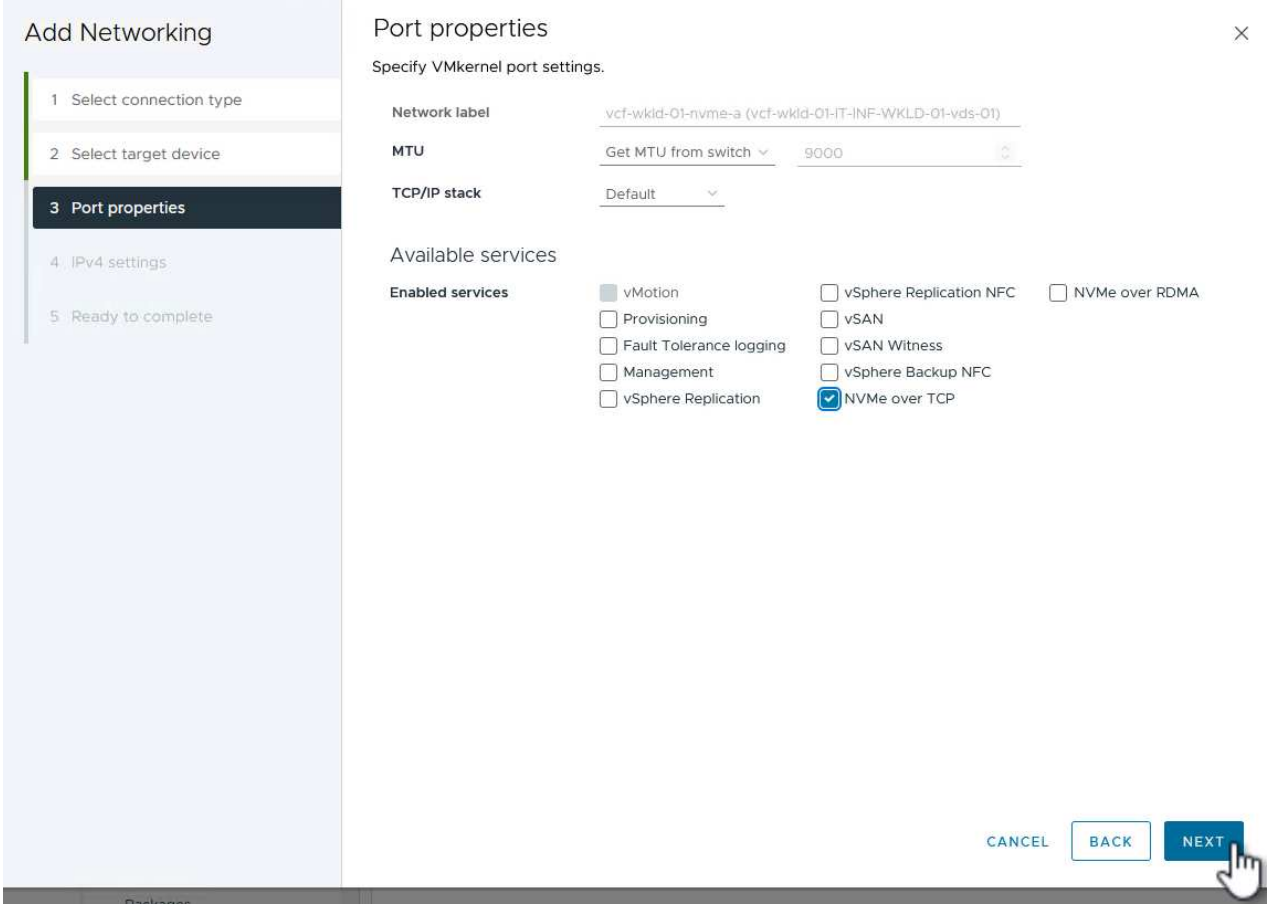
2. 연결 유형 선택 창에서 *VMkernel 네트워크 어댑터*를 선택하고 *다음*을 클릭하여 계속합니다.



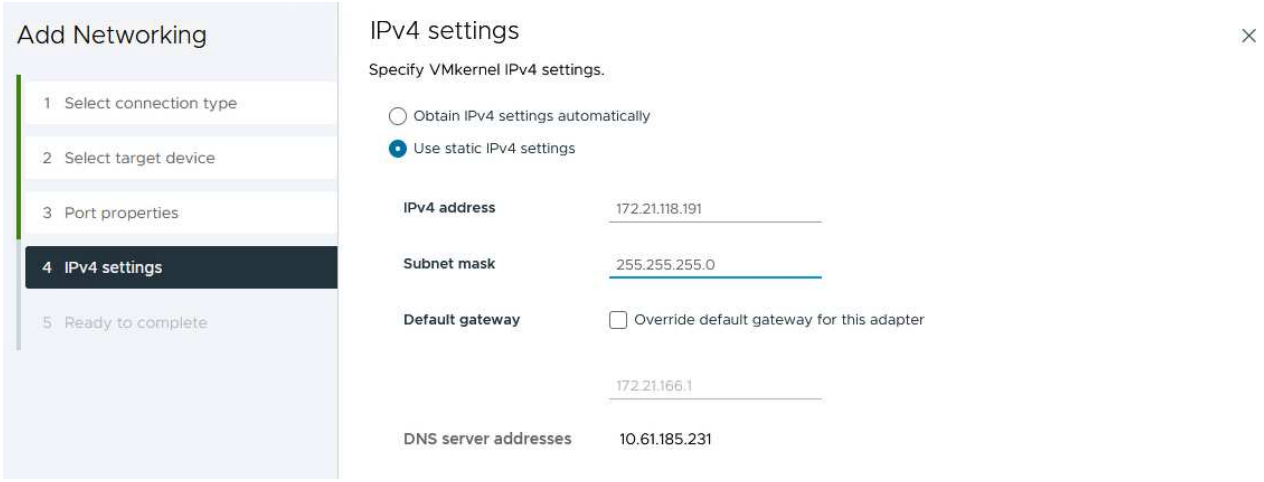
3. 대상 장치 선택 페이지에서 이전에 생성한 iSCSI용 분산 포트 그룹 중 하나를 선택합니다.



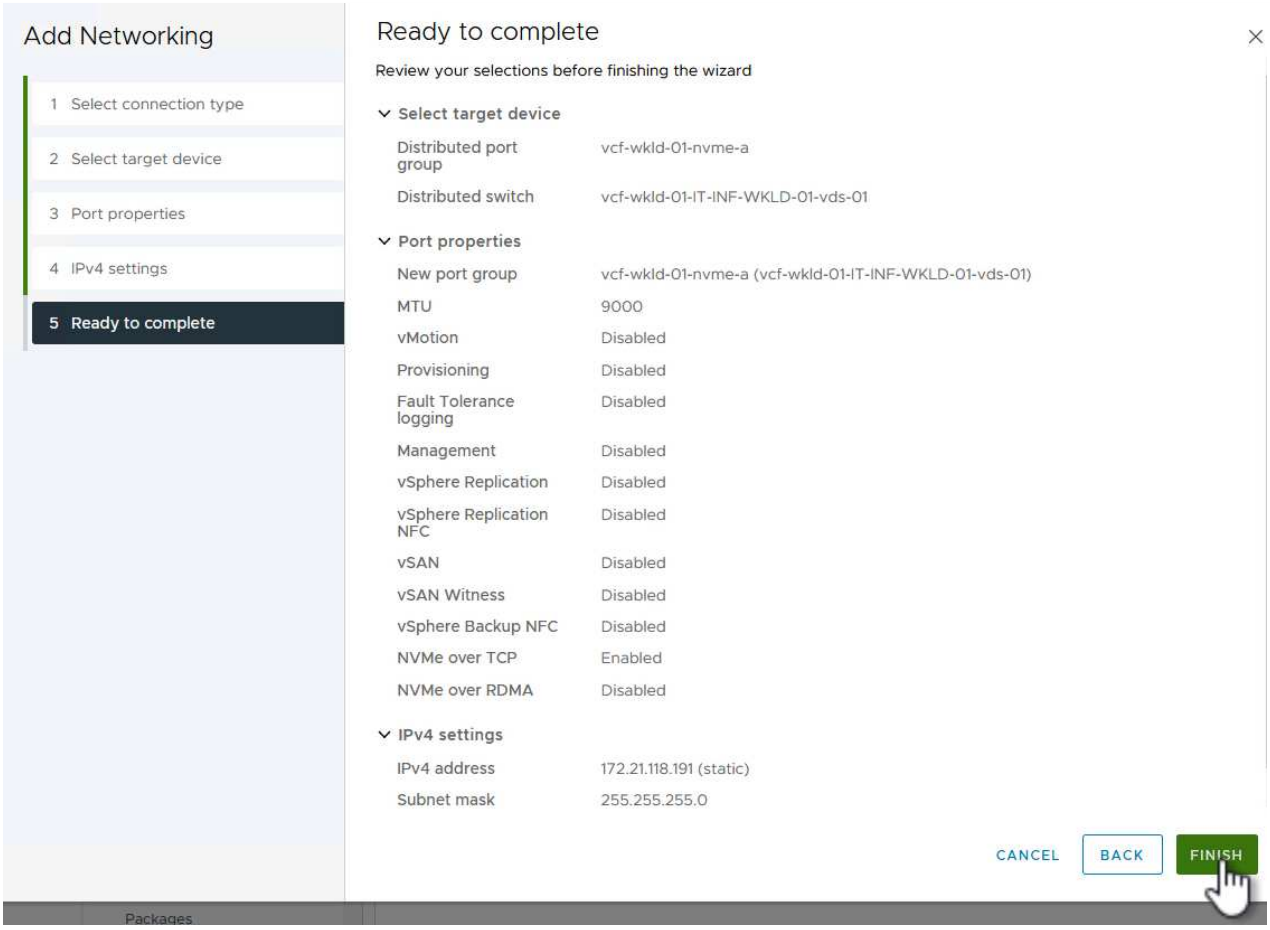
4. 포트 속성 페이지에서 **NVMe over TCP** 상자를 클릭하고 *다음*을 클릭하여 계속합니다.



5. **IPv4** 설정 페이지에서 **IP** 주소, *서브넷 마스크*를 입력하고 새로운 게이트웨이 IP 주소를 입력합니다(필요한 경우에만). 계속하려면 *다음*을 클릭하세요.



6. 완료 준비 페이지에서 선택 사항을 검토하고 *마침*을 클릭하여 VMkernel 어댑터를 만듭니다.



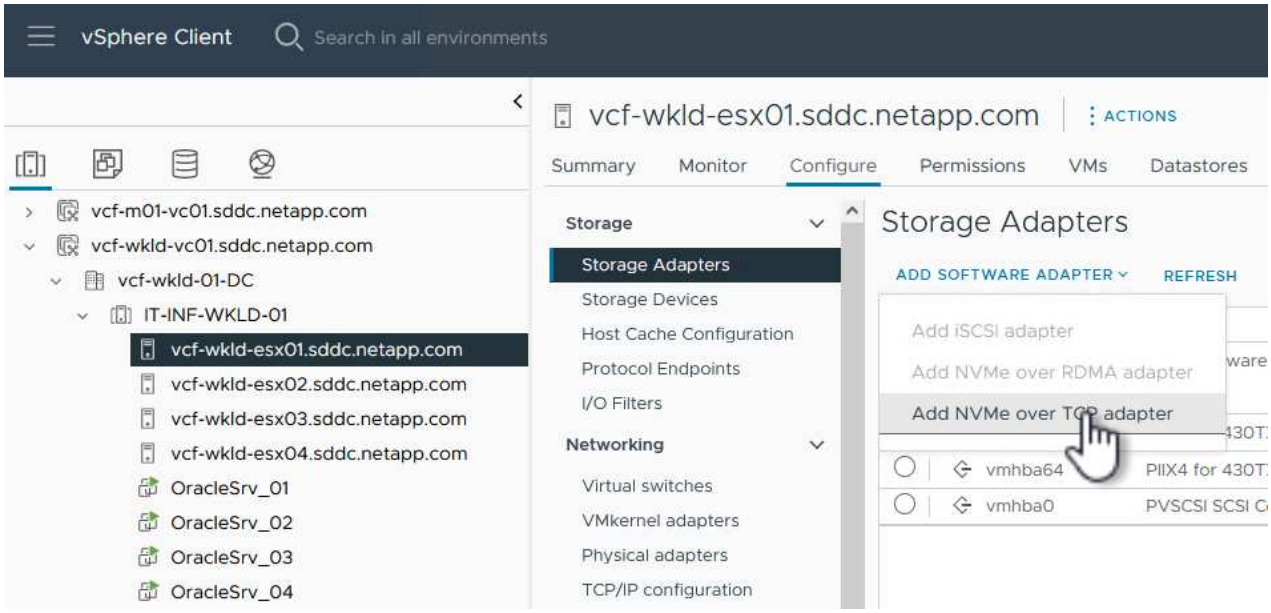
7. 두 번째 iSCSI 네트워크에 대한 VMkernel 어댑터를 생성하려면 이 과정을 반복합니다.

NVMe over TCP 어댑터 추가

워크로드 도메인 클러스터의 각 ESXi 호스트에는 스토리지 트래픽에 전용된 모든 NVMe/TCP 네트워크에 대해 NVMe over TCP 소프트웨어 어댑터가 설치되어 있어야 합니다.

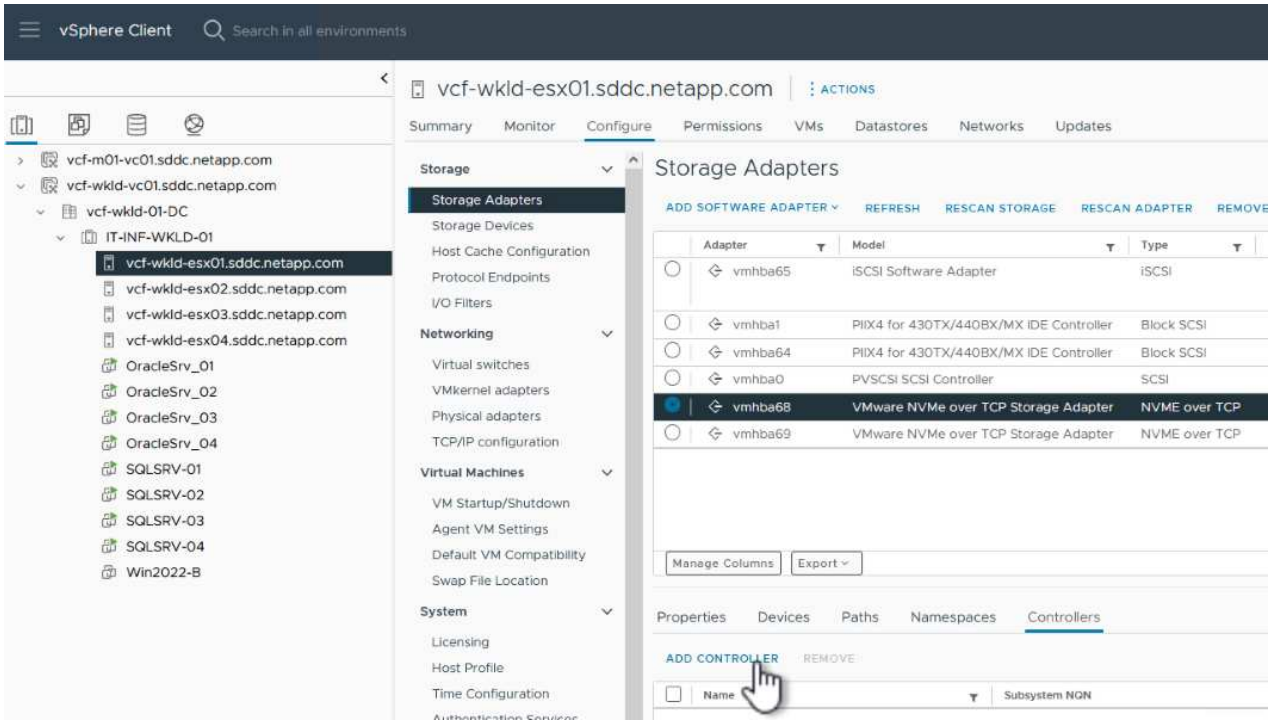
NVMe over TCP 어댑터를 설치하고 NVMe 컨트롤러를 검색하려면 다음 단계를 완료하세요.

1. vSphere 클라이언트에서 워크로드 도메인 클러스터의 ESXi 호스트 중 하나로 이동합니다. 구성 탭에서 메뉴의 스토리지 어댑터*를 클릭한 다음, *소프트웨어 어댑터 추가 드롭다운 메뉴에서 *NVMe over TCP 어댑터 추가*를 선택합니다.

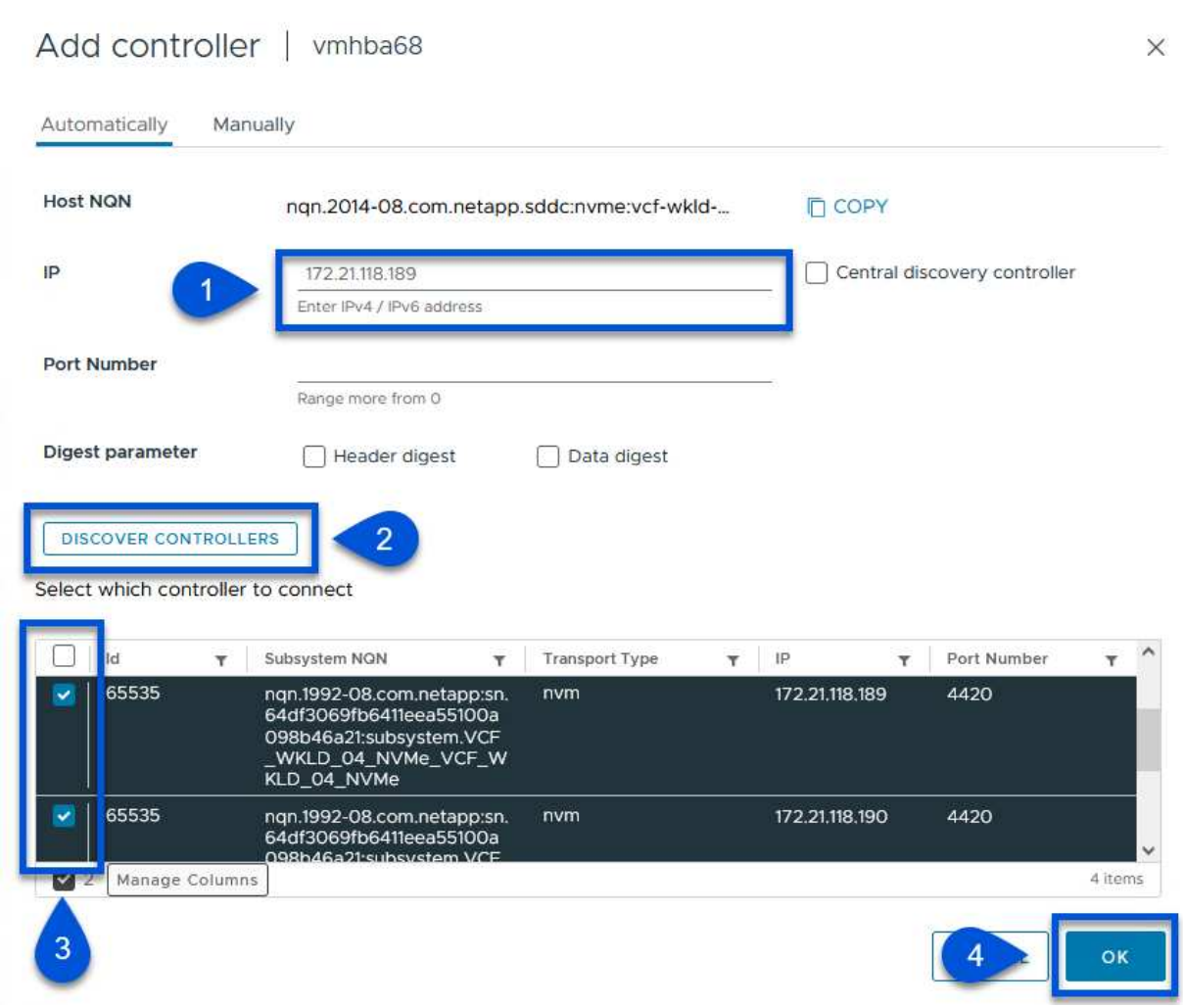


2. 소프트웨어 **NVMe over TCP** 어댑터 추가 창에서 물리적 네트워크 어댑터 드롭다운 메뉴에 액세스하여 NVMe 어댑터를 활성화할 올바른 물리적 네트워크 어댑터를 선택합니다.

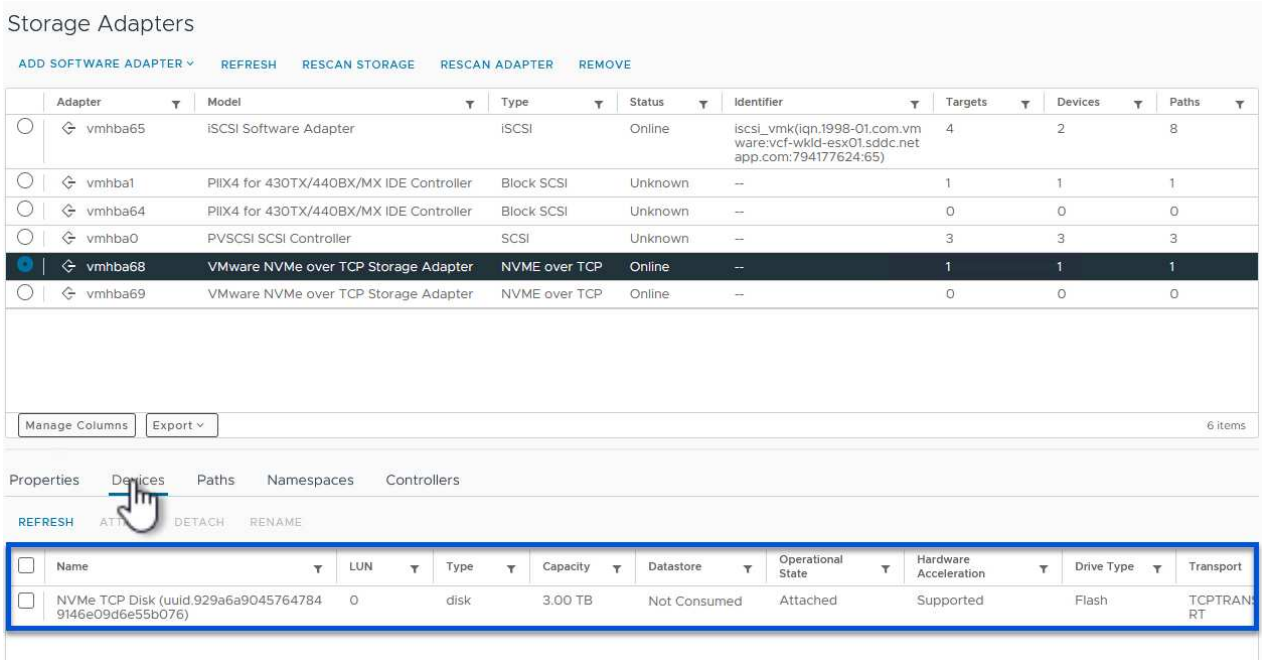
3. TCP 트래픽을 통한 NVMe에 할당된 두 번째 네트워크에 대해 이 프로세스를 반복하여 올바른 물리적 어댑터를 할당합니다.
4. 새로 설치된 NVMe over TCP 어댑터 중 하나를 선택하고, 컨트롤러 탭에서 *컨트롤러 추가*를 선택합니다.



5. 컨트롤러 추가 창에서 자동 탭을 선택하고 다음 단계를 완료합니다.
   - 이 NVMe over TCP 어댑터에 할당된 물리적 어댑터와 동일한 네트워크에 있는 SVM 논리 인터페이스 중 하나에 대한 IP 주소를 입력합니다.
   - 컨트롤러 검색 버튼을 클릭하세요.
   - 검색된 컨트롤러 목록에서 네트워크 주소가 NVMe over TCP 어댑터와 일치하는 두 컨트롤러의 확인란을 클릭합니다.
   - 선택한 컨트롤러를 추가하려면 확인 버튼을 클릭하세요.



6. 몇 초 후에 NVMe 네임스페이스가 장치 탭에 나타납니다.

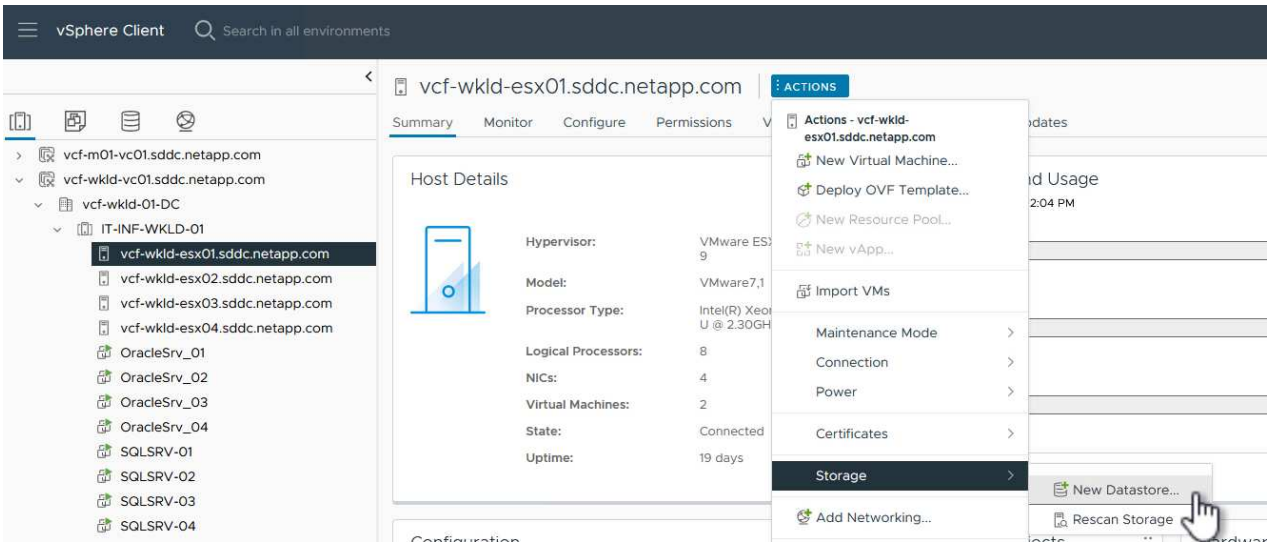


7. NVMe/TCP 트래픽을 위해 설정된 두 번째 네트워크에 대해 NVMe over TCP 어댑터를 생성하려면 이 절차를 반복합니다.

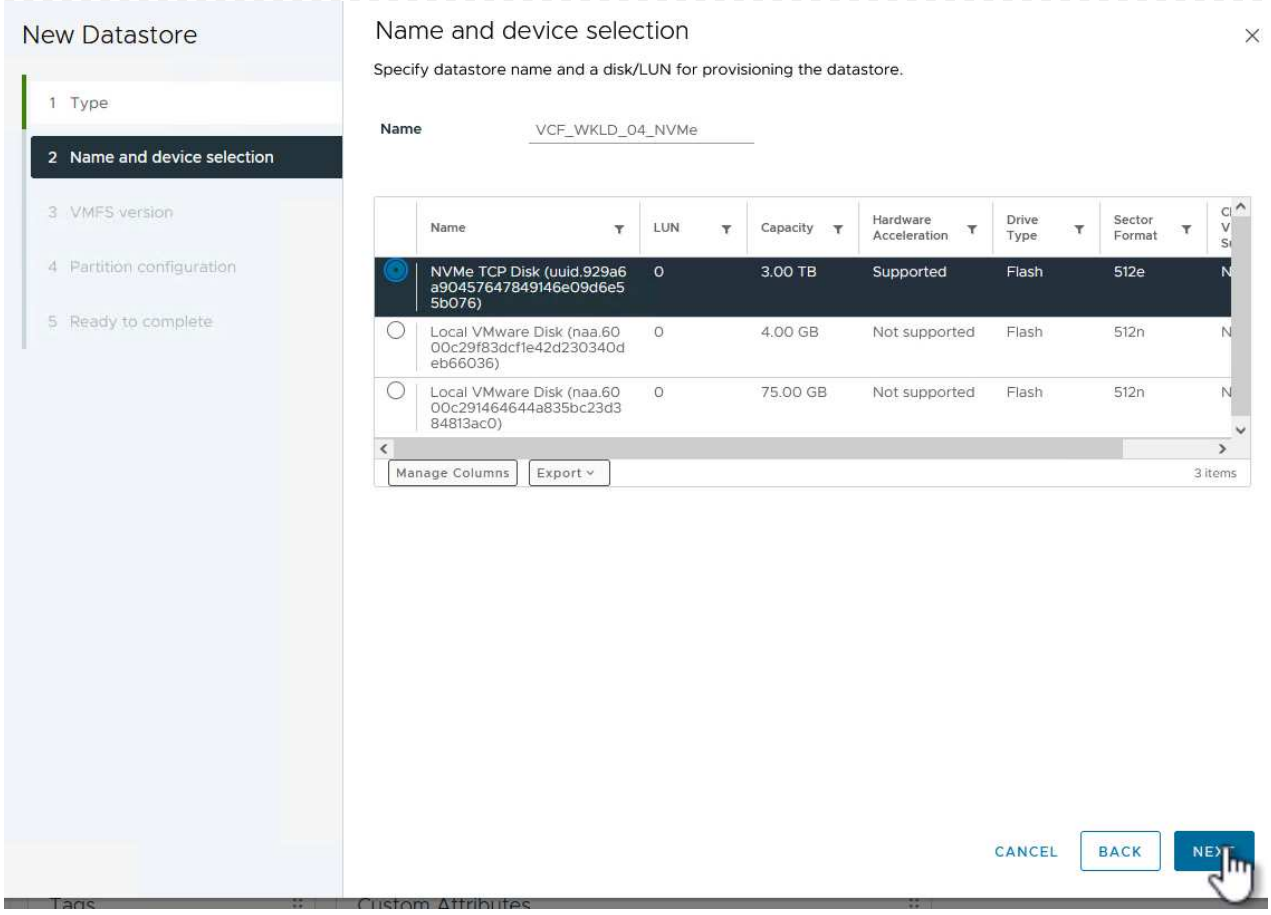
TCP 데이터 저장소를 통한 **NVMe** 배포

NVMe 네임스페이스에 VMFS 데이터 저장소를 생성하려면 다음 단계를 완료하세요.

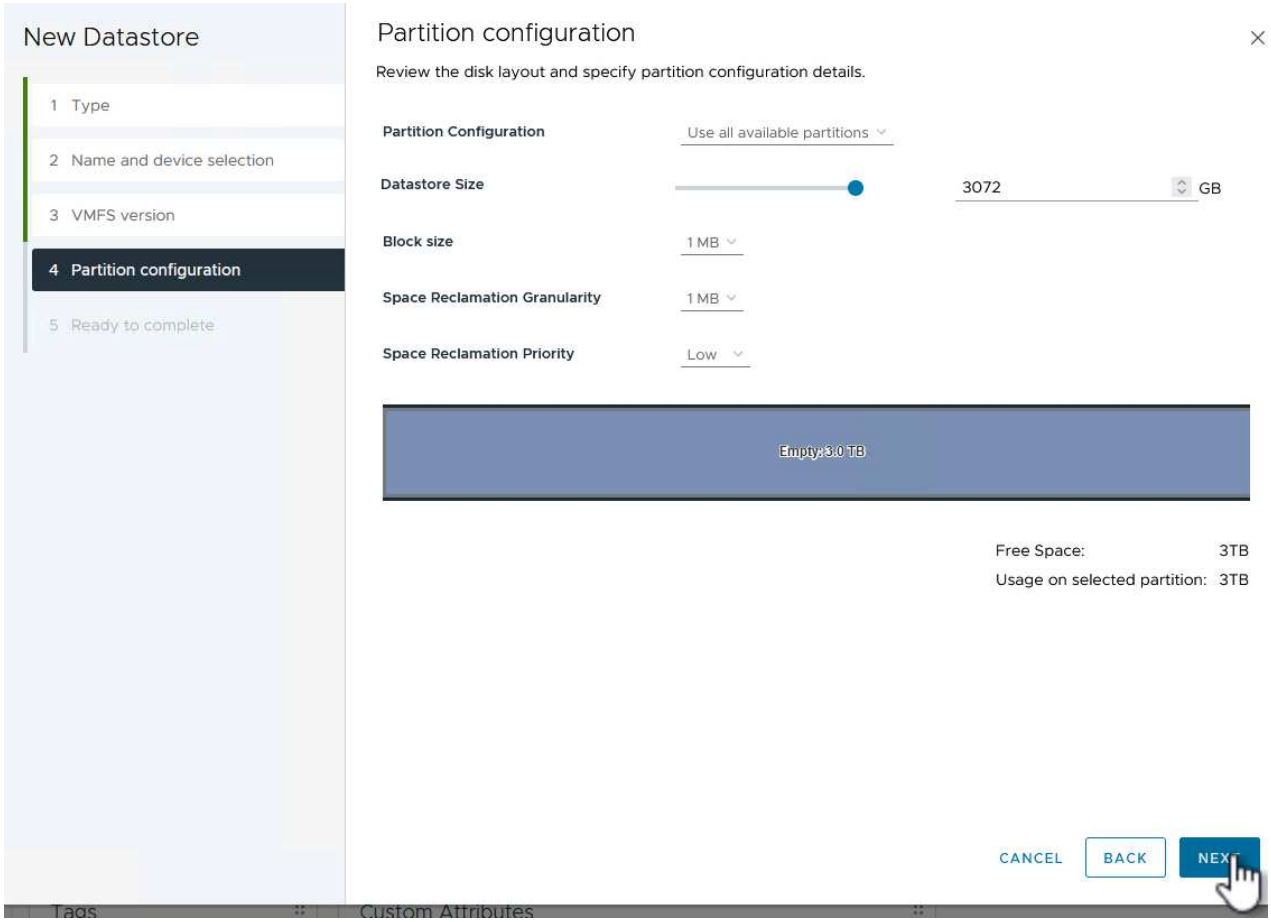
1. vSphere 클라이언트에서 워크로드 도메인 클러스터의 ESXi 호스트 중 하나로 이동합니다. 작업 메뉴에서 *저장소 > 새 데이터 저장소...*를 선택합니다.



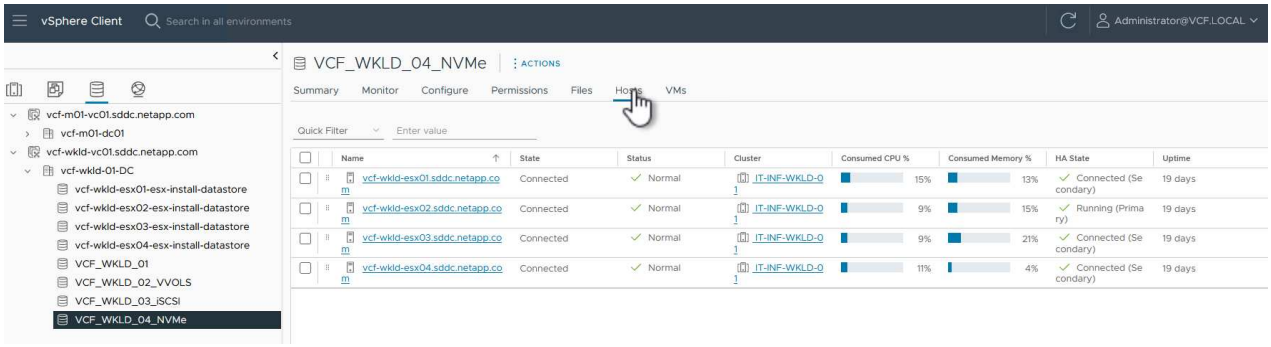
2. 새 데이터 저장소 마법사에서 유형으로 *VMFS*를 선택합니다. 계속하려면 *다음*을 클릭하세요.
3. 이름 및 장치 선택 페이지에서 데이터 저장소의 이름을 입력하고 사용 가능한 장치 목록에서 NVMe 네임스페이스를 선택합니다.



4. **VMFS** 버전 페이지에서 데이터 저장소의 VMFS 버전을 선택합니다.
5. 파티션 구성 페이지에서 기본 파티션 구성에 원하는 변경 사항을 적용합니다. 계속하려면 *다음*을 클릭하세요.



6. 완료 준비 페이지에서 요약을 검토하고 *마침*을 클릭하여 데이터 저장소를 만듭니다.
7. 인벤토리의 새 데이터 저장소로 이동하여 호스트 탭을 클릭합니다. 올바르게 구성된 경우 클러스터의 모든 ESXi 호스트가 나열되고 새 데이터 저장소에 액세스할 수 있어야 합니다.



추가 정보

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

VI 워크로드 도메인에 보조 스토리지로 FC 기반 VMFS 데이터 저장소 추가

이 사용 사례에서는 VMware Cloud Foundation(VCF) Virtual Infrastructure(VI) 워크로드 도메인에 대한 보조 스토리지로 파이버 채널(FC)을 사용하여 VMFS 데이터 저장소를 구성하는 절차를 설명합니다. 이 절차에서는 VMware vSphere용 ONTAP 도구 배포, VI 워크로드 vCenter 서버 등록, 스토리지 백엔드 정의, FC 데이터스토어 프로비저닝을 요약합니다.

파이버 채널의 이점

고성능: FC는 고속 데이터 전송률을 제공하므로 대량의 데이터에 빠르고 안정적으로 액세스해야 하는 애플리케이션에 이상적입니다.

낮은 지연 시간: 매우 낮은 지연 시간은 데이터베이스 및 가상화 환경과 같은 성능에 민감한 애플리케이션에 매우 중요합니다.

신뢰성: FC 네트워크는 내장된 중복성 및 오류 수정과 같은 기능을 갖추고 있어 견고성과 안정성이 뛰어난 것으로 알려져 있습니다.

전용 대역폭: FC는 스토리지 트래픽에 전용 대역폭을 제공하여 네트워크 혼잡 위험을 줄입니다.

NetApp 스토리지 시스템에서 파이버 채널을 사용하는 방법에 대한 자세한 내용은 다음을 참조하세요. "FC를 사용한 SAN 프로비저닝" .

시나리오 개요

VCF 보충 데이터 저장소는 vCenter를 사용한 2일차 작업의 일부로 제공됩니다. 이 시나리오에서는 다음과 같은 상위 수준 단계를 다룹니다.

- 관리 도메인에 ONTAP 도구 배포
- ONTAP 도구에 VI 워크로드 vCenter 서버 등록
- VMware vSphere용 ONTAP 도구 플러그인에서 스토리지 백엔드 정의
- FC 전송에 VMFS 프로비저닝

필수 조건

이 시나리오에는 다음과 같은 구성 요소와 구성이 필요합니다.

- FC 스위치에 연결된 FC 포트가 있는 ONTAP AFF 또는 ASA 스토리지 시스템.
- FC lifes로 생성된 SVM입니다.
- FC 스위치에 연결된 FC HBA가 있는 vSphere.
- FC 스위치에는 단일 이니시에이터-타겟 구역 설정이 구성됩니다.

> ONTAP 시스템의 물리적 FC 포트 대신 영역 구성에서 SVM FC 논리적 인터페이스를 사용합니다.

NetApp FC LUN에 대해 다중 경로를 권장합니다.

ONTAP 스토리지 시스템에서 파이버 채널을 구성하는 방법에 대한 자세한 내용은 다음을 참조하세요. "SAN 스토리지

관리" ONTAP 9 문서에서.

ONTAP 스토리지 시스템과 함께 VMFS를 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오."VMFS 배포 가이드" .

VI 워크로드 도메인에 대한 배포 단계

ONTAP 도구를 배포하고 이를 사용하여 VCF VI 워크로드 도메인에 VMFS 데이터 저장소를 생성하려면 다음 단계를 완료하세요.

- "vCenter 플러그인을 활성화하려면 VI 워크로드 vCenter를 등록하세요."
- "vSphere 클라이언트 인터페이스를 사용하여 스토리지 백엔드 정의"
- "FC에 VMFS 프로비저닝"

추가 정보

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

이 솔루션에 대한 비디오 데모

VCF 관리 도메인을 위한 보조 저장소로서의 VMFS(FC) 데이터 저장소

SnapCenter 로 VCF 보호

VMware vSphere용 SnapCenter 플러그인을 사용하여 VCF 워크로드 도메인을 보호하는 방법에 대해 알아보세요.

SnapCenter Plug-in for VMware vSphere 사용하여 VMware Cloud Foundation(VCF) 워크로드를 보호하는 데 사용할 수 있는 NetApp 솔루션에 대해 알아보세요. 이 플러그인은 백업과 복구를 간소화하고, 애플리케이션 일관성 백업을 보장하며, NetApp의 효율성 기술로 스토리지를 최적화합니다.

vSphere 클라이언트와의 원활한 통합을 제공하는 동시에 자동화된 워크플로와 확장 가능한 운영을 지원합니다. SnapMirror 복제 기능은 온프레미스 또는 클라우드에 2차 백업을 제공하여 가상화된 환경에서 강력한 데이터 보호와 운영 효율성을 제공합니다.

자세한 내용은 다음 솔루션을 참조하세요.

- "VCF 워크로드 도메인 보호"
- "VCF 다중 워크로드 도메인 보호"
- "NVMe로 VCF 워크로드 도메인 보호"
- "SnapCenter 플러그인과 BlueXP backup and recovery 통한 VMware용 3-2-1 데이터 보호"

VMware vSphere용 SnapCenter 플러그인을 사용하여 VCF 워크로드 도메인 보호

이 사용 사례에서는 VMware vSphere용 SnapCenter 플러그인을 사용하여 VMware Cloud Foundation(VCF) 워크로드 도메인에서 VM과 데이터 저장소를 백업하고 복원하는 절차를 설명합니다. 이 절차에서는 VMware vSphere용 SnapCenter 플러그인 배포, 스토리지 시스템 추가, 백업 정책 생성, VM 및 파일 복원 수행에 대한 내용을 요약합니다.

이 솔루션에서는 VMFS 데이터 저장소의 저장 프로토콜로 *iSCSI*가 사용됩니다.

시나리오 개요

이 시나리오에서는 다음과 같은 상위 수준 단계를 다룹니다.

- VI 워크로드 도메인에 SnapCenter Plug-in for VMware vSphere 배포합니다.
- SCV에 저장 시스템을 추가합니다.
- SCV에서 백업 정책을 만듭니다.
- SCV에서 리소스 그룹을 만듭니다.
- SCV를 사용하여 데이터 저장소나 특정 VM을 백업합니다.
- SCV를 사용하여 VM을 클러스터의 대체 위치로 복원합니다.
- SCV를 사용하여 Windows 파일 시스템으로 파일을 복원합니다.

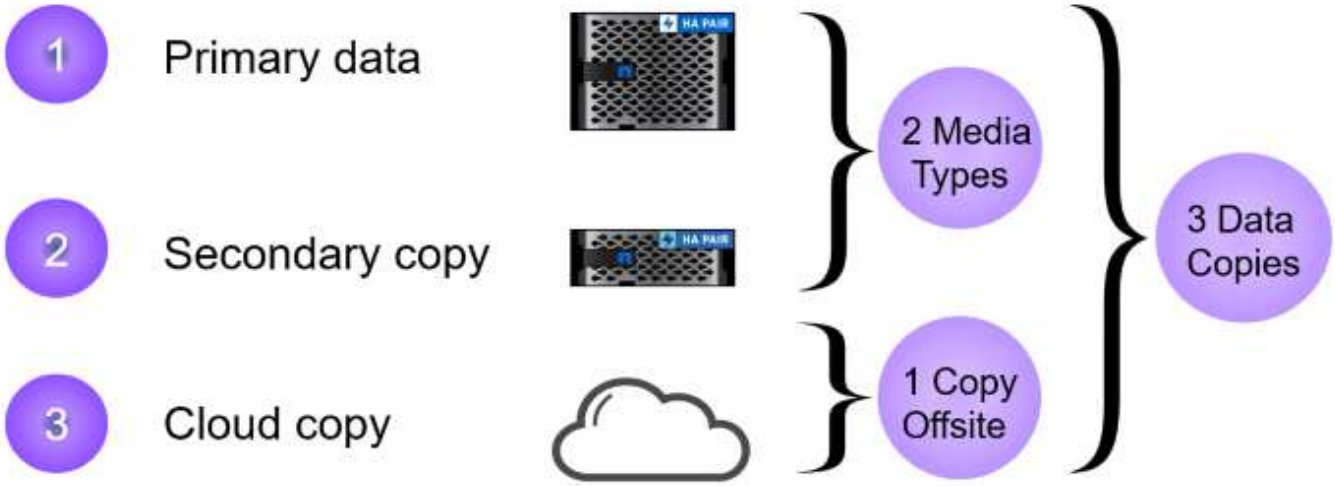
필수 조건

이 시나리오에는 다음과 같은 구성 요소와 구성이 필요합니다.

- 워크로드 도메인 클러스터에 할당된 iSCSI VMFS 데이터 저장소가 있는 ONTAP ASA 스토리지 시스템입니다.
- SnapMirror 사용하여 보조 백업을 수신하도록 구성된 보조 ONTAP 스토리지 시스템입니다.
- VCF 관리 도메인 배포가 완료되었으며 vSphere 클라이언트에 액세스할 수 있습니다.
- VI 워크로드 도메인이 이전에 배포되었습니다.
- 가상 머신은 SCV가 보호하도록 지정된 클러스터에 존재합니다.

iSCSI VMFS 데이터 저장소를 보조 저장소로 구성하는 방법에 대한 정보는 다음을 참조하세요."**VMware용 ONTAP 도구를 사용하여 관리 도메인의 보조 스토리지로 iSCSI 사용**" 이 문서에서. OTV를 사용하여 데이터 저장소를 배포하는 프로세스는 관리 및 워크로드 도메인에서 동일합니다.

> SCV로 백업을 보조 저장소에 복제하는 것 외에도, NetApp BlueXP backup and recovery 사용하여 3대(3) 클라우드 공급업체 중 하나의 개체 저장소에 데이터의 오프사이트 복사본을 만들 수 있습니다. 자세한 내용은 솔루션을 참조하세요."SnapCenter 플러그인과 BlueXP backup and recovery 통한 VMware용 3-2-1 데이터 보호" .



배포 단계

SnapCenter 플러그인을 배포하고 이를 사용하여 백업을 생성하고 VM과 데이터 저장소를 복원하려면 다음 단계를 완료하세요.

SCV를 배포하고 사용하여 **VI** 워크로드 도메인의 데이터를 보호합니다.

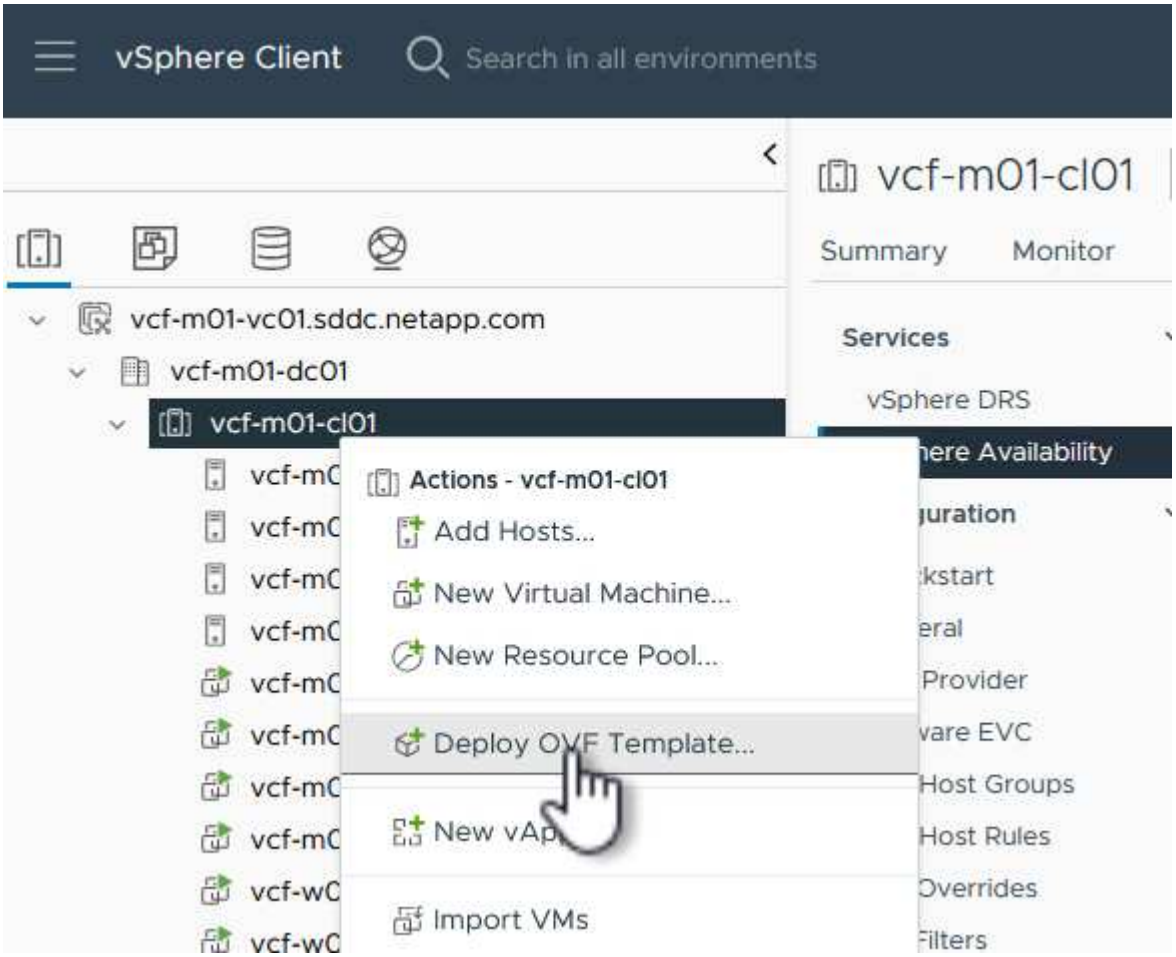
VI 워크로드 도메인에서 데이터를 보호하기 위해 SCV를 배포, 구성 및 사용하려면 다음 단계를 완료하세요.

SnapCenter Plug-in for VMware vSphere 배포

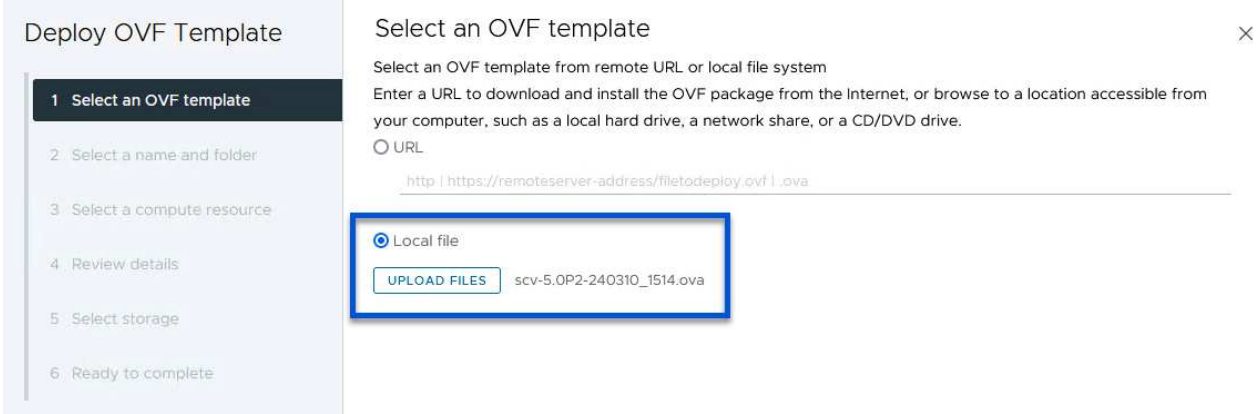
SnapCenter 플러그인은 VCF 관리 도메인에 호스팅되지만 VI 워크로드 도메인의 vCenter에 등록됩니다. 각 vCenter 인스턴스에는 하나의 SCV 인스턴스가 필요하며, 워크로드 도메인에는 단일 vCenter 인스턴스에서 관리하는 여러 클러스터가 포함될 수 있다는 점을 명심하세요.

vCenter 클라이언트에서 다음 단계를 완료하여 SCV를 VI 워크로드 도메인에 배포합니다.

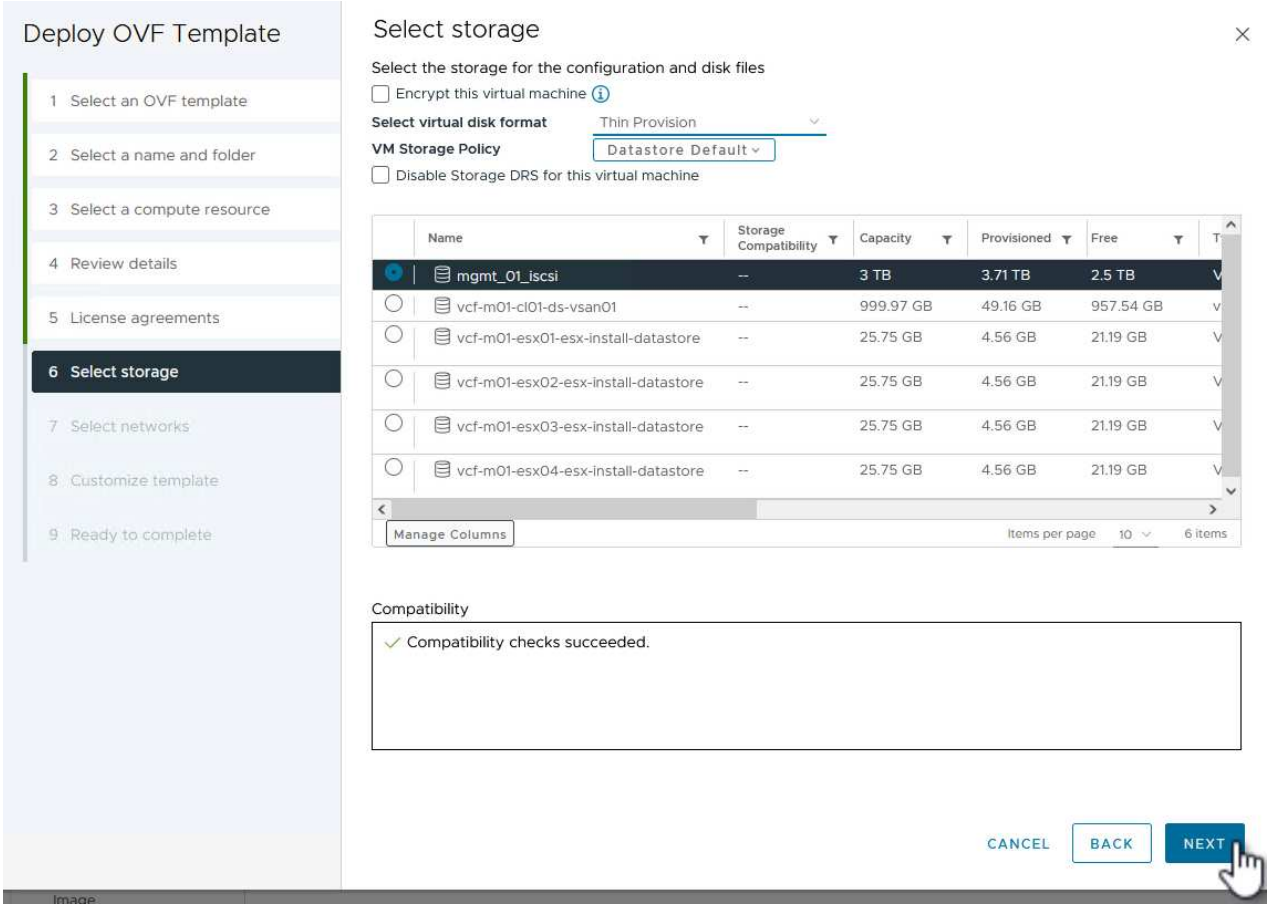
1. NetApp 지원 사이트의 다운로드 영역에서 SCV 배포를 위한 OVA 파일을 다운로드하세요."여기" .
2. 관리 도메인 vCenter Client에서 *OVF 템플릿 배포…*를 선택합니다.



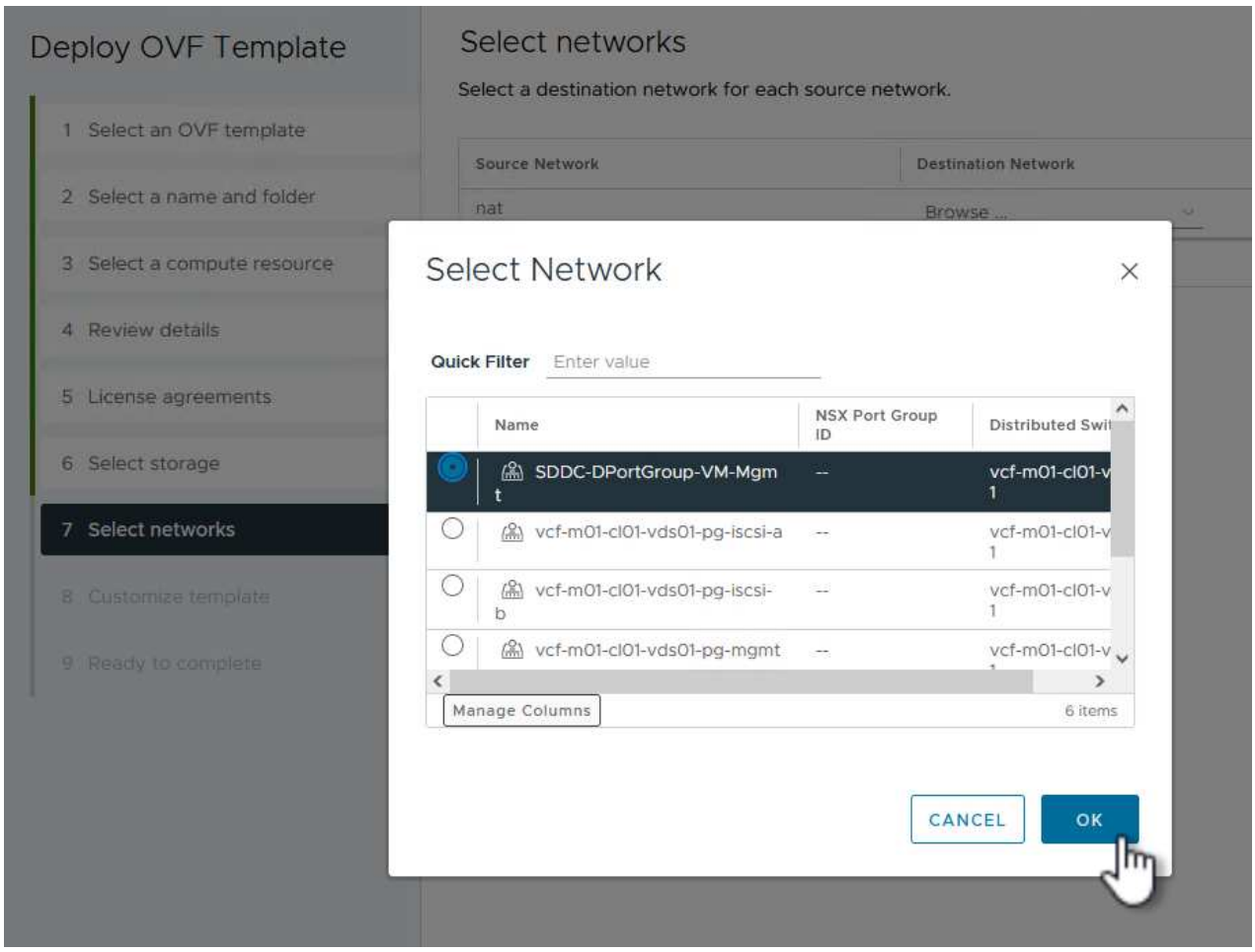
3. **OVF** 템플릿 배포 마법사에서 로컬 파일 라디오 버튼을 클릭한 다음 이전에 다운로드한 OVF 템플릿을 업로드하도록 선택합니다. 계속하려면 *다음*을 클릭하세요.



4. 이름 및 폴더 선택 페이지에서 SCV 데이터 브로커 VM의 이름과 관리 도메인의 폴더를 제공합니다. 계속하려면 *다음*을 클릭하세요.
5. 컴퓨팅 리소스 선택 페이지에서 VM을 설치할 관리 도메인 클러스터 또는 클러스터 내의 특정 ESXi 호스트를 선택합니다.
6. 세부 정보 검토 페이지에서 OVF 템플릿과 관련된 정보를 검토하고 라이선스 계약 페이지에서 라이선스 조건에 동의하세요.
7. 저장소 선택 페이지에서 VM이 설치될 데이터 저장소를 선택하고 *가상 디스크 형식*과 *VM 저장소 정책*을 선택합니다. 이 솔루션에서 VM은 ONTAP 스토리지 시스템에 있는 iSCSI VMFS 데이터 저장소에 설치됩니다. 이는 이전에 이 문서의 별도 섹션에서 배포한 내용입니다. 계속하려면 *다음*을 클릭하세요.



8. 네트워크 선택 페이지에서 워크로드 도메인 vCenter 어플라이언스와 기본 및 보조 ONTAP 스토리지 시스템 모두와 통신할 수 있는 관리 네트워크를 선택합니다.



9. 템플릿 사용자 지정 페이지에서 배포에 필요한 모든 정보를 작성하세요.
   - FQDN 또는 IP 및 워크로드 도메인 vCenter 어플라이언스의 자격 증명입니다.
   - SCV 관리 계정에 대한 자격 증명입니다.
   - SCV 유지 관리 계정에 대한 자격 증명입니다.
   - IPv4 네트워크 속성 세부 정보(IPv6도 사용 가능).
   - 날짜 및 시간 설정.

   계속하려면 *다음*을 클릭하세요.

Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Customize template

Customize the deployment properties of this software solution.

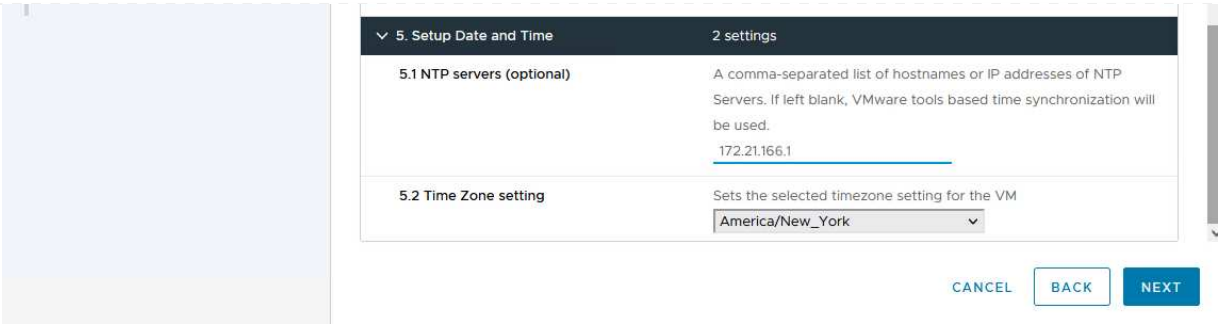
1. Register to existing vCenter	4 settings
1.1 vCenter Name(FQDN) or IP Address	cf-wkld-vc01.sddc.netapp.com
1.2 vCenter username	administrator@vcf.local
1.3 vCenter password	Password ••••••••• Confirm Password •••••••••
1.4 vCenter port	443
2. Create SCV Credentials	2 settings
2.1 Username	admin
2.2 Password	Password ••••••••• Confirm Password •••••••••
3. System Configuration	1 settings

Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Customize template

4.2 Setup IPv4 Network Properties	6 settings
4.2.1 IPv4 Address	IP address for the appliance. (Leave blank if DHCP is desired) 172.21.166.148
4.2.2 IPv4 Netmask	Subnet to use on the deployed network. (Leave blank if DHCP is desired) 255.255.255.0
4.2.3 IPv4 Gateway	Gateway on the deployed network. (Leave blank if DHCP is desired) 172.21.166.1
4.2.4 IPv4 Primary DNS	Primary DNS server's IP address. (Leave blank if DHCP is desired) 10.61.185.231
4.2.5 IPv4 Secondary DNS	Secondary DNS server's IP address. (optional - Leave blank if DHCP is desired) 10.61.186.231
4.2.6 IPv4 Search Domains (optional)	Comma separated list of search domain names to use when resolving host names. (Leave blank if DHCP is desired) netapp.com,sddc.netapp.com
3.3 Setup IPv6 Network Properties	6 settings
4.3.1 IPv6 Address	IP address for the appliance. (Leave blank if DHCP is desired)
4.3.2 IPv6 PrefixLen	Prefix length to use on the deployed network. (Leave blank if DHCP is desired)

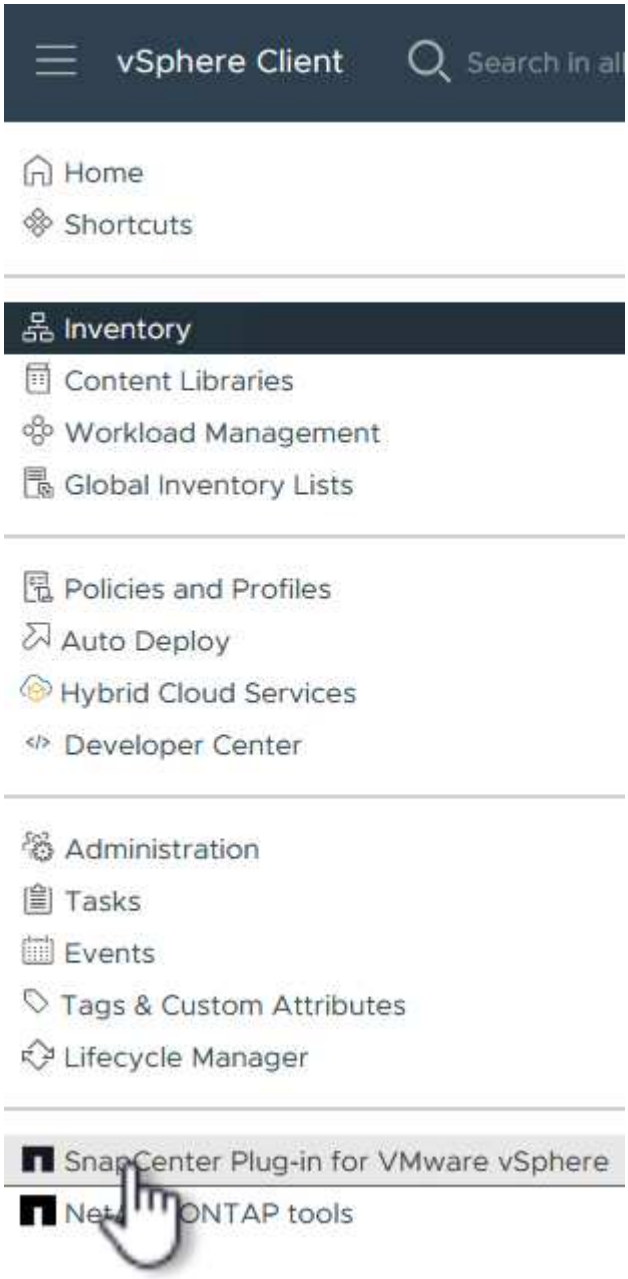


10. 마지막으로, *완료 준비 페이지*에서 모든 설정을 검토하고 마침을 클릭하여 배포를 시작합니다.

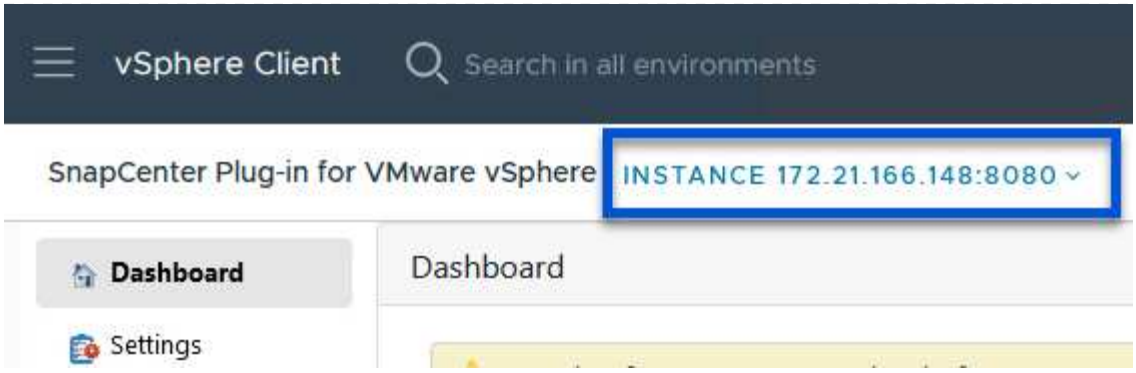
SCV에 스토리지 시스템 추가

SnapCenter 플러그인이 설치되면 다음 단계를 완료하여 SCV에 스토리지 시스템을 추가합니다.

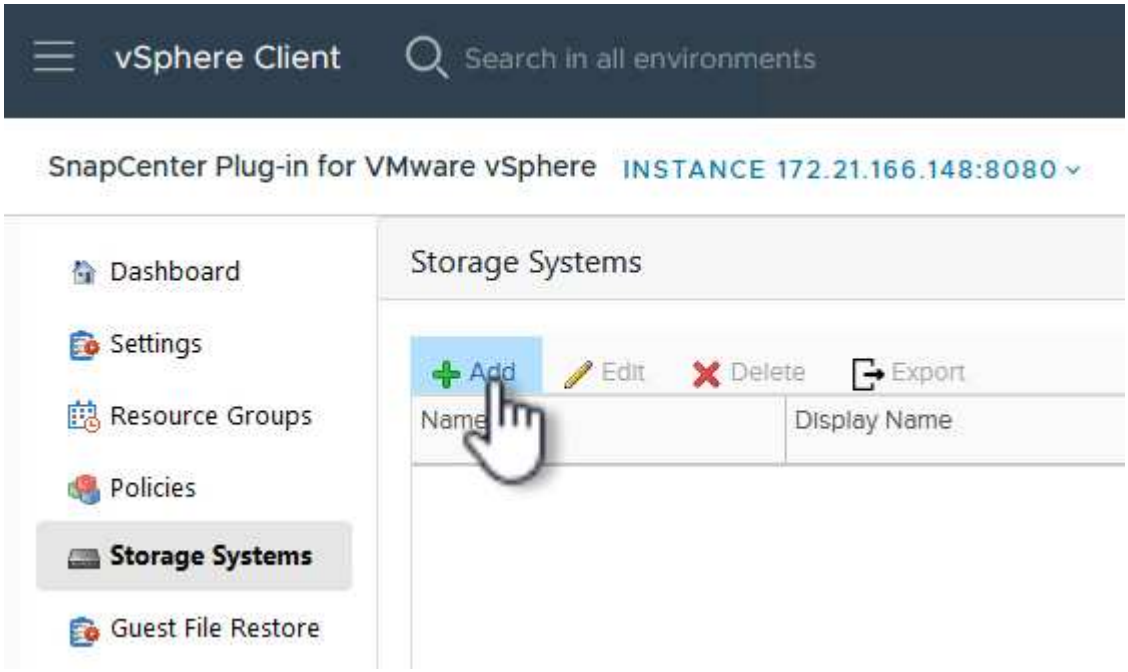
1. SCV는 vSphere Client의 기본 메뉴에서 액세스할 수 있습니다.



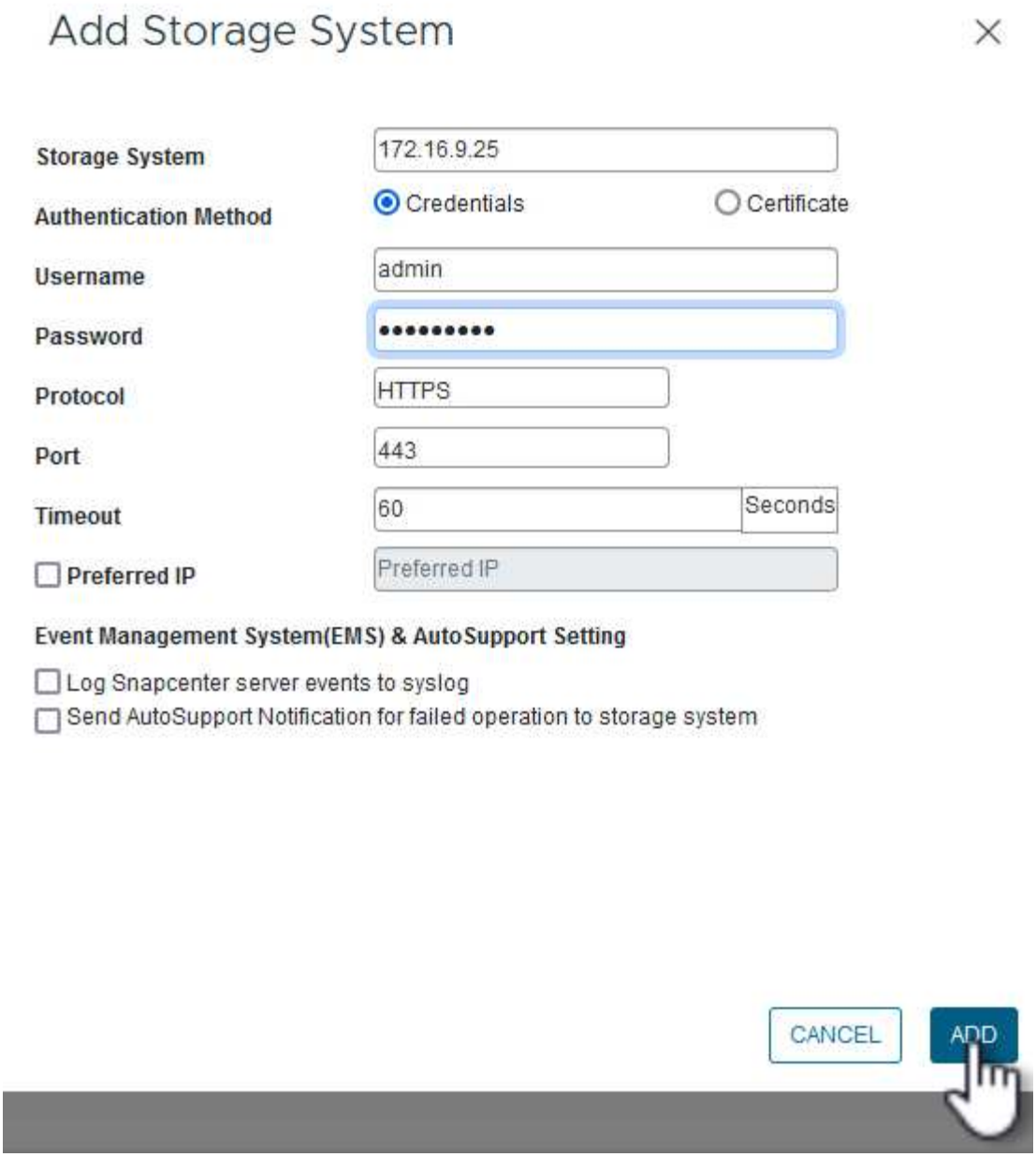
2. SCV UI 인터페이스 상단에서 보호할 vSphere 클러스터와 일치하는 올바른 SCV 인스턴스를 선택합니다.



3. 왼쪽 메뉴에서 *스토리지 시스템*으로 이동한 후 *추가*를 클릭하여 시작하세요.



4. 스토리지 시스템 추가 양식에서 추가할 ONTAP 스토리지 시스템의 IP 주소와 자격 증명을 입력하고 *추가*를 클릭하여 작업을 완료합니다.

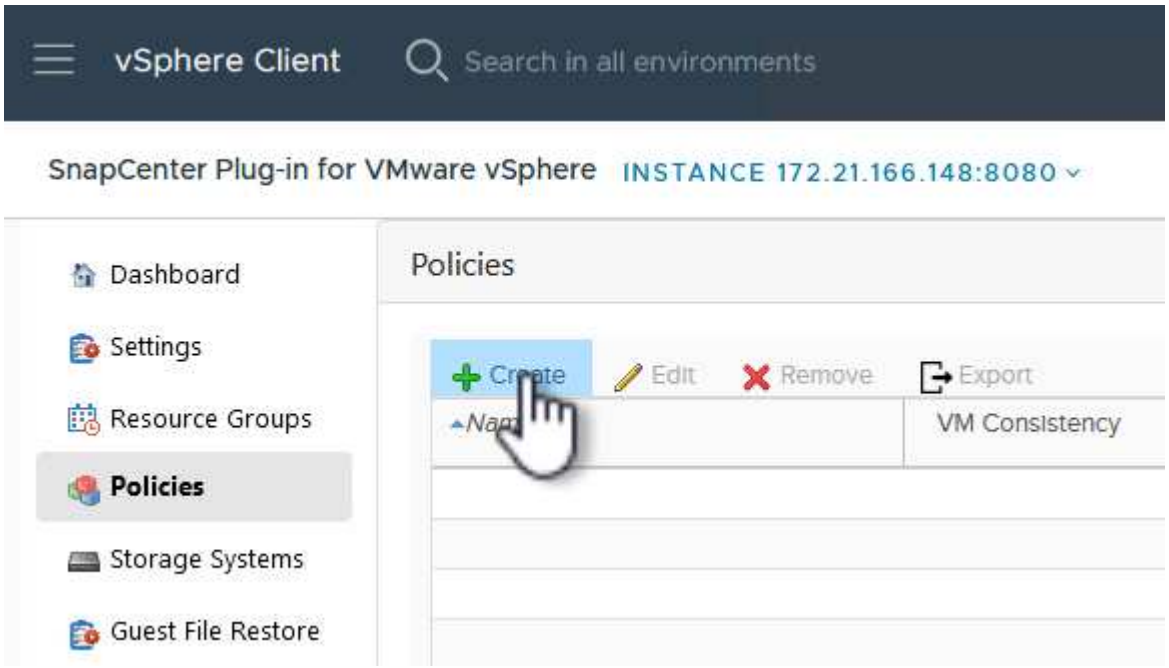


5. 보조 백업 대상으로 사용할 시스템을 포함하여 관리할 추가 저장 시스템에 대해 이 절차를 반복합니다.

SCV 백업 정책 생성에 대한 자세한 내용은 다음을 참조하세요."VM 및 데이터 저장소에 대한 백업 정책 생성" .

새 백업 정책을 만들려면 다음 단계를 완료하세요.

1. 왼쪽 메뉴에서 *정책*을 선택하고 *만들기*를 클릭하여 시작하세요.



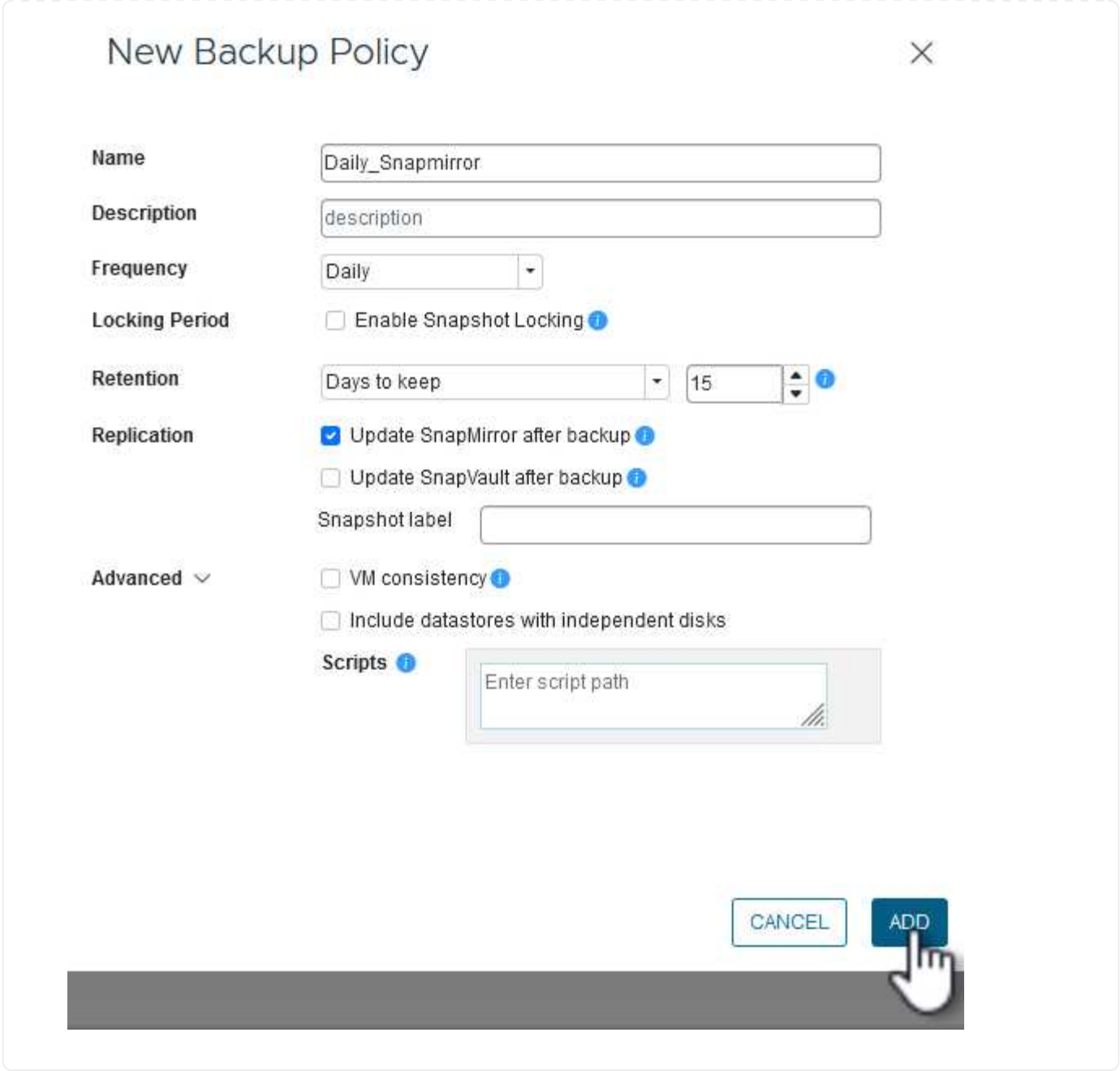
2. 새 백업 정책 양식에서 정책의 이름*과 *설명, 백업이 수행될 빈도, 백업이 보관되는 기간을 지정하는 보존 기간을 입력합니다.

   *잠금 기간*을 사용하면 ONTAP SnapLock 기능을 사용하여 변조 방지 스냅샷을 생성하고 잠금 기간을 구성할 수 있습니다.

   *복제*의 경우 ONTAP 스토리지 볼륨에 대한 기본 SnapMirror 또는 SnapVault 관계를 업데이트하도록 선택합니다.

   > SnapMirror 와 SnapVault 복제는 둘 다 ONTAP SnapMirror 기술을 사용하여 스토리지 볼륨을 보조 스토리지 시스템에 비동기적으로 복제하여 보호와 보안을 강화한다는 점에서 유사합니다. SnapMirror 관계의 경우 SCV 백업 정책에 지정된 보존 일정이 기본 볼륨과 보조 볼륨 모두의 보존을 관리합니다. SnapVault 관계를 사용하면 장기 보관 일정이나 다른 보관 일정에 대해 보조 스토리지 시스템에 별도의 보관 일정을 설정할 수 있습니다. 이 경우 스냅샷 레이블은 SCV 백업 정책과 보조 볼륨과 관련된 정책에 지정되어 독립적인 보존 일정을 적용할 볼륨을 식별합니다.

   추가 고급 옵션을 선택하고 *추가*를 클릭하여 정책을 만듭니다.

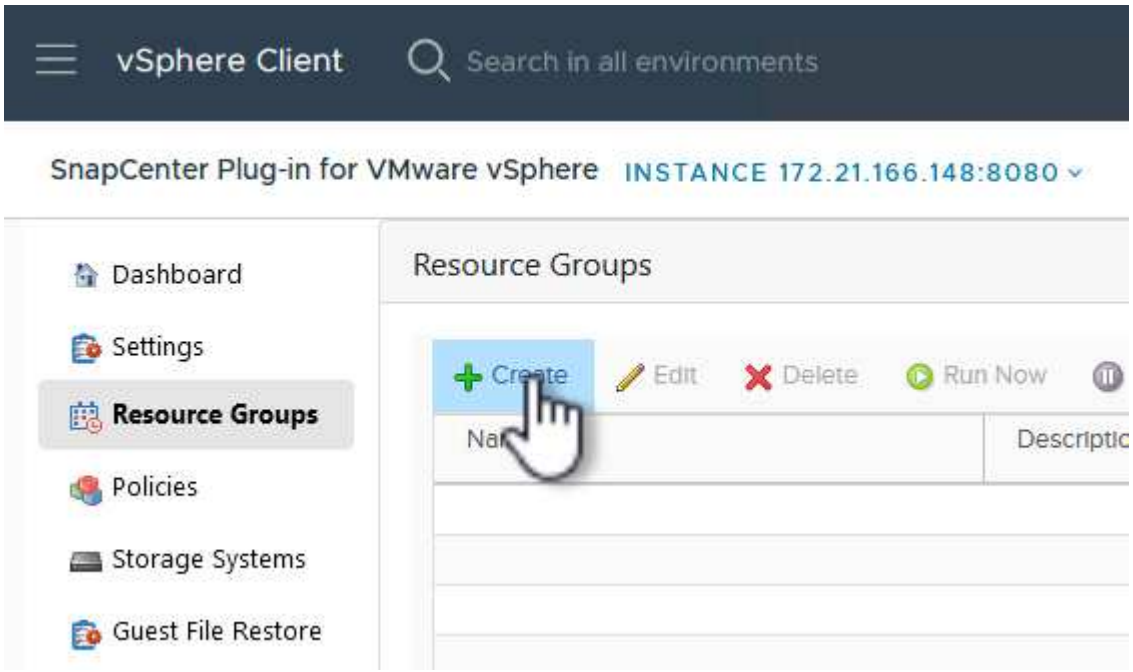

New Backup Policy
Name
Daily_Snapmirror
Description
description
Frequency
Daily
Locking Period
Enable Snapshot Locking
Retention
Days to keep
15
Replication
Update SnapMirror after backup
Update SnapVault after backup
Snapshot label
Advanced
VM consistency
Include datastores with independent disks
Scripts
Enter script path
CANCEL
ADD

SCV에서 리소스 그룹 생성

SCV 리소스 그룹 생성에 대한 자세한 내용은 다음을 참조하세요."리소스 그룹 생성" .

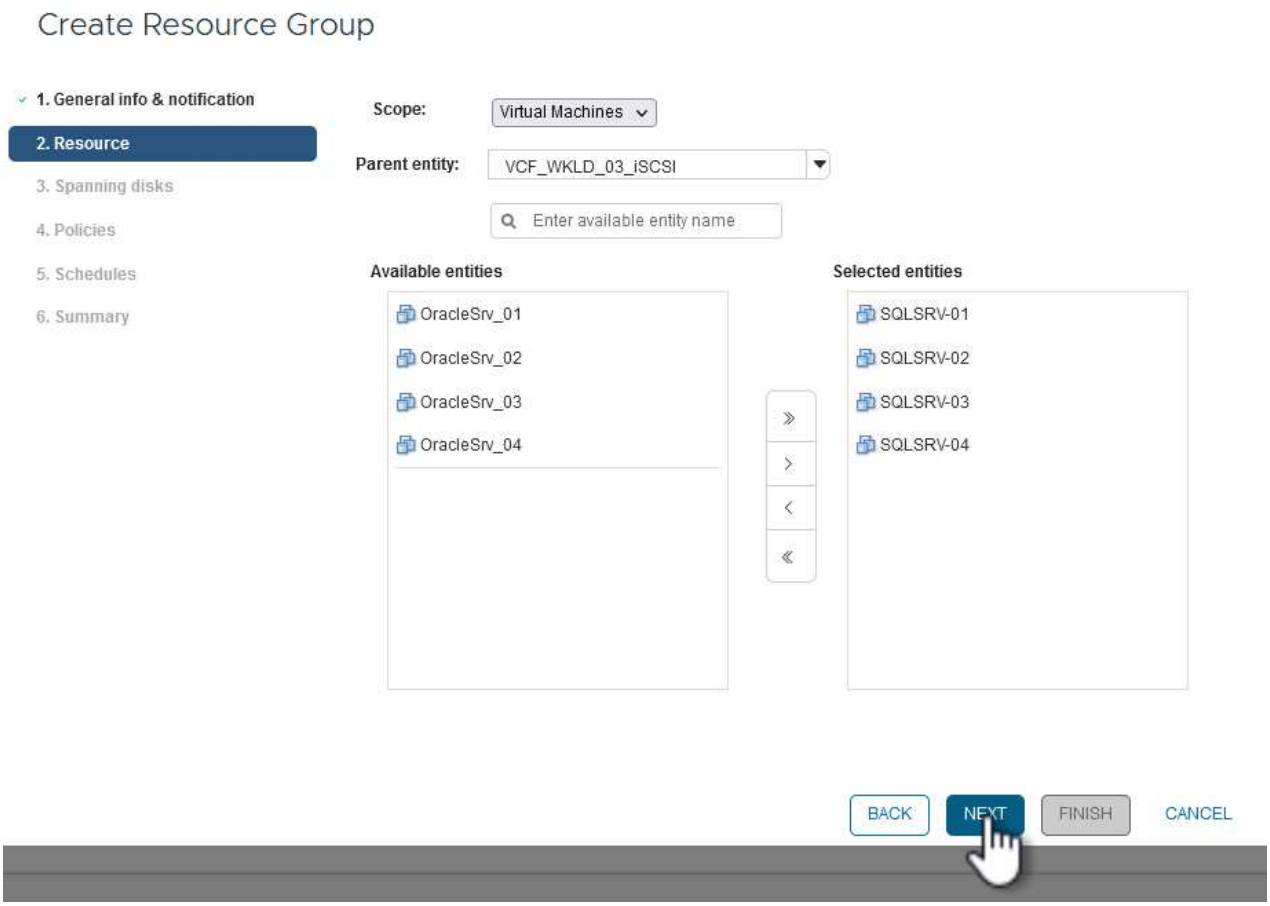
새 리소스 그룹을 만들려면 다음 단계를 완료하세요.

1. 왼쪽 메뉴에서 *리소스 그룹*을 선택하고 *만들기*를 클릭하여 시작하세요.

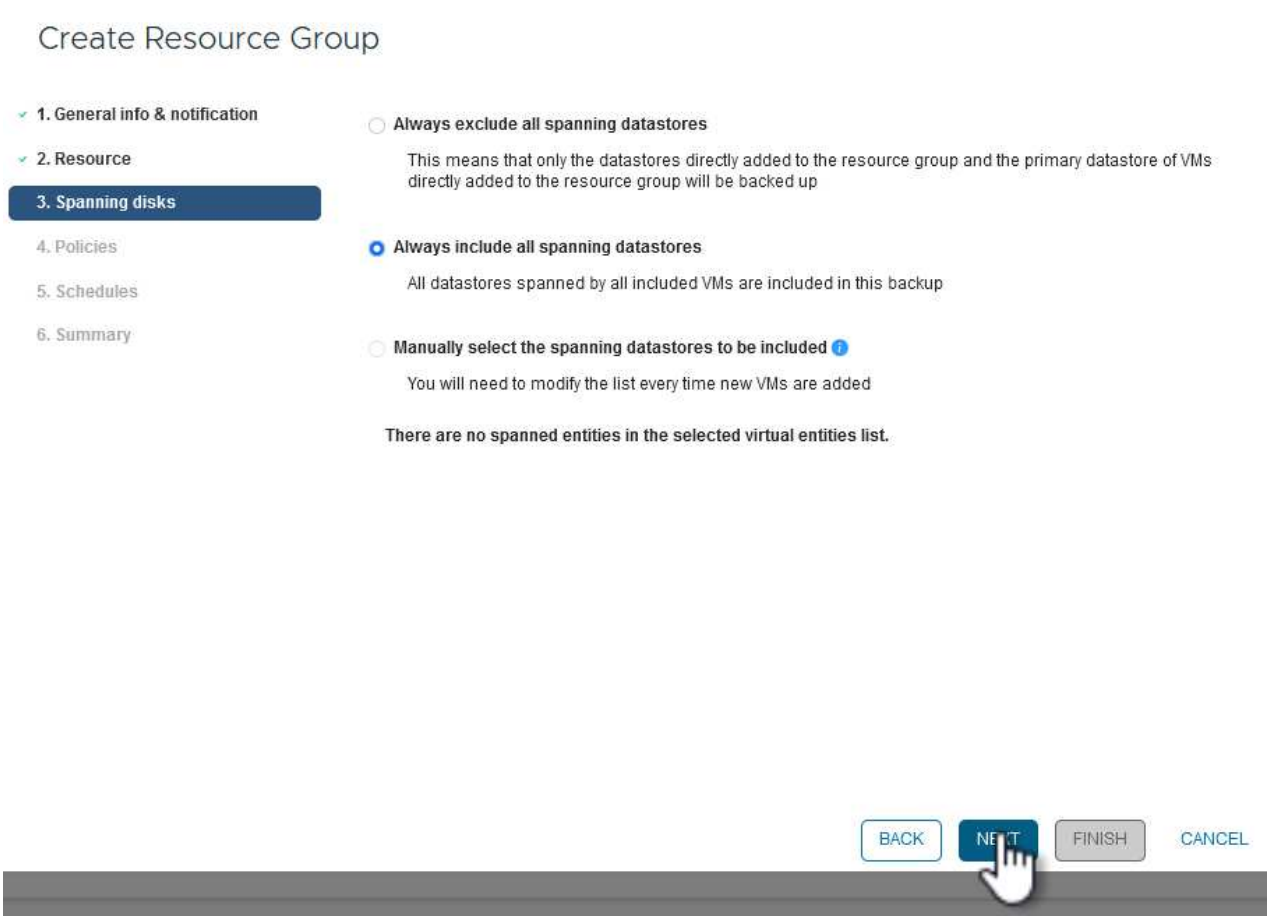


2. 일반 정보 및 알림 페이지에서 리소스 그룹 이름, 알림 설정, 스냅샷 이름 지정에 대한 추가 옵션을 제공합니다.
3. 리소스 페이지에서 리소스 그룹에서 보호할 데이터 저장소와 VM을 선택합니다. 계속하려면 *다음*을 클릭하세요.

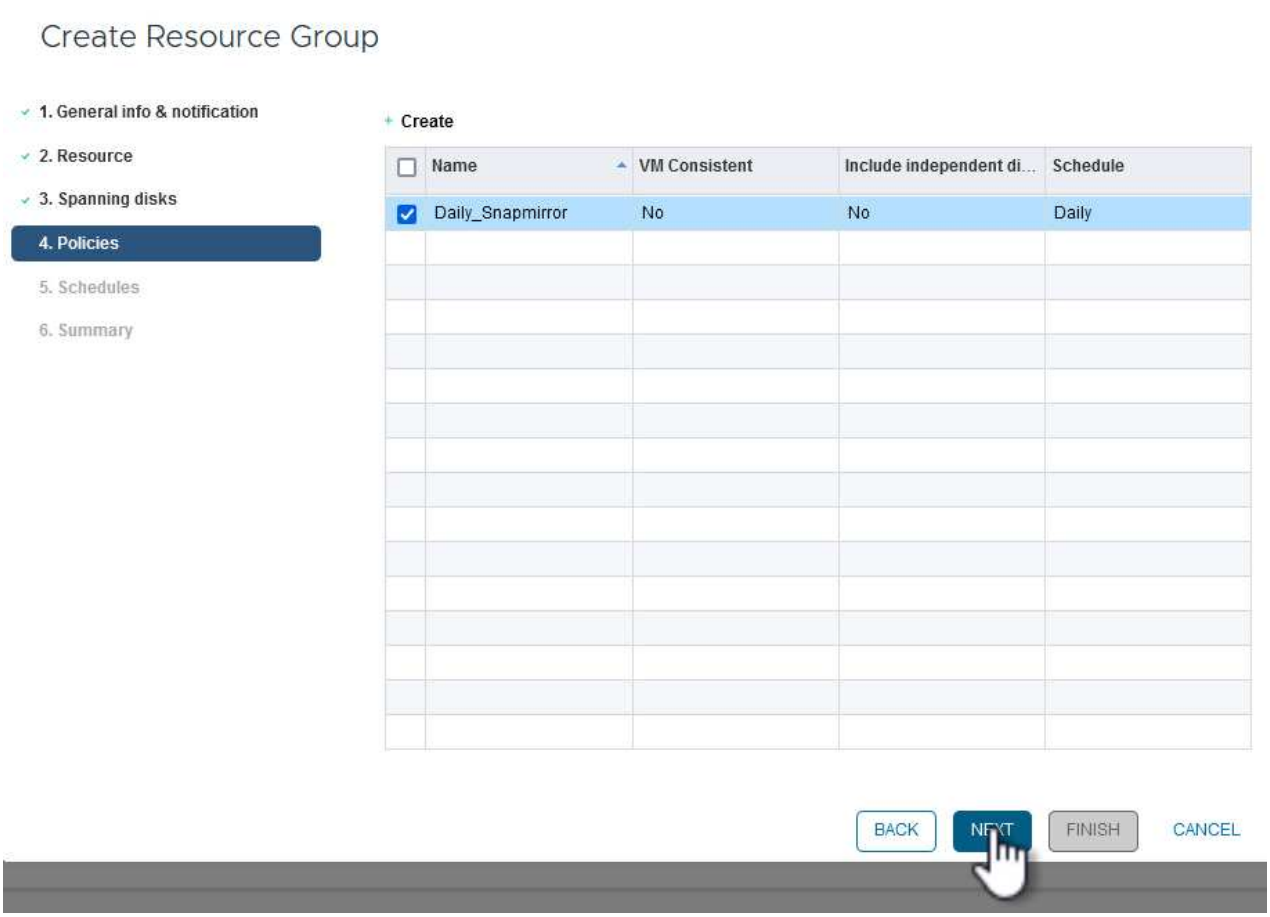
> 특정 VM만 선택한 경우에도 전체 데이터 저장소가 항상 백업됩니다. ONTAP 데이터 저장소를 호스팅하는 볼륨의 스냅샷을 찍기 때문입니다. 하지만 백업을 위해 특정 VM만 선택하면 해당 VM으로만 복원할 수 있는 기능이 제한됩니다.



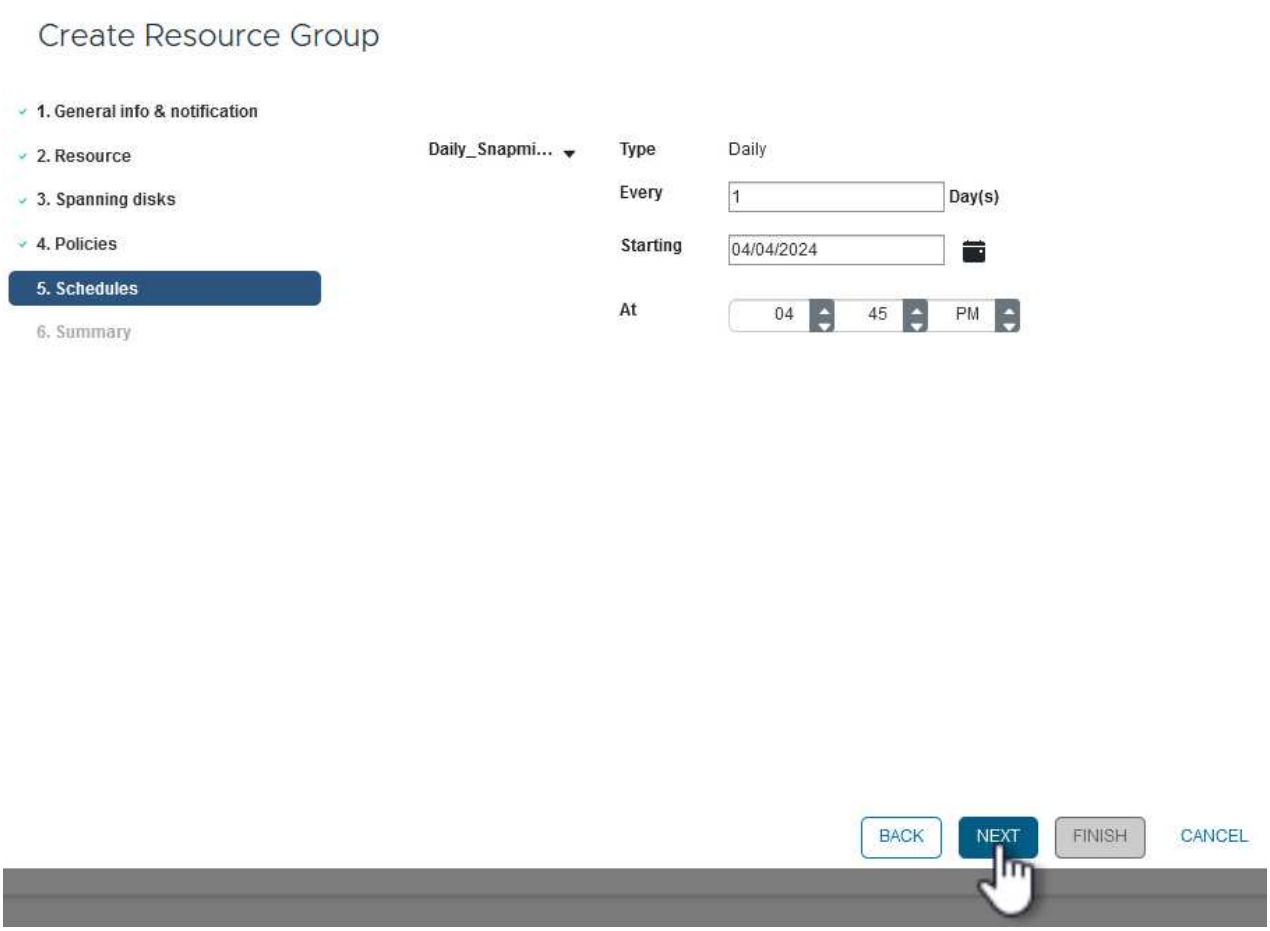
4. 디스크 확장 페이지에서 여러 데이터 저장소에 걸쳐 있는 VMDK를 사용하여 VM을 처리하는 방법에 대한 옵션을 선택합니다. 계속하려면 *다음*을 클릭하세요.



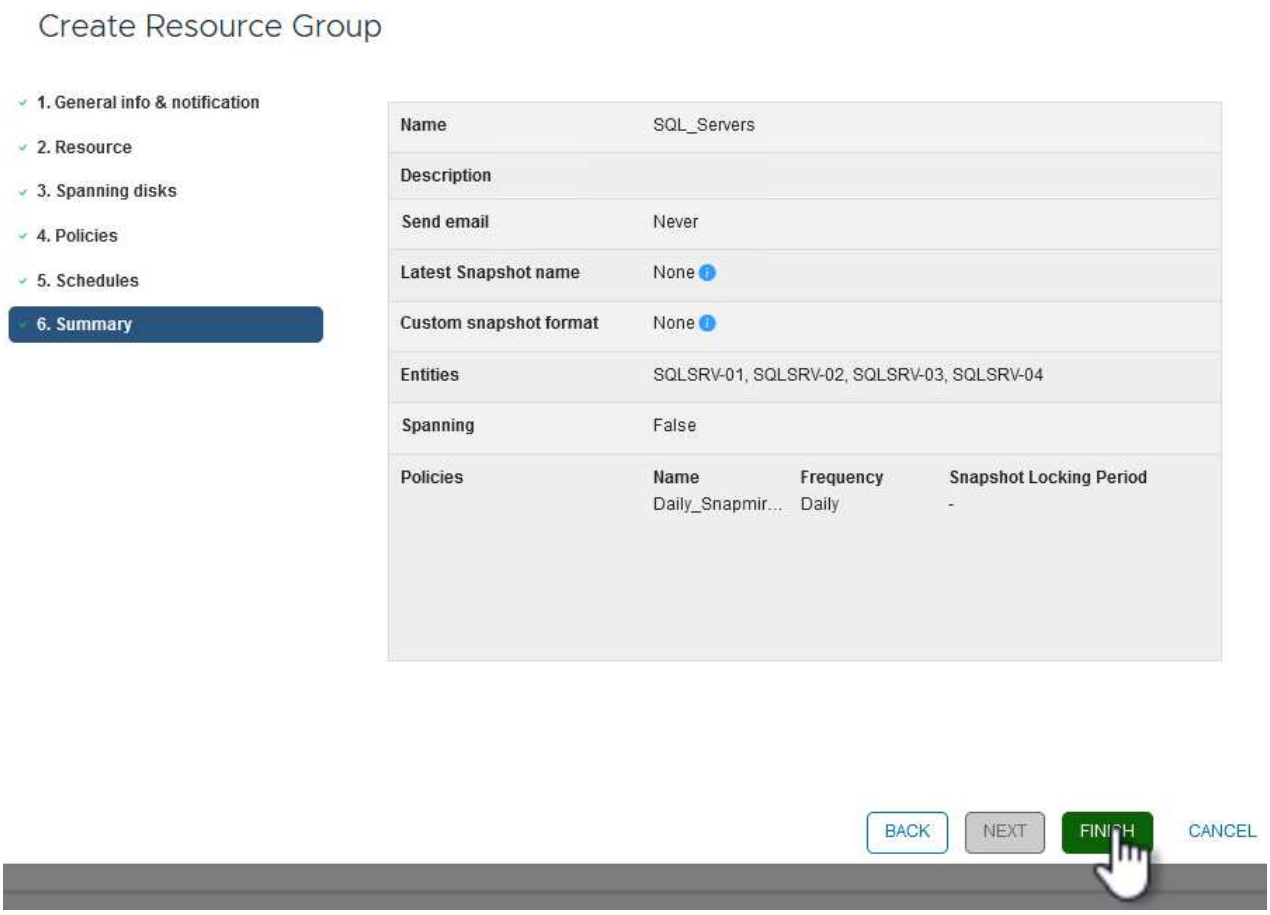
5. 정책 페이지에서 이 리소스 그룹과 함께 사용될 이전에 생성된 정책 하나 또는 여러 개의 정책을 선택합니다. 계속하려면 *다음*을 클릭하세요.



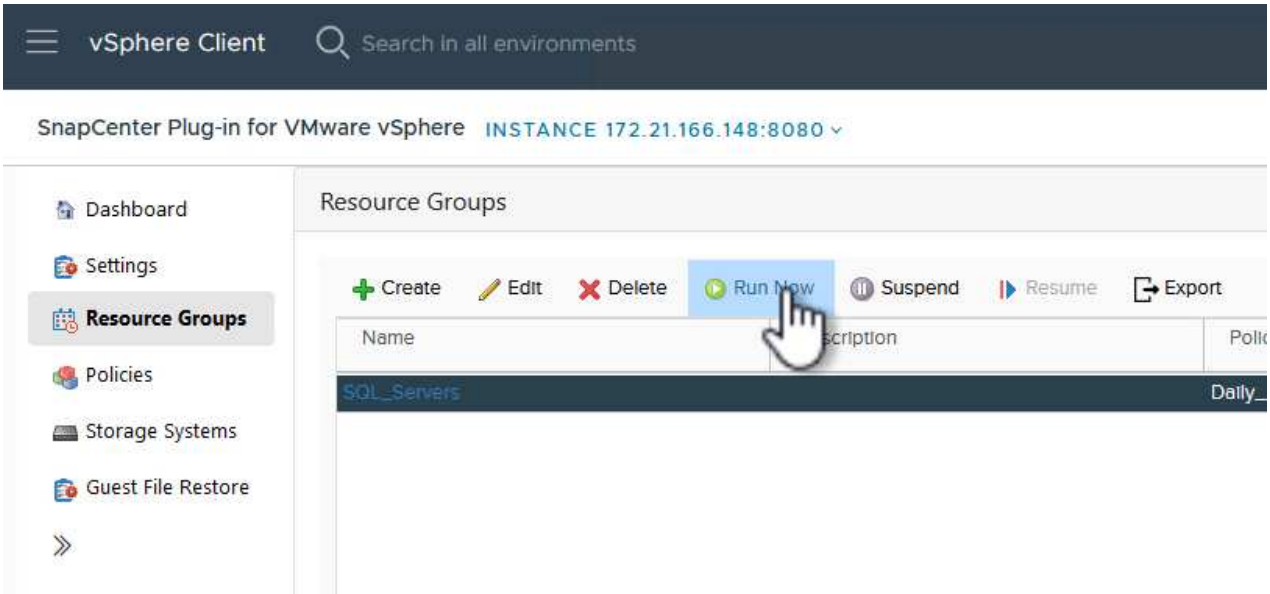
6. 일정 페이지에서 반복 및 시간을 구성하여 백업이 실행될 시기를 설정합니다. 계속하려면 *다음*을 클릭하세요.



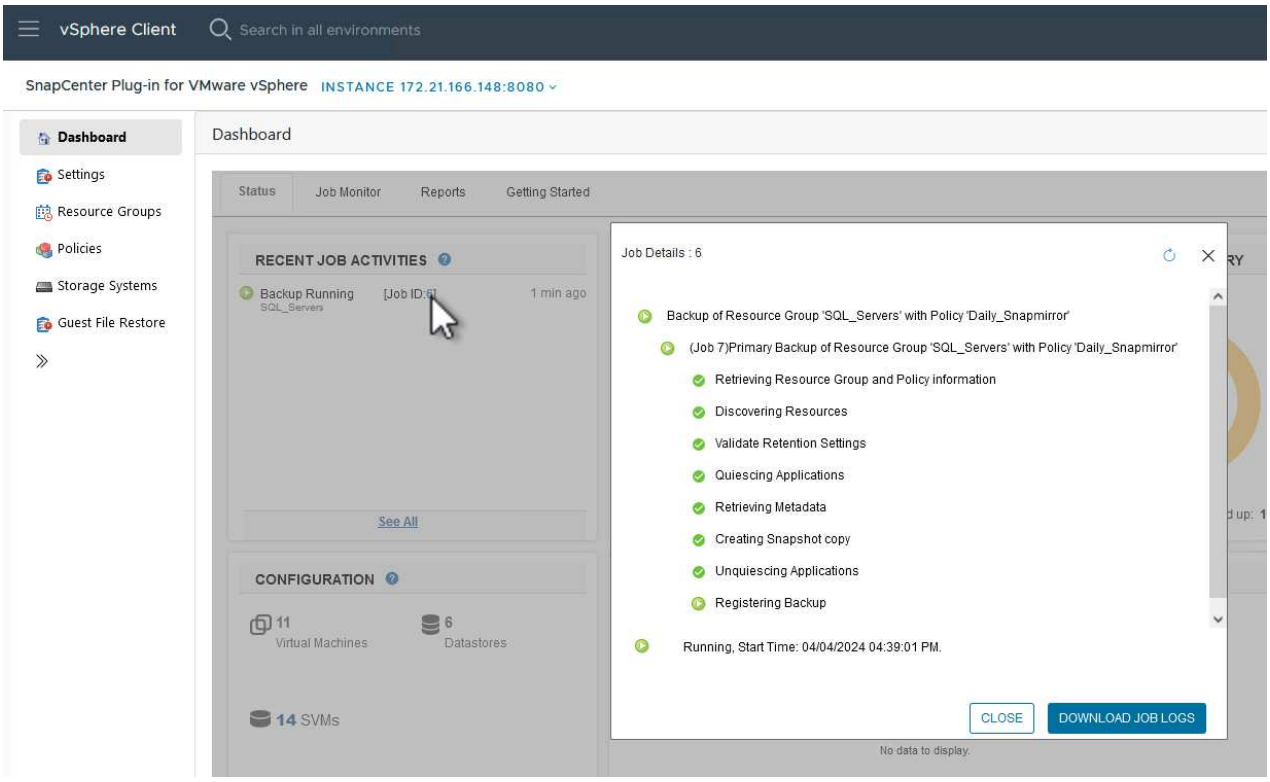
7. 마지막으로 *요약*을 검토하고 *마침*을 클릭하여 리소스 그룹을 만듭니다.



8. 리소스 그룹이 생성되면 지금 실행 버튼을 클릭하여 첫 번째 백업을 실행합니다.



9. 대시보드*로 이동한 후 *최근 작업 활동*에서 *작업 **ID** 옆에 있는 숫자를 클릭하여 작업 모니터를 열고 실행 중인 작업의 진행 상황을 확인하세요.



SCV를 사용하여 **VM, VMDK** 및 파일을 복원합니다**.**

SnapCenter 플러그인을 사용하면 기본 또는 보조 백업에서 VM, VMDK, 파일 및 폴더를 복원할 수 있습니다.

VM은 원래 호스트로 복원하거나, 동일한 vCenter Server에 있는 대체 호스트로 복원하거나, 동일한 vCenter나 연결 모드의 모든 vCenter에서 관리하는 대체 ESXi 호스트로 복원할 수 있습니다.

vVol VM은 원래 호스트로 복원될 수 있습니다.

기존 VM의 VMDK는 원본 또는 대체 데이터 저장소로 복원할 수 있습니다.

vVol VM의 VMDK는 원래 데이터 저장소로 복원될 수 있습니다.

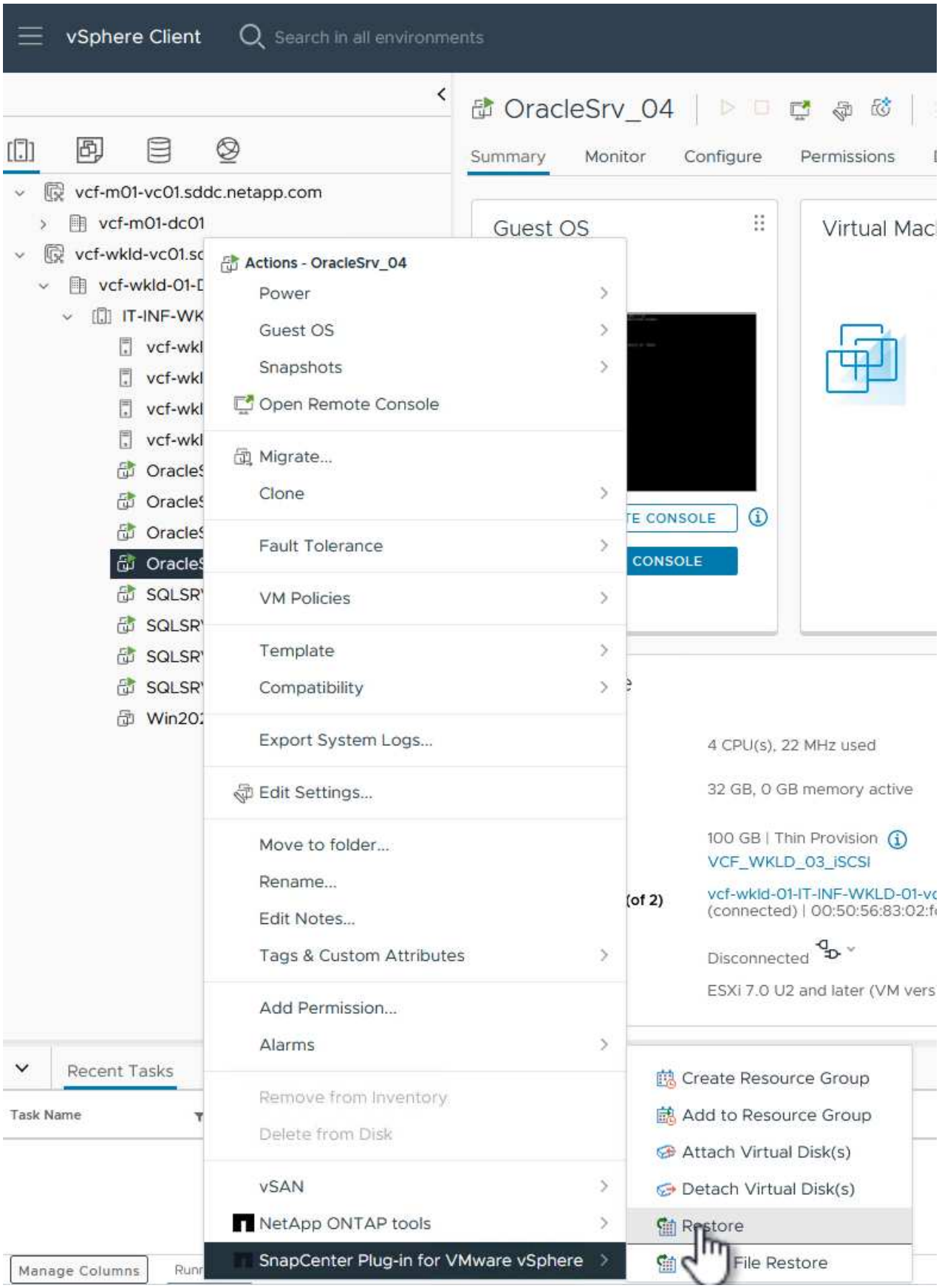
게스트 파일 복원 세션에서 개별 파일과 폴더를 복원할 수 있으며, 이때 가상 디스크의 백업 사본을 첨부한 다음 선택한 파일이나 폴더를 복원합니다.

VM, VMDK 또는 개별 폴더를 복원하려면 다음 단계를 완료하세요.

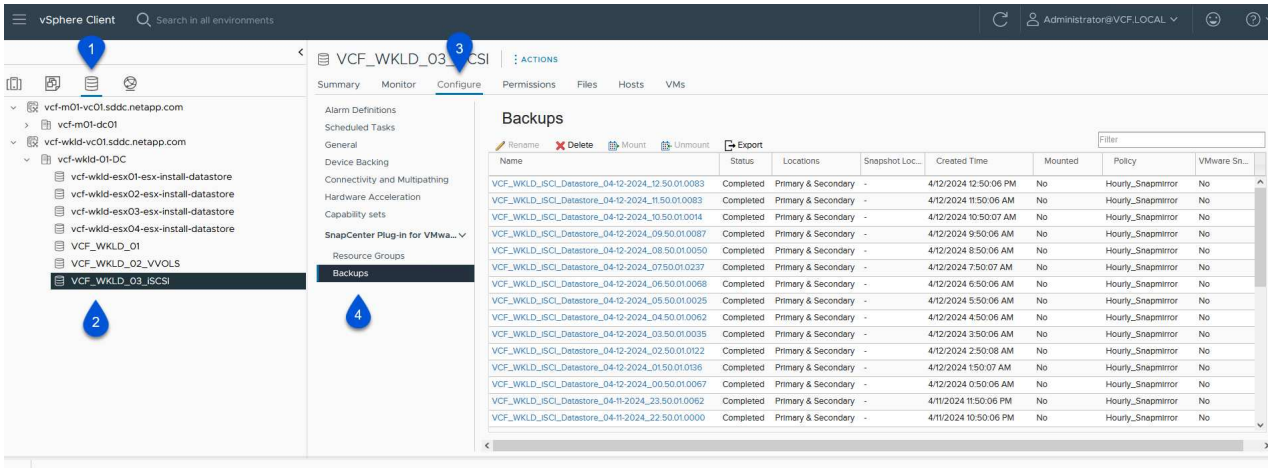
SnapCenter 플러그인을 사용하여 **VM** 복원

SCV로 VM을 복원하려면 다음 단계를 완료하세요.

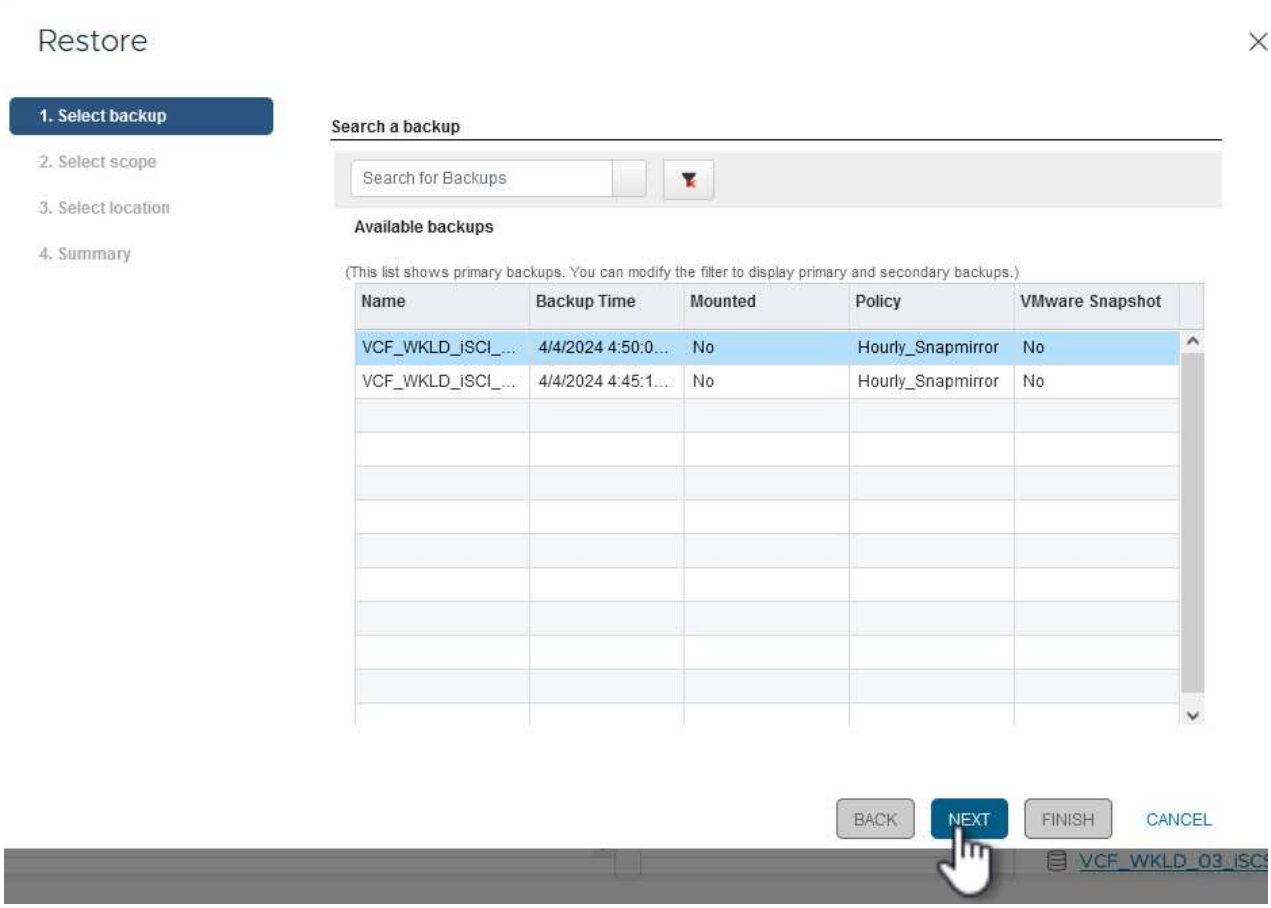
1. vSphere 클라이언트에서 복원할 VM으로 이동한 후 마우스 오른쪽 버튼을 클릭하고 * SnapCenter Plug-in for VMware vSphere*으로 이동합니다. 하위 메뉴에서 *복원*을 선택합니다.


vSphere Client
Search in all environments
OracleSrv_04
Summary
Monitor
Configure
Permissions
vcf-m01-vc01.sddc.netapp.com
vcf-m01-dc01
vcf-wkld-vc01.sc
vcf-wkld-01-D
IT-INF-WK
Guest OS
Virtual Mac
Actions - OracleSrv_04
Power
Guest OS
Snapshots
Open Remote Console
Migrate...
Clone
Fault Tolerance
VM Policies
Template
Compatibility
Export System Logs...
Edit Settings...
Move to folder...
Rename...
Edit Notes...
Tags & Custom Attributes
Add Permission...
Alarms
Remove from Inventory
Delete from Disk
vSAN
NetApp ONTAP tools
SnapCenter Plug-in for VMware vSphere
CONSOLE
4 CPU(s), 22 MHz used
32 GB, 0 GB memory active
100 GB | Thin Provision
VCF_WKLD_03_iSCSI
Disconnected
ESXi 7.0 U2 and later (VM vers
Recent Tasks
Task Name
Manage Columns
Create Resource Group
Add to Resource Group
Attach Virtual Disk(s)
Detach Virtual Disk(s)
Restore
File Restore

또 다른 방법은 인벤토리의 데이터 저장소로 이동한 다음 구성 탭에서 * SnapCenter Plug-in for VMware vSphere > 백업*으로 이동하는 것입니다. 선택한 백업에서 복원할 VM을 선택합니다.

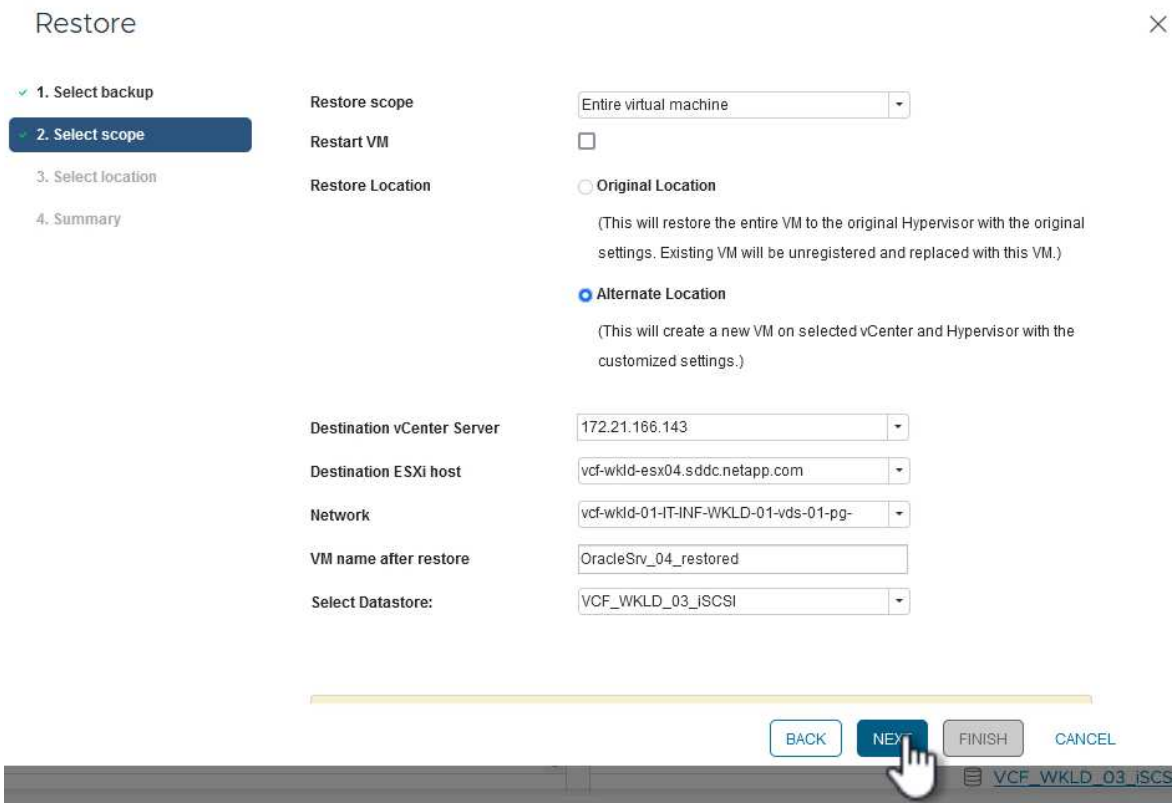


2. 복원 마법사에서 사용할 백업을 선택합니다. 계속하려면 *다음*을 클릭하세요.



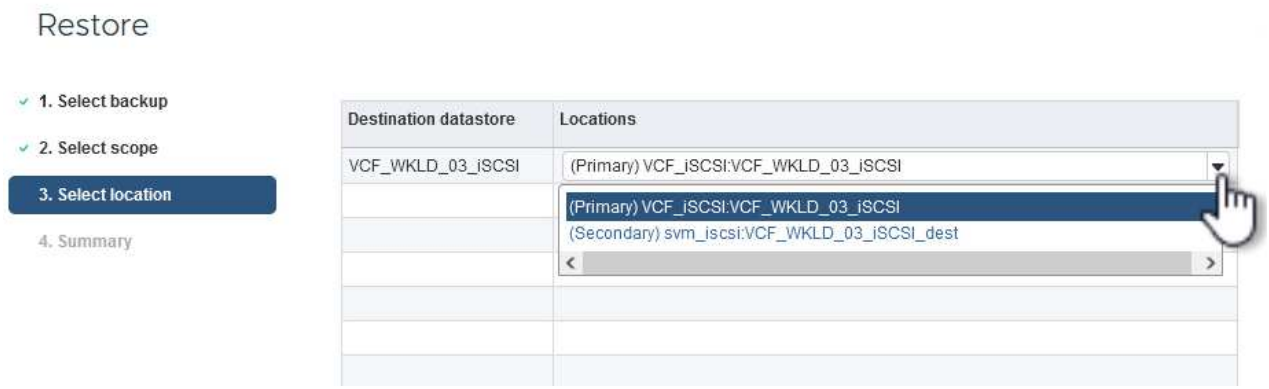
3. 범위 선택 페이지에서 필수 필드를 모두 작성하세요.

- 복원 범위 - 전체 가상 머신을 복원하도록 선택합니다.
- **VM** 다시 시작 - 복원 후 VM을 시작할지 여부를 선택합니다.
- 위치 복원 - 원래 위치나 다른 위치로 복원할지 선택하세요. 대체 위치를 선택할 때 각 필드에서 옵션을 선택하세요.
  - 대상 **vCenter** 서버 - 연결 모드의 로컬 vCenter 또는 대체 vCenter
  - 대상 **ESXi** 호스트
  - 회로망
  - 복원 후 **VM** 이름
  - 데이터 저장소 선택**:**

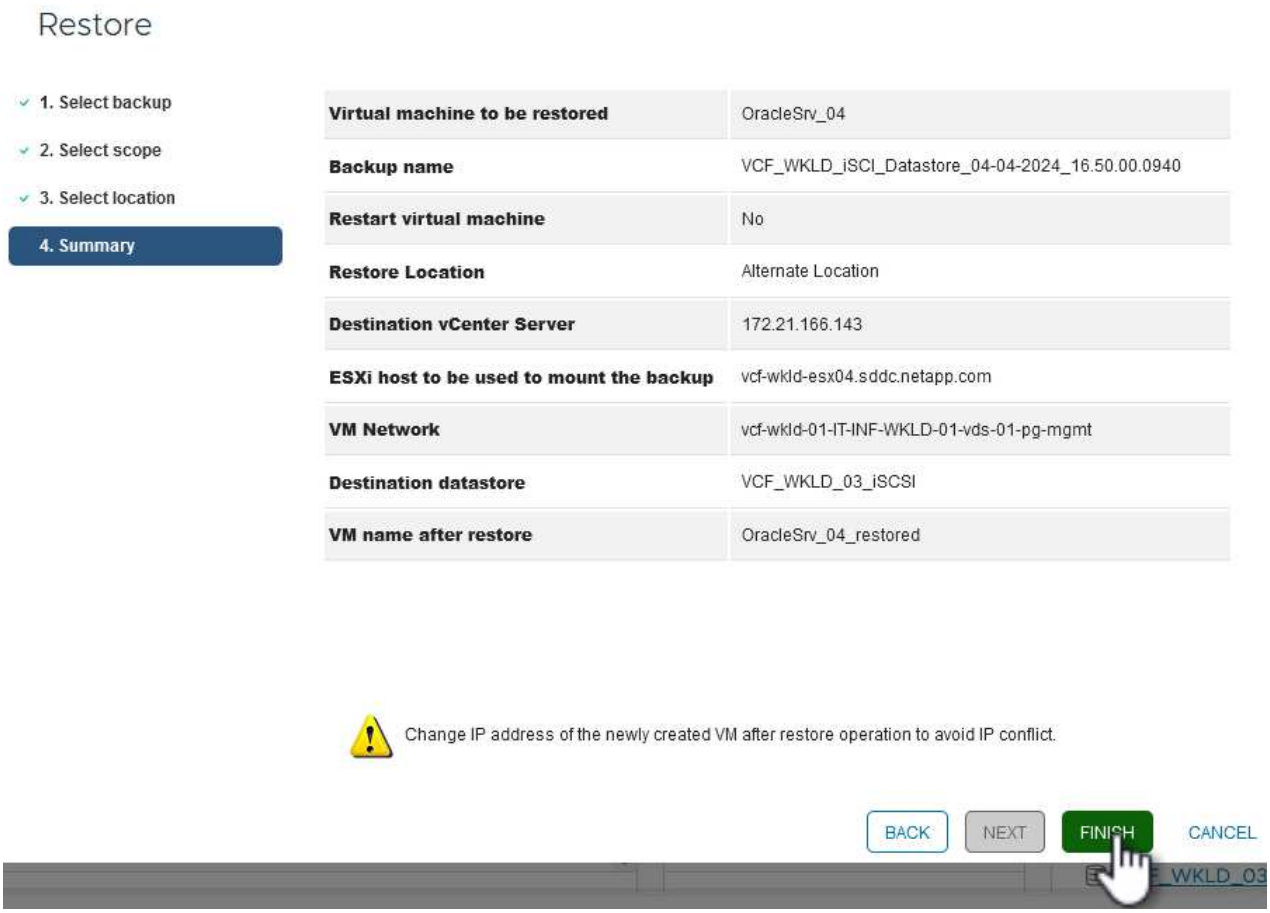


계속하려면 *다음*을 클릭하세요.

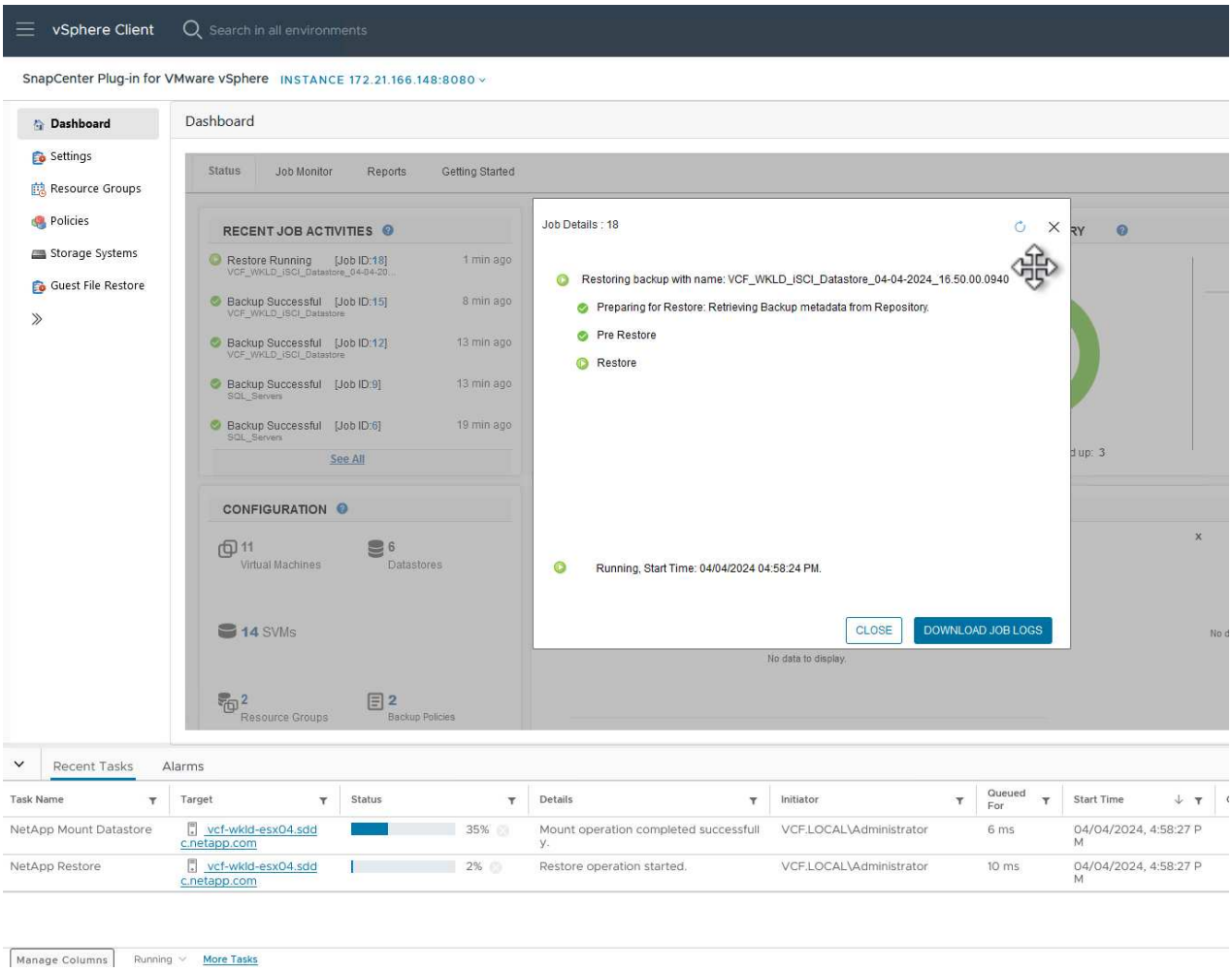
4. 위치 선택 페이지에서 기본 또는 보조 ONTAP 스토리지 시스템에서 VM을 복원하도록 선택합니다. 계속하려면 *다음*을 클릭하세요.



5. 마지막으로 *요약*을 검토하고 *마침*을 클릭하여 복원 작업을 시작합니다.



6. 복원 작업 진행 상황은 vSphere Client의 최근 작업 창과 SCV의 작업 모니터에서 모니터링할 수 있습니다.

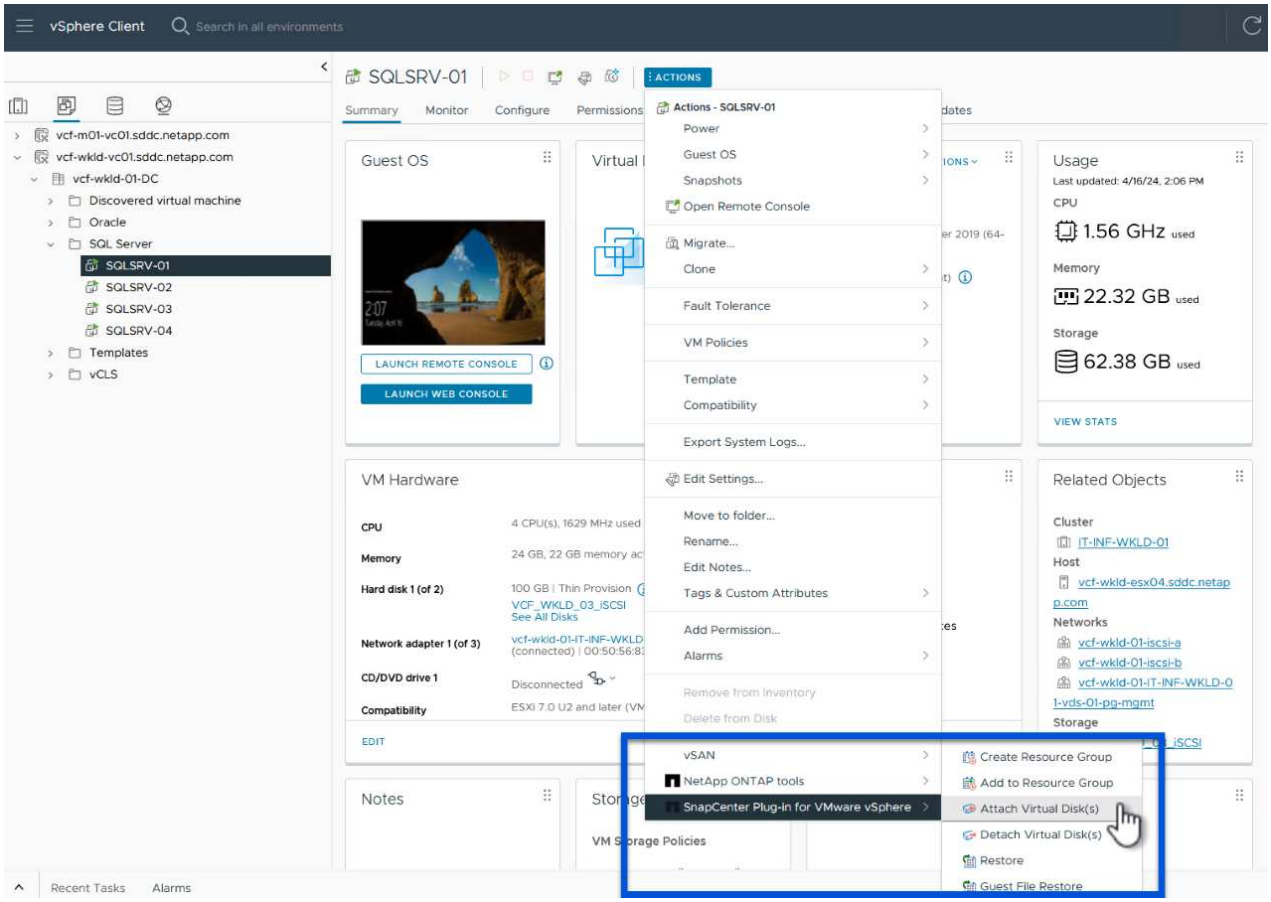

vSphere Client
Search in all environments
SnapCenter Plug-in for VMware vSphere
INSTANCE 172.21.166.148:8080
Dashboard
Settings
Resource Groups
Policies
Storage Systems
Guest File Restore
Dashboard
Status
Job Monitor
Reports
Getting Started
RECENT JOB ACTIVITIES
Restore Running [Job ID:18] 1 min ago
Backup Successful [Job ID:15] 8 min ago
Backup Successful [Job ID:12] 13 min ago
Backup Successful [Job ID:9] 13 min ago
Backup Successful [Job ID:6] 19 min ago
See All
CONFIGURATION
11 Virtual Machines
6 Datastores
14 SVMs
2 Resource Groups
2 Backup Policies
Job Details : 18
Restoring backup with name: VCF_WKLD_iSCI_Datastore_04-04-2024_16.50.00.0940
Preparing for Restore: Retrieving Backup metadata from Repository.
Pre Restore
Restore
Running, Start Time: 04/04/2024 04:58:24 PM.
CLOSE
DOWNLOAD JOB LOGS
No data to display.
Recent Tasks
Alarms
Task Name
Target
Status
Details
Initiator
Queued For
Start Time
NetApp Mount Datastore
vcf-wkld-esx04.sddc.netapp.com
35%
Mount operation completed successfully.
VCF.LOCAL\Administrator
6 ms
04/04/2024, 4:58:27 PM
NetApp Restore
vcf-wkld-esx04.sddc.netapp.com
2%
Restore operation started.
VCF.LOCAL\Administrator
10 ms
04/04/2024, 4:58:27 PM
Manage Columns
Running
More Tasks

SnapCenter 플러그인을 사용하여 **VMDK** 복원

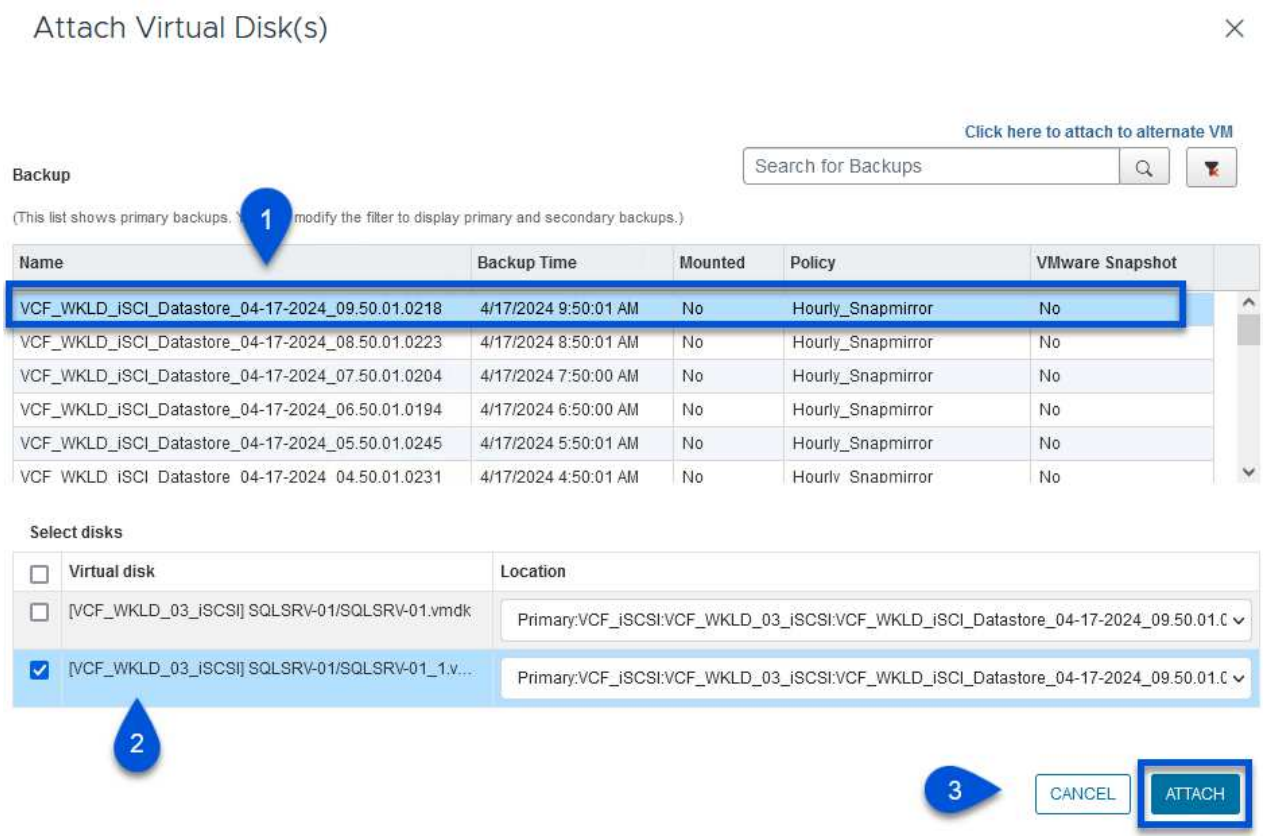
ONTAP 도구를 사용하면 VMDK를 원래 위치로 완전히 복원하거나 VMDK를 호스트 시스템에 새 디스크로 연결할 수 있습니다. 이 시나리오에서는 VMDK가 파일 시스템에 액세스하기 위해 Windows 호스트에 연결됩니다.

백업에서 VMDK를 연결하려면 다음 단계를 완료하세요.

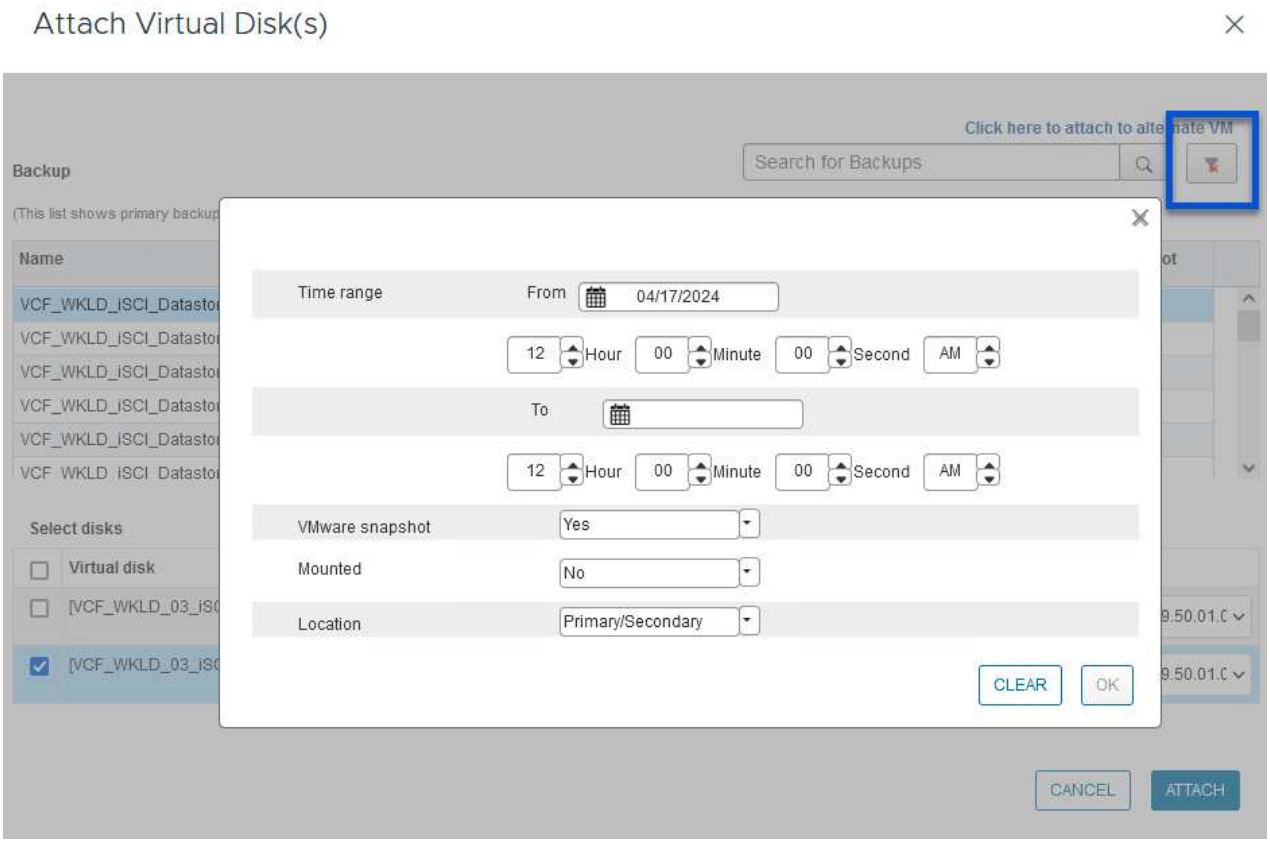
1. vSphere Client에서 VM으로 이동한 후, 작업 메뉴에서 * SnapCenter Plug-in for VMware vSphere > 가상 디스크 연결*을 선택합니다.



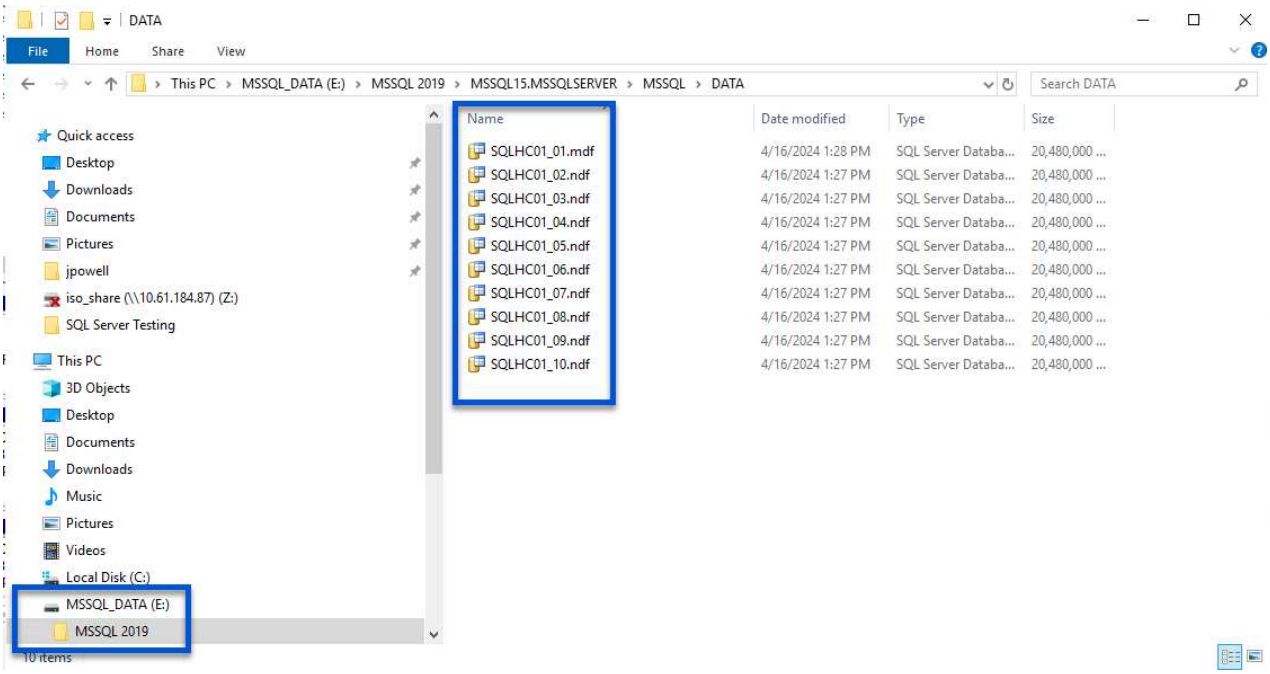
2. 가상 디스크 연결 마법사에서 사용할 백업 인스턴스와 연결할 특정 VMDK를 선택합니다.



필터 옵션을 사용하면 백업을 찾고 기본 및 보조 저장 시스템의 백업을 표시할 수 있습니다.



3. 모든 옵션을 선택한 후 첨부 버튼을 클릭하여 복구 프로세스를 시작하고 VMDK를 호스트에 연결했습니다.
4. 연결 절차가 완료되면 호스트 시스템의 OS에서 디스크에 액세스할 수 있습니다. 이 경우 SCV는 NTFS 파일 시스템이 있는 디스크를 Windows SQL Server의 E: 드라이브에 연결했고 파일 시스템의 SQL 데이터베이스 파일은 파일 탐색기를 통해 액세스할 수 있습니다.



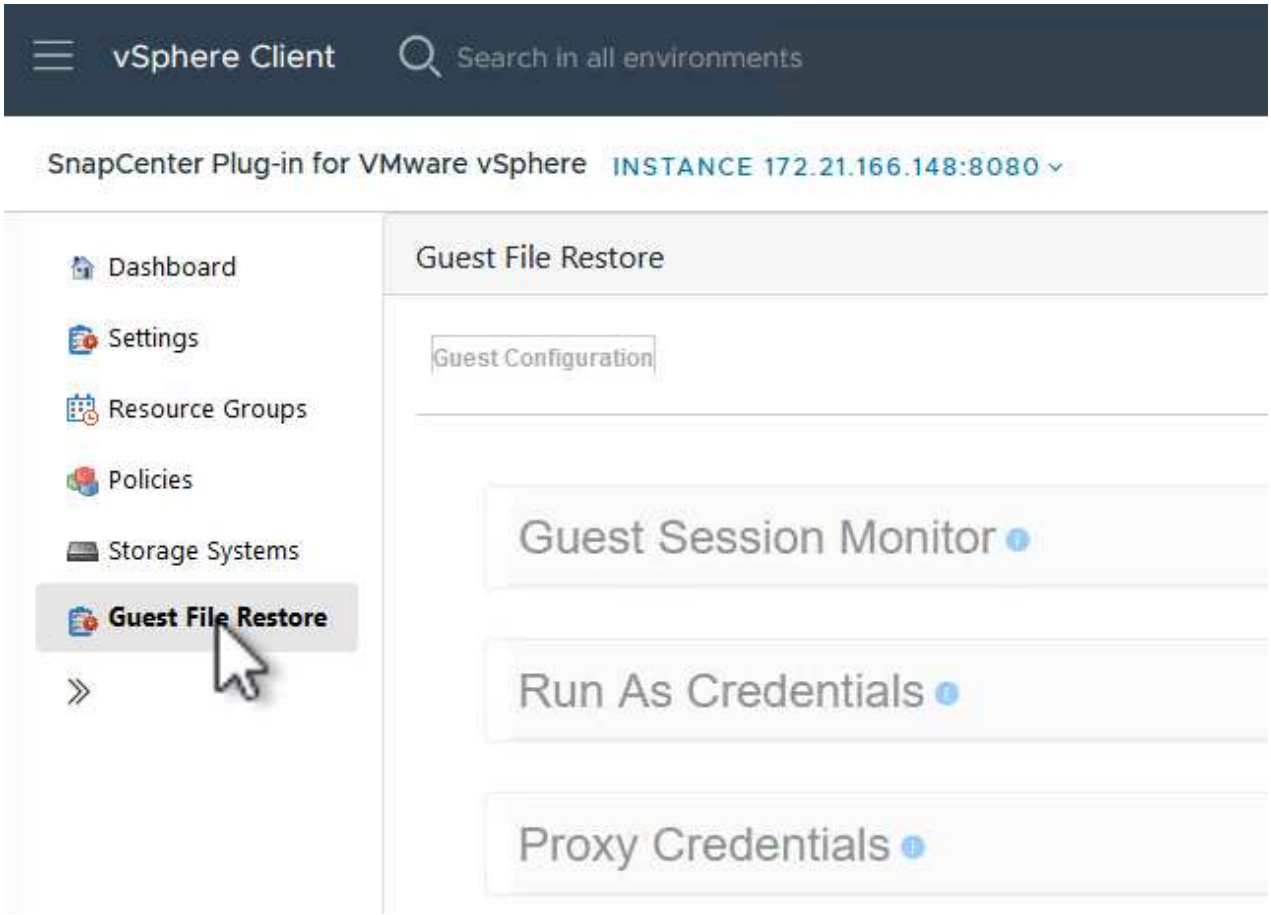
SnapCenter 플러그인을 사용한 게스트 파일 시스템 복원

ONTAP 도구는 Windows Server OS의 VMDK에서 게스트 파일 시스템을 복원하는 기능을 제공합니다. 이 작업은 SnapCenter 플러그인 인터페이스를 통해 중앙에서 수행됩니다.

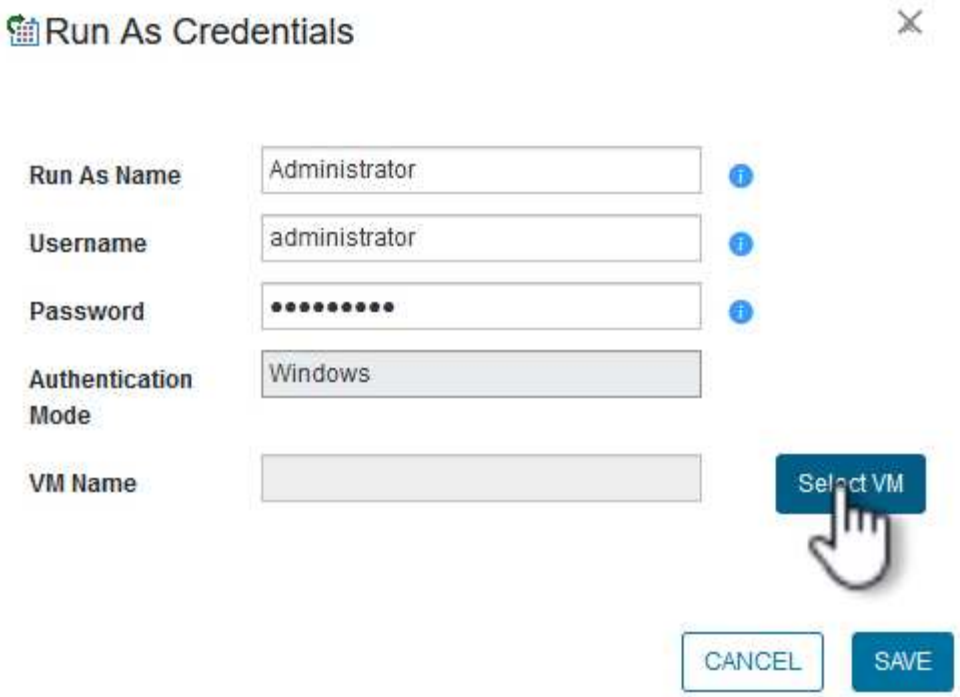
자세한 내용은 다음을 참조하세요."게스트 파일 및 폴더 복원" SCV 문서 사이트에서.

Windows 시스템에 대한 게스트 파일 시스템 복원을 수행하려면 다음 단계를 완료하세요.

1. 첫 번째 단계는 Windows 호스트 시스템에 대한 액세스를 제공하기 위해 실행 자격 증명을 만드는 것입니다. vSphere Client에서 CSV 플러그인 인터페이스로 이동한 다음 기본 메뉴에서 *게스트 파일 복원*을 클릭합니다.

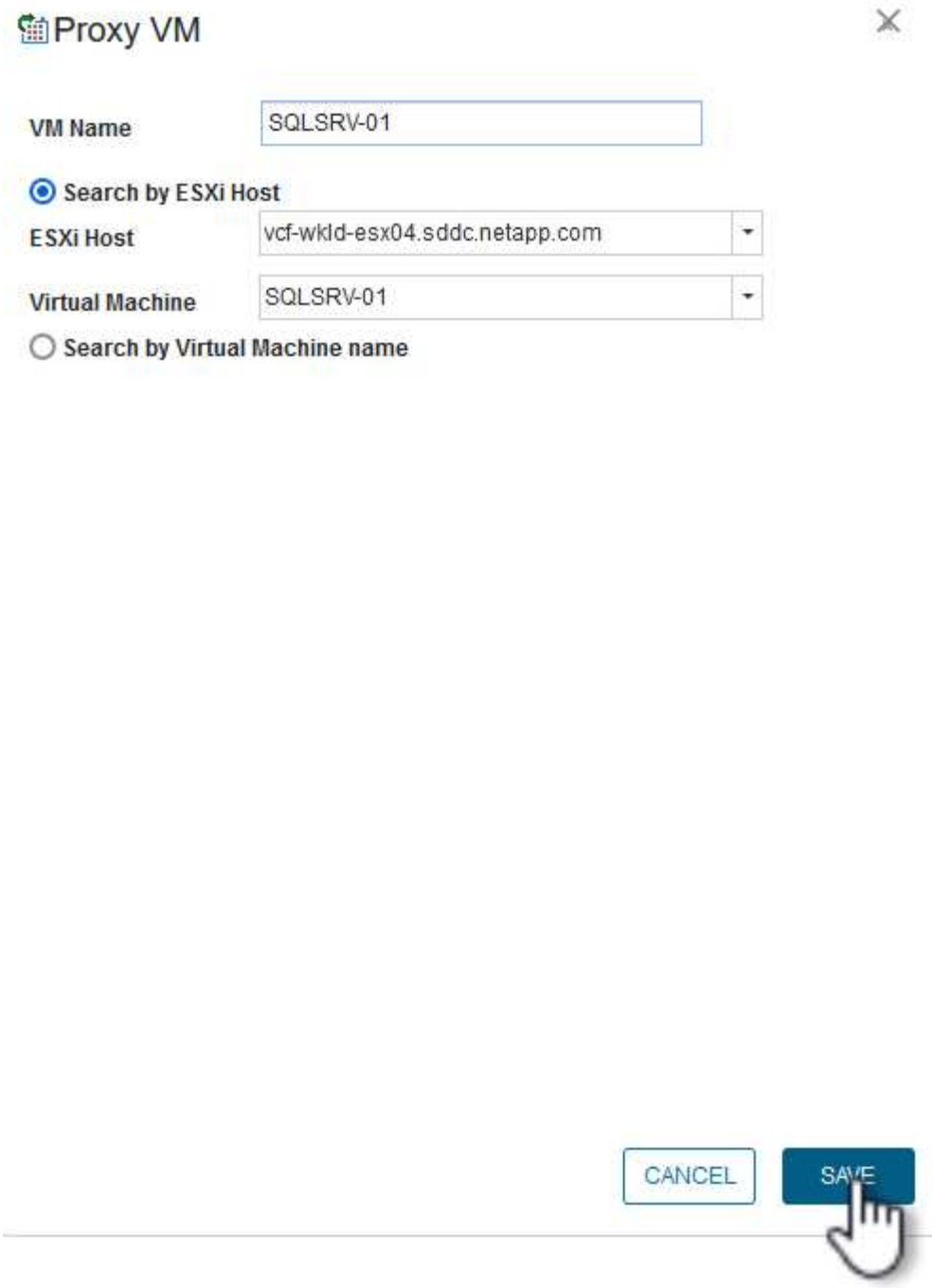


2. 자격 증명으로 실행*에서 ***+** 아이콘을 클릭하여 자격 증명으로 실행 창을 엽니다.
3. 자격 증명 레코드의 이름을 입력하고 Windows 시스템의 관리자 사용자 이름과 비밀번호를 입력한 다음 **VM** 선택 버튼을 클릭하여 복원에 사용할 선택적 프록시 VM을 선택합니다

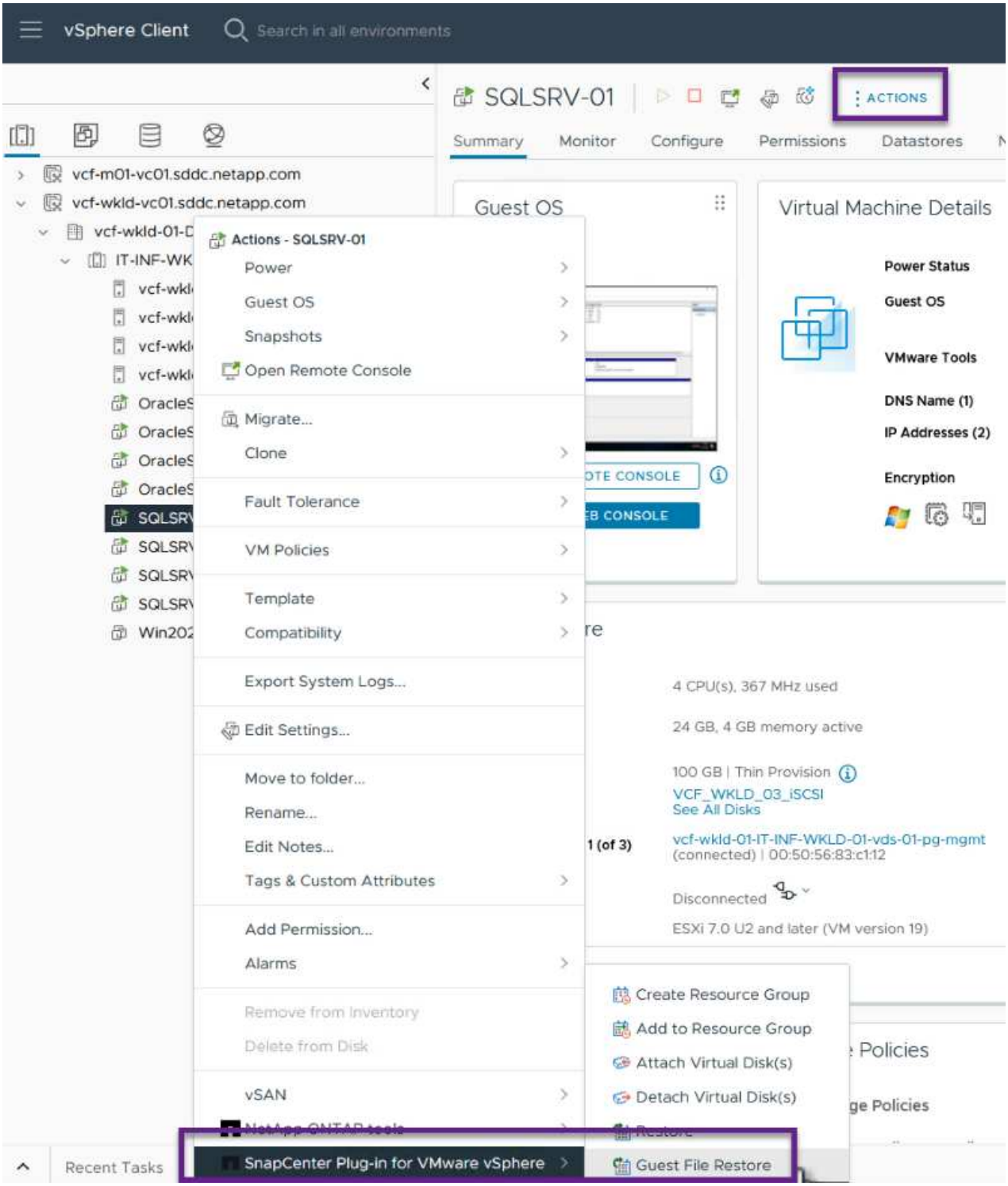


.

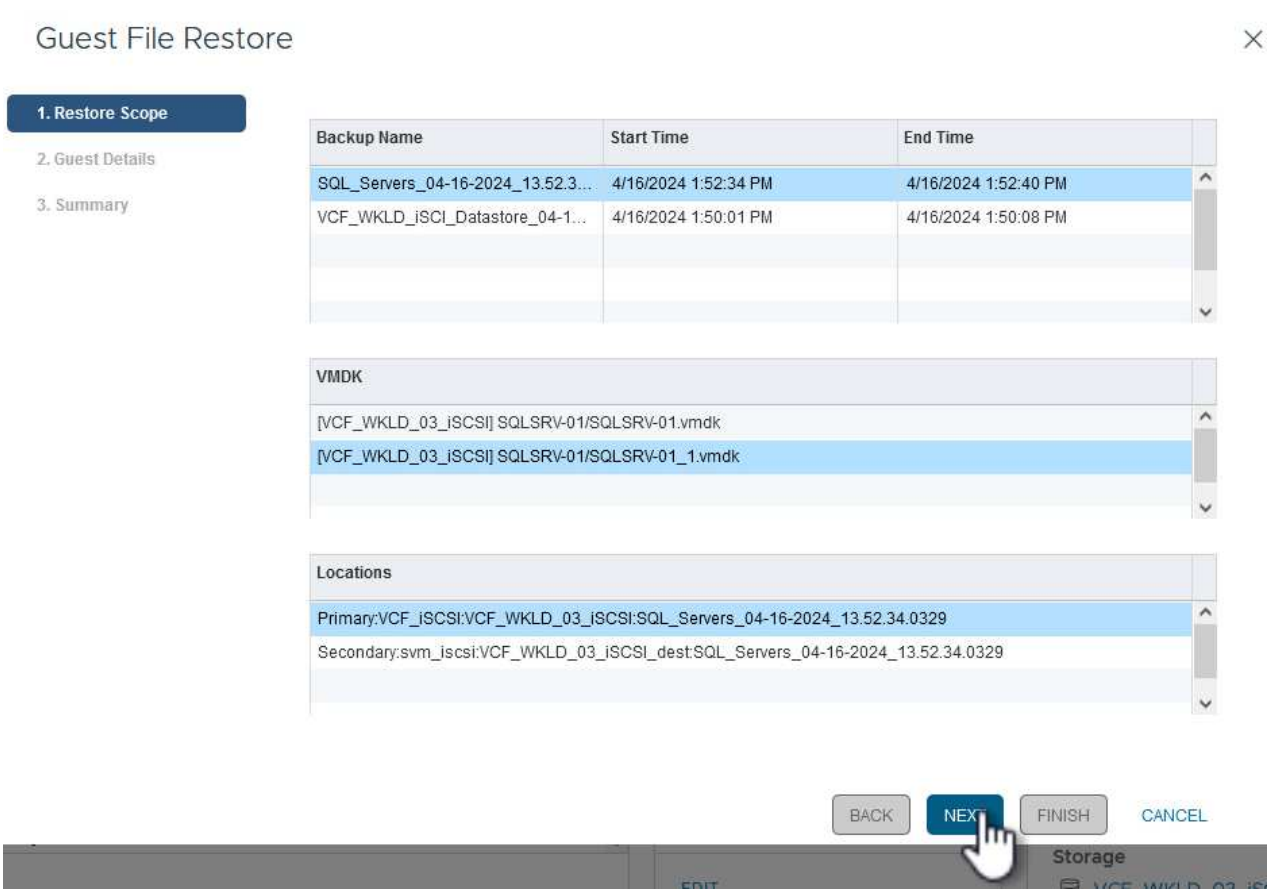
4. 프록시 VM 페이지에서 VM의 이름을 입력하고 ESXi 호스트나 이름으로 검색하여 VM을 찾습니다. 선택한 후 *저장*을 클릭하세요.



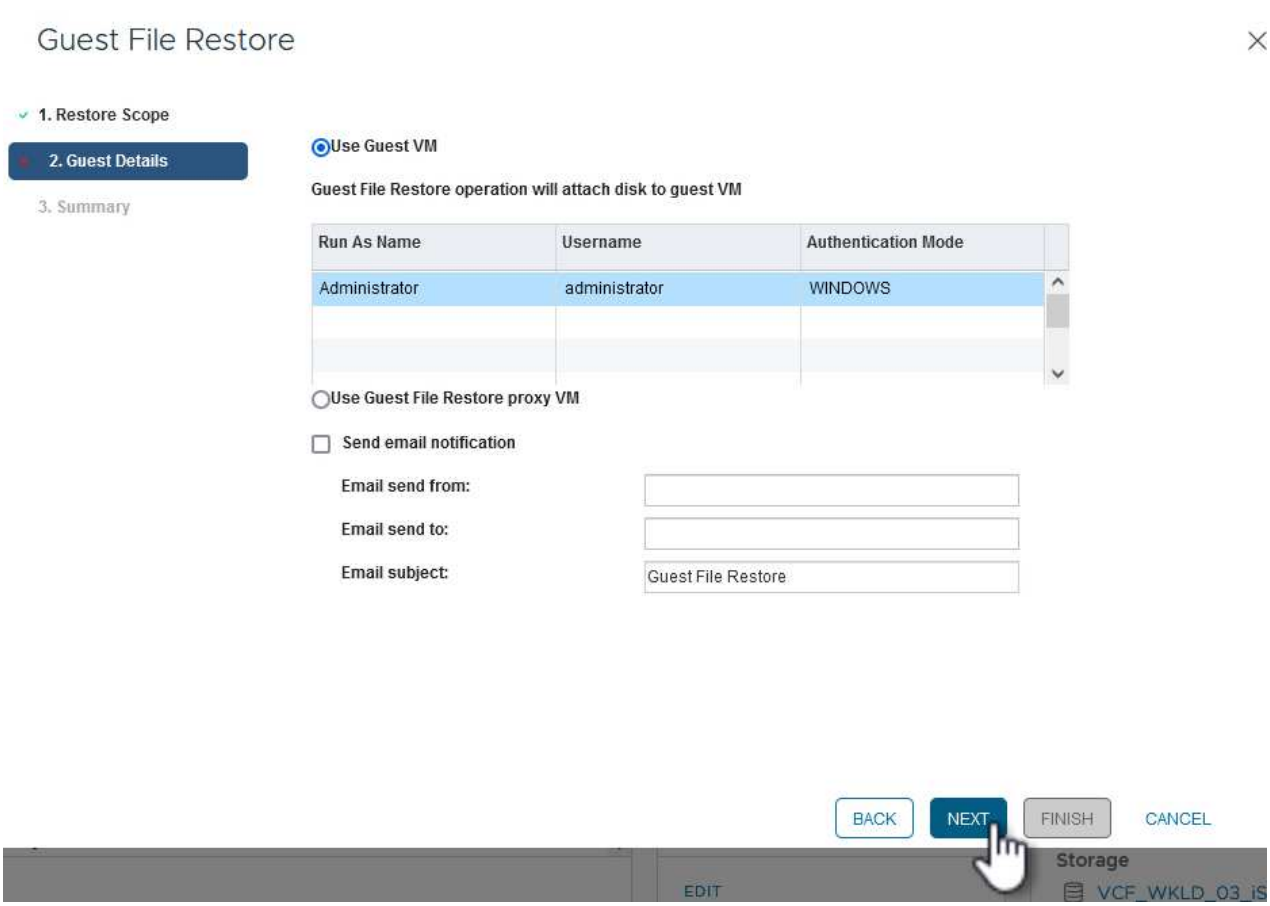
5. 자격 증명으로 실행 창에서 *저장*을 다시 클릭하여 레코드 저장을 완료합니다.
6. 다음으로, 인벤토리의 VM으로 이동합니다. 작업 메뉴에서 또는 VM을 마우스 오른쪽 버튼으로 클릭하고 * SnapCenter Plug-in for VMware vSphere > 게스트 파일 복원*을 선택합니다.



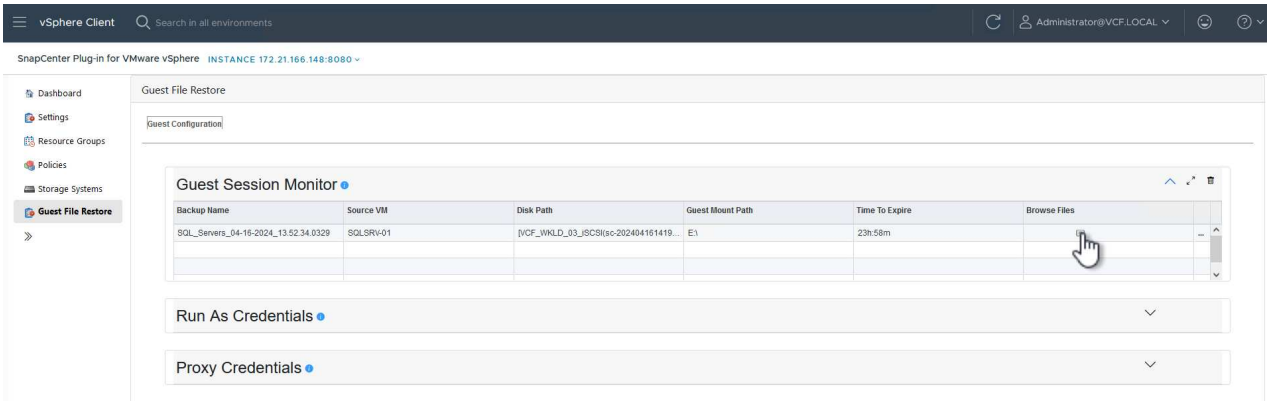
7. 게스트 파일 복원 마법사의 복원 범위 페이지에서 복원할 백업, 특정 VMDK, VMDK를 복원할 위치(기본 또는 보조)를 선택합니다. 계속하려면 *다음*을 클릭하세요.



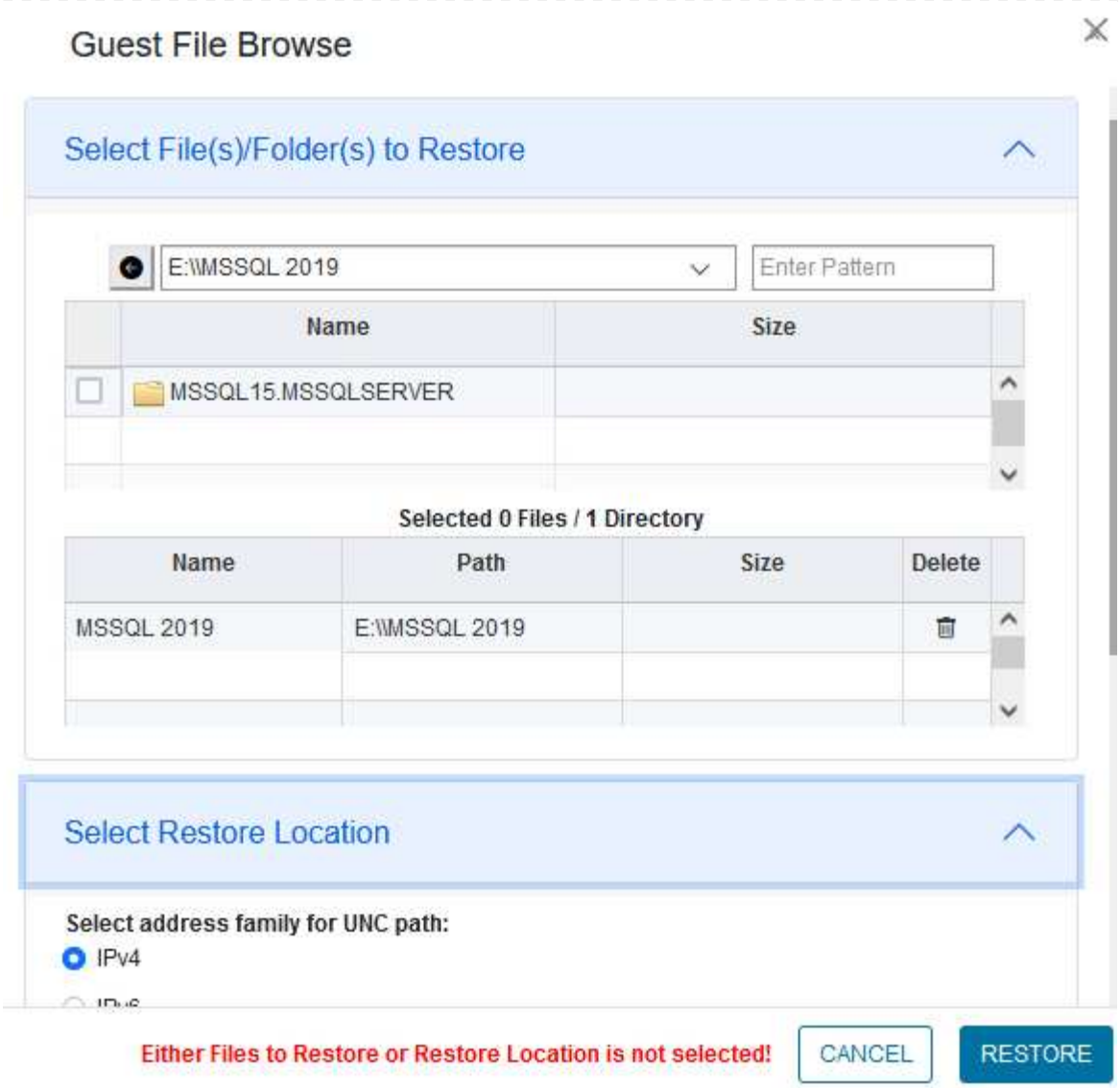
8. 게스트 세부 정보 페이지에서 복원에 게스트 **VM** 또는 *게스트 파일 복원 프록시 VM 사용*을 선택합니다. 또한, 원하시면 여기에 이메일 알림 설정을 입력하세요. 계속하려면 *다음*을 클릭하세요.

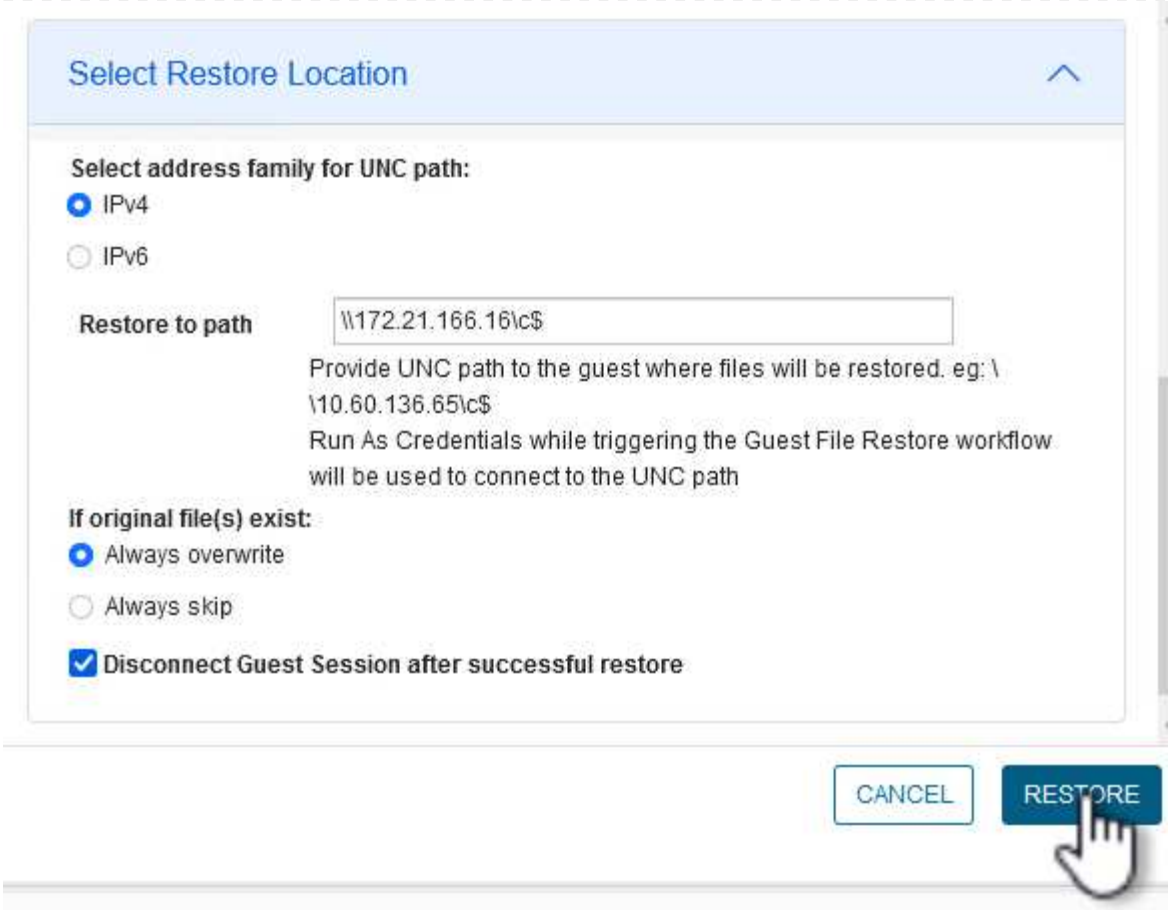


9. 마지막으로 요약 페이지를 검토하고 *마침*을 클릭하여 게스트 파일 시스템 복원 세션을 시작합니다.
10. SnapCenter 플러그인 인터페이스로 돌아와서 다시 게스트 파일 복원*으로 이동하여 *게스트 세션 모니터*에서 실행 중인 세션을 확인합니다. 계속하려면 *파일 찾아보기 아래의 아이콘을 클릭하세요.



11. 게스트 파일 찾아보기 마법사에서 복원할 폴더나 파일을 선택하고 복원할 파일 시스템 위치를 선택합니다. 마지막으로, 복원*을 클릭하여 *복원 프로세스를 시작합니다.


Guest File Browse
Select File(s)/Folder(s) to Restore
E:\MSSQL 2019
Enter Pattern
Name
Size
MSSQL15.MSSQLSERVER
Selected 0 Files / 1 Directory
Name
Path
Size
Delete
MSSQL 2019
E:\MSSQL 2019
Select Restore Location
Select address family for UNC path:
IPv4
Either Files to Restore or Restore Location is not selected!
CANCEL
RESTORE



12. 복원 작업은 vSphere Client 작업 창에서 모니터링할 수 있습니다.

추가 정보

VCF 구성에 대한 정보는 다음을 참조하세요. "VMware Cloud Foundation 문서" .

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요. "ONTAP 9 문서" 센터.

SnapCenter Plug-in for VMware vSphere 사용에 대한 정보는 다음을 참조하세요. "SnapCenter Plug-in for VMware vSphere 설명서" .

VMware vSphere용 SnapCenter 플러그인을 사용하여 VCF 관리 및 워크로드 도메인 보호

SnapCenter Plug-in for VMware vSphere 사용하여 여러 VCF 도메인을 보호하세요. 이 절차에는 각 도메인에 대한 플러그인 설정, 백업 정책 구성 및 복원 작업 수행이 포함됩니다.

VMware Cloud Foundation(VCF) 워크로드 도메인을 사용하면 조직에서 리소스를 여러 도메인으로 논리적으로 분리하여 다양한 워크로드를 그룹화하고 보안과 내결함성을 강화할 수 있습니다.

소개

도메인은 독립적으로 확장 가능하고, 특정 규정을 충족하며 다중 테넌시를 제공할 수 있습니다. VMware Cloud

Foundation(VCF)의 데이터 보호는 관리 도메인과 워크로드 도메인 전반에서 데이터의 가용성, 무결성 및 복구 가능성을 보장하는 데 중요한 측면입니다. VMware vSphere(SCV)용 NetApp SnapCenter Plug-in for VMware vSphere NetApp의 데이터 보호 기능을 VMware 환경에 통합하는 강력한 도구입니다. NetApp 스토리지에 호스팅된 VMware vSphere 가상 머신(VM)의 백업, 복원 및 복제를 간소화합니다.

이 문서에서는 SCV를 사용하여 VCF 다중 도메인을 보호하는 방법에 대한 배포 단계를 제공합니다.

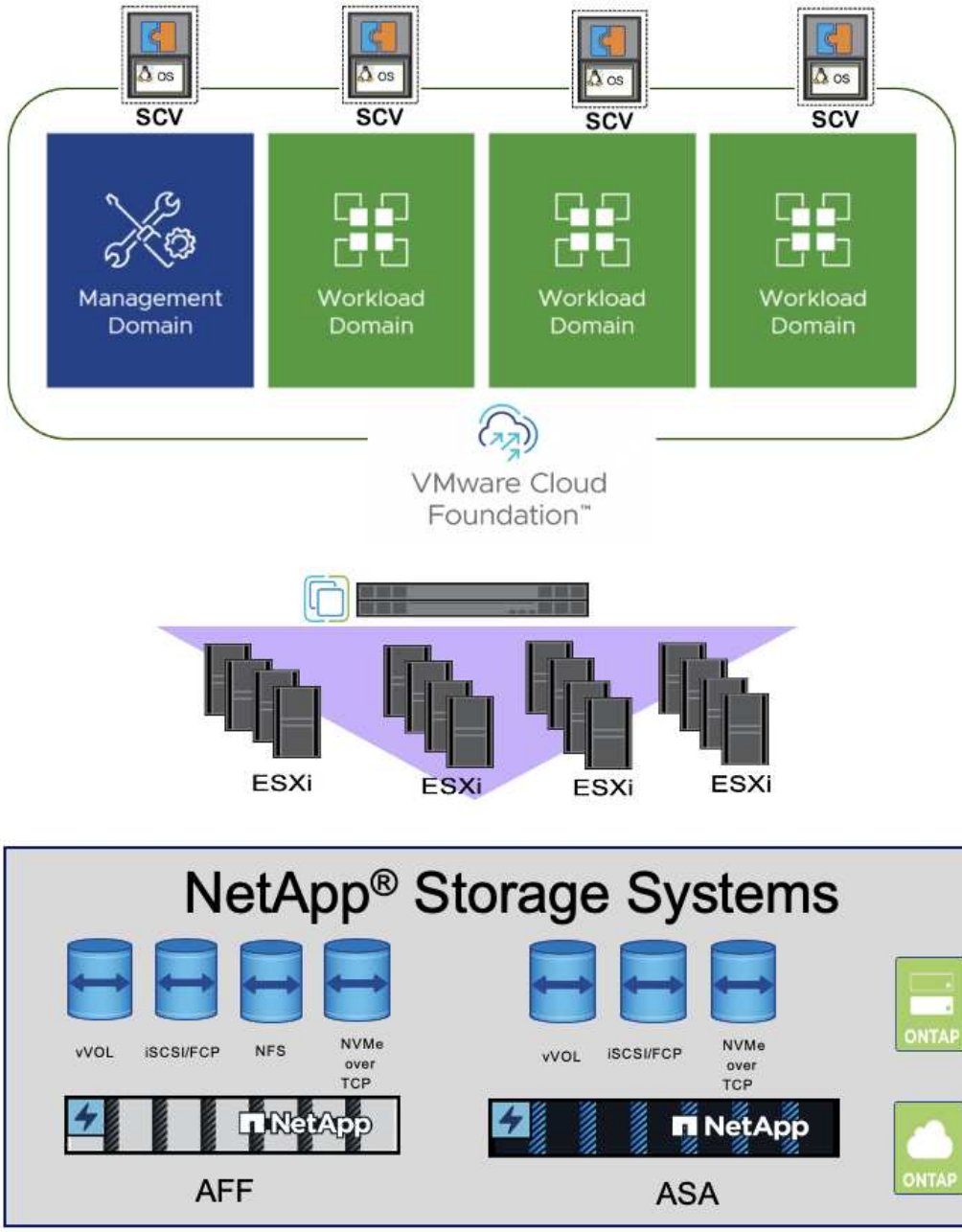
대상

VMware VCF 워크로드 도메인에 대한 데이터 보호 및 재해 복구를 보장하는 솔루션 아키텍트 또는 스토리지 관리자입니다.

아키텍처 개요

SCV는 OVA 파일을 사용하는 Linux 가상 어플라이언스로 배포되어 VM, 데이터 저장소, 파일 및 폴더에 대한 빠르고 공간 효율적이며 충돌 일관성이 뛰어나고 VM 일관성이 있는 백업 및 복원 작업을 제공합니다. SCV는 원격 플러그인 아키텍처를 사용합니다. 여러 SCV가 배포되어 VCF 관리 도메인 vCenter에 호스팅되었습니다. SCV와 VCF 도메인은 일대일 관계이므로 VCF 관리 도메인과 각 워크로드 도메인에는 하나의 SCV가 필요합니다.

ONTAP FAS, AFF 또는 All SAN Array(ASA) 기본 시스템에 있는 데이터이며 ONTAP FAS, AFF 또는 ASA 보조 시스템에 복제됩니다. SCV는 또한 SnapCenter Server와 함께 작동하여 SnapCenter 애플리케이션별 플러그인에 대한 VMware 환경에서 애플리케이션 기반 백업 및 복원 작업을 지원합니다. 자세한 내용은 다음을 확인하세요 ."SnapCenter Plug-in for VMware vSphere 설명서입니다."

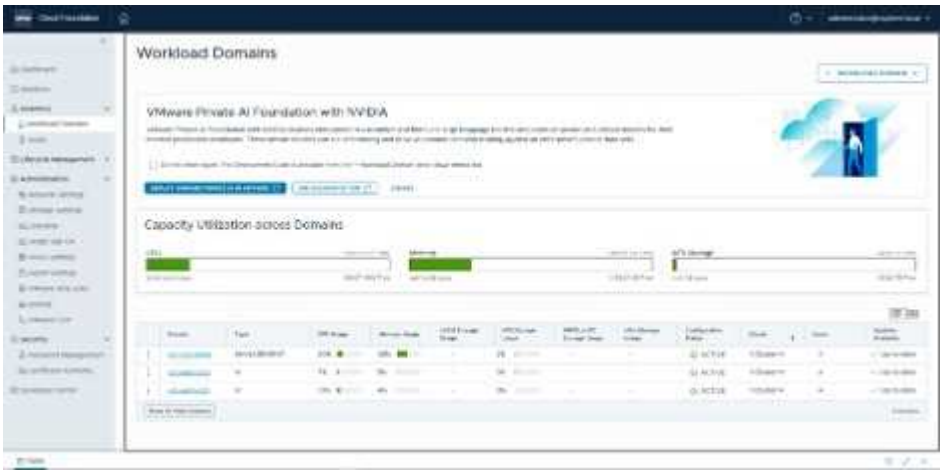


3-2-1 백업 규칙은 데이터 사본을 세 개 만들어 두 가지 유형의 미디어에 저장하고, 사본 한 개를 오프사이트에 보관하는 데이터 보호 전략입니다. BlueXP backup and recovery 온프레미스와 클라우드 환경 모두에서 광범위한 백업 및 복구 작업에 대한 단일 제어 평면을 제공하는 클라우드 기반 데이터 관리 도구입니다. NetApp BlueXP backup and recovery 제품군의 일부인 기능은 SCV(온프레미스)와 통합되어 데이터 사본을 클라우드의 개체 스토리지로 확장하는 기능입니다. 이를 통해 1차 또는 2차 저장소 백업에서 가져온 데이터의 세 번째 사본이 오프사이트에 생성됩니다. BlueXP backup and recovery 사용하면 이 두 온프레미스 위치 중 하나에서 데이터 사본을 전송하는 저장 정책을 쉽게 설정할 수 있습니다. 자세한 내용은 다음을 확인하세요."SnapCenter 플러그인과 BlueXP backup and recovery 통한 VMware용 3-2-1 데이터 보호" .

관리 도메인 및 여러 워크로드 도메인을 사용하여 **VCF** 배포

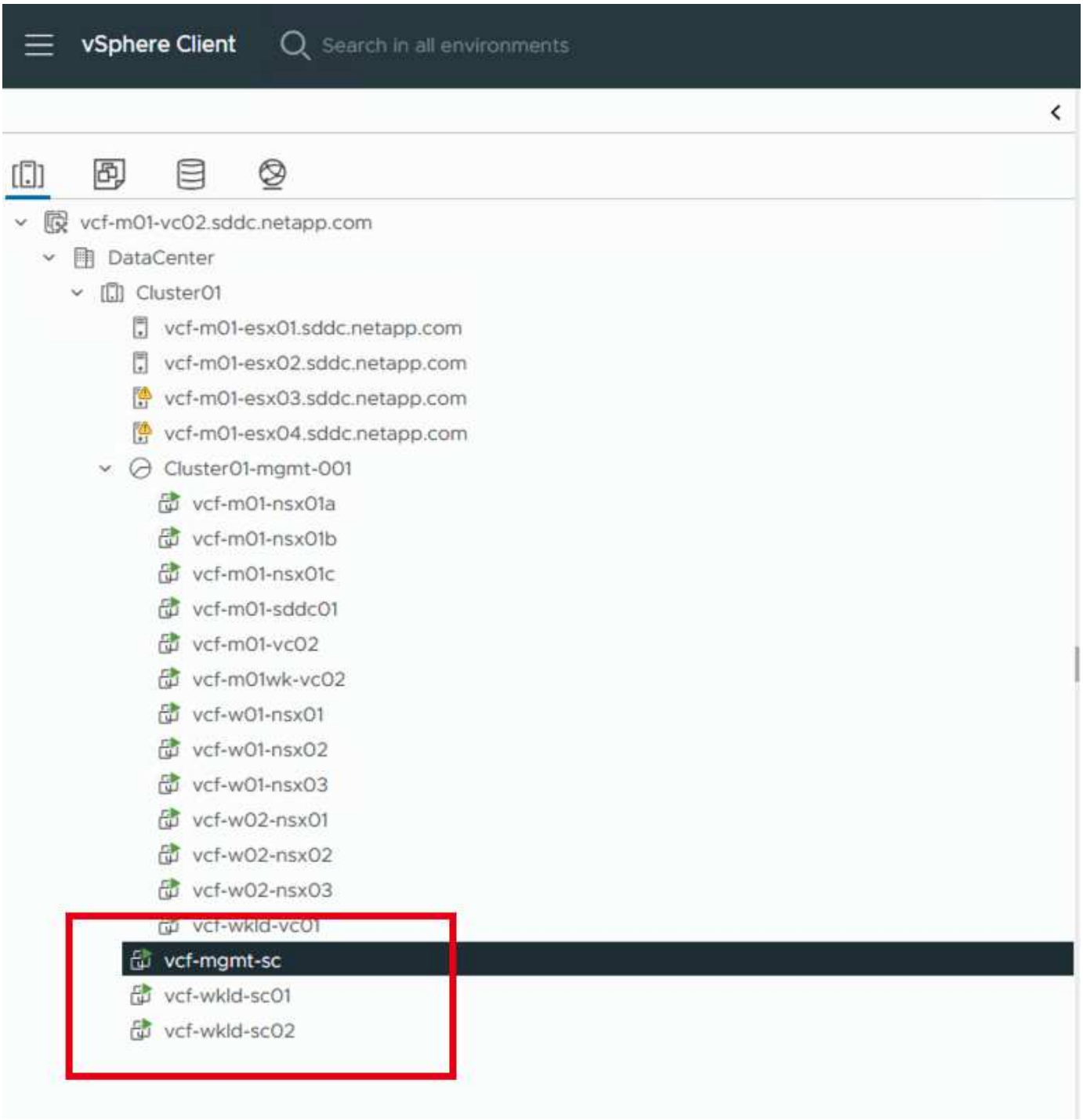
VCF 워크로드 도메인은 SDDC Manager에서 프로비저닝되고 애플리케이션 준비가 된 하나 이상의 vSphere 클러스터가 있는 ESXi 호스트 그룹입니다. 아래의 VCF 예에서는 하나의 관리 도메인과 두 개의 워크로드 도메인이

배포되었습니다. NetApp 스토리지를 사용하여 VCF를 배포하는 방법에 대한 자세한 내용은 다음을 확인하세요 ."NetApp VCF 배포 문서."



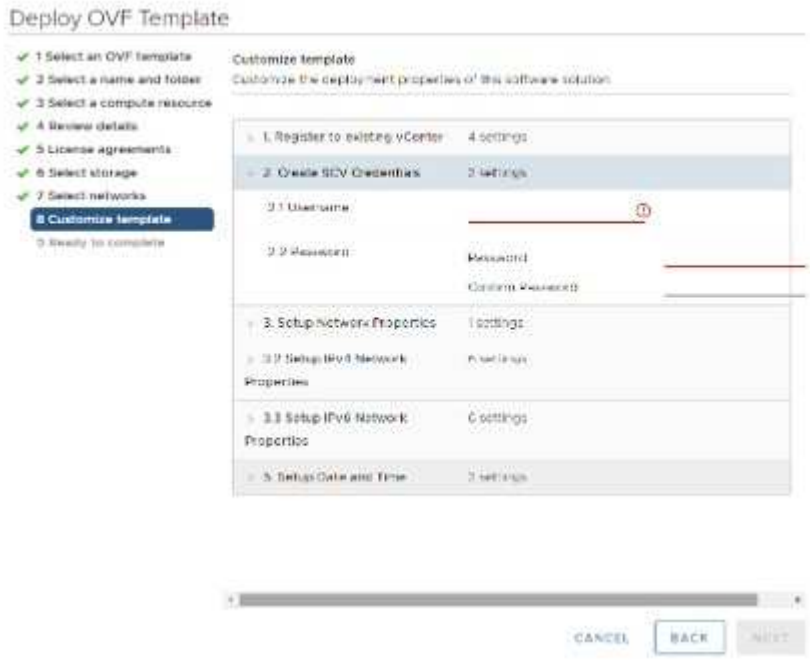
SCV 배치, 구성 및 복원 단계

작업 도메인의 수와 관리 도메인을 기반으로 여러 SCV를 배포해야 합니다. 아래 예에서는 두 개의 워크로드 도메인과 하나의 관리 도메인이 있고, 세 개의 SCV가 VCF 관리 도메인 vCenter에 배포되어 있는 것을 보여줍니다
.


vSphere Client
Search in all environments
vcf-m01-vc02.sddc.netapp.com
DataCenter
Cluster01
vcf-m01-esx01.sddc.netapp.com
vcf-m01-esx02.sddc.netapp.com
vcf-m01-esx03.sddc.netapp.com
vcf-m01-esx04.sddc.netapp.com
Cluster01-mgmt-001
vcf-m01-nsx01a
vcf-m01-nsx01b
vcf-m01-nsx01c
vcf-m01-sddc01
vcf-m01-vc02
vcf-m01wk-vc02
vcf-w01-nsx01
vcf-w01-nsx02
vcf-w01-nsx03
vcf-w02-nsx01
vcf-w02-nsx02
vcf-w02-nsx03
vcf-wkld-vc01
vcf-mgmt-sc
vcf-wkld-sc01
vcf-wkld-sc02

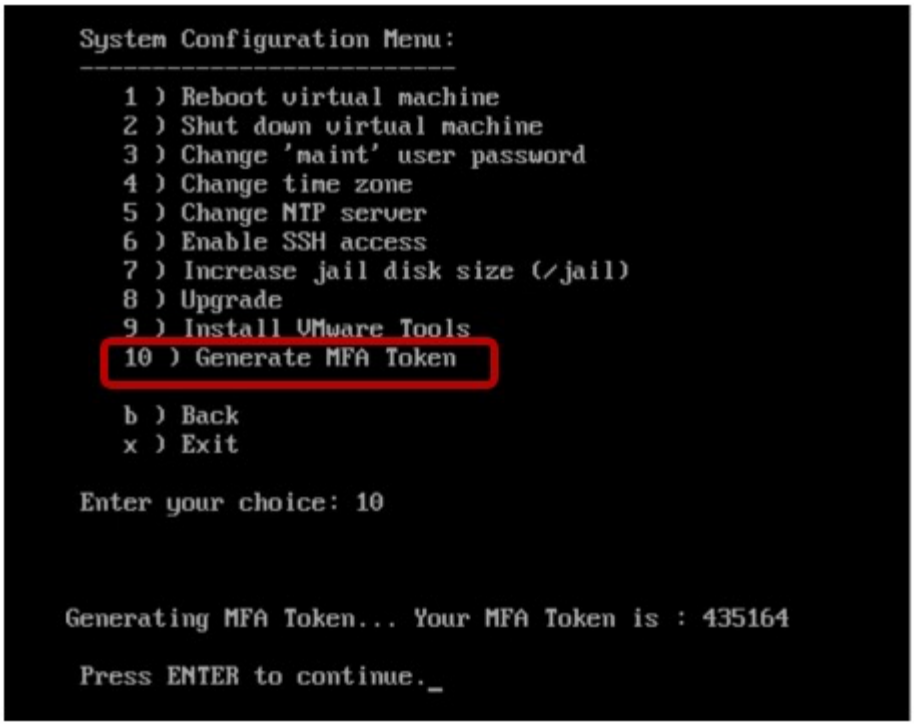
관리 도메인과 각 워크로드 도메인에 **SCV** 배포

1. "Open Virtual Appliance(OVA)를 다운로드하세요."
2. vSphere Client를 사용하여 vCenter Server에 로그인합니다. 관리 > 인증서 > 인증서 관리로 이동합니다. 신뢰할 수 있는 루트 인증서를 추가하고 각 인증서를 certs 폴더에 설치합니다. 인증서가 설치되면 OVA를 검증하고 배포할 수 있습니다.
3. VCF 워크로드 도메인 vCenter에 로그인하고 OVF 템플릿을 배포하여 VMware 배포 마법사를 시작합니다



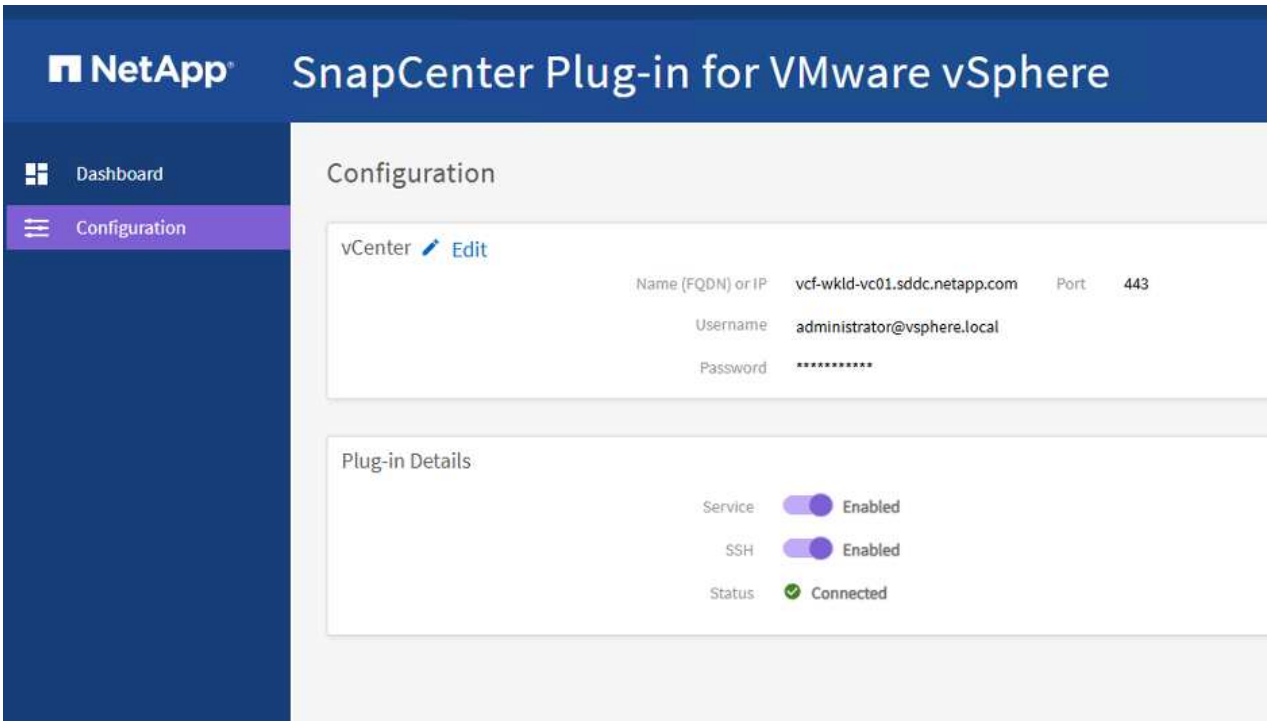
.

4. OVA의 전원을 켜서 SCV를 시작한 다음 VMware 도구 설치를 클릭합니다.
5. OVA 콘솔의 시스템 구성 메뉴에서 MFA 토큰을 생성합니다



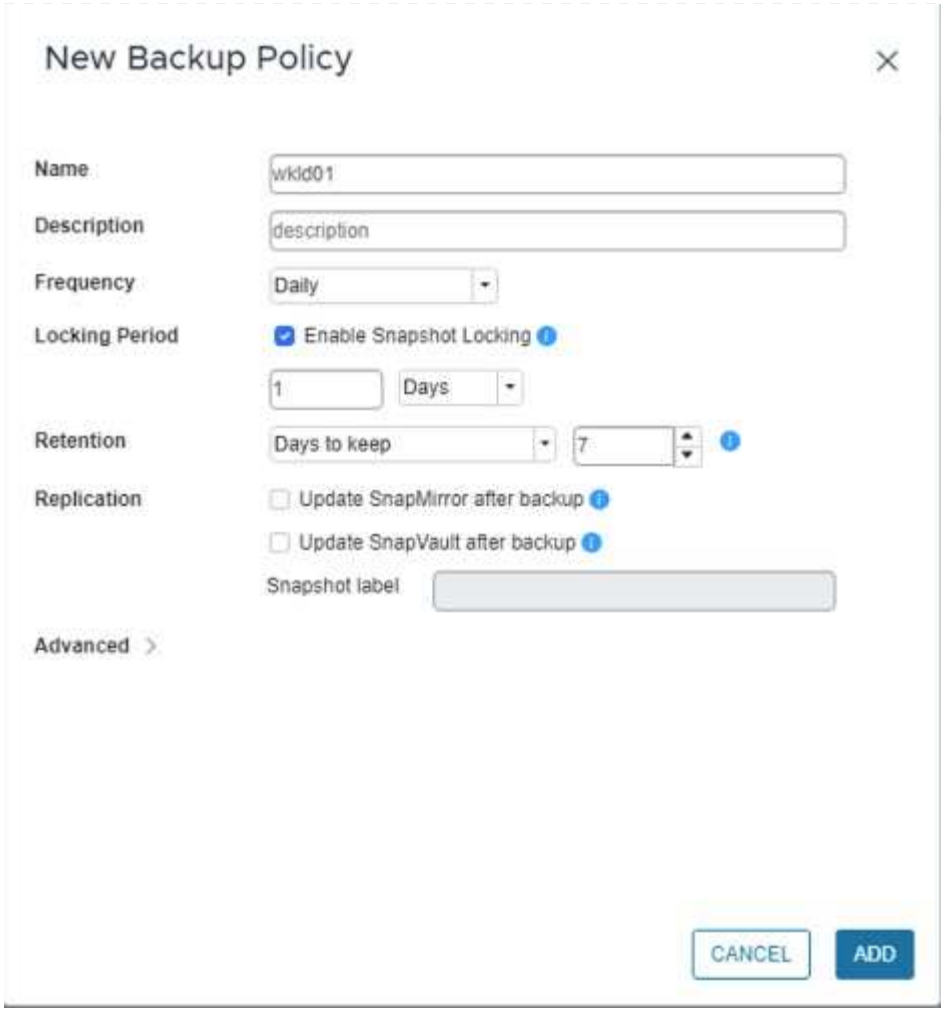
.

6. 배포 시 설정한 관리자 사용자 이름과 비밀번호, 그리고 유지 관리 콘솔을 사용하여 생성된 MFA 토큰을 사용하여 SCV 관리 GUI에 로그인합니다.
   `https://<appliance-IP-address>:8080` 관리 GUI에 접근합니다.

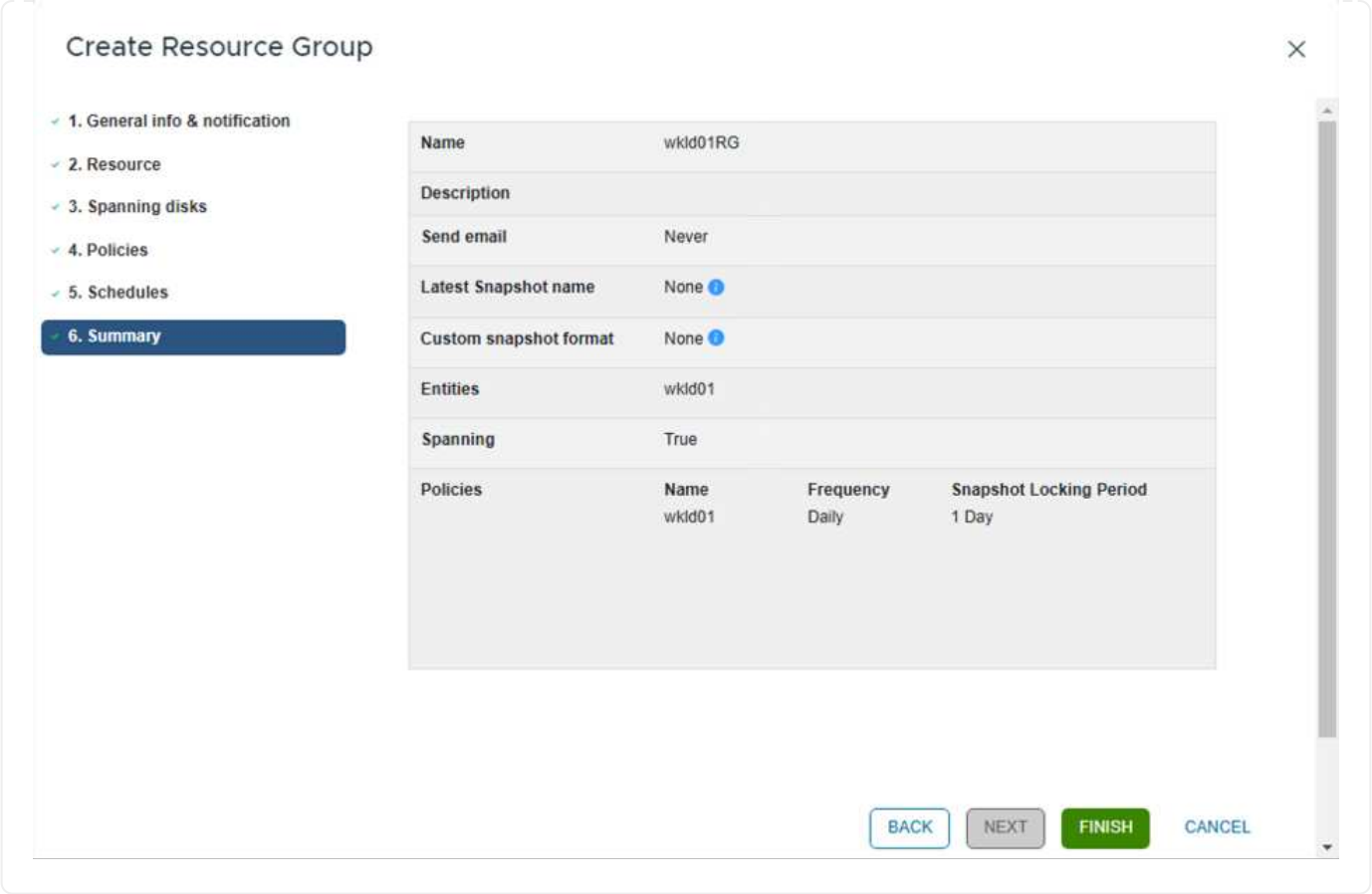


VM을 백업하거나 복원하려면 먼저 데이터 저장소를 호스팅하는 스토리지 클러스터나 VM을 추가한 다음, 보존 기간과 빈도에 대한 백업 정책을 만들고, 리소스를 보호하기 위한 리소스 그룹을 설정합니다
.

1. vCenter 웹 클라이언트에 로그인하고 도구 모음에서 메뉴를 클릭한 다음 SnapCenter Plug-in for VMware vSphere 과 스토리지 추가를 선택합니다. SCV 플러그인의 왼쪽 탐색 창에서 스토리지 시스템을 클릭한 다음 추가 옵션을 선택합니다. 스토리지 시스템 추가 대화 상자에서 기본 SVM 또는 클러스터 정보를 입력하고 추가를 선택합니다. NetApp 스토리지 IP 주소를 입력하고 로그인하세요.
2. 새 백업 정책을 만들려면 SCV 플러그인의 왼쪽 탐색 창에서 정책을 클릭하고 새 정책을 선택합니다. 새 백업 정책 페이지에서 정책 구성 정보를 입력하고 추가를 클릭합니다.



3. SCV 플러그인의 왼쪽 탐색 창에서 리소스 그룹을 클릭한 다음 만들기를 선택합니다. 리소스 그룹 생성 마법사의 각 페이지에 필요한 정보를 입력하고, 리소스 그룹에 포함할 VM과 데이터 저장소를 선택한 다음, 리소스 그룹에 적용할 백업 정책을 선택하고 백업 일정을 지정합니다.

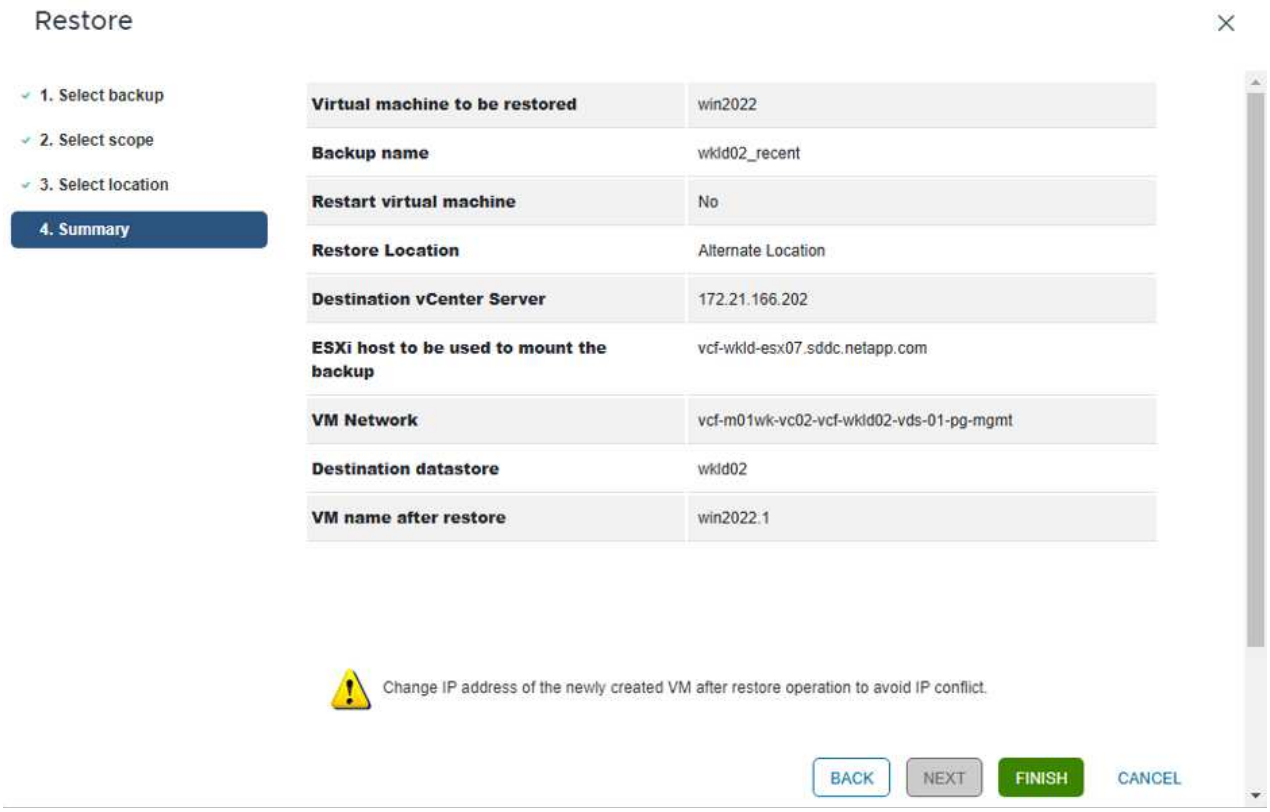

Create Resource Group
1. General info & notification
2. Resource
3. Spanning disks
4. Policies
5. Schedules
6. Summary
Name
wkld01RG
Description
Send email
Never
Latest Snapshot name
None
Custom snapshot format
None
Entities
wkld01
Spanning
True
Policies
Name
wkld01
Frequency
Daily
Snapshot Locking Period
1 Day
BACK
NEXT
FINISH
CANCEL

VM 및 파일 또는 폴더 백업 복원

백업된 VM, VMDK, 파일 및 폴더를 복원할 수 있습니다. VM은 동일한 vCenter Server에 있는 원래 호스트나 대체 호스트, 또는 동일한 vCenter에서 관리하는 대체 ESXi 호스트로 복원될 수 있습니다. 백업에 있는 파일에 액세스하려면 백업에서 기존 데이터 저장소를 마운트할 수 있습니다. 백업이 생성된 동일한 ESXi 호스트에 백업을 마운트하거나 동일한 유형의 VM 및 호스트 구성을 갖춘 대체 ESXi 호스트에 마운트할 수 있습니다. 호스트에 데이터 저장소를 여러 번 마운트할 수 있습니다. 개별 파일과 폴더는 게스트 파일 복원 세션에서도 복원할 수 있습니다. 이 세션에서는 가상 디스크의 백업 사본을 첨부한 다음 선택한 파일이나 폴더를 복원합니다. 파일과 폴더도 복구할 수 있습니다.

VM 복원 단계

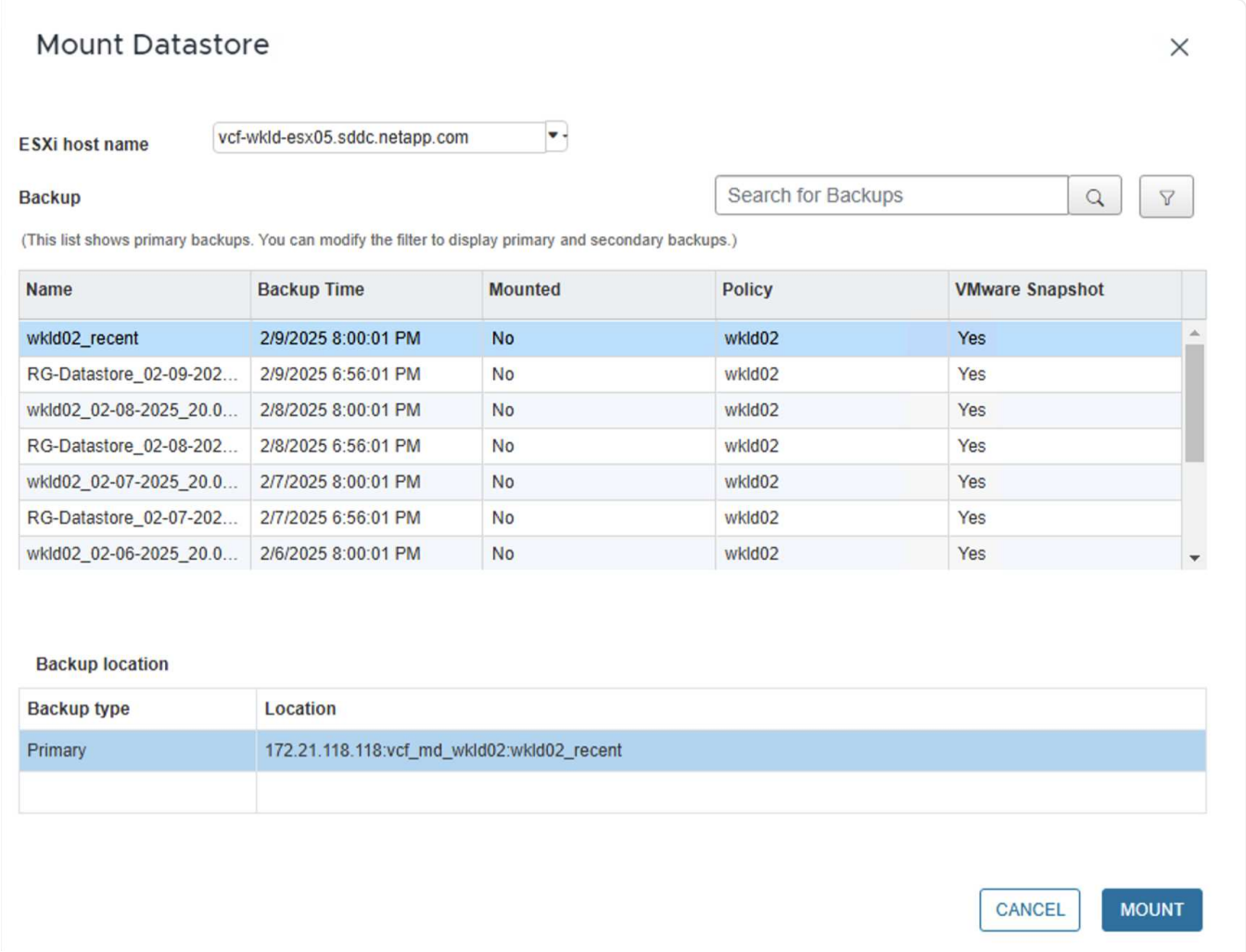
1. VMware vSphere 클라이언트 GUI에서 도구 모음의 메뉴를 클릭하고 드롭다운 목록에서 VM 및 템플릿을 선택한 다음, VM을 마우스 오른쪽 버튼으로 클릭하고 드롭다운 목록에서 SnapCenter Plug-in for VMware vSphere 선택한 다음, 보조 드롭다운 목록에서 복원을 선택하여 마법사를 시작합니다.
2. 복원 마법사에서 복원하려는 백업 스냅샷을 선택하고 복원 범위 필드에서 전체 가상 머신을 선택한 다음 복원 위치를 선택하고 백업을 마운트할 대상 정보를 입력합니다. 위치 선택 페이지에서 복원된 데이터 저장소의 위치를 선택합니다. 요약 페이지를 검토하고 마침을 클릭합니다.



3. 화면 하단의 최근 작업을 클릭하여 작업 진행 상황을 모니터링하세요.

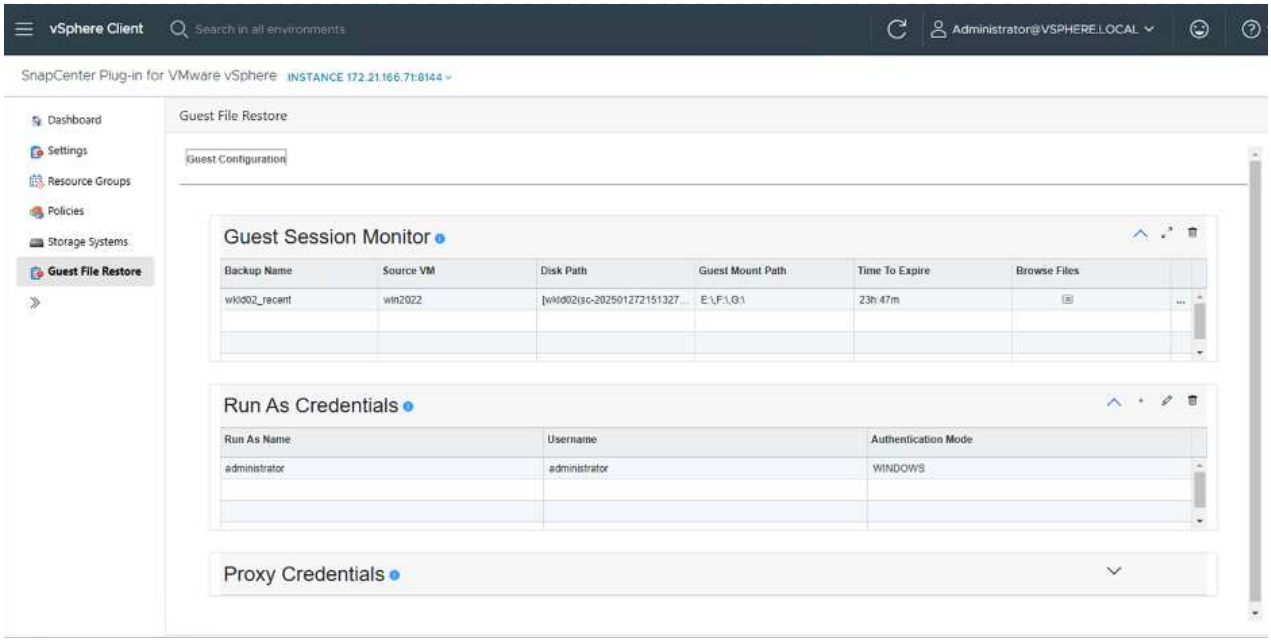
데이터 저장소 복원 단계

1. 데이터스토어를 마우스 오른쪽 버튼으로 클릭하고 SnapCenter Plug-in for VMware vSphere > 백업 마운트를 선택합니다.
2. 데이터 저장소 마운트 페이지에서 백업과 백업 위치(기본 또는 보조)를 선택한 다음 마운트를 클릭합니다.

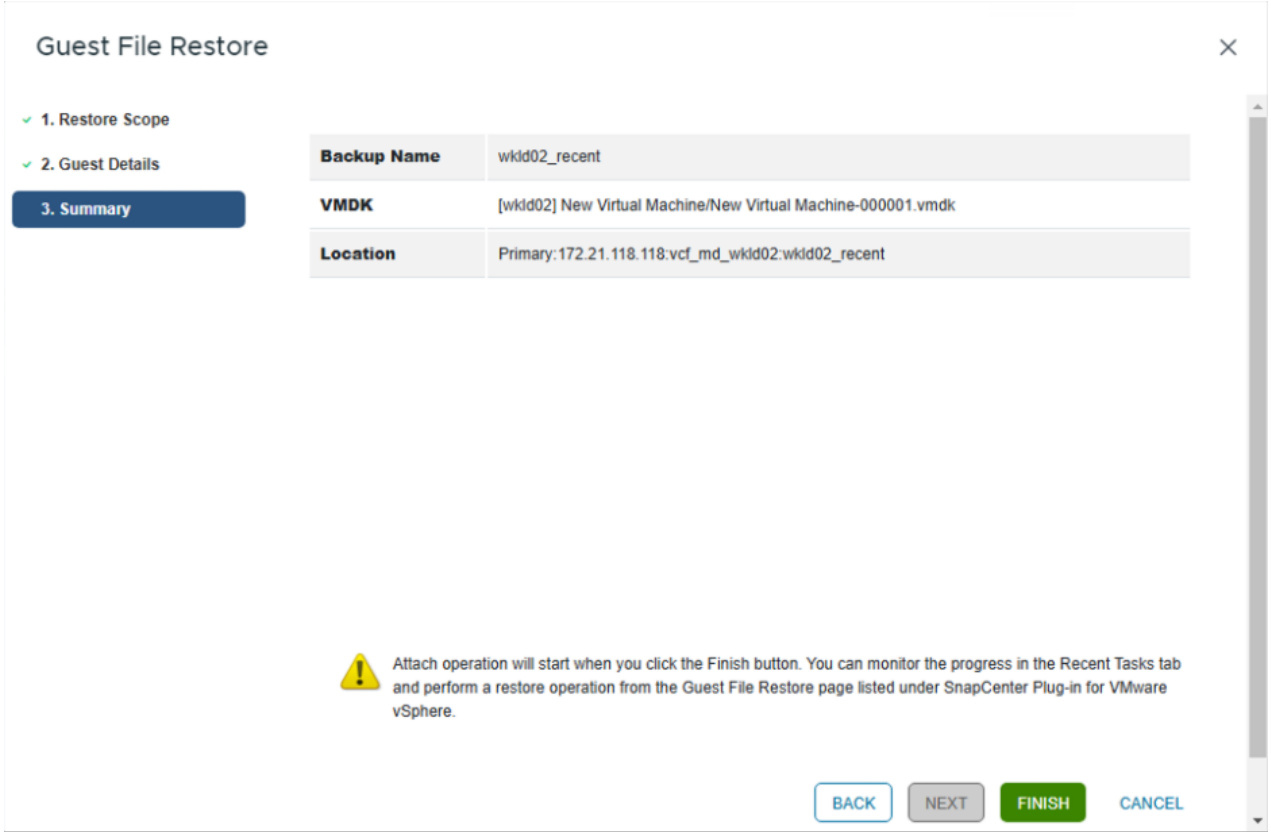


파일 및 폴더 복원 단계

1. 게스트 파일이나 폴더 복원 작업을 위해 가상 디스크를 연결하는 경우 복원하기 전에 연결 대상 VM에 자격 증명을 구성해야 합니다. SnapCenter Plug-in for VMware vSphere 에서 게스트 파일 복원 및 자격 증명으로 실행 섹션을 선택하고 사용자 자격 증명을 입력합니다. 사용자 이름에는 "관리자"를 입력해야 합니다.



2. vSphere 클라이언트에서 VM을 마우스 오른쪽 버튼으로 클릭하고 SnapCenter Plug-in for VMware vSphere > 게스트 파일 복원을 선택합니다. 복원 범위 페이지에서 백업 이름, VMDK 가상 디스크 및 위치(기본 또는 보조)를 지정합니다. 확인하려면 'Summery'를 클릭하세요.



VCP 다중 도메인용 NetApp SnapCenter 데이터 보호를 중앙 집중화하고, NetApp 스냅샷을 사용하여 백업에 필요한 시간과 저장 공간을 효율적으로 줄이고, 강력한 백업 및 복제 기능으로 대규모 VMware 환경을 지원하고, 전체 VM, 특정 VMDK 또는 개별 파일의 세분화된 복구를 허용합니다.

SCV를 사용하여 **VCF** 다중 도메인을 보호하는 비디오 데모

NetApp SCV를 사용하여 VMware VCF 다중 도메인 보호

VMware vSphere용 NVMe over TCP 스토리지 및 SnapCenter 플러그인을 사용하여 VCF 워크로드 도메인을 보호합니다.

SnapCenter Plug-in for VMware vSphere 사용하여 NVMe를 통해 VCF 워크로드 도메인을 보호하세요. 이 절차에는 플러그인 설정, 최적의 성능을 위한 NVMe over TCP 구성, 백업, 복원 또는 복제 작업 수행이 포함됩니다.

TCP를 통한 NVMe(Non-Volatile Memory Express)는 All Flash FAS (AFF) 및 All SAN Array(ASA)를 포함하여 VMware Cloud Foundation ESXi 서버와 NetApp 스토리지 간의 고속 데이터 전송을 용이하게 하는 최첨단 네트워크 프로토콜입니다.

소개

TCP를 통한 NVMe를 활용하면 까다로운 작업 부하에서도 낮은 지연 시간과 높은 처리량을 제공합니다. VMware vSphere(SCV)용 NetApp SnapCenter Plug-in for VMware vSphere 과 NVMe over TCP를 통합하면 효율적인 데이터 관리를 위한 강력한 조합이 제공되어 VMware 환경 내에서 백업, 복원 및 복제 작업이 향상됩니다.

TCP를 통한 **NVMe**의 이점

- 고성능: 낮은 지연 시간과 높은 데이터 전송 속도로 뛰어난 성능을 제공합니다. 이는 까다로운 애플리케이션과 대규모 데이터 작업에 매우 중요합니다.
- 확장성: 확장 가능한 구성을 지원하여 IT 관리자가 데이터 요구 사항이 증가함에 따라 인프라를 원활하게 확장할 수 있습니다.
- 효율성: 백업 및 복원 작업을 더 빠르게 진행하여 가동 중지 시간을 줄이고 전반적인 시스템 가용성을 향상시킵니다.

이 문서에서는 최적의 성능을 위해 NVMe over TCP를 활용하는 데 중점을 두고 VMware Cloud Foundation(VCF) 환경에서 SCV를 배포하고 관리하는 단계를 제공합니다.

대상

VMware VCF 워크로드 도메인에 대한 데이터 보호 및 재해 복구를 보장하는 솔루션 아키텍트 또는 스토리지 관리자입니다.

아키텍처 개요

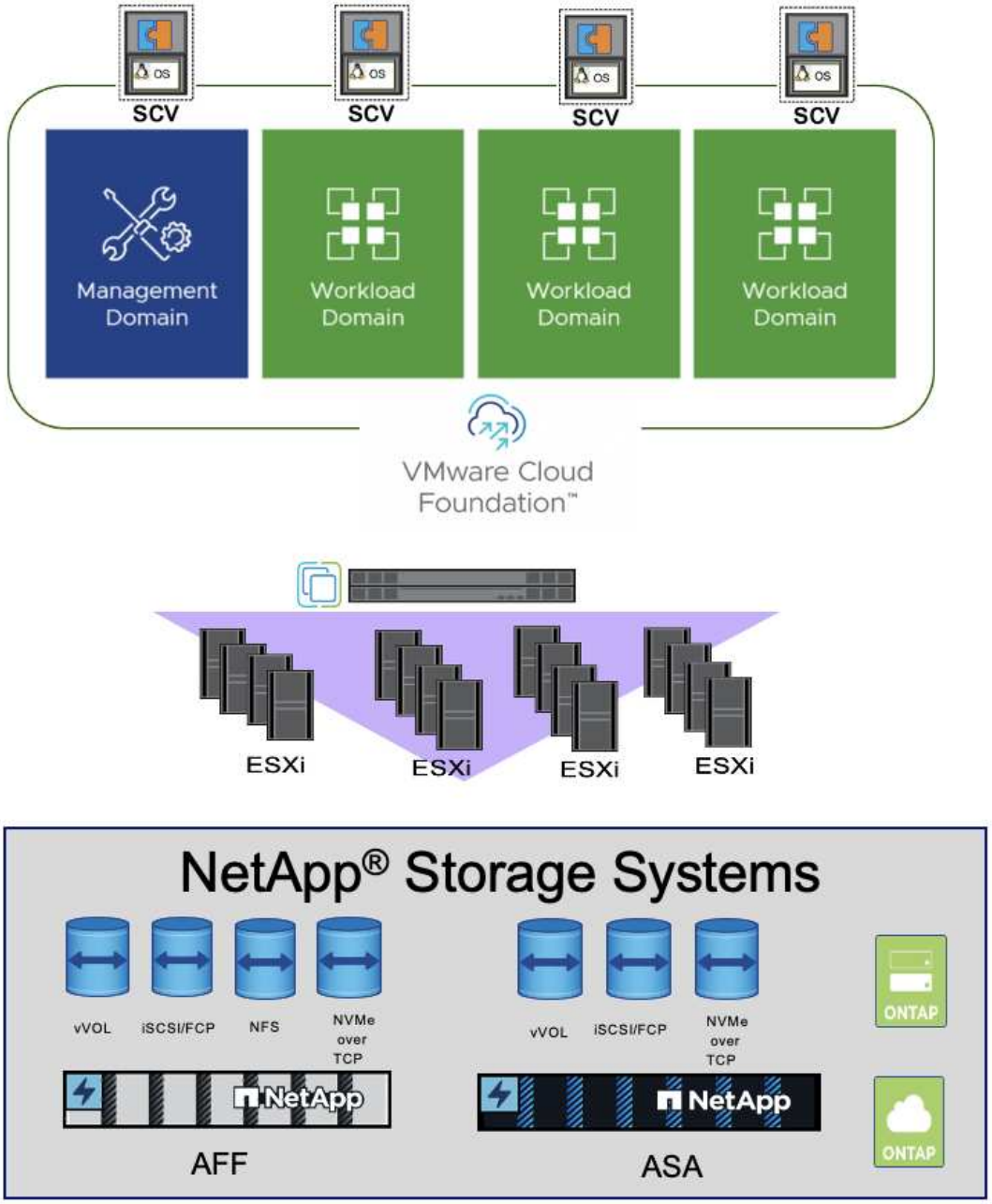
SCV는 VMware 환경의 VM, 데이터 저장소, 파일 및 폴더에 대한 빠르고 공간 효율적이며 충돌 일관성이 뛰어나고 VM 일관성이 있는 백업 및 복원 작업을 용이하게 하도록 설계된 강력한 도구입니다. SCV는 OVA 파일을 사용하여 Linux 가상 어플라이언스로 배포되며 원격 플러그인 아키텍처를 활용합니다.

SCV 배포 아키텍처

- 가상 어플라이언스 배포: SCV는 OVA 파일을 사용하여 Linux 가상 어플라이언스로 배포됩니다. 이 배포 방법은 간소화되고 효율적인 설정 프로세스를 보장합니다.
- 원격 플러그인 아키텍처: SCV는 원격 플러그인 아키텍처를 사용하여 여러 인스턴스를 관리하는 데 있어 확장성과 유연성을 제공합니다.

- 일대일 관계: 각 VCF 도메인에는 전용 SCV 인스턴스가 필요하므로 격리되고 효율적인 백업 및 복원 작업이 보장됩니다.

ONTAP 9.10.1 이상 버전에서는 NetApp AFF 와 ASA NVMe over TCP를 지원합니다. AFF 또는 ASA 기본 시스템에 있는 데이터로 ONTAP AFF 또는 ASA 보조 시스템으로 복제할 수 있습니다. SCV는 또한 SnapCenter Server와 함께 작동하여 SnapCenter 애플리케이션별 플러그인에 대한 VMware 환경에서 애플리케이션 기반 백업 및 복원 작업을 지원합니다. 자세한 내용은 다음을 확인하세요."SnapCenter Plug-in for VMware vSphere 설명서" 그리고"SnapCenter 로 워크로드 보호"



3-2-1 백업 규칙은 데이터 사본을 세 개 만들어 두 가지 유형의 미디어에 저장하고, 사본 한 개를 오프사이트에 보관하는 데이터 보호 전략입니다. BlueXP backup and recovery 온프레미스와 클라우드 환경 모두에서 광범위한 백업 및 복구 작업에 대한 단일 제어 평면을 제공하는 클라우드 기반 데이터 관리 도구입니다. NetApp BlueXP backup and recovery 제품군의 일부인 기능은 SCV(온프레미스)와 통합되어 데이터 사본을 클라우드의 개체 스토리지로 확장하는

기능입니다. 이를 통해 1차 또는 2차 저장소 백업에서 가져온 데이터의 세 번째 사본이 오프사이트에 생성됩니다. BlueXP backup and recovery 사용하면 이 두 온프레미스 위치 중 하나에서 데이터 사본을 전송하는 저장 정책을 쉽게 설정할 수 있습니다. 자세한 내용은 다음을 확인하세요."SnapCenter 플러그인과 BlueXP backup and recovery 통한 VMware용 3-2-1 데이터 보호" .

NVMe 배포 단계에서 **VCF**용 **SCV**

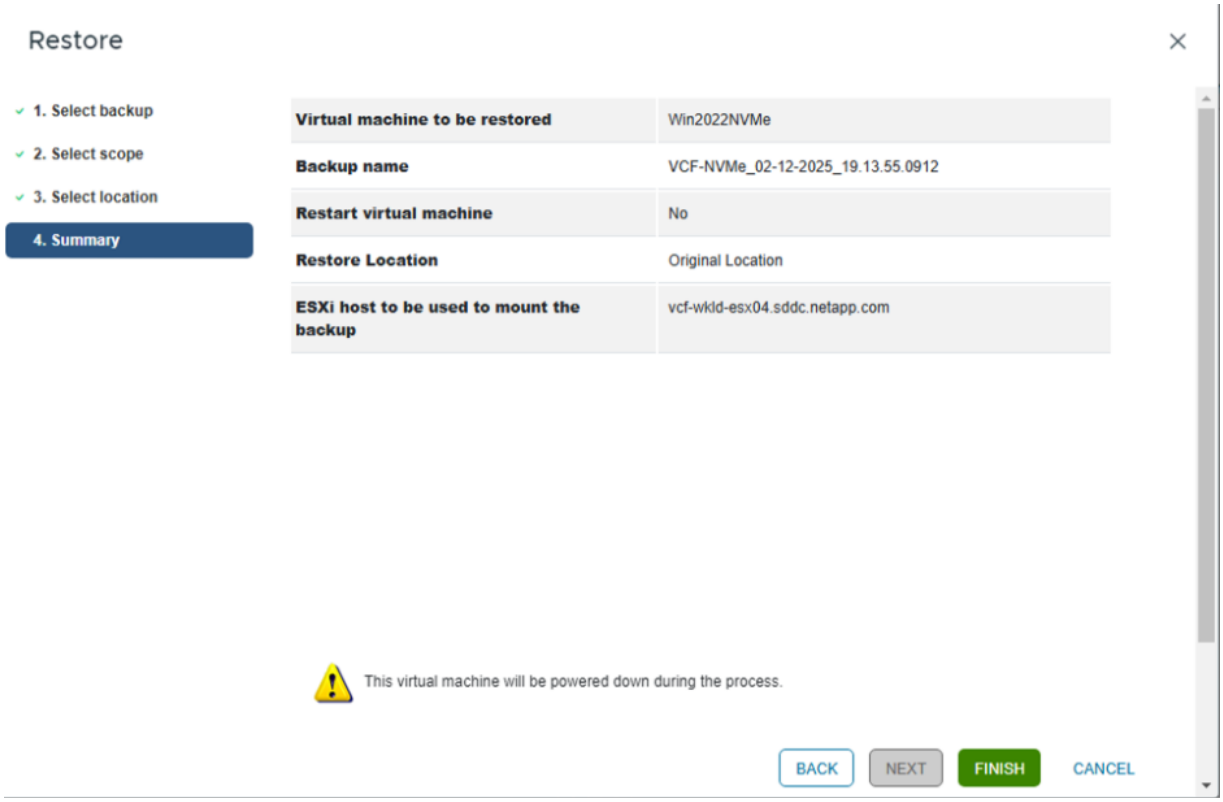
그만큼"ONTAP tools for VMware vSphere" (OTV)는 VMware 환경에서 NetApp 스토리지를 관리하기 위한 강력하고 효율적인 솔루션을 제공합니다. OTV는 vCenter Server와 직접 통합하여 스토리지 관리를 간소화하고, 데이터 보호를 강화하고, 성능을 최적화합니다. 선택 사항이기는 하지만 OTV를 구축하면 VMware 환경의 관리 기능과 전반적인 효율성을 크게 개선할 수 있습니다.

- "VCF 워크로드 도메인을 위한 NVMe/TCP 스토리지 생성"
- "VMware vSphere(SCV)에 대한 NetApp SnapCenter 구성"

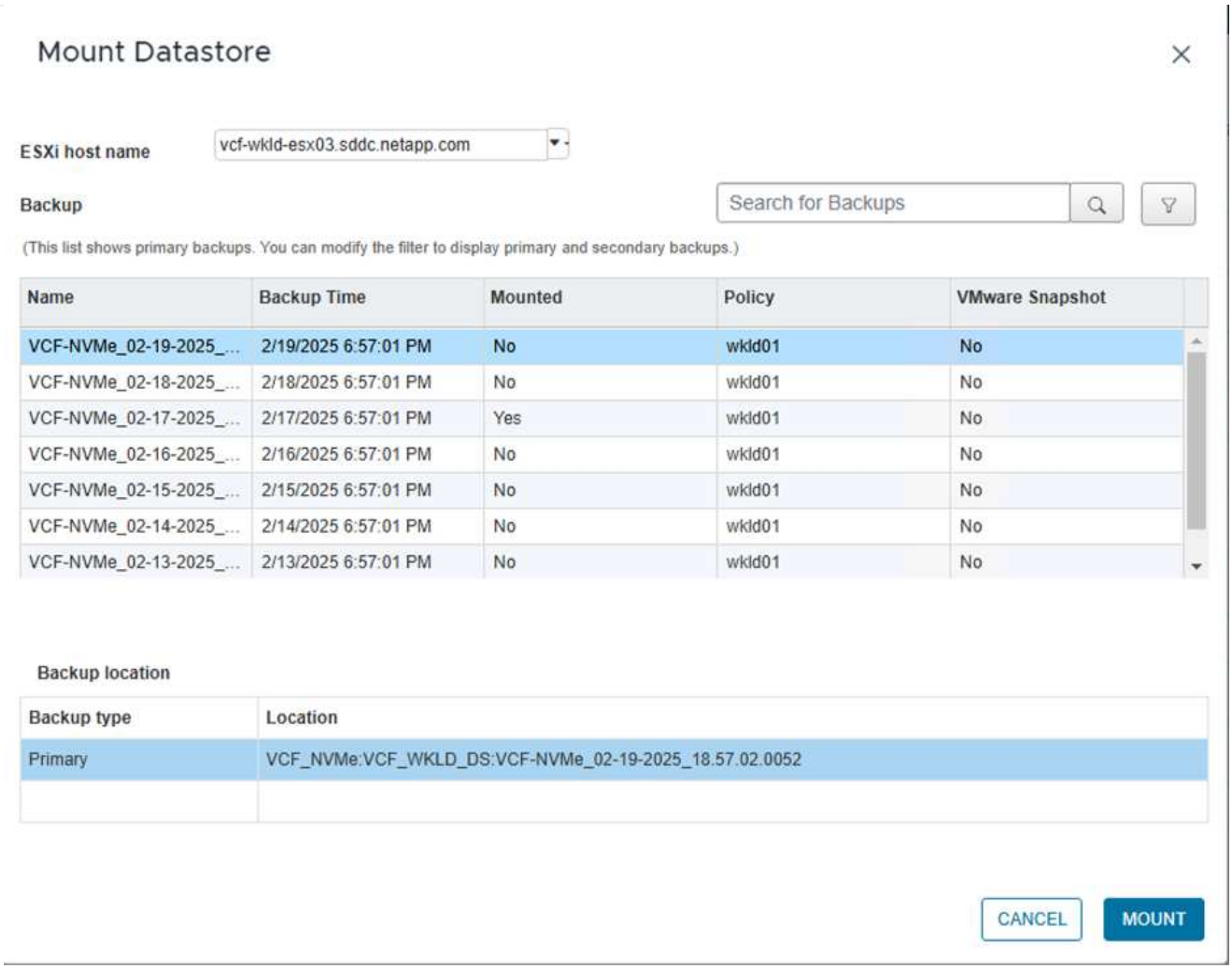
VM, 데이터 저장소, 가상 디스크 및 파일 또는 폴더 복원

SCV는 VMware 환경에 대한 포괄적인 백업 및 복원 기능을 제공합니다. VMFS 환경의 경우 SCV는 Storage VMotion과 함께 복제 및 마운트 작업을 사용하여 복원 작업을 수행합니다. 이를 통해 효율적이고 원활한 데이터 복구가 보장됩니다. 자세한 내용은 다음을 확인하세요."복원 작업이 수행되는 방식."

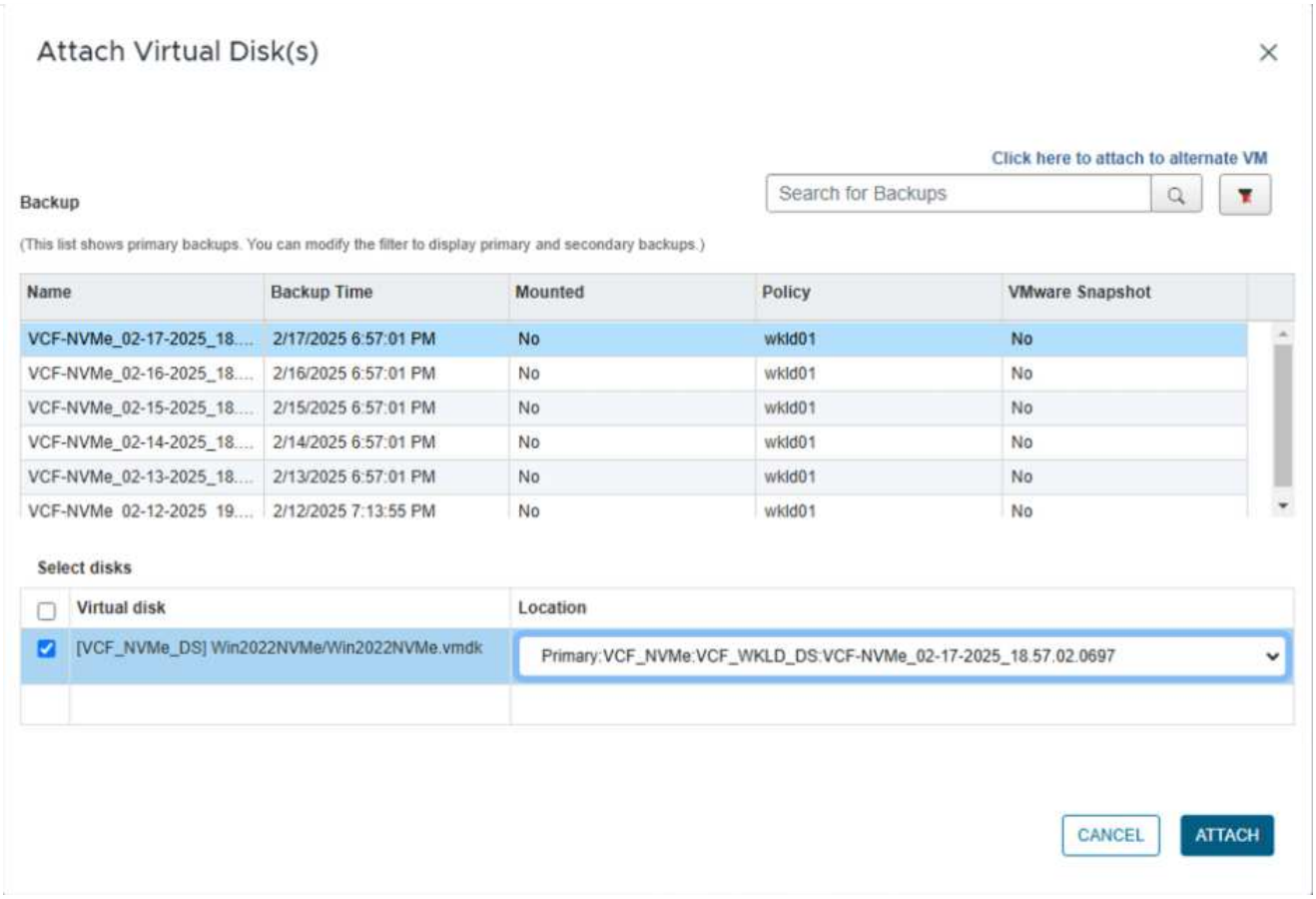
- VM 복원 동일한 vCenter Server 내의 원래 호스트나 동일한 vCenter Server에서 관리하는 대체 ESXi 호스트로 VM을 복원할 수 있습니다.
  a. VM을 마우스 오른쪽 버튼으로 클릭하고 드롭다운 목록에서 SnapCenter Plug-in for VMware vSphere 선택한 다음, 보조 드롭다운 목록에서 복원을 선택하여 마법사를 시작합니다.
  b. 복원 마법사에서 복원하려는 백업 스냅샷을 선택하고 복원 범위 필드에서 전체 가상 머신을 선택한 다음 복원 위치를 선택하고 백업을 마운트할 대상 정보를 입력합니다. 위치 선택 페이지에서 복원된 데이터 저장소의 위치를 선택합니다. 요약 페이지를 검토하고 마침을 클릭합니다
  .



- 백업에 있는 파일에 액세스하려면 백업에서 기존 데이터 저장소를 마운트할 수 있습니다. 백업이 생성된 동일한 ESXi 호스트에 백업을 마운트하거나 동일한 유형의 VM 및 호스트 구성을 갖춘 대체 ESXi 호스트에 마운트할 수 있습니다. 호스트에 데이터 저장소를 여러 번 마운트할 수 있습니다.
  a. 데이터스토어를 마우스 오른쪽 버튼으로 클릭하고 SnapCenter Plug-in for VMware vSphere > 백업 마운트를 선택합니다.
  b. 데이터 저장소 마운트 페이지에서 백업과 백업 위치(기본 또는 보조)를 선택한 다음 마운트를 클릭합니다.

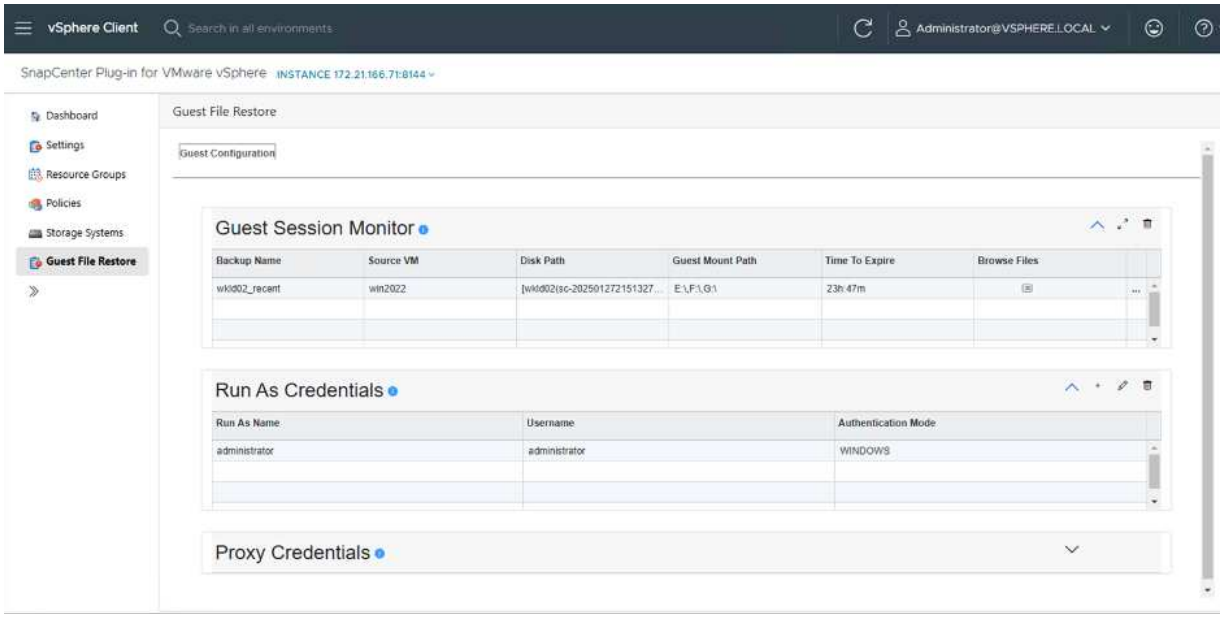


- 가상 디스크 연결 백업에서 하나 이상의 VMDK를 부모 VM에 연결하거나, 동일한 ESXi 호스트의 대체 VM에 연결하거나, 연결 모드에서 동일한 vCenter 또는 다른 vCenter가 관리하는 대체 ESXi 호스트의 대체 VM에 연결할 수 있습니다.
  a. VM을 마우스 오른쪽 버튼으로 클릭하고 SnapCenter Plug-in for VMware vSphere > 가상 디스크 연결을 선택합니다.
  b. 가상 디스크 연결 창에서 백업을 선택하고 연결할 디스크를 하나 이상 선택하고 연결할 위치(기본 또는 보조)를 선택합니다. 기본적으로 선택된 가상 디스크는 부모 VM에 연결됩니다. 선택한 가상 디스크를 동일한 ESXi 호스트의 대체 VM에 연결하려면 여기를 클릭하여 대체 VM에 연결을 선택하고 대체 VM을 지정합니다. 첨부를 클릭하세요.



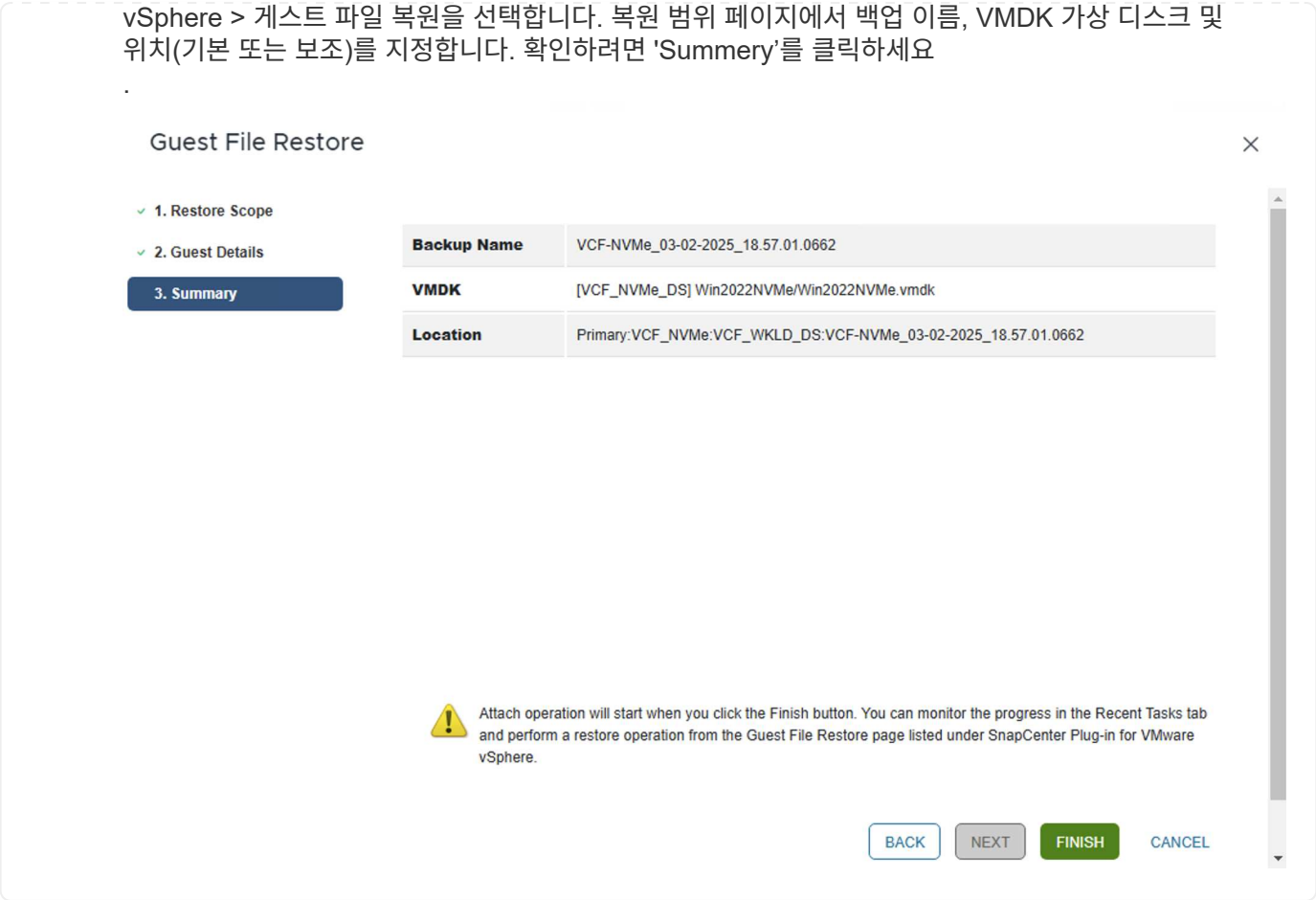
- 파일 및 폴더 복원 단계 개별 파일과 폴더는 게스트 파일 복원 세션에서 복원할 수 있습니다. 이 세션에서는 가상 디스크의 백업 사본을 첨부한 다음 선택한 파일이나 폴더를 복원합니다. 파일과 폴더도 복구할 수 있습니다. 더 자세한 내용을 확인하세요"SnapCenter 파일 및 폴더 복원."

  a. 게스트 파일이나 폴더 복원 작업을 위해 가상 디스크를 연결하는 경우 복원하기 전에 연결 대상 VM에 자격 증명을 구성해야 합니다. SnapCenter Plug-in for VMware vSphere 에서 게스트 파일 복원 및 자격 증명으로 실행 섹션을 선택하고 사용자 자격 증명을 입력합니다. 사용자 이름에는 "관리자"를 입력해야 합니다.



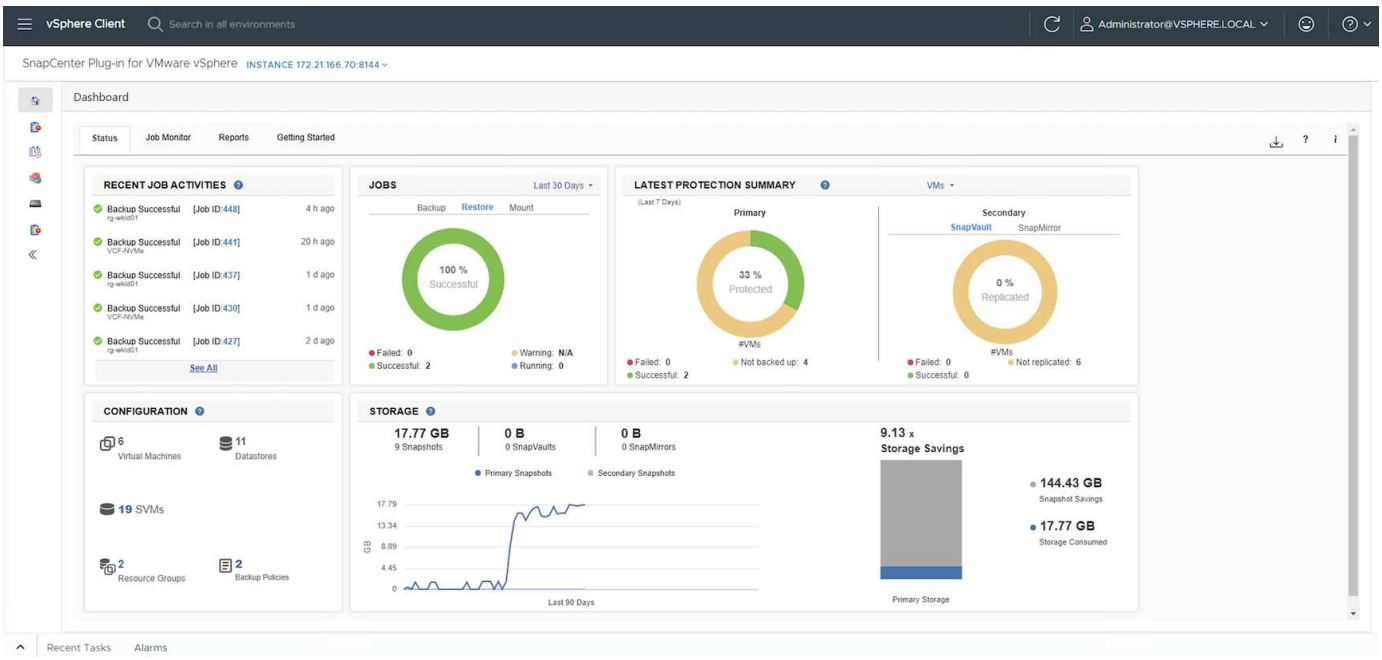
  b. vSphere 클라이언트에서 VM을 마우스 오른쪽 버튼으로 클릭하고 SnapCenter Plug-in for VMware

vSphere > 게스트 파일 복원을 선택합니다. 복원 범위 페이지에서 백업 이름, VMDK 가상 디스크 및 위치(기본 또는 보조)를 지정합니다. 확인하려면 'Summery'를 클릭하세요
.



모니터링 및 보고

SCV는 관리자가 백업 및 복원 작업을 효율적으로 관리하는 데 도움이 되는 강력한 모니터링 및 보고 기능을 제공합니다. 상태 정보를 보고, 작업을 모니터링하고, 작업 로그를 다운로드하고, 보고서에 액세스할 수 있으며 자세한 내용은 다음을 확인하세요."VMware vSphere Monitor and Report용 SnapCenter 플러그인."



NVMe over TCP와 VMware vSphere용 NetApp SnapCenter Plug-in for VMware vSphere 의 힘을 활용하면 조직은 VMware Cloud Foundation 워크로드 도메인에 대한 고성능 데이터 보호 및 재해 복구를 달성할 수 있습니다. 이러한 접근 방식은 빠르고 안정적인 백업 및 복원 작업을 보장하여 가동 중지 시간을 최소화하고 중요한 데이터를 보호합니다.

BlueXP 로 VMware 데이터 저장소 보호

BlueXP disaster recovery 사용하여 VMware 데이터 저장소를 보호하는 방법에 대해 알아보세요.

VMware를 위한 BlueXP disaster recovery 사용하여 재해 복구를 위한 NetApp 솔루션에 대해 알아보세요. 이를 통해 기본 사이트에서 재해 복구 사이트로 블록 수준 복제를 사용하여 재해 복구를 위한 강력한 솔루션이 제공됩니다.

BlueXP DRaaS는 랜섬웨어 공격을 포함한 사이트 장애 및 데이터 무결성 문제로부터 작업 부하를 보호하는 효과적이고 경제적인 방법입니다. 또한 NetApp BlueXP DRaaS는 관리형 클라우드 기반 재해 복구 솔루션을 제공하여 이러한 전략을 강화하고 재해 발생 시 신속한 복구와 최소한의 가동 중지 시간을 보장합니다.

기술적 세부 사항은 다음 솔루션을 참조하세요.

- "VMFS 데이터 저장소에 BlueXP DRaaS를 사용한 DR"
- "NFS 데이터 저장소에 BlueXP DRaaS를 사용한 DR"

VMware vSphere 및 BlueXP backup and recovery 위한 SnapCenter 플러그인을 사용하여 VMware에 대한 3-2-1 데이터 보호 구성

VMware vSphere 및 BlueXP backup and recovery 위한 SnapCenter 플러그인을 사용하여 VMware 환경에 대한 3-2-1 데이터 보호 전략을 구성합니다. 이 절차에는 기본 및 보조 ONTAP 클러스터에서 VM 및 데이터 저장소 백업을 설정하고, 플러그인과 BlueXP 구성하고, 안정적인 복구를 위해 클라우드 또는 오프사이트 스토리지로의 데이터 복제를 관리하는 작업이 포함됩니다.

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 SnapCenter Plug-in for VMware vSphere 사용하여 온프레미스 가상 머신의 기본 및 보조 백업을 생성하고, 가상 머신을 위한 BlueXP backup and recovery 사용하여 데이터 사본을 클라우드 스토리지 또는 StorageGRID 에 백업하는 3-2-1 백업 솔루션을 다룹니다.

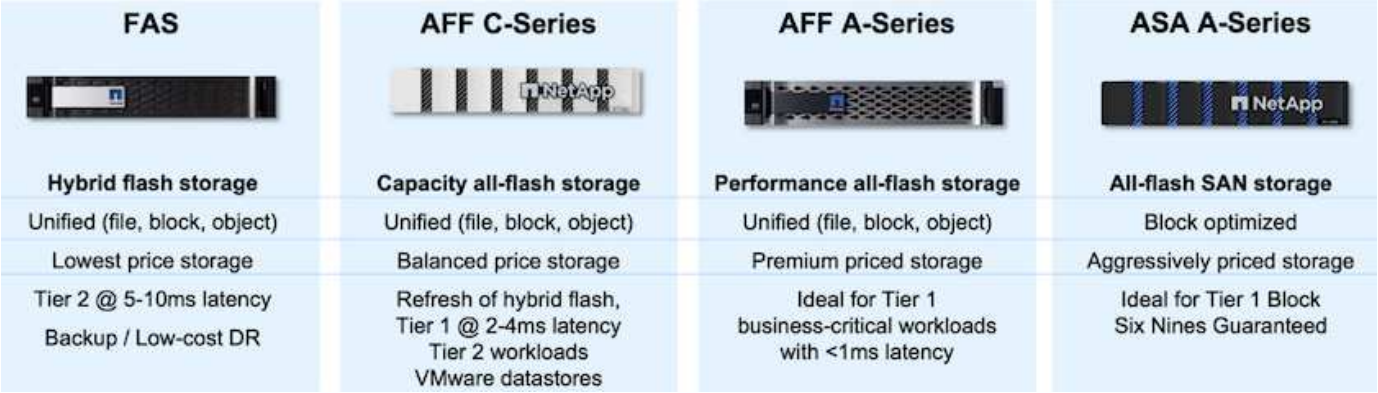
사용 사례

이 솔루션은 다음과 같은 사용 사례를 해결합니다.

- SnapCenter Plug-in for VMware vSphere 사용하여 온프레미스 가상 머신과 데이터 저장소를 백업하고 복원합니다.
- BlueXP backup and recovery 복구를 사용하여 ONTAP 클러스터에 호스팅된 온프레미스 가상 머신과 데이터 저장소를 백업하고 복원하고, 개체 스토리지에 백업합니다.

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" .

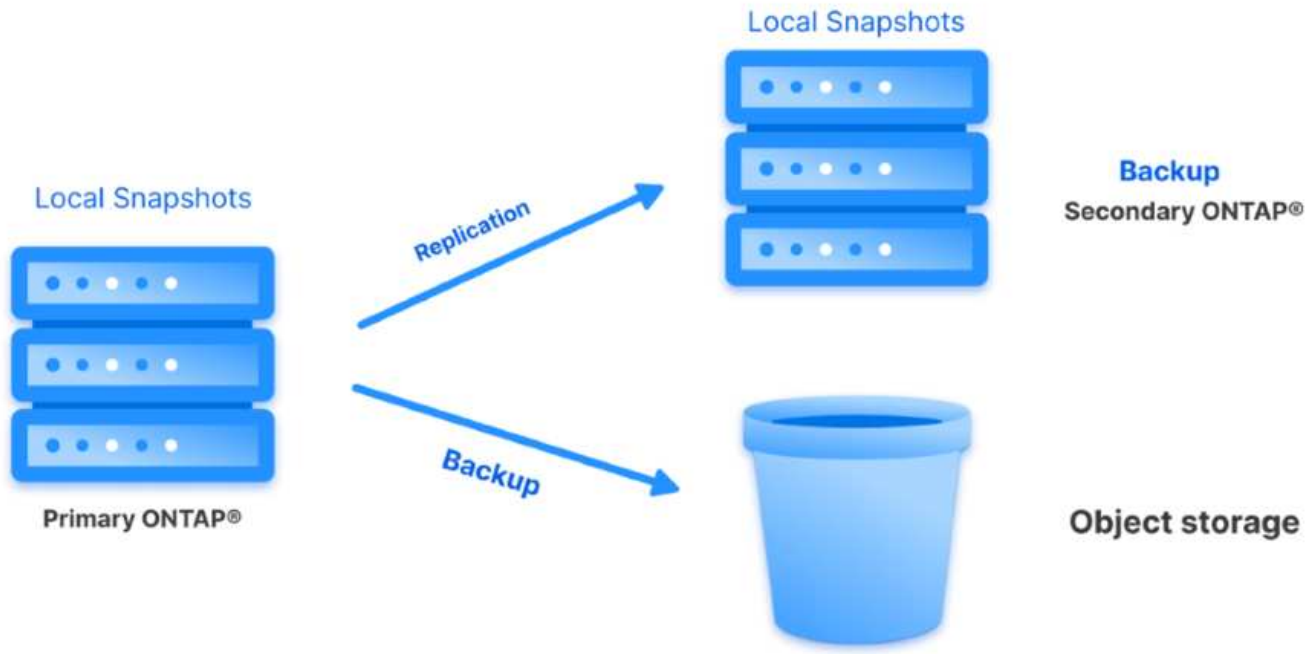
가상 머신을 위한 **BlueXP backup and recovery**

BlueXP backup and recovery 온프레미스와 클라우드 환경 모두에서 광범위한 백업 및 복구 작업에 대한 단일 제어 평면을 제공하는 클라우드 기반 데이터 관리 도구입니다. NetApp BlueXP backup and recovery 제품군의 일부인 기능은 VMware vSphere(온프레미스)용 SnapCenter 플러그인과 통합되어 데이터 사본을 클라우드의 개체 스토리지로 확장하는 기능입니다. 이를 통해 1차 또는 2차 저장소 백업에서 가져온 데이터의 세 번째 사본이 오프사이트에 생성됩니다. BlueXP backup and recovery 사용하면 이 두 온프레미스 위치 중 하나에서 데이터 사본을

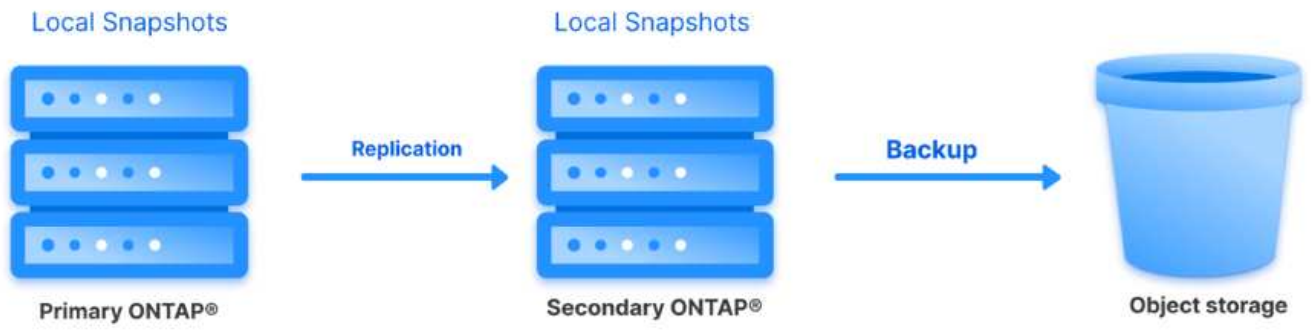
전송하는 저장 정책을 쉽게 설정할 수 있습니다.

BlueXP 백업 및 복구에서 소스로 기본 백업과 보조 백업을 선택하면 다음 두 가지 토폴로지 중 하나가 구현됩니다.

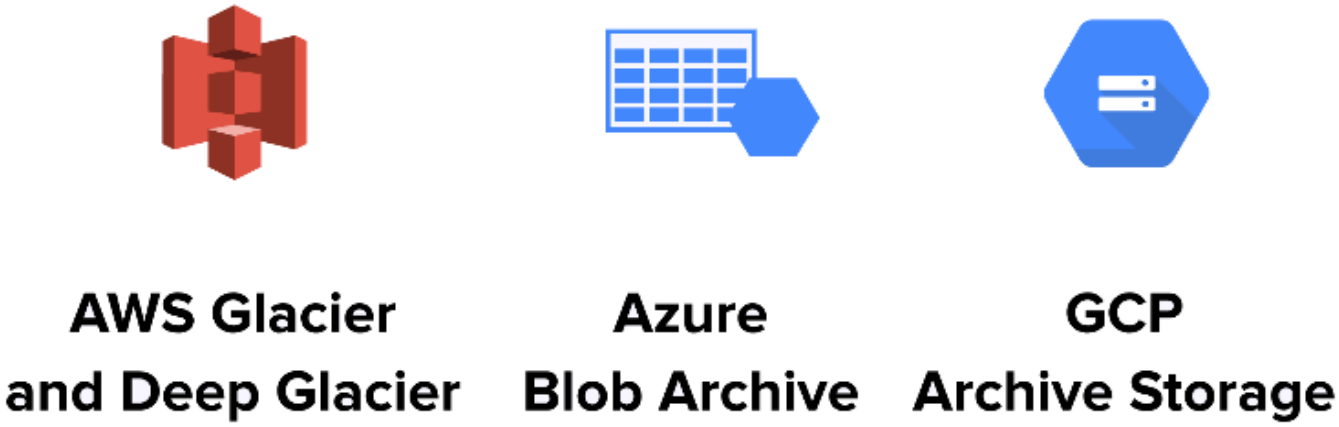
팬아웃 토폴로지 – SnapCenter Plug-in for VMware vSphere 을 통해 백업이 시작되면 로컬 스냅샷이 즉시 생성됩니다. 그런 다음 SCV는 가장 최근의 스냅샷을 Secondary ONTAP 클러스터에 복제하는 SnapMirror 작업을 시작합니다. BlueXP Backup and Recovery에서 정책은 클라우드 공급업체에서 선택한 개체 스토리지로 전송할 데이터의 스냅샷 복사본에 대한 소스로 기본 ONTAP 클러스터를 지정합니다.



계단식 토폴로지 – SCV를 사용하여 기본 및 보조 데이터 복사본을 만드는 것은 위에서 언급한 팬아웃 토폴로지와 동일합니다. 하지만 이번에는 백업이 보조 ONTAP 클러스터에서 시작되도록 지정하는 정책이 BlueXP Backup and Recovery에 생성됩니다.



BlueXP backup and recovery 사용하면 온프레미스 ONTAP 스냅샷의 백업 사본을 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 SCV와 BlueXP backup and recovery 에서 이 솔루션을 구성하고 백업 및 복원 작업을 실행하는 데 필요한 상위 수준의 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 머신에 대한 BlueXP 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. BlueXP 백업 및 복원을 사용하여 개체 스토리지에서 가상 머신을 복원합니다.

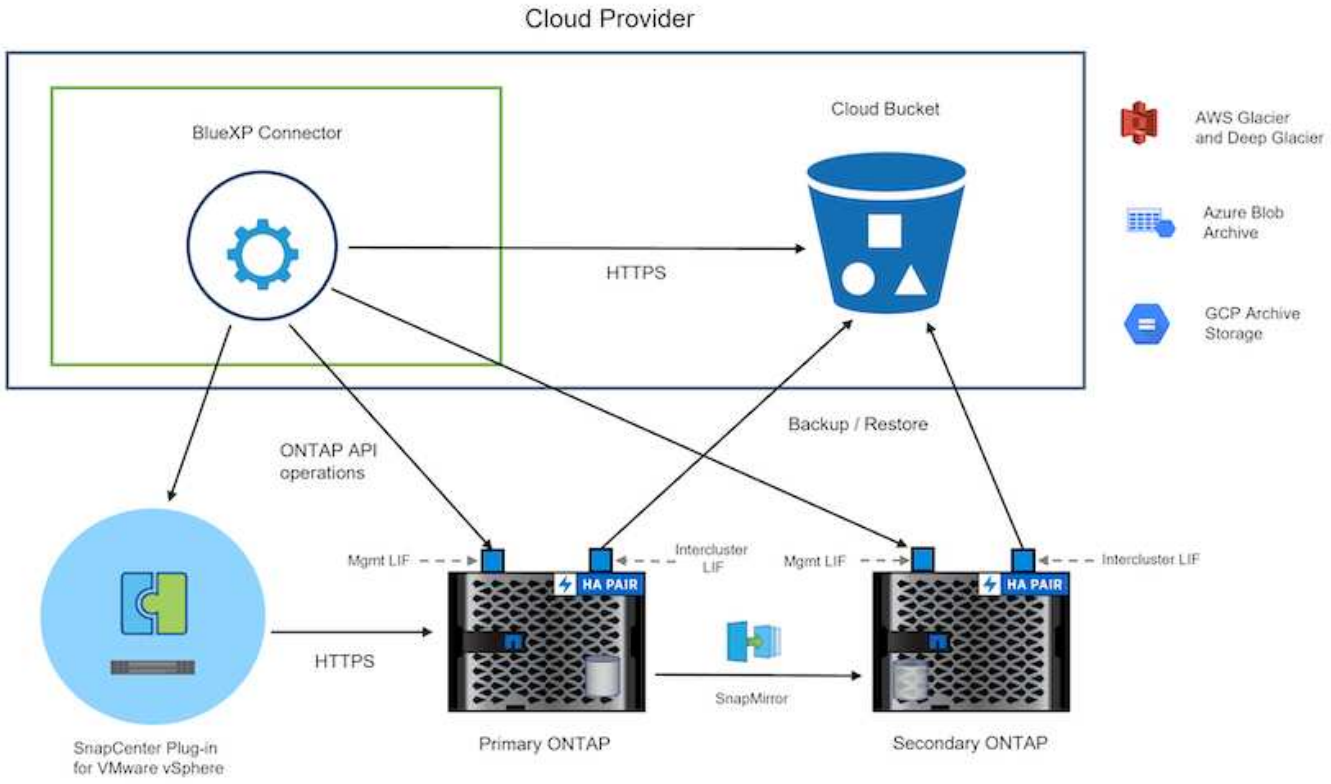
필수 조건

이 솔루션의 목적은 VMware vSphere, VCF VI 워크로드 도메인 또는 VCF 관리 도메인에서 실행되는 가상 머신의 데이터 보호를 시연하는 것입니다. 이 솔루션의 가상 머신은 NetApp ONTAP 에서 제공하는 NFS 데이터 저장소에 호스팅됩니다. 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. 클라우드 공급자를 위해 BlueXP 커넥터가 설치되었으며, 객체 스토리지 백업에 사용됩니다.
4. 백업할 가상 머신은 기본 ONTAP 스토리지 클러스터에 있는 NFS 데이터 저장소에 있습니다.
5. BlueXP 커넥터와 온프레미스 ONTAP 스토리지 클러스터 관리 인터페이스 간의 네트워크 연결.
6. BlueXP 커넥터와 온프레미스 SCV 어플라이언스 VM 간, 그리고 BlueXP 커넥터와 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

이 솔루션에서는 SnapCenter Plug-in for VMware vSphere 과 BlueXP backup and recovery 활용하여 온프레미스 데이터 센터에 있는 VMware vSphere 클러스터 내에서 Windows 및 Linux 가상 머신의 백업 및 복구를 수행하는 솔루션을 배포하고 검증하기 위한 자세한 지침을 제공합니다. 이 설정에서 가상 머신은 ONTAP A300 스토리지 클러스터에서 호스팅되는 NFS 데이터 저장소에 저장됩니다. 또한 별도의 ONTAP A300 스토리지 클러스터는 SnapMirror 사용하여 복제된 볼륨의 보조 대상 역할을 합니다. 또한 Amazon Web Services와 Azure Blob에 호스팅된 개체 스토리지가 세 번째 데이터 사본의 대상으로 사용되었습니다.

SCV가 관리하는 백업의 보조 사본에 대한 SnapMirror 관계를 생성하는 방법과 SCV와 BlueXP backup and recovery 에서 백업 작업을 구성하는 방법을 살펴보겠습니다.

SnapCenter Plug-in for VMware vSphere 에 대한 자세한 내용은 다음을 참조하세요. "SnapCenter Plug-in for VMware vSphere 설명서" .

BlueXP backup and recovery 에 대한 자세한 내용은 다음을 참조하세요. "BlueXP backup and recovery 문서" .

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 자동화된 BlueXP 에서 수행할 수 있으며, System Manager와 ONTAP CLI를 사용하여 수행할 수도 있습니다. 이러한 모든 방법에 대해서는 아래에서 논의합니다.

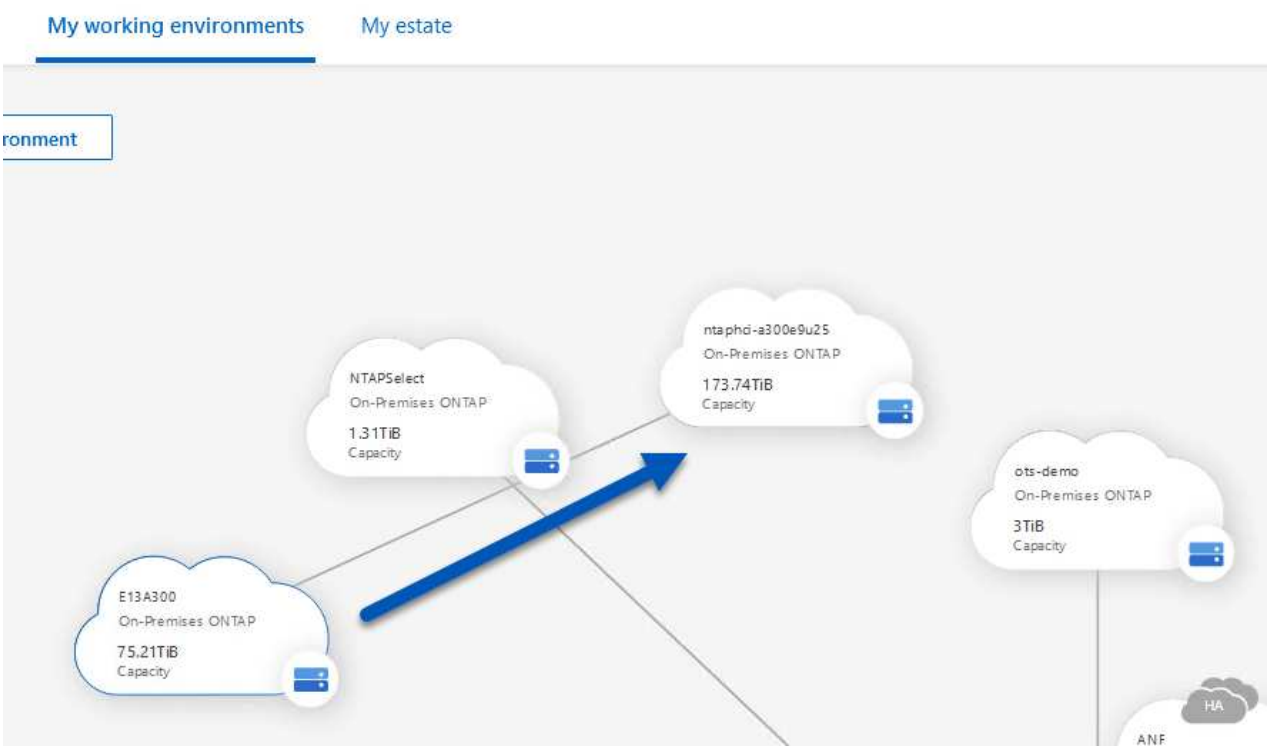
BlueXP 와 **SnapMirror** 관계 구축

다음 단계는 BlueXP 웹 콘솔에서 완료해야 합니다.

1차 및 **2**차 **ONTAP** 스토리지 시스템에 대한 복제 설정

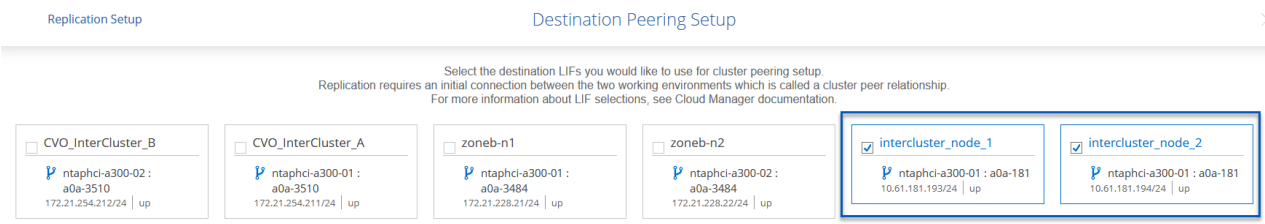
먼저 BlueXP 웹 콘솔에 로그인하고 Canvas로 이동합니다.

1. 소스(기본) ONTAP 스토리지 시스템을 대상(보조) ONTAP 스토리지 시스템으로 끌어서 놓습니다.

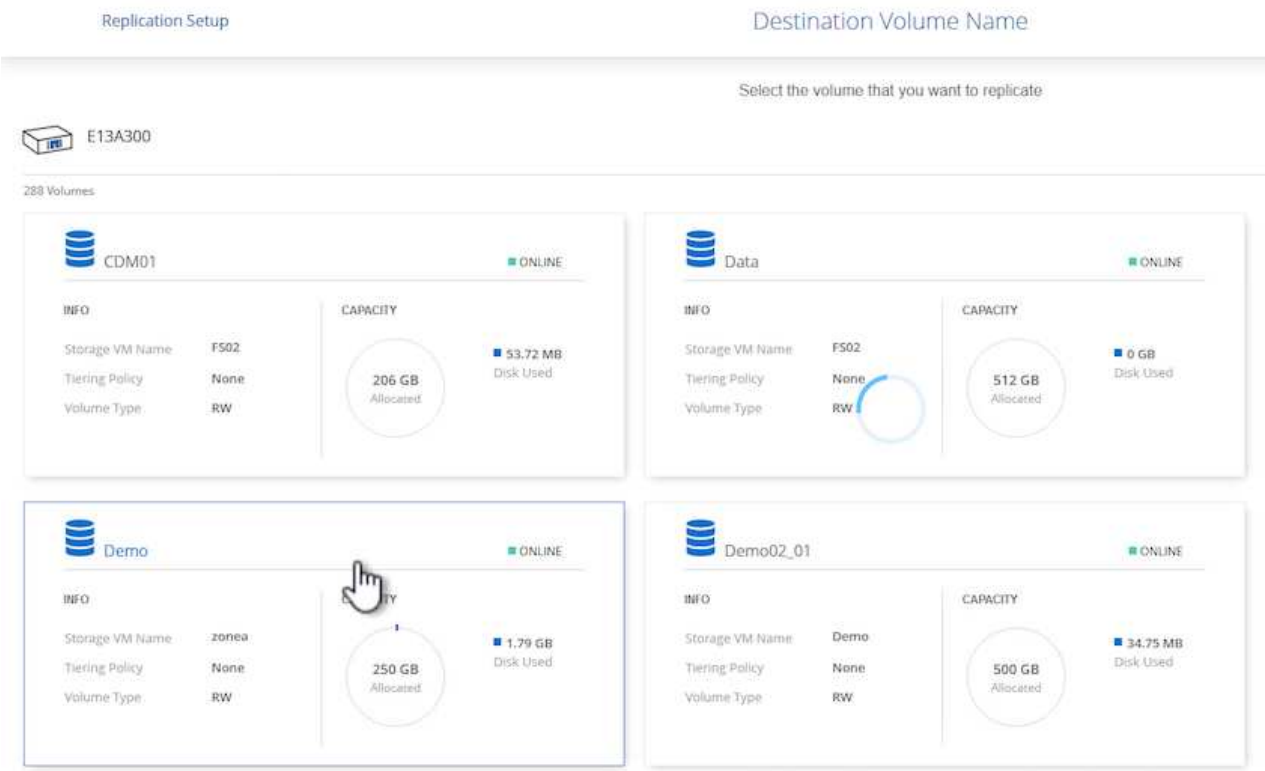


2. 나타나는 메뉴에서 *복제*를 선택합니다.

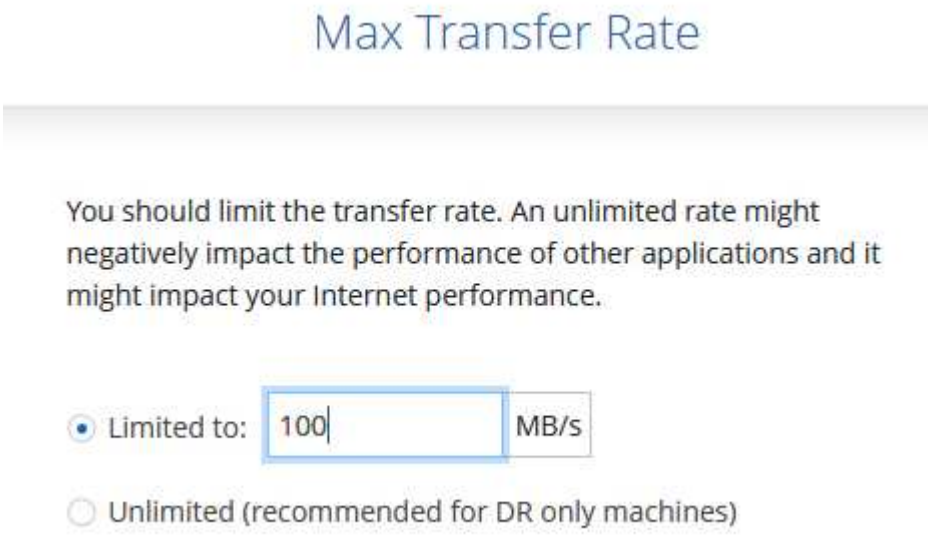
3. 대상 피어링 설정 페이지에서 스토리지 시스템 간 연결에 사용할 대상 Intercluster LIF를 선택합니다.



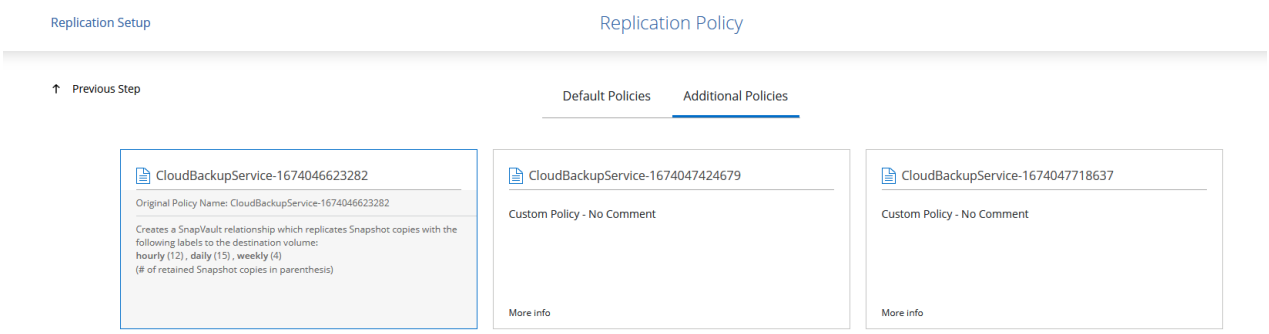
4. 대상 볼륨 이름 페이지에서 먼저 소스 볼륨을 선택한 다음 대상 볼륨 이름을 입력하고 대상 SVM과 집계를 선택합니다. 계속하려면 *다음*을 클릭하세요.



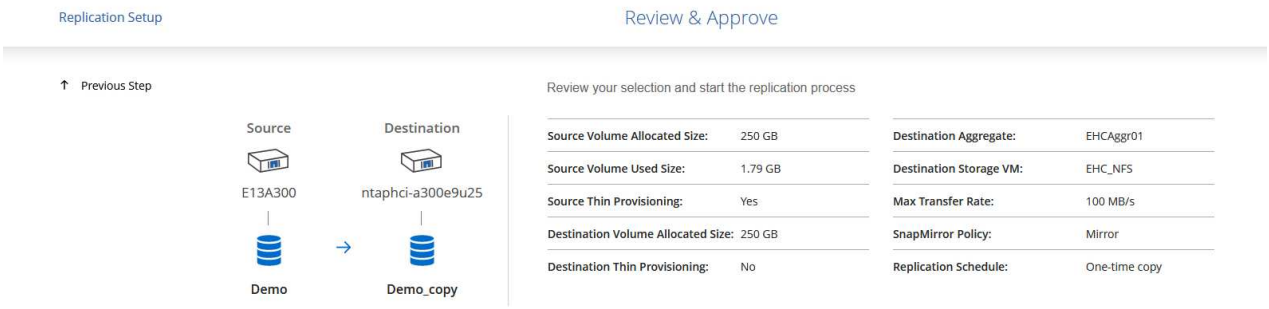
5. 복제가 발생할 최대 전송 속도를 선택합니다.



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.



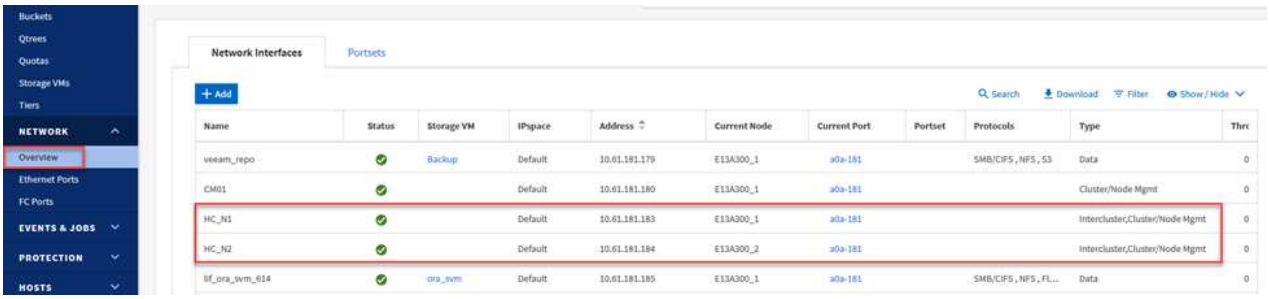
System Manager 및 **ONTAP CLI**를 사용하여 **SnapMirror** 관계 설정

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
```

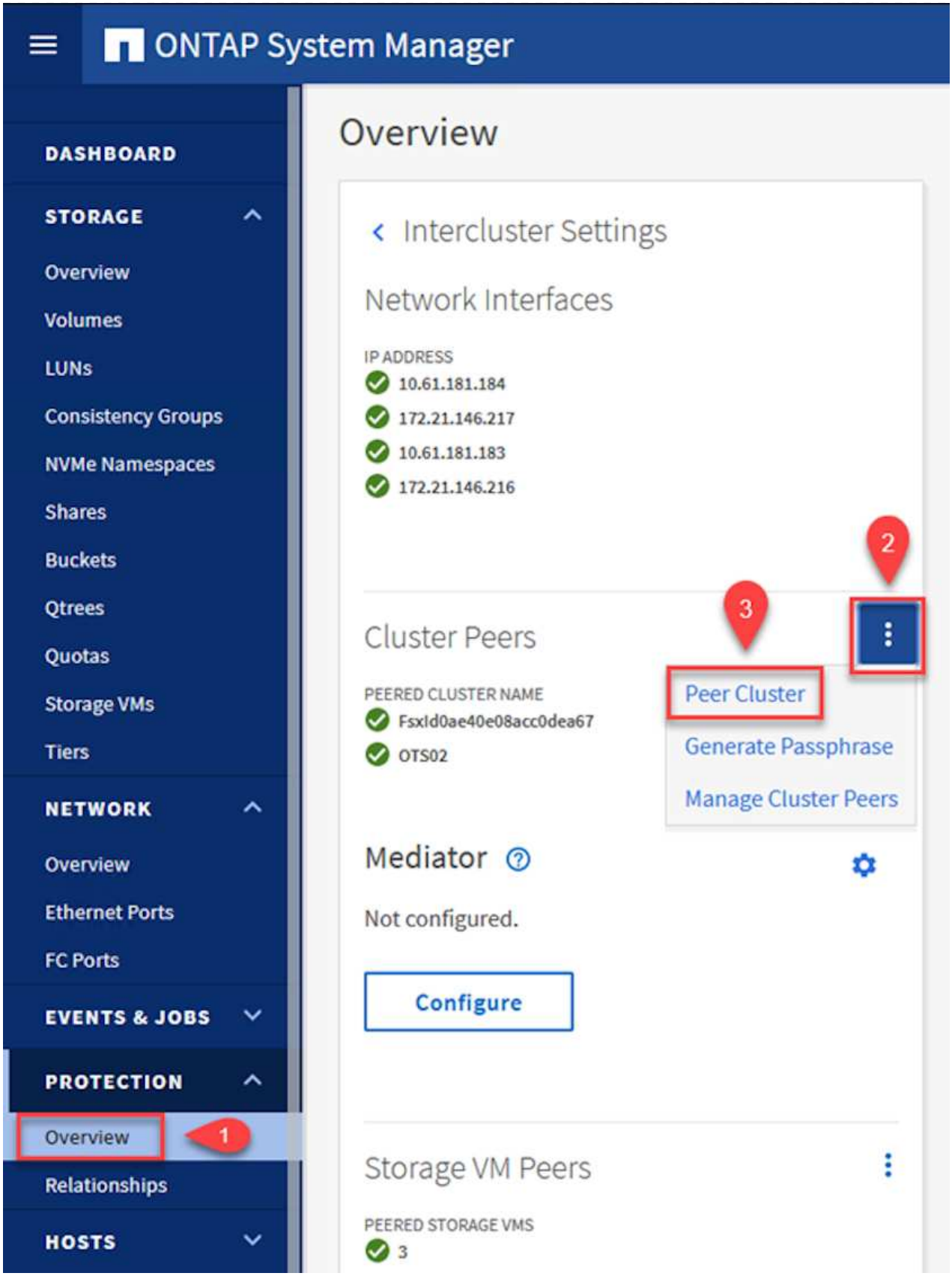
ONTAP 클러스터 간 클러스터 피어링 설정

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:
```

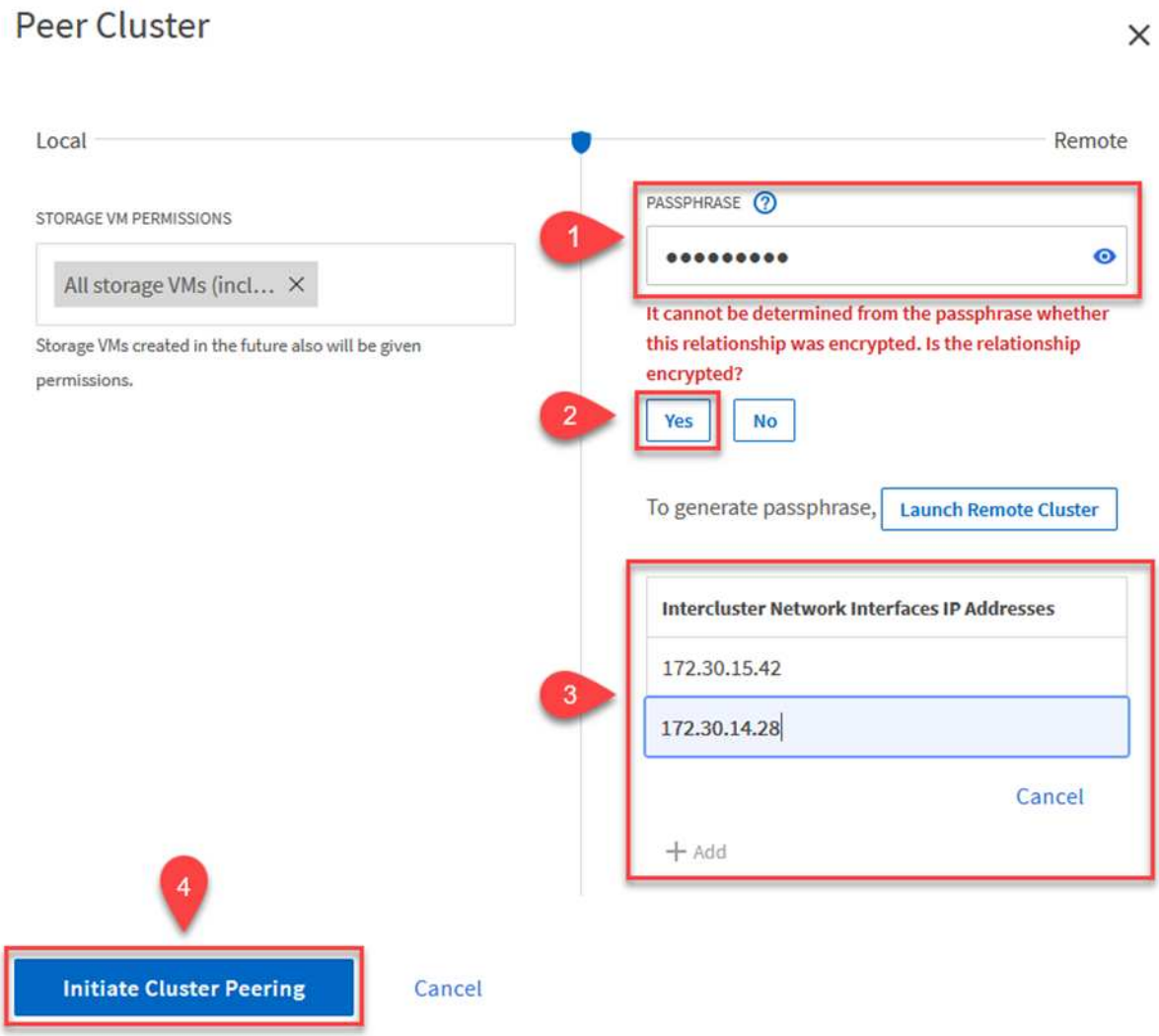
2. 소스 클러스터에서 ONTAP 시스템 관리자나 CLI를 사용하여 클러스터 피어 관계를 설정할 수 있습니다. ONTAP 시스템 관리자에서 보호 > 개요로 이동하여 피어 클러스터를 선택합니다.



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
```

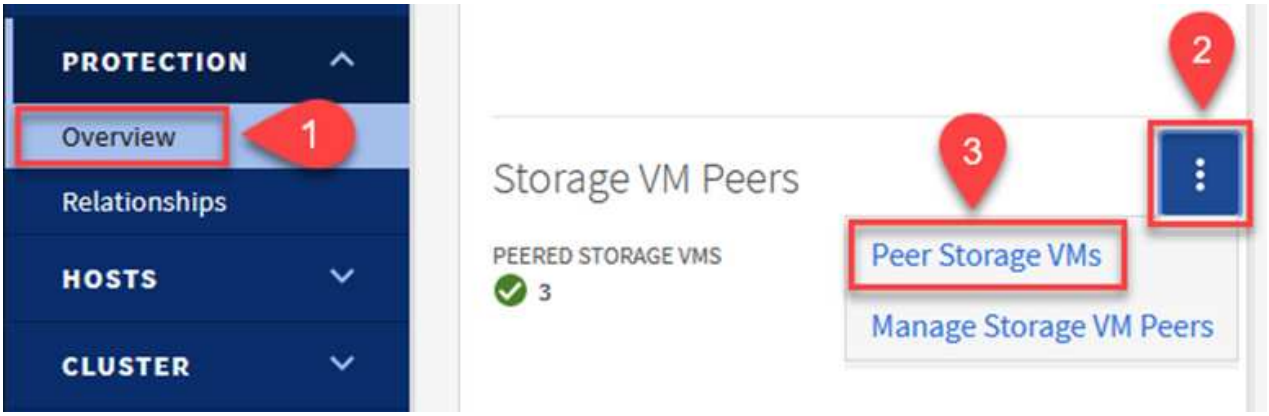
SVM 피어링 관계 설정

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

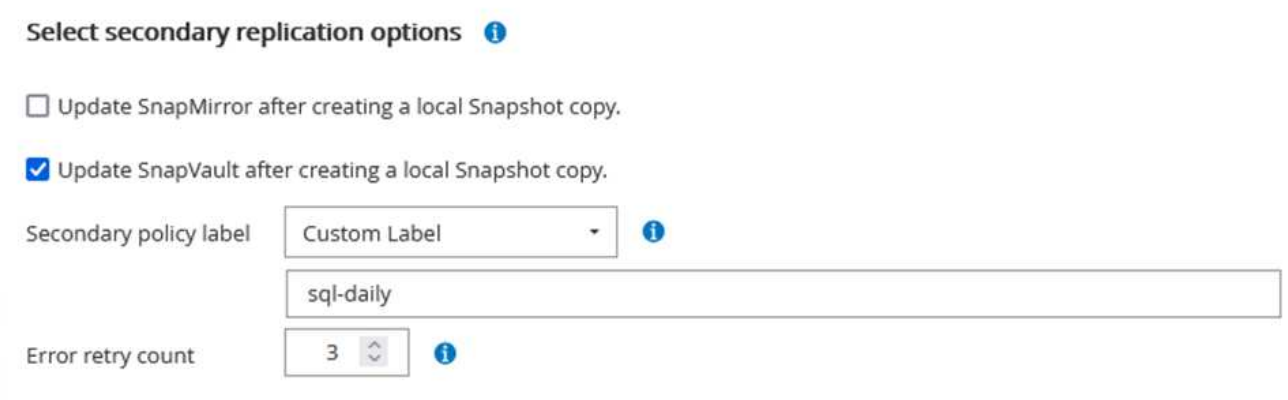
5. SVM 피어링 프로세스를 완료하려면 Peer Storage VMs를 클릭하세요.

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.

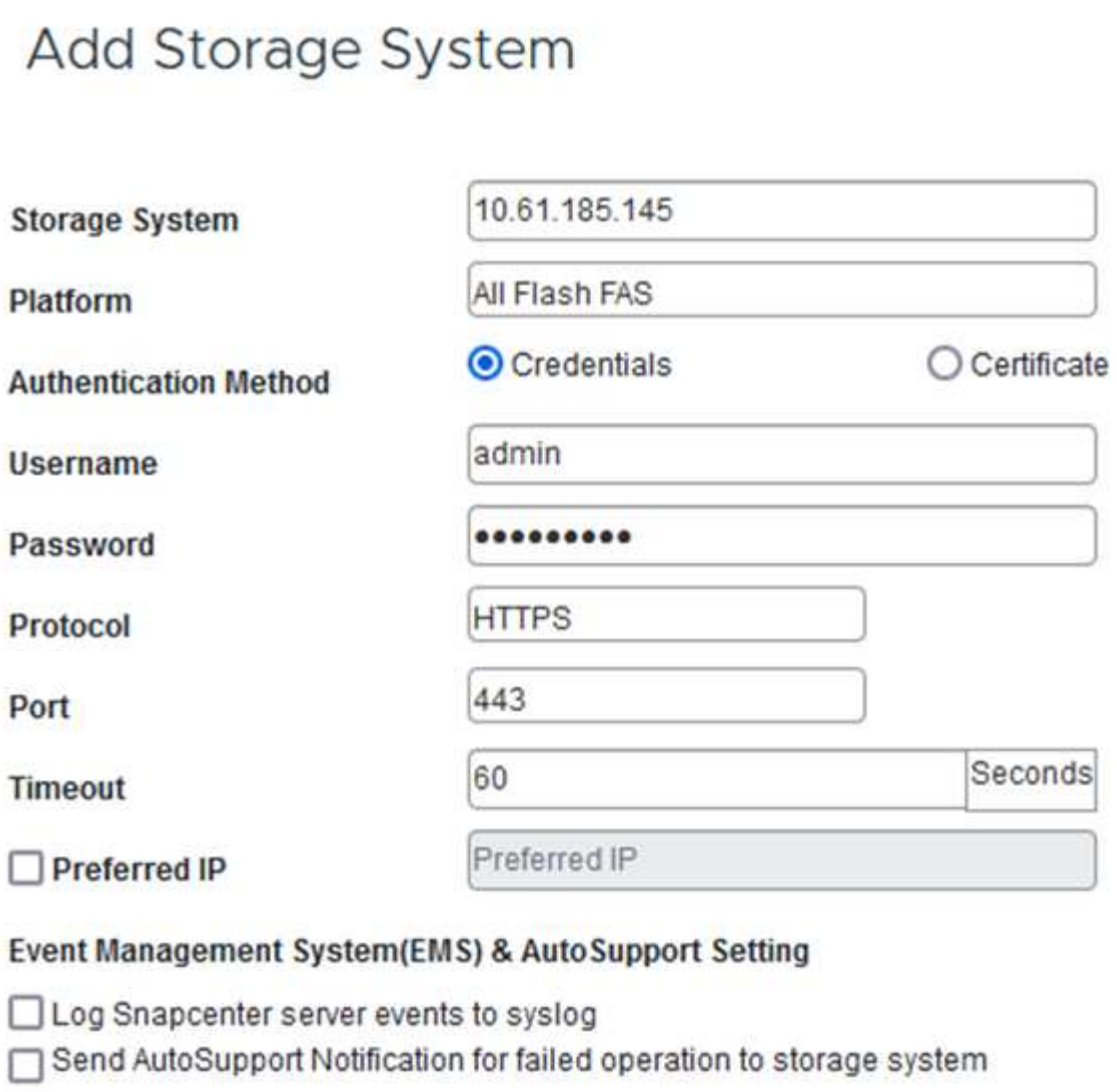
가상 머신과 데이터 저장소의 백업을 구성하려면 플러그인 인터페이스에서 다음 단계를 완료해야 합니다.

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.



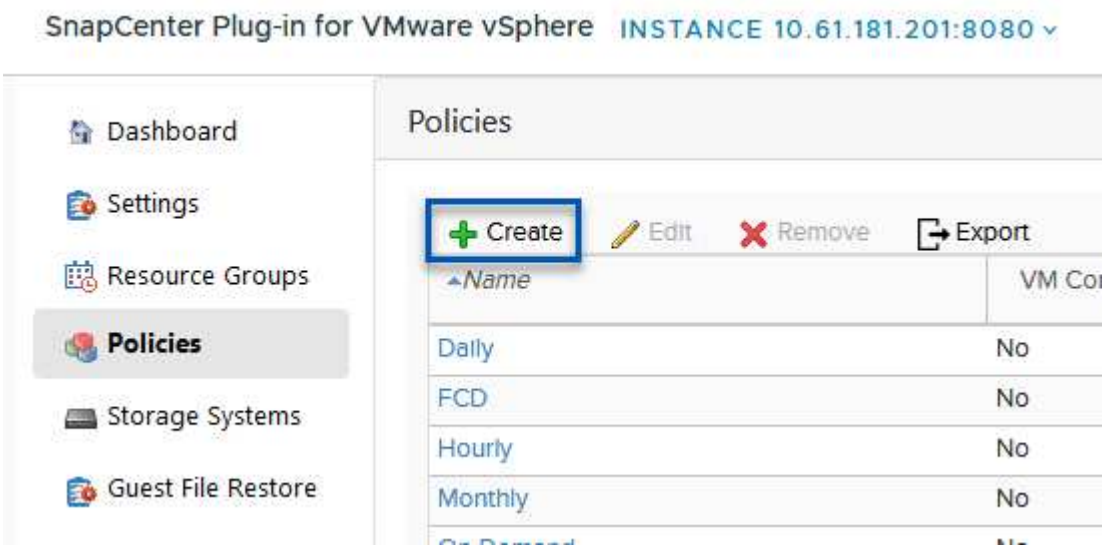
3. 보조 ONTAP 스토리지 시스템에 대해서도 이 절차를 반복합니다.

정책은 SCV가 관리하는 백업에 대한 보존 기간, 빈도 및 복제 옵션을 지정합니다.

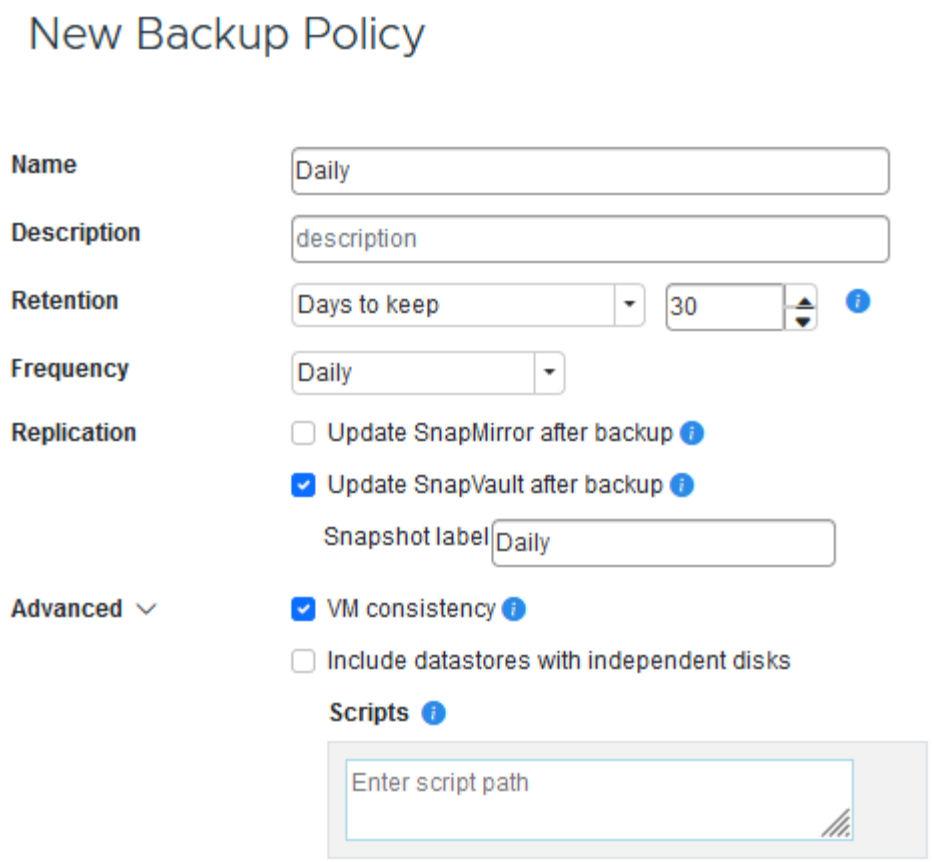
검토하다 "VM 및 데이터 저장소에 대한 백업 정책 생성" 자세한 내용은 설명서 섹션을 참조하세요.

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 클러스터에 복제된 SnapVault 복사본에 대해 특정 보존 기간이 있는 정책을 시행하는 데 사용할 수 있다는 점에서 유용합니다. SCV를 BlueXP 백업 및 복원과 함께 사용하는 경우 스냅샷 레이블 필드는 비어 있어야 하거나 BlueXP 백업 정책에 지정된 레이블과 [밑줄]#일치#해야 합니다.

3. 필요한 각 정책에 대해 이 절차를 반복합니다. 예를 들어, 일일, 주간, 월간 백업에 대해 별도의 정책을 적용합니다.

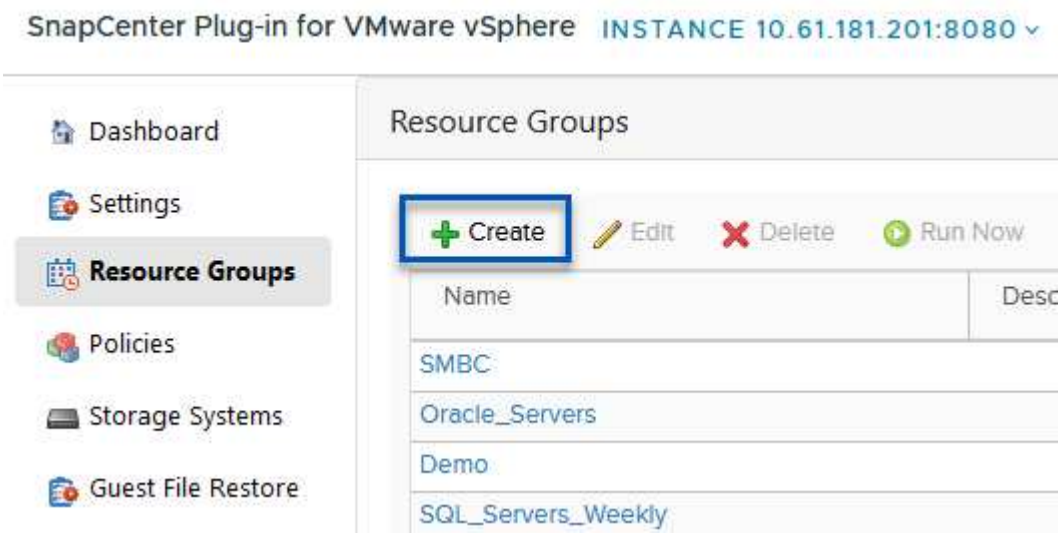
리소스 그룹 생성

리소스 그룹에는 백업 작업에 포함될 데이터 저장소와 가상 머신, 관련 정책 및 백업 일정이 포함되어 있습니다.

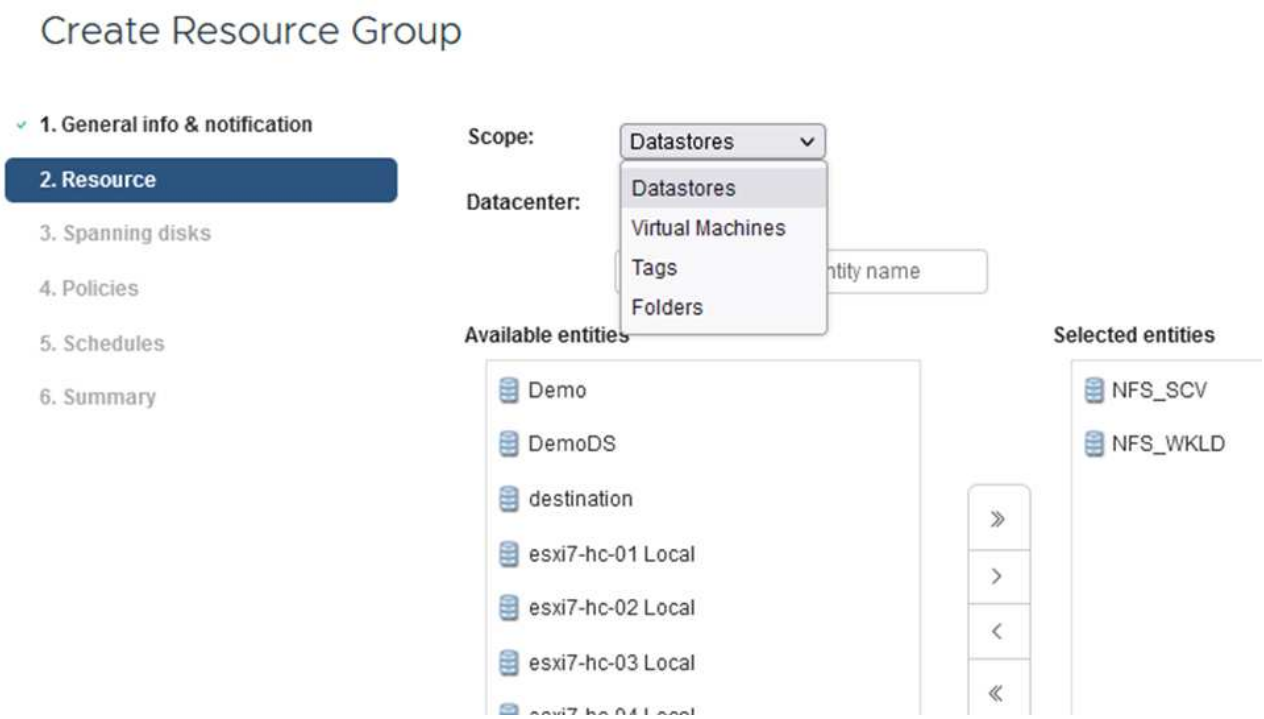
검토하다 "리소스 그룹 생성" 자세한 내용은 설명서 섹션을 참조하세요.

리소스 그룹을 만들려면 다음 단계를 완료하세요.

1. SnapCenter Plug-in for VMware vSphere 에서 왼쪽 메뉴의 리소스 그룹*으로 이동하여 *만들기 버튼을 클릭합니다.

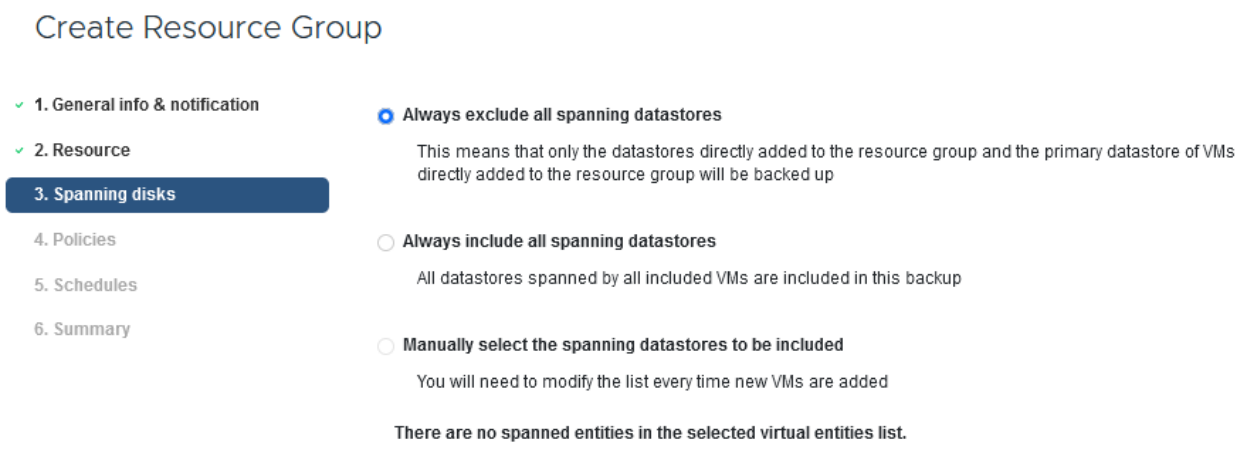


2. 리소스 그룹 만들기 마법사에서 그룹의 이름과 설명을 입력하고, 알림을 받는 데 필요한 정보도 입력합니다. *다음*을 클릭하세요
3. 다음 페이지에서 백업 작업에 포함할 데이터 저장소와 가상 머신을 선택한 후 *다음*을 클릭합니다.



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.

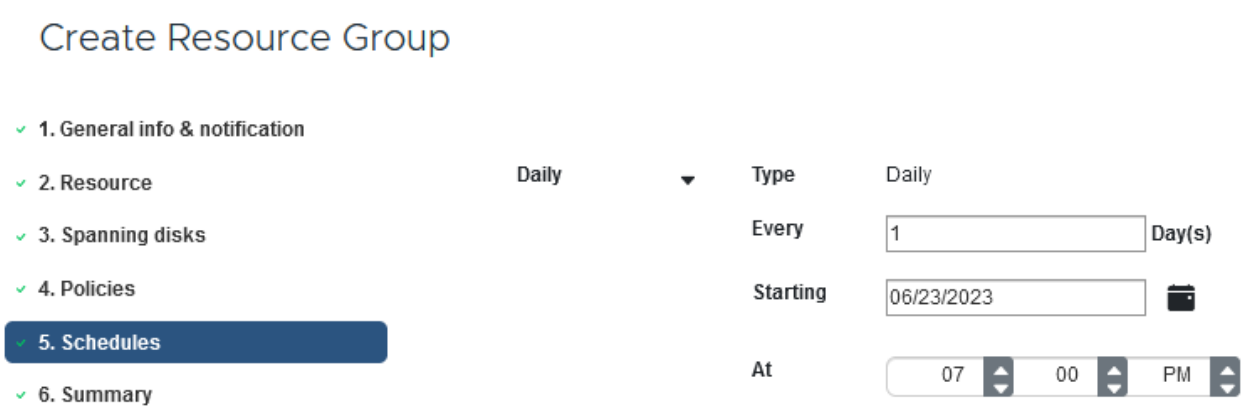


BlueXP backup and recovery 현재 여러 데이터 저장소에 걸쳐 있는 VMDK를 사용한 VM 백업을 지원하지 않습니다.

5. 다음 페이지에서 리소스 그룹과 연관될 정책을 선택하고 *다음*을 클릭합니다.

BlueXP backup and recovery 사용하여 SCV 관리 스냅샷을 개체 스토리지에 백업하는 경우 각 리소스 그룹은 단일 정책에만 연결될 수 있습니다.

6. 백업이 실행될 시간을 결정하는 일정을 선택하세요. *다음*을 클릭하세요.

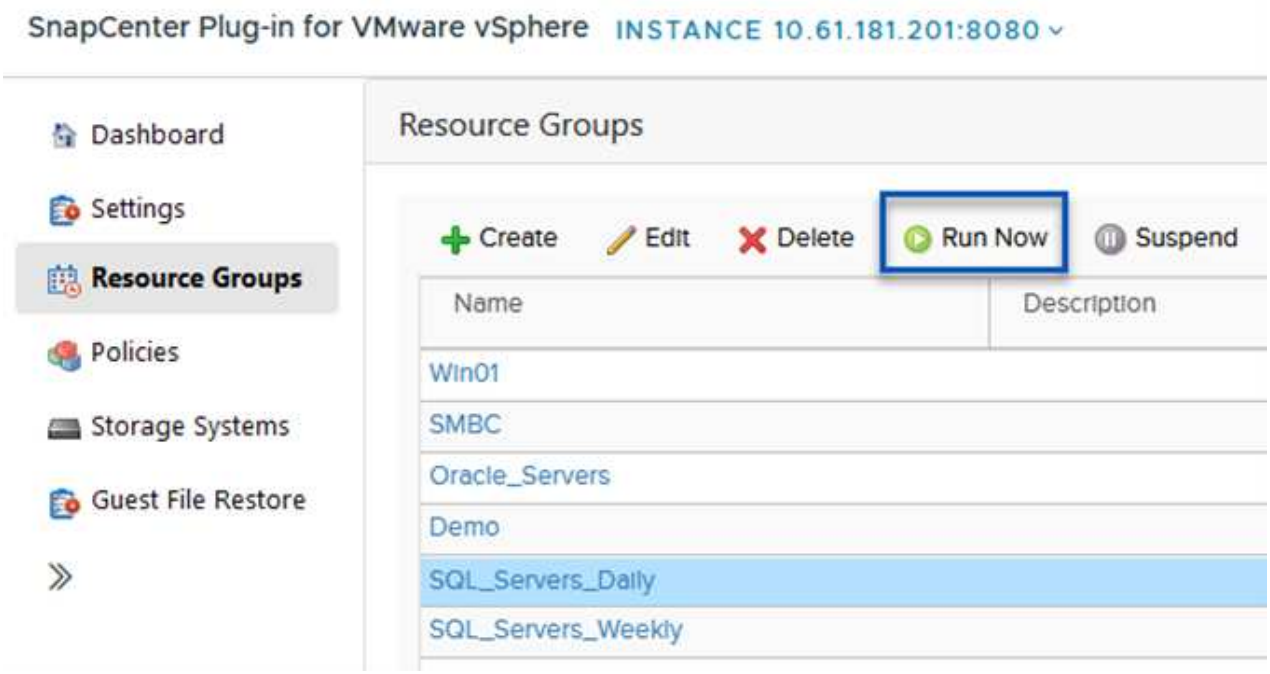


7. 마지막으로 요약 페이지를 검토한 후 *마침*을 클릭하여 리소스 그룹 생성을 완료합니다.

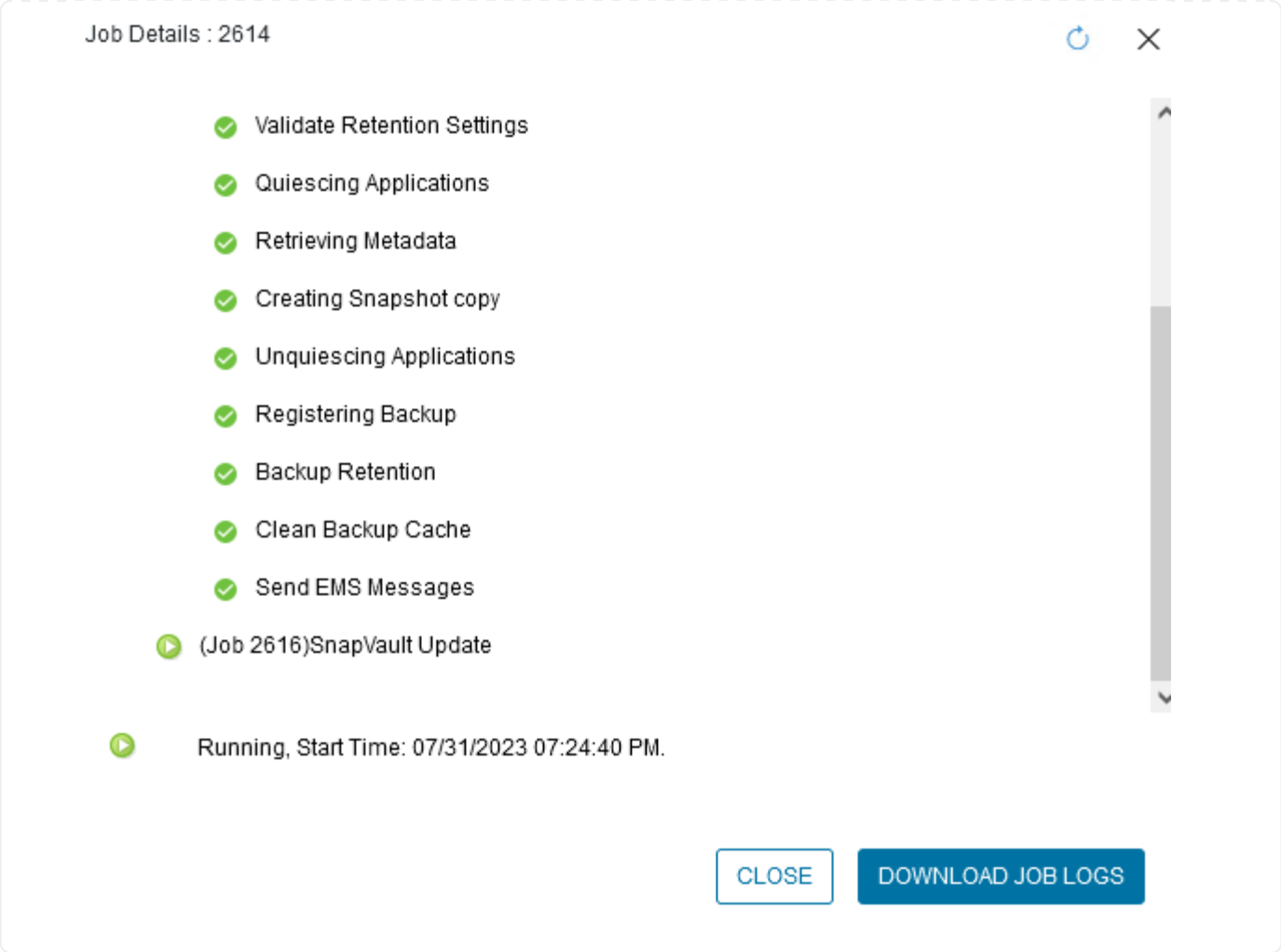
백업 작업 실행

마지막 단계에서는 백업 작업을 실행하고 진행 상황을 모니터링합니다. BlueXP backup and recovery 에서 리소스를 검색하려면 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.



BlueXP backup and recovery 에서 개체 스토리지에 대한 백업 구성

BlueXP 가 데이터 인프라를 효과적으로 관리하려면 먼저 커넥터를 설치해야 합니다. 커넥터는 리소스 검색 및 데이터 작업 관리에 관련된 작업을 실행합니다.

BlueXP 커넥터에 대한 자세한 내용은 다음을 참조하세요. "커넥터에 대해 알아보기" BlueXP 문서에서.

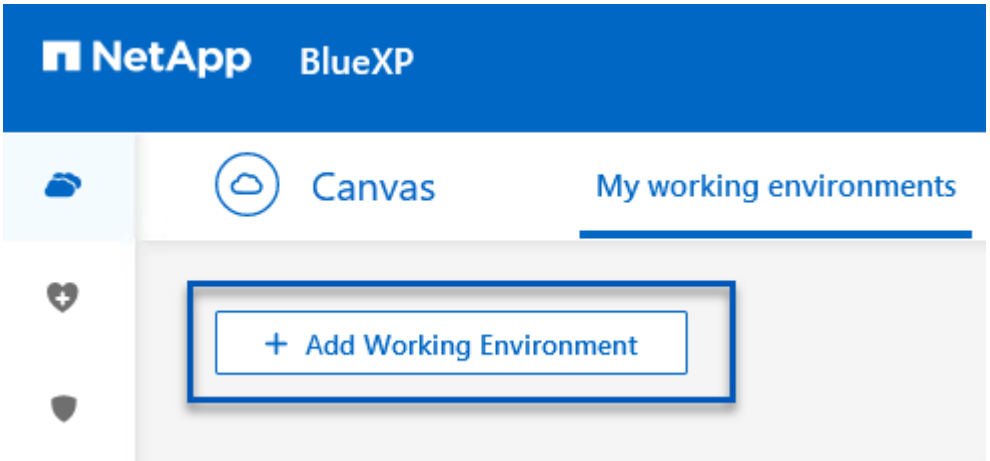
사용 중인 클라우드 공급자에 대한 커넥터가 설치되면 Canvas에서 개체 스토리지의 그래픽 표현을 볼 수 있습니다.

SCV 온프레미스에서 관리하는 데이터를 백업하도록 BlueXP backup and recovery 구성하려면 다음 단계를 완료하세요.

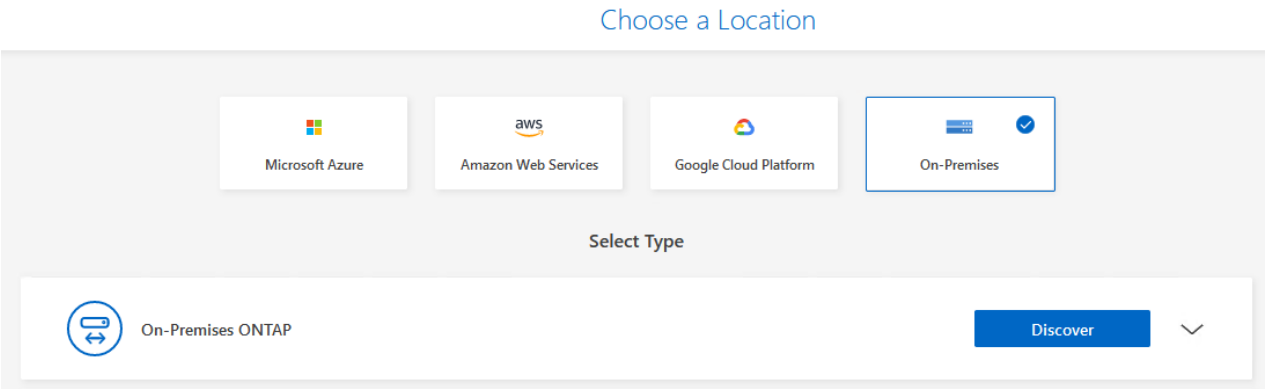
Canvas에 작업 환경 추가

첫 번째 단계는 BlueXP 에 온프레미스 ONTAP 스토리지 시스템을 추가하는 것입니다.

1. 캔버스에서 *작업 환경 추가*를 선택하여 시작하세요.



2. 위치 선택에서 사내*를 선택한 다음 *검색 버튼을 클릭합니다.



3. ONTAP 스토리지 시스템의 자격 증명을 입력하고 검색 버튼을 클릭하여 작업 환경을 추가합니다.

ONTAP Cluster IP

10.61.181.180

User Name

admin

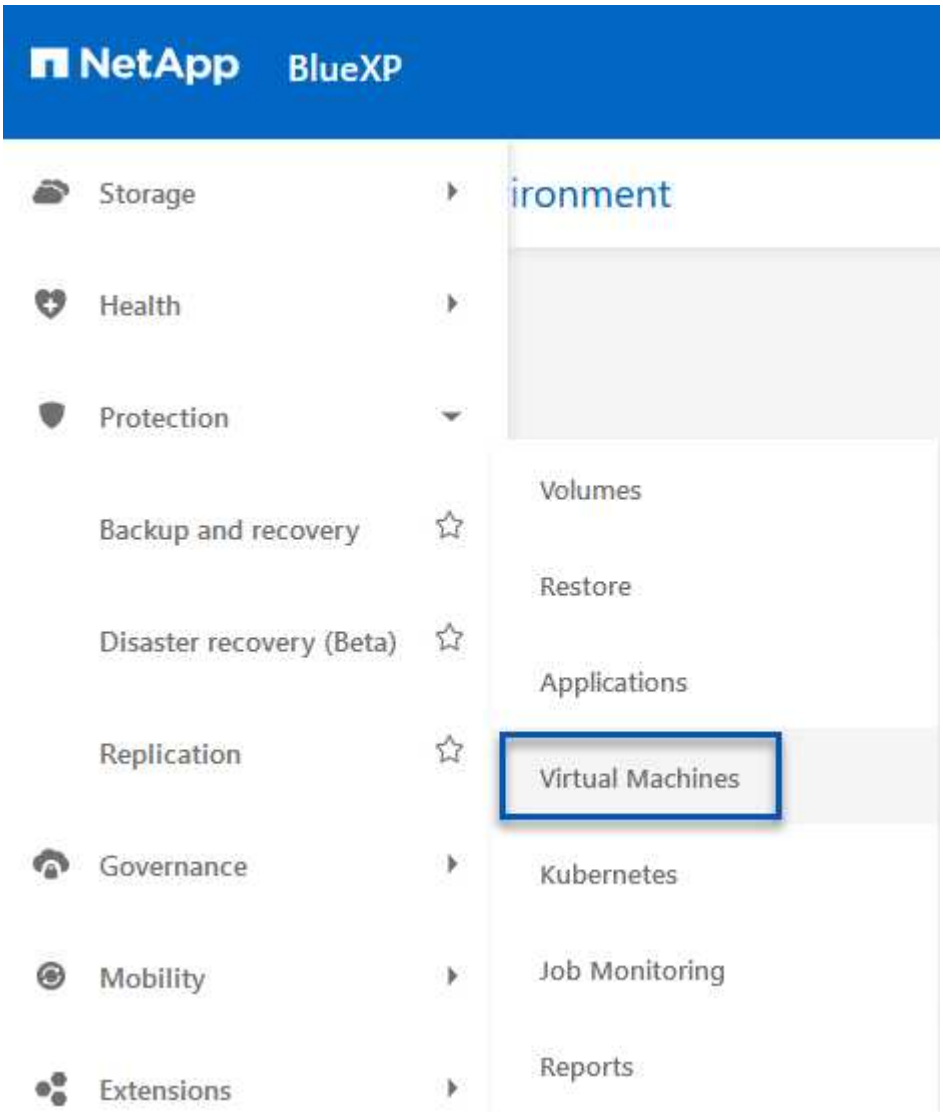
Password

••••••••••

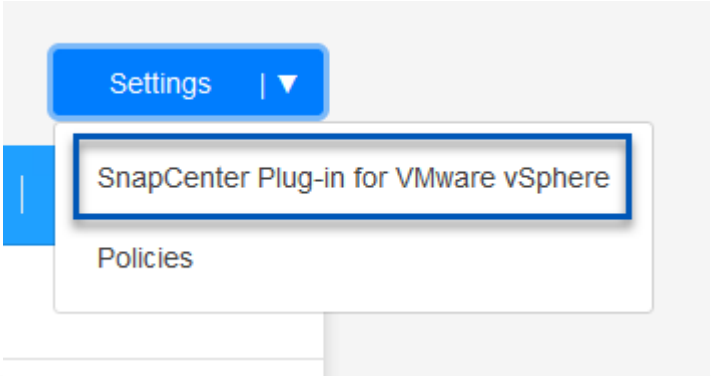
온프레미스 **SCV** 어플라이언스 및 **vCenter**를 검색하세요

온프레미스 데이터스토어와 가상 머신 리소스를 검색하려면 SCV 데이터 브로커에 대한 정보와 vCenter 관리 어플라이언스에 대한 자격 증명을 추가합니다.

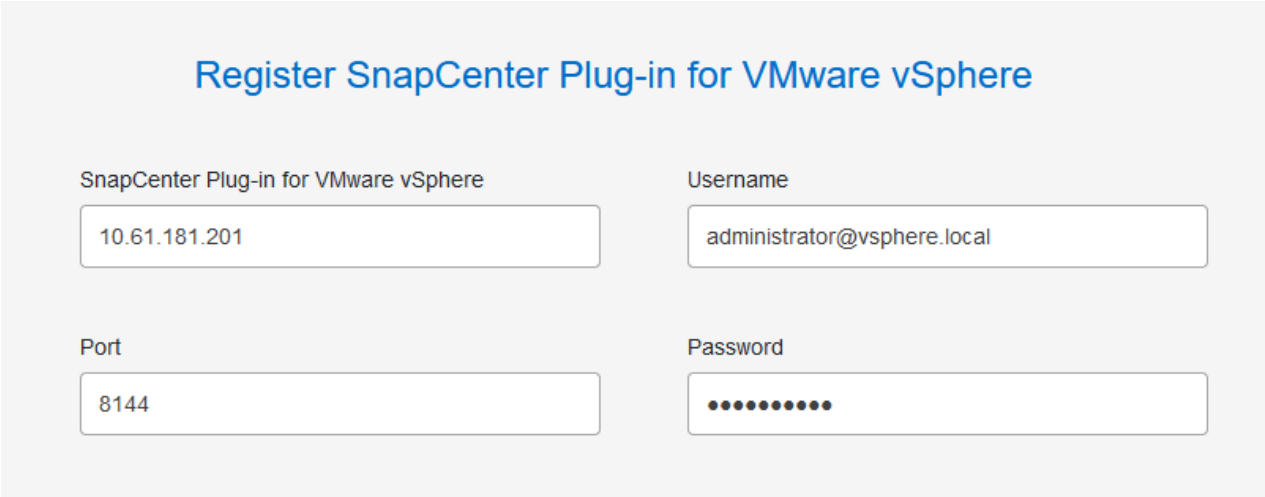
1. BlueXP 왼쪽 메뉴 선택에서 보호 **>** 백업 및 복구 **>** 가상 머신



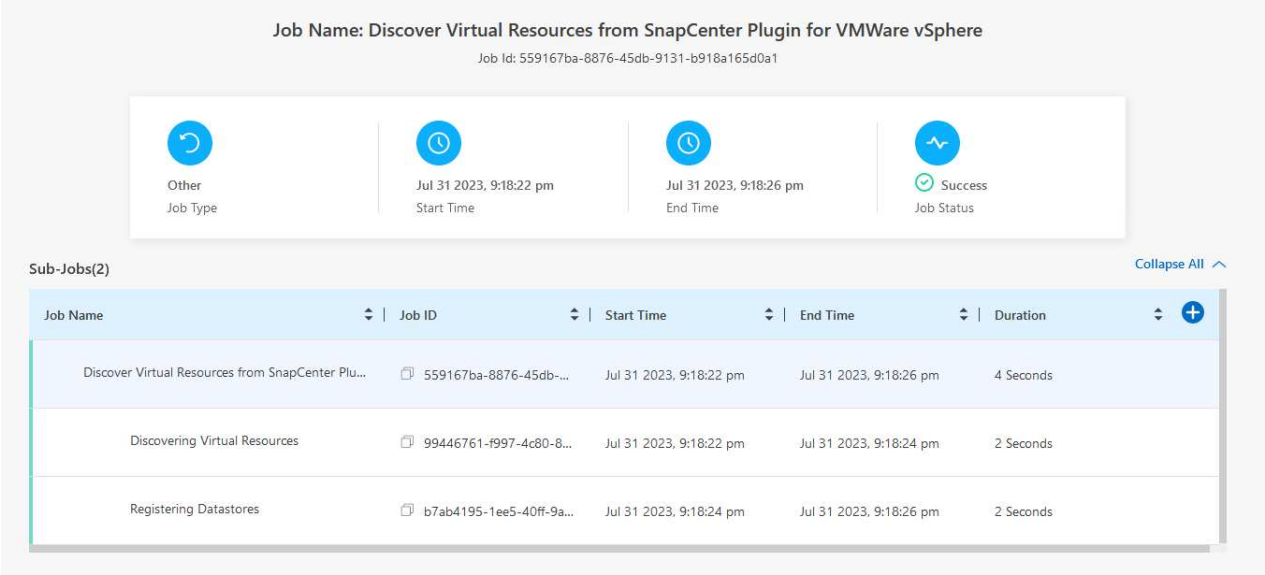
2. 가상 머신 메인 화면에서 설정 드롭다운 메뉴에 액세스하고 * SnapCenter Plug-in for VMware vSphere*을 선택합니다.



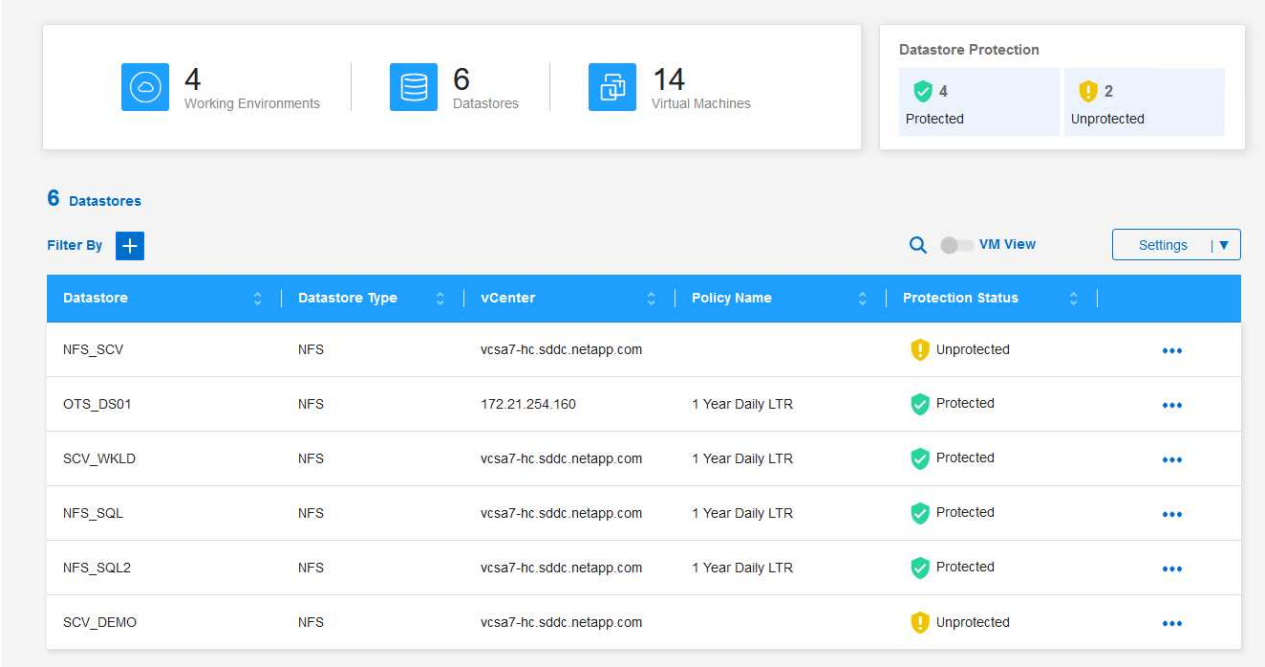
3. 등록 버튼을 클릭한 다음 SnapCenter 플러그인 어플라이언스의 IP 주소와 포트 번호, vCenter 관리 어플라이언스의 사용자 이름과 비밀번호를 입력합니다. 등록 버튼을 클릭하여 검색 과정을 시작하세요.



4. 작업 모니터링 탭에서 작업 진행 상황을 모니터링할 수 있습니다.



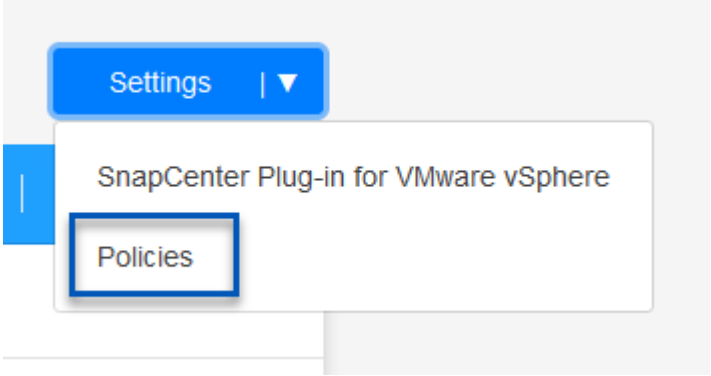
5. 검색이 완료되면 검색된 모든 SCV 어플라이언스의 데이터 저장소와 가상 머신을 볼 수 있습니다.


4
Working Environments
6
Datastores
14
Virtual Machines
Datastore Protection
4
Protected
2
Unprotected
6 Datastores
Filter By
VM View
Settings
Datastore
Datastore Type
vCenter
Policy Name
Protection Status
NFS_SCV NFS vcsa7-hc.sddc.netapp.com Unprotected
OTS_DS01 NFS 172.21.254.160 1 Year Daily LTR Protected
SCV_WKLD NFS vcsa7-hc.sddc.netapp.com 1 Year Daily LTR Protected
NFS_SQL NFS vcsa7-hc.sddc.netapp.com 1 Year Daily LTR Protected
NFS_SQL2 NFS vcsa7-hc.sddc.netapp.com 1 Year Daily LTR Protected
SCV_DEMO NFS vcsa7-hc.sddc.netapp.com Unprotected

가상 머신을 위한 BlueXP backup and recovery 에서 보존 기간, 백업 소스 및 보관 정책을 지정하는 정책을 만듭니다.

정책 생성에 대한 자세한 내용은 다음을 참조하세요. "데이터 저장소를 백업하기 위한 정책 생성" .

1. 가상 머신용 BlueXP backup and recovery 메인 페이지에서 설정 드롭다운 메뉴에 액세스하여 *정책*을 선택합니다.



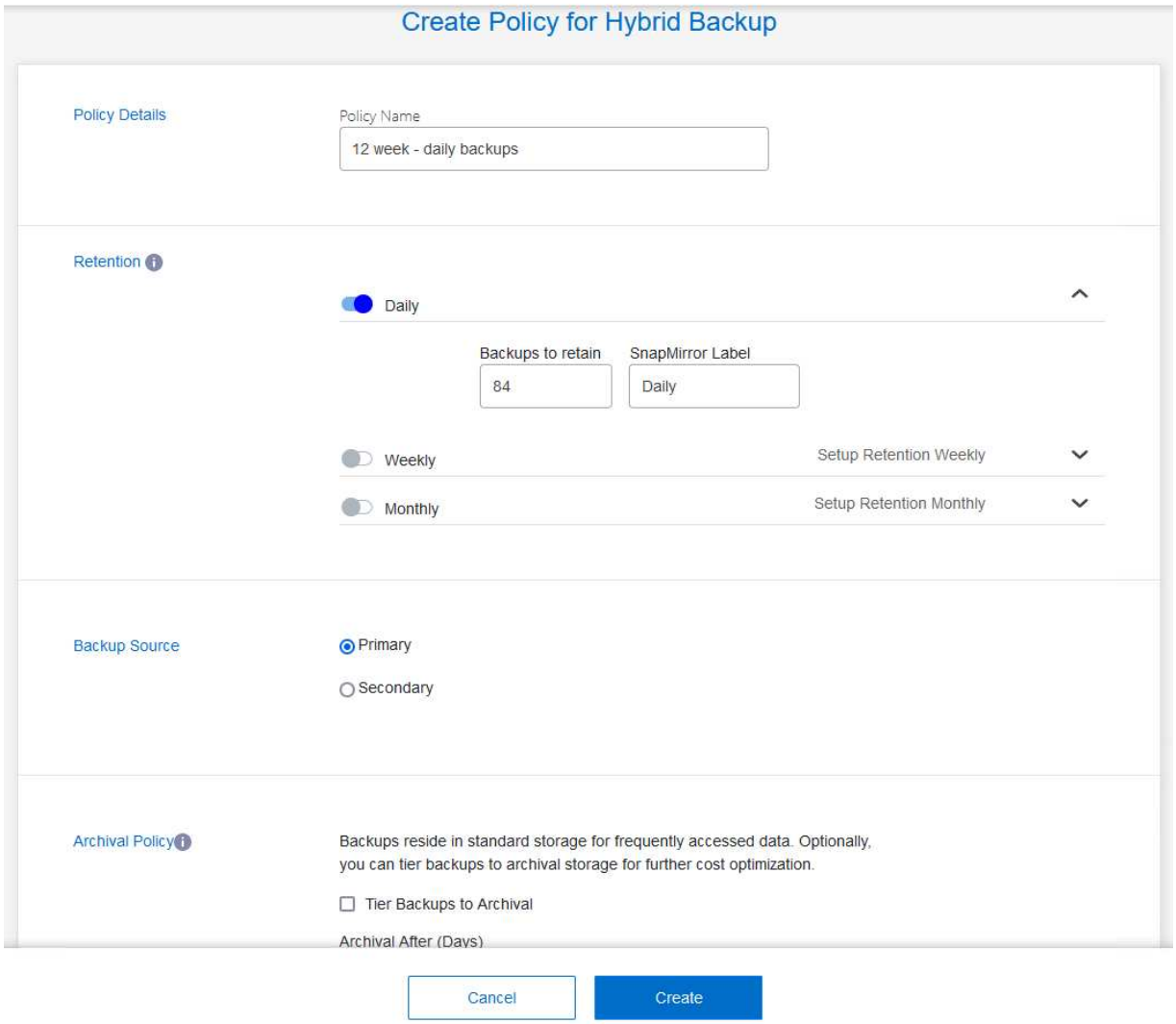
2. 정책 만들기*를 클릭하여 *하이브리드 백업 정책 만들기 창에 액세스합니다.

   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.

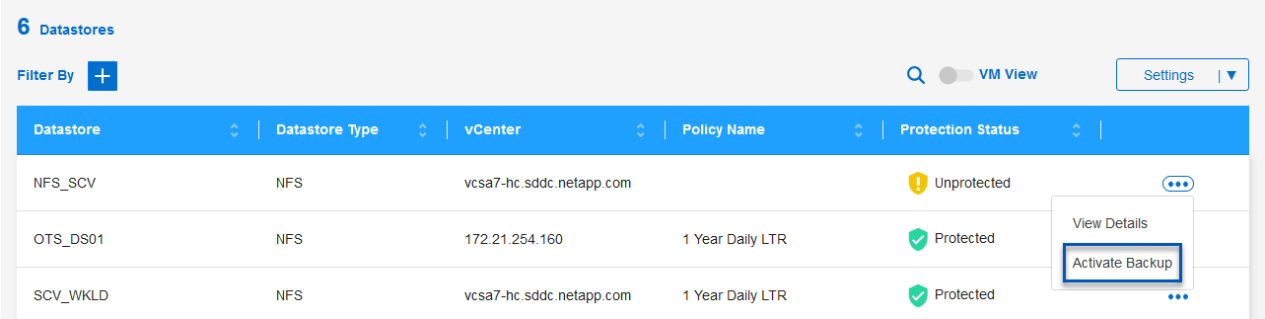
3. *만들기*를 클릭하여 정책 생성을 완료하세요.

Amazon Web Services에 데이터 저장소 백업

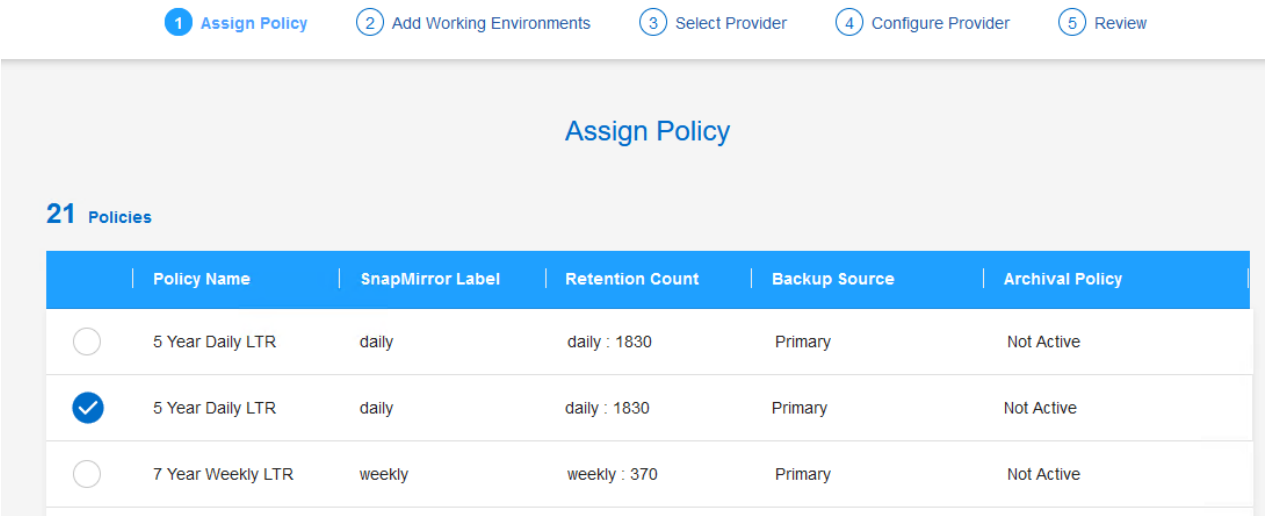
마지막 단계는 개별 데이터 저장소와 가상 머신에 대한 데이터 보호를 활성화하는 것입니다. 다음 단계에서는 AWS에 대한 백업을 활성화하는 방법을 설명합니다.

자세한 내용은 다음을 참조하세요. "Amazon Web Services에 데이터 저장소 백업" .

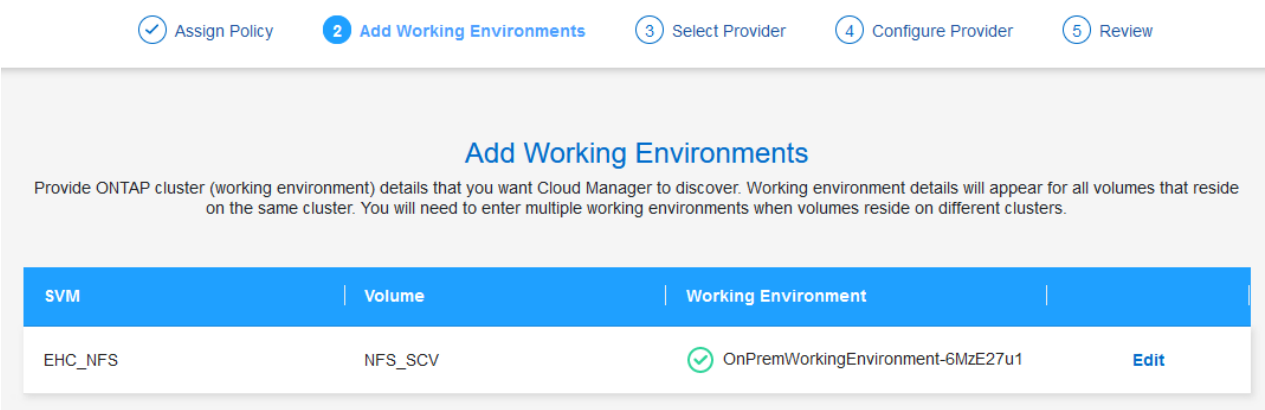
1. 가상 머신을 위한 BlueXP backup and recovery 메인 페이지에서 백업할 데이터 저장소의 설정 드롭다운에 액세스하여 *백업 활성화*를 선택합니다.



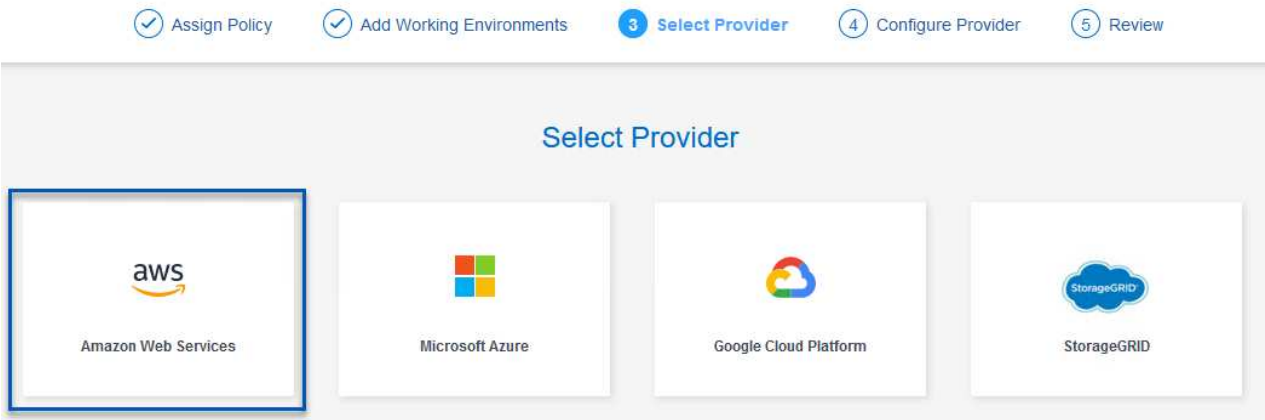
2. 데이터 보호 작업에 사용할 정책을 할당하고 *다음*을 클릭합니다.



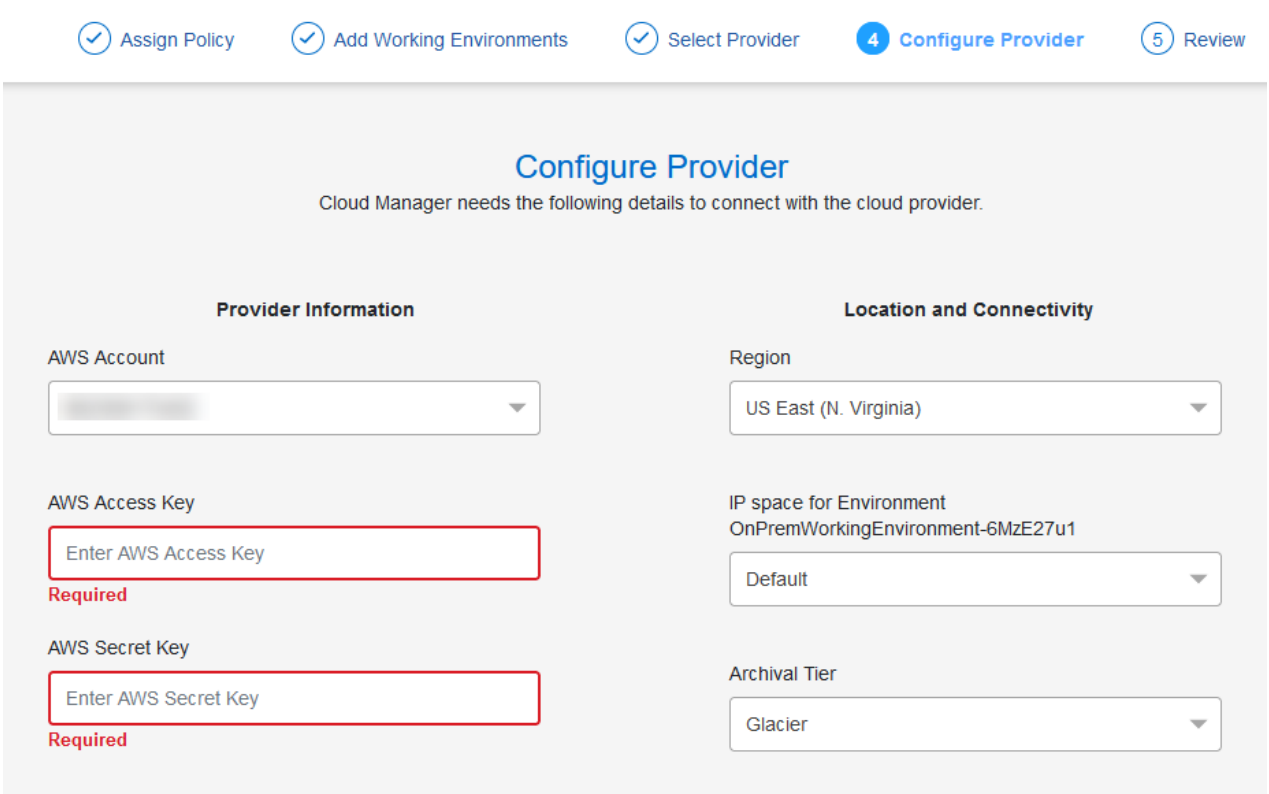
3. 작업 환경 추가 페이지에는 작업 환경이 이전에 검색된 경우 체크 표시가 있는 데이터 저장소와 작업 환경이 나타나야 합니다. 작업 환경을 이전에 발견하지 못한 경우 여기에 추가할 수 있습니다. 계속하려면 *다음*을 클릭하세요.



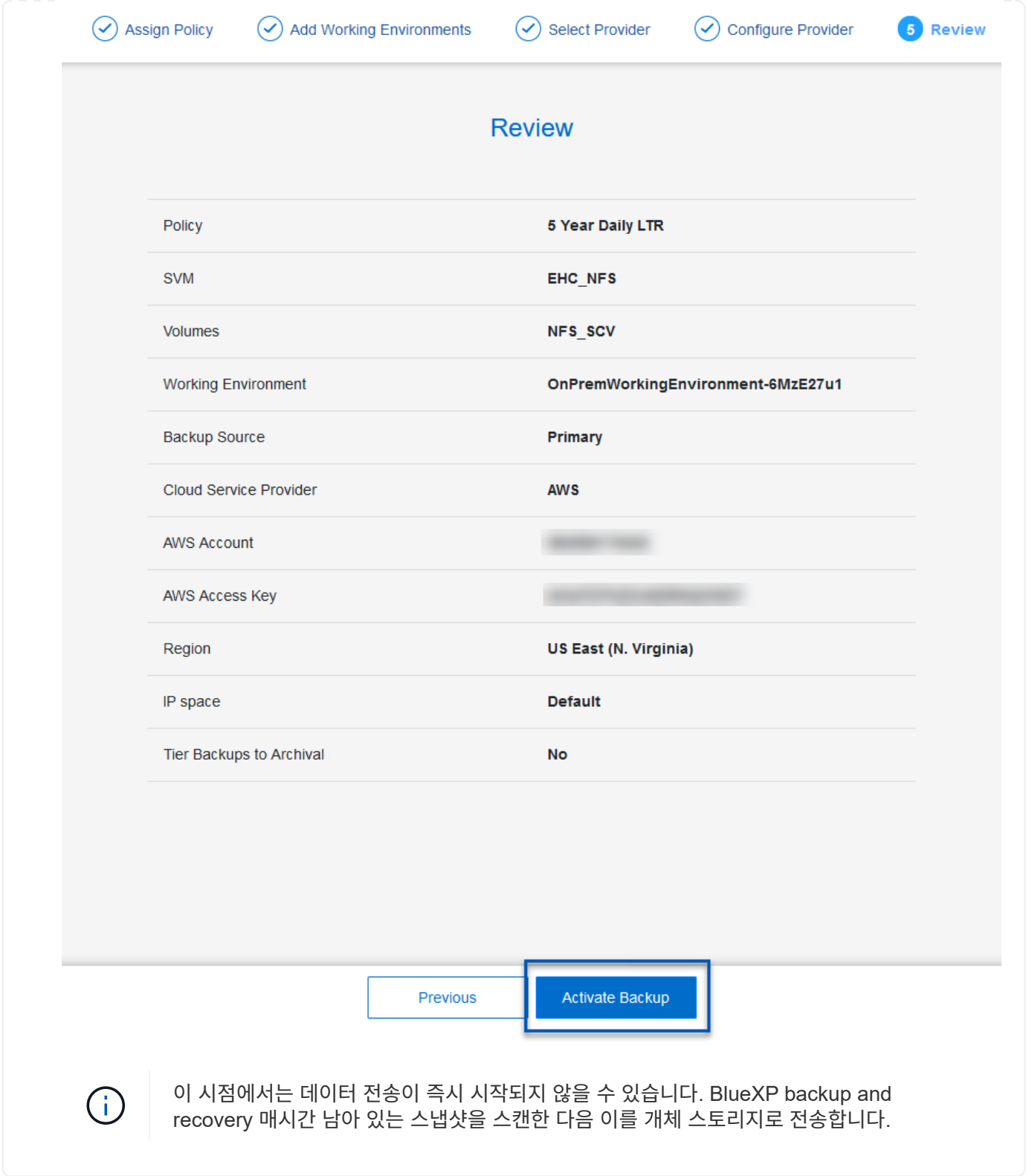
4. 공급자 선택 페이지에서 AWS를 클릭한 다음 다음 버튼을 클릭하여 계속합니다.



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.



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 과 가상 머신을 위한 BlueXP backup and recovery 의 데이터 복원 프로세스에 대한 개요를 제공합니다.

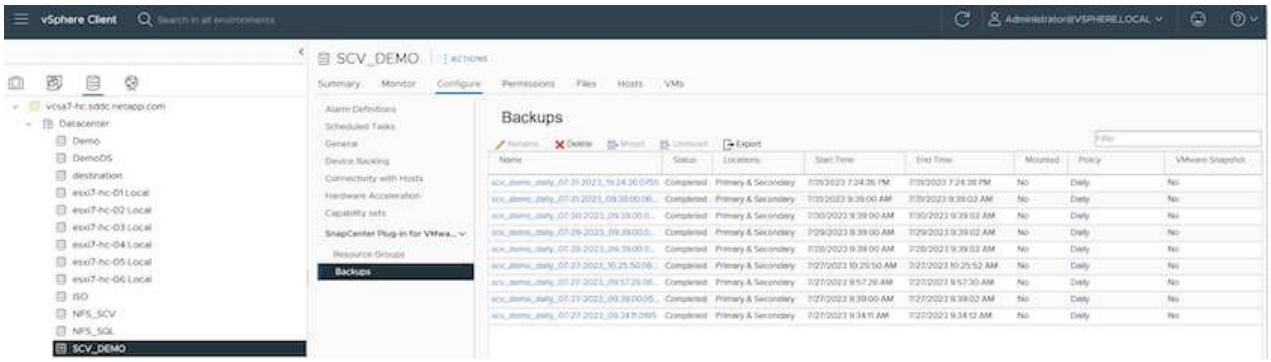
SnapCenter Plug-in for VMware vSphere 에서 가상 머신 복원

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.

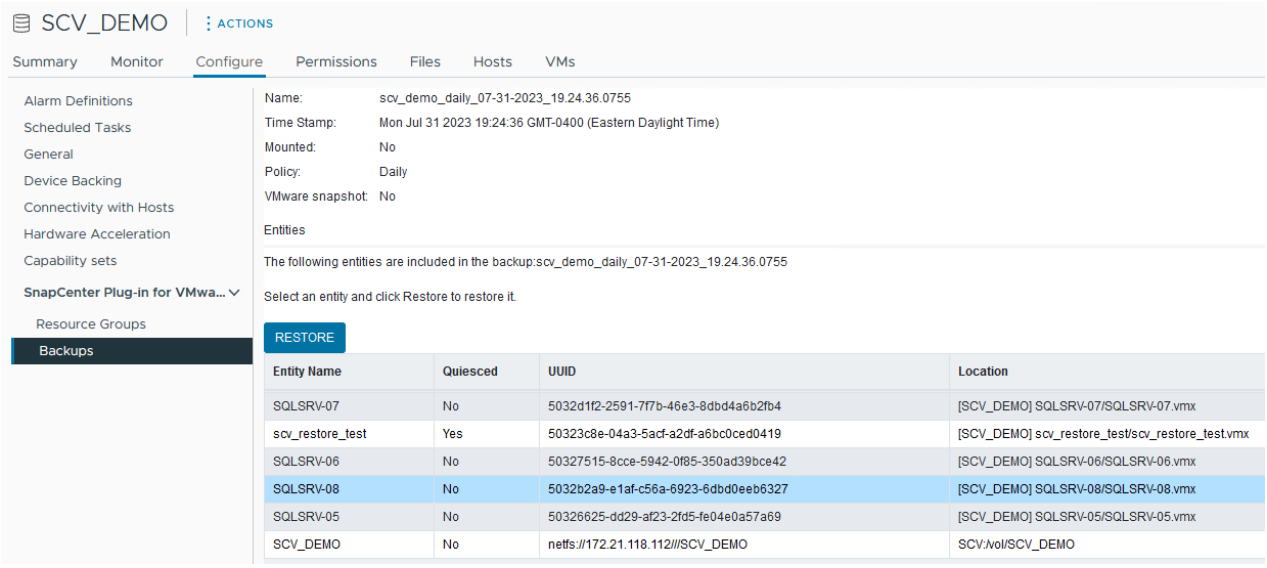
SCV에서 가상 머신 복원

기본 또는 보조 저장소에서 가상 머신을 복원하려면 다음 단계를 완료하세요.

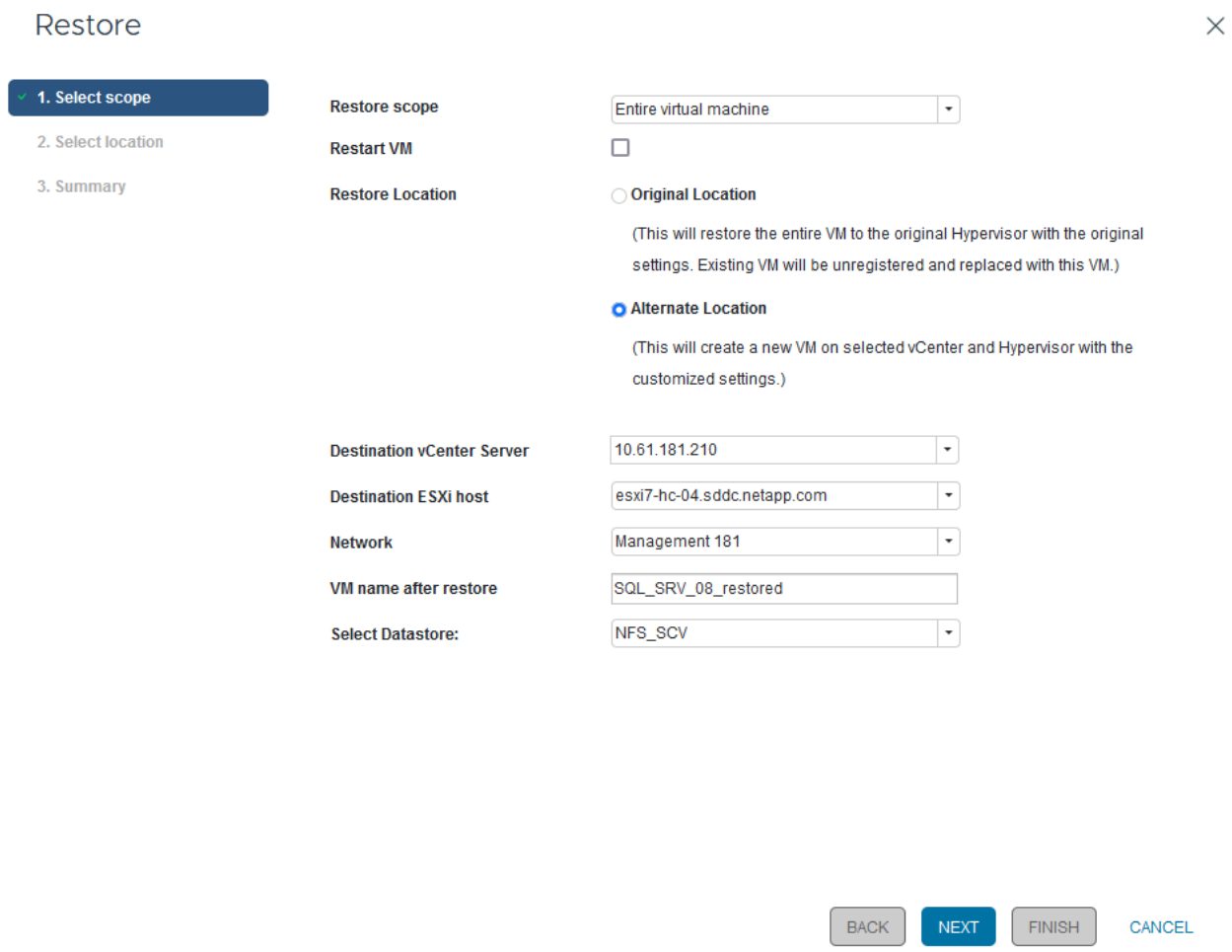
1. vCenter 클라이언트에서 *인벤토리 > 스토리지*로 이동한 다음 복원하려는 가상 머신이 포함된 데이터 저장소를 클릭합니다.
2. 구성 탭에서 *백업*을 클릭하면 사용 가능한 백업 목록에 액세스할 수 있습니다.



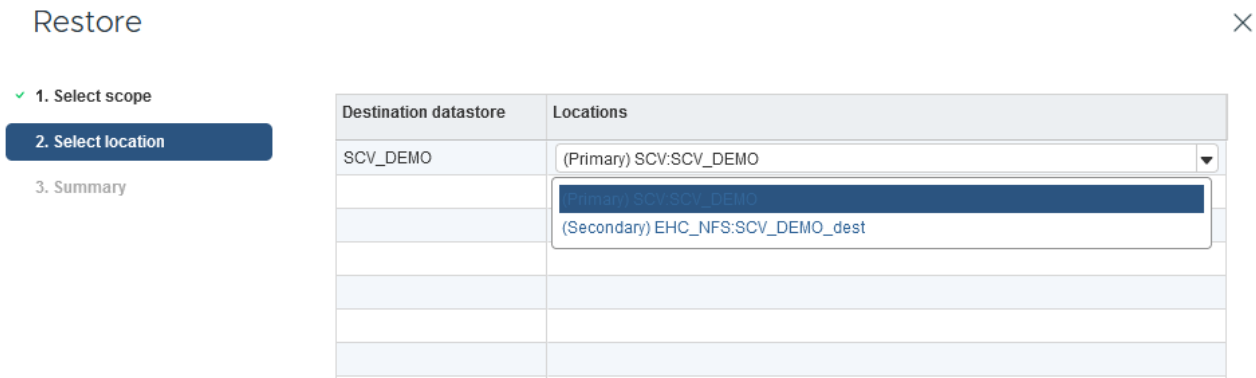
3. 백업을 클릭하여 VM 목록에 액세스한 다음 복원할 VM을 선택합니다. *복원*을 클릭하세요.



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.

BlueXP backup and recovery 통해 가상 머신 복원

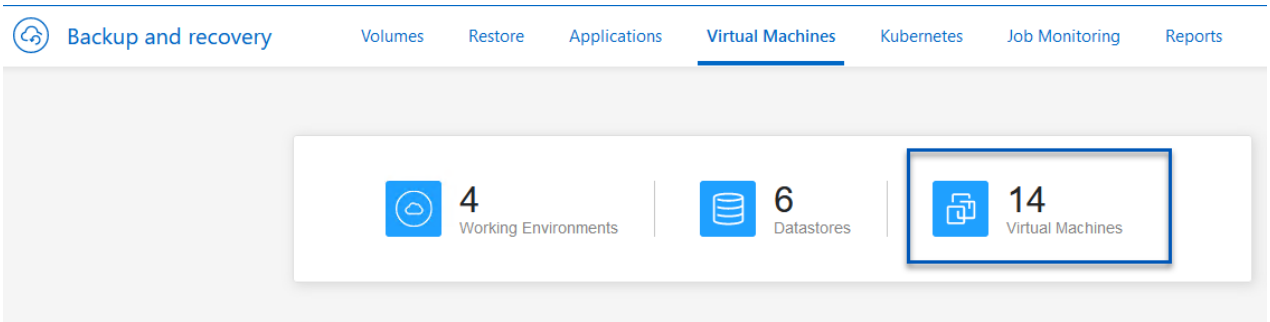
가상 머신을 위한 BlueXP backup and recovery 사용하면 가상 머신을 원래 위치로 복원할 수 있습니다. 복원 기능은 BlueXP 웹 콘솔을 통해 접근합니다.

자세한 내용은 다음을 참조하세요. "클라우드에서 가상 머신 데이터 복원" .

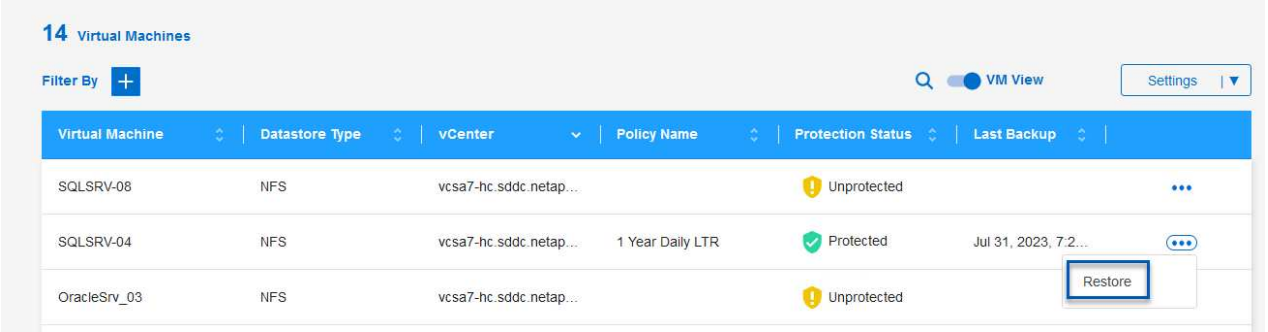
BlueXP backup and recovery 에서 가상 머신 복원

BlueXP backup and recovery 에서 가상 머신을 복원하려면 다음 단계를 완료하세요.

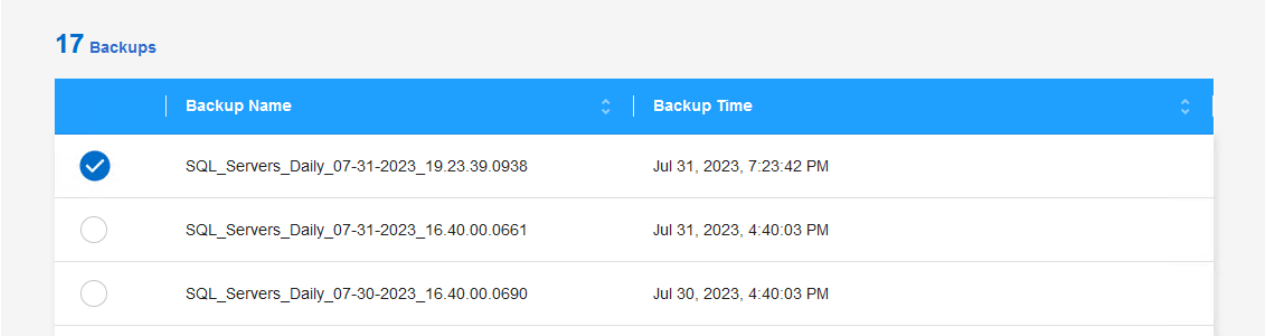
1. *보호 > 백업 및 복구 > 가상 머신*으로 이동한 후 가상 머신을 클릭하면 복원 가능한 가상 머신 목록을 볼 수 있습니다.



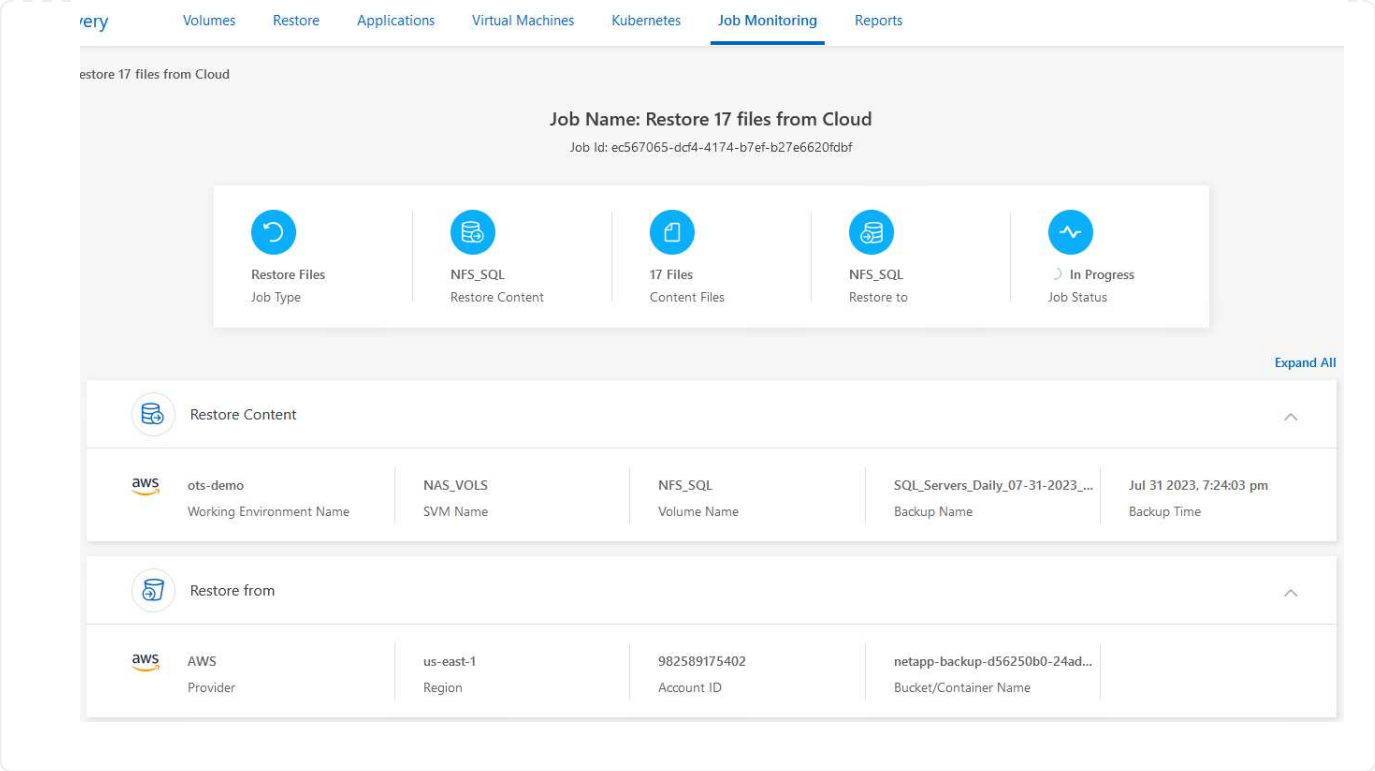
2. 복원할 VM의 설정 드롭다운 메뉴에 액세스하여 다음을 선택합니다.



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

3-2-1 백업 전략은 SnapCenter Plug-in for VMware vSphere 과 가상 머신용 BlueXP backup and recovery 와 함께 구현될 경우 데이터 보호를 위한 견고하고 안정적이며 비용 효율적인 솔루션을 제공합니다. 이 전략은 데이터 중복성과 접근성을 보장할 뿐만 아니라, 온프레미스 ONTAP 스토리지 시스템과 클라우드 기반 개체 스토리지 모두에서 모든 위치에서 데이터를 복원할 수 있는 유연성을 제공합니다.

이 문서에 제시된 사용 사례는 NetApp, VMware 및 주요 클라우드 공급업체 간의 통합을 강조하는 검증된 데이터 보호 기술에 중점을 둡니다. SnapCenter Plug-in for VMware vSphere VMware vSphere와 원활하게 통합되어 데이터 보호 작업을 효율적이고 중앙에서 관리할 수 있도록 해줍니다. 이러한 통합을 통해 가상 머신의 백업 및 복구 프로세스가 간소화되어 VMware 생태계 내에서 쉬운 일정 예약, 모니터링 및 유연한 복원 작업이 가능해집니다. 가상 머신을 위한 BlueXP backup and recovery 클라우드 기반 개체 스토리지에 가상 머신 데이터의 안전하고 공기 간격이 있는 백업을 제공하여 3대 1의 해결책을 제시합니다. 직관적인 인터페이스와 논리적인 워크플로는 중요한 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"
- "BlueXP 문서"

BlueXP disaster recovery 사용하여 **VMFS** 데이터 저장소에 대한 재해 복구 설정

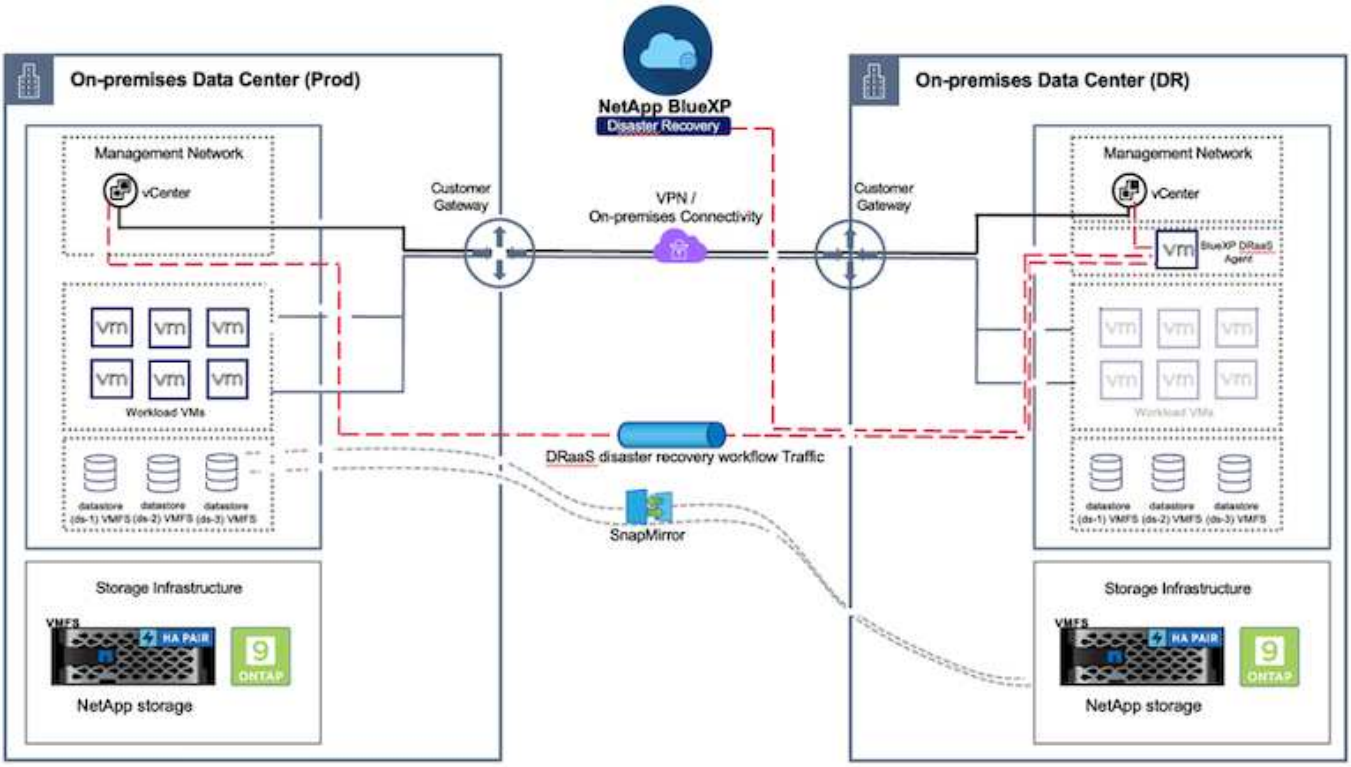
이 사용 사례에서는 VMware Virtual Machine File System(VMFS) 데이터 저장소를 사용하여 온프레미스 VMware VM에 대한 BlueXP disaster recovery 사용하여 재해 복구를 설정하는 절차를 설명합니다. 이 절차에는 BlueXP 계정과 커넥터 설정, ONTAP 시스템 간 SnapMirror 복제 설정, VMware vCenter와의 통합, 장애 조치 및 장애 복구 작업 자동화가 포함됩니다.

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.

소개

이 문서의 섹션에서는 온프레미스 VMware VM을 다른 지정된 사이트로 재해 복구하도록 BlueXP DRaaS를 구성하는 방법을 설명합니다. 이 설정의 일부로 BlueXP 계정, BlueXP 커넥터, BlueXP 작업 공간 내에 추가된 ONTAP 어레이는 VMware vCenter에서 ONTAP 스토리지로의 통신을 활성화하는 데 필요합니다. 또한, 이 문서에서는 사이트 간 복제를 구성하는 방법과 복구 계획을 설정하고 테스트하는 방법에 대해 자세히 설명합니다. 마지막 섹션에는 전체 사이트 장애 조치를 수행하는 방법과 기본 사이트가 복구되어 온라인으로 전환되었을 때 장애 복구하는 방법에 대한 지침이 나와 있습니다.

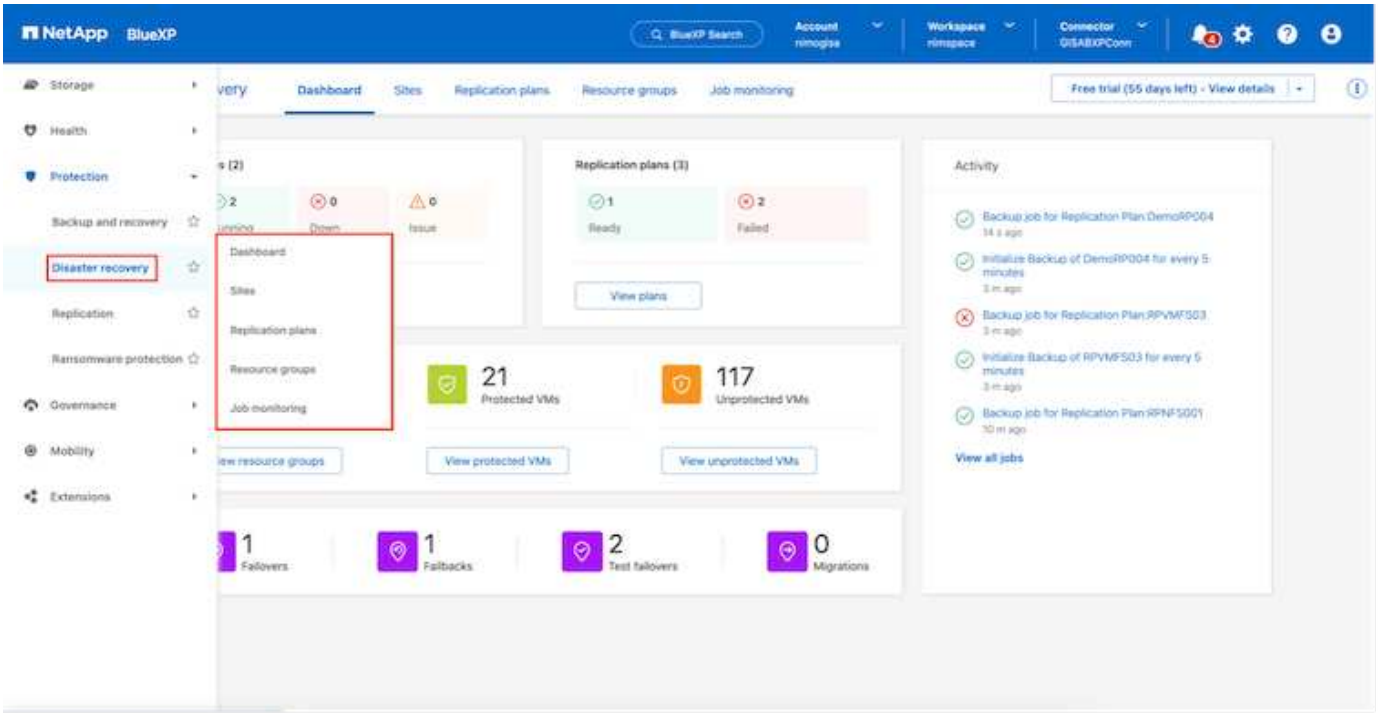
NetApp BlueXP 콘솔에 통합된 BlueXP disaster recovery 서비스를 사용하면 고객은 온프레미스 VMware vCenter와 ONTAP 스토리지를 검색하고, 리소스 그룹을 만들고, 재해 복구 계획을 수립하고, 이를 리소스 그룹과 연결하고, 장애 조치 및 장애 복구를 테스트하거나 실행할 수 있습니다. SnapMirror 두 사이트를 증분적 변경 사항으로 최신 상태로 유지하기 위해 스토리지 수준 블록 복제를 제공하며, 최대 5분의 RPO를 구현합니다. 운영 및 복제된 데이터 저장소에 영향을 주거나 추가 저장 비용을 발생시키지 않고도 정기적인 훈련으로 DR 절차를 시뮬레이션할 수도 있습니다. BlueXP disaster recovery ONTAP의 FlexClone 기술을 활용하여 DR 사이트에서 마지막으로 복제된 스냅샷으로부터 VMFS 데이터 저장소의 공간 효율적인 복사본을 생성합니다. DR 테스트가 완료되면 고객은 실제 복제된 프로덕션 리소스에 아무런 영향을 미치지 않고 간단히 테스트 환경을 삭제할 수 있습니다. 실제 장애 조치(계획된 것이든 계획되지 않은 것이든)가 필요한 경우, 몇 번의 클릭만으로 BlueXP disaster recovery 서비스는 지정된 재해 복구 사이트에서 보호된 가상 머신을 자동으로 불러오는 데 필요한 모든 단계를 조율합니다. 이 서비스는 또한 SnapMirror 기본 사이트와의 관계를 역전시키고, 필요한 경우 장애 복구 작업을 위해 보조 사이트의 변경 사항을 기본 사이트로 복제합니다. 이러한 모든 것들은 다른 잘 알려진 대안과 비교했을 때 훨씬 적은 비용으로 달성할 수 있습니다.



시작하기

BlueXP disaster recovery 시작하려면 BlueXP 콘솔을 사용한 다음 서비스에 액세스하세요.

1. BlueXP 에 로그인하세요.
2. BlueXP 왼쪽 탐색 창에서 보호 > 재해 복구를 선택합니다.
3. BlueXP disaster recovery 보드가 나타납니다.

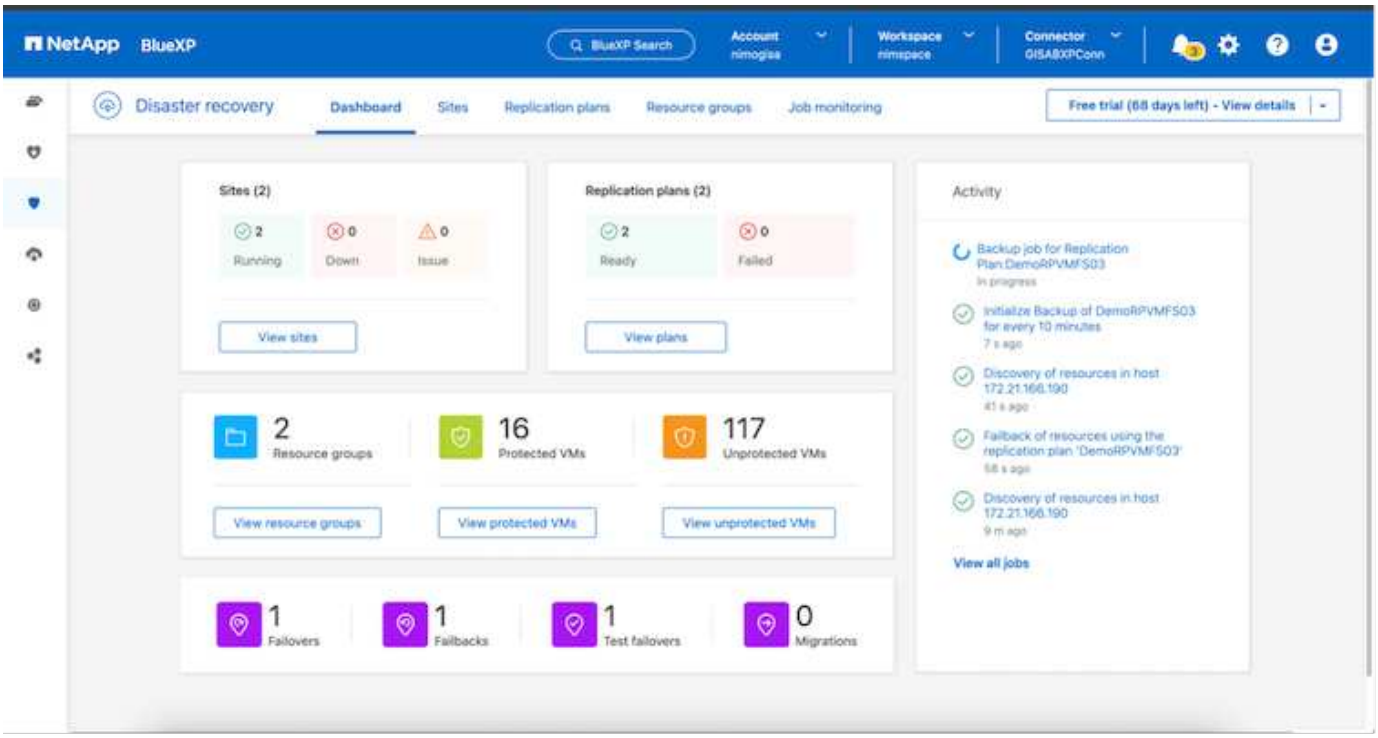


재해 복구 계획을 구성하기 전에 다음 전제 조건이 충족되었는지 확인하세요.

- BlueXP Connector는 NetApp BlueXP 에 설정되어 있습니다. 커넥터는 AWS VPC에 배포되어야 합니다.
- BlueXP 커넥터 인스턴스는 소스 및 대상 vCenter와 스토리지 시스템에 연결할 수 있습니다.
- VMware용 VMFS 데이터 저장소를 호스팅하는 온프레미스 NetApp 스토리지 시스템이 BlueXP 에 추가되었습니다.
- 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.

> NetApp BlueXP 커넥터를 재해 복구 사이트나 제3의 사이트에 배포하여 실제 중단이나 자연 재해 발생 시 BlueXP 커넥터가 네트워크를 통해 소스 및 대상 리소스와 통신할 수 있도록 권장합니다.

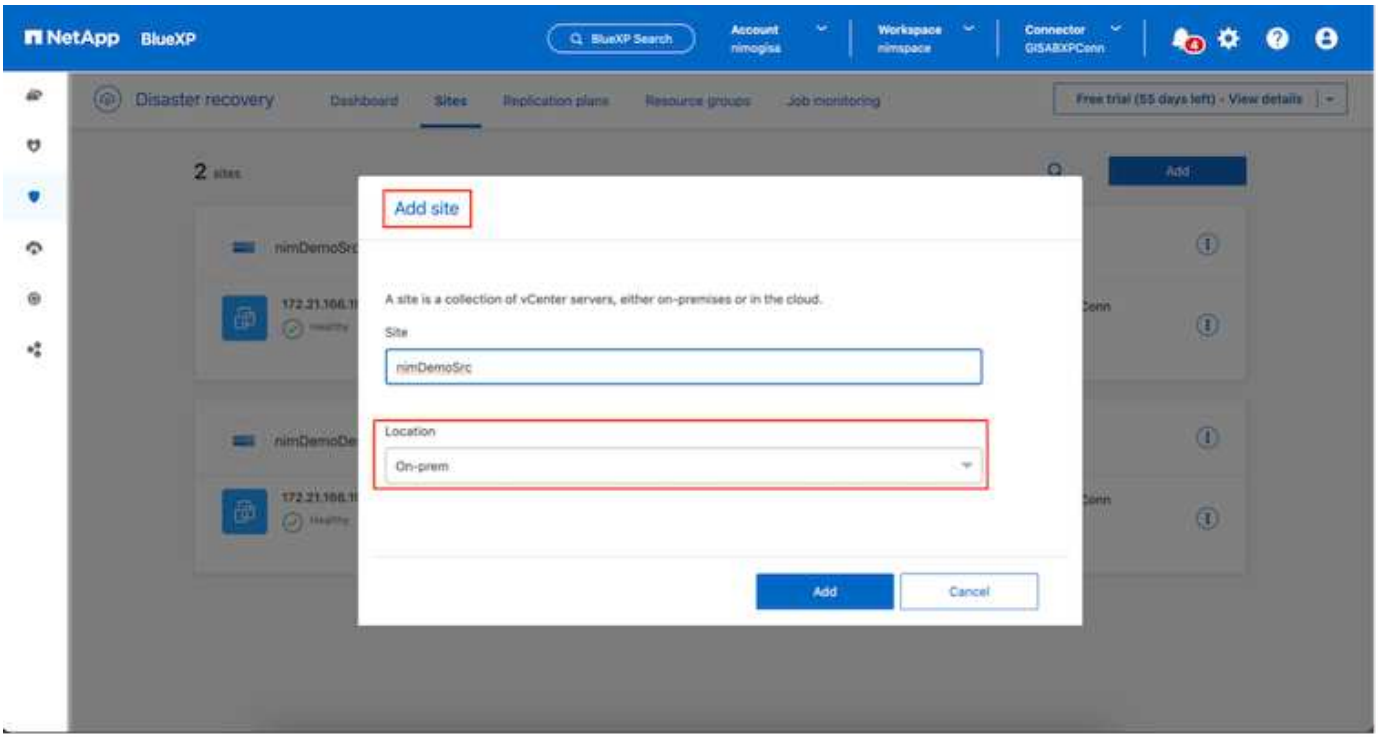


이 문서를 작성하는 시점에는 온프레미스 간 VMFS 데이터 저장소에 대한 지원이 기술 미리보기 단계에 있습니다. 이 기능은 FC 및 ISCSI 프로토콜 기반 VMFS 데이터 저장소에서 모두 지원됩니다.

BlueXP disaster recovery 구성

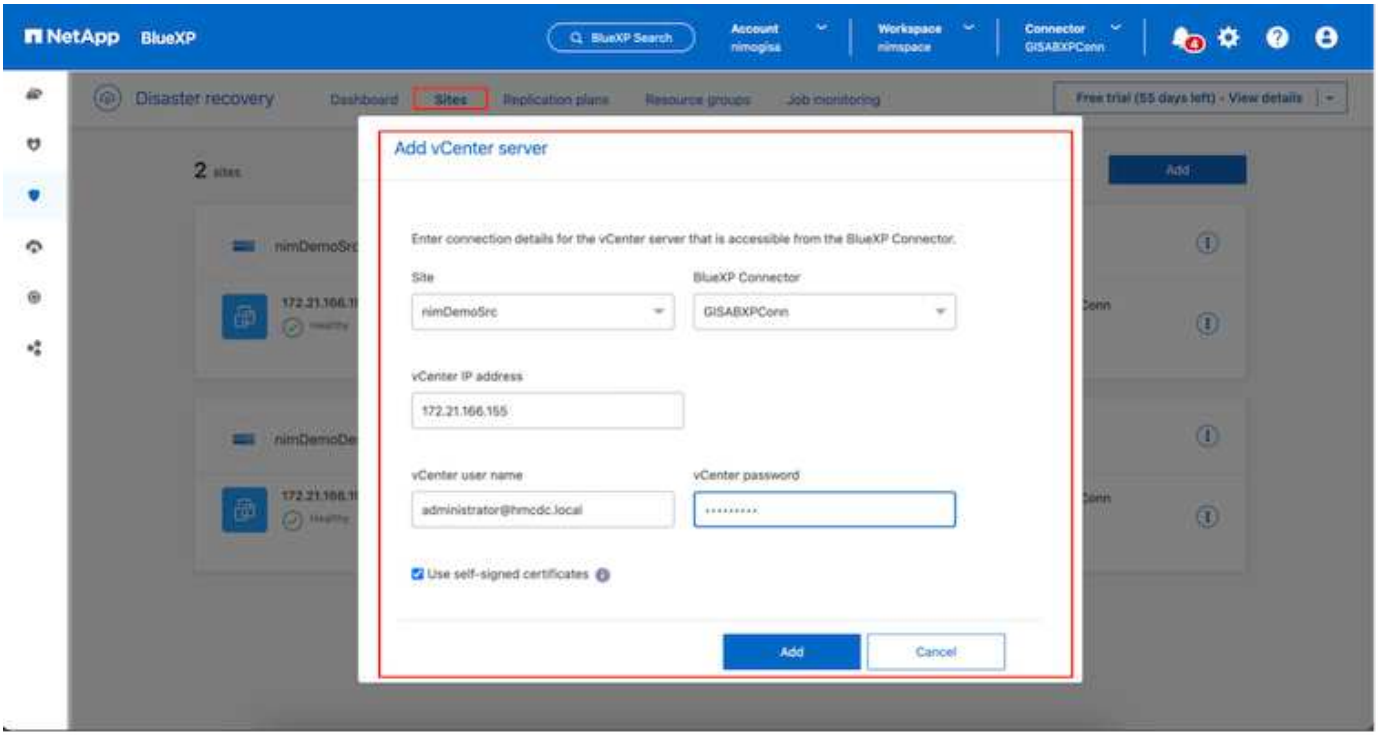
재해 복구를 준비하는 첫 번째 단계는 온프레미스 vCenter 및 스토리지 리소스를 검색하여 BlueXP disaster recovery에 추가하는 것입니다.

캔버스 내 작업 환경에 ONTAP 스토리지 시스템이 추가되었는지 확인하세요. BlueXP 콘솔을 열고 왼쪽 탐색에서 *보호 > 재해 복구*를 선택합니다. *vCenter 서버 검색*을 선택하거나 상단 메뉴를 사용하여 *사이트 > 추가 > vCenter 추가*를 선택합니다.

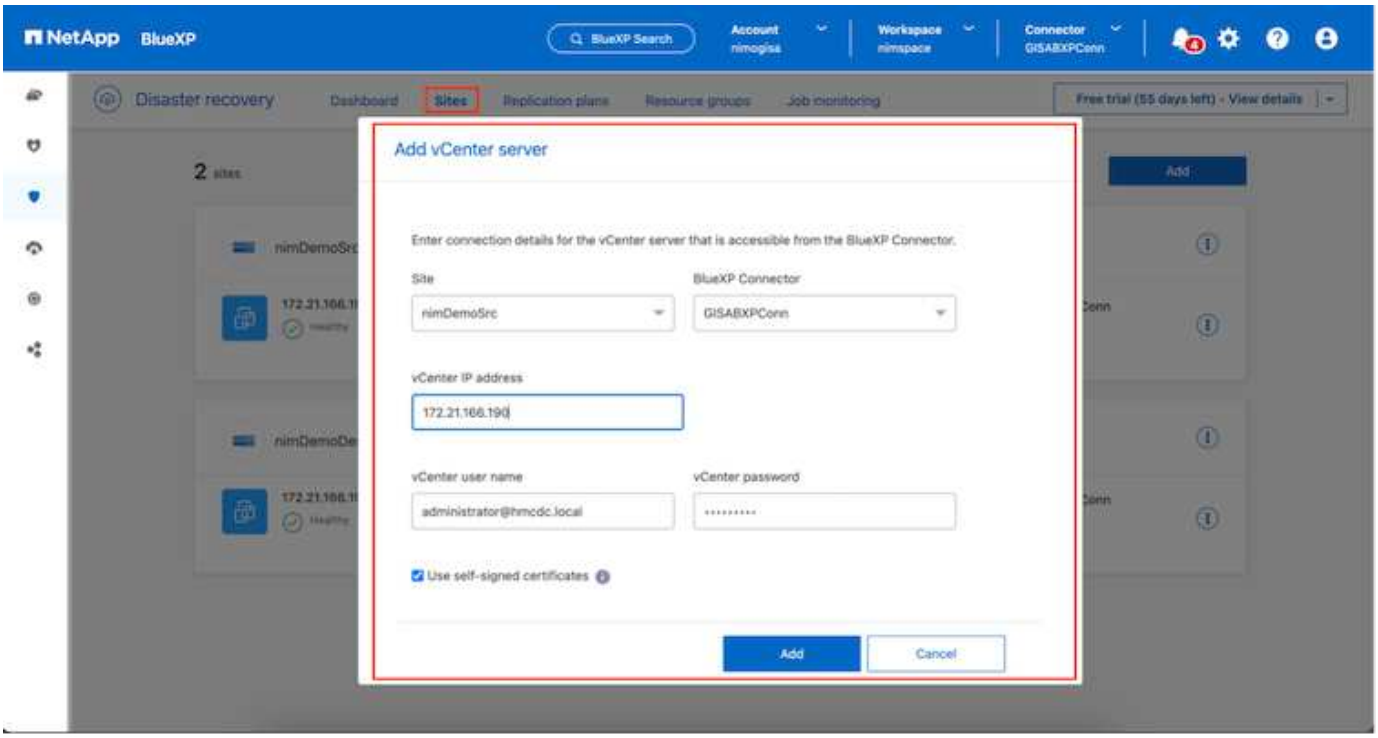


다음 플랫폼을 추가하세요:

- 원천. 온프레미스 vCenter.



- 목적지. VMC SDDC vCenter.



vCenter가 추가되면 자동 검색이 실행됩니다.

소스 사이트와 대상 사이트 간 스토리지 복제 구성

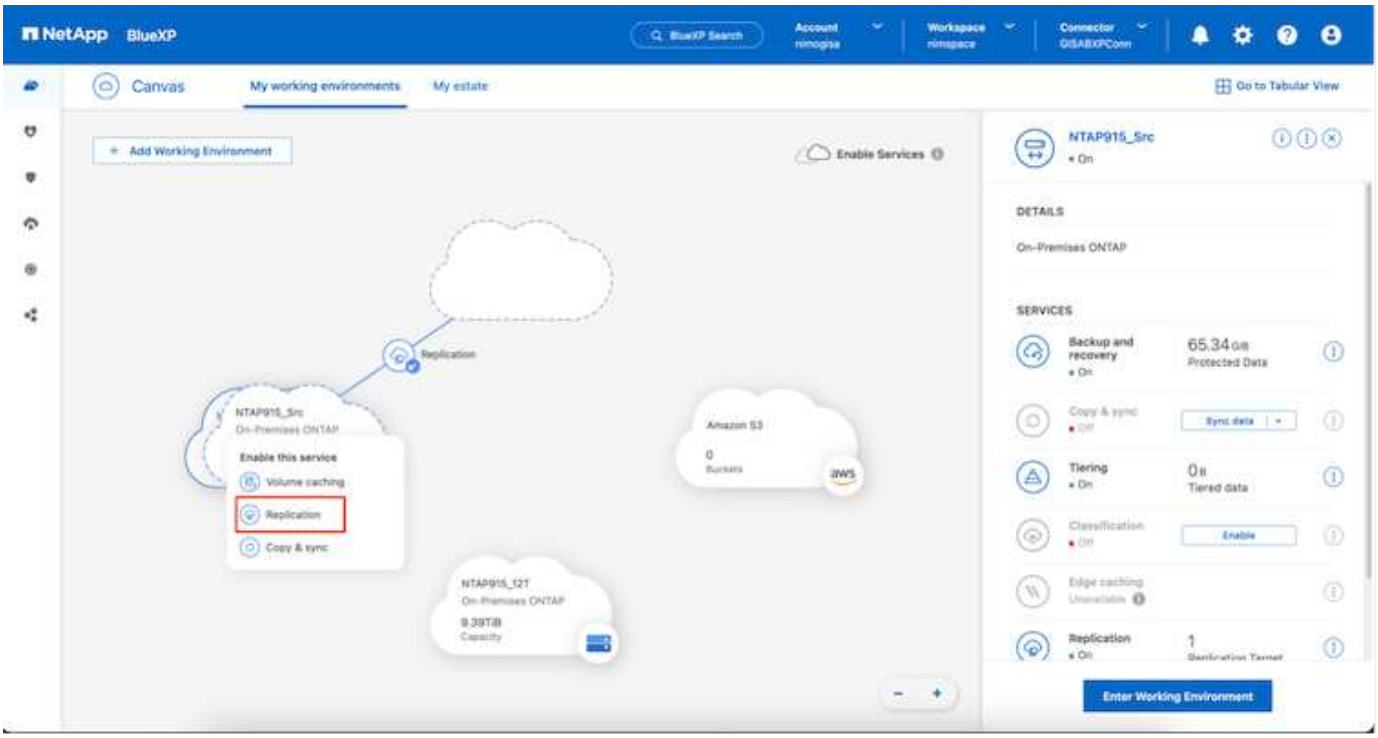
SnapMirror ONTAP 스냅샷을 활용하여 한 위치에서 다른 위치로의 데이터 전송을 관리합니다. 처음에는 소스 볼륨의 스냅샷을 기반으로 한 전체 복사본이 대상에 복사되어 기준 동기화를 수행합니다. 소스에서 데이터가 변경되면 새로운 스냅샷이 생성되어 기준 스냅샷과 비교됩니다. 변경된 것으로 확인된 블록은 대상에 복제되고, 최신 스냅샷이 현재 기준선 또는 최신 공통 스냅샷이 됩니다. 이를 통해 프로세스를 반복하고 증분 업데이트를 대상에 전송할 수 있습니다.

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.

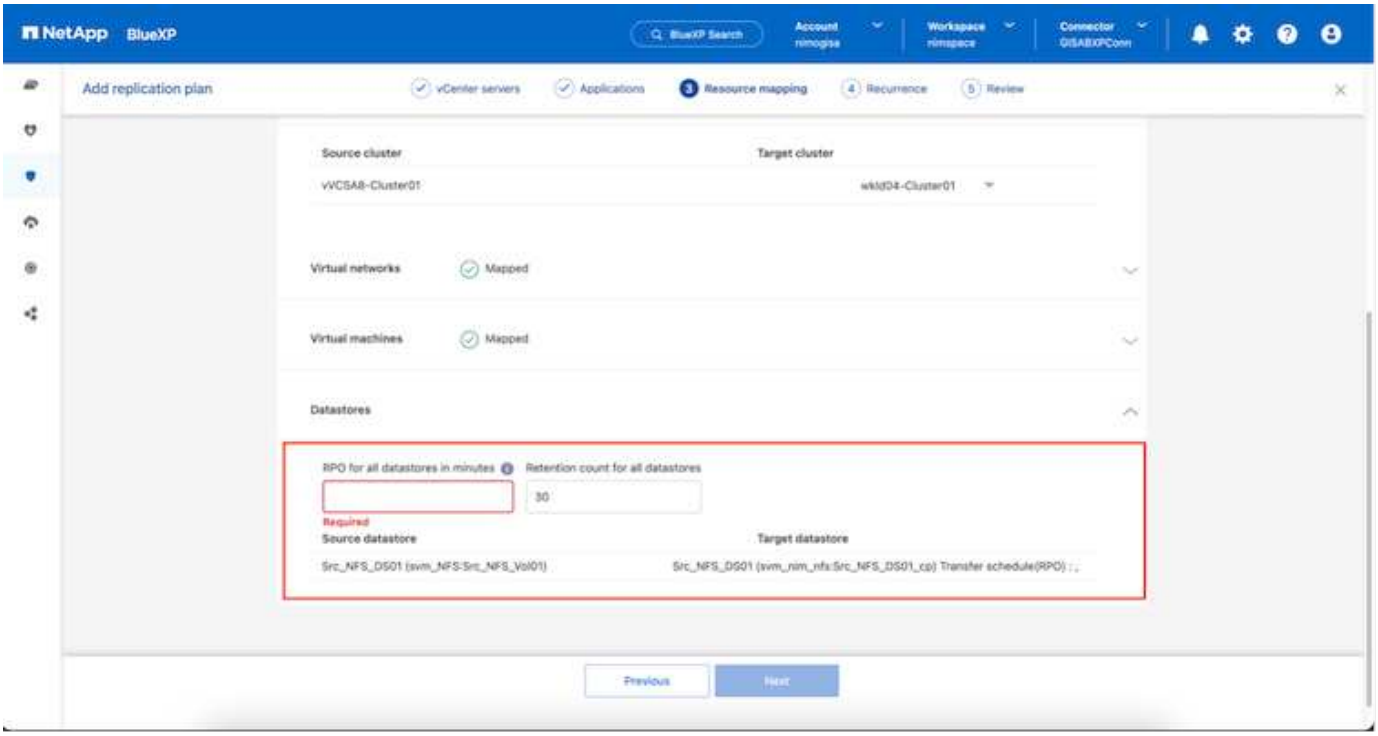
VMware 재해 복구를 설정하는 방법

SnapMirror 복제를 생성하는 프로세스는 모든 애플리케이션에서 동일하게 유지됩니다. 이 과정은 수동이거나 자동화될 수 있습니다. 가장 쉬운 방법은 BlueXP 활용하여 SnapMirror 복제를 구성하는 것입니다. 즉, 환경의 소스 ONTAP 시스템을 대상 환경으로 간단히 끌어서 놓아 나머지 프로세스를 안내하는 마법사를 실행하는 것입니다.



BlueXP DRaaS는 다음 두 가지 기준이 충족되는 경우 동일한 작업을 자동화할 수도 있습니다.

- 소스 클러스터와 대상 클러스터는 피어 관계를 갖습니다.
- 소스 SVM과 대상 SVM은 피어 관계를 갖습니다.

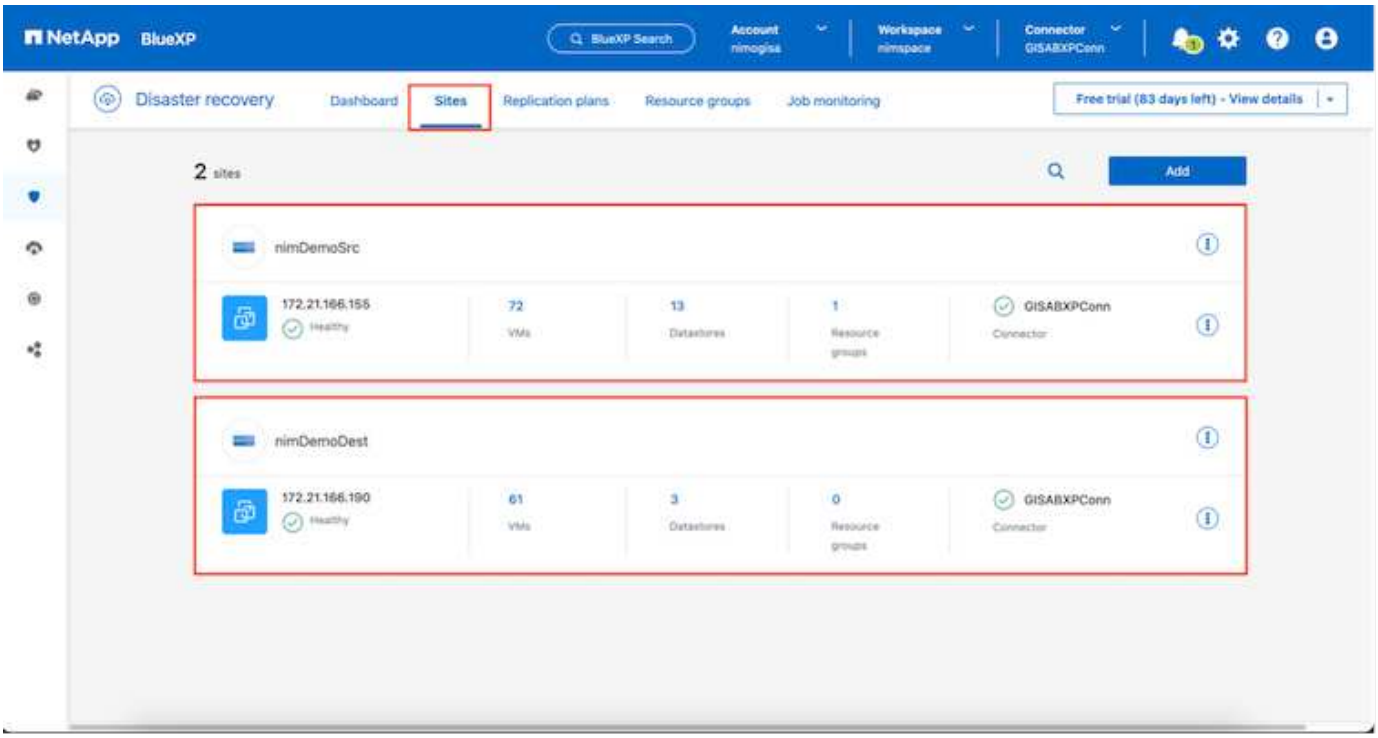


CLI를 통해 볼륨에 대한 SnapMirror 관계가 이미 구성된 경우 BlueXP DRaaS는 해당 관계를 선택하고 나머지 워크플로 작업을 계속 진행합니다.

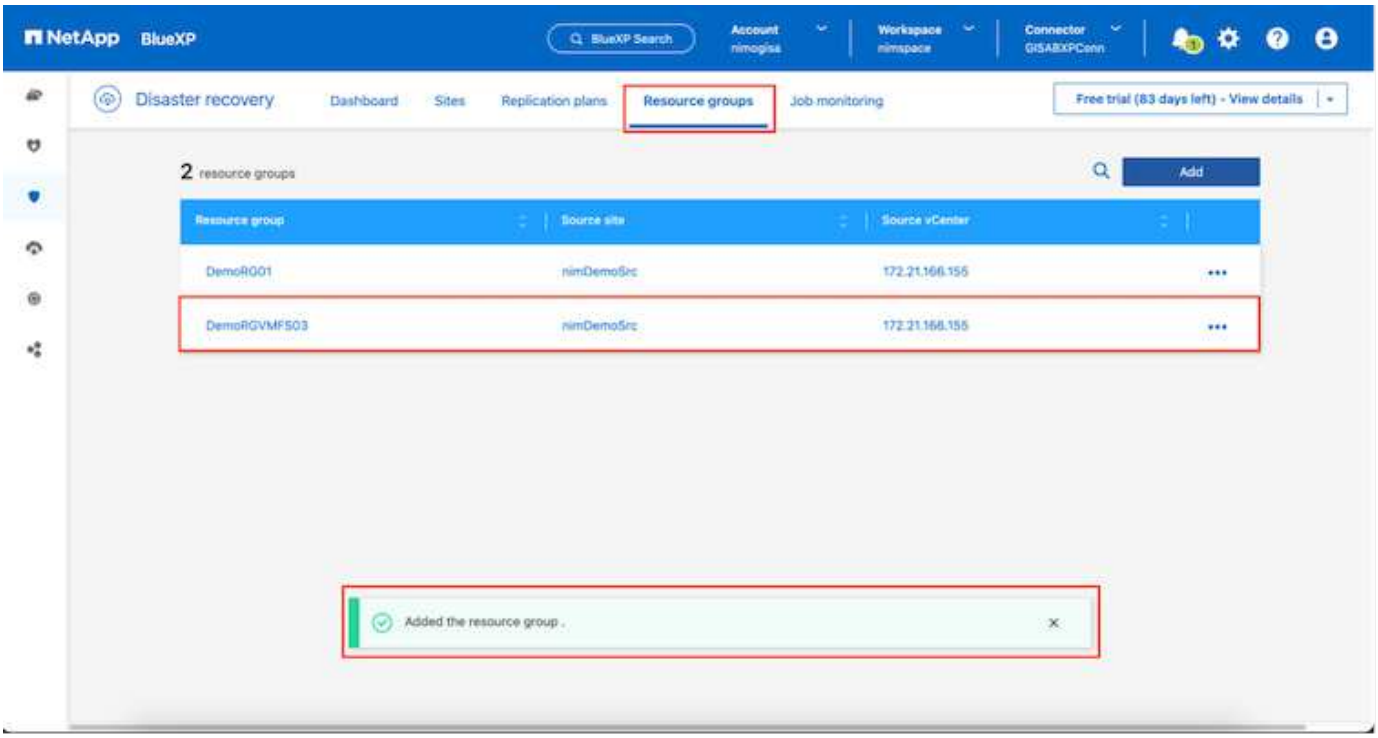
위의 접근 방식 외에도 ONTAP CLI나 시스템 관리자를 통해 SnapMirror 복제를 생성할 수도 있습니다. SnapMirror 사용하여 데이터를 동기화하는 데 사용되는 접근 방식과 관계없이 BlueXP DRaaS는 원활하고 효율적인 재해 복구 작업을 위한 워크플로를 조율합니다.

BlueXP disaster recovery 귀사를 위해 무엇을 해드릴 수 있나요**?**

소스 사이트와 대상 사이트가 추가되면 BlueXP disaster recovery 자동으로 심층 검색을 수행하고 관련 메타데이터와 함께 VM을 표시합니다. BlueXP disaster recovery 은 VM에서 사용하는 네트워크와 포트 그룹을 자동으로 감지하여 채웁니다.

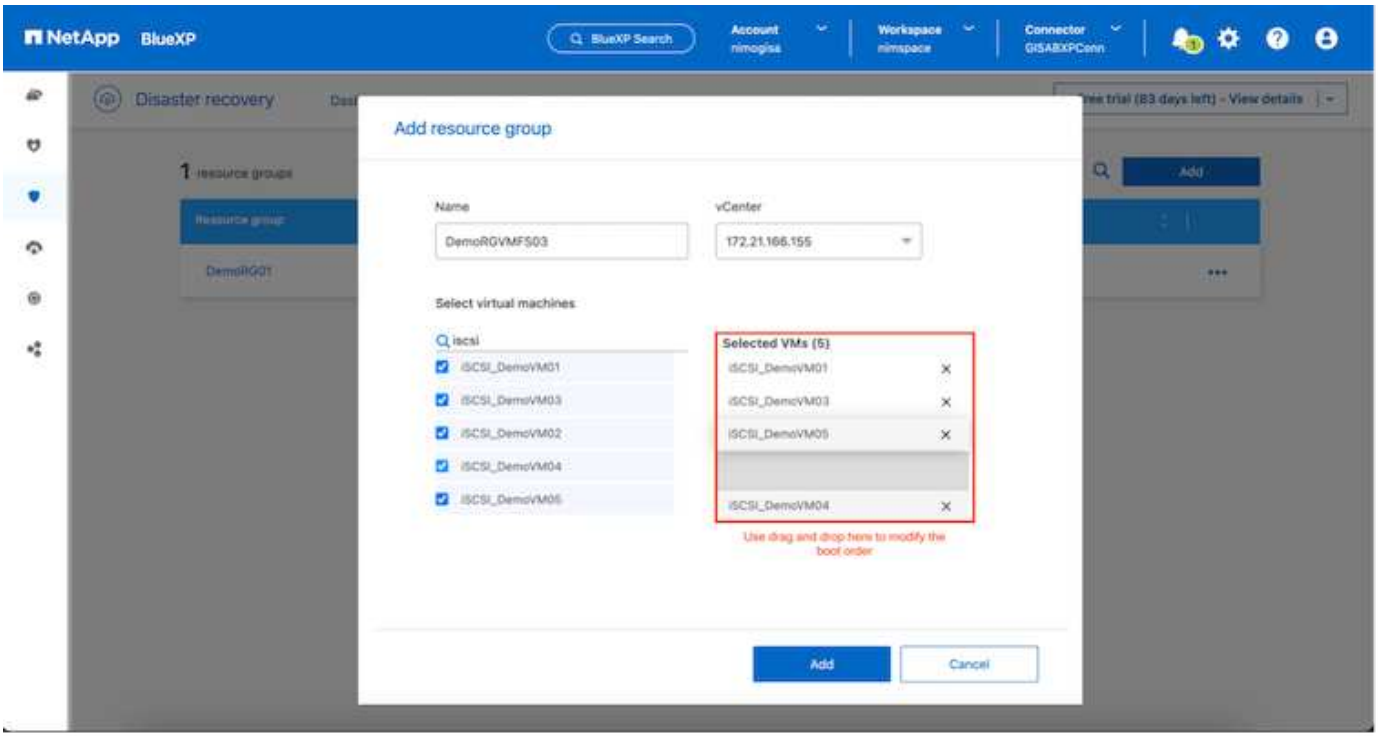


사이트가 추가된 후 VM을 리소스 그룹으로 그룹화할 수 있습니다. BlueXP disaster recovery 리소스 그룹을 사용하면 종속된 VM 세트를 논리적 그룹으로 그룹화할 수 있으며, 이 그룹에는 복구 시 실행될 수 있는 부팅 순서와 부팅 지연이 포함됩니다. 리소스 그룹을 만들려면 *리소스 그룹*으로 이동하여 *새 리소스 그룹 만들기*를 클릭하세요.

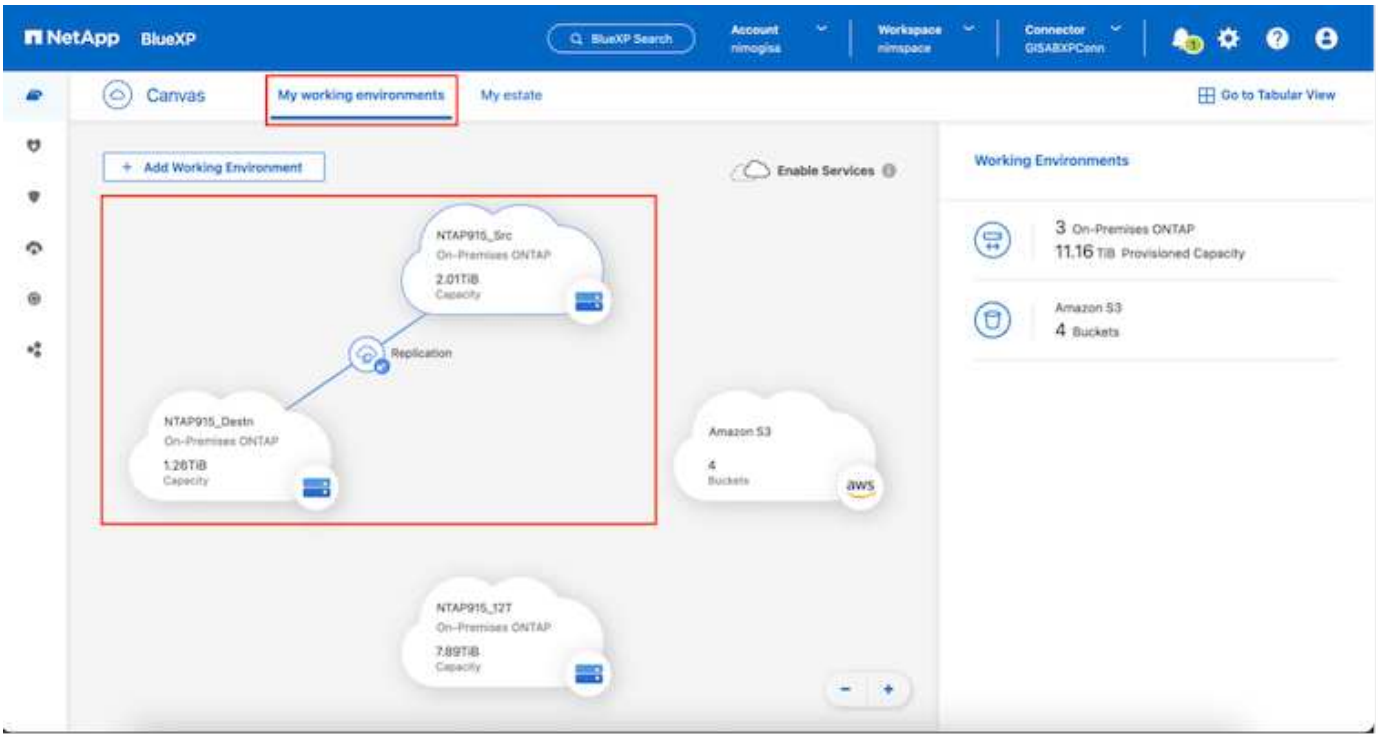


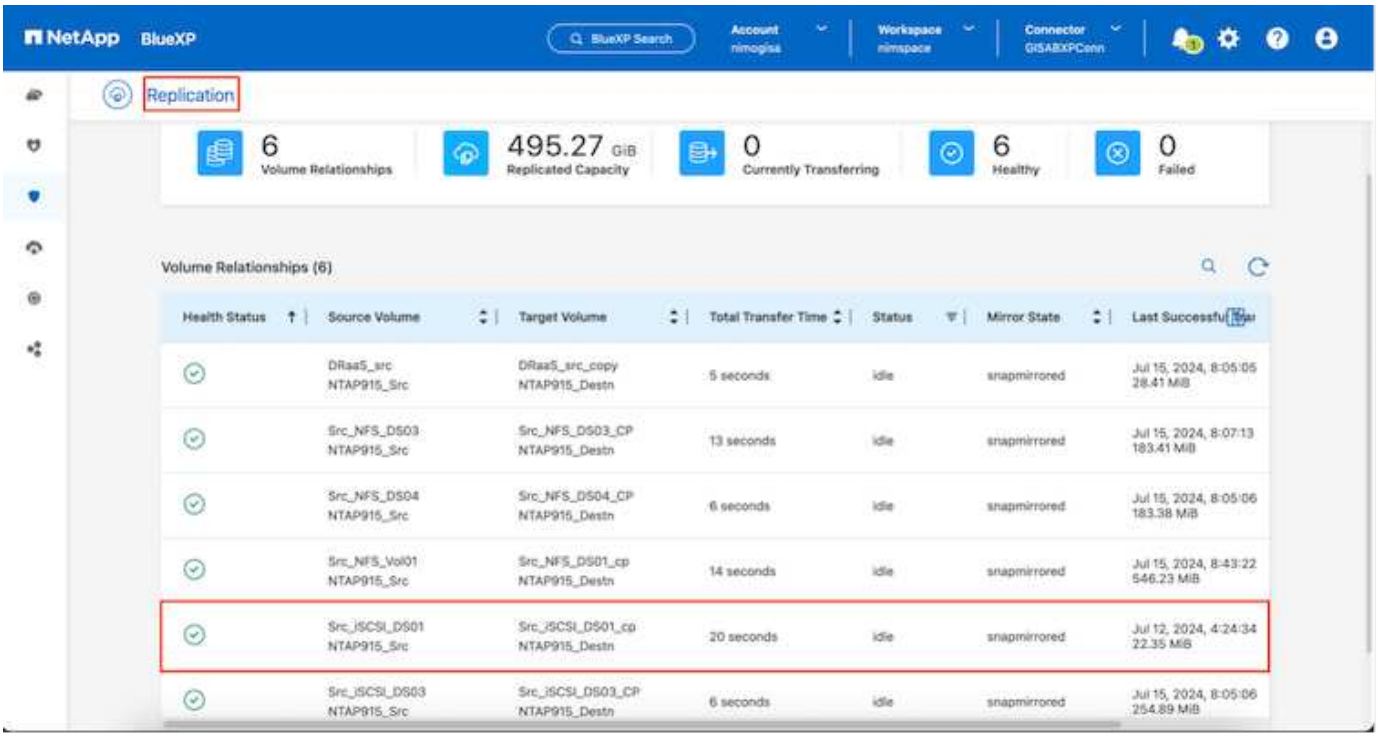
리소스 그룹은 복제 계획을 생성하는 동안에도 생성될 수 있습니다.

리소스 그룹을 만드는 동안 간단한 드래그 앤 드롭 메커니즘을 사용하여 VM의 부팅 순서를 정의하거나 수정할 수 있습니다.



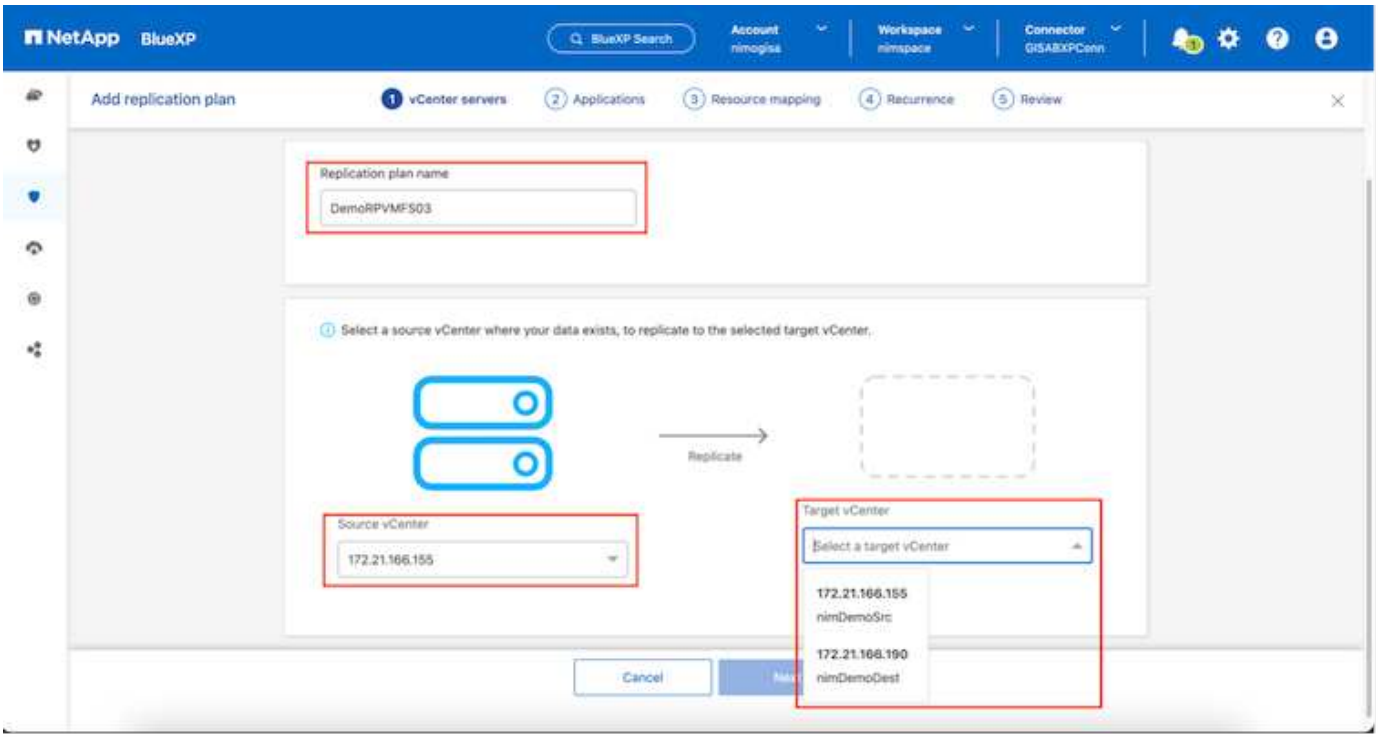
리소스 그룹을 만든 후 다음 단계는 재해 발생 시 가상 머신과 애플리케이션을 복구하기 위한 실행 청사진 또는 계획을 만드는 것입니다. 필수 구성 요소에서 언급했듯이 SnapMirror 복제는 사전에 구성할 수 있으며, DRaaS는 복제 계획을 만드는 동안 지정된 RPO 및 보존 횟수를 사용하여 구성할 수 있습니다.



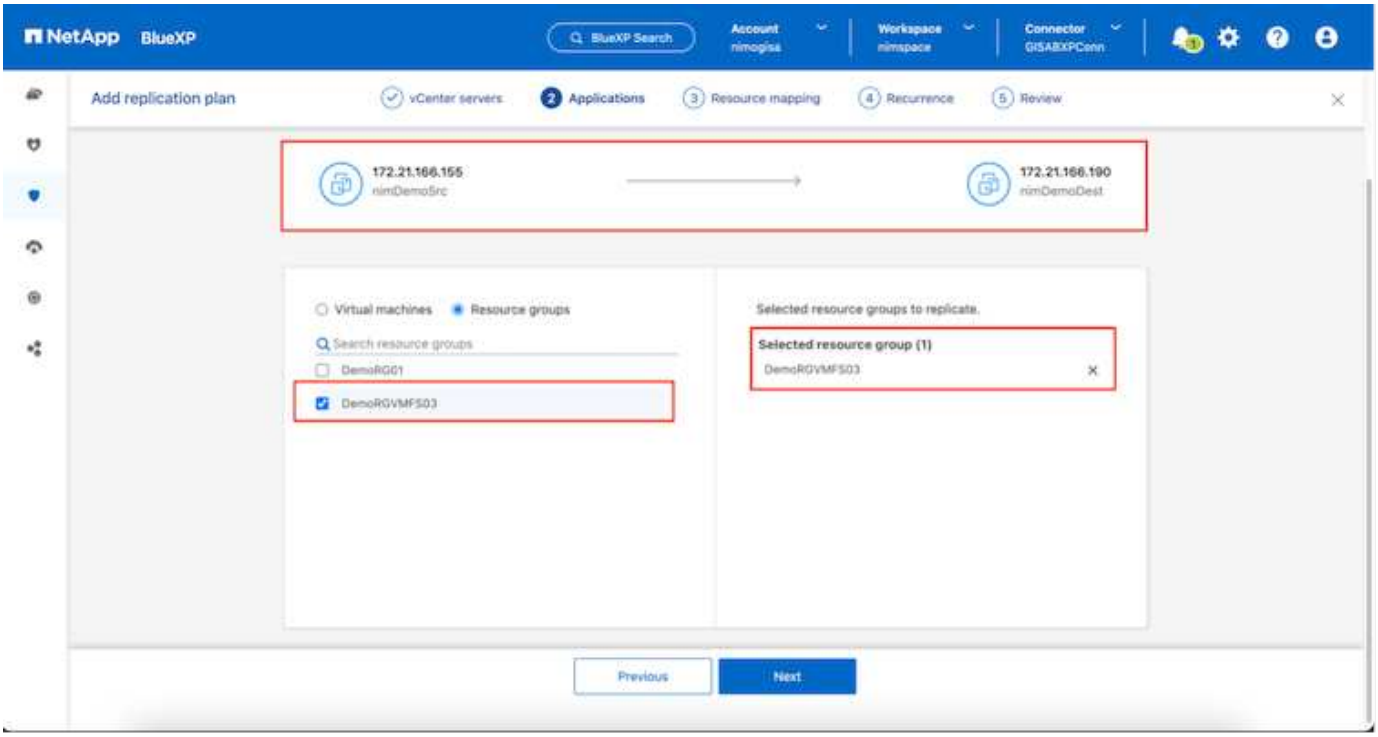


드롭다운에서 소스 및 대상 vCenter 플랫폼을 선택하여 복제 계획을 구성하고, 계획에 포함할 리소스 그룹을 선택하고, 애플리케이션을 복원하고 전원을 켜는 방법, 클러스터 및 네트워크 매핑을 그룹화합니다. 복구 계획을 정의하려면 복제 계획 탭으로 이동하여 *계획 추가*를 클릭합니다.

먼저 소스 vCenter를 선택한 다음 대상 vCenter를 선택합니다.



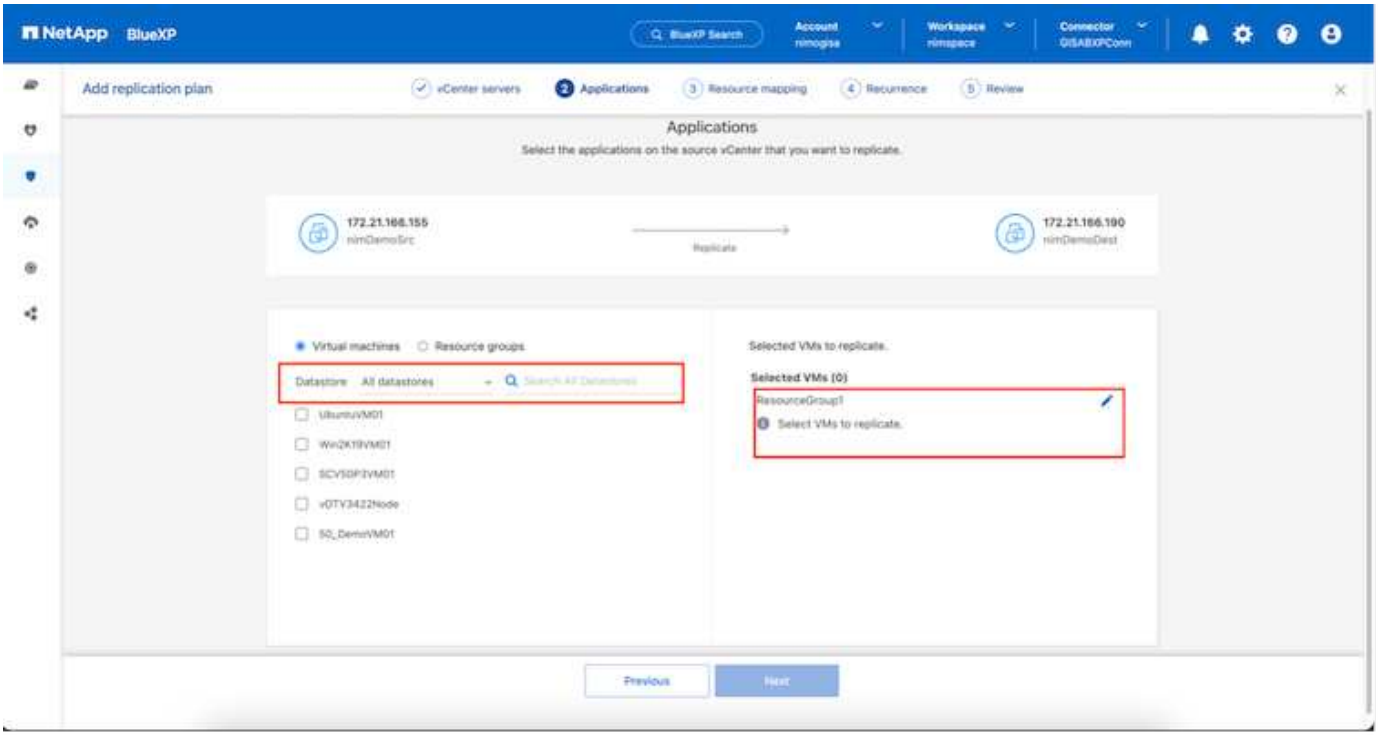
다음 단계는 기존 리소스 그룹을 선택하는 것입니다. 리소스 그룹이 생성되지 않은 경우 마법사는 복구 목표에 따라 필요한 가상 머신을 그룹화(기본적으로 기능적 리소스 그룹 생성)하는 데 도움을 줍니다. 이는 또한 애플리케이션 가상 머신을 복원하는 방법에 대한 작업 순서를 정의하는 데 도움이 됩니다.



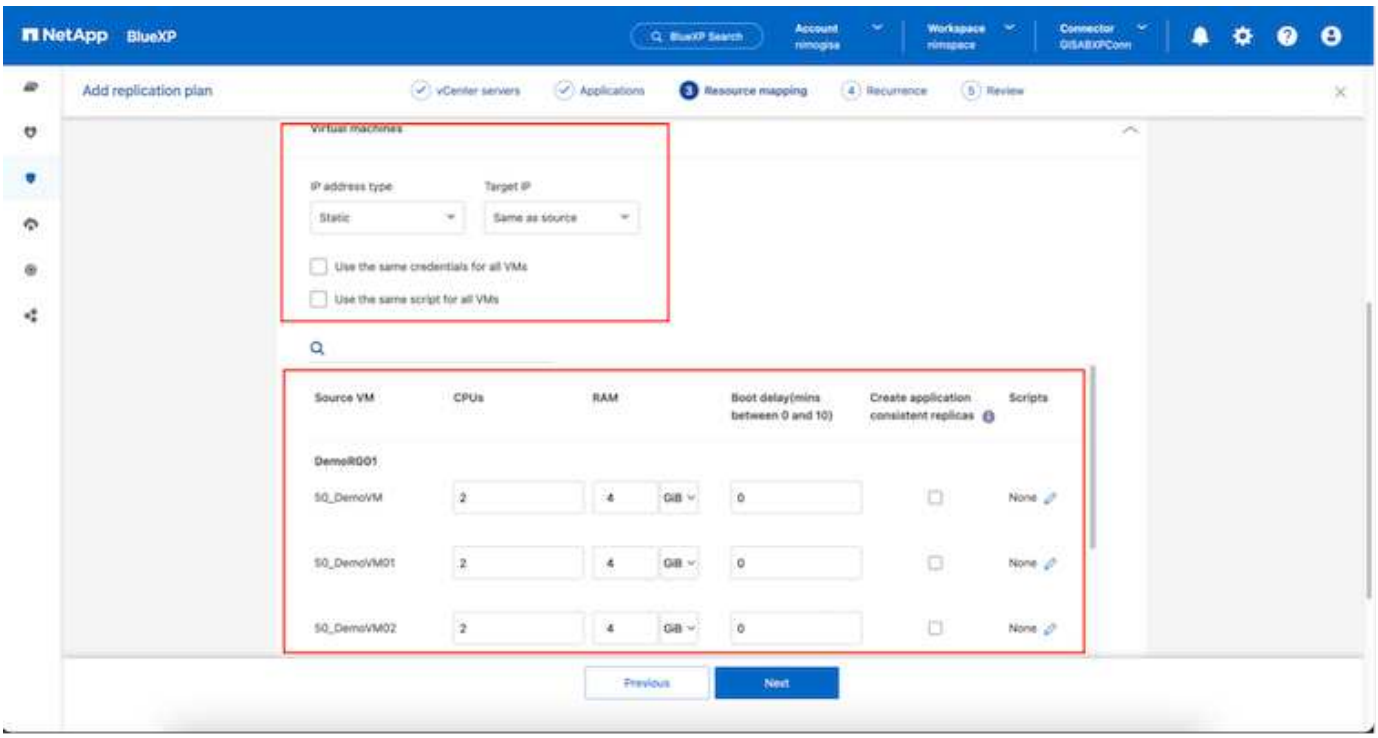
리소스 그룹을 사용하면 드래그 앤 드롭 기능을 사용하여 부팅 순서를 설정할 수 있습니다. 이를 사용하면 복구 프로세스 중에 VM의 전원이 켜지는 순서를 쉽게 수정할 수 있습니다.

리소스 그룹 내의 각 가상 머신은 순서에 따라 순차적으로 시작됩니다. 두 개의 리소스 그룹이 병렬로 시작됩니다.

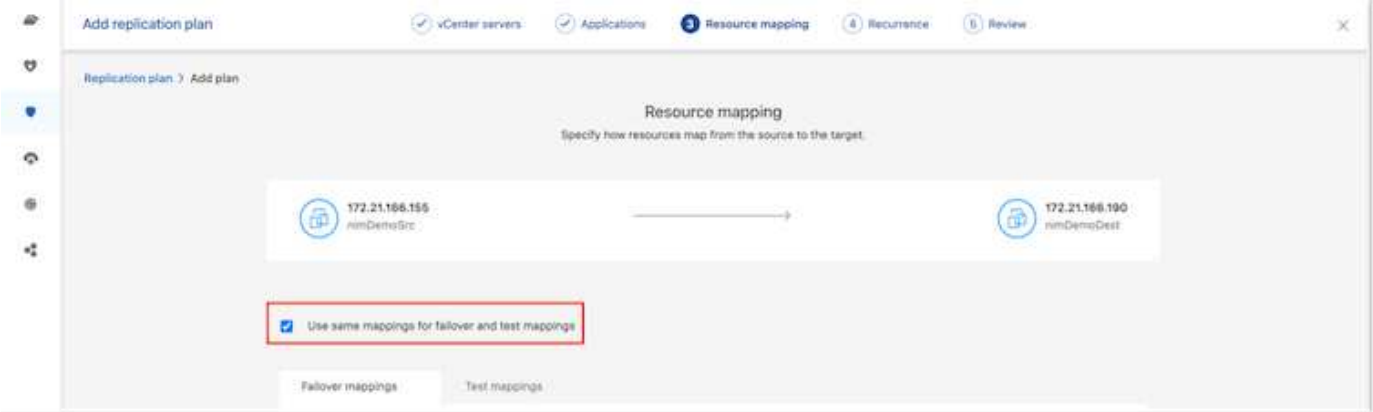
아래 스크린샷은 리소스 그룹이 사전에 생성되지 않은 경우 조직의 요구 사항에 따라 가상 머신이나 특정 데이터 저장소를 필터링하는 옵션을 보여줍니다.



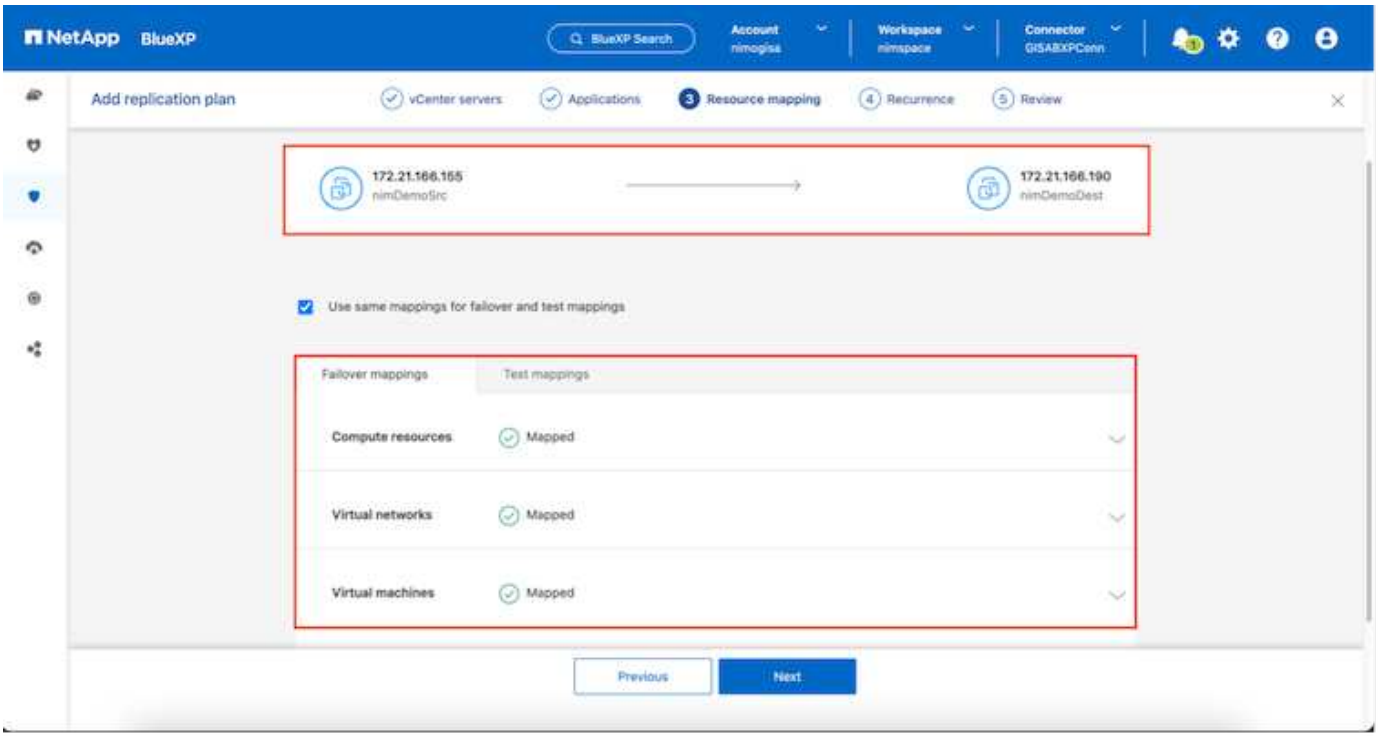
리소스 그룹을 선택한 후 장애 조치 매핑을 만듭니다. 이 단계에서는 소스 환경의 리소스가 대상 환경에 어떻게 매핑되는지 지정합니다. 여기에는 컴퓨팅 리소스, 가상 네트워크가 포함됩니다. IP 사용자 정의, 사전 및 사후 스크립트, 부팅 지연, 애플리케이션 일관성 등. 자세한 내용은 다음을 참조하세요."복제 계획 만들기" .



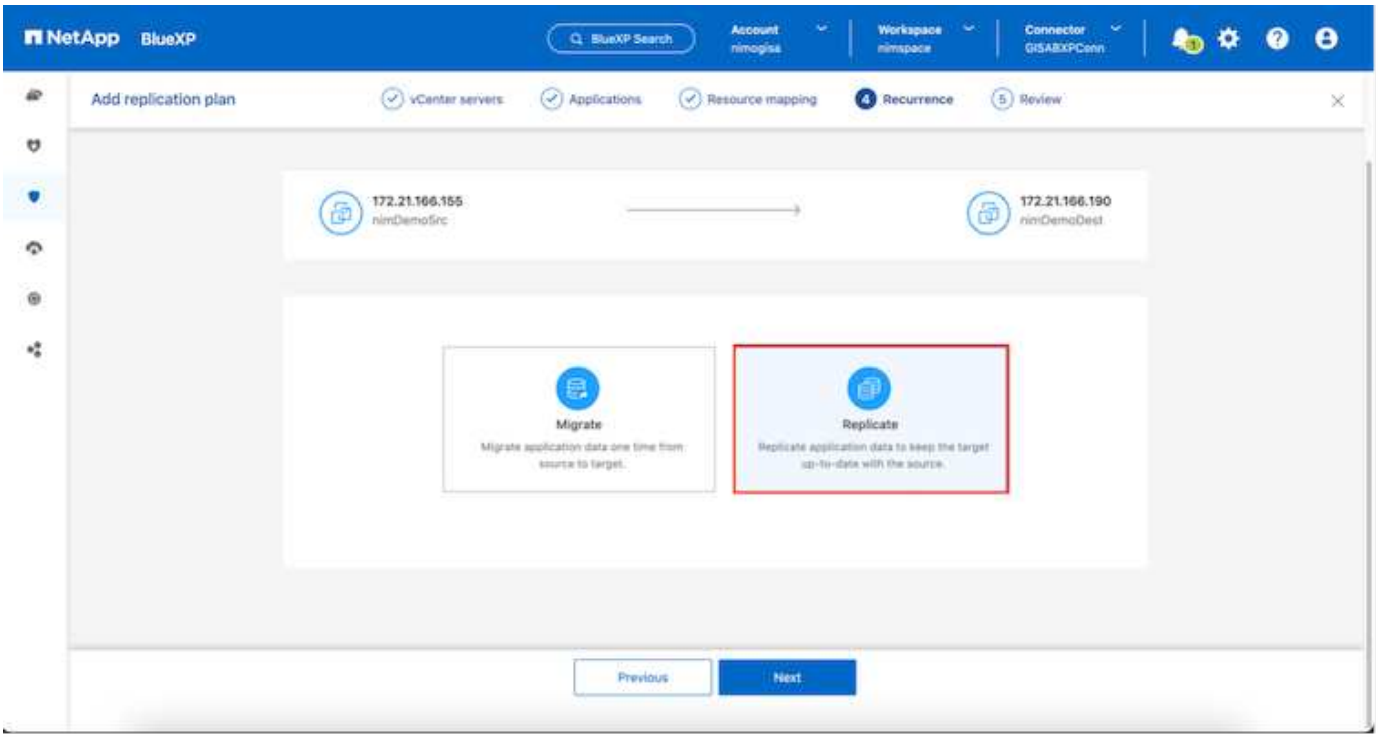
기본적으로 테스트 작업과 장애 조치 작업 모두에 동일한 매핑 매개변수가 사용됩니다. 테스트 환경에 다른 매핑을 적용하려면 아래와 같이 체크박스 선택을 해제한 후 테스트 매핑 옵션을 선택하세요.



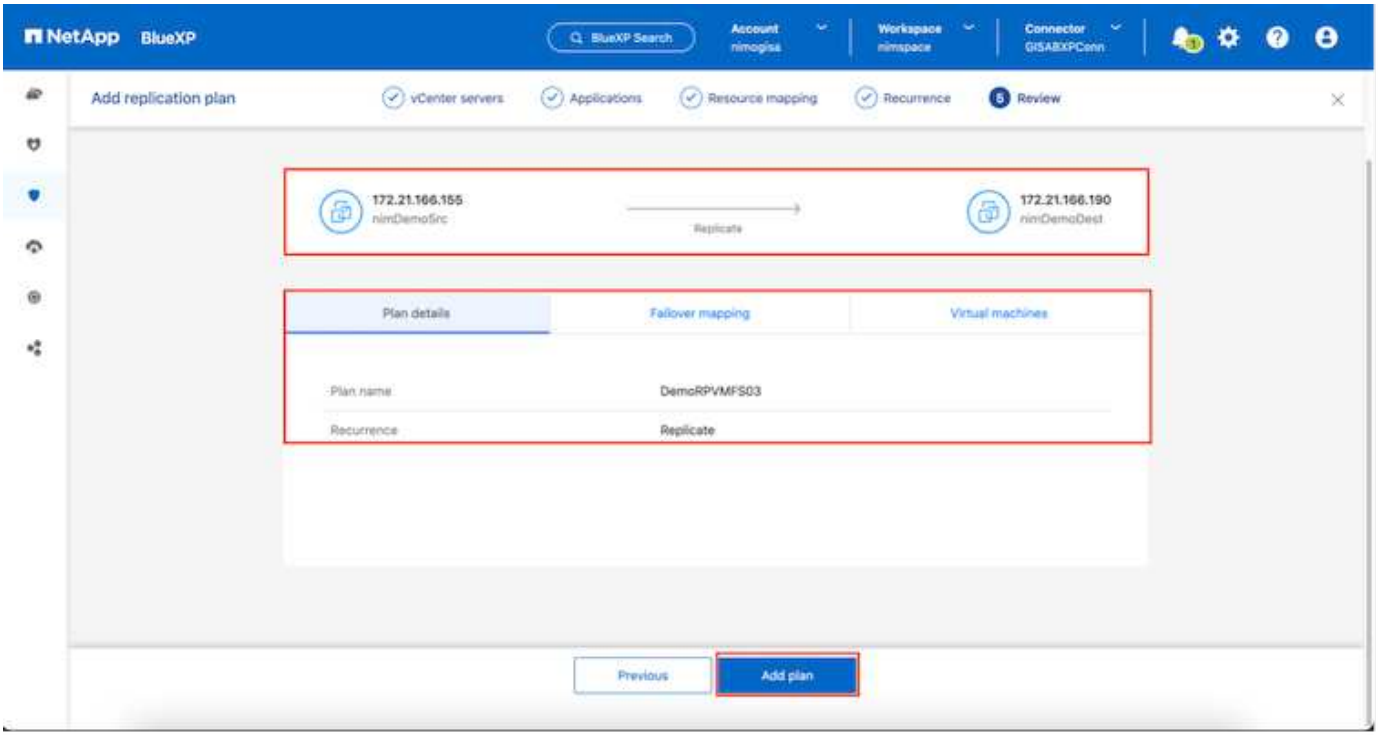
리소스 매핑이 완료되면 다음을 클릭합니다.

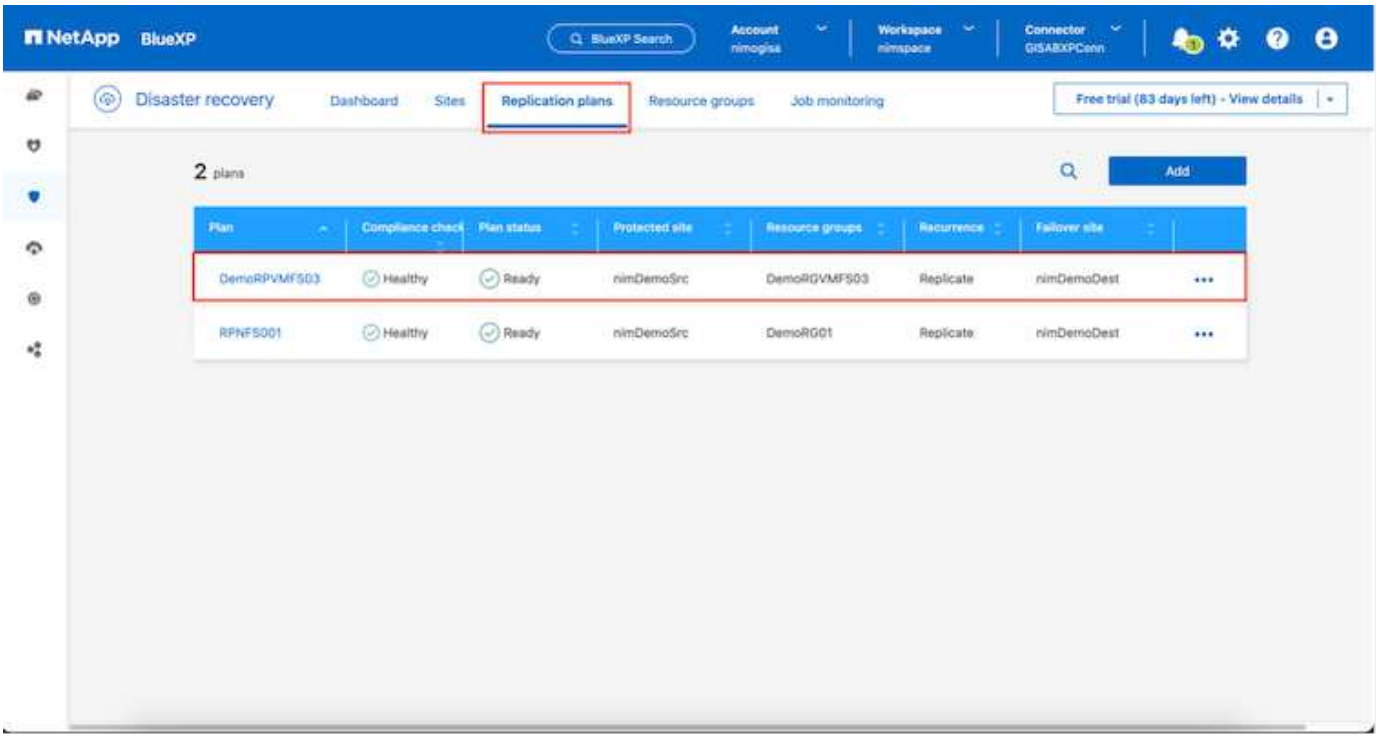


반복 유형을 선택하세요. 간단히 말해서, 마이그레이션(장애 조치를 사용한 일회성 마이그레이션) 또는 반복적 지속적 복제 옵션을 선택합니다. 이 연습에서는 복제 옵션이 선택되었습니다.

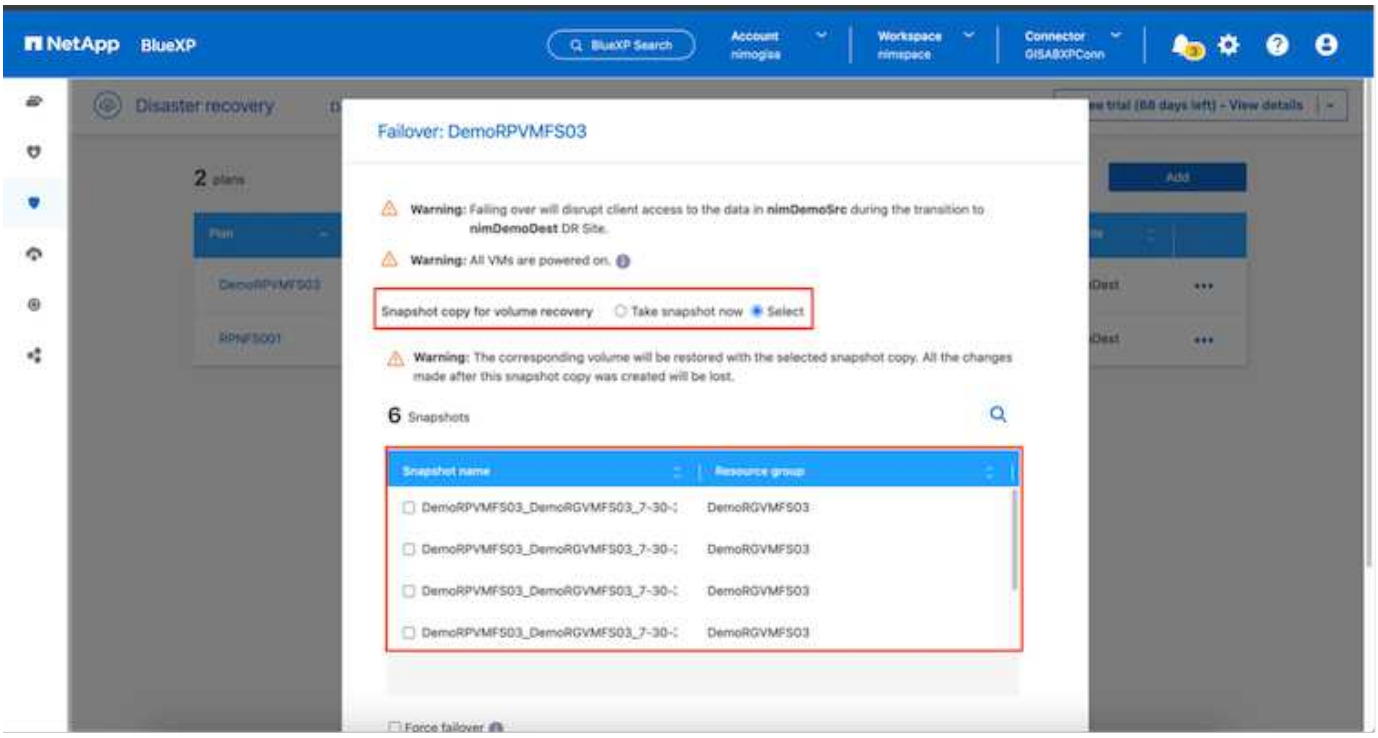


완료되면 생성된 매핑을 검토한 후 계획 추가를 클릭합니다.

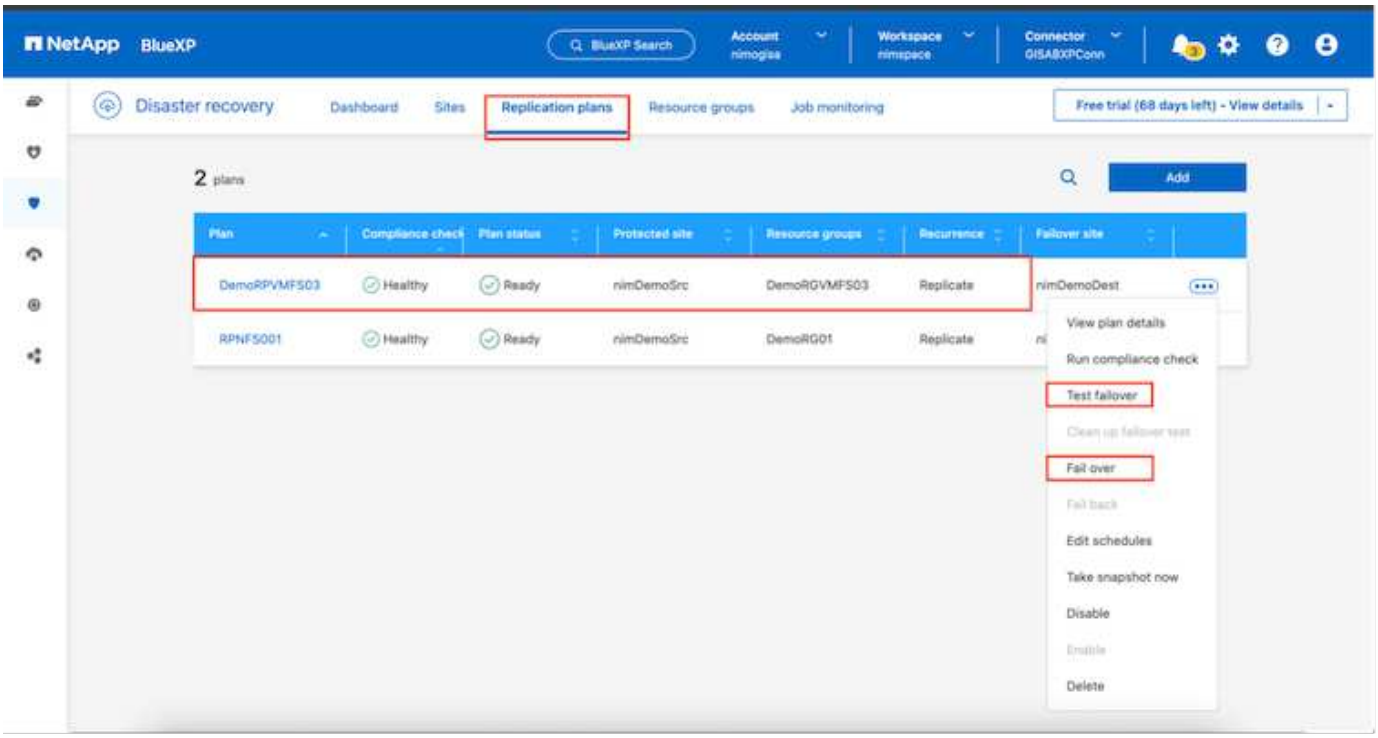




복제 계획이 생성되면 요구 사항에 따라 장애 조치 옵션, 테스트 장애 조치 옵션 또는 마이그레이션 옵션을 선택하여 장애 조치를 수행할 수 있습니다. BlueXP disaster recovery 복제 프로세스가 계획에 따라 30분마다 실행되도록 보장합니다. 장애 조치 및 테스트 장애 조치 옵션 동안 가장 최근의 SnapMirror 스냅샷 복사본을 사용할 수도 있고, SnapMirror 의 보존 정책에 따라 특정 시점 스냅샷 복사본에서 특정 스냅샷 복사본을 선택할 수도 있습니다. 랜섬웨어와 같이 최신 복제본이 이미 손상되거나 암호화된 경우와 같이 손상 이벤트가 발생한 경우 특정 시점 옵션이 매우 유용할 수 있습니다. BlueXP disaster recovery 사용 가능한 모든 복구 지점을 보여줍니다.



복제 계획에 지정된 구성으로 장애 조치 또는 테스트 장애 조치를 트리거하려면 장애 조치 또는 *테스트 장애 조치*를 클릭합니다.

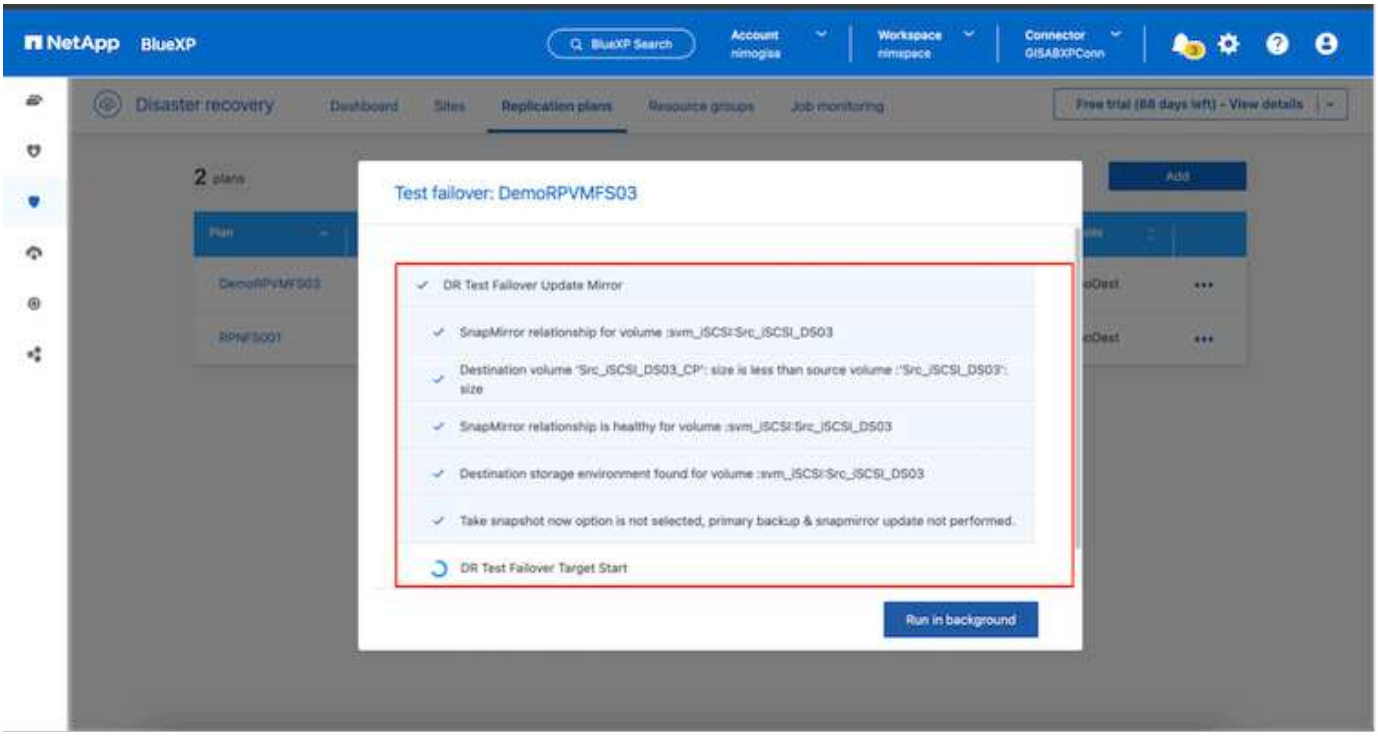


장애 조치 또는 테스트 장애 조치 작업 중에는 무슨 일이 일어나나요?

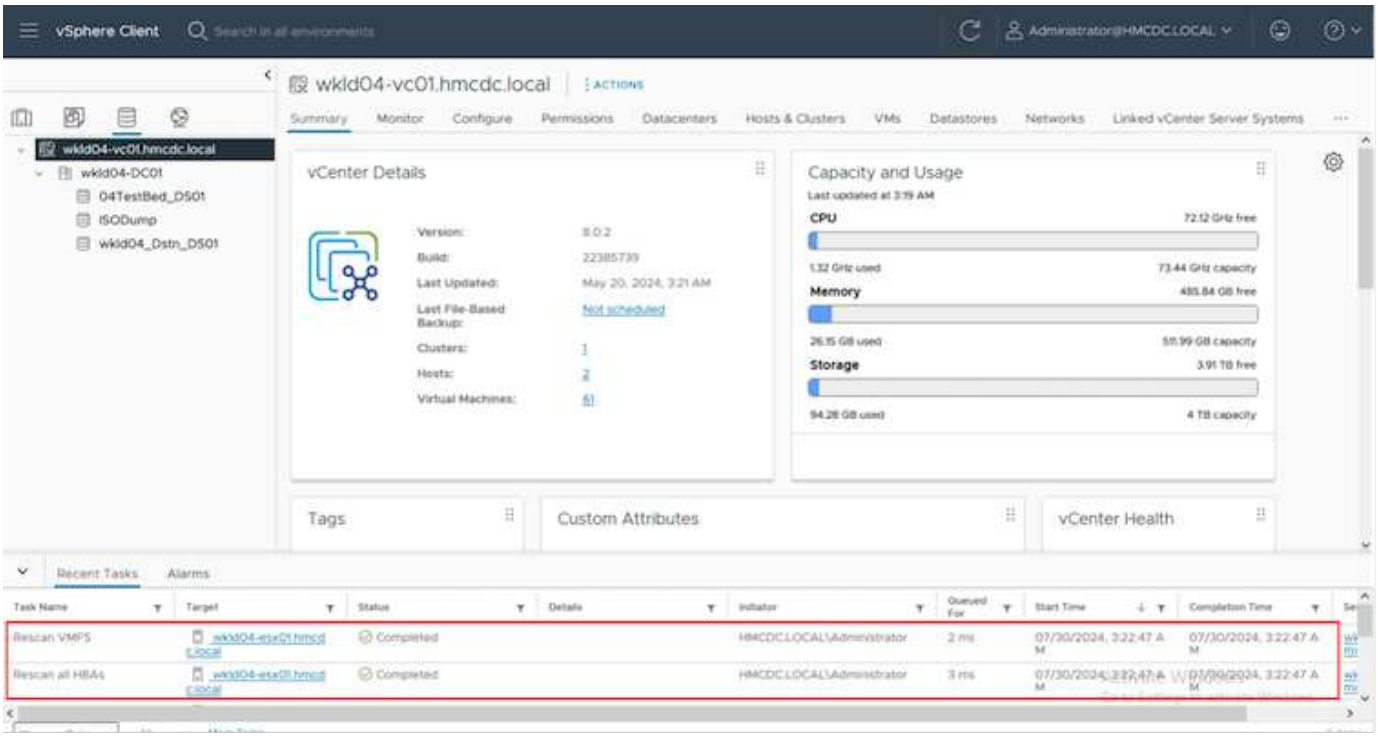
테스트 장애 조치 작업 중에 BlueXP disaster recovery 최신 스냅샷 복사본이나 대상 볼륨의 선택한 스냅샷을 사용하여 대상 ONTAP 스토리지 시스템에 FlexClone 볼륨을 생성합니다.

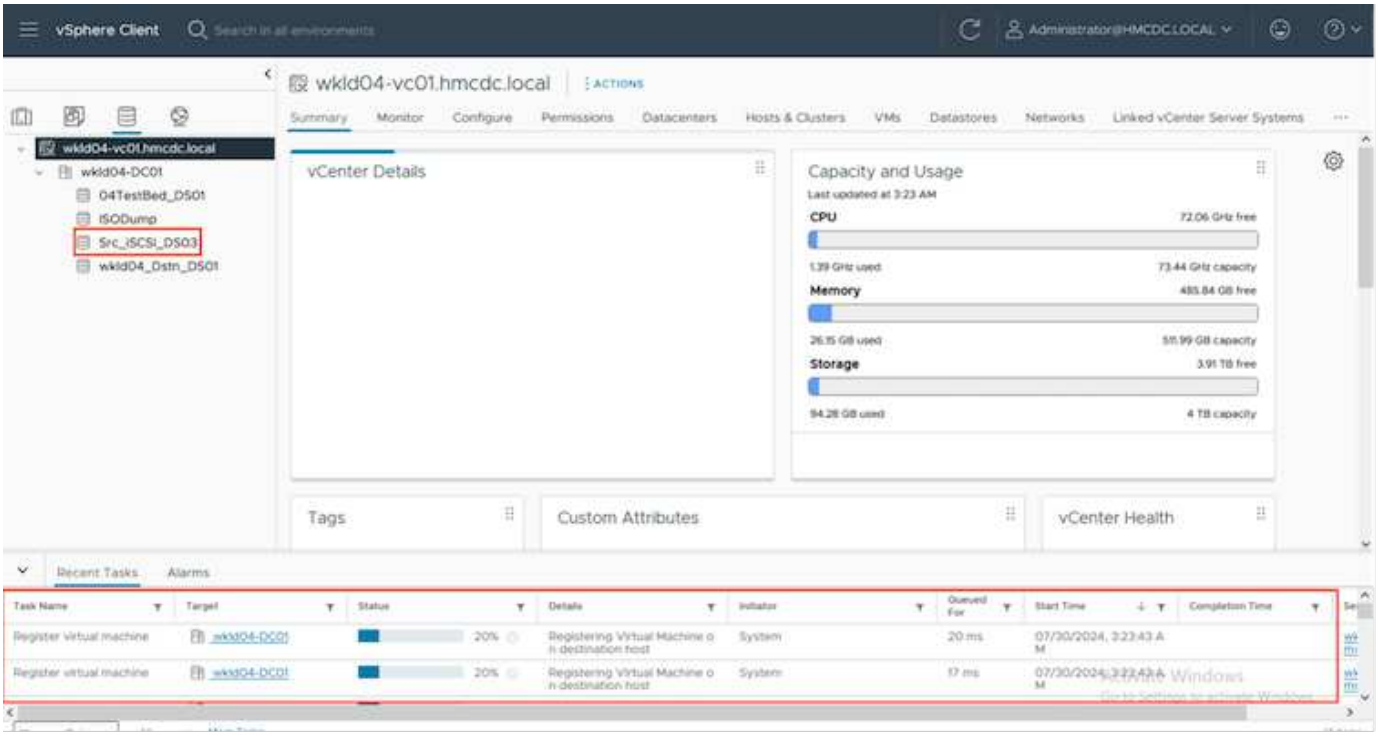
ⓘ 테스트 장애 조치 작업은 대상 ONTAP 스토리지 시스템에 복제된 볼륨을 생성합니다.

ⓘ 테스트 복구 작업을 실행해도 SnapMirror 복제에는 영향을 미치지 않습니다.



이 과정에서 BlueXP disaster recovery 원래 대상 볼륨을 매핑하지 않습니다. 대신, 선택한 스냅샷에서 새로운 FlexClone 볼륨을 만들고 FlexClone 볼륨을 백업하는 임시 데이터 저장소를 ESXi 호스트에 매핑합니다.



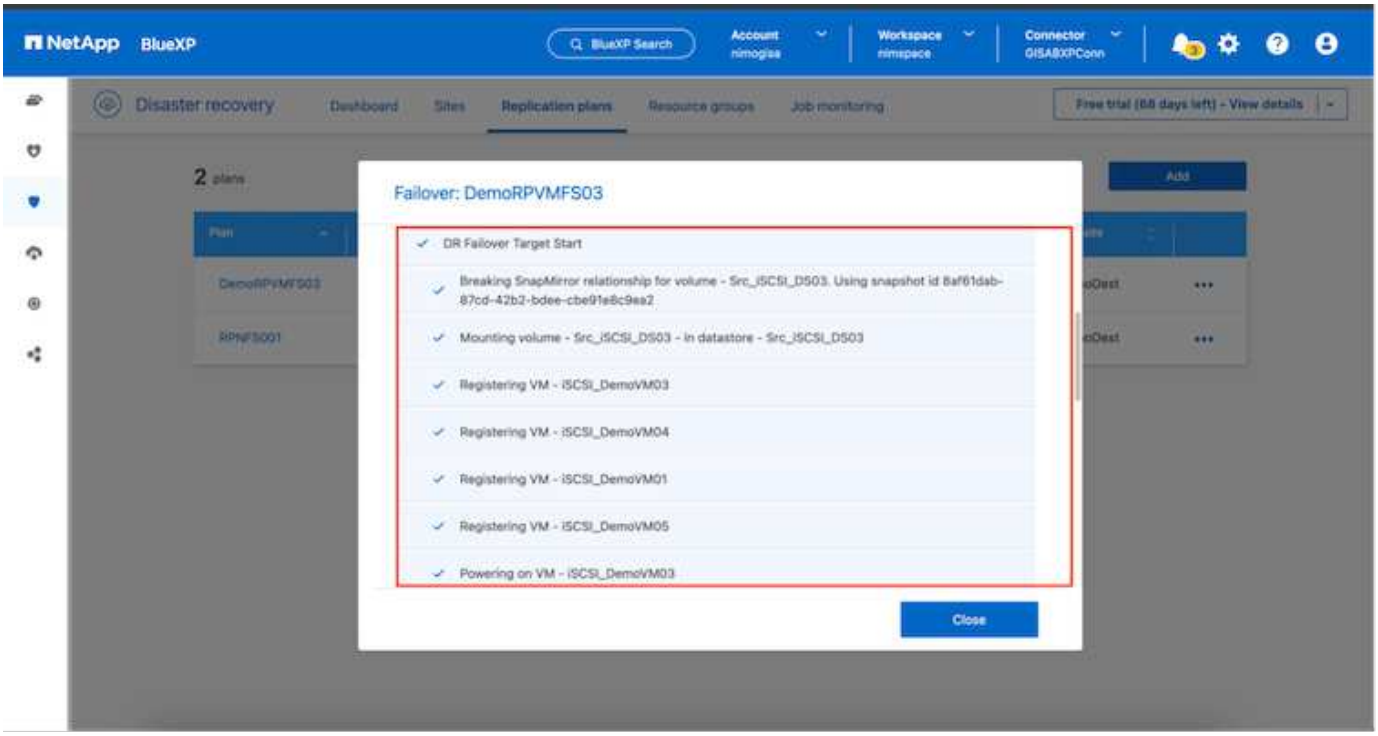


테스트 장애 조치 작업이 완료되면 "장애 조치 테스트 정리"를 사용하여 정리 작업을 트리거할 수 있습니다. 이 작업 중에 BlueXP disaster recovery 작업에 사용된 FlexClone 볼륨을 파괴합니다.

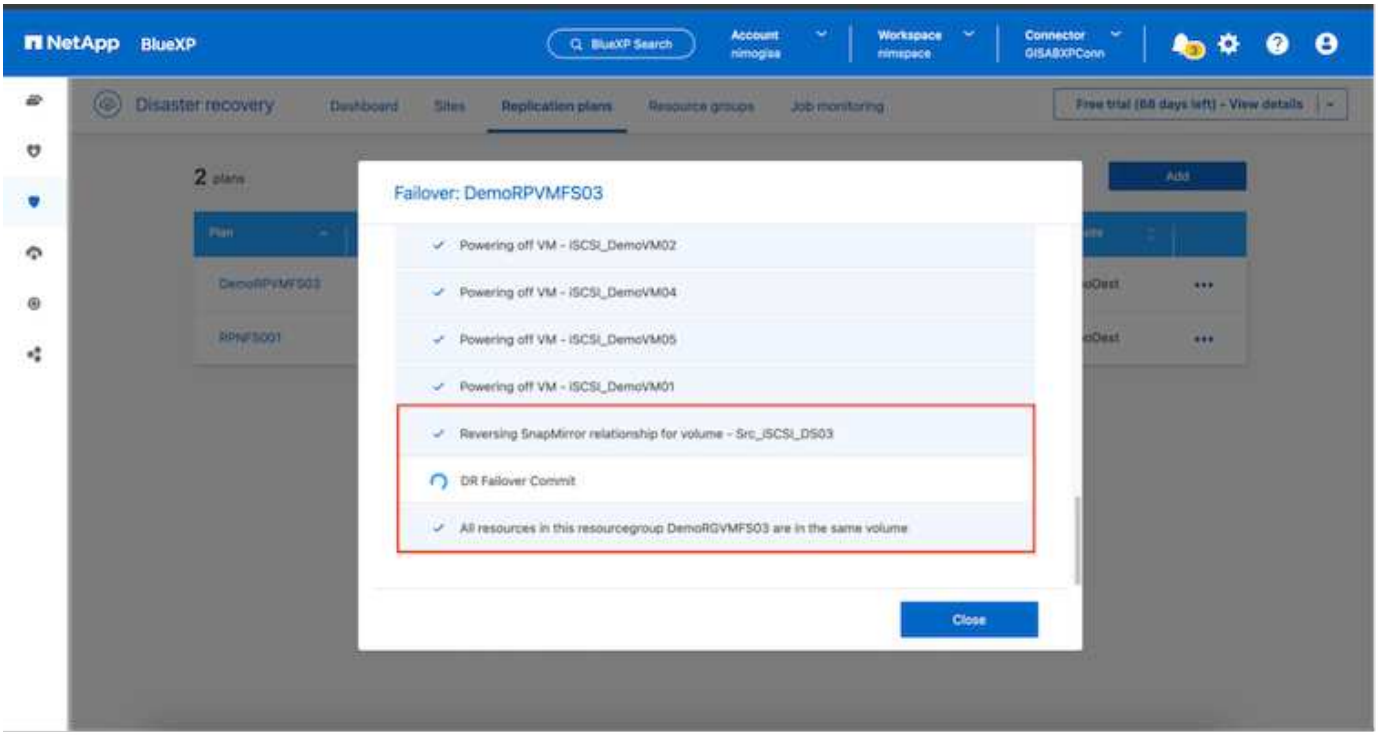
실제 재해가 발생하는 경우 BlueXP disaster recovery 다음 단계를 수행합니다.

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



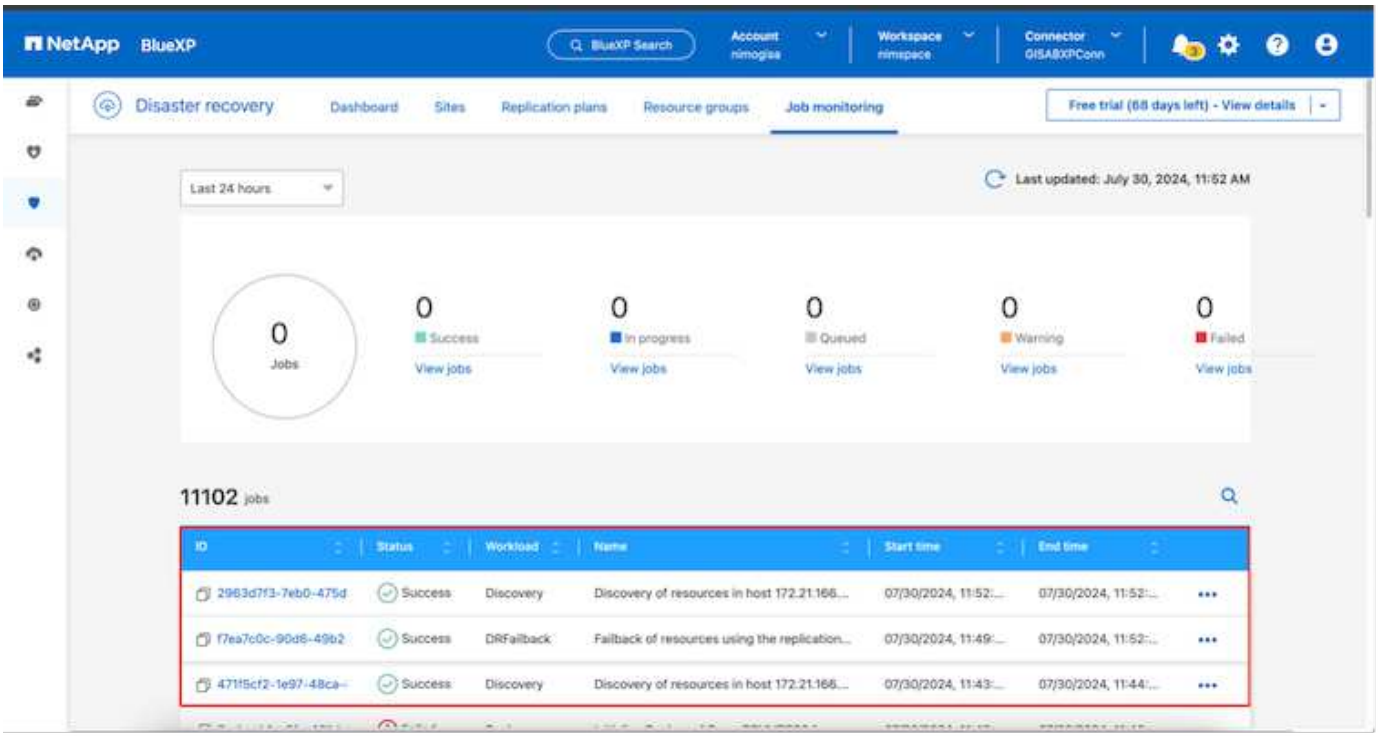
기본 사이트가 가동되면 BlueXP disaster recovery 통해 SnapMirror 에 대한 역방향 재동기화가 가능하고 장애 복구도 가능하며, 이 역시 버튼을 클릭하기만 하면 수행할 수 있습니다.



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.

BlueXP 또는 ONTAP CLI에서 해당 데이터 저장소 볼륨에 대한 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" .

BlueXP disaster recovery 사용하여 NFS 데이터 저장소에 대한 재해 복구 설정

이 사용 사례에서는 NFS 데이터 저장소를 사용하여 온프레미스 VMware VM에 대한 BlueXP disaster recovery 사용하여 재해 복구를 설정하는 절차를 설명합니다. 이 절차에는 BlueXP 계정과 커넥터 설정, VMware vCenter와 ONTAP 스토리지 간 통신을 활성화하기 위한 ONTAP 어레이 추가, 사이트 간 복제 구성, 복구 계획 생성 및 테스트가 포함됩니다.

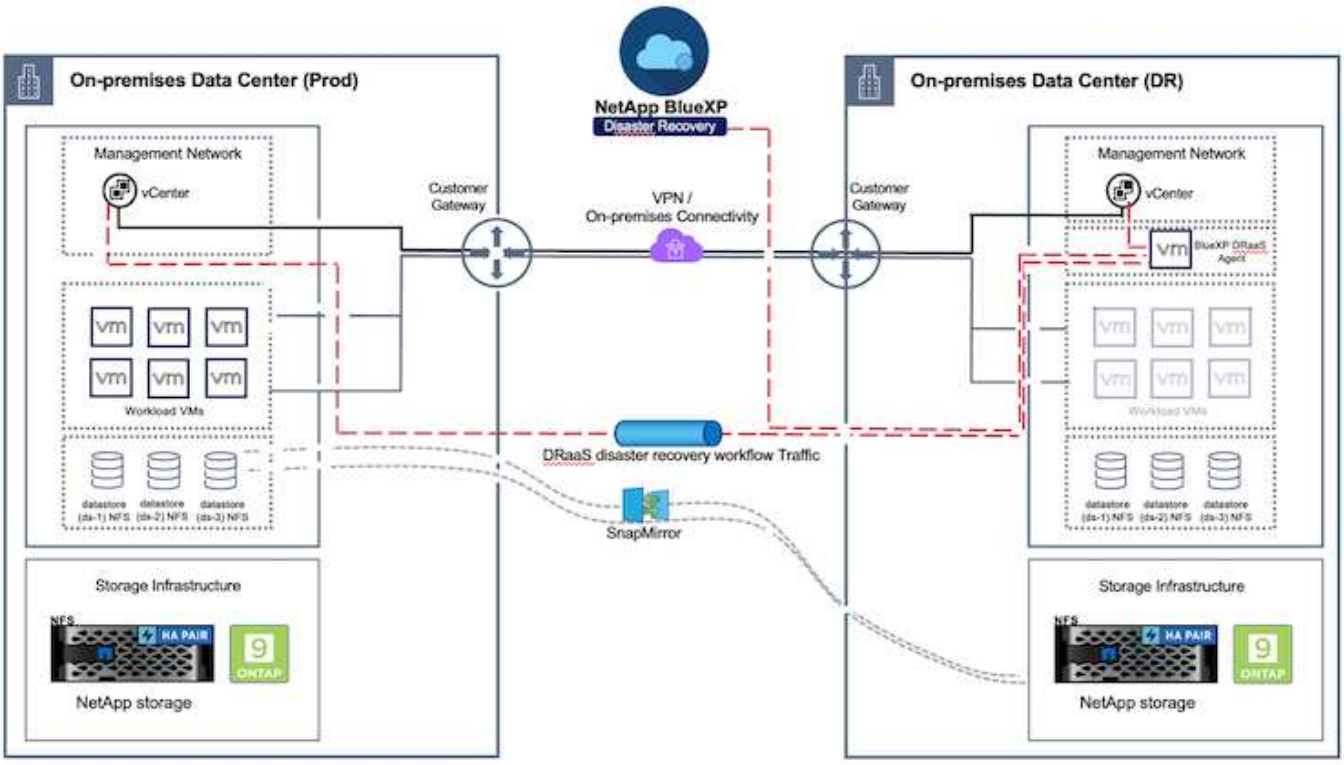
운영 사이트에서 재해 복구 사이트로 블록 수준 복제를 통해 재해 복구를 구현하는 것은 랜섬웨어 공격과 같은 사이트 중단 및 데이터 손상 이벤트로부터 작업 부하를 보호하는 탄력적이고 비용 효율적인 방법입니다. NetApp SnapMirror 복제를 사용하면 NFS 데이터 저장소가 있는 온프레미스 ONTAP 시스템에서 실행되는 VMware 워크로드를 VMware가 배포된 지정된 복구 데이터 센터에 있는 다른 ONTAP 스토리지 시스템으로 복제할 수 있습니다.

소개

이 문서의 섹션에서는 온프레미스 VMware VM을 다른 지정된 사이트로 재해 복구하도록 BlueXP DRaaS를 구성하는 방법을 설명합니다. 이 설정의 일부로 BlueXP 계정, BlueXP 커넥터, BlueXP 작업 공간 내에 추가된 ONTAP 어레이는 VMware vCenter에서 ONTAP 스토리지로의 통신을 활성화하는 데 필요합니다. 또한, 이 문서에서는 사이트 간 복제를 구성하는 방법과 복구 계획을 설정하고 테스트하는 방법에 대해 자세히 설명합니다. 마지막 섹션에는 전체 사이트 장애 조치를 수행하는 방법과 기본 사이트가 복구되어 온라인으로 전환되었을 때 장애 복구하는 방법에 대한 지침이 나와 있습니다.

NetApp BlueXP 콘솔에 통합된 BlueXP disaster recovery 서비스를 활용하면 회사에서는 온프레미스 VMware vCenter와 ONTAP 스토리지를 쉽게 찾을 수 있습니다. 그러면 조직에서는 리소스 그룹을 만들고, 재해 복구 계획을 수립하고, 이를 리소스 그룹과 연결하고, 장애 조치(failover) 및 장애 복구(failback)를 테스트하거나 실행할 수 있습니다. SnapMirror 두 사이트를 증분적 변경 사항으로 최신 상태로 유지하기 위해 스토리지 수준 블록 복제를 제공하며, 이를 통해 최대 5분의 복구 지점 목표(RPO)를 달성합니다. 또한, 생산에 영향을 주거나 추가적인 보관 비용을 발생시키지 않고도 재해 복구 절차를 시뮬레이션할 수 있습니다.

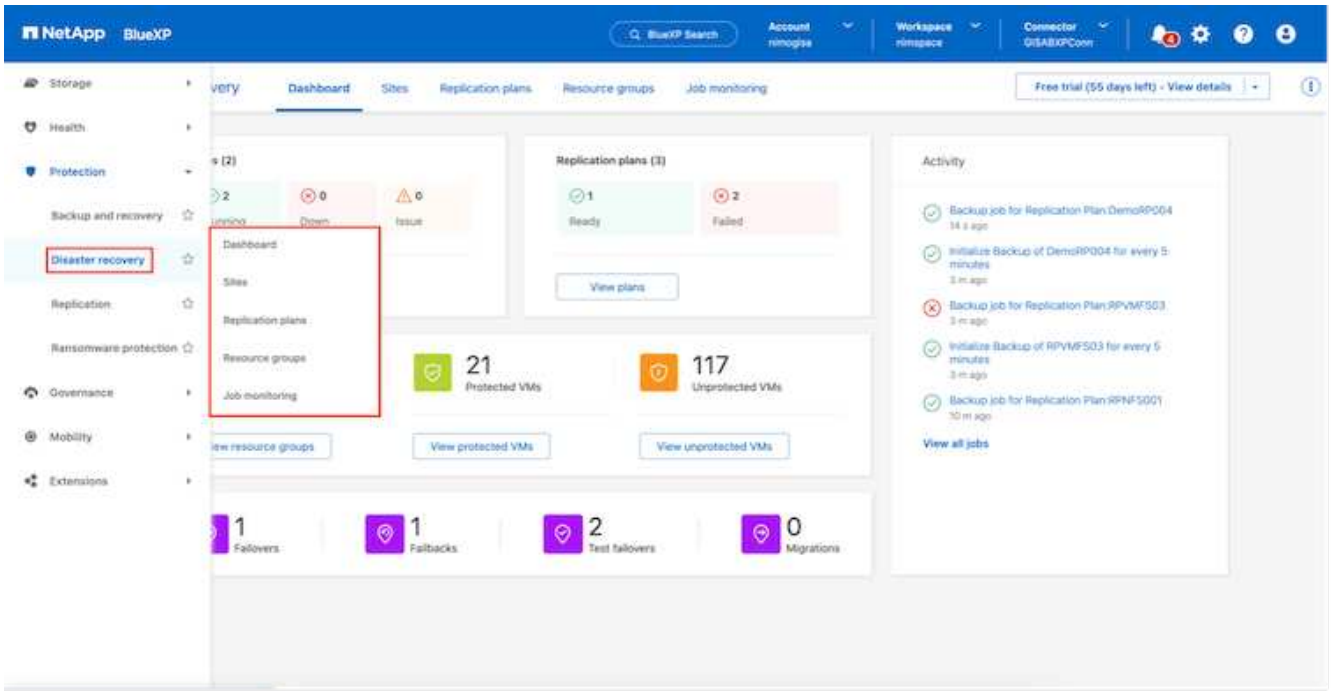
BlueXP disaster recovery ONTAP의 FlexClone 기술을 활용하여 재해 복구 사이트에서 마지막으로 복제된 스냅샷의 NFS 데이터 저장소의 공간 효율적인 복사본을 생성합니다. 재해 복구 테스트를 완료한 후, 고객은 실제 복제된 프로덕션 리소스에 영향을 주지 않고 테스트 환경을 쉽게 삭제할 수 있습니다. 실제로 장애 조치가 발생하는 경우 BlueXP disaster recovery 서비스는 단 몇 번의 클릭만으로 지정된 재해 복구 사이트에서 보호된 가상 머신을 자동으로 불러오기 위해 필요한 모든 단계를 조율합니다. 이 서비스는 또한 필요한 경우 장애 복구 작업을 위해 SnapMirror 와 기본 사이트의 관계를 역전시키고 보조 사이트의 변경 사항을 기본 사이트로 복제합니다. 이러한 모든 기능은 다른 잘 알려진 대안과 비교했을 때 비용이 훨씬 저렴합니다.



시작하기

BlueXP disaster recovery 시작하려면 BlueXP 콘솔을 사용한 다음 서비스에 액세스하세요.

1. BlueXP 에 로그인하세요.
2. BlueXP 왼쪽 탐색 창에서 보호 > 재해 복구를 선택합니다.
3. BlueXP disaster recovery 보드가 나타납니다.

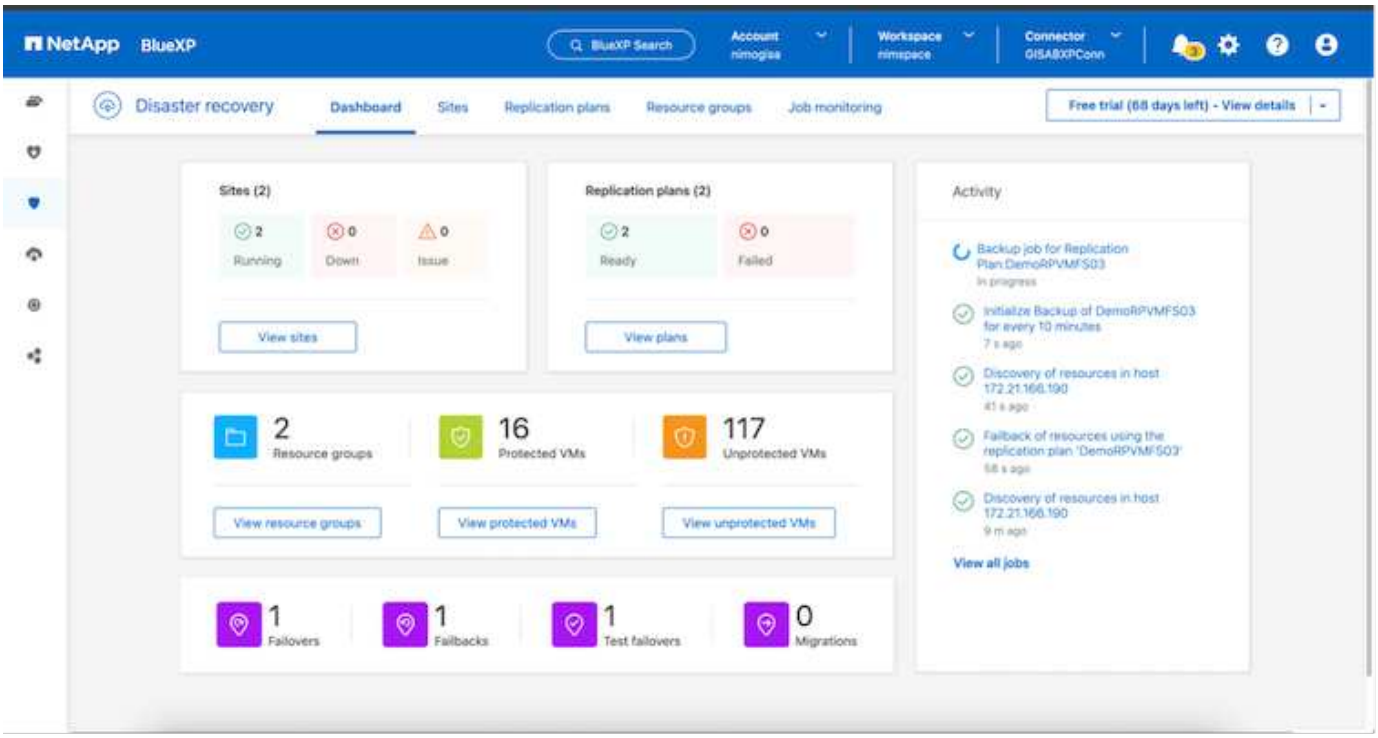


재해 복구 계획을 구성하기 전에 다음 전제 조건이 충족되었는지 확인하세요.

- BlueXP Connector는 NetApp BlueXP 에 설정되어 있습니다.
- BlueXP 커넥터 인스턴스는 소스 및 대상 vCenter와 스토리지 시스템에 연결할 수 있습니다.
- NetApp Data ONTAP 클러스터는 NFS 데이터 저장소를 제공합니다.
- VMware용 NFS 데이터 저장소를 호스팅하는 온프레미스 NetApp 스토리지 시스템이 BlueXP 에 추가되었습니다.
- 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.

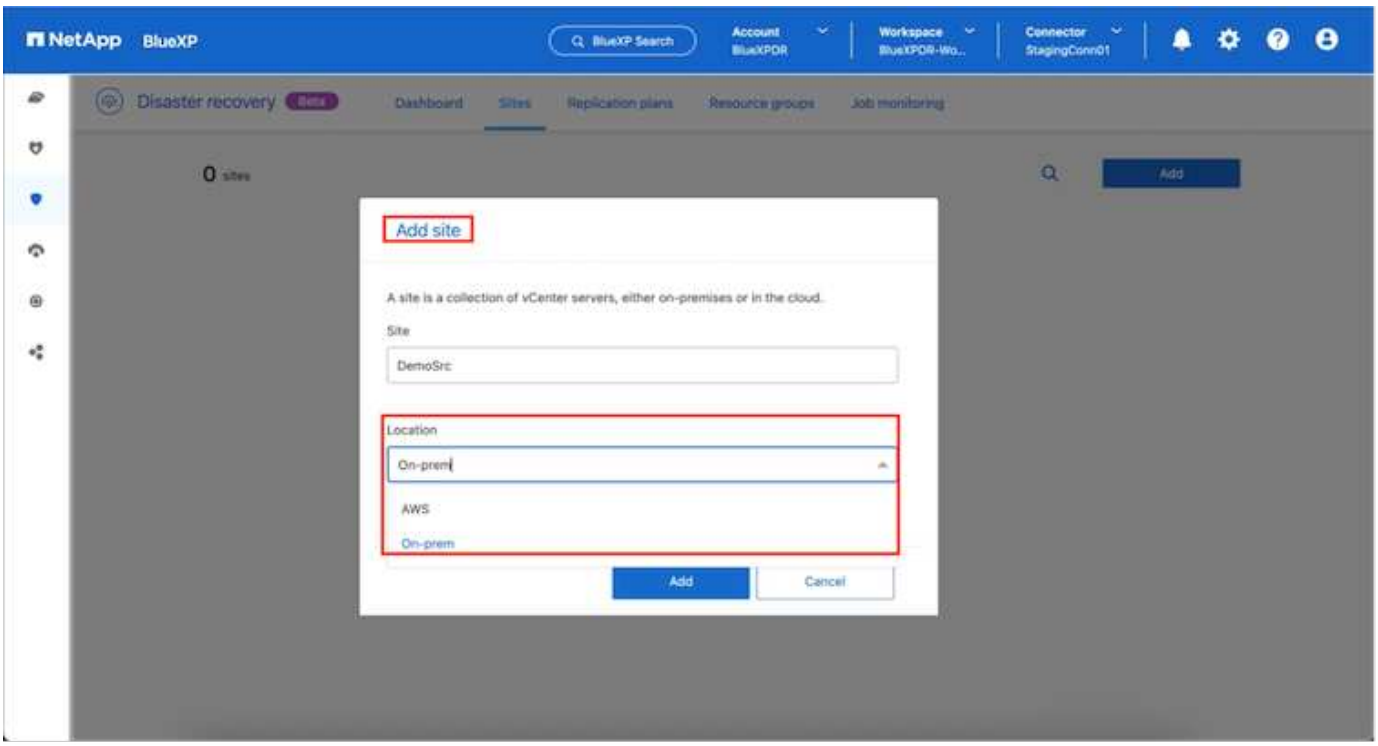
NetApp BlueXP BlueXP 를 배포할 것을 권장합니다.



BlueXP disaster recovery 구성

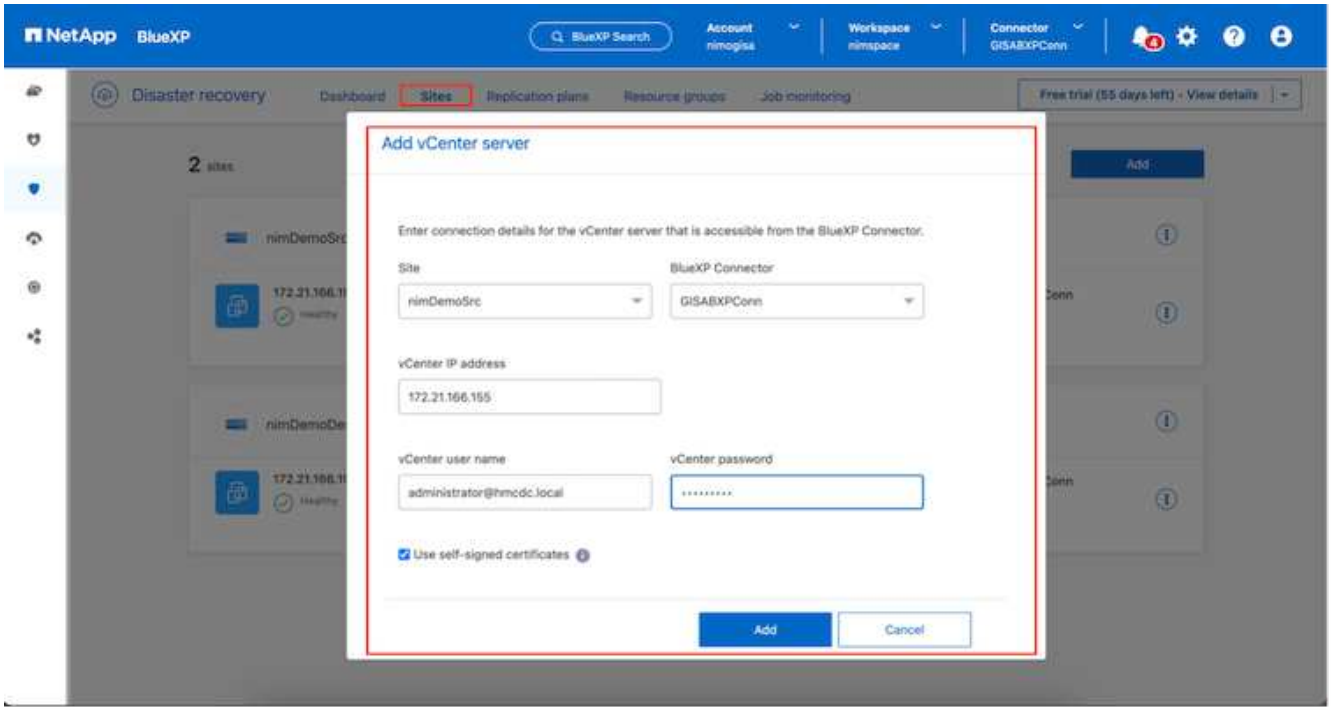
재해 복구를 준비하는 첫 번째 단계는 온프레미스 vCenter 및 스토리지 리소스를 검색하여 BlueXP disaster recovery에 추가하는 것입니다.

BlueXP 콘솔을 열고 왼쪽 탐색에서 *보호 > 재해 복구*를 선택합니다. *vCenter 서버 검색*을 선택하거나 상단 메뉴를 사용하여 *사이트 > 추가 > vCenter 추가*를 선택합니다.

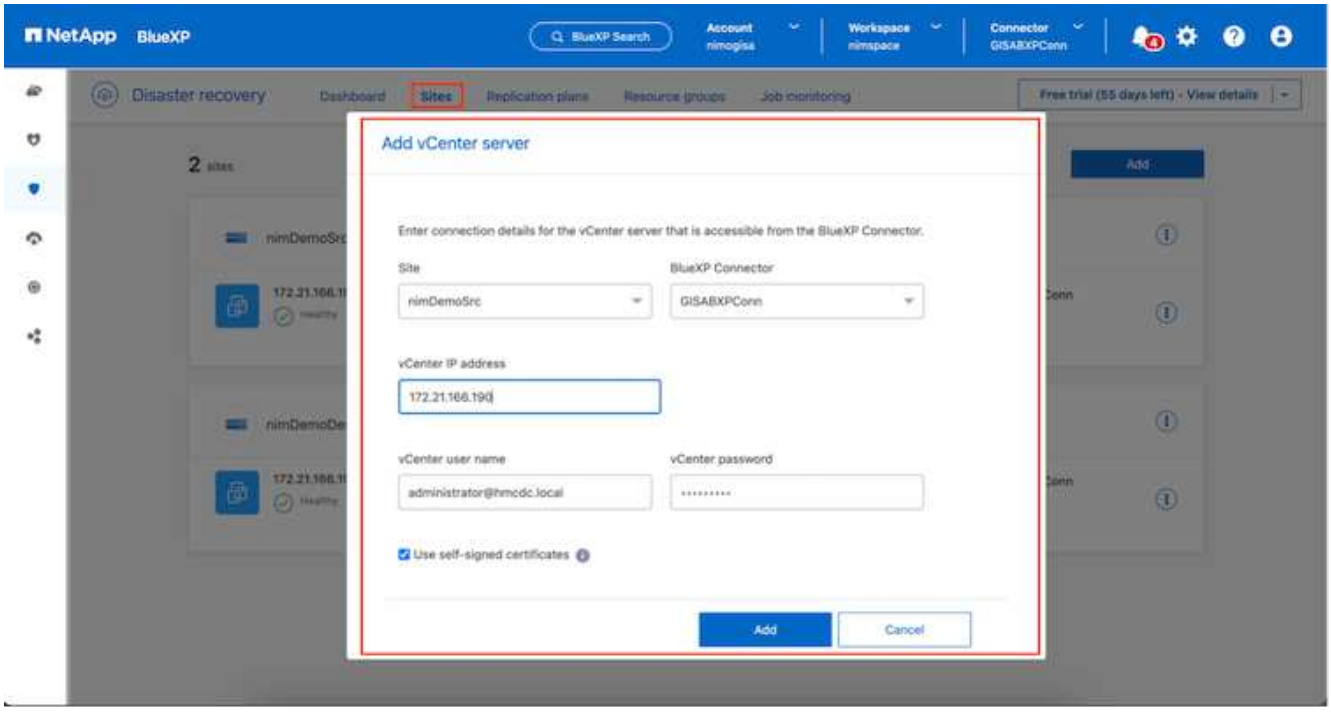


다음 플랫폼을 추가하세요:

- 원천. 온프레미스 vCenter.



- 목적지. VMC SDDC vCenter.



vCenter가 추가되면 자동 검색이 실행됩니다.

소스 사이트 배열과 대상 사이트 배열 간 스토리지 복제 구성

SnapMirror NetApp 환경에서 데이터 복제를 제공합니다. NetApp Snapshot 기술을 기반으로 구축된 SnapMirror 복제는 이전 업데이트 이후 변경되거나 추가된 블록만 복제하므로 매우 효율적입니다. SnapMirror NetApp

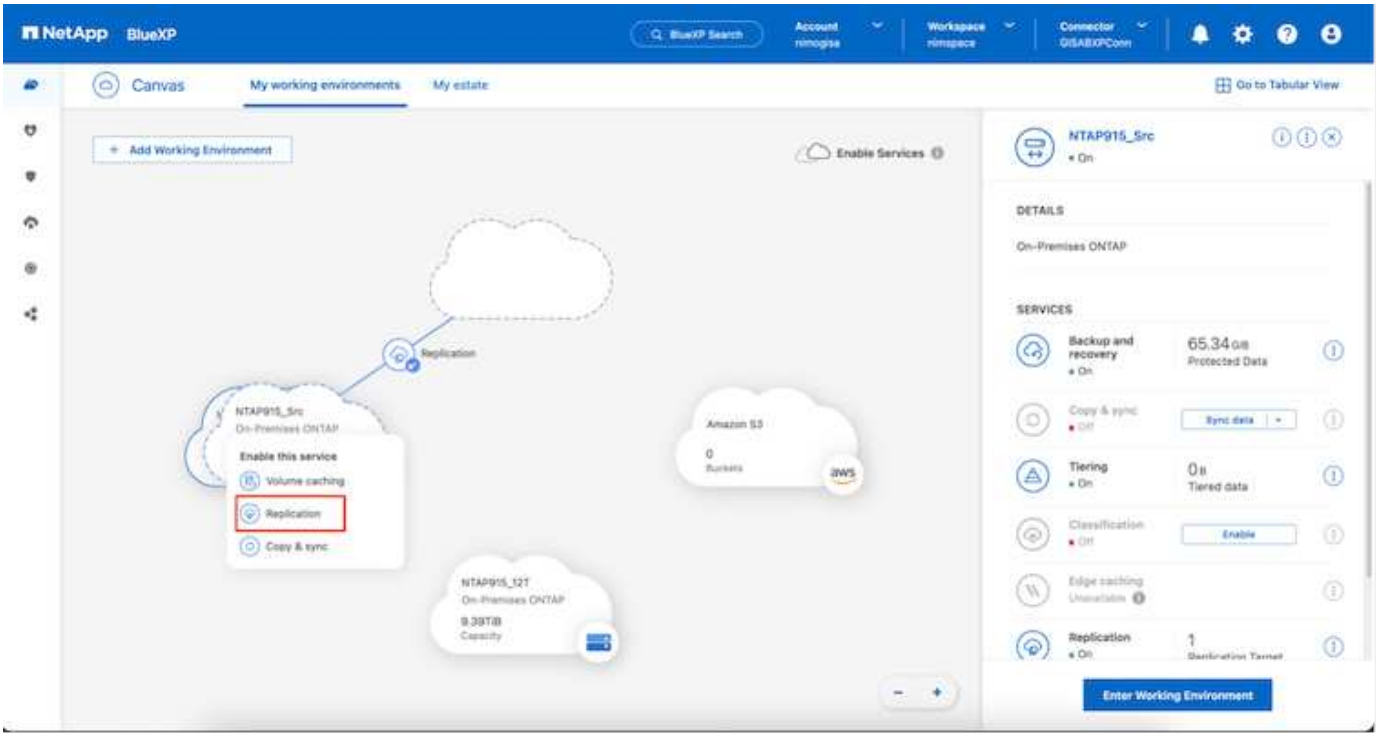
OnCommand System Manager 나 ONTAP CLI를 사용하여 쉽게 구성할 수 있습니다. BlueXP DRaaS는 클러스터와 SVM 피어링이 사전에 구성된 경우 SnapMirror 관계도 생성합니다.

기본 스토리지가 완전히 손실되지 않은 경우 SnapMirror 기본 사이트와 DR 사이트를 다시 동기화하는 효율적인 수단을 제공합니다. SnapMirror 두 사이트를 다시 동기화하여 SnapMirror 관계를 간단히 반대로 하여 DR 사이트에서 기본 사이트로 변경된 데이터나 새 데이터만 전송할 수 있습니다. 즉, BlueXP DRaaS의 복제 계획은 장애 조치 후 전체 볼륨을 다시 복사하지 않고도 어느 방향으로든 다시 동기화될 수 있습니다. 관계가 역방향으로 재동기화되는 경우 스냅샷 복사본의 마지막 성공적인 동기화 이후에 작성된 새 데이터만 대상으로 다시 전송됩니다.

> CLI 또는 시스템 관리자를 통해 볼륨에 대한 SnapMirror 관계가 이미 구성된 경우 BlueXP DRaaS는 해당 관계를 선택하고 나머지 워크플로 작업을 계속 진행합니다.

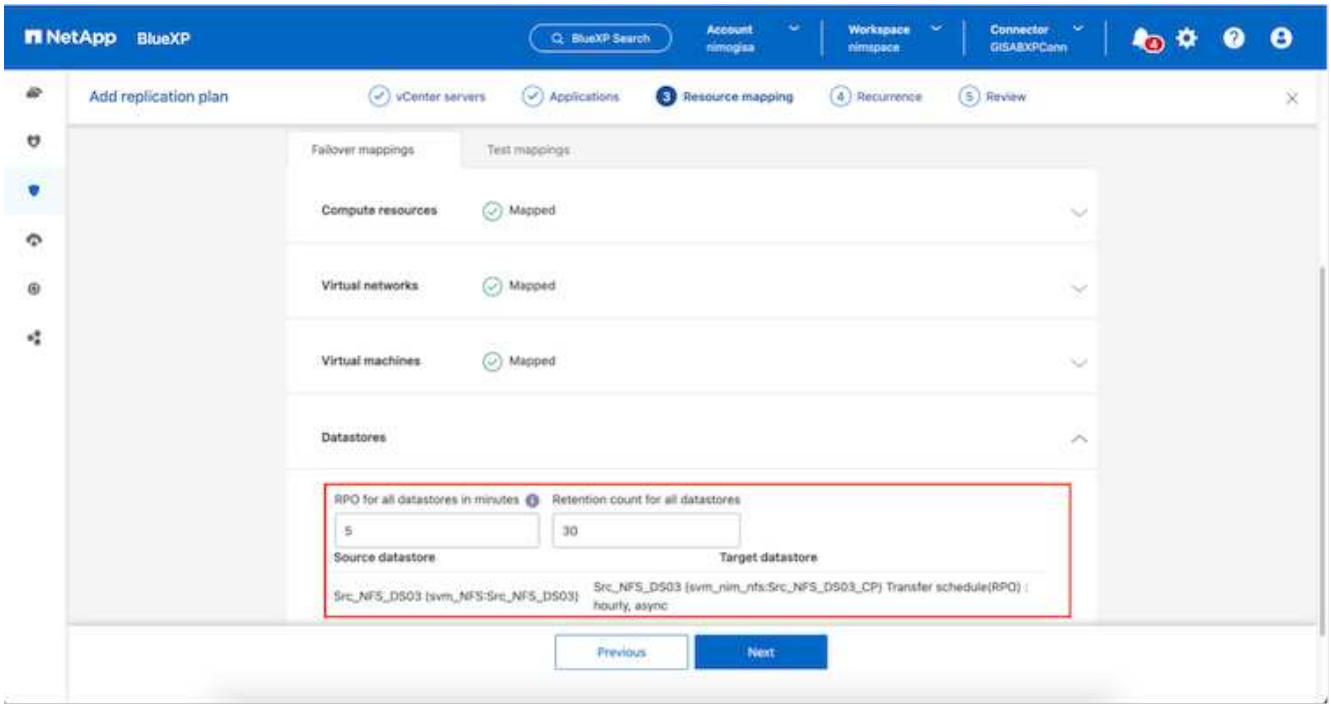
VMware 재해 복구를 설정하는 방법

SnapMirror 복제를 생성하는 프로세스는 모든 애플리케이션에서 동일하게 유지됩니다. 이 과정은 수동이거나 자동화될 수 있습니다. 가장 쉬운 방법은 BlueXP 활용하여 SnapMirror 복제를 구성하는 것입니다. 즉, 환경의 소스 ONTAP 시스템을 대상 환경으로 간단히 끌어서 놓아 나머지 프로세스를 안내하는 마법사를 실행하는 것입니다.



BlueXP DRaaS는 다음 두 가지 기준이 충족되는 경우 동일한 작업을 자동화할 수도 있습니다.

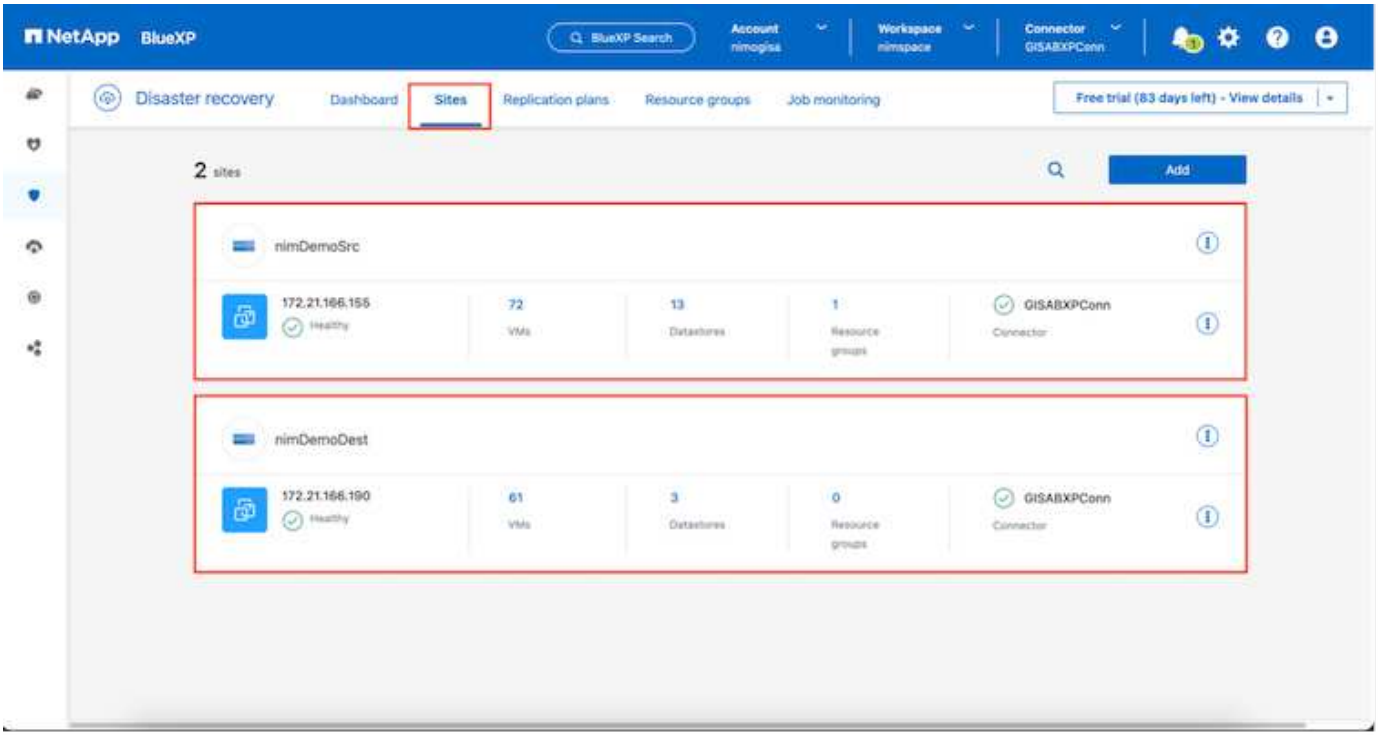
- 소스 클러스터와 대상 클러스터는 피어 관계를 갖습니다.
- 소스 SVM과 대상 SVM은 피어 관계를 갖습니다.



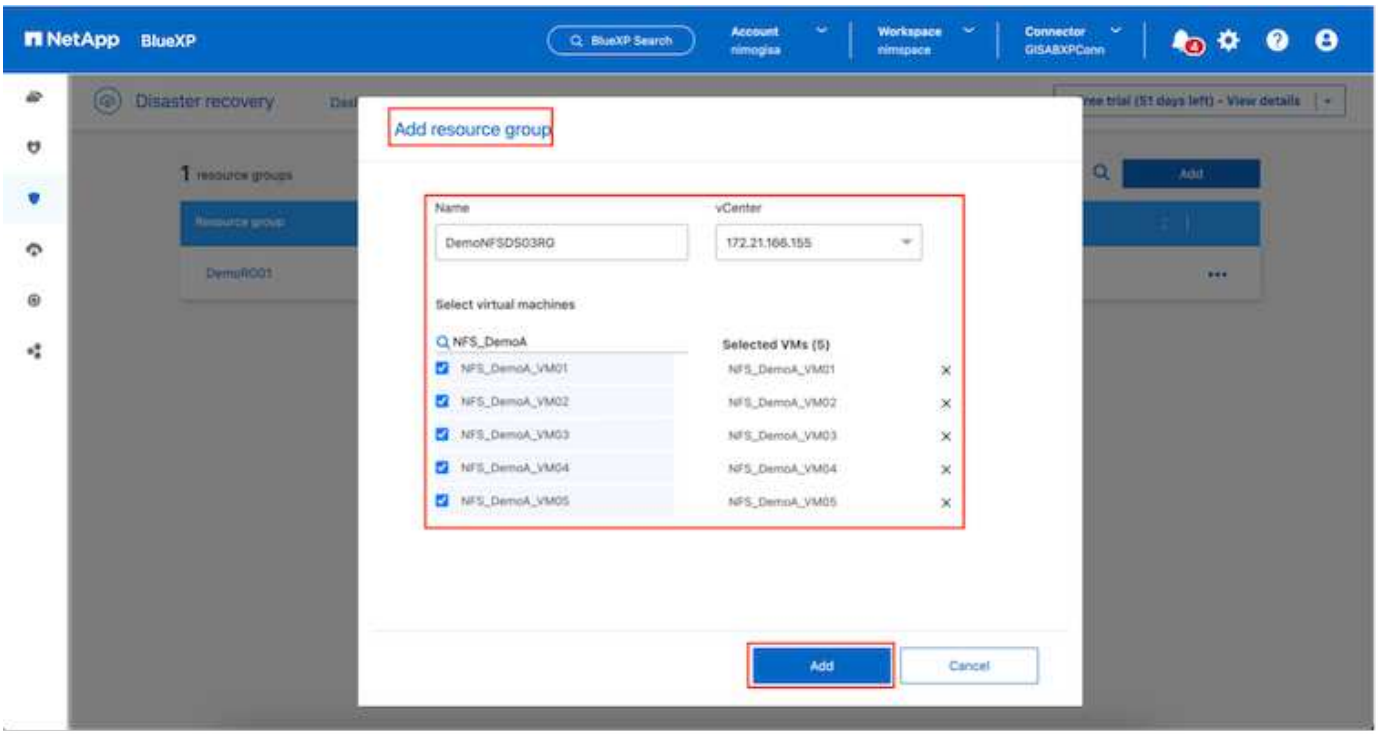
CLI를 통해 볼륨에 대한 SnapMirror 관계가 이미 구성된 경우 BlueXP DRaaS는 해당 관계를 선택하고 나머지 워크플로 작업을 계속 진행합니다.

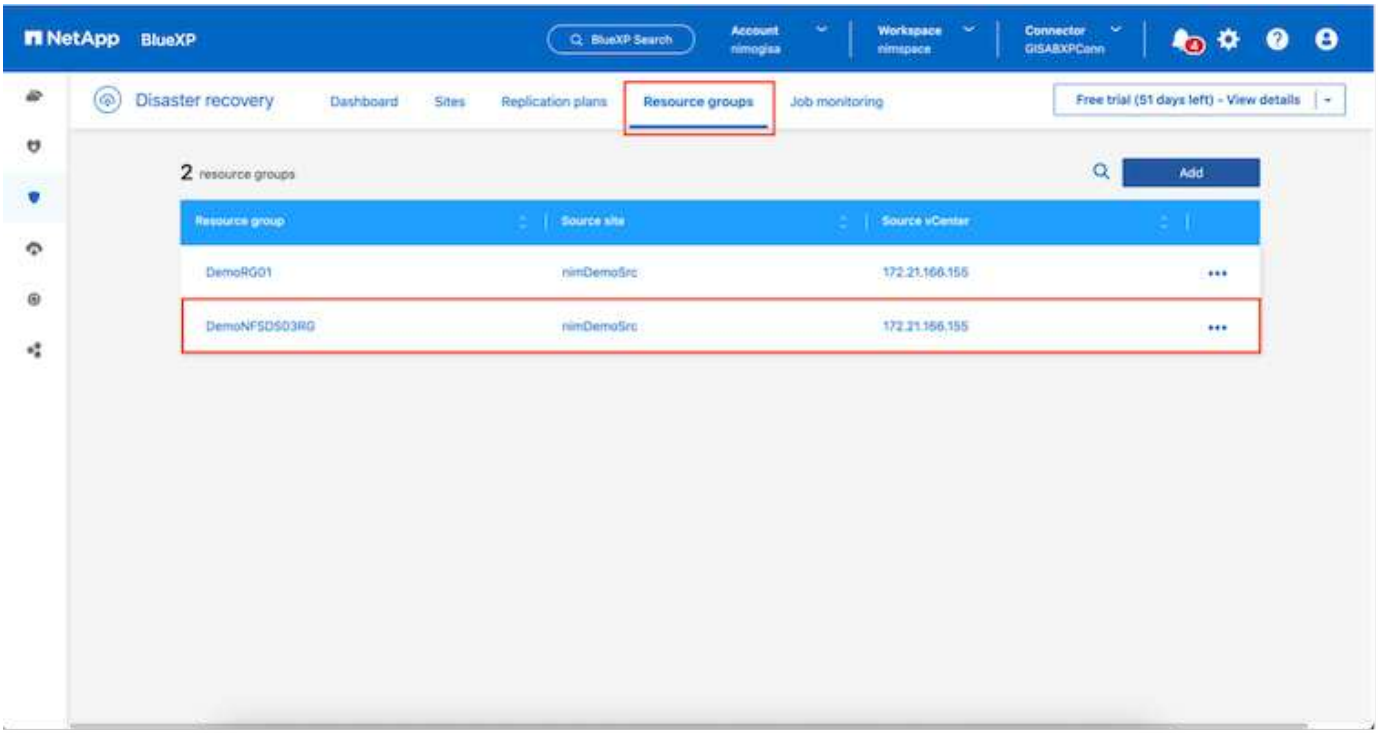
BlueXP disaster recovery 귀사를 위해 무엇을 해드릴 수 있나요**?**

소스 사이트와 대상 사이트가 추가되면 BlueXP disaster recovery 자동으로 심층 검색을 수행하고 관련 메타데이터와 함께 VM을 표시합니다. BlueXP disaster recovery 은 VM에서 사용하는 네트워크와 포트 그룹을 자동으로 감지하여 채웁니다.



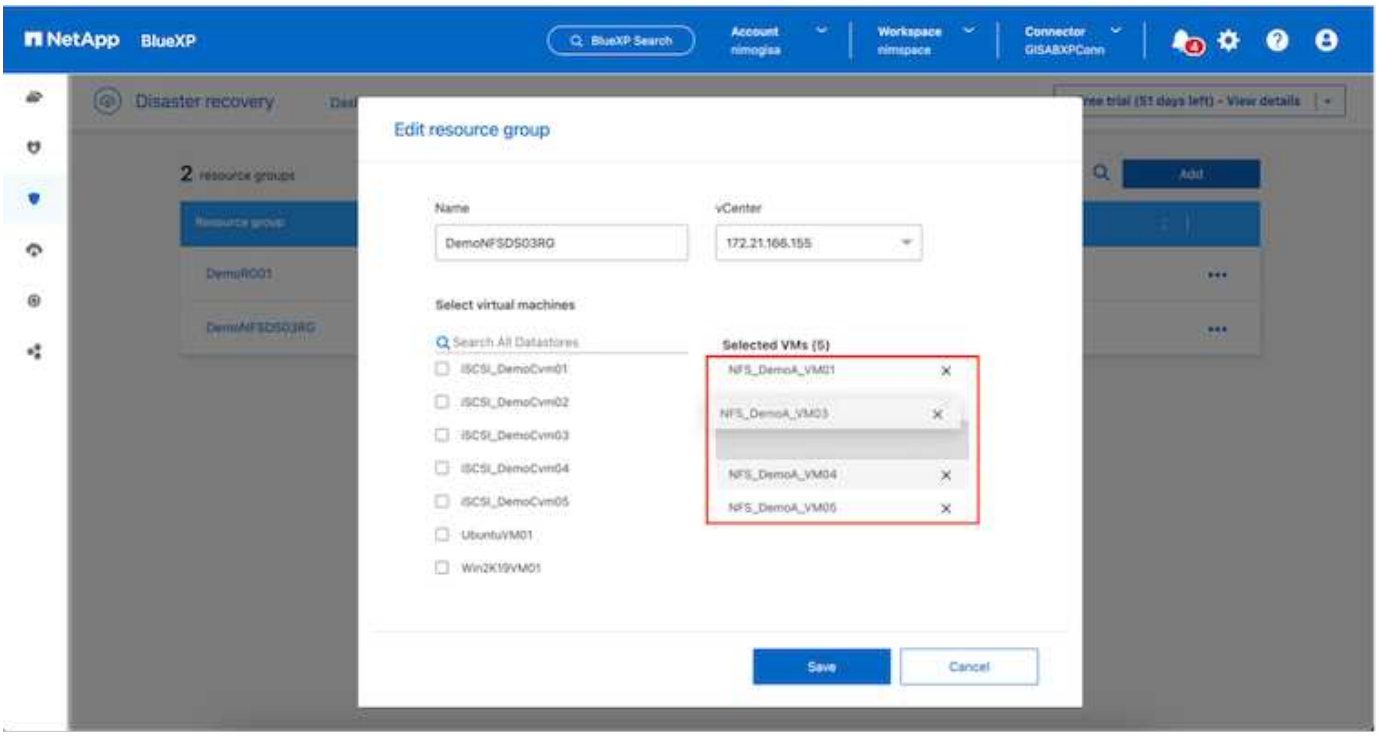
사이트가 추가된 후 VM을 리소스 그룹으로 그룹화할 수 있습니다. BlueXP disaster recovery 리소스 그룹을 사용하면 종속된 VM 세트를 논리적 그룹으로 그룹화할 수 있으며, 이 그룹에는 복구 시 실행될 수 있는 부팅 순서와 부팅 지연이 포함됩니다. 리소스 그룹을 만들려면 *리소스 그룹*으로 이동하여 *새 리소스 그룹 만들기*를 클릭하세요.



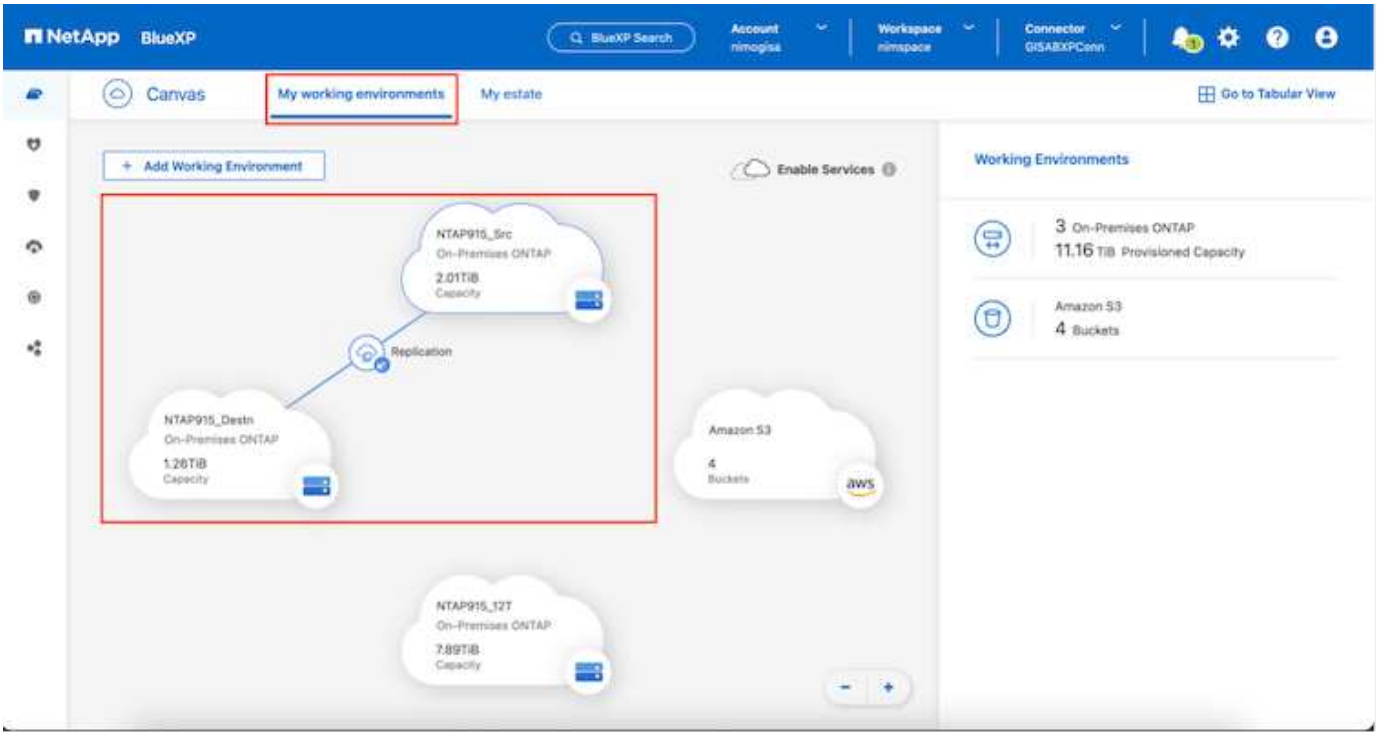


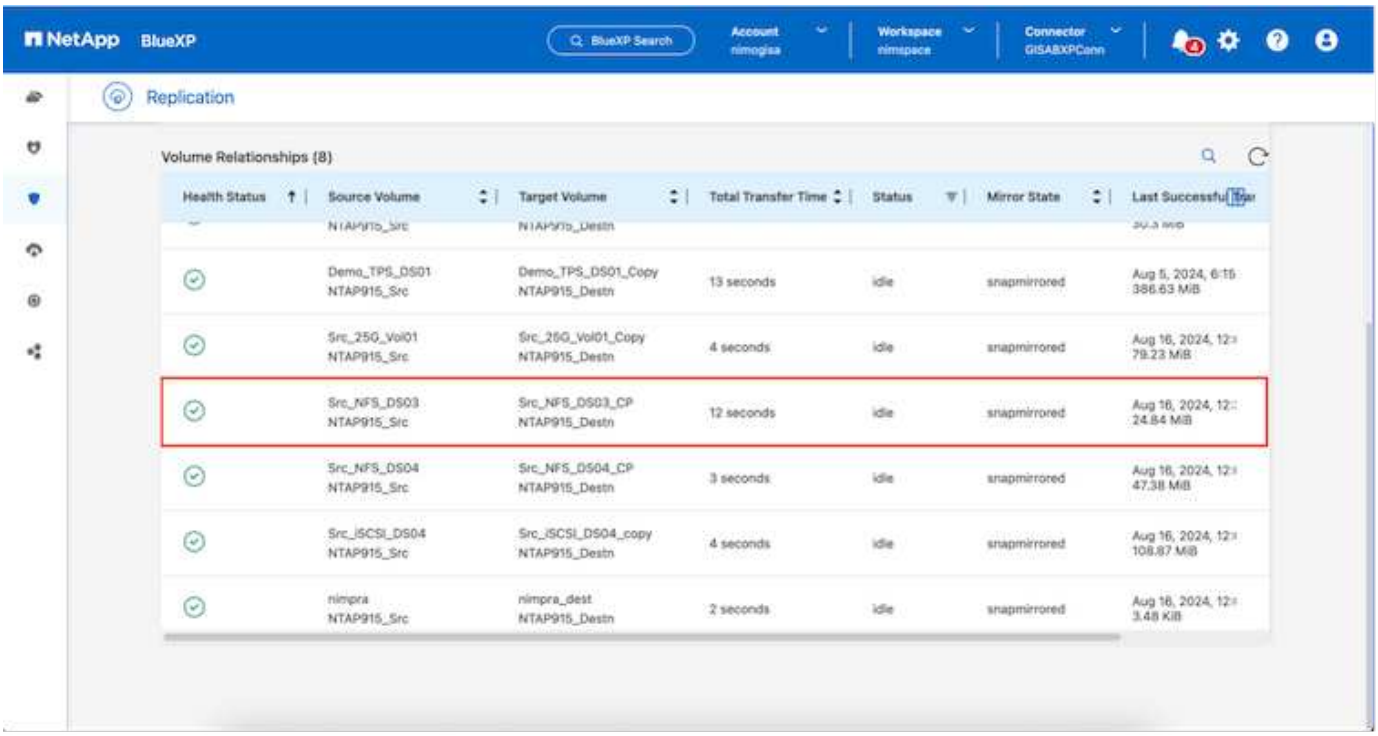
ⓘ 리소스 그룹은 복제 계획을 생성하는 동안에도 생성될 수 있습니다.

리소스 그룹을 만드는 동안 간단한 드래그 앤 드롭 메커니즘을 사용하여 VM의 부팅 순서를 정의하거나 수정할 수 있습니다.



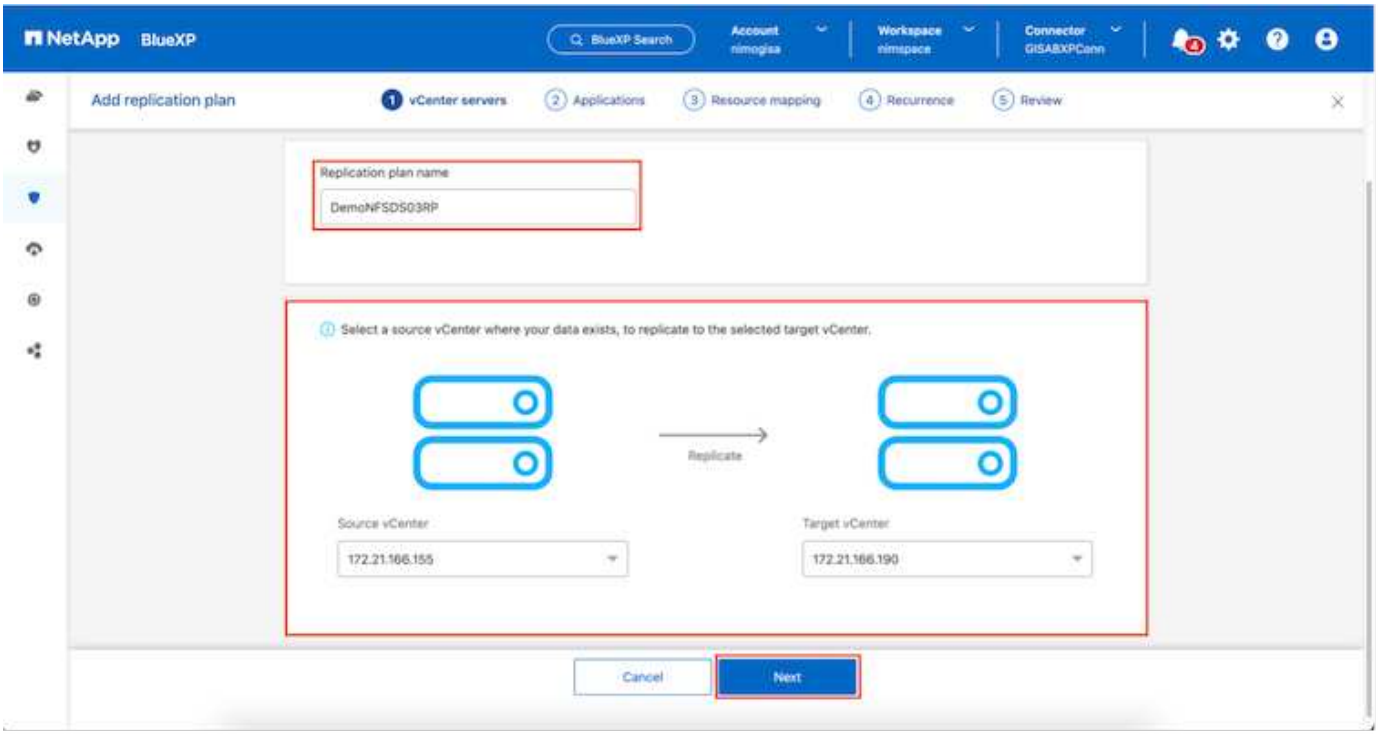
리소스 그룹을 만든 후 다음 단계는 재해 발생 시 가상 머신과 애플리케이션을 복구하기 위한 실행 청사진 또는 계획을 만드는 것입니다. 필수 구성 요소에서 언급했듯이 SnapMirror 복제는 사전에 구성할 수 있으며, DRaaS는 복제 계획을 만드는 동안 지정된 RPO 및 보존 횟수를 사용하여 구성할 수 있습니다.



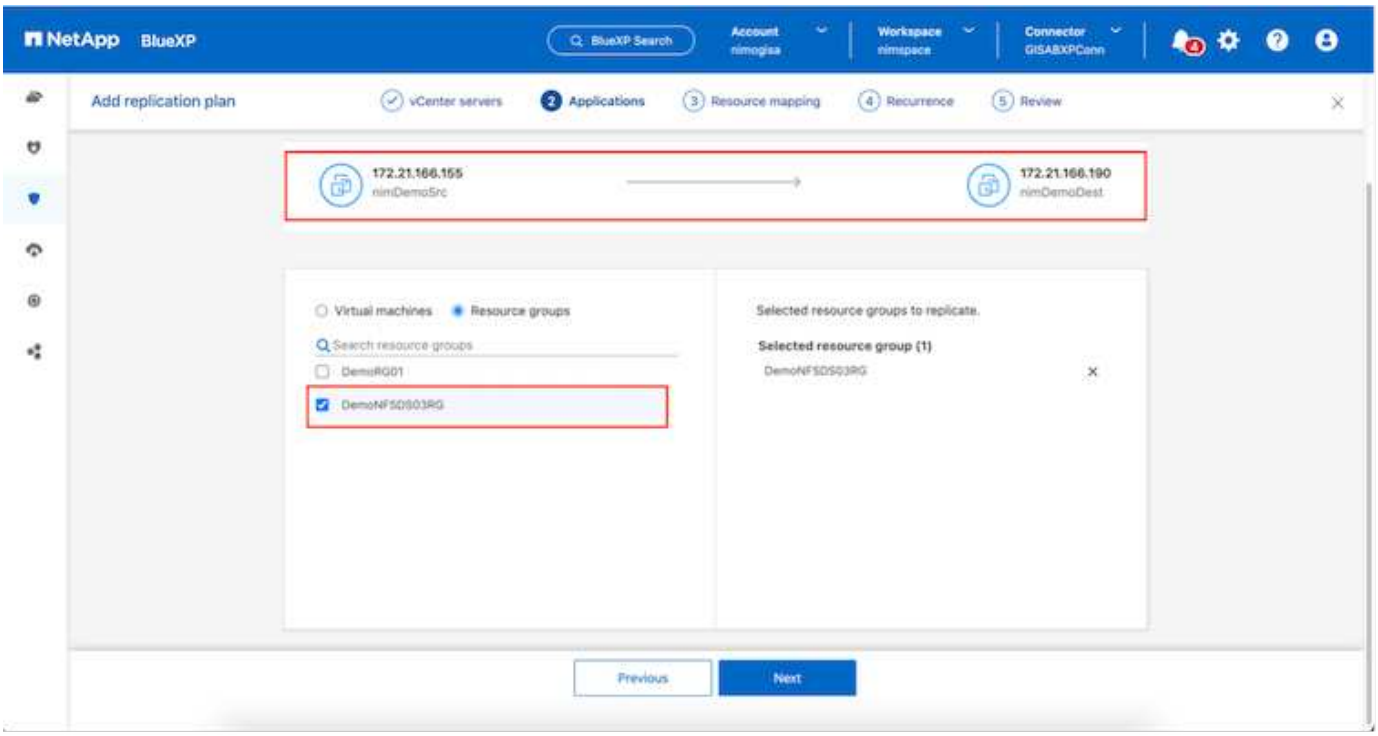


드롭다운에서 소스 및 대상 vCenter 플랫폼을 선택하여 복제 계획을 구성하고, 계획에 포함할 리소스 그룹을 선택하고, 애플리케이션을 복원하고 전원을 켜는 방법, 클러스터 및 네트워크 매핑을 그룹화합니다. 복구 계획을 정의하려면 복제 계획 탭으로 이동하여 *계획 추가*를 클릭합니다.

먼저 소스 vCenter를 선택한 다음 대상 vCenter를 선택합니다.



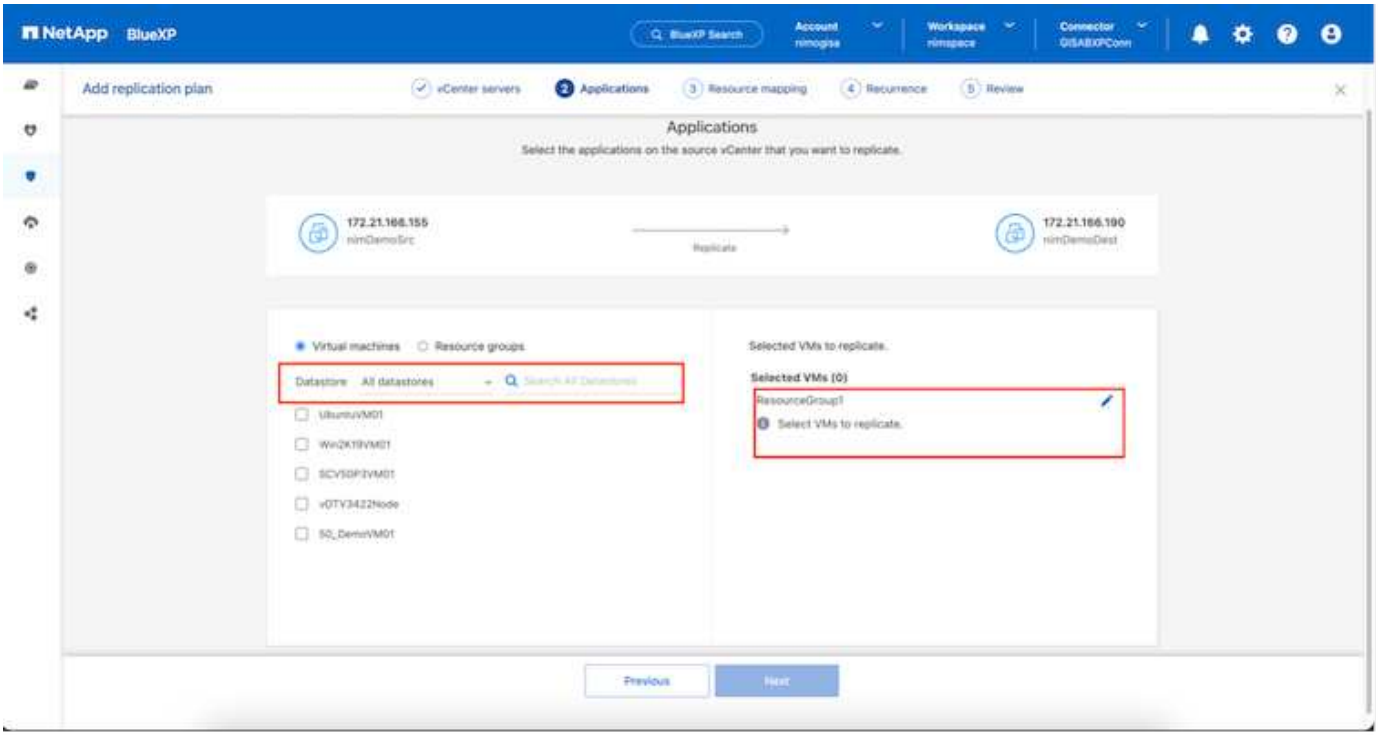
다음 단계는 기존 리소스 그룹을 선택하는 것입니다. 리소스 그룹이 생성되지 않은 경우 마법사는 복구 목표에 따라 필요한 가상 머신을 그룹화(기본적으로 기능적 리소스 그룹 생성)하는 데 도움을 줍니다. 이는 또한 애플리케이션 가상 머신을 복원하는 방법에 대한 작업 순서를 정의하는 데 도움이 됩니다.



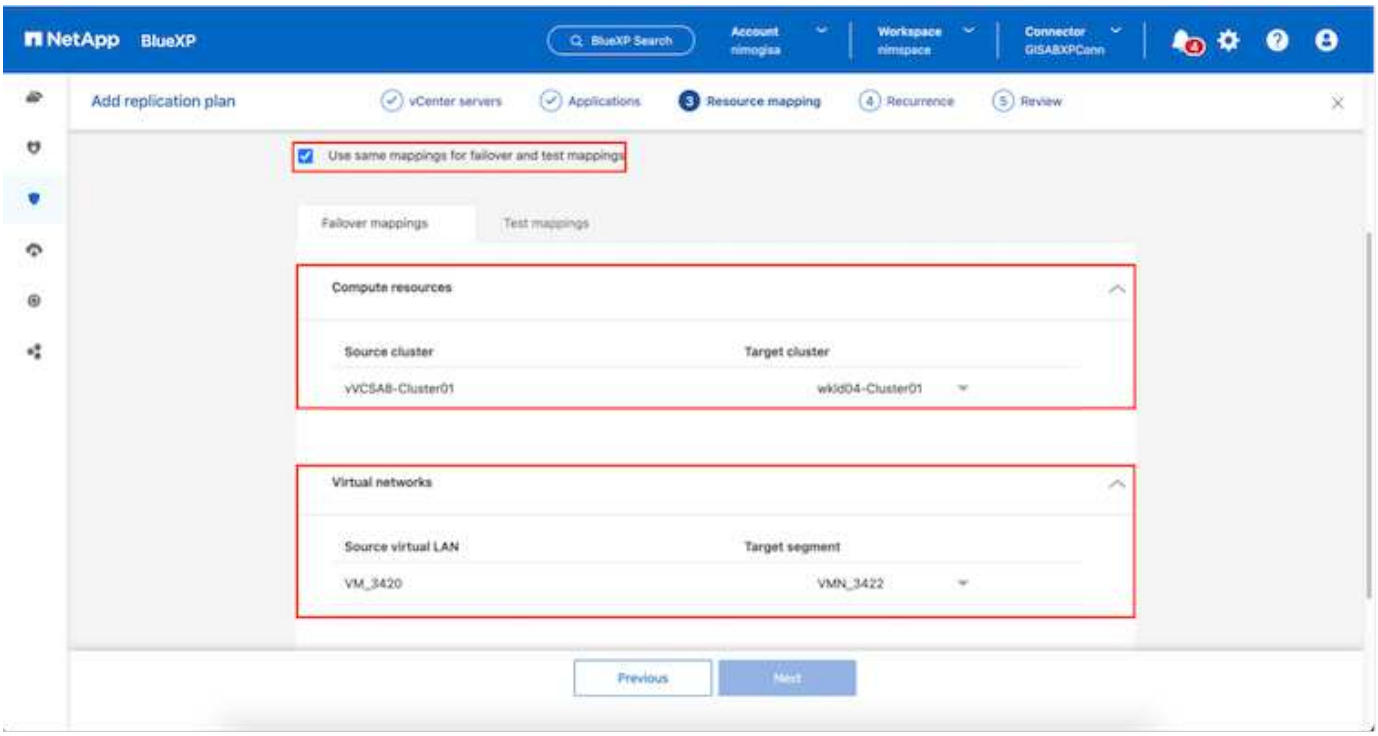
리소스 그룹을 사용하면 드래그 앤 드롭 기능을 사용하여 부팅 순서를 설정할 수 있습니다. 이를 사용하면 복구 프로세스 중에 VM의 전원이 켜지는 순서를 쉽게 수정할 수 있습니다.

리소스 그룹 내의 각 가상 머신은 순서에 따라 순차적으로 시작됩니다. 두 개의 리소스 그룹이 병렬로 시작됩니다.

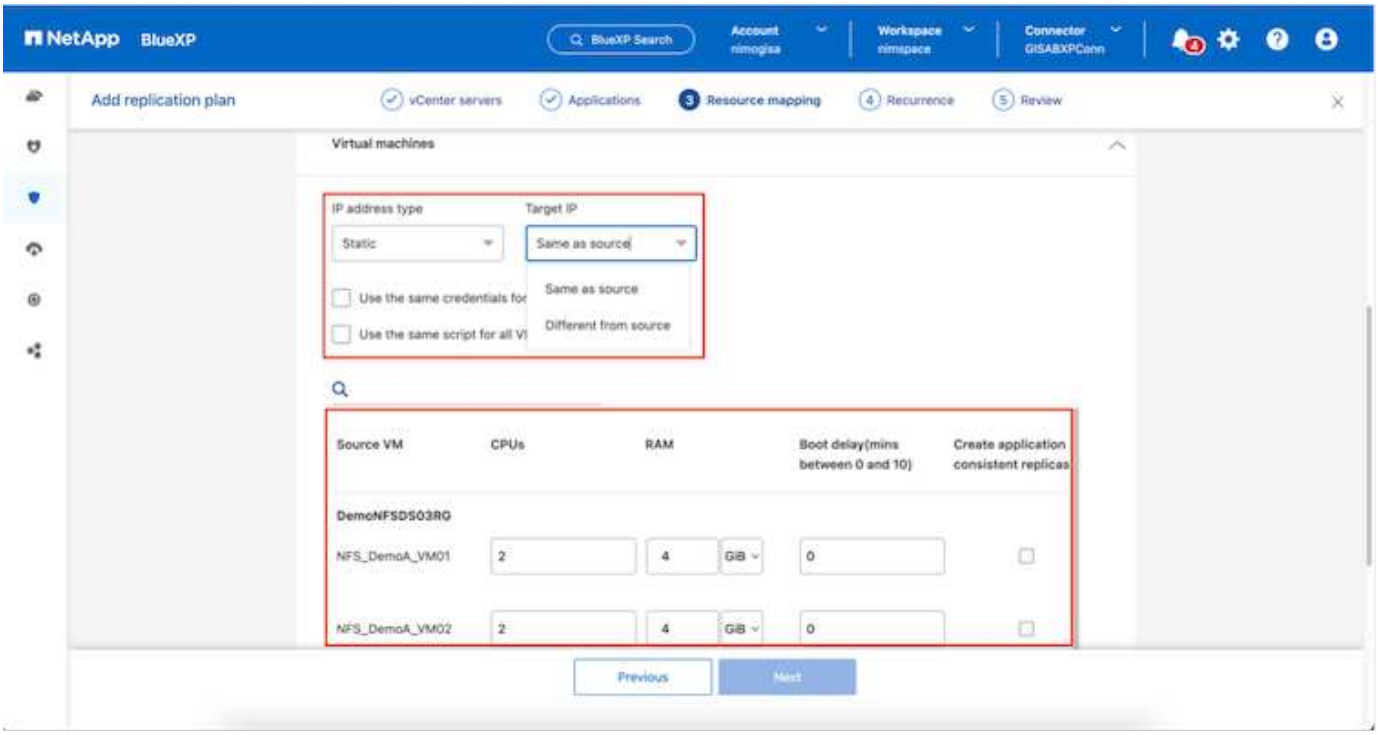
아래 스크린샷은 리소스 그룹이 사전에 생성되지 않은 경우 조직의 요구 사항에 따라 가상 머신이나 특정 데이터 저장소를 필터링하는 옵션을 보여줍니다.



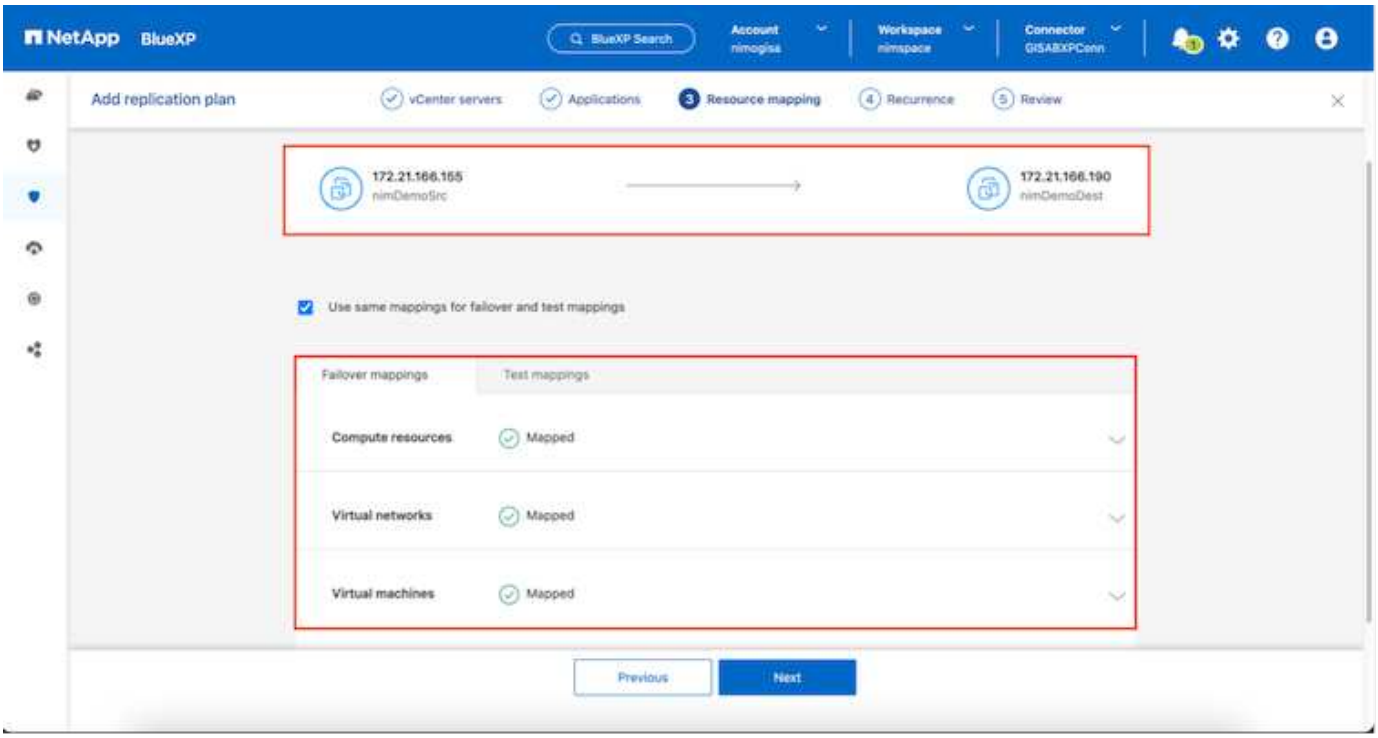
리소스 그룹을 선택한 후 장애 조치 매핑을 만듭니다. 이 단계에서는 소스 환경의 리소스가 대상 환경에 어떻게 매핑되는지 지정합니다. 여기에는 컴퓨팅 리소스, 가상 네트워크가 포함됩니다. IP 사용자 정의, 사전 및 사후 스크립트, 부팅 지연, 애플리케이션 일관성 등. 자세한 내용은 다음을 참조하세요."복제 계획 만들기" .



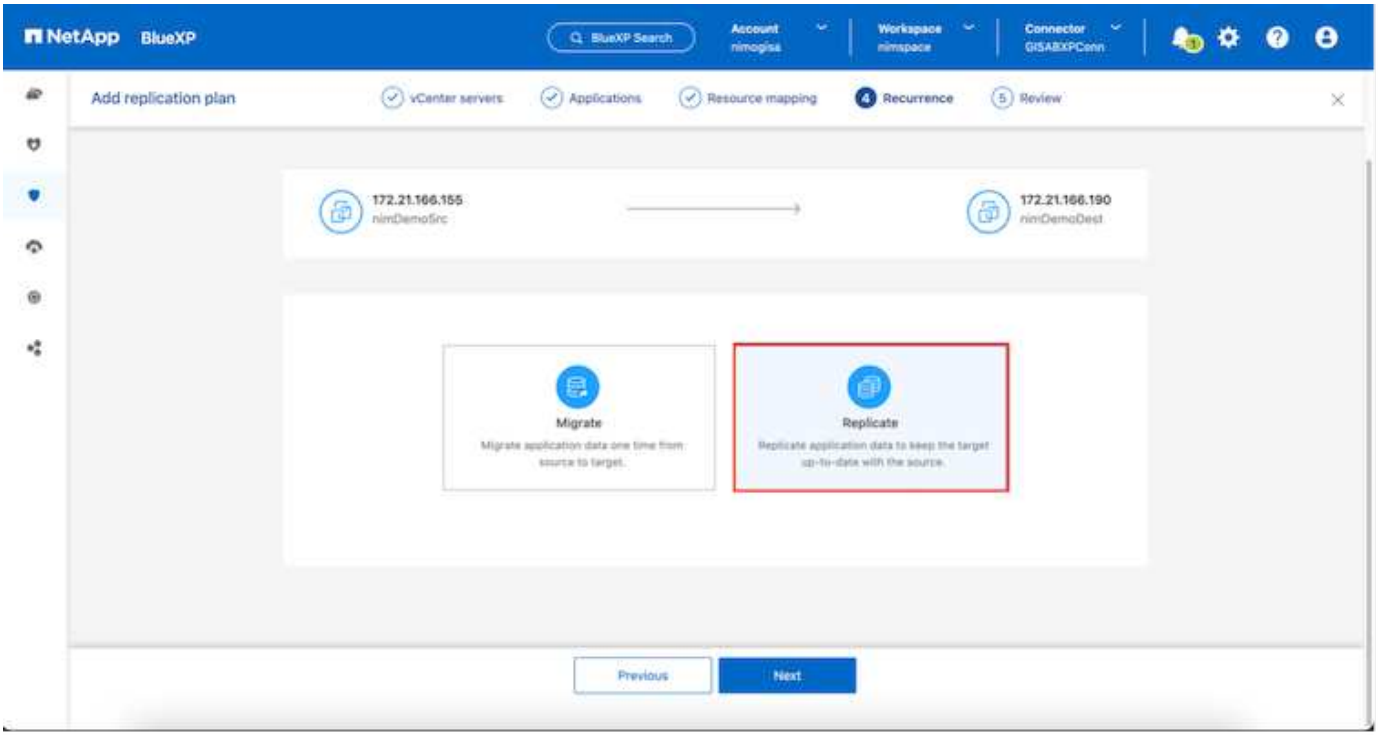
기본적으로 테스트 작업과 장애 조치 작업 모두에 동일한 매핑 매개변수가 사용됩니다. 테스트 환경에 대해 다른 매핑을 설정하려면 아래와 같이 체크박스 선택을 해제한 후 테스트 매핑 옵션을 선택하세요.



리소스 매핑이 완료되면 다음을 클릭합니다.

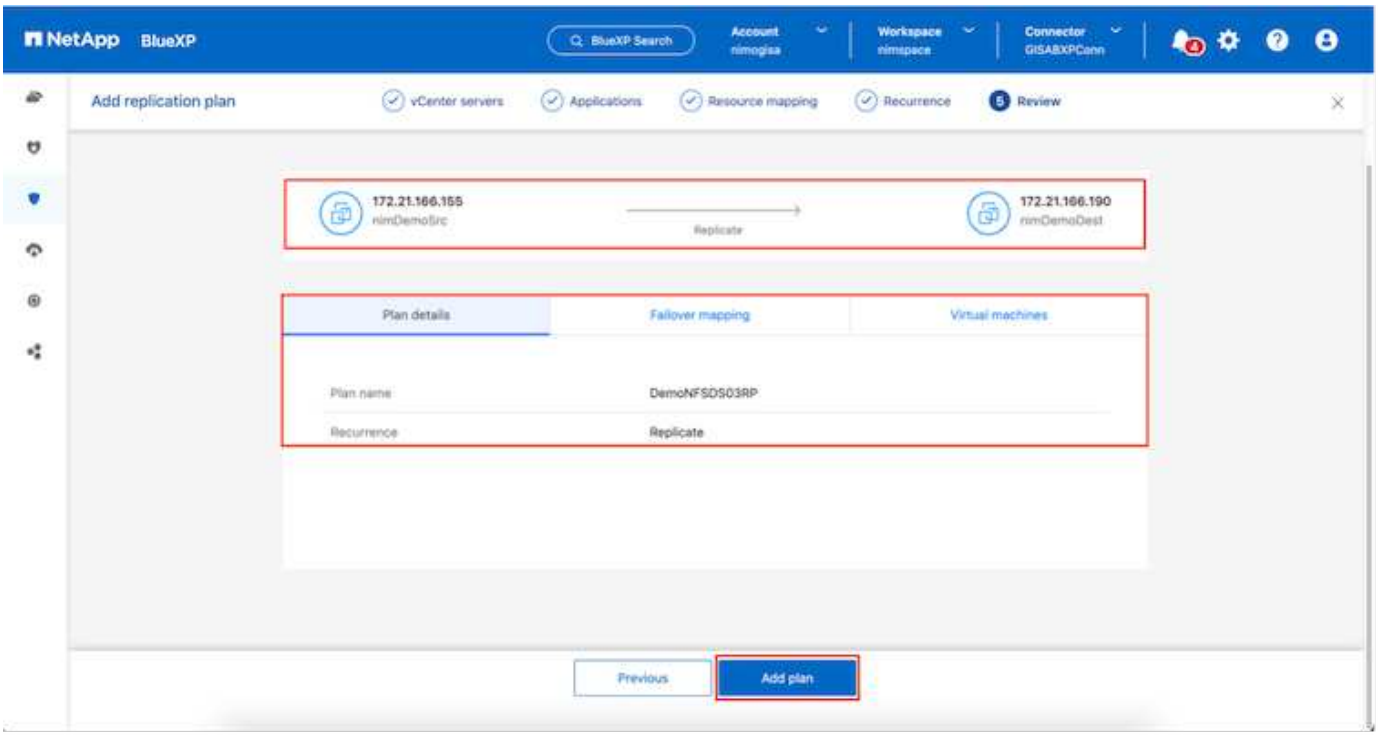


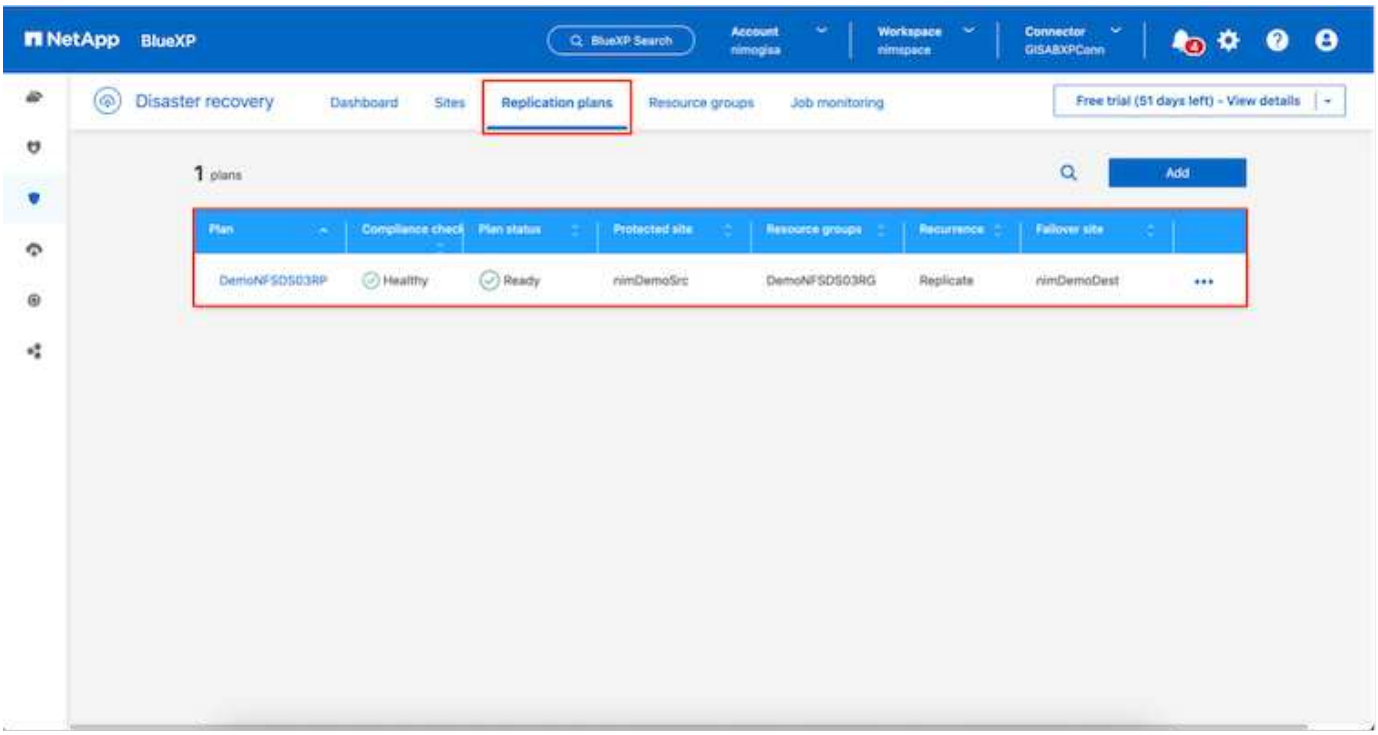
반복 유형을 선택하세요. 간단히 말해서, 마이그레이션(장애 조치를 사용한 일회성 마이그레이션) 또는 반복적 지속적 복제 옵션을 선택합니다. 이 연습에서는 복제 옵션이 선택되었습니다.



완료되면 생성된 매핑을 검토한 후 *계획 추가*를 클릭합니다.

> 다양한 볼륨과 SVM의 VM을 복제 계획에 포함할 수 있습니다. VM 배치(동일한 볼륨에 있는지, 동일한 SVM 내의 별도 볼륨인지, 서로 다른 SVM의 별도 볼륨인지)에 따라 BlueXP disaster recovery 일관성 그룹 스냅샷을 생성합니다.



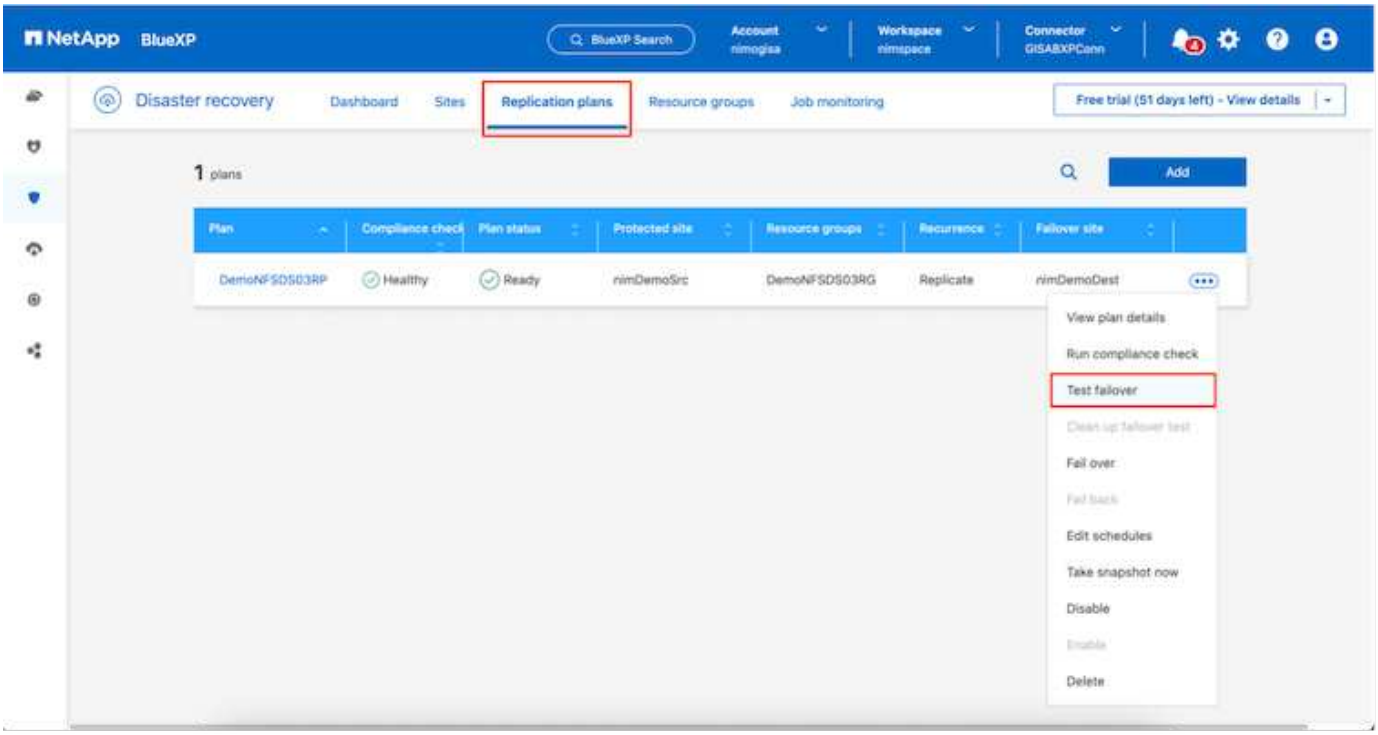


BlueXP DRaaS는 다음 워크플로로 구성됩니다.

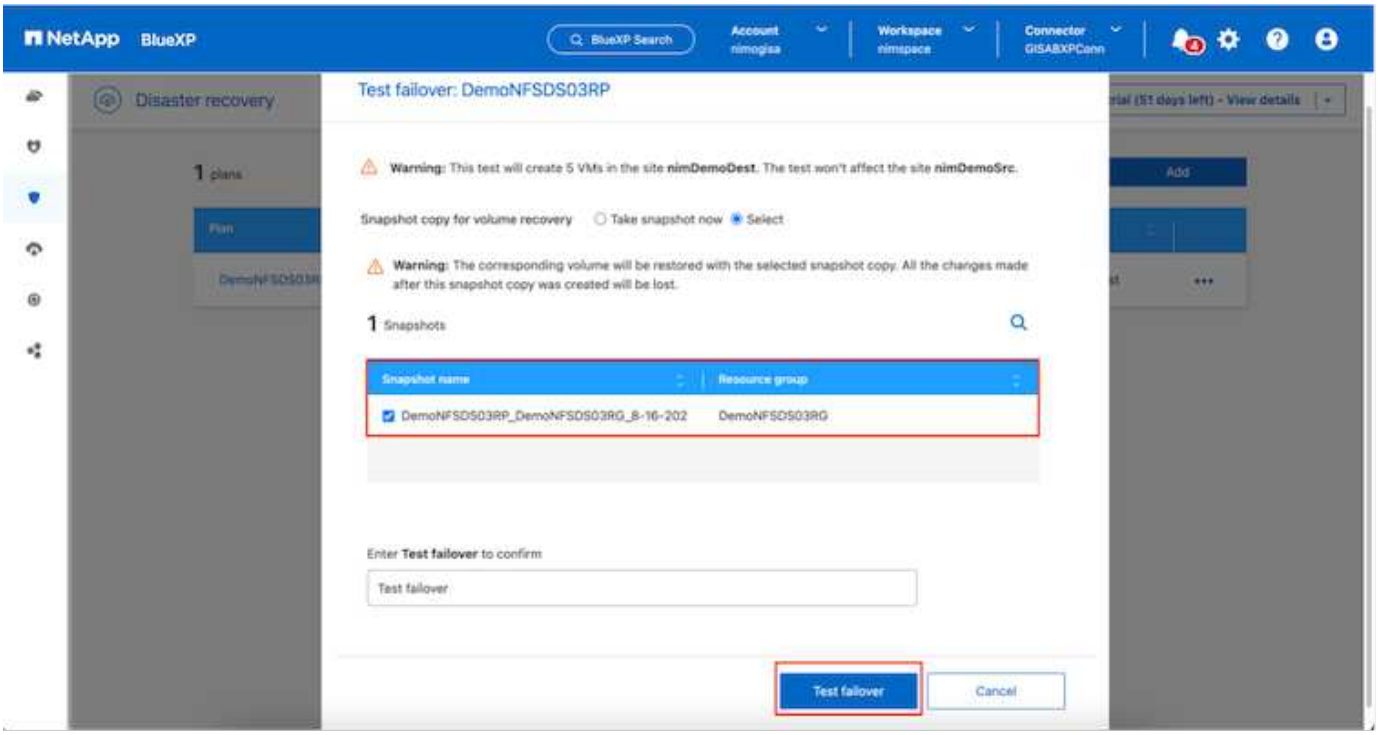
- 테스트 장애 조치(주기적 자동 시뮬레이션 포함)
- 클린업 페일오버 테스트
- 장애 조치
- 장애 복구

테스트 장애 조치

BlueXP DRaaS의 테스트 페일오버는 VMware 관리자가 프로덕션 환경을 방해하지 않고 복구 계획을 완전히 검증할 수 있도록 하는 운영 절차입니다.

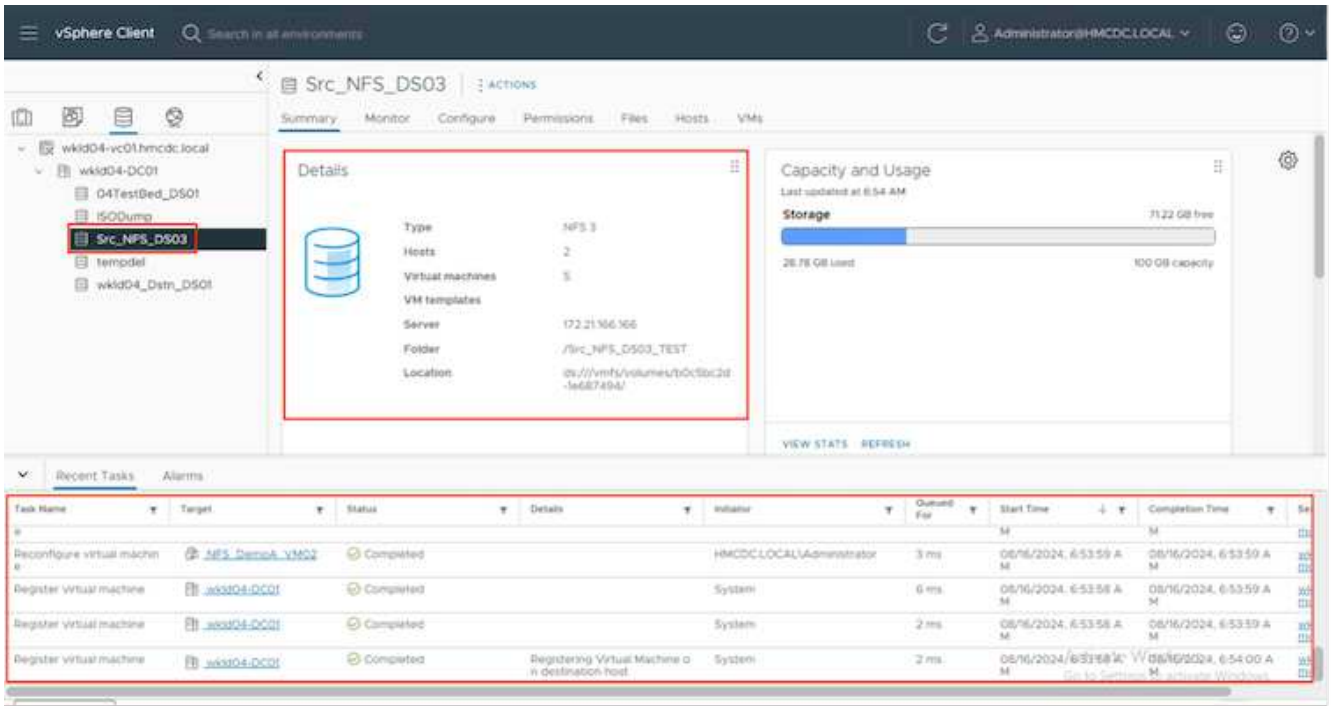


BlueXP DRaaS는 테스트 장애 조치 작업에서 스냅샷을 선택적 기능으로 선택하는 기능을 통합합니다. 이 기능을 사용하면 VMware 관리자는 최근 환경에서 변경된 사항이 대상 사이트에 복제되어 테스트 중에도 그대로 유지되는지 확인할 수 있습니다. 이러한 변경 사항에는 VM 게스트 운영 체제에 대한 패치가 포함됩니다.



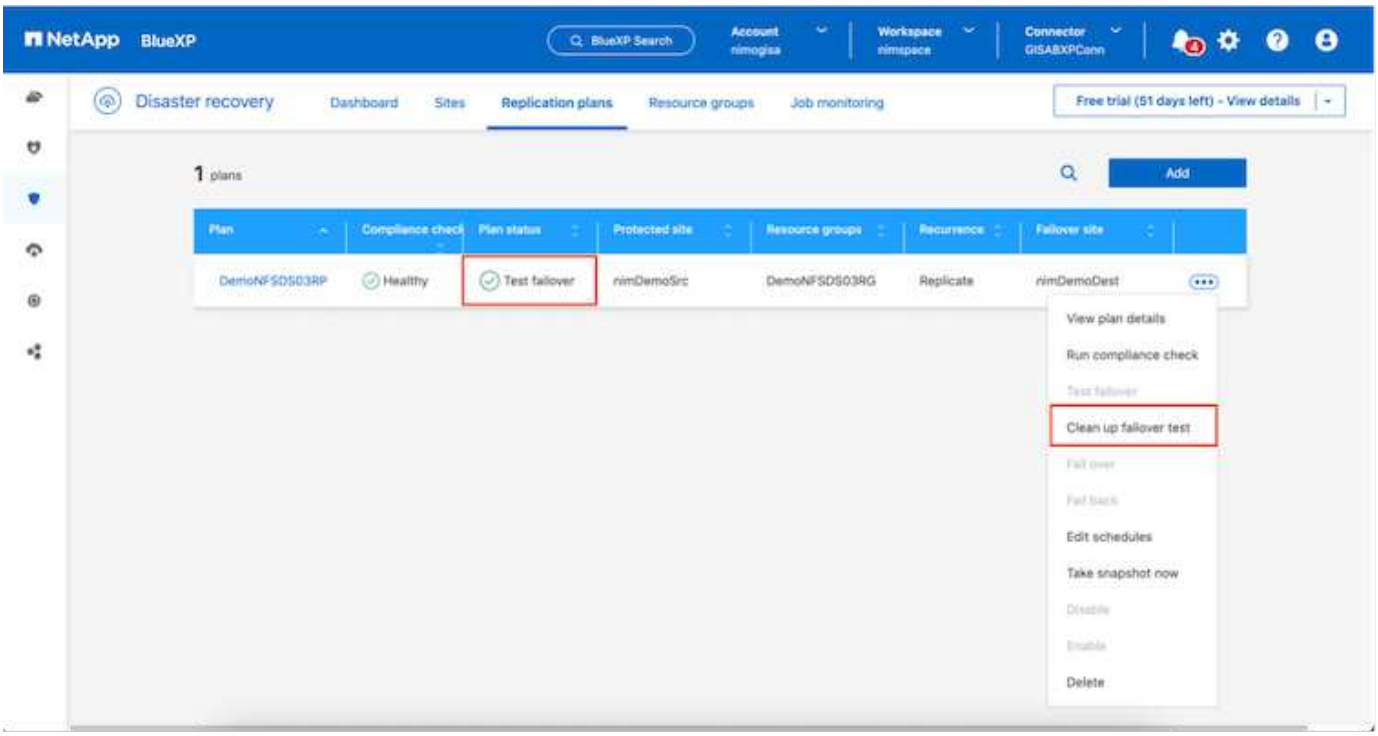
VMware 관리자가 테스트 장애 조치 작업을 실행하면 BlueXP DRaaS는 다음 작업을 자동화합니다.

- 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.



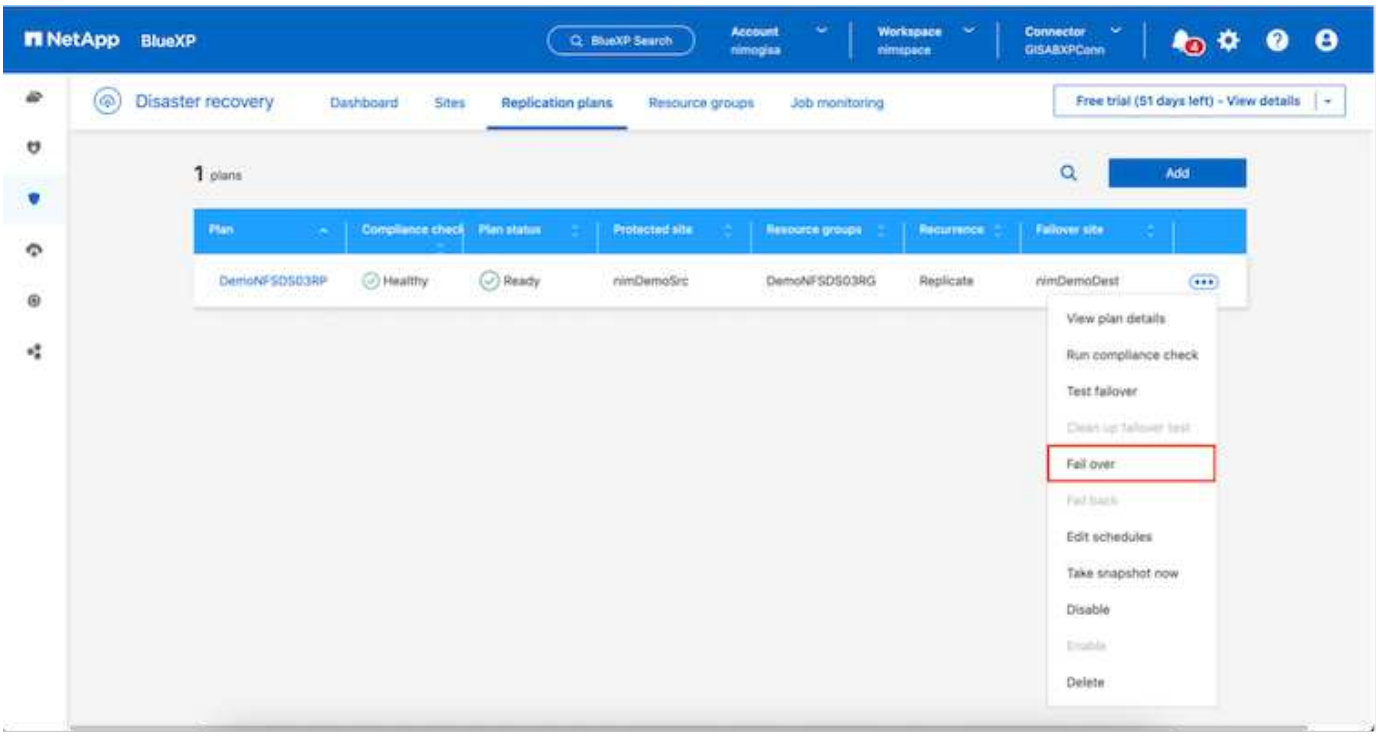
이 작업을 수행하면 가상 머신(VM)과 복제 계획 상태가 준비 상태로 재설정됩니다.

VMware 관리자가 복구 작업을 수행하면 BlueXP DRaaS는 다음 프로세스를 완료합니다.

1. 테스트에 사용된 FlexClone 복사본에서 복구된 각 VM의 전원을 끕니다.
2. 테스트 중 복구된 VM을 표시하는 데 사용된 FlexClone 볼륨을 삭제합니다.

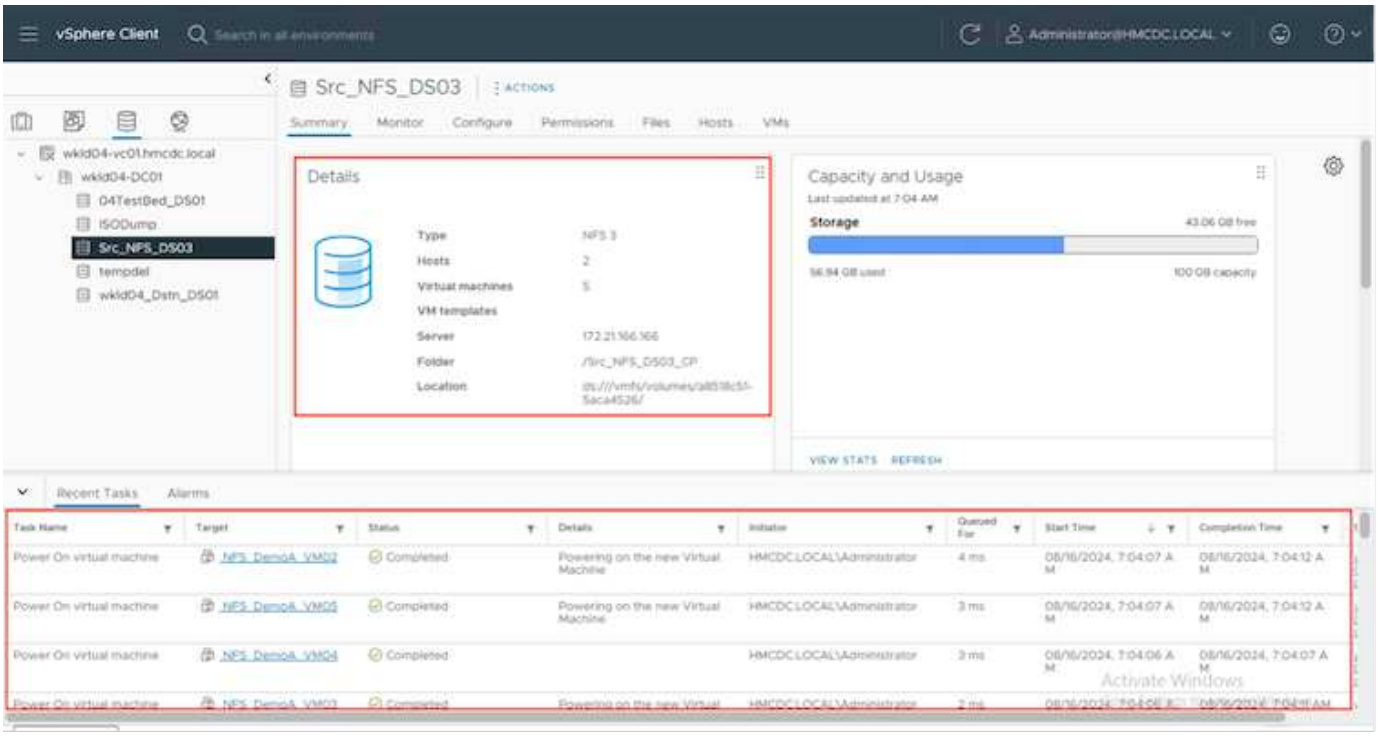
계획된 마이그레이션 및 장애 조치

BlueXP DRaaS는 실제 장애 조치를 수행하는 데 계획된 마이그레이션과 장애 조치라는 두 가지 방법을 제공합니다. 첫 번째 방법인 계획된 마이그레이션은 VM 종료 및 스토리지 복제 동기화를 프로세스에 통합하여 VM을 대상 사이트로 복구하거나 효과적으로 이동합니다. 계획된 마이그레이션에는 소스 사이트에 대한 액세스가 필요합니다. 두 번째 방법인 장애 조치(failover)는 계획된/계획되지 않은 장애 조치로, VM이 마지막 저장소 복제 간격에서 완료될 수 있었던 대상 사이트에서 복구됩니다. 솔루션에 설계된 RPO에 따라 DR 시나리오에서 어느 정도의 데이터 손실이 예상될 수 있습니다.



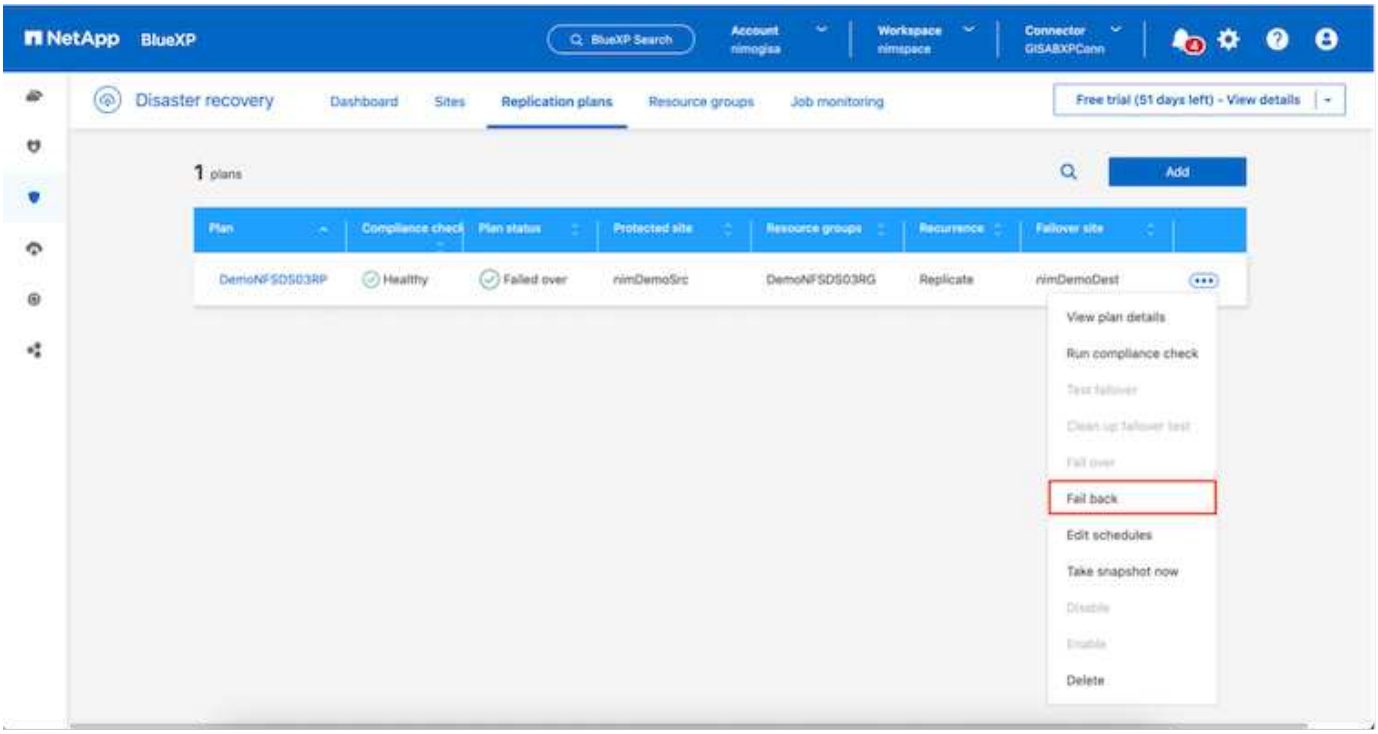
VMware 관리자가 장애 조치 작업을 수행하면 BlueXP DRaaS는 다음 작업을 자동화합니다.

- 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.

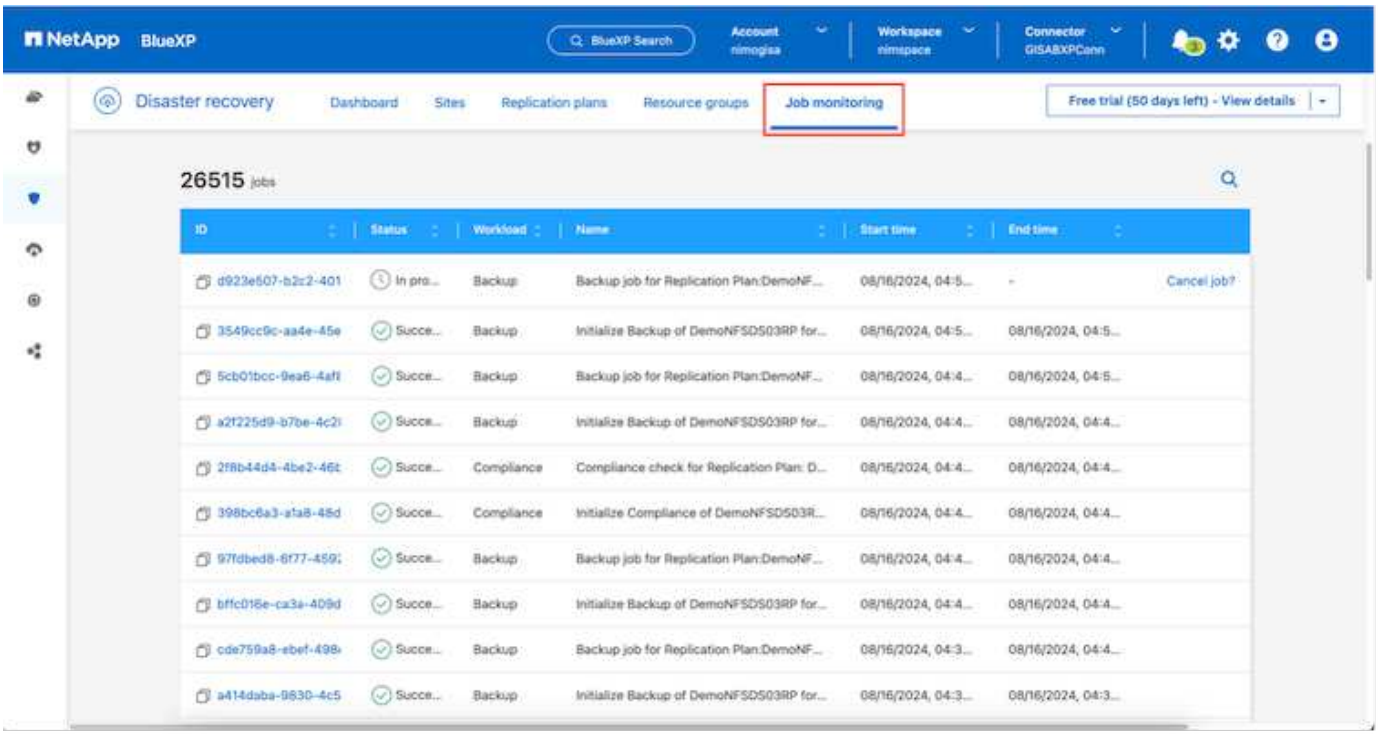
참고: BlueXP DRaaS는 복제 방향을 반전하기 전에 모든 변경 사항을 원본 소스 가상 머신으로 복제(재동기화)합니다. 이 프로세스는 대상으로의 장애 조치를 완료한 관계에서 시작되며 다음 단계를 포함합니다.

- 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.

BlueXP DRaaS에 액세스하고 구성하는 방법에 대한 자세한 내용은 다음을 참조하세요."VMware용 BlueXP 재해 복구에 대해 알아보세요" .

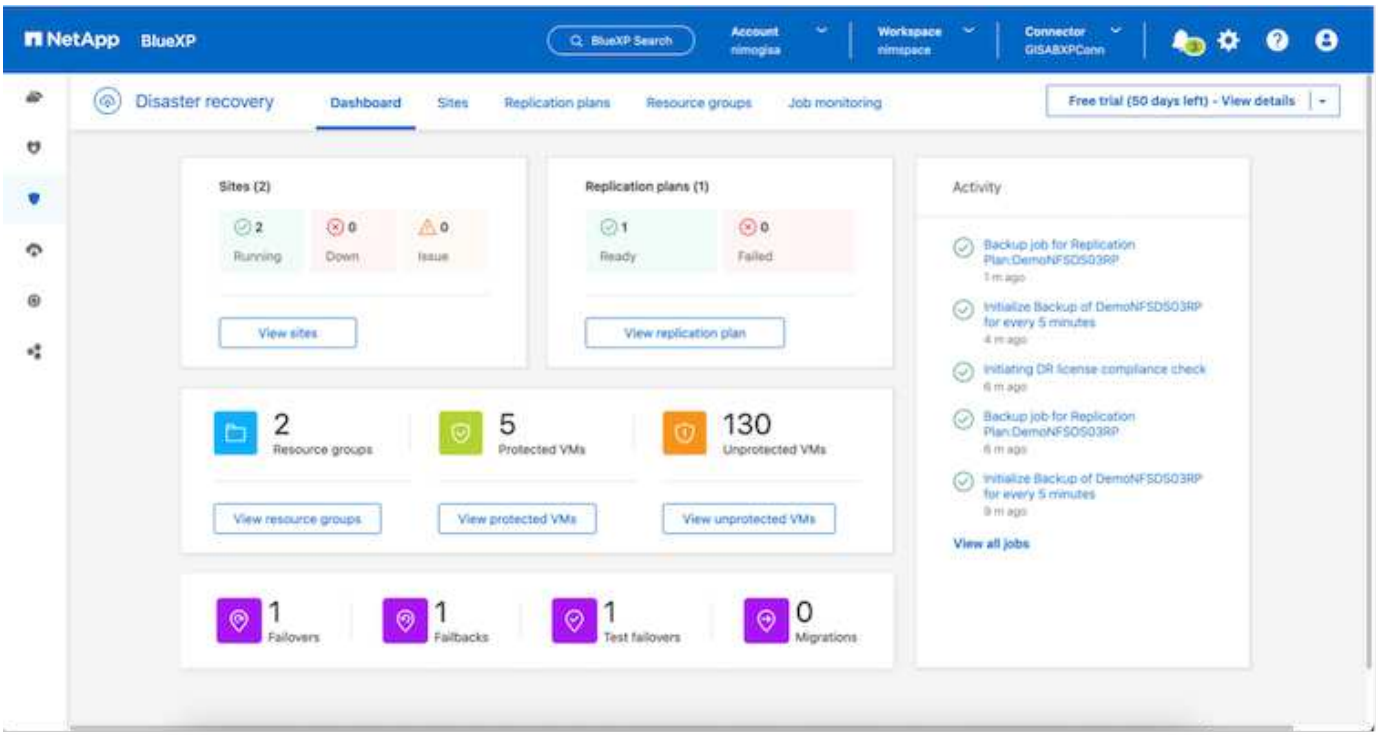
모니터링 및 대시보드

BlueXP 또는 ONTAP CLI에서 해당 데이터 저장소 볼륨에 대한 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.

BlueXP disaster recovery 보드를 사용하면 재해 복구 사이트와 복제 계획의 상태를 확실하게 평가할 수 있습니다. 이를 통해 관리자는 정상, 연결이 끊긴 또는 성능이 저하된 사이트와 계획을 신속하게 식별할 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" .

vSphere Metro Storage Cluster로 워크로드 보호

ONTAP 고가용성을 VMware vSphere Metro Storage Cluster(vMSC)와 통합하는 방법에 대해 알아보세요.

NetApp ONTAP 고가용성을 VMware vSphere Metro Storage Cluster(vMSC)와 통합하는 데 사용할 수 있는 NetApp 솔루션에 대해 알아보세요. 이는 VMware Cloud Foundation(VCF) 관리 및 VI 워크로드 도메인을 위한 강력한 솔루션을 제공합니다.

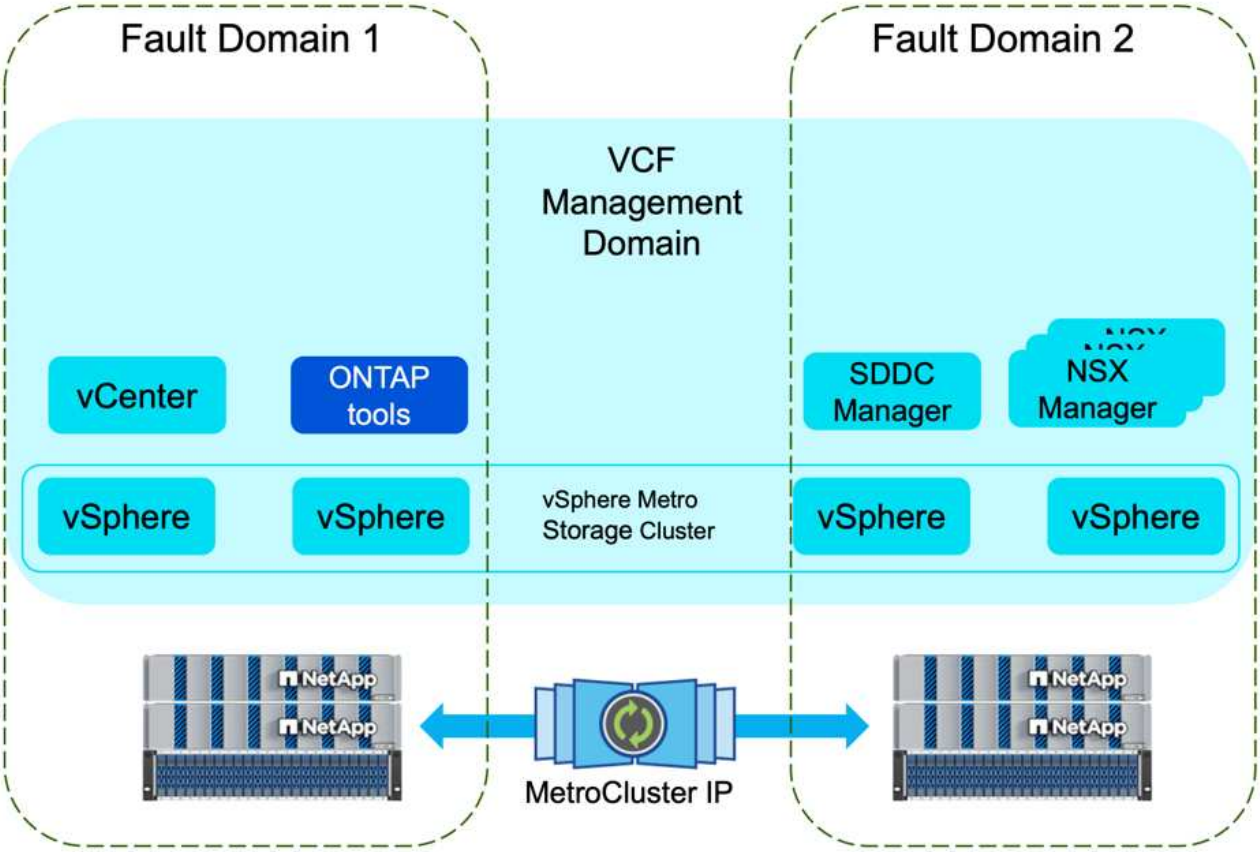
이러한 조합은 지리적으로 분산된 사이트에서 지속적인 데이터 가용성, 원활한 장애 조치 및 재해 복구를 보장하여 중요한 작업 부하에 대한 복원력과 운영 연속성을 향상시킵니다. SnapMirror 액티브 동기화는 사이트 전체에 장애가 발생하더라도 비즈니스 서비스가 계속 운영될 수 있도록 하며, 보조 복사본을 사용하여 애플리케이션이 투명하게 장애 조치되도록 지원합니다. SnapMirror 액티브 싱크를 사용하면 페일오버를 트리거하는 데 수동 작업이나 사용자 지정 스크립팅이 필요하지 않습니다.

자세한 내용은 다음 솔루션을 참조하세요.

- "SnapMirror Active Sync를 사용하여 관리 도메인에 대한 스트레치 클러스터"
- "MetroCluster 사용하여 관리 도메인에 대한 스트레치 클러스터"
- "SnapMirror Active Sync를 사용하여 VI 워크로드 도메인에 대한 스트레치 클러스터"
- "MetroCluster 사용하여 VI 워크로드 도메인에 대한 스트레치 클러스터"

MetroCluster 사용하여 VCF 관리 도메인에 대한 스트레치 클러스터 구성

이 사용 사례에서는 NFS를 기본 데이터 저장소로 사용하여 ONTAP MetroCluster 사용하여 VMware Cloud Foundation(VCF) 관리 도메인에 대한 스트레치 클러스터를 구성하는 절차를 설명합니다. 이 절차에는 vSphere 호스트와 vCenter Server 배포, NFS 데이터 저장소 프로비저닝, VCF 가져오기 도구를 사용하여 클러스터 검증, NSX 설정 구성, 환경을 VCF 관리 도메인으로 변환하는 작업이 포함됩니다.



소개

이 솔루션에서는 ONTAP MetroCluster 사용하여 NFS를 주 데이터 저장소로 하는 Stretched VCF 관리 도메인을 구현하는 방법을 보여드리겠습니다.

시나리오 개요

이 시나리오에서는 다음과 같은 상위 수준 단계를 다룹니다.

- vSphere 호스트와 vCenter 서버를 배포합니다.
- vSphere 호스트에 NFS 데이터 저장소를 프로비저닝합니다.
- vSphere 클러스터에 SDDC Manager를 배포합니다.
- VCF 가져오기 도구를 사용하여 vSphere 클러스터를 검증합니다.
- VCF 변환 중에 NSX를 생성하기 위해 JSON 파일을 구성합니다.

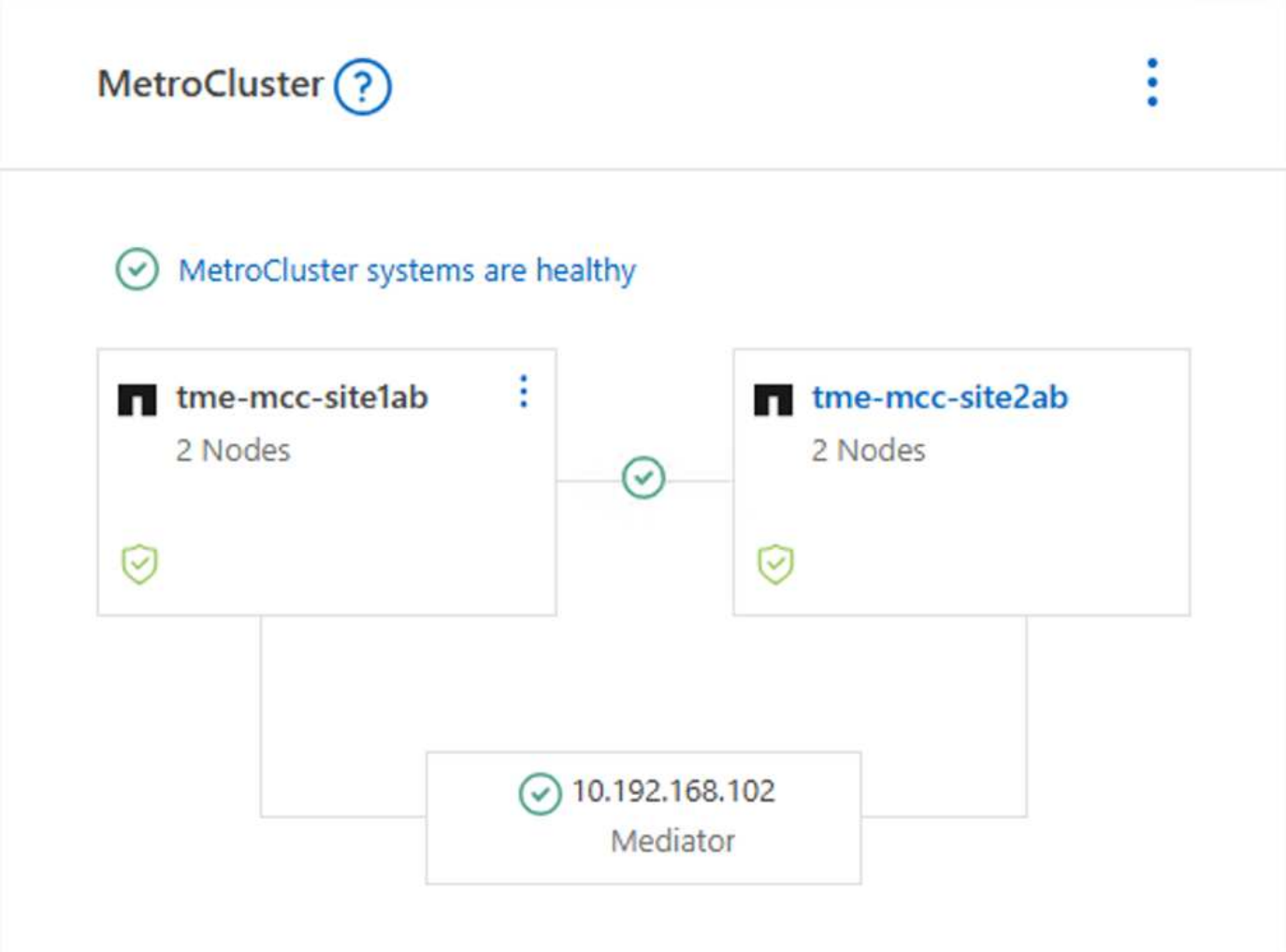
- VCF 가져오기 도구를 사용하여 vSphere 8 환경을 VCF 관리 도메인으로 변환합니다.

필수 조건

이 시나리오에는 다음과 같은 구성 요소와 구성이 필요합니다.

- 지원되는 ONTAP MetroCluster 구성
- NFS 트래픽을 허용하도록 구성된 스토리지 가상 머신(SVM)입니다.
- NFS 트래픽을 전달하고 SVM과 연관되는 논리적 인터페이스(LIF)가 IP 네트워크에 생성되었습니다.
- 네트워크 스위치에 연결된 4개의 ESXi 호스트가 있는 vSphere 8 클러스터.
- VCF 변환에 필요한 소프트웨어를 다운로드하세요.

다음은 MetroCluster 구성을 보여주는 시스템 관리자의 샘플 스크린샷입니다
.



그리고 여기에 두 가지 단층 도메인의 SVM 네트워크 인터페이스가 있습니다
.

Network interfaces Subnets

+ Add

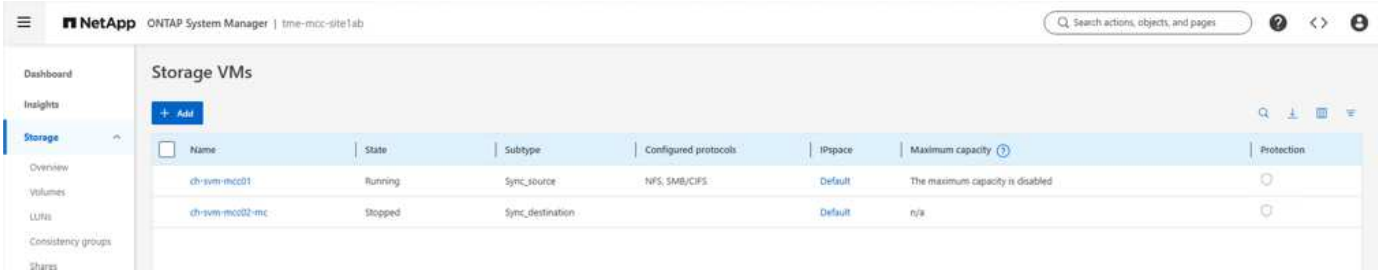
Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc02_8775		ch-svm-mcc02-mc	Default	10.192.164.230	tme-mcc-site1a
lif_ch-svm-mcc01_3118		ch-svm-mcc01	Default	10.192.164.225	tme-mcc-site1a
lif_ch-svm-mcc02_9778		ch-svm-mcc02-mc	Default	10.192.164.231	tme-mcc-site1b
lif_ch-svm-mcc01_6783		ch-svm-mcc01	Default	10.192.164.226	tme-mcc-site1b

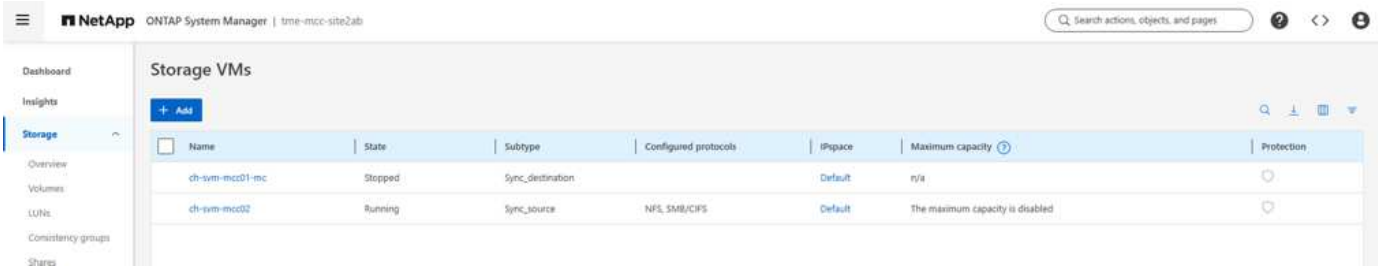
Network interfaces Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc01_3118		ch-svm-mcc01-mc	Default	10.192.164.225	tme-mcc-site2a
lif_ch-svm-mcc02_8775		ch-svm-mcc02	Default	10.192.164.230	tme-mcc-site2a
lif_ch-svm-mcc01_6783		ch-svm-mcc01-mc	Default	10.192.164.226	tme-mcc-site2b
lif_ch-svm-mcc02_9778		ch-svm-mcc02	Default	10.192.164.231	tme-mcc-site2b

[참고] SVM은 MetroCluster 의 오류 도메인 중 하나에서 활성화됩니다.





나타내다 "MetroCluster 를 갖춘 vMSC" .

vSphere를 VCF 5.2로 변환하거나 가져오기 위해 지원되는 저장소 및 기타 고려 사항은 다음을 참조하세요. "기존 vSphere 환경을 VMware Cloud Foundation으로 변환하거나 가져오기 전 고려 사항" .

VCF 관리 도메인으로 변환될 vSphere 클러스터를 생성하기 전에 다음을 참조하세요. "vSphere 클러스터에 대한 NSX 고려 사항"

필수 소프트웨어는 다음을 참조하세요. "기존 vSphere 환경을 변환하거나 가져오기 위한 소프트웨어 다운로드" .

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

배포 단계

NFS를 주 데이터 저장소로 사용하여 VCF Stretched Management Domain을 배포하려면

다음 단계를 완료하세요.

- vSphere 호스트와 vCenter를 배포합니다.
- vSphere 클러스터를 생성합니다.
- NFS 데이터 저장소를 제공합니다.
- VCF 가져오기 도구를 vCenter 어플라이언스에 복사합니다.
- VCF 가져오기 도구를 사용하여 vCenter 어플라이언스에 대한 사전 검사를 실행합니다.
- vCenter 클러스터에 SDDC 관리자 VM을 배포합니다.
- 변환 프로세스 중에 배포할 NSX 클러스터에 대한 JSON 파일을 만듭니다.
- 필요한 소프트웨어를 SDDC 관리자에 업로드합니다.
- vSphere 클러스터를 VCF 관리 도메인으로 변환합니다.

변환 프로세스 개요는 다음을 참조하세요. "VMware Cloud Foundation에서 vSphere 환경을 관리 도메인으로 변환하거나 vSphere 환경을 VI 워크로드 도메인으로 가져오기" .

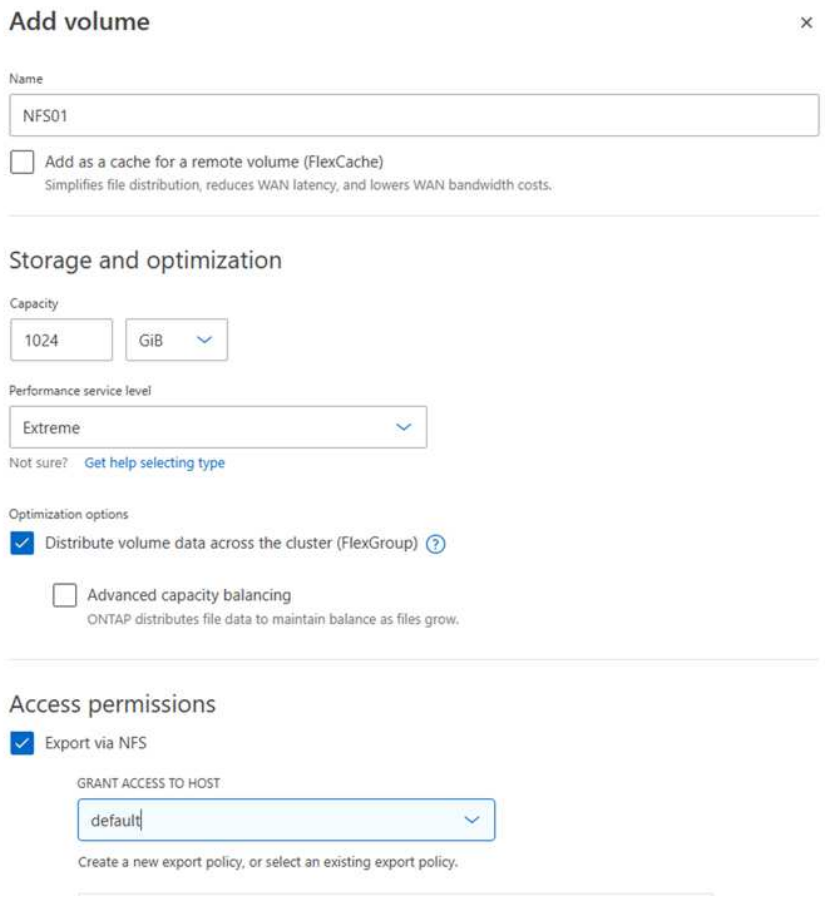
vSphere 호스트 및 **vCenter** 배포

Broadcom 지원 포털에서 다운로드한 ISO를 사용하여 호스트에 vSphere를 배포하거나 vSphere 호스트에 대한 기존 배포 옵션을 사용합니다.

VM을 호스팅하기 위해 **NFS** 데이터 저장소를 마운트합니다.

이 단계에서는 NFS 볼륨을 생성하고 이를 VM을 호스팅하기 위한 데이터 저장소로 마운트합니다.

1. 시스템 관리자를 사용하여 볼륨을 생성하고 vSphere 호스트의 IP 서브넷을 포함하는 내보내기 정책에 연결합니다.



2. vSphere 호스트에 SSH를 실행하고 NFS 데이터스토어를 마운트합니다
.

```
[root@SiteA-vs01:~] esxcli storage nfs add -c 4 -H 10.192.164.225 -s /NFS01 -v NFS01
[root@SiteA-vs01:~] esxcli storage nfs list
Volume Name  Host           Share   Vmknic  Accessible  Mounted  Connections  Read-Only   isPE  Hardware Acceleration
-----------  --------------  ------  ------  ----------  -------  -----------  ---------  -----  ---------------------
NFS01        10.192.164.225  /NFS01  None          true     true            4      false  false  Not Supported
[root@SiteA-vs01:~]
```

3. 추가 데이터 저장소가 필요한 경우 위의 단계를 반복하고 하드웨어 가속이 지원되는지 확인하세요
.

```
[root@MCCA01:~] esxcli storage nfs list
Volume Name  Host           Share   Vmknic  Accessible  Mounted  Connections  Read-Only   isPE  Hardware Acceleration
-----------  --------------  ------  ------  ----------  -------  -----------  ---------  -----  ---------------------
NFS02        10.192.164.230  /NFS02  None          true     true            4      false  false  Supported
NFS01        10.192.164.225  /NFS01  None          true     true            4      false  false  Supported
[root@MCCA01:~]
```

NFS 데이터스토어에 vCenter를 배포합니다. vCenter 어플라이언스에서 SSH 및 Bash 셸이 활성화되어 있는지 확인하세요.

vSphere 클러스터 생성

1. vSphere 웹 클라이언트에 로그인하고 NFS VAAI가 배포된 호스트 중 하나를 추가하여 데이터 센터와 vSphere 클러스터를 만듭니다. 우리는 클러스터의 모든 호스트를 단일 이미지 옵션으로 관리하기로 결정했습니다. [팁] 클러스터 수준에서 구성 관리를 선택하지 마세요. 추가 세부 사항은 다음을 참조하세요. "vSphere 클러스터에 대한 NSX 고려 사항" . ONTAP MetroCluster 사용한 vMSC 모범 사례는 다음을 확인하세요. "vMSC 설계 및 구현 지침"
2. 클러스터에 다른 vSphere 호스트를 추가합니다.
3. 분산 스위치를 생성하고 포트 그룹을 추가합니다.
4. "표준 vSwitch에서 분산 스위치로 네트워킹을 마이그레이션합니다."

vSphere 환경을 VCF 관리 도메인으로 변환

다음 섹션에서는 SDDC 관리자를 배포하고 vSphere 8 클러스터를 VCF 5.2 관리 도메인으로 변환하는 단계를 설명합니다. 필요한 경우, 추가 세부 정보는 VMware 문서를 참조하세요.

Broadcom의 VMware에서 제공하는 VCF 가져오기 도구는 vCenter 어플라이언스와 SDDC 관리자 모두에서 구성을 검증하고 vSphere 및 VCF 환경에 대한 변환 및 가져오기 서비스를 제공하는 유틸리티입니다.

자세한 내용은 다음을 참조하세요. "VCF 가져오기 도구 옵션 및 매개변수" .

VCF 가져오기 도구 복사 및 추출

VCF 가져오기 도구는 vCenter 어플라이언스에서 vSphere 클러스터가 VCF 변환 또는 가져오기 프로세스에 적합한지 확인하는 데 사용됩니다.

다음 단계를 완료하세요.

1. 다음 단계를 따르세요 "VCF 가져오기 도구를 대상 vCenter Appliance에 복사합니다." VMware Docs에서 VCF 가져오기 도구를 올바른 위치로 복사하세요.
2. 다음 명령을 사용하여 번들을 추출합니다.

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

vCenter 어플라이언스 검증

변환하기 전에 VCF 가져오기 도구를 사용하여 vCenter 어플라이언스를 검증합니다.

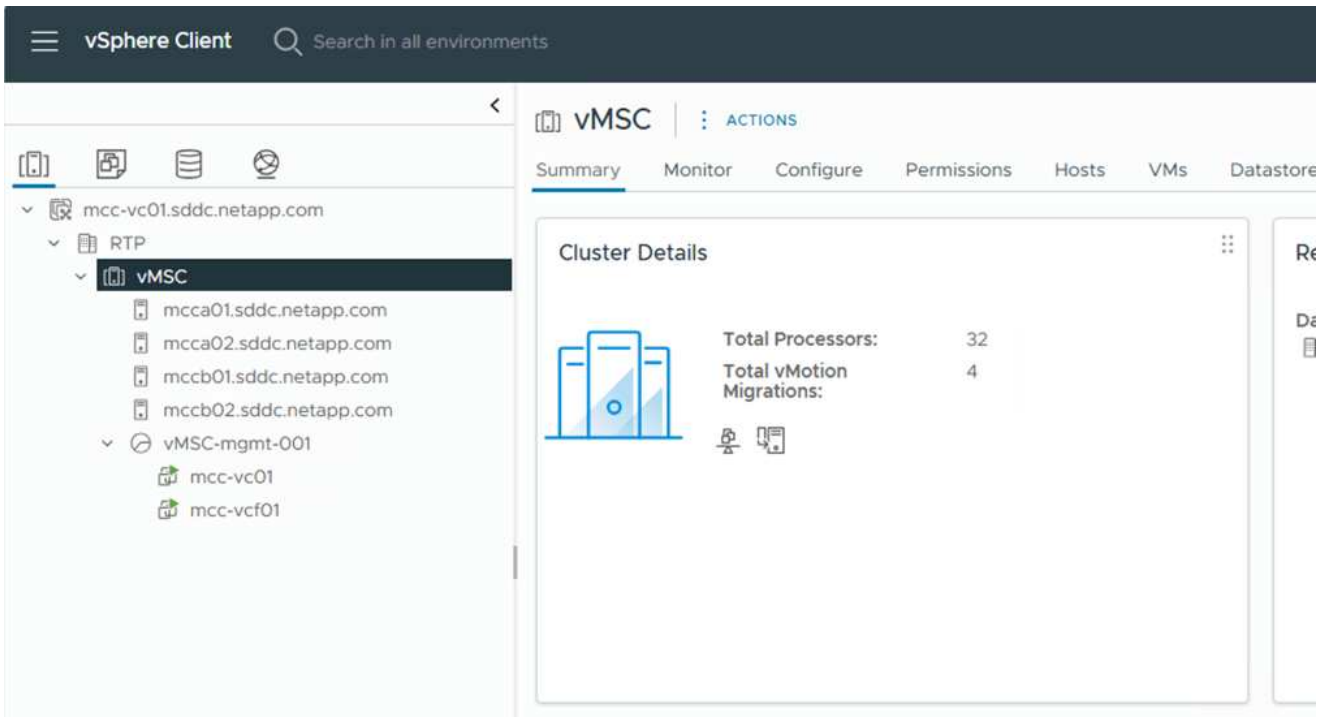
1. 다음 단계를 따르세요 "변환 전 대상 vCenter에서 사전 확인 실행" 검증을 실행하려면.
2. 다음 출력은 vCenter 어플라이언스가 사전 검사를 통과했음을 보여줍니다.

```
root@mcc-vc01 [ ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter mcc-vc01.sddc.netapp.com --sso-user administrator@vsphere.local
[2025-03-20 23:02:02,518] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.2-24494579
[2025-03-20 23:02:02,521] [INFO] vcf_brownfield: Please make sure you are always using the latest version of the scripts
Enter vCenter SSO password:
[2025-03-20 23:02:05,971] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2025-03-20 23:02:06,089] [INFO] vc_precheck: Connected to vCenter mcc-vc01.sddc.netapp.com in 0.12 seconds
[2025-03-20 23:02:06,092] [INFO] vc_precheck: Running pre-checks for vCenter mcc-vc01.sddc.netapp.com...
[2025-03-20 23:02:06,092] [INFO] vc_precheck: [1/10] VC BOM version check...                    PASS
[2025-03-20 23:02:06,135] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...            PASS
[2025-03-20 23:02:06,156] [INFO] vc_precheck: [3/10] Supported storage available check...       PASS
[2025-03-20 23:02:06,170] [INFO] vc_precheck: [4/10] vCenter VM location check...               PASS
[2025-03-20 23:02:06,424] [INFO] vc_precheck: [5/10] VxRail registration check...               PASS
[2025-03-20 23:02:06,614] [INFO] vc_precheck: [6/10] NSX-T registration check...                PASS
[2025-03-20 23:02:06,638] [INFO] vc_precheck: [7/10] Standalone host check...                   PASS
[2025-03-20 23:02:08,820] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...PASS
[2025-03-20 23:02:10,246] [INFO] vc_precheck: [9/10] ELM ring topology check...                 PASS
[2025-03-20 23:02:10,879] [INFO] vc_precheck: [10/10] WCP import check...                       PASS
[2025-03-20 23:02:10,880] [INFO] vc_precheck: All pre-checks passed!
[2025-03-20 23:02:10,881] [INFO] vc_precheck: Pre-checks for vCenter mcc-vc01.sddc.netapp.com completed in 4.79 seconds
root@mcc-vc01 [ ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset ]#
```

SDDC 관리자 배포

SDDC 관리자는 VCF 관리 도메인으로 변환될 vSphere 클러스터에 함께 배치되어야 합니다.

VMware Docs의 배포 지침에 따라 배포를 완료하세요.



참조하다 "대상 vCenter에 SDDC Manager Appliance 배포" .

NSX 배포를 위한 JSON 파일 생성

vSphere 환경을 VMware Cloud Foundation으로 가져오거나 변환하는 동안 NSX Manager를 배포하려면 NSX 배포 사양을 만듭니다. NSX 배포에는 최소 3개의 호스트가 필요합니다.

> 변환 또는 가져오기 작업에서 NSX Manager 클러스터를 배포하는 경우 NSX VLAN 지원 세그먼트가 사용됩니다. NSX-VLAN 지원 세그먼트의 제한 사항에 대한 자세한 내용은 "기존 vSphere 환경을 VMware Cloud Foundation으로 변환하거나 가져오기 전 고려 사항" 섹션을 참조하세요. NSX-VLAN 네트워킹 제한 사항에 대한 정보는 다음을 참조하세요. "기존 vSphere 환경을 VMware Cloud Foundation으로 변환하거나 가져오기 전 고려 사항" .

다음은 NSX 배포를 위한 JSON 파일의 예입니다.

```
{
  "deploy_without_license_keys": true,
  "form_factor": "small",
  "admin_password": "******************",
  "install_bundle_path": "/nfs/vmware/vcf/nfs-mount/bundle/bundle-
133764.zip",
  "cluster_ip": "10.61.185.114",
  "cluster_fqdn": "mcc-nsx.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "mcc-nsxa.sddc.netapp.com",
    "name": "mcc-nsxa",
    "ip_address": "10.61.185.111",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-nsxb.sddc.netapp.com",
    "name": "mcc-nsxb",
    "ip_address": "10.61.185.112",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-nsxc.sddc.netapp.com",
    "name": "mcc-nsxc",
    "ip_address": "10.61.185.113",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

SDDC 관리자의 vcf 사용자 홈 폴더에 JSON 파일을 복사합니다.

SDDC 관리자에 소프트웨어 업로드

VCF 가져오기 도구를 vcf 사용자의 홈 폴더로 복사하고 NSX 배포 번들을 SDDC 관리자의 /nfs/vmware/vcf/nfs-mount/bundle/ 폴더로 복사합니다.

보다 "SDDC 관리자 어플라이언스에 필요한 소프트웨어 업로드" 자세한 지침은 여기를 참조하세요.

변환 전 **vCenter**에 대한 자세한 확인

관리 도메인 변환 작업이나 VI 워크로드 도메인 가져오기 작업을 수행하기 전에 기존 vSphere 환경의 구성이 변환 또는 가져오기에 지원되는지 확인하기 위해 자세한 검사를 수행해야 합니다. . SDDC 관리자 어플라이언스에 사용자 vcf로 SSH를 실행합니다. . VCF 가져오기 도구를 복사한 디렉토리로 이동합니다. . 다음 명령을 실행하여 vSphere 환경을 변환할 수 있는지 확인하세요.

```
python3 vcf_brownfield.py check --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '********' --local-admin-password
'****************' --accept-trust
```

vSphere 클러스터를 VCF 관리 도메인으로 변환

VCF 가져오기 도구는 변환 과정을 수행하는 데 사용됩니다.

다음 명령은 vSphere 클러스터를 VCF 관리 도메인으로 변환하고 NSX 클러스터를 배포하기 위해 실행됩니다.

```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '******' --vcenter-root-password '********'
--local-admin-password '****************' --backup-password
'****************' --domain-name '<Mgmt-domain-name>' --accept-trust
--nsx-deployment-spec-path /home/vcf/nsx.json
```

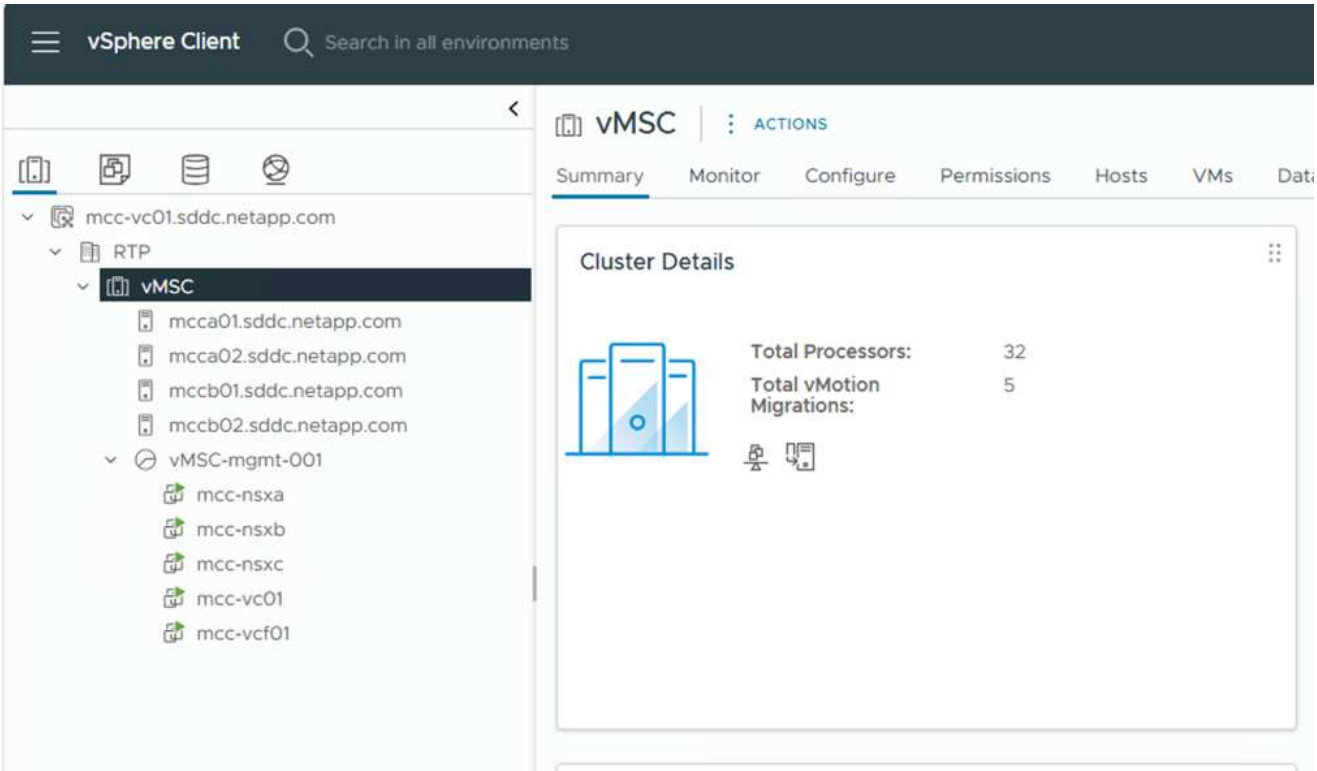
vSphere 호스트에서 여러 개의 데이터스토어를 사용할 수 있는 경우 기본적으로 NSX VM이 배포될 기본 데이터스토어로 간주해야 하는 데이터스토어가 무엇인지 묻습니다

.

전체 지침은 다음을 참조하세요. "VCF 변환 절차" .

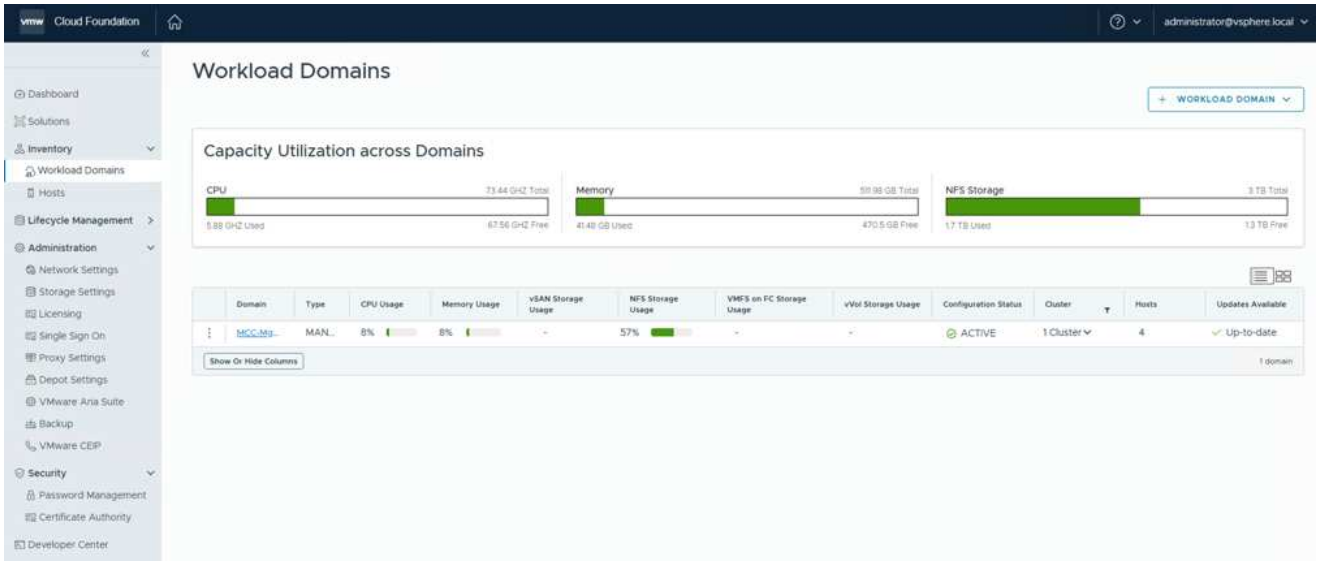
NSX VM은 vCenter에 배포됩니다

.



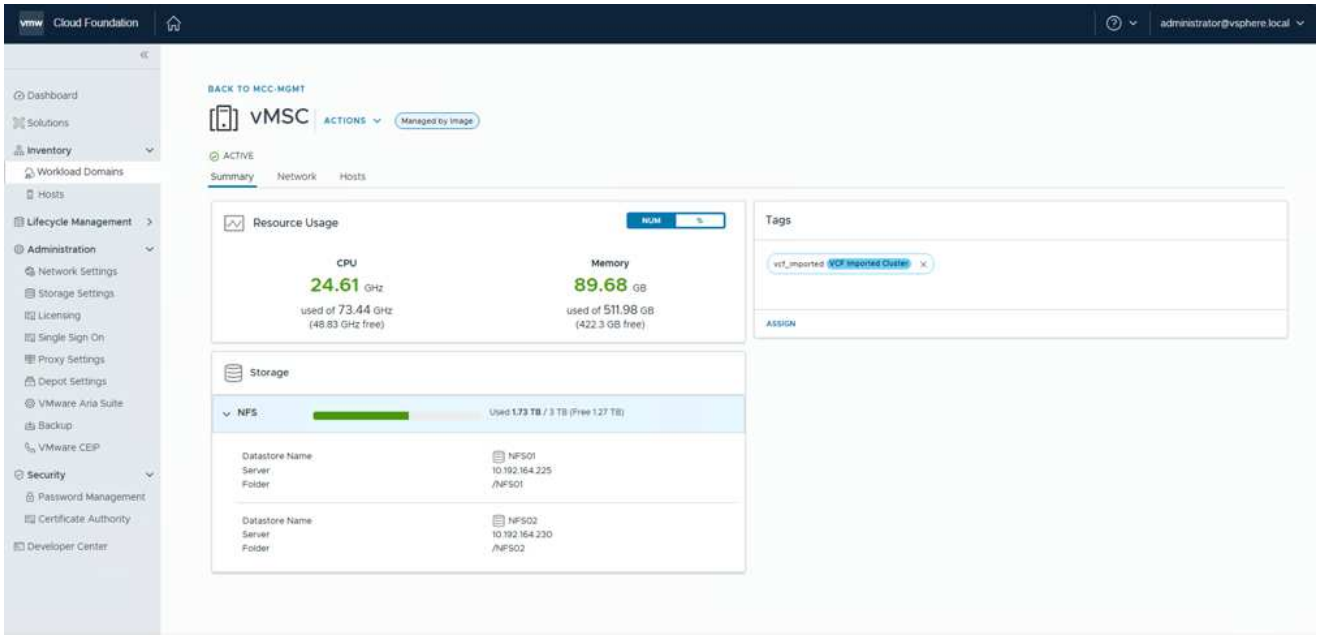
SDDC 관리자는 제공된 이름으로 생성된 관리 도메인과 데이터 저장소로 NFS를 표시합니다

.



클러스터를 검사하면 NFS 데이터 저장소에 대한 정보가 제공됩니다

.



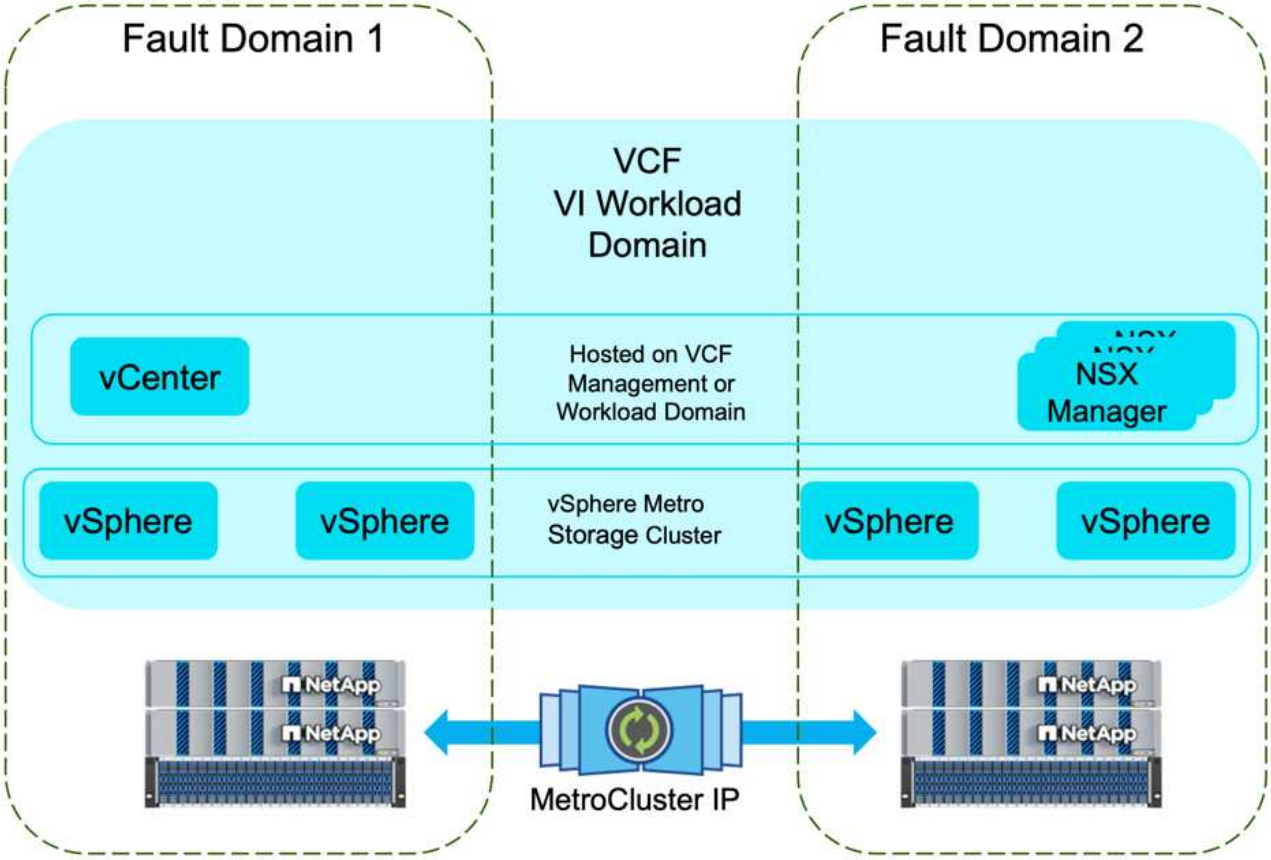
변환을 완료한 후에는 환경에 라이선스를 추가해야 합니다.

1. SDDC 관리자 UI에 로그인합니다.
2. 탐색 창에서 *관리 > 라이선싱*으로 이동합니다.
3. *+ 라이선스 키*를 클릭하세요.
4. 드롭다운 메뉴에서 제품을 선택하세요.
5. 라이센스 키를 입력하세요.
6. 라이센스에 대한 설명을 제공하세요.
7. *추가*를 클릭하세요.
8. 각 라이선스에 대해 이 단계를 반복합니다.

MetroCluster 사용하여 VI 워크로드 도메인에 대한 스트레치 클러스터 구성

이 사용 사례에서는 ONTAP MetroCluster 사용하여 NFS를 주 데이터 저장소로 하는 확장된 VCF VI 워크로드 도메인을 구성하는 절차를 설명합니다. 이 절차에는 vSphere 호스트와 vCenter Server 배포, NFS 데이터 저장소 프로비저닝, vSphere 클러스터 검증, VCF 변환 중 NSX 구성, vSphere 환경을 기존 VCF 관리 도메인으로 가져오는 작업이 포함됩니다.

VCF의 작업 부하는 vSphere Metro Storage Cluster(vMSC)로 보호됩니다. FC 또는 IP 배포가 가능한 ONTAP MetroCluster 일반적으로 VMFS 및 NFS 데이터 저장소의 내결함성을 제공하는 데 활용됩니다.



소개

이 솔루션에서는 ONTAP MetroCluster 사용하여 NFS를 주 데이터 저장소로 사용하여 Stetched VCF VI 워크로드 도메인을 구현하는 방법을 보여드리겠습니다. VI 워크로드 도메인은 SDDC Manager를 사용하여 배포하거나 기존 vSphere 환경을 VI 워크로드 도메인으로 가져올 수 있습니다.

시나리오 개요

이 시나리오에서는 다음과 같은 상위 수준 단계를 다룹니다.

- vSphere 호스트와 vCenter 서버를 배포합니다.
- vSphere 호스트에 NFS 데이터 저장소를 프로비저닝합니다.
- VCF 가져오기 도구를 사용하여 vSphere 클러스터를 검증합니다.
- VCF 변환 중에 NSX를 생성하기 위해 JSON 파일을 구성합니다.
- VCF 가져오기 도구를 사용하여 vSphere 8 환경을 VCF VI 워크로드 도메인으로 기존 VCF 관리 도메인으로 가져옵니다.

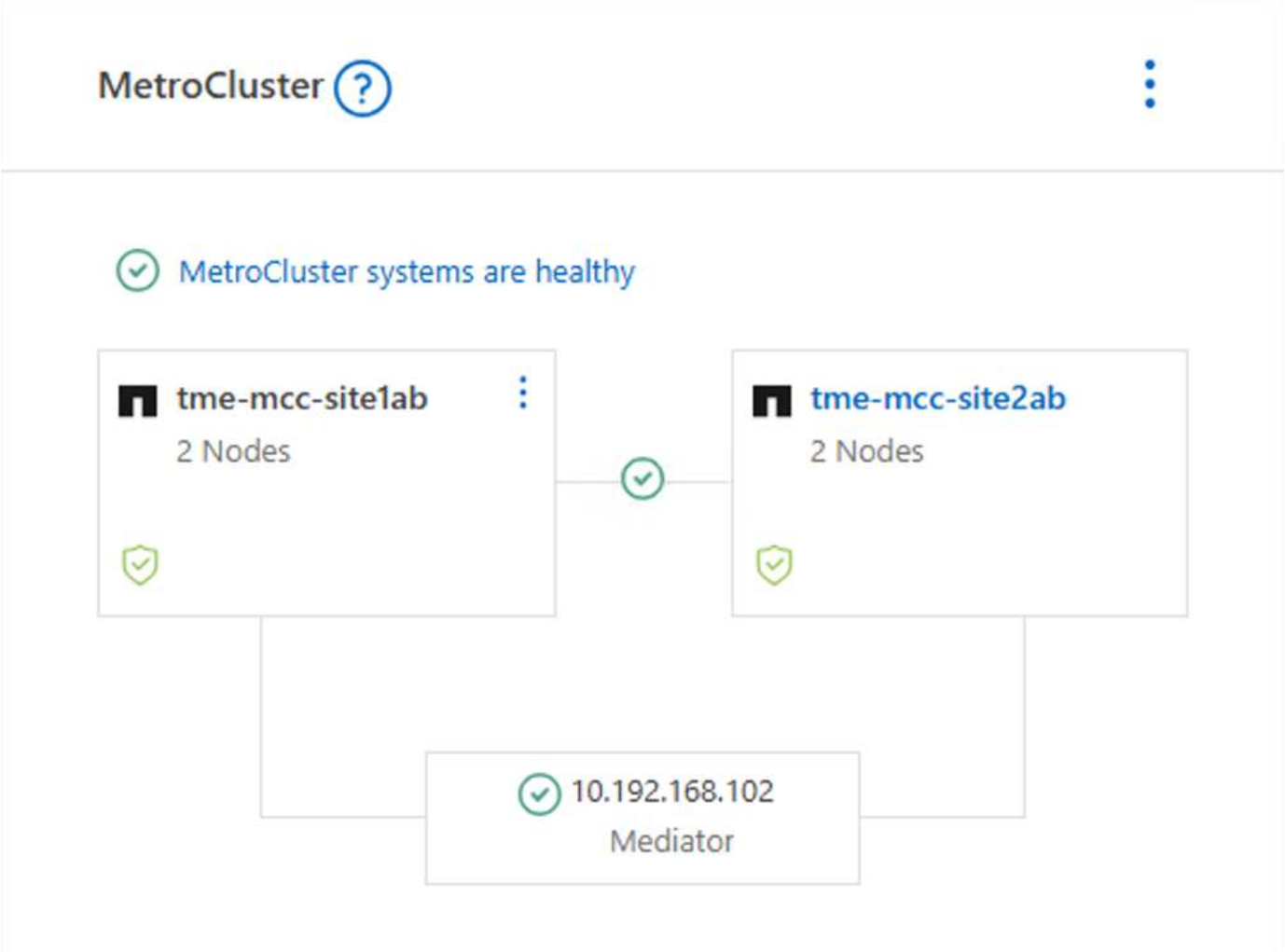
필수 조건

이 시나리오에는 다음과 같은 구성 요소와 구성이 필요합니다.

- 지원되는 ONTAP MetroCluster 구성

- NFS 트래픽을 허용하도록 구성된 스토리지 가상 머신(SVM)입니다.
- NFS 트래픽을 전달하고 SVM과 연관되는 논리적 인터페이스(LIF)가 IP 네트워크에 생성되었습니다.
- 네트워크 스위치에 연결된 4개의 ESXi 호스트가 있는 vSphere 8 클러스터.
- VCF 변환에 필요한 소프트웨어를 다운로드하세요.

다음은 MetroCluster 구성을 보여주는 시스템 관리자의 샘플 스크린샷입니다
.



그리고 여기에 두 단층 도메인의 SVM 네트워크 인터페이스가 있습니다
.

Network interfaces Subnets

+ Add

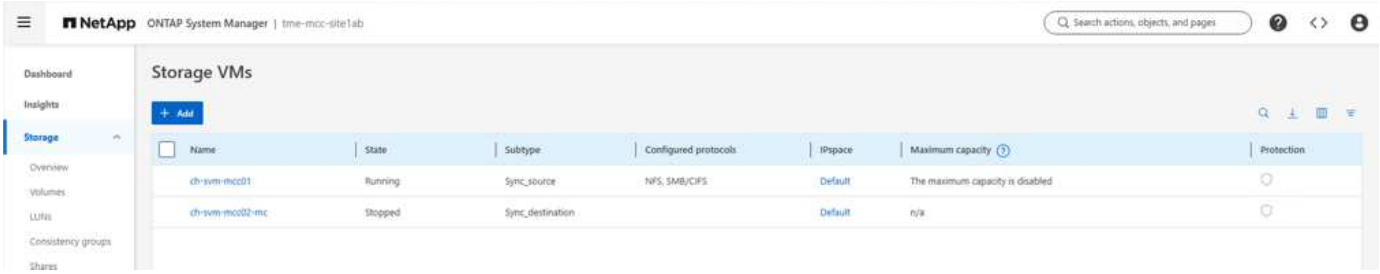
Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc02_8775		ch-svm-mcc02-mc	Default	10.192.164.230	tme-mcc-site1a
lif_ch-svm-mcc01_3118		ch-svm-mcc01	Default	10.192.164.225	tme-mcc-site1a
lif_ch-svm-mcc02_9778		ch-svm-mcc02-mc	Default	10.192.164.231	tme-mcc-site1b
lif_ch-svm-mcc01_6783		ch-svm-mcc01	Default	10.192.164.226	tme-mcc-site1b

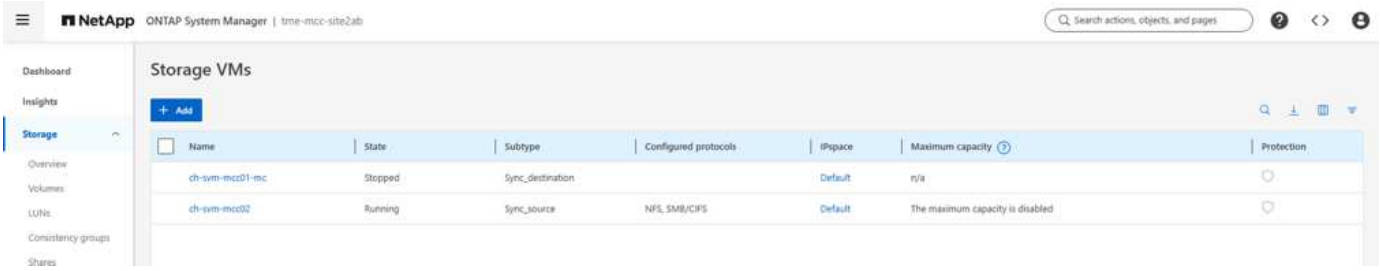
Network interfaces Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc01_3118		ch-svm-mcc01-mc	Default	10.192.164.225	tme-mcc-site2a
lif_ch-svm-mcc02_8775		ch-svm-mcc02	Default	10.192.164.230	tme-mcc-site2a
lif_ch-svm-mcc01_6783		ch-svm-mcc01-mc	Default	10.192.164.226	tme-mcc-site2b
lif_ch-svm-mcc02_9778		ch-svm-mcc02	Default	10.192.164.231	tme-mcc-site2b

[참고] SVM은 MetroCluster 의 오류 도메인 중 하나에서 활성화됩니다.





나타내다 "MetroCluster 를 갖춘 vMSC" .

vSphere를 VCF 5.2로 변환하거나 가져오기 위해 지원되는 저장소 및 기타 고려 사항은 다음을 참조하세요. "기존 vSphere 환경을 VMware Cloud Foundation으로 변환하거나 가져오기 전 고려 사항" .

VCF 관리 도메인으로 변환될 vSphere 클러스터를 생성하기 전에 다음을 참조하세요. "vSphere 클러스터에 대한 NSX 고려 사항"

필수 소프트웨어는 다음을 참조하세요. "기존 vSphere 환경을 변환하거나 가져오기 위한 소프트웨어 다운로드" .

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

배포 단계

NFS를 주 데이터 저장소로 사용하여 VCF Stretched Management Domain을 배포하려면

다음 단계를 완료하세요.

- vSphere 호스트와 vCenter를 배포합니다.
- vSphere 클러스터를 생성합니다.
- NFS 데이터 저장소를 제공합니다.
- VCF 가져오기 도구를 vCenter 어플라이언스에 복사합니다.
- VCF 가져오기 도구를 사용하여 vCenter 어플라이언스에 대한 사전 검사를 실행합니다.
- 가져오기 프로세스 중에 배포할 NSX 클러스터에 대한 JSON 파일을 만듭니다.
- 필요한 소프트웨어를 SDDC 관리자에 업로드합니다.
- vSphere 클러스터를 VCF VI 워크로드 도메인으로 변환합니다.

변환 프로세스 개요는 다음을 참조하세요. "VMware Cloud Foundation에서 vSphere 환경을 관리 도메인으로 변환하거나 vSphere 환경을 VI 워크로드 도메인으로 가져오기" .

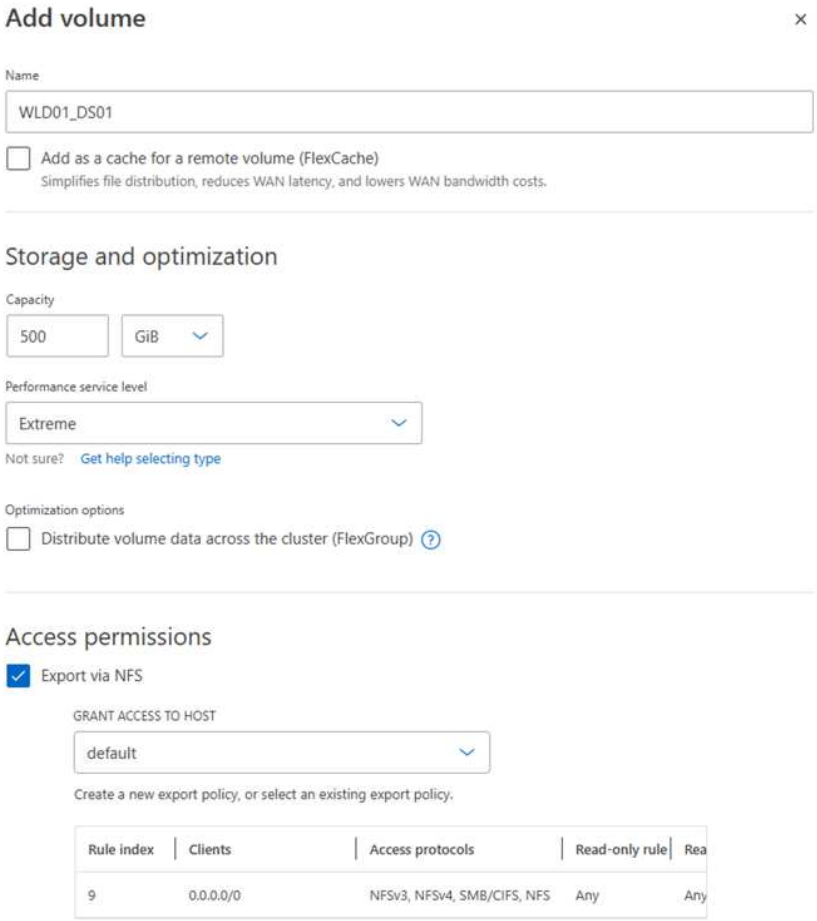
vSphere 호스트 및 **vCenter** 배포

Broadcom 지원 포털에서 다운로드한 ISO를 사용하여 호스트에 vSphere를 배포하거나 vSphere 호스트에 대한 기존 배포 옵션을 사용합니다.

VM을 호스팅하기 위해 **NFS** 데이터 저장소를 마운트합니다.

이 단계에서는 NFS 볼륨을 생성하고 이를 VM을 호스팅하기 위한 데이터 저장소로 마운트합니다.

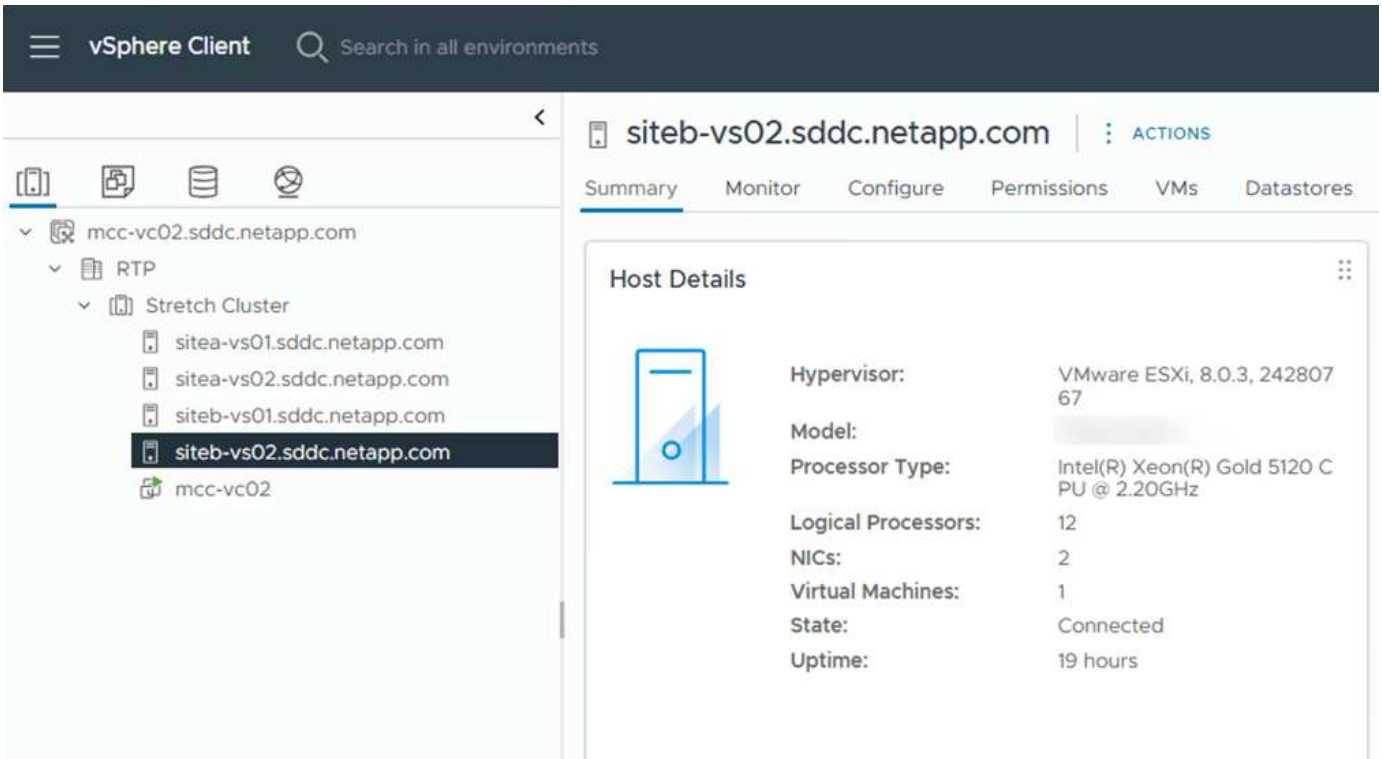
1. 시스템 관리자를 사용하여 볼륨을 생성하고 vSphere 호스트의 IP 서브넷을 포함하는 내보내기 정책에 연결합니다.



2. vSphere 호스트에 SSH를 실행하고 NFS 데이터스토어를 마운트합니다.

```
esxcli storage nfs add -c 4 -H 10.192.164.225 -s /WLD01_DS01 -v DS01
esxcli storage nfs add -c 4 -H 10.192.164.230 -s /WLD01_DS02 -v DS02
esxcli storage nfs list
```

NFS 데이터스토어에 vCenter를 배포합니다. vCenter 어플라이언스에서 SSH 및 Bash 셸이 활성화되어 있는지 확인하세요.



vSphere 클러스터 생성

1. vSphere 웹 클라이언트에 로그인하고 NFS VAAI가 배포된 호스트 중 하나를 추가하여 데이터 센터와 vSphere 클러스터를 만듭니다. 우리는 클러스터의 모든 호스트를 단일 이미지 옵션으로 관리하기로 결정했습니다. [팁] 클러스터 수준에서 구성 관리를 선택하지 마세요. 추가 세부 사항은 다음을 참조하세요. "vSphere 클러스터에 대한 NSX 고려 사항" . ONTAP MetroCluster 사용한 vMSC 모범 사례는 다음을 확인하세요. "vMSC 설계 및 구현 지침"
2. 클러스터에 다른 vSphere 호스트를 추가합니다.
3. 분산 스위치를 생성하고 포트 그룹을 추가합니다.
4. "표준 vSwitch에서 분산 스위치로 네트워킹을 마이그레이션합니다."

vSphere 환경을 **VCF VI** 워크로드 도메인으로 변환

다음 섹션에서는 SDDC 관리자를 배포하고 vSphere 8 클러스터를 VCF 5.2 관리 도메인으로 변환하는 단계를 설명합니다. 필요한 경우, 추가 세부 정보는 VMware 문서를 참조하세요.

Broadcom의 VMware에서 제공하는 VCF 가져오기 도구는 vCenter 어플라이언스와 SDDC 관리자 모두에서 구성을 검증하고 vSphere 및 VCF 환경에 대한 변환 및 가져오기 서비스를 제공하는 유틸리티입니다.

자세한 내용은 다음을 참조하세요. "VCF 가져오기 도구 옵션 및 매개변수" .

VCF 가져오기 도구 복사 및 추출

VCF 가져오기 도구는 vCenter 어플라이언스에서 vSphere 클러스터가 VCF 변환 또는 가져오기 프로세스에 적합한지 확인하는 데 사용됩니다.

다음 단계를 완료하세요.

1. 다음 단계를 따르세요 "VCF 가져오기 도구를 대상 vCenter Appliance에 복사합니다." VMware Docs에서 VCF 가져오기 도구를 올바른 위치로 복사하세요.
2. 다음 명령을 사용하여 번들을 추출합니다.

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

vCenter 어플라이언스 검증

VI 워크로드 도메인으로 가져오기 전에 VCF 가져오기 도구를 사용하여 vCenter 어플라이언스를 검증합니다.

1. 다음 단계를 따르세요 "변환 전 대상 vCenter에서 사전 검사 실행" 검증을 실행하려면.

NSX 배포를 위한 JSON 파일 생성

vSphere 환경을 VMware Cloud Foundation으로 가져오거나 변환하는 동안 NSX Manager를 배포하려면 NSX 배포 사양을 만듭니다. NSX 배포에는 최소 3개의 호스트가 필요합니다.

> 변환 또는 가져오기 작업에서 NSX Manager 클러스터를 배포하는 경우 NSX VLAN 지원 세그먼트가 사용됩니다. NSX-VLAN 지원 세그먼트의 제한 사항에 대한 자세한 내용은 "기존 vSphere 환경을 VMware Cloud Foundation으로 변환하거나 가져오기 전 고려 사항" 섹션을 참조하세요. NSX-VLAN 네트워킹 제한 사항에 대한 정보는 다음을 참조하세요. "기존 vSphere 환경을 VMware Cloud Foundation으로 변환하거나 가져오기 전 고려 사항" .

다음은 NSX 배포를 위한 JSON 파일의 예입니다.

```
{
  "deploy_without_license_keys": true,
  "form_factor": "small",
  "admin_password": "****************",
  "install_bundle_path": "/nfs/vmware/vcf/nfs-mount/bundle/bundle-
133764.zip",
  "cluster_ip": "10.61.185.105",
  "cluster_fqdn": "mcc-wld01-nsx.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "mcc-wld01-nsxa.sddc.netapp.com",
    "name": "mcc-wld01-nsxa",
    "ip_address": "10.61.185.106",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-wld01-nsxb.sddc.netapp.com",
    "name": "mcc-wld01-nsxb",
    "ip_address": "10.61.185.107",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-wld01-nsxc.sddc.netapp.com",
    "name": "mcc-wld01-nsxc",
    "ip_address": "10.61.185.108",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

SDDC 관리자의 vcf 사용자 홈 폴더에 JSON 파일을 복사합니다.

SDDC 관리자에 소프트웨어 업로드

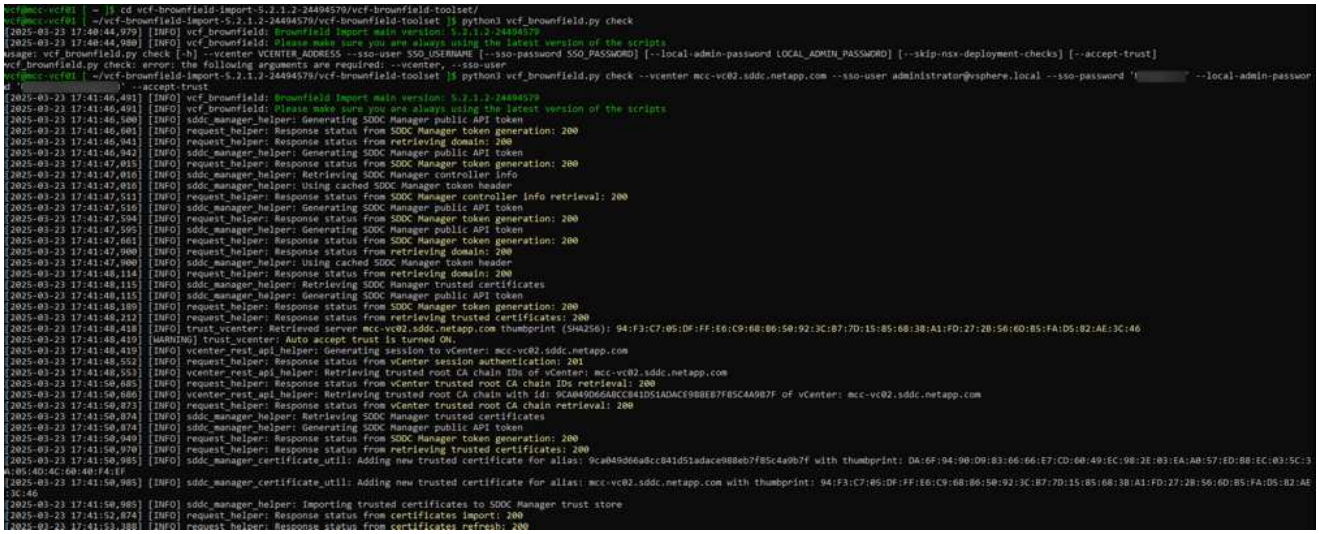
VCF 가져오기 도구를 vcf 사용자의 홈 폴더로 복사하고 NSX 배포 번들을 SDDC 관리자의 /nfs/vmware/vcf/nfs-mount/bundle/ 폴더로 복사합니다.

보다 "SDDC 관리자 어플라이언스에 필요한 소프트웨어 업로드" 자세한 지침은 여기를 참조하세요.

변환 전 **vCenter**에 대한 자세한 확인

관리 도메인 변환 작업이나 VI 워크로드 도메인 가져오기 작업을 수행하기 전에 기존 vSphere 환경의 구성이 변환 또는 가져오기에 지원되는지 확인하기 위해 자세한 검사를 수행해야 합니다. . SDDC 관리자 어플라이언스에 사용자 vcf로 SSH를 실행합니다. . VCF 가져오기 도구를 복사한 디렉토리로 이동합니다. . 다음 명령을 실행하여 vSphere 환경을 변환할 수 있는지 확인하세요.

```
python3 vcf_brownfield.py check --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '********' --local-admin-password
'****************' --accept-trust
```



vSphere 클러스터를 VCF VI 워크로드 도메인으로 변환

VCF 가져오기 도구는 변환 과정을 수행하는 데 사용됩니다.

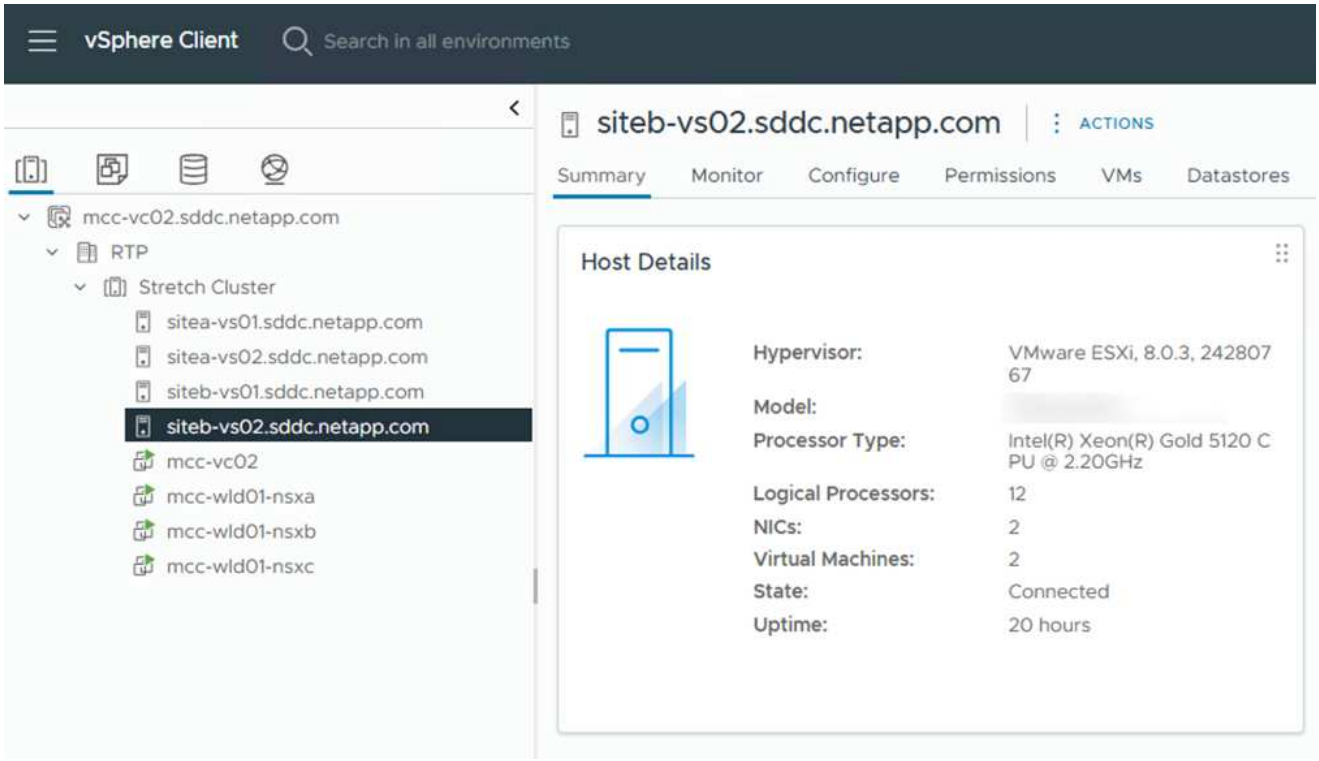
다음 명령은 vSphere 클러스터를 VCF 관리 도메인으로 변환하고 NSX 클러스터를 배포하기 위해 실행됩니다.

```
python3 vcf_brownfield.py import --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '******' --vcenter-root-password '********'
--local-admin-password '****************' --backup-password
'****************' --domain-name '<Mgmt-domain-name>' --accept-trust
--nsx-deployment-spec-path /home/vcf/nsx.json
```

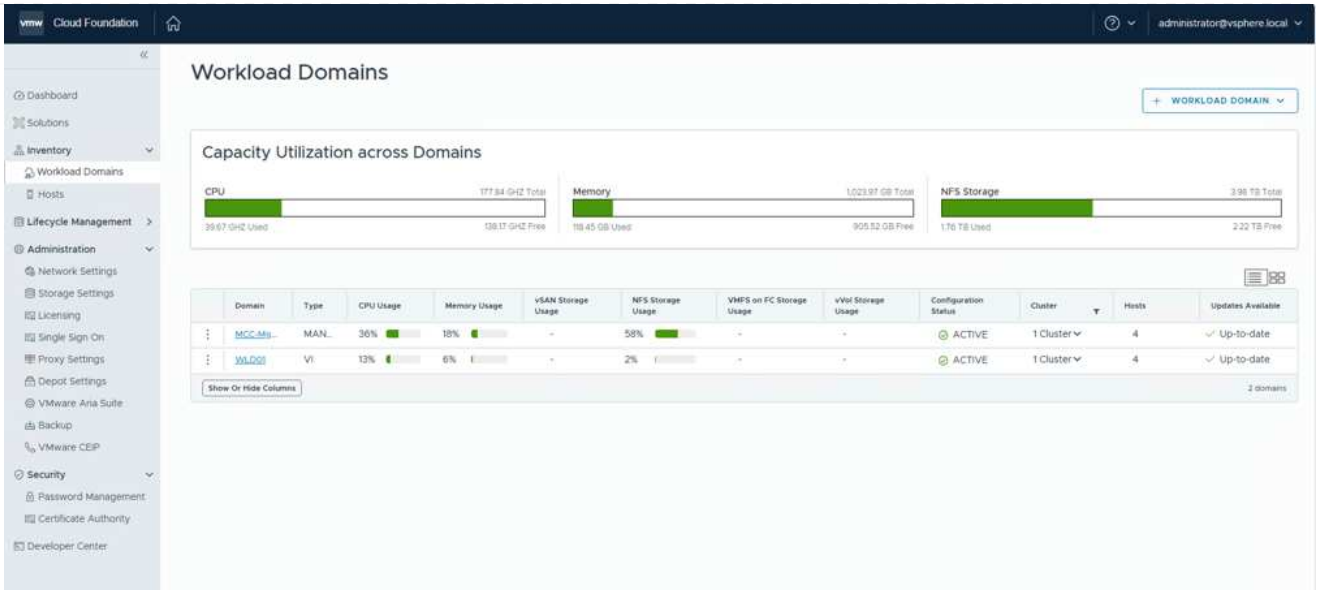
vSphere 호스트에 여러 개의 데이터스토어가 있는 경우에도 어떤 데이터스토어를 기본 데이터스토어로 간주해야 하는지 묻지 않습니다.

전체 지침은 다음을 참조하세요. "VCF 변환 절차" .

NSX VM은 vCenter에 배포됩니다
.

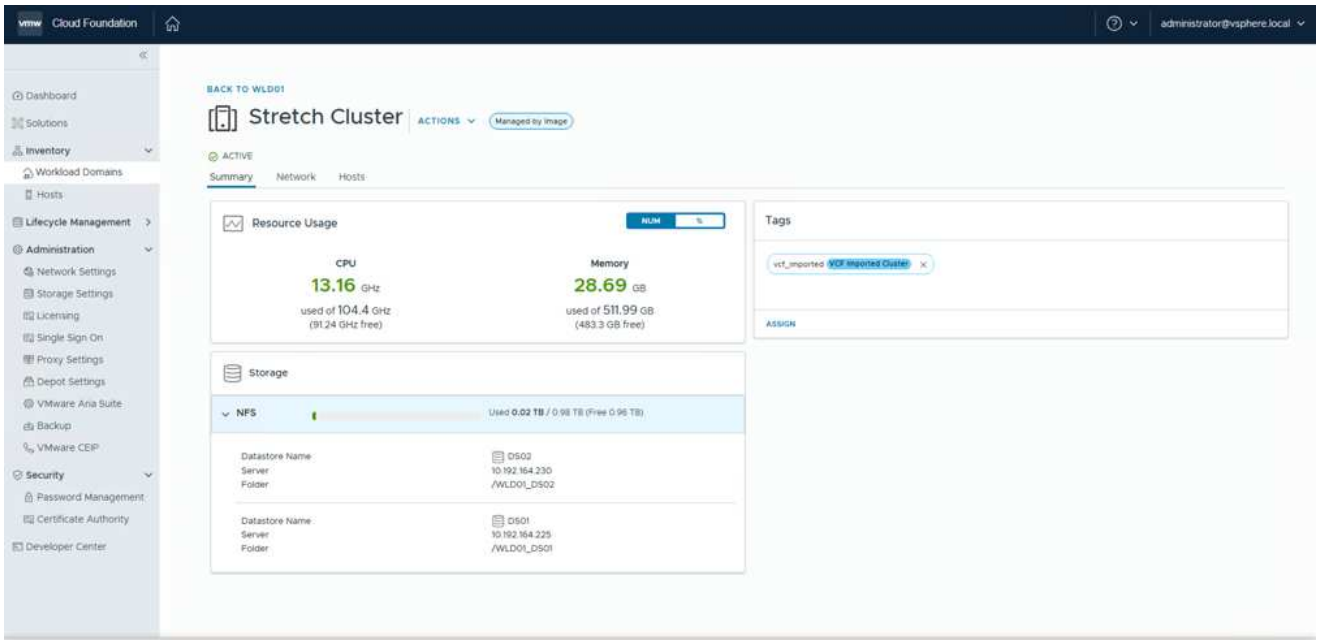


SDDC 관리자는 제공된 이름으로 생성된 VI 워크로드 도메인과 데이터 저장소로 NFS를 표시합니다
.



클러스터를 검사하면 NFS 데이터 저장소에 대한 정보가 제공됩니다

.



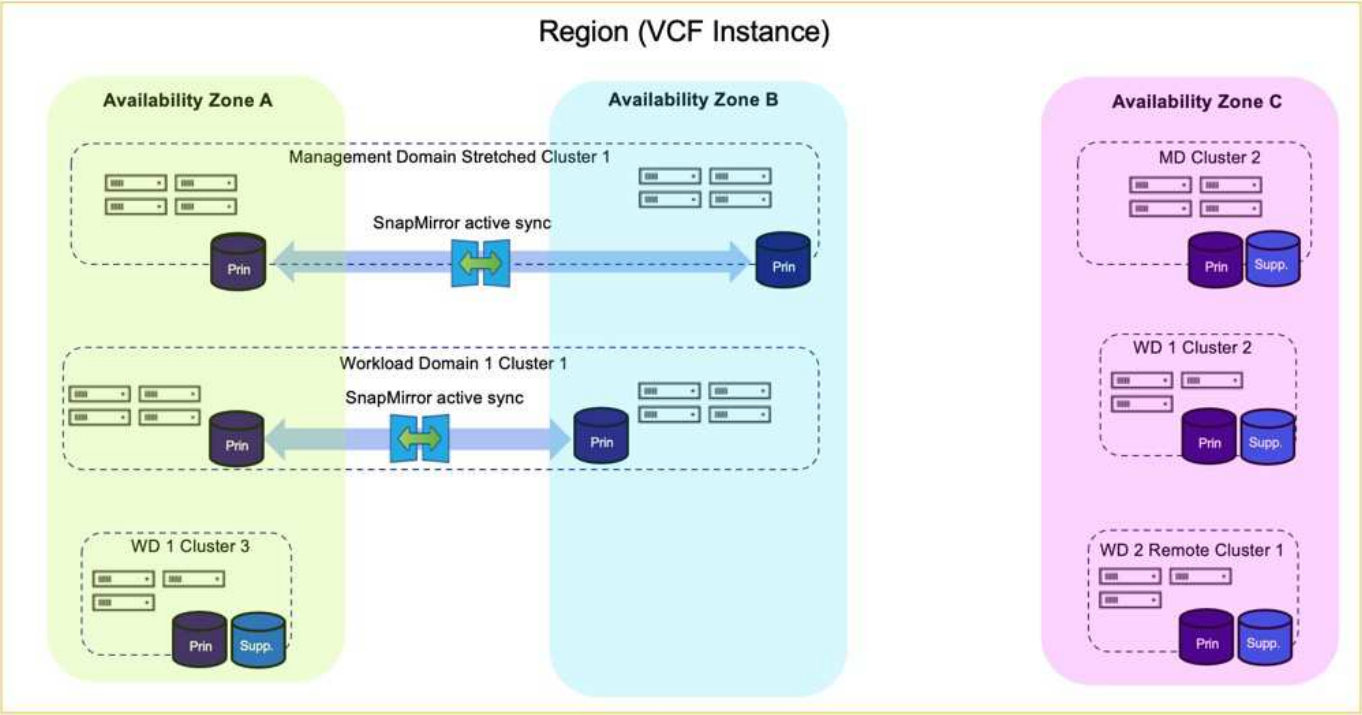
VCF에 라이선싱 추가

변환을 완료한 후에는 환경에 라이선스를 추가해야 합니다.

1. SDDC 관리자 UI에 로그인합니다.
2. 탐색 창에서 *관리 > 라이선싱*으로 이동합니다.
3. *+ 라이선스 키*를 클릭하세요.
4. 드롭다운 메뉴에서 제품을 선택하세요.
5. 라이센스 키를 입력하세요.
6. 라이센스에 대한 설명을 제공하세요.
7. *추가*를 클릭하세요.
8. 각 라이선스에 대해 이 단계를 반복합니다.

SnapMirror Active Sync를 사용하여 **VCF** 관리 도메인에 대한 스트레치 클러스터 구성

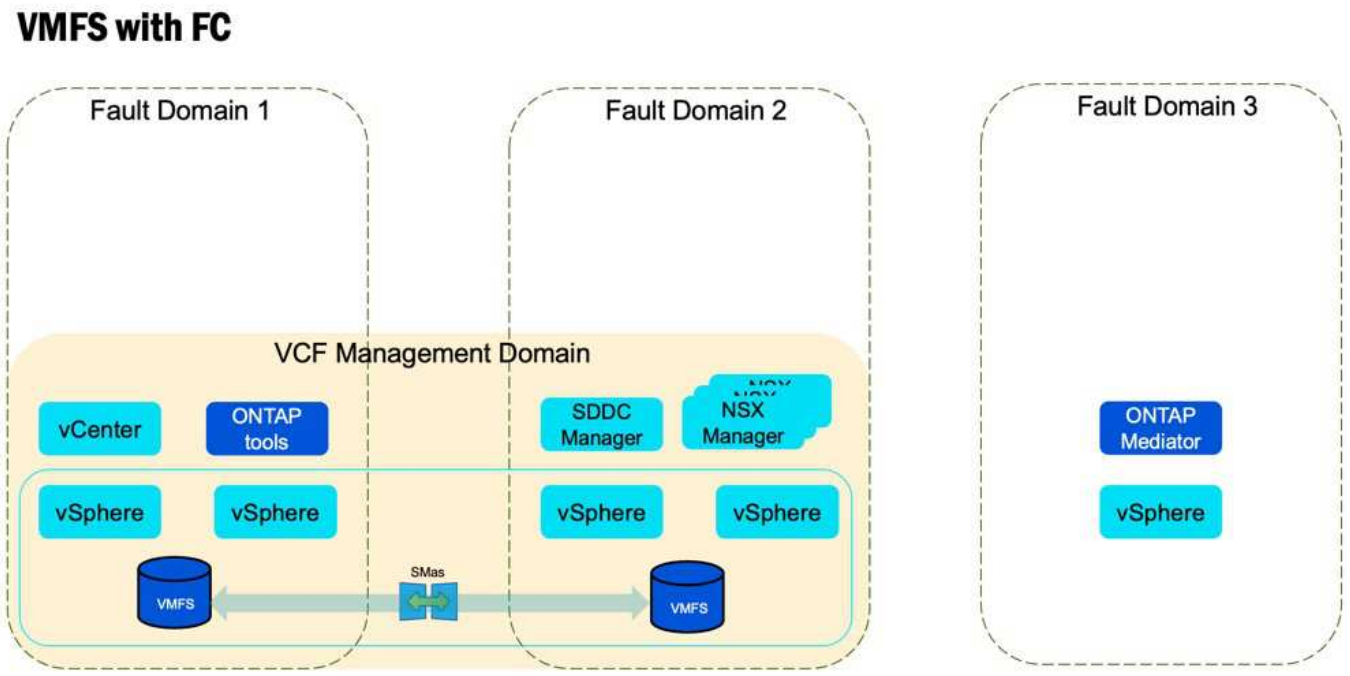
이 사용 사례에서는 ONTAP tools for VMware vSphere 사용하여 VCF 관리 도메인에 대한 스트레치 클러스터를 구성하는 절차를 설명합니다. 이 절차에는 vSphere 호스트와 vCenter Server 배포, ONTAP 도구 설치, SnapMirror Active Sync를 사용한 데이터 저장소 보호, 보호된 데이터 저장소로 VM 마이그레이션, 보조 스토리지 구성이 포함됩니다.



시나리오 개요

스트레치 클러스터 솔루션은 기본 클러스터나 VCF 관리 또는 워크로드 도메인의 추가 클러스터에 구현될 수 있습니다. FC의 VMFS는 주 데이터 저장소와 보조 데이터 저장소 모두에서 지원됩니다. iSCSI의 VMFS는 보조 데이터 저장소에서만 지원됩니다. SnapMirror 액티브 동기화를 사용하는 NVMe-oF의 VMFS 지원에 대해서는 IMT

참조하세요.



관리 도메인의 주 저장소

VCF 5.2 이상에서는 VCF 가져오기 도구를 사용하여 VSAN 없이도 관리 도메인을 배포할 수 있습니다. VCF 가져오기 도구의 변환 옵션을 사용하면"기존 vCenter 배포를 관리 도메인으로" . vCenter의 모든 클러스터는 관리 도메인의 일부가 됩니다.

1. vSphere 호스트 배포
2. 로컬 데이터 저장소에 vCenter Server를 배포합니다(vCenter는 관리 도메인으로 변환될 vSphere 호스트에 공존해야 함)
3. ONTAP tools for VMware vSphere 배포
4. VMware vSphere용 SnapCenter 플러그인 배포(선택 사항)
5. 데이터 저장소 생성(FC 영역 구성이 완료되어야 함)
6. vSphere 클러스터 보호
7. 새로 생성된 데이터 저장소로 VM 마이그레이션

클러스터가 확장되거나 축소될 때마다 클러스터의 ONTAP 도구에서 호스트 클러스터 관계를 업데이트하여 소스 또는 대상에 대한 변경 사항을 나타내야 합니다.

관리 도메인의 추가 스토리지

관리 도메인이 가동되면 ONTAP 도구를 사용하여 추가 데이터 저장소를 만들 수 있으며, 이를 통해 일관성 그룹 확장이 트리거됩니다.

vSphere 클러스터가 보호되면 클러스터의 모든 데이터 저장소도 보호됩니다.

Cloud Builder 도구를 사용하여 VCF 환경을 배포한 경우 iSCSI로 보조 스토리지를 생성하고, ONTAP 도구를 배포하여 iSCSI 데이터 저장소를 생성하고 vSphere 클러스터를 보호합니다.

클러스터가 확장되거나 축소될 때마다 클러스터의 ONTAP 도구에서 호스트 클러스터 관계를 업데이트하여 소스 또는 대상에 대한 변경 사항을 나타내야 합니다.

추가 정보

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

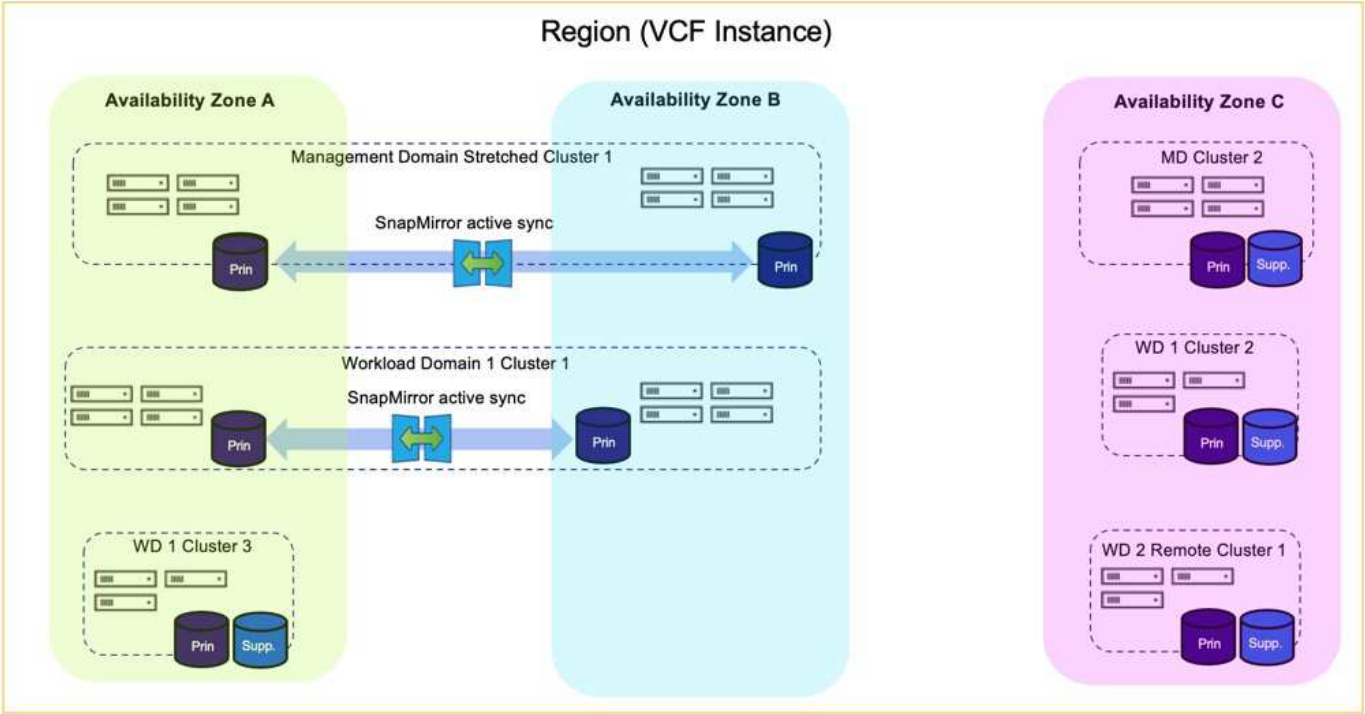
VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 5.2 설명서" .

이 솔루션에 대한 비디오 데모

ONTAP 도구를 사용한 VCF용 스트레치 클러스터

SnapMirror Active Sync를 사용하여 **VI** 워크로드 도메인에 대한 스트레치 클러스터 구성

이 사용 사례에서는 ONTAP tools for VMware vSphere 와 SnapMirror Active Sync를 사용하여 가상 인프라(VI) 워크로드 도메인에 대한 스트레치 클러스터를 구성하는 절차를 설명합니다. 이 절차에는 파이버 채널에서 VMFS를 사용하여 VCF 워크로드 도메인을 생성하고, ONTAP 도구로 vCenter를 등록하고, 스토리지 시스템을 등록하고, vSphere 클러스터를 보호하는 작업이 포함됩니다.



시나리오 개요

VCF 워크로드 도메인의 데이터 저장소는 SnapMirror Active Sync로 보호되어 스트레치 클러스터 솔루션을 제공할 수 있습니다. 보호 기능은 vSphere 클러스터 수준에서 활성화되며 클러스터의 모든 ONTAP 블록 데이터 저장소가 보호됩니다.

워크로드 도메인의 주 스토리지

워크로드 도메인은 VCF 가져오기 도구를 사용하여 가져오거나 SDDC 관리자를 사용하여 배포할 수 있습니다. SDDC 관리자를 사용하여 배포하면 기존 환경을 가져오는 것보다 더 많은 네트워킹 옵션이 제공됩니다.

1. FC에서 VMFS로 워크로드 도메인 생성
2. "vCenter 플러그인을 배포하려면 ONTAP 도구 관리자에 워크로드 도메인 vCenter를 등록하세요."
3. "ONTAP 도구에 저장 시스템 등록"
4. "vSphere 클러스터 보호"

클러스터가 확장되거나 축소될 때마다 클러스터의 ONTAP 도구에서 호스트 클러스터 관계를 업데이트하여 소스 또는 대상에 대한 변경 사항을 나타내야 합니다.

워크로드 도메인의 추가 스토리지

워크로드 도메인이 가동되고 실행되면 ONTAP 도구를 사용하여 추가 데이터 저장소를 만들 수 있으며, 이를 통해 일관성 그룹 확장이 트리거됩니다.

vSphere 클러스터가 보호되면 클러스터의 모든 데이터 저장소도 보호됩니다.

추가 정보

ONTAP 스토리지 시스템 구성에 대한 정보는 다음을 참조하세요."ONTAP 9 문서" 센터.

VCF 구성에 대한 정보는 다음을 참조하세요."VMware Cloud Foundation 문서" .

이 솔루션에 대한 비디오 데모

ONTAP 도구를 사용한 VCF용 스트레치 클러스터

VMware vSphere에서 ONTAP 데이터 저장소로 VM 마이그레이션

VMware vSphere 환경에서는 가상 머신을 NetApp ONTAP 지원 데이터 저장소로 마이그레이션하면 상당한 이점을 얻을 수 있습니다. vSAN, 타사 스토리지 시스템에서 이전하거나 기존 인프라를 업그레이드하는 경우 다양한 vMotion 시나리오와 마이그레이션 전략을 살펴보고 VM을 ONTAP 데이터 저장소로 원활하게 전환하세요. 이를 통해 ONTAP의 엔터프라이즈급 스토리지 기능을 활용하면서 비즈니스 연속성을 보장할 수 있습니다.

Broadcom의 VMware vSphere는 가상 머신을 호스팅하기 위한 VMFS, NFS 및 vVol 데이터 저장소를 지원합니다. 고객은 하이퍼 컨버지드 인프라나 중앙 집중식 공유 스토리지 시스템을 사용하여 데이터 저장소를 만들 수 있습니다.

고객은 ONTAP 기반 스토리지 시스템에서 호스팅하는 것이 공간 효율적인 스냅샷과 가상 머신 복제본을 제공하고, 데이터 센터와 클라우드에서 다양한 배포 모델을 선택할 수 있는 유연성, 모니터링 및 알림 도구를 통한 운영 효율성, 보안, 거버넌스 및 VM 데이터를 검사할 수 있는 선택적 규정 준수 도구 등을 제공하는 데 가치가 있다고 생각하는 경우가 많습니다.

ONTAP 데이터스토어에 호스팅된 VM은 VMware vSphere(SCV)용 SnapCenter 플러그인을 사용하여 보호할 수 있습니다. SCV는 스토리지 기반 스냅샷을 생성하고 원격 ONTAP 스토리지 시스템에도 복제합니다. 복원은 기본 또는 보조 스토리지 시스템에서 수행할 수 있습니다.

고객은 Cloud Insights 나 Aria Operations를 선택하거나 두 가지를 조합하거나 ONTAP API를 사용하여 문제 해결, 성능 모니터링, 보고 및 알림 기능을 제공하는 타사 도구를 선택할 수 있는 유연성을 갖습니다.

고객은 ONTAP Tools vCenter 플러그인이나 API를 사용하여 데이터스토어를 쉽게 프로비저닝할 수 있으며, 전원이 켜져 있는 동안에도 VM을 ONTAP 데이터스토어로 마이그레이션할 수 있습니다.

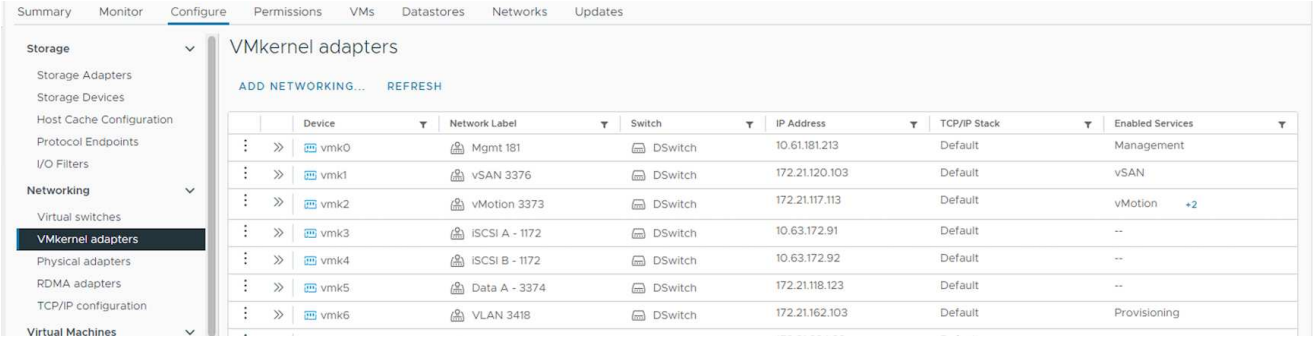
> Aria Automation, Tanzu(또는 기타 Kubernetes 플레이버)와 같은 외부 관리 도구를 사용하여 배포된 일부 VM은 일반적으로 VM 스토리지 정책에 따라 달라집니다. 동일한 VM 스토리지 정책 내에서 데이터 저장소 간에 마이그레이션하는 경우 애플리케이션에 미치는 영향이 적어야 합니다. 애플리케이션 소유자에게 문의하여 해당 VM을 새 데이터 저장소로 올바르게 마이그레이션하세요. vSphere 8이 도입되었습니다. "지연 시간에 민감한 애플리케이션을 위한 vSphere vMotion 알림" vMotion에 대한 애플리케이션을 준비합니다.

네트워크 요구 사항

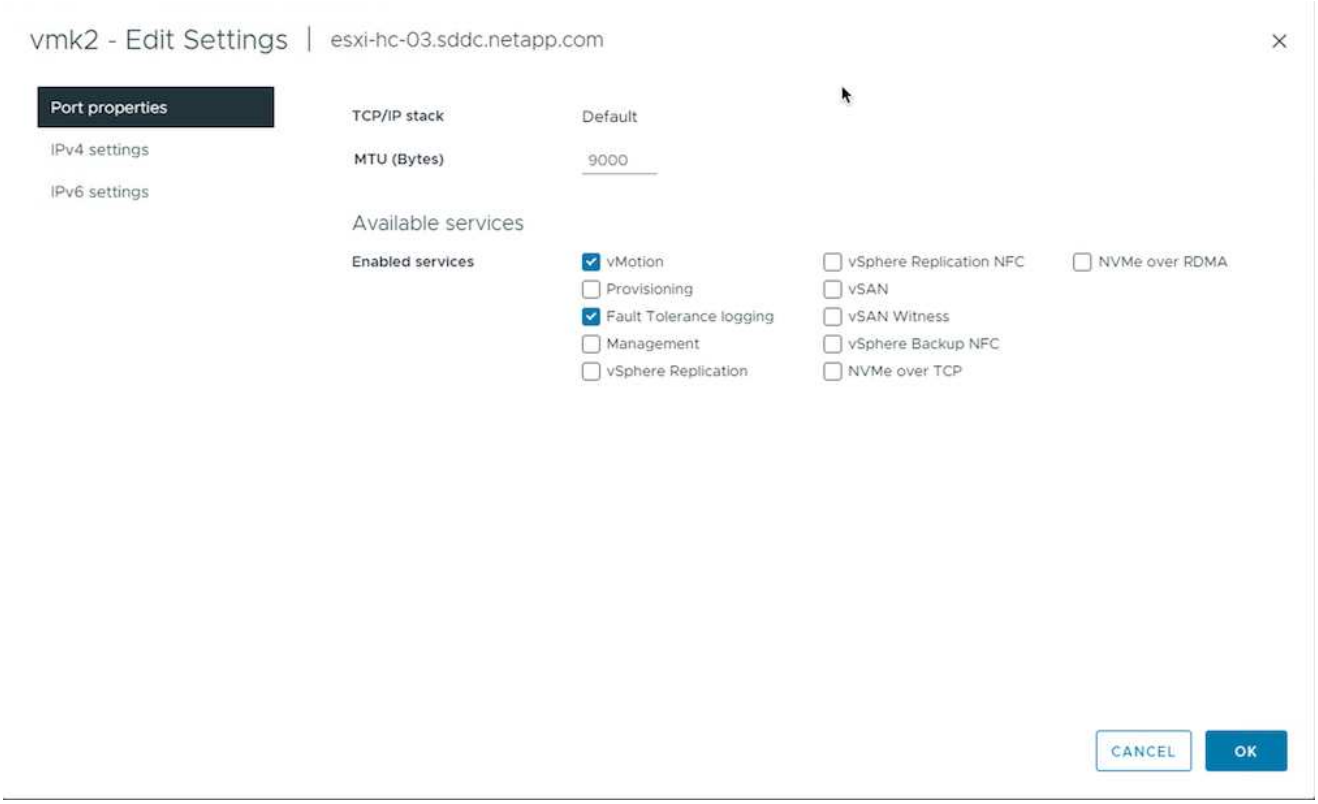
vMotion을 사용한 **VM** 마이그레이션

ONTAP 데이터 저장소에는 연결성, 내결함성 및 성능 향상을 제공하기 위해 이중 스토리지 네트워크가 이미 구축되어 있다고 가정합니다.

vSphere 호스트 간의 VM 마이그레이션도 vSphere 호스트의 VMKernel 인터페이스를 통해 처리됩니다. 핫 마이그레이션(전원이 켜진 VM)의 경우 vMotion이 활성화된 서비스가 있는 VMKernel 인터페이스가 사용되고, 콜드 마이그레이션(전원이 꺼진 VM)의 경우 프로비저닝 서비스가 활성화된 VMKernel 인터페이스가 데이터를 이동하는 데 사용됩니다. 유효한 인터페이스를 찾을 수 없는 경우 관리 인터페이스를 사용하여 데이터를 이동하는데, 이는 특정 사용 사례에서는 바람직하지 않을 수 있습니다.



VMKernel 인터페이스를 편집할 때 필요한 서비스를 활성화하는 옵션이 있습니다.



vMotion 및 Provisioning VMkernel 인터페이스에서 사용하는 포트 그룹에 대해 최소 두 개의 고속 활성 업링크 NIC를 사용할 수 있는지 확인하세요.

VM 마이그레이션 시나리오

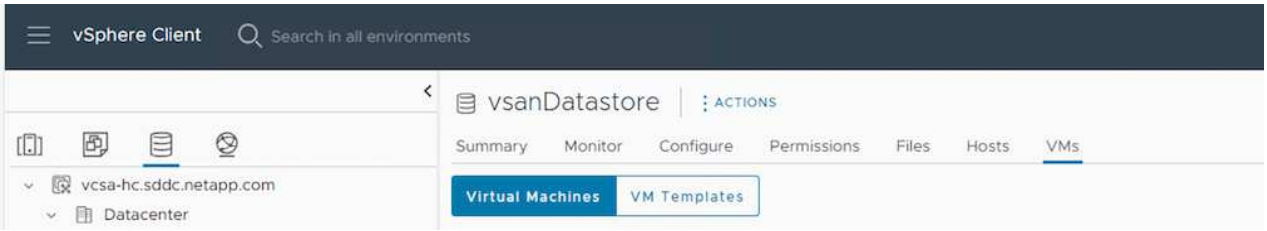
vMotion은 전원 상태와 관계없이 VM을 마이그레이션하는 데 자주 사용됩니다. 특정 시나리오에 대한 추가 고려 사항과 마이그레이션 절차는 아래에서 확인할 수 있습니다.

이해하다 "vSphere vMotion의 VM 조건 및 제한 사항" VM 마이그레이션 옵션을 진행하기 전에.

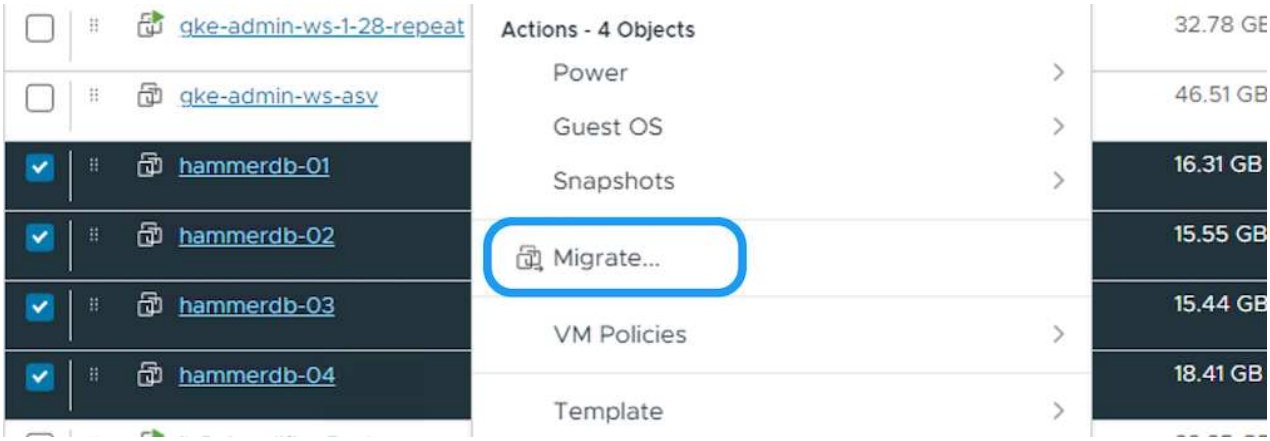
특정 **vSphere Datastore**에서 **VM** 마이그레이션

UI를 사용하여 VM을 새 데이터 저장소로 마이그레이션하려면 아래 절차를 따르세요.

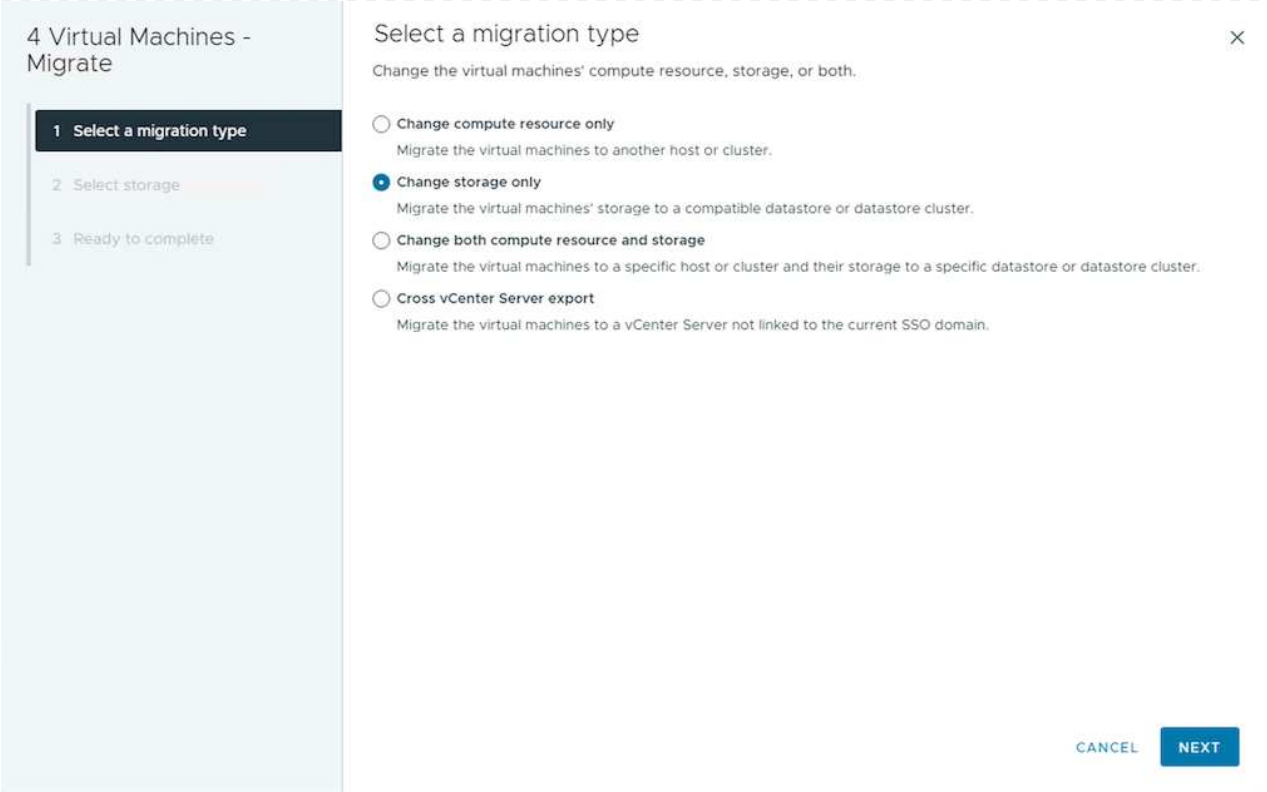
1. vSphere Web Client를 사용하여 스토리지 인벤토리에서 데이터스토어를 선택하고 VM 탭을 클릭합니다.



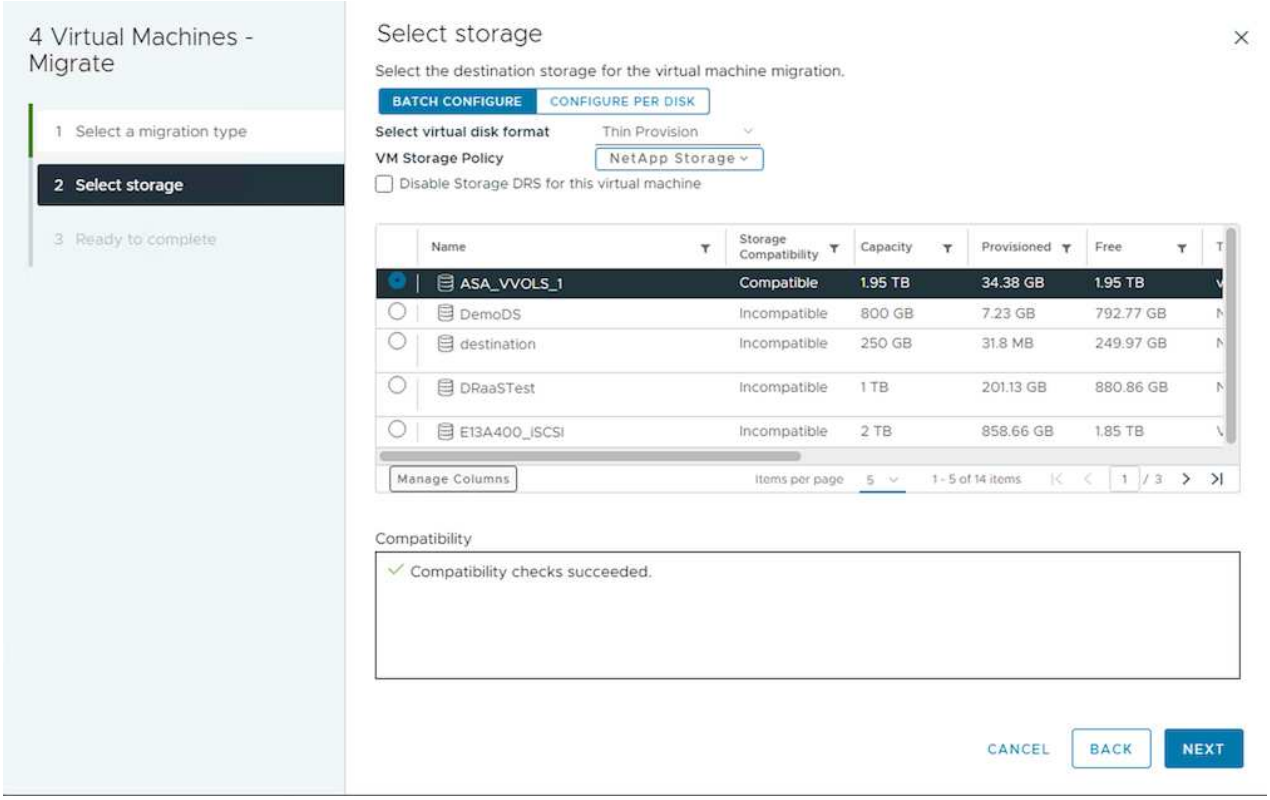
2. 마이그레이션이 필요한 VM을 선택하고 마우스 오른쪽 버튼을 클릭하여 마이그레이션 옵션을 선택합니다.



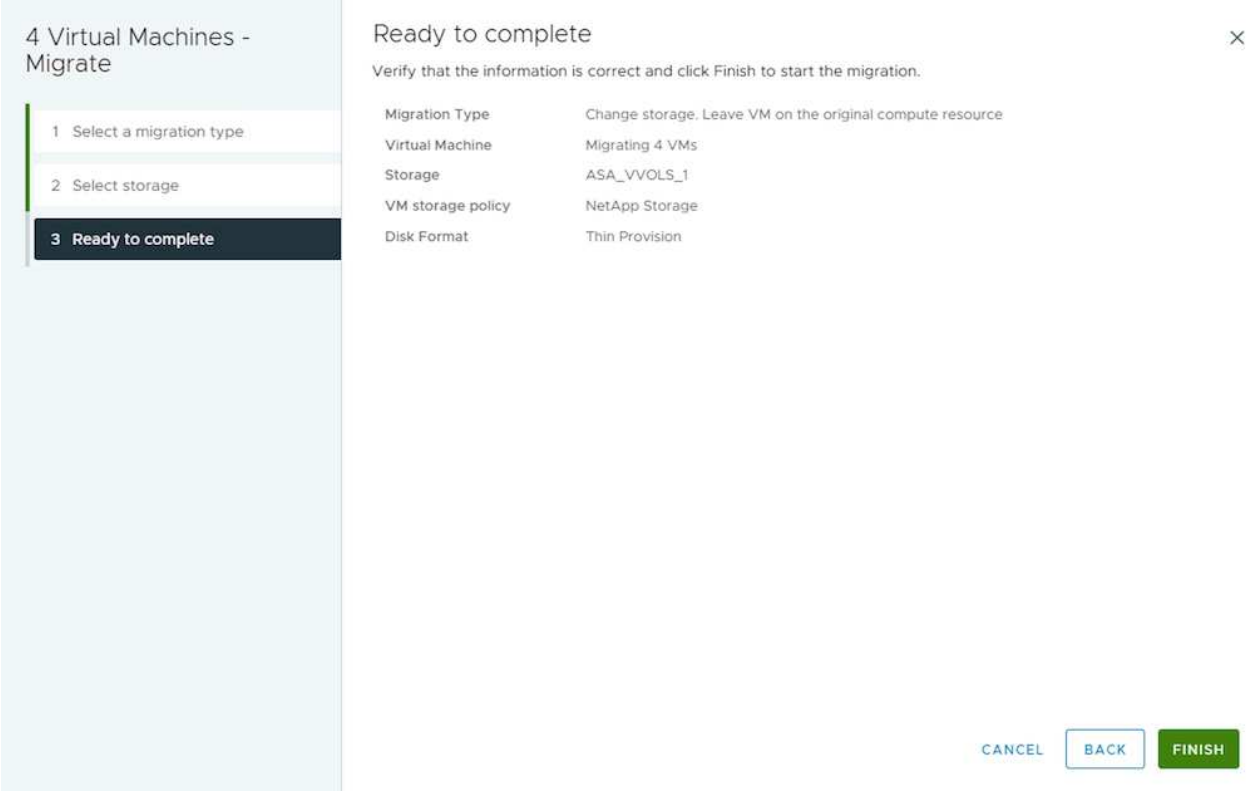
3. 저장소만 변경하는 옵션을 선택하고 다음을 클릭합니다.



4. 원하는 VM 스토리지 정책을 선택하고 호환되는 데이터 저장소를 선택하세요. 다음을 클릭하세요.



5. 검토하고 마침을 클릭하세요.



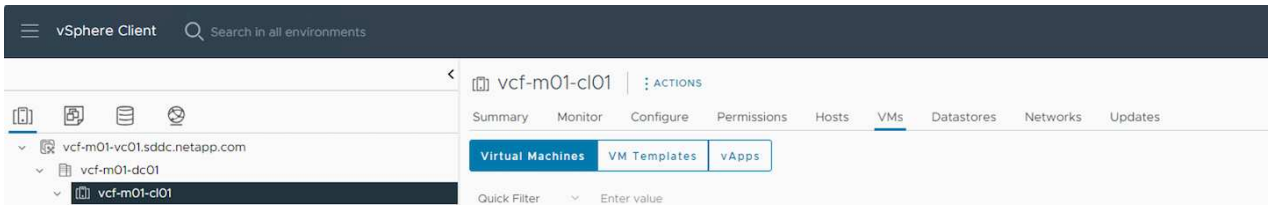
PowerCLI를 사용하여 VM을 마이그레이션하는 샘플 스크립트는 다음과 같습니다.

```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific datastore
$vm = Get-DataStore 'vSanDatastore' | Get-VM Har*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

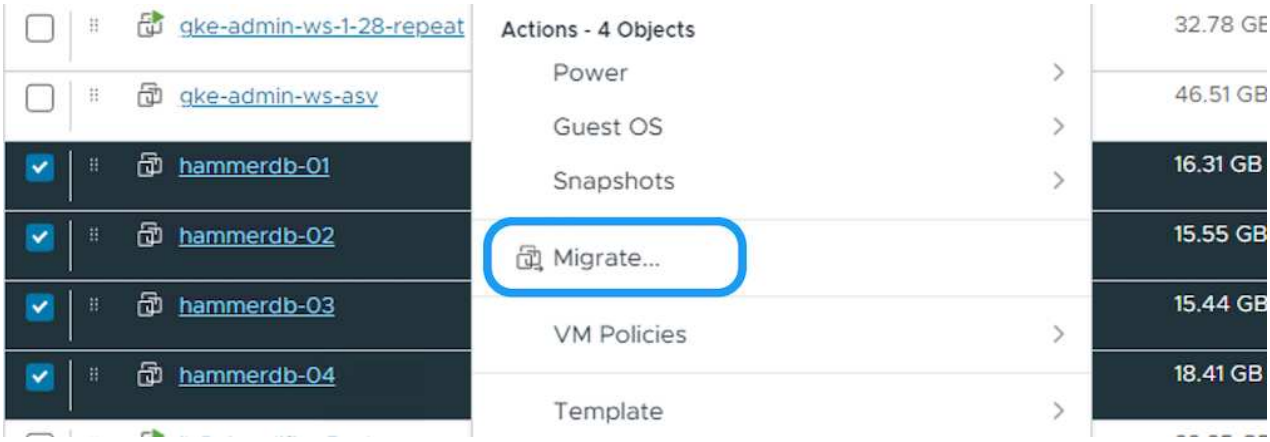
동일한 **vSphere** 클러스터의 **VM** 마이그레이션

UI를 사용하여 VM을 새 데이터 저장소로 마이그레이션하려면 아래 절차를 따르세요.

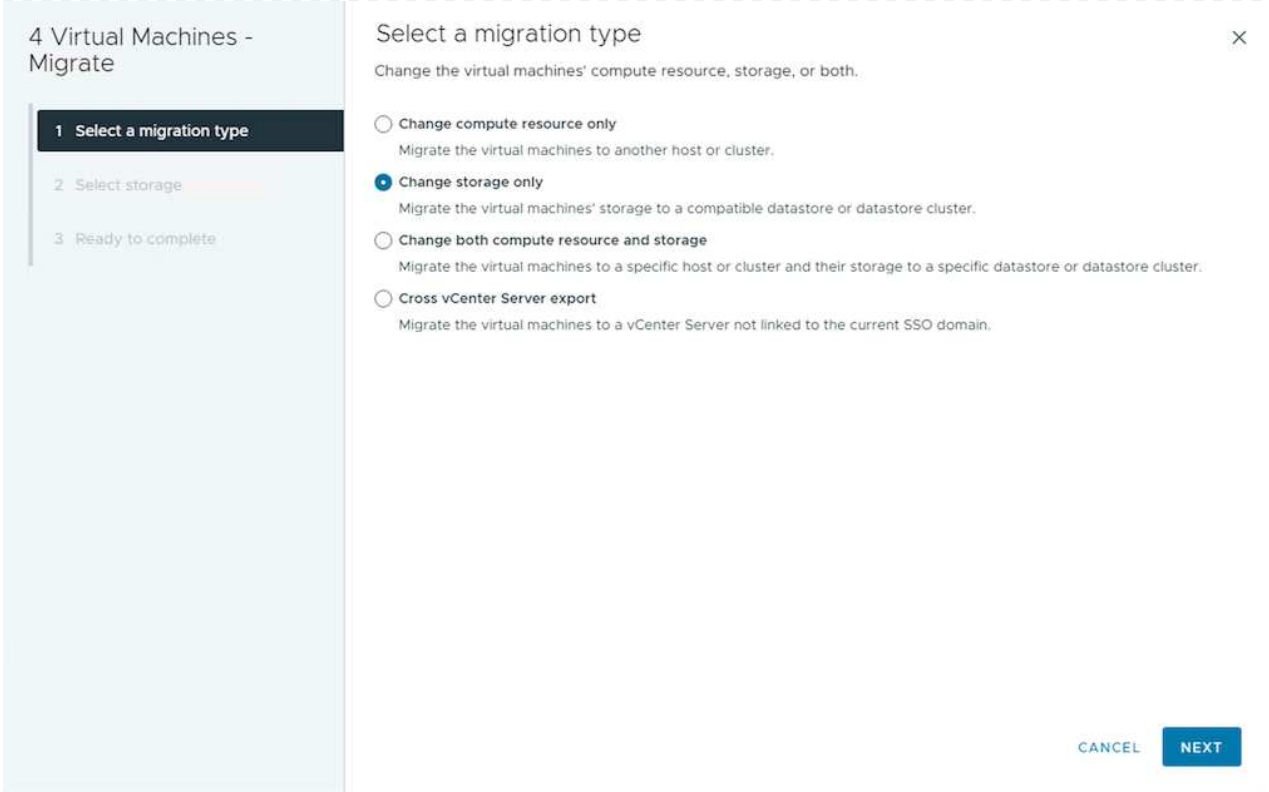
1. vSphere Web Client를 사용하여 호스트 및 클러스터 인벤토리에서 클러스터를 선택하고 VM 탭을 클릭합니다.



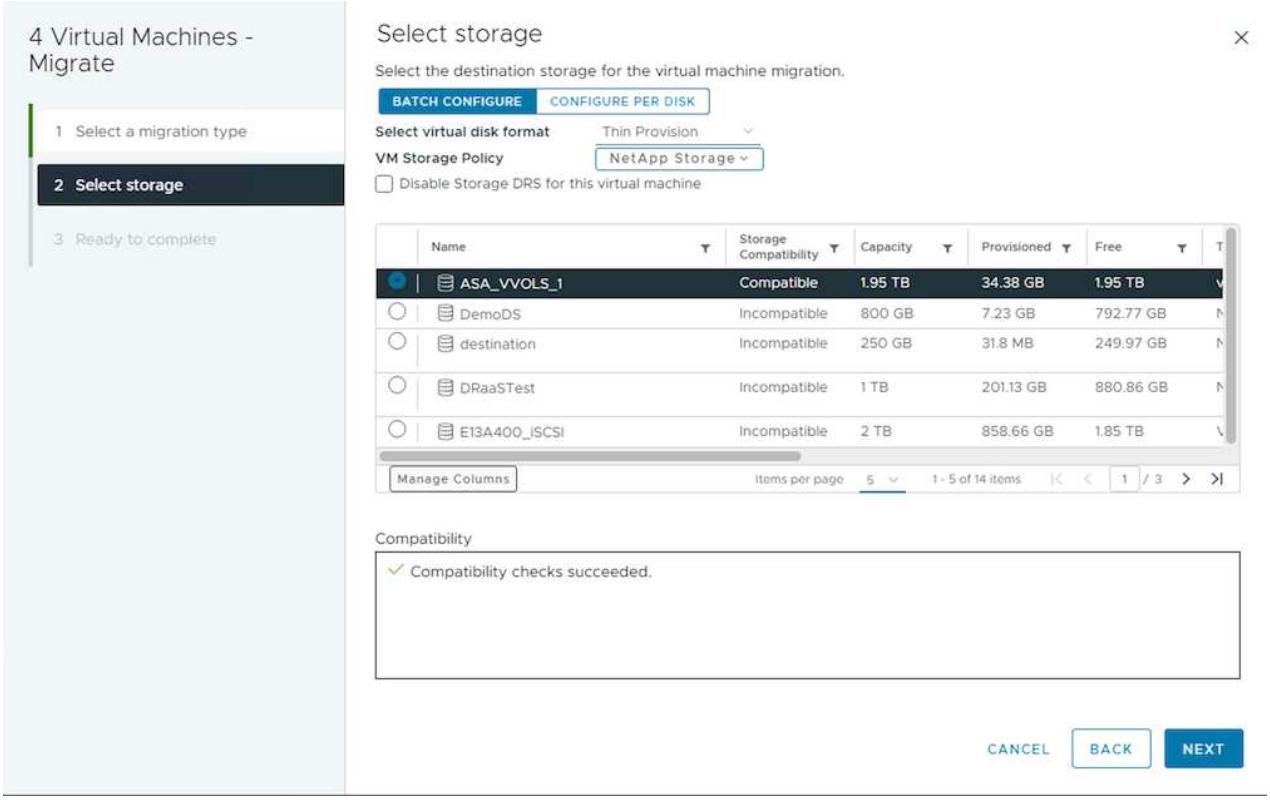
2. 마이그레이션이 필요한 VM을 선택하고 마우스 오른쪽 버튼을 클릭하여 마이그레이션 옵션을 선택합니다.



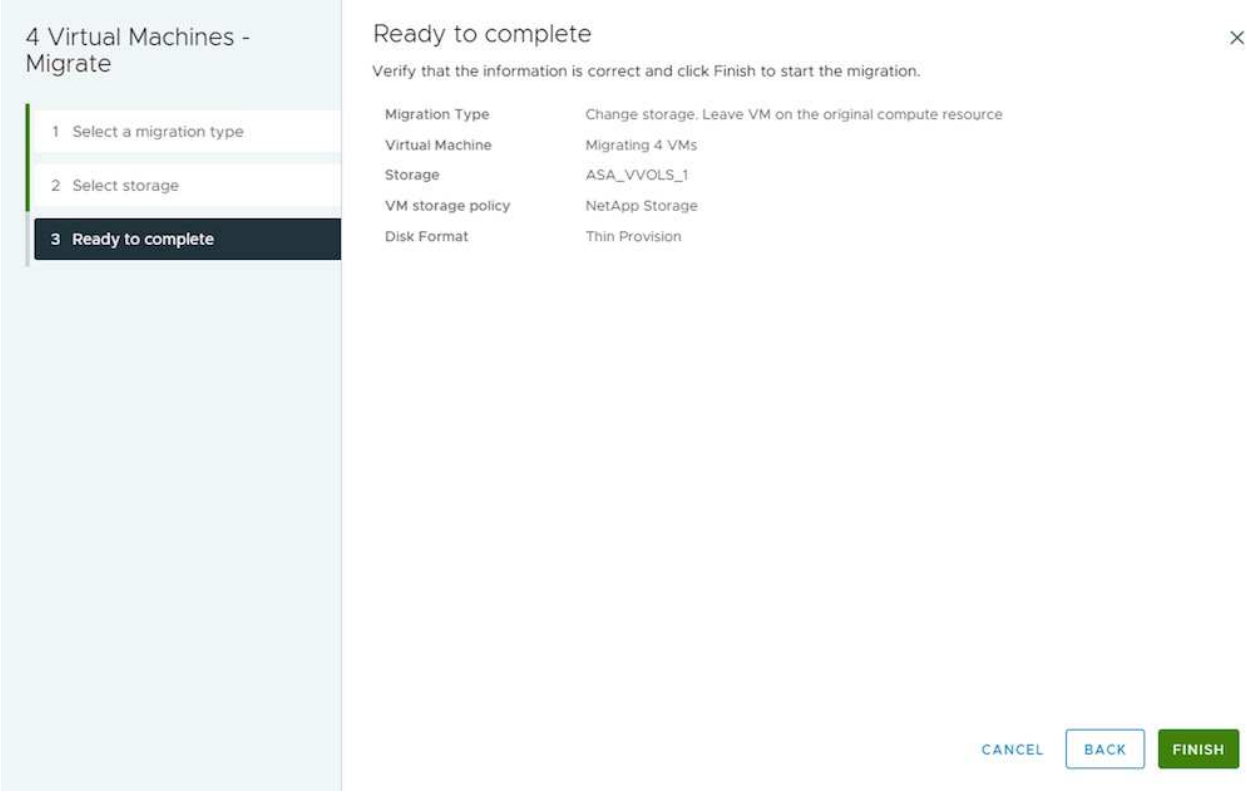
3. 저장소만 변경하는 옵션을 선택하고 다음을 클릭합니다.



4. 원하는 VM 스토리지 정책을 선택하고 호환되는 데이터 저장소를 선택하세요. 다음을 클릭하세요.



5. 검토하고 마침을 클릭하세요.



PowerCLI를 사용하여 VM을 마이그레이션하는 샘플 스크립트는 다음과 같습니다.

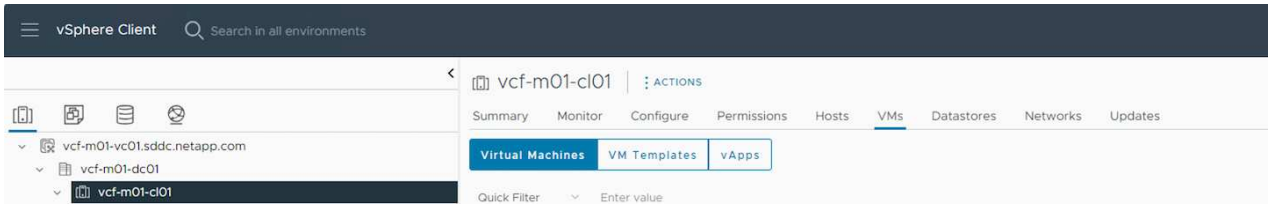
```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

데이터 저장소 클러스터가 완전 자동화된 스토리지 DRS(동적 리소스 스케줄링)와 함께 사용되고 두 데이터 저장소(소스 및 대상)가 동일한 유형(VMFS/NFS/vVol)인 경우, 두 데이터 저장소를 동일한 스토리지 클러스터에 유지하고 소스에서 유지 관리 모드를 활성화하여 소스 데이터 저장소에서 VM을 마이그레이션합니다. 경험은 컴퓨팅 호스트가 유지 관리를 위해 처리되는 방식과 유사합니다.

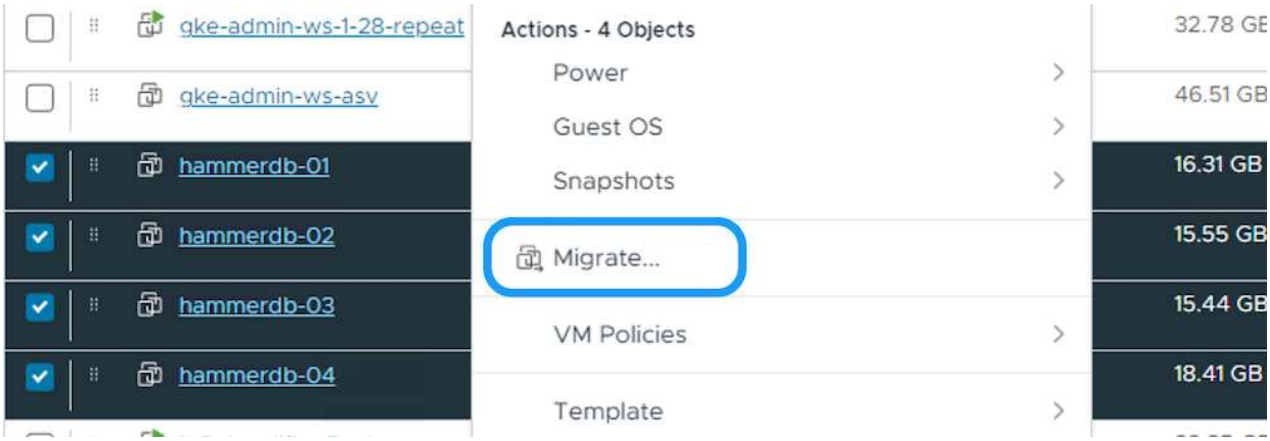
> 나타내다 "CPU 호환성 및 vSphere Enhanced vMotion 호환성" 소스 호스트와 대상 호스트가 서로 다른 CPU 제품군이나 모델인 경우.

UI를 사용하여 VM을 새 데이터 저장소로 마이그레이션하려면 아래 절차를 따르세요.

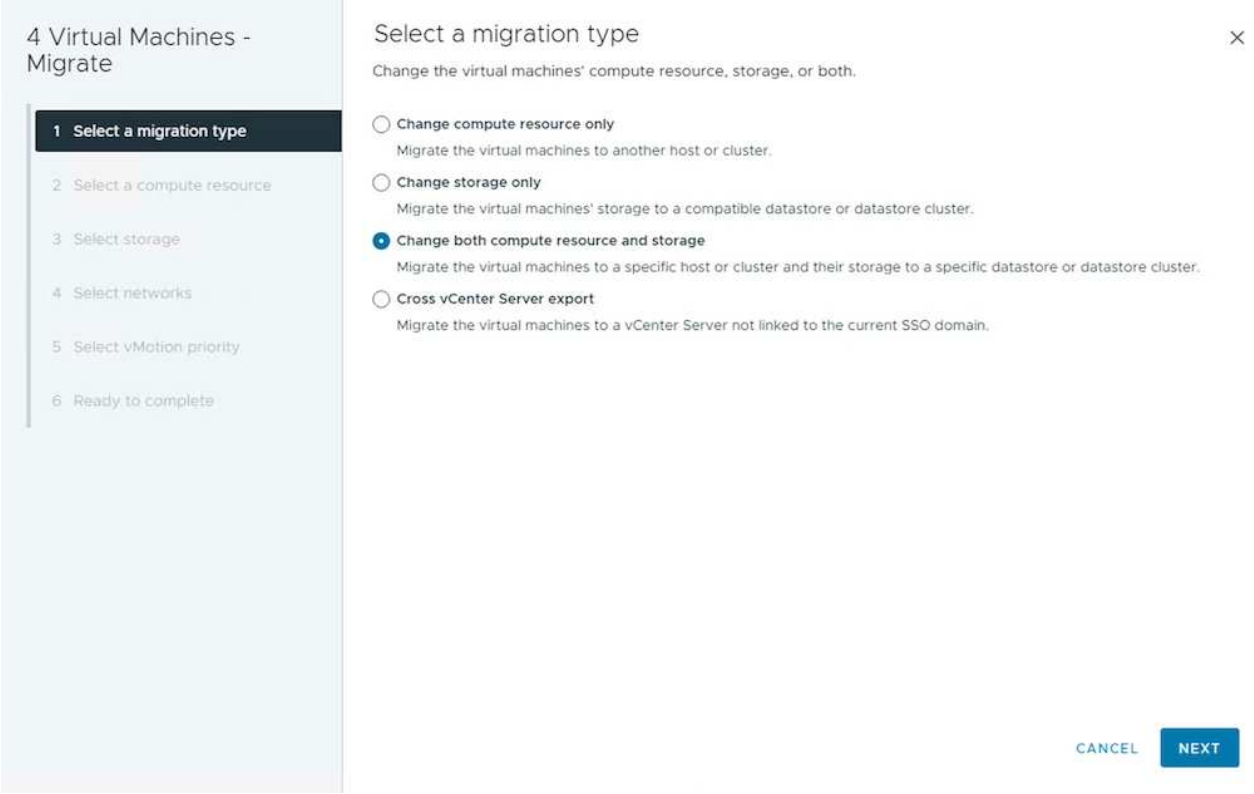
1. vSphere Web Client를 사용하여 호스트 및 클러스터 인벤토리에서 클러스터를 선택하고 VM 탭을 클릭합니다.



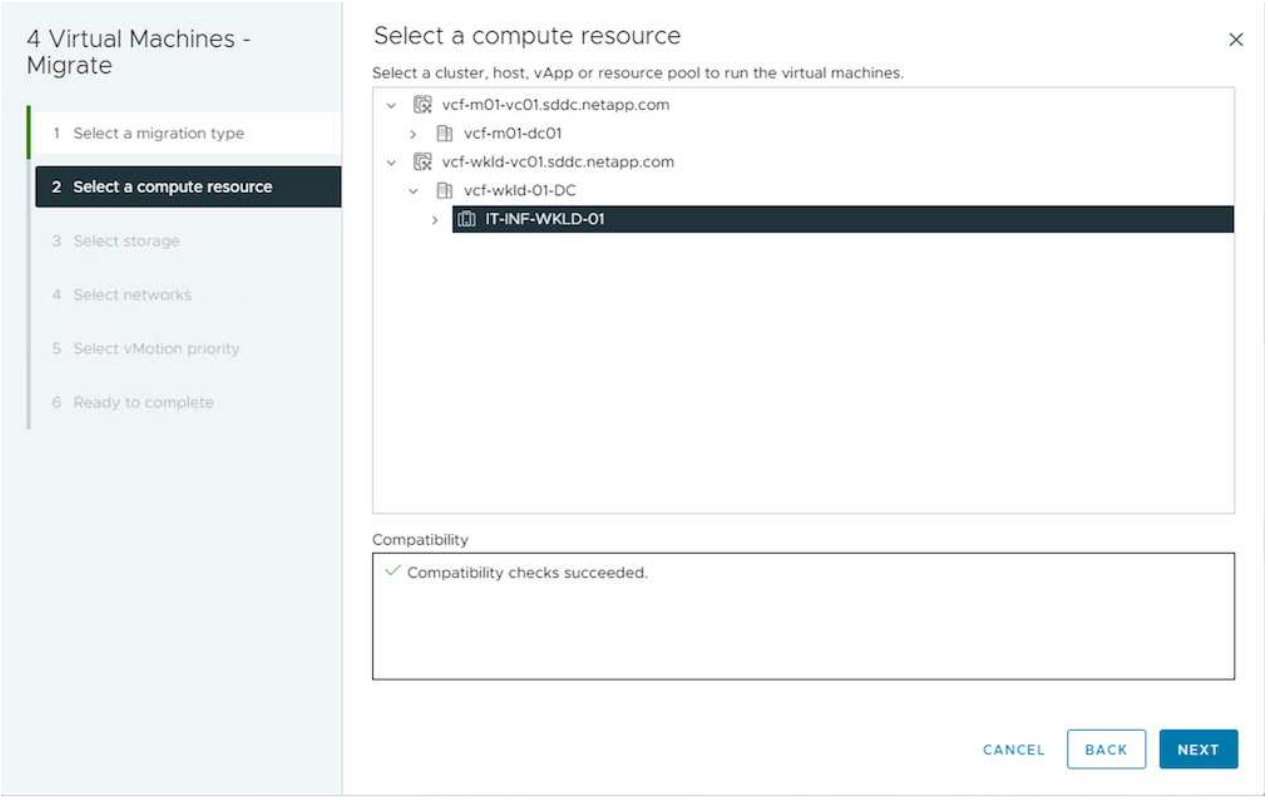
2. 마이그레이션이 필요한 VM을 선택하고 마우스 오른쪽 버튼을 클릭하여 마이그레이션 옵션을 선택합니다.



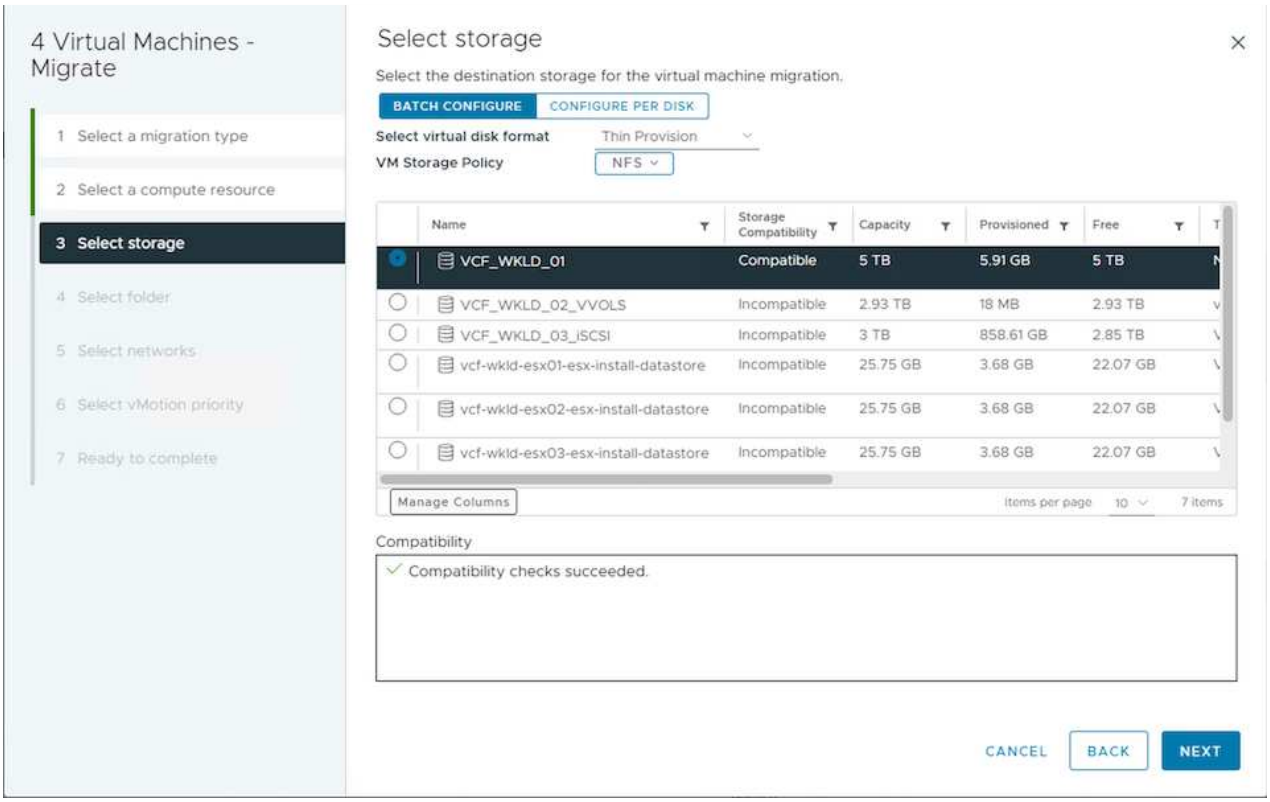
3. 컴퓨팅 리소스 및 스토리지를 변경하는 옵션을 선택하고 다음을 클릭합니다.



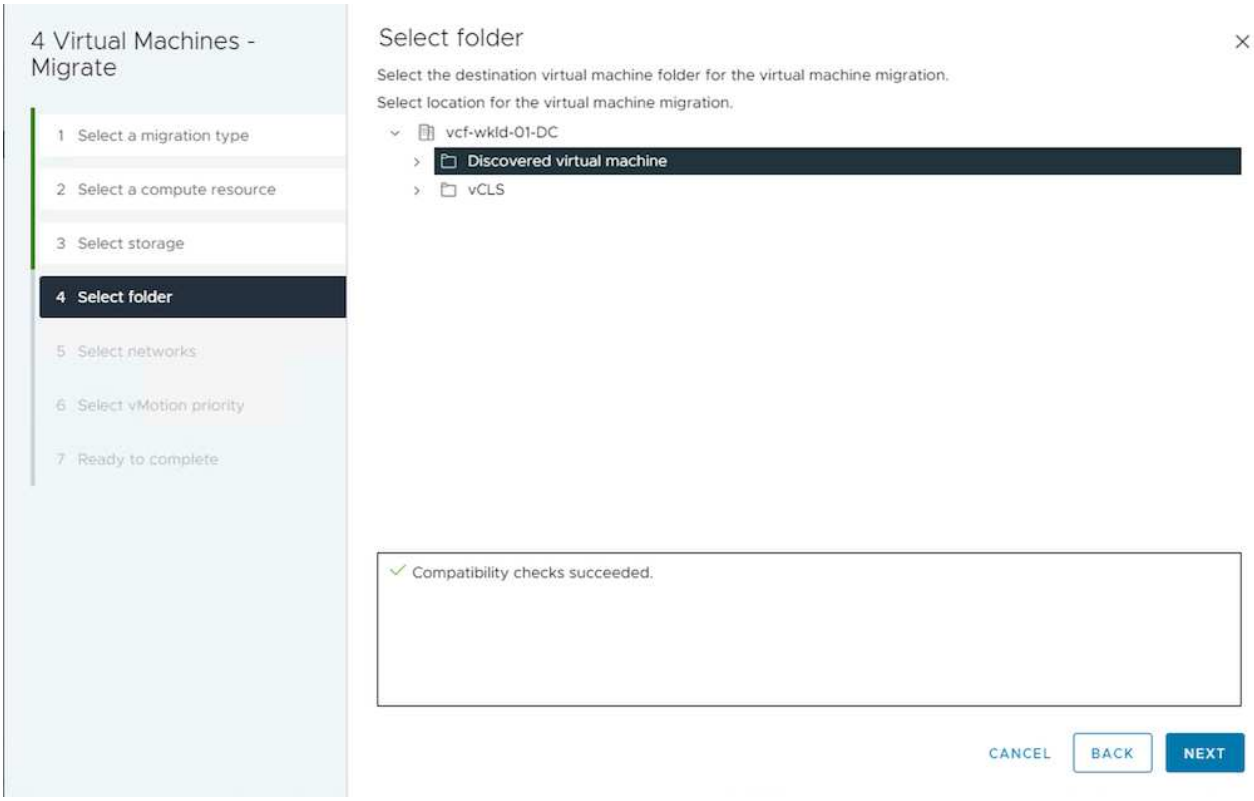
4. 탐색하여 마이그레이션할 올바른 클러스터를 선택하세요.



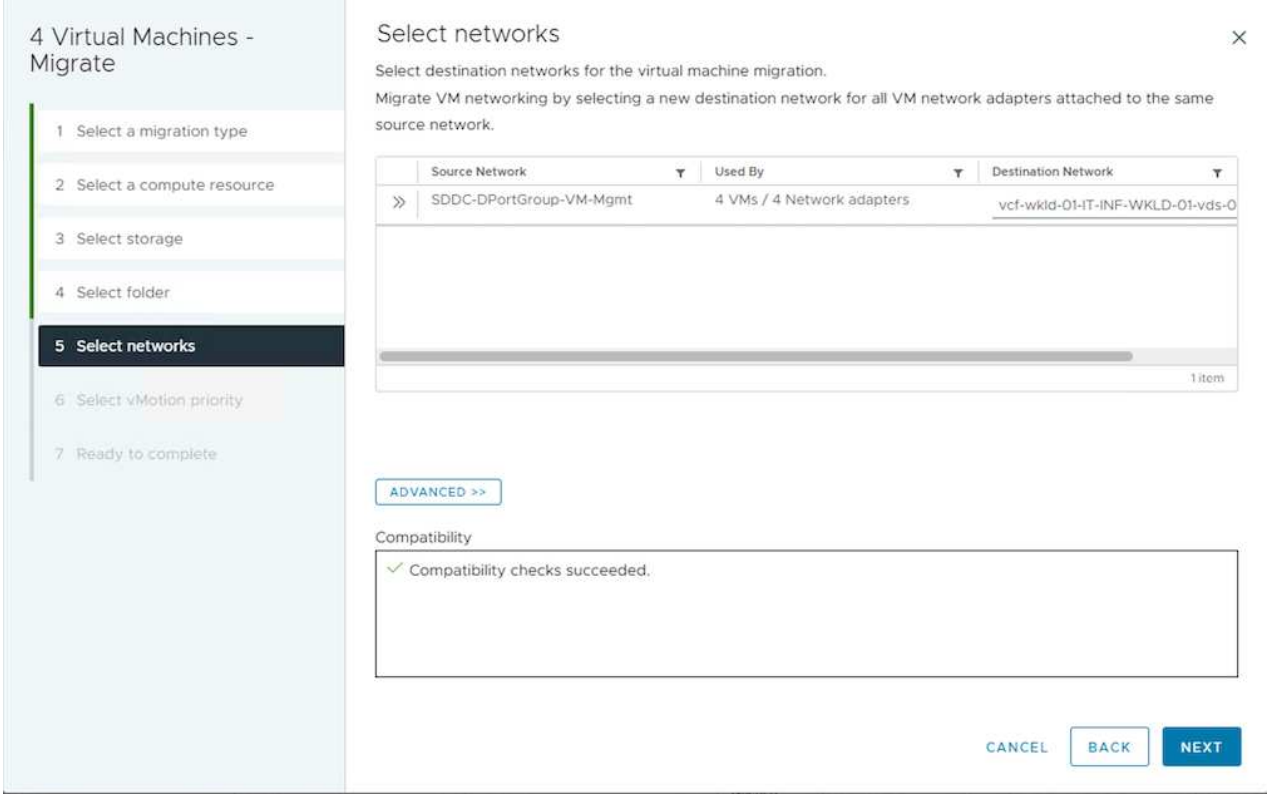
5. 원하는 VM 스토리지 정책을 선택하고 호환되는 데이터 저장소를 선택하세요. 다음을 클릭하세요.



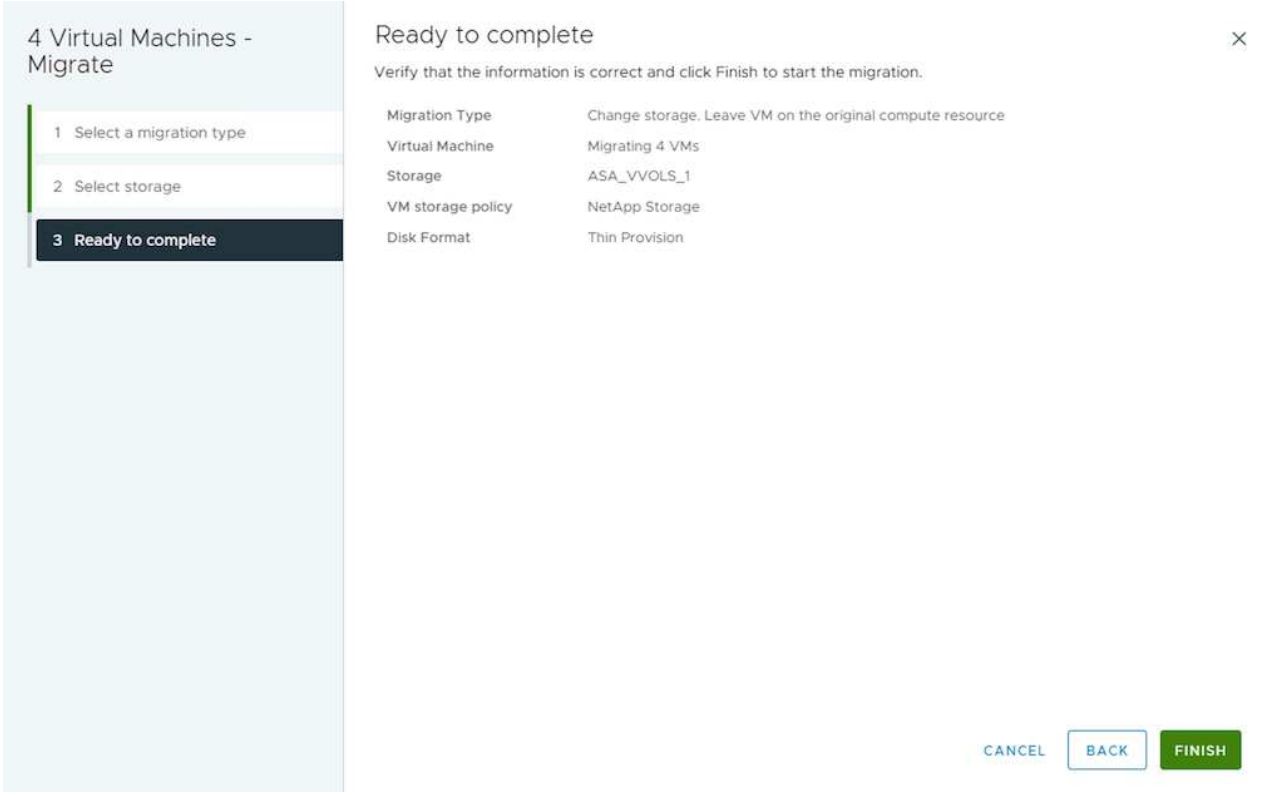
6. 대상 VM을 배치할 VM 폴더를 선택합니다.



7. 대상 포트 그룹을 선택하세요.



8. 검토하고 마침을 클릭하세요.



PowerCLI를 사용하여 VM을 마이그레이션하는 샘플 스크립트는 다음과 같습니다.

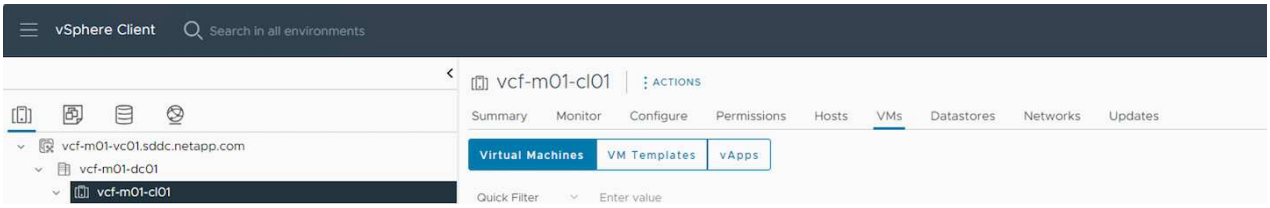
```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to another cluster and Datastore specified by Policy
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy)

#When Portgroup is specific to each cluster, replace the above command
with
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy) -PortGroup
(Get-VirtualPortGroup 'VLAN 101')

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

동일한 **SSO** 도메인의 **vCenter** 서버 간 **VM** 마이그레이션

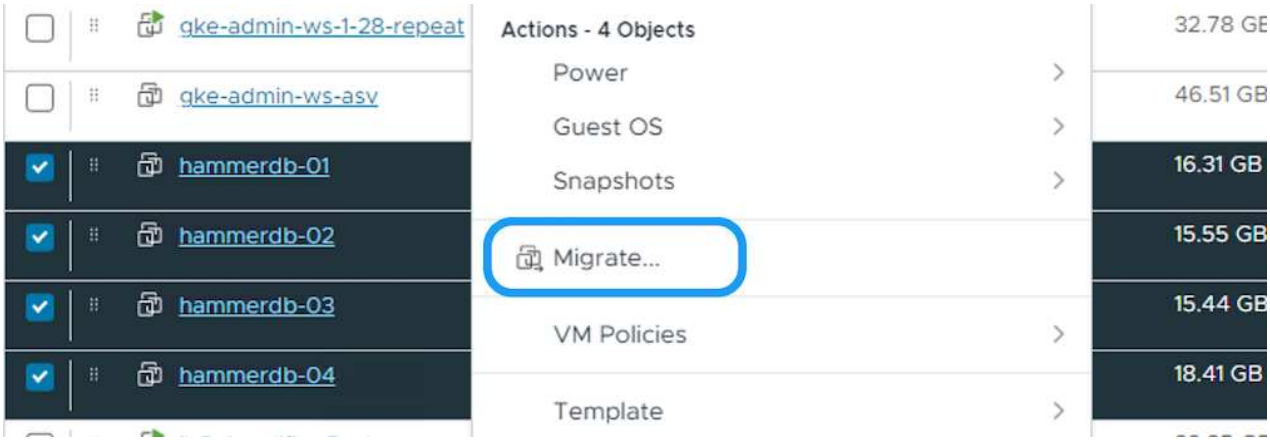
동일한 vSphere Client UI에 나열된 새 vCenter 서버로 VM을 마이그레이션하려면 아래 절차를 따르세요.

> 소스 및 대상 vCenter 버전 등과 같은 추가 요구 사항을 확인하려면 다음을 확인하세요. "vCenter 서버 인스턴스 간 vMotion 요구 사항에 대한 vSphere 설명서"

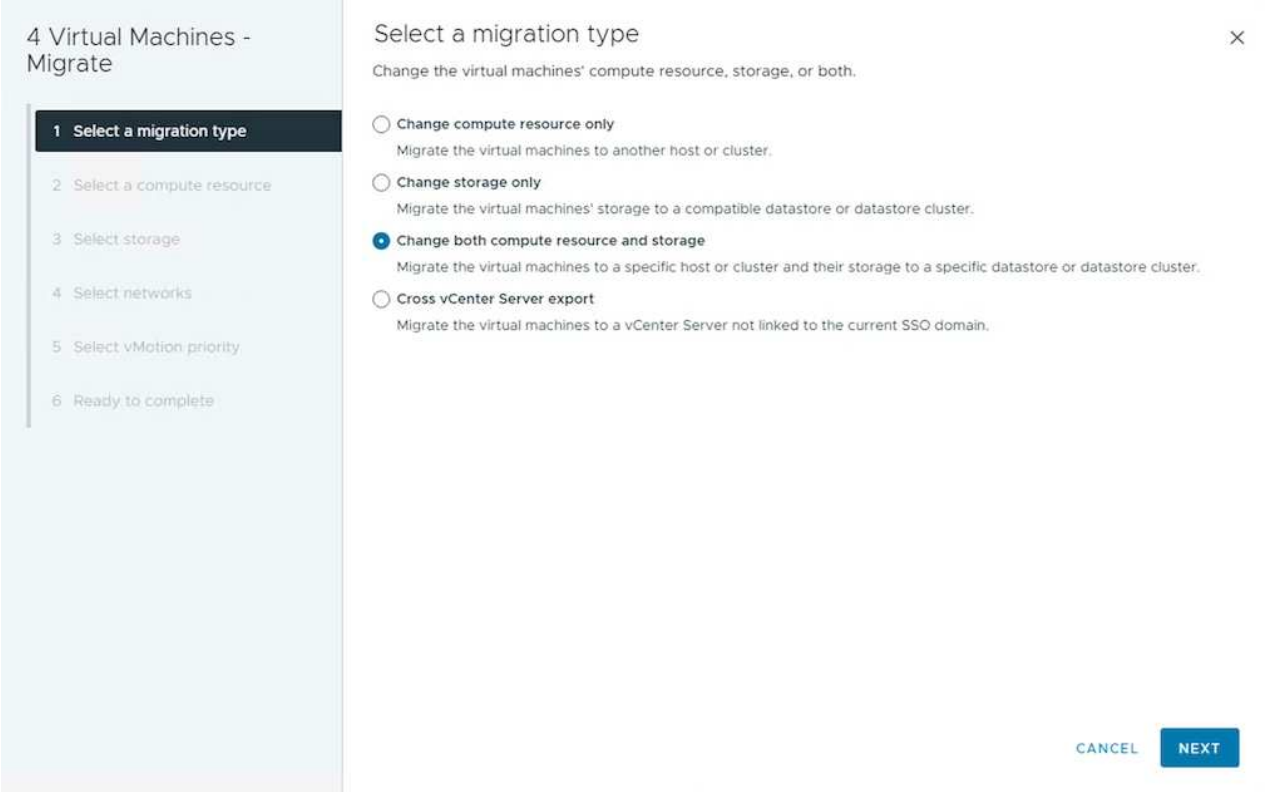
1. vSphere Web Client를 사용하여 호스트 및 클러스터 인벤토리에서 클러스터를 선택하고 VM 탭을 클릭합니다.



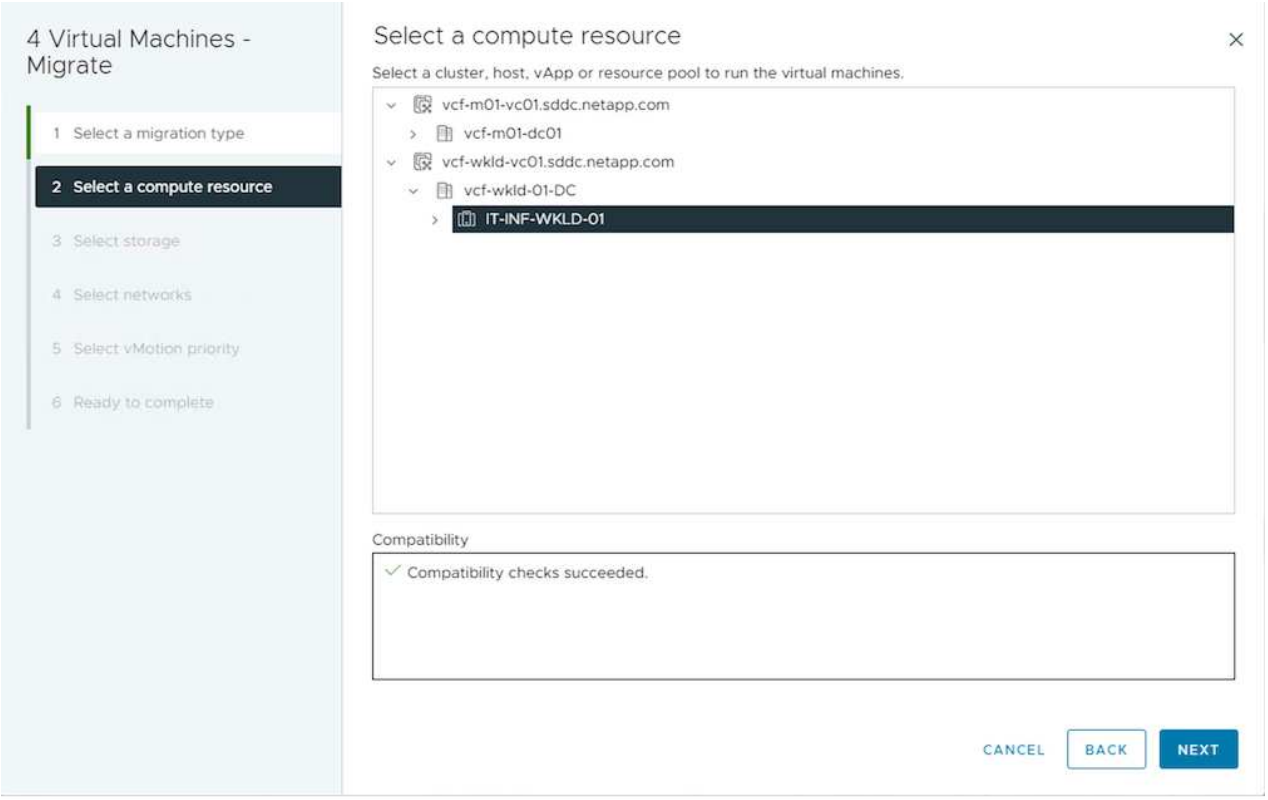
2. 마이그레이션이 필요한 VM을 선택하고 마우스 오른쪽 버튼을 클릭하여 마이그레이션 옵션을 선택합니다.



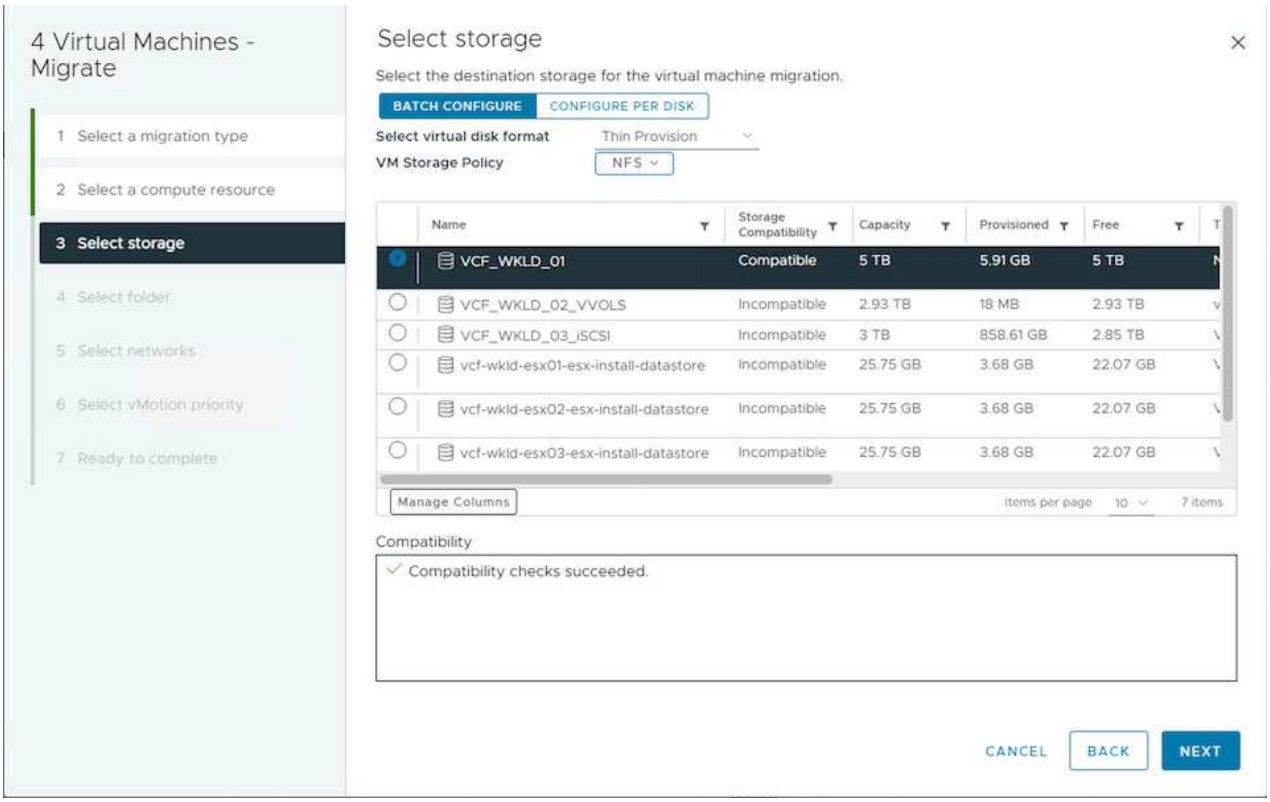
3. 컴퓨팅 리소스 및 스토리지를 변경하는 옵션을 선택하고 다음을 클릭합니다.



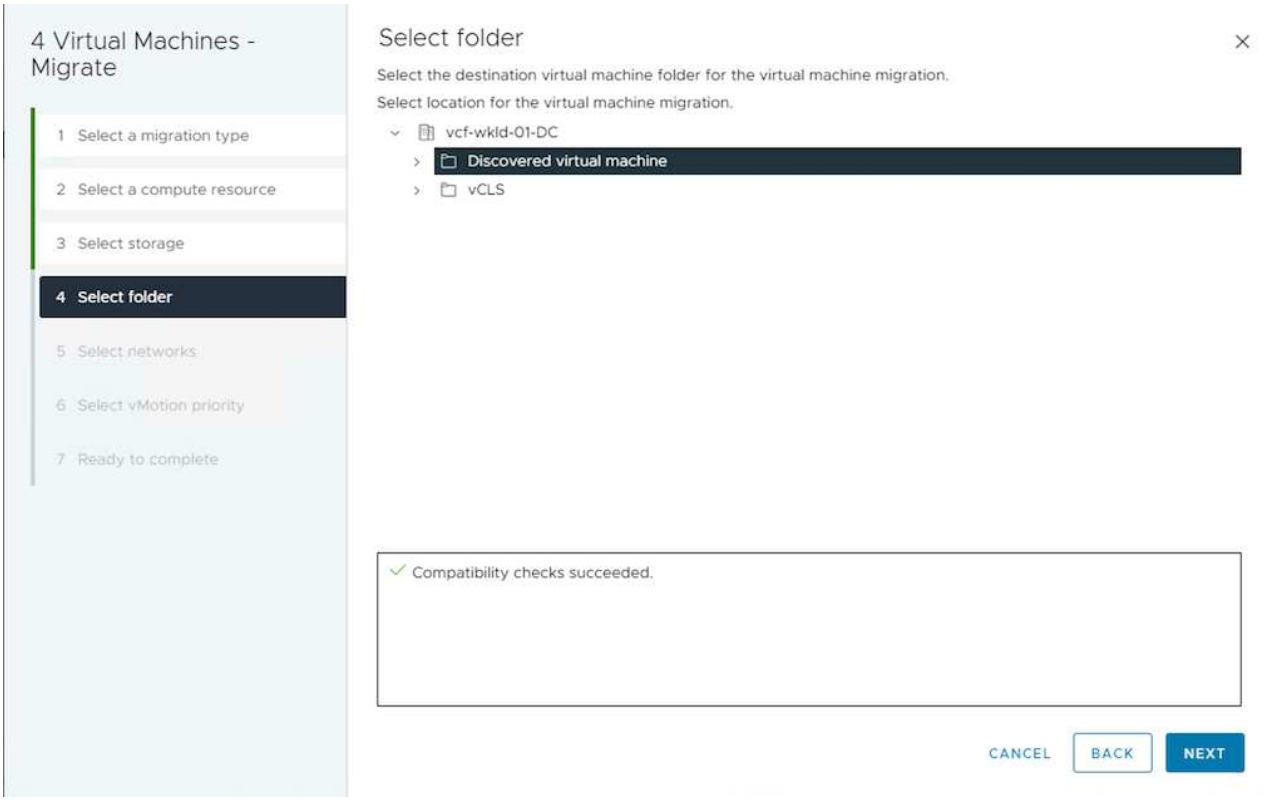
4. 대상 vCenter 서버에서 대상 클러스터를 선택합니다.



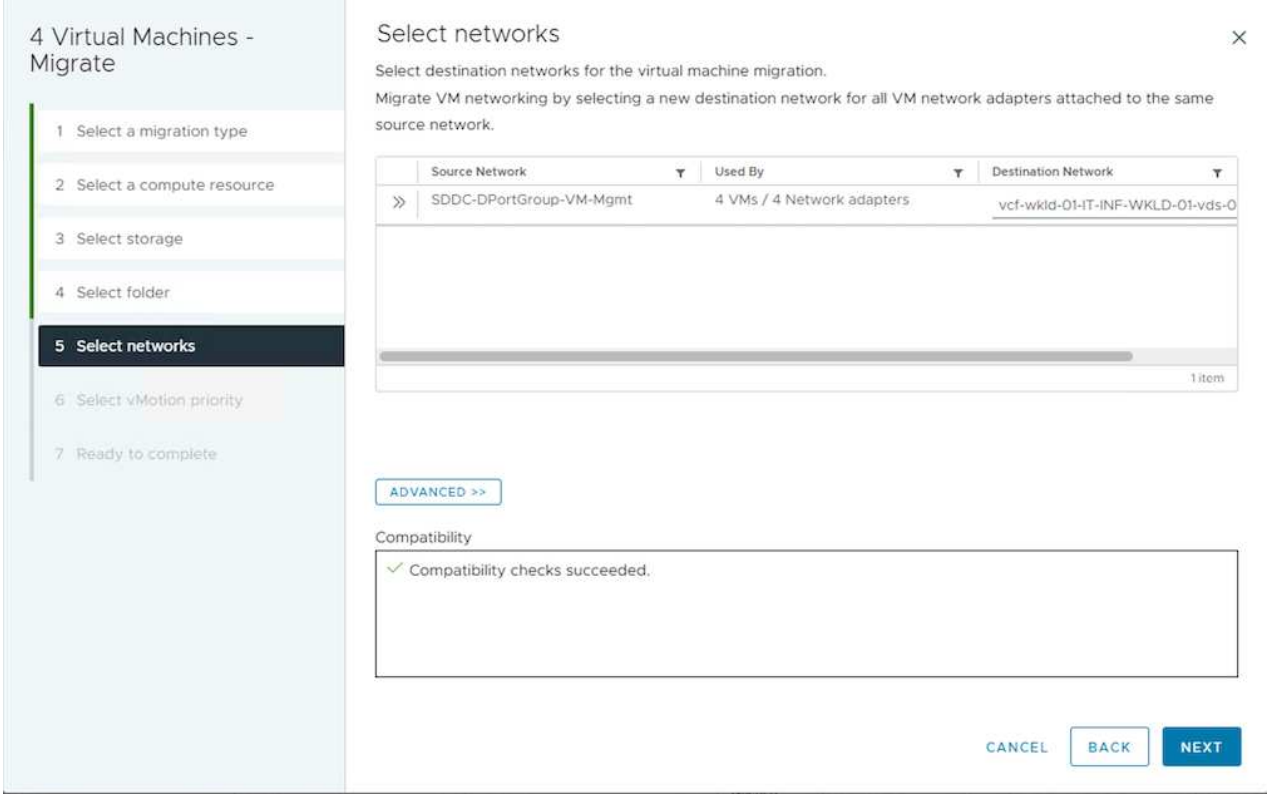
5. 원하는 VM 스토리지 정책을 선택하고 호환되는 데이터 저장소를 선택하세요. 다음을 클릭하세요.



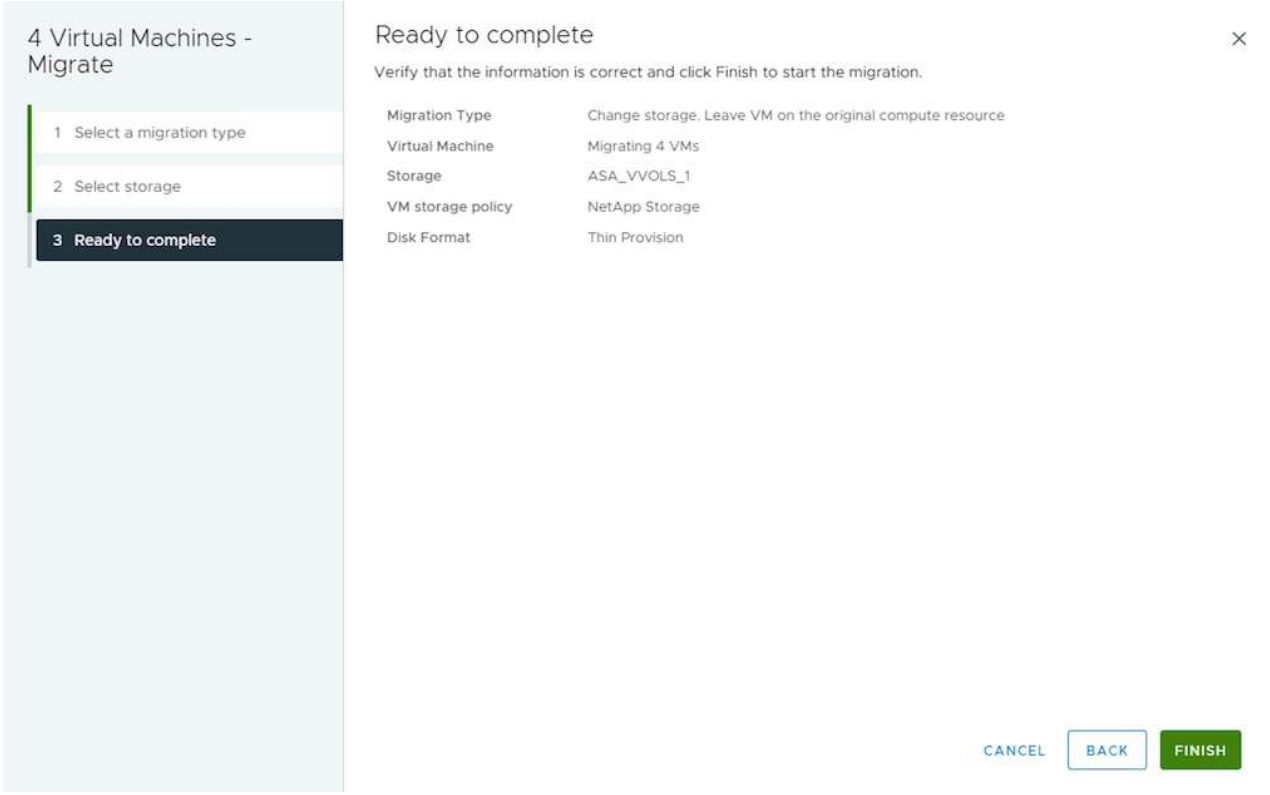
6. 대상 VM을 배치할 VM 폴더를 선택합니다.



7. 대상 포트 그룹을 선택하세요.



8. 마이그레이션 옵션을 검토하고 마침을 클릭합니다.



PowerCLI를 사용하여 VM을 마이그레이션하는 샘플 스크립트는 다음과 같습니다.

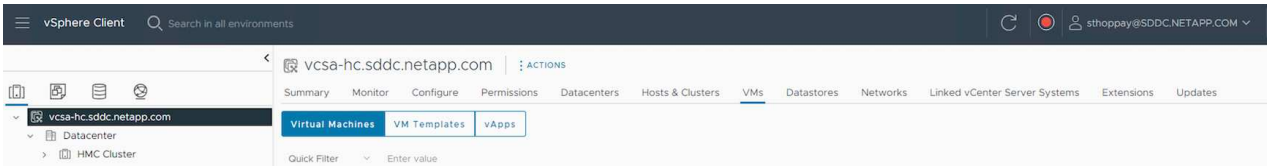
```
#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01'  -server $sourcevc| Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration
```

다양한 **SSO** 도메인의 **vCenter** 서버 간 **VM** 마이그레이션

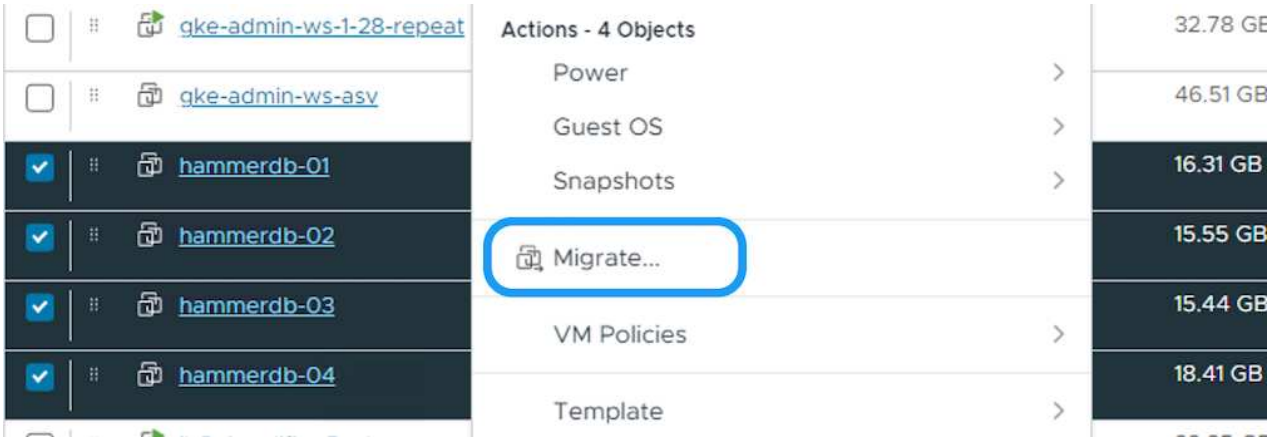
> 이 시나리오에서는 vCenter 서버 간에 통신이 존재한다고 가정합니다. 그렇지 않으면 아래 나열된 데이터 센터 위치 시나리오를 확인하세요. 필수 조건을 확인하세요 "Advanced Cross vCenter vMotion에 대한 vSphere 설명서"

UI를 사용하여 VM을 다른 vCenter 서버로 마이그레이션하려면 아래 절차를 따르세요.

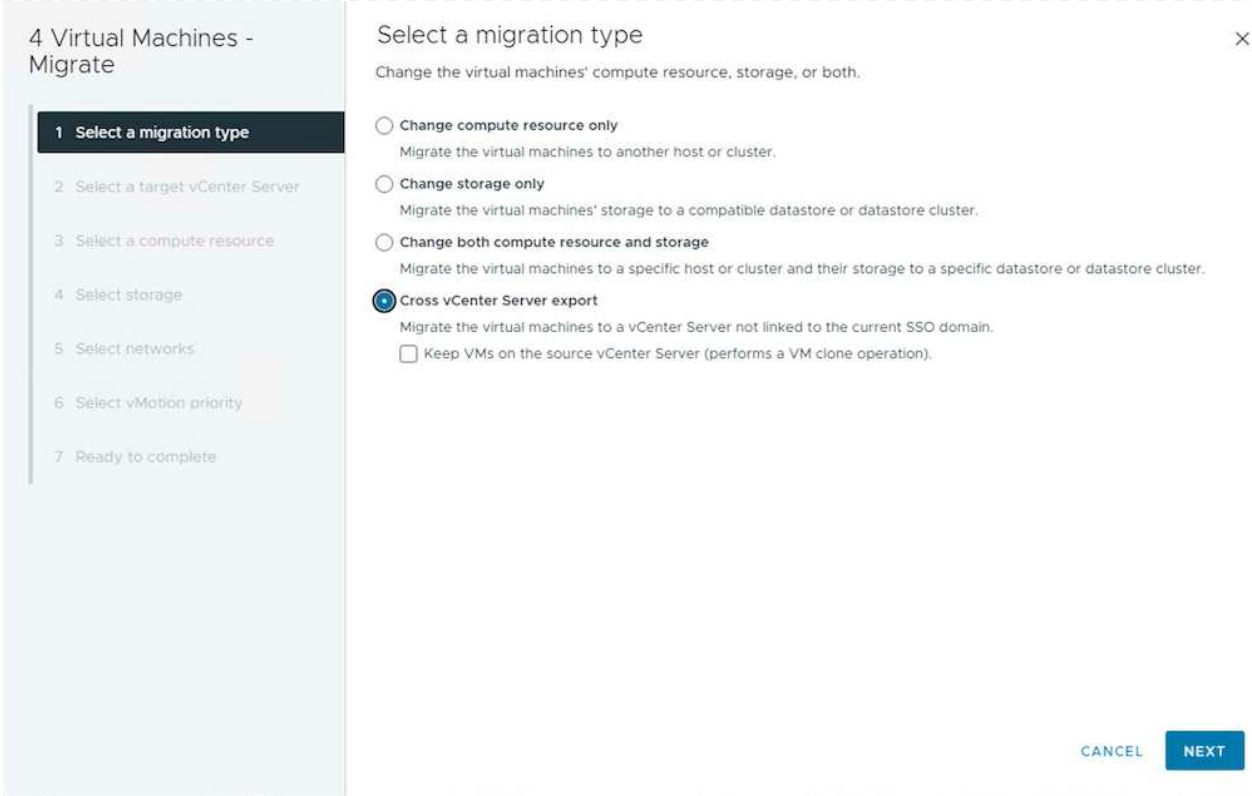
1. vSphere Web Client를 사용하여 소스 vCenter 서버를 선택하고 VM 탭을 클릭합니다.



2. 마이그레이션이 필요한 VM을 선택하고 마우스 오른쪽 버튼을 클릭하여 마이그레이션 옵션을 선택합니다.

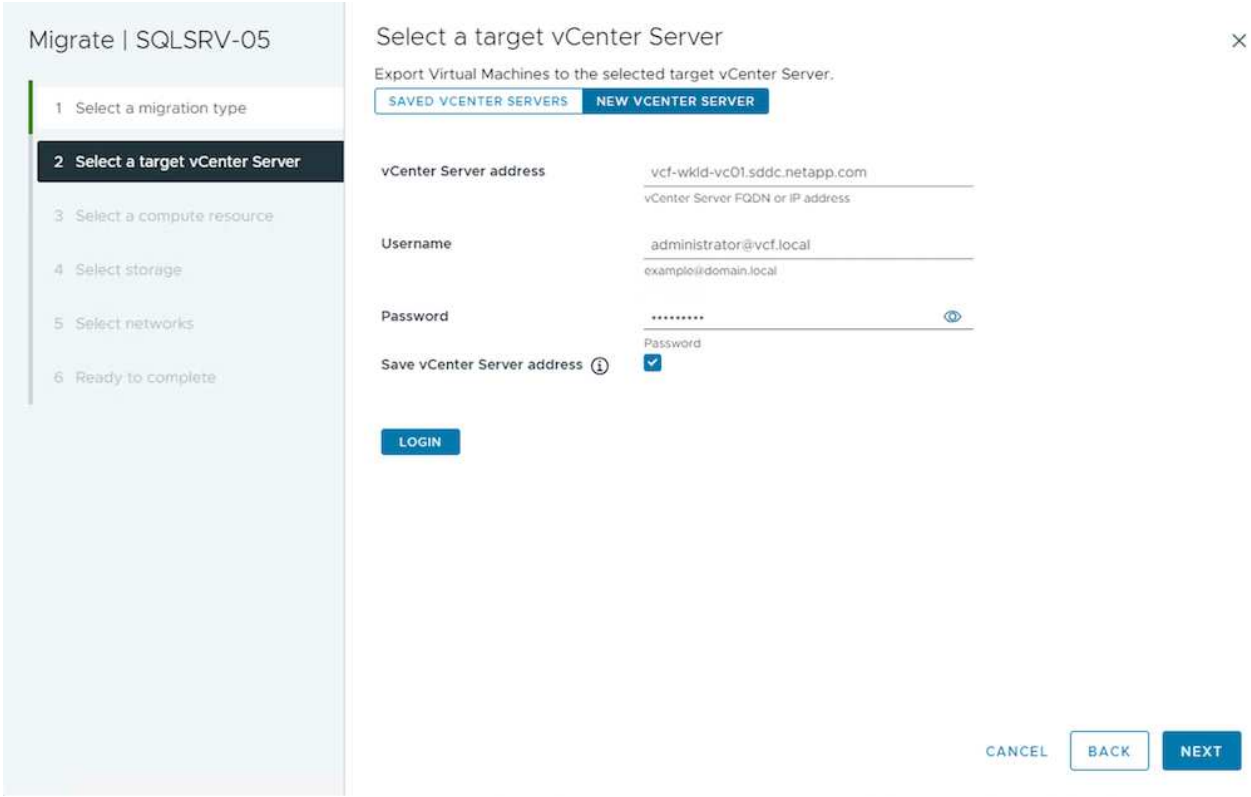


3. Cross vCenter Server 내보내기 옵션을 선택하고 다음을 클릭합니다.

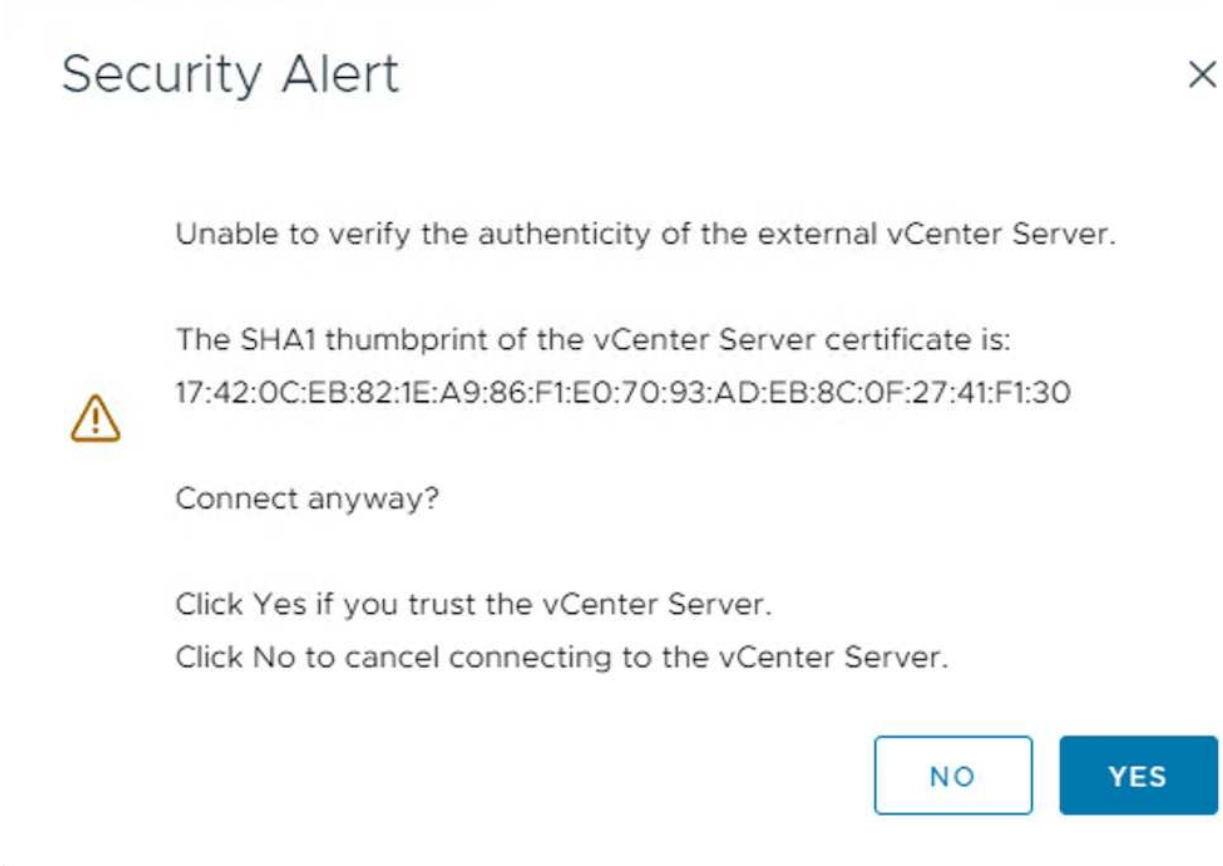


VM은 대상 vCenter 서버에서 가져올 수도 있습니다. 해당 절차에 대해 다음을 확인하세요. "고급 Cross vCenter vMotion을 사용하여 가상 머신 가져오기 또는 복제"

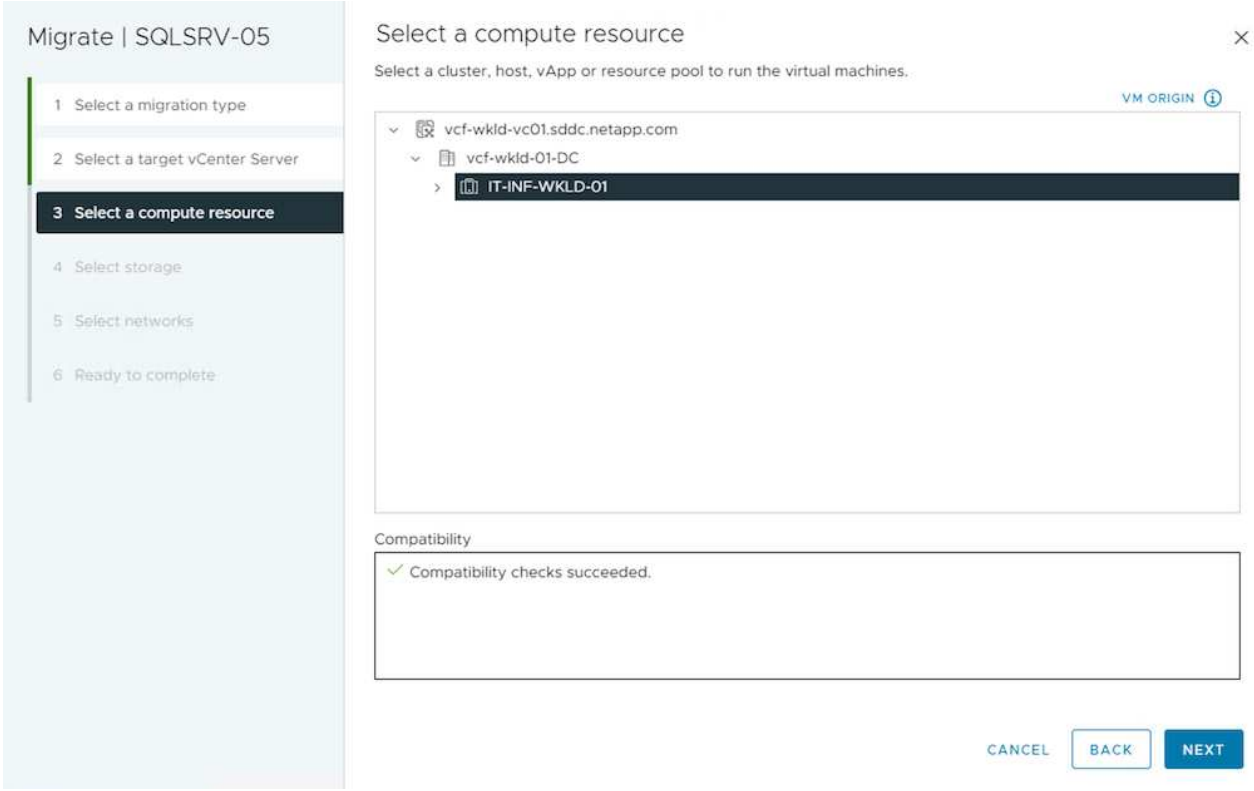
4. vCenter 자격 증명 세부 정보를 제공하고 로그인을 클릭합니다.



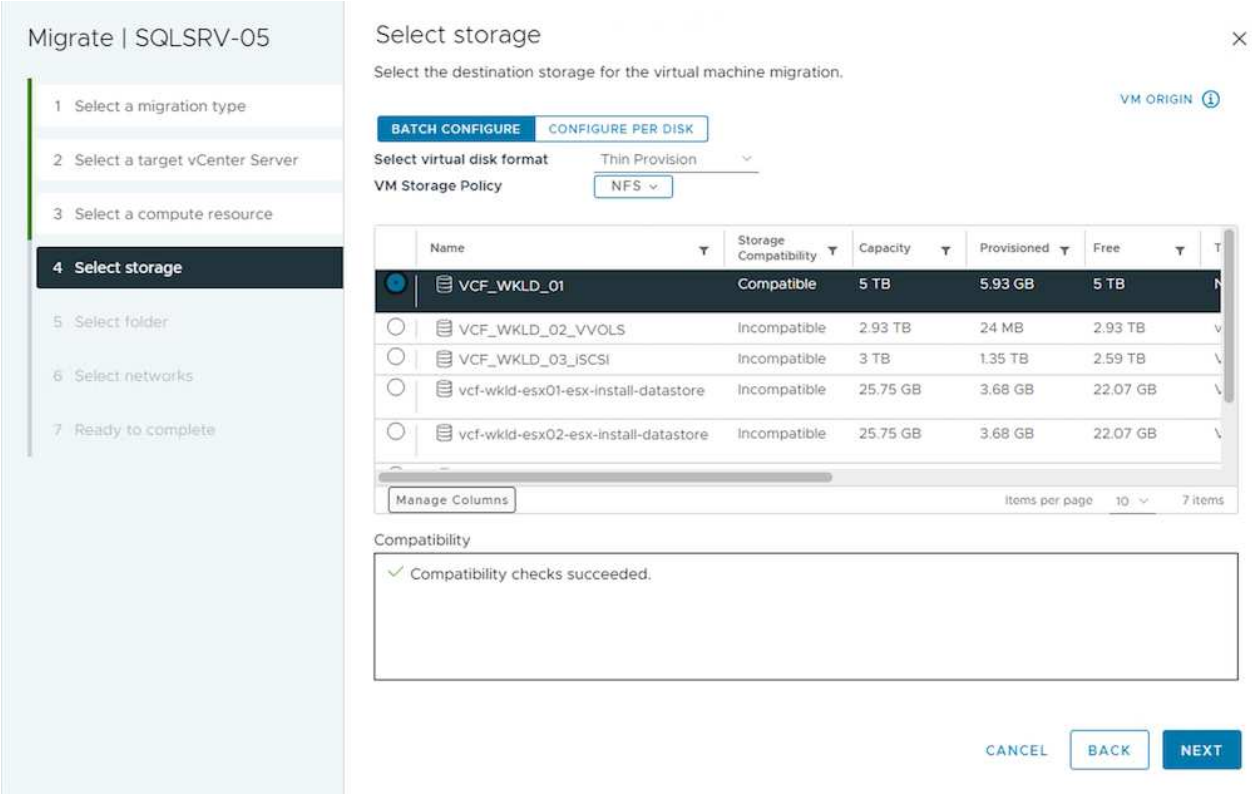
5. vCenter Server의 SSL 인증서 지문 확인 및 수락



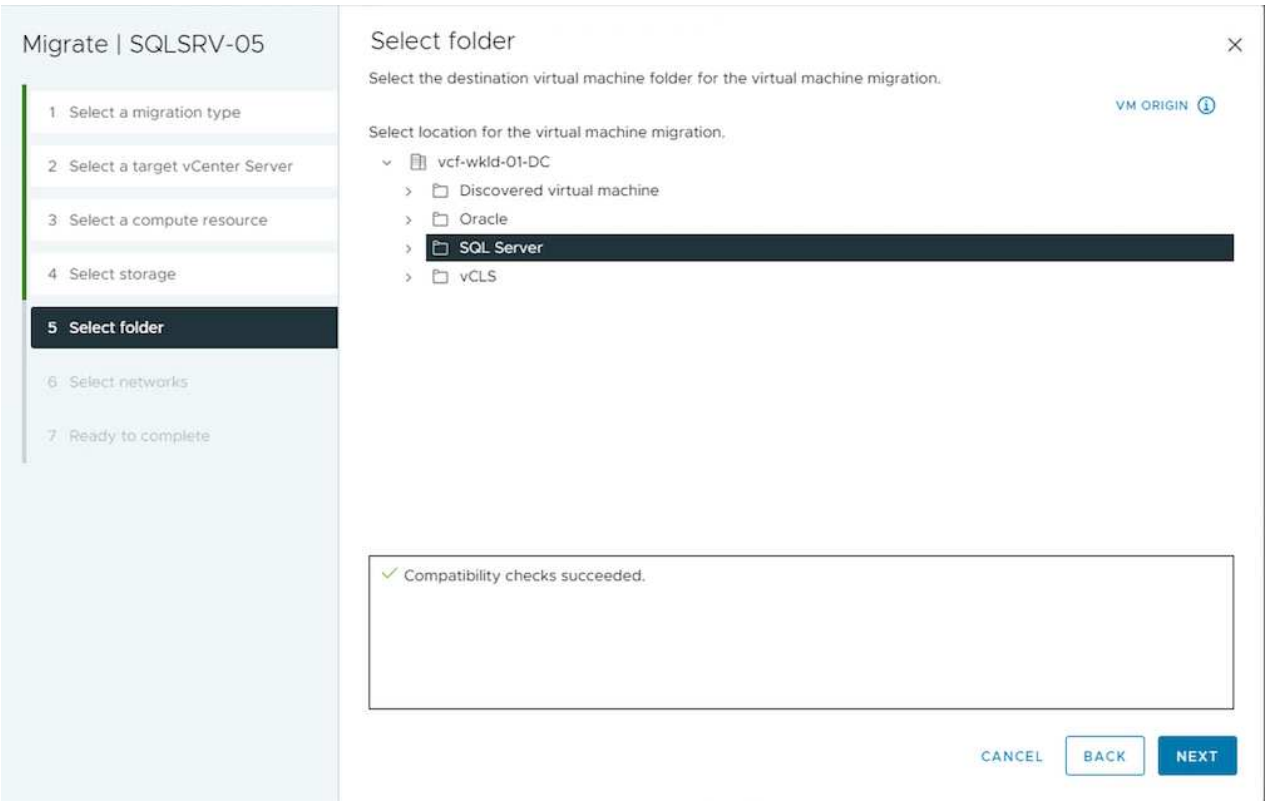
6. 대상 vCenter를 확장하고 대상 컴퓨팅 클러스터를 선택합니다.



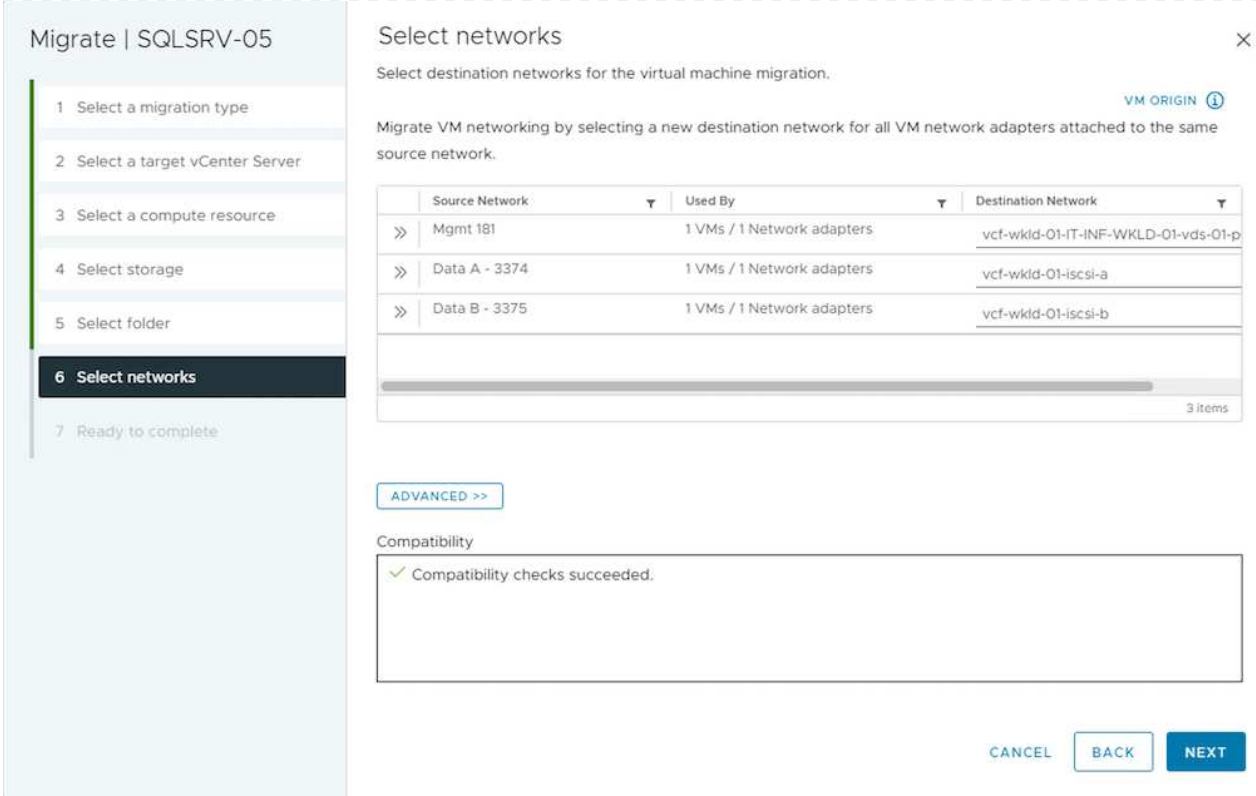
7. VM 스토리지 정책에 따라 대상 데이터 저장소를 선택합니다.



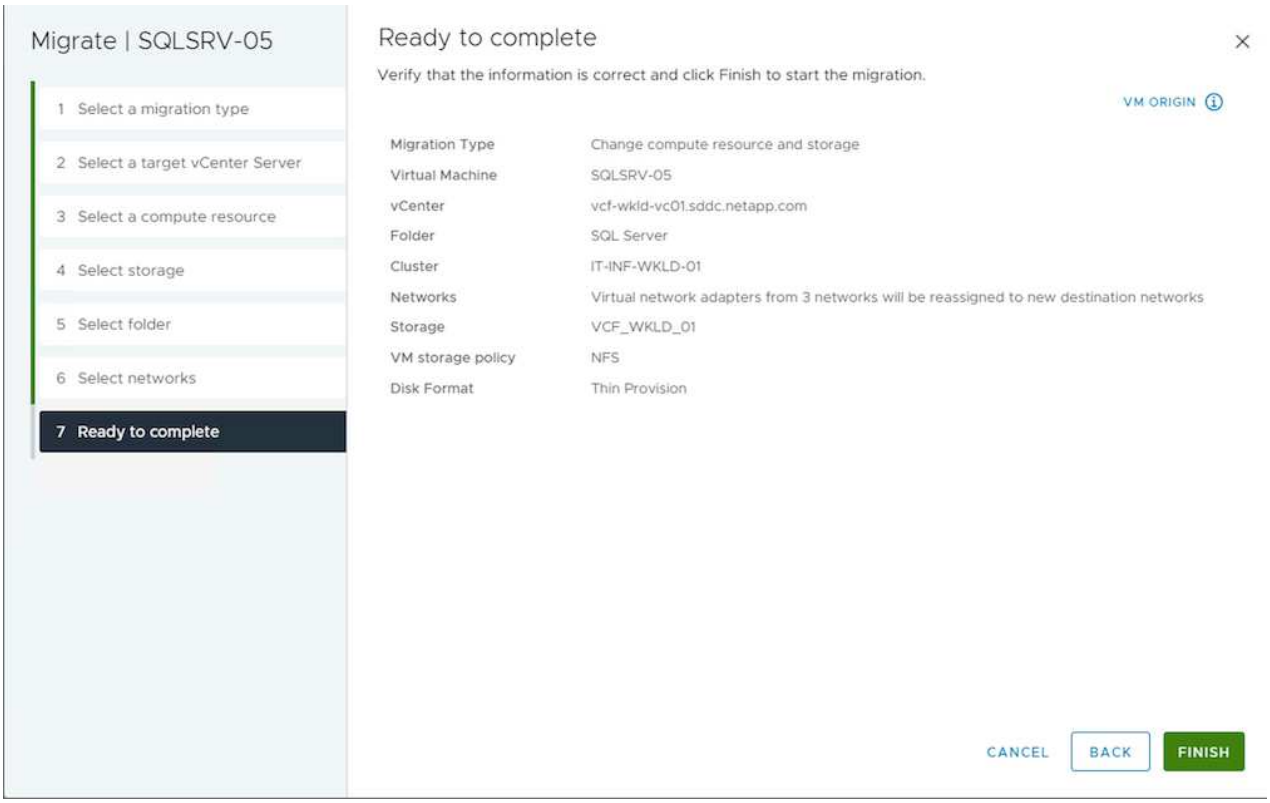
8. 대상 VM 폴더를 선택하세요.



9. 각 네트워크 인터페이스 카드 매핑에 대한 VM 포트 그룹을 선택합니다.



10. 검토 후 마침을 클릭하여 vCenter 서버에서 vMotion을 시작합니다.



PowerCLI를 사용하여 VM을 마이그레이션하는 샘플 스크립트는 다음과 같습니다.

```
#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'Source Cluster'  -server $sourcevc| Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration
```

데이터 센터 위치 간 **VM** 마이그레이션

- NSX Federation이나 다른 옵션을 사용하여 레이어 2 트래픽이 여러 데이터 센터에 걸쳐 확장되는 경우 vCenter 서버 간에 VM을 마이그레이션하는 절차를 따르세요.
- HCX는 다양한 "마이그레이션 유형" 가동 중지 없이 VM을 이동하기 위해 데이터 센터 전체에서 복제 지원 vMotion을 포함합니다.
- "사이트 복구 관리자(SRM)"일반적으로 재해 복구 목적으로 사용되며 스토리지 어레이 기반 복제를 활용한 계획된 마이그레이션에도 자주 사용됩니다.
- CDP(Continuous Data Protection) 제품 사용 "IO용 vSphere API(VAIO)" 데이터를 가로채서 원격 위치로 사본을 보내는 RPO 솔루션으로 거의 0에 가깝습니다.
- 백업 및 복구 제품도 활용할 수 있습니다. 하지만 종종 RTO가 길어집니다.
- "BlueXP 재해 복구 서비스(DRaaS)"스토리지 어레이 기반 복제를 활용하고 특정 작업을 자동화하여 대상 사이트에서 VM을 복구합니다.

하이브리드 클라우드 환경에서 **VM** 마이그레이션

- "하이브리드 연결 모드 구성"그리고 다음 절차를 따르세요"동일한 SSO 도메인의 vCenter 서버 간 VM 마이그레이션"
- HCX는 다양한 "마이그레이션 유형" 전원이 켜져 있는 동안 VM을 이동하기 위해 데이터 센터 전체에서 복제 지원 vMotion을 포함합니다.
  - "TR 4942: VMware HCX를 사용하여 FSx ONTAP 데이터 저장소로 워크로드 마이그레이션"
  - "TR-4940: VMware HCX를 사용하여 워크로드를 Azure NetApp Files 데이터 저장소로 마이그레이션 - 빠른 시작 가이드"
  - "VMware HCX를 사용하여 Google Cloud NetApp Volumes 데이터 저장소로 워크로드 마이그레이션 - 빠른 시작 가이드"
- "BlueXP 재해 복구 서비스(DRaaS)"스토리지 어레이 기반 복제를 활용하고 특정 작업을 자동화하여 대상 사이트에서 VM을 복구합니다.
- 지원되는 CDP(Continous Data Protection) 제품을 사용하는 경우 "IO용 vSphere API(VAIO)" 데이터를 가로채서 원격 위치로 사본을 보내는 RPO 솔루션으로 거의 0에 가깝습니다.

> 소스 VM이 블록 vVol 데이터 저장소에 있는 경우 SnapMirror 사용하여 다른 지원되는 클라우드 공급자의 Amazon FSx ONTAP 또는 Cloud Volumes ONTAP (CVO)로 복제하고 클라우드 네이티브 VM에서 iSCSI 볼륨으로 사용할 수 있습니다.

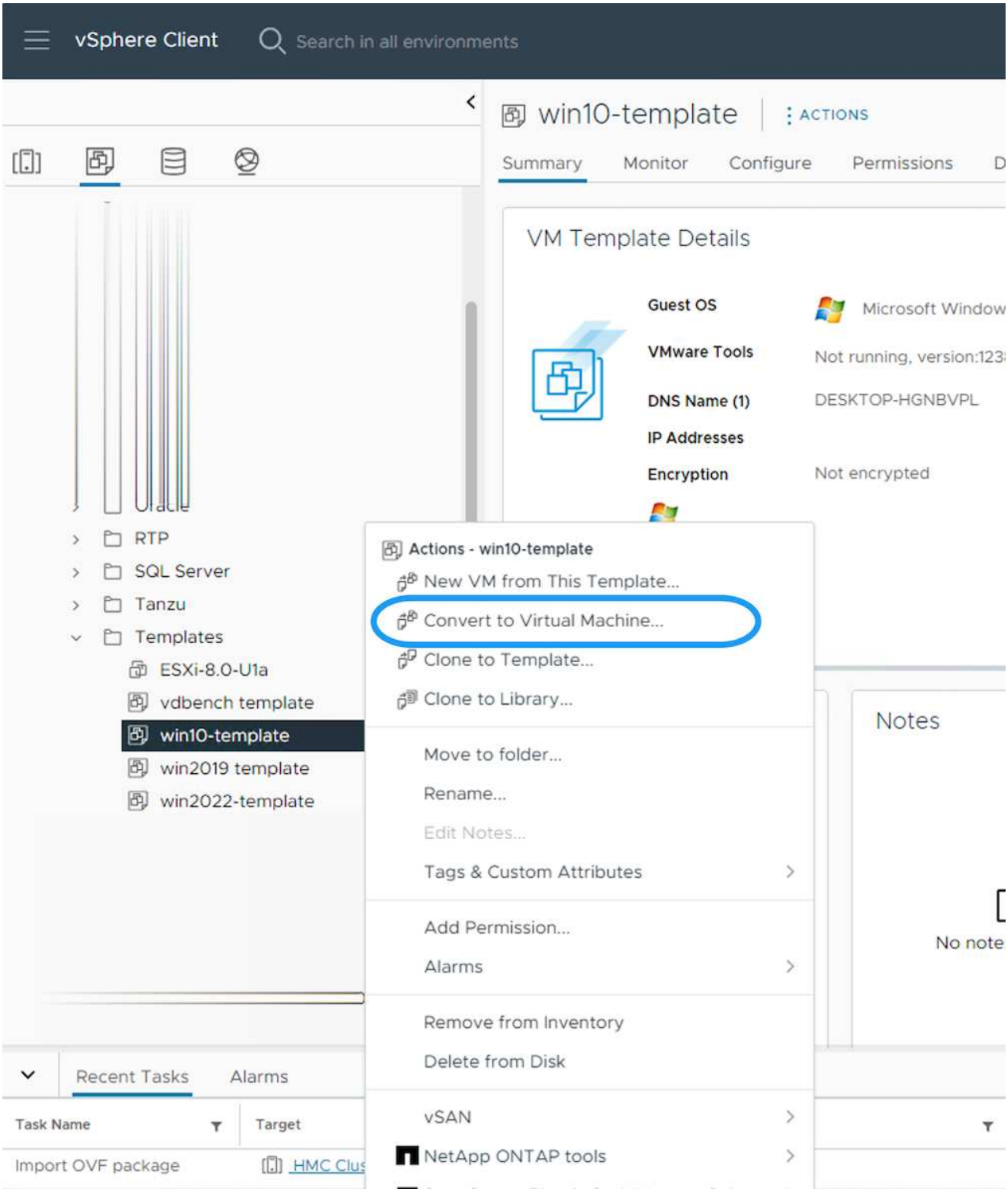
VM 템플릿 마이그레이션 시나리오

VM 템플릿은 vCenter Server나 콘텐츠 라이브러리에서 관리할 수 있습니다. VM 템플릿, OVF 및 OVA 템플릿, 기타 유형의 파일은 로컬 콘텐츠 라이브러리에 게시하여 배포하고 원격 콘텐츠 라이브러리에서 구독할 수 있습니다.

- vCenter 인벤토리에 저장된 VM 템플릿은 VM으로 변환할 수 있으며 VM 마이그레이션 옵션을 사용할 수 있습니다.
- OVF 및 OVA 템플릿, 콘텐츠 라이브러리에 저장된 다른 유형의 파일은 다른 콘텐츠 라이브러리에 복제될 수 있습니다.
- 콘텐츠 라이브러리 VM 템플릿은 모든 데이터 저장소에 호스팅될 수 있으며 새 콘텐츠 라이브러리에 추가해야 합니다.

데이터 저장소에 호스팅된 **VM** 템플릿 마이그레이션

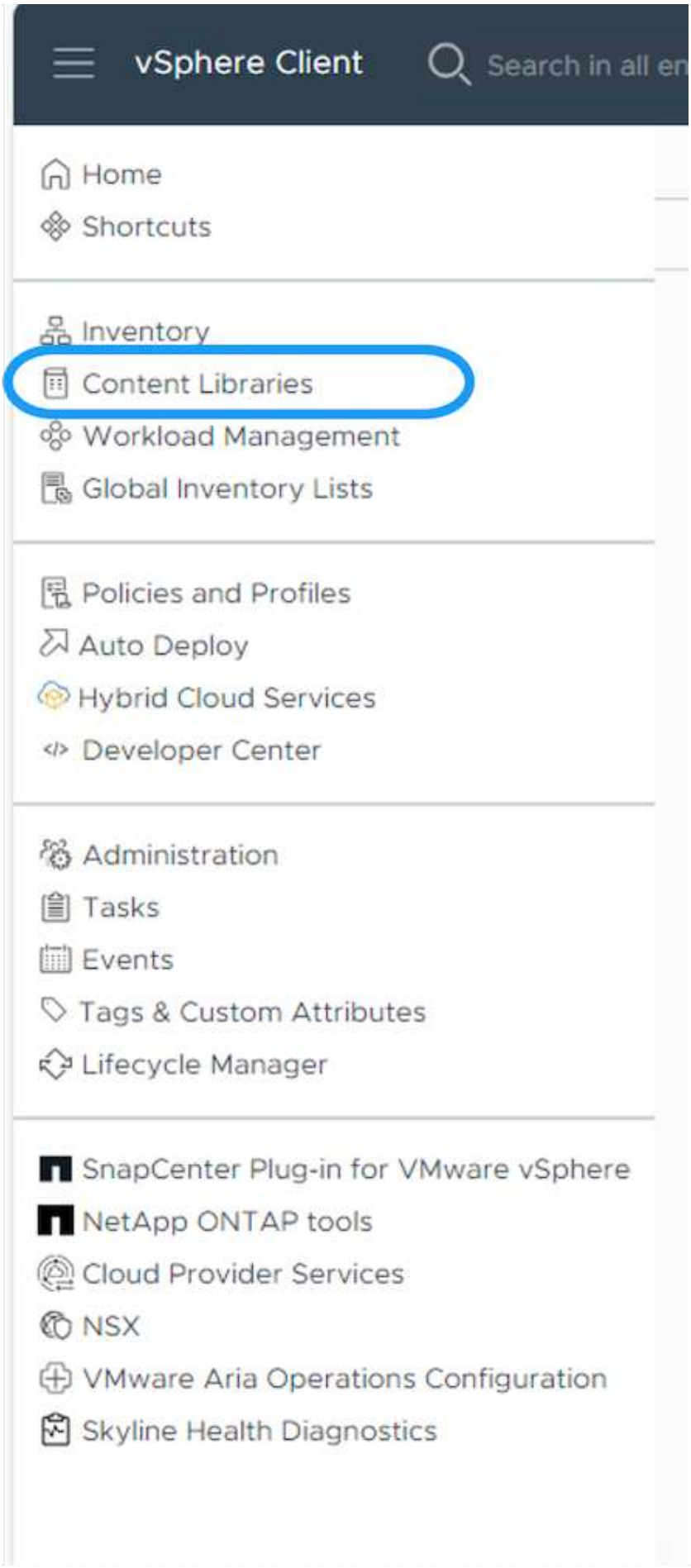
1. vSphere Web Client에서 VM 및 템플릿 폴더 보기 아래에 있는 VM 템플릿을 마우스 오른쪽 버튼으로 클릭하고 VM으로 변환하는 옵션을 선택합니다.



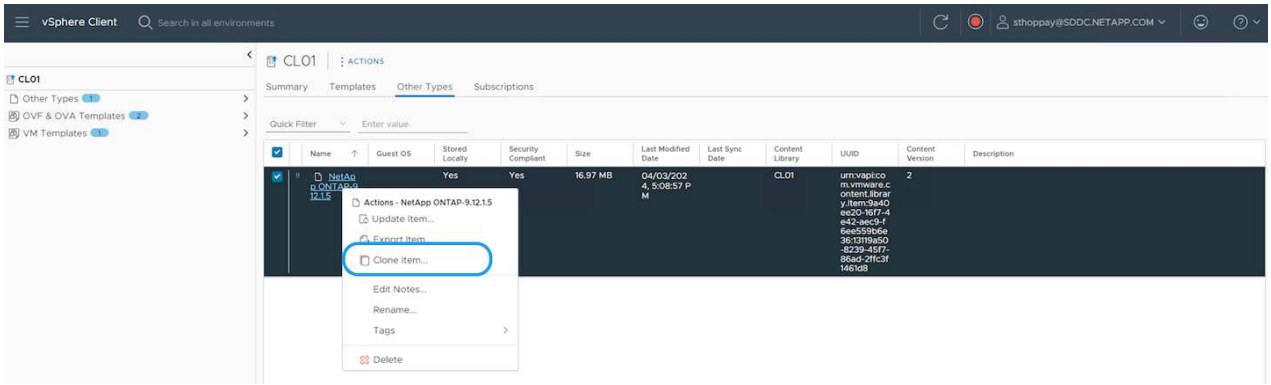
2. VM으로 변환한 후 VM 마이그레이션 옵션을 따르세요.

콘텐츠 라이브러리 항목 복제

1. vSphere Web Client에서 콘텐츠 라이브러리를 선택하세요.

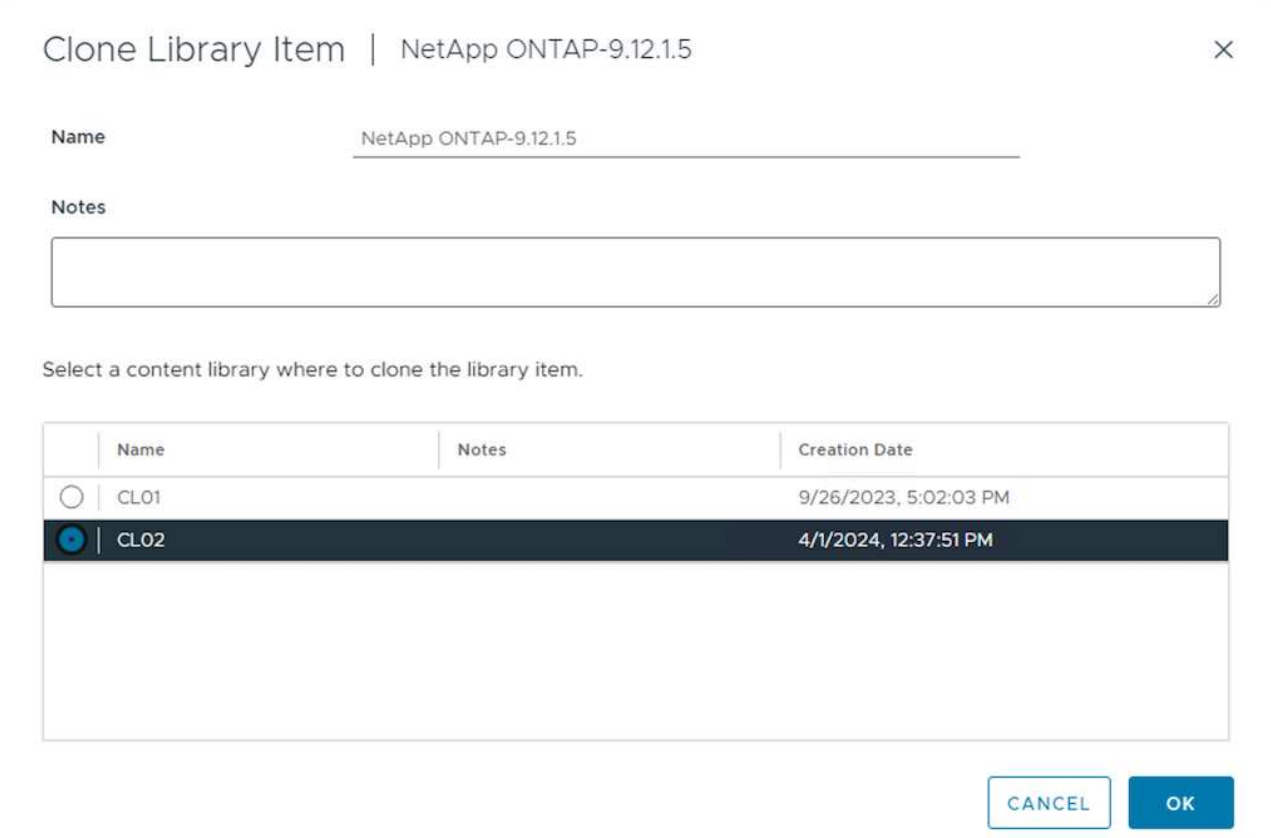

vSphere Client
Search in all en
Home
Shortcuts
Inventory
Content Libraries
Workload Management
Global Inventory Lists
Policies and Profiles
Auto Deploy
Hybrid Cloud Services
Developer Center
Administration
Tasks
Events
Tags & Custom Attributes
Lifecycle Manager
SnapCenter Plug-in for VMware vSphere
NetApp ONTAP tools
Cloud Provider Services
NSX
VMware Aria Operations Configuration
Skyline Health Diagnostics

2. 복제하려는 항목이 있는 콘텐츠 라이브러리를 선택하세요.
3. 항목을 마우스 오른쪽 버튼으로 클릭하고 항목 복제를 클릭합니다.

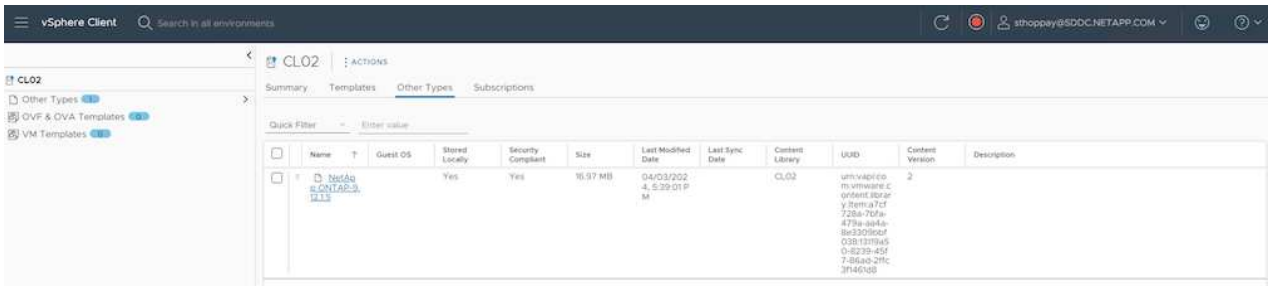


작업 메뉴를 사용하는 경우 작업을 수행할 올바른 대상 개체가 나열되어 있는지 확인하세요.

4. 대상 콘텐츠 라이브러리를 선택하고 확인을 클릭합니다.



5. 해당 항목이 대상 콘텐츠 라이브러리에서 사용 가능한지 확인합니다.

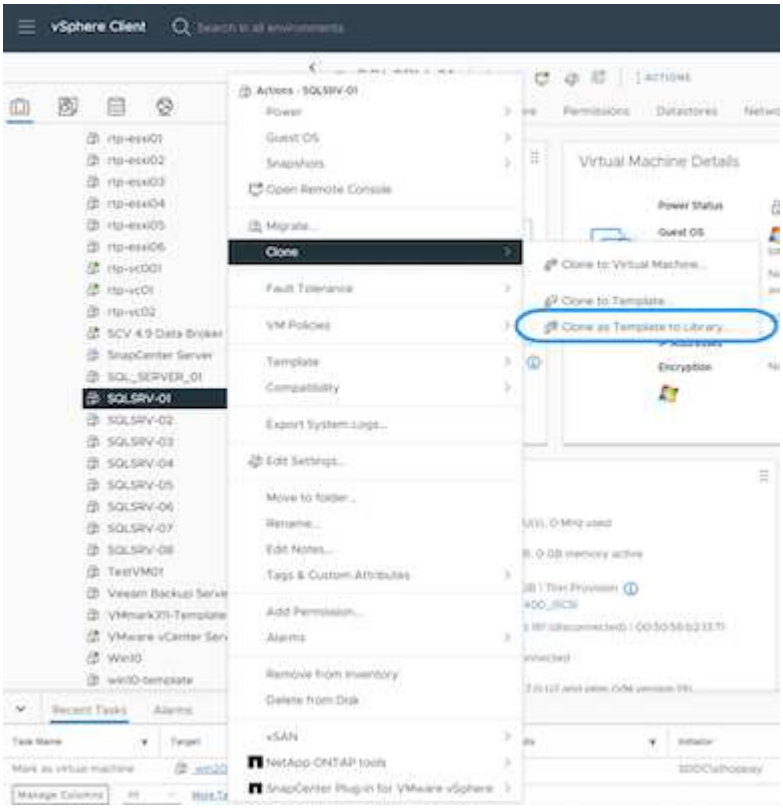


다음은 콘텐츠 라이브러리 CL01에서 CL02로 콘텐츠 라이브러리 항목을 복사하는 PowerCLI 스크립트 샘플입니다.

```
#Authenticate to vCenter Server(s)
$sourcevc = Connect-VIServer -server 'vcenter01.domain' -force
$targetvc = Connect-VIServer -server 'vcenter02.domain' -force

#Copy content library items from source vCenter content library CL01 to
target vCenter content library CL02.
Get-ContentLibaryItem -ContentLibary (Get-ContentLibary 'CL01' -Server
$sourcevc) | Where-Object { $_.ItemType -ne 'vm-template' } | Copy-
ContentLibaryItem -ContentLibrary (Get-ContentLibary 'CL02' -Server
$targetvc)
```

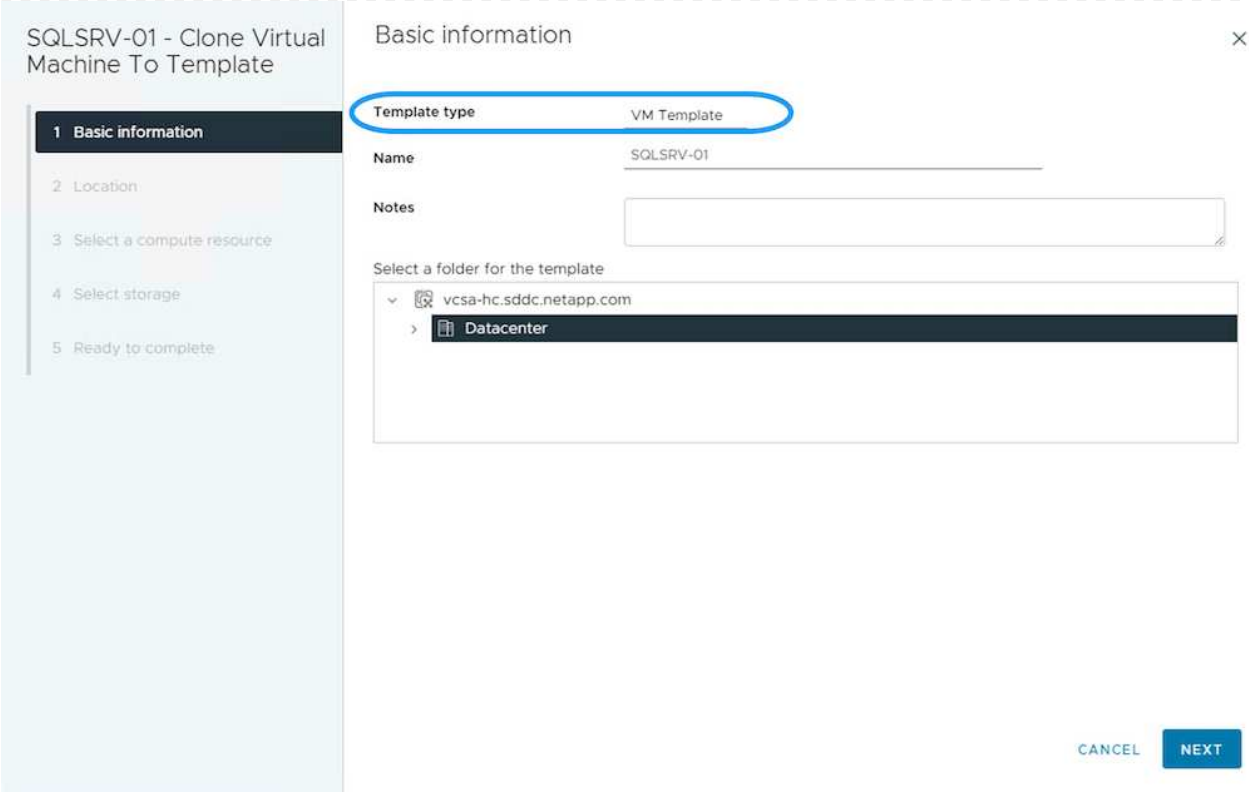
콘텐츠 라이브러리에 **VM**을 템플릿으로 추가

1. vSphere Web Client에서 VM을 선택하고 마우스 오른쪽 버튼을 클릭하여 라이브러리에서 템플릿으로 복제를 선택합니다.



> 라이브러리에서 복제할 VM 템플릿을 선택하면 OVF 및 OVA 템플릿으로만 저장할 수 있으며 VM 템플릿으로는 저장할 수 없습니다.

2. 템플릿 유형이 VM 템플릿으로 선택되었는지 확인하고 마법사의 지시에 따라 작업을 완료합니다.



콘텐츠 라이브러리의 VM 템플릿에 대한 추가 세부 정보는 다음을 확인하세요. "vSphere VM 관리 가이드"

사용 사례

타사 스토리지 시스템(**vSAN** 포함)에서 **ONTAP** 데이터 저장소로 마이그레이션합니다.

- ONTAP 데이터 저장소가 프로비저닝되는 위치에 따라 위에서 VM 마이그레이션 옵션을 선택합니다.

이전 버전에서 최신 버전의 **vSphere**로 마이그레이션합니다.

- 기존 업그레이드가 불가능한 경우, 새로운 환경을 구축하고 위의 마이그레이션 옵션을 사용할 수 있습니다.

Cross vCenter 마이그레이션 옵션에서 소스에서 내보내기 옵션을 사용할 수 없는 경우 대상에서 가져옵니다. 해당 절차에 대해 다음을 확인하세요."고급 Cross vCenter vMotion을 사용하여 가상 머신 가져오기 또는 복제"

VCF 워크로드 도메인으로 마이그레이션.

- 각 vSphere 클러스터에서 대상 워크로드 도메인으로 VM을 마이그레이션합니다.

> 소스 vCenter의 다른 클러스터에 있는 기존 VM과 네트워크 통신을 허용하려면 소스 vCenter vSphere 호스트를 전송 영역에 추가하여 NSX 세그먼트를 확장하거나 에지에 L2 브리지를 사용하여 VLAN에서 L2 통신을 허용합니다. NSX 문서를 확인하세요 "브리징을 위한 Edge VM 구성"

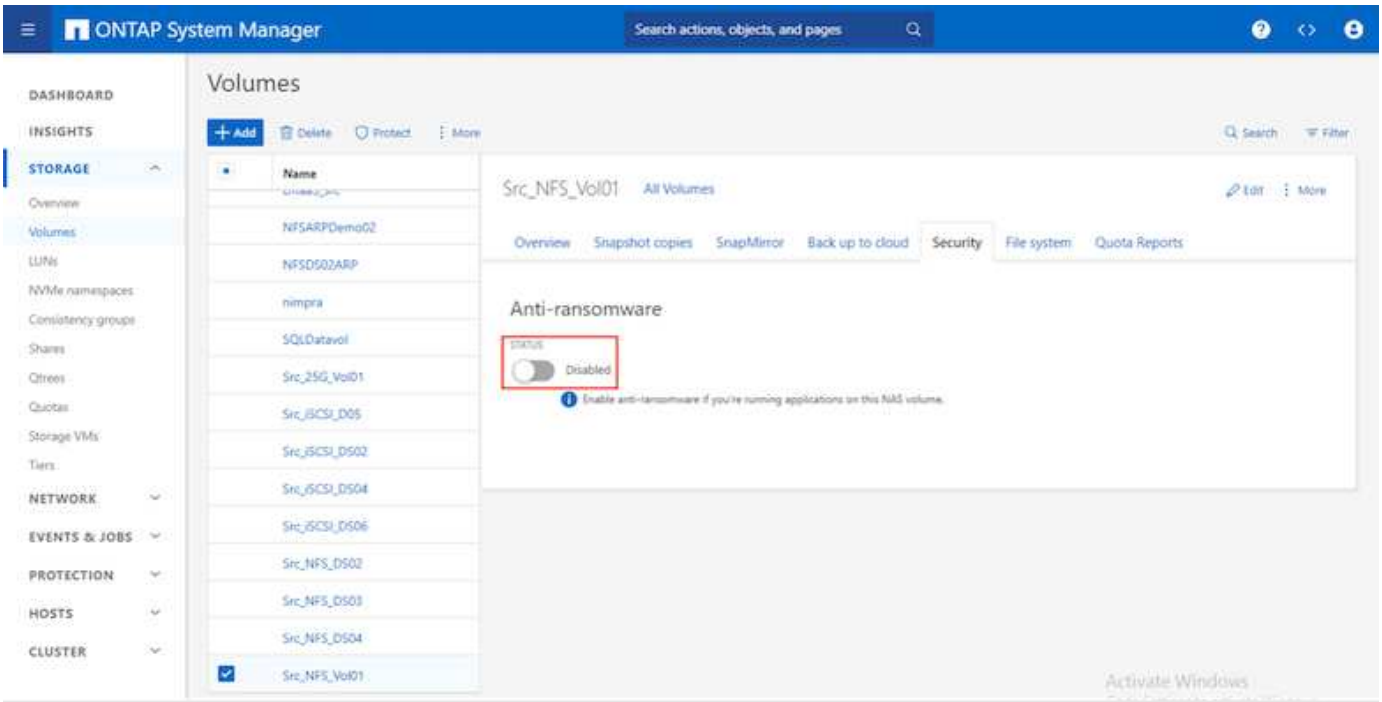
추가 자료

- "vSphere 가상 머신 마이그레이션"
- "vSphere vMotion을 사용하여 가상 머신 마이그레이션"
- "NSX 페더레이션의 Tier-0 게이트웨이 구성"
- "HCX 4.8 사용자 가이드"
- "VMware Live Recovery 설명서"
- "VMware용 BlueXP disaster recovery"

NFS 스토리지를 위한 자율형 랜섬웨어 보호

랜섬웨어를 가능한 한 일찍 감지하는 것은 확산을 막고 비용이 많이 드는 가동 중지 시간을 피하는 데 매우 중요합니다. 효과적인 랜섬웨어 탐지 전략에는 ESXi 호스트 및 게스트 VM 수준에서 여러 계층의 보호가 통합되어야 합니다. 랜섬웨어 공격에 대한 포괄적인 방어를 구축하기 위해 여러 가지 보안 조치가 구현되어 있지만, ONTAP 사용하면 전반적인 방어 방식에 더 많은 보호 계층을 추가할 수 있습니다. 몇 가지 기능을 꼽자면 스냅샷, 자율 랜섬웨어 보호, 변조 방지 스냅샷 등이 있습니다.

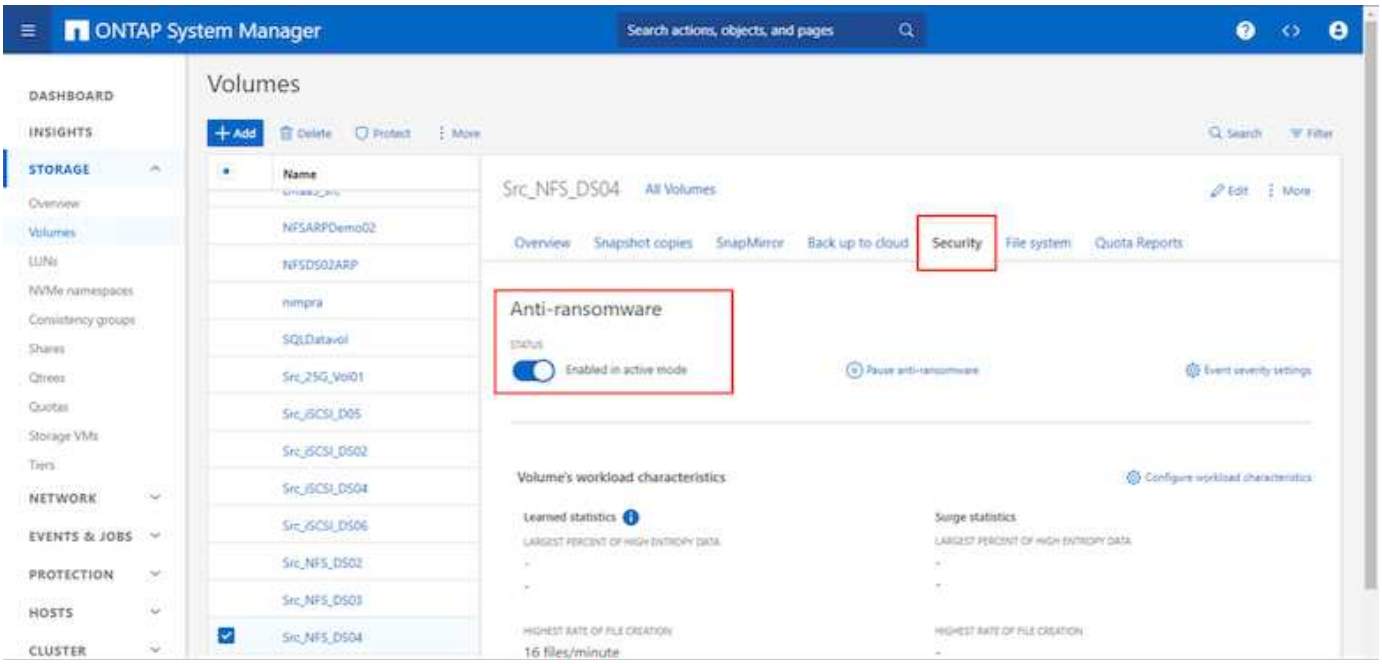
위에서 언급한 기능이 VMware와 함께 작동하여 랜섬웨어로부터 데이터를 보호하고 복구하는 방법을 살펴보겠습니다. vSphere와 게스트 VM을 공격으로부터 보호하려면 세분화, 엔드포인트에 EDR/XDR/SIEM 활용, 보안 업데이트 설치, 적절한 강화 지침 준수 등 여러 가지 조치를 취하는 것이 필수적입니다. 데이터 저장소에 있는 각 가상 머신은 표준 운영 체제도 호스팅합니다. 다중 계층 랜섬웨어 보호 전략의 필수 구성 요소인 기업용 서버용 맬웨어 방지 제품군을 설치하고 정기적으로 업데이트하세요. 이와 함께 데이터 저장소에 전원을 공급하는 NFS 볼륨에서 ARP(자율 랜섬웨어 보호)를 활성화합니다. ARP는 볼륨 워크로드 활동과 데이터 엔트로피를 살펴보는 내장된 온박스 ML을 활용하여 랜섬웨어를 자동으로 감지합니다. ARP는 ONTAP 내장 관리 인터페이스나 시스템 관리자를 통해 구성할 수 있으며 볼륨별로 활성화됩니다.



현재 기술 미리보기 단계에 있는 새로운 NetApp ARP/AI를 사용하면 학습 모드가 필요하지 않습니다. 대신 AI 기반 랜섬웨어 감지 기능으로 바로 활성 모드로 전환할 수 있습니다.

ONTAP One을 사용하면 이러한 모든 기능 세트가 완전히 무료입니다. 라이선스 장벽에 대한 걱정 없이 NetApp의 강력한 데이터 보호, 보안 및 ONTAP 제공하는 모든 기능을 이용하세요.

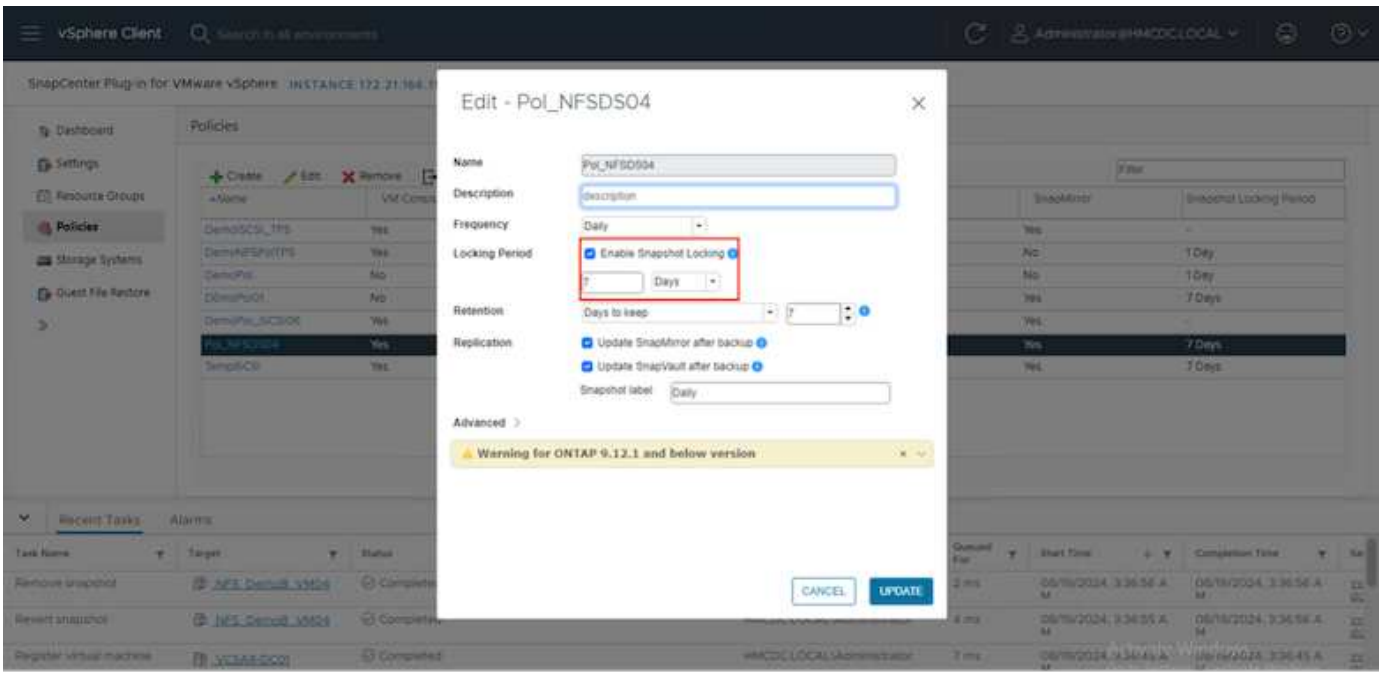
활성 모드가 되면 랜섬웨어일 가능성이 있는 비정상적인 볼륨 활동을 찾기 시작합니다. 비정상적인 활동이 감지되면 자동으로 스냅샷 복사본이 즉시 생성되어 파일 감염 시점에 최대한 가까운 복원 지점을 제공합니다. ARP는 암호화된 볼륨에 새로운 확장자가 추가되거나 파일 확장자가 수정될 때 VM 외부에 있는 NFS 볼륨에서 VM 특정 파일 확장자의 변경 사항을 감지할 수 있습니다.



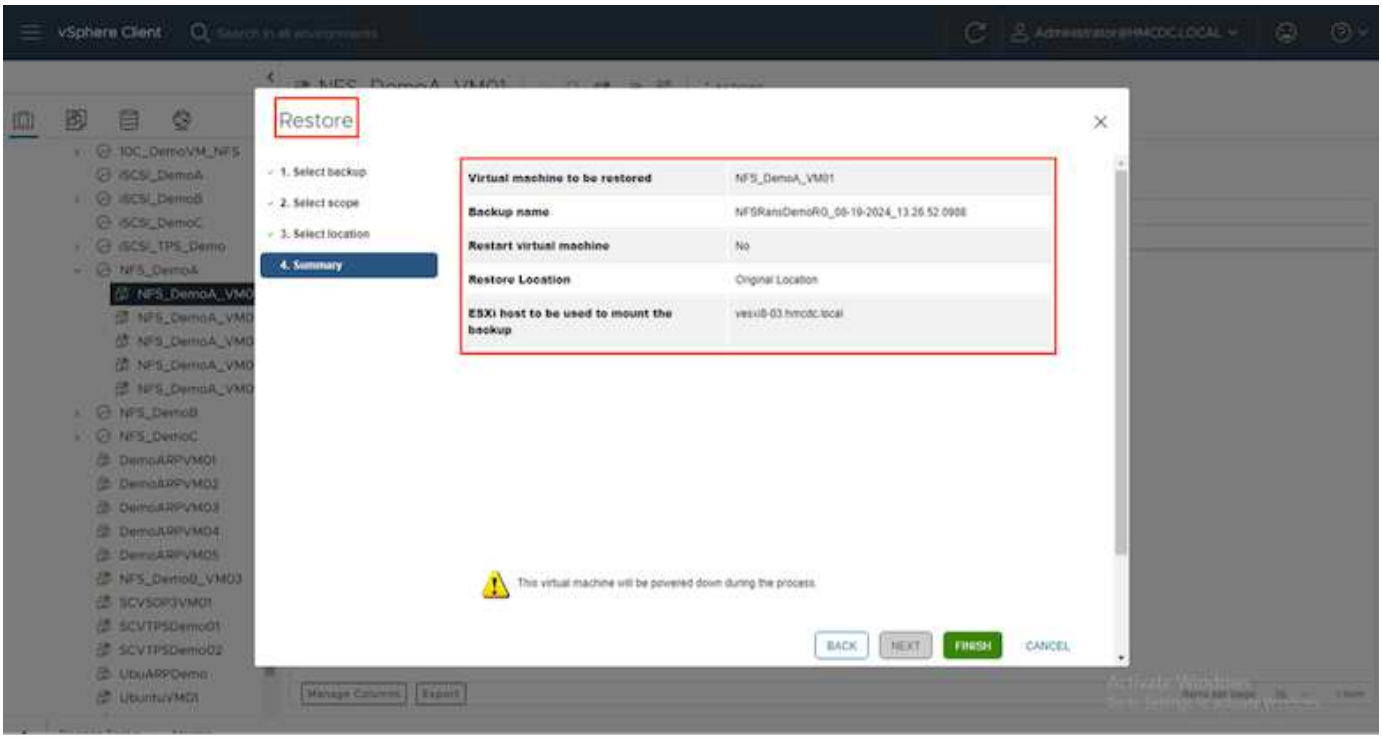
랜섬웨어 공격이 가상 머신(VM)을 표적으로 삼아 VM 외부의 파일을 변경하지 않고 VM 내부의 파일을 변경하는 경우에도 고급 랜섬웨어 보호(ARP)는 VM의 기본 엔트로피가 낮으면(예: .txt, .docx 또는 .mp4 파일) 위협을 감지합니다. 이 시나리오에서 ARP가 보호 스냅샷을 생성하더라도 VM 외부의 파일 확장자가 변조되지 않았기 때문에 위협 경고는 생성되지 않습니다. 이러한 시나리오에서 초기 방어 계층은 이상을 식별하지만 ARP는 엔트로피를 기반으로 스냅샷을 만드는 데 도움이 됩니다.

자세한 내용은 "ARP 및 가상 머신" 섹션을 참조하세요."ARP 사용 사례 및 고려 사항" .

파일에서 백업 데이터로 이동하는 랜섬웨어 공격은 이제 파일 암호화를 시작하기 전에 백업 및 스냅샷 복구 지점을 삭제하려고 시도하여 이를 표적으로 삼는 경우가 늘고 있습니다. 그러나 ONTAP 사용하면 기본 또는 보조 시스템에서 변조 방지 스냅샷을 생성하여 이를 방지할 수 있습니다."NetApp 스냅샷 복사 잠금" .



이러한 스냅샷 사본은 랜섬웨어 공격자나 사기성 관리자가 삭제하거나 변경할 수 없으므로 공격을 받은 후에도 사용할 수 있습니다. 데이터 저장소나 특정 가상 머신이 영향을 받는 경우 SnapCenter 몇 초 만에 가상 머신 데이터를 복구하여 조직의 가동 중지 시간을 최소화할 수 있습니다.

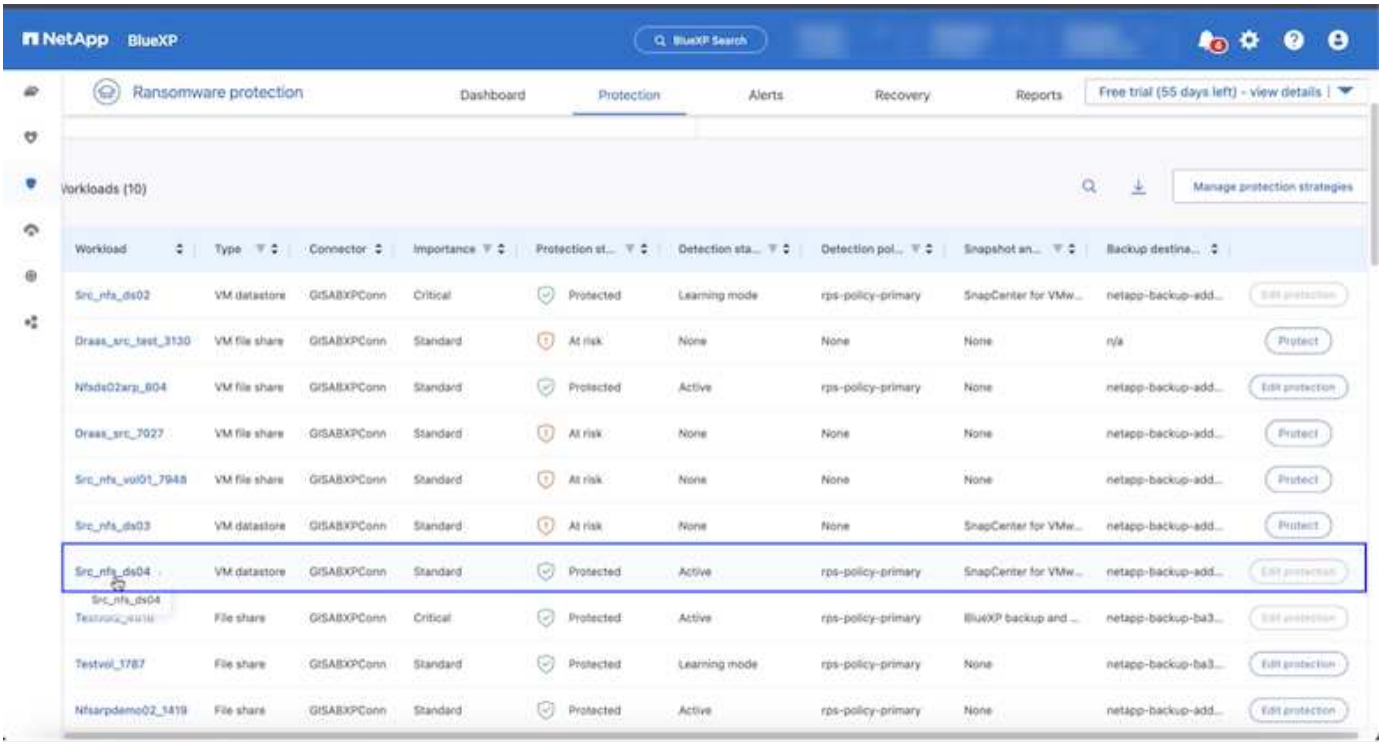


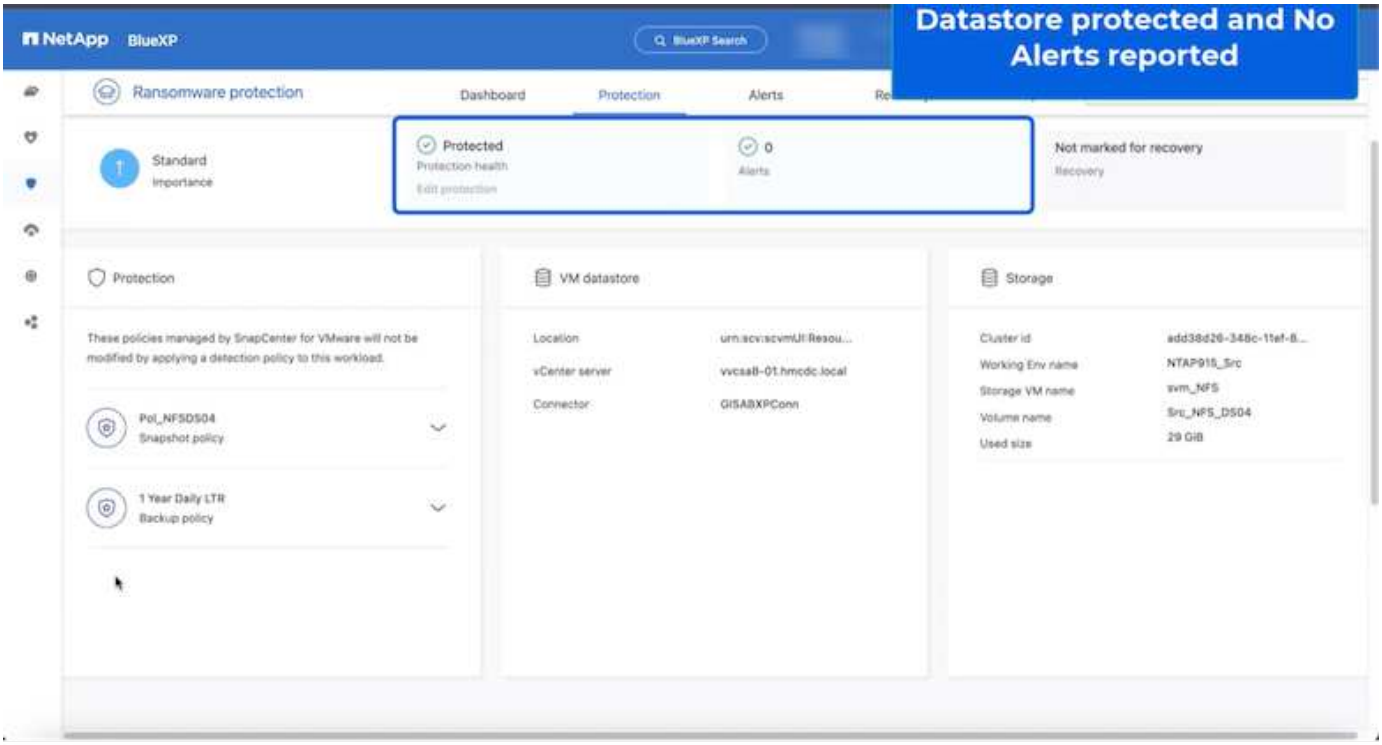
위의 내용은 ONTAP 스토리지가 기존 기술에 추가적인 계층을 추가하여 환경의 미래지향성을 강화하는 방식을 보여줍니다.

추가 정보는 다음 지침을 참조하세요."랜섬웨어에 대한 NetApp 솔루션" .

이제 이 모든 것을 SIEM 도구로 조율하고 통합해야 하는 경우 BlueXP ransomware protection 와 같은 오프탭 서비스를 사용할 수 있습니다. 랜섬웨어로부터 데이터를 보호하도록 설계된 서비스입니다. 이 서비스는 온프레미스 NFS 스토리지의 Oracle, MySQL, VM 데이터 저장소, 파일 공유 등의 애플리케이션 기반 워크로드에 대한 보호 기능을 제공합니다.

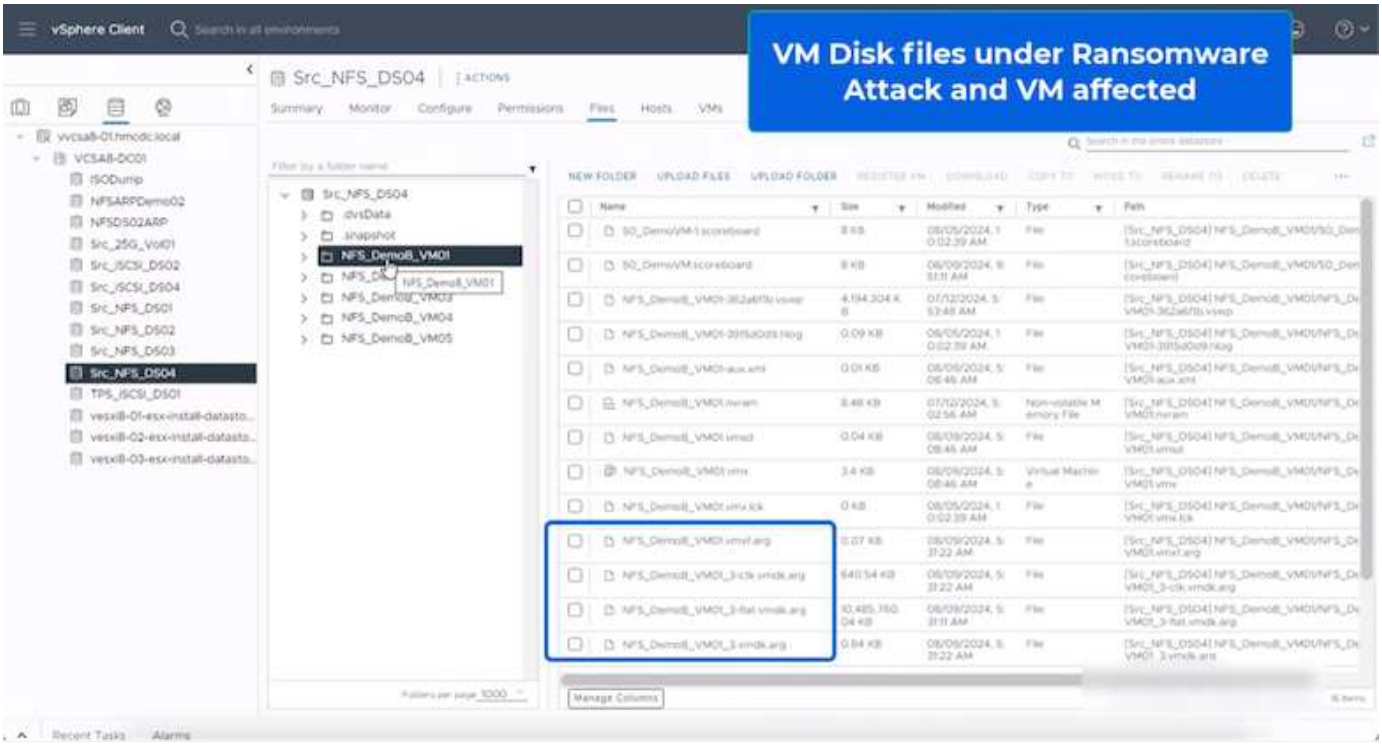
이 예에서 NFS 데이터 저장소 "Src_NFS_DS04"는 BlueXP ransomware protection 사용하여 보호됩니다.



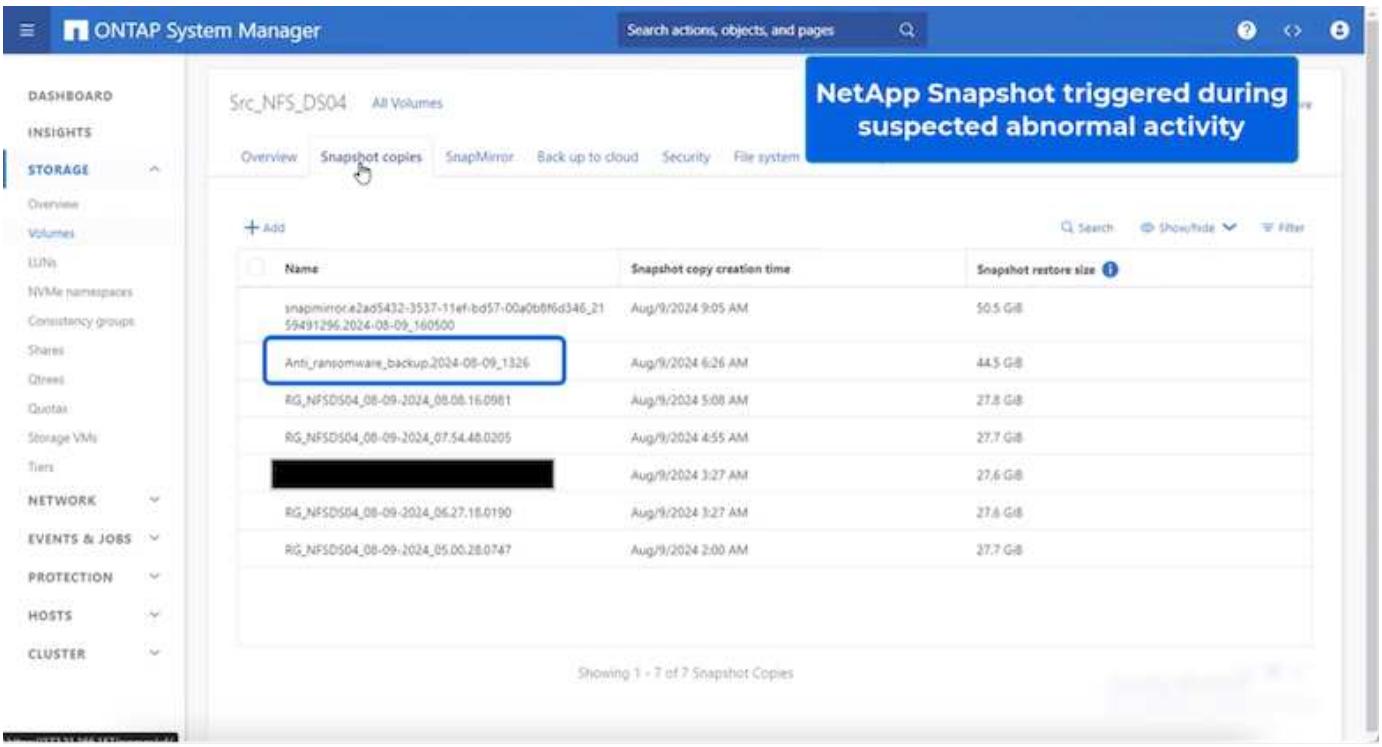


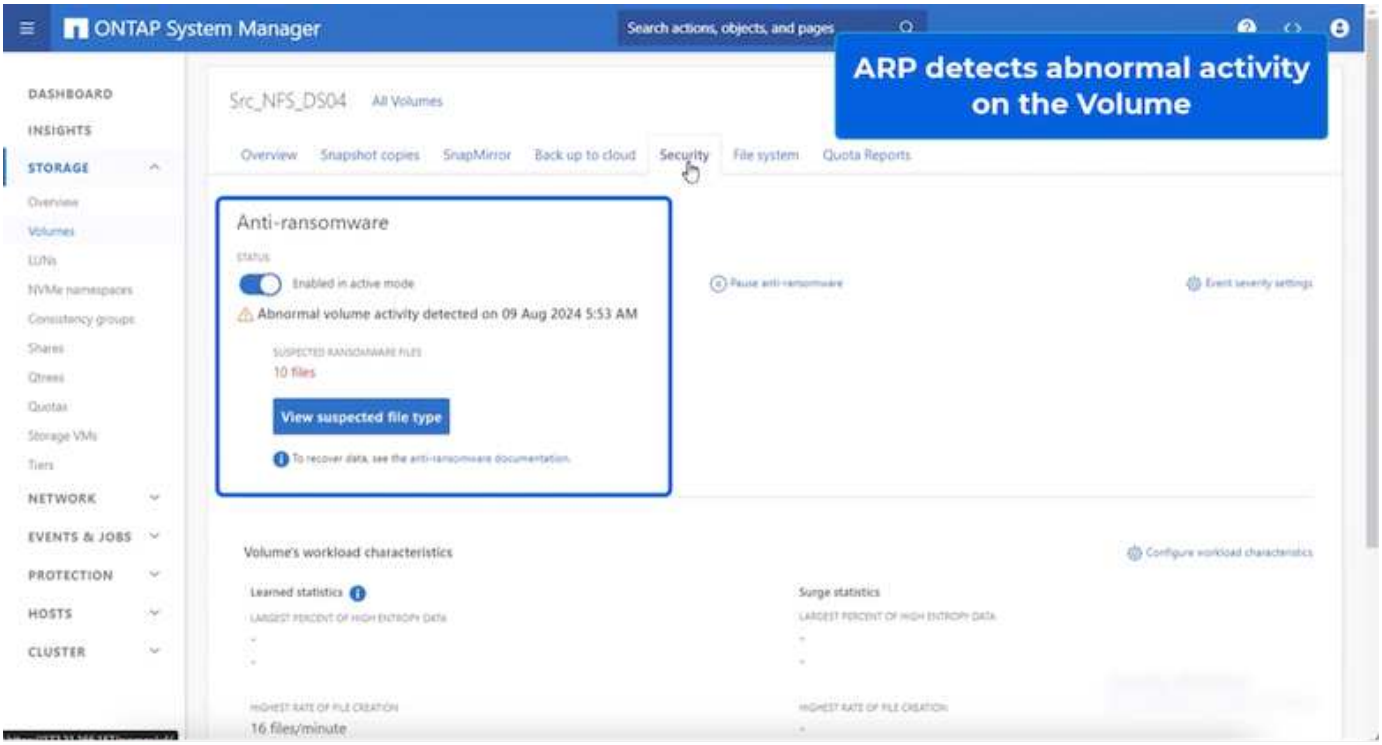
BlueXP ransomware protection 구성에 대한 자세한 내용은 다음을 참조하세요."BlueXP ransomware protection 설정" 그리고"BlueXP ransomware protection 설정 구성" .

이제 예를 들어 이를 살펴보겠습니다. 이 연습에서는 데이터 저장소 "Src_NFS_DS04"가 영향을 받습니다.

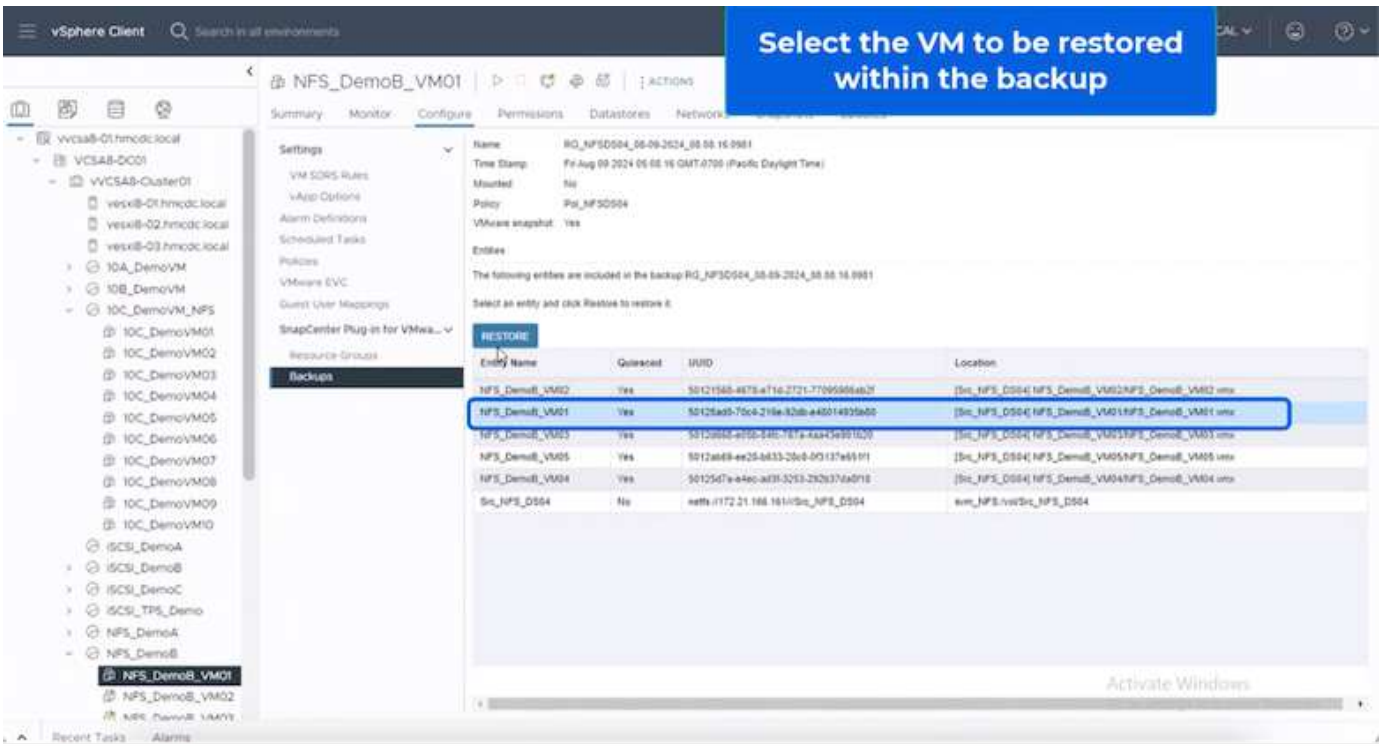


ARP는 감지되자마자 볼륨에 대한 스냅샷을 즉시 트리거했습니다.





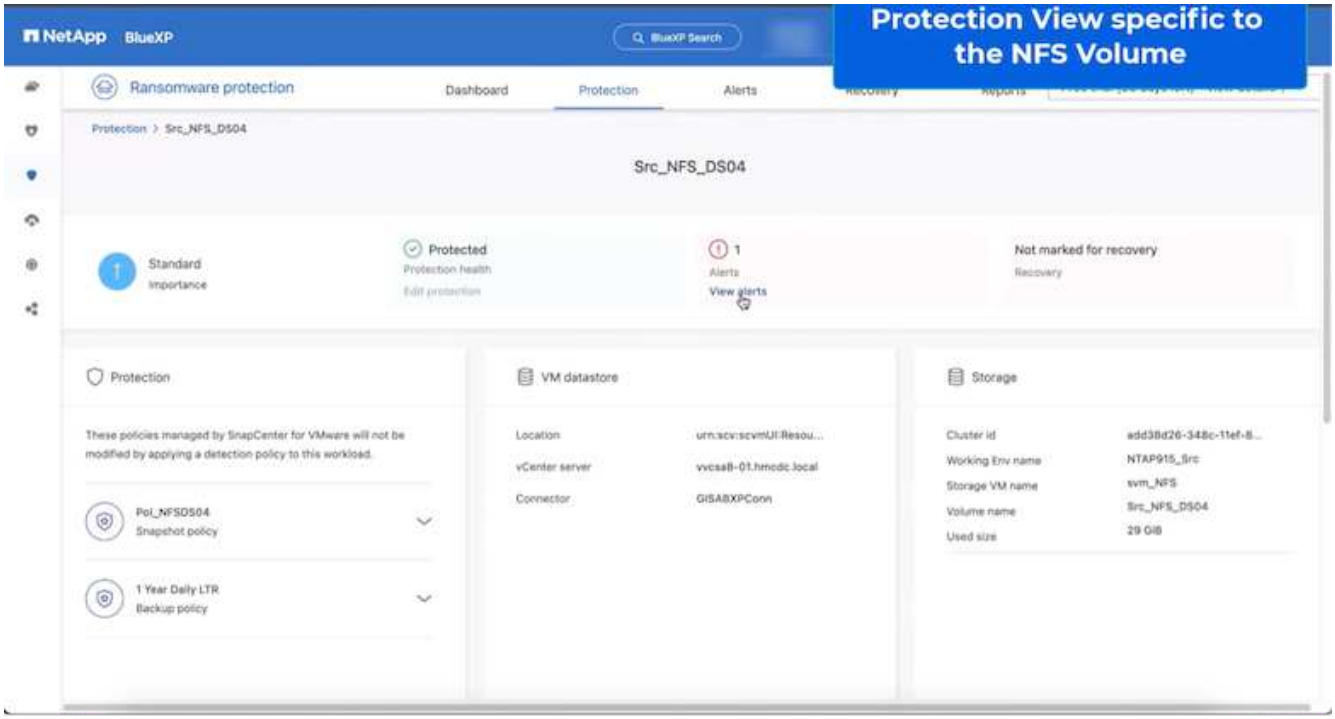
포렌식 분석이 완료되면 SnapCenter 또는 BlueXP ransomware protection 사용하여 신속하고 원활하게 복원할 수 있습니다. SnapCenter 사용하여 영향을 받은 가상 머신으로 이동하여 복원할 적절한 스냅샷을 선택합니다.



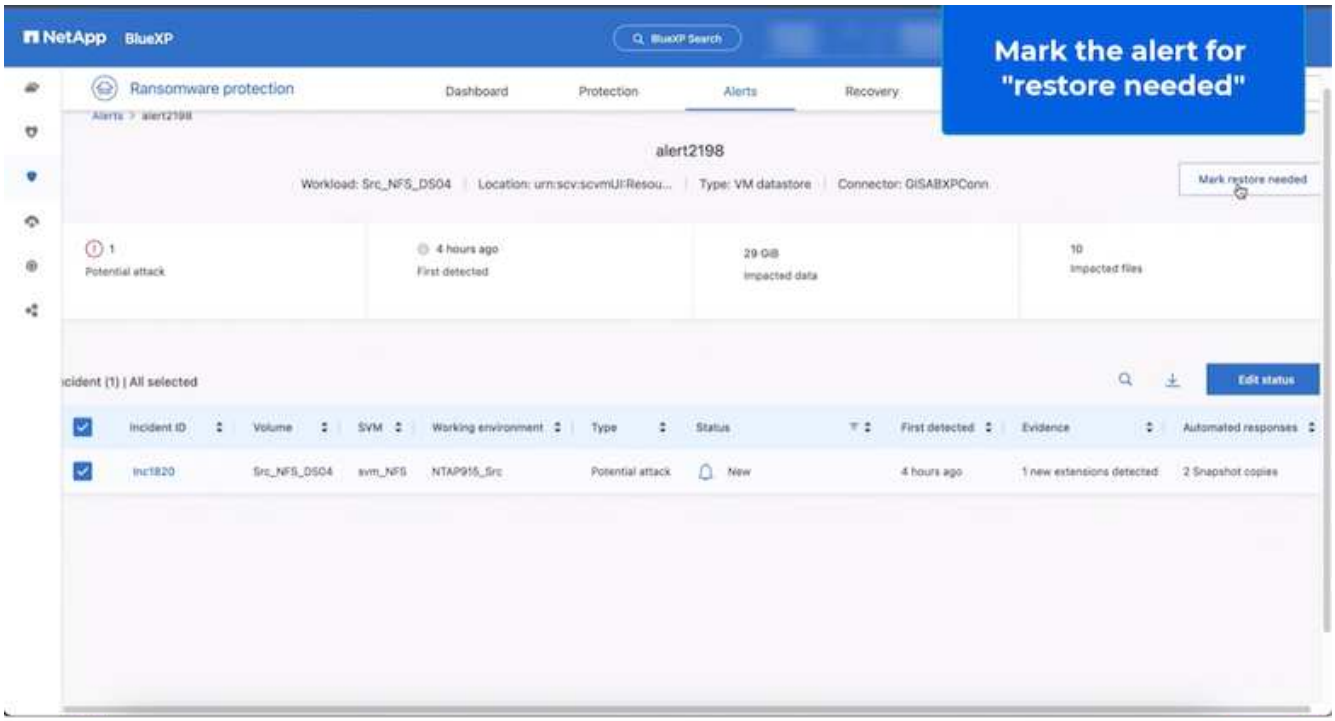
이 섹션에서는 BlueXP ransomware protection VM 파일이 암호화된 랜섬웨어 사고로부터 복구를 어떻게 조율하는지 살펴봅니다.

> VM이 SnapCenter 에서 관리되는 경우 BlueXP ransomware protection VM 일관성 프로세스를 사용하여 VM을 이전 상태로 복원합니다.

1. BlueXP ransomware protection 에 액세스하면 BlueXP ransomware protection 보드에 알림이 나타납니다.
2. 생성된 경고에 대한 특정 볼륨의 인시던트를 검토하려면 경고를 클릭하세요.

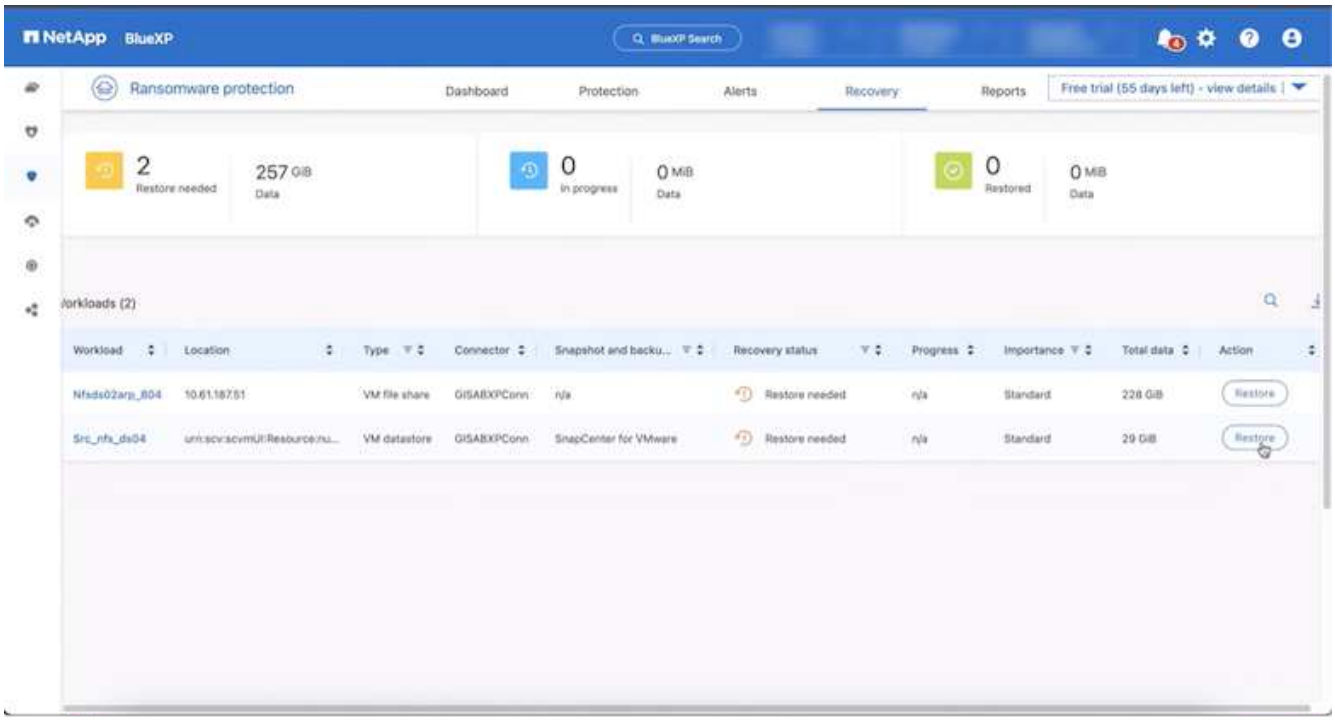


3. "복원 필요 표시"를 선택하여 랜섬웨어 사고를 복구 준비로 표시합니다(사고가 중화되면).

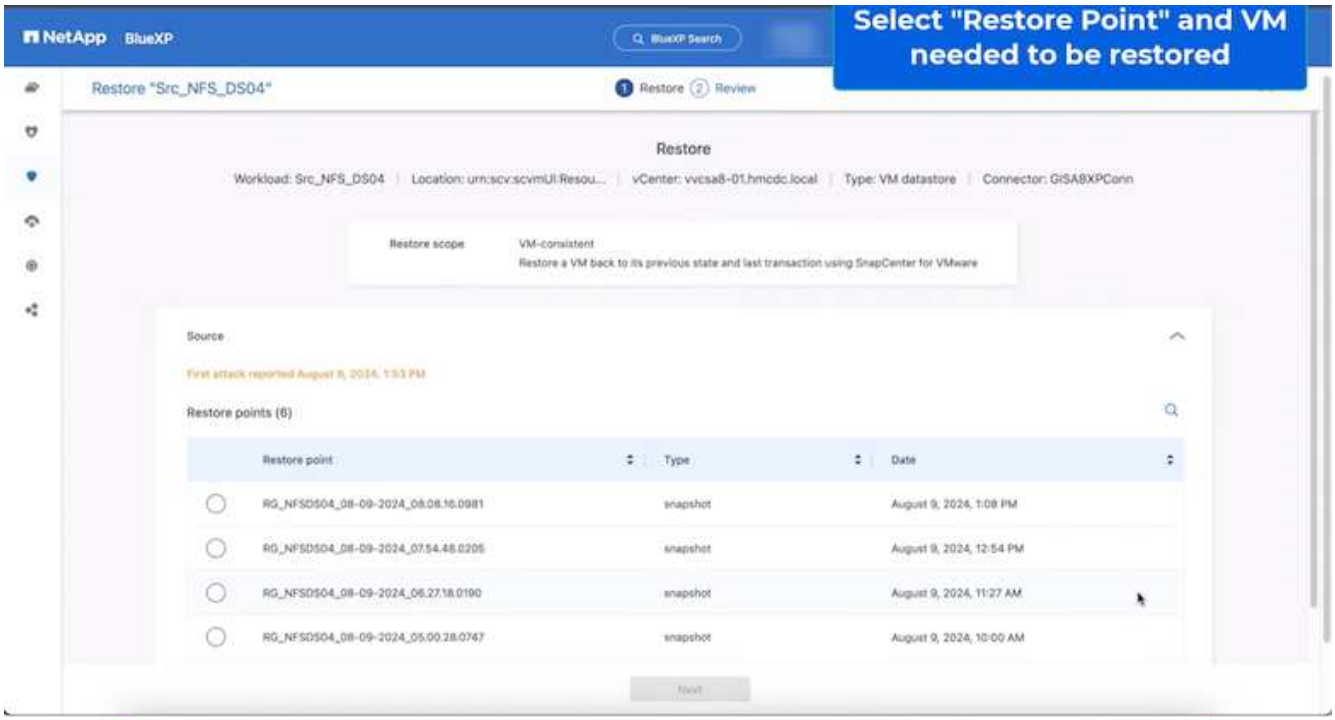


ⓘ 사건이 거짓 양성으로 판명되면 경고를 해제할 수 있습니다.

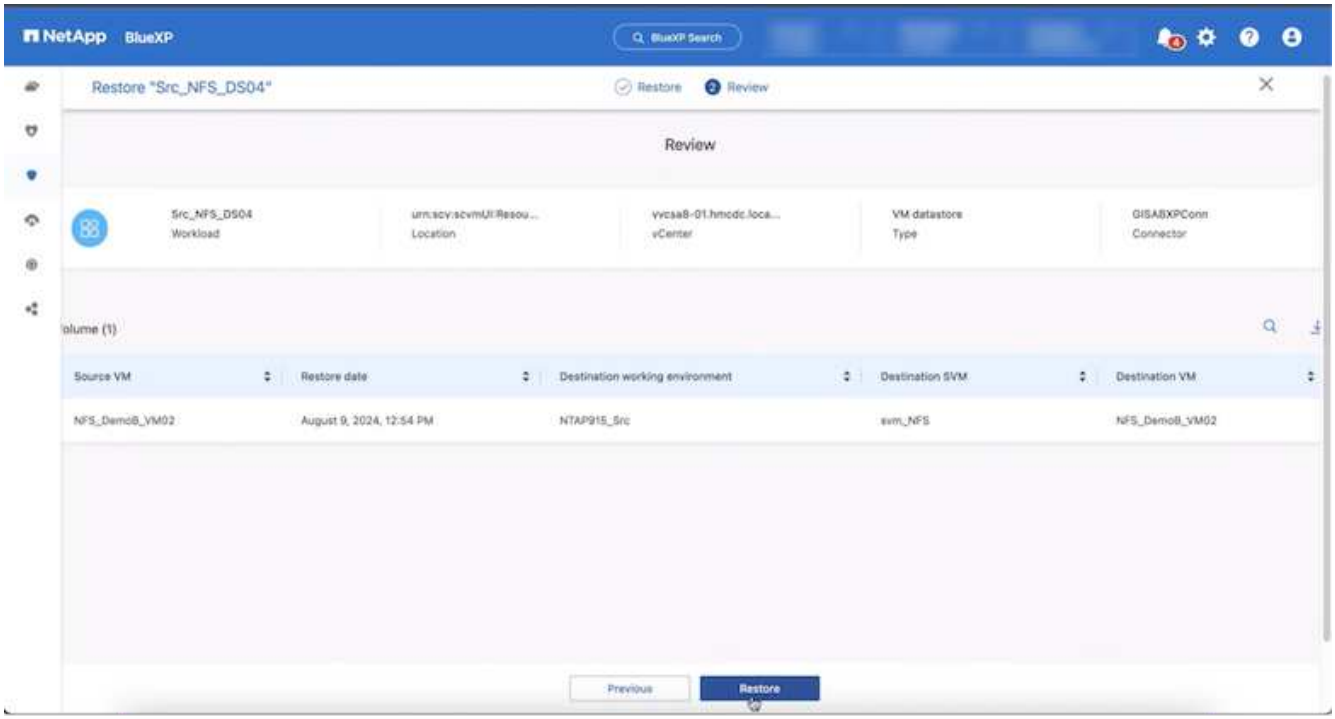
4. 복구 탭으로 이동하여 복구 페이지에서 작업 부하 정보를 검토하고 "복원 필요" 상태에 있는 데이터 저장소 볼륨을 선택하고 복원을 선택합니다.



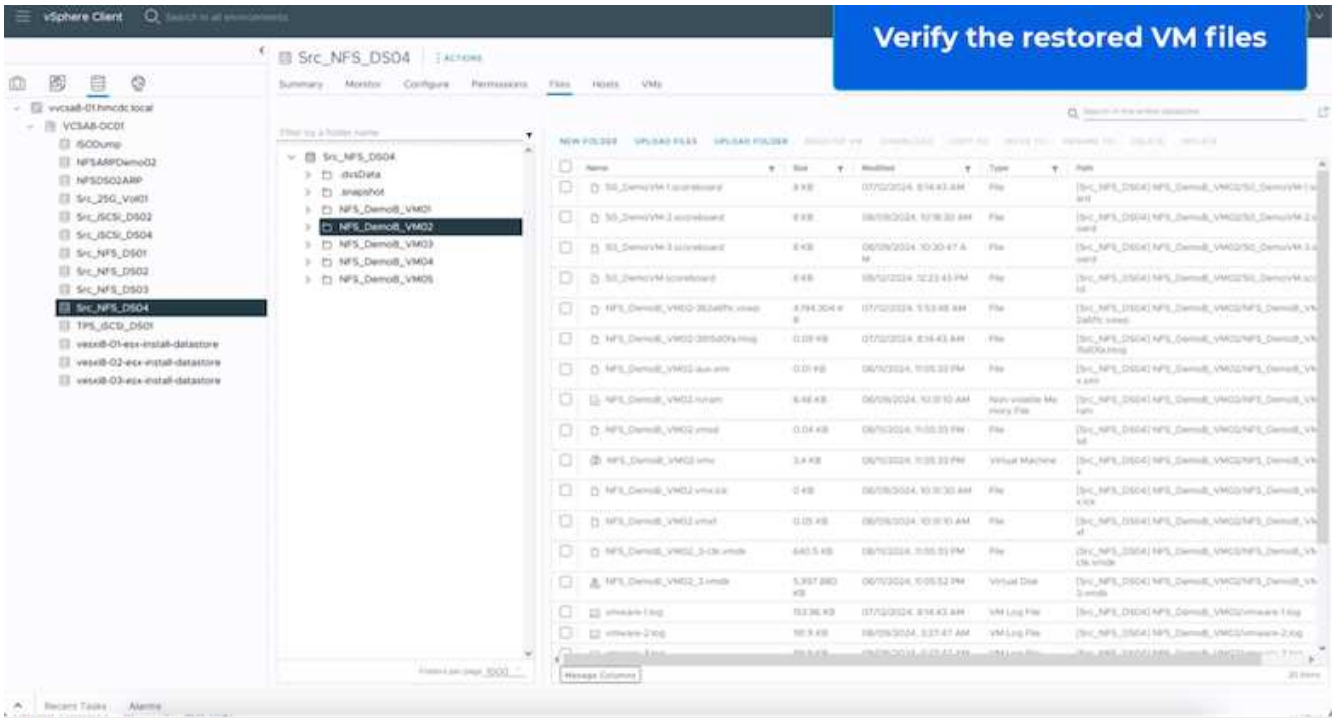
5. 이 경우 복원 범위는 "VM별"입니다(VM용 SnapCenter 의 경우 복원 범위는 "VM별"입니다).



6. 데이터를 복원하는 데 사용할 복원 지점을 선택하고 대상을 선택한 후 복원을 클릭합니다.



7. 상단 메뉴에서 복구를 선택하면 복구 페이지에서 작업 부하를 검토할 수 있습니다. 복구 페이지에서는 작업 상태가 여러 상태로 이동합니다. 복원이 완료되면 VM 파일이 아래와 같이 복원됩니다.



복구는 애플리케이션에 따라 VMware용 SnapCenter 또는 SnapCenter 플러그인에서 수행할 수 있습니다.

NetApp 솔루션은 가시성, 탐지 및 치료를 위한 다양하고 효과적인 도구를 제공하여 랜섬웨어를 조기에 발견하고 확산을 방지하며 필요한 경우 신속하게 복구하여 비용이 많이 드는 가동 중지 시간을 피할 수 있도록 지원합니다. 기존의 계층적 방어 솔루션이 여전히 널리 사용되고 있으며, 가시성과 감지를 위해 타사 및 파트너 솔루션도 많이 사용됩니다. 효과적인

복구는 모든 위협에 대응하는 데 있어 여전히 중요한 부분입니다.

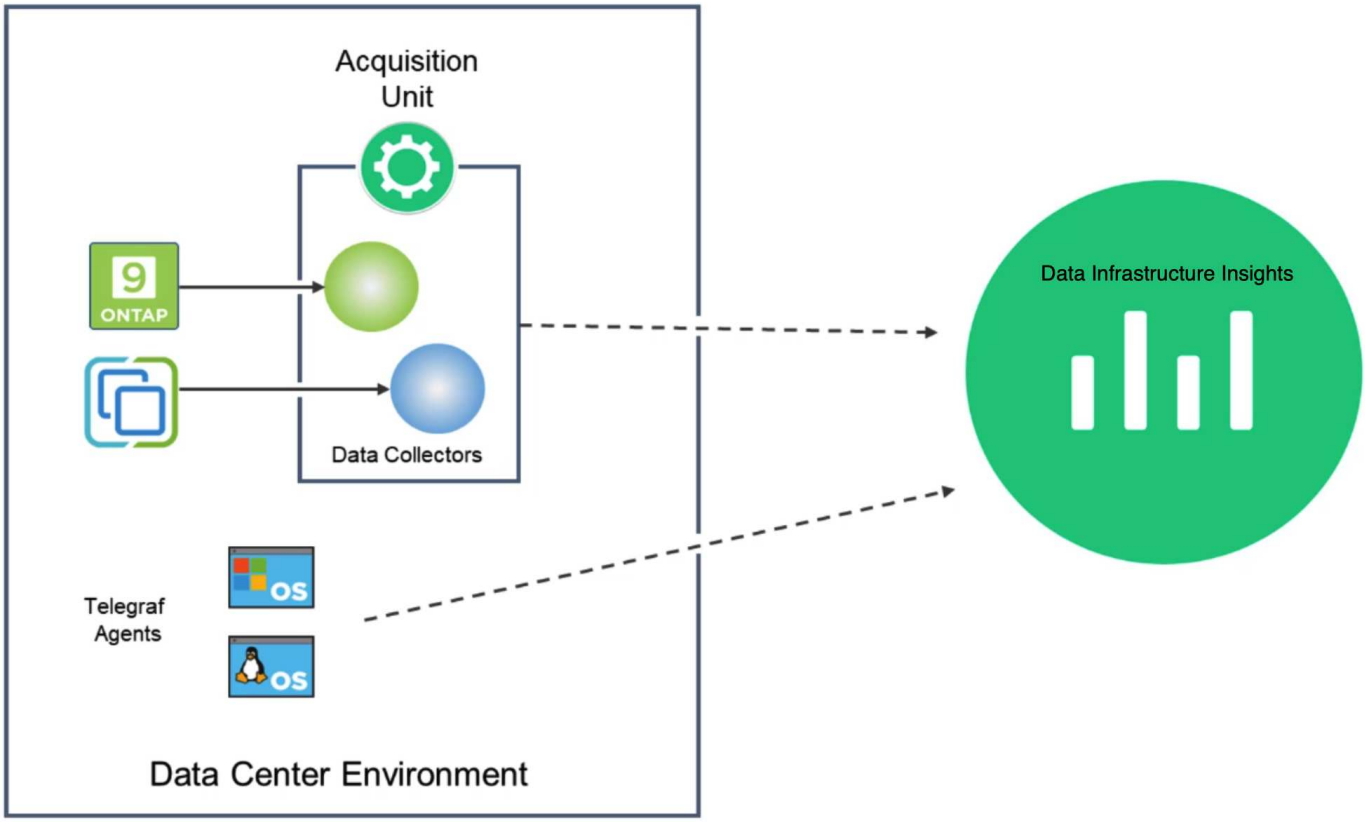
Data Infrastructure Insights 사용하여 온프레미스 스토리지 모니터링

NetApp Data Infrastructure Insights (이전 명칭 Cloud Insights)는 온프레미스와 클라우드 모두에서 IT 인프라의 성능, 상태 및 비용을 모니터링하고 분석하도록 설계된 클라우드 기반 플랫폼입니다. 데이터 수집기를 배포하고, 성과 지표를 분석하고, 대시보드를 사용하여 문제를 식별하고 리소스를 최적화하는 방법을 알아보세요.

Data Infrastructure Insights 통한 온프레미스 스토리지 모니터링

Data Infrastructure Insights VMware vSphere 및 NetApp ONTAP 스토리지 시스템과 같은 자산에 대한 데이터 수집기를 설정한 Acquisition Unit 소프트웨어를 통해 운영됩니다. 이러한 수집기는 데이터를 수집하여 Data Infrastructure Insights 로 전송합니다. 그런 다음 플랫폼은 다양한 대시보드, 위젯, 메트릭 쿼리를 활용하여 사용자가 해석할 수 있는 통찰력 있는 분석으로 데이터를 구성합니다.

Data Infrastructure Insights 아키텍처 다이어그램:



솔루션 배포 개요

이 솔루션은 Data Infrastructure Insights 사용하여 온프레미스 VMware vSphere 및 ONTAP 스토리지 시스템을 모니터링하는 방법을 소개합니다.

이 목록은 이 솔루션에서 다루는 상위 수준의 단계를 제공합니다.

1. vSphere 클러스터에 대한 데이터 수집기를 구성합니다.
2. ONTAP 스토리지 시스템에 대한 데이터 수집기를 구성합니다.
3. 주석 규칙을 사용하여 자산에 태그를 지정합니다.
4. 자산을 탐색하고 상관관계를 분석합니다.
5. Top VM Latency 대시보드를 사용하여 노이즈가 많은 이웃을 분리합니다.
6. VM의 크기를 적절하게 조정할 수 있는 기회를 파악합니다.
7. 쿼리를 사용하여 메트릭을 분리하고 정렬합니다.

필수 조건

이 솔루션은 다음 구성 요소를 사용합니다.

1. ONTAP 9.13이 탑재된 NetApp All-Flash SAN 어레이 A400.
2. VMware vSphere 8.0 클러스터.
3. NetApp BlueXP 계정.
4. 로컬 VM에 설치되고 자산에 네트워크로 연결되어 데이터 수집이 가능한 NetApp Data Infrastructure Insights Acquisition Unit 소프트웨어입니다.

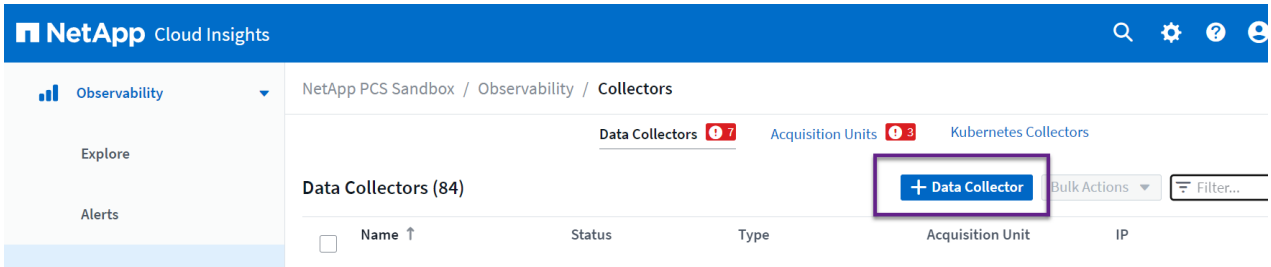
솔루션 배포

데이터 수집기 구성

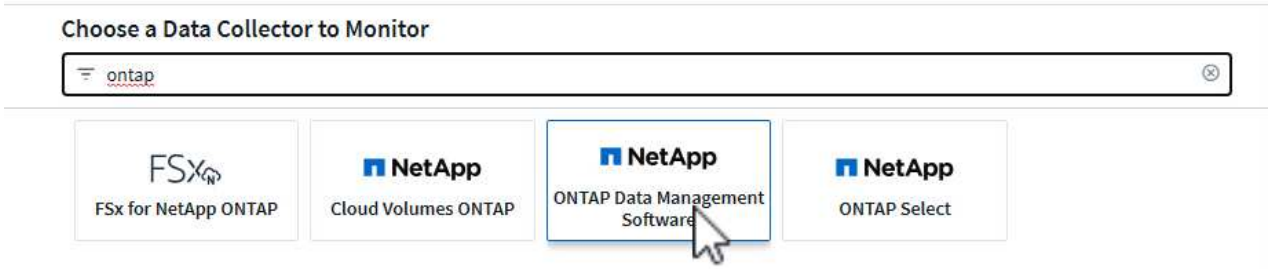
VMware vSphere 및 ONTAP 스토리지 시스템에 대한 데이터 수집기를 구성하려면 다음 단계를 완료하세요.

ONTAP 스토리지 시스템에 대한 데이터 수집기 추가

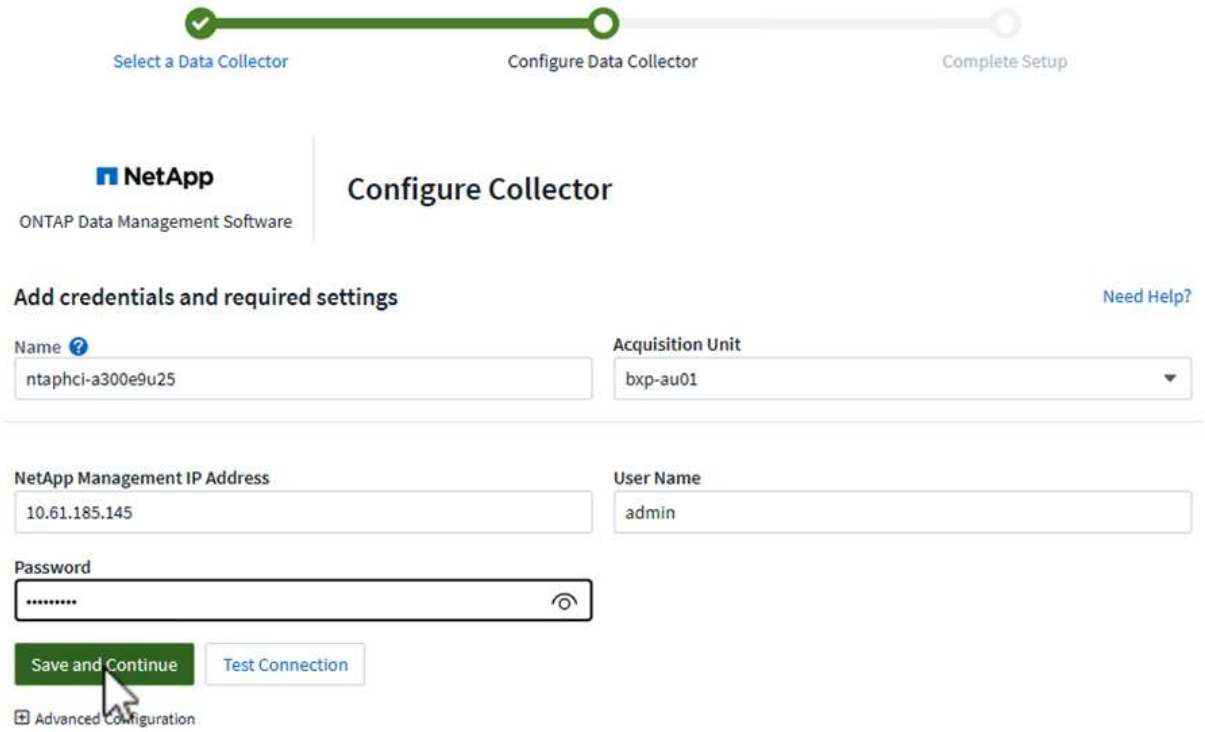
1. Data Infrastructure Insights 에 로그인한 후 *관찰성 > 수집기 > 데이터 수집기*로 이동하고 버튼을 눌러 새 데이터 수집기를 설치합니다.



2. 여기에서 * ONTAP*을 검색하고 * ONTAP 데이터 관리 소프트웨어*를 클릭하세요.

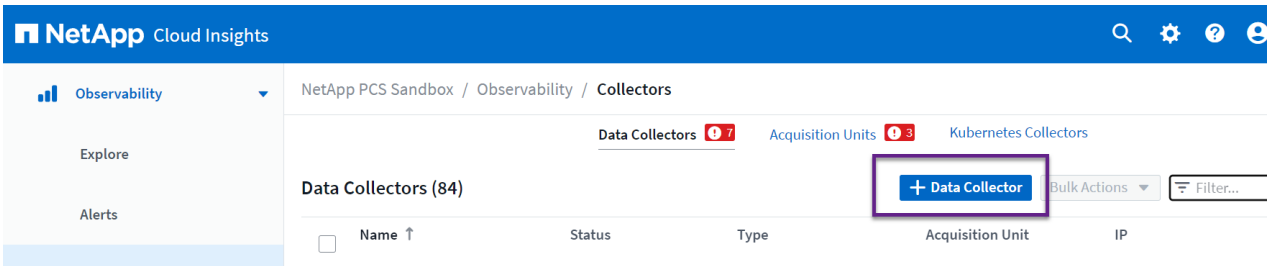


3. 수집기 구성 페이지에서 수집기의 이름을 입력하고, 올바른 *수집 단위*를 지정하고 ONTAP 스토리지 시스템의 자격 증명을 제공합니다. *저장 및 계속*을 클릭한 다음 페이지 하단의 *설정 완료*를 클릭하여 구성을 완료합니다.

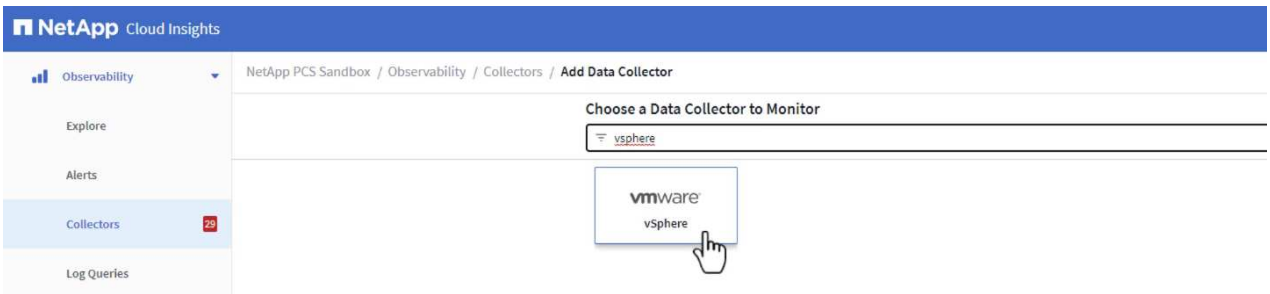


VMware vSphere 클러스터에 대한 데이터 수집기 추가

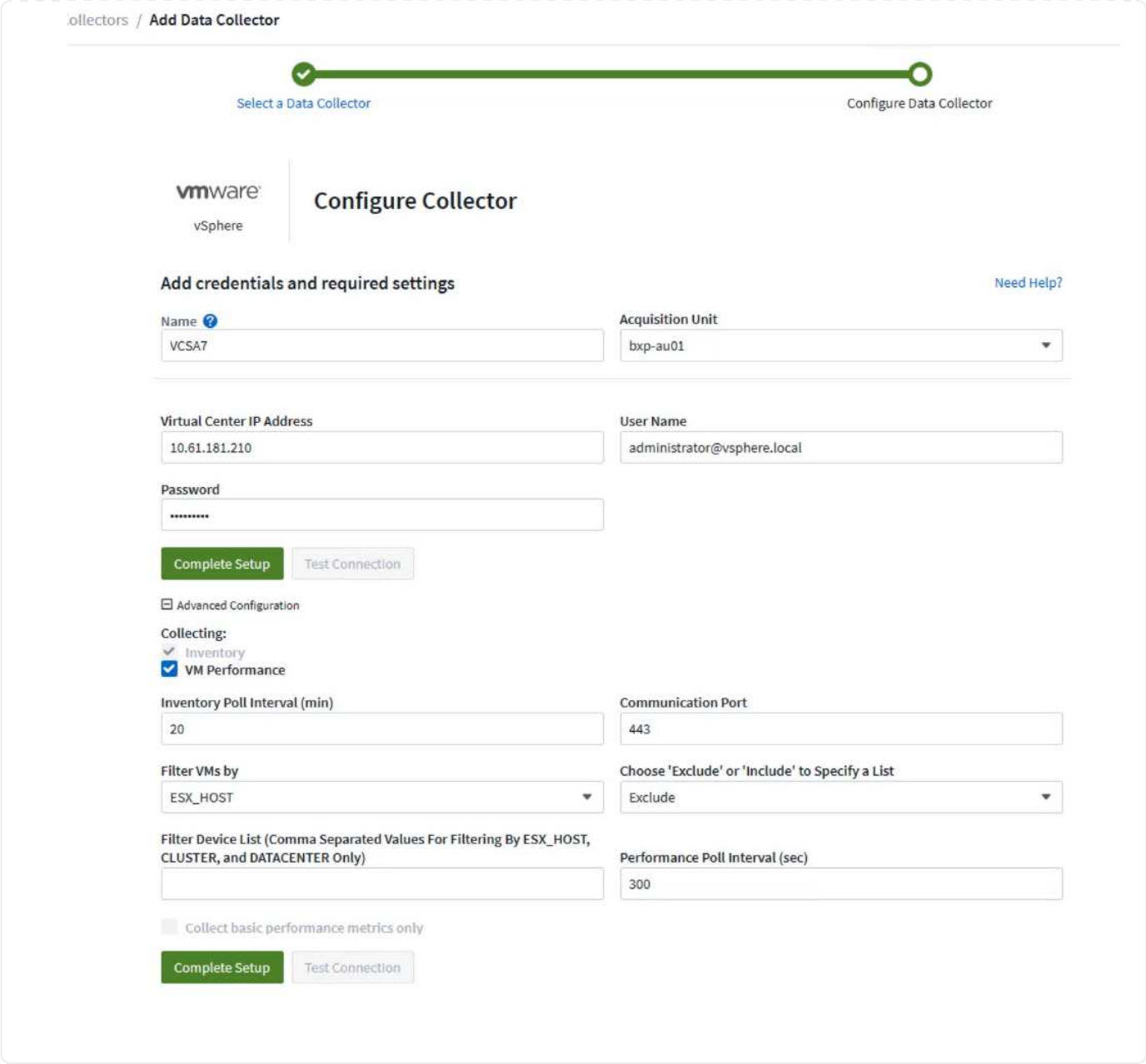
1. 다시 한번, *관찰성 > 수집기 > 데이터 수집기*로 이동한 후 버튼을 눌러 새 데이터 수집기를 설치합니다.



2. 여기에서 *vSphere*를 검색하고 *VMware vSphere*를 클릭합니다.



3. 수집기 구성 페이지에서 수집기의 이름을 입력하고, 올바른 *수집 단위*를 지정하고 vCenter Server에 대한 자격 증명을 제공합니다. *저장 및 계속*을 클릭한 다음 페이지 하단의 *설정 완료*를 클릭하여 구성을 완료합니다.



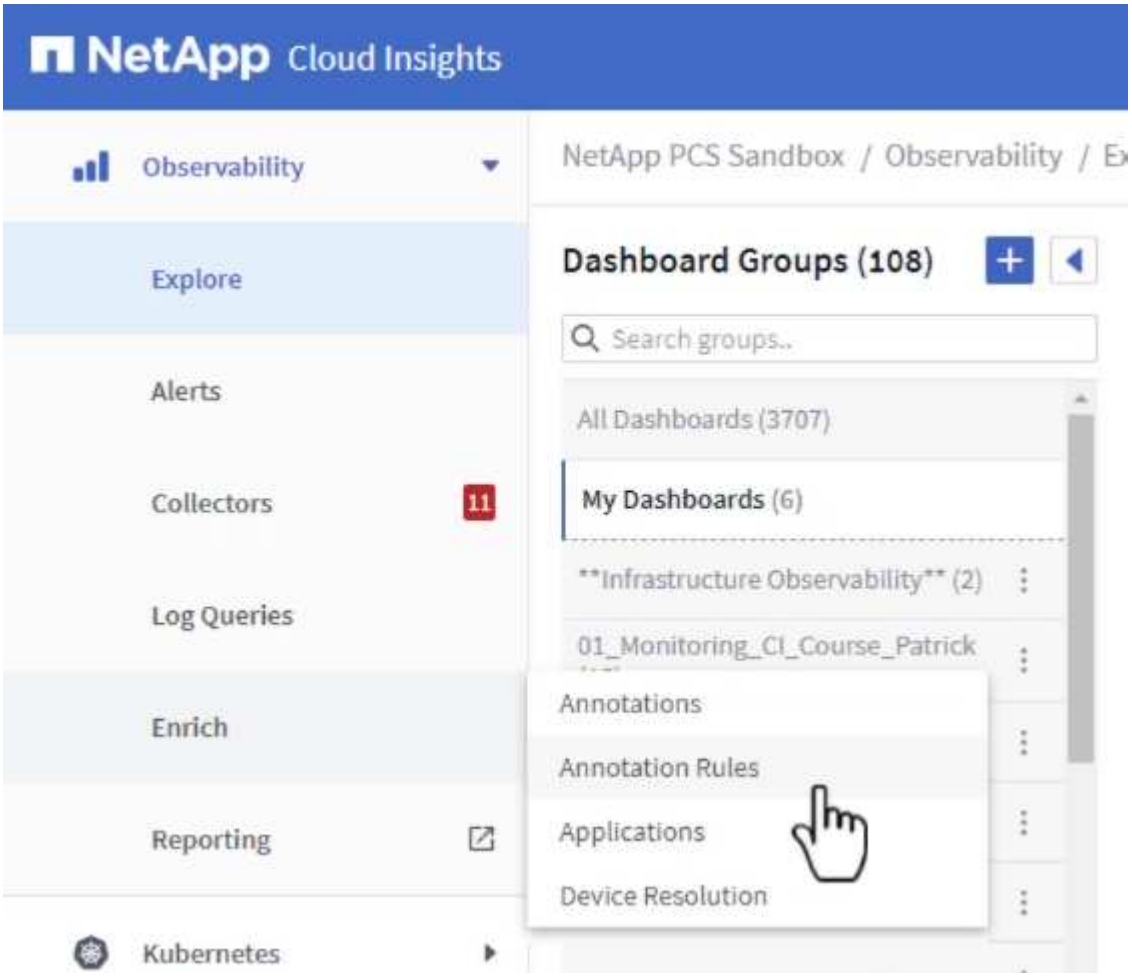
자산에 주석 추가

주석은 자산에 태그를 지정하여 Cloud Insights 에서 제공하는 다양한 뷰와 메트릭 쿼리에서 필터링하고 식별할 수 있는 유용한 방법입니다.

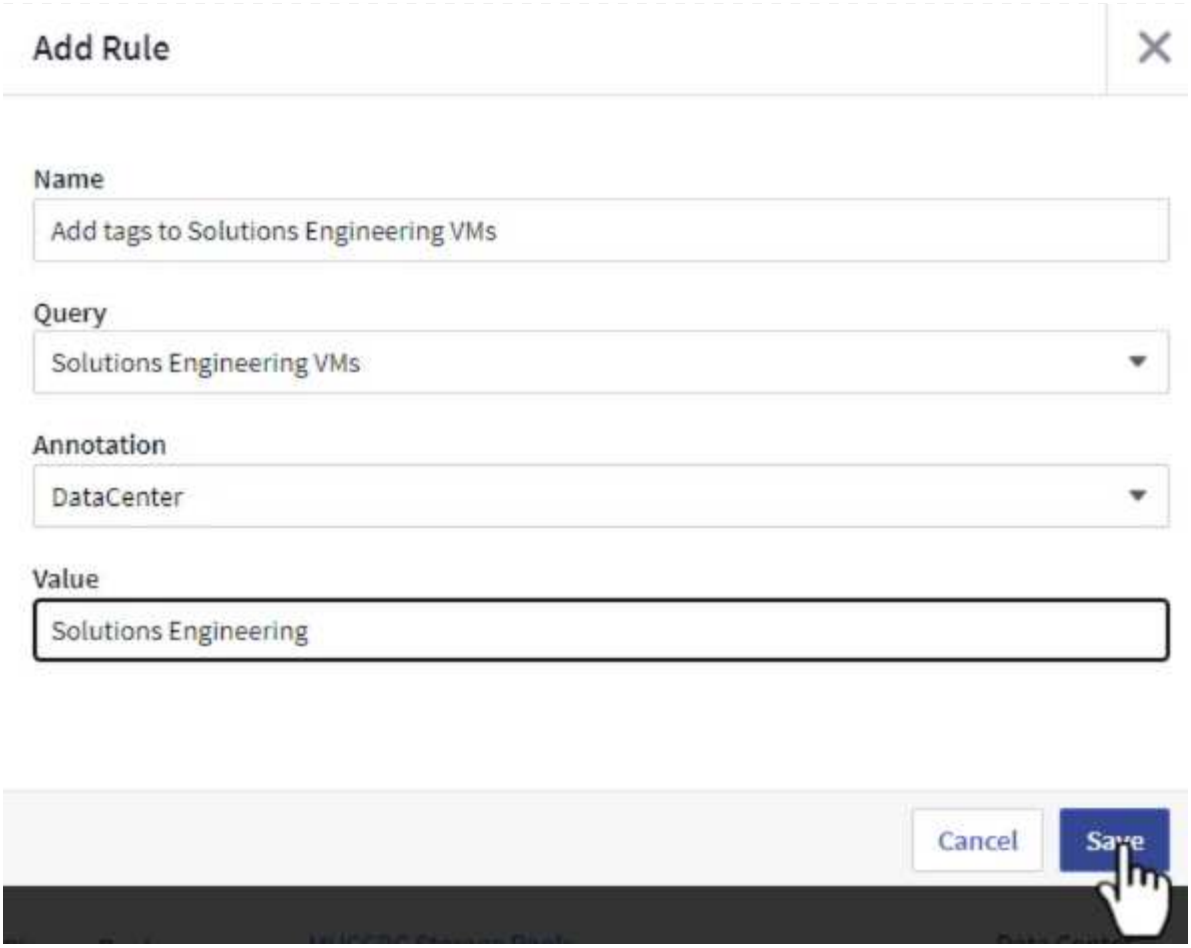
이 섹션에서는 *데이터 센터*로 필터링하기 위해 가상 머신 자산에 주석을 추가합니다.

주석 규칙을 사용하여 자산에 태그 지정

1. 왼쪽 메뉴에서 관찰성 > 강화 > 주석 규칙*으로 이동한 다음 오른쪽 상단에 있는 *+ 규칙 버튼을 클릭하여 새 규칙을 추가합니다.



2. 규칙 추가 대화 상자에서 규칙의 이름을 입력하고, 규칙이 적용될 쿼리, 영향을 받는 주석 필드, 채워질 값을 찾습니다.



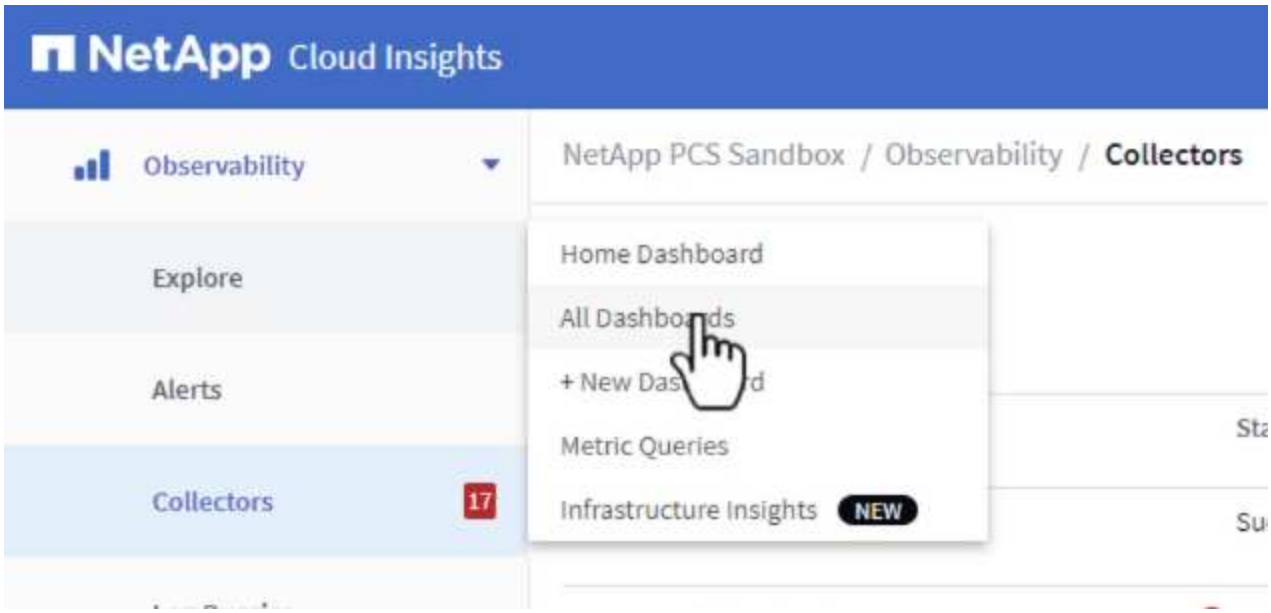
3. 마지막으로, 주석 규칙 페이지의 오른쪽 상단 모서리에 있는 *모든 규칙 실행*을 클릭하여 규칙을 실행하고 자산에 주석을 적용합니다.

자산 탐색 및 상관관계 분석

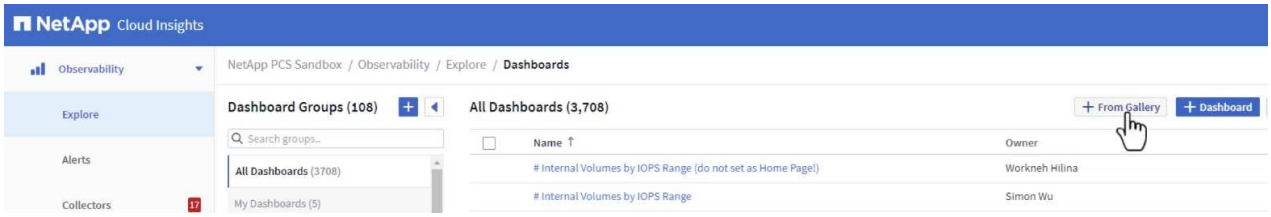
Cloud Insights 스토리지 시스템과 vSphere 클러스터에서 함께 실행되는 자산에 대한 논리적인 결론을 도출합니다.

이 섹션에서는 대시보드를 사용하여 자산을 상호 연관시키는 방법을 설명합니다.

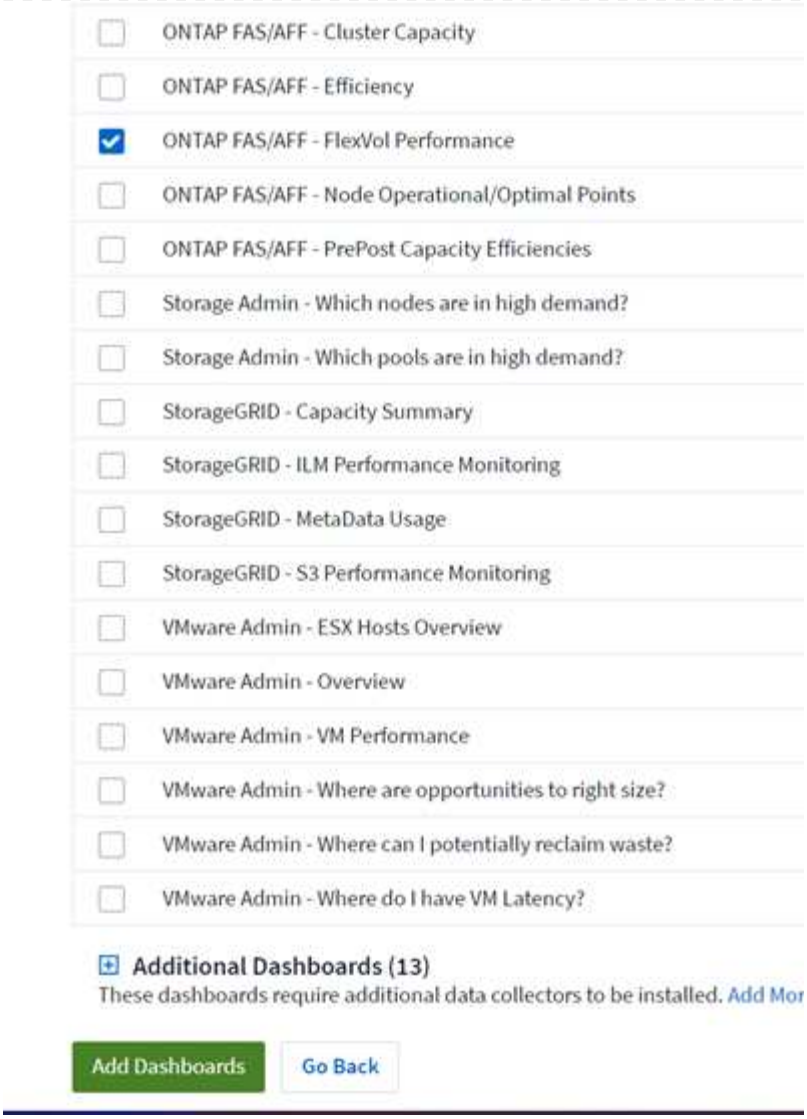
1. 왼쪽 메뉴에서 *관찰성 > 탐색 > 모든 대시보드*로 이동합니다.



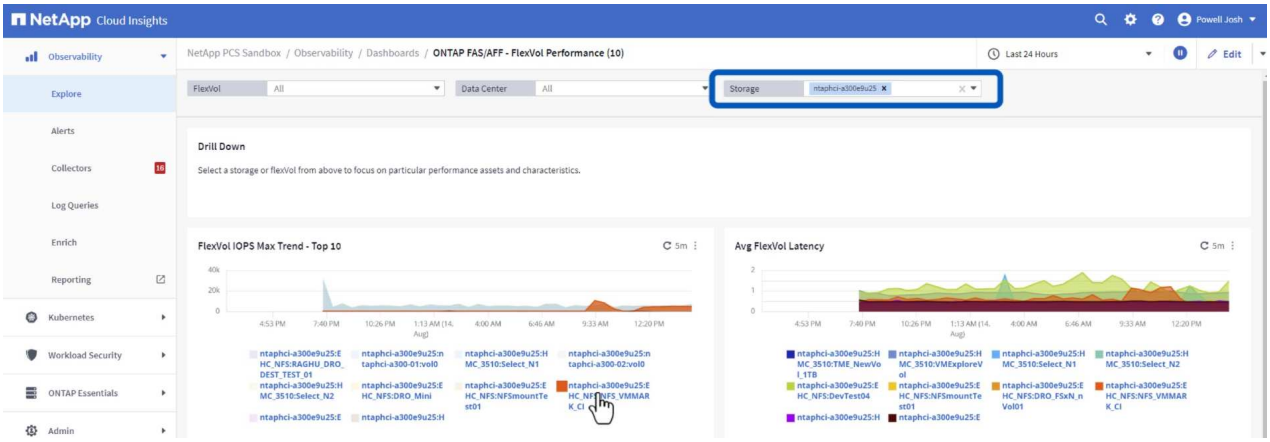
2. **+** 갤러리에서 버튼을 클릭하면 가져올 수 있는 기성 대시보드 목록이 표시됩니다.



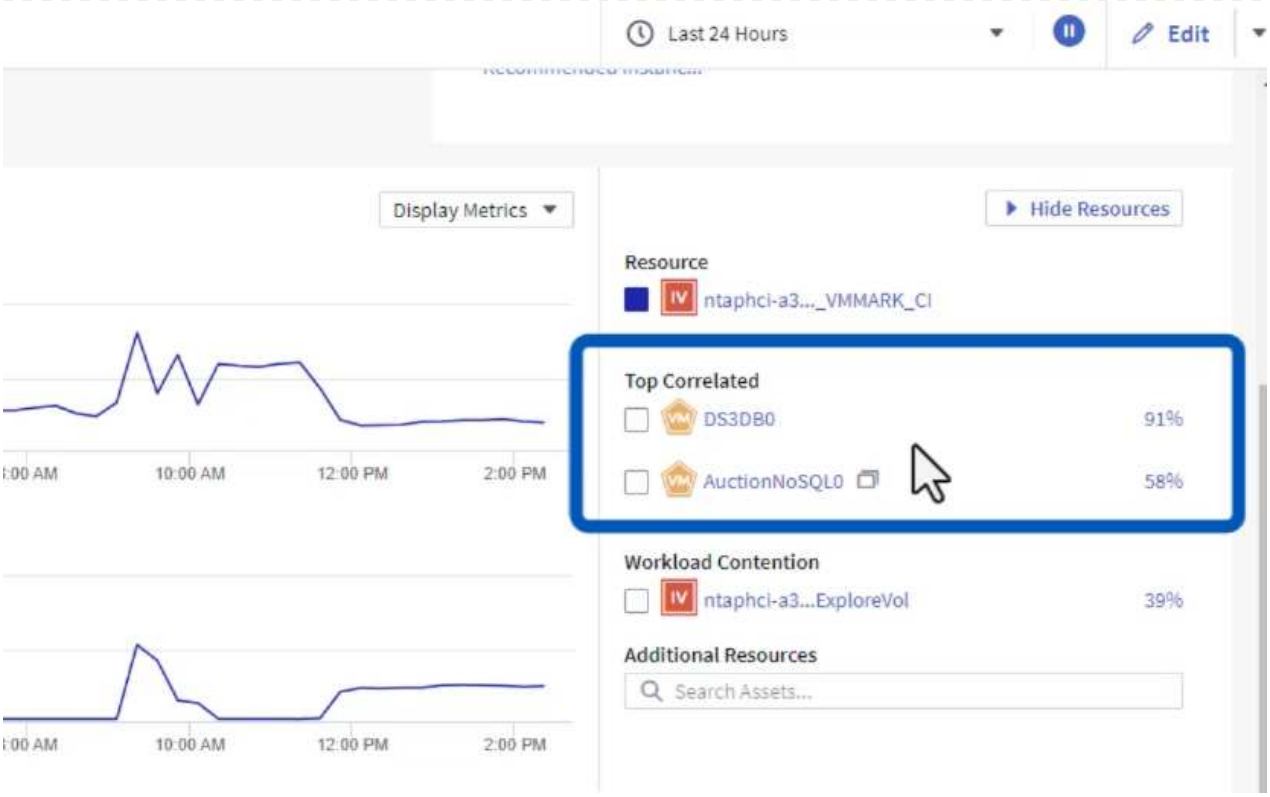
3. 목록에서 FlexVol 성능에 대한 대시보드를 선택하고 페이지 하단에 있는 대시보드 추가 버튼을 클릭합니다.



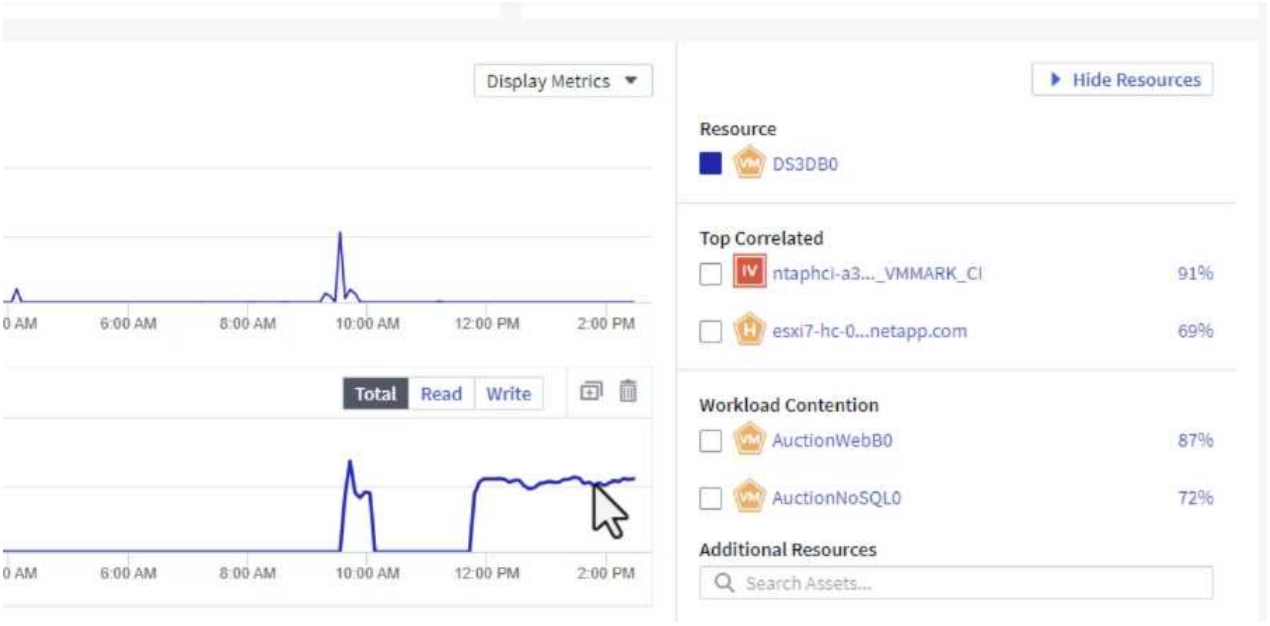
4. 가져온 후 대시보드를 엽니다. 여기에서 자세한 성능 데이터가 포함된 다양한 위젯을 볼 수 있습니다. 필터를 추가하여 단일 스토리지 시스템을 보고, 스토리지 볼륨을 선택하여 세부 정보를 자세히 살펴보세요.



5. 이 보기에서는 이 스토리지 볼륨과 관련된 다양한 메트릭과 볼륨에서 실행 중인 가장 많이 활용되고 상관관계가 있는 가상 머신을 볼 수 있습니다.



6. 가장 활용도가 높은 VM을 클릭하면 해당 VM에 대한 측정항목이 자세히 표시되어 잠재적인 문제를 확인할 수 있습니다.



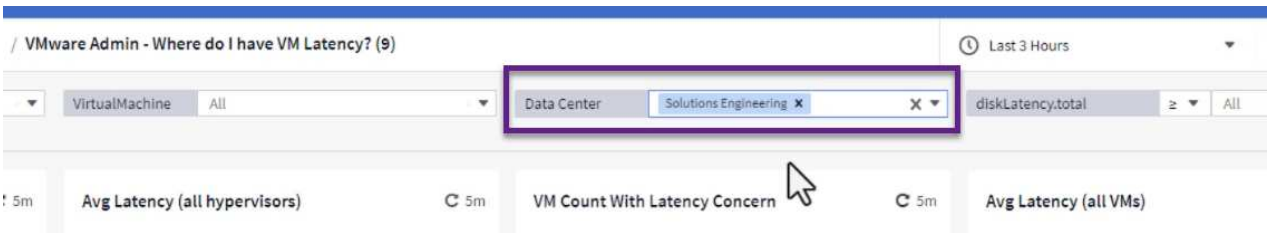
Cloud Insights 사용하여 소음이 많은 이웃을 식별하세요

Cloud Insights 동일한 스토리지 볼륨에서 실행되는 다른 VM에 부정적인 영향을 미치는 피어 VM을 쉽게 분리할 수 있는 대시보드 기능을 제공합니다.

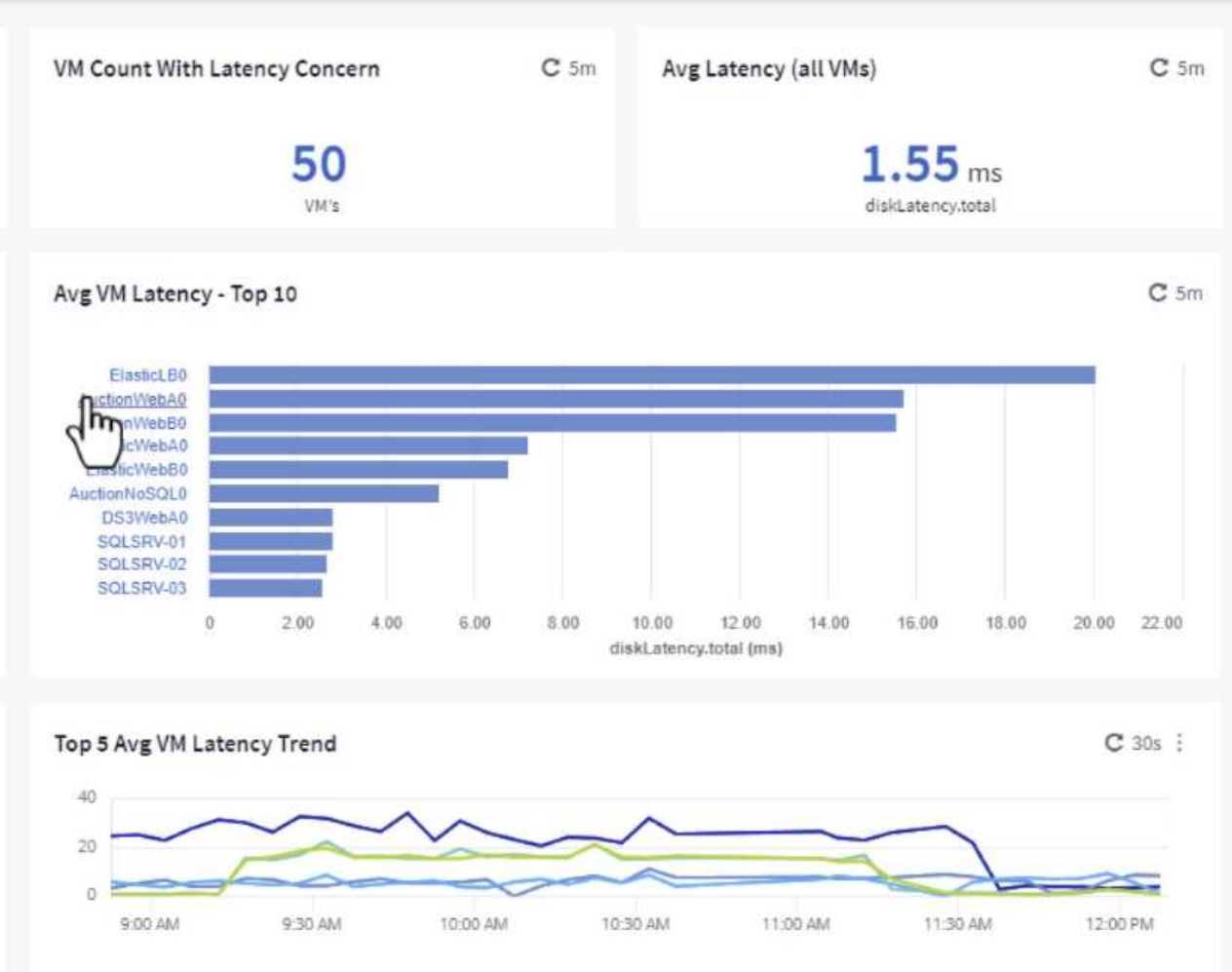
상위 **VM** 대기 시간 대시보드를 사용하여 노이즈가 많은 이웃을 분리합니다.

1. 이 예에서는 *갤러리*에서 *VMware 관리자 - VM 지연 시간은 어디에 있습니까?*라는 대시보드에 액세스합니다.

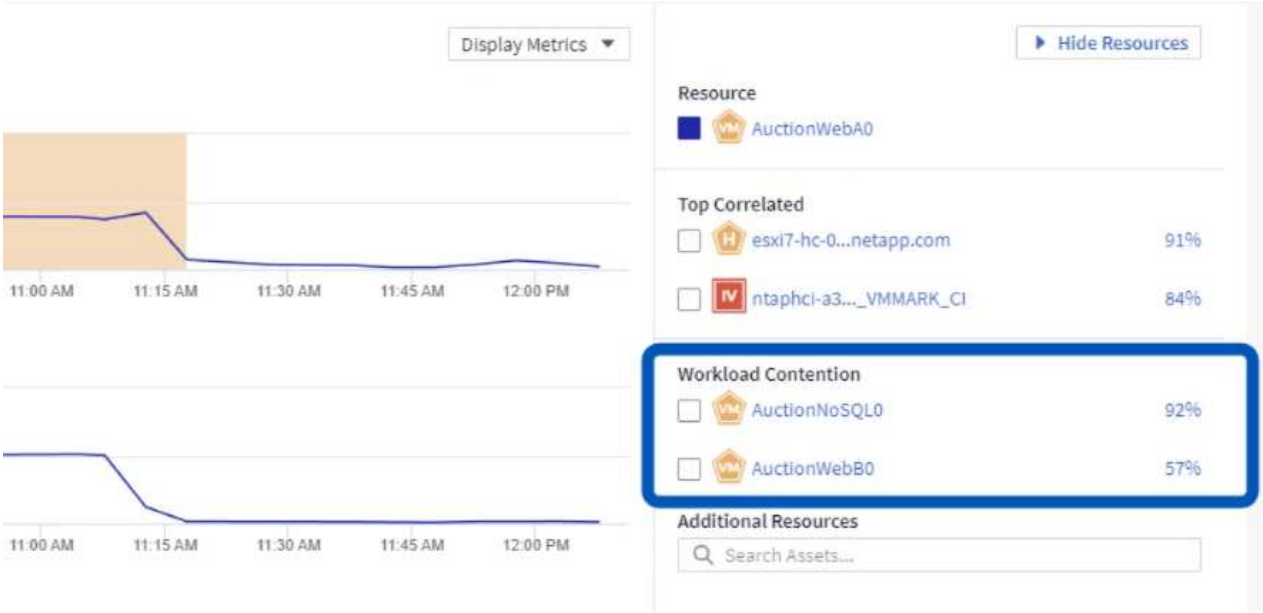
2. 다음으로, 이전 단계에서 만든 데이터 센터 주석으로 필터링하여 자산의 하위 집합을 확인합니다.



3. 이 대시보드는 평균 지연 시간을 기준으로 상위 10개 VM 목록을 보여줍니다. 여기에서 해당 VM을 클릭하여 세부 정보를 확인하세요.



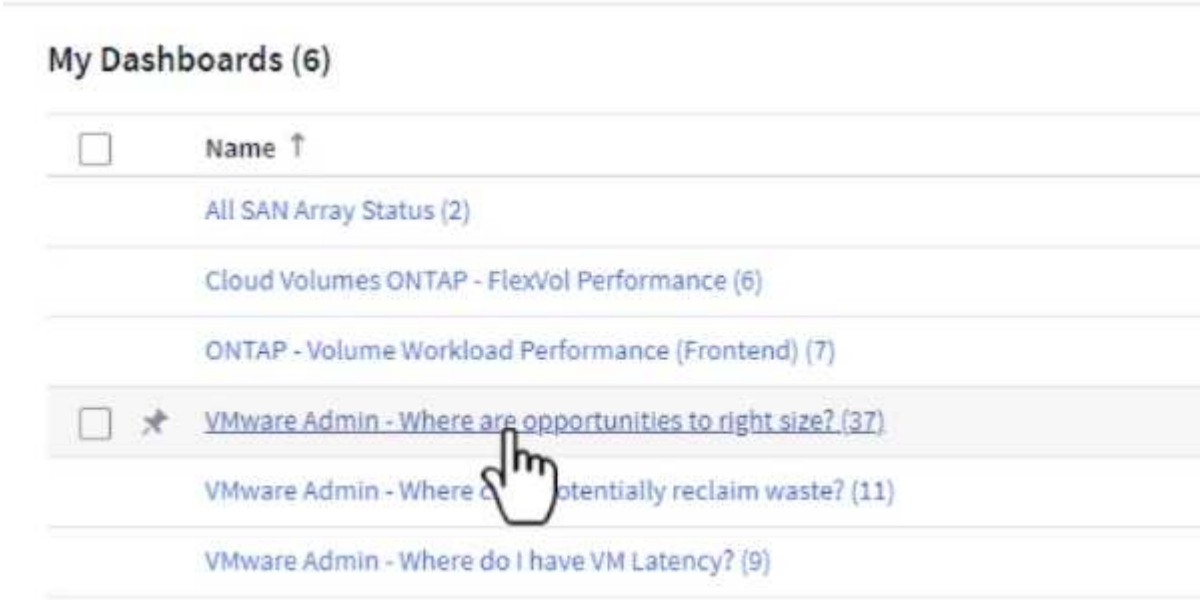
4. 잠재적으로 작업 부하 경합을 일으킬 수 있는 VM이 나열되어 있으며 사용 가능합니다. 이러한 VM 성능 측정 항목을 자세히 살펴보고 잠재적인 문제를 조사하세요.



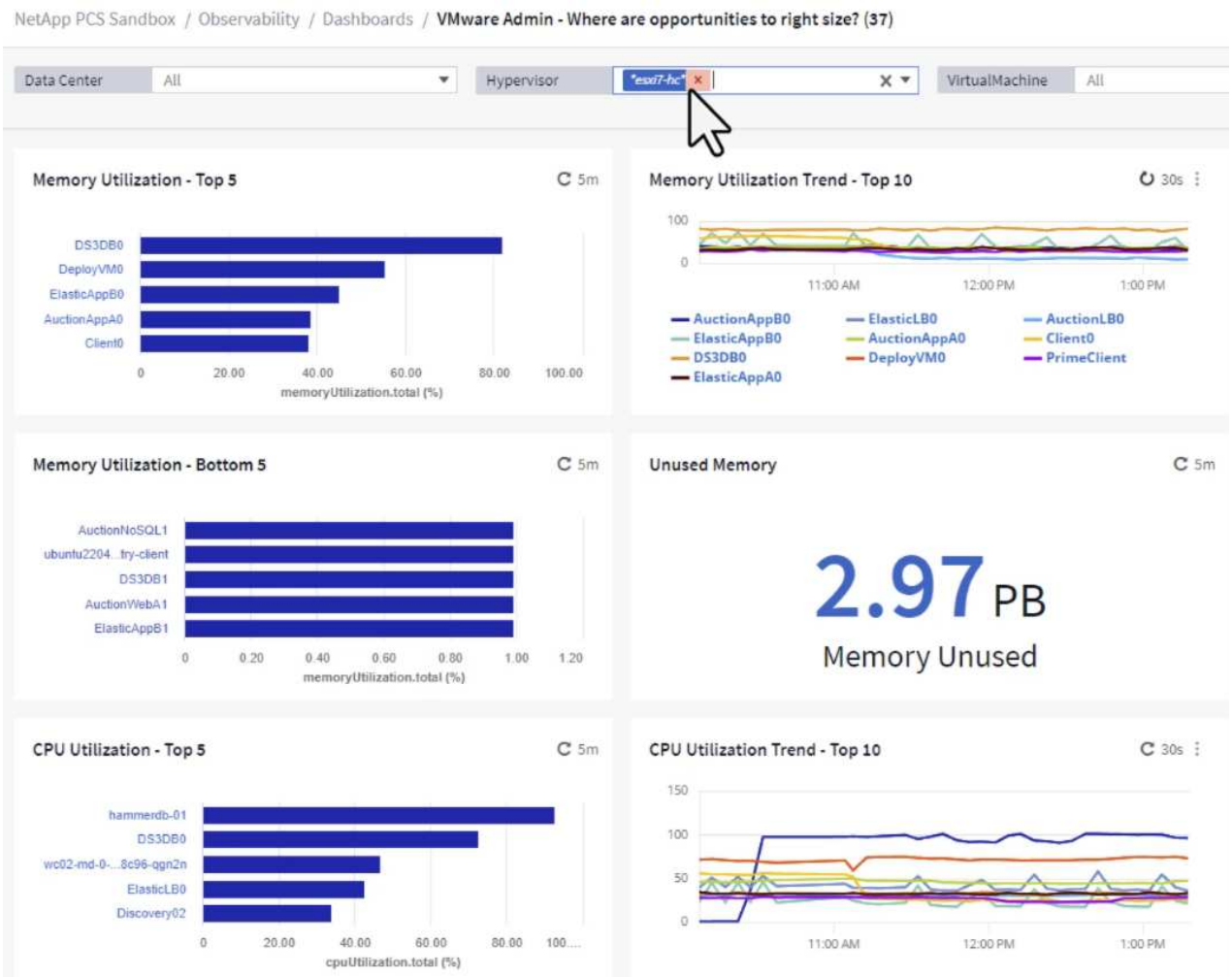
Cloud Insights 에서 과도하게 활용되거나 활용도가 낮은 리소스를 확인하세요**.**

VM 리소스를 실제 작업 부하 요구 사항에 맞게 조정하면 리소스 활용도를 최적화하여 인프라와 클라우드 서비스 비용을 절감할 수 있습니다. Cloud Insights 의 데이터는 사용자 정의가 가능하여 활용도가 과도하거나 낮은 VM을 쉽게 표시할 수 있습니다.

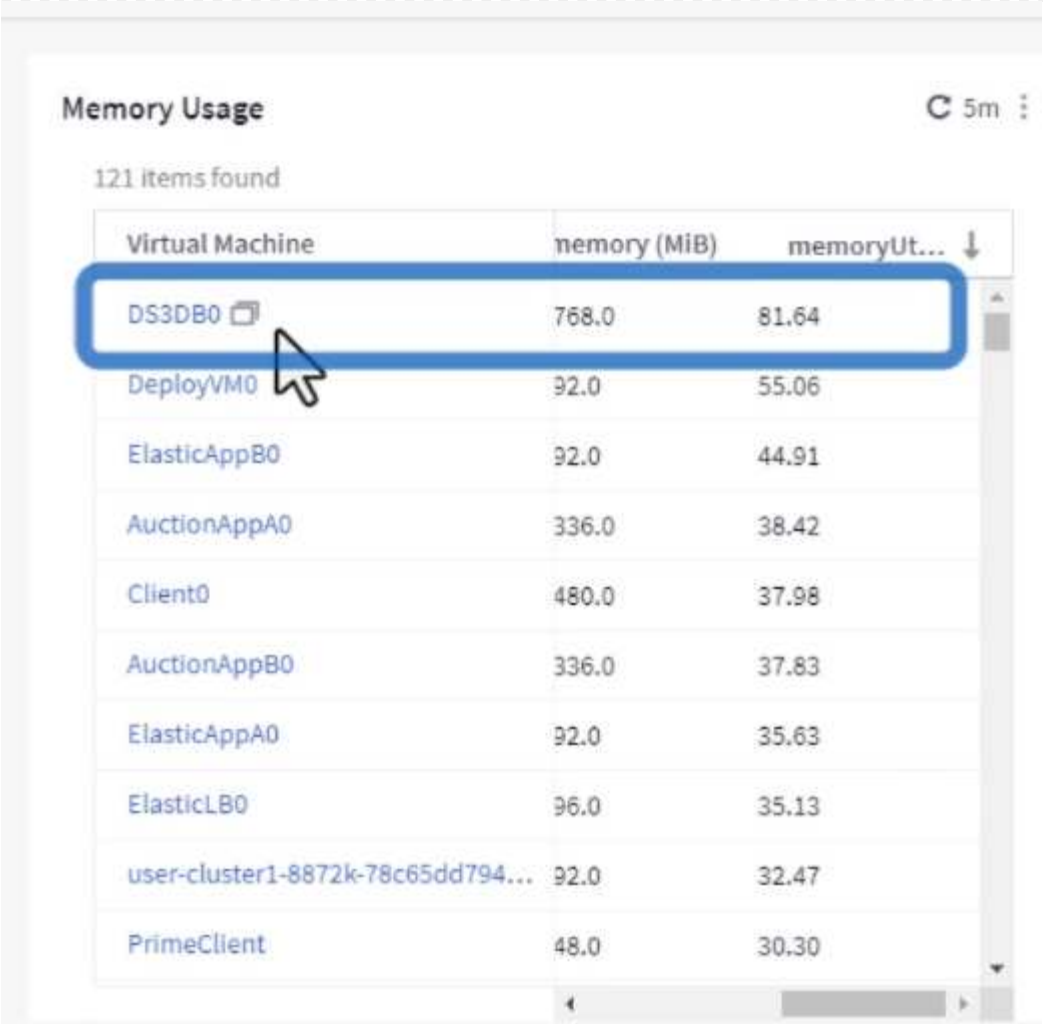
1. 이 예에서는 *갤러리*에서 *VMware Admin - 적절한 규모로 기회를 찾을 수 있는 곳은 어디인가요?*라는 대시보드에 액세스합니다.



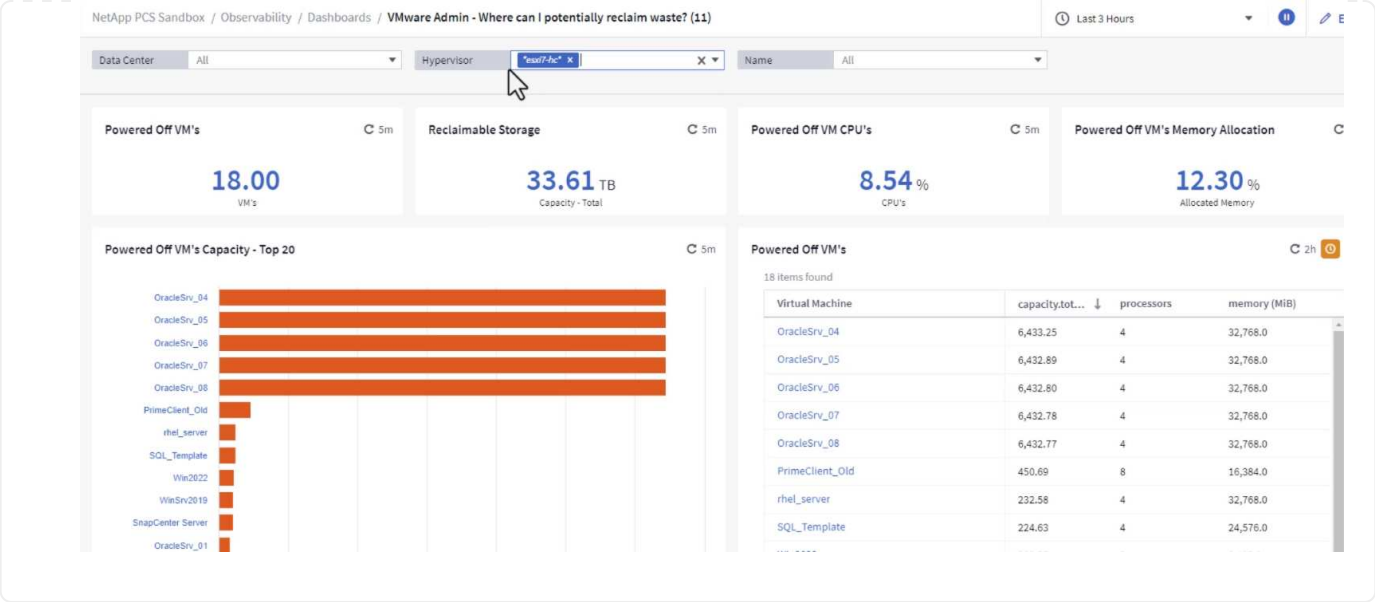
2. 먼저 클러스터의 모든 ESXi 호스트를 필터링합니다. 그러면 메모리와 CPU 사용률을 기준으로 상위 및 하위 VM의 순위를 볼 수 있습니다.



3. 표를 사용하면 정렬이 가능하며, 선택한 데이터 열에 따라 더 자세한 정보를 제공할 수 있습니다.



4. *VMware 관리자 - 낭비를 잠재적으로 어디에서 회수할 수 있나요?*라는 또 다른 대시보드는 전원이 꺼진 VM을 용량 사용량별로 정렬하여 보여줍니다.

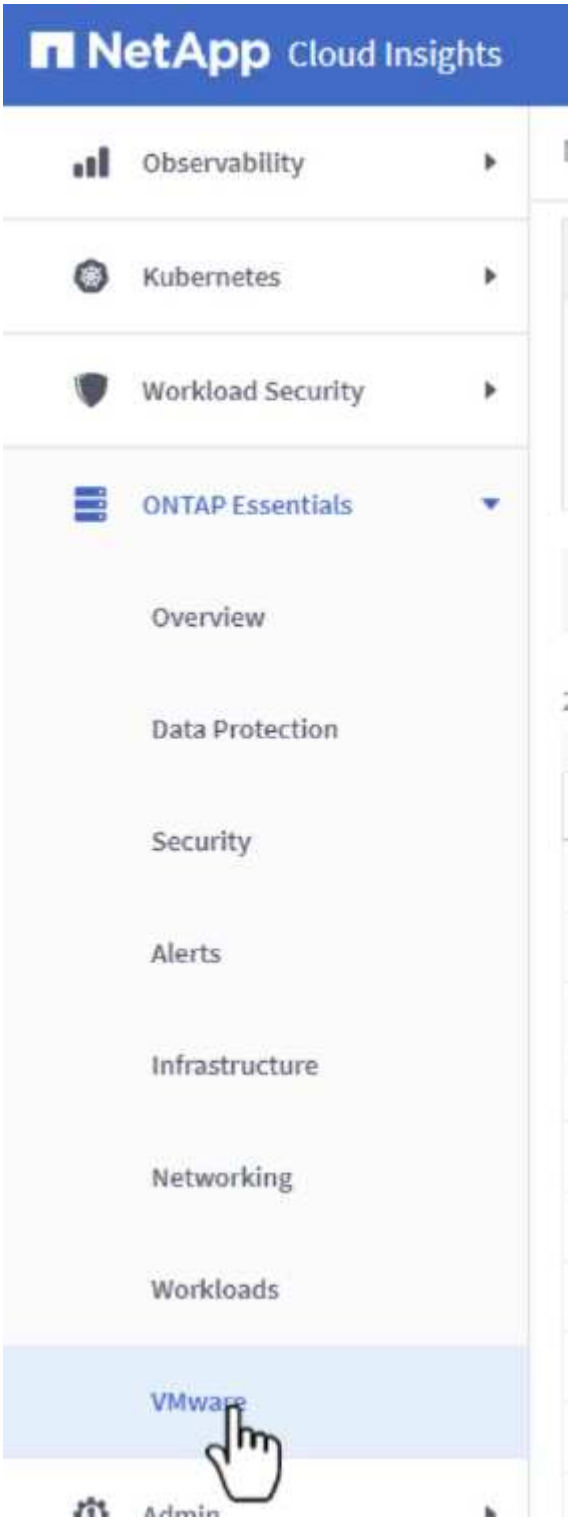


쿼리를 사용하여 메트릭을 분리하고 정렬합니다.

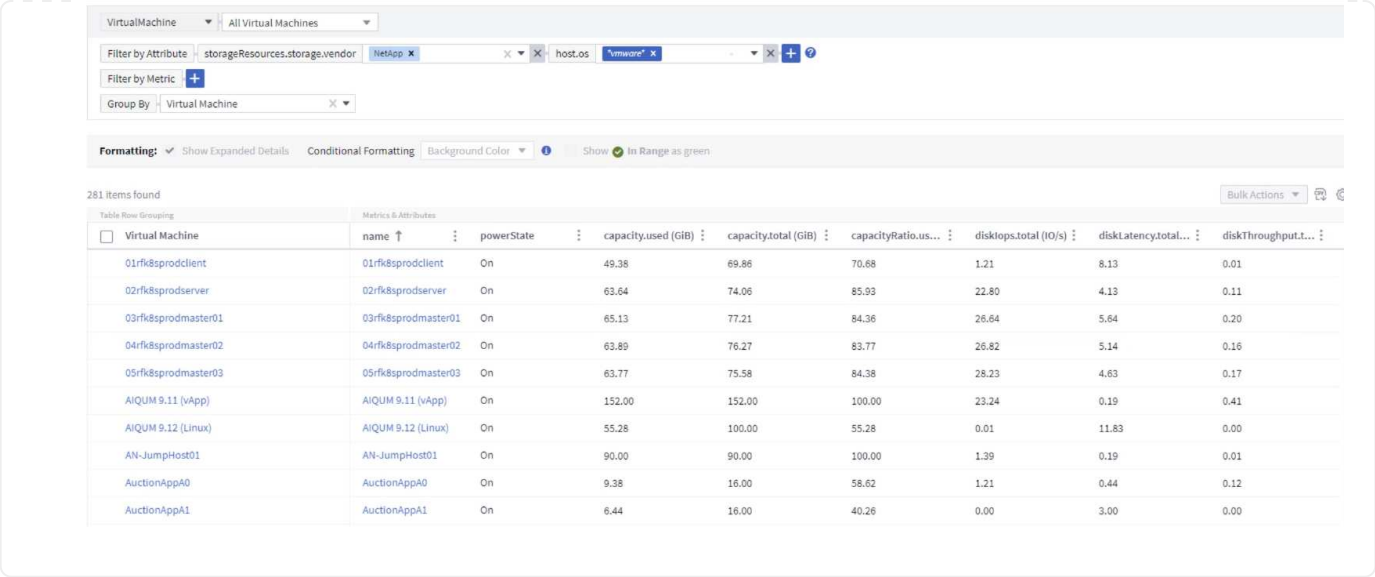
Cloud Insights 수집하는 데이터의 양은 매우 포괄적입니다. 메트릭 쿼리는 유용한 방식으로 대량의 데이터를 정렬하고 구성하는 강력한 방법을 제공합니다.

ONTAP Essentials에서 자세한 **VMware** 쿼리 보기

1. 포괄적인 VMware 메트릭 쿼리에 액세스하려면 * ONTAP Essentials > VMware*로 이동하세요.



2. 이 보기에서는 상단에 데이터를 필터링하고 그룹화하기 위한 여러 옵션이 표시됩니다. 모든 데이터 열은 사용자 정의가 가능하며, 추가 열도 쉽게 추가할 수 있습니다.



결론

이 솔루션은 NetApp Cloud Insights 를 시작하는 방법을 배우고 이 관찰 솔루션이 제공할 수 있는 강력한 기능 중 일부를 보여주기 위한 입문서로 설계되었습니다. 이 제품에는 수백 개의 대시보드와 지표 쿼리가 내장되어 있어 즉시 쉽게 작업을 시작할 수 있습니다. Cloud Insights 의 전체 버전은 30일 체험판으로 제공되며, NetApp 고객에게는 기본 버전이 무료로 제공됩니다.

추가 정보

이 솔루션에 제시된 기술에 대해 자세히 알아보려면 다음 추가 정보를 참조하세요.

- "NetApp BlueXP 및 Data Infrastructure Insights 랜딩 페이지"
- "NetApp Data Infrastructure Insights 설명서"

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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