FlexPod 솔루션

FlexPod

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/flexpod/index.html on November 04, 2025.
Always check docs.netapp.com for the latest.

목차

FlexPod 솔루션 1
FlexPod 정의 2
FlexPod 익스프레스 기술 사양 2
TR-4293: FlexPod 익스프레스 기술 사양 2
FlexPod 플랫폼 2
FlexPod 규칙 2
지원되는 구성과 검증된 FlexPod 구성 비교 2
스토리지 소프트웨어 3
최소 하드웨어 요구 사항 3
최소 소프트웨어 요구 사항 4
연결 요구 사항 4
기타 요구 사항 5
레거시 장비 6
추가 정보 7
FlexPod 데이터 센터 기술 사양 7
TR-4036: FlexPod 데이터 센터 기술 사양 7
FlexPod 플랫폼 8
FlexPod 규칙 8
NetApp ONTAP를 참조하십시오 8
Cisco Nexus 스위칭 운영 모드 8
최소 하드웨어 요구 사항 9
최소 소프트웨어 요구 사항 10
연결 요구 사항 10
기타 요구 사항 11
선택적 기능 11
Cisco 구성 요소 25
NetApp 구성 요소 30
전원 및 케이블 연결 요구 사항 31
기술 사양 및 참조 자료 33
레거시 장비 40
추가 정보를 찾을 수 있는 위치 40
FlexPod 데이터 센터 42
NetApp SnapMirror 비즈니스 연속성 및 ONTAP 9.10이 설치된 FlexPod 데이터 센터 42
TR-4920: NetApp SnapMirror 비즈니스 연속성 및 ONTAP 9.10을 지원하는 FlexPod 데이터 센터 42
소개 42
FlexPod SM-BC 솔루션 44
솔루션 검증 53
결론 94
추가 정보 및 버전 기록을 찾을 수 있는 위치 95

VMware vSphere 7.0 및 NetApp ONTAP 9.7을 사용하는 FlexPod 데이터 센터 - 구축 98
FlexPod 데이터 센터 및 Cisco Intersight, NetApp ONTAP 9.7 - 설계 99
FlexPod 데이터 센터 및 Cisco Intersight, NetApp ONTAP 9.7 - 배포 99
FlexPod 데이터 센터 및 Cisco Intersight, NetApp ONTAP 9.7 - 설계 99
VMware vSphere 6.7 U2, Cisco UCS fouth-generation Fabric 및 NetApp ONTAP 9.6이 지원되는 FlexPod 데이터 센터 99
VMware vSphere 6.7 U1, Cisco UCS 4세대 패브릭 및 NetApp AFF A-Series를 지원하는 FlexPod 데이터 센터 - 설계 100
VMware vSphere 6.7 U1, Cisco UCS 4세대 패브릭 및 NetApp AFF A-Series를 지원하는 FlexPod 데이터 센터 100
FlexPod 데이터 센터 및 Cisco ACI 멀티 포드, NetApp MetroCluster IP, VMware vSphere 6.7-Design 101
NetApp MetroCluster IP 및 VMware vSphere 6.7-Deployment가 포함된 Cisco ACI 멀티 포드를 지원하는 FlexPod 데이터 센터 101
하이브리드 클라우드 103
FlexPod 하이브리드 클라우드 및 Cloud Volumes ONTAP for Epic 103
TR-4960: FlexPod 하이브리드 클라우드 with Cloud Volumes ONTAP for Epic 103
솔루션 구성 요소 105
설치 및 구성 109
SAN 구성 113
솔루션 검증 119
결론 127
추가 정보를 찾을 수 있는 위치 127
NetApp Cloud Volumes ONTAP 및 Cisco Intersight가 지원되는 Google 클라우드 플랫폼용 FlexPod 하이브리드 클라우드 128
TR-4939: NetApp Cloud Volumes ONTAP 및 Cisco Intersight가 지원되는 Google 클라우드 플랫폼용 FlexPod 하이브리드 클라우드 128
솔루션 구성 요소 131
설치 및 구성 135
솔루션 검증 200
결론 207
NetApp Astra 및 Cisco Intersight, Red Hat OpenShift를 포함하는 FlexPod 하이브리드 클라우드 210
TR-4936: NetApp Astra 및 Cisco Intersight for Red Hat OpenShift를 포함하는 FlexPod 하이브리드 클라우드 210
솔루션 구성 요소 213
설치 및 구성 220
솔루션 검증 242
결론 263
FlexPod용 NetApp Cloud Insights 265
TR-4868: FlexPod용 NetApp Cloud Insights 265
사용 사례 265
있습니다 266
설계 고려 사항 268

FlexPod for Cloud Insights 구축 . . . 268
사용 사례 . . . 280
비디오 및 데모 . . . 288
추가 정보 . . . 288
FlexPod with FabricPool - Amazon AWS S3로 비활성 데이터 계층화 . . . 289
TR-4801: FabricPool를 지원하는 FlexPod - Amazon AWS S3에 대한 비활성 데이터 계층화 . . . 289
FlexPod 개요 및 아키텍처 . . . 289
FabricPool . . . 291
FabricPool 요구 사항 . . . 295
구성 . . . 299
성능 고려 사항 . . . 310
소유 비용 . . . 310
결론 . . . 310
추가 정보를 찾을 수 있는 위치 . . . 310
Cisco CloudCenter 및 NetApp 프라이빗 스토리지를 사용하는 하이브리드 클라우드용 FlexPod 데이터 센터 - 설계 . . . 311
엔터프라이즈 데이터베이스 . . . 312
제공합니다 . . . 312
FlexPod 기반 SAP 소개 . . . 312
파이버 채널 SAN과 Cisco UCS Manager 4.0 및 NetApp ONTAP 9.7을 사용하는 SAP용 FlexPod 데이터 센터 솔루션 . . . 312
SAP 비 HANA with SQL 백서 - 설계 . . . 312
Cisco UCS 3세대 패브릭 및 NetApp AFF A-Series가 지원되는 SAP 솔루션용 FlexPod 데이터 센터 . . . 313
파이버 채널 SAN과 Cisco UCS Manager 4.0 및 NetApp ONTAP 9.7-Design을 사용하는 SAP용 FlexPod 데이터 센터 솔루션 . . . 313
Cisco ACI, Cisco UCS Manager 4.0 및 NetApp AFF A-Series-Design이 포함된 SAP용 FlexPod 데이터 센터 솔루션 . . . 313
Cisco ACI, Cisco UCS Manager 4.0 및 NetApp AFF A-Series-Deployment가 있는 SAP용 FlexPod 데이터 센터 . . . 314
Cisco UCS Manager 4.0 및 NetApp AFF A-Series-Design을 사용하는 SAP 솔루션용 FlexPod 데이터 센터 . . . 314
SLES 12 SP3 및 RHEL 7.4가 설치된 Cisco UCS M5 서버에서 Cisco ACI를 지원하는 SAP용 FlexPod Datacenter 솔루션 . . . 314
NetApp AFF A-Series 및 Cisco UCS Manager 3.2를 사용하는 IP 기반 스토리지가 있는 SAP용 FlexPod 데이터 센터 솔루션 . . . 315
파이버 채널 SAN과 Cisco UCS Manager 4.0 및 NetApp ONTAP 9.7을 사용하는 SAP용 FlexPod 데이터 센터 솔루션 . . . 315
FlexPod with SQL에 SAP 애플리케이션 서버 구축 . . . 315
Cisco ACI, Cisco UCS Manager 4.0 및 NetApp AFF A-Series가 지원되는 SAP용 FlexPod 데이터 센터 . . . 316
Cisco ACI, Cisco UCS Manager 4.0 및 NetApp AFF A-Series-Design이 포함된 SAP용 FlexPod 데이터 센터 솔루션 . . . 316
Cisco UCS 3세대 패브릭 및 NetApp AFF A-Series가 지원되는 SAP용 FlexPod 데이터 센터 솔루션 . . . 316

Cisco UCS Manager 4.0 및 NetApp AFF A-Series-Design을 사용하는 SAP용 FlexPod 데이터 센터 솔루션 317
오라클 317
Cisco UCS 및 NetApp AFF A-Series에서 Oracle RAC 데이터베이스가 지원되는 FlexPod 데이터 센터 317
Oracle Linux 기반 Oracle RAC 지원 FlexPod 데이터 센터 318
Cisco UCS 및 NetApp AFF A-Series에서 Oracle RAC 데이터베이스가 지원되는 FlexPod 데이터 센터 319
Microsoft SQL Server를 참조하십시오 319
Microsoft SQL Server 2019 및 VMware vSphere 6.7용 FlexPod 데이터 센터 319
Microsoft SQL Server 2016 및 VMware vSphere 6.5가 설치된 FlexPod Datacenter 319
VMware 및 Hyper-V에서 실행되는 Linux VM에서 Microsoft SQL Server 2017을 지원하는 FlexPod 데이터 센터 320
VMware 및 Hyper-V에서 실행되는 Linux VM에서 Microsoft SQL Server 2017을 지원하는 FlexPod 데이터 센터 320
의료 321
유전체학을 위한 FlexPod 321
TR-4911: FlexPod 유전체학 321
FlexPod에 게놈 워크로드를 구축할 경우의 이점 323
솔루션 인프라 하드웨어 및 소프트웨어 구성 요소 327
유전체학 - GATK 설정 및 실행 331
JAR 파일을 사용하여 GATK 실행을 위한 출력입니다 340
/GATK 스크립트를 사용하여 GATK 실행을 위한 출력 343
Cromwell 엔진을 사용하여 GATK 실행을 위한 출력 345
GPU 설정 349
결론 358
MEDITECH 방향 사이징 가이드용 FlexPod 360
TR-4774: MEDITECH 방향 크기 조정을 위한 FlexPod 360
MEDITECH 워크로드 개요 362
소형, 중형 및 대형 아키텍처의 기술 사양 365
추가 정보 369
감사의 말 370
MEDITECH용 FlexPod 데이터 센터 배포 가이드 370
TR-4753: MEDITECH용 FlexPod 데이터 센터 배포 가이드 370
설계 380
구축 및 구성 383
MEDITECH 모듈 및 구성 요소 396
감사의 말 398
추가 정보를 찾을 수 있는 위치 398
의료 영상용 FlexPod 399
TR-4865: 의료 영상용 FlexPod 399
있습니다 411
솔루션 인프라 하드웨어 및 소프트웨어 구성 요소 421

솔루션 사이징 422
모범 사례 424
결론 429
추가 정보 429
가상 데스크톱 인프라 431
Citrix Virtual Apps & Desktops 1912 LTSR 및 VMware vSphere 7을 지원하는 FlexPod 데이터 센터(최대 6000개 시트 431
최대 6700개 시트를 지원하는 VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 및 NetApp ONTAP 9.6을 갖춘 FlexPod 데이터 센터 431
Citrix 및 NVIDIA를 통한 3D 그래픽 시각화 - 백서 431
6000개 시트용 Citrix XenDesktop/XenApp 7.15 및 VMware vSphere 6.5 업데이트 1이 설치된 FlexPod Datacenter 432
VMware Horizon View 7.3 및 VMware vSphere 6.5 업데이트 1이 설치된 FlexPod 데이터 센터(5,000개 시트의 경우 Cisco UCS Manager 3.2 포함 432
최대 6700개 시트를 지원하는 VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 및 NetApp ONTAP 9.6을 갖춘 FlexPod 데이터 센터 432
최신 앱 434
딥 러닝-디자인을 위한 Cisco UCS 480mL와 AI 및 ML을 결합한 FlexPod 데이터 센터 434
FlexPod을 지원하는 Cisco 컨테이너 플랫폼에 NetApp Trident CSI 플러그인을 구축하십시오 434
OpenShift Container Platform 4용 FlexPod 데이터 센터 - 배포 434
컨테이너 관리용 Docker Enterprise Edition을 사용하는 FlexPod 데이터 센터 435
OpenShift 컨테이너 플랫폼 4-Design용 FlexPod 데이터 센터 435
Cisco UCS를 통해 VMware 및 NVIDIA를 이용한 3D 그래픽 시각화 - 백서 435
Citrix 및 NVIDIA를 통한 3D 그래픽 시각화 - 백서 435
FlexPod 익스프레스 437
FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series 설계 가이드 를 참조하십시오 437
NVA-1139-design:FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series 437
프로그램 요약 437
기술 요구 사항 440
디자인 선택 441
결론 447
추가 정보를 찾을 수 있는 위치 447
FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series 구축 가이드 를 참조하십시오 447
NVA-1142-deploy: FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series-NVA Deployment 447
솔루션 개요 448
기술 요구 사항 451
FlexPod Express 케이블링 정보 452
구현 절차 455
결론 541
감사의 말 541
추가 정보를 찾을 수 있는 위치 542

버전 기록 542
FlexPod Express with Cisco UCS C-Series and AFF A220 Series 설계 가이드 를 참조하십시오 542
NVA-1125-design: FlexPod Express with Cisco UCS C-Series and AFF A220 Series 542
프로그램 요약 542
솔루션 개요 544
기술 요구 사항 545
디자인 선택 546
솔루션 검증 551
결론 552
추가 정보를 찾을 수 있는 위치 552
FlexPod Express with Cisco UCS C-Series and AFF A220 Series 구축 가이드 를 참조하십시오 552
NVA-1123-deploy:FlexPod Express with VMware vSphere 6.7 and NetApp AFF A220 구축 가이드 552
솔루션 개요 553
기술 요구 사항 555
FlexPod Express 케이블링 정보 556
구현 절차 559
결론 633
추가 정보를 찾을 수 있는 위치 633
직접 연결 IP 기반 스토리지를 사용하는 VMware vSphere 6.7U1 및 NetApp AFF A220을 지원하는 FlexPod Express 633
NVA-1131-deploy: VMware vSphere 6.7U1 및 NetApp AFF A220을 지원하는 FlexPod Express(직접 연결 IP 기반 스토리지 포함 633
솔루션 개요 634
기술 요구 사항 637
FlexPod 익스프레스 케이블 연결 정보 637
구현 절차 639
결론 743
추가 정보 744
FlexPod Express for VMware vSphere 7.0 with Cisco UCS Mini 및 NetApp AFF/FAS-NVA-Deployment 744
FlexPod 및 보안 745
FlexPod, 랜섬웨어에 대한 솔루션 745
TR-4802: FlexPod, 랜섬웨어에 대한 솔루션 745
FlexPod 개요 747
랜섬웨어 차단 조치 748
FlexPod에서 데이터 보호 및 복구 750
대가를 지불하지 않고 비즈니스 운영을 지속하십시오 763
결론 763
감사의 말 764
추가 정보 764
FIPS 140-2 Security-호환 FlexPod 솔루션을 통한 의료 서비스 지원 764
TR-4892: FIPS 140-2 Security-compliant FlexPod solution for healthcare 764

의료 분야의 사이버 보안 위협 765
FIPS 140-2 개요 767
컨트롤 플레인 대 데이터 플레인 768
FlexPod Cisco UCS 컴퓨팅 및 FIPS 140-2 769
FlexPod Cisco 네트워킹 및 FIPS 140-2 770
FlexPod NetApp ONTAP 스토리지 및 FIPS 140-2 774
FlexPod 통합 인프라의 솔루션 이점 781
추가 FlexPod 보안 고려 사항 784
결론 785
감사의 말, 버전 기록 및 추가 정보를 찾을 수 있는 위치 785
NetApp ONTAP 스토리지와 Cisco Intersight 789
Cisco Intersight with NetApp Storage 빠른 시작 가이드 를 참조하십시오 789
소개 789
새로운 기능 789
2024년 1월 789
2023년 11월 789
2023년 8월 790
2023년 7월 790
2023년 6월 790
2023년 4월 791
2023년 1월 791
2022년 8월 791
2022년 7월 791
2022년 4월 792
2022년 1월 792
2021년 10월 793
알려진 문제 793
요구 사항 793
하드웨어 및 소프트웨어 요구 사항 794
Cisco Intersight 라이센스 요구 사항 794
시작하기 전에 794
NetApp Active IQ Unified Manager 설치 또는 업그레이드 794
Cisco Intersight Assist 가상 어플라이언스를 설치합니다 795
IMT 서비스용 AIQ UM 프록시 서버를 구성합니다 800
청구 대상 801
Cisco Intersight에서 NetApp 스토리지 모니터링 802
스토리지 인벤토리 개요 802
스토리지 위젯 803
사용 사례 805
사용 사례 1: NetApp 스토리지 인벤토리 및 위젯 모니터링 805
사용 사례 2: 참조 워크플로우를 사용하여 NetApp 스토리지 오케스트레이션 805

사용 사례 3: 디자이너가 필요 없는 양식을 사용하는 사용자 지정 워크플로 . . . 806
검토할 수 있습니다 . . . 809
Cisco UCSM, VMware vSphere 7.0 및 NetApp ONTAP 9를 사용하는 FlexPod용 엔드 투 엔드 NVMe . . . 809
TR-4914: Cisco UCSM, VMware vSphere 7.0 및 NetApp ONTAP 9를 사용하는 FlexPod용 엔드 투 엔드 NVMe . . . 809
테스트 접근 방식 . . . 811
테스트 결과 . . . 814
결론 . . . 817
법적 고지 . . . 820
저작권 . . . 820
상표 . . . 820
특허 . . . 820
개인 정보 보호 정책 . . . 820

FlexPod 솔루션

FlexPod 정의

FlexPod 익스프레스 기술 사양

TR-4293: FlexPod 익스프레스 기술 사양

Karthick Radhakrishnan, Arvind Ramakrishnan, Lindsey Street, Savita Kumari, NetApp에서 근무했습니다

FlexPod Express는 Cisco UCS(Cisco Unified Computing System) 및 Cisco Nexus 스위치 제품군을 기반으로 사전 설계된 모범 사례 아키텍처이며, NetApp FAS 또는 NetApp E-Series 스토리지를 사용하여 스토리지 계층을 구축합니다. FlexPod Express는 다양한 가상화 하이퍼바이저와 운영 체제(OS) 및 엔터프라이즈 워크로드를 실행하는 데 적합한 플랫폼입니다.

FlexPod Express는 기본 구성뿐만 아니라 다양한 사용 사례와 요구 사항을 수용할 수 있도록 규모를 조정할 수 있는 유연성도 제공합니다. 이 문서에서는 사용된 스토리지 시스템, FlexPod Express with NetApp FAS 및 FlexPod Express with E-Series를 기반으로 FlexPod Express 구성을 분류합니다.

FlexPod 플랫폼

FlexPod 플랫폼에는 3가지 플랫폼이 있습니다.

- * FlexPod 데이터 센터. * 이 플랫폼은 워크로드 엔터프라이즈 애플리케이션, 가상화, VDI, 퍼블릭 및 프라이빗 클라우드에 적합한 대규모 확장형 가상 데이터 센터 인프라입니다. FlexPod 데이터 센터에서는 에 나와 있는 고유 사양이 제공됩니다 "TR-4036: FlexPod 데이터 센터 기술 사양".
- * FlexPod 익스프레스. * 이 플랫폼은 원격 사무소 및 에지 사용 사례를 대상으로 하는 소형 통합 인프라입니다.

이 문서에서는 FlexPod 익스프레스 플랫폼의 기술 사양을 제공합니다.

FlexPod 규칙

FlexPod 설계는 다양한 구성 요소와 소프트웨어 버전을 포함하는 유연한 인프라를 허용합니다.

규칙 집합을 사용하여 유효한 FlexPod 구성을 빌드하거나 어셈블합니다. 이 문서에 나와 있는 숫자 및 규칙은 FlexPod의 최소 요구사항이므로 다른 환경과 사용 사례에 따라 포함된 제품군에서도 확장할 수 있습니다.

지원되는 구성과 검증된 FlexPod 구성 비교

FlexPod 아키텍처는 이 문서에 설명된 규칙 집합으로 정의됩니다. 하드웨어 구성 요소 및 소프트웨어 구성은 Cisco HCL(하드웨어 호환 목록) 및 에서 지원해야 합니다 "NetApp 상호 운용성 매트릭스 툴(IMT)".

CVD(Cisco Validated Design) 또는 NVA(NetApp Verified Architecture)는 각각 가능한 FlexPod 구성입니다. Cisco와 NetApp은 이러한 구성 조합을 문서화하고 광범위한 엔드 투 엔드 테스트를 통해 이러한 조합을 검증합니다. 이 문서에서 설명하는 지침을 따르고 모든 구성 요소가 Cisco HCL 및 NetApp에서 호환되는 것으로 나열된 경우, 이러한 구성에서 벗어난 FlexPod 구축이 완전히 지원됩니다 "IMT".

예를 들어, 소프트웨어, 하드웨어 및 구성이 이 문서에 정의된 지침을 충족하는 경우 스토리지 컨트롤러 또는 Cisco

UCS 서버를 추가하고 소프트웨어를 최신 버전으로 업그레이드할 수 있습니다.

스토리지 소프트웨어

FlexPod Express는 NetApp ONTAP 또는 SANtricity 운영 체제를 실행하는 스토리지 시스템을 지원합니다.

NetApp ONTAP를 참조하십시오

NetApp ONTAP 소프트웨어는 AFF 및 FAS 스토리지 시스템에서 실행되는 운영 체제입니다. ONTAP은 무중단 운영, 무중단 업그레이드 및 민첩한 데이터 인프라를 지원하는 확장성이 뛰어난 스토리지 아키텍처를 제공합니다.

ONTAP에 대한 자세한 내용은 를 참조하십시오 "ONTAP 제품 페이지".

E-Series SANtricity 소프트웨어

E-Series SANtricity 소프트웨어는 E-Series 스토리지 시스템에서 실행되는 운영 체제입니다. SANtricity는 다양한 애플리케이션 요구를 충족하는 매우 유연한 시스템을 제공하며 기본 제공되는 고가용성 및 다양한 데이터 보호 기능을 제공합니다.

자세한 내용은 를 참조하십시오 "SANtricity 제품 페이지".

최소 하드웨어 요구 사항

이 섹션에서는 다양한 버전의 FlexPod Express에 대한 최소 하드웨어 요구 사항을 설명합니다.

FAS 익스프레스 및 NetApp FlexPod

기본 스토리지에 NetApp FAS 컨트롤러를 사용하는 FlexPod 익스프레스 솔루션의 하드웨어 요구사항에는 이 섹션에 설명되어 있는 구성이 포함됩니다.

CIMC 기반 구성(독립 실행형 랙 서버)

CIMC(Cisco Integrated Management Controller) 구성에는 다음과 같은 하드웨어 구성요소가 포함됩니다.

- 이중화 구성의 10Gbps 표준 이더넷 스위치 2개(Cisco Nexus 31108 권장, Cisco Nexus 3000 및 9000 모델 지원)
- Cisco UCS C-Series 독립 실행형 랙 서버
- 2노드 클러스터로 구축된 고가용성(HA) 쌍 구성에서 AFF C190, AFF A250, FAS2600 또는 FAS 2700 시리즈 컨트롤러 2개

Cisco UCS로 관리하는 이기종 구성

Cisco UCS 관리 확인에는 다음 하드웨어 구성요소가 포함됩니다.

- 중복 구성의 10Gbps 표준 이더넷 스위치 2개(Cisco Nexus 3524 권장)
- Cisco UCS 5108 AC(Alternating Current) 블레이드 서버 섀시 1개
- 2개의 Cisco UCS 6324 패브릭 인터커넥트

- Cisco UCS B-Series 서버(최소 4개의 Cisco UCS B200 M5 블레이드 서버)
- HA 쌍 구성에서 AFF C190, AFF A250, FAS2750 또는 FAS2720 컨트롤러 2개(컨트롤러당 2개의 UTA2 포트 필요)

E-Series를 지원하는 **FlexPod Express**

E-Series 스타터 구성이 포함된 FlexPod Express의 하드웨어 요구사항은 다음과 같습니다.

- 2개의 Cisco UCS 6324 패브릭 인터커넥트
- Cisco UCS Mini 섀시 5108 AC2 또는 DC2 1개(Cisco UCS 6324 패브릭 상호 연결은 AC2 및 DC2 섀시에서만 지원됨)
- Cisco UCS B-Series 서버(최소 2개의 Cisco UCS B200 M4 블레이드 서버)
- 최소 12개 디스크 드라이브가 장착된 E-Series E2824 스토리지 시스템의 HA 쌍 구성 1개
- 이중화 구성의 10Gbps 표준 이더넷 스위치 2개(데이터 센터의 기존 스위치 사용 가능)

이러한 하드웨어 구성 요소는 솔루션의 초기 구성을 구축하는 데 필요합니다. 필요에 따라 블레이드 서버와 디스크 드라이브를 추가할 수 있습니다. E-Series E2824 스토리지 시스템을 더 높은 플랫폼으로 교체할 수 있으며 All-Flash 시스템으로 실행할 수도 있습니다.

최소 소프트웨어 요구 사항

이 섹션에서는 다양한 버전의 FlexPod Express에 대한 최소 소프트웨어 요구 사항에 대해 설명합니다.

AFF Express with NetApp FAS 또는 **FlexPod**의 소프트웨어 요구 사항

FAS Express with NetApp FlexPod의 소프트웨어 요구사항은 다음과 같습니다.

- ONTAP 9.1 이상
- Cisco NX-OS 버전 7.0(3) I6(1) 이상
- Cisco UCS 관리 구성에서 Cisco UCS Manager UCS 4.0(1b)

모든 소프트웨어가 에 나열되고 지원되어야 합니다 "NetApp IMT를 참조하십시오". 특정 소프트웨어 기능의 경우 이전 아키텍처에 나열된 최소 버전보다 더 최신 버전의 코드가 필요할 수 있습니다.

FlexPod Express with E-Series의 소프트웨어 요구사항입니다

E-Series와 FlexPod Express의 소프트웨어 요구사항은 다음과 같습니다.

- E-Series SANtricity 소프트웨어 11.30 이상
- Cisco UCS Manager 4.0(1b):

모든 소프트웨어가 에 나열되고 지원되어야 합니다 "NetApp IMT를 참조하십시오".

연결 요구 사항

이 섹션에서는 다양한 버전의 FlexPod Express에 대한 연결 요구 사항에 대해 설명합니다.

FAS Express with NetApp FlexPod의 연결 요구 사항

NetApp FAS를 사용한 FlexPod Express의 연결 요구사항은 다음과 같습니다.

- 스토리지 컨트롤러가 패브릭 인터커넥트에 연결된 Cisco UCS 관리 구성은 제외하고 NetApp FAS 스토리지 컨트롤러는 Cisco Nexus 스위치에 직접 연결되어야 합니다.
- 핵심 FlexPod 구성 요소 사이에 추가 장비를 인라인으로 배치할 수 없습니다.
- Cisco Nexus 3000/9000 시리즈 스위치를 NetApp 스토리지 컨트롤러에 연결하려면 가상 포트 채널(vPC)이 필요합니다.
- 반드시 필요한 것은 아니지만 환경 전체에서 점보 프레임 지원을 사용하도록 설정하는 것이 좋습니다.

FlexPod Express와 NetApp E-Series의 연결 요구사항

E-Series와 FlexPod Express의 연결 요구사항은 다음과 같습니다.

- E-Series 스토리지 컨트롤러는 패브릭 인터커넥트에 직접 연결되어야 합니다.
- 핵심 FlexPod 구성 요소 사이에 추가 장비를 인라인으로 배치해서는 안 됩니다.
- VPC는 패브릭 상호 연결과 이더넷 스위치 사이에 필요합니다.

AFF Express with NetApp FlexPod의 연결 요구 사항

NetApp AFF를 사용한 FlexPod Express의 연결 요구사항은 다음과 같습니다.

- 스토리지 컨트롤러가 패브릭에 연결되어 있는 Cisco UCS 관리 구성의 경우를 제외하고 NetApp AFF 스토리지 컨트롤러는 Cisco Nexus 스위치에 직접 연결되어 있어야 합니다. 상호 연결.
- 핵심 FlexPod 구성 요소 사이에 추가 장비를 인라인으로 배치할 수 없습니다.
- Cisco Nexus 3000/9000 시리즈 스위치를 NetApp 스토리지 컨트롤러에 연결하려면 가상 포트 채널(vPC)이 필요합니다.
- 반드시 필요한 것은 아니지만 환경 전체에서 점보 프레임 지원을 사용하도록 설정하는 것이 좋습니다.

기타 요구 사항

FlexPod 익스프레스에 대한 추가 요구 사항은 다음과 같습니다.

- 다음을 포함하여 모든 장비에 대해 유효한 지원 계약이 필요합니다.
  - Cisco 장비를 위한 SMARTnet 지원
  - NetApp 장비에 대한 SupportEdge Advisor 또는 SupportEdge Premium 지원
- 모든 소프트웨어 구성 요소가 에 나열되고 지원되어야 합니다 "NetApp IMT를 참조하십시오".
- 모든 NetApp 하드웨어 구성 요소가 에 나열되고 지원되어야 합니다 "NetApp Hardware Universe를 참조하십시오".
- 모든 Cisco 하드웨어 구성 요소는 에 나열되고 지원되어야 합니다 "Cisco HCL".

레거시 장비

다음 표에는 NetApp 레거시 스토리지 컨트롤러 옵션이 나와 있습니다.

스토리지 컨트롤러	**FAS** 부품 번호	기술 사양
FAS2520	선택한 개별 옵션을 기준으로 합니다	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS2552	선택한 개별 옵션을 기준으로 합니다	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS2554	선택한 개별 옵션을 기준으로 합니다	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS8020	선택한 개별 옵션을 기준으로 합니다	http://www.netapp.com/us/products/storage-systems/fas8000/fas8000-tech-specs.aspx

다음 표에는 NetApp FAS의 기존 디스크 쉘프 옵션이 나와 있습니다.

디스크 쉘프	부품 번호	기술 사양
DE1600	E-X5682A-DM-0E-R6-C	"디스크 쉘프 기술 사양 NetApp Hardware Universe에서 지원되는 드라이브"
DE5600	E-X4041A-12-R6	"디스크 쉘프 기술 사양 NetApp Hardware Universe에서 지원되는 드라이브"
DE6600	X-48564-00-R6	"디스크 쉘프 기술 사양 NetApp Hardware Universe에서 지원되는 드라이브"

기존 **NetApp FAS** 컨트롤러

다음 표에는 레거시 NetApp FAS 컨트롤러 옵션이 나와 있습니다.

현재 부품	**FAS2554**	**FAS2552**	**FAS2520**
구성	4U 섀시 내 컨트롤러 2개	2U 섀시 내 컨트롤러 2개	2U 섀시 내 컨트롤러 2개
최대 기본 용량	576TB	509TB	336TB
내부 드라이브	24	24	12
최대 드라이브 수(내부 및 외부)	144	144	84
최대 볼륨 크기입니다	60TB		
최대 애그리게이트 크기입니다	120TB		

현재 부품	FAS2554	FAS2552	FAS2520
최대 LUN 수입니다	컨트롤러당 2,048개		
스토리지 네트워킹이 지원됩니다	iSCSI, FC, FCoE, NFS 및 CIFS를 지원합니다		iSCSI, NFS 및 CIFS를 지원합니다
최대 NetApp FlexVol 볼륨 수입니다	컨트롤러당 1,000개		
최대 NetApp 스냅샷 복사본 수	컨트롤러당 255,000개		

NetApp FAS 모델에 대한 자세한 내용은 를 참조하십시오 "FAS 모델 섹션" Hardware Universe에서

추가 정보

이 문서에 설명된 정보에 대한 자세한 내용은 다음 문서 및 웹 사이트를 참조하십시오.

- AFF and FAS 시스템 설명서 센터 를 참조하십시오

  "https://docs.netapp.com/platstor/index.jsp"

- AFF 문서 리소스 페이지

  "https://www.netapp.com/us/documentation/all-flash-fas.aspx"

- FAS 스토리지 시스템 문서 리소스 페이지

  "https://www.netapp.com/us/documentation/fas-storage-systems.aspx"

- FlexPod

  "https://flexpod.com/"

- NetApp 설명서

  "https://docs.netapp.com"

FlexPod 데이터 센터 기술 사양

TR-4036: FlexPod 데이터 센터 기술 사양

Arvind Ramakrishnan, Jyh-shing Chen, NetApp

FlexPod 플랫폼은 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 스위치 제품군, NetApp 스토리지 컨트롤러(AFF, ASA 또는 FAS 시스템)를 기반으로 사전 설계되며 모범 사례 데이터 센터 아키텍처를 제공합니다.

FlexPod는 다양한 가상화 하이퍼바이저 및 베어 메탈 운영 체제 및 엔터프라이즈 워크로드를 실행하는 데 적합한 플랫폼입니다. FlexPod는 기본 구성뿐만 아니라 다양한 사용 사례와 요구사항에 맞게 사이징 및 최적화할 수 있는 유연성도 제공합니다.

전체 FlexPod 구성을 주문하기 전에 를 참조하십시오 "FlexPod 통합 인프라" 최신 버전의 기술 사양을 보려면 netapp.com 페이지를 참조하십시오.

"다음: FlexPod 플랫폼."

FlexPod 플랫폼

FlexPod 플랫폼에는 2가지 플랫폼이 있습니다.

- * FlexPod 데이터 센터. * 이 플랫폼은 워크로드 엔터프라이즈 애플리케이션, 가상화, 가상 데스크톱 인프라(VDI), 퍼블릭, 프라이빗, 하이브리드 클라우드 워크로드에 적합한 대규모 확장형 가상 데이터 센터 인프라입니다.
- * FlexPod 익스프레스. * 이 플랫폼은 원격 사무소와 에지 사용 사례를 타겟으로 하는 소형 컨버지드 인프라입니다. FlexPod Express에는 에 설명되어 있는 자체 사양이 있습니다 "FlexPod 익스프레스 기술 사양"

이 문서에서는 FlexPod 데이터 센터 플랫폼의 기술 사양을 제공합니다.

FlexPod 규칙

FlexPod 설계는 다양한 구성 요소와 소프트웨어 버전을 포함하는 유연한 인프라를 지원합니다.

규칙 집합을 사용하여 유효한 FlexPod 구성을 빌드하거나 어셈블합니다. 이 문서에 나와 있는 숫자와 규칙은 FlexPod 구성에 대한 최소 요구 사항입니다. 또한 포함된 제품군에서도 다양한 환경과 사용 사례에 맞게 확장할 수 있습니다.

NetApp ONTAP를 참조하십시오

NetApp ONTAP 소프트웨어는 모든 NetApp FAS, AFF 및 AFF ASA(All SAN Array) 시스템에 설치됩니다. FlexPod는 ONTAP 소프트웨어를 통해 검증되었으며 무중단 운영, 무중단 업그레이드 및 민첩한 데이터 인프라를 지원하는 확장성이 뛰어난 스토리지 아키텍처를 제공합니다.

ONTAP에 대한 자세한 내용은 를 참조하십시오 "ONTAP 데이터 관리 소프트웨어" 제품 페이지.

Cisco Nexus 스위칭 운영 모드

특정 FlexPod 구축의 스위칭 구성 요소로 다양한 Cisco Nexus 제품을 사용할 수 있습니다. 이러한 옵션의 대부분은 기존 Cisco Nexus OS 또는 NX-OS 소프트웨어를 활용합니다. Cisco Nexus 스위치 제품군은 제품 라인 내에서 다양한 기능을 제공합니다. 이러한 기능은 이 문서의 뒷부분에서 자세히 설명합니다.

소프트웨어 정의 네트워킹 분야에서 Cisco가 제공하는 서비스를 ACI(Application Centric Infrastructure)라고 합니다. 패브릭 모드라고도 하는 ACI 모드를 지원하는 Cisco Nexus 9300 시리즈는 Cisco Nexus 9300 시리즈입니다. 이러한 스위치는 NX-OS 또는 독립 실행형 모드로도 구축할 수 있습니다.

Cisco ACI는 특정 애플리케이션의 요구사항에 중점을 둔 데이터 센터 구축을 대상으로 합니다. 애플리케이션은 일련의 프로파일과 계약을 통해 인스턴스화되며, 이를 통해 호스트 또는 가상 머신(VM)과의 접속이 네트워크를 통해 스토리지까지 모두 가능합니다.

FlexPod는 Cisco Nexus 스위치의 두 가지 운영 모드에서 검증되었습니다. ACI 및 NX-OS 모드에 대한 자세한 내용은

다음 Cisco 페이지를 참조하십시오.

- "Cisco 애플리케이션 중심 인프라"
- "Cisco NX-OS 소프트웨어"

최소 하드웨어 요구 사항

FlexPod 데이터 센터 구성에는 스위치, 패브릭 인터커넥트, 서버, NetApp 스토리지 컨트롤러를 비롯한 최소 하드웨어 요구사항이 있습니다.

Cisco UCS 서버를 사용해야 합니다. 검증된 설계에는 C-Series 서버와 B-Series 서버가 모두 사용되었습니다. Cisco Nexus Fabric Extender(FEX)는 C-Series 서버에서 선택 사항입니다.

FlexPod 구성에는 다음과 같은 최소 하드웨어 요구 사항이 있습니다.

- 이중 구성의 Cisco Nexus 스위치 2개 이 구성은 Cisco Nexus 5000, 7000 또는 9000 시리즈의 이중 스위치 2개로 구성될 수 있습니다. 두 스위치는 동일한 모델이어야 하며 동일한 작동 모드로 구성해야 합니다.

  ACI 아키텍처를 구축할 경우 다음과 같은 추가 요구 사항을 준수해야 합니다.

  - Cisco Nexus 9000 시리즈 스위치를 스파인 토폴로지에 구축합니다.
  - 세 개의 Cisco APIC(Application Policy Infrastructure Controller)를 사용합니다.
- 이중 구성의 Cisco UCS 6200, 6300 또는 6400 Series Fabric Interconnect 2개.
- Cisco UCS 서버:
  - 이 솔루션이 B 시리즈 서버를 사용하는 경우 Cisco UCS 5108 B 시리즈 블레이드 서버 섀시 1개와 Cisco UCS B 시리즈 블레이드 서버 2개, 2104, 2204/8, 2408 또는 2304 I/O 모듈(IOM) 2개.
  - 솔루션이 C-Series 서버를 사용하는 경우 Cisco UCS C-Series 랙 서버 2대가 사용됩니다.

    Cisco UCS C-Series 랙 서버를 더 많이 구축할 경우 2232PP FEX 모듈 쌍을 선택할 수 있습니다. 하지만 2232PP 는 하드웨어 요구 사항이 아닙니다.
- 고가용성(HA) 쌍 구성에서 2개의 NetApp 스토리지 컨트롤러:

  이 구성은 지원되는 모든 NetApp FAS, AFF 또는 ASA 시리즈 스토리지 컨트롤러로 구성될 수 있습니다. 를 참조하십시오 "NetApp Hardware Universe를 참조하십시오" 지원되는 FAS, AFF 및 ASA 컨트롤러 모델의 최신 목록을 제공하는 애플리케이션입니다.

  - HA 구성을 사용하려면 데이터 액세스를 위해 컨트롤러당 2개의 이중 인터페이스가 필요합니다. 인터페이스는 FCoE, FC 또는 10/25/100Gb 이더넷(GbE)일 수 있습니다.
  - 솔루션이 NetApp ONTAP를 사용하는 경우 NetApp에서 승인한 클러스터 인터커넥트 토폴로지가 필요합니다. 자세한 내용은 를 참조하십시오 "스위치" 탭을 Hardware Universe 클릭합니다.
  - 솔루션이 ONTAP를 사용하는 경우 데이터 액세스를 위해 컨트롤러당 최소 2개의 추가 10/25/100GbE 포트가 필요합니다.
  - 2개의 노드가 있는 ONTAP 클러스터의 경우 스위치가 없는 2노드 클러스터를 구성할 수 있습니다.
  - 2개 이상의 노드가 있는 ONTAP 클러스터의 경우 클러스터 인터커넥트 스위치 쌍이 필요합니다.
- 지원되는 디스크 유형이 포함된 NetApp 디스크 쉘프 1개 의 쉘프 탭을 참조하십시오 "NetApp Hardware

Universe를 참조하십시오" 지원되는 디스크 쉘프 모델의 최신 목록

최소 소프트웨어 요구 사항

FlexPod 구성에는 다음과 같은 최소 소프트웨어 요구 사항이 있습니다.

- NetApp ONTAP:
  - ONTAP 소프트웨어 버전은 ONTAP 9.1 이상이 필요합니다
- Cisco UCS Manager 릴리즈:
  - Cisco UCS 6200 Series Fabric Interconnect — 2.2(8a)
  - Cisco UCS 6300 Series Fabric Interconnect — 3.1(1e)
  - Cisco UCS 6400 Series Fabric Interconnect — 4.0(1)
- Cisco Intersight 관리 모드:
  - Cisco UCS 6400 Series Fabric Interconnect – 4.1(2)
- Cisco Nexus 5000 시리즈 스위치의 경우 NX-OS 5.1.x를 포함한 Cisco NX-OS 소프트웨어 릴리스 5.0(3)N1(1c) 이상
- Cisco Nexus 7000 시리즈 스위치의 경우:
  - 4슬롯 섀시에는 Cisco NX-OS 소프트웨어 릴리스 6.1(2) 이상이 필요합니다
  - 9슬롯 섀시에는 Cisco NX-OS 소프트웨어 릴리스 5.2 이상이 필요합니다
  - 10슬롯 섀시에는 Cisco NX-OS 소프트웨어 릴리즈 4.0 이상이 필요합니다
  - 18슬롯 섀시에는 Cisco NX-OS 소프트웨어 릴리즈 4.1 이상이 필요합니다
- Cisco Nexus 9000 시리즈 스위치의 경우 Cisco NX-OS 소프트웨어 릴리즈 6.1(2) 이상

FlexPod 구성에 사용되는 소프트웨어가 NetApp에서 지원 및 목록에 있어야 합니다 "IMT". 일부 기능은 나열된 것보다 최신 소프트웨어 릴리스를 필요로 할 수 있습니다.

연결 요구 사항

FlexPod 구성에는 다음과 같은 연결 요구 사항이 있습니다.

- 모든 구성 요소를 사용하려면 별도의 100Mbps 이더넷/1Gb 이더넷 대역외 관리 네트워크가 필요합니다.
- 환경 전체에 점보 프레임 지원을 설정하는 것이 좋지만 필수는 아닙니다.
- Cisco UCS Fabric Interconnect 어플라이언스 포트는 iSCSI 및 NAS 연결에만 권장됩니다.
- 핵심 FlexPod 구성 요소 사이에 추가 장비를 배치할 수 없습니다.

업링크 연결:

- 가상 포트 채널(vPC)을 지원하려면 NetApp 스토리지 컨트롤러의 포트를 Cisco Nexus 5000, 7000 또는 9000 시리즈 스위치에 연결해야 합니다.
- VPC는 Cisco Nexus 5000, 7000 또는 9000 시리즈 스위치에서 NetApp 스토리지 컨트롤러로 필요합니다.
- VPC는 Cisco Nexus 5000, 7000 또는 9000 시리즈 스위치에서 패브릭 상호 연결까지 필요합니다.

- vPC에 대해 최소 2개의 연결이 필요합니다. 애플리케이션 로드 및 성능 요구사항에 따라 vPC 내의 연결 수를 늘릴 수 있습니다.

직접 연결:

- 패브릭 인터커넥트에 직접 연결된 NetApp 스토리지 컨트롤러 포트를 그룹화하여 포트 채널을 설정할 수 있습니다. VPC는 이 구성에서 지원되지 않습니다.
- FCoE 포트 채널은 엔드 투 엔드 FCoE 설계에 권장됩니다.

SAN 부팅:

- FlexPod 솔루션은 iSCSI, FC 또는 FCoE 프로토콜을 사용하여 SAN 부팅 아키텍처를 기반으로 설계되었습니다. SAN에서의 부팅 기술을 사용하면 데이터 센터 인프라에 가장 유연한 구성이 가능하며 각 인프라 구성 요소 내에서 다양한 기능을 사용할 수 있습니다. SAN에서 부팅하는 것이 가장 효율적인 구성이지만 로컬 서버 스토리지에서 부팅하는 것은 유효하고 지원되는 구성입니다.
- FC를 통한 SAN 부팅 - NVMe는 지원되지 않습니다.

기타 요구 사항

FlexPod 아키텍처에는 다음과 같은 추가 상호 운용성 및 지원 관련 요구사항이 있습니다.

- 모든 하드웨어 및 소프트웨어 구성요소는 NetApp에서 지원 및 나열되어야 합니다 "IMT", "Cisco UCS 하드웨어 및 소프트웨어 호환성 목록"및 Cisco UCS 하드웨어 및 소프트웨어 상호 운용성 매트릭스 툴에 액세스할 수 있습니다.
- 다음을 포함하여 모든 장비에 대해 유효한 지원 계약이 필요합니다.
  - Cisco 장비에 대한 Smart Net Total Care(SmartNet) 지원
  - NetApp 장비에 대한 SupportEdge Advisor 또는 SupportEdge Premium 지원
- 판매 주문에 대한 관련 판매 속성은 다음을 지원합니다.
  - FlexPod 권한
  - FlexPod 솔루션 지원 자격

자세한 내용은 NetApp을 참조하십시오 "IMT".

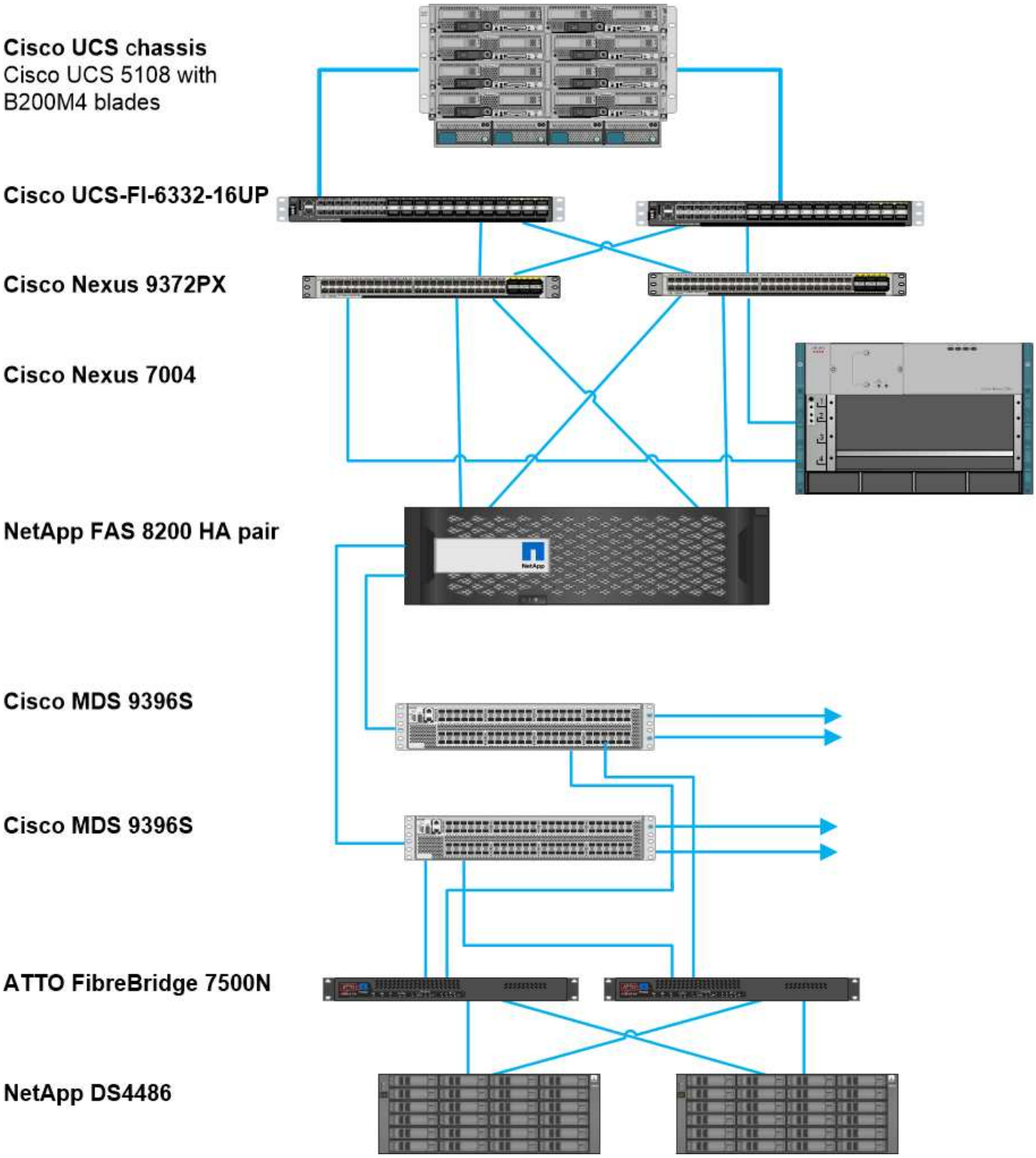
선택적 기능

NetApp은 FlexPod 데이터 센터 아키텍처를 한층 더 향상하기 위해 몇 가지 선택적 구성요소를 지원합니다. 선택적 구성 요소는 다음 하위 섹션에 설명되어 있습니다.

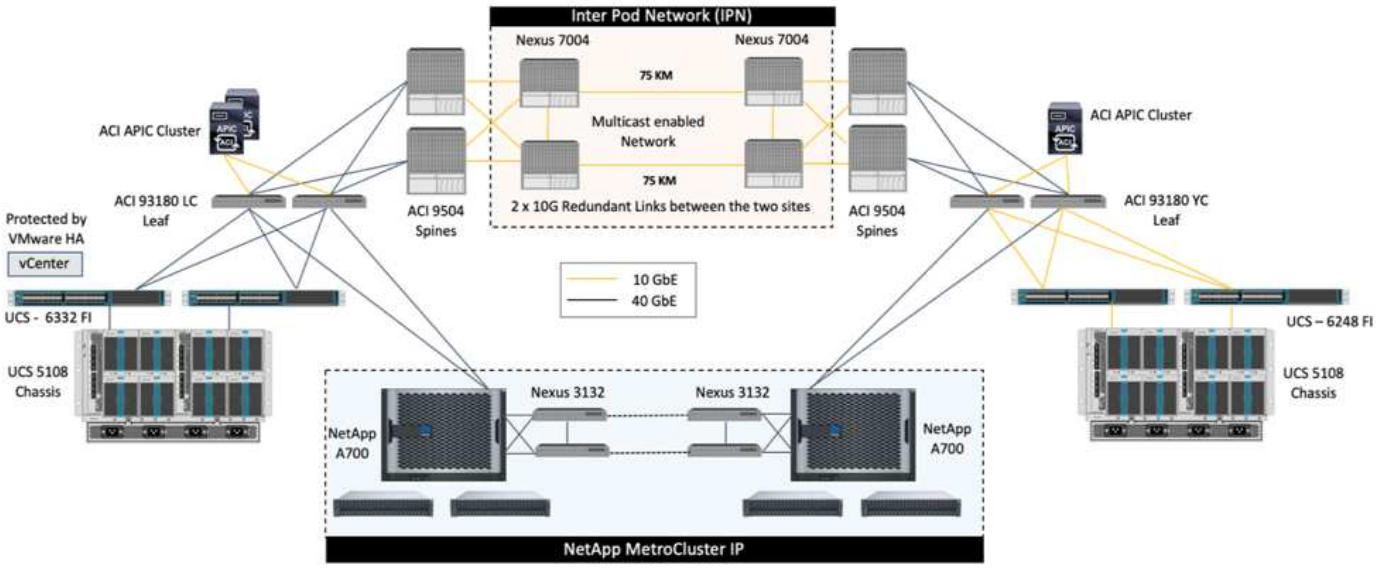
MetroCluster

FlexPod는 2노드 또는 4노드 클러스터 구성에서 지속적인 가용성을 제공하기 위해 두 가지 유형의 NetApp MetroCluster 소프트웨어를 지원합니다. MetroCluster은 중요한 워크로드를 위해 동기식 복제를 제공합니다. Cisco 스위칭과 연결된 이중 사이트 구성이 필요합니다. 사이트 간 최대 지원 거리는 MetroCluster FC의 경우 300km(186마일)이며 MetroCluster IP의 경우 700km(약 35마일)까지 증가합니다. 다음 그림에서는 각각 NetApp MetroCluster 아키텍처를 지원하는 FlexPod 데이터 센터와 NetApp MetroCluster IP 아키텍처를 지원하는 FlexPod 데이터 센터를 보여 줍니다.

다음 그림은 NetApp MetroCluster 아키텍처를 지원하는 FlexPod 데이터 센터를 보여 줍니다.

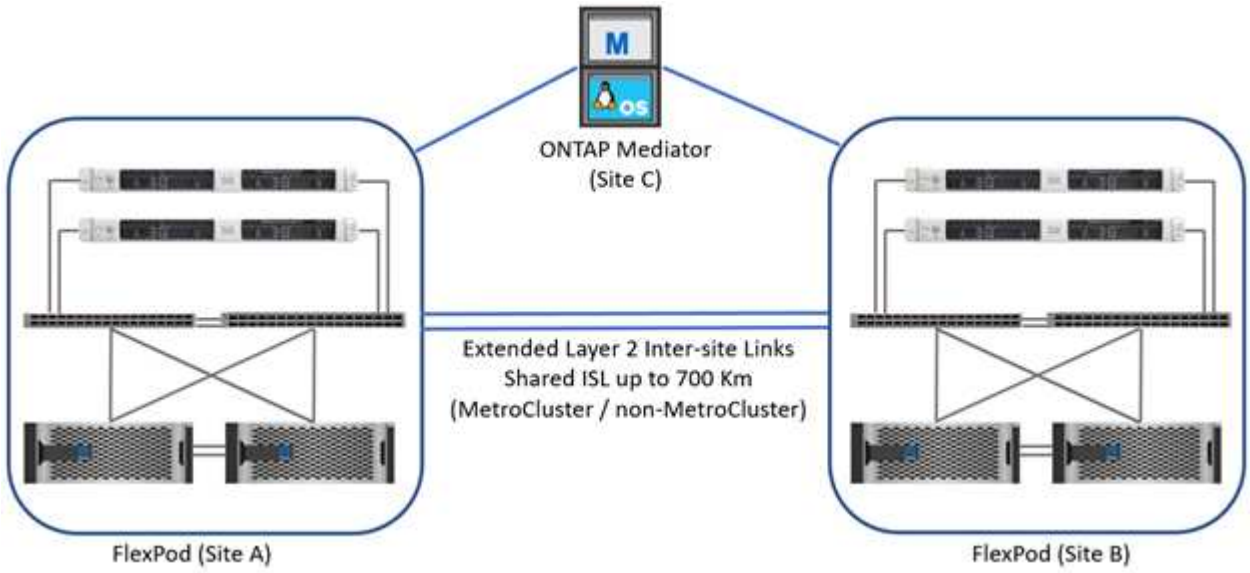


다음 그림은 NetApp MetroCluster IP 아키텍처를 지원하는 FlexPod 데이터 센터를 보여 줍니다.



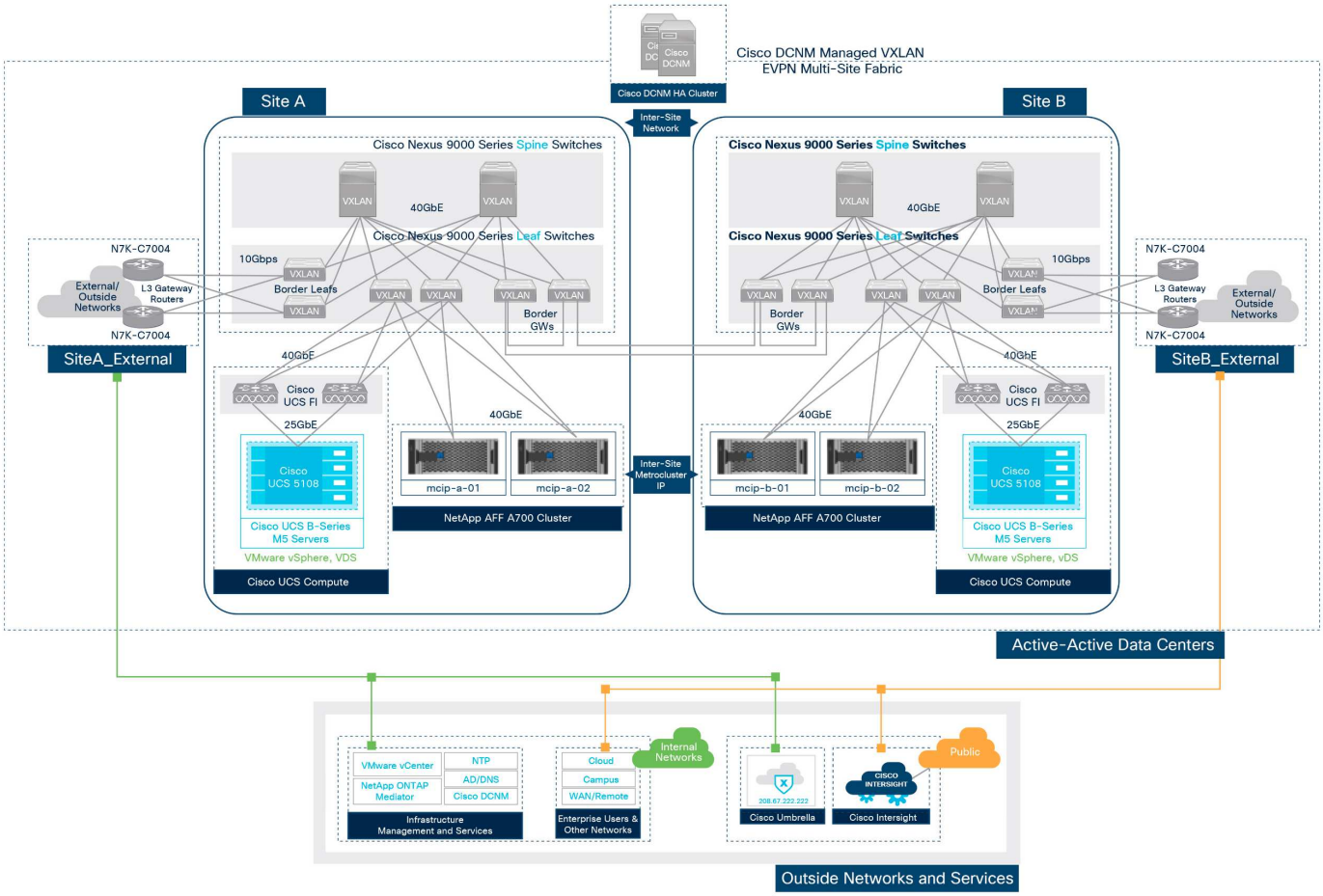
ONTAP 9.8부터 ONTAP 중재자를 세 번째 사이트에 배포하여 MetroCluster IP 솔루션을 모니터링하고 사이트 재해가 발생할 때 예상치 못한 자동 전환을 지원할 수 있습니다.

계층 2 사이트 간 연결이 확장된 FlexPod MetroCluster IP 솔루션 배포의 경우 다음 그림과 같이 네트워크 대역폭 및 스위치가 요구 사항을 충족하는 경우 ISL을 공유하고 MetroCluster 스위치를 호환되는 FlexPod IP 스위치로 사용하여 비용을 절감할 수 있습니다. ISL 공유 및 규정 준수 스위치가 있는 FlexPod MetroCluster IP 솔루션을 보여 줍니다.

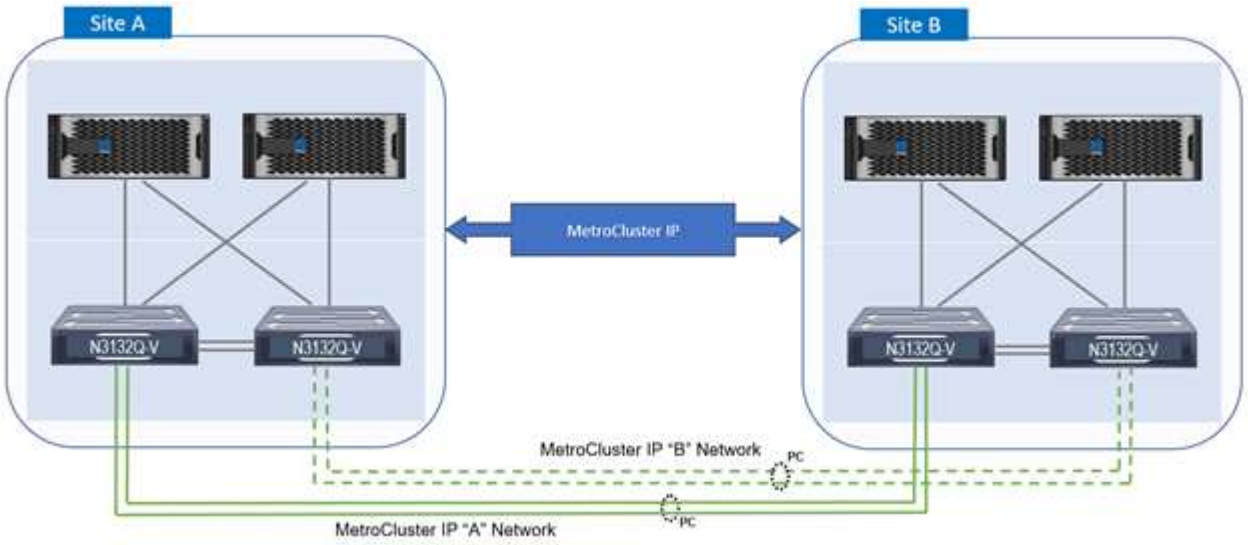


다음 두 그림에서는 VXLAN 멀티 사이트 패브릭 구축을 지원하는 FlexPod MetroCluster IP 솔루션을 위한 VXLAN 멀티 사이트 패브릭 및 MetroCluster IP 스토리지 패브릭을 보여 줍니다.

- FlexPod MetroCluster IP 솔루션용 VXLAN 멀티 사이트 패브릭



- FlexPod MetroCluster IP 솔루션용 MetroCluster IP 스토리지 패브릭



엔드 투 엔드 **FC-NVMe**

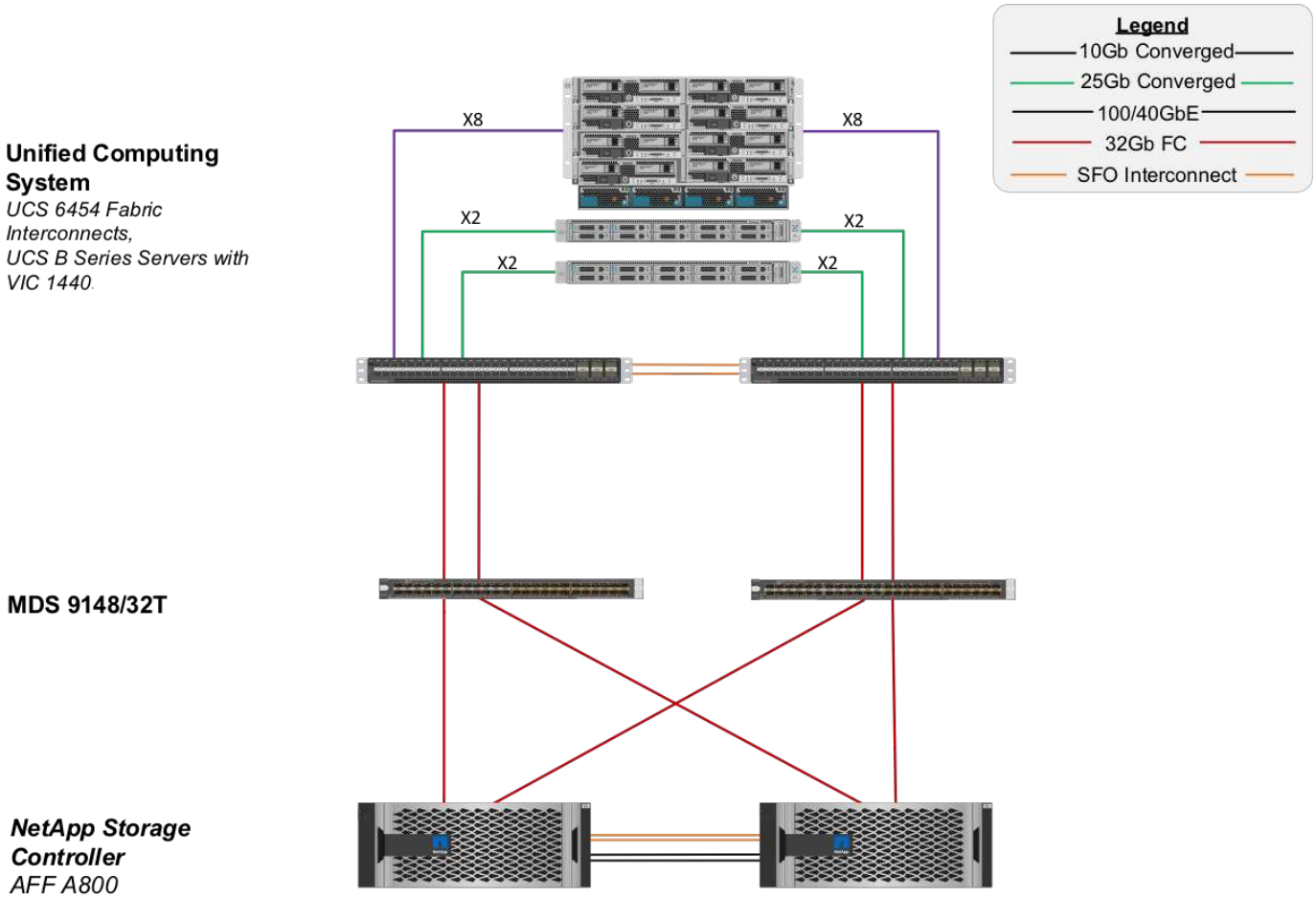
엔드 투 엔드 FC-NVMe는 고객의 기존 SAN 인프라를 실시간 애플리케이션으로 원활하게 확장하는 동시에 IOPS 및 처리량을 높이고 지연 시간을 단축합니다.

기존 32G FC SAN 전송을 사용하여 NVMe 및 SCSI 워크로드를 동시에 전송할 수 있습니다.

다음 그림에서는 Cisco MDS를 사용하는 FC용 FlexPod 데이터 센터를 보여 줍니다.

FlexPod 구성 및 성능 이점에 대한 자세한 내용은 을 참조하십시오 "FlexPod용 엔드 투 엔드 NVMe 백서 소개"

ONTAP 구현에 대한 자세한 내용은 를 참조하십시오 "TR-4684: NVMe로 최신 SAN 구현 및 구성".



Cisco MDS를 통해 **FC SAN** 부팅

전용 SAN 네트워크를 사용하여 확장성을 증대하기 위해 FlexPod는 Cisco MDS 스위치를 통한 FC와 Cisco Nexus 93108TC-FX와 같은 FC 지원을 갖춘 Nexus 스위치를 지원합니다. Cisco MDS를 통한 FC SAN 부팅 옵션에는 다음과 같은 라이센스 및 하드웨어 요구 사항이 있습니다.

- NetApp 스토리지 컨트롤러당 최소 2개의 FC 포트, 각 SAN 패브릭당 1개의 포트
- 각 NetApp 스토리지 컨트롤러에 대한 FC 라이센스
- NetApp에서 지원되는 Cisco MDS 스위치 및 펌웨어 버전입니다 "IMT"

MDS 기반 설계에 대한 자세한 지침은 CVD를 참조하십시오 "VMware vSphere 6.7U1 파이버 채널 및 iSCSI를 지원하는 FlexPod 데이터 센터 구축 가이드".

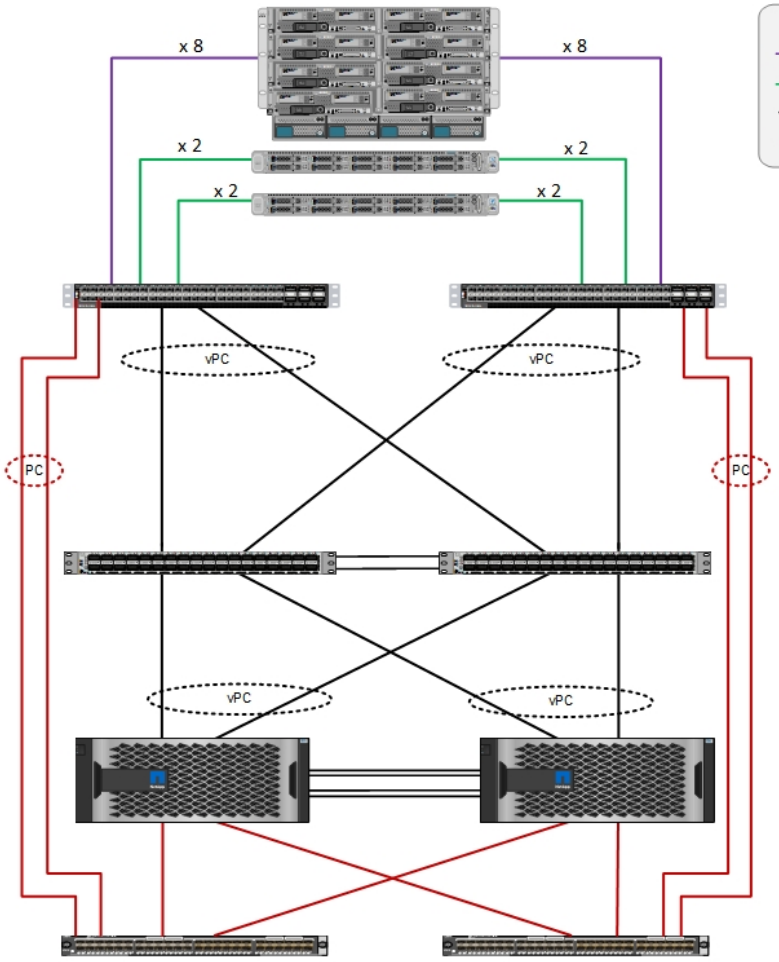
다음 그림은 MDS 연결을 지원하는 FC용 FlexPod 데이터 센터와 Cisco Nexus 93180YC-FX를 사용하는 FC용 FlexPod 데이터 센터의 예를 보여 줍니다.

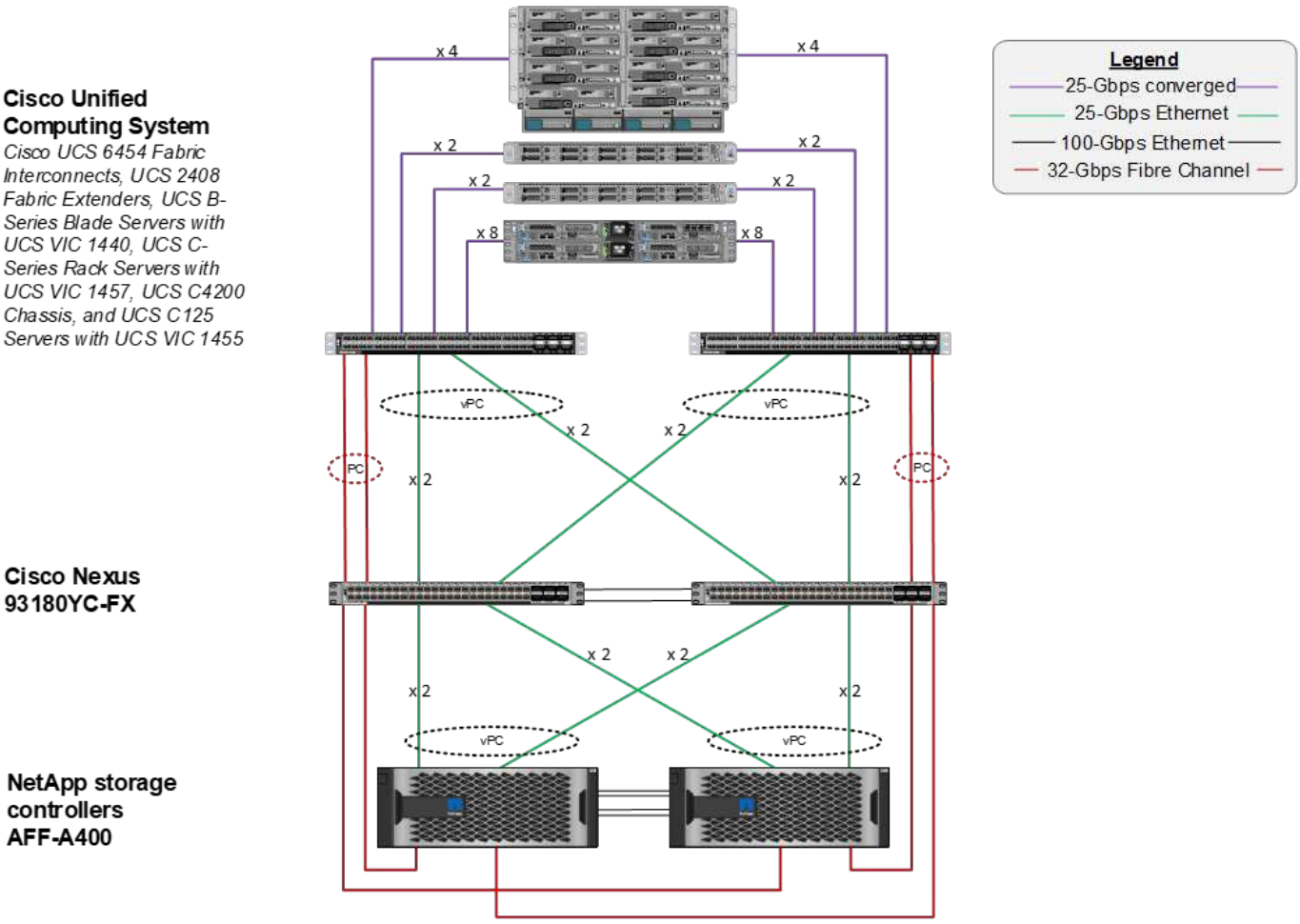
Cisco Unified Computing System
Cisco UCS 6454 Fabric Interconnects, UCS B-Series Blade Servers with UCS VIC 1440, and UCS C-Series Rack Servers with UCS VIC 1457

Cisco Nexus 9336C-FX2

NetApp storage controllers AFF-A800

Cisco MDS 9148T or 9132T switch





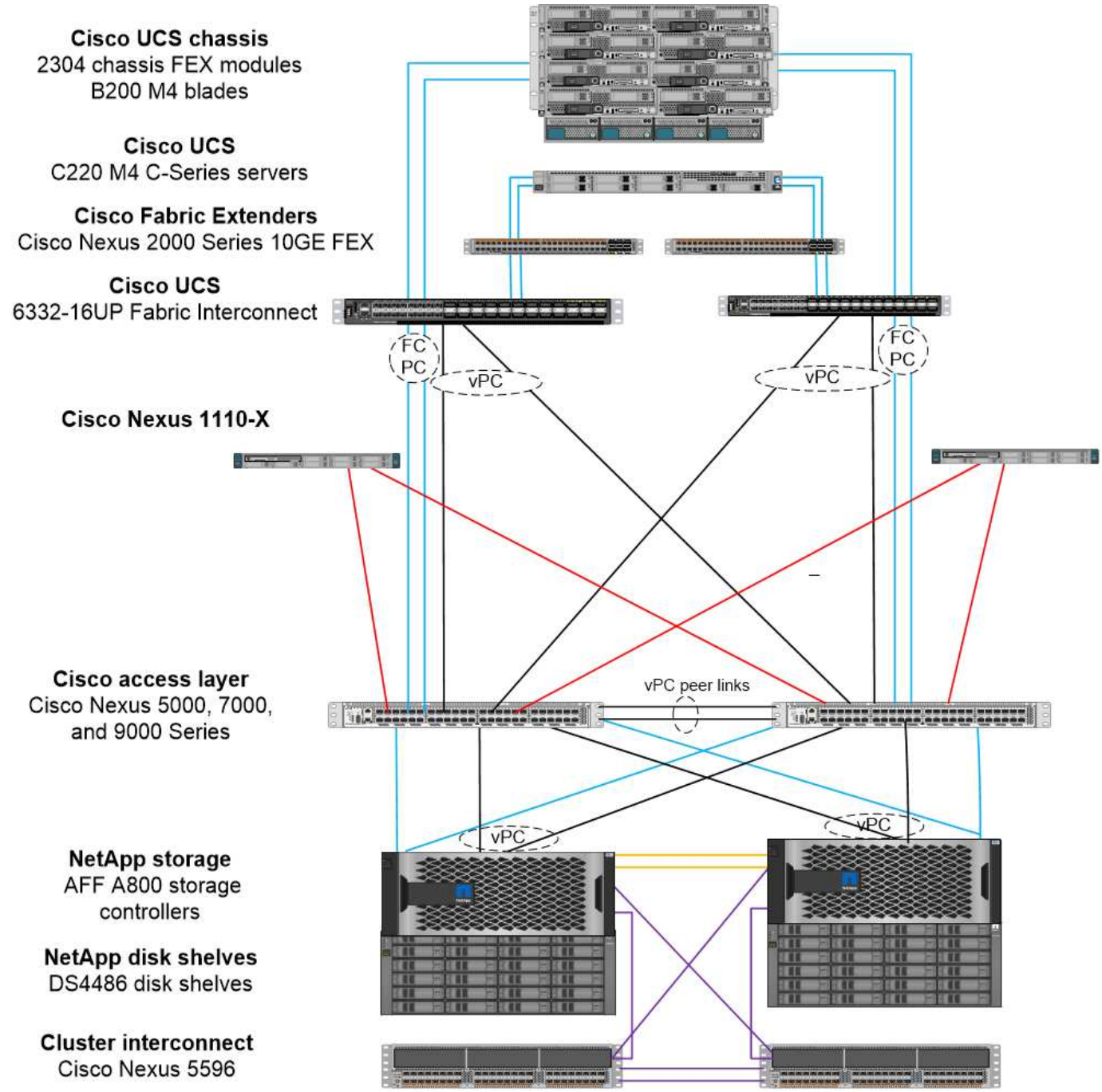
Cisco Nexus로 FC SAN 부팅

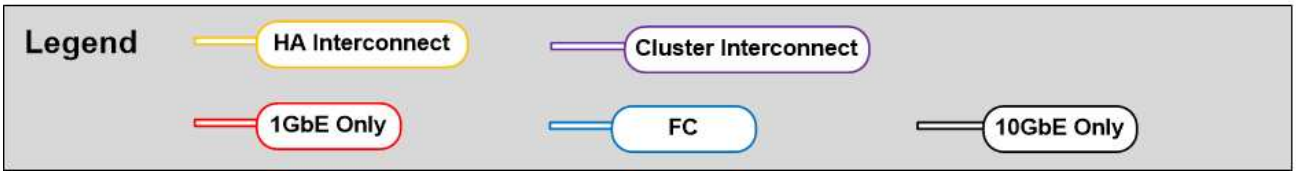
기존 FC SAN 부팅 옵션에는 다음과 같은 라이센스 및 하드웨어 요구 사항이 있습니다.

- Cisco Nexus 5000 시리즈 스위치에서 FC 조닝을 수행하는 경우 Cisco Nexus 5000 시리즈 스위치(FC_features_PKG)에 대한 스토리지 프로토콜 서비스 패키지 라이센스가 필요합니다.
- Cisco Nexus 5000 시리즈 스위치에서 FC 조닝을 수행하는 경우 패브릭 인터커넥트와 Cisco Nexus 5000 시리즈 스위치 사이에 SAN 링크가 필요합니다. 추가 이중화를 위해 링크 간에 SAN 포트 채널을 사용하는 것이 좋습니다.
- Cisco Nexus 5010, 5020 및 5548P 스위치에는 Cisco UCS Fabric Interconnect와 NetApp 스토리지 컨트롤러에 연결하기 위한 별도의 FC 또는 범용 포트(UP) 모듈이 필요합니다.
- Cisco Nexus 93180YC-FX에는 FC를 지원하는 기능을 위한 FC 기능 라이센스가 필요합니다.
- 각 NetApp 스토리지 컨트롤러에는 연결을 위해 최소 2개의 8/16/32Gb FC 포트가 필요합니다.
- NetApp 스토리지 컨트롤러에 FC 라이센스가 필요합니다.

> Cisco Nexus 7000 또는 9000 스위치 제품군을 사용할 경우 패브릭 인터커넥트에서 FC 조닝을 수행하지 않는 한 기존 FC를 사용할 수 없습니다. 이 경우 스위치에 대한 SAN 업링크는 지원되지 않습니다.

다음 그림에서는 FC 연결 구성을 보여 줍니다.





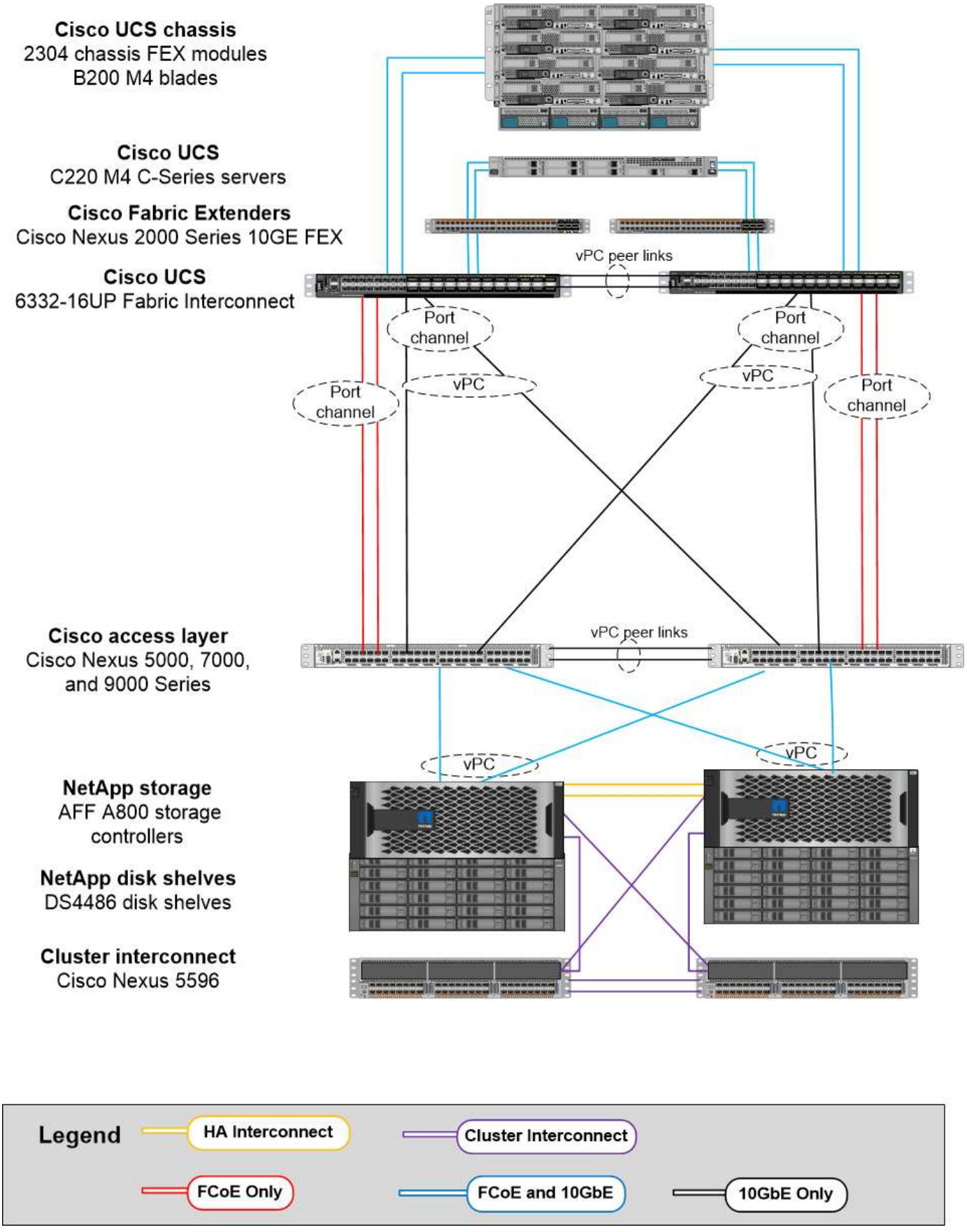
FCoE SAN 부팅 옵션

FCoE SAN 부팅 옵션에는 다음과 같은 라이센스 및 하드웨어 요구 사항이 있습니다.

- 스위치에서 FC 조닝을 수행하는 경우 Cisco Nexus 5000 또는 7000 시리즈 스위치(FC_features_PKG")에 대한 스토리지 프로토콜 서비스 패키지 라이센스가 필요합니다.
- 스위치에서 FC 조닝을 수행하는 경우 패브릭 인터커넥트와 Cisco Nexus 5000 또는 7000 시리즈 스위치 간에 FCoE 업링크가 필요합니다. 추가 이중화를 위해 링크 간에 FCoE 포트 채널도 권장됩니다.
- 온보드 UTA2(Unified Target Adapter 2) 포트가 없는 경우, 각 NetApp 스토리지 컨트롤러에는 FCoE 연결을 위한 이중 포트 UTA(Unified Target Adapter) 애드온 카드가 1개 이상 필요합니다.
- 이 옵션에는 NetApp 스토리지 컨트롤러에 FC 라이센스가 필요합니다.
- 스위치에서 Cisco Nexus 7000 Series 스위치 및 FC 조닝을 수행하는 경우 FCoE를 지원할 수 있는 라인 카드가 필요합니다.

> Cisco Nexus 9000 시리즈 스위치를 사용할 경우 패브릭 인터커넥트에서 FC 조닝을 수행하고 스토리지를 어플라이언스 포트를 통한 패브릭 인터커넥트에 연결하지 않는 한 FCoE를 사용할 수 없습니다. 이 경우 스위치에 대한 FCoE 업링크는 지원되지 않습니다.

다음 그림에서는 FCoE 부팅 시나리오를 보여 줍니다.


Cisco UCS chassis
2304 chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
Port channel
Port channel
Port channel
vPC
vPC
Port channel
Cisco access layer
Cisco Nexus 5000, 7000, and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage controllers
NetApp disk shelves
DS4486 disk shelves
Cluster interconnect
Cisco Nexus 5596
Legend
HA Interconnect
Cluster Interconnect
FCoE Only
FCoE and 10GbE
10GbE Only

iSCSI 부트 옵션

iSCSI 부팅 옵션에는 다음과 같은 라이센스 및 하드웨어 요구 사항이 있습니다.

- NetApp 스토리지 컨트롤러에 iSCSI 라이센스가 필요합니다.
- iSCSI를 부팅할 수 있는 Cisco UCS Server의 어댑터가 필요합니다.
- NetApp 스토리지 컨트롤러에서 2포트 10Gbps 이더넷 어댑터가 필요합니다.

다음 그림은 iSCSI를 사용하여 부팅되는 이더넷 전용 구성을 보여 줍니다.

Cisco UCS chassis
2304 Chassis FEX modules
B200 M4 blades

Cisco UCS
C220 M4 C-Series servers

Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX

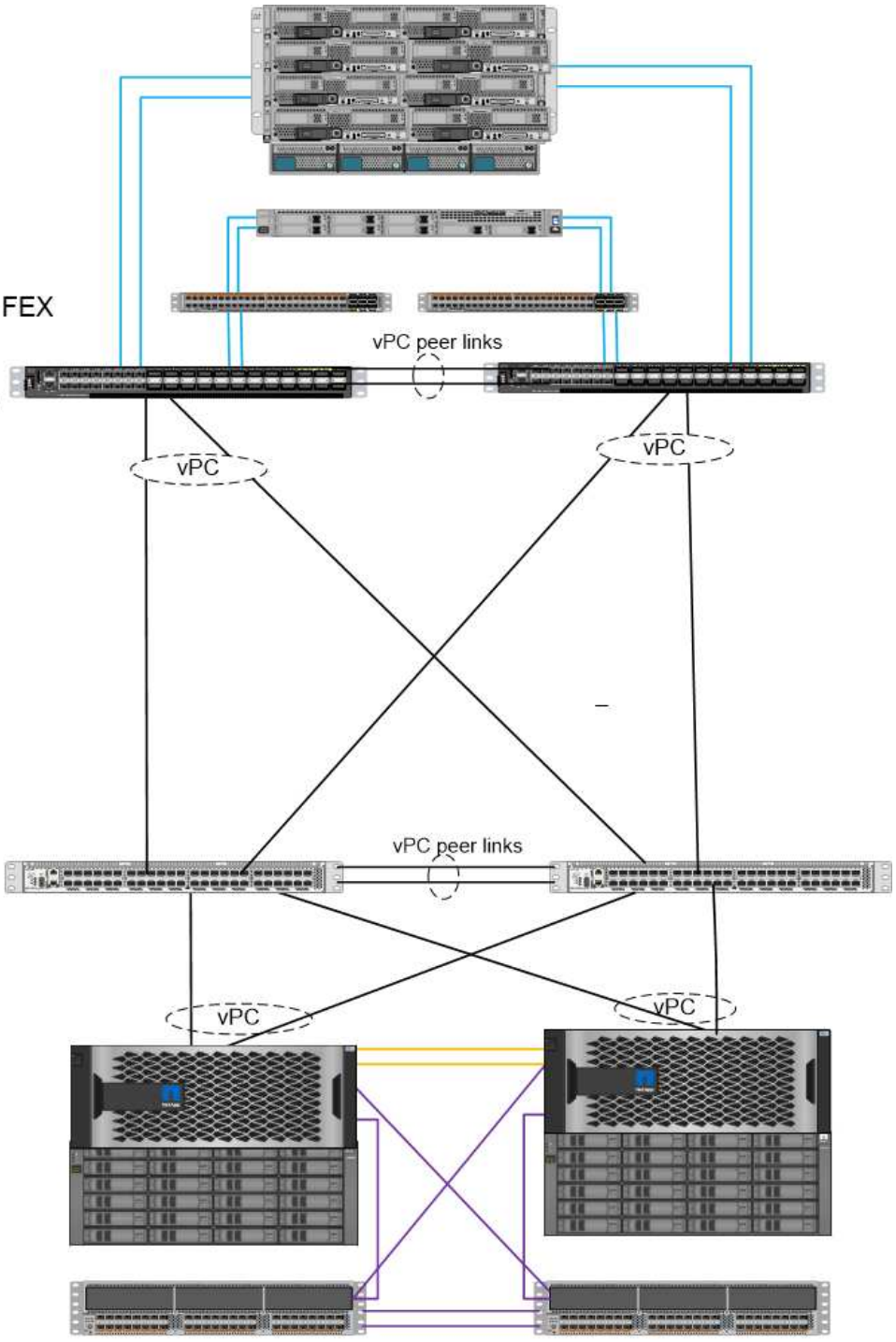
Cisco UCS
6332-16UP Fabric Interconnect

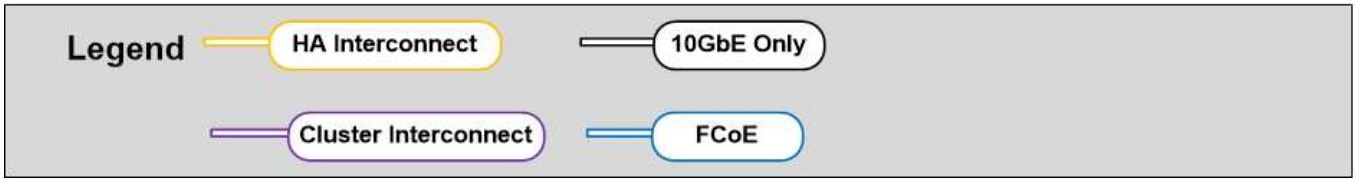
Cisco access layer
Cisco Nexus 5000, 7000, and 9000 Series

NetApp storage
AFF A800 storage controllers

NetApp disk shelves
DS4486 Disk shelves

Cluster Interconnect
Cisco Nexus 5596





Cisco UCS를 NetApp 스토리지와 직접 연결

NetApp AFF 및 FAS 컨트롤러는 업스트림 SAN 스위치 없이 Cisco UCS 패브릭 인터커넥트에 직접 연결할 수 있습니다.

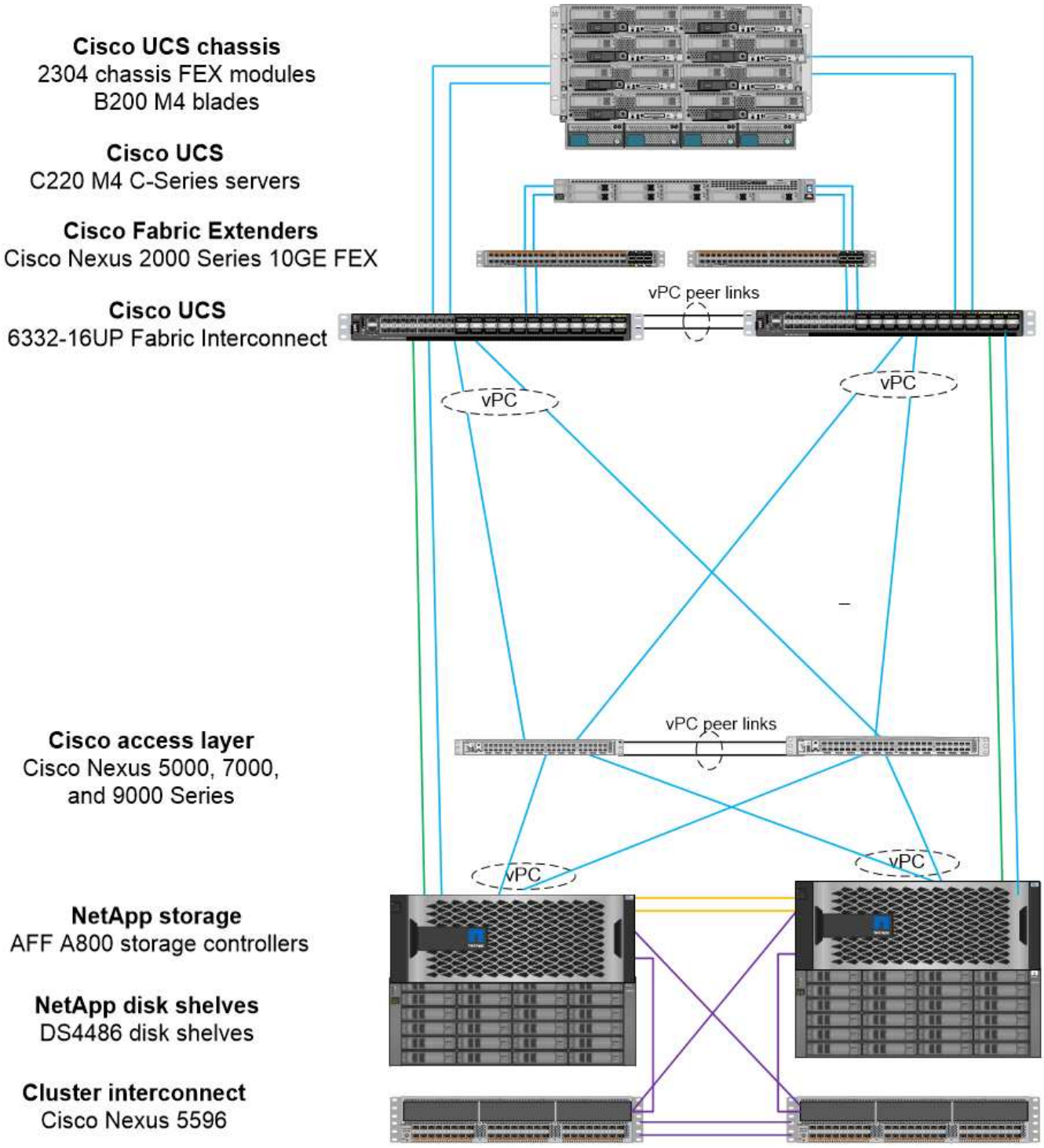
NetApp 스토리지에 직접 연결하는 데 네 가지 Cisco UCS 포트 유형을 사용할 수 있습니다.

- * 스토리지 FC 포트. * 이 포트를 NetApp 스토리지의 FC 포트에 직접 연결합니다.
- * 스토리지 FCoE 포트. * 이 포트를 NetApp 스토리지의 FCoE 포트에 직접 연결합니다.
- 어플라이언스 포트. * 이 포트를 NetApp 스토리지의 10GbE 포트에 직접 연결합니다.
- * 유니파이드 스토리지 포트. * 이 포트를 NetApp UTA에 직접 연결

라이센스 및 하드웨어 요구 사항은 다음과 같습니다.

- NetApp 스토리지 컨트롤러에 프로토콜 라이센스가 필요합니다.
- 서버에 Cisco UCS 어댑터(이니시에이터)가 필요합니다. 지원되는 Cisco UCS 어댑터 목록은 NetApp을 참조하십시오 "IMT".
- NetApp 스토리지 컨트롤러의 타겟 어댑터가 필요합니다.

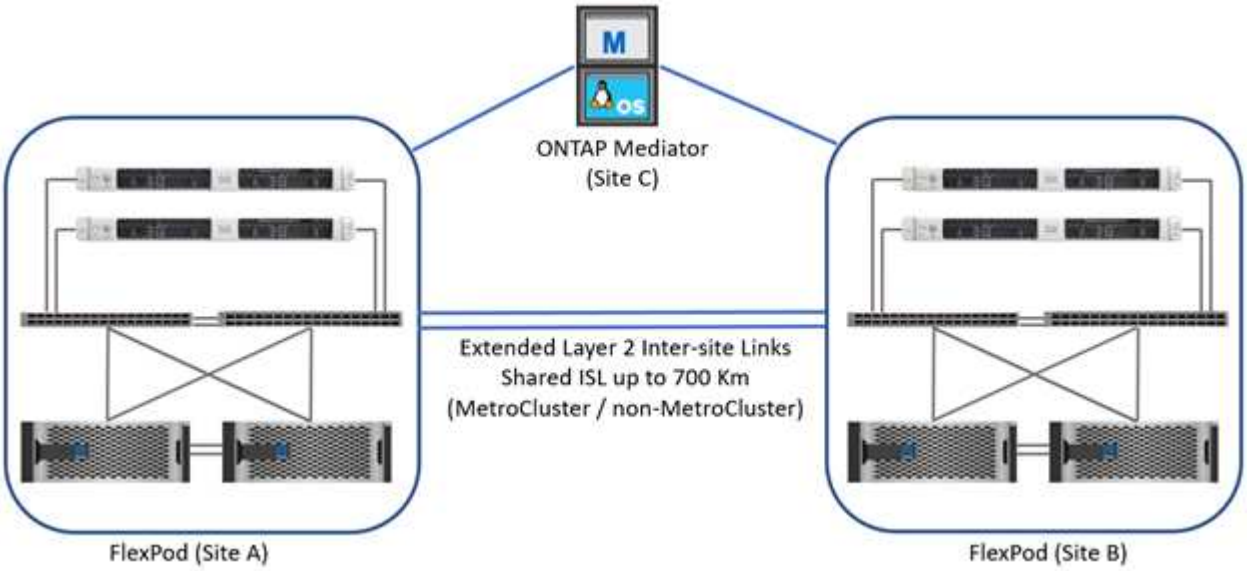
다음 그림은 FC 직접 연결 구성을 보여 줍니다.


Cisco UCS chassis
2304 chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
vPC
vPC
Cisco access layer
Cisco Nexus 5000, 7000,
and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage controllers
NetApp disk shelves
DS4486 disk shelves
Cluster interconnect
Cisco Nexus 5596
Legend
HA Interconnect
Cluster Interconnect
FC
FCoE
10GbE Only

- 참고: *

- Cisco UCS는 FC 스위칭 모드에서 구성됩니다.
- 타겟의 FCoE 포트와 패브릭 상호 연결은 FCoE 스토리지 포트로 구성됩니다.
- 타겟에서 패브릭 인터커넥트까지의 FC 포트는 FC 스토리지 포트로 구성됩니다.

다음 그림은 iSCSI/Unified IP 직접 연결 구성을 보여 줍니다.



- 참고: *
- Cisco UCS는 이더넷 스위칭 모드에서 구성됩니다.
- 타겟의 iSCSI 포트와 패브릭 상호 연결은 iSCSI 데이터용 이더넷 스토리지 포트로 구성됩니다.
- 타겟에서 패브릭 인터커넥트까지의 이더넷 포트는 CIFS/NFS 데이터용 이더넷 스토리지 포트로 구성됩니다.

Cisco 구성 요소

Cisco는 솔루션의 컴퓨팅 및 네트워킹 계층을 모두 포괄하는 FlexPod 설계 및 아키텍처에 상당한 기여를 했습니다. 이 섹션에서는 FlexPod에 사용할 수 있는 Cisco UCS 및 Cisco Nexus 옵션에 대해 설명합니다. FlexPod는 Cisco UCS B-Series 서버와 C-Series 서버를 모두 지원합니다.

Cisco UCS 패브릭 인터커넥트 옵션

FlexPod 아키텍처에는 이중 패브릭 인터커넥트가 필요합니다. 한 쌍의 패브릭 인터커넥트에 여러 Cisco UCS 섀시를 추가할 경우, 환경의 최대 섀시 수는 아키텍처 및 포트 제한에 따라 결정됩니다.

다음 표에 나와 있는 부품 번호는 기본 패브릭 인터커넥트용으로 제공됩니다. 전원 공급 장치(PSU) 또는 SFP+, QSFP+ 또는 확장 모듈은 포함되지 않습니다. 추가 패브릭 인터커넥트가 지원됩니다. 을 참조하십시오 "NetApp IMT를 참조하십시오" 를 참조하십시오.

Cisco UCS 패브릭 인터커넥트	부품 번호	기술 사양
Cisco UCS 6332UP	UCS-FI-6332-UP	"Cisco UCS 6332 패브릭 인터커넥트"

Cisco UCS 패브릭 인터커넥트	부품 번호	기술 사양
Cisco UCS 6454	UCS-FI-6454-U	"Cisco UCS 6454 Fabric 상호 연결"

Cisco UCS 6454

Cisco UCS 6454 시리즈는 회선 속도, 지연 시간이 짧은 무손실 10/25/40/100GbE 이더넷 및 FCoE 연결과 이더넷 또는 FC 운영을 지원하는 통합 포트를 제공합니다. 44개의 10/25Gbps 포트는 10Gbps 또는 25Gbps 통합 이더넷으로 작동할 수 있으며, 그 중 8개는 FC용 8/16/32Gbps에서 작동할 수 있는 통합 포트입니다. 4개의 포트는 레거시 연결을 위해 1/10/25Gbps에서 작동하며, 6개의 QSFP 포트는 40/100Gbps 업링크 포트 또는 브레이크아웃 포트로 사용됩니다. 100Gbps 어댑터를 지원하는 NetApp 스토리지 컨트롤러를 사용하여 100Gbps 종단간 네트워크 연결을 설정할 수 있습니다. 어댑터 및 플랫폼 지원에 대한 자세한 내용은 을 참조하십시오 "NetApp Hardware Universe를 참조하십시오".

포트에 대한 자세한 내용은 를 참조하십시오 "Cisco UCS 6454 Fabric 상호 연결" 데이터시트.

100Gb QSFP 데이터 모듈의 기술 사양은 을 참조하십시오 "Cisco 100GBASE QSFP 모듈 데이터시트".

Cisco UCS B-Series 섀시 옵션

Cisco UCS B-Series 블레이드를 사용하려면 Cisco UCS B-Series 섀시가 있어야 합니다. 아래 표에는 Cisco UCS BSeries 섀시 옵션이 설명되어 있습니다.

Cisco UCS B-Series 섀시	부품 번호	기술 사양
Cisco UCS 5108	N20-C6508	"Cisco UCS 5100 시리즈 블레이드 서버 섀시"

각 Cisco UCS 5108 블레이드 섀시에는 패브릭 인터커넥트에 대한 이중 연결을 제공하기 위해 2개의 Cisco UCS 2200/2300/2400 시리즈 IOM이 있어야 합니다.

Cisco UCS B-Series 블레이드 서버 옵션

Cisco UCS B-Series 블레이드 서버는 다양한 CPU, 메모리 및 I/O 옵션과 함께 반폭과 전폭으로 제공됩니다. 다음 표에 나열된 부품 번호는 기본 서버에 대한 것입니다. CPU, 메모리, 드라이브 또는 메자닌 어댑터 카드는 포함되지 않습니다. FlexPod 아키텍처에서는 다양한 구성 옵션을 사용할 수 있으며 지원됩니다.

Cisco UCS B-Series 블레이드	부품 번호	기술 사양
Cisco UCS B200 M6	UCSB-B200-M6	"Cisco UCS B200 M6 블레이드 서버"

에서 지원되는 경우 이전 세대의 Cisco UCS B 시리즈 블레이드를 FlexPod 아키텍처에서 사용할 수 있습니다 "Cisco UCS 하드웨어 및 소프트웨어 호환성 목록". Cisco UCS B-Series 블레이드 서버에도 유효한 SmartNet 지원 계약이 있어야 합니다.

Cisco UCS X-Series 섀시 옵션

Cisco UCS X-Series 컴퓨팅 노드를 사용하려면 Cisco UCS X-Series 섀시가 있어야 합니다. 다음 표에서는 Cisco UCS X-Series 섀시 옵션에 대해 설명합니다.

Cisco UCS X-Series 블레이드	부품 번호	기술 사양
Cisco UCS 9508 M6	UCSX-9508	"Cisco UCX9508 X 시리즈 섀시"

각 Cisco UCS 9508 섀시에는 패브릭 인터커넥트에 대한 이중 연결을 제공하기 위해 2개의 Cisco UCS 9108 IFM(Intelligent Fabric Module)이 있어야 합니다.

Cisco UCS X-Series 장치 옵션

Cisco UCS X-Series 컴퓨팅 노드는 다양한 CPU, 메모리 및 I/O 옵션과 함께 사용할 수 있습니다. 다음 표에 나열된 부품 번호는 기본 노드에 대한 것입니다. CPU, 메모리, 드라이브 또는 메자닌 어댑터 카드는 포함되지 않습니다. FlexPod 아키텍처에서는 다양한 구성 옵션을 사용할 수 있으며 지원됩니다.

Cisco UCS X-Series 컴퓨팅 노드	부품 번호	기술 사양
Cisco UCS X210c M6	UCSX-210C-M6	"Cisco UCS X210c M6 컴퓨팅 노드"

Cisco UCS C-Series 랙 서버 옵션

Cisco UCS C-Series 랙 서버는 다양한 CPU, 메모리, I/O 옵션과 함께 1개 및 2개의 랙 유닛(RU) 버전으로 제공됩니다. 아래 두 번째 표에 나열된 부품 번호는 기본 서버에 대한 것입니다. CPU, 메모리, 드라이브, PCIe(Peripheral Component Interconnect Express) 카드 또는 Cisco Fabric Extender는 포함되지 않습니다. FlexPod 아키텍처에서는 다양한 구성 옵션을 사용할 수 있으며 지원됩니다.

다음 표에는 Cisco UCS C-Series 랙 서버 옵션이 나와 있습니다.

Cisco UCS C-Series 랙 서버	부품 번호	기술 사양
Cisco UCS C220 M6	UCSC-C220-M6	"Cisco UCS C220 M6 랙 서버"
Cisco UCS C225 M6	UCSC - C225-M6	"Cisco UCS C225 M6 랙 서버"
Cisco UCS C240 M6	UCSC-C240-M6	"Cisco UCS C240 M6 랙 서버"
Cisco UCS C245 M6	UCSC-C245-M6	"Cisco UCS C245 M6 랙 서버"

에서 지원되는 경우 이전 세대의 Cisco UCS C-Series 서버를 FlexPod 아키텍처에서 사용할 수 있습니다 "Cisco UCS 하드웨어 및 소프트웨어 호환성 목록". Cisco UCS C-Series 서버도 유효한 SmartNet 지원 계약이 있어야 합니다.

Cisco Nexus 5000 시리즈 스위치 옵션

FlexPod 아키텍처에는 중복 Cisco Nexus 5000, 7000 또는 9000 시리즈 스위치가 필요합니다. 아래 표에 나열된 부품 번호는 Cisco Nexus 5000 시리즈 섀시용으로 SFP 모듈, 애드온 FC 또는 이더넷 모듈을 포함하지 않습니다.

Cisco Nexus 5000 시리즈 스위치	부품 번호	기술 사양
Cisco Nexus 56128P	N5K-C56128P	"Cisco Nexus 5600 플랫폼 스위치"
Cisco Nexus 5672UP-16G	N5K-C5672UP-16G	
Cisco Nexus 5596UP	N5K-C5596UP-FA	"Cisco Nexus 5548 및 5596 스위치"
Cisco Nexus 5548UP	N5K-C5548UP-FA	

Cisco Nexus 7000 시리즈 스위치 옵션

FlexPod 아키텍처에는 중복 Cisco Nexus 5000, 7000 또는 9000 시리즈 스위치가 필요합니다. 아래 표에 나열된 부품 번호는 Cisco Nexus 7000 Series 섀시용으로, SFP 모듈, 라인 카드 또는 전원 공급 장치는 포함되지 않지만 팬 트레이는 포함되어 있습니다.

Cisco Nexus 7000 시리즈 스위치	부품 번호	기술 사양
Cisco Nexus 7004	N7K-C7004	"Cisco Nexus 7000 4슬롯 스위치"
Cisco Nexus 7009	N7K-C7009	"Cisco Nexus 7000 9슬롯 스위치"
Cisco Nexus 7702	N7K-C7702	"Cisco Nexus 7700 2슬롯 스위치"
Cisco Nexus 7706	N77-C7706	"Cisco Nexus 7700 6슬롯 스위치"

Cisco Nexus 9000 시리즈 스위치 옵션

FlexPod 아키텍처에는 중복 Cisco Nexus 5000, 7000 또는 9000 시리즈 스위치가 필요합니다. 아래 표에 나열된 부품 번호는 Cisco Nexus 9000 시리즈 섀시용으로 SFP 모듈 또는 이더넷 모듈을 포함하지 않습니다.

Cisco Nexus 9000 시리즈 스위치	부품 번호	기술 사양
Cisco Nexus 93180YC-FX	N9K-C93180YC-FX	"Cisco Nexus 9300 시리즈 스위치"
Cisco Nexus 93180YC-EX	N9K-93180YC-EX	
Cisco Nexus 9336PQ ACI 척추	N9K-C9336PQ	
Cisco Nexus 9332PQ	N9K-C9332PQ	
Cisco Nexus 9336C-FX2	N9K-C9336C-FX2	
Cisco Nexus 92304QC	N9K-C92304QC	"Cisco Nexus 9200 시리즈 스위치"
Cisco Nexus 9236C	N9K-9236C	

일부 Cisco Nexus 9000 시리즈 스위치에는 다른 모델이 있습니다. 이러한 변종은 FlexPod 솔루션의 일부로 지원됩니다. Cisco Nexus 9000 시리즈 스위치의 전체 목록은 를 참조하십시오 "Cisco Nexus 9000 시리즈 스위치" 를 참조하십시오.

Cisco APIC 옵션

Cisco ACI를 배포할 때는 섹션에 있는 항목 외에 Cisco APIs 3개를 구성해야 합니다 "Cisco Nexus 9000 시리즈 스위치". Cisco APIC 크기에 대한 자세한 내용은 를 참조하십시오 "Cisco Application Centric Infrastructure 데이터시트 를 참조하십시오."

APIC 제품 사양에 대한 자세한 내용은 의 표 1에서 표 3을 참조하십시오 "Cisco Application Policy Infrastructure Controller 데이터시트 를 참조하십시오".

Cisco Nexus 패브릭 익스텐더 옵션

C-Series 서버를 사용하는 대규모 FlexPod 아키텍처에는 중복 Cisco Nexus 2000 시리즈 랙 마운트 FEX가 권장됩니다. 아래 표에는 몇 가지 Cisco Nexus FEX 옵션이 설명되어 있습니다. 대체 FEX 모델도 지원됩니다. 자세한 내용은 를 참조하십시오 "Cisco UCS 하드웨어 및 소프트웨어 호환성 목록".

Cisco Nexus 랙 마운트 **FEX**	부품 번호	기술 사양
Cisco Nexus 2232PP	N2K-C2232PP	"Cisco Nexus 2000 시리즈 패브릭 익스텐더"
Cisco Nexus 2232TM-E	N2K-C2232TM-E	
Cisco Nexus 2348UPQ	N2K-C2348UPQ	"Cisco Nexus 2300 플랫폼 패브릭 익스텐더"
Cisco Nexus 2348TQCisco Nexus 2348TQ-E	N2K-C2348TQN2K-C2348TQ-E	

Cisco MDS 옵션

Cisco MDS 스위치는 FlexPod 아키텍처의 선택적 구성 요소입니다. FC SAN용 Cisco MDS 스위치를 구축할 때는 이중화된 SAN 스위치 패브릭이 필요합니다. 아래 표에는 지원되는 Cisco MDS 스위치의 일부 부품 번호와 세부 정보가 나와 있습니다. 를 참조하십시오 "NetApp IMT를 참조하십시오" 및 "Cisco 하드웨어 및 소프트웨어 호환성 목록" 지원되는 SAN 스위치의 전체 목록을 확인하십시오.

Cisco MDS 9000 시리즈 스위치	부품 번호	설명
Cisco MDS 9148T	DS-C9148T-24IK	"Cisco MDS 9100 시리즈 스위치"
Cisco MDS 9132T	DS-C9132T-MEK9	
Cisco MDS 9396S	DS-C9396S-K9	"Cisco MDS 9300 시리즈 스위치"

Cisco 소프트웨어 라이센스 옵션

Cisco Nexus 스위치에서 스토리지 프로토콜을 활성화하려면 라이센스가 필요합니다. Cisco Nexus 5000 및 7000 시리즈 스위치 모두 SAN 부팅 구현에 FC 또는 FCoE 프로토콜을 활성화하려면 스토리지 서비스 라이센스가 필요합니다. Cisco Nexus 9000 시리즈 스위치는 현재 FC 또는 FCoE를 지원하지 않습니다.

필요한 라이선스와 해당 라이선스의 부품 번호는 FlexPod 솔루션의 각 구성 요소에 대해 선택하는 옵션에 따라 달라집니다. 예를 들어, 소프트웨어 라이센스 부품 번호는 포트 수와 선택한 Cisco Nexus 5000 또는 7000 시리즈 스위치에 따라 다릅니다. 정확한 부품 번호는 영업 담당자에게 문의하십시오. 아래 표에는 Cisco 소프트웨어 라이센스 옵션이 나열되어 있습니다.

Cisco 소프트웨어 라이센스	부품 번호	라이센스 정보
Cisco Nexus 5500 스토리지 라이센스, 8, 48 및 96포트	N55-8P-SSK9/N55-48P-SSK9/N55-96P-SSK9	"Cisco NX-OS 소프트웨어 기능 라이센스 등록"
Cisco Nexus 5010/5020 스토리지 프로토콜 라이센스	N5010-SSK9/N5020-SSK9	
Cisco Nexus 5600 스토리지 프로토콜 라이센스	N56-16p-SSK9/N5672-72p-SSK9/N56128-128P-SSK9	
Cisco Nexus 7000 스토리지 엔터프라이즈 라이센스	N7K-SAN1K9	
Cisco Nexus 9000 엔터프라이즈 서비스 라이센스	N95-LAN1K9/N93-LAN1K9	

Cisco 지원 라이센스 옵션

FlexPod 아키텍처의 모든 Cisco 장비에는 유효한 SmartNet 지원 계약이 필요합니다.

각 제품에 따라 다를 수 있으므로 해당 라이선스에 필요한 라이센스와 부품 번호는 영업 담당자가 확인해야 합니다. 아래 표에는 Cisco 지원 라이센스 옵션이 나열되어 있습니다.

Cisco 지원 라이센스	사용권 안내서
Smart Net Total Care 현장지원 프리미엄	"Cisco Smart Net Total Care 서비스"

NetApp 구성 요소

NetApp 스토리지 컨트롤러는 부팅 및 애플리케이션 데이터 스토리지 모두를 위한 FlexPod 아키텍처의 스토리지 기반을 제공합니다. NetApp의 구성 요소에는 스토리지 컨트롤러, 클러스터 인터커넥트 스위치, 드라이브 및 디스크 쉘프, 라이센스 옵션이 있습니다.

NetApp 스토리지 컨트롤러 옵션

FlexPod 아키텍처에는 중복 NetApp FAS, AFF 또는 AFF ASA 컨트롤러가 필요합니다. 컨트롤러는 ONTAP 소프트웨어를 실행합니다. 스토리지 컨트롤러를 주문할 경우 컨트롤러에 기본 소프트웨어 버전이 사전 로드될 수 있습니다. ONTAP의 경우 전체 클러스터를 주문합니다. 완벽한 클러스터에는 스토리지 컨트롤러 쌍과 클러스터 인터커넥트(스위치 또는 스위치 없음)가 포함됩니다.

선택한 스토리지 플랫폼에 따라 다양한 옵션과 구성을 사용할 수 있습니다. 이러한 추가 구성 요소에 대한 자세한 내용은 영업 담당자에게 문의하십시오.

아래 표에 나열된 컨트롤러 제품군은 Cisco Nexus 스위치에 대한 연결이 원활하므로 FlexPod 데이터 센터 솔루션에 사용하기에 적합합니다. 를 참조하십시오 "NetApp Hardware Universe를 참조하십시오" 각 컨트롤러 모델에 대한 자세한 호환성 정보

스토리지 컨트롤러 제품군	기술 사양
AFF A 시리즈	"AFF A 시리즈 문서"
AFF ASA A 시리즈	"AFF ASA A 시리즈 문서"
FAS 시리즈	"FAS 시리즈 문서"

클러스터 인터커넥트 스위치 옵션

다음 표에는 FlexPod 아키텍처에 사용할 수 있는 Nexus 클러스터 인터커넥트 스위치가 나와 있습니다. 또한 FlexPod는 구축 중인 ONTAP 버전과 호환되는 비 Cisco 스위치를 포함하여 ONTAP에서 지원하는 모든 클러스터 스위치를 지원합니다. 를 참조하십시오 "NetApp Hardware Universe를 참조하십시오" 특정 스위치 모델에 대한 추가 호환성 세부 정보를 확인하십시오.

클러스터 인터커넥트 스위치	기술 사양
Cisco Nexus 3132Q-V	"NetApp 설명서: Cisco Nexus 3132Q-V 스위치"
Cisco Nexus 9336C-FX2	"NetApp 설명서: Cisco Nexus 9336C-FX2 스위치"

NetApp 디스크 쉘프 및 드라이브 옵션

모든 스토리지 컨트롤러에 NetApp 디스크 쉘프가 하나 이상 필요합니다.

선택한 NetApp 쉘프 유형에 따라 해당 쉘프 내에서 사용 가능한 드라이브 유형이 결정됩니다.

모든 디스크 쉘프와 디스크 부품 번호는 세일즈 담당자에게 문의하십시오.

지원되는 드라이브에 대한 자세한 내용을 보려면 다음 표에서 NetApp Hardware Universe 링크를 클릭한 다음 지원되는 드라이브 를 선택합니다.

디스크 쉘프	기술 사양
DS224C	"NetApp Hardware Universe의 디스크 쉘프 및 스토리지 미디어 지원 드라이브"
DS212C	
DS460C	
NS224	

NetApp 소프트웨어 라이센스 옵션

다음 표에는 FlexPod 데이터 센터 아키텍처에 사용할 수 있는 NetApp 소프트웨어 라이센스 옵션이 나와 있습니다. NetApp 소프트웨어는 FAS 및 AFF 컨트롤러 레벨에서 라이센스가 부여됩니다.

NetApp 소프트웨어 라이센스	부품 번호	기술 사양
SW, 전체 BNDL(컨트롤러), -C	SW-8XXX-COMP-BNDL-C	"제품 라이브러리 A – Z"
SW, ONTAP Essentials(컨트롤러), -C	SW-8XXX-ONTAP9-C	

NetApp은 라이센스 옵션을 지원합니다

SupportEdge Premium 아키텍처에는 NetApp FlexPod 라이센스가 필요하지만, 라이센스에 대한 부품 번호는 FlexPod 설계에서 선택하는 옵션에 따라 달라집니다. 예를 들어, 소프트웨어 라이센스 부품 번호는 선택한 FAS 컨트롤러에 따라 다릅니다. 개별 지원 라이센스에 대한 정확한 부품 번호에 대한 자세한 내용은 영업 담당자에게 문의하십시오. 아래 표에는 SupportEdge 라이센스의 예가 나와 있습니다.

NetApp은 라이센스를 제공합니다	부품 번호	기술 사양
SupportEdge Premium 4시간 현장 - 개월:36	CS-O2-4시간	"NetApp SupportEdge Premium를 참조하십시오"

전원 및 케이블 연결 요구 사항

FlexPod 설계에는 전원 및 케이블 연결에 대한 최소 요구 사항이 있습니다.

전원 요구 사항

FlexPod 데이터 센터의 전원 요구 사항은 FlexPod 데이터 센터 구성이 설치된 위치에 따라 다릅니다.

필요한 최대 전력과 기타 자세한 전력 정보에 대한 자세한 내용은 섹션에 나와 있는 각 하드웨어 구성 요소의 기술 사양을 참조하십시오 "기술 사양 및 참조: 하드웨어 구성 요소".

Cisco UCS 전원 데이터에 대한 자세한 내용은 를 참조하십시오 "Cisco UCS 전력 계산기".

NetApp 스토리지 컨트롤러 전원 데이터에 대한 자세한 내용은 를 참조하십시오 "NetApp Hardware Universe를

참조하십시오". 플랫폼 에서 구성에 사용할 스토리지 플랫폼(FAS/V-Series 또는 AFF)을 선택합니다. ONTAP 버전 및 스토리지 컨트롤러를 선택하고 결과 표시 버튼을 클릭합니다.

최소 케이블 요구 사항

필요한 케이블 및 어댑터의 수와 유형은 FlexPod 데이터 센터 구축에 따라 다릅니다. 케이블 유형, 트랜시버 유형 및 번호는 요구 사항에 따라 설계 프로세스 중에 결정됩니다. 아래 표에는 필요한 최소 케이블 수가 나열되어 있습니다.

하드웨어	모델 번호	케이블이 필요합니다
Cisco UCS 섀시	Cisco UCS 5108	Cisco UCS 2104XP, 2204XP 또는 2208XP 모듈당 2개 이상의 쌍축 케이블
Cisco UCS Fabric 상호 연결	Cisco UCS 6248UP	• 관리 포트용 Cat5e 케이블 2개 • L1, L2 상호 연결을 위한 Cat5e 케이블 2개, 패브릭 상호 연결 한 쌍당 • Fabric 상호 연결당 2축 케이블 4개 이상 • 패브릭 인터커넥트당 FC 케이블 4개 이상
	Cisco UCS 6296UP	Cisco UCS 6332-16UP
	Cisco UCS 6454	Cisco UCS 6332
	• 관리 포트용 Cat5e 케이블 2개 • L1, L2 상호 연결을 위한 Cat5e 케이블 2개, 패브릭 상호 연결 한 쌍당 • Fabric 상호 연결당 2축 케이블 4개 이상	Cisco UCS 6324
	• 10/100/1000Mbps 관리 포트 2개 • Fabric 상호 연결당 2개 이상의 Twinax 케이블	Cisco Nexus 5000 및 7000 시리즈 스위치
	Cisco Nexus 5000 시리즈	
• 스위치당 10GbE Fibre 또는 Twinax 케이블 2개 이상 • 스위치당 FC 케이블 2개 이상(FC/FCoE 연결이 필요한 경우)	Cisco Nexus 7000 시리즈	Cisco Nexus 9000 시리즈 스위치

하드웨어	모델 번호	케이블이 필요합니다
Cisco Nexus 9000 시리즈	스위치당 10GbE 케이블 2개 이상	NetApp FAS 컨트롤러
AFF A 시리즈	• 스토리지 컨트롤러당 하나의 SAS 또는 SATA 케이블 • 레거시 FC를 사용하는 경우 컨트롤러당 최소 2개의 FC 케이블을 사용해야 합니다 • 컨트롤러당 최소 2개의 10GbE 케이블 • 컨트롤러당 관리용 GbE 케이블 1개 이상 • ONTAP의 경우 클러스터 인터커넥트 스위치 쌍당 짧은 Twinax 케이블 8개가 필요합니다	
FAS 시리즈	제공합니다	DS212C
디스크 쉘프당 SAS, SATA 또는 FC 케이블 2개		DS224C
		DS460C
		NS224

기술 사양 및 참조 자료

기술 사양은 섀시, FEX, 서버, 스위치, 스위치 등 FlexPod 솔루션의 하드웨어 구성 요소에 대한 세부 정보를 제공합니다. 및 스토리지 컨트롤러.

Cisco UCS B-Series 블레이드 서버 섀시

아래 표와 같은 Cisco UCS B-Series 블레이드 서버 섀시의 기술 사양에는 다음 구성요소가 포함됩니다.

- 랙 유닛 수
- 최대 블레이드 수
- 통합 패브릭 기능
- 서버당 미드플레인 I/O 대역폭
- FEX의 I/O 베이 수입니다

구성 요소	**Cisco UCS 5100** 시리즈 블레이드 서버 섀시
랙 유닛	6
최대 전체 폭 블레이드	4
최대 반폭 블레이드	8
통합 패브릭 지원	예
미드플레인 I/O	서버당 최대 80Gbps의 I/O 대역폭

구성 요소	**Cisco UCS 5100** 시리즈 블레이드 서버 섀시
FEX용 I/O 베이	Cisco UCS 2104XP, 2204/8XP, 2408XP 및 2304 FEX용 베이 2개

자세한 내용은 를 참조하십시오 "Cisco UCS 5100 시리즈 블레이드 서버 섀시 데이터시트".

Cisco UCS B-Series 블레이드 서버

아래 표와 같은 Cisco UCS B-Series 블레이드 서버의 기술 사양은 다음과 같습니다.

- 프로세서 소켓 수입니다
- 프로세서 지원
- 메모리 용량
- 크기 및 속도
- SAN 부팅 지원
- 메자닌 어댑터 슬롯 수
- I/O 최대 처리량
- 폼 팩터
- 섀시당 최대 서버 수입니다

구성 요소	**Cisco UCS** 데이터시트 를 참조하십시오
Cisco UCS B200 M6	"Cisco UCS B200 M6 블레이드 서버"

Cisco UCS C-Series 랙 서버

Cisco UCS C-Series 랙 서버의 기술 사양에는 프로세서 지원, 최대 메모리 용량, PCIe 슬롯 수, 폼 팩터 크기 등이 포함됩니다. 호환되는 UCS 서버 모델에 대한 자세한 내용은 를 참조하십시오 "Cisco 하드웨어 호환성" 목록. 다음 표에서는 C-Series 랙 서버 데이터 시트 및 Cisco UCS C-Series 섀시 옵션을 각각 보여 줍니다.

구성 요소	**Cisco UCS** 데이터시트 를 참조하십시오
Cisco UCS C220 M6	"Cisco UCS C220 M6 랙 서버"
Cisco UCS C225 M6	"Cisco UCS C225 M6 랙 서버"
Cisco UCS C240 M6	"Cisco UCS C240 M6 랙 서버"
Cisco UCS C245 M6	"Cisco UCS C245 M6 랙 서버"

Cisco UCS X-Series 섀시

아래 표와 같은 Cisco UCS X-Series 섀시의 기술 사양에는 다음 구성요소가 포함됩니다.

- 랙 유닛 수
- 최대 노드 수입니다
- 통합 패브릭 기능

- IFM의 I/O 베이 수입니다

구성 요소	**Cisco UCS 9508 X-Series** 컴퓨팅 노드 섀시
랙 유닛	7
최대 노드 수입니다	8
통합 패브릭 지원	예
IFM용 I/O 베이	Cisco UCS 9108 IFM(Intelligent Fabric Module)용 베이 2개

자세한 내용은 를 참조하십시오 "Cisco UCS X9508 X 시리즈 섀시 데이터시트".

Cisco UCS X-Series 컴퓨팅 노드

다음 표에 나와 있는 것처럼 Cisco UCS X-Series 컴퓨팅 노드의 기술 사양에는 다음 구성요소가 포함됩니다.

- 프로세서 소켓 수입니다
- 프로세서 지원
- 메모리 용량
- 크기 및 속도
- SAN 부팅 지원
- 메자닌 어댑터 슬롯 수
- I/O 최대 처리량
- 폼 팩터
- 섀시당 최대 컴퓨팅 노드 수

구성 요소	Cisco UCS 데이터시트 를 참조하십시오
Cisco UCS X210c M6	"Cisco UCS X210c M6 컴퓨팅 노드"

FlexPod AI, ML 및 **DL**용 **GPU** 권장 사항

아래 표에 나열된 Cisco UCS C-Series 랙 서버는 AI, ML 및 DL 워크로드를 호스팅하는 FlexPod 아키텍처에서 사용할 수 있습니다. Cisco UCS C480 ML M5 서버는 AI, ML 및 DL 워크로드를 위해 특별 제작되었고 NVIDIA의 SXM2 기반 GPU를 사용하는 한편, 다른 서버는 PCIe 기반 GPU를 사용합니다.

아래 표에는 이러한 서버와 함께 사용할 수 있는 권장 GPU도 나와 있습니다.

서버	**GPU**를 만나보십시오
Cisco UCS C220 M6	NVIDIA T4
Cisco UCS C225 M6	NVIDIA T4
Cisco UCS C240 M6	NVIDIA Tesla A10, A100
Cisco UCS C245 M6	NVIDIA Tesla A10, A100

Cisco UCS B-Series 블레이드 서버용 Cisco UCS VIC 어댑터

Cisco UCS B-Series 블레이드 서버용 Cisco UCS VIC(Virtual Interface Card) 어댑터의 기술 사양에는 다음 구성요소가 포함됩니다.

- 업링크 포트 수
- 포트당 성능(IOPS)
- 전원
- 블레이드 포트 수입니다
- 하드웨어 오프로드
- 단일 루트 입출력 가상화(SR-IOV) 지원

현재 검증된 모든 FlexPod 아키텍처는 Cisco UCS VIC를 사용합니다. 다른 어댑터는 NetApp에 나열된 경우 지원됩니다 "IMT" 및 는 FlexPod 배포와 호환되지만 해당 참조 아키텍처에 요약된 모든 기능을 제공하지 못할 수도 있습니다. 다음 표에서는 Cisco UCS VIC 어댑터 데이터시트를 보여 줍니다.

구성 요소	**Cisco UCS** 데이터시트 를 참조하십시오
Cisco UCS 가상 인터페이스 어댑터	"Cisco UCS VIC 데이터시트"

Cisco UCS 패브릭 인터커넥트

Cisco UCS 패브릭 인터커넥트를 위한 기술 사양에는 폼 팩터 크기, 총 포트 수 및 확장 슬롯 수, 처리량 용량이 포함됩니다. 다음 표에서는 Cisco UCS 패브릭 인터커넥트 데이터시트를 보여 줍니다.

구성 요소	**Cisco UCS** 데이터시트 를 참조하십시오
Cisco UCS 6248UP	"Cisco UCS 6200 시리즈 패브릭 인터커넥트"
Cisco UCS 6296UP	
Cisco UCS 6324	"Cisco UCS 6324 패브릭 인터커넥트"
Cisco UCS 6300	"Cisco UCS 6300 Series Fabric Interconnect"
Cisco UCS 6454	"Cisco UCS 6400 시리즈 패브릭 인터커넥트"

Cisco Nexus 5000 시리즈 스위치

폼 팩터 크기, 총 포트 수, 계층 3 모듈 및 부속 카드 지원을 포함한 Cisco Nexus 5000 시리즈 스위치의 기술 사양은 각 모델 제품군의 데이터시트에 포함되어 있습니다. 이러한 데이터시트는 다음 표에서 확인할 수 있습니다.

구성 요소	**Cisco Nexus** 데이터시트 를 참조하십시오
Cisco Nexus 5548UP	"Cisco Nexus 5548UP 스위치"
Cisco Nexus 5596UP(2U)	"Cisco Nexus 5596UP 스위치"
Cisco Nexus 56128P	"Cisco Nexus 56128P 스위치"
Cisco Nexus 5672UP	"Cisco Nexus 5672UP 스위치"

Cisco Nexus 7000 시리즈 스위치

폼 팩터 크기와 최대 포트 수를 포함한 Cisco Nexus 7000 시리즈 스위치의 기술 사양은 각 모델 제품군의 데이터시트에 포함되어 있습니다. 이러한 데이터시트는 다음 표에서 확인할 수 있습니다.

구성 요소	Cisco Nexus 데이터시트 를 참조하십시오
Cisco Nexus 7004	"Cisco Nexus 7000 시리즈 스위치"
Cisco Nexus 7009	
Cisco Nexus 7010	
Cisco Nexus 7018	
Cisco Nexus 7702	"Cisco Nexus 7700 시리즈 스위치"
Cisco Nexus 7706	
Cisco Nexus 7710	
Cisco Nexus 7718	

Cisco Nexus 9000 시리즈 스위치

Cisco Nexus 9000 시리즈 스위치의 기술 사양은 각 모델의 데이터시트에 포함되어 있습니다. 사양에는 폼 팩터 크기, 수퍼바이저, 패브릭 모듈 및 라인 카드 슬롯 수, 최대 포트 수가 포함됩니다. 이러한 데이터시트는 다음 표에서 확인할 수 있습니다.

구성 요소	Cisco Nexus 데이터시트 를 참조하십시오
Cisco Nexus 9000 시리즈	"Cisco Nexus 9000 시리즈 스위치"
Cisco Nexus 9500 시리즈	"Cisco Nexus 9500 시리즈 스위치"
Cisco Nexus 9300 시리즈	"Cisco Nexus 9300 시리즈 스위치"
Cisco Nexus 9336PQ ACI 스파인 스위치	"Cisco Nexus 9336PQ ACI 스파인 스위치"
Cisco Nexus 9200 시리즈	"Cisco Nexus 9200 플랫폼 스위치"

Cisco 애플리케이션 정책 인프라 컨트롤러

Cisco ACI를 구축할 경우 섹션에 있는 항목 외에 추가로 Cisco ACI를 배포합니다 "Cisco Nexus 9000 시리즈 스위치 "세 개의 Cisco APIs를 구성해야 합니다. 다음 표에는 Cisco APIC 데이터시트가 나와 있습니다.

구성 요소	Cisco Application Policy Infrastructure 데이터시트입니다
Cisco 애플리케이션 정책 인프라 컨트롤러	"Cisco APIC 데이터시트 를 참조하십시오"

Cisco Nexus 패브릭 익스텐더 세부 정보

Cisco Nexus FEX의 기술 사양에는 속도, 고정 포트 및 링크 수, 폼 팩터 크기 등이 포함됩니다.

다음 표에는 Cisco Nexus 2000 Series FEX 데이터시트가 나와 있습니다.

구성 요소	**Cisco Nexus** 패브릭 익스텐더 데이터시트
Cisco Nexus 2000 시리즈 패브릭 익스텐더	"Nexus 2000 시리즈 FEX 데이터시트"

SFP 모듈

SFP 모듈에 대한 자세한 내용은 다음 리소스를 참조하십시오.

- Cisco 10Gb SFP에 대한 자세한 내용은 를 참조하십시오 "Cisco 10기가비트 모듈".
- Cisco 25GB SFP에 대한 자세한 내용은 를 참조하십시오 "Cisco 25 기가비트 모듈".
- Cisco QSFP 모듈에 대한 자세한 내용은 을 참조하십시오 "Cisco 40GBASE QSFP 모듈 데이터시트".
- Cisco 100GB SFP에 대한 자세한 내용은 를 참조하십시오 "Cisco 100 기가비트 모듈".
- Cisco FC SFP 모듈에 대한 자세한 내용은 을 참조하십시오 "Cisco MDS 9000 Family Pluggable 트랜시버 데이터시트입니다".
- 지원되는 모든 Cisco SFP 및 트랜시버 모듈에 대한 자세한 내용은 을 참조하십시오 "Cisco SFP 및 SFP+ 트랜시버 모듈 설치 참고 사항" 및 "Cisco 트랜시버 모듈".

NetApp 스토리지 컨트롤러

NetApp 스토리지 컨트롤러의 기술 사양에는 다음 구성요소가 포함됩니다.

- 섀시 구성
- 랙 유닛 수
- 메모리 용량
- NetApp FlashCache 캐싱
- 애그리게이트 크기
- 볼륨 크기
- LUN 수입니다
- 지원되는 네트워크 스토리지
- 최대 NetApp FlexVol 볼륨 수입니다
- 지원되는 최대 SAN 호스트 수입니다
- 최대 스냅샷 복사본 수

FAS 시리즈

사용 가능한 모든 FAS 스토리지 컨트롤러 모델은 FlexPod 데이터 센터에서 사용할 수 있습니다. 모든 FAS 시리즈 스토리지 컨트롤러에 대한 자세한 사양은 에서 확인할 수 있습니다 "NetApp Hardware Universe를 참조하십시오". 특정 FAS 모델에 대한 자세한 내용은 다음 표에 나와 있는 플랫폼별 설명서를 참조하십시오.

구성 요소	**FAS** 시리즈 컨트롤러 플랫폼 설명서
FAS9000 시리즈	"FAS9000 시리즈 데이터시트"
FAS8700 시리즈	"FAS8700 시리즈 데이터시트"

구성 요소	**FAS** 시리즈 컨트롤러 플랫폼 설명서
FAS8300 시리즈	"FAS8300 시리즈 데이터시트"
500f 시리즈	"FAS500f 시리즈 데이터시트 를 참조하십시오"
FAS2700 시리즈	"FAS2700 시리즈 데이터시트"

AFF A 시리즈

NetApp AFF A-Series 스토리지 컨트롤러의 모든 현재 모델은 FlexPod에서 사용할 수 있습니다. 추가 정보는 "AFF 기술 사양" 데이터시트와 에서 "NetApp Hardware Universe를 참조하십시오" 확인할 수 있습니다. 특정 AFF 모델에 대한 자세한 내용은 다음 표에 나와 있는 플랫폼별 설명서를 참조하십시오.

구성 요소	**AFF A-Series** 컨트롤러 플랫폼 설명서
NetApp AFF A800	"AFF A800 플랫폼 문서"
NetApp AFF A700	"AFF A700 플랫폼 문서"
NetApp AFF A700s를 참조하십시오	"AFF A700s 플랫폼 문서"
NetApp AFF A400	"AFF A400 플랫폼 문서"
NetApp AFF A250	"AFF A250 플랫폼 문서"

AFF ASA A 시리즈

NetApp AFF ASA A-Series 스토리지 컨트롤러의 모든 현재 모델은 FlexPod에서 사용할 수 있습니다. 자세한 내용은 All SAN 어레이 설명서 리소스, ONTAP AFF All SAN 어레이 시스템 기술 보고서 및 NetApp Hardware Universe에서 확인할 수 있습니다. 특정 AFF 모델에 대한 자세한 내용은 다음 표에 나와 있는 플랫폼별 설명서를 참조하십시오.

구성 요소	**AFF A-Series** 컨트롤러 플랫폼 설명서
NetApp AFF ASA A800	"AFF ASA A800 플랫폼 문서"
NetApp AFF ASA A700	"AFF ASA A700 플랫폼 문서"
NetApp AFF ASA A400	"AFF ASA A400 플랫폼 문서"
NetApp AFF ASA A250	"AFF ASA A250 플랫폼 문서"
NetApp AFF ASA A220을 참조하십시오	"AFF ASA A220 플랫폼 문서"

제공합니다

NetApp 디스크 쉘프의 기술 사양에는 폼 팩터 크기, 엔클로저당 드라이브 수, 쉘프 I/O 모듈 등이 포함되어 있으며, 이 설명서는 다음 표를 참조하십시오. 자세한 내용은 를 참조하십시오 "NetApp 디스크 쉘프 및 스토리지 미디어 기술 사양" 및 "NetApp Hardware Universe를 참조하십시오".

구성 요소	**NetApp FAS/AFF** 디스크 쉘프 문서
NetApp DS212C 디스크 쉘프	"DS212C 디스크 쉘프 문서"
NetApp DS224C 디스크 쉘프	"DS224C 디스크 쉘프 문서"
NetApp DS460C 디스크 쉘프	"DS460C 디스크 쉘프 문서"
NetApp NS224 NVMe-SSD 디스크 쉘프	"NS224 디스크 쉘프 문서"

NetApp 드라이브

NetApp 드라이브의 기술 사양에는 폼 팩터 크기, 디스크 용량, 디스크 RPM, 지원 컨트롤러 및 ONTAP 버전 요구사항이 포함됩니다. 이러한 사양은 의 드라이브 섹션에서 찾을 수 있습니다 "NetApp Hardware Universe를 참조하십시오".

레거시 장비

FlexPod은 현재 Cisco 및 NetApp에서 판매하기 위한 기존 장비와 새 장비를 사용할 수 있는 유연한 솔루션입니다. Cisco와 NetApp의 특정 장비 모델이 EOL(End of Life)으로 지정되는 경우가 있습니다.

이러한 장비 모델은 더 이상 사용할 수 없지만, EOA(End-of-Availability) 날짜 이전에 이러한 모델 중 하나를 구입한 경우 FlexPod 구성에서 해당 장비를 사용할 수 있습니다. FlexPod에서 더 이상 판매되지 않는 기존 장비 모델의 전체 목록은 에서 참조할 수 있습니다 "NetApp 서비스 및 지원 제품 프로그램 이용 종료 색인".

기존 Cisco 장비에 대한 자세한 내용은 에 대한 Cisco EOL 및 EOA 공지를 참조하십시오 "Cisco UCS C-Series 랙 서버", "Cisco UCS B-Series 블레이드 서버", 및 "Nexus 스위치".

레거시 FC 패브릭에는 다음이 포함됩니다.

- 2GB 패브릭
- 4GB 패브릭

레거시 소프트웨어에는 다음이 포함됩니다.

- 7-Mode, 7.3.5 이상에서 작동하는 NetApp Data ONTAP
- ONTAP 8.1.x ~ 9.0.x
- Cisco UCS Manager 1.3 이상
- Cisco UCS Manager 2.1 ~ 2.2.7

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대한 자세한 내용은 다음 문서 및 웹 사이트를 참조하십시오.

- NetApp 제품 설명서

  "https://docs.netapp.com/"

- NetApp 지원 커뮤니케이션

  "https://mysupport.netapp.com/info/communications/index.html"

- NetApp 상호 운용성 매트릭스 툴(IMT)

  "https://mysupport.netapp.com/matrix/#welcome"

- NetApp Hardware Universe를 참조하십시오

  "https://hwu.netapp.com/"

- NetApp 지원

  "https://mysupport.netapp.com/"

FlexPod 데이터 센터

NetApp SnapMirror 비즈니스 연속성 및 ONTAP 9.10이 설치된 FlexPod 데이터 센터

TR-4920: NetApp SnapMirror 비즈니스 연속성 및 ONTAP 9.10을 지원하는 FlexPod 데이터 센터

Jyh-shing Chen, NetApp

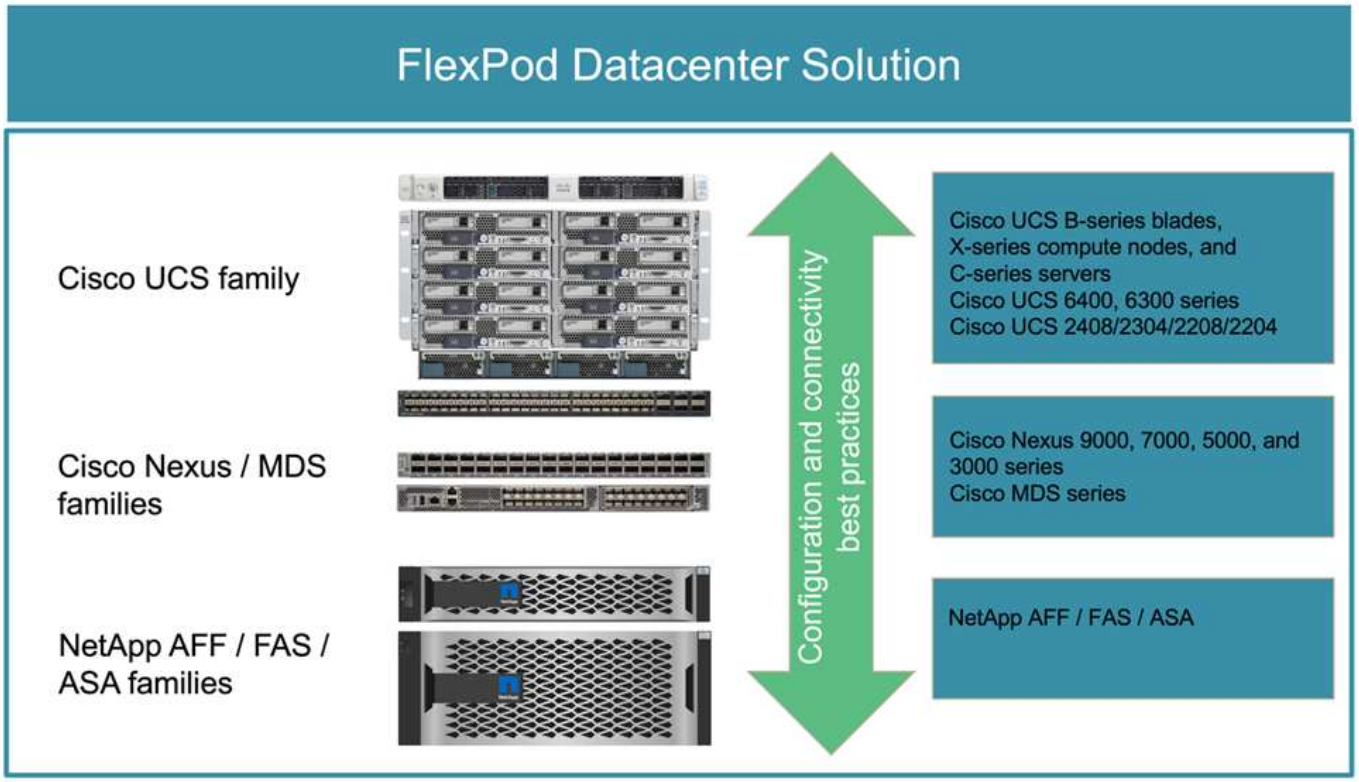
소개

FlexPod 솔루션

FlexPod은 Cisco와 NetApp의 다음 구성 요소를 포함하는 모범 사례 통합 인프라 데이터 센터 아키텍처입니다.

- Cisco UCS(Cisco Unified Computing System)
- Cisco Nexus 및 MDS 스위치 제품군
- NetApp FAS, NetApp AFF 및 NetApp ASA(All SAN Array) 시스템

다음 그림에서는 FlexPod 솔루션을 만드는 데 사용되는 일부 구성 요소를 보여 줍니다. 이러한 구성요소는 Cisco와 NetApp의 모범 사례에 따라 연결 및 구성되었으므로 다양한 엔터프라이즈 워크로드를 안심하고 실행할 수 있는 이상적인 플랫폼을 제공합니다.



CVD(Cisco Validated Design) 및 NVA(NetApp Verified Architecture)의 대규모 포트폴리오를 사용할 수 있습니다.

CVD 및 NVA는 모든 주요 데이터 센터 워크로드를 다루며, NetApp과 Cisco on FlexPod 솔루션 간의 지속적인 협력 및 혁신을 통해 얻은 결과입니다.

FlexPod CVD 및 NVA는 제작 프로세스에서 포괄적인 테스트 및 검증을 통합했으며, 파트너와 고객이 FlexPod 솔루션을 배포하고 채택하도록 도와주는 참조 솔루션 아키텍처 설계와 단계별 배포 가이드를 제공합니다. 기업은 이러한 CVD 및 NVA를 설계 및 구현 가이드로 사용하여 위험을 줄이고 솔루션 다운타임을 줄이며 구축하는 FlexPod 솔루션의 가용성, 확장성, 유연성 및 보안을 강화할 수 있습니다.

표시된 각 FlexPod 구성요소 제품군(Cisco UCS, Cisco Nexus/MDS 스위치 및 NetApp 스토리지)은 FlexPod의 구성 및 연결 모범 사례에 필요한 기능을 지원하는 동시에 인프라를 스케일업 또는 스케일다운할 수 있는 플랫폼 및 리소스 옵션을 제공합니다. 또한 FlexPod는 추가 FlexPod 스택을 롤아웃하여 일관된 다중 구축이 필요한 환경을 위해 스케일아웃할 수 있습니다.

재해 복구 및 비즈니스 연속성

기업에서 재해에 따라 애플리케이션 및 데이터 서비스를 빠르게 복구할 수 있도록 다양한 방법을 채택할 수 있습니다. DR(재해 복구) 및 BC(비즈니스 연속성) 계획을 세우고, 비즈니스 목표를 충족하는 솔루션을 구현하며, 재해 시나리오를 정기적으로 테스트하여 재해 상황이 발생한 후에도 재해를 복구하고 중요한 비즈니스 서비스를 계속할 수 있습니다.

회사마다 애플리케이션 및 데이터 서비스의 유형에 따라 DR 및 BC 요구사항이 다를 수 있습니다. 일부 애플리케이션과 데이터는 긴급 상황이나 재해 상황에서 필요하지 않을 수 있으며, 비즈니스 요구사항을 지원하기 위해 계속 사용 가능한 애플리케이션이 필요할 수도 있습니다.

미션 크리티컬 애플리케이션 및 데이터 서비스를 사용할 수 없을 때 비즈니스에 방해가 될 수 있는 경우, 비즈니스에 고려해야 할 유지 관리 및 재해 시나리오 유형 등의 질문에 대해 신중하게 평가해야 합니다. 재해 발생 시 기업이 손실을 감수할 수 있는 데이터의 양과 복구 시간이 얼마나 빨라야 하고 얼마나 빨리 발생해야 하는지를 나타냅니다.

수익 창출을 위해 데이터 서비스를 이용하는 기업의 경우 다양한 단일 장애 지점 시나리오뿐만 아니라 지속적인 비즈니스 운영을 위한 사이트 중단 재해 시나리오를 견딜 수 있는 솔루션으로 데이터 서비스를 보호해야 할 필요가 있습니다.

복구 지점 목표 및 복구 시간 목표

복구 지점 목표(RPO)는 손실을 감수할 수 있는 데이터의 양 또는 데이터를 복구할 수 있는 시점을 측정합니다. 일일 백업 계획을 사용하면 재해 발생 시 마지막 백업 이후 데이터 변경 사항이 손실될 수 있기 때문에 하루 동안 데이터를 손실할 수 있습니다. 비즈니스 크리티컬 및 미션 크리티컬 데이터 서비스의 경우, 데이터 손실 없이 데이터를 보호하기 위해 제로 RPO와 관련 계획 및 인프라가 필요할 수 있습니다.

복구 시간 목표(RTO)는 데이터를 사용할 수 없는 상태로 유지하는 데 걸리는 시간 또는 데이터 서비스를 신속하게 백업해야 하는 시간을 측정합니다. 예를 들어, 회사의 크기로 인해 특정 데이터 집합에 기존 테이프를 사용하는 백업 및 복구 구현이 있을 수 있습니다. 따라서 백업 테이프에서 데이터를 복원하려면 인프라 오류가 발생한 경우 몇 시간이나 며칠이 걸릴 수 있습니다. 또한 시간 고려 사항에는 데이터 복원과 함께 인프라를 백업할 시간도 포함되어야 합니다. 미션 크리티컬 데이터 서비스의 경우 매우 낮은 RTO가 필요할 수 있으므로 비즈니스 연속성을 위해 데이터 서비스를 신속하게 온라인으로 전환하는 데 몇 초 또는 몇 분의 장애 조치 시간도 허용할 수 있습니다.

SM - BC

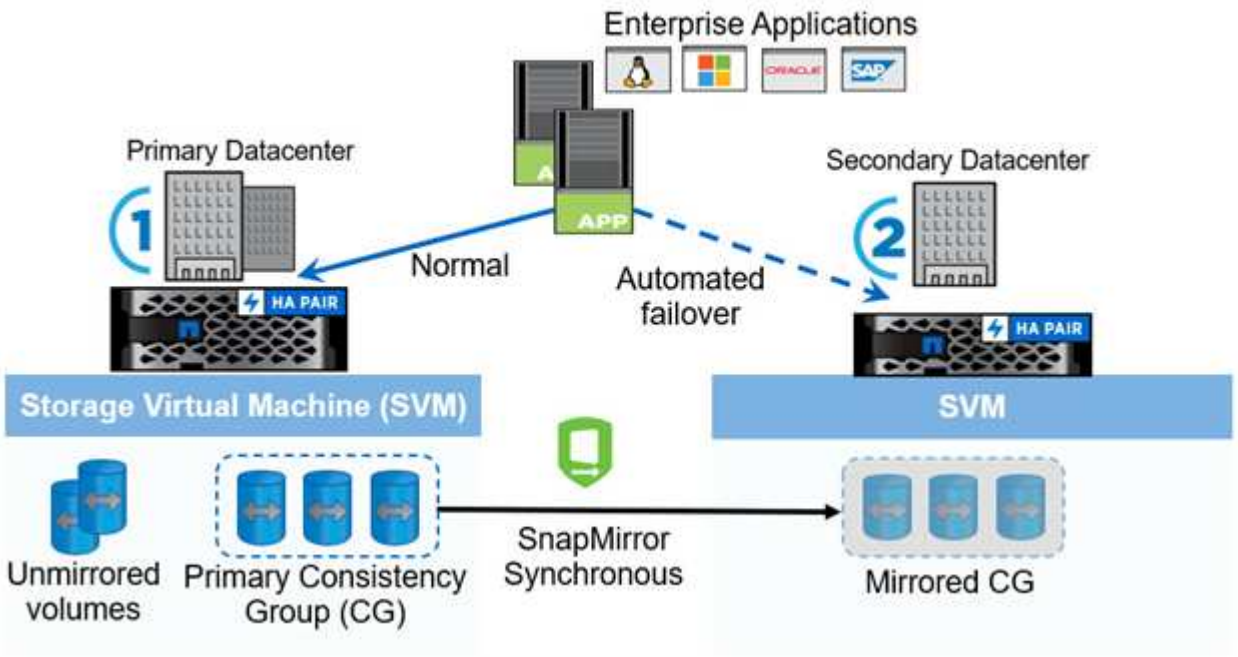
ONTAP 9.8부터 NetApp SM-BC를 통해 투명한 애플리케이션 장애 조치를 위해 SAN 워크로드를 보호할 수 있습니다. 두 AFF 클러스터 간에 일관성 그룹 관계를 생성하거나 데이터 복제를 위해 두 ASA 클러스터 간에 일관성 그룹 관계를 생성하여 제로 RPO 및 제로에 가까운 RTO를 달성할 수 있습니다.

SM-BC 솔루션은 IP 네트워크를 통해 SnapMirror Synchronous 기술을 사용하여 데이터를 복제합니다. iSCSI 또는 FC 프로토콜 기반 SAN LUN을 사용하여 애플리케이션 레벨 세분화와 자동 페일오버를 제공하여 Microsoft SQL

Server, Oracle 등과 같은 비즈니스에 중요한 데이터 서비스를 보호합니다. 세 번째 사이트에 구축된 ONTAP 중재자가 SM-BC 솔루션을 모니터링하고 사이트 재해 시 자동 페일오버를 지원합니다.

일관성 그룹(CG)은 비즈니스 연속성을 위해 보호해야 하는 애플리케이션 워크로드에 대한 쓰기 순서 일관성 보장을 제공하는 FlexVol 볼륨의 모음입니다. 특정 시점의 볼륨 컬렉션에 대해 충돌 시에도 정합성이 보장되는 Snapshot 복사본을 동시에 사용할 수 있습니다. CG 관계라고도 하는 SnapMirror 관계는 소스 CG와 대상 CG 간에 설정됩니다. CG에 속하는 것으로 선택된 볼륨 그룹은 애플리케이션 인스턴스, 애플리케이션 인스턴스 그룹 또는 전체 솔루션에 매핑할 수 있습니다. 또한 비즈니스 요구 사항 및 변경 사항에 따라 필요에 따라 SM-BC 정합성 보장 그룹 관계를 생성하거나 삭제할 수 있습니다.

다음 그림과 같이 일관성 그룹의 데이터는 재해 복구 및 비즈니스 연속성을 위해 두 번째 ONTAP 클러스터에 복제됩니다. 애플리케이션은 두 ONTAP 클러스터 모두에서 LUN에 연결됩니다. 일반적으로 운영 클러스터에서 I/O를 제공하고 운영 클러스터에서 재해가 발생할 경우 보조 클러스터에서 자동으로 재개합니다. SM-BC 솔루션을 설계할 때는 지원되는 한도를 초과하지 않도록 CG 관계에 대해 지원되는 오브젝트 수(예: 최대 20개의 CG 및 최대 200개의 엔드포인트)를 준수해야 합니다.



"다음: FlexPod SM-BC 솔루션"

FlexPod SM-BC 솔루션

"이전: 소개."

솔루션 개요

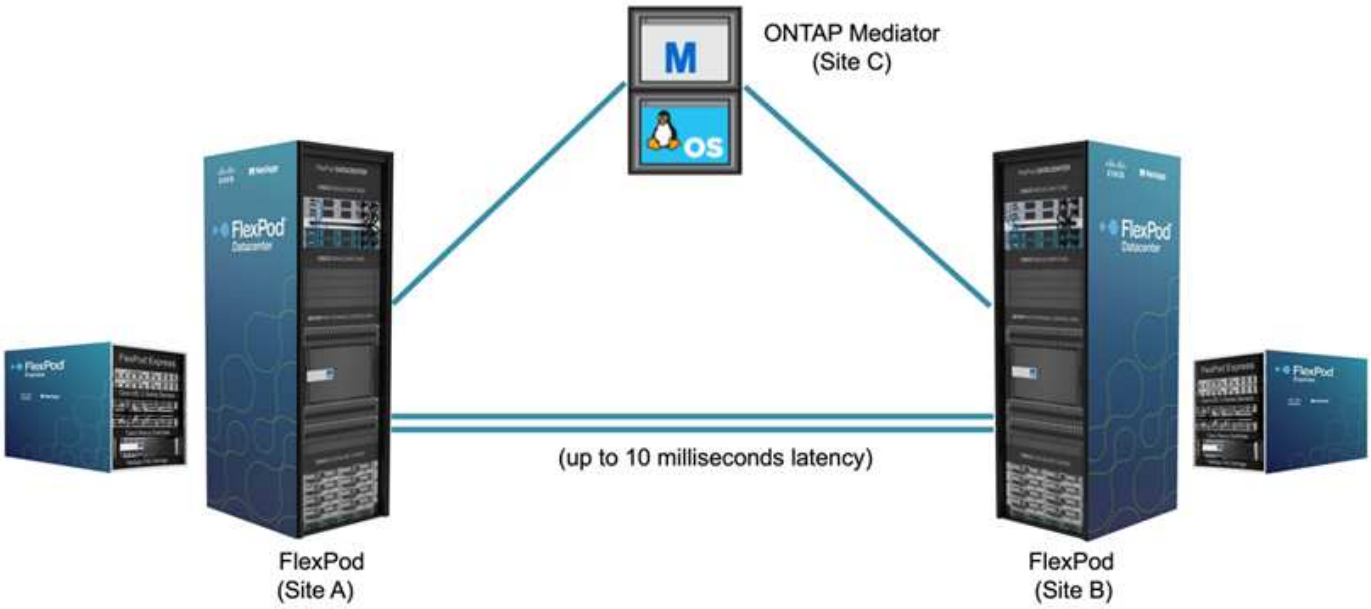
높은 수준의 FlexPod SM-BC 솔루션은 두 개의 FlexPod 시스템으로 구성되어 있으며, 서로 연결되고 서로 연결되어 어느 정도 거리가 떨어져 있는 두 개의 사이트에 배치되어 사이트 장애 시에도 무중단 업무 운영을 제공할 수 있는 가용성이 높고 유연성이 뛰어나며 신뢰성이 높은 데이터 센터 솔루션을 제공합니다.

FlexPod SM-BC 솔루션을 구축하기 위해 두 개의 새로운 FlexPod 인프라를 구축할 뿐만 아니라, SM-BC와 호환되는 두 개의 기존 FlexPod 인프라에 솔루션을 구축하거나 기존 FlexPod와 함께 새로운 FlexPod를 추가하여 구축할 수도 있습니다.

FlexPod SM-BC 솔루션의 두 FlexPod 시스템은 구성에서 동일하지 않아도 됩니다. 그러나 두 ONTAP 클러스터는 두 AFF 시스템 또는 두 ASA 시스템 중 하나의 스토리지 제품군이어야 하지만 반드시 동일한 하드웨어 모델이 아니어야 합니다. SM-BC 솔루션은 FAS 시스템을 지원하지 않습니다.

두 FlexPod 사이트는 솔루션 대역폭과 서비스 품질 요구 사항을 충족하는 네트워크 연결이 필요하며, ONTAP SM-BC 솔루션에서 요구하는 대로 사이트 간 라운드 트립 지연 시간이 10밀리초(10ms) 미만입니다. 이 FlexPod SM-BC 솔루션 검증을 위해 두 FlexPod 사이트는 동일한 실험실에서 확장된 Layer-2 네트워크를 통해 상호 연결됩니다.

NetApp ONTAP SM-BC 솔루션은 두 NetApp 스토리지 클러스터 간에 동기식 복제를 제공하여 캠퍼스 또는 도심 지역에서 고가용성 및 재해 복구를 지원합니다. 세 번째 사이트에 구축된 ONTAP 중재자가 솔루션을 모니터링하고 사이트 재해 시 자동 페일오버를 지원합니다. 다음 그림은 솔루션 구성 요소에 대한 개략적인 보기를 제공합니다.



FlexPod SM-BC 솔루션을 사용하면 VMware vSphere 기반 프라이빗 클라우드를 분산형의 통합 인프라에 구축할 수 있습니다. 통합 솔루션을 사용하면 여러 사이트를 단일 솔루션 인프라로 통합하여 다양한 단일 장애 지점 및 전체 사이트 장애로부터 데이터 서비스를 보호할 수 있습니다.

이 기술 보고서에서는 FlexPod SM-BC 솔루션의 일부 엔드 투 엔드 설계 고려 사항을 중점적으로 다룹니다. 실무자는 다양한 FlexPod CVD 및 NVA에서 사용 가능한 정보를 참조하여 FlexPod 솔루션 구현 세부정보를 추가로 받는 것이 좋습니다.

이 솔루션은 CVD에 문서화된 FlexPod 모범 사례를 기반으로 두 개의 FlexPod 시스템을 구축하여 검증되었지만, SM-BC 솔루션의 요구사항을 고려합니다. 이 보고서에 설명된 구축된 FlexPod SM-BC 솔루션은 다양한 장애 시나리오 및 시뮬레이션된 사이트 장애 시나리오 중에 복구 성능 및 내결함성을 검증했습니다.

솔루션 요구 사항

FlexPod SM-BC 솔루션은 다음과 같은 주요 요구 사항을 충족하도록 설계되었습니다.

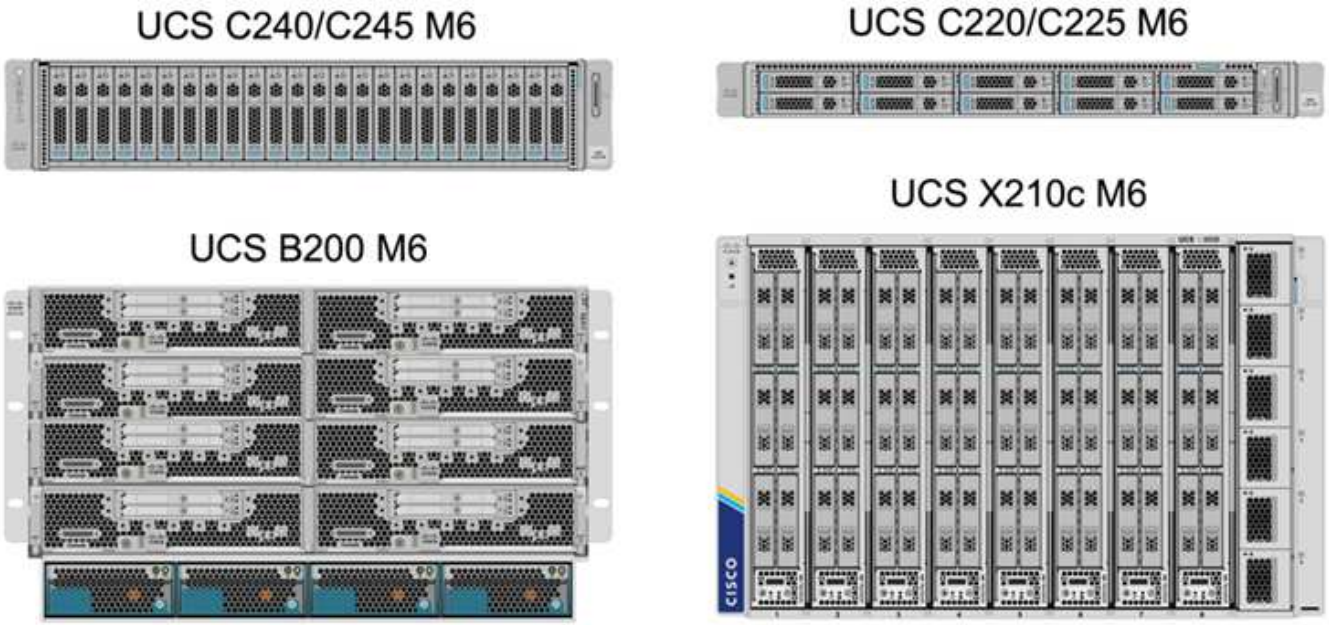
- 전체 데이터 센터(사이트)에 장애가 발생할 경우 비즈니스 크리티컬 애플리케이션 및 데이터 서비스를 위한 비즈니스 연속성
- 데이터 센터 간에 워크로드 이동성을 통해 유연하고 분산된 워크로드 배치
- 정상 운영 중에 동일한 데이터 센터 사이트에서 가상 머신 데이터에 로컬로 액세스하는 사이트 친화성
- 사이트 장애 발생 시 데이터 손실 없이 빠른 복구

Cisco 컴퓨팅 구성 요소

Cisco UCS는 통합 컴퓨팅 인프라로 통합 컴퓨팅 리소스, 통합 패브릭 및 통합 관리를 제공합니다. 기업에서는 이 솔루션을 사용하여 가상화 및 베어 메탈 워크로드를 비롯한 애플리케이션의 구축을 자동화하고 가속화할 수 있습니다. Cisco UCS는 원격 및 지점, 데이터 센터 및 하이브리드 클라우드 사용 사례를 비롯한 광범위한 구축 사용 사례를 지원합니다. 특정 솔루션 요구 사항에 따라 FlexPod Cisco 컴퓨팅 구현은 다양한 범위의 구성 요소를 사용할 수 있습니다. 다음 하위 섹션에서는 UCS 구성요소 중 일부에 대한 추가 정보를 제공합니다.

UCS 서버 및 컴퓨팅 노드

다음 그림은 UCS C-Series 랙 서버, B-Series 블레이드 서버가 포함된 UCS 5108 섀시, X-Series 컴퓨팅 노드가 포함된 새로운 UCS X9508 섀시 등 UCS 서버 구성요소의 예를 보여줍니다. Cisco UCS C-Series 랙 서버는 1개 및 2개의 랙 유닛(RU) 폼 팩터, Intel 및 AMD CPU 기반 모델, 다양한 CPU 속도 및 코어, 메모리, I/O 옵션으로 제공됩니다. Cisco UCS B-Series 블레이드 서버와 새로운 X-Series 컴퓨팅 노드를 다양한 CPU, 메모리 및 I/O 옵션과 함께 사용할 수도 있으며, 이러한 모든 기능을 FlexPod 아키텍처에서 지원하여 다양한 비즈니스 요구사항을 충족합니다.



이 그림에 표시된 최신 세대 C220/C225/C240/C245 M6 랙 서버, B200 M6 블레이드 서버 및 X210c 컴퓨팅 노드 외에도 이전 세대의 랙 및 블레이드 서버가 계속 지원되는 경우에도 사용할 수 있습니다.

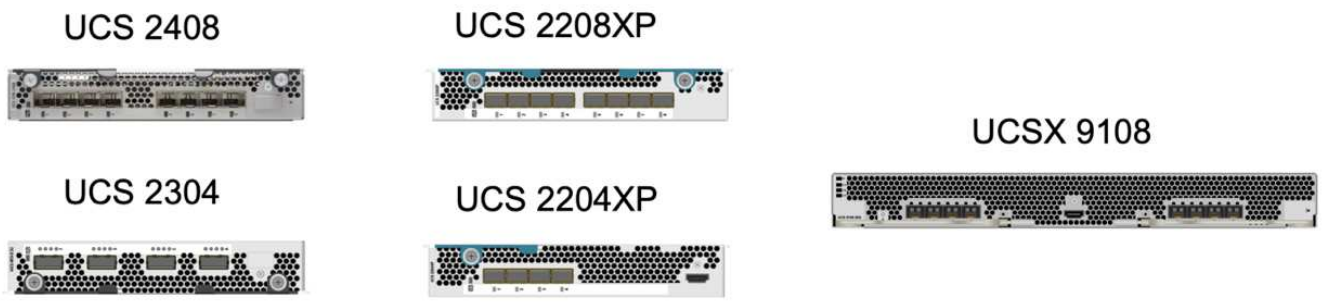
I/O 모듈 및 지능형 패브릭 모듈

I/O 모듈(IOM)/Fabric Extender 및 IFM(Intelligent Fabric Module)은 각각 Cisco UCS 5108 블레이드 서버 섀시 및 Cisco UCS X9508 X 시리즈 섀시에 대한 통합 패브릭 연결을 제공합니다.

4세대 UCS IOM 2408에는 UCS 5108 섀시를 패브릭 인터커넥트(FI)와 연결하기 위한 25G 통합 이더넷 포트 8개가 있습니다. 각 2408에는 미드플레인을 통해 섀시의 각 블레이드 서버에 4개의 10-G 백플레인 이더넷 연결이 있습니다.

UCSX 9108 25G IFM에는 패브릭 상호 연결을 통해 UCS X9508 섀시의 블레이드 서버를 연결하기 위한 8개의 25-G 통합 이더넷 포트가 있습니다. 각 9108에는 X9108 섀시의 각 UCS X210c 컴퓨팅 노드에 대한 25-G 연결 4개가 있습니다. 9108 IFM은 패브릭 상호 연결과 함께 작동하여 섀시 환경을 관리합니다.

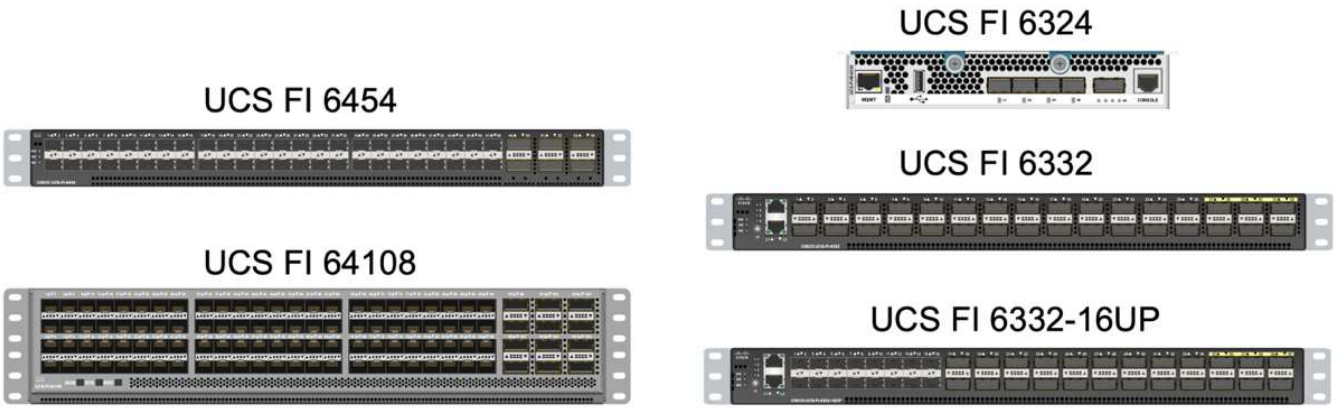
다음 그림은 UCS 5108 섀시의 UCS 2408 및 이전 IOM 세대 및 X9508 섀시의 경우 9108 IFM을 보여 줍니다.



UCS Fabric 인터커넥트

Cisco UCS FI(Fabric Interconnect)는 전체 Cisco UCS에 대한 연결 및 관리 기능을 제공합니다. 일반적으로 액티브/액티브 쌍으로 구축되는 이 시스템의 FI는 모든 구성 요소를 Cisco UCS Manager 또는 Cisco Intersight에서 제어하는 고가용성 단일 관리 도메인에 통합합니다. Cisco UCS FI는 단일 케이블 세트를 사용하여 LAN, SAN 및 관리 트래픽을 지원하는 짧은 지연 시간과 무손실 컷스루 스위칭을 제공하는 단일 통합 패브릭을 시스템에 제공합니다.

4세대 Cisco UCS FI에는 UCS FI 6454 및 64108의 두 가지 모델이 있습니다. 여기에는 10/25Gbps 이더넷 포트, 1/10/25Gbps 이더넷 포트, 40/100Gbps 이더넷 업 링크 포트, 10/25Gigabit Ethernet 또는 8/16/32Gbps 파이버 채널을 지원할 수 있는 통합 포트 등이 포함됩니다. 다음 그림은 4세대 Cisco UCS FI와 함께 지원되는 3세대 모델도 보여 줍니다.



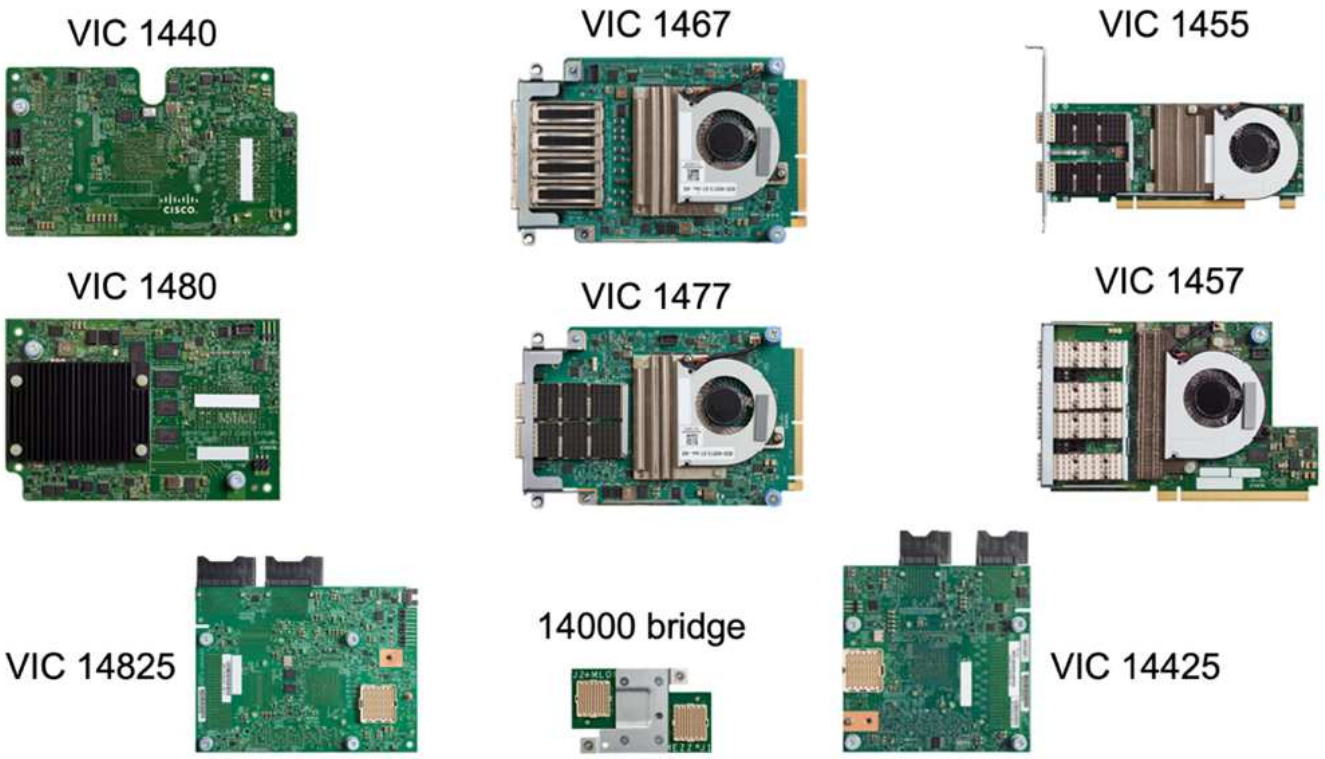
Cisco UCS X-Series 섀시를 지원하려면 Intersight 관리 모드(IMM)로 구성된 4세대 패브릭 상호 연결이 필요합니다. 그러나 Cisco UCS 5108 B 시리즈 섀시는 IMM 모드와 UCSM 관리 모드 모두에서 지원됩니다.

UCS FI 6324는 IOM 폼 팩터를 사용하며 소형 UCS 도메인만 필요한 구축을 위해 UCS Mini 섀시에 내장되어 있습니다.

UCS 가상 인터페이스 카드

Cisco UCS VICS(Virtual Interface Card)는 랙 및 블레이드 서버의 시스템 관리 및 LAN 및 SAN 연결을 통합합니다. vNIC(Virtual Network Interface Card) 또는 Cisco SingleConnect 기술을 사용하는 vHBA(Virtual Host Bus Adapter)로 최대 256개의 가상 장치를 지원합니다. 가상화의 결과로 VIC 카드는 네트워크 연결을 크게 간소화하고 솔루션 배포에 필요한 네트워크 어댑터, 케이블 및 스위치 포트의 수를 줄입니다. 다음 그림은 B 시리즈, C 시리즈 서버

및 X 시리즈 컴퓨팅 노드에 사용할 수 있는 일부 Cisco UCS VICS를 보여 줍니다.



다양한 어댑터 모델은 포트 수, 포트 속도 및 폼 팩터가 서로 다른 블레이드 및 랙 서버를 지원하며, 모듈식 MLOM(LAN on Motherboard), 메자닌 카드 및 PCIe 인터페이스를 지원합니다. 어댑터는 10/25/40/100G 이더넷 및 FCoE(Fibre Channel over Ethernet)의 일부 조합을 지원할 수 있습니다. Cisco의 CNA(Converged Network Adapter) 기술을 통합하고 종합적인 기능 세트를 지원하며 어댑터 관리 및 애플리케이션 구축을 단순화합니다. 예를 들어 VIC는 Cisco UCS 패브릭 상호 연결 포트를 가상 머신으로 확장하는 Cisco의 VM-FEX(Data Center Virtual Machine Fabric Extender) 기술을 지원하므로 서버 가상화 구축을 간소화할 수 있습니다.

mLOM, 메자닌 및 포트 확장기 및 브리지 카드 구성에서 Cisco VIC를 결합하면 블레이드 서버에서 사용할 수 있는 대역폭과 연결을 최대한 활용할 수 있습니다. 예를 들어, X210c 컴퓨팅 노드에 대해 VIC 14825(mLOM) 및 14425(메자닌) 및 14000(브리지 카드)의 25-G 링크 2개를 사용하여 결합된 VIC 대역폭은 2 x 50-G + 2 x 50-G 입니다. 또는 듀얼 IFM 구성을 사용하여 서버당 100G/IFM 및 서버당 총 200g

Cisco UCS 제품군, 기술 사양 및 문서에 대한 자세한 내용은 를 참조하십시오 "Cisco UCS" 웹 사이트를 참조하십시오.

Cisco 스위칭 구성 요소

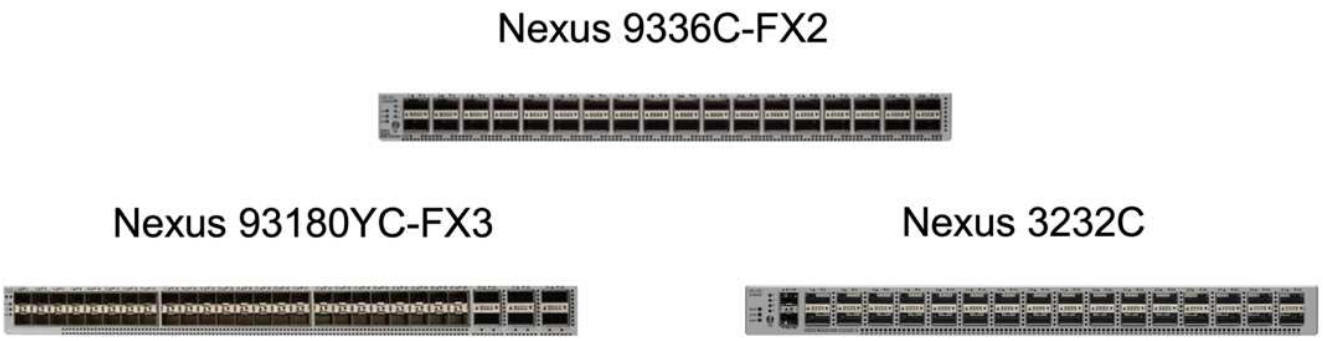
Nexus 스위치

FlexPod은 Cisco Nexus 시리즈 스위치를 사용하여 Cisco UCS와 NetApp 스토리지 컨트롤러 간의 통신에 이더넷 스위칭 패브릭을 제공합니다. FlexPod 배포에는 Cisco Nexus 3000, 5000, 7000, 9000 시리즈를 비롯하여 현재 지원되는 모든 Cisco Nexus 스위치 모델이 지원됩니다.

FlexPod 구축을 위한 스위치 모델을 선택할 때 성능, 포트 속도, 포트 밀도, 스위칭 지연 시간, 또한 설계 목표뿐 아니라 스위치의 지원 시간(TimeSpan)을 위해 ACI 및 VXLAN과 같은 프로토콜을 지원합니다.

최신 FlexPod CVD에 대한 검증에서는 Nexus 9336C-FX2 및 Nexus 93180YC-FX3과 같은 Cisco Nexus 9000 시리즈 스위치를 사용합니다. 이 스위치는 고성능 40/100G 및 10//25G 포트, 짧은 지연 시간, 뛰어난 전력 효율성을 소형 1U 폼 팩터에서 제공합니다. 업링크 포트 및 브레이크아웃 케이블을 통해 추가 속도가 지원됩니다. 다음 그림은 이

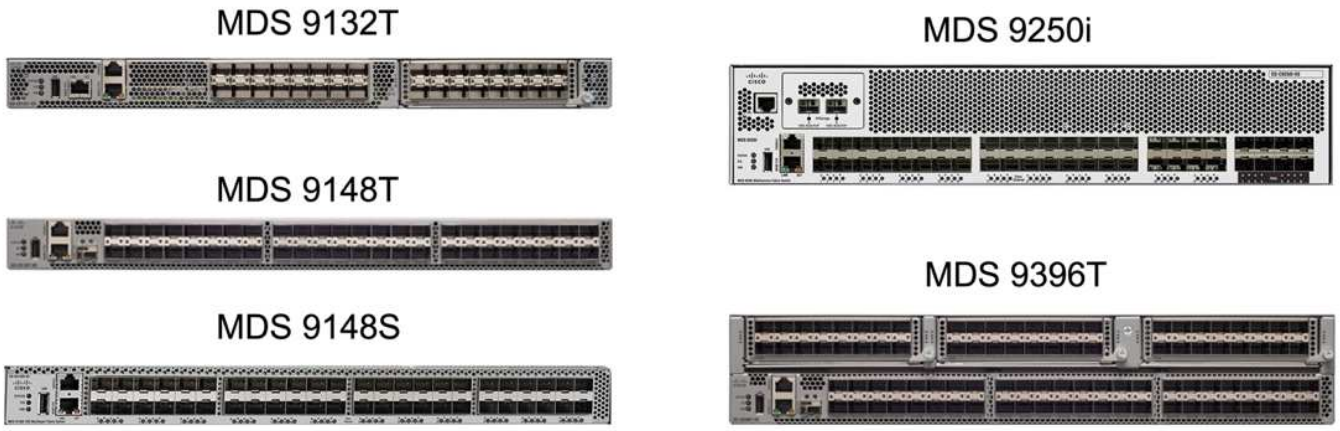
검증에 사용된 Nexus 9336C-FX2 및 Nexus 3232C를 포함하여 몇 개의 Cisco Nexus 9k 및 3k 스위치를 보여줍니다.



을 참조하십시오 "Cisco 데이터 센터 스위치" 사용 가능한 Nexus 스위치 및 사양 및 문서에 대한 자세한 내용은

MDS 스위치

Cisco MDS 9100/9200/9300 시리즈 패브릭 스위치는 FlexPod 아키텍처의 선택적 구성 요소입니다. 이러한 스위치는 매우 안정적이고, 매우 유연하고, 안전하며, Fabric의 트래픽 흐름에 대한 가시성을 제공할 수 있습니다. 다음 그림에서는 애플리케이션 및 비즈니스 요구 사항을 충족하기 위해 FlexPod 솔루션을 위한 이중화된 FC SAN 패브릭을 구축하는 데 사용할 수 있는 MDS 스위치의 예를 보여 줍니다.



Cisco MDS 9132T/9148T/9396T 고성능 32G 멀티레이어 패브릭 스위치는 비용 효율적이며 매우 안정적이고 유연하며 확장성이 뛰어납니다. 고급 스토리지 네트워킹 기능은 관리가 용이하며 전체 Cisco MDS 9000 제품군 포트폴리오와 호환되므로 안정적인 SAN 구현이 가능합니다.

이 차세대 하드웨어 플랫폼에는 최첨단 SAN 분석 및 원격 측정 기능이 내장되어 있습니다. 프레임 헤더 검사에서 추출된 원격 측정 데이터를 Cisco Data Center Network Manager를 비롯한 분석 시각화 플랫폼으로 스트리밍할 수 있습니다. MDS 9148S와 같이 16G FC를 지원하는 MDS 스위치도 FlexPod에서 지원됩니다. 또한 FC 프로토콜 외에 FCoE 및 FCIP 프로토콜을 지원하는 MDS 9250i와 같은 멀티서비스 MDS 스위치도 FlexPod 솔루션 포트폴리오에 포함됩니다.

9132T 및 9396T와 같은 반모듈식 MDS 스위치에서 추가 포트 확장 모듈 및 포트 라이센스를 추가하여 추가 디바이스 접속을 지원할 수 있습니다. 9148T와 같은 고정 스위치에서는 필요에 따라 포트 라이센스를 추가할 수 있습니다. 이와 같이 확장 가능한 지불 유연성을 통해 운영 비용 구성 요소를 제공하여 MDS 스위치 기반 SAN 인프라를 구축하고 운영하는 데 드는 자본 비용을 절감할 수 있습니다.

을 참조하십시오 "Cisco MDS 패브릭 스위치" 사용 가능한 MDS Fabric 스위치에 대한 자세한 내용은 를 참조하십시오 "NetApp IMT를 참조하십시오" 및 "Cisco 하드웨어 및 소프트웨어 호환성 목록" 지원되는 SAN 스위치의 전체 목록을

확인하십시오.

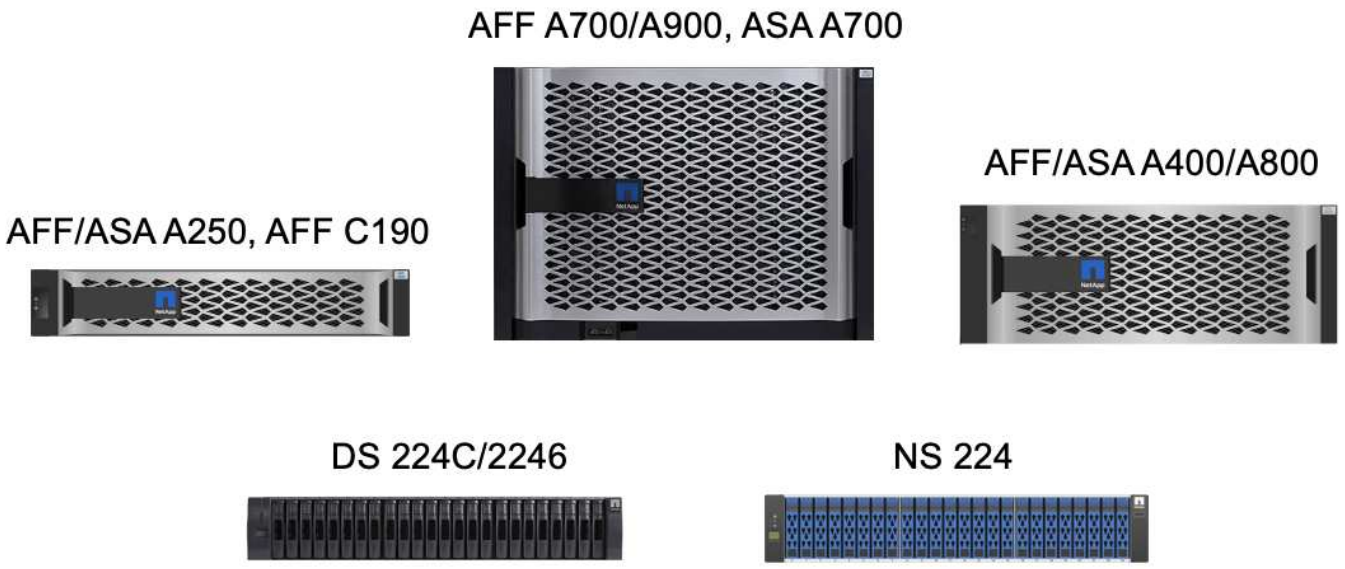
NetApp 구성 요소

ONTAP 소프트웨어 9.8 이상을 실행하는 이중 NetApp AFF 또는 ASA 컨트롤러는 FlexPod SM-BC 솔루션을 생성해야 합니다. SM-BC 배포에서는 ONTAP 혁신, 성능 및 품질 향상을 지속적으로 활용하고 SM-BC 지원에 대한 최대 개체 수를 늘릴 수 있도록 현재 9.10.1인 최신 ONTAP 릴리스를 권장합니다.

업계 최고의 성능과 혁신 기능을 갖춘 NetApp AFF 및 ASA 컨트롤러는 엔터프라이즈 데이터 보호 기능과 강력한 데이터 관리 기능을 제공합니다. AFF 및 ASA 시스템은 NVMe 연결 SSD 및 NVMe over Fibre Channel(NVMe/FC) 프론트 엔드 호스트 연결을 포함한 엔드 투 엔드 NVMe 기술을 지원합니다. NVMe/FC 기반 SAN 인프라를 채택하면 워크로드 처리량을 높이고 I/O 지연 시간을 줄일 수 있습니다. 하지만 SM-BC 솔루션은 현재 iSCSI 및 FC 프로토콜만 지원하므로 NVMe/FC 기반 데이터 저장소는 SM-BC로 보호되지 않는 워크로드에 대해서만 사용할 수 있습니다.

NetApp AFF 및 ASA 스토리지 컨트롤러는 또한 고객이 NetApp Data Fabric에서 지원하는 원활한 데이터 이동성을 활용할 수 있도록 하이브리드 클라우드 기반을 제공합니다. Data Fabric을 사용하면 데이터가 생성되는 에지에서 코어, 사용될 코어로, 그리고 클라우드로 데이터를 쉽게 가져올 수 있습니다. 또한 온디맨드 방식으로 탄력적인 컴퓨팅 및 AI 및 ML 기능을 활용하여 비즈니스 인사이트를 얻을 수 있습니다.

다음 그림과 같이 NetApp은 고객의 성능 및 용량 요구사항을 충족할 수 있도록 다양한 스토리지 컨트롤러와 디스크 쉘프를 제공합니다. NetApp AFF 및 ASA 컨트롤러 기능 및 사양에 대한 자세한 내용은 다음 표를 참조하십시오.



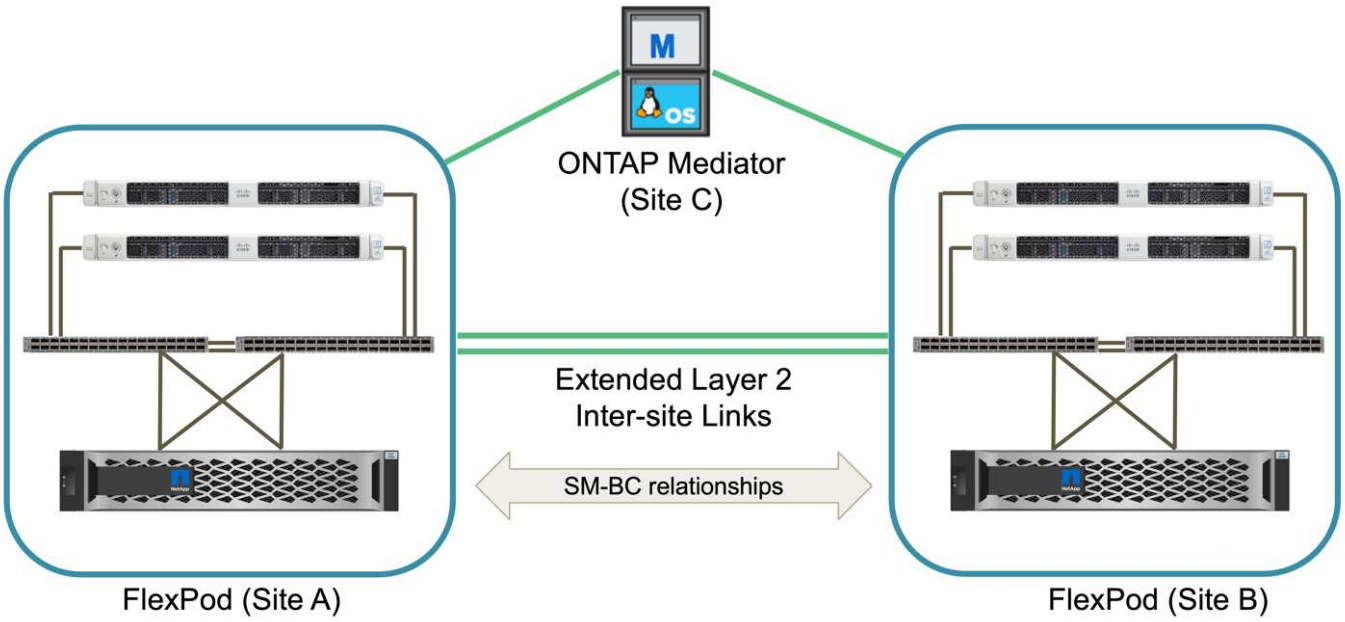
제품군	기술 사양
AFF 시리즈	"AFF 시리즈 문서"
ASA 시리즈	"ASA 시리즈 문서"

을 참조하십시오 "NetApp 디스크 쉘프 및 스토리지 미디어 문서" 및 "NetApp Hardware Universe를 참조하십시오" 각 스토리지 컨트롤러 모델에 대해 디스크 쉘프 및 지원되는 디스크 쉘프에 대한 자세한 내용은 를 참조하십시오.

솔루션 토폴로지

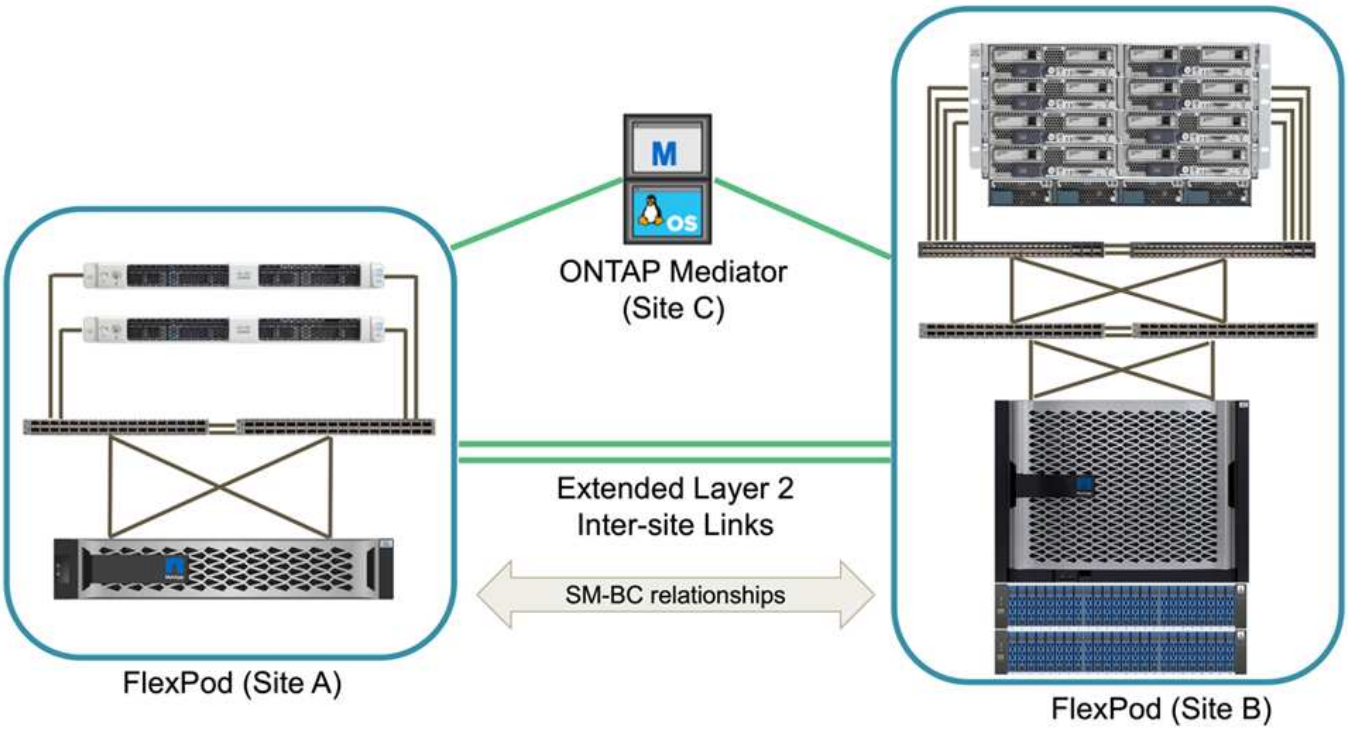
FlexPod 솔루션은 유연한 토폴로지로 다양한 솔루션 요구사항을 충족하도록 확장하거나 축소할 수 있습니다. 다음 그림과 같이 비즈니스 연속성 보호가 필요하고 최소한의 컴퓨팅 및 스토리지 리소스만 단순한 솔루션 토폴로지를 사용할 수 있습니다. 이 간단한 토폴로지에서는 추가 디스크 쉘프 없이 컨트롤러에 SSD가 있는 UCS C-Series 랙 서버와

AFF/ASA 컨트롤러를 사용합니다.



이중화된 컴퓨팅, 네트워크 및 스토리지 구성 요소는 구성 요소 간의 이중화 연결로 상호 연결됩니다. 고가용성 설계로 솔루션 복원력을 제공하고 단일 장애 지점 시나리오를 견딜 수 있습니다. 멀티 사이트 설계와 ONTAP SM-BC 동기식 데이터 복제 관계는 단일 사이트 스토리지 장애가 발생할 가능성에도 불구하고 비즈니스 크리티컬 데이터 서비스를 제공합니다.

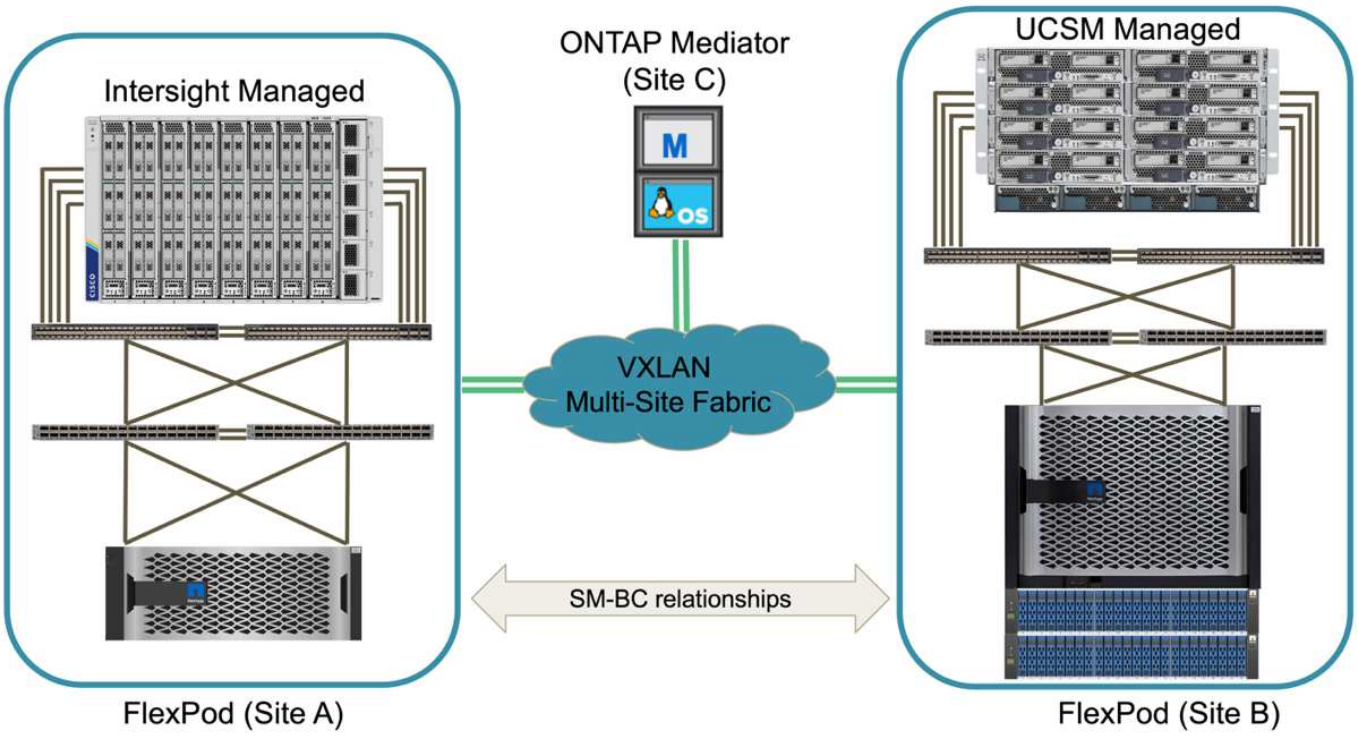
데이터 센터와 대도시 지역의 지사 간에 회사에서 사용할 수 있는 비대칭 배포 토폴로지는 다음 그림과 같이 나타날 수 있습니다. 이와 같이 비대칭 설계에서는 데이터 센터에 더 많은 컴퓨팅 및 스토리지 리소스를 갖춘 고성능 FlexPod가 필요합니다. 그러나 지사 요구 사항은 더 적으며 훨씬 더 작은 FlexPod를 통해 충족할 수 있습니다.



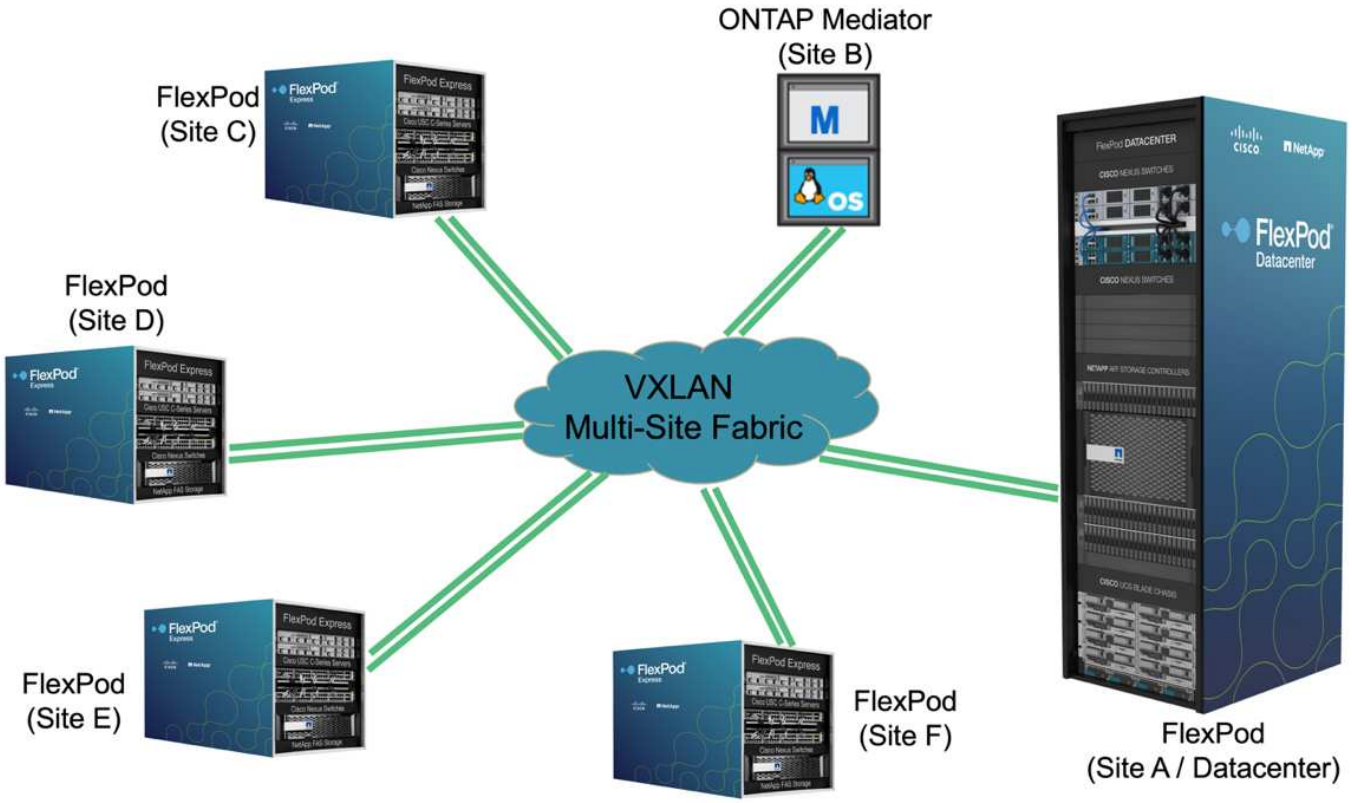
컴퓨팅 및 스토리지 리소스 요구 사항이 더 크고 사이트가 여러 개인 기업의 경우 VXLAN 기반 멀티 사이트 패브릭을

통해 여러 사이트에서 원활한 네트워크 패브릭을 통해 애플리케이션 이동성을 지원하여 모든 사이트에서 애플리케이션을 제공할 수 있습니다.

새로운 FlexPod 인스턴스로 보호해야 하는 Cisco UCS 5108 섀시 및 B-Series 블레이드 서버를 사용하는 기존 FlexPod 솔루션이 있을 수 있습니다. 새 FlexPod 인스턴스는 다음 그림과 같이 Cisco Intersight에서 관리하는 X210c 컴퓨팅 노드와 함께 최신 UCS X9508 섀시를 사용할 수 있습니다. 이 경우 각 사이트의 FlexPod 시스템은 더 큰 데이터센터 패브릭에 연결되고 사이트는 상호 연결 네트워크를 통해 연결되어 VXLAN 멀티 사이트 패브릭을 형성합니다.



비즈니스 연속성을 제공하기 위해 모든 데이터를 보호해야 하는 도심 지역에 데이터 센터와 여러 지사를 둔 회사의 경우 다음 그림에 나와 있는 FlexPod SM-BC 구축 토폴로지를 구현하여 중요한 애플리케이션 및 데이터 서비스를 보호하여 모든 지점 사이트에서 제로 RPO 및 제로에 가까운 RTO 목표를 달성할 수 있습니다.



이 구축 모델을 위해 각 지사는 데이터센터와 SM-BC 관계 및 정합성 보장 그룹을 설정합니다. 지원되는 SM-BC 개체 제한을 고려해야 하므로 전반적인 일관성 그룹 관계 및 끝점 수가 데이터 센터에서 지원되는 최대값을 초과하지 않습니다.

"다음: 솔루션 검증 개요"

솔루션 검증

솔루션 검증 - 개요

"이전: FlexPod SM-BC 솔루션"

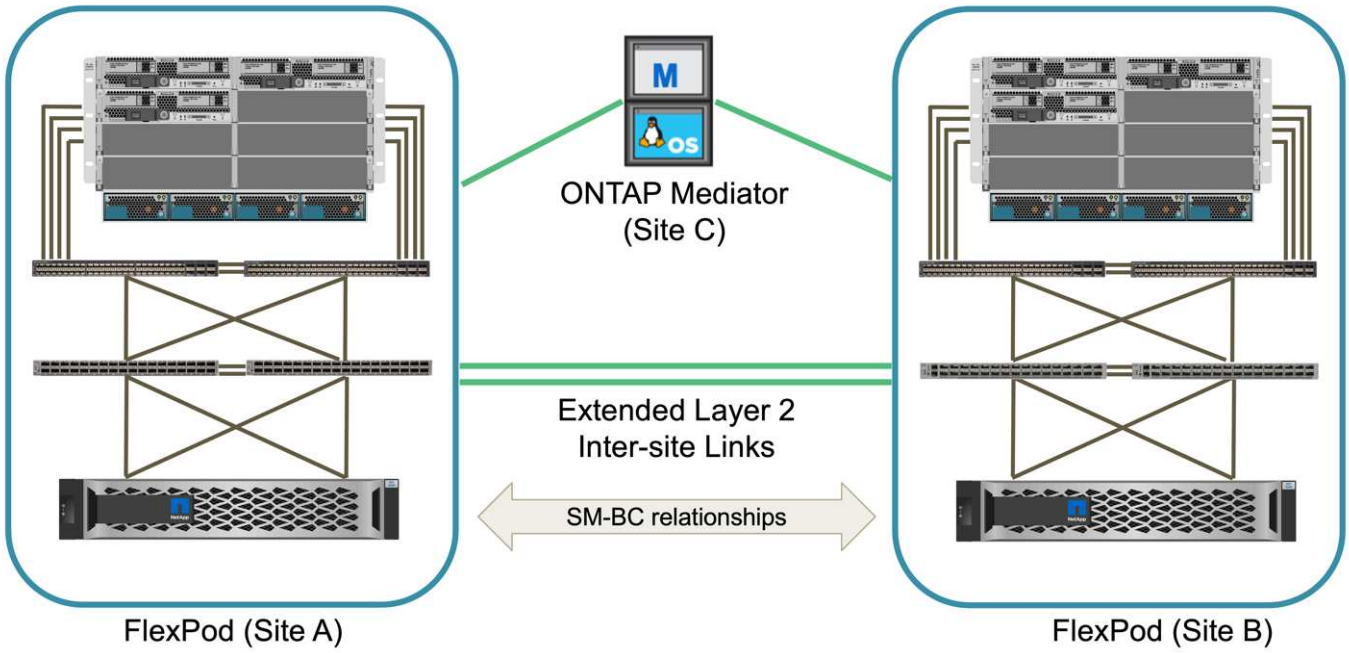
FlexPod SM-BC 솔루션 설계 및 구현 세부사항은 특정 FlexPod 상황 구성 및 솔루션 목표에 따라 달라집니다. 일반적인 비즈니스 연속성 요구 사항이 정의된 후 FlexPod SM-BC 솔루션은 두 개의 새로운 FlexPod 시스템을 갖춘 완전히 새로운 솔루션을 구현하거나, 다른 사이트에 새 FlexPod를 추가하여 기존 FlexPod와 페어링하거나, 두 기존 FlexPod 시스템을 함께 페어링하여 생성할 수 있습니다.

FlexPod 솔루션은 그 특성상 유연성이 뛰어나므로 지원되는 모든 FlexPod 구성과 구성 요소를 사용할 수 있습니다. 이 섹션의 나머지 부분에서는 VMware 기반 가상 인프라 솔루션에 대해 수행된 구현 검증에 대한 정보를 제공합니다. SM-BC 관련 측면을 제외하고 표준 FlexPod 구축 프로세스를 따릅니다. 일반적인 FlexPod 구현 정보에 대해서는 특정 구성에 적합한 FlexPod CVD 및 NVA를 참조하십시오.

검증 토폴로지

FlexPod SM-BC 솔루션의 검증을 위해 NetApp, Cisco 및 VMware에서 지원하는 기술 구성요소가 사용됩니다. 이 솔루션은 사이트 A의 ONTAP 9.10.1, 이중 Cisco Nexus 9336C-FX2 스위치를 실행하는 NetApp AFF A250 HA 쌍과

사이트 B의 이중 Cisco Nexus 3232C 스위치, Cisco UCS 6454 FI를 양쪽 사이트에서 모두 지원합니다. 그리고 VMware vSphere 7.0u2를 실행하고 UCS Manager 및 VMware vCenter Server에서 관리하는 각 사이트에 Cisco UCS B200 M5 서버 3개가 있습니다. 다음 그림은 사이트 A에서 실행되는 두 개의 FlexPod 시스템과 사이트 C에서 실행되는 확장된 계층 2 사이트 간 링크 및 ONTAP 중재자에 의해 연결된 사이트 B의 구성 요소 수준 솔루션 검증 토폴로지를 보여 줍니다



하드웨어 및 소프트웨어

다음 표에는 솔루션 검증에 사용된 하드웨어 및 소프트웨어가 나와 있습니다. Cisco, NetApp 및 VMware는 FlexPod의 특정 구현에 대한 지원을 결정하는 데 사용되는 상호 운용성 매트릭스를 보유하고 있습니다.

- "http://support.netapp.com/matrix/"
- "Cisco UCS 하드웨어 및 소프트웨어 상호 운용성 툴"
- "http://www.vmware.com/resources/compatibility/search.php"

범주	구성 요소	소프트웨어 버전	수량
컴퓨팅	Cisco UCS Fabric Interconnect 6454	4.2(1f)	4개(사이트당 2개)
	Cisco UCS B200 M5 서버	4.2(1f)	6개(사이트당 3개)
	Cisco UCS IOM 2204XP	4.2(1f)	4개(사이트당 2개)
	Cisco VIC 1440(PID:UCSB-mLOM-40G-04)	5.2(1a)	2(사이트당 1개)
	Cisco VIC 1340(PID:UCSB-mLOM-40G-03)	4.5(1a)	4개(사이트당 2개)
네트워크	Cisco Nexus 9336C-FX2	9.3(6)	2(사이트 A)
	Cisco Nexus 3232C	9.3(6)	2(사이트 B)

범주	구성 요소	소프트웨어 버전	수량
스토리지	NetApp AFF A250	9.10.1	4개(사이트당 2개)
	NetApp 시스템 관리자	9.10.1	2(사이트당 1개)
	NetApp Active IQ Unified Manager를 참조하십시오	9.10	1
	VMware vSphere용 NetApp ONTAP 툴	9.10	1
	VMware vSphere용 NetApp SnapCenter 플러그인	4.6	1
	NetApp ONTAP 중재자	1.3	1
	NAbox(NAbox)	3.0.2	1
	NetApp 수집	21.11.1-1	1
포함되었습니다	VMware ESXi	7.0U2	6개(사이트당 3개)
	VMware ESXi nenic 이더넷 드라이버	1.0.35.0	6개(사이트당 3개)
	VMware vCenter를 참조하십시오	7.0U2	1
	VMware VAAI용 NetApp NFS 플러그인	2.0	6개(사이트당 3개)
테스트 중	Microsoft Windows	2022	1
	Microsoft SQL Server를 참조하십시오	2019년	1
	Microsoft SQL Server Management Studio 를 참조하십시오	18.10	1
	HammerDB	4.3	1
	Microsoft Windows	10	6개(사이트당 3개)
	Iometer를 표시합니다	1.1.0	6개(사이트당 3개)

"다음: 솔루션 검증 - 컴퓨팅."

솔루션 검증 - 컴퓨팅

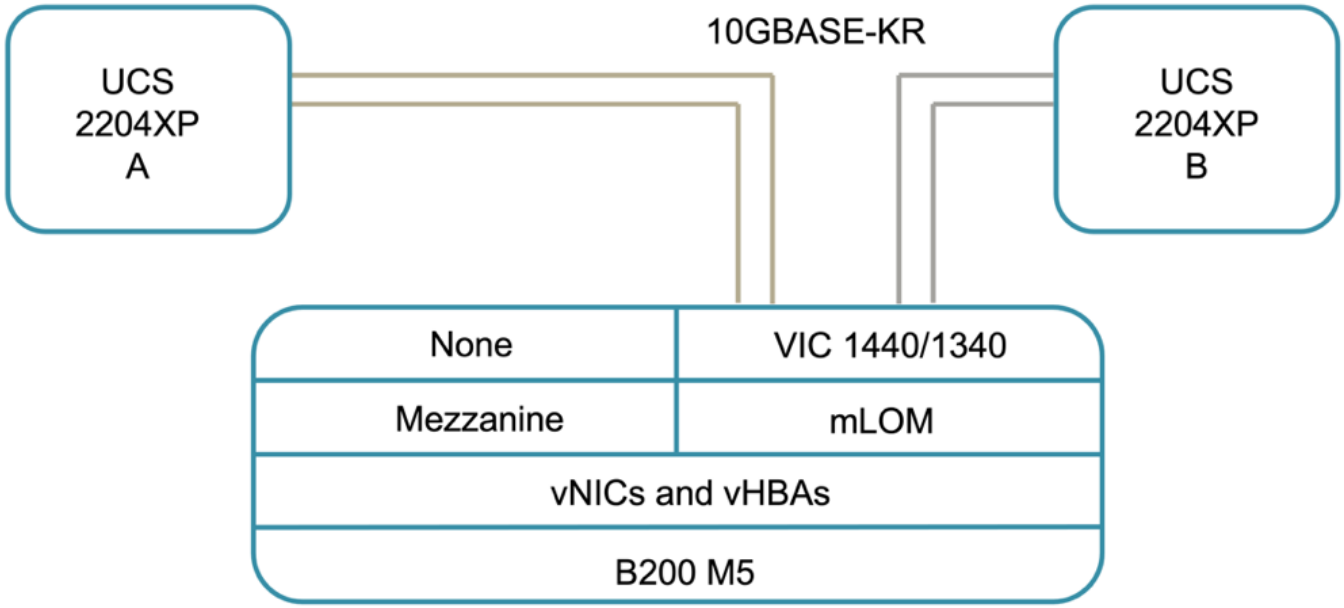
"사전 구성: 솔루션 검증 - 개요"

FlexPod SM-BC 솔루션의 컴퓨팅 구성은 일반적인 FlexPod 솔루션 모범 사례를 따릅니다. 다음 섹션에서는 검증에 사용된 연결 및 구성 중 일부를 설명합니다. 또한 SM-BC 관련 고려 사항 중 일부는 구축 참조 및 지침을 제공하기 위해 강조되어 있습니다.

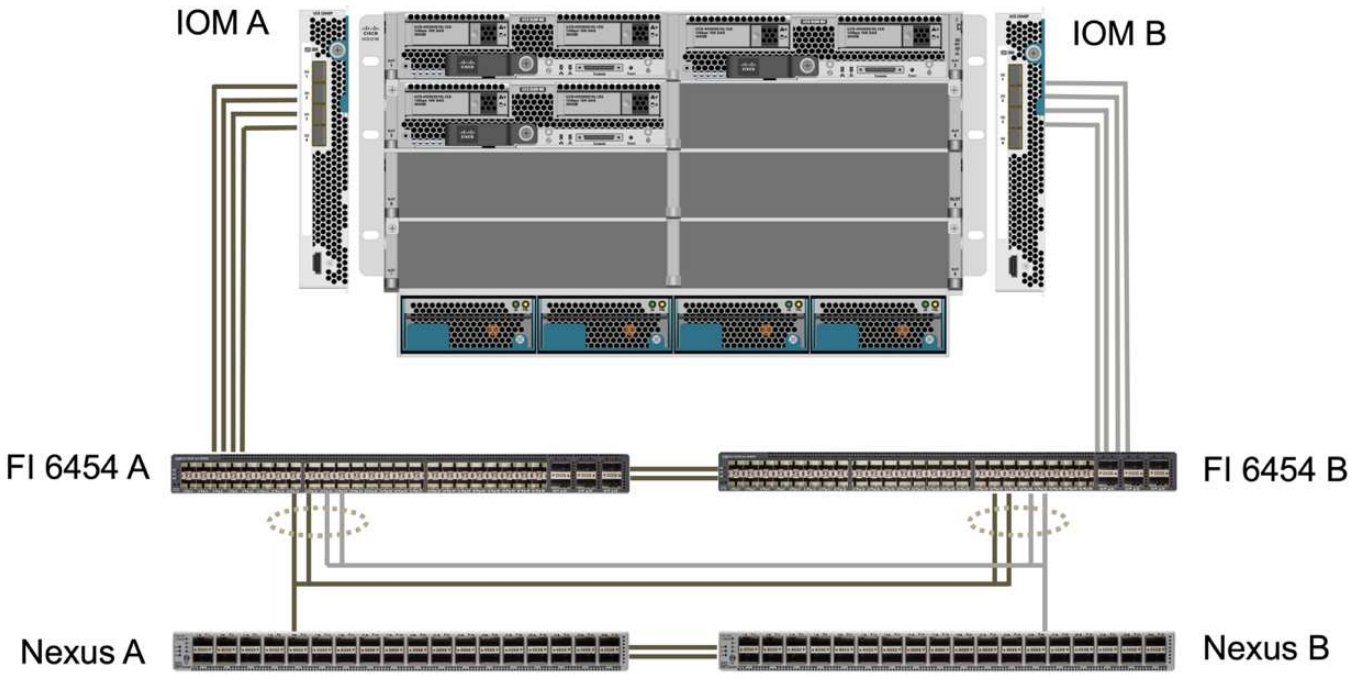
연결성

UCS 5108 섀시 후면판 연결을 통해 UCS B200 블레이드 서버와 IOM 간의 연결이 UCS VIC 카드에 의해 제공됩니다.

검증에 사용된 UCS 2204XP 패브릭 익스텐더에는 각 서버에 2개씩 등 8개의 절반 너비 블레이드 서버에 연결할 수 있는 16개의 10G 포트가 있습니다. 서버 연결 대역폭을 높이기 위해 추가 메자닌 기반 VIC를 추가하여 각 서버에 4개의 10G 연결을 제공하는 대체 UCS 2408 IOM에 서버를 연결할 수 있습니다.



UCS 5108 섀시와 검증에 사용된 UCS 6454 FI 간의 연결은 4개의 10G 연결을 사용하는 IOM 2204XP에서 제공합니다. 이러한 연결을 위해 FI 포트 1 - 4가 서버 포트로 구성됩니다. FI 포트 25~28은 로컬 사이트의 Nexus 스위치 A 및 B에 대한 네트워크 업링크 포트로 구성됩니다. 다음 그림과 표에는 UCS 5108 섀시 및 Nexus 스위치에 연결할 UCS 6454 FI의 연결 다이어그램 및 포트 연결 정보가 나와 있습니다.



로컬 장치	로컬 포트	원격 장치	원격 포트
UCS 6454 FI A	1	IOM A를 지원합니다	1

로컬 장치	로컬 포트	원격 장치	원격 포트
	2		2
	3		3
	4		4
	25	Nexus A	1월 13일
	26		2012년 1월 13일
	27	Nexus B	3월 1일-13일
	28		4월 1일-13일
	L1	UCS 6454 FI B	L1
	L2		L2
UCS 6454 FI B	1	IOM B를 클릭합니다	1
	2		2
	3		3
	4		4
	25	Nexus A	3월 1일-13일
	26		4월 1일-13일
	27	Nexus B	1월 13일
	28		2012년 1월 13일
	L1	UCS 6454 FI A	L1
	L2		L2



사이트 A는 Nexus 9336C-FX2switches를 사용하고 사이트 B는 Nexus 3232C 스위치를 사용함에도 불구하고 위의 연결은 A와 B 사이트 모두에서 비슷합니다. Nexus to Fi 연결에는 40g~4x10G 브레이크아웃 케이블이 사용됩니다. Nexus에 대한 FI 연결은 포트 채널을 사용하고 가상 포트 채널은 Nexus 스위치에서 구성되어 각 FI에 대한 연결을 통합합니다.



IOM, FI 및 Nexus 스위치 구성요소를 서로 다른 방법으로 함께 사용할 경우 환경 조합에 적절한 케이블과 포트 속도를 사용해야 합니다.



더 빠른 연결 또는 더 많은 연결을 지원하는 구성 요소를 사용하여 추가 대역폭을 달성할 수 있습니다. 이를 지원하는 구성 요소와의 연결을 추가하여 이중화를 추가로 구현할 수 있습니다.

서비스 프로필

UCSM(UCS Manager) 또는 Cisco Intersight에서 관리하는 패브릭 인터커넥트를 사용하는 블레이드 서버 섀시는 UCSM에서 사용할 수 있는 서비스 프로필과 Intersight에서 서버 프로필을 사용하여 서버를 추상화할 수 있습니다. 이 검증에서는 UCSM 및 서비스 프로필을 사용하여 서버 관리를 간소화합니다. 서비스 프로필을 사용하면 원래 서비스 프로필을 새 하드웨어와 연결하기만 하면 서버를 교체하거나 업그레이드할 수 있습니다.

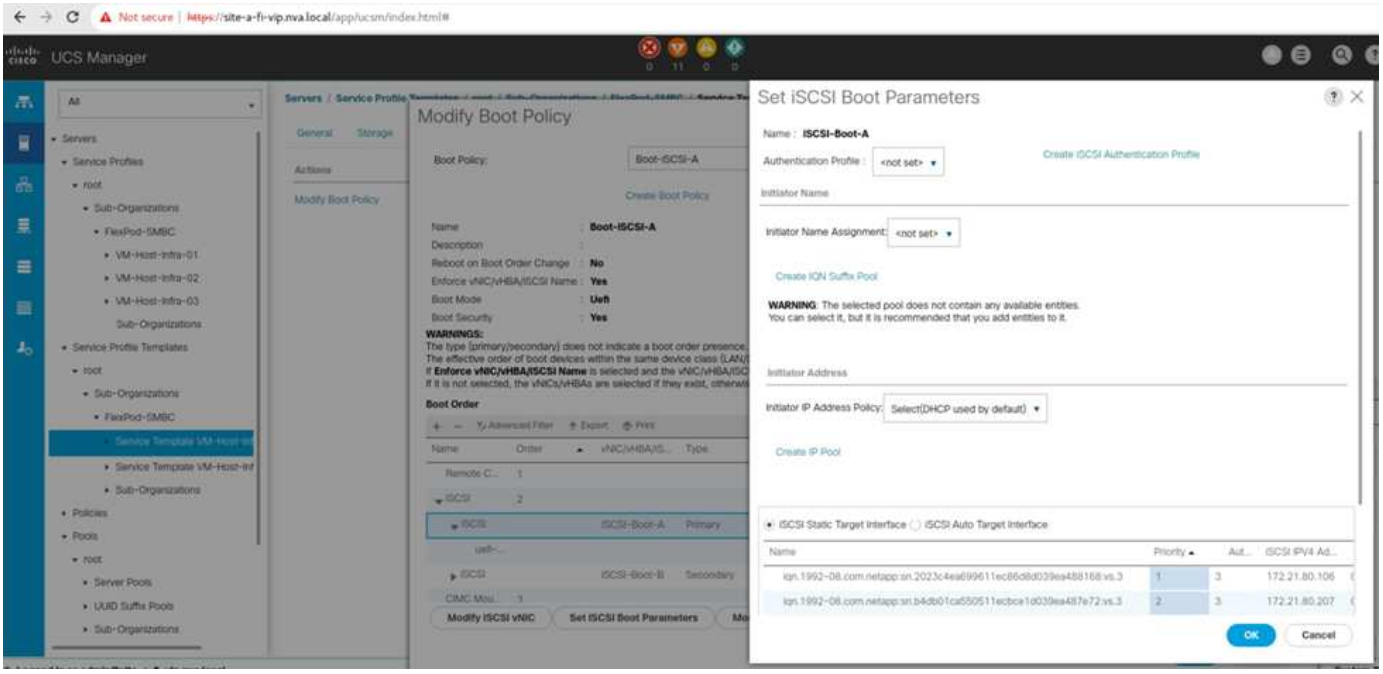
생성된 서비스 프로필은 VMware ESXi 호스트에 대해 다음을 지원합니다.

- iSCSI 프로토콜을 사용하여 양쪽 사이트의 AFF A250 스토리지에서 SAN을 부팅합니다.
- 다음과 같은 서버에 대해 6개의 vNIC가 생성됩니다.
  - 2개의 중복 vNIC(vSwitch0-A 및 vSwitch0-B)는 대역 내 관리 트래픽을 전달합니다. 선택 사항으로, 이러한 vNIC는 SM-BC로 보호되지 않는 NFS 프로토콜 데이터에서도 사용할 수 있습니다.
  - vSphere 분산 스위치는 2개의 중복 vNIC(VDS-A 및 VDS-B)를 사용하여 VMware vMotion 및 기타 애플리케이션 트래픽을 전송합니다.
  - iSCSI - iSCSI에서 사용하는 vNIC - iSCSI-A 경로에 대한 액세스를 제공하는 vSwitch입니다.
  - iSCSI-B vSwitch에서 iSCSI-B vNIC를 사용하여 iSCSI-B 경로에 대한 액세스를 제공합니다.

SAN 부팅

iSCSI SAN 부팅 구성의 경우 iSCSI 부트 매개 변수가 두 iSCSI 패브릭에서 iSCSI 부팅을 허용하도록 설정됩니다. 운영 클러스터를 사용할 수 없을 때 iSCSI SAN 부팅 LUN이 보조 클러스터에서 제공되는 SM-BC 페일오버 시나리오를 수용하기 위해 iSCSI 정적 타겟 구성에는 사이트 A와 사이트 B의 타겟이 모두 포함되어야 합니다 또한 부팅 LUN 가용성을 최대화하려면 모든 스토리지 컨트롤러에서 부팅하도록 iSCSI 부트 매개 변수 설정을 구성합니다.

다음 그림과 같이 Set iSCSI Boot 매개 변수 대화 상자의 서비스 프로필 템플릿의 부팅 정책에서 iSCSI 정적 대상을 구성할 수 있습니다. 다음 표에는 고가용성을 달성하기 위해 위에서 설명한 부팅 전략을 구현하는 권장 iSCSI 부팅 매개 변수 설정 구성이 나와 있습니다.



iSCSI 패브릭	우선 순위	iSCSI 타겟	iSCSI LIF
iSCSI A	1	사이트 A iSCSI 타겟	사이트 A 컨트롤러 1 iSCSI A LIF
	2	사이트 B iSCSI 타겟입니다	사이트 B 컨트롤러 2 iSCSI A LIF
iSCSI B 를 선택합니다	1	사이트 B iSCSI 타겟입니다	사이트 B 컨트롤러 1 iSCSI B LIF입니다

iSCSI 패브릭	우선 순위	iSCSI 타겟	iSCSI LIF
	2	사이트 A iSCSI 타겟	사이트 A 컨트롤러 2 iSCSI B LIF

"다음: 솔루션 검증 - 네트워크."

솔루션 검증 - 네트워크

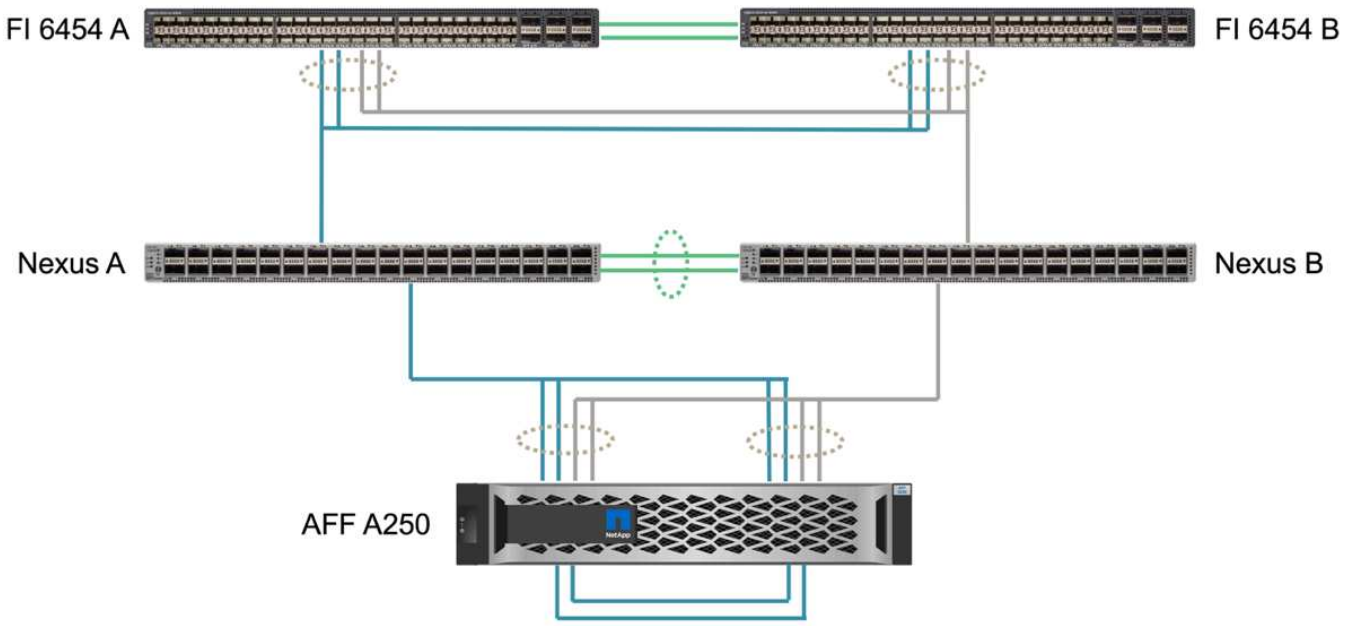
"이전: 솔루션 검증 - 컴퓨팅."

FlexPod SM-BC 솔루션의 네트워크 구성은 각 사이트의 일반적인 FlexPod 솔루션 Best Practice를 따릅니다. 사이트 간 연결의 경우, 솔루션 검증 구성은 두 사이트의 FlexPod Nexus 스위치를 서로 연결하여 두 사이트 간에 VLAN을 확장하는 사이트 간 연결을 제공합니다. 다음 섹션에서는 검증에 사용된 연결 및 구성 중 일부를 설명합니다.

연결성

각 사이트의 FlexPod Nexus 스위치는 고가용성 구성에서 UCS 컴퓨팅과 ONTAP 스토리지 간의 로컬 연결을 제공합니다. 이중화 구성 요소와 이중화 연결을 통해 단일 장애 지점 시나리오에 대한 복원력을 제공합니다.

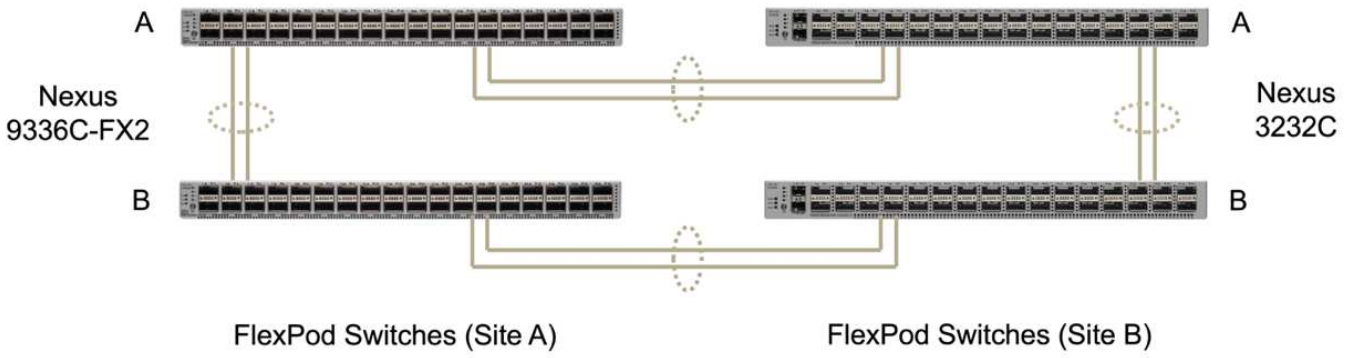
다음 다이어그램은 각 사이트의 Nexus 스위치 로컬 연결을 보여 줍니다. 다이어그램에 표시된 내용 외에 표시되지 않은 각 구성 요소에 대한 콘솔 및 관리 네트워크 연결도 있습니다. 40G~4 x 10G 브레이크아웃 케이블은 Nexus 스위치를 UCS FI 및 ONTAP AFF A250 스토리지 컨트롤러에 연결하는 데 사용됩니다. 또는 100G~4개의 25G 브레이크아웃 케이블을 사용하여 Nexus 스위치와 AFF A250 스토리지 컨트롤러 간의 통신 속도를 높일 수도 있습니다. 간단하게 하기 위해 2개의 AFF A250 컨트롤러는 케이블 연결 그림을 위해 논리적으로 나란히 표시됩니다. 두 스토리지 컨트롤러 간의 두 가지 연결을 통해 스토리지가 스위치가 없는 클러스터를 구성할 수 있습니다.



다음 표에는 각 사이트에 있는 Nexus 스위치와 AFF A250 스토리지 컨트롤러 간의 접속이 나와 있습니다.

로컬 장치	로컬 포트	원격 장치	원격 포트
Nexus A	1/10/1	AFF A250 A	E1A
	1/10/2		e1b
	1/10/3	AFF A250 B	E1A
	1/10/4		e1b
Nexus B	1/10/1	AFF A250 A	e1c
	1/10/2		e1d
	1/10/3	AFF A250 B	e1c
	1/10/4		e1d

사이트 A와 사이트 B의 FlexPod 스위치 간 연결은 다음 그림에 나와 있는 케이블 연결 세부 정보와 함께 표시됩니다. 각 사이트에 있는 두 스위치 간의 연결이 vPC 피어 링크에 대한 것입니다. 반면, 사이트 간 스위치 간의 연결은 사이트 간 링크를 제공합니다. 이 링크는 원격 사이트 리소스에 대한 인터클러스터 통신, SM-BC 데이터 복제, 대역 내 관리 및 데이터 액세스를 위해 사이트 전체에서 VLAN을 확장합니다.



로컬 장치	로컬 포트	원격 장치	원격 포트
사이트 A 스위치 A	33	사이트 B 스위치 A	31
	34		32
	25	사이트 A 스위치 B	25
	26		26
사이트 A 스위치 B	33	사이트 B 스위치 B	31
	34		32
	25	사이트 A 스위치 A	25
	26		26
사이트 B 스위치 A	31	사이트 A 스위치 A	33
	32		34
	25	사이트 B 스위치 B	25
	26		26

로컬 장치	로컬 포트	원격 장치	원격 포트
사이트 B 스위치 B	31	사이트 A 스위치 B	33
	32		34
	25	사이트 B 스위치 A	25
	26		26

위 표에는 각 FlexPod 스위치의 관점에서 연결된 정보가 나와 있습니다. 따라서 표에 가독성을 위한 중복 정보가 포함되어 있습니다.

포트 채널 및 가상 포트 채널입니다

포트 채널은 대역폭 집선 및 링크 장애 복구를 위해 LACP(Link Aggregation Control Protocol)를 사용하여 링크 집계를 활성화합니다. 가상 포트 채널(vPC)을 사용하면 두 Nexus 스위치 간의 포트 채널 연결이 논리적으로 하나로 표시됩니다. 따라서 단일 링크 장애 또는 단일 스위치 장애와 같은 시나리오에 대한 장애 복구 성능이 더욱 향상됩니다.

스토리지에 대한 UCS 서버 트래픽은 IOM A에서 FI A로, IOM B에서 FI B로 경로를 가져가 Nexus 스위치에 도달하기 전에 먼저 합니다. Nexus 스위치에 대한 Fi 연결이 FI 측의 포트 채널과 Nexus 스위치 측의 가상 포트 채널을 활용함에 따라 UCS 서버는 두 Nexus 스위치를 통해 경로를 효과적으로 사용할 수 있으며 단일 장애 지점 시나리오에서도 유지될 수 있습니다. 이전 그림과 같이 두 사이트 간에 Nexus 스위치가 상호 연결되어 있습니다. 사이트 간에 스위치 쌍을 연결하는 링크는 각각 두 개이며 포트 채널 구성도 사용합니다.

대역 내 관리, 클러스터 간 및 iSCSI/NFS 데이터 스토리지 프로토콜 연결은 중복 구성에서 각 사이트의 스토리지 컨트롤러를 로컬 Nexus 스위치에 상호 연결하여 제공됩니다. 각 스토리지 컨트롤러는 2개의 Nexus 스위치에 연결됩니다. 스토리지 인터페이스 그룹의 일부로 구성된 4개의 연결은 복구 성능을 높여 줍니다. Nexus 스위치 측에서는 이러한 포트도 스위치 간 vPC에 속합니다.

다음 표에는 각 사이트의 포트 채널 ID 및 사용량이 나열되어 있습니다.

포트 채널 **ID**입니다	사용
10	로컬 Nexus 피어 링크
15	패브릭 인터커넥트 A 링크
16	패브릭 인터커넥트 B 링크
27	스토리지 컨트롤러 A 링크
28	스토리지 컨트롤러 B 링크
100	사이트 간 스위치 A 링크
200	사이트 간 스위치 B 링크

VLAN

다음 표에는 FlexPod SM-BC 솔루션 검증 환경을 설정하기 위해 구성된 VLAN과 해당 사용량이 나열되어 있습니다.

이름	**VLAN ID**입니다	사용
네이티브 - VLAN	2	기본 VLAN 대신 기본 VLAN으로 사용되는 VLAN 2(1)

이름	**VLAN ID**입니다	사용
OOB-MGMT-VLAN	3333	장치용 대역외 관리 VLAN
IB-MGMT-VLAN	3334	ESXi 호스트에 대한 대역 내 관리 VLAN, VM 관리 등
NFS-VLAN	3335	NFS 트래픽용 선택적 NFS VLAN
iSCSI-A-VLAN	3336	iSCSI - iSCSI 트래픽을 위한 패브릭 VLAN입니다
iSCSI-B-VLAN	3337	iSCSI 트래픽용 iSCSI-B 패브릭 VLAN
VMotion - VLAN	3338	VMware vMotion 트래픽 VLAN
VM-Traffic-VLAN	3339	VMware VM 트래픽 VLAN
인터클러스터 - VLAN	3340	ONTAP 클러스터 피어 통신을 위한 인터클러스터 VLAN

SM-BC는 비즈니스 연속성을 위해 NFS 또는 CIFS 프로토콜을 지원하지 않지만, 비즈니스 연속성을 위해 보호할 필요가 없는 워크로드에 사용할 수 있습니다. 이 검증을 위해 NFS 데이터 저장소가 생성되지 않았습니다.

"다음: 솔루션 검증 - 스토리지."

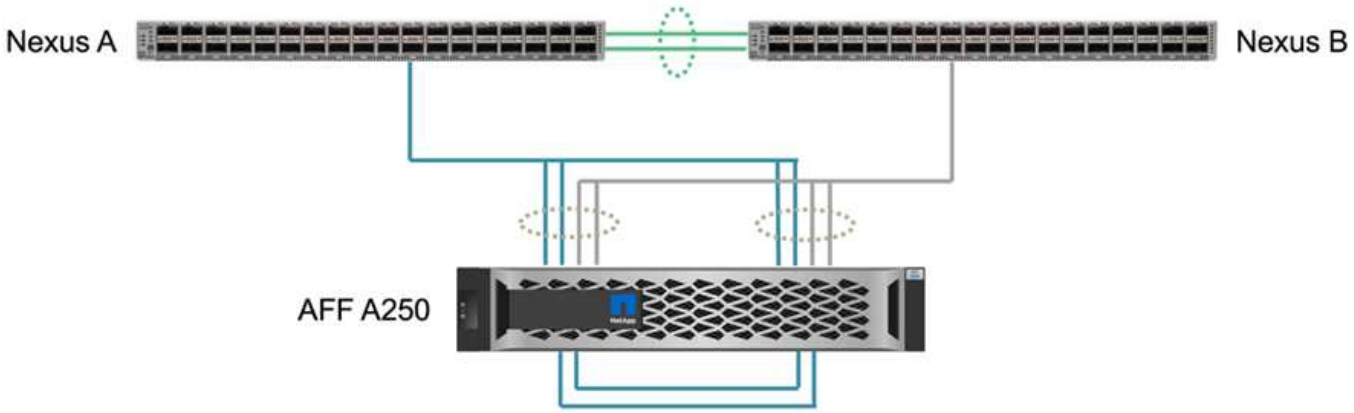
솔루션 검증 **-** 스토리지

"이전: 솔루션 검증 - 네트워크."

FlexPod SM-BC 솔루션의 스토리지 구성은 각 사이트의 일반적인 FlexPod 솔루션 모범 사례를 따릅니다. SM-BC 클러스터 피어링과 데이터 복제의 경우 두 사이트의 FlexPod 스위치 간에 설정된 사이트 간 링크를 사용합니다. 다음 섹션에서는 검증에 사용된 연결 및 구성 중 일부를 설명합니다.

연결성

로컬 UCS FI 및 블레이드 서버에 대한 스토리지 연결은 로컬 사이트의 Nexus 스위치를 통해 제공됩니다. 사이트 간 Nexus 스위치 연결을 통해 원격 UCS 블레이드 서버에서도 스토리지에 액세스할 수 있습니다. 다음 그림과 표에서는 스토리지 연결 다이어그램과 각 사이트의 스토리지 컨트롤러에 대한 연결 목록을 보여 줍니다.

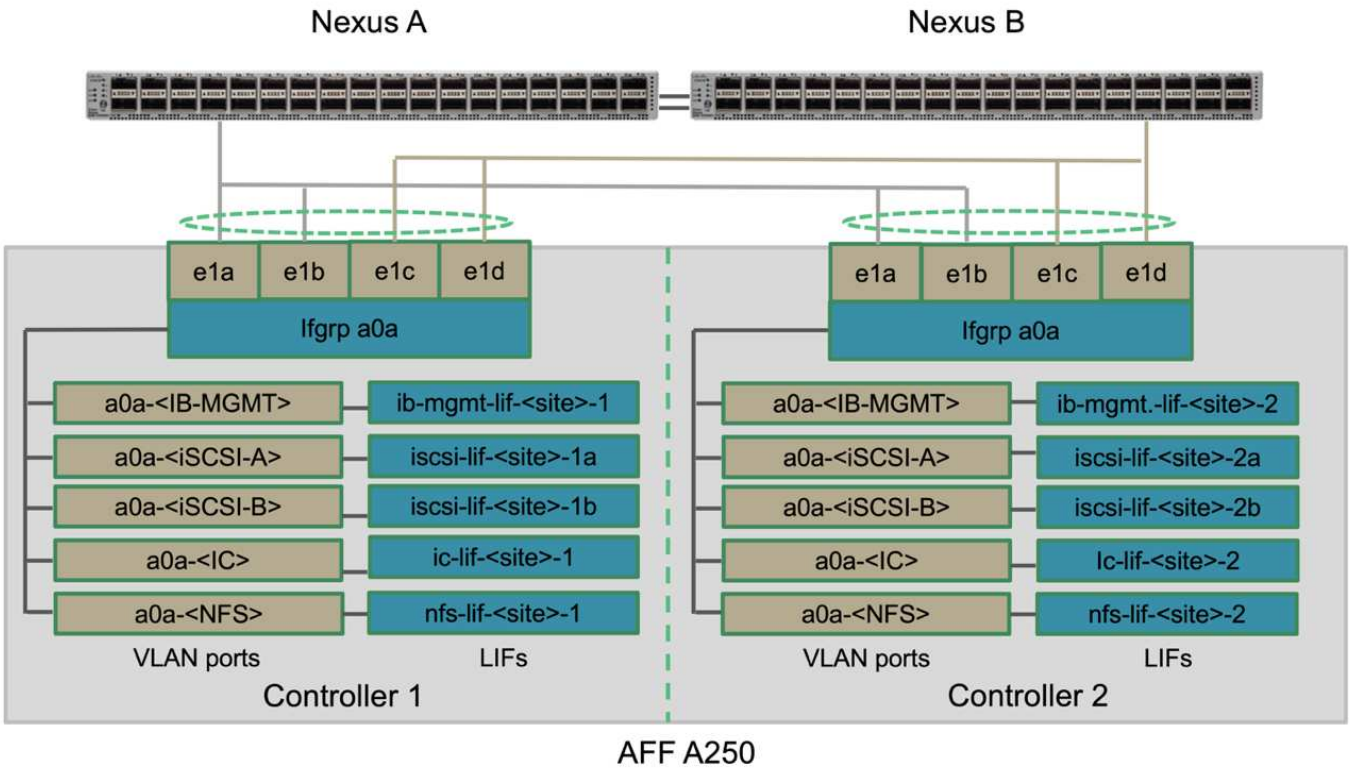


로컬 장치	로컬 포트	원격 장치	원격 포트
AFF A250 A	e0c	AFF A250 B	e0c
	e0d		e0d
	E1A	Nexus A	1/10/1
	e1b		1/10/2
	e1c	Nexus B	1/10/1
	e1d		1/10/2
AFF A250 B	e0c	AFF A250 A	e0c
	e0d		e0d
	E1A	Nexus A	1/10/3
	e1b		1/10/4
	e1c	Nexus B	1/10/3
	e1d		1/10/4

연결 및 인터페이스

각 스토리지 컨트롤러의 물리적 포트 2개가 각 Nexus 스위치에 연결되어 대역폭 애그리게이션 및 이중화를 위해 제공됩니다. 이러한 4개의 접속은 스토리지의 인터페이스 그룹 구성에 포함됩니다. Nexus 스위치의 해당 포트는 링크 집선 및 복원력에 대한 vPC에 사용됩니다.

대역 내 관리, 클러스터 간 및 NFS/iSCSI 데이터 스토리지 프로토콜은 VLAN을 사용합니다. VLAN 포트는 인터페이스 그룹에 생성되어 다른 유형의 트래픽을 분리합니다. 각 기능에 대한 논리 인터페이스(LIF)는 해당 VLAN 포트 위에 생성됩니다. 다음 그림에서는 물리적 연결, 인터페이스 그룹, VLAN 포트 및 논리 인터페이스 간의 관계를 보여 줍니다.

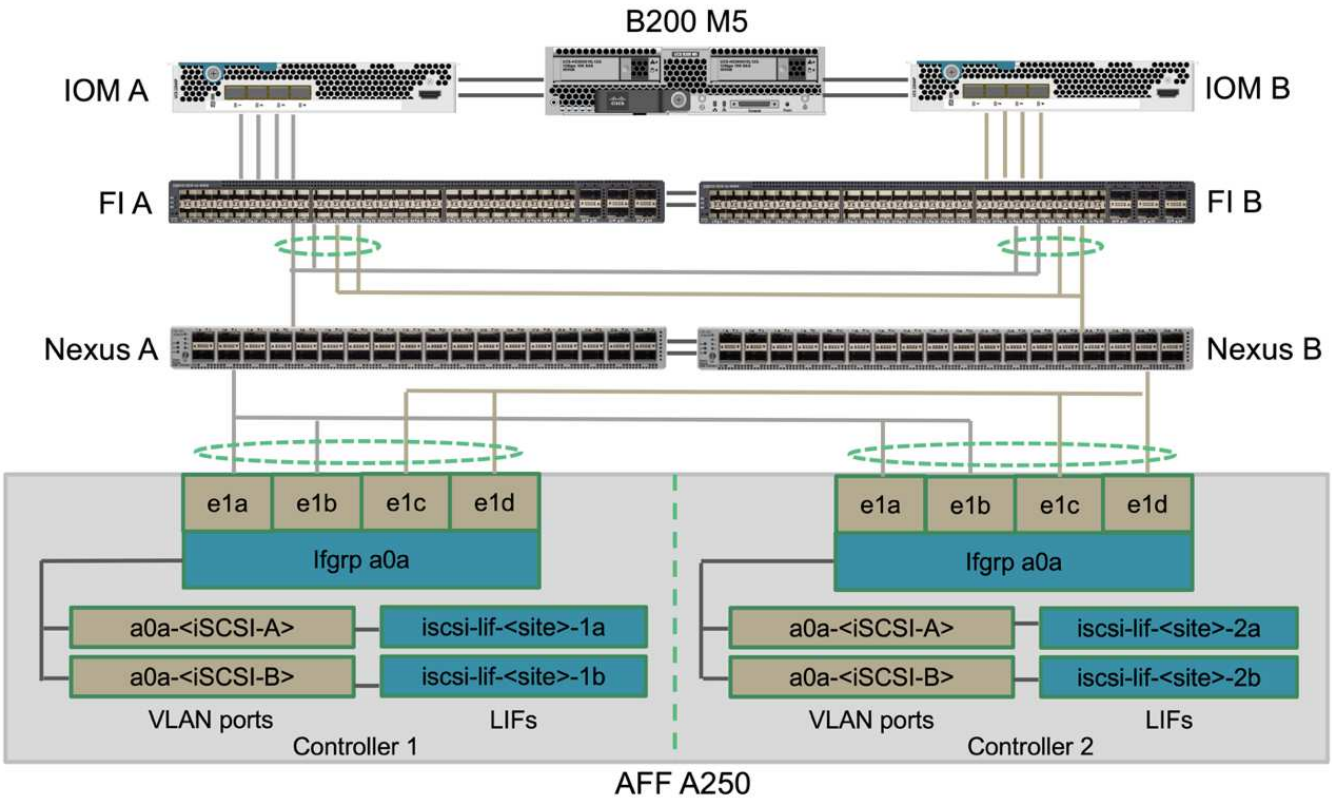


SAN 부팅

FlexPod 솔루션에서 Cisco UCS 서버용 SAN 부트를 구현하는 것이 좋습니다. SAN 부팅을 구현하면 NetApp 스토리지 시스템 내에서 운영 체제를 안전하게 보호할 수 있으므로 더 나은 성능과 유연성을 얻을 수 있습니다. 이 솔루션의 경우 iSCSI SAN 부팅이 검증되었습니다.

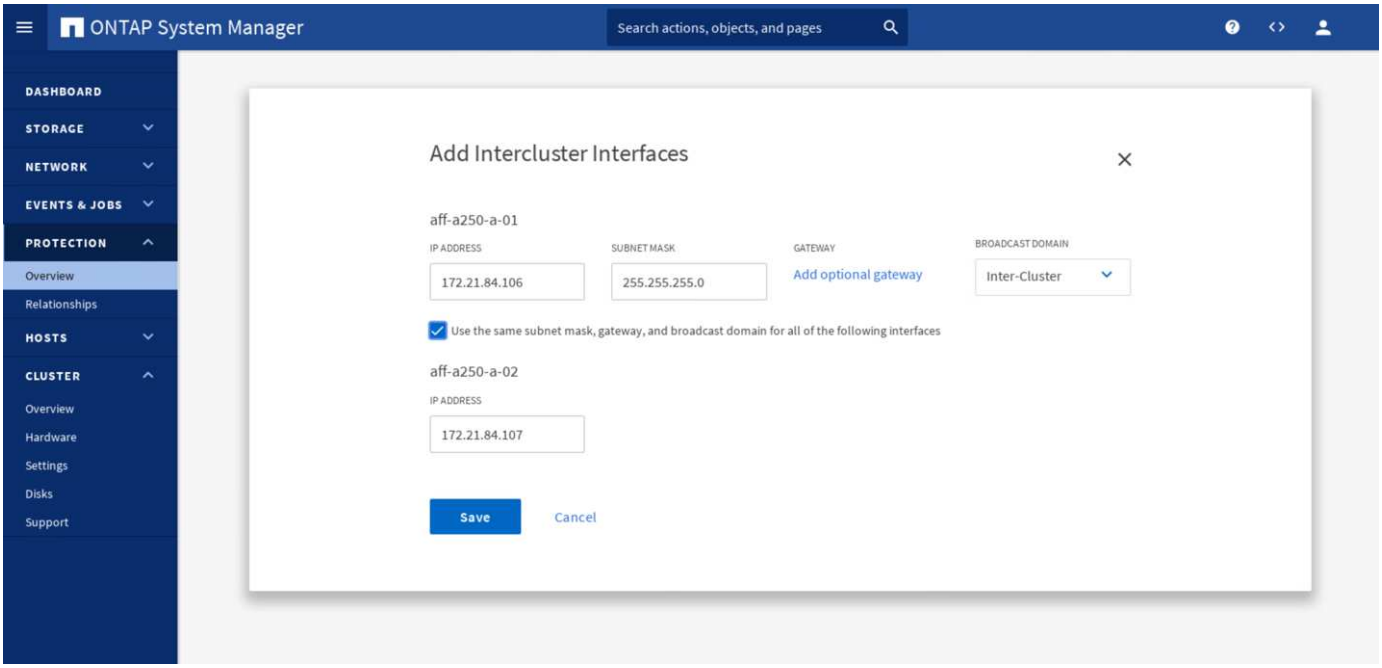
다음 그림은 NetApp 스토리지에서 Cisco UCS 서버의 iSCSI SAN 부팅에 대한 연결을 보여 줍니다. iSCSI SAN 부팅에서 각 Cisco UCS 서버에는 서버에서 스토리지까지 모두 이중화된 연결을 제공하는 2개의 iSCSI vNIC(각 SAN 패브릭당 1개)가 할당됩니다. Nexus 스위치에 연결된 10/25-G 이더넷 스토리지 포트(이 예에서는 E1A, e1b, e1c 및 e1d)는 함께 그룹화하여 하나의 인터페이스 그룹(ifgrp)을 구성합니다(이 예에서는 a0a). iSCSI VLAN 포트는 ifgrp에서 생성되며 iSCSI VLAN 포트에서 iSCSI LIF가 생성됩니다.

각 iSCSI 부트 LUN은 부트 igroup에서 부트 LUN을 서버의 IQN(iSCSI 정규화된 이름)과 연결하여 iSCSI LIF를 통해 부팅되는 서버에 매핑됩니다. 서버의 부팅 igroup에는 각 vNIC/SAN 패브릭마다 하나씩 두 개의 IQN이 포함되어 있습니다. 이 기능을 사용하면 권한이 부여된 서버만 해당 서버에 대해 특별히 생성된 부팅 LUN에 액세스할 수 있습니다.



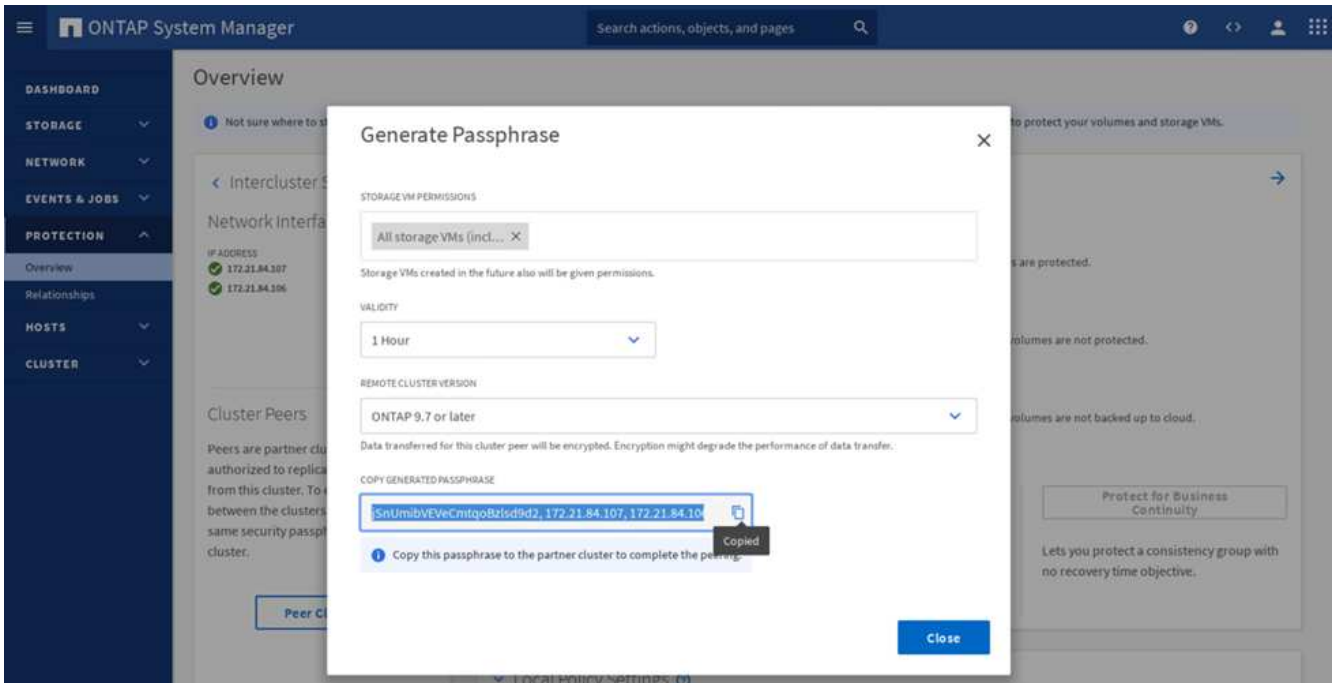
클러스터 피어링

ONTAP 클러스터 피어는 인터클러스터 LIF를 통해 통신합니다. ONTAP System Manager를 사용하여 두 클러스터에 대해 보호 > 개요 창에서 필요한 인터클러스터 LIF를 만들 수 있습니다.

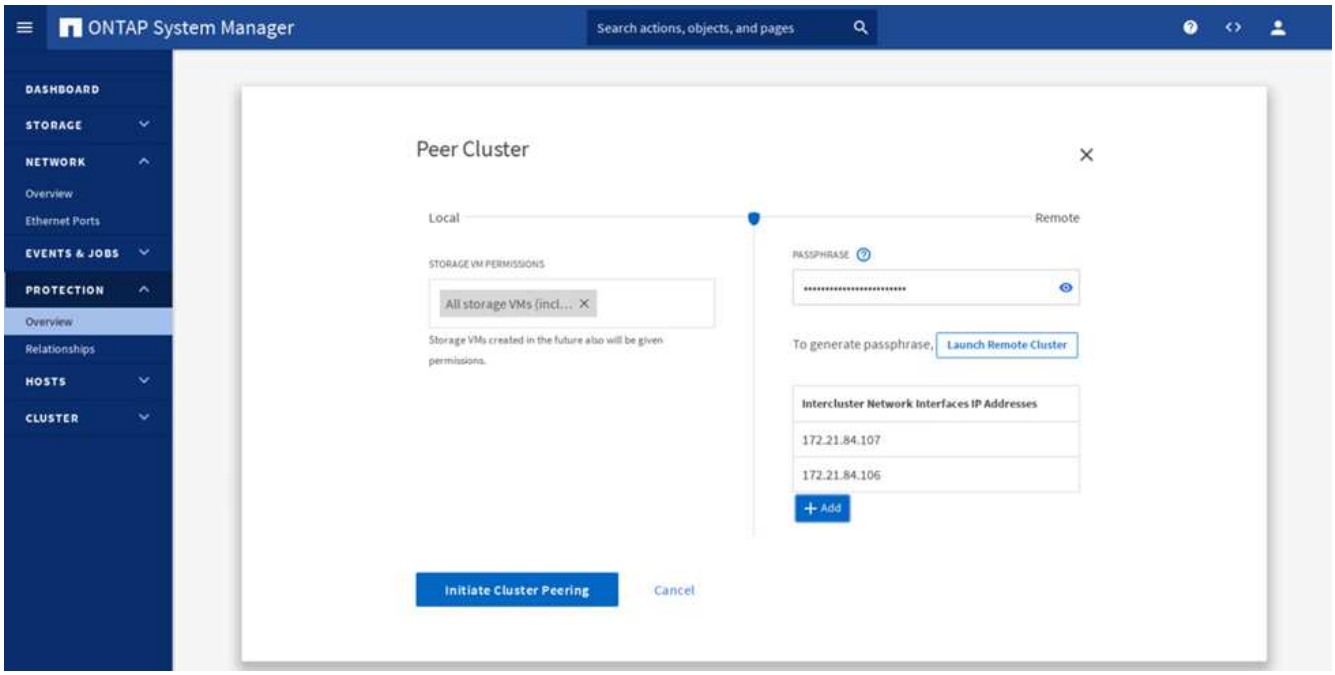


두 클러스터를 함께 클러스터하려면 다음 단계를 완료하십시오.

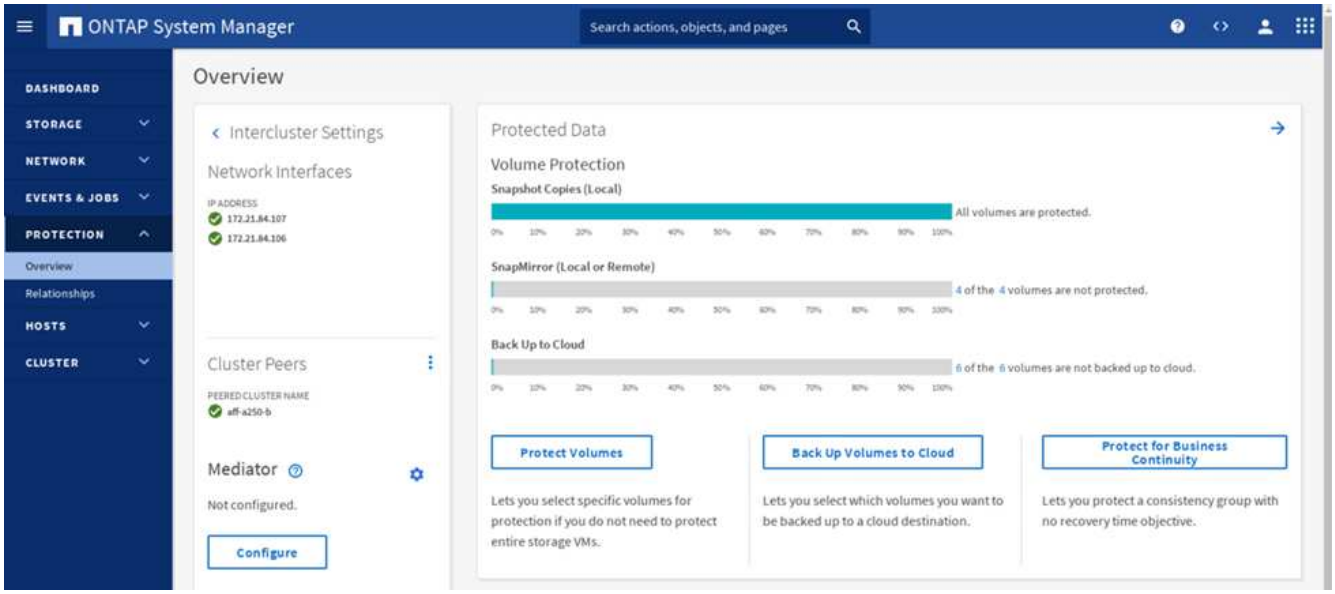
1. 첫 번째 클러스터에서 클러스터 피어링 암호를 생성합니다.



2. 두 번째 클러스터에서 피어 클러스터 옵션을 호출하고 암호 구문 및 인터클러스터 LIF 정보를 제공합니다.



3. System Manager 보호 > 개요 창에 클러스터 피어 정보가 표시됩니다.

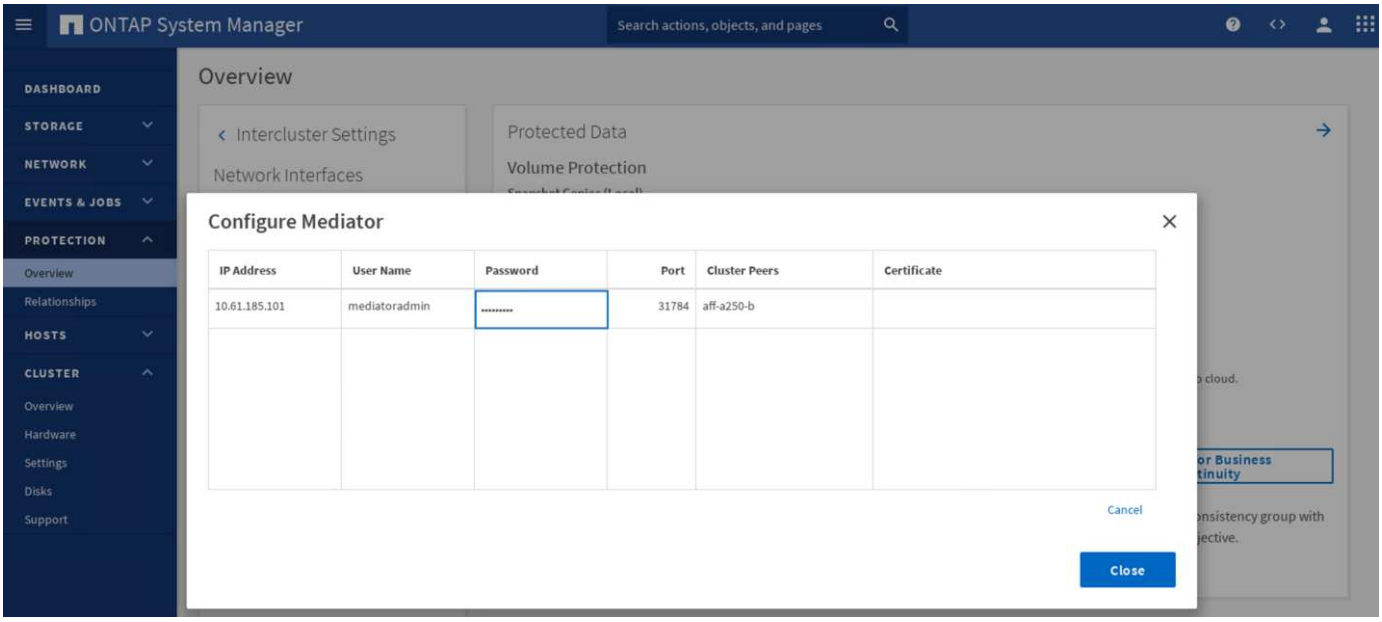


ONTAP 중재자 설치 및 구성

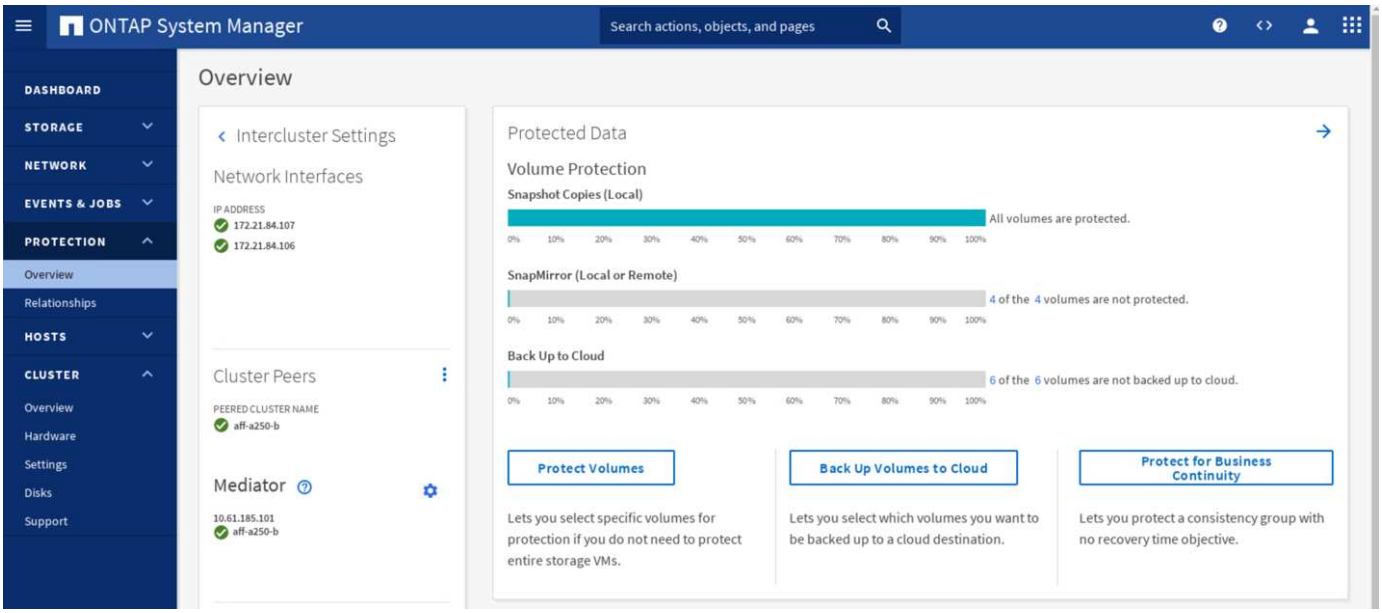
ONTAP 중재자가 SM-BC 관계에서 ONTAP 클러스터에 대한 쿼럼을 설정합니다. 장애가 감지되면 자동 장애 조치를 조정하고 각 클러스터가 동시에 기본 클러스터로 제어를 설정하려고 할 때 브레인 분할 시나리오를 방지하는 데 도움이 됩니다.

ONTAP 중재자를 설치하기 전에 을 확인하십시오 "ONTAP 중재자 서비스를 설치하거나 업그레이드합니다" 사전 요구 사항, 지원되는 Linux 버전 및 지원되는 다양한 Linux 운영 체제에 설치하는 절차를 보려면 페이지를 참조하십시오.

ONTAP 중재자를 설치한 후 ONTAP 클러스터에 ONTAP 중재자의 보안 인증서를 추가한 다음 System Manager 보호 > 개요 창에서 ONTAP 중재자를 구성할 수 있습니다. 다음 스크린샷은 ONTAP 중재자 구성 GUI를 보여 줍니다.



필요한 정보를 제공하면 구성된 ONTAP 중재자가 시스템 관리자 보호 > 개요 창에 나타납니다.



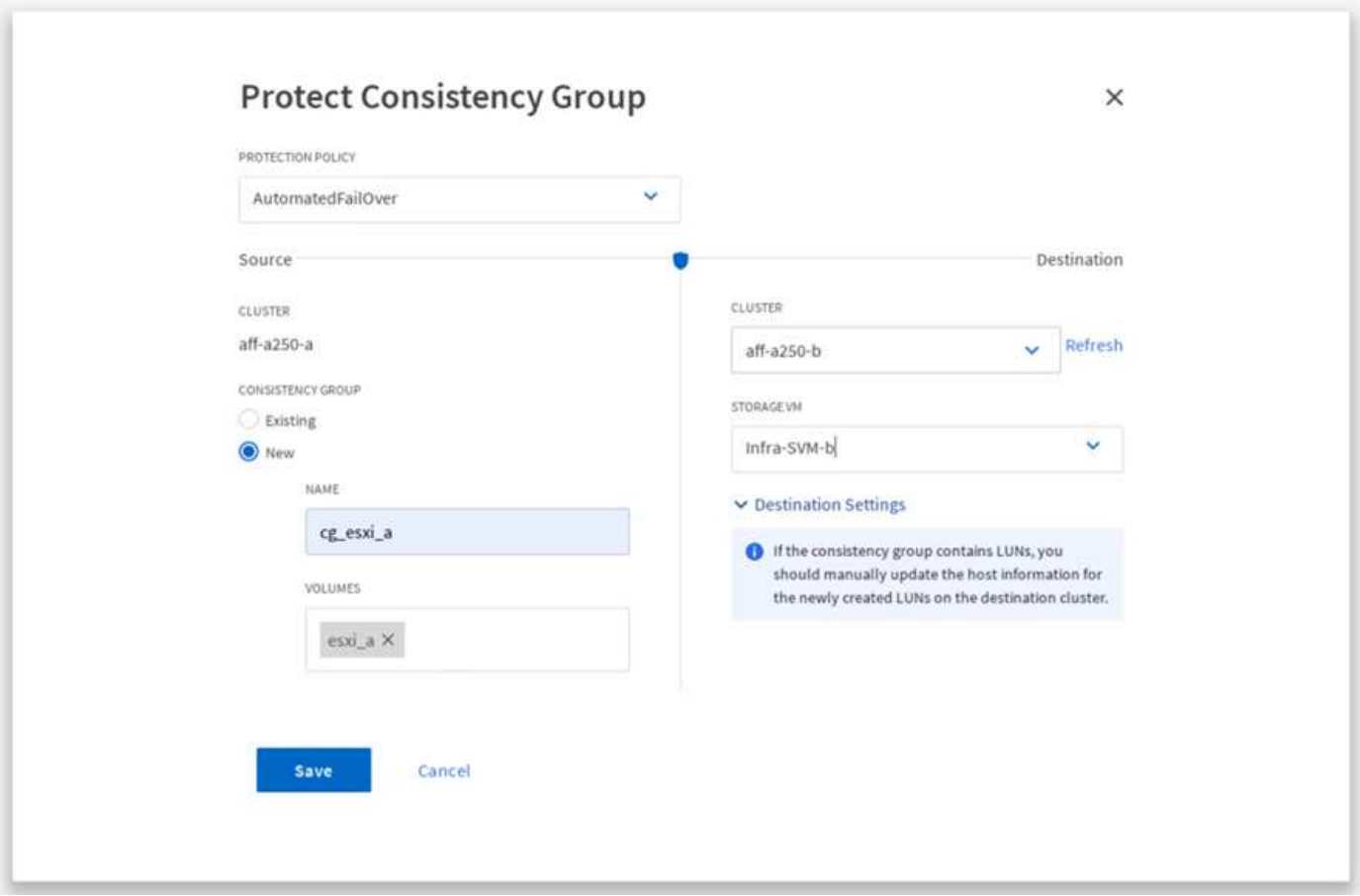
SM-BC 정합성 보장 그룹

정합성 보장 그룹은 지정된 볼륨 컬렉션을 포함하는 애플리케이션 워크로드에 대해 쓰기 순서 정합성을 보장합니다. ONTAP 9.10.1의 경우 몇 가지 중요한 제한 사항과 제한 사항이 있습니다.

- 클러스터에서 SM-BC 정합성 보장 그룹 관계의 최대 수는 20개입니다.
- SM-BC 관계당 지원되는 최대 볼륨 수는 16개입니다.
- 클러스터의 총 소스 및 대상 엔드포인트의 최대 수는 200개입니다.

자세한 내용은 의 ONTAP SM-BC 설명서를 참조하십시오 "제한 및 제한 사항".

검증 구성의 경우 ONTAP System Manager를 사용하여 정합성 보장 그룹을 생성하여 ESXi 부팅 LUN과 두 사이트의 공유 데이터 저장소 LUN을 모두 보호했습니다. 정합성 보장 그룹 생성 대화 상자는 보호 > 개요 > 무중단 업무 운영 보호 > 정합성 보장 그룹 보호 로 이동하여 액세스할 수 있습니다. 정합성 보장 그룹을 생성하려면 필요한 소스 볼륨, 대상 클러스터 및 대상 스토리지 가상 머신 정보를 생성하여 생성합니다.

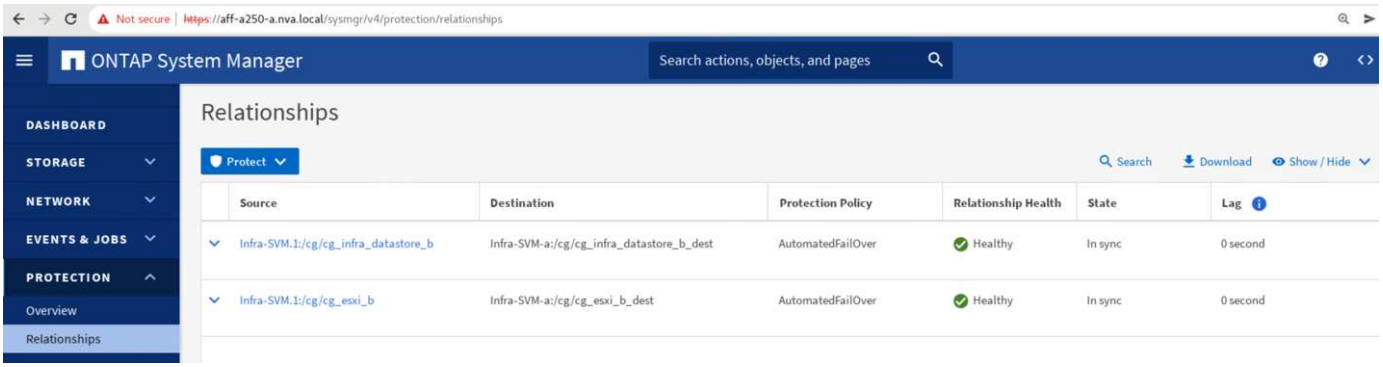


다음 표에는 검증 테스트를 위해 생성된 4개의 정합성 보장 그룹과 각 정합성 보장 그룹에 포함된 볼륨이 나와 있습니다.

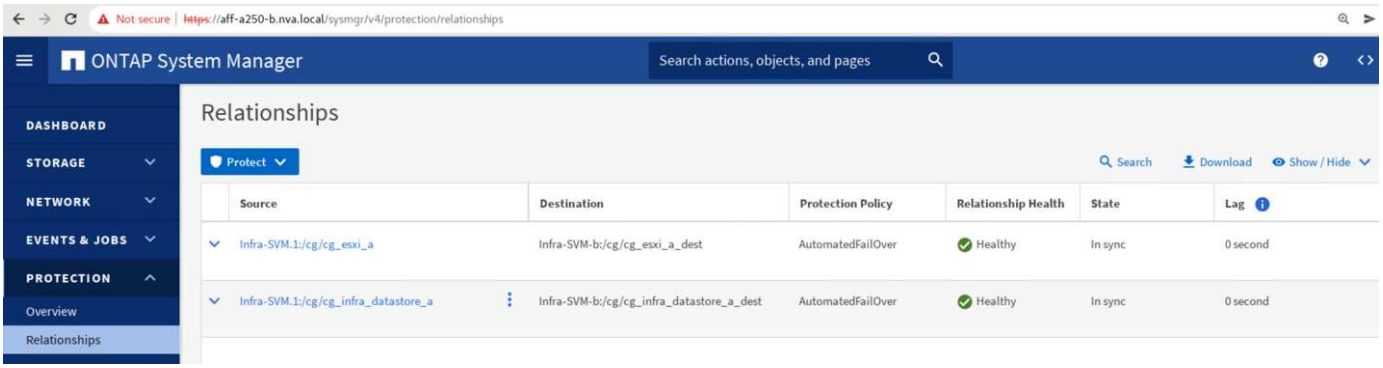
시스템 관리자	일관성 그룹	볼륨
사이트 A	CG_ESXi_A	ESXi_A
사이트 A	cg_infra_datastore_a입니다	infra_datastore_A_01 infra_datastore_A_02
사이트 B	CG_ESXi_b입니다	ESXi_b
사이트 B	cg_infra_datastore_b입니다	infra_datastore_b_01 infra_datastore_b_02

일관성 그룹이 생성된 후에는 사이트 A 및 사이트 B의 해당 보호 관계 아래에 표시됩니다

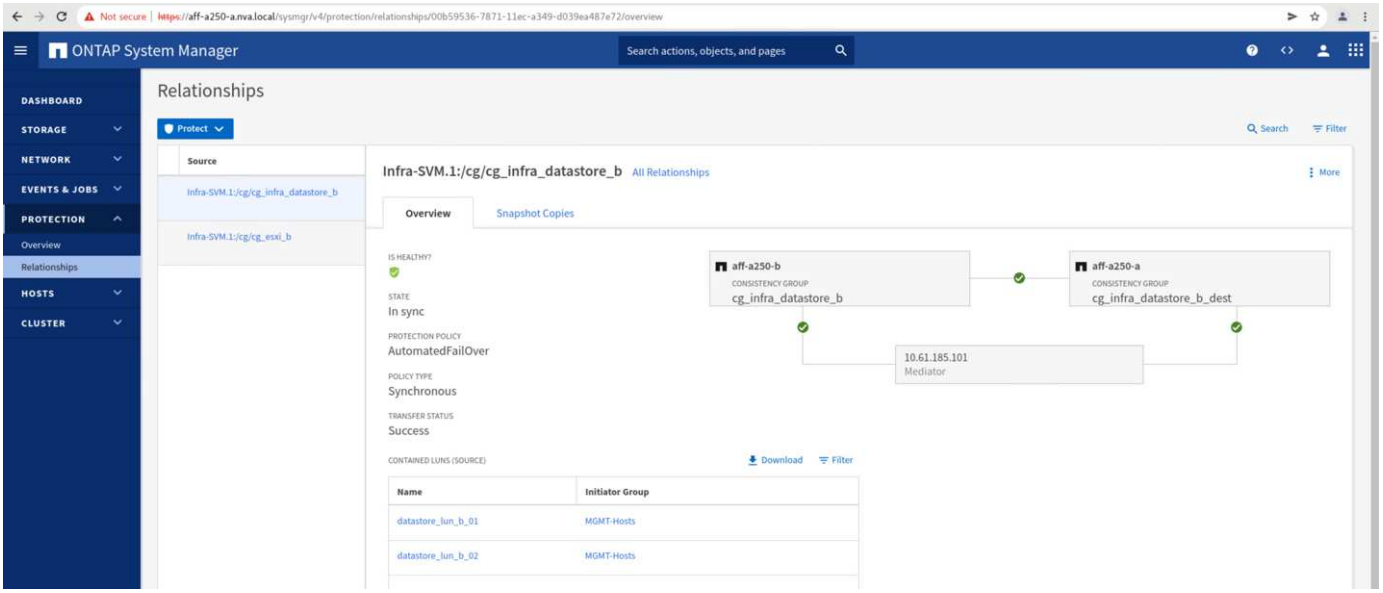
이 스크린샷은 사이트 A의 일관성 그룹 관계를 보여 줍니다



이 스크린샷은 사이트 B의 일관성 그룹 관계를 보여 줍니다



이 스크린샷은 CG_infra_datastore_b 그룹에 대한 정합성 보장 그룹 관계 세부 정보를 보여 줍니다.



볼륨, **LUN** 및 호스트 매핑

일관성 그룹이 생성되고 나면 SnapMirror는 소스 볼륨과 타겟 볼륨을 동기화하여 데이터가 항상 동기화될 수 있도록 합니다. 원격 사이트의 대상 볼륨은 _ dest가 끝나는 볼륨 이름을 전달합니다. 예를 들어 사이트 A 클러스터의 ESXi_A 볼륨의 경우 사이트 B에 해당하는 ESXi_A_dest 데이터 보호(DP) 볼륨이 있습니다

이 스크린샷은 사이트 A의 볼륨 정보를 보여 줍니다

```
aff-a250-a::> vol show -vserver Infra-SVM-a
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-a esxi_a     aggr1_aff_a250_a_01 online RW     320GB    315.9GB    1%
Infra-SVM-a esxi_b_dest aggr1_aff_a250_a_02 online DP   3.86GB    638.4MB   83%
Infra-SVM-a infra_datastore_a_01 aggr1_aff_a250_a_01 online RW 1TB 717.6GB  29%
Infra-SVM-a infra_datastore_a_02 aggr1_aff_a250_a_02 online RW 1TB 828.4GB  19%
Infra-SVM-a infra_svm_root aggr1_aff_a250_a_01 online RW   1GB    966.5MB    0%
Infra-SVM-a infra_svm_root_m01 aggr1_aff_a250_a_01 online LS 1GB  966.6MB    0%
Infra-SVM-a infra_svm_root_m02 aggr1_aff_a250_a_02 online LS 1GB  966.6MB    0%
Infra-SVM-a vol_infra_datastore_b_01_dest aggr1_aff_a250_a_01 online DP 138.7GB 31.52GB  76%
Infra-SVM-a vol_infra_datastore_b_02_dest aggr1_aff_a250_a_01 online DP 49.37GB 9.03GB  80%
9 entries were displayed.
```

이 스크린샷은 사이트 B의 볼륨 정보를 보여 줍니다

```
aff-a250-b::> vol show -vserver Infra-SVM-b
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-b esxi_a_dest aggr1_aff_a250_b_02 online DP   4.10GB    768.2MB   80%
Infra-SVM-b esxi_b     aggr1_aff_a250_b_01 online RW     320GB    315.8GB    1%
Infra-SVM-b infra_datastore_b_01 aggr1_aff_a250_b_01 online RW 1TB 911.9GB  10%
Infra-SVM-b infra_datastore_b_02 aggr1_aff_a250_b_02 online RW 1TB 964.0GB   5%
Infra-SVM-b infra_svm_root aggr1_aff_a250_b_01 online RW   1GB    966.9MB    0%
Infra-SVM-b infra_svm_root_m01 aggr1_aff_a250_b_01 online LS 1GB  967.0MB    0%
Infra-SVM-b infra_svm_root_m02 aggr1_aff_a250_b_02 online LS 1GB  967.0MB    0%
Infra-SVM-b vol_infra_datastore_a_01_dest aggr1_aff_a250_b_02 online DP 270.0GB 27.39GB  89%
Infra-SVM-b vol_infra_datastore_a_02_dest aggr1_aff_a250_b_02 online DP 202.8GB 28.20GB  85%
9 entries were displayed.
```

투명한 애플리케이션 페일오버를 지원하기 위해 미러링된 SM-BC LUN도 대상 클러스터의 호스트에 매핑되어야 합니다. 이를 통해 호스트는 소스 클러스터와 대상 클러스터 모두에서 LUN에 대한 경로를 올바르게 볼 수 있습니다. 사이트 A와 사이트 B의 "igroup show" 및 "lun show" 출력은 다음 두 스크린샷에서 캡처됩니다. 생성된 매핑에서 클러스터의 각 ESXi 호스트는 고유한 SAN 부팅 LUN을 ID 0으로, 4개의 모든 공유 iSCSI 데이터 저장소 LUN으로 인식합니다.

이 스크린샷은 사이트 A 클러스터의 호스트 igroup 및 LUN 매핑을 보여 줍니다.

```
aff-a250-a::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-a MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
Infra-SVM-a VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-a VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-a VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-a VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-a VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-a VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-a::> lun show -m
Vserver    Path                                        Igroup   LUN ID  Protocol
---------- ------------------------------------------  -------  ------  --------
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-01             VM-Host-Infra-a-01  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-02             VM-Host-Infra-a-02  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-03             VM-Host-Infra-a-03  0  iscsi
Infra-SVM-a /vol/esxi_a/swap_lun_a                     MGMT-Hosts   13  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-01        VM-Host-Infra-b-01  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-02        VM-Host-Infra-b-02  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-03        VM-Host-Infra-b-03  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/swap_lun_b                MGMT-Hosts   23  iscsi
Infra-SVM-a /vol/infra_datastore_a_01/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-a /vol/infra_datastore_a_02/datastore_lun_a_02  MGMT-Hosts  12  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_01_dest/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_02_dest/datastore_lun_b_02  MGMT-Hosts  22  iscsi
12 entries were displayed.
```

이 스크린샷은 사이트 B 클러스터에 대한 호스트 igroup 및 LUN 매핑을 보여 줍니다.

```
aff-a250-b::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-b MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-b VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-b VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-b VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-b VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-b::> lun show -m
Vserver    Path                                        Igroup   LUN ID  Protocol
---------- ------------------------------------------  -------  ------  --------
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-01      VM-Host-Infra-a-01  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-02      VM-Host-Infra-a-02  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-03      VM-Host-Infra-a-03  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/swap_lun_a              MGMT-Hosts   13  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-01           VM-Host-Infra-b-01  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-02           VM-Host-Infra-b-02  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-03           VM-Host-Infra-b-03  0  iscsi
Infra-SVM-b /vol/esxi_b/swap_lun_b                   MGMT-Hosts   23  iscsi
Infra-SVM-b /vol/infra_datastore_b_01/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-b /vol/infra_datastore_b_02/datastore_lun_b_02  MGMT-Hosts  22  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_01_dest/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_02_dest/datastore_lun_a_02  MGMT-Hosts  12  iscsi
12 entries were displayed.
```

"다음: 솔루션 검증 - 가상화."

솔루션 검증 - 가상화

"이전: 솔루션 검증 - 스토리지."

다중 사이트 FlexPod SM-BC 솔루션에서 단일 VMware vCenter가 전체 솔루션의 가상 인프라스트럭처 리소스를 관리합니다. 두 데이터 센터의 호스트는 두 데이터 센터를 포괄하는 단일 VMware HA 클러스터에 참여합니다. 호스트는 정의된 SM-BC 관계가 있는 스토리지를 두 사이트 모두에서 액세스할 수 있는 NetApp SM-BC 솔루션에 액세스할 수 있습니다.

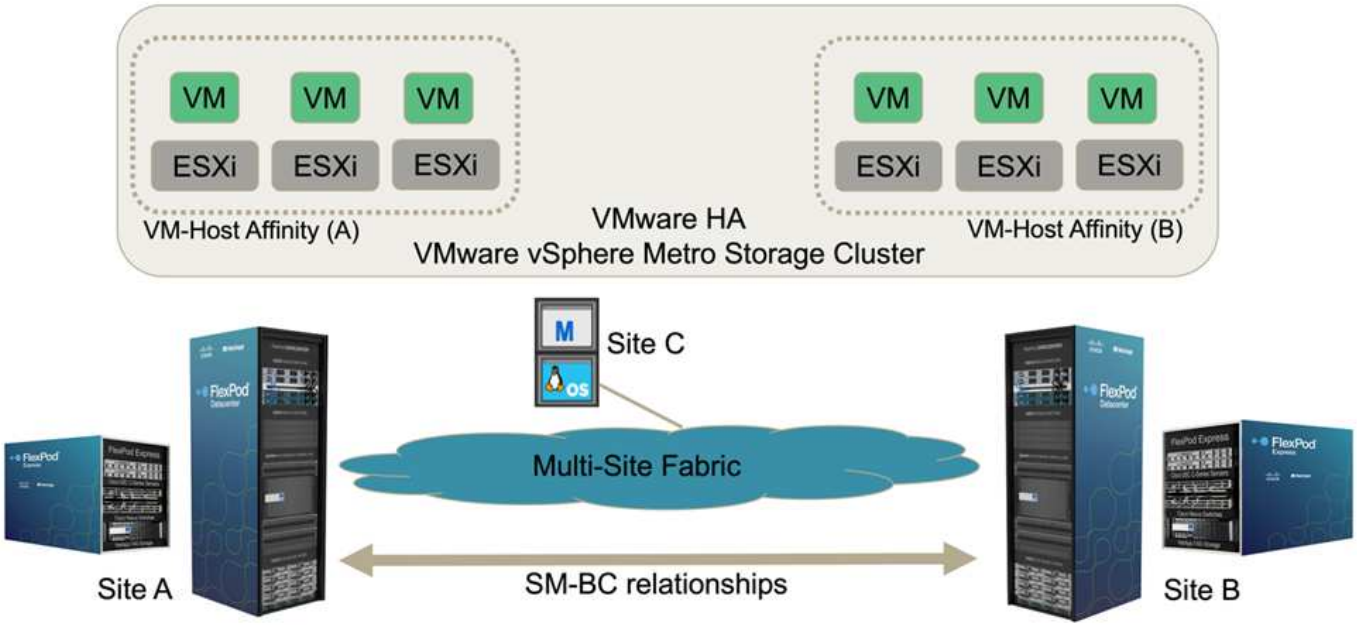
TH SM-BC 솔루션 스토리지는 VMware vMSC(vSphere Metro Storage Cluster) 기능의 일관된 액세스 모델을 준수하므로 재해 및 다운타임을 방지할 수 있습니다. 가상 시스템의 성능을 최적화하려면 로컬 NetApp AFF A250 시스템에서 가상 머신 디스크를 호스팅하여 WAN 링크 전반의 지연 시간 및 트래픽을 정상 운영 상태에서 최소화해야 합니다.

설계 구현의 일부로 두 사이트에 걸친 가상 시스템의 배포를 결정해야 합니다. 사이트 기본 설정 및 애플리케이션 요구 사항에 따라 두 사이트에 걸쳐 가상 머신 사이트 선호도와 애플리케이션 배포를 결정할 수 있습니다. VMware 클러스터 VM/호스트 그룹 및 VM/호스트 규칙은 VM/호스트 선호도를 구성하여 원하는 사이트의 호스트에서 VM이 실행되고 있는지 확인하는 데 사용됩니다.

그러나 두 사이트에서 VM을 실행할 수 있는 구성을 사용하면 원격 사이트 호스트의 VMware HA에서 VM을 다시

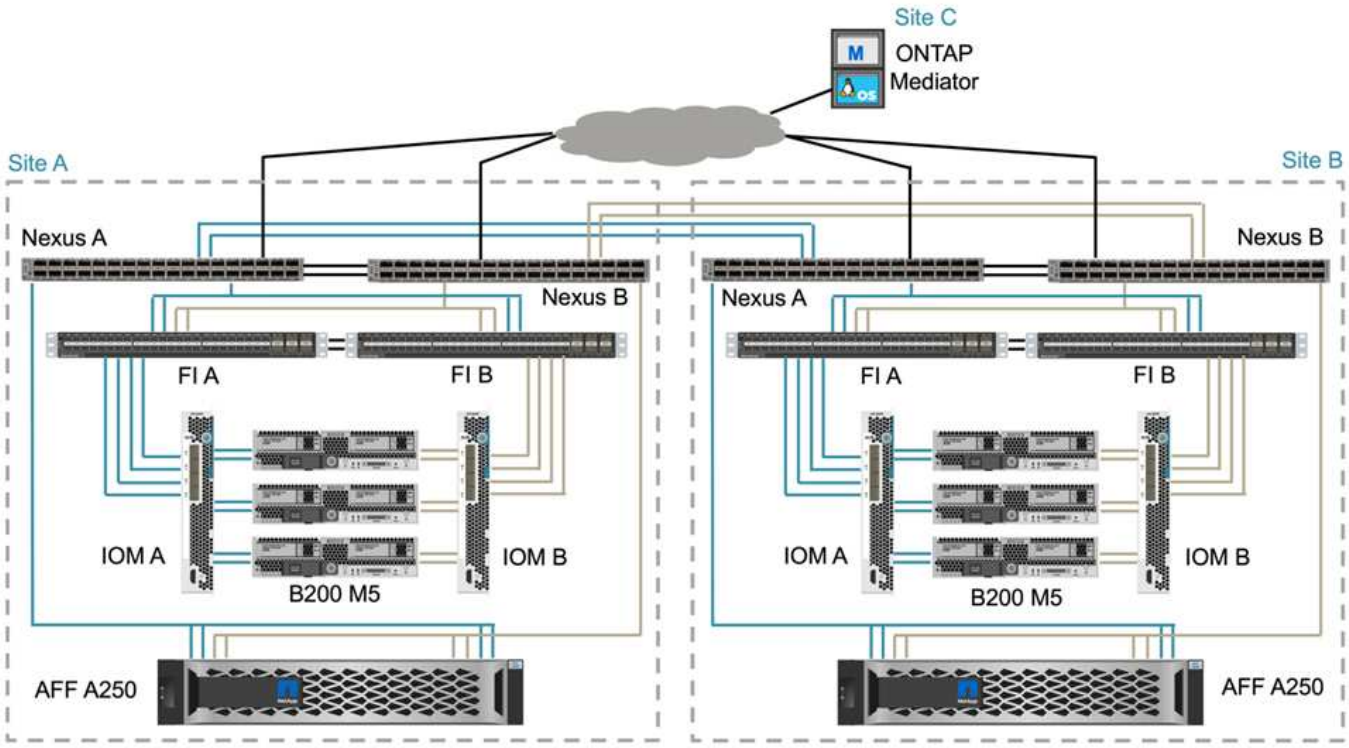
시작하여 솔루션 복원력을 제공할 수 있습니다. 두 사이트에서 실행할 가상 머신을 수용하려면 모든 ESXi 호스트에 모든 iSCSI 공유 데이터 저장소를 마운트하여 사이트 간에 가상 머신을 원활하게 vMotion 작업을 수행해야 합니다.

다음 그림에서는 컴퓨팅 및 스토리지 서비스에 고가용성을 제공하는 VMware HA 및 vMSC 기능을 모두 포함하는 상위 수준의 FlexPod SM-BC 솔루션 가상화 뷰를 보여 줍니다. 액티브-액티브 데이터 센터 솔루션 아키텍처는 사이트 간 워크로드 이동성을 지원하고 DR/BC 보호 기능을 제공합니다.



엔드 투 엔드 네트워크 연결

FlexPod SM-BC 솔루션에는 각 사이트의 FlexPod 인프라, 사이트 간 네트워크 연결 및 필요한 RPO 및 RTO 목표를 충족하기 위해 세 번째 사이트에 구축된 ONTAP 중재자가 포함됩니다. 다음 그림은 각 사이트의 Cisco UCS B200M5 서버와 사이트 내부 및 사이트 전체에서 SM-BC 기능을 지원하는 NetApp 스토리지 간의 엔드-투-엔드 네트워크 연결을 보여 줍니다.



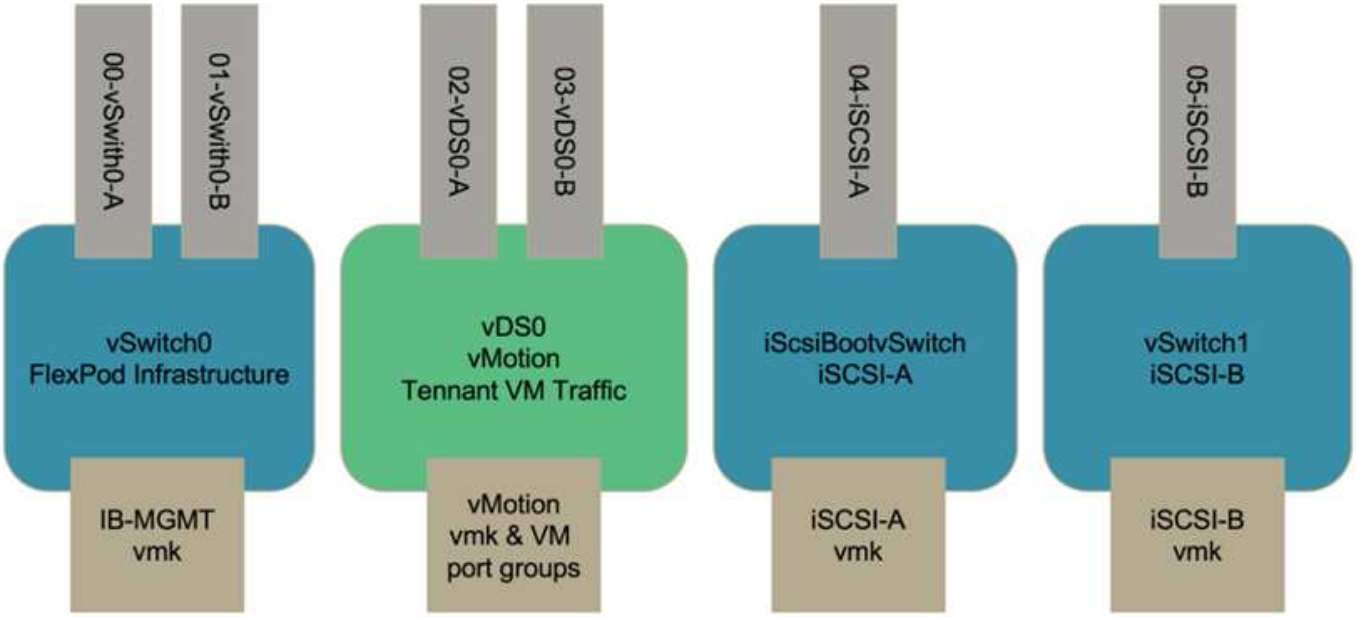
FlexPod 배포 아키텍처는 이 솔루션 유효성 검사를 위해 각 사이트에서 동일합니다. 그러나 이 솔루션은 비대칭 배포를 지원하며 요구 사항을 충족하는 기존 FlexPod 솔루션에 추가할 수도 있습니다.

확장된 계층 2 아키텍처는 각 데이터 센터에서 포트 채널형 Cisco UCS 컴퓨팅과 NetApp 스토리지 간의 연결과 데이터 센터 간의 연결을 제공하는 원활한 다중 사이트 데이터 패브릭에 사용됩니다. 필요한 경우 포트 채널 구성 및 가상 포트 채널 구성은 컴퓨팅, 네트워크 및 스토리지 계층 간의 대역폭 집계 및 내결함성 및 사이트 간 링크에 사용됩니다. 따라서 UCS 블레이드 서버는 로컬 및 원격 NetApp 스토리지 모두에 대한 연결 및 다중 경로 액세스를 지원합니다.

가상 네트워킹

클러스터의 각 호스트는 위치에 관계없이 동일한 가상 네트워킹을 사용하여 구축됩니다. 이 설계는 VMware 가상 스위치(vSwitch)와 VMware vDS(Virtual Distributed Switch)를 사용하여 다양한 트래픽 유형을 분리합니다. VMware vSwitch는 주로 FlexPod 인프라스트럭처 네트워크에 사용되고 vDS는 애플리케이션 네트워크에 사용되나 반드시 필요한 것은 아닙니다.

가상 스위치(vSwitch, VDS)는 가상 스위치당 2개의 업링크와 함께 구축되며, ESXi 하이퍼바이저 레벨의 업링크를 Cisco UCS 소프트웨어에서 vmnics 및 vNIC(Virtual NIC)라고 합니다. vNIC는 Cisco UCS 서비스 프로필을 사용하여 각 서버의 Cisco UCS VIC 어댑터에 생성됩니다. vNIC 6개가 정의되었으며, vSwitch0의 경우 2개, vDS0의 경우 2개, vSwitch1의 경우 2개, iSCSI 업링크의 경우 2개가 정의됩니다.



vSwitch0은 VMware ESXi 호스트 구성 중에 정의되며 FlexPod 인프라스트럭처 관리 VLAN 및 관리를 위한 ESXi 호스트 VMK(VMkernel) 포트가 포함되어 있습니다. 필요한 모든 중요 인프라스트럭처 관리 가상 머신에 대해 인프라스트럭처 관리 가상 머신 포트 그룹도 vSwitch0에 배치됩니다.

FlexPod 인프라를 종료하거나 전원을 껐다가 켠 후 원래 실행 중인 호스트가 아닌 호스트에서 해당 관리 가상 시스템을 활성화하려고 할 경우 VDS 대신 vSwitch0에 이러한 관리 인프라 가상 시스템을 배치하는 것이 중요합니다. vSwitch0의 네트워크에서 정상적으로 부팅됩니다. 이 프로세스는 VMware vCenter가 관리 가상 머신인 경우 특히 중요합니다. vCenter가 VDS에 있고 다른 호스트로 이동한 다음 부팅된 경우 부팅 후 네트워크에 연결되지 않습니다.

이 설계에는 두 개의 iSCSI 부트 vSwitch가 사용됩니다. Cisco UCS iSCSI 부팅에는 iSCSI 부팅을 위한 별도의 vNIC가 필요합니다. 이러한 vNIC는 해당 패브릭의 iSCSI VLAN을 기본 VLAN으로 사용하며 해당 iSCSI 부트 vSwitch에 연결됩니다. 필요에 따라 새 VDS를 배포하거나 기존 VDS를 사용하여 VDS에 iSCSI 네트워크를 배포할 수도 있습니다.

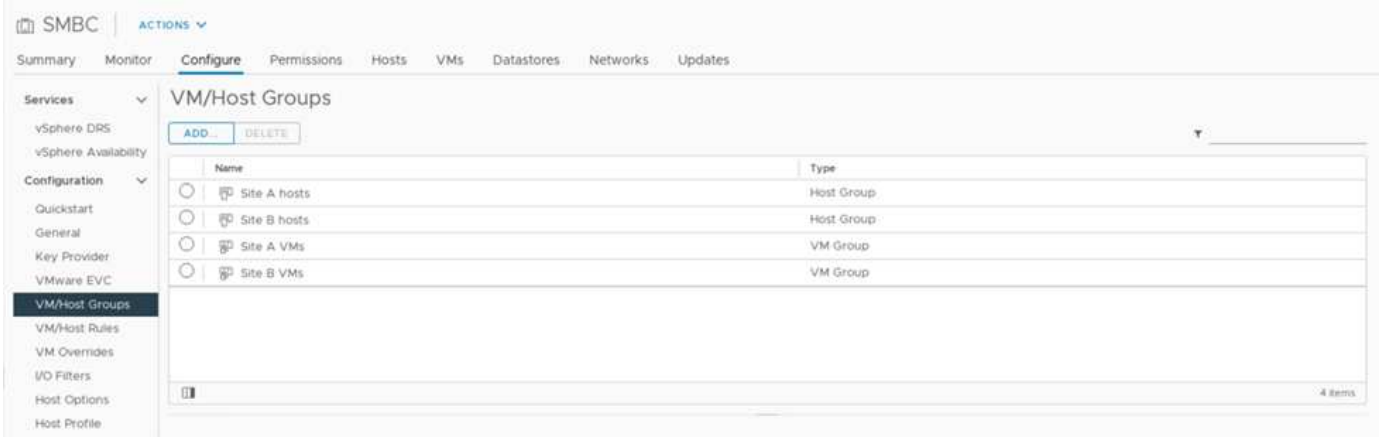
VM-호스트 선호도 그룹 및 규칙

두 SM-BC 사이트의 ESXi 호스트에서 가상 머신을 실행하려면 모든 ESXi 호스트가 두 사이트에서 iSCSI 데이터 저장소를 마운트해야 합니다. 두 사이트의 데이터 저장소가 모든 ESXi 호스트에 의해 올바르게 마운트된 경우 vMotion을 사용하는 모든 호스트 간에 가상 머신을 마이그레이션할 수 있으며 VM은 해당 데이터 저장소에서 생성된 모든 가상 디스크에 대한 액세스를 계속 유지할 수 있습니다.

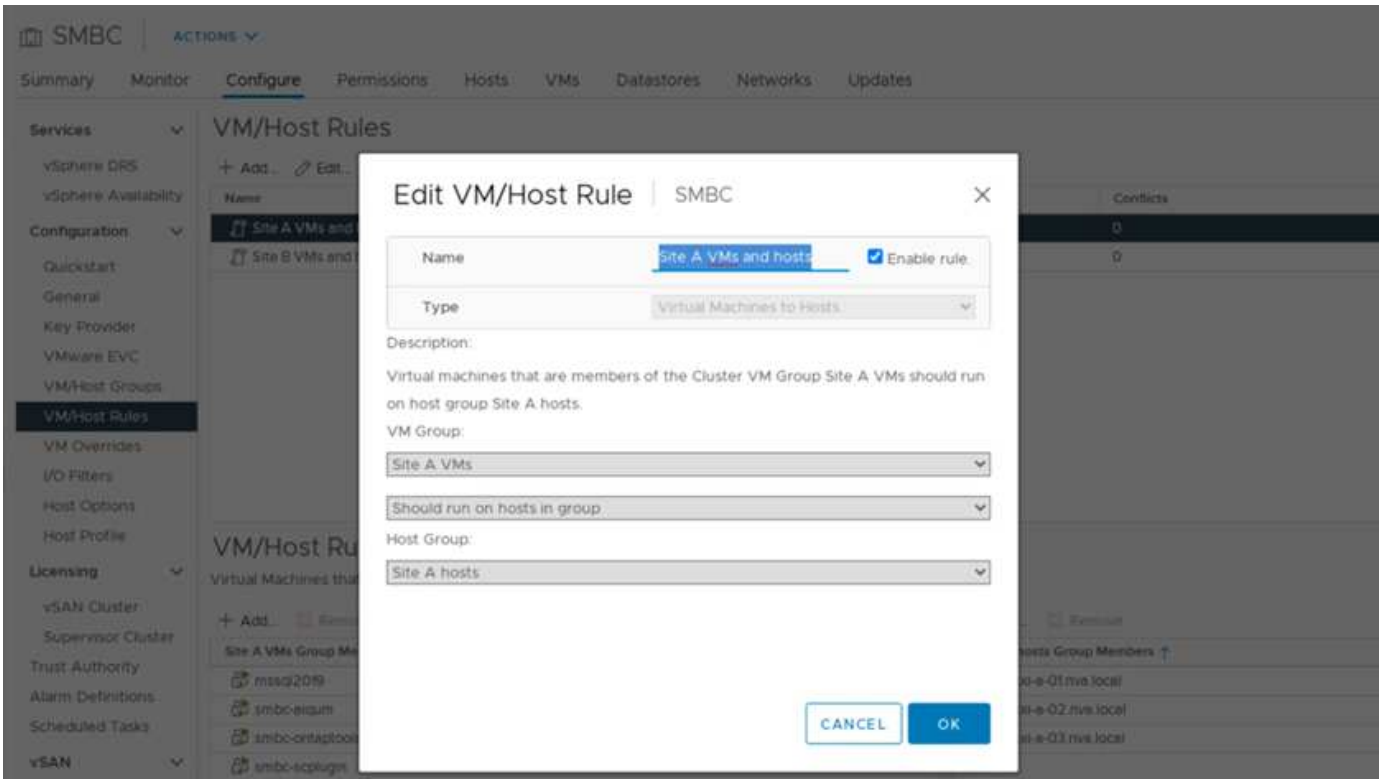
로컬 데이터 저장소를 사용하는 가상 머신의 경우 가상 디스크가 원격 사이트의 호스트로 마이그레이션되면 가상 디스크에 대한 액세스가 원격으로 되어 사이트 간의 물리적 거리로 인해 읽기 작업 지연 시간이 늘어납니다. 따라서 로컬 호스트에 가상 시스템을 유지하고 사이트의 로컬 스토리지를 활용하는 것이 좋습니다.

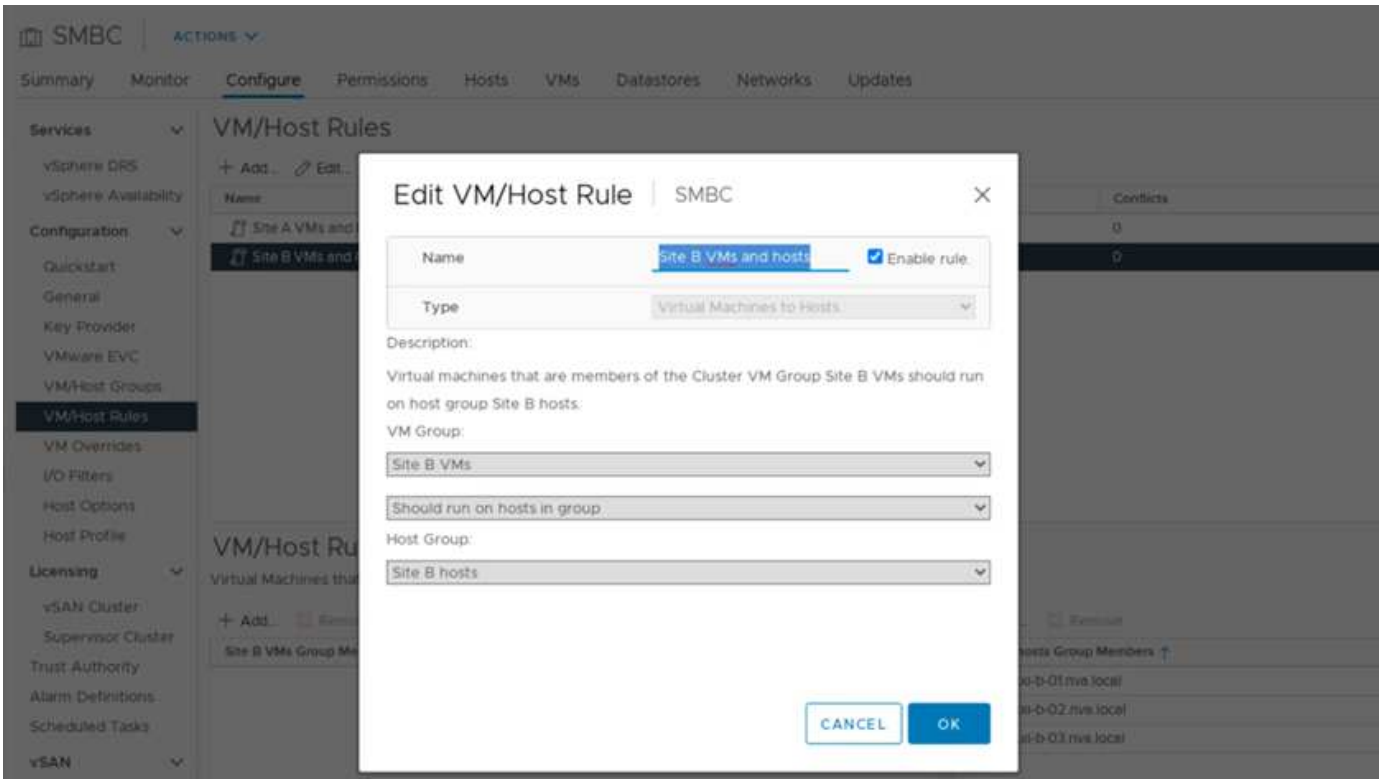
VM/호스트 선호도 메커니즘을 사용하여 VM/호스트 그룹을 사용하여 특정 사이트에 있는 가상 머신 및 호스트에 대한 VM 그룹 및 호스트 그룹을 생성할 수 있습니다. VM/호스트 규칙을 사용하여 따를 VM 및 호스트에 대한 정책을 지정할 수 있습니다. 사이트 유지 관리 또는 재해 시나리오 중에 사이트 간에 가상 시스템 마이그레이션을 허용하려면 이러한 유연성을 위해 "그룹의 호스트에서 실행해야 함" 정책 사양을 사용합니다.

다음 스크린샷은 사이트 A와 사이트 B 호스트 및 VM에 대해 두 개의 호스트 그룹과 두 개의 VM 그룹이 생성되었음을 보여 줍니다



또한 다음 두 그림에서는 사이트 A 및 사이트 B VM이 "그룹의 호스트에서 실행해야 함" 정책을 사용하여 각 사이트의 호스트에서 실행될 수 있도록 만들어진 VM/호스트 규칙을 보여 줍니다.

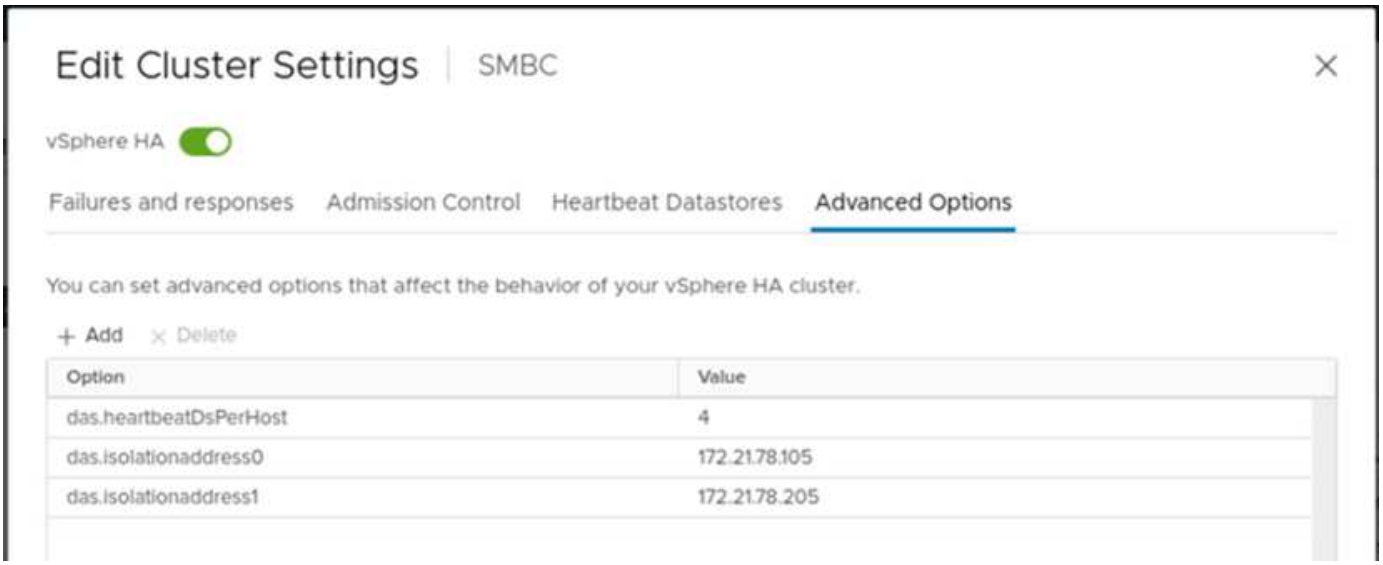




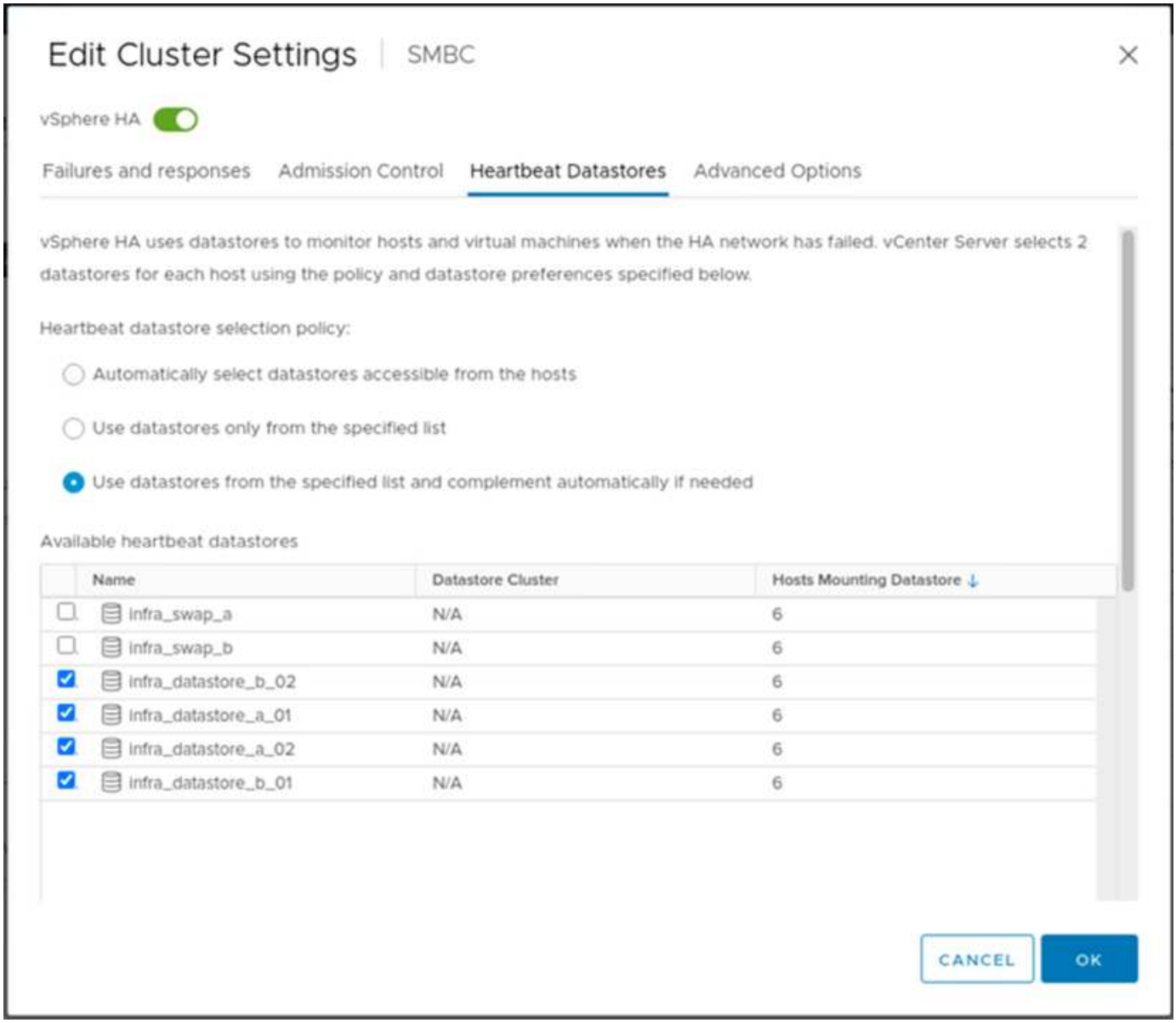
vSphere HA 하트비트입니다

VMware vSphere HA에는 호스트 상태 검증을 위한 하트비트 메커니즘이 있습니다. 기본 하트비트 메커니즘은 네트워킹을 통해, 보조 하트비트 메커니즘은 데이터 저장소를 통해 이루어집니다. 하트비트가 수신되지 않으면 기본 게이트웨이나 수동으로 구성된 격리 주소를 ping하여 하트비트가 네트워크에서 격리되는지 결정합니다. 데이터 저장소 하트비트의 경우 확대 클러스터에 대해 하트비트 데이터 저장소를 최소 2개에서 4개로 늘리는 것이 좋습니다.

솔루션 검증을 위해 두 개의 ONTAP 클러스터 관리 IP 주소가 격리 주소로 사용됩니다. 또한 다음 그림과 같이 값이 4인 권장 vSphere HA 고급 옵션 d.heartbeatDsPerHost가 추가되었습니다.



하트비트 데이터 저장소의 경우 다음 그림과 같이 클러스터에서 4개의 공유 데이터 저장소를 지정하고 자동으로 보완합니다.



VMware HA 클러스터 및 VMware vSphere Metro 스토리지 클러스터에 대한 추가 Best Practice와 구성은 를 참조하십시오 "vSphere HA 클러스터 생성 및 사용", "VMware vMSC(vSphere Metro Storage Cluster)" 및 에 대한 VMware KB를 참조하십시오 "NetApp ONTAP with NetApp SnapMirror 비즈니스 연속성(SM-BC) 및 VMware vSphere Metro Storage Cluster(vMSC)".

"다음으로 솔루션 검증 시나리오를 살펴보겠습니다."

솔루션 검증 시나리오

"이전: 솔루션 검증 - 가상화."

FlexPod Datacenter SM-BC 솔루션은 다양한 단일 장애 지점 시나리오와 사이트 재해에서 데이터 서비스를 보호합니다. 각 사이트에 구현된 이중화 설계는 고가용성을 제공하며, 사이트 간 동기식 데이터 복제를 통해 SM-BC를 구현하면 한 사이트의 사이트 전체에 걸친 재해 발생 시 데이터 서비스를 보호할 수 있습니다. 배포된 솔루션은 원하는 솔루션 기능 및 솔루션이 보호되도록 설계된 다양한 장애 시나리오에 대해 검증되었습니다.

솔루션 기능을 검증하고 부분 및 전체 사이트 장애 시나리오를 시뮬레이션하기 위해 다양한 테스트 사례가 사용됩니다. Cisco Validated Design Program의 기존 FlexPod 데이터 센터 솔루션에서 이미 수행된 테스트의 중복을 최소화하기 위해 이 보고서의 중점 내용은 솔루션의 SM-BC 관련 측면에 있습니다. 실무자가 구현 검증을 위해 거쳐야 하는 일반적인 FlexPod 유효성 검사가 몇 가지 포함되어 있습니다.

솔루션 검증을 위해 ESXi 호스트당 하나의 Windows 10 가상 머신이 두 사이트의 모든 ESXi 호스트에 생성되었습니다. IOMeter 도구가 설치되어 공유 로컬 iSCSI 데이터 저장소에서 매핑된 두 개의 가상 데이터 디스크에 대한 I/O를 생성하는 데 사용되었습니다. 구성된 IOMeter 워크로드 매개 변수는 8KB I/O, 75% 읽기 및 50% 랜덤으로 각 데이터 디스크에 대해 8개의 탁월한 I/O 명령을 구성했습니다. 수행되는 대부분의 테스트 시나리오에서 IOMeter I/O를 계속 수행하면 해당 시나리오에서 데이터 서비스 중단이 발생하지는 않았음을 알 수 있습니다.

SM-BC는 데이터베이스 서버와 같은 비즈니스 애플리케이션에 매우 중요하기 때문에 Windows Server 2022의 가상 머신에 있는 Microsoft SQL Server 2019 인스턴스는 로컬 사이트의 스토리지를 사용할 수 없고 애플리케이션 없이 원격 사이트 스토리지에서 데이터 서비스가 재개될 때 애플리케이션이 계속 실행되는지 확인하기 위한 테스트의 일부로 포함되어 있었습니다 운영 중단:

ESXi 호스트 **iSCSI SAN** 부팅 테스트입니다

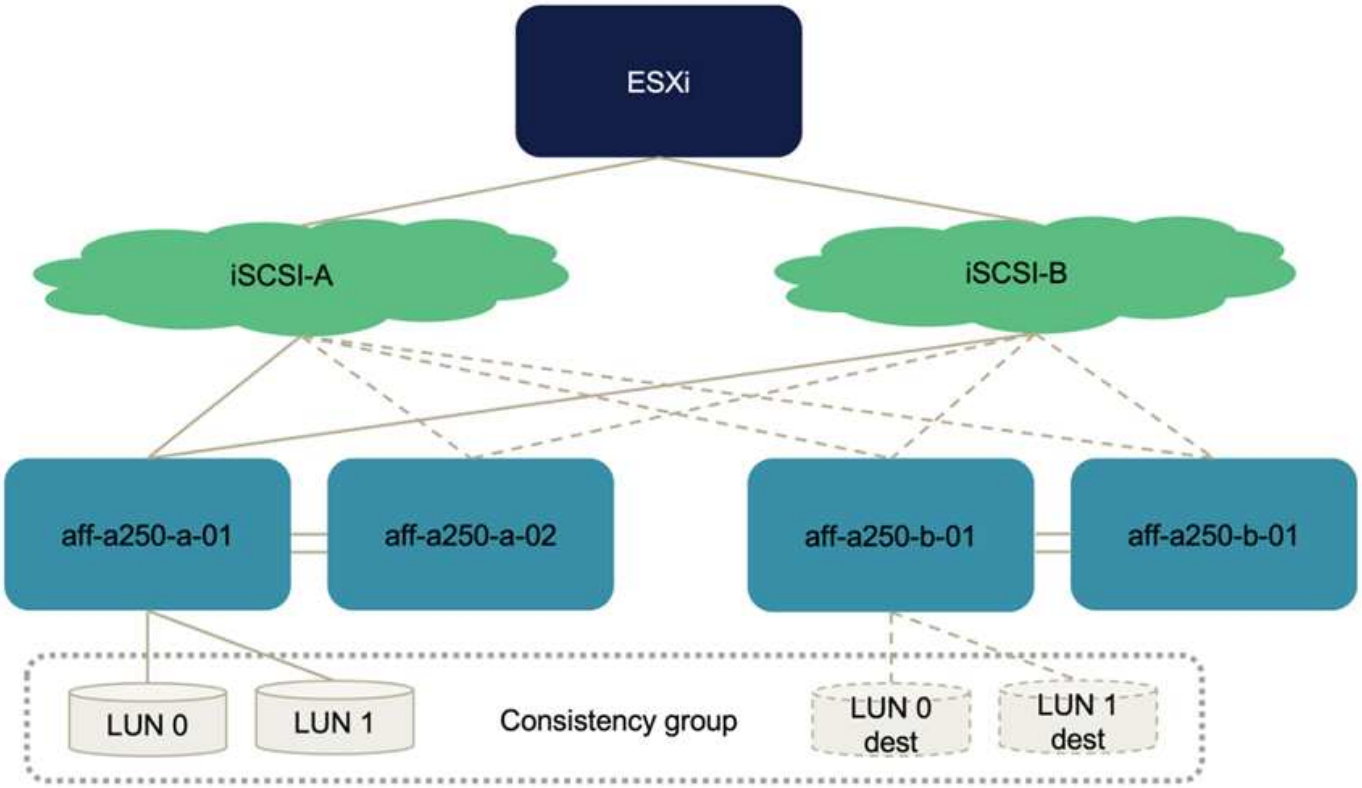
솔루션의 ESXi 호스트는 iSCSI SAN에서 부팅하도록 구성됩니다. SAN 부트를 사용하면 추가 구성 변경 없이 IT가 부팅할 수 있도록 서버의 서비스 프로필을 새 서버와 연결할 수 있으므로 서버 교체 시 서버 관리가 간소화됩니다.

로컬 iSCSI 부트 LUN에서 사이트에 있는 ESXi 호스트를 부팅하는 것 외에도 로컬 스토리지 컨트롤러가 Takeover 상태에 있거나 로컬 스토리지 클러스터를 완전히 사용할 수 없을 때 ESXi 호스트를 부팅하기 위해 테스트가 수행되었습니다. 이러한 검증 시나리오에서는 ESXi 호스트가 설계별로 올바르게 구성되어 있는지 확인하고 스토리지 유지 보수 또는 재해 복구 시나리오에서 부팅하여 비즈니스 연속성을 제공합니다.

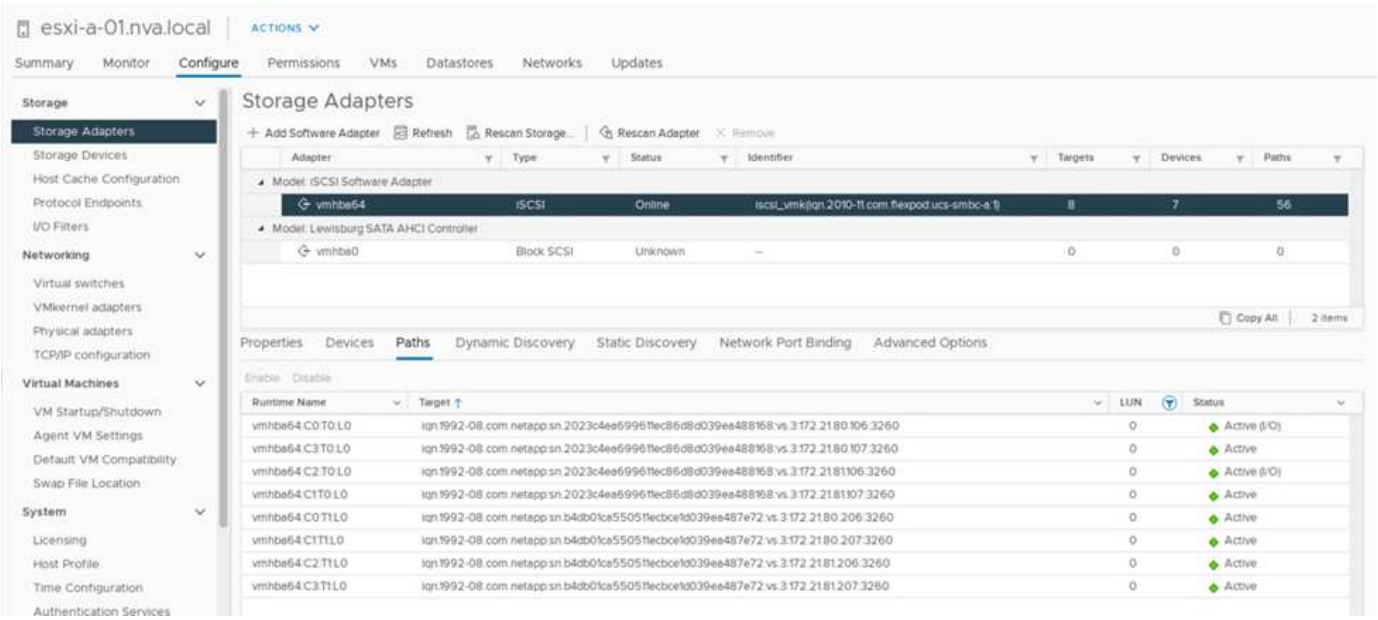
SM-BC 정합성 보장 그룹 관계가 구성되기 전에 스토리지 컨트롤러 HA 쌍에서 호스팅되는 iSCSI LUN의 경로가 4개(Best Practice 구현을 기반으로 각 iSCSI 패브릭을 통해 2개)입니다. 호스트는 2개의 iSCSI VLAN/패브릭을 통해 LUN 호스팅 컨트롤러에 연결할 수 있고 컨트롤러의 고가용성 파트너를 통해 LUN에 연결할 수 있습니다.

SM-BC 정합성 보장 그룹 관계가 구성되고 미러링된 LUN이 이니시에이터에 제대로 매핑되면 LUN의 경로 수가 두 배가 됩니다. 이 구축 환경에서는 2개의 활성/최적화 경로와 2개의 활성/최적화 경로를 갖는 것에서부터 2개의 활성/최적화 경로와 6개의 활성/비최적화 경로를 갖는 것까지 모두 포함됩니다.

다음 그림에서는 LUN 0과 같이 ESXi 호스트가 LUN을 액세스하는 데 사용할 수 있는 경로를 보여 줍니다. LUN이 사이트 A 컨트롤러 01에 연결되므로 해당 컨트롤러를 통해 LUN에 직접 액세스하는 2개의 경로만 액티브/최적화되고 나머지 6개 경로만 액티브/비최적화되어 있습니다.



다음 스토리지 디바이스 경로 정보 스크린샷은 ESXi 호스트에서 두 가지 유형의 디바이스 경로를 보는 방법을 보여 줍니다. 두 개의 Active/Optimized Path는 Active(I/O) Path 상태를 가지고 있는 것으로 표시되며, 6개의 Active/Non-Optimized Path는 Active로 표시됩니다. 또한 Target 열에는 두 개의 iSCSI 타겟과 타겟에 액세스할 수 있는 각 iSCSI LIF IP 주소가 표시됩니다.



스토리지 컨트롤러 중 하나가 유지보수 또는 업그레이드를 위해 중단되면 다운 컨트롤러에 연결되는 두 개의 경로를 더 이상 사용할 수 없으며 대신 경로 상태가 'dad'로 표시됩니다.

정합성 보장 그룹의 페일오버가 수동 페일오버 테스트 또는 자동 재해 페일오버로 인해 운영 스토리지 클러스터에서 발생하는 경우, 보조 스토리지 클러스터는 SM-BC 정합성 보장 그룹의 LUN에 대한 데이터 서비스를 계속 제공합니다. LUN ID는 보존되고 데이터는 동기식으로 복제되므로 SM-BC 정합성 보장 그룹에 의해 보호되는 모든 ESXi 호스트

부팅 LUN은 원격 스토리지 클러스터에서 계속 사용할 수 있습니다.

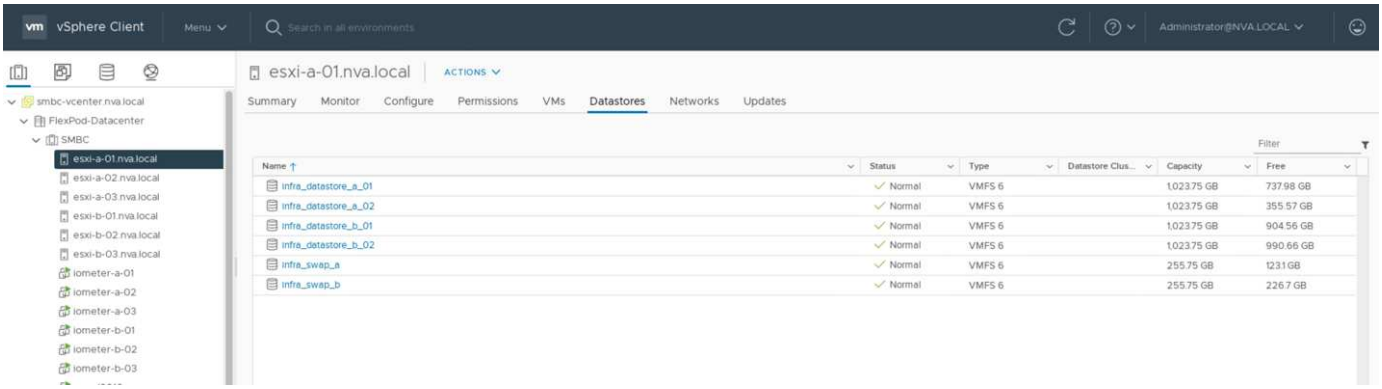
VMware vMotion 및 VM/호스트 선호도 테스트

일반 FlexPod VMware 데이터 센터 솔루션은 FC, iSCSI, NVMe 및 NFS와 같은 멀티 프로토콜을 지원하지만 FlexPod SM-BC 솔루션 기능은 일반적으로 비즈니스 크리티컬 솔루션에 사용되는 FC 및 iSCSI SAN 프로토콜을 지원합니다. 이 검증에서는 iSCSI 프로토콜 기반 데이터 저장소와 iSCSI SAN 부팅만 사용합니다.

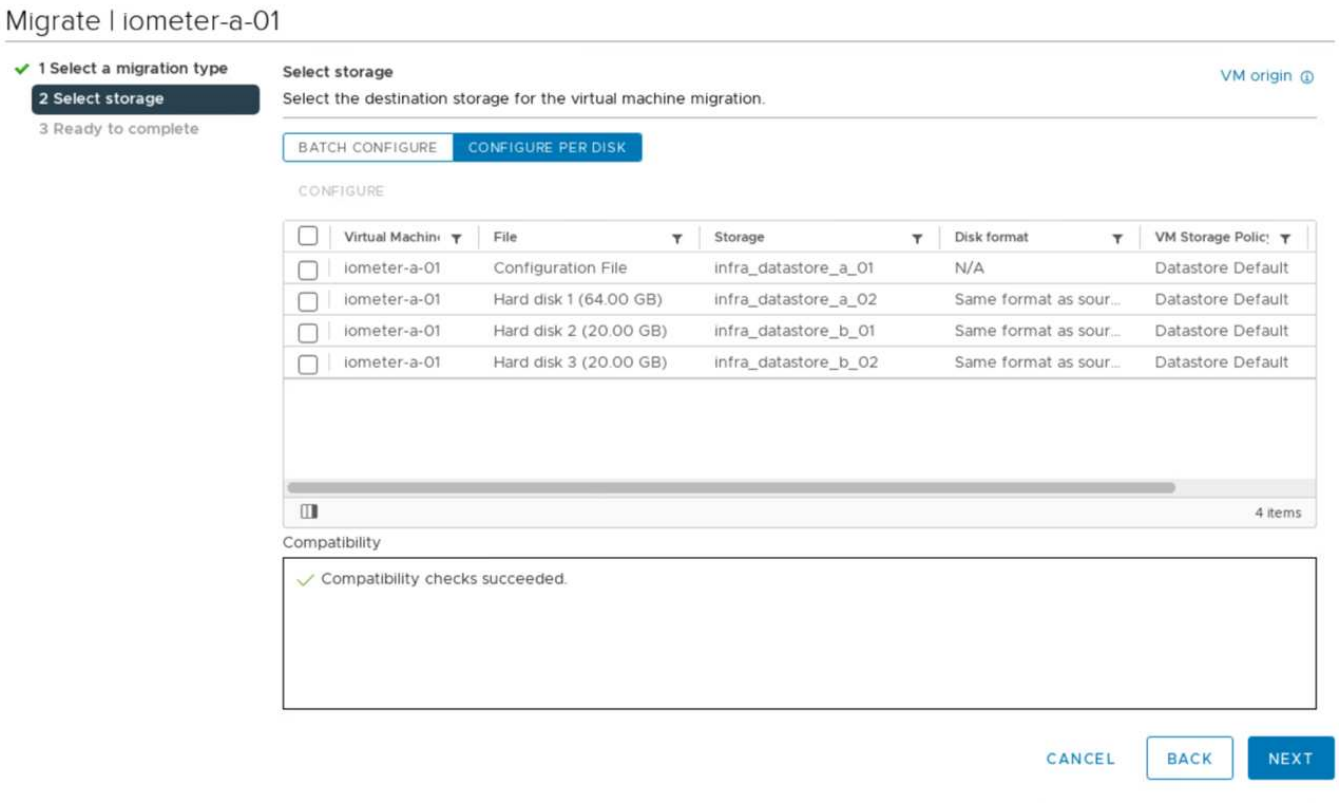
가상 머신이 SM-BC 사이트 중 하나에서 스토리지 서비스를 사용할 수 있도록 하려면 두 사이트의 iSCSI 데이터 저장소를 클러스터의 모든 호스트에서 마운트해야 두 사이트 간에 가상 머신을 마이그레이션할 수 있고 재해 페일오버 시나리오를 수행할 수 있습니다.

사이트 간 SM-BC 정합성 보장 그룹 보호가 필요하지 않은 가상 인프라에서 실행되는 애플리케이션의 경우 NFS 프로토콜 및 NFS 데이터 저장소도 사용할 수 있습니다. 이 경우 비즈니스 크리티컬 애플리케이션이 SM-BC 정합성 보장 그룹에 의해 보호되는 SAN 데이터 저장소를 제대로 사용하여 비즈니스 연속성을 제공하도록 VM용 스토리지를 할당할 때는 주의해야 합니다.

다음 스크린샷은 호스트가 두 사이트에서 iSCSI 데이터 저장소를 마운트하도록 구성되어 있음을 보여 줍니다.



다음 그림과 같이 두 사이트에서 사용 가능한 iSCSI 데이터 저장소 간에 가상 시스템 디스크를 마이그레이션할 수 있습니다. 성능을 고려하려면 로컬 스토리지 클러스터의 스토리지를 사용하여 가상 시스템에 대해 디스크 I/O 지연 시간을 줄이는 것이 좋습니다. 특히 100km 거리당 약 1ms의 물리적 왕복 거리 지연 시간 때문에 두 사이트가 서로 떨어져 있는 경우 더욱 그렇습니다.



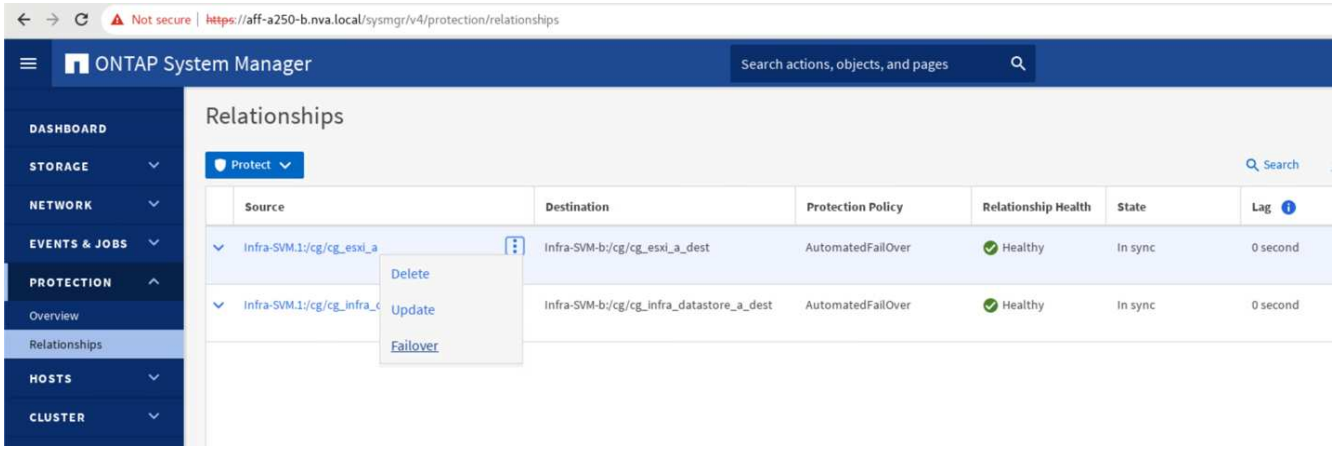
사이트 간 및 동일한 사이트의 다른 호스트에 대한 가상 머신의 vMotion 테스트가 수행되어 성공했습니다. 사이트 간에 가상 머신을 수동으로 마이그레이션한 후에는 VM/호스트 선호도 규칙이 가상 머신을 정상 조건 하에 있는 그룹으로 활성화하고 다시 마이그레이션합니다.

계획된 스토리지 페일오버

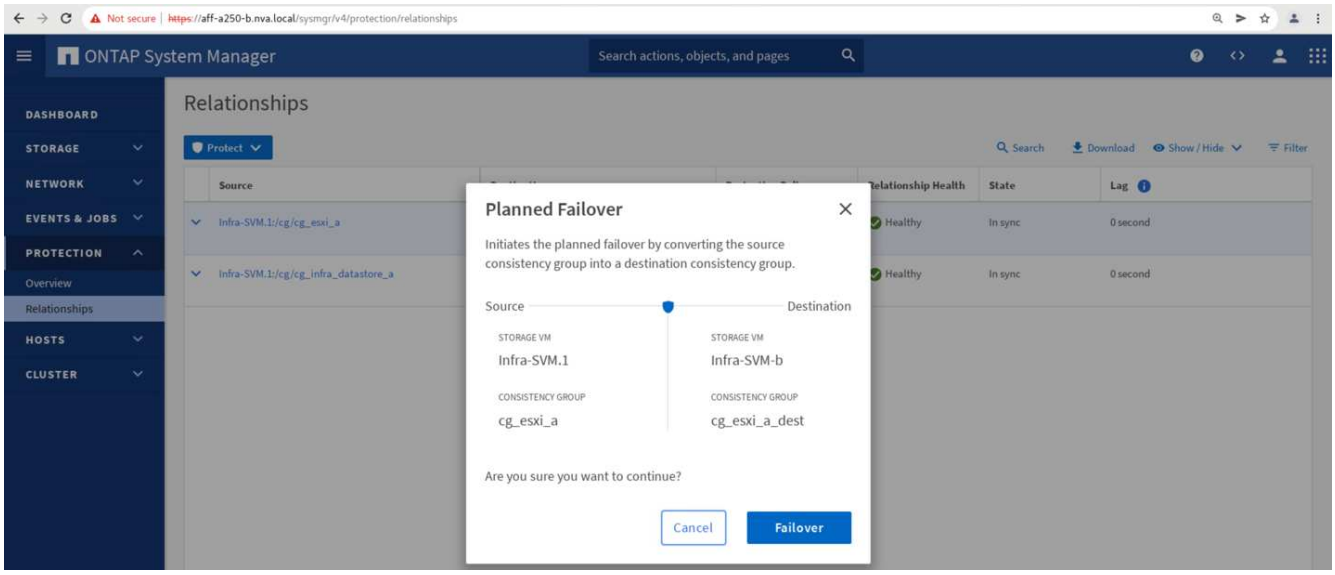
스토리지 페일오버 후 솔루션이 제대로 작동하는지 확인하려면 초기 구성 후 솔루션에 대해 계획된 스토리지 페일오버 작업을 수행해야 합니다. 이 테스트는 I/O 중단을 일으킬 수 있는 연결 또는 구성 문제를 식별하는 데 도움이 될 수 있습니다. 연결 또는 구성 문제를 정기적으로 테스트하고 해결하면 실제 사이트 재해가 발생할 때 중단 없는 데이터 서비스를 제공하는 데 도움이 됩니다. 계획된 스토리지 페일오버는 예약된 스토리지 유지보수 작업 전에 사용할 수 있으므로 영향을 받지 않는 사이트에서 데이터 서비스를 제공할 수 있습니다.

사이트 A 스토리지 데이터 서비스의 수동 페일오버를 사이트 B에 시작하려면 사이트 B ONTAP 시스템 관리자를 사용하여 작업을 수행할 수 있습니다.

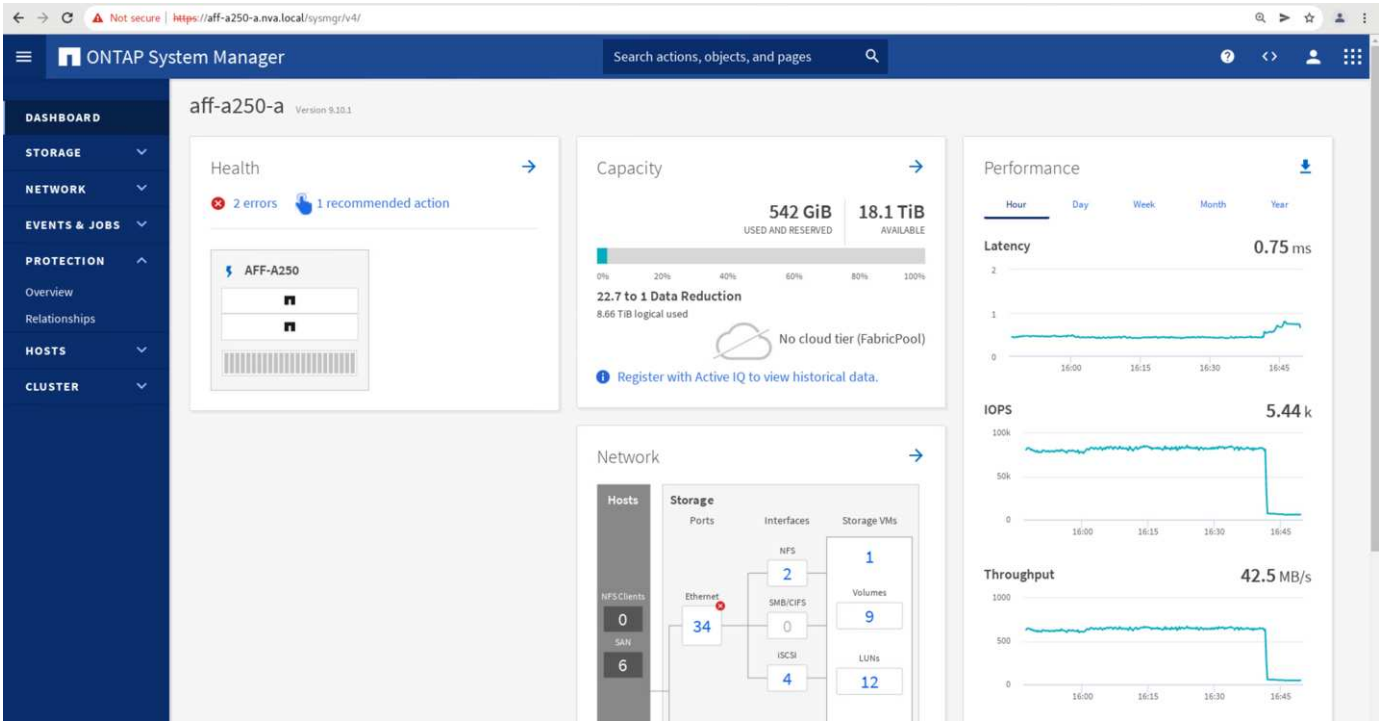
1. 보호 > 관계 화면으로 이동하여 정합성 보장 그룹 관계 상태가 '동기화 중'인지 확인합니다. 아직 동기화 중인 상태라면 장애 조치를 수행하기 전에 동기화 중 상태가 될 때까지 기다립니다.
2. 소스 이름 옆의 점을 확장하고 장애 조치를 클릭합니다.



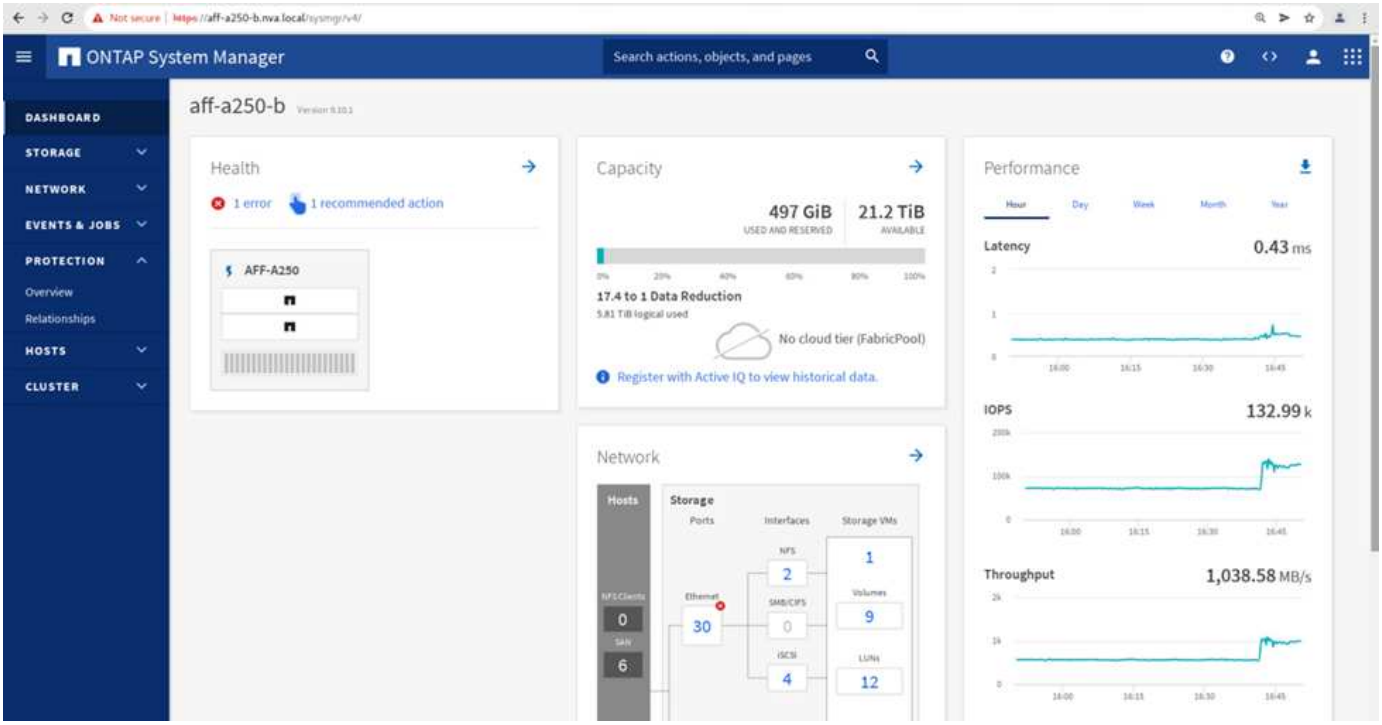
3. 작업을 시작할 대체 작동을 확인합니다.



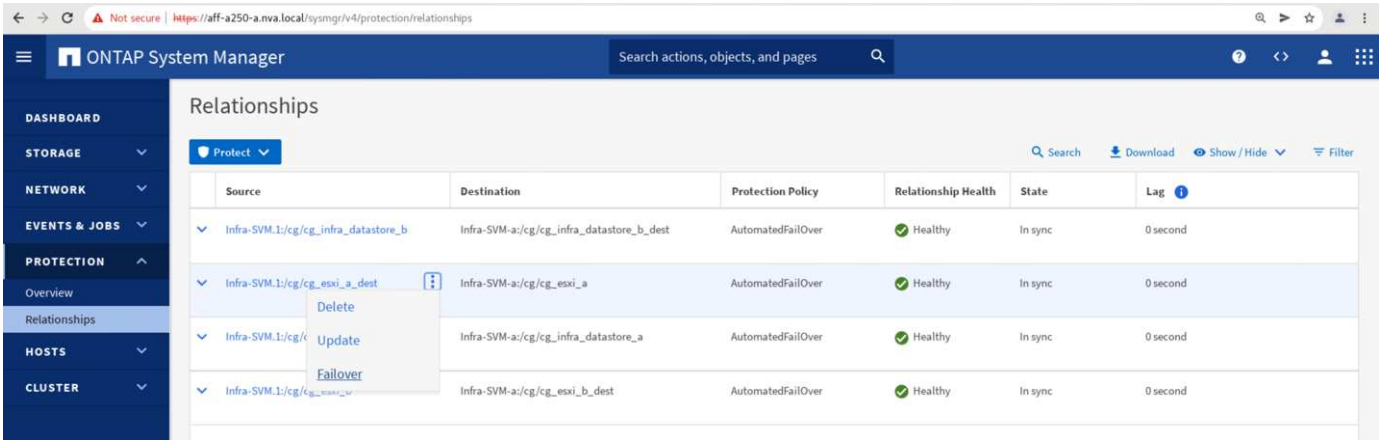
사이트 B System Manager GUI에서 두 정합성 보장 그룹 CG_ESXi_A와 CG_infra_datastore_A의 페일오버를 시작한 직후 사이트 A에서 두 정합성 보장 그룹을 사이트 B로 이동했습니다 그 결과, 사이트의 I/O가 System Manager 성능 창에 표시된 것처럼 크게 감소했습니다.



반면, 사이트 B System Manager 대시보드의 성능 창에는 사이트 A에서 약 130K IOP로 이동하는 추가 I/O 덕분에 IOP가 크게 증가한 것으로 표시됩니다. 약 1GB/s의 처리량과 1밀리초 미만의 I/O 지연 시간을 유지했습니다.

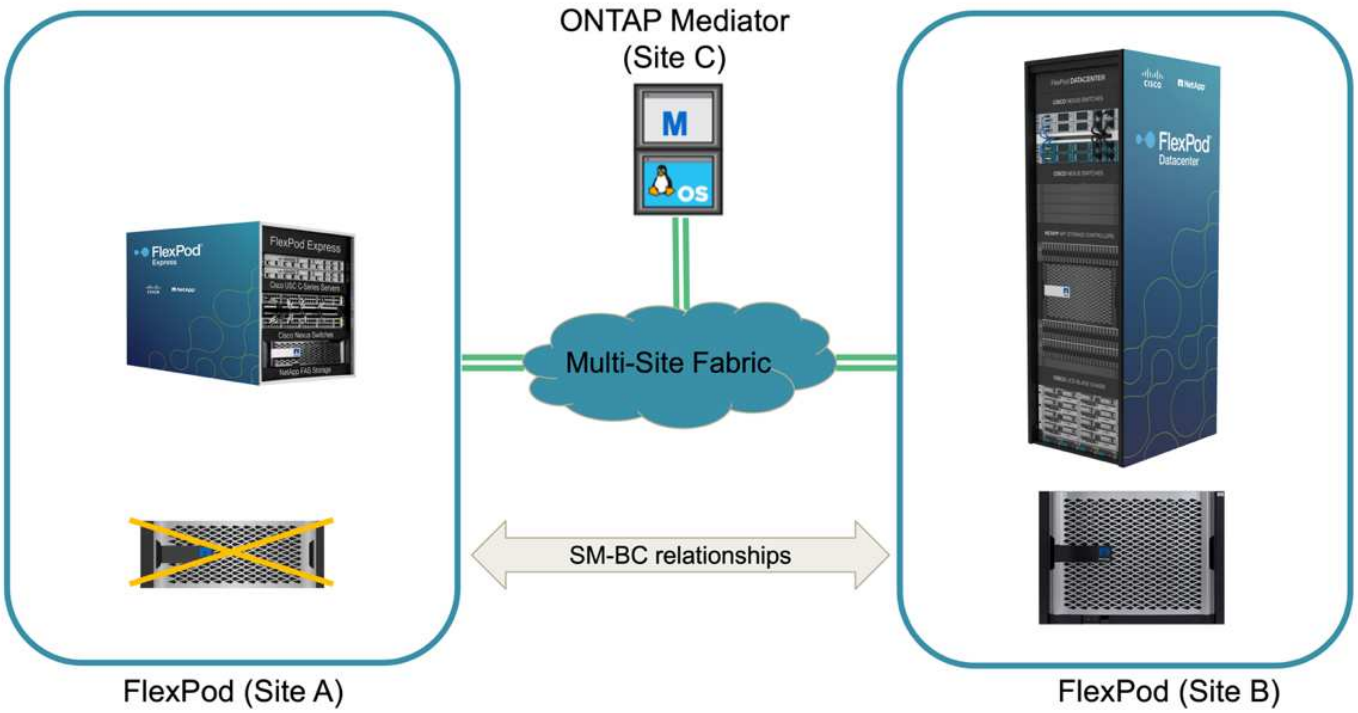


I/O가 사이트 A에서 사이트 B로 투명하게 마이그레이션되면 예약된 유지 관리를 위해 사이트 A 스토리지 컨트롤러를 가져올 수 있습니다. 유지 관리 작업 또는 테스트가 완료되고 사이트 A 스토리지 클러스터가 백업 및 작동 가능으로 전환된 후 장애 조치를 수행하기 전에 정합성 보장 그룹 보호 상태가 다시 "동기화 중"으로 바뀔 때까지 기다린 후 사이트 B의 페일오버 입출력을 사이트 A로 되돌립니다 유지 관리 또는 테스트를 위해 사이트가 다운되는 시간이 길어질수록 데이터가 동기화되고 정합성 보장 그룹이 '동기화 중' 상태로 되돌아가는 데 시간이 더 오래 걸립니다.



계획되지 않은 스토리지 페일오버

계획되지 않은 스토리지 페일오버는 실제 재해가 발생하거나 재해 시뮬레이션 중에 발생할 수 있습니다. 예를 들어 사이트 A의 스토리지 시스템에서 정전이 발생하거나, 계획되지 않은 스토리지 페일오버가 트리거되고, 사이트 A LUN에 대한 데이터 서비스가 SM-BC 관계에 의해 보호되면 사이트 B에서 계속 이어지는 그림을 참조하십시오

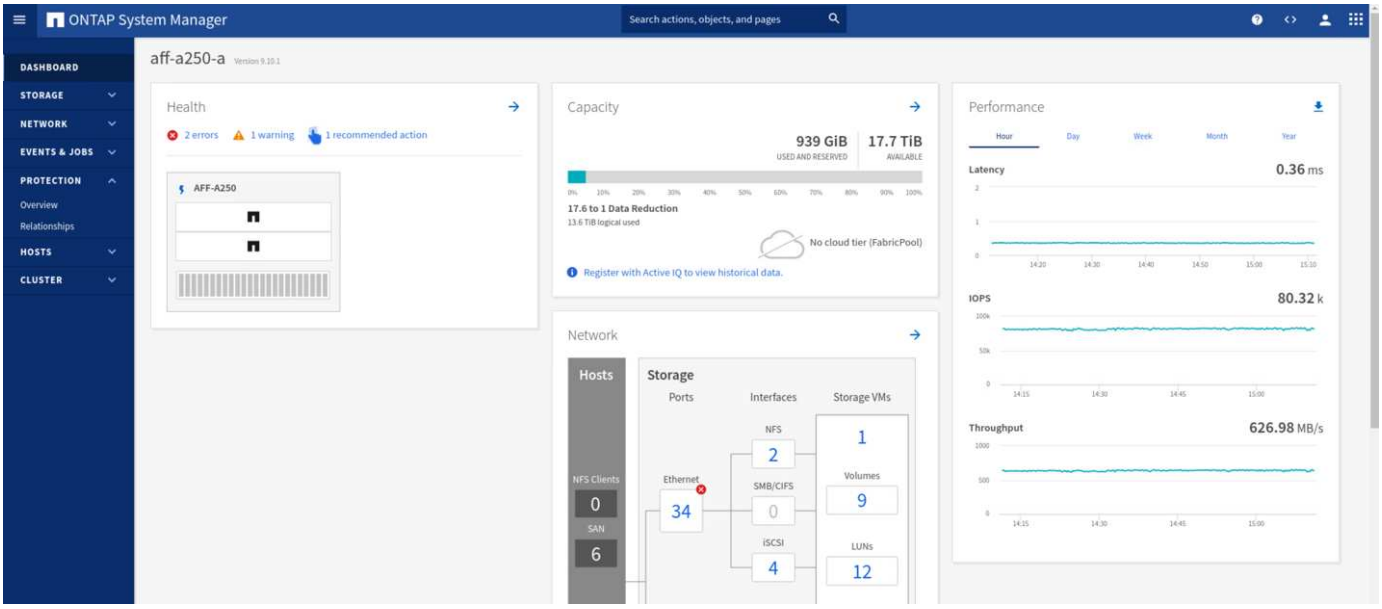


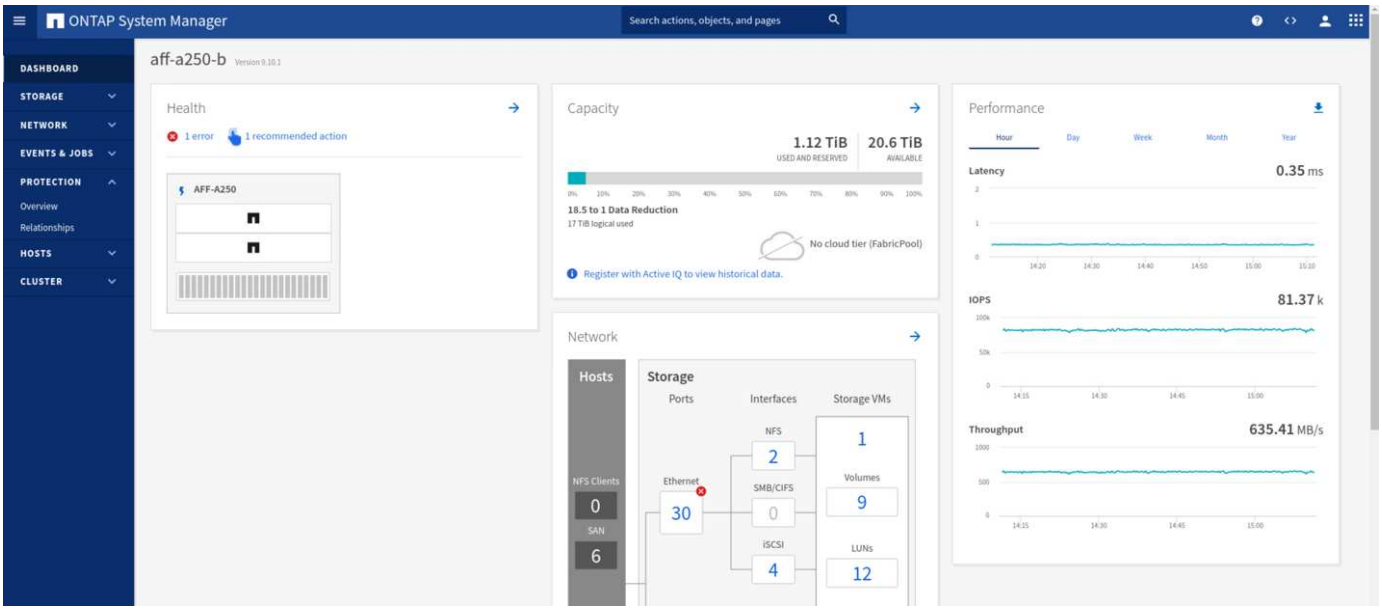
사이트 A에서 스토리지 재해를 시뮬레이션하기 위해 전원 스위치를 물리적으로 끄고 컨트롤러에 대한 전원 공급을 중단하면 사이트 A의 두 스토리지 컨트롤러의 전원을 끌 수 있습니다. 또는 스토리지 컨트롤러 서비스 프로세서의 시스템 전원 관리 명령을 사용하여 컨트롤러의 전원을 끕니다.

사이트의 스토리지 클러스터에 손실이 발생할 경우 사이트 A 스토리지 클러스터에서 데이터 서비스가 갑자기 중지됩니다. 그런 다음, 세 번째 사이트에서 SM-BC 솔루션을 모니터링하는 ONTAP 중재자가 사이트의 스토리지 장애 상태를 감지하고 SM-BC 솔루션에서 자동화된 계획되지 않은 페일오버를 수행할 수 있도록 합니다. 이를 통해 사이트 B 스토리지 컨트롤러는 사이트 A와의 SM-BC 정합성 보장 그룹 관계에 구성된 LUN에 대해 데이터 서비스를 계속할 수 있습니다

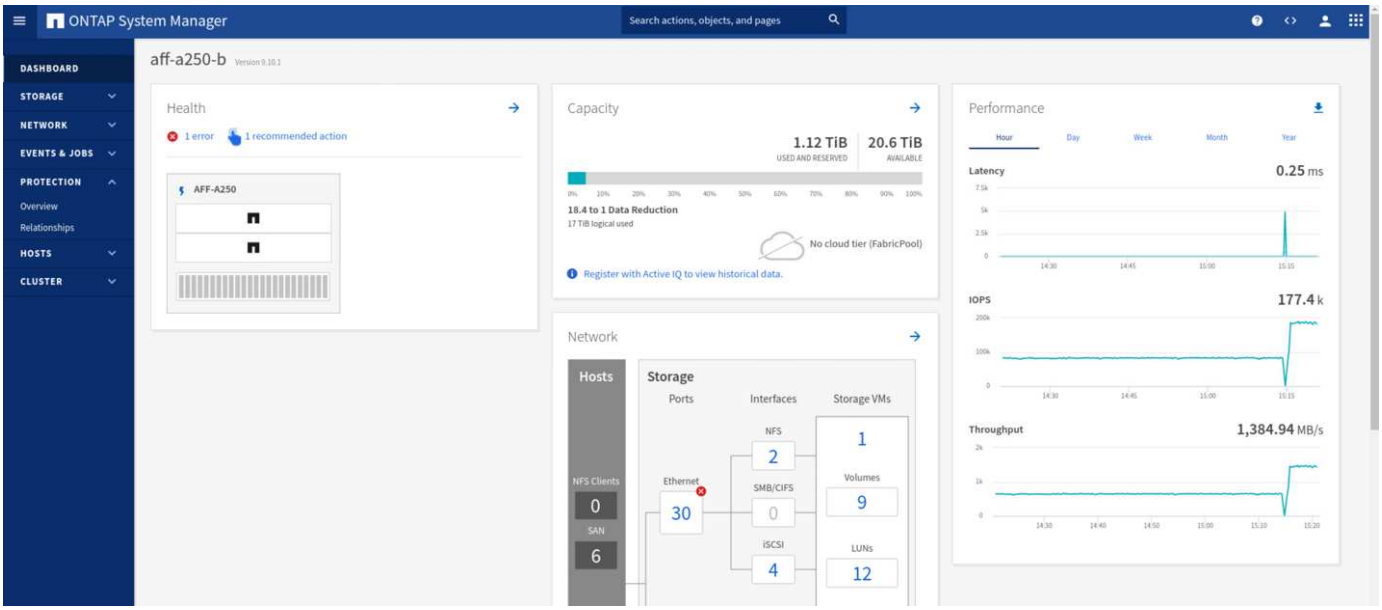
애플리케이션 측면에서 운영 체제가 LUN의 경로 상태를 확인한 후 남아 있는 사이트 B 스토리지 컨트롤러에 대한 사용 가능한 경로에서 입출력을 재개하는 동안 데이터 서비스가 잠시 일시 중지됩니다.

검증 테스트 중에 두 사이트의 VM에 있는 IOMeter 툴은 로컬 데이터 저장소에 대한 입출력을 생성합니다. 사이트 A 클러스터의 전원이 꺼진 후 입출력이 잠시 일시 중지되었다가 나중에 다시 시작됩니다. 각 사이트에서 약 80k IOPS와 600MB/s 처리량을 보여 주는 재해 전에 사이트 A와 사이트 B의 스토리지 클러스터 대시보드에 대한 다음 두 그림을 참조하십시오.

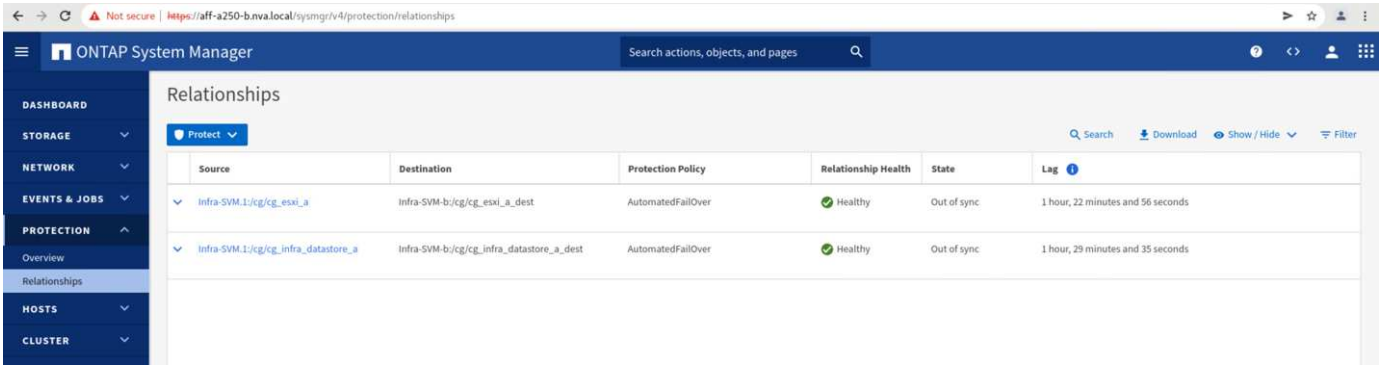




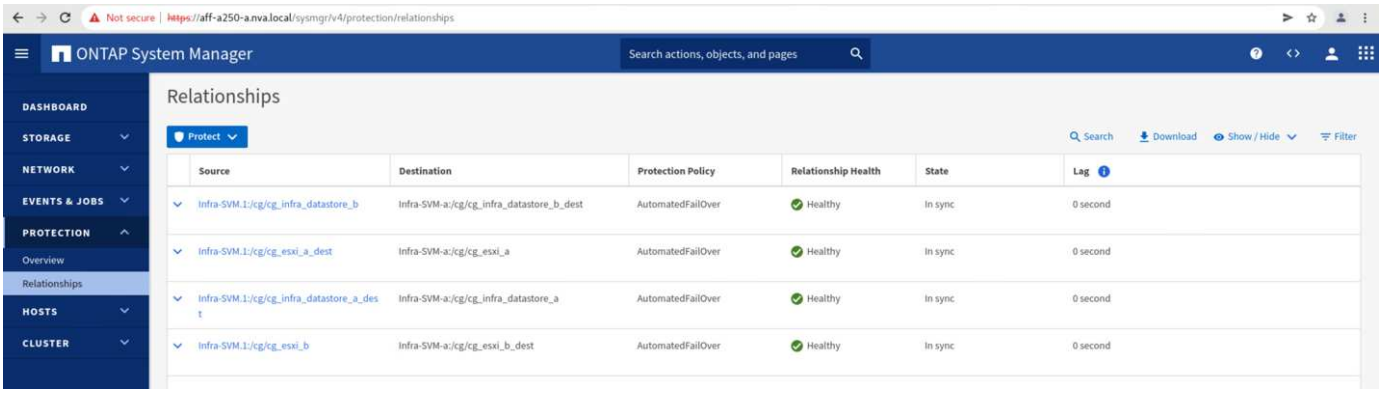
사이트 A에서 스토리지 컨트롤러의 전원을 끈 후 사이트 B 스토리지 컨트롤러 I/O가 급격히 증가하여 사이트 A를 대신하여 추가 데이터 서비스를 제공하는지를 육안으로 확인할 수 있습니다(다음 그림 참조). 또한 IOMeter VM의 GUI는 사이트 A 스토리지 클러스터 중단에도 불구하고 I/O가 계속 유지된다는 것을 보여 주었습니다. SM-BC 관계에 의해 보호되지 않는 LUN에서 백업한 추가 데이터 저장소가 있는 경우 스토리지 재해가 발생할 때 해당 데이터 저장소에 더 이상 액세스할 수 없습니다. 따라서 다양한 애플리케이션 데이터의 비즈니스 요구 사항을 평가하고 비즈니스 연속성을 제공하기 위해 이를 SM-BC 관계에 의해 보호되는 데이터 저장소에 적절히 배치하는 것이 중요합니다.



사이트 A 클러스터가 다운된 상태에서 정합성 보장 그룹의 관계는 다음 그림과 같이 동기화 중단 상태로 표시됩니다. 사이트 A의 스토리지 컨트롤러에 대한 전원을 다시 켜면 스토리지 클러스터가 부팅되고 사이트 A와 사이트 B 간의 데이터 동기화가 자동으로 수행됩니다.



사이트 B의 데이터 서비스를 사이트 A로 다시 반환하기 전에 사이트 A System Manager를 확인하고 SM-BC 관계가 제대로 인식되었는지, 그리고 상태가 다시 동기화되었는지 확인해야 합니다. 정합성 보장 그룹이 동기화 중임을 확인한 후 수동 페일오버 작업을 시작하여 정합성 보장 그룹 관계의 데이터 서비스를 사이트 A로 다시 반환할 수 있습니다



사이트 유지 관리 또는 사이트 장애 완료

현장에 현장 유지 보수, 전력 손실 또는 허리케인이나 지진과 같은 자연 재해로 인한 영향이 있을 수 있습니다. 따라서 FlexPod SM-BC 솔루션이 모든 비즈니스 크리티컬 애플리케이션 및 데이터 서비스에 대해 이러한 장애를 극복할 수

있도록 적절히 구성되도록 계획되었거나 계획되지 않은 사이트 장애 시나리오를 실행하는 것이 중요합니다. 다음 사이트 관련 시나리오가 검증되었습니다.

- 가상 시스템 및 중요 데이터 서비스를 다른 사이트로 마이그레이션하여 사이트 유지 관리 시나리오를 계획했습니다
- 재해 시뮬레이션을 위해 서버 및 스토리지 컨트롤러의 전원을 꺼서 계획되지 않은 사이트 중단 시나리오

계획된 사이트 유지 관리를 위해 사이트를 준비하려면 영향을 받는 가상 시스템을 vMotion과 함께 사이트 외부로 마이그레이션하고, 가상 머신 및 중요 데이터 서비스를 대체 사이트로 마이그레이션하려면 SM-BC 정합성 보장 그룹 관계의 수동 페일오버가 필요합니다. 테스트는 두 가지 다른 순서로 수행되었습니다. 먼저 vMotion을 실행한 후 SM-BC 페일오버 및 SM-BC 페일오버 후에 vMotion을 먼저 실행하여 가상 머신이 계속 실행되고 데이터 서비스가 중단되지 않는지 확인했습니다.

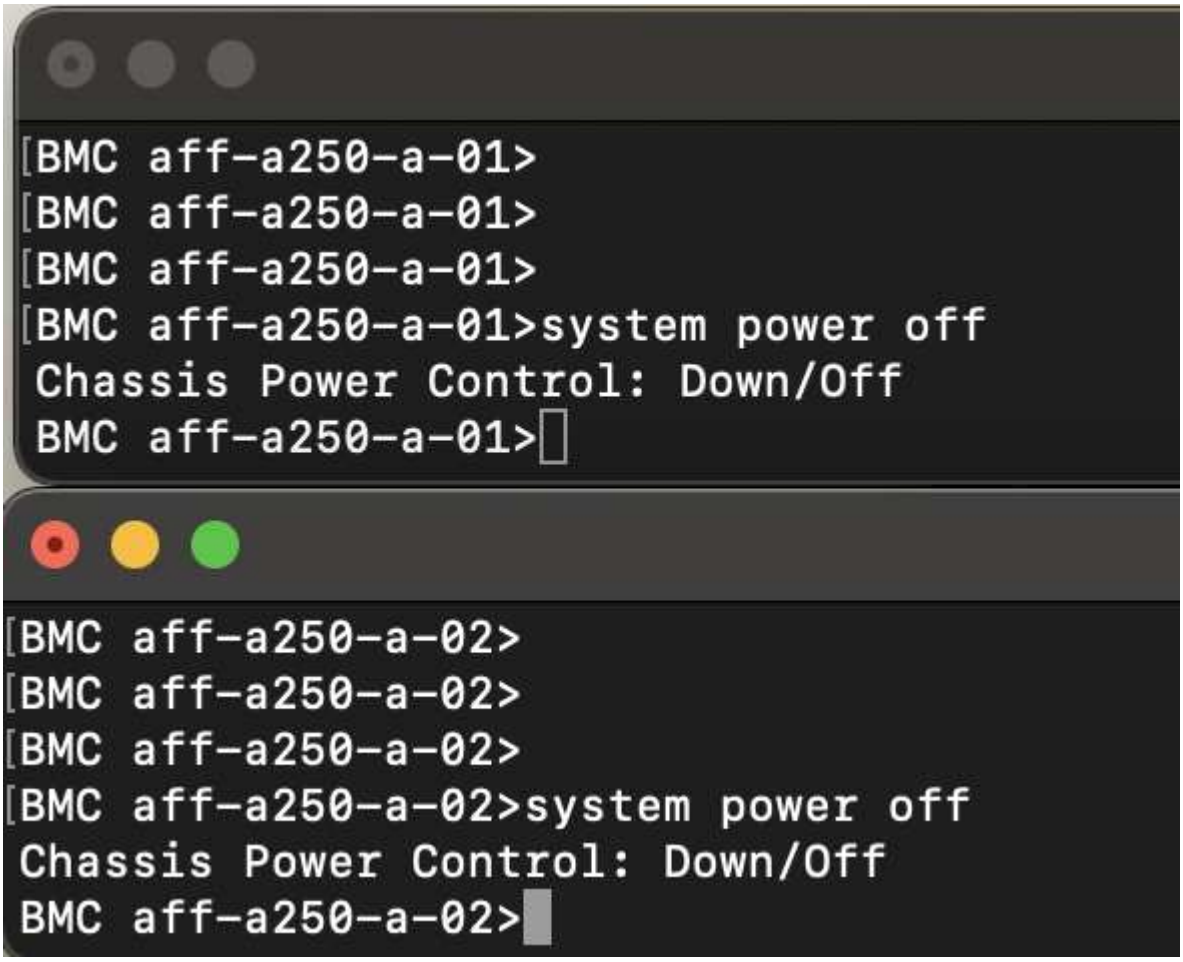
계획된 마이그레이션을 수행하기 전에 VM/호스트 선호도 규칙을 업데이트하여 현재 사이트에서 실행 중인 VM이 유지 보수 중인 사이트에서 자동으로 마이그레이션되도록 합니다. 다음 스크린샷은 사이트 A에서 사이트 B로 자동으로 마이그레이션할 VM에 대한 사이트 A VM/호스트 선호도 규칙을 수정하는 예를 보여 줍니다. 이제 사이트 B에서 VM을 실행해야 하는 대신 VM을 수동으로 마이그레이션할 수 있도록 선호도 규칙을 일시적으로 비활성화할 수도 있습니다.



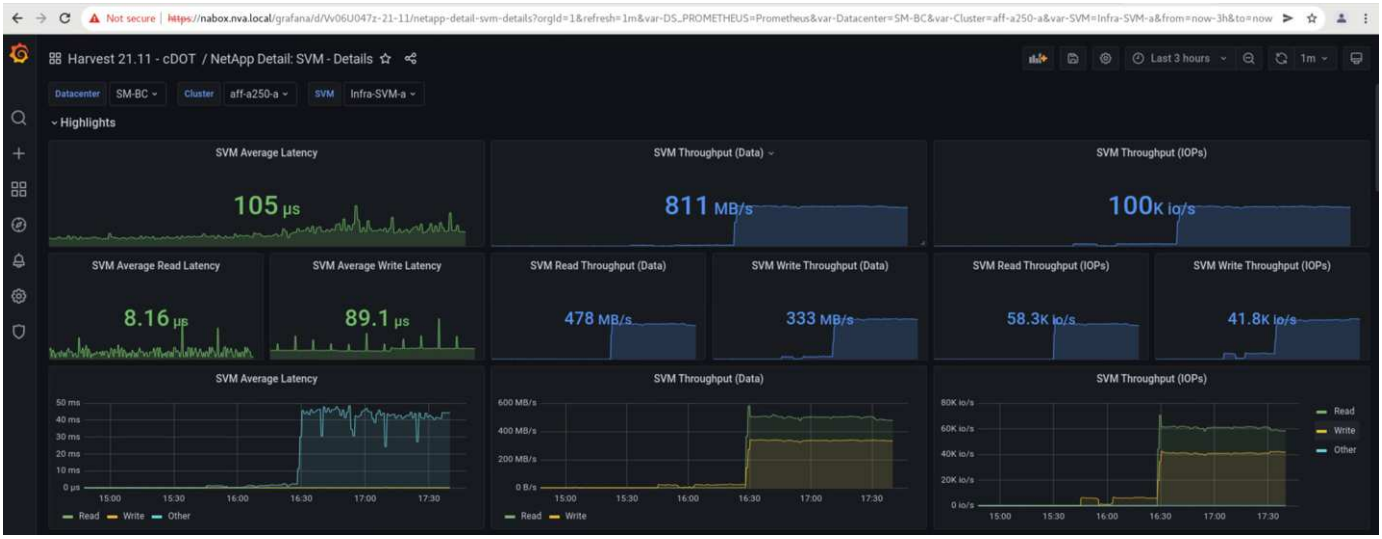
가상 머신 및 스토리지 서비스를 마이그레이션한 후에는 서버, 스토리지 컨트롤러, 디스크 쉘프 및 스위치의 전원을 끄고 필요한 사이트 유지 관리 작업을 수행할 수 있습니다. 사이트 유지 관리가 완료되고 FlexPod 인스턴스가 백업되면 VM에 대한 호스트 그룹 선호도를 변경하여 원래 사이트로 돌아갈 수 있습니다. 그런 다음 "그룹의 호스트에서 실행해야 함" VM/호스트 사이트 선호도 규칙을 다시 "그룹의 호스트에서 실행해야 함"으로 변경하여 재해가 발생할 경우 다른 사이트의 호스트에서 가상 시스템을 실행할 수 있도록 해야 합니다. 검증 테스트를 위해 모든 가상 시스템이 다른 사이트로 성공적으로 마이그레이션되었으며, SM-BC 관계에 대한 페일오버를 수행한 후에도 데이터 서비스가 문제 없이 계속됩니다.

계획되지 않은 사이트 재해 시뮬레이션의 경우 서버 및 스토리지 컨트롤러의 전원을 꺼서 사이트 재해를 시뮬레이션했습니다. VMware HA 기능은 다운된 가상 시스템을 감지하고 정상 작동하는 사이트에서 해당 가상 시스템을 다시 시작합니다. 또한 세 번째 사이트에서 실행 중인 ONTAP 중재자가 사이트 장애를 감지하고 정상 작동하는 사이트가 페일오버를 시작하고 필요에 따라 중단 사이트에 데이터 서비스를 제공하기 시작합니다.

다음 스크린샷은 사이트의 스토리지 재해 시뮬레이션을 위해 스토리지 컨트롤러의 서비스 프로세서 CLI를 사용하여 사이트의 전원을 갑자기 끄는 것을 보여 줍니다.



NetApp Harvest 데이터 수집 툴에서 캡처되고 NAbox 모니터링 도구의 Grafana 대시보드에 표시되는 스토리지 클러스터의 스토리지 가상 머신 대시보드는 다음 두 개의 스크린샷에 나와 있습니다. IOPS 및 처리량 그래프의 오른쪽에서 볼 수 있듯이, 사이트 B 클러스터는 사이트 A 클러스터가 다운된 직후 클러스터 A 스토리지 워크로드를 선택합니다.



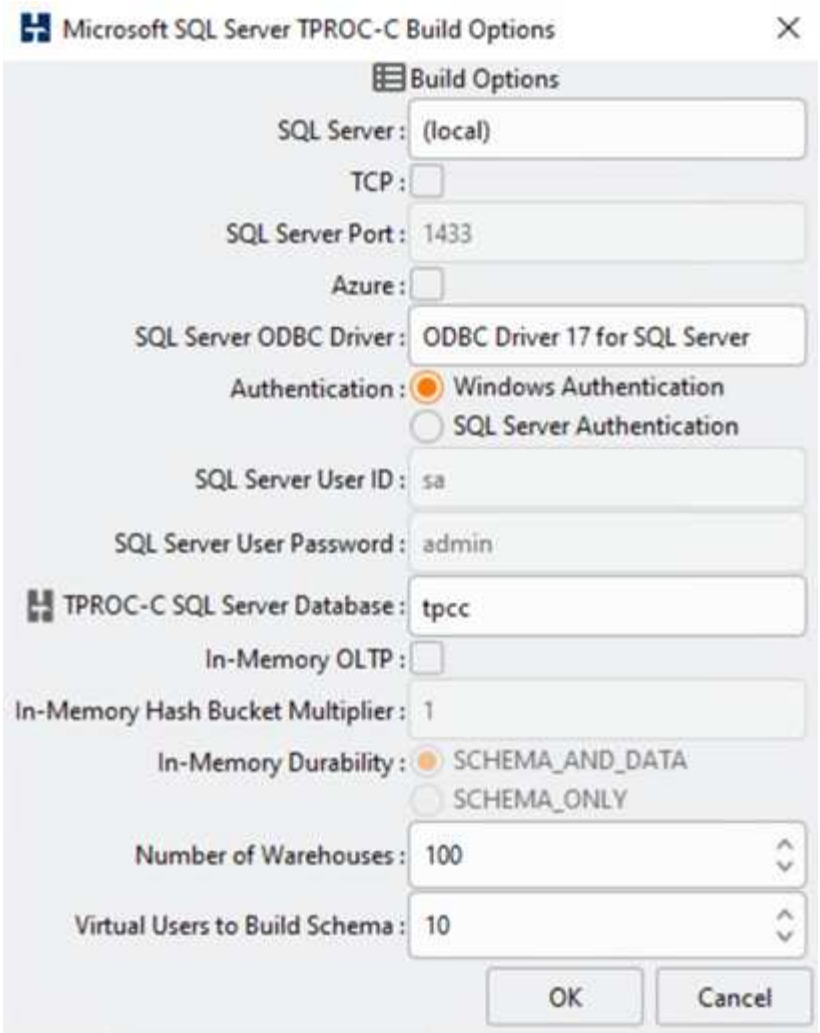


Microsoft SQL Server를 참조하십시오

Microsoft SQL Server는 엔터프라이즈 IT를 위해 널리 채택되고 배포된 데이터베이스 플랫폼입니다. Microsoft SQL Server 2019 릴리스는 관계형 및 분석 엔진에 많은 새로운 기능과 향상된 기능을 제공합니다. 이 솔루션은 사내, 클라우드에서 실행되는 애플리케이션과 하이브리드 퍼블릭 클라우드 모두에서 2가지 워크로드를 지원합니다. 또한 Windows, Linux 및 컨테이너를 포함한 여러 플랫폼에 배포할 수 있습니다.

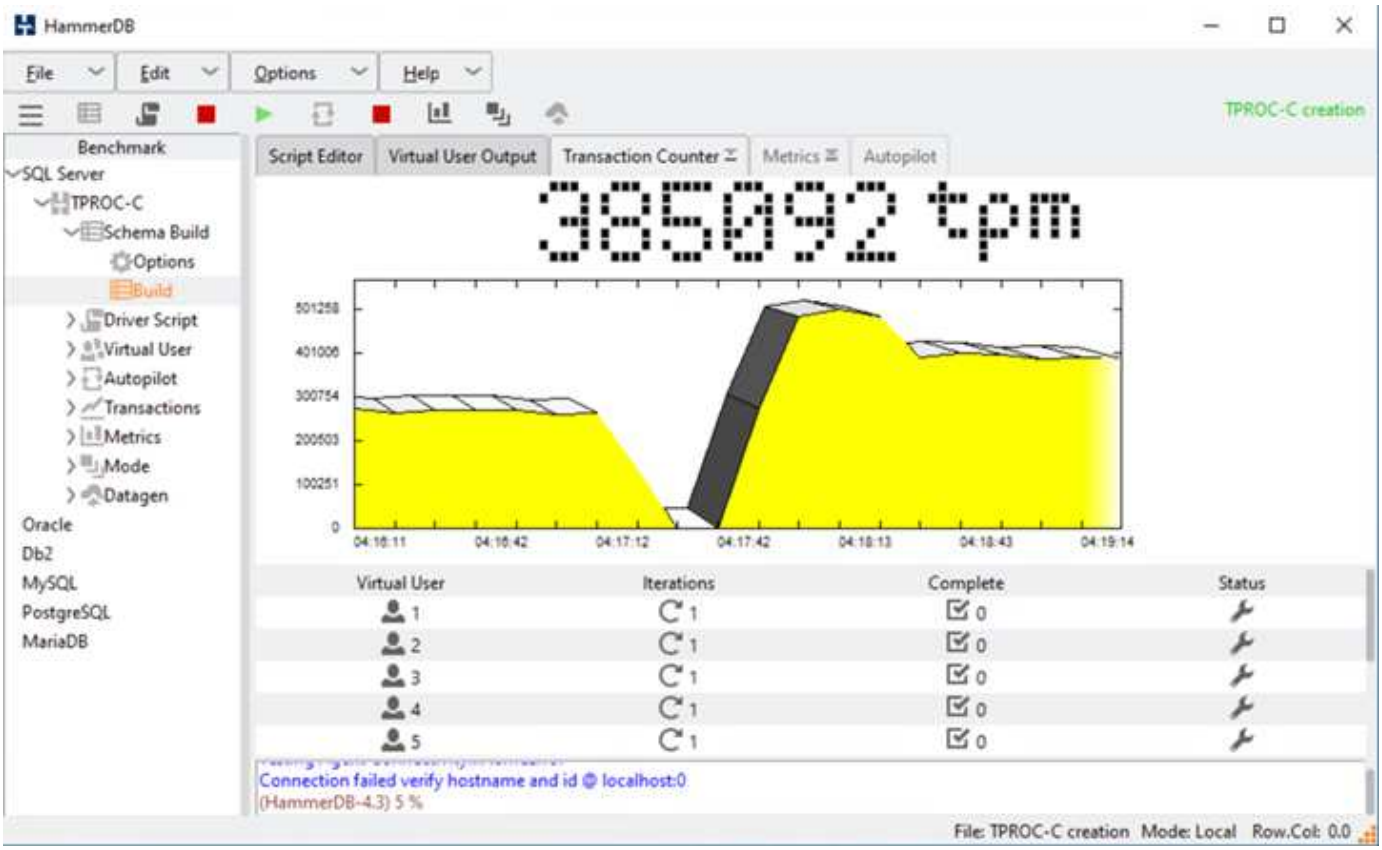
FlexPod SM-BC 솔루션의 비즈니스 크리티컬 워크로드 검증에 따라, Windows Server 2022 VM에 설치된 Microsoft SQL Server 2019가 SM-BC 계획 및 계획되지 않은 스토리지 페일오버 테스트를 위한 IOMeter VM과 함께 포함됩니다. Windows Server 2022 VM에서는 SQL Server를 관리하기 위해 SQL Server Management Studio가 설치됩니다. 테스트를 위해 HammerDB 데이터베이스 도구를 사용하여 데이터베이스 트랜잭션을 생성합니다.

Microsoft SQL Server TPROC-C 워크로드를 사용하여 테스트하도록 HammerDB 데이터베이스 테스트 도구를 구성했습니다. 스키마 빌드 구성의 경우 다음 스크린샷과 같이 10명의 가상 사용자가 있는 100개의 웨어하우스를 사용하도록 옵션이 업데이트되었습니다.



스키마 빌드 옵션이 업데이트된 후 스키마 빌드 프로세스가 시작되었습니다. 몇 분 후에 시스템 프로세서 CLI 명령을 사용하여 두 노드 AFF A250 스토리지 클러스터의 두 노드 전원을 동시에 꺼서 예정되지 않은 사이트 B 스토리지 클러스터 장애가 발생했습니다.

데이터베이스 트랜잭션을 잠시 일시 중지한 후 재해 복구를 위한 자동 페일오버가 시작되고 트랜잭션이 다시 시작되었습니다. 다음 스크린샷은 해당 시간에 대한 HammerDB 트랜잭션 카운터 스크린샷을 보여 줍니다. Microsoft SQL Server의 데이터베이스는 일반적으로 사이트 B 스토리지 클러스터에 상주하므로 사이트 B의 스토리지가 다운된 후 트랜잭션이 잠시 일시 중지되었다가 자동 페일오버가 발생한 후 다시 시작됩니다.



Storge 클러스터 메트릭은 NetApp Harvest 모니터링 툴이 설치된 NAbox 툴을 사용하여 캡처되었습니다. 결과는 스토리지 가상 머신 및 기타 스토리지 개체에 대한 사전 정의된 Grafana 대시보드에 표시됩니다. 대시보드는 사이트 B와 사이트 A에 대해 분리된 읽기 및 쓰기 통계와 함께 지연 시간, 처리량, IOPS 및 추가 세부 정보에 대한 매트릭스를 제공합니다

이 스크린샷은 사이트 B 스토리지 클러스터에 대한 NAbox Grafana 성능 대시보드를 보여줍니다.



사이트 B 스토리지 클러스터의 IOPS는 재해가 발생하기 전에 약 100K IOPS 였습니다. 그런 다음, 성능 메트릭이 재해로 인해 그래프 오른쪽에서 0으로 급격히 하락하는 것을 보였습니다. 사이트 B 스토리지 클러스터가 다운되었기 때문에 재해가 발생한 후 사이트 B 클러스터에서 아무것도 수집되지 않았습니다.

반면 사이트 A 스토리지 클러스터의 IOPS는 자동 페일오버 후 사이트 B에서 추가 워크로드를 선택했습니다. 다음

스크린샷에서는 IOPS 및 처리량 그래프의 오른쪽에 추가 워크로드를 쉽게 볼 수 있습니다. 이 그래프에는 사이트 A 스토리지 클러스터의 NAbox Grafana 성능 대시보드가 나와 있습니다.



위의 스토리지 재해 테스트 시나리오에서는 데이터베이스가 상주하는 사이트 B에서 Microsoft SQL Server 워크로드가 전체 스토리지 클러스터 중단 시에도 계속 유지될 수 있다는 것이 확인되었습니다. 애플리케이션은 재해가 감지되고 페일오버가 발생한 후 사이트에서 스토리지 클러스터로 제공되는 데이터 서비스를 투명하게 사용했습니다.

컴퓨팅 계층에서 특정 사이트에서 실행 중인 VM에 호스트 장애가 발생하면 VM은 VMware HA 기능을 통해 자동으로 다시 시작하도록 설계되어 있습니다. 전체 사이트 컴퓨팅 중단을 위해 VM/호스트 선호도 규칙을 통해 남아 있는 사이트에서 VM을 다시 시작할 수 있습니다. 하지만 비즈니스 크리티컬 애플리케이션에서 무중단 서비스를 제공하려면 애플리케이션 다운타임을 방지하기 위해 Microsoft Failover Cluster 또는 Kubernetes 컨테이너 기반 애플리케이션 아키텍처와 같은 애플리케이션 기반 클러스터링이 필요합니다. 이 기술 보고서의 범위를 벗어나는 애플리케이션 기반 클러스터링의 구현 방법은 관련 문서를 참조하십시오.

"다음: 결론."

결론

"이전: 솔루션 검증 시나리오."

SM-BC가 포함된 FlexPod 데이터 센터는 액티브-액티브 데이터 센터 설계를 사용하여 비즈니스 크리티컬 워크로드에 비즈니스 연속성 및 재해 복구를 제공합니다. 일반적으로 이 솔루션은 Metro 지역에 지리적으로 분산된 별도의 위치에 구축된 두 데이터 센터를 서로 연결합니다. NetApp SM-BC 솔루션은 동기식 복제를 사용하여 사이트 장애로부터 비즈니스 크리티컬 데이터 서비스를 보호합니다. 이 솔루션을 사용하려면 두 개의 FlexPod 배포 사이트에 10밀리초 미만의 라운드 트립 네트워크 지연 시간이 있어야 합니다.

세 번째 사이트에 구축된 NetApp ONTAP 중재자가 SM-BC 솔루션을 모니터링하고 사이트 재해가 탐지될 때 자동 페일오버를 지원합니다. VMware HA 및 VMware vSphere Metro Storage Cluster 구성을 지원하는 VMware vCenter는 NetApp SM-BC와 원활하게 연동되므로 원하는 제로 RPO 및 제로에 가까운 RTO 목표를 충족할 수 있습니다.

FlexPod SM-BC 솔루션은 기존 FlexPod 인프라스트럭처에서 요구 사항을 충족하는 경우 또는 기존 FlexPod에 FlexPod 솔루션을 추가하여 비즈니스 연속성 목표를 달성할 수도 있습니다. NetApp과 Cisco는 Cisco Intersight, Ansible, HashCorp Terraform 기반 자동화 등의 추가 관리, 모니터링 및 자동화 툴을 사용하여 솔루션을 쉽게

모니터링하고 운영에 대한 통찰력을 확보하며 구축 및 운영을 자동화할 수 있습니다.

Microsoft SQL Server와 같은 비즈니스에 중요한 애플리케이션의 관점에서 볼 때 ONTAP SM-BC CG 관계에 의해 보호되는 VMware 데이터 저장소에 상주하는 데이터베이스는 사이트 스토리지 중단이 발생해도 계속 사용할 수 있습니다. 검증 테스트 중에 확인된 바와 같이, 데이터베이스가 상주하는 스토리지 클러스터의 정전이 발생한 후 SM-BC CG 관계의 페일오버가 발생하고 Microsoft SQL Server 트랜잭션이 애플리케이션 중단 없이 재개됩니다.

애플리케이션의 세분화된 데이터 보호를 통해 비즈니스 크리티컬 애플리케이션에 ONTAP SM-BC CG 관계를 생성하여 제로 RPO 및 제로에 가까운 RTO 요구사항을 충족할 수 있습니다. 따라서 Microsoft SQL Server 애플리케이션이 실행 중인 VMware 클러스터가 사이트 스토리지 가동 중단 시에도 유지될 수 있도록 각 사이트에 있는 ESXi 호스트의 부팅 LUN도 SM-BC CG 관계에 의해 보호됩니다.

FlexPod의 유연성과 확장성을 활용하면 비즈니스 요구사항의 변화에 따라 성장 및 발전할 수 있는 적절한 규모의 인프라로 시작할 수 있습니다. 이 검증된 설계를 통해 분산된 통합 인프라에 VMware vSphere 기반 프라이빗 클라우드를 안정적으로 구축할 수 있으므로, 많은 단일 장애 지점 시나리오에 대한 복원력과 중요 비즈니스 데이터 서비스를 보호하지 못하는 사이트 장애 복구 기능을 갖춘 솔루션을 제공할 수 있습니다.

"다음: 추가 정보 및 버전 기록을 찾을 위치."

추가 정보 및 버전 기록을 찾을 수 있는 위치

"이전: 결론."

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

FlexPod

- FlexPod 홈 페이지

  "https://www.flexpod.com"

- FlexPod용 Cisco Validated Design 및 구축 가이드

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- Cisco 서버 - UCS(Unified Computing System)

  "https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html"

- NetApp 제품 설명서

  "https://www.netapp.com/support-and-training/documentation/"

- UCS 관리 모드, VMware vSphere 7.0 U2 및 NetApp ONTAP 9.9에서 Cisco UCS 4.2(1)가 지원되는 FlexPod 데이터 센터 설계 가이드

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2_design.html"

- UCS 관리 모드, VMware vSphere 7.0 U2 및 NetApp ONTAP 9.9에서 Cisco UCS 4.2(1)가 지원되는 FlexPod 데이터 센터 구축 가이드

"https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html"

- Cisco UCS X-Series, VMware 7.0 U2 및 NetApp ONTAP 9.9를 지원하는 FlexPod 데이터 센터 설계 가이드

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"

- FlexPod 데이터 센터 및 Cisco UCS X 시리즈, VMware 7.0 U2 및 NetApp ONTAP 9.9 구축 가이드

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmware_7u2.html"

- FlexPod Express for VMware vSphere 7.0 with Cisco UCS Mini 및 NetApp AFF/FAS NVA 설계 가이드

  https://www.netapp.com/pdf.html?item=/media/22621-nva-1154-DESIGN.pdf

- FlexPod Express for VMware vSphere 7.0 with Cisco UCS Mini 및 NetApp AFF/FAS NVA 구축 가이드

  https://www.netapp.com/pdf.html?item=/media/21938-nva-1154-DEPLOY.pdf

- VXLAN 멀티 사이트 프런트엔드 패브릭을 사용하는 FlexPod MetroCluster IP

  "https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/flexpod-metrocluster-ip-vxlan-multi-site-wp.pdf"

- NAbox(NAbox)

  "https://nabox.org"

- NetApp 수집

  "https://github.com/NetApp/harvest/releases"

SM - BC

- SM - BC

  "https://docs.netapp.com/us-en/ontap/smbc/index.html"

- TR-4878: SM-BC(SnapMirror 비즈니스 연속성) ONTAP 9.8

  https://www.netapp.com/pdf.html?item=/media/21888-tr-4878.pdf

- SnapMirror 관계 ONTAP 9를 올바르게 삭제하는 방법

  "https://kb.netapp.com/Advice_and_Troubleshooting/Data_Protection_and_Security/SnapMirror/How_to_correctly_delete_a_SnapMirror_relationship_ONTAP_9"

- SnapMirror Synchronous 재해 복구 기본 사항

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-synchronous-disaster-recovery-basics-concept.html"

- 비동기식 SnapMirror 재해 복구 기본 사항

"https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-disaster-recovery-concept.html#data-protection-relationships"

- 데이터 보호 및 재해 복구

  "https://docs.netapp.com/us-en/ontap/data-protection-disaster-recovery/index.html"

- ONTAP 중재자 서비스를 설치하거나 업그레이드합니다

  "https://docs.netapp.com/us-en/ontap/mediator/index.html"

VMware vSphere HA 및 **vSphere Metro Storage Cluster**를 지원합니다

- vSphere HA 클러스터 생성 및 사용

  "https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-5432CA24-14F1-44E3-87FB-61D937831CF6.html"

- VMware vMSC(vSphere Metro Storage Cluster)

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-vmsc"

- VMware vSphere Metro Storage Cluster 권장 사례

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-recommended-practices"

- NetApp ONTAP with NetApp SnapMirror SM-BC(Business Continuity) with VMware vSphere Metro Storage Cluster(vMSC). (83370)

  "https://kb.vmware.com/s/article/83370"

- VMware vSphere Metro Storage Cluster 및 ONTAP를 사용하여 계층 1 애플리케이션과 데이터베이스를 보호합니다

  "https://community.netapp.com/t5/Tech-ONTAP-Blogs/Protect-tier-1-applications-and-databases-with-VMware-vSphere-Metro-Storage/ba-p/171636"

Microsoft SQL 및 **HammerDB**

- Microsoft SQL Server 2019

  "https://www.microsoft.com/en-us/sql-server/sql-server-2019"

- VMware vSphere 기반 Microsoft SQL Server 설계 Best Practices Guide를 참조하십시오

  "https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/sql-server-on-vmware-best-practices-guide.pdf"

- HammerDB 웹 사이트

  "https://www.hammerdb.com"

호환성 매트릭스

- Cisco UCS 하드웨어 호환성 매트릭스

  "https://ucshcltool.cloudapps.cisco.com/public/"

- NetApp 상호 운용성 매트릭스 툴

  "https://support.netapp.com/matrix/"

- NetApp Hardware Universe를 참조하십시오

  "https://hwu.netapp.com"

- VMware 호환성 가이드 를 참조하십시오

  "http://www.vmware.com/resources/compatibility/search.php"

버전 기록

버전	날짜	문서 버전 기록
버전 1.0	2022년 4월	최초 릴리스.

VMware vSphere 7.0 및 NetApp ONTAP 9.7을 사용하는 FlexPod 데이터 센터 - 구축

John George, Cisco Sree Lakshmi Lanka, NetApp

이 문서에서는 NetApp AFF A400 All-Flash 스토리지 시스템에서 NetApp ONTAP 9.7을 지원하는 Cisco 및 NetApp FlexPod 데이터 센터, 2세대 인텔 제온 스케일러블 프로세서와 VMware vSphere 7.0을 지원하는 Cisco UCS Manager 통합 소프트웨어 릴리스 4.1(2)에 대해 설명합니다. Cisco UCS Manager(UCSM) 4.1(2)은 다음과 같은 사항을 통합 지원합니다.

- 현재 모든 Cisco UCS Fabric Interconnect 모델: 6200, 6300, 6324(Cisco UCS Mini)
- 6400
- 2200/2300/2400 시리즈 IOM
- Cisco UCS B-Series 를 참조하십시오
- Cisco UCS C-Series 를 참조하십시오

Cisco Intersight 및 NetApp Active IQ SaaS 관리 플랫폼도 포함되어 있습니다.

NetApp ONTAP 9.7, Cisco UCS Unified 소프트웨어 릴리즈 4.1(2) 및 VMware vSphere 7.0이 포함된 FlexPod 데이터 센터는 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 9000 스위치 제품군, MDS 9000 Multilayer 패브릭 스위치, ONTAP 9.7 데이터 관리 소프트웨어를 실행하는 NetApp AFF A 시리즈 스토리지 어레이를 완벽하게 지원합니다.

"VMware vSphere 7.0 및 NetApp ONTAP 9.7을 사용하는 FlexPod 데이터 센터 - 구축"

FlexPod 데이터 센터 및 Cisco Intersight, NetApp ONTAP 9.7 - 설계

John George, Cisco Scott Kovacs, NetApp

이 문서에서는 Cisco 및 NetApp 기술을 공유 클라우드 인프라로 구축하기 위한 검증된 접근 방식인 Cisco 및 NetApp FlexPod 솔루션에 대해 설명합니다. 이 검증된 설계는 FlexPod에서 엔터프라이즈급 데이터 센터에서 가장 많이 사용되는 가상화 플랫폼인 VMware vSphere를 구축하기 위한 프레임워크를 제공합니다.

"FlexPod 데이터 센터 및 Cisco Intersight, NetApp ONTAP 9.7 - 설계"

FlexPod 데이터 센터 및 Cisco Intersight, NetApp ONTAP 9.7 - 배포

John George, Cisco Scott Kovacs, NetApp

현재 데이터 센터 설계의 업계 동향은 공유 인프라를 사용하는 것입니다. 엔터프라이즈 고객은 사전 검증된 IT 플랫폼과 함께 가상화를 사용함으로써 애플리케이션 사일로에서 벗어나 빠르게 구축할 수 있는 공유 인프라로 전환하여 민첩성을 높이고 비용을 절감함으로써 클라우드로의 전환에 착수했습니다. Cisco와 NetApp은 최고 수준의 스토리지, 서버 및 네트워크 구성요소를 사용하여 다양한 워크로드의 기초가 되는 FlexPod를 제공함으로써 빠르고 자신 있게 구축할 수 있는 효율적인 아키텍처 설계를 지원합니다.

"FlexPod 데이터 센터 및 Cisco Intersight, NetApp ONTAP 9.7 - 배포"

FlexPod 데이터 센터 및 Cisco Intersight, NetApp ONTAP 9.7 - 설계

John George, Cisco Scott Kovacs, NetApp

이 문서에서는 Cisco 및 NetApp 기술을 공유 클라우드 인프라로 구축하기 위한 검증된 솔루션에 대해 설명합니다. 이 검증된 설계는 FlexPod에서 엔터프라이즈급 데이터 센터에서 가장 많이 사용되는 가상화 플랫폼인 VMware vSphere를 구축하기 위한 프레임워크를 제공합니다.

FlexPod은 광범위한 엔터프라이즈 워크로드 및 사용 사례를 지원하는 업계 최고의 통합 인프라입니다. 이 솔루션을 통해 고객은 통합 인프라에 VMware vSphere 기반 프라이빗 클라우드를 빠르고 안정적으로 구축할 수 있습니다.

"FlexPod 데이터 센터 및 Cisco Intersight, NetApp ONTAP 9.7 - 설계"

VMware vSphere 6.7 U2, Cisco UCS fouth-generation Fabric 및 NetApp ONTAP 9.6이 지원되는 FlexPod 데이터 센터

John George, Cisco Sree Lakshmi Lanka, NetApp

이 문서에서는 NetApp ONTAP 9.6 및 Cisco UCS Manager 통합 소프트웨어 릴리즈 4.0(4),

2세대 인텔 제온 스케일러블 프로세서, VMware vSphere 6.7 U2가 설치된 Cisco 및 NetApp FlexPod 데이터 센터에 대해 설명합니다. Cisco UCS Manager(UCSM) 4.0(4)은 다음 사항을 통합 지원합니다.

- 현재 모든 Cisco UCS Fabric Interconnect 모델: 6200, 6300, 6324(Cisco UCS Mini)
- 6454
- 2200/2300/2400 시리즈 IOM
- Cisco UCS B-Series 를 참조하십시오
- Cisco UCS C-Series 를 참조하십시오.

NetApp ONTAP 9.6, Cisco UCS Unified Software Release 4.0(4) 및 VMware vSphere 6.7 U2가 포함된 FlexPod 데이터 센터는 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 9000 스위치 제품군, MDS 9000 Multilayer 패브릭 스위치, ONTAP 9를 실행하는 NetApp AFF A-Series 스토리지 어레이를 제공할 좋은 기회입니다.

"VMware vSphere 6.7 U2, Cisco UCS 4세대 패브릭 및 NetApp ONTAP 9.6이 지원되는 FlexPod 데이터 센터"

VMware vSphere 6.7 U1, Cisco UCS 4세대 패브릭 및 NetApp AFF A-Series를 지원하는 FlexPod 데이터 센터 - 설계

John George, Cisco Sree Lakshmi Lanka, NetApp

이 문서에서는 Cisco 및 NetApp 기술을 공유 클라우드 인프라로 구축하기 위한 검증된 접근 방식인 Cisco 및 NetApp FlexPod 솔루션에 대해 설명합니다. 이 검증된 설계는 FlexPod에서 엔터프라이즈급 데이터 센터에서 가장 많이 사용되는 가상화 플랫폼인 VMware vSphere를 구축하기 위한 프레임워크를 제공합니다.

FlexPod은 광범위한 엔터프라이즈 워크로드 및 사용 사례를 지원하는 업계 최고의 통합 인프라입니다. 이 솔루션을 통해 고객은 통합 인프라에 VMware vSphere 기반 프라이빗 클라우드를 빠르고 안정적으로 구축할 수 있습니다.

권장 솔루션 아키텍처는 Cisco UCS(Cisco Unified Computing System) 기반 위에 구축되어 Cisco UCS B-Series 블레이드 및 C-Series 랙 서버, Cisco UCS 6454 Fabric Interconnect, Cisco Nexus 9000 시리즈 스위치, Cisco MDS 파이버 채널 스위치 등 Cisco UCS 하드웨어 플랫폼을 지원합니다. 및 NetApp All Flash Series 스토리지 어레이를 모두 활용할 수 있습니다. 또한 스토리지 활용을 최적화하고 프라이빗 클라우드를 지원하는 여러 가지 새로운 기능을 제공하는 VMware vSphere 6.7 Update 1이 포함되어 있습니다.

"VMware vSphere 6.7 U1, Cisco UCS 4세대 패브릭 및 NetApp AFF A-Series를 지원하는 FlexPod 데이터 센터 - 설계"

VMware vSphere 6.7 U1, Cisco UCS 4세대 패브릭 및 NetApp AFF A-Series를 지원하는 FlexPod 데이터 센터

John George, Cisco Scott Kovacs, NetApp

이 문서에서는 Cisco UCS Manager 통합 소프트웨어 릴리즈 4.0(2) 및 VMware vSphere 6.7 U1이 설치된 Cisco 및 NetApp FlexPod 데이터 센터에 대해 설명합니다. Cisco UCS Manager(UCSM) 4.0(2)은 현재 모든 Cisco UCS Fabric Interconnect 모델(6200, 6300,

6324(Cisco UCS Mini), 6454,2200/2300 시리즈 IOM, Cisco UCS B-Series 및 Cisco UCS C-Series를 통합 지원합니다. Cisco UCS Unified Software Release 4.0(2) 및 VMware vSphere 6.7 U1을 지원하는 FlexPod 데이터 센터는 Cisco UCS(Unified Computing System), Cisco Nexus 9000 스위치 제품군, MDS 9000 멀티레이어 패브릭 스위치를 기반으로 사전 설계된 모범 사례 데이터 센터 아키텍처입니다. ONTAP 9 스토리지 OS를 실행하는 NetApp AFF A-Series 스토리지 어레이를 제공할 좋은 기회입니다.

"VMware vSphere 6.7 U1, Cisco UCS 4세대 패브릭 및 NetApp AFF A-Series를 지원하는 FlexPod 데이터 센터"

FlexPod 데이터 센터 및 Cisco ACI 멀티 포드, NetApp MetroCluster IP, VMware vSphere 6.7-Design

Haseeb Niazi, Cisco Arvind Ramakrishnan, NetApp

이 문서에서는 고가용성 멀티 데이터 센터 솔루션을 제공하기 위해 Cisco ACI Multi-Pod 및 NetApp MetroCluster IP 솔루션을 FlexPod 데이터 센터에 통합하는 방법을 설명합니다. 멀티 데이터 센터 아키텍처는 무중단 워크로드 이동성을 활용하여 두 데이터 센터 간에 워크로드의 균형을 조정할 수 있는 기능을 제공하므로 중단을 유지할 필요 없이 사이트 간에 서비스를 마이그레이션할 수 있습니다.

ACI 멀티 포드와 NetApp MetroCluster IP 솔루션이 지원하는 FlexPod는 다음과 같은 이점을 제공합니다.

- 데이터 센터 간에 원활하게 워크로드를 이동할 수 있습니다
- 사이트 전체에 일관된 정책 적용
- 지리적으로 분산된 데이터 센터에서 Layer-2 확장
- 유지 관리 시 다운타임 방지 강화
- 재해 방지 및 복구

"FlexPod 데이터 센터 및 Cisco ACI 멀티 포드, NetApp MetroCluster IP, VMware vSphere 6.7-Design"

NetApp MetroCluster IP 및 VMware vSphere 6.7-Deployment가 포함된 Cisco ACI 멀티 포드를 지원하는 FlexPod 데이터 센터

Haseeb Niazi, Cisco Ramesh Issac, Cisco Arvind Ramakrishnan, NetApp

Cisco와 NetApp은 전략적 데이터 센터 플랫폼을 지원하는 일련의 FlexPod 솔루션을 제공하기 위해 협력하고 있습니다. FlexPod 솔루션은 컴퓨팅, 스토리지 및 네트워킹에 대한 모범 설계 사례를 통합하는 통합 아키텍처를 제공하므로 다양한 구성 요소 간의 호환성을 보장하기 위해 통합 아키텍처를 검증하여 IT 위험을 최소화할 수 있습니다. 또한 이 솔루션은 배포의 다양한 단계(계획, 설계 및 구현)에서 사용할 수 있는 문서화된 설계 지침, 배포 지침 및 지원을 제공하여 IT 당면 과제를 해결합니다.

"NetApp MetroCluster IP 및 VMware vSphere 6.7-Deployment가 포함된 Cisco ACI 멀티 포드를 지원하는

FlexPod 데이터 센터"

하이브리드 클라우드

FlexPod 하이브리드 클라우드 및 Cloud Volumes ONTAP for Epic

TR-4960: FlexPod 하이브리드 클라우드 with Cloud Volumes ONTAP for Epic

파트너 후원: 

Kamini Singh, NetApp

디지털 혁신의 핵심은 데이터를 통해 더 많은 작업을 수행하는 것입니다. 병원에서는 조직을 운영하고 환자를 효과적으로 지원하기 위해 대량의 데이터를 생성하고 필요로 합니다. 환자 치료 및 직원 일정 및 의료 리소스 관리 시 정보가 수집 및 처리됩니다.

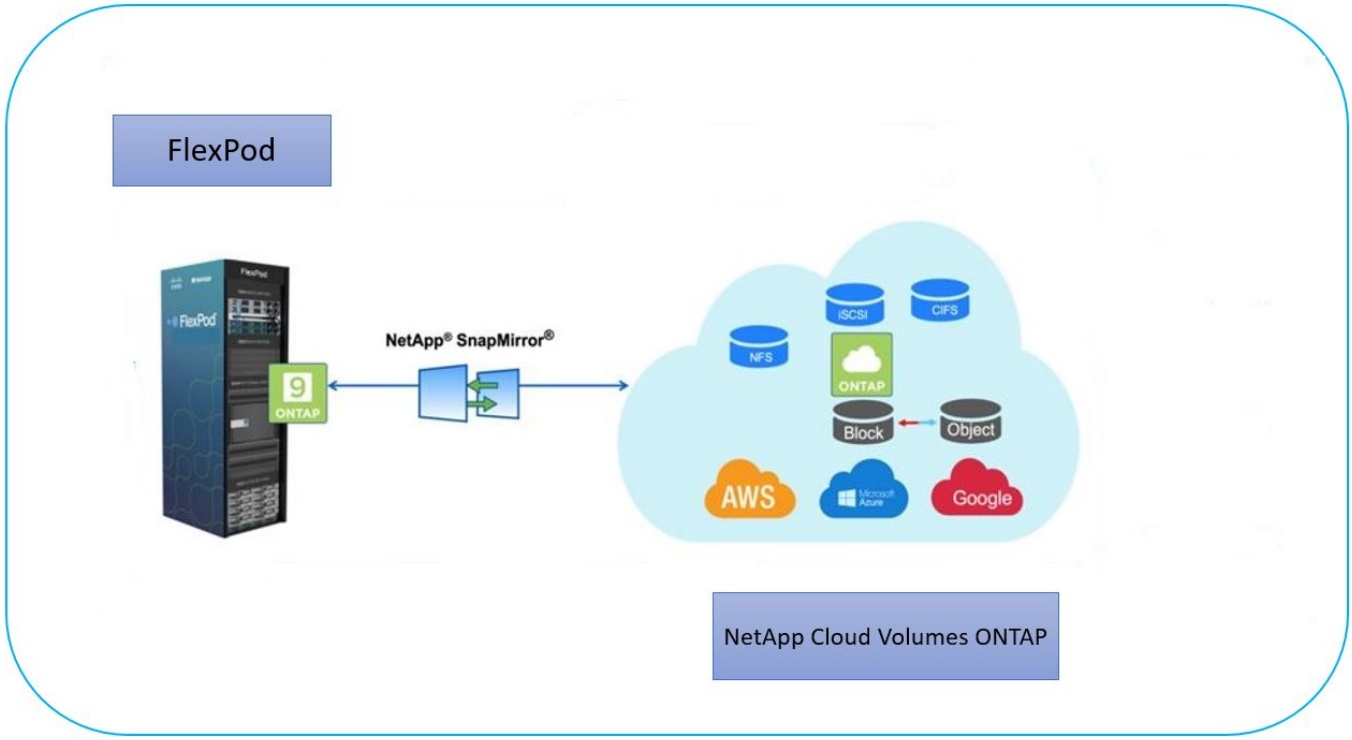
날로 증가하는 의료 데이터의 크기와 이러한 데이터에서 얻을 수 있는 중요한 통찰력으로 인해 의료 데이터 서비스와 데이터 보호의 중요성과 도전 과제가 모두 가중되고 있습니다. 첫째, 데이터 복구, 의료 비즈니스 연속성 또는 규정 준수 요구사항을 충족하려면 의료 데이터를 모두 사용하고 보호해야 합니다.

둘째, 의료 데이터를 쉽게 분석할 수 있도록 해야 합니다. 이 분석에서는 종종 인공 지능(AI) 및 머신 러닝(ML) 기반 접근 방식을 사용하여 의료 비즈니스가 솔루션을 개선하고 비즈니스 가치를 창출할 수 있도록 도와줍니다.

셋째, 데이터 서비스 인프라와 데이터 보호 방법론은 의료 비즈니스의 성장에 따라 의료 데이터의 증가를 수용해야 합니다. 또한, 데이터 분석 또는 보관을 위해 데이터를 에지에서 코어 및 클라우드로 이동해야 하기 때문에 데이터 이동성이 점점 더 중요해지고 있습니다.

NetApp은 의료 등의 엔터프라이즈 애플리케이션을 위한 단일 데이터 관리 솔루션을 제공하며 병원이 디지털 혁신을 향한 여정을 안내할 수 있습니다. NetApp Cloud Volumes ONTAP은 FlexPod 데이터 센터에서 AWS와 같은 퍼블릭 클라우드에 구축된 Cloud Volumes ONTAP으로 데이터를 효율적으로 복제할 수 있는 의료 데이터 관리 솔루션을 제공합니다.

Cloud Volumes ONTAP는 비용 효율적이고 안전한 퍼블릭 클라우드 리소스를 활용하여 매우 효율적인 데이터 복제, 내장된 스토리지 효율성 및 간단한 DR 테스트를 통해 클라우드 기반 재해 복구(DR)를 개선합니다. 이러한 시스템은 통합 제어 및 끌어서 놓기 방식으로 관리되므로 모든 종류의 오류, 장애 또는 재해로부터 비용 효율적으로 보호할 수 있습니다. Cloud Volumes ONTAP은 증분 업데이트를 통해 타겟을 최신 상태로 유지하는 블록 레벨 데이터 복제용 솔루션으로 NetApp SnapMirror 기술을 제공합니다.



대상

이 문서는 NetApp 및 파트너 솔루션 엔지니어(SE) 및 프로페셔널 서비스 직원을 대상으로 합니다. NetApp은 독자가 다음과 같은 배경 지식을 가지고 있다고 가정합니다.

- SAN 및 NAS 개념을 확실하게 이해합니다
- NetApp ONTAP 스토리지 시스템에 대한 기술적 지식
- ONTAP 소프트웨어의 구성 및 관리에 대한 기술적 지식

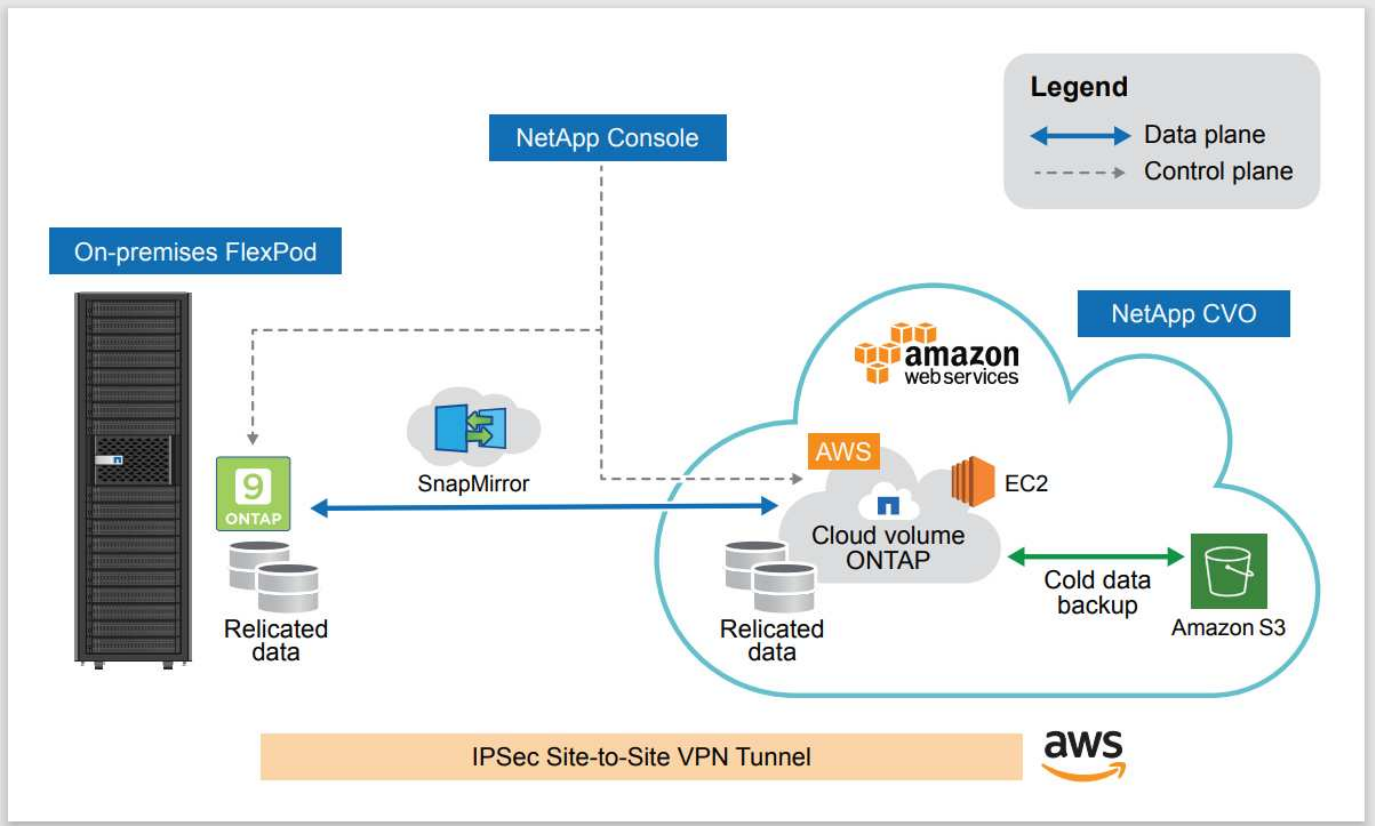
솔루션 이점

NetApp Cloud Volumes ONTAP와 통합된 FlexPod 데이터 센터는 의료 워크로드에 다음과 같은 이점을 제공합니다.

- * 맞춤형 보호. * Cloud Volumes ONTAP는 증분 업데이트를 통해 ONTAP에서 클라우드로 블록 레벨 데이터 복제를 제공하여 대상을 최신 상태로 유지합니다. 사용자는 동기화 일정을 지정하여 소스의 변경 내용이 전송되는 시기를 결정할 수 있습니다. 이를 통해 모든 종류의 의료 데이터에 대한 맞춤형 보호가 제공됩니다.
- * 장애 조치 및 장애 복구. * 재해가 발생하면 스토리지 관리자가 클라우드 볼륨으로 신속하게 장애 조치를 설정할 수 있습니다. 운영 사이트가 복구되면 DR 환경에서 생성된 새 데이터가 소스 볼륨과 다시 동기화되어 2차 데이터 복제가 다시 설정됩니다. 이러한 방식으로 중단 없이 의료 데이터를 쉽게 복구할 수 있습니다.
- * 효율성 * 보조 클라우드 복사본의 스토리지 공간 및 비용은 데이터 압축, 씬 프로비저닝, 중복제거를 통해 최적화됩니다. 의료 데이터는 압축 및 중복제거된 형태로 블록 레벨에서 전송되므로 전송 속도가 빨라집니다. 또한 데이터는 저비용 오브젝트 스토리지로 자동 계층화되며 DR 시나리오와 같은 액세스 시에만 고성능 스토리지로 돌아갑니다. 따라서 지속적으로 발생하는 스토리지 비용이 크게 절감됩니다.
- 랜섬웨어 보호**.** NetApp Console 랜섬웨어 보호는 온프레미스 및 클라우드 환경 전반의 데이터 소스를 검사하고, 보안 취약성을 탐지하고, 현재 보안 상태와 위험 점수를 제공합니다. 그런 다음 추가 조사하고 수정을 위해 따를 수 있는 실행 가능한 권장 사항을 제공합니다. 이를 통해 중요한 의료 데이터를 랜섬웨어 공격으로부터 보호할 수 있습니다.

솔루션 토폴로지

이 섹션에서는 솔루션의 논리적 토폴로지를 설명합니다. 다음 그림은 온프레미스 환경인 FlexPod , Amazon Web Services(AWS)에서 실행되는 NetApp Cloud Volumes ONTAP (CVO), NetApp Console SaaS 플랫폼으로 구성된 솔루션 토폴로지를 나타냅니다.



컨트롤 평면과 데이터 평면은 끝점 사이에 명확하게 표시됩니다. 데이터 플레인은 FlexPod의 All-Flash FAS에서 실행되는 ONTAP 인스턴스와 안전한 사이트 간 VPN 연결을 활용하여 AWS의 NetApp CVO 인스턴스 간에 실행됩니다. 사내 FlexPod 데이터 센터에서 NetApp Cloud Volumes ONTAP으로 의료 워크로드 데이터 복제를 NetApp SnapMirror 복제 방식으로 처리합니다. 이 솔루션에서 NetApp CVO 인스턴스에 상주하는 콜드 데이터를 AWS S3에 선택적으로 백업 및 계층화할 수도 있습니다.

"다음: 솔루션 구성 요소."

솔루션 구성 요소

"이전: 솔루션 개요."

FlexPod

FlexPod는 가상화된 솔루션과 가상화되지 않은 솔루션 모두를 위한 통합된 기반을 형성하는 정의된 하드웨어 및 소프트웨어 세트입니다. FlexPod에는 NetApp ONTAP 스토리지, Cisco Nexus 네트워킹, Cisco MDS 스토리지 네트워킹 및 Cisco UCS(Unified Computing System)가 포함되어 있습니다.

의료 조직에서는 디지털 혁신을 촉진하고 환자 경험 및 결과를 개선할 수 있는 솔루션을 찾고 있습니다. FlexPod를 사용하면 안전하고 확장 가능한 플랫폼을 통해 효율성을 높이고, 직원들이 정보에 근거하여 보다 신속하게 결정을 내릴 수 있도록 함으로써 환자를 보다 효과적으로 간호할 수 있습니다.

FlexPod는 다음과 같은 이점을 제공하므로 의료 워크로드 요구사항에 이상적인 플랫폼입니다.

- 작업 최적화를 통해 통찰력을 높이고 환자 결과를 개선할 수 있습니다.
- 확장 가능하고 안정적인 인프라로 이미징 애플리케이션 간소화
- EHR과 같은 의료 관련 앱을 위한 검증된 접근 방식으로 빠르고 효율적으로 배포

EHR

EHR(Electronic Health Records)은 중간 규모 및 대규모 의료 그룹, 병원 및 통합 의료 조직을 위한 소프트웨어를 만듭니다. 또한 커뮤니티 병원, 학술 시설, 아동 기관, 안전망 제공자 및 다중 병원 시스템도 고객이 포함됩니다. EHR 통합 소프트웨어는 임상, 액세스 및 수익 기능을 확장하여 집으로 확장합니다.

의료 기관 조직은 업계 최고의 EHR에 투자함으로써 얻을 수 있는 이익을 극대화해야 한다는 압박을 받고 있습니다. 고객은 EHR 솔루션 및 미션 크리티컬 애플리케이션을 위한 데이터 센터를 설계할 때 데이터 센터 아키텍처에서 다음 목표를 식별하는 경우가 많습니다.

- EHR 애플리케이션의 고가용성
- 고성능
- 데이터 센터에 EHR을 손쉽게 구현할 수 있습니다
- 새로운 EHR 릴리즈 또는 애플리케이션을 사용하여 성장을 실현할 수 있는 민첩성과 확장성
- 비용 효율성
- 관리 용이성, 안정성 및 지원 용이성
- 강력한 데이터 보호, 백업, 복구 및 비즈니스 연속성

FlexPod 는 EHR 인증을 받았으며 Intel Xeon 프로세서가 탑재된 Cisco UCS, Red Hat Enterprise Linux(RHEL) 및 VMware ESXi를 통한 가상화를 포함하는 플랫폼 Cisco 지원합니다. ONTAP 실행하는 NetApp 스토리지에 대한 EHR의 높은 편의성 수준 순위와 결합된 이 플랫폼을 사용하면 FlexPod 통해 완벽하게 관리되는 프라이빗 클라우드에서 의료 애플리케이션을 실행할 수 있으며, 이는 모든 퍼블릭 클라우드 공급자에도 연결할 수 있습니다.

NetApp Console

NetApp Console 은 IT 전문가와 클라우드 아키텍트가 NetApp 클라우드 솔루션을 사용하여 하이브리드 멀티클라우드 인프라를 중앙에서 관리할 수 있도록 하는 엔터프라이즈급 SaaS 기반 관리 플랫폼입니다. 온프레미스 및 클라우드 스토리지를 보고 관리하기 위한 중앙 집중식 시스템을 제공하며, 하이브리드 및 여러 클라우드 공급자와 계정을 지원합니다. 자세한 내용은 다음을 참조하세요. "NetApp Console 설명서".

콘솔 에이전트

콘솔 에이전트 인스턴스를 사용하면 콘솔에서 퍼블릭 클라우드 환경 내의 리소스와 프로세스를 관리할 수 있습니다. 콘솔에서 제공하는 많은 기능을 사용하려면 콘솔 에이전트가 필요하며, 클라우드나 온프레미스 네트워크에 배포할 수 있습니다.

콘솔 에이전트는 다음 위치에서 지원됩니다.

- Amazon Web Services에서 직접 지원합니다
- Microsoft Azure를 참조하십시오
- Google 클라우드

- 온프레미스

"콘솔 에이전트에 대해 자세히 알아보세요".

NetApp Cloud Volumes ONTAP를 참조하십시오

NetApp Cloud Volumes ONTAP는 클라우드에서 ONTAP 데이터 관리 소프트웨어를 실행하여 파일 및 블록 워크로드에 대한 고급 데이터 관리 기능을 제공하는 소프트웨어 정의 스토리지 오퍼링입니다. Cloud Volumes ONTAP을 사용하면 클라우드 스토리지 비용을 최적화하고 애플리케이션 성능을 높이는 동시에 데이터 보호, 보안 및 규정 준수를 향상할 수 있습니다.

주요 이점은 다음과 같습니다.

- * 스토리지 효율성 * 내장 데이터 중복제거, 데이터 압축, 씬 프로비저닝, 즉각적인 클로닝을 활용하여 스토리지 비용을 최소화합니다.
- * 고가용성. * 클라우드 환경에서 장애가 발생할 경우 엔터프라이즈급 안정성과 지속적인 운영을 제공합니다.
- * 데이터 보호. * Cloud Volumes ONTAP은 업계 최고의 NetApp 복제 기술인 SnapMirror를 사용하여 사내 데이터를 클라우드로 복제하므로 여러 사용 사례에서 2차 복사본을 쉽게 사용할 수 있습니다. Cloud Volumes ONTAP는 또한 클라우드 백업과 통합되어 클라우드 데이터를 보호하고 장기적으로 아카이빙하기 위한 백업 및 복원 기능을 제공합니다.
- * 데이터 계층화. * 애플리케이션을 오프라인으로 전환하지 않고도 필요에 따라 고성능 및 저성능 스토리지 풀을 전환할 수 있습니다.
- * 애플리케이션 정합성: * NetApp SnapCenter 기술을 사용하여 NetApp Snapshot 복사본의 일관성을 제공합니다.
- * 데이터 보안. * Cloud Volumes ONTAP는 데이터 암호화를 지원하고 바이러스 및 랜섬웨어에 대한 보호를 제공합니다.
- * 개인 정보 보호 규정 준수 제어. * Cloud Data Sense와 통합하여 데이터 컨텍스트를 이해하고 중요한 데이터를 식별할 수 있습니다.

더 자세한 정보는 다음을 참조하세요."Cloud Volumes ONTAP" .

NetApp Active IQ Unified Manager를 참조하십시오

NetApp Active IQ Unified Manager를 사용하면 커뮤니티 지혜 및 AI 분석을 제공하는, 새롭게 재설계된 직관적인 단일 인터페이스를 통해 ONTAP 스토리지 클러스터를 모니터링할 수 있습니다. 이 솔루션은 스토리지 환경 및 스토리지 환경에서 실행되는 가상 시스템에 대한 포괄적인 운영, 성능 및 사전 통찰력을 제공합니다. 스토리지 인프라에서 문제가 발생하면 Unified Manager에서 문제의 세부 정보를 알려 근본 원인을 파악할 수 있습니다. 가상 머신 대시보드에서는 VM의 성능 통계를 볼 수 있으므로 vSphere 호스트에서 네트워크를 거쳐 마지막으로 스토리지까지 전체 입출력 경로를 조사할 수 있습니다.

일부 이벤트는 문제를 해결하기 위해 취할 수 있는 개선 조치도 제공합니다. 이벤트가 발생할 때 e-메일 및 SNMP 트랩을 통해 알림을 받도록 이벤트에 대한 사용자 지정 알림을 구성할 수 있습니다. Active IQ Unified Manager를 사용하면 용량 및 사용 추세를 예측하여 사용자의 스토리지 요구 사항을 계획할 수 있으므로 문제 발생 전에 조치를 취할 수 있고 장기적인 문제를 야기할 수 있는 사후 대처 방식의 단기 결정을 방지할 수 있습니다.

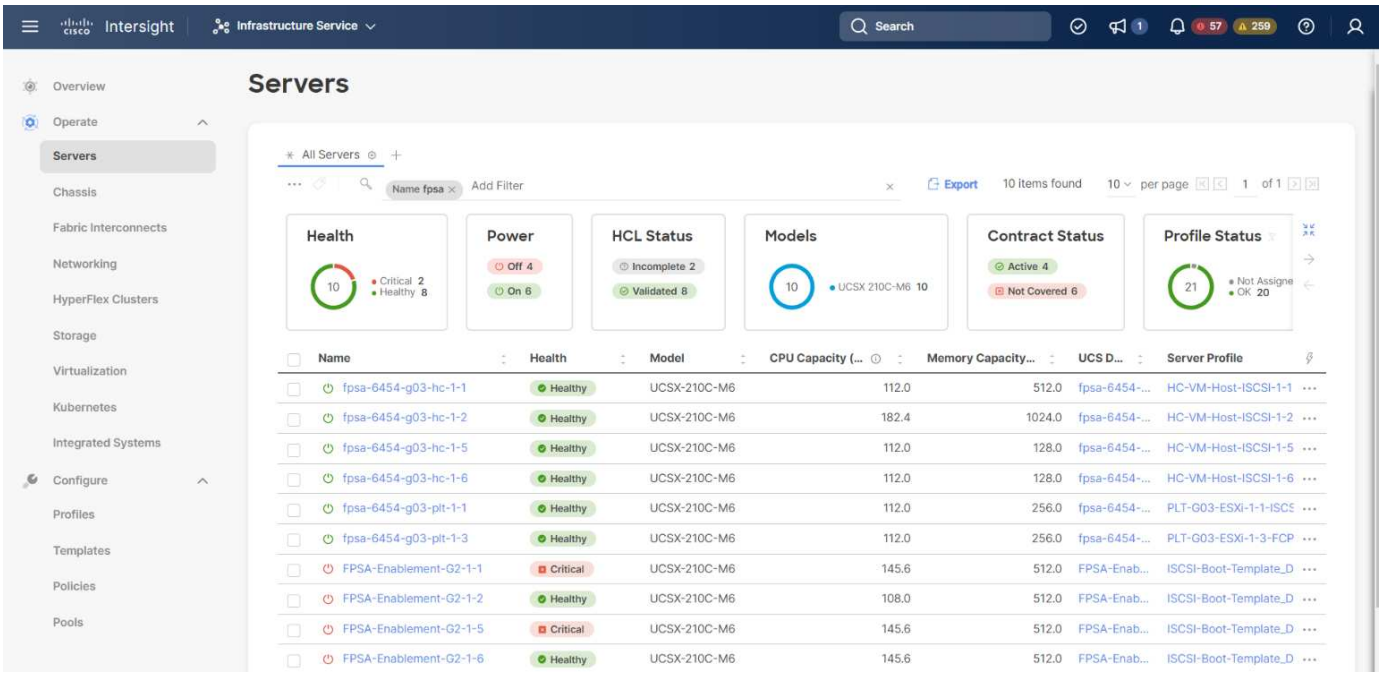
자세한 내용은 다음을 참조하세요. "Active IQ Unified Manager".

Cisco Intersight를 참조하십시오

Cisco Intersight는 기존 및 클라우드 네이티브 애플리케이션과 인프라에 대한 지능형 자동화, 관찰 가능성 및 최적화를 제공하는 SaaS 플랫폼입니다. 이 플랫폼은 IT 팀의 변화를 주도하는 데 도움이 되며 하이브리드 클라우드용으로 설계된 운영 모델을 제공합니다. Cisco Intersight는 다음과 같은 이점을 제공합니다.

- 신속한 제공.* Intersight는 민첩한 기반 소프트웨어 개발 모델로 인해 자주 업데이트되고 지속적인 혁신을 통해 클라우드 또는 고객의 데이터 센터에서 서비스로 제공됩니다. 따라서 고객은 중요한 비즈니스 요구를 지원하는 데 집중할 수 있습니다.
- * 운영 간소화. * Intersight는 공통 인벤토리, 인증 및 API가 포함된 안전한 단일 툴을 사용하여 운영을 간소화함으로써 전체 스택 및 모든 위치에서 작업을 수행할 수 있으므로 팀 간의 사일로를 제거할 수 있습니다. 이를 통해 온프레미스 물리적 서버와 하이퍼바이저를 VM, K8s, 서버리스, 자동화 등으로 관리할 수 있습니다. 사내 및 퍼블릭 클라우드 모두에서 최적화 및 비용 제어
- 지속적인 최적화**.** Cisco Intersight가 제공하는 인텔리전스를 사용하여 Cisco TAC뿐만 아니라 모든 계층에서 환경을 지속적으로 최적화할 수 있습니다. 이 인텔리전스는 권장 및 자동화 작업으로 변환되므로 워크로드 이동, 물리적 서버 상태 모니터링, 함께 작동하는 퍼블릭 클라우드의 비용 절감 권장 사항에 이르기까지 모든 변화에 실시간으로 대응할 수 있습니다.

Cisco Intersight를 사용하면 UCSM 관리 모드(UMM)와 Intersight 관리 모드(IMM)의 두 가지 관리 작업 모드를 사용할 수 있습니다. 패브릭 상호 연결의 초기 설정 중에 패브릭 연결 Cisco UCS 시스템에 대한 네이티브 UCSM 관리 모드(UMM) 또는 Intersight 관리 모드(IMM)를 선택할 수 있습니다. 이 솔루션에서는 네이티브 IMM이 사용됩니다. 다음 그림에서는 Cisco Intersight 대시보드를 보여 줍니다.



VMware vSphere 7.0

VMware vSphere는 CPU, 스토리지 및 네트워킹을 비롯한 대규모 인프라스트럭처 모음을 원활하고 다재다능하며 동적인 운영 환경으로 포괄적으로 관리할 수 있는 가상화 플랫폼입니다. 개별 시스템을 관리하는 기존 운영 체제와 달리 VMware vSphere는 전체 데이터 센터의 인프라를 통합하여 필요한 애플리케이션에 빠르고 동적으로 할당할 수 있는 리소스를 갖춘 강력한 단일 리소스를 생성합니다.

VMware vSphere 및 해당 구성 요소에 대한 자세한 내용은 다음을 참조하세요."VMware vSphere를 참조하십시오" .

VMware vCenter Server를 참조하십시오

VMware vCenter Server는 단일 콘솔에서 모든 호스트와 VM을 통합 관리하고 클러스터, 호스트 및 VM의 성능 모니터링을 통합합니다. VMware vCenter Server를 통해 관리자는 컴퓨팅 클러스터, 호스트, VM, 스토리지, 게스트 OS, 가상 인프라스트럭처의 기타 주요 구성 요소 VMware vCenter는 VMware vSphere 환경에서 사용할 수 있는 다양한 기능을 관리합니다.

자세한 내용은 다음을 참조하세요."VMware vCenter를 참조하십시오" .

하드웨어 및 소프트웨어 개정

이 하이브리드 클라우드 솔루션은 정의된 대로 지원되는 소프트웨어, 펌웨어 및 하드웨어 버전을 실행하는 모든 FlexPod 환경으로 확장될 수 있습니다."NetApp 상호 운용성 매트릭스 툴" ,"UCS 하드웨어 및 소프트웨어 호환성" , 그리고"VMware 호환성 가이드 를 참조하십시오" .

다음 표에는 사내 FlexPod 하드웨어 및 소프트웨어 개정 버전이 나와 있습니다.

구성 요소	제품	버전
컴퓨팅	Cisco UCS X210c M6	5.0(1b)
	Cisco UCS Fabric 인터커넥트 6454	4.2(2a)
네트워크	Cisco Nexus 9336C-FX2 NX-OS	9.3(9)
스토리지	NetApp AFF A400	ONTAP 9.11.1P2
	VMware vSphere용 NetApp ONTAP 툴	9.11
	VMware VAAI용 NetApp NFS 플러그인	2.0
	NetApp Active IQ Unified Manager를 참조하십시오	9.11P1
소프트웨어	VMware vSphere를 참조하십시오	7.0(U3)
	VMware ESXi nenic 이더넷 드라이버	1.0.35.0
	VMware vCenter 어플라이언스	7.0.3
	Cisco Intersight Assist 가상 어플라이언스	1.0.9-342

다음 표는 Console 및 Cloud Volumes ONTAP 버전을 보여줍니다.

공급업체	제품	버전
넷엡	콘솔	3.9.24
	Cloud Volumes ONTAP	ONTAP 9.11

"다음: 설치 및 구성"

설치 및 구성

"이전: 솔루션 구성 요소."

NetApp Cloud Volumes ONTAP 구축

Cloud Volumes ONTAP 인스턴스를 구성하려면 다음 단계를 수행하십시오.

1. 퍼블릭 클라우드 서비스 공급자 환경을 준비합니다.

   솔루션 구성을 위해 퍼블릭 클라우드 서비스 공급자의 환경 세부 정보를 수집해야 합니다. 예를 들어, AWS(Amazon Web Services) 환경을 준비하기 위해서는 AWS 액세스 키, AWS 암호 키, 지역, VPC, 서브넷 등과 같은 기타 네트워크 세부 정보가 필요합니다.

2. VPC 엔드포인트 게이트웨이를 구성합니다.

   VPC와 AWS S3 서비스 간의 연결을 활성화하려면 VPC 엔드 포인트 게이트웨이가 필요합니다. 이 기능은 게이트웨이 유형의 엔드포인트입니다. CVO에서 백업을 활성화하는 데 사용됩니다.

3. NetApp Console 액세스합니다.

   콘솔 및 기타 클라우드 서비스에 액세스하려면 가입해야 합니다. "NetApp Console" . 콘솔 계정에서 작업 공간 및 사용자를 설정하려면 다음을 참조하세요. "NetApp Console 설정 및 관리" . 콘솔에서 직접 클라우드 공급자의 콘솔 에이전트를 배포할 수 있는 권한이 있는 계정이 필요합니다. 필요한 권한을 얻으려면 다음을 참조하세요. "NetApp Console 에 대한 권한 요약" .

4. 콘솔 에이전트를 배포합니다.

   Cloud Volume ONTAP 시스템을 추가하기 전에 콘솔 에이전트를 배포해야 합니다. 콘솔 에이전트가 없는 상태에서 첫 번째 Cloud Volumes ONTAP 시스템을 만들려고 하면 콘솔에서 메시지를 표시합니다. AWS 콘솔에서 콘솔 에이전트를 배포하려면 다음을 참조하세요. "AWS의 콘솔 에이전트 설치 옵션" .

5. AWS에서 Cloud Volumes ONTAP를 시작합니다.

   Cloud Volumes ONTAP는 단일 시스템 구성에서 실행하거나 AWS에서 HA 쌍으로 실행할 수 있습니다. "단계별 지침을 읽습니다".

   이러한 단계에 대한 자세한 내용은 를 참조하십시오 "AWS의 Cloud Volumes ONTAP 빠른 시작 가이드".

   이 솔루션에서는 AWS에 단일 노드 Cloud Volumes ONTAP 시스템을 구축했습니다.

사내 **FlexPod** 구축

FlexPod with UCS X-Series, VMware, NetApp ONTAP 설계에 대한 자세한 내용은 를 참조하십시오 "Cisco UCS X-Series 및 FlexPod 데이터 센터" 설계 가이드. 이 문서에서는 FlexPod 데이터 센터 인프라 내에 Cisco Intersight-managed UCS X-Series 플랫폼을 통합하기 위한 설계 지침을 제공합니다.

사내 FlexPod 인스턴스를 구축하는 방법은 을 참조하십시오 "제공합니다".

이 문서에서는 FlexPod 데이터 센터 인프라 내에 Cisco Intersight-managed UCS X-Series 플랫폼을 통합하기 위한 구축 지침을 제공합니다. 이 문서에서는 성공적인 구축을 위한 구성 및 모범 사례에 대해 설명합니다.

FlexPod는 UCS 관리 모드 및 Cisco Intersight 관리 모드(IMM) 모두에 배포할 수 있습니다. UCS 관리 모드에서 FlexPod를 구축하는 경우 다음을 참조하십시오 "설계 가이드" 이것입니다 "구축 가이드".

Ansible을 사용하여 인프라를 코드로 자동화하여 FlexPod 구축을 자동화할 수 있습니다. 다음은 End-to-End FlexPod 구축을 위한 GitHub 저장소에 대한 링크입니다.

- UCS 관리 모드, NetApp ONTAP 및 VMware vSphere에서 Cisco UCS와 함께 FlexPod의 Ansible 구성을 확인할 수 있습니다 "여기".
- IMM, NetApp ONTAP 및 VMware vSphere에서 Cisco UCS를 사용하는 FlexPod의 Ansible 구성을 볼 수 있습니다 "여기".

사내 **ONTAP** 스토리지 구성

이 섹션에서는 이 솔루션과 관련된 몇 가지 중요한 ONTAP 구성 단계에 대해 설명합니다.

1. iSCSI 서비스가 실행 중인 SVM을 구성합니다.

```
1. vserver create -vserver Healthcare_SVM -rootvolume
Healthcare_SVM_root -aggregate aggr1_A400_G0312_01 -rootvolume-security
-style unix
2. vserver add-protocols -vserver Healthcare_SVM -protocols iscsi
3. vserver iscsi create -vserver Healthcare_SVM

   To verify:

   A400-G0312::> vserver iscsi show -vserver Healthcare_SVM
   Vserver: Healthcare_SVM
   Target Name:
   iqn.1992-08.com.netapp:sn.1fbf00f438c111ed866cd039ea91fb56:vs.3
   Target Alias: Healthcare_SVM
   Administrative Status: up
```

   클러스터 구성 중에 iSCSI 라이센스가 설치되지 않은 경우 iSCSI 서비스를 생성하기 전에 라이센스를 설치해야 합니다.

2. FlexVol 볼륨을 생성합니다.

```
1. volume create -vserver Healthcare_SVM -volume hc_iscsi_vol -aggregate
aggr1_A400_G0312_01 -size 500GB -state online -policy default -space
guarantee none
```

3. iSCSI 액세스를 위한 인터페이스를 추가합니다.

```
1. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01a
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node01-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
2. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01b
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node01-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> -status-admin up
3. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02a
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node02-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
4. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02b
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node02-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> -status-admin up
```

이 솔루션에서 NetApp은 각 노드에 2개씩 총 4개의 iSCSI 논리 인터페이스(LIF)를 생성했습니다.

FlexPod 인스턴스가 실행되고 vCenter가 배포되고 모든 ESXi 호스트가 추가된 후에는 NetApp ONTAP 스토리지에 연결 및 액세스하는 서버 역할을 하는 Linux VM을 구축해야 합니다. 이 솔루션에서는 vCenter에 CentOS 8 인스턴스를 설치했습니다.

4. LUN을 생성합니다.

```
1. lun create -vserver Healthcare_SVM -path /vol/hc_iscsi_vol/iscsi_lun1
-size 200GB -ostype linux -space-reserve disabled
```

EHR은 저널 및 애플리케이션 워크로드, EHR 운영 데이터베이스(ODB)의 경우 서버에 iSCSI LUN으로 스토리지를 제공할 것을 권장합니다. 또한 NetApp은 성능을 향상하는 AIX 버전과 RHEL 운영 체제 버전이 있는 경우 FCP 및 NVMe/FC의 사용을 지원합니다. FCP 및 NVMe/FC는 동일한 패브릭에서 공존할 수 있습니다.

5. igroup 작성

```
1. igroup create -vserver Healthcare_SVM -igroup ehr -protocol iscsi
-ostype linux -initiator iqn.1994-05.com.redhat:8e91e9769336
```

Igroup은 서버가 LUN에 액세스할 수 있도록 하는 데 사용됩니다. Linux 호스트의 경우 서버 IQN을 파일에서 찾을 수 있습니다 `/etc/iscsi/initiatorname.iscsi`.

6. LUN을 igroup에 매핑합니다.

```
1. lun mapping create -vserver Healthcare_SVM -path
/vol/hc_iscsi_vol/iscsi_lun1 -igroup ehr -lun-id 0
```

NetApp Console 에 온프레미스 **FlexPod** 스토리지 추가

콘솔을 사용하여 FlexPod 스토리지를 시스템에 추가하려면 다음 단계를 완료하세요.

1. 탐색 메뉴에서 저장소 > *시스템*을 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 *온프레미스*를 선택합니다.
3. On-Premises ONTAP * 를 선택합니다. 다음 * 을 클릭합니다.
4. ONTAP 클러스터 세부 정보 페이지에서 클러스터 관리 IP 주소와 admin 사용자 계정의 암호를 입력합니다. 그런 다음 * 추가 * 를 클릭합니다.
5. 세부 정보 및 자격 증명 페이지에서 작업 환경의 이름과 설명을 입력한 다음 * GO * 를 클릭합니다.

   콘솔은 ONTAP 클러스터를 검색하고 시스템 페이지에 시스템으로 추가합니다.

자세한 내용은 페이지를 참조하십시오 "사내 ONTAP 클러스터에 대해 알아보십시오".

"다음: SAN 구성."

SAN 구성

"이전: 설치 및 구성."

이 섹션에서는 EHR이 소프트웨어를 NetApp 스토리지와 가장 완벽하게 통합하도록 지원하는 데 필요한 호스트 측 구성에 대해 설명합니다. 이 부문에서는 Linux 운영 체제용 호스트 통합에 대해 구체적으로 논의합니다. 를 사용합니다 "NetApp 상호 운용성 매트릭스 툴(IMT)" 소프트웨어 및 펌웨어의 모든 버전을 검증합니다.

ⓘ 다음 구성 단계는 이 솔루션에 사용된 CentOS 8 호스트에만 적용됩니다.

NetApp 호스트 유틸리티 키트

NetApp 스토리지 시스템에 접속되어 있는 호스트의 운영 체제에 NetApp Host Utility Kit(Host Utilities)를 설치하는 것이 좋습니다. 기본 Microsoft MPIO(Multipath I/O)가 지원됩니다. OS는 다중 경로에 대해 ALUA(Asymmetric Logical Unit Access)를 지원해야 합니다. Host Utilities를 설치하면 NetApp 스토리지에 대한 HBA(호스트 버스 어댑터) 설정이 구성됩니다.

NetApp Host Utilities를 다운로드할 수 있습니다 "여기". 이 솔루션에서는 호스트에 Linux Host Utilities 7.1을 설치했습니다.

```
[root@hc-cloud-secure-1 ~]# rpm -ivh netapp_linux_unified_host_utilities-
7-1.x86_64.rpm
```

ONTAP 스토리지에 대해 알아보십시오

로그인이 발생해야 할 때 iSCSI 서비스가 실행되고 있는지 확인합니다. 타겟의 특정 포털 또는 타겟의 모든 포털에 대한 로그인 모드를 설정하려면 을 사용합니다 `iscsiadm` 명령.

```
[root@hc-cloud-secure-1 ~]# rescan-scsi-bus.sh
[root@hc-cloud-secure-1 ~]# iscsiadm -m discovery -t sendtargets -p
<iscsi-lif-ip>
[root@hc-cloud-secure-1 ~]# iscsiadm -m node -L all
```

이제 를 사용할 수 있습니다 `sanlun` 호스트에 접속된 LUN에 대한 정보를 표시합니다. 호스트에서 루트로 로그인되어 있는지 확인합니다.

```
[root@hc-cloud-secure-1 ~]# sanlun lun show
controller(7mode/E-Series)/
                                      device    host              lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------------
---
Healthcare_SVM                         /dev/sdb host33  iSCSI    200g
cDOT
                       /vol/hc_iscsi_vol/iscsi_lun1

Healthcare_SVM                         /dev/sdc host34  iSCSI    200g
cDOT
                       /vol/hc_iscsi_vol/iscsi_lun1
```

다중 경로를 구성합니다

장치 매퍼 다중 경로(DM 다중 경로)는 Linux의 기본 다중 경로 유틸리티입니다. 중복 및 성능 개선에 사용할 수 있습니다. 서버와 스토리지 간의 여러 I/O 경로를 집계하거나 결합하여 OS 레벨에서 단일 디바이스를 생성합니다.

1. 시스템에서 DM 다중 경로를 설정하기 전에 시스템이 업데이트되었고 가 포함되어 있는지 확인합니다 `device-mapper-multipath` 패키지.

   ```
   [root@hc-cloud-secure-1 ~]# rpm -qa|grep multipath
   device-mapper-multipath-libs-0.8.4-31.el8.x86_64
   device-mapper-multipath-0.8.4-31.el8.x86_64
   ```

2. 구성 파일은 입니다 `/etc/multipath.conf` 파일. 아래와 같이 구성 파일을 업데이트합니다.

```
[root@hc-cloud-secure-1 ~]# cat /etc/multipath.conf
defaults {
   path_checker      readsector0
   no_path_retry      fail
}
devices {
   device {
      vendor         "NETAPP  "
      product         "LUN.*"
      no_path_retry     queue
      path_checker      tur
   }
}
```

3. 다중 경로 서비스를 활성화하고 시작합니다.

```
[root@hc-cloud-secure-1 ~]# systemctl enable multipathd.service
[root@hc-cloud-secure-1 ~]# systemctl start  multipathd.service
```

4. 로드 가능한 커널 모듈을 추가합니다 `dm-multipath` 다중 경로 서비스를 다시 시작합니다. 마지막으로 경로 다중화 상태를 확인합니다.

```
[root@hc-cloud-secure-1 ~]# modprobe -v dm-multipath
insmod /lib/modules/4.18.0-408.el8.x86_64/kernel/drivers/md/dm-
multipath.ko.xz

[root@hc-cloud-secure-1 ~]# systemctl restart multipathd.service

[root@hc-cloud-secure-1 ~]# multipath -ll
3600a09803831494c372b545a4d786278 dm-2 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 33:0:0:0 sdb 8:16 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
`- 34:0:0:0 sdc 8:32 active ready running
```

이러한 단계에 대한 자세한 내용은 을 참조하십시오 "여기".

물리적 볼륨을 생성합니다

를 사용합니다 `pvcreate` 물리적 볼륨으로 사용할 블록 디바이스를 초기화하는 명령입니다. 초기화는 파일 시스템을 포맷하는 것과 유사합니다.

```
[root@hc-cloud-secure-1 ~]# pvcreate /dev/sdb
Physical volume "/dev/sdb" successfully created.
```

볼륨 그룹을 생성합니다

하나 이상의 물리적 볼륨에서 볼륨 그룹을 생성하려면 를 사용합니다 `vgcreate` 명령. 이 명령은 이름으로 새 볼륨 그룹을 생성하고 하나 이상의 물리적 볼륨을 추가합니다.

```
[root@hc-cloud-secure-1 ~]# vgcreate datavg /dev/sdb
Volume group "datavg" successfully created.
```

를 클릭합니다 `vgdisplay` 명령을 사용하여 볼륨 그룹 속성(예: 크기, 익스텐트, 물리적 볼륨 수 등)을 고정 형식으로 표시할 수 있습니다.

```
[root@hc-cloud-secure-1 ~]# vgdisplay datavg
  --- Volume group ---
  VG Name               datavg
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  1
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                0
  Open LV               0
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               <200.00 GiB
  PE Size               4.00 MiB
  Total PE              51199
  Alloc PE / Size       0 / 0
  Free  PE / Size       51199 / <200.00 GiB
  VG UUID               C7jmI0-J0SS-Cq91-t6b4-A9xw-nTfi-RXcy28
```

논리적 볼륨을 생성합니다

논리적 볼륨을 생성할 때 볼륨 그룹을 구성하는 물리적 볼륨에서 사용 가능한 익스텐트를 사용하여 볼륨 그룹에서 논리적 볼륨이 조각됩니다.

```
[root@hc-cloud-secure-1 ~]# lvcreate - l 100%FREE -n datalv datavg
Logical volume "datalv" created.
```

이 명령은 라는 논리적 볼륨을 생성합니다 `datalv` 에서는 볼륨 그룹의 할당되지 않은 모든 공간을 사용합니다 `datavg`.

파일 시스템을 생성합니다

```
[root@hc-cloud-secure-1 ~]# mkfs.xfs -K /dev/datavg/datalv
meta-data=/dev/datavg/datalv     isize=512    agcount=4, agsize=13106944
blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=0 inobtcount=0
data     =                       bsize=4096   blocks=52427776, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=25599, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

마운트할 폴더를 만듭니다

```
[root@hc-cloud-secure-1 ~]# mkdir /file1
```

파일 시스템을 마운트합니다

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1

[root@hc-cloud-secure-1 ~]# df -k
Filesystem                1K-blocks    Used Available Use% Mounted on
devtmpfs                    8072804       0   8072804   0% /dev
tmpfs                       8103272       0   8103272   0% /dev/shm
tmpfs                       8103272    9404   8093868   1% /run
tmpfs                       8103272       0   8103272   0% /sys/fs/cgroup
/dev/mapper/cs-root        45496624 5642104  39854520  13% /
/dev/sda2                   1038336  258712    779624  25% /boot
/dev/sda1                    613184    7416    605768   2% /boot/efi
tmpfs                       1620652      12   1620640   1% /run/user/42
tmpfs                       1620652       0   1620652   0% /run/user/0
/dev/mapper/datavg-datalv 209608708 1494520 208114188   1% /file1
```

이러한 작업에 대한 자세한 내용은 페이지를 참조하십시오 "LVM 관리 및 CLI 명령".

데이터 생성

`Dgen.pl`EHR의 I/O 시뮬레이터(GenerateIO)를 위한 Perl 스크립트 데이터 생성기입니다. LUN 내부의 데이터는 EHR을 통해 생성됩니다. `Dgen.pl` 스크립트. 이 스크립트는 EHR 데이터베이스의 데이터와 유사한 데이터를 생성하도록 설계되었습니다.

```
[root@hc-cloud-secure-1 ~]# cd GenerateIO-1.17.3/

[root@hc-cloud-secure-1 GenerateIO-1.17.3]# ./dgen.pl --directory /file1
--jobs 80

[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37
dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38
dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39
dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40
dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80

[root@hc-cloud-secure-1 file1]# df -k .
Filesystem                1K-blocks  Used       Available  Use%  Mounted
on
/dev/mapper/datavg-datalv  209608708  178167156  31441552   85%   /file1
```

를 실행하는 동안 Dgen.pl 스크립트는 기본적으로 파일 시스템의 85%를 데이터 생성에 사용합니다.

사내 **ONTAP**와 **Cloud Volumes ONTAP** 간에 **SnapMirror** 복제를 구성합니다

NetApp SnapMirror는 LAN 또는 WAN을 통해 데이터를 고속으로 복제하여 가상 환경과 기존 환경 모두에서 높은 데이터 가용성과 빠른 데이터 복제를 실현할 수 있습니다. 데이터를 NetApp 스토리지 시스템에 복제하고 2차 데이터를 지속적으로 업데이트함으로써 데이터가 최신 상태로 유지되고 필요할 때마다 사용할 수 있고 외부 복제 서버가 필요하지 않습니다.

온프레미스 ONTAP 시스템과 CVO 간에 SnapMirror 복제를 구성하려면 다음 단계를 완료하십시오.

1. 탐색 메뉴에서 저장소 > *시스템*을 선택합니다.
2. 시스템에서 소스 볼륨이 포함된 시스템을 선택하고 볼륨을 복제할 시스템으로 끌어온 다음 *복제*를 선택합니다.

   나머지 단계에서는 Cloud Volumes ONTAP와 온프레미스 ONTAP 클러스터 간에 동기식 관계를 만드는 방법을 설명합니다.

3. * 소스 및 대상 피어링 설정 * 이 페이지가 나타나면 클러스터 피어 관계에 대한 모든 인터클러스터 LIF를 선택합니다.
4. * 소스 볼륨 선택. * 복제할 볼륨을 선택합니다.
5. * 대상 디스크 유형 및 계층화. * 타겟이 Cloud Volumes ONTAP 시스템인 경우 대상 디스크 유형을 선택하고 데이터 계층화 활성화 여부를 선택합니다.
6. * 대상 볼륨 이름: * 대상 볼륨 이름을 지정하고 대상 애그리게이트를 선택합니다. 대상이 ONTAP 클러스터인 경우 대상 스토리지 VM도 지정해야 합니다.
7. * 최대 전송 속도. * 데이터를 전송할 수 있는 최대 속도(초당 메가바이트)를 지정합니다.
8. * 복제 정책. * 기본 정책을 선택하거나 * 추가 정책 * 을 클릭한 다음 고급 정책 중 하나를 선택합니다. 도움이 필요한 경우 "복제 정책에 대해 자세히 알아보십시오".
9. 별표. * 1회 복사 또는 반복 일정을 선택합니다. 몇 가지 기본 스케줄을 사용할 수 있습니다. 다른 일정을 사용하려면 에서 새 일정을 만들어야 합니다 `destination cluster` System Manager 사용:
10. * 검토. * 선택 사항을 검토하고 * Go * 를 클릭합니다.

이러한 구성 단계에 대한 자세한 내용은 을 참조하십시오 "여기".

콘솔이 데이터 복제 프로세스를 시작합니다. 이 단계에서는 온프레미스 ONTAP 시스템과 Cloud Volumes ONTAP 사이에 설정된 복제 서비스를 볼 수 있습니다.

Cloud Volumes ONTAP 클러스터에서 새로 생성된 볼륨을 볼 수 있습니다.

또한, 온프레미스 볼륨과 클라우드 볼륨 사이에 SnapMirror 관계가 설정되어 있는지 확인할 수도 있습니다.

복제 작업에 대한 자세한 내용은 * Replication * 탭에서 확인할 수 있습니다.

"다음: 솔루션 검증."

솔루션 검증

"이전: SAN 구성."

이 섹션에서는 몇 가지 솔루션 사용 사례를 검토합니다.

- SnapMirror의 주요 사용 사례 중 하나는 데이터 백업입니다. SnapMirror는 동일한 클러스터 내에서 또는 원격 타겟에 데이터를 복제하여 기본 백업 툴로 사용할 수 있습니다.
- DR 환경을 사용하여 애플리케이션 개발 테스트(개발/테스트) 실행
- 운영 환경에서 재해가 발생할 경우 DR을 수행합니다.
- 데이터 배포 및 원격 데이터 액세스

특히, 이 솔루션에서 검증된 비교적 소수의 사용 사례는 SnapMirror 복제의 전체 기능을 나타내지 않습니다.

애플리케이션 개발 및 테스트(개발/테스트)

애플리케이션의 개발 속도를 높이기 위해 DR 사이트에서 복제된 데이터를 신속하게 클론 복제하여 개발/테스트 애플리케이션에 사용할 수 있습니다. DR 및 개발/테스트 환경의 코로케이션을 통해 백업 또는 DR 시설의 활용률을 대폭 개선할 수 있으며, 온디맨드 개발/테스트 클론을 통해 운영으로 더 빠르게 전환하기 위해 필요한 수만큼의 데이터 복사본을 제공할 수 있습니다.

NetApp FlexClone 기술을 사용하면 보조 복사본에 대한 읽기-쓰기 액세스를 통해 모든 운영 데이터를 사용할 수 있는지 확인할 때 SnapMirror 대상 FlexVol 볼륨의 읽기-쓰기 복사본을 빠르게 만들 수 있습니다.

DR 환경을 사용하여 애플리케이션 개발/테스트를 수행하려면 다음 단계를 완료하십시오.

1. 운영 데이터의 복제본을 만듭니다. 이렇게 하려면 사내 볼륨의 애플리케이션 스냅샷을 수행합니다. 애플리케이션 스냅샷 생성은 3단계로 구성됩니다. `Lock`, `Snap`, 및 `Unlock`.

   a. 입출력이 일시 중단되고 애플리케이션이 정합성을 유지하도록 파일 시스템을 일시 중지합니다. C 단계에서 unquiesce 명령이 실행될 때까지 파일 시스템에 대한 모든 애플리케이션 쓰기는 대기 상태로 유지됩니다 단계 a, b 및 c는 투명한 프로세스 또는 애플리케이션 SLA에 영향을 주지 않는 워크플로우를 통해 실행됩니다.

   ```
   [root@hc-cloud-secure-1 ~]# fsfreeze -f /file1
   ```

   이 옵션은 지정된 파일 시스템을 새 수정에서 동결하도록 요청합니다. 파일 시스템이 언동결될 때까지 파일 시스템에 쓰기 시도하는 모든 프로세스가 차단됩니다.

   b. 온프레미스 볼륨의 스냅샷을 생성합니다.

   ```
   A400-G0312::> snapshot create -vserver Healthcare_SVM -volume
   hc_iscsi_vol -snapshot kamini
   ```

   c. 파일 시스템 중지를 해제하고 입출력을 다시 시작합니다

   ```
   [root@hc-cloud-secure-1 ~]# fsfreeze -u /file1
   ```

   이 옵션은 파일 시스템의 중지를 해제하고 작업을 계속 진행하는 데 사용됩니다. 고정으로 차단된 파일 시스템 수정은 차단되지 않으며 완료될 수 있습니다.

   위에 설명한 SnapCenter의 일부로 워크플로우를 완벽하게 오케스트레이션한 NetApp SnapCenter를 사용하여 애플리케이션 정합성을 보장하는 스냅샷을 수행할 수도 있습니다. 자세한 내용은 을 참조하십시오 "여기".

2. 운영 시스템과 DR 시스템이 동기화된 상태로 유지되도록 SnapMirror 업데이트 작업을 수행합니다.

   ```
   singlecvoaws::> snapmirror update -destination-path
   svm_singlecvoaws:hc_iscsi_vol_copy -source-path
   Healthcare_SVM:hc_iscsi_vol

   Operation is queued: snapmirror update of destination
   "svm_singlecvoaws:hc_iscsi_vol_copy".
   ```

   SnapMirror 업데이트는 복제 탭 아래의 NetApp Console GUI를 통해서도 수행할 수 있습니다.

3. 이전에 생성한 애플리케이션 스냅샷을 기반으로 FlexClone 인스턴스를 생성합니다.

```
singlecvoaws::> volume clone create -flexclone kamini_clone -type RW
-parent-vserver svm_singlecvoaws -parent-volume hc_iscsi_vol_copy
-junction-active true -foreground true -parent-snapshot kamini

[Job 996] Job succeeded: Successful
```

이전 작업의 경우 새 스냅샷을 생성할 수도 있지만 애플리케이션 정합성을 보장하기 위해 위와 동일한 단계를 따라야 합니다.

4. FlexClone 볼륨을 활성화하여 클라우드에서 EHR 인스턴스를 가져오십시오.

```
singlecvoaws::> lun mapping create -vserver svm_singlecvoaws -path
/vol/kamini_clone/iscsi_lun1 -igroup ehr-igroup -lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                    Igroup    LUN ID
Protocol
---------- -------------- --------------- -----  --------   ------
---------
svm_singlecvoaws
                 /vol/kamini_clone/iscsi_lun1    ehr-igroup   0    iscsi
```

5. 클라우드의 EHR 인스턴스에서 다음 명령을 실행하여 데이터 또는 파일 시스템에 액세스합니다.
   a. ONTAP 스토리지에 대해 알아보십시오. 다중 경로 상태를 확인합니다.

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show

Output:
controller(7mode/E-Series)/         device    host              lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                    /vol/kamini_clone/iscsi_lun1
sudo multipath -ll

Output:
3600a09806631755a452b543041313053 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

b. 볼륨 그룹을 활성화합니다.

```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

c. 파일 시스템을 마운트하고 파일 시스템 정보 요약을 표시합니다.

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                1K-blocks  Used     Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708 183987096  25621612  88%
/file1
```

이를 통해 애플리케이션 개발/테스트에 DR 환경을 사용할 수 있는지 검증합니다. DR 스토리지에서 애플리케이션 개발/테스트를 수행하면 리소스가 더 많이 사용되지 않을 수 있으며, 그렇지 않을 경우 많은

시간이 유휴 상태로 낭비될 수 있습니다.

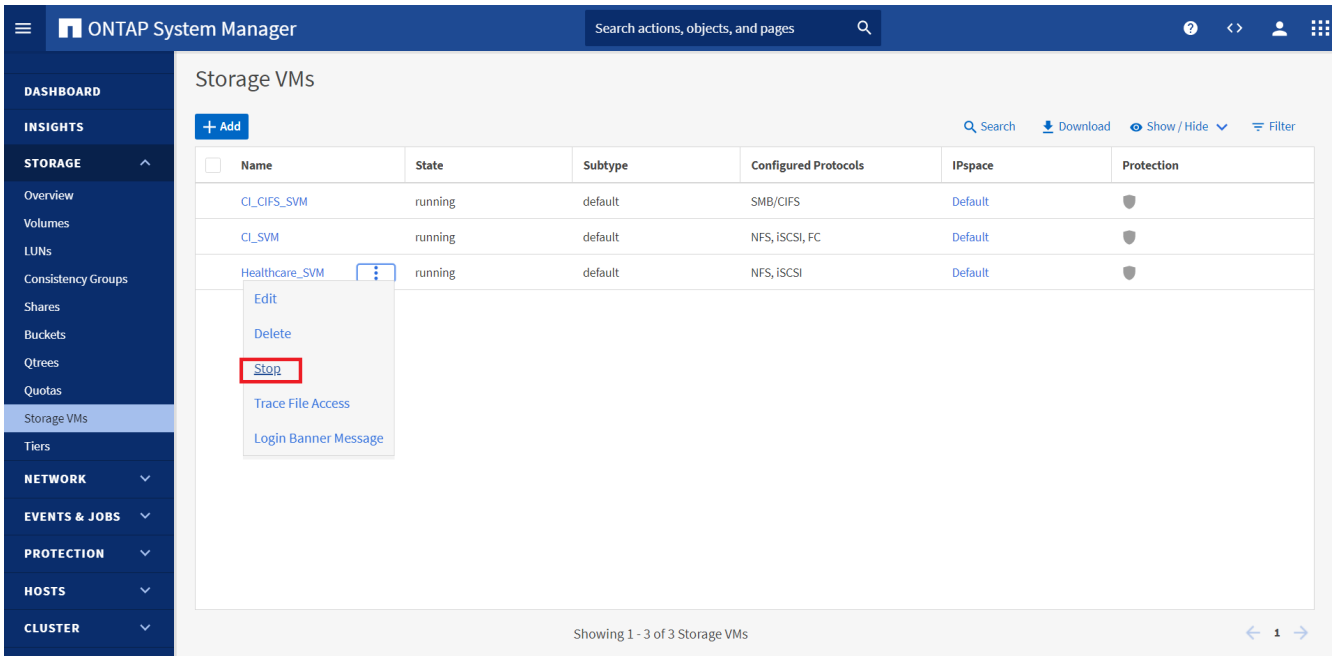
재해 복구

SnapMirror 기술은 DR 계획의 일부로도 사용됩니다. 중요한 데이터가 다른 물리적 위치에 복제되는 경우 심각한 재해로 인해 비즈니스 크리티컬 애플리케이션에서 장시간 데이터를 사용할 수 없게 될 필요가 없습니다. 클라이언트는 운영 사이트의 손상, 실수로 인한 삭제, 자연 재해 등으로부터 복구할 때까지 네트워크를 통해 복제된 데이터에 액세스할 수 있습니다.

기본 사이트로 페일백할 경우 SnapMirror는 SnapMirror 관계를 반대로 전환하여 DR 사이트를 운영 사이트와 재동기화하여 변경된 데이터 또는 새 데이터만 DR 사이트의 운영 사이트로 다시 전송합니다. 기본 운영 사이트에서 정상적인 애플리케이션 운영을 재개한 후 SnapMirror는 기본 전송을 다시 수행하지 않고도 DR 사이트로 계속 전송합니다.

성공적인 DR 시나리오의 검증을 수행하려면 다음 단계를 수행하십시오.

1. 사내 ONTAP 볼륨을 호스팅하는 SVM을 중지하여 소스(운영) 측에서 재해 상황을 시뮬레이션합니다 (`hc_iscsi_vol`)를 클릭합니다.



잦은 애플리케이션 스냅샷을 생성할 수 있도록 FlexPod 인스턴스의 온프레미스 ONTAP와 AWS의 Cloud Volumes ONTAP 간에 SnapMirror 복제가 이미 설정되어 있는지 확인하십시오.

SVM이 중지된 후 `hc_iscsi_vol` 볼륨이 콘솔에 표시되지 않습니다.

2. CVO에서 DR을 활성화합니다.

   a. 온프레미스 ONTAP와 Cloud Volumes ONTAP 간의 SnapMirror 복제 관계를 깨뜨려 CVO 타겟 볼륨을 홍보하십시오 (`hc_iscsi_vol_copy`)를 프로덕션 환경으로 이동합니다.

      SnapMirror 관계가 손상되면 타겟 볼륨 유형이 데이터 보호(DP)에서 읽기/쓰기(RW)로 변경됩니다.

```
singlecvoaws::> volume show -volume hc_iscsi_vol_copy -fields typev
server          volume            type
--------------- ----------------- ----
svm_singlecvoaws hc_iscsi_vol_copy RW
```

b. Cloud Volumes ONTAP에서 대상 볼륨을 활성화하여 클라우드의 EC2 인스턴스에서 EHR 인스턴스를 불러옵니다.

```
singlecvoaws::> lun mapping create -vserver svm_singlecvoaws -path
/vol/hc_iscsi_vol_copy/iscsi_lun1 -igroup ehr-igroup -lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                    Igroup   LUN ID
Protocol
---------- ----------------------------------  --------  ------
---------
svm_singlecvoaws
            /vol/hc_iscsi_vol_copy/iscsi_lun1  ehr-igroup  0    iscsi
```

c. 클라우드의 EHR 인스턴스에서 데이터 및 파일 시스템에 액세스하려면 먼저 ONTAP 스토리지를 검색하고 경로 다중화 상태를 확인하십시오.

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show
Output:
controller(7mode/E-Series)/         device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                  /vol/hc_iscsi_vol_copy/iscsi_lun1
sudo multipath -ll
Output:
3600a09806631755a452b543041313051 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

d. 그런 다음 볼륨 그룹을 활성화합니다.

```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

e. 마지막으로 파일 시스템을 마운트하고 파일 시스템 정보를 표시합니다.

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                 1K-blocks  Used      Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708  183987096  25621612  88%
/file1
```

이 출력은 사용자가 운영 사이트를 재해에서 복구할 때까지 네트워크를 통해 복제된 데이터에 액세스할 수 있음을 보여 줍니다.

f. SnapMirror 관계를 반대로 설정합니다. 이 작업을 수행하면 소스 볼륨과 대상 볼륨의 역할이 반전됩니다.

이 작업을 수행하면 원본 소스 볼륨의 내용이 대상 볼륨의 컨텐츠로 덮어쓰여집니다. 이 기능은 오프라인 상태인 소스 볼륨을 다시 활성화하려는 경우에 유용합니다.

이제 CVO 볼륨이 됩니다 (`hc_iscsi_vol_copy`)가 소스 볼륨이 되고 온-프레미스 볼륨이 됩니다 (`hc_iscsi_vol`)가 대상 볼륨이 됩니다.

마지막 데이터 복제와 소스 볼륨이 비활성화된 시간 사이에 원본 소스 볼륨에 기록된 데이터는 보존되지 않습니다.

a. CVO 볼륨에 대한 쓰기 액세스를 확인하려면 클라우드의 EHR 인스턴스에서 새 파일을 생성하십시오.

```
cd /file1/
sudo touch newfile
```

운영 사이트가 다운되어도 클라이언트는 계속 데이터에 액세스할 수 있으며 이제 소스 볼륨인 Cloud Volumes ONTAP 볼륨에 대한 쓰기를 수행할 수도 있습니다.

기본 사이트로 페일백할 경우 SnapMirror는 SnapMirror 관계를 반대로 전환하여 DR 사이트를 운영 사이트와 재동기화하여 변경된 데이터 또는 새 데이터만 DR 사이트의 운영 사이트로 다시 전송합니다. 기본 운영 사이트에서 정상적인 애플리케이션 운영을 재개한 후 SnapMirror는 기본 전송을 다시 수행하지 않고도 DR 사이트로 계속 전송합니다.

이 섹션에서는 운영 사이트가 재해에 의해 적중될 때 DR 시나리오의 성공적인 해결을 보여 줍니다. 이제 소스 사이트가 복구를 수행하는 동안 클라이언트에 제공할 수 있는 애플리케이션에서 데이터를 안전하게 사용할 수 있습니다.

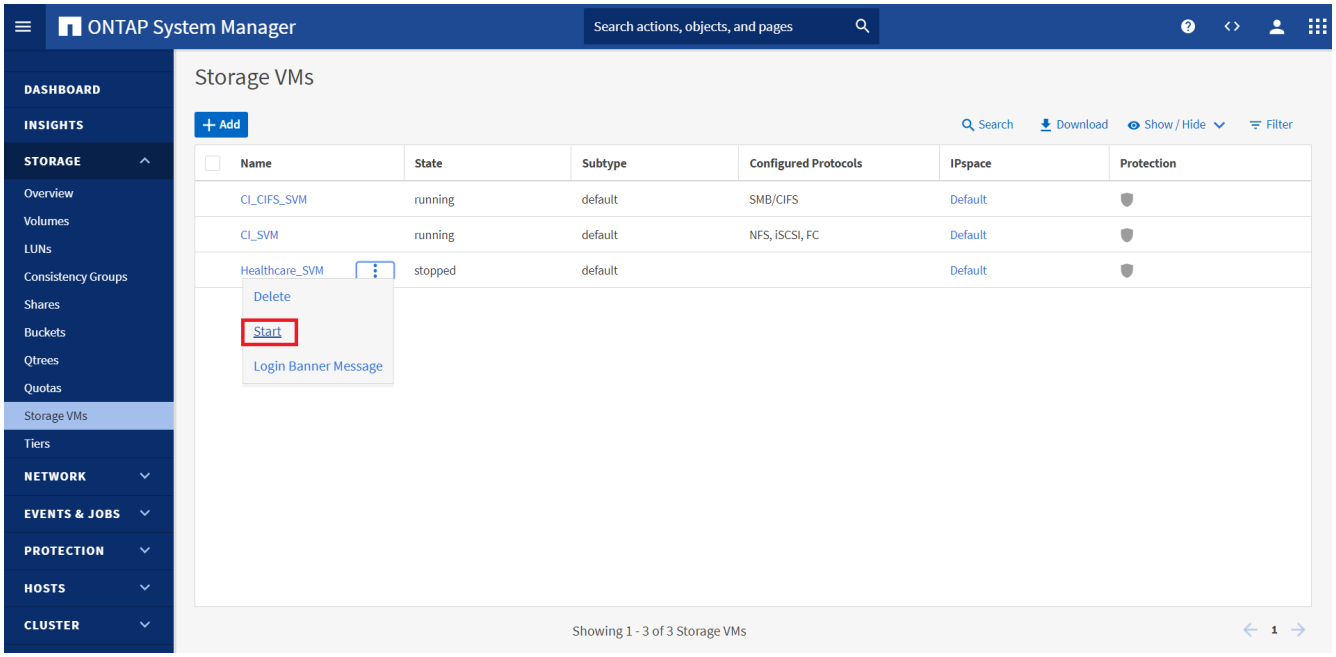
운영 사이트에서 데이터 검증

운영 사이트가 복구된 후에는 원래 구성이 복원되고 클라이언트가 소스 사이트의 데이터에 액세스할 수 있는지 확인해야 합니다.

이 섹션에서는 소스 사이트를 방문하여 사내 ONTAP와 Cloud Volumes ONTAP 간의 SnapMirror 관계를 복원하고, 마지막으로 소스 엔드에서 데이터 무결성 검사를 수행하는 방법에 대해 설명합니다

다음 절차를 사용하여 운영 사이트의 데이터를 확인할 수 있습니다.

1. 이제 소스 사이트가 작동 중인지 확인하십시오. 그렇게 하려면 사내 ONTAP 볼륨을 호스팅하는 SVM을 시작하십시오 (`hc_iscsi_vol`)를 클릭합니다.



2. Cloud Volumes ONTAP와 온프레미스 ONTAP 간의 SnapMirror 복제 관계를 깨뜨려 온프레미스 볼륨을 홍보하십시오 (`hc_iscsi_vol`) 프로덕션 환경으로 돌아갑니다.

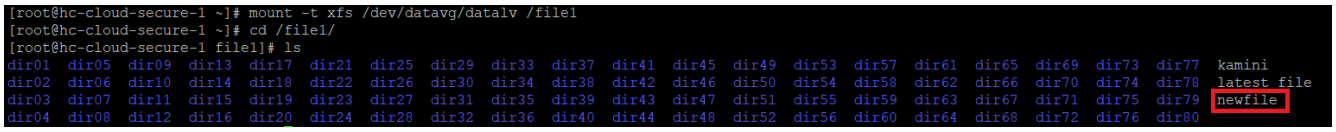
   SnapMirror 관계가 손상되면 사내 볼륨 유형이 데이터 보호(DP)에서 읽기/쓰기(RW)로 변경됩니다.

```
A400-G0312::> volume show -volume hc_iscsi_vol -fields type
vserver         volume       type
--------------- ------------ ----
Healthcare_SVM hc_iscsi_vol RW
```

3. SnapMirror 관계를 반대로 설정합니다. 이제 사내 ONTAP 볼륨으로 이동합니다 (`hc_iscsi_vol`)는 이전 소스 볼륨과 Cloud Volumes ONTAP 볼륨이 됩니다 (`hc_iscsi_vol_copy`)가 대상 볼륨이 됩니다.

   다음 단계를 수행하여 원래 구성을 성공적으로 복원했습니다.

4. 온프레미스 EHR 인스턴스를 재부팅합니다. 파일 시스템을 마운트하고 가 올바른지 확인합니다 `newfile` 생산이 중단되었을 때 클라우드의 EHR 인스턴스에서 생성한도 여기에 존재합니다.



소스에서 대상으로 데이터 복제가 성공적으로 완료되었으며 데이터 무결성이 유지되었음을 유추할 수 있습니다. 그러면 운영 사이트에서 데이터 검증이 완료됩니다.

"다음: 결론."

결론

"이전: 솔루션 검증."

하이브리드 클라우드 구축은 대부분의 의료 조직에서 언제든지 데이터 가용성을 제공하는 데 목표를 두고 있습니다. 이 솔루션에서는 Cloud Volumes ONTAP 기반의 FlexPod 하이브리드 클라우드 솔루션을 구축하고, NetApp SnapMirror 복제 기술을 활용하여 일부 사용 사례를 검증함으로써 의료 애플리케이션과 워크로드를 백업 및 복구했습니다.

FlexPod는 Cisco와 NetApp의 전략적 파트너십을 통해 엄격한 테스트와 검증을 거친 통합 인프라로서 예측 가능한 낮은 지연 시간의 시스템 성능과 고가용성을 제공하도록 설계되었습니다. 이 접근 방식은 EHR 시스템의 사용자에게 높은 편안함 수준을 제공하며 궁극적으로는 최상의 응답 시간을 제공합니다.

온프레미스 데이터 센터에서 NetApp 스토리지 기능을 실행하는 것처럼 NetApp을 사용하면 클라우드에서 EHR 운영, 재해 복구, 백업 또는 계층화를 실행할 수 있습니다. NetApp Cloud Volumes ONTAP을 통해 NetApp은 클라우드에서 EHR을 효과적으로 실행하는 데 필요한 엔터프라이즈급 기능과 성능을 제공합니다. NetApp 클라우드 옵션은 iSCSI를 통한 블록 오버와 NFS 또는 SMB를 통한 파일 오버를 제공합니다.

이 솔루션은 의료 조직의 요구사항을 충족하여 디지털 혁신을 위한 조치를 취할 수 있도록 합니다. 또한 애플리케이션 및 워크로드를 효율적으로 관리하는 데도 도움이 됩니다.

"다음: 추가 정보를 찾을 위치."

추가 정보를 찾을 수 있는 위치

"이전: 결론."

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

- FlexPod 홈 페이지

  "https://www.flexpod.com"

- FlexPod용 Cisco Validated Design 및 구축 가이드

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- NetApp Console

  "https://console.netapp.com/"

- NetApp Cloud Volumes ONTAP를 참조하십시오

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html"

- AWS에서 Cloud Volumes ONTAP를 빠르게 시작합니다

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html"

- SnapMirror 복제

  "https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html"

- TR-3928: Epic을 위한 NetApp 모범 사례

  https://www.netapp.com/pdf.html?item=/media/17137-tr3928pdf.pdf

- TR-4693: Epic EHR용 FlexPod 데이터 센터 구축 가이드

  "https://www.netapp.com/media/10658-tr-4693.pdf"

- Epic을 위한 FlexPod

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmw_epic.html"

- NetApp 상호 운용성 매트릭스 툴

  "http://support.netapp.com/matrix/"

- Cisco UCS 하드웨어 및 소프트웨어 상호 운용성 툴

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- VMware 호환성 가이드 를 참조하십시오

  "http://www.vmware.com/resources/compatibility/search.php"

버전 기록

버전	날짜	문서 버전 기록
버전 1.0	2023년 3월	초기 버전

NetApp Cloud Volumes ONTAP 및 Cisco Intersight가 지원되는 Google 클라우드 플랫폼용 FlexPod 하이브리드 클라우드

TR-4939: NetApp Cloud Volumes ONTAP 및 Cisco Intersight가 지원되는 Google 클라우드 플랫폼용 FlexPod 하이브리드 클라우드

Ruchika Lahoti, NetApp

소개

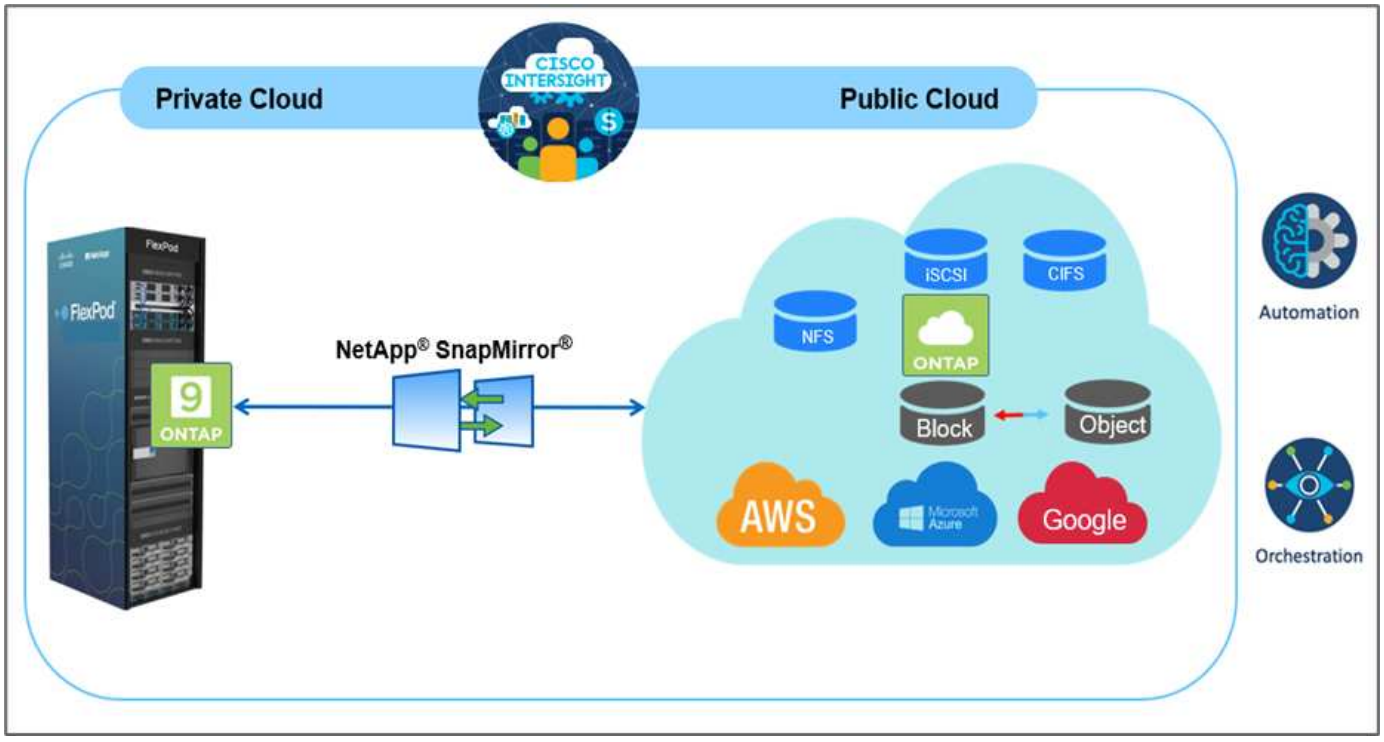
DR(재해 복구)으로 데이터를 보호하는 것은 비즈니스 연속성을 유지하는 데 있어 중요한 목표입니다. DR을 통해 조직은 비즈니스 운영을 2차 위치로 페일오버하고 나중에 복구한 후 운영 사이트로 효율적이고 안정적으로 페일백할 수 있습니다. 자연 재해, 네트워크 장애, 소프트웨어 취약성 및 인적 오류와 같은 여러 가지 우려 때문에 DR 전략을 개발하는 것이 IT의 최우선 과제가 됩니다.

DR의 경우 기본 사이트에서 실행 중인 모든 워크로드를 DR 사이트에서 충실히 복제해야 합니다. 또한 데이터베이스, 파일 서비스, NFS 및 iSCSI 스토리지 등의 모든 엔터프라이즈 데이터에 대한 최신 복사본이 조직에 있어야 합니다. 운영 환경의 데이터는 계속 업데이트되므로 변경사항을 정기적으로 DR 사이트로 전송해야 합니다.

대부분의 조직은 인프라와 사이트의 독립성 요구사항으로 인해 DR 환경을 구축하는 데 어려움을 겪고 있습니다. 필요한 리소스 수와 2차 데이터 센터의 설정, 테스트, 유지 관리 비용이 매우 높아서 일반적으로 전체 운영 환경의 비용이 거의 들지 않습니다. 데이터를 지속적으로 동기화하고 원활한 페일오버 및 페일백을 설정하면서 적절한 보호 기능을 통해 데이터 사용 공간을 최소화하는 것은 쉽지 않습니다. DR 사이트를 구축한 후에는 운영 환경의 데이터를 복제하고 동기화된 상태를 계속 유지해야 합니다.

이 기술 보고서에서는 FlexPod 통합 인프라 솔루션, Google Cloud의 NetApp Cloud Volumes ONTAP, DR을 위한 하이브리드 클라우드 데이터 센터를 구축하는 Cisco Intersight를 소개합니다. 이 솔루션에서는 Cisco Intersight Cloud Orchestrator를 사용하여 사내 ONTAP 워크플로우를 설계 및 실행하는 방법에 대해 논의합니다. 또한 하시코프 테르래양식용 Cisco Intersight Service를 사용하여 NetApp Cloud Volumes ONTAP를 구현하고 FlexPod와 Cloud Volumes ONTAP 간의 데이터 복제 및 DR을 조정 및 자동화하는 방법에 대해서도 설명합니다.

다음 그림에서는 솔루션 개요를 제공합니다.



이 솔루션은 다음과 같은 여러 가지 이점을 제공합니다.

- * 오케스트레이션 및 자동화 * Cisco Intersight는 자동화를 통해 제공되는 일관된 오케스트레이션 프레임워크를 제공하여 FlexPod 하이브리드 클라우드 인프라의 일상적인 운영을 단순화합니다.
- * 맞춤형 보호. * Cloud Volumes ONTAP는 증분 업데이트를 통해 ONTAP에서 클라우드로 블록 레벨 데이터 복제를 제공하여 대상을 최신 상태로 유지합니다. 사용자는 전송되는 소스의 변경 사항에 따라 5분마다 또는

1시간마다 동기화 일정을 지정할 수 있습니다.

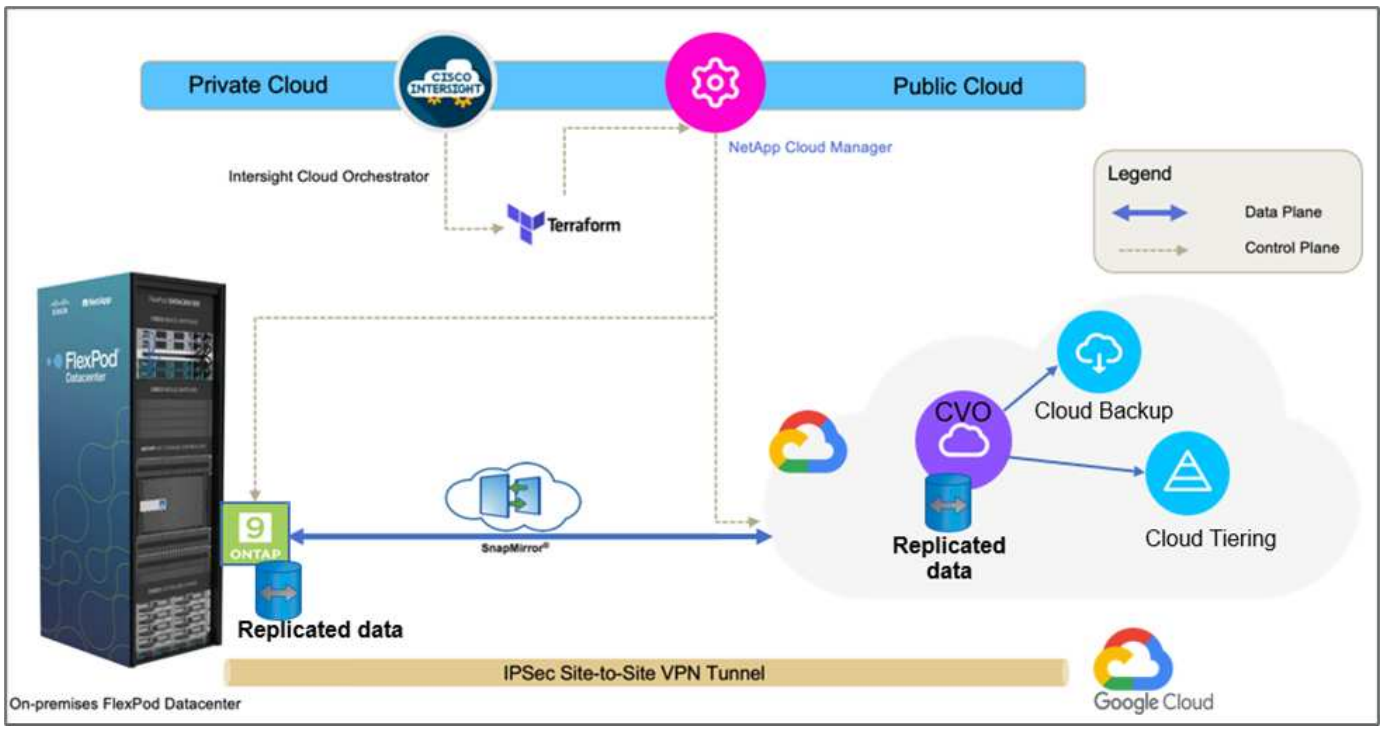
- * 원활한 페일오버 및 페일백. * 재해가 발생하면 스토리지 관리자가 클라우드 볼륨으로 빠르게 페일오버할 수 있습니다. 운영 사이트가 복구되면 DR 환경에서 생성된 새 데이터가 소스 볼륨과 다시 동기화되어 2차 데이터 복제를 다시 설정합니다.
- * 효율성: * 보조 클라우드 복사본의 스토리지 공간 및 비용은 데이터 압축, 씬 프로비저닝, 중복제거를 통해 최적화됩니다. 데이터는 압축 및 중복제거된 형태로 블록 레벨에서 전송되므로 전송 속도가 향상됩니다. 또한 데이터는 저비용 오브젝트 스토리지로 자동 계층화되며 DR 시나리오와 같은 액세스 시에만 고성능 스토리지로 돌아갑니다. 따라서 지속적으로 발생하는 스토리지 비용이 크게 절감됩니다.
- * IT 생산성 향상. * Intersight를 인프라 및 애플리케이션 라이프사이클 관리를 위한 안전한 단일 엔터프라이즈급 플랫폼으로 사용하면 솔루션의 규모에 따라 구성 관리 및 수동 작업 자동화를 간소화할 수 있습니다.

대상

이 문서의 대상에는 세일즈 엔지니어, 현장 컨설턴트, 프로페셔널 서비스, IT 매니저, IT 효율성을 제공하고 IT 혁신을 지원하는 인프라를 활용하려는 파트너 엔지니어, 사이트 안정성 엔지니어, 클라우드 설계자, 클라우드 엔지니어, 고객이 포함됩니다.

솔루션 토폴로지

이 섹션에서는 솔루션의 논리적 토폴로지를 설명합니다. 다음 그림은 사내 FlexPod 환경, Google Cloud에서 실행되는 NetApp Cloud Volumes ONTAP, Cisco Intersight 및 NetApp Cloud Manager의 솔루션 토폴로지를 나타낸 것입니다.



컨트롤 평면과 데이터 평면은 끝점 사이에 명확하게 표시됩니다. 데이터 플레인은 안전한 사이트-사이트 VPN 연결을 사용하여 FlexPod All Flash FAS에서 실행되는 ONTAP 인스턴스를 Google Cloud의 NetApp Cloud Volumes ONTAP 인스턴스에 연결합니다.

FlexPod에서 NetApp Cloud Volumes ONTAP으로 워크로드 데이터 복제를 처리하는 작업은 NetApp SnapMirror에서 처리하며, 전체 프로세스는 온프레미스 및 클라우드 환경 모두에서 Cisco Intersight Cloud Orchestrator를 사용하여 오케스트레이션합니다. Cisco Intersight Cloud Orchestrator는 NetApp Cloud Manager가

NetApp Cloud Volumes ONTAP 구축과 관련된 운영을 수행하고 데이터 복제 관계를 확립하기 위해 Terraform 리소스 공급자를 사용합니다.

이 솔루션에서는 NetApp Cloud Volumes ONTAP 인스턴스에 상주하는 콜드 데이터를 Google Cloud 스토리지에 선택적으로 백업 및 계층화할 수 있습니다.

"다음: 솔루션 구성 요소."

솔루션 구성 요소

"이전: 솔루션 개요"

FlexPod

FlexPod는 가상화된 솔루션과 가상화되지 않은 솔루션 모두를 위한 통합된 기반을 형성하는 정의된 하드웨어 및 소프트웨어 세트입니다. FlexPod에는 NetApp ONTAP 스토리지, Cisco Nexus 네트워킹, Cisco MDS 스토리지 네트워킹 및 Cisco UCS(Unified Computing System)가 포함되어 있습니다. 이 설계는 네트워킹, 컴퓨팅 및 스토리지가 하나의 데이터 센터 랙에 장착되거나 고객의 데이터 센터 설계에 따라 배포될 수 있을 만큼 유연합니다. 포트 밀도를 통해 네트워킹 구성 요소가 여러 구성을 수용할 수 있습니다.

Cisco Intersight를 참조하십시오

Cisco Intersight는 기존 및 클라우드 네이티브 애플리케이션과 인프라에 대한 지능형 자동화, 관찰 가능성 및 최적화를 제공하는 SaaS 플랫폼입니다. 이 플랫폼은 IT 팀의 변화를 주도하는 데 도움이 되며 하이브리드 클라우드용으로 설계된 운영 모델을 제공합니다. Cisco Intersight는 다음과 같은 이점을 제공합니다.

- 신속한 제공.* 민첩한 기반 소프트웨어 개발 모델로 인해 잦은 업데이트와 지속적인 혁신을 통해 클라우드 또는 고객의 데이터 센터에서 서비스로 제공됩니다. 따라서 고객은 LOB에 대한 제공 속도를 높이는 데 주력할 수 있습니다.
- * 운영 간소화. * 공통의 인벤토리, 인증 및 API가 포함된 안전한 단일 툴을 사용하여 운영을 간소화함으로써 전체 스택 및 모든 위치에서 작업을 수행할 수 있으므로 팀 간의 사일로를 제거할 수 있습니다. 사내 물리적 서버 및 하이퍼바이저 관리부터 VM, K8s, 서버리스, 자동화, 사내 및 퍼블릭 클라우드 전반에서 최적화 및 비용 제어
- * 지속적인 최적화. * Cisco Intersight가 모든 계층 및 Cisco TAC에 제공하는 인텔리전스를 사용하여 환경을 지속적으로 최적화합니다. 이 인텔리전스는 권장 및 자동화 작업으로 변환되므로 작업 부하 이동, 물리적 서버 상태 모니터링, 작업 중인 퍼블릭 클라우드 비용 절감 권장 사항 등 모든 변화에 실시간으로 대응할 수 있습니다.

Cisco Intersight를 사용하면 UCSM 관리 모드(UMM)와 Intersight 관리 모드(IMM)의 두 가지 관리 작업 모드를 사용할 수 있습니다. 패브릭 상호 연결의 초기 설정 중에 패브릭 연결 Cisco UCS 시스템에 대한 네이티브 UMM 또는 IMM을 선택할 수 있습니다. 이 솔루션에서는 네이티브 IMM이 사용됩니다.

Cisco Intersight 라이센스

Cisco Intersight는 여러 계층의 가입 기반 라이센스를 사용합니다.

Cisco Intersight 라이센스 계층은 다음과 같습니다.

- * Cisco Intersight Essentials. * 모든 기본 기능과 함께 다음 기능이 포함되어 있습니다.
  - Cisco UCS 센트럴
  - Cisco IMC 감독자 자격

- 서버 프로파일을 사용한 정책 기반 구성
- 펌웨어 관리
- 하드웨어 호환성 목록(HCL)과의 호환성 평가

- * Cisco Intersight Advantage. * Essentials 계층의 기능과 다음 기능이 포함됩니다.
  - 물리적 컴퓨팅, 네트워크, 스토리지, VMware 가상화 및 AWS 퍼블릭 클라우드에서 위젯, 인벤토리, 용량, 활용률 기능 및 도메인 간 인벤토리 상관 관계
  - 고객이 영향을 받는 엔드포인트 장치에 대한 중요한 보안 경고 및 현장 알림을 받을 수 있는 Cisco 보안 권고 서비스입니다.
- * Cisco Intersight Premier. * Cisco Intersight Premier는 Advantage 계층에서 제공되는 기능 외에도 다음과 같은 기능을 제공합니다.
  - Cisco 및 타사 컴퓨팅, 네트워크, 스토리지, 통합 시스템, 가상화, 컨테이너 및 퍼블릭 클라우드 플랫폼을 사용하고 있습니다
  - Cisco UCS Director의 전체 구독 신청은 추가 비용 없이 가능합니다.

Intersight Licensing 및 각 라이센스에서 지원되는 기능에 대한 자세한 내용은 를 참조하십시오 "여기".

> 이 솔루션에서는 가시화 클라우드 오케스트레이터 및 Intersight 서비스를 하시사테라폼에 사용합니다. 이러한 기능은 Intersight Premier 라이센스가 있는 사용자가 사용할 수 있으므로 이 라이센스 계층을 활성화해야 합니다.

ICO와의 Terraform 클라우드 통합

Cisco Intersight Cloud Orchestrator(ICO)를 사용하여 TFC(Terraform Cloud) API를 호출하는 워크플로우를 생성하고 실행할 수 있습니다. 웹 API 요청 호출 작업은 Terraform Cloud를 대상으로 지원하며 HTTP 메서드를 사용하여 Terraform Cloud API로 구성할 수 있습니다. 따라서 워크플로에서는 일반 API 작업 및 기타 작업을 사용하여 여러 Terraform Cloud API를 호출하는 작업을 조합하여 사용할 수 있습니다. ICO 기능을 사용하려면 프리미어 라이센스가 필요합니다.

Cisco Intersight Assist를 참조하십시오

Cisco Intersight Assist를 사용하면 엔드포인트 장치를 Cisco Intersight에 추가할 수 있습니다. 데이터 센터에는 Cisco Intersight와 직접 연결되지 않는 여러 장치가 있을 수 있습니다. Cisco Intersight에서 지원되지만 직접 연결되지 않는 장치는 연결 메커니즘이 필요합니다. Cisco Intersight Assist는 이러한 연결 메커니즘을 제공하며 Cisco Intersight에 장치를 추가할 수 있도록 도와줍니다.

Cisco Intersight Assist는 OVA(Open Virtual Appliance) 파일 형식에 포함된 배포 가능한 가상 머신으로 배포되는 Cisco Intersight Virtual Appliance 내에서 사용할 수 있습니다. ESXi 서버에 어플라이언스를 설치할 수 있습니다. 자세한 내용은 를 참조하십시오 "Cisco Intersight 가상 어플라이언스 시작 가이드".

Intersight Assist를 Intersight에 사용한 후 Intersight Assist 옵션을 통해 클레임 장치를 청구할 수 있습니다. 자세한 내용은 을 참조하십시오 "시작하기".

NetApp Cloud Volumes ONTAP를 참조하십시오

- 내장된 데이터 중복제거, 데이터 압축, 씬 프로비저닝 및 복제를 활용하여 스토리지 비용을 최소화합니다.
- 클라우드 환경에서 장애 발생 시에도 지속적인 운영과 엔터프라이즈급 안정성 제공
- Cloud Volumes ONTAP는 업계 최고의 복제 기술인 NetApp SnapMirror를 사용하여 온프레미스 데이터를

클라우드로 복제하므로 여러 사용 사례에서 2차 복사본을 쉽게 사용할 수 있습니다.

- Cloud Volumes ONTAP은 또한 Cloud Backup Service와 통합되어 클라우드 데이터를 보호하고 장기간 보관하기 위한 백업 및 복원 기능을 제공합니다.
- 애플리케이션을 오프라인으로 전환하지 않고도 필요에 따라 고성능 및 고성능 스토리지 풀 간에 전환할 수 있습니다.
- NetApp SnapCenter를 사용하여 스냅샷 복사본의 일관성 제공
- Cloud Volumes ONTAP는 데이터 암호화를 지원하고 바이러스 및 랜섬웨어에 대한 보호를 제공합니다.
- 클라우드 데이터 센스와 통합되어 데이터 컨텍스트를 이해하고 중요한 데이터를 식별할 수 있습니다.

Cloud Central을 참조하십시오

Cloud Central은 NetApp 클라우드 데이터 서비스에 액세스하고 이를 관리할 수 있는 중앙의 위치입니다. 이러한 서비스를 사용하여 클라우드에서 중요한 애플리케이션을 실행하고, 자동화된 DR 사이트를 생성하고, SaaS 데이터를 백업하고, 여러 클라우드 간에 데이터를 효과적으로 마이그레이션 및 제어할 수 있습니다. 자세한 내용은 을 참조하십시오 "Cloud Central을 참조하십시오".

클라우드 관리자

Cloud Manager는 엔터프라이즈급 SaaS 기반 관리 플랫폼으로, IT 전문가와 클라우드 설계자가 NetApp 클라우드 솔루션을 사용하여 하이브리드 멀티 클라우드 인프라를 중앙에서 관리할 수 있도록 지원합니다. 이 솔루션은 중앙 집중식 시스템을 통해 사내 및 클라우드 스토리지를 확인 및 관리하여 여러 하이브리드 클라우드 공급자와 계정을 지원합니다. 자세한 내용은 을 참조하십시오 "클라우드 관리자".

커넥터

Connector를 사용하면 Cloud Manager에서 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리할 수 있습니다. Connector 인스턴스는 Cloud Manager에서 제공하는 다양한 기능을 사용해야 하며 클라우드 또는 사내 네트워크에 구축할 수 있습니다. 커넥터는 다음 위치에서 지원됩니다.

- 설치하고
- Microsoft Azure를 참조하십시오
- Google 클라우드
- 온프레미스

NetApp Active IQ Unified Manager를 참조하십시오

NetApp Active IQ Unified Manager를 사용하면 재설계된 직관적인 단일 인터페이스에서 ONTAP 스토리지 클러스터를 모니터링하여 커뮤니티의 지혜 및 AI 분석을 제공할 수 있습니다. 스토리지 환경 및 스토리지 환경에서 실행되는 가상 시스템에 대한 포괄적인 운영, 성능 및 사전 예방적 통찰력을 제공합니다. 스토리지 인프라에서 문제가 발생하면 Unified Manager에서 문제의 세부 정보를 알려 근본 원인을 파악할 수 있습니다. 가상 머신 대시보드에서는 VM의 성능 통계를 볼 수 있으므로 vSphere 호스트에서 네트워크를 거쳐 마지막으로 스토리지까지 전체 입출력 경로를 조사할 수 있습니다.

일부 이벤트는 문제를 해결하기 위해 취할 수 있는 개선 조치도 제공합니다. 이벤트가 발생할 때 e-메일 및 SNMP 트랩을 통해 알림을 받도록 이벤트에 대한 사용자 지정 알림을 구성할 수 있습니다. Active IQ Unified Manager를 사용하면 용량 및 사용 추세를 예측하여 문제가 발생하기 전에 능동적으로 조치를 취함으로써 장기적인 문제를 해결할 수 있는 단기적인 의사 결정을 방지할 수 있으므로 사용자의 스토리지 요구 사항을 계획할 수 있습니다.

VMware vSphere를 참조하십시오

VMware vSphere는 CPU, 스토리지 및 네트워킹을 포함한 대규모 인프라 컬렉션을 완벽하고 다재다능한 동적 운영 환경으로 전체적으로 관리하는 가상화 플랫폼입니다. 개별 시스템을 관리하는 기존 운영 체제와 달리 VMware vSphere는 전체 데이터 센터의 인프라를 통합하여 필요한 애플리케이션에 빠르고 동적으로 할당할 수 있는 리소스를 갖춘 강력한 단일 시스템을 구축합니다.

VMware vSphere에 대한 자세한 내용은 을 참조하십시오 "이 링크".

VMware vSphere vCenter를 참조하십시오

VMware vCenter Server는 단일 콘솔에서 모든 호스트와 VM을 통합 관리하고 클러스터, 호스트 및 VM의 성능 모니터링을 통합합니다. VMware vCenter Server를 통해 관리자는 컴퓨팅 클러스터, 호스트, VM, 스토리지, 게스트 OS, 가상 인프라스트럭처의 기타 주요 구성 요소 VMware vCenter는 VMware vSphere 환경에서 사용할 수 있는 다양한 기능을 관리합니다.

하드웨어 및 소프트웨어 버전

이 하이브리드 클라우드 솔루션은 NetApp 상호 운용성 매트릭스 툴 및 Cisco UCS 하드웨어 호환성 목록에 정의된 대로 지원되는 소프트웨어, 펌웨어, 하드웨어 버전을 실행하는 FlexPod 환경으로 확장할 수 있습니다.

사내 환경의 기준 플랫폼으로 사용되는 FlexPod 솔루션은 설명된 지침과 사양에 따라 배포되었습니다 "여기".

이 환경 내의 네트워크는 ACI 기반입니다. 자세한 내용은 을 참조하십시오 "여기".

- 자세한 내용은 다음 링크를 참조하십시오.
- "NetApp 상호 운용성 매트릭스 툴"
- "VMware 호환성 가이드 를 참조하십시오"
- "Cisco UCS 하드웨어 및 소프트웨어 상호 운용성 툴"

다음 표에는 FlexPod 하드웨어 및 소프트웨어 버전이 나와 있습니다.

구성 요소	제품	버전
컴퓨팅	Cisco UCS X210C-M6	5.0(1b)
	Cisco UCS Fabric 인터커넥트 6454	4.2(2a)
네트워크	Cisco Nexus 9332C(척추)	14.2(7초)
	Cisco Nexus 9336C-FX2(리프)	14.2(7초)
	Cisco ACI를 참조하십시오	4.2(7개)
스토리지	NetApp AFF A220을 참조하십시오	9.11.1
	VMware vSphere용 NetApp ONTAP 툴	9.10
	VMware VAAI용 NetApp NFS 플러그인	2.0-15
	Active IQ Unified Manager	9.11
소프트웨어	vSphere ESXi	7.0(U3)

구성 요소	제품	버전
	VMware vCenter 어플라이언스	7.0.3
	Cisco Intersight Assist 가상 어플라이언스	1.0.11-306

Terraform 구성은 Terraform Cloud for Business 계정에서 실행됩니다. Terraform 구성에서는 NetApp Cloud Manager의 Terraform 공급자를 사용합니다.

다음 표에는 공급업체, 제품 및 버전이 나와 있습니다.

구성 요소	제품	버전
하시코프	Terraform(Terraform	1.2.7

다음 표에서는 Cloud Manager 및 Cloud Volumes ONTAP 버전을 보여 줍니다.

구성 요소	제품	버전
넷엡	Cloud Volumes ONTAP	9.11
	클라우드 관리자	3.9.21

"다음: 설치 및 구성 - FlexPod 배포"

설치 및 구성

FlexPod 구축

"이전: 솔루션 구성 요소."

설계 및 관련 모범 사례의 다양한 요소 구성을 비롯하여 FlexPod 설계 및 배포 세부 사항에 대한 자세한 내용은 을 참조하십시오 "FlexPod을 위한 Cisco 검증 설계".

FlexPod는 UCS 관리 모드와 Cisco Intersight 관리 모드 모두에서 구축할 수 있습니다. UCS 관리 모드에서 FlexPod를 구축하는 경우 최신 Cisco Validated Design을 찾을 수 있습니다 "여기".

Cisco UCS(Cisco Unified Compute System) X-Series는 클라우드에서 구성 및 관리되는 완전히 새로운 모듈식 컴퓨팅 시스템입니다. 최신 애플리케이션의 요구 사항을 충족하고 적응성이 뛰어나고 미래를 대비한 모듈식 설계를 통해 운영 효율성, 민첩성 및 확장성을 개선하도록 설계되었습니다. FlexPod 인프라 내에 Cisco Intersight-managed UCS X-Series 플랫폼을 통합하는 방법에 대한 설계 지침을 확인할 수 있습니다 "여기".

Cisco ACI 지원 FlexPod를 찾을 수 있습니다 "여기".

"다음: Cisco Intersight 구성."

Cisco Intersight 구성

"이전: FlexPod 배포."

Cisco Intersight 및 Intersight Assist를 구성하려면 찾은 FlexPod용 Cisco 검증 설계를

참조하십시오 "여기".

"다음: ICO 사전 요구 사항에 대한 Terraform 클라우드 통합."

ICO 사전 요구 사항으로 Terraform Cloud 통합

"이전: Cisco Intersight 구성."

절차 1: Cisco Intersight 및 Terraform Cloud 연결

1. 관련 Terraform Cloud 계정 세부 정보를 제공하여 Terraform 클라우드 타겟을 청구하거나 생성합니다.
2. 고객이 데이터 센터에 에이전트를 설치하고 Terraform Cloud와 통신할 수 있도록 프라이빗 클라우드에 대한 Terraform Cloud Agent 타겟을 생성합니다.

   자세한 내용은 을 참조하십시오 "이 링크".

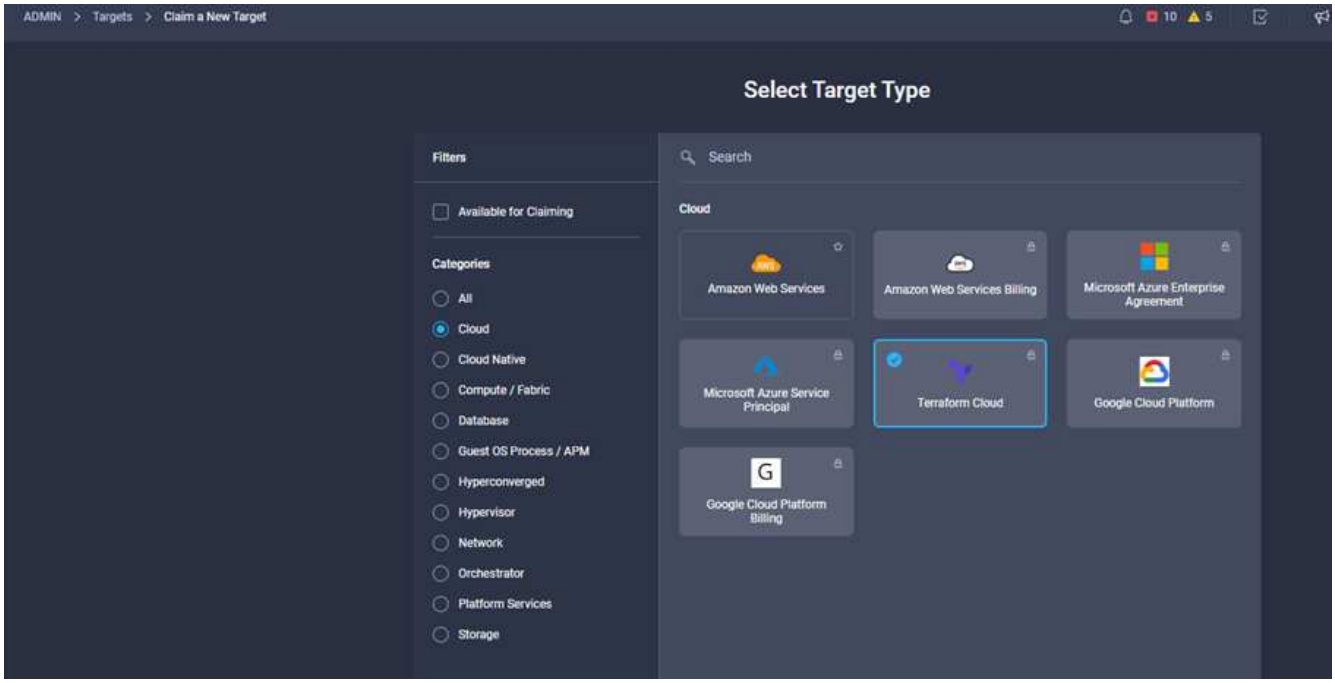
절차 2: 사용자 토큰을 생성합니다

Terraform Cloud의 대상을 추가하려면 Terraform Cloud 설정 페이지에서 사용자 이름 및 API 토큰을 제공해야 합니다.

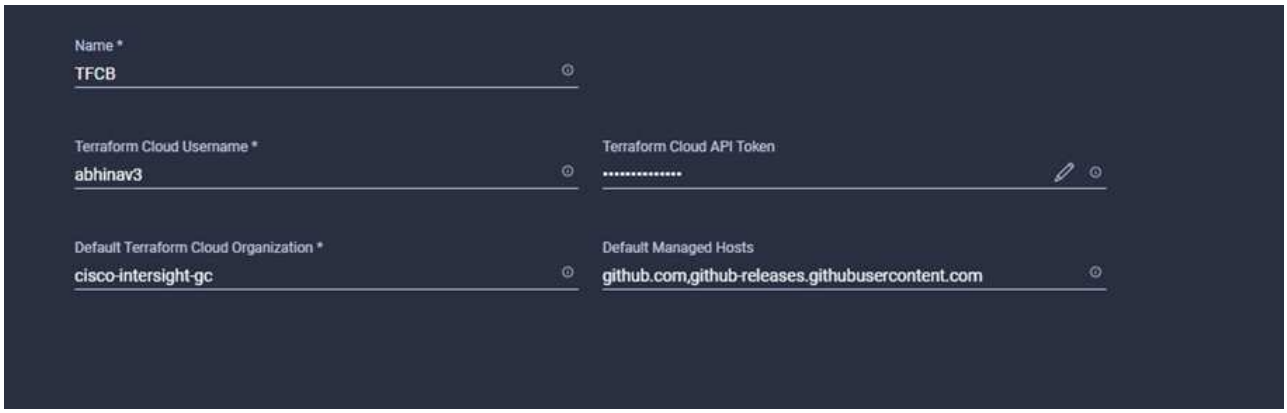
1. Terraform Cloud에 로그인하고 * 사용자 토큰 * 으로 이동합니다. "https://app.terraform.io/app/settings/tokens".
2. Create a new API token * 을 클릭합니다.
3. 이름을 지정하여 토큰을 저장하고 안전한 장소에 보관합니다.

절차 3: 클라우드 타겟 Terraform을 청구하십시오

1. 계정 관리자, 장치 관리자 또는 장치 기술자 권한과 Intersight에 로그인합니다.
2. admin > Targets > Claim a New Target * 으로 이동합니다.
3. 범주 * 에서 * 클라우드 * 를 클릭합니다.
4. Terraform Cloud * 를 클릭하고 * Start * 를 클릭합니다.



5. 다음 이미지에 표시된 대로 대상의 이름, Terraform Cloud의 사용자 이름, API 토큰 및 기본 조직을 Terraform Cloud에 입력합니다.
6. 기본 관리 호스트 * 필드에서 다른 관리 호스트와 함께 다음 링크를 추가해야 합니다.
   - github.com
   - github-releases.githubusercontent.com



모든 항목이 올바르게 입력되면 * Intersight Targets * 섹션에 Terraform Cloud 목표가 표시됩니다.

절차 **4:** 클라우드 에이전트 **Terraform** 추가

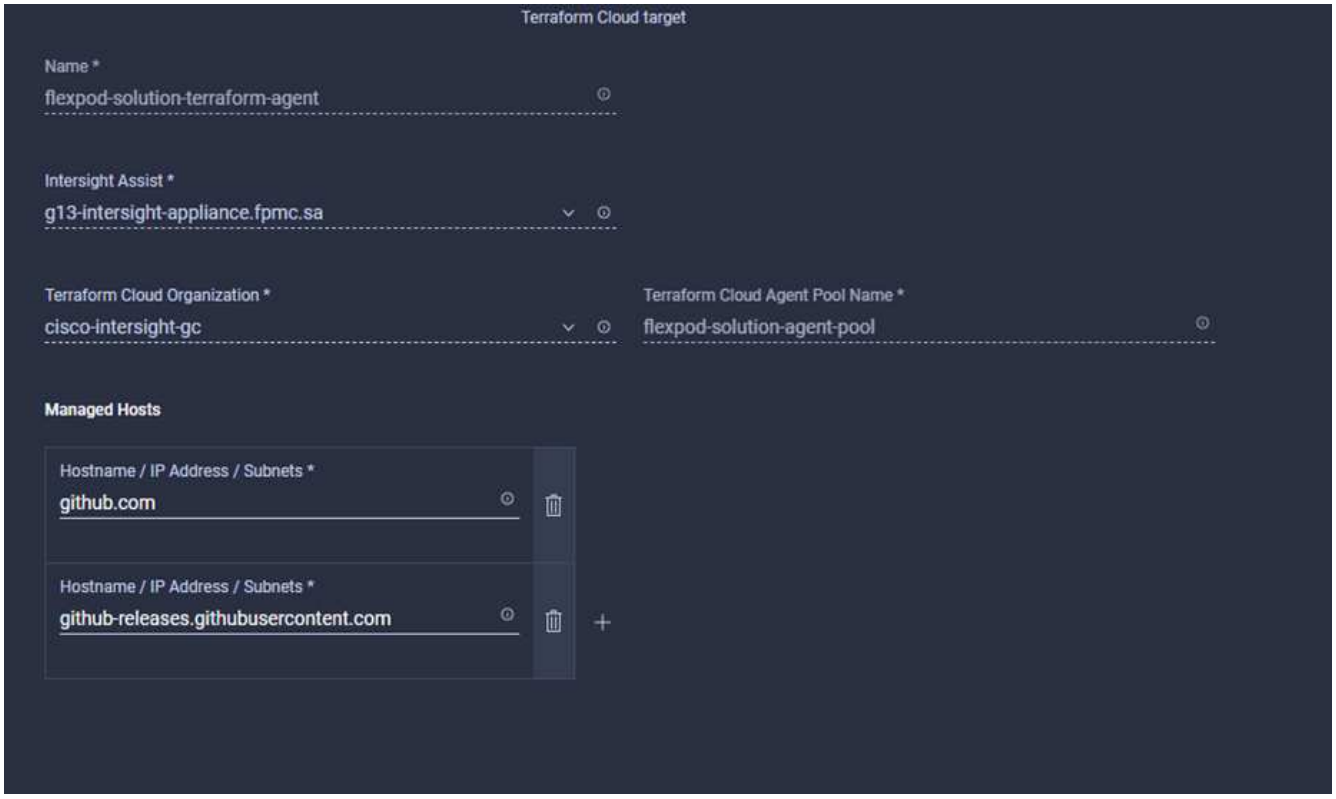
필수 구성 요소:

- Terraform 클라우드 대상.
- Terraform Cloud Agent를 배포하기 전에 Intersight Assist를 Intersight에 요청하였습니다.

각 보조 기능에 대해 5명의 상담원만 요청할 수 있습니다.

Terraform에 대한 연결을 만든 후에는 Terraform Agent를 스핀업하여 Terraform 코드를 실행해야 합니다.

1. Terraform 클라우드 목표의 드롭다운 목록에서 * 클라우드 에이전트 청구 * 를 클릭합니다.
2. Terraform Cloud 에이전트의 세부 정보를 입력합니다. 다음 스크린샷은 Terraform 에이전트에 대한 구성 세부 정보를 보여 줍니다.



Terraform Agent 속성을 업데이트할 수 있습니다. 대상이 * 연결되지 않음 * 상태이고 * 연결됨 * 상태인 적이 없는 경우 Terraform 에이전트에 대한 토큰이 생성되지 않습니다.

에이전트 검증이 성공하고 에이전트 토큰이 생성되면 조직 및/또는 에이전트 풀을 재구성할 수 없습니다. Terraform 에이전트를 성공적으로 배포하면 * Connected * 상태가 표시됩니다.

Terraform Cloud 통합을 활성화하고 주장하면 하나 이상의 Terraform Cloud 에이전트를 Cisco Intersight Assist에 배포할 수 있습니다. Terraform Cloud 에이전트는 Terraform Cloud 대상의 하위 대상으로 모델링됩니다. 상담원 목표를 청구할 때 목표 클레임이 진행 중임을 나타내는 메시지가 표시됩니다.

몇 초 후 타겟이 * Connected * 상태로 이동되고 Intersight 플랫폼은 에이전트에서 Terraform Cloud 게이트웨이로 HTTPS 패킷을 라우팅합니다.

Terraform 상담원은 올바른 클레임을 받아야 하며 대상 아래에 * Connected * 로 표시되어야 합니다.

"다음으로 퍼블릭 클라우드 서비스 공급자를 구성합니다."

퍼블릭 클라우드 서비스 공급자 구성

"이전: ICO 사전 요구 사항에 대한 Terraform Cloud 통합."

절차 **1: NetApp Cloud Manager**에 액세스하십시오

NetApp Cloud Manager 및 기타 클라우드 서비스에 액세스하려면 에 가입해야 합니다 "NetApp Cloud Central에서".

Cloud Central 계정에서 작업 영역 및 사용자를 설정하려면 을 클릭합니다 "여기".

절차 **2:** 커넥터 전개

Google Cloud에 Connector를 배포하려면 다음을 참조하십시오 "링크".

"그 다음: 하이브리드 클라우드 NetApp 스토리지의 자동화된 구축"

하이브리드 클라우드 **NetApp** 스토리지 자동 구축

"이전: 공용 클라우드 서비스 공급자 구성"

Google 클라우드

먼저, API를 사용하도록 설정하고 Cloud Manager에 Connector와 같은 프로젝트나 다른 프로젝트에 있는 Cloud Volumes ONTAP 시스템을 배포 및 관리할 수 있는 권한을 제공하는 서비스 계정을 만들어야 합니다.

Google Cloud 프로젝트에 커넥터를 배포하기 전에 커넥터가 사용자 구내 또는 다른 클라우드 공급자에서 실행되고 있지 않은지 확인합니다.

Cloud Manager에서 직접 Connector를 구축하기 전에 다음 두 가지 권한 세트가 있어야 합니다.

- Cloud Manager에서 Connector VM 인스턴스를 시작할 수 있는 권한이 있는 Google 계정을 사용하여 Connector를 배포해야 합니다.
- Connector를 배포할 때 VM 인스턴스를 선택하라는 메시지가 표시됩니다. Cloud Manager는 서비스 계정에서 권한을 받아 사용자를 대신하여 Cloud Volumes ONTAP 시스템을 생성하고 관리합니다. 서비스 계정에 사용자 지정 역할을 첨부하면 권한이 제공됩니다. 사용자와 서비스 계정에 필요한 권한이 포함된 YAML 파일을 두 개 설정해야 합니다. 를 사용하는 방법을 알아보십시오 "YAML 파일을 사용하여 권한을 설정합니다" 여기.

을 참조하십시오 "자세한 비디오입니다" 모든 필수 사전 요구 사항에 대해.

Cloud Volumes ONTAP 배포 모드 및 아키텍처

Cloud Volumes ONTAP는 Google Cloud에서 단일 노드 시스템으로 고가용성(HA) 노드 쌍으로 제공됩니다. 요구사항에 따라 Cloud Volumes ONTAP 구축 모드를 선택할 수 있습니다. 단일 노드 시스템을 HA 쌍으로 업그레이드하는 것은 지원되지 않습니다. 단일 노드 시스템과 HA 쌍 간에 전환하려면 새 시스템을 구축하고 기존 시스템의 데이터를 새 시스템으로 복제해야 합니다.

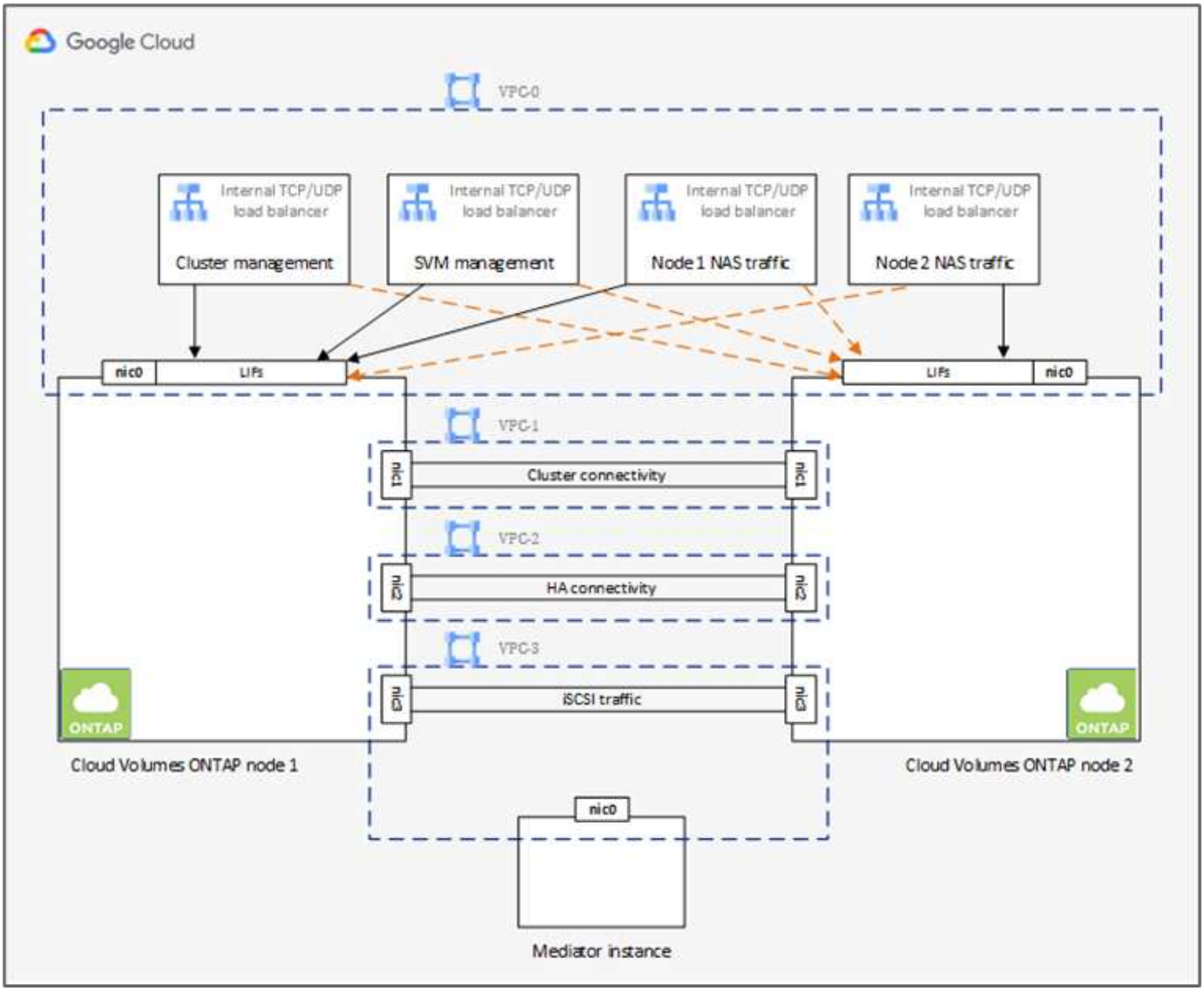
Google Cloud의 고가용성 **Cloud Volumes ONTAP**

Google Cloud는 여러 지리적 지역 및 한 지역 내의 여러 영역에 리소스를 배포할 수 있도록 지원합니다. HA 구축은 강력한 n1-표준 또는 n2-표준 시스템 유형을 사용하는 ONTAP 노드 2개로 구성되어 Google Cloud에서 사용할 수 있습니다. 두 Cloud Volumes ONTAP 노드 간에 데이터가 동기식으로 복제되어 장애 발생 시 가용성을 제공합니다. Cloud Volumes ONTAP의 HA 구축을 위해서는 각 VPC에 VPC 4개와 프라이빗 서브넷이 필요합니다. 4개의 VPC에 있는 서브넷에는 중복되는 CIDR 범위가 없어야 합니다.

4개의 VPC는 다음과 같은 용도로 사용됩니다.

- VPC 0은 데이터 및 Cloud Volumes ONTAP 노드에 대한 인바운드 통신을 지원합니다.
- VPC 1 는 Cloud Volumes ONTAP 노드 간 클러스터 연결을 제공합니다.
- VPC 2는 노드 간 비휘발성 RAM(NVRAM) 복제를 지원합니다.
- VPC 3은 노드 재구축을 위한 HA 중재자 인스턴스 및 디스크 복제 트래픽에 연결하는 데 사용됩니다.

다음 이미지는 Goggle Cloud의 고가용성 Cloud Volumes ONTAP를 보여줍니다.



자세한 내용은 을 참조하십시오 "이 링크".

Google Cloud의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항은 을 참조하십시오 "이 링크".

데이터 계층화에 대한 자세한 내용은 를 참조하십시오 "이 링크".

환경 사전 요구 사항 설정

Cloud Volumes ONTAP 클러스터 자동 생성, 온프레미스 볼륨과 클라우드 볼륨 간 SnapMirror 구성, 클라우드 볼륨 생성 등의 작업은 Terraform 구성을 사용하여 수행됩니다. 이러한 Terraform 구성은 Terraform Cloud for Business 계정에서 호스팅됩니다. Intersight Cloud Orchestrator를 사용하면 Terraform Cloud for Business 계정에서 작업

영역을 만들고, 모든 필수 변수를 작업 영역에 추가하고, Terraform Plan을 실행하는 등의 작업을 조정할 수 있습니다.

이러한 자동화 및 오케스트레이션 작업의 경우 다음 섹션에 설명된 대로 몇 가지 요구사항과 데이터가 필요합니다.

GitHub 리포지토리

Terraform 코드를 호스팅하려면 GitHub 계정이 필요합니다. Intersight Orchestrator는 Terraform Cloud for Business 계정에 새 작업 공간을 만듭니다. 이 작업 영역은 버전 제어 워크플로로 구성됩니다. 이를 위해 Terraform 구성을 GitHub 리포지토리에 유지하고 작업 영역을 만드는 동안 입력으로 제공해야 합니다.

"이 GitHub 링크를 클릭합니다" 다양한 리소스를 포함하는 Terraform 구성을 제공합니다. 이 리포지토리를 포크하고 GitHub 계정에서 복사본을 만들 수 있습니다.

이 리포지터리에서 provider.tf는 필요한 Terraform 공급자에 대한 정의를 갖습니다. NetApp Cloud Manager의 Terraform 공급자가 사용됩니다.

변수 tf에는 변수 선언이 모두 있습니다. 이러한 변수의 값은 Intersight Cloud Orchestrator의 워크플로 입력으로 입력됩니다. 이렇게 하면 값을 작업 공간에 전달하고 Terraform 구성을 실행할 수 있는 편리한 방법이 제공됩니다.

'소스.TF'는 작업 환경에 온프레미스 ONTAP를 추가하고, Google Cloud에 단일 노드 Cloud Volumes ONTAP 클러스터를 생성하고, 온프레미스 및 Cloud Volumes ONTAP 간에 SnapMirror 관계를 설정하고, Cloud Volumes ONTAP에 클라우드 볼륨을 생성하는 데 필요한 다양한 리소스를 정의합니다.

이 리포지토리에서:

- 'provider.tf'는 NetApp Cloud Manager를 필수 Terraform 공급업체를 위한 정의로 보유하고 있습니다.
- variables.tf에는 Intersight Cloud Orchestrator 워크플로의 입력으로 사용되는 변수 선언이 있습니다. 이렇게 하면 값을 작업 공간에 전달하고 Terraform 구성을 실행할 수 있는 편리한 방법이 제공됩니다.
- resources.tf는 작업 환경에 온프레미스 ONTAP를 추가하고, Google Cloud에 단일 노드 Cloud Volumes ONTAP 클러스터를 생성하고, 온프레미스 및 Cloud Volumes ONTAP 간에 SnapMirror 관계를 설정하고, Cloud Volumes ONTAP에 클라우드 볼륨을 생성하는 등 다양한 리소스를 정의합니다.

추가 리소스 블록을 추가하여 Cloud Volumes ONTAP에 여러 볼륨을 생성하거나 COUNT 또는 'For_each' Terraform 구문을 사용할 수 있습니다.

Terraform 작업 공간, 모듈 및 정책 집합을 Terraform 구성이 포함된 git 저장소로 연결하려면 Terraform Cloud가 GitHub repo에 액세스해야 합니다.

클라이언트를 추가하면 클라이언트의 OAuth 토큰 ID가 Intersight Cloud Orchestrator의 워크플로 입력 중 하나로 사용됩니다.

1. Terraform Cloud for Business 계정에 로그인합니다. 설정 > 공급자 * 로 이동합니다.
2. VCS 공급자 추가 * 를 클릭합니다.
3. 버전을 선택합니다.
4. 공급자 설정 * 의 단계를 따릅니다.
5. VCS 제공자 * 에서 추가된 클라이언트를 볼 수 있습니다. OAuth 토큰 ID를 기록해 둡니다.

NetApp Cloud Manager API 작업에서 토큰을 새로 고칠 수 있습니다

Cloud Manager에는 웹 브라우저 인터페이스 외에도 SaaS 인터페이스를 통해 소프트웨어 개발자가 Cloud Manager 기능에 직접 액세스할 수 있도록 지원하는 REST API가 있습니다. Cloud Manager 서비스는 확장 가능한 개발 플랫폼을 총체적으로 형성하는 몇 가지 개별 구성요소로 구성되어 있습니다. 새로 고침 토큰을 사용하면 각 API 호출에 대해 권한 부여 헤더에 추가하는 액세스 토큰을 생성할 수 있습니다.

NetApp-cloudManager 공급자는 API를 직접 호출하지 않고 업데이트 토큰을 사용하여 Terraform 리소스를 해당 API 호출로 변환합니다. 에서 NetApp Cloud Manager API 작업에 대한 업데이트 토큰을 생성해야 합니다 "NetApp Cloud Central에서".

Cloud Volumes ONTAP 클러스터 생성, SnapMirror 구성 등과 같은 Cloud Manager 리소스를 생성하려면 Cloud Manager Connector의 클라이언트 ID가 필요합니다.

1. Cloud Manager 로그인: "https://cloudmanager.netapp.com/".
2. 커넥터 * 를 클릭합니다.
3. 커넥터 관리 * 를 클릭합니다.
4. 줄임표를 클릭하고 커넥터 ID를 복사합니다.

Cisco Intersight Cloud Orchestrator 워크플로우를 개발합니다

Cisco Intersight Cloud Orchestrator는 다음과 같은 경우 Cisco Intersight에서 사용할 수 있습니다.

- Intersight Premier 라이센스를 설치했습니다.
- 계정 관리자, 스토리지 관리자, 가상화 관리자 또는 서버 관리자이며 최소 하나의 서버가 할당되어 있습니다.

워크플로 디자이너

Workflow Designer를 사용하면 새 워크플로(작업 및 데이터 형식)를 만들고 기존 워크플로를 편집하여 Cisco Intersight에서 대상을 관리할 수 있습니다.

Workflow Designer를 시작하려면 * Orchestration > Workflow * 로 이동합니다. 대시보드에는 * 내 워크플로 *, * 샘플 워크플로 * 및 * 모든 워크플로 * 탭 아래에 다음 세부 정보가 표시됩니다.

- 검증 상태
- 마지막 실행 상태
- 실행 횟수별 상위 워크플로
- 상위 워크플로 범주
- 시스템 정의 워크플로 수
- 대상별 상위 워크플로

대시보드를 사용하여 탭을 생성, 편집, 클론 복제 또는 삭제할 수 있습니다. 사용자 지정 보기 탭을 만들려면 * + * 를 클릭하고 이름을 지정한 다음 열, 태그 열 및 위젯에 표시되어야 하는 필수 매개 변수를 선택합니다. 탭에 * 잠금 * 아이콘이 없으면 탭 이름을 바꿀 수 있습니다.

대시보드 아래에는 다음 정보를 표시하는 표 형식의 워크플로 목록이 있습니다.

- 표시 이름

- 설명
- 시스템 정의
- 기본 버전
- 실행
- 마지막 실행 상태
- 검증 상태
- 마지막 업데이트
- 조직

작업 열에서 다음 작업을 수행할 수 있습니다.

- * 실행. * 워크플로를 실행합니다.
- * 기록. * 워크플로 실행 기록을 표시합니다.
- * 버전 관리 * 워크플로의 버전을 만들고 관리합니다.
- * 삭제. * 워크플로를 삭제합니다.
- * 재시도. * 실패한 워크플로를 다시 시도하십시오.

워크플로우

다음 단계로 구성된 워크플로를 만듭니다.

- * 워크플로 정의 * 표시 이름, 설명 및 기타 중요한 속성을 지정합니다.
- * 워크플로 입력 및 워크플로 출력을 정의합니다. * 워크플로 실행에 필요한 입력 매개 변수와 성공적인 실행에 생성된 출력을 지정합니다
- * 워크플로 작업을 추가합니다. * 워크플로를 수행하는 데 필요한 워크플로 작업을 워크플로 디자이너에서 하나 이상 추가합니다.
- * 워크플로 유효성 검사. * 워크플로를 검증하여 작업 입력 및 출력 연결에 오류가 없는지 확인합니다.

사내 **FlexPod** 스토리지를 위한 워크플로우를 생성합니다

온-프레미스 FlexPod 스토리지에 대한 워크플로우를 구성하려면 를 참조하십시오 "이 링크".

"다음: DR 워크플로우."

DR 워크플로우

"이전: 하이브리드 클라우드 NetApp 스토리지의 자동화된 구축"

단계의 순서는 다음과 같습니다.

1. 워크플로를 정의합니다.
    - 재해 복구 워크플로와 같이 사용자에게 친숙한 짧은 이름을 생성합니다.
2. 워크플로 입력을 정의합니다. 이 워크플로우를 위해 취하는 입력은 다음과 같습니다.

- 볼륨 옵션(볼륨 이름, 마운트 경로)
- 볼륨 용량입니다
- 새 데이터 저장소와 연결된 데이터 센터입니다
- 데이터 저장소가 호스팅되는 클러스터입니다
- vCenter에서 생성할 새 데이터 저장소의 이름입니다
- 새 데이터 저장소의 유형 및 버전입니다
- Terraform 조직의 이름입니다
- Terraform 작업 영역
- Terraform 작업 영역에 대한 설명입니다
- Terraform 구성을 실행하는 데 필요한 변수(민감하고 민감하지 않음
- 계획을 시작한 이유

3. 워크플로 작업을 추가합니다.

   FlexPod의 작업과 관련된 작업은 다음과 같습니다.

   - FlexPod에서 볼륨을 생성합니다.
   - 생성된 볼륨에 스토리지 엑스포트 정책을 추가합니다.
   - 새로 생성된 볼륨을 VMware vCenter의 데이터 저장소에 매핑합니다.

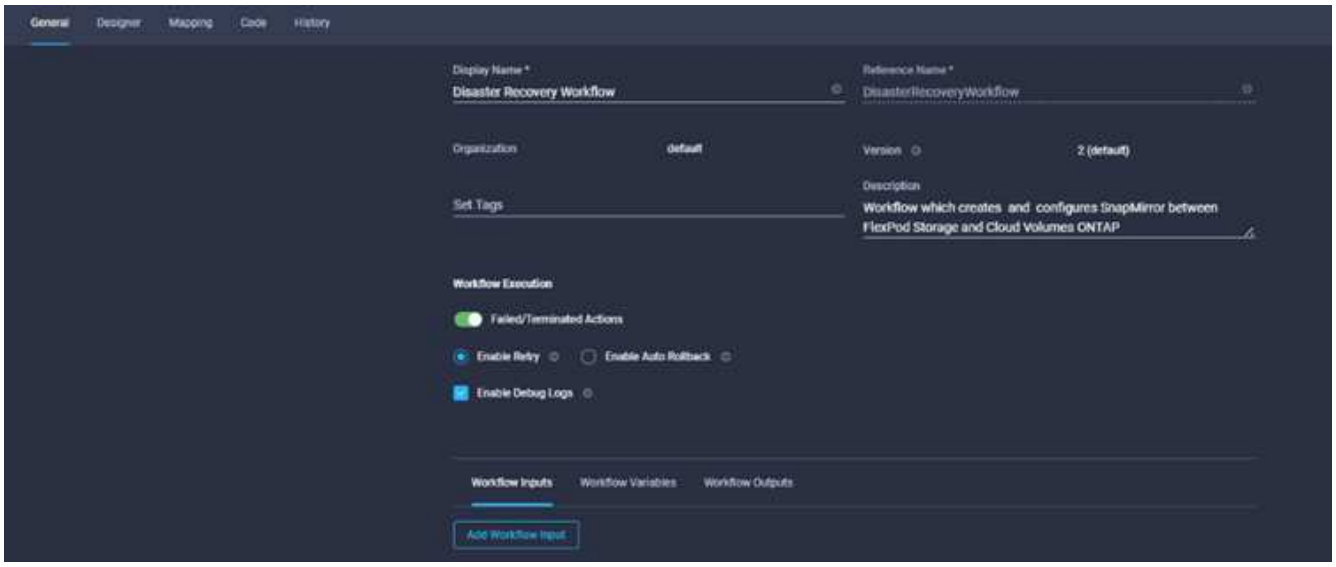
     Cloud Volumes ONTAP 클러스터 생성과 관련된 작업:

   - Terraform 작업 영역을 추가합니다
   - Terraform 변수를 추가합니다
   - Terraform 중요 변수를 추가합니다
   - 새 Terraform 계획을 시작합니다
   - Terraform 실행을 확인합니다

4. 워크플로를 확인합니다.

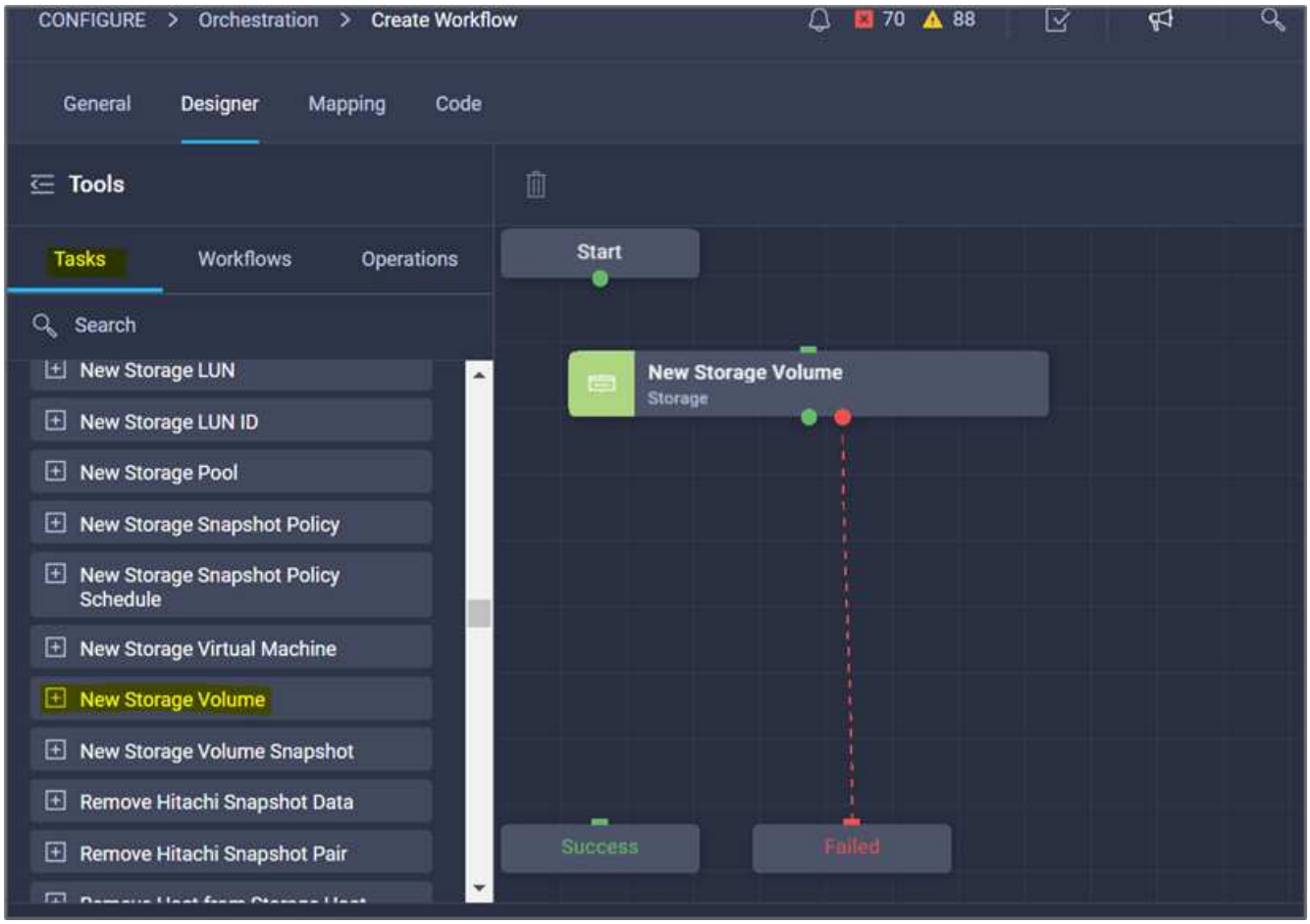
절차 **1:** 워크플로를 만듭니다

1. 왼쪽 탐색 창에서 * Orchestration * 을 클릭하고 * Create Workflow * 를 클릭합니다.
2. 일반 * 탭에서:
   a. 표시 이름 제공(재해 복구 워크플로우)
   b. 조직을 선택하고 태그를 설정한 다음 설명을 입력합니다.
3. 저장 을 클릭합니다.



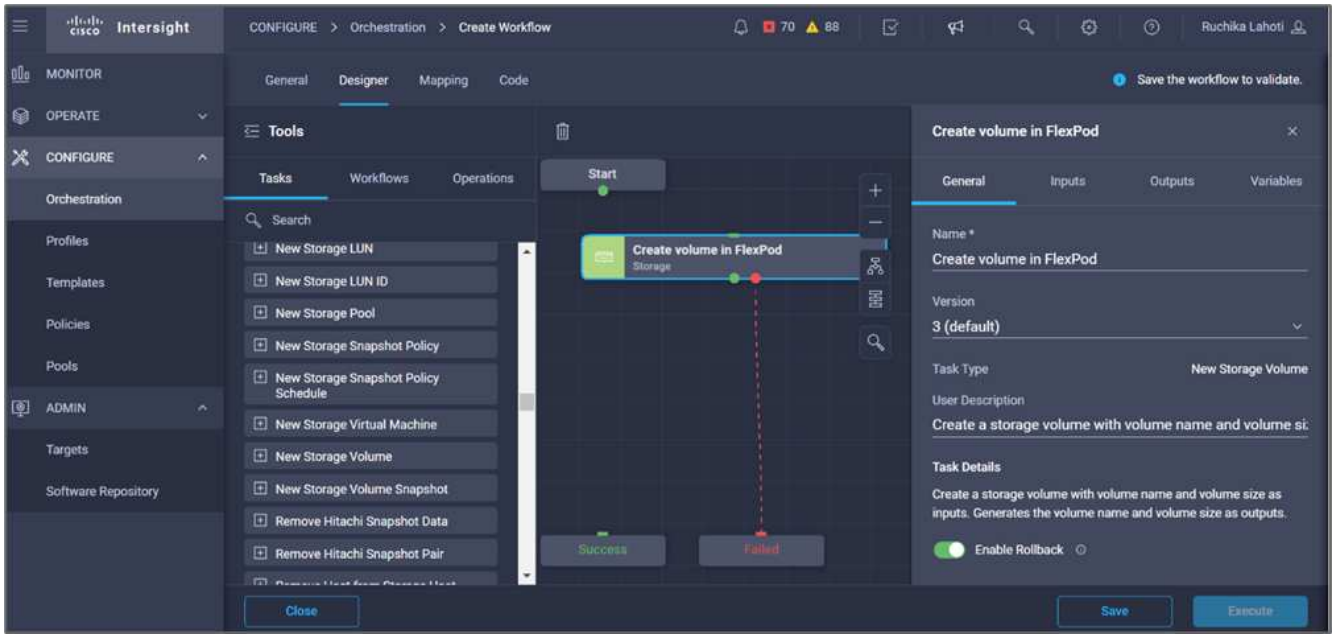
절차 **2. FlexPod**에서 새 볼륨을 생성합니다

1. 디자이너 * 탭으로 이동하고 * 도구 * 섹션에서 * 작업 * 을 클릭합니다.
2. Tools * 섹션에서 * Storage > New Storage Volume * 작업을 * Design * 영역으로 끌어다 놓습니다.
3. 새 저장소 볼륨 * 을 클릭합니다.

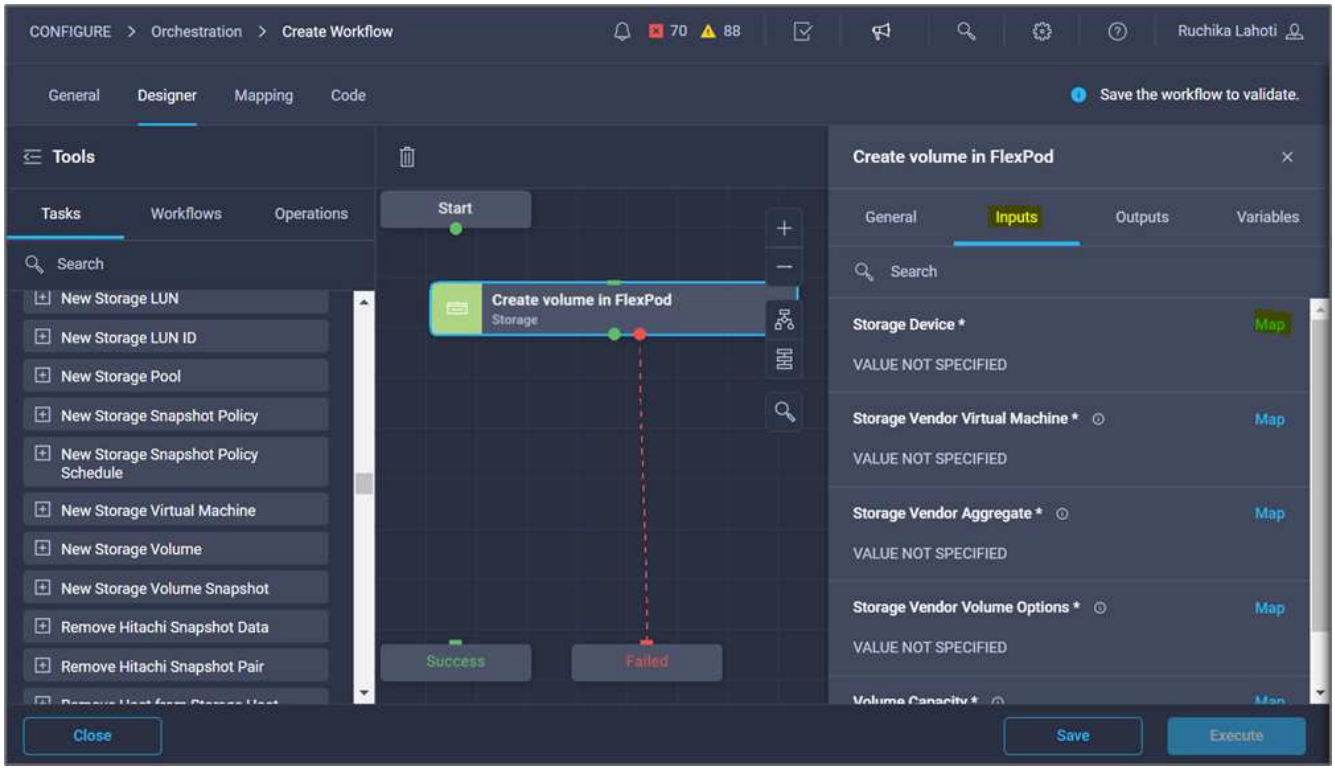


4. 작업 속성 * 영역에서 * 일반 * 탭을 클릭합니다. 필요에 따라 이 작업의 이름과 설명을 변경할 수 있습니다. 이

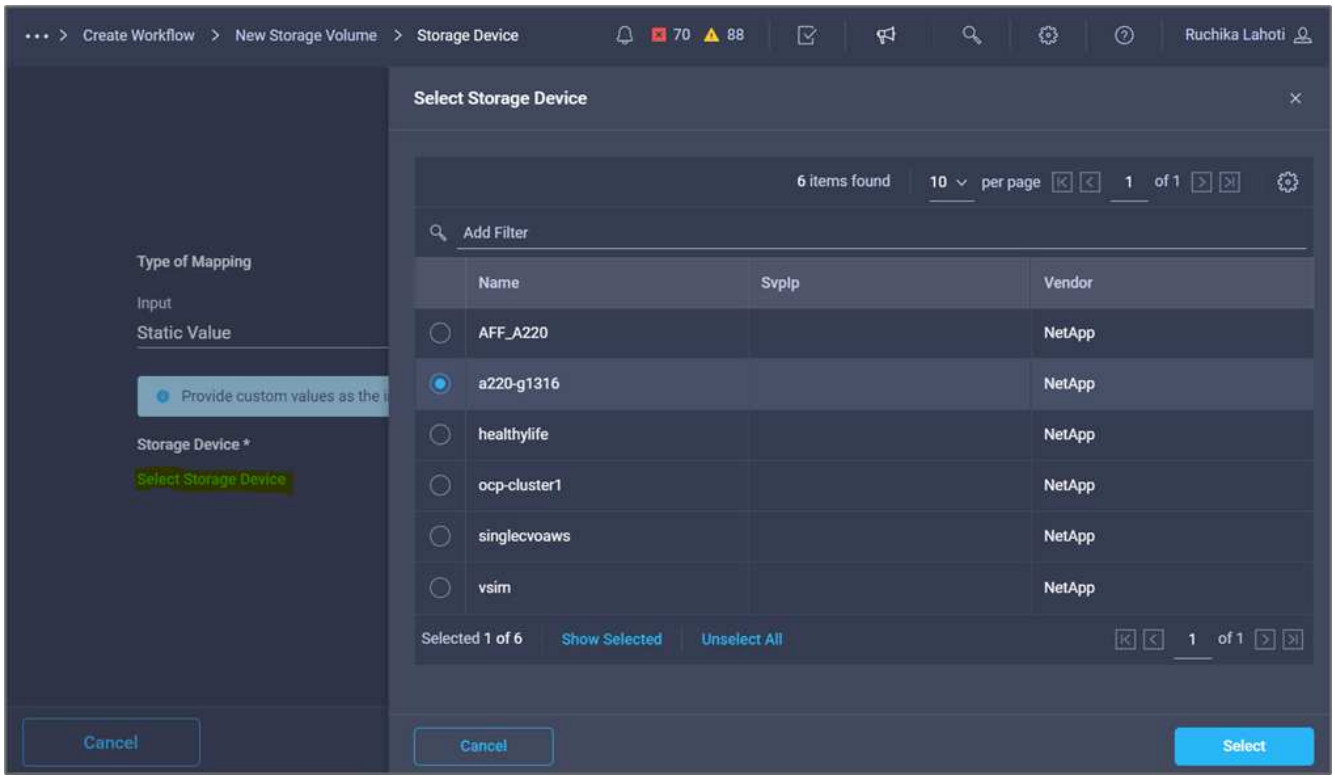
예에서 작업 이름은 * FlexPod * 에서 볼륨 생성 * 입니다.



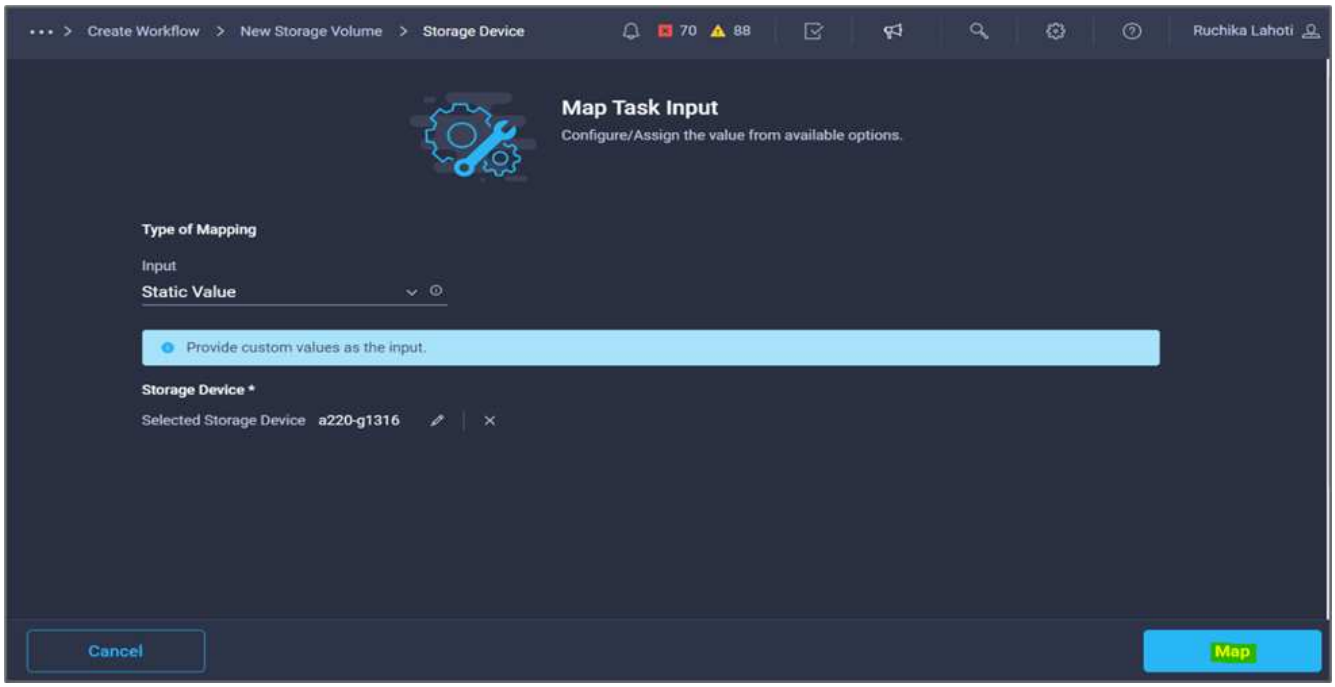
5. 작업 속성 * 영역에서 * 입력 * 을 클릭합니다.
6. Storage Device * 필드에서 * Map * 을 클릭합니다.



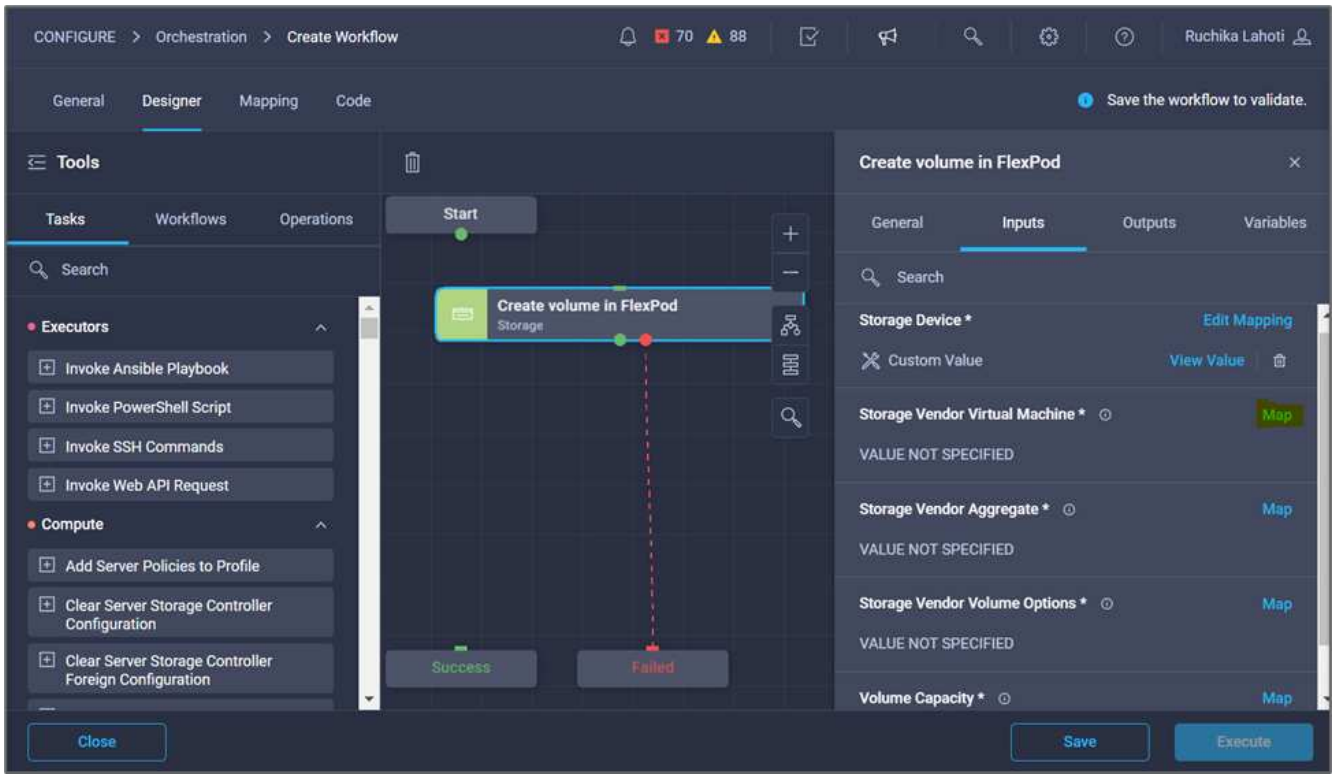
7. 정적 값 * 을 선택하고 * 저장 장치 선택 * 을 클릭합니다.
8. 추가된 스토리지 대상을 클릭하고 * 선택 * 을 클릭합니다.



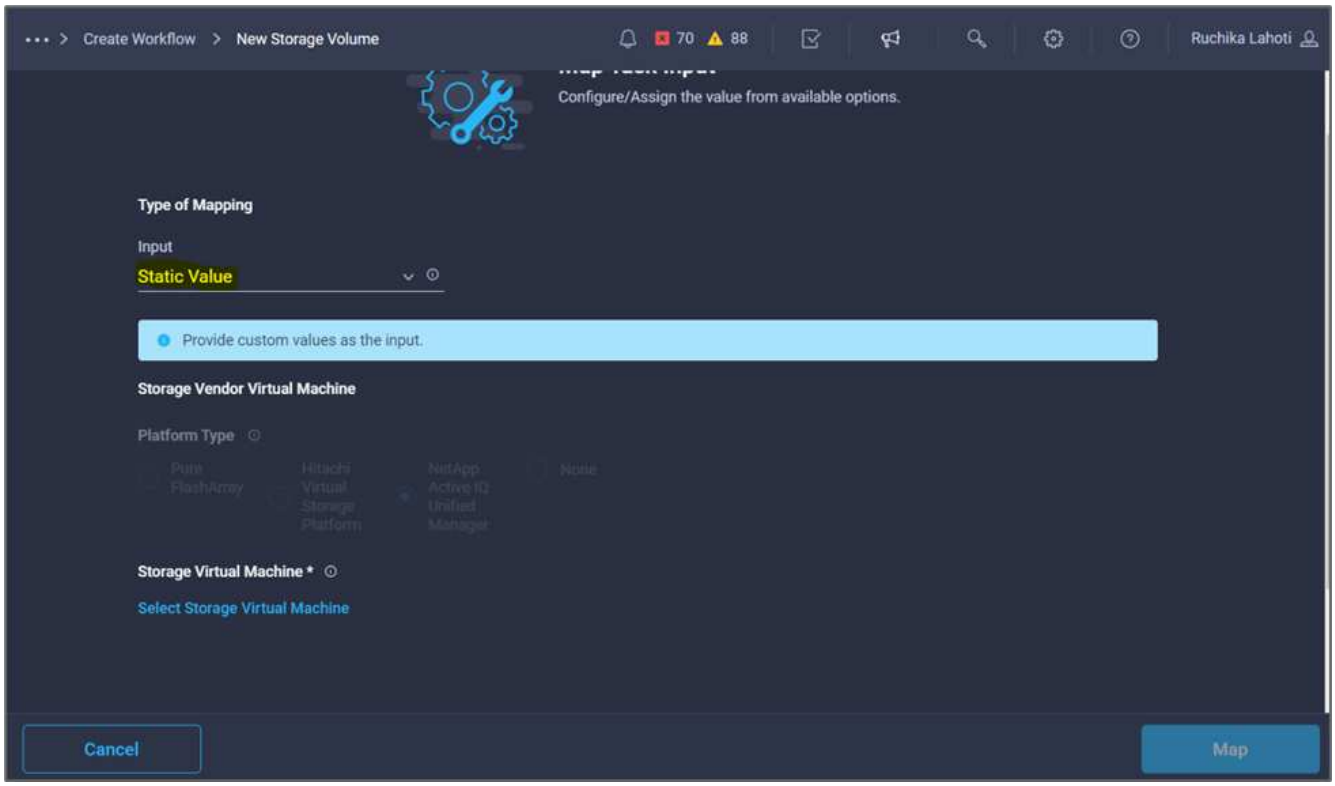
9. Map * 을 클릭합니다.



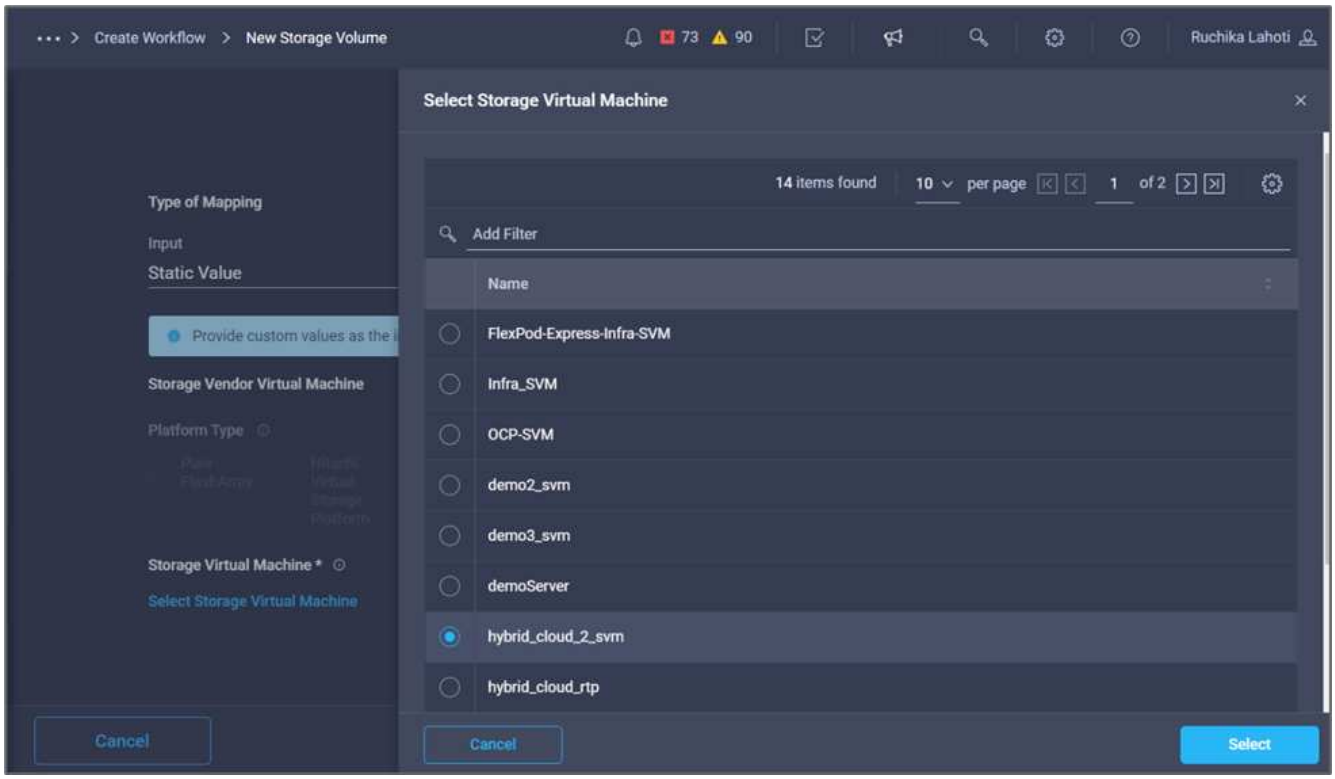
10. Storage Vendor Virtual Machine * 필드에서 * Map * 을 클릭합니다.



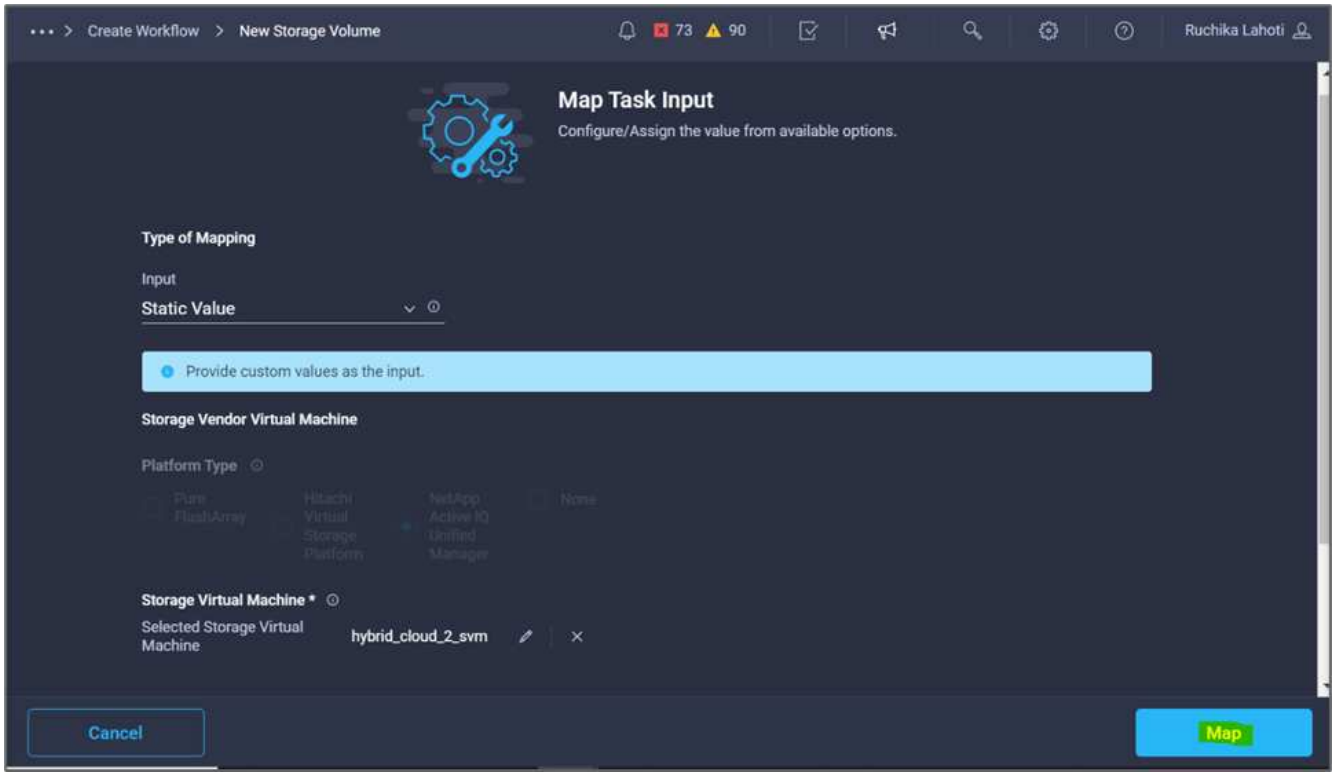
11. 정적 값 * 을 선택하고 * 스토리지 가상 머신 선택 * 을 클릭합니다.



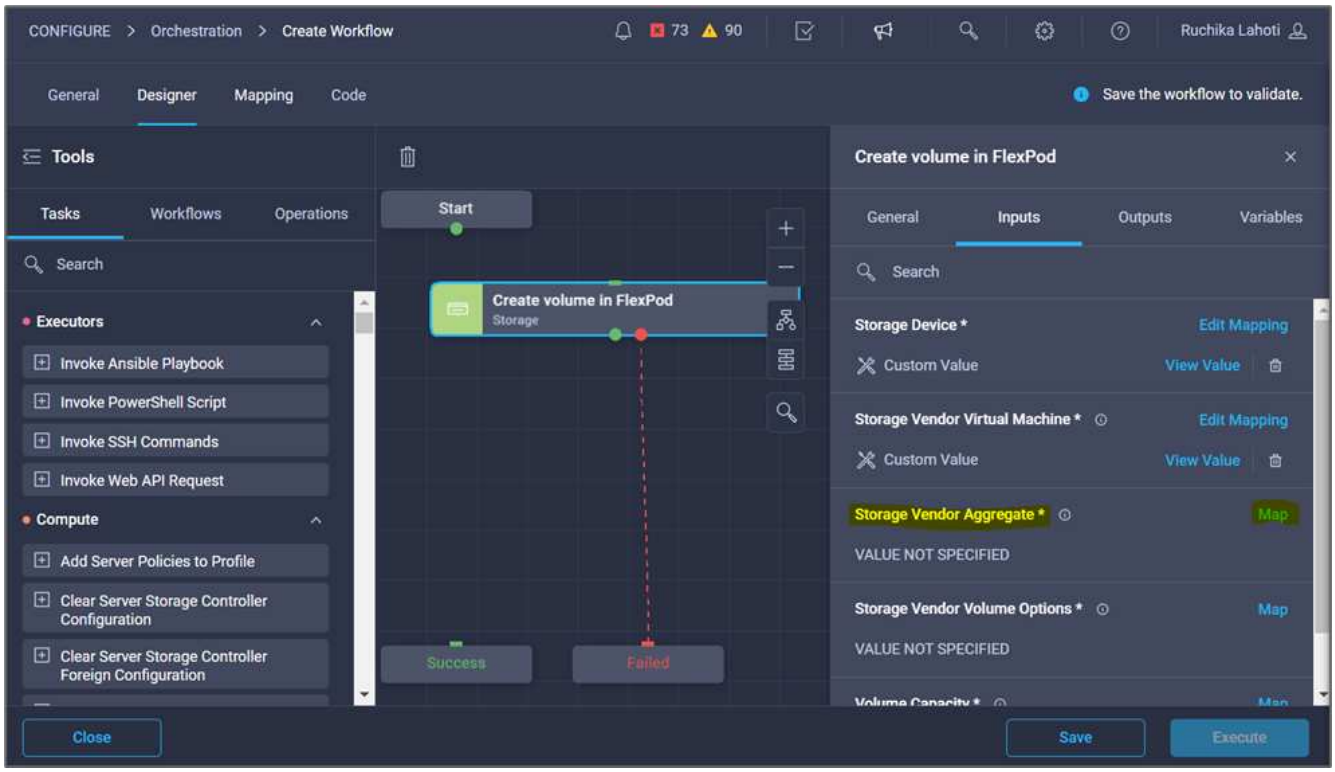
12. 볼륨을 생성해야 하는 스토리지 가상 머신을 선택하고 * Select * 를 클릭합니다.



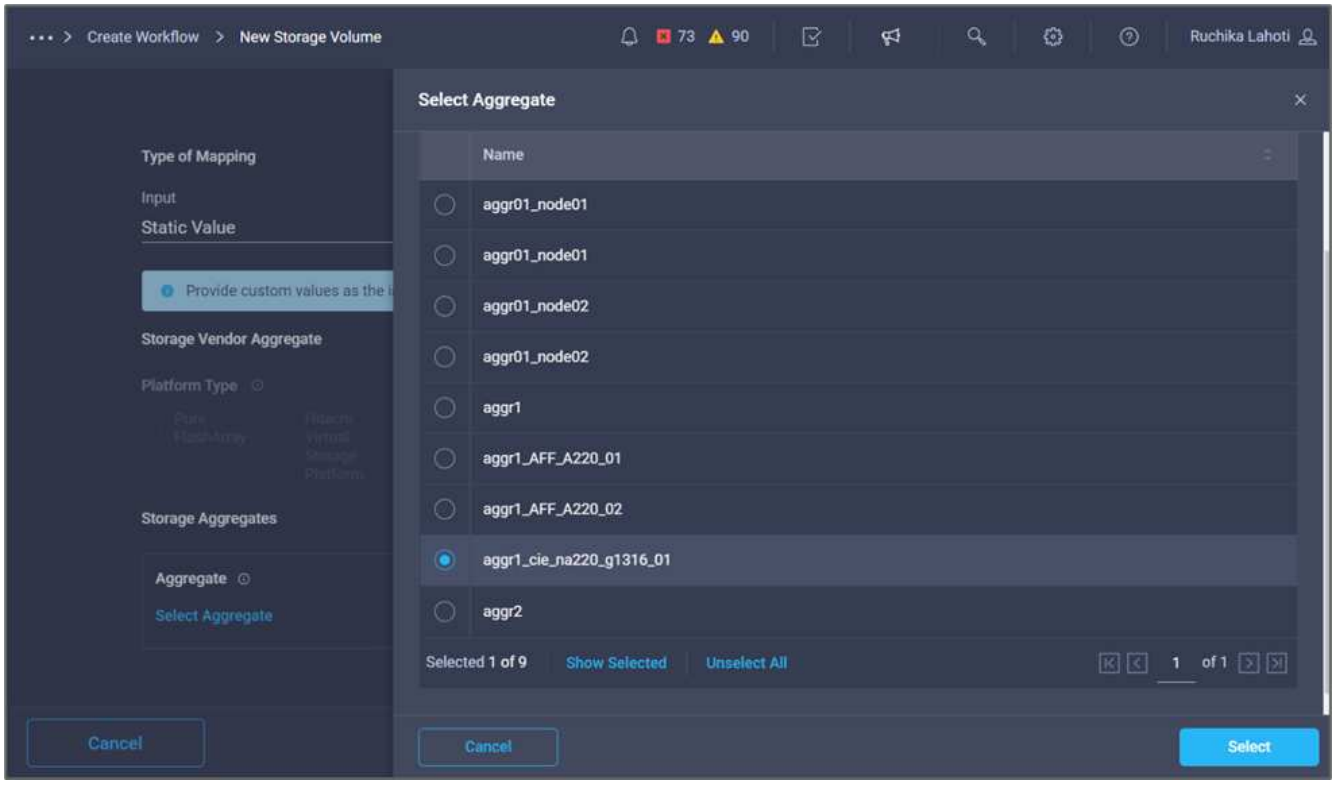
13. Map * 을 클릭합니다.



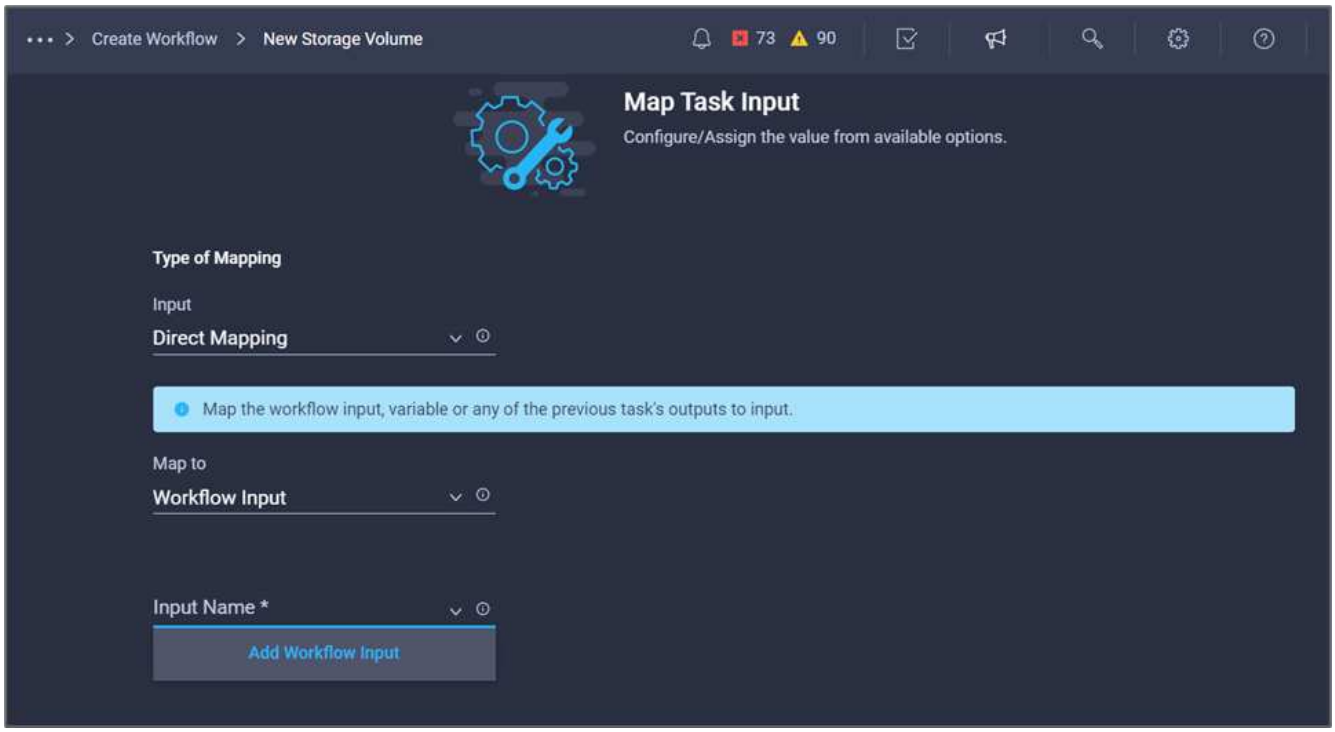
14. 스토리지 공급업체 집계 * 필드에서 * 맵 * 을 클릭합니다.



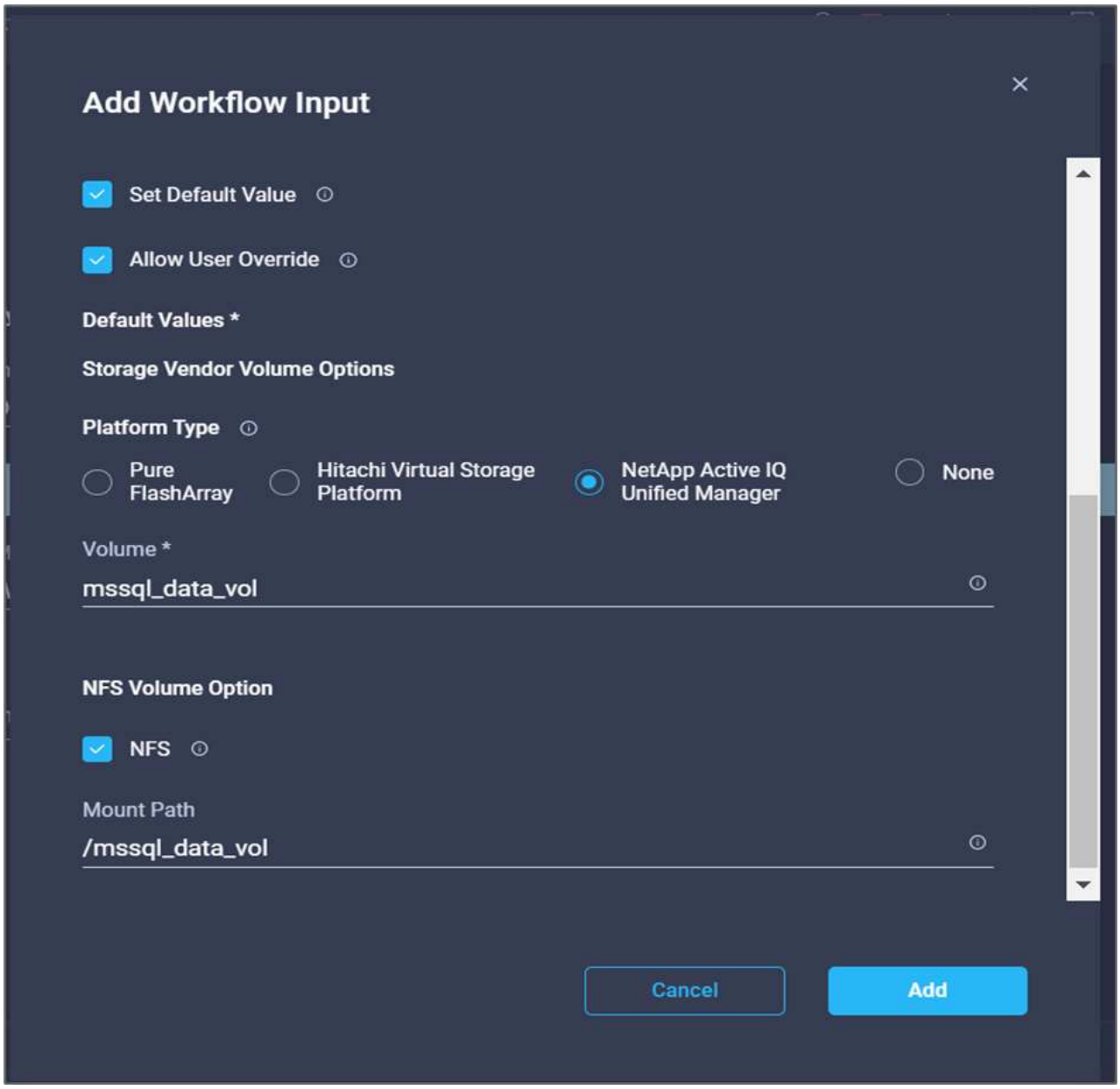
15. 정적 값 * 을 선택하고 * 스토리지 애그리게이트 선택 * 을 클릭합니다. Aggregate를 선택하고 * Select * 를 클릭합니다.



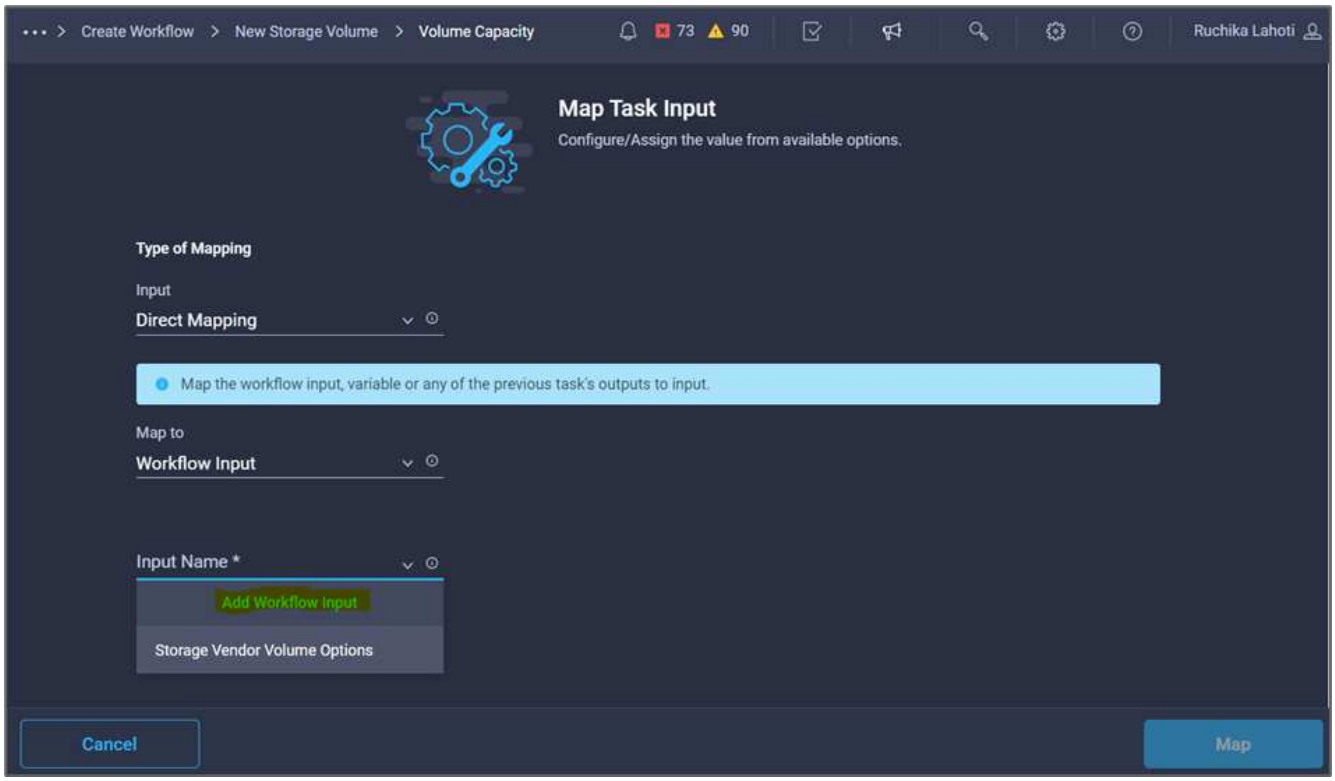
16. Map * 을 클릭합니다.
17. 스토리지 공급업체 볼륨 옵션 * 필드에서 * 맵 * 을 클릭합니다.
18. 직접 매핑 * 을 선택하고 * 워크플로 입력 * 을 클릭합니다.



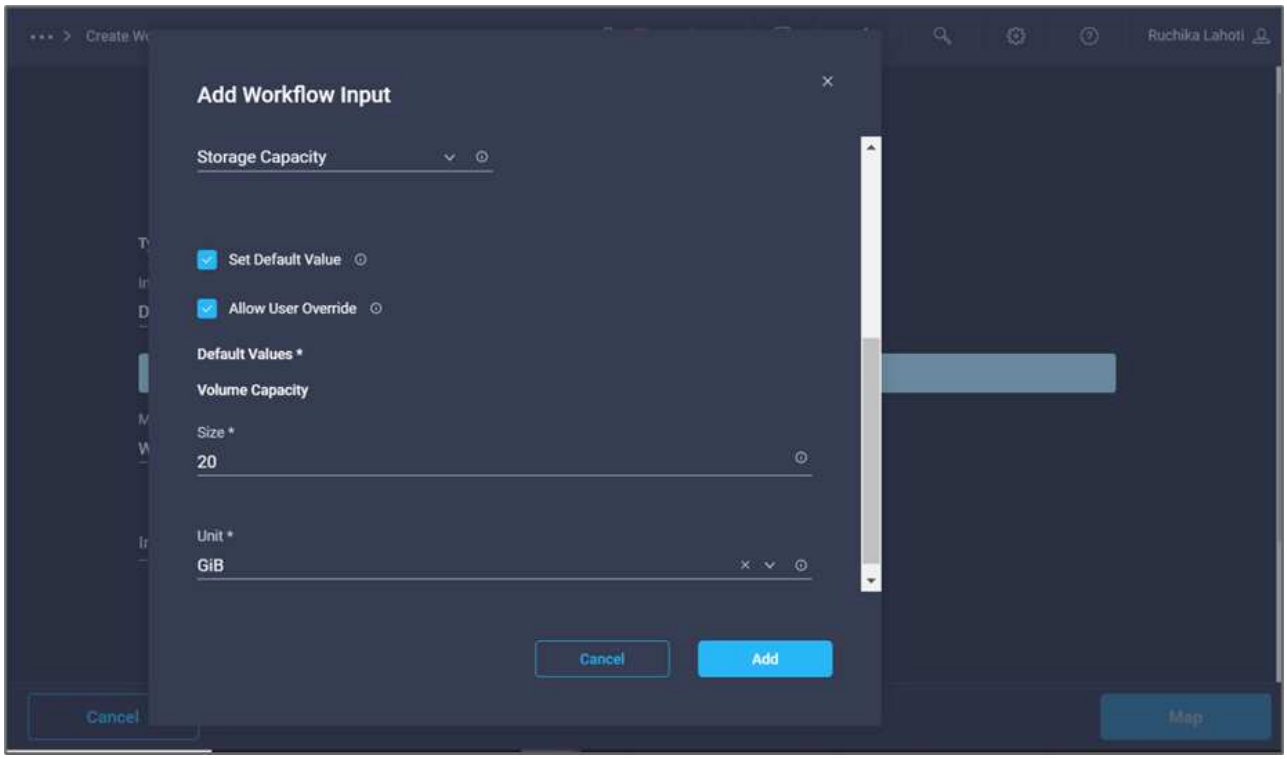
19. 입력 추가 마법사에서 다음 단계를 완료합니다.
    a. 표시 이름과 참조 이름을 입력합니다(선택 사항).
    b. 유형 * 에 대해 * 스토리지 공급업체 볼륨 옵션 * 이 선택되어 있는지 확인합니다.
    c. Set Default Value(기본값 설정) 및 Override(무시) * 를 클릭합니다.
    d. 필수 * 를 클릭합니다.
    e. 플랫폼 유형 * 을 * NetApp Active IQ Unified Manager * 로 설정합니다.
    f. 볼륨 * 에서 생성된 볼륨의 기본값을 제공합니다.
    g. NFS * 를 클릭합니다. NFS가 설정되면 NFS 볼륨이 생성됩니다. 이 값을 false로 설정하면 SAN 볼륨이 생성됩니다.
    h. 마운트 경로를 제공하고 * 추가 * 를 클릭합니다.



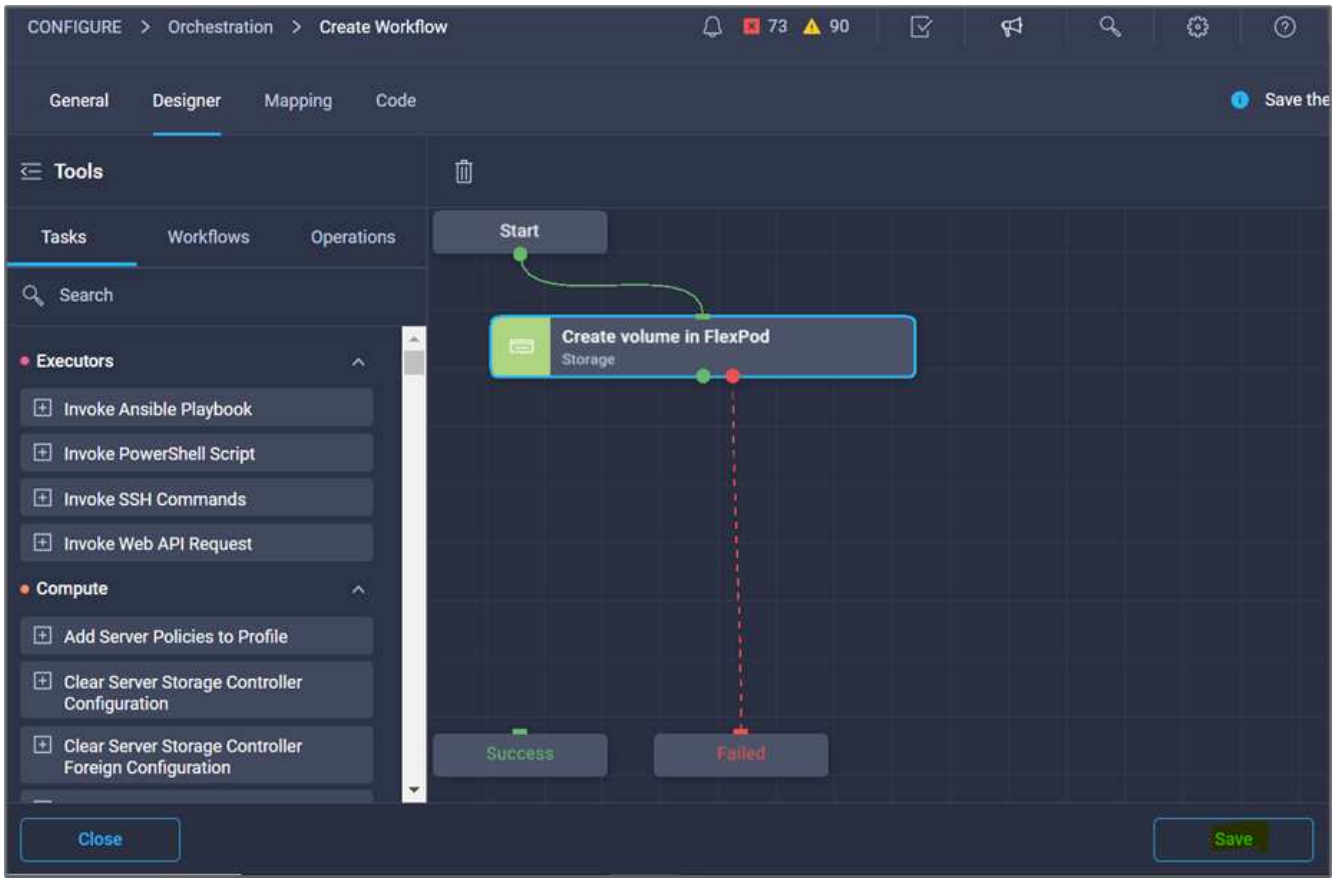
20. Map * 을 클릭합니다.
21. Volume Capacity * 필드에서 * Map * 을 클릭합니다.
22. 직접 매핑 * 을 선택하고 * 워크플로 입력 * 을 클릭합니다.
23. 입력 이름 * 을 클릭하고 * 워크플로 입력 생성 * 을 클릭합니다.



24. 입력 추가 마법사에서 다음을 수행합니다.
    a. 표시 이름과 참조 이름을 입력합니다(선택 사항).
    b. 필수 * 를 클릭합니다.
    c. Type * 에서 * 스토리지 용량 * 을 선택합니다.
    d. Set Default Value(기본값 설정) 및 Override(무시) * 를 클릭합니다.
    e. 볼륨 크기 및 단위에 대한 기본값을 제공합니다.
    f. 추가 * 를 클릭합니다.



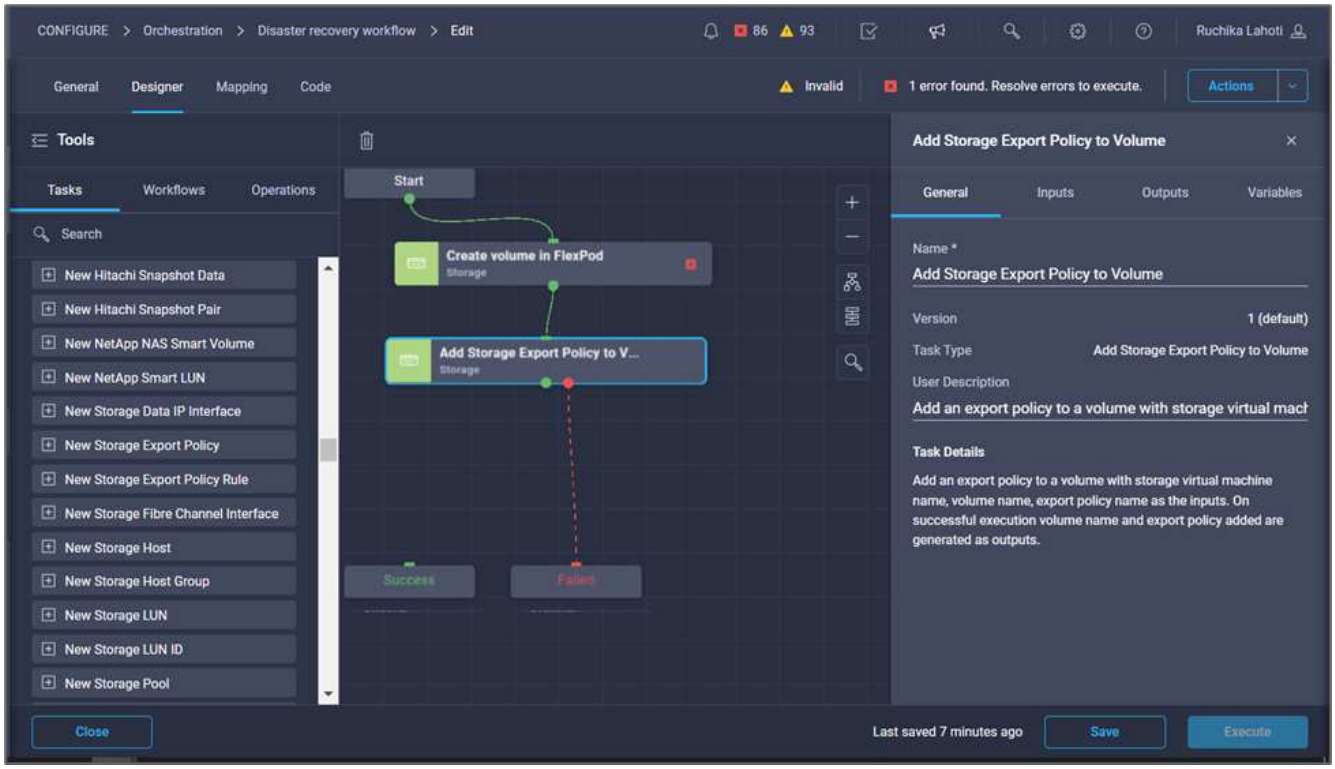
25. Map * 을 클릭합니다.
26. 커넥터를 사용하여 * 시작 * 과 * FlexPod * 에서 볼륨 만들기 작업 사이에 연결을 만들고 * 저장 * 을 클릭합니다.



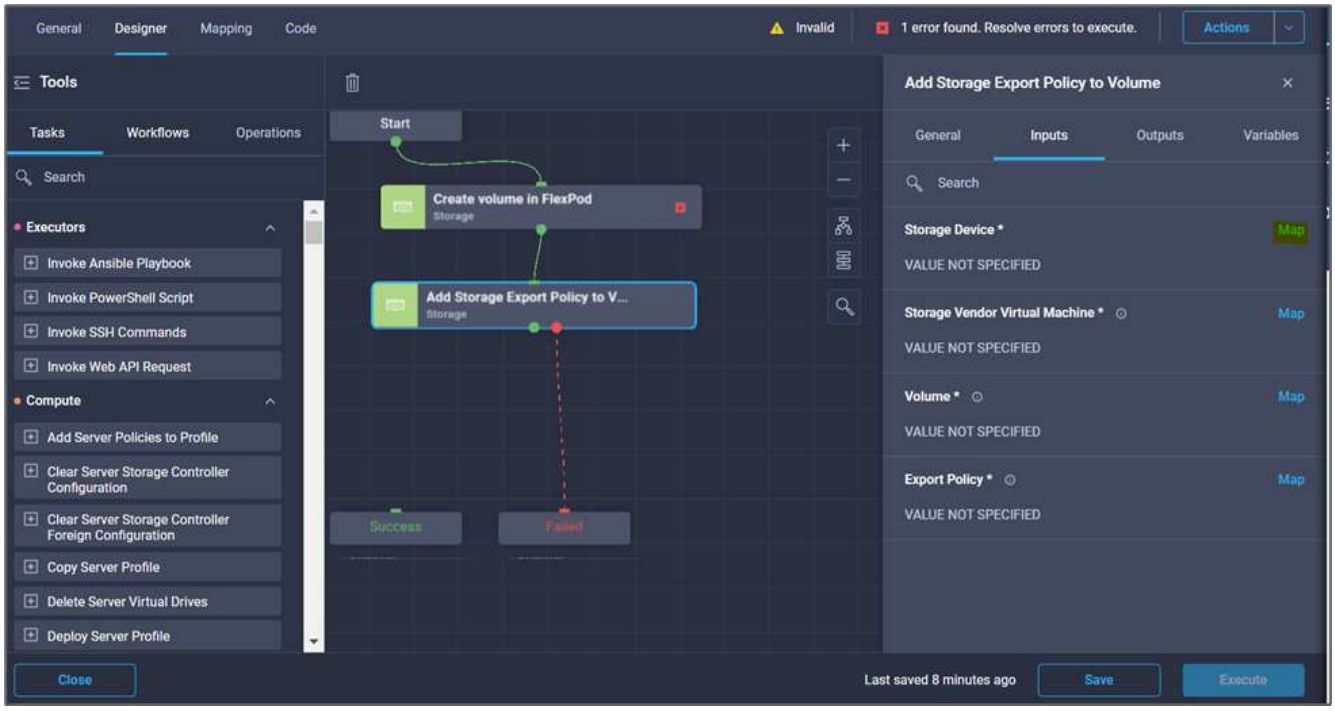
지금 오류를 무시합니다. 이 오류는 성공적인 전환을 지정하는 데 필요한 * FlexPod * 에서 볼륨 생성 * 및 * 성공 * 작업 사이에 연결이 없기 때문에 표시됩니다.

절차 **3:** 스토리지 엑스포트 정책 추가

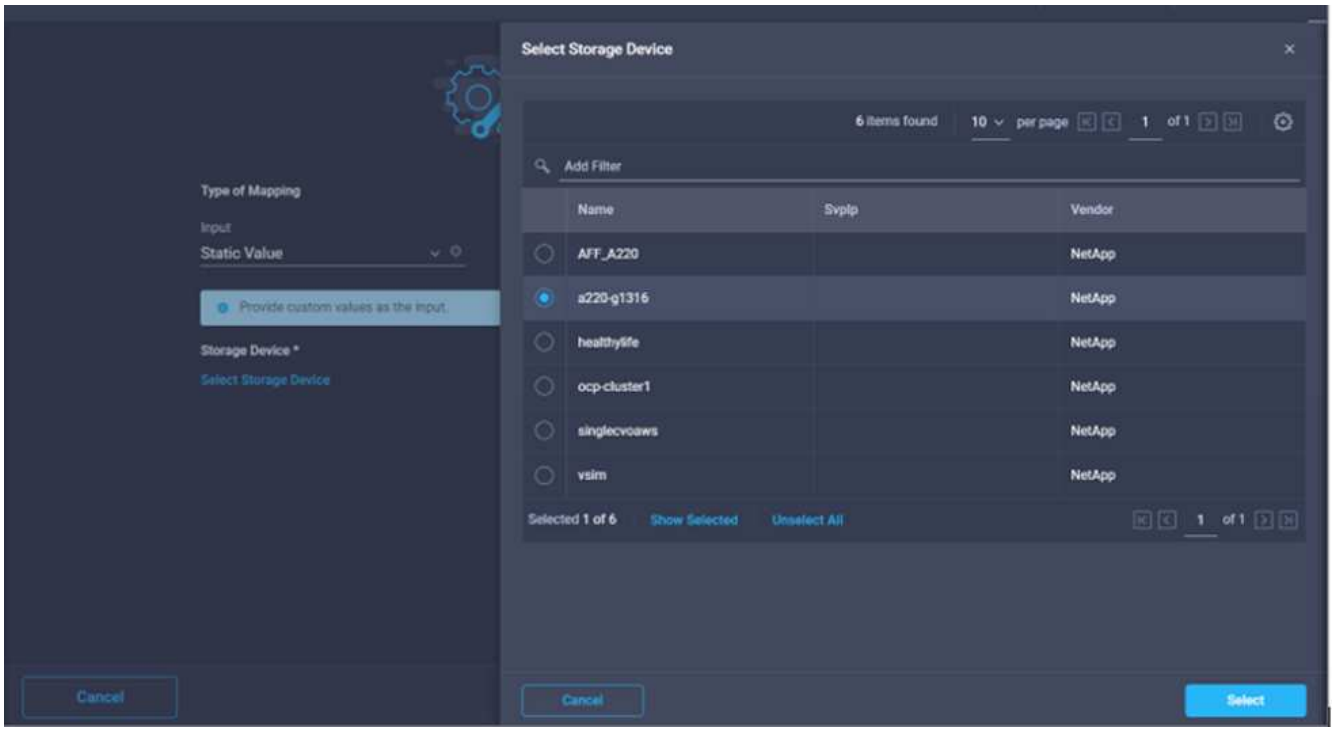
1. 디자이너 * 탭으로 이동하고 * 도구 * 섹션에서 * 작업 * 을 클릭합니다.
2. Design * 영역의 * Tools * 섹션에서 * Storage > Add Storage Export Policy to Volume * 작업을 끌어서 놓습니다.
3. 볼륨에 스토리지 내보내기 정책 추가 * 를 클릭합니다. 작업 속성 * 영역에서 * 일반 * 탭을 클릭합니다. 필요에 따라 이 작업의 이름과 설명을 변경할 수 있습니다. 이 예에서 작업 이름은 스토리지 내보내기 정책 추가 입니다.
4. 커넥터를 사용하여 작업 * FlexPod * 에서 볼륨 생성 및 * 스토리지 내보내기 정책 추가 * 간에 연결을 설정합니다. 저장 * 을 클릭합니다.



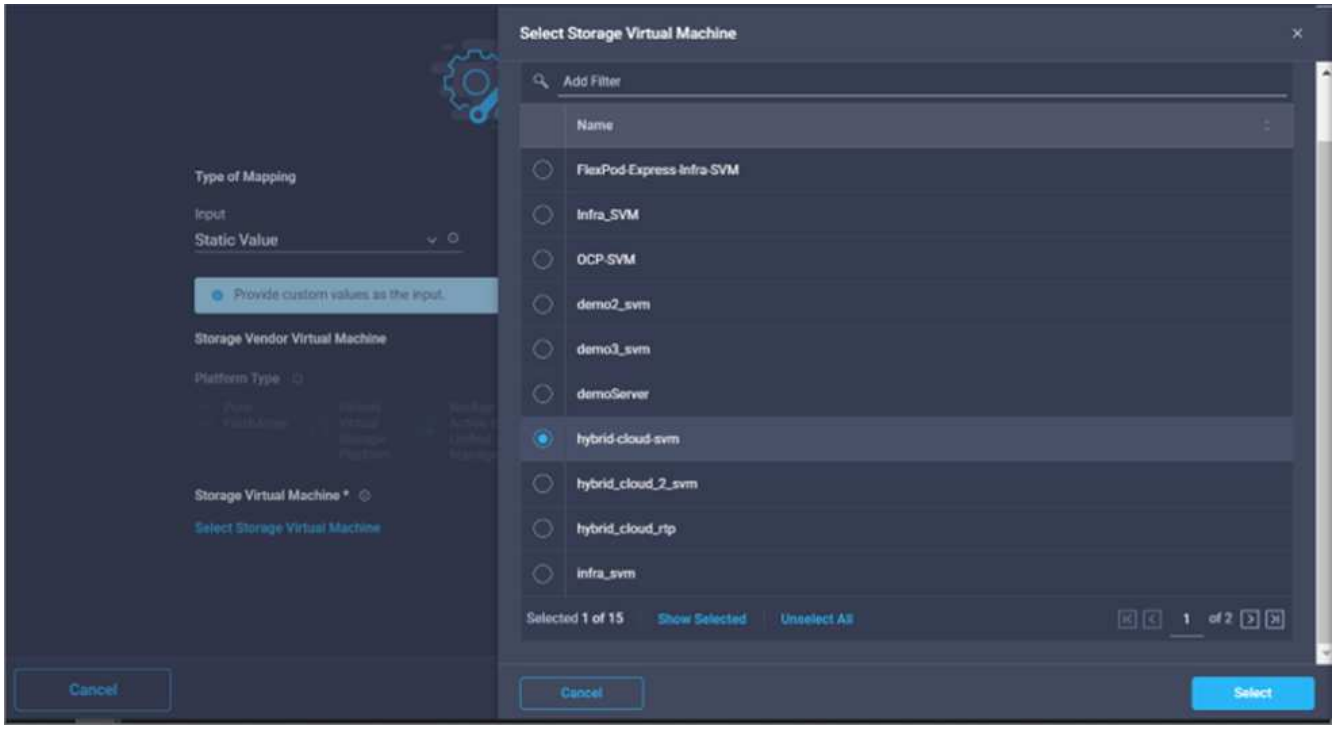
5. 작업 속성 * 영역에서 * 입력 * 을 클릭합니다.
6. Storage Device * 필드에서 * Map * 을 클릭합니다.



7. 정적 값 * 을 선택하고 * 저장 장치 선택 * 을 클릭합니다. 새 스토리지 볼륨을 생성하는 이전 작업을 생성하는 동안 추가한 동일한 스토리지 타겟을 선택합니다.
8. Map * 을 클릭합니다.

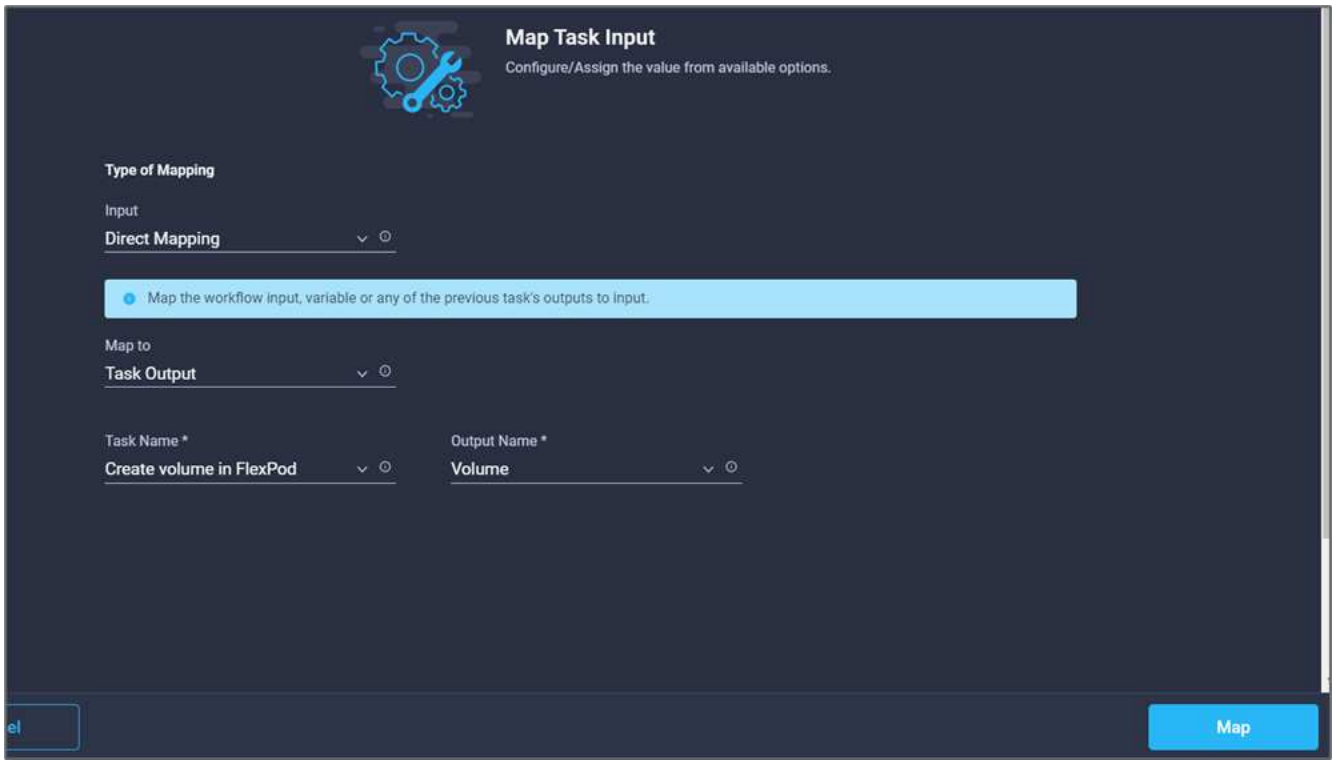


9. Storage Vendor Virtual Machine * 필드에서 * Map * 을 클릭합니다.
10. 정적 값 * 을 선택하고 * 스토리지 가상 머신 선택 * 을 클릭합니다. 새 스토리지 볼륨을 생성하는 이전 작업을 생성하는 동안 추가한 동일한 스토리지 가상 머신을 선택합니다.

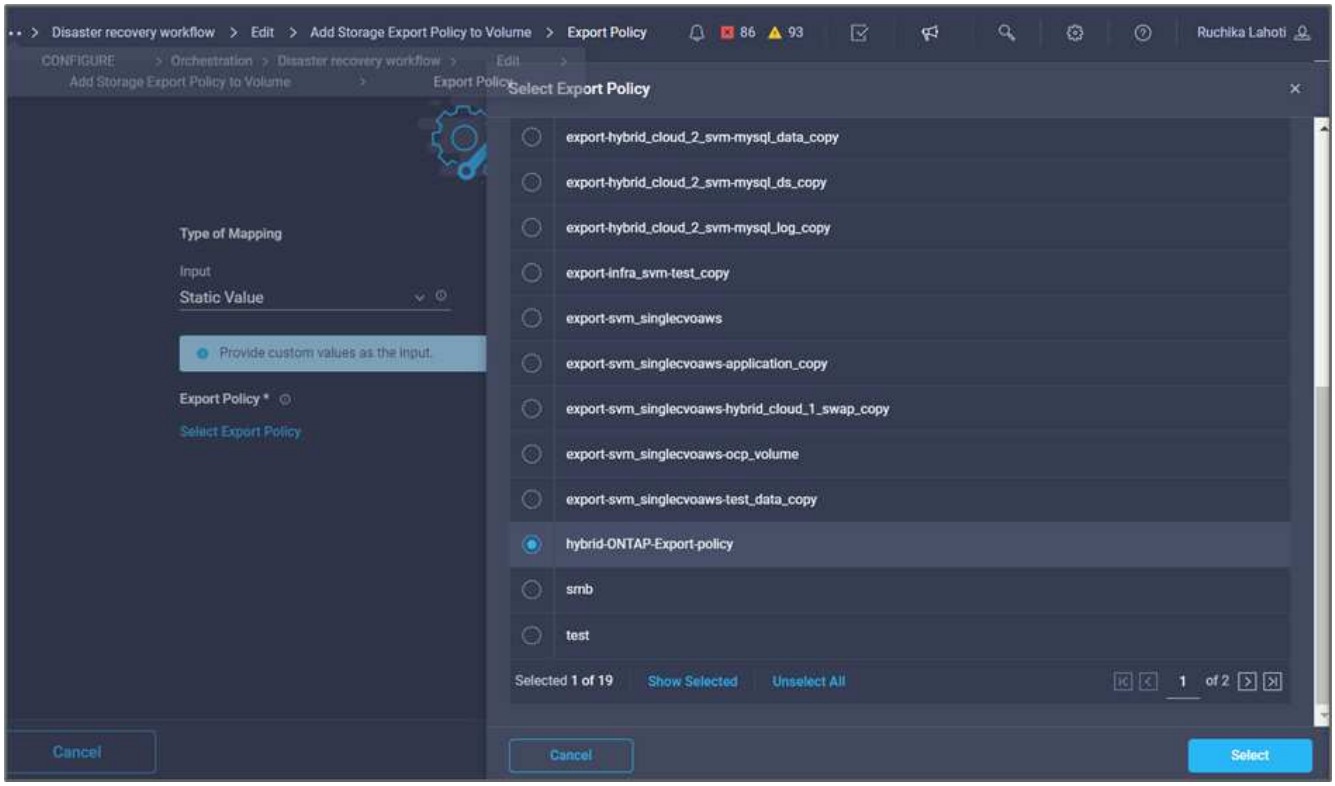


11. Map * 을 클릭합니다.
12. Volume * 필드에서 * Map * 을 클릭합니다.
13. 작업 이름 * 을 클릭한 다음 * FlexPod * 에서 볼륨 생성 을 클릭합니다. 출력 이름 * 을 클릭한 다음 * 볼륨 * 을 클릭합니다.

> Cisco Intersight Cloud Orchestrator에서는 이전 작업의 결과를 새 작업의 입력으로 제공할 수 있습니다. 이 예에서 * 볼륨 * 정보는 * FlexPod * 에서 볼륨 생성 작업에서 * 저장소 내보내기 정책 추가 * 작업에 대한 입력으로 제공되었습니다.



14. Map * 을 클릭합니다.
15. Export Policy * 필드에서 * Map * 을 클릭합니다.
16. 정적 값 * 을 선택하고 * 내보내기 정책 선택 * 을 클릭합니다. 생성된 엑스포트 정책을 선택합니다.

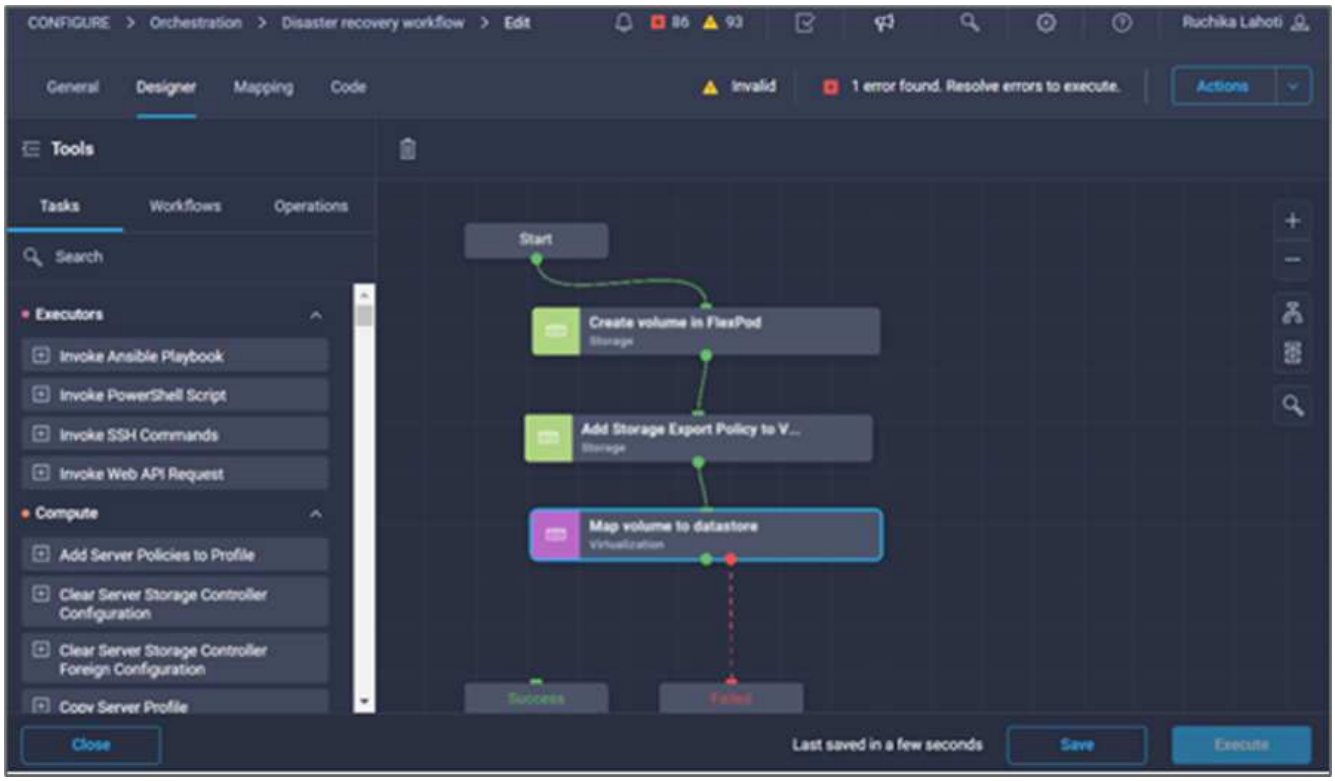


17. 지도 * 를 클릭한 다음 * 저장 * 을 클릭합니다.

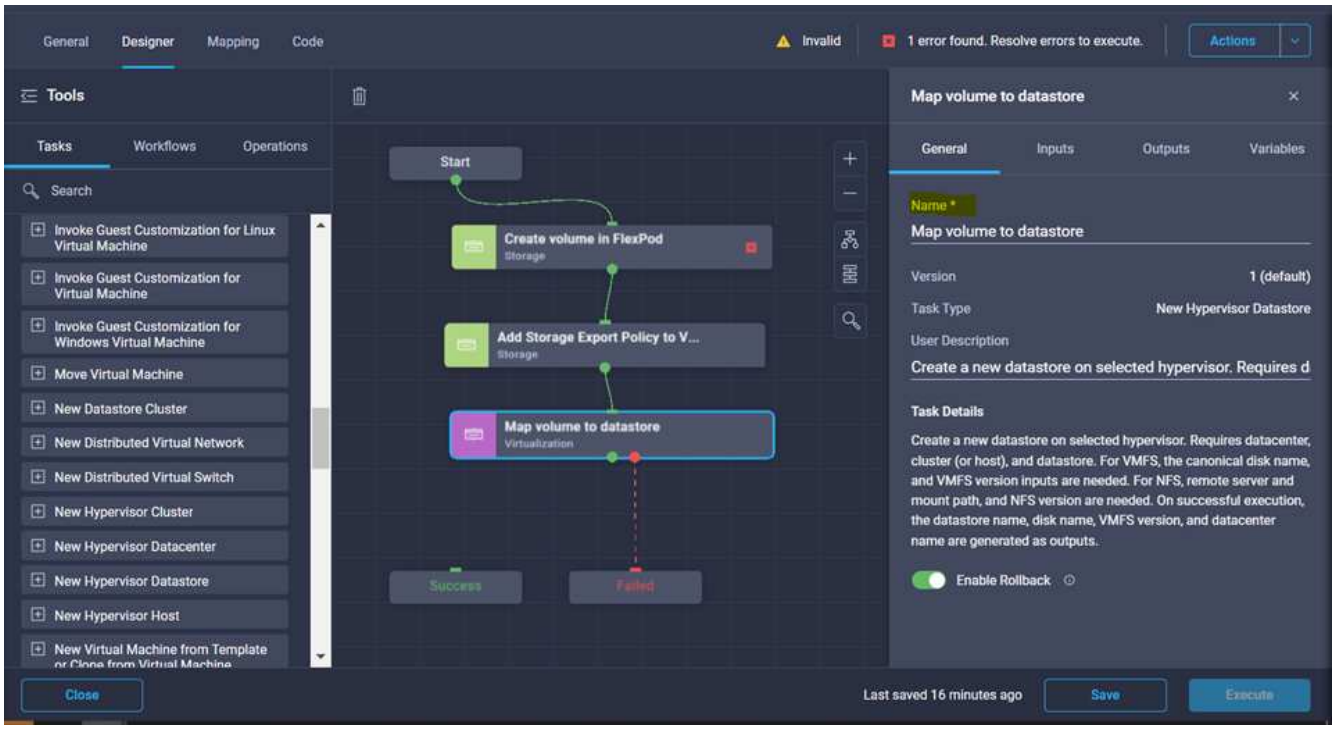
그러면 볼륨에 엑스포트 정책이 추가됩니다. 그런 다음 생성된 볼륨을 매핑하는 새 데이터 저장소를 생성합니다.

절차 **4: FlexPod** 볼륨을 데이터 저장소에 매핑

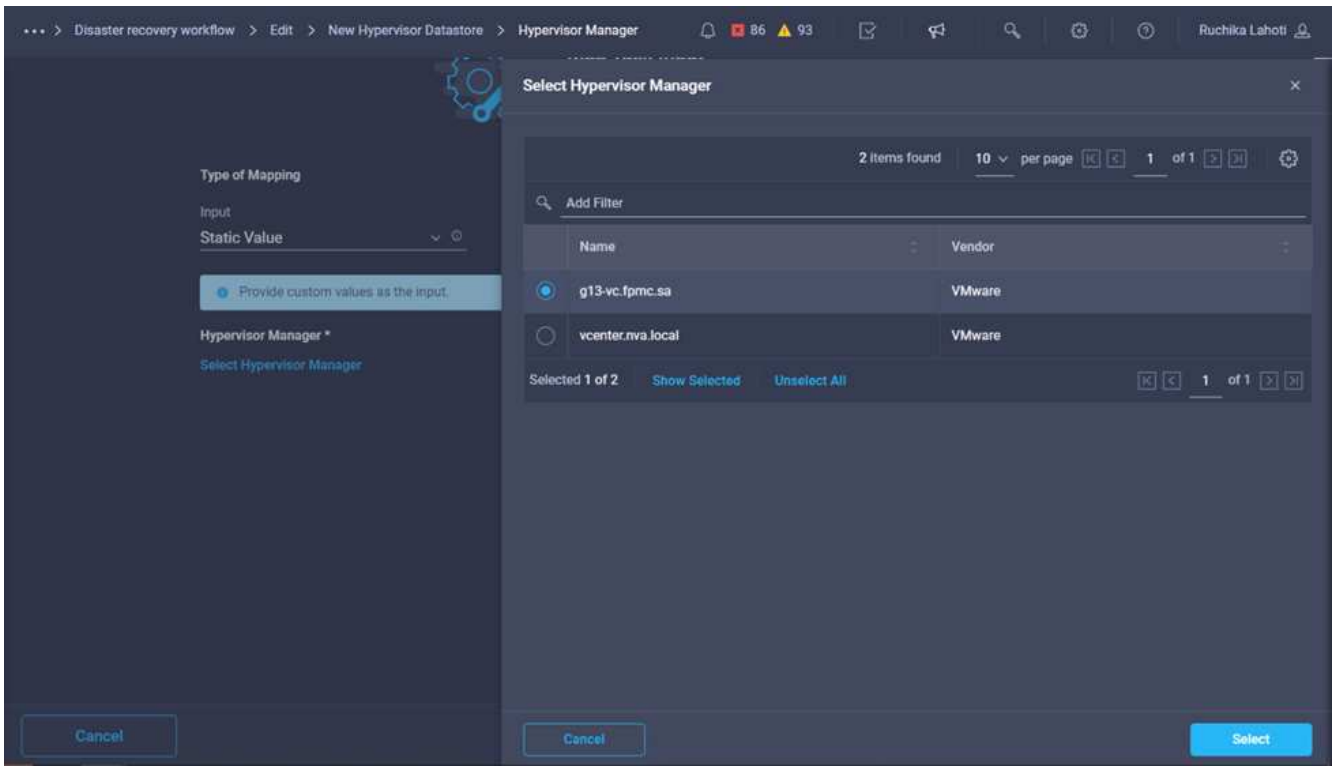
1. 디자이너 * 탭으로 이동하고 * 도구 * 섹션에서 * 작업 * 을 클릭합니다.
2. Design * 영역의 * Tools * 섹션에서 * Virtualization > New Hypervisor Datastore * 작업을 끌어다 놓습니다.
3. Connector를 사용하여 * Add Storage Export Policy * 와 * New Hypervisor Datastore * 작업을 연결합니다. 저장 * 을 클릭합니다.



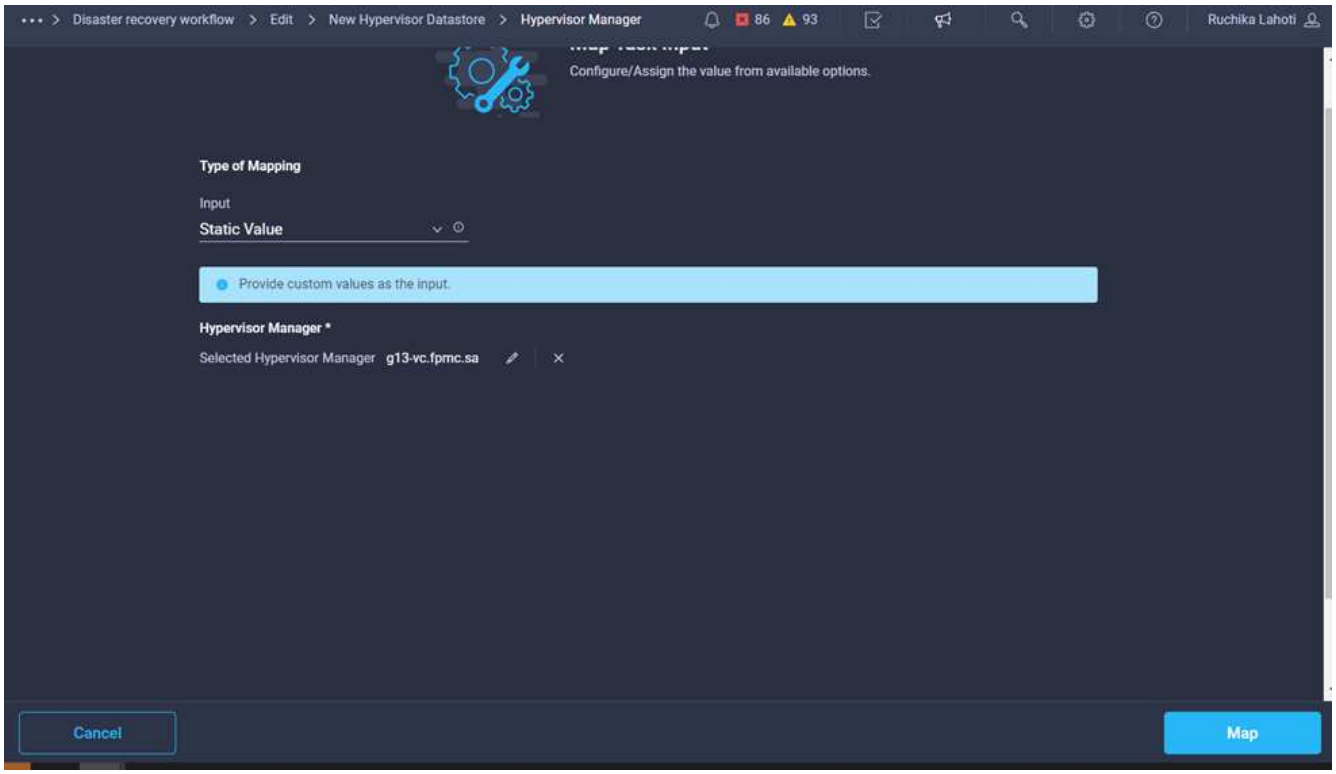
4. New Hypervisor Datastore * 를 클릭합니다. 작업 속성 * 영역에서 * 일반 * 탭을 클릭합니다. 필요에 따라 이 작업의 이름과 설명을 변경할 수 있습니다. 이 예에서 작업 이름은 * 데이터 저장소에 볼륨 매핑 * 입니다.



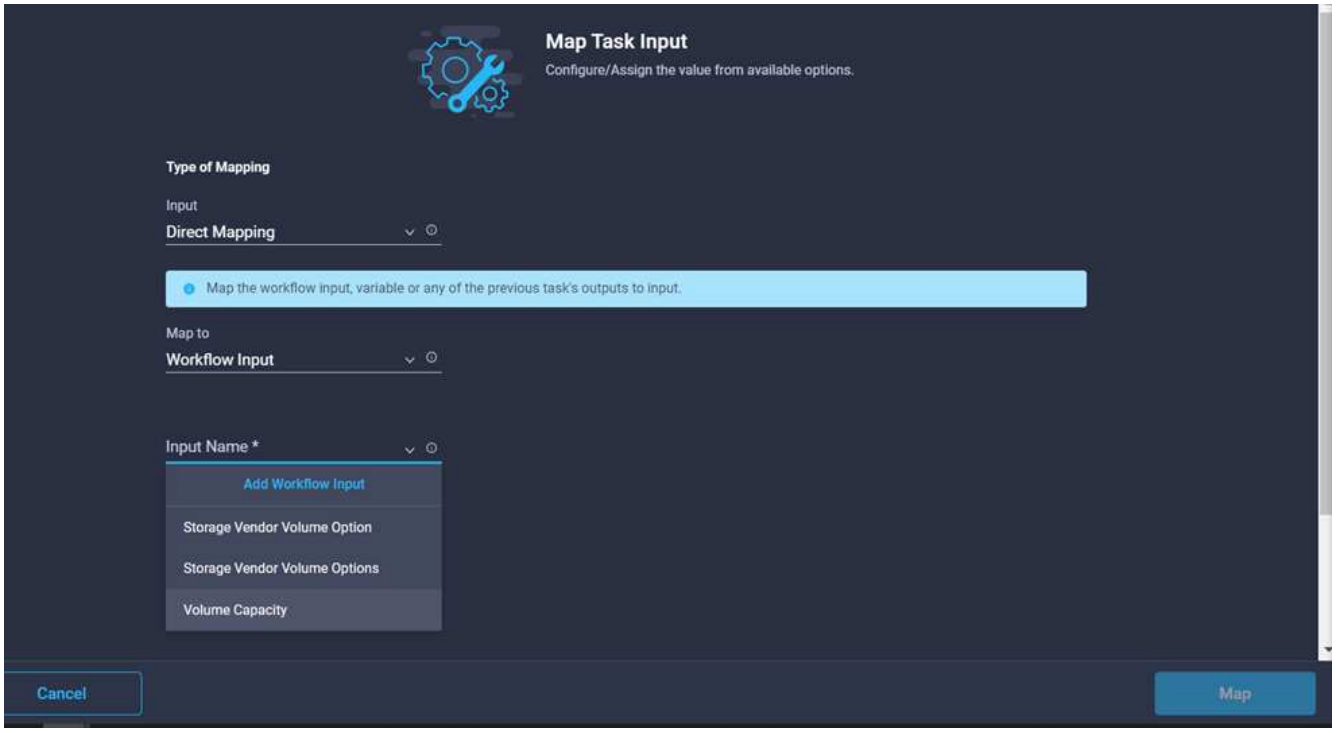
5. 작업 속성 * 영역에서 * 입력 * 을 클릭합니다.
6. 하이퍼바이저 관리자 * 필드에서 * 맵 * 을 클릭합니다.
7. 정적 값 * 을 선택하고 * 하이퍼바이저 관리자 선택 * 을 클릭합니다. VMware vCenter 타겟을 클릭합니다.



8. Map * 을 클릭합니다.



9. 데이터 센터 * 필드에서 * 맵 * 을 클릭합니다. 새 데이터 저장소와 연결된 데이터 센터입니다.
10. 직접 매핑 * 을 선택하고 * 워크플로 입력 * 을 클릭합니다.
11. 입력 이름 * 을 클릭한 다음 * 워크플로 입력 작성 * 을 클릭합니다.



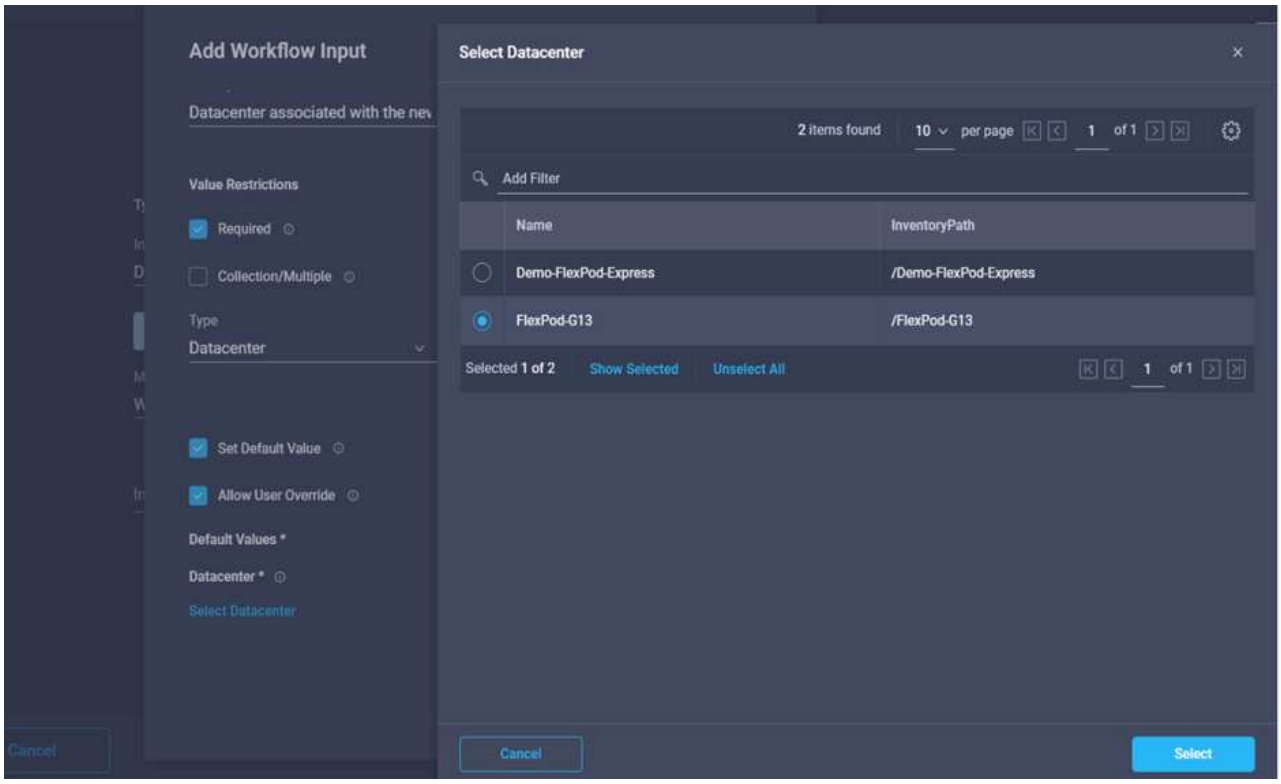
12. 입력 추가 마법사에서 다음 단계를 완료합니다.
    a. 표시 이름과 참조 이름을 입력합니다(선택 사항).

b. 유형으로 * Datacenter * 를 선택합니다.

c. Set Default Value(기본값 설정) 및 Override(무시) * 를 클릭합니다.

d. 데이터 센터 선택 * 을 클릭합니다.

e. 새 데이터 저장소와 연결된 데이터 센터를 클릭한 다음 * Select * 를 클릭합니다.

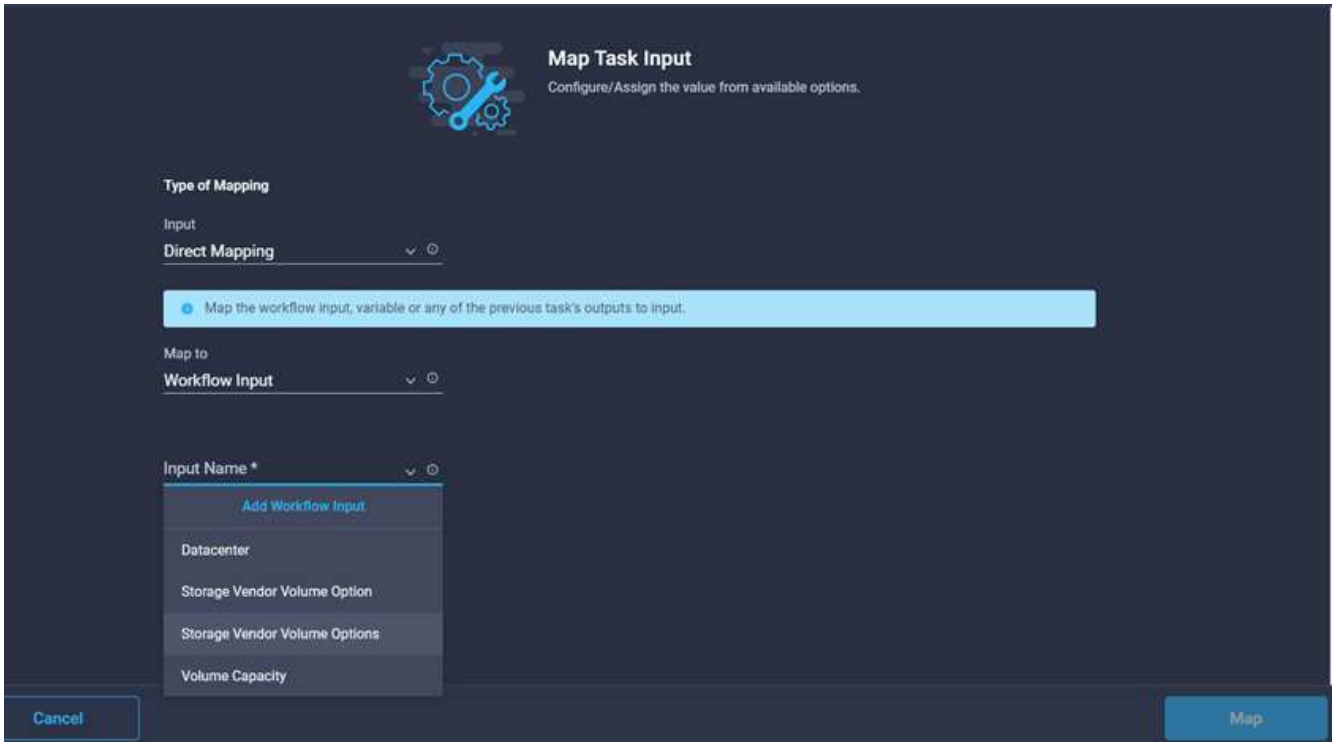


▪ 추가 * 를 클릭합니다.

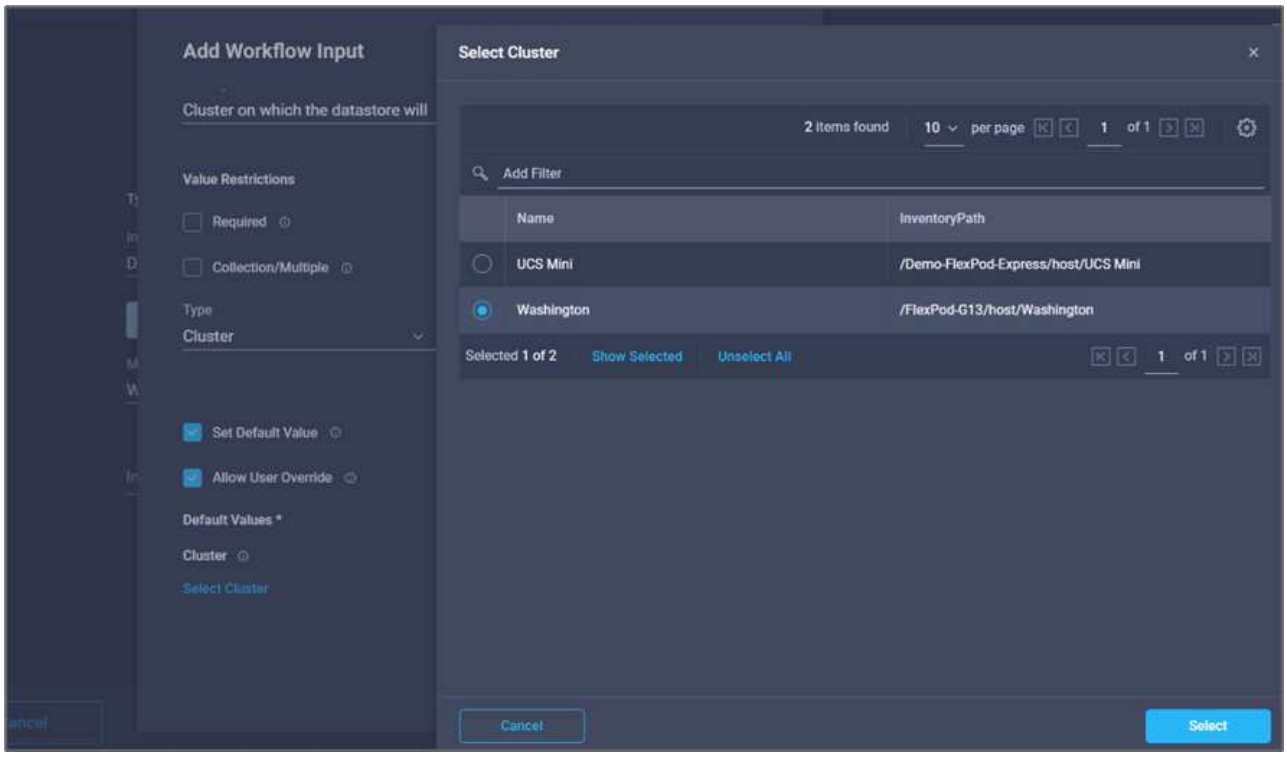
13. Map * 을 클릭합니다.

14. Cluster * 필드에서 * Map * 을 클릭합니다.

15. 직접 매핑 * 을 선택하고 * 워크플로 입력 * 을 클릭합니다.

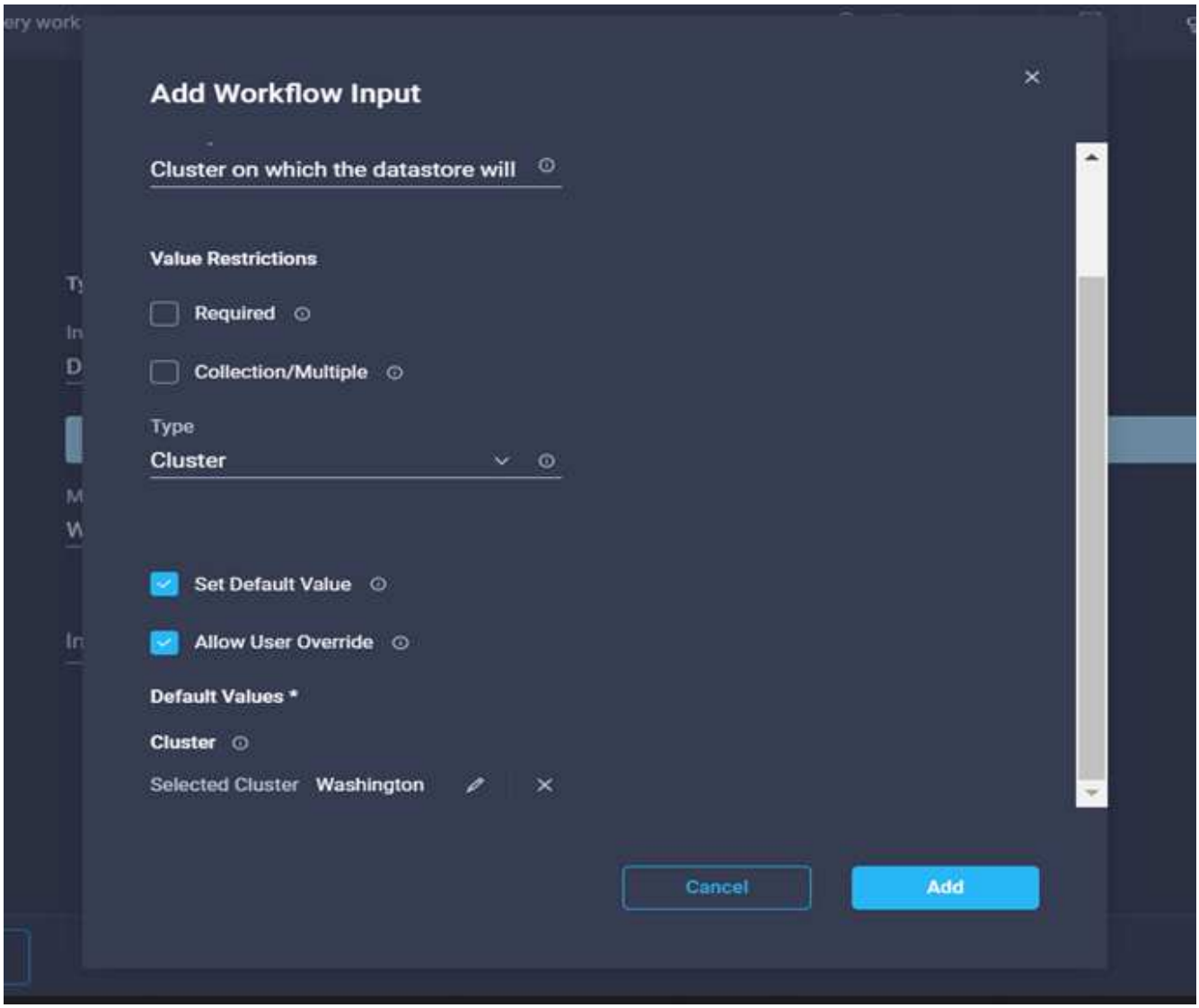


16. 입력 추가 마법사에서 다음 단계를 완료합니다.
    a. 표시 이름과 참조 이름을 입력합니다(선택 사항).
    b. 필수 * 를 클릭합니다.
    c. 유형으로 Cluster(클러스터) 를 선택합니다.
    d. Set Default Value(기본값 설정) 및 Override(무시) * 를 클릭합니다.
    e. Select Cluster * 를 클릭합니다.
    f. 새 데이터 저장소와 연결된 클러스터를 클릭합니다.
    g. 선택 * 을 클릭합니다.

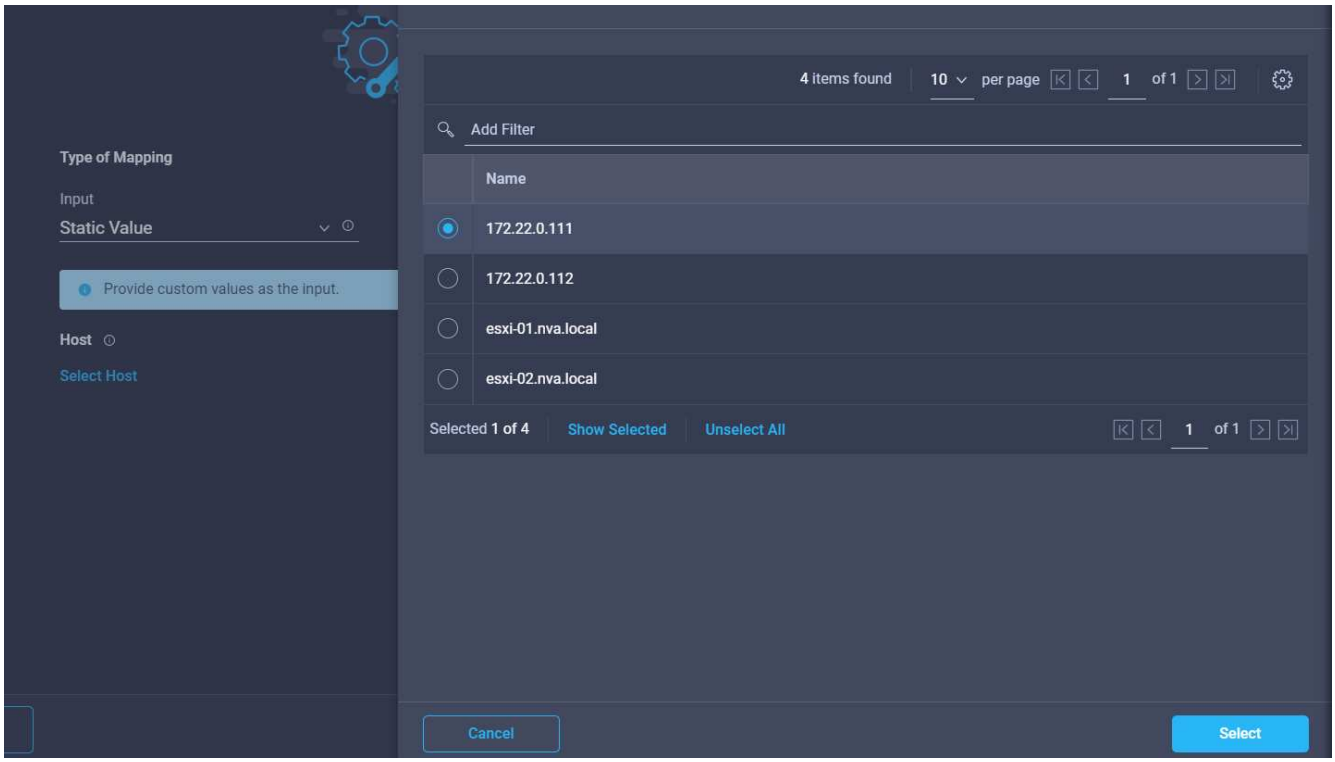


h. 추가 * 를 클릭합니다.

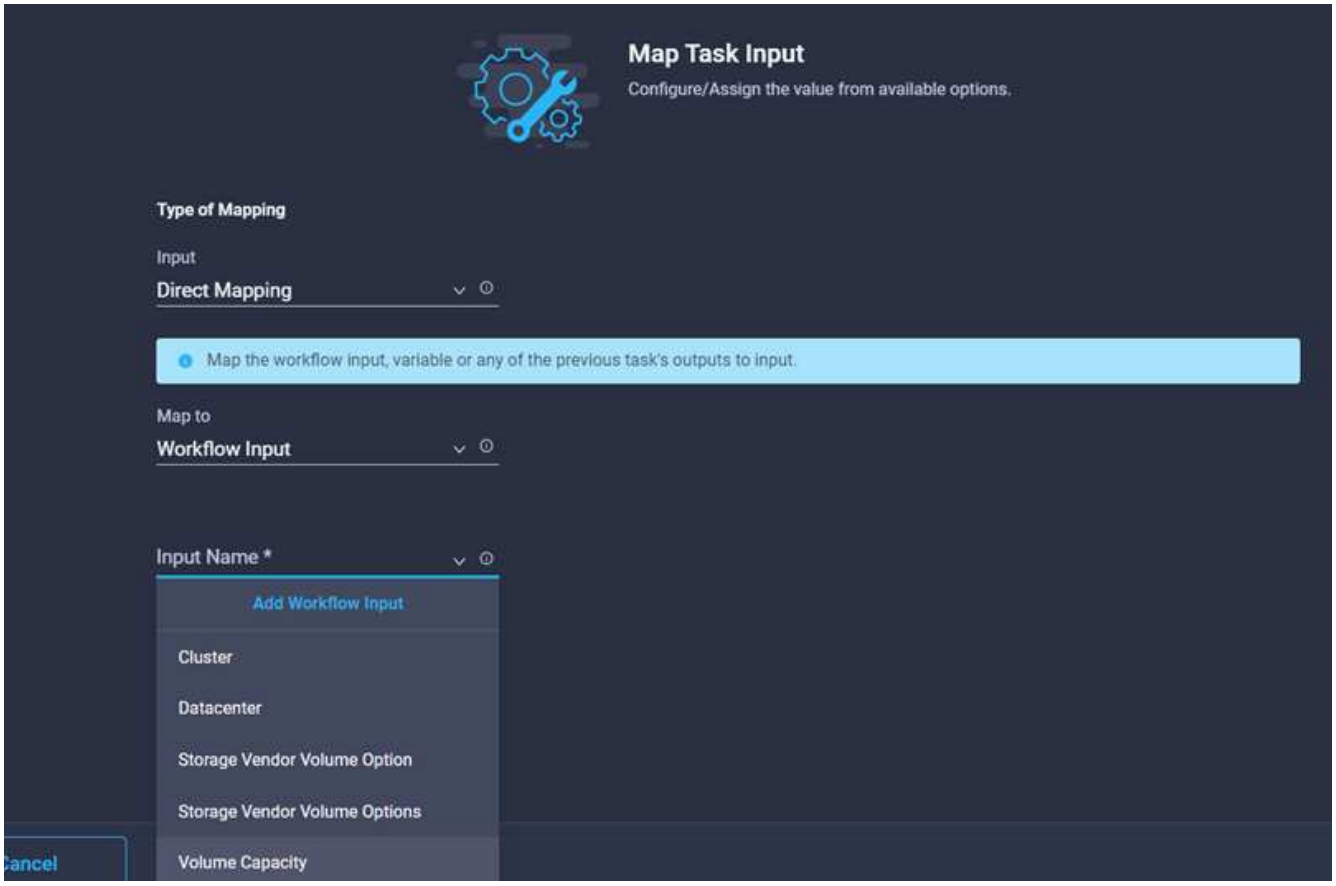
17. Map * 을 클릭합니다.
18. Host * 필드에서 * Map * 을 클릭합니다.



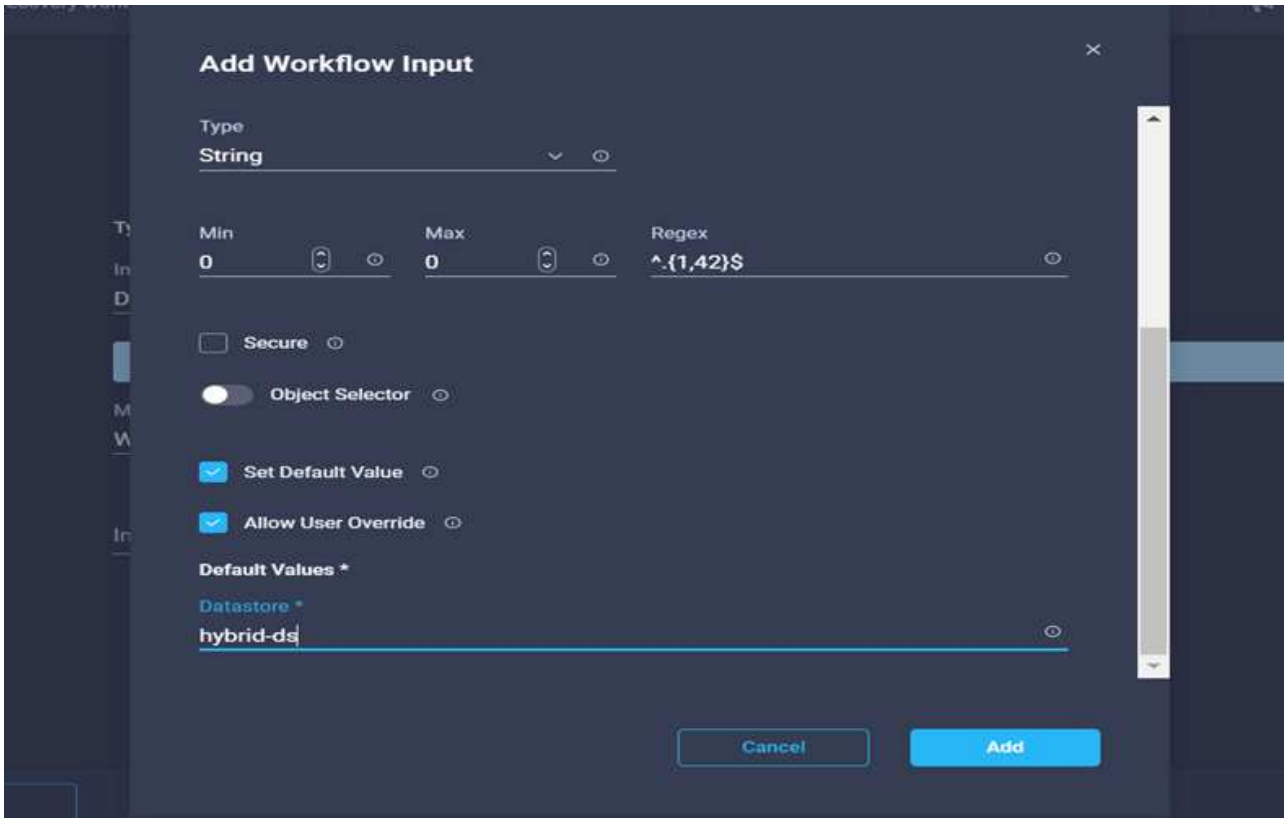
19. 정적 값 * 을 선택하고 데이터 저장소가 호스팅될 호스트를 클릭합니다. 클러스터를 지정하면 호스트가 무시됩니다.



20. 선택 및 매핑 * 을 클릭합니다.
21. Datastore * 필드에서 * Map * 을 클릭합니다.
22. 직접 매핑 * 을 선택하고 * 워크플로 입력 * 을 클릭합니다.
23. 입력 이름 * 을 클릭하고 * 워크플로 입력 생성 * 을 클릭합니다.



24. 입력 추가 마법사에서 다음을 수행합니다.
    a. 표시 이름과 참조 이름을 입력합니다(선택 사항).
    b. 필수 * 를 클릭합니다.
    c. Set Default Value(기본값 설정) 및 Override(무시) * 를 클릭합니다.
    d. 데이터 저장소에 대한 기본값을 제공하고 * Add * 를 클릭합니다.

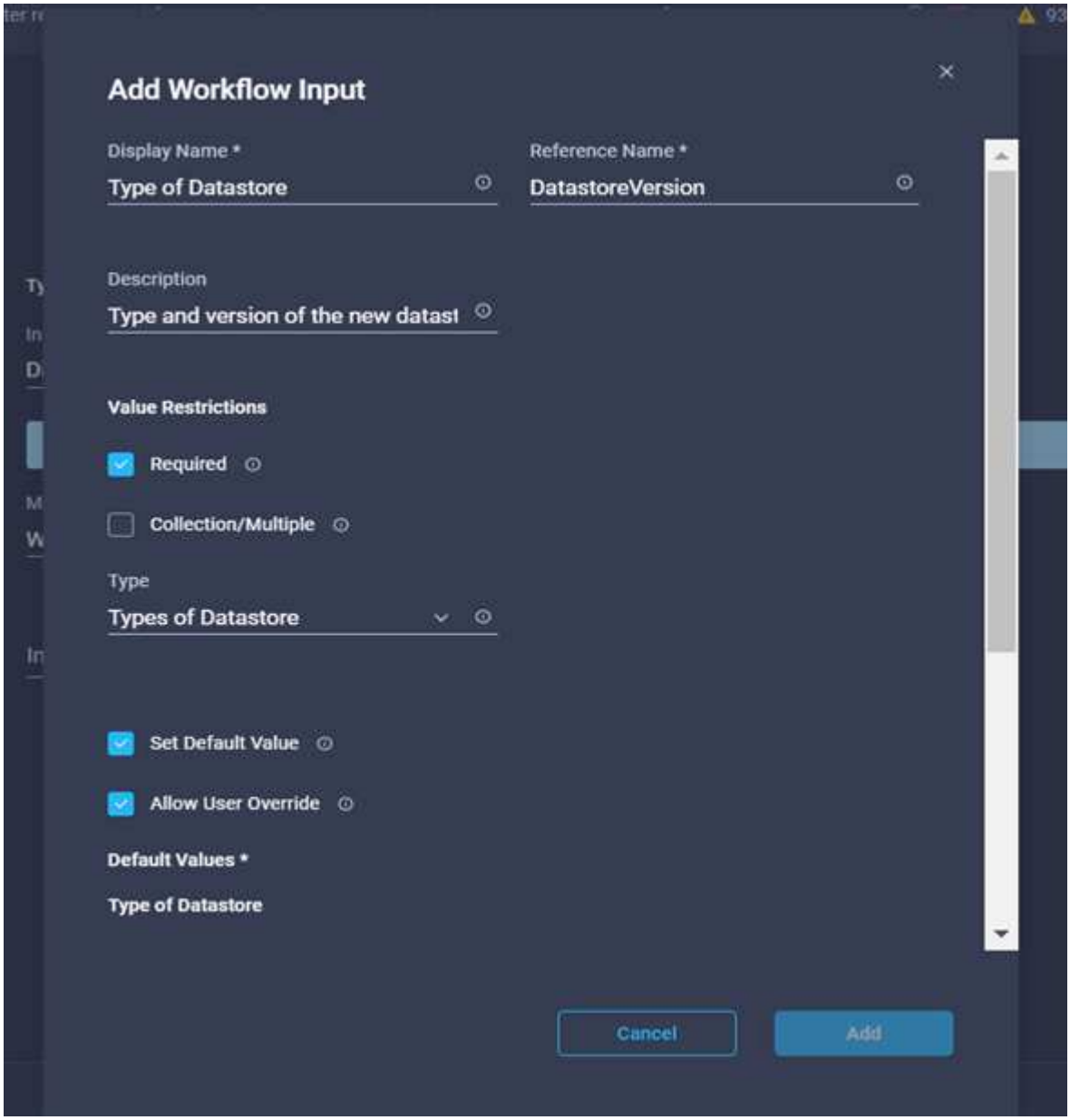


25. Map * 을 클릭합니다.
26. 입력 필드에서 * Map * 을 클릭합니다 * 데이터 저장소 유형 *.
27. 직접 매핑 * 을 선택하고 * 워크플로 입력 * 을 클릭합니다.
28. 입력 이름 * 을 클릭하고 * 워크플로 입력 생성 * 을 클릭합니다.



29. 입력 추가 마법사에서 다음 단계를 완료합니다.
    a. 표시 이름 및 참조 이름(선택 사항)을 입력하고 * 필수 * 를 클릭합니다.

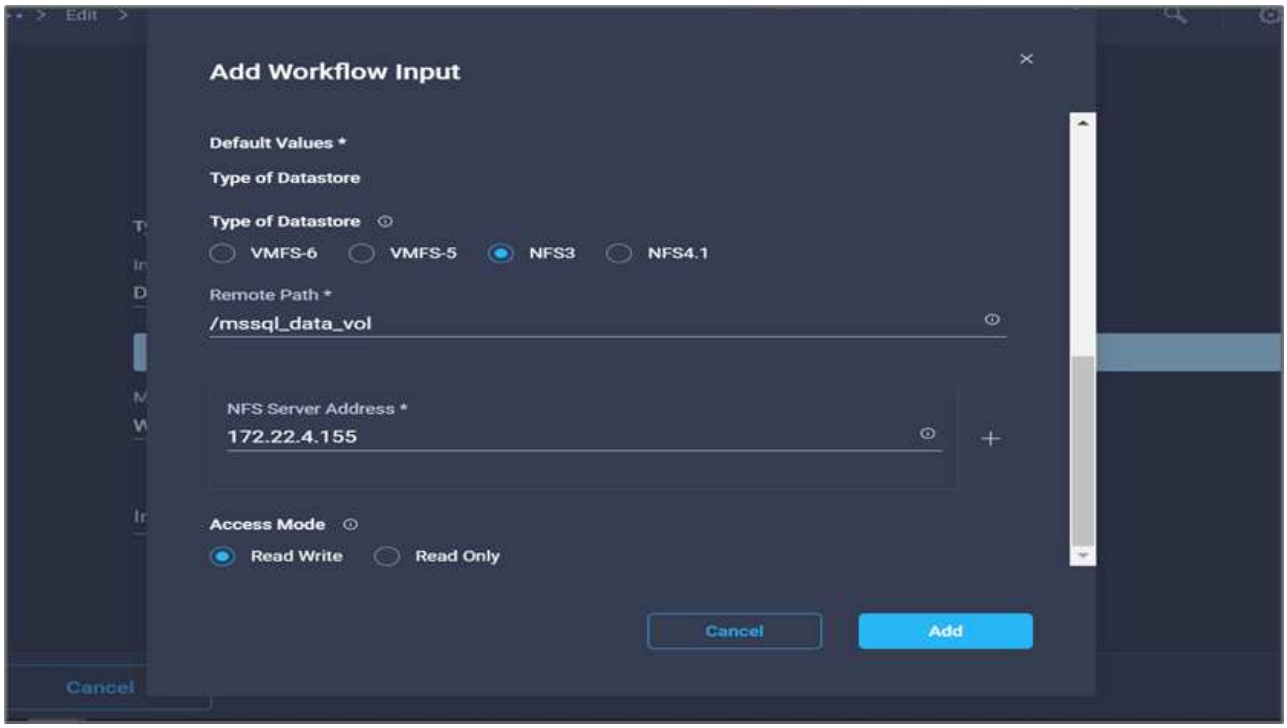
b. 데이터 저장소 유형 * 을 선택하고 * 기본값 설정 및 재정의 * 를 클릭합니다.



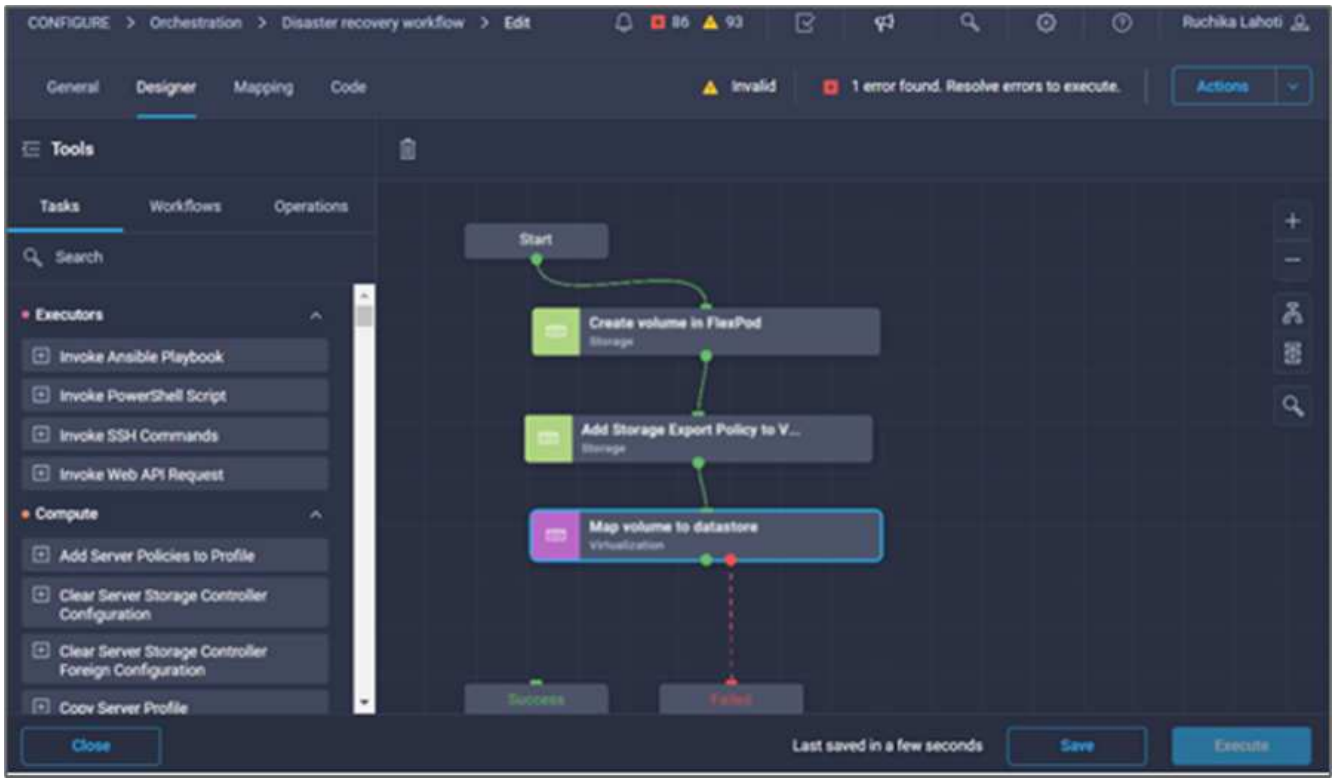
c. 원격 경로를 제공합니다. NFS 마운트 지점의 원격 경로입니다.

d. NFS 서버 주소 에 원격 NFS 서버의 호스트 이름 또는 IP 주소를 입력합니다.

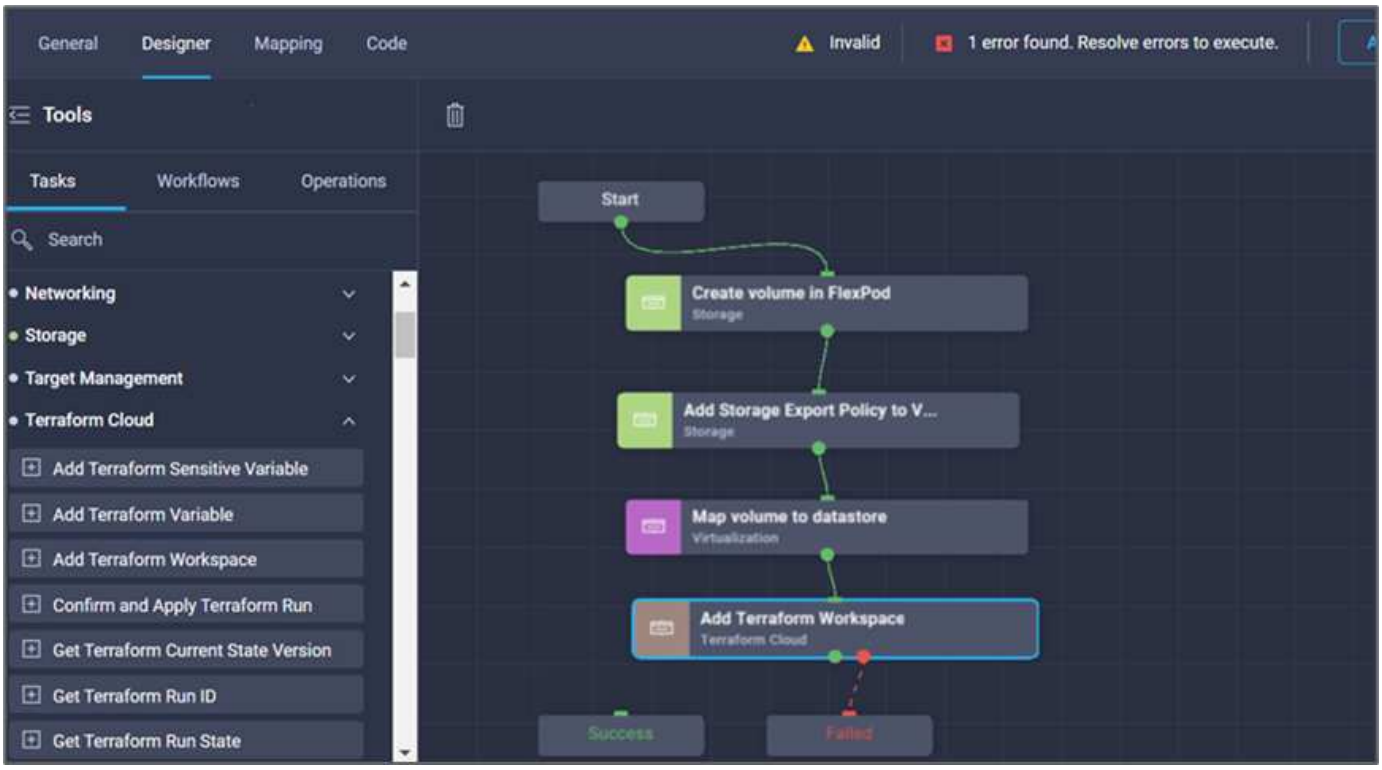
e. 액세스 모드 * 를 클릭합니다. 액세스 모드는 NFS 서버에 대한 것입니다. 볼륨을 읽기 전용으로 내보내는 경우 읽기 전용 을 클릭합니다. 추가 * 를 클릭합니다.



30. Map * 을 클릭합니다.
31. 저장 * 을 클릭합니다.

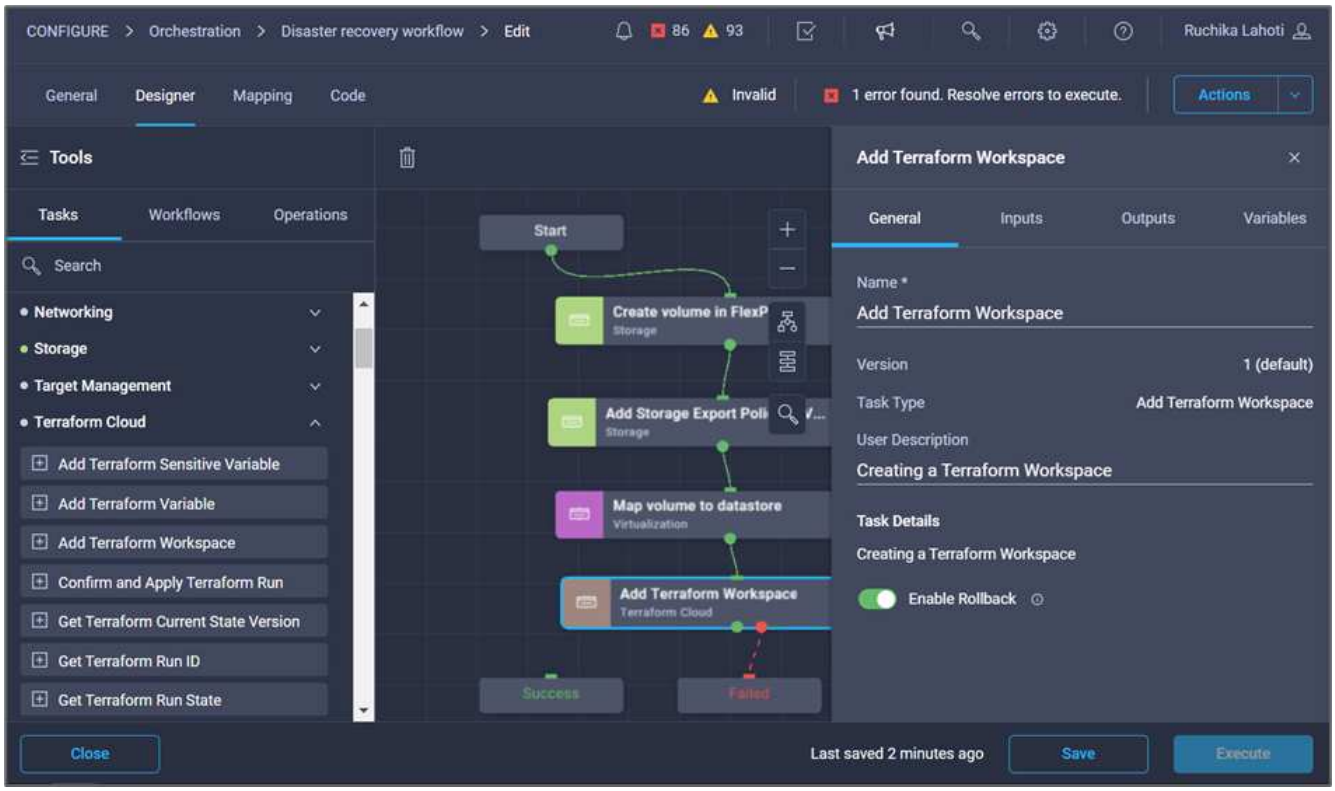


이것으로 데이터 저장소 생성 작업이 완료되었습니다. 사내 FlexPod 데이터 센터에서 수행한 모든 작업이 완료됩니다.

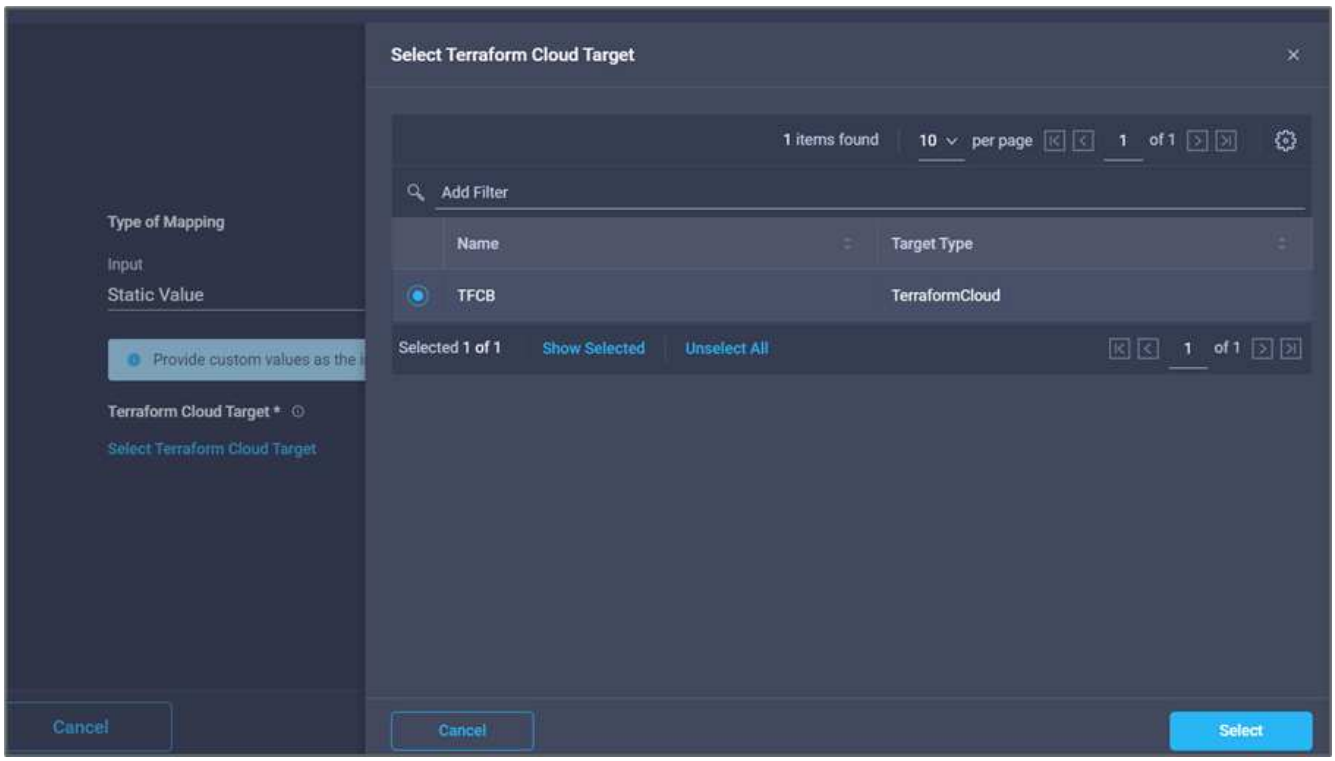


절차 **5:** 새 **Terraform** 작업 영역을 추가합니다

1. 디자이너 * 탭으로 이동하고 * 도구 * 섹션에서 * 작업 * 을 클릭합니다.
2. 디자인 영역의 도구 섹션에서 * Terraform Cloud > Terraform Workspace * 작업 추가를 끌어서 놓습니다.
3. Connector를 사용하여 * Map 볼륨을 Datastore * 에 연결하고 * Terraform Workspace * 작업을 추가하고 * Save * 를 클릭합니다.
4. Terraform Workspace 추가 * 를 클릭합니다. 작업 속성 영역에서 * 일반 * 탭을 클릭합니다. 필요에 따라 이 작업의 이름 및 설명을 변경할 수 있습니다.

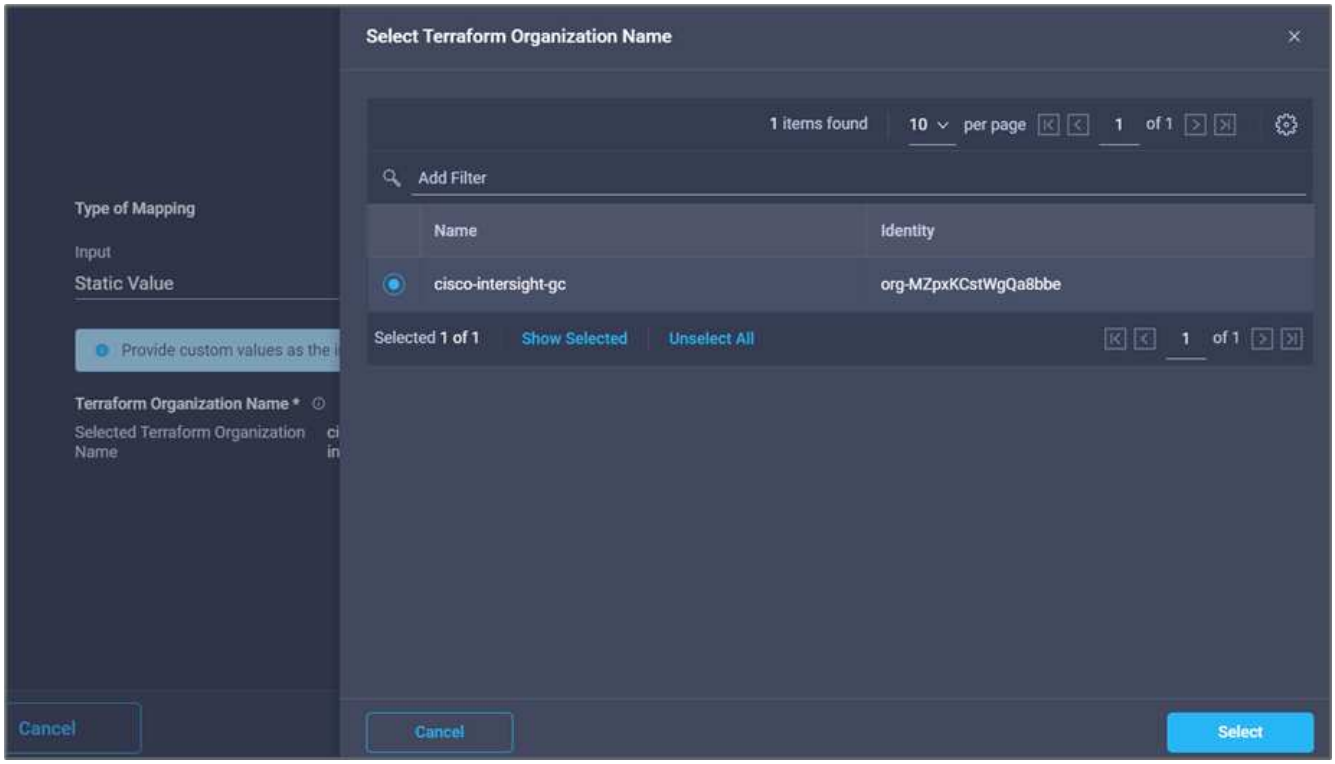


5. 작업 속성 영역에서 * 입력 * 을 클릭합니다.
6. 입력 필드 * Terraform Cloud Target * 에서 * Map * 을 클릭합니다.
7. 정적 값 * 을 선택하고 * 클라우드 타겟 선택 * 을 클릭합니다. 에 설명된 대로 추가한 Terraform Cloud for Business 계정을 선택합니다 "HaashCorp Terraform에 대한 Cisco Intersight 서비스를 구성합니다"".

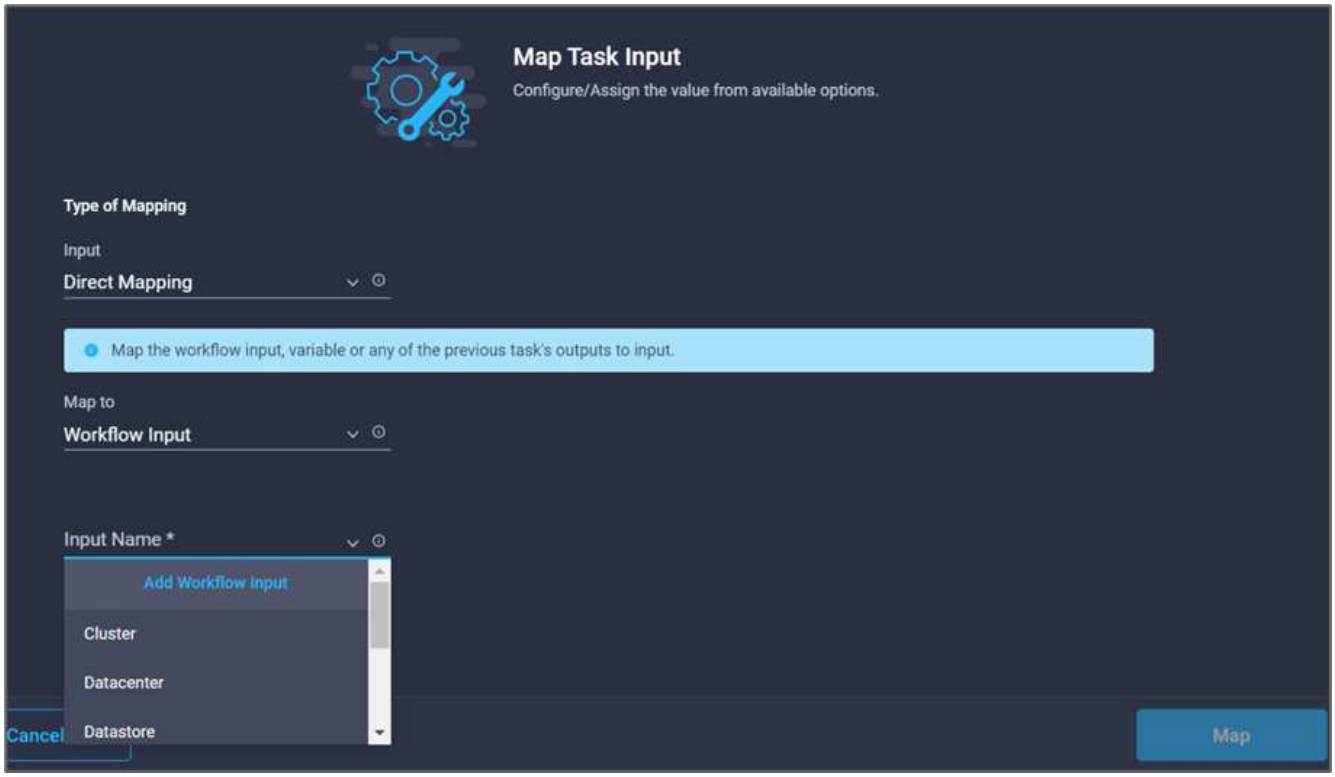


8. Map * 을 클릭합니다.

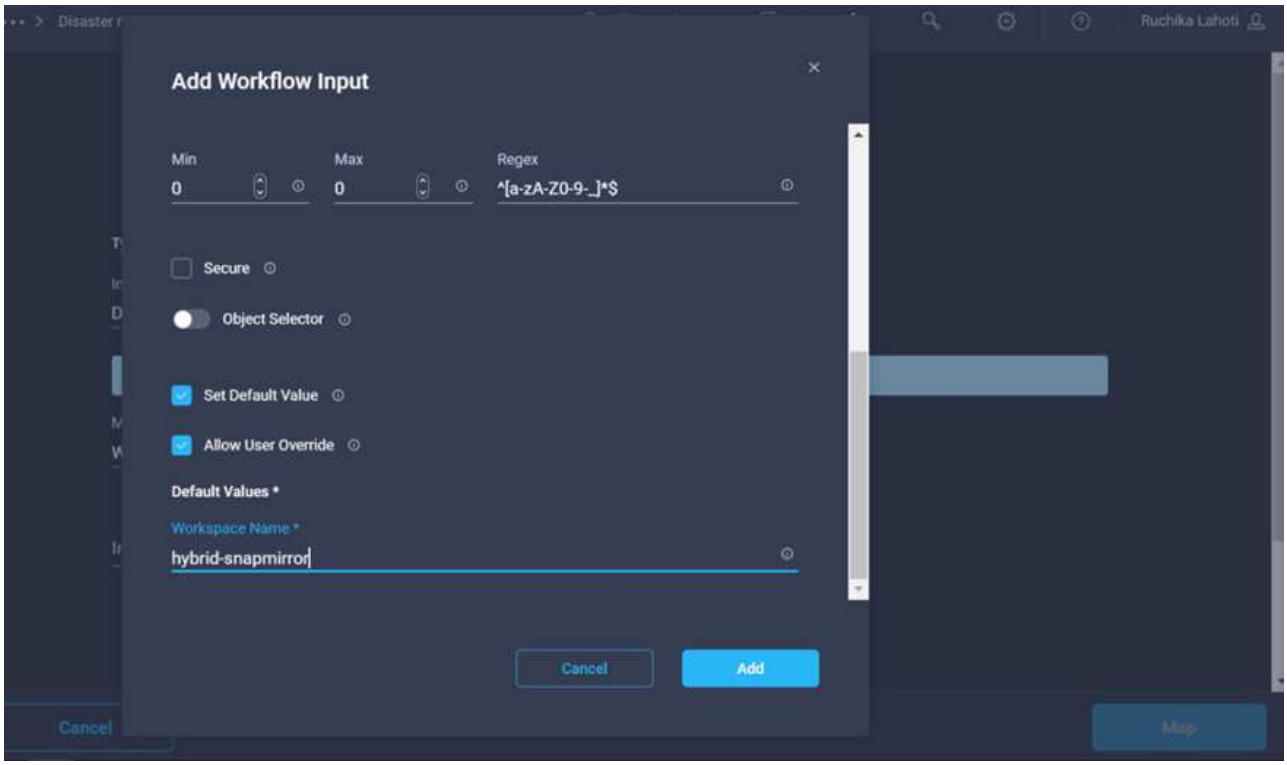
9. 입력 필드 * Terraform 조직 이름 * 에서 * Map * 을 클릭합니다.
10. 정적 값 * 을 선택한 다음 * 조직 구조 선택 * 을 클릭합니다. Terraform Cloud for Business 계정에 속해 있는 Terraform 조직의 이름을 선택합니다.



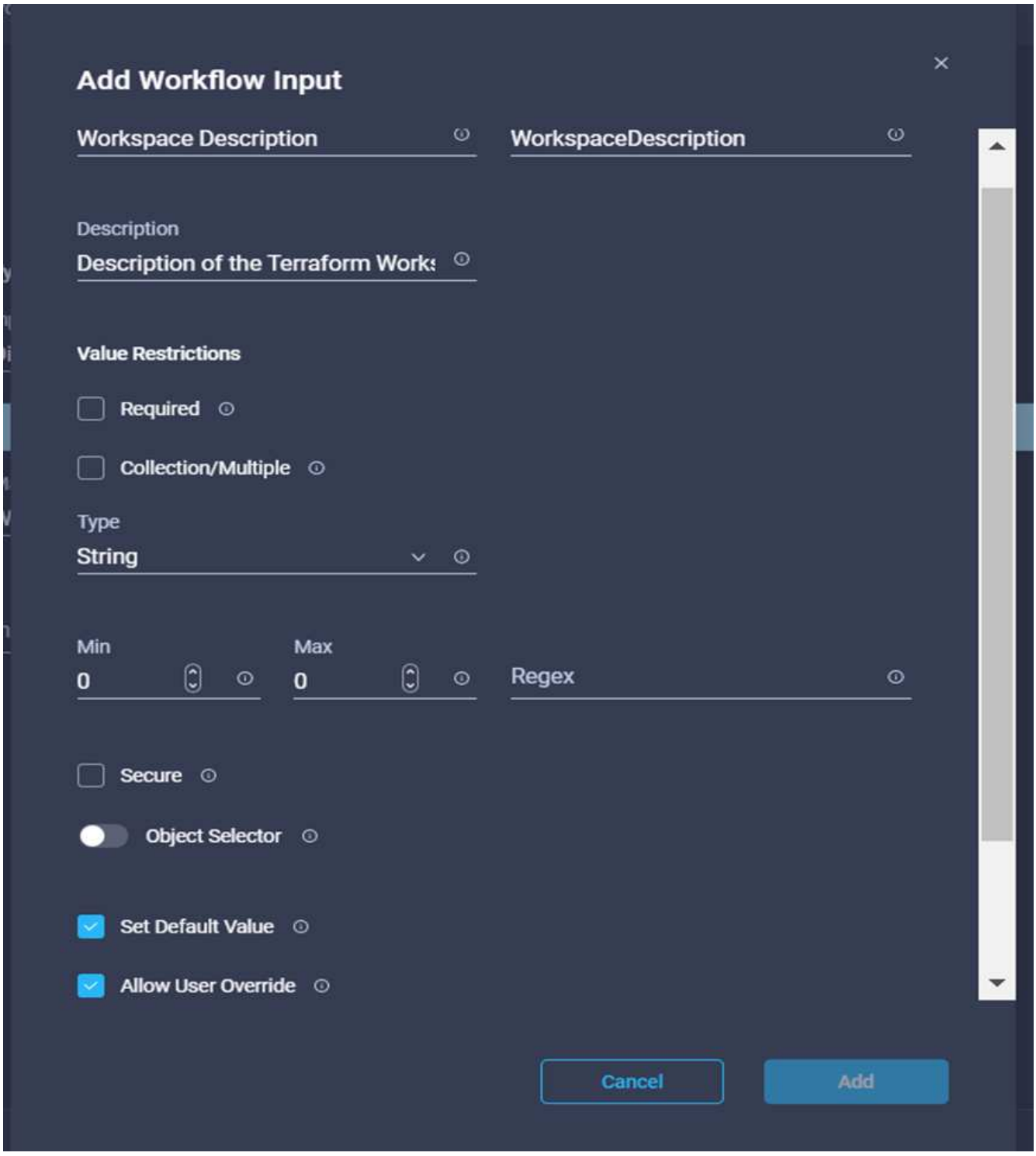
11. Map * 을 클릭합니다.
12. Terraform Workspace Name * 필드에서 * Map * 을 클릭합니다. Terraform Cloud for Business 계정의 새 작업 영역입니다.
13. 직접 매핑 * 을 선택하고 * 워크플로 입력 * 을 클릭합니다.
14. 입력 이름 * 을 클릭하고 * 워크플로 입력 생성 * 을 클릭합니다.



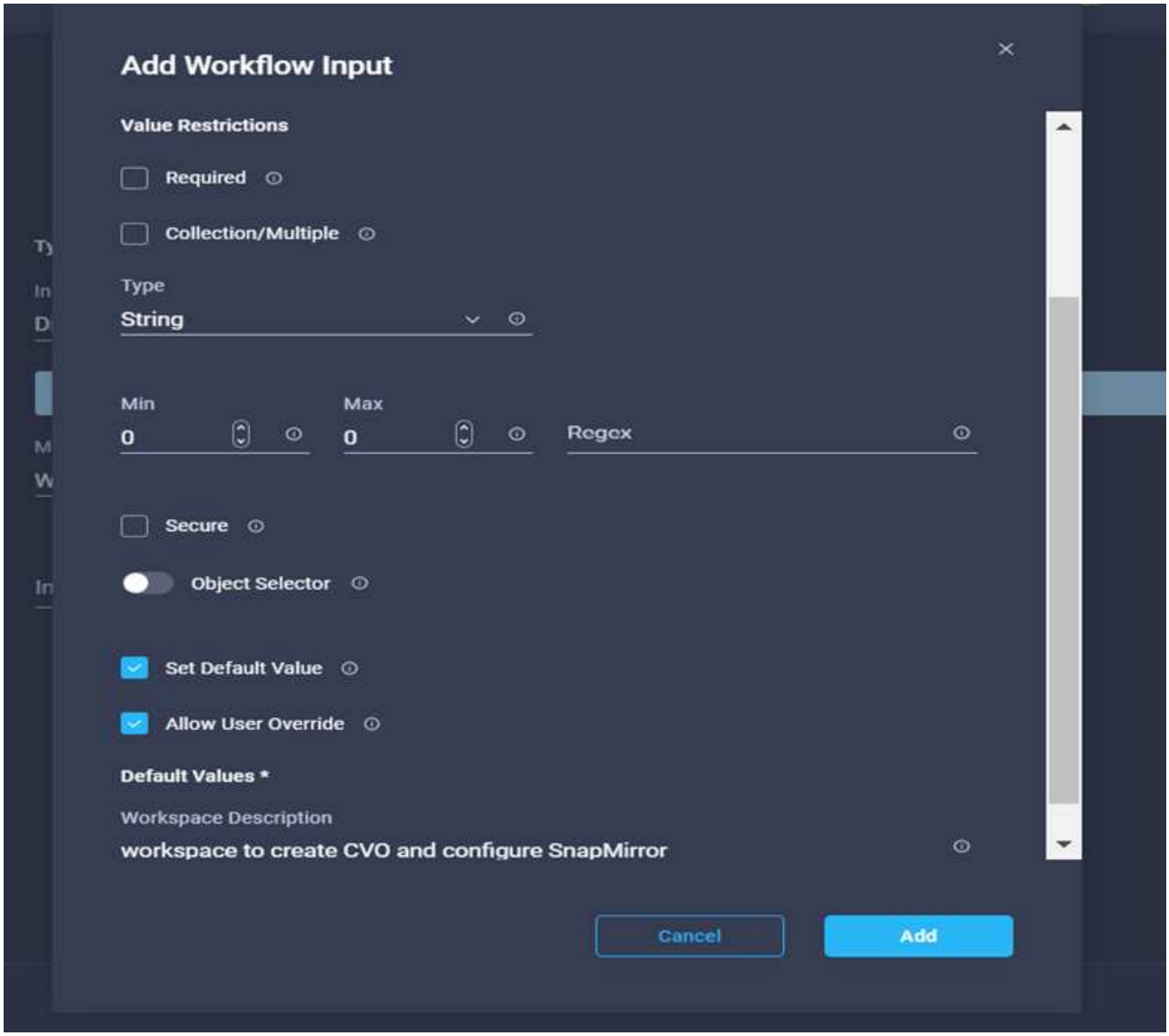
15. 입력 추가 마법사에서 다음 단계를 완료합니다.
    a. 표시 이름과 참조 이름을 입력합니다(선택 사항).
    b. 필수 * 를 클릭합니다.
    c. Type * 에 대해 * String * 을 선택해야 합니다.
    d. Set Default Value(기본값 설정) 및 Override(무시) * 를 클릭합니다.
    e. 작업 영역의 기본 이름을 제공합니다.
    f. 추가 * 를 클릭합니다.



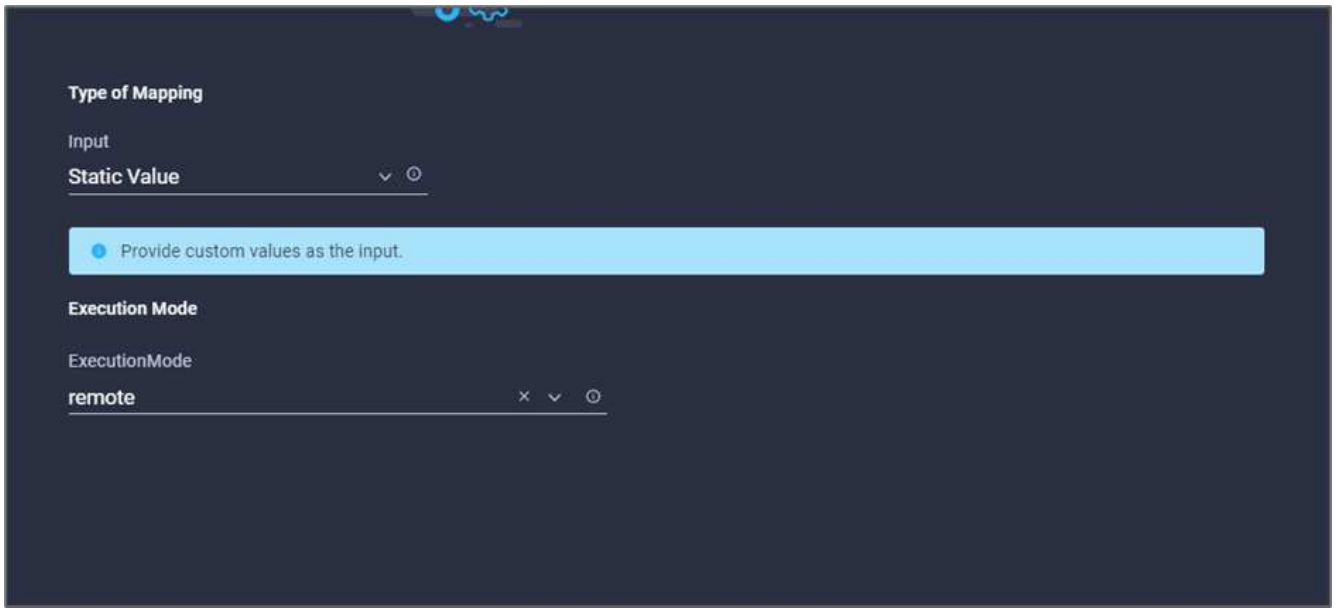
16. Map * 을 클릭합니다.
17. Workspace Description * 필드에서 * Map * 을 클릭합니다.
18. 직접 매핑 * 을 선택하고 * 워크플로 입력 * 을 클릭합니다.
19. 입력 이름 * 을 클릭하고 * 워크플로 입력 생성 * 을 클릭합니다.



20. 입력 추가 마법사에서 다음 단계를 완료합니다.
    a. 표시 이름과 참조 이름을 입력합니다(선택 사항).
    b. Type * 에 대해 * String * 을 선택해야 합니다.
    c. Set Default Value(기본값 설정) 및 Override(무시) * 를 클릭합니다.
    d. 작업 영역 설명을 입력하고 * 추가 * 를 클릭합니다.



21. Map * 을 클릭합니다.
22. Execution Mode * 필드에서 * Map * 을 클릭합니다.
23. 정적 값 * 을 선택하고 * 실행 모드 * 를 클릭한 다음 * 원격 * 을 클릭합니다.



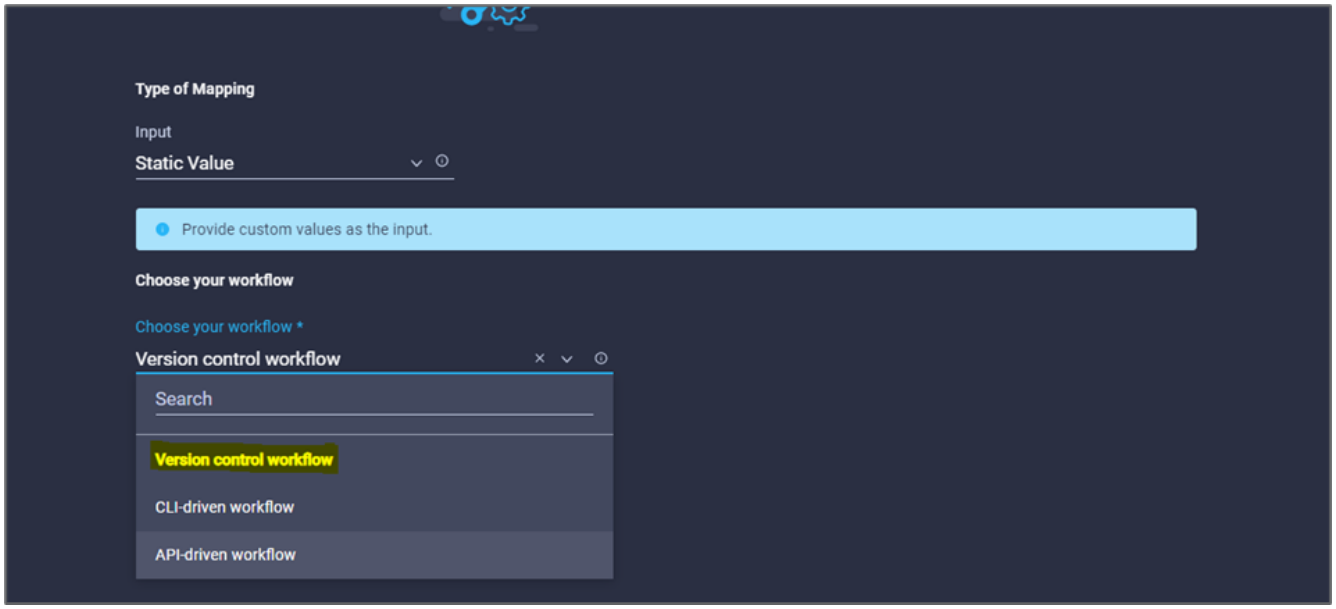
24. Map * 을 클릭합니다.
25. Apply Method * 필드에서 * Map * 을 클릭합니다.
26. 정적 값 * 을 선택하고 * 메서드 적용 * 을 클릭합니다. Manual Apply * 를 클릭합니다.



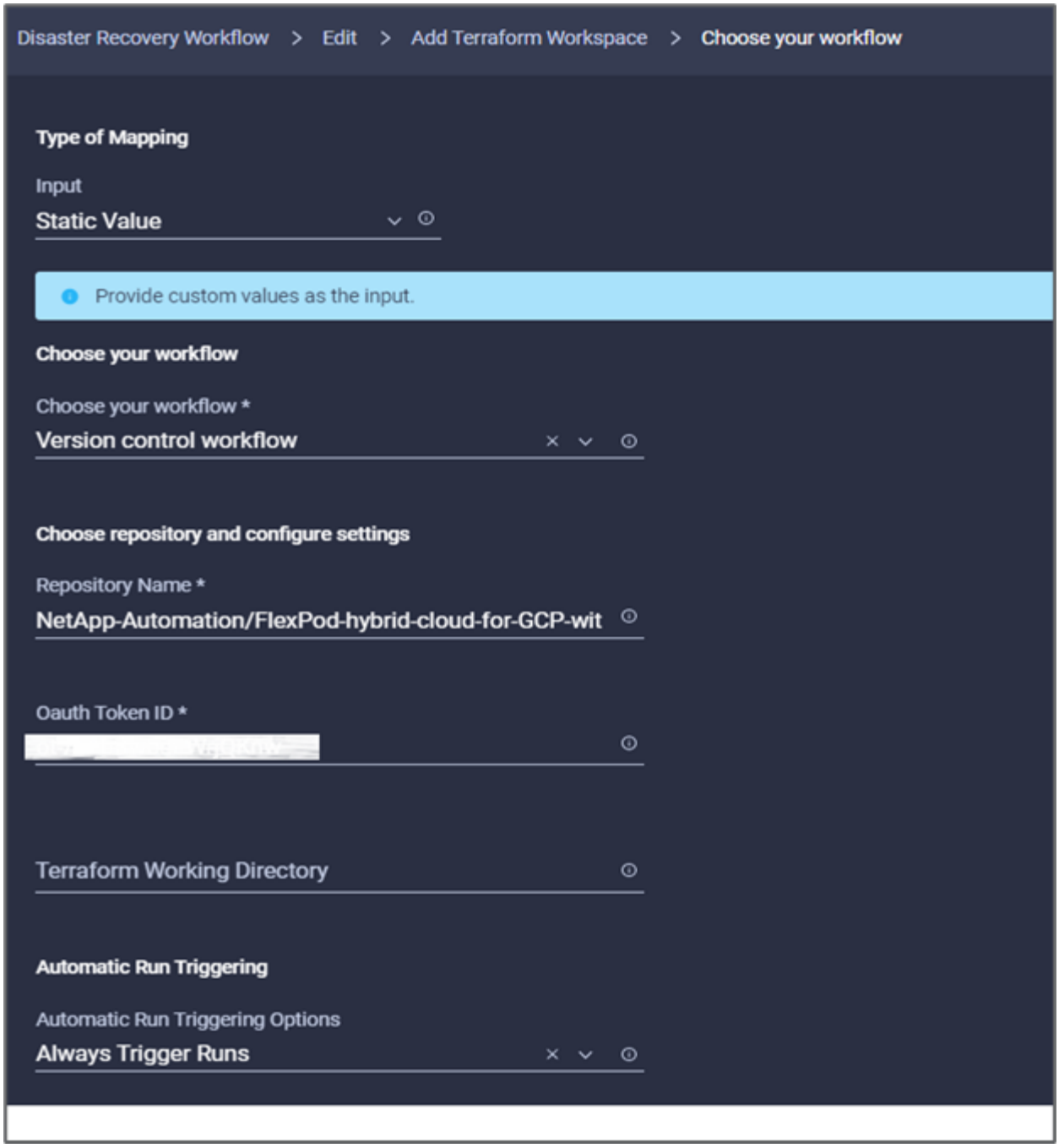
27. Map * 을 클릭합니다.
28. 사용자 인터페이스 * 필드에서 * 맵 * 을 클릭합니다.
29. 정적 값 * 을 선택하고 * 사용자 인터페이스 * 를 클릭합니다. 콘솔 UI * 를 클릭합니다.



30. Map * 을 클릭합니다.
31. 입력 필드에서 * Map * 을 클릭하고 워크플로를 선택합니다.
32. 정적 값 * 을 선택하고 * 워크플로 선택 * 을 클릭합니다. 버전 제어 워크플로 * 를 클릭합니다.



33. 다음 GitHub 리포지토리 세부 정보를 제공합니다.
    a. 리포지토리 이름 * 에서 섹션에 자세히 설명된 리포지토리 이름을 입력합니다 ""환경 필수 구성 요소 설정"".
    b. 섹션에 자세히 설명된 대로 OAuth 토큰 ID를 제공합니다 ""환경 필수 구성 요소 설정"".
    c. 자동 트리거 실행 * 옵션을 선택합니다.



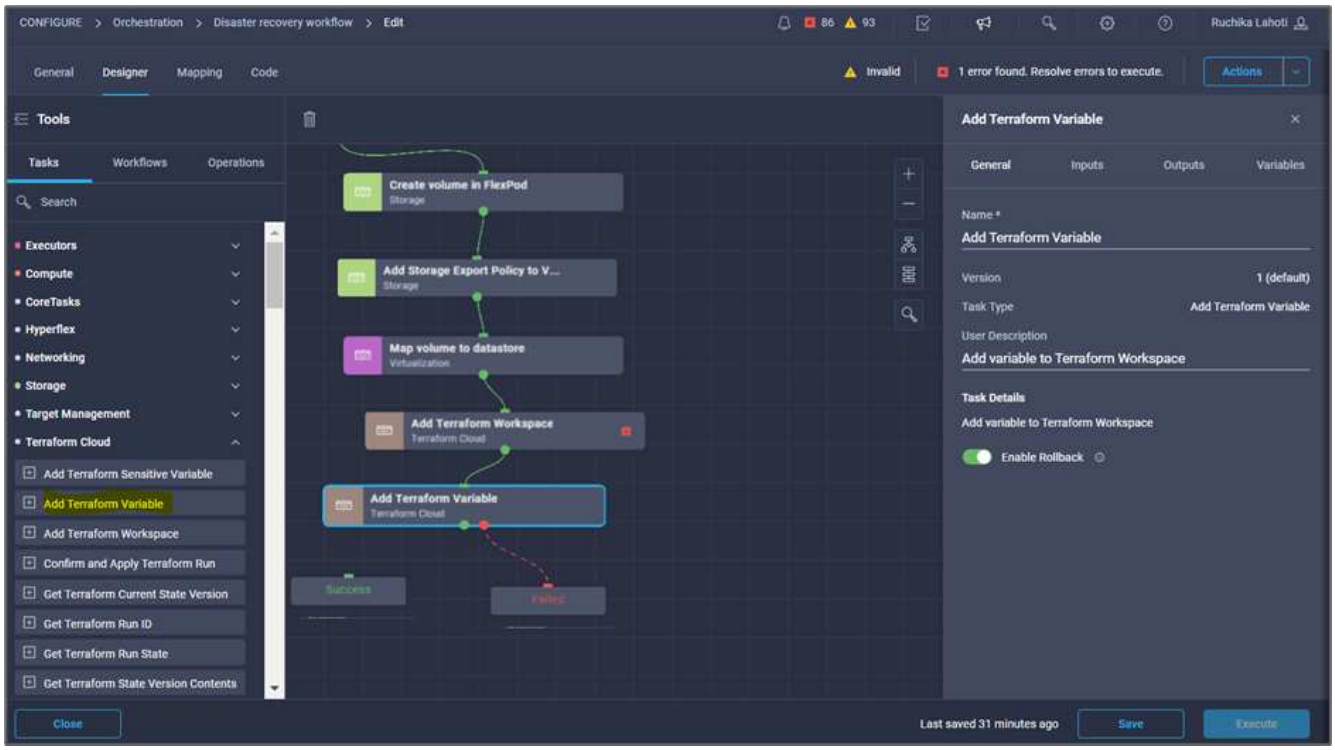
34. Map * 을 클릭합니다.
35. 저장 * 을 클릭합니다.

그러면 Terraform Cloud for Business 계정에서 작업 영역을 만드는 작업이 완료됩니다.

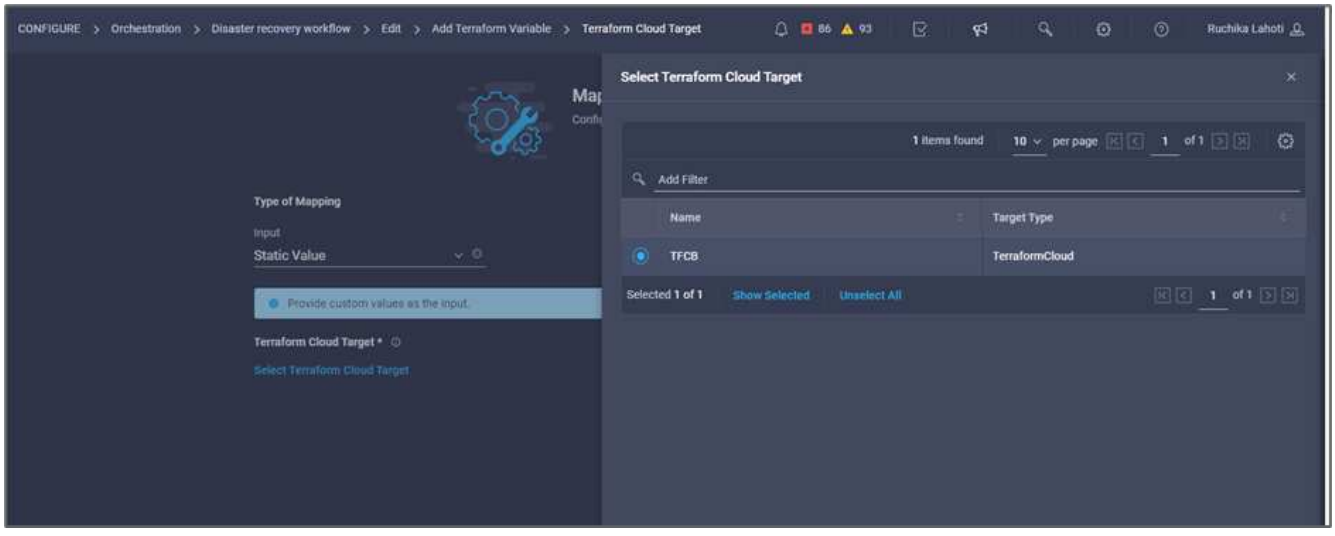
절차 **6:** 작업 영역에 중요하지 않은 변수를 추가합니다

1. Designer * 탭으로 이동하고 * Tools * 섹션에서 * Workflow를 클릭합니다.
2. * Design * 영역의 * Tools * 섹션에서 * Terraform > Add Terraform Variables * (Terraform 변수 추가) 워크플로우를 끌어서 놓습니다.
3. Connector를 사용하여 * Terraform Workspace 추가 * 및 * Terraform 변수 추가 * 작업을 연결합니다. 저장 * 을 클릭합니다.

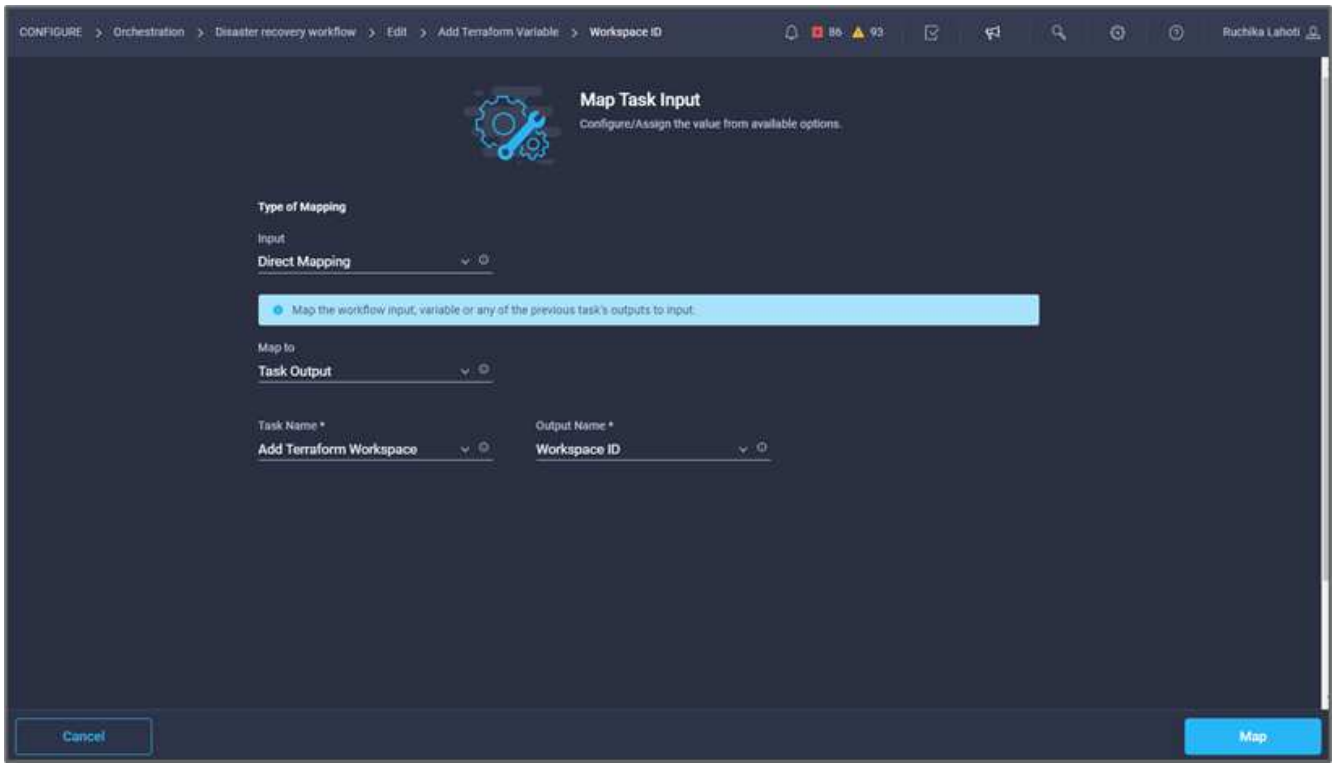
4. Terraform 변수 추가 * 를 클릭합니다. Workflow Properties * 영역에서 * General * 탭을 클릭합니다. 필요에 따라 이 작업의 이름과 설명을 변경할 수 있습니다.



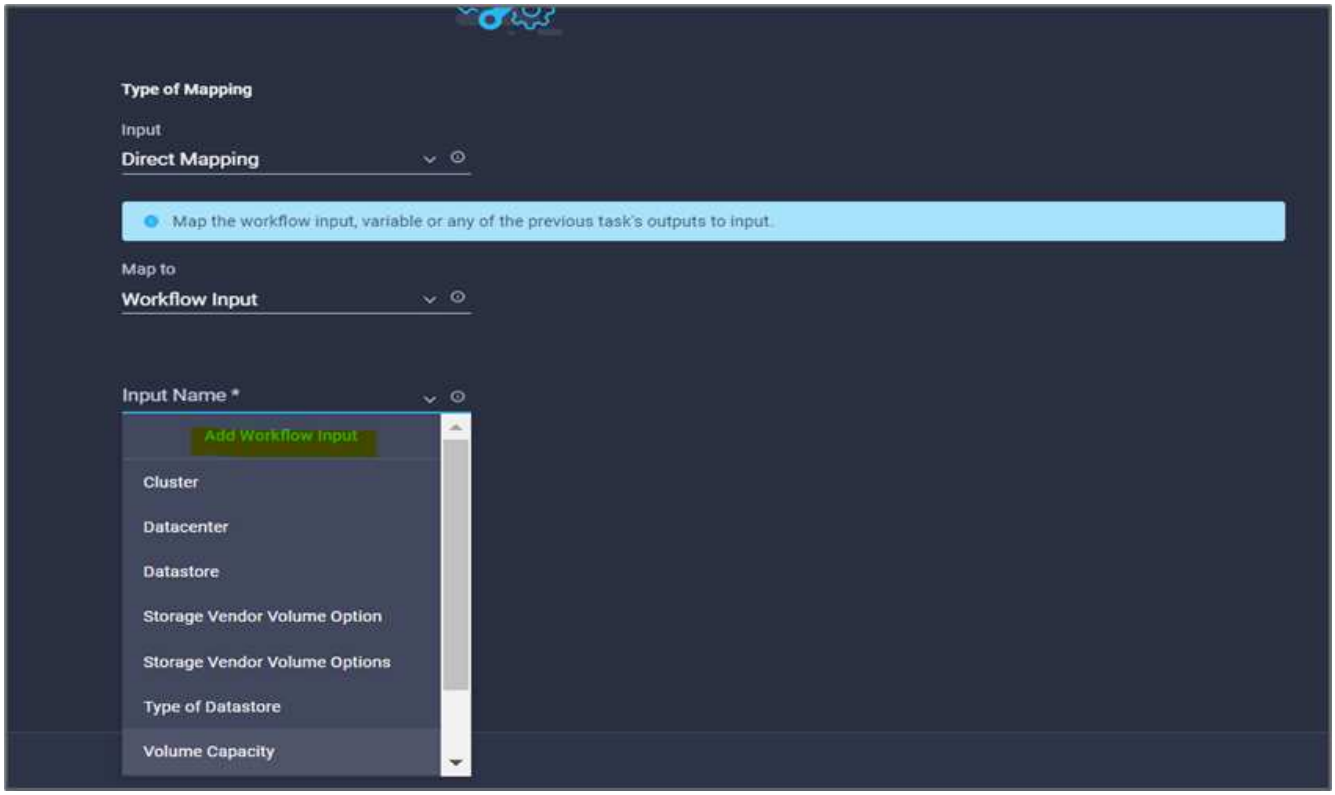
5. Workflow Properties * 영역에서 * Inputs * 를 클릭합니다.
6. Terraform Cloud Target * 필드에서 * Map * 을 클릭합니다.
7. 정적 값 * 을 선택하고 * 클라우드 타겟 선택 * 을 클릭합니다. 에 설명된 대로 추가한 Terraform Cloud for Business 계정을 선택합니다 "HaashCorp Terraform에 대한 Cisco Intersight 서비스를 구성합니다"".



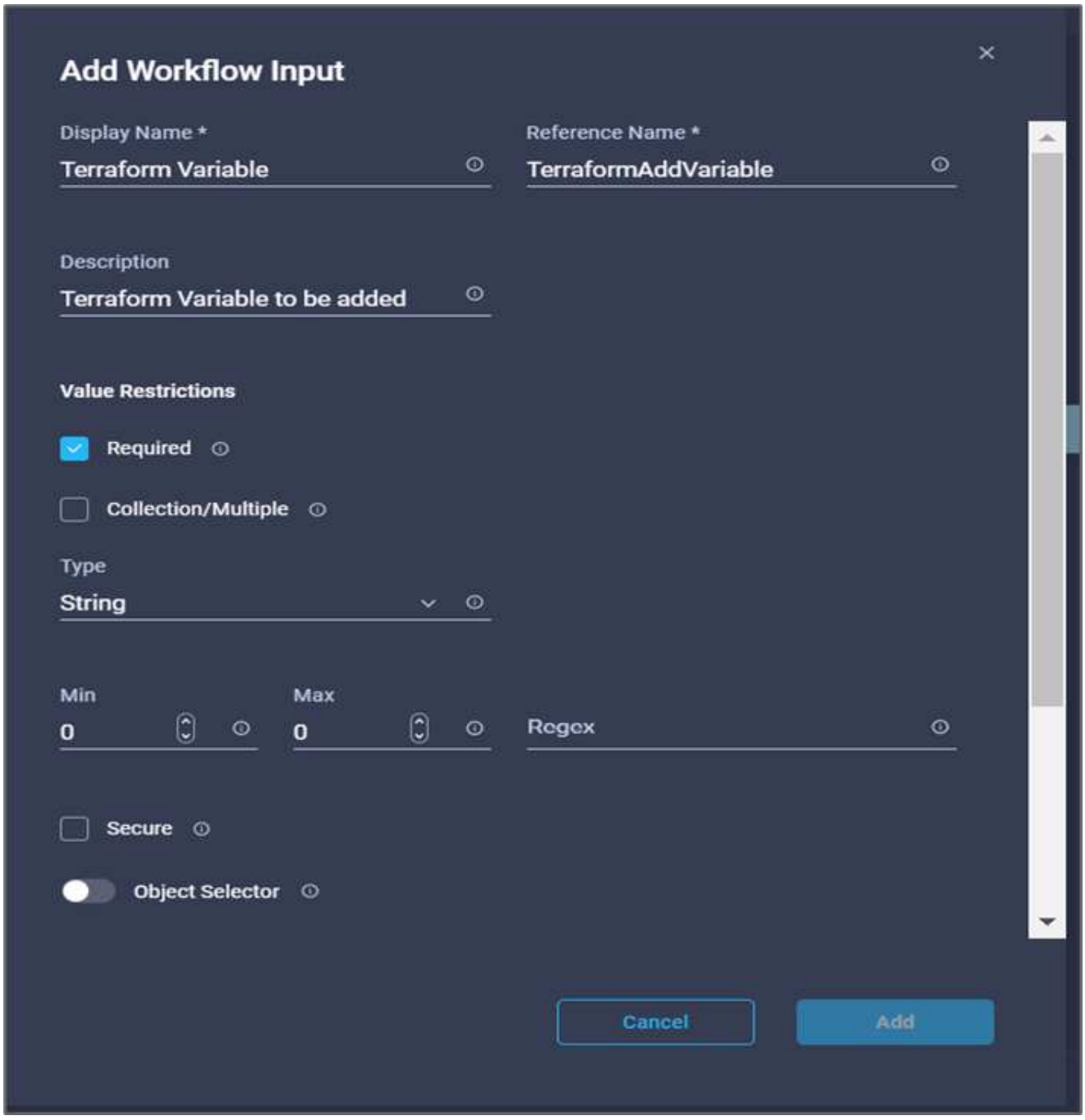
8. Map * 을 클릭합니다.
9. Terraform 조직 이름 * 필드에서 * 맵 * 을 클릭합니다.
10. 정적 값 * 을 선택하고 * 조직 Terraform 선택 * 을 클릭합니다. Terraform Cloud for Business 계정에 속해 있는 Terraform 조직의 이름을 선택합니다.



11. Map * 을 클릭합니다.
12. Terraform Workspace Name * 필드에서 * Map * 을 클릭합니다.
13. 직접 매핑 * 을 선택하고 * 작업 출력 * 을 클릭합니다.
14. 작업 이름 * 을 클릭하고 * Terraform 작업 영역 추가 * 를 클릭합니다.



15. 출력 이름 * 을 클릭하고 * 작업 공간 이름 * 을 클릭합니다.
16. Map * 을 클릭합니다.
17. 변수 추가 옵션 * 필드에서 * 맵 * 을 클릭합니다.
18. 직접 매핑 * 을 선택하고 * 워크플로 입력 * 을 클릭합니다.
19. 입력 이름 * 을 클릭하고 * 워크플로 입력 생성 * 을 클릭합니다.

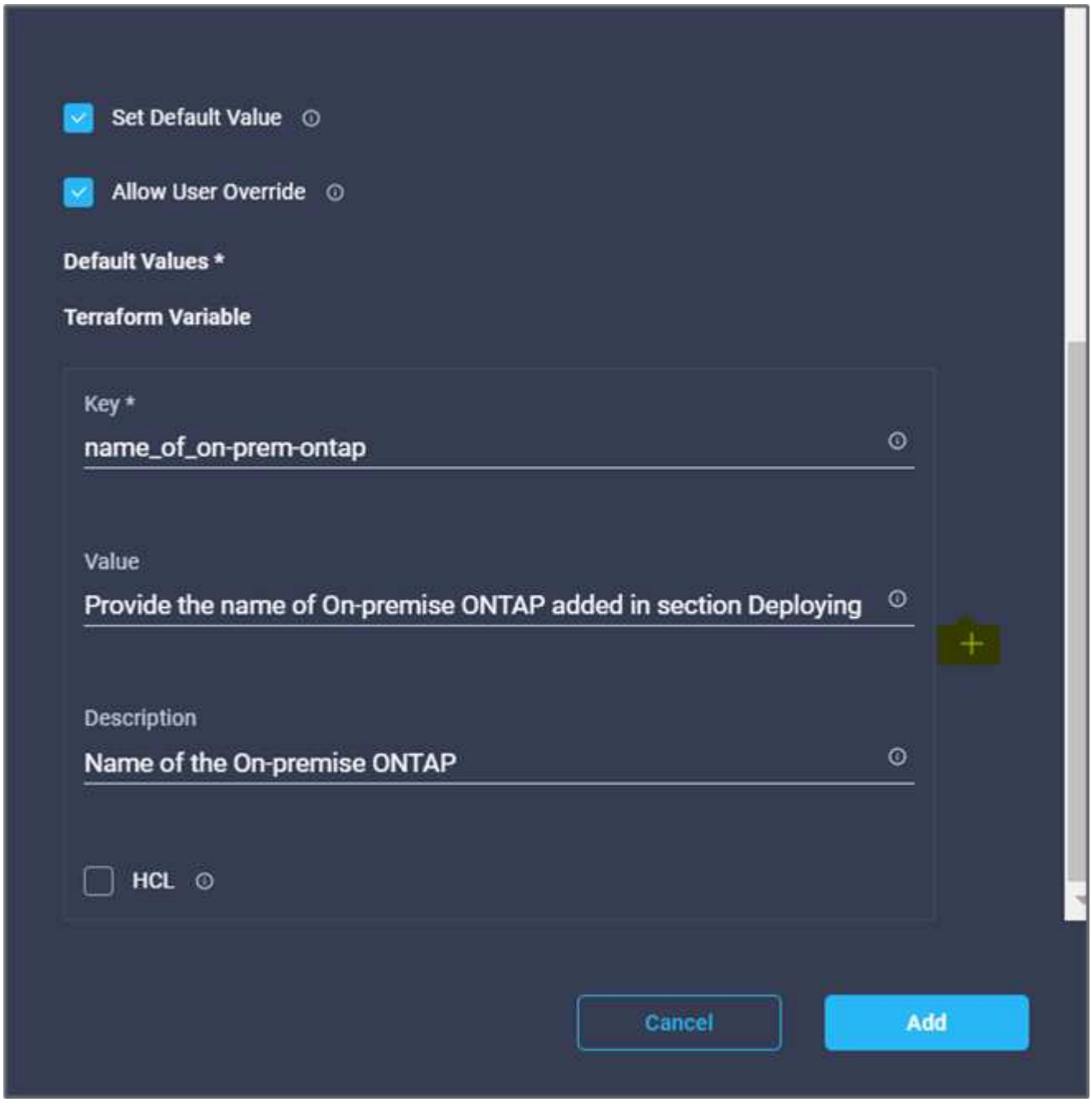


20. 입력 추가 마법사에서 다음 단계를 완료합니다.
    a. 표시 이름과 참조 이름을 입력합니다(선택 사항).
    b. Type * 에 대해 * String * 을 선택해야 합니다.

c. Set Default Value(기본값 설정) 및 Override(무시) * 를 클릭합니다.

d. 변수 유형 * 을 클릭한 다음 * 비민감 변수 * 를 클릭합니다.

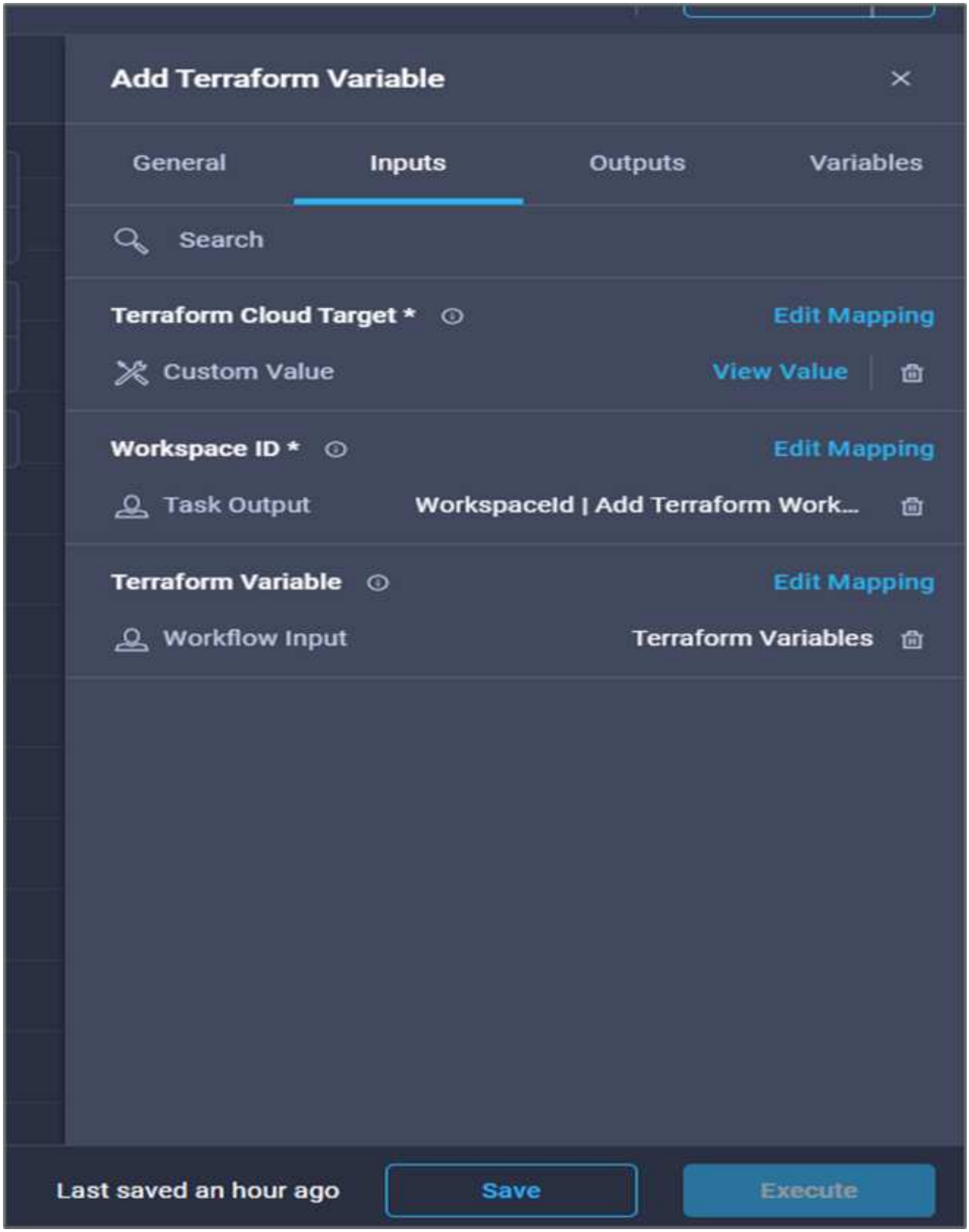
21. Terraform 변수 추가 * 섹션에서 다음 정보를 제공합니다.
    - * 키. * 'name_of_on-premise-ONTAP'입니다
    - * 값. * 온-프레미스 ONTAP의 이름을 제공합니다.
    - * 설명. * 온-프레미스 ONTAP의 이름입니다.
22. 변수를 추가하려면 * + * 를 클릭합니다.



23. 다음 표와 같이 모든 Terraform 변수를 추가합니다. 기본값을 제공할 수도 있습니다.

Terraform 변수 이름입니다	설명
이름_of_on-premise-ONTAP	온프레미스 ONTAP(FlexPod)의 이름
사내 - ONTAP_cluster_IP	스토리지 클러스터 관리 인터페이스의 IP 주소입니다
사내 - ONTAP_USER_NAME	스토리지 클러스터의 관리자 사용자 이름입니다
Zone(영역)	작업 환경을 생성할 GCP 지역
서브넷_id	작업 환경을 생성할 GCP 서브넷 ID입니다
VPC_ID입니다	작업 환경을 생성할 VPC ID입니다
capacity_package_name입니다	사용할 라이센스 유형입니다
source_volume	소스 볼륨의 이름입니다
source_storage_vm_name입니다	소스 SVM의 이름입니다
destination_volume	Cloud Volumes ONTAP의 볼륨 이름입니다
복제 일정 _	기본값은 1시간입니다
볼륨 _ 의 이름 _ 을(를) _ create_on_cvo 로 지정합니다	클라우드 볼륨의 이름입니다
작업 공간 ID	작업 환경을 생성할 workspace_id입니다
프로젝트_ID	작업 환경을 생성할 PROJECT_ID입니다
cvo_cluster의 이름입니다	Cloud Volumes ONTAP 작업 환경의 이름입니다
GCP_SERVICE_ACCOUNT입니다	Cloud Volumes ONTAP 작업 환경의 GCP_SERVICE_ACCOUNT입니다

24. 지도 * 를 클릭한 다음 * 저장 * 을 클릭합니다.



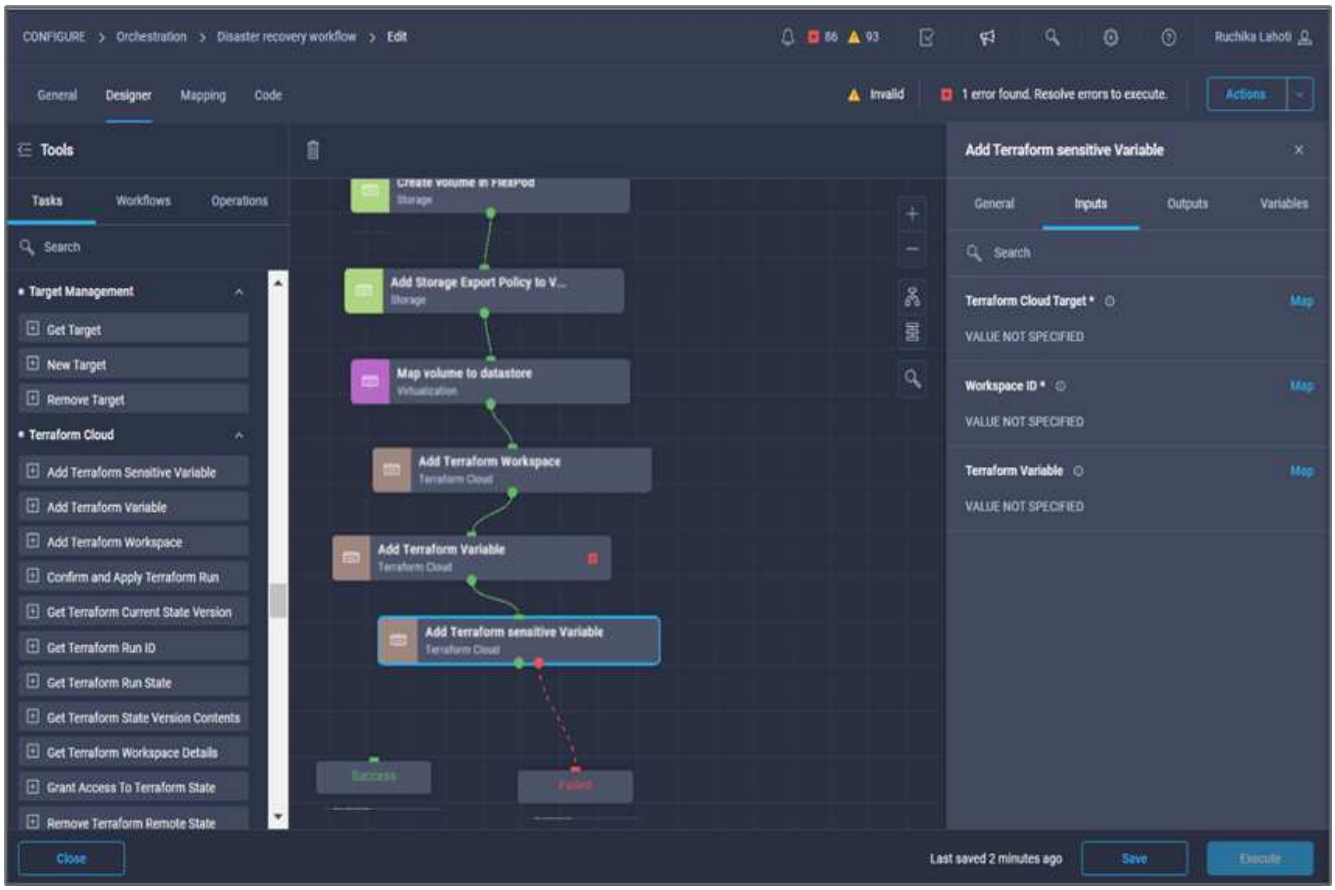
그러면 필요한 Terraform 변수를 작업 공간에 추가하는 작업이 완료됩니다. 그런 다음 필요한 중요 Terraform 변수를 작업 공간에 추가합니다. 두 가지 모두를 하나의 작업으로 결합할 수도 있습니다.

절차 **7:** 작업 영역에 중요한 변수를 추가합니다

1. 디자이너 * 탭으로 이동하고 * 도구 * 섹션에서 * 워크플로 * 를 클릭합니다.
2. * Design * 영역의 * Tools * 섹션에서 * Terraform > Add Terraform Variables * (Terraform 변수 추가) 워크플로우를 끌어서 놓습니다.
3. Connector를 사용하여 2개의 * Terraform Workspace * 추가 작업을 연결합니다. 저장 * 을 클릭합니다.

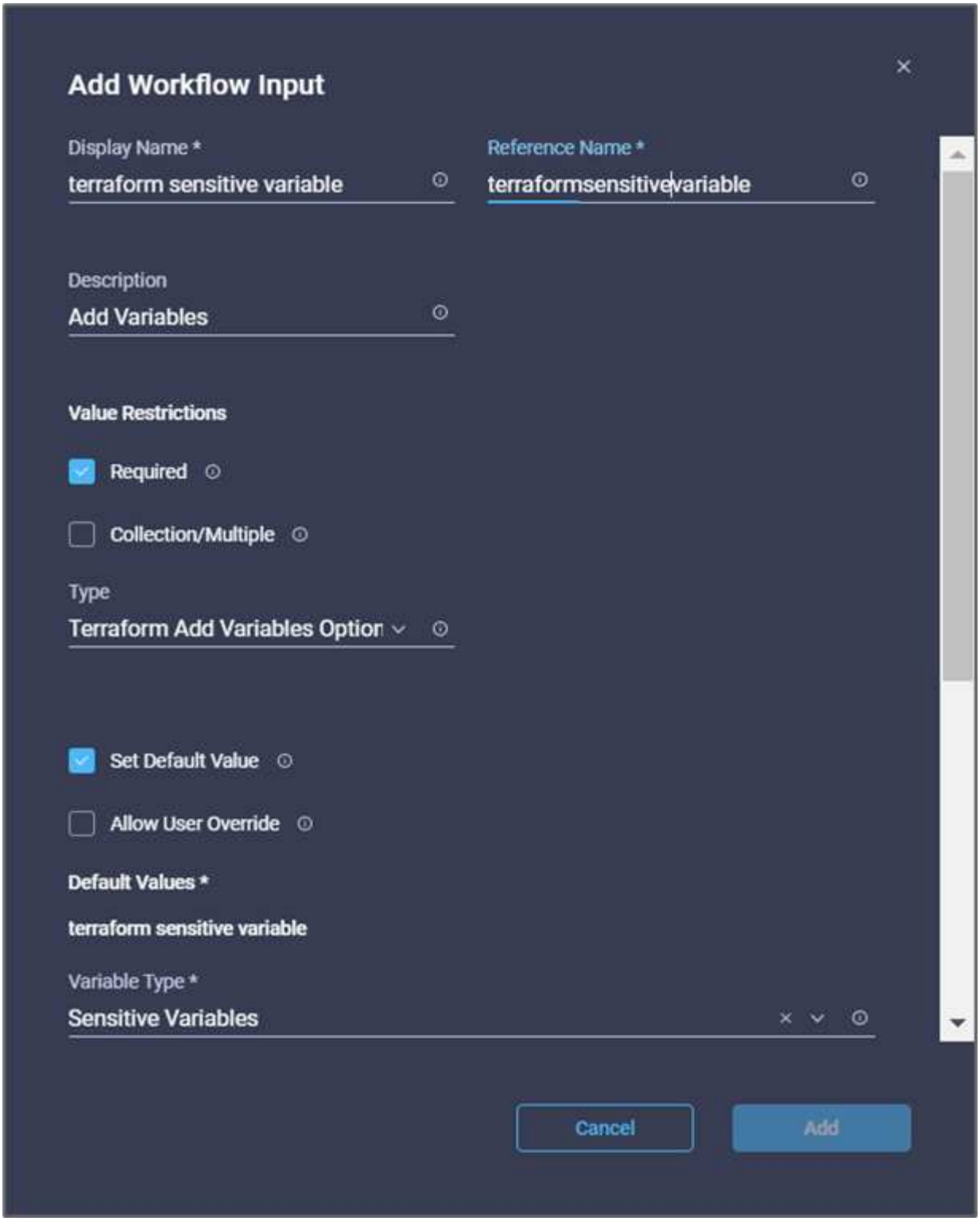
> 두 작업의 이름이 동일함을 나타내는 경고가 나타납니다. 다음 단계에서 작업 이름을 변경했으므로 지금 오류를 무시합니다.

4. Terraform 변수 추가 * 를 클릭합니다. Workflow Properties * 영역에서 * General * 탭을 클릭합니다. 이름을 * Terraform Sensitive Variables * 로 변경합니다.



5. Workflow Properties * 영역에서 * Inputs * 를 클릭합니다.
6. Terraform Cloud Target * 필드에서 * Map * 을 클릭합니다.
7. 정적 값 * 을 선택하고 * 클라우드 타겟 선택 * 을 클릭합니다. 섹션에 추가된 Terraform Cloud for Business 계정을 선택합니다 "HaashCorp Terraform에 대한 Cisco Intersight 서비스를 구성합니다".”
8. Map * 을 클릭합니다.
9. Terraform 조직 이름 * 필드에서 * 맵 * 을 클릭합니다.
10. 정적 값 * 을 선택하고 * 조직 Terraform 선택 * 을 클릭합니다. Terraform Cloud for Business 계정에 속해 있는 Terraform 조직의 이름을 선택합니다.
11. Map * 을 클릭합니다.

12. Terraform Workspace Name * 필드에서 * Map * 을 클릭합니다.
13. 직접 매핑 * 을 선택하고 * 작업 출력 * 을 클릭합니다.
14. 작업 이름 * 을 클릭한 다음 * Terraform 작업 영역 추가 * 를 클릭합니다.
15. 출력 이름 * 을 클릭하고 출력 * 작업 공간 이름 * 을 클릭합니다.
16. Map * 을 클릭합니다.
17. 변수 추가 옵션 * 필드에서 * 맵 * 을 클릭합니다.
18. 직접 매핑 * 을 선택한 다음 * 워크플로 입력 * 을 클릭합니다.
19. 입력 이름 * 을 클릭하고 * 워크플로 입력 생성 * 을 클릭합니다.
20. 입력 추가 마법사에서 다음 단계를 완료합니다.
    a. 표시 이름과 참조 이름을 입력합니다(선택 사항).
    b. 유형에 대해 * Terraform 변수 추가 옵션 * 을 선택해야 합니다.
    c. 기본값 설정 * 을 클릭합니다.
    d. 변수 유형 * 을 클릭한 다음 * 민감한 변수 * 를 클릭합니다.
    e. 추가 * 를 클릭합니다.



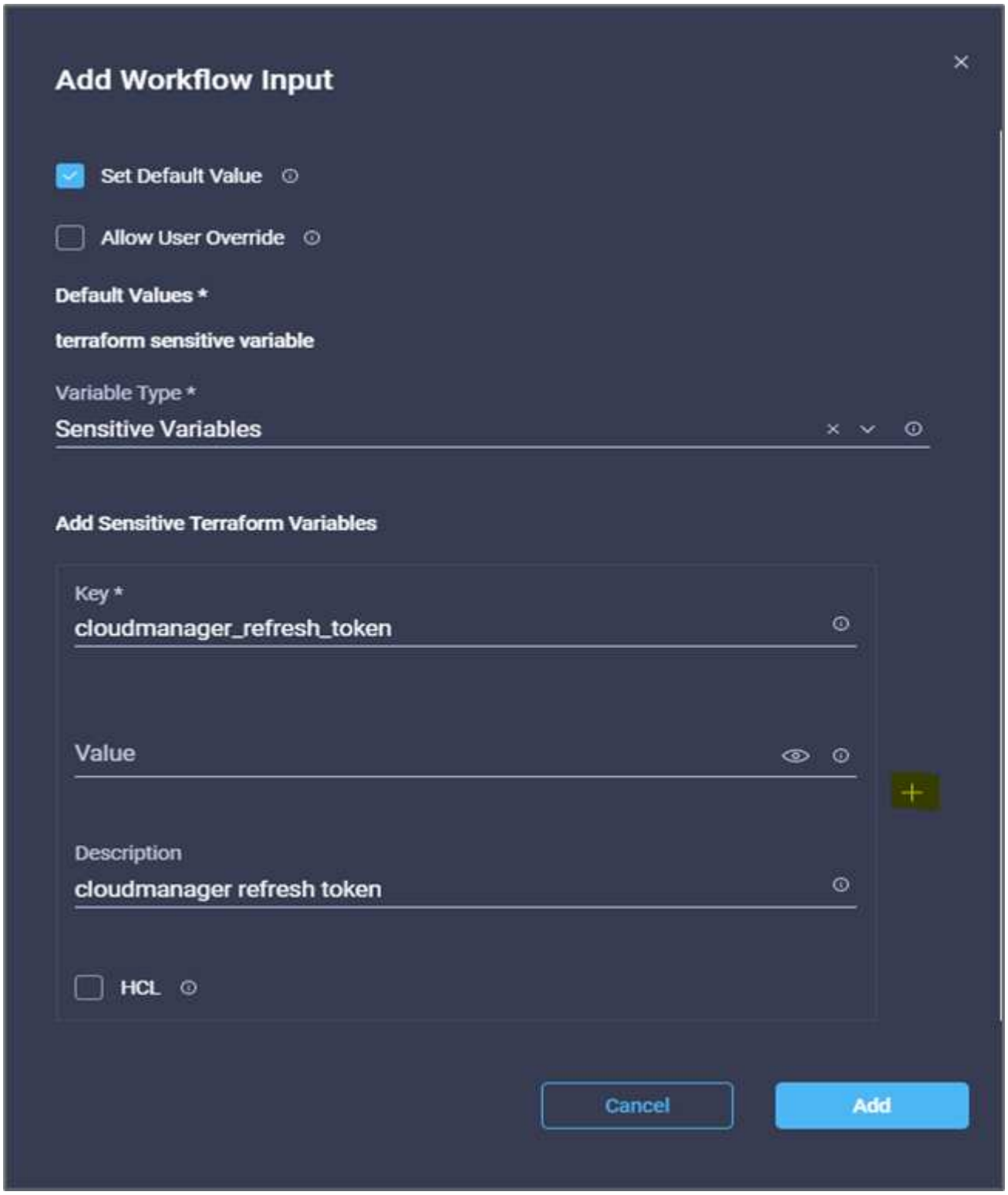
21. Terraform 변수 추가 * 섹션에서 다음 정보를 제공합니다.

    ◦ 키. * 'cloudmanager_refresh_token'.

    ◦ * 가치. * NetApp Cloud Manager API 작업에 대한 업데이트 토큰을 입력합니다.

    ◦ * 설명 * 토큰 새로 고침.

NetApp Cloud Manager API 작업을 위한 업데이트 토큰을 얻는 방법에 대한 자세한 내용은 섹션을 참조하십시오 ""환경 필수 구성 요소 설정.""



22. 아래 표와 같이 Terraform에 민감한 변수를 모두 추가합니다. 기본값을 제공할 수도 있습니다.

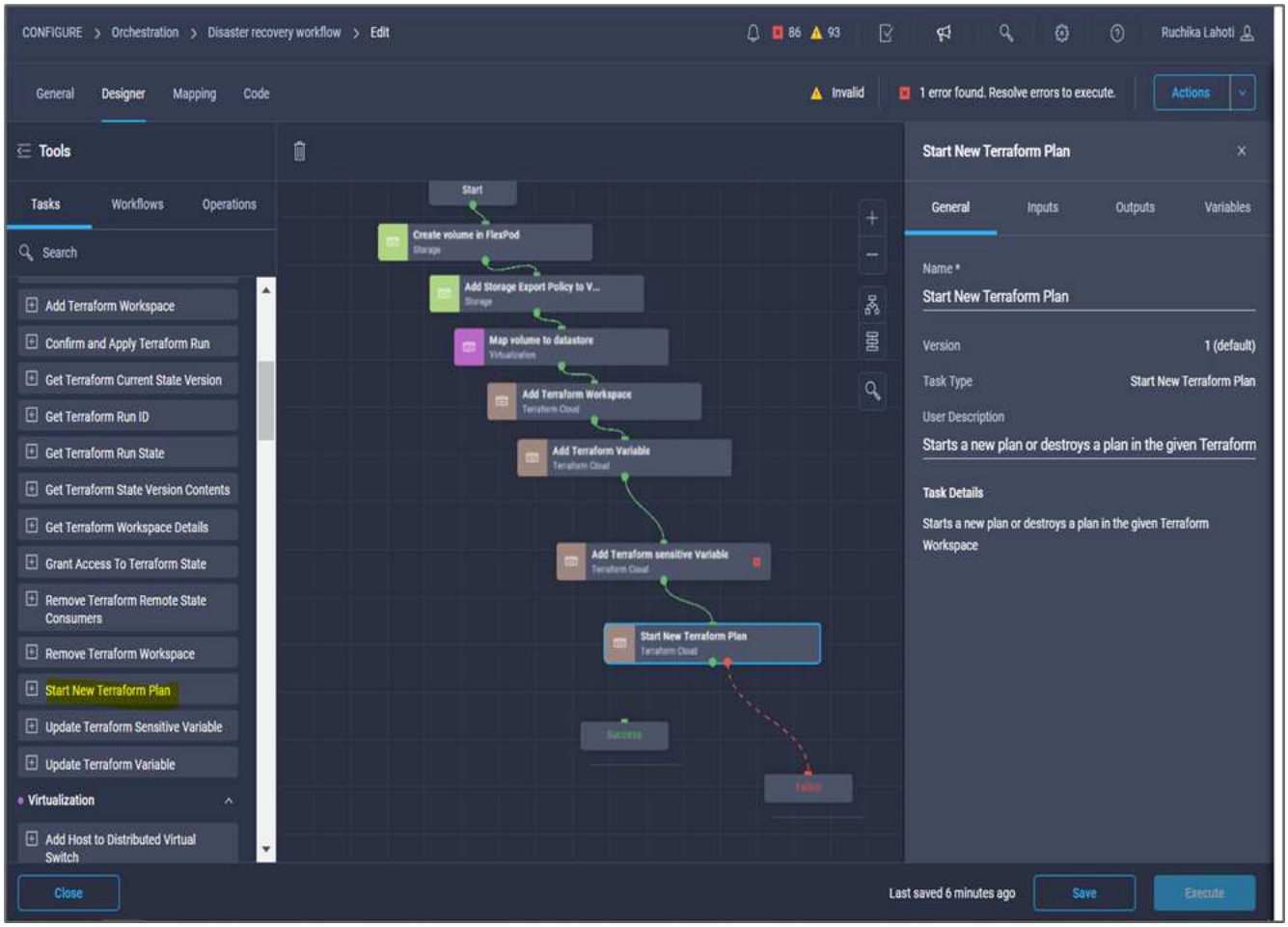
Terraform 민감한 변수 이름입니다	설명
cloudmanager_refresh_token을 참조하십시오	토큰을 새로 고칩니다. 다음에서 받기:

Terraform 민감한 변수 이름입니다	설명
커넥터_ID	Cloud Manager Connector의 클라이언트 ID입니다. 에서 구할 수 있습니다
CVO_ADMIN_PASSWORD를 입력합니다	Cloud Volumes ONTAP의 admin 암호입니다
사내 - ONTAP_USER_PASSWORD	스토리지 클러스터의 admin 암호입니다

23. Map * 을 클릭합니다. 그러면 필요한 Terraform 중요 변수를 작업 공간에 추가하는 작업이 완료됩니다. 그런 다음 구성된 작업 영역에서 새 Terraform 계획을 시작합니다.

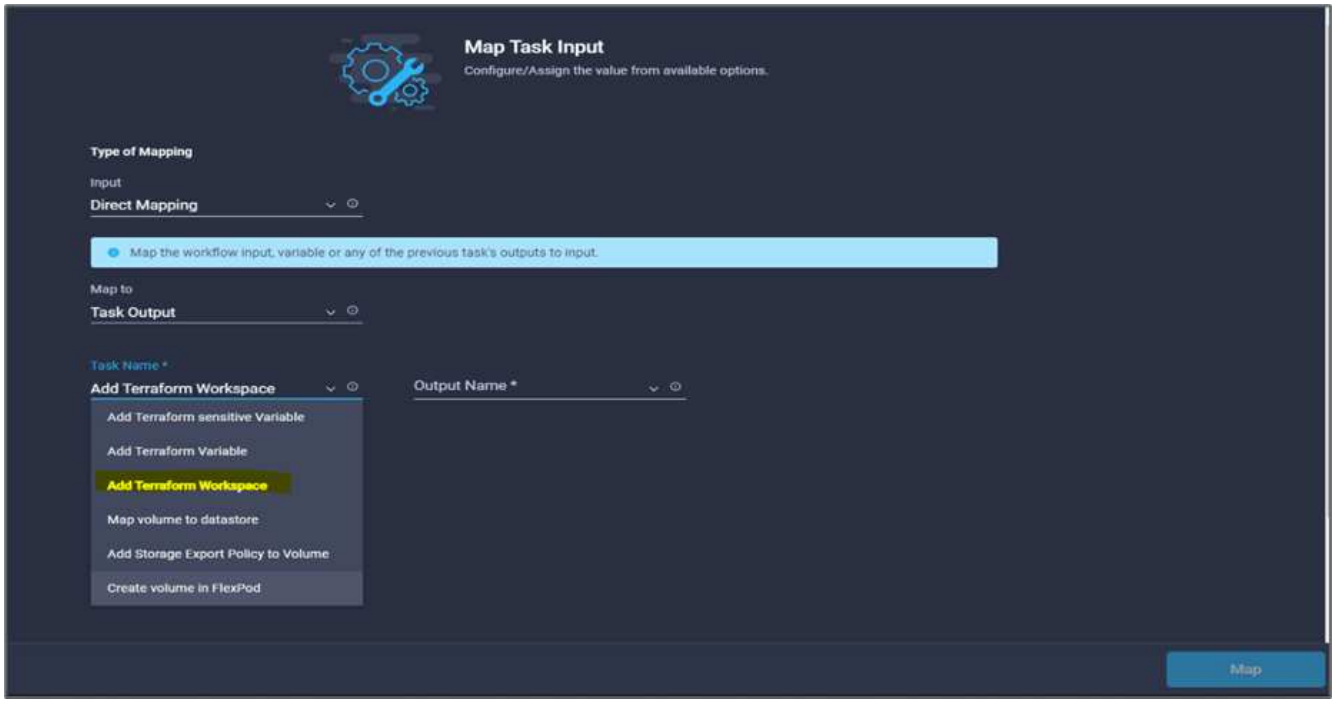
절차 **8:** 새 **Terraform** 계획을 시작합니다

1. 디자이너 * 탭으로 이동하고 * 도구 * 섹션에서 * 작업 * 을 클릭합니다.
2. * Design * 영역의 * Tools * 섹션에서 * Terraform Cloud > Start New Terraform Plan * 작업을 끌어서 놓습니다.
3. Connector를 사용하여 태스크 * Terraform Sensitive Variables * 추가 및 * 새 Terraform Plan 작업 시작 * 을 연결합니다. 저장 * 을 클릭합니다.
4. Start New Terraform Plan * 을 클릭합니다. 작업 속성 * 영역에서 * 일반 * 탭을 클릭합니다. 필요에 따라 이 작업의 이름과 설명을 변경할 수 있습니다.

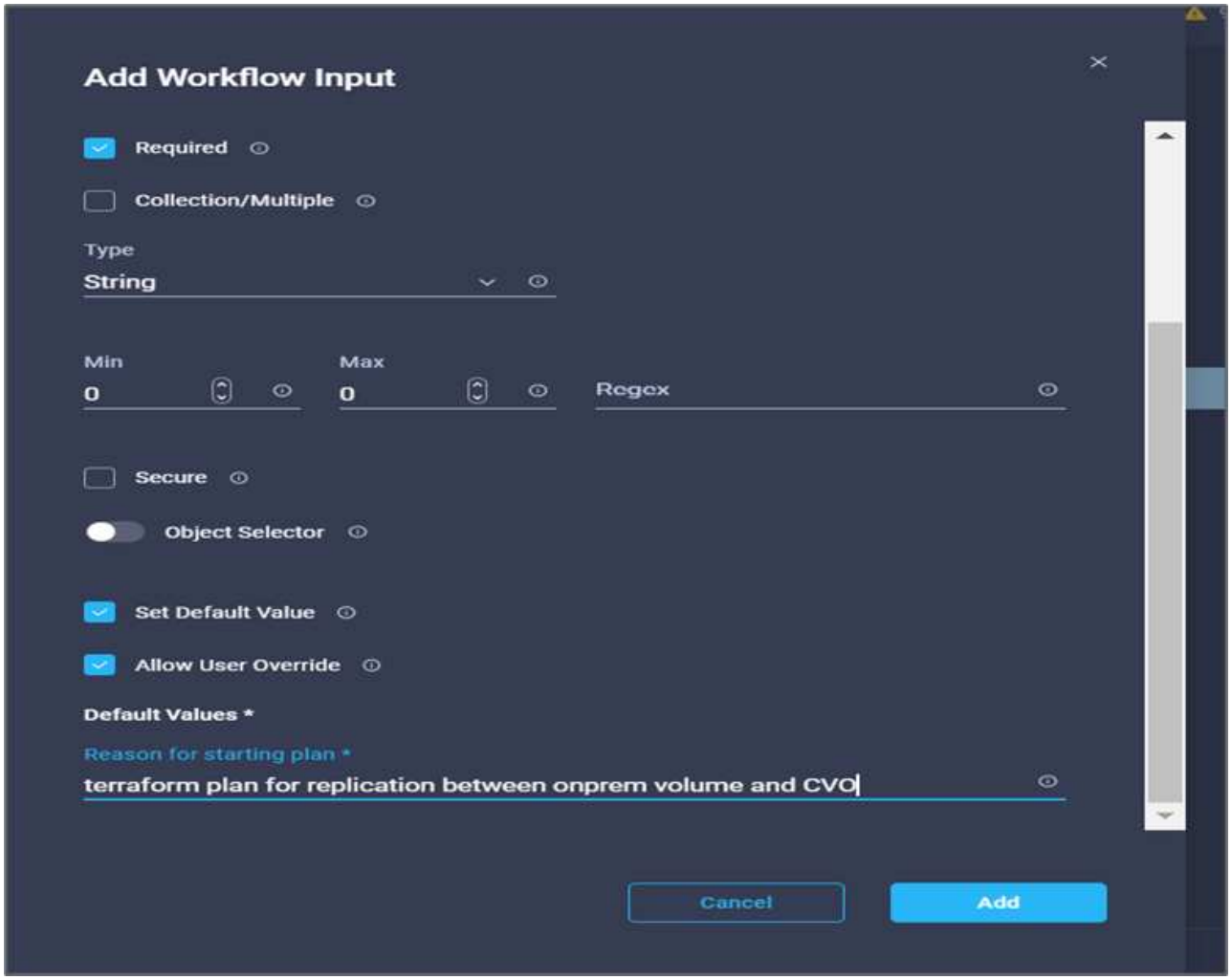


5. 작업 속성 * 영역에서 * 입력 * 을 클릭합니다.
6. Terraform Cloud Target * 필드에서 * Map * 을 클릭합니다.

7. 정적 값 * 을 선택하고 * 클라우드 타겟 선택 * 을 클릭합니다. "Configuring Cisco Intersight Service for HashiCorp Terraform" 섹션에 추가된 Terraform Cloud for Business 계정을 선택합니다.
8. Map * 을 클릭합니다.
9. Workspace ID * 필드에서 * Map * 을 클릭합니다.
10. 직접 매핑 * 을 선택하고 * 작업 출력 * 을 클릭합니다.
11. 작업 이름 * 을 클릭한 다음 * Terraform 작업 영역 추가 * 를 클릭합니다.



12. 출력 이름 *, * 작업 공간 ID *, * 맵 * 을 차례로 클릭합니다.
13. 계획 시작 이유 * 필드에서 * 맵 * 을 클릭합니다.
14. 직접 매핑 * 을 선택한 다음 * 워크플로 입력 * 을 클릭합니다.
15. 입력 이름 * 을 클릭한 다음 * 워크플로 입력 작성 * 을 클릭합니다.
16. 입력 추가 마법사에서 다음 단계를 완료합니다.
    a. 표시 이름과 참조 이름을 입력합니다(선택 사항).
    b. Type * 에 대해 * String * 을 선택해야 합니다.
    c. Set Default Value(기본값 설정) 및 Override(무시) * 를 클릭합니다.
    d. 계획 시작 이유 * 에 대한 기본값을 입력하고 * 추가 * 를 클릭합니다.



17. Map * 을 클릭합니다.
18. Plan Operation * 필드에서 * Map * 을 클릭합니다.
19. 정적 값 * 을 선택하고 * 계획 작업 * 을 클릭합니다. 새 계획 * 을 클릭합니다.



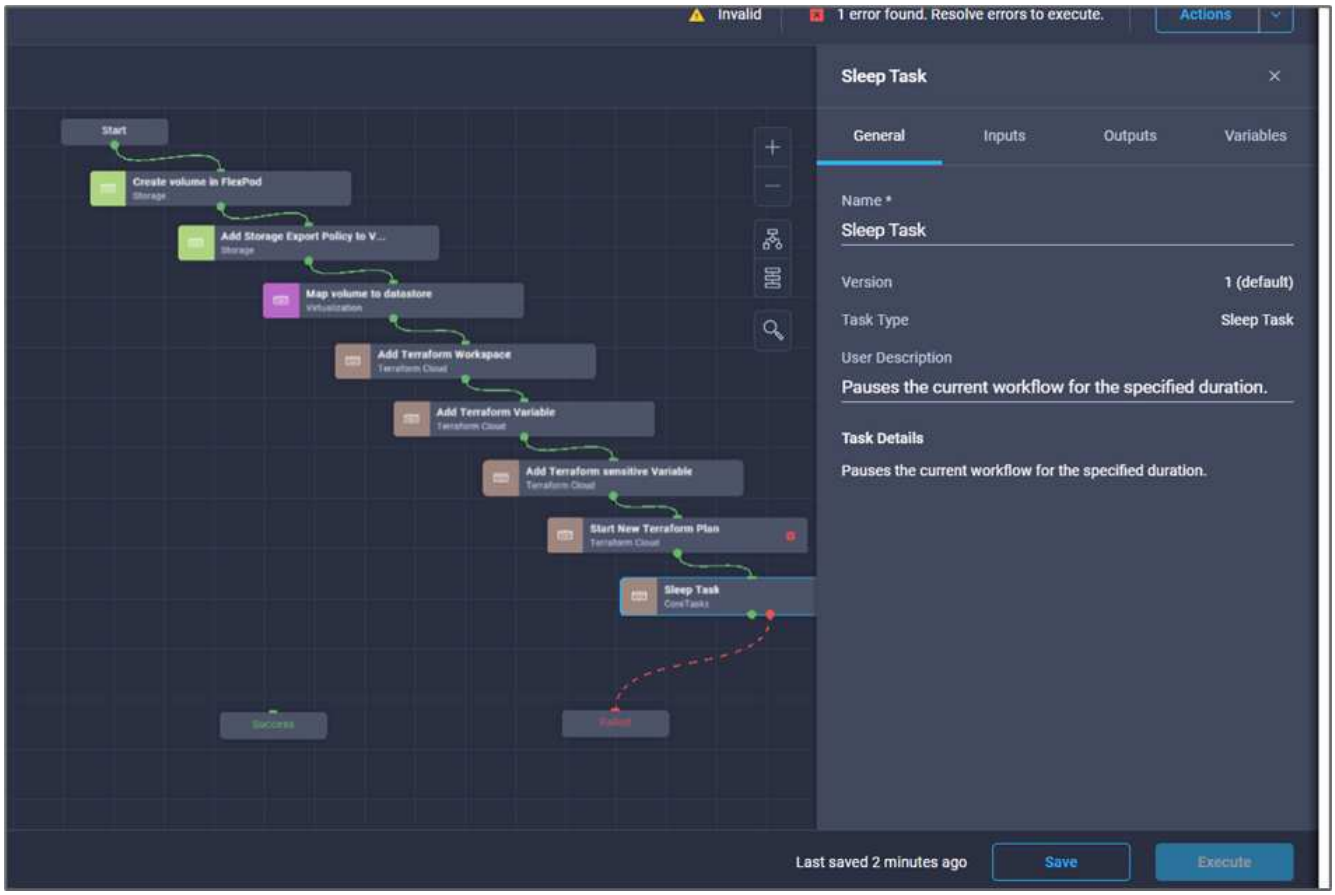
20. Map * 을 클릭합니다.
21. 저장 * 을 클릭합니다.

그러면 Terraform Cloud for Business 계정에 Terraform 플랜을 추가하는 작업이 완료됩니다. 그런 다음 몇 초 동안 절전 작업을 만듭니다.

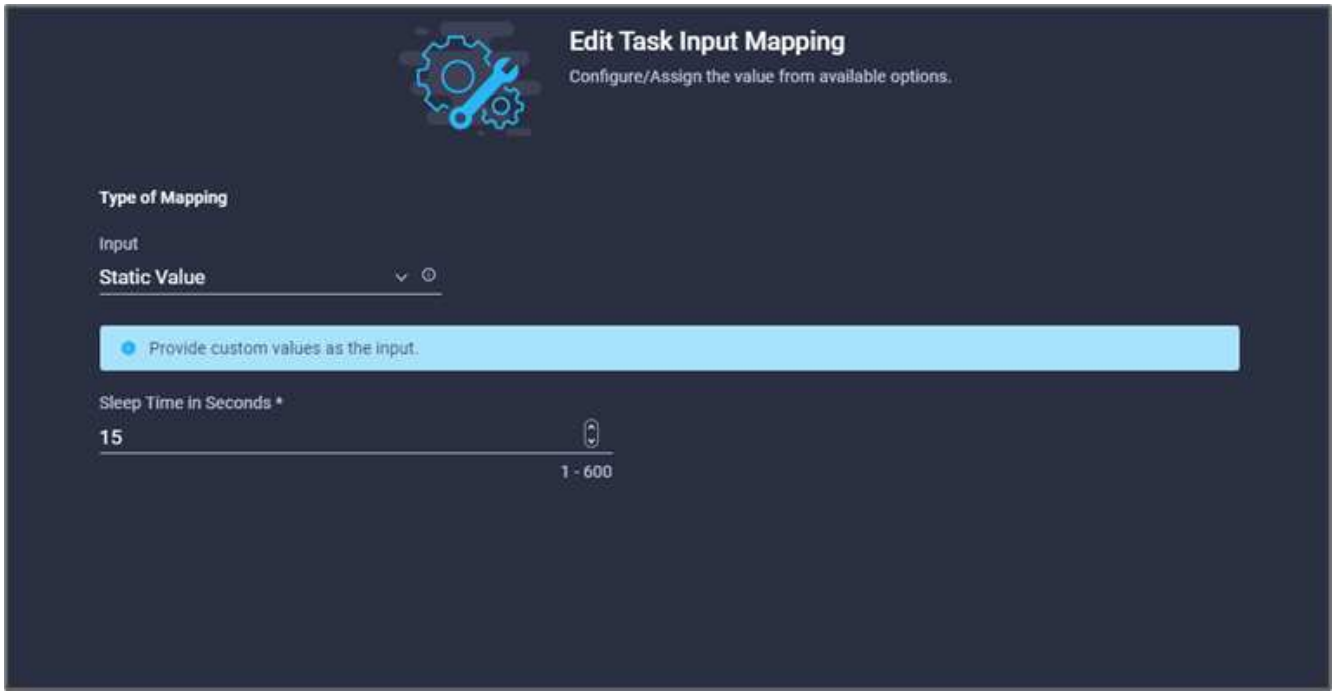
절차 **9:** 동기화를 위한 절전 작업

Terraform 적용에는 RunID가 필요하며, 이 ID는 Terraform 계획 작업의 일부로 생성됩니다. Terraform Plan과 Terraform Apply 작업 사이에 몇 초 동안 대기하면 타이밍 문제가 방지됩니다.

1. 디자이너 * 탭으로 이동하고 * 도구 * 섹션에서 * 작업 * 을 클릭합니다.
2. Design * 영역의 * Tools * 섹션에서 * Core Tasks > Sleep Task * 를 끌어 놓습니다.
3. 커넥터를 사용하여 작업을 연결합니다 * 새 Terraform 계획 시작 * 및 * 절전 작업 *. 저장 * 을 클릭합니다.



4. 절전 작업 * 을 클릭합니다. 작업 속성 * 영역에서 * 일반 * 탭을 클릭합니다. 필요에 따라 이 작업의 이름과 설명을 변경할 수 있습니다. 이 예제에서 작업 이름은 * Synchronize * 입니다.
5. 작업 속성 * 영역에서 * 입력 * 을 클릭합니다.
6. [초 단위 절전 시간] 필드에서 * 맵 * 을 클릭합니다.
7. 정적 값 * 을 선택하고 * 절전 시간(초) * 에 * 15 * 를 입력합니다.

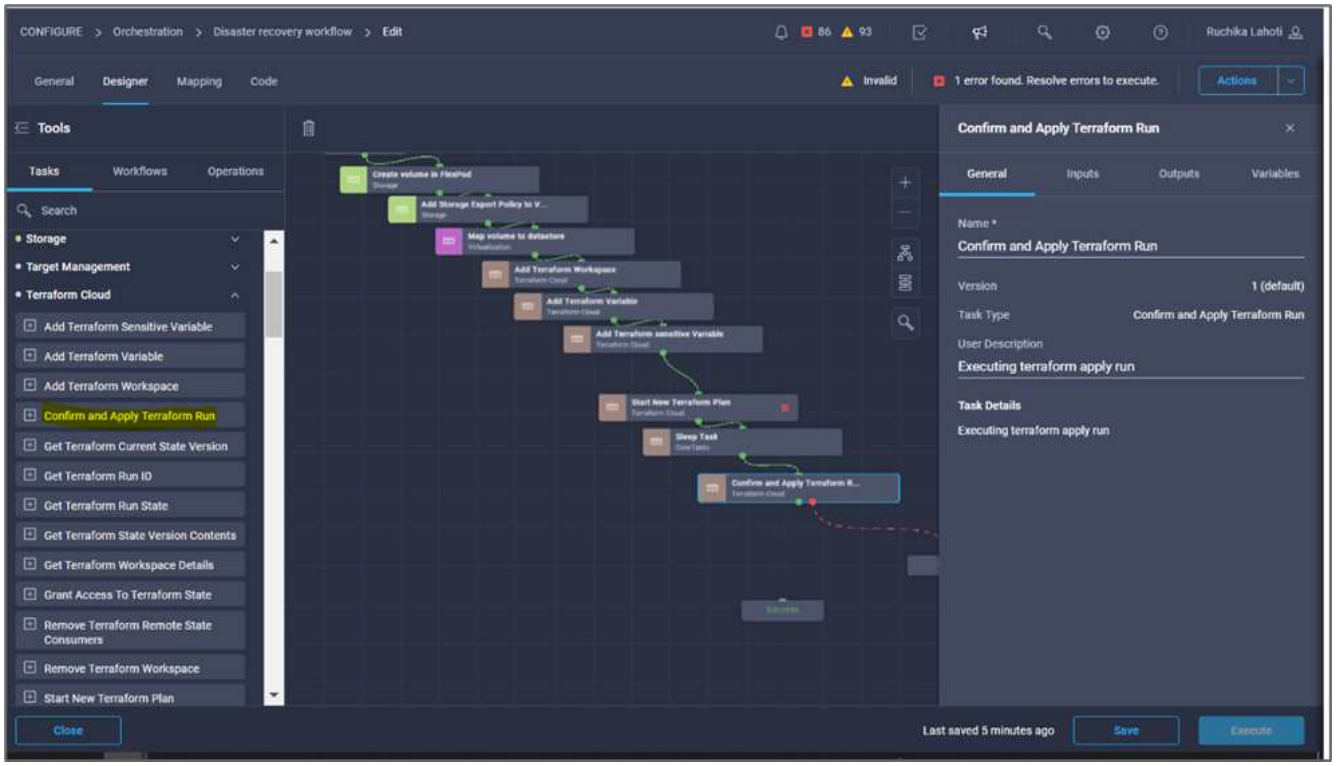


8. Map * 을 클릭합니다.
9. 저장 * 을 클릭합니다.

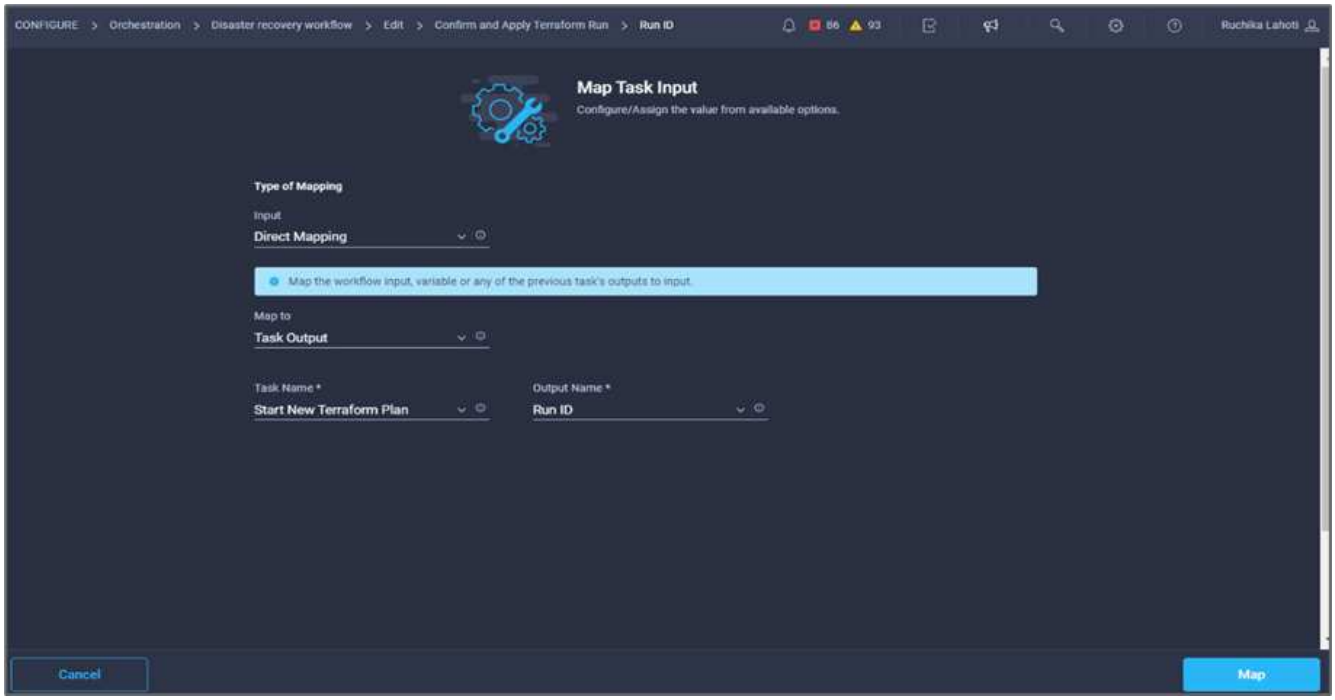
이것으로 수면 작업이 완료되었습니다. 그런 다음 이 워크플로의 마지막 작업을 만들어 Terraform 실행을 확인하고 적용합니다.

절차 **10: Terraform** 실행을 확인하고 적용합니다

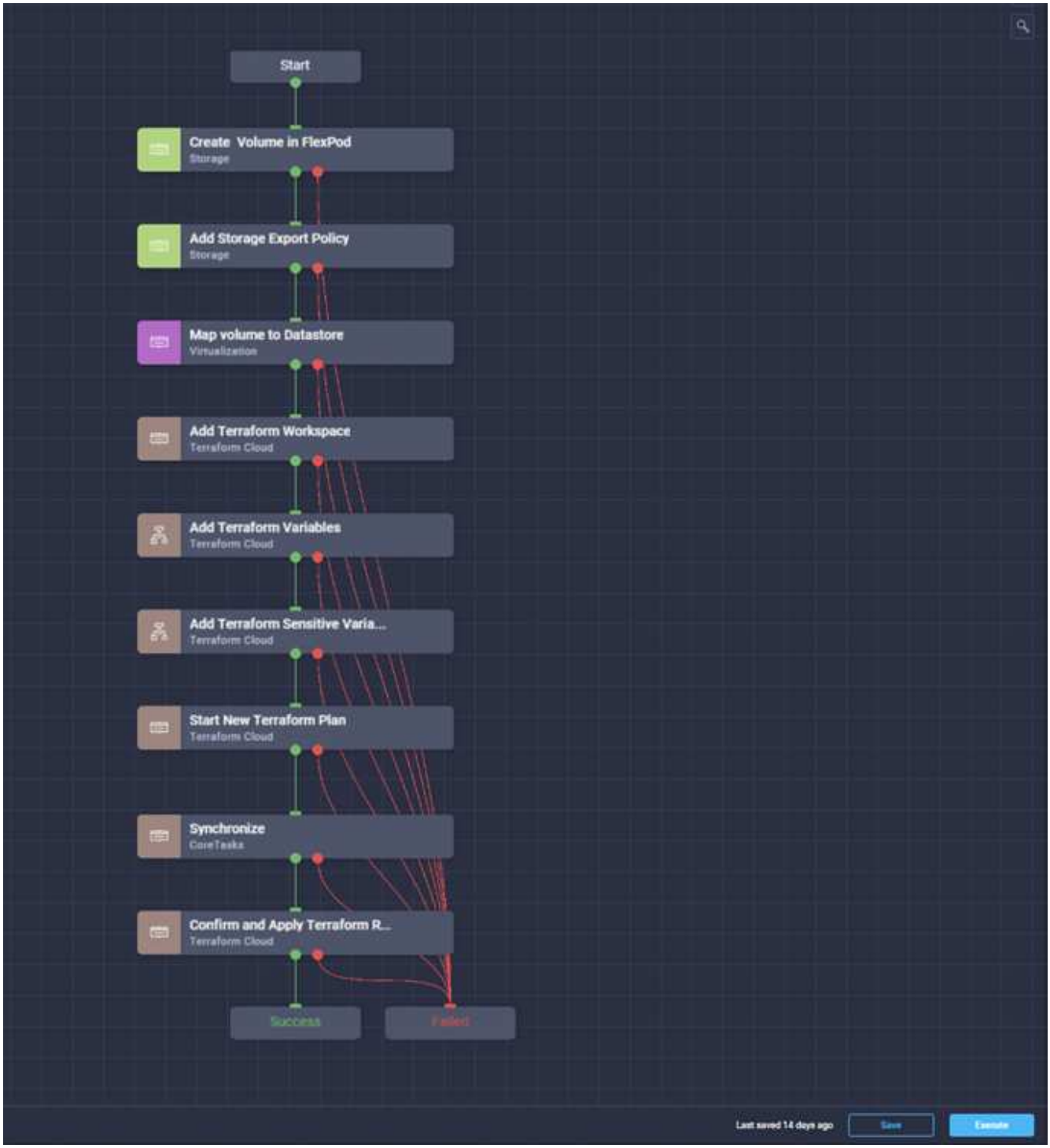
1. 디자이너 * 탭으로 이동하고 * 도구 * 섹션에서 * 작업 * 을 클릭합니다.
2. * Design * 영역의 * Tools * 섹션에서 * Terraform Cloud > Confirm and Apply Terraform Run * 작업을 끌어서 놓습니다.
3. 커넥터를 사용하여 작업 * 동기화 * 및 * Terraform 실행 확인 및 적용 * 을 연결합니다. 저장 * 을 클릭합니다.
4. Confirm(확인) * 과 * Apply Terraform Run(Terraform 실행 적용) * 을 클릭합니다. 작업 속성 * 영역에서 * 일반 * 탭을 클릭합니다. 필요에 따라 이 작업의 이름과 설명을 변경할 수 있습니다.



5. 작업 속성 * 영역에서 * 입력 * 을 클릭합니다.
6. Terraform Cloud Target * 필드에서 * Map * 을 클릭합니다.
7. 정적 값 * 을 선택하고 * 클라우드 타겟 선택 * 을 클릭합니다. 에 추가된 Terraform Cloud for Business 계정을 선택합니다 "HaashCorp Terraform에 대한 Cisco Intersight 서비스를 구성합니다".”
8. Map * 을 클릭합니다.
9. Run ID * 필드에서 * Map * 을 클릭합니다.
10. 직접 매핑 * 을 선택하고 * 작업 출력 * 을 클릭합니다.
11. 작업 이름 * 을 클릭하고 * 새 Terraform 계획 시작 * 을 클릭합니다.
12. 출력 이름 * 을 클릭한 다음 * 실행 ID * 를 클릭합니다.



13. Map * 을 클릭합니다.
14. 저장 * 을 클릭합니다.
15. 모든 작업이 정렬되도록 * 워크플로 자동 정렬 * 을 클릭합니다. 저장 * 을 클릭합니다.



그러면 Terraform 실행 확인 및 적용 작업이 완료됩니다. Connector를 사용하여 * Terraform Run * 작업 확인 및 적용과 * Success * 및 * Failed * 작업 간에 연결합니다.

절차 **11: Cisco**에서 만든 워크플로 가져오기

Cisco Intersight Cloud Orchestrator를 사용하면 Cisco Intersight 계정에서 시스템으로 워크플로우를 내보낸 다음 다른 계정으로 가져올 수 있습니다. JSON 파일은 사용자 계정으로 가져올 수 있는 기본 워크플로를 내보내서 생성되었습니다.

Workflow 구성 요소의 JSON 파일은 에서 사용할 수 있습니다 "GitHub 리포지토리".

"다음: 컨트롤러에서 Terraform 실행."

컨트롤러에서 **Terraform** 실행

"이전: DR 워크플로우."

컨트롤러를 사용하여 Terraform 계획을 실행할 수 있습니다. 이미 ICO 워크플로를 사용하여 Terraform 계획을 실행한 경우 이 섹션을 건너뛸 수 있습니다.

필수 구성 요소

솔루션의 설정은 인터넷에 액세스할 수 있고 Terraform의 설치가 정상적으로 작동하는 관리 워크스테이션에서 시작합니다.

Terraform 설치 설명서를 찾을 수 있습니다 "여기".

GitHub 를 다시 복제합니다

프로세스의 첫 번째 단계는 GitHub를 관리 워크스테이션의 새 빈 폴더에 복제하는 것입니다. GitHub 리포지토리를 클론하려면 다음 단계를 완료하십시오.

1. 관리 워크스테이션에서 프로젝트의 새 폴더를 만듭니다. 이 폴더 안에 '/root/SnapMirror-cvo'라는 새 폴더를 만들고 GitHub에 다시 복제합니다.
2. 관리 워크스테이션에서 명령줄 또는 콘솔 인터페이스를 열고 디렉토리를 방금 생성한 새 폴더로 변경합니다.
3. 다음 명령을 사용하여 GitHub 컬렉션을 복제합니다.

```
Git clone https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO
```

1. 디렉터리를 'napmirror-cvo'라는 새 폴더로 변경합니다.
    ◦ Terraform 실행 *



- * 초기화 * (로컬) Terraform 환경을 초기화합니다. 일반적으로 세션당 한 번만 실행됩니다.
- * Plan. * Terraform 상태를 클라우드의 AS-IN 상태와 비교하고 실행 계획을 수립 및 표시합니다. 이렇게 해도 배포는 변경되지 않습니다(읽기 전용).
- * 적용 * 계획 단계에서 계획을 적용합니다. 이렇게 하면 배포(읽기 및 쓰기)가 변경될 수 있습니다.
- * destroy. * 이 특정 Terraform 환경에 의해 관리되는 모든 리소스입니다.

  자세한 내용은 을 참조하십시오 "여기".

"다음: 솔루션 검증."

솔루션 검증

"이전: 컨트롤러에서 Terraform 실행."

이 섹션에서는 샘플 데이터 복제 워크플로우를 사용하여 솔루션을 다시 검토하고, 몇 가지 측정을 통해 FlexPod에서 실행되는 NetApp ONTAP 인스턴스에서 Google Cloud에서 실행되는 NetApp Cloud Volumes ONTAP로 데이터 복제가 수행되었는지 확인합니다.

이 솔루션에서 Cisco Intersight 워크플로우 오케스트레이터를 사용했으며 이 오케스트레이터는 앞으로도 당사의 활용 사례에 사용될 것입니다.

특히, 이 솔루션에 사용되는 제한된 Cisco Intersight 워크플로 집합은 Cisco Intersight에 장착된 전체 워크플로 집합을 나타내지 않습니다. 특정 요구 사항에 따라 사용자 지정 워크플로우를 생성하고 Cisco Intersight에서 트리거하도록 할 수 있습니다.

성공적인 DR 시나리오에 대한 유효성 검사를 수행하려면 먼저 FlexPod에 속한 ONTAP의 볼륨에서 SnapMirror를 사용하여 Cloud Volumes ONTAP로 데이터를 이동합니다. 그런 다음 Google 클라우드 컴퓨팅 인스턴스에서 데이터에 액세스한 후 데이터 무결성 검사를 수행할 수 있습니다.

이 솔루션의 성공 기준을 확인하는 데 사용되는 단계는 다음과 같습니다.

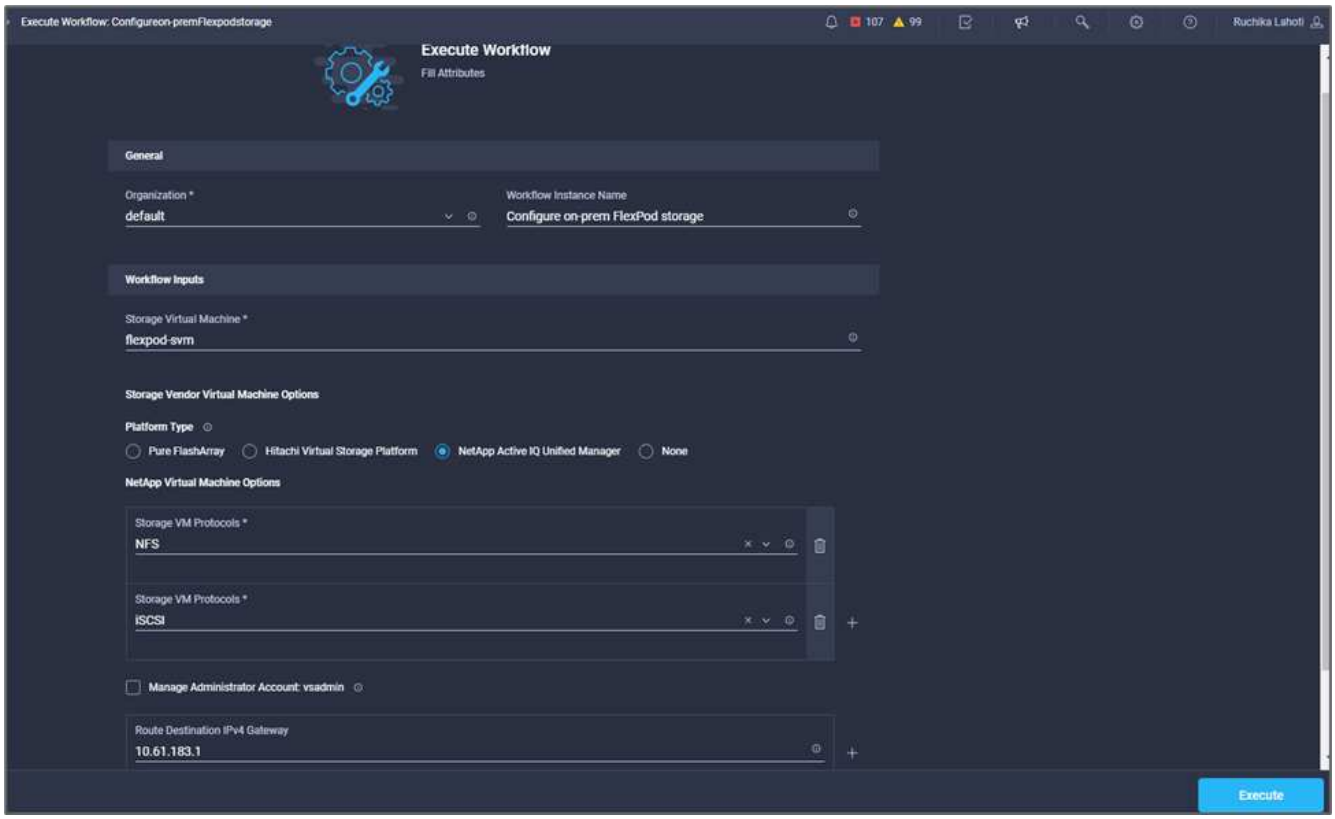
1. FlexPod의 ONTAP 볼륨에 있는 샘플 데이터 세트에 SHA256 체크섬을 생성합니다.
2. FlexPod에서 ONTAP와 Cloud Volumes ONTAP 간에 볼륨 SnapMirror 관계를 설정합니다.
3. 샘플 데이터 세트를 FlexPod에서 Cloud Volumes ONTAP로 복제합니다.
4. SnapMirror 관계를 유지하고 Cloud Volumes ONTAP의 볼륨을 운영 볼륨으로 승격하십시오.
5. Cloud Volumes ONTAP 볼륨과 데이터 세트를 Google Cloud의 컴퓨팅 인스턴스에 매핑합니다.
6. Cloud Volumes ONTAP의 샘플 데이터세트에 SHA256 체크섬을 생성합니다.
7. 소스와 대상의 체크섬을 비교합니다. 아마도 양쪽의 체크섬이 일치합니다.

온-프레미스 워크플로를 실행하려면 다음 단계를 완료합니다.

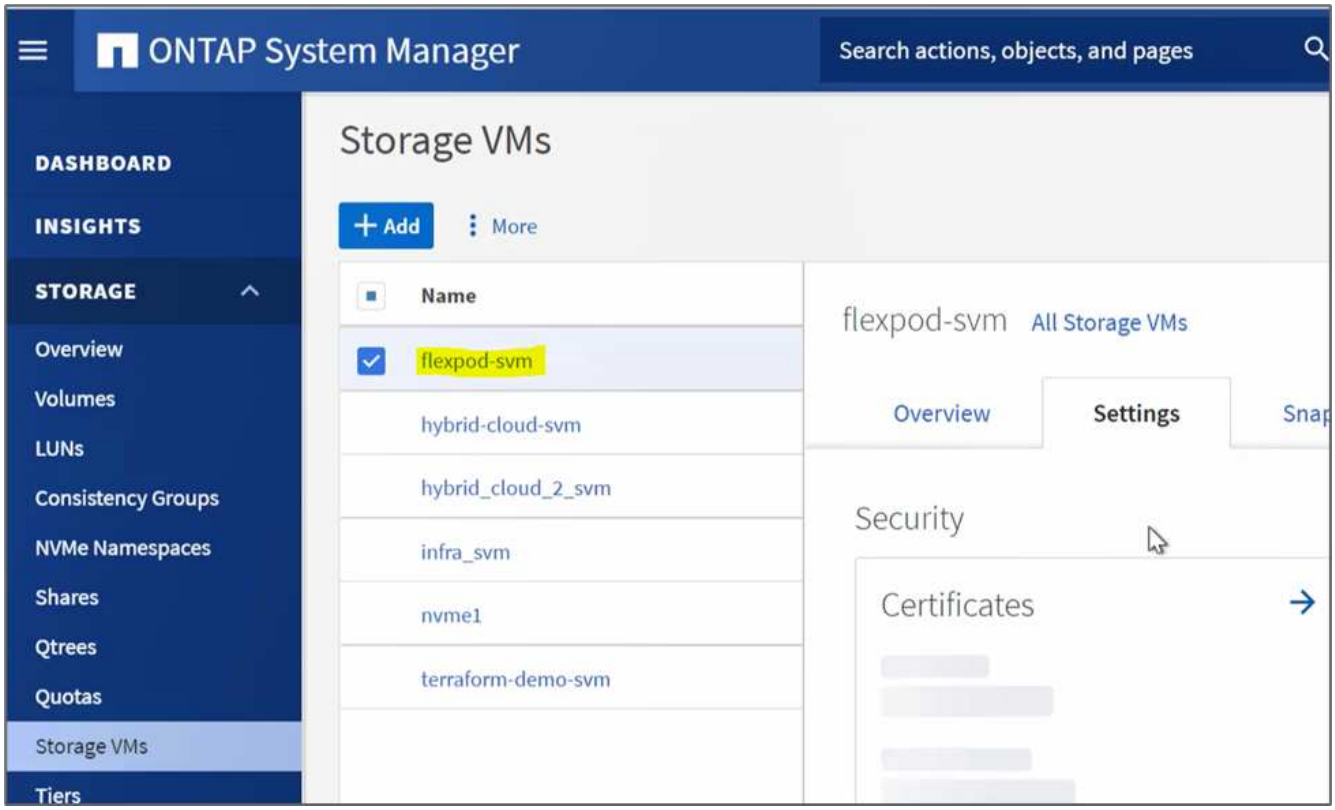
1. Intersight에서 온-프레미스 FlexPod에 대한 워크플로를 만듭니다.



2. 필요한 입력을 제공하고 워크플로우를 실행합니다.



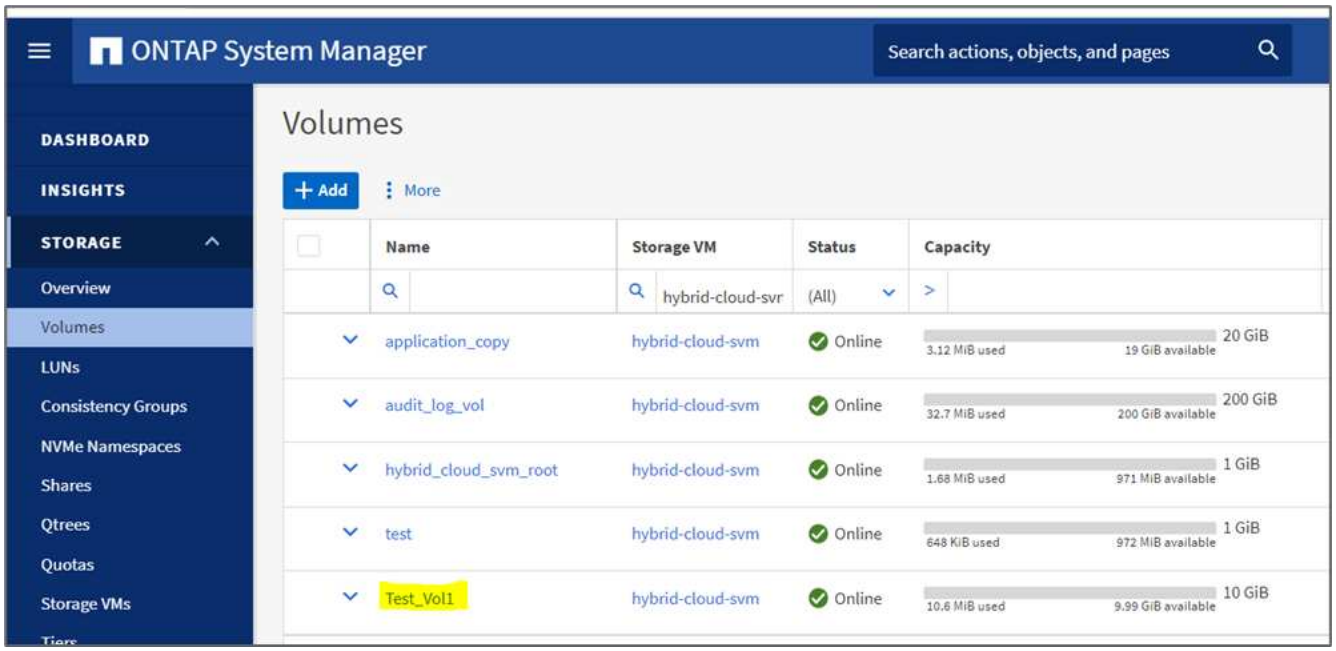
3. 시스템 관리자에서 새로 생성한 SVM을 확인합니다.



4. 또 다른 재해 복구 워크플로우를 생성 및 실행하여 온프레미스 FlexPod에 볼륨을 생성하고 FlexPod와 Cloud Volumes ONTAP에서 이 볼륨 간에 SnapMirror 관계를 설정합니다.



5. ONTAP system manager에서 새로 생성된 볼륨을 확인합니다.

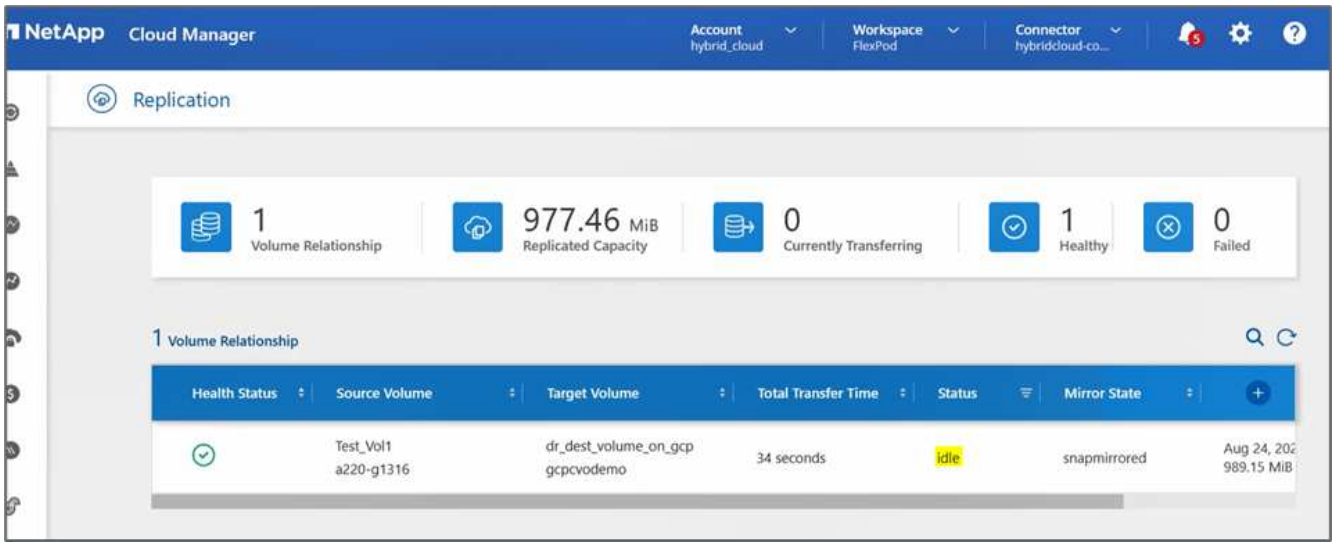


6. 동일한 NFS 볼륨을 사내 가상 머신에 마운트한 다음 샘플 데이터 세트를 복사하고 체크섬을 수행합니다.

```
root@hybridcloudbackup:/snapmirror_demo# mount -t nfs 172.22.4.157:/Test_Vol1 /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo# df -kh
Filesystem                Size  Used Avail Use% Mounted on
udev                      1.9G     0  1.9G   0% /dev
tmpfs                     394M  1.1M  393M   1% /run
/dev/sda2                  16G   11G  4.2G  72% /
tmpfs                     2.0G     0  2.0G   0% /dev/shm
tmpfs                     5.0M     0  5.0M   0% /run/lock
tmpfs                     2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1                 55M   55M     0 100% /snap/core18/1705
/dev/loop2                 69M   69M     0 100% /snap/lxd/14804
/dev/loop0                 28M   28M     0 100% /snap/snapd/7264
172.22.4.157:/Test_Vol1    10G  512K   10G   1% /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo#
```

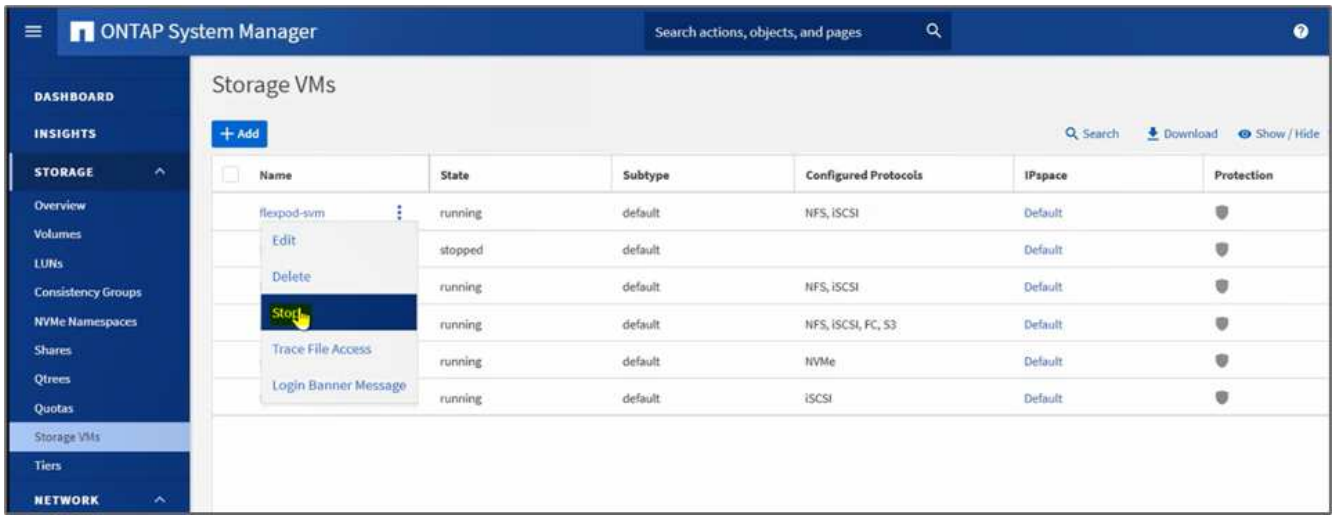
```
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo# sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo#
```

7. Cloud Manager에서 복제 상태를 확인합니다. 데이터 크기에 따라 데이터 전송에 몇 분이 걸릴 수 있습니다. 이 작업이 완료되면 SnapMirror 상태를 * 유휴 * 로 볼 수 있습니다.

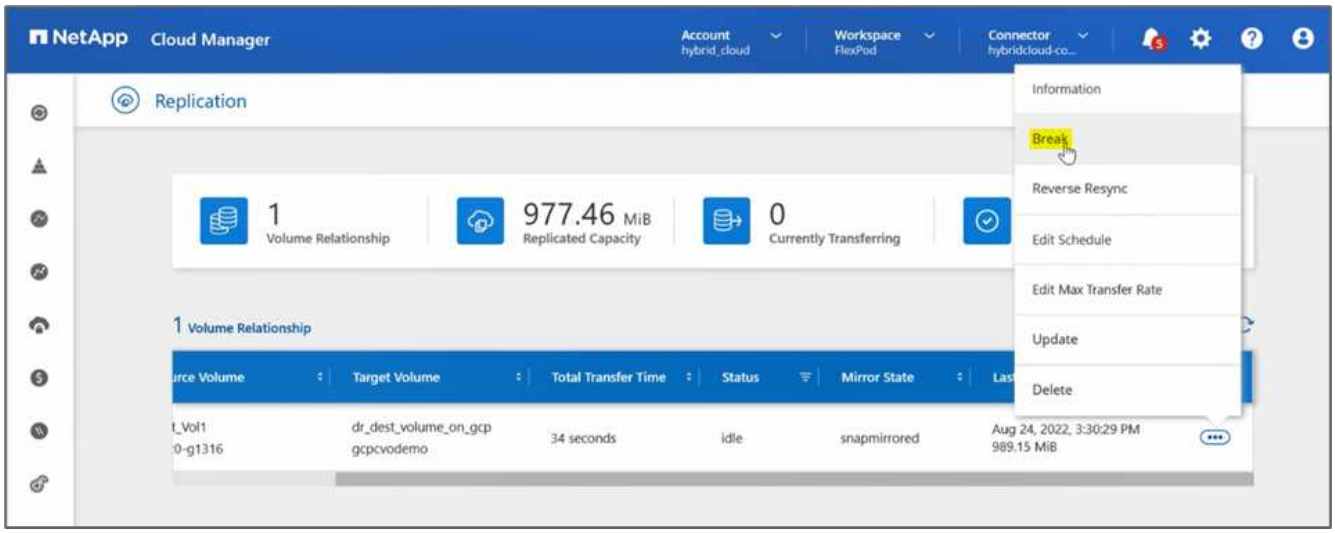


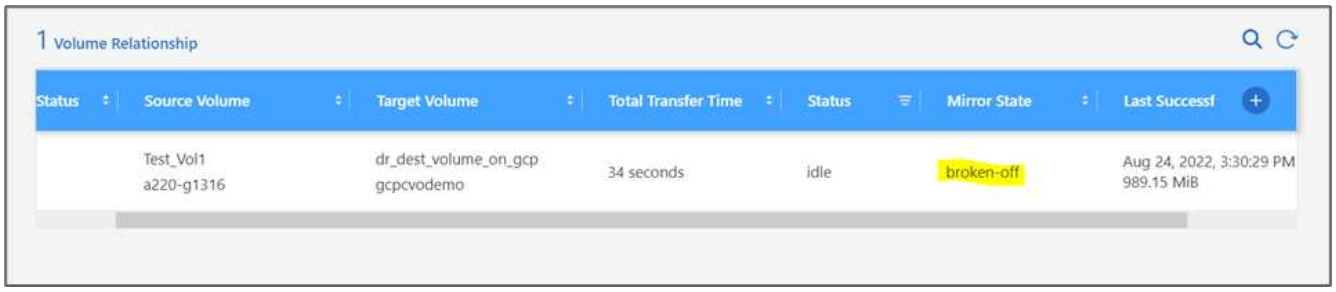
8. 데이터 전송이 완료되면 Test_vol1 볼륨을 호스팅하는 SVM을 중지하여 소스 측에서 재해를 시뮬레이션합니다.

   SVM이 중지된 후에는 Cloud Manager에서 Test_vol1 볼륨이 표시되지 않습니다.

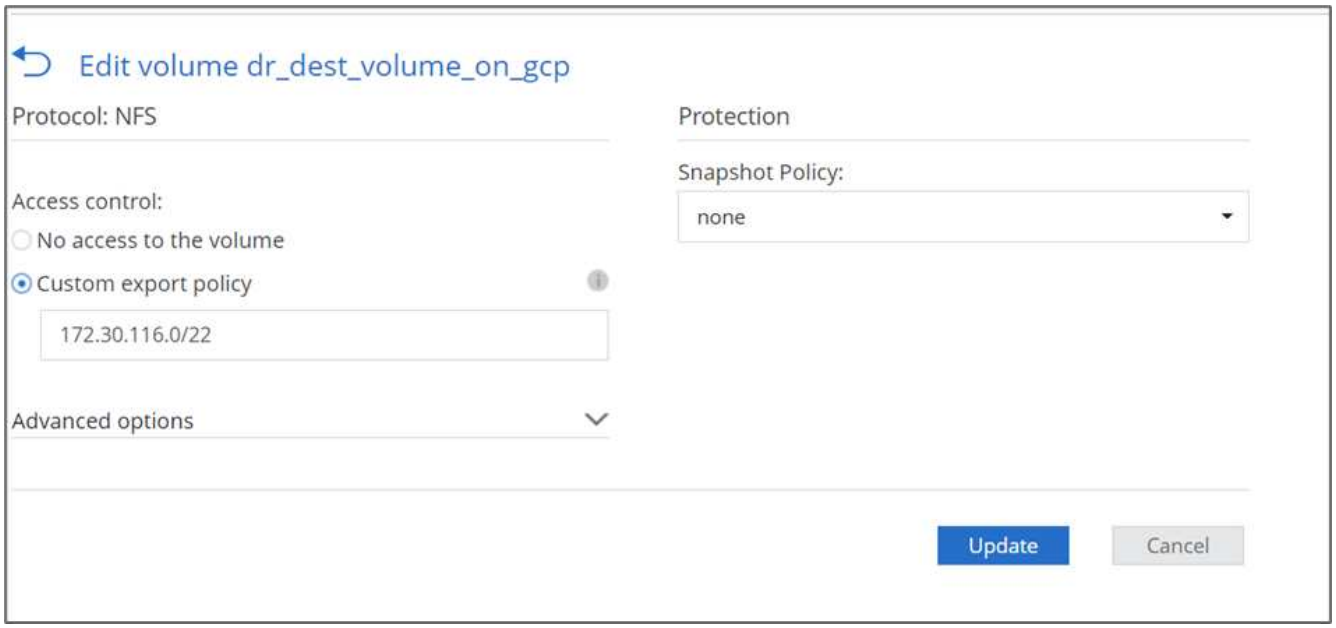


9. 복제 관계를 끊은 후 Cloud Volumes ONTAP 대상 볼륨을 운영 볼륨으로 승격합니다.

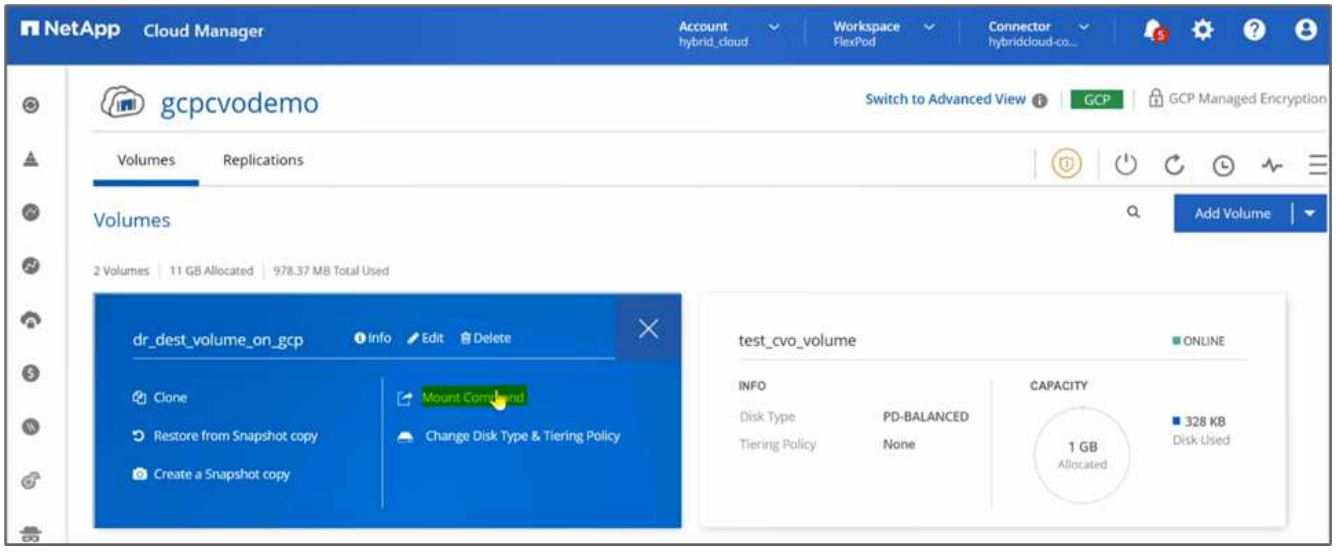




10. 볼륨을 편집하고 내보내기 정책에 연결하여 클라이언트 액세스를 활성화합니다.



11. 볼륨에 대한 즉시 사용 가능한 마운트 명령을 가져옵니다.





12. 컴퓨팅 인스턴스에 볼륨을 마운트하고 데이터가 대상 볼륨에 있는지 확인한 다음 'ample_dataset_2GB' 파일의 SHA256 체크섬을 생성합니다.

```
drwxr-xr-x 21 root   root             4096 Aug 24 10:20 ../
-rwxr-xr-x  1 nobody 4294967294 1015306240 Aug 24 09:59 test.zip*
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$ sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
```

13. 소스(FlexPod)와 대상(Cloud Volumes ONTAP) 모두에서 체크섬 값을 비교합니다.
14. 체크섬은 소스 및 대상과 일치합니다.

소스에서 대상으로 데이터 복제가 성공적으로 완료되었으며 데이터 무결성이 유지되었는지 확인할 수 있습니다. 이제 소스 사이트가 복구를 수행하는 동안 애플리케이션에서 이 데이터를 안전하게 사용하여 클라이언트에 제공할 수 있습니다.

"다음: 결론."

결론

"이전: 솔루션 검증."

이 솔루션에서는 Cisco Intersight Cloud Orchestrator를 기반으로 하는 퍼블릭 클라우드를 통해 DR 솔루션을 구축하는 데 NetApp Cloud Data Service, Cloud Volumes ONTAP 및 FlexPod Datacenter 인프라가 사용되었습니다. FlexPod 솔루션은 고객이 애플리케이션 및 비즈니스 제공 프로세스를 현대화할 수 있도록 지속적으로 진화해 왔습니다. 이 솔루션을 사용하면 DR 솔루션 비용을 낮게 유지하면서 임시 또는 전체 시간 DR 계획을 위한 전환 위치로 퍼블릭 클라우드에 BCDR 계획을 수립할 수 있습니다.

사내 FlexPod와 NetApp Cloud Volumes ONTAP 간 데이터 복제는 검증된 SnapMirror 기술을 통해 처리되었지만, 데이터 이동성 요구사항에 맞춰 Cloud Sync와 같은 다른 NetApp 데이터 전송 및 동기화 툴을 선택할 수도 있습니다. TLS/AES 기반의 내장 암호화 기술로 전송 중인 데이터의 보안

애플리케이션에 대한 임시 DR 계획이 있거나 비즈니스에 대한 전체 재해 복구 계획이 있는 경우 이 솔루션에 사용되는 제품 포트폴리오는 규모에 따라 두 가지 요구 사항을 모두 충족할 수 있습니다. Cisco Intersight Workflow

Orchestrator를 기반으로 하므로 사전 구축된 워크플로우를 통해 프로세스를 재구성할 필요가 없으며 BCDR 계획의 구현 속도를 높일 수 있습니다.

이 솔루션을 사용하면 Cisco Intersight Cloud Orchestrator에서 제공하는 자동화 및 오케스트레이션을 통해 하이브리드 클라우드 전반에서 FlexPod 온프레미스 및 데이터 복제를 매우 쉽고 편리하게 관리할 수 있습니다.

추가 정보를 찾을 수 있는 위치

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

GitHub를 참조하십시오

- 모든 Terraform 설정이 사용됩니다

  "https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO"

- 워크플로 가져오기를 위한 JSON 파일

  "https://github.com/ucs-compute-solutions/FlexPod_DR_Workflows"

Cisco Intersight를 참조하십시오

- Cisco Intersight 도움말 센터

  "https://intersight.com/help/saas/home"

- Cisco Intersight Cloud Orchestrator 설명서:

  "https://intersight.com/help/saas/features/orchestration/configure#intersight_cloud_orchestrator"

- HiashCorp Terraform 문서용 Cisco Intersight 서비스

  "https://intersight.com/help/saas/features/terraform_cloud/admin"

- Cisco Intersight 데이터시트

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html"

- Cisco Intersight Cloud Orchestrator 데이터 시트

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-cloud-orch-aag-cte-en.html"

- HiashCorp Terraform Data Sheet를 위한 Cisco Intersight 서비스

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-terraf-ser-aag-cte-en.html"

FlexPod

- FlexPod 홈 페이지

"https://www.flexpod.com"

- FlexPod용 Cisco Validated Design 및 구축 가이드

  "UCS 관리 모드, VMware vSphere 7.0 U2 및 NetApp ONTAP 9.9에서 Cisco UCS 4.2(1)가 지원되는 FlexPod 데이터 센터 설계 가이드"

- Cisco UCS X-Series 및 FlexPod 데이터 센터

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"

상호 운용성

- NetApp 상호 운용성 매트릭스 툴

  "http://support.netapp.com/matrix/"

- Cisco UCS 하드웨어 및 소프트웨어 상호 운용성 툴

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- VMware 호환성 가이드 를 참조하십시오

  "http://www.vmware.com/resources/compatibility/search.php"

NetApp Cloud Volumes ONTAP 참조 문서

- NetApp 클라우드 관리자

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- Cloud Volumes ONTAP

  https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-gcp.html

- Cloud Volumes ONTAP TCO 계산기

  https://cloud.netapp.com/google-cloud-calculator

- Cloud Volumes ONTAP Sizer

  "https://cloud.netapp.com/cvo-sizer"

- 클라우드 평가 툴

  https://cloud.netapp.com/assessments

- NetApp 하이브리드 클라우드

  https://cloud.netapp.com/hybrid-cloud

- Cloud Manager API 설명서

"https://docs.netapp.com/us-en/occm/reference_infrastructure_as_code.html"

문제 해결

"https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Cloud_Volumes_ONTAP_(CVO)"

Terraform(Terraform

- Terraform 클라우드

  "https://www.terraform.io/cloud"

- Terraform 문서

  "https://www.terraform.io/docs/"

- NetApp Cloud Manager 레지스트리

  "https://registry.terraform.io/providers/NetApp/netapp-cloudmanager/lates"

GCP

- GCP용 ONTAP 고가용성

  "https://cloud.netapp.com/blog/gcp-cvo-blg-what-makes-cloud-volumes-ontap-high-availability-for-gcp-tick"

- GCP 페르쿼트

  https://netapp.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=f3d0368b-7165-4d43-a76e-ae01011853d6

NetApp Astra 및 Cisco Intersight, Red Hat OpenShift를 포함하는 FlexPod 하이브리드 클라우드

TR-4936: NetApp Astra 및 Cisco Intersight for Red Hat OpenShift를 포함하는 FlexPod 하이브리드 클라우드

Abhinav Singh입니다

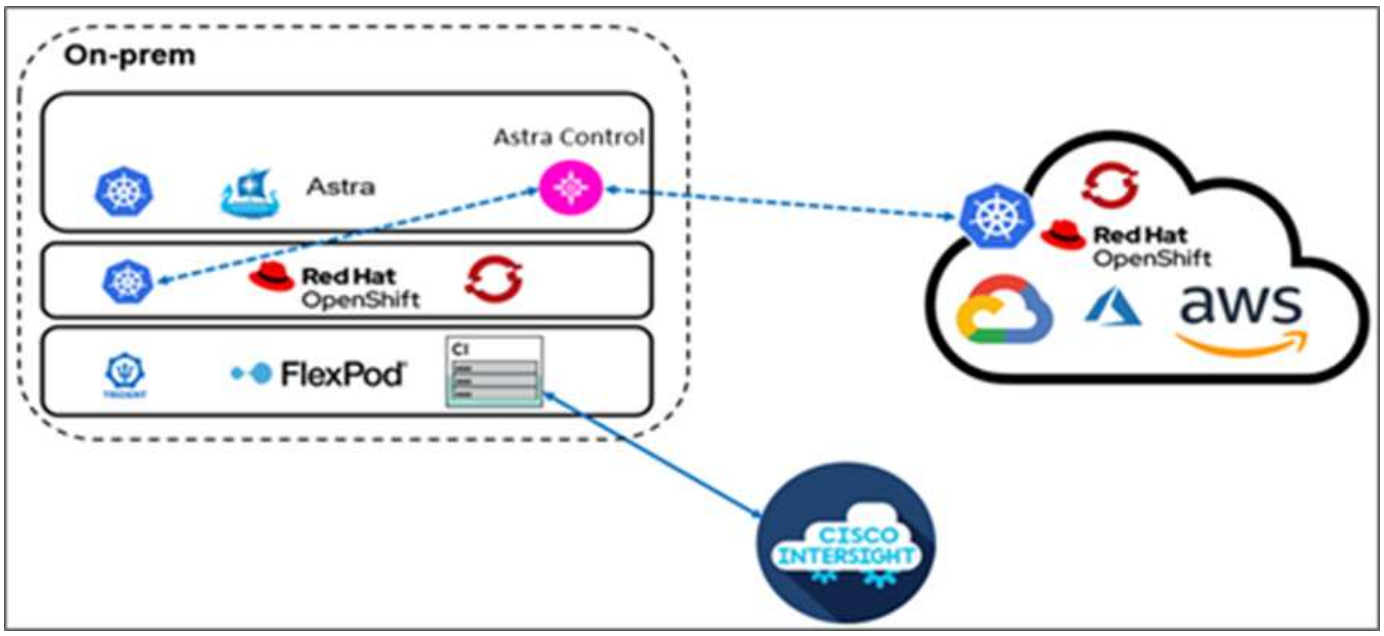
소개

컨테이너와 Kubernetes가 컨테이너화된 앱의 개발, 구축, 실행, 관리, 확장을 위한 실질적인 선택이 됨에 따라 기업에서 비즈니스 크리티컬 애플리케이션을 점차 실행하고 있습니다. 비즈니스 크리티컬 애플리케이션은 주로 상태에 따라 달라집니다. 상태 저장 응용 프로그램은 상태, 데이터 및 구성 정보를 연결하며 비즈니스 논리를 실행하기 위해 이전 데이터 트랜잭션에 의존합니다. Kubernetes에서 실행 중인 비즈니스 크리티컬 애플리케이션은 기존 애플리케이션과 같은 가용성 및 비즈니스 연속성 요구사항을 지속적으로 충족합니다. 서비스 중단이 매출, 생산성 및 회사 평판에 심각한 영향을 미칠 수 있습니다. 따라서 클러스터, 온프레미스 데이터 센터 및 하이브리드 클라우드 환경 내부와 클러스터 간에 Kubernetes 워크로드를 빠르고 쉽게 보호, 복구, 이동하는 것이 매우 중요합니다. 기업들은 비즈니스를 하이브리드 클라우드 모델로 전환하고 애플리케이션을 클라우드 네이티브 폼 팩터로 전환하는 이점을 누리고 있습니다.

이 기술 보고서는 FlexPod 통합 인프라 솔루션 기반 Red Hat OpenShift Container Platform과 NetApp Astra

Control Center를 결합하여 AWS(Amazon Web Services)로 확장하여 하이브리드 클라우드 데이터 센터를 구축합니다. 친숙함을 바탕으로 구축 "FlexPod 및 Red Hat OpenShift", 이 문서에서는 설치, 구성, 애플리케이션 보호 워크플로우 및 사내/클라우드 간 애플리케이션 마이그레이션부터 시작되는 NetApp Astra Control Center에 대해 설명합니다. 또한, Red Hat OpenShift에서 실행되는 컨테이너형 애플리케이션에 NetApp Astra Control Center를 사용할 때 백업 및 복구, 비즈니스 연속성 등의 애플리케이션 인식 데이터 관리 기능의 이점에 대해 설명합니다.

다음 그림에서는 솔루션 개요를 보여 줍니다.



대상

이 문서는 CTO(최고 기술 책임자), 애플리케이션 개발자, 클라우드 솔루션 설계자, SRE(사이트 안정성 엔지니어), DevOps 엔지니어, ITOps 및 컨테이너식 애플리케이션의 설계, 호스팅, 관리에 중점을 둔 프로페셔널 서비스 팀을 대상으로 합니다.

NetApp Astra Control – 주요 사용 사례

NetApp Astra Control은 클라우드 네이티브 마이크로서비스를 처리하는 고객을 위해 애플리케이션 보호를 단순화하는 것을 목표로 합니다.

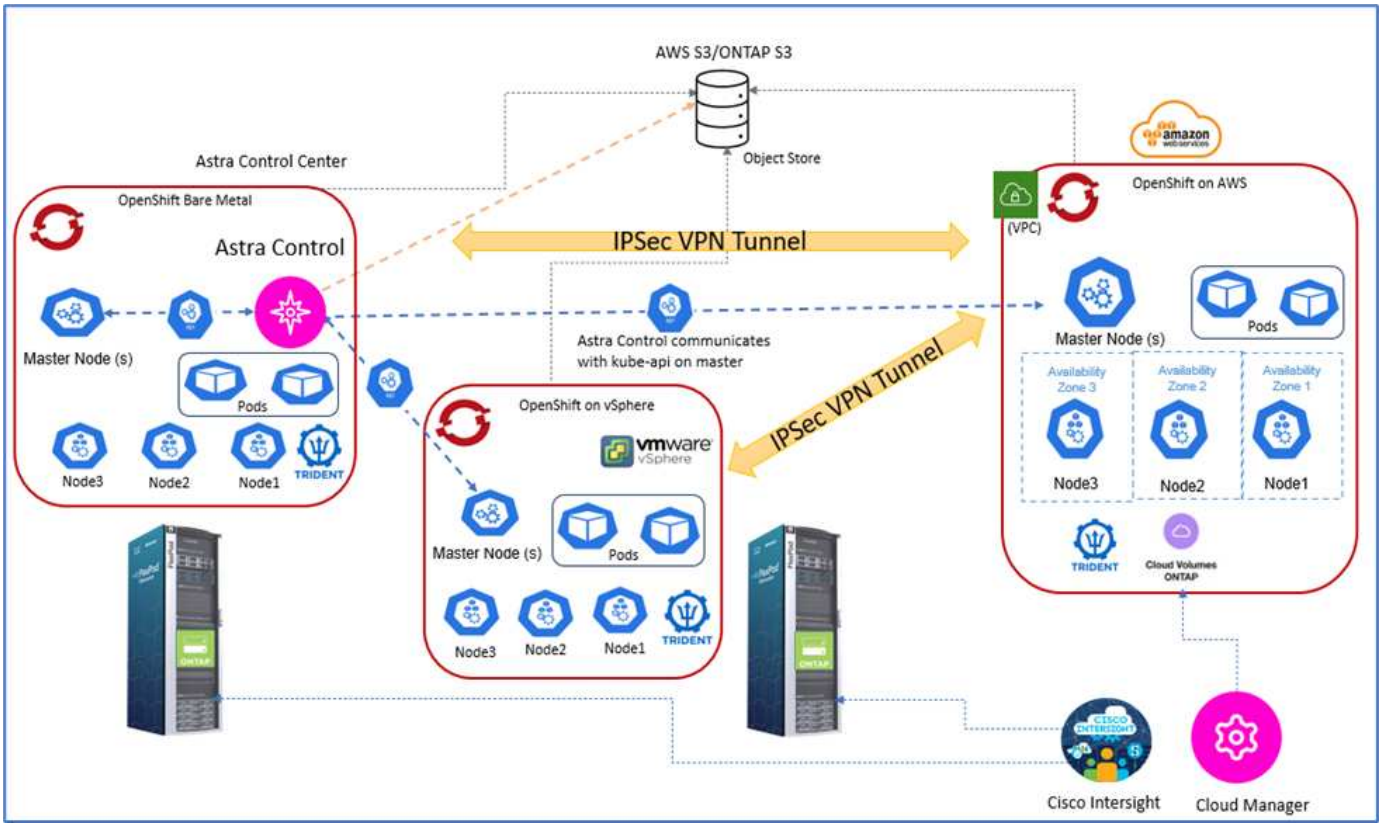
- * 스냅샷을 사용한 시점(PiT) 애플리케이션 표현 * Astra Control을 사용하면 Kubernetes에서 실행되는 애플리케이션의 구성 세부 정보와 관련 영구 스토리지를 포함하는 컨테이너화된 애플리케이션의 엔드 투 엔드 스냅샷을 생성할 수 있습니다. 인시던트가 발생한 경우 버튼 클릭 시 정상 작동이 확인된 상태로 응용 프로그램을 복원할 수 있습니다.
- * 전체 복제 애플리케이션 백업. * Astra Control을 사용하면 사전 정의된 일정에 따라 전체 애플리케이션 백업을 수행할 수 있습니다. 이 백업은 애플리케이션을 동일한 K8s 클러스터 또는 자동화된 방식으로 필요에 따라 다른 K8s 클러스터로 복원하는 데 사용할 수 있습니다.
- * 클론을 사용한 애플리케이션 이식성 및 마이그레이션 * Astra Control을 사용하면 전체 애플리케이션과 함께 Kubernetes 클러스터 간에 또는 동일한 K8s 클러스터 내에서 데이터를 복제할 수 있습니다. 이 기능은 또한 클러스터의 위치에 관계없이 K8s 클러스터 간에 애플리케이션을 포팅하거나 마이그레이션하는 데 도움이 됩니다 (클론 생성 후 소스 애플리케이션 인스턴스를 삭제하기만 함).
- * 응용 프로그램 일관성 사용자 지정. * Astra Control을 사용하면 실행 후크를 활용하여 응용 프로그램 중지 상태 정의를 제어할 수 있습니다. 스냅샷 및 백업 워크플로우에 '사전' 및 '사후' 실행 후크를 놓으면 스냅샷 또는 백업을 수행하기 전에 응용 프로그램이 자동으로 정지됩니다.

- * 응용 프로그램 수준 재해 복구(DR) 자동화 * Astra Control을 사용하면 컨테이너화된 응용 프로그램에 대한 BCDR(비즈니스 연속성 재해 복구) 계획을 구성할 수 있습니다. NetApp SnapMirror는 백엔드에서 사용되며 DR 워크플로우의 전체 구현이 자동화됩니다.

솔루션 토폴로지

이 섹션에서는 솔루션의 논리적 토폴로지를 설명합니다.

다음 그림은 OpenShift 컨테이너 플랫폼 클러스터를 실행하는 FlexPod 사내 환경과 NetApp Cloud Volumes ONTAP, Cisco Intersight, NetApp Cloud Manager SaaS 플랫폼을 지원하는 AWS 기반 셀프 관리 OpenShift Container Platform 클러스터로 구성된 솔루션 토폴로지를 나타낸 것입니다.



첫 번째 OpenShift Container Platform 클러스터는 FlexPod에 베어 메탈 설치이고, 두 번째 OpenShift Container Platform 클러스터는 FlexPod에서 실행되는 VMware vSphere에 배포되며, 세 번째 OpenShift Container Platform 클러스터는 로 배포됩니다 "프라이빗 클러스터" 자체 관리 인프라로서 AWS에 있는 기존 VPC(가상 프라이빗 클라우드)에 통합할 수 있습니다.

이 솔루션에서 FlexPod는 사이트 간 VPN을 통해 AWS에 연결되지만, 고객은 직접 연결 구현을 사용하여 하이브리드 클라우드로 확장할 수도 있습니다. Cisco Intersight는 FlexPod 인프라 구성 요소를 관리하는 데 사용됩니다.

이 솔루션에서 Astra Control Center는 FlexPod 및 AWS에서 실행되는 OpenShift Container Platform 클러스터에서 호스팅되는 컨테이너식 애플리케이션을 관리합니다. Astra Control Center는 FlexPod에서 실행되는 OpenShift 베어 메탈 인스턴스에 설치됩니다. Astra Control은 마스터 노드의 kube-API와 통신하며 Kubernetes 클러스터의 변경 사항을 지속적으로 확인합니다. K8s 클러스터에 추가된 모든 새 애플리케이션이 자동으로 검색되어 관리 작업에 사용할 수 있게 됩니다.

Astra Control Center를 사용하여 컨테이너화된 애플리케이션을 스냅샷으로 캡처할 수 있습니다. 애플리케이션 스냅샷은 예약된 보호 정책 또는 필요 시 트리거될 수 있습니다. Astra가 지원하는 애플리케이션의 경우 스냅샷이 충돌에 따라 정합성이 보장됩니다. 애플리케이션 스냅샷은 영구 볼륨의 애플리케이션 데이터 스냅샷과 해당 애플리케이션과

관련된 다양한 Kubernetes 리소스의 애플리케이션 메타데이터를 구성합니다.

Astra Control을 사용하여 사전 정의된 백업 스케줄을 사용하거나 필요에 따라 애플리케이션 전체 복제본 백업을 생성할 수 있습니다. 오브젝트 스토리지는 애플리케이션 데이터의 백업을 저장하는 데 사용됩니다. NetApp ONTAP S3, NetApp StorageGRID 및 모든 일반 S3 구현을 오브젝트 저장소로 사용할 수 있습니다.

"다음: 솔루션 구성 요소."

솔루션 구성 요소

"이전: 솔루션 개요"

FlexPod

FlexPod는 가상화된 솔루션과 가상화되지 않은 솔루션 모두를 위한 통합된 기반을 형성하는 정의된 하드웨어 및 소프트웨어 세트입니다. FlexPod에는 NetApp ONTAP 스토리지, Cisco Nexus 네트워킹, Cisco MDS 스토리지 네트워킹, Cisco UCS(Unified Computing System)가 포함되어 있습니다. 이 설계는 네트워킹, 컴퓨팅 및 스토리지가 하나의 데이터 센터 랙에 장착되거나 고객의 데이터 센터 설계에 따라 배포될 수 있을 만큼 유연합니다. 포트 밀도를 통해 네트워킹 구성 요소가 여러 구성을 수용할 수 있습니다.

아스트라 컨트롤

Astra Control은 퍼블릭 클라우드와 사내 모두에서 호스팅되는 클라우드 네이티브 애플리케이션을 위한 애플리케이션 인식 데이터 보호 서비스를 제공합니다. Astra Control은 Kubernetes에서 실행되는 컨테이너식 애플리케이션을 위한 데이터 보호, 재해 복구 및 마이그레이션 기능을 제공합니다.

피처

Astra Control은 Kubernetes 애플리케이션 데이터 라이프사이클 관리에 중요한 기능을 제공합니다.

- 영구 스토리지를 자동으로 관리합니다
- 애플리케이션 정합성이 보장되는 온디맨드 스냅샷 및 백업을 생성합니다
- 자동화된 정책 기반 스냅샷 및 백업 작업
- 하이브리드 클라우드 설정에서 Kubernetes 클러스터 간에 애플리케이션 및 관련 데이터를 마이그레이션합니다
- 애플리케이션을 동일한 K8s 클러스터 또는 다른 K8s 클러스터로 클론 복제합니다
- 애플리케이션 보호 상태를 시각화합니다
- 그래픽 사용자 인터페이스 및 REST API의 전체 목록을 제공하여 기존 사내 툴에서 모든 보호 워크플로우를 구현합니다.

Astra Control은 Kubernetes 클러스터에서 생성된 관련 리소스에 대한 통찰력을 포함하는 컨테이너식 애플리케이션에 대한 단일 창 방식의 시각화를 제공합니다. 단일 포털을 통해 모든 클러스터, 모든 앱, 모든 클라우드 또는 모든 데이터 센터를 볼 수 있습니다. 온프레미스 또는 퍼블릭 클라우드의 모든 환경에서 Astra Control API를 사용하여 데이터 관리 워크플로우를 구축할 수 있습니다.

Astra Control 소비 모델

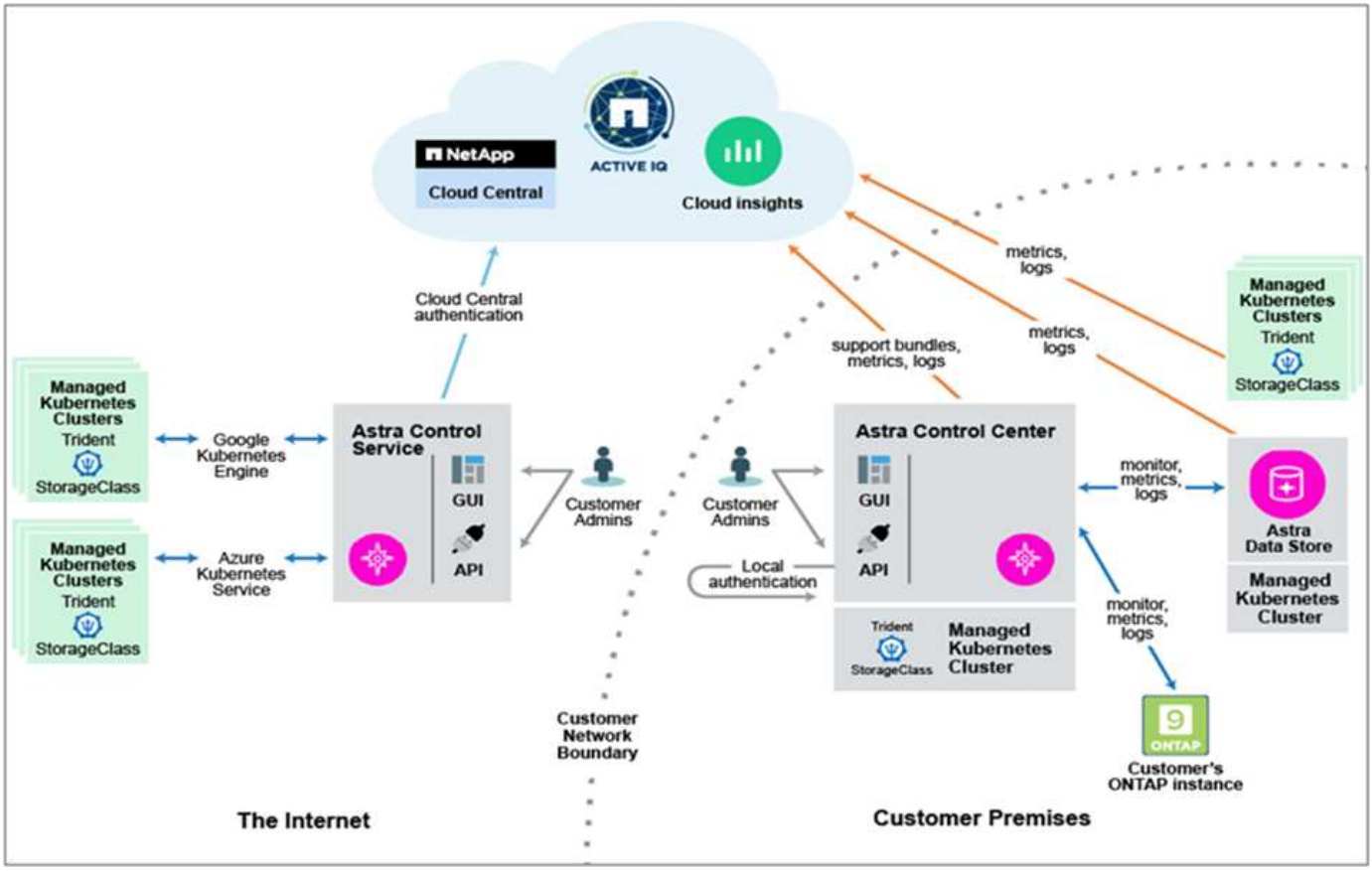
Astra Control은 두 가지 소비 모델로 제공됩니다.

- * Astra Control Service. * NetApp에서 호스팅하는 완전 관리형 서비스로, GKE(Google Kubernetes Engine), AKS(Azure Kubernetes Service)에서 Kubernetes 클러스터의 애플리케이션 인식 데이터 관리를 제공합니다.

- * Astra Control Center. * 사내 및 하이브리드 클라우드 환경에서 실행되는 Kubernetes 클러스터의 애플리케이션 인식 데이터 관리를 제공하는 자체 관리 소프트웨어입니다.

이 기술 보고서에서는 Kubernetes에서 실행되는 클라우드 네이티브 애플리케이션을 관리하기 위해 Astra Control Center를 활용합니다.

다음 이미지는 Astra Control 아키텍처를 보여 줍니다.



아스트라 트리덴트

Astra Trident는 컨테이너 및 Kubernetes 배포를 위한 완전히 지원되는 오픈 소스 스토리지 오케스트레이터입니다. 이 제품은 처음부터 와 같은 업계 표준 인터페이스를 사용하여 컨테이너화된 애플리케이션의 지속성 요구를 충족하도록 설계되었습니다 "컨테이너 스토리지 인터페이스(CSI)". Astra Trident를 사용하면 마이크로서비스 및 컨테이너식 애플리케이션에서 NetApp 스토리지 시스템 포트폴리오에서 제공하는 엔터프라이즈급 스토리지 서비스를 활용할 수 있습니다.

Astra Trident Kubernetes 클러스터에 Pod 형태로 배포되며 Kubernetes 워크로드에 대한 동적 스토리지 오케스트레이션 서비스를 제공합니다. NetApp ONTAP (NetApp AFF, NetApp FAS, NetApp ONTAP Select, Cloud, Amazon FSx for NetApp ONTAP), NetApp Element 소프트웨어(NetApp SolidFire) 및 Azure NetApp Files 서비스를 포함한 NetApp의 광범위한 포트폴리오에서 컨테이너화된 애플리케이션이 영구 스토리지를 빠르고 쉽게 사용할 수 있도록 해줍니다. FlexPod 환경에서 Astra Trident 는 NetApp AFF 및 FAS 시스템, Cloud Volumes ONTAP 과 같은 ONTAP 스토리지 플랫폼에 호스팅된 NetApp FlexVol 볼륨 및 LUN에 의해 지원되는 컨테이너에 대한 영구 볼륨을 동적으로 프로비저닝하고 관리하는 데 사용됩니다. Trident 또한 Astra Control이 제공하는 애플리케이션 보호 체계 구현에 있어서 핵심적인 역할을 합니다. Astra Trident 에 대한 자세한 내용은 다음을 참조하세요. "Astra Trident 문서."

스토리지 백엔드

Astra Trident를 사용하려면 지원되는 스토리지 백엔드가 필요합니다. Trident 백엔드는 Trident와 스토리지 시스템 간의 관계를 정의합니다. Trident는 해당 스토리지 시스템과 통신하는 방법과 Trident가 스토리지 시스템에서 볼륨을 프로비저닝하는 방법을 알려줍니다. Trident는 스토리지 클래스에 정의된 요구 사항과 일치하는 백엔드에서 스토리지 풀을 자동으로 제공합니다.

- ONTAP AFF 및 FAS 스토리지 백엔드 스토리지 소프트웨어 및 하드웨어 플랫폼인 ONTAP는 핵심 스토리지 서비스, 다중 스토리지 액세스 프로토콜 지원 및 NetApp Snapshot 복사본 및 미러링과 같은 스토리지 관리 기능을 제공합니다.
- Cloud Volumes ONTAP 스토리지 백엔드
- "Astra 데이터 저장소" 스토리지 백엔드

NetApp Cloud Volumes ONTAP를 참조하십시오

NetApp Cloud Volumes ONTAP는 파일 및 블록 워크로드에 대한 고급 데이터 관리 기능을 제공하는 소프트웨어 정의 스토리지 오퍼링입니다. Cloud Volumes ONTAP을 사용하면 클라우드 스토리지 비용을 최적화하고 애플리케이션 성능을 높이는 동시에 데이터 보호, 보안 및 규정 준수를 향상할 수 있습니다.

주요 이점은 다음과 같습니다.

- 내장된 데이터 중복제거, 데이터 압축, 씬 프로비저닝 및 복제를 활용하여 스토리지 비용을 최소화합니다.
- 클라우드 환경에서 장애가 발생할 경우 엔터프라이즈급 안정성과 지속적인 운영을 보장합니다.
- Cloud Volumes ONTAP는 업계 최고 수준의 NetApp 복제 기술인 SnapMirror를 활용하여 사내 데이터를 클라우드로 복제하므로 여러 사용 사례에서 보조 복사본을 쉽게 사용할 수 있습니다.
- Cloud Volumes ONTAP은 또한 Cloud Backup Service과 통합되어 클라우드 데이터를 보호하고 장기적으로 보관하기 위한 백업 및 복원 기능을 제공합니다.
- 애플리케이션을 오프라인으로 전환하지 않고도 필요에 따라 고성능 및 고성능 스토리지 풀 간에 전환할 수 있습니다.
- NetApp SnapCenter를 사용하여 스냅샷 복사본의 일관성 보장
- Cloud Volumes ONTAP는 데이터 암호화를 지원하고 바이러스 및 랜섬웨어에 대한 보호를 제공합니다.
- 클라우드 데이터 센스와 통합되어 데이터 컨텍스트를 이해하고 중요한 데이터를 식별할 수 있습니다.

Cloud Central을 참조하십시오

Cloud Central은 NetApp 클라우드 데이터 서비스에 액세스하고 이를 관리할 수 있는 중앙의 위치입니다. 이러한 서비스를 사용하여 클라우드에서 중요한 애플리케이션을 실행하고, 자동화된 DR 사이트를 생성하고, 데이터를 백업하고, 여러 클라우드 간에 데이터를 효과적으로 마이그레이션 및 제어할 수 있습니다. 자세한 내용은 을 참조하십시오 "Cloud Central을 참조하십시오."

클라우드 관리자

Cloud Manager는 엔터프라이즈급 SaaS 기반 관리 플랫폼으로, IT 전문가 및 클라우드 설계자가 NetApp의 클라우드 솔루션을 사용하여 하이브리드 멀티 클라우드 인프라를 중앙에서 관리할 수 있도록 지원합니다. 이 솔루션은 사내 및 클라우드 스토리지를 중앙 집중식으로 확인 및 관리할 수 있는 시스템을 제공하여 하이브리드, 다중 클라우드 공급자 및 계정을 지원합니다. 자세한 내용은 을 참조하십시오 "클라우드 관리자".

커넥터

Connector는 Cloud Manager가 퍼블릭 클라우드 환경 내의 리소스 및 프로세스를 관리할 수 있도록 하는 인스턴스입니다. Cloud Manager가 제공하는 다양한 기능을 사용하려면 Connector가 필요합니다. Connector는 클라우드 또는 온프레미스 네트워크에 구축할 수 있습니다.

커넥터는 다음 위치에서 지원됩니다.

- 설치하고
- Microsoft Azure를 참조하십시오
- Google 클라우드
- 온프레미스

Connector에 대한 자세한 내용은 을 참조하십시오 "이 링크."

NetApp Cloud Insights를 참조하십시오

NetApp 클라우드 인프라 모니터링 툴인 Cloud Insights를 사용하면 Astra Control Center에서 관리하는 Kubernetes 클러스터의 성능과 활용률을 모니터링할 수 있습니다. Cloud Insights는 스토리지 사용량과 워크로드를 상호 연관시킵니다. Astra Control Center에서 Cloud Insights 연결을 활성화하면 Astra Control Center UI 페이지에 원격 측정 정보가 표시됩니다.

NetApp Active IQ Unified Manager를 참조하십시오

NetApp Active IQ Unified Manager를 사용하면 재설계된 직관적인 단일 인터페이스를 통해 ONTAP 스토리지 클러스터를 모니터링하여 커뮤니티의 지혜 및 AI 분석을 제공할 수 있습니다. 스토리지 환경과 VM(가상 시스템)에 대한 포괄적인 운영, 성능 및 사전 통찰력을 제공합니다. 스토리지 인프라에서 문제가 발생하면 Unified Manager에서 문제의 세부 정보를 알려 근본 원인을 파악하는 데 도움을 줄 수 있습니다. VM 대시보드에서는 VM의 성능 통계를 볼 수 있으므로 VMware vSphere 호스트에서 네트워크를 거쳐 마지막으로 스토리지까지 전체 입출력 경로를 조사할 수 있습니다. 일부 이벤트는 문제를 해결하기 위해 취할 수 있는 개선 조치도 제공합니다. 문제가 발생할 때 e-메일 및 SNMP 트랩을 통해 알림을 받도록 이벤트에 대한 사용자 지정 알림을 구성할 수 있습니다. Active IQ Unified Manager를 사용하면 용량 및 사용 추세를 예측하여 문제가 발생하기 전에 능동적으로 조치를 취함으로써 장기적인 문제를 해결할 수 있는 단기적인 의사 결정을 방지할 수 있으므로 사용자의 스토리지 요구 사항을 계획할 수 있습니다.

Cisco Intersight를 참조하십시오

Cisco Intersight는 기존 및 클라우드 네이티브 애플리케이션과 인프라에 대한 지능형 자동화, 관찰 가능성 및 최적화를 제공하는 SaaS 플랫폼입니다. 이 플랫폼은 IT 팀의 변화를 이끌어내는 데 도움이 되며 하이브리드 클라우드용으로 설계된 운영 모델을 제공합니다.

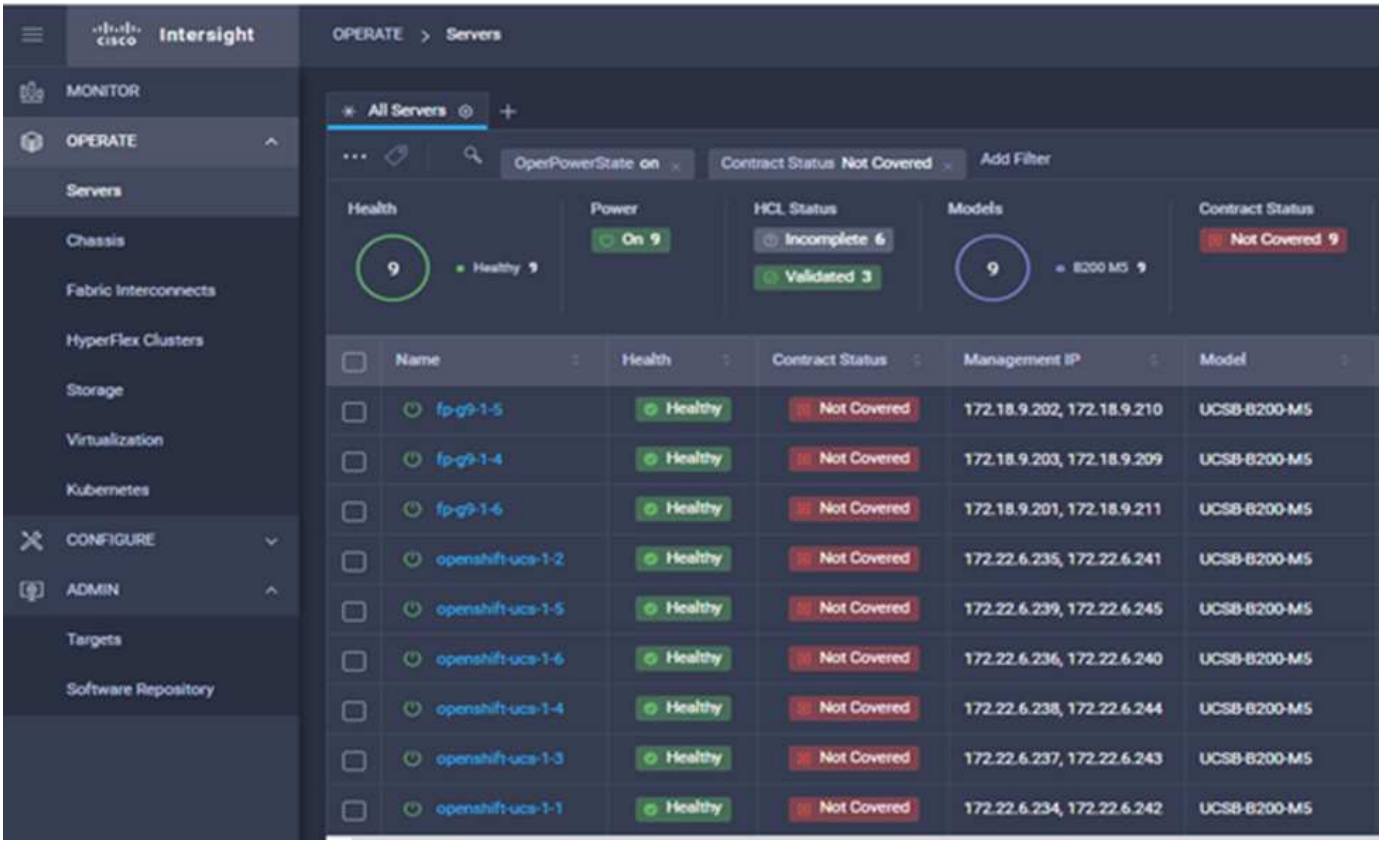
Cisco Intersight는 다음과 같은 이점을 제공합니다.

- 신속한 제공.* 민첩한 기반 소프트웨어 개발 모델로 인해 잦은 업데이트와 지속적인 혁신을 통해 클라우드 또는 고객의 데이터 센터에서 서비스로 제공됩니다. 따라서 고객은 LOB에 대한 제공 속도를 높이는 데 주력할 수 있습니다.
- * 운영 간소화. * 공통의 인벤토리, 인증 및 API가 포함된 안전한 단일 툴을 사용하여 운영을 간소화함으로써 전체 스택 및 모든 위치에서 작업을 수행할 수 있으므로 팀 간의 사일로를 제거할 수 있습니다. 사내 물리적 서버 및 하이퍼바이저 관리부터 VM, K8s, 서버리스, 자동화, 사내 및 퍼블릭 클라우드 전반에서 최적화 및 비용 제어
- * 지속적인 최적화. * Cisco Intersight가 모든 계층 및 Cisco TAC에 제공하는 인텔리전스를 사용하여 환경을 지속적으로 최적화합니다. 이 인텔리전스는 권장 및 자동화 작업으로 변환되므로 워크로드 이동, 물리적 서버 상태

모니터링, K8s 클러스터 자동 크기 조정, 작업 중인 퍼블릭 클라우드 비용 절감 권장 사항 등 모든 변화에 실시간으로 대응할 수 있습니다.

Cisco Intersight를 사용하면 UCSM 관리 모드(UMM)와 Intersight 관리 모드(IMM)의 두 가지 관리 작업 모드를 사용할 수 있습니다. 패브릭 상호 연결의 초기 설정 중에 패브릭 연결 Cisco UCS 시스템에 대한 네이티브 UMM 또는 IMM을 선택할 수 있습니다. 이 솔루션에서는 네이티브 UMM이 사용됩니다.

다음 이미지는 Cisco Intersight 대시보드를 보여 줍니다.

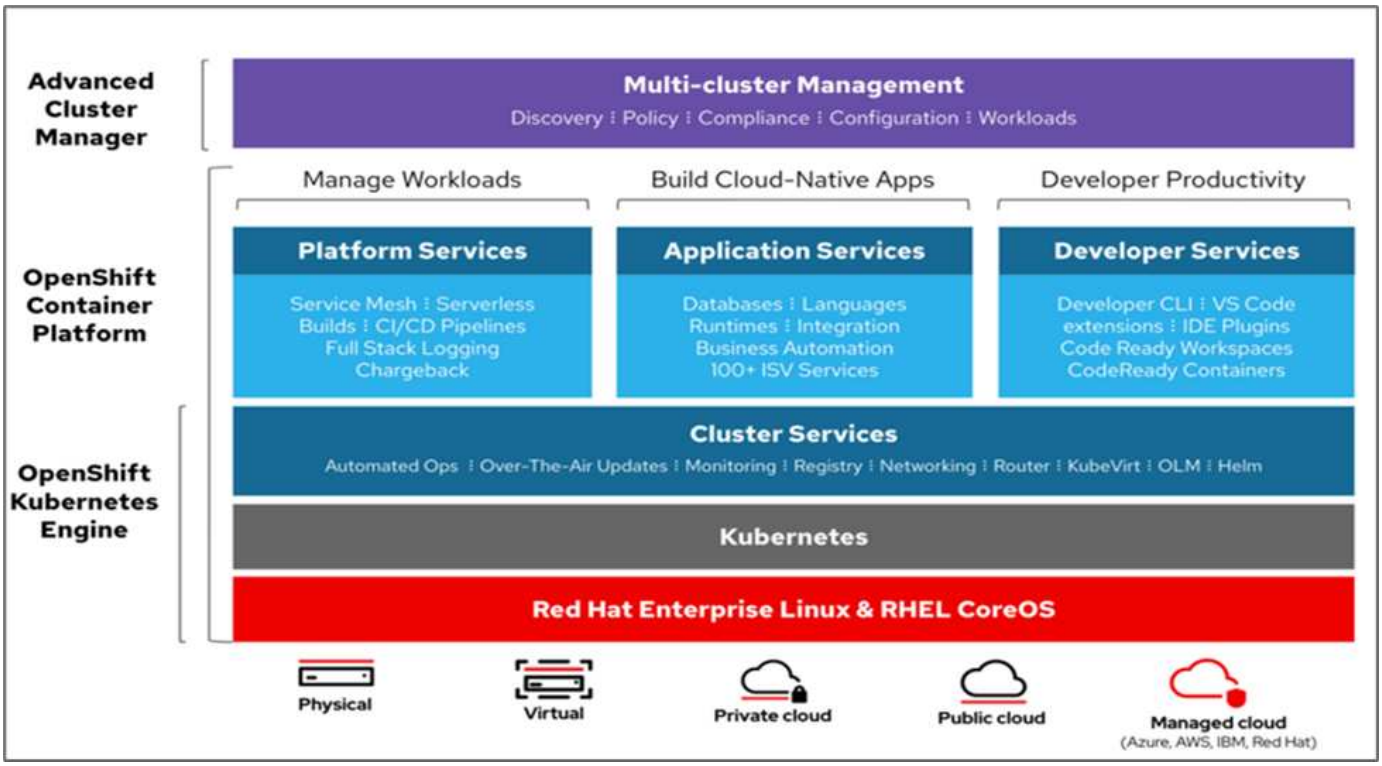


Red Hat OpenShift Container Platform

Red Hat OpenShift Container Platform은 컨테이너 애플리케이션 플랫폼으로, CRI-O와 Kubernetes를 통합하고 API 및 웹 인터페이스를 제공하여 이러한 서비스를 관리합니다. CRI-O는 Kubernetes 컨테이너 런타임 인터페이스(CRI)를 구현하여 OCI(Open Container Initiative) 호환 런타임 사용을 지원합니다. Kubernetes의 런타임 동안 Docker를 사용하는 것이 아니라 경량입니다.

OpenShift Container Platform을 사용하면 컨테이너를 만들고 관리할 수 있습니다. 컨테이너는 운영체제 및 기본 인프라와 관계없이 자체 환경에서 실행되는 독립 실행형 프로세스입니다. OpenShift Container Platform은 컨테이너 기반 애플리케이션을 개발, 배포 및 관리하는 데 도움이 됩니다. 또한 필요에 따라 애플리케이션을 생성, 수정 및 배포할 수 있는 셀프 서비스 플랫폼을 제공하므로 개발 및 릴리스 라이프사이클 단축이 가능합니다. OpenShift Container Platform은 마이크로서비스 기반의 작은 분리된 유닛으로, 서로 연동되는 아키텍처를 제공합니다. 이 제품은 Kubernetes 클러스터 위에서 실행되며, 안정적인 클러스터 키-가치 저장소인 etcd에 저장된 오브젝트 관련 데이터가 함께 사용됩니다.

다음 이미지는 Red Hat OpenShift Container 플랫폼의 개요입니다.



Kubernetes 인프라

OpenShift Container Platform에서 Kubernetes는 CRI-O 런타임 호스트 세트 전반에서 컨테이너식 애플리케이션을 관리하고 구축, 유지 관리, 애플리케이션 확장을 위한 메커니즘을 제공합니다. CRI-O 서비스 패키지는 컨테이너화된 애플리케이션을 인스턴스화하고 실행합니다.

Kubernetes 클러스터는 하나 이상의 마스터와 작업자 노드 집합으로 구성됩니다. 이 솔루션 설계에는 하드웨어 및 소프트웨어 스택의 고가용성(HA) 기능이 포함되어 있습니다. Kubernetes 클러스터는 3개의 마스터 노드와 2개 이상의 작업자 노드로 HA 모드에서 실행되도록 설계되어 있어 클러스터의 단일 장애 지점이 없도록 합니다.

Red Hat Core OS

OpenShift Container Platform은 CoreOS 및 Red Hat Atomic Host 운영 체제의 일부 최상의 기능을 결합한 컨테이너 중심의 운영 체제인 Red Hat Enterprise Linux CoreOS(RHCOS)를 사용합니다. RHCOS는 OpenShift Container Platform에서 컨테이너화된 애플리케이션을 실행하도록 특별히 설계되었으며, 새로운 툴과 함께 작동하여 빠른 설치, 운영자 기반 관리 및 간편한 업그레이드를 제공합니다.

RHCOS에는 다음과 같은 기능이 포함되어 있습니다.

- 점화 - OpenShift Container Platform이 처음 시스템을 가져와서 구성할 때 첫 번째 부팅 시스템 구성으로 사용하는 점화 시스템입니다.
- 운영 체제와 긴밀하게 통합된 Kubernetes 네이티브 컨테이너 런타임 구현인 CRI-O를 통해 효율적이고 최적화된 Kubernetes 경험을 제공할 수 있습니다. CRI-O는 컨테이너를 실행, 중지 및 재시작할 수 있는 기능을 제공합니다. OpenShift Container Platform 3에서 사용된 Docker 컨테이너 엔진을 완전히 대체합니다.
- Kubernetes의 기본 노드 에이전트인 Kubelet는 컨테이너 시작 및 모니터링을 담당합니다.

VMware vSphere 7.0

VMware vSphere는 CPU, 스토리지 및 네트워킹을 포함한 대규모 인프라 컬렉션을 완벽하고 다재다능한 동적 운영 환경으로 전체적으로 관리하는 가상화 플랫폼입니다. 개별 시스템을 관리하는 기존 운영 체제와 달리 VMware

vSphere는 전체 데이터 센터의 인프라를 통합하여 필요한 애플리케이션에 빠르고 동적으로 할당할 수 있는 리소스를 갖춘 강력한 단일 시스템을 구축합니다.

자세한 내용은 을 참조하십시오 "VMware vSphere를 참조하십시오".

VMware vSphere vCenter를 참조하십시오

VMware vCenter Server는 단일 콘솔에서 모든 호스트와 VM을 통합 관리하고 클러스터, 호스트 및 VM의 성능 모니터링을 통합합니다. VMware vCenter Server를 통해 관리자는 컴퓨팅 클러스터, 호스트, VM, 스토리지, 게스트 OS, 가상 인프라스트럭처의 기타 주요 구성 요소 VMware vCenter는 VMware vSphere 환경에서 사용할 수 있는 다양한 기능을 관리합니다.

하드웨어 및 소프트웨어 개정

이 솔루션은 에 정의된 대로 지원되는 소프트웨어, 펌웨어 및 하드웨어 버전을 실행하는 FlexPod 환경으로 확장할 수 있습니다 "NetApp 상호 운용성 매트릭스 툴" 및 "Cisco UCS 하드웨어 호환성 목록" OpenShift 클러스터는 VMware vSphere뿐만 아니라 베어 메탈 방식으로 FlexPod에 설치됩니다.

여러 OpenShift(k8s) 클러스터를 관리하려면 Astra Control Center의 단일 인스턴스만 필요하고, 각 OpenShift 클러스터마다 Trident CSI가 설치됩니다. Astra Control Center는 이러한 OpenShift 클러스터에 설치할 수 있습니다. 이 솔루션에서 Astra Control Center는 OpenShift 베어 메탈 클러스터에 설치됩니다.

다음 표에는 OpenShift의 FlexPod 하드웨어 및 소프트웨어 개정 버전이 나와 있습니다.

구성 요소	제품	버전
컴퓨팅	Cisco UCS Fabric 인터커넥트 6454	4.1(3c)
	Cisco UCS B200 M5 서버	4.1(3c)
네트워크	Cisco Nexus 9336C-FX2 NX-OS	9.3(8)
스토리지	NetApp AFF A700	9.11.1
	NetApp Astra Control Center를 참조하십시오	22.04.0
	NetApp Astra Trident CSI 플러그인	22.04.0
	NetApp Active IQ Unified Manager를 참조하십시오	9.11
소프트웨어	VMware ESXi nenic 이더넷 드라이버	1.0.35.0
	vSphere ESXi	7.0(U2)
	VMware vCenter 어플라이언스	7.0 U2b
	Cisco Intersight Assist 가상 어플라이언스	1.0.9-342
	OpenShift 컨테이너 플랫폼	4.9
	OpenShift Container Platform 마스터 노드	RHCOS 4.9
	OpenShift 컨테이너 플랫폼 작업자 노드	RHCOS 4.9

다음 표에는 AWS의 OpenShift용 소프트웨어 버전이 나와 있습니다.

구성 요소	제품	버전
컴퓨팅	마스터 인스턴스 유형: M5.xLarge	해당 없음
	작업자 인스턴스 유형: M5.Large	해당 없음
네트워크	가상 프라이빗 클라우드 전송 게이트웨이	해당 없음
스토리지	NetApp Cloud Volumes ONTAP를 참조하십시오	9.11.1
	NetApp Astra Trident CSI 플러그인	22.04.0
소프트웨어	OpenShift 컨테이너 플랫폼	4.9
	OpenShift Container Platform 마스터 노드	RHCOS 4.9
	OpenShift 컨테이너 플랫폼 작업자 노드	RHCOS 4.9

"다음: OpenShift Container Platform 4 베어메탈 설치용 FlexPod"

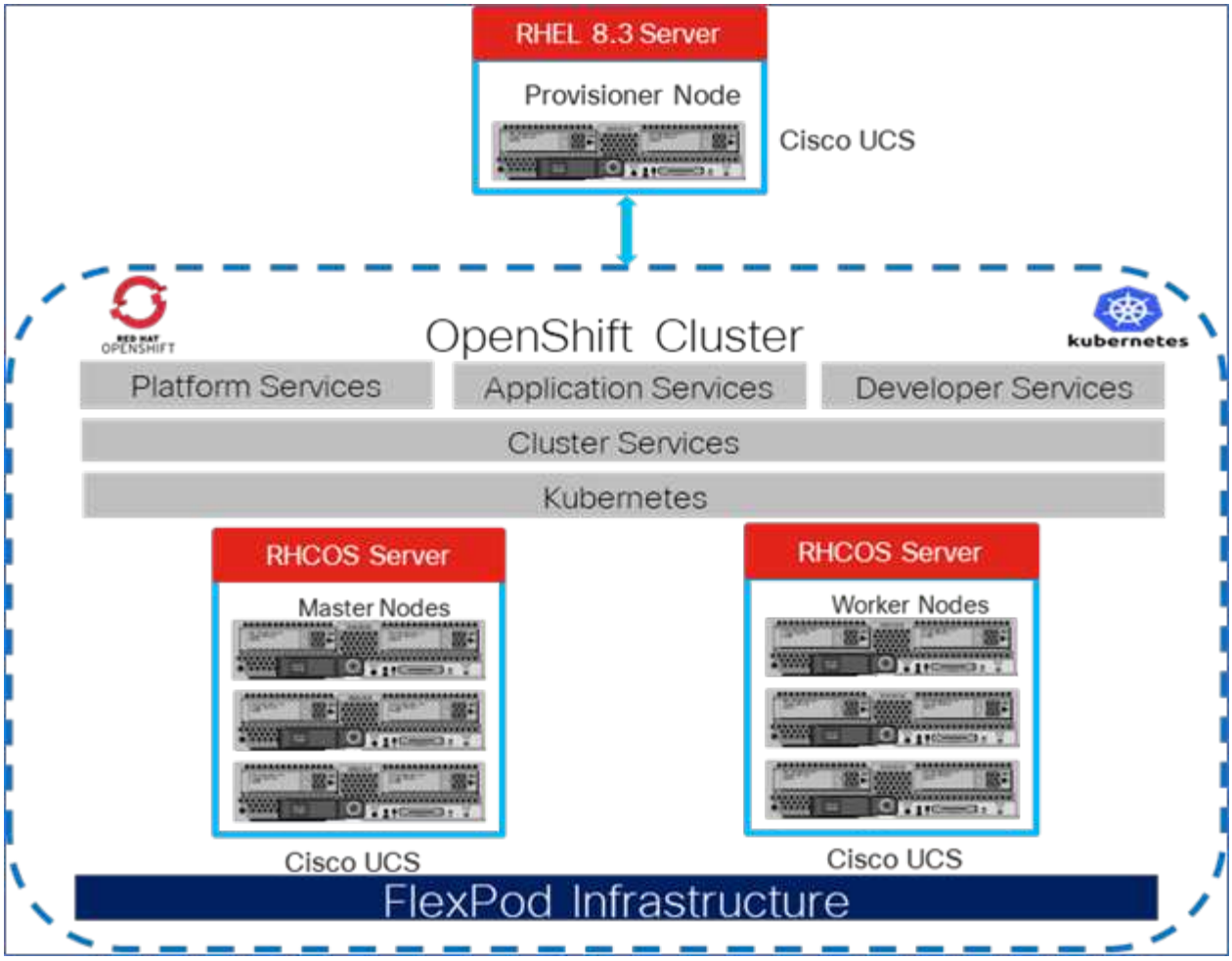
설치 및 구성

OpenShift Container Platform 4용 **FlexPod** 베어 메탈 설치

"이전: 솔루션 구성 요소."

OpenShift Container Platform 4 베어메탈 설계, 구축 세부 정보, NetApp Astra Trident 설치 및 구성을 위한 FlexPod를 알아보려면 를 참조하십시오 "FlexPod 및 OpenShift CVD(Cisco Validated Design and Deployment Guide)". 이 CVD에서는 Ansible을 사용한 FlexPod 및 OpenShift 컨테이너 플랫폼 구축에 대해 설명합니다. 또한 CVD는 Astra Control Center를 구축 및 구성하기 위한 몇 가지 사전 요구 사항에 따라 작업자 노드, Astra Trident 설치, 스토리지 백엔드 및 스토리지 클래스 구성을 준비하는 방법에 대한 자세한 정보를 제공합니다.

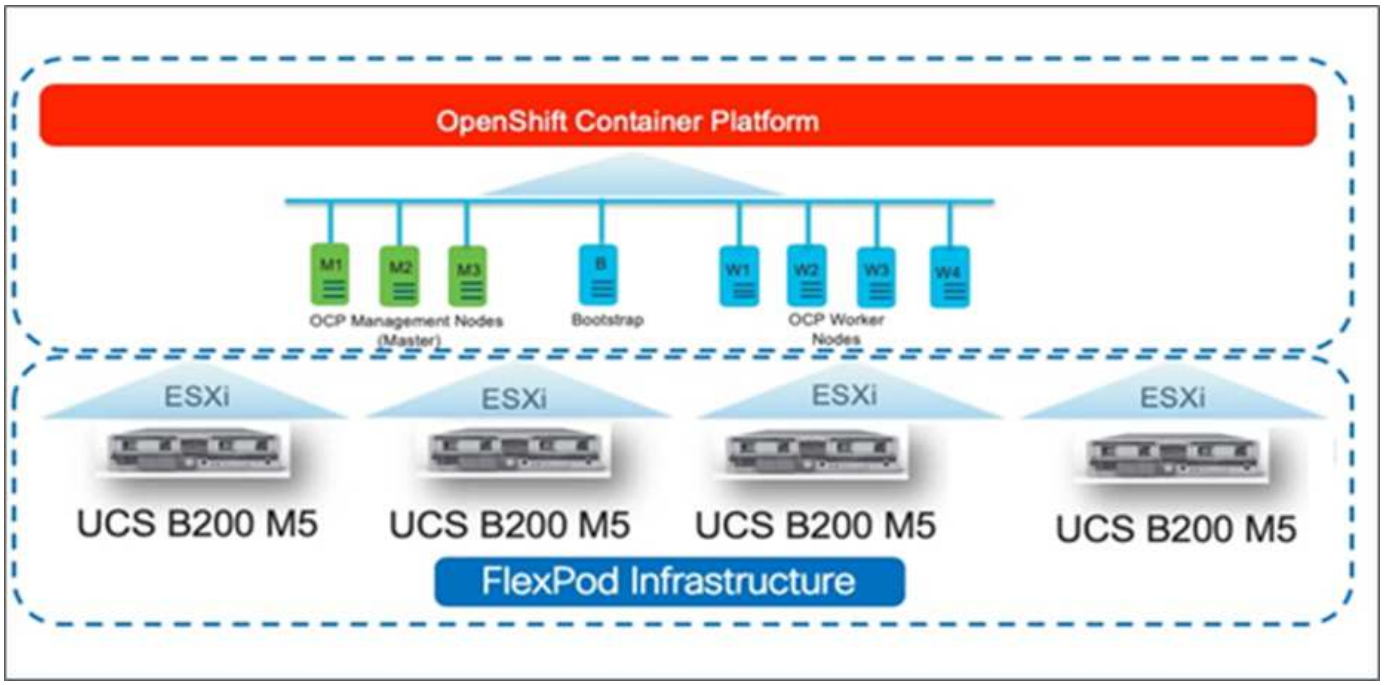
다음 그림은 FlexPod의 OpenShift 컨테이너 플랫폼 4 베어 메탈 을 보여 줍니다.



VMware 설치 기반 **OpenShift Container Platform 4**용 **FlexPod**

VMware vSphere를 실행하는 FlexPod에서 Red Hat OpenShift Container Platform 4 배포에 대한 자세한 내용은 을 참조하십시오 "OpenShift 컨테이너 플랫폼용 FlexPod 데이터 센터 4".

다음 그림에서는 vSphere 기반의 OpenShift Container Platform 4용 FlexPod를 보여 줍니다.

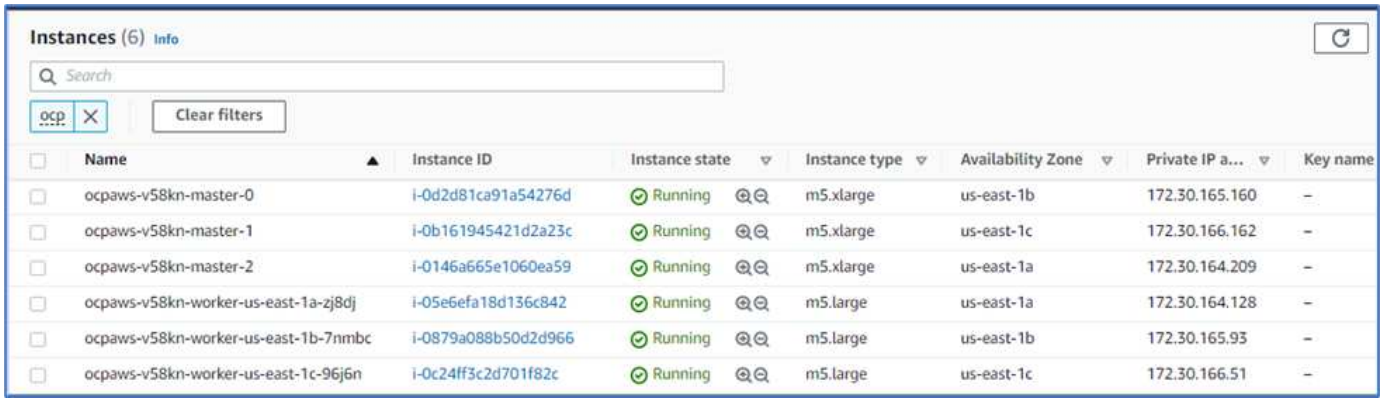


"다음으로, AWS의 Red Hat OpenShift입니다."

AWS 기반 **Red Hat OpenShift**

"이전: OpenShift Container Platform 4 베어메탈 설치용 FlexPod"

DR 사이트로 AWS에 별도의 자가 관리 OpenShift Container Platform 4 클러스터가 구축됩니다. 마스터 노드와 작업자 노드는 고가용성을 위해 세 개의 가용성 영역에 걸쳐 있습니다.



```
[ec2-user@ip-172-30-164-92 ~]$ oc get nodes
NAME                                STATUS   ROLES    AGE   VERSION
ip-172-30-164-128.ec2.internal   Ready    worker   29m   v1.22.8+f34b40c
ip-172-30-164-209.ec2.internal   Ready    master   36m   v1.22.8+f34b40c
ip-172-30-165-160.ec2.internal   Ready    master   33m   v1.22.8+f34b40c
ip-172-30-165-93.ec2.internal    Ready    worker   30m   v1.22.8+f34b40c
ip-172-30-166-162.ec2.internal   Ready    master   36m   v1.22.8+f34b40c
ip-172-30-166-51.ec2.internal    Ready    worker   28m   v1.22.8+f34b40c
```

OpenShift는 로 배포됩니다 "프라이빗 클러스터" AWS 기반 기존 VPC에. 사설 OpenShift Container Platform 클러스터는 외부 엔드포인트를 노출하지 않으며 내부 네트워크에서만 액세스할 수 있고 인터넷에서는 볼 수 없습니다. NetApp Cloud Manager를 사용하여 단일 노드 NetApp Cloud Volumes ONTAP를 구축하고 Astra Trident에 스토리지 백엔드를 제공합니다.

AWS에 OpenShift를 설치하는 방법에 대한 자세한 내용은 를 참조하십시오 "OpenShift 문서".

"다음은 NetApp Cloud Volumes ONTAP의 차례입니다."

NetApp Cloud Volumes ONTAP를 참조하십시오

"이전: AWS의 Red Hat OpenShift"

NetApp Cloud Volumes ONTAP 인스턴스는 AWS에 구축되며 Astra Trident에 백엔드 스토리지 역할을 합니다. Cloud Volumes ONTAP 작업 환경을 추가하기 전에 커넥터를 구축해야 합니다. 커넥터가 없는 상태에서 첫 번째 Cloud Volumes ONTAP 작업 환경을 생성하려고 하면 Cloud Manager에서 메시지가 표시됩니다. AWS에 Connector를 구축하려면 를 참조하십시오 "커넥터를 작성합니다".

AWS에 Cloud Volumes ONTAP를 구축하려면 를 참조하십시오 "AWS 환경을 위한 빠른 시작".

Cloud Volumes ONTAP를 구축한 후 Astra Trident를 설치하고 OpenShift Container Platform 클러스터에서 스토리지 백엔드 및 스냅샷 클래스를 구성할 수 있습니다.

"다음: OpenShift Container Platform에 Astra Control Center를 설치합니다."

OpenShift Container Platform에 **Astra Control Center** 설치

"이전: NetApp Cloud Volumes ONTAP."

FlexPod에서 실행되는 OpenShift 클러스터나 Cloud Volumes ONTAP 스토리지 백엔드가 있는 AWS에 Astra Control Center를 설치할 수 있습니다. 이 솔루션에서 Astra Control Center는 OpenShift 베어 메탈 클러스터에 구축됩니다.

Astra Control Center는 설명된 표준 프로세스를 사용하여 설치할 수 있습니다 "여기" 또는 Red Hat OpenShift OperatorHub를 참조하십시오. Astra Control Operator는 Red Hat 공인 운영자입니다. 이 솔루션에서는 Red Hat OperatorHub를 사용하여 Astra Control Center를 설치합니다.

- Astra Control Center는 여러 Kubernetes 배포를 지원합니다. Red Hat OpenShift의 경우 지원되는 버전에 Red Hat OpenShift Container Platform 4.8 또는 4.9가 포함됩니다.
- Astra Control Center에는 환경 및 최종 사용자의 애플리케이션 리소스 요구 사항 외에 다음과 같은 리소스가 필요합니다.

구성 요소	요구 사항
스토리지 백엔드 용량입니다	최소 500GB가 제공됩니다
작업자 노드	최소 3개의 작업자 노드, 각각 4개의 CPU 코어, 12GB RAM
FQDN(정규화된 도메인 이름) 주소입니다	Astra Control Center의 FQDN 주소입니다
아스트라 트리덴트	Astra Trident 21.04 이상 설치 및 구성
수신 컨트롤러 또는 로드 밸런서	FQDN으로 확인할 IP 주소를 제공하도록 수신 컨트롤러를 URL 또는 로드 밸런서와 함께 Astra Control Center를 노출하도록 구성합니다

- Astra Control Center 빌드 이미지를 푸시할 수 있는 기존 개인 이미지 레지스트리가 있어야 합니다. 이미지를 업로드하는 이미지 레지스트리의 URL을 제공해야 합니다.

> 일부 이미지는 특정 워크플로우를 실행하는 동안 가져오며, 필요에 따라 컨테이너가 생성되고 제거됩니다.

- Astra Control Center에서는 스토리지 클래스를 생성하고 기본 스토리지 클래스로 설정해야 합니다. Astra Control Center는 Astra Trident에서 제공하는 다음과 같은 ONTAP 드라이버를 지원합니다.
  - ONTAP - NAS
  - ONTAP-NAS-Flexgroup입니다
  - ONTAP-SAN
  - ONTAP-SAN - 경제성

> 배포된 OpenShift 클러스터에 ONTAP 백엔드로 설치 및 구성된 Astra Trident가 있으며 기본 스토리지 클래스도 정의되어 있다고 가정합니다.

- OpenShift 환경에서 애플리케이션을 복제하려면 OpenShift가 볼륨을 마운트하고 파일 소유권을 변경할 수 있도록 Astra Control Center를 허용해야 합니다. 이러한 작업을 허용하도록 ONTAP 엑스포트 정책을 수정하려면 다음 명령을 실행합니다.

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

두 번째 OpenShift 운영 환경을 관리되는 컴퓨팅 리소스로 추가하려면 Astra Trident 볼륨 스냅샷 기능이 활성화되어 있는지 확인합니다. Astra Trident를 사용하여 볼륨 스냅샷을 활성화하고 테스트하려면 공식 을 참조하십시오 "Astra Trident 지침".

- A "VolumeSnapClass" 애플리케이션이 관리되는 모든 Kubernetes 클러스터에서 구성되어야 합니다. 여기에는 Astra Control Center가 설치된 K8s 클러스터도 포함될 수 있습니다. Astra Control Center는 실행 중인 K8s 클러스터에서 애플리케이션을 관리할 수 있습니다.

설명합니다

- * 라이센스. * Astra Control Center를 사용하여 애플리케이션을 관리하려면 Astra Control Center 라이센스가 필요합니다.
- * Namespaces. * 네임스페이스는 Astra Control Center에서 응용 프로그램으로 관리할 수 있는 가장 큰 엔터티입니다. 기존 네임스페이스에서 응용 프로그램 레이블 및 사용자 지정 레이블을 기준으로 구성 요소를 필터링하고 리소스의 하위 집합을 응용 프로그램으로 관리하도록 선택할 수 있습니다.
- * StorageClass. * StorageClass가 명시적으로 설정된 응용 프로그램을 설치하고 응용 프로그램을 복제해야 하는 경우 클론 작업의 타겟 클러스터에 원래 지정된 StorageClass가 있어야 합니다. 명시적으로 StorageClass를 동일한 StorageClass가 없는 클러스터로 설정한 응용 프로그램을 클론 복제하지 못합니다.
- Kubernetes 리소스 * Astra Control에서 캡처하지 않은 Kubernetes 리소스를 사용하는 애플리케이션에는 전체 애플리케이션 데이터 관리 기능이 없을 수 있습니다. Astra Control은 다음과 같은 Kubernetes 리소스를 캡처할 수 있습니다.

Kubernetes 리소스		
클러스터 역할	ClusterRoleBinding 을 참조하십시오	ConfigMap을 클릭합니다
사용자 지정 리소스 정의	CustomResource 를 선택합니다	경작업
DemonSet	HorizontalPodAutoscaler	침투
DeploymentConfig(배포 구성	뮤atingWebhook	PersistentVolumeClaim
포드	팟캐스트 예산	팟캐스트 템플릿
네트워크 정책	ReplicaSet입니다	역할
RoleBinding 을 클릭합니다	루트	비밀
Webhook을 확인합니다		

OpenShift OperatorHub를 사용하여 **Astra Control Center**를 설치합니다

다음 절차에서는 Red Hat OperatorHub를 사용하여 Astra Control Center를 설치합니다. 이 솔루션에서 Astra Control Center는 FlexPod에서 실행되는 베어 메탈 OpenShift 클러스터에 설치됩니다.

1. 에서 Astra Control Center 번들('Astra-control-center-[version].tar.gz')을 다운로드합니다 "NetApp Support 사이트".
2. Astra Control Center 인증서 및 키용 .zip 파일을 에서 다운로드합니다 "NetApp Support 사이트".
3. 번들의 서명을 확인합니다.

```
openssl dgst -sha256 -verify astra-control-center[version].pub
-signature <astra-control-center[version].sig astra-control-
center[version].tar.gz
```

4. Astra 이미지를 추출합니다.

```
tar -vxzf astra-control-center-[version].tar.gz
```

5. Astra 디렉토리로 변경합니다.

```
cd astra-control-center-[version]
```

6. 이미지를 로컬 레지스트리에 추가합니다.

```
For Docker:
docker login [your_registry_path]OR
For Podman:
podman login [your_registry_path]
```

7. 적절한 스크립트를 사용하여 이미지를 로드하고, 이미지에 태그를 지정한 다음 로컬 레지스트리에 해당 이미지를 푸시합니다.

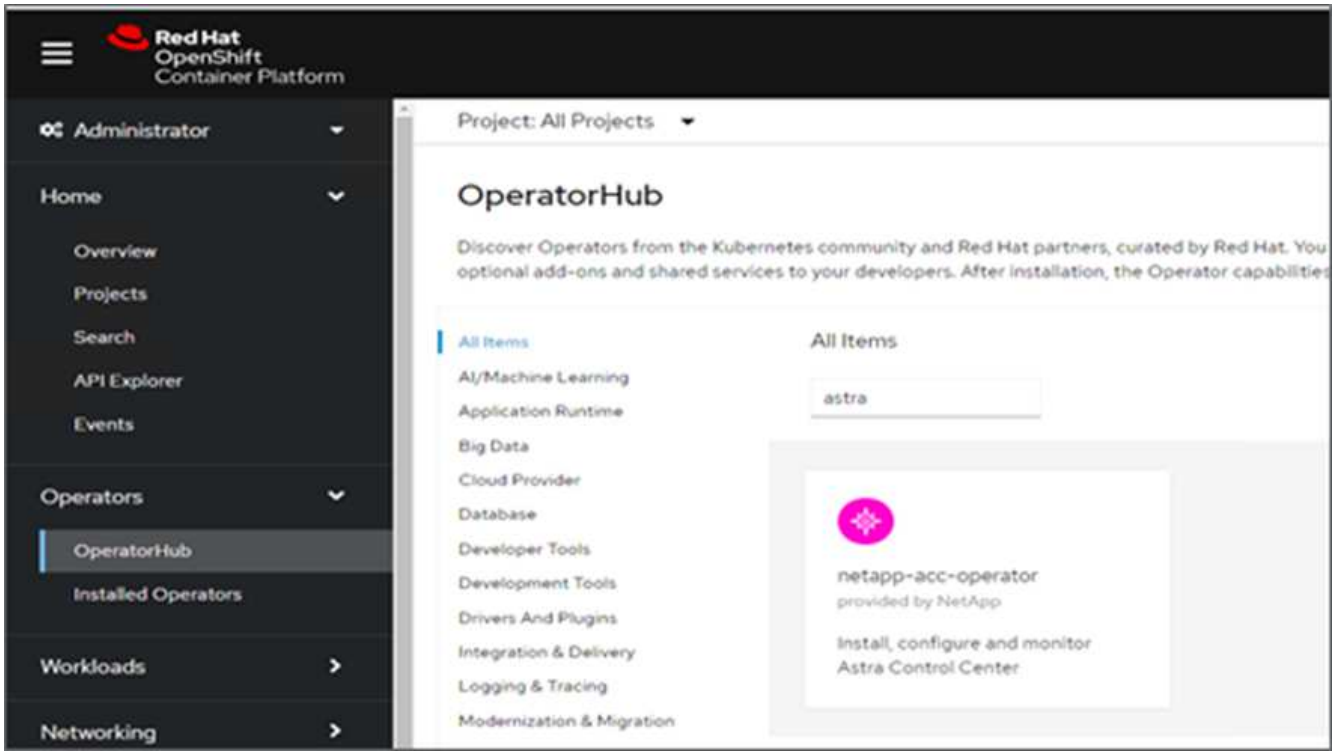
   Docker의 경우:

```
export REGISTRY=[Docker_registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded
image: //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done
```

   Podman의 경우:

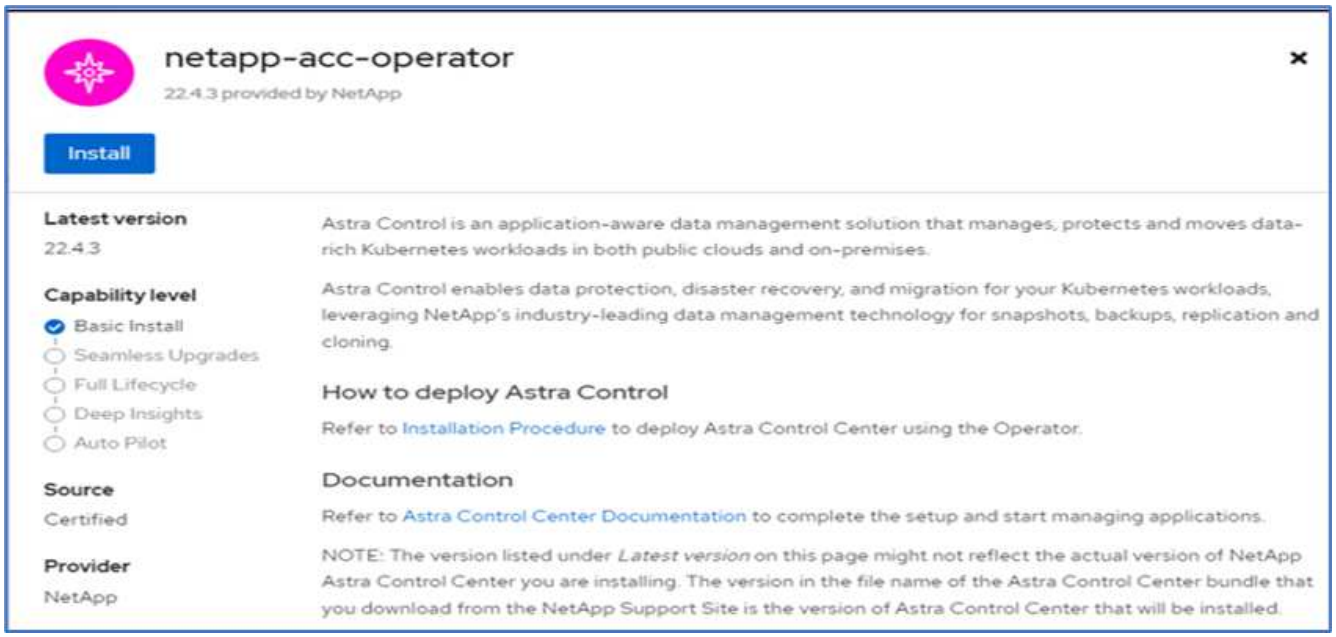
```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  podman push ${REGISTRY}/${astraImage}
done
```

8. 베어 메탈 OpenShift 클러스터 웹 콘솔에 로그인합니다. 측면 메뉴에서 Operators > OperatorHub 를 선택합니다. NetApp-acc-operator를 나열하려면 "Astra"를 입력합니다.

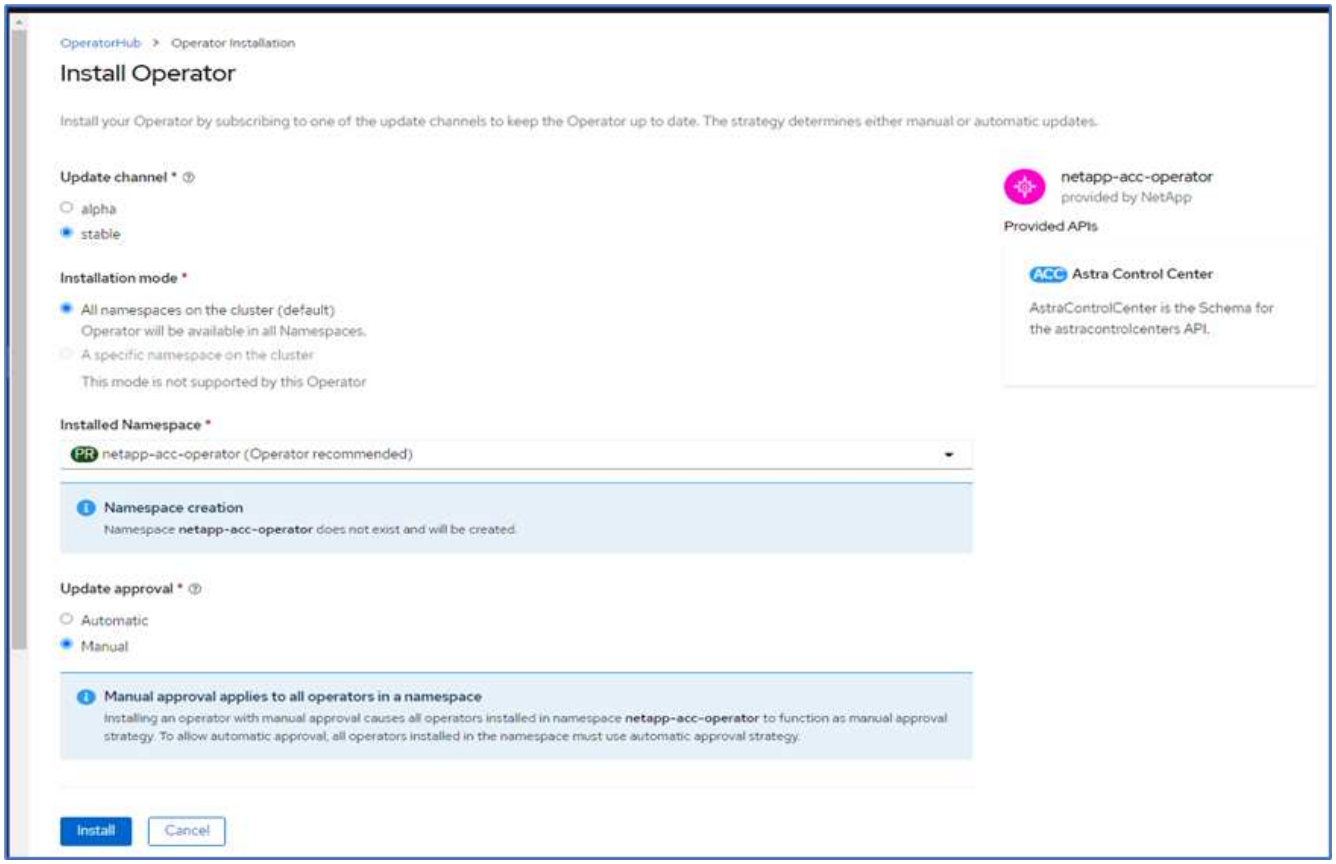


'NetApp-acc-operator'는 인증된 Red Hat OpenShift Operator로, OperatorHub 카탈로그 아래에 나열되어 있습니다.

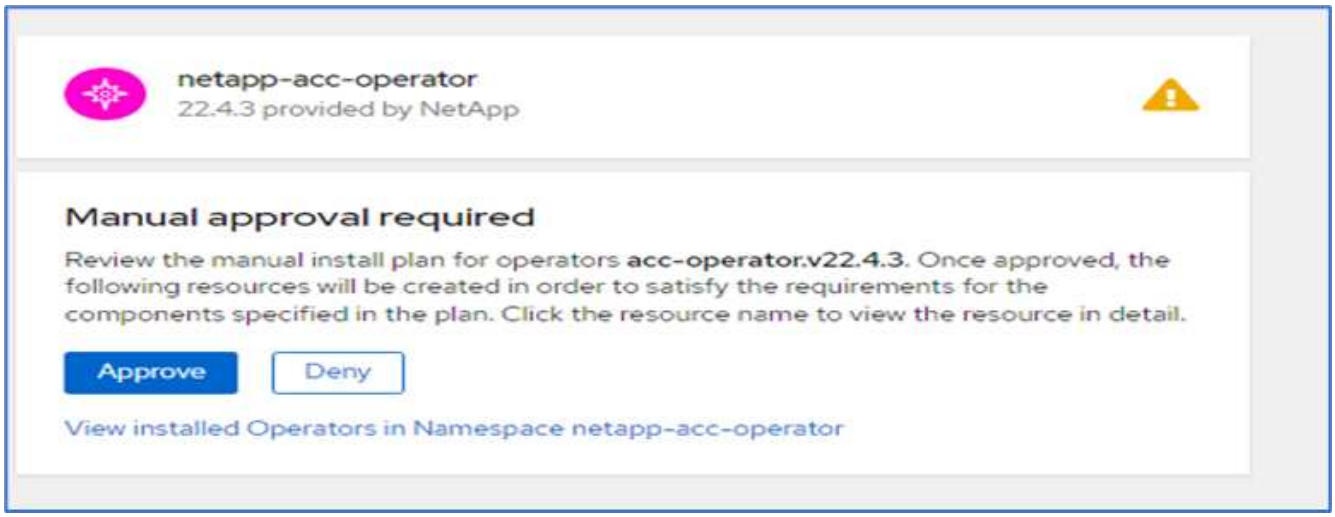
9. 'NetApp-acc-operator'를 선택하고 '설치'를 클릭합니다.



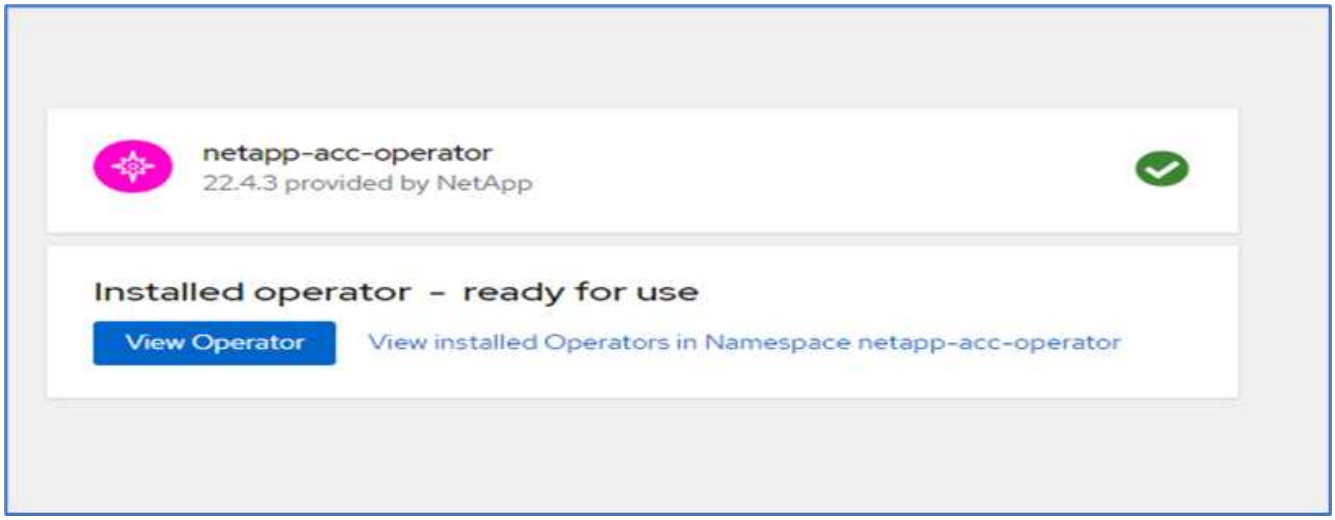
10. 적절한 옵션을 선택하고 설치 를 클릭합니다.



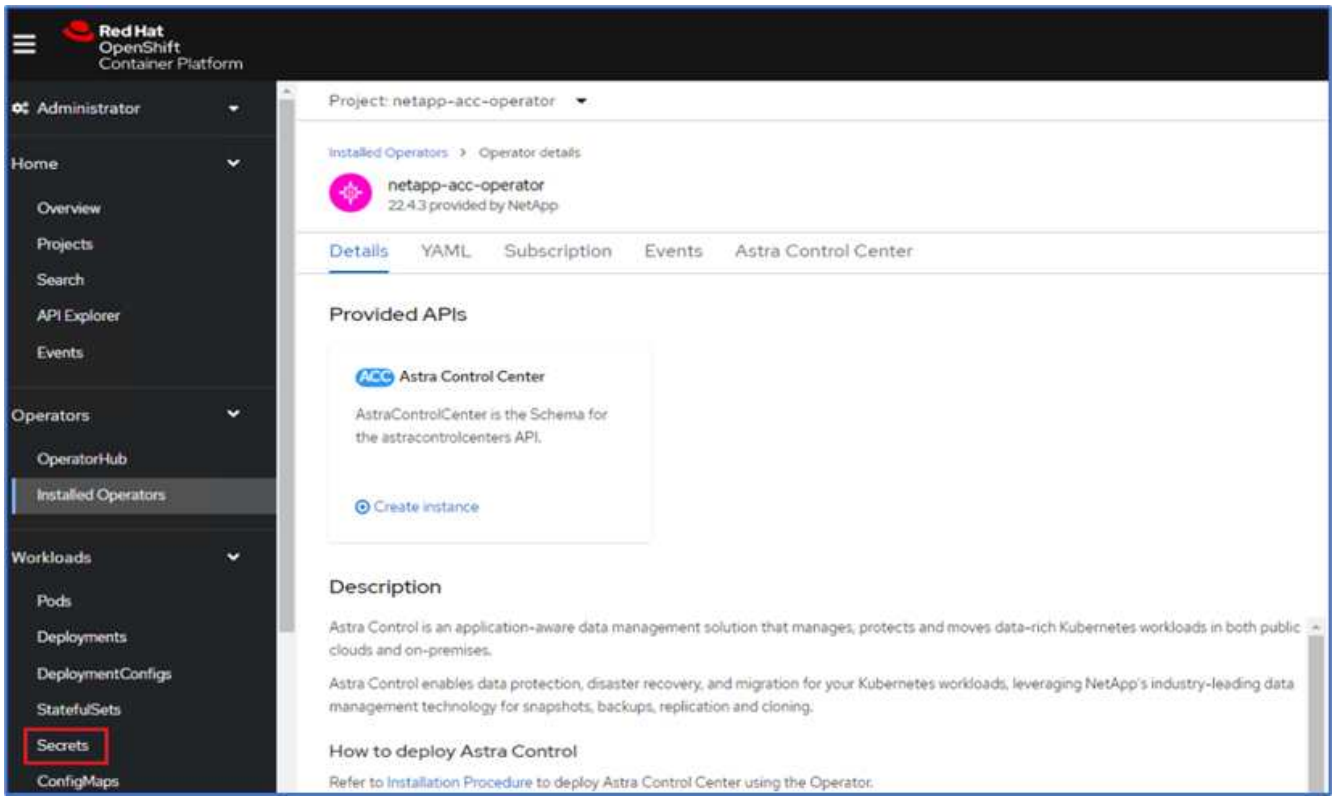
11. 설치를 승인하고 운영자가 설치될 때까지 기다립니다.



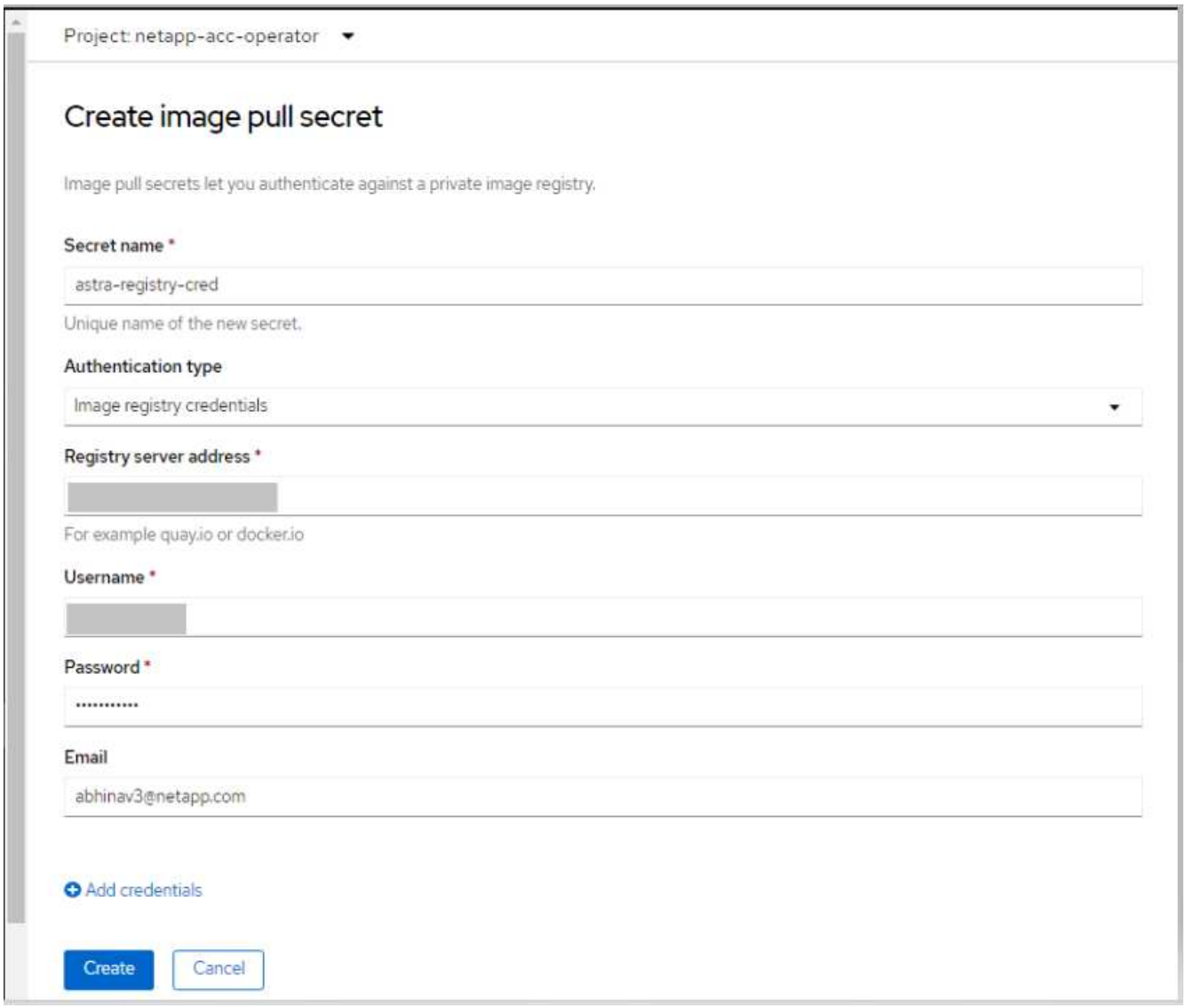
12. 이 단계에서 오퍼레이터는 성공적으로 설치되고 사용할 준비가 완료됩니다. View Operator(작업자 보기) 를 클릭하여 Astra Control Center 설치를 시작합니다.



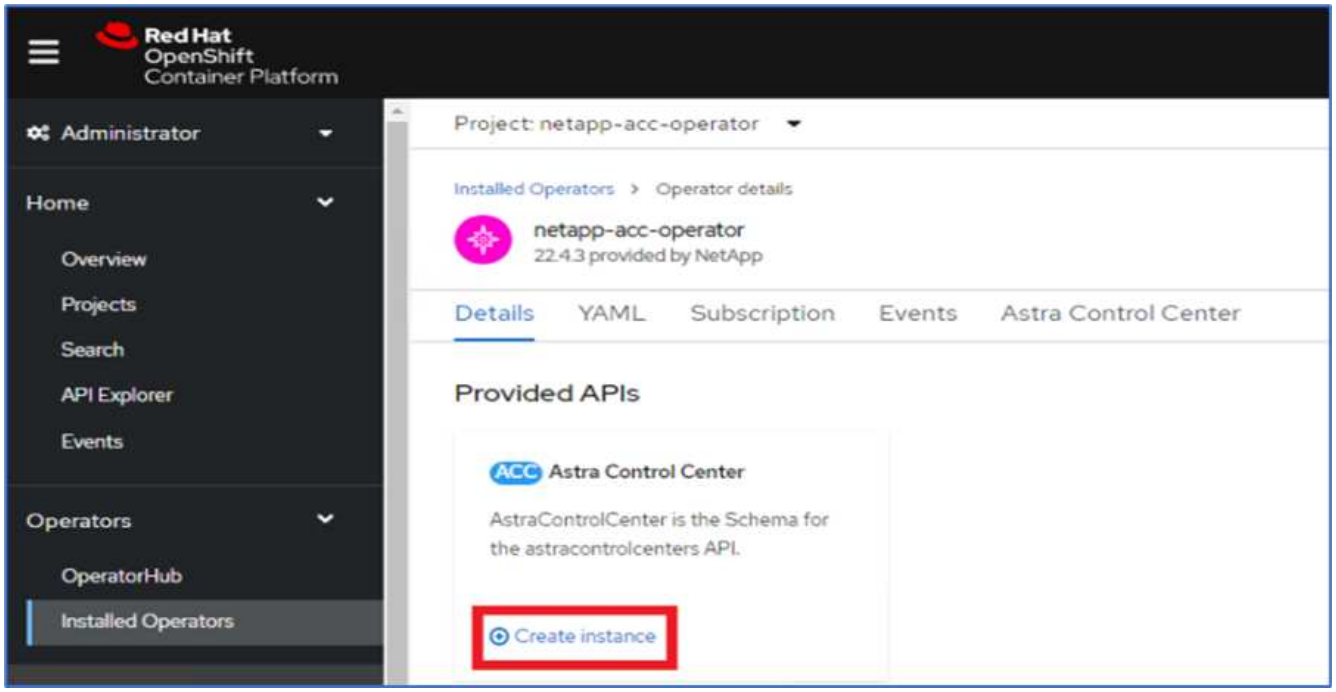
13. Astra Control Center를 설치하기 전에 앞서 푸시한 Docker 레지스트리에서 Astra 이미지를 다운로드하기 위한 풀 비밀을 생성합니다.



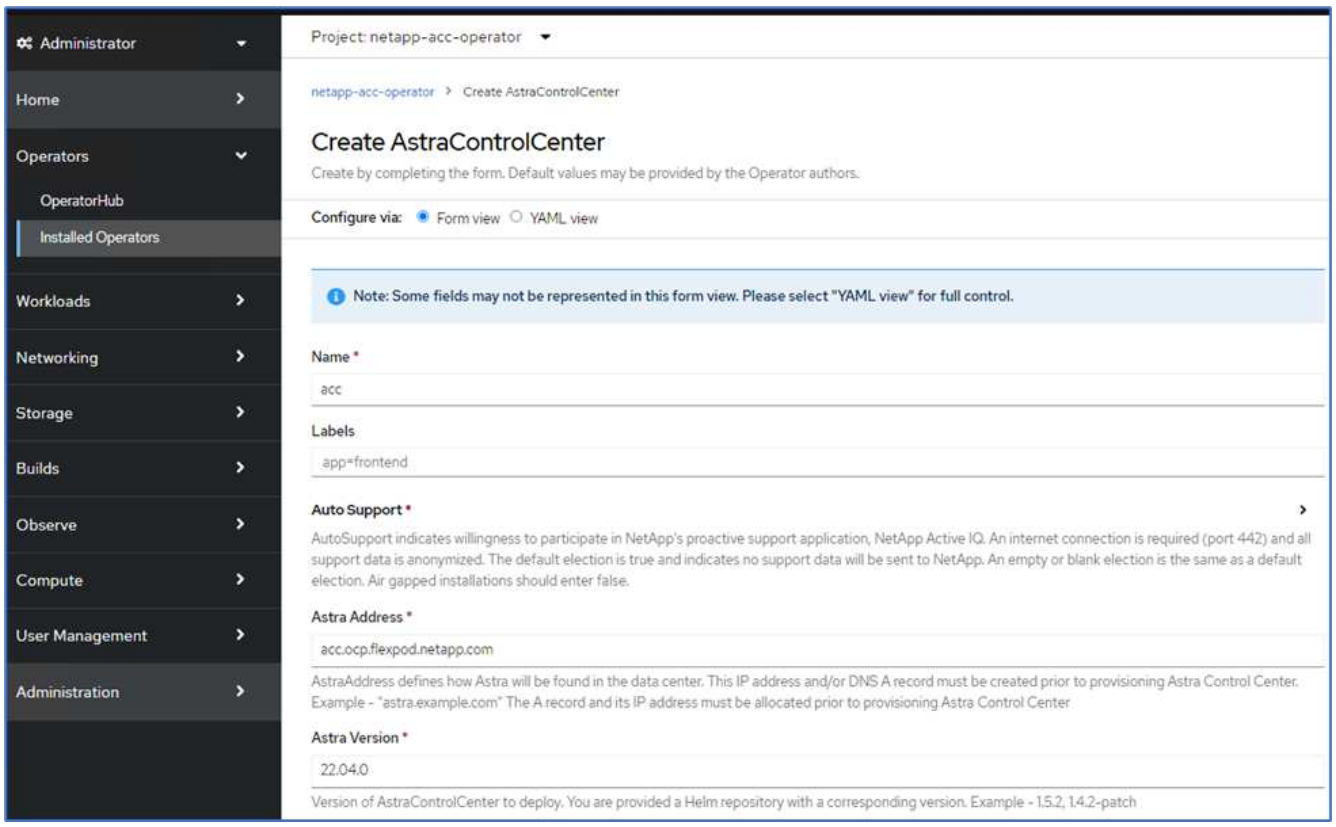
14. Docker 프라이빗 레포에서 Astra Control Center 이미지를 풀려면 'NetApp-acc-operator' 네임스페이스에서 암호를 생성하십시오. 이 비밀 이름은 나중에 Astra Control Center YAML manifest에서 제공합니다.



15. 측면 메뉴에서 Operators > Installed Operators 를 선택하고 제공된 API 섹션에서 Create instance 를 클릭합니다.



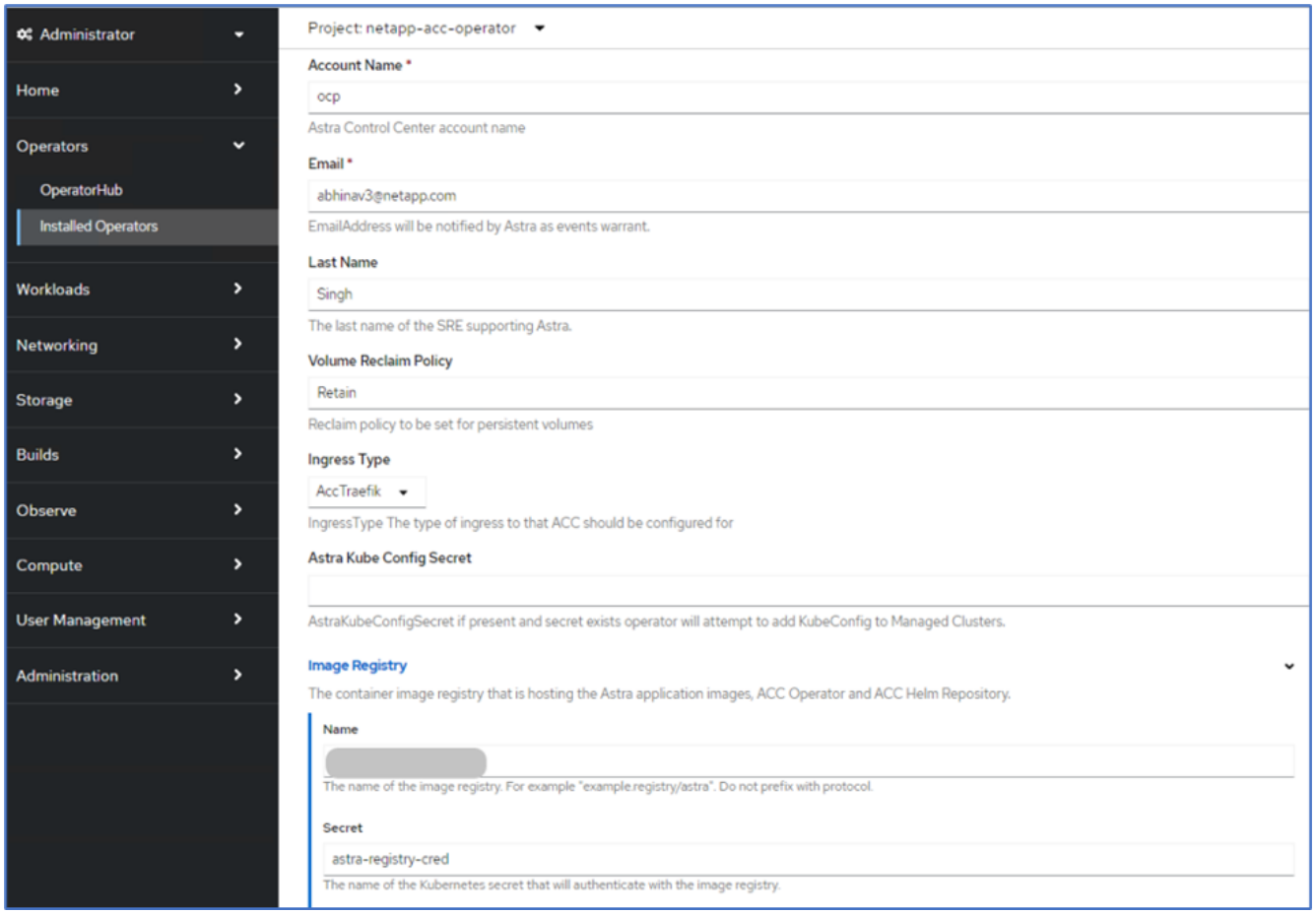
16. Create AstraControlCenter 양식을 완료합니다. 이름, Astra 주소 및 Astra 버전을 입력합니다.



Astra Address 아래에 Astra Control Center의 FQDN 주소를 입력합니다. 이 주소는 Astra Control Center 웹 콘솔에 액세스하는 데 사용됩니다. FQDN도 연결 가능한 IP 네트워크로 확인되어야 하며 DNS에서 구성해야 합니다.

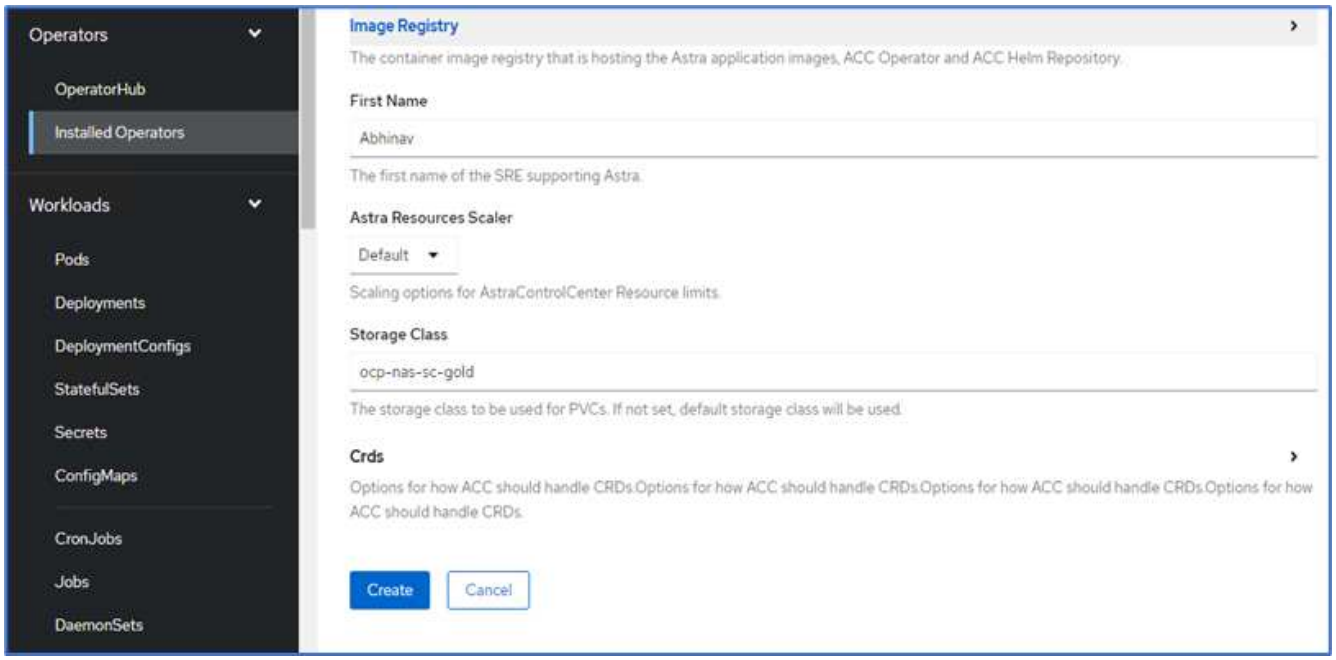
17. 계정 이름, 이메일 주소, 관리자 성을 입력하고 기본 볼륨 복원 정책을 유지합니다. 부하 분산 장치를 사용하는 경우 수신 유형을 "AccTraefik"로 설정합니다. 그렇지 않으면 Ingress.Controller로 Generic을 선택합니다. 이미지

레지스트리에서 컨테이너 이미지 레지스트리 경로 및 암호를 입력합니다.

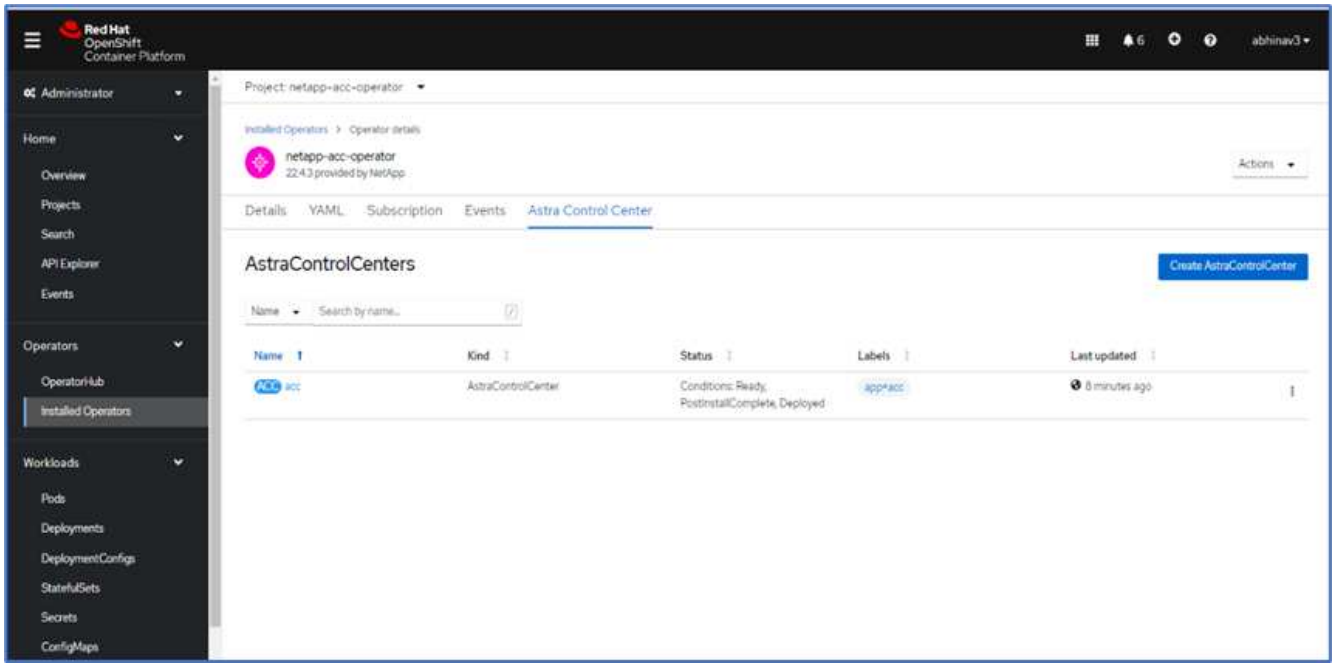


이 솔루션에서는 Metallb 로드 밸런서가 사용됩니다. 따라서 수신 유형은 AccTraefik입니다. 그러면 Astra Control Center traefik 게이트웨이가 워크로드 밸런서의 Kubernetes 서비스로 표시됩니다.

18. admin 이름을 입력하고, 리소스 확장을 구성하고, 스토리지 클래스를 제공합니다. 생성 을 클릭합니다.



Astra Control Center 인스턴스의 상태는 배포 에서 준비 로 변경해야 합니다.



19. 모든 시스템 구성 요소가 성공적으로 설치되어 있고 모든 Pod가 실행 중인지 확인합니다.

```
root@abhinav-ansible# oc get pods -n netapp-acc-operator
NAME                                               READY   STATUS
RESTARTS   AGE
acc-helm-repo-77745b49b5-7zg2v                     1/1     Running   0
10m
acc-operator-controller-manager-5c656c44c6-tqnmn   2/2     Running   0
13m
activity-589c6d59f4-x2sfs                          1/1     Running   0
6m4s
api-token-authentication-4q5lj                     1/1     Running   0
5m26s
api-token-authentication-pzptd                     1/1     Running   0
5m27s
api-token-authentication-tbtg6                     1/1     Running   0
5m27s
asup-669df8d49-qps54                               1/1     Running   0
5m26s
authentication-5867c5f56f-dnpp2                    1/1     Running   0
3m54s
bucketservice-85495bc475-5zcc5                     1/1     Running   0
5m55s
cert-manager-67f486bbc6-txhh6                      1/1     Running   0
9m5s
cert-manager-cainjector-75959db744-4l5p5           1/1     Running   0
9m6s
```

```
cert-manager-webhook-765556b869-g6wdf             1/1     Running   0
9m6s
cloud-extension-5d595f85f-txrfl                   1/1     Running   0
5m27s
cloud-insights-service-674649567b-5s4wd           1/1     Running   0
5m49s
composite-compute-6b58d48c69-46vhc                1/1     Running   0
6m11s
composite-volume-6d447fd959-chnrt                 1/1     Running   0
5m27s
credentials-66668f8ddd-8qc5b                      1/1     Running   0
7m20s
entitlement-fd6fc5c58-wxnmh                       1/1     Running   0
6m20s
features-756bbb7c7c-rgcrm                         1/1     Running   0
5m26s
fluent-bit-ds-278pg                               1/1     Running   0
3m35s
fluent-bit-ds-5pqc6                               1/1     Running   0
3m35s
fluent-bit-ds-8l7cq                               1/1     Running   0
3m35s
fluent-bit-ds-9qbft                               1/1     Running   0
3m35s
fluent-bit-ds-nj475                               1/1     Running   0
3m35s
fluent-bit-ds-x9pd8                               1/1     Running   0
3m35s
graphql-server-698d6f4bf-kftwc                    1/1     Running   0
3m20s
identity-5d4f4c87c9-wjz6c                         1/1     Running   0
6m27s
influxdb2-0                                       1/1     Running   0
9m33s
krakend-657d44bf54-8cb56                          1/1     Running   0
3m21s
license-594bbdc-rghdg                             1/1     Running   0
6m28s
login-ui-6c65fbbbd4-jg8wz                         1/1     Running   0
3m17s
loki-0                                            1/1     Running   0
9m30s
metrics-facade-75575f69d7-hnlk6                   1/1     Running   0
6m10s
monitoring-operator-65dff79cfb-z78vk              2/2     Running   0
3m47s
```

```
nats-0                                            1/1     Running   0
10m
nats-1                                            1/1     Running   0
9m43s
nats-2                                            1/1     Running   0
9m23s
nautilus-7bb469f857-4hlc6                         1/1     Running   0
6m3s
nautilus-7bb469f857-vz94m                         1/1     Running   0
4m42s
openapi-8586db4bcd-gwwvf                          1/1     Running   0
5m41s
packages-6bdb949cfb-nrq8l                         1/1     Running   0
6m35s
polaris-consul-consul-server-0                    1/1     Running   0
9m22s
polaris-consul-consul-server-1                    1/1     Running   0
9m22s
polaris-consul-consul-server-2                    1/1     Running   0
9m22s
polaris-mongodb-0                                 2/2     Running   0
9m22s
polaris-mongodb-1                                 2/2     Running   0
8m58s
polaris-mongodb-2                                 2/2     Running   0
8m34s
polaris-ui-5df7687dbd-trcnf                       1/1     Running   0
3m18s
polaris-vault-0                                   1/1     Running   0
9m18s
polaris-vault-1                                   1/1     Running   0
9m18s
polaris-vault-2                                   1/1     Running   0
9m18s
public-metrics-7b96476f64-j88bw                   1/1     Running   0
5m48s
storage-backend-metrics-5fd6d7cd9c-vcb4j          1/1     Running   0
5m59s
storage-provider-bb85ff965-m7qrq                  1/1     Running   0
5m25s
telegraf-ds-4zqgz                                 1/1     Running   0
3m36s
telegraf-ds-cp9x4                                 1/1     Running   0
3m36s
telegraf-ds-h4n59                                 1/1     Running   0
3m36s
```

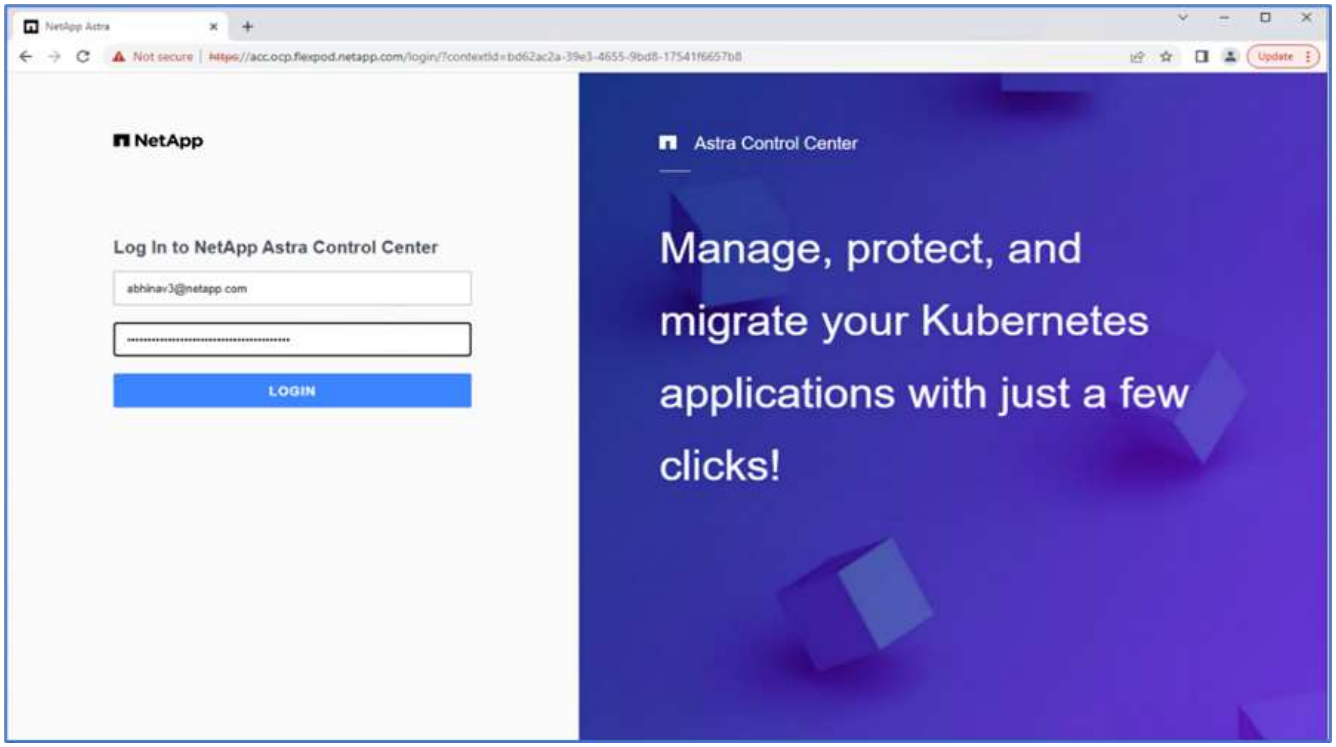
```
telegraf-ds-jnp2q                                 1/1     Running   0
3m36s
telegraf-ds-pdz5j                                 1/1     Running   0
3m36s
telegraf-ds-znqtp                                 1/1     Running   0
3m36s
telegraf-rs-rt64j                                 1/1     Running   0
3m36s
telemetry-service-7dd9c74bfc-sfkzt                1/1     Running   0
6m19s
tenancy-d878b7fb6-wf8x9                           1/1     Running   0
6m37s
traefik-6548496576-5v2g6                          1/1     Running   0
98s
traefik-6548496576-g82pq                          1/1     Running   0
3m8s
traefik-6548496576-psn49                          1/1     Running   0
38s
traefik-6548496576-qrkfd                          1/1     Running   0
2m53s
traefik-6548496576-srs6r                          1/1     Running   0
98s
trident-svc-679856c67-78kbt                       1/1     Running   0
5m27s
vault-controller-747d664964-xmn6c                 1/1     Running   0
7m37s
```

각 POD는 실행 중 상태여야 합니다. 시스템 포드를 구축하는 데 몇 분 정도 걸릴 수 있습니다.

20. 모든 Pod가 실행 중인 경우 다음 명령을 실행하여 1회 암호를 검색합니다. YAML 출력 버전에서 'tatus.deploymentState` 필드에 배포된 값을 확인한 후 'Status.uuid' 값을 복사합니다. 암호는 'ACC-'로, 이어서 UUID 값이 된다. (ACC - [UUID]).

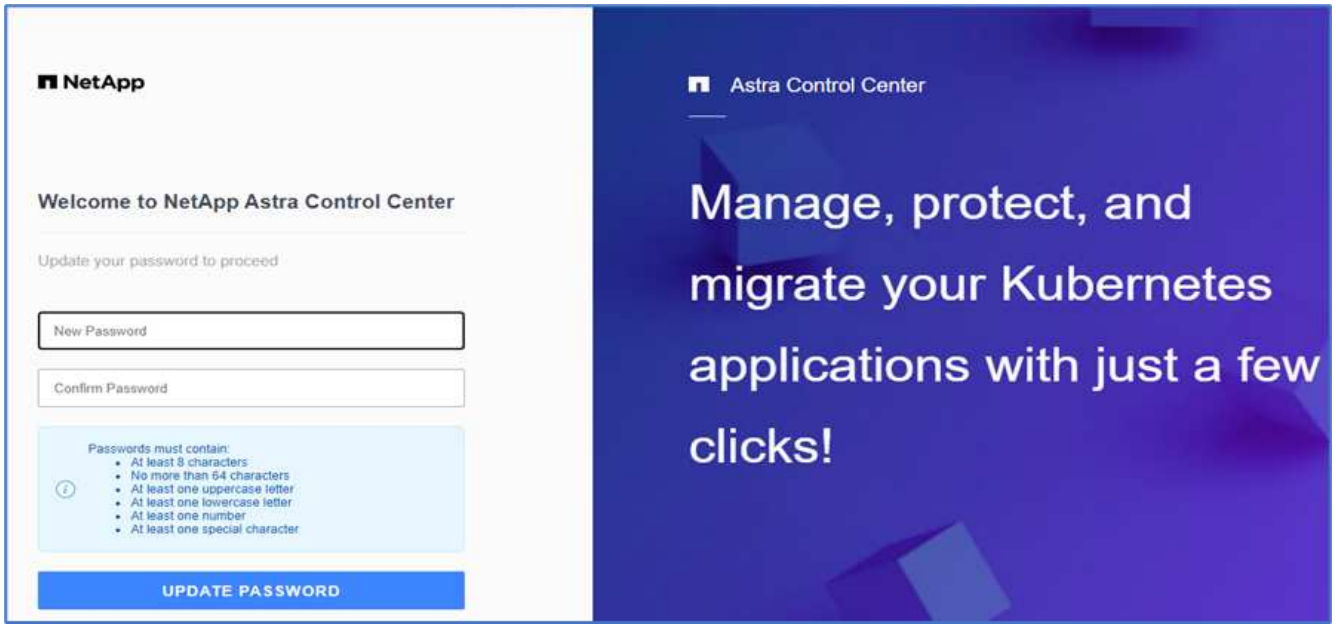
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

21. 브라우저에서 제공한 FQDN을 사용하여 URL로 이동합니다.
22. 설치 중에 제공된 이메일 주소인 기본 사용자 이름과 1회 암호 ACC-[UUID]를 사용하여 로그인합니다.



잘못된 암호를 세 번 입력하면 관리자 계정이 15분 동안 잠깁니다.

23. 암호를 변경하고 계속 진행합니다.

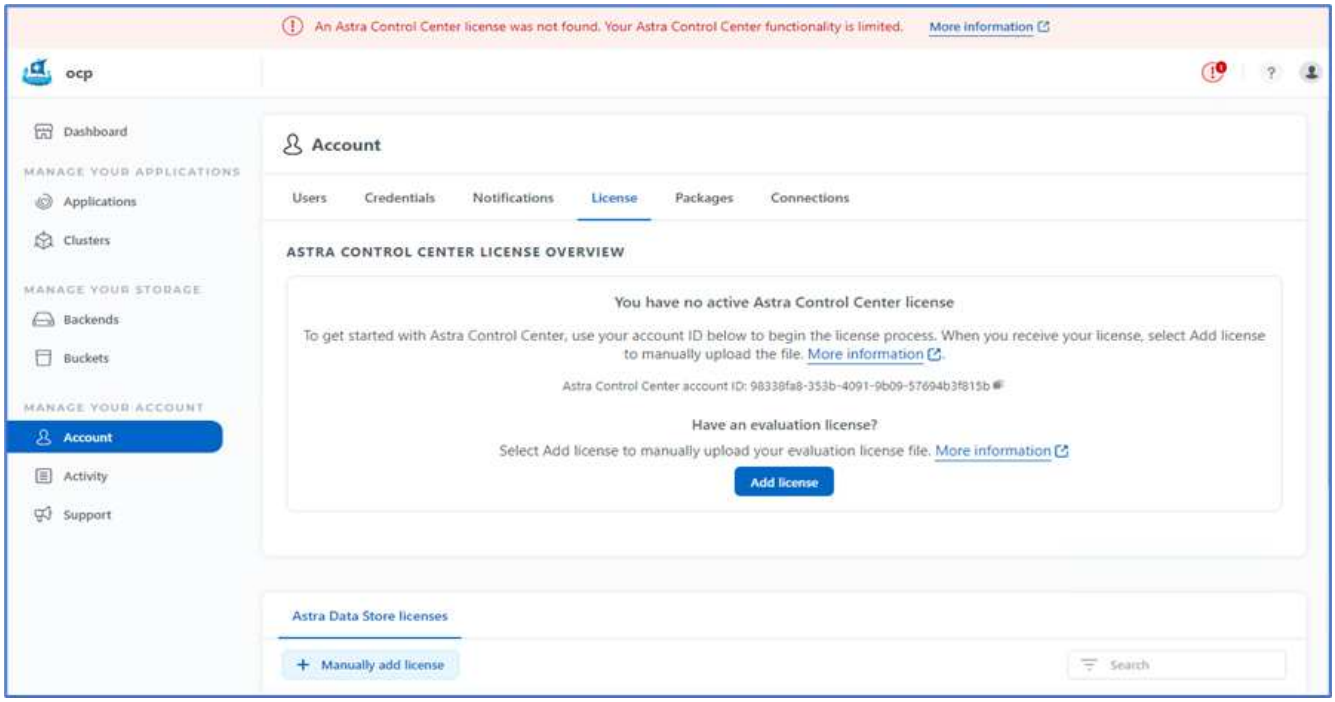


Astra Control Center 설치에 대한 자세한 내용은 를 참조하십시오 "Astra Control Center 설치 개요" 페이지.

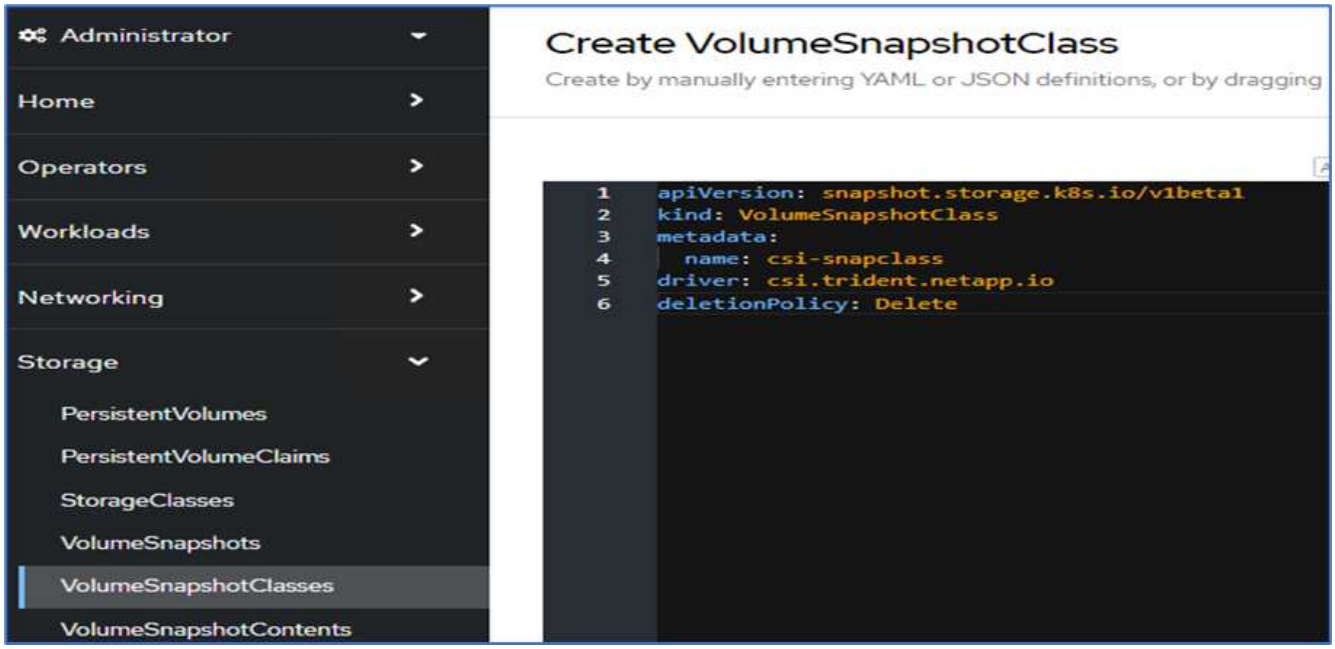
Astra Control Center를 설정합니다

Astra Control Center를 설치한 후 UI에 로그인하고 라이센스를 업로드하고, 클러스터를 추가하고, 스토리지를 관리하고, 버킷을 추가합니다.

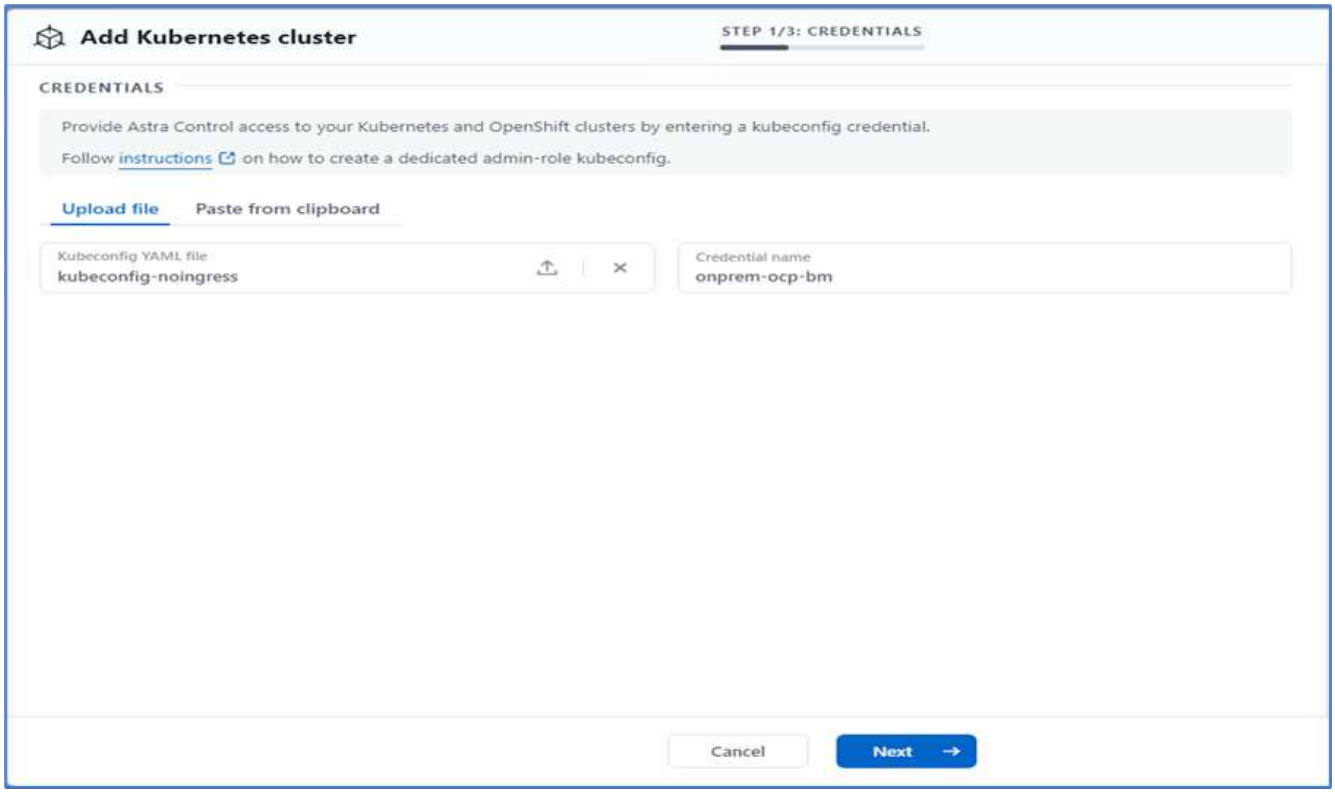
1. 홈 페이지의 계정 에서 라이센스 탭으로 이동하고 라이센스 추가 를 선택하여 Astra 라이센스를 업로드합니다.



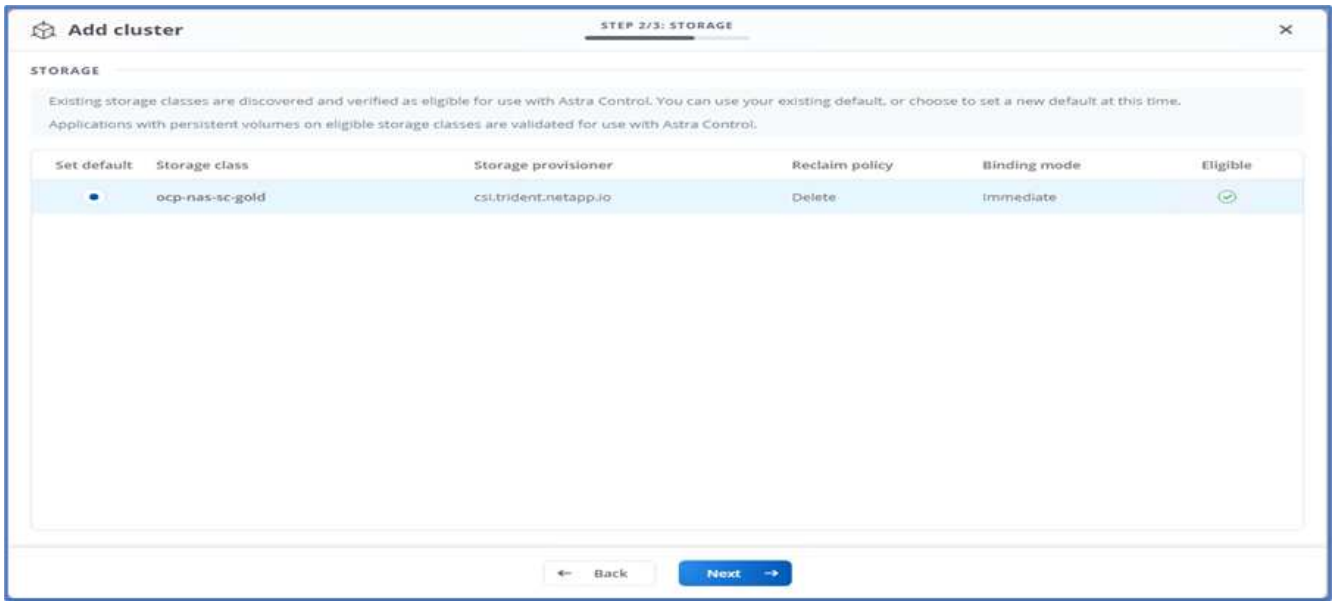
2. OpenShift 클러스터를 추가하기 전에 OpenShift 웹 콘솔에서 Astra Trident Volume 스냅샷 클래스를 생성합니다. 볼륨 스냅샷 클래스는 'csi.trident.netapp.io` 드라이버'로 구성됩니다.



3. Kubernetes 클러스터를 추가하려면 홈 페이지의 클러스터 로 이동하고 Kubernetes 클러스터 추가 를 클릭합니다. 그런 다음 클러스터에 대한 kubecononfig 파일을 업로드하고 자격 증명 이름을 제공합니다. 다음 을 클릭합니다.



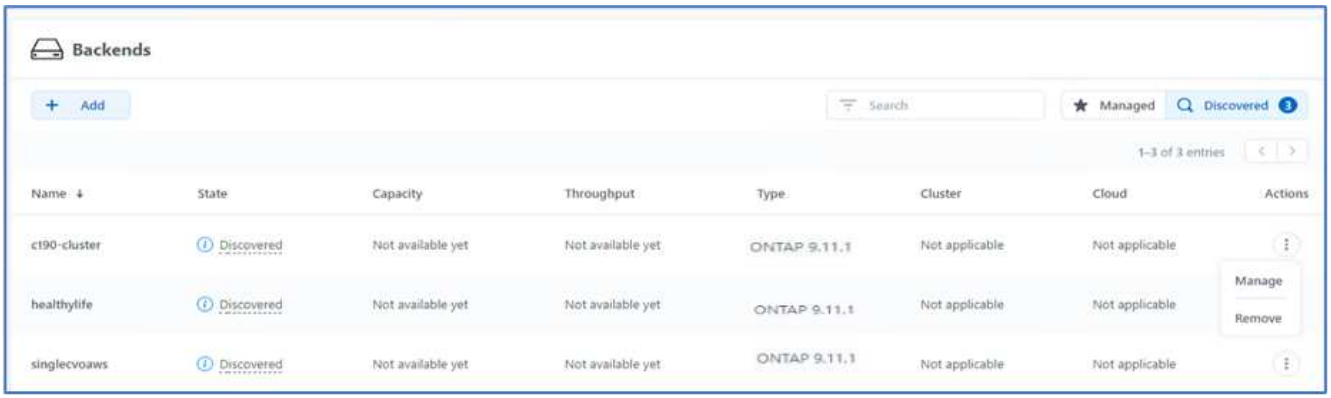
4. 기존 스토리지 클래스가 자동으로 검색됩니다. 기본 스토리지 클래스를 선택하고 다음 을 클릭한 다음 클러스터 추가 를 클릭합니다.



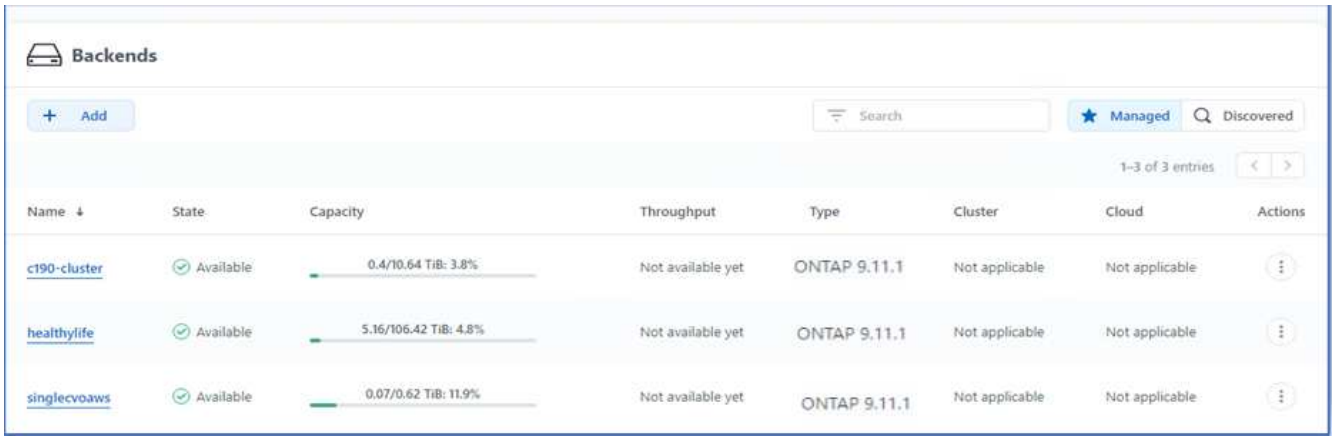
5. 몇 분 내에 클러스터가 추가됩니다. OpenShift Container Platform 클러스터를 추가하려면 1-4단계를 반복합니다.

> OpenShift 운영 환경을 관리되는 컴퓨팅 리소스로 추가하려면 Astra Trident를 확인하십시오 "VolumeSnapshotClass 객체" 정의됩니다.

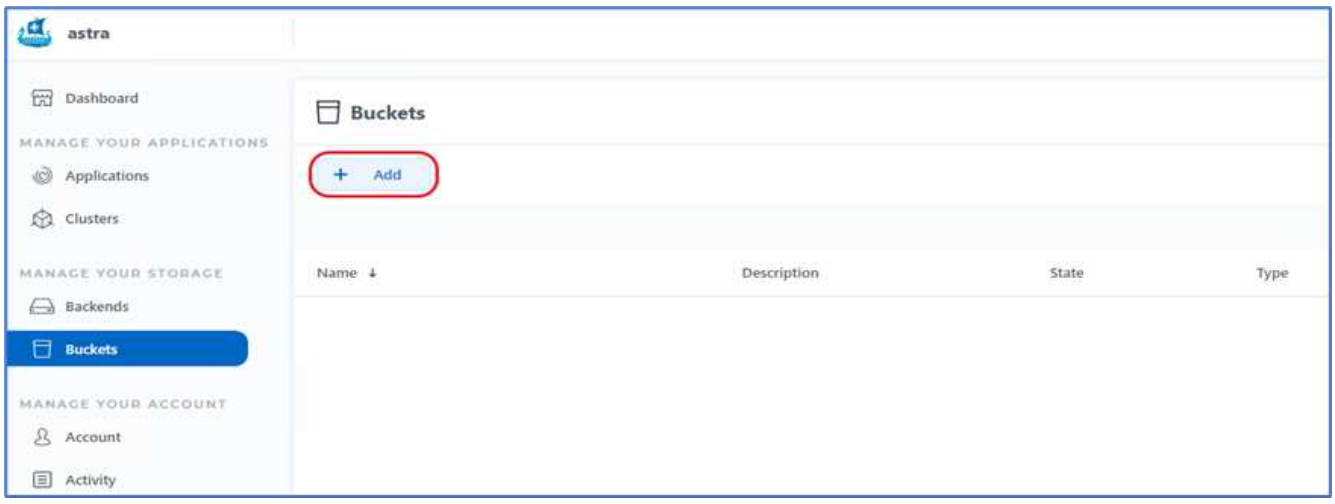
6. 스토리지를 관리하려면 백엔드로 이동하여 관리하려는 백엔드에 대한 작업에서 세 개의 점을 클릭합니다. 관리 를 클릭합니다.



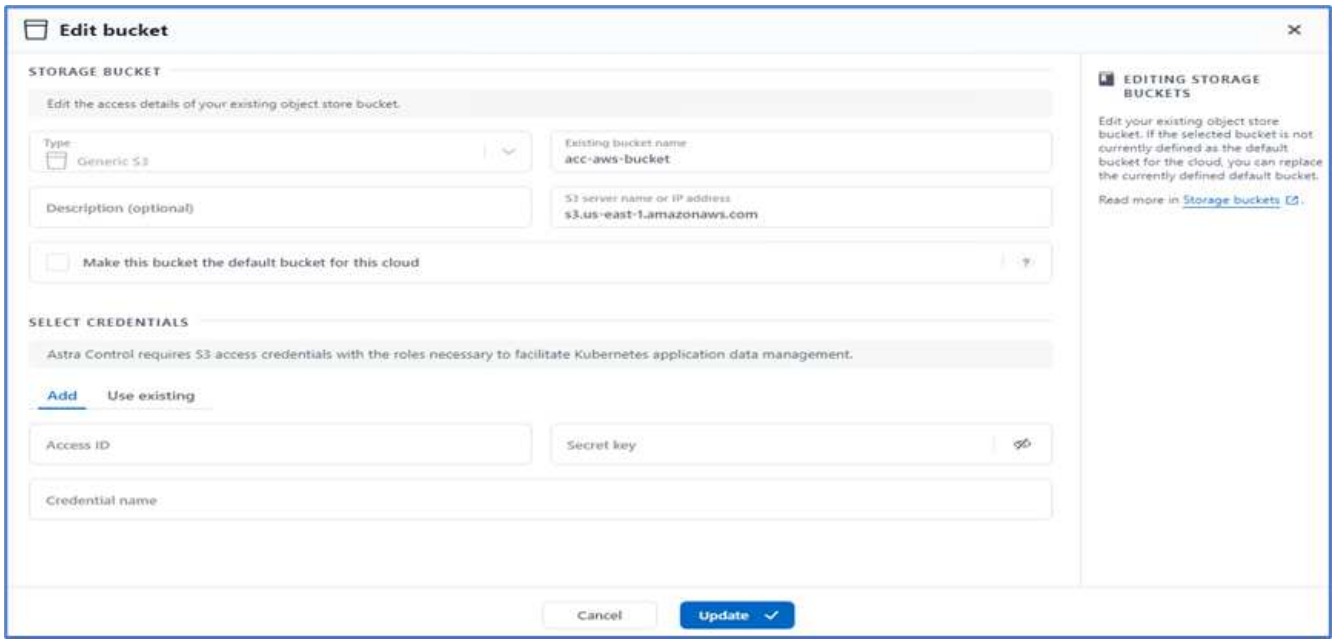
7. ONTAP 자격 증명을 입력하고 Next를 클릭합니다. 정보를 검토하고 관리 를 클릭합니다. 백엔드는 다음 예제와 같아야 합니다.



8. Astra Control에 버킷을 추가하려면 Bucket 을 선택하고 Add 를 클릭합니다.

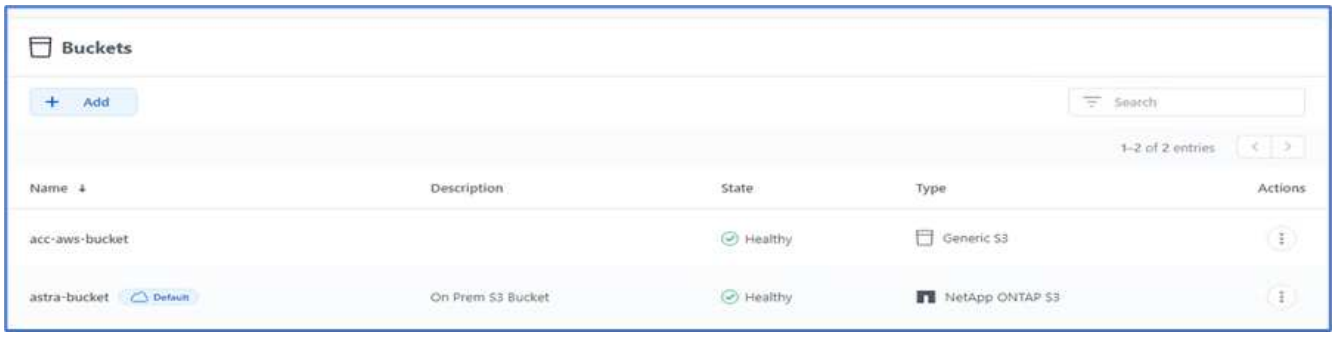


9. 버킷 유형을 선택하고 버킷 이름, S3 서버 이름 또는 IP 주소와 S3 자격 증명을 제공합니다. 업데이트 를 클릭합니다.



이 솔루션에서는 AWS S3 및 ONTAP S3 버킷을 모두 사용합니다. StorageGRID를 사용할 수도 있습니다.

Bucket 상태는 정상 상태여야 합니다.



Astra Control Center에서 애플리케이션 인식 데이터 관리를 위한 Kubernetes 클러스터 등록 시, Astra Control은 역할 바인딩 및 NetApp 모니터링 네임스페이스를 자동으로 생성하여 애플리케이션 Pod 및 작업자 노드에서 메트릭 및 로그를 수집합니다. 지원되는 ONTAP 기반 스토리지 클래스 중 하나를 기본값으로 설정합니다.

먼저 해 "Astra Control 관리에 클러스터를 추가합니다"클러스터(Astra Control 외)에 앱을 설치한 다음 Astra Control의 앱 페이지로 이동하여 앱과 리소스를 관리할 수 있습니다. Astra로 앱을 관리하는 방법에 대한 자세한 내용은 을 참조하십시오 "설명합니다".

"다음: 솔루션 검증 개요"

솔루션 검증

개요

"이전: OpenShift Container Platform에 Astra Control Center 설치."

이 섹션에서는 몇 가지 사용 사례와 함께 솔루션을 다시 살펴봅니다.

- 원격 백업에서 클라우드 실행 중인 다른 OpenShift 클러스터로 Stateful 애플리케이션을 복원합니다.
- OpenShift 클러스터의 동일한 네임스페이스에 stateful 애플리케이션을 복원합니다.
- 한 FlexPod 시스템(OpenShift Container Platform Bare Metal)에서 다른 FlexPod 시스템(VMware의 OpenShift Container Platform)으로 복제하여 애플리케이션 이동성 보장

그뿐만 아니라 이 솔루션에서 검증된 사용 사례는 몇 가지 뿐입니다. 이 검증은 Astra Control Center의 전체 기능을 나타내는 것은 아닙니다.

"다음: 원격 백업을 사용한 애플리케이션 복구"

원격 백업을 사용한 애플리케이션 복구

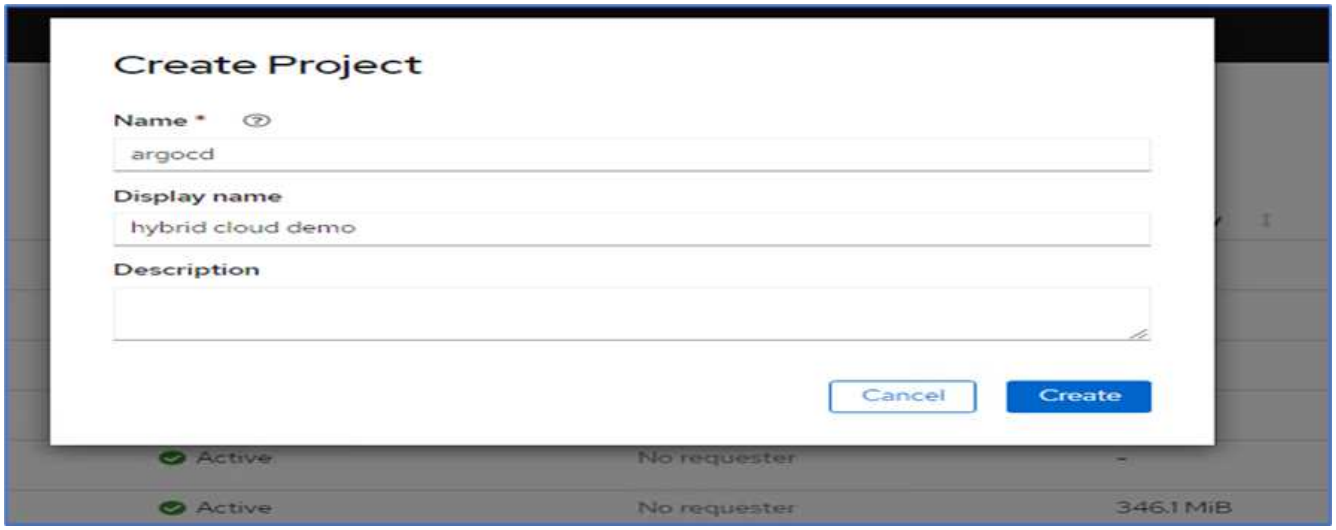
"이전: 솔루션 검증 개요"

Astra를 사용하면 애플리케이션 정합성이 보장된 전체 백업을 수행할 수 있습니다. 이 백업을 사용하여 사내 데이터 센터 또는 퍼블릭 클라우드에서 실행 중인 다른 Kubernetes 클러스터로 데이터를 가진 애플리케이션을 복원할 수 있습니다.

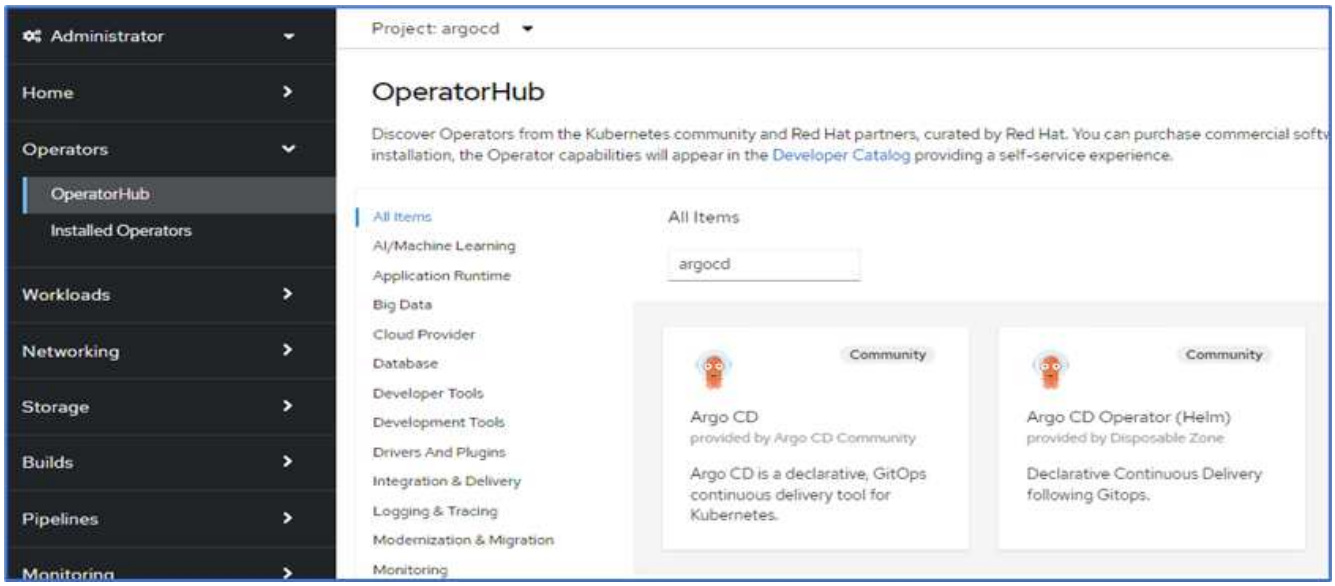
성공적인 애플리케이션 복구를 검증하려면 FlexPod 시스템에서 실행 중인 애플리케이션의 사내 장애를 시뮬레이션하고 원격 백업을 사용하여 클라우드에서 실행 중인 K8s 클러스터로 애플리케이션을 복구합니다.

샘플 응용 프로그램은 데이터베이스에 MySQL을 사용하는 가격 목록 응용 프로그램입니다. 배포를 자동화하기 위해 을 사용했습니다 "argo CD" 도구. argo CD는 선언적 GitOps, 지속적인 Kubernetes 제공 툴입니다.

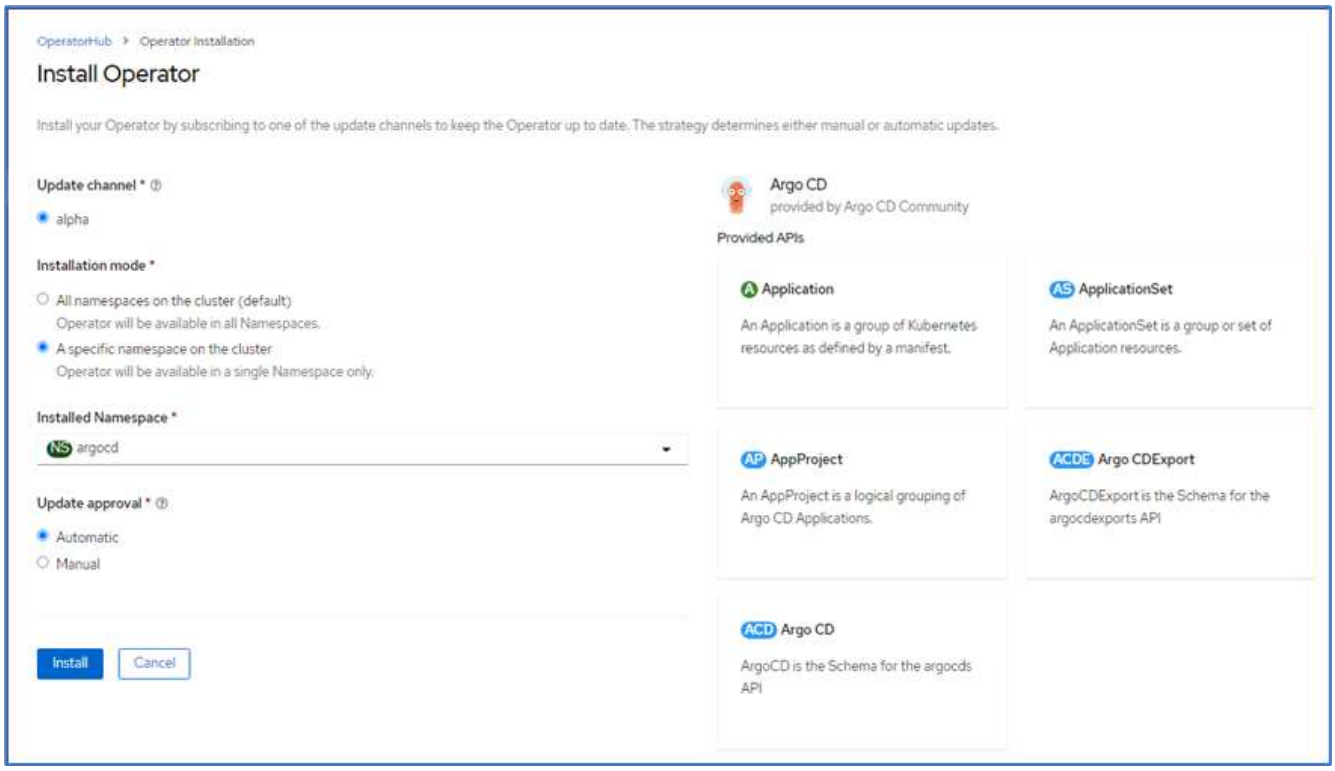
1. 온-프레미스 OpenShift 클러스터에 로그인하여 이름이 argocd인 새 프로젝트를 만듭니다.



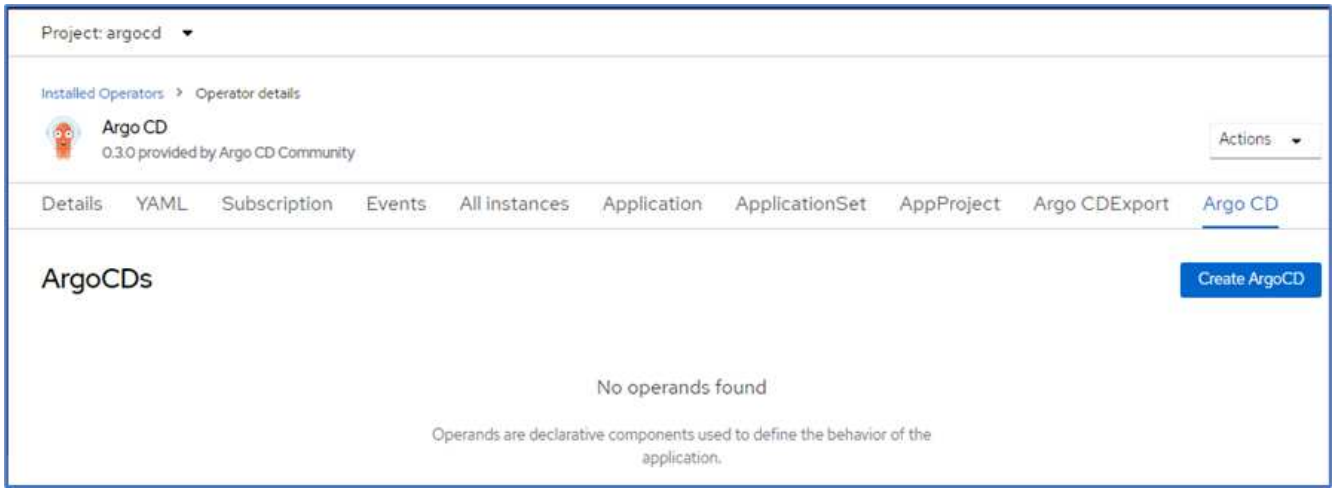
2. OperatorHub에서 argocd를 검색하고 Argo CD 연산자를 선택합니다.



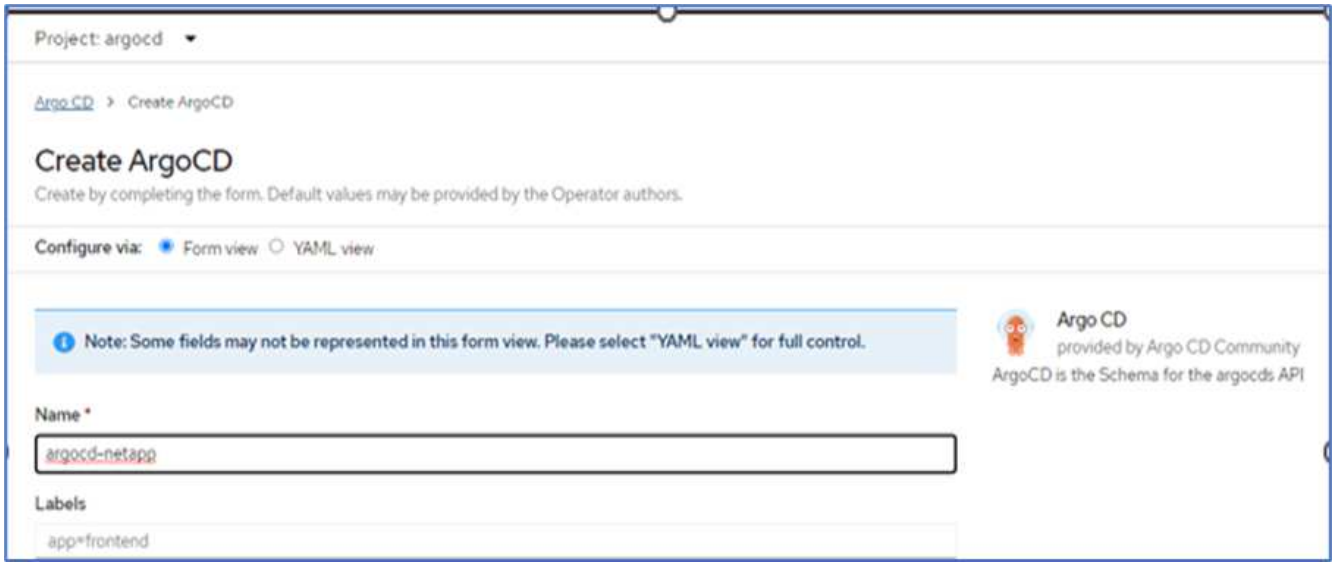
3. 'argocd' 네임스페이스에 연산자를 설치합니다.



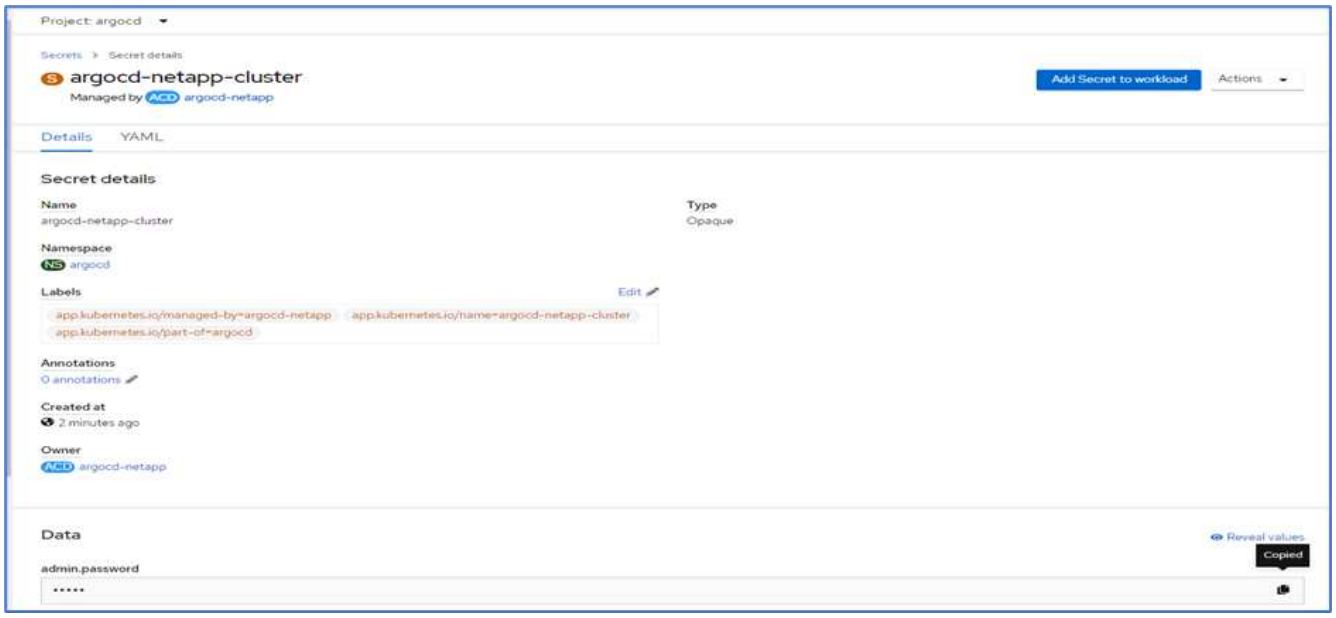
4. 운영자로 이동하여 ArgoCD 생성 을 클릭합니다.



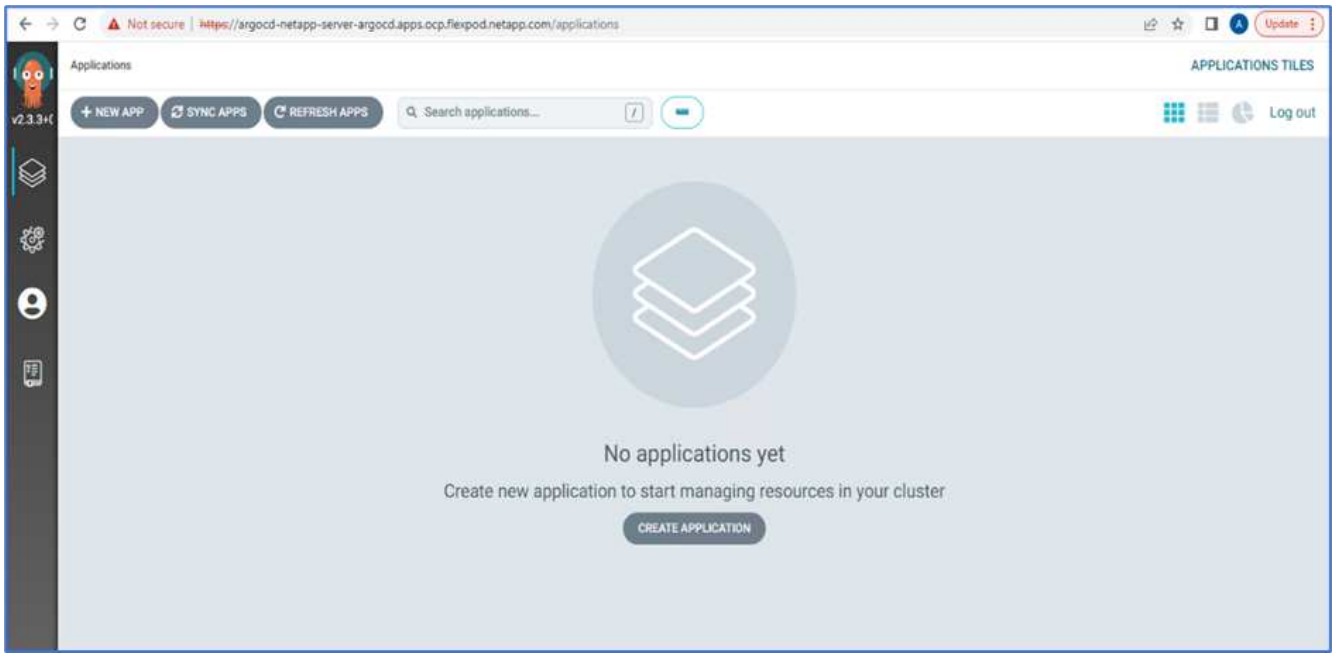
5. 아르고 CD 인스턴스를 "argocd" 프로젝트에 배포하려면 이름을 입력하고 만들기 를 클릭합니다.



6. Argo CD에 로그인하려면 기본 사용자는 admin이고 암호는 "argocd-NetApp-cluster"라는 이름의 비밀 파일에 있어야 합니다.



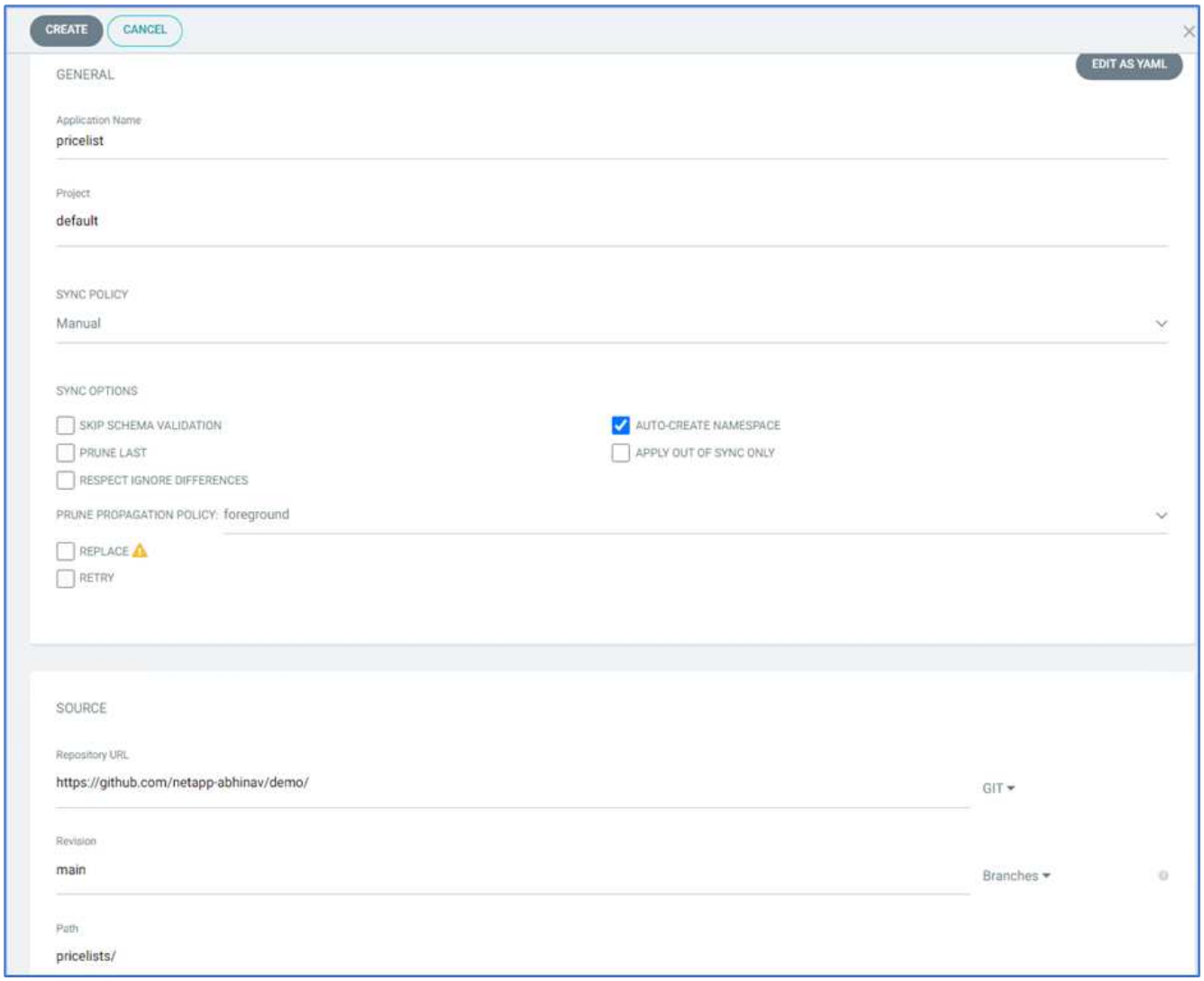
7. 측면 메뉴에서 루트 > 위치를 선택하고 "argocd" 루트의 URL을 클릭합니다. 사용자 이름과 암호를 입력합니다.



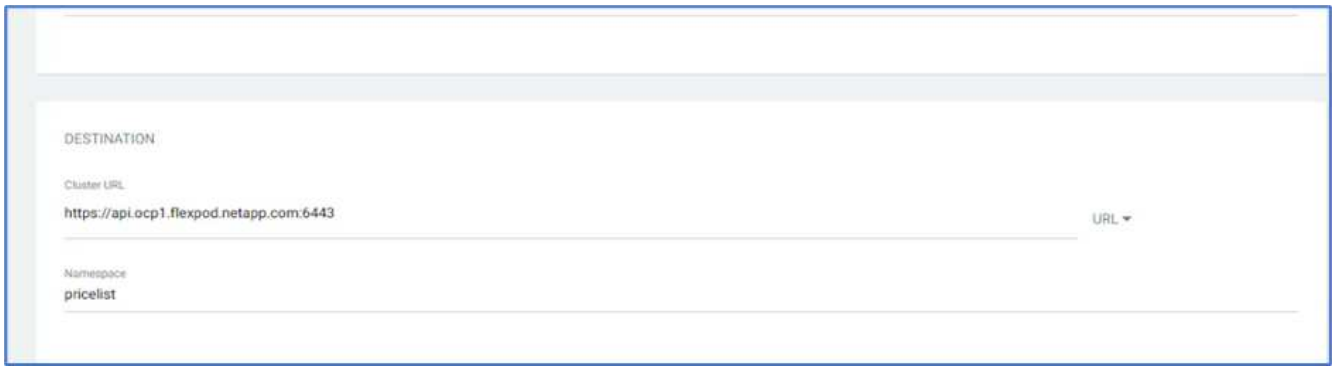
8. CLI를 통해 Argo CD에 온-프레미스 OpenShift 클러스터를 추가합니다.

```
####Login to Argo CD####
abhinav3@abhinav-ansible$ argocd-linux-amd64 login argocd-netapp-server-
argocd.apps.ocp.flexpod.netapp.com --insecure
Username: admin
Password:
'admin:login' logged in successfully
Context'argocd-netapp-server-argocd.apps.ocp.flexpod.netapp.com' updated
####List the On-Premises OpenShift cluster####
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add
ERRO[0000] Choose a context name from:
CURRENT  NAME
CLUSTER              SERVER
*        default/api-ocp-flexpod-netapp-com:6443/abhinav3
api-ocp-flexpod-netapp-com:6443
https://api.ocp.flexpod.netapp.com:6443
         default/api-ocp1-flexpod-netapp-com:6443/abhinav3
api-ocp1-flexpod-netapp-com:6443
https://api.ocp1.flexpod.netapp.com:6443
####Add On-Premises OpenShift cluster###
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add default/api-
ocp1-flexpod-netapp-com:6443/abhinav3
WARNING: This will create a service account `argocd-manager` on the
cluster referenced by context `default/api-ocp1-flexpod-netapp-
com:6443/abhinav3` with full cluster level admin privileges. Do you want
to continue [y/N]? y
INFO[0002] ServiceAccount "argocd-manager" already exists in namespace
"kube-system"
INFO[0002] ClusterRole "argocd-manager-role" updated
INFO[0002] ClusterRoleBinding "argocd-manager-role-binding" updated
Cluster 'https://api.ocp1.flexpod.netapp.com:6443' added
```

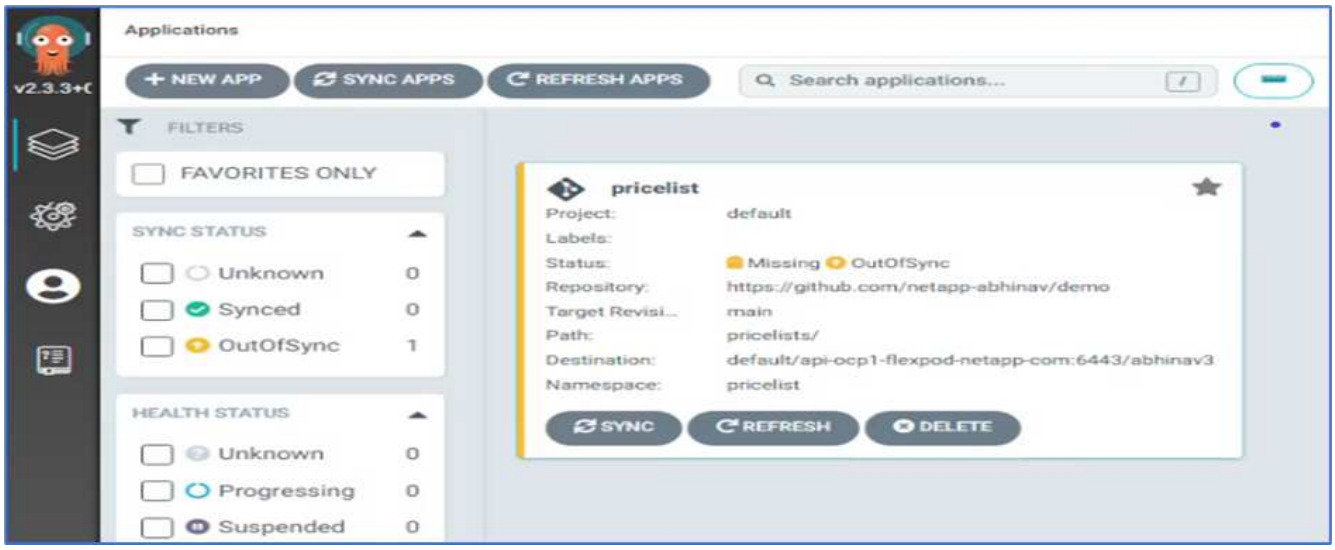
9. ArgoCD UI에서 새 앱 을 클릭하고 앱 이름 및 코드 리포지토리에 대한 세부 정보를 입력합니다.



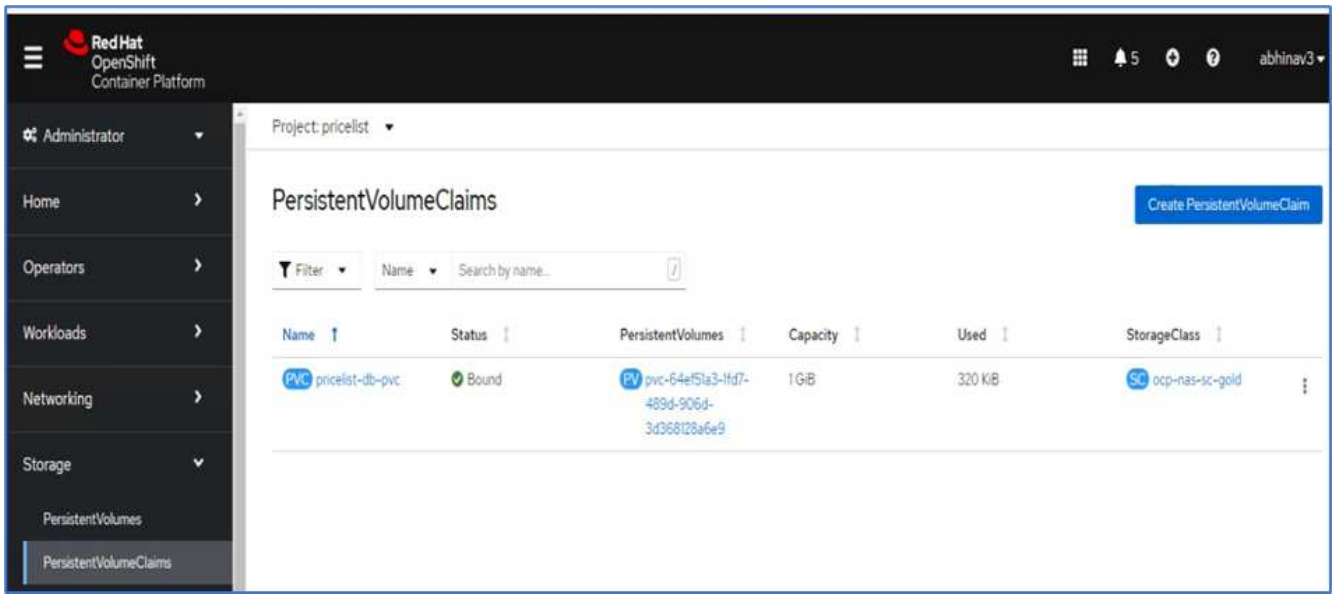
10. 네임스페이스와 함께 앱을 배포할 OpenShift 클러스터를 입력합니다.



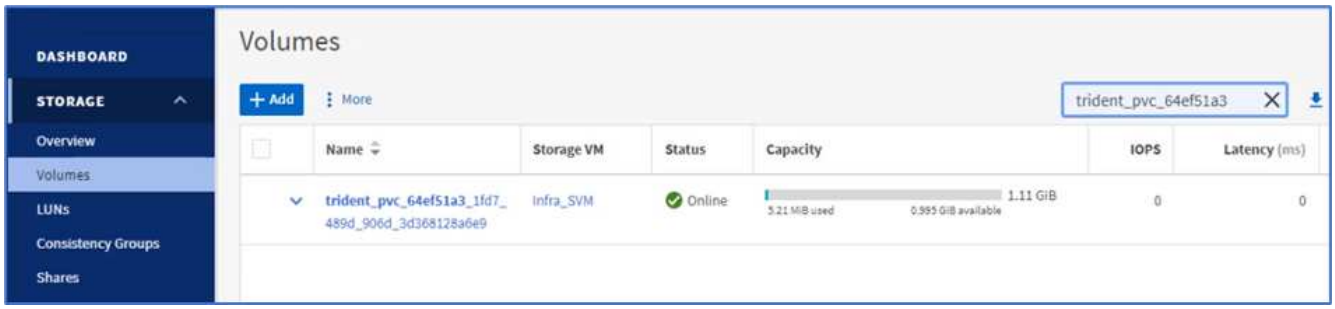
11. 온-프레미스 OpenShift 클러스터에 앱을 배포하려면 동기화 를 클릭합니다.



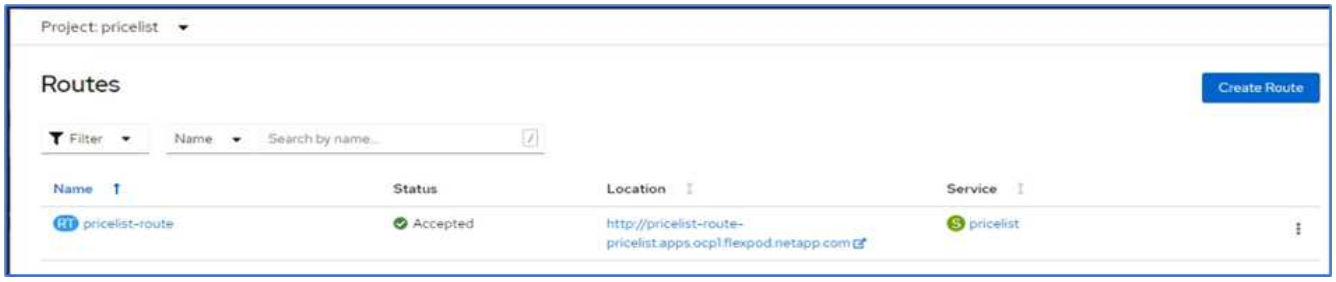
12. OpenShift Container Platform 콘솔에서 Project Pricelist로 이동한 후 Storage에서 PVC의 이름과 크기를 확인합니다.



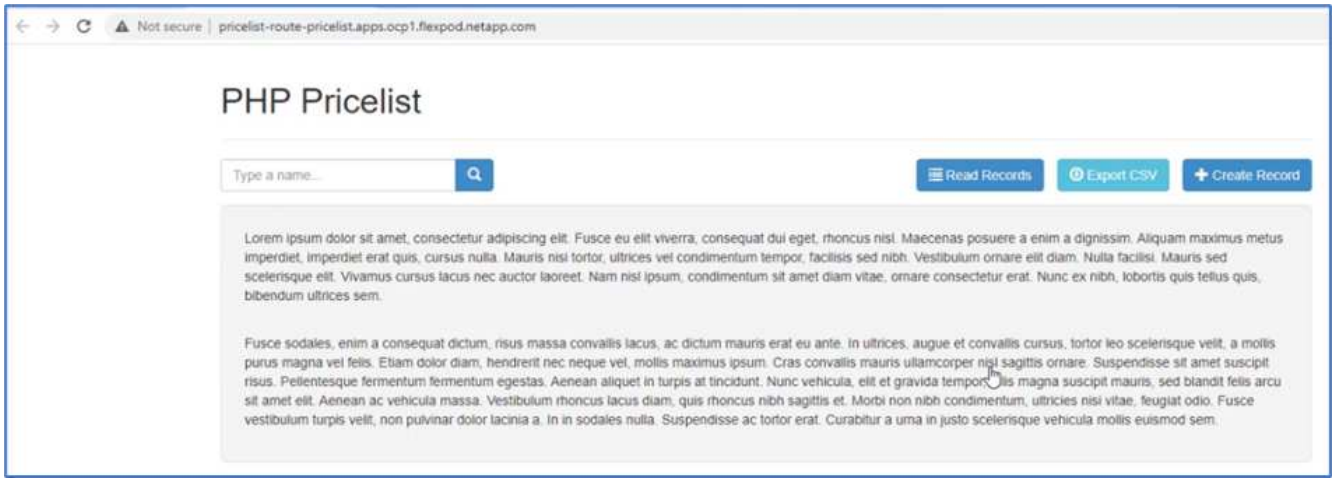
13. System Manager에 로그인하여 PVC를 확인합니다.



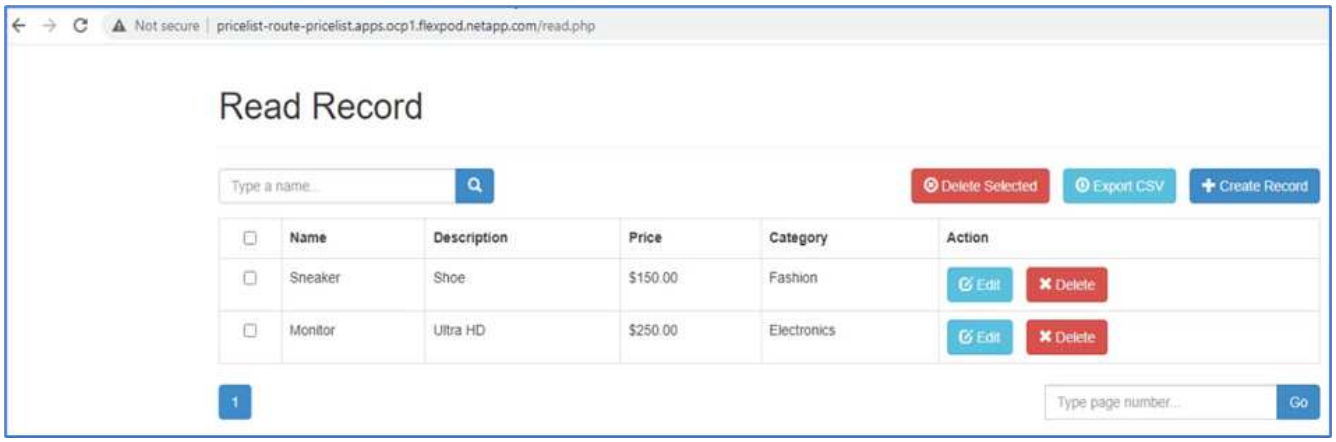
14. Pod가 실행된 후 측면 메뉴에서 네트워킹 > 경로를 선택하고 위치 에서 URL을 클릭합니다.



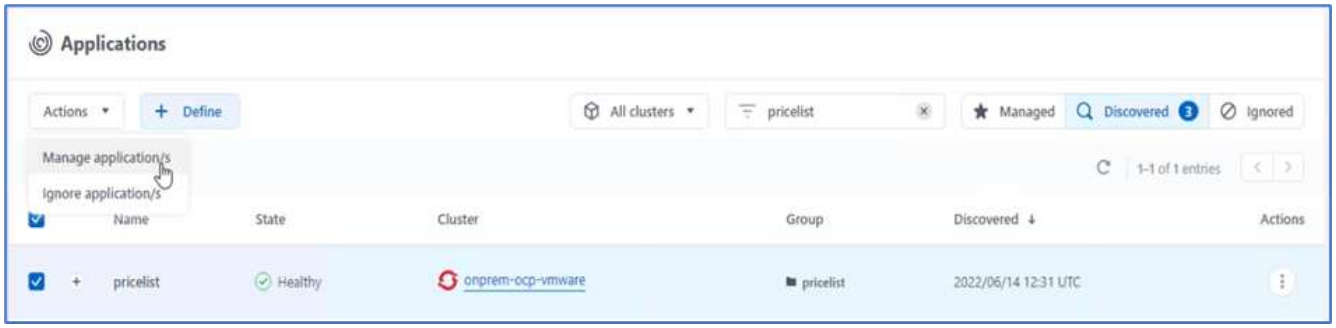
15. 가격 목록 앱 홈 페이지가 표시됩니다.



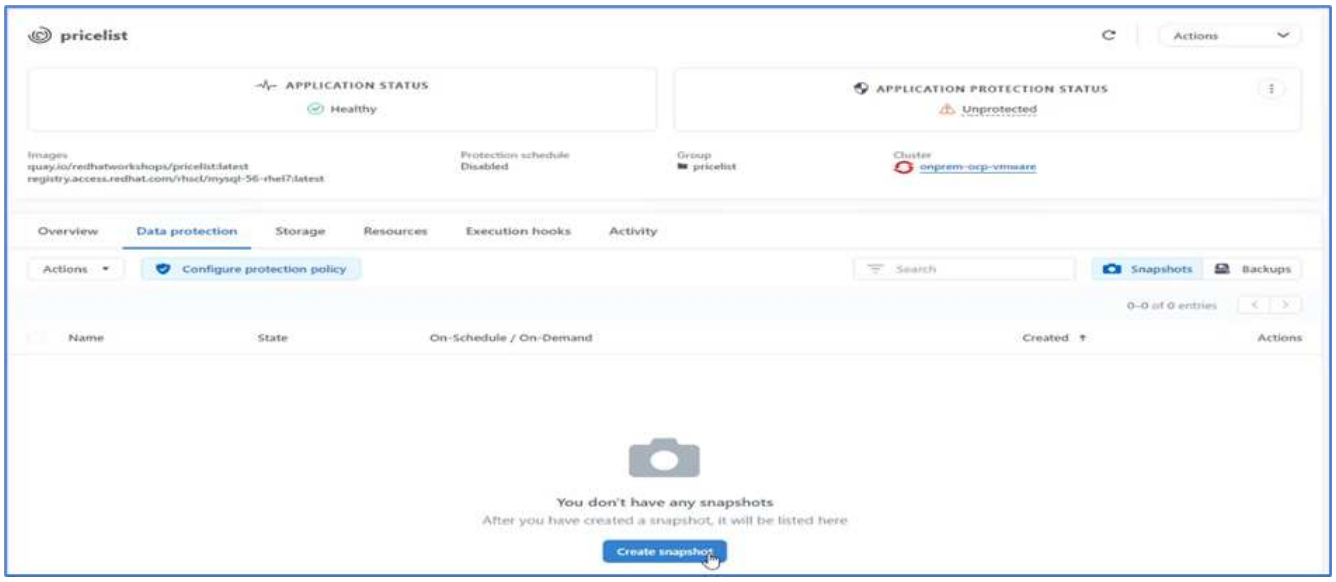
16. 웹 페이지에서 몇 개의 레코드를 만듭니다.



17. 이 앱은 Astra Control Center에서 발견됩니다. 앱을 관리하려면 응용 프로그램 > 검색으로 이동하여 가격 목록 앱을 선택하고 작업 에서 응용 프로그램 관리 를 클릭합니다.

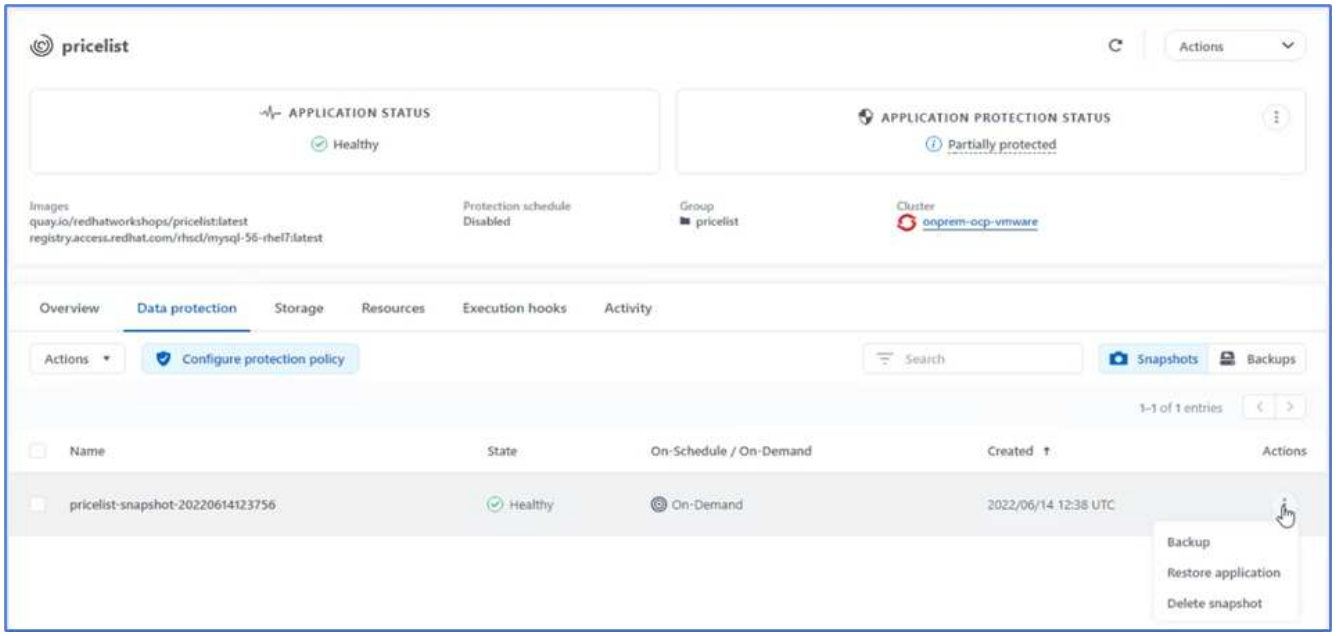


18. 가격 목록 앱을 클릭하고 데이터 보호 를 선택합니다. 이때 스냅샷 또는 백업이 없어야 합니다. 스냅샷 생성 을 클릭하여 필요 시 스냅샷을 생성합니다.

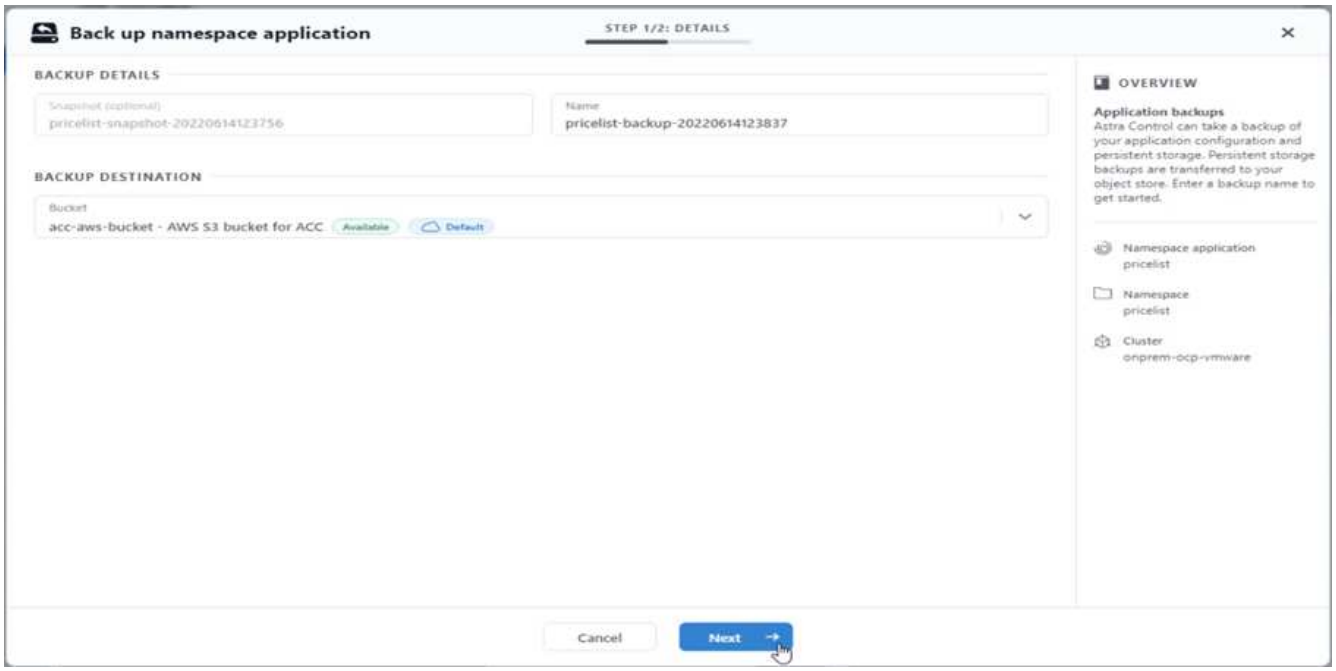


NetApp Astra Control Center는 주문형 스냅샷과 예약된 스냅샷 및 백업을 모두 지원합니다.

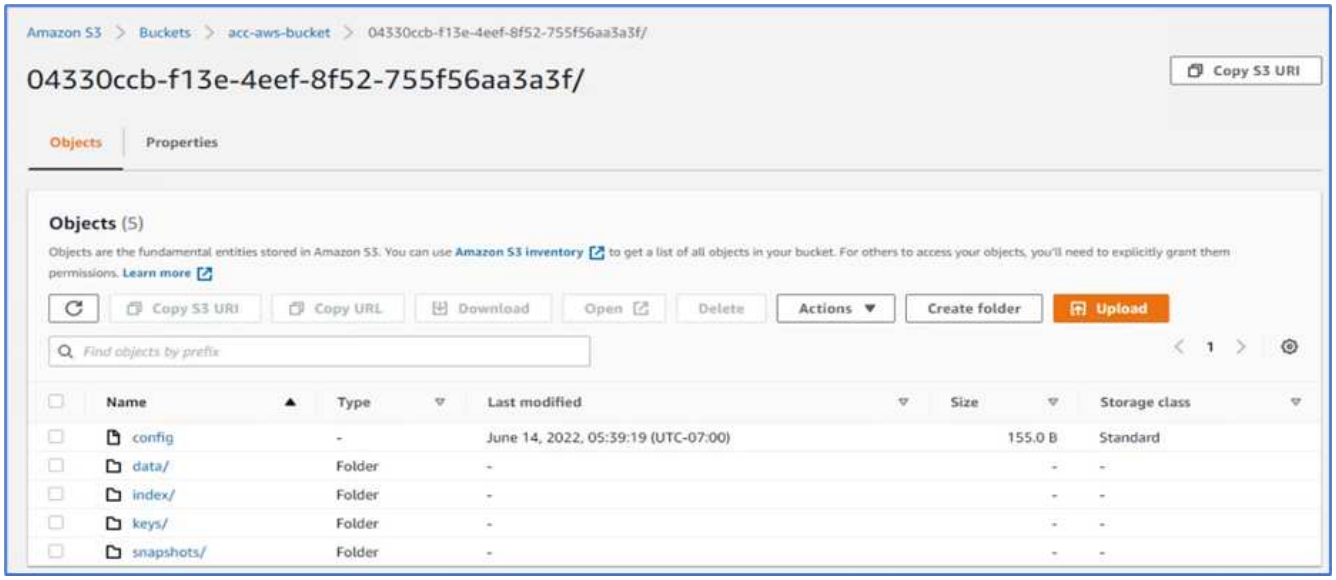
19. 스냅샷이 생성되고 상태가 양호하면 해당 스냅샷을 사용하여 원격 백업을 생성합니다. 이 백업은 S3 버킷에 저장됩니다.



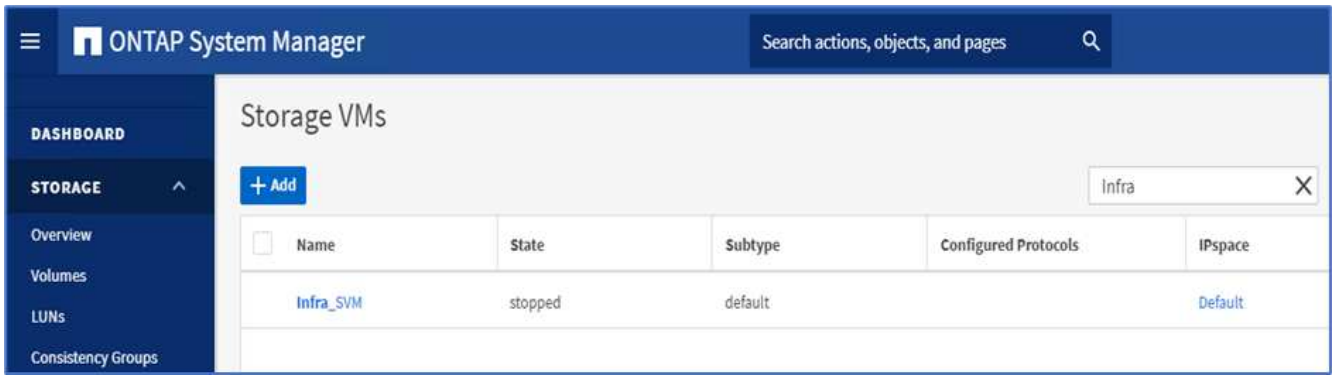
20. AWS S3 버킷을 선택하고 백업 작업을 시작합니다.



21. 백업 작업에서는 AWS S3 버킷에 여러 오브젝트가 포함된 폴더를 생성해야 합니다.



22. 원격 백업이 완료되면 PV의 백업 볼륨을 호스팅하는 SVM(스토리지 가상 머신)을 중지하여 온프레미스 재해 상황을 시뮬레이션합니다.

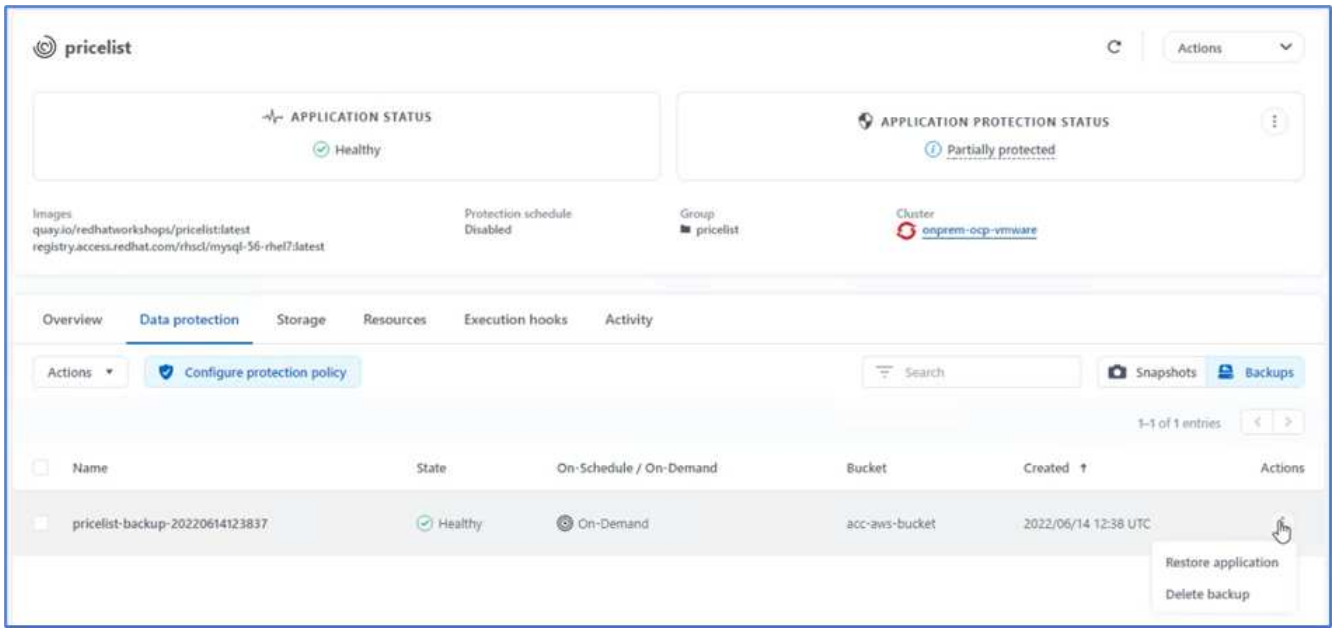


23. 웹 페이지를 새로 고쳐 중단을 확인합니다. 웹 페이지를 사용할 수 없습니다.

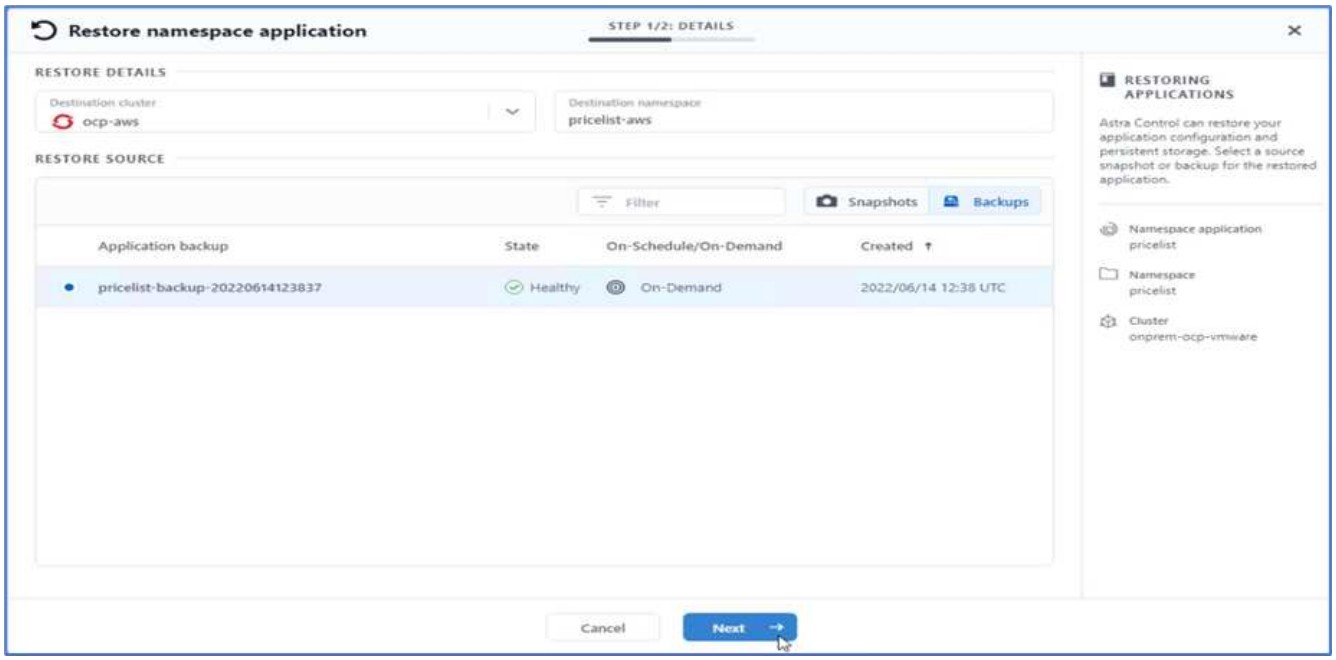


예상대로 웹 사이트가 다운되었습니다. 이제 Astra를 사용하여 AWS에서 실행되는 OpenShift 클러스터로 원격 백업에서 앱을 빠르게 복구하겠습니다.

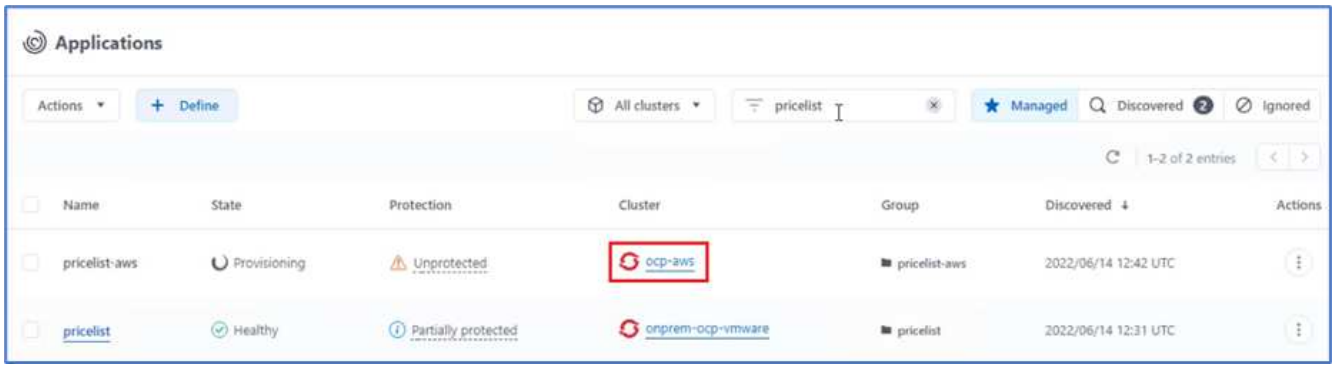
24. Astra Control Center에서 Pricelist 앱을 클릭하고 Data Protection > Backups를 선택합니다. 백업을 선택하고 작업 에서 응용 프로그램 복원 을 클릭합니다.



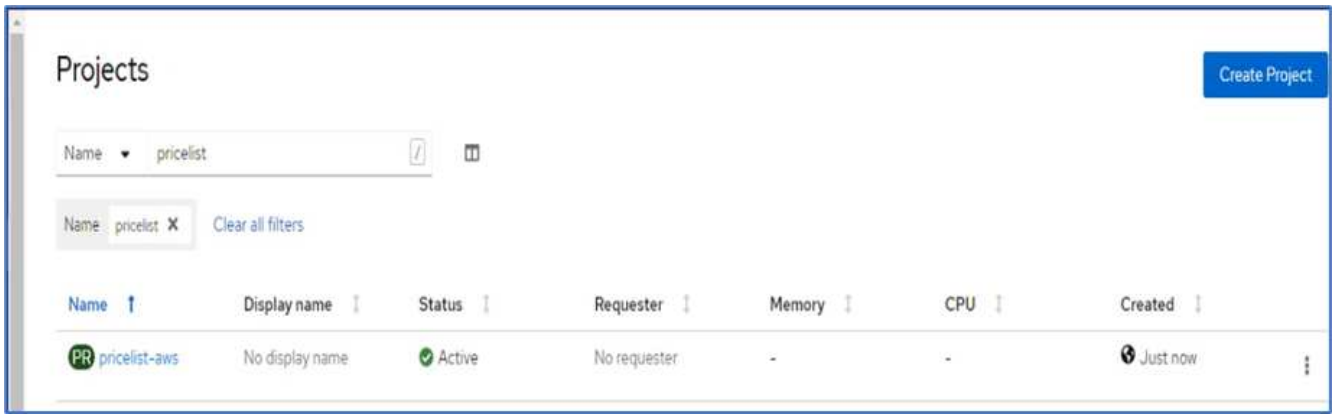
25. 대상 클러스터로 OCP-AWS를 선택하고 이름 공간에 이름을 지정합니다. 필요 시 백업, 다음, 복원을 차례로 클릭합니다.



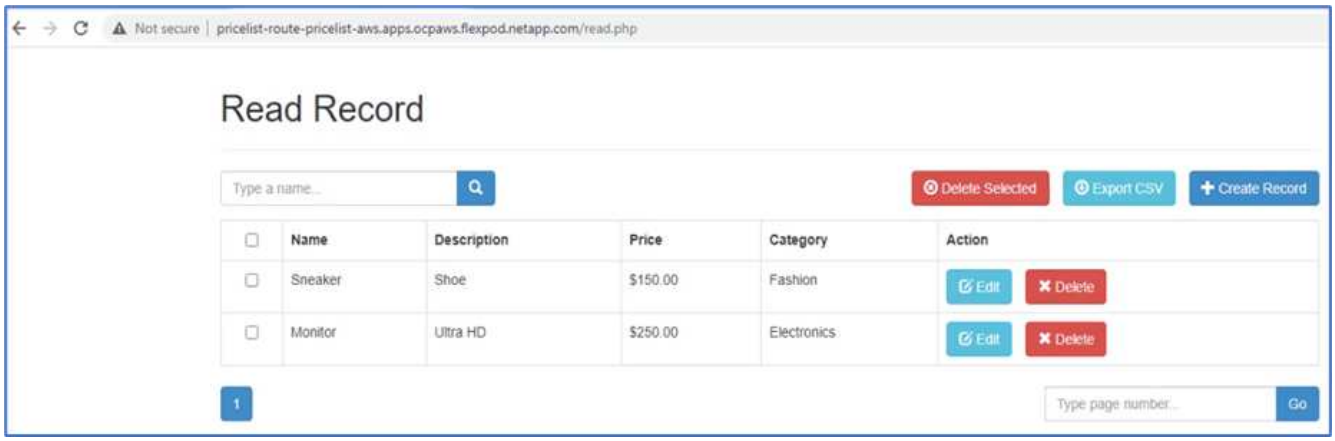
26. AWS에서 실행되는 OpenShift 클러스터에서 'pricelist-app'이라는 이름의 새 앱이 표시됩니다.



27. OpenShift 웹 콘솔에서도 동일하게 확인합니다.



28. Pricelist-AWS 프로젝트 아래의 모든 포드가 실행 중인 후 루트 로 이동한 다음 URL을 클릭하여 웹 페이지를 시작합니다.



이 프로세스는 Pricelist 애플리케이션이 성공적으로 복원되었으며 Astra Control Center의 도움을 받아 AWS에서 원활하게 실행되는 OpenShift 클러스터에서 데이터 무결성이 유지되었는지 확인합니다.

DevTest를 위한 스냅샷 복사본 및 애플리케이션 이동성으로 데이터 보호

이 사용 사례는 다음 섹션에 설명된 대로 두 부분으로 구성됩니다.

파트 **1**

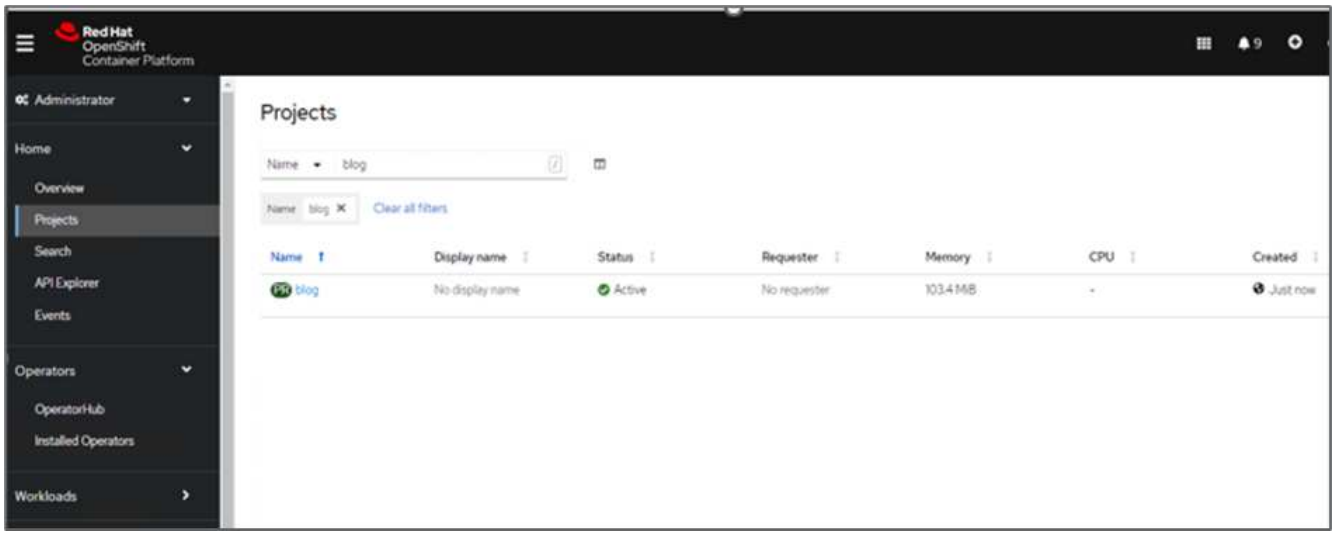
Astra Control Center를 사용하면 로컬 데이터 보호를 위해 애플리케이션 인식 스냅샷을 생성할 수 있습니다. 실수로 데이터를 삭제하거나 손상된 경우 이전에 기록된 스냅샷을 사용하여 응용 프로그램 및 관련 데이터를 알려진 양호한 상태로 되돌릴 수 있습니다.

이 시나리오에서 개발 및 테스트(DevTest) 팀은 Ghost 블로그 응용 프로그램인 샘플 상태 저장 응용 프로그램(블로그 사이트)을 배포하고 일부 콘텐츠를 추가하며 앱을 사용 가능한 최신 버전으로 업그레이드합니다. Ghost 응용 프로그램은 SQLite를 데이터베이스에 사용합니다. 애플리케이션을 업그레이드하기 전에 Astra Control Center를 사용하여 데이터 보호를 위한 스냅샷(필요 시)을 생성합니다. 자세한 단계는 다음과 같습니다.

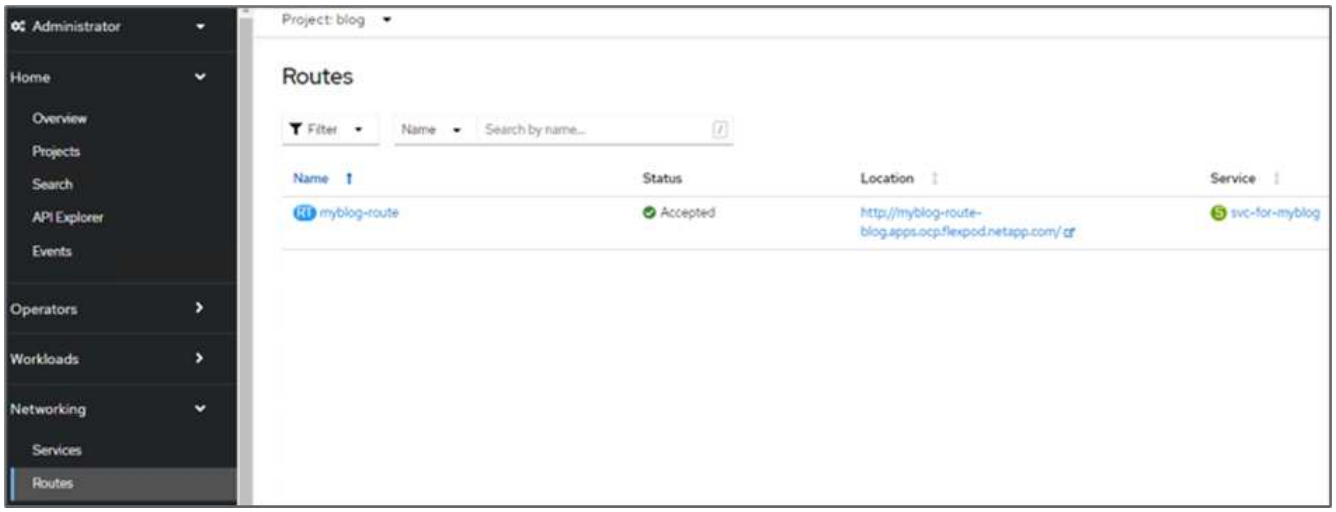
1. 샘플 블로깅 앱을 배포하고 ArgoCD에서 동기화합니다.



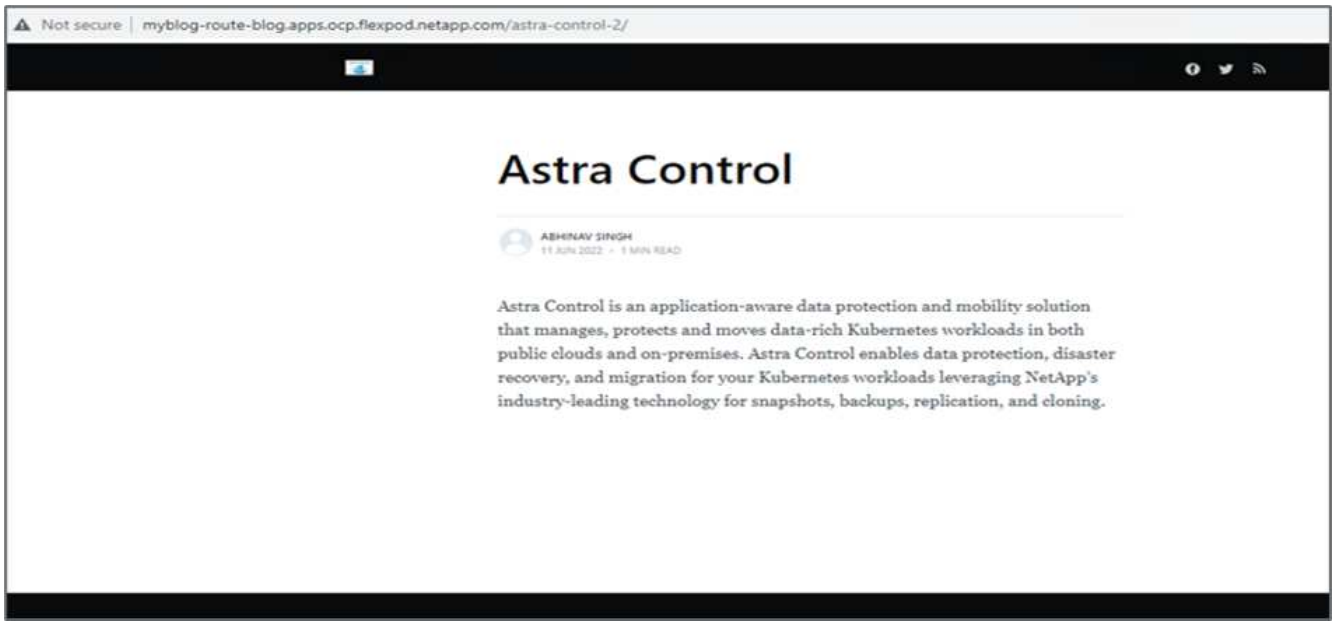
2. 첫 번째 OpenShift 클러스터에 로그인한 후 Project로 이동하여 검색 표시줄에 Blog를 입력합니다.



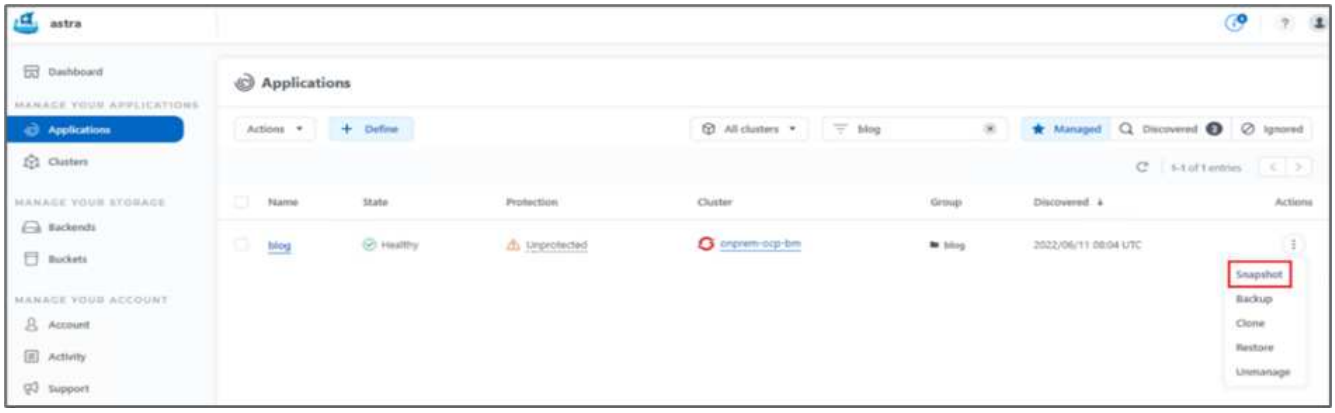
3. 측면 메뉴에서 네트워킹 > 경로를 선택하고 URL을 클릭합니다.



4. 블로그 홈 페이지가 표시됩니다. 일부 콘텐츠를 블로그 사이트에 추가하고 게시합니다.



5. Astra Control Center로 이동합니다. 먼저 검색된 탭에서 앱을 관리하고 스냅샷 복사본을 만듭니다.

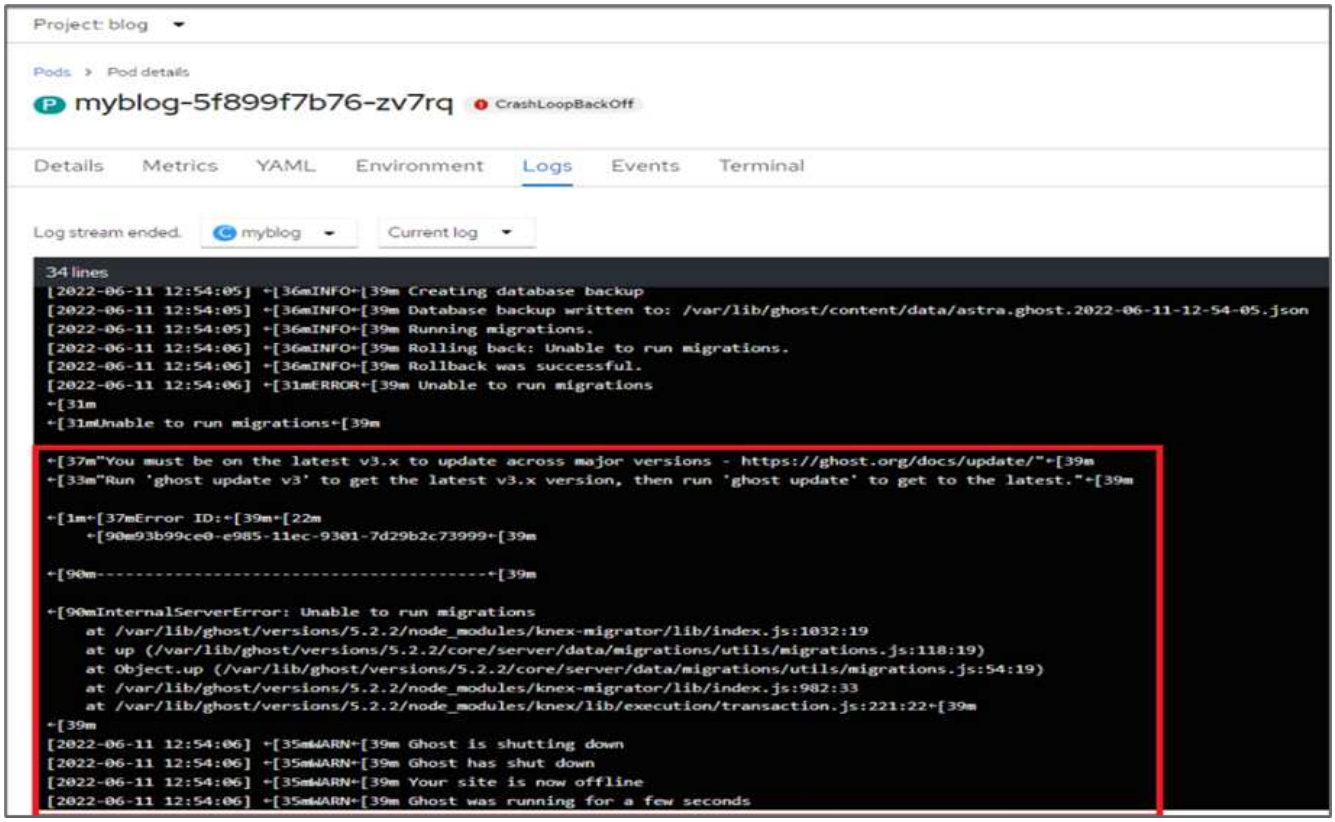


스냅샷, 백업 또는 둘 모두를 정의된 일정에 따라 생성하여 앱을 보호할 수도 있습니다. 자세한 내용은 을 참조하십시오 "스냅샷 및 백업으로 애플리케이션 보호".

6. 주문형 스냅샷이 생성된 후 앱을 최신 버전으로 업그레이드하십시오. 현재 이미지 버전은 고스트: 3.6-알파인(Ghost: 3.6-알파인)이며 타겟 버전은 유령: 최신이다. 앱을 업그레이드하려면 Git 리포지토리로 직접 변경하고 Argo CD에 동기화하십시오.

```
spec:
  containers:
  - name: myblog
    image: ghost:latest
    imagePullPolicy: Always
    ports:
    - containerPort: 2368
```

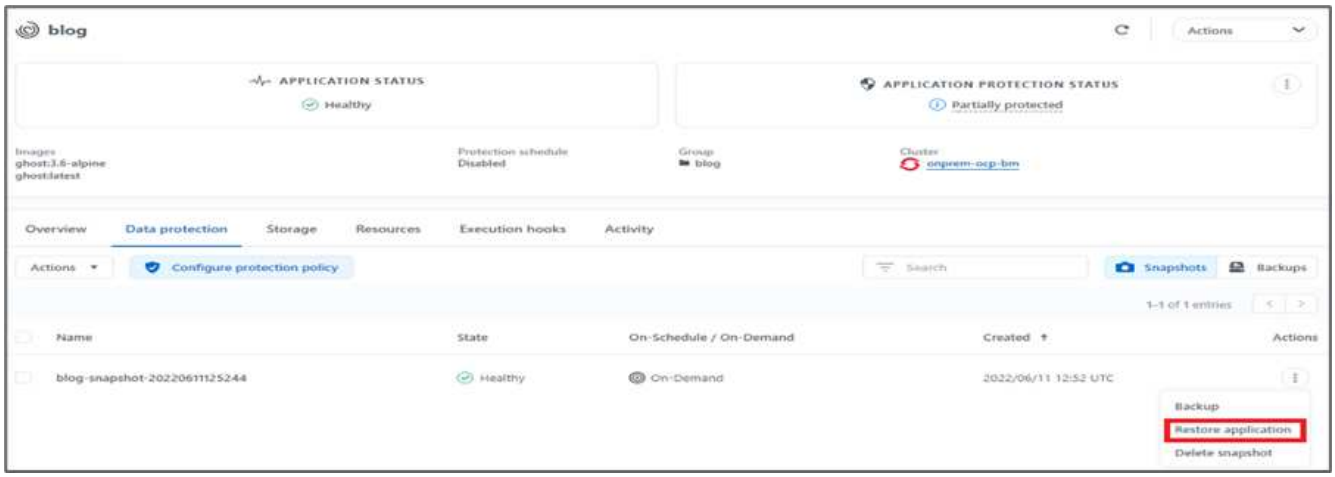
7. 블로그 사이트가 다운되고 전체 응용 프로그램이 손상되었기 때문에 최신 버전으로 직접 업그레이드할 수 없습니다.



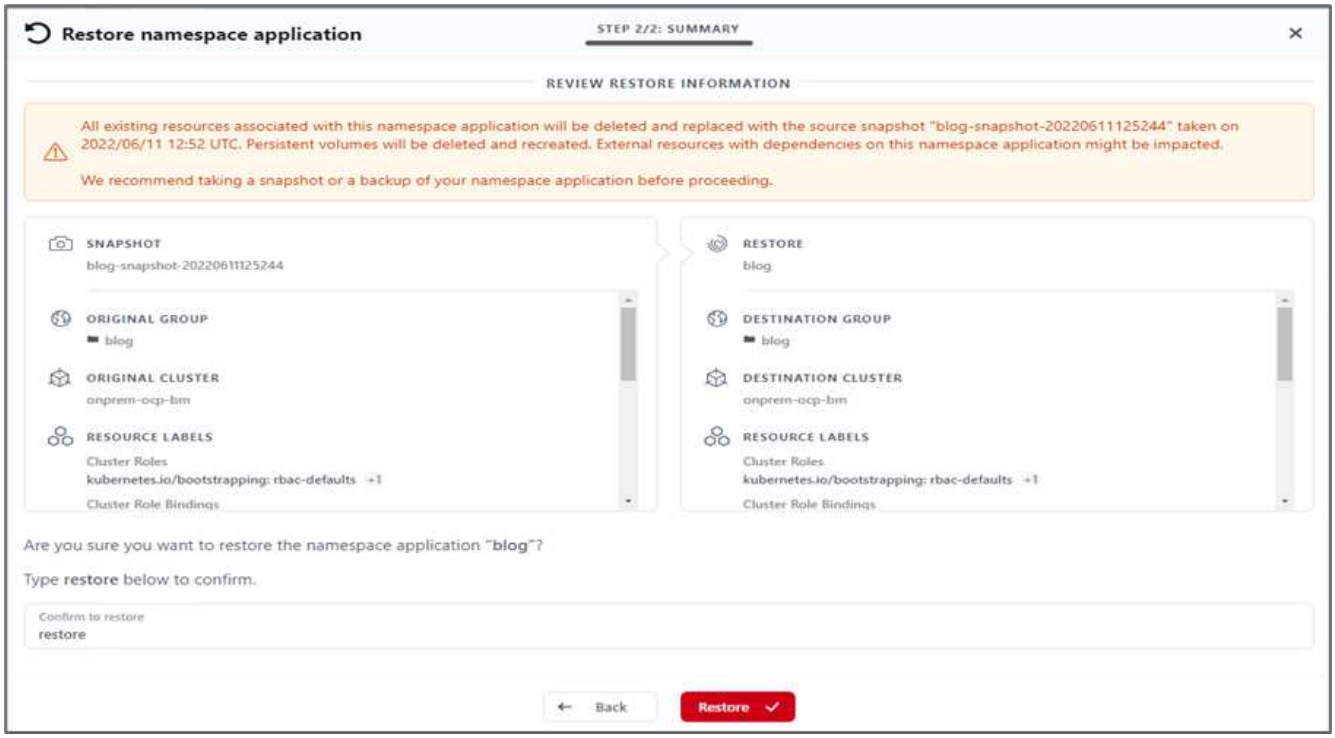
8. 블로그 사이트를 사용할 수 없음을 확인하려면 URL을 새로 고치십시오.



9. 스냅샷에서 앱을 복구합니다.



10. 앱은 동일한 OpenShift 클러스터에서 복원됩니다.



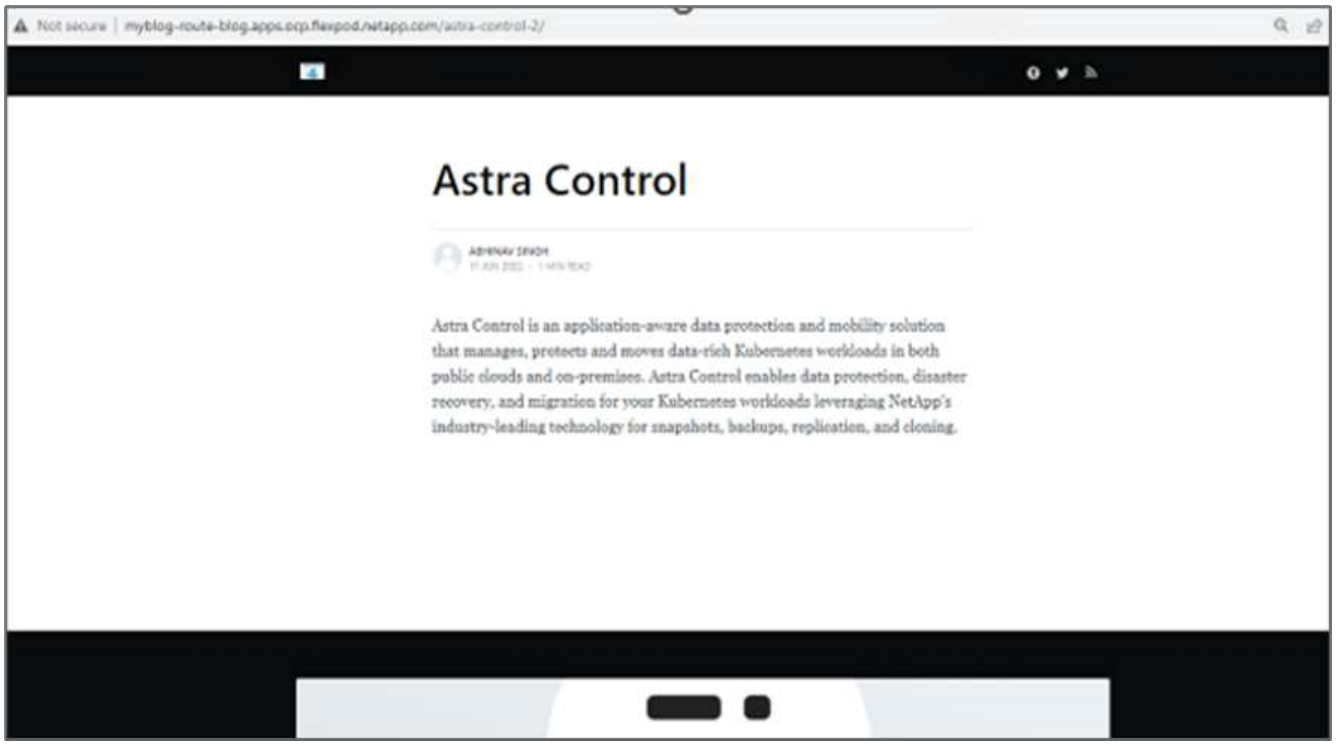
11. 앱 복원 프로세스가 즉시 시작됩니다.



12. 몇 분 후 사용 가능한 스냅샷에서 앱이 성공적으로 복구됩니다.



13. 웹 페이지를 사용할 수 있는지 확인하려면 URL을 새로 고치십시오.

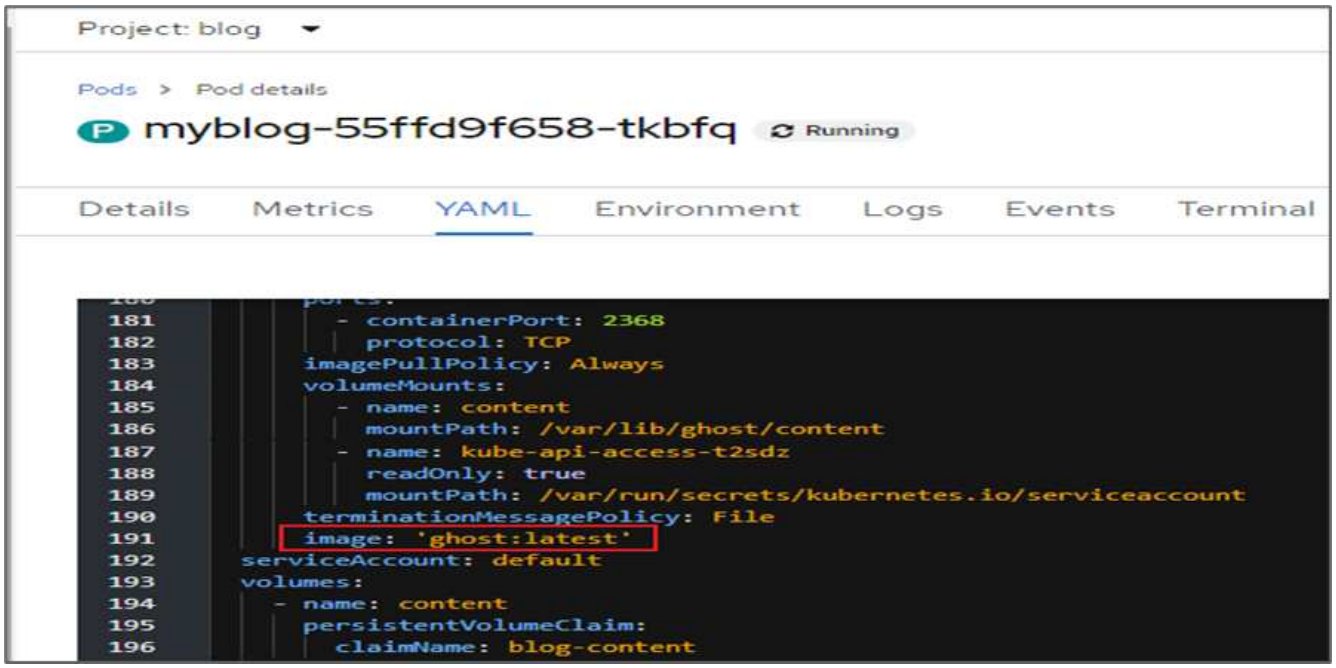


DevTest 팀은 Astra Control Center를 통해 스냅샷을 사용하여 블로그 사이트 앱 및 관련 데이터를 성공적으로 복구할 수 있습니다.

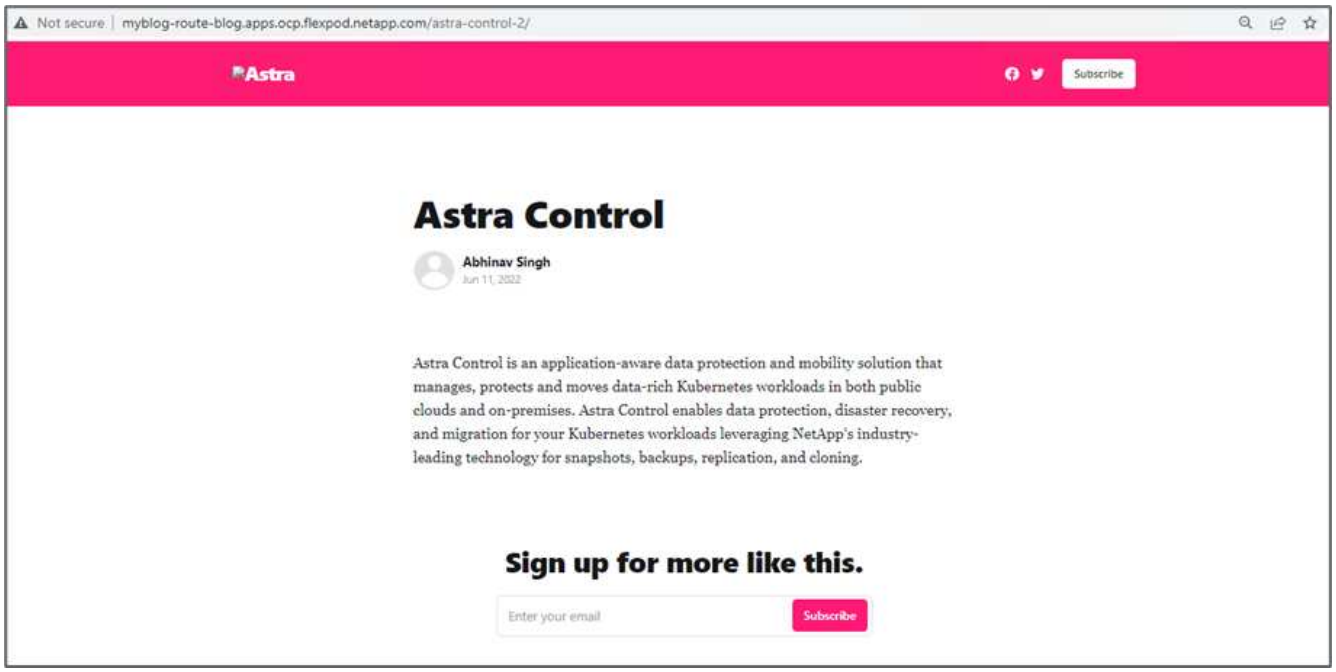
2부

Astra Control Center를 사용하면 클러스터 위치에 관계없이 온프레미스 또는 클라우드의 전체 애플리케이션과 함께 Kubernetes 클러스터 간에 데이터를 이동할 수 있습니다.

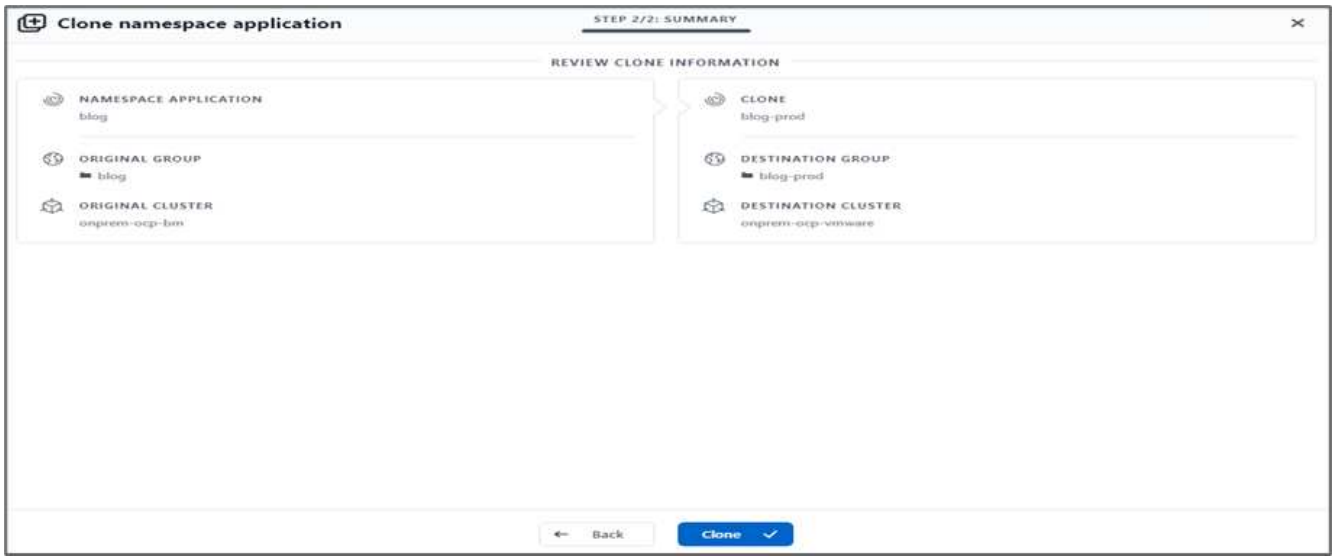
1. DevTest 팀은 처음에 앱을 지원되는 버전('Ghost-4.6-Alpine')으로 업그레이드한 후 최종 버전('Ghost-latest')으로 업그레이드하여 프로덕션을 준비합니다. 그런 다음 다른 FlexPod 시스템에서 실행되는 프로덕션 OpenShift 클러스터에 클론 복제된 앱을 업그레이드합니다.
2. 이때 앱이 최신 버전으로 업그레이드되어 운영 클러스터에 클론 복제할 준비가 됩니다.



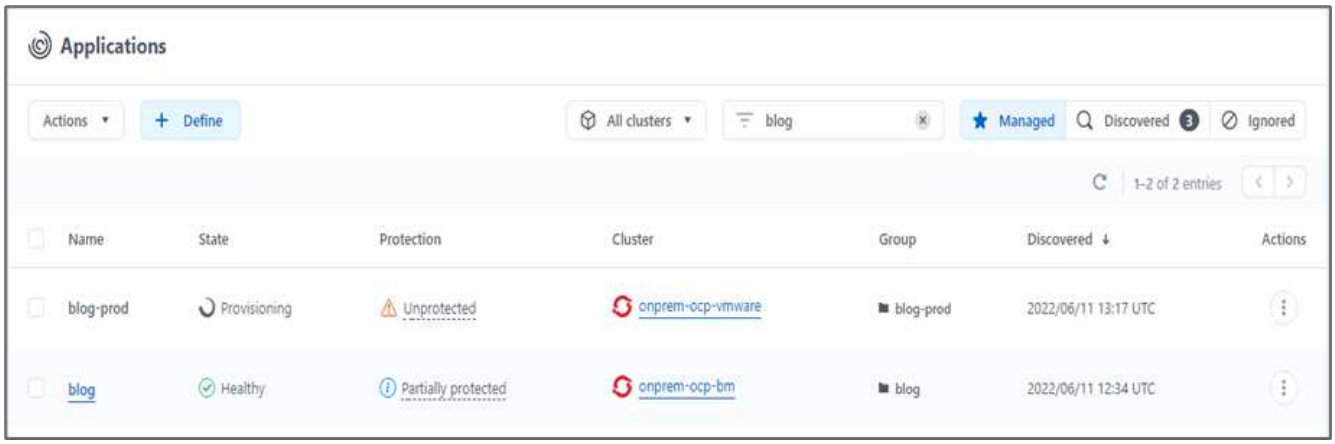
3. 새 테마를 확인하려면 블로그 사이트를 새로 고칩니다.



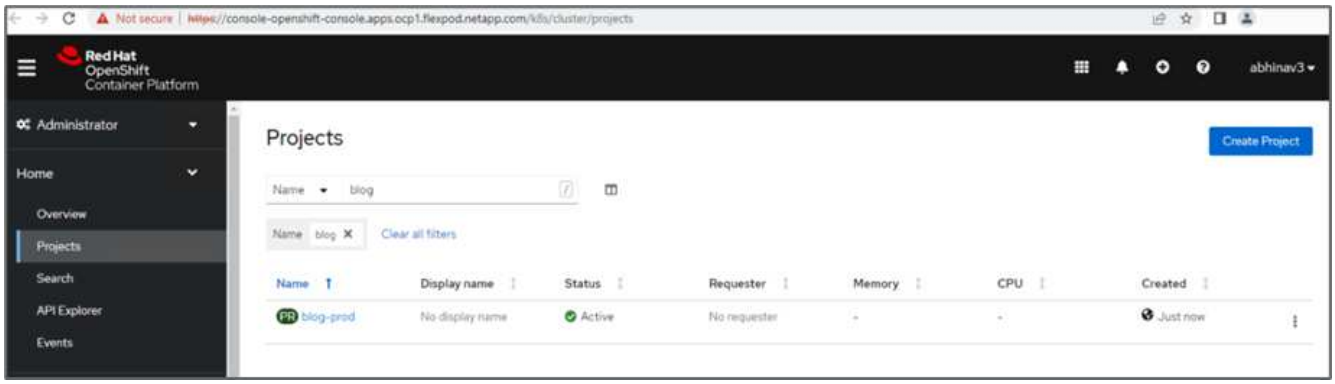
4. Astra Control Center에서 VMware vSphere에서 실행 중인 다른 운영 OpenShift 클러스터로 앱을 복제합니다.



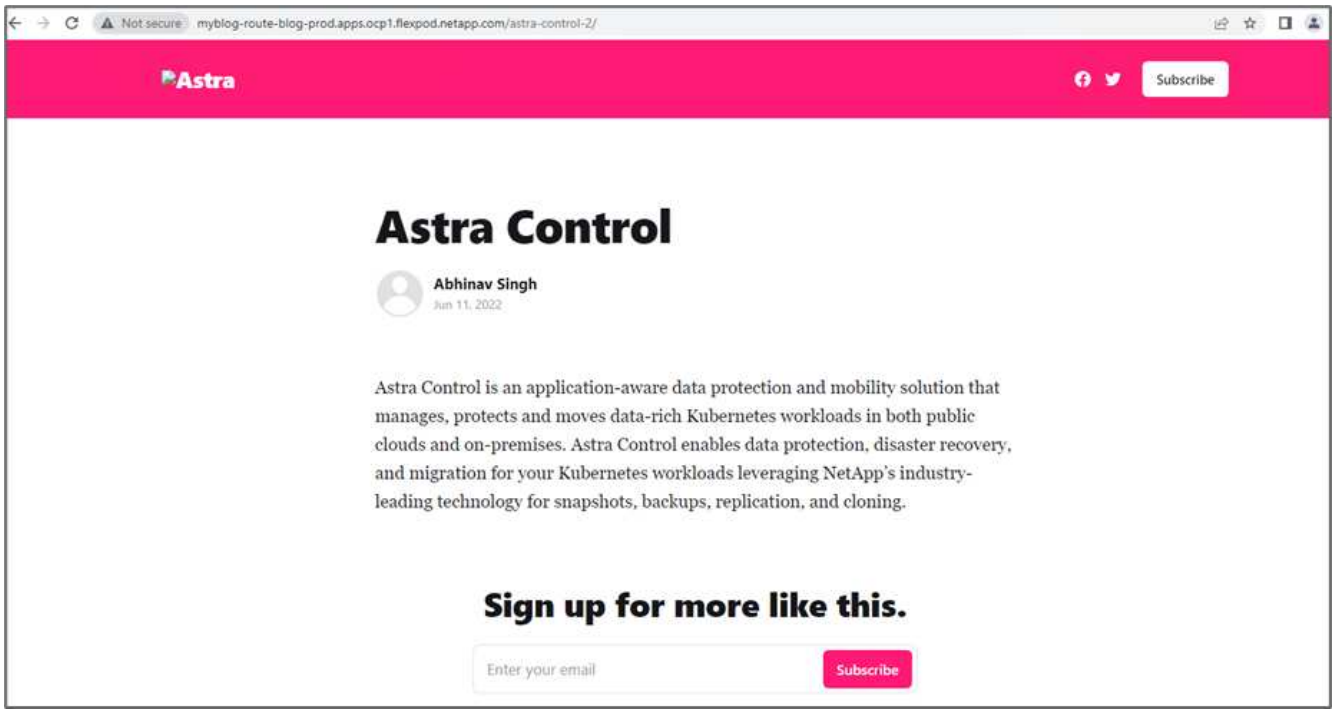
이제 운영 OpenShift 클러스터에서 새 애플리케이션 클론이 프로비저닝됩니다.



5. Production OpenShift 클러스터에 로그인하여 프로젝트 블로그를 검색합니다.



6. 측면 메뉴에서 네트워킹 > 경로를 선택하고 위치 아래에서 URL을 클릭합니다. 콘텐츠가 포함된 동일한 홈페이지가 표시됩니다.



이것으로 Astra Control Center 솔루션 검증을 마치겠습니다. 이제 Kubernetes 클러스터의 위치에 관계없이 전체 애플리케이션과 해당 데이터를 Kubernetes 클러스터 간에 복제할 수 있습니다.

"다음: 결론."

결론

"이전: 원격 백업을 사용한 애플리케이션 복구."

이 솔루션에서는 NetApp Astra 포트폴리오를 사용하여 FlexPod 및 AWS에서 실행되는 컨테이너식 애플리케이션에 대한 보호 계획을 구현했습니다. NetApp Astra Control Center 및 Astra Trident와 Cloud Volumes ONTAP, Red Hat OpenShift 및 FlexPod 인프라와 함께 이 솔루션의 핵심 구성요소를 구성했습니다.

NetApp은 스냅샷 캡처를 통해 애플리케이션 보호를 입증했으며 전체 복사본 백업을 실행하여 클라우드 및 사내 환경에서 실행되는 서로 다른 K8s 클러스터 간에 애플리케이션을 복원합니다.

또한, K8s 클러스터 전체에 애플리케이션을 클론 복제함으로써 고객이 원하는 위치에서 원하는 K8s 클러스터로 애플리케이션을 마이그레이션할 수 있도록 했습니다.

FlexPod은 고객이 애플리케이션 및 비즈니스 제공 프로세스를 현대화할 수 있도록 지속적으로 진화해 왔습니다. FlexPod 고객은 이 솔루션을 사용하여 임시 또는 전체 시간 DR 계획을 위한 위치로 퍼블릭 클라우드를 사용하는 클라우드 네이티브 애플리케이션에 대한 BCDR 계획을 자신 있게 구축하는 동시에 솔루션 비용을 절감할 수 있습니다.

Astra Control을 사용하면 클러스터의 위치에 관계없이 전체 애플리케이션과 함께 Kubernetes 클러스터 간에 데이터를 이동할 수 있습니다. 또한 클라우드 네이티브 애플리케이션을 더 빠르게 구축, 운영, 보호할 수 있습니다.

문제 해결

문제 해결 지침은 을 참조하십시오 "온라인 설명서".

추가 정보를 찾을 수 있는 위치

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

- FlexPod 홈 페이지

  "https://www.flexpod.com"

- FlexPod용 Cisco Validated Design 및 구축 가이드

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- Ansible을 사용하여 VMware용 코드로 인프라를 포함하는 FlexPod 구축

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html#AnsibleAutomationWorkflowandSolutionDeployment"

- Ansible을 사용한 Red Hat OpenShift 베어 메탈 의 코드로서 인프라를 포함하는 FlexPod 구축

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_iac_redhat_openshift.html"

- Cisco UCS 하드웨어 및 소프트웨어 상호 운용성 툴

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Cisco Intersight 데이터시트

  "https://intersight.com/help/saas/home"

- NetApp Astra 문서

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra Control Center를 참조하십시오

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra Trident

  "https://docs.netapp.com/us-en/trident/index.html"

- NetApp 클라우드 관리자

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- NetApp Cloud Volumes ONTAP를 참조하십시오

  "https://docs.netapp.com/us-en/occm/task_getting_started_aws.html"

- Red Hat OpenShift

  "https://www.openshift.com/"

- NetApp 상호 운용성 매트릭스 툴

  "http://support.netapp.com/matrix/"

버전 기록

버전	날짜	문서 버전 기록
버전 1.0	2022년 7월	ACC 22.04.0 해제

FlexPod용 NetApp Cloud Insights

TR-4868: FlexPod용 NetApp Cloud Insights

NetApp, Alan Cowles

파트너 후원: 

이 기술 보고서에 설명된 솔루션은 NetApp FlexPod 데이터 센터 솔루션의 일부로 구축되는 NetApp ONTAP를 실행하는 NetApp AFF A800 스토리지 시스템을 모니터링하는 NetApp Cloud Insights 서비스의 구성입니다.

고객 가치

이 솔루션에 대한 자세한 내용은 ONTAP를 운영 스토리지 시스템으로 구축하는 하이브리드 클라우드 환경을 위한 완벽한 기능을 갖춘 모니터링 솔루션에 관심이 있는 고객에게 제공하는 가치를 제공합니다. 여기에는 NetApp AFF 및 FAS 스토리지 시스템을 사용하는 FlexPod 환경이 포함됩니다.

사용 사례

이 솔루션은 다음과 같은 사용 사례에 적용됩니다.

- FlexPod 솔루션의 일부로 구축된 ONTAP 스토리지 시스템에서 다양한 리소스와 사용률을 모니터링하려는 조직
- AFF 또는 FAS 시스템을 통해 FlexPod 솔루션에서 발생하는 문제의 해결 시간을 단축하고 문제를 해결하려는 조직
- 비용 최적화 예상에 관심이 있는 조직(예: 낭비되는 리소스에 대한 자세한 정보와 FlexPod를 포함한 ONTAP 환경에서 비용 절감을 실현할 수 있는 맞춤형 대시보드 포함)

대상

이 솔루션의 대상 고객은 다음과 같은 그룹을 포함합니다.

- IT 경영진 및 비용 최적화 및 비즈니스 연속성 관련 담당자
- 데이터 센터 또는 하이브리드 클라우드 설계 및 관리에 관심이 있는 솔루션 설계자
- 문제 해결 및 인시던트 해결을 담당하는 기술 지원 엔지니어

계획, 문제 해결, 유지 관리 및 비즈니스 연속성 보장을 지원하는 데 사용할 수 있는 여러 가지 유용한 데이터 유형을 제공하도록 Cloud Insights를 구성할 수 있습니다. Cloud Insights로 FlexPod 데이터 센터 솔루션을 모니터링하고 집계된 데이터를 쉽게 파악할 수 있는 맞춤형 대시보드에 제공합니다. 구축 환경의 리소스를 수요 증가에 맞게 확장할 필요가 있는 시기를 예측할 수 있을 뿐만 아니라 시스템 내에서 문제를 일으키는 특정 애플리케이션 또는 스토리지 볼륨을 식별할 수도 있습니다. 이를 통해 모니터링 중인 인프라를 예측 가능하고 기대치에 따라 수행할 수 있으므로 조직에서 정의된 SLA를 이행하고 필요에 따라 인프라를 확장할 수 있으므로 낭비와 추가 비용이 발생하지 않습니다.

있습니다

이 섹션에서는 Cloud Insights에서 모니터링하는 NetApp AFF A800 시스템을 비롯하여 FlexPod 데이터 센터 통합 인프라의 아키텍처를 검토합니다.

솔루션 기술

FlexPod 데이터 센터 솔루션은 가용성과 확장성이 뛰어나고 검증 및 지원되는 통합 인프라 환경을 제공하기 위한 최소 구성 요소는 다음과 같습니다.

- NetApp ONTAP 스토리지 노드 2개(HA 쌍 1개)
- Cisco Nexus 데이터 센터 네트워크 스위치 2개
- Cisco MDS 패브릭 스위치 2개(FC 구축의 경우 선택 사항)
- 2개의 Cisco UCS 패브릭 인터커넥트
- 2개의 Cisco UCS B-Series 블레이드 서버가 포함된 Cisco UCS 블레이드 섀시 1개

또는

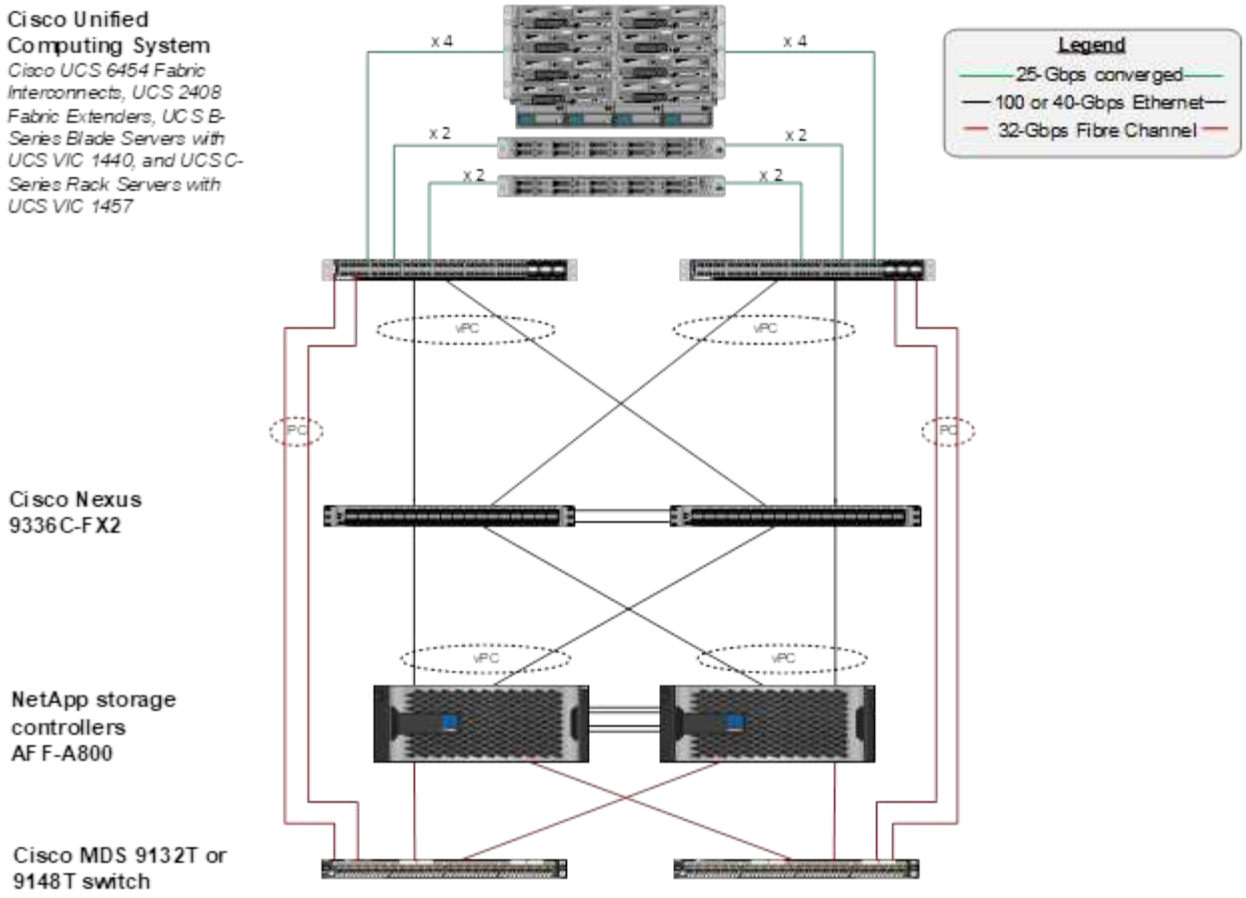
- 2개의 Cisco UCS C-Series 랙마운트 서버

Cloud Insights에서 데이터를 수집하려면 조직은 획득 장치를 FlexPod 데이터 센터 환경 내에서 또는 데이터를 수집하는 구성 요소에 연결할 수 있는 위치에 가상 또는 물리적 시스템으로 배포해야 합니다. 지원되는 여러 Windows 또는 Linux 운영 체제를 실행하는 시스템에 획득 장치 소프트웨어를 설치할 수 있습니다. 다음 표에는 이 소프트웨어의 솔루션 구성요소가 나와 있습니다.

운영 체제	버전
Microsoft Windows	10
Microsoft Windows Server를 참조하십시오	2012, 2012 R2, 2016, 2019년
Red Hat Enterprise Linux	7.2–7.6
CentOS	7.2–7.6
Oracle Enterprise Linux	7.5
데비안	9
우분투	18.04 LTS

아키텍처 다이어그램

다음 그림에서는 솔루션 아키텍처를 보여 줍니다.



하드웨어 요구 사항

다음 표에는 솔루션을 구현하는 데 필요한 하드웨어 구성요소가 나와 있습니다. 이 솔루션을 구체적으로 구축하는 데 사용되는 하드웨어 구성요소는 고객 요구사항에 따라 다를 수 있습니다.

하드웨어	수량
Cisco Nexus 9336C-FX2	2
Cisco UCS 6454 Fabric 상호 연결	2
Cisco UCS 5108 블레이드 섀시	1
Cisco UCS 2408 패브릭 익스텐더	2
Cisco UCS B200 M5 블레이드	2
NetApp AFF A800	2

소프트웨어 요구 사항

다음 표에는 솔루션을 구현하는 데 필요한 소프트웨어 구성요소가 나와 있습니다. 이 솔루션을 구체적으로 구축하는 데 사용되는 소프트웨어 구성요소는 고객 요구사항에 따라 다를 수 있습니다.

소프트웨어	버전
Cisco Nexus 펌웨어	9.3(5)
Cisco UCS 버전	4.1(2a)

소프트웨어	버전
NetApp ONTAP 버전	9.7
NetApp Cloud Insights 버전	2020년 9월, 기본
Red Hat Enterprise Linux	7.6
VMware vSphere를 참조하십시오	6.7U3

사용 사례 세부 정보

이 솔루션은 다음과 같은 사용 사례에 적용됩니다.

- 스토리지 시스템 위험 평가 및 스토리지 최적화를 위한 권장사항을 위해 NetApp Active IQ 디지털 자문업체에게 제공되는 데이터를 통한 환경 분석
- 시스템 통계를 실시간으로 검사하여 FlexPod 데이터 센터 솔루션에 구축된 ONTAP 스토리지 시스템의 문제 해결
- 맞춤형 대시보드를 생성하여 FlexPod 데이터 센터 통합 인프라에 구축된 ONTAP 스토리지 시스템의 특정 관심 지점을 쉽게 모니터링할 수 있습니다.

설계 고려 사항

FlexPod 데이터 센터 솔루션은 Cisco와 NetApp이 설계한 통합 인프라로, 엔터프라이즈 워크로드 실행을 위한 동적이고 가용성이 높으며 확장 가능한 데이터 센터 환경을 제공합니다. 솔루션의 컴퓨팅 및 네트워킹 리소스는 Cisco UCS 및 Nexus 제품에서 제공되며, 스토리지 리소스는 ONTAP 스토리지 시스템에서 제공됩니다. 업데이트된 하드웨어 모델 또는 소프트웨어 및 펌웨어 버전이 출시되면 솔루션 설계가 정기적으로 향상됩니다. 이러한 세부 정보는 솔루션 설계 및 구축에 대한 모범 사례와 함께 CVD(Cisco Validated Design) 또는 NVA(NetApp Verified Architecture) 문서에 수집되고 정기적으로 게시됩니다.

FlexPod 데이터 센터 솔루션 설계를 자세히 설명하는 최신 CVD 문서를 사용할 수 있습니다 "여기".

FlexPod for Cloud Insights 구축

솔루션을 배포하려면 다음 작업을 완료해야 합니다.

1. Cloud Insights 서비스에 가입합니다
2. 획득 유닛으로 구성할 VMware 가상 머신(VM)을 생성합니다
3. RHEL(Red Hat Enterprise Linux) 호스트를 설치합니다
4. Cloud Insights 포털에서 획득 장치 인스턴스를 생성하고 소프트웨어를 설치합니다
5. 모니터링되는 스토리지 시스템을 FlexPod 데이터 센터에서 Cloud Insights로 추가합니다.

NetApp Cloud Insights 서비스에 등록

NetApp Cloud Insights 서비스에 등록하려면 다음 단계를 완료하십시오.

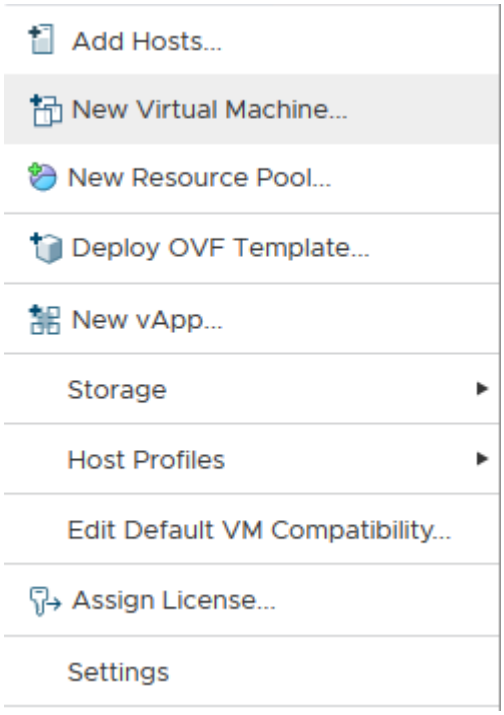
1. 로 이동합니다 "https://cloud.netapp.com/cloud-insights"
2. 화면 중앙에 있는 버튼을 클릭하여 14일 무료 평가판을 시작하거나 오른쪽 위에 있는 링크를 클릭하여 기존 NetApp

Cloud Central 계정에 로그인하거나 로그인할 수 있습니다.

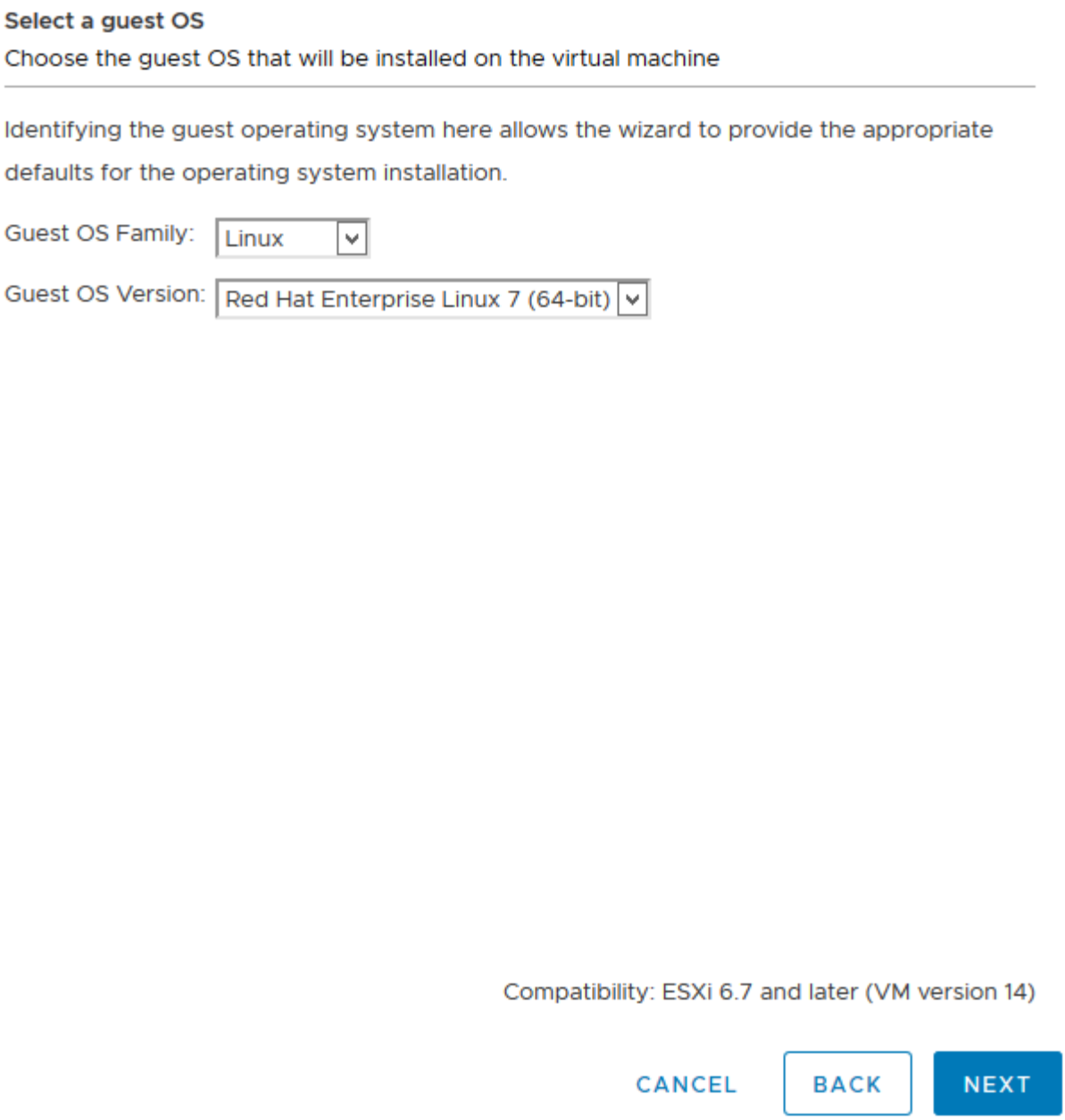
VMware 가상 시스템을 생성하여 수집 단위로 구성합니다

획득 장치로 구성할 VMware VM을 생성하려면 다음 단계를 수행하십시오.

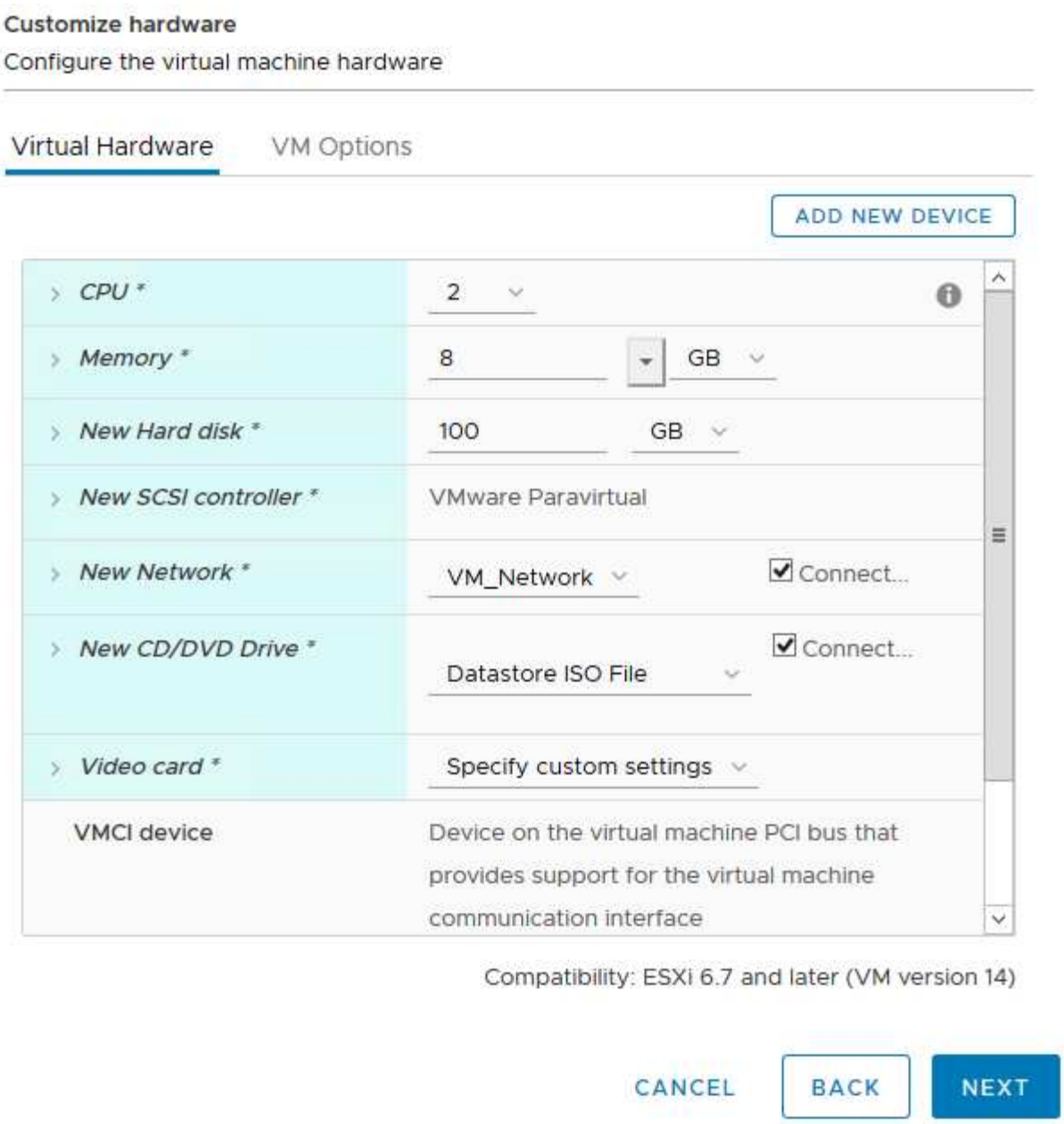
1. 웹 브라우저를 시작하고 VMware vSphere에 로그인하여 VM을 호스팅할 클러스터를 선택합니다.
2. 해당 클러스터를 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 Create a Virtual Machine을 선택합니다.



3. 새 가상 머신 마법사에서 다음 을 클릭합니다.
4. VM 이름을 지정하고 설치할 데이터 센터를 선택한 후 다음을 클릭합니다.
5. 다음 페이지에서 VM을 설치할 클러스터, 노드 또는 리소스 그룹을 선택하고 다음 을 클릭합니다.
6. VM을 호스팅하는 공유 데이터 저장소를 선택하고 Next를 클릭합니다.
7. VM의 호환성 모드가 'ESXi 6.7 이상'으로 설정되어 있는지 확인하고 Next를 클릭합니다.
8. 게스트 OS 제품군 Linux, 게스트 OS 버전: Red Hat Enterprise Linux 7(64비트) 을 선택합니다.



9. 다음 페이지에서는 VM의 하드웨어 리소스를 사용자 지정할 수 있습니다. Cloud Insights 획득 장치는 다음 리소스가 필요합니다. 리소스를 선택한 후 다음을 클릭합니다.
   a. CPU 2개
   b. 8GB RAM
   c. 100GB의 하드 디스크 공간
   d. 포트 443에서 SSL 연결을 통해 FlexPod 데이터 센터 및 Cloud Insights 서버의 리소스에 연결할 수 있는 네트워크.
   e. 부팅하기 위해 선택한 Linux 배포(Red Hat Enterprise Linux)의 ISO 이미지.

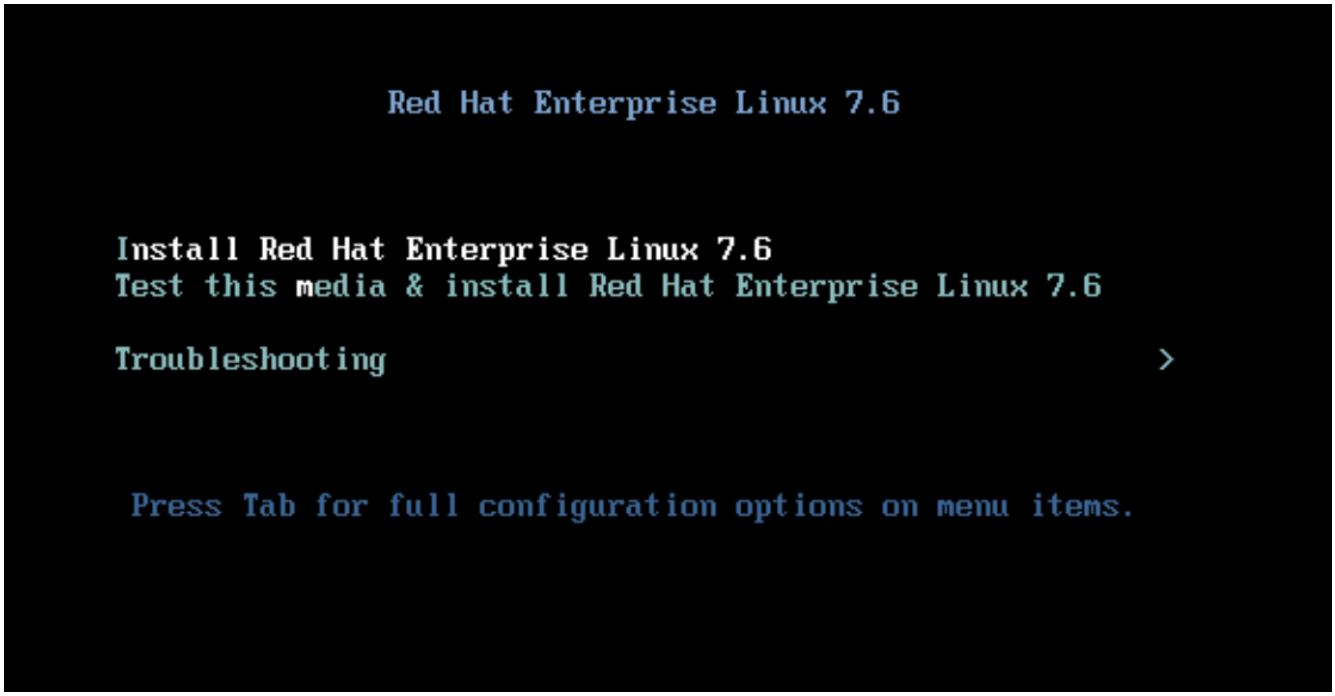


10. VM을 생성하려면 Ready to Complete 페이지에서 설정을 검토하고 Finish를 클릭합니다.

Red Hat Enterprise Linux를 설치합니다

Red Hat Enterprise Linux를 설치하려면 다음 단계를 수행하십시오.

1. VM의 전원을 켜고 창을 클릭하여 가상 콘솔을 시작한 다음 Red Hat Enterprise Linux 7.6 설치 옵션을 선택합니다.



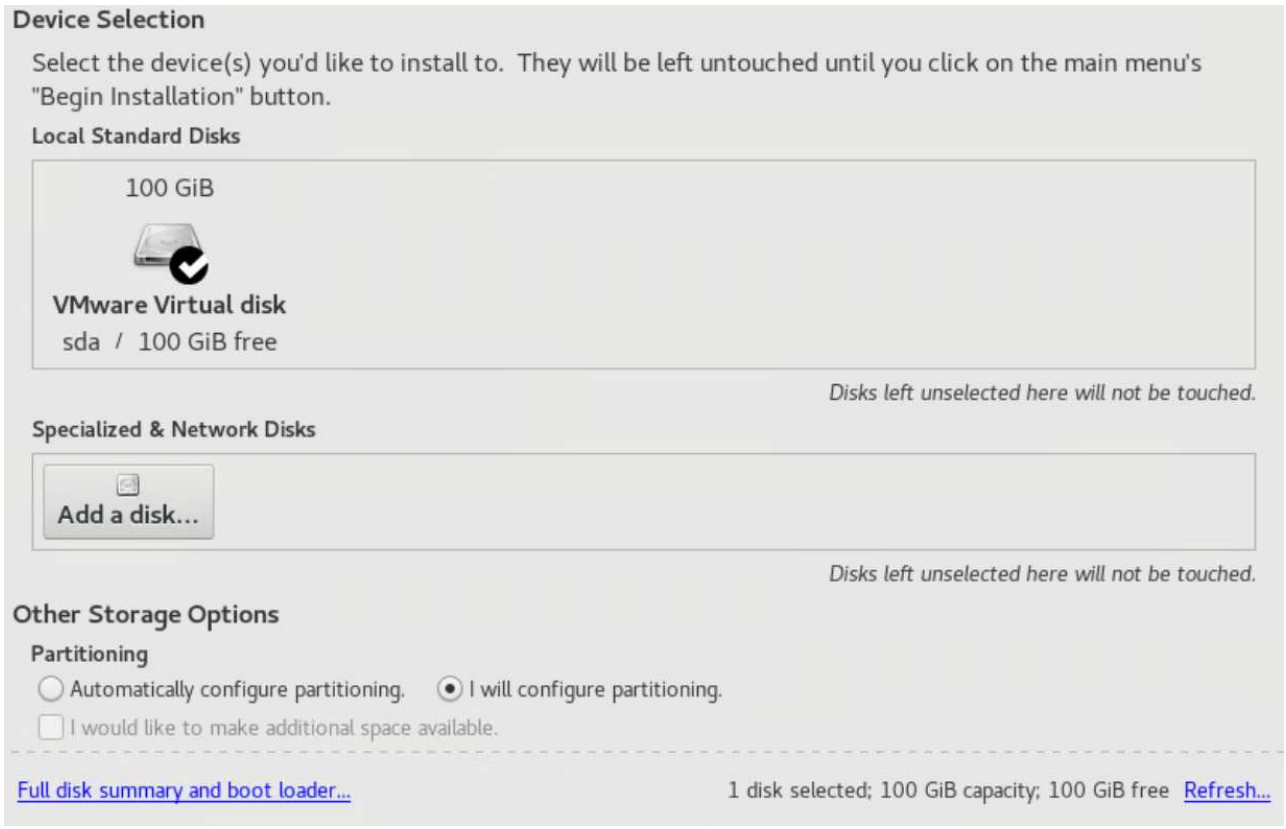
2. 원하는 언어를 선택하고 계속 을 클릭합니다.

   다음 페이지는 설치 요약입니다. 이러한 옵션의 대부분에 대해 기본 설정을 사용할 수 있어야 합니다.

3. 다음 옵션을 수행하여 스토리지 레이아웃을 사용자 지정해야 합니다.

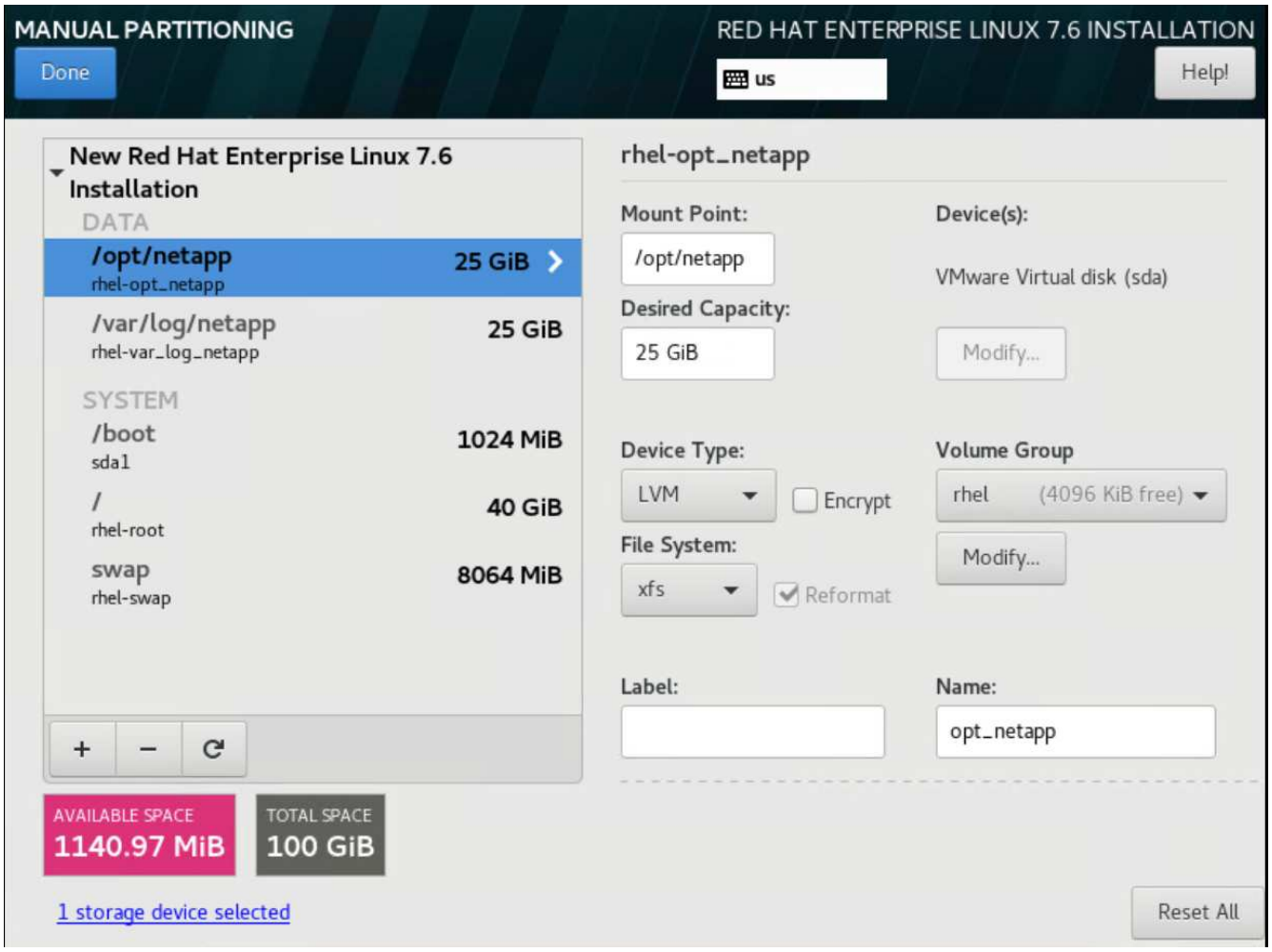
   a. 서버의 파티션을 사용자 지정하려면 설치 대상을 클릭합니다.

   b. VMware 가상 디스크 100GiB가 검은색 확인 표시로 선택되었는지 확인하고 I'I'I'I'I'I'DIT Configure Partitioning 라디오 버튼을 선택합니다.



c. 완료 를 클릭합니다.

파티션 테이블을 사용자 정의할 수 있는 새 메뉴가 표시됩니다. 각각 25GB를 '/opt/netapp' 및 '/var/log/netapp'에 지정합니다. 나머지 스토리지를 시스템에 자동으로 할당할 수 있습니다.

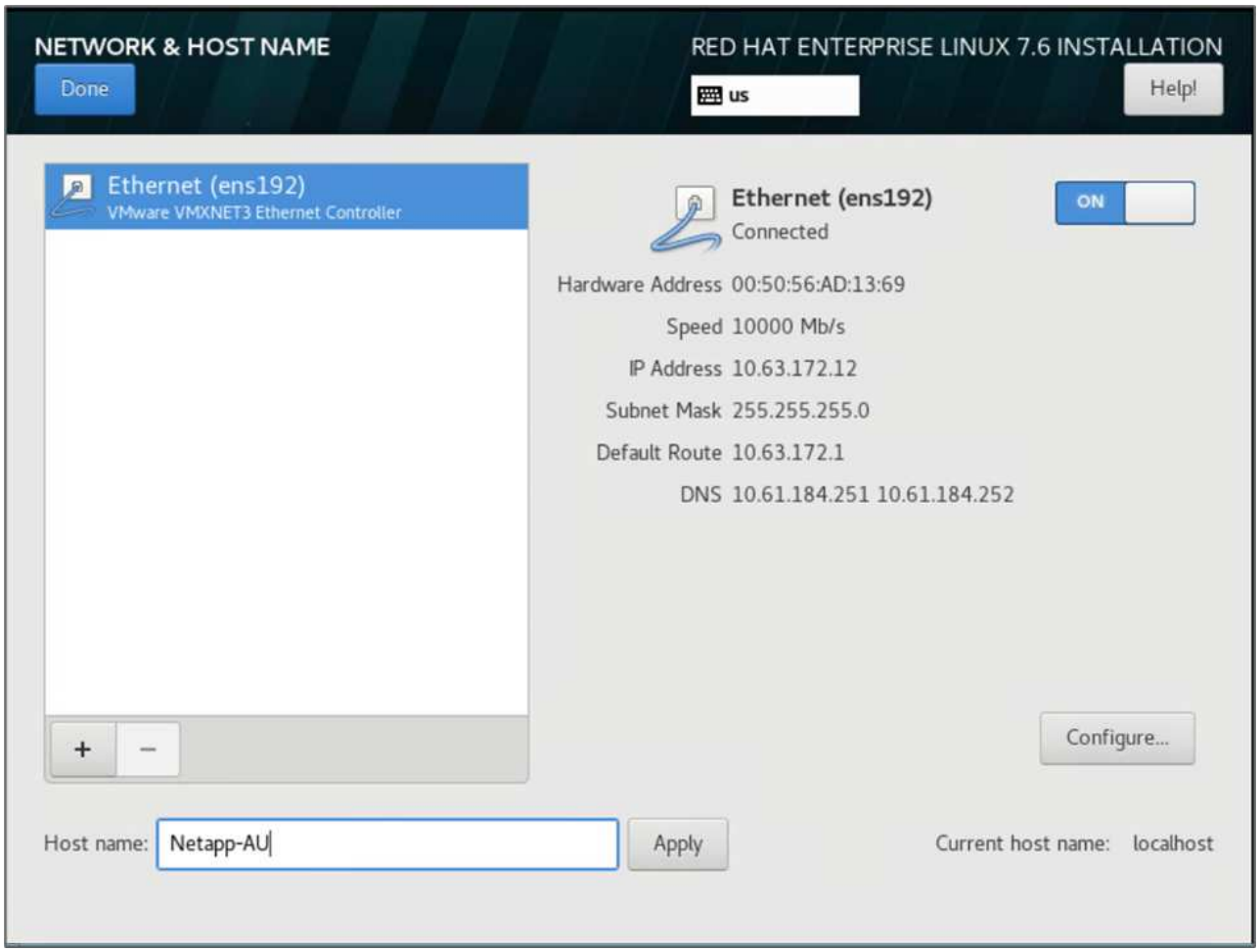


a. 설치 요약으로 돌아가려면 완료를 클릭합니다.

4. 네트워크 및 호스트 이름을 클릭합니다.

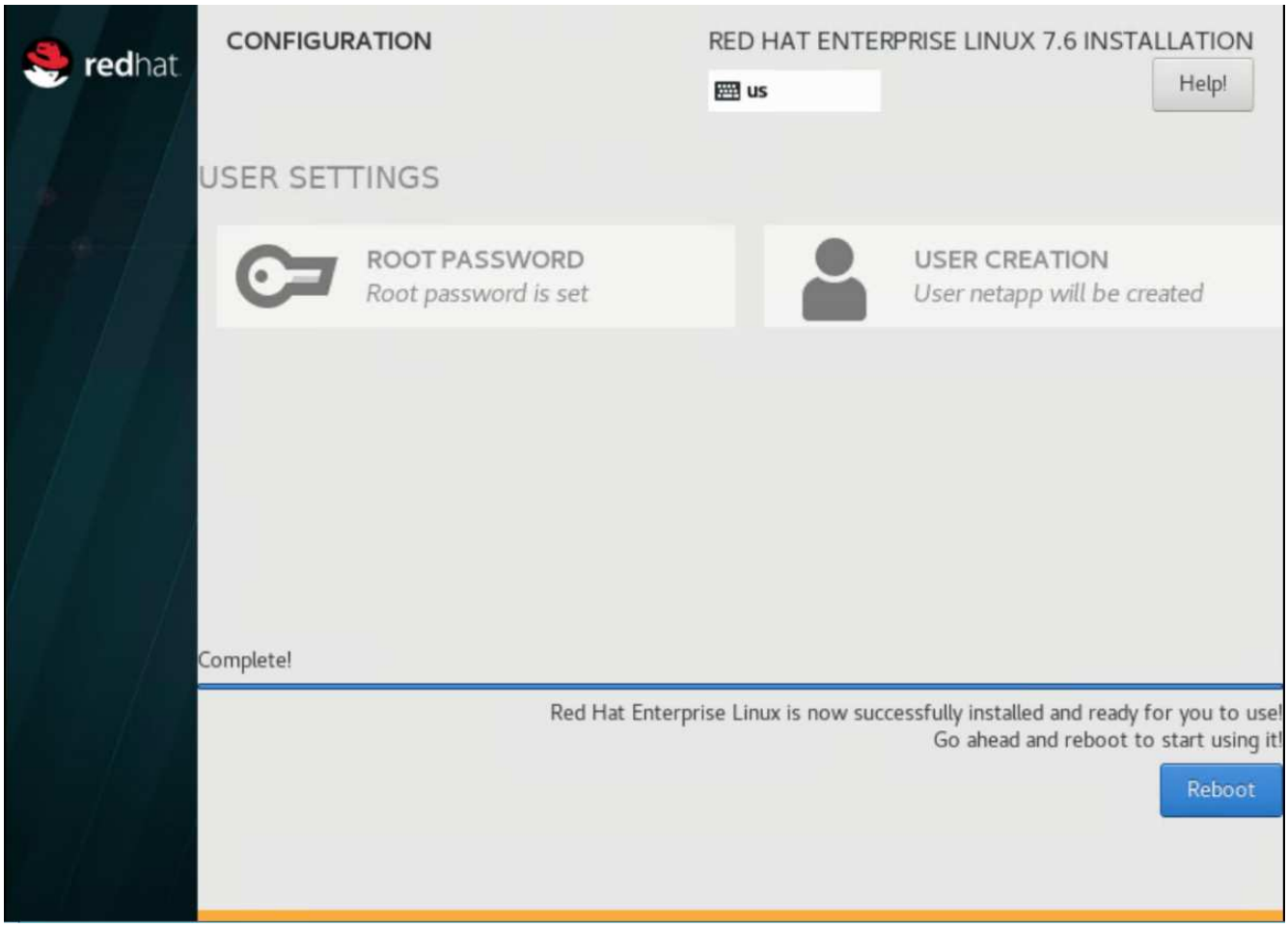
a. 서버의 호스트 이름을 입력합니다.

b. 슬라이더 단추를 클릭하여 네트워크 어댑터를 켭니다. 네트워크에 DHCP(Dynamic Host Configuration Protocol)가 구성되어 있으면 IP 주소를 받게 됩니다. 그렇지 않은 경우 구성을 클릭하고 주소를 수동으로 할당합니다.



c. . 완료 를 클릭하여 설치 요약으로 돌아갑니다.

5. 설치 요약 페이지에서 설치 시작을 클릭합니다.
6. 설치 진행률 페이지에서 루트 암호를 설정하거나 로컬 사용자 계정을 만들 수 있습니다. 설치가 완료되면 재부팅 을 클릭하여 서버를 다시 시작합니다.



7. 시스템이 재부팅된 후 서버에 로그인하여 Red Hat 서브스크립션 관리자에 등록하십시오.

```
[root@Netapp-AU ~]# subscription-manager register
Registering to: subscription.rhsm.redhat.com:443/subscription
Username: alan.cowles@netapp.com
Password:
The system has been registered with ID: a47f2e7b-81cd-4757-85c7-eb1818c2c2a1
The registered system name is: Netapp-AU
[root@Netapp-AU ~]#
```

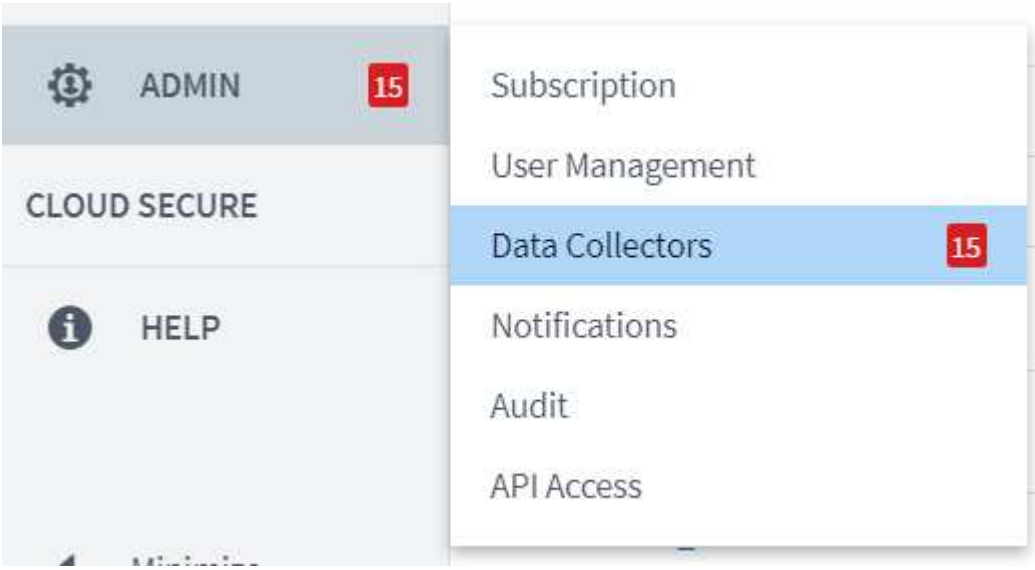
8. Red Hat Enterprise Linux에 사용 가능한 서브스크립션을 첨부하십시오.

```
[root@Netapp-AU ~]# subscription-manager attach --pool=8a85f99b710f3b1901713b90b9e154cf
Successfully attached a subscription for: Red Hat Enterprise Linux, Standard Support (128 Sockets, NFR, Partner Only)
[root@Netapp-AU ~]#
```

Cloud Insights 포털에서 획득 장치 인스턴스를 생성하고 소프트웨어를 설치합니다

Cloud Insights 포털에서 획득 장치 인스턴스를 만들고 소프트웨어를 설치하려면 다음 단계를 수행하십시오.

1. Cloud Insights의 홈 페이지에서 왼쪽 메인 메뉴의 관리자 항목 위로 마우스를 가져가 메뉴에서 데이터 수집기 를 선택합니다.



2. Data Collector 페이지의 상단 중앙에서 획득 장치 링크를 클릭합니다.

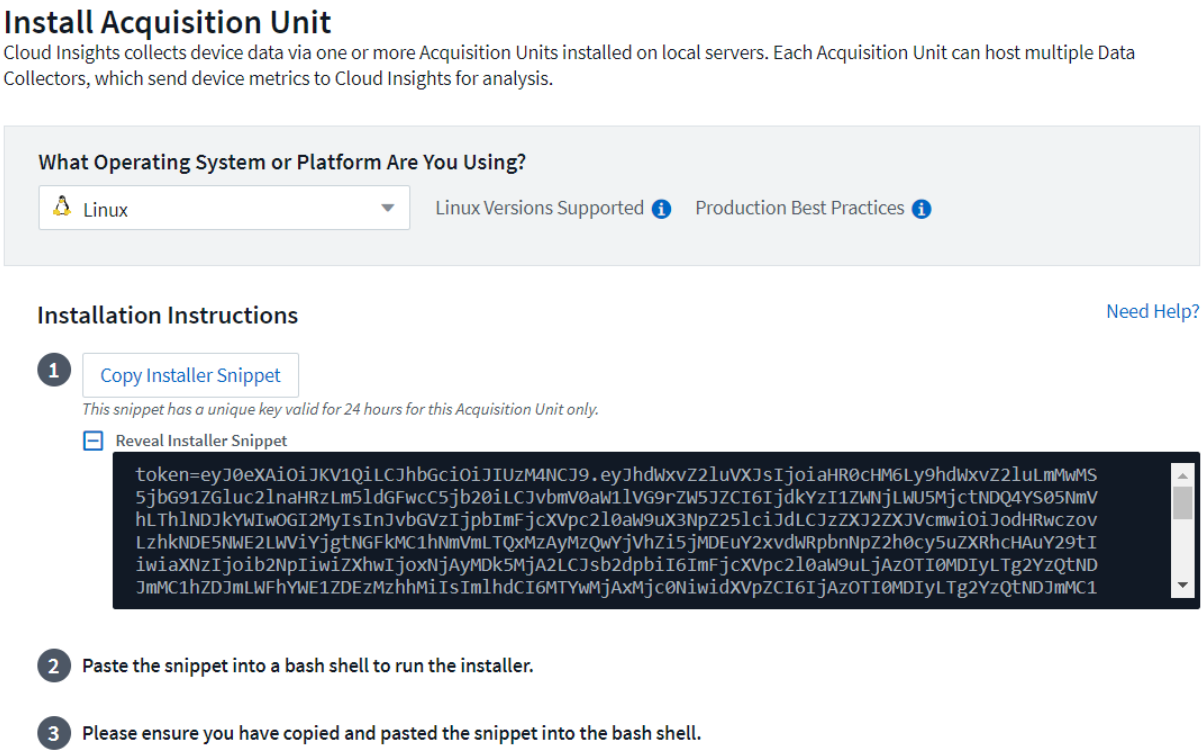


3. 새 획득 장치를 생성하려면 오른쪽에 있는 버튼을 클릭합니다.



4. 획득 장치를 호스팅하는 데 사용할 운영 체제를 선택하고 웹 페이지에서 설치 스크립트를 복사하는 단계를 따릅니다.

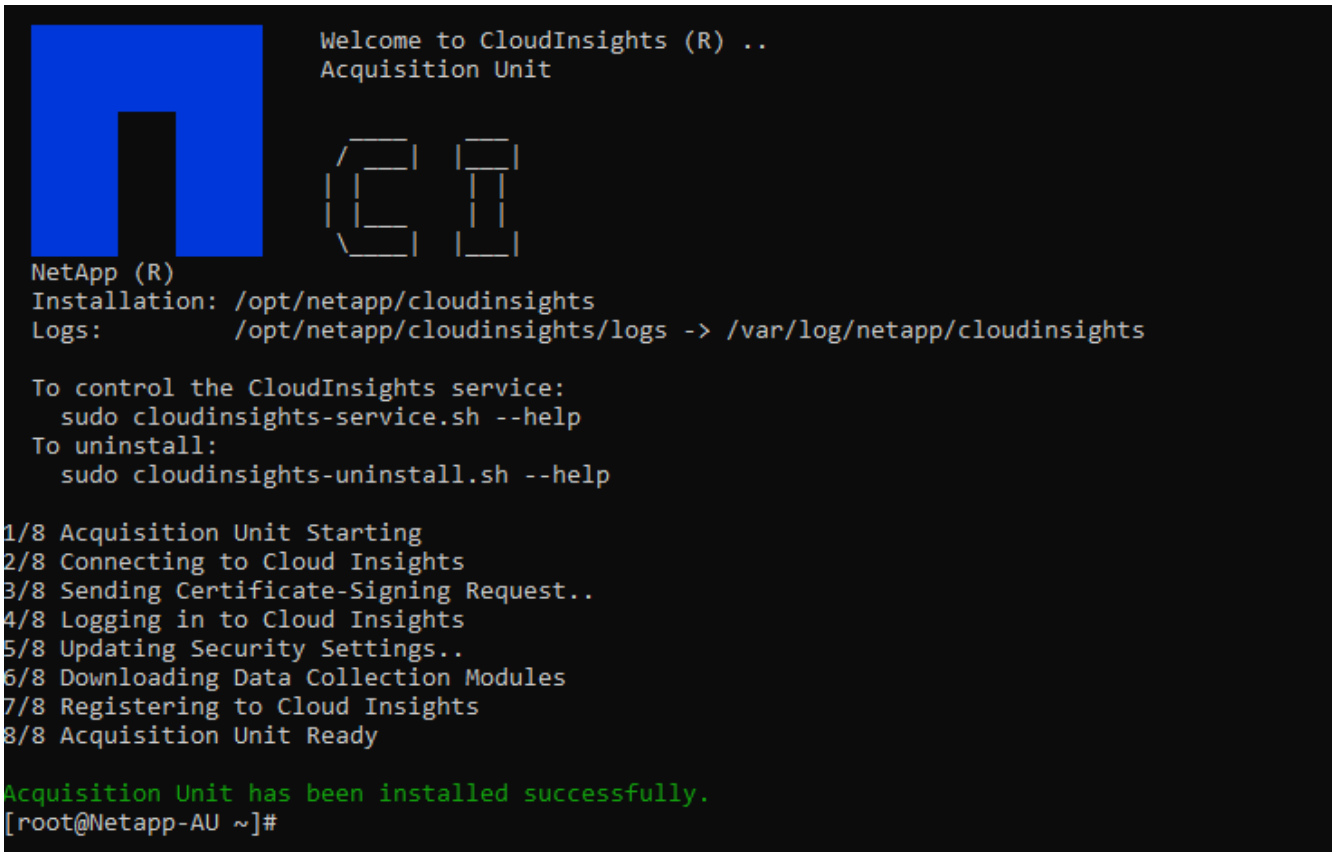
   이 예에서는 Linux 서버로서, 호스트의 CLI에 붙여넣을 코드 조각과 토큰을 제공합니다. 웹 페이지는 획득 장치가 연결될 때까지 대기합니다.



5. 프로비저닝된 Red Hat Enterprise Linux 시스템의 CLI에 스니펫을 붙여 넣고 Enter 를 클릭합니다.

```
[root@Netapp-AU ~]# token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9.eyJhdWxvZ2luVXJsIjoiaHR0cHM6Ly9hdWxvZ2luLmMwMS5jbG91ZGluc
2lnaHRzLm5ldGFwcC5jb20iLCJvbmV0aW1lVG9rZW5JZCI6IjQ5ZTY0MGM5LTY5MTItNDQ4Yi04YmI4LTIwNGY2OTQ2YzY1YSIsInJvbGVzIjpbImFjcXVpc
2l0aW9uX3NpZ25lciJdLCJzZXJ2ZXJVcmwiOiJodHRwczovLzhkNDE5NWE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZi5jMDEuY2xvdWRpbnNpZ2h0c
y5uZXRhcHAuY29tIiwiaXNzIjoib2NpIiwiZXhwIjoxNjAyMTgyNzg2LCJsb2dpbiI6ImFjcXVpc2l0aW9uLjc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZ
TcxZjk0ODRiZCIsImlhdCI6MTYwMjA5NjMyNiwidXVpZCI6Ijc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZTcxZjk0ODRiZCIsInRlbmFudCI6IjhkNDE5N
WE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZiIsInRlbmFudFN1YmRvbWFpbiI6InBzMTMyNSJ9.RvWLR3wH1_k6fIOCiO_h-Wok2STfFPDj7VksmXqw
-GZ-JqSIe8SZE4Sv3DuWrWM6 domainUrl=https://8d4195a6-ebb8-4ad0-a6ef-41302340b5af.c01.cloudinsights.netapp.com/rest/v1/au
version=1.253.0 bootstrap=cloudinsights-au-install-bootstrap.sh && curl $proxy_auth_scheme -H "Authorization: Bearer $to
ken" -o $bootstrap $domainUrl/installerBootstrap && sudo chmod 755 $bootstrap && sudo /bin/bash -c "TOKEN=$token HTTPS_P
ROXY=$https_proxy PROXY_AUTH_SCHEME=$proxy_auth_scheme AU_VERSION=$version INSTALLER_NAME=cloudinsights-linux-au-install
er-$version INSTALLER_URL=$domainUrl/installers/linux/$version ./$bootstrap"
```

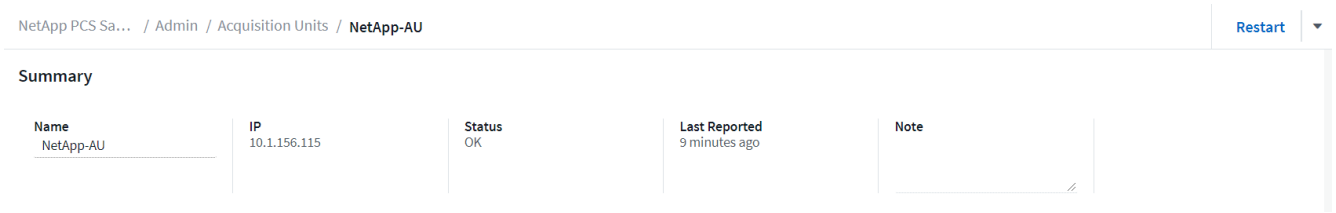
설치 프로그램이 압축된 패키지를 다운로드하고 설치를 시작합니다. 설치가 완료되면 획득 장치가 NetApp Cloud Insights에 등록되었다는 메시지가 표시됩니다.



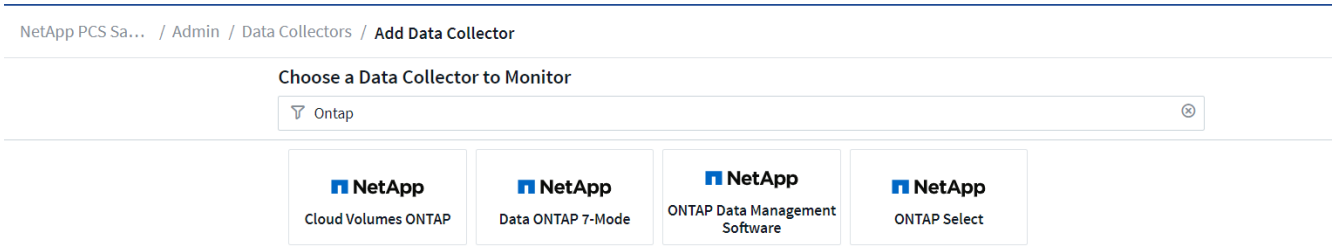
모니터링되는 스토리지 시스템을 **FlexPod** 데이터 센터에서 **Cloud Insights**로 추가합니다

FlexPod 구축 환경에서 ONTAP 스토리지 시스템을 추가하려면 다음 단계를 수행하십시오.

1. Cloud Insights 포털의 획득 장치 페이지로 돌아가서 새로 등록된 장치를 찾습니다. 장치 요약을 표시하려면 단위를 클릭합니다.

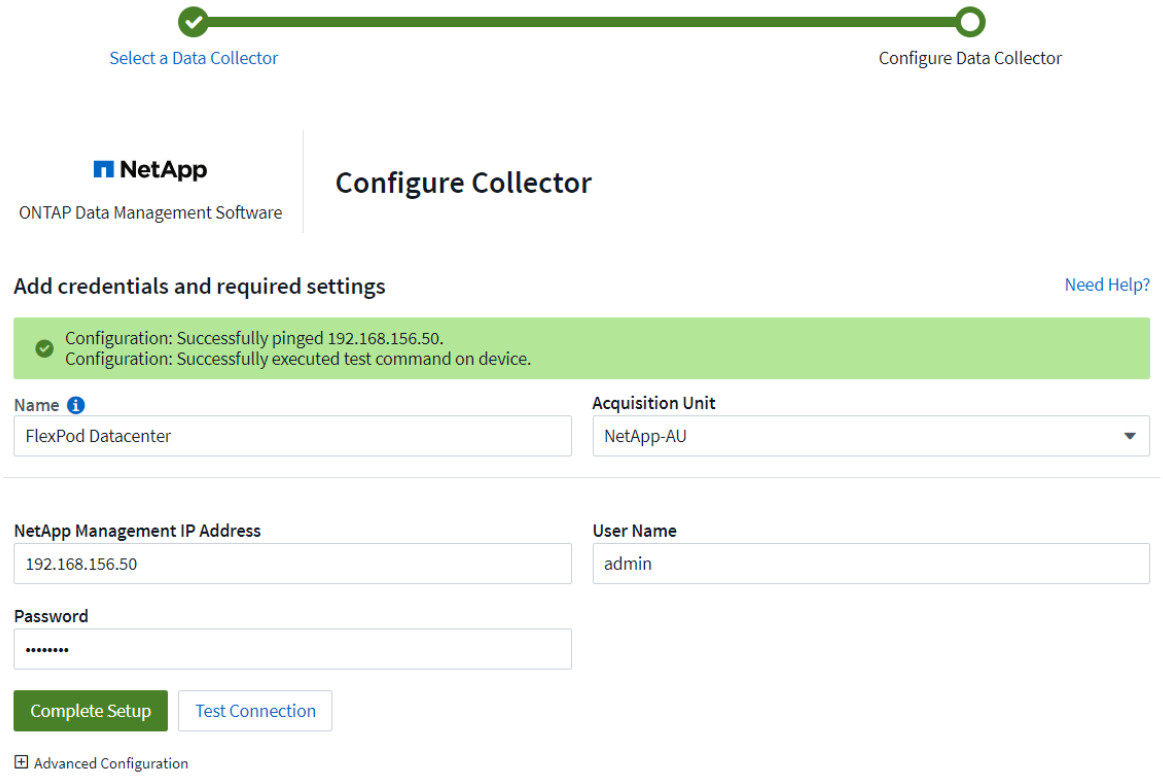


2. 스토리지 시스템을 추가하는 마법사를 시작하려면 요약 페이지에서 데이터 수집기 생성을 위한 버튼을 클릭합니다. 첫 번째 페이지에는 데이터를 수집할 수 있는 모든 시스템이 표시됩니다. 검색 표시줄을 사용하여 ONTAP를 검색합니다.



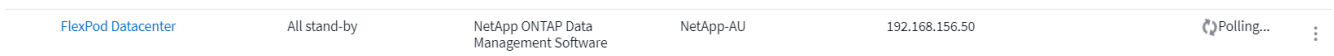
3. ONTAP 데이터 관리 소프트웨어를 선택합니다.

   배포 이름을 지정하고 사용할 획득 장치를 선택할 수 있는 페이지가 표시됩니다. ONTAP 시스템에 대한 연결 정보 및 자격 증명을 제공하고 연결을 테스트하여 확인할 수 있습니다.



4. 설정 완료 를 클릭합니다.

   포털은 데이터 수집기 페이지로 돌아가고 데이터 수집기는 첫 번째 폴링을 시작하여 FlexPod 데이터 센터에 있는 ONTAP 스토리지 시스템에서 데이터를 수집합니다.



사용 사례

Cloud Insights 데이터 센터 솔루션을 모니터링할 수 있도록 FlexPod가 설정 및 구성되어

있으므로 대시보드에서 수행할 수 있는 몇 가지 작업을 탐색하여 환경을 평가하고 모니터링할 수 있습니다. 이 섹션에서는 Cloud Insights의 5가지 주요 사용 사례를 중점적으로 살펴보겠습니다.

- Active IQ 통합
- 실시간 대시보드 탐색
- 사용자 지정 대시보드 만들기
- 고급 문제 해결
- 스토리지 최적화

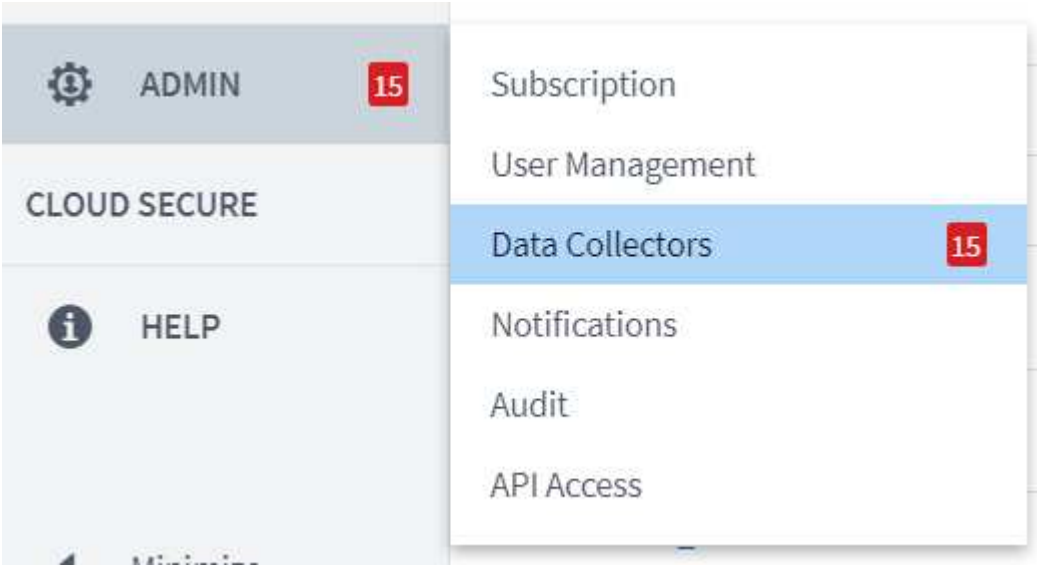
Active IQ 통합

Cloud Insights는 Active IQ 스토리지 모니터링 플랫폼에 완전히 통합되어 있습니다. FlexPod 데이터 센터 솔루션의 일부로 구축된 ONTAP 시스템은 각 시스템에 내장된 AutoSupport 기능을 통해 정보를 NetApp으로 다시 전송하도록 자동으로 구성됩니다. 이러한 보고서는 예약된 일정에 따라 생성되거나 시스템에서 장애가 감지될 때마다 동적으로 생성됩니다. AutoSupport를 통해 전달되는 데이터는 집계되어 Cloud Insights의 Active IQ 메뉴 아래에 쉽게 액세스할 수 있는 대시보드에 표시됩니다.

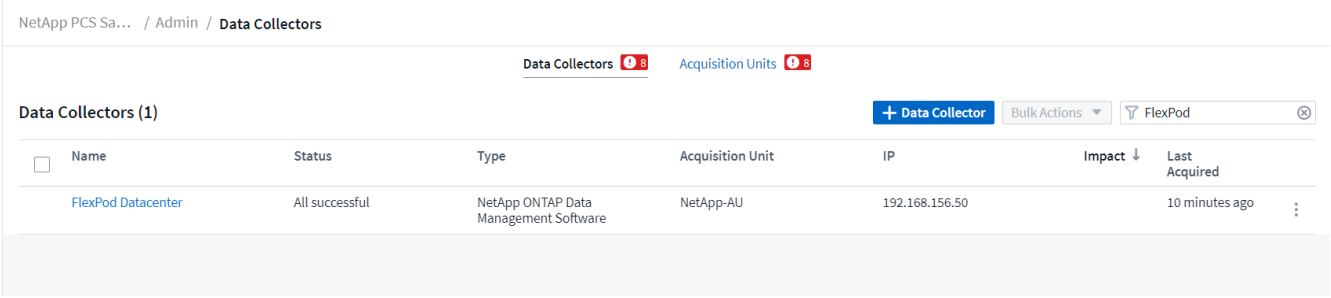
Cloud Insights 대시보드를 통해 Active IQ 정보에 액세스합니다

Cloud Insights 대시보드를 통해 Active IQ 정보에 액세스하려면 다음 단계를 완료하십시오.

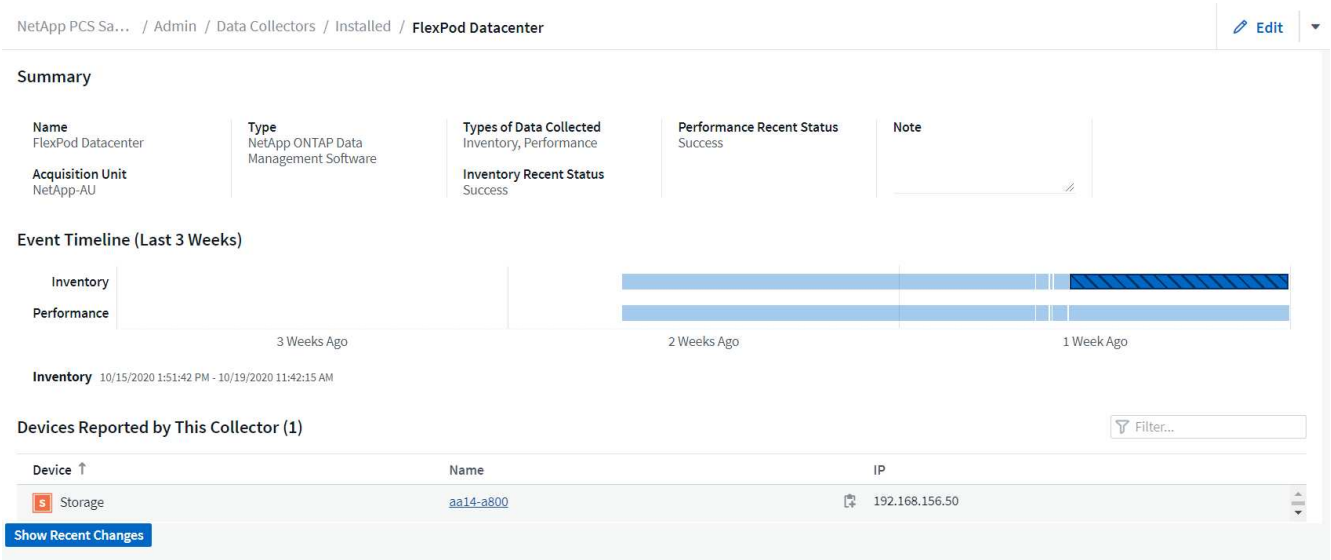
1. 왼쪽에 있는 관리 메뉴에서 Data Collector 옵션을 클릭합니다.



2. 사용자 환경의 특정 Data Collector에 대한 필터입니다. 이 예제에서는 FlexPod라는 용어를 기준으로 필터링합니다.

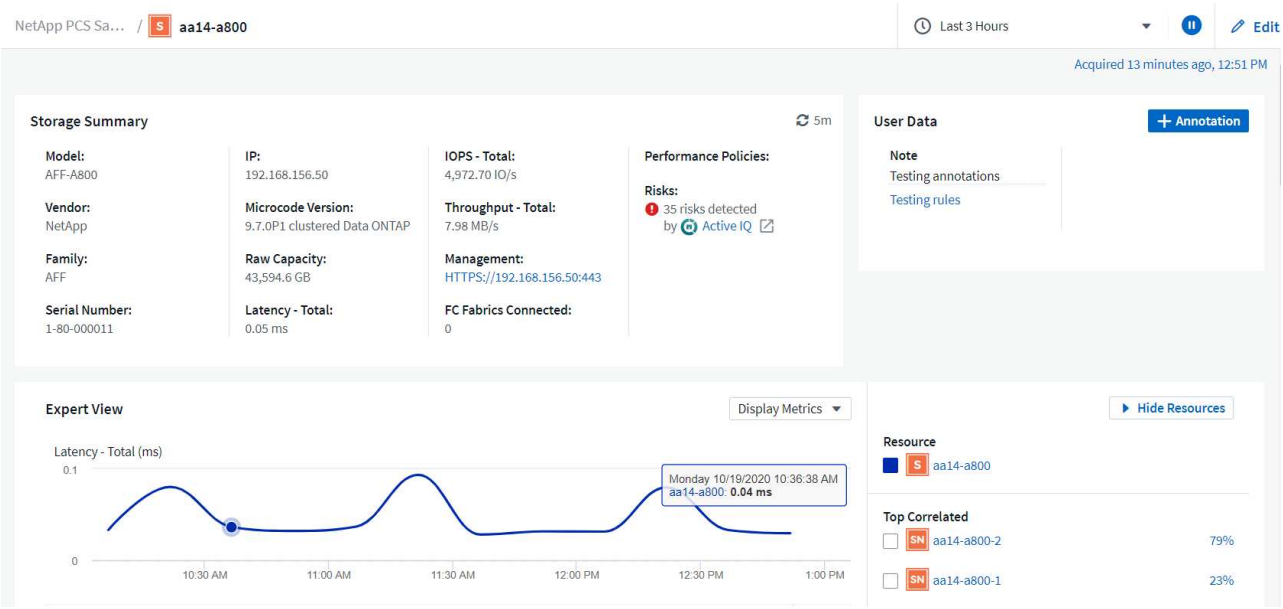


3. Data Collector를 클릭하여 해당 Collector에서 모니터링하는 환경 및 장치에 대한 요약을 가져옵니다.

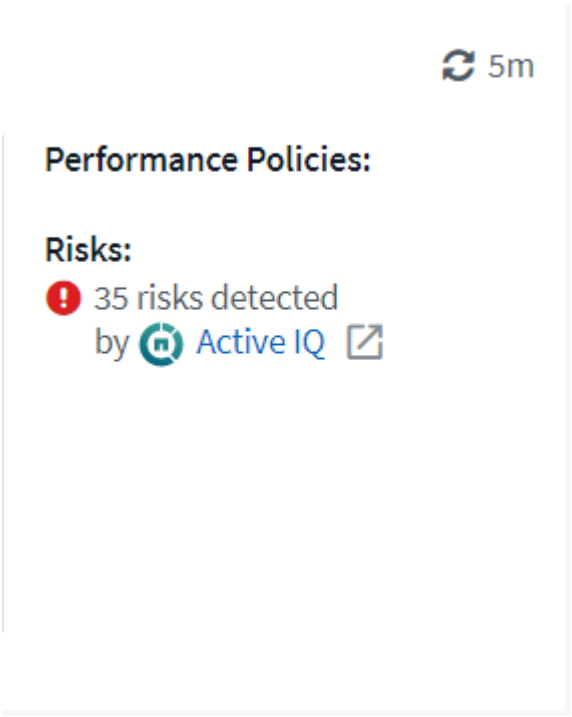


아래쪽 장치 목록에서 모니터링할 ONTAP 스토리지 시스템의 이름을 클릭합니다. 다음과 같은 세부 정보를 포함하여 시스템에 대해 수집된 정보의 대시보드가 표시됩니다.

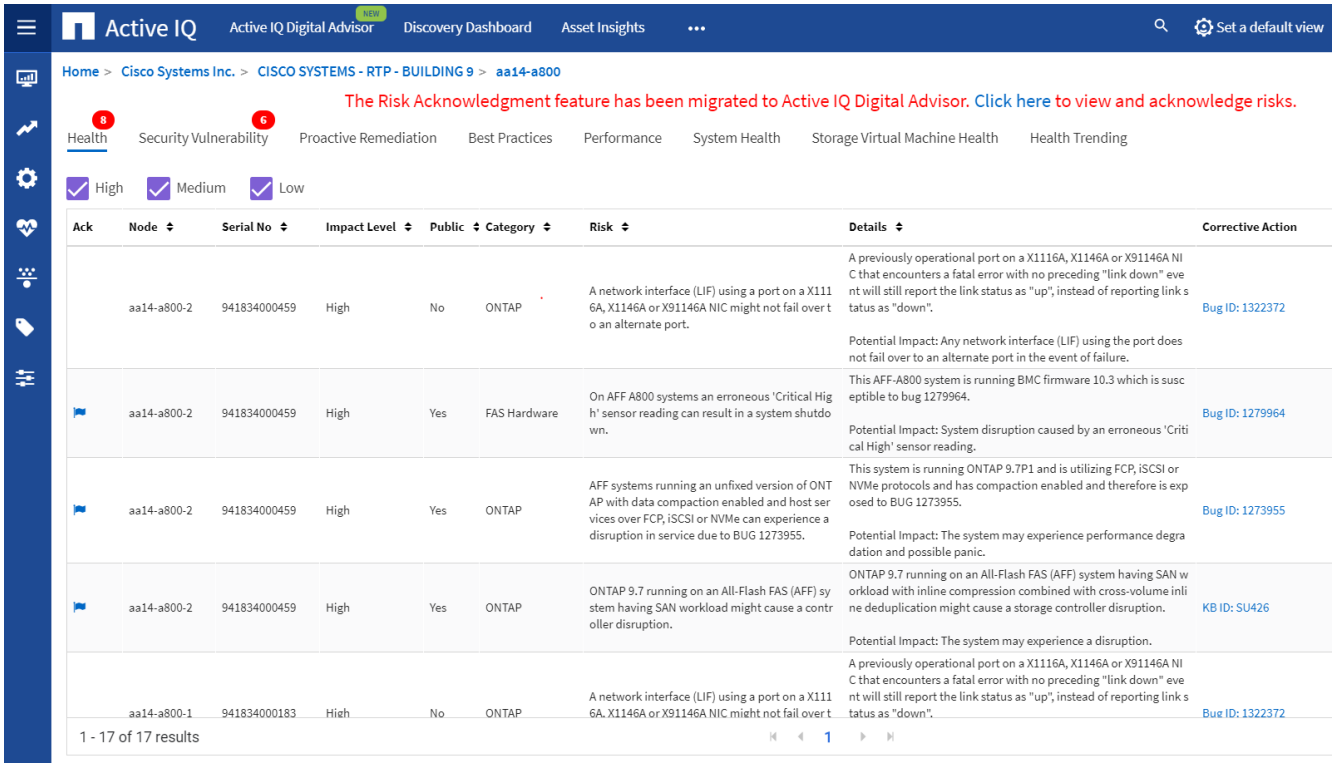
- 모델
- 가족
- ONTAP 버전
- 물리적 용량
- 평균 IOPS
- 평균 지연 시간
- 평균 처리량



또한 이 페이지의 성능 정책 섹션에서 NetApp Active IQ에 대한 링크를 찾을 수 있습니다.



4. 새 브라우저 탭을 열고 영향을 받는 노드, 위험의 중요도와 식별된 문제를 해결하기 위해 취해야 할 적절한 조치가 표시된 위험 완화 페이지로 이동하려면 Active IQ 링크를 클릭하십시오.

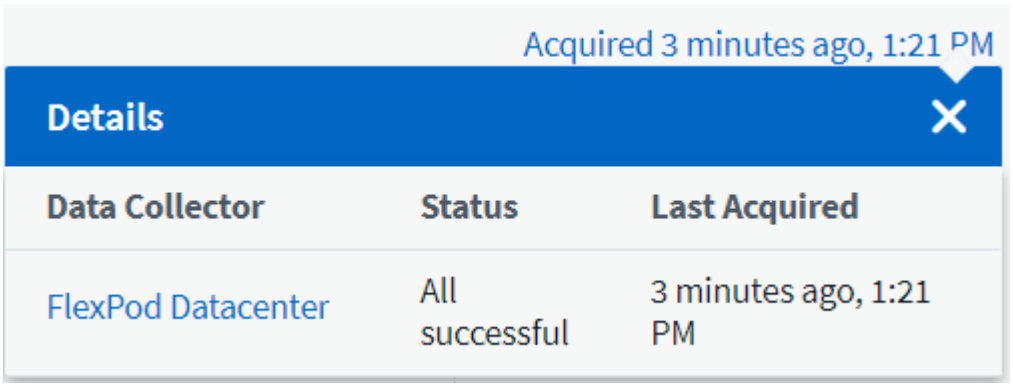


실시간 대시보드를 탐색합니다

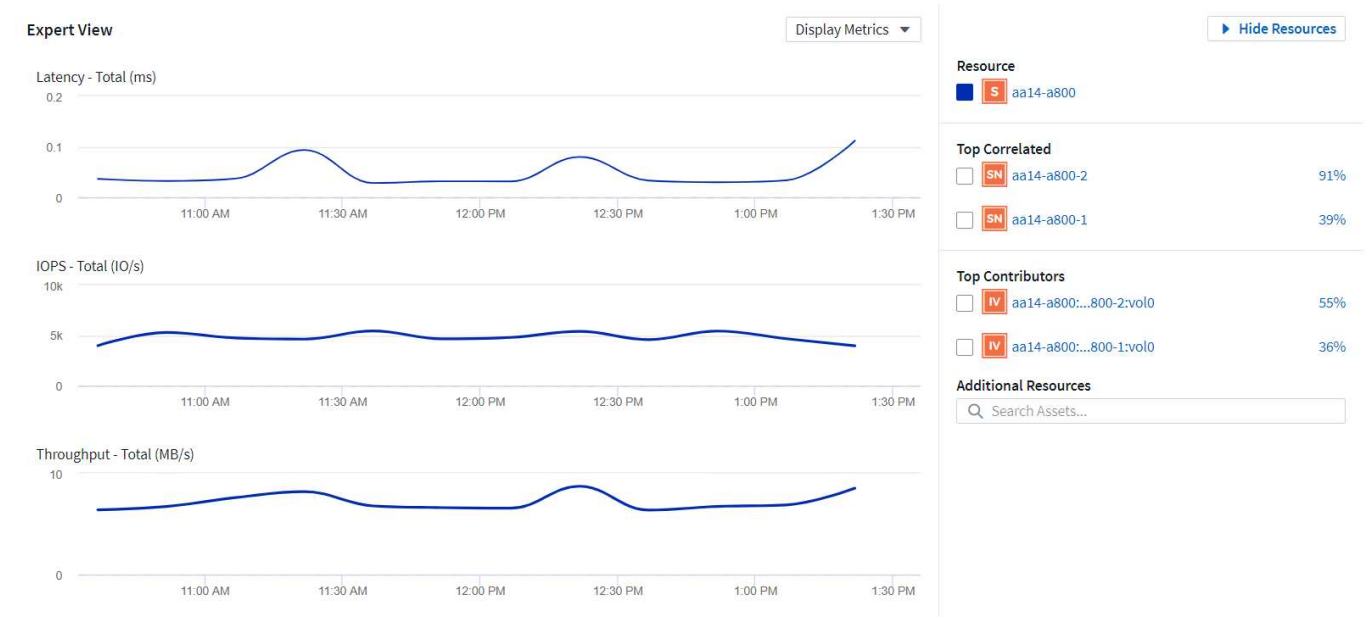
Cloud Insights는 FlexPod 데이터 센터 솔루션에 구축된 ONTAP 스토리지 시스템에서 폴링한 정보의 실시간 대시보드를 표시할 수 있습니다. Cloud Insights 획득 장치는 정기적으로 데이터를 수집하고 기본 스토리지 시스템 대시보드를 수집된 정보로 채웁니다.

Cloud Insights 대시보드를 통해 실시간 그래프에 액세스할 수 있습니다

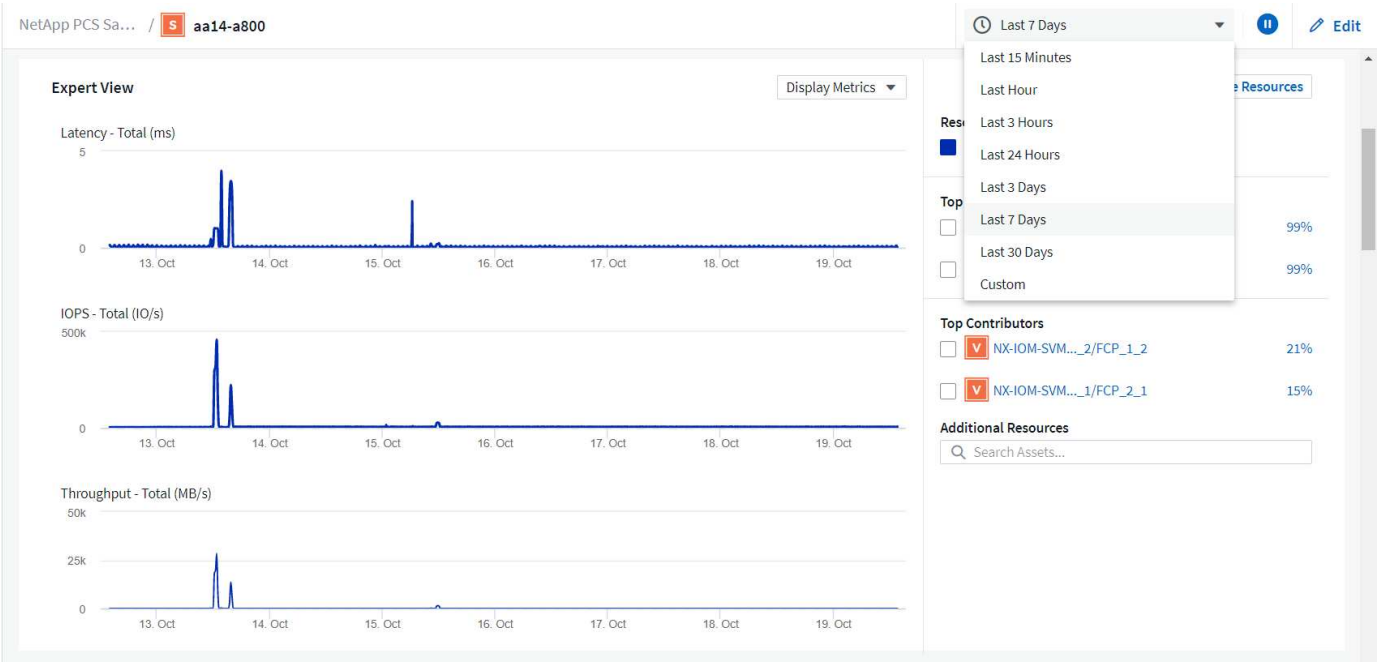
스토리지 시스템 대시보드에서 Data Collector가 마지막으로 정보를 업데이트한 시간을 확인할 수 있습니다. 이 예제는 아래 그림에 나와 있습니다.



기본적으로 스토리지 시스템 대시보드에는 폴링 중인 스토리지 시스템의 시스템 전체 메트릭이 표시되는 대화형 그래프가 여러 개 표시되며, 전문가 보기 섹션의 지연 시간, IOPS 및 처리량 등 각 개별 노드별로 표시됩니다. 이러한 기본 그래프의 예는 아래 그림에 나와 있습니다.



기본적으로 그래프에는 최근 3시간 동안의 정보가 표시되지만 스토리지 시스템 대시보드 오른쪽 상단 근처에 있는 드롭다운 목록에서 여러 다른 값 또는 사용자 지정 값으로 설정할 수 있습니다. 이는 아래 그림에 나와 있습니다.



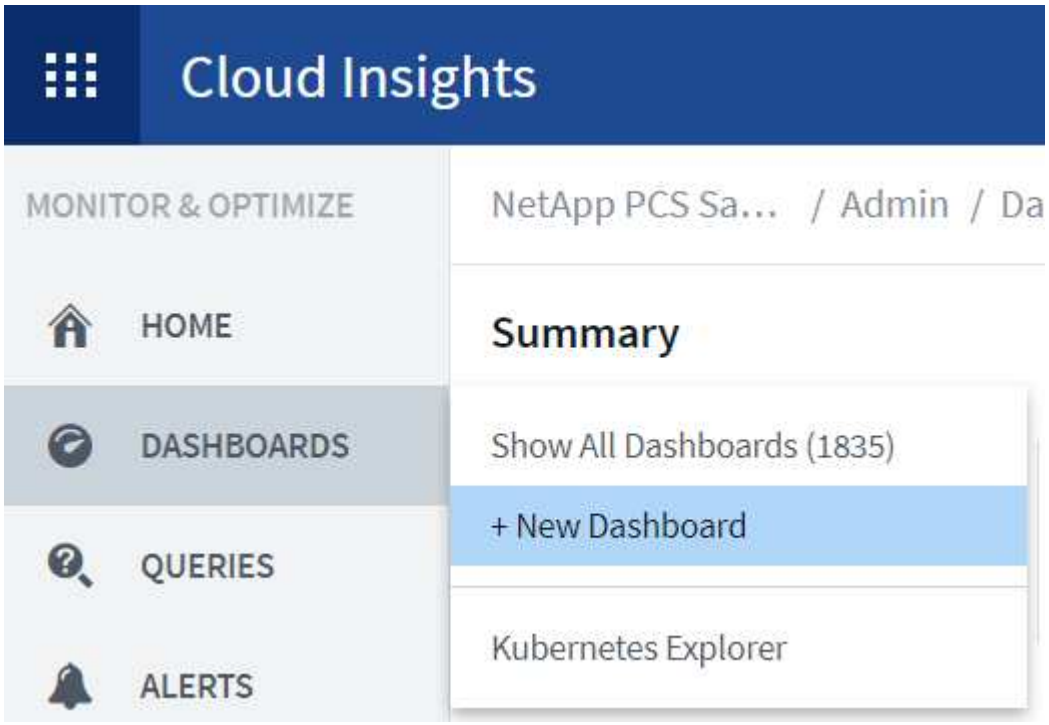
사용자 지정 대시보드를 생성합니다

Cloud Insights를 사용하면 시스템 전반의 정보를 표시하는 기본 대시보드를 사용할 수 있을 뿐만 아니라 FlexPod 데이터 센터 솔루션의 특정 스토리지 볼륨에 대한 리소스 사용에 초점을 맞출 수 있도록 완벽하게 사용자 지정된 대시보드를 만들 수 있습니다. 따라서 컨버지드 인프라에 구축된 애플리케이션은 이러한 볼륨을 사용하여 효율적으로 실행됩니다. 이렇게 하면 데이터 센터 환경에서 특정 애플리케이션과 이러한 애플리케이션이 소비하는 리소스를 보다 효율적으로 시각화하는 데 도움이 됩니다.

스토리지 리소스를 평가하기 위한 맞춤형 대시보드 생성

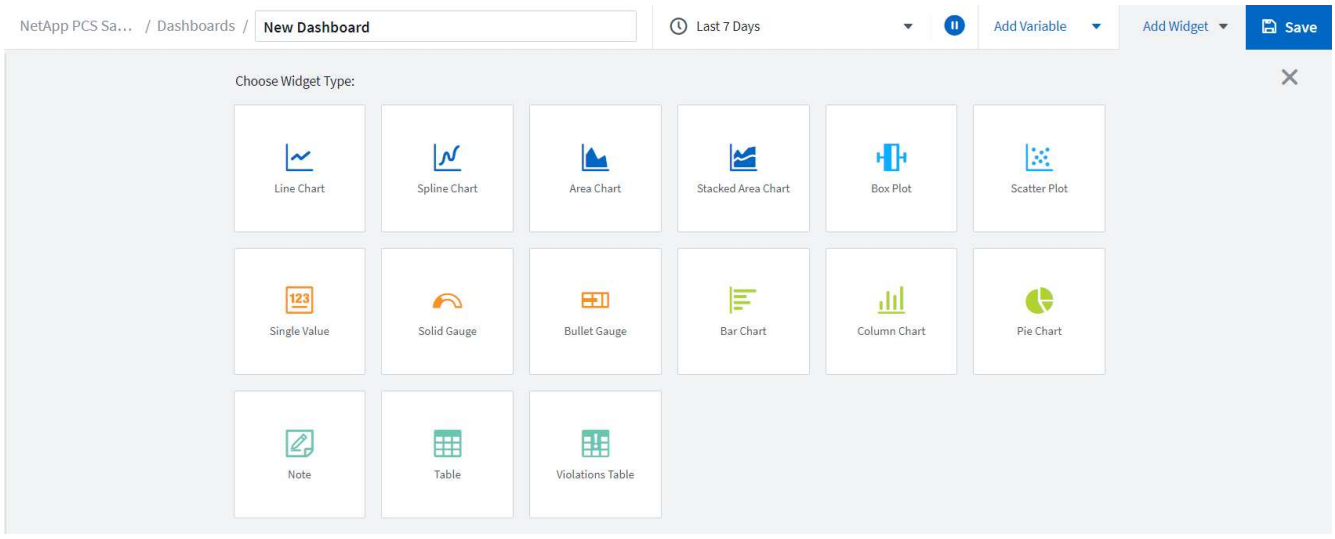
스토리지 리소스를 평가하기 위한 맞춤형 대시보드를 생성하려면 다음 단계를 완료하십시오.

1. 사용자 지정 대시보드를 만들려면 Cloud Insights 기본 메뉴에서 대시보드 위에 마우스 포인터를 놓고 드롭다운 목록에서 + 새 대시보드 를 클릭합니다.



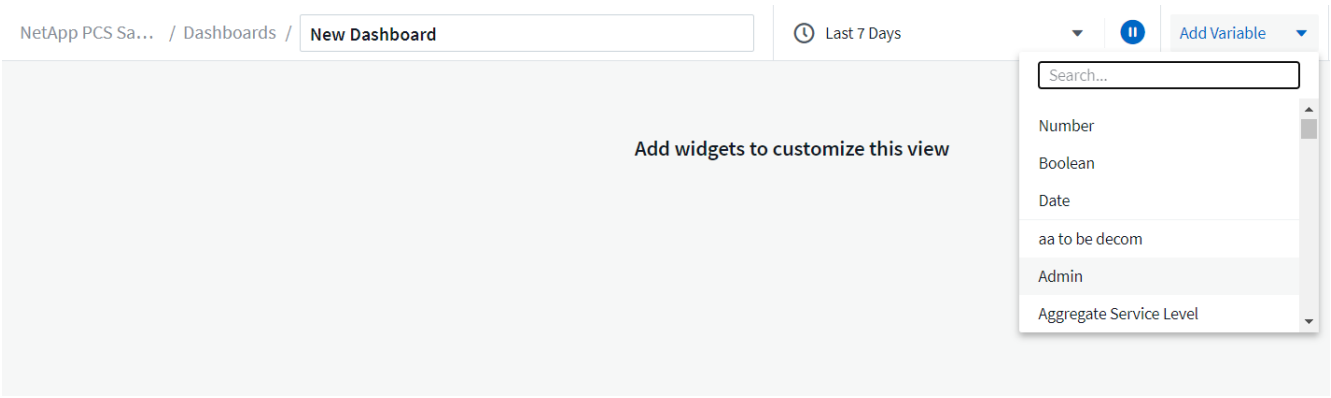
새 대시보드 창이 열립니다.

2. 대시보드 이름을 지정하고 데이터를 표시하는 데 사용되는 위젯 유형을 선택합니다. 수집된 데이터를 표시할 수 있도록 여러 그래프 유형 또는 노트나 표 유형 중에서 선택할 수 있습니다.



3. 변수 추가 메뉴에서 사용자 정의 변수를 선택합니다.

   이를 통해 제공되는 데이터에 보다 구체적이거나 특수한 요소를 표시할 수 있습니다.



4. 사용자 지정 대시보드를 생성하려면 사용할 위젯 유형을 선택합니다. 예를 들어, 볼륨별 스토리지 사용률을 표시하는 원형 차트를 선택할 수 있습니다.

   a. Add Widget(위젯 추가) 드롭다운 목록에서 Pie Chart(파이 차트) 위젯을 선택합니다.

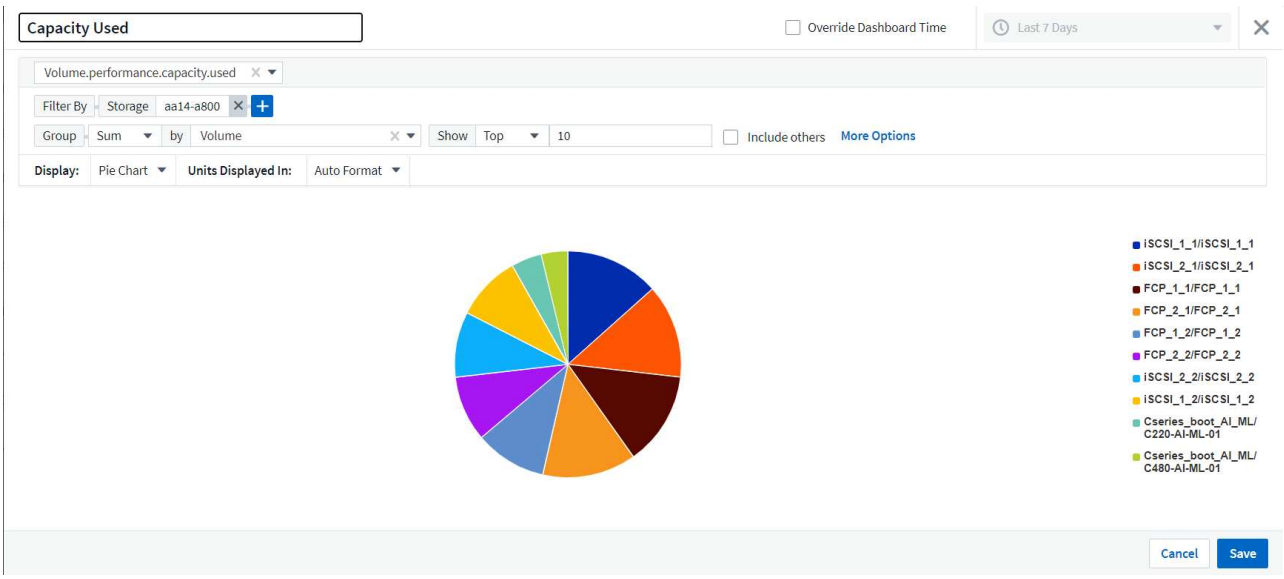
   b. 위젯의 이름을 '사용된 용량'과 같은 설명이 포함된 식별자로 지정합니다.

   c. 표시할 개체를 선택합니다. 예를 들어, 키 용어 볼륨별로 검색하고 'volume.performance.capacity.used'을 선택할 수 있습니다.

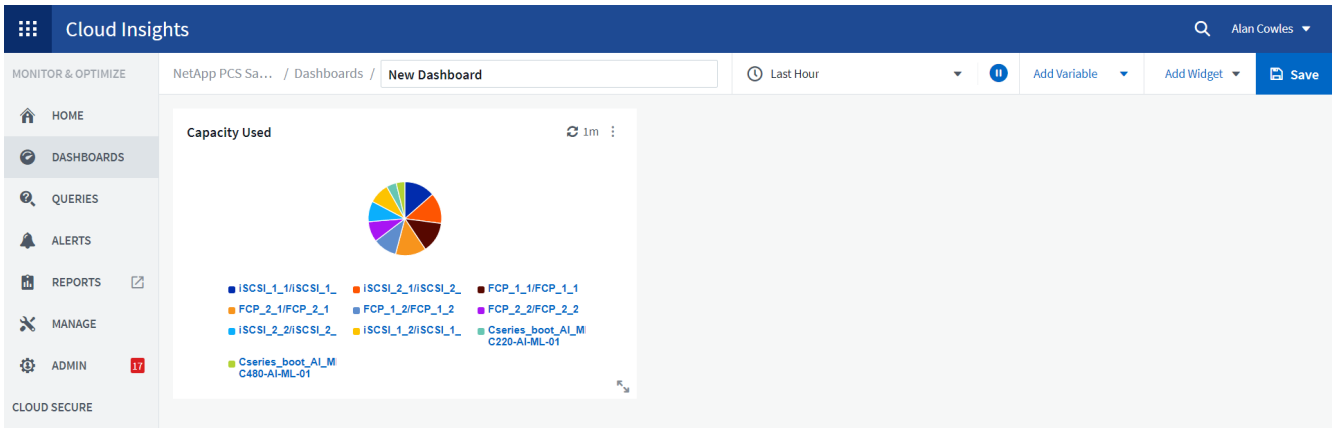
   d. 스토리지 시스템별로 필터링하려면 필터를 사용하고 FlexPod 데이터 센터 솔루션의 스토리지 시스템 이름을 입력합니다.

   e. 표시할 정보를 사용자 지정합니다. 기본적으로 이 선택 항목은 ONTAP 데이터 볼륨을 표시하고 상위 10개 볼륨을 나열합니다.

   f. 사용자 지정된 대시보드를 저장하려면 저장 을 클릭합니다.



   사용자 지정 위젯을 저장한 후 브라우저는 새로 생성된 위젯을 표시하는 새 대시보드 페이지로 돌아가 데이터 폴링 기간 수정과 같은 대화형 작업을 수행할 수 있습니다.



고급 문제 해결

Cloud Insights를 사용하면 FlexPod 데이터 센터 통합 인프라의 모든 스토리지 환경에 고급 문제 해결 방법을 적용할 수 있습니다. 위에서 언급한 각 기능의 구성 요소, 즉 Active IQ 통합, 실시간 통계를 제공하는 기본 대시보드, 사용자 지정 대시보드를 사용하면 발생할 수 있는 문제가 조기에 감지되어 신속하게 해결됩니다. 고객은 Active IQ의 위험 목록을 사용하여 보고된 구성 오류를 찾거나 보고된 버그 또는 이를 해결할 수 있는 패치된 버전의 코드를 발견할 수 있습니다. Cloud Insights 홈 페이지의 실시간 대시보드를 관찰하면 시스템 성능의 패턴을 파악하는 데 도움이 됩니다. 시스템 성능 패턴은 증가 문제에 대한 초기 지표일 수 있으며 이를 신속하게 해결하는 데 도움이 됩니다. 마지막으로, 맞춤형 대시보드를 생성할 수 있으므로 고객은 인프라에서 가장 중요한 자산에 집중하고 이를 직접 모니터링하여 비즈니스 연속성 목표를 달성할 수 있습니다.

스토리지 최적화

Cloud Insights에서 수집한 데이터를 활용하여 문제 해결 외에도 FlexPod 데이터 센터 통합 인프라 솔루션에 구축된 ONTAP 스토리지 시스템을 최적화할 수 있습니다. 성능 수요가 높은 여러 VM이 동일한 데이터 저장소를 공유하기 때문에 볼륨에 높은 지연 시간이 표시되는 경우 해당 정보가 Cloud Insights 대시보드에 표시됩니다. 이 정보를 사용하여 스토리지 관리자는 하나 이상의 VM을 다른 볼륨으로 마이그레이션하거나, 스토리지 볼륨을 애그리게이트 계층 간에 마이그레이션하거나, ONTAP 스토리지 시스템의 노드 간에 마이그레이션하도록 선택하여 성능을 최적화할 수 있습니다. Active IQ와 Cloud Insights의 통합을 통해 얻은 정보는 구성 문제를 부각하여 기대 성능보다 낮은 문제를 야기하고, 구현 시 문제를 해결하고, 최적의 상태로 조정된 스토리지 시스템을 보장할 수 있는 권장 수정 조치를 제공할 수 있습니다.

비디오 및 데모

NetApp Cloud Insights를 사용하여 사내 환경의 리소스를 평가하는 비디오 데모를 볼 수 있습니다 "여기".

NetApp Cloud Insights를 사용하여 인프라를 모니터링하고 인프라에 대한 경고 임계값을 설정하는 방법에 대한 비디오 데모를 볼 수 있습니다 "여기".

NetApp Cloud Insights를 사용하여 환경의 개별 애플리케이션 평가 비디오 데모를 볼 수 있습니다 "여기".

추가 정보

이 문서에 설명된 정보에 대한 자세한 내용은 다음 웹 사이트를 참조하십시오.

- Cisco 제품 설명서

"https://www.cisco.com/c/en/us/support/index.html"

- FlexPod 데이터 센터

  "https://www.flexpod.com"

- NetApp Cloud Insights를 참조하십시오

  "https://cloud.netapp.com/cloud-insights"

- NetApp 제품 설명서

  "https://docs.netapp.com"

FlexPod with FabricPool - Amazon AWS S3로 비활성 데이터 계층화

TR-4801: FabricPool를 지원하는 FlexPod - Amazon AWS S3에 대한 비활성 데이터 계층화

Scott Kovacs, NetApp을 참조하십시오

플래시 스토리지의 가격이 계속 하락하고 있기 때문에 이전에 플래시 스토리지로 적합하지 않은 워크로드 및 애플리케이션에 사용할 수 있습니다. 그러나 스토리지 투자를 가장 효율적으로 활용하는 것은 IT 관리자에게 여전히 매우 중요합니다. IT 부서는 예산을 거의 또는 전혀 사용하지 않고 고성능 서비스를 제공해야 하는 지속적인 압박을 지속적으로 수행하고 있습니다. 이러한 요구사항을 해결하기 위해 NetApp FabricPool을 사용하면 자주 사용하지 않는 데이터를 값비싼 온프레미스 플래시 스토리지에서 퍼블릭 클라우드의 보다 비용 효율적인 스토리지 계층으로 이동하여 클라우드의 경제성을 활용할 수 있습니다. 자주 액세스하지 않는 데이터를 클라우드로 이동하면 AFF 또는 FAS 시스템에서 중요한 플래시 스토리지 공간을 확보하여 비즈니스 크리티컬 워크로드에 고성능 플래시 계층에 더 많은 용량을 제공할 수 있습니다.

이 기술 보고서에서는 NetApp과 Cisco의 FlexPod 통합 인프라 아키텍처를 기반으로 NetApp ONTAP의 FabricPool 데이터 계층화 기능을 검토합니다. 이 기술 보고서에서 설명된 개념을 충분히 활용하려면 FlexPod 데이터 센터 통합 인프라 아키텍처 및 ONTAP 스토리지 소프트웨어에 대해 잘 알고 있어야 합니다. FlexPod과 ONTAP에 대한 친숙도를 기반으로 FabricPool의 작동 방식 및 사내 플래시 스토리지를 더욱 효율적으로 사용하는 방법에 대해 설명합니다. 이 보고서의 내용 대부분은 에서 자세히 다룹니다 "TR-4598 FabricPool 모범 사례" 및 기타 ONTAP 제품 설명서를 참조하십시오. FlexPod 인프라에 대한 콘텐츠가 압축되었으며 FabricPool의 모든 사용 사례에 대해서는 다루지 않습니다. 검사한 모든 기능과 개념은 ONTAP 9.6에서 사용할 수 있습니다.

FlexPod에 대한 자세한 내용은 에서 확인할 수 있습니다 "TR-4036 FlexPod 데이터 센터 기술 사양".

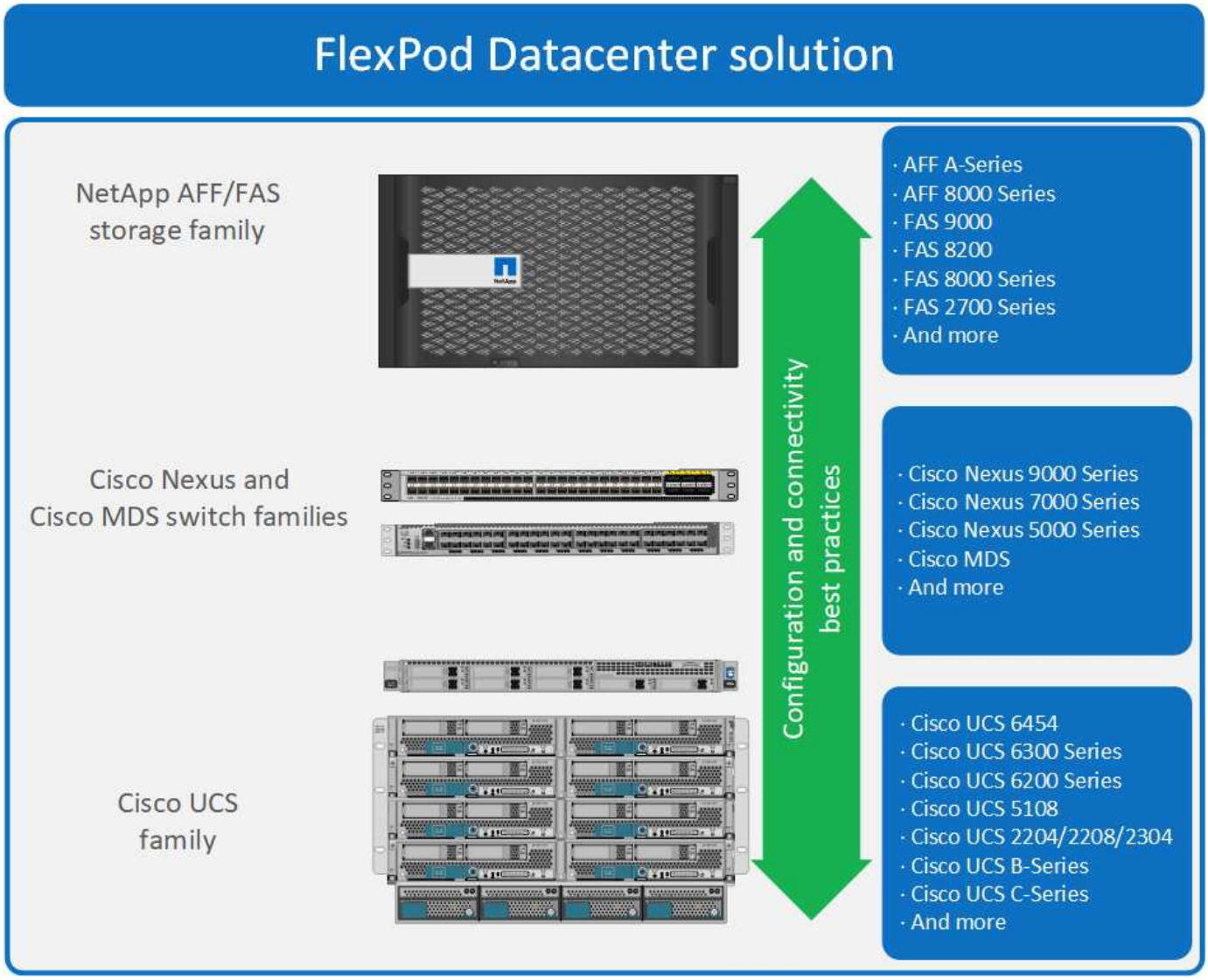
FlexPod 개요 및 아키텍처

FlexPod 개요

FlexPod는 가상화된 솔루션과 가상화되지 않은 솔루션 모두를 위한 통합된 기반을 형성하는 정의된 하드웨어 및 소프트웨어 세트입니다. FlexPod에는 NetApp AFF 스토리지, Cisco Nexus 네트워킹, Cisco MDS 스토리지 네트워킹, Cisco UCS(Cisco Unified Computing System) 및 VMware vSphere 소프트웨어가 단일 패키지에

포함되어 있습니다. 이 설계는 네트워킹, 컴퓨팅 및 스토리지가 하나의 데이터 센터 랙에 장착되거나 고객의 데이터 센터 설계에 따라 배포될 수 있을 만큼 유연합니다. 포트 밀도를 통해 네트워킹 구성 요소가 여러 구성을 수용할 수 있습니다.

FlexPod 아키텍처의 한 가지 이점은 고객의 요구사항에 맞게 환경을 사용자 지정하거나 유연하게 변경할 수 있다는 것입니다. FlexPod 유닛은 요구사항 및 요구사항의 변화에 따라 쉽게 확장할 수 있습니다. 단위는 스케일업(FlexPod 유닛에 리소스 추가) 및 스케일아웃(FlexPod 유닛 추가) 모두 확장 가능합니다. FlexPod 참조 아키텍처는 파이버 채널 및 IP 기반 스토리지 솔루션의 복원력, 비용 이점 및 간편한 구축을 강조합니다. 단일 인터페이스에서 여러 프로토콜을 지원할 수 있는 스토리지 시스템은 고객이 직접 선택할 수 있는 선택권을 제공하며 실질적인 1선 아키텍처 역할을 하므로 투자를 보호합니다. 다음 그림은 FlexPod의 많은 하드웨어 구성 요소를 보여줍니다.

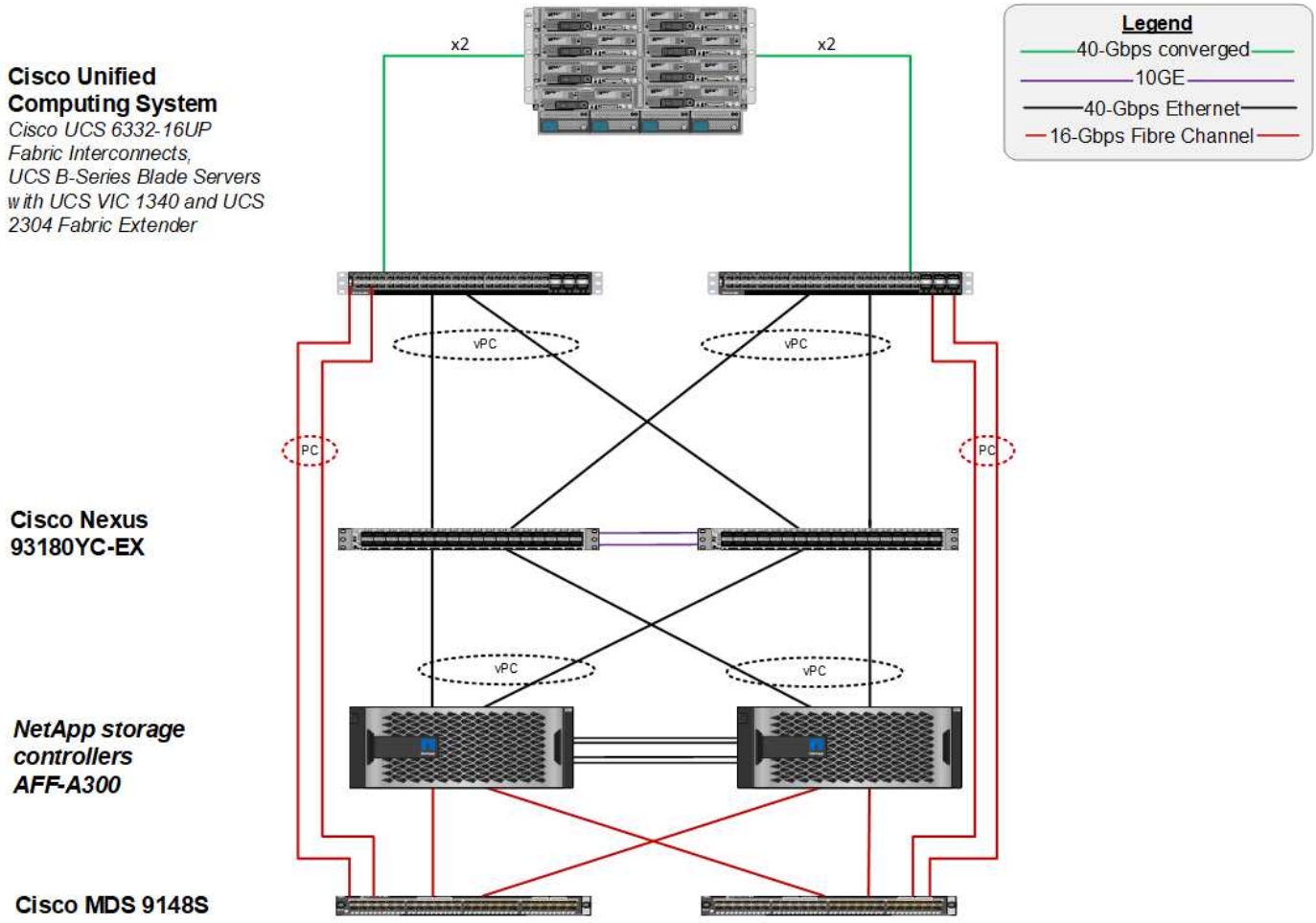


FlexPod 아키텍처

다음 그림에서는 VMware vSphere 및 FlexPod 솔루션의 구성 요소와 Cisco UCS 6454 패브릭 상호 연결에 필요한 네트워크 연결을 보여 줍니다. 이 설계에는 다음과 같은 구성 요소가 있습니다.

- Cisco UCS 5108 블레이드 섀시와 Cisco UCS 패브릭 인터커넥트 간에 포트 채널형 40Gb 이더넷 연결
- Cisco UCS 패브릭 인터커넥트와 Cisco Nexus 9000 사이의 40Gb 이더넷 연결
- Cisco Nesxus 9000과 NetApp AFF A300 스토리지 어레이 간 40Gb 이더넷 연결

이러한 인프라 옵션은 Cisco UCS 패브릭 인터커넥트와 NetApp AFF A300 간에 Cisco MDS 스위치가 도입되면서 확장되었습니다. 이 구성은 공유 스토리지에 대한 16Gb FC 블록 레벨 액세스 기능을 갖춘 FC 부팅 호스트를 제공합니다. 레퍼런스 아키텍처는 아키텍처에 추가 스토리지가 추가될 때 호스트에서 Cisco UCS 패브릭 인터커넥트로 재연결할 필요가 없기 때문에 한 번만 연결 전략을 보강합니다.



FabricPool

FabricPool 개요

FabricPool은 ONTAP의 하이브리드 스토리지 솔루션으로, All-Flash(SSD) 애그리게이트를 성능 계층으로 사용하고 퍼블릭 클라우드 서비스의 오브젝트 저장소를 클라우드 계층으로 사용합니다. 이 구성을 사용하면 데이터 액세스 빈도 여부에 따라 정책 기반 데이터 이동이 가능합니다. FabricPool는 FAS에서 AFF 플랫폼의 ONTAP 및 All-SSD 애그리게이트를 모두 지원합니다. 데이터 처리는 블록 레벨에서 수행되며, 자주 액세스되는 데이터 블록은 All-Flash 성능 계층에서 핫 블록으로 태깅되고 자주 액세스하지 않는 블록이 콜드 블록으로 태깅됩니다.

FabricPool를 사용하면 성능, 효율성, 보안 또는 보호 기능의 저하 없이 스토리지 비용을 절감할 수 있습니다. FabricPool는 엔터프라이즈 애플리케이션에 투명하며, 애플리케이션 인프라를 재설계할 필요 없이 스토리지 TCO를 절감하여 클라우드 효율성을 사용합니다.

FlexPod은 FabricPool의 스토리지 계층화 기능을 활용하여 ONTAP 플래시 스토리지를 더욱 효율적으로 사용할 수 있습니다. NetApp SnapCenter for vSphere의 비활성 가상 머신(VM), 자주 사용되지 않는 VM 템플릿, VM 백업은 데이터 저장소 볼륨에서 귀중한 공간을 소모할 수 있습니다. 콜드 데이터를 클라우드 계층으로 이동하여 FlexPod 인프라에 호스팅된 고성능, 미션 크리티컬 애플리케이션을 위한 공간과 리소스를 확보할 수 있습니다.

Fibre Channel 및 iSCSI 프로토콜은 일반적으로 시간 초과(60-120초)가 발생하기 전에 더 오래 걸리지만 NAS 프로토콜과 같은 방식으로 연결을 다시 시도하지 않습니다. SAN 프로토콜 시간이 초과되면 애플리케이션을 다시 시작해야 합니다. 짧은 운영 중단이라도 SAN 프로토콜을 사용하는 운영 애플리케이션에 심각한 영향을 줄 수 있습니다. 퍼블릭 클라우드에 대한 연결을 보장할 방법이 없기 때문입니다. 이 문제를 방지하려면 SAN 프로토콜을 통해 액세스하는 데이터를 계층화할 때 프라이빗 클라우드를 사용하는 것이 좋습니다.

ONTAP 9.6에서 FabricPool는 Alibaba 클라우드 오브젝트 스토리지 서비스, Amazon AWS S3, Google 클라우드 스토리지, IBM 클라우드 오브젝트 스토리지, Microsoft Azure Blob Storage 등 주요 퍼블릭 클라우드 공급자와 통합됩니다. 이 보고서에서는 Amazon AWS S3 스토리지를 원하는 클라우드 오브젝트 계층으로 중점적으로 다룹니다.

복합 집계

FabricPool 인스턴스는 ONTAP 플래시 애그리게이트를 AWS S3 버킷과 같은 클라우드 오브젝트 저장소와 연결하여 복합 애그리게이트를 만들어 냅니다. 복합 집계 내에 볼륨이 생성되면 FabricPool의 계층화 기능을 활용할 수 있습니다. 볼륨에 데이터를 쓸 때 ONTAP은 각 데이터 블록에 온도를 할당합니다. 블록이 처음 기록되면 뜨거워진 온도가 할당됩니다. 시간이 경과함에 따라 데이터에 액세스하지 않으면 마지막으로 콜드 상태가 할당될 때까지 냉각 프로세스가 수행됩니다. 자주 액세스하지 않는 데이터 블록은 성능 SSD 애그리게이트와 클라우드 오브젝트 저장소로 계층화합니다.

블록이 콜드 블록으로 지정된 시점과 클라우드 오브젝트 스토리지로 이동한 시점 간의 기간은 ONTAP의 볼륨 계층화 정책에 의해 수정됩니다. 블록 냉각에 필요한 일 수를 제어하는 ONTAP 설정을 수정하여 더 세부적으로 설정할 수 있습니다. 데이터 계층화는 기존 볼륨 스냅샷, vSphere VM 백업용 SnapCenter 및 기타 NetApp Snapshot 기반 백업, VM 템플릿, 자주 액세스하지 않는 VM 데이터 등 vSphere 데이터 저장소에서 자주 사용하지 않는 블록입니다.

비활성 데이터 보고

비활성 데이터 보고(IDR)는 ONTAP에서 사용할 수 있으며, 이를 통해 집계에서 계층화할 수 있는 콜드 데이터의 양을 평가할 수 있습니다. IDR은 ONTAP 9.6에서 기본적으로 활성화되어 있으며, 볼륨의 비활성 데이터를 결정하기 위해 기본 31일 냉각 정책을 사용합니다.

계층화하는 콜드 데이터의 양은 볼륨에 설정된 계층화 정책에 따라 달라집니다. 이 양은 기본 31일 냉각 기간을 사용하여 IDR에서 감지한 콜드 데이터 양과 다를 수 있습니다.

오브젝트 생성 및 데이터 이동

FabricPool는 NetApp WAFL 블록 레벨에서 작동하며, 냉각 블록을 스토리지 오브젝트로 연결하고 이러한 오브젝트를 클라우드 계층으로 마이그레이션합니다. 각 FabricPool 개체는 4MB이며 1,024개의 4KB 블록으로 구성됩니다. 주요 클라우드 공급업체의 성능 권장 사항에 따라 개체 크기가 4MB로 수정되며 변경할 수 없습니다. 콜드 블록을 읽고 핫 상태로 만든 경우 4MB 객체에서 요청된 블록만 페치되어 성능 계층으로 다시 이동됩니다. 전체 오브젝트와 전체 파일이 다시 마이그레이션되지 않습니다. 필요한 블록만 마이그레이션됩니다.

ONTAP에서 순차적 읽기에 대한 기회를 감지할 경우 성능을 향상시키기 위해 클라우드 계층에서 블록을 읽은 후 이를 읽습니다.

기본적으로 성능 애그리게이트의 활용률이 50% 이상인 경우에만 데이터가 클라우드 계층으로 이동됩니다. 이 임계값은 성능 플래시 계층에서 더 적은 양의 데이터 스토리지를 클라우드로 이동할 수 있도록 더 낮은 비율로 설정할 수 있습니다. 이 기능은 계층화 전략이 콜드 데이터를 이동하는 경우 애그리게이트의 용량이 거의 도달한 경우에만 유용할 수 있습니다.

성능 계층 활용률이 70% 이상인 경우, 성능 계층에 다시 기록되지 않고 클라우드 계층에서 콜드 데이터를 직접

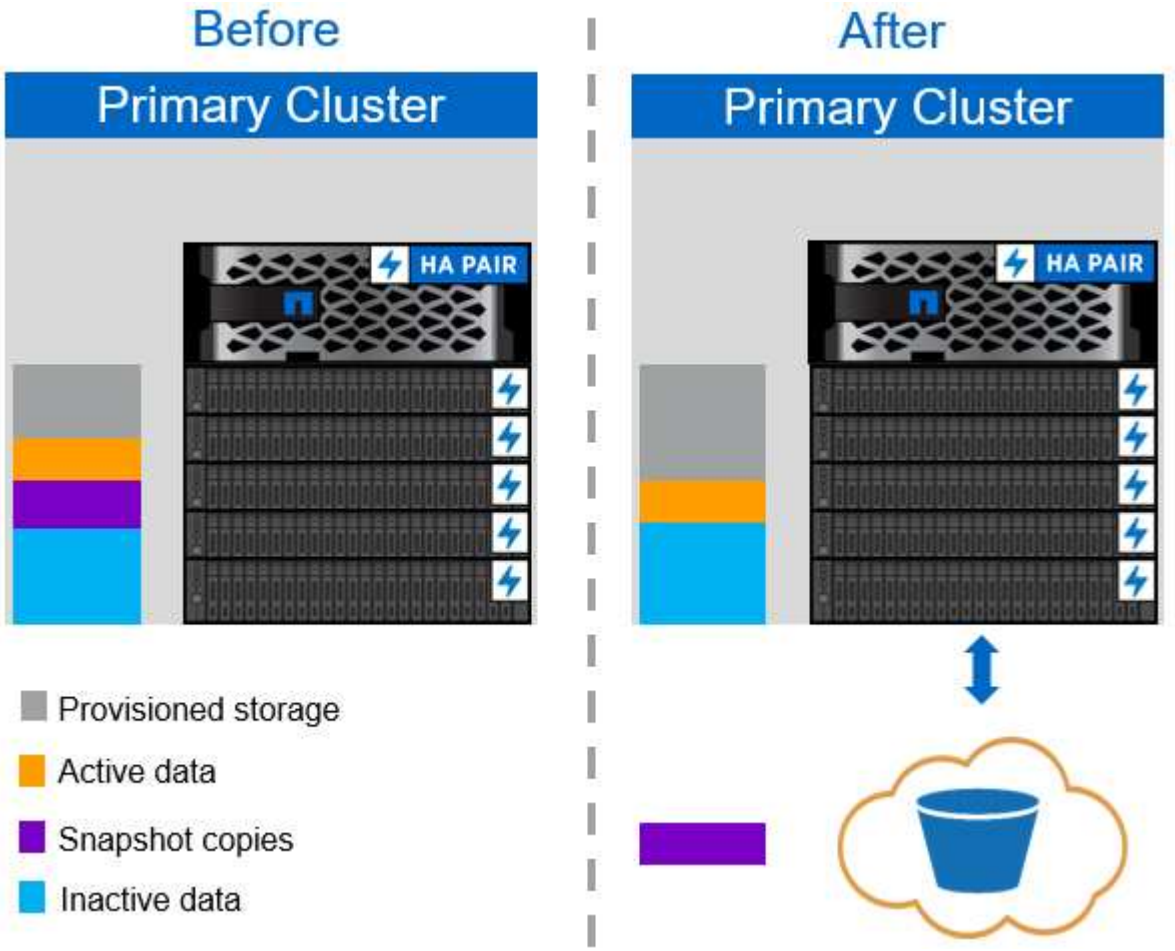
읽습니다. FabricPool는 자주 사용되는 애그리게이트에서 콜드 데이터 쓰기를 방지함으로써 활성 데이터에 대한 애그리게이트를 보존합니다.

성능 계층 공간을 재확보할 수 있습니다

앞서 설명했듯이, FabricPool의 주요 사용 사례는 고성능 사내 플래시 스토리지를 가장 효율적으로 사용하는 것입니다. FlexPod 가상 인프라의 볼륨 스냅샷과 VM 백업의 형태로 콜드 데이터는 상당히 많은 비용이 드는 플래시 스토리지를 차지할 수 있습니다. 스냅샷 전용 또는 자동의 두 가지 계층화 정책 중 하나를 구현하여 중요한 성능 계층 스토리지를 확보할 수 있습니다.

스냅샷 전용 계층화 정책

다음 그림에 나와 있는 스냅샷 전용 계층화 정책은 공간을 차지하지만 활성 파일 시스템과 블록을 공유하지 않는 VM의 vSphere 백업을 위한 SnapCenter 및 콜드 볼륨 스냅샷 데이터를 클라우드 오브젝트 저장소로 이동합니다. 스냅샷 전용 계층화 정책은 콜드 데이터 블록을 클라우드 계층으로 이동합니다. 복원이 필요한 경우 클라우드의 콜드 블록이 핫 상태로 되고 사내 성능 플래시 계층으로 다시 이동됩니다.

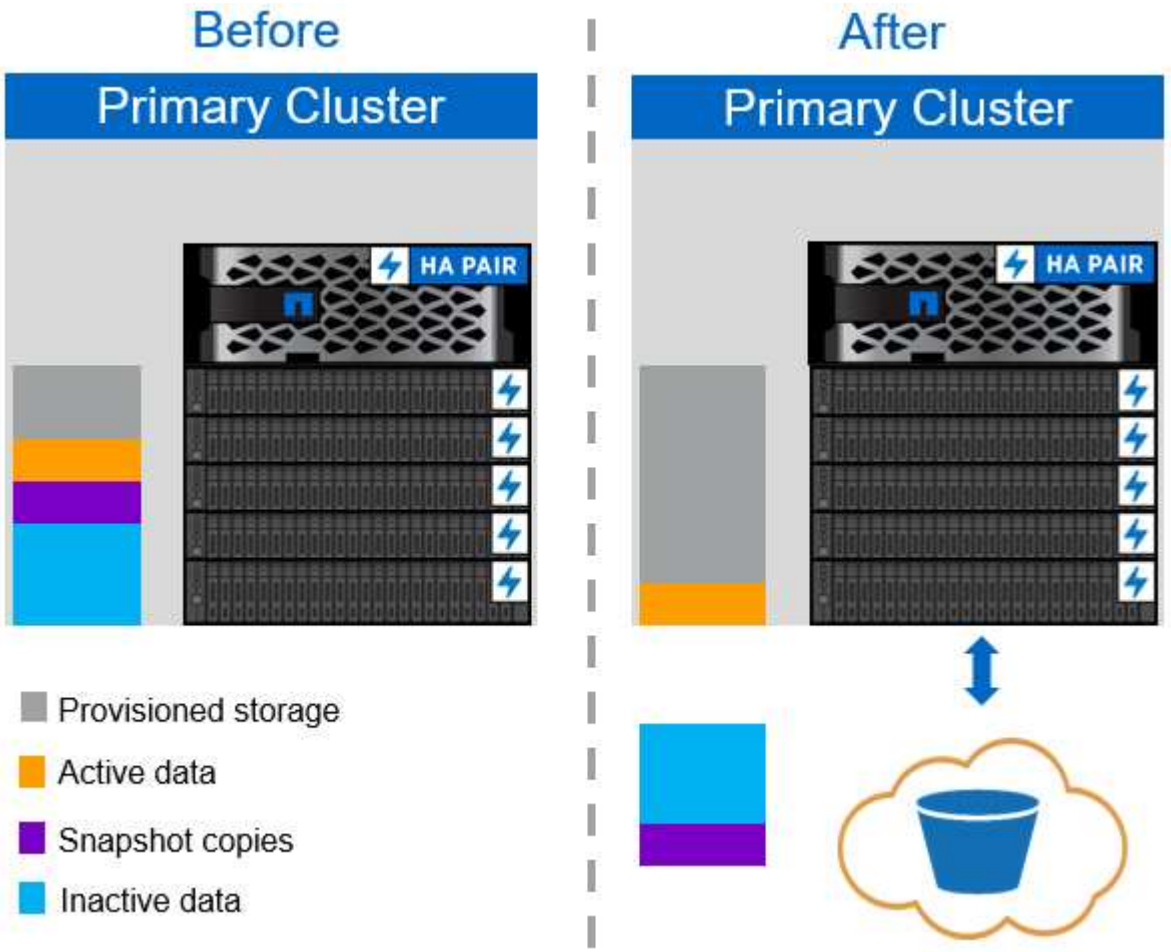


자동 계층화 정책

다음 그림에 나와 있는 FabricPool 자동 계층화 정책은 콜드 스냅샷 데이터 블록을 클라우드로 이동할 뿐만 아니라 액티브 파일 시스템의 콜드 블록도 모두 이동합니다. 여기에는 VM 템플릿과 데이터 저장소 볼륨의 사용되지 않는 VM 데이터가 포함될 수 있습니다. 이동하는 콜드 블록은 볼륨에 대한 계층화-최소-냉각-일 설정으로 제어됩니다. 클라우드 계층의 콜드 블록이 애플리케이션에서 무작위로 읽히는 경우 해당 블록이 핫 블록으로 만들어졌으며 성능 계층으로 다시 돌아갑니다. 하지만 콜드 블록을 바이러스 백신 스캐너와 같은 순차적 프로세스에서 읽는 경우 블록이 콜드 상태로 유지되고 클라우드 오브젝트 저장소에서 유지되지만 성능 계층으로 다시 이동되지 않습니다.

자동 계층화 정책을 사용하면 자주 액세스하지 않는 블록이 클라우드 연결 속도로 클라우드 계층에서 다시 가져옵니다. 애플리케이션의 지연 시간에 민감한 경우 VM 성능에 영향을 미칠 수 있으며, 데이터 저장소에서 자동 계층화 정책을 사용하기 전에 이 정책을 고려해야 합니다. 적절한 성능을 위해 10GbE 속도로 포트에 Intercluster LIF를 배치하는 것이 좋습니다.

오브젝트 저장소 프로파일러는 FabricPool 애그리게이트에 연결하기 전에 오브젝트 저장소에 대한 대기 시간 및 처리량을 테스트하는 데 사용해야 합니다.



모든 계층화 정책

자동 및 스냅샷 전용 정책과 달리 모든 계층화 정책은 전체 데이터 볼륨을 즉시 클라우드 계층으로 이동합니다. 이 정책은 데이터를 기록 또는 규제 목적으로 보관해야 하지만 거의 액세스하지 않는 보조 데이터 보호 또는 아카이브 볼륨에 가장 적합합니다. 데이터 저장소에 기록된 모든 데이터가 클라우드 계층으로 즉시 이동되므로 VMware 데이터 저장소 볼륨에는 All 정책이 권장되지 않습니다. 후속 읽기 작업은 클라우드에서 수행되며 데이터 저장소 볼륨에 상주하는 VM 및 애플리케이션의 성능 문제가 발생할 가능성이 있습니다.

보안

보안은 클라우드 및 FabricPool의 중앙 관심사입니다. ONTAP의 모든 기본 보안 기능은 성능 계층에서 지원되며, 데이터가 클라우드 계층으로 전송될 때 안전하게 보호됩니다. FabricPool는 를 사용합니다 "AES-256-GCM" 성능 계층에서 암호화 알고리즘을 사용하며 이 암호화 수준을 클라우드 계층으로 유지합니다. 클라우드 오브젝트 저장소로 이동하는 데이터 블록은 TLS(Transport Layer Security) v1.2를 통해 보호되어 스토리지 계층 간의 데이터 기밀성 및 무결성을 유지합니다.

암호화되지 않은 연결을 통해 클라우드 오브젝트 저장소와 통신하는 것은 지원되지만 NetApp에서는 권장하지 않습니다.

데이터 암호화

데이터 암호화는 지적 재산, 거래 정보 및 개인 식별 고객 정보를 보호하는 데 매우 중요합니다. FabricPool는 NVE(NetApp Volume Encryption) 및 NetApp Storage Encryption(NSE)을 완벽하게 지원하여 기존 데이터 보호 전략을 유지합니다. 성능 계층에서 암호화된 모든 데이터는 클라우드 계층으로 이동할 때 암호화된 상태로 유지됩니다. 클라이언트측 암호화 키는 ONTAP의 소유이며 서버측 오브젝트 저장소 암호화 키는 해당 클라우드 오브젝트 저장소에서 소유합니다. NVE로 암호화되지 않은 모든 데이터는 AES-256-GCM 알고리즘으로 암호화됩니다. 다른 AES-256 암호화 암호는 지원되지 않습니다.

NSE 또는 NVE는 선택 사항이며 FabricPool를 사용할 필요가 없습니다.

FabricPool 요구 사항

FabricPool를 사용하려면 ONTAP 9.2 이상 및 이 섹션에 나열된 플랫폼 중 한 플랫폼에서 SSD 애그리게이트를 사용해야 합니다. 추가 FabricPool 요구사항은 연결된 클라우드 계층에 따라 다릅니다. AFF은 NetApp FabricPool C190과 같이 비교적 작은 용량의 고정된 엔트리 레벨 AFF 플랫폼의 경우 비활성 데이터를 클라우드 계층으로 이동하는 데 매우 효율적입니다.

플랫폼

FabricPool는 다음 플랫폼에서 지원됩니다.

- NetApp AFF를 참조하십시오
  - A800
  - A700S, A700
  - A320, A300
  - A220, A200
  - C190
  - AFF8080, AFF8060 및 AFF8040
- NetApp FAS를 참조하십시오
  - FAS9000
  - FAS8200
  - FAS8080, FAS8060, FAS8040을 지원합니다
  - FAS2750, FAS2720
  - FAS2650, FAS2620

FAS 플랫폼의 SSD 애그리게이트만 FabricPool를 사용할 수 있습니다.

- 계층에서 실현해 보십시오
  - Alibaba Cloud Object Storage Service(Standard, Infrequent Access)

- Amazon S3(Standard, Standard-IA, One Zone-IA, 지능형 계층화)
- Amazon Commercial Cloud Services(C2S)
- Google 클라우드 스토리지(다중 지역, 지역, 니어라인, Coldline)
- IBM Cloud Object Storage(Standard, Vault, Cold Vault, Flex)
- Microsoft Azure Blob 스토리지(핫 및 쿨)

인터클러스터 **LIF**

FabricPool를 사용하는 클러스터 고가용성(HA) 쌍에는 클라우드 계층과 통신하기 위해 두 개의 인터클러스터 논리 인터페이스(LIF)가 필요합니다. 또한 추가 HA 쌍에 대한 인터클러스터 LIF를 생성하여 클라우드 계층을 해당 노드의 Aggregate에 원활하게 연결하는 것이 좋습니다.

ONTAP에서 AWS S3 오브젝트 저장소에 연결하는 데 사용하는 LIF는 10Gbps 포트에 있어야 합니다.

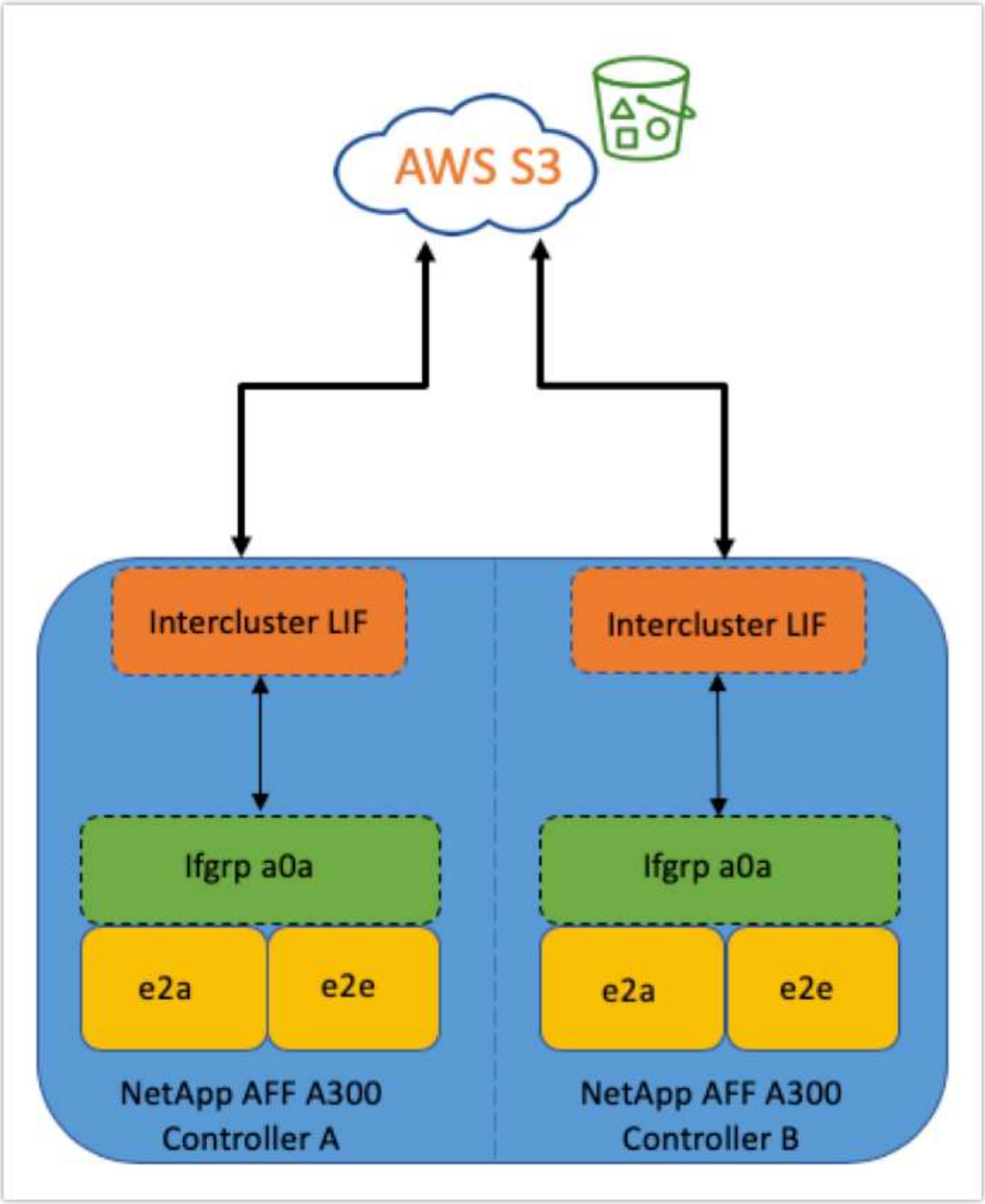
다른 라우팅을 사용하는 노드에서 여러 개의 Intercluser LIF를 사용하는 경우 다른 IPspace에 LIF를 배치하는 것이 좋습니다. 구성 중에 FabricPool는 여러 IPspace에서 선택할 수 있지만 인터클러스터 IPspace 내에서 특정 LIF를 선택할 수 없습니다.

인터클러스터 LIF를 비활성화하거나 삭제하면 클라우드 계층과의 통신이 중단됩니다.

연결성

FabricPool 읽기 지연 시간은 클라우드 계층에 연결하는 기능입니다. 다음 그림에 나와 있는 10Gbps 포트를 사용하는 인터클러스터 LIF는 적절한 성능을 제공합니다. 특정 네트워크 환경의 지연 시간 및 처리량을 확인하여 FabricPool 성능에 미치는 영향을 확인하는 것이 좋습니다.

저성능 환경에서 FabricPool를 사용하는 경우 클라이언트 애플리케이션에 대한 최소 성능 요구 사항을 계속해서 충족하고 그에 따라 복구 시간 목표를 조정해야 합니다.



오브젝트 저장소 프로파일러

오브젝트 저장소 프로파일러는 아래에 표시되어 있으며 ONTAP CLI를 통해 사용할 수 있습니다. 이 프로파일러는 FabricPool 애그리게이트에 연결되기 전에 오브젝트 저장소의 지연 시간 및 처리량 성능을 테스트합니다.

클라우드 계층을 오브젝트 저장소 프로파일러와 함께 사용하려면 먼저 ONTAP에 추가해야 합니다.

다음 명령을 사용하여 ONTAP의 고급 권한 모드에서 오브젝트 저장소 프로파일러를 시작합니다.

```
storage aggregate object-store profiler start -object-store-name <name>
-node <name>
```

결과를 보려면 다음 명령을 실행합니다.

```
storage aggregate object-store profiler show
```

클라우드 계층은 성능 계층(일반적으로 초당 GB)과 유사한 성능을 제공하지 않습니다. FabricPool 애그리게이트는 SATA급 성능을 손쉽게 제공할 수 있지만, SATA급 성능이 필요하지 않은 계층화 솔루션의 지연 시간이 10초 만에 가장 높고 처리량이 적은 것도 용인할 수 있습니다.

```
bb09-a300-2::*> storage aggregate object-store profiler show
Object store config name: aws_infra_fp_bk_1
Node name: bb09-a300-2-1
Status: Active. Issuing GETs
Start time: 10/3/2019 12:37:24

Op      Size       Total     Failed            Latency(ms)          Throughput
                                          min       max       avg
-------------------------------------------------------------------------------
PUT     4MB        1084      0         336       5951      2817     69.55MB
GET     4KB        158636    0         27        1132      41       32.22MB
GET     8KB        0         0         0         0         0        0B
GET     32KB       0         0         0         0         0        0B
GET     256KB      0         0         0         0         0        0B
5 entries were displayed.
```

볼륨

스토리지 씬 프로비저닝은 FlexPod 가상 인프라 관리자의 표준 관행입니다. NetApp VSC(Virtual Storage Console)는 NetApp 모범 사례에 따라 공간 보장(씬 프로비저닝) 및 최적화된 스토리지 효율성 설정 없이 VMware 데이터 저장소용 스토리지 볼륨을 프로비저닝합니다. VSC를 사용하여 VMware 데이터 저장소를 생성하는 경우 데이터 저장소 볼륨에 공간 보장을 할당하지 않기 때문에 추가 작업이 필요하지 않습니다.

FabricPool에서는 없음(예: 볼륨) 이외의 공간 보장을 사용하여 볼륨이 포함된 애그리게이트에 클라우드 계층을 연결할 수 없습니다.

```
volume modify -space-guarantee none
```

'pace-보증 없음' 매개 변수를 설정하면 볼륨에 대한 씬 프로비저닝이 제공됩니다. 이 보증 유형의 볼륨에서 사용하는 공간은 초기 볼륨 크기에 의해 결정되는 대신 추가되는 데이터로 인해 증가합니다. 이 방식은 FabricPool에서 매우 중요합니다. 볼륨에서 핫 상태가 되고 성능 계층으로 다시 복귀되는 클라우드 계층 데이터를 지원해야 하기 때문입니다.

라이센싱

FabricPool에서는 타사 오브젝트 스토리지 공급자(예: Amazon S3)를 AFF 및 FAS 하이브리드 플래시 시스템의 클라우드 계층으로 연결할 때 용량 기반 라이센스가 필요합니다.

FabricPool 라이센스는 영구 또는 기간 기반(1년 또는 3년) 형식으로 제공됩니다.

클라우드 계층에 저장되는 데이터 양(사용된 용량)이 라이센스가 부여된 용량에 도달하면 클라우드 계층에 대한 계층화가 중지됩니다. 모든 계층화 정책을 사용하여 SnapMirror 복사본을 볼륨으로 포함하는 추가 데이터는 라이센스 용량이 증가할 때까지 계층화할 수 없습니다. 계층화가 중지되더라도 클라우드 계층에서 데이터에 계속 액세스할 수 있습니다. 사용 허가된 용량이 증가할 때까지 추가 콜드 데이터는 SSD에 남아 있습니다.

추가 지원 비용이 적용될 수 있지만, 무료 10TB 용량, 기간 기반 FabricPool 라이센스는 새 ONTAP 9.5 이상 클러스터를 구입할 때 제공됩니다. FabricPool 라이센스(기존 라이센스에 대한 추가 용량 포함)는 1TB 단위로 구입할 수 있습니다.

FabricPool 라이센스는 FabricPool 애그리게이트가 포함되지 않은 클러스터에서만 삭제할 수 있습니다.

FabricPool 라이센스는 클러스터 전반에 적용됩니다. 라이센스를 구매할 때 UUID를 사용할 수 있어야 합니다 (`cluster identify show`)를 클릭합니다. 추가 라이센스 정보는 를 참조하십시오 "NetApp 기술 자료".

구성

소프트웨어 개정

다음 표에서는 검증된 하드웨어 및 소프트웨어 버전을 보여 줍니다.

레이어	장치	이미지	설명
스토리지	NetApp AFF A300	ONTAP 9.6P2	
컴퓨팅	Cisco UCS VIC 1340이 장착된 Cisco UCS B200 M5 블레이드 서버	릴리스 4.0(4b)	
네트워크	Cisco Nexus 6332-16UP 패브릭 인터커넥트	릴리스 4.0(4b)	
	NX-OS 독립 실행형 모드의 Cisco Nexus 93180YC-EX 스위치	릴리스 7.0(3) i7(6)	
스토리지 네트워크	Cisco MDS 9148S	릴리즈 8.3(2)	
하이퍼바이저		VMware vSphere ESXi 6.7U2	ESXi 6.7.0,13006603
		VMware vCenter Server를 참조하십시오	vCenter Server 6.7.0.30000 빌드 13639309
클라우드 공급자		Amazon AWS S3	기본 옵션이 있는 표준 S3 버킷

FabricPool의 기본 요구 사항은 에 나와 있습니다 "FabricPool 요구 사항". 모든 기본 요구 사항이 충족되면 다음 단계를

수행하여 FabricPool를 구성합니다.

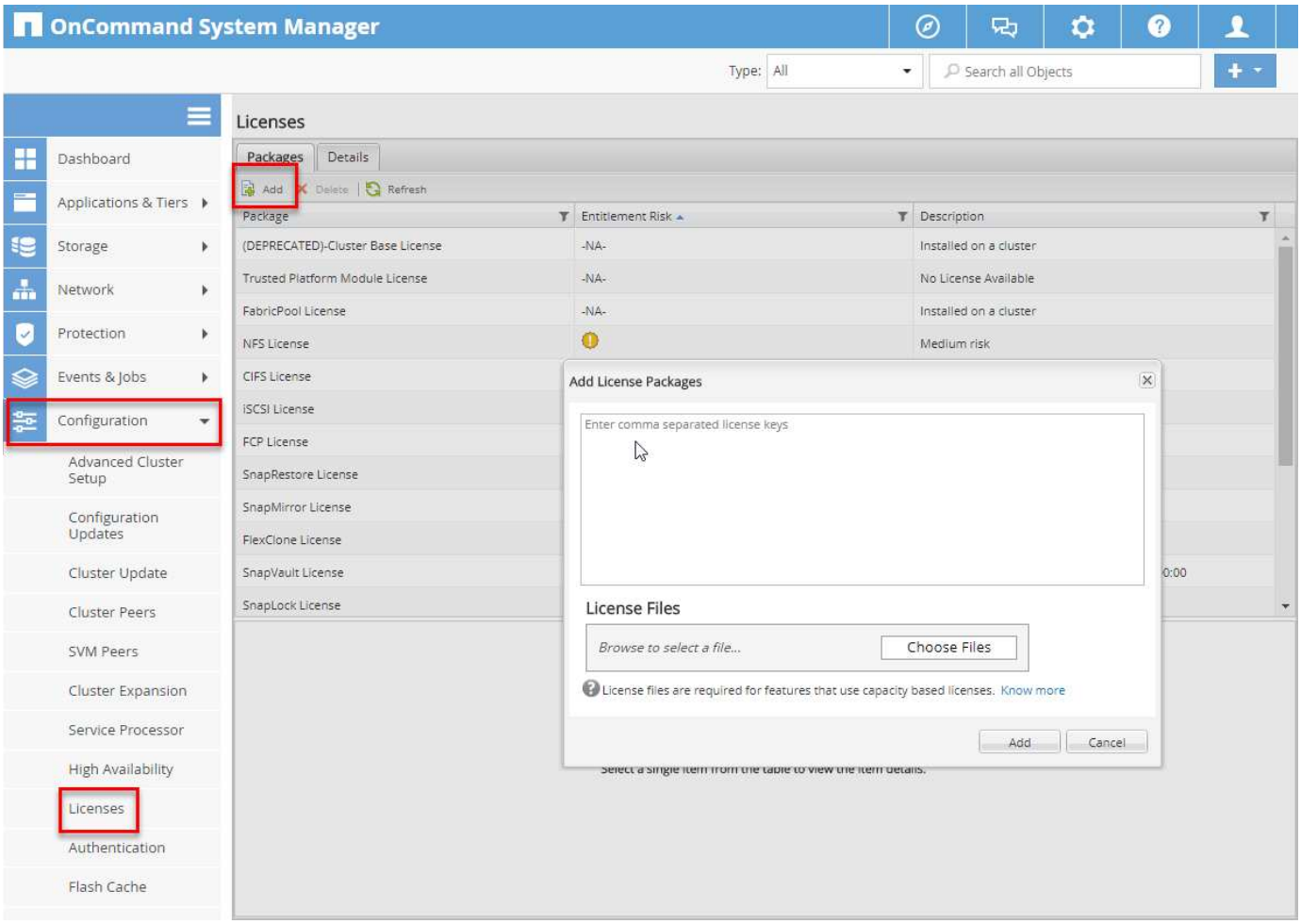
1. FabricPool 라이센스를 설치합니다.
2. AWS S3 오브젝트 저장소 버킷을 생성합니다.
3. ONTAP에 클라우드 계층을 추가합니다.
4. 클라우드 계층을 Aggregate에 연결합니다.
5. 볼륨 계층화 정책을 설정합니다.

"다음: FabricPool 라이센스를 설치합니다."

FabricPool 라이센스를 설치합니다

NetApp 라이센스 파일을 받은 후 OnCommand System Manager로 설치할 수 있습니다. 라이센스 파일을 설치하려면 다음 단계를 수행하십시오.

1. 구성 을 클릭합니다.
2. 클러스터 를 클릭합니다.
3. 라이센스 를 클릭합니다.
4. 추가 를 클릭합니다.
5. 파일 선택 을 클릭하여 파일을 찾아 선택합니다.
6. 추가 를 클릭합니다.



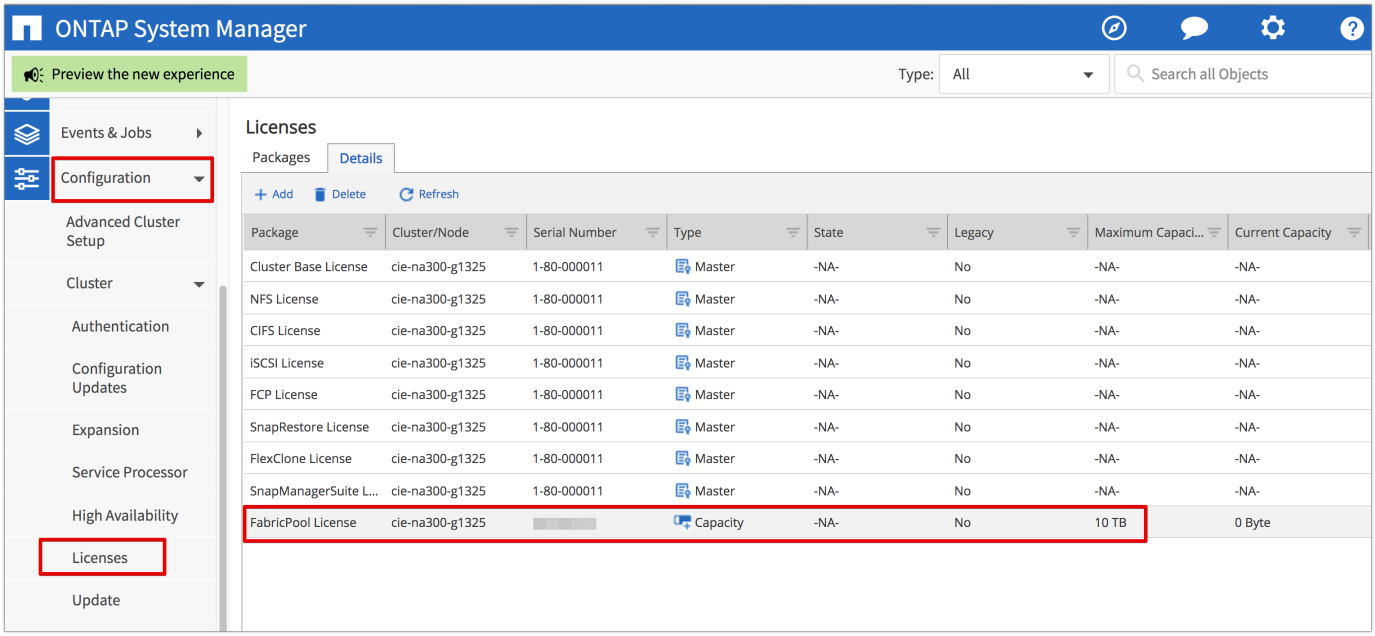
라이센스 용량

ONTAP CLI 또는 OnCommand System Manager를 사용하여 라이센스 용량을 볼 수 있습니다. 라이센스 용량을 확인하려면 ONTAP CLI에서 다음 명령을 실행합니다.

```
system license show-status
```

OnCommand 시스템 관리자에서 다음 단계를 완료합니다.

1. 구성 을 클릭합니다.
2. 라이센스 를 클릭합니다.
3. 세부 정보 탭을 클릭합니다.



최대 용량과 현재 용량은 FabricPool 라이센스 행에 나열됩니다.

"다음: AWS S3 버킷을 생성합니다."

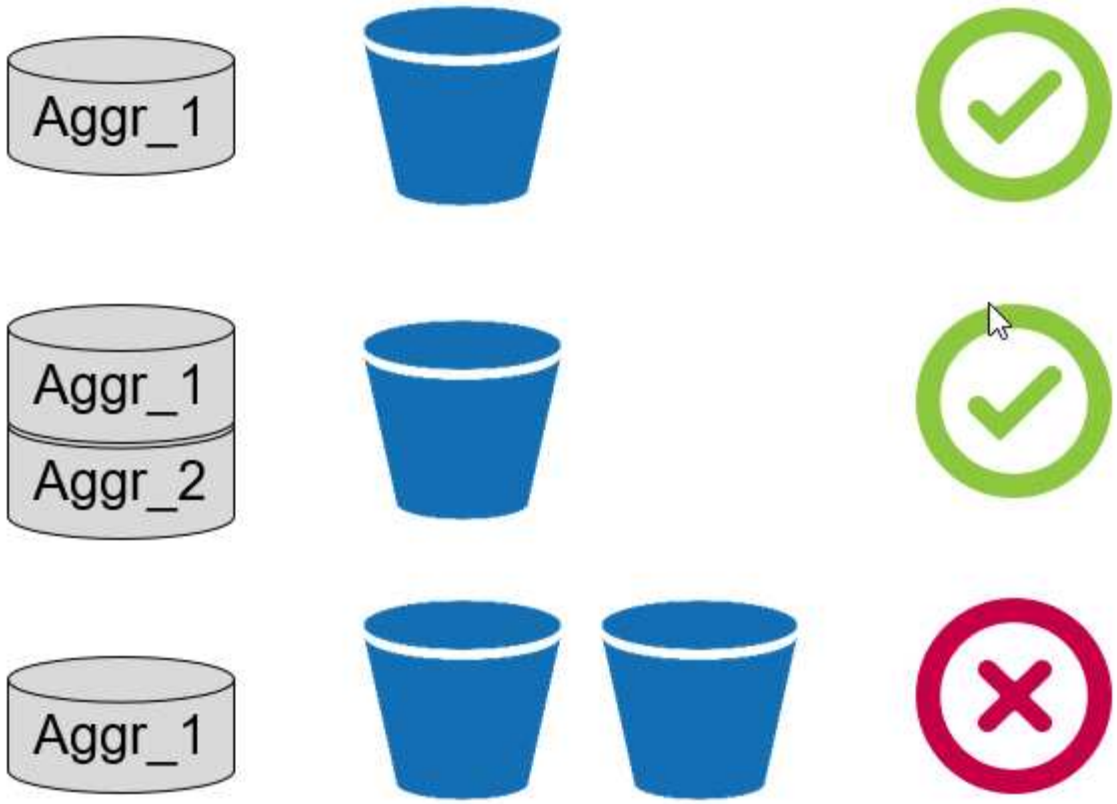
AWS S3 버킷을 생성합니다

버킷은 데이터를 보관하는 오브젝트 저장소 컨테이너입니다. 데이터를 클라우드에 계층으로 애그리게이트에 추가하려면 먼저 버킷의 이름과 위치를 제공해야 합니다.

버킷은 OnCommand 시스템 관리자, OnCommand Unified Manager 또는 ONTAP를 사용하여 생성할 수 없습니다.

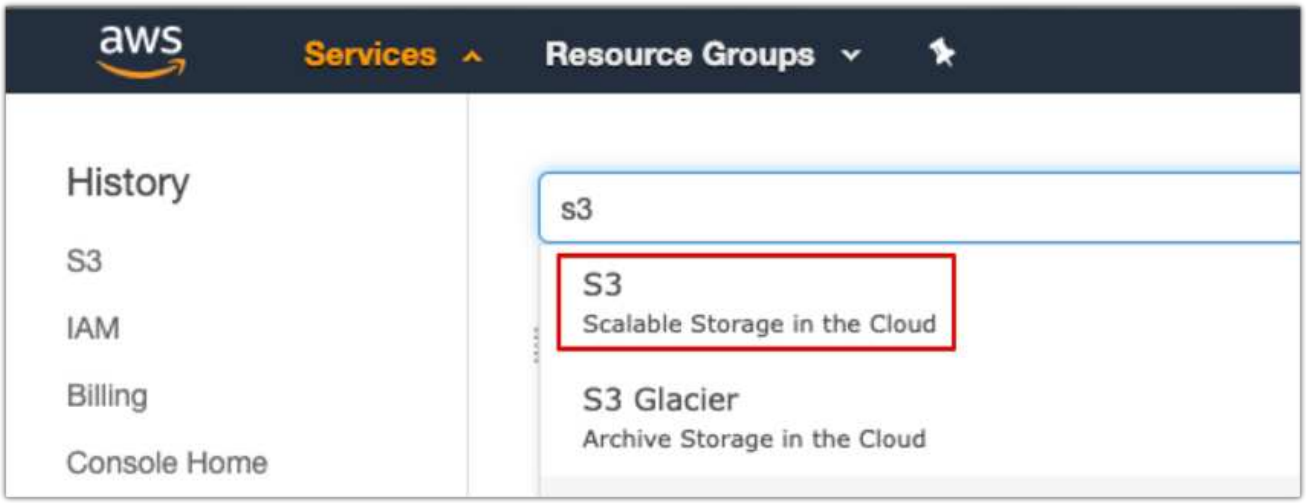
다음 그림과 같이 FabricPool는 Aggregate당 하나의 버킷 어태치먼트를 지원합니다. 단일 버킷은 단일 Aggregate에 연결할 수 있으며, 단일 버킷은 여러 Aggregate에 연결할 수 있습니다. 하지만 단일 aggregate를 여러 버킷에 연결할 수는 없습니다. 단일 버킷은 클러스터의 여러 Aggregate에 연결할 수 있지만, NetApp은 여러 클러스터의 Aggregate에 단일 버킷을 연결하는 것을 권장하지 않습니다.

스토리지 아키텍처를 계획할 때는 버킷-애그리게이트 관계가 성능에 미치는 영향을 고려합니다. 많은 오브젝트 저장소 공급자가 버킷 또는 컨테이너 수준에서 지원되는 최대 IOPS 수를 설정합니다. 최대 성능이 필요한 환경에서는 여러 개의 버킷을 사용하여 오브젝트 저장소 IOPS 제한이 여러 FabricPool 애그리게이트 전체의 성능에 영향을 미칠 수 있는 가능성을 줄여야 합니다. 단일 버킷 또는 컨테이너를 클러스터의 모든 FabricPool 애그리게이트로 연결하는 것은 클라우드 계층 성능보다 관리가 더 중요한 환경에 도움이 될 수 있습니다.

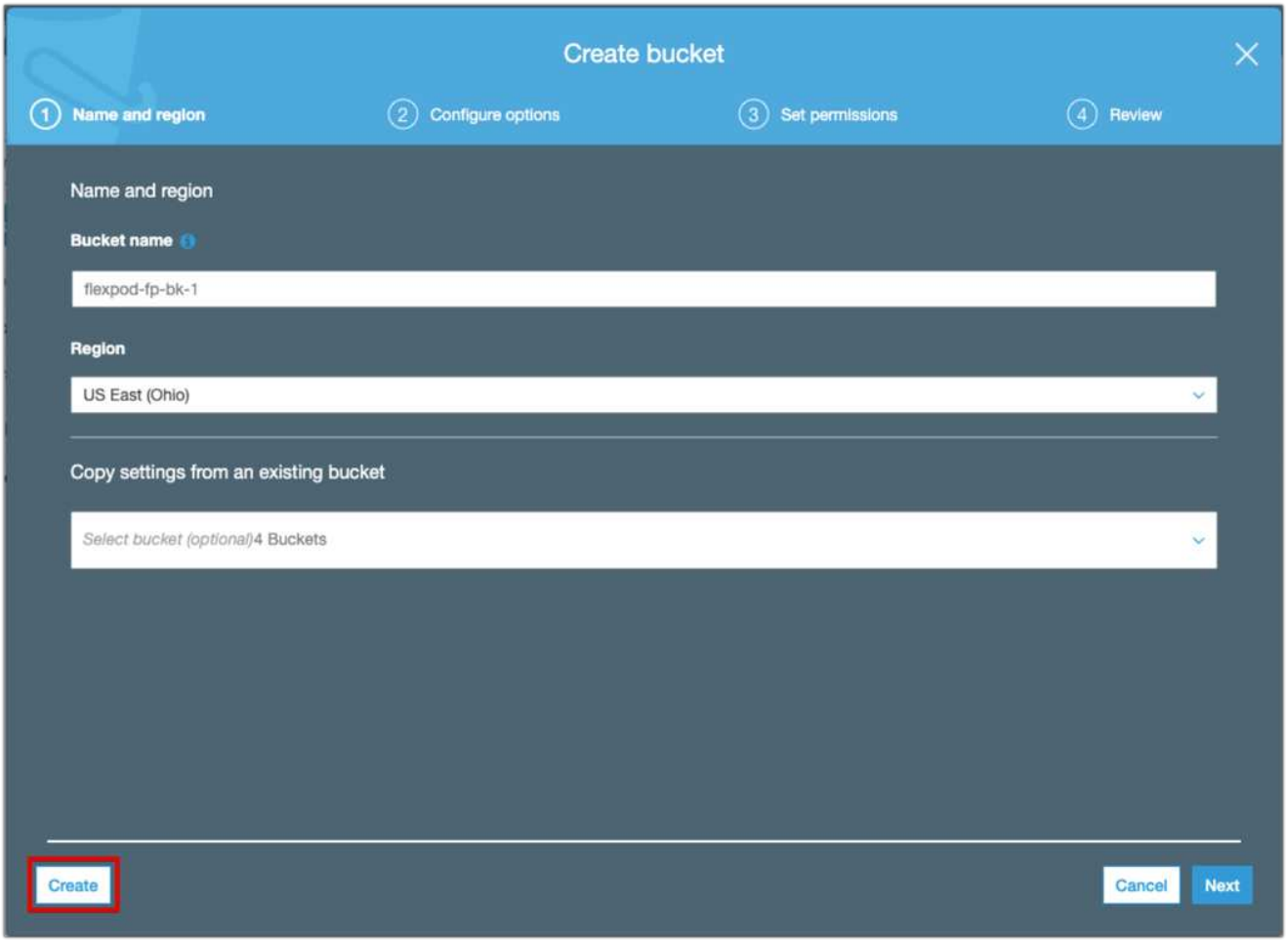


S3 버킷을 생성합니다

1. 홈 페이지의 AWS 관리 콘솔에서 검색 표시줄에 S3를 입력합니다.
2. 클라우드에서 S3 확장형 스토리지 를 선택합니다.



3. S3 홈 페이지에서 Create Bucket(버킷 생성) 을 선택합니다.
4. DNS 호환 이름을 입력하고 버킷을 생성할 지역을 선택합니다.



5. 생성 을 클릭하여 오브젝트 저장소 버킷을 생성합니다.

"다음: ONTAP에 클라우드 계층을 추가합니다"

ONTAP에 클라우드 계층을 추가합니다

오브젝트 저장소를 Aggregate에 첨부하려면 먼저 ONTAP에 추가하여 식별해야 합니다. 이 작업은 OnCommand 시스템 관리자 또는 ONTAP CLI를 사용하여 완료할 수 있습니다.

FabricPool은 Amazon S3, IBM 오브젝트 클라우드 스토리지, Microsoft Azure Blob Storage 오브젝트 저장소를 클라우드 계층으로 지원합니다.

다음 정보가 필요합니다.

- 서버 이름(FQDN)(예: '3.amazonaws.com')
- 액세스 키 ID입니다
- 비밀 키
- 컨테이너 이름(버킷 이름)

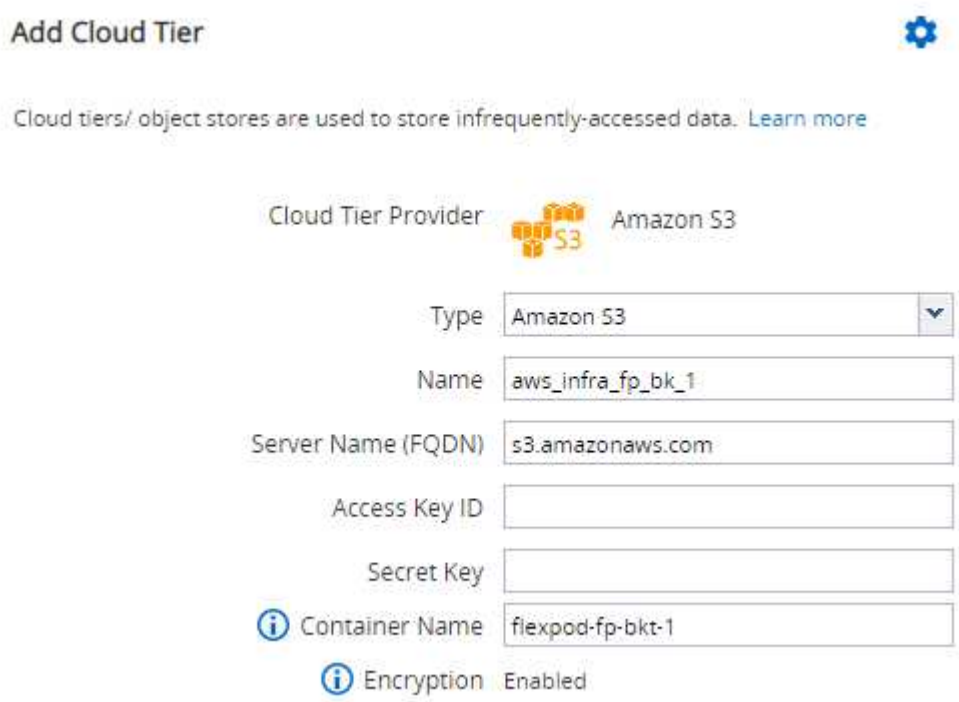
OnCommand 시스템 관리자

OnCommand System Manager를 사용하여 클라우드 계층을 추가하려면 다음 단계를 수행하십시오.

1. OnCommand 시스템 관리자를 시작합니다.
2. 스토리지를 클릭합니다.
3. Aggregate & Disks를 클릭합니다.
4. Cloud Tiers 를 클릭합니다.
5. 오브젝트 저장소 공급자를 선택합니다.
6. 개체 저장소 공급자에 필요한 텍스트 필드를 입력합니다.

   컨테이너 이름 필드에 오브젝트 저장소의 버킷 또는 컨테이너 이름을 입력합니다.

7. Save and Attach Aggregate 를 클릭합니다.



ONTAP CLI를 참조하십시오

ONTAP CLI를 사용하여 클라우드 계층을 추가하려면 다음 명령을 입력합니다.

```
object-store config create
-object-store-name <name>
-provider-type <AWS>
-port <443/8082> (AWS)
-server <name>
-container-name <bucket-name>
-access-key <string>
-secret-password <string>
-ssl-enabled true
-ipspace default
```

"다음: ONTAP 애그리게이트에 클라우드 계층을 연결합니다."

클라우드 계층을 **ONTAP** 애그리게이트에 연결합니다

ONTAP에서 오브젝트 저장소를 추가하고 식별한 후 FabricPool를 생성하려면 오브젝트 저장소를 Aggregate에 연결해야 합니다. 이 작업은 OnCommand 시스템 관리자 또는 ONTAP CLI를 사용하여 완료할 수 있습니다.

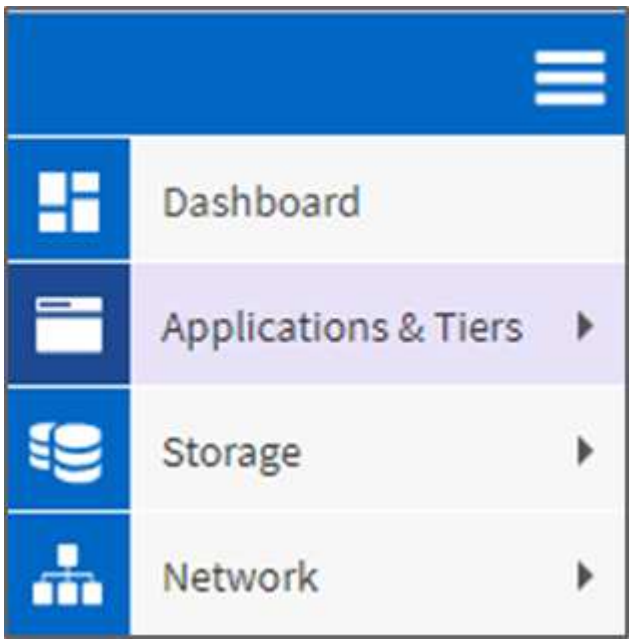
둘 이상의 오브젝트 저장소 유형을 클러스터에 연결할 수 있지만 각 애그리게이트에는 하나의 오브젝트 저장소 유형만 연결할 수 있습니다. 예를 들어, 한 Aggregate는 Google Cloud를 사용할 수 있고 다른 Aggregate는 Amazon S3를 사용할 수 있지만 하나의 Aggregate는 두 곳에 연결할 수 없습니다.

클라우드 계층을 애그리게이트에 연결하는 것은 영구적인 작업입니다. 클라우드 계층은 연결된 애그리게이트로부터 연결 해제할 수 없습니다.

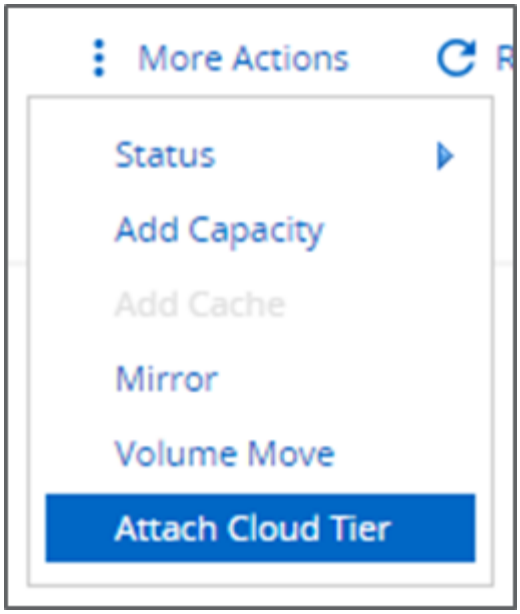
OnCommand 시스템 관리자

OnCommand System Manager를 사용하여 클라우드 계층을 Aggregate에 연결하려면 다음 단계를 수행하십시오.

1. OnCommand 시스템 관리자를 시작합니다.
2. 애플리케이션 및 계층 을 클릭합니다.



3. Storage Tiers를 클릭합니다.
4. Aggregate를 클릭합니다.
5. 작업 을 클릭하고 클라우드 계층 연결 을 선택합니다.



6. 클라우드 계층을 선택합니다.
7. Aggregate의 볼륨에 대한 계층화 정책을 확인하고 업데이트합니다(선택 사항). 기본적으로 볼륨 계층화 정책은 Snapshot 전용 으로 설정됩니다.
8. 저장 을 클릭합니다.

ONTAP CLI를 참조하십시오

ONTAP CLI를 사용하여 클라우드 계층을 애그리게이트에 연결하려면 다음 명령을 실행합니다.

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <name>
```

예:

```
storage aggregate object-store attach -aggregate aggr1 -object-store-name
- aws_infra_fp_bk_1
```

"다음: 볼륨 계층화 정책을 설정합니다."

볼륨 계층화 정책 설정

기본적으로 볼륨은 없음 볼륨 계층화 정책을 사용합니다. 볼륨 생성 후에는 OnCommand 시스템 관리자 또는 ONTAP CLI를 사용하여 볼륨 계층화 정책을 변경할 수 있습니다.

FlexPod와 함께 사용할 경우 FabricPool는 자동, 스냅샷 전용 및 없음이라는 세 가지 볼륨 계층화 정책을 제공합니다.

- * 자동 *

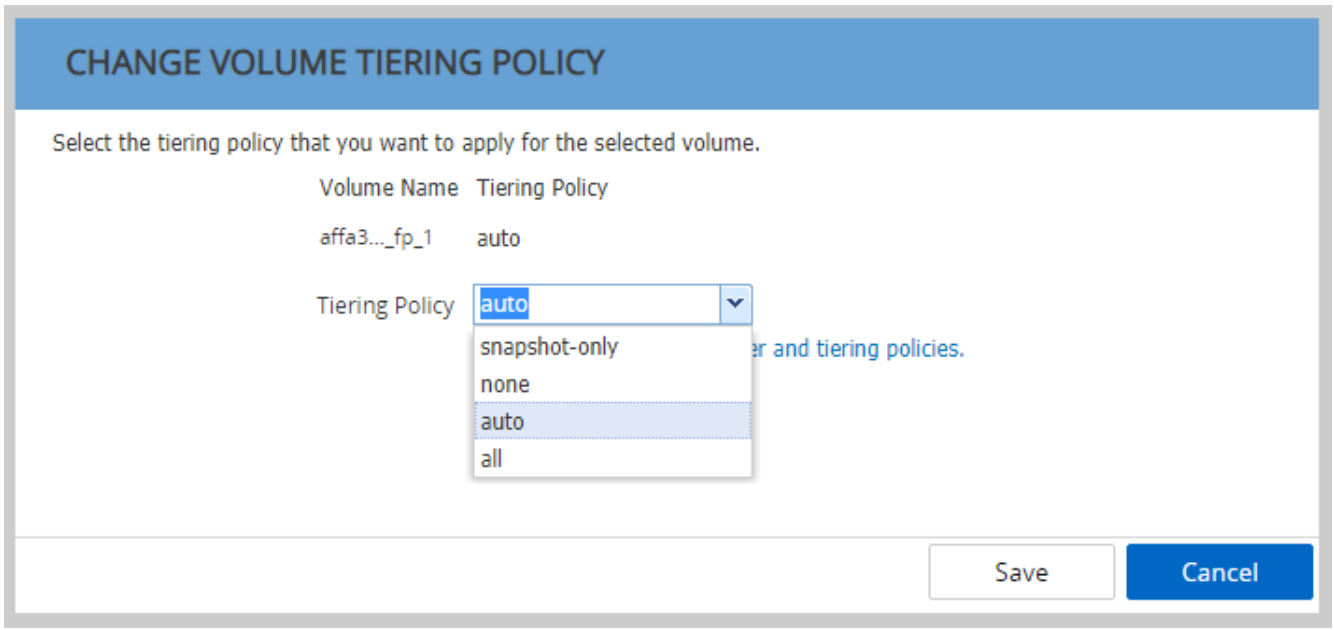
- 볼륨의 모든 콜드 블록이 클라우드 계층으로 이동됩니다. Aggregate가 50% 이상 활용된다고 가정하면 비활성 블록이 콜드 상태가 되는 데 약 31일이 걸립니다. 자동 냉각 기간은 계층화-최소-냉각-일 설정을 사용하여 2일에서 63일 사이에서 조정할 수 있습니다.
- 계층화 정책이 Auto로 설정된 볼륨의 콜드 블록이 무작위로 읽혀지면 핫 블록이 되어 성능 계층에 기록됩니다.
- 계층화 정책이 Auto로 설정된 볼륨의 콜드 블록이 순차적으로 읽으면 콜드 블록이 클라우드 계층에 그대로 유지됩니다. 성능 계층에 기록되지 않습니다.

- * 스냅샷 전용 *
  - 활성 파일 시스템과 공유되지 않는 볼륨의 콜드 스냅샷 블록이 클라우드 계층으로 이동합니다. Aggregate가 50% 이상 활용된다고 가정하면 비활성 스냅샷 블록이 콜드 상태가 되는 데 약 2일이 걸립니다. 스냅샷 전용 냉각 기간은 계층화-최소-냉각-일" 설정을 사용하여 2-63일로 조정할 수 있습니다.
  - 계층화 정책이 Snapshot 전용으로 설정된 볼륨의 콜드 블록을 읽는 경우 핫 블록으로 만들어지고 성능 계층에 기록됩니다.
- * 없음(기본값) *
  - 사용 안 함 으로 설정된 볼륨은 계층화 정책에 따라 콜드 데이터를 클라우드 계층으로 계층화하지 않습니다.
  - 계층화 정책을 없음으로 설정하면 새 계층화가 방지됩니다.
  - 이전에 클라우드 계층으로 이동한 볼륨 데이터는 핫 상태가 되고 성능 계층으로 자동으로 다시 이동될 때까지 클라우드 계층에 그대로 유지됩니다.

OnCommand 시스템 관리자

OnCommand 시스템 관리자를 사용하여 볼륨의 계층화 정책을 변경하려면 다음 단계를 수행하십시오.

1. OnCommand 시스템 관리자를 시작합니다.
2. 볼륨을 선택합니다.
3. 기타 작업 을 클릭하고 계층화 정책 변경 을 선택합니다.
4. 볼륨에 적용할 계층화 정책을 선택합니다.
5. 저장 을 클릭합니다.



ONTAP CLI를 참조하십시오

ONTAP CLI를 사용하여 볼륨의 계층화 정책을 변경하려면 다음 명령을 실행합니다.

```
volume modify -vserver <svm_name> -volume <volume_name>
-tiering-policy <auto|snapshot-only|all|none>
```

"다음: 볼륨 계층화 최소 냉각 기간을 설정합니다."

볼륨 계층화 최소 냉각 일 수 설정

'Tiering-Minimum-Cooling-Days' 설정은 자동 또는 스냅샷 전용 정책을 사용하여 볼륨에 있는 비활성 데이터를 계층화하기에 앞서 경과해야 하는 일 수를 결정합니다.

자동

자동 계층화 정책의 기본 "계층화-최소-냉각-일" 설정은 31일입니다.

읽기 작업은 블록 온도를 고온으로 유지하기 때문에 이 값을 늘리면 계층화할 수 있는 데이터의 양이 줄어들고 성능 계층에 보관되는 데이터의 양이 증가할 수 있습니다.

이 값을 기본값인 31일에서 줄이려면 콜드 으로 표시되기 전에 데이터가 더 이상 활성 상태가 아니어야 합니다. 예를 들어, 여러 날 워크로드가 7일에 상당한 수의 쓰기를 수행할 것으로 예상되는 경우 볼륨의 '계층화-최소-냉각-일' 설정을 8일 이내에 설정해야 합니다.

오브젝트 스토리지는 파일 또는 블록 스토리지와 같은 트랜잭션 중심 스토리지가 아닙니다. 지나치게 공격적인 최소 냉각 일 수를 사용해 볼륨에 객체로 저장된 파일을 변경하면 새 오브젝트가 작성되고 기존 오브젝트가 조각화되고 스토리지 비효율성이 부가될 수 있습니다.

스냅샷 전용

스냅샷 전용 계층화 정책의 기본 '계층화-최소-냉각-일' 설정은 2일입니다. 최소 2일이 지나면 백그라운드 프로세스가 추가 시간을 제공하여 스토리지 효율성을 최대화하고 일상적인 데이터 보호 프로세스에서 클라우드 계층에서 데이터를 읽을 필요가 없도록 합니다.

ONTAP CLI를 참조하십시오

ONTAP CLI를 사용하여 볼륨의 "Tiering-Minimum-Cooling-Days" 설정을 변경하려면 다음 명령을 실행합니다.

```
volume modify -vserver <svm_name> -volume <volume_name> -tiering-minimum
-cooling-days <2-63>
```

고급 권한 수준이 필요합니다.

계층화 정책을 자동 및 스냅샷 전용 간에 또는 그 반대로 변경하면 성능 계층에서 블록의 비활성 기간이 재설정됩니다. 예를 들어, 20일 동안 비활성 상태인 성능 계층의 데이터와 함께 자동 볼륨 계층화 정책을 사용하는 볼륨은 계층화 정책이 스냅샷 전용으로 설정된 경우 성능 계층 데이터 비활성 상태가 0일로 재설정됩니다.

성능 고려 사항

성능 계층 사이징

사이징을 고려할 때 성능 계층은 다음 작업을 수행할 수 있어야 합니다.

- 핫 데이터 지원
- 계층화 검사가 데이터를 클라우드 계층으로 이동할 때까지 콜드 데이터를 지원합니다
- 핫 상태가 되고 성능 계층에 다시 기록되는 클라우드 계층 데이터 지원
- 연결된 클라우드 계층과 연결된 WAFL 메타데이터 지원

대부분의 환경에서 FabricPool 애그리게이트에서 1:10 성능/용량 비율은 매우 보수적인 반면 스토리지는 상당히 절약됩니다. 예를 들어, 200TB를 클라우드 계층에 계층화하려는 경우 성능 계층 애그리게이트는 최소한 20TB여야 합니다.



성능 계층 용량이 70%를 초과하는 경우 클라우드 계층에서 성능 계층으로 쓰기 작업이 해제됩니다. 이 경우 블록이 클라우드 계층에서 직접 읽힙니다.

클라우드 계층 사이징

사이징을 고려할 때 클라우드 계층 역할을 하는 오브젝트 저장소는 다음 작업을 수행할 수 있어야 합니다.

- 기존 콜드 데이터 읽기 지원
- 새로운 콜드 데이터 쓰기 지원
- 개체 삭제 및 조각 모음을 지원합니다

소유 비용

를 클릭합니다 "FabricPool 경제 계산기" 는 독립 IT 분석 기업인 Evaluator Group을 통해 사용 가능하여 사내 및 클라우드 간 콜드 데이터 스토리지 비용 절감을 프로젝트에 사용할 수 있습니다. 계산기는 자주 액세스하지 않는 데이터를 성능 계층에 저장하는 비용과 나머지 데이터 라이프사이클 동안 클라우드 계층으로 보내는 비용을 확인하기 위한 간단한 인터페이스를 제공합니다. 5년간의 계산을 기준으로 소스 용량, 데이터 증가, 스냅샷 용량 및 콜드 데이터의 비율이라는 4가지 주요 요소를 사용하여 해당 기간에 따른 스토리지 비용을 결정합니다.

결론

클라우드로의 전환 여정은 조직, 부서 간, 조직 내의 부서 간에도 다양합니다. 어떤 사람들은 빠른 도입을 선택하기도 하고, 어떤 사람들은 보다 보수적인 접근 방식을 택하기도 합니다. FabricPool은 조직의 규모와 클라우드의 채택 속도에 상관없이 기업의 클라우드 전략에 적합하며, FlexPod 인프라의 효율성 및 확장성 이점을 추가로 보여줍니다.

추가 정보를 찾을 수 있는 위치

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

- FabricPool 모범 사례

  "www.netapp.com/us/media/tr-4598.pdf"

- NetApp 제품 설명서

  "https://docs.netapp.com"

- TR-4036: FlexPod 데이터 센터 기술 사양

  "https://www.netapp.com/us/media/tr-4036.pdf"

Cisco CloudCenter 및 NetApp 프라이빗 스토리지를 사용하는 하이브리드 클라우드용 FlexPod 데이터 센터 - 설계

Haseeb Niazi, Cisco David Arnette, NetApp

CVD(Cisco Validated Design)는 고객 구현을 촉진하고 개선하기 위해 설계, 테스트 및 문서화된 시스템 및 솔루션을 제공합니다. 이러한 설계는 고객의 비즈니스 요구를 해결하고 설계부터 배포까지 안내하기 위해 개발된 솔루션 포트폴리오에 광범위한 기술과 제품을 통합합니다.

"Cisco CloudCenter 및 NetApp 프라이빗 스토리지를 사용하는 하이브리드 클라우드용 FlexPod 데이터 센터 - 설계"

엔터프라이즈 데이터베이스

제공합니다

FlexPod 기반 SAP 소개

FlexPod 플랫폼은 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 스위치 제품군, NetApp 스토리지 컨트롤러를 기반으로 사전 설계되고 모범 사례 데이터 센터 아키텍처를 제공합니다.

FlexPod는 SAP 애플리케이션 실행에 적합한 플랫폼이며, 여기에 제공된 솔루션을 사용하여 맞춤형 데이터 센터 통합 모델을 통해 SAP HANA를 빠르고 안정적으로 구축할 수 있습니다. FlexPod는 기본 구성뿐만 아니라 다양한 사용 사례와 요구사항에 맞게 사이징 및 최적화할 수 있는 유연성도 제공합니다.

파이버 채널 SAN과 Cisco UCS Manager 4.0 및 NetApp ONTAP 9.7을 사용하는 SAP용 FlexPod 데이터 센터 솔루션

Pramod Ramamurhy, Cisco Marco Schoen, NetApp

이 문서에서는 NetApp AFF A400 스토리지 기반 NetApp ONTAP 9.7을 지원하는 Cisco 및 NetApp FlexPod 데이터 센터와 SAP HANA용 2세대 인텔 제온 스케일러블 프로세서가 포함된 Cisco UCS Manager 유니파이드 소프트웨어 릴리스 4.1(1)에 대해 설명합니다.

NetApp ONTAP 9.7 및 Cisco UCS 통합 소프트웨어 릴리스 4.1(1)이 포함된 FlexPod 데이터 센터는 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 9000 스위치 제품군, MDS 9000 멀티레이어 패브릭 스위치, ONTAP 9.7 스토리지 OS를 실행하는 NetApp AFF A 시리즈 스토리지 어레이를 살펴봅니다.

"파이버 채널 SAN과 Cisco UCS Manager 4.0 및 NetApp ONTAP 9.7을 사용하는 SAP용 FlexPod 데이터 센터 솔루션"

SAP 비 HANA with SQL 백서 - 설계

현재 IT 업계에서 데이터 센터 솔루션의 획기적인 변화가 목격되고 있습니다. 최근 몇 년간 사전 검증되고 엔지니어링된 데이터 센터 솔루션에 상당한 관심이 있었습니다. 중요 영역에 가상화 기술을 도입함으로써 이러한 솔루션의 설계 원칙과 아키텍처에 상당한 영향을 미쳤습니다. 따라서 베어 메탈 시스템에서 실행 중인 많은 애플리케이션을 새로운 가상화 통합 솔루션으로 마이그레이션할 수 있었습니다. FlexPod는 IT 부서의 빠르게 변화하는 요구사항을 해결하기 위해 사전 검증되고 엔지니어링된 데이터 센터 솔루션 중 하나입니다. Cisco와 NetApp은 파트너십을 통해 데이터베이스, ERP(전사적 자원 관리), CRM(고객 관계 관리) 및 웹 애플리케이션을 포함한 다양한 엔터프라이즈 워크로드를 위한 기반으로 동급 최고의 컴퓨팅, 네트워킹 및 스토리지 구성요소를 사용하는 FlexPod를 제공하고 있습니다.

IT 애플리케이션, 특히 데이터베이스의 통합은 최근 몇 년 동안 상당한 관심을 불러왔습니다. 지난 몇 년 동안 가장 널리 채택되고 배포된 데이터베이스 플랫폼은 Microsoft SQL Server입니다. SQL Server 데이터베이스는 종종 데이터베이스의 무분별한 확장을 수반하며, 이에 따라 서버 활용도가 낮은 문제, 잘못된 라이센싱, 보안 문제, 관리 문제, 막대한 운영 비용 등과 같은 IT 과제도 발생합니다. 따라서 SQL Server 데이터베이스는 보다 강력하고 유연하며 복원력이 뛰어난 플랫폼에 통합할 수 있는 적합합니다. 이 문서에서는 SQL Server 데이터베이스의 배포 및 통합을 위한 FlexPod 참조 아키텍처에 대해 설명합니다.

"SAP 비 HANA with SQL 백서 - 설계"

Cisco UCS 3세대 패브릭 및 NetApp AFF A-Series가 지원되는 SAP 솔루션용 FlexPod 데이터 센터

Pramod Ramamurhy, Cisco Marco Schoen, NetApp

이 문서에서는 지원되는 2세대 인텔 제온 스케일러블 프로세서 기반 SAP HANA용 Cisco 및 NetApp FlexPod 데이터 센터의 구현 방법에 대해 설명합니다.

Cisco UCS Manager(UCSM) 4.0(4)은 현재 모든 Cisco UCS Fabric Interconnect 모델(6200, 6300, 6324 및 6454), 2200/2300 시리즈 IOM, Cisco UCS B-Series 블레이드, Cisco UCS C-Series 랙 폼 팩터 서버를 통합 지원합니다. Cisco UCS 통합 소프트웨어 릴리스 4.0(4D) 및 NetApp ONTAP 9.6을 사용하는 FlexPod 데이터 센터는 Cisco UCS, Cisco Nexus 9000 스위치 제품군 및 NetApp AFF A 시리즈 스토리지 어레이를 기반으로 사전 설계된 모범 사례 데이터 센터 아키텍처입니다.

"Cisco UCS 3세대 패브릭 및 NetApp AFF A-Series가 지원되는 SAP 솔루션용 FlexPod 데이터 센터"

파이버 채널 SAN과 Cisco UCS Manager 4.0 및 NetApp ONTAP 9.7-Design을 사용하는 SAP용 FlexPod 데이터 센터 솔루션

Pramod Ramamurhy, Cisco Marco Schoen, NetApp

Cisco와 NetApp은 전략적 데이터 센터 플랫폼을 지원하는 일련의 FlexPod 솔루션을 제공하기 위해 협력하고 있습니다. FlexPod 솔루션은 컴퓨팅, 스토리지 및 네트워크 설계 모범 사례를 통합하는 통합 아키텍처를 제공하므로 다양한 구성 요소 간의 호환성을 보장하기 위해 통합 아키텍처를 검증하여 IT 위험을 최소화할 수 있습니다. 또한 이 솔루션은 배포의 다양한 단계(계획, 설계 및 구현)에서 사용할 수 있는 문서화된 설계 지침, 배포 지침 및 지원을 제공하여 IT 당면 과제를 해결합니다.

"파이버 채널 SAN과 Cisco UCS Manager 4.0 및 NetApp ONTAP 9.7-Design을 사용하는 SAP용 FlexPod 데이터 센터 솔루션"

Cisco ACI, Cisco UCS Manager 4.0 및 NetApp AFF A-Series-Design이 포함된 SAP용 FlexPod 데이터 센터 솔루션

Pramod Ramamurhy, Cisco Marco Schoen, NetApp

이 문서에서는 SAP HANA TDI(Tailored Data Center Integration) 환경을 구축하기 위한 검증된 접근 방법으로 Cisco ACI 통합 FlexPod 솔루션에 대해 설명합니다. 검증된 이 설계는 Cisco 및 NetApp의 모범 사례를 바탕으로 SAP HANA를 구축하기 위한 지침과 프레임워크를 제공합니다.

권장되는 솔루션 아키텍처는 Cisco UCS(Unified Computing System)에서 다음 구성 요소가 포함된 Cisco UCS 하드웨어 플랫폼을 지원하는 통합 소프트웨어 릴리즈를 사용합니다.

- Intel Optane Data Center DCPMM(Persistent Memory Module) 옵션으로 구성할 수 있는 Cisco UCS B-Series 블레이드 서버 및 Cisco UCS C-Series 랙 서버
- Cisco UCS 6400 시리즈 패브릭 인터커넥트

- Cisco Nexus 9000 Series Leaf 및 Spine 스위치
- NetApp All Flash 시리즈 스토리지 어레이를 제공할 좋은 기회입니다

또한 이 문서에서는 Red Hat Enterprise Linux 및 SAP HANA용 SUSE Linux Enterprise Server 모두에 대한 검증을 제공합니다.

"Cisco ACI, Cisco UCS Manager 4.0 및 NetApp AFF A-Series-Design이 포함된 SAP용 FlexPod 데이터 센터 솔루션"

Cisco ACI, Cisco UCS Manager 4.0 및 NetApp AFF A-Series-Deployment가 있는 SAP용 FlexPod 데이터 센터

Pramod Ramamurhy, Cisco Marco Schoen, NetApp

이 문서에서는 FlexPod 인프라의 SAP HANA 맞춤형 데이터 센터 통합 옵션에 대한 아키텍처 및 구축 절차를 설명합니다. 이 옵션은 다음과 같이 구성되어 있습니다.

- 2세대 인텔 제온 스케일러블 프로세서가 지원하는 Cisco UCS(Cisco UCS)
- Cisco ACI(Application Centric Infrastructure)를 활용하는 스위칭 제품
- NetApp A-Series AFF 어레이를 제공할 좋은 기회입니다.

이 문서는 SAP HANA 구축에 대한 자세한 구성 단계를 보여주는 것입니다

"Cisco ACI, Cisco UCS Manager 4.0 및 NetApp AFF A-Series-Deployment가 있는 SAP용 FlexPod 데이터 센터"

Cisco UCS Manager 4.0 및 NetApp AFF A-Series-Design을 사용하는 SAP 솔루션용 FlexPod 데이터 센터

Pramod Ramamurhy, Cisco Marco Schoen, NetApp

이 문서에서는 SAP HANA TDI(Tailored Data Center Integration) 환경을 구축하기 위해 검증된 접근 방식인 Cisco 및 NetApp FlexPod 솔루션에 대해 설명합니다. 검증된 이 설계는 Cisco 및 NetApp의 모범 사례를 바탕으로 SAP HANA를 구축하기 위한 지침과 프레임워크를 제공합니다.

FlexPod은 광범위한 엔터프라이즈 워크로드 및 사용 사례를 지원하는 업계 최고의 통합 인프라입니다. 이 솔루션을 사용하면 맞춤형 데이터 센터 통합 모드 모델을 통해 SAP HANA를 빠르고 안정적으로 구축할 수 있습니다.

"Cisco UCS Manager 4.0 및 NetApp AFF A-Series-Design을 사용하는 SAP 솔루션용 FlexPod 데이터 센터"

SLES 12 SP3 및 RHEL 7.4가 설치된 Cisco UCS M5 서버에서 Cisco ACI를 지원하는 SAP용 FlexPod Datacenter 솔루션

Pramod Ramamurhy, Cisco Marco Schoen, NetApp

이 문서에서는 업계 최고의 SDN(소프트웨어 정의 네트워킹 솔루션)인 Cisco ACI(Application Centric Infrastructure)를 활용하는 Cisco 컴퓨팅 및 스위칭 제품으로 구성된 FlexPod 인프라의 SAP HANA 맞춤형 데이터 센터 통합 옵션과 NetApp A 시리즈 AFF 어레이에 대한 아키텍처 및

구축 절차를 설명합니다. 이 문서의 목적은 SAP HANA 구축에 대한 자세한 구성 단계와 함께 설계 원칙을 보여주는 것입니다.

"SLES 12 SP3 및 RHEL 7.4가 설치된 Cisco UCS M5 서버에서 Cisco ACI를 지원하는 SAP용 FlexPod Datacenter 솔루션"

NetApp AFF A-Series 및 Cisco UCS Manager 3.2를 사용하는 IP 기반 스토리지가 있는 SAP용 FlexPod 데이터 센터 솔루션

Shailendra Munrunjaya, Cisco Ralf Klahr, Cisco Marco Schoen, NetApp

이 문서에 자세히 설명된 참조 아키텍처는 IP 기반 스토리지 솔루션의 복원력, 비용 이점 및 간편한 구축에 대해 중점적으로 설명합니다. 단일 인터페이스에서 여러 프로토콜을 지원할 수 있는 스토리지 시스템은 사용자가 직접 선택할 수 있고 실제로 유선 연결 아키텍처이기 때문에 투자를 보호할 수 있습니다. 이 솔루션은 확장 가능한 SAP HANA 워크로드를 호스팅하도록 설계되었습니다.

"NetApp AFF A-Series 및 Cisco UCS Manager 3.2를 사용하는 IP 기반 스토리지가 있는 SAP용 FlexPod 데이터 센터 솔루션"

파이버 채널 SAN과 Cisco UCS Manager 4.0 및 NetApp ONTAP 9.7을 사용하는 SAP용 FlexPod 데이터 센터 솔루션

Pramod Ramamurhy, Cisco Marco Schoen, NetApp

이 문서에서는 NetApp AFF A400 스토리지 기반 NetApp ONTAP 9.7을 지원하는 Cisco 및 NetApp FlexPod 데이터 센터와 SAP HANA용 2세대 인텔 제온 스케일러블 프로세서가 포함된 Cisco UCS Manager 유니파이드 소프트웨어 릴리스 4.1(1)에 대해 설명합니다.

NetApp ONTAP 9.7 및 Cisco UCS 통합 소프트웨어 릴리스 4.1(1)이 포함된 FlexPod 데이터 센터는 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 9000 스위치 제품군, MDS 9000 멀티레이어 패브릭 스위치, ONTAP 9.7 스토리지 OS를 실행하는 NetApp AFF A 시리즈 스토리지 어레이를 살펴봅니다.

"파이버 채널 SAN과 Cisco UCS Manager 4.0 및 NetApp ONTAP 9.7을 사용하는 SAP용 FlexPod 데이터 센터 솔루션"

FlexPod with SQL에 SAP 애플리케이션 서버 구축

FlexPod는 IT 부서의 빠르게 변화하는 요구사항을 충족하도록 설계된 사전 검증되고 엔지니어링된 데이터 센터 솔루션입니다. Cisco와 NetApp은 파트너십을 통해 데이터베이스, ERP(전사적 자원 관리), CRM(고객 관계 관리) 및 웹 애플리케이션을 포함한 다양한 엔터프라이즈 워크로드를 위한 기반으로 동급 최고의 컴퓨팅, 네트워킹 및 스토리지 구성요소를 사용하는 FlexPod를 제공합니다. IT 애플리케이션, 특히 데이터베이스의 통합은 최근 몇 년 동안 상당한 관심을 불러왔습니다. 지난 몇 년 동안 가장 널리 채택되고 배포된 데이터베이스 플랫폼은 Microsoft SQL Server입니다. SQL Server 데이터베이스는 종종 데이터베이스의 무분별한 확장을 수반하며, 이에 따라 서버 활용도가 낮은 문제, 잘못된 라이센싱, 보안 문제, 관리 문제, 막대한 운영 비용 등과 같은 IT 과제도 발생합니다. 따라서 SQL Server 데이터베이스는 보다 강력하고 유연하며 복원력이 뛰어난 플랫폼에 통합할 수 있는 적합합니다. 이 문서에서는 SQL

Server 데이터베이스의 배포 및 통합을 위한 FlexPod 참조 아키텍처에 대해 설명합니다.

"FlexPod with SQL에 SAP 애플리케이션 서버 구축"

Cisco ACI, Cisco UCS Manager 4.0 및 NetApp AFF A-Series가 지원되는 SAP용 FlexPod 데이터 센터

Pramod Ramamurhy, Cisco Marco Schoen, NetApp

이 문서에서는 FlexPod 인프라의 SAP HANA 맞춤형 데이터 센터 통합 옵션에 대한 아키텍처 및 구축 절차를 설명합니다. 이 옵션은 다음과 같이 구성되어 있습니다.

- 2세대 인텔 제온 스케일러블 프로세서가 지원하는 Cisco UCS(Cisco UCS)
- Cisco ACI(Application Centric Infrastructure)를 활용하는 스위칭 제품
- NetApp A-Series AFF 어레이를 제공할 좋은 기회입니다.

"Cisco ACI, Cisco UCS Manager 4.0 및 NetApp AFF A-Series가 지원되는 SAP용 FlexPod 데이터 센터"

Cisco ACI, Cisco UCS Manager 4.0 및 NetApp AFF A-Series-Design이 포함된 SAP용 FlexPod 데이터 센터 솔루션

Pramod Ramamurhy, Cisco Marco Schoen, NetApp

이 문서에서는 SAP HANA TDI(Tailored Data Center Integration) 환경을 구축하기 위한 검증된 접근 방법으로 Cisco ACI 통합 FlexPod 솔루션에 대해 설명합니다. 검증된 이 설계는 Cisco 및 NetApp의 모범 사례를 바탕으로 SAP HANA를 구축하기 위한 지침과 프레임워크를 제공합니다.

권장되는 솔루션 아키텍처는 Cisco UCS(Unified Computing System)에서 다음 구성 요소가 포함된 Cisco UCS 하드웨어 플랫폼을 지원하는 통합 소프트웨어 릴리즈를 사용합니다.

- Intel Optane Data Center DCPMM(Persistent Memory Module) 옵션으로 구성할 수 있는 Cisco UCS B-Series 블레이드 서버 및 Cisco UCS C-Series 랙 서버
- Cisco UCS 6400 시리즈 패브릭 인터커넥트
- Cisco Nexus 9000 Series Leaf 및 Spine 스위치
- NetApp All Flash 시리즈 스토리지 어레이를 제공할 좋은 기회입니다

또한 이 문서에서는 Red Hat Enterprise Linux 및 SAP HANA용 SUSE Linux Enterprise Server 모두에 대한 검증을 제공합니다.

"Cisco ACI, Cisco UCS Manager 4.0 및 NetApp AFF A-Series-Design이 포함된 SAP용 FlexPod 데이터 센터 솔루션"

Cisco UCS 3세대 패브릭 및 NetApp AFF A-Series가 지원되는 SAP용 FlexPod 데이터 센터 솔루션

Shailendra Munrunjaya, Cisco Ralf Klahr, Cisco Marco Schoen, NetApp

이 문서에서는 2세대 인텔 제온 스케일러블 프로세서가 지원하는 Cisco UCS(Cisco UCS) 기반 SAP HANA용 Cisco 및 NetApp FlexPod 데이터 센터의 구축 방법에 대해 설명합니다.

Cisco UCS Manager(UCSM) 4.0(4)은 현재 모든 Cisco UCS Fabric Interconnect 모델(6200, 6300, 6324 및 6454), 2200/2300 시리즈 IOM, Cisco UCS B-Series 블레이드, Cisco UCS C-Series 랙 폼 팩터 서버를 통합 지원합니다. Cisco UCS 통합 소프트웨어 릴리스 4.0(4D) 및 NetApp ONTAP 9.6을 사용하는 FlexPod 데이터 센터는 Cisco UCS, Cisco Nexus 9000 스위치 제품군 및 NetApp AFF A 시리즈 스토리지 어레이를 기반으로 하는 사전 설계식 모범 사례 데이터 센터 아키텍처입니다.

"Cisco UCS 3세대 패브릭 및 NetApp AFF A-Series가 지원되는 SAP용 FlexPod 데이터 센터 솔루션"

Cisco UCS Manager 4.0 및 **NetApp AFF A-Series-Design**을 사용하는 **SAP**용 **FlexPod** 데이터 센터 솔루션

Pramod Ramamurhy, Cisco Marco Schoen, NetApp

이 문서에서는 SAP HANA TDI(Tailored Data Center Integration) 환경을 구축하기 위해 검증된 접근 방식인 Cisco 및 NetApp FlexPod 솔루션에 대해 설명합니다. 검증된 이 설계는 Cisco 및 NetApp의 모범 사례를 바탕으로 SAP HANA를 구축하기 위한 지침과 프레임워크를 제공합니다.

FlexPod은 광범위한 엔터프라이즈 워크로드 및 사용 사례를 지원하는 업계 최고의 통합 인프라입니다. 이 솔루션을 사용하면 맞춤형 데이터 센터 통합 모드 모델을 통해 SAP HANA를 빠르고 안정적으로 구축할 수 있습니다.

권장되는 솔루션 아키텍처는 Cisco UCS(Unified Computing System)에서 다음 구성 요소가 포함된 Cisco UCS 하드웨어 플랫폼을 지원하는 통합 소프트웨어 릴리즈를 사용합니다.

- Cisco UCS B-Series 블레이드 서버 및 Cisco UCS C-Series 랙 서버는 Intel Optane Data Center DCPMM(Persistent Memory Module) 옵션으로 구성할 수 있습니다
- Cisco UCS 6300 시리즈 Fabric Interconnect
- Cisco Nexus 9000 시리즈 스위치
- NetApp All Flash 시리즈 스토리지 어레이를 제공할 좋은 기회입니다

또한 이 문서에서는 Red Hat Enterprise Linux 및 SAP HANA용 SUSE Linux Enterprise Server 모두에 대한 유효성 검사를 제공합니다.

"Cisco UCS Manager 4.0 및 NetApp AFF A-Series-Design을 사용하는 SAP용 FlexPod 데이터 센터 솔루션"

오라클

Cisco UCS 및 **NetApp AFF A-Series**에서 **Oracle RAC** 데이터베이스가 지원되는 **FlexPod** 데이터 센터

Tushar Patel, Cisco Hardikkumar Vyas

Cisco의 검증된 설계에는 고객 배포를 촉진하고 개선하기 위해 설계, 테스트 및 문서화된 시스템 및 솔루션이 포함됩니다. 이러한 설계는 고객의 비즈니스 요구를 해결하기 위해 개발된 솔루션 포트폴리오에 광범위한 기술과 제품을 통합합니다. Cisco와 NetApp은 파트너십을 통해

FlexPod 다양한 워크로드의 기반 역할을 하며 고객 요구사항을 기반으로 효율적인 아키텍처 설계를 지원합니다. FlexPod 솔루션은 Cisco 및 NetApp 기술을 공유 클라우드 인프라로 구축하기 위한 검증된 접근 방식입니다.

NetApp All Flash AFF 시스템을 지원하는 FlexPod 데이터 센터는 Cisco와 NetApp의 동급 최고 기술을 엔터프라이즈 애플리케이션을 위한 강력한 통합 플랫폼으로 결합하는 통합 인프라 플랫폼입니다. Cisco와 NetApp은 Oracle과 긴밀하게 협력하여 오늘날의 비즈니스에 필요한 가장 까다로운 트랜잭션 및 응답 시간에 민감한 데이터베이스를 지원합니다.

CVD(Cisco Validated Design)에서는 고가용성 Oracle RAC 데이터베이스 환경을 구축하기 위해 Cisco UCS 및 NetApp All Flash AFF 스토리지를 사용하는 참조 FlexPod 데이터 센터 아키텍처에 대해 설명합니다. 이 문서에서는 관련된 구성 요소의 하드웨어 및 소프트웨어 구성과 다양한 테스트 결과를 보여 줍니다. 또한 Cisco UCS 컴퓨팅 서버, Cisco Fabric Interconnect 스위치, Cisco MDS 스위치, Cisco Nexus 스위치, NetApp AFF 스토리지 및 Oracle RAC 데이터베이스를 사용하는 구현 및 모범 사례 지침을 제공합니다.

"Cisco UCS 및 NetApp AFF A-Series에서 Oracle RAC 데이터베이스가 지원되는 FlexPod 데이터 센터"

Oracle Linux 기반 **Oracle RAC** 지원 **FlexPod** 데이터 센터

Tushar Patel, Cisco Niranjan Mohapatra, Cisco John Elliott, NetApp

Cisco UCS(Cisco Unified Computing System)는 컴퓨팅, 네트워크, 스토리지 액세스 및 가상화를 하나의 통합 시스템으로 통합하는 차세대 데이터 센터 플랫폼입니다. Cisco UCS는 미션 크리티컬 데이터베이스 워크로드의 아키텍처에 이상적인 플랫폼입니다. Cisco UCS 플랫폼, NetApp 스토리지 및 Oracle RAC(Real Application Cluster) 아키텍처를 결합하면 더욱 신속한 구축, 더욱 폭넓은 선택의 유연성, 효율성 및 낮은 위험을 지원하여 IT 혁신을 가속할 수 있습니다. CVD(Cisco Validated Design)에서는 Oracle 12c RAC 데이터베이스를 지원하는 유연한 멀티 테넌트, 고성능 및 복원력을 갖춘 FlexPod 참조 아키텍처를 중점적으로 다룹니다.

NetApp과 Cisco가 개발한 FlexPod 플랫폼은 사전 검증된 스토리지, 네트워킹 및 서버 기술을 제공하는 유연한 통합 인프라 솔루션입니다. 이 제품은 전반적인 컴퓨팅 비용을 절감하면서 비즈니스 요구에 대한 IT의 응답 속도를 높이도록 설계되었습니다. 가동 시간을 최대화하고 위험은 최소화하십시오. FlexPod 구성요소는 시기적절하고 반복 가능하며 일관된 구현을 지원하도록 통합되고 표준화되었습니다. 각 FlexPod 배포의 전력, 설치 공간, 사용 가능 용량, 성능 및 비용을 정확하게 계획할 수 있습니다.

FlexPod는 최신 기술을 수용하고 데이터 센터의 워크로드를 효율적으로 단순화하여 IT의 가치 제공 방식을 재정의합니다.

- Flash Pool 플래시가 포함된 NetApp FAS 하이브리드 어레이의 기능을 활용하여 특정 애플리케이션 또는 환경을 위한 회전식 미디어와 플래시를 정확한 비율로 구축하는 기능을 제공합니다.
- 사전 검증된 플랫폼을 활용하여 비즈니스 중단을 최소화하고 IT 민첩성을 높이며 구축 시간을 몇 개월에서 몇 주로 단축합니다.
- 관리 시간과 TCO(총 소유 비용)를 50% 절감할 수 있습니다.
- 데이터 센터 워크로드에 대한 하드웨어 성능 요구사항을 지속적으로 충족하거나 초과 충족합니다.

"Oracle Linux 기반 Oracle RAC 지원 FlexPod 데이터 센터"

Cisco UCS 및 NetApp AFF A-Series에서 Oracle RAC 데이터베이스가 지원되는 FlexPod 데이터 센터

Tushar Patel, Cisco Hardikkumar Vyas

NetApp All Flash AFF 시스템을 지원하는 FlexPod 데이터 센터는 Cisco와 NetApp의 동급 최고 기술을 엔터프라이즈 애플리케이션을 위한 강력한 통합 플랫폼으로 결합하는 통합 인프라 플랫폼입니다. Cisco와 NetApp은 Oracle과 긴밀하게 협력하여 오늘날의 비즈니스에 필요한 가장 까다로운 트랜잭션 및 응답 시간에 민감한 데이터베이스를 지원합니다.

CVD(Cisco Validated Design)에서는 고가용성 Oracle RAC 데이터베이스 환경을 구축하기 위해 Cisco UCS 및 NetApp All Flash AFF 스토리지를 사용하는 참조 FlexPod 데이터 센터 아키텍처에 대해 설명합니다. 이 문서에서는 관련된 구성 요소의 하드웨어 및 소프트웨어 구성과 다양한 테스트 결과를 보여 줍니다. 또한 Cisco UCS 컴퓨팅 서버, Cisco Fabric Interconnect 스위치, Cisco MDS 스위치, Cisco Nexus 스위치, NetApp AFF 스토리지 및 Oracle RAC 데이터베이스를 사용하는 구현 및 모범 사례 지침을 제공합니다.

"Cisco UCS 및 NetApp AFF A-Series에서 Oracle RAC 데이터베이스가 지원되는 FlexPod 데이터 센터"

Microsoft SQL Server를 참조하십시오

Microsoft SQL Server 2019 및 VMware vSphere 6.7용 FlexPod 데이터 센터

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Bhalodia, NetApp

이 문서에서는 최신 하드웨어 및 소프트웨어 제품을 사용하는 FlexPod 참조 아키텍처에 대해 설명하고 VMware ESXi 가상화 환경에서 Microsoft SQL Server 2019 데이터베이스를 호스팅하기 위한 구축 권장 사항을 제공합니다. 또한 이 솔루션은 Cisco CWOM(Workload Optimization Manager)을 사용하여 SQL 워크로드와 인프라 모두에서 최적의 효율적인 리소스 활용을 위한 자동화된 권장 사항을 제공합니다.

유니파이드 소프트웨어 릴리스 4.1.1c를 사용하여 Cisco UCS(Cisco Unified Computing System)를 기반으로 Cisco UCS B-Series 블레이드 서버, Cisco UCS 6400 패브릭 인터커넥트, Cisco Nexus 9000 시리즈 스위치, NetApp AFF 시리즈 스토리지 어레이 등 Cisco UCS 하드웨어 플랫폼을 지원합니다.

"Microsoft SQL Server 2019 및 VMware vSphere 6.7용 FlexPod 데이터 센터"

Microsoft SQL Server 2016 및 VMware vSphere 6.5가 설치된 FlexPod Datacenter

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco David Arnette, NetApp

이 문서에서는 최신 하드웨어 및 소프트웨어 제품을 사용하는 FlexPod 참조 아키텍처에 대해 설명하고 가상화된 환경에서 Microsoft SQL Server 데이터베이스를 구축하기 위한 구성 권장 사항을 제공합니다.

권장되는 솔루션 아키텍처는 Cisco UCS(Cisco Unified Computing System) 기반 Cisco UCS와 함께 유니파이드 소프트웨어 릴리즈를 사용하여 Cisco UCS B-Series 블레이드 서버, Cisco UCS 6300 Fabric Interconnect, Cisco Nexus 9000 시리즈 스위치, NetApp All Flash Series 스토리지 어레이를 포함한 Cisco UCS 하드웨어 플랫폼을 지원합니다. 또한 이 솔루션에는 VMware vSphere 6.5, vSphere 6.5가 포함되어 있어 스토리지 활용을 최적화하고 프라이빗 클라우드를 지원하는 다양한 새로운 기능을 제공합니다.

"Microsoft SQL Server 2016 및 VMware vSphere 6.5가 설치된 FlexPod Datacenter"

VMware 및 **Hyper-V**에서 실행되는 **Linux VM**에서 **Microsoft SQL Server 2017**을 지원하는 **FlexPod** 데이터 센터

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Bhalodia, NetApp

이 문서에서는 최신 하드웨어 및 소프트웨어 제품을 사용하는 FlexPod 참조 아키텍처에 대해 설명하고, SQL Server 배포를 위한 Microsoft의 Linux 지원을 통해 VMware ESXi 및 Microsoft Windows Hyper-V 가상화 환경에서 Microsoft SQL Server 데이터베이스를 호스팅하기 위한 배포 권장 사항을 제공합니다.

권장되는 솔루션 아키텍처는 통합 소프트웨어 릴리즈 4.0.1c를 사용하는 Cisco UCS(Cisco Unified Computing System)를 기반으로 Cisco UCS B-Series 블레이드 서버, Cisco UCS 6300 Fabric Interconnect, Cisco Nexus 9000 시리즈 스위치, NetApp AFF 시리즈 스토리지 어레이를 포함한 Cisco UCS 하드웨어 플랫폼을 지원합니다.

"VMware 및 Hyper-V에서 실행되는 Linux VM에서 Microsoft SQL Server 2017을 지원하는 FlexPod 데이터 센터"

VMware 및 **Hyper-V**에서 실행되는 **Linux VM**에서 **Microsoft SQL Server 2017**을 지원하는 **FlexPod** 데이터 센터

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Bhalodia, NetApp

이 문서에서는 최신 하드웨어 및 소프트웨어 제품을 사용하는 FlexPod 참조 아키텍처에 대해 설명하고, SQL Server 배포를 위한 Microsoft의 Linux 지원을 통해 VMware ESXi 및 Microsoft Windows Hyper-V 가상화 환경에서 Microsoft SQL Server 데이터베이스를 호스팅하기 위한 배포 권장 사항을 제공합니다.

권장 솔루션 아키텍처는 Cisco UCS(Cisco Unified Computing System) 기반 위에 구축된 유니파이드 소프트웨어 릴리즈 4.0.1c를 사용하여 Cisco UCS B-Series 블레이드 서버, Cisco UCS 6300 패브릭 인터커넥트, Cisco Nexus 9000 시리즈 스위치, NetApp AFF 시리즈 스토리지 어레이 등 Cisco UCS 하드웨어 플랫폼을 지원합니다.

"VMware 및 Hyper-V에서 실행되는 Linux VM에서 Microsoft SQL Server 2017을 지원하는 FlexPod 데이터 센터"

의료

유전체학을 위한 **FlexPod**

TR-4911: FlexPod 유전체학

NetApp, JayaKishore Esanakula

의료 및 생명 과학에 유전체학보다 더 중요한 의학 분야는 거의 없으며 유전체학은 의사와 간호사를 위한 핵심 임상 도구로 빠르게 부상하고 있습니다. 유전체학을 의료 영상 및 디지털 병리학과 결합하면 환자의 유전자가 치료 프로토콜의 영향을 받을 수 있는 방법을 이해하는 데 도움이 됩니다. 의료 분야에서 유전체학이 성공하려면 규모에 따른 데이터 상호 운용성이 크게 중요합니다. 최종 목표는 방대한 양의 유전자 데이터를 파악하고 임상적으로 관련된 상관 관계 및 변이를 파악하여 진단을 개선하고 정밀 약물을 현실화시키는 것입니다. 유전체학은 질병 발병의 근원, 질병의 발전 방식, 효과적인 치료법 및 전략을 이해하는 데 도움이 됩니다. 유전체학은 예방, 진단 및 치료를 포괄하는 많은 이점을 지니고 있습니다. 의료 조직에서는 다음과 같은 여러 당면 과제를 해결하기 위해 노력하고 있습니다.

- 진료 품질 개선
- 가치 기반 케어
- 데이터 급증
- 정밀 의학
- 펜데믹
- 웨어러블, 원격 모니터링 및 관리
- 사이버 보안

표준화된 임상 경로 및 임상 프로토콜은 현대 의학의 중요한 구성 요소 중 하나입니다. 표준화의 주요 측면 중 하나는 의료 기록 뿐만 아니라 게놈 데이터에도 의료 서비스 공급자 간의 상호 운용성입니다. 가장 큰 질문은 의료 조직에서 개인 유전체학 데이터 및 관련 의료 기록에 대한 환자 소유권을 대신 유전자 데이터에 대한 소유권을 양도합니까?

상호 운용이 가능한 환자 데이터는 최근 폭발적인 데이터 증가에 따른 원동력인 정밀 의학의 핵심 요소입니다. 정밀 의학의 목적은 건강 관리, 질병 예방, 진단 및 치료 솔루션을 보다 효과적이고 정확하게 만드는 것입니다.

데이터 증가율은 기하급수적으로 상승했습니다. 2021년 2월 초에 미국 실험실은 주당 약 8,000개의 COVID-19 균주를 염기서열했습니다. 염기서열화된 게놈은 2021년 4월까지 주당 29,000개로 증가했습니다. 완전한 염기서열을 갖춘 각 인간 게놈의 크기는 약 125GB입니다. 따라서 주당 2만 9천 게놈을 염기서열화하는 속도로 휴지 중인 전체 게놈 스토리지는 연간 180페타바이트 이상이 될 것입니다. 여러 국가에서 게놈 감시를 개선하고 세계 보건 문제의 다음 물결에 대비하기 위해 게놈 역학을 위한 리소스를 제공하고 있습니다.

게놈 연구 비용의 감소는 유례없는 속도로 유전자 검사 및 연구를 주도하고 있습니다. 세 가지 PS는 컴퓨터 성능, 데이터의 개인 정보 보호 및 의료 개인화의 변곡점에 있습니다. 2025년까지 연구자들은 1억~20억 개의 인간 게놈을 염기서열화될 것으로 추정하고 있습니다. 유전체학이 효과적이고 가치 있는 제안을 하려면 유전체학 기능이 진료 워크플로우의 원활한 일부여야 합니다. 유전체학은 환자 방문 시 쉽게 액세스하고 조치를 취할 수 있어야 합니다. 환자 전자 의료 기록 데이터를 환자 게놈 데이터와 통합하는 것도 마찬가지로 중요합니다. FlexPod와 같은 최첨단 통합 인프라가 등장하면서 기업은 의사, 간호사 및 클리닉 관리자의 일상 업무 흐름에 유전체학 기능을 활용할 수 있습니다. 최신 FlexPod 플랫폼에 대한 자세한 내용은 다음을 참조하십시오 "Cisco UCS X-Series 지원 FlexPod 데이터 센터

백서".

의사의 경우 유전체학의 진정한 가치는 정밀 의학 및 환자의 게놈 데이터를 기반으로 한 맞춤형 치료 계획을 포함합니다. 과거에 임상의와 데이터 과학자 간에 상당한 시너지 효과를 경험한 적이 없으며, 유전체학은 최근 기술 혁신을 통해 이점을 얻고 있으며, 의료 조직과 업계 기술 리더 간의 진정한 협력 관계를 통해 이점을 얻고 있습니다.

학술 의료 센터와 기타 의료 및 생명 과학 조직은 게놈 과학 분야의 우수 센터(COE)를 설립하는 데 주력하고 있습니다. 닥터 Charlie Gersbach, 박사 그렉 크로포드와 닥터 Duke University의 Tim E Reddy는 다음과 같이 말합니다. "우리는 유전자가 단순한 바이너리 스위치로 켜지거나 꺼지는 것이 아니라 여러 개의 유전자 규제 스위치가 함께 작동한다는 것을 알고 있습니다. 또한 "게놈의 이 부분 중 어느 것도 단독으로 효과가 없다는 것을 확인했습니다. 게놈은 매우 복잡한 웹으로, 진화가 발전해 왔습니다."("참조")를 클릭합니다.

NetApp과 Cisco는 10년 이상 FlexPod 플랫폼의 증분적 개선을 구현하기 위해 노력하고 있습니다. 모든 고객 피드백은 FlexPod의 가치 스트림 및 기능 세트와 함께 듣고 평가하며 연결됩니다. FlexPod를 전 세계적으로 신뢰할 수 있는 통합 인프라 플랫폼으로 차별화하는 피드백, 협업, 개선 및 축하의 연속적 루프입니다. 이 플랫폼은 처음부터 의료 조직을 위한 가장 안정적이고 강력하며 다재다능하고 민첩한 플랫폼으로 간소화되고 설계되었습니다.

범위

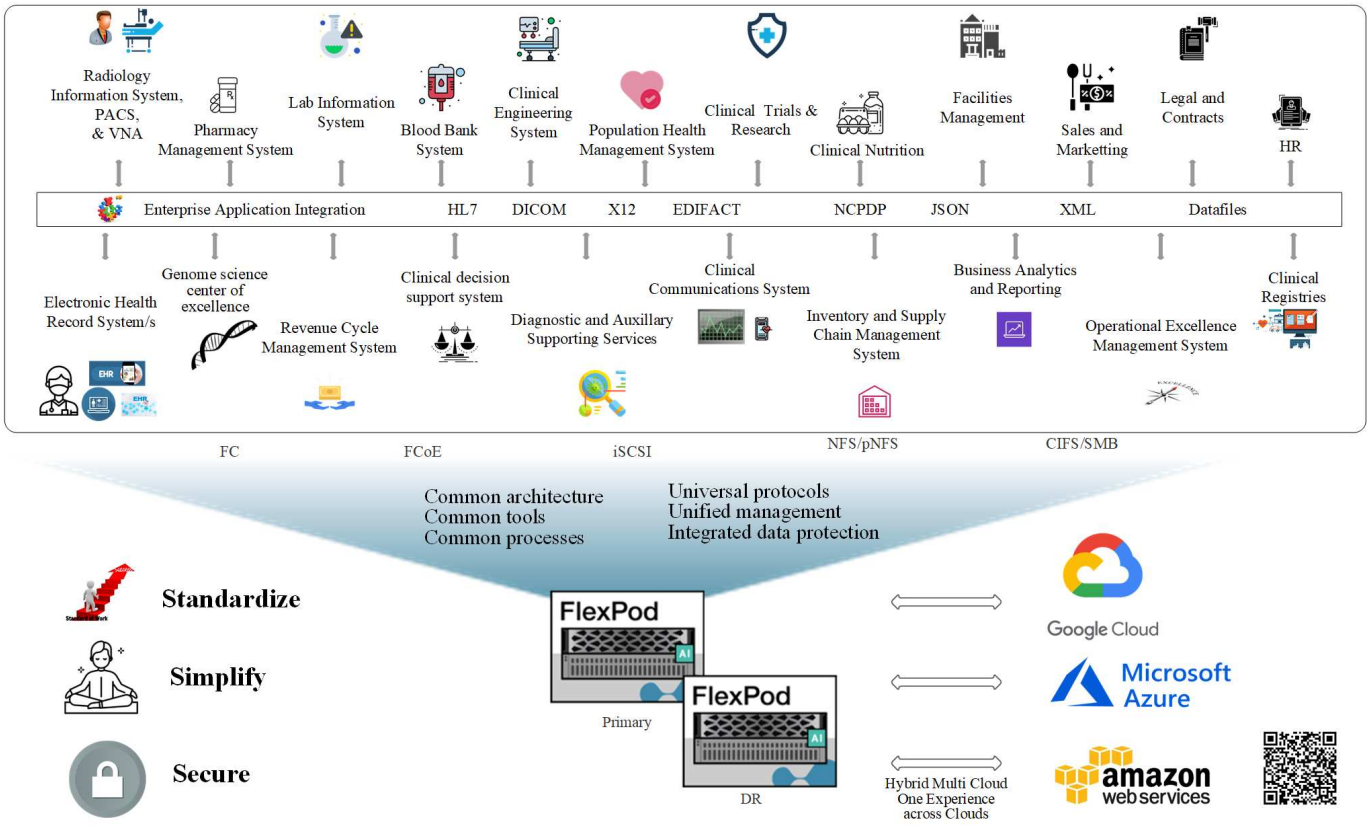
FlexPod 통합 인프라 플랫폼을 사용하는 의료 조직은 하나 이상의 게놈 워크로드를 다른 임상 및 비임상 의료 애플리케이션과 함께 호스팅할 수 있습니다. 이 기술 보고서에서는 FlexPod 플랫폼 검증 중에 GATK라는 업계 표준 오픈 소스 게놈 도구를 사용합니다. 그러나 유전체학 또는 GATK에 대한 보다 자세한 설명은 이 문서의 범위를 벗어납니다.

대상

이 문서는 의료 산업의 기술 리더 및 Cisco와 NetApp 파트너 솔루션 엔지니어 및 프로페셔널 서비스 직원을 위한 것입니다. NetApp은 사용자가 컴퓨팅 및 스토리지 사이징 개념을 잘 이해하고 있을 뿐만 아니라 의료 위협, 의료 보안, 의료 IT 시스템, Cisco UCS 및 NetApp 스토리지 시스템에 대한 기술적 지식을 갖추고 있다고 가정합니다.

FlexPod에 구축된 병원 기능

일반적인 한 병원은 IT 시스템을 다각화했습니다. 이러한 시스템의 대부분은 공급업체에서 구입한 반면 병원 시스템에 의해 구축된 시스템은 거의 없습니다. 따라서 병원 시스템은 데이터 센터의 다양한 인프라 환경을 관리해야 합니다. 병원이 시스템을 FlexPod와 같은 통합 인프라 플랫폼으로 통합할 경우, 조직은 데이터 센터 운영을 표준화할 수 있습니다. FlexPod를 통해 의료 조직은 임상 및 비임상 시스템을 동일한 플랫폼에 구현하여 데이터 센터의 운영을 통합할 수 있습니다.



"다음: FlexPod에 게놈 워크로드를 구축할 때의 이점"

FlexPod에 게놈 워크로드를 구축할 경우의 이점

"이전: 소개."

이 섹션에서는 FlexPod 통합 인프라 플랫폼에서 게놈 워크로드를 실행할 때의 이점에 대해 간략하게 설명합니다. 병원의 기능을 신속하게 설명해 보겠습니다. 다음 비즈니스 아키텍처 보기에는 하이브리드 클라우드 지원 FlexPod 통합 인프라 플랫폼에 구축된 병원의 기능이 나와 있습니다.

- * 의료 분야의 사일로 방지 * 의료 분야의 사일로는 매우 큰 문제가 있습니다. 부서는 종종 자체 하드웨어 및 소프트웨어 세트로 고립되는 경우가 많으며, 선택에 의해 유기적으로 발전된 형태로 나타납니다. 예: 방사선학, 심장학, EHR, 유전체학, 분석, 수익 주기 및 기타 부서에는 전용 소프트웨어 및 하드웨어 세트가 포함됩니다. 의료 조직에서는 제한된 세트의 IT 전문가를 보유하고 있어 하드웨어 및 소프트웨어 자산을 관리할 수 있습니다. 이러한 변곡점은 매우 다양한 하드웨어 및 소프트웨어 세트를 관리할 것으로 예상되는 경우에 발생합니다. 공급업체에서 의료 조직에 제공하는 농축 프로세스의 부합집합 때문에 이질성이 더 나빠집니다.
- * 소규모로 시작하여 성장. * GATK 툴 키트는 FlexPod와 같은 최고의 제품군 플랫폼인 CPU 실행을 위해 튜닝됩니다. FlexPod는 네트워크, 컴퓨팅 및 스토리지의 독립적인 확장성을 지원합니다. 유전체학 기능과 환경이 성장함에 따라 소규모로 시작하여 확장할 수 있습니다. 의료 조직에서는 게놈 워크로드를 실행하기 위해 특수 플랫폼에 투자할 필요가 없습니다. 대신, FlexPod와 같은 다양한 플랫폼을 활용하여 유전체학 워크로드 및 유전체학 워크로드 이외의 워크로드를 동일한 플랫폼에서 실행할 수 있습니다. 예를 들어, 소아 부서에서 게놈 기술을 구현하려는 경우 IT 리더가 기존 FlexPod 인스턴스에서 컴퓨팅, 스토리지 및 네트워킹을 프로비저닝할 수 있습니다. 게놈 사업 유닛이 확장됨에 따라 의료 조직에서 필요에 따라 FlexPod 플랫폼을 확장할 수 있습니다.

- * 단일 제어 창과 탁월한 유연성 * Cisco Intersight는 애플리케이션과 인프라를 연결하여 IT 운영을 대폭 간소화함으로써 베어 메탈 서버 및 하이퍼바이저에서 서버리스 애플리케이션에 대한 가시성과 관리를 제공함으로써 비용을 절감하고 위험을 완화합니다. 이 통합 SaaS 플랫폼은 타사 플랫폼 및 툴과 기본적으로 통합되는 통합 개방형 API 설계를 사용합니다. 또한 모바일 앱을 사용하여 사이트 또는 어디서나 데이터 센터 운영 팀에서 관리할 수 있습니다.

  사용자는 Intersight를 관리 플랫폼으로 활용하여 환경에 실질적인 가치를 빠르게 실현할 수 있습니다. Intertersight는 여러 일일 수동 작업을 자동화하여 오류를 제거하고 일상 작업을 간소화합니다. 또한 Intersight가 지원하는 고급 지원 기능을 통해 어답터가 문제를 사전에 해결하고 문제 해결 시간을 단축할 수 있습니다. 이러한 결합을 통해 조직은 애플리케이션 인프라에 드는 시간과 비용을 훨씬 줄이고 핵심 비즈니스 개발에 더 많은 시간을 투자할 수 있습니다.

  조직에서 Intersight 관리 및 FlexPod의 간편한 확장 가능 아키텍처를 활용하여 단일 FlexPod 플랫폼에서 여러 게놈 워크로드를 실행할 수 있으므로, 활용률을 높이고 총 소유 비용(TCO)을 절감할 수 있습니다. FlexPod를 사용하면 작은 FlexPod Express부터 시작하여 대규모 FlexPod 데이터 센터 구현까지 유연하게 사이징할 수 있습니다. Cisco Intersight에 내장된 역할 기반 액세스 제어 기능을 통해 의료 기관은 강력한 액세스 제어 메커니즘을 구현할 수 있으므로 별도의 인프라 스택이 필요하지 않습니다. 의료 조직 내의 여러 사업부에서 유전체학을 핵심 역량으로 활용할 수 있습니다.

  궁극적으로 FlexPod는 IT 운영을 단순화하고 운영 비용을 절감할 수 있도록 지원하며, IT 인프라 관리자는 IT 인프라를 통해 운영에 부담을 주는 대신 임상의가 혁신을 실현할 수 있도록 지원하는 작업에 집중할 수 있습니다.

- 검증된 설계 및 결과 보장 * FlexPod 설계 및 구축 가이드는 반복 가능한 것으로 입증되었으며, FlexPod를 안심하고 구축하는 데 필요한 포괄적인 구성 세부 정보와 업계 모범 사례를 제공합니다. Cisco 및 NetApp의 검증된 설계 가이드, 구축 가이드 및 아키텍처를 통해 의료 또는 생명 과학 조직은 처음부터 검증되고 신뢰할 수 있는 플랫폼을 구축할 때 불확실한 추측을 배제할 수 있습니다. FlexPod를 사용하면 구축 시간을 단축하고 비용, 복잡성, 위험을 줄일 수 있습니다. FlexPod의 검증된 설계 및 구축 가이드를 통해 FlexPod를 다양한 게놈 분야의 워크로드에 이상적인 플랫폼으로 구축할 수 있습니다.

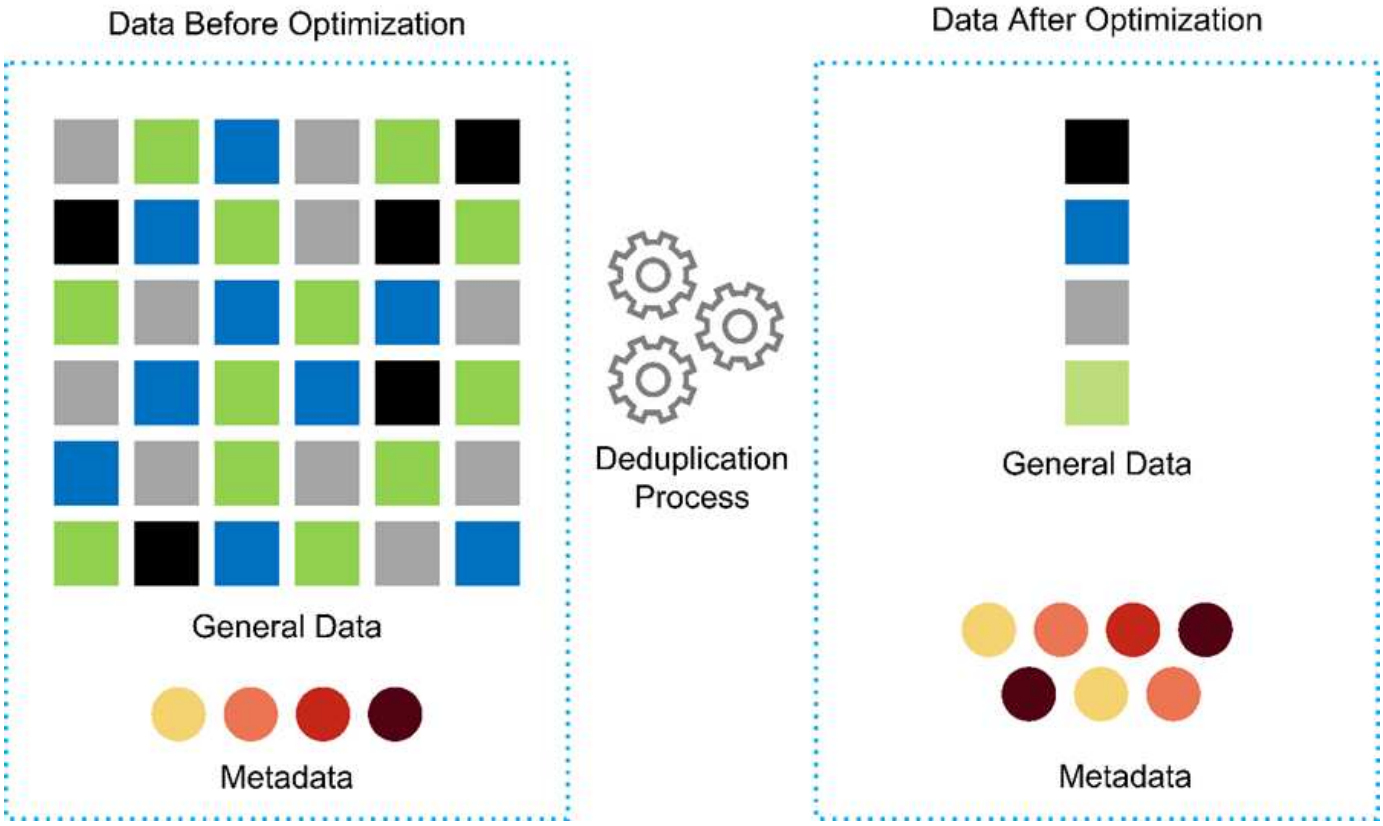
- * 혁신 및 민첩성 * FlexPod는 Epic, Cerner, MEDITECH 및 필립스 아그파, GE와 같은 이미징 시스템과 같은 EHR에 의해 이상적인 플랫폼으로 권장됩니다. 에 대한 자세한 내용은 을 참조하십시오 "롤링을 영광으로 생각합니다" 대상 플랫폼 아키텍처는 Epic userweb을 참조하십시오. 유전체학을 기반으로 합니다 "FlexPod" 의료 기관이 민첩하게 혁신 여정을 계속할 수 있도록 지원합니다. FlexPod를 사용하면 조직 변화를 자연스럽게 구현할 수 있습니다. 조직이 FlexPod 플랫폼을 기반으로 표준화할 경우, 의료 IT 전문가는 시간, 노력, 리소스를 프로비저닝하여 혁신을 위한 프로비저닝을 수행할 수 있으며 따라서 에코시스템 요구사항에 따라 민첩해 질 수 있습니다.

- * 데이터 자유화. * FlexPod 통합 인프라 플랫폼과 NetApp ONTAP 스토리지 시스템을 통해 게놈 데이터를 단일 플랫폼에서 다양한 프로토콜을 사용하여 액세스하고 사용할 수 있습니다. NetApp ONTAP 기반의 FlexPod는 단순하고 직관적이며 강력한 하이브리드 클라우드 플랫폼을 제공합니다. NetApp ONTAP 기반의 Data Fabric은 물리적 경계를 넘어 여러 사이트 간에, 그리고 애플리케이션을 포괄하는 데이터를 제공합니다. Data Fabric은 데이터 중심 세계에서 데이터 중심 기업을 위해 구축되었습니다. 데이터는 여러 위치에서 생성되고 사용되며 다른 위치, 애플리케이션 및 인프라와 활용되어 공유되어야 합니다. 따라서 이를 관리하기 위해서는 일관되고 통합된 방법이 필요합니다. FlexPod을 사용하면 IT 팀이 지속적으로 증가하는 IT 복잡성을 관리하고 간소화할 수 있습니다.

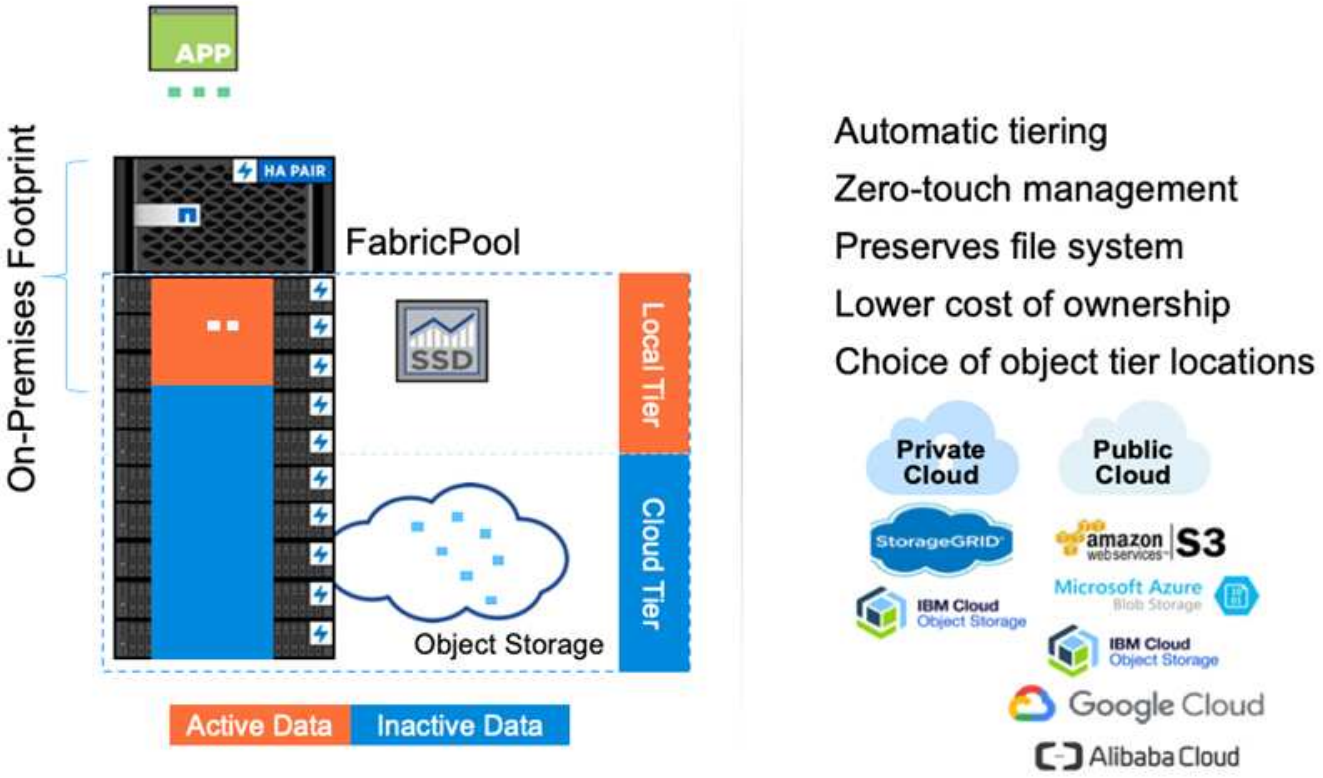
- 보안 멀티 테넌시 * FlexPod는 FIPS 140-2 준수 암호화 모듈을 사용하므로 조직은 보안을 사후 방책이 아닌 기본 요소로 구현할 수 있습니다. FlexPod를 사용하는 조직은 플랫폼의 규모에 관계없이 단일 통합 인프라 플랫폼에서 안전한 멀티 테넌시를 구현할 수 있습니다. 안전한 멀티 테넌시와 QoS를 지원하는 FlexPod는 워크로드 분리 및 사용률 극대화를 지원합니다. 따라서 활용률이 저조할 가능성이 있는 전문 플랫폼에 자본을 종속시키지 않고 관리하기 위한 전문 기술이 필요합니다.

- * 스토리지 효율성 * 유전체학 에는 기본 스토리지에 업계 최고의 스토리지 효율성 기능이 있어야 합니다. 중복제거(인라인 및 주문형), 데이터 압축 및 데이터 컴팩션( )과 같은 NetApp 스토리지 효율성 기능을 사용하여 스토리지 비용을 절감할 수 있습니다 "참조")를 클릭합니다. NetApp 중복 제거는 FlexVol 볼륨에서 블록 레벨 중복 제거를 제공합니다. 기본적으로, 중복제거는 중복 블록을 제거하여 FlexVol 볼륨에 고유한 블록만 저장합니다. 중복 제거는 높은 수준의 정밀도로 작동하며 FlexVol 볼륨의 액티브 파일 시스템에서 작동합니다. 다음 그림은 NetApp

중복제거의 작동 방식을 보여줍니다. 중복제거는 애플리케이션에 투명합니다. 따라서 NetApp 시스템을 사용하는 모든 애플리케이션에서 생성된 데이터를 중복제거하는 데 사용할 수 있습니다. 볼륨 중복 제거를 인라인 프로세스로 백그라운드 프로세스로 실행할 수 있습니다. CLI, NetApp ONTAP System Manager 또는 NetApp Active IQ Unified Manager를 통해 자동으로 실행하거나, 스케줄을 지정하거나, 수동으로 실행하도록 구성할 수 있습니다.



- * 유전체학 상호 운용성 지원 * ONTAP FlexCache은 파일 배포를 간소화하고 WAN 대기 시간을 줄이며 WAN 대역폭 비용을 절감하는 원격 캐싱 기능입니다("참조")를 클릭합니다. 유전체 변종 식별 및 주석 작업 중 주요 활동 중 하나는 임상의의 협업입니다. ONTAP FlexCache 기술은 협업하는 임상의가 서로 다른 지리적 위치에 있는 경우에도 데이터 처리량을 높여줍니다. 일반적으로 *.BAM 파일(1GB ~ 100GB)의 크기를 고려할 때, 기본 플랫폼이 서로 다른 지리적 위치에 있는 임상의가 파일을 사용할 수 있도록 하는 것이 중요합니다. ONTAP FlexCache with FlexPod를 사용하면 게놈 데이터와 애플리케이션을 실질적인 멀티사이트 준비가 완료되어 전 세계 연구자 간의 협업을 원활하게 하면서 짧은 지연 시간과 높은 처리량을 지원할 수 있습니다. 멀티사이트 설정에서 게놈 애플리케이션을 실행하는 의료 조직은 Data Fabric을 사용하여 스케일아웃하여 비용과 속도의 관리 효율성을 균형 있게 유지할 수 있습니다.
- * 스토리지 플랫폼의 지능형 사용. * FlexPod는 ONTAP 자동 계층화 및 NetApp Fabric Pool 기술을 사용하여 데이터 관리를 간소화합니다. FabricPool은 성능, 효율성, 보안 또는 보호 기능을 그대로 유지하면서 스토리지 비용을 절감할 수 있도록 지원합니다. FabricPool는 엔터프라이즈 애플리케이션에 투명하며, 애플리케이션 인프라를 재설계할 필요 없이 스토리지 TCO를 절감하여 클라우드 효율성을 사용합니다. FlexPod은 FabricPool의 스토리지 계층화 기능을 활용하여 ONTAP 플래시 스토리지를 더욱 효율적으로 사용할 수 있습니다. 자세한 내용은 을 "FabricPool 및 FlexPod"참조하십시오. 다음 다이어그램에서는 FabricPool 및 그 이점에 대해 간략하게 설명합니다.



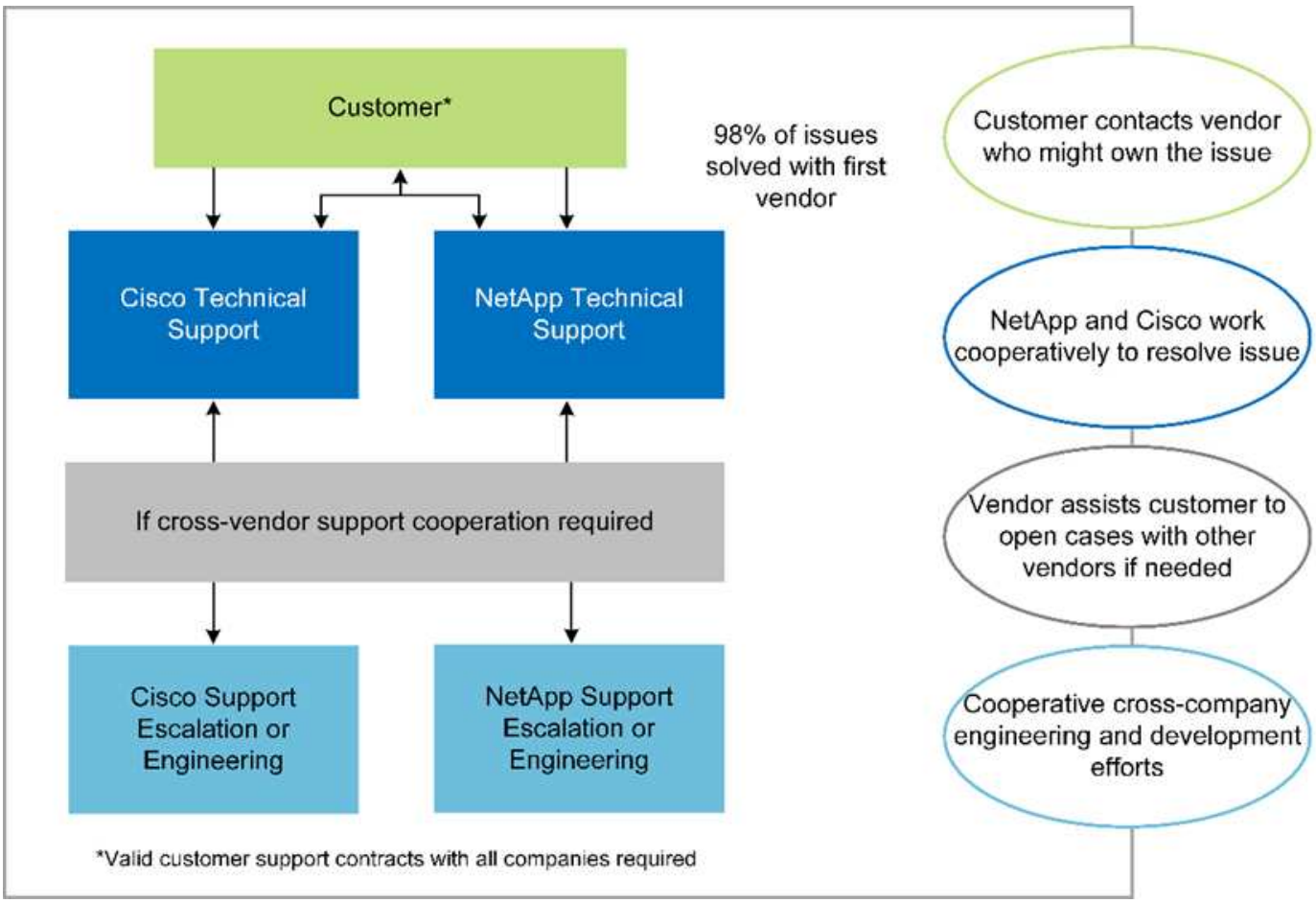
- * 더 빠른 변형 분석 및 주석 * FlexPod 플랫폼은 구축 및 운영화 속도가 빠릅니다. FlexPod 플랫폼을 사용하면 대기 시간이 짧고 처리량이 많은 데이터를 대규모로 사용할 수 있어 청능사가 협업할 수 있습니다. 상호 운용성이 향상되어 혁신이 가능합니다. 의료 조직에서는 유전체 및 유전체 이외의 워크로드를 나란히 실행할 수 있습니다. 즉, 유전체학 여정을 시작하는 데 특수 플랫폼이 필요하지 않습니다.

  FlexPod ONTAP는 스토리지 플랫폼에 정기적으로 최첨단 기능을 추가합니다. FlexPod 데이터 센터는 FC-NVMe를 구축하여 고성능 스토리지가 필요한 애플리케이션에 액세스할 수 있도록 지원하는 최적의 공유 인프라 기반입니다. FC-NVMe가 고가용성, 다중 경로, 추가 운영 체제 지원을 포함하는 방향으로 발전함에 따라, FlexPod은 이러한 기능을 지원하는 데 필요한 확장성과 안정성을 제공하는 엄선된 플랫폼에 적합합니다. 엔드 투 엔드 NVMe를 통해 빠른 I/O를 지원하는 ONTAP를 통해 게놈 분석을 더욱 빠르게 완료할 수 있습니다("참조")를 클릭합니다.

  시퀀싱된 원시 게놈 데이터는 큰 파일 크기를 생성하므로 변형 분석기에서 이러한 파일을 사용할 수 있게 하여 시료 수집에서 변형 주석까지 걸리는 총 시간을 줄이는 것이 중요합니다. 스토리지 액세스 및 데이터 전송 프로토콜로 사용되는 NVMe(Nonvolatile Memory Express)는 전례 없는 수준의 처리량과 가장 빠른 응답 시간을 제공합니다. FlexPod는 PCIe(PCI Express Bus)를 통해 플래시 스토리지에 액세스하는 동안 NVMe 프로토콜을 구축합니다. PCIe를 사용하면 수만 개의 명령 큐를 구현하여 병렬 처리 및 처리량을 높일 수 있습니다. 스토리지에서 메모리로 이르는 단일 프로토콜을 통해 데이터에 빠르게 액세스할 수 있습니다.

- * 처음부터 임상 연구를 위한 민첩성 * 유연하고 확장 가능한 스토리지 용량 및 성능을 통해 의료 연구 기관은 탄력적인 또는 JIT(Just-In-Time) 방식으로 환경을 최적화할 수 있습니다. 스토리지를 컴퓨팅 및 네트워크 인프라와 분리하여 FlexPod 플랫폼을 중단 없이 스케일업 및 스케일아웃할 수 있습니다. FlexPod 플랫폼은 Cisco Intersight를 사용하여 기본 제공 워크플로우와 사용자 지정 자동화 워크플로우를 모두 사용하여 관리할 수 있습니다. Cisco Intersight 워크플로를 통해 의료 조직에서는 애플리케이션 수명 주기 관리 시간을 줄일 수 있습니다. 학술 의료 센터에서 환자 데이터를 익명화하여 연구 정보학 및/또는 연구 센터용으로 사용할 수 있도록 해야 하는 경우, IT 조직은 Cisco Intersight FlexPod 워크플로우를 활용하여 보안 데이터 백업, 복제 및 복원을 몇 시간이 아닌 몇 초 이내에 수행할 수 있습니다. NetApp Trident 및 Kubernetes를 사용하면 IT 조직에서 새로운 데이터 과학자를 프로비저닝하고 모델 개발에 임상 데이터를 몇 분, 때로는 몇 초 안에 사용할 수 있습니다.

- * 게놈 데이터 보호. * NetApp SnapLock은 파일을 저장한 후 지우거나 쓰기가 불가능한 상태로 커밋할 수 있는 특별한 용도의 볼륨을 제공합니다. FlexVol 볼륨에 상주하는 사용자의 운영 데이터는 NetApp SnapMirror 또는 SnapVault 기술을 통해 SnapLock 볼륨으로 미러링하거나 저장할 수 있습니다. SnapLock 볼륨의 파일, 볼륨 자체 및 해당 호스팅 애그리게이트는 보존 기간이 끝날 때까지 삭제할 수 없습니다. ONTAP FPolicy 소프트웨어 조직을 사용하면 특정 확장명의 파일에 대한 작업을 허용하지 않을 경우 랜섬웨어 공격을 방지할 수 있습니다. FPolicy 이벤트는 특정 파일 작업에 대해 트리거될 수 있습니다. 이 이벤트는 정책에 연결되어 있어야 하는 엔진을 호출합니다. 랜섬웨어를 포함할 수 있는 파일 확장자 세트로 정책을 구성할 수 있습니다. 허용되지 않는 확장명을 가진 파일이 무단 작업을 수행하려고 하면 FPolicy가 해당 작업이 실행되지 않도록 합니다 ("참조")를 클릭합니다.
- * FlexPod 공동 지원. * NetApp과 Cisco는 FlexPod 통합 인프라의 고유한 지원 요구사항을 충족하는 강력하고 확장 가능하며 유연한 지원 모델인 FlexPod 공동 지원을 확립했습니다. 이 모델은 NetApp과 Cisco의 경험, 리소스, 기술 지원 전문성을 합쳐 문제 영역에 관계없이, FlexPod 지원 문제를 식별하고 해결할 수 있는 효율적인 프로세스를 제공합니다. 다음 그림은 FlexPod 공동 지원 모델을 개략적으로 보여 줍니다. 고객은 문제를 소유할 수 있는 공급업체에 문의하고 Cisco와 NetApp은 함께 문제를 해결합니다. Cisco와 NetApp은 문제를 해결하기 위해 수작업을 수행하는 회사 간 엔지니어링 및 개발 팀을 보유하고 있습니다. 이 지원 모델은 번역 중 정보 손실을 줄이고 신뢰를 제공하며 가동 중지 시간을 줄여줍니다.



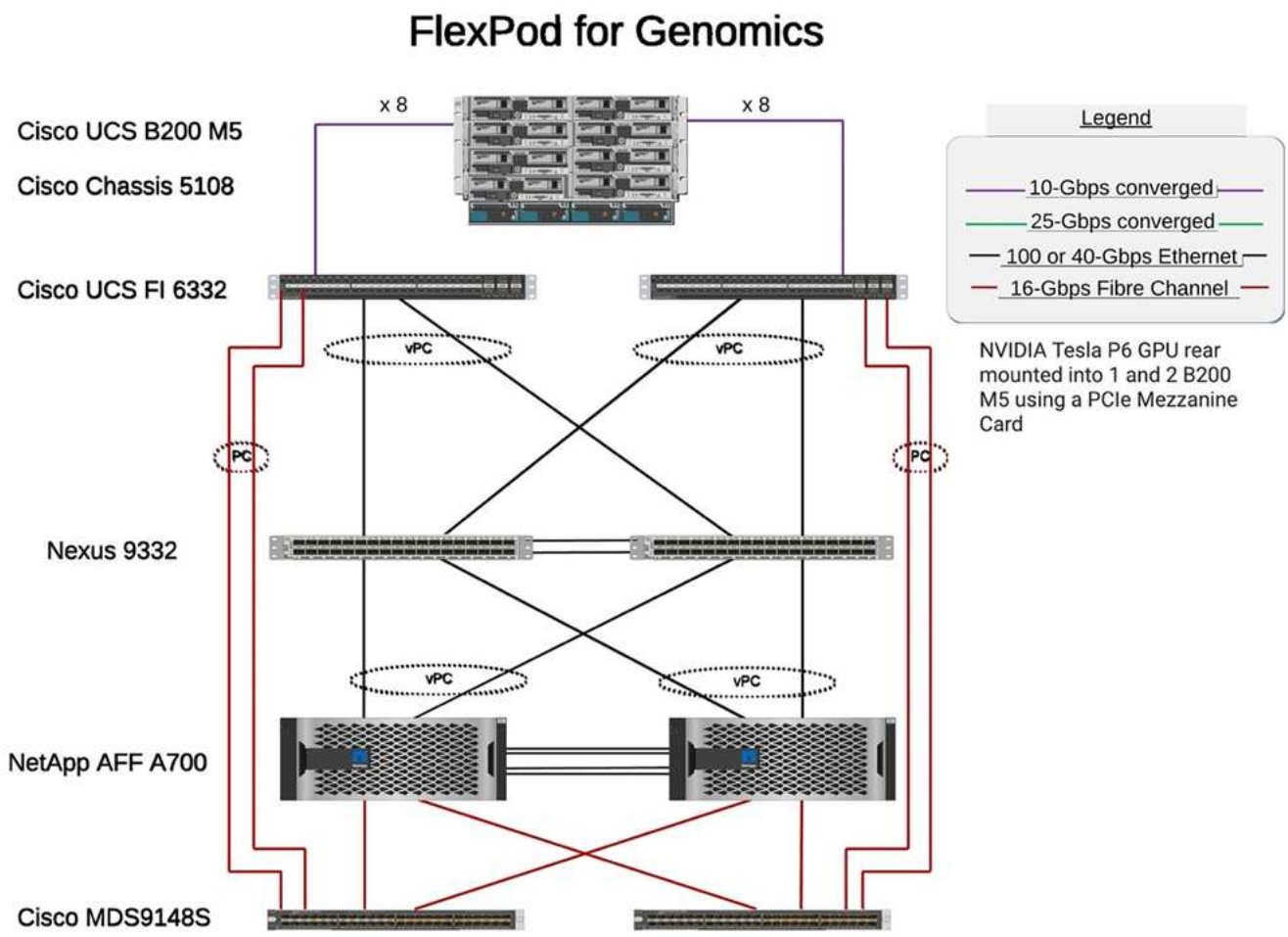
"다음: 솔루션 인프라 하드웨어 및 소프트웨어 구성 요소"

솔루션 인프라 하드웨어 및 소프트웨어 구성 요소

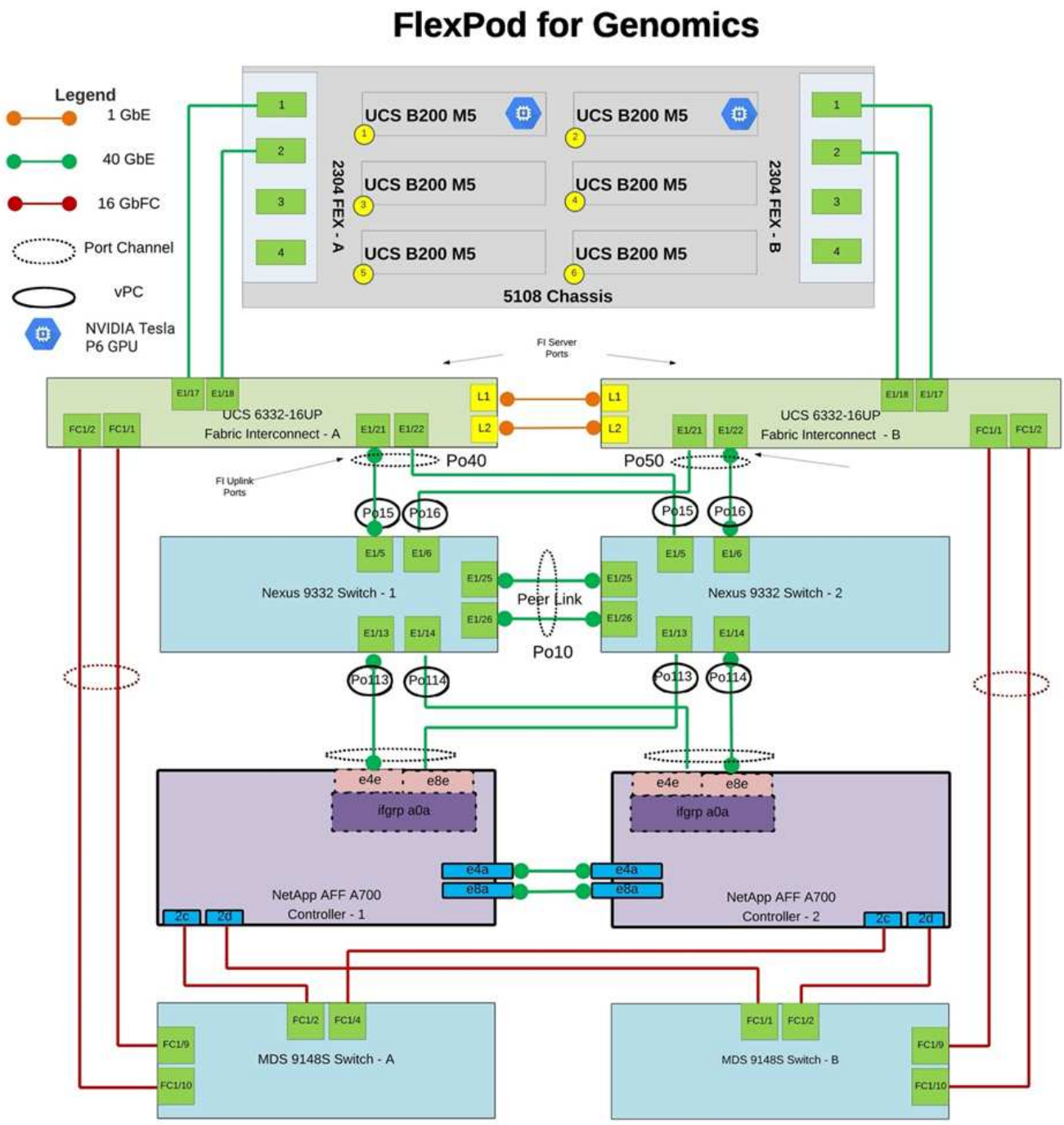
"이전:FlexPod에서 게놈 워크로드를 구축할 때의 이점"

다음 그림은 GATK 설정 및 검증에 사용되는 FlexPod 시스템을 보여 줍니다. 우리는 중고 "VMware vSphere 7.0 및 NetApp ONTAP 9.7을 사용하는 FlexPod 데이터 센터 CVD(Cisco

Validated Design)" 설치 프로세스 중



다음 다이어그램은 FlexPod 케이블 연결 세부 정보를 보여 줍니다.



다음 표에는 FlexPod에서 GATK 테스트 활성화 중에 사용되는 하드웨어 구성 요소가 나열되어 있습니다. 여기 가 있습니다 "NetApp 상호 운용성 매트릭스 툴" (IMT) 및 "Cisco HCL(하드웨어 호환 목록)".

레이어	제품군	수량 및 모델	세부 정보
컴퓨팅	Cisco UCS 5108 섀시	1 또는 2	
	Cisco UCS 블레이드 서버	6 B200 M5	각각 20개 이상의 코어, 2.7GHz 및 128-384GB RAM이 있습니다

레이어	제품군	수량 및 모델	세부 정보
	Cisco UCS 가상 인터페이스 카드(VIC)	Cisco UCS 1440	를 참조하십시오
	Cisco UCS Fabric 인터커넥트 2개	6332	-
네트워크	Cisco Nexus 스위치	2x Cisco Nexus 9332	-
스토리지 네트워크	SMB/CIFS, NFS 또는 iSCSI 프로토콜을 통한 스토리지 액세스를 위한 IP 네트워크	위와 동일한 네트워크 스위치	-
	FC를 통한 스토리지 액세스	Cisco MDS 9148S 2개	-
스토리지	NetApp AFF A700 All-Flash 스토리지 시스템	클러스터 1개	2개의 노드로 클러스터
	디스크 쉘프	DS224C 또는 NS224 디스크 쉘프 1개	24개 드라이브로 완전히 채워집니다
	SSD를 지원합니다	24, 1.2TB 이상의 용량	-

이 표에는 인프라 소프트웨어가 나와 있습니다.

소프트웨어	제품군	버전 또는 릴리스	세부 정보
다양하다	리눅스	RHEL 8.3	-
	Windows	Windows Server 2012 R2(64비트)	-
	NetApp ONTAP를 참조하십시오	ONTAP 9.8 이상	-
	Cisco UCS 6120 패브릭 인터커넥트	Cisco UCS Manager 4.1 이상	-
	Cisco 이더넷 3000 또는 9000 시리즈 스위치	9000 시리즈, 7.0(3) i7(7) 이상(3000 시리즈, 9.2(4) 이상	-
	Cisco FC: Cisco MDS 9132T	8.4(1a) 이상	-
	하이퍼바이저	VMware vSphere ESXi 7.0	-
스토리지	하이퍼바이저 관리 시스템	VMware vCenter Server 7.0(vCSA) 이상	-
네트워크	NetApp 가상 스토리지 콘솔(VSC)	VSC 9.7 이상	-
	NetApp SnapCenter를 참조하십시오	SnapCenter 4.3 이상	-
	Cisco UCS Manager를 참조하십시오	4.1(3c) 이상	
하이퍼바이저	ESXi		

소프트웨어	제품군	버전 또는 릴리스	세부 정보
관리	하이퍼바이저 관리 시스템 VMware vCenter Server 7.0(vCSA) 이상		
	NetApp 가상 스토리지 콘솔(VSC)	VSC 9.7 이상	
	NetApp SnapCenter를 참조하십시오	SnapCenter 4.3 이상	
	Cisco UCS Manager를 참조하십시오	4.1(3c) 이상	

"다음: 유전체학 - GATK 설정 및 실행"

유전체학 - GATK 설정 및 실행

"이전: 솔루션 인프라 하드웨어 및 소프트웨어 구성 요소"

국립인간게놈연구소("NHGRI"), “유전체학(Genomics)은 이러한 유전자의 상호 작용 및 인간 환경의 상호 작용을 포함하여 사람의 모든 유전자(게놈)를 연구하는 학문을 말합니다. ”

에 따르면 "NHGRI"“디옥시리보핵산(DNA)은 거의 모든 생물의 활동을 개발하고 지시하는 데 필요한 지침이 들어 있는 화학 화합물입니다. DNA 분자는 2개의 꼬임, 쌍을 이룬 가닥으로 만들어졌으며, 종종 이중 나선이라고 합니다.” “유기체의 전체 DNA 세트를 게놈(genome)이라고 합니다.”

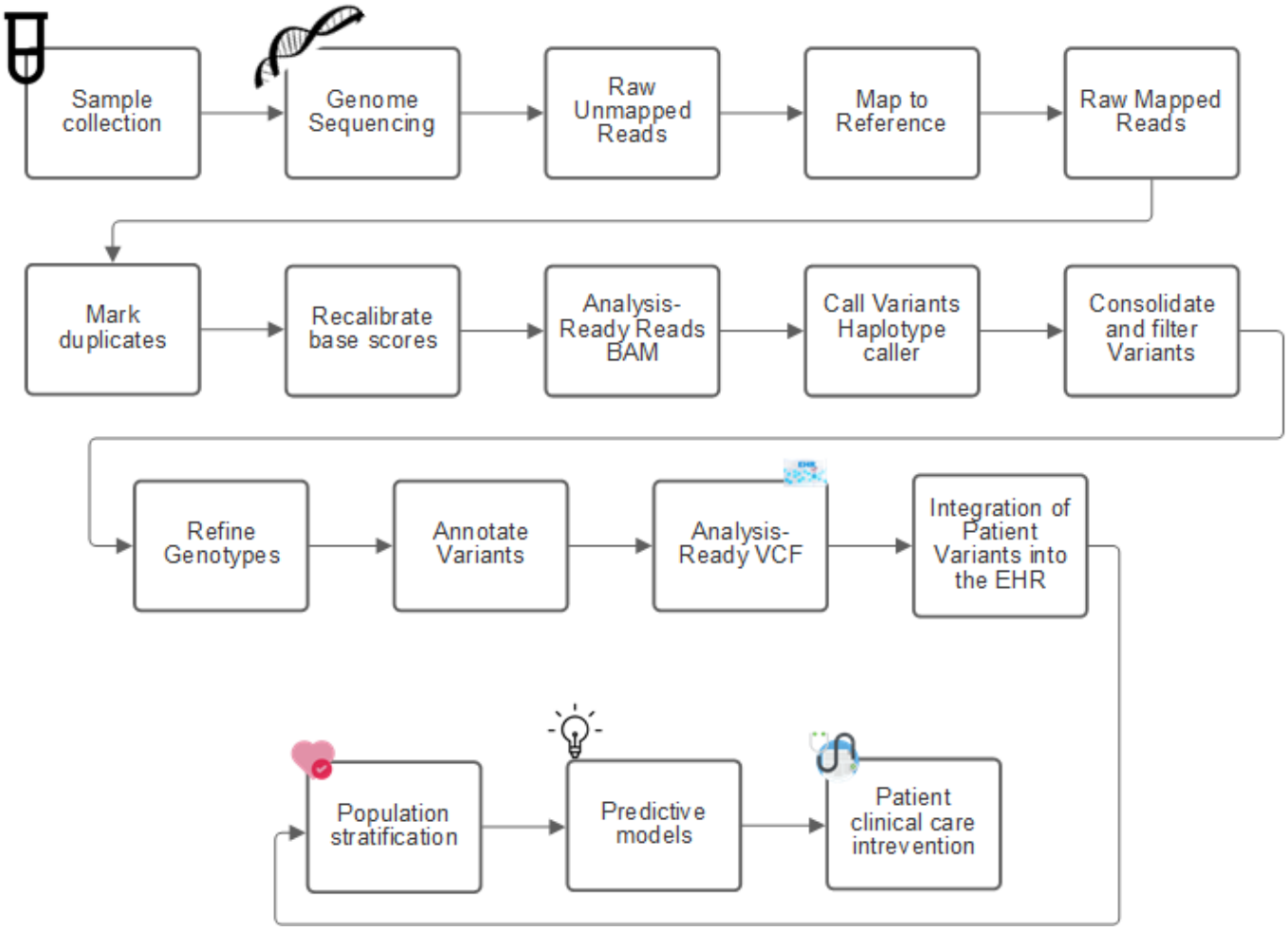
염기서열분석은 DNA 가닥에서 베이스의 정확한 순서를 결정하는 프로세스입니다. 오늘날 사용되는 가장 일반적인 염기서열분석 유형 중 하나는 합성에 의한 시퀀싱입니다. 이 기술은 형광 신호를 방출하여 베이스를 정렬합니다. 연구자들은 DNA 염기서열분석을 사용하여 유전적 변이와 사람이 아직 배아 단계에 있는 동안 질병의 발육이나 진행에 영향을 줄 수 있는 돌연변이를 검색할 수 있습니다.

시료에서 변형 식별, 주석 및 예측에 이르기까지

유전체학을 다음 단계로 분류할 수 있습니다. 전체 목록은 아닙니다.

1. 검체 채취.
2. "게놈 염기서열분석" 시퀀서를 사용하여 원시 데이터를 생성합니다.
3. 사전 처리. 예를 들면, 다음과 같습니다. "중복 제거" 사용 "Picard".
4. 게놈 분석.
    a. 참조 게놈에 매핑.
    b. "변형 모델" 식별 및 주석은 일반적으로 GATK 및 유사한 도구를 사용하여 수행됩니다.
5. EHR(전자 건강 기록) 시스템에 통합
6. "집단 층화" 그리고 지리적 위치와 인종 배경에서 유전적 변이를 식별합니다.
7. "예측 모델" 유의한 단일 뉴클레오티드 다형성 사용.
8. "검증".

다음 그림은 샘플링에서 변형 식별, 주석 및 예측에 이르는 프로세스를 보여 줍니다.



인간 게놈 프로젝트는 2003년 4월에 완료되었으며 이 프로젝트는 공용 도메인에서 사용할 수 있는 인간 게놈 염기서열의 고품질 시뮬레이션을 만들었습니다. 이 참조 게놈은 게놈 분야의 연구 및 개발 분야에서 폭발적으로 성장하였습니다. 거의 모든 인간 질병에는 인간의 유전자에 대한 서명이 있습니다. 최근까지 의사들은 겸상 적혈구 빈혈(Sickle cell anaemia)과 같은 선천성 기형을 예측하여 결정하기 위해 유전자를 활용하고 있었다. 이는 단일 유전자의 변화로 인한 특정 상속 패턴으로 인해 발생한다. 인간 게놈 프로젝트에서 사용 가능한 데이터의 보화가 유전체학 능력의 출현으로 이어졌습니다.

유전체학은 다양한 이점을 제공합니다. 다음은 의료 및 생명 과학 분야에서 얻을 수 있는 다양한 이점입니다.

- 치료 시점의 진단 향상
- 예후가 양호하다
- 정밀 의학
- 맞춤형 치료 계획
- 질병 모니터링 개선
- 부작용 사고 감소
- 치료법 이용 향상
- 질병 모니터링 개선
- 유전자형을 기반으로 한 임상 시험에 대한 효과적인 임상 시험 참여 및 더 나은 환자 선택.

유전체학은 입니다 "십자형 괴수," 데이터 세트의 라이프사이클 전반에서 컴퓨팅 수요가 그 이유는 수집, 스토리지, 배포, 분석 때문입니다.

게놈 분석 툴킷(GATK)

GATK는 에서 데이터 과학 플랫폼으로 개발되었습니다 "Broad Institute(광범위한 기관". GATK는 게놈 분석, 특히 변형 발견, 식별, 주석 및 유전형 분석을 지원하는 오픈 소스 도구 세트입니다. GATK의 장점 중 하나는 도구 및 또는 명령 집합을 연결하여 완전한 워크플로를 만들 수 있다는 것입니다. 광범위한 연구소가 직면한 주요 과제는 다음과 같습니다.

- 질병의 근본 원인과 생물학적 메커니즘을 이해합니다.
- 질환의 근본 원인에 작용하는 치료 중재술을 파악합니다.
- 인체 생리학에서 변이형(variant)에서 기능까지 가시선을 이해합니다.
- 표준 및 정책 생성 "프레임워크" 게놈 데이터 표현, 스토리지, 분석, 보안 등에 사용됩니다.
- 상호 운용 가능한 게놈 집계 데이터베이스(gnomAD)를 표준화하고 계층화합니다.
- 정밀도가 높은 환자의 게놈 기반 모니터링, 진단 및 치료
- 증상이 나타나기 훨씬 전에 질병을 예측하는 도구를 구현하는 데 도움을 줍니다.
- 여러 분야의 공동 협력자들을 만들고 역량을 강화하여 바이오메딘에서 가장 까다롭고 중요한 문제를 해결할 수 있도록 지원합니다.

GATK 및 광학원에 따르면 게놈 시퀀싱은 병리학 검사실에서 프로토콜로 취급해야 합니다. 모든 작업은 시료 및 실험 전반에서 잘 문서화되고 최적화되고 재현 가능하며 일관성이 있습니다. 다음은 Broad Institute에서 권장하는 단계 집합입니다. 자세한 내용은 을 참조하십시오 "GATK 웹 사이트".

FlexPod 설정

유전체학 워크로드 검증에는 FlexPod 인프라 플랫폼의 처음부터 새로 설치가 포함됩니다. FlexPod 플랫폼은 가용성이 높으며 독립적으로 확장할 수 있습니다. 예를 들어, 네트워크, 스토리지 및 컴퓨팅을 독립적으로 확장할 수 있습니다. FlexPod 환경을 설정하기 위해 다음 Cisco Validated Design Guide를 참조 아키텍처 문서로 사용했습니다. "VMware vSphere 7.0 및 NetApp ONTAP 9.7을 사용하는 FlexPod 데이터 센터". 다음 FlexPod 플랫폼 설정 하이라이트를 참조하십시오.

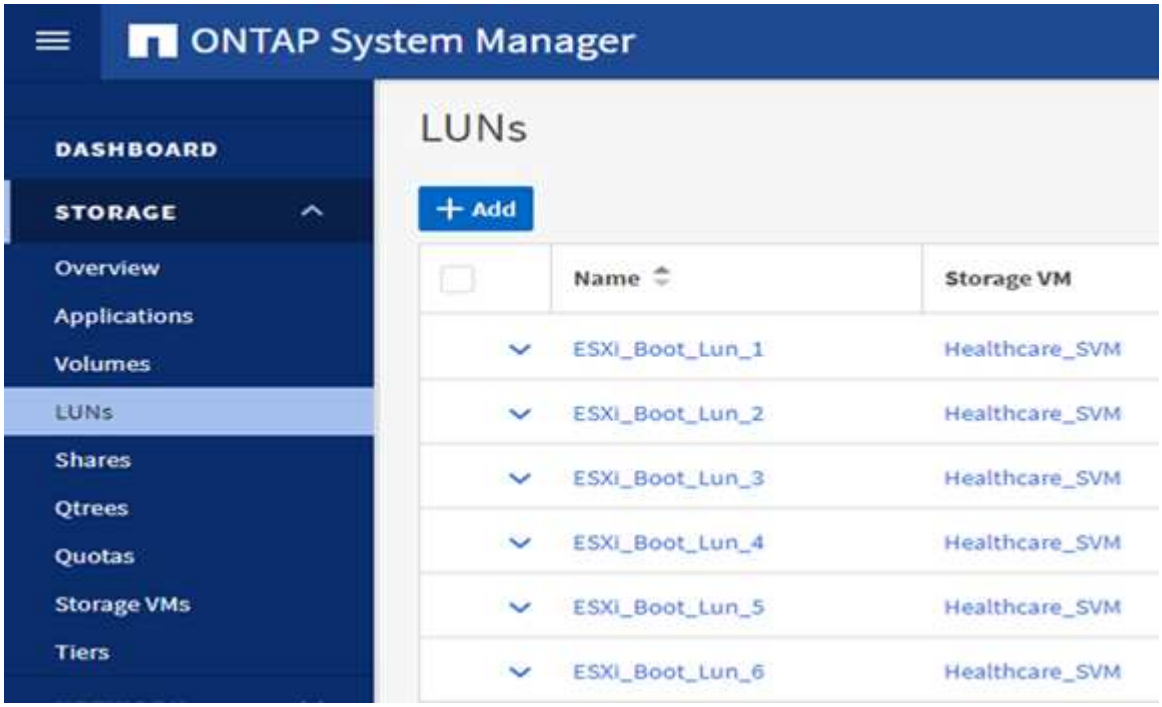
FlexPod 랩 설정을 수행하려면 다음 단계를 완료하십시오.

1. FlexPod 랩 설정 및 검증에서는 다음과 같은 IP4 예약 및 VLAN을 사용합니다.

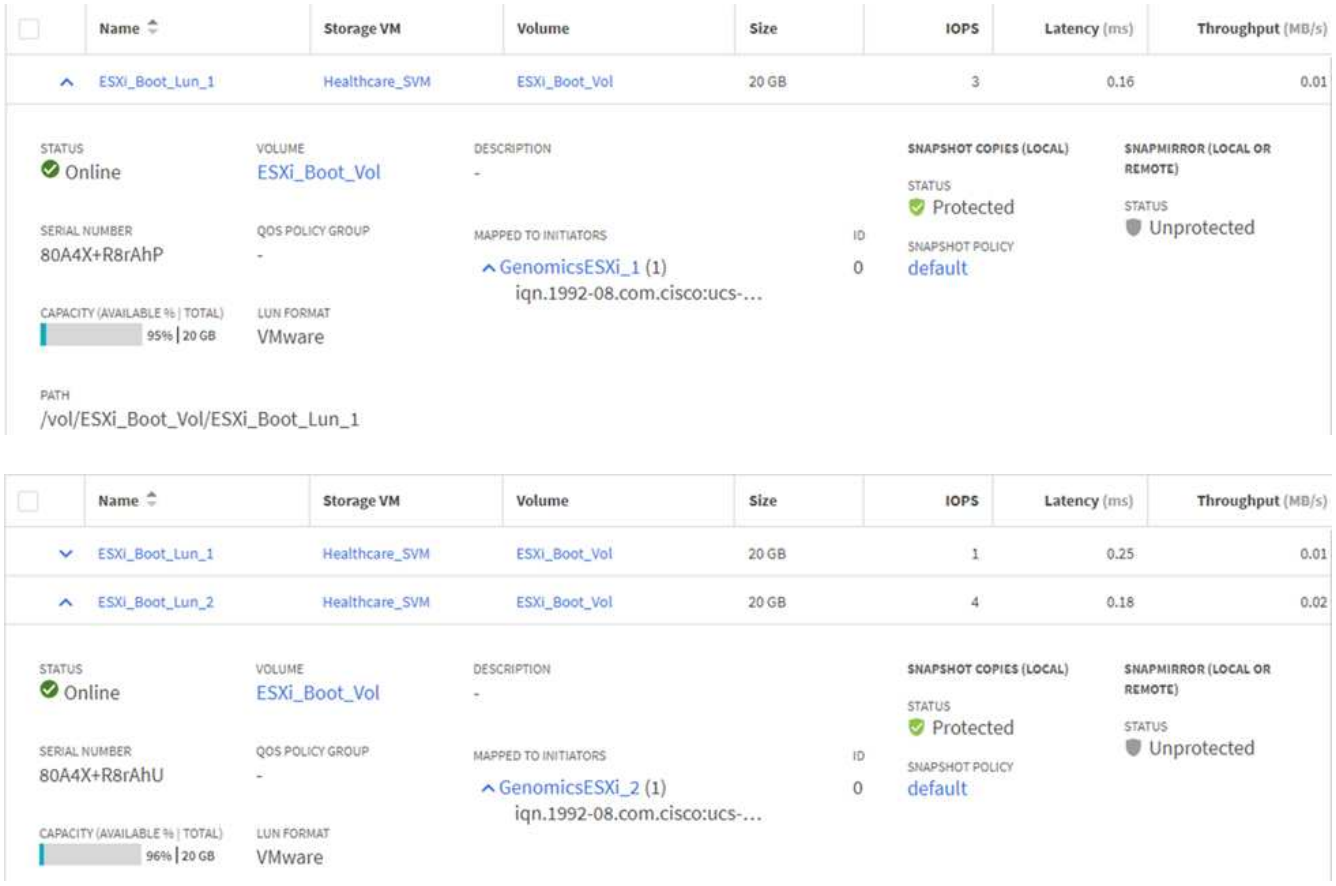
IP Reservations

VLAN	IP Range	Subnet Mask	Purpose
3281	172.21.25 /24	255.255.255.0	IB-MGMT
3282	172.21.26 /24	255.255.255.0	vMotion
3283	172.21.27 /24	255.255.255.0	VM
3284	172.21.28 /24	255.255.255.0	NFS
3285	172.21.29 /24	255.255.255.0	iSCSI-A
3286	172.21.30 /24	255.255.255.0	iSCSI-B

2. ONTAP SVM에서 iSCSI 기반 부팅 LUN을 구성합니다.



3. LUN을 iSCSI 이니시에이터 그룹에 매핑합니다.

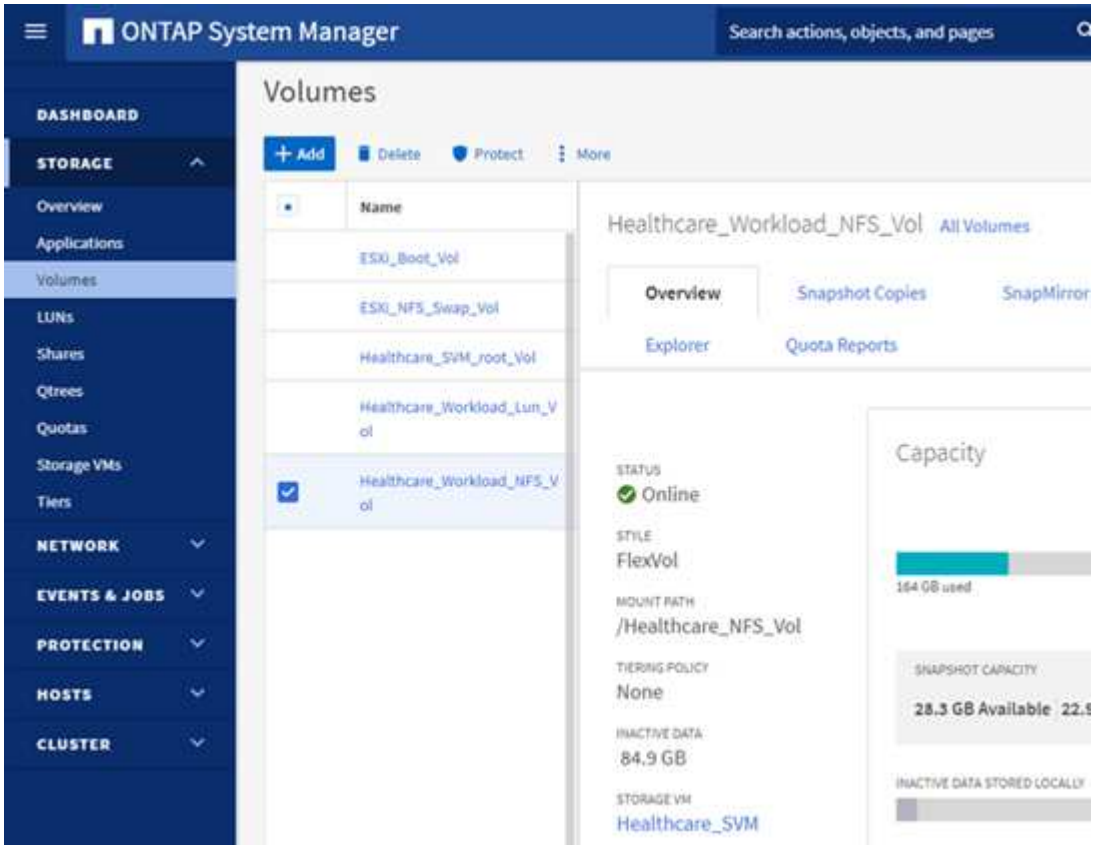


4. iSCSI 부트를 사용하여 vSphere 7.0을 설치합니다.

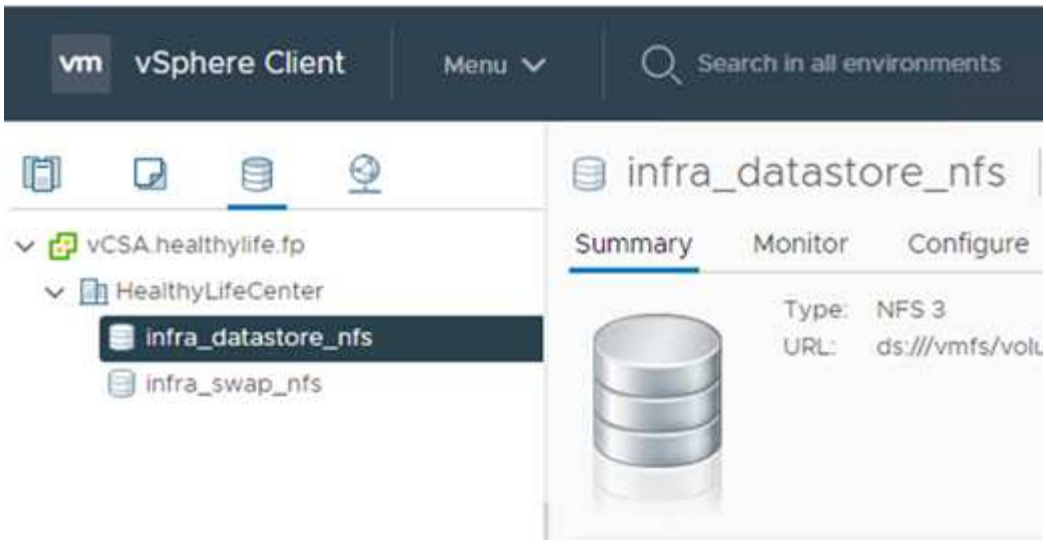
5. vCenter에 ESXi 호스트를 등록합니다.



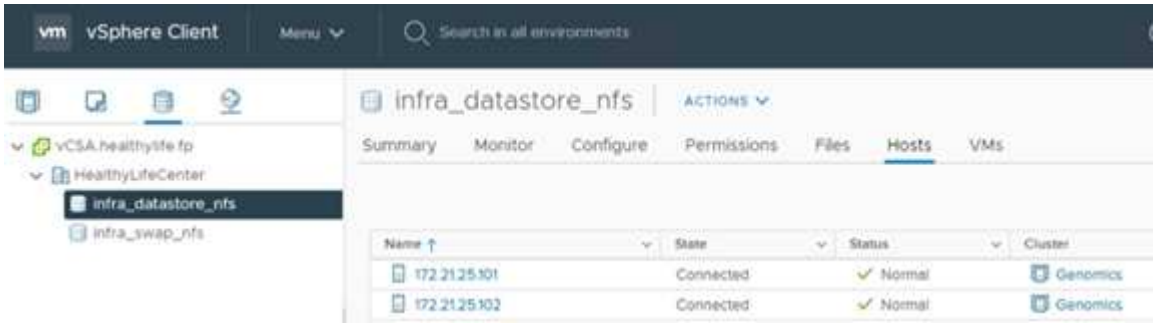
6. ONTAP 스토리지에서 NFS 데이터 저장소 'infra_datastore_nfs'를 프로비저닝합니다.



7. vCenter에 데이터 저장소를 추가합니다.



8. vCenter를 사용하여 ESXi 호스트에 NFS 데이터 저장소를 추가합니다.



9. vCenter를 사용하여 RHEL(Red Hat Enterprise Linux) 8.3 VM을 생성하여 GATK를 실행합니다.
10. NFS 데이터 저장소는 VM에 제공되며 GATK 실행 파일, 스크립트, BAM(Binary Alignment Map) 파일, 참조 파일, 인덱스 파일, 사전 파일 및 variant Calling용 아웃 파일을 저장하는 데 사용되는 "/mnt/geninary"에 마운트됩니다.

```
[root@genomics1 genomics]# df | grep genomics
/dev/sdb              308587328  5699492 287142812   2% /mnt/genomics
[root@genomics1 genomics]#
```

GATK 설정 및 실행

RedHat Enterprise 8.3 Linux VM에 다음 필수 구성 요소를 설치합니다.

- Java 8 또는 SDK 1.8 이상
- Broad Institute에서 GATK 4.2.0.0 다운로드 "GitHub 사이트". 게놈 시퀀스 데이터는 일반적으로 탭으로 구분된 ASCII 열 형태로 저장됩니다. 그러나 ASCII에서는 저장할 공간이 너무 많이 필요합니다. 따라서 BAM(\ **.BAM)** 파일이라는 새로운 표준이 발전했습니다**. BAM** 파일은 시퀀스 데이터를 압축**,** 인덱싱 및 바이너리 형식으로 저장합니다**.** 저희가 **"**다운로드되었습니다**"** 에서 **GATK** 실행을 위해 공개적으로 사용할 수 있는 **BAM** 파일 집합 **"**공용 도메인입니다**".** 또한 인덱스 파일**(**\.dai), 사전 파일(*)도 다운로드했습니다. 참조 데이터 파일(*. fasta) 동일한 공용 도메인에서.

다운로드 후 GATK 도구 키트에는 JAR 파일과 지원 스크립트 세트가 있습니다.

- GATK-PACKAGE-4.2.0.0-LOCAL.JAR 실행 파일

- GATK 스크립트 파일.

BAM 파일과 해당 인덱스, 사전 및 참조 게놈 파일을 아버지, 어머니, 아들 *.BAM 파일로 구성된 제품군에 다운로드했습니다.

크롬웰 엔진

Cromwell은 워크플로우 관리를 지원하는 과학적 워크플로우에 맞춰 설계된 오픈 소스 엔진입니다. 크렘웰 엔진은 2개로 작동할 수 있습니다 "모드", 서버 모드 또는 단일 워크플로 실행 모드. 크롬웰 엔진의 동작은 를 사용하여 제어할 수 있습니다 "Cromwell 엔진 구성 파일".

- 서버 모드 * 를 활성화합니다 "휴식" 크렘웰 엔진의 워크플로 실행.
- * 실행 모드. * 실행 모드는 Cromwell에서 단일 워크플로를 실행하는 데 가장 적합합니다. "참조" 실행 모드에서 사용할 수 있는 전체 옵션 세트를 확인합니다.

당사는 크롬웰 엔진을 사용하여 워크플로우 및 파이프라인을 대규모로 실행합니다. 크롬웰 엔진은 사용자 친화적인 엔진을 사용합니다 "워크플로 설명 언어" (WDL) 기반 스크립팅 언어입니다. Cromwell은 CWL(Common Workflow Language)이라는 두 번째 워크플로 스크립팅 표준도 지원합니다. 이 기술 보고서를 통해 WDL을 사용했습니다. WDL은 원래 Broad Institute for 게놈 분석 파이프라인에 의해 개발되었습니다. WDL 워크플로를 사용하려면 다음을 비롯한 몇 가지 전략을 사용할 수 있습니다.

- * 선형 체인 * 이름에서 알 수 있듯이 작업 #1의 출력은 작업 #2에 입력으로 전송됩니다.
- * 다중 입력/출력. * 각 작업은 후속 작업에 대한 입력으로 여러 출력을 보낼 수 있다는 점에서 선형 연쇄와 유사합니다.
- * Scatter-Gather. * 이 전략은 이벤트 중심 아키텍처에서 특히 사용되는 가장 강력한 EAI(엔터프라이즈 애플리케이션 통합) 전략 중 하나입니다. 각 작업은 분리된 방식으로 실행되며 각 작업의 출력은 최종 출력으로 통합됩니다.

WDL을 사용하여 독립 실행형 모드에서 GATK를 실행하는 경우 다음 3단계가 있습니다.

1. 'womtool.jar'를 사용하여 구문을 검증합니다.

```
[root@genomics1 ~]#  java -jar womtool.jar validate ghplo.wdl
```

2. 입력 JSON을 생성합니다.

```
[root@genomics1 ~]#  java -jar womtool.jar inputs ghplo.wdl > ghplo.json
```

3. 크롬웰 엔진과 크롬웰.jar로 워크플로우를 실행합니다.

```
[root@genomics1 ~]#  java -jar cromwell.jar run ghplo.wdl --inputs
ghplo.json
```

GATK는 여러 가지 방법으로 실행할 수 있습니다. 이 문서에서는 이러한 세 가지 방법을 설명합니다.

JAR 파일을 사용하여 GATK 실행

hplotype variant 호출자를 사용하여 단일 variant 호출 파이프라인 실행을 살펴보겠습니다.

```
[root@genomics1 ~]#  java -Dsamjdk.use_async_io_read_samtools=false \
-Dsamjdk.use_async_io_write_samtools=true \
-Dsamjdk.use_async_io_write_tribble=false \
-Dsamjdk.compression_level=2 \
-jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar \
HaplotypeCaller \
--input /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
--output workshop_1906_2-germline_bams_father.validation.vcf \
--reference /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta
```

이 실행 방법에서는 GATK 로컬 실행 jar 파일을 사용하고, 단일 Java 명령을 사용하여 jar 파일을 호출하고, 명령에 여러 매개 변수를 전달합니다.

1. 이 매개변수는 우리가 'HaplotypeCaller' 변종 호출자 파이프라인을 호출한다는 것을 나타냅니다.
2. '--input'은 입력 BAM 파일을 지정합니다.
3. '--output'은 variant 호 형식(*.vcf)으로 variant 출력 파일을 지정한다. ("참조")를 클릭합니다.
4. 참조 매개 변수를 사용하여 기준 게놈을 전달합니다.

실행 후 출력 상세 정보는 섹션에서 확인할 수 있습니다 "JAR 파일을 사용하여 GATK 실행을 위한 출력입니다."

/GATK 스크립트를 사용하여 GATK 실행

GATK Tool Kit는 './GATK' 스크립트를 이용하여 실행할 수 있다. 다음 명령을 살펴보겠습니다.

```
[root@genomics1 execution]# ./gatk \
--java-options "-Xmx4G" \
HaplotypeCaller \
-I /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
-R /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
-O /mnt/genomics/GATK/TEST\ DATA/variants.vcf
```

명령에 여러 매개 변수를 전달합니다.

- 이 매개변수는 우리가 'HaplotypeCaller' 변종 호출자 파이프라인을 호출한다는 것을 나타냅니다.
- '-I'는 입력 BAM 파일을 지정합니다.
- '-O'는 variant 호 형식(*.vcf)으로 variant 출력 파일을 지정한다. ("참조")를 클릭합니다.

- R 파라미터로 기준 게놈을 통과하고 있다.

실행 후 출력 상세 정보는 섹션에서 확인할 수 있습니다 "016e203cf9beada735f224ab14d0b3af"

크렘웰 엔진을 사용하여 GATK를 실행합니다

Cromwell 엔진을 사용하여 GATK 실행을 관리합니다. 명령줄 및 매개 변수를 살펴보겠습니다.

```
[root@genomics1 genomics]# java -jar cromwell-65.jar \
run /mnt/genomics/GATK/seq/ghplo.wdl  \
--inputs /mnt/genomics/GATK/seq/ghplo.json
```

여기서는 '-jar' 매개 변수를 전달하여 'Cromwell-65.jar'와 같이 jar 파일을 실행하려고 한다는 것을 나타내어 Java 명령을 호출합니다. 전달된 다음 매개 변수('run')는 Cromwell 엔진이 실행 모드에서 실행 중임을 나타내며, 다른 가능한 옵션은 서버 모드입니다. 다음 매개변수는 실행 모드에서 파이프라인을 실행하는 데 사용해야 하는 ' *.wdl'입니다. 다음 매개 변수는 실행 중인 워크플로우에 대한 입력 매개 변수 세트입니다.

다음은 ghplo.wdl 파일의 내용입니다.

```
[root@genomics1 seq]# cat ghplo.wdl
workflow helloHaplotypeCaller {
  call haplotypeCaller
}
task haplotypeCaller {
  File GATK
  File RefFasta
  File RefIndex
  File RefDict
  String sampleName
  File inputBAM
  File bamIndex
  command {
    java -jar ${GATK} \
         HaplotypeCaller \
        -R ${RefFasta} \
        -I ${inputBAM} \
        -O ${sampleName}.raw.indels.snps.vcf
  }
  output {
    File rawVCF = "${sampleName}.raw.indels.snps.vcf"
  }
}
[root@genomics1 seq]#
```

다음은 Cromwell 엔진에 대한 입력이 있는 해당 JSON 파일입니다.

```
[root@genomics1 seq]# cat ghplo.json
{
"helloHaplotypeCaller.haplotypeCaller.GATK": "/mnt/genomics/GATK/gatk-
4.2.0.0/gatk-package-4.2.0.0-local.jar",
"helloHaplotypeCaller.haplotypeCaller.RefFasta": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta",
"helloHaplotypeCaller.haplotypeCaller.RefIndex": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta.fai",
"helloHaplotypeCaller.haplotypeCaller.RefDict": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.dict",
"helloHaplotypeCaller.haplotypeCaller.sampleName": "fatherbam",
"helloHaplotypeCaller.haplotypeCaller.inputBAM": "/mnt/genomics/GATK/TEST
DATA/bam/workshop_1906_2-germline_bams_father.bam",
"helloHaplotypeCaller.haplotypeCaller.bamIndex": "/mnt/genomics/GATK/TEST
DATA/bam/workshop_1906_2-germline_bams_father.bai"
}
[root@genomics1 seq]#
```

Cromwell은 실행을 위해 인메모리 데이터베이스를 사용합니다. 실행 후 출력 로그를 섹션에서 확인할 수 있습니다 "Cromwell 엔진을 사용하여 GATK 실행을 위한 출력"

GATK 실행 방법에 대한 종합적인 단계는 를 참조하십시오 "GATK 문서".

"다음: JAR 파일을 사용하여 GATK 실행을 위한 출력."

JAR 파일을 사용하여 GATK 실행을 위한 출력입니다

"이전: 유전체학 - GATK 설정 및 실행"

JAR 파일을 사용하여 GATK를 실행하면 다음과 같은 샘플 출력이 생성됩니다.

```
[root@genomics1 execution]# java -Dsamjdk.use_async_io_read_samtools=false
\
-Dsamjdk.use_async_io_write_samtools=true \
-Dsamjdk.use_async_io_write_tribble=false \
-Dsamjdk.compression_level=2 \
-jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar \
HaplotypeCaller \
--input /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
--output workshop_1906_2-germline_bams_father.validation.vcf \
--reference /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
22:52:58.430 INFO  NativeLibraryLoader - Loading libgkl_compression.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
```

```
local.jar!/com/intel/gkl/native/libgkl_compression.so
Aug 17, 2021 10:52:58 PM
shaded.cloud_nio.com.google.auth.oauth2.ComputeEngineCredentials
runningOnComputeEngine
INFO: Failed to detect whether we are running on Google Compute Engine.
22:52:58.541 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller - The Genome Analysis Toolkit (GATK)
v4.2.0.0
22:52:58.542 INFO  HaplotypeCaller - For support and documentation go to
https://software.broadinstitute.org/gatk/
22:52:58.542 INFO  HaplotypeCaller - Executing as
root@genomics1.healthylife.fp on Linux v4.18.0-305.3.1.el8_4.x86_64 amd64
22:52:58.542 INFO  HaplotypeCaller - Java runtime: OpenJDK 64-Bit Server
VM v1.8.0_302-b08
22:52:58.542 INFO  HaplotypeCaller - Start Date/Time: August 17, 2021
10:52:58 PM EDT
22:52:58.542 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller - HTSJDK Version: 2.24.0
22:52:58.542 INFO  HaplotypeCaller - Picard Version: 2.25.0
22:52:58.542 INFO  HaplotypeCaller - Built for Spark Version: 2.4.5
22:52:58.542 INFO  HaplotypeCaller - HTSJDK Defaults.COMPRESSION_LEVEL : 2
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_READ_FOR_SAMTOOLS : false
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_SAMTOOLS : true
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_TRIBBLE : false
22:52:58.543 INFO  HaplotypeCaller - Deflater: IntelDeflater
22:52:58.543 INFO  HaplotypeCaller - Inflater: IntelInflater
22:52:58.543 INFO  HaplotypeCaller - GCS max retries/reopens: 20
22:52:58.543 INFO  HaplotypeCaller - Requester pays: disabled
22:52:58.543 INFO  HaplotypeCaller - Initializing engine
22:52:58.804 INFO  HaplotypeCaller - Done initializing engine
22:52:58.809 INFO  HaplotypeCallerEngine - Disabling physical phasing,
which is supported only for reference-model confidence output
22:52:58.820 INFO  NativeLibraryLoader - Loading libgkl_utils.so from
jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_utils.so
22:52:58.821 INFO  NativeLibraryLoader - Loading libgkl_pairhmm_omp.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_pairhmm_omp.so
22:52:58.854 INFO  IntelPairHmm - Using CPU-supported AVX-512 instructions
```

```
22:52:58.854 INFO  IntelPairHmm - Flush-to-zero (FTZ) is enabled when
running PairHMM
22:52:58.854 INFO  IntelPairHmm - Available threads: 16
22:52:58.854 INFO  IntelPairHmm - Requested threads: 4
22:52:58.854 INFO  PairHMM - Using the OpenMP multi-threaded AVX-
accelerated native PairHMM implementation
22:52:58.872 INFO  ProgressMeter - Starting traversal
22:52:58.873 INFO  ProgressMeter -        Current Locus  Elapsed Minutes
Regions Processed   Regions/Minute
22:53:00.733 WARN  InbreedingCoeff - InbreedingCoeff will not be
calculated at position 20:9999900 and possibly subsequent; at least 10
samples must have called genotypes
22:53:08.873 INFO  ProgressMeter -          20:17538652              0.2
58900         353400.0
22:53:17.681 INFO  HaplotypeCaller - 405 read(s) filtered by:
MappingQualityReadFilter
0 read(s) filtered by: MappingQualityAvailableReadFilter
0 read(s) filtered by: MappedReadFilter
0 read(s) filtered by: NotSecondaryAlignmentReadFilter
6628 read(s) filtered by: NotDuplicateReadFilter
0 read(s) filtered by: PassesVendorQualityCheckReadFilter
0 read(s) filtered by: NonZeroReferenceLengthAlignmentReadFilter
0 read(s) filtered by: GoodCigarReadFilter
0 read(s) filtered by: WellformedReadFilter
7033 total reads filtered
22:53:17.681 INFO  ProgressMeter -          20:63024652              0.3
210522         671592.9
22:53:17.681 INFO  ProgressMeter - Traversal complete. Processed 210522
total regions in 0.3 minutes.
22:53:17.687 INFO  VectorLoglessPairHMM - Time spent in setup for JNI call
: 0.010347438
22:53:17.687 INFO  PairHMM - Total compute time in PairHMM
computeLogLikelihoods() : 0.259172573
22:53:17.687 INFO  SmithWatermanAligner - Total compute time in java
Smith-Waterman : 1.27 sec
22:53:17.687 INFO  HaplotypeCaller - Shutting down engine
[August 17, 2021 10:53:17 PM EDT]
org.broadinstitute.hellbender.tools.walkers.haplotypecaller.HaplotypeCalle
r done. Elapsed time: 0.32 minutes.
Runtime.totalMemory()=5561122816
[root@genomics1 execution]#
```

출력 파일은 실행 후 지정된 위치에 있습니다.

"fb08e15744e912200b45cf04b5fce2ad"

/GATK 스크립트를 사용하여 GATK 실행을 위한 출력

"이전: JAR 파일을 사용하여 GATK 실행을 위한 출력."

'./GATK' 스크립트를 사용하여 GATK를 실행하면 다음과 같은 샘플 출력이 생성됩니다.

```
[root@genomics1 gatk-4.2.0.0]# ./gatk --java-options "-Xmx4G" \
HaplotypeCaller \
-I /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
-R /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
-O /mnt/genomics/GATK/TEST\ DATA/variants.vcf
Using GATK jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar
Running:
    java -Dsamjdk.use_async_io_read_samtools=false
-Dsamjdk.use_async_io_write_samtools=true
-Dsamjdk.use_async_io_write_tribble=false -Dsamjdk.compression_level=2
-Xmx4G -jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar
HaplotypeCaller -I /mnt/genomics/GATK/TEST DATA/bam/workshop_1906_2-
germline_bams_father.bam -R /mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta -O /mnt/genomics/GATK/TEST
DATA/variants.vcf
23:29:45.553 INFO  NativeLibraryLoader - Loading libgkl_compression.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_compression.so
Aug 17, 2021 11:29:45 PM
shaded.cloud_nio.com.google.auth.oauth2.ComputeEngineCredentials
runningOnComputeEngine
INFO: Failed to detect whether we are running on Google Compute Engine.
23:29:45.686 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.686 INFO  HaplotypeCaller - The Genome Analysis Toolkit (GATK)
v4.2.0.0
23:29:45.686 INFO  HaplotypeCaller - For support and documentation go to
https://software.broadinstitute.org/gatk/
23:29:45.687 INFO  HaplotypeCaller - Executing as
root@genomics1.healthylife.fp on Linux v4.18.0-305.3.1.el8_4.x86_64 amd64
23:29:45.687 INFO  HaplotypeCaller - Java runtime: OpenJDK 64-Bit Server
VM v11.0.12+7-LTS
23:29:45.687 INFO  HaplotypeCaller - Start Date/Time: August 17, 2021 at
11:29:45 PM EDT
23:29:45.687 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.687 INFO  HaplotypeCaller -
```

```
-----------------------------------------------------------
23:29:45.687 INFO  HaplotypeCaller - HTSJDK Version: 2.24.0
23:29:45.687 INFO  HaplotypeCaller - Picard Version: 2.25.0
23:29:45.687 INFO  HaplotypeCaller - Built for Spark Version: 2.4.5
23:29:45.688 INFO  HaplotypeCaller - HTSJDK Defaults.COMPRESSION_LEVEL : 2
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_READ_FOR_SAMTOOLS : false
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_SAMTOOLS : true
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_TRIBBLE : false
23:29:45.688 INFO  HaplotypeCaller - Deflater: IntelDeflater
23:29:45.688 INFO  HaplotypeCaller - Inflater: IntelInflater
23:29:45.688 INFO  HaplotypeCaller - GCS max retries/reopens: 20
23:29:45.688 INFO  HaplotypeCaller - Requester pays: disabled
23:29:45.688 INFO  HaplotypeCaller - Initializing engine
23:29:45.804 INFO  HaplotypeCaller - Done initializing engine
23:29:45.809 INFO  HaplotypeCallerEngine - Disabling physical phasing,
which is supported only for reference-model confidence output
23:29:45.818 INFO  NativeLibraryLoader - Loading libgkl_utils.so from
jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_utils.so
23:29:45.819 INFO  NativeLibraryLoader - Loading libgkl_pairhmm_omp.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_pairhmm_omp.so
23:29:45.852 INFO  IntelPairHmm - Using CPU-supported AVX-512 instructions
23:29:45.852 INFO  IntelPairHmm - Flush-to-zero (FTZ) is enabled when
running PairHMM
23:29:45.852 INFO  IntelPairHmm - Available threads: 16
23:29:45.852 INFO  IntelPairHmm - Requested threads: 4
23:29:45.852 INFO  PairHMM - Using the OpenMP multi-threaded AVX-
accelerated native PairHMM implementation
23:29:45.868 INFO  ProgressMeter - Starting traversal
23:29:45.868 INFO  ProgressMeter -        Current Locus  Elapsed Minutes
Regions Processed   Regions/Minute
23:29:47.772 WARN  InbreedingCoeff - InbreedingCoeff will not be
calculated at position 20:9999900 and possibly subsequent; at least 10
samples must have called genotypes
23:29:55.868 INFO  ProgressMeter -          20:18885652              0.2
63390         380340.0
23:30:04.389 INFO  HaplotypeCaller - 405 read(s) filtered by:
MappingQualityReadFilter
0 read(s) filtered by: MappingQualityAvailableReadFilter
0 read(s) filtered by: MappedReadFilter
0 read(s) filtered by: NotSecondaryAlignmentReadFilter
6628 read(s) filtered by: NotDuplicateReadFilter
```

```
0 read(s) filtered by: PassesVendorQualityCheckReadFilter
0 read(s) filtered by: NonZeroReferenceLengthAlignmentReadFilter
0 read(s) filtered by: GoodCigarReadFilter
0 read(s) filtered by: WellformedReadFilter
7033 total reads filtered
23:30:04.389 INFO  ProgressMeter -          20:63024652              0.3
210522         681999.9
23:30:04.389 INFO  ProgressMeter - Traversal complete. Processed 210522
total regions in 0.3 minutes.
23:30:04.395 INFO  VectorLoglessPairHMM - Time spent in setup for JNI call
: 0.012129203000000002
23:30:04.395 INFO  PairHMM - Total compute time in PairHMM
computeLogLikelihoods() : 0.267345217
23:30:04.395 INFO  SmithWatermanAligner - Total compute time in java
Smith-Waterman : 1.23 sec
23:30:04.395 INFO  HaplotypeCaller - Shutting down engine
[August 17, 2021 at 11:30:04 PM EDT]
org.broadinstitute.hellbender.tools.walkers.haplotypecaller.HaplotypeCalle
r done. Elapsed time: 0.31 minutes.
Runtime.totalMemory()=2111832064
[root@genomics1 gatk-4.2.0.0]#
```

출력 파일은 실행 후 지정된 위치에 있습니다.

"다음: Cromwell 엔진을 사용하여 GATK 실행을 위한 출력."

Cromwell 엔진을 사용하여 GATK 실행을 위한 출력

"11fffe01d469840980d9b9a5f45bf9ed"

크롬웰 엔진을 사용하여 GATK를 실행하면 다음과 같은 샘플 출력이 생성됩니다.

```
[root@genomics1 genomics]# java -jar  cromwell-65.jar run
/mnt/genomics/GATK/seq/ghplo.wdl  --inputs
/mnt/genomics/GATK/seq/ghplo.json
[2021-08-18 17:10:50,78] [info] Running with database db.url =
jdbc:hsqldb:mem:856a1f0d-9a0d-42e5-9199-
5e6c1d0f72dd;shutdown=false;hsqldb.tx=mvcc
[2021-08-18 17:10:57,74] [info] Running migration
RenameWorkflowOptionsInMetadata with a read batch size of 100000 and a
write batch size of 100000
[2021-08-18 17:10:57,75] [info] [RenameWorkflowOptionsInMetadata] 100%
[2021-08-18 17:10:57,83] [info] Running with database db.url =
jdbc:hsqldb:mem:6afe0252-2dc9-4e57-8674-
ce63c67aa142;shutdown=false;hsqldb.tx=mvcc
[2021-08-18 17:10:58,17] [info] Slf4jLogger started
```

```
[2021-08-18 17:10:58,33] [info] Workflow heartbeat configuration:
{
  "cromwellId" : "cromid-41b7e30",
  "heartbeatInterval" : "2 minutes",
  "ttl" : "10 minutes",
  "failureShutdownDuration" : "5 minutes",
  "writeBatchSize" : 10000,
  "writeThreshold" : 10000
}
[2021-08-18 17:10:58,38] [info] Metadata summary refreshing every 1
second.
[2021-08-18 17:10:58,38] [info] No metadata archiver defined in config
[2021-08-18 17:10:58,38] [info] No metadata deleter defined in config
[2021-08-18 17:10:58,40] [info] KvWriteActor configured to flush with
batch size 200 and process rate 5 seconds.
[2021-08-18 17:10:58,40] [info] WriteMetadataActor configured to flush
with batch size 200 and process rate 5 seconds.
[2021-08-18 17:10:58,44] [info] CallCacheWriteActor configured to flush
with batch size 100 and process rate 3 seconds.
[2021-08-18 17:10:58,44] [warn] 'docker.hash-lookup.gcr-api-queries-per-
100-seconds' is being deprecated, use 'docker.hash-lookup.gcr.throttle'
instead (see reference.conf)
[2021-08-18 17:10:58,54] [info] JobExecutionTokenDispenser - Distribution
rate: 50 per 1 seconds.
[2021-08-18 17:10:58,58] [info] SingleWorkflowRunnerActor: Version 65
[2021-08-18 17:10:58,58] [info] SingleWorkflowRunnerActor: Submitting
workflow
[2021-08-18 17:10:58,64] [info] Unspecified type (Unspecified version)
workflow 3e246147-b1a9-41dc-8679-319f81b7701e submitted
[2021-08-18 17:10:58,66] [info] SingleWorkflowRunnerActor: Workflow
submitted 3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,66] [info] 1 new workflows fetched by cromid-41b7e30:
3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,67] [info] WorkflowManagerActor: Starting workflow
3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,68] [info] WorkflowManagerActor: Successfully started
WorkflowActor-3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,68] [info] Retrieved 1 workflows from the
WorkflowStoreActor
[2021-08-18 17:10:58,70] [info] WorkflowStoreHeartbeatWriteActor
configured to flush with batch size 10000 and process rate 2 minutes.
[2021-08-18 17:10:58,76] [info] MaterializeWorkflowDescriptorActor
[3e246147]: Parsing workflow as WDL draft-2
[2021-08-18 17:10:59,34] [info] MaterializeWorkflowDescriptorActor
[3e246147]: Call-to-Backend assignments:
helloHaplotypeCaller.haplotypeCaller -> Local
```

```
[2021-08-18 17:11:00,54] [info] WorkflowExecutionActor-3e246147-b1a9-41dc-
8679-319f81b7701e [3e246147]: Starting
helloHaplotypeCaller.haplotypeCaller
[2021-08-18 17:11:01,56] [info] Assigned new job execution tokens to the
following groups: 3e246147: 1
[2021-08-18 17:11:01,70] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: java -jar
/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-41dc-
8679-319f81b7701e/call-haplotypeCaller/inputs/-179397211/gatk-package-
4.2.0.0-local.jar \
     HaplotypeCaller \
    -R /mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-
b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/inputs/604632695/workshop_1906_2-germline_ref_ref.fasta \
    -I /mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-
b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/inputs/604617202/workshop_1906_2-germline_bams_father.bam
\
    -O fatherbam.raw.indels.snps.vcf
[2021-08-18 17:11:01,72] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: executing: /bin/bash
/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-41dc-
8679-319f81b7701e/call-haplotypeCaller/execution/script
[2021-08-18 17:11:03,49] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: job id: 26867
[2021-08-18 17:11:03,53] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: Status change from -
to WaitingForReturnCode
[2021-08-18 17:11:03,54] [info] Not triggering log of token queue status.
Effective log interval = None
[2021-08-18 17:11:23,65] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: Status change from
WaitingForReturnCode to Done
[2021-08-18 17:11:25,04] [info] WorkflowExecutionActor-3e246147-b1a9-41dc-
8679-319f81b7701e [3e246147]: Workflow helloHaplotypeCaller complete.
Final Outputs:
{
  "helloHaplotypeCaller.haplotypeCaller.rawVCF": "/mnt/genomics/cromwell-
executions/helloHaplotypeCaller/3e246147-b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/execution/fatherbam.raw.indels.snps.vcf"
}
[2021-08-18 17:11:28,43] [info] WorkflowManagerActor: Workflow actor for
3e246147-b1a9-41dc-8679-319f81b7701e completed with status 'Succeeded'.
The workflow will be removed from the workflow store.
[2021-08-18 17:11:32,24] [info] SingleWorkflowRunnerActor workflow
finished with status 'Succeeded'.
```

```
{
  "outputs": {
    "helloHaplotypeCaller.haplotypeCaller.rawVCF":
"/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-
41dc-8679-319f81b7701e/call-
haplotypeCaller/execution/fatherbam.raw.indels.snps.vcf"
  },
  "id": "3e246147-b1a9-41dc-8679-319f81b7701e"
}
[2021-08-18 17:11:33,45] [info] Workflow polling stopped
[2021-08-18 17:11:33,46] [info] 0 workflows released by cromid-41b7e30
[2021-08-18 17:11:33,46] [info] Shutting down WorkflowStoreActor - Timeout
= 5 seconds
[2021-08-18 17:11:33,46] [info] Shutting down WorkflowLogCopyRouter -
Timeout = 5 seconds
[2021-08-18 17:11:33,46] [info] Shutting down JobExecutionTokenDispenser -
Timeout = 5 seconds
[2021-08-18 17:11:33,46] [info] Aborting all running workflows.
[2021-08-18 17:11:33,46] [info] JobExecutionTokenDispenser stopped
[2021-08-18 17:11:33,46] [info] WorkflowStoreActor stopped
[2021-08-18 17:11:33,47] [info] WorkflowLogCopyRouter stopped
[2021-08-18 17:11:33,47] [info] Shutting down WorkflowManagerActor -
Timeout = 3600 seconds
[2021-08-18 17:11:33,47] [info] WorkflowManagerActor: All workflows
finished
[2021-08-18 17:11:33,47] [info] WorkflowManagerActor stopped
[2021-08-18 17:11:33,64] [info] Connection pools shut down
[2021-08-18 17:11:33,64] [info] Shutting down SubWorkflowStoreActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down JobStoreActor - Timeout =
1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down CallCacheWriteActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] SubWorkflowStoreActor stopped
[2021-08-18 17:11:33,64] [info] Shutting down ServiceRegistryActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down DockerHashActor - Timeout =
1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down IoProxy - Timeout = 1800
seconds
[2021-08-18 17:11:33,64] [info] CallCacheWriteActor Shutting down: 0
queued messages to process
[2021-08-18 17:11:33,64] [info] JobStoreActor stopped
[2021-08-18 17:11:33,64] [info] CallCacheWriteActor stopped
[2021-08-18 17:11:33,64] [info] KvWriteActor Shutting down: 0 queued
messages to process
```

```
[2021-08-18 17:11:33,64] [info] IoProxy stopped
[2021-08-18 17:11:33,64] [info] WriteMetadataActor Shutting down: 0 queued
messages to process
[2021-08-18 17:11:33,65] [info] ServiceRegistryActor stopped
[2021-08-18 17:11:33,65] [info] DockerHashActor stopped
[2021-08-18 17:11:33,67] [info] Database closed
[2021-08-18 17:11:33,67] [info] Stream materializer shut down
[2021-08-18 17:11:33,67] [info] WDL HTTP import resolver closed
[root@genomics1 genomics]#
```

"다음: GPU 설정."

GPU 설정

"이전: Cromwell 엔진을 사용하여 GATK 실행을 위한 출력."

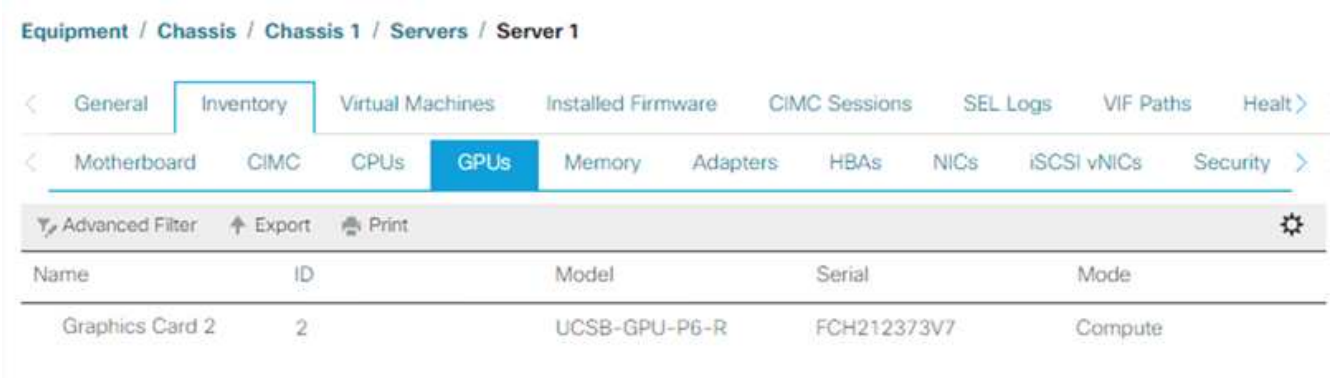
발행 당시에는 GATK 툴이 사내 GPU 기반 실행을 기본적으로 지원하지 않았습니다. 독자가 GATK용 PCIe 메자닌 카드를 사용하여 후면 장착 NVIDIA Tesla P6 GPU에서 FlexPod를 사용하는 것이 얼마나 간단한지 이해할 수 있도록 다음 설정 및 지침이 제공됩니다.

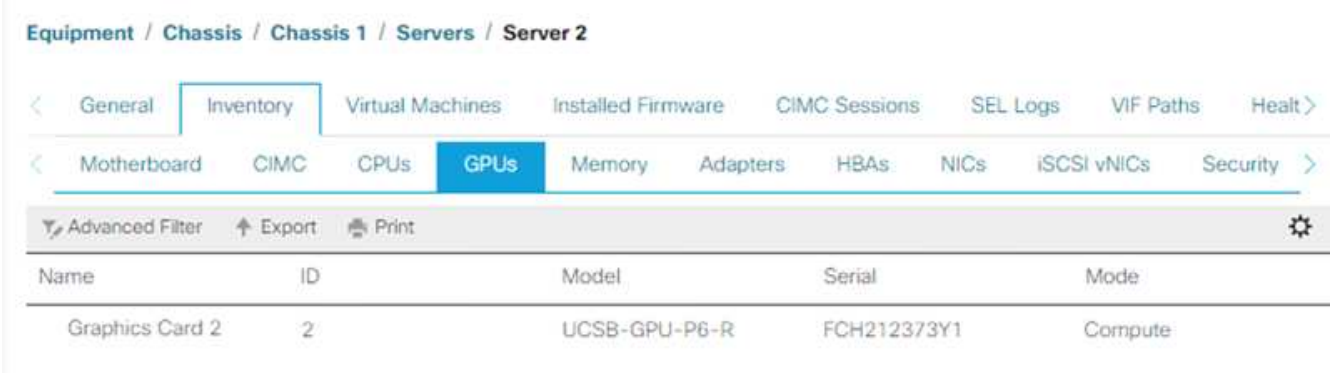
다음 CVD(Cisco-Validated Design)를 참조 아키텍처와 모범 사례 가이드로 사용하여 FlexPod 환경을 설정하여 GPU를 사용하는 애플리케이션을 실행할 수 있습니다.

- "딥 러닝용 Cisco UCS 480mL가 포함된 AI/ML용 FlexPod 데이터 센터"

다음은 이 설정 과정에서 기억해야 할 요점입니다.

1. 우리는 UCS B200 M5 서버의 메자닌 슬롯에 PCIe NVIDIA Tesla P6 GPU를 사용했습니다.





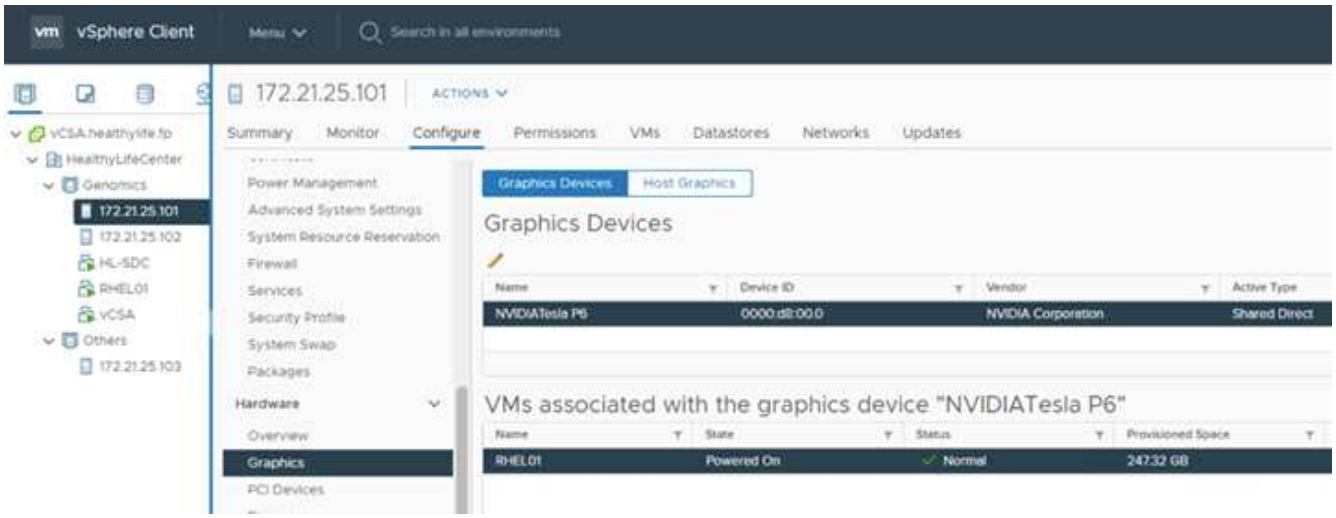
2. 이 설정을 위해 NVIDIA 파트너 포털에 등록되어 컴퓨팅 모드에서 GPU를 사용할 수 있는 평가 라이센스(소유권한이라고도 함)를 받았습니다.
3. NVIDIA 파트너 웹 사이트에서 필요한 NVIDIA vGPU 소프트웨어를 다운로드했습니다.
4. NVIDIA 파트너 웹 사이트에서 자격 '*.bin' 파일을 다운로드했습니다.
5. NVIDIA vGPU 라이센스 서버를 설치하고 NVIDIA 파트너 사이트에서 다운로드한 ' *.bin' 파일을 사용하여 라이센스 서버에 사용 권한을 추가했습니다.
6. NVIDIA 파트너 포털에서 배포할 올바른 NVIDIA vGPU 소프트웨어 버전을 선택하십시오. 이 설정에서는 드라이버 버전 460.73.02를 사용했습니다.
7. 이 명령은 를 설치합니다 "NVIDIA vGPU Manager" ESXi에서

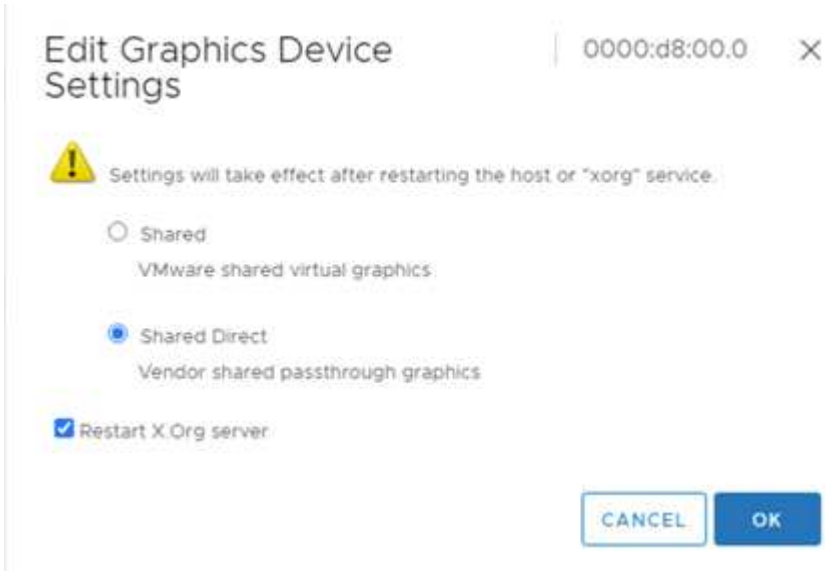
```
[root@localhost:~] esxcli software vib install -v
/vmfs/volumes/infra_datastore_nfs/nvidia/vib/NVIDIA_bootbank_NVIDIA-
VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992.vib
Installation Result
Message: Operation finished successfully.
Reboot Required: false
VIBs Installed: NVIDIA_bootbank_NVIDIA-
VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992
VIBs Removed:
VIBs Skipped:
```

8. ESXi 서버를 재부팅한 후 다음 명령을 실행하여 설치를 검증하고 GPU 상태를 확인하십시오.

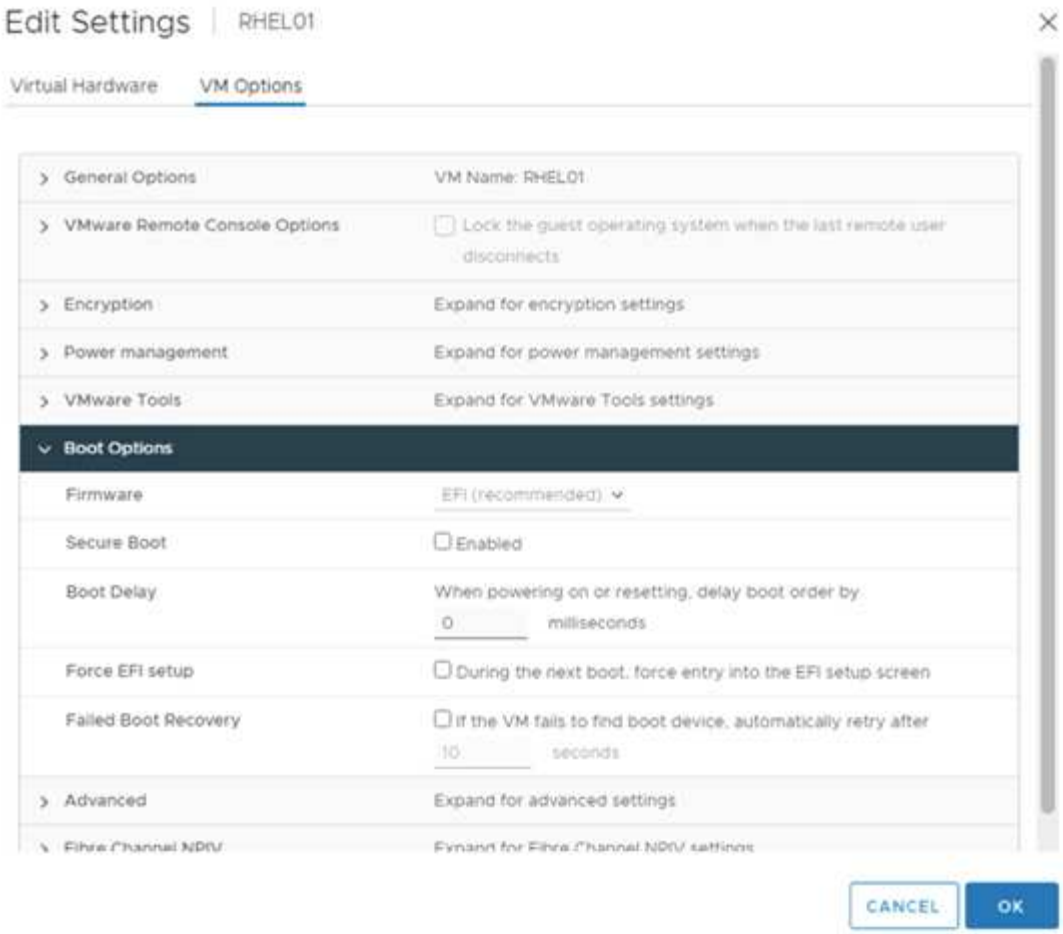
```
[root@localhost:~] nvidia-smi
Wed Aug 18 21:37:19 2021
+-----------------------------------------------------------------------------
------+
| NVIDIA-SMI 460.73.02    Driver Version: 460.73.02    CUDA Version: N/A
|
|-------------------------------+----------------------
+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
Compute M. |
|                               |                      |
MIG M. |
|===============================+======================+===============
======|
|   0  Tesla P6            On   | 00000000:D8:00.0 Off |
0 |
| N/A   35C    P8     9W /  90W |  15208MiB / 15359MiB |      0%
Default |
|                               |                      |
N/A |
+-------------------------------+----------------------
+----------------------+
+-----------------------------------------------------------------------------
------+
| Processes:
|
|  GPU   GI   CI        PID   Type   Process name                  GPU
Memory |
|        ID   ID                                                   Usage
|
|=============================================================================
======|
|    0   N/A  N/A   2812553    C+G   RHEL01
15168MiB |
+-----------------------------------------------------------------------------
------+
[root@localhost:~]
```

9. vCenter를 사용하면 "구성" 그래픽 장치 설정을 “Shared Direct”로 지정합니다.





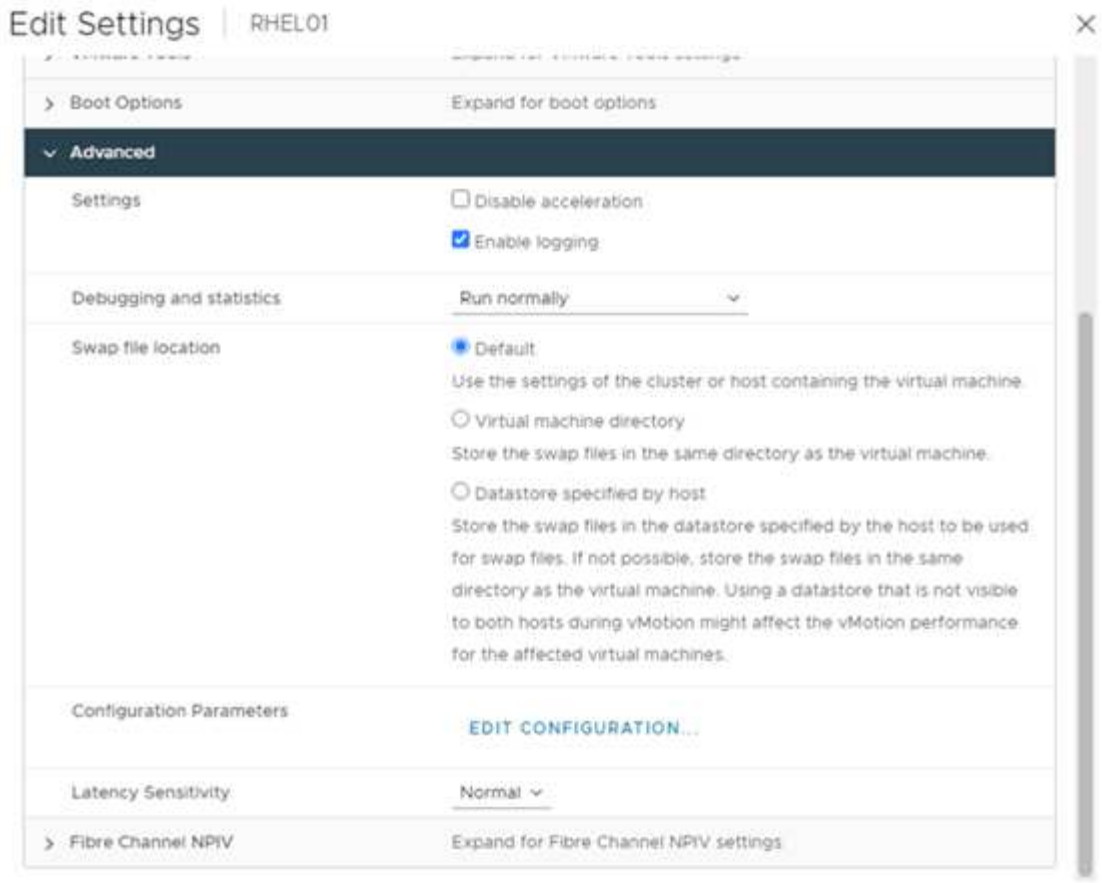
10. RedHat VM의 보안 부팅이 비활성화되어 있는지 확인합니다.
11. VM 부트 옵션 펌웨어가 EFI("참조")를 클릭합니다.

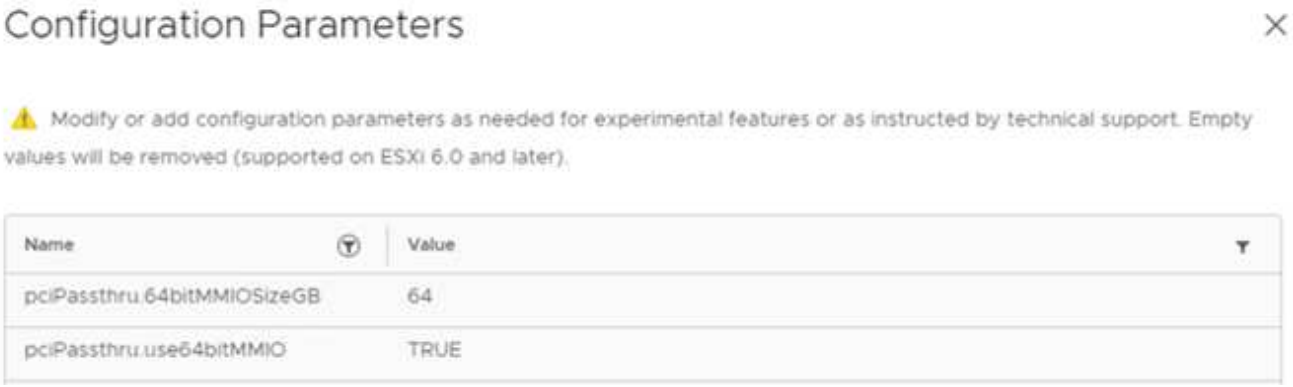


12. 다음 매개 변수가 VM 옵션 고급 편집 구성에 추가되었는지 확인합니다. "pciPassthru.64bitMMIOSizeGB" 매개 변수의 값은 GPU 메모리와 VM에 할당된 GPU 수에 따라 달라집니다. 예를 들면 다음과 같습니다.

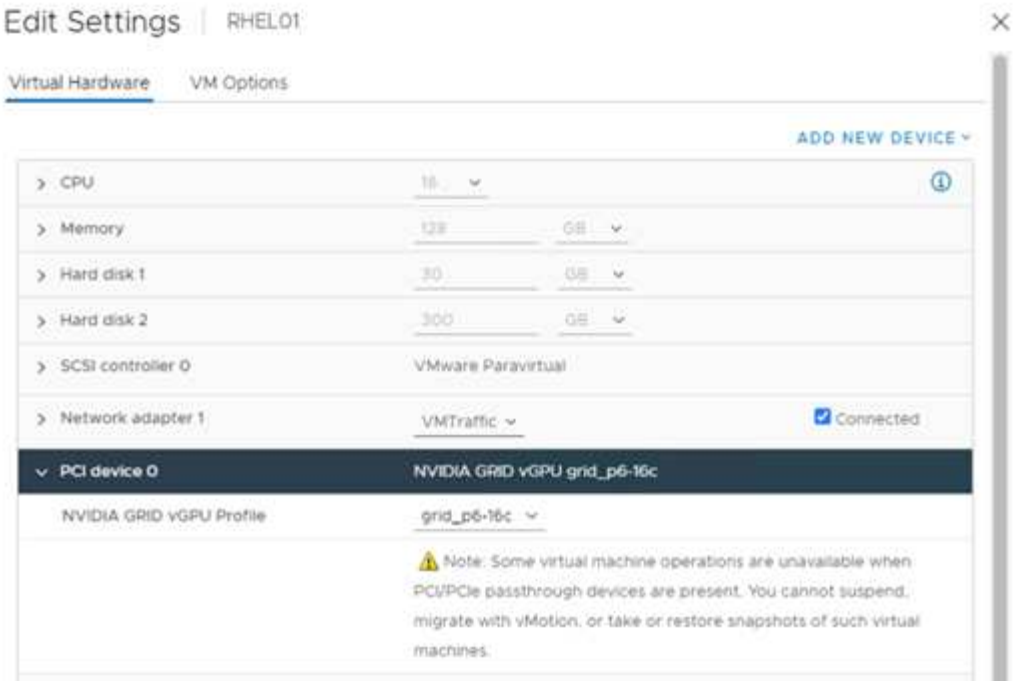
    a. VM에 4개의 32GB V100 GPU가 할당된 경우 이 값은 128이어야 합니다.

    b. VM에 16GB P6 GPU 4개가 할당된 경우 이 값은 64여야 합니다.





13. vGPU를 vCenter의 가상 머신에 새 PCI 장치로 추가할 때는 NVIDIA GRID vGPU를 PCI Device 유형으로 선택해야 합니다.
14. 사용 중인 GPU, GPU 메모리 및 사용 목적(예: 그래픽 대 컴퓨팅)에 맞는 GPU 프로필을 선택합니다.



15. RedHat Linux VM에서 NVIDIA 드라이버는 다음 명령을 실행하여 설치할 수 있습니다.

```
[root@genomics1 genomics]#sh NVIDIA-Linux-x86_64-460.73.01-grid.run
```

16. 다음 명령을 실행하여 올바른 vGPU 프로필이 보고되고 있는지 확인합니다.

```
[root@genomics1 genomics]# nvidia-smi -query-gpu=gpu_name
-format=csv,noheader -id=0 | sed -e 's/ /-/g'
GRID-P6-16C
[root@genomics1 genomics]#
```

17. 재부팅 후 올바른 NVIDIA vGPU가 드라이버 버전과 함께 보고되었는지 확인합니다.

```
[root@genomics1 genomics]# nvidia-smi
Wed Aug 18 20:30:56 2021
+-----------------------------------------------------------------------------
------+
| NVIDIA-SMI 460.73.01    Driver Version: 460.73.01    CUDA Version:
11.2     |
|-------------------------------+----------------------
+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
Compute M. |
|                               |                      |
MIG M. |
|===============================+======================+===============
======|
|   0  GRID P6-16C         On   | 00000000:02:02.0 Off |
N/A |
| N/A   N/A    P8    N/A /  N/A |   2205MiB / 16384MiB |      0%
Default |
|                               |                      |
N/A |
+-------------------------------+----------------------
+----------------------+
+-----------------------------------------------------------------------------
------+
| Processes:
|
|  GPU   GI   CI        PID   Type   Process name                  GPU
Memory |
|        ID   ID                                                   Usage
|
|=============================================================================
======|
|    0   N/A  N/A      8604      G   /usr/libexec/Xorg
13MiB |
+-----------------------------------------------------------------------------
------+
[root@genomics1 genomics]#
```

18. 라이센스 서버 IP가 vGPU 그리드 구성 파일의 VM에 구성되어 있는지 확인합니다.
    a. 템플릿을 복사합니다.

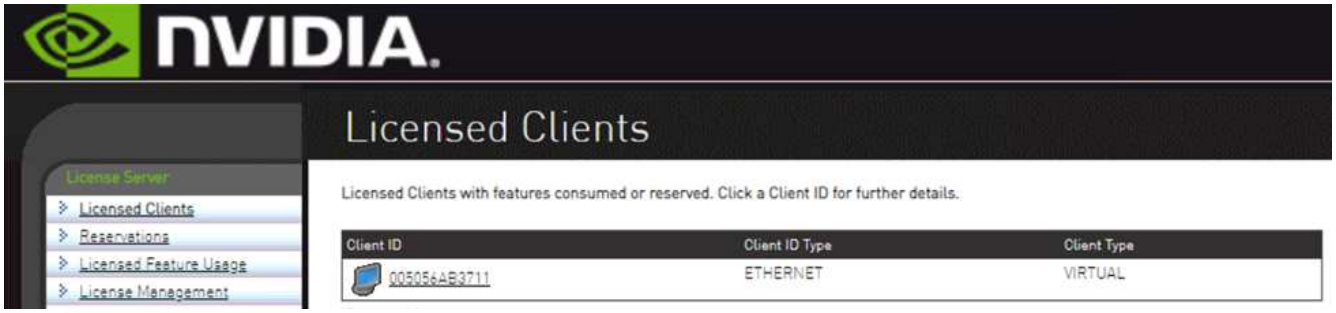
```
[root@genomics1 genomics]# cp /etc/nvidia/gridd.conf.template
/etc/nvidia/gridd.conf
```

b. 파일 '/etc/nvidia/rrid.conf'를 편집하고 라이센스 서버 IP 주소를 추가한 다음 기능 유형을 1로 설정합니다.

```
ServerAddress=192.168.169.10
```

```
FeatureType=1
```

19. VM을 다시 시작한 후 라이센스 서버의 허가된 클라이언트 아래에 아래와 같은 항목이 표시됩니다.



20. GATK 및 Cromwell 소프트웨어 다운로드에 대한 자세한 내용은 솔루션 설정 섹션을 참조하십시오.
21. GATK가 구내에서 GPU를 사용할 수 있으면 워크플로 설명 언어 ' *. wdl은 아래와 같이 런타임 특성을 가지고 있다.

```
task ValidateBAM {
  input {
    # Command parameters
    File input_bam
    String output_basename
    String? validation_mode
    String gatk_path
    # Runtime parameters
    String docker
    Int machine_mem_gb = 4
    Int addtional_disk_space_gb = 50
  }
  Int disk_size = ceil(size(input_bam, "GB")) + addtional_disk_space_gb
  String output_name = "${output_basename}_${validation_mode}.txt"
  command {
    ${gatk_path} \
      ValidateSamFile \
      --INPUT ${input_bam} \
      --OUTPUT ${output_name} \
      --MODE ${default="SUMMARY" validation_mode}
  }
  runtime {
    gpuCount: 1
    gpuType: "nvidia-tesla-p6"
    docker: docker
    memory: machine_mem_gb + " GB"
    disks: "local-disk " + disk_size + " HDD"
  }
  output {
    File validation_report = "${output_name}"
  }
}
```

"다음: 결론."

결론

"이전: GPU 설정"

전 세계의 많은 의료 기관이 FlexPod를 공통 플랫폼으로 표준화했습니다. FlexPod를 사용하면 의료 기능을 안심하고 구현할 수 있습니다. ONTAP with NetApp FlexPod는 업계 최고 수준의 프로토콜 집합을 즉시 구현할 수 있는 표준 기능을 제공합니다. 유전체학을 특정 환자의 유전체학을 실행하라는 요청의 근원과 관계없이 FlexPod 플랫폼에서 상호 운용성, 접근성, 가용성 및 확장성이 기본으로 제공됩니다. FlexPod 플랫폼에서 표준화하면 혁신 문화가 전염됩니다.

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대한 자세한 내용은 다음 문서 및 웹 사이트를 참조하십시오.

- 딥 러닝용 Cisco UCS 480mL가 포함된 AI/ML용 FlexPod 데이터 센터

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_480ml_aiml_deployment.pdf"

- VMware vSphere 7.0 및 NetApp ONTAP 9.7을 사용하는 FlexPod 데이터 센터

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/fp_vmware_vsphere_7_0_ontap_9_7.html"

- ONTAP 9 문서 센터

  "http://docs.netapp.com"

- 민첩하고 효율적인 FlexPod으로 데이터 센터 현대화 실현

  "https://www.flexpod.com/idc-white-paper/"

- 의료 부문의 AI

  "https://www.netapp.com/us/media/na-369.pdf"

- 의료 분야의 혁신을 지원하는 FlexPod

  "https://flexpod.com/solutions/verticals/healthcare/"

- Cisco와 NetApp의 FlexPod

  "https://flexpod.com/"

- 의료 분야 AI 및 분석(NetApp)

  "https://www.netapp.com/us/artificial-intelligence/healthcare-ai-analytics/index.aspx"

- 의료 스마트 인프라 선택이 가능한 AI는 성공을 높여줍니다

  https://www.netapp.com/pdf.html?item=/media/7410-wp-7314.pdf

- ONTAP 9.8이 지원되는 FlexPod 데이터 센터, Cisco Intersight용 ONTAP 스토리지 커넥터 및 Cisco Intersight 관리 모드

  https://www.netapp.com/pdf.html?item=/media/25001-tr-4883.pdf

- FlexPod Datacenter 및 Red Hat Enterprise Linux OpenStack 플랫폼

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_openstack_osp6.html"

버전 기록

버전	날짜	문서 버전 기록
버전 1.0	2021년 11월	최초 릴리스.

MEDITECH 방향 사이징 가이드용 FlexPod

TR-4774: MEDITECH 방향 크기 조정을 위한 FlexPod

Brandon AGEE, John Duignan, NetApp Mike Brennan, Cisco 존 에브메르

파트너 후원: 

이 보고서는 MEDITECH EHR 애플리케이션 소프트웨어 환경에 대한 FlexPod 사이징 지침을 제공합니다.

목적

FlexPod 시스템은 MEDITECH의 드넓은 서비스, 6.x, 5.x 및 Magic 서비스를 호스팅하기 위해 구축할 수 있습니다. MEDITECH 애플리케이션 계층을 호스팅하는 FlexPod 서버는 신뢰할 수 있는 고성능 인프라를 위한 통합 플랫폼을 제공합니다. FlexPod 통합 플랫폼은 숙련된 FlexPod 채널 파트너가 신속하게 구축하며 Cisco 및 NetApp 기술 지원 센터에서 지원합니다.

사이징은 MEDITECH의 하드웨어 구성 제안서와 MEDITECH 작업 문서의 정보를 기반으로 합니다. 목표는 컴퓨팅, 네트워크 및 스토리지 인프라 구성요소에 대한 최적의 크기를 결정하는 것입니다.

를 클릭합니다 "MEDITECH 워크로드 개요" 섹션에서는 MEDITECH 환경에서 찾을 수 있는 컴퓨팅 및 스토리지 워크로드의 유형에 대해 설명합니다.

를 클릭합니다 "소규모, 중간 규모 및 대규모 아키텍처에 대한 기술 사양" 섹션에서는 섹션에 설명된 다양한 스토리지 아키텍처에 대한 샘플 BOM을 자세히 설명합니다. 제공된 설정은 일반 지침일 뿐입니다. 항상 작업 부하에 따라 sizer를 사용하여 시스템의 크기를 조정하고 그에 따라 구성을 조정합니다.

전반적인 솔루션 이점

FlexPod 아키텍처를 기반으로 MEDITECH 환경을 실행하면 의료 조직의 생산성을 향상시키고 자본 및 운영 비용을 줄일 수 있습니다. FlexPod은 Cisco와 NetApp의 전략적 파트너십을 통해 사전 검증된 엄격한 테스트를 거친 통합 인프라를 제공합니다. 지연 시간이 짧고 예측 가능한 시스템 성능과 고가용성을 제공하도록 특별히 설계되고 제작되었습니다. 이 접근 방식은 MEDITECH EHR 시스템 사용자의 응답 시간을 단축합니다.

Cisco와 NetApp의 FlexPod 솔루션은 고성능, 모듈식, 사전 검증, 통합, 가상화 및 효율성, 확장성 및 비용 효율적인 플랫폼 MEDITECH가 포함된 FlexPod 데이터 센터는 다음과 같은 의료 산업에 고유한 이점을 제공합니다.

- * 모듈식 아키텍처 *. FlexPod는 각 특정 워크로드에 맞게 사용자 지정된 FlexPod 시스템으로 MEDITECH 모듈식 아키텍처의 다양한 요구를 해결합니다. 모든 구성 요소는 클러스터 서버 및 스토리지 관리 패브릭을 통해 연결되며 일관된 관리 툴셋을 사용합니다.
- * 운영 간소화 및 비용 절감 *. 기존 플랫폼을 보다 효율적이고 확장 가능한 공유 리소스로 대체함으로써 기존 플랫폼의 비용과 복잡성을 제거하고 임상의가 어디에 있든 지원할 수 있습니다. 이 솔루션을 사용하면 리소스를 더

효율적으로 사용하여 ROI(투자 수익)를 높일 수 있습니다.

- * 인프라의 구축 시간 단축 *. MEDITECH가 포함된 FlexPod 데이터 센터의 통합 설계를 통해 고객은 현장 및 원격 데이터 센터 모두에서 새로운 인프라를 빠르고 쉽게 가동 및 실행할 수 있습니다.
- * 스케일아웃 아키텍처 *. 실행 중인 애플리케이션을 재구성하지 않고도 SAN 및 NAS를 테라바이트에서 수십 페타바이트 단위로 확장할 수 있습니다.
- 무중단 운영 *: 비즈니스를 중단하지 않고 스토리지 유지보수, 하드웨어 라이프사이클 운영 및 소프트웨어 업그레이드를 수행할 수 있습니다.
- * 보안 멀티 테넌시 *. 이 이점은 가상화된 서버 및 공유 스토리지 인프라의 더 많은 요구사항을 지원하여 시설별 정보의 안전한 멀티 테넌시를 지원합니다. 이 이점은 여러 데이터베이스 및 소프트웨어 인스턴스를 호스팅하는 경우 중요합니다.
- * 풀링된 리소스 최적화 *. 이 이점은 물리적 서버 및 스토리지 컨트롤러 수를 줄이고, 워크로드 수요 로드 밸런싱을 수행하고, 활용률을 높이고, 성능을 동시에 개선하는 데 도움이 됩니다.
- * 서비스 품질(QoS). * FlexPod은 전체 스택에서 서비스 품질(QoS)을 제공합니다. 업계 최고 수준의 QoS 스토리지 정책을 통해 공유 환경에서 차별화된 서비스 수준을 지원합니다. 이러한 정책을 통해 워크로드에 맞는 성능을 최적화하고 급등하는 애플리케이션을 격리 및 제어하는 데 도움을 줄 수 있습니다.
- * 스토리지 효율성 *. NetApp 7:1 스토리지 효율성으로 스토리지 비용을 절감할 수 있습니다.
- * 민첩성 *. FlexPod 시스템에서 제공하는 업계 최고의 워크플로우 자동화, 오케스트레이션, 관리 툴을 사용하면 비즈니스 요청에 훨씬 더 빠르게 대응할 수 있습니다. 이러한 비즈니스 요청은 MEDITECH 백업 및 더 많은 테스트 및 교육 환경의 프로비저닝에서 인구 상태 관리 이니셔티브를 위한 분석 데이터베이스 복제까지 다양합니다.
- * 생산성 *. 이 솔루션을 신속하게 배포하고 확장하여 최적의 청능사 최종 사용자 환경을 구현할 수 있습니다.
- * 데이터 패브릭 *. NetApp Data Fabric 아키텍처는 물리적 경계 및 애플리케이션 전반에 걸쳐 데이터를 제공합니다. NetApp Data Fabric은 데이터 중심 세계에서 데이터 중심 기업을 위해 구축되었습니다. 데이터는 여러 위치에서 생성 및 사용되며 종종 애플리케이션 및 인프라와 공유됩니다. Data Fabric은 일관되고 통합된 데이터를 관리할 수 있는 방법을 제공합니다. 또한 IT에서 데이터를 더 많이 제어하고 끊임없이 증가하는 IT 복잡성을 단순화할 수 있습니다.

범위

이 문서에서는 Cisco UCS 및 NetApp ONTAP 기반 스토리지를 사용하는 환경에 대해 설명합니다. MEDITECH 호스팅을 위한 샘플 참조 아키텍처를 제공합니다.

다음 항목은 다루지 않습니다.

- SPM(NetApp System Performance Modeler) 또는 기타 NetApp 사이징 툴을 사용하여 세부 사이징 지침을 확인할 수 있습니다.
- 비운영 워크로드에 대한 사이징

대상

이 문서는 NetApp 및 파트너 시스템 엔지니어와 NetApp 프로페셔널 서비스 직원을 대상으로 합니다. NetApp은 사용자가 컴퓨팅 및 스토리지 사이징 개념을 잘 이해하고 있으며 Cisco UCS 및 NetApp 스토리지 시스템에 대한 기술적 지식이 충분히 있다고 가정합니다.

관련 문서

다음 기술 보고서 및 기타 문서는 이 기술 보고서와 관련이 있으며, FlexPod 인프라에서 MEDITECH를 사이징, 설계 및 배포하는 데 필요한 전체 문서 세트를 작성합니다.

- "TR-4753: MEDITECH용 FlexPod 데이터 센터 배포 가이드"
- "TR-4190: MEDITECH 환경을 위한 NetApp 사이징 지침"
- "TR-4319: MEDITECH 환경을 위한 NetApp 구축 지침"

일부 보고서에 액세스하려면 NetApp Field Portal의 로그인 자격 증명이 필요합니다.

MEDITECH 워크로드 개요

이 섹션에서는 MEDITECH 환경에서 얻을 수 있는 컴퓨팅 및 스토리지 워크로드의 유형에 대해 설명합니다.

MEDITECH 및 백업 워크로드

MEDITECH 환경에 맞게 NetApp 스토리지 시스템을 사이징할 때는 MEDITECH 운영 워크로드와 백업 워크로드를 모두 고려해야 합니다.

MEDITECH 호스트
MEDITECH 호스트는 데이터베이스 서버입니다. 이 호스트는 MEDITECH 파일 서버(광활함, 6.x 또는 C/S 5.x 플랫폼) 또는 Magic 시스템(매직 플랫폼)이라고도 합니다. 이 문서에서는 MEDITECH 호스트라는 용어를 사용하여 MEDITECH 파일 서버 및 Magic 시스템을 참조합니다.

다음 섹션에서는 이러한 두 워크로드의 I/O 특성 및 성능 요구사항에 대해 설명합니다.

MEDITECH 워크로드

MEDITECH 환경에서 MEDITECH 소프트웨어를 실행하는 여러 서버는 MEDITECH 시스템이라는 통합 시스템으로 다양한 작업을 수행합니다. MEDITECH 시스템에 대한 자세한 내용은 MEDITECH 설명서를 참조하십시오.

- 프로덕션 MEDITECH 환경의 경우 해당 MEDITECH 설명서를 참조하여 NetApp 스토리지 시스템 사이징에 포함되어야 하는 MEDITECH 호스트 수와 스토리지 용량을 확인하십시오.
- 새 MEDITECH 환경의 경우 하드웨어 구성 제안 문서를 참조하십시오. 기존 MEDITECH 환경의 경우 하드웨어 평가 작업 문서를 참조하십시오. 하드웨어 평가 작업은 MEDITECH 티켓과 연결됩니다. 고객은 MEDITECH에서 이러한 문서 중 하나를 요청할 수 있습니다.

호스트를 추가하여 용량과 성능을 향상시키도록 MEDITECH 시스템을 확장할 수 있습니다. 각 호스트에는 데이터베이스 및 애플리케이션 파일을 위한 스토리지 용량이 필요합니다. 각 MEDITECH 호스트에서 사용할 수 있는 스토리지는 호스트에서 생성된 입출력도 지원해야 합니다. MEDITECH 환경에서는 각 호스트에 대해 LUN을 사용하여 해당 호스트의 데이터베이스 및 애플리케이션 스토리지 요구 사항을 지원할 수 있습니다. MEDITECH 범주의 유형과 배포하는 플랫폼 유형에 따라 각 MEDITECH 호스트와 시스템 전체의 워크로드 특성이 결정됩니다.

MEDITECH 범주

MEDITECH는 배포 크기를 1에서 6 사이의 범주 번호와 연결합니다. 범주 1은 가장 작은 MEDITECH 배포이며 범주 6은 가장 큰 배포입니다. 각 범주와 관련된 MEDITECH 애플리케이션 사양의 예로는 다음과 같은 메트릭이 있습니다.

- 병원 침대 수
- 연간 입원 환자 수

- 연간 외래 환자 수
- 매년 응급실 방문
- 연간 검사 횟수
- 1일 입원 환자 처방
- 외래 환자 처방전/일일

MEDITECH 범주에 대한 자세한 내용은 MEDITECH 범주 참조 시트를 참조하십시오. MEDITECH에서 고객 또는 MEDITECH 시스템 설치 프로그램을 통해 이 시트를 얻을 수 있습니다.

MEDITECH 플랫폼

MEDITECH의 4가지 플랫폼:

- 드넓은 공간을 제공합니다
- MEDITECH 6.x
- 클라이언트/서버 5.x(C/S 5.x)
- 마법

MEDITECH의 경우, 6.x 및 C/S 5.x 플랫폼의 경우 각 호스트의 입출력 특성이 요청 크기가 4,000인 100% 랜덤으로 정의됩니다. MEDITECH Magic 플랫폼의 경우 각 호스트의 입출력 특성은 요청 크기가 8,000 또는 16,000인 100% 랜덤으로 정의됩니다. MEDITECH에 따르면 일반적인 매직 프로덕션 배포의 요청 크기는 8,000 또는 16,000입니다.

읽기 및 쓰기 비율은 구축하는 플랫폼에 따라 다릅니다. MEDITECH는 읽기 및 쓰기의 평균 조합을 추정하고 백분율로 표시합니다. 또한 MEDITECH는 특정 MEDITECH 플랫폼의 각 MEDITECH 호스트에 필요한 평균 지속 IOPS 값을 예측합니다. 아래 표에는 MEDITECH에서 제공하는 플랫폼별 I/O 특성이 요약되어 있습니다.

MEDITECH 범주	**MEDITECH** 플랫폼	평균 랜덤 읽기 **%**	평균 랜덤 쓰기 **%**	**MEDITECH** 호스트당 평균 지속 **IOPS**
1	드넓은 6.x	20	80	750입니다
2-6	드넓은 공간을 제공합니다	20	80	750입니다
	6.x	20	80	750입니다
	C/S 5.x	40	60	600
	마법	90	10	400

MEDITECH 시스템에서 각 호스트의 평균 IOPS 레벨은 위 표에 정의된 IOPS 값과 같아야 합니다. 각 플랫폼을 기반으로 올바른 스토리지 사이징을 결정하려면 위의 표에 지정된 IOPS 값이 에 설명된 사이징 방법론의 일부로 사용됩니다 "소규모, 중간 규모 및 대규모 아키텍처에 대한 기술 사양" 섹션을 참조하십시오.

MEDITECH는 각 호스트에 대해 평균 랜덤 쓰기 지연 시간을 1ms 미만으로 유지해야 합니다. 그러나 백업 및 재할당 작업 중에 쓰기 지연 시간을 최대 2ms까지 일시적으로 늘릴 수 있는 것으로 간주됩니다. 또한 MEDITECH는 범주 1 호스트의 경우 평균 랜덤 읽기 지연 시간이 7ms 미만이고 범주 2 호스트의 경우 5ms 미만이어야 합니다. 이러한 지연 시간 요구 사항은 어떤 MEDITECH 플랫폼을 사용하는지에 관계없이 모든 호스트에 적용됩니다.

아래 표에는 MEDITECH 워크로드에 대한 NetApp 스토리지의 크기를 조정할 때 고려해야 하는 I/O 특성이 요약되어 있습니다.

매개 변수	**MEDITECH** 범주	드넓은 공간을 제공합니다	**MEDITECH 6.x**	**C/S 5.x**	마법
요청 크기입니다	1-6	4K	4K	4K	8K 또는 16K
랜덤/순차		100% 랜덤	100% 랜덤	100% 랜덤	100% 랜덤
평균 지속 IOPS	1	750입니다	750입니다	해당 없음	해당 없음
	2-6	750입니다	750입니다	600	400
읽기/쓰기 속도	1-6	20% 읽기, 80% 쓰기	20% 읽기, 80% 쓰기	40% 읽기, 60% 쓰기	90% 읽기, 10% 쓰기
쓰기 지연 시간		1ms 미만	1ms 미만	1ms 미만	1ms 미만
일시적인 최대 쓰기 지연 시간입니다	1-6	2ms 미만	2ms 미만	2ms 미만	2ms 미만
읽기 지연 시간	1	7ms 미만	7ms 미만	해당 없음	해당 없음
	2-6	5ms 미만	5ms 미만	5ms 미만	5ms 미만

범주 3에서 6까지의 MEDITECH 호스트는 범주 2와 동일한 I/O 특성을 갖습니다. MEDITECH 범주 2 - 6의 경우 각 범주에 구축된 호스트 수가 다릅니다.

NetApp 스토리지 시스템은 이전 섹션에서 설명한 성능 요구사항을 충족할 수 있도록 사이징해야 합니다. NetApp 스토리지 시스템은 MEDITECH 운영 워크로드 외에도 다음 섹션에 설명된 대로 백업 작업 중에 이러한 MEDITECH 성능 목표를 유지할 수 있어야 합니다.

백업 워크로드 설명

MEDITECH 인증 백업 소프트웨어는 MEDITECH 시스템의 각 MEDITECH 호스트에서 사용하는 LUN을 백업합니다. 백업이 애플리케이션 정합성 보장 상태에 있도록 백업 소프트웨어는 MEDITECH 시스템을 중지시키고 디스크에 대한 입출력 요청을 일시 중단합니다. 시스템이 중지 상태에 있는 동안 백업 소프트웨어는 NetApp 스토리지 시스템에 명령을 발행하여 LUN이 포함된 볼륨의 NetApp 스냅샷 복사본을 생성합니다. 나중에 백업 소프트웨어가 MEDITECH 시스템을 중지하여 운영 I/O 요청을 데이터베이스로 계속 진행할 수 있도록 합니다. 스냅샷 복사본을 기반으로 NetApp FlexClone 볼륨이 생성됩니다. 이 볼륨은 LUN을 호스팅하는 상위 볼륨에서 운영 입출력 요청이 계속 진행되는 동안 백업 소스에서 사용됩니다.

백업 소프트웨어에서 생성되는 워크로드는 FlexClone 볼륨에 상주하는 LUN을 순차적으로 읽음으로써 발생합니다. 워크로드는 요청 크기가 64,000인 100% 순차적 읽기 워크로드로 정의됩니다. MEDITECH 운영 워크로드의 성능 기준은 필요한 IOPS 및 관련 읽기/쓰기 지연 시간 수준을 유지하는 것입니다. 그러나 백업 워크로드의 경우 백업 작업 중에 생성되는 전체 데이터 처리량(MBps)으로 주의를 이동합니다. MEDITECH LUN 백업은 8시간 백업 기간에 완료되어야 하지만, NetApp은 모든 MEDITECH LUN 백업을 6시간 이내에 완료할 것을 권장합니다. 백업을 6시간 이내에 완료하는 것을 목표로 MEDITECH 워크로드의 계획되지 않은 증가, NetApp ONTAP 백그라운드 작업 또는 시간의 경과에 따른 데이터 증가와 같은 이벤트를 완화합니다. 이러한 이벤트 중 하나라도 발생하면 추가 백업 시간이 발생할 수 있습니다. 백업 소프트웨어는 저장된 애플리케이션 데이터의 양에 관계없이 각 MEDITECH 호스트에 대해 전체 LUN의 블록 레벨 백업을 수행합니다.

이 창 내에서 백업을 완료하는 데 필요한 순차적 읽기 처리량을 계산하는 방법은 다음과 같은 다른 요인의 기능입니다.

- 원하는 백업 기간
- LUN의 수입니다

- 백업할 각 LUN의 크기입니다

예를 들어 각 호스트의 LUN 크기가 200GB인 50개 호스트 MEDITECH 환경에서는 백업할 총 LUN 용량이 10TB입니다.

10TB의 데이터를 8시간 내에 백업하려면 다음과 같은 처리량이 필요합니다.

- = (10 x 10^6)MB(8 x 3,600)s
- = 347.2MBps

그러나 예상치 못한 이벤트를 고려하여 6시간 이상의 여유 공간을 제공하기 위해 5.5시간의 보수적인 백업 윈도우가 선택됩니다.

10TB의 데이터를 8시간 내에 백업하려면 다음과 같은 처리량이 필요합니다.

- = (10 x 10^6) MB(5.5 x 3,600)s
- = 500Mbps

500Mbps의 처리량에서 5.5시간 이내에 백업을 완료할 수 있으며, 8시간의 백업 요구 사항에서도 편안하게 백업이 가능합니다.

아래 표에는 스토리지 시스템의 크기를 조정할 때 사용할 백업 워크로드의 I/O 특성이 요약되어 있습니다.

매개 변수	모든 플랫폼
요청 크기입니다	64K
랜덤/순차	100% 순차적
읽기/쓰기 속도	100% 읽기
평균 처리량	MEDITECH 호스트의 수와 각 LUN의 크기에 따라 백업이 8시간 이내에 완료되어야 합니다.
백업 기간이 필요합니다	8시간

MEDITECH용 **Cisco UCS** 참조 아키텍처

MEDITECH on FlexPod의 아키텍처는 MEDITECH, Cisco 및 NetApp의 지침과 모든 규모의 MEDITECH 고객과 협력하는 파트너 경험을 바탕으로 합니다. 이 아키텍처는 고객의 데이터 센터 전략(소규모 또는 대규모, 중앙 집중식, 분산 또는 멀티 테넌트)에 따라 적응 가능하며 MEDITECH의 모범 사례를 적용합니다.

MEDITECH를 배포할 때 Cisco는 MEDITECH의 모범 사례와 직접 일치하는 Cisco UCS 참조 아키텍처를 설계했습니다. Cisco UCS는 고성능, 고가용성, 안정성, 확장성을 위해 긴밀하게 통합된 솔루션을 제공하여 수천 개의 병상을 보유한 의사 및 병원 시스템을 지원합니다.

소형, 중형 및 대형 아키텍처의 기술 사양

이 섹션에서는 다양한 크기의 스토리지 아키텍처에 대한 샘플 BOM에 대해 설명합니다.

소형, 중형 및 대형 아키텍처용 **BOM.**

FlexPod 설계는 다양한 구성 요소와 소프트웨어 버전을 포괄하는 유연한 인프라입니다. 사용 "TR-4036: FlexPod 기술

사양" 유효한 FlexPod 구성을 조립하는 방법에 대한 설명서로, 아래 표의 구성은 FlexPod의 최소 요구사항이며 단지 샘플일 뿐입니다. 다양한 환경 및 사용 사례에 따라 각 제품군별로 구성을 확장할 수 있습니다.

이 사이징 연습의 경우 Category 3 MEDITECH 환경에 해당하고, Medium에서 Category 5까지, Large에서 Category 6까지

	작은 크기	중간	대형
플랫폼	하나의 NetApp AFF A220 All-Flash 스토리지 시스템 HA 쌍입니다	하나의 NetApp AFF A220 HA 쌍입니다	NetApp AFF A300 All-Flash 스토리지 시스템 HA 쌍 1개
디스크 쉘프	9TB x 3.8TB	13TB x 3.8TB	19TB x 3.8TB
MEDITECH 데이터베이스 크기입니다	3TB-12TB	17TB	> 30TB
MEDITECH IOPS	22,000 IOPS 미만	25,000 IOPS 초과	32,000 IOPS 초과
총 IOPS	22000	27000	35000
원시	34.2TB	49.4TB	68.4TB
사용 가능한 용량	18.53TiB	27.96TiB	33.82TiB
실제 용량(2:1 스토리지 효율성)	55.6TiB	83.89TiB	101.47TiB

일부 고객 환경에서는 여러 MEDITECH 운영 워크로드가 동시에 실행되거나 더 높은 IOPS 요구 사항이 있을 수 있습니다. 이 경우, NetApp 세일즈 팀과 협력하여 필요한 IOPS 및 용량에 따라 스토리지 시스템을 조정합니다. 따라서 워크로드를 처리하는 데 적합한 플랫폼을 결정할 수 있어야 합니다. 예를 들어, NetApp AFF A700 All-Flash 스토리지 시스템 HA 쌍에서 여러 MEDITECH 환경을 성공적으로 실행하는 고객이 있습니다.

다음 표에는 MEDITECH 구성에 필요한 표준 소프트웨어가 나와 있습니다.

소프트웨어	제품군	버전 또는 릴리스	세부 정보
스토리지	ONTAP	ONTAP 9.4 일반 가용성(GA)	
네트워크	Cisco UCS 패브릭 인터커넥트	Cisco UCSM 4.x	현재 권장 릴리스
	Cisco Nexus 이더넷 스위치	7.0(3) i7(6)	현재 권장 릴리스
	Cisco FC: Cisco MDS 9132T	8.3(2)	현재 권장 릴리스
하이퍼바이저	하이퍼바이저	VMware vSphere ESXi 6.7을 참조하십시오	
	가상 머신(VM)	Windows 2016	

소프트웨어	제품군	버전 또는 릴리스	세부 정보
관리	하이퍼바이저 관리 시스템	VMware vCenter Server 6.7 U1(VCSA)	
	NetApp 가상 스토리지 콘솔(VSC)	VSC 7.0P1	
	NetApp SnapCenter를 참조하십시오	SnapCenter 4.0	
	Cisco UCS Manager를 참조하십시오	4.x	

다음 표에서는 소규모(범주 3) 구성 예, 즉 인프라 구성 요소를 보여 줍니다.

레이어	제품군	수량 및 모델	세부 정보
컴퓨팅	Cisco UCS 5108 섀시	1	최대 8개의 반폭 또는 4개의 전폭 블레이드를 지원합니다. 서버 요구 사항이 증가함에 따라 섀시를 추가합니다.
	Cisco 섀시 I/O 모듈	2 x 2208	8GB x 10GB 업링크 포트
	Cisco UCS 블레이드 서버	B200 M5 4개	각각 2개의 14코어, 2.6GHz 이상의 클럭 속도 및 384GB BIOS 3.2(3#)
	Cisco UCS 가상 인터페이스 카드	UCS 1440 4개	VMware ESXi FNIC FC 드라이버:1.6.0.47 VMware ESXi eNIC 이더넷 드라이버:1.0.27.0(상호 운용성 매트릭스 참조:
	Cisco UCS Fabric Interconnect(Fi) 2개	UCS 6454 FI 2개	10/25/100Gb 이더넷 및 32Gb FC를 지원하는 4세대 패브릭 인터커넥트
네트워크	Cisco 이더넷 스위치	Nexus 9336c-FX2 2개	1GB, 10GB, 25GB, 40GB, 100GB입니다
스토리지 네트워크	BLOB 스토리지용 IP 네트워크 Nexus 9k		FI 및 UCS 섀시
	FC: Cisco MDS 9132T		Cisco 9132T 스위치 2개
스토리지	NetApp AFF A300 All-Flash 스토리지 시스템	1개의 HA 쌍	모든 MEDITECH 워크로드(파일 서버, 이미지 서버, SQL Server, VMware 등)를 위한 2노드 클러스터
	DS224C 디스크 쉘프	DS224C 디스크 쉘프 1개	
	솔리드 스테이트 드라이브(SSD)	9 x 3.8TB	

다음 표에서는 중간 규모(범주 5)의 구성 예, 즉 인프라 구성 요소를 보여 줍니다

레이어	제품군	수량 및 모델	세부 정보
컴퓨팅	Cisco UCS 5108 섀시	1	최대 8개의 반폭 또는 4개의 전폭 블레이드를 지원합니다. 서버 요구 사항이 증가함에 따라 섀시를 추가합니다.
	Cisco 섀시 I/O 모듈	2 x 2208	8GB x 10GB 업링크 포트
	Cisco UCS 블레이드 서버	B200 M5 6개	각각 16코어 2개, 2.5GHz/이상의 클럭 속도, 384GB 이상의 메모리 BIOS 3.2(3#)
	Cisco UCS 가상 인터페이스 카드(VIC)	UCS 1440 VICS 6개	VMware ESXi FNIC FC 드라이버:1.6.0.47 VMware ESXi eNIC 이더넷 드라이버:1.0.27.0(상호 운용성 매트릭스 참조:)
	Cisco UCS Fabric Interconnect(Fi) 2개	UCS 6454 FI 2개	10GB/25GB/100Gb 이더넷 및 32Gb FC를 지원하는 4세대 패브릭 인터커넥트
네트워크	Cisco 이더넷 스위치	Nexus 9336c-FX2 2개	1GB, 10GB, 25GB, 40GB, 100GB입니다
스토리지 네트워크	BLOB 스토리지용 IP 네트워크 Nexus 9k		
	FC: Cisco MDS 9132T		Cisco 9132T 스위치 2개
스토리지	NetApp AFF A220 All-Flash 스토리지 시스템	2개의 HA 쌍	모든 MEDITECH 워크로드(파일 서버, 이미지 서버, SQL Server, VMware 등)를 위한 2노드 클러스터
	DS224C 디스크 쉘프	DS224C 디스크 쉘프 1개	
	SSD를 지원합니다	3.8TB 13개	

다음 표에서는 대규모(범주 6) 구성 예, 즉 인프라 구성 요소를 보여 줍니다.

레이어	제품군	수량 및 모델	세부 정보
컴퓨팅	Cisco UCS 5108 섀시	1	
	Cisco 섀시 I/O 모듈	2 x 2208	10GB 업링크 포트 8개
	Cisco UCS 블레이드 서버	8x B200 M5	각각 24코어 2개, 2.7GHz 및 768GB BIOS 3.2(3#)
	Cisco UCS 가상 인터페이스 카드(VIC)	UCS 1440 VICS 8개	VMware ESXi FNIC FC 드라이버: 1.6.0.47 VMware ESXi eNIC 이더넷 드라이버: 1.0.27.0 (상호 운용성 매트릭스 검토:
	2 x Cisco UCS 패브릭 인터커넥트(FI)	UCS 6454 FI 2개	10GB/25GB/100Gb 이더넷 및 32Gb FC를 지원하는 4세대 패브릭 인터커넥트
네트워크	Cisco 이더넷 스위치	Nexus 9336c-FX2 2개	Cisco Nexus 9332PQ1 2개, 10GB, 25GB, 40GB, 100GB
스토리지 네트워크	BLOB 스토리지용 IP 네트워크 N9k		
	FC: Cisco MDS 9132T		Cisco 9132T 스위치 2개
스토리지	AFF A300	1개의 HA 쌍	모든 MEDITECH 워크로드(파일 서버, 이미지 서버, SQL Server, VMware 등)를 위한 2노드 클러스터
	DS224C 디스크 쉘프	DS224C 디스크 쉘프 1개	
	SSD를 지원합니다	19 x 3.8TB	

이러한 구성은 사이징 지침을 위한 출발점을 제공합니다. 일부 고객 환경에서는 여러 MEDITECH 운영 및 비 MEDITECH 워크로드가 동시에 실행되거나 더 높은 IOP 요구사항이 있을 수 있습니다. NetApp 세일즈 팀과 협력하여 필요한 IOPS, 워크로드 및 용량을 기준으로 스토리지 시스템의 규모를 조정하면서 워크로드를 지원하는 데 적합한 플랫폼을 결정해야 합니다.

추가 정보

이 문서에 설명된 정보에 대한 자세한 내용은 다음 문서 또는 웹 사이트를 참조하십시오.

- FC Cisco Validated Design이 구축된 FlexPod 데이터 센터

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html"

- MEDITECH 환경을 위한 NetApp 배포 지침:

  "https://fieldportal.netapp.com/content/248456" (NetApp 로그인 필요)

- MEDITECH 환경을 위한 NetApp 사이징 지침

  "www.netapp.com/us/media/tr-4190.pdf"

- Epic EHR용 FlexPod 데이터 센터 구축

  "www.netapp.com/us/media/tr-4693.pdf"

- FlexPod 설계 구역

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- NetApp AFF, vSphere 6.5U1 및 Cisco UCS Manager를 사용하는 FC 스토리지(MDS 스위치)가 포함된 FlexPod DC

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html"

- Cisco 의료

  https://www.cisco.com/c/en/us/solutions/industries/healthcare.html?dtid=osscdc000283

감사의 말

다음 사람들은 이 가이드의 작성 및 작성에 기여했습니다.

- Brandon AGEE, NetApp 기술 마케팅 엔지니어
- John Duignan, NetApp 의료 솔루션 설계자 - 의료
- Ketan Mota, NetApp 제품 매니저
- Jon Ebmeier, Cisco Systems, Inc. 기술 솔루션 설계자
- Mike Brennan, Cisco Systems, Inc. 제품 매니저

MEDITECH용 FlexPod 데이터 센터 배포 가이드

TR-4753: MEDITECH용 FlexPod 데이터 센터 배포 가이드

Brandon AGEE 및 John Duignan, NetApp Mike Brennan 및 Cisco Jon Ebmeier

파트너 후원:

전반적인 솔루션 이점

의료 기관은 FlexPod 아키텍처 기반으로 MEDITECH 환경을 실행하여 직원 생산성을 향상시키고 자본 및 운영 비용을 절감할 수 있습니다. MEDITECH용 FlexPod 데이터 센터는 다음과 같은 의료 산업에만 해당되는 다양한 이점을 제공합니다.

- * 운영 간소화 및 비용 절감. * 기존 플랫폼을 어디에서나 임상의를 지원할 수 있는 보다 효율적이고 확장 가능한 공유 리소스로 교체하여 기존 플랫폼의 비용과 복잡성을 제거합니다. 이 솔루션은 리소스 활용률을 높여 ROI(투자 수익률)를 높입니다.

- 인프라 배포 속도 향상**.** 기존 데이터 센터든 원격 위치든 FlexPod 데이터 센터의 통합 및 테스트를 거친 설계를 통해 적은 노력으로 새 인프라를 보다 빠르게 가동 및 실행할 수 있습니다.
- * 인증 스토리지. * MEDITECH가 포함된 NetApp ONTAP 데이터 관리 소프트웨어는 테스트를 거쳐 인증된 스토리지 공급업체의 우수한 안정성을 제공합니다. MEDITECH는 다른 인프라 구성 요소를 인증하지 않습니다.
- * 스케일아웃 아키텍처. * 실행 중인 애플리케이션을 재구성하지 않고 SAN 및 NAS를 테라바이트(TB)에서 수십 페타바이트(PB)로 확장할 수 있습니다.
- 무중단 운영 * 비즈니스 중단 없이 스토리지 유지보수, 하드웨어 라이프사이클 운영, FlexPod 업그레이드를 수행할 수 있습니다.
- * 보안 멀티 테넌시. * 가상화된 서버 및 스토리지 공유 인프라의 증가하는 요구 사항을 지원하여, 특히 시스템이 여러 데이터베이스 및 소프트웨어 인스턴스를 호스팅하는 경우 시설별 정보의 안전한 멀티 테넌시를 가능하게 합니다.
- 풀링된 리소스 최적화 * 물리적 서버 및 스토리지 컨트롤러 수 감소, 로드 밸런싱 워크로드 수요 증가, 성능 향상을 통해 사용률 향상
- * QoS(서비스 품질). * FlexPod는 전체 스택에서 QoS를 제공합니다. 업계 최고 수준의 QoS 네트워크, 컴퓨팅 및 스토리지 정책을 통해 공유 환경에서 차별화된 서비스 수준을 지원합니다. 이러한 정책을 통해 워크로드에 맞는 성능을 최적화하고 급등하는 애플리케이션을 격리 및 제어하는 데 도움을 줄 수 있습니다.
- * 스토리지 효율성. * 에 따라 스토리지 "NetApp 7:1 스토리지 효율성 보장" 비용을 절감합니다.
- * 민첩성 * FlexPod 시스템이 제공하는 업계 최고의 워크플로우 자동화, 오케스트레이션 및 관리 툴을 통해 IT 팀은 비즈니스 요청에 훨씬 더 빠르게 대응할 수 있습니다. 이러한 비즈니스 요청은 MEDITECH 백업 및 더 많은 테스트 및 교육 환경의 프로비저닝에서 인구 상태 관리 이니셔티브를 위한 분석 데이터베이스 복제까지 다양합니다.
- * 생산성 향상. * 최적의 최종 사용자 환경을 위해 이 솔루션을 빠르게 배포하고 확장할 수 있습니다.
- * NetApp Data Fabric. * NetApp Data Fabric 아키텍처는 물리적 경계 및 애플리케이션 전반에 걸쳐 데이터를 제공합니다. NetApp Data Fabric은 데이터 중심 세계에서 데이터 중심 기업을 위해 구축되었습니다. 데이터가 여러 위치에서 생성되고 사용되며, 다른 위치, 애플리케이션 및 인프라와 이를 활용 및 공유해야 하는 경우가 많습니다. 일관되고 통합된 데이터를 관리할 방법이 필요합니다. Data Fabric은 데이터의 제어 능력을 높이고 점점 더 복잡해지는 IT 복잡성을 단순화하는 방법을 제공합니다.

FlexPod

MEDITECH EHR에 대한 새로운 인프라 접근 방식

귀사와 같은 의료 제공자 조직은 업계 최고의 MEDITECH EHR(Electronic Health Records)에 대한 실질적 투자의 혜택을 극대화해야 한다는 압박을 받고 있습니다. 미션 크리티컬 애플리케이션의 경우 고객이 MEDITECH 솔루션용으로 데이터 센터를 설계할 때 데이터 센터 아키텍처에 대해 다음과 같은 목표를 식별하는 경우가 많습니다.

- MEDITECH 애플리케이션의 고가용성
- 고성능
- 데이터 센터에 MEDITECH를 손쉽게 구현할 수 있습니다
- 새로운 MEDITECH 릴리즈 또는 애플리케이션을 통해 성장을 지원하는 민첩성과 확장성
- 비용 효율성
- MEDITECH 지침 및 타겟 플랫폼과의 정렬
- 관리 용이성, 안정성 및 지원 용이성
- 강력한 데이터 보호, 백업, 복구 및 비즈니스 연속성

MEDITECH 사용자는 조직이 책임 있는 관리 조직으로 발전하고 묶인 보상 모델에 맞게 조정됨에 따라 보다 효율적이고 민첩한 IT 제공 모델로 필요한 MEDITECH 인프라를 제공해야 하는 과제를 안고 있습니다.

사전 검증된 통합 인프라의 가치

예측 가능한 지연 시간이 짧은 시스템 성능과 고가용성을 제공하기 위한 가장 중요한 요구 사항으로 인해 MEDITECH는 고객의 하드웨어 요구 사항에 따라 규범적으로 사용됩니다.

FlexPod는 Cisco와 NetApp의 전략적 파트너십을 통해 사전 검증을 거쳐 엄격하게 테스트된 통합 인프라입니다. 지연 시간이 짧고 예측 가능한 시스템 성능과 고가용성을 제공하도록 특별히 설계되고 제작되었습니다. 이 접근 방식은 MEDITECH 규정을 준수하고 궁극적으로 MEDITECH 시스템 사용자에게 최적의 응답 시간을 제공합니다.

Cisco와 NetApp의 FlexPod 솔루션은 고성능, 모듈식, 사전 검증, 통합, 가상화 및 효율성, 확장성 및 비용 효율적인 플랫폼 다음과 같은 기능을 제공합니다.

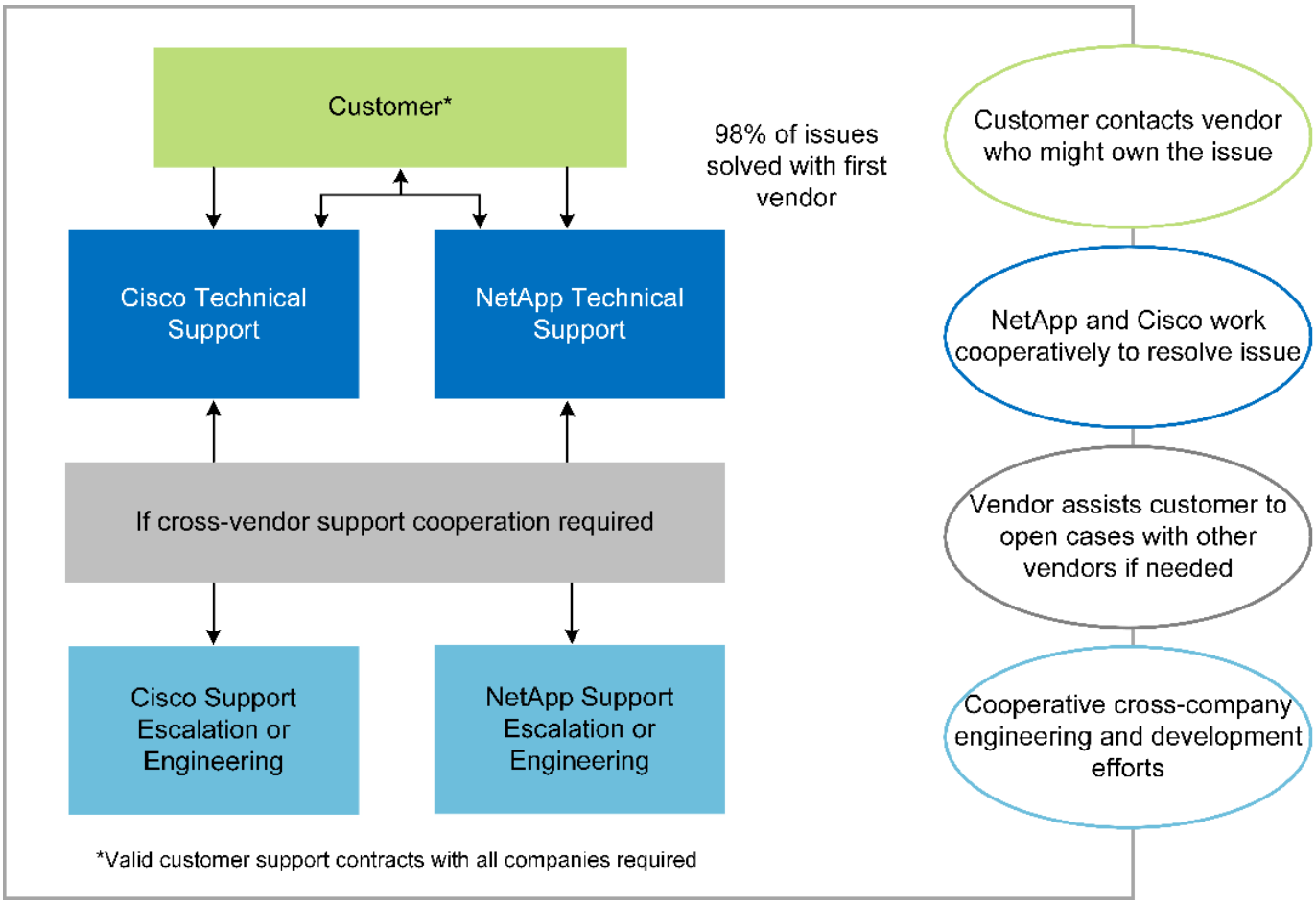
- * 모듈식 아키텍처 * FlexPod는 각 특정 워크로드에 맞게 특수 구성된 FlexPod 플랫폼을 통해 MEDITECH 모듈식 아키텍처의 다양한 요구를 충족합니다. 모든 구성요소는 클러스터 서버 및 스토리지 관리 패브릭과 일관된 관리 툴셋을 통해 연결됩니다.
- * 통합 스택의 각 레벨별로 업계 최고 수준의 기술 * Cisco, NetApp, VMware 및 Microsoft Windows가 각각 서버, 네트워킹, 스토리지, 운영 체제 범주에서 업계 분석가에 의해 1위 또는 2위로 선정되었습니다.
- * 표준화되고 유연한 IT를 통한 투자 보호 * FlexPod 참조 아키텍처는 새로운 제품 버전 및 업데이트를 예상하고 있으며, 향후 기술이 출시될 때 이를 수용할 수 있도록 철저한 지속적인 상호 운용성 테스트를 실시할 예정입니다.
- * 광범위한 환경에 걸쳐 검증된 구축 * 널리 사용되는 하이퍼바이저, 운영 체제, 애플리케이션 및 인프라 소프트웨어를 통해 사전 테스트 및 공동 검증을 거친 FlexPod는 여러 MEDITECH 고객 조직에 설치되었습니다.

검증된 **FlexPod** 아키텍처 및 공동 지원

FlexPod은 검증된 데이터 센터 솔루션으로, 성능에 부정적인 영향을 주지 않고 증가하는 워크로드 수요를 지원하기 위해 쉽게 확장 가능한 유연한 공유 인프라를 제공합니다. 이 솔루션은 FlexPod 아키텍처를 활용하여 다음과 같은 FlexPod의 모든 이점을 제공합니다.

- * MEDITECH 워크로드 요구 사항을 충족하는 성능 * MEDITECH 하드웨어 구성 제안 요구 사항에 따라 필요한 I/O 및 지연 시간 요구 사항을 충족하기 위해 다양한 ONTAP 플랫폼을 구축할 수 있습니다.
- * 임상 데이터 증가를 쉽게 수용할 수 있는 확장성 * 기존 제한 없이 필요에 따라 가상 머신(VM), 서버 및 스토리지 용량을 동적으로 확장
- * 효율성 향상. * 통합 가상화 인프라를 사용하면 관리 시간과 TCO를 모두 줄일 수 있습니다. 통합 가상화 인프라를 사용하면 관리가 더 쉽고 데이터를 보다 효율적으로 저장하는 동시에 MEDITECH 소프트웨어의 성능을 향상시킬 수 있습니다.
- * 위험 감소. * 구축 추측 작업을 없애고 지속적인 워크로드 최적화를 지원하는 정의된 아키텍처에 구축된 사전 검증된 플랫폼을 통해 비즈니스 중단을 최소화합니다.
- * FlexPod 공동 지원. * NetApp과 Cisco는 FlexPod 통합 인프라의 고유한 지원 요구사항을 충족할 수 있는 강력하고 확장 가능하며 유연한 지원 모델인 공동 지원을 확립했습니다. 이 모델은 NetApp과 Cisco의 경험, 리소스, 기술 지원 전문성을 합쳐 문제 영역에 관계없이, FlexPod 지원 문제를 식별하고 해결할 수 있는 효율적인 프로세스를 제공합니다. FlexPod 공동 지원 모델을 통해 FlexPod 시스템은 효율적으로 운영되며 최신 기술의 이점을 활용할 수 있으며, 숙련된 팀과 협력하여 통합 문제를 해결합니다.

  FlexPod 공동 지원은 FlexPod 통합 인프라에서 MEDITECH와 같은 비즈니스 크리티컬 애플리케이션을 실행하는 의료 조직에 특히 유용합니다. 다음 그림은 FlexPod 공동 지원 모델을 보여줍니다.



이러한 이점 외에도 MEDITECH 솔루션이 포함된 FlexPod 데이터 센터 스택의 각 구성 요소는 MEDITECH EHR 워크플로우에 특별한 이점을 제공합니다.

Cisco Unified Computing System

자체 통합 자체 인식 시스템인 Cisco UCS(Unified Computing System)는 통합 I/O 인프라와 상호 연결되는 단일 관리 도메인으로 구성됩니다. MEDITECH 환경용 Cisco UCS는 인프라에서 최대 가용성으로 중요한 환자 정보를 제공할 수 있도록 MEDITECH 인프라 권장 사항 및 모범 사례에 맞게 조정되었습니다.

Cisco UCS 아키텍처에 대한 MEDITECH의 기반은 Cisco UCS 기술로, 통합 시스템 관리, 인텔 제온 프로세서 및 서버 가상화를 갖추고 있습니다. 이러한 통합 기술은 데이터 센터 문제를 해결하고 MEDITECH의 데이터 센터 설계 목표를 달성하는 데 도움을 줍니다. Cisco UCS는 LAN, SAN 및 시스템 관리를 랙 서버, 블레이드 서버 및 VM을 위한 하나의 간소화된 링크로 통합합니다. Cisco UCS는 Cisco Unified Fabric과 Cisco FEX Technology(Fabric Extender Technology)를 통합하여 Cisco UCS의 모든 구성요소를 단일 네트워크 패브릭 및 단일 네트워크 계층으로 연결하는 엔드 투 엔드 I/O 아키텍처입니다.

이 시스템은 여러 블레이드 섀시, 랙 서버, 랙 및 데이터 센터를 통합하고 확장하는 단일 또는 다중 논리 유닛으로 구축할 수 있습니다. 이 시스템은 기존 블레이드 서버 섀시 및 랙 서버를 채우는 여러 중복 장치를 제거하는 매우 단순화된 아키텍처를 구현합니다. 기존 시스템에서는 이더넷, FC 어댑터, 섀시 관리 모듈과 같은 이중 장치로 인해 복잡성이 가중됩니다. Cisco UCS는 모든 I/O 트래픽에 단일 관리 지점과 단일 제어 지점을 제공하는 이중 Cisco UCS Fabric Interconnect(FI) 쌍으로 구성됩니다.

Cisco UCS는 서비스 프로필을 사용하여 Cisco UCS 인프라의 가상 서버가 올바르게 구성되었는지 확인합니다. 서비스 프로필은 각 분야의 전문가가 생성한 네트워크, 스토리지 및 컴퓨팅 정책으로 구성됩니다. 서비스 프로필에는 LAN 및 SAN 주소 지정, I/O 구성, 펌웨어 버전, 부팅 순서, 네트워크 가상 LAN(VLAN), 물리적 포트 및 QoS 정책과 같은 서버 ID에 대한 중요한 서버 정보가 포함되어 있습니다. 서비스 프로필은 몇 시간 또는 며칠이 아니라 몇 분 내에 동적으로

생성하고 시스템의 모든 물리적 서버와 연결할 수 있습니다. 물리적 서버와 서비스 프로파일 연결은 간단한 단일 작업으로 수행되므로 물리적 구성 변경 없이 환경의 서버 간에 ID를 마이그레이션할 수 있습니다. 폐기된 서버의 교체를 신속하게 베어 메탈 프로비저닝할 수 있습니다.

서비스 프로필을 사용하면 기업 전체에서 서버를 일관성 있게 구성할 수 있습니다. 여러 Cisco UCS 관리 도메인이 사용되는 경우 Cisco UCS Central은 글로벌 서비스 프로필을 사용하여 도메인 전체에서 구성 및 정책 정보를 동기화할 수 있습니다. 유지 관리를 한 도메인에서 수행해야 하는 경우 가상 인프라를 다른 도메인으로 마이그레이션할 수 있습니다. 이 접근 방식은 단일 도메인이 오프라인일 때도 애플리케이션이 고가용성을 계속 실행할 수 있도록 하는 데 도움이 됩니다.

Cisco UCS는 서버 구성 요구 사항을 충족한다는 것을 입증하기 위해 수년간 MEDITECH와 함께 광범위한 테스트를 거쳤습니다. Cisco UCS는 MEDITECH 제품 리소스 시스템 지원 사이트에 나열된 지원되는 서버 플랫폼입니다.

Cisco 네트워킹

Cisco Nexus 스위치 및 Cisco MDS 다계층 디렉터는 엔터프라이즈급 연결 및 SAN 통합을 제공합니다. Cisco 멀티 프로토콜 스토리지 네트워킹은 FC, FICON(Fibre Connection), FCoE(FC over Ethernet), iSCSI(SCSI over IP), FCIP(FC over IP)와 같은 유연성과 옵션을 제공하여 비즈니스 위험을 줄입니다.

Cisco Nexus 스위치는 단일 플랫폼에서 가장 포괄적인 데이터 센터 네트워크 기능 세트 중 하나를 제공합니다. 데이터 센터와 캠퍼스 코어 모두를 위한 높은 성능과 밀도를 제공합니다. 또한 복원력이 뛰어난 모듈식 플랫폼에서 데이터 센터 통합, 행 종료 및 데이터 센터 인터커넥트 구축을 위한 전체 기능 세트를 제공합니다.

Cisco UCS는 컴퓨팅 리소스를 Cisco Nexus 스위치 및 통합 I/O 패브릭과 통합하여 다양한 유형의 네트워크 트래픽을 식별 및 처리합니다. 이러한 트래픽에는 스토리지 I/O, 스트림되는 데스크톱 트래픽, 관리 및 임상 및 비즈니스 애플리케이션에 대한 액세스가 포함됩니다. 다음과 같은 이점을 얻을 수 있습니다.

- * 인프라 확장성 * 가상화, 효율적인 전력 및 냉각, 자동화 기능을 통한 클라우드 확장, 고밀도 및 고성능 모두 효율적인 데이터 센터 확장을 지원합니다.
- * 운영 연속성. * 이 설계에는 하드웨어, NX-OS 소프트웨어 기능 및 관리가 통합되어 다운타임이 없는 환경을 지원합니다.
- * 네트워크 및 컴퓨터 QoS. * Cisco는 네트워크, 스토리지 및 컴퓨팅 패브릭 전반에서 정책 중심의 CoS(서비스 클래스)와 QoS를 제공하여 미션 크리티컬 애플리케이션의 성능을 최적화합니다.
- * 전송 유연성. * 비용 효율적인 솔루션으로 새로운 네트워킹 기술을 점진적으로 도입합니다.

Cisco UCS와 Cisco Nexus 스위치 및 Cisco MDS 다중 계층 디렉터는 MEDITECH에 최적의 컴퓨팅, 네트워킹 및 SAN 연결 솔루션을 제공합니다.

NetApp ONTAP를 참조하십시오

ONTAP 소프트웨어를 실행하는 NetApp 스토리지는 전체 스토리지 비용을 절감하는 동시에 MEDITECH 워크로드에 필요한 짧은 지연 시간의 읽기 및 쓰기 응답 시간 및 IOPS를 제공합니다. ONTAP는 All-Flash 및 하이브리드 스토리지 구성을 모두 지원하므로 MEDITECH 요구 사항을 충족하는 최적의 스토리지 플랫폼을 구축할 수 있습니다. NetApp 플래시 가속 시스템은 MEDITECH의 검증 및 인증을 받았으며 MEDITECH 고객으로서 지연 시간에 민감한 MEDITECH 작업에 핵심적인 성능 및 응답 속도를 제공합니다. 단일 클러스터에서 여러 오류 도메인을 생성하여 NetApp 시스템은 운영 환경을 비운영 시스템에서 격리할 수도 있습니다. 또한 NetApp 시스템은 ONTAP QoS를 지원하는 워크로드의 최소 성능 보장 수준으로 성능 문제를 줄입니다.

ONTAP 소프트웨어의 스케일아웃 아키텍처는 다양한 I/O 워크로드에 유연하게 대응할 수 있습니다. 임상 애플리케이션에 필요한 처리량과 짧은 지연 시간을 제공하는 동시에 모듈식 스케일아웃 아키텍처를 제공하기 위해 All-Flash 구성은 일반적으로 ONTAP 아키텍처에서 사용됩니다. NetApp AFF 노드는 높은 처리량의 대규모 데이터 세트를 저장하는 데 적합한 하이브리드(HDD 및 플래시) 스토리지 노드와 동일한 스케일아웃 클러스터에서 결합할 수 있습니다.

MEDITECH 승인 백업 솔루션과 함께 값비싼 SSD(Solid State Drive) 스토리지에서 다른 노드의 보다 경제적인 HDD 스토리지로 MEDITECH 환경을 복제, 복제 및 백업할 수 있습니다. 이 접근 방식은 SAN 기반 클론 생성 및 운영 풀 백업에 대한 MEDITECH 지침을 충족하거나 초과합니다.

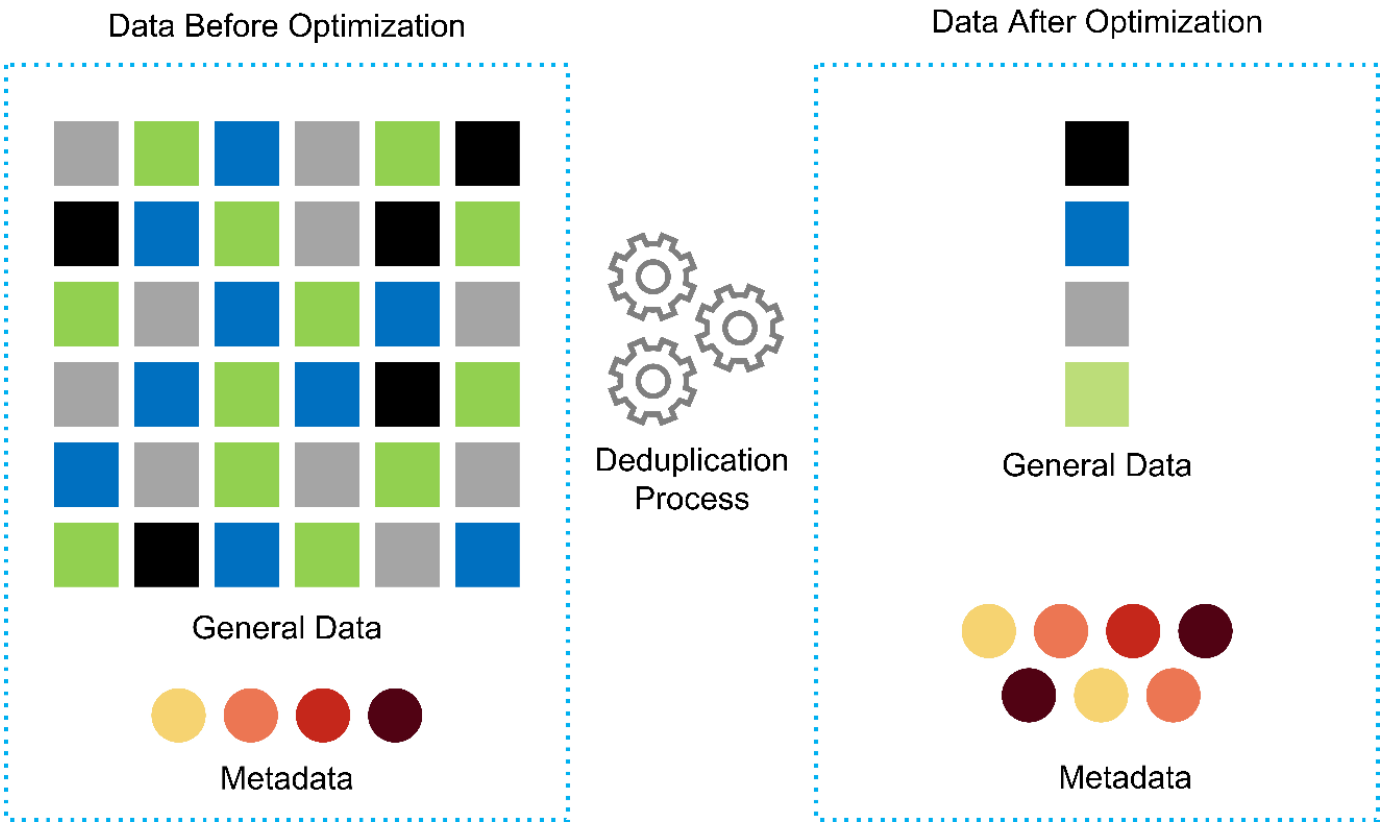
MEDITECH 환경에는 관리 간소화, 가용성 및 자동화 향상, 필요한 총 스토리지 용량 감소 등 많은 ONTAP 기능이 특히 유용합니다. 다음과 같은 기능을 제공합니다.

- * 탁월한 성능 * NetApp AFF 솔루션은 유니파이드 스토리지 아키텍처, ONTAP 소프트웨어, 관리 인터페이스, 다양한 데이터 서비스, 고급 기능 세트를 공유하고 FAS 있습니다. 혁신적인 All-Flash 미디어와 ONTAP을 결합하여 업계 최고 수준의 ONTAP 소프트웨어와 All-Flash 스토리지의 높은 IOPS와 일관되게 낮은 지연 시간을 제공합니다.
- * 스토리지 효율성. * 중복제거, NetApp FlexClone 데이터 복제 기술, 인라인 압축, 인라인 컴팩션, 씬 복제, 씬 프로비저닝으로 총 용량 요구사항을 줄입니다. 애그리게이트 중복제거.

  NetApp 중복제거 기능은 NetApp FlexVol 볼륨 또는 데이터 구성요소의 블록 레벨 중복제거를 제공합니다. 기본적으로, 중복제거는 중복된 블록을 제거해 고유한 블록만 FlexVol 볼륨 또는 데이터 구성요소에 저장합니다.

  중복제거는 고도의 세분성을 제공하며 FlexVol 볼륨 또는 데이터 구성요소의 액티브 파일 시스템에서 작동합니다. 이 데이터는 애플리케이션에 영향을 미치지 않으므로 중복 제거를 사용하여 NetApp 시스템을 사용하는 모든 애플리케이션에서 생성된 데이터를 중복 제거할 수 있습니다. 볼륨 중복 제거를 인라인 프로세스로 실행할 수 있습니다(ONTAP 8.3.2부터). CLI, NetApp ONTAP System Manager 또는 NetApp Active IQ Unified Manager를 통해 자동으로 실행하거나, 스케줄을 지정하거나, 수동으로 실행하도록 구성할 수 있는 백그라운드 프로세스로 실행할 수도 있습니다.

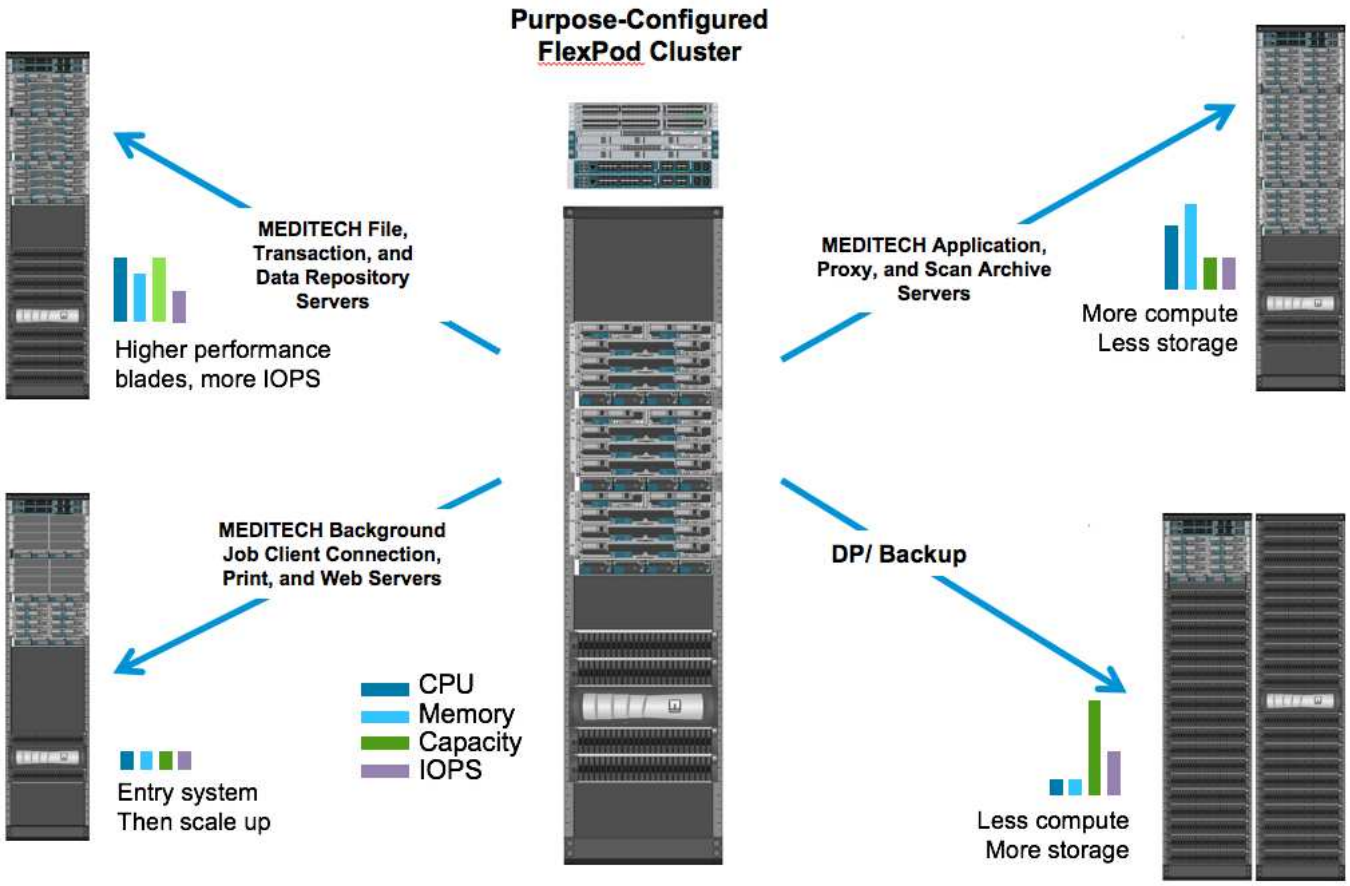
  다음 그림에서는 NetApp 중복 제거가 최고 수준에서 작동하는 방식을 보여 줍니다.



- 공간 효율적인 클로닝 * FlexClone 기능을 사용하면 거의 즉각적으로 클론을 생성하여 백업 및 테스트 환경의 업데이트 기능을 지원할 수 있습니다. 이러한 클론은 변경된 경우에만 더 많은 스토리지를 사용합니다.

- * NetApp Snapshot 및 SnapMirror 기술. * ONTAP는 MEDITECH 호스트가 사용하는 LUN(논리 유닛 번호)의 공간 효율적인 스냅샷 복사본을 생성할 수 있습니다. 이중 사이트 구축의 경우 SnapMirror 소프트웨어를 구현하여 더 많은 데이터 복제 및 복원력을 높일 수 있습니다.
- * 통합 데이터 보호. * 완전한 데이터 보호 및 재해 복구 기능을 통해 중요 데이터 자산을 보호하고 재해 복구를 제공할 수 있습니다.
- 무중단 운영 * 데이터를 오프라인으로 전환하지 않고도 업그레이드와 유지보수를 수행할 수 있습니다.
- * QoS 및 AQoS(적응형 QoS). * 스토리지 QoS를 통해 잠재적인 대규모 워크로드를 제한할 수 있습니다. 더 중요한 것은 QoS가 MEDITECH 프로덕션과 같은 중요 워크로드에 대한 최소 성능을 보장할 수 있다는 것입니다. 경합을 제한함으로써 NetApp QoS는 성능 관련 문제를 줄일 수 있습니다. AQoS는 사전 정의된 정책 그룹에서 작동하며, 볼륨에 직접 적용할 수 있습니다. 이러한 정책 그룹은 처리량 상한 또는 볼륨 대비 크기를 자동으로 확장하여 볼륨 크기에 따라 IOPS와 TB, 기가바이트의 비율을 유지할 수 있습니다.
- * NetApp Data Fabric. * NetApp Data Fabric은 클라우드와 온프레미스 환경에서 데이터 관리를 단순화하고 통합하여 디지털 혁신을 가속합니다. 데이터 가시성과 통찰력, 데이터 액세스 및 제어, 데이터 보호 및 보안을 위한 일관되고 통합된 데이터 관리 서비스 및 애플리케이션을 제공합니다. NetApp은 AWS(Amazon Web Services), Azure, Google Cloud Platform 및 IBM Cloud 클라우드와 통합되어 다양한 선택의 기회를 제공합니다.

다음 그림에서는 MEDITECH 워크로드를 위한 FlexPod 아키텍처를 보여 줍니다.



MEDITECH 개요

MEDITECH로 알려진 Medical Information Technology, Inc.는 매사추세츠에 기반을 둔 소프트웨어 기업으로, 의료 조직을 위한 정보 시스템을 제공합니다. Meditech는 최신 환자 데이터를 저장 및 구성할 수 있도록 설계된 EHR 시스템을 제공하며 임상 직원에게 데이터를 제공합니다. 환자 데이터에는 인구통계 정보, 의료 기록, 약물, 검사실 검사 결과가 포함되며 이에 국한되지 않습니다. 방사선 영상 및 나이, 신장, 체중 등의 개인 정보.

이 문서에서는 MEDITECH 소프트웨어가 지원하는 다양한 기능에 대해 설명합니다. 부록 A에서는 이러한 광범위한 MEDITECH 함수 집합에 대한 자세한 정보를 제공합니다. MEDITECH 애플리케이션은 이러한 기능을 지원하기 위해 여러 VM이 필요합니다. 이러한 애플리케이션을 배포하려면 MEDITECH의 권장 사항을 참조하십시오.

스토리지 시스템 관점에서 각 구축 시 모든 MEDITECH 소프트웨어 시스템에는 분산 환자 중심 데이터베이스가 필요합니다. MEDITECH에는 Windows 운영 체제를 사용하는 고유한 전용 데이터베이스가 있습니다.

브리지헤드와 Commvault는 NetApp과 MEDITECH에서 인증한 2가지 백업 소프트웨어 애플리케이션입니다. 이 문서의 범위에는 이러한 백업 응용 프로그램의 배포에 대한 내용이 포함되어 있지 않습니다.

이 문서의 주요 초점은 FlexPod 스택(서버 및 스토리지)이 EHR 환경의 MEDITECH 데이터베이스 및 백업 요구 사항에 대한 성능 기반 요구 사항을 충족하도록 지원하는 것입니다.

특정 **MEDITECH** 워크로드를 위해 특별 제작되었습니다

MEDITECH는 서버, 네트워크 또는 스토리지 하드웨어, 하이퍼바이저 또는 운영 체제를 재판매하지 않습니다. 하지만 인프라 스택의 각 구성요소에 대한 특정 요구사항이 있습니다. 따라서 Cisco와 NetApp은 공동으로 테스트를 실시하여 FlexPod 데이터 센터를 성공적으로 구성, 구축 및 지원하여 귀사와 같은 고객의 MEDITECH 운영 환경 요구사항을 충족할 수 있도록 했습니다.

MEDITECH 범주

MEDITECH는 배포 크기를 1에서 6 사이의 범주 번호와 연결합니다. 범주 1은 가장 작은 MEDITECH 배포이며 범주 6은 가장 큰 MEDITECH 배포입니다.

각 범주에서 MEDITECH 호스트의 I/O 특성 및 성능 요구 사항에 대한 자세한 내용은 NetApp을 참조하십시오 "TR-4190: MEDITECH 환경을 위한 NetApp 사이징 지침".

MEDITECH 플랫폼

MEDITECH의 광활한 플랫폼은 회사의 EHR 소프트웨어의 최신 버전입니다. 이전 MEDITECH 플랫폼은 Client/Server 5.x 및 Magic입니다. 이 섹션에서는 MEDITECH 호스트 및 해당 스토리지 요구 사항과 관련된 MEDITECH 플랫폼(광범위, 6.x, C/S 5.x 및 Magic에 적용 가능)에 대해 설명합니다.

이전의 모든 MEDITECH 플랫폼에서 여러 서버가 MEDITECH 소프트웨어를 실행하여 다양한 작업을 수행합니다. 이전 그림에서는 애플리케이션 데이터베이스 서버 및 기타 MEDITECH 서버로 사용되는 MEDITECH 호스트를 비롯한 일반적인 MEDITECH 시스템을 보여 줍니다. 다른 MEDITECH 서버의 예로는 데이터 저장소 애플리케이션, 스캐닝 및 아카이빙 애플리케이션, 백그라운드 작업 클라이언트 등이 있습니다. 다른 MEDITECH 서버의 전체 목록은 "하드웨어 구성 제안"(신규 구축) 및 "하드웨어 평가 작업"(기존 구축) 문서를 참조하십시오. MEDITECH 시스템 통합자나 MEDITECH TAM(기술 계정 관리자)을 통해 MEDITECH에서 이러한 문서를 얻을 수 있습니다.

MEDITECH 호스트

MEDITECH 호스트는 데이터베이스 서버입니다. 이 호스트는 MEDITECH 파일 서버(광활함, 6.x 또는 C/S 5.x 플랫폼) 또는 Magic 시스템(매직 플랫폼)이라고도 합니다. 이 문서에서는 MEDITECH 호스트라는 용어를 사용하여 MEDITECH 파일 서버 또는 Magic 시스템을 참조합니다.

MEDITECH 호스트는 Microsoft Windows Server 운영 체제에서 실행되는 물리적 서버 또는 VM이 될 수 있습니다. 일반적으로 MEDITECH 호스트는 VMware ESXi 서버에서 실행되는 Windows VM으로 구축됩니다. 이 쓰기 작업을 통해 VMware는 MEDITECH에서 지원하는 유일한 하이퍼바이저입니다. MEDITECH 호스트는 Windows 시스템의 Microsoft Windows 드라이브(예: 드라이브 E)에 프로그램, 사전 및 데이터 파일을 저장합니다.

가상 환경에서 Windows E 드라이브는 물리적 호환성 모드에서 RDM(Raw Device Mapping)을 통해 VM에 연결된

LUN에 상주합니다. 이 시나리오에서 VMDK(Virtual Machine Disk) 파일을 Windows E 드라이브로 사용하는 것은 MEDITECH에서 지원되지 않습니다.

MEDITECH 호스트 워크로드 I/O 특성

각 MEDITECH 호스트와 시스템 전체의 I/O 특성은 배포하는 MEDITECH 플랫폼에 따라 다릅니다. 모든 MEDITECH 플랫폼(광활하게 펼쳐진 6.x, C/S 5.x 및 Magic)은 100% 랜덤 워크로드를 생성합니다.

MEDITECH의 넓은 플랫폼은 호스트당 쓰기 작업 비율이 가장 높고 전체 IOPS가 가장 높고 그 뒤에 6.x, C/S 5.x 및 Magic 플랫폼이 있기 때문에 가장 까다로운 워크로드를 생성합니다.

MEDITECH 워크로드 설명에 대한 자세한 내용은 을 참조하십시오 "TR-4190: MEDITECH 환경을 위한 NetApp 사이징 지침".

스토리지 네트워크

MEDITECH는 NetApp FAS 또는 AFF 시스템과 모든 범주의 MEDITECH 호스트 간의 데이터 트래픽에 FC 프로토콜을 사용해야 합니다.

MEDITECH 호스트에 대한 스토리지 프레젠테이션입니다

각 MEDITECH 호스트는 다음과 같은 두 개의 Windows 드라이브를 사용합니다.

- * 드라이브 C. * 이 드라이브는 Windows Server 운영 체제 및 MEDITECH 호스트 애플리케이션 파일을 저장합니다.
- * Drive E * MEDITECH 호스트는 Windows Server 운영 체제의 드라이브 E에 프로그램, 사전 및 데이터 파일을 저장합니다. 드라이브 E는 FC 프로토콜을 사용하여 NetApp FAS 또는 AFF 시스템에서 매핑된 LUN입니다. MEDITECH는 MEDITECH 호스트의 IOPS 및 읽기/쓰기 지연 시간 요구 사항이 충족되도록 FC 프로토콜을 사용해야 합니다.

볼륨 및 LUN 명명 규칙

MEDITECH는 모든 LUN에 대해 특정 명명 규칙을 사용해야 합니다.

스토리지를 구축하기 전에 MEDITECH 하드웨어 구성 제안을 확인하여 LUN의 명명 규칙을 확인합니다. MEDITECH 백업 프로세스는 백업할 특정 LUN을 적절하게 식별하기 위해 볼륨 및 LUN 명명 규칙에 의존합니다.

포괄적인 관리 툴 및 자동화 기능

Cisco UCS Manager 및 Cisco UCS

Cisco는 탁월한 데이터 센터 인프라, 즉 단순화, 보안 및 확장성을 제공하기 위해 세 가지 핵심 요소에 주력하고 있습니다. 플랫폼 모듈성이 결합된 Cisco UCS Manager 소프트웨어는 간편하고 안전하며 확장 가능한 데스크톱 가상화 플랫폼을 제공합니다.

- * Simplified. * Cisco UCS는 업계 표준 컴퓨팅에 대한 새롭고 혁신적인 접근 방식을 제공하며 모든 워크로드에 데이터센터 인프라의 코어를 제공합니다. Cisco UCS는 필요한 서버 수 감소, 서버당 사용되는 케이블 수 감소 등 다양한 기능과 이점을 제공합니다. 또 다른 중요한 기능은 Cisco UCS 서비스 프로필을 통해 서버를 신속하게 구축하거나 재프로비저닝할 수 있는 기능입니다. 관리할 서버 및 케이블 수가 더 적고 서버 및 애플리케이션 워크로드 프로비저닝이 간소화되어 운영이 간소화됩니다. Cisco UCS Manager 서비스 프로필을 사용하면 몇 분 이내에 블레이드 및 랙 서버 점수를 프로비저닝할 수 있습니다. Cisco UCS 서비스 프로필은 서버 통합 Runbook을 제거하고 구성 드리프트를 제거합니다. 이 접근 방식은 최종 사용자의 생산성 향상, 비즈니스 민첩성 향상, IT 리소스 할당 등의 작업을 수행합니다.

Cisco UCS Manager는 서버, 네트워크, 스토리지 액세스 인프라의 구성 및 프로비저닝과 같이 자주 발생하는 일상적인 데이터 센터 운영을 자동화합니다. 또한, 메모리 공간이 큰 Cisco UCS B-Series 블레이드 서버 및 C-Series 랙 서버는 높은 애플리케이션 사용자 밀도를 지원하여 서버 인프라 요구사항을 줄여줍니다.

간소화로 인해 MEDITECH 인프라 구축이 더욱 신속하고 성공적으로 수행되도록 할 수 있습니다.

- * 보안. * VM은 물리적 이전 VM보다 기본적으로 더 안전하지만 새로운 보안 문제를 야기합니다. 가상 데스크톱과 같은 공통 인프라를 사용하는 업무상 중요한 웹 및 애플리케이션 서버는 이제 보안 위협에 대한 위험이 더 높습니다. VM 간 트래픽은 이제 IT 관리자가 특히 VMware vMotion을 사용하는 VM이 서버 인프라 간에 이동하는 동적 환경에서 해결해야 하는 중요한 보안 고려 사항이 됩니다.

  따라서 가상화는 특히 확장된 컴퓨팅 인프라 전반에서 VM 이동성의 역동적이고 유동적인 특성을 고려할 때 정책 및 보안에 대한 VM 수준의 인식을 필요로 합니다. 새로운 가상 데스크톱을 손쉽게 확산하면 가상화 인식 네트워크 및 보안 인프라의 중요성이 더욱 커지고 있습니다. 데스크톱 가상화를 위한 Cisco UCS, Cisco MDS 및 Cisco Nexus 제품군 솔루션, Cisco 데이터 센터 인프라는 강력한 데이터 센터, 네트워크 및 데스크톱 보안을 제공하며 데스크톱에서 하이퍼바이저에 이르는 포괄적인 보안을 제공합니다. 가상 데스크톱, VM 인식 정책 및 관리, LAN 및 WAN 인프라 전반의 네트워크 보안을 세분화하여 보안이 강화됩니다.

- * 확장성. * 가상화 솔루션의 성장은 필연적이므로 솔루션은 확장 가능하고 예측 가능한 확장성을 제공해야 합니다. Cisco 가상화 솔루션은 높은 VM 밀도(서버당 VM)를 지원하며, 더 많은 서버는 거의 선형적인 성능으로 확장할 수 있습니다. Cisco 데이터 센터 인프라는 성장을 위한 유연한 플랫폼을 제공하고 비즈니스 민첩성을 개선합니다. Cisco UCS Manager 서비스 프로필을 사용하면 온디맨드 호스트 프로비저닝을 수행할 수 있으며, 수십 개의 호스트를 구축할 때 수백 개의 호스트를 쉽게 구축할 수 있습니다.

  Cisco UCS 서버는 거의 선형적인 성능과 확장성을 제공합니다. Cisco UCS는 특허 받은 Cisco 확장 메모리 기술을 구현하여 더 적은 수의 소켓으로 대용량 메모리 공간을 제공합니다(2소켓 및 4소켓 서버에서 최대 1TB의 메모리 확장성 지원). Cisco UCS Server의 총 대역폭은 서버당 최대 80Gbps까지 확장할 수 있으며, 노스바운드 Cisco UCS Fabric Interconnect는 라인 속도로 2Tbps까지 출력할 수 있습니다. 이 기능은 데스크톱 가상화 I/O 및 메모리 병목 현상을 방지하는 데 도움이 됩니다. 지연 시간이 짧은 고성능 Unified Fabric 기반 네트워킹 아키텍처를 갖춘 Cisco UCS는 고해상도 비디오 및 통신 트래픽을 비롯한 많은 양의 가상 데스크톱 트래픽을 지원합니다. 또한 ONTAP은 FlexPod 가상화 솔루션의 일부로 부팅 및 로그인 폭증 시 데이터 가용성과 최적의 성능을 유지할 수 있도록 지원합니다.

  Cisco UCS, Cisco MDS 및 Cisco Nexus 데이터 센터 인프라 설계는 성장을 위한 뛰어난 플랫폼을 제공합니다. 서버, 네트워크 및 스토리지 리소스를 투명하게 확장하여 데스크톱 가상화, 데이터 센터 애플리케이션, 클라우드 컴퓨팅을 지원할 수 있습니다.

VMware vCenter Server를 참조하십시오

VMware vCenter Server는 MEDITECH 환경을 관리할 수 있는 중앙 집중식 플랫폼을 제공하므로 의료 조직이 다음과 같이 가상 인프라를 안심하고 자동화 및 제공할 수 있습니다.

- * 간단한 구축. * 가상 어플라이언스를 사용하여 vCenter Server를 빠르고 쉽게 구축할 수 있습니다.
- * 중앙 집중식 제어 및 가시성 * 단일 위치에서 전체 VMware vSphere 인프라스트럭처를 관리합니다.
- * 사전 최적화. * 최대 효율성을 위해 리소스를 할당 및 최적화합니다.
- * 관리. * 강력한 플러그인과 도구를 사용하여 관리를 단순화하고 제어를 확장합니다.

VMware vSphere용 **Virtual Storage Console**을 참조하십시오

NetApp의 VSC(가상 스토리지 콘솔), VASA(vSphere API for Storage Awareness) 공급자, VMware SRA(Storage Replication Adapter) for VMware vSphere는 단일 가상 어플라이언스를 만듭니다. 이 제품군은 SRA 및 VASA

Provider를 vCenter Server에 대한 플러그인으로 포함하여 NetApp 스토리지 시스템을 사용하는 VMware 환경에서 VM에 대한 엔드-투-엔드 라이프사이클 관리를 제공합니다.

VSC, VASA Provider, SRA를 위한 가상 어플라이언스는 VMware vSphere Web Client와 원활하게 통합되며 SSO 서비스를 사용할 수 있습니다. VMware vCenter Server 인스턴스가 여러 개 있는 환경에서는 관리할 각 vCenter Server 인스턴스에 자체 등록된 VSC 인스턴스가 있어야 합니다. VSC 대시보드 페이지에서는 데이터 저장소 및 VM의 전체 상태를 빠르게 확인할 수 있습니다.

VSC, VASA Provider, SRA를 위한 가상 어플라이언스를 구축하면 다음과 같은 작업을 수행할 수 있습니다.

- * VSC를 사용하여 스토리지를 구축 및 관리하고 ESXi 호스트를 구성할 수 있습니다. * VSC를 사용하면 자격 증명을 추가하고, 자격 증명을 제거하고, 자격 증명을 할당하고, VMware 환경의 스토리지 컨트롤러에 대한 사용 권한을 설정할 수 있습니다. 또한 NetApp 스토리지 시스템에 연결된 ESXi 서버를 관리할 수도 있습니다. 몇 번의 클릭만으로 모든 호스트에 대해 호스트 시간 초과, NAS 및 다중 경로에 대해 권장되는 Best Practice 값을 설정할 수 있습니다. 저장소 세부 정보를 보고 진단 정보를 수집할 수도 있습니다.
- * VASA Provider를 사용하여 스토리지 기능 프로필을 생성하고 알람을 설정할 수 있습니다. * VASA Provider 확장을 활성화하면 VASA Provider for ONTAP가 VSC에 등록됩니다. 스토리지 용량 프로파일과 가상 데이터 저장소를 생성하여 사용할 수 있습니다. 볼륨 및 애그리게이트의 임계값이 거의 가득 찼을 때 알림을 보내도록 알람을 설정할 수도 있습니다. 가상 데이터 저장소에서 생성된 VMDK 및 VM의 성능을 모니터링할 수 있습니다.
- * 재해 복구에 SRA를 사용합니다. * SRA를 사용하여 장애 시 재해 복구를 위해 사용자 환경에서 보호 및 복구 사이트를 구성할 수 있습니다.

NetApp OnCommand Insight and ONTAP를 참조하십시오

NetApp OnCommand Insight는 인프라 관리를 MEDITECH 서비스 제공망으로 통합합니다. 이러한 접근 방식을 통해 의료 기관은 스토리지, 네트워크 및 컴퓨팅 인프라를 보다 효율적으로 제어, 자동화 및 분석할 수 있습니다. IT 조직은 현재 인프라를 최적화하여 최대 이점을 얻고 구매할 항목과 시기를 결정하는 프로세스를 간소화할 수 있습니다. 또한 복잡한 기술 마이그레이션과 관련된 위험을 완화할 수 있습니다. 에이전트가 필요하지 않으므로 설치가 간단하고 업무 중단이 발생하지 않습니다. 설치된 스토리지 및 SAN 장치를 지속적으로 발견하고 전체 스토리지 환경을 완전히 파악할 수 있도록 상세 정보를 수집합니다. 잘못 사용되거나, 잘못 정렬되거나, 활용률이 낮거나, 격리된 자산을 신속하게 파악하고 다시 회수하여 향후의 확장을 가속화할 수 있습니다. OnCommand Insight는 다음과 같은 이점을 제공합니다.

- * 기존 리소스 최적화 * 문제를 방지하고 서비스 수준을 충족하기 위해 검증된 모범 사례를 사용하여 잘못 사용되거나 활용률이 낮거나 격리된 자산 식별
- * 더 나은 결정을 내리십시오. * 실시간 데이터를 사용하면 용량 문제를 더욱 빠르게 해결하여 향후 구매를 정확하게 계획하고 과도한 지출을 피하고 자본 지출을 연기할 수 있습니다.
- * IT 이니셔티브를 가속화하십시오. * 가상 환경을 더 잘 이해하여 위험을 관리하고 다운타임을 최소화하고 클라우드 구축 시간을 단축하십시오.

설계

MEDITECH용 FlexPod의 아키텍처는 MEDITECH, Cisco 및 NetApp의 지침과 모든 규모의 MEDITECH 고객과 협업하는 파트너의 경험을 바탕으로 합니다. 이 아키텍처는 데이터 센터 전략, 조직의 규모, 시스템이 중앙 집중형, 분산 또는 멀티 테넌트 중 어디에 있는지에 따라 적응성이 뛰어나고 MEDITECH의 모범 사례를 적용합니다.

올바른 스토리지 아키텍처는 총 IOPS의 전체 크기에 따라 결정됩니다. 성능만 중요한 요소가 아니므로 추가 고객 요구사항을 기반으로 더 많은 노드 수를 사용할 수도 있습니다. NetApp 스토리지를 사용하면 요구사항의 변화에 따라 쉽고 중단 없이 클러스터를 확장할 수 있습니다. 또한 운영 중단 없이 클러스터에서 노드를 제거하여 장비를 용도 변경하거나 장비를 새로 고칠 수 있습니다.

NetApp ONTAP 스토리지 아키텍처의 이점은 다음과 같습니다.

- * 손쉬운 무중단 스케일업 및 스케일아웃 * ONTAP 무중단 운영을 사용하면 디스크와 노드를 업그레이드, 추가, 제거할 수 있습니다. 4개 노드로 시작한 후 6개 노드로 이동하거나 더 큰 컨트롤러로 중단 없이 업그레이드할 수 있습니다.
- * 스토리지 효율성 * 중복제거, NetApp FlexClone, 인라인 압축, 인라인 컴팩션, 씬 복제를 통해 총 용량 요구사항 감소 씬 프로비저닝 및 애그리게이트 중복제거. FlexClone 기능을 사용하면 거의 즉시 클론을 생성하여 백업 및 테스트 환경 업데이트를 지원할 수 있습니다. 이러한 클론은 변경된 경우에만 더 많은 스토리지를 사용합니다.
- * 재해 복구 섀도우 데이터베이스 서버. * 재해 복구 섀도우 데이터베이스 서버는 비즈니스 연속성 전략의 일부입니다(스토리지 읽기 전용 기능을 지원하고 스토리지 읽기/쓰기 인스턴스로 구성될 수 있음). 따라서 세 번째 스토리지 시스템의 배치 및 사이징은 일반적으로 운영 데이터베이스 스토리지 시스템과 동일합니다.
- * 데이터베이스 일관성(일부 고려 사항 필요) * 비즈니스 연속성과 관련하여 NetApp SnapMirror 백업 복사본을 사용하는 경우 을 참조하십시오 "TR-3446: SnapMirror 비동기 개요 및 모범 사례 가이드".

스토리지 레이아웃

MEDITECH 호스트용 전용 Aggregate

MEDITECH의 고성능 및 고가용성 요구 사항을 충족하기 위한 첫 번째 단계는 MEDITECH 환경의 스토리지 레이아웃을 적절하게 설계하여 MEDITECH 호스트 운영 워크로드를 전용 고성능 스토리지로 격리하는 것입니다.

MEDITECH 호스트의 프로그램, 사전 및 데이터 파일을 저장하기 위해 각 스토리지 컨트롤러에 하나의 전용 애그리게이트를 프로비저닝해야 합니다. 동일한 디스크를 사용하고 성능에 영향을 주는 다른 워크로드의 가능성을 없애기 위해 해당 애그리게이트에서 다른 스토리지는 프로비저닝되지 않습니다.

> 다른 MEDITECH 서버에 대해 용량 할당하는 스토리지는 MEDITECH 호스트에서 사용되는 LUN의 전용 애그리게이트에 배치해서는 안 됩니다. 다른 MEDITECH 서버의 스토리지를 별도의 Aggregate에 배치해야 합니다. 다른 MEDITECH 서버의 스토리지 요구 사항은 "하드웨어 구성 제안"(신규 구축) 및 "하드웨어 평가 작업"(기존 구축) 문서에서 확인할 수 있습니다. MEDITECH 시스템 통합자나 MEDITECH TAM(기술 계정 관리자)을 통해 MEDITECH에서 이러한 문서를 얻을 수 있습니다. NetApp 솔루션 엔지니어는 NetApp MEDITECH ISV(Independent Software Vendor) 팀과 협의하여 적절하고 완벽한 NetApp 스토리지 사이징 구성을 지원할 수 있습니다.

MEDITECH 호스트 워크로드를 모든 스토리지 컨트롤러에 균등하게 분산시킵니다

NetApp FAS 및 AFF 시스템은 하나 이상의 고가용성 쌍으로 구축됩니다. 각 스토리지 컨트롤러에 MEDITECH의 넓은 워크로드와 6.x 워크로드를 균등하게 배포하여 컴퓨팅, 네트워크 및 캐싱 리소스를 각 스토리지 컨트롤러에 적용하는 것이 좋습니다.

다음 지침에 따라 각 스토리지 컨트롤러에 MEDITECH 워크로드를 균등하게 분산시키십시오.

- 각 MEDITECH 호스트의 IOPS를 알고 있는 경우 각 컨트롤러가 MEDITECH 호스트에서 유사한 수의 IOPS를 서비스하는지 확인하여 MEDITECH의 넓은 워크로드와 6.x 워크로드를 모든 스토리지 컨트롤러에 균등하게 분산시킬 수 있습니다.
- 각 MEDITECH 호스트의 IOPS를 모르는 경우에도 MEDITECH의 드넓은 워크로드와 6.x 워크로드를 모든 스토리지 컨트롤러에 균등하게 분산시킬 수 있습니다. MEDITECH 호스트의 애그리게이트 용량이 모든 스토리지 컨트롤러에 균등하게 분산되는지 확인하여 이 작업을 완료합니다. 이렇게 하면 MEDITECH 호스트 전용으로 사용되는 모든 데이터 집마다 디스크 수가 동일합니다.
- 비슷한 디스크 유형과 동일한 RAID 그룹을 사용하여 워크로드를 균등하게 분산하기 위해 두 컨트롤러의 스토리지 애그리게이트를 만들 수 있습니다. 스토리지 애그리게이트를 생성하려면 NetApp 인증 통합업체에 문의하십시오.

MEDITECH에 따르면 MEDITECH 시스템의 두 호스트는 나머지 호스트보다 높은 IOPS를 생성합니다. 이 두 호스트의 LUN은 별도의 스토리지 컨트롤러에 배치해야 합니다. 시스템을 배포하기 전에 MEDITECH 팀의 도움을 받아 이 두 호스트를 식별해야 합니다.

저장 장치 배치

MEDITECH 호스트용 데이터베이스 스토리지

MEDITECH 호스트의 데이터베이스 스토리지는 NetApp FAS 또는 AFF 시스템에서 블록 디바이스, 즉 LUN으로 제공됩니다. LUN은 일반적으로 Windows 운영 체제에 E 드라이브로 마운트됩니다.

기타 스토리지

MEDITECH 호스트 운영 체제와 데이터베이스 애플리케이션은 일반적으로 스토리지에 상당한 양의 IOPS를 생성합니다. MEDITECH 호스트 VM 및 해당 VMDK 파일에 대한 스토리지 프로비저닝은 MEDITECH 성능 임계값을 충족하는 데 필요한 스토리지와는 독립적인 것으로 간주됩니다.

다른 MEDITECH 서버에 대해 프로비저닝된 스토리지는 MEDITECH 호스트가 사용하는 LUN의 전용 애그리게이트에 배치해서는 안 됩니다. 다른 MEDITECH 서버용 스토리지를 별도의 Aggregate에 배치합니다.

스토리지 컨트롤러 구성

고가용성

컨트롤러 장애의 영향을 줄이고 스토리지 시스템의 무중단 업그레이드를 활성화하려면 고가용성 모드에서 컨트롤러를 사용하여 스토리지 시스템을 구성해야 합니다.

고가용성 컨트롤러 쌍 구성에서는 디스크 쉘프를 여러 경로를 통해 컨트롤러에 연결해야 합니다. 이 연결은 단일 경로 장애로부터 보호하여 스토리지 복원력을 높이고 컨트롤러 페일오버가 발생할 경우 성능 일관성을 개선합니다.

스토리지 컨트롤러 페일오버 중 스토리지 성능

고가용성 쌍의 컨트롤러로 구성된 스토리지 시스템의 경우, 컨트롤러 장애가 발생할 가능성이 낮은 경우 파트너 컨트롤러가 장애가 발생한 컨트롤러의 스토리지 리소스 및 워크로드를 대신 처리합니다. 컨트롤러 장애가 있는 경우 고객과 상의하여 성능 요구사항을 충족하고 시스템을 적절하게 사이징하는 것이 중요합니다.

하드웨어 지원 테이크오버

두 스토리지 컨트롤러 모두에서 하드웨어 지원 테이크오버 기능을 설정하는 것이 좋습니다.

하드웨어 지원 테이크오버는 스토리지 컨트롤러 페일오버 시간을 최소화하도록 설계되었습니다. 하나의 컨트롤러의 원격 LAN 모듈 또는 서비스 프로세서 모듈이 하트비트 시간 제한 트리거보다 빠르게 컨트롤러 장애에 대해 파트너에게 알릴 수 있으므로 장애 조치에 걸리는 시간이 줄어듭니다. 하드웨어 지원 테이크오버 기능은 고가용성 구성의 스토리지 컨트롤러에 대해 기본적으로 설정됩니다.

하드웨어 지원 테이크오버에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 문서 센터".

디스크 유형입니다

MEDITECH 워크로드의 낮은 읽기 지연 시간 요구사항을 지원하려면 MEDITECH 호스트 전용 AFF 시스템의 애그리게이트에 고성능 SSD를 사용하는 것이 좋습니다.

NetApp AFF를 참조하십시오

NetApp은 높은 처리량이 요구되는 MEDITECH 워크로드와 랜덤 데이터 액세스 패턴 및 짧은 지연 시간 요구사항을 해결하기 위해 고성능 AFF 어레이를 제공합니다. MEDITECH 워크로드의 경우 AFF 어레이는 HDD를 기반으로 하는 시스템에 비해 뛰어난 성능을 제공합니다. 플래시 기술과 엔터프라이즈 데이터 관리를 결합하면 성능, 가용성 및 스토리지 효율성이라는 세 가지 주요 영역에서 이점을 얻을 수 있습니다.

NetApp 지원 툴 및 서비스

NetApp은 완벽한 지원 툴 및 서비스 세트를 제공합니다. NetApp AutoSupport 툴은 하드웨어 장애나 시스템 구성 오류가 있는 경우 NetApp AFF/FAS 시스템에서 사용하도록 설정 및 구성해야 합니다. NetApp 지원 팀은 콜홈 경고를 통해 적시에 문제를 해결합니다. NetApp Active IQ는 NetApp 시스템의 AutoSupport 정보를 기반으로 예측 가능한 사전 통찰력을 제공하여 가용성, 효율성 및 성능을 향상하는 웹 기반 애플리케이션입니다.

구축 및 구성

개요

이 문서에 제공된 FlexPod 구축에 대한 NetApp 스토리지 지침은 다음과 같습니다.

- ONTAP를 사용하는 환경
- Cisco UCS 블레이드 및 랙 마운트 서버를 사용하는 환경

이 문서는 다음 사항을 다루지 않습니다.

- FlexPod 데이터 센터 환경의 세부 구축

  자세한 내용은 을 참조하십시오 "FC Cisco Validated Design이 구축된 FlexPod 데이터 센터" (CVD)

- MEDITECH 소프트웨어 환경, 참조 아키텍처 및 통합 모범 사례 지침을 간략하게 설명합니다.

  자세한 내용은 을 참조하십시오 "TR-4300i: MEDITECH 환경용 NetApp FAS 및 All-Flash 스토리지 시스템 모범 사례 가이드" (NetApp 로그인 필요).

- 정량적 성능 요구 사항 및 사이징 지침

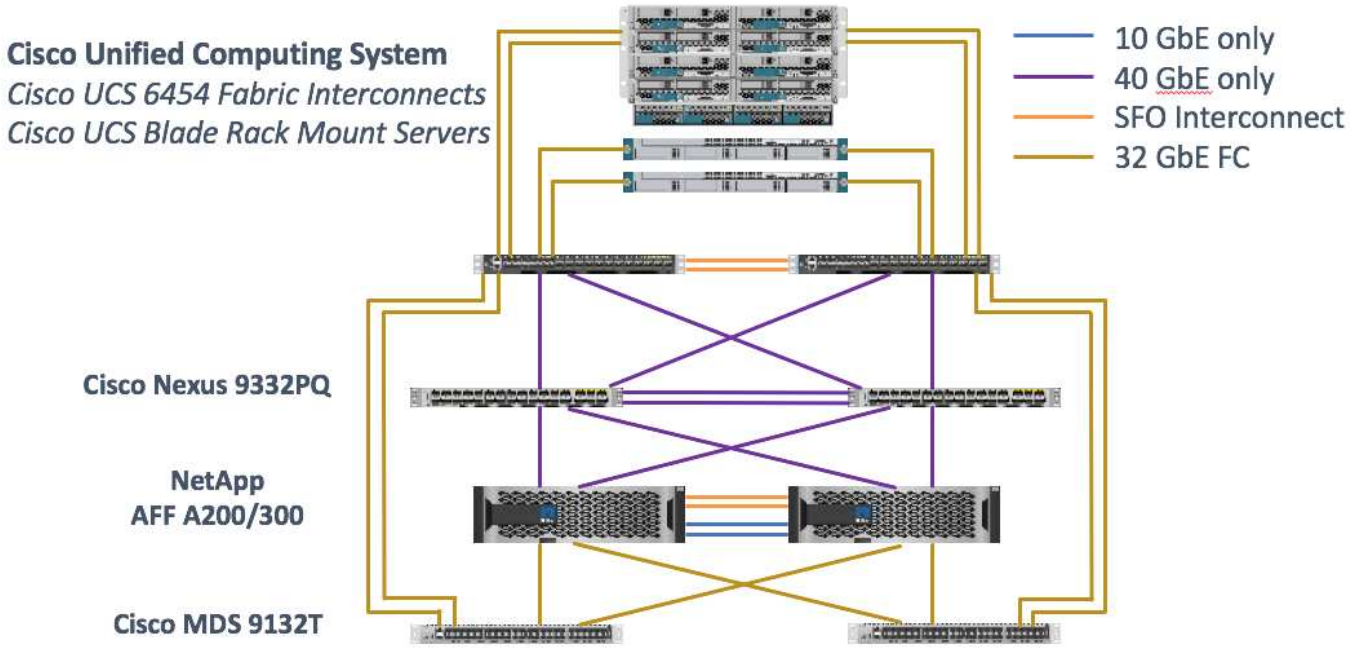
  자세한 내용은 을 참조하십시오 "TR-4190: MEDITECH 환경을 위한 NetApp 사이징 지침".

- NetApp SnapMirror 기술을 사용하여 백업 및 재해 복구 요구사항을 충족합니다.
- 일반 NetApp 스토리지 구축 지침:

이 섹션에서는 인프라 구축 모범 사례를 사용한 구성 예를 제공하고 다양한 인프라 하드웨어 및 소프트웨어 구성 요소와 사용할 수 있는 버전을 나열합니다.

케이블 연결 다이어그램

다음 그림에서는 MEDITECH 구축을 위한 32Gb FC/40GbE 토폴로지 다이어그램을 보여 줍니다.



항상 를 사용하십시오 "상호 운용성 매트릭스 툴(IMT)" 모든 소프트웨어 및 펌웨어 버전이 지원되는지 확인합니다. 섹션의 표 "MEDITECH 모듈 및 구성 요소" 에는 솔루션 테스트에 사용된 인프라 하드웨어 및 소프트웨어 구성요소가 나와 있습니다.

"다음: 기본 인프라 구성"

기본 인프라 구성

네트워크 연결

인프라를 구성하기 전에 다음 네트워크 연결이 설정되어야 합니다.

- 포트 채널과 vPC(가상 포트 채널)를 사용하는 링크 집계를 통해 대역폭 및 가용성을 높일 수 있습니다.
  - VPC는 Cisco FI와 Cisco Nexus 스위치 간에 사용됩니다.
  - 각 서버에는 Unified Fabric에 대한 중복 연결 기능을 갖춘 vNIC(Virtual Network Interface Card)가 있습니다. NIC 페일오버는 이중화를 위해 FI 간에 사용됩니다.
  - 각 서버에는 Unified Fabric에 대한 이중화 접속 기능을 갖춘 vHBA(Virtual Host Bus Adapter)가 있습니다.
- Cisco UCS FI는 권장 사항에 따라 최종 호스트 모드로 구성되어 업링크 스위치에 vNIC를 동적으로 고정할 수 있습니다.

스토리지 연결

인프라스트럭처를 구성하기 전에 다음과 같은 스토리지 접속을 설정해야 합니다.

- 스토리지 포트 인터페이스 그룹(ifgroup, vPC)
- 스위치 N9K-A에 대한 10Gb 링크
- 스위치 N9K-B에 대한 10Gb 링크
- 대역 내 관리(액티브-패시브 결합):

- 관리 스위치 N9K-A에 대한 1GB 링크
- 관리 스위치 N9K-B에 대한 1GB 링크

- Cisco MDS 스위치를 통한 32Gb FC 엔드 투 엔드 연결, 단일 이니시에이터 조닝 구성
- 상태 비저장 컴퓨팅을 최대한 실현하기 위한 FC SAN 부팅. 서버는 AFF 스토리지 클러스터에서 호스팅되는 부팅 볼륨의 LUN에서 부팅됩니다
- 모든 MEDITECH 워크로드는 스토리지 컨트롤러 노드에 분산되는 FC LUN에서 호스팅됩니다

호스트 소프트웨어

다음 소프트웨어를 설치해야 합니다.

- Cisco UCS 블레이드에 설치된 ESXi
- VMware vCenter 설치 및 구성(vCenter에 등록된 모든 호스트 포함)
- VMware vCenter에 VSC를 설치 및 등록했습니다
- NetApp 클러스터가 구성되었습니다

"다음: Cisco UCS 블레이드 서버 및 스위치 구성"

Cisco UCS 블레이드 서버 및 스위치 구성

MEDITECH용 FlexPod 소프트웨어는 모든 레벨에서 내결함성을 제공하도록 설계되었습니다. 시스템에 단일 장애 지점이 없습니다. 최적의 성능을 위해 핫 스페어 블레이드 서버를 사용하는 것이 좋습니다.

이 문서에서는 MEDITECH 소프트웨어용 FlexPod 환경의 기본 구성에 대한 자세한 지침을 제공합니다. 이 섹션에서는 FlexPod 구성의 Cisco UCS 컴퓨팅 플랫폼 요소를 준비하기 위한 몇 가지 예에 대해 개략적인 단계를 설명합니다. 이 지침을 수행하기 전에 의 지침에 따라 FlexPod 구성을 랙에 설치하고, 전원을 공급하며, 케이블로 연결해야 합니다 "FlexPod vSphere 6.5 업데이트 1, NetApp AFF A 시리즈 및 Cisco UCS Manager 3.2를 사용하는 파이버 채널 스토리지가 있는 데이터 센터"CVD

Cisco Nexus 스위치 구성

이 솔루션을 위해 내결함성을 갖춘 Cisco Nexus 9300 시리즈 이더넷 스위치 쌍이 구축되었습니다. 에 설명된 대로 이러한 스위치에 케이블을 연결해야 합니다 "케이블 연결 다이어그램" 섹션을 참조하십시오. Cisco Nexus 구성을 사용하면 이더넷 트래픽 흐름이 MEDITECH 애플리케이션에 최적화되도록 할 수 있습니다.

1. 초기 설정 및 라이센스를 완료한 후 다음 명령을 실행하여 두 스위치에서 글로벌 구성 매개 변수를 설정합니다.

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
port-channel load-balance src-dst l4port
ntp server <global-ntp-server-ip> use-vrf management
ntp master 3
ip route 0.0.0.0/0 <ib-mgmt-vlan-gateway>
copy run start
```

2. 글로벌 구성 모드를 사용하여 각 스위치에서 솔루션에 대한 VLAN을 생성합니다.

```
vlan <ib-mgmt-vlan-id>
name IB-MGMT-VLAN
vlan <native-vlan-id>
name Native-VLAN
vlan <vmotion-vlan-id>
name vMotion-VLAN
vlan <vm-traffic-vlan-id>
name VM-Traffic-VLAN
vlan <infra-nfs-vlan-id>
name Infra-NFS-VLAN
exit
copy run start
```

3. 에 따라 문제 해결을 위해 NTP(Network Time Protocol) 분산 인터페이스, 포트 채널, 포트 채널 매개 변수 및 포트 설명을 생성합니다 "FlexPod vSphere 6.5 업데이트 1, NetApp AFF A 시리즈 및 Cisco UCS Manager 3.2를 사용하는 파이버 채널 스토리지가 있는 데이터 센터"CVD

Cisco MDS 9132T 구성

Cisco MDS 9100 시리즈 FC 스위치는 NetApp AFF A200 또는 AFF A300 컨트롤러와 Cisco UCS 컴퓨팅 패브릭 간에 이중화된 32Gb FC 연결을 제공합니다. 에 설명된 대로 케이블을 연결해야 합니다 "케이블 연결 다이어그램" 섹션을 참조하십시오.

1. 각 MDS 스위치의 콘솔에서 다음 명령을 실행하여 솔루션에 필요한 기능을 설정합니다.

```
configure terminal
feature npiv
feature fport-channel-trunk
```

2. 의 FlexPod Cisco MDS 스위치 구성 섹션에 따라 개별 포트, 포트 채널 및 설명을 구성합니다 "FC Cisco Validated Design이 구축된 FlexPod 데이터 센터".
3. 솔루션에 필요한 VSAN(Virtual SAN)을 생성하려면 글로벌 구성 모드에서 다음 단계를 수행하십시오.
   a. Fabric-A MDS 스위치의 경우 다음 명령을 실행합니다.

```
vsan database
vsan <vsan-a-id>
vsan <vsan-a-id> name Fabric-A
exit
zone smart-zoning enable vsan <vsan-a-id>
vsan database
vsan <vsan-a-id> interface fc1/1
vsan <vsan-a-id> interface fc1/2
vsan <vsan-a-id> interface port-channel110
vsan <vsan-a-id> interface port-channel112
```

명령의 마지막 두 줄에 있는 포트 채널 번호는 참조 문서를 사용하여 개별 포트, 포트 채널 및 설명을 프로비저닝할 때 생성되었습니다.

b. Fabric-B MDS 스위치의 경우 다음 명령을 실행합니다.

```
vsan database
vsan <vsan-b-id>
vsan <vsan-b-id> name Fabric-B
exit
zone smart-zoning enable vsan <vsan-b-id>
vsan database
vsan <vsan-b-id> interface fc1/1
vsan <vsan-b-id> interface fc1/2
vsan <vsan-b-id> interface port-channel111
vsan <vsan-b-id> interface port-channel113
```

명령의 마지막 두 줄에 있는 포트 채널 번호는 참조 문서를 사용하여 개별 포트, 포트 채널 및 설명을 프로비저닝할 때 생성되었습니다.

4. 각 FC 스위치에 대해 참조 문서의 세부 정보를 사용하여 각 장치를 직관적으로 식별할 수 있도록 디바이스 별칭 이름을 생성합니다.
5. 마지막으로, 다음과 같이 각 MDS 스위치에 대해 4단계에서 생성한 디바이스 별칭 이름을 사용하여 FC 존을 생성합니다.
   a. Fabric-A MDS 스위치의 경우 다음 명령을 실행합니다.

```
configure terminal
zone name VM-Host-Infra-01-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-01-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zone name VM-Host-Infra-02-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-02-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zoneset name Fabric-A vsan <vsan-a-id>
member VM-Host-Infra-01-A
member VM-Host-Infra-02-A
exit
zoneset activate name Fabric-A vsan <vsan-a-id>
exit
show zoneset active vsan <vsan-a-id>
```

b. Fabric-B MDS 스위치의 경우 다음 명령을 실행합니다.

```
configure terminal
zone name VM-Host-Infra-01-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-01-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zone name VM-Host-Infra-02-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-02-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zoneset name Fabric-B vsan <vsan-b-id>
member VM-Host-Infra-01-B
member VM-Host-Infra-02-B
exit
zoneset activate name Fabric-B vsan <vsan-b-id>
exit
show zoneset active vsan <vsan-b-id>
```

Cisco UCS 구성 지침

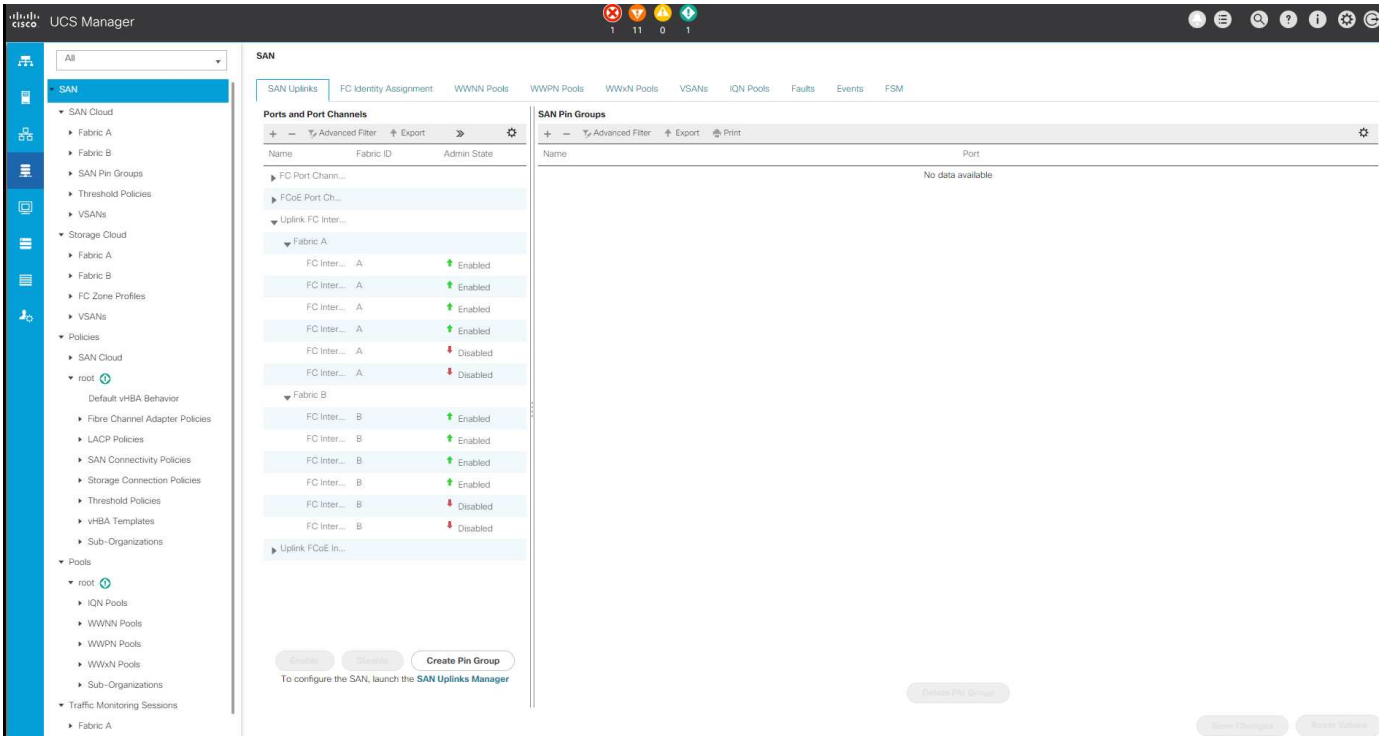
Cisco UCS를 통해 MEDITECH 고객은 네트워크, 스토리지 및 컴퓨팅 분야의 실무 전문가를 활용하여 고객의 특정 요구에 맞게 환경을 조정하는 정책 및 템플릿을 작성할 수 있습니다. 생성된 정책 및 템플릿은 Cisco 블레이드 및 랙

서버를 일관성 있고 반복 가능하며 안정적이며 신속하게 구축할 수 있도록 서비스 프로필에 결합할 수 있습니다.

Cisco UCS는 도메인이라는 Cisco UCS 시스템을 관리하는 세 가지 방법을 제공합니다.

- Cisco UCS Manager HTML5 GUI
- Cisco UCS CLI
- 다중 도메인 환경을 위한 Cisco UCS Central

다음 그림은 Cisco UCS Manager의 SAN 노드에 대한 샘플 스크린샷입니다.



대규모 구축에서는 주요 MEDITECH 기능 구성 요소 레벨에서 내결함성을 더욱 높일 수 있는 독립적인 Cisco UCS 도메인을 구축할 수 있습니다.

두 개 이상의 데이터 센터를 통한 내결함성 설계에서 Cisco UCS Central은 기업 전반의 호스트 간 일관성을 위한 글로벌 정책 및 글로벌 서비스 프로필을 설정하는 데 중요한 역할을 합니다.

Cisco UCS 컴퓨팅 플랫폼을 설정하려면 다음 절차를 완료하십시오. Cisco UCS 5108 AC 블레이드 섀시에 Cisco UCS B200 M5 블레이드 서버를 설치한 후 다음 절차를 수행하십시오. 또한 에 설명된 대로 케이블 연결 요구 사항을 경쟁해야 합니다 "케이블 연결 다이어그램" 섹션을 참조하십시오.

1. Cisco UCS Manager 펌웨어를 버전 3.2(2f) 이상으로 업그레이드합니다.
2. 도메인에 대한 보고, Cisco Call Home 기능 및 NTP 설정을 구성합니다.
3. 각 Fabric Interconnect에서 서버 및 업링크 포트를 구성합니다.
4. 섀시 검색 정책을 편집합니다.
5. 대역 외 관리, UUID(Universal Unique Identifier), MAC 주소, 서버, WWNN(Worldwide Node Name) 및 WWPN(Worldwide Port Name)을 위한 주소 풀을 생성합니다.
6. 이더넷 및 FC 업링크 포트 채널과 VSAN을 생성합니다.

7. SAN 연결, 네트워크 제어, 서버 풀 검증, 전원 제어, 서버 BIOS, 및 기본 유지 관리.
8. vNIC 및 vHBA 템플릿을 생성합니다.
9. vMedia 및 FC 부팅 정책을 생성합니다.
10. 각 MEDITECH 플랫폼 요소에 대한 서비스 프로필 템플릿 및 서비스 프로필을 생성합니다.
11. 서비스 프로필을 적절한 블레이드 서버와 연결합니다.

FlexPod용 Cisco UCS 서비스 프로필의 각 주요 요소를 구성하는 단계에 대한 자세한 내용은 를 참조하십시오 "FlexPod vSphere 6.5 업데이트 1, NetApp AFF A 시리즈 및 Cisco UCS Manager 3.2를 사용하는 파이버 채널 스토리지가 있는 데이터 센터"CVD 문서

"다음은 ESXi 구성 Best Practice입니다."

ESXi 구성 **Best Practice**

ESXi 호스트 측 구성의 경우 엔터프라이즈 데이터베이스 워크로드를 실행할 때 VMware 호스트를 구성합니다.

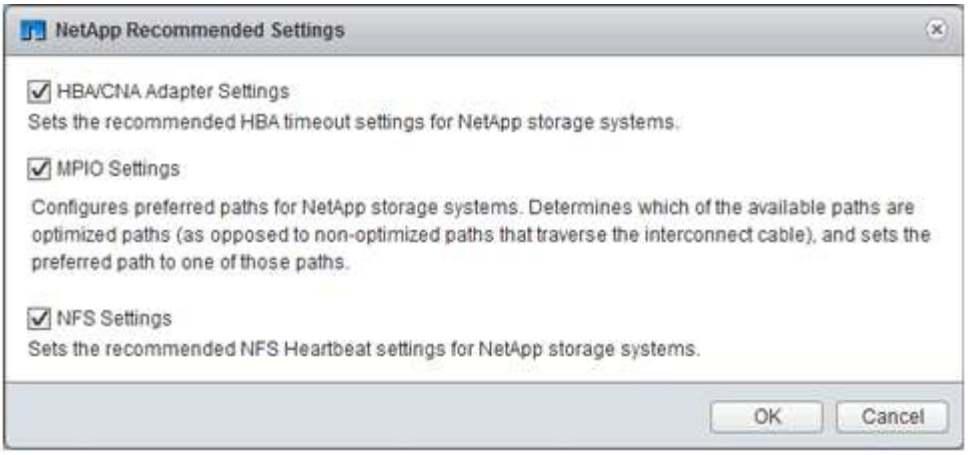
- VMware vSphere용 VSC는 NetApp 스토리지 시스템에 가장 적합한 ESXi 호스트 경로 다중화 설정 및 HBA 시간 초과 설정을 확인하고 설정합니다. VSC 세트는 NetApp의 엄격한 내부 테스트를 기반으로 합니다.
- 스토리지 성능을 최적화하려면 VMware VAAI(vStorage API - Array Integration)를 지원하는 스토리지 하드웨어를 사용하는 것이 좋습니다. VAAI용 NetApp 플러그인은 ESXi 호스트에 설치된 VMware 가상 디스크 라이브러리를 통합하는 소프트웨어 라이브러리입니다. VMware VAAI 패키지를 사용하면 특정 작업을 물리적 호스트에서 스토리지 시스템으로 오프로드할 수 있습니다.

  스토리지 레벨에서 씬 프로비저닝 및 하드웨어 가속 등의 작업을 수행하여 ESXi 호스트의 워크로드를 줄일 수 있습니다. 복사본 오프로드 기능 및 공간 예약 기능으로 VSC 작업의 성능을 향상합니다. 플러그인 설치 패키지를 다운로드하고 NetApp Support 사이트에서 플러그인 설치 지침을 확인할 수 있습니다.

  VSC는 NetApp 스토리지 컨트롤러의 최적의 성능과 성공적인 페일오버를 위해 ESXi 호스트 시간 초과, 다중 경로 설정, HBA 시간 초과 설정 및 기타 값을 설정합니다. 다음 단계를 수행하십시오.

  a. VMware vSphere Web Client 홈 페이지에서 vCenter > 호스트 를 선택합니다.
  b. 호스트를 마우스 오른쪽 버튼으로 클릭한 다음 Actions > NetApp VSC > Set Recommended Values를 선택합니다.
  c. NetApp 권장 설정 대화 상자에서 시스템에 가장 적합한 값을 선택합니다.

     표준 권장 값은 기본적으로 설정됩니다.



a. 확인 을 클릭합니다.

"다음: NetApp 구성"

NetApp 구성입니다

MEDITECH 소프트웨어 환경용 NetApp 스토리지는 고가용성 쌍 구성에서 스토리지 컨트롤러를 사용합니다. FC 프로토콜을 통해 두 컨트롤러에서 MEDITECH 데이터베이스 서버로 스토리지를 제공해야 합니다. 이 구성은 정상 작동 중에 두 컨트롤러의 스토리지를 모두 사용하여 애플리케이션 로드를 균등하게 분산합니다.

ONTAP 구성

이 섹션에서는 관련 ONTAP 명령을 사용하는 구축 및 프로비저닝 절차의 예를 설명합니다. 에서는 고가용성 컨트롤러 쌍을 사용하는 NetApp이 권장하는 스토리지 레이아웃을 구현하기 위해 스토리지가 프로비저닝되는 방식을 중점적으로 보여 줍니다. ONTAP의 주요 장점 중 하나는 기존 고가용성 쌍을 방해하지 않으면서 스케일아웃하는 것입니다.

ONTAP 라이센스

스토리지 컨트롤러를 설정한 후 라이센스를 적용하여 NetApp에서 권장하는 ONTAP 기능을 사용하도록 설정합니다. MEDITECH 워크로드에 대한 라이센스는 FC, CIFS 및 NetApp Snapshot, SnapRestore, FlexClone, SnapMirror 기술을 사용합니다.

라이센스를 구성하려면 NetApp ONTAP 시스템 관리자를 열고 구성 - 라이센스로 이동한 다음 적절한 라이센스를 추가합니다.

또는 다음 명령을 실행하여 CLI를 사용하여 라이센스를 추가합니다.

```
license add -license-code <code>
```

AutoSupport 구성

NetApp AutoSupport 툴은 HTTPS를 통해 요약 지원 정보를 NetApp에 보냅니다. AutoSupport를 구성하려면 다음 ONTAP 명령을 실행합니다.

```
autosupport modify -node * -state enable
autosupport modify -node * -mail-hosts <mailhost.customer.com>
autosupport modify -node prod1-01 -from prod1-01@customer.com
autosupport modify -node prod1-02 -from prod1-02@customer.com
autosupport modify -node * -to storageadmins@customer.com
autosupport modify -node * -support enable
autosupport modify -node * -transport https
autosupport modify -node * -hostnamesubj true
```

하드웨어 지원 테이크오버 구성

각 노드에서 하드웨어 지원 테이크오버를 활성화하여 컨트롤러 장애가 발생할 가능성이 낮은 상황에서 테이크오버 시작에 걸리는 시간을 최소화합니다. 하드웨어 지원 테이크오버를 구성하려면 다음 단계를 완료합니다.

1. 다음 ONTAP 명령을 xxx로 실행합니다.

   파트너 주소 옵션을 'prod1-01'에 대한 관리 포트의 IP 주소로 설정합니다.

   ```
   MEDITECH::> storage failover modify -node prod1-01 -hwassist-partner-ip
   <prod1-02-mgmt-ip>
   ```

2. 다음 ONTAP 명령을 xxx에 실행합니다.

   파트너 주소 옵션을 'cluster1-02'에 대한 관리 포트의 IP 주소로 설정합니다.

   ```
   MEDITECH::> storage failover modify -node prod1-02 -hwassist-partner-ip
   <prod1-01-mgmt-ip>
   ```

3. 다음 ONTAP 명령을 실행하여 "prod1-01"과 "prod1-02" HA 컨트롤러 쌍 모두에서 하드웨어 지원 테이크오버를 활성화합니다.

   ```
   MEDITECH::> storage failover modify -node prod1-01 -hwassist true
   MEDITECH::> storage failover modify -node prod1-02 -hwassist true
   ```

"다음: 집계 구성."

애그리게이트 구성

NetApp RAID DP를 참조하십시오

NetApp RAID DP 기술은 일반 NetApp Flash Pool 애그리게이트를 포함하여 NetApp FAS 또는 AFF 시스템의 모든 애그리게이트를 위한 RAID 유형으로 권장됩니다. MEDITECH 설명서에 RAID 10의 사용이 지정되어 있을 수 있지만 MEDITECH는 RAID DP 사용을 승인했습니다.

RAID 그룹 크기 및 RAID 그룹 수

기본 RAID 그룹 크기는 16입니다. 이 크기는 특정 사이트의 MEDITECH 호스트에 대한 집계를 위한 최적의 크기일 수도 있고 그렇지 않을 수도 있습니다. RAID 그룹에 사용할 것을 권장한 디스크 수에 대해서는 를 참조하십시오 "NetApp TR-3838: 스토리지 서브시스템 구성 가이드".

RAID 그룹 크기와 RAID 그룹 크기가 같은 하나 이상의 디스크 그룹이 있는 애그리게이트에 디스크를 추가하는 것이 권장되므로 스토리지 확장에는 RAID 그룹 크기가 중요합니다. RAID 그룹 수는 데이터 디스크 수와 RAID 그룹 크기에 따라 달라집니다. 필요한 데이터 디스크의 수를 확인하려면 SPM(NetApp System Performance Modeler) 사이징 툴을 사용하십시오. 데이터 디스크 수를 결정한 후 RAID 그룹 크기를 조정하여 디스크 유형당 RAID 그룹 크기에 대해 권장되는 범위 내에서 패리티 디스크 수를 최소화합니다.

MEDITECH 환경에 SPM 사이징 툴을 사용하는 방법에 대한 자세한 내용은 을 참조하십시오 "NetApp TR-4190: MEDITECH 환경을 위한 NetApp 사이징 지침".

스토리지 확장 고려 사항

더 많은 디스크로 애그리게이트를 확장할 경우, 애그리게이트 RAID 그룹 크기와 같은 그룹으로 디스크를 추가하십시오. 이 방법을 따라하면 애그리게이트 전체에서 성능 일관성을 제공할 수 있습니다.

예를 들어, RAID 그룹 크기가 20인 Aggregate에 스토리지를 추가하려면 NetApp에서 권장하는 디스크 수는 하나 이상의 20-디스크 그룹입니다. 디스크를 20, 40, 60 등으로 추가해야 합니다.

애그리게이트를 확장한 후에는 영향을 받는 볼륨에서 재할당 작업을 실행하거나, 애그리게이트를 실행하여 기존 데이터 스트라이프를 새 디스크에 분산하여 성능을 향상할 수 있습니다. 이 작업은 특히 기존 집계가 거의 가득 찬 경우 유용합니다.

비운영 시간 동안에는 CPU 및 디스크 사용량이 많은 작업이므로 일정 재할당을 계획해야 합니다.

애그리게이트 확장 후 재할당을 사용하는 방법에 대한 자세한 내용은 를 참조하십시오 "NetApp TR-3929: 재할당 모범 사례 가이드".

Aggregate 레벨의 Snapshot 복사본

Aggregate 레벨의 NetApp 스냅샷 복사본 예약 공간을 0으로 설정하고 기본 애그리게이트 스냅샷 스케줄을 비활성화합니다. 가능하면 기존의 모든 애그리게이트 레벨 스냅샷 복사본을 삭제합니다.

"다음: 스토리지 가상 머신 구성"

스토리지 가상 머신 구성

이 섹션은 ONTAP 8.3 이상 버전에 구축하는 방법을 다룹니다.

SVM(스토리지 가상 머신)은 ONTAP API 및 ONTAP CLI에서 SVM이라고도 합니다.

MEDITECH 호스트 LUN용 SVM

MEDITECH 호스트의 LUN이 포함된 애그리게이트를 소유 및 관리하려면 ONTAP 스토리지 클러스터당 하나의 전용 SVM을 생성해야 합니다.

SVM 언어 인코딩 설정

모든 SVM에 대해 언어 인코딩을 설정하는 것이 좋습니다. SVM 생성 시 언어 인코딩 설정을 지정하지 않으면 기본 언어 인코딩 설정이 사용됩니다. 기본 언어 인코딩 설정은 ONTAP의 경우 c UTF-8입니다. 언어 인코딩을 설정한 후에는 나중에 무한 확장 볼륨을 가진 SVM의 언어를 수정할 수 없습니다.

볼륨이 생성될 때 다른 설정을 명시적으로 지정하지 않으면 SVM과 연결된 볼륨이 SVM 언어 인코딩 설정을 상속합니다. 특정 작업을 사용하려면 사이트의 모든 볼륨에서 언어 인코딩 설정을 일관되게 사용해야 합니다. 예를 들어, SnapMirror에서는 소스 및 타겟 SVM에 동일한 언어 인코딩 설정이 필요합니다.

"다음: 볼륨 구성."

볼륨 구성

볼륨 프로비저닝

MEDITECH 호스트용 MEDITECH 볼륨은 일반 또는 씬 프로비저닝될 수 있습니다.

기본 볼륨 레벨 스냅샷 복사본

스냅샷 복사본은 백업 워크플로우의 일부로 생성됩니다. 각 스냅샷 복사본을 사용하여 MEDITECH LUN에 저장된 데이터에 다른 시간에 액세스할 수 있습니다. MEDITECH 승인 백업 솔루션은 이러한 Snapshot 복제본을 기반으로 씬 프로비저닝된 FlexClone 볼륨을 생성하여 MEDITECH LUN의 시점 복제본을 제공합니다. MEDITECH 환경은 승인된 백업 소프트웨어 솔루션과 통합됩니다. 따라서 MEDITECH 운영 데이터베이스 LUN을 구성하는 각 NetApp FlexVol 볼륨에서 기본 스냅샷 복사본 스케줄을 사용하지 않도록 설정하는 것이 좋습니다.

- 중요: * FlexClone 볼륨은 상위 데이터 볼륨 공간을 공유하기 때문에 백업 서버가 생성하는 MEDITECH 데이터 LUN 및 FlexClone 볼륨에 충분한 공간을 확보하는 것이 중요합니다. FlexClone 볼륨은 데이터 볼륨보다 더 많은 공간을 차지하지 않습니다. 그러나 MEDITECH LUN에서 짧은 시간 내에 대규모 삭제가 발생하면 클론 볼륨이 증가할 수 있습니다.

애그리게이트당 볼륨 수입니다

Flash Pool 또는 NetApp Flash Cache 캐싱을 사용하는 NetApp FAS 시스템의 경우 MEDITECH 프로그램, 사전 및 데이터 파일 저장용 Aggregate당 3개 이상의 볼륨을 프로비저닝하는 것이 좋습니다.

AFF 시스템의 경우 MEDITECH 프로그램, 사전 및 데이터 파일을 저장하기 위해 애그리게이트당 4개 이상의 볼륨을 전용으로 할당하는 것이 좋습니다.

볼륨 레벨 재할당 스케줄

특히 MEDITECH, 6.x 및 C/S 5.x 플랫폼과 같은 쓰기 집약적인 워크로드에서 스토리지의 데이터 레이아웃이 시간이 지남에 따라 최적화되지 않습니다. 시간이 지나면서 순차적 읽기 지연 시간이 증가하여 백업을 완료하는 데 더 오랜 시간이 걸릴 수 있습니다. 잘못된 데이터 레이아웃 또는 조각화는 쓰기 지연 시간에 영향을 줄 수도 있습니다. 볼륨 레벨 재할당을 사용하여 디스크의 데이터 레이아웃을 최적화하여 쓰기 지연 시간과 순차적 읽기 액세스를 향상시킬 수 있습니다. 향상된 스토리지 레이아웃을 통해 할당된 8시간 내에 백업을 완료할 수 있습니다.

모범 사례
NetApp은 최소한 매주 볼륨 재할당 일정을 구현하여 할당된 유지보수 다운타임 동안 또는 운영 사이트에서 사용량이 적은 시간 동안 재할당 작업을 실행할 것을 권장합니다. NetApp은 재할당 작업을 컨트롤러당 한 번에 하나의 볼륨에 대해 실행할 것을 적극 권장합니다.

프로덕션 데이터베이스 스토리지에 적합한 볼륨 재할당 일정을 결정하는 방법에 대한 자세한 내용은 의 3.12절을 참조하십시오 "NetApp TR-3929: 재할당 모범 사례 가이드". 또한 이 섹션에서는 사용 중인 사이트에 대한 주간 재할당 일정을 만드는 방법에 대해서도 설명합니다.

"다음: LUN 구성."

LUN 구성

사용자 환경의 MEDITECH 호스트 수에 따라 NetApp FAS 또는 AFF 시스템 내에서 생성되는 LUN의 수가 결정됩니다. 하드웨어 구성 제안에서는 각 LUN의 크기를 지정합니다.

LUN 프로비저닝

MEDITECH 호스트용 MEDITECH LUN은 일반 또는 씬 프로비저닝될 수 있습니다.

LUN 운영 체제 유형입니다

생성되는 LUN을 올바르게 정렬하려면 LUN의 운영 체제 유형을 올바르게 설정해야 합니다. 잘못 정렬된 LUN은 불필요한 쓰기 작업 오버헤드를 발생하므로 잘못 정렬된 LUN을 수정하는 데 비용이 많이 듭니다.

MEDITECH 호스트 서버는 일반적으로 VMware vSphere 하이퍼바이저를 사용하여 가상화된 Windows Server 환경에서 실행됩니다. 호스트 서버는 베어 메탈 서버의 Windows Server 환경에서도 실행할 수 있습니다. 설정할 운영 체제 유형 값을 확인하려면 의 "LUN 생성" 섹션을 참조하십시오 "Clustered Data ONTAP 8.3 명령: 수동 페이지 참조".

LUN 크기입니다

각 MEDITECH 호스트의 LUN 크기를 확인하려면 MEDITECH의 하드웨어 구성 제안(새 배포) 또는 하드웨어 평가 작업(기존 배포) 문서를 참조하십시오.

LUN 표시

MEDITECH는 FC 프로토콜을 사용하여 프로그램, 사전 및 데이터 파일용 스토리지를 MEDITECH 호스트에 LUN으로 제공해야 합니다. VMware 가상 환경에서 LUN은 MEDITECH 호스트를 호스팅하는 VMware ESXi 서버에 제공됩니다. 그런 다음 VMware ESXi 서버에 제공되는 각 LUN은 물리적 호환성 모드에서 RDM을 사용하여 각 MEDITECH 호스트 VM에 매핑됩니다.

적절한 LUN 명명 규칙을 사용하여 LUN을 MEDITCH 호스트에 제공해야 합니다. 예를 들어, 간편한 관리를 위해 MEDITECH 호스트 Mt-host-01에 LUN MTFS01E를 제공해야 합니다.

MEDITECH 및 백업 시스템 설치 프로그램과 상담할 때 MEDITECH 하드웨어 구성 제안을 참조하여 MEDITECH 호스트가 사용하는 LUN에 대해 일관된 명명 규칙을 고안합니다.

MEDITECH LUN 이름의 예로는 MTFS05E가 있으며, 다음과 같은 이름이 있습니다.

- mTFS는 MEDITECH 파일 서버(MEDITECH 호스트용)를 나타냅니다.
- 05는 호스트 번호 5를 나타냅니다.
- E는 Windows E 드라이브를 나타냅니다.

"다음: 이니시에이터 그룹 구성"

이니시에이터 그룹 구성

FC를 데이터 네트워크 프로토콜로 사용할 경우 각 스토리지 컨트롤러에 두 개의 이니시에이터 그룹(igroup)을 생성합니다. 첫 번째 igroup에는 MEDITECH 호스트 VM(MEDITECH용 igroup)을 호스팅하는 VMware ESXi 서버의 FC 호스트 인터페이스 카드 WWPN이 포함되어 있습니다.

환경 설정에 따라 MEDITECH igroup 운영 체제 유형을 설정해야 합니다. 예를 들면 다음과 같습니다.

- Windows Server 환경에서 베어 메탈 서버 하드웨어에 설치된 애플리케이션의 경우 igroup 운영 체제 유형 'Windows'를 사용합니다.
- VMware vSphere 하이퍼바이저를 사용하여 가상화된 애플리케이션에 대해 igroup 운영 체제 유형 'VMware'를 사용합니다.

> igroup의 운영 체제 유형이 LUN의 운영 체제 유형과 다를 수 있습니다. 예를 들어 가상화된 MEDITECH 호스트의 경우 igroup 운영 체제 유형을 "VMware"로 설정해야 합니다. 가상화된 MEDITECH 호스트에서 사용되는 LUN의 경우 운영 체제 유형을 "Windows 2008 이상"으로 설정해야 합니다. MEDITECH 호스트 운영 체제가 Windows Server 2008 R2 64비트 Enterprise Edition 이기 때문에 이 설정을 사용합니다.

운영 체제 유형에 대한 올바른 값을 확인하려면 에서 "LUN iGroup 생성" 및 "LUN 생성" 섹션을 참조하십시오 "Clustered Data ONTAP 8.2 명령: 수동 페이지 참조".

"다음: LUN 매핑"

LUN 매핑

MEDITECH 호스트의 LUN 매핑은 LUN을 생성할 때 설정됩니다.

MEDITECH 모듈 및 구성 요소

MEDITECH 애플리케이션은 여러 모듈과 구성 요소를 포함합니다. 다음 표에는 이러한 모듈에서 다루는 기능이 나열되어 있습니다. 이러한 모듈의 설정 및 배포에 대한 자세한 내용은 MEDITECH 설명서를 참조하십시오.

기능	유형
연결성	• 웹 서버 • 라이브 애플리케이션 서버(Wi-Web 통합) • 애플리케이션 서버(Wi) 테스트 • SAML 인증 서버(Wi) • SAML 프록시 서버(Wi) • 데이터베이스 서버
검토할 수 있습니다	• 파일 서버 • 백그라운드 작업 클라이언트 • 연결 서버 • 트랜잭션 서버
스캔 및 보관	• 이미지 서버
데이터 저장소	• SQL 서버
비즈니스 및 임상 분석	• BCA(Live Intelligence Server) • 인텔리전스 서버(BCA) 테스트 • 데이터베이스 서버(BCA)
홈 케어	• 원격 사이트 솔루션 • 연결성 • 검토할 수 있습니다 • 인쇄 중 • 현장 장치 • 스캔 중 • 호스팅된 사이트 요구 사항 • 방화벽 구성
지원	• 백그라운드 작업 클라이언트(CAL – 클라이언트 액세스 라이선스)
사용자 장치	• 태블릿 • 고정 장치

기능	유형
인쇄 중	• 라이브 네트워크 인쇄 서버(필수, 이미 있을 수 있음) • 네트워크 인쇄 서버 테스트(필수, 이미 있을 수 있음)
타사 요구 사항	• 첫 번째 데이터뱅크(FDB) MedKnowledge Framework v4.3

감사의 말

다음 사람들은 이 가이드의 작성에 기여했습니다.

- Brandon AGEE, NetApp 기술 마케팅 엔지니어
- NetApp 기술 마케팅 엔지니어 Atul Bhalodia
- NetApp 선임 제품 매니저 Ketan Mota
- John Duignan, NetApp 의료 솔루션 설계자
- Cisco의 Jon Ebmeier
- Cisco의 Mike Brennan 씨

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대한 자세한 내용은 다음 문서 또는 웹 사이트를 참조하십시오.

FlexPod 디자인 영역

- "FlexPod 설계 구역"
- "NetApp AFF, vSphere 6.5U1 및 Cisco UCS Manager를 사용하는 FC 스토리지(MDS 스위치)가 포함된 FlexPod 데이터 센터"

NetApp 기술 보고서

- "TR-3929: Reallocate 모범 사례 가이드"
- "TR-3987: InterSystems Caché용 Snap Creator Framework 플러그인"
- "TR-4300i: MEDITECH 환경용 NetApp FAS 및 All-Flash 스토리지 시스템 모범 사례 가이드"
- "TR-4017: FC SAN 모범 사례"
- "TR-3446: SnapMirror 비동기 개요 및 모범 사례 가이드"

ONTAP 설명서

- "NetApp 제품 설명서"
- "vSphere용 VSC(Virtual Storage Console) 문서"
- "ONTAP 9 문서 센터":

- "ESXi용 FC Express 가이드"

- "모든 ONTAP 9.3 문서":
  - "소프트웨어 설치 안내서"
  - "디스크 및 애그리게이트 전원 가이드"
  - "SAN 관리 가이드를 참조하십시오"
  - "SAN 구성 가이드 를 참조하십시오"
  - "Windows Express용 FC 구성 가이드 를 참조하십시오"
  - "FC SAN에 최적화된 AFF 설정 가이드"
  - "High-Availability 구성 가이드 를 참조하십시오"
  - "논리적 스토리지 관리 가이드"
  - "성능 관리 전원 가이드"
  - "SMB/CIFS 구성 전원 가이드"
  - "SMB/CIFS 참조"
  - "데이터 보호 전원 가이드"
  - "데이터 보호 테이프 백업 및 복구 가이드"
  - "NetApp 암호화 기능 가이드 를 참조하십시오"
  - "네트워크 관리 가이드 를 참조하십시오"
  - "명령: ONTAP 9.3에 대한 수동 페이지 참조"

Cisco Nexus, MDS, Cisco UCS 및 **Cisco UCS Manager** 가이드

- "Cisco UCS 서버 개요"
- "Cisco UCS 블레이드 서버 개요"
- "Cisco UCS B200 M5 데이터시트"
- "Cisco UCS Manager 개요"
- "Cisco UCS Manager 3.2(3a) 인프라 번들" (Cisco.com 인증 필요)
- "Cisco Nexus 9300 플랫폼 스위치"
- "Cisco MDS 9132T FC 스위치"

의료 영상용 **FlexPod**

TR-4865: 의료 영상용 **FlexPod**

NetApp의 Jaya Kishore Esanakula 및 Atil Bhalodia

의료 영상 촬영은 의료 조직에서 생성한 모든 데이터의 70%를 차지합니다. 디지털 기법의 발전 및 새로운 기법의 등장과 함께 데이터의 양은 계속해서 증가합니다. 예를 들어, 아날로그에서 디지털 병리학으로 전환하면 현재 적용되는 데이터 관리 전략에 문제가 되는 속도로 이미지

크기가 크게 증가합니다.

최근 COVID-19로 디지털 혁신을 명확하게 재구성할 수 있었습니다 "보고서"COVID-19는 디지털 상거래를 5년 더 빠르게 진행해 왔습니다. 문제 해결자에 의한 기술적 혁신은 우리가 일상 생활을 영위하는 방식을 근본적으로 변화시키고 있습니다. 이러한 기술 중심 변화는 의료계를 비롯한 우리 삶의 중요한 여러 측면을 정밀 검사할 것입니다.

의료는 향후 몇 년간 큰 변화를 겪을 것으로 기대됩니다. COVID는 최소한 몇 년 동안 업계를 선도할 의료 부문의 혁신을 가속화하고 있습니다. 이러한 변화의 핵심은 안정성을 저해하지 않으면서 보다 저렴하고, 사용 가능하며, 접근성이 뛰어난 펜데믹 취급에 있어 의료의 유연성을 높여야 한다는 것입니다.

이러한 의료 변화의 기초에는 잘 설계된 플랫폼이 있습니다. 플랫폼을 측정하는 주요 지표 중 하나는 플랫폼 변경 사항을 쉽게 구현할 수 있다는 것입니다. 속도가 새로운 규모이고 데이터 보호가 침해될 수 없습니다. 세계에서 가장 중요한 데이터 중 일부는 임상의를 지원하는 임상 시스템에서 생성 및 사용되고 있습니다. NetApp은 임상의가 필요로 하는 사내, 클라우드 또는 하이브리드 환경의 환자 치료를 위해 중요한 데이터를 제공하고 있습니다. 하이브리드 멀티 클라우드 환경은 IT 아키텍처를 위한 최신 상태입니다.

아시다시피 헬스케어는 공급자와 환자(의사, 간호사, 방사선 의사, 의료 기기 기술자 등)를 중심으로 돌아가고 있습니다. 환자와 공급자를 더 가까이 모을 때 지리적 위치를 단순한 데이터 포인트로 만드는 것이 공급자와 환자가 필요로 할 때 기반 플랫폼을 제공하는 것이 더 중요합니다. 플랫폼은 장기적인, 효율성과 비용 효율성을 모두 갖추고 있어야 합니다. 환자 진료 비용을 더 낮추려는 노력의 일환으로 "책임 관리 조직" (ACOS)는 효율적인 플랫폼을 통해 역량을 강화할 수 있습니다.

의료 조직에서 사용하는 의료 정보 시스템의 경우, 구축과 구매라는 질문에는 하나의 해답이 있습니다. 바로 구매입니다. 이는 주관적인 여러 가지 이유로 인해 발생할 수 있습니다. 수년 간 구매 결정을 내릴 경우 이기종 정보 시스템을 구축할 수 있습니다. 각 시스템에는 플랫폼에 구축된 특정 요구 사항이 있습니다. 가장 중요한 문제는 정보 시스템에 필요한 대용량의 다양한 스토리지 프로토콜과 성능 수준이 있기 때문에 플랫폼 표준화와 최적의 운영 효율성이 매우 중요한 문제로 나타납니다. 의료 조직에서는 다양한 기술과 SME 보유가 필요한 대규모 플랫폼 집합과 같은 사소한 운영 요구 사항에 따라 이러한 관심의 범위가 넓어지기 때문에 업무상 중요한 문제에 집중할 수 없습니다.

이러한 과제는 다음과 같은 범주로 분류할 수 있습니다.

- 이기종 스토리지 필요
- 부서 사일로
- IT 운영 복잡성
- 클라우드 연결
- 사이버 보안
- 인공 지능 및 딥 러닝

FlexPod를 사용하면 단일 플랫폼에서 FC, FCoE, iSCSI, NFS/pNFS, SMB/CIFS를 모두 지원할 수 있습니다. 인력, 프로세스 및 기술은 FlexPod가 설계하고 구축한 DNA의 일부입니다. FlexPod 적응형 QoS는 동일한 기본 FlexPod 플랫폼에서 여러 미션 크리티컬 임상 시스템을 지원하여 부서 사일로를 무너뜨릴 수 있도록 도와줍니다. FlexPod는 FedRAMP 인증 및 FIPS 140-2 인증을 받았습니다. 또한, 의료 조직에서는 인공 지능 및 딥 러닝과 같은 기회에 직면해 있습니다. FlexPod과 NetApp은 이러한 과제를 해결하고 표준화된 플랫폼에서 사내 또는 하이브리드 멀티 클라우드 설정에서 필요한 곳에 데이터를 제공합니다. 자세한 내용과 일련의 고객 성공 사례는 를 참조하십시오 "FlexPod 의료".

일반적인 의료 영상 정보 및 PACS 시스템에는 다음과 같은 기능이 있습니다.

- 리셉션 및 등록
- 스케줄링

- 이미징
- 전사
- 관리
- 데이터 교환
- 이미지 아카이브
- 임상의를 위한 이미지 캡처 및 읽기 기술 및 이미지 보기를 위한 이미지 보기

의료 부문은 영상 촬영과 관련하여 다음과 같은 임상적 과제를 해결하려고 노력하고 있습니다.

- 의 광범위한 채택 "자연어 처리" (NLP) - 이미지 판독을 위해 기술자 및 의사의 지원. 방사선 부서는 음성 인식 기능을 통해 보고서를 변환할 수 있습니다. NLP는 특히 DICOM 이미지에 포함된 DICOM 태그를 사용하여 환자 기록을 식별하고 익명화할 수 있습니다. NLP 기능을 사용하려면 이미지 처리 시 지연 시간이 짧은 고성능 플랫폼이 필요합니다. FlexPod QoS는 성능과 더불어 미래의 성장에 대비한 성숙한 용량 예측도 제공합니다.
- ACOS 및 지역 의료 기관의 표준화된 임상 경로 및 프로토콜 채택 확대 역사적으로 임상 경로는 임상 결정을 안내하는 통합 작업 흐름보다는 정적 지침 세트로 사용되었습니다. NLP 및 영상 처리 기능이 발전함에 따라 영상의 DICOM 태그를 임상 경로에 통합하여 임상 결정을 내릴 수 있습니다. 따라서 이러한 프로세스에는 기반 인프라 플랫폼 및 스토리지 시스템으로부터의 고성능, 낮은 지연 시간 및 높은 처리량이 필요합니다.
- 합성곱 신경망(convolutional neural networks)을 활용하는 ML 모델은 이미지 처리 기능을 실시간으로 자동화할 수 있으므로 GPU를 지원하는 인프라가 필요합니다. FlexPod는 동일한 시스템에 구축된 CPU와 GPU 컴퓨팅 구성요소를 모두 제공하며, CPU와 GPU를 독립적으로 확장할 수 있습니다.
- DICOM 태그가 임상 모범 사례 권고에서 사실로 사용되는 경우 시스템은 지연 시간이 짧고 처리량이 많은 DICOM 아티팩트를 더 많이 판독해야 합니다.
- 영상을 평가할 때 조직 전반에서 방사선 기사 간의 실시간 협업을 위해서는 최종 사용자 컴퓨팅 장치에서 고성능 그래픽 처리가 필요합니다. NetApp은 하이엔드 그래픽 사용 사례에 맞게 특별히 설계되고 검증된 업계 최고의 VDI 솔루션을 제공합니다. 자세한 내용은 을 참조하십시오 "여기".
- ACO 의료 기관의 이미지 및 미디어 관리는 의료 분야의 디지털 영상 및 통신( )과 같은 프로토콜을 사용하여 이미지의 기록 시스템에 관계없이 단일 플랫폼을 사용할 수 있습니다 "DICOM"DICOM 영구 객체("WADO")
- 건강 정보 교환("IE")에는 메시지에 포함된 이미지가 포함됩니다.
- 핸드헬드, 무선 스캔 장치(예: 휴대폰에 연결된 포켓 핸드헬드 초음파 스캐너)와 같은 모바일 기법에는 엣지, 코어 및 클라우드에서 DoD 수준의 보안, 안정성 및 지연 시간을 지원하는 강력한 네트워크 인프라가 필요합니다. "NetApp 구현 Data Fabric" 규모에 따라 확장 가능한 기능을 제공합니다.
- 최신 Modality는 저장 공간이 기하급수적으로 필요합니다. 예를 들어, CT 및 MRI는 각 Modality에 수백 MB를 필요로 하지만 디지털 병리학 영상(전체 슬라이드 영상 포함)은 크기가 몇 GB가 될 수 있습니다. FlexPod는 와 함께 "성능, 신뢰성 및 확장성을 기본 특성에 따라 제공합니다"설계되었습니다.

잘 설계된 의료 영상 시스템 플랫폼은 혁신의 핵심입니다. FlexPod 아키텍처는 업계 최고의 스토리지 효율성을 바탕으로 유연한 컴퓨팅 및 스토리지 기능을 제공합니다.

전반적인 솔루션 이점

의료 기관은 FlexPod 아키텍처 기반에서 이미징 애플리케이션 환경을 실행함으로써 직원 생산성이 향상되고 자본 및 운영 비용이 절감될 것으로 기대할 수 있습니다. FlexPod은 예측 가능한 짧은 지연 시간의 시스템 성능과 고가용성을 제공하도록 설계되고 설계된 엄격한 테스트를 거쳐 사전 검증된 통합형 솔루션을 제공합니다. 이러한 접근 방식은 의료 영상 시스템 사용자에게 높은 수준의 편안함을 제공하고 궁극적으로 최적의 응답 시간을 제공합니다.

이미징 시스템의 여러 구성 요소를 사용하려면 SMB/CIFS, NFS, ext4 또는 NTFS 파일 시스템에 데이터를 저장해야 할

수 있습니다. 이 요구사항은 인프라에서 NFS, SMB/CIFS 및 SAN 프로토콜을 통한 데이터 액세스를 제공해야 함을 의미합니다. 단일 NetApp 스토리지 시스템에서 NFS, SMB/CIFS 및 SAN 프로토콜을 지원할 수 있으므로 프로토콜별 스토리지 시스템에 대한 기존 관행이 필요하지 않습니다.

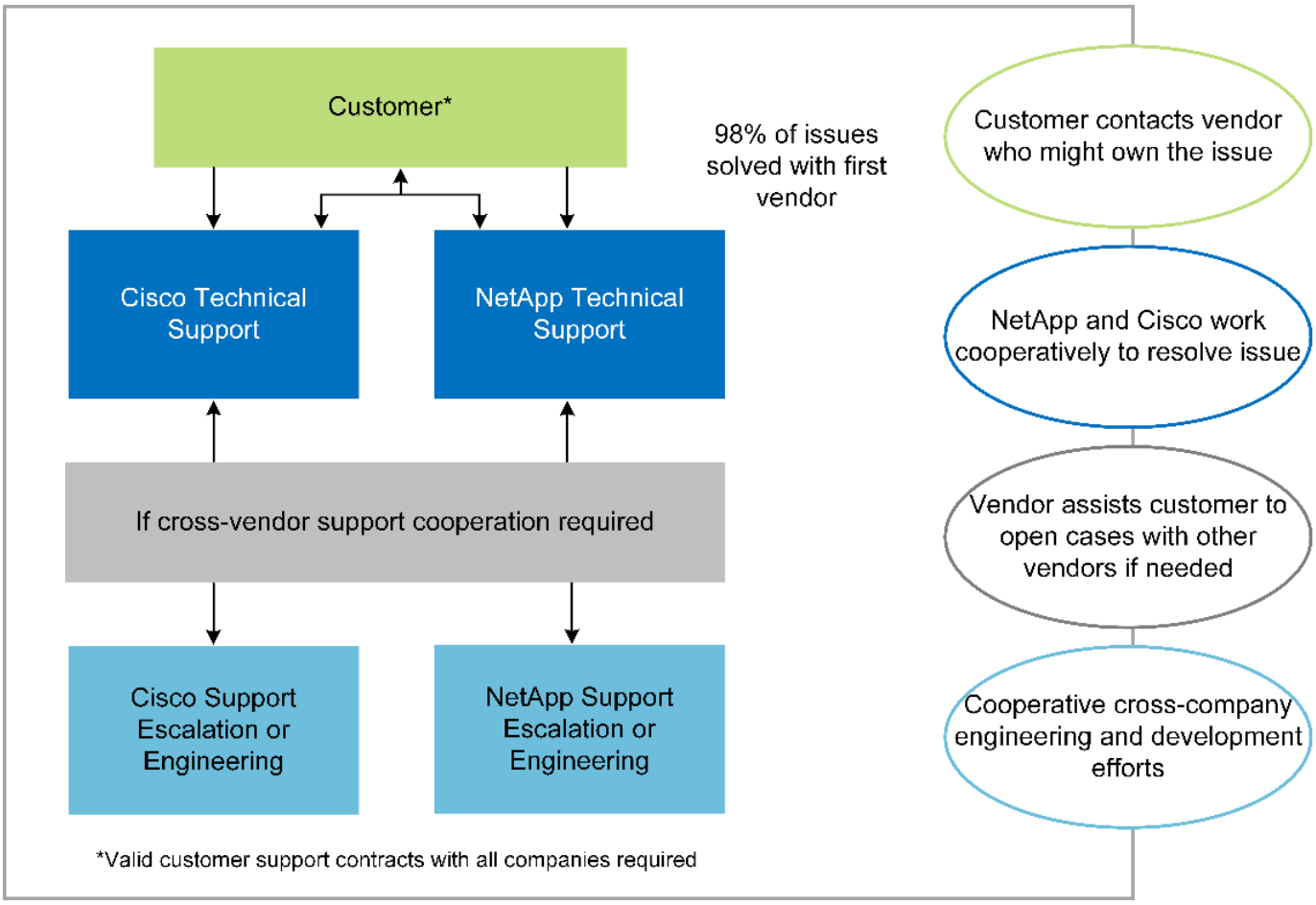
FlexPod 인프라는 모듈식, 통합, 가상화, 확장성(스케일아웃 및 스케일업), 비용 효율적인 플랫폼입니다. FlexPod 플랫폼을 사용하면 컴퓨팅, 네트워크, 스토리지를 독립적으로 확장하여 애플리케이션 구축을 가속할 수 있습니다. 모듈식 아키텍처를 사용하므로 시스템 스케일아웃 및 업그레이드 작업 중에도 무중단 운영이 가능합니다.

FlexPod는 의료 이미징 산업에 고유한 여러 가지 이점을 제공합니다.

- ?대기 시간이 낮은 시스템 성능.* 방사선과 전문의 시간은 고부가가치의 리소스이며 방사선과 의사의 시간을 효율적으로 사용하는 것이 가장 중요합니다. 이미지 또는 비디오가 로드되기를 기다린다면 임상의가 버너아웃할 수 있으며 청능사의 효율성 및 환자 안전에 영향을 줄 수 있습니다.
- * 모듈식 아키텍처 * FlexPod 구성요소는 클러스터 서버, 스토리지 관리 패브릭 및 통합 관리 툴셋을 통해 연결됩니다. 영상 촬영 시설이 매년 증가하고 연구 건수가 늘어날수록 그에 따라 기본 인프라를 확장해야 할 필요성이 커지게 됩니다. FlexPod는 컴퓨팅, 스토리지 및 네트워크를 독립적으로 확장할 수 있습니다.
- * 기존 데이터 센터든 원격지든 상관없이 의료 영상을 지원하는 FlexPod 데이터 센터의 통합 및 테스트 설계를 통해 적은 노력으로 새 인프라를 보다 빠르게 가동 및 실행할 수 있습니다.
- * 가속화된 애플리케이션 배포. * 사전 검증된 아키텍처는 모든 워크로드에 대한 구현 통합 시간과 위험을 줄이고 NetApp 기술은 인프라 구축을 자동화합니다. 의료 영상, 하드웨어 교체 또는 확장의 초기 롤아웃에 솔루션을 사용하는 경우, 프로젝트의 비즈니스 가치로 더 많은 리소스를 이동할 수 있습니다.
- * 운영 간소화 및 비용 절감. * 기존 독점 플랫폼을 워크로드의 동적 요구 사항을 충족할 수 있는 보다 효율적이고 확장 가능한 공유 리소스로 교체하여 비용 및 복잡성을 제거할 수 있습니다. 이 솔루션은 인프라 리소스 활용률을 높여 ROI(투자 수익률)를 높입니다.
- * 스케일아웃 아키텍처 * 실행 중인 애플리케이션을 재구성하지 않고도 SAN 및 NAS를 테라바이트에서 수십 페타바이트로 확장할 수 있습니다.
- 무중단 운영 * 비즈니스 중단 없이 스토리지 유지보수, 하드웨어 라이프사이클 운영, 소프트웨어 업그레이드를 수행할 수 있습니다.
- * 보안 멀티 테넌시. * 이 이점은 가상화된 서버 및 스토리지 공유 인프라의 증가하는 요구를 지원하여 특히 데이터베이스 및 소프트웨어의 여러 인스턴스를 호스팅하는 경우 시설별 정보의 안전한 멀티 테넌시를 가능하게 합니다.
- 풀링된 리소스 최적화 * 이 이점은 물리적 서버 및 스토리지 컨트롤러 수, 로드 밸런싱 워크로드 수요를 줄이고 활용률을 높이는 동시에 성능을 개선하는 데 도움이 됩니다.
- * QoS(서비스 품질). * FlexPod는 전체 스택에서 QoS를 제공합니다. 업계 최고 수준의 QoS 스토리지 정책을 통해 공유 환경에서 차별화된 서비스 수준을 실현할 수 있습니다. 이러한 정책은 워크로드에 맞게 성능을 최적화하고 급등하는 애플리케이션을 격리하고 제어하는 데 도움이 됩니다.
- * QoS를 사용하여 스토리지 계층 SLA 지원. * 일반적으로 의료 영상 환경에 필요한 다양한 스토리지 계층에 대해 서로 다른 스토리지 시스템을 구축할 필요가 없습니다. 여러 계층에 특정 QoS 정책을 사용하는 여러 NetApp FlexVol 볼륨이 있는 단일 스토리지 클러스터는 이러한 목적을 충족할 수 있습니다. 이러한 접근 방식을 통해 특정 스토리지 계층의 변화하는 요구사항을 동적으로 수용하여 스토리지 인프라를 공유할 수 있습니다. NetApp AFF는 FlexVol 볼륨 레벨에서 QoS를 지원하여 스토리지 계층에 대해 서로 다른 SLA를 지원할 수 있으므로, 애플리케이션의 스토리지 계층에 서로 다른 스토리지 시스템이 필요하지 않습니다.
- * 스토리지 효율성. * 의료 이미지는 일반적으로 이미지 응용 프로그램에서 2.5:1 정도 수준의 jpeg2k 무손실 압축으로 사전 압축됩니다. 그러나 이는 이미징 애플리케이션 및 공급업체에 따라 다릅니다. 1PB 이상의 대규모 이미징 애플리케이션 환경에서는 NetApp 스토리지 효율성 기능을 통해 스토리지를 5~10% 절약할 수 있으며 스토리지 비용도 줄일 수 있습니다. 이미징 애플리케이션 공급업체 및 NetApp 실무 전문가와 협력하여 의료 이미징 시스템에 잠재적인 스토리지 효율성을 제공합니다.

- * 민첩성 * FlexPod 시스템에서 제공하는 업계 최고의 워크플로우 자동화, 오케스트레이션 및 관리 툴을 통해 IT 팀은 비즈니스 요청에 훨씬 더 빠르게 대응할 수 있습니다. 이러한 비즈니스 요청에는 의료 영상 백업, 추가 테스트 및 교육 환경의 프로비저닝, 인구 건강 관리 이니셔티브를 위한 분석 데이터베이스 복제까지 다양합니다.
- * 더 높은 생산성 * 이 솔루션은 임상의의 최종 사용자 경험을 최적화하기 위해 신속하게 배포하고 확장할 수 있습니다.
- * Data Fabric. * NetApp이 제공하는 Data Fabric은 물리적 경계 및 애플리케이션 전반에 걸쳐 데이터를 제공합니다. NetApp이 제공하는 Data Fabric은 데이터 중심 세계에서 데이터 중심 기업을 위해 구축되었습니다. 데이터는 여러 위치에서 생성되고 사용되며 다른 위치, 애플리케이션 및 인프라와 활용되어 공유되어야 합니다. 그러므로 당신은 일관되고 통합된 방식으로 데이터를 관리하기를 원합니다. 이 솔루션을 사용하면 데이터를 관리할 수 있어 IT 팀이 끊임없이 증가하는 IT 복잡성을 단순하게 관리할 수 있습니다.
- * FabricPool. * NetApp ONTAP FabricPool를 사용하면 성능, 효율성, 보안, 보호를 그대로 유지하면서 스토리지 비용을 절감할 수 있습니다. FabricPool는 엔터프라이즈 애플리케이션에 투명하며, 애플리케이션 인프라를 재설계할 필요 없이 스토리지 TCO를 절감하여 클라우드 효율성을 사용합니다. FlexPod은 FabricPool의 스토리지 계층화 기능을 활용하여 ONTAP 플래시 스토리지를 더욱 효율적으로 사용할 수 있습니다. 자세한 내용은 를 참조하십시오 "FabricPool 및 FlexPod".
- * FlexPod 보안. * 보안은 FlexPod의 토대입니다. 지난 몇 년 동안 랜섬웨어는 심각하고 증가하는 위협이 되었습니다. 랜섬웨어는 암호화 바이러스, 암호화를 사용하여 악성 소프트웨어를 빌드하는 방법을 기반으로 하는 맬웨어입니다. 이 맬웨어는 대칭 키 암호화와 비대칭 키 암호화를 모두 사용하여 피해자의 데이터를 잠그고 데이터 암호를 해독할 키를 제공하는 대가로 금전을 요구합니다. FlexPod이 랜섬웨어와 같은 위협을 완화하는 데 어떤 도움이 되는지 알아보려면 을 참조하십시오. "랜섬웨어에 대한 솔루션" FlexPod 인프라 구성 요소는 연방 정보 처리 표준을 "제공합니다" 준수합니다.
- * FlexPod 공동 지원. * NetApp과 Cisco는 FlexPod 통합 인프라의 고유한 지원 요구사항을 충족하는 강력하고 확장 가능하며 유연한 지원 모델인 FlexPod 공동 지원을 확립했습니다. 이 모델은 NetApp과 Cisco의 경험, 리소스, 기술 지원 전문성을 합쳐 문제 영역에 관계없이, FlexPod 지원 문제를 식별하고 해결할 수 있는 효율적인 프로세스를 제공합니다. FlexPod 공동 지원 모델을 통해 FlexPod 시스템이 효율적으로 작동하고 최신 기술의 이점을 누리는지 확인하는 동시에, 통합 문제를 해결할 수 있는 숙련된 팀을 제공할 수 있습니다.

  FlexPod 공동 지원은 의료 조직에서 비즈니스 크리티컬 애플리케이션을 실행하는 경우에 특히 유용합니다. 아래 그림은 FlexPod 공동 지원 모델의 개요입니다.



범위

이 의료 영상 솔루션 호스팅을 위한 Cisco Unified Computing System(Cisco UCS) 및 NetApp ONTAP 기반 FlexPod 인프라의 기술 개요를 제공합니다.

대상

이 문서는 의료 산업의 기술 리더 및 Cisco와 NetApp 파트너 솔루션 엔지니어 및 프로페셔널 서비스 직원을 위한 것입니다. NetApp은 사용자가 컴퓨팅 및 스토리지 사이징 개념을 잘 이해하고 있을 뿐만 아니라 의료 이미지 시스템, Cisco UCS 및 NetApp 스토리지 시스템에 대한 기술적 지식을 갖추고 있다고 가정합니다.

의료 영상 응용 프로그램

일반적인 의료 영상 애플리케이션은 함께 중소, 중견 및 대형 의료 조직을 위한 엔터프라이즈급 이미징 솔루션을 만드는 일련의 애플리케이션을 제공합니다.

제품군의 핵심에는 다음과 같은 임상 기능이 있습니다.

- 엔터프라이즈 이미징 저장소
- 방사선학 및 심장학과 같은 기존 영상 소스를 지원합니다. 또한 안과학, 피부과, 대장내시경검사 및 사진 및 비디오와 같은 기타 의료 영상 촬영 분야도 지원합니다.
- "사진 보관 및 통신 시스템" (PACS) - 기존 방사선 필름의 역할을 대체하는 컴퓨터화된 수단입니다
- VNA(Enterprise Imaging Vendor Neutral Archive):

    - DICOM 및 비 DICOM 문서의 확장 가능한 통합
    - 중앙 의료 영상 시스템
    - 기업 내 여러(PACSs) 간의 문서 동기화 및 데이터 무결성 지원
    - 다음과 같은 문서 메타데이터를 활용하는 규칙 기반 전문가 시스템을 통한 문서 수명 주기 관리:
    - Modality type(양식 유형)
    - 연구 기간
    - 환자 나이(현재 및 이미지 캡처 시)
    - 기업 내부 및 외부(HIE)의 단일 통합 지점:
    - 상황 인식 문서 링크
    - Health Level Seven International(HL7), DICOM 및 WADO
    - 스토리지에 상관없는 아카이브 기능
- HL7 및 컨텍스트 인식 연결을 사용하는 다른 건강 정보 시스템과의 통합:
    - EHR은 환자 차트, 영상 작업 흐름 등의 환자 이미지에 대한 직접 링크를 구현할 수 있습니다.
    - 환자의 종방향 치료 영상 내역을 EHR에 포함시키는 데 도움이 됩니다.
- 방사선 기술사 워크플로
- 어떤 장치에서든 어디에서나 이미지를 볼 수 있는 엔터프라이즈 제로 풋프린트 뷰어입니다
- 후향적 및 실시간 데이터를 활용하는 분석 도구:
    - 규정 준수 보고
    - 운영 보고서
    - 품질 관리 및 품질 보증 보고서

의료 기관 및 플랫폼 사이즈의 크기

의료 기관은 ACO와 같은 프로그램을 지원하는 표준 기반 방법을 사용하여 광범위하게 분류할 수 있습니다. 이러한 분류 중 하나는 임상 통합 네트워크(CIN)의 개념을 사용합니다. 입증된 표준 임상 프로토콜 및 경로를 준수하여 의료 가치를 개선하고 환자 비용을 절감할 경우 병원 그룹을 CIN이라고 할 수 있습니다. CIN 내의 병원에서는 CIN의 핵심 가치를 따르는 온보드 의사에게 제어 및 관행이 마련되어 있습니다. 일반적으로 통합 전송 네트워크(IDN)는 병원 및 의사 그룹으로 제한되어 있습니다. CIN은 기존의 IDN 경계를 넘고 CIN은 여전히 ACO의 일부가 될 수 있습니다. CIN의 원칙에 따라 의료 기관은 중소, 중견, 대형으로 분류할 수 있습니다.

소규모 의료 기관

의료 기관은 외래 클리닉과 외래 진료실이 있는 단일 병원만 포함하지만 CIN에는 속하지 않는 소규모 의료 기관입니다. 의사는 간병인 업무를 수행하고 치료 연속체 동안 환자 치료를 조정합니다. 이러한 소규모 조직에는 일반적으로 의사가 운영하는 시설이 포함됩니다. 환자를 위한 통합 치료로 응급 및 외상 치료를 제공할 수도 있고 제공하지 않을 수도 있습니다. 일반적으로 소규모 의료 기관은 연간 약 250,000건의 임상 이미징 연구를 수행합니다. 이미징 센터는 소규모 의료 조직으로 간주되며 이미징 서비스를 제공합니다. 일부 조직은 다른 조직에 방사선 구술 서비스를 제공합니다.

중간 규모의 의료 기관

다음과 같이 집중적인 조직이 있는 여러 병원 시스템이 포함된 경우 중간 규모의 의료 기관으로 간주됩니다.

- 성인 진료 클리닉 및 성인 입원 환자 병원
- 노동 및 배달 부서
- 육아 클리닉 및 아동 입원 병원
- 암 치료 센터
- 성인 응급실
- 어린이 응급 부서
- 가족 의학과 1차 진료소
- 성인 외상 치료 센터
- 아동 외상 치료 센터

중간 규모의 의료 기관에서는 의사가 CIN의 원칙을 따르고 단일 단위로 작동합니다. 병원에서는 병원, 의사, 약국 청구 기능이 분리되어 있습니다. 병원은 학술 연구 기관과 연계될 수 있으며 중재적 임상 연구 및 임상시험을 수행할 수 있습니다. 중간 규모의 의료 기관은 연간 최대 500,000건의 임상 이미징 연구를 수행합니다.

대규모 의료 기관

중간 규모의 의료 조직의 특성을 포함하고 여러 지리적 위치에 있는 커뮤니티에 중간 규모의 임상 기능을 제공하는 의료 조직은 규모가 큰 것으로 간주됩니다.

대규모 의료 기관은 일반적으로 다음과 같은 기능을 수행합니다.

- 중앙 사무실을 통해 전체 기능을 관리합니다
- 다른 병원과 합작 벤처에 참여하고 있습니다
- 지불인 조직과 연간 요금을 협상합니다
- 주 및 지역별로 지급인 요금을 협상합니다
- MU(Meaningful Use) 프로그램에 참여합니다
- 표준 기반 PSM(Population Health Management) 도구를 사용하여 인구 건강 코호트에 대한 고급 임상 연구를 수행합니다
- 연간 최대 100만 건의 임상 이미징 연구를 수행합니다

CIN에 참여하는 일부 대규모 의료 기관에는 AI 기반 이미징 판독 기능도 있습니다. 이러한 조직은 일반적으로 연간 1백만 에서 2백만 건의 임상 이미징 연구를 수행합니다.

이러한 다양한 규모의 조직이 최적의 크기의 FlexPod 시스템으로 어떻게 변환되는지 살펴보기 전에 FlexPod 시스템의 다양한 FlexPod 구성 요소와 다양한 기능을 이해해야 합니다.

FlexPod

Cisco Unified Computing System

Cisco UCS는 통합 I/O 인프라와 상호 연결되는 단일 관리 도메인으로 구성됩니다. 의료 영상 환경을 위한 Cisco UCS는 NetApp 의료 영상 시스템 인프라 권장사항 및 모범 사례와 일치하도록 조정되었으므로 인프라는 중요 환자 정보를 최대 가용성으로 제공할 수 있습니다.

엔터프라이즈 의료 이미징의 컴퓨팅 기반은 Cisco UCS 기술로서 통합 시스템 관리, 인텔 제온 프로세서 및 서버 가상화를 갖추고 있습니다. 이러한 통합 기술은 데이터 센터 문제를 해결하고 일반적인 의료 영상 시스템을 통해 데이터

센터 설계 목표를 달성할 수 있도록 지원합니다. Cisco UCS는 LAN, SAN 및 시스템 관리를 랙 서버, 블레이드 서버 및 가상 머신(VM)을 위한 하나의 간소화된 링크로 통합합니다. Cisco UCS는 단일 관리 지점과 모든 I/O 트래픽에 단일 제어 지점을 제공하는 이중 Cisco UCS 패브릭 인터커넥트 쌍으로 구성됩니다.

Cisco UCS는 서비스 프로필을 사용하여 Cisco UCS 인프라의 가상 서버를 올바르고 일관되게 구성할 수 있습니다. 서비스 프로필에는 LAN 및 SAN 주소 지정, I/O 구성, 펌웨어 버전, 부팅 순서, 네트워크 가상 LAN(VLAN), 물리적 포트 및 QoS 정책과 같은 서버 ID에 대한 중요한 서버 정보가 포함됩니다. 서비스 프로필은 몇 시간 또는 며칠이 아니라 몇 분 내에 동적으로 생성하고 시스템의 모든 물리적 서버와 연결할 수 있습니다. 물리적 서버와 서비스 프로필을 연결하는 작업은 물리적 구성 변경 없이 환경의 서버 간에 ID를 마이그레이션할 수 있는 간단한 단일 작업으로 수행됩니다. 또한 장애가 발생한 서버의 교체를 신속하게 베어 메탈 프로비저닝할 수 있습니다.

서비스 프로필을 사용하면 기업 전체에서 서버가 일관성 있게 구성되었는지 확인할 수 있습니다. Cisco UCS Central은 여러 Cisco UCS 관리 도메인을 사용할 때 글로벌 서비스 프로필을 사용하여 도메인 전체에서 구성 및 정책 정보를 동기화할 수 있습니다. 유지 관리를 한 도메인에서 수행해야 하는 경우 가상 인프라를 다른 도메인으로 마이그레이션할 수 있습니다. 이 접근 방식을 사용하면 단일 도메인이 오프라인일 때도 애플리케이션이 고가용성을 통해 계속 실행됩니다.

Cisco UCS는 블레이드 및 랙 서버 컴퓨팅을 위한 차세대 솔루션입니다. 이 시스템은 지연 시간이 짧은 무손실 40GbE 통합 네트워크 패브릭을 엔터프라이즈급 x86 아키텍처 서버와 통합합니다. 이 시스템은 모든 리소스가 통합된 관리 도메인에 참여하는 확장 가능한 통합 다중 섀시 플랫폼입니다. Cisco UCS는 가상화 시스템과 비가상화 시스템 모두에 대한 엔드 투 엔드 프로비저닝 및 마이그레이션 지원을 통해 간단하고 안정적이며 안전하게 새로운 서비스를 제공할 수 있도록 지원합니다. Cisco UCS는 다음과 같은 기능을 제공합니다.

- 종합적인 관리
- 근본적인 단순화
- 고성능

Cisco UCS는 다음 요소로 구성됩니다.

- * 컴퓨팅. * 이 시스템은 완전히 새로운 차원의 컴퓨팅 시스템을 기반으로 하며 인텔 제온 스케일러블 프로세서 제품군 기반의 랙 마운트 및 블레이드 서버를 통합합니다.
- * 네트워크. * 이 시스템은 지연 시간이 짧은 무손실 40Gbps 통합 네트워크 패브릭으로 통합됩니다. 이 네트워크 기반은 오늘날 별도의 네트워크인 LAN, SAN 및 고성능 컴퓨팅 네트워크를 통합합니다. 통합 패브릭은 네트워크 어댑터, 스위치 및 케이블의 수를 줄이고 전력 및 냉각 요구 사항을 줄여 비용을 절감합니다.
- 가상화 *. * 이 시스템은 가상 환경의 확장성, 성능 및 운영 제어 능력을 강화하여 가상화의 잠재력을 최대한 활용합니다. Cisco 보안, 정책 적용 및 진단 기능이 이제 가상화 환경으로 확장되어 변화하는 비즈니스 및 IT 요구 사항을 보다 효과적으로 지원할 수 있습니다.
- * 스토리지 액세스. * 이 시스템은 통합 패브릭을 통해 SAN 스토리지와 NAS에 대한 통합 액세스를 제공합니다. 또한 소프트웨어 정의 스토리지에 이상적인 시스템입니다. 단일 프레임워크에서 얻은 이점을 활용하여 단일 창에서 컴퓨팅과 스토리지 서버를 모두 관리하므로, 시스템에 I/O 임계치를 조절해야 하는 경우 QoS를 구현할 수 있습니다. 또한 서버 관리자는 스토리지 리소스에 스토리지 액세스 정책을 미리 할당하여 스토리지 연결 및 관리를 간소화하고 생산성을 높일 수 있습니다. 외부 스토리지 외에도 랙 서버와 블레이드 서버 모두 내장 하드웨어 RAID 컨트롤러를 통해 액세스할 수 있는 내부 스토리지가 있습니다. Cisco UCS Manager에서 스토리지 프로필 및 디스크 구성 정책을 설정하면 호스트 OS와 애플리케이션 데이터의 스토리지 요구사항이 사용자 정의 RAID 그룹에 의해 충족됩니다. 결과적으로 가용성이 향상되고 성능이 향상됩니다.
- * 관리. * 이 시스템은 모든 시스템 구성요소를 고유한 방식으로 통합하여 전체 솔루션을 Cisco UCS Manager를 통해 단일 엔터티로 관리할 수 있도록 합니다. 모든 시스템 구성 및 운영을 관리하기 위해 Cisco UCS Manager는 직관적인 GUI, CLI, 강력한 API를 기반으로 구축된 Microsoft Windows PowerShell용 강력한 스크립팅 라이브러리 모듈을 제공합니다.

Cisco Unified Computing System은 액세스 계층 네트워킹 및 서버를 융합합니다. 이 고성능 차세대 서버 시스템은

데이터 센터에 높은 수준의 워크로드 민첩성 및 확장성을 제공합니다.

Cisco UCS Manager를 참조하십시오

Cisco UCS Manager에는 Cisco UCS의 모든 소프트웨어 및 하드웨어 구성요소를 통합 관리할 수 있는 기능이 내장되어 있습니다. UCS Manager는 단일 연결 기술을 사용하여 수천 개의 VM에 대한 여러 섀시를 관리, 제어 및 관리합니다. 관리자는 직관적인 GUI, CLI 또는 XML API를 통해 소프트웨어를 사용하여 전체 Cisco UCS를 단일 논리 엔터티로 관리합니다. Cisco UCS Manager는 고가용성을 위해 클러스터된 액티브-대기 구성을 사용하는 Cisco UCS 6300 Series 패브릭 인터커넥트 쌍에 상주합니다.

Cisco UCS Manager는 서버, 네트워크, 스토리지를 통합하는 통합 내장 관리 인터페이스를 제공합니다. Cisco UCS Manager는 자동 검색을 수행하여 의 인벤토리를 감지하고 관리하며 추가하거나 변경하는 시스템 구성 요소를 프로비저닝합니다. 타사 통합을 위한 포괄적인 XML API 세트를 제공하며 9,000개의 통합 지점을 노출합니다. 또한 자동화를 위한 맞춤형 개발, 오케스트레이션을 지원하고 새로운 차원의 시스템 가시성과 제어 기능을 제공합니다.

서비스 프로필은 가상화 환경과 비가상화 환경 모두에 이점을 제공합니다. 서버 간에 워크로드를 이동하거나 서비스를 위해 서버를 오프라인으로 전환하는 등 가상화되지 않은 서버의 이동성을 높여줍니다. 또한 가상화 클러스터와 프로필을 함께 사용하여 새로운 리소스를 온라인으로 쉽게 가져올 수 있으며 기존 VM 이동성을 보완할 수 있습니다.

Cisco UCS Manager에 대한 자세한 내용은 를 참조하십시오 "Cisco UCS Manager 제품 페이지".

Cisco UCS 차별화 요소

Cisco Unified Computing System은 데이터 센터에서 서버를 관리하는 방식을 획기적으로 바꾸고 있습니다. Cisco UCS 및 Cisco UCS Manager의 고유한 차별화 요소를 참조하십시오.

- * 내장된 관리. * Cisco UCS에서 서버는 패브릭 상호 연결에 포함된 펌웨어에 의해 관리되므로 외부 물리적 또는 가상 장치를 관리할 필요가 없습니다.
- * 통합 패브릭. * 블레이드 서버 섀시 또는 랙 서버에서 패브릭 상호 연결까지 Cisco UCS에서는 LAN, SAN 및 관리 트래픽에 단일 이더넷 케이블이 사용됩니다. 이 통합 I/O를 통해 필요한 케이블, SFP, 어댑터의 수가 감소되어 전체 솔루션의 자본 및 운영 비용이 절감됩니다.
- * 자동 검색. * 섀시에 블레이드 서버를 삽입하거나 패브릭 상호 연결에 랙 서버를 연결하기만 하면 관리 작업 없이 컴퓨팅 리소스의 검색 및 인벤토리가 자동으로 수행됩니다. 통합 패브릭과 자동 검색을 결합하여 Cisco UCS의 전선회 아키텍처를 지원하며, 이 아키텍처의 컴퓨팅 기능을 손쉽게 확장할 수 있을 뿐만 아니라 기존 외부 LAN, SAN 및 관리 네트워크에 대한 연결도 유지할 수 있습니다.
- * 정책 기반 리소스 분류. * Cisco UCS Manager에서 컴퓨팅 리소스를 검색할 때 정의한 정책에 따라 지정된 리소스 풀로 자동으로 분류될 수 있습니다. 이 기능은 멀티테넌트 클라우드 컴퓨팅에 유용합니다.
- * 결합된 랙 및 블레이드 서버 관리 * Cisco UCS Manager는 동일한 Cisco UCS 도메인 하에서 B-Series 블레이드 서버 및 C-Series 랙 서버를 관리할 수 있습니다. 이 기능은 상태 비저장 컴퓨팅과 함께 컴퓨팅 리소스를 하드웨어 폼 팩터에 종속되지 않습니다.
- * 모델 기반 관리 아키텍처 * Cisco UCS Manager 아키텍처 및 관리 데이터베이스는 모델 기반 및 데이터 기반입니다. 관리 모델에서 작동하도록 제공되는 개방형 XML API를 통해 Cisco UCS Manager를 다른 관리 시스템과 쉽고 확장 가능한 통합할 수 있습니다.
- * 정책, 풀 및 템플릿 * Cisco UCS Manager의 관리 방식은 복잡한 구성 대신 정의된 정책, 풀 및 템플릿을 기반으로 합니다. 컴퓨팅, 네트워크 및 스토리지 리소스를 관리하기 위한 간단하고 느슨하게 결합된 데이터 기반 접근 방식을 사용할 수 있습니다.
- * 느슨한 참조 무결성 * Cisco UCS Manager에서 서비스 프로필, 포트 프로필 또는 정책은 다른 정책 또는 참조 무결성이 느슨한 다른 논리적 리소스를 참조할 수 있습니다. 참조 정책은 참조 정책을 작성할 때 존재할 수 없지만 다른 정책이 참조하는 경우에도 참조 정책을 삭제할 수 있습니다. 이 기능을 사용하면 서로 다른 실무 전문가가 독립적으로 작업할 수 있습니다. 네트워크, 스토리지, 보안, 서버, 가상화 등 다양한 도메인의 다양한 전문가가 함께

작업하여 복잡한 작업을 수행할 수 있도록 함으로써 뛰어난 유연성을 얻을 수 있습니다.

- * 정책 해결. * Cisco UCS Manager에서는 실제 테넌트 및 조직 관계를 모방하는 조직 단위 계층 구조의 트리 구조를 만들 수 있습니다. 조직 계층 구조의 다양한 수준에서 다양한 정책, 풀 및 템플릿을 정의할 수 있습니다. 이름으로 다른 정책을 참조하는 정책은 가장 가까운 정책 일치를 갖는 조직 계층에서 확인됩니다. 루트 조직의 계층 구조에서 특정 이름의 정책이 발견되지 않으면 "default"라는 특수 정책이 검색됩니다. 이 정책 해결 방법은 자동화하기 쉬운 관리 API를 구현하고 다양한 조직의 소유자에게 뛰어난 유연성을 제공합니다.
- * 서비스 프로파일 및 상태 비저장 컴퓨팅. * 서비스 프로필은 다양한 ID와 정책을 전달하는 서버의 논리적 표현입니다. 이 논리 서버는 리소스 요구 사항을 충족하는 한 모든 물리적 컴퓨팅 리소스에 할당할 수 있습니다. 상태 비저장 컴퓨팅을 사용하면 서버를 몇 분 이내에 조달할 수 있으며, 이전에는 기존 서버 관리 시스템에서 며칠이 소요되었습니다.
- * 내장된 멀티 테넌시 지원 * 정책, 풀, 템플릿, 느슨한 참조 무결성, 조직 계층 구조의 정책 해상도, 컴퓨팅 리소스에 대한 서비스 프로필 기반 접근 방식을 통해 Cisco UCS Manager는 프라이빗 클라우드와 퍼블릭 클라우드에서 일반적으로 관찰되는 멀티 테넌트 환경에 기본적으로 적합합니다.
- * 확장 메모리. * 엔터프라이즈급 Cisco UCS B200 M5 블레이드 서버는 절반 너비 블레이드 폼 팩터로 Cisco Unified Computing System 포트폴리오의 기능을 확장합니다. Cisco UCS B200 M5는 최대 3TB의 RAM으로 최신 Intel Xeon 확장형 프로세서 CPU의 성능을 활용합니다. 이 기능을 사용하면 많은 구축에 필요하거나 특정 아키텍처에서 빅 데이터와 같은 대규모 메모리 작업을 지원하는 데 필요한 VM 대 물리적 서버 비율을 크게 실현할 수 있습니다.
- * 가상화 인식 네트워크 * Cisco Virtual Machine Fabric Extender(VM-FEX) 기술을 사용하면 액세스 네트워크 계층에서 호스트 가상화를 인식할 수 있습니다. 이러한 인식은 네트워크 관리자 팀이 정의하는 포트 프로필을 통해 가상 네트워크를 관리할 때 가상화로 인해 컴퓨팅 및 네트워크 도메인이 오염되는 것을 방지합니다. VM-FEX는 하드웨어에서 스위칭을 수행하여 하이퍼바이저 CPU를 오프로드하므로 하이퍼바이저 CPU가 더 많은 가상화 관련 작업을 수행할 수 있습니다. 클라우드 관리를 단순화하기 위해 VM-FEX 기술은 VMware vCenter, Linux KVM(커널 기반 가상 머신) 및 Microsoft Hyper-V SR-IOV와 완벽하게 통합됩니다.
- * 간소화된 QoS. * FC와 이더넷이 Cisco UCS에 내장되어 있음에도 불구하고 QoS 및 무손실 이더넷을 기본적으로 지원하므로 원활하게 사용할 수 있습니다. 하나의 GUI 패널에 모든 시스템 클래스를 표현함으로써 Cisco UCS Manager에서 네트워크 QoS를 단순화합니다.

Cisco Nexus IP 및 MDS 스위치

Cisco Nexus 스위치 및 Cisco MDS 다계층 디렉터는 엔터프라이즈급 연결 및 SAN 통합을 제공합니다. Cisco 멀티 프로토콜 스토리지 네트워킹은 FC, FICON(Fibre Connection), FCoE(FC over Ethernet), iSCSI, FCIP(FC over IP)와 같은 유연성과 옵션을 제공하여 비즈니스 위험을 줄여줍니다.

Cisco Nexus 스위치는 단일 플랫폼에서 가장 포괄적인 데이터 센터 네트워크 기능 세트 중 하나를 제공합니다. 데이터 센터와 캠퍼스 코어 모두를 위한 높은 성능과 밀도를 제공합니다. 또한 복원력이 뛰어난 모듈식 플랫폼에서 데이터 센터 통합, 행 종료 및 데이터 센터 인터커넥트 구축을 위한 전체 기능 세트를 제공합니다.

Cisco UCS는 컴퓨팅 리소스를 Cisco Nexus 스위치 및 통합 패브릭과 통합하여 다양한 유형의 네트워크 트래픽을 식별 및 처리합니다. 이러한 트래픽에는 스토리지 I/O, 스트림되는 데스크톱 트래픽, 관리 및 임상 및 비즈니스 애플리케이션에 대한 액세스가 포함됩니다. 다음과 같은 기능을 이용할 수 있습니다.

- * 인프라 확장성 * 가상화, 효율적인 전력 및 냉각, 자동화, 고밀도 및 성능으로 클라우드 확장이 모두 효율적인 데이터 센터 성장을 지원합니다.
- * 운영 연속성. * 이 설계에는 하드웨어, Cisco NX-OS 소프트웨어 기능 및 관리가 통합되어 다운타임이 없는 환경을 지원합니다.
- * 전송 유연성. * 이 비용 효율적인 솔루션을 통해 새로운 네트워킹 기술을 점진적으로 채택할 수 있습니다.

Cisco UCS와 Cisco Nexus 스위치, MDS 멀티레이어 디렉터는 엔터프라이즈 의료 이미지 처리 시스템을 위한 컴퓨팅,

네트워킹 및 SAN 연결 솔루션을 제공합니다.

NetApp All-Flash 스토리지를 활용할 수 있습니다

ONTAP 소프트웨어를 실행하는 NetApp 스토리지는 의료 이미지 처리 시스템 워크로드에 필요한 짧은 지연 시간의 읽기 및 쓰기 응답 시간과 높은 IOPS를 제공하면서 전체 스토리지 비용을 줄여줍니다. 일반적인 의료 영상 시스템 요구사항을 충족하는 최적의 스토리지 시스템을 구축할 수 있도록 ONTAP은 All-Flash 및 하이브리드 스토리지 구성을 모두 지원합니다. NetApp 플래시 스토리지는 고성능 및 응답 시간의 주요 구성 요소를 제공하여 지연 시간에 민감한 의료 이미지 시스템 작업을 지원하는 의료 이미지 시스템 고객에게 제공합니다. 또한 단일 클러스터에서 여러 개의 장애 도메인을 생성하여 운영 환경을 비운영 환경과 격리할 수 있습니다. 또한, NetApp은 ONTAP 최소 QoS가 적용되는 워크로드에 대해 시스템 성능이 특정 수준 이하로 떨어지지 않도록 보장하여 시스템의 성능 문제를 줄입니다.

ONTAP 소프트웨어의 스케일아웃 아키텍처는 다양한 I/O 워크로드에 유연하게 대응할 수 있습니다. 임상 애플리케이션에 필요한 처리량과 짧은 지연 시간을 제공하고 모듈식 스케일아웃 아키텍처를 제공하기 위해 All-Flash 구성은 일반적으로 ONTAP 아키텍처에서 사용됩니다. NetApp AFF 노드를 하이브리드(HDD 및 플래시) 스토리지 노드와 동일한 스케일아웃 클러스터에 결합할 수 있으며, 처리량이 많은 대규모 데이터 세트를 저장하는 데 적합합니다. 의료 이미징 시스템 환경을 값비싼 SSD 스토리지에서 다른 노드의 보다 경제적인 HDD 스토리지로 복제, 복제 및 백업할 수 있습니다. NetApp 클라우드 지원 스토리지와 NetApp에서 제공하는 Data Fabric을 사용하면 사내 또는 클라우드의 오브젝트 스토리지에 백업할 수 있습니다.

의료 영상 촬영의 경우, ONTAP는 대부분의 주요 의료 영상 시스템에서 검증을 거쳤습니다. 즉, 의료 영상 촬영을 위한 빠르고 안정적인 성능을 제공하도록 테스트를 거쳤습니다. 또한 다음 기능을 사용하면 관리를 단순화하고, 가용성과 자동화를 늘리고, 필요한 총 스토리지 양을 줄일 수 있습니다.

- * 탁월한 성능 * NetApp AFF 솔루션은 동일한 유니파이드 스토리지 아키텍처, ONTAP 소프트웨어, 관리 인터페이스, 다양한 데이터 서비스 및 고급 기능 세트를 NetApp FAS 제품군의 나머지 제품과 공유합니다. 혁신적인 All-Flash 미디어와 ONTAP을 결합하여 업계 최고의 ONTAP 소프트웨어를 통해 All-Flash 스토리지의 높은 IOPS와 일관되게 낮은 지연 시간을 확보할 수 있습니다.
- * 스토리지 효율성. * NetApp SME와 함께 전체 용량 요구사항을 줄여 특정 의료 영상 시스템이 어떻게 적용되는지 이해할 수 있습니다.
- * 공간 효율적인 클론 복제. * FlexClone 기능을 사용하면 시스템에서 클론을 거의 즉시 생성하여 백업 및 테스트 환경 업데이트를 지원할 수 있습니다. 이러한 클론은 변경된 경우에만 추가 스토리지를 사용합니다.
- * 통합 데이터 보호. * 완벽한 데이터 보호 및 재해 복구 기능을 통해 중요 데이터 자산을 보호하고 재해 복구를 제공할 수 있습니다.
- 무중단 운영 * 데이터를 오프라인으로 전환하지 않고도 업그레이드와 유지보수를 수행할 수 있습니다.
- * QoS. * 스토리지 QoS를 통해 잠재적인 대규모 워크로드를 제한할 수 있습니다. 더 중요한 것은, QoS는 의료 영상 시스템의 생산 환경과 같은 중요한 작업 부하에 대해 시스템 성능이 특정 수준 이하로 떨어지지 않도록 최소 성능 보장을 제공하는 것입니다. 또한 경합을 제한하여 NetApp QoS로 성능 관련 문제도 줄일 수 있습니다.
- * Data Fabric. * 디지털 혁신을 가속하기 위해 NetApp에서 제공하는 Data Fabric은 클라우드 및 사내 환경에서 데이터 관리를 단순화하고 통합합니다. 우수한 데이터 가시성 및 통찰력, 데이터 액세스 및 제어, 데이터 보호 및 보안을 위해 일관되고 통합된 데이터 관리 서비스 및 애플리케이션을 제공합니다. NetApp은 AWS, Azure, Google Cloud 및 IBM Cloud와 같은 대규모 퍼블릭 클라우드와 통합되어 폭넓은 선택의 기회를 제공합니다.

호스트 가상화 **- VMware vSphere**

FlexPod 아키텍처는 업계 최고의 가상화 플랫폼인 VMware vSphere 6.x에서 검증되었습니다. VMware ESXi 6.x는 VM을 구축하고 실행하는 데 사용됩니다. vCenter Server Appliance 6.x는 ESXi 호스트 및 VM을 관리하는 데 사용됩니다. Cisco UCS B200 M5 블레이드에서 실행되는 여러 ESXi 호스트가 VMware ESXi 클러스터를 구성하는 데 사용됩니다. VMware ESXi 클러스터는 모든 클러스터 노드에서 컴퓨팅, 메모리 및 네트워크 리소스를 풀링하며 클러스터에서 실행 중인 VM에 대한 복구 성능을 갖춘 플랫폼을 제공합니다. VMware ESXi 클러스터 기능, vSphere

고가용성 및 DRS(Distributed Resource Scheduler)는 모두 vSphere 클러스터의 허용 범위를 활용하여 장애를 방지하며 VMware ESXi 호스트에 리소스를 분산시킵니다.

NetApp 스토리지 플러그인 및 Cisco UCS 플러그인은 VMware vCenter와 통합되어 필요한 스토리지 및 컴퓨팅 리소스에 대한 운영 워크플로우를 지원합니다.

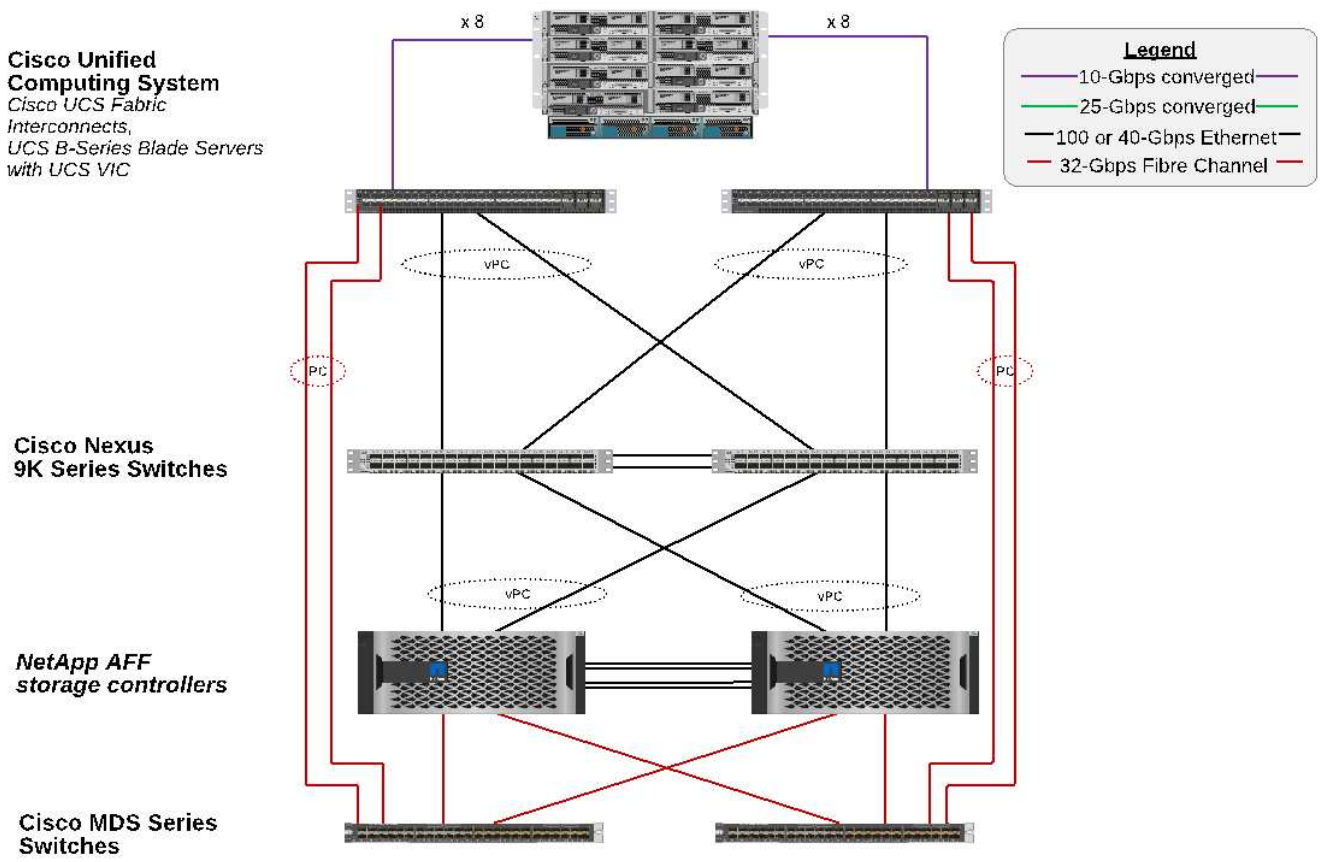
VMware ESXi 클러스터와 vCenter Server는 VM에 의료 이미지 환경을 구축하기 위한 중앙 집중식 플랫폼을 제공합니다. 의료 조직에서는 다음과 같이 업계 최고의 가상 인프라를 안심하고 활용할 수 있습니다.

- * 간단한 구축. * 가상 어플라이언스를 사용하여 vCenter Server를 빠르고 쉽게 구축할 수 있습니다.
- * 중앙 집중식 제어 및 가시성 * 단일 위치에서 전체 vSphere 인프라스트럭처를 관리합니다.
- * 사전 최적화. * 최대 효율성을 위해 리소스를 할당, 최적화 및 마이그레이션합니다.
- * 관리. * 강력한 플러그인과 도구를 사용하여 관리를 단순화하고 제어를 확장합니다.

있습니다

FlexPod 아키텍처는 전체 컴퓨팅, 네트워크 및 스토리지 스택에서 구성 요소 또는 링크에 장애가 발생할 경우 고가용성을 제공하도록 설계되었습니다. 클라이언트 액세스 및 스토리지 액세스를 위한 다중 네트워크 경로는 로드 밸런싱과 최적의 리소스 사용률을 제공합니다.

다음 그림은 의료 영상 시스템 솔루션 구축을 위한 16Gb FC/40Gb 이더넷(40GbE) 토폴로지를 보여줍니다.



스토리지 아키텍처

이 섹션의 스토리지 아키텍처 지침을 사용하여 엔터프라이즈 의료 영상 시스템용 스토리지 인프라를 구성합니다.

제공합니다

일반적인 기업 의료 영상 환경은 여러 가지 스토리지 계층으로 구성됩니다. 각 계층에는 특정 성능 및 스토리지 프로토콜 요구사항이 있습니다. NetApp 스토리지는 다양한 RAID 기술을 지원합니다. 자세한 내용은 섹션을 참조하십시오 "여기". 다음은 NetApp AFF 스토리지 시스템이 이미징 시스템에 다양한 스토리지 계층의 요구사항을 지원하는 방법입니다.

- * 성능 스토리지(계층 1). * 이 계층은 데이터베이스, OS 드라이브, VMware VMFS(Virtual Machine File System) 데이터 저장소 등을 위한 고성능 및 높은 중복성을 제공합니다. 블록 I/O는 ONTAP에 구성된 것처럼 파이버 케이블을 통해 SSD의 공유 스토리지 어레이로 이동합니다. 최소 지연 시간은 1ms~3ms이며 가끔 최대 5ms입니다. 이 저장 계층은 일반적으로 단기 저장 캐시에 사용되며, 일반적으로 온라인 DICOM 이미지에 대한 빠른 액세스를 위해 6 ~ 12개월의 이미지 저장 공간이 사용됩니다. 이 계층은 이미지 캐시, 데이터베이스 백업 등에 고성능 및 높은 중복성을 제공합니다. NetApp All-Flash 어레이는 지속적인 대역폭에서 1ms 미만의 지연 시간을 제공하며, 이는 일반적인 엔터프라이즈 의료 영상 환경에서 예상되는 서비스 시간보다 훨씬 짧습니다. NetApp ONTAP는 RAID-TEC(3중 패리티 RAID로 3개 디스크 장애 유지) 및 RAID DP(2개 디스크 장애를 지원하는 이중 패리티 RAID)를 모두 지원합니다.
- * 아카이브 스토리지(계층 2). * 이 계층은 일반적인 비용 최적화 파일 액세스, 대용량 볼륨용 RAID 5 또는 RAID 6 스토리지, 장기간 저비용/성능 아카이빙에 사용됩니다. NetApp ONTAP는 RAID-TEC(3중 패리티 RAID로 3개 디스크 장애 유지) 및 RAID DP(2개 디스크 장애를 지원하는 이중 패리티 RAID)를 모두 지원합니다. FlexPod의

NetApp FAS는 NFS/SMB를 통해 SAS 디스크 어레이에 대한 이미징 애플리케이션 I/O를 지원합니다. NetApp FAS 시스템은 지속적인 대역폭에서 최대 10ms의 지연 시간을 제공하며, 이는 엔터프라이즈 의료 영상 시스템 환경에서 스토리지 계층 2에 필요한 서비스 시간보다 훨씬 짧습니다.

하이브리드 클라우드 환경의 클라우드 기반 아카이빙은 S3 또는 유사 프로토콜을 사용하는 퍼블릭 클라우드 스토리지 공급업체에 아카이빙하는 데 사용할 수 있습니다. NetApp SnapMirror 기술을 사용하면 All-Flash 또는 FAS 어레이에서 느린 디스크 기반 스토리지 어레이로 또는 Cloud Volumes ONTAP for AWS, Azure 또는 Google Cloud로 이미징 데이터를 복제할 수 있습니다.

NetApp SnapMirror는 통합 데이터 복제를 통해 의료 영상 시스템을 보호하는 업계 최고의 데이터 복제 기능을 제공합니다. 플래시, 디스크, 클라우드에 이르는 교차 플랫폼 복제를 통해 Data Fabric 전반에서 데이터 보호 관리를 단순화합니다.

- 데이터를 NetApp 스토리지 시스템 간에 원활하고 효율적으로 전송하여 동일한 타겟 볼륨 및 I/O 스트림으로 백업 및 재해 복구 기능을 모두 지원합니다.
- 보조 볼륨으로 페일오버 보조 스토리지의 특정 시점 Snapshot에서 복구
- 데이터 무손실 동기식 복제(RPO=0)를 사용하여 가장 중요한 워크로드를 보호합니다.
- 네트워크 트래픽 감소 효율적인 운영을 통해 스토리지 설치 공간을 축소
- 변경된 데이터 블록만 전송함으로써 네트워크 트래픽을 줄입니다.
- 중복제거, 압축, 컴팩션을 포함하여 전송 중에 운영 스토리지에서 스토리지 효율성 이점을 유지합니다.
- 네트워크 압축을 통해 추가적인 인라인 효율성 제공

더 많은 정보를 찾을 "여기"수 있습니다.

아래 표에는 특정 지연 시간 및 처리량 성능 특성에 대해 일반적인 의료 영상 시스템에 필요한 각 계층이 나열되어 있습니다.

제공합니다	요구 사항	권장사항은 **NetApp**에서 제공합니다
1	지연 시간 35~500Mbps의 처리량 1~5ms	지연 시간이 1ms 미만인 AFF A300 고가용성(HA) 2개와 디스크 쉘프 2개로 AFF에서는 최대 1.6GBps의 처리량을 처리할 수 있습니다
2	온프레미스 아카이브	최대 30ms의 지연 시간을 제공하는 FAS
	클라우드에 아카이브	NetApp StorageGRID 소프트웨어를 사용하여 Cloud Volumes ONTAP로 SnapMirror 복제 또는 백업 아카이브

스토리지 네트워크 연결

FC 패브릭

- FC 패브릭은 컴퓨팅에서 스토리지로의 호스트 OS I/O를 위한 것입니다.
- FC 패브릭 2개(패브릭 A 및 패브릭 B)는 각각 Cisco UCS 패브릭 A 및 UCS 패브릭 B에 연결됩니다.
- FC 논리 인터페이스(LIF) 2개가 있는 SVM(스토리지 가상 머신)은 각 컨트롤러 노드에 있습니다. 각 노드에서 한 LIF는 패브릭 A에 연결되고 다른 LIF는 패브릭 B에 연결됩니다

- 16Gbps FC 엔드 투 엔드 접속은 Cisco MDS 스위치를 통해 이루어집니다. 단일 이니시에이터, 여러 타겟 포트 및 조닝이 모두 구성됩니다.
- FC SAN 부트는 상태 비저장 컴퓨팅을 생성하는 데 사용됩니다. 서버는 AFF 스토리지 클러스터에서 호스팅되는 부팅 볼륨의 LUN에서 부팅됩니다.

iSCSI, NFS 및 **SMB/CIFS**를 통한 스토리지 액세스를 위한 **IP** 네트워크

- 각 컨트롤러 노드의 SVM에는 2개의 iSCSI LIF가 있습니다. 각 노드에서 하나의 LIF가 패브릭 A에 연결되고 두 번째 LIF는 패브릭 B에 연결됩니다
- 각 컨트롤러 노드의 SVM에 2개의 NAS 데이터 LIF가 있습니다. 각 노드에서 하나의 LIF가 패브릭 A에 연결되고 두 번째 LIF는 패브릭 B에 연결됩니다
- 스위치 N9k-A에 대한 10Gbps 링크 및 스위치 N9k-B에 대한 10Gbps 링크에 대한 스토리지 포트 인터페이스 그룹(가상 포트 채널[vPC]
- VM에서 스토리지까지 ext4 또는 NTFS 파일 시스템의 워크로드:
  - IP를 통한 iSCSI 프로토콜.
- NFS 데이터 저장소에서 호스팅되는 VM:
  - VM OS I/O는 Nexus 스위치를 통해 여러 이더넷 경로를 통과합니다.

대역 내 관리(액티브-패시브 결합)

- 관리 스위치 N9k-A에 대한 1Gbps 링크 및 관리 스위치 N9k-B에 대한 1Gbps 링크

백업 및 복구

FlexPod 데이터 센터는 NetApp ONTAP 데이터 관리 소프트웨어에서 관리하는 스토리지 어레이를 기반으로 합니다. ONTAP 소프트웨어는 20년 이상 발전을 거듭하여 VM, Oracle 데이터베이스, SMB/CIFS 파일 공유 및 NFS에 다양한 데이터 관리 기능을 제공합니다. NetApp Snapshot 기술, SnapMirror 기술, NetApp FlexClone 데이터 복제 기술과 같은 보호 기술도 제공합니다. NetApp SnapCenter 소프트웨어에는 VM, SMB/CIFS 파일 공유, NFS, Oracle 데이터베이스 백업 및 복구를 위한 ONTAP Snapshot, SnapRestore 및 FlexClone 기능을 사용할 수 있는 서버 및 GUI 클라이언트가 있습니다.

NetApp SnapCenter 소프트웨어는 "특허 획득" Snapshot 기술: NetApp 스토리지 볼륨에서 전체 VM 또는 Oracle 데이터베이스의 백업을 즉시 생성합니다. Oracle RMAN(Recovery Manager)과 비교할 때 Snapshot 복사본은 블록의 물리적 복사본으로 저장되지 않으므로 전체 기본 백업 복사본이 필요하지 않습니다. 스냅샷 복사본은 스냅샷 복사본이 생성될 때 ONTAP WAFL 파일 시스템에 존재했던 스토리지 블록에 대한 포인터로 저장됩니다. 이처럼 밀접한 물리적 관계로 인해 Snapshot 복사본은 원래 데이터와 동일한 스토리지 어레이에 유지됩니다. 파일 레벨에서 스냅샷 복사본을 생성하여 백업에 대한 세부적인 제어를 제공할 수도 있습니다.

스냅샷 기술은 쓰기 시 리디렉션 기술을 기반으로 합니다. 처음에는 메타데이터 포인터만 포함하고 스토리지 블록으로 첫 번째 데이터가 변경될 때까지 공간을 많이 사용하지 않습니다. 스냅샷 복사본에 의해 기존 블록이 잠겨 있는 경우 ONTAP WAFL 파일 시스템이 새 블록을 액티브 복사본으로 기록합니다. 이 방식을 사용하면 쓰기 시 변경 기술에서 발생하는 이중 쓰기를 방지할 수 있습니다.

Oracle 데이터베이스 백업의 경우 Snapshot 복사본을 사용하면 시간을 크게 절약할 수 있습니다. 예를 들어, RMAN만 사용하여 완료하는 데 26시간이 걸리는 백업에는 SnapCenter 소프트웨어를 사용하는 데 2분도 걸리지 않습니다.

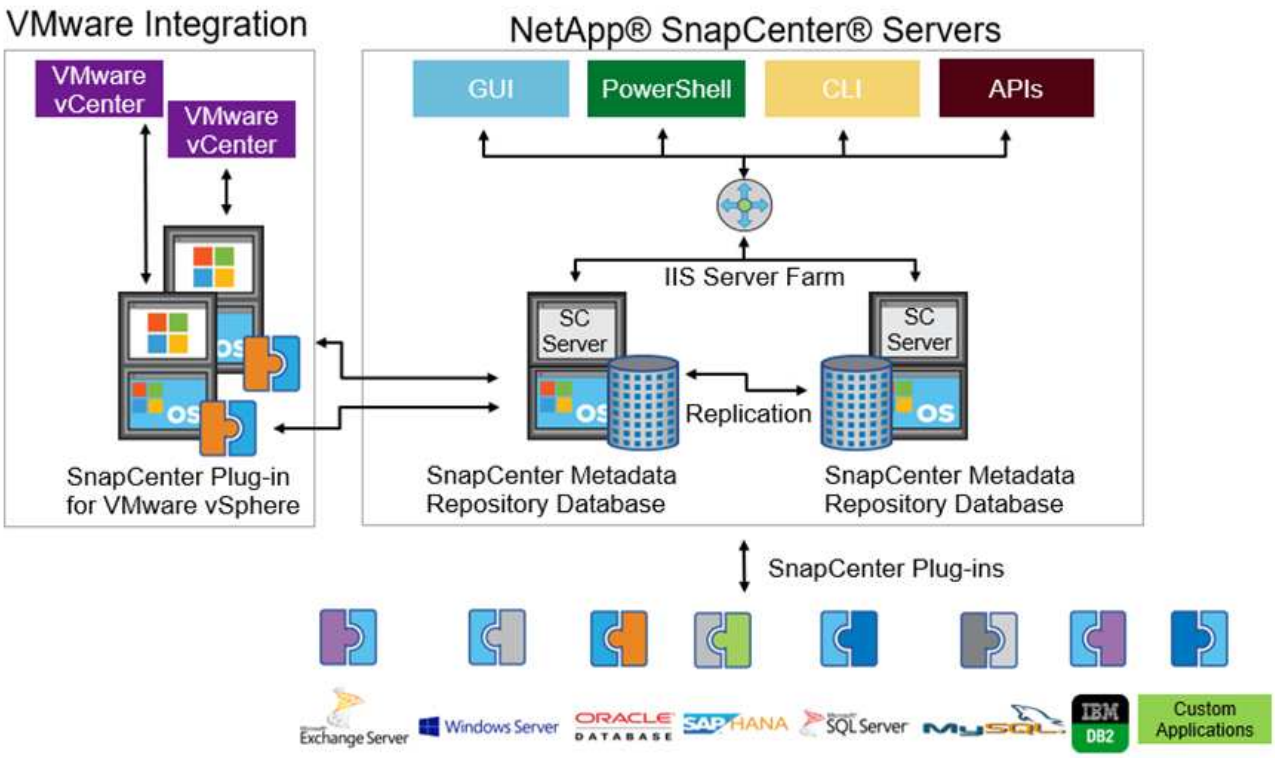
또한 데이터 복원으로 데이터 블록을 복사하는 것이 아니라 스냅샷 복사본이 생성될 때 애플리케이션 정합성이 보장된 스냅샷 블록 이미지에 대한 포인터를 대칭 이동하면 스냅샷 백업 복사본을 거의 즉시 복원할 수 있습니다. SnapCenter 클론 복제에서는 기존 스냅샷 복사본에 대한 메타데이터 포인터의 개별 복사본을 만들고 새 복사본을 타겟 호스트에

마운트합니다. 또한 이 프로세스는 빠르고 스토리지 효율성도 뛰어납니다.

다음 표에는 Oracle RMAN과 NetApp SnapCenter 소프트웨어의 주요 차이점이 요약되어 있습니다.

	백업	복원	복제	전체 백업 필요	공간 사용	오프 사이트 카피
RMAN	느림	느림	느림	예	높음	예
SnapCenter	빠릅니다	빠릅니다	빠릅니다	아니요	낮음	예

다음 그림은 SnapCenter 아키텍처를 보여 줍니다.



NetApp MetroCluster 구성은 전 세계 수천 개의 기업에서 고가용성(HA), 데이터 무손실, 무중단 운영을 데이터 센터 내외부에서 사용합니다. MetroCluster는 서로 다른 위치 또는 장애 도메인에 있는 두 ONTAP 클러스터 간에 데이터와 구성을 동기식으로 미러링하는 ONTAP 소프트웨어의 무료 기능입니다. MetroCluster는 두 가지 목표, 즉 클러스터에 기록된 데이터를 동기식으로 미러링함으로써 RPO(복구 시점 목표 없음)를 자동으로 처리하여 애플리케이션에 대해 지속적으로 사용 가능한 스토리지를 제공합니다. 구성을 미러링하고 두 번째 사이트의 데이터에 대한 액세스를 자동화하여 RTO(복구 시간 목표)가 거의 필요하지 않습니다. MetroCluster는 두 사이트에 있는 두 독립 클러스터 간에 데이터와 구성을 자동으로 미러링하여 단순화를 제공합니다. 스토리지가 한 클러스터 내에서 프로비저닝되면 두 번째 사이트의 두 번째 클러스터에 자동으로 미러링됩니다. NetApp SyncMirror 기술은 RPO가 0인 모든 데이터의 전체 복사본을 제공합니다. 따라서 한 사이트의 워크로드는 언제든지 다른 사이트로 전환하고 데이터 손실 없이 데이터를 계속 제공할 수 있습니다. 자세한 내용은 을 참조하십시오 "여기".

네트워킹

Cisco Nexus 스위치 쌍은 컴퓨팅에서 스토리지로의 IP 트래픽 및 의료 영상 시스템 이미지 뷰어의 외부 클라이언트에 대한 중복 경로를 제공합니다.

- 포트 채널과 vPC를 사용하는 Link Aggregation이 전체적으로 채택되어 더 높은 대역폭과 고가용성을 위한 설계가 가능합니다.
  - VPC는 NetApp 스토리지 어레이와 Cisco Nexus 스위치 간에 사용됩니다.
  - VPC는 Cisco UCS 패브릭 인터커넥트와 Cisco Nexus 스위치 간에 사용됩니다.
  - 각 서버에는 vNIC(Virtual Network Interface Card)가 있으며, 통합 패브릭과의 중복 연결이 가능합니다. NIC 페일오버는 이중화를 위해 Fabric 상호 연결 간에 사용됩니다.
  - 각 서버에는 vHBA(Virtual Host Bus Adapter)가 있으며, 통합 패브릭과 이중화된 접속이 가능합니다.
- Cisco UCS 패브릭 상호 연결은 권장 사항에 따라 최종 호스트 모드로 구성되어 업링크 스위치에 vNIC를 동적으로 고정할 수 있습니다.
- FC 스토리지 네트워크는 한 쌍의 Cisco MDS 스위치를 통해 제공됩니다.

컴퓨팅 **- Cisco Unified Computing System**

서로 다른 패브릭 인터커넥트를 통해 제공되는 2개의 Cisco UCS 패브릭은 2개의 장애 도메인을 제공합니다. 각 패브릭은 IP 네트워킹 스위치 및 다른 FC 네트워킹 스위치에 모두 연결됩니다.

VMware ESXi를 실행하기 위한 FlexPod 모범 사례에 따라 각 Cisco UCS 블레이드에 동일한 서비스 프로필이 생성됩니다. 각 서비스 프로필에는 다음 구성 요소가 있어야 합니다.

- NFS, SMB/CIFS 및 클라이언트 또는 관리 트래픽을 전달하는 vNIC 2개(각 Fabric에 1개
- NFS, SMB/CIFS 및 클라이언트 또는 관리 트래픽용 vNIC에 필요한 추가 VLAN
- iSCSI 트래픽을 전달하는 vNIC 2개(각 Fabric에 1개
- 스토리지에 대한 FC 트래픽을 위한 스토리지 FC HBA 2개(각 패브릭에 1개씩
- SAN 부팅

포함되었습니다

VMware ESXi 호스트 클러스터는 워크로드 VM을 실행합니다. 클러스터는 Cisco UCS 블레이드 서버에서 실행되는 ESXi 인스턴스로 구성됩니다.

각 ESXi 호스트에는 다음과 같은 네트워크 구성 요소가 포함됩니다.

- FC 또는 iSCSI를 통해 SAN 부팅
- NetApp 스토리지에서 LUN 부팅(부팅 OS용 전용 FlexVol)
- NFS, SMB/CIFS 또는 관리 트래픽을 위한 VMNIC(Cisco UCS vNIC) 2개
- 스토리지에 대한 FC 트래픽을 위한 2개의 스토리지 HBA(Cisco UCS FC vHBA
- 표준 스위치 또는 분산 가상 스위치(필요에 따라)
- 워크로드 VM용 NFS 데이터 저장소
- 관리, 클라이언트 트래픽 네트워크 및 VM용 스토리지 네트워크 포트 그룹
- 각 VM에 대한 관리, 클라이언트 트래픽 및 스토리지 액세스(NFS, iSCSI 또는 SMB/CIFS)를 위한 네트워크 어댑터
- VMware DRS가 활성화되었습니다
- 기본 다중 경로가 스토리지에 대한 FC 또는 iSCSI 경로에 대해 활성화되었습니다

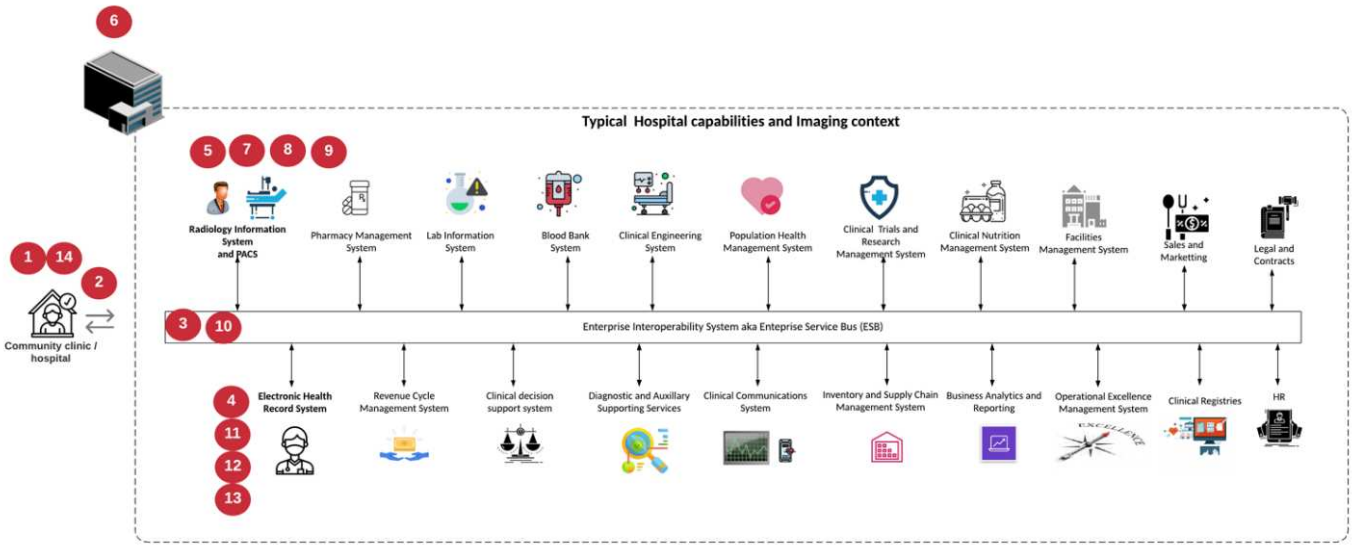
- VM에 대한 VMware 스냅샷이 꺼져 있습니다
- VM 백업을 위해 VMware에 구축된 NetApp SnapCenter

의료 영상 시스템 아키텍처

의료 조직에서 의료 영상 시스템은 중요한 애플리케이션이며 환자 등록부터 시작하여 수익 주기 동안 청구 관련 활동으로 끝나는 임상 워크플로우에 제대로 통합됩니다.

다음 다이어그램은 일반적인 대형 병원에 관련된 다양한 시스템을 보여 줍니다. 이 다이어그램은 일반적인 의료 영상 시스템의 아키텍처 구성 요소를 확대하기 전에 의료 영상 시스템에 구조적 컨텍스트를 제공하기 위한 것입니다. 워크플로는 매우 다양하며 병원과 사용 사례별로 다릅니다.

아래 그림은 환자, 지역 병원 및 대형 병원의 맥락에서 의료 영상 시스템을 보여줍니다.



1. 환자는 증상이 있는 지역 클리닉을 방문합니다. 상담 중에 커뮤니티 의사는 HL7 주문 메시지 형식으로 더 큰 병원으로 전송되는 영상 순서를 지정합니다.
2. 커뮤니티 주치의 EHR 시스템은 대형 병원으로 HL7 ORDER/ORD 메시지를 전송합니다.
3. 엔터프라이즈 상호 운용성 시스템(ESB(Enterprise Service Bus)라고도 함)은 주문 메시지를 처리하여 EHR 시스템에 주문 메시지를 보냅니다.
4. EHR은 주문 메시지를 처리합니다. 환자 레코드가 없으면 새 환자 레코드가 생성됩니다.
5. EHR은 의료 영상 시스템에 영상 주문을 전송합니다.
6. 환자가 대형 병원에 영상 촬영을 위해 전화합니다.
7. 영상 촬영 접수 및 등록 데스크는 방사선 정보 또는 유사한 시스템을 사용하여 영상 촬영 예약을 위해 환자를 예약합니다.
8. 환자가 영상 촬영 예약을 위해 도착하고 영상 또는 비디오가 생성되어 PACS로 전송됩니다.
9. 방사선과 전문의는 하이엔드/GPU 그래픽 지원 진단 뷰어를 사용하여 이미지를 읽고 PACS의 영상에 주석을 추가합니다. 특정 이미징 시스템에는 인공 지능(AI) 지원 효율성 향상 기능이 이미징 워크플로우에 내장되어 있습니다.
10. 이미지 주문 결과는 ESB를 통해 HL7 ORU 메시지를 통해 오더 결과 형식으로 EHR에 전송됩니다.
11. EHR은 주문 결과를 환자 기록에 처리하고 컨텍스트 인식 링크를 통해 축소판 이미지를 실제 DICOM 이미지에

배치합니다. 의사는 EHR 내에서 고해상도 이미지가 필요한 경우 진단 뷰어를 실행할 수 있습니다.

12. 의사는 영상을 검토하고 환자 기록에 의사 메모를 입력합니다. 의사는 임상 결정 지원 시스템을 사용하여 검토 프로세스를 개선하고 환자에 대한 적절한 진단을 도울 수 있습니다.
13. 그런 다음 EHR 시스템은 주문 결과를 커뮤니티 병원에 주문 결과 메시지 형식으로 전송합니다. 이때 커뮤니티 병원이 전체 영상을 수신할 수 있으면 WADO 또는 DICOM을 통해 영상이 전송됩니다.
14. 커뮤니티 의사는 진단을 완료하고 환자에게 다음 단계를 제공합니다.

일반적인 의료 영상 시스템은 N-계층형 아키텍처를 사용합니다. 의료 영상 시스템의 핵심 구성 요소는 다양한 애플리케이션 구성 요소를 호스팅하는 애플리케이션 서버입니다. 일반적인 응용 프로그램 서버는 Java 런타임 기반 또는 C#.Net CLR 기반 서버입니다. 대부분의 엔터프라이즈 의료 영상 솔루션은 Oracle Database Server 또는 MS SQL Server 또는 Sybase를 기본 데이터베이스로 사용합니다. 또한 일부 기업 의료 영상 시스템은 지리적 지역에 대한 콘텐츠 가속화 및 캐싱에 데이터베이스를 사용합니다. 일부 엔터프라이즈 의료 영상 시스템은 또한 DICOM 인터페이스 및/또는 API용 엔터프라이즈 통합 서버와 함께 MongoDB, Redis 등의 NoSQL 데이터베이스를 사용합니다.

일반적인 의료용 영상 시스템은 두 가지 사용자 세트(진단 사용자/방사선과 전문의 또는 영상을 주문한 임상의나 의사)에 대한 영상에 대한 액세스를 제공합니다.

방사선 전문의는 일반적으로 물리적 또는 가상 데스크톱 인프라의 일부인 하이엔드 컴퓨팅 및 그래픽 워크스테이션에서 실행 중인 하이엔드 그래픽 지원 진단 뷰어를 사용합니다. 가상 데스크톱 인프라 전환을 시작하려는 경우 추가 정보를 찾을 수 있습니다 "여기".

허리케인 카트리나가 루이지애나의 주요 교육 병원 중 2곳을 파괴했을 때, 리더들이 모여 사상 최대 3000개 이상의 가상 데스크톱을 포함한 탄력적인 전자 의료 기록 시스템을 구축했습니다. 사용 사례 참조 아키텍처 및 FlexPod 참조 번들에 대한 자세한 내용은 를 참조하십시오 "여기".

임상의는 다음 두 가지 주요 방법으로 이미지에 액세스합니다.

- * 웹 기반 액세스. * 이는 일반적으로 EHR 시스템에서 PACS 이미지를 환자의 전자 의료 기록(EMR)에 컨텍스트 인식 링크로 내장하고, 이미지 워크플로우, 절차 워크플로우, 진행 노트 워크플로우 등에 배치할 수 있는 링크를 포함하는 데 사용됩니다. 웹 기반 링크는 환자 포털을 통해 환자에 대한 이미지 액세스를 제공하는 데도 사용됩니다. 웹 기반 액세스는 컨텍스트 인식 링크라는 기술 패턴을 사용합니다. 컨텍스트 인식 링크는 DICOM 미디어에 대한 정적 링크/URI가 될 수도 있고 사용자 지정 매크로를 사용하여 동적으로 생성된 링크/URI가 될 수도 있습니다.
- * Thick client. * 일부 기업 의료 시스템에서는 두꺼운 클라이언트 기반 접근 방식을 사용하여 이미지를 볼 수도 있습니다. 환자의 EMR 내에서 또는 독립 실행형 애플리케이션으로 씩 클라이언트를 시작할 수 있습니다.

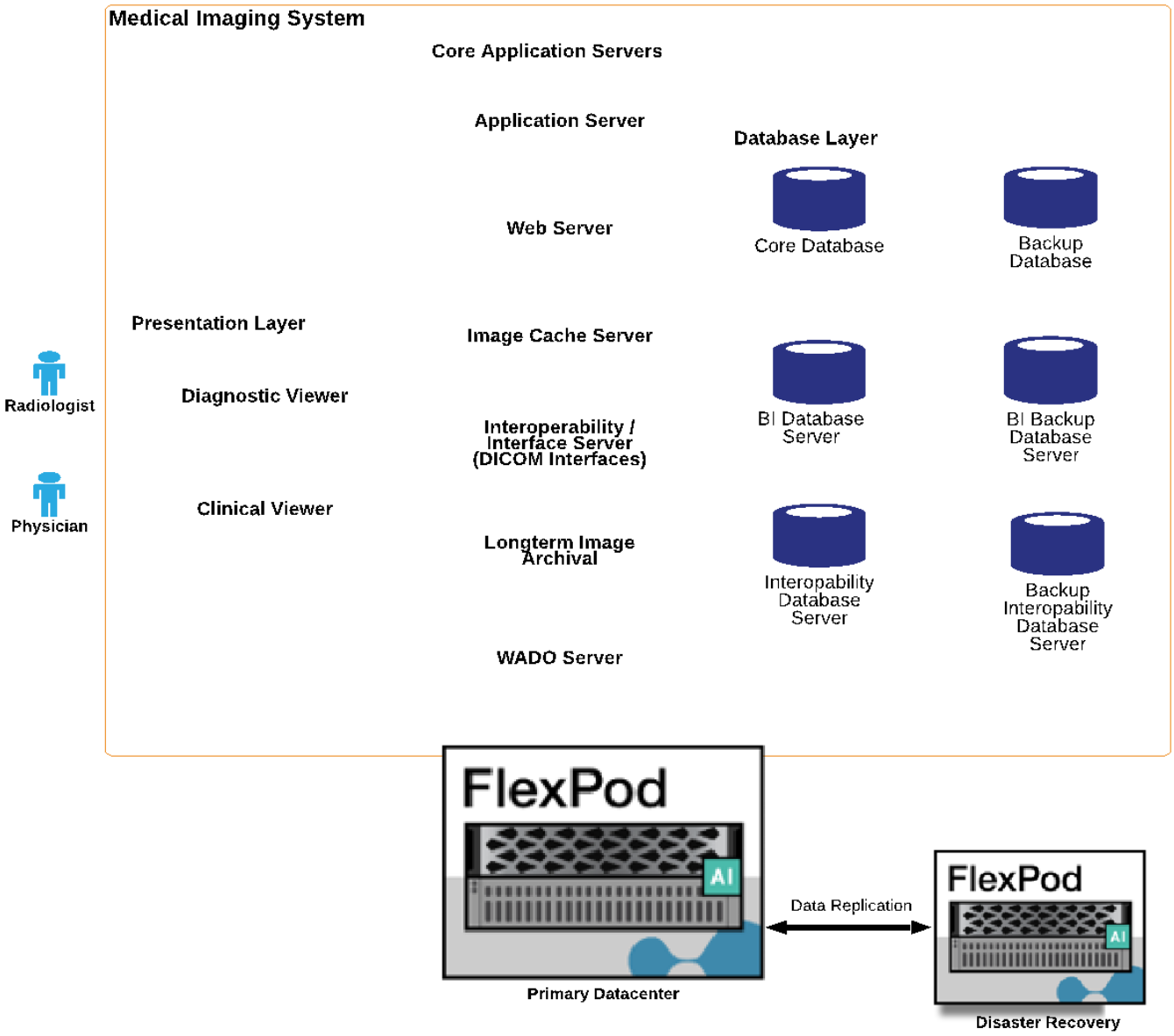
의료 영상 시스템은 의사 커뮤니티 또는 CIN 참여 의사에게 영상 액세스를 제공할 수 있습니다. 일반적인 의료 영상 시스템에는 의료 조직 내부 및 외부의 다른 의료 IT 시스템과의 이미지 상호 운용성을 지원하는 구성 요소가 포함되어 있습니다. 커뮤니티 의사는 웹 기반 애플리케이션을 통해 이미지에 액세스하거나 이미지 상호 운용성을 위해 이미지 교환 플랫폼을 활용할 수 있습니다. 영상 교환 플랫폼은 일반적으로 WADO 또는 DICOM을 기본 영상 교환 프로토콜로 사용합니다.

의료 영상 시스템은 교실에서 사용할 PACS 또는 영상 시스템이 필요한 교육 의료 센터도 지원할 수 있습니다. 학술 활동을 지원하기 위해, 일반적인 의료 영상 시스템은 보다 작은 설치 공간 또는 교육 전용 영상 환경에서 PACS 시스템의 기능을 가질 수 있습니다. 일반적인 벤더 중립적 보관 시스템과 일부 엔터프라이즈급 의료 영상 시스템은 교육 목적으로 사용되는 영상을 익명화할 수 있는 DICOM 영상 태그 변형 기능을 제공합니다. 태그 모핑은 의료 기관이 서로 다른 공급업체의 의료 영상 시스템 간에 공급업체 중립적인 방식으로 DICOM 이미지를 교환할 수 있도록 합니다. 또한 태그 모르핑은 의료 영상 시스템이 의료 영상을 위한 기업 차원의 벤더 중립적 보관 기능을 구현할 수 있게 해줍니다.

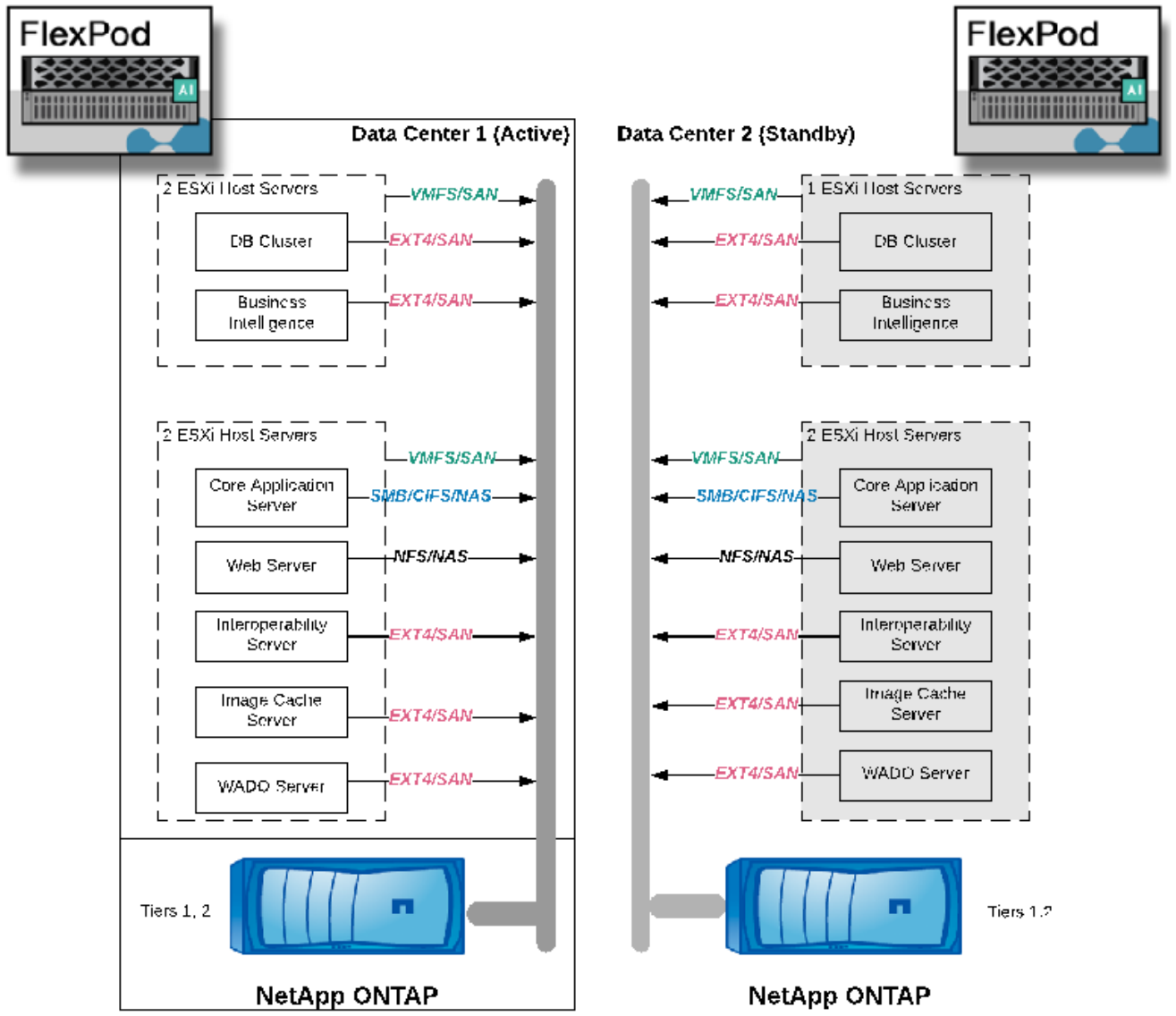
의료 영상 시스템은 "GPU 기반 컴퓨팅 기능" 이미지를 사전 처리하여 효율성을 개선하여 인간의 작업 흐름을 개선하기 위해 사용하기 시작했습니다. 일반적인 기업 의료 영상 시스템은 업계 최고의 NetApp 스토리지 효율성 기능을 활용합니다. 엔터프라이즈 의료 영상 시스템은 일반적으로 백업, 복구 및 복원 작업에 RMAN을 사용합니다. 성능을 향상하고 백업을 생성하는 데 걸리는 시간을 줄이기 위해 스냅샷 기술을 백업 작업에 사용할 수 있으며 SnapMirror

기술을 복제에 사용할 수 있습니다.

아래 그림은 계층화된 아키텍처 보기의 논리적 애플리케이션 구성 요소를 보여 줍니다.



아래 그림은 물리적 애플리케이션 구성 요소를 보여줍니다.



논리적 애플리케이션 구성요소를 사용하려면 인프라에서 다양한 프로토콜 및 파일 시스템을 지원해야 합니다. NetApp ONTAP 소프트웨어는 업계 최고의 프로토콜 및 파일 시스템 세트를 지원합니다.

아래 표에는 애플리케이션 구성 요소, 스토리지 프로토콜 및 파일 시스템 요구 사항이 나와 있습니다.

응용 프로그램 구성 요소	**SAN/NAS**	파일 시스템 유형입니다	제공합니다	복제 유형입니다
VMware 호스트 운영 DB	로컬	산	VMFS를 참조하십시오	계층 1
응용 프로그램	VMware 호스트 운영 DB	반복	산	VMFS를 참조하십시오
계층 1	응용 프로그램	VMware 호스트 운영 애플리케이션	로컬	산
VMFS를 참조하십시오	계층 1	응용 프로그램	VMware 호스트 운영 애플리케이션	반복

응용 프로그램 구성 요소	**SAN/NAS**	파일 시스템 유형입니다	제공합니다	복제 유형입니다
산	VMFS를 참조하십시오	계층 1	응용 프로그램	핵심 데이터베이스 서버
산	ext4	계층 1	응용 프로그램	백업 데이터베이스 서버
산	ext4	계층 1	없음	이미지 캐시 서버
NAS	SMB/CIFS	계층 1	없음	보관 서버
NAS	SMB/CIFS	계층 2	응용 프로그램	웹 서버
NAS	SMB/CIFS	계층 1	없음	WADO 서버
산	NFS 를 참조하십시오	계층 1	응용 프로그램	비즈니스 인텔리전스 서버
산	NTFS입니다	계층 1	응용 프로그램	비즈니스 인텔리전스 백업
산	NTFS입니다	계층 1	응용 프로그램	상호 운용성 서버
산	ext4	계층 1	응용 프로그램	상호 운용성 데이터베이스 서버

솔루션 인프라 하드웨어 및 소프트웨어 구성 요소

다음 표에는 의료 영상 시스템용 FlexPod 인프라의 하드웨어 및 소프트웨어 구성 요소가 각각 나열되어 있습니다.

레이어	제품군	수량 및 모델	세부 정보
컴퓨팅	Cisco UCS 5108 섀시	1 또는 2	연간 연구 수를 지원하는 데 필요한 블레이드 수에 따라 달라집니다
	Cisco UCS 블레이드 서버	B200 M5	2개 이상의 코어, 2.7GHz 및 128-384GB RAM이 있는 연간 검사 수를 기준으로 한 블레이드의 수
	Cisco UCS 가상 인터페이스 카드(VIC)	Cisco UCS 1440	를 참조하십시오
	2 x Cisco UCS 패브릭 인터커넥트	6454 이상	–
네트워크	Cisco Nexus 스위치	Cisco Nexus 3000 시리즈 또는 9000 시리즈 2개	–
스토리지 네트워크	SMB/CIFS, NFS 또는 iSCSI 프로토콜을 통한 스토리지 액세스를 위한 IP 네트워크	위와 동일한 네트워크 스위치	–
	FC를 통한 스토리지 액세스	Cisco MDS 9132T 2개	–

레이어	제품군	수량 및 모델	세부 정보
스토리지	NetApp AFF A400 All-Flash 스토리지 시스템	1개 이상의 HA 쌍	2개 이상의 노드로 클러스터
	디스크 쉘프	DS224C 또는 NS224 디스크 쉘프 1개 이상	24개 드라이브로 완전히 채워집니다
	SSD를 지원합니다	>24, 1.2TB 이상의 용량	–

소프트웨어	제품군	버전 또는 릴리스	세부 정보
기업용 의료 영상 시스템			
	MS SQL 또는 Oracle Database Server	의료 영상 시스템 공급업체가 제안한 대로	
	MongoDB Server와 같은 SQL DB는 없습니다	의료 영상 시스템 공급업체가 제안한 대로	
	애플리케이션 서버	의료 영상 시스템 공급업체가 제안한 대로	
	통합 서버(MS BizTalk, MuleSoft, Rhapsody, Tibco)	의료 영상 시스템 공급업체가 제안한 대로	
	VM	Linux(64비트)	
	VM	Windows Server(64비트)	
스토리지	ONTAP	ONTAP 9.7 이상	
네트워크	Cisco UCS 6120 패브릭 인터커넥트	Cisco UCS Manager 4.1 이상	
	Cisco 이더넷 스위치	9.2(3) i7(2) 이상	
	Cisco FC: Cisco MDS 9132T	8.4(2) 이상	
하이퍼바이저	하이퍼바이저	VMware vSphere ESXi 6.7 U2 이상	
관리	하이퍼바이저 관리 시스템	VMware vCenter Server 6.7 U1(vCSA) 이상	
	NetApp 가상 스토리지 콘솔(VSC)	VSC 9.7 이상	
	SnapCenter	SnapCenter 4.3 이상	

솔루션 사이징

스토리지 사이징

이 섹션에서는 스터디 수와 해당 인프라 요구 사항에 대해 설명합니다.

다음 표에 나와 있는 스토리지 요구 사항에서는 기존 데이터가 1년 가치가 있고 1년 동안 기본 시스템(계층 1, 2)에서 연구 증가가 예상된다고 가정합니다. 처음 2년 이후 3년간 예상되는 추가 스토리지 요구사항은 별도로 나열되어 있습니다.

	작은 크기	중간	대형
연간 연구	250,000건 미만의 연구	250K – 500K 연구	50만–100만 연구
Tier 1 스토리지			
IOPS(평균)	1.5k – 5K	5K – 15K	15K – 40K
IOPS(최대)	5K	2만	6만 5천
처리량	50–100Mbps	50 ~ 150MBps	100–300Mbps
용량 데이터 센터 1(이전 데이터 1년 및 신규 연구 1년)	70TB	140TB	260TB
용량 데이터 센터 1 (신규 연구에 4년 더 필요함)	25TB	45TB	80TB
용량 데이터 센터 2(이전 데이터 1년 및 신규 연구 1년)	45TB	110TB	165TB
용량 데이터 센터 2 (신규 연구를 위해 4년 추가 필요)	25TB	45TB	80TB
Tier 2 스토리지			
IOPS(평균)	1K	2K	3K
용량 데이터 센터 1	320TB	800TB	2000TB

컴퓨팅 사이징

아래 표에는 소형, 중형 및 대형 의료 영상 시스템에 대한 컴퓨팅 요구사항이 나와 있습니다.

	작은 크기	중간	대형
연간 연구	250,000건 미만의 연구	250K – 500K 연구	50만–100만 연구
데이터 센터 1			
VM 수입니다	21	27	35
총 가상 CPU(vCPU) 수입니다	56	124를 참조하십시오	220
총 메모리 요구 사항	225GB	450GB	900GB
물리적 서버(블레이드) 사양(vCPU 1개 - 코어 1개 가정)	각각 20개의 코어와 192GB RAM이 장착된 서버 4대	각각 20개의 코어와 128GB RAM이 장착된 서버 8대	각각 20개 코어와 128GB RAM이 장착된 서버 14대
데이터 센터 2			
VM 수입니다	15	17	22
총 vCPU 수입니다	42	72	140
총 메모리 요구 사항	179GB	243GB	513GB

	작은 크기	중간	대형
물리적 서버(블레이드) 사양(vCPU 1개 = 코어 1개 가정)	서버 3대, 코어 20개, RAM 168GB	각각 20개의 코어와 128GB RAM이 장착된 서버 6대	각각 24개 코어와 128GB RAM이 장착된 서버 8대

네트워킹 및 **Cisco UCS** 인프라 사이징

아래 표에는 소형, 중형 및 대형 의료 영상 시스템에 대한 네트워킹 및 Cisco UCS 인프라 요구사항이 나와 있습니다.

	작은 크기	중간	대형
데이터 센터 1			
스토리지 노드 포트 수입니다	CNA(Converged Network Adapter) 2개, FC 2개	CNA 2개, FC 2개	CNA 2개, FC 2개
IP 네트워크 스위치 포트(Cisco Nexus 9000)	48포트 스위치	48포트 스위치	48포트 스위치
FC 스위치(Cisco MDS)	32포트 스위치	32포트 스위치	48포트 스위치
Cisco UCS 섀시 수	1 x 5108	1 x 5108	2 x 5108
Cisco UCS 6120 패브릭 인터커넥트	2 x 6332	2 x 6332	2 x 6332
데이터 센터 2			
Cisco UCS 섀시 수	1 x 5108	1 x 5108	1 x 5108
Cisco UCS 6120 패브릭 인터커넥트	2 x 6332	2 x 6332	2 x 6332
스토리지 노드 포트 수입니다	CNA 2개, FC 2개	CNA 2개, FC 2개	CNA 2개, FC 2개
IP 네트워크 스위치 포트(Cisco Nexus 9000)	48포트 스위치	48포트 스위치	48포트 스위치
FC 스위치(Cisco MDS)	32포트 스위치	32포트 스위치	48포트 스위치

모범 사례

스토리지 모범 사례

고가용성

NetApp 스토리지 클러스터 설계는 모든 레벨에서 고가용성을 제공합니다.

- 클러스터 노드
- 백엔드 스토리지 접속 구성
- 3가지 디스크 장애를 지원할 수 있는 RAID TEC
- 2개의 디스크 장애를 감당할 수 있는 RAID DP
- 각 노드에서 2개의 물리적 네트워크에 대한 물리적 연결

- 스토리지 LUN 및 볼륨에 대한 다중 데이터 경로

보안 멀티 테넌시

NetApp SVM(스토리지 가상 시스템)은 보안 도메인, 정책 및 가상 네트워킹을 분리하기 위해 가상 스토리지 어레이를 제공합니다. NetApp은 스토리지 클러스터에서 데이터를 호스팅하는 각 테넌트 조직에 대해 별도의 SVM을 생성할 것을 권장합니다.

NetApp 스토리지 모범 사례

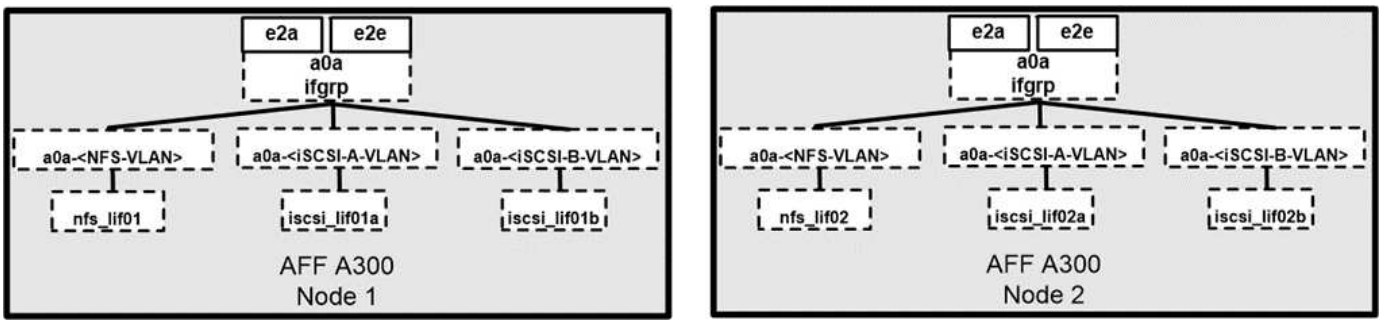
다음과 같은 NetApp 스토리지 모범 사례를 고려해 보십시오.

- NetApp AutoSupport 기술을 항상 사용하도록 설정하십시오. 그러면 HTTPS를 통해 지원 요약 정보가 NetApp에 전송됩니다.
- 가용성과 이동성을 최대화하기 위해 NetApp ONTAP 클러스터의 각 노드에서 SVM용으로 LIF를 생성해야 합니다. ALUA(Asymmetric Logical Unit Access)는 경로를 구문 분석하고 활성 최적화(직접) 경로와 최적화되지 않은 활성 경로를 식별하는 데 사용됩니다. ALUA는 FC 또는 FCoE 및 iSCSI 모두에 사용됩니다.
- LUN만 포함된 볼륨은 내부적으로 마운트할 필요가 없으며 접합 경로가 필요하지 않습니다.
- 대상 인증을 위해 ESXi에서 CHAP(Challenge-Handshake Authentication Protocol)를 사용하는 경우 ONTAP에서도 구성해야 합니다. CLI('vserver iSCSI security create') 또는 NetApp ONTAP System Manager(스토리지 > SVM > SVM 설정 > 프로토콜 > iSCSI에서 이니시에이터 보안 편집)를 사용하십시오.

SAN 부팅

FlexPod 데이터 센터 솔루션에서 Cisco UCS 서버용 SAN 부팅을 구축하는 것이 좋습니다. 이 단계를 통해 운영 체제를 NetApp AFF 스토리지 시스템으로 안전하게 보호하면서 더 나은 성능을 제공할 수 있습니다. 이 솔루션에 요약된 설계는 iSCSI SAN 부팅을 사용합니다.

iSCSI SAN 부팅에서 각 Cisco UCS 서버에는 스토리지에 대한 이중 연결을 제공하는 2개의 iSCSI vNIC(각 SAN 패브릭당 1개)가 할당됩니다. 이 예의 스토리지 포트인 e2a와 E2E는 Cisco Nexus 스위치에 연결되어 함께 그룹화하여 인터페이스 그룹(ifgrp)이라는 하나의 논리 포트(이 예에서는 a0a)를 구성합니다. iSCSI VLAN은 igroup에 생성되고 iSCSI LIF는 iSCSI 포트 그룹(이 예에서는 a0a-<iSCSI-A-VLAN>)에 생성됩니다. iSCSI 부트 LUN은 igroup을 사용하여 iSCSI LIF를 통해 서버에 노출됩니다. 이렇게 하면 권한이 있는 서버만 부팅 LUN에 액세스할 수 있습니다. 포트 및 LIF 레이아웃에 대한 자세한 내용은 아래 그림을 참조하십시오.



NAS 네트워크 인터페이스와 달리 SAN 네트워크 인터페이스는 장애 발생 시 페일오버되도록 구성되지 않습니다. 대신, 네트워크 인터페이스를 사용할 수 없게 되면 호스트는 사용 가능한 네트워크 인터페이스에 대해 최적화된 새 경로를 선택합니다. NetApp에서 지원하는 표준인 ALUA는 호스트가 최상의 스토리지 경로를 식별할 수 있도록 SCSI 타겟에 대한 정보를 제공합니다.

스토리지 효율성 및 씬 프로비저닝

NetApp은 운영 워크로드를 위한 최초의 중복제거 기능과 인라인 데이터 컴팩션을 통해 압축을 강화하고 작은 파일 및 I/O를 효율적으로 저장하는 등 스토리지 효율성 혁신에 있어 업계를 선도하고 있습니다. ONTAP는 인라인 및 백그라운드 중복제거와 인라인 및 백그라운드 압축을 모두 지원합니다.

블록 환경에서 중복 제거의 이점을 실현하려면 LUN이 씬 프로비저닝되어야 합니다. LUN이 여전히 VM 관리자가 프로비저닝된 용량을 차지하는 것으로 보이더라도 중복 제거 절약 효과가 다른 요구에 사용될 볼륨으로 반환됩니다. 이러한 LUN을 LUN 크기의 2배에 달하는 용량으로 씬 프로비저닝된 FlexVol 볼륨에 구축하는 것이 좋습니다. 이러한 방식으로 LUN을 구축하면 FlexVol 볼륨이 할당량만 됩니다. LUN이 사용하는 스토리지가 FlexVol 볼륨과 포함된 애그리게이트에 보고됩니다.

중복제거를 최대한 절약하거나, 백그라운드 중복제거를 예약하는 것이 좋습니다. 그러나 이러한 프로세스는 실행 중일 때 시스템 리소스를 사용합니다. 따라서 가장 좋은 방법은 자주 사용하지 않는 시간(예: 주말)에 일정을 세우거나 자주 실행하여 변경된 데이터 처리 횟수를 줄이는 것입니다. AFF 시스템의 자동 백그라운드 중복제거는 전경 작업에 미치는 영향을 훨씬 덜 줍니다. 백그라운드 압축(하드 디스크 기반 시스템의 경우)도 리소스를 사용하므로 성능 요구사항이 제한적인 2차 워크로드에만 사용해야 합니다.

서비스 품질

ONTAP 소프트웨어를 실행하는 시스템에서는 ONTAP 스토리지 QoS 기능을 사용하여 초당 메가비트(MBps) 단위의 처리량을 제한하고 파일, LUN, 볼륨 또는 전체 SVM과 같은 서로 다른 스토리지 개체에 대한 IOPS를 제한할 수 있습니다. 적응형 QoS는 데이터 저장소 용량 및 사용된 공간에 따라 동적으로 조정되는 IOPS 바닥(QoS 최소) 및 상한(QoS 최대)을 설정하는 데 사용됩니다.

처리량 제한은 다른 워크로드에 영향을 주지 않는지 확인하기 위해 배포 전에 알 수 없거나 테스트 워크로드를 제어하는 데 유용합니다. 또한 이러한 제한을 사용하여 제한된 워크로드가 확인된 후에 이를 제한할 수도 있습니다. ONTAP의 SAN 오브젝트에 일관된 성능을 제공하기 위해 IOPS를 기반으로 하는 최소 서비스 레벨도 지원됩니다.

NFS 데이터 저장소를 사용하면 QoS 정책을 전체 FlexVol 볼륨 또는 해당 볼륨 내의 개별 가상 머신 디스크(VMDK) 파일에 적용할 수 있습니다. ONTAP LUN을 사용하는 VMFS 데이터 저장소(Hyper-V의 클러스터 공유 볼륨 [CSV])에서는 LUN이 포함된 FlexVol 볼륨 또는 개별 LUN에 QoS 정책을 적용할 수 있습니다. 하지만 ONTAP는 VMFS를 인식할 수 없기 때문에 개별 VMDK 파일에 QoS 정책을 적용할 수 없습니다. VSC 7.1 이상과 함께 VMware 가상 볼륨(VVol)을 사용하면 스토리지 기능 프로필을 사용하여 개별 VM에서 최대 QoS를 설정할 수 있습니다.

VMFS 또는 CSV를 비롯한 LUN에 QoS 정책을 할당하려면 VSC 홈 페이지의 스토리지 시스템 메뉴에서 ONTAP SVM('Vserver'으로 표시됨), LUN 경로 및 일련 번호를 확인할 수 있습니다. 스토리지 시스템(SVM)을 선택한 다음 Related Objects > SAN을 선택합니다. ONTAP 툴 중 하나를 사용하여 QoS를 지정할 때 이 접근 방식을 사용합니다.

오브젝트에 대한 QoS 최대 처리량 제한을 Mbps 단위로, IOPS 단위로 설정할 수 있습니다. 둘 다 사용하는 경우 첫 번째 제한에 도달하면 ONTAP에서 적용됩니다. 워크로드에는 여러 개체가 포함될 수 있으며 QoS 정책을 하나 이상의 워크로드에 적용할 수 있습니다. 여러 워크로드에 정책을 적용하면 워크로드에서는 정책의 총 한도를 공유합니다. 중첩된 개체는 지원되지 않습니다(예: 볼륨 내의 파일의 경우 각 개체는 고유한 정책을 가질 수 없음). QoS 최소값을 IOPS에서만 설정할 수 있습니다.

스토리지 레이아웃

이 섹션에서는 스토리지의 LUN, 볼륨 및 애그리게이트 레이아웃에 대한 모범 사례를 설명합니다.

스토리지 **LUN**

최적의 성능, 관리 및 백업을 위해 NetApp은 다음과 같은 LUN 설계 모범 사례를 권장합니다.

- 데이터베이스 데이터와 로그 파일을 저장할 별도의 LUN을 생성합니다.
- Oracle 데이터베이스 로그 백업을 저장할 각 인스턴스에 대해 별도의 LUN을 생성합니다. LUN은 동일한 볼륨의 일부일 수 있습니다.
- 데이터베이스 파일 및 로그 파일에 대한 씬 프로비저닝(공간 예약 옵션 사용 안 함)으로 LUN을 프로비저닝합니다.
- 모든 이미징 데이터는 FC LUN에 호스팅됩니다. FlexVol 볼륨에서 서로 다른 스토리지 컨트롤러 노드가 소유한 Aggregate에 분산되는 LUN을 생성합니다.

스토리지 볼륨에 LUN을 배치하려면 다음 섹션의 지침을 따르십시오.

스토리지 볼륨

최적의 성능 및 관리를 위해 다음과 같은 볼륨 설계 모범 사례를 따르는 것이 좋습니다.

- 개별 스토리지 볼륨에서 I/O 집약적 쿼리로 데이터베이스를 격리합니다.
- 단일 LUN 또는 볼륨에 데이터 파일을 배치할 수 있지만 높은 처리량을 위해서는 여러 볼륨/LUN을 사용하는 것이 좋습니다.
- 여러 LUN을 사용하는 경우 지원되는 모든 파일 시스템을 사용하여 입출력 병렬 처리를 수행할 수 있습니다.
- 데이터베이스 파일 및 트랜잭션 로그를 별도의 볼륨에 배치하여 복구 세분성을 높입니다.
- 자동 크기, 스냅샷 예약, QoS 등과 같은 볼륨 특성을 사용하는 것을 고려해 보십시오.

애그리게이트

Aggregate는 NetApp 스토리지 구성의 운영 스토리지 컨테이너로, 데이터 디스크와 패리티 디스크로 구성된 하나 이상의 RAID 그룹을 포함합니다.

NetApp은 데이터 파일과 트랜잭션 로그 파일을 분리한 상태로 공유 및 전용 애그리게이트를 사용하여 다양한 I/O 워크로드 특성 테스트를 수행했습니다. 테스트 결과, RAID 그룹 및 드라이브(HDD 또는 SSD)가 더 많은 대형 Aggregate가 스토리지 성능을 최적화 및 개선하고 관리자가 다음과 같은 두 가지 이유로 더 쉽게 관리할 수 있는 것으로 나타났습니다.

- 하나의 대형 Aggregate는 모든 드라이브에서 I/O 기능을 모든 파일에 사용할 수 있도록 합니다.
- 하나의 대형 Aggregate는 디스크 공간을 가장 효율적으로 사용합니다.

효과적인 재해 복구를 위해 재해 복구 사이트에서 별도의 스토리지 클러스터의 일부인 애그리게이트에 비동기식 복제본을 배치하고 SnapMirror 기술을 사용하여 콘텐츠를 복제하는 것이 좋습니다.

최적의 스토리지 성능을 위해 aggregate에서 사용 가능한 공간을 10% 이상 확보하는 것이 좋습니다.

AFF A300 시스템(드라이브 24개가 포함된 디스크 쉘프 2개)에 대한 스토리지 애그리게이트 레이아웃 지침은 다음과 같습니다.

- 스페어 드라이브 2개를 보관합니다.
- 고급 디스크 파티셔닝을 사용하여 각 드라이브에 3개의 파티션, 즉 루트와 데이터를 작성하십시오.
- 각 애그리게이트에 총 20개의 데이터 파티션과 2개의 패리티 파티션을 사용합니다.

백업 **Best Practice**

NetApp SnapCenter는 VM 및 데이터베이스 백업에 사용됩니다. 권장되는 백업 모범 사례는 다음과 같습니다.

- 백업을 위한 스냅샷 복사본을 생성하기 위해 SnapCenter를 구축한 경우 VM 및 애플리케이션 데이터를 호스팅하는 FlexVol의 스냅샷 스케줄을 끄십시오.
- 호스트 부팅 LUN을 위한 전용 FlexVol를 생성합니다.
- 같은 용도로 사용되는 VM에 대해 유사하거나 단일 백업 정책을 사용합니다.
- 워크로드 유형별로 비슷하거나 단일 백업 정책을 사용하십시오. 예를 들어, 모든 데이터베이스 워크로드에 비슷한 정책을 사용하십시오. 데이터베이스, 웹 서버, 최종 사용자 가상 데스크톱 등에 대해 서로 다른 정책을 사용합니다.
- SnapCenter에서 백업 확인을 활성화합니다.
- NetApp SnapVault 백업 솔루션에 백업 Snapshot 복사본 아카이브를 구성합니다.
- 아카이브 일정에 따라 운영 스토리지에 백업 보존을 구성합니다.

인프라 모범 사례

네트워킹 모범 사례

NetApp에서는 다음과 같은 네트워킹 모범 사례를 권장합니다.

- 시스템에 운영 및 스토리지 트래픽을 위한 이중화된 물리적 NIC가 포함되어 있는지 확인합니다.
- 컴퓨팅과 스토리지 간의 iSCSI, NFS 및 SMB/CIFS 트래픽에 대해 별도의 VLAN을 사용합니다.
- 시스템에 의료용 영상 시스템에 대한 클라이언트 액세스를 위한 전용 VLAN이 포함되어 있는지 확인하십시오.

FlexPod 인프라 설계 및 구축 가이드에서 추가 네트워킹 모범 사례를 확인할 수 있습니다.

컴퓨팅 모범 사례

NetApp에서는 다음과 같은 컴퓨팅 모범 사례를 따르는 것이 좋습니다.

- 지정된 각 vCPU가 물리적 코어에서 지원되는지 확인합니다.

가상화 모범 사례

권장되는 가상화 모범 사례는 다음과 같습니다.

- VMware vSphere 6 이상을 사용합니다.
- ESXi 호스트 서버 BIOS 및 OS 계층을 Custom Controlled – High Performance로 설정합니다.
- 사용량이 적은 시간에 백업을 생성합니다.

의료 영상 시스템 모범 사례

일반적인 의료 영상 시스템의 다음 모범 사례와 일부 요구 사항을 참조하십시오.

- 가상 메모리를 오버 커밋하지 마십시오.
- 총 vCPU 수가 물리적 CPU 수와 같은지 확인합니다.

- 대규모 환경인 경우 전용 VLAN이 필요합니다.
- 전용 HA 클러스터를 사용하여 데이터베이스 VM 구성
- VM OS VMDK가 고속 계층 1 스토리지에 호스팅되는지 확인합니다.
- 의료 영상 시스템 공급업체와 협력하여 신속한 배포 및 유지 관리를 위해 VM 템플릿을 준비하는 가장 좋은 방법을 파악합니다.
- 관리, 스토리지 및 운영 네트워크에서는 데이터베이스에 대한 LAN 분리가 필요하며, VMware vMotion에 대해 격리된 VLAN이 있어야 합니다.
- "SnapMirror를 참조하십시오"vSphere 기반 복제 대신 라는 NetApp 스토리지 어레이 기반 복제 기술을 사용하십시오.
- VMware API를 활용하는 백업 기술을 사용합니다. 백업 윈도우는 일반 운영 시간을 벗어나야 합니다.

결론

의료 기관은 FlexPod에서 의료 영상 환경을 실행하여 직원 생산성을 높이고 자본 및 운영 비용을 절감할 수 있습니다. FlexPod는 Cisco와 NetApp의 전략적 파트너십을 통해 사전 검증을 거쳐 엄격하게 테스트된 통합 인프라를 제공합니다. 지연 시간이 짧고 예측 가능한 시스템 성능과 고가용성을 제공하도록 특별히 설계되고 제작되었습니다. 이러한 접근 방식은 의료 영상 시스템 사용자에게 우수한 사용자 경험과 최적의 응답 시간을 제공합니다.

의료 이미징 시스템의 여러 구성 요소에는 SMB/CIFS, NFS, ext4 및 NTFS 파일 시스템의 데이터 저장소가 필요합니다. 따라서 인프라는 NFS, SMB/CIFS 및 SAN 프로토콜을 통해 데이터 액세스를 제공해야 합니다. NetApp 스토리지 시스템은 단일 스토리지 어레이에서 이러한 프로토콜을 지원합니다.

고가용성, 스토리지 효율성, 스냅샷 복사본 기반의 예약된 빠른 백업, 빠른 복원 작업, 재해 복구를 위한 데이터 복제 및 FlexPod 스토리지 인프라 기능은 모두 업계 선두의 데이터 스토리지 및 관리 시스템을 제공합니다.

추가 정보

이 문서에 설명된 정보에 대한 자세한 내용은 다음 문서 및 웹 사이트를 참조하십시오.

- 딥 러닝 설계 가이드용 Cisco UCS 480mL가 포함된 AI/ML용 FlexPod 데이터 센터

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_c480m5l_aiml_design.html"

- VMware vSphere 6.7 U1, Cisco UCS 4세대 및 NetApp AFF A-Series를 지원하는 FlexPod 데이터 센터 인프라

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_datacenter_vmware_netappaffa.html"

- FlexPod 데이터 센터 SnapCenter를 사용한 Oracle 데이터베이스 백업 솔루션 개요

  "https://www.netapp.com/us/media/sb-3999.pdf"

- Cisco UCS 및 NetApp AFF A-Series에서 Oracle RAC 데이터베이스가 지원되는 FlexPod 데이터 센터

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_orc12cr2_affaseries.html"

- Oracle Linux 기반 Oracle RAC 지원 FlexPod 데이터 센터

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_orcrac_12c_bm.html"

- Microsoft SQL Server용 FlexPod

  "https://flexpod.com/solutions/use-cases/microsoft-sql-server/"

- Cisco와 NetApp의 FlexPod

  "https://flexpod.com/"

- "MongoDB용 NetApp 솔루션" 솔루션 개요(NetApp 로그인 필요)

  "https://fieldportal.netapp.com/content/734702"

- TR-4700: Oracle 데이터베이스용 SnapCenter 플러그인

  "https://www.netapp.com/us/media/tr-4700.pdf"

- NetApp 제품 설명서

  "https://www.netapp.com/us/documentation/index.aspx"

- 가상 데스크톱 인프라(VDI) 솔루션을 위한 FlexPod

  "https://flexpod.com/solutions/use-cases/virtual-desktop-infrastructure/"

가상 데스크톱 인프라

Citrix Virtual Apps & Desktops 1912 LTSR 및 VMware vSphere 7을 지원하는 FlexPod 데이터 센터(최대 6000개 시트

Jeff Nichols, Cisco Suresh Thoppay, NetApp Dre Jackson, NetApp

이 문서에서는 최대 6000명의 최종 사용자 컴퓨팅 사용자를 위한 가상 데스크톱 인프라의 아키텍처 및 설계를 제공합니다. 이 솔루션은 5세대 Cisco UCS B200 M5 블레이드 서버에서 가상화되어 AFF A400 스토리지 어레이에서 VMware vSphere 7.01 업데이트 1에서 FC SAN으로 부팅됩니다. 가상 데스크톱은 RDS 호스팅 공유 데스크톱(6000), 풀링 및/또는 비영구 호스팅 가상 Windows 10 데스크톱(5000)이 혼합된 Citrix Provisioning Server 1912 LTSR 및 Citrix RDS/Citrix Virtual Apps & Desktops 1912 LTSR을 사용하여 구동됩니다. 사용자 모집단을 지원하기 위해 Citrix Machine Creation Services(5000)를 통해 프로비저닝한 영구 호스팅된 가상 Windows 10 데스크톱입니다. 해당하는 경우 이 문서에서는 이 솔루션의 고객 구축에 대한 모범 사례 권장사항과 사이징 지침을 제공합니다.

"Citrix Virtual Apps amp; Desktops 1912 LTSR 및 VMware vSphere 7을 지원하는 FlexPod 데이터 센터(최대 6000개 시트)"

최대 6700개 시트를 지원하는 VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 및 NetApp ONTAP 9.6을 갖춘 FlexPod 데이터 센터

Vadim Lebedev, Cisco Suresh Thoppay, NetApp

이 문서에서는 FlexPod 데이터 센터(Cisco UCS 및 NetApp AFF A300 및 NetApp ONTAP 데이터 관리 소프트웨어)의 5,000명~6000명 데스크톱 워크로드, 최종 사용자 컴퓨팅 환경에 대한 참조 아키텍처 및 설계 가이드를 제공합니다. 이 솔루션에는 VMware Horizon 서버 기반 RDS Windows Server 2019 세션, VMware Horizon 영구 전체 클론 Microsoft Windows 10 가상 데스크톱, VMware vSphere 6.7U2에서 VMware Horizon 비영구, 즉각적인 클론 Microsoft Windows 10 가상 데스크톱이 포함되어 있습니다

"최대 6700개 시트를 지원하는 VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 및 NetApp ONTAP 9.6을 갖춘 FlexPod 데이터 센터"

Citrix 및 NVIDIA를 통한 3D 그래픽 시각화 - 백서

이 문서에서는 SPECviewperf 13을 사용하는 Cisco UCS C240 M5 및 B200 M5 서버에서 NVIDIA Tesla P4, P6 및 P40 카드를 사용하는 Citrix XenServer 기반 Citrix XenDesktop의 성능에 대해 설명합니다.

"Citrix 및 NVIDIA를 통한 3D 그래픽 시각화 - 백서"

6000개 시트용 Citrix XenDesktop/XenApp 7.15 및 VMware vSphere 6.5 업데이트 1이 설치된 FlexPod Datacenter

Vadim Lebedev, Cisco Chris Rodriguez, NetApp

이 문서에서는 NetApp AFF(All Flash FAS) A300 스토리지, VMware vSphere ESXi 6.5 하이퍼바이저 플랫폼과 함께 Cisco UCS에 구축된 Citrix XenApp/XenDesktop 7.15를 사용하여 가상 데스크톱 및 애플리케이션 설계를 위한 참조 아키텍처를 제공합니다.

데스크톱 및 애플리케이션 가상화 환경은 끊임없이 변화하고 있습니다. 새로운 M5 고성능 Cisco UCS 블레이드 서버와 Cisco UCS Unified Fabric이 FlexPod 검증 인프라의 일부로 결합되어 최신 세대의 NetApp AFF 스토리지가 더욱 콤팩트하고 강력하며 더 안정적이고 효율적인 플랫폼이 되었습니다.

"6000개 시트용 Citrix XenDesktop/XenApp 7.15 및 VMware vSphere 6.5 업데이트 1이 설치된 FlexPod Datacenter"

VMware Horizon View 7.3 및 VMware vSphere 6.5 업데이트 1이 설치된 FlexPod 데이터 센터(5,000개 시트의 경우 Cisco UCS Manager 3.2 포함

Ramesh Guduru, Cisco David Arnette, NetApp

이 문서에서는 Cisco UCS 및 NetApp AFF(All Flash FAS) A300 스토리지가 있는 FlexPod 데이터 센터에서 최대 5000명의 혼합 워크로드를 지원하는 최종 사용자 컴퓨팅 환경에 대한 참조 아키텍처, 설계 가이드 및 구축을 제공합니다. 이 솔루션에는 VMware Horizon 서버 기반 원격 데스크톱 서버 호스팅 세션, VMware Horizon 영구 Microsoft Windows 10 가상 데스크톱, VMware vSphere 6.5의 VMware Horizon 비영구 Microsoft Windows 10 즉각적인 클론 가상 데스크톱이 포함되어 있습니다.

"VMware Horizon View 7.3 및 VMware vSphere 6.5 업데이트 1이 설치된 FlexPod 데이터 센터(5,000개 시트의 경우 Cisco UCS Manager 3.2 포함"

최대 6700개 시트를 지원하는 VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 및 NetApp ONTAP 9.6을 갖춘 FlexPod 데이터 센터

Vadim Lebedev, Cisco Suresh Thoppay, NetApp

이 문서에서는 Cisco UCS 및 NetApp AFF A300 및 NetApp ONTAP 데이터 관리 소프트웨어가 설치된 FlexPod 데이터 센터에서 5,000명 ~ 6000명의 데스크톱 워크로드 최종 사용자 컴퓨팅 환경에 대한 참조 아키텍처 및 설계 가이드를 제공합니다. 이 솔루션에는 VMware Horizon 서버 기반 RDS Windows Server 2019 세션, VMware Horizon 영구, 전체 클론 Microsoft Windows 10 가상 데스크톱, VMware vSphere 6.7 U2 기반의 VMware Horizon 비영구, 즉각적인 클론 Microsoft Windows 10 가상 데스크톱이 포함되어 있습니다.

"최대 6700개 시트를 지원하는 VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 및 NetApp ONTAP 9.6을 갖춘 FlexPod 데이터 센터"

최신 앱

딥 러닝-디자인을 위한 **Cisco UCS 480mL**와 **AI** 및 **ML**을 결합한 **FlexPod** 데이터 센터

Haseeb Niazi, Cisco Arvind Ramakrishnan, NetApp

이 문서에서는 통합 인프라 내에서 AI 및 ML 기능을 제공하기 위한 통합 접근 방식을 제공하기 위해 Cisco UCS C480 ML M5 플랫폼을 FlexPod 데이터 센터 솔루션에 통합하는 작업에 대한 설계 세부 정보를 제공합니다. 고객에게 AI 및 ML 기능을 기존의 FlexPod 시스템을 관리하는 데 사용하는 익숙한 툴과 결합하는 서버를 관리할 수 있는 기능을 제공함으로써 딥 러닝 플랫폼 구축 비용뿐만 아니라 관리 오버헤드를 크게 줄입니다. 이 CVD에 포함된 설계에는 동시 AI 및 ML 워크로드를 위한 추가 옵션으로 2개의 NVIDIA T4 GPU가 장착된 C220 M5 서버 및 2개의 NVIDIA V100 32GB PCIe 카드가 장착된 C240 M5 서버와 같은 다른 Cisco UCS 플랫폼도 포함됩니다.

"딥 러닝-디자인을 위한 Cisco UCS 480mL와 AI 및 ML을 결합한 FlexPod 데이터 센터"

FlexPod을 지원하는 **Cisco** 컨테이너 플랫폼에 **NetApp Trident CSI** 플러그인을 구축하십시오

이 문서에서는 FlexPod 솔루션의 Cisco 컨테이너 플랫폼 Kubernetes 테넌트 클러스터에 NetApp CSI(Trident Container Storage Interface) 플러그인을 구축하는 단계별 절차를 제공합니다.

"FlexPod을 지원하는 Cisco 컨테이너 플랫폼에 NetApp Trident CSI 플러그인을 구축하십시오"

OpenShift Container Platform 4용 **FlexPod** 데이터 센터 **-** 배포

NetApp, Cisco Alan Cowles, Haseeb Niazi

Red Hat OpenShift는 하이브리드 클라우드 및 멀티 클라우드 구현을 관리할 수 있는 엔터프라이즈용 Kubernetes 컨테이너 플랫폼입니다. Red Hat OpenShift Container Platform에는 하이브리드 클라우드, 엔터프라이즈 컨테이너, Kubernetes 개발 및 배포에 필요한 모든 기능이 포함되어 있습니다. 엔터프라이즈급 Linux 운영 체제, 컨테이너 런타임, 네트워킹, 모니터링, 컨테이너 레지스트리, 인증 및 권한 부여 솔루션을 제공합니다.

Red Hat OpenShift를 FlexPod 데이터 센터 솔루션과 결합하면 컨테이너 인프라의 배포 및 관리를 단순화할 수 있습니다. 고객은 효율성 향상, 데이터 보호 향상, 위험 감소, 새로운 비즈니스 요구사항을 수용하기 위해 고가용성 엔터프라이즈급 인프라 스택을 확장할 수 있는 유연성 등의 이점을 누릴 수 있습니다. 조직에서는 사전 검증된 통합 솔루션 접근 방식을 통해 애플리케이션 현대화 및 디지털 혁신 이니셔티브에 필요한 속도, 유연성, 확장성을 실현할 수 있습니다.

"OpenShift Container Platform 4용 FlexPod 데이터 센터 - 배포"

컨테이너 관리용 **Docker Enterprise Edition**을 사용하는 **FlexPod** 데이터 센터

Muhammad Afzal, Cisco John George, Cisco Amit Borulkar, NetApp Uday Shetty, Docker

Docker는 개발자 및 IT 운영 부서에서 분산된 애플리케이션을 어디서나 구축, 배송 및 실행할 수 있는 세계 최고의 소프트웨어 컨테이너 플랫폼입니다. 마이크로서비스 아키텍처로 차세대 IT를 설계하여 모놀리식 애플리케이션에 많은 투자를 한 기업은 애플리케이션 아키텍처를 현대화하고 조직의 경쟁력 및 비용 효율성을 유지하는 전략으로 Docker를 채택할 방법을 모색하고 있습니다. 컨테이너화는 개발자와 IT 운영 부서가 모든 인프라에서 애플리케이션을 구축 및 구축하는 데 필요한 민첩성, 제어 및 이동성을 제공합니다. Docker 플랫폼을 사용하면 분산된 애플리케이션을 운영 중단 없이 동적으로 변경할 수 있는 경량 애플리케이션 컨테이너로 쉽게 구성할 수 있습니다. 이 기능을 통해 애플리케이션을 개발, 테스트 및 프로덕션 환경에서 로컬 또는 가상 시스템에서 실행 중인 환경, 데이터 센터 및 서로 다른 클라우드 서비스 공급업체의 네트워크 전체에서 이식할 수 있습니다.

"컨테이너 관리용 Docker Enterprise Edition을 사용하는 FlexPod 데이터 센터"

OpenShift 컨테이너 플랫폼 **4-Design**용 **FlexPod** 데이터 센터

NetApp, Cisco Alan Cowles, Haseeb Niazi

Cisco와 NetApp은 전략적 데이터 센터 플랫폼을 지원하는 일련의 FlexPod 솔루션을 제공하기 위해 협력하고 있습니다. FlexPod 솔루션은 컴퓨팅, 스토리지 및 네트워크 설계에 대한 모범 사례를 통합하는 통합 아키텍처를 제공하므로 다양한 구성 요소 간의 호환성을 보장하기 위해 통합 아키텍처의 유효성을 검증하여 IT 위험을 최소화할 수 있습니다. 또한 이 솔루션은 배포의 다양한 단계(계획, 설계 및 구현)에서 사용할 수 있는 문서화된 설계 지침, 배포 지침 및 지원을 제공하여 IT 당면 과제를 해결합니다.

"OpenShift 컨테이너 플랫폼 4-Design용 FlexPod 데이터 센터"

Cisco UCS를 통해 **VMware** 및 **NVIDIA**를 이용한 **3D** 그래픽 시각화 **-** 백서

이 문서에서는 Cisco UCS C240 M5 랙 서버 및 B200 M5 블레이드 서버에서 NVIDIA Tesla P4, P6 및 P40 솔루션을 사용한 VMware ESXi 하이퍼바이저 및 VMware Horizon의 성능에 대해 설명합니다.

"Cisco UCS를 통해 VMware 및 NVIDIA를 이용한 3D 그래픽 시각화 - 백서"

Citrix 및 **NVIDIA**를 통한 **3D** 그래픽 시각화 **-** 백서

이 문서에서는 SPECviewperf 13을 사용하는 Cisco UCS C240 M5 및 B200 M5 서버에서 NVIDIA Tesla P4, P6 및 P40 카드를 사용하는 Citrix XenServer 기반 Citrix XenDesktop의

성능에 대해 설명합니다.

"Citrix 및 NVIDIA를 통한 3D 그래픽 시각화 - 백서"

FlexPod 익스프레스

FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series 설계 가이드 를 참조하십시오

NVA-1139-design:FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series

Savita Kumari, NetApp에서 기술 지원

파트너 후원: 

업계 동향에 따르면 많은 데이터 센터가 공유 인프라 및 클라우드 컴퓨팅으로 전환하고 있습니다. 또한 기업에서는 데이터 센터에서 친숙한 기술을 사용하는 원격 사무소 및 지사를 위해 간편하고 효율적인 솔루션을 찾고 있습니다.

FlexPod Express는 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 스위치 제품군, NetApp AFF 시스템을 기반으로 사전 설계되고 모범 사례 데이터 센터 아키텍처입니다. FlexPod Express의 구성 요소는 FlexPod 데이터 센터 구성 요소와 비슷하므로 더 작은 규모로 전체 IT 인프라 환경에서 관리 시너지 효과를 실현할 수 있습니다. FlexPod 데이터 센터 및 FlexPod 익스프레스는 가상화 및 베어 메탈 운영 체제 및 엔터프라이즈 워크로드를 위한 최적의 플랫폼입니다.

"다음: 프로그램 요약."

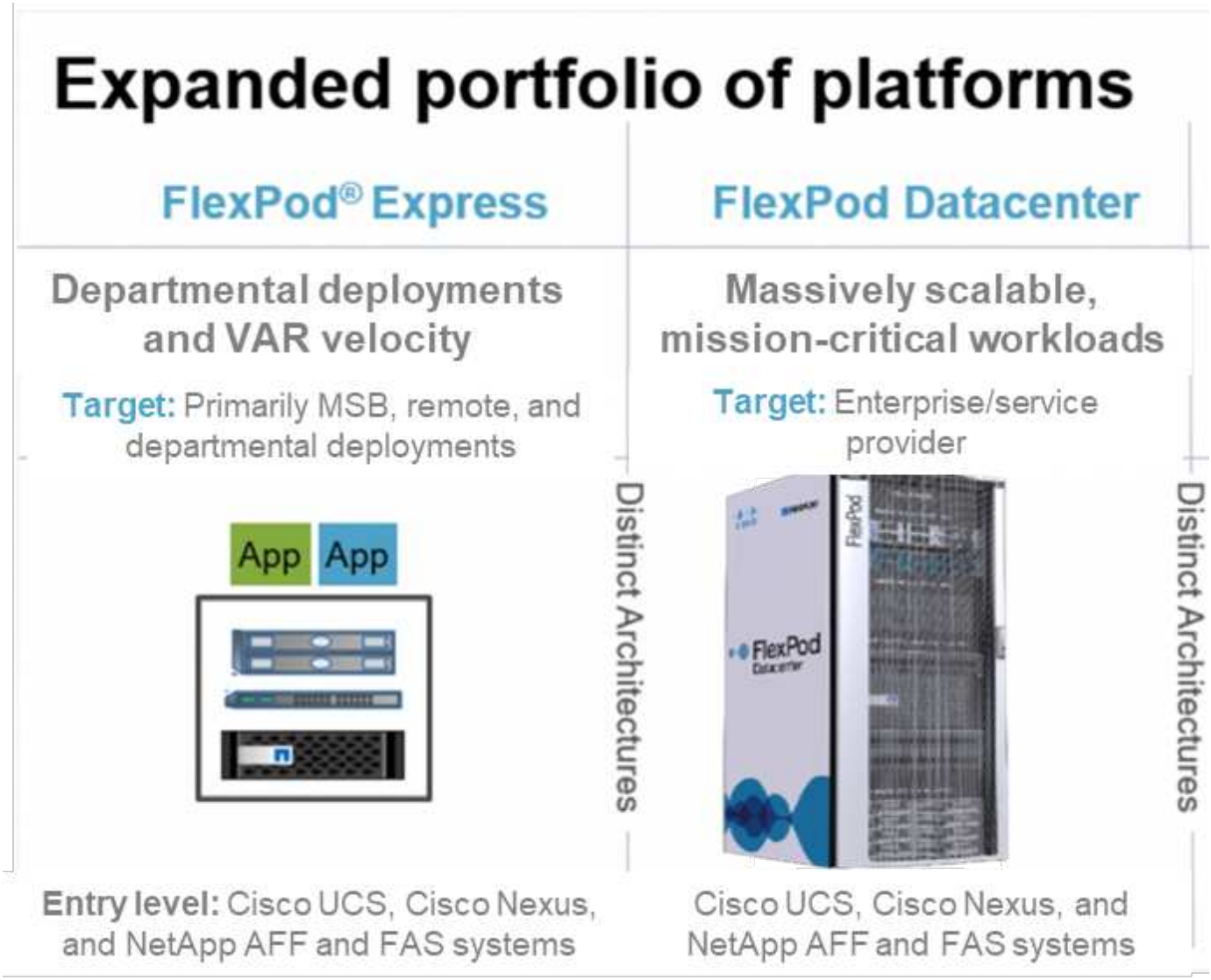
프로그램 요약

FlexPod 통합 인프라 포트폴리오

FlexPod 참조 아키텍처는 CVD(Cisco Validated Design) 또는 NVA(NetApp Verified Architecture)로 제공됩니다. 특정 CVD 또는 NVA의 고객 요구 사항을 기반으로 한 편차는 이러한 변형으로 인해 지원되지 않는 구성이 구축되지 않는 경우 허용됩니다.

다음 그림과 같이 FlexPod 포트폴리오에는 FlexPod 익스프레스 및 FlexPod 데이터 센터 솔루션이 포함되어 있습니다.

- * FlexPod 익스프레스 * 는 Cisco 및 NetApp의 기술을 사용하는 엔트리 레벨 솔루션입니다.
- * FlexPod 데이터 센터 * 는 다양한 워크로드 및 애플리케이션을 위한 최적의 다목적 토대를 제공합니다.



NetApp 검증 아키텍처 프로그램

NetApp 검증 아키텍처 프로그램에서는 NetApp 솔루션을 위한 검증된 아키텍처를 고객에게 제공합니다. NVA 솔루션의 특징은 다음과 같습니다.

- 철저한 테스트를 거친 아키텍처
- 기본적으로 규범적인 아키텍처
- 구축 위험 최소화
- 출시 시간 단축 이 가이드는 VMware vSphere를 사용한 FlexPod Express 설계에 대해 자세히 설명합니다.

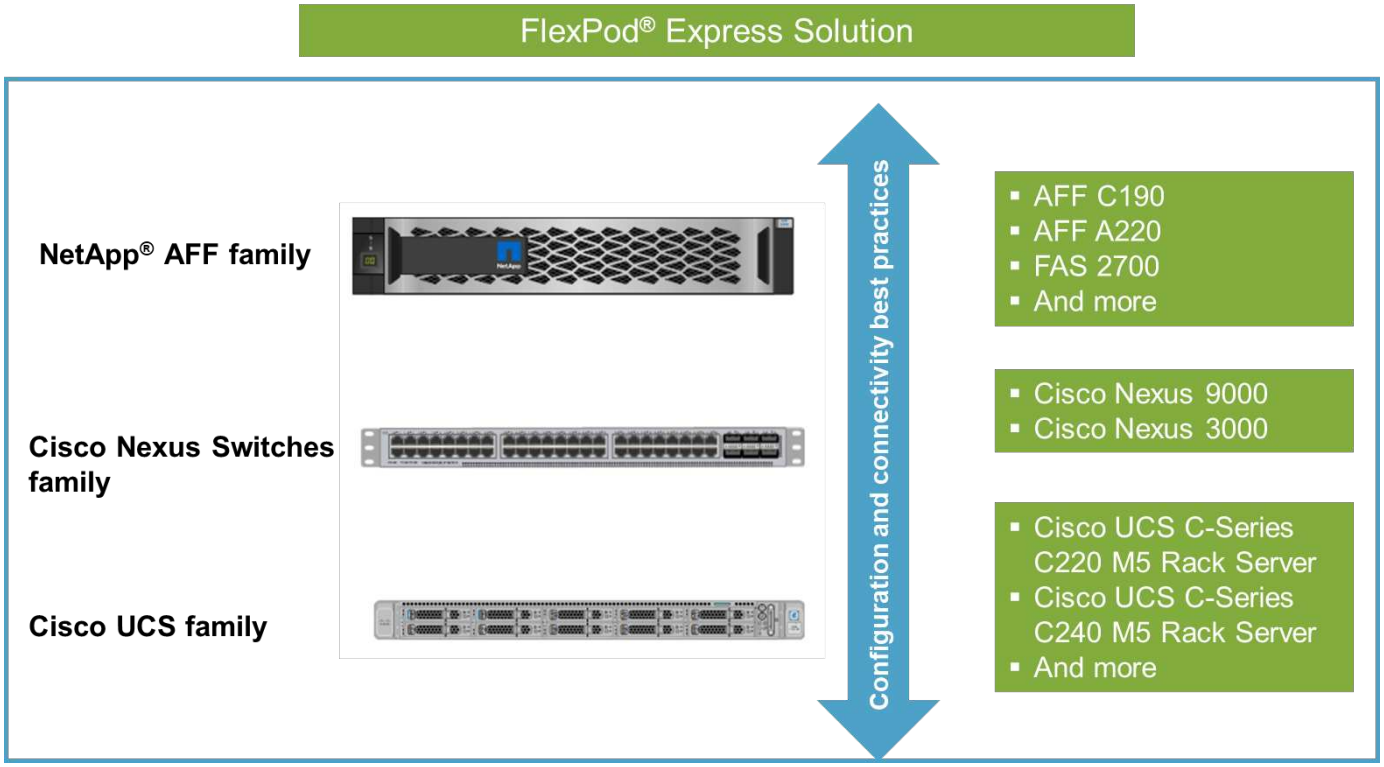
또한, 이 설계에서는 NetApp ONTAP 9.6 소프트웨어, Cisco Nexus 31108 스위치 및 Cisco UCS C220 M5 서버를 하이퍼바이저 노드로 실행하는 완전히 새로운 AFF C190 시스템을 활용합니다.

솔루션 개요

FlexPod Express는 혼합 가상화 워크로드를 실행하도록 설계되었습니다. 원격 사무소, 지점 및 중소 및 중견 기업을 타겟으로 합니다. 또한 특정 목적에 맞는 전용 솔루션을 구현하려는 대규모 기업에도 적합합니다. FlexPod 익스프레스를 위한 이 새로운 솔루션은 NetApp ONTAP 9.6, NetApp AFF C190 시스템 및 VMware vSphere

6.7U2와 같은 새로운 기술을 추가합니다.

다음 그림에서는 FlexPod Express 솔루션에 포함된 하드웨어 구성 요소를 보여 줍니다.

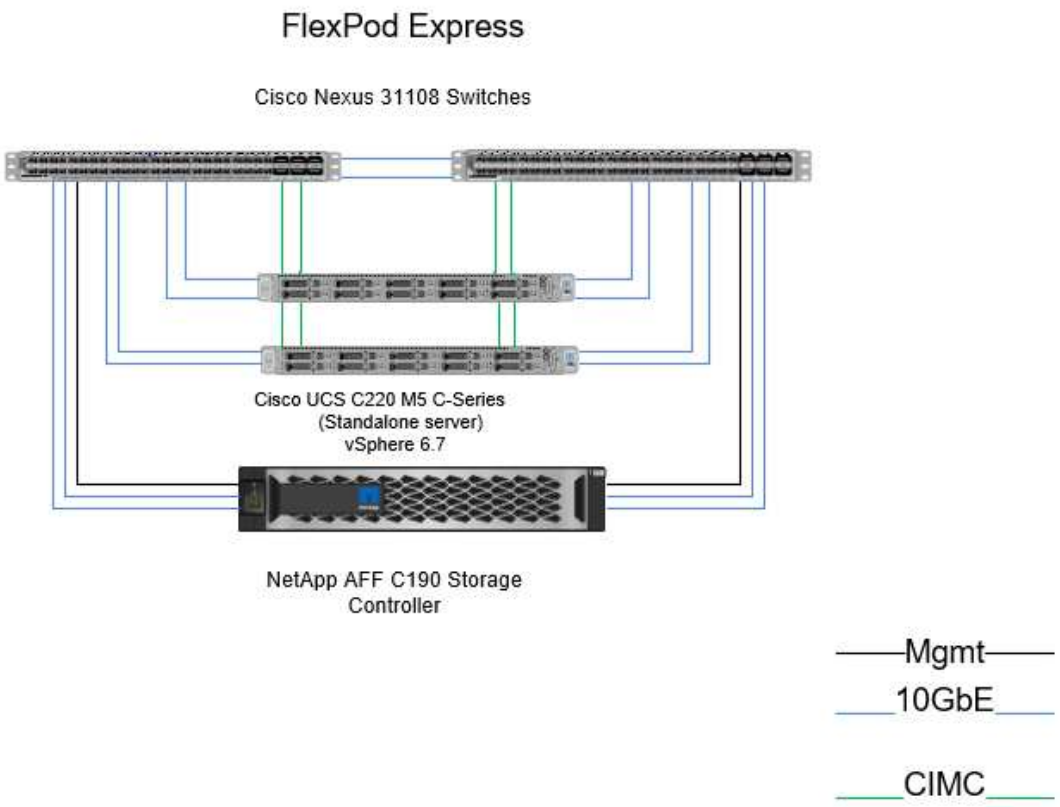


대상

이 문서는 IT 효율성을 제공하고 IT 혁신을 지원하기 위해 구축된 인프라를 활용하려는 사용자를 위해 작성되었습니다. 이 문서의 대상에는 세일즈 엔지니어, 현장 컨설턴트, 프로페셔널 서비스 직원, IT 매니저, 파트너 엔지니어 및 고객.

솔루션 기술

이 솔루션은 NetApp, Cisco 및 VMware의 최신 기술을 활용합니다. 이 제품은 ONTAP 9.6 소프트웨어, 이중 Cisco Nexus 31108 스위치 및 VMware vSphere 6.7U2를 실행하는 Cisco UCS C220 M5 랙 서버를 실행하는 새로운 NetApp AFF C190 시스템을 갖추고 있습니다. 다음 그림에 나와 있는 검증된 이 솔루션은 10기가비트 이더넷(10GbE) 기술을 사용합니다. 또한 FlexPod 익스프레스 아키텍처가 조직의 변화하는 비즈니스 요구에 적응할 수 있도록 한 번에 두 개의 하이퍼바이저 노드를 추가하여 확장하는 방법에 대한 지침도 제공됩니다.



"다음: 기술 요구 사항."

기술 요구 사항

FlexPod Express를 사용하려면 선택한 하이퍼바이저와 네트워크 속도에 따라 하드웨어 및 소프트웨어 구성요소를 조합해야 합니다. 또한 FlexPod Express는 하이퍼바이저 노드를 시스템에 추가하는 데 필요한 하드웨어 구성요소를 2개 단위로 배치합니다.

하드웨어 요구 사항

선택한 하이퍼바이저에 관계없이 모든 FlexPod Express 구성은 동일한 하드웨어를 사용합니다. 따라서 비즈니스 요구사항이 변경되더라도 동일한 FlexPod Express 하드웨어에서 다른 하이퍼바이저를 사용할 수 있습니다.

다음 표에는 이 FlexPod Express 구성과 이 솔루션 구축에 필요한 하드웨어 구성요소가 나와 있습니다. 솔루션 구현에 사용되는 하드웨어 구성요소는 고객 요구사항에 따라 다를 수 있습니다.

하드웨어	수량
AFF C190 2노드 클러스터	1
Cisco UCS C220 M5 서버	2
Cisco Nexus 31108 스위치	2
Cisco UCS C220 M5 랙 서버용 Cisco UCS VIC(Virtual Interface Card) 1457	2

소프트웨어 요구 사항

다음 표에는 FlexPod 익스프레스 솔루션의 아키텍처를 구현하는 데 필요한 소프트웨어 구성 요소가 나열되어 있습니다.

소프트웨어	버전	세부 정보
CIMC(Cisco Integrated Management Controller)	4.0.4	C220 M5 랙 서버용
Cisco NX-OS입니다	7.0(3) i7(6)	Cisco Nexus 31108 스위치의 경우
NetApp ONTAP를 참조하십시오	9.6	NetApp AFF C190 컨트롤러의 경우

다음 표에는 FlexPod Express의 모든 VMware vSphere 구축에 필요한 소프트웨어가 나와 있습니다.

소프트웨어	버전
VMware vCenter Server 어플라이언스	6.7U2
VMware vSphere ESXi	6.7U2
ESXi용 NetApp VAAI 플러그인	1.1.2
NetApp 가상 스토리지 콘솔	9.6

"다음: 디자인 선택."

디자인 선택

이 섹션에 나열된 기술은 아키텍처 설계 단계에서 선택되었습니다. 각 기술은 FlexPod 익스프레스 인프라 솔루션에서 특정 목적에 부합합니다.

ONTAP 9.6이 설치된 **NetApp AFF C190** 시리즈

이 솔루션은 NetApp AFF C190 시스템 및 ONTAP 9.6 소프트웨어의 최신 NetApp 제품 중 2개를 활용합니다.

AFF C190 시스템

대상 그룹은 경제적인 가격으로 All-Flash 기술로 IT 인프라를 현대화하려는 고객입니다. AFF C190 시스템은 새로운 ONTAP 9.6 및 플래시 번들 라이센스와 함께 제공됩니다. 즉, 다음 기능이 탑재되어 있습니다.

- CIFS, NFS, iSCSI 및 FCP
- NetApp SnapMirror 데이터 복제 소프트웨어, NetApp SnapVault 백업 소프트웨어, NetApp SnapRestore 데이터 복구 소프트웨어, NetApp SnapManager 스토리지 관리 소프트웨어 제품군 및 NetApp SnapCenter 소프트웨어
- FlexVol 기술
- 중복제거, 압축, 컴팩션
- 씬 프로비저닝
- 스토리지 QoS
- NetApp RAID DP 기술
- NetApp Snapshot 기술

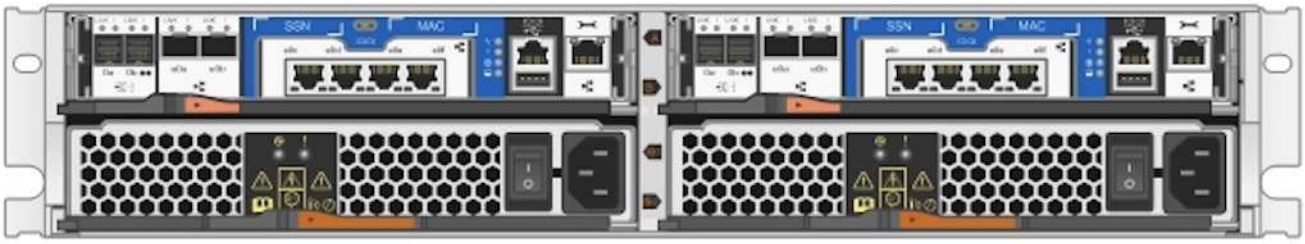
- FabricPool

다음 그림은 호스트 접속에 대한 두 가지 옵션을 보여 줍니다.

다음 그림에서는 SFP+ 모듈을 삽입할 수 있는 UTA 2 포트를 보여 줍니다.



다음 그림은 기존 RJ-45 이더넷 케이블을 통한 연결을 위한 10GBASE-T 포트를 보여줍니다.



10GBASE-T 포트 옵션의 경우 10GBASE-T 기반 업링크 스위치가 있어야 합니다.

AFF C190 시스템은 960GB SSD에서만 제공됩니다. 다음 네 가지 확장 단계를 선택할 수 있습니다.

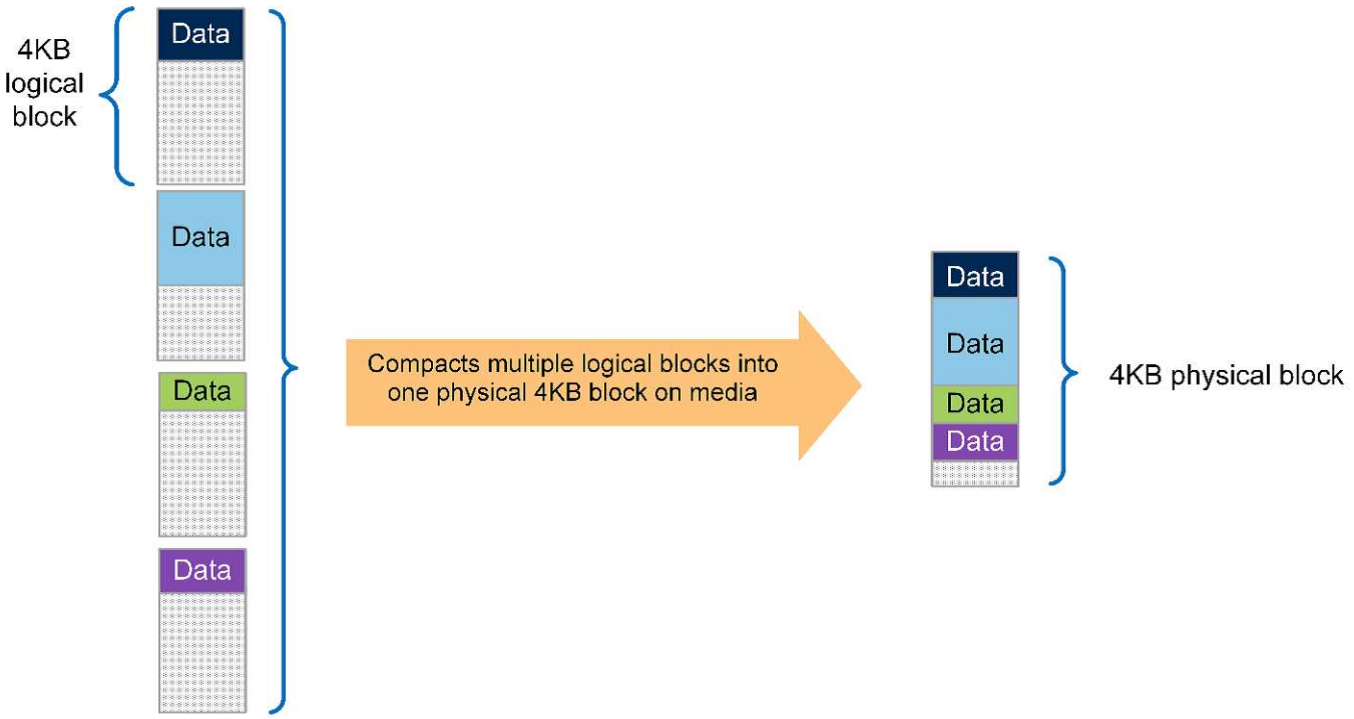
- 8x 960GB
- 12x 960GB
- 18x 960GB
- 24x 960GB

AFF C190 하드웨어 시스템에 대한 자세한 내용은 를 참조하십시오 "NetApp AFF C190 All-Flash 어레이 페이지".

ONTAP 9.6 소프트웨어

NetApp AFF C190 시스템은 새로운 ONTAP 9.6 데이터 관리 소프트웨어를 사용합니다. ONTAP 9.6은 업계 최고의 엔터프라이즈 데이터 관리 소프트웨어입니다. 새로운 버전에는 새로운 수준의 단순성과 유연성, 강력한 데이터 관리 기능, 스토리지 효율성, 업계 최고 수준의 클라우드 통합이 결합되어 있습니다.

ONTAP 9.6에는 FlexPod 익스프레스 솔루션에 적합한 여러 가지 기능이 있습니다. 가장 중요한 것은 NetApp이 스토리지 효율성을 위해 노력하고 있다는 점입니다. 이는 소규모 구축에 있어서 가장 중요한 기능 중 하나입니다. 중복제거, 압축, 컴팩션, 씬 프로비저닝 같은 NetApp 스토리지 효율성 기능의 특징은 ONTAP 9.6에서 확인할 수 있습니다. NetApp WAFL 시스템은 항상 4KB 블록을 씁니다. 블록이 4KB의 할당된 공간을 사용하지 않을 때 다중 블록을 4KB 블록으로 결합합니다. 다음 그림에서는 이 프로세스를 보여 줍니다.



ONTAP 9.6은 이제 NVMe 볼륨의 선택적 512바이트 블록 크기를 지원합니다. 이 기능은 기본적으로 512바이트 블록을 사용하는 VMware VMFS(Virtual Machine File System)에서 원활하게 작동합니다. 기본 4K 크기를 그대로 사용하거나 512바이트 블록 크기를 선택적으로 설정할 수 있습니다.

ONTAP 9.6의 기타 향상된 기능은 다음과 같습니다.

- * NetApp Aggregate Encryption(NAE). * NAE는 애그리게이트 레벨에서 키를 할당하며, 따라서 애그리게이트의 모든 볼륨을 암호화합니다. 이 기능을 사용하면 볼륨을 애그리게이트 레벨에서 암호화 및 중복제거할 수 있습니다.
- NetApp ONTAP FlexGroup 볼륨 개선 *. ONTAP 9.6에서는 FlexGroup 볼륨의 이름을 쉽게 변경할 수 있습니다. 데이터를 로 마이그레이션하기 위해 새 볼륨을 생성할 필요가 없습니다. ONTAP 시스템 관리자 또는 CLI를 사용하여 볼륨 크기를 줄일 수도 있습니다.
- * FabricPool 개선. * ONTAP 9.6은 오브젝트 저장소를 클라우드 계층으로 추가로 지원합니다. 또한 Google Cloud 및 Alibaba Cloud Object Storage Service(OSS)에 대한 지원도 목록에 추가되었습니다. FabricPool은 AWS S3, Azure Blob, IBM Cloud 오브젝트 스토리지 및 NetApp StorageGRID 오브젝트 기반 스토리지 소프트웨어를 비롯한 여러 오브젝트 저장소를 지원합니다.
- SnapMirror 향상 기능 * ONTAP 9.6에서는 소스 어레이를 떠나기 전에 새 볼륨 복제 관계가 기본적으로 암호화되고 SnapMirror 대상에서 암호가 해독됩니다.

Cisco Nexus 3000 시리즈

Cisco Nexus 31108PC-V는 48개의 SFP+ 포트와 6개의 QSFP28 포트를 갖춘 10Gbps SFP+ 기반 ToR(Top-of-Rack) 스위치입니다. 각 SFP+ 포트는 100Mbps, 10Gbps 속도에서 작동할 수 있으며, 각 QSFP28 포트는 네이티브 100Gbps 또는 40Gbps 모드 또는 4x 10Gbps 모드로 작동할 수 있어 유연한 마이그레이션 옵션을 제공합니다. 이 스위치는 짧은 지연 시간과 낮은 전력 소비에 최적화된 진정한 PHY 없는 스위치입니다.

Cisco Nexus 31108PC-V 사양에는 다음 구성 요소가 포함됩니다.

- 31108PC-V에서 최대 1.2Tbps의 스위칭 용량 및 포워딩 속도 2.16Tbps
- 48개의 SFP 포트는 1 및 10기가비트 이더넷(10GbE)을 지원하며, 6개의 QSFP28 포트는 각각 4개의 10GbE

또는 40GbE 또는 100GbE를 지원합니다

다음 그림은 Cisco Nexus 31108PC-V 스위치입니다.



Cisco Nexus 31108PC-V 스위치에 대한 자세한 내용은 을 참조하십시오 "Cisco Nexus 3172PQ, 3172TQ, 3172TQ-32T, 3172PQ-XL 및 3172TQ-XL 스위치 데이터 시트".

Cisco UCS C-Series 를 참조하십시오

FlexPod 익스프레스 구축에서는 다양한 구성 옵션으로 Cisco UCS C-Series 랙 서버를 FlexPod 익스프레스 설치시 특정 요구사항에 맞게 구성할 수 있기 때문에 Cisco UCS C-Series 랙 서버를 선택했습니다.

Cisco UCS C-Series 랙 서버는 업계 표준 폼 팩터에서 유니파이드 컴퓨팅을 제공하여 TCO를 절감하고 민첩성을 향상합니다.

Cisco UCS C-Series 랙 서버는 다음과 같은 이점을 제공합니다.

- Cisco UCS의 폼 팩터 중립적인 엔트리 레벨
- 애플리케이션을 간편하고 신속하게 구축
- 통합 컴퓨팅 혁신 및 이점을 랙 서버로 확장
- 친숙한 랙 패키지의 고유한 이점을 통해 고객의 선택 옵션 증가

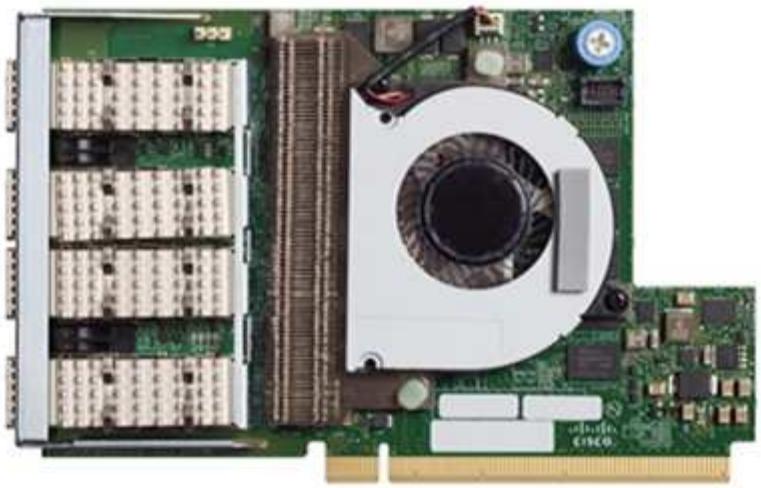


위 그림에 표시된 Cisco UCS C220 M5 랙 서버는 업계에서 가장 다양한 범용 엔터프라이즈 인프라 및 애플리케이션 서버 중 하나입니다. 이 서버는 가상화, 협업 및 베어 메탈 애플리케이션을 비롯하여 광범위한 워크로드에 업계 최고의 성능과 효율성을 제공하는 고밀도 2소켓 랙 서버입니다. Cisco UCS C-Series 랙 서버는 독립형 서버로 또는 Cisco UCS의 일부로 구축할 수 있으므로 Cisco의 표준 기반 통합 컴퓨팅 혁신 기술을 활용하여 고객의 TCO를 절감하고 비즈니스 민첩성을 높일 수 있습니다.

C220 M5 서버에 대한 자세한 내용은 를 참조하십시오 "Cisco UCS C220 M5 랙 서버 데이터 시트".

C220 M5 랙 서버용 **Cisco UCS VIC 1457** 연결

다음 그림에 표시된 Cisco UCS VIC 1457 어댑터는 M5 세대의 Cisco UCS C-Series 서버용으로 설계된 4중 포트 소형 폼 팩터 플러그 가능(SFP28) 모듈식 마더보드 LAN(mLOM) 카드입니다. 이 카드는 10/25Gbps 이더넷 또는 FCoE를 지원합니다. 이 카드는 PCIe 표준 호환 인터페이스를 호스트에 제공할 수 있으며, NIC 또는 HBA로 동적으로 구성할 수 있습니다.



Cisco UCS VIC 1457 어댑터에 대한 자세한 내용은 를 참조하십시오 "Cisco UCS 가상 인터페이스 카드 1400 시리즈 데이터 시트".

VMware vSphere 6.7U2

VMware vSphere 6.7U2는 FlexPod Express에서 사용할 수 있는 하이퍼바이저 옵션 중 하나입니다. VMware vSphere를 사용하면 구입한 컴퓨팅 용량을 최대한 활용하는 동시에 전력 및 냉각 설치 공간을 줄일 수 있습니다. 또한 VMware vSphere를 사용하면 vSphere 호스트 클러스터(유지 관리 모드의 VMware Distributed Resource Scheduler 또는 VMware DRS-MM)에서 하드웨어 장애 보호(VMware High Availability 또는 VMware HA)와 컴퓨팅 리소스 로드 밸런싱을 수행할 수 있습니다.

커널만 다시 시작하므로 VMware vSphere 6.7U2를 사용하면 하드웨어를 다시 시작하지 않고도 vSphere ESXi를 로드하여 빠르게 부팅할 수 있습니다. vSphere 6.7U2 vSphere 클라이언트(HTML5 기반 클라이언트)에는 코드 캡처 및 API 탐색을 지원하는 개발자 센터와 같은 몇 가지 새로운 개선 사항이 있습니다. 코드 캡처를 사용하면 vSphere Client에 작업을 기록하여 간단하고 사용 가능한 코드 출력을 제공할 수 있습니다. vSphere 6.7U2에는 DRS와 같은 새로운 기능이 유지 보수 모드(DRS-mm)에 포함되어 있습니다.

VMware vSphere 6.7U2는 다음과 같은 기능을 제공합니다.

- VMware는 외부 VMware PSC(Platform Services Controller) 구축 모델을 더 이상 사용하지 않습니다.

  다음 주요 vSphere 릴리즈부터는 외부 PSC를 사용할 수 없습니다.

- vCenter Server 어플라이언스 백업 및 복구를 위한 새로운 프로토콜 지원 지원되는 프로토콜 선택 사항으로 NFS 및 SMB 소개, 최대 총 7개(HTTP, HTTPS, FTP, FTPS, SCP, NFS 및 SMB) - 파일 기반 백업 또는 복구 작업을 위해 vCenter Server를 구성할 때 필요합니다.
- 콘텐츠 라이브러리 사용 시 새로운 기능. 이제 vCenter Server가 향상된 연결 모드로 구성되어 있으면 컨텐츠 라이브러리 간에 네이티브 VM 템플릿 동기화를 사용할 수 있습니다.
- 로 업데이트합니다 "클라이언트 플러그인 페이지".
- VMware vSphere Update Manager는 vSphere Client에도 향상된 기능을 추가합니다. 한 화면에서 연결 확인 규정 준수를 수행하고 조치를 수정할 수 있습니다.

VMware vSphere 6.7 U2에 대한 자세한 내용은 를 참조하십시오 "VMware vSphere 블로그 페이지를 참조하십시오".

VMware vCenter Server 6.7 U2 업데이트에 대한 자세한 내용은 를 참조하십시오 "릴리즈 노트".

이 솔루션은 vSphere 6.7U2에서 검증되었지만 에서 다른 구성 요소에 대해 검증된 모든 vSphere 버전을 지원합니다 "NetApp 상호 운용성 매트릭스 툴(IMT)". NetApp은 수정 및 향상된 기능을 위해 다음 버전의 vSphere를 구축할 것을 권장합니다.

부트 아키텍처

FlexPod 익스프레스 부트 아키텍처에서 지원되는 옵션은 다음과 같습니다.

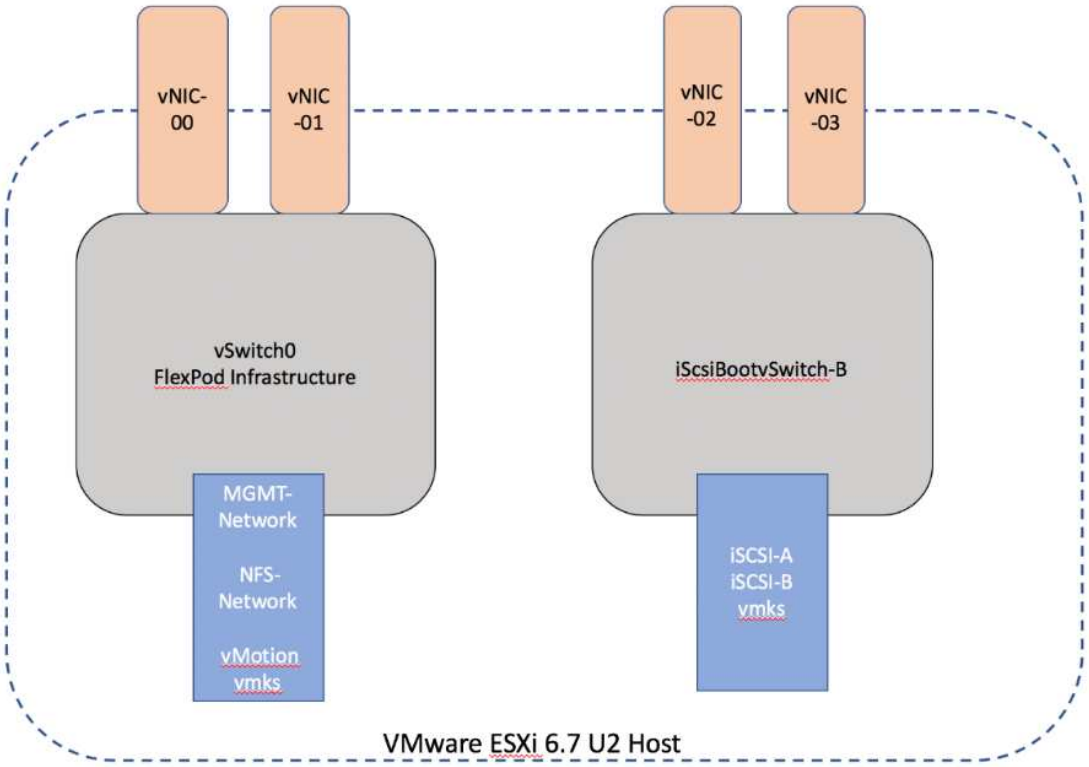
- iSCSI SAN LUN 을 선택합니다
- Cisco FlexFlash SD 카드
- 로컬 디스크

FlexPod 데이터 센터는 iSCSI LUN에서 부팅되므로 FlexPod 익스프레스를 위한 iSCSI 부트를 사용하여 솔루션 관리성이 향상됩니다.

ESXi 호스트 가상 네트워크 인터페이스 카드 레이아웃

Cisco UCS VIC 1457에는 4개의 물리적 포트가 있습니다. 이 솔루션 검증에는 ESXi 호스트를 사용할 때 이러한 4개의 물리적 포트가 포함되어 있습니다. NIC 수가 더 작거나 큰 경우 VMNIC 번호가 다를 수 있습니다.

iSCSI 부트 구현에서 iSCSI 부트는 iSCSI 부트를 위해 별도의 vNIC(Virtual Network Interface Card)가 필요합니다. 이러한 vNIC는 적절한 패브릭의 iSCSI VLAN을 기본 VLAN으로 사용하며 다음 그림과 같이 iSCSI 부트 vSwitch에 연결됩니다.



"다음: 결론."

결론

FlexPod Express의 검증된 설계는 업계 최고 수준의 구성 요소를 사용하는 간단하고 효율적인 솔루션입니다. FlexPod Express는 하이퍼바이저 플랫폼을 위한 확장 및 제공 옵션을 제공하여 특정 비즈니스 요구에 맞게 조정할 수 있습니다. FlexPod Express는 중소 및 중견 기업, 원격 사무소, 지사 및 전용 솔루션이 필요한 기타 기업을 위해 설계되었습니다.

"다음: 추가 정보를 찾을 위치."

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대한 자세한 내용은 다음 문서 및 웹 사이트를 참조하십시오.

- AFF and FAS 시스템 설명서 센터 를 참조하십시오

  "https://docs.netapp.com/platstor/index.jsp"

- AFF 문서 리소스 페이지

  "https://www.netapp.com/us/documentation/all-flash-fas.aspx"

- FlexPod Express with VMware vSphere 6.7 및 NetApp AFF C190 구축 가이드(진행 중)
- NetApp 설명서

  "https://docs.netapp.com"

FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series 구축 가이드 를 참조하십시오

NVA-1142-deploy: FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series-NVA Deployment

Savita Kumari, NetApp에서 기술 지원

업계 동향에 따르면 많은 데이터 센터가 공유 인프라 및 클라우드 컴퓨팅으로 전환하고 있습니다. 또한 기업에서는 데이터 센터에 친숙한 기술을 사용하는 원격 사무소 및 지사를 위해 간편하고 효율적인 솔루션을 찾고 있습니다.

FlexPod ® Express는 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 스위치 제품군, NetApp ® 스토리지 기술을 기반으로 사전 설계되고 모범 사례 데이터 센터 아키텍처입니다. FlexPod 익스프레스 시스템의 구성요소는 FlexPod 데이터 센터와 비슷하기 때문에 더 작은 규모로 전체 IT 인프라 환경에서 관리 시너지 효과를 실현할 수 있습니다. FlexPod 데이터 센터 및 FlexPod 익스프레스는 가상화 및 베어 메탈 운영 체제 및 엔터프라이즈 워크로드를 위한 최적의 플랫폼입니다.

FlexPod 데이터 센터 및 FlexPod 익스프레스는 기본 구성을 제공하며 다양한 사용 사례 및 요구 사항을 수용할 수 있도록 크기를 조정할 수 있는 유연성을 갖추고 있습니다. 기존 FlexPod 데이터 센터 고객은 익숙한 툴을 사용하여 FlexPod 익스프레스 시스템을 관리할 수 있습니다. 새로운 FlexPod Express 고객은 환경 확장에 따라 FlexPod 데이터 센터 관리로 쉽게 전환할 수 있습니다.

FlexPod Express는 원격 사무소, 지점 및 중소기업을 위한 최적의 인프라 기반입니다. 전용 워크로드에 대한 인프라를 제공하려는 고객에게 최적의 솔루션입니다.

FlexPod Express는 거의 모든 워크로드에 적합한 관리하기 쉬운 인프라를 제공합니다.

솔루션 개요

이 FlexPod 익스프레스 솔루션은 FlexPod 통합 인프라 프로그램의 일부입니다.

FlexPod 통합 인프라 프로그램

FlexPod 참조 아키텍처는 CVD(Cisco Validated Design) 또는 NVA(NetApp Verified Architecture)로 제공됩니다. 지정된 CVD 또는 NVA의 고객 요구 사항에 따른 편차는 이러한 변형으로 지원되지 않는 구성이 생성되지는 않을 경우 허용됩니다.

FlexPod 프로그램에는 FlexPod 익스프레스 및 FlexPod 데이터 센터의 두 가지 솔루션이 포함되어 있습니다.

- * FlexPod 익스프레스. * 는 Cisco 및 NetApp의 기술을 갖춘 엔트리 레벨 솔루션을 고객에게 제공합니다.
- * FlexPod 데이터 센터 * 는 다양한 워크로드 및 애플리케이션을 위한 최적의 다목적 토대를 제공합니다.



NetApp 검증 아키텍처 프로그램

NetApp 검증 아키텍처 프로그램에서는 NetApp 솔루션을 위한 검증된 아키텍처를 고객에게 제공합니다. NetApp 검증 아키텍처는 다음과 같은 품질의 NetApp 솔루션 아키텍처를 제공합니다.

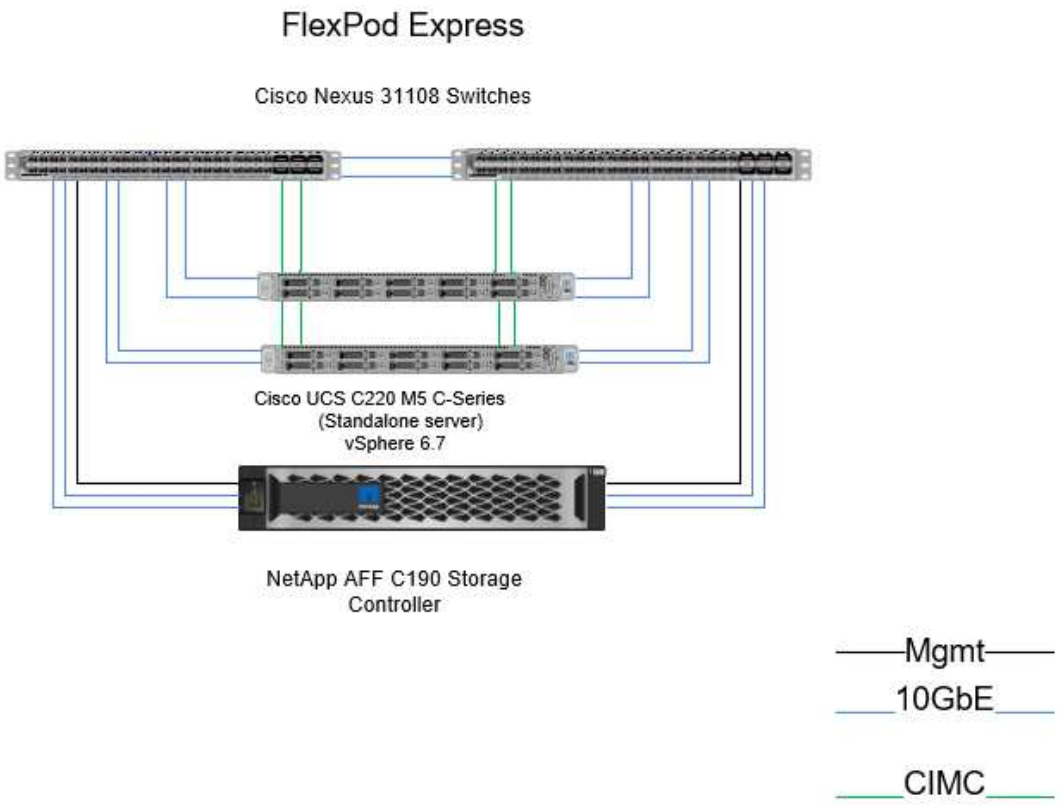
- 철저한 테스트
- 기본적으로 규범적인 아키텍처
- 구축 위험 최소화
- 시장 출시 기간 단축

이 가이드에서는 VMware vSphere를 사용한 FlexPod Express 설계에 대해 자세히 설명합니다. 또한 이 설계에서는 완전히 새로운 AFF C190 시스템(NetApp ONTAP ® 9.6 실행), Cisco Nexus 31108 및 Cisco UCS C-Series C220 M5 서버를 하이퍼바이저 노드로 사용합니다.

솔루션 기술

이 솔루션은 NetApp, Cisco 및 VMware의 최신 기술을 활용합니다. 이 솔루션에는 ONTAP 9.6, 이중 Cisco Nexus

31108 스위치 및 VMware vSphere 6.7U2를 실행하는 Cisco UCS C220 M5 랙 서버를 실행하는 새로운 NetApp AFF C190이 포함되어 있습니다. 이 검증된 솔루션은 10GbE 기술을 사용합니다. 또한 FlexPod 익스프레스 아키텍처가 조직의 변화하는 비즈니스 요구에 적응할 수 있도록 한 번에 두 개의 하이퍼바이저 노드를 추가하여 컴퓨팅 용량을 확장하는 방법에 대한 지침도 제공됩니다.



VIC 1457에서 4개의 물리적 10GbE 포트를 효율적으로 사용하려면 각 서버에서 상단 랙 스위치까지 2개의 추가 링크를 생성하십시오.

사용 사례 요약

FlexPod 익스프레스 솔루션은 다음과 같은 여러 사용 사례에 적용할 수 있습니다.

- 원격 사무소 또는 지점 사무소
- 중소기업
- 비용 효율적인 전용 솔루션이 필요한 환경

FlexPod Express는 가상화된 혼합 워크로드에 가장 적합합니다. 이 솔루션은 vSphere 6.7U2에서 검증되었지만 NetApp Interoperability Matrix Tool에 의해 다른 구성 요소와 함께 검증된 모든 vSphere 버전을 지원합니다. 다음과 같은 수정 사항 및 향상된 기능 때문에 vSphere 6.7U2를 구축하는 것이 좋습니다.

- HTTP, HTTPS, FTP, FTPS 등 vCenter Server Appliance 백업 및 복원을 위한 새로운 프로토콜 지원 SCP, NFS 및 SMB
- 콘텐츠 라이브러리를 활용할 때 새로운 기능을 제공합니다. 이제 vCenter Server가 향상된 연결 모드로 구성되어

있으면 컨텐츠 라이브러리 간에 네이티브 VM 템플릿을 동기화할 수 있습니다.

- 업데이트된 클라이언트 플러그인 페이지.
- VUM(vSphere Update Manager) 및 vSphere Client에 향상된 기능이 추가되었습니다. 이제 한 화면에서 연결, 규정 준수 확인 및 수정 작업을 모두 수행할 수 있습니다.

이 주제에 대한 자세한 내용은 를 참조하십시오 "vSphere 6.7U2 페이지" 및 "vCenter Server 6.7U2 릴리즈 노트".

기술 요구 사항

FlexPod 익스프레스 시스템에는 하드웨어 및 소프트웨어 구성 요소의 조합이 필요합니다. 또한 FlexPod Express는 하이퍼바이저 노드를 시스템에 추가하는 데 필요한 하드웨어 구성요소를 2개 단위로 설명합니다.

하드웨어 요구 사항

선택한 하이퍼바이저에 관계없이 모든 FlexPod Express 구성은 동일한 하드웨어를 사용합니다. 따라서 비즈니스 요구사항이 변경되더라도 동일한 FlexPod Express 하드웨어에서 다른 하이퍼바이저를 사용할 수 있습니다.

다음 표에는 FlexPod Express 구성 및 구축에 필요한 하드웨어 구성요소가 나와 있습니다. 솔루션 구현에 사용되는 하드웨어 구성요소는 고객 요구사항에 따라 다를 수 있습니다.

하드웨어	수량
AFF C190 2노드 클러스터	1
Cisco C220 M5 서버	2
Cisco Nexus 31108PC-V 스위치	2
Cisco UCS C220 M5 랙 서버용 Cisco UCS VIC(가상 인터페이스 카드) 1457	2

이 표에는 10GbE 구현을 위한 기본 구성 외에 필요한 하드웨어가 나와 있습니다.

하드웨어	수량
Cisco UCS C220 M5 서버	2
Cisco VIC 1457	2

소프트웨어 요구 사항

다음 표에는 FlexPod 익스프레스 솔루션의 아키텍처를 구현하는 데 필요한 소프트웨어 구성 요소가 나열되어 있습니다.

소프트웨어	버전	세부 정보
CIMC(Cisco Integrated Management Controller)	4.0.4	Cisco UCS C220 M5 랙 서버용
Cisco nenic 드라이버	1.0.0.29	VIC 1457 인터페이스 카드용
Cisco NX-OS입니다	7.0(3) i7(6)	Cisco Nexus 31108PC-V 스위치용
NetApp ONTAP를 참조하십시오	9.6	AFF C190 컨트롤러의 경우

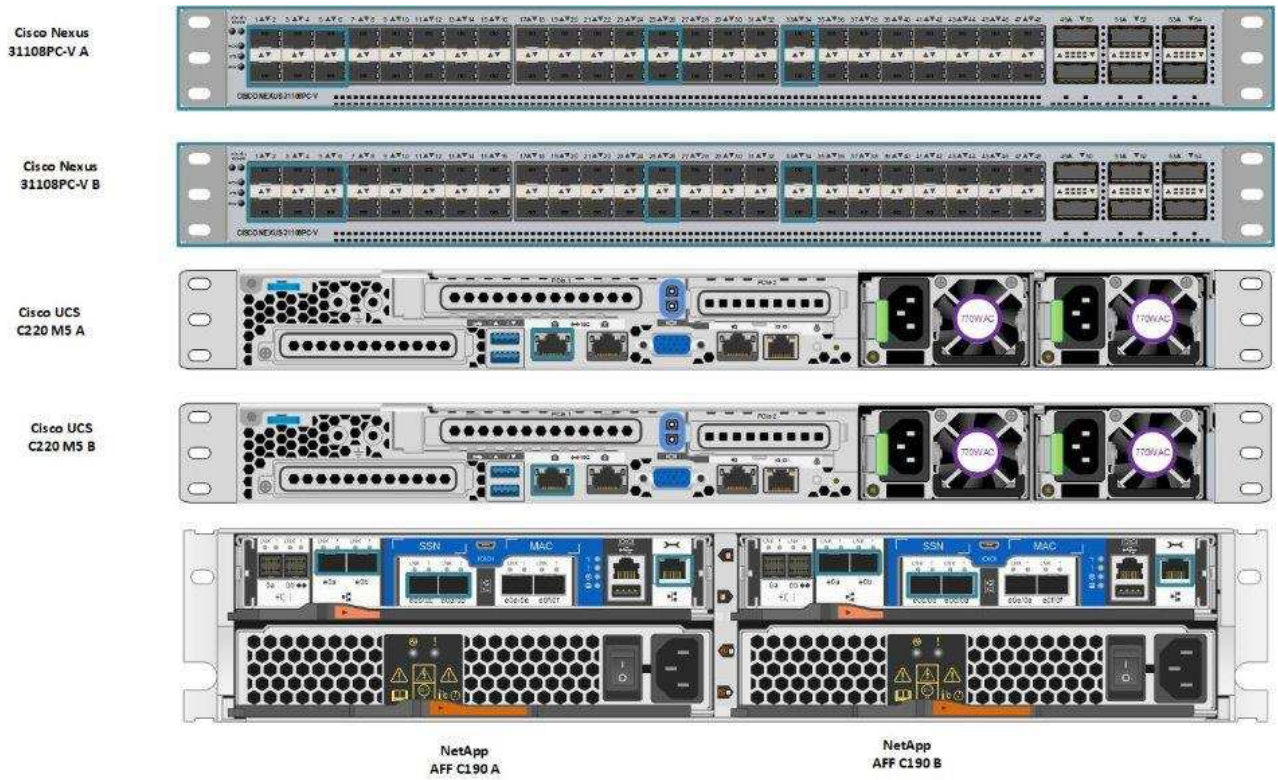
이 표에는 FlexPod Express의 모든 VMware vSphere 구축에 필요한 소프트웨어가 나열되어 있습니다.

소프트웨어	버전
VMware vCenter Server 어플라이언스	6.7U2
VMware vSphere ESXi 하이퍼바이저	6.7U2
ESXi용 NetApp VAAI 플러그인	1.1.2
NetApp VSC를 기반으로 합니다	9.6

FlexPod Express 케이블링 정보

이 참조 검증은 다음 그림 및 표와 같이 케이블로 연결됩니다.

이 그림은 참조 검증 케이블 연결을 보여 줍니다.



다음 표에는 Cisco Nexus 스위치 31108PC-V-A의 케이블 연결 정보가 나와 있습니다

로컬 장치	로컬 포트	원격 장치	원격 포트
Cisco Nexus 스위치 31108PC-V A	eth1/1	NetApp AFF C190 스토리지 컨트롤러 A	e0c
	eth1/2	NetApp AFF C190 스토리지 컨트롤러 B	e0c
	eth1/3	Cisco UCS C220 C-Series 독립 실행형 서버 A	MLOM0
	eth1/4	Cisco UCS C220 C-Series 독립 실행형 서버 B	MLOM0
	eth1/5	Cisco UCS C220 C-Series 독립 실행형 서버 A	MLOM1
	eth1/6	Cisco UCS C220 C-Series 독립 실행형 서버 B	MLOM1
	eth1/25	Cisco Nexus 스위치 31108PC-V B	eth1/25
	Eth1/26	Cisco Nexus 스위치 31108PC-V B	Eth1/26
	Eth1/33	NetApp AFF C190 스토리지 컨트롤러 A	e0M
	eth1/34	Cisco UCS C220 C-Series 독립 실행형 서버 A	CIMC(FEX135/1/25)

이 표에는 Cisco Nexus 스위치 31108PC-V-B의 케이블 연결 정보가 나와 있습니다

로컬 장치	로컬 포트	원격 장치	원격 포트
Cisco Nexus 스위치 31108PC-V B	eth1/1	NetApp AFF C190 스토리지 컨트롤러 A	e0d
	eth1/2	NetApp AFF C190 스토리지 컨트롤러 B	e0d
	eth1/3	Cisco UCS C220 C-Series 독립 실행형 서버 A	MLOM2
	eth1/4	Cisco UCS C220 C-Series 독립 실행형 서버 B	MLOM2
	eth1/5	Cisco UCS C220 C-Series 독립 실행형 서버 A	MLOM3
	eth1/6	Cisco UCS C220 C-Series 독립 실행형 서버 B	MLOM3
	eth1/25	Cisco Nexus 스위치 31108 A	eth1/25
	Eth1/26	Cisco Nexus 스위치 31108 A	Eth1/26
	Eth1/33	NetApp AFF C190 스토리지 컨트롤러 B	e0M
	eth1/34	Cisco UCS C220 C-Series 독립 실행형 서버 B	CIMC(FEX135/1/26)

이 표에는 NetApp AFF C190 스토리지 컨트롤러 A의 케이블 연결 정보가 나와 있습니다

로컬 장치	로컬 포트	원격 장치	원격 포트
NetApp AFF C190 스토리지 컨트롤러 A	e0a	NetApp AFF C190 스토리지 컨트롤러 B	e0a
	e0b	NetApp AFF C190 스토리지 컨트롤러 B	e0b
	e0c	Cisco Nexus 스위치 31108PC-V A	eth1/1
	e0d	Cisco Nexus 스위치 31108PC-V B	eth1/1
	e0M	Cisco Nexus 스위치 31108PC-V A	Eth1/33

이 표에는 NetApp AFF C190 스토리지 컨트롤러 B의 케이블 연결 정보가 나와 있습니다

로컬 장치	로컬 포트	원격 장치	원격 포트
NetApp AFF C190 스토리지 컨트롤러 B	e0a	NetApp AFF C190 스토리지 컨트롤러 A	e0a
	e0b	NetApp AFF C190 스토리지 컨트롤러 A	e0b
	e0c	Cisco Nexus 스위치 31108PC-V A	eth1/2
	e0d	Cisco Nexus 스위치 31108PC-V B	eth1/2
	e0M	Cisco Nexus 스위치 31108PC-V B	Eth1/33

구현 절차

개요

이 문서에서는 완전히 이중화된 고가용성 FlexPod Express 시스템을 구성하는 방법에 대해 자세히 설명합니다. 이러한 이중화를 반영하기 위해 각 단계에서 구성 요소를 구성 요소 A 또는 구성 요소 B라고 합니다 예를 들어 컨트롤러 A와 컨트롤러 B는 이 문서에 프로비저닝된 NetApp 스토리지 컨트롤러 2개를 식별합니다. 스위치 A와 스위치 B는 Cisco Nexus 스위치 쌍을 나타냅니다.

또한 서버 A, 서버 B 등으로 순차적으로 구분되는 여러 Cisco UCS 호스트를 프로비저닝하는 단계도 설명합니다.

사용자 환경과 관련된 정보를 단계별로 포함해야 함을 나타내기 위해 명령 구조의 일부로 '<<text>>'이 표시됩니다. 'VLAN create' 명령은 다음 예를 참조하십시오.

```
Controller01> network port vlan create -node <<var_nodeA>> -vlan-name
<<var_vlan-name>>
```

이 문서를 사용하여 FlexPod Express 환경을 완전히 구성할 수 있습니다. 이 프로세스에서 다양한 단계를 수행하려면 고객별 명명 규칙, IP 주소 및 VLAN(Virtual Local Area Network) 스키마를 삽입해야 합니다. 다음 표에서는 이 가이드에 설명된 대로 구축에 필요한 VLAN을 설명합니다. 이 표는 특정 사이트 변수를 기반으로 완료할 수 있으며 문서 구성 단계를 구현하는 데 사용할 수 있습니다.

별도의 대역내 및 대역외 관리 VLAN을 사용하는 경우 이러한 VLAN 간에 레이어 3 경로를 만들어야 합니다. 이 검증에서는 공통 관리 VLAN이 사용되었습니다.

VLAN 이름입니다	**VLAN**의 용도	**VLAN ID**입니다	
관리 VLAN	관리 인터페이스용 VLAN	3437	vSwitch0
NFS VLAN	NFS 트래픽용 VLAN	3438	vSwitch0

VLAN 이름입니다	**VLAN**의 용도	**VLAN ID**입니다	
VMware vMotion VLAN	가상 머신(VM)을 하나의 물리적 호스트에서 다른 물리적 호스트로 이동하도록 지정된 VLAN	3441	vSwitch0
VM 트래픽 VLAN	VM 애플리케이션 트래픽용 VLAN	3442	vSwitch0
iSCSI-A-VLAN	패브릭 A의 iSCSI 트래픽용 VLAN	3439	iSciBootvSwitch
iSCSI-B-VLAN	패브릭 B의 iSCSI 트래픽용 VLAN	3440	iSciBootvSwitch
네이티브 VLAN	태그가 지정되지 않은 프레임이 할당되는 VLAN입니다	2	

FlexPod Express를 구성하는 동안 VLAN 번호가 필요합니다. VLAN은 "<<var_xxxx_vlan>>"라고 하며, 여기서 "xxxx"는 VLAN의 목적(예: iSCSI-A)입니다.

이 검증에는 두 개의 vSwitch가 생성됩니다.

다음 표에는 솔루션 vSwitch가 나와 있습니다.

vSwitch 이름입니다	활성 어댑터	포트	**MTU**	로드 밸런싱
vSwitch0	Vmnic2, vmnic4	기본값(120)	9000입니다	IP 해시를 기반으로 하는 라우트입니다
iSciBootvSwitch	Vmnic3, vmnic5	기본값(120)	9000입니다	발신 가상 포트 ID를 기반으로 하는 라우트입니다.

로드 밸런싱의 IP 해시 방법을 사용하려면 정적(모드 켜짐) 포트 채널과 함께 SRC-DST-IP EtherChannel을 사용하는 기본 물리적 스위치에 대해 적절한 구성이 필요합니다. 스위치 구성이 잘못되어 연결이 간헐적으로 이루어지는 경우 포트 채널 설정 문제를 해결하는 동안 ESXi 관리 vmkernel 포트와의 통신을 복구하기 위해 Cisco 스위치에서 연결된 두 개의 업링크 포트 중 하나를 일시적으로 종료합니다.

다음 표에는 생성된 VMware VM이 나와 있습니다.

VM 설명입니다	호스트 이름입니다
VMware vCenter Server를 참조하십시오	FlexPod-VCSA를 참조하십시오
가상 스토리지 콘솔	FlexPod-VSC를 참조하십시오

Cisco Nexus 31108PC-V 구축

이 섹션에서는 FlexPod 익스프레스 환경에서 사용되는 Cisco Nexus 331108PC-V 스위치 구성에 대해 자세히 설명합니다.

Cisco Nexus 31108PC-V 스위치의 초기 설정

다음 절차에서는 기본 FlexPod Express 환경에서 사용할 Cisco Nexus 스위치를 구성하는 방법에 대해 설명합니다.

> 이 절차에서는 NX-OS 소프트웨어 릴리즈 7.0(3) i7(6)을 실행하는 Cisco Nexus 31108PC-V를 사용하고 있다고 가정합니다.

1. 초기 부팅이 완료되고 스위치의 콘솔 포트에 연결되면 Cisco NX-OS 설정이 자동으로 시작됩니다. 이 초기 구성에서는 스위치 이름, mgmt0 인터페이스 구성, SSH(Secure Shell) 설정과 같은 기본 설정을 지정합니다.
2. FlexPod 익스프레스 관리 네트워크는 여러 가지 방법으로 구성할 수 있습니다. 31108PC-V 스위치의 mgmt0 인터페이스를 기존 관리 네트워크에 연결할 수도 있고, 31108PC-V 스위치의 mgmt0 인터페이스를 연속 연결 구성으로 연결할 수도 있습니다. 하지만 이 링크는 SSH 트래픽과 같은 외부 관리 액세스에 사용할 수 없습니다.

   > 이 구축 가이드에서는 FlexPod Express Cisco Nexus 31108PC-V 스위치가 기존 관리 네트워크에 연결되어 있습니다.

3. Cisco Nexus 31108PC-V 스위치를 구성하려면 스위치 전원을 켜고 화면 메시지에 따라 두 스위치를 초기 설정하고 스위치 관련 정보에 해당하는 값을 대체합니다.

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
  Enter the switch name : 31108PC-V-B
  Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
    Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
    Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
  Configure advanced IP options? (yes/no) [n]: n
  Enable the telnet service? (yes/no) [n]: n
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
    Number of rsa key bits <1024-2048> [1024]: <enter>
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_ntp_ip>>
  Configure default interface layer (L3/L2) [L2]: <enter>
  Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]: <enter>
```

4. 그러면 구성 요약이 표시됩니다. 구성을 편집할지 묻는 메시지가 나타납니다. 구성이 올바르면 n을 입력합니다.

```
Would you like to edit the configuration? (y
es/no) [n]: n
```

5. 그런 다음 이 구성을 사용하고 저장할지 묻는 메시지가 표시됩니다. 그렇다면 y를 입력합니다.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Cisco Nexus 스위치 B에 대해 이 절차를 반복합니다

고급 기능을 활성화합니다

추가 구성 옵션을 제공하려면 Cisco NX-OS에서 특정 고급 기능을 사용하도록 설정해야 합니다. Cisco Nexus 스위치 A 및 스위치 B에서 적절한 기능을 사용하도록 설정하려면 명령(config t)을 사용하여 구성 모드를 시작하고 다음 명령을 실행합니다.

```
feature interface-vlan
feature lacp
feature vpc
```

기본 포트 채널 로드 밸런싱 해쉬는 소스 및 타깃 IP 주소를 사용하여 포트 채널의 인터페이스에 대한 로드 밸런싱 알고리즘을 결정합니다. 소스 및 타깃 IP 주소보다 많은 입력을 해쉬 알고리즘에 제공하면 포트 채널 멤버 전체에 걸쳐 더 효율적으로 분산될 수 있습니다. 동일한 이유로 소스 및 타깃 TCP 포트를 해쉬 알고리즘에 추가하는 것이 좋습니다.

구성 모드(config t)에서 다음 명령을 입력하여 Cisco Nexus 스위치 A 및 스위치 B의 글로벌 포트 채널 로드 밸런싱 구성을 설정하십시오.

```
port-channel load-balance src-dst ip-l4port
```

글로벌 스패닝 트리를 구성합니다

Cisco Nexus 플랫폼은 브리지 보장이라는 새로운 보호 기능을 사용합니다. 브리지 보장은 스패닝 트리 알고리즘을 더 이상 실행하지 않는 장치에서 데이터 트래픽을 계속 전달하는 단방향 링크 또는 기타 소프트웨어 장애를 방지합니다. 플랫폼에 따라 네트워크 또는 가장자리를 포함한 여러 상태 중 하나에 포트를 배치할 수 있습니다.

기본적으로 모든 포트가 네트워크 포트로 간주되도록 브리지 보장을 설정하는 것이 좋습니다. 이 설정은 네트워크 관리자가 각 포트의 구성을 검토하도록 합니다. 또한 확인되지 않은 에지 포트 또는 브리지 보장 기능이 활성화되지 않은 인접 장치와 같은 가장 일반적인 구성 오류도 표시됩니다. 또한 스패닝 트리에서 너무 적은 포트가 아니라 많은 포트를 차단하는 편이 더 안전합니다. 그러면 기본 포트 상태를 통해 네트워크의 전반적인 안정성을 향상할 수 있습니다.

특히 브리지 보장을 지원하지 않는 서버, 스토리지 및 업링크 스위치를 추가할 때는 스패닝 트리 상태에 세심한 주의를 기울여야 합니다. 이러한 경우 포트를 활성화하려면 포트 유형을 변경해야 할 수 있습니다.

브리지 프로토콜 데이터 단위(BPDU) 보호대는 기본적으로 다른 보호 계층으로 에지 포트에서 활성화됩니다. 네트워크의 루프를 방지하기 위해 이 기능은 다른 스위치의 BPDU가 이 인터페이스에 표시되는 경우 포트를 종료합니다.

구성 모드(config t)에서 다음 명령을 실행하여 Cisco Nexus 스위치 A 및 스위치 B에서 기본 포트 유형과 BPDU 가드를 포함한 기본 스패닝 트리 옵션을 구성하십시오.

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
ntp server <<var_ntp_ip>> use-vrf management
ntp master 3
```

VLAN을 정의합니다

VLAN이 서로 다른 개별 포트를 구성하기 전에 스위치에서 레이어 2 VLAN을 정의해야 합니다. 향후 문제 해결이 용이하도록 VLAN 이름을 지정하는 것도 좋은 방법입니다.

구성 모드(config t)에서 다음 명령을 실행하여 Cisco Nexus 스위치 A 및 스위치 B의 계층 2 VLAN을 정의하고 설명하십시오.

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

액세스 및 관리 포트 설명을 구성합니다

레이어 2 VLAN에 이름을 할당하는 경우와 마찬가지로, 모든 인터페이스에 대한 설정 설명은 프로비저닝과 문제 해결에 도움이 될 수 있습니다.

각 스위치의 구성 모드(config t)에서 FlexPod Express 대규모 구성에 대한 다음 포트 설명을 입력합니다.

Cisco Nexus 스위치 **A**

```
int eth1/1
  description AFF C190-A e0c
int eth1/2
  description AFF C190-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0 vSwitch0
int eth1/4
  description UCS-Server-B: MLOM port 0 vSwitch0
int eth1/5
  description UCS-Server-A: MLOM port 1 iScsiBootvSwitch
int eth1/6
  description UCS-Server-B: MLOM port 1 iScsiBootvSwitch
int eth1/25
  description vPC peer-link 31108PC-V-B 1/25
int eth1/26
  description vPC peer-link 31108PC-V-B 1/26
int eth1/33
  description AFF C190-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Cisco Nexus 스위치 B

```
int eth1/1
  description AFF C190-A e0d
int eth1/2
  description AFF C190-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 2 vSwitch0
int eth1/4
description UCS-Server-B: MLOM port 2 vSwitch0
int eth1/5
  description UCS-Server-A: MLOM port 3 iScsiBootvSwitch
int eth1/6
  description UCS-Server-B: MLOM port 3 iScsiBootvSwitch
int eth1/25
  description vPC peer-link 31108PC-V-A 1/25
int eth1/26
  description vPC peer-link 31108PC-V-A 1/26
int eth1/33
  description AFF C190-B e0M
int eth1/34
  description UCS Server B: CIMC
```

서버와 스토리지 모두의 관리 인터페이스는 일반적으로 단일 VLAN만 사용합니다. 따라서 관리 인터페이스 포트를 액세스 포트로 구성합니다. 각 스위치에 대한 관리 VLAN을 정의하고 스패닝 트리 포트 유형을 에지로 변경합니다.

구성 모드(config t)에서 다음 명령을 입력하여 서버와 스토리지 모두의 관리 인터페이스에 대한 포트 설정을 구성하십시오.

Cisco Nexus 스위치 **A**

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Cisco Nexus 스위치 **B**

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

가상 포트 채널 글로벌 구성을 수행합니다

가상 포트 채널(vPC)을 사용하면 물리적으로 두 개의 서로 다른 Cisco Nexus 스위치에 연결된 링크가 세 번째 장치에 단일 포트 채널로 표시될 수 있습니다. 세 번째 장치는 스위치, 서버 또는 다른 네트워킹 장치일 수 있습니다. vPC는 계층 2 다중 경로를 제공할 수 있으므로 대역폭을 높이고, 노드 간에 여러 개의 병렬 경로를 활성화하고, 대체 경로가 있는 로드 밸런싱 트래픽을 통해 이중화를 생성할 수 있습니다.

vPC는 다음과 같은 이점을 제공합니다.

- 단일 장치에서 두 업스트림 장치에 걸쳐 포트 채널을 사용하도록 설정
- 스패닝 트리 프로토콜 차단 포트 제거
- 루프 없는 토폴로지 제공
- 사용 가능한 모든 업링크 대역폭 사용
- 링크 또는 디바이스에 장애가 발생할 경우 빠른 컨버전스를 제공합니다
- 링크 레벨의 복원력 제공
- 고가용성 제공 지원

vPC 기능이 제대로 작동하려면 두 Cisco Nexus 스위치 간의 몇 가지 초기 설정이 필요합니다. 연속 인접 mgmt0 구성을 사용하는 경우에는 인터페이스에 정의된 주소를 사용하고 "ping"\< 스위치_A/B_mgmt0_ip_addr>>VRF" 관리

명령을 사용하여 통신 가능 여부를 확인해야 합니다.

구성 모드(config t)에서 다음 명령을 실행하여 두 스위치에 대한 vPC 글로벌 구성을 설정하십시오.

Cisco Nexus 스위치 **A**

```
vpc domain 1
 role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf
management
peer-switch
peer-gateway
auto-recovery
delay restore 150
ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

Cisco Nexus 스위치 **B**

```
vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  delay-restore 150
   ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

스토리지 포트 채널을 구성합니다

NetApp 스토리지 컨트롤러는 LACP(Link Aggregation Control Protocol)를 사용하여 네트워크에 대해 active-active 연결을 허용합니다. LACP 사용이 선호되는 이유는 LACP가 스위치 간에 협상과 로깅을 모두 추가하기 때문입니다. 네트워크가 vPC에 맞게 설정되므로 이 접근 방식을 통해 스토리지에서 별도의 물리적 스위치로의 active-active 연결을 설정할 수 있습니다. 각 컨트롤러에는 각 스위치에 대한 링크가 2개 있습니다. 하지만 4개의 모든 링크는 동일한 vPC 및 인터페이스 그룹(ifgrp)의 일부입니다.

구성 모드(config t)에서 각 스위치에 대해 다음 명령을 실행하여 개별 인터페이스를 구성하고 NetApp AFF 컨트롤러에 연결된 포트에 대한 결과 포트 채널 구성을 설정하십시오.

1. 스위치 A와 스위치 B에서 다음 명령을 실행하여 스토리지 컨트롤러 A의 포트 채널을 구성합니다.

```
int eth1/1
  channel-group 11 mode active
int Po11
  description vPC to Controller-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11
  no shut
```

2. 스위치 A와 스위치 B에서 다음 명령을 실행하여 스토리지 컨트롤러 B의 포트 채널을 구성합니다.

```
int eth1/2
  channel-group 12 mode active
int Po12
  description vPC to Controller-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
  no shut
exit
copy run start
```

서버 연결을 구성합니다

Cisco UCS 서버에는 데이터 트래픽과 iSCSI를 사용한 ESXi 운영 체제 부팅에 사용되는 4포트 가상 인터페이스 카드 VIC1457이 있습니다. 이러한 인터페이스는 서로 간에 페일오버되도록 구성되어 단일 링크를 넘어 추가적인 이중화를 제공합니다. 이러한 링크를 여러 스위치에 걸쳐 분산하면 완전한 스위치 장애가 발생해도 서버가 가동 상태를 유지할 수 있습니다.

구성 모드(config t)에서 다음 명령을 실행하여 각 서버에 연결된 인터페이스에 대한 포트 설정을 구성하십시오.

Cisco Nexus 스위치 **A: Cisco UCS** 서버 **A** 및 **Cisco UCS** 서버 **B** 구성

```
int eth1/5
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

Cisco Nexus 스위치 **B: Cisco UCS** 서버 **A** 및 **Cisco UCS** 서버 **B** 구성

```
int eth1/6
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

서버 포트 채널을 구성합니다

스위치 A와 스위치 B에서 다음 명령을 실행하여 서버 A에 대한 포트 채널을 구성합니다.

```
int eth1/3
  channel-group 13 mode active
int Po13
  description vPC to Server-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 13
  no shut
```

스위치 A와 스위치 B에서 다음 명령을 실행하여 서버 B에 대한 포트 채널을 구성합니다.

```
int eth1/4
  channel-group 14 mode active
int Po14
  description vPC to Server-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 14
  no shut
```

이 솔루션 검증에 9000의 MTU가 사용되었습니다. 그러나 애플리케이션 요구 사항에 적합한 MTU에 대해 다른 값을 구성할 수 있습니다. FlexPod 솔루션에서 동일한 MTU 값을 설정하는 것이 중요합니다. 구성 요소 간의 MTU 구성이 잘못되면 패킷이 손실되고 이러한 패킷은 다시 전송되어야 하며 솔루션의 전반적인 성능에 영향을 미칩니다.

Cisco UCS 서버를 추가하여 솔루션을 확장하거나, 스위치 A 및 B에서 새로 추가한 서버가 연결된 스위치 포트를 사용하여 이전 명령을 실행합니다

기존 네트워크 인프라로 업링크

사용 가능한 네트워크 인프라에 따라 여러 가지 방법과 기능을 사용하여 FlexPod 환경을 업링크할 수 있습니다. 기존 Cisco Nexus 환경이 존재하는 경우, NetApp은 vPC를 사용하여 FlexPod 환경에 포함된 Cisco Nexus 31108 스위치를 인프라로 업링크하는 것을 권장합니다. 업링크는 10GbE 인프라스트럭처 솔루션의 경우 10GbE 업링크, 필요한 경우 1GbE 인프라스트럭처 솔루션의 경우 1GbE가 될 수 있습니다. 앞서 설명한 절차를 사용하여 기존 환경에 대한 업링크 vPC를 생성할 수 있습니다. 구성이 완료된 후 각 스위치에 대한 구성을 저장하려면 copy start를 실행해야 합니다.

"다음은 NetApp 스토리지 구축 절차(1부)입니다."

NetApp 스토리지 구축 절차(1부)

이 섹션에서는 NetApp AFF 스토리지 구축 절차를 설명합니다.

NetApp 스토리지 컨트롤러 AFF C190 시리즈 설치

NetApp Hardware Universe를 참조하십시오

NetApp HWU(Hardware Universe) 애플리케이션은 특정 ONTAP 버전에 대해 지원되는 하드웨어 및 소프트웨어 구성요소를 제공합니다. 현재 ONTAP 소프트웨어가 지원하는 모든 NetApp 스토리지 어플라이언스에 대한 구성 정보를 제공합니다. 구성요소 호환성 표도 제공합니다.

사용하려는 하드웨어 및 소프트웨어 구성 요소가 설치하려는 ONTAP 버전에서 지원되는지 확인합니다.

에 액세스합니다 "HWU" 응용 프로그램 - 시스템 구성 가이드를 봅니다. 컨트롤러 탭을 클릭하여 원하는 사양의 ONTAP 소프트웨어 버전과 NetApp 스토리지 어플라이언스 간의 호환성을 확인하십시오.

또는 스토리지 어플라이언스별로 구성 요소를 비교하려면 스토리지 시스템 비교 를 클릭합니다.

컨트롤러 **AFFC190 Series** 사전 요구사항
스토리지 시스템의 물리적 위치를 계획하려면 NetApp Hardware Universe를 참조하십시오. 다음 섹션을 참조하십시오. • 전기 요구 사항 • 지원되는 전원 코드 • 온보드 포트 및 케이블

스토리지 컨트롤러

AFF의 컨트롤러에 대한 물리적 설치 절차를 따릅니다 "C190" 문서화:

NetApp ONTAP 9.6

구성 워크시트

설치 스크립트를 실행하기 전에 제품 설명서에서 구성 워크시트를 작성하십시오. 구성 워크시트는 ONTAP 9.6 소프트웨어 설치 가이드에서 사용할 수 있습니다.

이 시스템은 스위치가 없는 2노드 클러스터 구성에서 설정됩니다.

다음 표는 ONTAP 9.6 설치 및 구성 정보를 제공합니다.

클러스터 세부 정보	클러스터 세부 정보 값입니다
클러스터 노드 A IP 주소입니다	<<var_NodeA_mgmt_ip>> 를 입력합니다
클러스터 노드 A 넷마스크	<<var_NodeA_mgmt_mask>> 를 입력합니다
클러스터 노드 A 게이트웨이	<<var_NodeA_mgmt_gateway>> 를 참조하십시오
클러스터 노드 A 이름	<<var_NodeA>> 를 참조하십시오
클러스터 노드 B IP 주소입니다	<<var_NodeB_mgmt_ip>> 를 입력합니다
클러스터 노드 B 넷마스크	<<var_NodeB_mgmt_mask>> 를 입력합니다
클러스터 노드 B 게이트웨이	<<var_NodeB_mgmt_gateway>> 를 참조하십시오
클러스터 노드 B 이름	<<var_NodeB>> 를 참조하십시오
ONTAP 9.6 URL입니다	<<var_url_boot_software>>
클러스터의 이름입니다	<<var_clustername>> 를 클릭합니다
클러스터 관리 IP 주소입니다	<<var_clustermgmt_ip>> 를 입력합니다
클러스터 B 게이트웨이	<<var_clustermgmt_gateway>> 를 클릭합니다
클러스터 B 넷마스크	<<var_clustermgmt_mask>> 를 입력합니다

클러스터 세부 정보	클러스터 세부 정보 값입니다
도메인 이름	<<var_domain_name>>
DNS 서버 IP(둘 이상 입력할 수 있음)	var_dns_server_ip입니다
NTP 서버 IP(둘 이상 입력할 수 있음)	<<var_ntp_server_ip>> 를 참조하십시오

노드 **A**를 구성합니다

노드 A를 구성하려면 다음 단계를 완료하십시오.

1. 스토리지 시스템 콘솔 포트에 연결합니다. Loader-A 메시지가 표시됩니다. 하지만 스토리지 시스템이 재부팅 루프 상태인 경우 다음 메시지가 표시될 때 Ctrl-C를 눌러 자동 부팅 루프를 종료합니다.

   ```
   Starting AUTOBOOT press Ctrl-C to abort…
   ```

   시스템이 부팅되도록 합니다.

   ```
   autoboot
   ```

2. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.

   ⓘ ONTAP 9.6이 부팅 중인 소프트웨어 버전이 아닌 경우 다음 단계를 계속하여 새 소프트웨어를 설치하십시오. ONTAP 9.6이 부팅 중인 버전인 경우 옵션 8 및 y를 선택하여 노드를 재부팅합니다. 그런 다음 14단계를 계속합니다.

3. 새 소프트웨어를 설치하려면 옵션 7을 선택합니다.
4. 업그레이드를 수행하려면 y 를 입력합니다.
5. 다운로드에 사용할 네트워크 포트로 e0M을 선택합니다.
6. 지금 재부팅하려면 y를 입력하십시오.
7. 각 위치에 e0M의 IP 주소, 넷마스크 및 기본 게이트웨이를 입력합니다.

   ```
   <<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
   ```

8. 소프트웨어를 찾을 수 있는 URL을 입력합니다.

   ⓘ 이 웹 서버는 Ping할 수 있어야 합니다.

   ```
   <<var_url_boot_software>>
   ```

9. 사용자 이름에 대해 Enter 키를 눌러 사용자 이름이 없음을 나타냅니다.
10. 새로 설치한 소프트웨어를 이후 재부팅에 사용할 기본값으로 설정하려면 y 를 입력합니다.

11. y를 입력하여 노드를 재부팅합니다.

> 새 소프트웨어를 설치할 때 시스템이 BIOS 및 어댑터 카드에 대한 펌웨어 업그레이드를 수행할 수 있으며, 이로 인해 LOADER-A 프롬프트에서 재부팅되고 중지될 수 있습니다. 이러한 작업이 발생하면 시스템이 이 절차를 벗어날 수 있습니다.

12. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.
13. Clean Configuration(구성 정리) 및 Initialize All Disks(모든 디스크 초기화) 에 대해 옵션 4 를 선택합니다.
14. 디스크를 제로화하려면 y를 입력하고 구성을 재설정한 다음 새 파일 시스템을 설치합니다.
15. y 를 입력하여 디스크의 모든 데이터를 지웁니다.

> 연결된 디스크의 수와 유형에 따라 루트 애그리게이트의 초기화 및 생성을 완료하는 데 90분 이상이 걸릴 수 있습니다. 초기화가 완료되면 스토리지 시스템이 재부팅됩니다. SSD를 초기화하는 데 걸리는 시간은 상당히 줄어듭니다. 노드 A용 디스크가 제로화하는 동안 노드 B 구성을 계속할 수 있습니다.

노드 A를 초기화하는 동안 노드 B를 구성합니다

노드 **B**를 구성합니다

노드 B를 구성하려면 다음 단계를 완료하십시오.

1. 스토리지 시스템 콘솔 포트에 연결합니다. Loader-A 메시지가 표시됩니다. 하지만 스토리지 시스템이 재부팅 루프 상태인 경우 다음 메시지가 표시될 때 Ctrl-C를 눌러 자동 부팅 루프를 종료합니다.

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.

```
autoboot
```

3. 메시지가 나타나면 Ctrl-C를 누릅니다.

> ONTAP 9.6이 부팅 중인 소프트웨어 버전이 아닌 경우 다음 단계를 계속하여 새 소프트웨어를 설치하십시오. ONTAP 9.6이 부팅 중인 버전인 경우 옵션 8 및 y를 선택하여 노드를 재부팅합니다. 그런 다음 14단계를 계속합니다.

4. 새 소프트웨어를 설치하려면 옵션 7.A를 선택합니다
5. 업그레이드를 수행하려면 y 를 입력합니다.
6. 다운로드에 사용할 네트워크 포트로 e0M을 선택합니다.
7. 지금 재부팅하려면 y를 입력하십시오.
8. 각 위치에 e0M의 IP 주소, 넷마스크 및 기본 게이트웨이를 입력합니다.

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. 소프트웨어를 찾을 수 있는 URL을 입력합니다.

   이 웹 서버는 Ping할 수 있어야 합니다.

```
<<var_url_boot_software>>
```

10. 사용자 이름에 대해 Enter 키를 눌러 사용자 이름이 없음을 나타냅니다.
11. 새로 설치한 소프트웨어를 이후 재부팅에 사용할 기본값으로 설정하려면 y 를 입력합니다.
12. y를 입력하여 노드를 재부팅합니다.

    새 소프트웨어를 설치할 때 시스템이 BIOS 및 어댑터 카드에 대한 펌웨어 업그레이드를 수행할 수 있으며, 이로 인해 LOADER-A 프롬프트에서 재부팅되고 중지될 수 있습니다. 이러한 작업이 발생하면 시스템이 이 절차를 벗어날 수 있습니다.

13. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.
14. Clean Configuration(구성 정리) 및 Initialize All Disks(모든 디스크 초기화) 에 대해 옵션 4 를 선택합니다.
15. 디스크를 제로화하려면 y를 입력하고 구성을 재설정한 다음 새 파일 시스템을 설치합니다.
16. y 를 입력하여 디스크의 모든 데이터를 지웁니다.

    연결된 디스크의 수와 유형에 따라 루트 애그리게이트의 초기화 및 생성을 완료하는 데 90분 이상이 걸릴 수 있습니다. 초기화가 완료되면 스토리지 시스템이 재부팅됩니다. SSD를 초기화하는 데 걸리는 시간은 상당히 줄어듭니다.

노드 **A** 구성 및 클러스터 구성 계속

스토리지 컨트롤러 A(노드 A) 콘솔 포트에 연결된 콘솔 포트 프로그램에서 노드 설정 스크립트를 실행합니다. 이 스크립트는 ONTAP 9.6이 처음으로 노드에서 부팅될 때 나타납니다.

ONTAP 9.6에서 노드 및 클러스터 설정 절차가 약간 변경되었습니다. 이제 클러스터 설정 마법사를 사용하여 클러스터의 첫 번째 노드를 구성하고 NetApp ONTAP System Manager(이전의 OnCommand ® System Manager)를 사용하여 클러스터를 구성할 수 있습니다.

1. 프롬프트에 따라 노드 A를 설정합니다

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. 노드의 관리 인터페이스의 IP 주소로 이동합니다.

> CLI를 사용하여 클러스터를 설정할 수도 있습니다. 이 문서에서는 System Manager의 설정에 따라 클러스터 설정에 대해 설명합니다.

3. Guided Setup(안내식 설정) 을 클릭하여 클러스터를 구성합니다.
4. 클러스터 이름은 <<var_clustername>>'을, 구성 중인 각 노드에 대해서는 <<var_NodeA>>'와 <<var_NodeB>>를 입력합니다. 스토리지 시스템에 사용할 암호를 입력합니다. 클러스터 유형으로 Switchless Cluster를 선택합니다. 클러스터 기본 라이센스를 입력합니다.
5. 클러스터, NFS 및 iSCSI에 대한 기능 라이센스도 입력할 수 있습니다.
6. 클러스터를 생성 중임을 나타내는 상태 메시지가 표시됩니다. 이 상태 메시지는 여러 상태를 순환합니다. 이 과정은 몇 분 정도 소요됩니다.
7. 네트워크를 구성합니다.
   a. IP 주소 범위 옵션을 선택 취소합니다.

b. Cluster Management IP Address 필드(<<var_clustermgmt_ip>>)에 넷마스크 필드(<<var_clustermgmt_mask>>)에 <<var_clustermgmt_gateway>>)를 입력합니다. 다음을 사용하십시오. 포트 필드의 선택기로 노드 A의 e0M을 선택합니다

c. 노드 A의 노드 관리 IP가 이미 채워져 있습니다. 노드 B에 대해 '<<var_NodeA_mgmt_ip>>'를 입력합니다

d. DNS Domain Name 필드에 '<<var_domain_name>>'을 입력합니다. DNS 서버 IP 주소 필드에 '<<var_dns_server_ip>>'를 입력합니다.



여러 DNS 서버 IP 주소를 입력할 수 있습니다.

e. Primary NTP Server 필드에 10.63.172.162 를 입력한다.



대체 NTP 서버를 입력할 수도 있습니다. '<<var_ntp_server_ip>>'의 IP 주소 '10.63.172.162'는 Nexus Mgmt IP입니다.

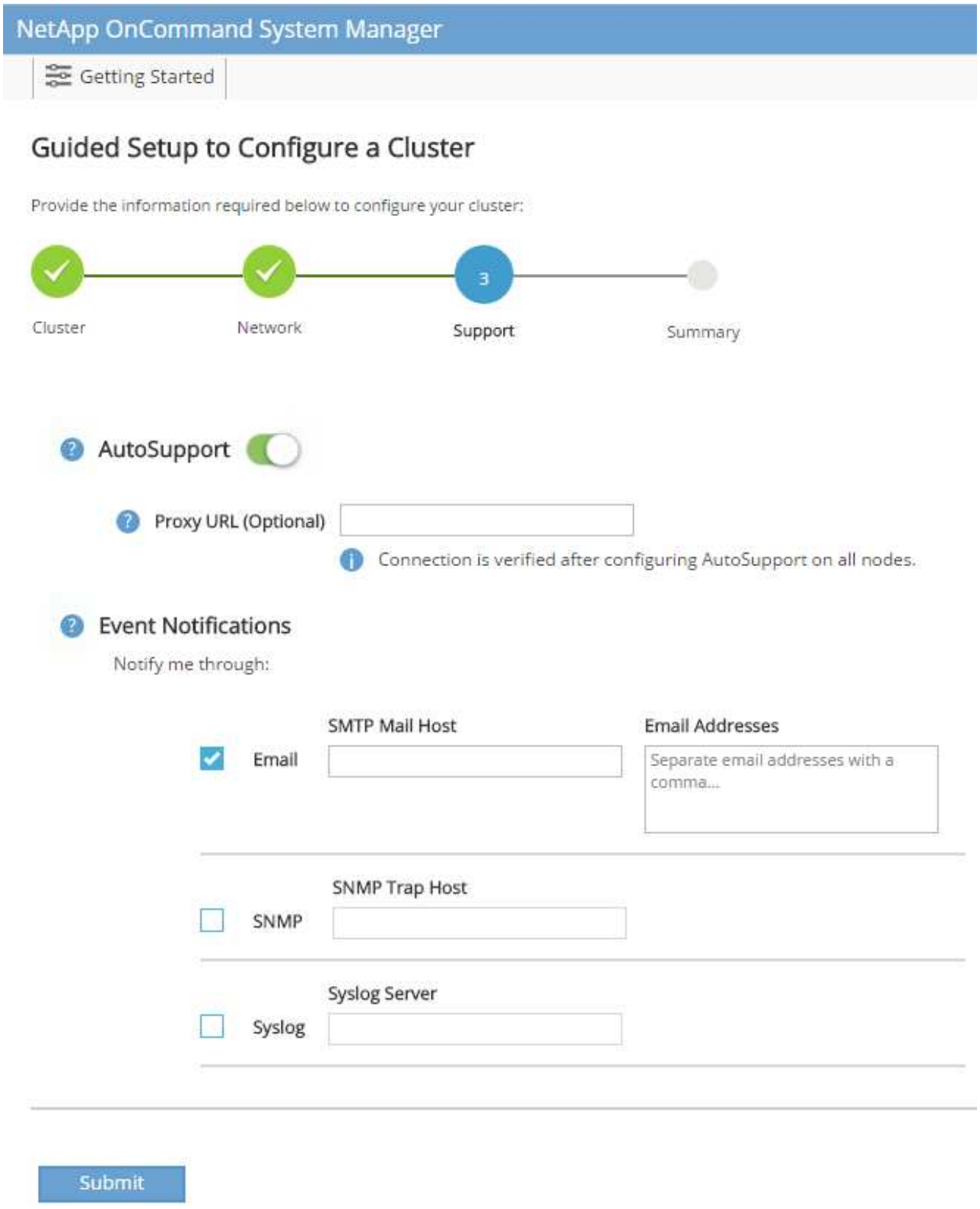
8. 지원 정보를 구성합니다.

a. 환경에 AutoSupport에 액세스하기 위한 프록시가 필요한 경우 프록시 URL에 URL을 입력합니다.

b. 이벤트 알림에 대한 SMTP 메일 호스트 및 이메일 주소를 입력합니다.



계속하려면 이벤트 알림 방법을 설정해야 합니다. 방법 중 하나를 선택할 수 있습니다.



시스템에서 클러스터 구성이 완료되었다는 메시지가 표시되면 클러스터 관리 를 클릭하여 스토리지를 구성합니다.

스토리지 클러스터 구성 계속

스토리지 노드 및 기본 클러스터를 구성한 후에는 스토리지 클러스터 구성을 계속할 수 있습니다.

모든 스페어 디스크를 제로합니다

클러스터의 모든 스페어 디스크를 제로하려면 다음 명령을 실행합니다.

```
disk zerospares
```

온보드 **UTA2** 포트 속성을 설정합니다

1. ucadmin show 명령을 실행하여 포트의 현재 모드 및 현재 유형을 확인합니다.

```
AFF C190::> ucadmin show
                     Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF C190_A     0c       cna       target     -        -          online
AFF C190_A     0d       cna       target     -        -          online
AFF C190_A     0e       cna       target     -        -          online
AFF C190_A     0f       cna       target     -        -          online
AFF C190_B     0c       cna       target     -        -          online
AFF C190_B     0d       cna       target     -        -          online
AFF C190_B     0e       cna       target     -        -          online
AFF C190_B     0f       cna       target     -        -          online
8 entries were displayed.
```

2. 사용 중인 포트의 현재 모드가 CNA인지, 그리고 현재 유형이 타겟으로 설정되어 있는지 확인합니다. 그렇지 않은 경우 다음 명령을 사용하여 포트 속성을 변경합니다.

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

이전 명령을 실행하려면 포트가 오프라인 상태여야 합니다. 포트를 오프라인으로 전환하려면 다음 명령을 실행합니다.

```
network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down
```

포트 속성을 변경한 경우 변경 사항을 적용하려면 각 노드를 재부팅해야 합니다.

관리 논리 인터페이스의 이름을 바꿉니다

관리 논리 인터페이스(LIF)의 이름을 변경하려면 다음 단계를 수행하십시오.

1. 현재 관리 LIF 이름을 표시합니다.

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

2. 클러스터 관리 LIF의 이름을 바꿉니다.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_cluster_mgmt_lif_1 -newname cluster_mgmt
```

3. 노드 B 관리 LIF의 이름을 바꿉니다.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF C190_B_1 -newname AFF C190-02_mgmt1
```

클러스터 관리에서 자동 되돌리기 설정

클러스터 관리 인터페이스에서 자동 되돌리기 매개 변수를 설정합니다.

```
network interface modify -vserver <<clustername>> -lif cluster_mgmt -auto-
revert true
```

서비스 프로세서 네트워크 인터페이스를 설정합니다

각 노드의 서비스 프로세서에 정적 IPv4 주소를 할당하려면 다음 명령을 실행합니다.

```
system service-processor network modify -node <<var_nodeA>> -address
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify -node <<var_nodeB>> -address
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

서비스 프로세서 IP 주소는 노드 관리 IP 주소와 동일한 서브넷에 있어야 합니다.

ONTAP에서 스토리지 페일오버 설정

스토리지 페일오버가 설정되었는지 확인하려면 페일오버 쌍에서 다음 명령을 실행합니다.

1. 스토리지 페일오버 상태를 확인합니다.

```
storage failover show
```

'<<var_NodeA>>'와 '<<var_NodeB>>'는 모두 테이크오버를 수행할 수 있어야 합니다. 노드가 테이크오버 수행 가능한 경우 3단계로 이동하십시오.

2. 두 노드 중 하나에서 페일오버가 사용되도록 설정합니다.

```
storage failover modify -node <<var_nodeA>> -enabled true
```

한 노드에서 페일오버가 사용되도록 설정하면 두 노드 모두에서 설정됩니다.

3. 2노드 클러스터의 HA 상태를 확인합니다.

2개 이상의 노드가 있는 클러스터에는 이 단계를 적용할 수 없습니다.

```
cluster ha show
```

4. 고가용성이 구성된 경우 6단계로 이동합니다. 고가용성이 구성된 경우 명령을 실행하면 다음 메시지가 표시됩니다.

```
High Availability Configured: true
```

5. 2노드 클러스터에만 HA 모드를 사용하도록 설정합니다.

2개 이상의 노드가 있는 클러스터에서는 페일오버에 문제가 발생하므로 이 명령을 실행하지 마십시오.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. 하드웨어 지원이 올바르게 구성되어 있는지 확인하고 필요한 경우 파트너 IP 주소를 수정합니다.

```
storage failover hwassist show
```

"Keep Alive Status: Error:" 메시지는 컨트롤러 중 하나가 파트너의 hwassist keep alive 경고를 받지 못했음을 나타내며, 이는 하드웨어 지원이 구성되지 않았음을 나타냅니다. 다음 명령을 실행하여 하드웨어 지원을 구성합니다.

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

ONTAP에서 점보 프레임 MTU 브로드캐스트 도메인을 생성합니다

MTU가 9000인 데이터 브로드캐스트 도메인을 생성하려면 다음 명령을 실행합니다.

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

기본 브로드캐스트 도메인에서 데이터 포트를 제거합니다

10GbE 데이터 포트는 iSCSI/NFS 트래픽에 사용되며 이러한 포트는 기본 도메인에서 제거해야 합니다. 포트 e0e 및 e0f는 사용되지 않으며 기본 도메인에서도 제거해야 합니다.

브로드캐스트 도메인에서 포트를 제거하려면 다음 명령을 실행합니다.

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

UTA2 포트에서 흐름 제어를 사용하지 않도록 설정합니다

외부 장치에 연결된 모든 UTA2 포트에서 흐름 제어를 사용하지 않도록 설정하는 것이 NetApp의 모범 사례입니다. 흐름 제어를 사용하지 않도록 설정하려면 다음 명령을 실행합니다.

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
```

ONTAP에서 인터페이스 그룹 **LACP**를 구성합니다

이 인터페이스 그룹 유형에 2개 이상의 이더넷 인터페이스와 LACP를 지원하는 스위치가 필요합니다. 섹션 5.1의 이 가이드에 설명된 단계를 기준으로 구성되었는지 확인합니다.

클러스터 프롬프트에서 다음 단계를 완료합니다.

```
ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d
```

ONTAP에서 점보 프레임을 구성합니다

점보 프레임(일반적으로 9,000바이트 MTU 사용)을 사용하도록 ONTAP 네트워크 포트를 구성하려면 클러스터 쉘에서 다음 명령을 실행합니다.

```
AFF C190::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
AFF C190::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
```

ONTAP에서 VLAN을 생성합니다

ONTAP에서 VLAN을 생성하려면 다음 단계를 수행하십시오.

1. NFS VLAN 포트를 생성하여 데이터 브로드캐스트 도메인에 추가합니다.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
<<var_nfs_vlan_id>>
```

2. iSCSI VLAN 포트를 생성하여 데이터 브로드캐스트 도메인에 추가합니다.

```
network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>,<<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>,<<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>
```

3. MGMT-VLAN 포트를 생성합니다.

```
network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>
```

ONTAP에서 데이터 애그리게이트를 생성합니다

ONTAP 설정 프로세스 중에 루트 볼륨이 포함된 애그리게이트가 생성됩니다. 추가 애그리게이트를 생성하려면 애그리게이트 이름, 애그리게이트를 생성할 노드, 애그리게이트에 포함된 디스크 수를 결정합니다.

Aggregate를 생성하려면 다음 명령을 실행합니다.

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

구성에 최소 하나의 디스크(가장 큰 디스크 선택)를 스페어로 보관합니다. 모범 사례는 각 디스크 유형 및 크기에 대해 하나 이상의 스페어를 두는 것입니다.

5개의 디스크로 시작합니다. 스토리지를 추가해야 할 때 디스크를 애그리게이트에 추가할 수 있습니다.

디스크 비우기가 완료될 때까지 애그리게이트를 생성할 수 없습니다. 집계 생성 상태를 표시하려면 'aggr show' 명령을 실행합니다. aggr1_NodeA가 온라인 상태가 될 때까지 진행하지 마십시오.

ONTAP에서 표준 시간대를 구성합니다

시간 동기화를 구성하고 클러스터에서 표준 시간대를 설정하려면 다음 명령을 실행합니다.

```
timezone <<var_timezone>>
```

예를 들어 미국 동부의 표준 시간대는 America/New_York입니다. 표준 시간대 이름을 입력하기 시작하면 Tab 키를 눌러 사용 가능한 옵션을 확인합니다.

ONTAP에서 SNMP를 구성합니다

SNMP를 구성하려면 다음 단계를 수행하십시오.

1. 위치 및 연락처와 같은 SNMP 기본 정보를 구성합니다. 이 정보는 SNMP에서 'SysLocation', 'SysContact' 변수로 표시됩니다.

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_snmp_location>>"
snmp init 1
options snmp.enable on
```

2. 원격 호스트에 보낼 SNMP 트랩을 구성합니다.

```
snmp traphost add <<var_snmp_server_fqdn>>
```

ONTAP에서 SNMPv1을 구성합니다

SNMPv1을 구성하려면 커뮤니티라는 공유 암호 일반 텍스트 암호를 설정합니다.

```
snmp community add ro <<var_snmp_community>>
```

NMP community delete all 명령을 주의하여 사용한다. 다른 모니터링 제품에 커뮤니티 문자열을 사용하는 경우 이 명령은 해당 문자열을 제거합니다.

ONTAP에서 SNMPv3을 구성합니다

SNMPv3을 사용하려면 인증을 위해 사용자를 정의하고 구성해야 합니다. SNMPv3을 구성하려면 다음 단계를 수행하십시오.

1. Security snmpusers 명령을 실행하여 엔진 ID를 조회한다.
2. 'snmpv3user'라는 사용자를 생성합니다.

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. 권한 있는 엔터티의 엔진 ID를 입력하고 인증 프로토콜로 md5를 선택합니다.
4. 메시지가 나타나면 인증 프로토콜에 사용할 최소 길이 8자로 된 암호를 입력합니다.
5. 개인 정보 보호 프로토콜로 des 를 선택합니다.
6. 메시지가 나타나면 개인 정보 보호 프로토콜에 사용할 최소 길이 8자로 된 암호를 입력합니다.

ONTAP에서 AutoSupport HTTPS를 구성합니다

NetApp AutoSupport 툴은 HTTPS를 통해 지원 요약 정보를 NetApp에 보냅니다. AutoSupport를 구성하려면 다음 명령을 실행합니다.

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

스토리지 가상 머신을 생성합니다

인프라 스토리지 가상 시스템(SVM)을 생성하려면 다음 단계를 완료하십시오.

1. 'vserver create' 명령을 실행합니다.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. NetApp VSC를 위한 인프라-SVM 애그리게이트 목록에 데이터 애그리게이트를 추가합니다.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. NFS와 iSCSI를 남겨두고 SVM에서 사용하지 않는 스토리지 프로토콜을 제거합니다.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. 인프라 SVM에서 NFS 프로토콜을 사용하고 실행합니다.

```
nfs create -vserver Infra-SVM -udp disabled
```

5. NetApp NFS VAAI 플러그인에 대한 'VM vStorage' 매개 변수를 설정합니다. 그런 다음 NFS가 구성되었는지 확인합니다.

```
vserver nfs modify –vserver Infra-SVM –vstorage enabled
vserver nfs show
```

SVM은 이전에 SVM을 vserver라고 했기 때문에 명령줄에서는 "vserver"가 명령을 앞에 표시합니다.

ONTAP에서 NFSv3을 구성합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
ESXi 호스트 NFS IP 주소입니다	<<var_esxi_hostA_nfs_ip>> 를 참조하십시오
ESXi 호스트 B NFS IP 주소입니다	<<var_esxi_hostB_nfs_ip>> 를 참조하십시오

SVM에서 NFS를 구성하려면 다음 명령을 실행합니다.

1. 기본 엑스포트 정책에서 각 ESXi 호스트에 대한 규칙을 생성합니다.
2. 생성 중인 각 ESXi 호스트에 대해 규칙을 할당합니다. 각 호스트에는 고유한 규칙 인덱스가 있습니다. 첫 번째 ESXi 호스트에는 규칙 인덱스 1이 있고 두 번째 ESXi 호스트에는 규칙 인덱스 2가 있습니다.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 2 –protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. 인프라 SVM 루트 볼륨에 엑스포트 정책을 할당합니다.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

vSphere를 설정한 후 NetApp VSC는 엑스포트 정책을 자동으로 처리합니다. 설치하지 않은 경우 Cisco UCS C-Series 서버를 추가할 때 엑스포트 정책 규칙을 생성해야 합니다.

ONTAP에서 iSCSI 서비스를 생성합니다

SVM에서 iSCSI 서비스를 생성하려면 다음 명령을 실행합니다. 또한 이 명령은 iSCSI 서비스를 시작하고 SVM에 대한 iSCSI IQN을 설정합니다. iSCSI가 구성되었는지 확인합니다.

```
iscsi create -vserver Infra-SVM
iscsi show
```

ONTAP에서 SVM 루트 볼륨의 로드 공유 미러를 생성합니다

ONTAP에서 SVM 루트 볼륨의 로드 공유 미러를 생성하려면 다음 단계를 수행하십시오.

1. 각 노드에서 인프라 SVM 루트 볼륨의 로드 공유 미러가 될 볼륨을 생성합니다.

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
aggr1_nodeA –size 1GB –type DP
volume create –vserver Infra_Vserver –volume rootvol_m02 –aggregate
aggr1_nodeB –size 1GB –type DP
```

2. 15분마다 루트 볼륨 미러 관계를 업데이트하는 작업 스케줄을 생성합니다.

```
job schedule interval create -name 15min -minutes 15
```

3. 미러링 관계를 생성합니다.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. 미러링 관계를 초기화하고 미러링 관계가 만들어졌는지 확인합니다.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
snapmirror show
```

ONTAP에서 HTTPS 액세스를 구성합니다

스토리지 컨트롤러에 대한 보안 액세스를 구성하려면 다음 단계를 수행하십시오.

1. 인증서 명령에 액세스할 수 있도록 권한 수준을 높입니다.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. 일반적으로 자체 서명된 인증서가 이미 있습니다. 다음 명령을 실행하여 인증서를 확인합니다.

```
security certificate show
```

3. 표시된 각 SVM에서 인증서 공통 이름은 SVM의 DNS FQDN과 일치해야 합니다. 네 개의 기본 인증서를 삭제하고 자체 서명된 인증서 또는 인증 기관의 인증서로 대체해야 합니다.

> 인증서를 만들기 전에 만료된 인증서를 삭제하는 것이 좋습니다. 만료된 인증서를 삭제하려면 보안 인증서 삭제 명령을 실행합니다. 다음 명령에서 Tab completion을 사용하여 각 기본 인증서를 선택하고 삭제합니다.

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. 자체 서명된 인증서를 생성하고 설치하려면 다음 명령을 일회성 명령으로 실행합니다. 인프라 SVM 및 클러스터 SVM에 대한 서버 인증서를 생성합니다. 다시 한 번 탭 완료 기능을 사용하면 이러한 명령을 쉽게 완료할 수 있습니다.

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm.netapp.com
-type server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 3650 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. 다음 단계에 필요한 매개 변수의 값을 가져오려면 security certificate show 명령을 실행합니다.
6. '–server-enabled true' 및 '–client-enabled false' 매개 변수를 사용하여 방금 만든 각 인증서를 활성화합니다. 다시 탭 완료를 사용합니다.

```
security ssl modify [TAB] …
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. SSL 및 HTTPS 액세스를 구성 및 활성화하고 HTTP 액세스를 비활성화합니다.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
–vserver <<var_clustername>>
```

명령 실행 중 일부에서 항목이 존재하지 않는다는 오류 메시지가 반환되는 것은 정상입니다.

8. 관리 권한 수준으로 되돌아가며 설치를 생성하여 SVM을 웹에서 사용할 수 있도록 합니다.

```
set -privilege admin
vserver services web modify -name spi -vserver * -enabled true
```

ONTAP에서 NetApp FlexVol 볼륨을 생성합니다

NetApp FlexVol ® 볼륨을 생성하려면 볼륨 이름, 크기 및 해당 볼륨을 입력합니다. 2개의 VMware 데이터 저장소 볼륨과 서버 부팅 볼륨을 생성합니다.

```
volume create -vserver Infra-SVM -volume infra_datastore -aggregate
aggr1_nodeB -size 500GB -state online -policy default -junction-path
/infra_datastore -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
-efficiency-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

ONTAP에서 LUN을 생성합니다

2개의 부팅 LUN을 생성하려면 다음 명령을 실행합니다.

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```

Cisco UCS C-Series 서버를 더 추가할 때는 부팅 LUN을 더 생성해야 합니다.

ONTAP에서 iSCSI LIF를 생성합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
스토리지 노드 A iSCSI LIF01A	<<var_NodeA_iscsi_lif01a_ip>> 를 참조하십시오
스토리지 노드 A iSCSI LIF01A 네트워크 마스크입니다	<<var_NodeA_iscsi_lif01a_mask>>
스토리지 노드 A iSCSI LIF01B	<<var_NodeA_iscsi_liff 01b_ip>> 를 참조하십시오

세부 정보	상세 값
스토리지 노드 A iSCSI LIF01B 네트워크 마스크입니다	<<var_NodeA_iscsi_liff 01b_mask>>
스토리지 노드 B iSCSI LIF01A	<<var_NodeB_iscsi_liff 01a_ip>>
스토리지 노드 B iSCSI LIF01A 네트워크 마스크입니다	<<var_NodeB_iscsi_liff 01a_mask>>
스토리지 노드 B iSCSI LIF01B	<<var_NodeB_iscsi_liff 01b_ip>>
스토리지 노드 B iSCSI LIF01B 네트워크 마스크입니다	<<var_NodeB_iscsi_liff 01b_mask>>

각 노드에 2개의 iSCSI LIF를 4개 생성합니다.

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface show
```

ONTAP에서 NFS LIF를 생성합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
스토리지 노드 A NFS LIF 01 IP입니다	<<var_NodeA_nfs_lif_01_ip>>
스토리지 노드 A NFS LIF 01 네트워크 마스크	<<var_NodeA_nfs_lif_01_mask>>
스토리지 노드 B NFS LIF 02 IP	<<var_NodeB_nfs_lif_02_ip>>
스토리지 노드 B NFS LIF 02 네트워크 마스크	<<var_NodeB_nfs_lif_02_mask>>

NFS LIF를 생성합니다.

```
network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface show
```

인프라 **SVM** 관리자를 추가합니다

다음 표에는 SVM 관리자를 추가하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
Vsmgmt IP	<<var_svm_mgmt_ip>> 를 입력합니다
Vsmgmt 네트워크 마스크	<<var_svm_mgmt_mask>>
Vsmgmt 기본 게이트웨이	<<var_svm_mgmt_gateway>>

관리 네트워크에 인프라 SVM 관리자 및 SVM 관리 논리 인터페이스를 추가하려면 다음 단계를 완료하십시오.

1. 다음 명령을 실행합니다.

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data
-data-protocol none –home-node <<var_nodeB>> -home-port  e0M –address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
–failover-policy broadcast-domain-wide –firewall-policy mgmt –auto-
revert true
```

ⓘ 여기서 SVM 관리 IP는 스토리지 클러스터 관리 IP와 동일한 서브넷에 있어야 합니다.

2. 기본 경로를 생성하여 SVM 관리 인터페이스가 외부 환경에 도달할 수 있도록 합니다.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. SVM vsadmin 사용자의 암호를 설정하고 사용자 잠금을 해제합니다.

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock –username vsadmin –vserver Infra-SVM
```

"다음으로 Cisco UCS C-Series 랙 서버를 구축합니다."

Cisco UCS C-Series 랙 서버 구축

이 섹션에서는 FlexPod Express 구성에 사용할 Cisco UCS C-Series 독립 실행형 랙 서버를 구성하기 위한 절차를 세부적으로 설명합니다.

CIMC에 대한 초기 Cisco UCS C-Series 독립 실행형 서버 설정을 수행합니다

Cisco UCS C-Series 독립 실행형 서버에 대한 CIMC 인터페이스의 초기 설정을 위해 다음 단계를 완료합니다.

다음 표에는 각 Cisco UCS C-Series 독립 실행형 서버에 대한 CIMC를 구성하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
CIMC IP 주소	CIMC_IP>\< CIMC_IP>>
CIMC 서브넷 마스크	CIMC_NETMASK
CIMC 기본 게이트웨이	CIMC_GATELOGATE>\<<CIMC_Gateway>

ⓘ 이 검증에 사용된 CIMC 버전은 CIMC 4.0입니다(4).

모든 서버

1. 서버와 함께 제공된 Cisco 키보드, 비디오 및 마우스(KVM) 동글을 서버 앞의 KVM 포트에 연결합니다. VGA 모니터와 USB 키보드의 플러그를 적절한 KVM 동글 포트에 꽂습니다.

   서버의 전원을 켜고 CIMC 구성을 시작할지 묻는 메시지가 표시되면 F8 키를 누릅니다.



2. CIMC 구성 유틸리티에서 다음 옵션을 설정합니다.

   a. 네트워크 인터페이스 카드(NIC) 모드:

      전용 '[X]'

   b. IP(기본):

      IPv4: '[X]'

      DHCP 활성화: "[]"

      CIMC IP:<<CIMC_IP>>'를 선택합니다

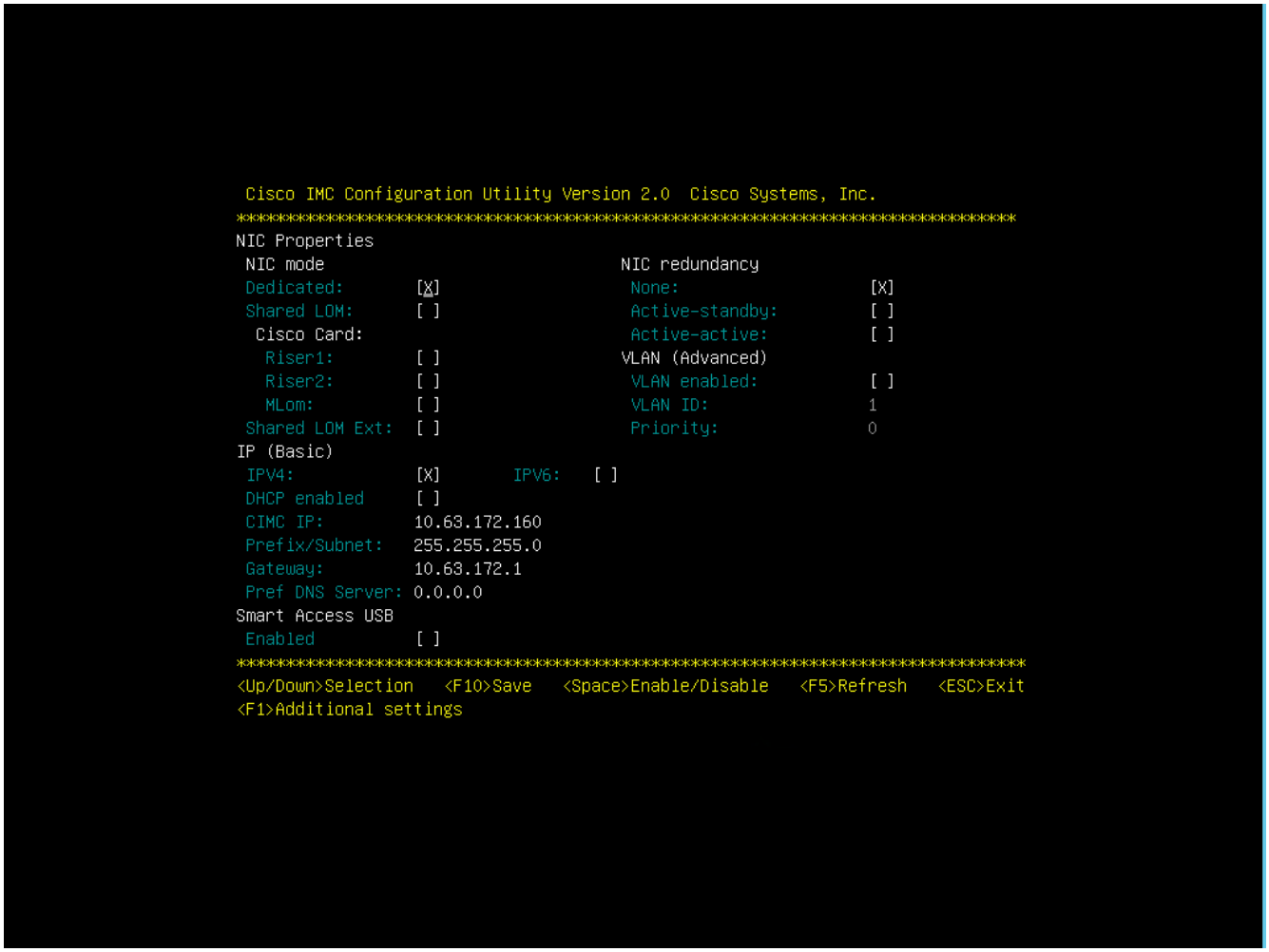
      Prefix/Subnet:<<CIMC_Netmask>>'입니다

      Gateway:<<CIMC_Gateway>>'입니다

   c. VLAN(고급): VLAN 태깅을 사용하지 않도록 설정하려면 선택되지 않은 상태로 둡니다.

      NIC 이중화

      없음: '[X]'



3. F1을 눌러 추가 설정을 확인합니다.

   a. 공통 속성:

      호스트 이름: "\< ESXi_host_name>>"

      동적 DNS: "[]"

      공장 출하시 기본값: 선택하지 않은 상태로 둡니다.

   b. 기본 사용자(기본):

      기본 암호: "<<admin_password>>"

      '\<<admin_password>' 암호를 다시 입력하십시오

      포트 속성: 기본값을 사용합니다.

   포트 프로파일: 선택하지 않은 상태로 둡니다.

4. F10 키를 눌러 CIMC 인터페이스 구성을 저장합니다.
5. 구성을 저장한 후 Esc 키를 눌러 종료합니다.

Cisco UCS C-Series 서버 iSCSI 부트를 구성합니다

이 FlexPod Express 구성에서 VIC1457은 iSCSI 부팅에 사용됩니다.

다음 표에는 iSCSI 부트를 구성하는 데 필요한 정보가 나와 있습니다.

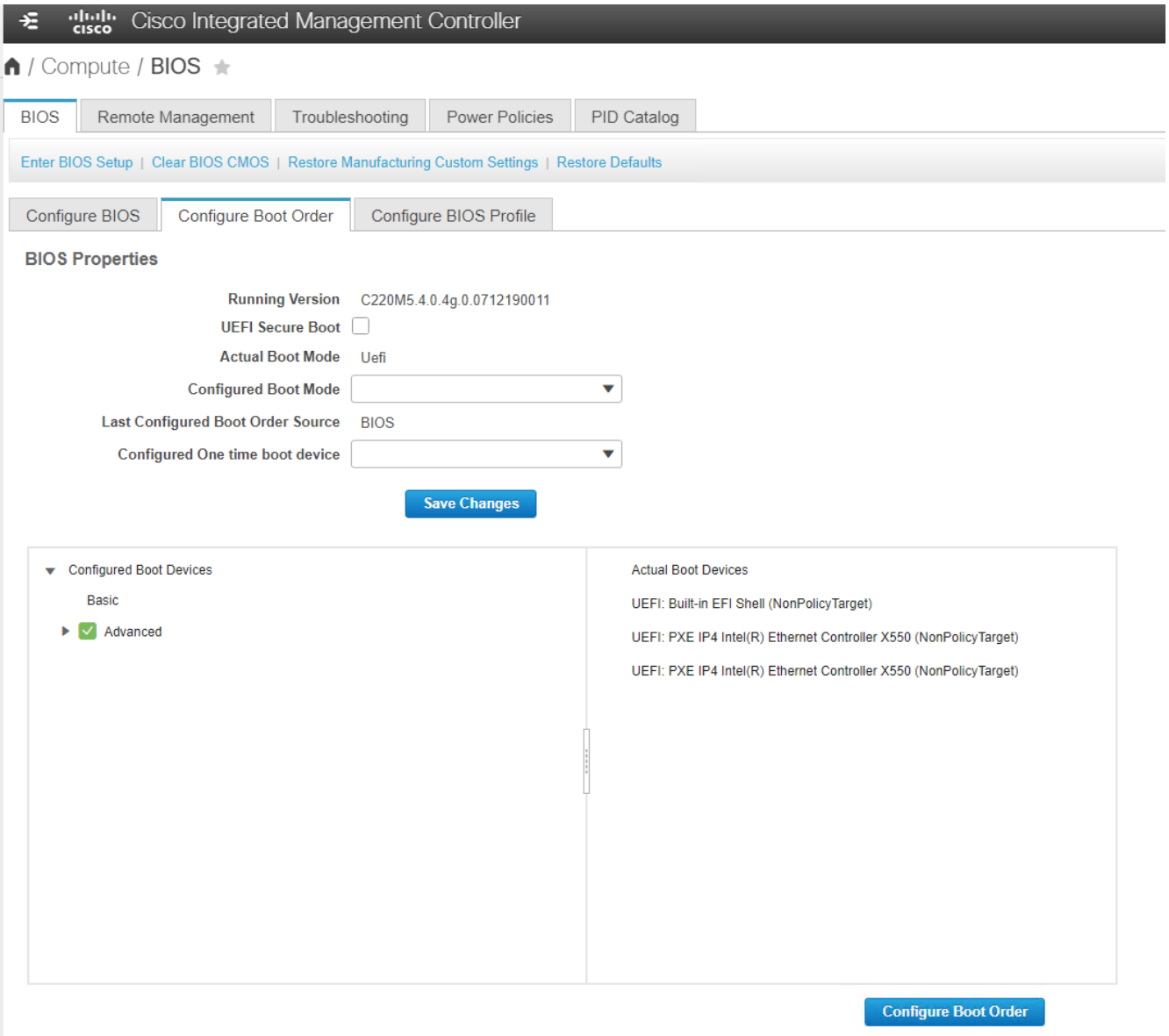
기울임꼴로 표시된 글꼴은 각 ESXi 호스트에 대해 고유한 변수를 나타냅니다.

세부 정보	상세 값
ESXi 호스트 이니시에이터에서 이름을 입력합니다	<<var_UCS_initiator_name_a>>
ESXi 호스트 iSCSI - A IP	<<var_esxi_host_iscsiA_ip>>
ESXi 호스트 iSCSI - 네트워크 마스크입니다	<<var_esxi_host_iscsiA_mask>>
ESXi 호스트 iSCSI 기본 게이트웨이입니다	<<var_esxi_host_iscsiA_gateway>>
ESXi 호스트 이니시에이터 B 이름입니다	<<var_UCS_initiator_name_B>>
ESXi 호스트 iSCSI-B IP	<<var_esxi_host_iscsiB_ip>>
ESXi 호스트 iSCSI-B 네트워크 마스크	<<var_esxi_host_iscsiB_mask>>
ESXi 호스트 iSCSI-B 게이트웨이	<<var_esxi_host_iscsiB_gateway>>
IP 주소 iscsi_liff 01a	<<var_iscsi_liff 01a>>
IP 주소 iscsi_lif02a	<<var_iscsi_lif02a>> 를 참조하십시오
IP 주소 iscsi_liff 01b	<<var_iscsi_liff 01b>>
IP 주소 iscsi_liff 02b	<<var_iscsi_liff 02b>> 를 참조하십시오
infra_SVM IQN을 선택합니다	<<var_SVM_IQN>>을 참조하십시오

부팅 순서 구성

부팅 순서 구성을 설정하려면 다음 단계를 수행하십시오.

1. CIMC 인터페이스 브라우저 창에서 Compute 탭을 클릭하고 BIOS를 선택합니다.
2. Configure Boot Order(부팅 순서 구성) 를 클릭한 다음 OK(확인) 를 클릭합니다.



3. Add Boot Device(부팅 장치 추가) 에서 장치를 클릭하고 Advanced(고급) 탭으로 이동하여 다음 장치를 구성합니다.

   a. 가상 미디어 추가:

      이름: kvm-cd-dvd

      하위 유형: KVM 매핑된 DVD

      상태: 활성화됨

      순서: 1

   b. iSCSI 부팅 추가:

      이름: iscsi-a

      상태: 활성화됨

주문: 2

슬롯: mLOM

포트: 1

c. Add iSCSI Boot(iSCSI 부팅 추가) 를 클릭합니다.

이름: iSCSI-B

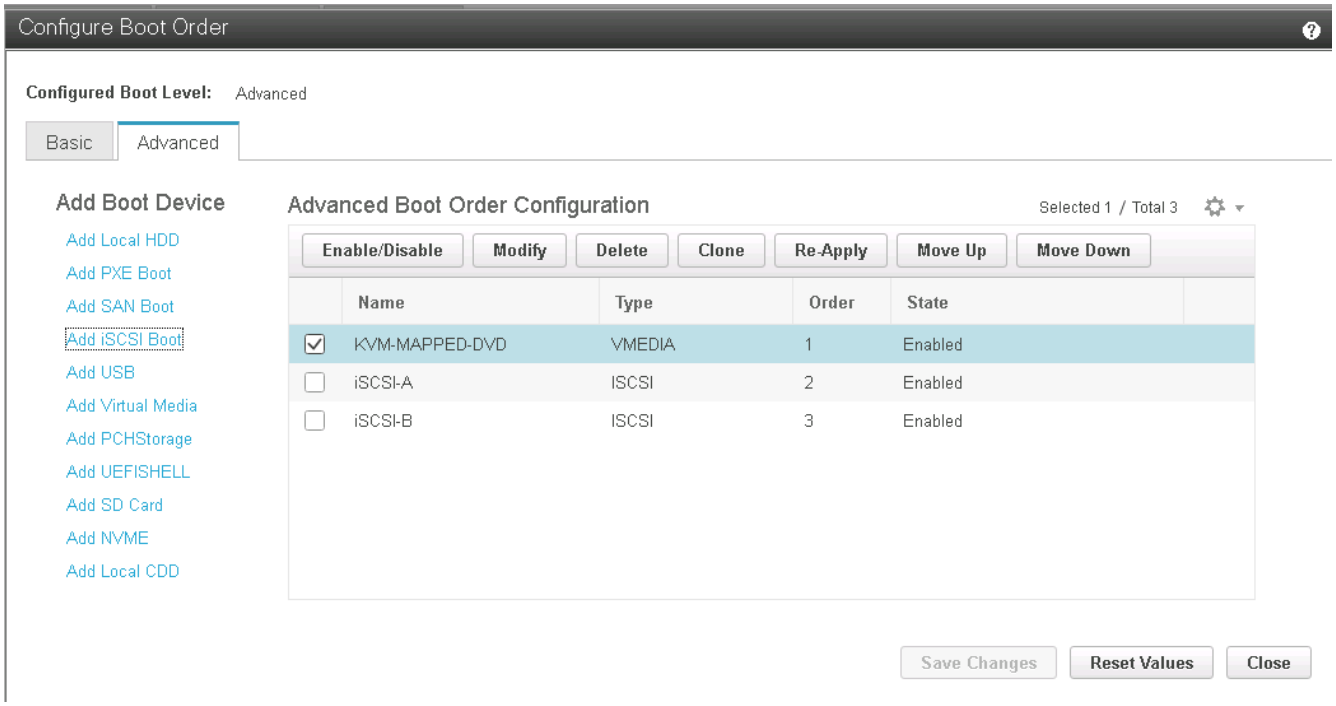
상태: 활성화됨

순서: 3

슬롯: mLOM

포트: 3

4. 장치 추가를 클릭합니다.
5. 변경 내용 저장 을 클릭한 다음 닫기 를 클릭합니다.



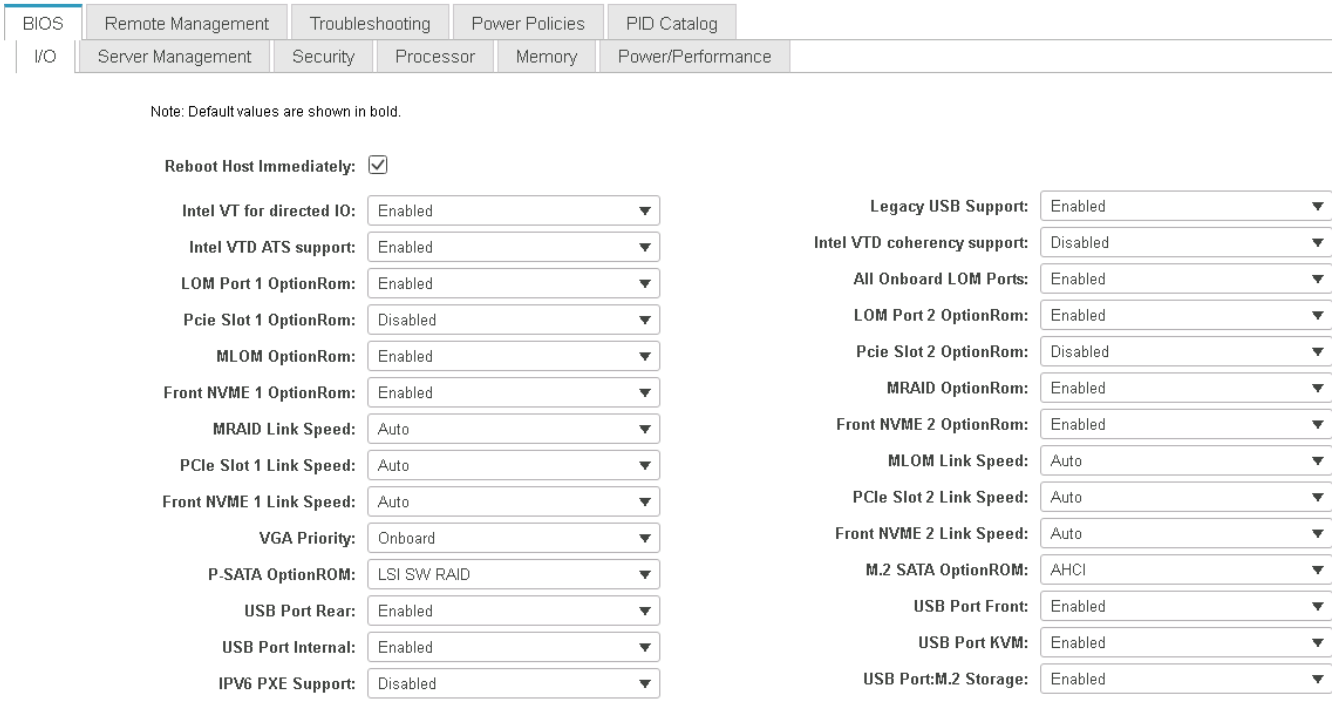
6. 새 부팅 순서로 부팅하려면 서버를 재부팅합니다.

RAID 컨트롤러 비활성화**(**있는 경우**)**

C 시리즈 서버에 RAID 컨트롤러가 포함되어 있는 경우 다음 단계를 수행하십시오. SAN 구성으로 부팅할 때 RAID 컨트롤러가 필요하지 않습니다. 선택적으로 서버에서 RAID 컨트롤러를 물리적으로 제거할 수도 있습니다.

1. Compute 탭의 CIMC의 왼쪽 탐색 창에서 BIOS를 클릭합니다.
2. Configure BIOS 를 선택합니다.

3. PCIe 슬롯: HBA 옵션 ROM으로 아래로 스크롤합니다.
4. 이 값이 아직 비활성화되지 않은 경우 비활성화로 설정합니다.

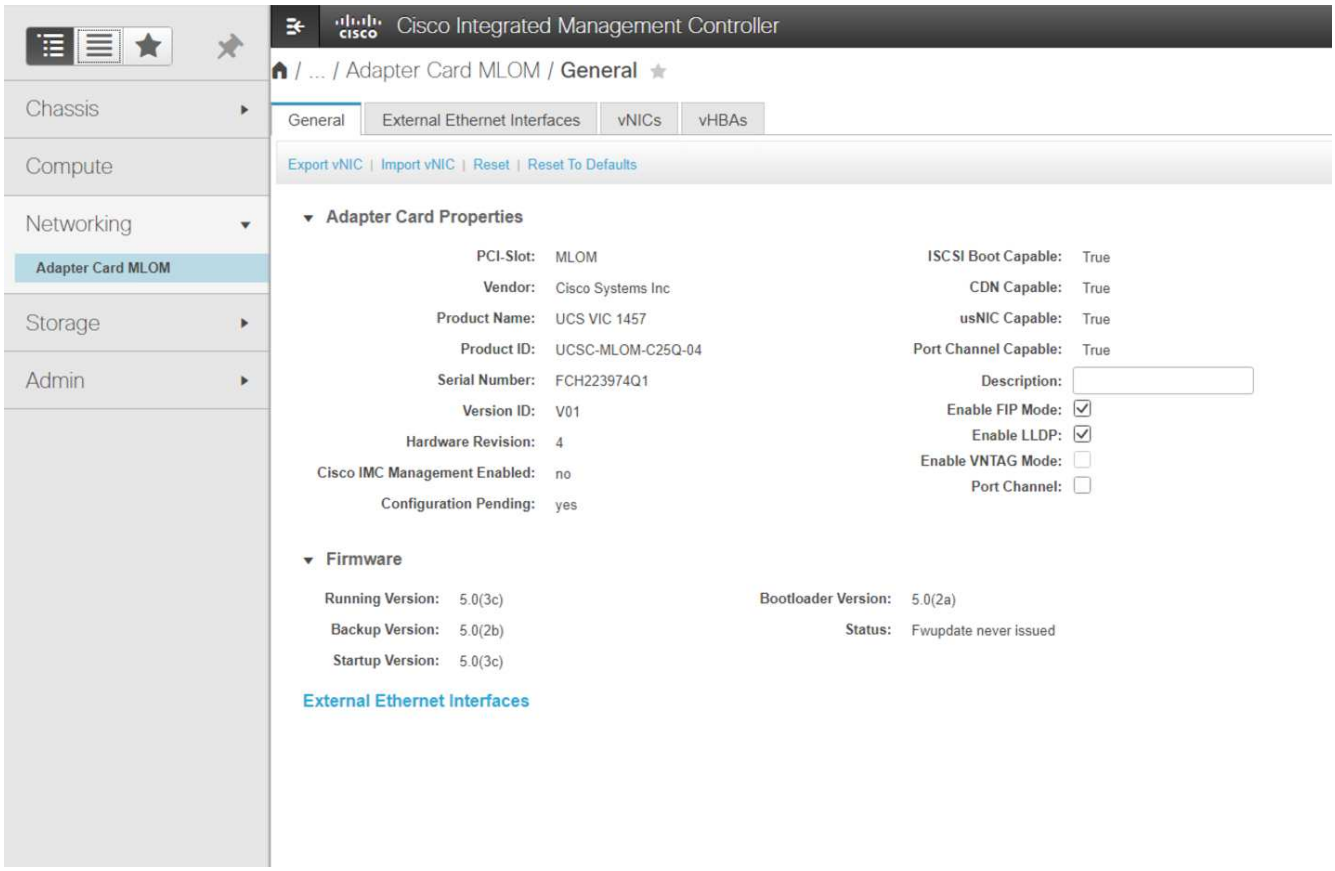


iSCSI 부트에 대해 **Cisco VIC1457**을 구성합니다

다음 구성 단계는 iSCSI 부트에 대한 Cisco VIC 1457에 대한 것입니다.

> 포트 0, 1, 2 및 3 간의 기본 포트 채널링을 해제해야 4개의 개별 포트를 구성할 수 있습니다. 포트 채널링이 꺼져 있지 않으면 VIC 1457에 대해 포트 두 개만 나타납니다. CIMC에서 포트 채널을 설정하려면 다음 단계를 완료하십시오.

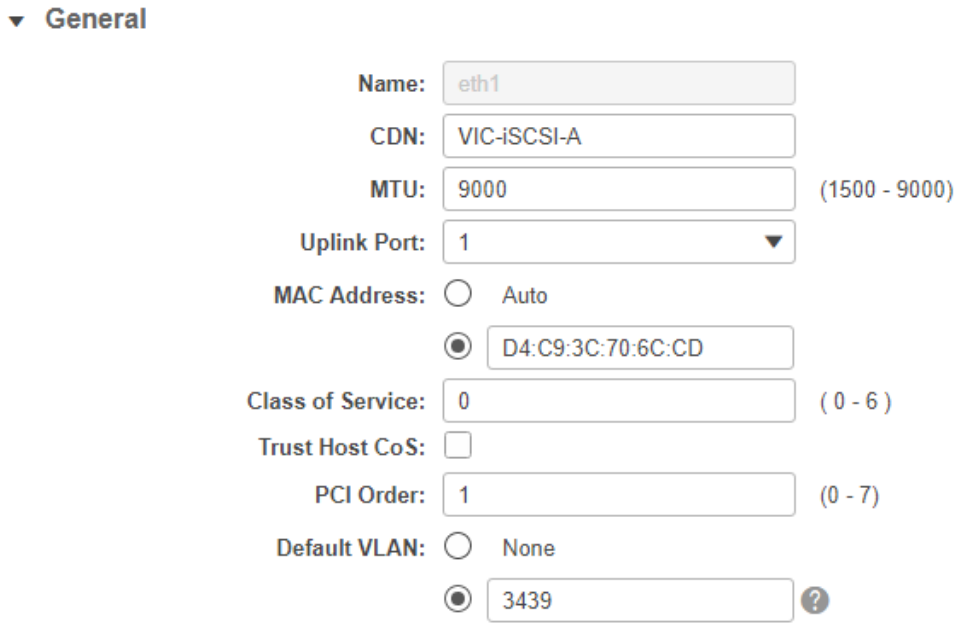
1. 네트워킹 탭에서 어댑터 카드 mLOM을 클릭합니다.
2. 일반 탭에서 포트 채널을 선택 취소합니다.
3. 변경 내용을 저장하고 CIMC를 재부팅합니다.



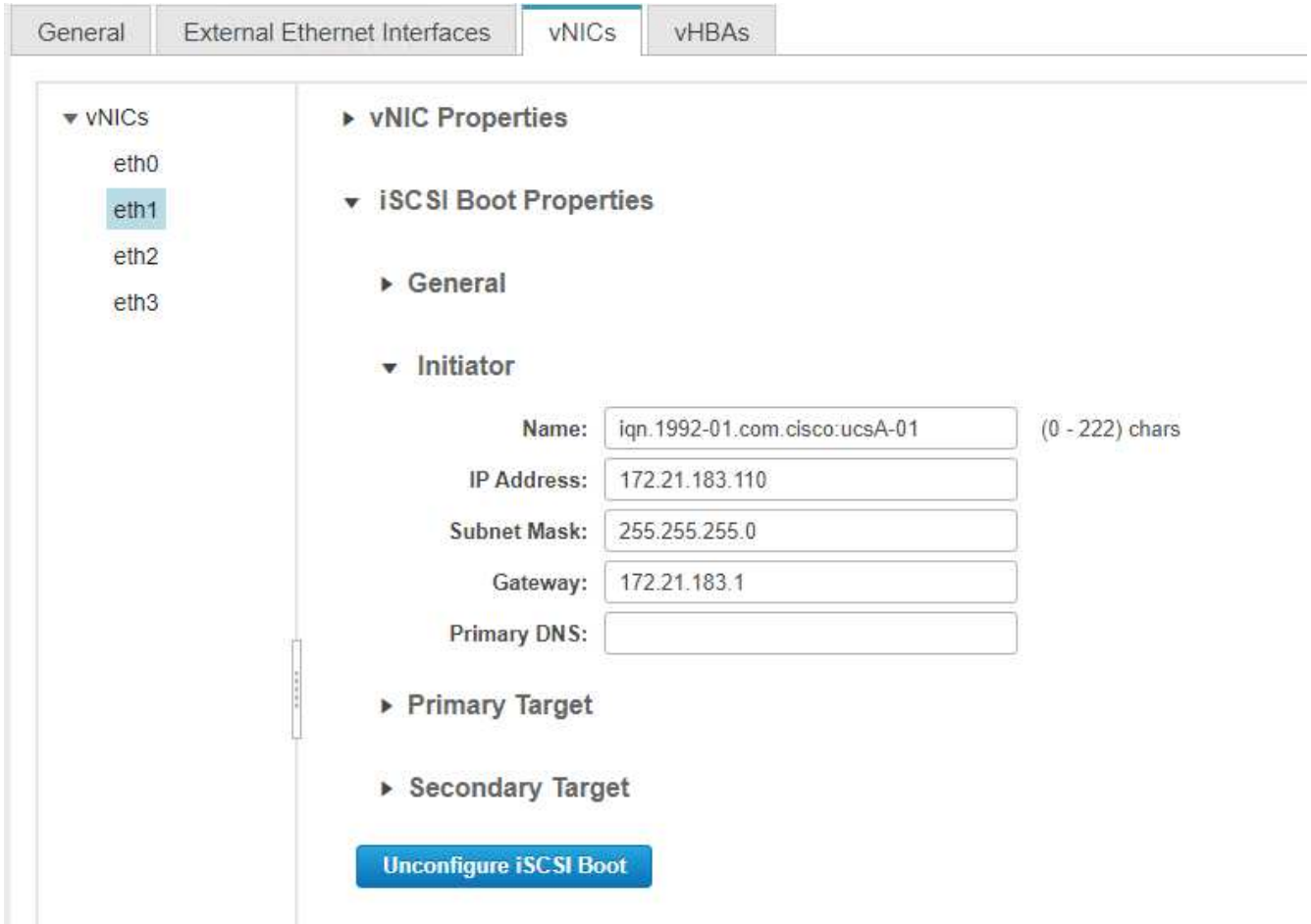
iSCSI vNIC를 생성합니다

iSCSI vNIC를 생성하려면 다음 단계를 수행하십시오.

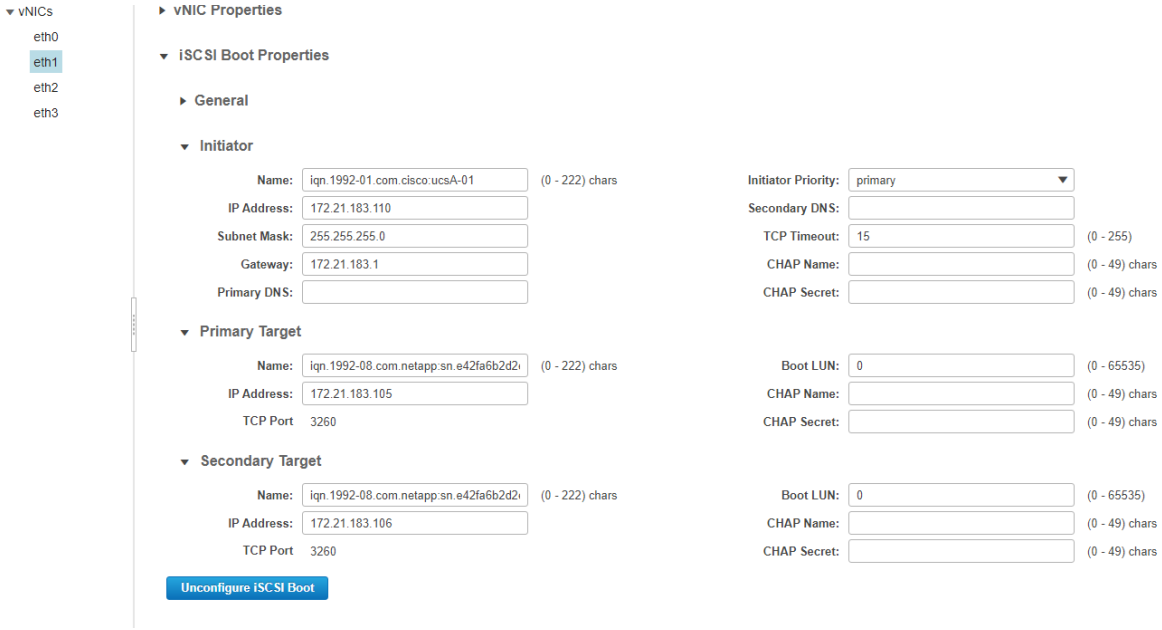
1. 네트워킹 탭에서 어댑터 카드 mLOM 을 클릭합니다.
2. vNIC 추가를 클릭하여 vNIC를 생성합니다.
3. vNIC 추가 섹션에서 다음 설정을 입력합니다.
   - 이름: eth1
   - CDN 이름: iSCSI-vNIC-A
   - MTU: 9000
   - 기본 VLAN:<<var_iscsi_vlan_a>>'입니다
   - VLAN 모드: 트렁크
   - PXE 부팅 활성화: 확인
4. vNIC 추가 를 클릭한 다음 확인 을 클릭합니다.
5. 이 과정을 반복하여 두 번째 vNIC를 추가합니다.
   - vNIC eth3의 이름을 지정합니다.
   - CDN 이름: iSCSI-vNIC-B
   - VLAN으로 '<<var_iscsi_vlan_b>>'를 입력합니다.
   - 업링크 포트를 3으로 설정합니다.



6. 왼쪽에서 vNIC eth1을 선택합니다.



7. iSCSI 부트 속성에서 이니시에이터 세부 정보를 입력합니다.
   - 이름:<<var_ucsa_initiator_name_a>>'
   - IP 주소: "<<var_esxi_hostA_iscsiA_ip>>"
   - 서브넷 마스크: "<<var_esxi_hostA_iscsiA_mask>>"
   - 게이트웨이: "\<<var_esxi_hostA_iscsiA_gateway>>"



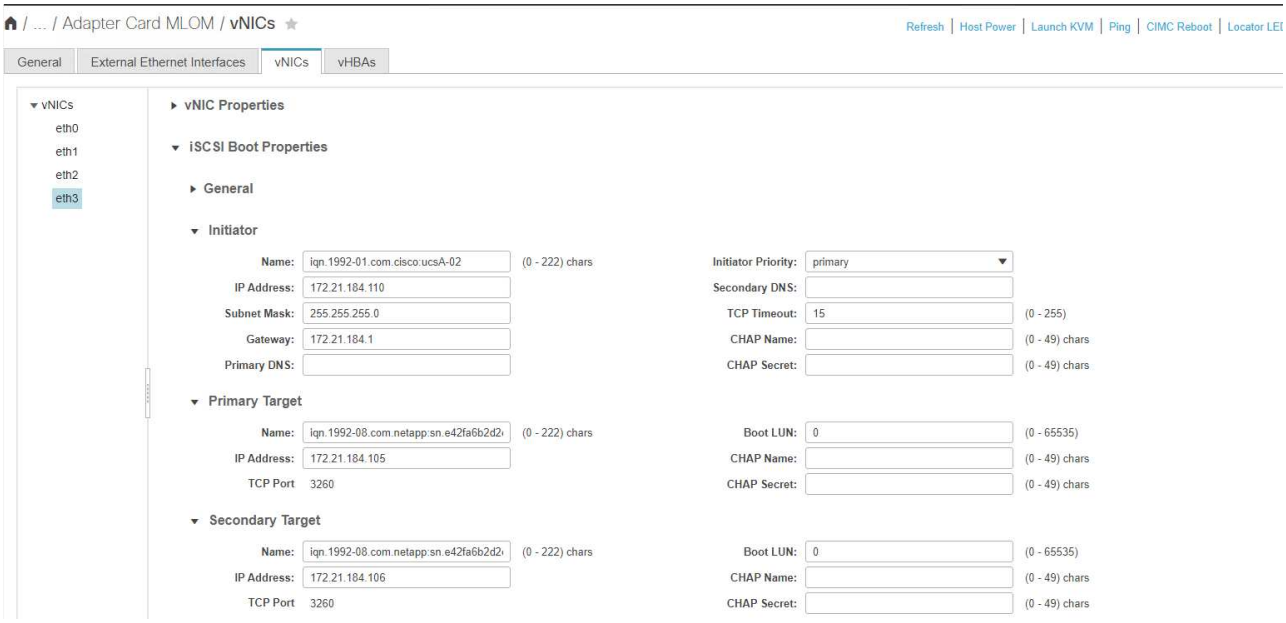
8. 기본 타겟 세부 정보를 입력합니다.
   - 이름: 인프라 SVM의 IQN 번호입니다
   - IP 주소: iSCSI_liff 01a의 IP 주소입니다
   - 부팅 LUN: 0
9. 2차 타겟 세부 정보를 입력합니다.
   - 이름: 인프라 SVM의 IQN 번호입니다
   - IP 주소: iscsi_lif02a 의 IP 주소입니다
   - 부팅 LUN: 0

> "vserver iscsi show" 명령을 실행하여 스토리지 IQN 번호를 확인할 수 있습니다.

> 각 vNIC의 IQN 이름을 기록해야 합니다. 나중에 필요한 단계일 수 있습니다. 또한 이니시에이터의 IQN 이름은 각 서버 및 iSCSI vNIC에 대해 고유해야 합니다.

10. 변경 내용 저장 을 클릭합니다.
11. vNIC eth3을 선택하고 호스트 이더넷 인터페이스 섹션 상단에 있는 iSCSI 부트 버튼을 클릭합니다.
12. 이 과정을 반복하여 eth3을 구성합니다.
13. 이니시에이터 세부 정보를 입력합니다.

- 이름:<<var_ucsa_initiator_name_b>>'
- IP 주소: "<<var_esxi_hostB_iscsib_ip>>"
- 서브넷 마스크: "<<var_esxi_hostB_iscsib_mask>>"
- 게이트웨이:\<<var_esxi_hostB_iscsib_gateway>'



14. 기본 타겟 세부 정보를 입력합니다.
    - 이름: 인프라 SVM의 IQN 번호입니다
    - IP 주소: iSCSI_liff 01b의 IP 주소입니다
    - 부팅 LUN: 0
15. 2차 타겟 세부 정보를 입력합니다.
    - 이름: 인프라 SVM의 IQN 번호입니다
    - IP 주소: iSCSI_liff 02b의 IP 주소입니다
    - 부팅 LUN: 0

> "vserver iscsi show" 명령을 사용하여 스토리지 IQN 번호를 가져올 수 있습니다.

> 각 vNIC의 IQN 이름을 기록해야 합니다. 나중에 필요한 단계일 수 있습니다.

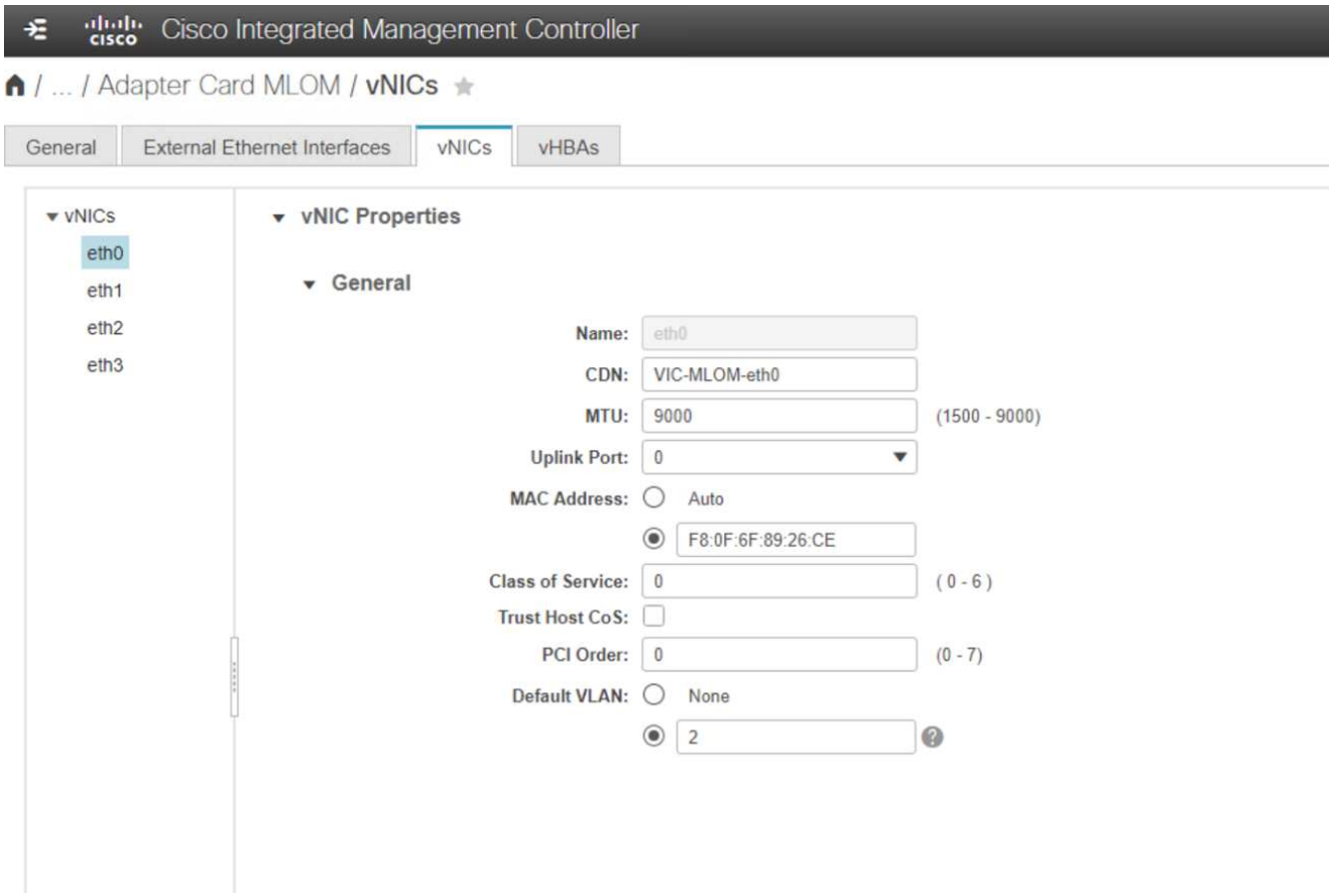
16. 변경 내용 저장 을 클릭합니다.
17. 이 프로세스를 반복하여 Cisco UCS 서버 B에 대한 iSCSI 부팅을 구성합니다

ESXi용 **vNIC**를 구성합니다

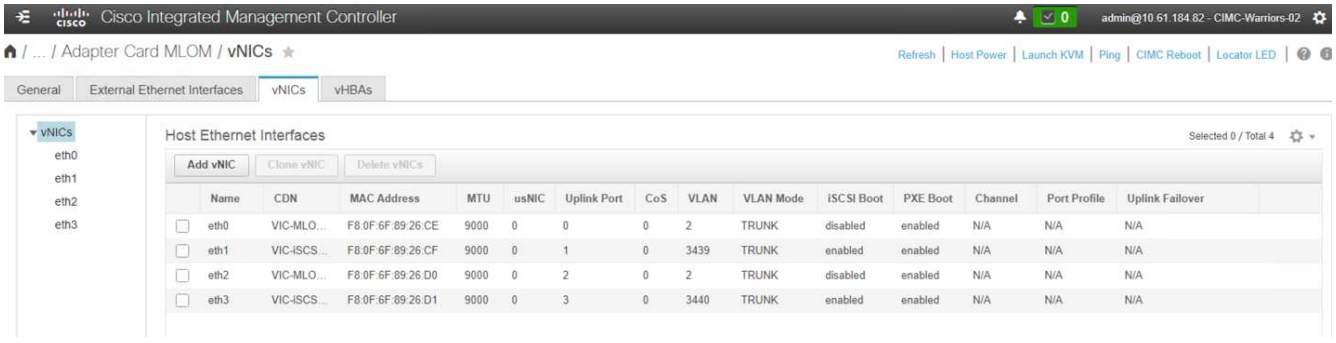
ESXi용 vNIC를 구성하려면 다음 단계를 수행하십시오.

1. CIMC 인터페이스 브라우저 창에서 인벤토리 를 클릭한 다음 오른쪽 창에서 Cisco VIC 어댑터 를 클릭합니다.

2. 네트워킹 > 어댑터 카드 mLOM 에서 vNIC 탭을 선택한 다음 아래에서 vNIC를 선택합니다.
3. eth0 을 선택하고 속성 을 클릭합니다.
4. MTU를 9000으로 설정합니다. 변경 내용 저장 을 클릭합니다.
5. VLAN을 네이티브 VLAN 2로 설정합니다.



6. eth1에 대해 3단계와 4단계를 반복하여 업링크 포트가 eth1에 대해 1로 설정되어 있는지 확인합니다.



이 절차는 각 초기 Cisco UCS 서버 노드 및 환경에 추가된 각 추가 Cisco UCS 서버 노드에 대해 반복해야 합니다.

"다음은 NetApp AFF 스토리지 구축 절차(2부)입니다."

NetApp AFF 스토리지 구축 절차(2부)

ONTAP SAN 부팅 스토리지를 설정합니다

iSCSI igroup을 생성합니다

이 단계를 위해서는 서버 구성에서 iSCSI 이니시에이터 IQN이 필요합니다.

igroup을 생성하려면 클러스터 관리 노드의 SSH 연결에서 다음 명령을 실행합니다. 이 단계에서 만든 3개의 igroup을 보려면 'igroup show' 명령을 실행합니다.

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-A –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_a_iSCSI-
A_vNIC_IQN>>,<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-B –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_b_iSCSI-
A_vNIC_IQN>>,<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```

Cisco UCS C-Series 서버를 추가할 때는 이 단계를 완료해야 합니다.

부팅 LUN을 igroup에 매핑합니다

```
To map boot LUNs to igroups, run the following commands from the cluster
management SSH connection:
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra-A –igroup
VM-Host-Infra-A –lun-id 0
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra-B –igroup
VM-Host-Infra-B –lun-id 0
```

Cisco UCS C-Series 서버를 추가할 때는 이 단계를 완료해야 합니다.

"다음: VMware vSphere 6.7U2 구축 절차"

VMware vSphere 6.7U2 구축 절차

이 섹션에서는 FlexPod Express 구성에 VMware ESXi 6.7U2를 설치하기 위한 절차를 자세히 설명합니다. 다음 구현 절차는 이전 섹션에서 설명한 환경 변수를 포함하도록 커스터마이징되었습니다.

이러한 환경에 VMware ESXi를 설치하는 방법은 여러 가지가 있습니다. 이 절차에서는 Cisco UCS C-Series 서버용 CIMC 인터페이스의 가상 KVM 콘솔과 가상 미디어 기능을 사용하여 원격 설치 미디어를 각 개별 서버에 매핑합니다.

이 절차는 Cisco UCS 서버 A 및 Cisco UCS 서버 B에 대해 완료되어야 합니다

클러스터에 추가된 노드에 대해 이 절차를 완료해야 합니다.

Cisco UCS C-Series 독립 실행형 서버에 대한 CIMC 인터페이스에 로그인합니다

다음 단계에서는 Cisco UCS C-Series 독립 실행형 서버의 CIMC 인터페이스에 로그인하는 방법을 자세히 설명합니다. CIMC 인터페이스에 로그인하여 가상 KVM을 실행해야 관리자가 원격 미디어를 통해 운영 체제 설치를 시작할 수 있습니다.

모든 호스트

1. 웹 브라우저로 이동하고 Cisco UCS C-Series의 CIMC 인터페이스에 대한 IP 주소를 입력합니다. 이 단계에서는 CIMC GUI 애플리케이션이 시작됩니다.
2. 관리자의 사용자 이름과 자격 증명을 사용하여 CIMC UI에 로그인합니다.
3. 주 메뉴에서 서버 탭을 선택합니다.
4. Launch KVM Console을 클릭합니다.



5. 가상 KVM 콘솔에서 Virtual Media 탭을 선택합니다.
6. CD/DVD 매핑 을 선택합니다.

먼저 가상 디바이스 활성화 를 클릭해야 할 수도 있습니다. 메시지가 표시되면 이 세션 수락 을 선택합니다.

7. VMware ESXi 6.7U2 설치 관리자 ISO 이미지 파일을 찾아 이동하고 Open을 클릭합니다. 장치 매핑 을 클릭합니다.
8. Power 메뉴를 선택하고 Power Cycle System (Cold Boot) 을 선택합니다. 예 를 클릭합니다.

VMware ESXi를 설치합니다

다음 단계에서는 각 호스트에 VMware ESXi를 설치하는 방법을 설명합니다.

ESXi 6.7U2 Cisco 사용자 지정 이미지를 다운로드합니다

1. 로 이동합니다 "VMware vSphere 다운로드 페이지" 사용자 정의 ISO의 경우.
2. ESXi 6.7U2 설치 CD의 Cisco 사용자 지정 이미지 옆에 있는 다운로드로 이동 을 클릭합니다.
3. ESXi 6.7U2 설치 CD(ISO)용 Cisco 사용자 지정 이미지를 다운로드합니다.
4. 시스템이 부팅되면 VMware ESXi 설치 미디어의 존재 여부가 자동으로 감지됩니다.
5. 나타나는 메뉴에서 VMware ESXi 설치 프로그램을 선택합니다. 설치 프로그램이 로드되는데, 이 작업은 몇 분 정도 걸릴 수 있습니다.
6. 설치 프로그램 로드가 완료된 후 Enter 키를 눌러 설치를 계속합니다.
7. 최종 사용자 사용권 계약을 읽은 후 동의하고 F11 키를 눌러 설치를 계속합니다.

8. 이전에 ESXi용 설치 디스크로 설정된 NetApp LUN을 선택하고 Enter 키를 눌러 설치를 계속합니다.



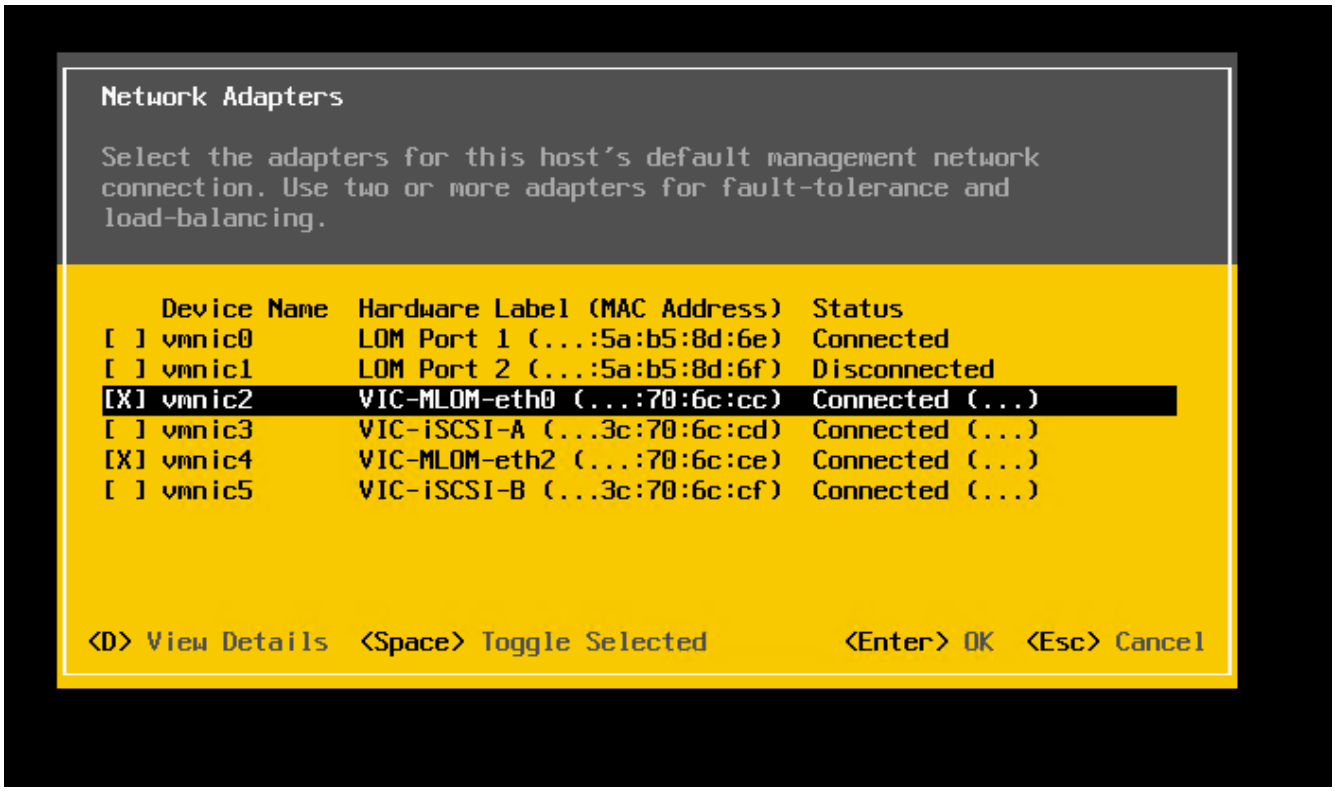
9. 적절한 자판 배열을 선택하고 Enter 키를 누릅니다.
10. 루트 암호를 입력 및 확인하고 Enter 키를 누릅니다.
11. 볼륨에서 기존 파티션이 제거된다는 경고 메시지가 표시됩니다. F11 키를 눌러 설치를 계속합니다. ESXi 설치 후 서버가 재부팅됩니다.

VMware ESXi 호스트 관리 네트워킹을 설정합니다

다음 단계에서는 각 VMware ESXi 호스트의 관리 네트워크를 추가하는 방법을 설명합니다.

모든 호스트

1. 서버 재부팅이 완료된 후 F2 키를 눌러 시스템 커스터마이징 옵션을 시작합니다.
2. root라는 로그인 이름과 이전에 설치 과정에서 입력한 루트 암호를 사용하여 로그인합니다.
3. Configure Management Network 옵션을 선택합니다.
4. Network Adapters 를 선택하고 Enter 키를 누릅니다.
5. vSwitch0에 대해 원하는 포트를 선택합니다. Enter 키를 누릅니다.
6. CIMC의 eth0 및 eth1에 해당하는 포트를 선택합니다.



7. VLAN (optional)을 선택하고 Enter 키를 누릅니다.
8. VLAN ID '<<mgmt_vlan_id>>'를 입력합니다. Enter 키를 누릅니다.
9. Configure Management Network 메뉴에서 IPv4 Configuration을 선택하여 관리 인터페이스의 IP 주소를 구성합니다. Enter 키를 누릅니다.
10. 화살표 키를 사용하여 정적 IPv4 주소 설정 을 강조 표시하고 스페이스바를 사용하여 이 옵션을 선택합니다.
11. VMware ESXi 호스트 "\< ESXi_host_mgmt_ip>>"를 관리하기 위한 IP 주소를 입력합니다.
12. VMware ESXi 호스트 "\< ESXi_host_mgmt_netmask>"의 서브넷 마스크를 입력합니다.
13. VMware ESXi 호스트 '\< ESXi_host_mgmt_gateway>'의 기본 게이트웨이를 입력합니다.
14. Enter 키를 눌러 IP 구성의 변경 사항을 적용합니다.
15. IPv6 구성 메뉴로 들어갑니다.
16. 스페이스바를 사용하여 IPv6 사용(재시작 필요) 옵션을 선택 취소하여 IPv6을 사용하지 않도록 설정합니다. Enter 키를 누릅니다.
17. DNS 설정을 구성하는 메뉴로 들어갑니다.
18. IP 주소는 수동으로 할당되므로 DNS 정보도 수동으로 입력해야 합니다.
19. Primary DNS 서버의 IP 주소 "\< nameserver_ip>>"를 입력합니다.
20. (선택 사항) 보조 DNS 서버의 IP 주소를 입력합니다.
21. VMware ESXi 호스트 이름 "\< ESXi_host_FQDN>"의 FQDN을 입력합니다.
22. Enter 키를 눌러 DNS 구성의 변경 사항을 적용합니다.
23. Esc 키를 눌러 Configure Management Network 하위 메뉴를 종료합니다.
24. Y 를 눌러 변경 사항을 확인하고 서버를 재부팅합니다.

25. 문제 해결 옵션 을 선택한 다음 ESXi Shell 및 SSH 활성화 를 선택합니다.

    이러한 문제 해결 옵션은 고객의 보안 정책에 따라 정품 확인 후 비활성화할 수 있습니다.

26. Esc 키를 두 번 눌러 기본 콘솔 화면으로 돌아갑니다.
27. CIMC Macros > Static Macros > Alt-F 드롭다운 메뉴에서 Alt-F1 을 클릭합니다.
28. ESXi 호스트에 대한 올바른 자격 증명을 사용하여 로그인합니다.
29. 프롬프트에서 다음 esxcli 명령 목록을 순차적으로 입력하여 네트워크 연결을 활성화합니다.

```
esxcli network vswitch standard policy failover set -v vSwitch0 -a
vmnic2,vmnic4 -l iphash
```

ESXi 호스트를 구성합니다

다음 표의 정보를 사용하여 각 ESXi 호스트를 구성합니다.

세부 정보	상세 값
ESXi 호스트 이름입니다	ESXi_host_FQDN>>
ESXi 호스트 관리 IP입니다	ESXi_host_mgmt_ip>>
ESXi 호스트 관리 마스크입니다	ESXi_host_mgmt_netmask>>
ESXi 호스트 관리 게이트웨이	ESXi_host_mgmt_gateway>>
ESXi 호스트 NFS IP입니다	ESXi_host_nfs_ip>>
ESXi 호스트 NFS 마스크입니다	ESXi_host_nfs_netmask>>
ESXi 호스트 NFS 게이트웨이	ESXi_host_nfs_gateway>>
ESXi 호스트 vMotion IP입니다	ESXi_HOST_vMotion_IP>>
ESXi 호스트 vMotion 마스크	ESXi_host_vMotion_netmask>>
ESXi 호스트 vMotion 게이트웨이	ESXi_host_vMotion_gateway>>
ESXi 호스트 iSCSI - A IP	ESXi_host_iscsi-a_ip>>
ESXi 호스트 iSCSI - 마스크	ESXi_host_iscsi-a_netmask>>
ESXi 호스트 iSCSI - 게이트웨이	ESXi_host_iscsi-a_gateway>>
ESXi 호스트 iSCSI-B IP	ESXi_host_iscsi-B_ip>>
ESXi 호스트 iSCSI-B 마스크	ESXi_host_iscsi-B_netmask>>
ESXi 호스트 iSCSI-B 게이트웨이	ESXi_host_scsi-B_gateway>>

ESXi 호스트에 로그인합니다

ESXi 호스트에 로그인하려면 다음 단계를 수행하십시오.

1. 웹 브라우저에서 호스트의 관리 IP 주소를 엽니다.

2. 설치 프로세스 중에 지정한 암호 및 루트 계정을 사용하여 ESXi 호스트에 로그인합니다.
3. VMware 사용자 환경 개선 프로그램에 대한 설명을 읽어 보십시오. 적절한 응답을 선택한 후 OK(확인) 를 클릭합니다.

iSCSI 부트를 구성합니다

iSCSI 부트를 구성하려면 다음 단계를 수행하십시오.

1. 왼쪽에서 네트워킹 을 선택합니다.
2. 오른쪽에서 Virtual Switches 탭을 선택합니다.



3. iSciBootvSwitch 를 클릭합니다.
4. 설정 편집 을 선택합니다.
5. MTU를 9000으로 변경하고 저장 을 클릭합니다.
6. iSCSIBootPG 포트의 이름을 iSCSIBootPG-A로 바꿉니다

> 이 구성에서는 Vmnic3 및 vmnic5가 iSCSI 부팅에 사용됩니다. ESXi 호스트에 추가 NIC가 있는 경우 vmnic 번호가 다를 수 있습니다. iSCSI 부트에 사용되는 NIC를 확인하려면 CIMC의 iSCSI vNIC의 MAC 주소를 ESXi의 vmnics와 일치시킵니다.

7. 가운데 창에서 VMkernel NIC 탭을 선택합니다.
8. Add VMkernel NIC 를 선택합니다.
   a. iSciBootPG-B의 새 포트 그룹 이름을 지정합니다
   b. 가상 스위치에 대해 iSciBootvSwitch를 선택합니다.
   c. VLAN ID에 '<<iscsib_vlan_id>>'를 입력합니다.
   d. MTU를 9000으로 변경합니다.
   e. IPv4 설정 을 확장합니다.

f. 정적 설정을 선택합니다.

g. Address 에 "<<var_hosta_iscsib_ip>>"를 입력합니다.

h. 서브넷 마스크에 '<<var_hosta_iscsib_mask>>'를 입력합니다.

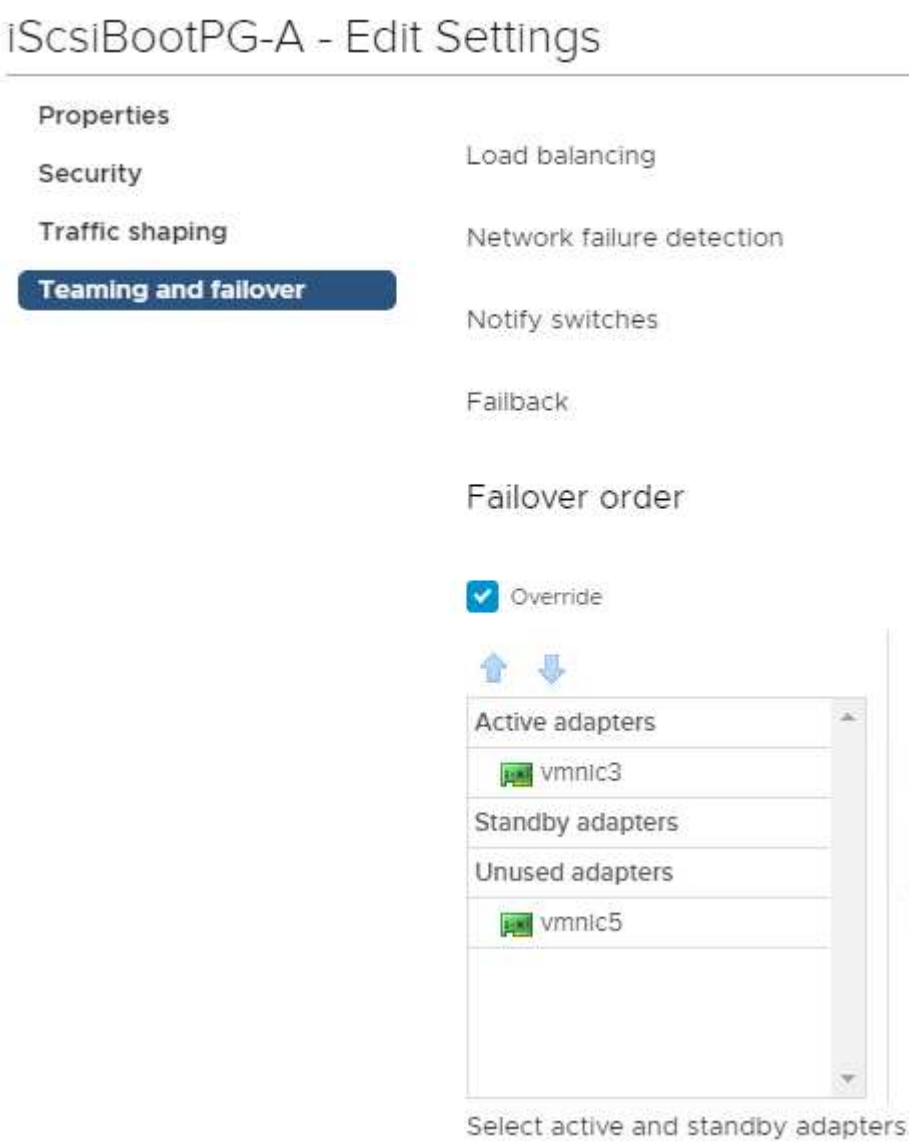
i. 생성 을 클릭합니다.

iSciBootPG-A에서 MTU를 9000으로 설정합니다

9. 페일오버를 설정하려면 다음 단계를 수행하십시오.

a. iSCSIBootPG-A > 계층화 및 페일오버 > 페일오버 순서 > Vmnic3에서 설정 편집 을 클릭합니다. Vmnic3이 활성 상태이고 vmnic5가 사용되지 않아야 합니다.

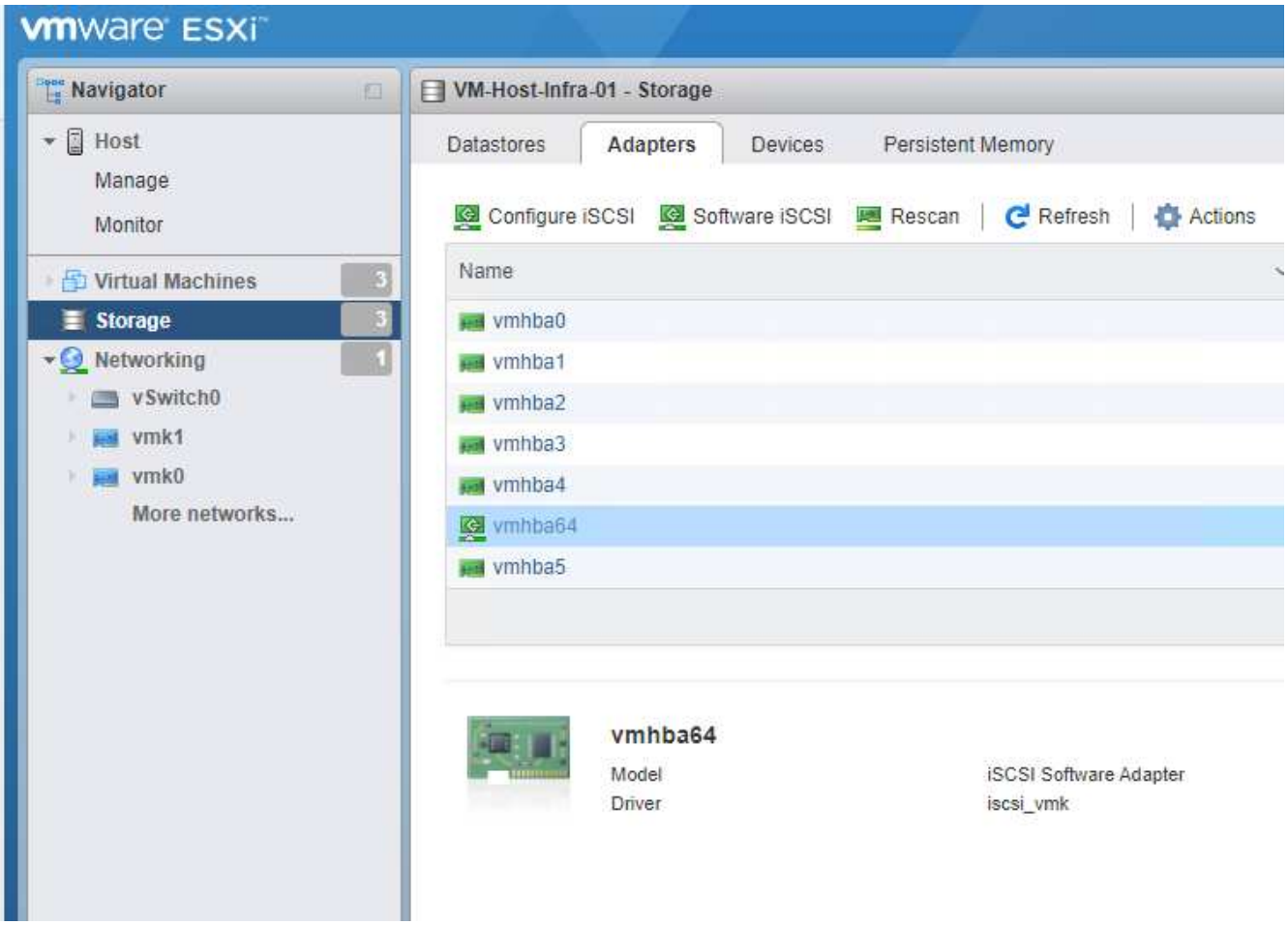
b. iSCSIBootPG-B > 팀 구성 및 장애 조치 > 장애 조치 순서 > Vmnic5에서 설정 편집 을 클릭합니다. Vmnic5는 활성 상태이고 vmnic3는 사용하지 않아야 합니다.



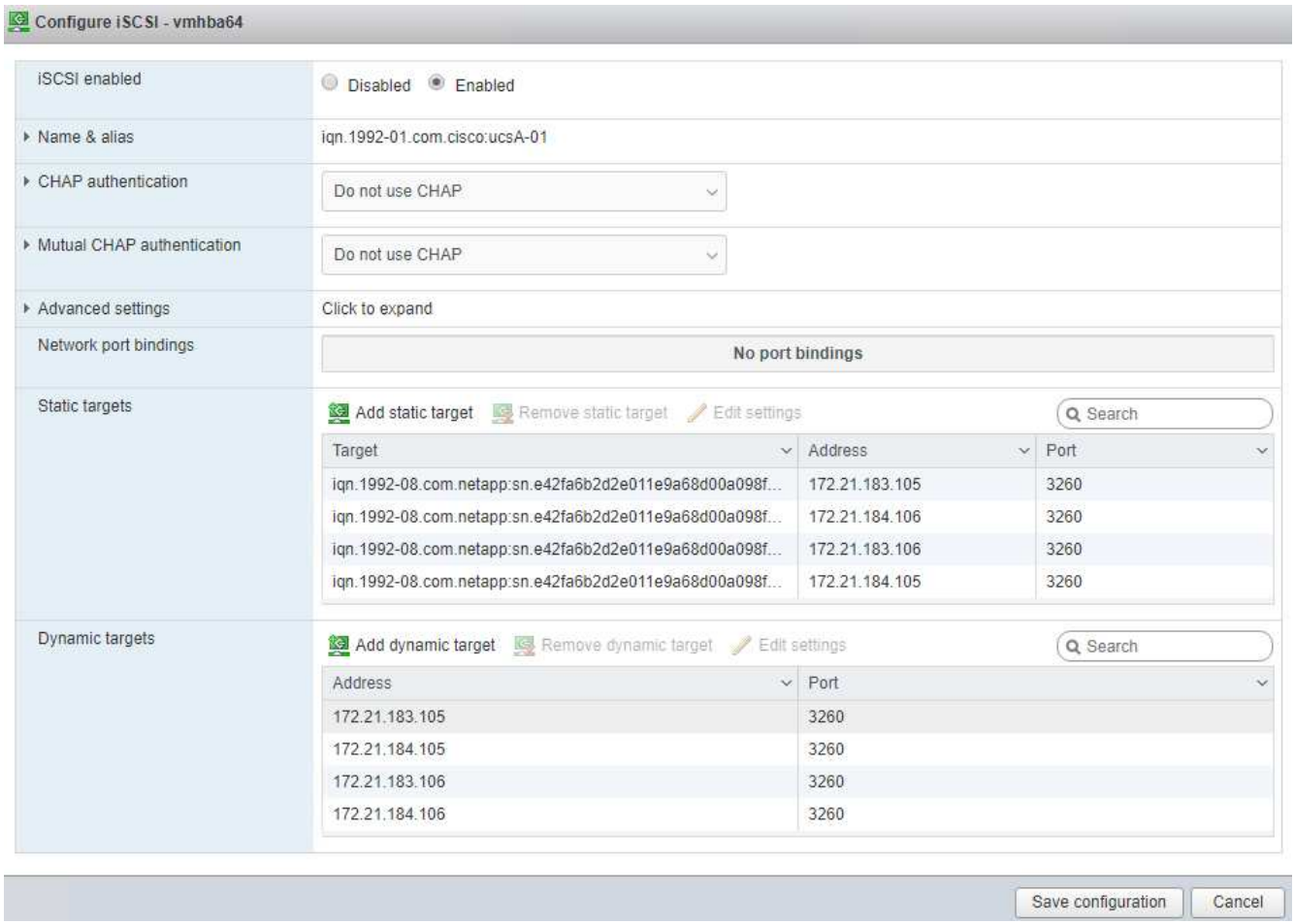
iSCSI 다중 경로를 구성합니다

ESXi 호스트에 iSCSI 다중 경로를 설정하려면 다음 단계를 수행하십시오.

1. 왼쪽 탐색 창에서 스토리지 를 선택합니다. 어댑터를 클릭합니다.
2. iSCSI 소프트웨어 어댑터를 선택하고 iSCSI 구성 을 클릭합니다.



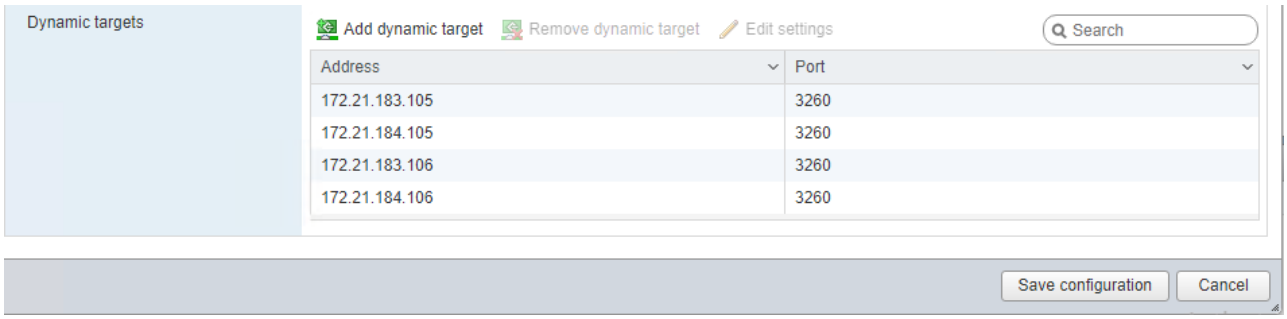
3. 동적 대상에서 동적 대상 추가를 클릭합니다.



4. IP 주소 'iscsi_lif01a'를 입력합니다.

   a. IP 주소 iscsi_liff 01b, iscsi_liff 02a, iscsi_liff 02b와 함께 이 과정을 반복합니다.

   b. 구성 저장 을 클릭합니다.



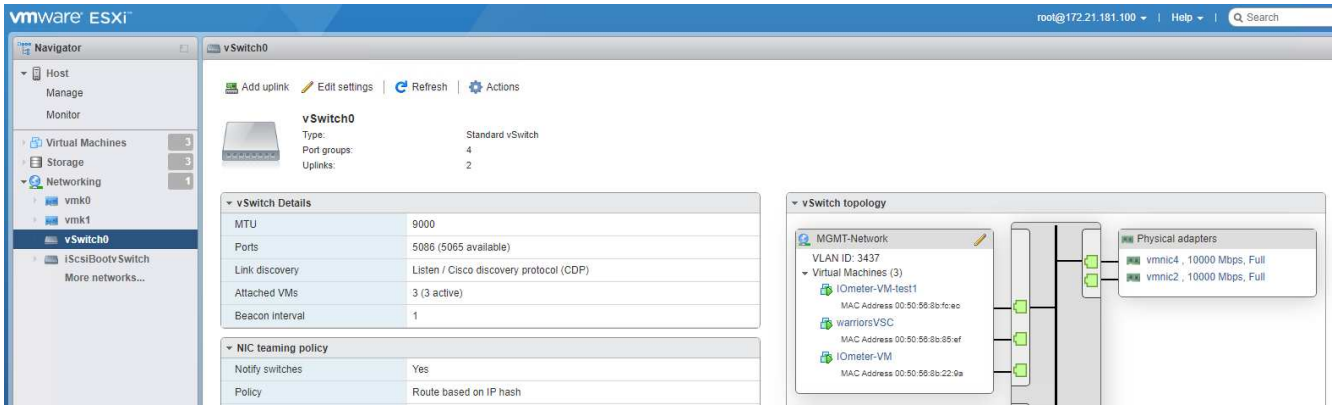
NetApp 클러스터에서 network interface show 명령을 실행하거나 System Manager의 네트워크 인터페이스 탭을 확인하여 iSCSI LIF IP 주소를 찾을 수 있습니다.

ESXi 호스트를 구성합니다

ESXi 부트를 구성하려면 다음 단계를 수행하십시오.

1. 왼쪽 탐색 창에서 네트워킹 을 선택합니다.

2. vSwitch0을 선택합니다.



3. 설정 편집 을 선택합니다.
4. MTU를 9000으로 변경합니다.
5. NIC 티밍을 확장하고 vmnic2 및 vmnic4가 활성으로 설정되어 있고 NIC 티밍과 장애 조치가 IP 해시를 기준으로 라우팅으로 설정되어 있는지 확인합니다.

> 로드 밸런싱의 IP 해시 방법을 사용하려면 기본 물리적 스위치를 정적(모드 온) 포트 채널과 함께 SRC-DST-IP EtherChannel을 사용하여 올바르게 구성해야 합니다. 스위치 구성 오류로 인해 연결이 간헐적으로 끊길 수 있습니다. 이 경우 포트 채널 설정 문제를 해결하는 동안 Cisco 스위치에서 연결된 두 개의 업링크 포트 중 하나를 일시적으로 종료하여 ESXi 관리 vmkernel 포트로의 통신을 복구합니다.

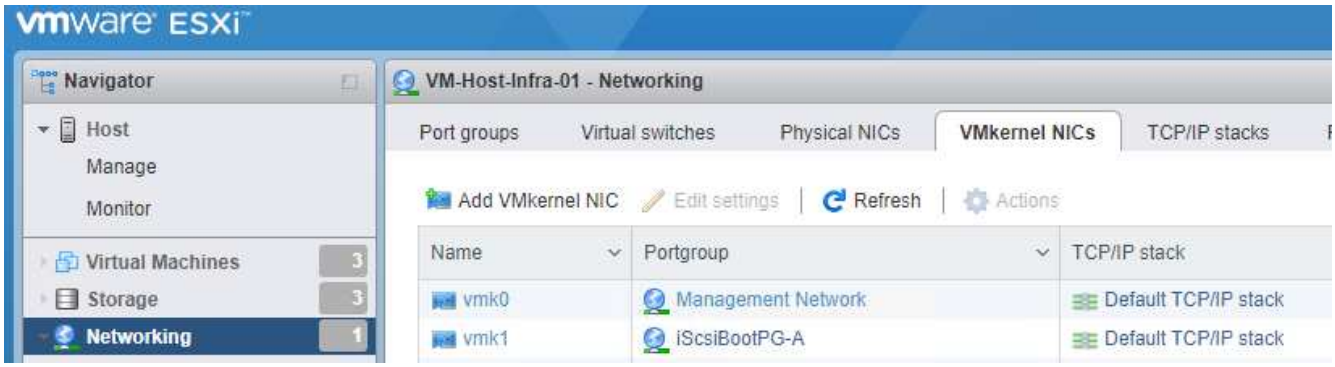
포트 그룹과 **VMkernel NIC**를 구성합니다

포트 그룹과 VMkernel NIC를 구성하려면 다음 단계를 완료합니다.

1. 왼쪽 탐색 창에서 네트워킹 을 선택합니다.
2. 포트 그룹 탭을 마우스 오른쪽 단추로 클릭합니다.



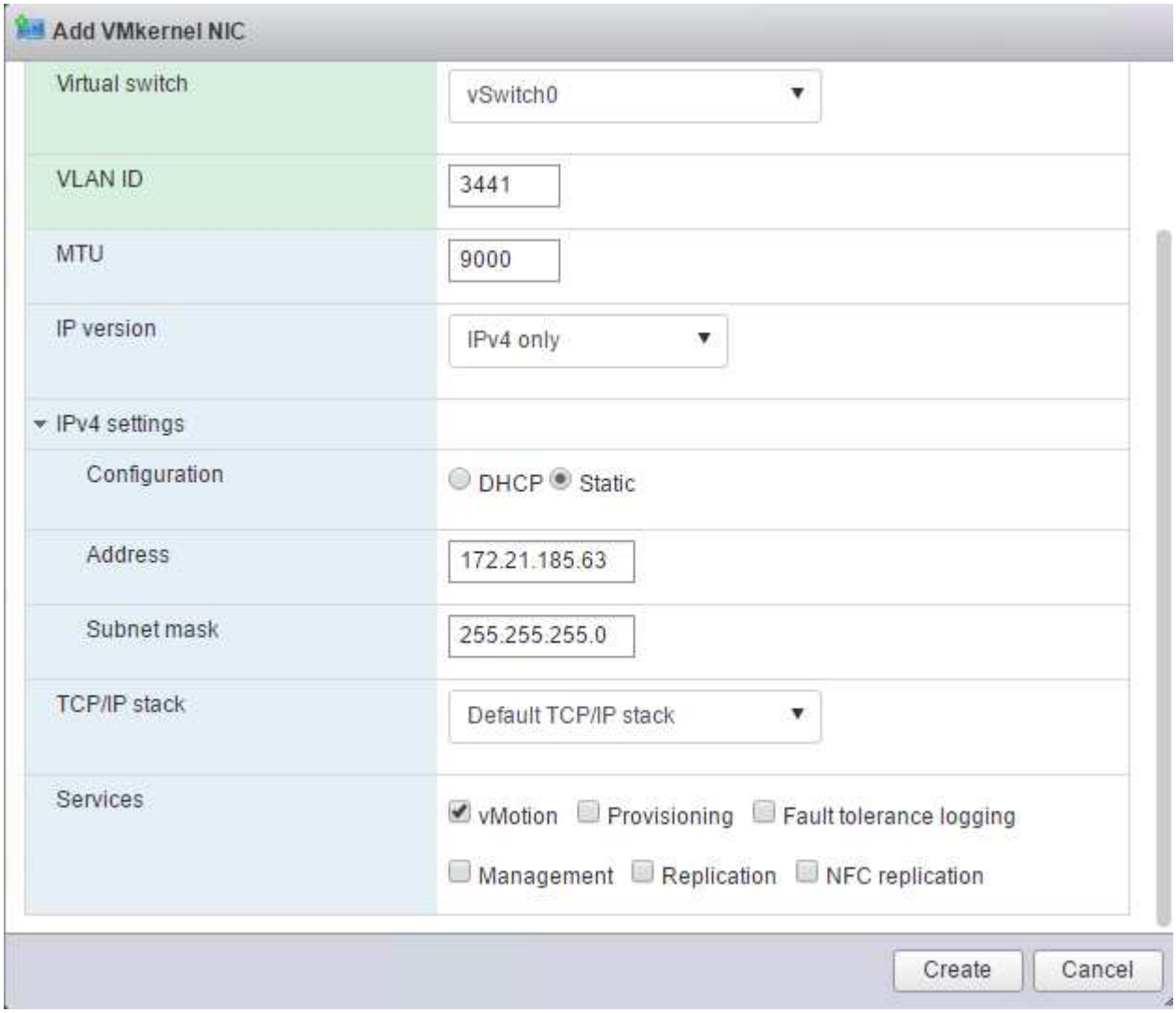
3. VM Network를 마우스 오른쪽 버튼으로 클릭하고 Edit를 선택합니다. VLAN ID를 '<<var_vm_traffic_vlan>>'로 변경합니다.
4. 포트 그룹 추가 를 클릭합니다.
    a. 포트 그룹의 이름을 MGMT-Network로 지정합니다.
    b. VLAN ID에 '<<mgmt_vlan>>'를 입력합니다.
    c. vSwitch0이 선택되어 있는지 확인합니다.
    d. 저장 을 클릭합니다.
5. VMkernel NIC 탭을 클릭합니다.



6. Add VMkernel NIC 를 선택합니다.
    a. 새 포트 그룹을 선택합니다.
    b. 포트 그룹의 이름을 NFS-Network로 지정합니다.
    c. VLAN ID에 '<<nfs_vlan_id>>'를 입력합니다.
    d. MTU를 9000으로 변경합니다.
    e. IPv4 설정 을 확장합니다.
    f. 정적 설정을 선택합니다.
    g. Address 에 "<<var_hosta_nfs_ip>>"를 입력합니다.
    h. 서브넷 마스크에 '<<var_hosta_nfs_mask>>'를 입력합니다.
    i. 생성 을 클릭합니다.
7. 이 프로세스를 반복하여 vMotion VMkernel 포트를 생성합니다.
8. Add VMkernel NIC 를 선택합니다.
    a. 새 포트 그룹을 선택합니다.
    b. 포트 그룹의 이름을 vMotion으로 지정합니다.
    c. VLAN ID에 '\< vMotion_vlan_id>>'를 입력합니다.
    d. MTU를 9000으로 변경합니다.
    e. IPv4 설정 을 확장합니다.
    f. 정적 설정을 선택합니다.
    g. Address 에 "<<var_hosta_vmotion_ip>>"를 입력합니다.

h. 서브넷 마스크에 '<<var_hosta_vmotion_mask>>'를 입력합니다.

i. IPv4 설정 후 vMotion 확인란이 선택되어 있는지 확인합니다.

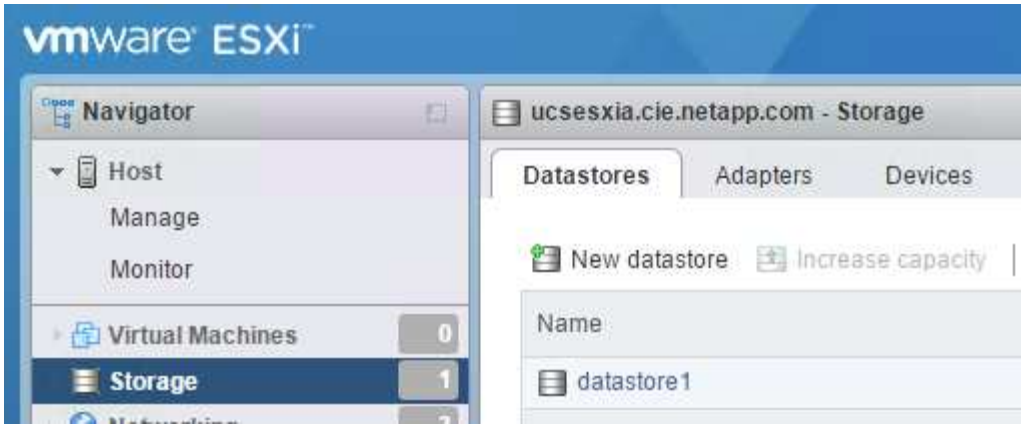


라이센싱에서 허용하는 경우 VMware vSphere 분산 스위치를 사용하는 등 여러 가지 방법으로 ESXi 네트워킹을 구성할 수 있습니다. 비즈니스 요구 사항을 충족하는 데 필요한 경우 FlexPod Express에서 대체 네트워크 구성이 지원됩니다.

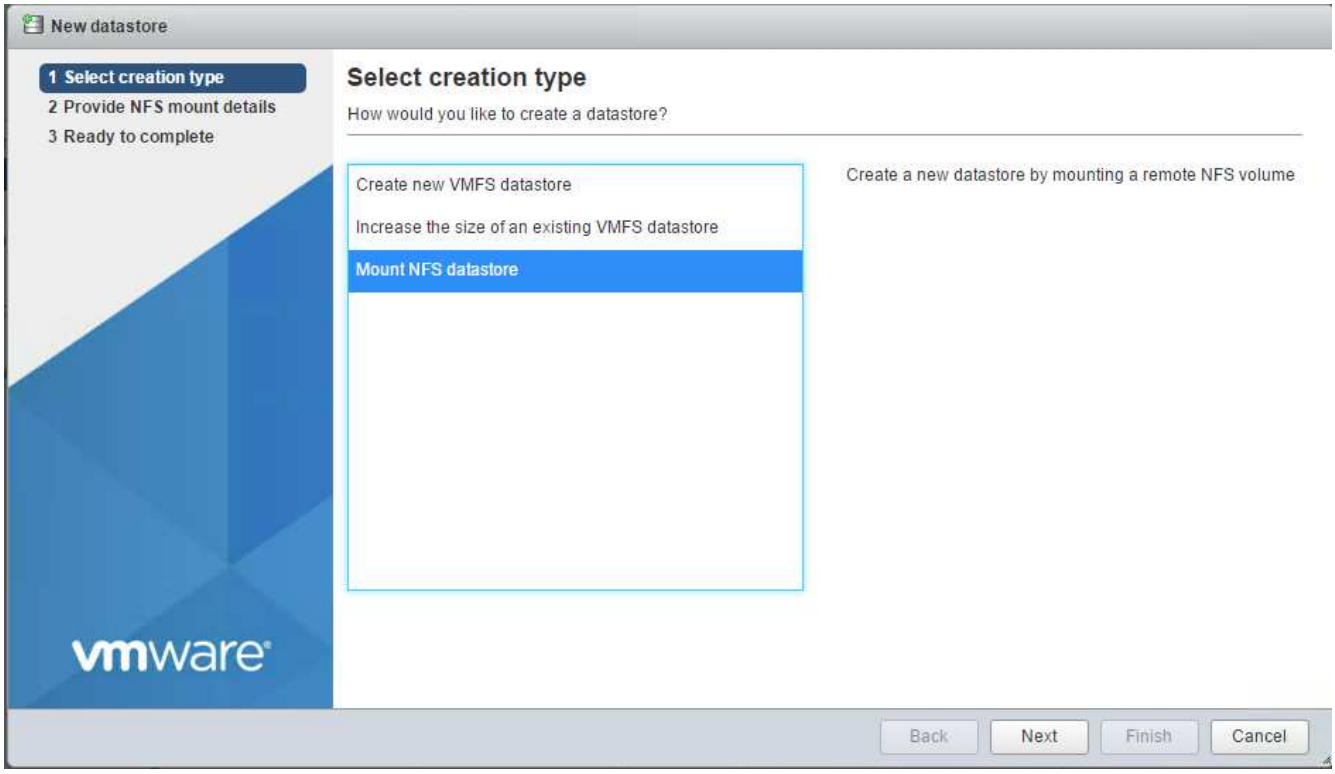
첫 번째 데이터 저장소를 마운트합니다

첫 번째로 마운트할 데이터스토어는 VM용 infra_datastore 데이터 저장소와 VM 스왑 파일을 위한 infra_swap 데이터 저장소입니다.

1. 왼쪽 탐색 창에서 스토리지 를 클릭한 다음 새 데이터 저장소 를 클릭합니다.



2. Mount NFS Datastore를 선택합니다.



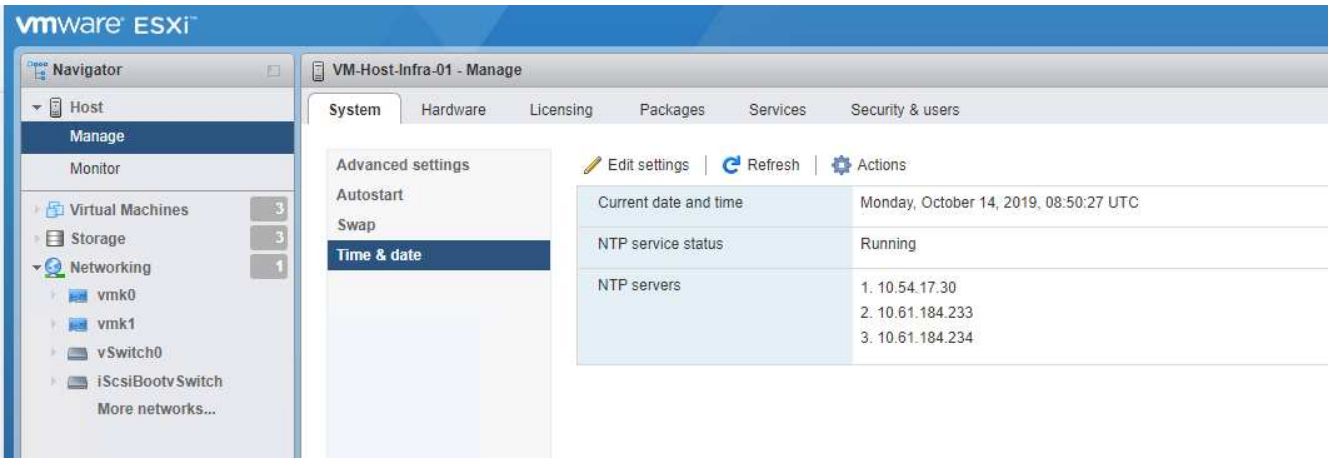
3. NFS 마운트 세부 정보 제공 페이지에 다음 정보를 입력합니다.
   - 이름: 'infra_datastore'
   - NFS 서버:\<<var_NodeA_nfs_lif>'
   - 공유: '/infra_datastore'
   - NFS 3이 선택되어 있는지 확인합니다.
4. 마침 을 클릭합니다. 최근 작업 창에서 작업이 완료된 것을 볼 수 있습니다.
5. 이 프로세스를 반복하여 'infra_swap' 데이터 저장소를 마운트합니다.
   - 이름: infra_swap
   - NFS 서버:\<<var_NodeA_nfs_lif>'
   - 공유: '/infra_swap'

◦ NFS 3이 선택되어 있는지 확인합니다.

NTP를 구성합니다

ESXi 호스트에 대해 NTP를 구성하려면 다음 단계를 수행하십시오.

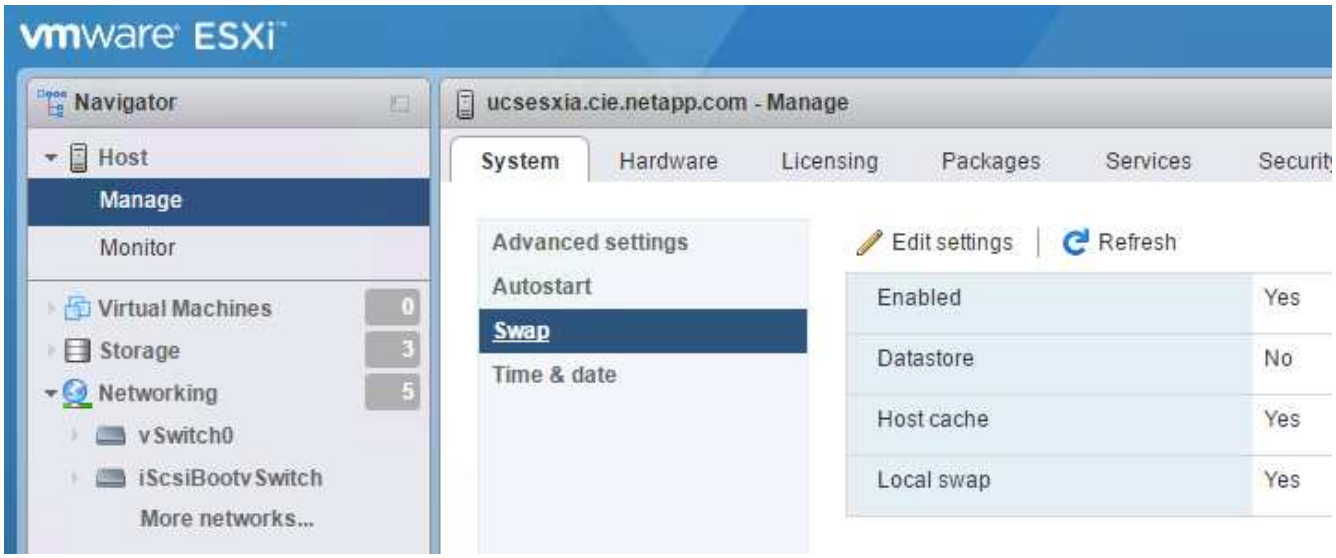
1. 왼쪽 탐색 창에서 관리 를 클릭합니다. 오른쪽 창에서 시스템 을 선택한 다음 시간 및 날짜 를 클릭합니다.
2. Use Network Time Protocol (Enable NTP Client) 을 선택합니다.
3. Start and Stop with Host 를 NTP 서비스 시작 정책으로 선택합니다.
4. NTP 서버로 '<<var_ntp>>'를 입력합니다. 여러 NTP 서버를 설정할 수 있습니다.
5. 저장 을 클릭합니다.



VM 스왑 파일 위치를 이동합니다

다음 단계에서는 VM 스왑 파일 위치를 이동하는 방법을 자세히 설명합니다.

1. 왼쪽 탐색 창에서 관리 를 클릭합니다. 오른쪽 창에서 시스템을 선택한 다음 바꾸기를 클릭합니다.



2. 설정 편집 을 클릭합니다. Datastore 옵션에서 infra_swap을 선택합니다.



3. 저장 을 클릭합니다.

"다음: VMware vCenter Server 6.7U2 설치 절차"

VMware vCenter Server 6.7U2 설치 절차

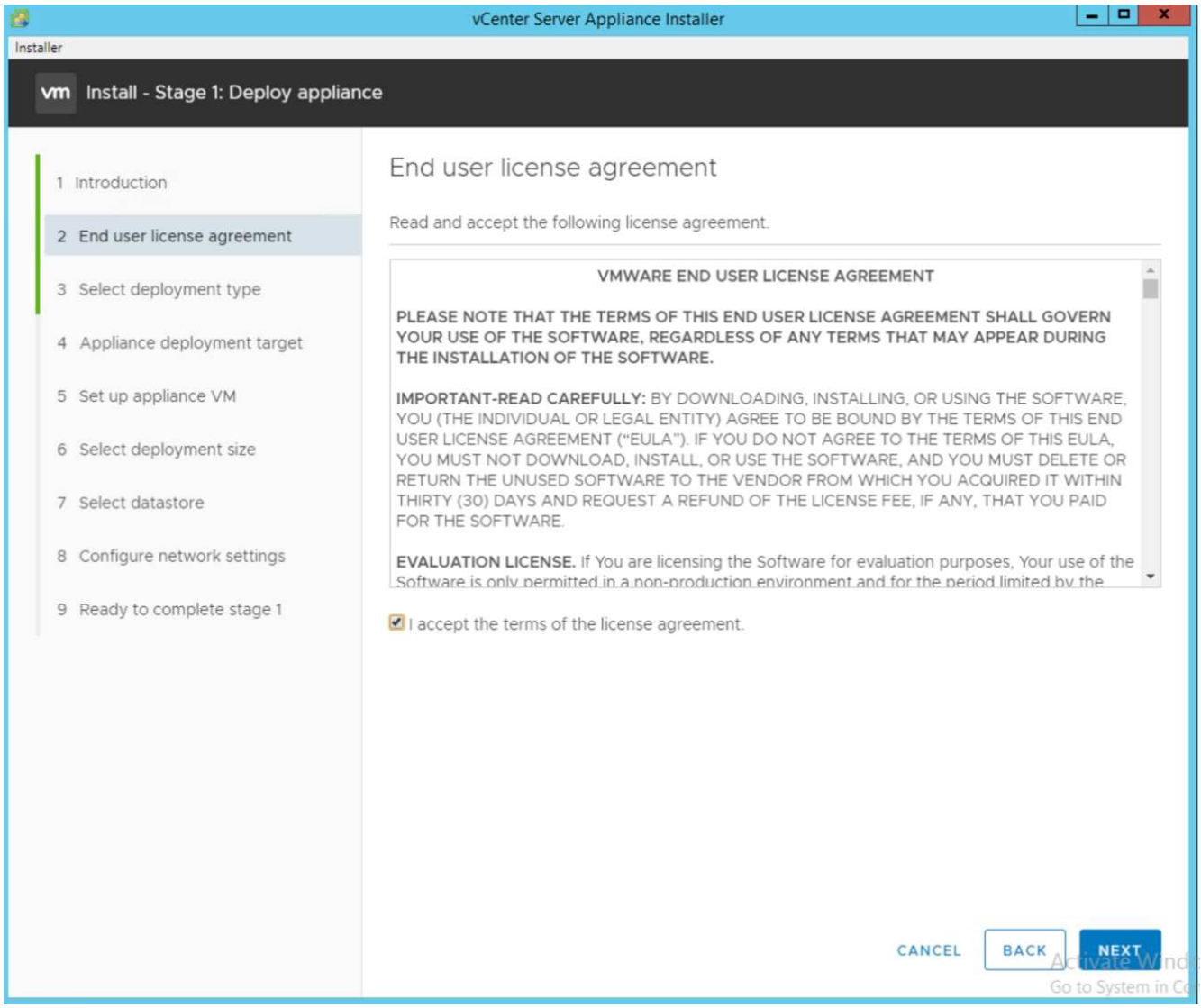
이 섹션에서는 FlexPod Express 구성에 VMware vCenter Server 6.7을 설치하는 절차를 자세히 설명합니다.

FlexPod Express는 VCSA(VMware vCenter Server Appliance)를 사용합니다.

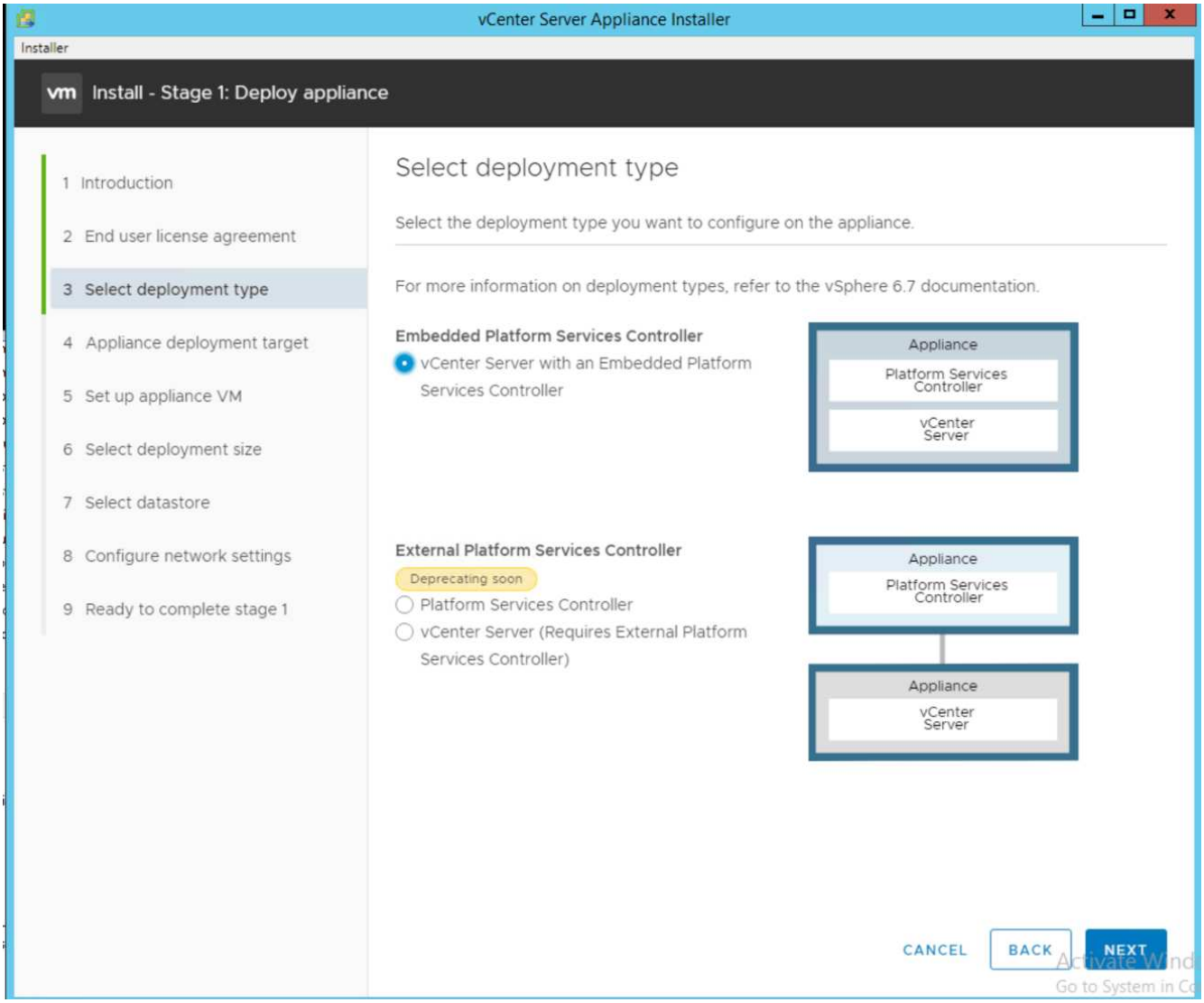
VMware vCenter Server Appliance를 다운로드합니다

VMware vCenter Server Appliance(VCSA)를 다운로드하려면 다음 단계를 수행하십시오.

1. VCSA를 다운로드합니다. ESXi 호스트를 관리할 때 vCenter Server 가져오기 아이콘을 클릭하여 다운로드 링크를 액세스합니다.
2. VMware 사이트에서 VCSA를 다운로드합니다.
3. Microsoft Windows vCenter Server 설치 가능한 가 지원되지만 VMware는 새로운 구축에 VCSA를 권장합니다.
4. ISO 이미지를 마운트합니다.
5. vcsa-UI-installer> Win32 디렉터리로 이동합니다. installer.exe를 두 번 클릭합니다.
6. 설치 를 클릭합니다.
7. 소개 페이지에서 다음 을 클릭합니다.

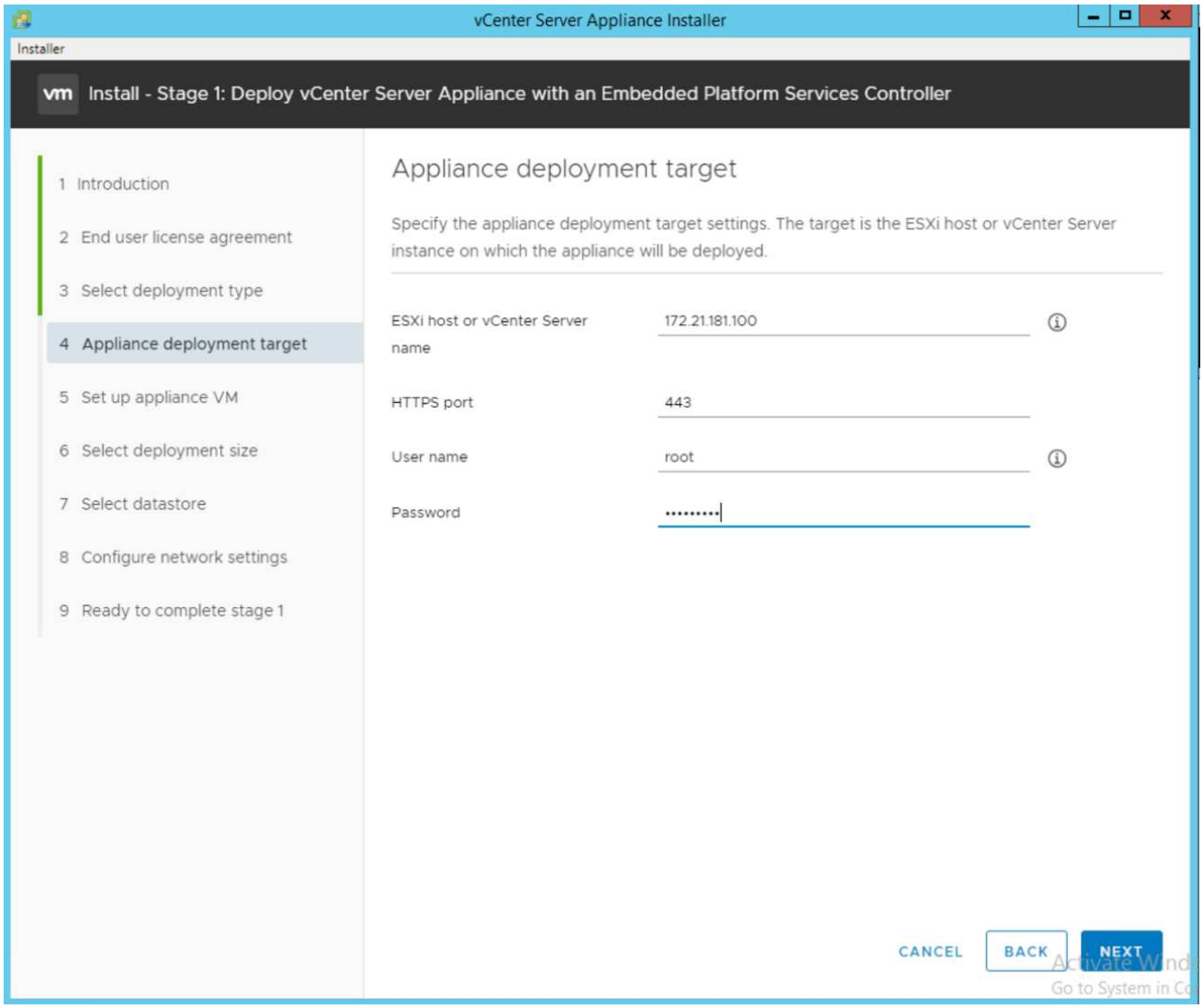


8. 배포 유형으로 임베디드 플랫폼 서비스 컨트롤러 를 선택합니다.

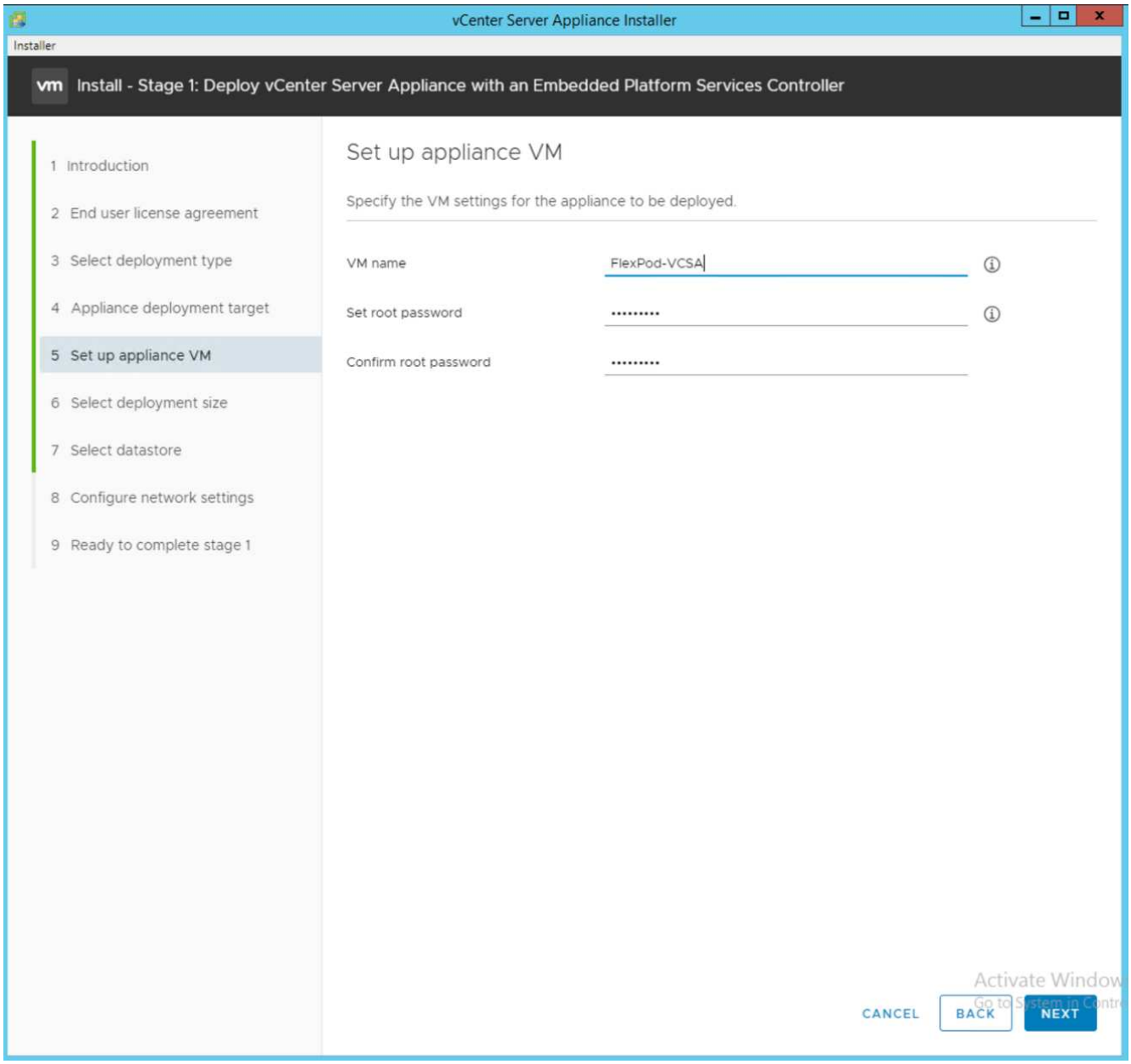


필요한 경우 외부 플랫폼 서비스 컨트롤러 배포도 FlexPod Express 솔루션의 일부로 지원됩니다.

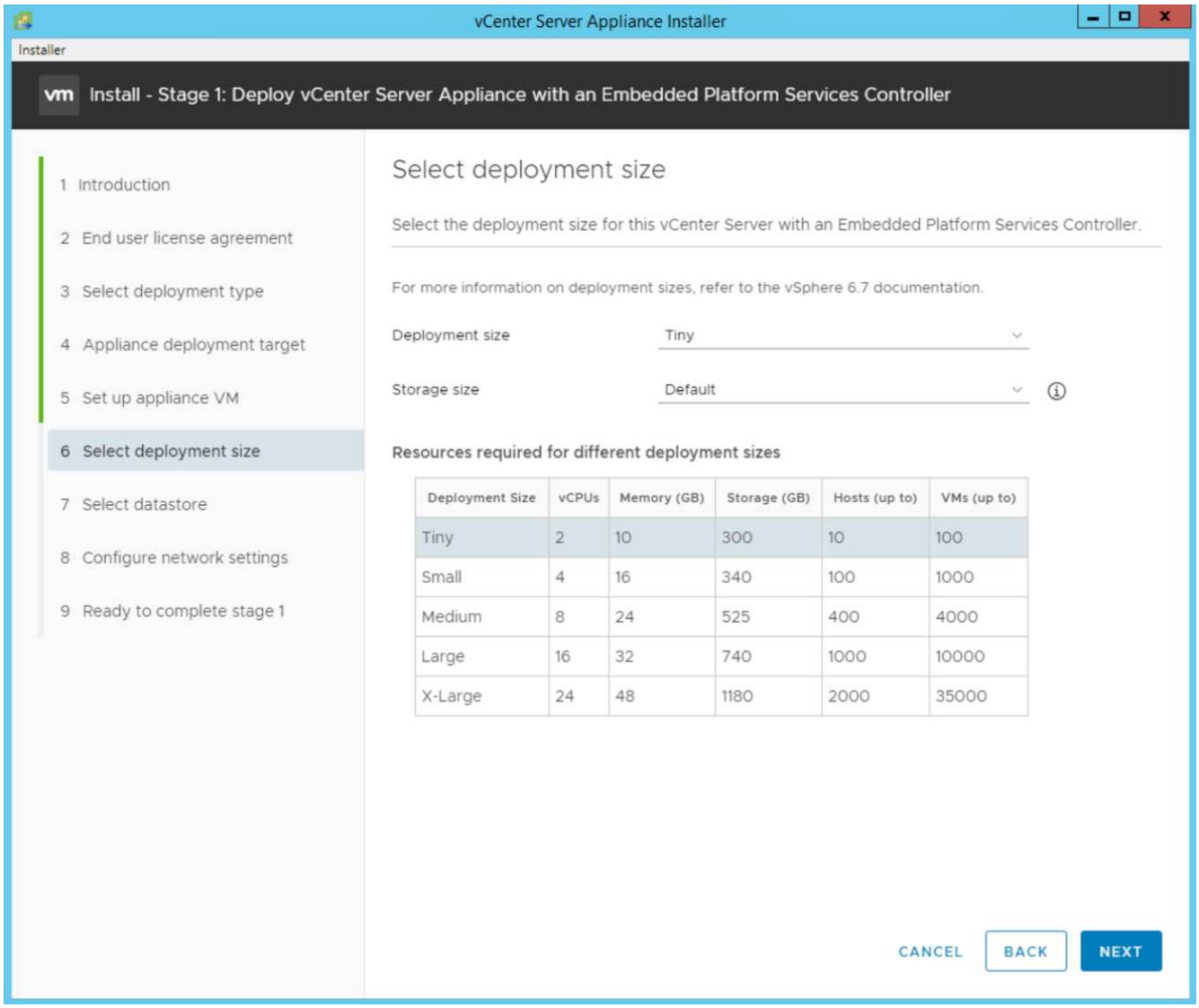
9. 어플라이언스 배포 대상에서 배포한 ESXi 호스트의 IP 주소, 루트 사용자 이름 및 루트 암호를 입력합니다.



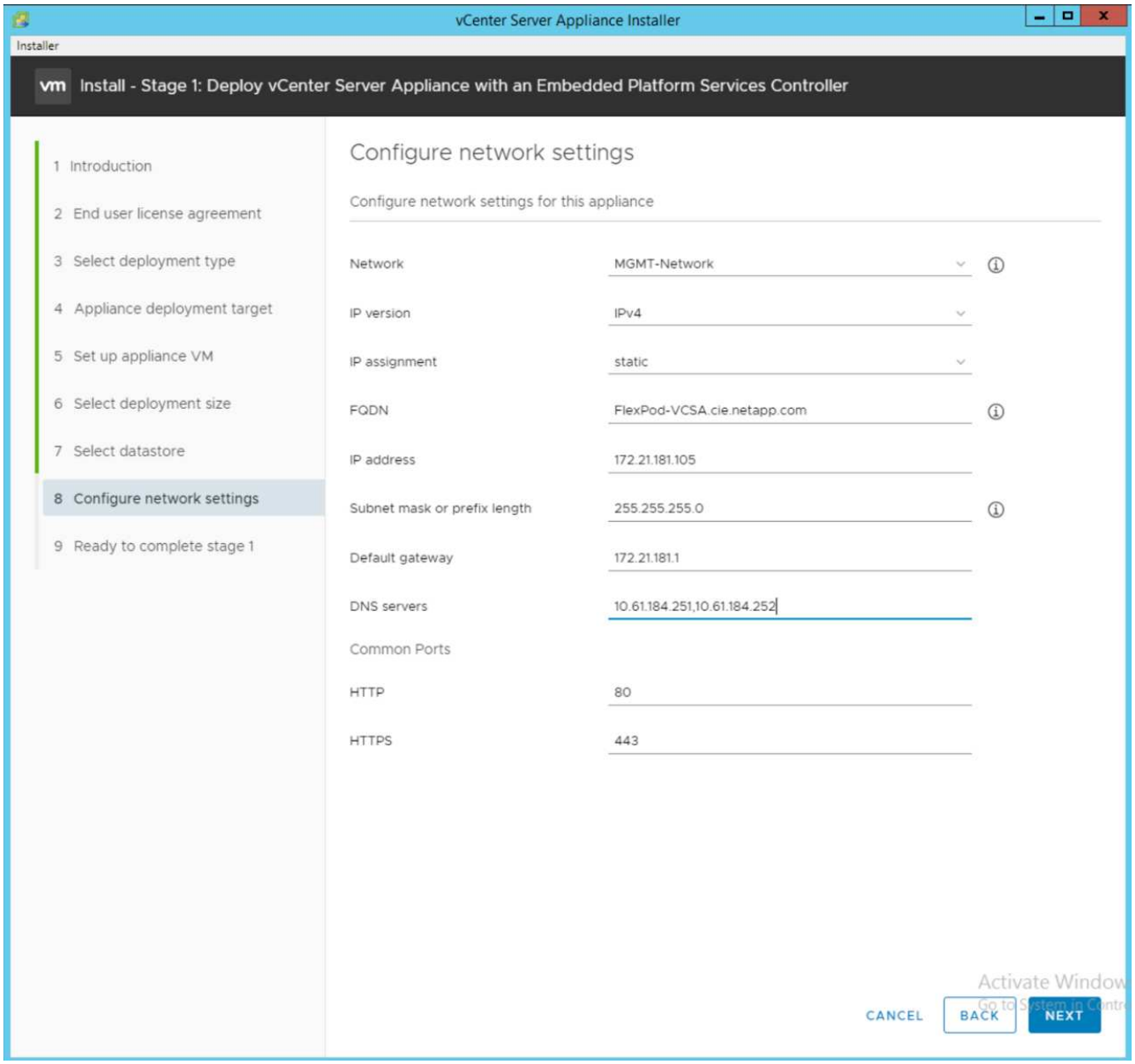
10. VCSA를 VCSA에 사용할 VM 이름 및 루트 암호로 입력하여 어플라이언스 VM을 설정합니다.



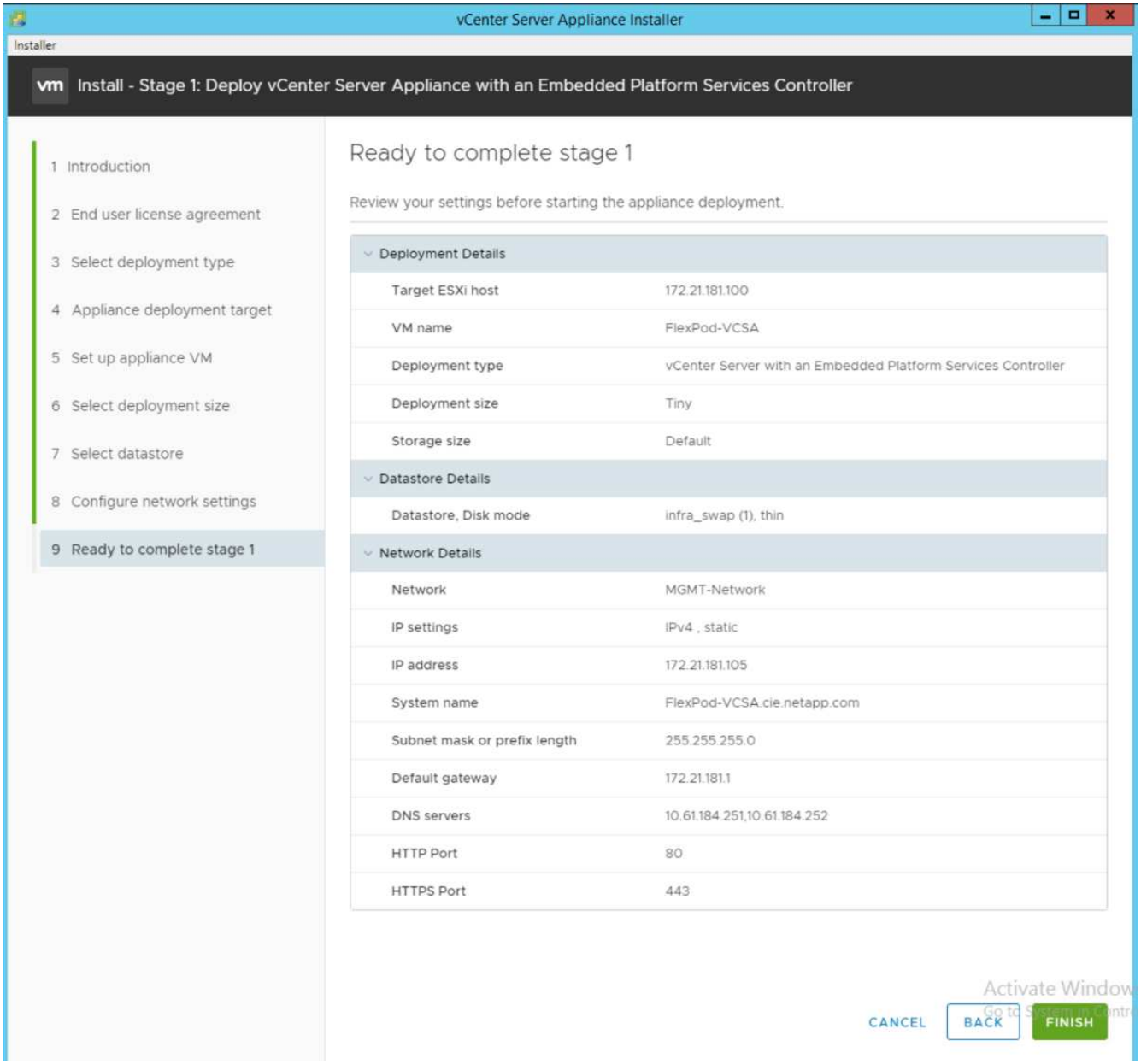
11. 환경에 가장 적합한 구축 크기를 선택합니다. 다음 을 클릭합니다.



12. 'infra_datastore' 데이터 저장소를 선택합니다. 다음 을 클릭합니다.
13. 네트워크 설정 구성 페이지에 다음 정보를 입력하고 다음 을 클릭합니다.
    a. Network 에서 MGMT-Network 를 선택합니다.
    b. VCSA에 사용할 FQDN 또는 IP를 입력합니다.
    c. 사용할 IP 주소를 입력합니다.
    d. 사용할 서브넷 마스크를 입력합니다.
    e. 기본 게이트웨이를 입력합니다.
    f. DNS 서버를 입력합니다.
14. 1단계 완료 준비 페이지에서 입력한 설정이 올바른지 확인합니다. 마침 을 클릭합니다.

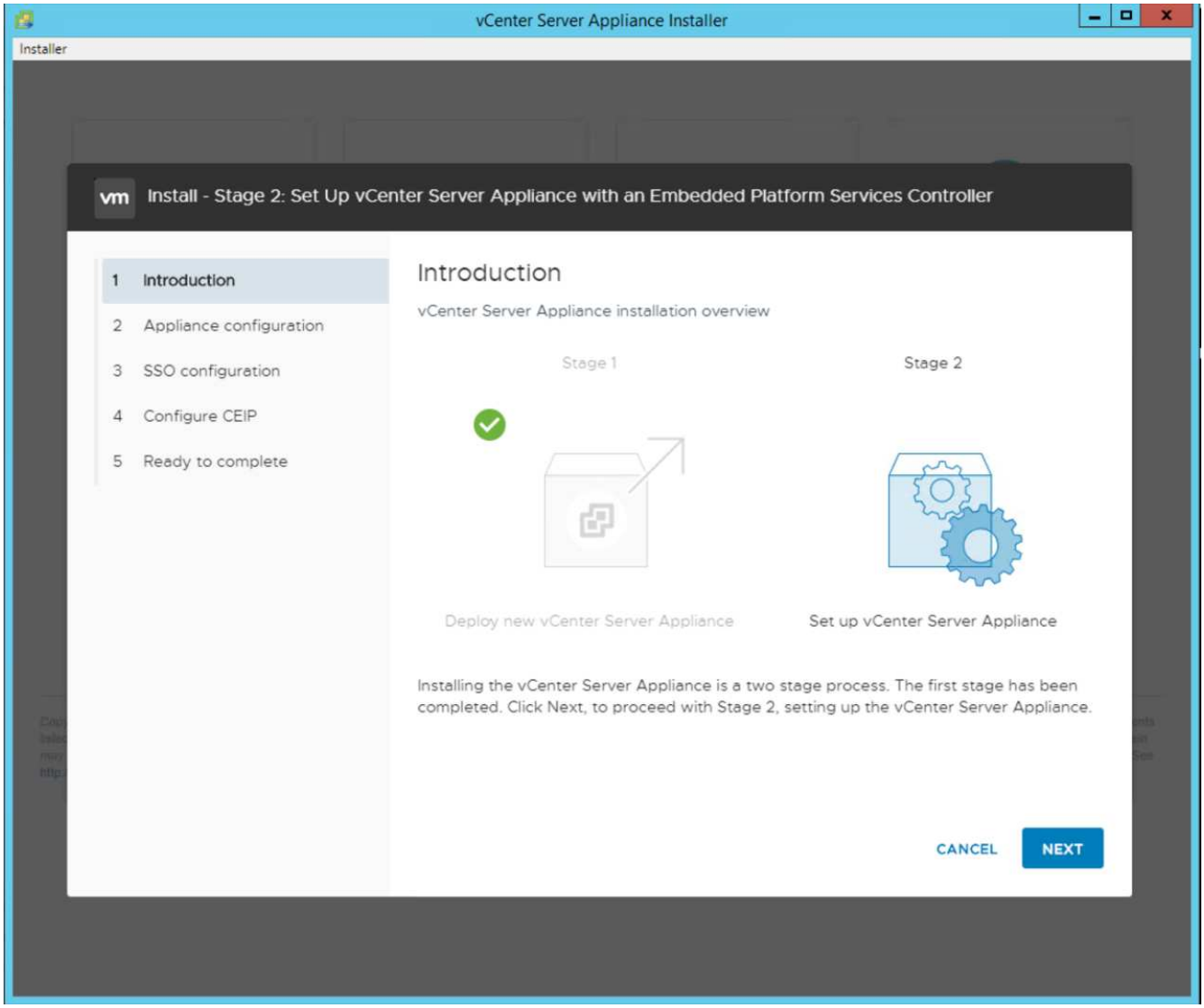


15. 어플라이언스 배포를 시작하기 전에 1단계의 설정을 검토하십시오.

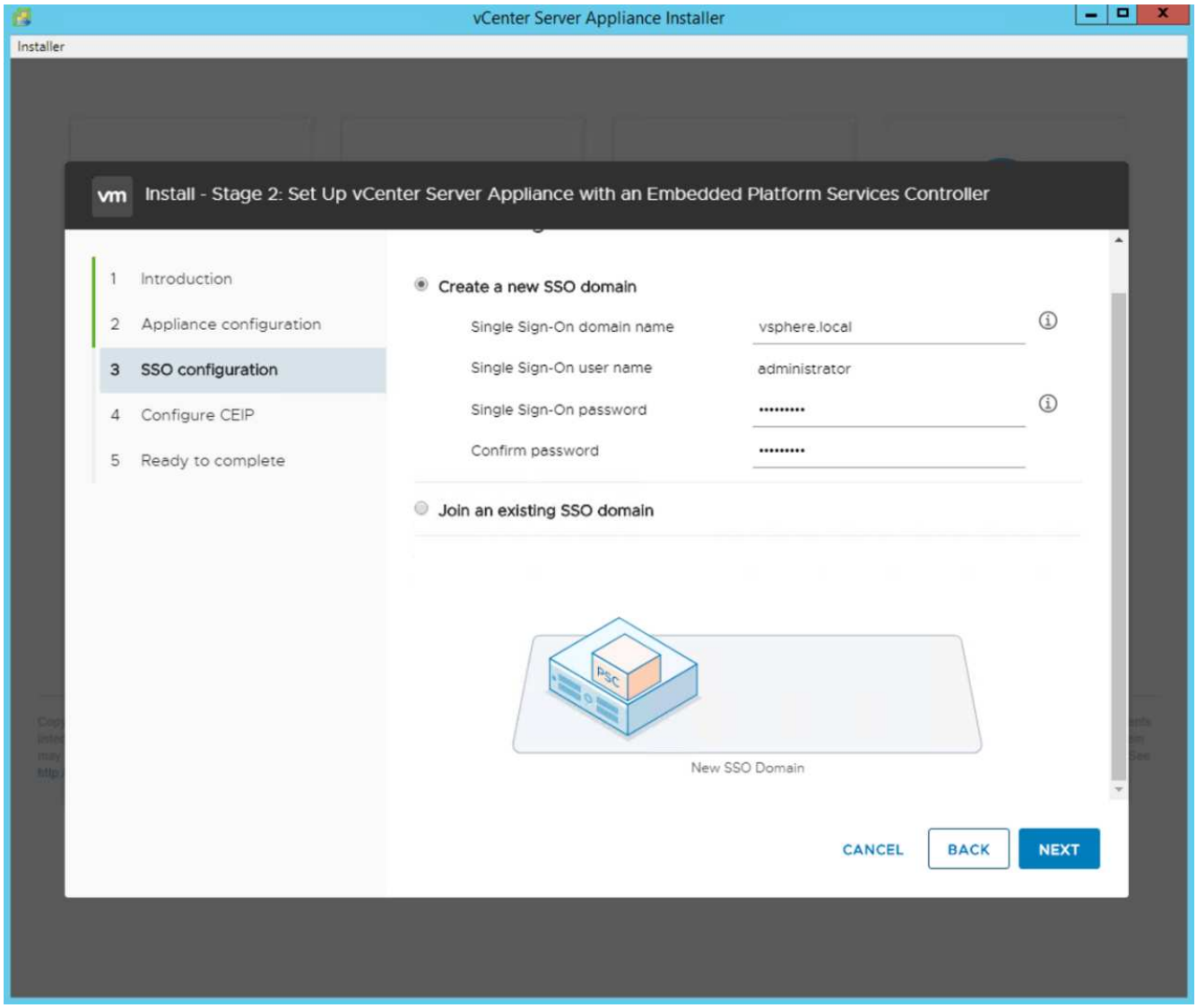


VCSA가 지금 설치됩니다. 이 과정은 몇 분 정도 소요됩니다.

16. 1단계가 완료되면 완료되었다는 메시지가 나타납니다. 계속 을 클릭하여 2단계 구성을 시작합니다.
17. 2단계 소개 페이지에서 다음 을 클릭합니다.

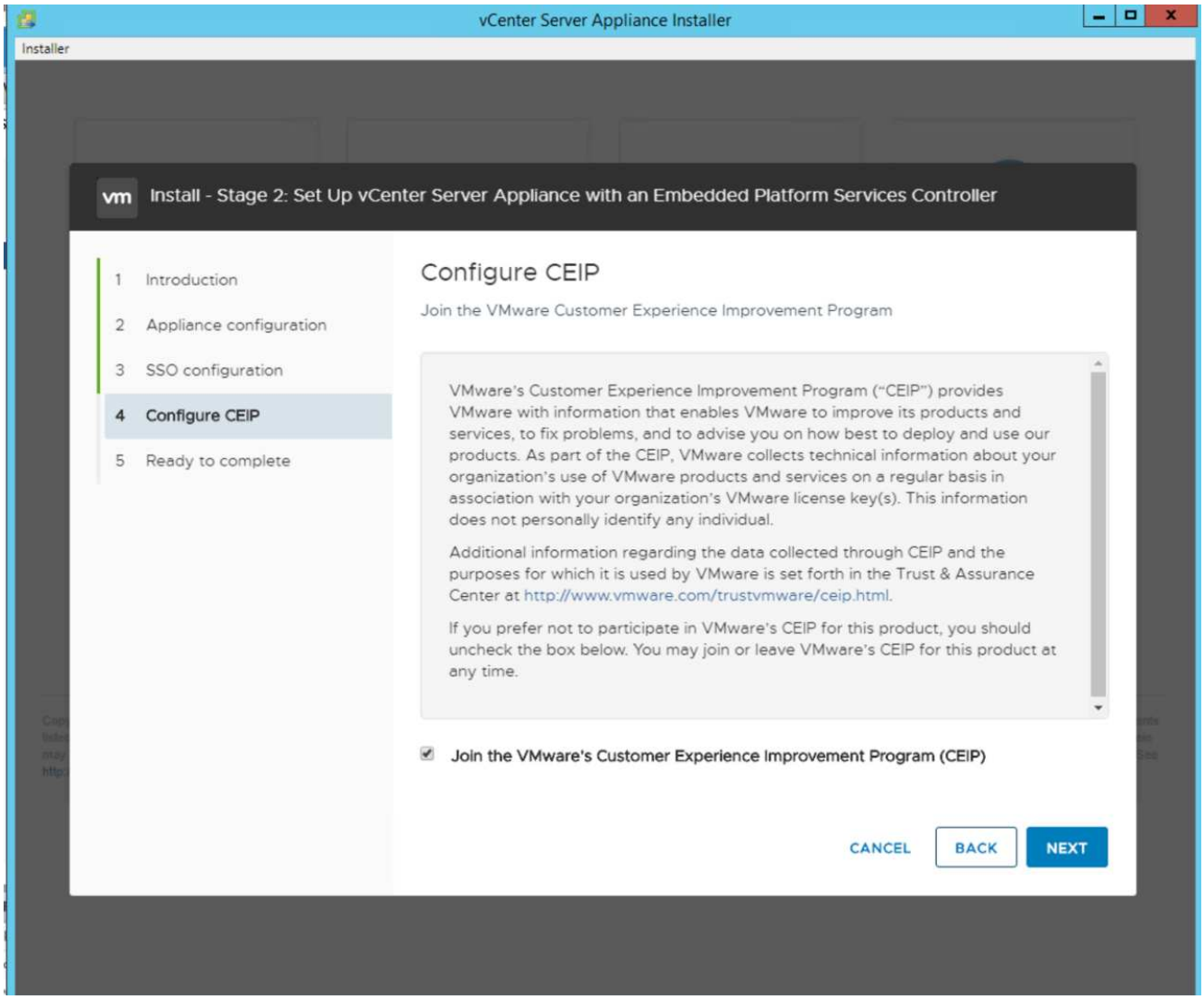


18. NTP 서버 주소에 대해 '<<var_ntp_id>>'를 입력합니다. 여러 NTP IP 주소를 입력할 수 있습니다.
19. vCenter Server HA(고가용성)를 사용하려는 경우 SSH 액세스가 설정되어 있는지 확인합니다.
20. SSO 도메인 이름, 암호 및 사이트 이름을 구성합니다. 다음 을 클릭합니다.

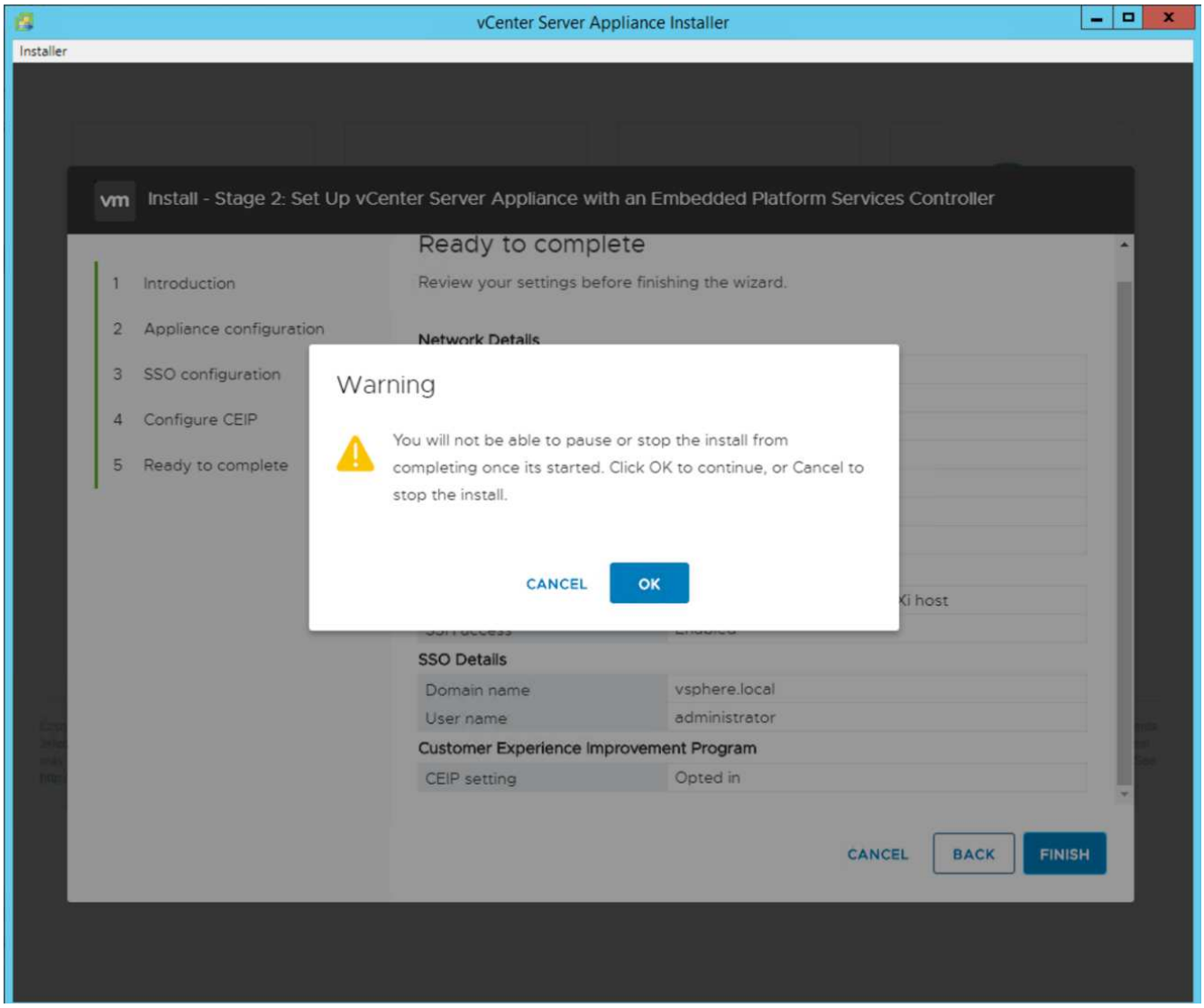


특히 "vsphere.local" 도메인 이름을 벗어나는 경우 이러한 값을 참조로 기록합니다.

21. 원하는 경우 VMware 고객 경험 프로그램에 참여하십시오. 다음 을 클릭합니다.



22. 설정 요약을 봅니다. 마침 을 클릭하거나 뒤로 단추를 사용하여 설정을 편집합니다.
23. 설치가 시작된 후 설치를 일시 중지하거나 중지할 수 없다는 메시지가 나타납니다. 계속하려면 확인을 클릭하십시오.



어플라이언스 설정이 계속됩니다. 이 작업은 몇 분 정도 걸립니다.

설정이 성공했음을 나타내는 메시지가 나타납니다.

24. vCenter Server에 액세스하기 위해 설치 관리자가 제공하는 링크를 클릭할 수 있습니다.

"다음: VMware vCenter Server 6.7U2 및 vSphere 클러스터링 구성"

VMware vCenter Server 6.7U2 및 **vSphere** 클러스터링 구성

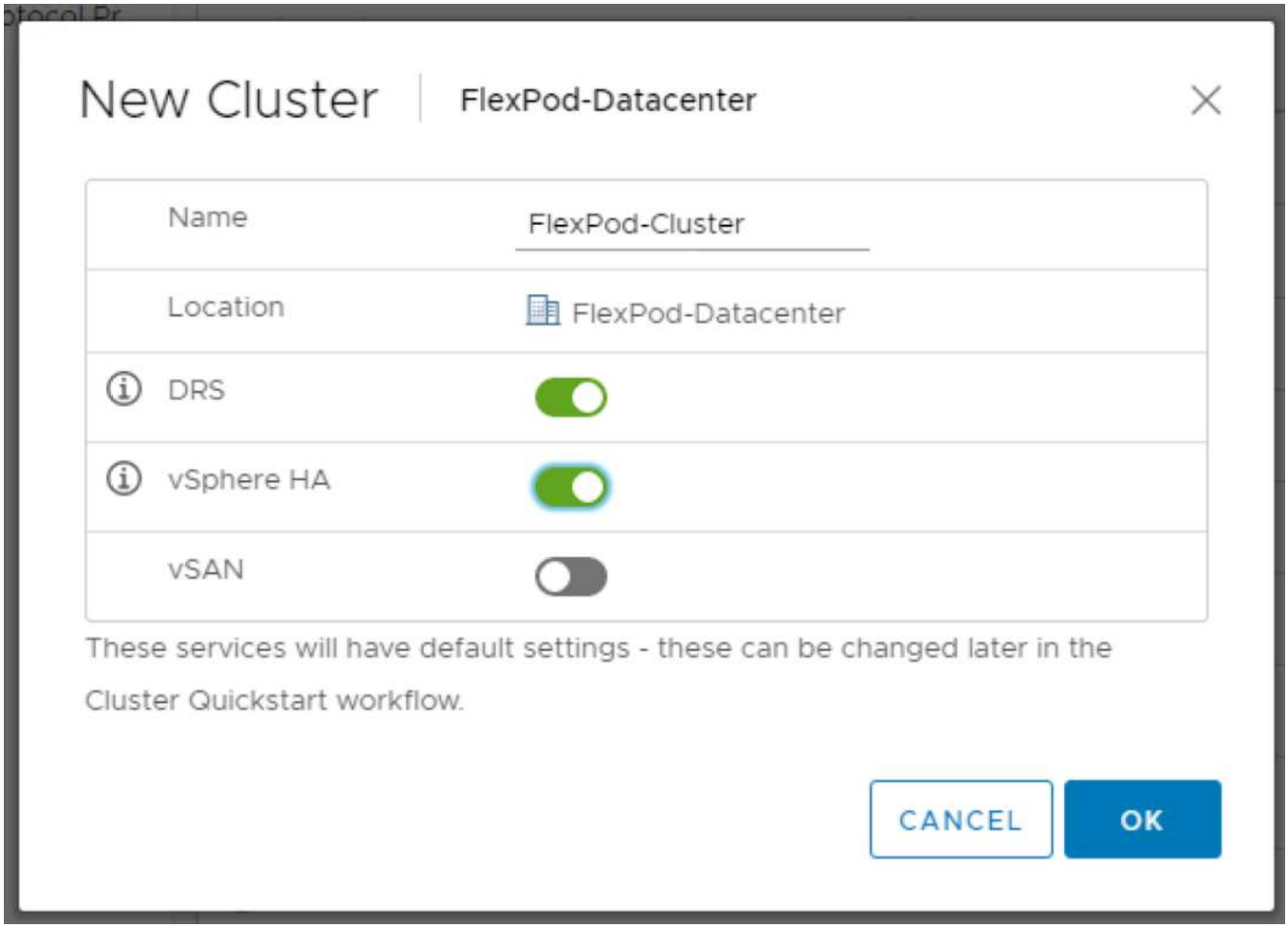
VMware vCenter Server 6.7 및 vSphere 클러스터링을 구성하려면 다음 단계를 수행하십시오.

1. "https://<<FQDN 또는 vCenter의 IP>>/vSphere-client/"로 이동합니다.
2. vSphere Client 시작 을 클릭합니다.
3. 사용자 이름 mailto:administrator@vspehre.loca l [administrator^]@vSphere.local과 VCSA 설정 프로세스 중에 입력한 SSO 암호를 사용하여 로그인합니다.
4. vCenter 이름을 마우스 오른쪽 버튼으로 클릭하고 New Datacenter를 선택합니다.
5. 데이터 센터의 이름을 입력하고 확인 을 클릭합니다.

vSphere 클러스터를 생성합니다

vSphere 클러스터를 생성하려면 다음 단계를 수행하십시오.

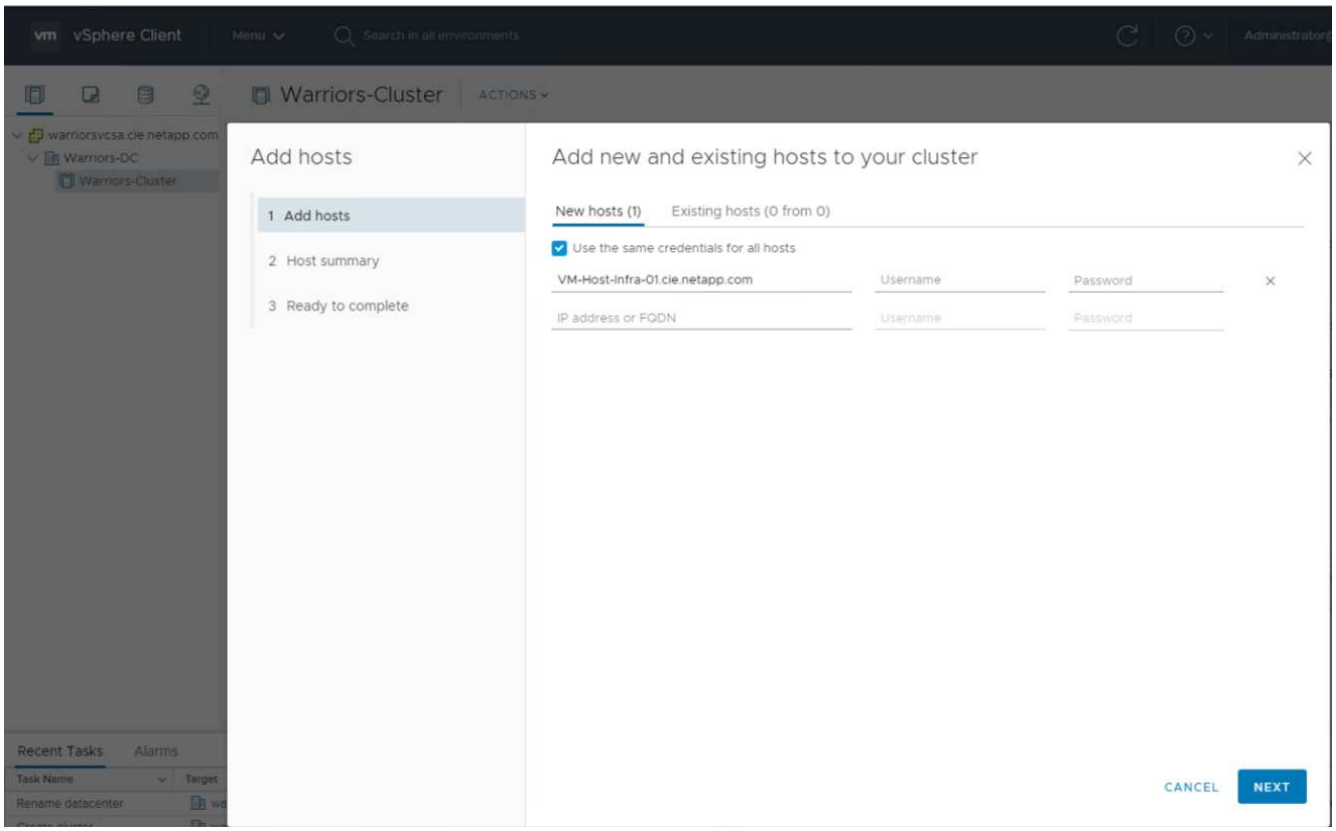
1. 새로 생성된 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 New Cluster를 선택합니다.
2. 클러스터의 이름을 입력합니다.
3. 확인란을 선택하여 DR 및 vSphere HA를 설정합니다.
4. 확인 을 클릭합니다.



클러스터에 ESXi 호스트를 추가합니다

클러스터에 ESXi 호스트를 추가하려면 다음 단계를 수행하십시오.

1. 클러스터를 마우스 오른쪽 버튼으로 클릭하고 Add Host를 선택합니다.



2. 클러스터에 ESXi 호스트를 추가하려면 다음 단계를 수행하십시오.
   a. 호스트의 IP 또는 FQDN을 입력합니다. 다음 을 클릭합니다.
   b. 루트 사용자 이름과 암호를 입력합니다. 다음 을 클릭합니다.
   c. 예를 클릭하여 호스트의 인증서를 VMware 인증서 서버에서 서명한 인증서로 바꿉니다.
   d. 호스트 요약 페이지에서 다음 을 클릭합니다.
   e. 녹색 + 아이콘을 클릭하여 vSphere 호스트에 라이센스를 추가합니다.
3. 이 단계는 원할 경우 나중에 완료할 수 있습니다.
   a. 다음 을 클릭하여 잠금 모드를 해제합니다.
   b. VM 위치 페이지에서 다음 을 클릭합니다.
   c. 완료 준비 페이지를 검토합니다. 뒤로 단추를 사용하여 변경하거나 마침 을 선택합니다.
4. Cisco UCS 호스트 B에 대해 1단계와 2단계를 반복합니다

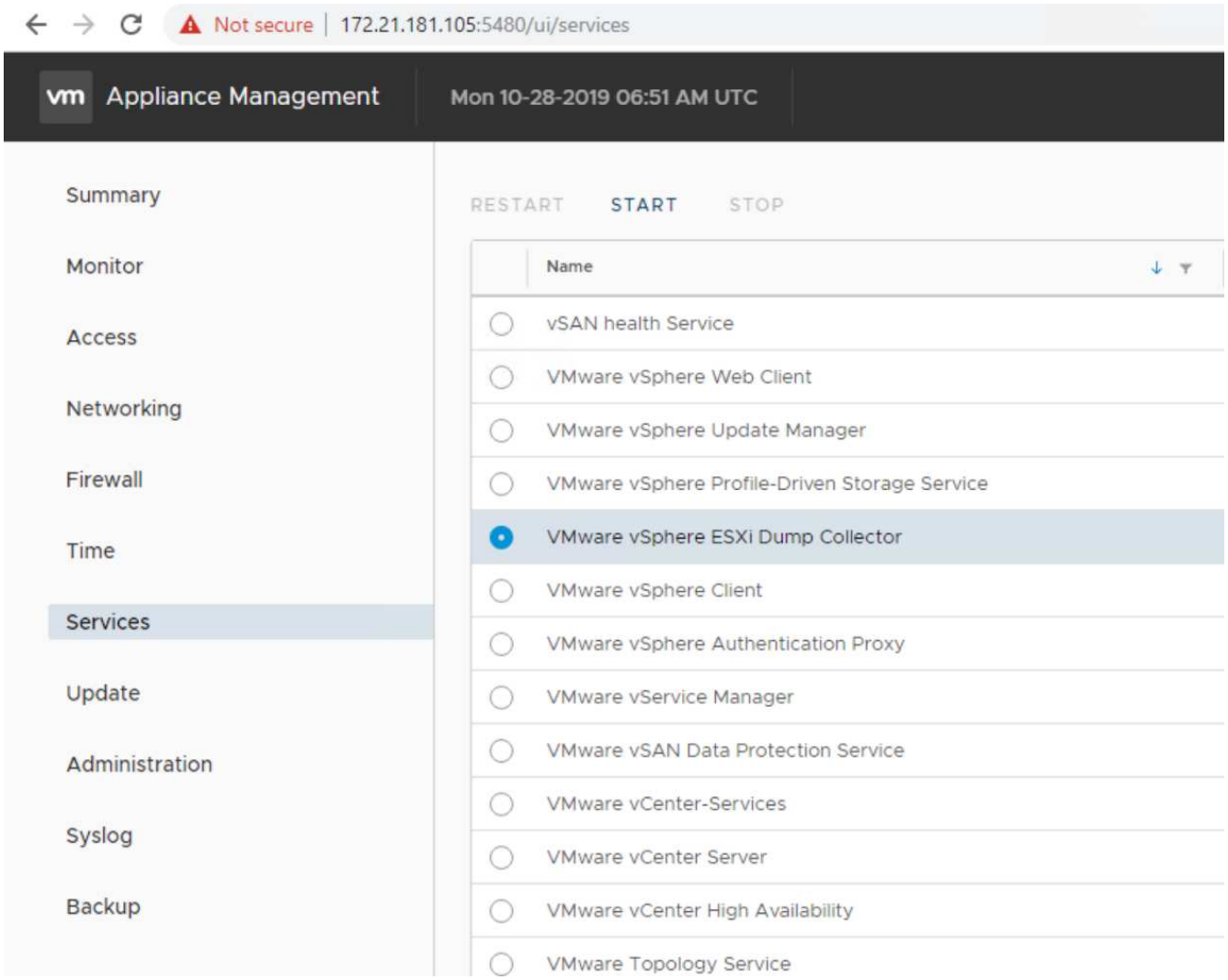
> FlexPod Express 구성에 추가된 모든 호스트에 대해 이 프로세스를 완료해야 합니다.

ESXi 호스트에서 코어 덤프를 구성합니다

ESXi 호스트에서 코어 덤프를 구성하려면 다음 단계를 수행하십시오.

1. https:// 에 로그인합니다 "vCenter 를 참조하십시오" IP: 5480/, 사용자 이름으로 root를 입력하고 루트 암호를 입력합니다.
2. 서비스를 클릭하고 VMware vSphere ESXi Dump Collector를 선택합니다.

3. VMware vSphere ESXi Dump Collector 서비스를 시작합니다.



4. SSH를 사용하여 관리 IP ESXi 호스트에 연결하고 사용자 이름에 root를 입력한 다음 루트 암호를 입력합니다.
5. 다음 명령을 실행합니다.

```
esxcli system coredump network set -i ip_address_of_core_dump_collector
-v vmk0 -o 6500
esxcli system coredump network set --enable=true
esxcli system coredump network check
```

6. 최종 명령어를 입력하면 확인된 netdump server가 실행 중인 것으로 확인되었다는 메시지가 나타난다.

```
root@VM-Host-Infra-01:~] esxcli system coredump network set -i 172.21.181.105 -
 vmk0 -o 6500
root@VM-Host-Infra-01:~]
root@VM-Host-Infra-01:~] esxcli system coredump network set --enable=true
root@VM-Host-Infra-01:~] esxcli system coredump network check
erified the configured netdump server is running
```

FlexPod Express에 추가된 모든 호스트에 대해 이 프로세스를 완료해야 합니다.

이 검증에서 "ip_address_of_core_dump_collector"는 vCenter IP입니다.

"다음: NetApp Virtual Storage Console 9.6 구축 절차"

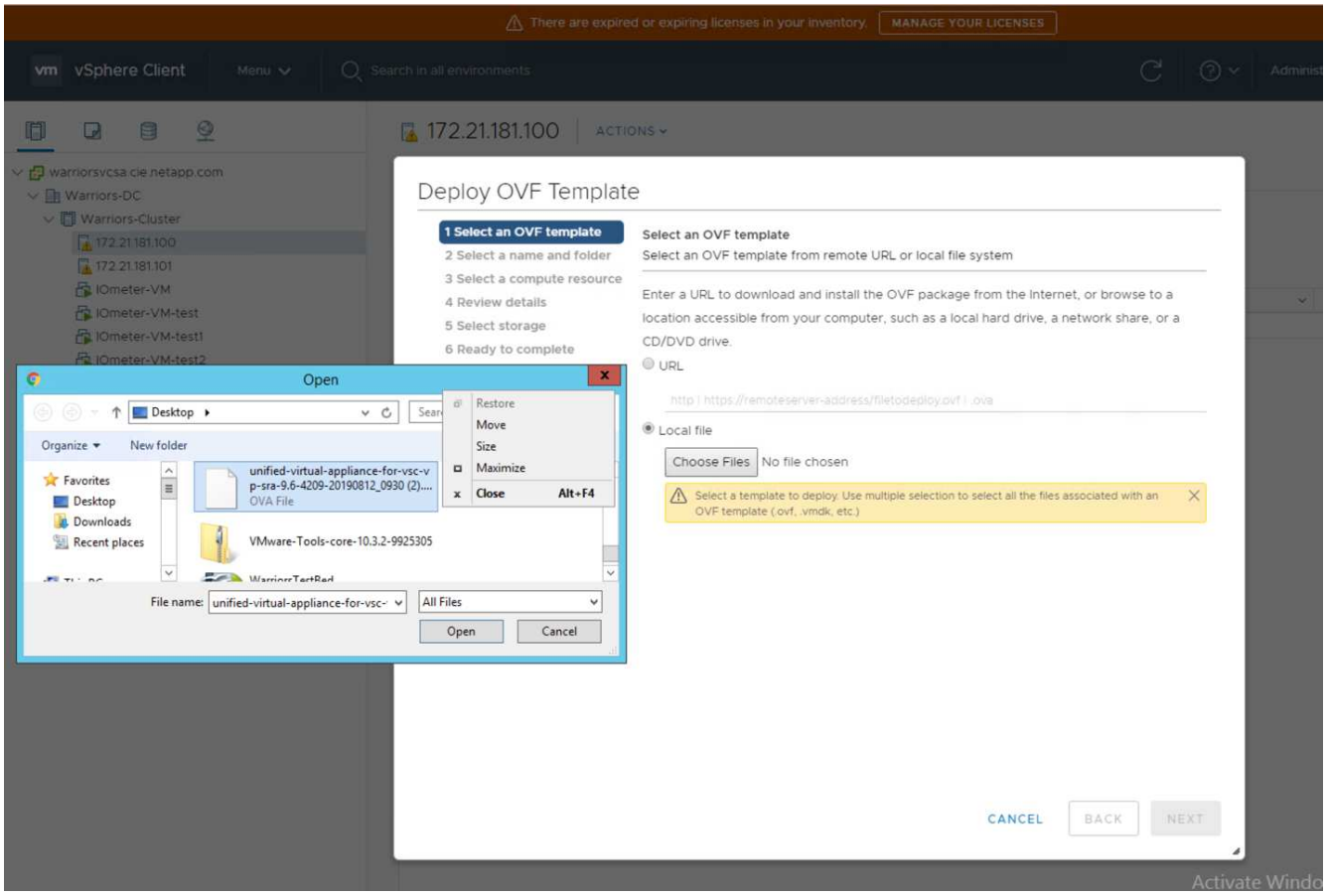
NetApp Virtual Storage Console 9.6 구축 절차

이 섹션에서는 NetApp VSC(가상 스토리지 콘솔)의 구축 절차를 설명합니다.

Virtual Storage Console 9.6을 설치합니다

OVF(Open Virtualization Format) 배포를 사용하여 VSC 9.6 소프트웨어를 설치하려면 다음 단계를 수행하십시오.

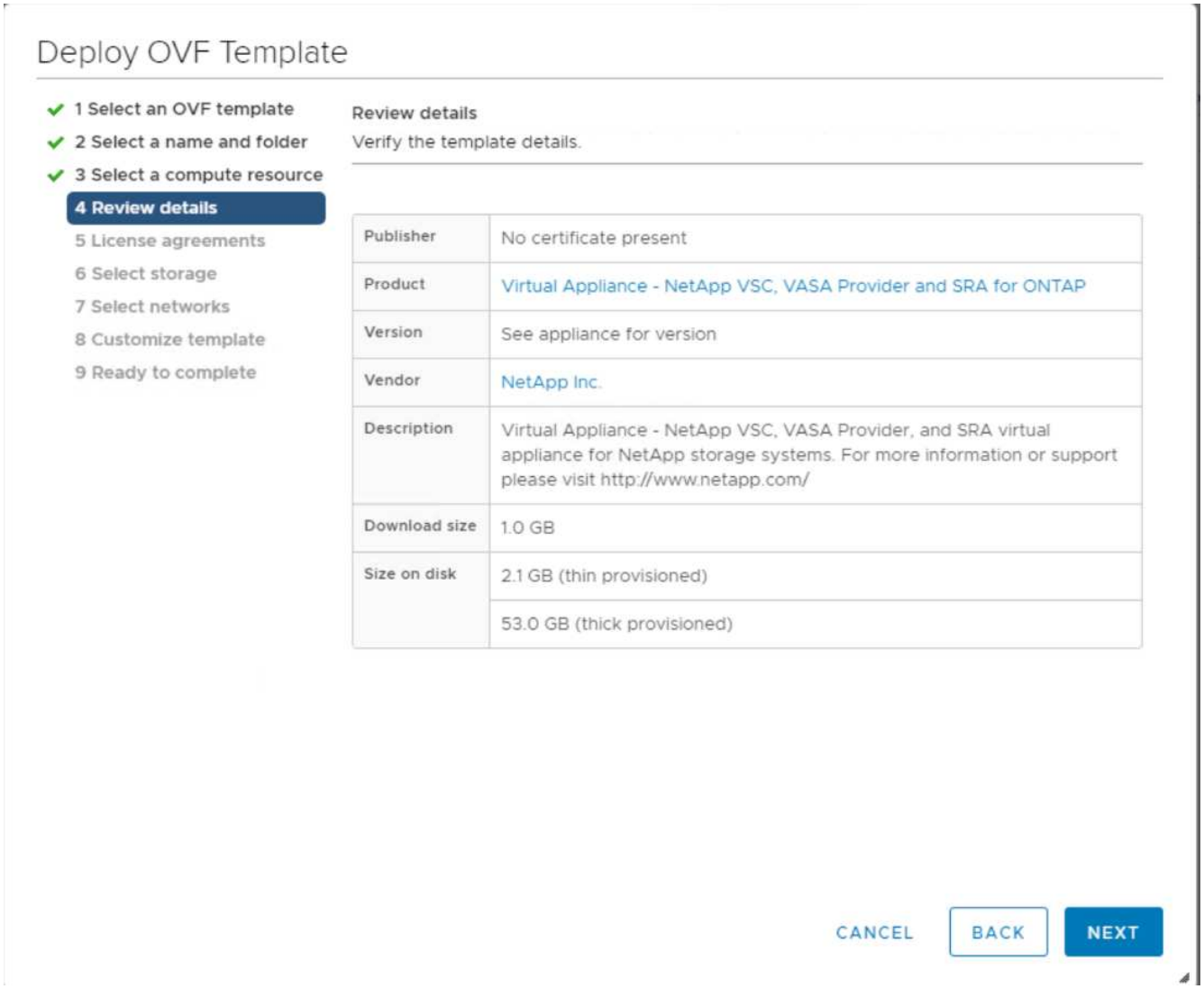
1. vSphere Web Client > Host Cluster > Deploy OVF Template 으로 이동합니다.
2. NetApp Support 사이트에서 다운로드한 VSC OVF 파일로 이동합니다.



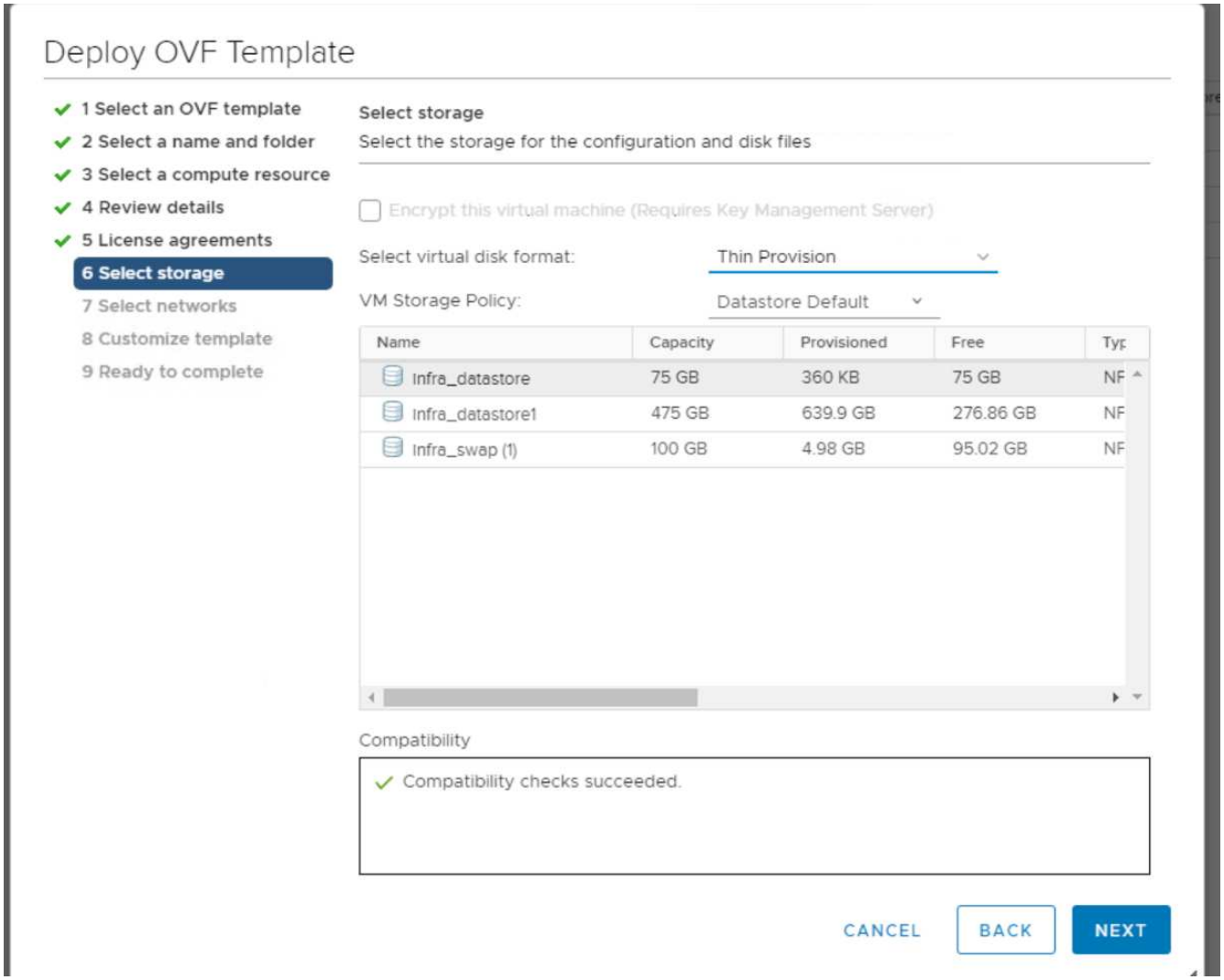
3. VM 이름을 입력하고 배포할 데이터 센터 또는 폴더를 선택합니다. 다음 을 클릭합니다.



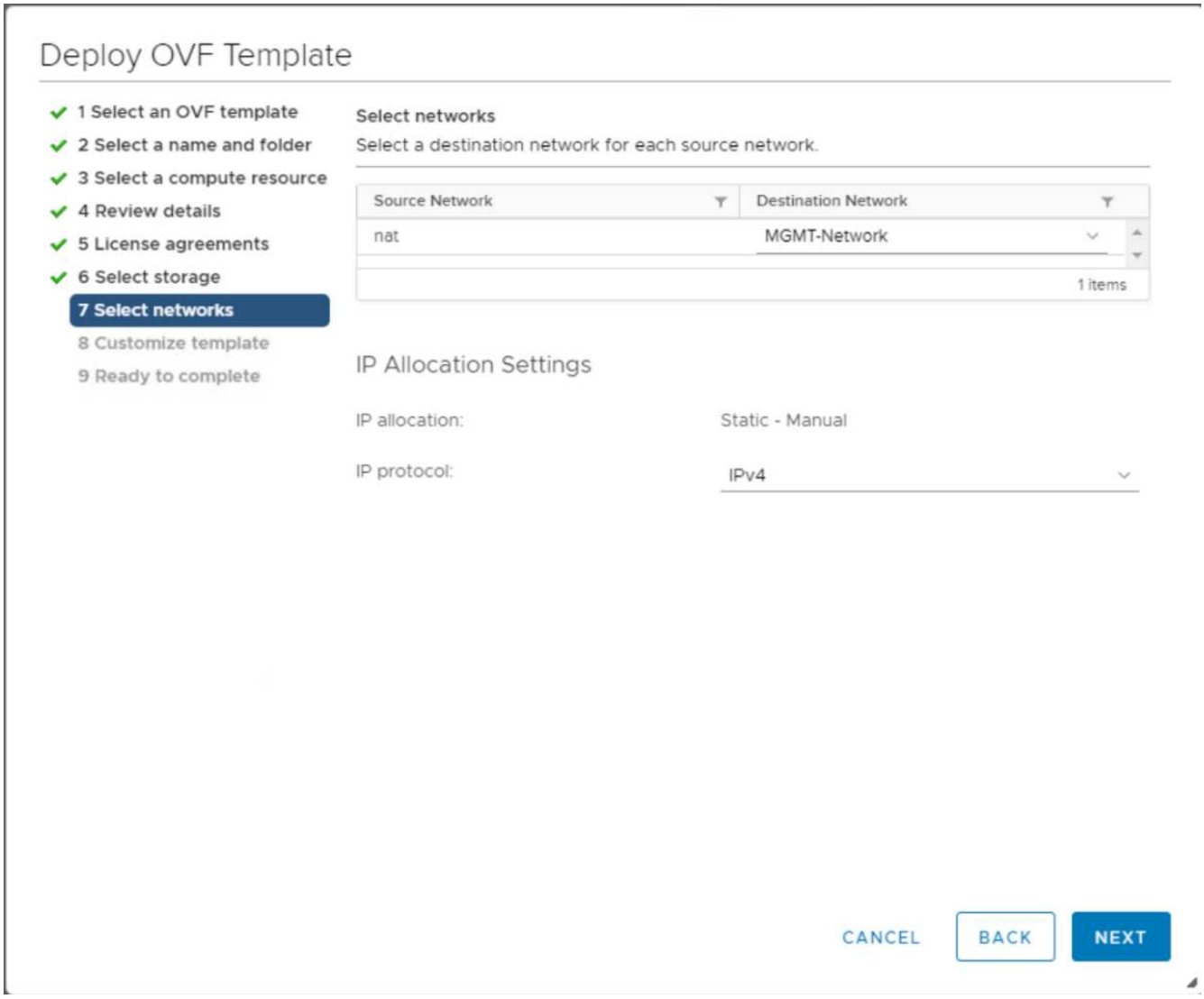
4. FlexPod-Cluster ESXi 클러스터를 선택하고 Next를 클릭합니다.
5. 세부 정보를 검토하고 Next를 클릭합니다.



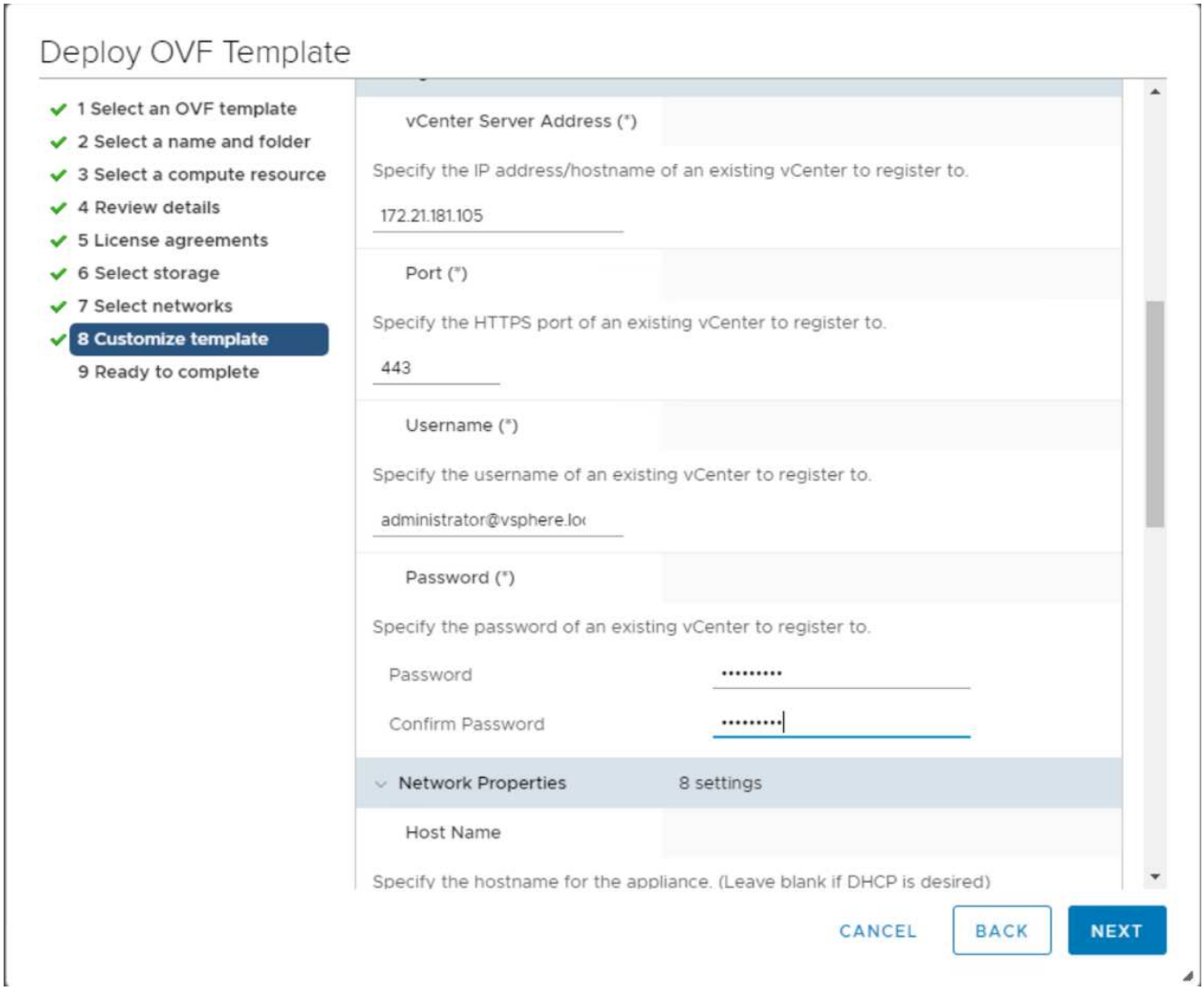
6. Accept(수락) 를 클릭하여 라이센스를 수락하고 Next(다음) 를 클릭합니다.
7. Thin Provision 가상 디스크 형식과 NFS 데이터 저장소 중 하나를 선택합니다. 다음 을 클릭합니다.



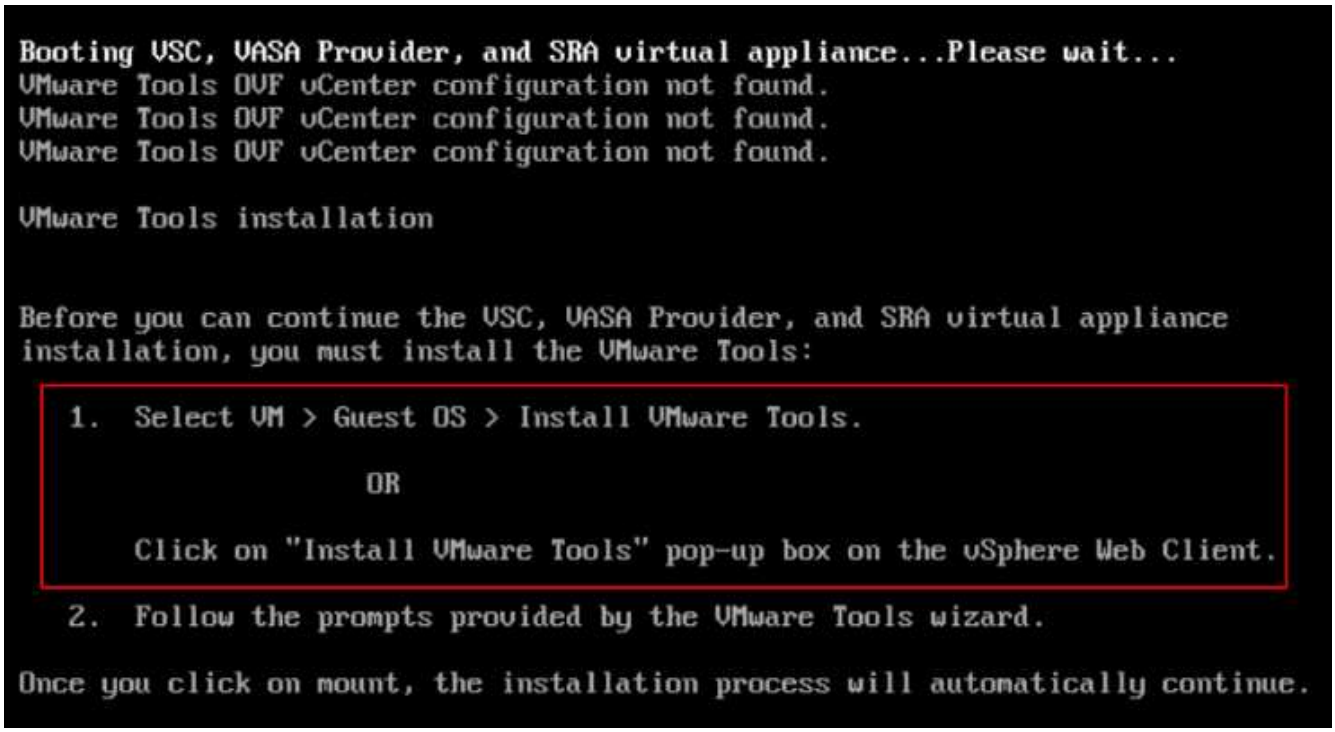
8. 네트워크 선택에서 대상 네트워크를 선택하고 다음을 클릭합니다.



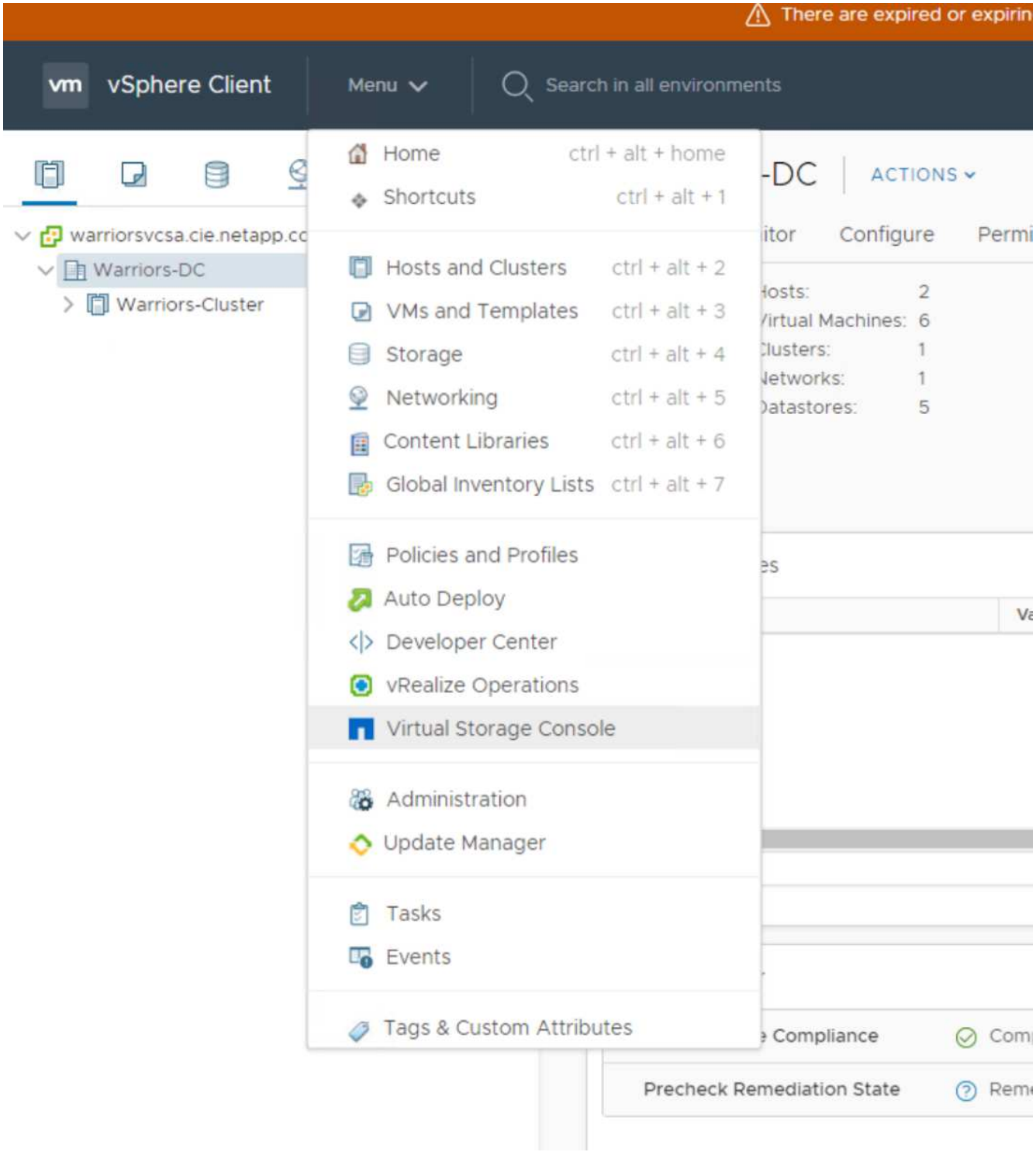
9. 템플릿 사용자 지정에서 VSC 관리자 암호, vCenter 이름 또는 IP 주소, 기타 구성 정보를 입력하고 다음을 클릭합니다.



10. 입력한 구성 세부 정보를 검토하고 Finish를 클릭하여 NetApp-VSC VM 구축을 완료합니다.
11. NetApp-VSC VM의 전원을 켜고 VM 콘솔을 엽니다.
12. NetApp-VSC VM 부팅 프로세스 중에 VMware 툴을 설치하라는 메시지가 표시됩니다. vCenter에서 NetApp-VSC VM > 게스트 OS > VMware 툴 설치 를 선택합니다.



13. OVF 템플릿 사용자 지정 중에 네트워킹 구성 및 vCenter 등록 정보가 제공되었습니다. 따라서 NetApp VSC VM을 실행한 후 VSC, VASA(vSphere API for Storage Awareness), VMware SRA(Storage Replication Adapter)가 vCenter에 등록됩니다.
14. vCenter Client에서 로그아웃하고 다시 로그인합니다. 홈 메뉴에서 NetApp VSC가 설치되었는지 확인합니다.



NetApp NFS VAAI 플러그인을 다운로드하고 설치합니다

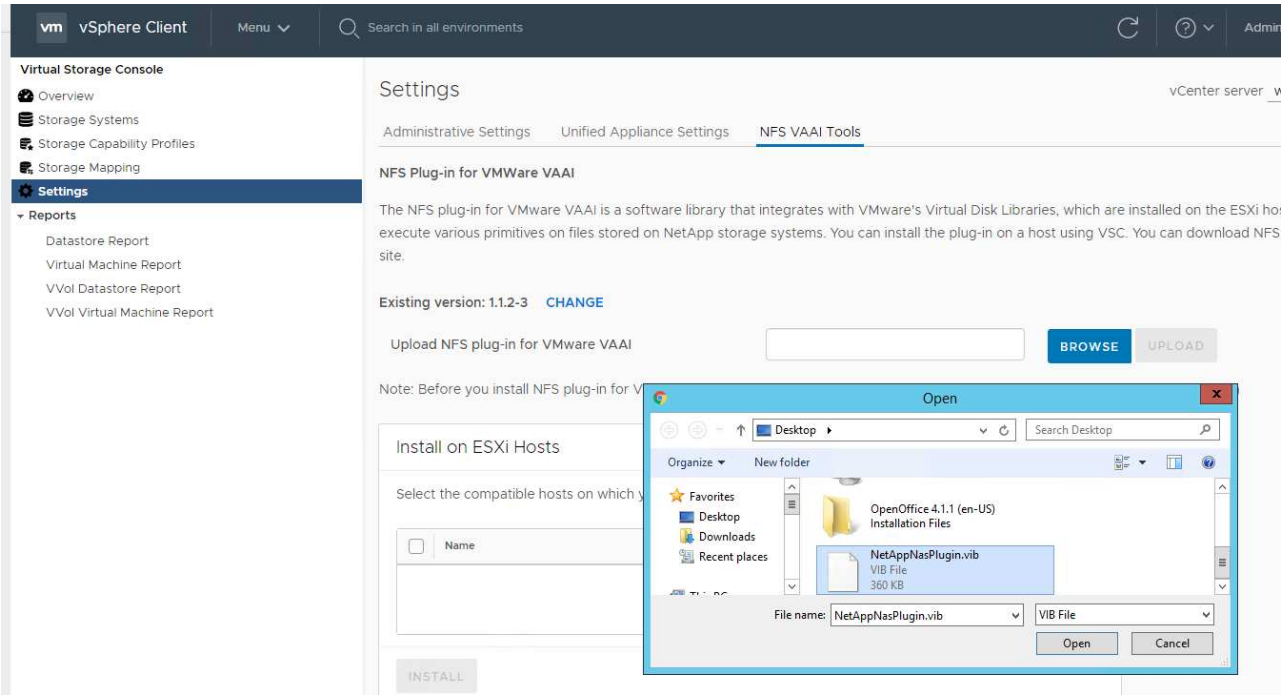
NetApp NFS VAAI 플러그인을 다운로드하고 설치하려면 다음 단계를 완료하십시오.

1. NetApp NFS Plug-in 1.1.2 for VMware를 다운로드합니다. NFS 플러그인 다운로드 페이지에서 VIB' 파일을 로컬 컴퓨터 또는 관리 호스트에 저장합니다.
2. NetApp NFS Plug-in for VMware VAAI 다운로드:
   a. 로 이동합니다 "소프트웨어 다운로드 페이지".

b. 아래로 스크롤하여 VMware VAAI용 NetApp NFS 플러그인 을 클릭합니다.

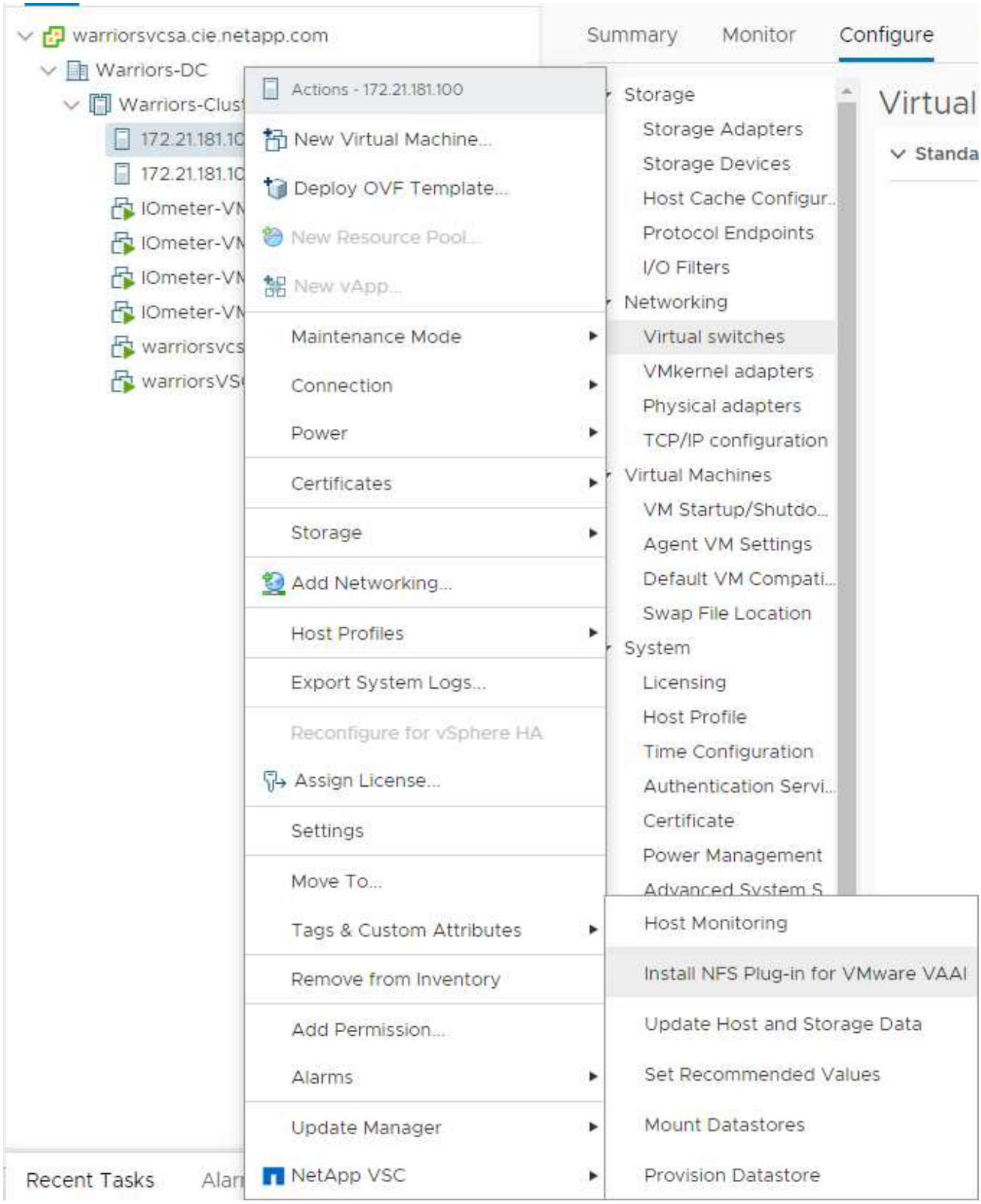
c. vSphere 웹 클라이언트의 홈 화면에서 가상 스토리지 콘솔을 선택합니다.

d. Virtual Storage Console > Settings > NFS VAAI Tools 에서 Select File 을 선택하고 다운로드한 플러그인이 저장된 위치로 이동하여 NFS 플러그인을 업로드합니다.



3. 업로드 를 클릭하여 플러그인을 vCenter로 전송합니다.

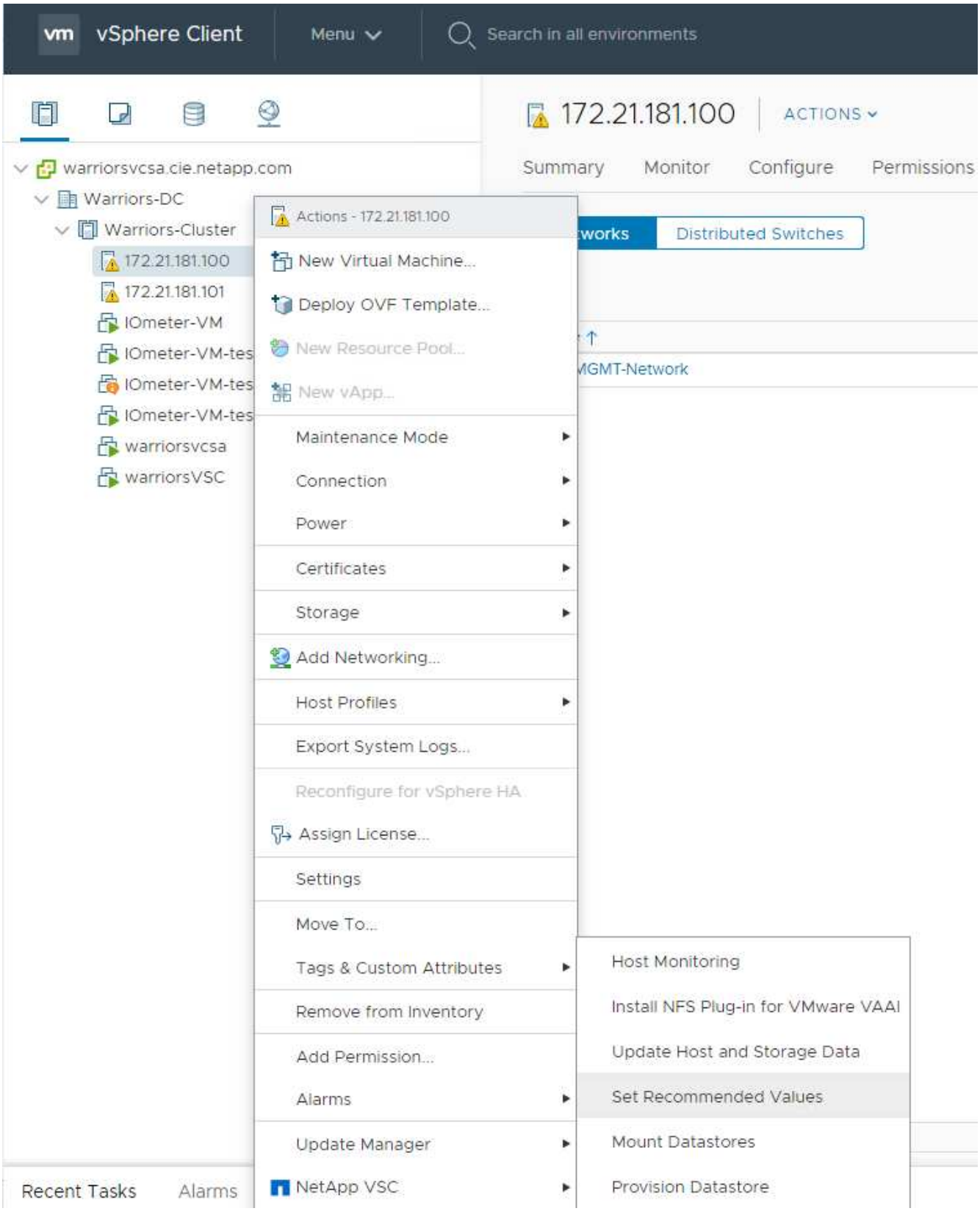
4. 호스트를 선택한 다음 NetApp VSC > Install NFS Plug-in for VMware VAAI 를 선택합니다.



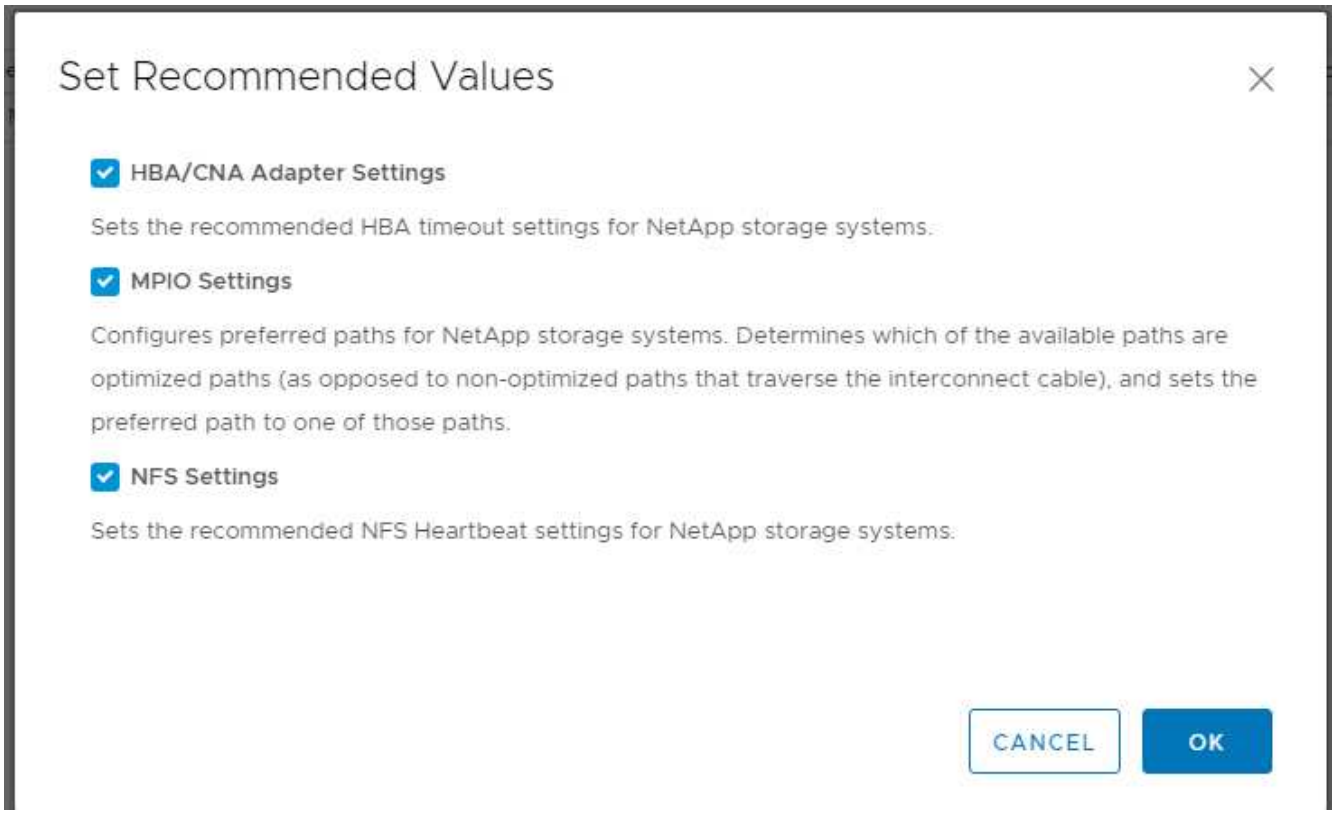
ESXi 호스트에 대한 최적의 스토리지 설정을 사용합니다

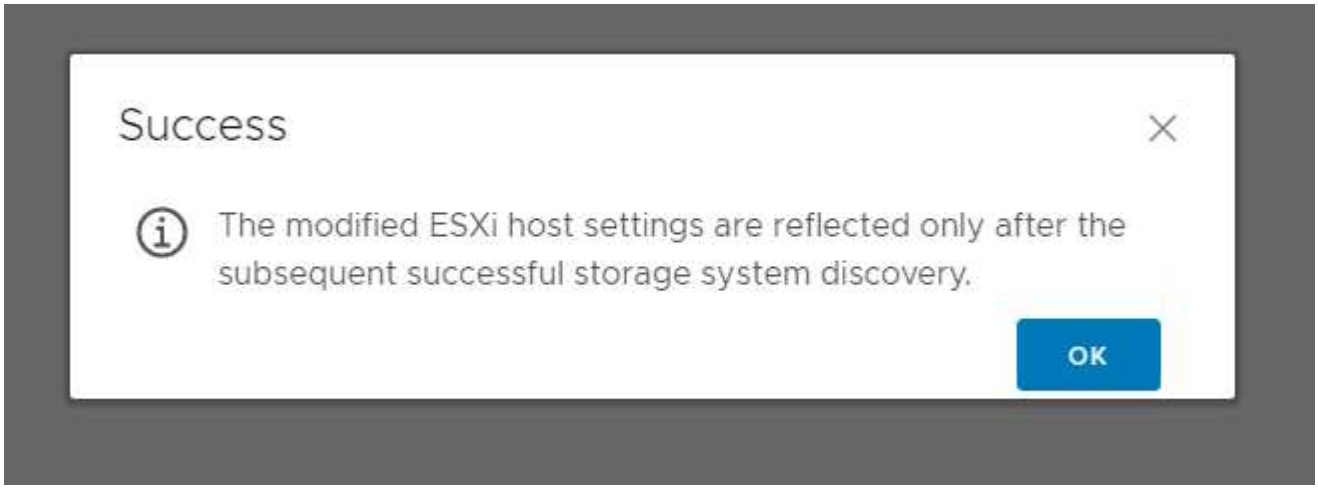
VSC를 사용하면 NetApp 스토리지 컨트롤러에 연결된 모든 ESXi 호스트의 스토리지 관련 설정을 자동으로 구성할 수 있습니다. 이러한 설정을 사용하려면 다음 단계를 완료하십시오.

1. 홈 화면에서 vCenter > 호스트 및 클러스터 를 선택합니다. 각 ESXi 호스트에 대해 NetApp VSC > Set Recommended Values를 마우스 오른쪽 버튼으로 클릭하고 선택합니다.



2. 선택한 vSphere 호스트에 적용할 설정을 선택합니다. 확인 을 클릭하여 설정을 적용합니다.





3. 이러한 설정을 적용한 후 ESXi 호스트를 재부팅합니다.

결론

FlexPod Express는 업계 최고의 구성요소를 사용하는 검증된 설계를 통해 간단하고 효율적인 솔루션을 제공합니다. 구성요소 추가를 통해 확장하여 특정 비즈니스 요구에 맞게 FlexPod Express를 조정할 수 있습니다. FlexPod Express는 전용 솔루션이 필요한 중소기업, ROBO 및 기타 기업을 위해 설계되었습니다.

감사의 말

저자는 John George가 이 설계에 대한 지원과 기여에 대해 인정하기를 원합니다.

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대한 자세한 내용은 다음 문서 및/또는 웹 사이트를 참조하십시오.

NetApp 제품 설명서

http://docs. "넷엡"com

FlexPod Express with Guide를 참조하십시오

NVA-1139-design:FlexPod Express with Cisco UCS C-Series 및 NetApp AFF C190 Series

"https://www.netapp.com/us/media/nva-1139-design.pdf"

버전 기록

버전	날짜	문서 버전 기록
버전 1.0	2019년 11월	최초 릴리스.

FlexPod Express with Cisco UCS C-Series and AFF A220 Series 설계 가이드 를 참조하십시오

NVA-1125-design: FlexPod Express with Cisco UCS C-Series and AFF A220 Series

Savita Kumari, NetApp과의 파트너십:

업계 동향에 따르면 많은 데이터 센터가 공유 인프라 및 클라우드 컴퓨팅으로 전환하고 있습니다. 또한 기업에서는 데이터 센터에서 친숙한 기술을 활용하여 원격 사무소 및 지사를 위한 간편하고 효율적인 솔루션을 찾고 있습니다.

FlexPod Express는 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 스위치 제품군, NetApp AFF를 기반으로 사전 설계되고 모범 사례 데이터 센터 아키텍처입니다. FlexPod Express의 구성 요소는 FlexPod 데이터 센터 구성 요소와 비슷하므로 더 작은 규모로 전체 IT 인프라 환경에서 관리 시너지 효과를 실현할 수 있습니다. FlexPod 데이터 센터 및 FlexPod 익스프레스는 가상화 및 베어 메탈 운영 체제 및 엔터프라이즈 워크로드를 위한 최적의 플랫폼입니다.

"다음: 프로그램 요약."

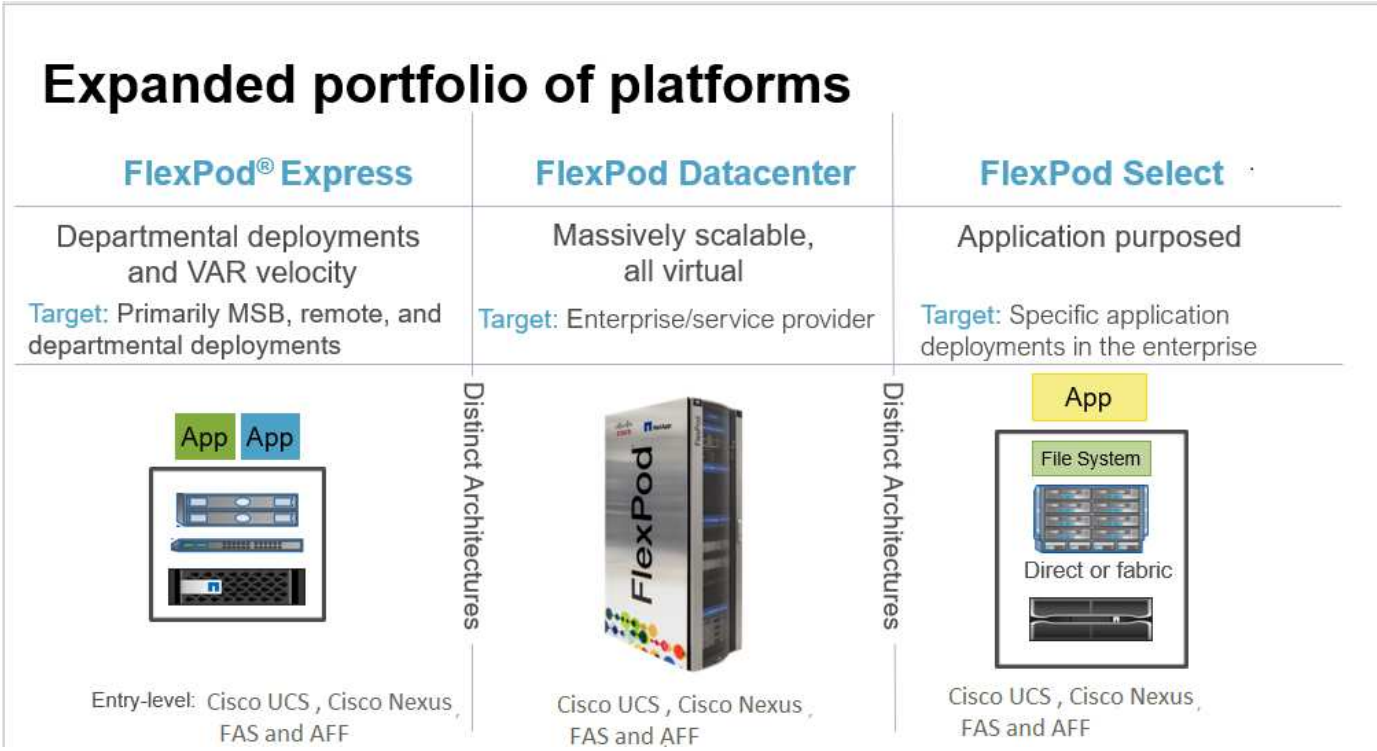
프로그램 요약

FlexPod 통합 인프라 포트폴리오

FlexPod 참조 아키텍처는 CVD(Cisco Validated Design) 또는 NVA(NetApp Verified Architecture)로 제공됩니다. 특정 CVD 또는 NVA의 고객 요구 사항을 기반으로 편차가 지원되지 않는 구성을 구축해야 하는 경우 허용됩니다.

다음 그림과 같이 FlexPod 포트폴리오에는 FlexPod 익스프레스, FlexPod 데이터 센터 및 FlexPod 선택의 세 가지 솔루션이 포함되어 있습니다.

- * FlexPod 익스프레스. * 는 Cisco와 NetApp의 기술로 구성된 엔트리 레벨 솔루션을 제공합니다.
- * FlexPod 데이터 센터 * 는 다양한 워크로드 및 애플리케이션을 위한 최적의 다목적 토대를 제공합니다.
- * FlexPod 선택. * FlexPod 데이터 센터의 최고 기능을 통합하고 특정 애플리케이션에 맞게 인프라를 조정합니다.



NetApp 검증 아키텍처 프로그램

NVA 프로그램은 NetApp 솔루션을 위한 검증된 아키텍처를 고객에게 제공합니다. NVA는 NetApp 솔루션의 다음과 같은 특징을 의미합니다.

- 철저한 테스트를 거친 아키텍처
- 기본적으로 규범적인 아키텍처
- 구축 위험 최소화
- 출시 시기를 단축합니다

이 가이드에서는 VMware vSphere를 사용한 FlexPod Express 설계에 대해 자세히 설명합니다. 또한, 이 설계는 NetApp ONTAP 9.4 소프트웨어, Cisco Nexus 3172P 스위치 및 Cisco UCS C220 M5 서버를 하이퍼바이저 노드로 실행하는 완전히 새로운 AFF A220 시스템을 활용합니다.

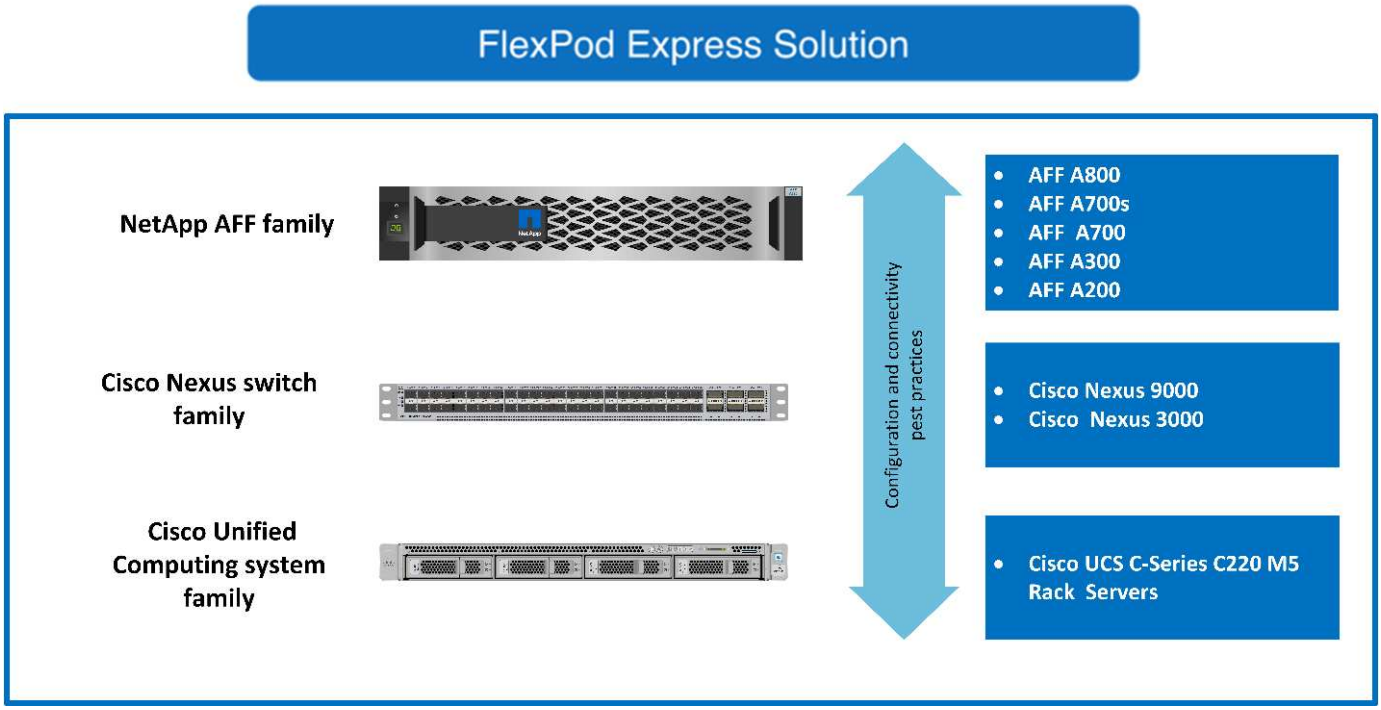
이 문서는 AFF A220에서 검증되었습니다. 하지만 이 솔루션은 FAS2700도 지원합니다.

"다음: 솔루션 개요"

솔루션 개요

FlexPod Express는 혼합 가상화 워크로드를 실행하도록 설계되었습니다. 원격 사무소, 지점 및 중소 및 중견 기업을 타겟으로 합니다. 또한 전용 솔루션을 특정 목적에 구축하고자 하는 대규모 기업에도 적합합니다. FlexPod Express를 위한 이 새로운 솔루션에는 NetApp ONTAP 9.4, NetApp AFF A220 및 VMware vSphere 6.7과 같은 새로운 기술이 추가되었습니다.

다음 그림에서는 FlexPod Express 솔루션에 포함된 하드웨어 구성 요소를 보여 줍니다.

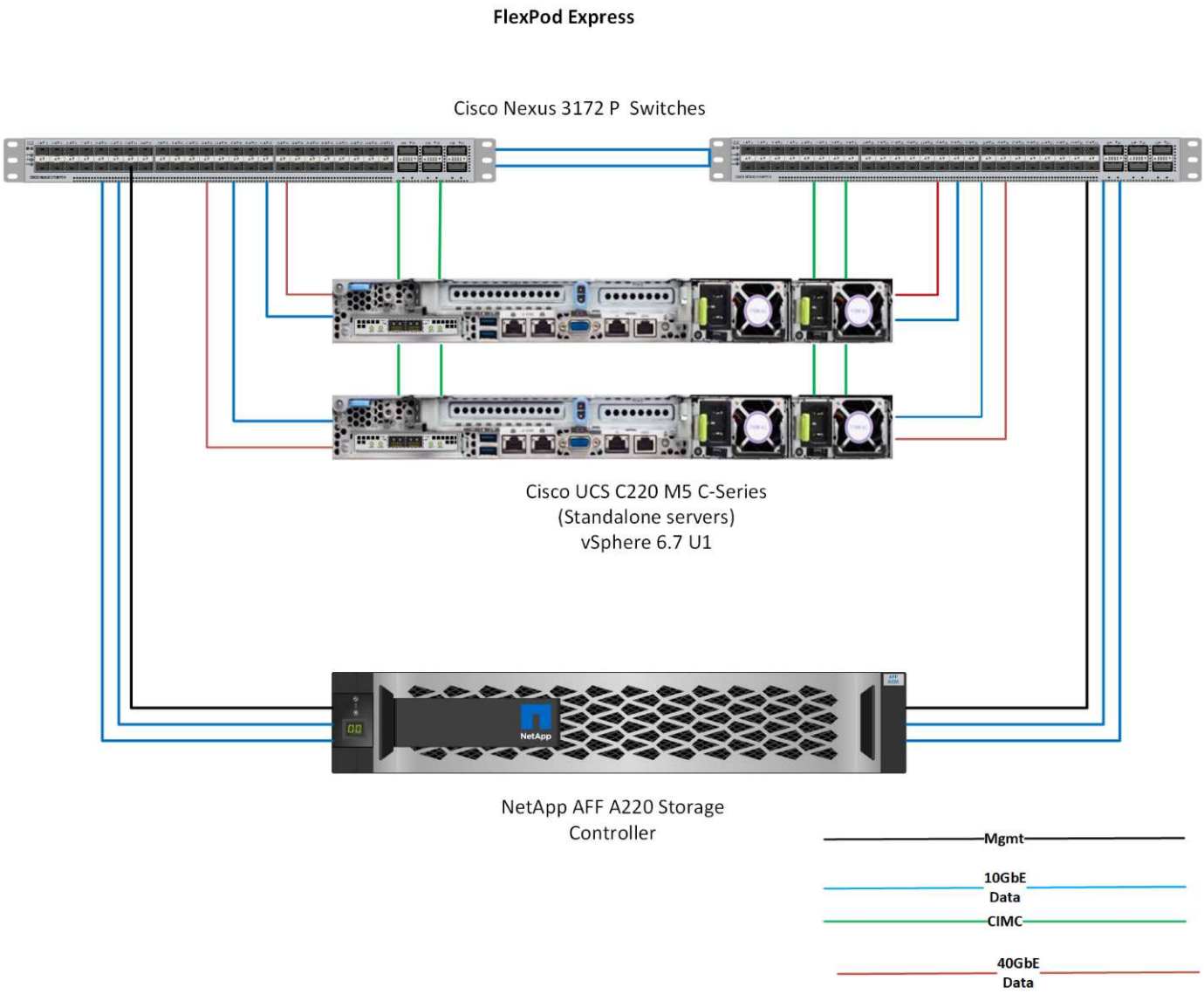


대상

이 문서는 IT 효율성을 제공하고 IT 혁신을 지원하는 인프라를 활용하려는 사용자를 위해 작성되었습니다. 이 문서의 대상에는 세일즈 엔지니어, 현장 컨설턴트, 프로페셔널 서비스 직원, IT 매니저, 파트너 엔지니어 및 고객.

솔루션 기술

이 솔루션은 NetApp, Cisco 및 VMware의 최신 기술을 활용합니다. 이 솔루션에는 ONTAP 9.4 소프트웨어, 이중 Cisco Nexus 3172P 스위치 및 VMware vSphere 6.7을 실행하는 Cisco UCS C220 M5 랙 서버를 실행하는 새로운 NetApp AFF A220 시스템이 포함되어 있습니다. 이 검증된 솔루션은 10기가비트 이더넷(10GbE) 기술을 사용합니다. 다음 그림에서는 개요를 보여 줍니다. 또한 FlexPod 익스프레스 아키텍처가 조직의 변화하는 비즈니스 요구에 적응할 수 있도록 한 번에 두 개의 하이퍼바이저 노드를 추가하여 확장하는 방법에 대한 지침도 제공됩니다.



40GbE는 검증되지 않았지만 지원되는 인프라입니다.

"다음: 기술 요구 사항."

기술 요구 사항

FlexPod Express를 사용하려면 선택한 하이퍼바이저와 네트워크 속도에 따라 하드웨어 및 소프트웨어 구성요소를 조합해야 합니다. 또한 FlexPod Express는 하이퍼바이저 노드를 시스템에 추가하는 데 필요한 하드웨어 구성요소를 2개 단위로 배치합니다.

하드웨어 요구 사항

선택한 하이퍼바이저에 관계없이 모든 FlexPod Express 구성은 동일한 하드웨어를 사용합니다. 따라서 비즈니스 요구사항이 변경되더라도 두 하이퍼바이저 중 하나를 동일한 FlexPod Express 하드웨어에서 실행할 수 있습니다.

다음 표에는 모든 FlexPod Express 구성과 솔루션 구축에 필요한 하드웨어 구성요소가 나와 있습니다. 이 솔루션을 구체적으로 구축하는 데 사용되는 하드웨어 구성요소는 고객 요구사항에 따라 다를 수 있습니다.

하드웨어	수량
AFF A220 2노드 클러스터	1
Cisco UCS C220 M5 서버	2
Cisco Nexus 3172P 스위치	2
Cisco UCS C220 M5 랙 서버용 Cisco UCS VIC(Virtual Interface Card) 1387	2
Cisco CVR-QSFP-SFP 10G 어댑터	4

소프트웨어 요구 사항

다음 표에서는 FlexPod Express 솔루션의 아키텍처를 구현하는 데 필요한 소프트웨어 구성 요소를 보여 줍니다.

다음 표에는 기본 FlexPod Express 구현에 대한 소프트웨어 요구 사항이 나와 있습니다.

소프트웨어	버전	세부 정보
CIMC(Cisco Integrated Management Controller)	3.1.3	C220 M5 랙 서버용
Cisco NX-OS입니다	nxos.7.0.3.I7.5.bin	Cisco Nexus 3172P 스위치용
NetApp ONTAP를 참조하십시오	9.4	AFF A220 컨트롤러

다음 표에는 FlexPod Express의 모든 VMware vSphere 구축에 필요한 소프트웨어가 나와 있습니다.

소프트웨어	버전
VMware vCenter Server 어플라이언스	6.7
VMware vSphere ESXi	6.7
ESXi용 NetApp VAAI 플러그인	1.1.2

"다음: 디자인 선택."

디자인 선택

이 설계를 설계하는 과정에서 다음과 같은 기술이 선택되었습니다. 각 기술은 FlexPod 익스프레스 인프라 솔루션에서 특정 목적에 부합합니다.

NetApp AFF A220 시리즈(ONTAP 9.4 포함)

이 솔루션은 NetApp AFF A220과 ONTAP 9.4 소프트웨어 등 두 가지 최신 NetApp 제품을 활용합니다.

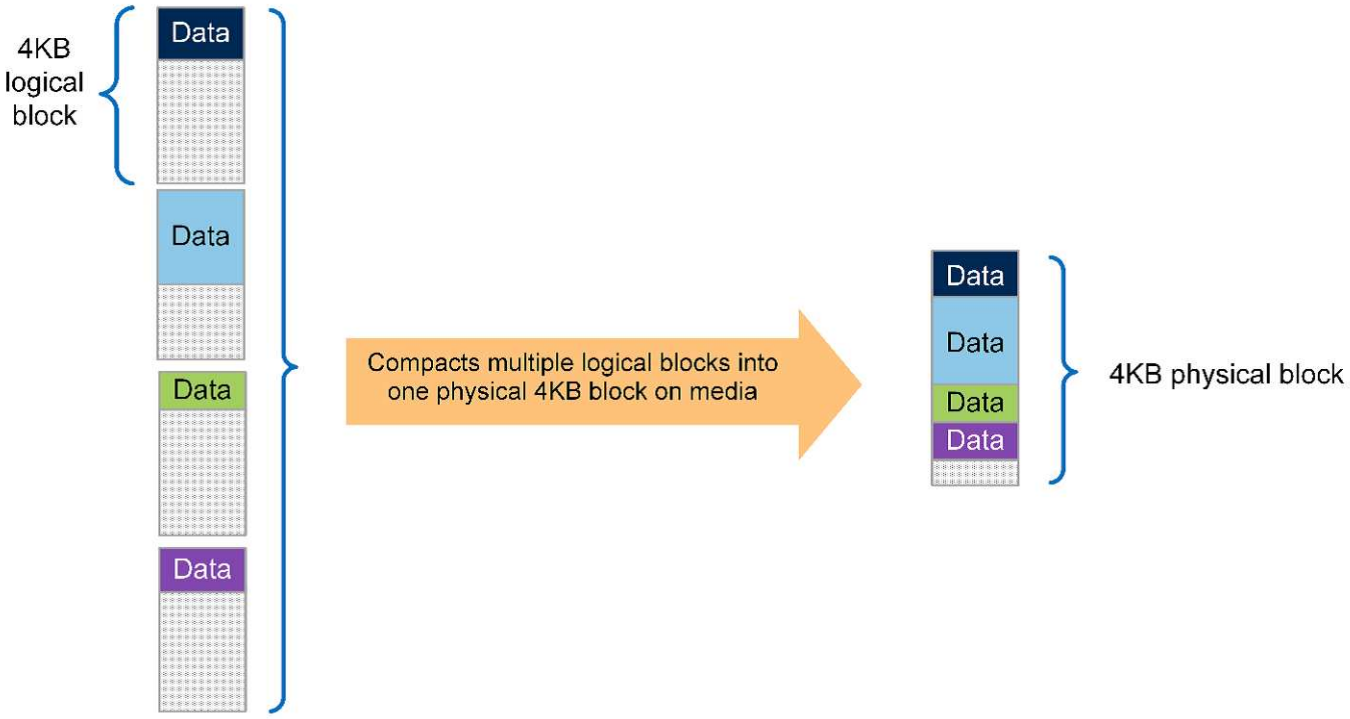
AFF A220 시스템

AFF A220 하드웨어 시스템에 대한 자세한 내용은 를 참조하십시오 "AFF A 시리즈 홈 페이지".

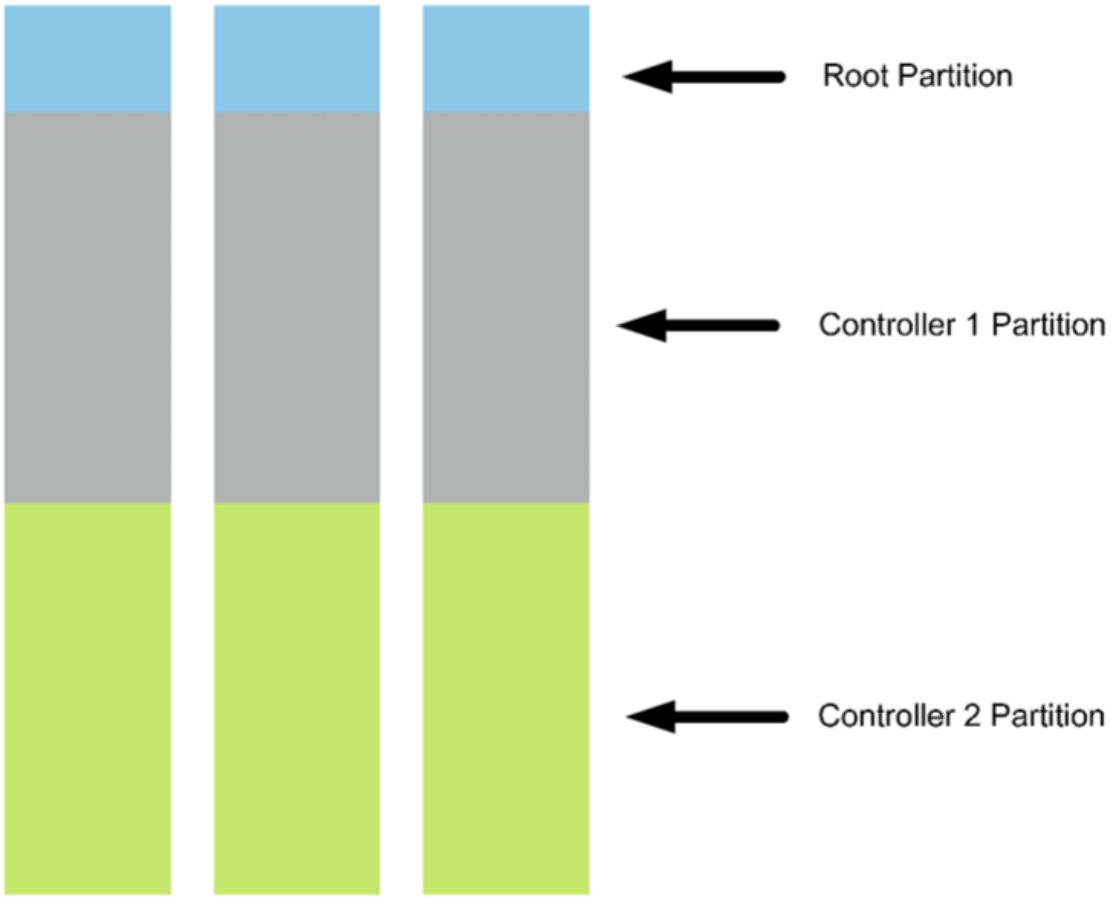
ONTAP 9.4 소프트웨어

NetApp AFF A220 시스템은 새로운 ONTAP 9.4 소프트웨어를 사용합니다. ONTAP 9.4는 업계 최고의 엔터프라이즈 데이터 관리 소프트웨어입니다. 새로운 버전에는 새로운 수준의 단순성과 유연성, 강력한 데이터 관리 기능, 스토리지 효율성, 업계 최고 수준의 클라우드 통합이 결합되어 있습니다.

ONTAP 9.4에는 FlexPod Express 솔루션에 적합한 여러 기능이 있습니다. 가장 중요한 것은 NetApp이 스토리지 효율성을 위해 노력하고 있다는 점입니다. 이는 소규모 구축에 있어서 가장 중요한 기능 중 하나입니다. 중복제거, 압축, 씬 프로비저닝과 같은 NetApp 스토리지 효율성 기능의 특징은 ONTAP 9.4에 새로 추가된 압축 기능입니다. NetApp WAFL 시스템은 항상 4KB 블록을 쓰기 때문에 컴팩션은 블록이 4KB의 할당된 공간을 사용하지 않을 때 여러 블록을 4KB 블록으로 결합합니다. 다음 그림에서는 이 프로세스를 보여 줍니다.



또한 AFF A220 시스템에서 루트 데이터 파티셔닝을 활용할 수 있습니다. 이러한 파티셔닝으로 루트 애그리게이트 및 두 데이터 애그리게이트를 시스템의 디스크에 스트라이핑할 수 있습니다. 따라서 2노드 AFF A220 클러스터의 두 컨트롤러는 aggregate에 있는 모든 디스크의 성능을 활용할 수 있습니다. 다음 그림을 참조하십시오.



이러한 기능은 FlexPod 익스프레스 솔루션을 보완하는 몇 가지 핵심 기능일 뿐입니다. ONTAP 9.4의 추가 기능에 대한 자세한 내용은 를 참조하십시오 "ONTAP 9 데이터 관리 소프트웨어 데이터시트입니다". 또한 "ONTAP 9 문서 센터" ONTAP 9.4를 포함하도록 업데이트된 NetApp를 참조하십시오.

Cisco Nexus 3000 시리즈

Cisco Nexus 3172P는 1/10/40/100Gbps 스위칭을 제공하는 강력하고 비용 효율적인 스위치입니다. Cisco Nexus 3172PQ 스위치는 Unified Fabric 제품군의 일부로서 랙 상단형 데이터 센터 구축을 위한 소형 1랙 유닛(1RU) 스위치입니다. (다음 그림 참조) 1RU에서 최대 72개의 1/10GbE 포트 또는 48개의 1/10GbE 포트를 제공하며 1RU에서 6개의 40GbE 포트를 제공합니다. 또한 물리적 계층의 유연성을 극대화하기 위해 1/10/40Gbps를 지원합니다.

다양한 Cisco Nexus 시리즈 모델이 동일한 기본 운영 체제인 NX-OS를 실행하므로 FlexPod Express 및 FlexPod Datacenter 솔루션에서 여러 Cisco Nexus 모델이 지원됩니다.

성능 사양은 다음과 같습니다.

- 모든 포트에서 회선 속도 트래픽 처리량(계층 2와 3 모두
- 최대 9216바이트(점보 프레임)의 구성 가능한 최대 전송 단위(MTU)



Cisco Nexus 3172 스위치에 대한 자세한 내용은 을 참조하십시오 "Cisco Nexus 3172PQ, 3172TQ, 3172TQ-32T, 3172PQ-XL 및 3172TQ-XL 스위치 데이터 시트".

Cisco UCS C-Series 를 참조하십시오

FlexPod 익스프레스 구축에서는 다양한 구성 옵션으로 Cisco UCS C-Series 랙 서버를 FlexPod 익스프레스 설치시 특정 요구사항에 맞게 구성할 수 있기 때문에 Cisco UCS C-Series 랙 서버를 선택했습니다.

Cisco UCS C-Series 랙 서버는 업계 표준 폼 팩터에서 유니파이드 컴퓨팅을 제공하여 TCO를 절감하고 민첩성을 향상합니다.

Cisco UCS C-Series 랙 서버는 다음과 같은 이점을 제공합니다.

- Cisco UCS의 폼 팩터 중립적인 엔트리 레벨
- 애플리케이션을 간편하고 신속하게 구축
- 통합 컴퓨팅 혁신 및 이점을 랙 서버로 확장
- 친숙한 랙 패키지의 고유한 이점을 통해 고객의 선택 옵션 증가



이전 그림의 Cisco UCS C220 M5 랙 서버(이전 그림 참조)는 업계에서 가장 다양한 범용 엔터프라이즈 인프라 및 애플리케이션 서버 중 하나입니다. 이 서버는 가상화, 협업 및 베어 메탈 애플리케이션을 비롯하여 광범위한 워크로드에 업계 최고의 성능과 효율성을 제공하는 고밀도 2소켓 랙 서버입니다. Cisco UCS C-Series 랙 서버는 독립형 서버로 또는 Cisco UCS의 일부로 구축할 수 있으므로 Cisco의 표준 기반 통합 컴퓨팅 혁신 기술을 활용하여 고객의 TCO를 줄이고 비즈니스 민첩성을 높일 수 있습니다.

C220 M5 서버에 대한 자세한 내용은 를 참조하십시오 "Cisco UCS C220 M5 랙 서버 데이터 시트".

C220 M5 랙 서버용 연결 옵션

C220 M5 랙 서버의 연결 옵션은 다음과 같습니다.

- * Cisco UCS VIC 1387 *

  Cisco UCS VIC 1387(다음 그림 참조)은 모듈식-LAN-On-Motherboard(mLOM) 폼 팩터에서 이중 포트 확장 QSFP+ 40GbE 및 FCoE(FC over Ethernet)를 제공합니다. mLOM 슬롯을 사용하면 PCIe(Peripheral Component Interconnect Express) 슬롯을 사용하지 않고도 Cisco VIC를 설치할 수 있으므로 I/O 확장성이 향상됩니다.



Cisco UCS VIC 1387 어댑터에 대한 자세한 내용은 를 참조하십시오 "Cisco UCS 가상 인터페이스 카드 1387" 데이터 시트.

- * CVR-QSFP-SFP 10G 어댑터 *

  Cisco QSA 모듈은 QSFP 포트를 SFP 또는 SFP+ 포트로 변환합니다. 이 어댑터를 사용하는 고객은 SFP+ 또는 SFP 모듈 또는 케이블을 사용하여 네트워크의 다른 쪽 끝에 있는 저속 포트에 연결할 수 있습니다. 이러한 유연성 덕분에 고밀도 40GbE QSFP 플랫폼의 사용을 극대화하여 40GbE로 비용 효율적으로 전환할 수 있습니다. 이 어댑터는 모든 SFP+ 광학 및 케이블 연결 장치를 지원하며 여러 1GbE SFP 모듈을 지원합니다. 이 프로젝트는 10GbE 연결을 사용하여 검증되었으며 VIC 1387이 40GbE이기 때문에 다음 그림에 나와 있는 CVR-QSFP-SFP SFP 10G 어댑터가 변환에 사용됩니다.



VMware vSphere 6.7을 참조하십시오

VMware vSphere 6.7은 FlexPod Express와 함께 사용할 수 있는 하나의 하이퍼바이저 옵션입니다. VMware vSphere를 사용하면 구입한 컴퓨팅 용량을 최대한 활용하는 동시에 전력 및 냉각 설치 공간을 줄일 수 있습니다. 또한 VMware vSphere를 사용하면 vSphere 호스트 클러스터(VMware Distributed Resource Scheduler 또는 VMware DRS)에서 하드웨어 장애 보호(VMware High Availability 또는 VMware HA)와 컴퓨팅 리소스 로드 밸런싱을 수행할 수 있습니다.

VMware vSphere 6.7은 커널만 다시 시작하므로 고객은 하드웨어를 다시 시작하지 않고 vSphere ESXi를 로드하는 "빠른 부팅"을 수행할 수 있습니다. 이 기능은 빠른 부팅 허용 목록에 있는 플랫폼 및 드라이버에서만 사용할 수

있습니다. vSphere 6.7은 vSphere Web Client의 기능 중 약 90%를 수행할 수 있는 vSphere Client의 기능을 확장합니다.

vSphere 6.7에서 VMware는 고객이 호스트 단위가 아닌 VM(가상 머신)별로 EVC(Enhanced vMotion Compatibility)를 설정할 수 있도록 이 기능을 확장했습니다. vSphere 6.7에서 VMware는 즉각적인 클론을 생성하는 데 사용할 수 있는 API도 공개했습니다.

다음은 vSphere 6.7 U1의 몇 가지 기능입니다.

- HTML5 웹 기반 vSphere Client의 모든 기능을 갖추고 있습니다
- vMotion을 사용하여 NVIDIA GRID vGPU VM을 지원합니다. 인텔 FPGA 지원.
- vCenter Server Converge Tool을 사용하여 외부 PSC에서 내부 PC로 이동합니다.
- vSAN(HCI 업데이트)의 향상된 기능.
- 향상된 콘텐츠 라이브러리.

vSphere 6.7 U1에 대한 자세한 내용은 을 참조하십시오 "vCenter Server 6.7 업데이트 1의 새로운 기능". 이 솔루션은 vSphere 6.7에서 검증되었지만 NetApp Interoperability Matrix Tool에 의해 다른 구성 요소와 함께 검증된 모든 vSphere 버전을 지원합니다. 수정 및 향상된 기능을 위해 vSphere 6.7U1을 구축하는 것이 좋습니다.

부트 아키텍처

다음은 FlexPod 익스프레스 부트 아키텍처에서 지원되는 옵션입니다.

- iSCSI SAN LUN 을 선택합니다
- Cisco FlexFlash SD 카드
- 로컬 디스크

FlexPod 데이터 센터는 iSCSI LUN에서 부팅되므로 FlexPod 익스프레스에 iSCSI 부트를 사용하여 솔루션 관리성이 향상됩니다.

"다음: 솔루션 검증."

솔루션 검증

Cisco와 NetApp은 고객을 위한 최고의 인프라 플랫폼 역할을 할 수 있도록 FlexPod Express를 설계 및 구축했습니다. 업계 최고의 구성 요소로 설계되었기 때문에 고객은 FlexPod Express를 인프라 기반으로 신뢰할 수 있습니다. FlexPod 포트폴리오의 기본 원칙에 따라 FlexPod Express 아키텍처는 Cisco 및 NetApp 데이터 센터 설계자와 엔지니어가 철저히 테스트했습니다. 중복성 및 가용성부터 개별 기능에 이르기까지 전체 FlexPod Express 아키텍처는 고객에 대한 신뢰를 유지하고 설계 프로세스에 대한 신뢰를 구축하는 것으로 검증되었습니다.

VMware vSphere 6.7은 FlexPod Express 인프라스트럭처 구성 요소에서 검증되었습니다. 이 검증에는 하이퍼바이저를 위한 10GbE 업링크 연결 옵션이 포함되었습니다.

"다음: 결론."

결론

FlexPod Express는 업계 최고의 구성요소를 사용하는 검증된 설계를 통해 간단하고 효율적인 솔루션을 제공합니다. FlexPod Express는 하이퍼바이저 플랫폼을 위한 옵션을 제공하고 확장하여 특정 비즈니스 요구에 맞게 조정할 수 있습니다. FlexPod Express는 중소 및 중견 기업, 원격 사무소, 지사 및 전용 솔루션이 필요한 기타 기업을 염두에 두고 설계되었습니다.

"다음: 추가 정보를 찾을 위치."

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대한 자세한 내용은 다음 문서 및 웹 사이트를 참조하십시오.

- NetApp 설명서

  "https://docs.netapp.com"

- FlexPod Express with VMware vSphere 6.7 및 NetApp AFF A220 구축 가이드 를 참조하십시오

  "https://www.netapp.com/us/media/nva-1123-deploy.pdf"

FlexPod Express with Cisco UCS C-Series and AFF A220 Series 구축 가이드 를 참조하십시오

NVA-1123-deploy:FlexPod Express with VMware vSphere 6.7 and NetApp AFF A220 구축 가이드

Savita Kumari, NetApp에서 기술 지원

파트너 후원: 

업계 동향에 따르면 많은 데이터 센터가 공유 인프라 및 클라우드 컴퓨팅으로 전환하고 있습니다. 또한 기업에서는 데이터 센터에 친숙한 기술을 활용하여 원격 사무소 및 지사를 위한 간편하고 효율적인 솔루션을 찾고 있습니다.

FlexPod Express는 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 스위치 제품군, NetApp 스토리지 기술을 기반으로 사전 설계되고 모범 사례 데이터 센터 아키텍처입니다. FlexPod 익스프레스 시스템의 구성요소는 FlexPod 데이터 센터와 비슷하기 때문에 더 작은 규모로 전체 IT 인프라 환경에서 관리 시너지 효과를 실현할 수 있습니다. FlexPod 데이터 센터 및 FlexPod 익스프레스는 가상화 및 베어 메탈 운영 체제 및 엔터프라이즈 워크로드를 위한 최적의 플랫폼입니다.

FlexPod 데이터 센터 및 FlexPod 익스프레스는 기본 구성을 제공하며 다양한 사용 사례 및 요구 사항을 수용할 수 있도록 크기를 조정할 수 있는 유연성을 갖추고 있습니다. 기존 FlexPod 데이터 센터 고객은 익숙한 툴을 사용하여 FlexPod 익스프레스 시스템을 관리할 수 있습니다. 새로운 FlexPod Express 고객은 환경 확장에 따라 FlexPod 데이터 센터 관리에 쉽게 적응할 수 있습니다.

FlexPod Express는 원격 사무소, 지점 및 중소기업을 위한 최적의 인프라 기반입니다. 전용 워크로드에 대한 인프라를 제공하려는 고객에게 최적의 솔루션입니다.

FlexPod Express는 거의 모든 워크로드에 적합한 관리하기 쉬운 인프라를 제공합니다.

솔루션 개요

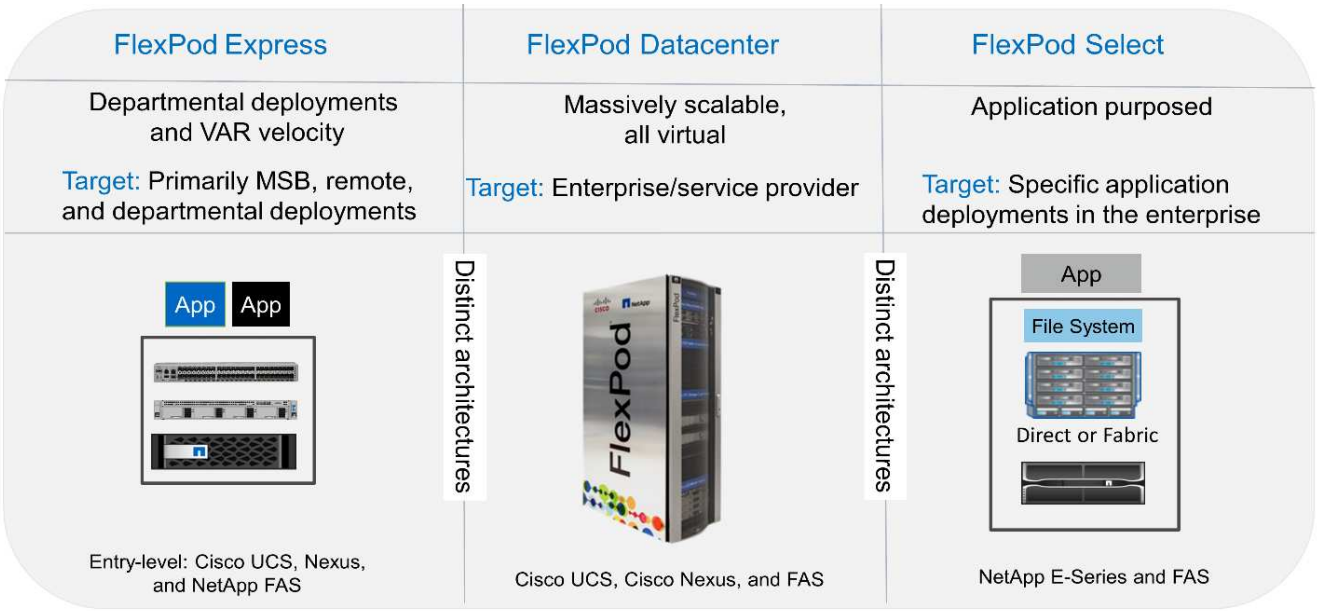
이 FlexPod 익스프레스 솔루션은 FlexPod 통합 인프라 프로그램의 일부입니다.

FlexPod 통합 인프라 프로그램

FlexPod 참조 아키텍처는 CVD(Cisco Validated Design) 또는 NVA(NetApp Verified Architecture)로 제공됩니다. 지정된 CVD 또는 NVA의 고객 요구 사항에 따른 편차는 이러한 변형으로 지원되지 않는 구성이 생성되지는 않을 경우 허용됩니다.

아래 그림과 같이 FlexPod 프로그램에는 FlexPod 익스프레스, FlexPod 데이터 센터, FlexPod 선택의 세 가지 솔루션이 포함되어 있습니다.

- * FlexPod 익스프레스. * 는 Cisco 및 NetApp의 기술을 갖춘 엔트리 레벨 솔루션을 고객에게 제공합니다.
- * FlexPod 데이터 센터 * 는 다양한 워크로드 및 애플리케이션을 위한 최적의 다목적 토대를 제공합니다.
- * FlexPod 선택. * FlexPod 데이터 센터의 최고 기능을 통합하고 특정 애플리케이션에 맞게 인프라를 조정합니다.



NetApp 검증 아키텍처 프로그램

NetApp 검증 아키텍처 프로그램에서는 NetApp 솔루션을 위한 검증된 아키텍처를 고객에게 제공합니다. NetApp 검증 아키텍처는 다음과 같은 품질의 NetApp 솔루션 아키텍처를 제공합니다.

- 철저한 테스트를 거친 아키텍처

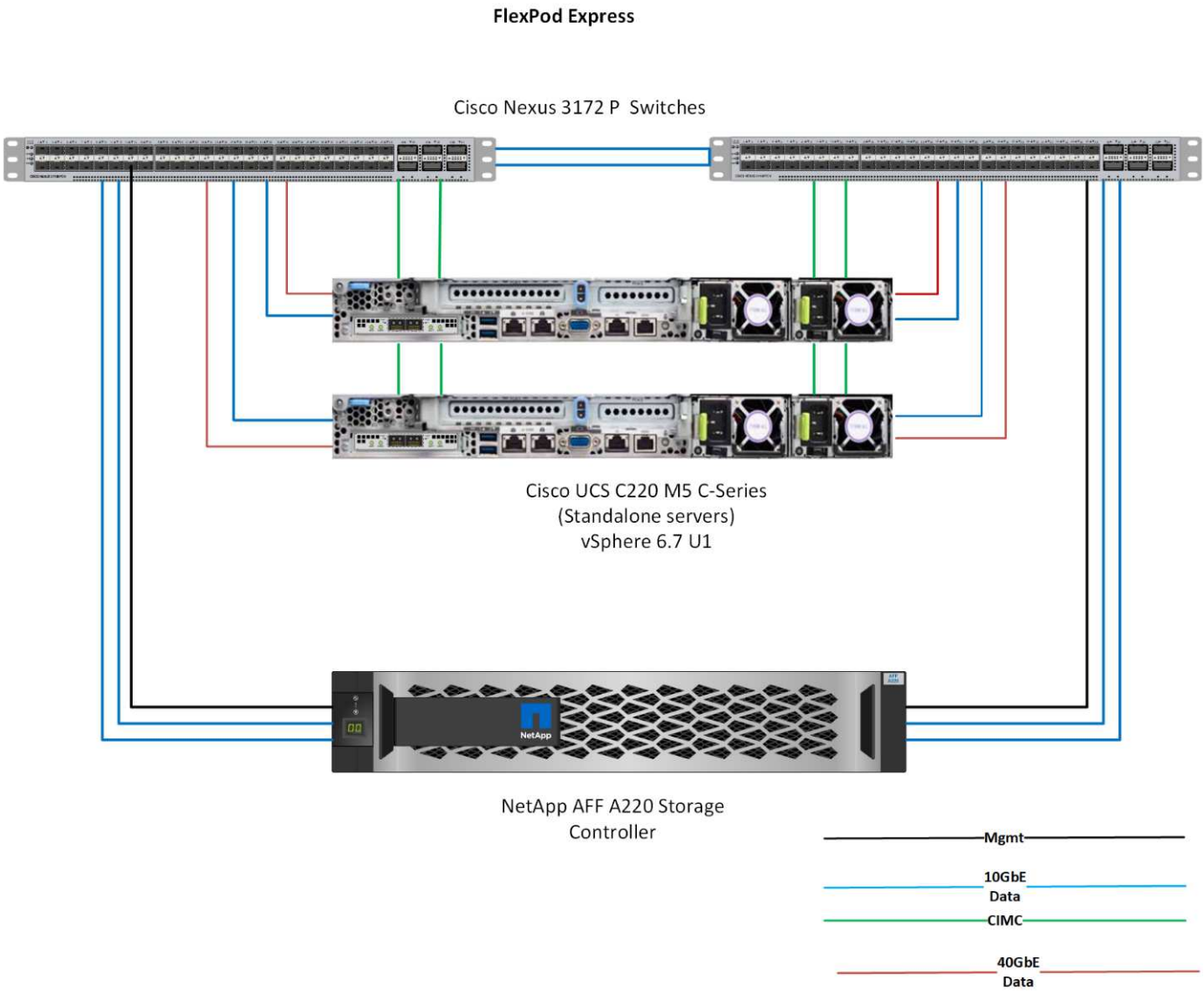
- 기본적으로 규범적인 아키텍처
- 구축 위험 최소화
- 출시 시기를 단축합니다

이 가이드에서는 VMware vSphere를 사용한 FlexPod Express 설계에 대해 자세히 설명합니다. 또한, 이 설계는 NetApp ONTAP 9.4, Cisco Nexus 3172P, Cisco UCS C-Series C220 M5 서버를 하이퍼바이저 노드로 실행하는 완전히 새로운 AFF A220 시스템을 사용합니다.

솔루션 기술

이 솔루션은 NetApp, Cisco 및 VMware의 최신 기술을 활용합니다. 이 솔루션에는 ONTAP 9.4, 이중 Cisco Nexus 3172P 스위치 및 VMware vSphere 6.7을 실행하는 Cisco UCS C220 M5 랙 서버를 실행하는 새로운 NetApp AFF A220이 포함되어 있습니다. 이 검증된 솔루션은 10GbE 기술을 사용합니다. 또한 FlexPod 익스프레스 아키텍처가 조직의 변화하는 비즈니스 요구에 적응할 수 있도록 한 번에 두 개의 하이퍼바이저 노드를 추가하여 컴퓨팅 용량을 확장하는 방법에 대한 지침도 제공됩니다.

다음 그림에서는 VMware vSphere 10GbE 아키텍처를 사용하는 FlexPod Express를 보여 줍니다.



이 검증에서는 10GbE 연결과 40GbE의 Cisco UCS VIC 1387을 사용합니다. 10GbE 연결을 위해 CVR-QSFP-SFP-SFP 10G 어댑터가 사용됩니다.

사용 사례 요약

FlexPod 익스프레스 솔루션은 다음과 같은 여러 사용 사례에 적용할 수 있습니다.

- 원격 사무소 및 지사
- 중소기업
- 비용 효율적인 전용 솔루션이 필요한 환경

FlexPod Express는 가상화된 혼합 워크로드에 가장 적합합니다.

이 솔루션은 vSphere 6.7에서 검증되었지만 NetApp Interoperability Matrix Tool에 의해 다른 구성 요소와 함께 검증된 모든 vSphere 버전을 지원합니다. 수정 및 향상된 기능을 위해 vSphere 6.7U1을 구축하는 것이 좋습니다.

다음은 vSphere 6.7 U1의 몇 가지 기능입니다.

- HTML5 웹 기반 vSphere Client의 모든 기능을 갖추고 있습니다
- vMotion을 사용하여 NVIDIA GRID vGPU VM을 지원합니다. 인텔 FPGA 지원
- vCenter Server Converge Tool을 사용하여 외부 PSC에서 내부 PC로 이동합니다
- vSAN(HCI 업데이트) 기능 향상
- 향상된 콘텐츠 라이브러리

vSphere 6.7 U1에 대한 자세한 내용은 을 참조하십시오 "vCenter Server 6.7 업데이트 1의 새로운 기능".

기술 요구 사항

FlexPod 익스프레스 시스템에는 하드웨어 및 소프트웨어 구성 요소의 조합이 필요합니다. 또한 FlexPod Express는 하이퍼바이저 노드를 시스템에 추가하는 데 필요한 하드웨어 구성요소를 2개 단위로 설명합니다.

하드웨어 요구 사항

선택한 하이퍼바이저에 관계없이 모든 FlexPod Express 구성은 동일한 하드웨어를 사용합니다. 따라서 비즈니스 요구사항이 변경되더라도 두 하이퍼바이저 중 하나를 동일한 FlexPod Express 하드웨어에서 실행할 수 있습니다.

다음 표에는 모든 FlexPod Express 구성에 필요한 하드웨어 구성요소가 나와 있습니다.

하드웨어	수량
AFF A220 HA 쌍	1
Cisco C220 M5 서버	2
Cisco Nexus 3172P 스위치	2

하드웨어	수량
C220 M5 서버용 Cisco UCS 가상 인터페이스 카드(VIC) 1387	2
CVR-QSFP-SFP 10G 어댑터	4

다음 표에는 10GbE 구현을 위한 기본 구성 외에 필요한 하드웨어가 나와 있습니다.

하드웨어	수량
Cisco UCS C220 M5 서버	2
Cisco VIC 1387	2
CVR-QSFP-SFP 10G 어댑터	4

소프트웨어 요구 사항

다음 표에는 FlexPod Express 솔루션의 아키텍처를 구현하는 데 필요한 소프트웨어 구성 요소가 나열되어 있습니다.

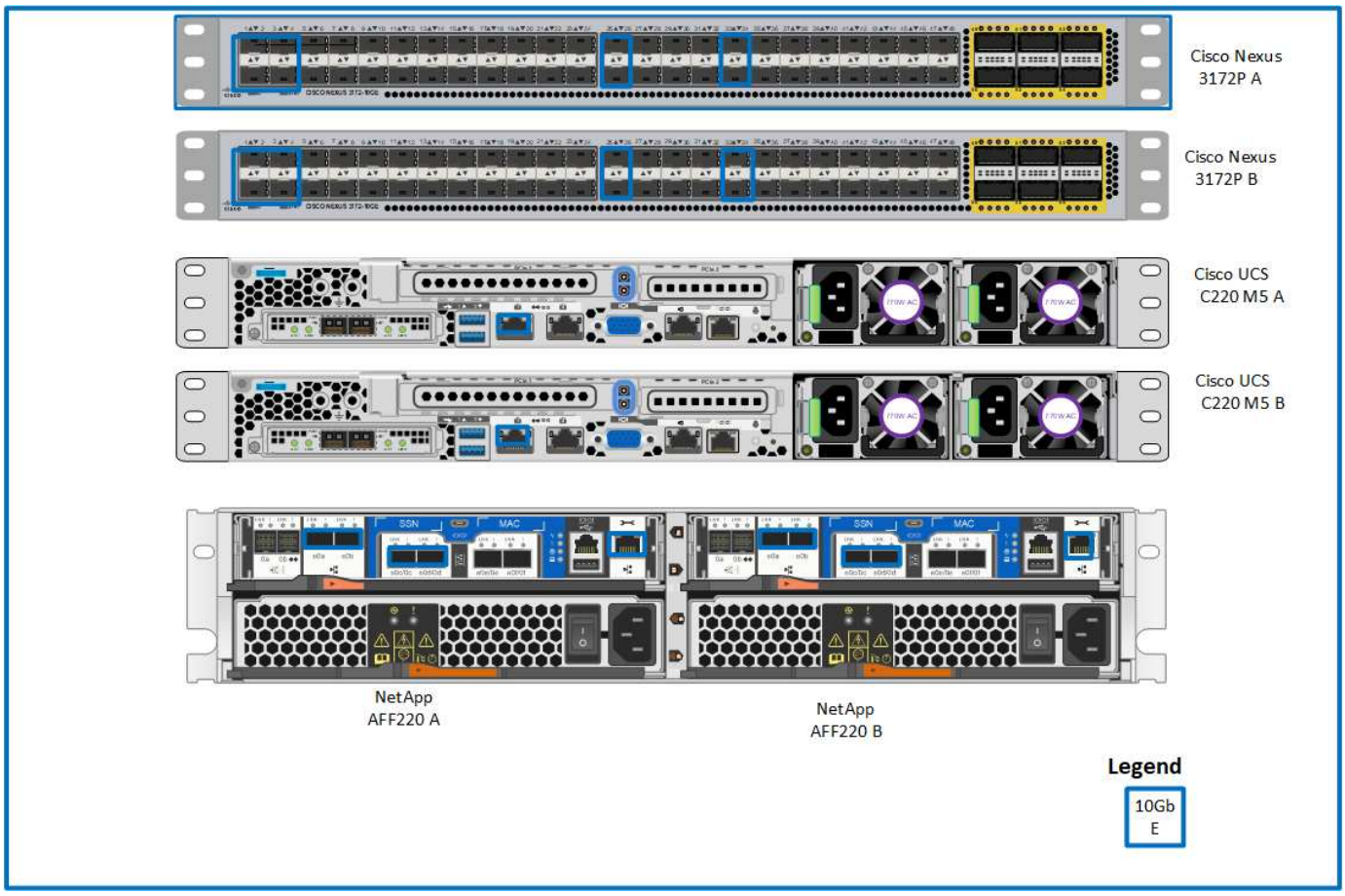
소프트웨어	버전	세부 정보
CIMC(Cisco Integrated Management Controller)	3.1(3G)	Cisco UCS C220 M5 랙 서버용
Cisco nenic 드라이버	1.0.25.0	VIC 1387 인터페이스 카드의 경우
Cisco NX-OS입니다	nxos.7.0.3.I7.5.bin	Cisco Nexus 3172P 스위치용
NetApp ONTAP를 참조하십시오	9.4	AFF A220 컨트롤러

다음 표에는 FlexPod Express의 모든 VMware vSphere 구축에 필요한 소프트웨어가 나와 있습니다.

소프트웨어	버전
VMware vCenter Server 어플라이언스	6.7
VMware vSphere ESXi 하이퍼바이저	6.7
ESXi용 NetApp VAAI 플러그인	1.1.2

FlexPod Express 케이블링 정보

다음 그림은 참조 검증 케이블 연결을 보여 줍니다.



다음 표에서는 Cisco Nexus 스위치 3172P A 의 케이블 연결 정보를 보여 줍니다

로컬 장치	로컬 포트	원격 장치	원격 포트
Cisco Nexus 스위치 3172P A	eth1/1	NetApp AFF A220 스토리지 컨트롤러 A입니다	e0c
	eth1/2	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0c
	eth1/3	Cisco UCS C220 C-Series 독립 실행형 서버 A	CVR-QSFP-SFP 10G 어댑터가 있는 MLOM1
	eth1/4	Cisco UCS C220 C-Series 독립 실행형 서버 B	CVR-QSFP-SFP 10G 어댑터가 있는 MLOM1
	eth1/25	Cisco Nexus 스위치 3172P B	eth1/25
	Eth1/26	Cisco Nexus 스위치 3172P B	Eth1/26
	Eth1/33	NetApp AFF A220 스토리지 컨트롤러 A입니다	e0M
	eth1/34	Cisco UCS C220 C-Series 독립 실행형 서버 A	CIMC를 참조하십시오

다음 표에서는 Cisco Nexus 스위치 3172P B 의 케이블 연결 정보를 보여 줍니다

로컬 장치	로컬 포트	원격 장치	원격 포트
Cisco Nexus 스위치 3172P B	eth1/1	NetApp AFF A220 스토리지 컨트롤러 A입니다	e0d
	eth1/2	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0d
	eth1/3	Cisco UCS C220 C-Series 독립 실행형 서버 A	CVR-QSFP-SFP 10G 어댑터가 포함된 MLOM2
	eth1/4	Cisco UCS C220 C-Series 독립 실행형 서버 B	CVR-QSFP-SFP 10G 어댑터가 포함된 MLOM2
	eth1/25	Cisco Nexus 스위치 3172P A	eth1/25
	Eth1/26	Cisco Nexus 스위치 3172P A	Eth1/26
	Eth1/33	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0M
	eth1/34	Cisco UCS C220 C-Series 독립 실행형 서버 B	CIMC를 참조하십시오

다음 표에서는 NetApp AFF A220 스토리지 컨트롤러 A의 케이블 연결 정보를 보여 줍니다

로컬 장치	로컬 포트	원격 장치	원격 포트
NetApp AFF A220 스토리지 컨트롤러 A입니다	e0a	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0a
	e0b	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0b
	e0c	Cisco Nexus 스위치 3172P A	eth1/1
	e0d	Cisco Nexus 스위치 3172P B	eth1/1
	e0M	Cisco Nexus 스위치 3172P A	Eth1/33

다음 표에서는 NetApp AFF A220 스토리지 컨트롤러 B의 케이블 연결 정보를 보여 줍니다

로컬 장치	로컬 포트	원격 장치	원격 포트
NetApp AFF A220 스토리지 컨트롤러 B입니다	e0a	NetApp AFF A220 스토리지 컨트롤러 A입니다	e0a
	e0b	NetApp AFF A220 스토리지 컨트롤러 A입니다	e0b
	e0c	Cisco Nexus 스위치 3172P A	eth1/2
	e0d	Cisco Nexus 스위치 3172P B	eth1/2

로컬 장치	로컬 포트	원격 장치	원격 포트
	e0M	Cisco Nexus 스위치 3172P B	Eth1/33

구현 절차

이 문서에서는 완전히 이중화된 고가용성 FlexPod Express 시스템을 구성하는 방법에 대해 자세히 설명합니다. 이러한 이중화를 반영하기 위해 각 단계에서 구성 요소를 구성 요소 A 또는 구성 요소 B라고 합니다 예를 들어 컨트롤러 A와 컨트롤러 B는 이 문서에 프로비저닝된 NetApp 스토리지 컨트롤러 2개를 식별합니다. 스위치 A와 스위치 B는 Cisco Nexus 스위치 쌍을 나타냅니다.

또한 서버 A, 서버 B 등으로 순차적으로 구분되는 여러 Cisco UCS 호스트를 프로비저닝하는 단계도 설명합니다.

사용자 환경과 관련된 정보를 단계별로 포함해야 함을 나타내기 위해 명령 구조의 일부로 '<<text>>'이 표시됩니다. 'VLAN create' 명령은 다음 예를 참조하십시오.

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

이 문서를 사용하여 FlexPod Express 환경을 완전히 구성할 수 있습니다. 이 프로세스에서 다양한 단계를 수행하려면 고객별 명명 규칙, IP 주소 및 VLAN(Virtual Local Area Network) 스키마를 삽입해야 합니다. 아래 표에는 이 가이드에 설명된 대로 구축에 필요한 VLAN이 설명되어 있습니다. 이 표는 특정 사이트 변수를 기반으로 완료할 수 있으며 문서 구성 단계를 구현하는 데 사용할 수 있습니다.

별도의 대역내 및 대역외 관리 VLAN을 사용하는 경우 이러한 VLAN 간에 레이어 3 경로를 만들어야 합니다. 이 검증에서는 공통 관리 VLAN이 사용되었습니다.

이름	**VLAN**의 용도	이 문서의 유효성을 검사하는 데 사용되는 **ID**입니다
관리 VLAN	관리 인터페이스용 VLAN	3437
네이티브 VLAN	태그가 지정되지 않은 프레임이 할당되는 VLAN입니다	2
NFS VLAN	NFS 트래픽용 VLAN	3438
VMware vMotion VLAN	하나의 물리적 호스트에서 다른 물리적 호스트로 가상 시스템을 이동할 수 있도록 지정된 VLAN입니다	3441
가상 머신 트래픽 VLAN	가상 머신 애플리케이션 트래픽용 VLAN	3442
iSCSI-A-VLAN	패브릭 A의 iSCSI 트래픽용 VLAN	3439
iSCSI-B-VLAN	패브릭 B의 iSCSI 트래픽용 VLAN	3440

FlexPod Express를 구성하는 동안 VLAN 번호가 필요합니다. VLAN은 "<<var_xxxx_vlan>>"라고 하며, 여기서 "xxxx"는 VLAN의 목적(예: iSCSI-A)입니다.

아래 표에는 생성된 VMware 가상 머신이 나와 있습니다.

가상 머신 설명입니다	호스트 이름입니다
VMware vCenter Server를 참조하십시오	

Cisco Nexus 3172P 구축 절차

다음 섹션에서는 FlexPod 익스프레스 환경에 사용되는 Cisco Nexus 3172P 스위치 구성에 대해 자세히 설명합니다.

Cisco Nexus 3172P 스위치의 초기 설정

다음 절차에서는 기본 FlexPod Express 환경에서 사용할 Cisco Nexus 스위치를 구성하는 방법에 대해 설명합니다.

> 이 절차에서는 NX-OS 소프트웨어 릴리즈 7.0(3) i7(5)을 실행하는 Cisco Nexus 3172P를 사용하고 있다고 가정합니다.

1. 초기 부팅이 완료되고 스위치의 콘솔 포트에 연결되면 Cisco NX-OS 설정이 자동으로 시작됩니다. 이 초기 구성에서는 스위치 이름, mgmt0 인터페이스 구성, SSH(Secure Shell) 설정과 같은 기본 설정을 지정합니다.
2. FlexPod 익스프레스 관리 네트워크는 여러 가지 방법으로 구성할 수 있습니다. 3172P 스위치의 mgmt0 인터페이스를 기존 관리 네트워크에 연결할 수도 있고, 3172P 스위치의 mgmt0 인터페이스를 연속 연결 구성으로 연결할 수도 있습니다. 하지만 이 링크는 SSH 트래픽과 같은 외부 관리 액세스에 사용할 수 없습니다.

   이 구축 가이드에서는 FlexPod 익스프레스 Cisco Nexus 3172P 스위치를 기존 관리 네트워크에 연결합니다.
3. Cisco Nexus 3172P 스위치를 구성하려면 스위치의 전원을 켠 후 여기 에 나온 것처럼 화면 메시지에 따라 두 스위치를 초기 설정하고 스위치 관련 정보에 적절한 값을 대체하십시오.

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
  Enter the switch name : 3172P-B
  Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
    Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
    Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
  Configure advanced IP options? (yes/no) [n]: n
  Enable the telnet service? (yes/no) [n]: n
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
    Number of rsa key bits <1024-2048> [1024]:  <enter>
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_ntp_ip>>
  Configure default interface layer (L3/L2) [L2]: <enter>
  Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:  <enter>
```

4. 그러면 구성 요약이 표시됩니다. 구성을 편집할지 묻는 메시지가 나타납니다. 구성이 올바르면 n을 입력합니다.

```
Would you like to edit the configuration? (yes/no) [n]: n
```

5. 그런 다음 이 구성을 사용하고 저장할지 묻는 메시지가 표시됩니다. 그렇다면 y를 입력합니다.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Cisco Nexus 스위치 B에 대해 이 절차를 반복합니다

고급 기능을 활성화합니다

추가 구성 옵션을 제공하려면 Cisco NX-OS에서 특정 고급 기능을 사용하도록 설정해야 합니다.

> interface-vlan 기능은 본 문서 전반에 걸쳐 설명한 back-to-back mgmt0 옵션을 사용하는 경우에만 필요합니다. 이 기능을 사용하면 IP 주소를 인터페이스 VLAN(스위치 가상 인터페이스)에 할당하여 SSH를 통해 스위치에 대한 대역 내 관리 통신을 사용할 수 있습니다.

1. Cisco Nexus 스위치 A와 스위치 B에서 적절한 기능을 활성화하려면 '(config t)' 명령을 사용하여 구성 모드를 시작하고 다음 명령을 실행하십시오.

```
feature interface-vlan
feature lacp
feature vpc
```

   기본 포트 채널 로드 밸런싱 해쉬는 소스 및 타깃 IP 주소를 사용하여 포트 채널의 인터페이스에 대한 로드 밸런싱 알고리즘을 결정합니다. 소스 및 타깃 IP 주소보다 많은 입력을 해쉬 알고리즘에 제공하면 포트 채널 멤버 전체에 걸쳐 더 효율적으로 분산될 수 있습니다. 동일한 이유로 소스 및 타깃 TCP 포트를 해쉬 알고리즘에 추가하는 것이 좋습니다.

2. 구성 모드('config t')에서 다음 명령을 입력하여 Cisco Nexus 스위치 A 및 스위치 B의 글로벌 포트 채널 로드 밸런싱 구성을 설정하십시오.

```
port-channel load-balance src-dst ip-l4port
```

글로벌 스패닝 트리 구성을 수행합니다

Cisco Nexus 플랫폼은 브리지 보장이라는 새로운 보호 기능을 사용합니다. 브리지 보장은 스패닝 트리 알고리즘을 더 이상 실행하지 않는 장치에서 데이터 트래픽을 계속 전달하는 단방향 링크 또는 기타 소프트웨어 장애를 방지합니다. 플랫폼에 따라 네트워크 또는 가장자리를 포함한 여러 상태 중 하나에 포트를 배치할 수 있습니다.

기본적으로 모든 포트가 네트워크 포트로 간주되도록 브리지 보장을 설정하는 것이 좋습니다. 이 설정은 네트워크 관리자가 각 포트의 구성을 검토하도록 합니다. 또한 확인되지 않은 에지 포트 또는 브리지 보장 기능이 활성화되지 않은 인접 장치와 같은 가장 일반적인 구성 오류도 표시됩니다. 또한 스패닝 트리에서 너무 적은 포트가 아니라 많은 포트를 차단하는 편이 더 안전합니다. 그러면 기본 포트 상태를 통해 네트워크의 전반적인 안정성을 향상할 수 있습니다.

특히 브리지 보장을 지원하지 않는 서버, 스토리지 및 업링크 스위치를 추가할 때는 스패닝 트리 상태에 세심한 주의를 기울여야 합니다. 이러한 경우 포트를 활성화하려면 포트 유형을 변경해야 할 수 있습니다.

브리지 프로토콜 데이터 단위(BPDU) 보호대는 기본적으로 다른 보호 계층으로 에지 포트에서 활성화됩니다. 네트워크의 루프를 방지하기 위해 이 기능은 다른 스위치의 BPDU가 이 인터페이스에 표시되는 경우 포트를 종료합니다.

구성 모드('config t')에서 다음 명령을 실행하여 Cisco Nexus 스위치 A 및 스위치 B에서 기본 포트 유형과 BPDU 가드를 포함한 기본 스패닝 트리 옵션을 구성하십시오.

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

VLAN을 정의합니다

VLAN이 서로 다른 개별 포트를 구성하기 전에 스위치에서 계층 2 VLAN을 정의해야 합니다. 향후 문제 해결이 용이하도록 VLAN 이름을 지정하는 것도 좋은 방법입니다.

구성 모드('config t')에서 다음 명령을 실행하여 Cisco Nexus 스위치 A 및 스위치 B의 계층 2 VLAN을 정의하고 설명하십시오.

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

액세스 및 관리 포트 설명을 구성합니다

계층 2 VLAN에 이름을 할당하는 경우와 마찬가지로, 모든 인터페이스에 대한 설정 설명은 프로비저닝과 문제 해결에 도움이 될 수 있습니다.

각 스위치의 구성 모드('config t')에서 FlexPod Express 대규모 구성에 대한 다음 포트 설명을 입력합니다.

Cisco Nexus 스위치 **A**

```
int eth1/1
  description AFF A220-A e0c
int eth1/2
  description AFF A220-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0
int eth1/4
  description UCS-Server-B: MLOM port 0
int eth1/25
  description vPC peer-link 3172P-B 1/25
int eth1/26
  description vPC peer-link 3172P-B 1/26
int eth1/33
  description AFF A220-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Cisco Nexus 스위치 **B**

```
int eth1/1
  description AFF A220-A e0d
int eth1/2
  description AFF A220-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 1
int eth1/4
  description UCS-Server-B: MLOM port 1
int eth1/25
  description vPC peer-link 3172P-A 1/25
int eth1/26
  description vPC peer-link 3172P-A 1/26
int eth1/33
  description AFF A220-B e0M
int eth1/34
  description UCS Server B: CIMC
```

서버 및 스토리지 관리 인터페이스를 구성합니다

서버와 스토리지 모두의 관리 인터페이스는 일반적으로 단일 VLAN만 사용합니다. 따라서 관리 인터페이스 포트를 액세스 포트로 구성합니다. 각 스위치에 대한 관리 VLAN을 정의하고 스패닝 트리 포트 유형을 에지로 변경합니다.

구성 모드('config t')에서 다음 명령을 입력하여 서버와 스토리지 모두의 관리 인터페이스에 대한 포트 설정을 구성하십시오.

Cisco Nexus 스위치 **A**

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Cisco Nexus 스위치 **B**

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

가상 포트 채널 글로벌 구성을 수행합니다

가상 포트 채널(vPC)을 사용하면 물리적으로 두 개의 서로 다른 Cisco Nexus 스위치에 연결된 링크가 세 번째 장치에 단일 포트 채널로 표시될 수 있습니다. 세 번째 장치는 스위치, 서버 또는 다른 네트워킹 장치일 수 있습니다. vPC는 계층 2 다중 경로를 제공할 수 있으므로 대역폭을 높이고, 노드 간에 여러 개의 병렬 경로를 활성화하고, 대체 경로가 있는 로드 밸런싱 트래픽을 통해 이중화를 생성할 수 있습니다.

vPC는 다음과 같은 이점을 제공합니다.

- 단일 장치에서 두 업스트림 장치에 걸쳐 포트 채널을 사용하도록 설정
- 스패닝 트리 프로토콜 차단 포트 제거
- 루프 없는 토폴로지 제공
- 사용 가능한 모든 업링크 대역폭 사용
- 링크 또는 디바이스에 장애가 발생할 경우 빠른 컨버전스를 제공합니다
- 링크 레벨의 복원력 제공
- 고가용성 제공 지원

vPC 기능이 제대로 작동하려면 두 Cisco Nexus 스위치 간의 몇 가지 초기 설정이 필요합니다. 연속 인접 mgmt0 구성을 사용하는 경우에는 인터페이스에 정의된 주소를 사용하고 ping을 사용하여 통신 가능 여부를 확인해야 합니다[switch_A/B_mgmt0_ip_addr]VRF 관리 명령어

구성 모드('config t')에서 다음 명령을 실행하여 두 스위치에 대한 vPC 글로벌 구성을 설정하십시오.

Cisco Nexus 스위치 **A**

```
vpc domain 1
 role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

Cisco Nexus 스위치 B

```
vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25- 26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

스토리지 포트 채널을 구성합니다

NetApp 스토리지 컨트롤러는 LACP(Link Aggregation Control Protocol)를 사용하여 네트워크에 대해 active-active 연결을 허용합니다. LACP 사용이 선호되는 이유는 LACP가 스위치 간에 협상과 로깅을 모두 추가하기 때문입니다. 네트워크가 vPC에 맞게 설정되므로 이 접근 방식을 통해 스토리지에서 별도의 물리적 스위치로의 active-active 연결을 설정할 수 있습니다. 각 컨트롤러에는 각 스위치에 대한 링크가 2개 있습니다. 그러나 4개의 링크 모두 동일한 vPC 및 인터페이스 그룹(IFGRP)에 속합니다.

구성 모드('config t')에서 각 스위치에 대해 다음 명령을 실행하여 개별 인터페이스를 구성하고 NetApp AFF 컨트롤러에 연결된 포트에 대한 결과 포트 채널 구성을 설정하십시오.

1. 스위치 A와 스위치 B에서 다음 명령을 실행하여 스토리지 컨트롤러 A의 포트 채널을 구성합니다.

```
int eth1/1
  channel-group 11 mode active
int Po11
  description vPC to Controller-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11
  no shut
```

2. 스위치 A와 스위치 B에서 다음 명령을 실행하여 스토리지 컨트롤러 B의 포트 채널을 구성합니다

```
int eth1/2
  channel-group 12 mode active
int Po12
  description vPC to Controller-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
  no shut
exit
copy run start
```



이 솔루션 검증에서 MTU 9000이 사용되었습니다. 그러나 애플리케이션 요구 사항에 따라 MTU의 적절한 값을 구성할 수 있습니다. FlexPod 솔루션에서 동일한 MTU 값을 설정하는 것이 중요합니다. 구성 요소 간의 MTU 구성이 잘못되면 패킷이 손실되고 이러한 패킷이 생성됩니다.

서버 연결을 구성합니다

Cisco UCS 서버에는 데이터 트래픽과 iSCSI를 사용한 ESXi 운영 체제 부팅에 사용되는 2포트 가상 인터페이스 카드 VIC1387이 있습니다. 이러한 인터페이스는 서로 간에 페일오버되도록 구성되어 단일 링크를 넘어 추가적인 이중화를 제공합니다. 이러한 링크를 여러 스위치에 걸쳐 분산하면 완전한 스위치 장애가 발생해도 서버가 가동 상태를 유지할 수 있습니다.

구성 모드('config t')에서 다음 명령을 실행하여 각 서버에 연결된 인터페이스에 대한 포트 설정을 구성합니다.

Cisco Nexus 스위치 **A: Cisco UCS** 서버 **A** 및 **Cisco UCS** 서버 **B** 구성

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu9216
  no shut
exit
copy run start
```

Cisco Nexus 스위치 **B: Cisco UCS** 서버 **A** 및 **Cisco UCS** 서버 **B** 구성

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

이 솔루션 검증에서 MTU 9000이 사용되었습니다. 그러나 애플리케이션 요구 사항에 따라 MTU의 적절한 값을 구성할 수 있습니다. FlexPod 솔루션에서 동일한 MTU 값을 설정하는 것이 중요합니다. 구성 요소 간의 MTU 구성이 잘못되면 패킷이 손실되고 이러한 패킷은 다시 전송되어야 합니다. 이 문제는 솔루션의 전반적인 성능에 영향을 줍니다.

Cisco UCS 서버를 추가하여 솔루션을 확장하거나, 스위치 A 및 B에서 새로 추가한 서버가 연결된 스위치 포트를 사용하여 이전 명령을 실행합니다

기존 네트워크 인프라로 업링크

사용 가능한 네트워크 인프라에 따라 여러 가지 방법과 기능을 사용하여 FlexPod 환경을 업링크할 수 있습니다. 기존 Cisco Nexus 환경이 존재하는 경우, NetApp은 vPC를 사용하여 FlexPod 환경에 포함된 Cisco Nexus 3172P 스위치를 인프라로 업링크하는 것을 권장합니다. 업링크는 10GbE 인프라스트럭처 솔루션의 경우 10GbE 업링크 또는 필요한 경우 1GbE 인프라스트럭처 솔루션의 경우 1GbE일 수 있습니다. 앞서 설명한 절차를 사용하여 기존 환경에 대한 업링크 vPC를 생성할 수 있습니다. 구성이 완료된 후 각 스위치에 대한 구성을 저장하려면 copy run start를 실행해야 합니다.

"다음: NetApp 스토리지 구현 절차(1부)"

NetApp 스토리지 구축 절차(1부)

이 섹션에서는 NetApp AFF 스토리지 구축 절차를 설명합니다.

NetApp 스토리지 컨트롤러 AFF2xx 시리즈 설치

NetApp Hardware Universe를 참조하십시오

NetApp HWU(Hardware Universe) 애플리케이션은 특정 ONTAP 버전에 대해 지원되는 하드웨어 및 소프트웨어 구성요소를 제공합니다. 현재 ONTAP 소프트웨어가 지원하는 모든 NetApp 스토리지 어플라이언스에 대한 구성 정보를 제공합니다. 구성요소 호환성 표도 제공합니다.

사용하려는 하드웨어 및 소프트웨어 구성 요소가 설치하려는 ONTAP 버전에서 지원되는지 확인합니다.

1. 에 액세스합니다 "HWU" 응용 프로그램 - 시스템 구성 가이드를 봅니다. 컨트롤러 탭을 클릭하여 원하는 사양의 ONTAP 소프트웨어 버전과 NetApp 스토리지 어플라이언스 간의 호환성을 확인하십시오.
2. 또는 스토리지 어플라이언스별로 구성 요소를 비교하려면 스토리지 시스템 비교 를 클릭합니다.

컨트롤러 AFF2XX 시리즈 사전 요구 사항
스토리지 시스템의 물리적 위치를 계획하려면 NetApp Hardware Universe를 참조하십시오. 전기 요구 사항, 지원되는 전원 코드, 온보드 포트 및 케이블 섹션을 참조하십시오.

스토리지 컨트롤러

의 컨트롤러에 대한 물리적 설치 절차를 따릅니다 "AFF A220 문서".

NetApp ONTAP 9.4

구성 워크시트

설치 스크립트를 실행하기 전에 제품 설명서에서 구성 워크시트를 작성하십시오. 구성 워크시트는 에서 사용할 수 있습니다 "ONTAP 9.4 소프트웨어 설정 설명서".

ⓘ 이 시스템은 스위치가 없는 2노드 클러스터 구성에서 설정됩니다.

다음 표에는 ONTAP 9.4 설치 및 구성 정보가 나와 있습니다.

클러스터 세부 정보	클러스터 세부 정보 값입니다
클러스터 노드 A IP 주소입니다	<<var_NodeA_mgmt_ip>> 를 입력합니다
클러스터 노드 A 넷마스크	<<var_NodeA_mgmt_mask>> 를 입력합니다
클러스터 노드 A 게이트웨이	<<var_NodeA_mgmt_gateway>> 를 참조하십시오
클러스터 노드 A 이름	<<var_NodeA>> 를 참조하십시오
클러스터 노드 B IP 주소입니다	<<var_NodeB_mgmt_ip>> 를 입력합니다
클러스터 노드 B 넷마스크	<<var_NodeB_mgmt_mask>> 를 입력합니다

클러스터 세부 정보	클러스터 세부 정보 값입니다
클러스터 노드 B 게이트웨이	<<var_NodeB_mgmt_gateway>> 를 참조하십시오
클러스터 노드 B 이름	<<var_NodeB>> 를 참조하십시오
ONTAP 9.4 URL	<<var_url_boot_software>>
클러스터의 이름입니다	<<var_clustername>> 를 클릭합니다
클러스터 관리 IP 주소입니다	<<var_clustermgmt_ip>> 를 입력합니다
클러스터 B 게이트웨이	<<var_clustermgmt_gateway>> 를 클릭합니다
클러스터 B 넷마스크	<<var_clustermgmt_mask>> 를 입력합니다
도메인 이름	<<var_domain_name>>
DNS 서버 IP(둘 이상 입력할 수 있음)	<<var_dns_server_ip>> 를 참조하십시오
NTP 서버 IP(둘 이상 입력할 수 있음)	<<var_ntp_server_ip>> 를 참조하십시오

노드 **A**를 구성합니다

노드 A를 구성하려면 다음 단계를 완료하십시오.

1. 스토리지 시스템 콘솔 포트에 연결합니다. Loader-A 메시지가 표시됩니다. 하지만 스토리지 시스템이 재부팅 루프 상태인 경우 다음 메시지가 표시될 때 Ctrl-C를 눌러 자동 부팅 루프를 종료합니다.

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. 시스템이 부팅되도록 합니다.

```
autoboot
```

3. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.

   ONTAP 9.4가 부팅 중인 소프트웨어 버전이 아닌 경우 다음 단계를 계속하여 새 소프트웨어를 설치합니다. ONTAP 9.4가 부팅 중인 버전인 경우 옵션 8 및 y를 선택하여 노드를 재부팅합니다. 그런 다음 14단계를 계속합니다.

4. 새 소프트웨어를 설치하려면 옵션 '7'을 선택합니다.
5. 업그레이드를 수행하려면 y를 입력하십시오.
6. 다운로드에 사용할 네트워크 포트로 e0M 을 선택합니다.
7. 지금 재부팅하려면 y를 입력하십시오.
8. 각 위치에 e0M의 IP 주소, 넷마스크 및 기본 게이트웨이를 입력합니다.

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

9. 소프트웨어를 찾을 수 있는 URL을 입력합니다.

이 웹 서버는 Ping할 수 있어야 합니다.

```
<<var_url_boot_software>>
```

10. 사용자 이름에 대해 Enter 키를 눌러 사용자 이름이 없음을 나타냅니다.
11. 새로 설치한 소프트웨어를 이후 재부팅에 사용할 기본값으로 설정하려면 'y'를 입력합니다.
12. 노드를 재부팅하려면 y를 입력합니다.

    새 소프트웨어를 설치할 때 시스템이 BIOS 및 어댑터 카드에 대한 펌웨어 업그레이드를 수행할 수 있으며, 이로 인해 LOADER-A 프롬프트에서 재부팅되고 중지될 수 있습니다. 이러한 작업이 발생하면 시스템이 이 절차를 벗어날 수 있습니다.

13. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.
14. Clean Configuration 및 Initialize All Disks 옵션을 4로 선택합니다.
15. 디스크를 제로화하려면 y를 입력하고 구성을 재설정한 다음 새 파일 시스템을 설치합니다.
16. 디스크에 있는 모든 데이터를 지우려면 'y'를 입력합니다.

    연결된 디스크의 수와 유형에 따라 루트 애그리게이트의 초기화 및 생성을 완료하는 데 90분 이상이 걸릴 수 있습니다. 초기화가 완료되면 스토리지 시스템이 재부팅됩니다. SSD를 초기화하는 데 걸리는 시간은 상당히 줄어듭니다. 노드 A용 디스크가 제로화하는 동안 노드 B 구성을 계속할 수 있습니다.

17. 노드 A를 초기화하는 동안 노드 B를 구성합니다

노드 **B**를 구성합니다

노드 B를 구성하려면 다음 단계를 완료하십시오.

1. 스토리지 시스템 콘솔 포트에 연결합니다. Loader-A 메시지가 표시됩니다. 하지만 스토리지 시스템이 재부팅 루프 상태인 경우 다음 메시지가 표시될 때 Ctrl-C를 눌러 자동 부팅 루프를 종료합니다.

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.

```
autoboot
```

3. 메시지가 나타나면 Ctrl-C를 누릅니다.

    ONTAP 9.4가 부팅 중인 소프트웨어 버전이 아닌 경우 다음 단계를 계속하여 새 소프트웨어를 설치합니다. ONTAP 9.4가 부팅 중인 버전인 경우 옵션 8 및 y를 선택하여 노드를 재부팅합니다. 그런 다음 14단계를 계속합니다.

4. 새 소프트웨어를 설치하려면 옵션 7을 선택합니다.
5. 업그레이드를 수행하려면 y를 입력하십시오.

6. 다운로드에 사용할 네트워크 포트로 e0M 을 선택합니다.
7. 지금 재부팅하려면 y를 입력하십시오.
8. 각 위치에 e0M의 IP 주소, 넷마스크 및 기본 게이트웨이를 입력합니다.

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. 소프트웨어를 찾을 수 있는 URL을 입력합니다.

   이 웹 서버는 Ping할 수 있어야 합니다.

```
<<var_url_boot_software>>
```

10. 사용자 이름에 대해 Enter 키를 눌러 사용자 이름이 없음을 나타냅니다.
11. 새로 설치한 소프트웨어를 이후 재부팅에 사용할 기본값으로 설정하려면 'y'를 입력합니다.
12. 노드를 재부팅하려면 y를 입력합니다.

    새 소프트웨어를 설치할 때 시스템이 BIOS 및 어댑터 카드에 대한 펌웨어 업그레이드를 수행할 수 있으며, 이로 인해 LOADER-A 프롬프트에서 재부팅되고 중지될 수 있습니다. 이러한 작업이 발생하면 시스템이 이 절차를 벗어날 수 있습니다.

13. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.
14. Clean Configuration(구성 정리) 및 Initialize All Disks(모든 디스크 초기화) 에 대해 옵션 4 를 선택합니다.
15. 디스크를 제로화하려면 y를 입력하고 구성을 재설정한 다음 새 파일 시스템을 설치합니다.
16. 디스크에 있는 모든 데이터를 지우려면 'y'를 입력합니다.

    연결된 디스크의 수와 유형에 따라 루트 애그리게이트의 초기화 및 생성을 완료하는 데 90분 이상이 걸릴 수 있습니다. 초기화가 완료되면 스토리지 시스템이 재부팅됩니다. SSD를 초기화하는 데 걸리는 시간은 상당히 줄어듭니다.

노드 **A** 구성 및 클러스터 구성 계속

스토리지 컨트롤러 A(노드 A) 콘솔 포트에 연결된 콘솔 포트 프로그램에서 노드 설정 스크립트를 실행합니다. 이 스크립트는 ONTAP 9.4가 노드에서 처음 부팅될 때 나타납니다.

ONTAP 9.4에서 노드 및 클러스터 설정 절차가 약간 변경되었습니다. 이제 클러스터 설정 마법사를 사용하여 클러스터의 첫 번째 노드를 구성하고 System Manager를 사용하여 클러스터를 구성할 수 있습니다.

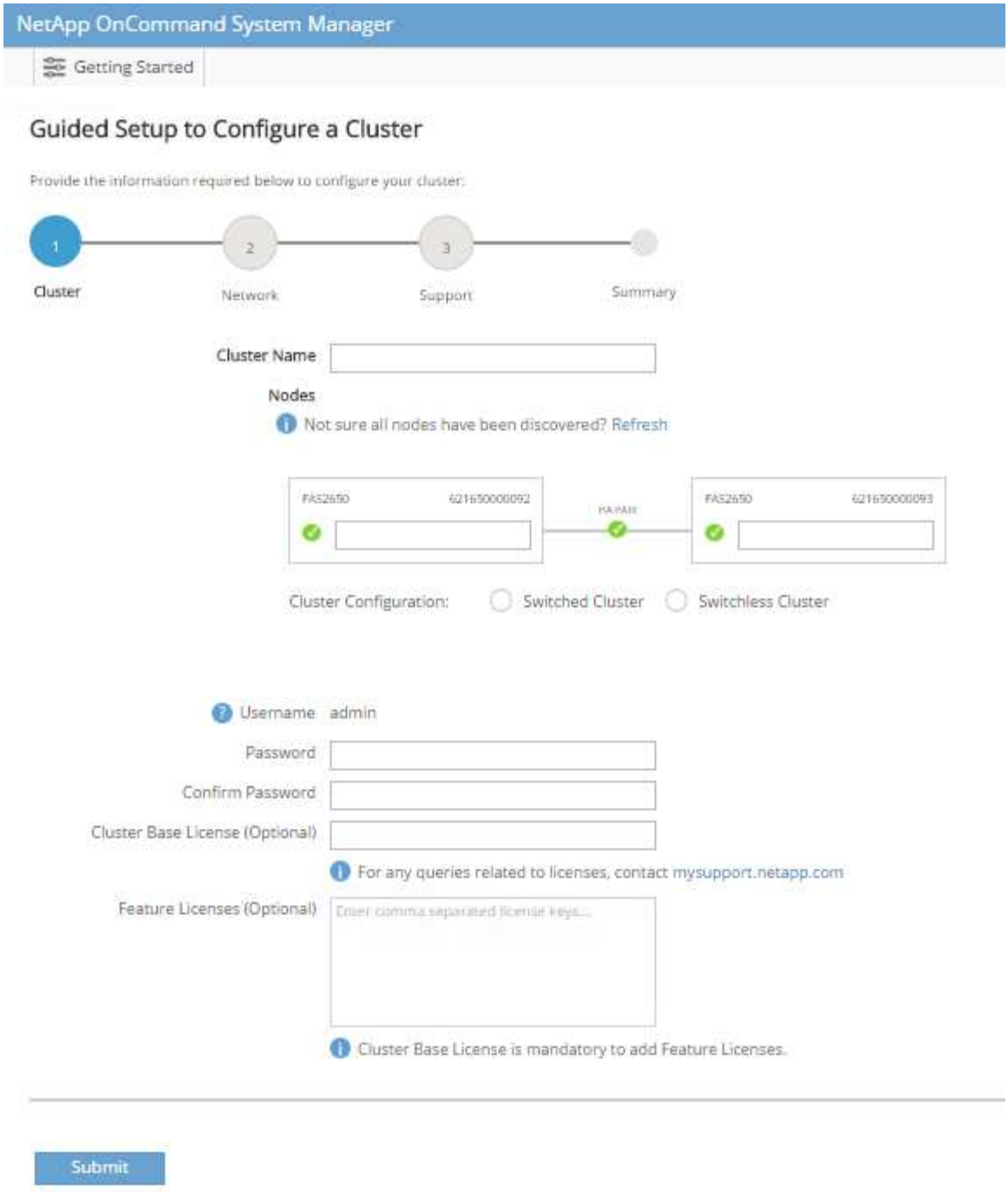
1. 프롬프트에 따라 노드 A를 설정합니다

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. 노드의 관리 인터페이스의 IP 주소로 이동합니다.

   CLI를 사용하여 클러스터를 설정할 수도 있습니다. 이 문서에서는 NetApp System Manager의 안내에 따라 설정을 사용하는 클러스터 설정에 대해 설명합니다.

3. Guided Setup(안내식 설정) 을 클릭하여 클러스터를 구성합니다.
4. 클러스터 이름은 <<var_clustername>>'을, 구성 중인 각 노드에 대해서는 <<var_NodeA>>'와 <<var_NodeB>>를 입력합니다. 스토리지 시스템에 사용할 암호를 입력합니다. 클러스터 유형으로 Switchless Cluster를 선택합니다. 클러스터 기본 라이센스를 입력합니다.



5. 클러스터, NFS 및 iSCSI에 대한 기능 라이센스도 입력할 수 있습니다.
6. 클러스터를 생성 중임을 나타내는 상태 메시지가 표시됩니다. 이 상태 메시지는 여러 상태를 순환합니다. 이 과정은 몇 분 정도 소요됩니다.
7. 네트워크를 구성합니다.
   a. IP 주소 범위 옵션을 선택 취소합니다.
   b. Cluster Management IP Address 필드(<<var_clustermgmt_ip>>)에 넷마스크 필드(<<var_clustermgmt_mask>>)에 <<var_clustermgmt_gateway>>)를 입력합니다. 다음을 사용하십시오. 포트 필드의 선택기로 노드 A의 e0M을 선택합니다
   c. 노드 A의 노드 관리 IP가 이미 채워져 있습니다. 노드 B에 대해 '<<var_NodeA_mgmt_ip>>'를 입력합니다

d. DNS Domain Name 필드에 '<<var_domain_name>>'을 입력합니다. DNS 서버 IP 주소 필드에 '<<var_dns_server_ip>>'를 입력합니다.

   여러 DNS 서버 IP 주소를 입력할 수 있습니다.

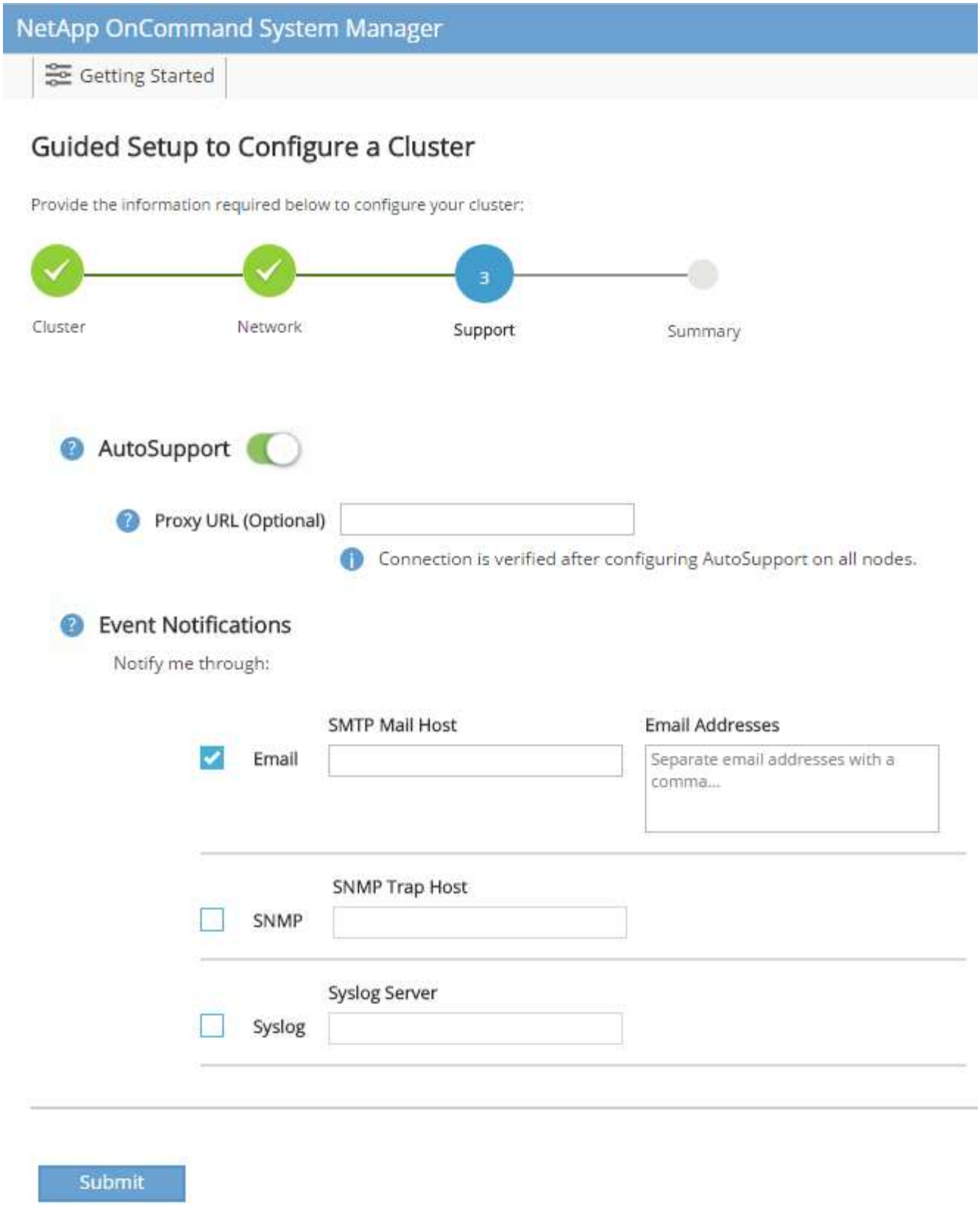
e. Primary NTP Server 필드에 '<<var_ntp_server_ip>>'를 입력합니다.

   대체 NTP 서버를 입력할 수도 있습니다.

8. 지원 정보를 구성합니다.

   a. 환경에 AutoSupport에 액세스하기 위한 프록시가 필요한 경우 프록시 URL에 URL을 입력합니다.
   b. 이벤트 알림에 대한 SMTP 메일 호스트 및 이메일 주소를 입력합니다.

      계속하려면 이벤트 알림 방법을 설정해야 합니다. 방법 중 하나를 선택할 수 있습니다.



9. 클러스터 구성이 완료되었으면 클러스터 관리 를 클릭하여 스토리지를 구성합니다.

스토리지 노드 및 기본 클러스터를 구성한 후에는 스토리지 클러스터 구성을 계속할 수 있습니다.

모든 스페어 디스크를 제로합니다

클러스터의 모든 스페어 디스크를 제로하려면 다음 명령을 실행합니다.

```
disk zerospares
```

온보드 **UTA2** 포트 속성을 설정합니다

1. ucadmin show 명령을 실행하여 현재 모드와 포트의 현재 유형을 확인합니다.

```
AFF A220::> ucadmin show
                      Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF A220_A     0c       fc       target     -        -          online
AFF A220_A     0d       fc       target     -        -          online
AFF A220_A     0e       fc       target     -        -          online
AFF A220_A     0f       fc       target     -        -          online
AFF A220_B     0c       fc       target     -        -          online
AFF A220_B     0d       fc       target     -        -          online
AFF A220_B     0e       fc       target     -        -          online
AFF A220_B     0f       fc       target     -        -          online
8 entries were displayed.
```

2. 사용 중인 포트의 현재 모드가 CNA인지, 현재 유형이 'target'으로 설정되어 있는지 확인합니다. 그렇지 않은 경우 다음 명령을 사용하여 포트 속성을 변경합니다.

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

이전 명령을 실행하려면 포트가 오프라인 상태여야 합니다. 포트를 오프라인으로 전환하려면 다음 명령을 실행합니다.

```
`network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down`
```

포트 속성을 변경한 경우 변경 사항을 적용하려면 각 노드를 재부팅해야 합니다.

관리 논리 인터페이스**(LIF)** 이름 바꾸기

관리 LIF의 이름을 변경하려면 다음 단계를 수행하십시오.

1. 현재 관리 LIF 이름을 표시합니다.

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

2. 클러스터 관리 LIF의 이름을 바꿉니다.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_cluster_mgmt_lif_1 -newname cluster_mgmt
```

3. 노드 B 관리 LIF의 이름을 바꿉니다.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF A220_B_1 -newname AFF A220-02_mgmt1
```

클러스터 관리에서 자동 되돌리기 설정

클러스터 관리 인터페이스에서 자동 되돌리기 매개 변수를 설정합니다.

```
network interface modify -vserver <<clustername>> -lif cluster_mgmt -auto-
revert true
```

서비스 프로세서 네트워크 인터페이스를 설정합니다

각 노드의 서비스 프로세서에 정적 IPv4 주소를 할당하려면 다음 명령을 실행합니다.

```
system service-processor network modify -node <<var_nodeA>> -address
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify -node <<var_nodeB>> -address
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

ⓘ 서비스 프로세서 IP 주소는 노드 관리 IP 주소와 동일한 서브넷에 있어야 합니다.

ONTAP에서 스토리지 페일오버 설정

스토리지 페일오버가 설정되었는지 확인하려면 페일오버 쌍에서 다음 명령을 실행합니다.

1. 스토리지 페일오버 상태를 확인합니다.

```
storage failover show
```

'<<var_NodeA>>'와 '<<var_NodeB>>'는 모두 테이크오버를 수행할 수 있어야 합니다. 노드가 테이크오버 수행 가능한 경우 3단계로 이동하십시오.

2. 두 노드 중 하나에서 페일오버가 사용되도록 설정합니다.

```
storage failover modify -node <<var_nodeA>> -enabled true
```

한 노드에서 페일오버가 사용되도록 설정하면 두 노드 모두에서 설정됩니다.

3. 2노드 클러스터의 HA 상태를 확인합니다.

2개 이상의 노드가 있는 클러스터에는 이 단계를 적용할 수 없습니다.

```
cluster ha show
```

4. 고가용성이 구성된 경우 6단계로 이동합니다. 고가용성이 구성된 경우 명령을 실행하면 다음 메시지가 표시됩니다.

```
High Availability Configured: true
```

5. 2노드 클러스터에만 HA 모드를 사용하도록 설정합니다.

> ⓘ 2개 이상의 노드가 있는 클러스터에서는 페일오버에 문제가 발생하므로 이 명령을 실행하지 마십시오.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. 하드웨어 지원이 올바르게 구성되어 있는지 확인하고 필요한 경우 파트너 IP 주소를 수정합니다.

```
storage failover hwassist show
```

"Keep Alive Status: Error: whwassist keep alive alert from partner(활성 상태 유지: 오류: 파트너의 hwassist keep alive 경고를 수신하지 못했습니다)" 메시지는 하드웨어 지원이 구성되지 않았음을 나타냅니다. 다음 명령을 실행하여 하드웨어 지원을 구성합니다.

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

ONTAP에서 점보 프레임 **MTU** 브로드캐스트 도메인을 생성합니다

MTU가 9000인 데이터 브로드캐스트 도메인을 생성하려면 다음 명령을 실행합니다.

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

기본 브로드캐스트 도메인에서 데이터 포트를 제거합니다

10GbE 데이터 포트는 iSCSI/NFS 트래픽에 사용되며 이러한 포트는 기본 도메인에서 제거해야 합니다. 포트 e0e 및 e0f는 사용되지 않으며 기본 도메인에서도 제거해야 합니다.

브로드캐스트 도메인에서 포트를 제거하려면 다음 명령을 실행합니다.

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

UTA2 포트에서 흐름 제어를 사용하지 않도록 설정합니다

외부 장치에 연결된 모든 UTA2 포트에서 흐름 제어를 사용하지 않도록 설정하는 것이 NetApp의 모범 사례입니다. 흐름 제어를 사용하지 않도록 설정하려면 다음 명령을 실행합니다.

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
```

ONTAP에서 **IFGRP LACP**를 구성합니다

이 인터페이스 그룹 유형에 2개 이상의 이더넷 인터페이스와 LACP를 지원하는 스위치가 필요합니다. 스위치가 올바르게 구성되었는지 확인합니다.

클러스터 프롬프트에서 다음 단계를 완료합니다.

```
ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d
```

NetApp ONTAP에서 점보 프레임을 구성합니다

ONTAP 네트워크 포트에서 점보 프레임(일반적으로 9,000바이트 MTU 사용)을 사용하도록 구성하려면 클러스터 쉘에서 다음 명령을 실행합니다.

```
AFF A220::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
```

ONTAP에서 **VLAN**을 생성합니다

ONTAP에서 VLAN을 생성하려면 다음 단계를 수행하십시오.

1. NFS VLAN 포트를 생성하여 데이터 브로드캐스트 도메인에 추가합니다.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
<<var_nfs_vlan_id>>
```

2. iSCSI VLAN 포트를 생성하여 데이터 브로드캐스트 도메인에 추가합니다.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>
```

3. MGMT-VLAN 포트를 생성합니다.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>
```

ONTAP에서 애그리게이트를 생성합니다

ONTAP 설정 프로세스 중에 루트 볼륨이 포함된 애그리게이트가 생성됩니다. 추가 애그리게이트를 생성하려면 애그리게이트 이름, 애그리게이트를 생성할 노드, 애그리게이트에 포함된 디스크 수를 결정합니다.

Aggregate를 생성하려면 다음 명령을 실행합니다.

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

구성에 최소 하나의 디스크(가장 큰 디스크 선택)를 스페어로 보관합니다. 모범 사례는 각 디스크 유형 및 크기에 대해 하나 이상의 스페어를 두는 것입니다.

5개의 디스크로 시작합니다. 스토리지를 추가해야 할 때 디스크를 애그리게이트에 추가할 수 있습니다.

디스크 비우기가 완료될 때까지 애그리게이트를 생성할 수 없습니다. 집계 생성 상태를 표시하려면 'aggr show' 명령을 실행합니다. aggr1 _ NodeA가 온라인이 될 때까지 진행하지 마십시오.

ONTAP에서 시간대를 구성합니다

시간 동기화를 구성하고 클러스터에서 표준 시간대를 설정하려면 다음 명령을 실행합니다.

```
timezone <<var_timezone>>
```

예를 들어 미국 동부의 시간대는 미국/뉴욕입니다. 표준 시간대 이름을 입력하기 시작하면 Tab 키를 눌러 사용 가능한 옵션을 확인합니다.

ONTAP에서 SNMP를 구성합니다

SNMP를 구성하려면 다음 단계를 수행하십시오.

1. 위치 및 연락처와 같은 SNMP 기본 정보를 구성합니다. 이 정보는 SNMP에서 'SysLocation', 'SysContact' 변수로 표시됩니다.

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_snmp_location>>"
snmp init 1
options snmp.enable on
```

2. 원격 호스트에 보낼 SNMP 트랩을 구성합니다.

```
snmp traphost add <<var_snmp_server_fqdn>>
```

ONTAP에서 SNMPv1을 구성합니다

SNMPv1을 구성하려면 커뮤니티라는 공유 암호 일반 텍스트 암호를 설정합니다.

```
snmp community add ro <<var_snmp_community>>
```

NMP community delete all 명령을 주의하여 사용한다. 다른 모니터링 제품에 커뮤니티 문자열을 사용하는 경우 이 명령은 해당 문자열을 제거합니다.

ONTAP에서 SNMPv3을 구성합니다

SNMPv3을 사용하려면 인증을 위해 사용자를 정의하고 구성해야 합니다. SNMPv3을 구성하려면 다음 단계를 수행하십시오.

1. Security snmpusers 명령을 실행하여 엔진 ID를 조회한다.
2. 'snmpv3user'라는 사용자를 생성합니다.

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. 신뢰할 수 있는 엔터티의 엔진 ID를 입력하고 인증 프로토콜로 md5 를 선택한다.
4. 메시지가 나타나면 인증 프로토콜에 사용할 최소 길이 8자로 된 암호를 입력합니다.
5. 개인 정보 보호 프로토콜로 'des'를 선택합니다.
6. 메시지가 나타나면 개인 정보 보호 프로토콜에 사용할 최소 길이 8자로 된 암호를 입력합니다.

ONTAP에서 **AutoSupport HTTPS**를 구성합니다

NetApp AutoSupport 툴은 HTTPS를 통해 지원 요약 정보를 NetApp에 보냅니다. AutoSupport를 구성하려면 다음 명령을 실행합니다.

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

스토리지 가상 머신을 생성합니다

인프라 스토리지 가상 시스템(SVM)을 생성하려면 다음 단계를 완료하십시오.

1. 'vserver create' 명령을 실행합니다.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. NetApp VSC를 위한 인프라-SVM 애그리게이트 목록에 데이터 애그리게이트를 추가합니다.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. NFS와 iSCSI를 남겨두고 SVM에서 사용하지 않는 스토리지 프로토콜을 제거합니다.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. 인프라 SVM에서 NFS 프로토콜을 사용하고 실행합니다.

```
`nfs create -vserver Infra-SVM -udp disabled`
```

5. NetApp NFS VAAI 플러그인에 대한 'VM vStorage' 매개 변수를 설정합니다. 그런 다음 NFS가 구성되었는지 확인합니다.

```
`vserver nfs modify –vserver Infra-SVM –vstorage enabled`
`vserver nfs show `
```

스토리지 가상 시스템이 이전에 서버라고 불리기 때문에 명령줄에서는 'vserver'가 명령을 앞에 표시합니다.

ONTAP에서 **NFSv3**을 구성합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
ESXi 호스트 NFS IP 주소입니다	<<var_esxi_hostA_nfs_ip>> 를 참조하십시오
ESXi 호스트 B NFS IP 주소입니다	<<var_esxi_hostB_nfs_ip>> 를 참조하십시오

SVM에서 NFS를 구성하려면 다음 명령을 실행합니다.

1. 기본 엑스포트 정책에서 각 ESXi 호스트에 대한 규칙을 생성합니다.
2. 생성 중인 각 ESXi 호스트에 대해 규칙을 할당합니다. 각 호스트에는 고유한 규칙 인덱스가 있습니다. 첫 번째 ESXi 호스트에는 규칙 인덱스 1이 있고 두 번째 ESXi 호스트에는 규칙 인덱스 2가 있습니다.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 2 –protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. 인프라 SVM 루트 볼륨에 엑스포트 정책을 할당합니다.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

vSphere를 설정한 후 NetApp VSC는 엑스포트 정책을 자동으로 처리합니다. 설치하지 않은 경우 Cisco UCS C-Series 서버를 추가할 때 엑스포트 정책 규칙을 생성해야 합니다.

ONTAP에서 **iSCSI** 서비스를 생성합니다

iSCSI 서비스를 생성하려면 다음 단계를 완료하십시오.

1. SVM에서 iSCSI 서비스를 생성합니다. 또한 이 명령은 iSCSI 서비스를 시작하고 SVM에 대한 iSCSI IQN을 설정합니다. iSCSI가 구성되었는지 확인합니다.

```
iscsi create -vserver Infra-SVM
iscsi show
```

ONTAP에서 **SVM** 루트 볼륨의 로드 공유 미러를 생성합니다

1. 각 노드에서 인프라 SVM 루트 볼륨의 로드 공유 미러가 될 볼륨을 생성합니다.

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
aggr1_nodeA –size 1GB –type DP
volume create –vserver Infra_Vserver –volume rootvol_m02 –aggregate
aggr1_nodeB –size 1GB –type DP
```

2. 15분마다 루트 볼륨 미러 관계를 업데이트하는 작업 스케줄을 생성합니다.

```
job schedule interval create -name 15min -minutes 15
```

3. 미러링 관계를 생성합니다.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. 미러링 관계를 초기화하고 미러링 관계가 만들어졌는지 확인합니다.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
snapmirror show
```

ONTAP에서 **HTTPS** 액세스를 구성합니다

스토리지 컨트롤러에 대한 보안 액세스를 구성하려면 다음 단계를 수행하십시오.

1. 인증서 명령에 액세스할 수 있도록 권한 수준을 높입니다.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. 일반적으로 자체 서명된 인증서가 이미 있습니다. 다음 명령을 실행하여 인증서를 확인합니다.

```
security certificate show
```

3. 표시된 각 SVM에서 인증서 공통 이름은 SVM의 DNS FQDN과 일치해야 합니다. 네 개의 기본 인증서를 삭제하고 자체 서명된 인증서 또는 인증 기관의 인증서로 대체해야 합니다.

   인증서를 만들기 전에 만료된 인증서를 삭제하는 것이 좋습니다. 만료된 인증서를 삭제하려면 보안 인증서 삭제 명령을 실행합니다. 다음 명령에서 Tab completion을 사용하여 각 기본 인증서를 선택하고 삭제합니다.

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. 자체 서명된 인증서를 생성하고 설치하려면 다음 명령을 일회성 명령으로 실행합니다. 인프라 SVM 및 클러스터 SVM에 대한 서버 인증서를 생성합니다. 다시 한 번 탭 완료 기능을 사용하면 이러한 명령을 쉽게 완료할 수 있습니다.

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm. netapp.com
-type  server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. 다음 단계에서 필요한 매개 변수 값을 얻으려면 'security certificate show' 명령을 실행합니다.
6. '–server-enabled true' 및 '–client-enabled false' 매개 변수를 사용하여 방금 만든 각 인증서를 활성화합니다. 다시 탭 완료를 사용합니다.

```
security ssl modify [TAB] …
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. SSL 및 HTTPS 액세스를 구성 및 활성화하고 HTTP 액세스를 비활성화합니다.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be
         interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
–vserver <<var_clustername>>
```

명령 실행 중 일부에서 항목이 존재하지 않는다는 오류 메시지가 반환되는 것은 정상입니다.

8. 관리 권한 수준으로 되돌아가며 SVM을 웹에서 사용할 수 있도록 설정을 생성합니다.

```
set -privilege admin
vserver services web modify -name spi|ontapi|compat -vserver * -enabled
true
```

ONTAP에서 **NetApp FlexVol** 볼륨을 생성합니다

NetApp FlexVol 볼륨을 생성하려면 볼륨 이름, 크기 및 이 볼륨이 있는 애그리게이트를 입력합니다. 2개의 VMware 데이터 저장소 볼륨과 서버 부팅 볼륨을 생성합니다.

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB -state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

ONTAP에서 중복 제거를 설정합니다

적절한 볼륨에서 중복 제거를 설정하려면 다음 명령을 실행합니다.

```
volume efficiency on -vserver Infra-SVM -volume infra_datastore_1
volume efficiency on -vserver Infra-SVM -volume esxi_boot
```

ONTAP에서 **LUN**을 생성합니다

2개의 부팅 LUN을 생성하려면 다음 명령을 실행합니다.

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```

Cisco UCS C-Series 서버를 더 추가할 때는 부팅 LUN을 더 생성해야 합니다.

ONTAP에서 iSCSI LIF를 생성합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
스토리지 노드 A iSCSI LIF01A	<<var_NodeA_iscsi_lif01a_ip>> 를 참조하십시오
스토리지 노드 A iSCSI LIF01A 네트워크 마스크입니다	<<var_NodeA_iscsi_lif01a_mask>>
스토리지 노드 A iSCSI LIF01B	<<var_NodeA_iscsi_liff 01b_ip>> 를 참조하십시오
스토리지 노드 A iSCSI LIF01B 네트워크 마스크입니다	<<var_NodeA_iscsi_liff 01b_mask>>
스토리지 노드 B iSCSI LIF01A	<<var_NodeB_iscsi_liff 01a_ip>>
스토리지 노드 B iSCSI LIF01A 네트워크 마스크입니다	<<var_NodeB_iscsi_liff 01a_mask>>
스토리지 노드 B iSCSI LIF01B	<<var_NodeB_iscsi_liff 01b_ip>>
스토리지 노드 B iSCSI LIF01B 네트워크 마스크입니다	<<var_NodeB_iscsi_liff 01b_mask>>

1. 각 노드에 2개의 iSCSI LIF를 4개 생성합니다.

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface show
```

ONTAP에서 NFS LIF를 생성합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
스토리지 노드 A NFS LIF 01 IP입니다	<<var_NodeA_nfs_lif_01_ip>>
스토리지 노드 A NFS LIF 01 네트워크 마스크	<<var_NodeA_nfs_lif_01_mask>>
스토리지 노드 B NFS LIF 02 IP	<<var_NodeB_nfs_lif_02_ip>>
스토리지 노드 B NFS LIF 02 네트워크 마스크	<<var_NodeB_nfs_lif_02_mask>>

1. NFS LIF를 생성합니다.

```
network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up -failover-policy broadcast-
domain-wide -firewall-policy data -auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up -failover-policy broadcast-
domain-wide -firewall-policy data -auto-revert true
network interface show
```

인프라 **SVM** 관리자를 추가합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
Vsmgmt IP	<<var_svm_mgmt_ip>> 를 입력합니다
Vsmgmt 네트워크 마스크	<<var_svm_mgmt_mask>>
Vsmgmt 기본 게이트웨이	<<var_svm_mgmt_gateway>>

관리 네트워크에 인프라 SVM 관리자 및 SVM 관리 논리 인터페이스를 추가하려면 다음 단계를 완료하십시오.

1. 다음 명령을 실행합니다.

```
network interface create -vserver Infra-SVM -lif vsmgmt -role data
-data-protocol none -home-node <<var_nodeB>> -home-port  e0M -address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
-failover-policy broadcast-domain-wide -firewall-policy mgmt -auto-
revert true
```

ⓘ 여기서 SVM 관리 IP는 스토리지 클러스터 관리 IP와 동일한 서브넷에 있어야 합니다.

2. 기본 경로를 생성하여 SVM 관리 인터페이스가 외부 환경에 도달할 수 있도록 합니다.

```
network route create -vserver Infra-SVM -destination 0.0.0.0/0 -gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. SVM vsadmin 사용자의 암호를 설정하고 사용자 잠금을 해제합니다.

```
security login password -username vsadmin -vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock -username vsadmin -vserver Infra-SVM
```

"다음: Cisco UCS C-Series 랙 서버 구현 절차"

Cisco UCS C-Series 랙 서버 구축 절차

다음 섹션에서는 FlexPod Express 구성에 사용할 Cisco UCS C-Series 독립 실행형 랙 서버를 구성하기 위한 절차를 세부적으로 설명합니다.

Cisco 통합 관리 서버에 대한 초기 **Cisco UCS C-Series** 독립 실행형 서버 설정을 수행합니다

Cisco UCS C-Series 독립 실행형 서버에 대한 CIMC 인터페이스의 초기 설정을 위해 다음 단계를 완료합니다.

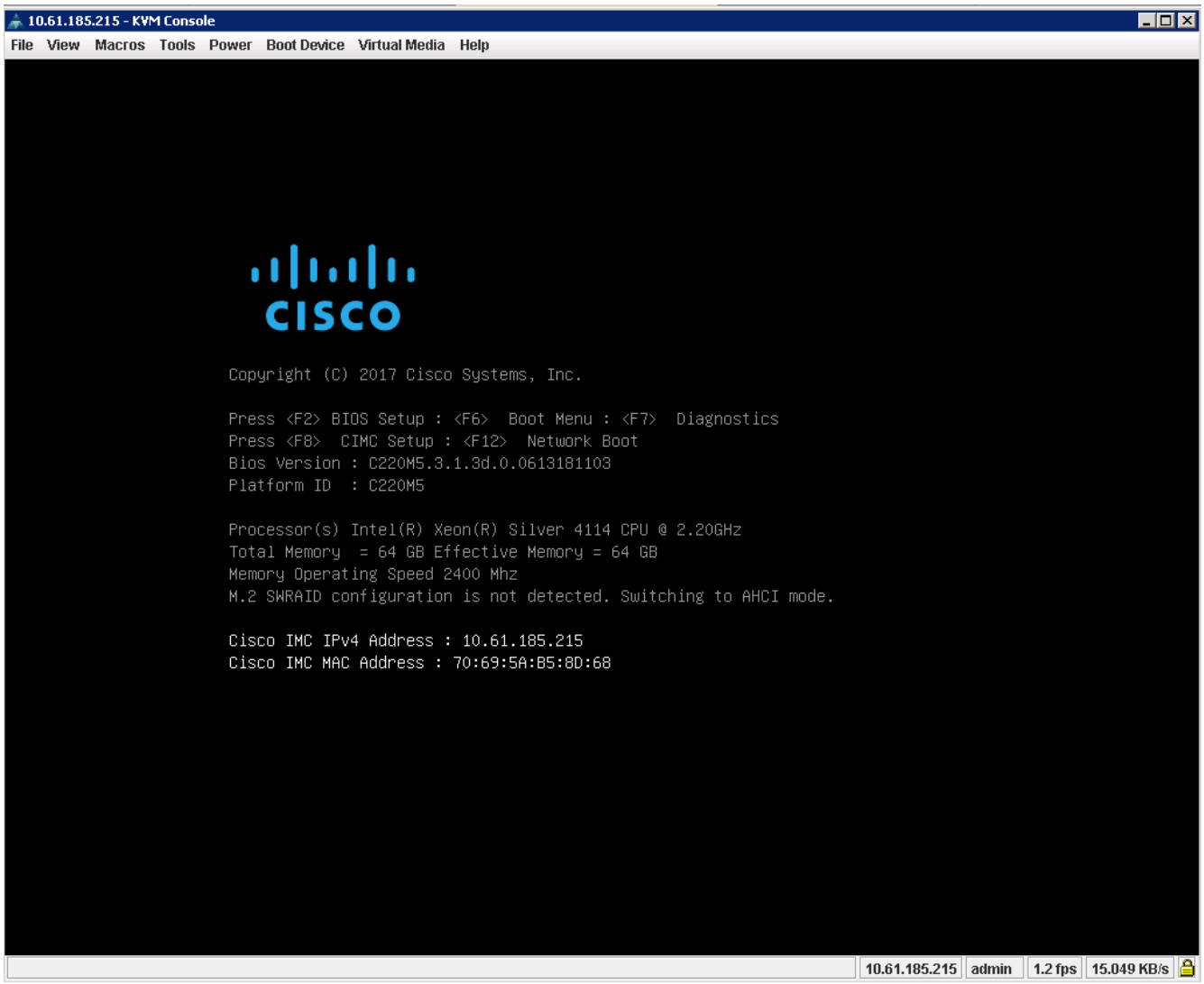
다음 표에는 각 Cisco UCS C-Series 독립 실행형 서버에 대한 CIMC를 구성하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
CIMC IP 주소	CIMC_IP>\< CIMC_IP>>
CIMC 서브넷 마스크	CIMC_Netmask>\<CIMC_NETMASK>>
CIMC 기본 게이트웨이	CIMC_GATELOGATE>\<<CIMC_Gateway>

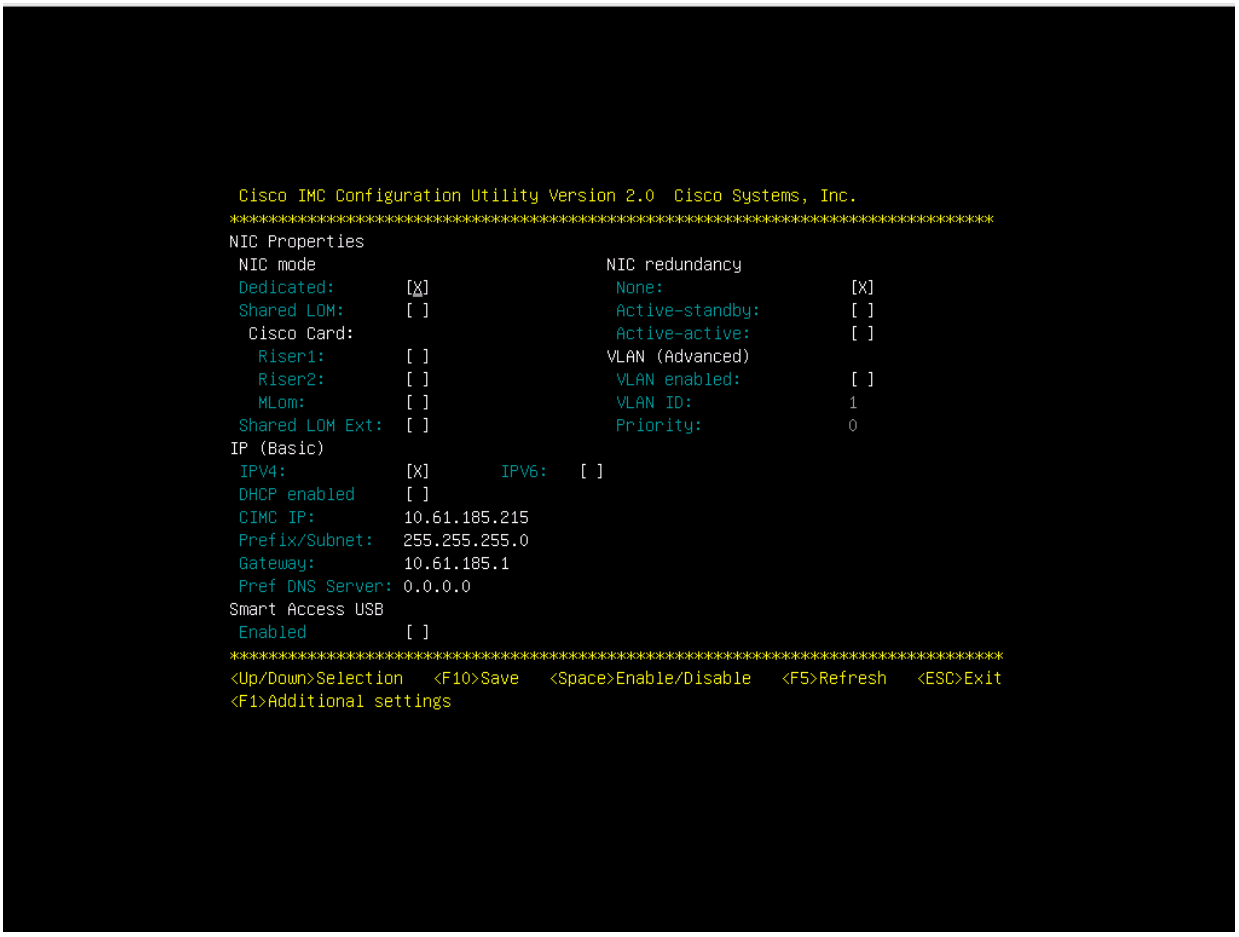
이 검증에 사용된 CIMC 버전은 CIMC 3.1.3(g)입니다.

모든 서버

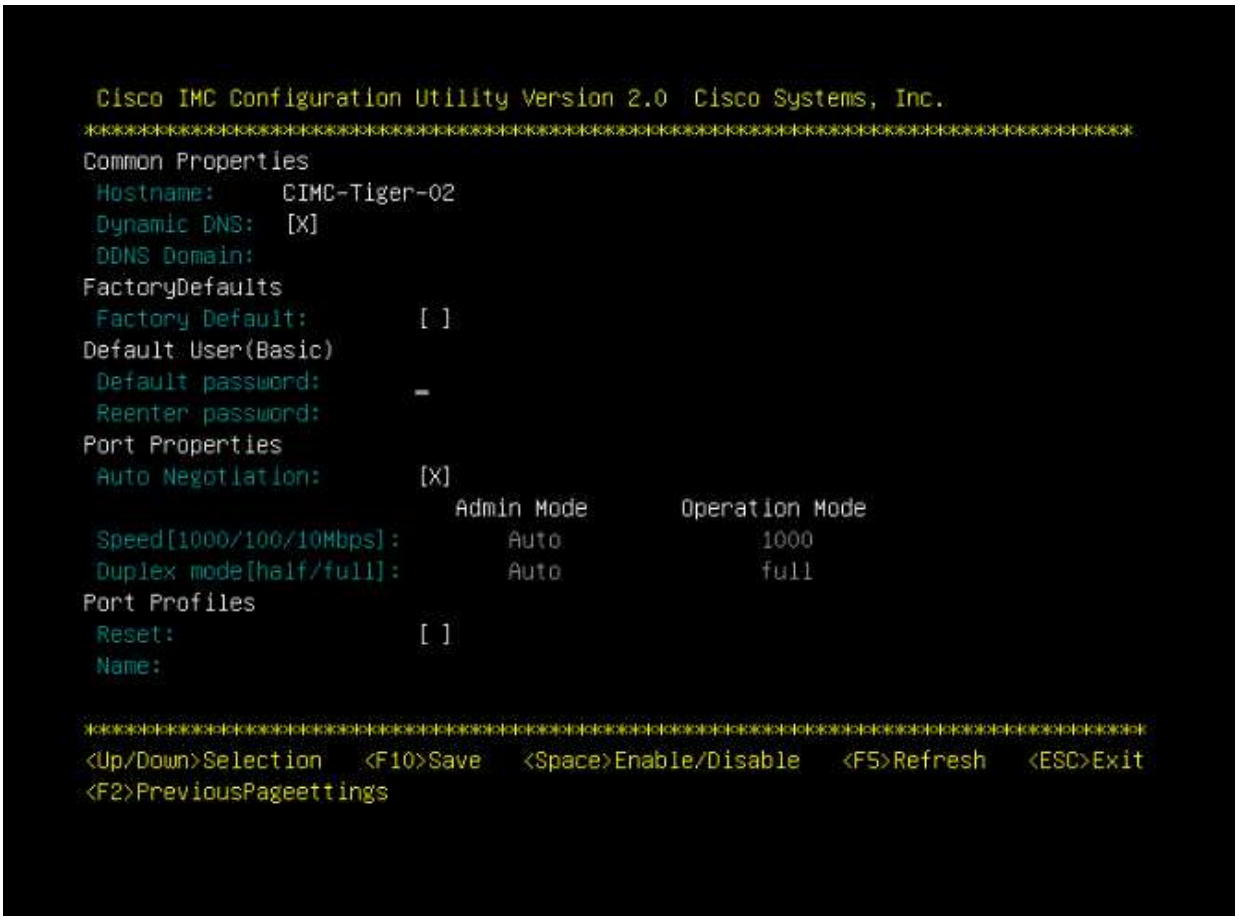
1. 서버와 함께 제공된 Cisco 키보드, 비디오 및 마우스(KVM) 동글을 서버 앞의 KVM 포트에 연결합니다. VGA 모니터와 USB 키보드의 플러그를 적절한 KVM 동글 포트에 꽂습니다.
2. 서버의 전원을 켜고 CIMC 구성을 시작할지 묻는 메시지가 표시되면 F8 키를 누릅니다.



3. CIMC 구성 유틸리티에서 다음 옵션을 설정합니다.
   - 네트워크 인터페이스 카드(NIC) 모드:
     - 전용 [X]
   - IP(기본):
     - IPv4: [X]
     - DHCP 활성화: [ ]
     - CIMC IP:<<CIMC_IP>>
     - 접두사/서브넷:\< CIMC_Netmask>>
     - 게이트웨이:<<CIMC_Gateway>>
   - VLAN(고급): VLAN 태깅을 사용하지 않도록 설정하려면 선택되지 않은 상태로 둡니다.
     - NIC 이중화
     - 없음: [X]



4. 추가 설정을 보려면 F1 키를 누릅니다.
   - 공통 속성:
     - 호스트 이름:\< ESXi_host_name>>
     - 동적 DNS: [ ]
     - 공장 출하시 기본값: 선택하지 않은 상태로 둡니다.
   - 기본 사용자(기본):
     - 기본 암호:<<admin_password>>
     - 암호 <<admin_password>>를 다시 입력하십시오
     - 포트 속성: 기본값을 사용합니다.
     - 포트 프로파일: 선택하지 않은 상태로 둡니다.



5. F10 키를 눌러 CIMC 인터페이스 구성을 저장합니다.
6. 구성을 저장한 후 Esc 키를 눌러 종료합니다.

Cisco UCS C-Series 서버 iSCSI 부팅을 구성합니다

이 FlexPod Express 구성에서 VIC1387은 iSCSI 부팅에 사용됩니다.

다음 표에는 iSCSI 부트를 구성하는 데 필요한 정보가 나와 있습니다.

기울임꼴로 표시된 글꼴은 각 ESXi 호스트에 대해 고유한 변수를 나타냅니다.

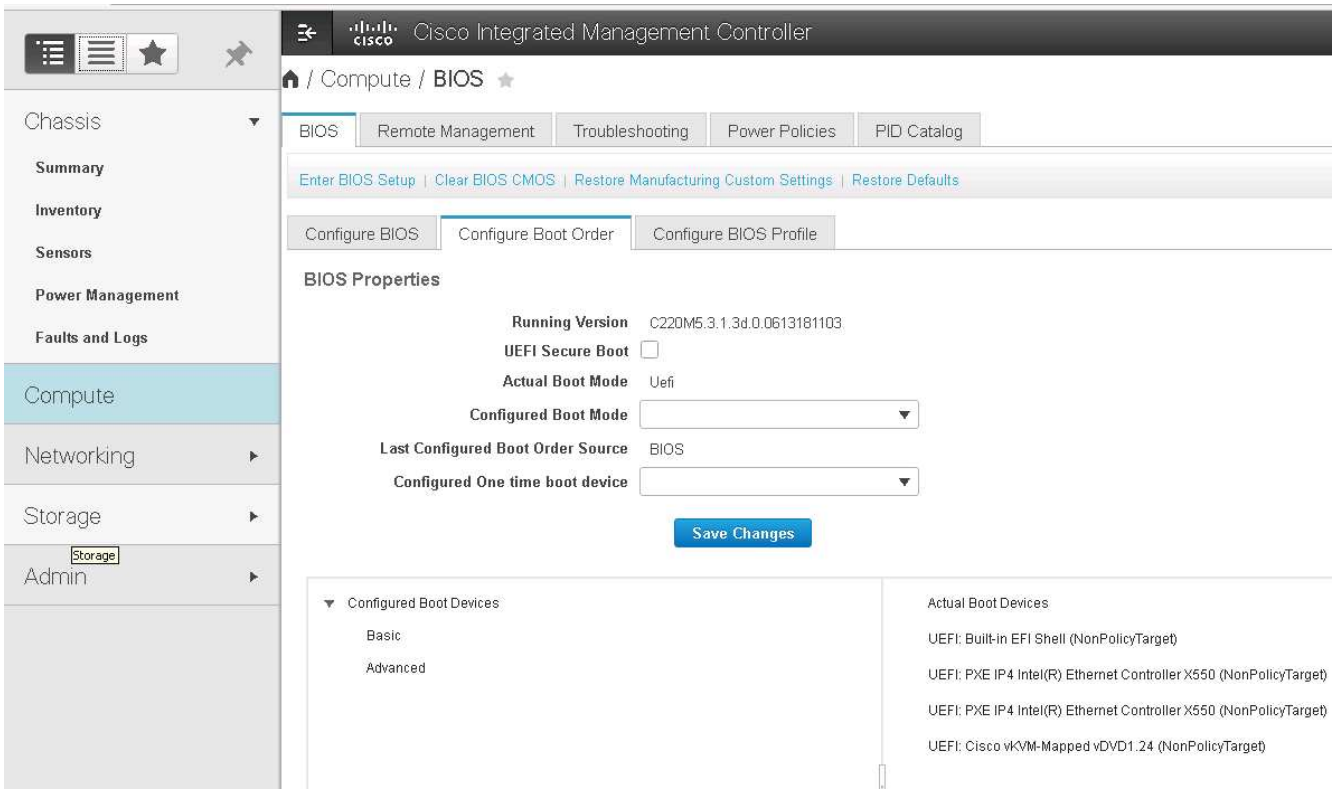
세부 정보	상세 값
ESXi 호스트 이니시에이터에서 이름을 입력합니다	<<var_UCS_initiator_name_a>>
ESXi 호스트 iSCSI - A IP	<<var_esxi_host_iscsiA_ip>>
ESXi 호스트 iSCSI - 네트워크 마스크입니다	<<var_esxi_host_iscsiA_mask>>
ESXi 호스트 iSCSI 기본 게이트웨이입니다	<<var_esxi_host_iscsiA_gateway>>
ESXi 호스트 이니시에이터 B 이름입니다	<<var_UCS_initiator_name_B>>
ESXi 호스트 iSCSI-B IP	<<var_esxi_host_iscsiB_ip>>
ESXi 호스트 iSCSI-B 네트워크 마스크	<<var_esxi_host_iscsiB_mask>>
ESXi 호스트 iSCSI-B 게이트웨이	<<var_esxi_host_iscsiB_gateway>>

세부 정보	상세 값
IP 주소 iscsi_liff 01a	
IP 주소 iscsi_lif02a	
IP 주소 iscsi_liff 01b	
IP 주소 iscsi_liff 02b	
infra_SVM IQN을 선택합니다	

부팅 순서 구성

부팅 순서 구성을 설정하려면 다음 단계를 수행하십시오.

1. CIMC 인터페이스 브라우저 창에서 Server 탭을 클릭하고 BIOS를 선택합니다.
2. Configure Boot Order(부팅 순서 구성) 를 클릭한 다음 OK(확인) 를 클릭합니다.



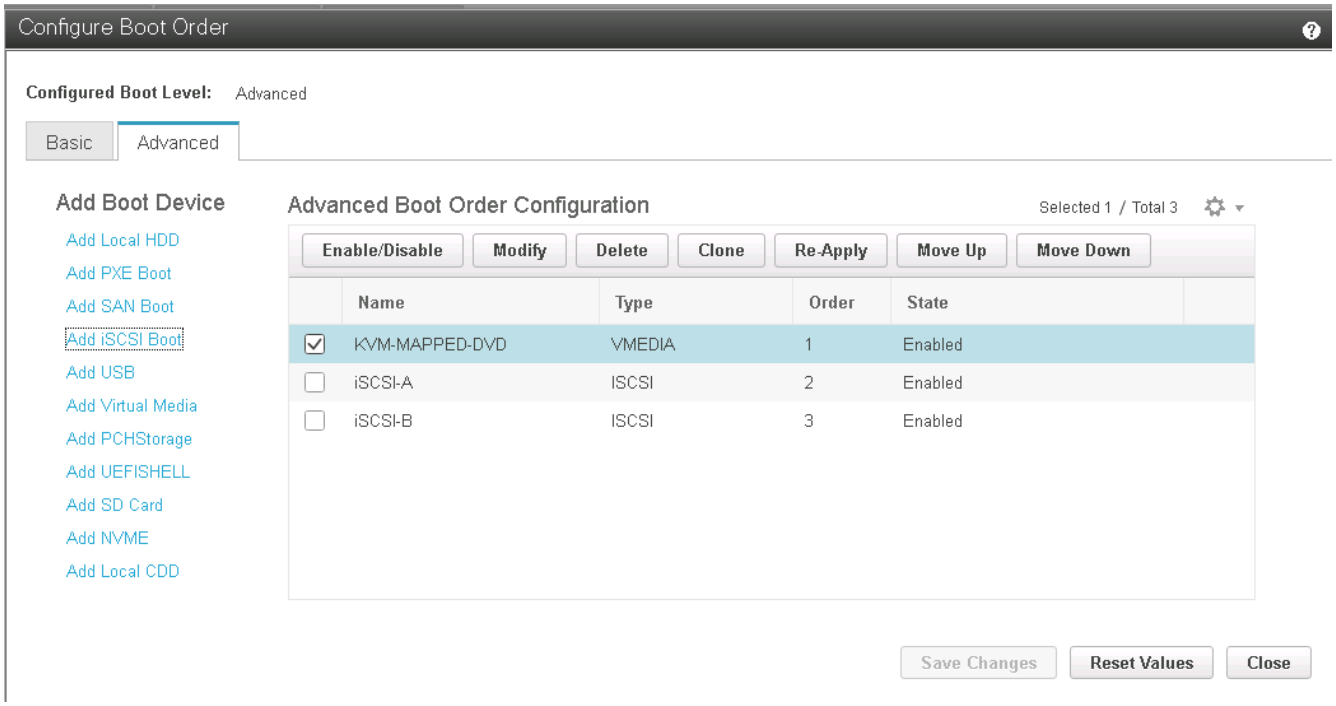
3. Add Boot Device(부팅 장치 추가) 에서 장치를 클릭하고 Advanced(고급) 탭으로 이동하여 다음 장치를 구성합니다.
   - 가상 미디어를 추가합니다
     - 이름: kvm-cd-dvd
     - 하위 유형: KVM 매핑된 DVD
     - 상태: 활성화됨
     - 순서: 1
   - iSCSI 부트를 추가합니다.

- 이름: iscsi-a
- 상태: 활성화됨
- 주문: 2
- 슬롯: mLOM
- 포트: 0

◦ Add iSCSI Boot 를 클릭합니다.

- 이름: iSCSI-B
- 상태: 활성화됨
- 순서: 3
- 슬롯: mLOM
- 포트: 1

4. 장치 추가를 클릭합니다.
5. 변경 내용 저장 을 클릭한 다음 닫기 를 클릭합니다.



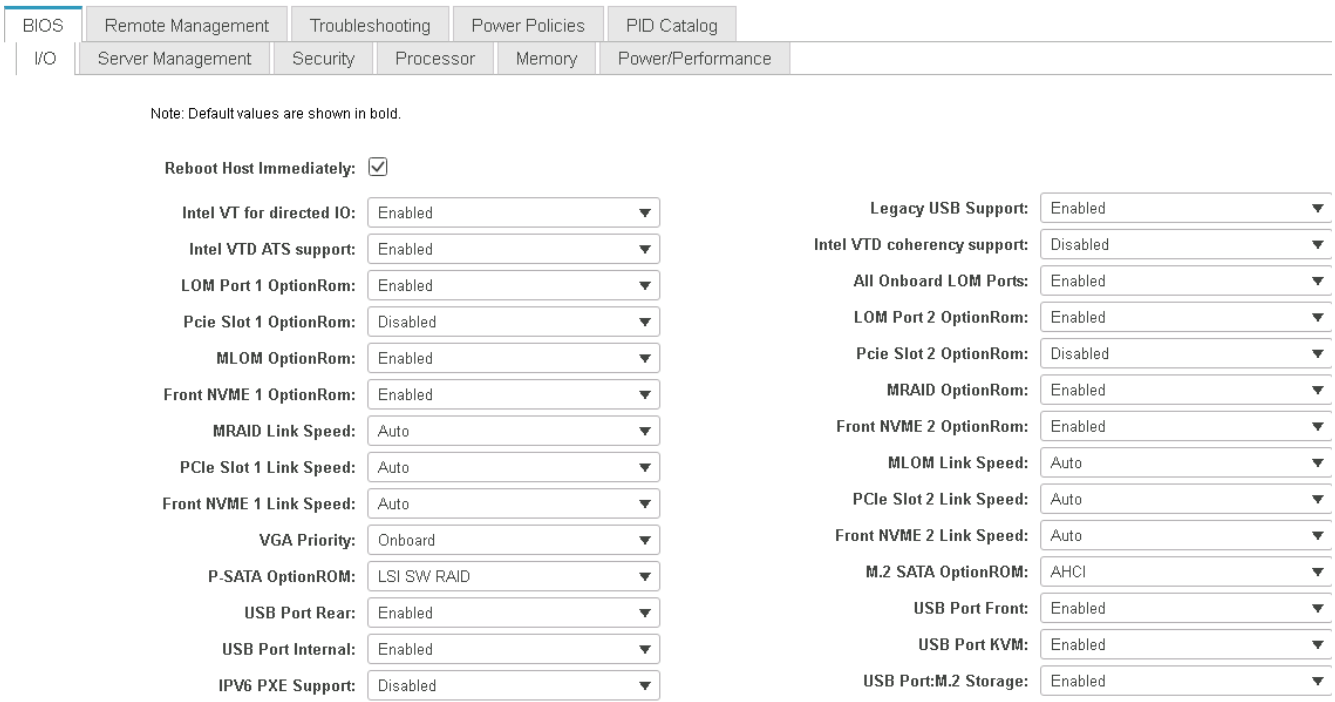
6. 새 부팅 순서로 부팅하려면 서버를 재부팅합니다.

RAID 컨트롤러 비활성화(있는 경우)

C 시리즈 서버에 RAID 컨트롤러가 포함되어 있는 경우 다음 단계를 수행하십시오. SAN 구성으로 부팅할 때 RAID 컨트롤러가 필요하지 않습니다. 선택적으로 서버에서 RAID 컨트롤러를 물리적으로 제거할 수도 있습니다.

1. CIMC의 왼쪽 탐색 창에서 BIOS를 클릭합니다.
2. Configure BIOS 를 선택합니다.
3. PCIe 슬롯: HBA 옵션 ROM으로 아래로 스크롤합니다.

4. 이 값이 아직 비활성화되지 않은 경우 비활성화로 설정합니다.



iSCSI 부트에 대해 **Cisco VIC1387**을 구성합니다

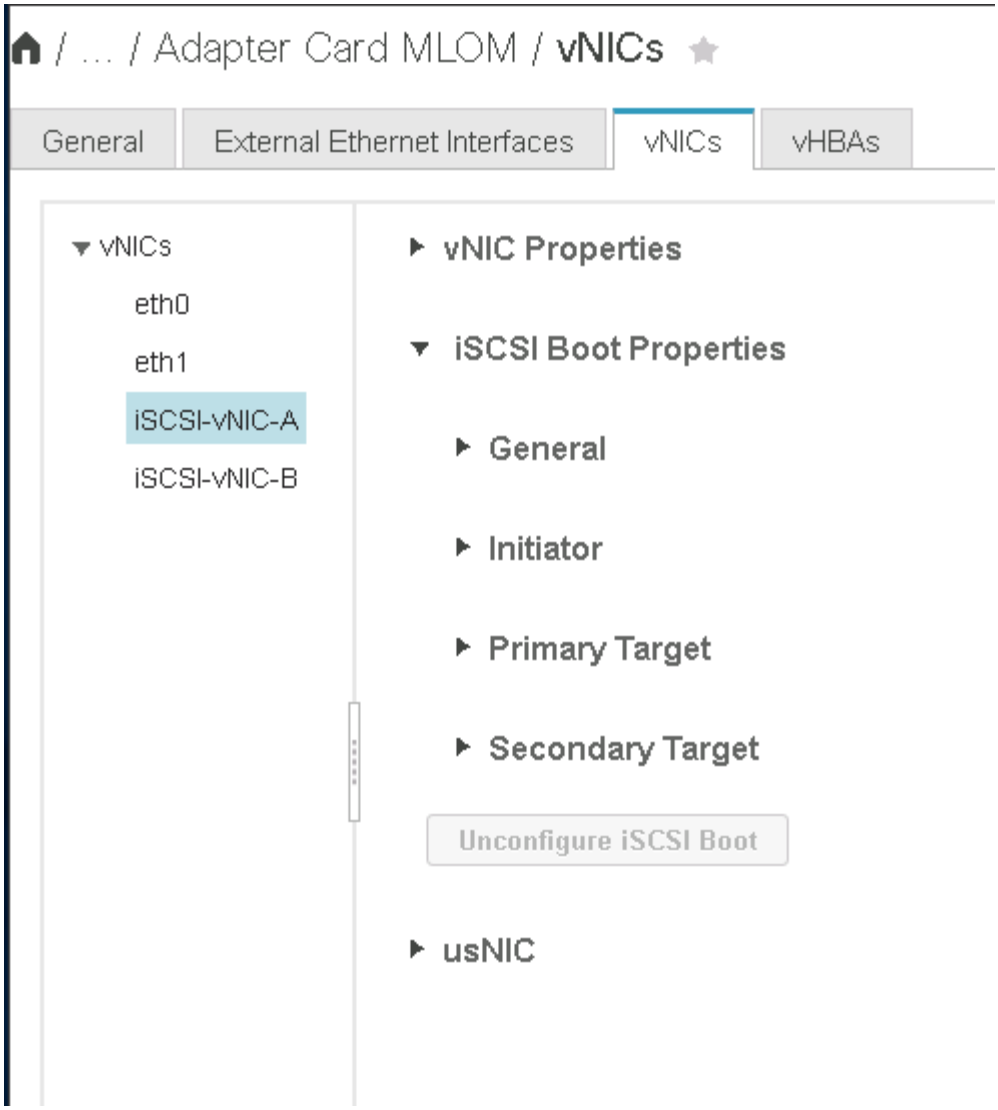
다음 구성 단계는 iSCSI 부트에 대한 Cisco VIC 1387에 대한 것입니다.

iSCSI vNIC를 생성합니다

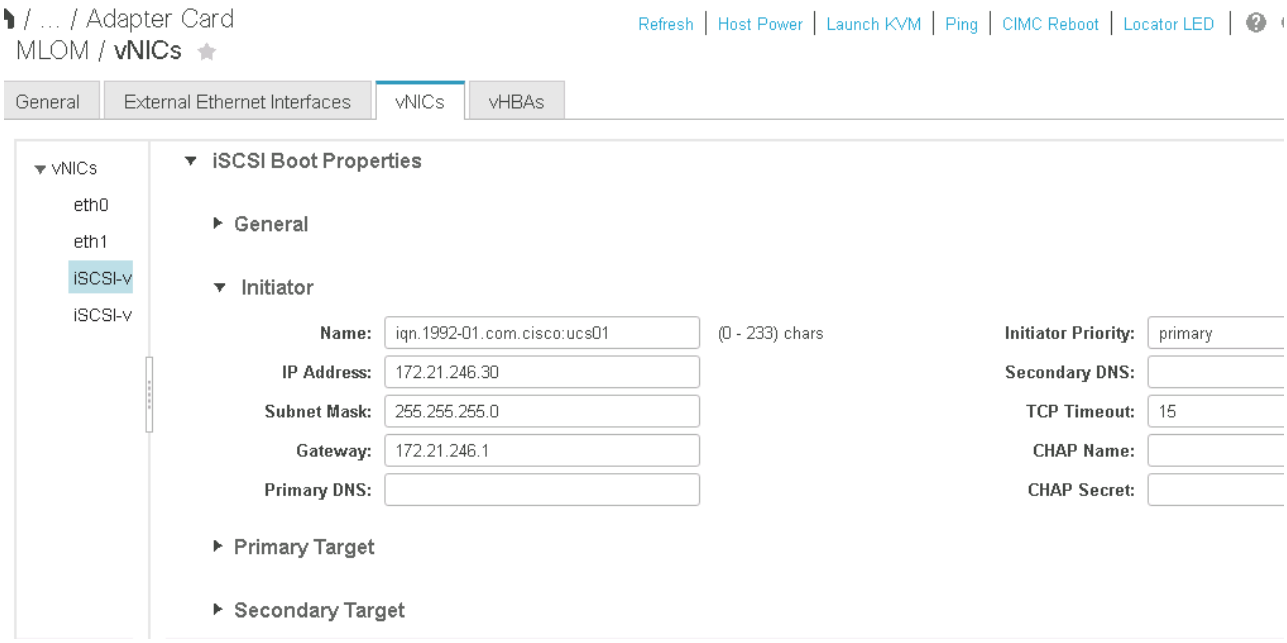
1. 추가 를 클릭하여 vNIC를 생성합니다.
2. vNIC 추가 섹션에서 다음 설정을 입력합니다.
   - 이름: iscsi-vNIC-A
   - MTU: 9000
   - 기본 VLAN:<<var_iscsi_vlan_a>>'입니다
   - VLAN 모드: 트렁크
   - PXE 부팅 활성화: 확인



3. vNIC 추가 를 클릭한 다음 확인 을 클릭합니다.
4. 이 과정을 반복하여 두 번째 vNIC를 추가합니다.
   a. vNIC의 이름을 iSCSI-vNIC-B로 지정합니다.
   b. VLAN으로 '<<var_iscsi_vlan_b>>'를 입력합니다.
   c. 업링크 포트를 "1"로 설정합니다.
5. 왼쪽에서 vNIC의 iSCSI-vNIC-A를 선택합니다.



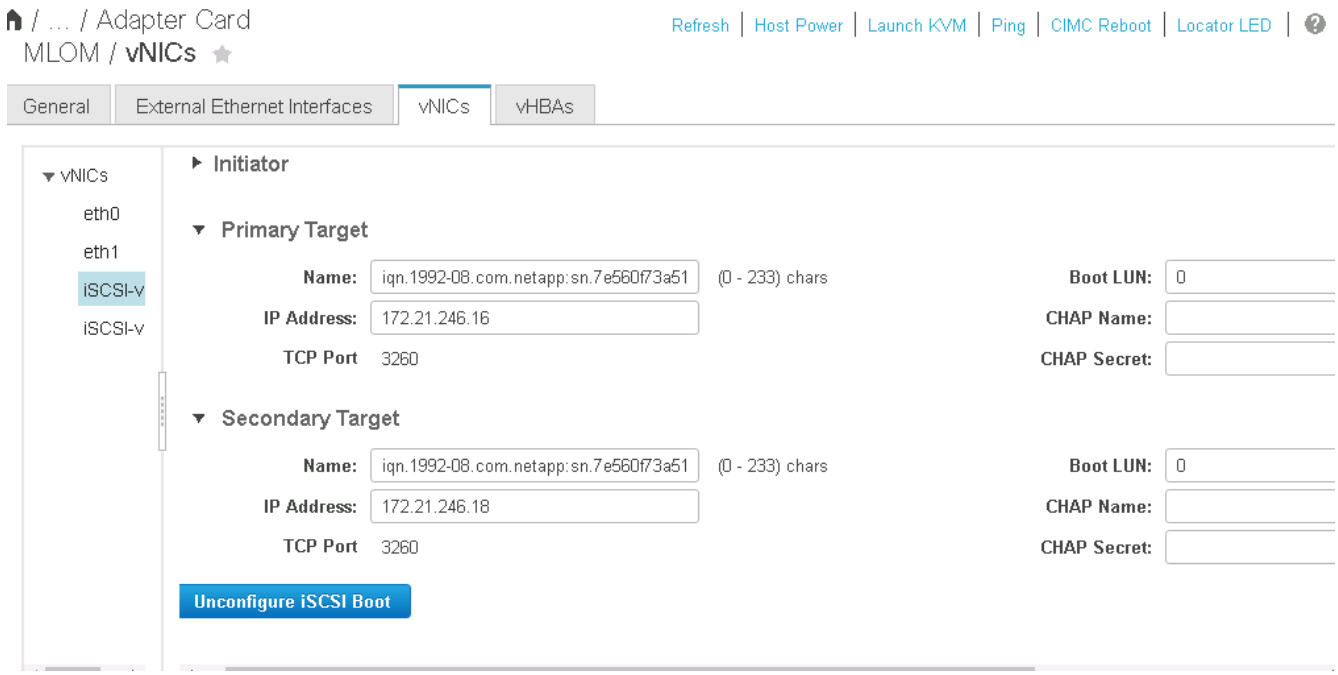
6. iSCSI 부트 속성에서 이니시에이터 세부 정보를 입력합니다.
   - 이름:<<var_ucsa_initiator_name_a>>
   - IP 주소:<<var_esxi_hostA_iscsiA_ip>>
   - 서브넷 마스크:<<var_esxi_hostA_iscsiA_mask>>
   - 게이트웨이:<<var_esxi_hostA_iscsiA_gateway>>



7. 기본 타겟 세부 정보를 입력합니다.
   - 이름: 인프라 SVM의 IQN 번호입니다
   - IP 주소: iSCSI_liff 01a IP 주소
   - 부팅 LUN: 0
8. 2차 타겟 세부 정보를 입력합니다.
   - 이름: 인프라 SVM의 IQN 번호입니다
   - IP address: iSCSI_liff 02a의 IP 주소입니다
   - 부팅 LUN: 0

   "vserver iscsi show" 명령을 실행하여 스토리지 IQN 번호를 확인할 수 있습니다.

   각 vNIC의 IQN 이름을 기록해야 합니다. 나중에 필요한 단계일 수 있습니다.



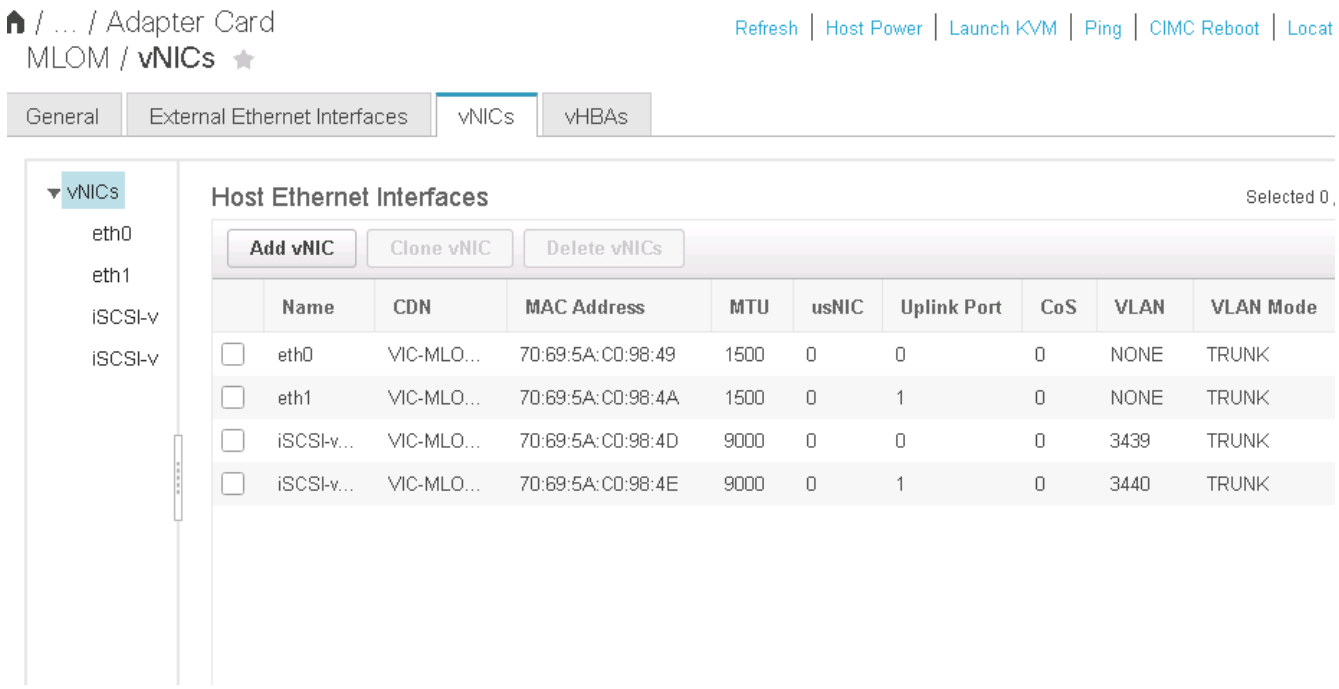
9. Configure iSCSI 를 클릭합니다.
10. vNIC의 iSCSI-vNIC-B를 선택하고 Host Ethernet Interfaces 섹션 상단에 있는 iSCSI Boot 버튼을 클릭합니다.
11. 이 과정을 반복하여 iSCSI-vNIC-B를 구성합니다.
12. 이니시에이터 세부 정보를 입력합니다.
    - 이름:<<var_ucsa_initiator_name_b>>'
    - IP 주소: "<<var_esxi_hostB_iscsib_ip>>"
    - 서브넷 마스크: "<<var_esxi_hostB_iscsib_mask>>"
    - 게이트웨이:\<<var_esxi_hostB_iscsib_gateway>'
13. 기본 타겟 세부 정보를 입력합니다.
    - 이름: 인프라 SVM의 IQN 번호입니다
    - IP 주소: iSCSI_liff 01b 의 IP 주소입니다
    - 부팅 LUN: 0
14. 2차 타겟 세부 정보를 입력합니다.
    - 이름: 인프라 SVM의 IQN 번호입니다
    - IP 주소: iSCSI_liff 02b의 IP 주소입니다
    - 부팅 LUN: 0

    "vserver iscsi show" 명령을 사용하여 스토리지 IQN 번호를 가져올 수 있습니다.

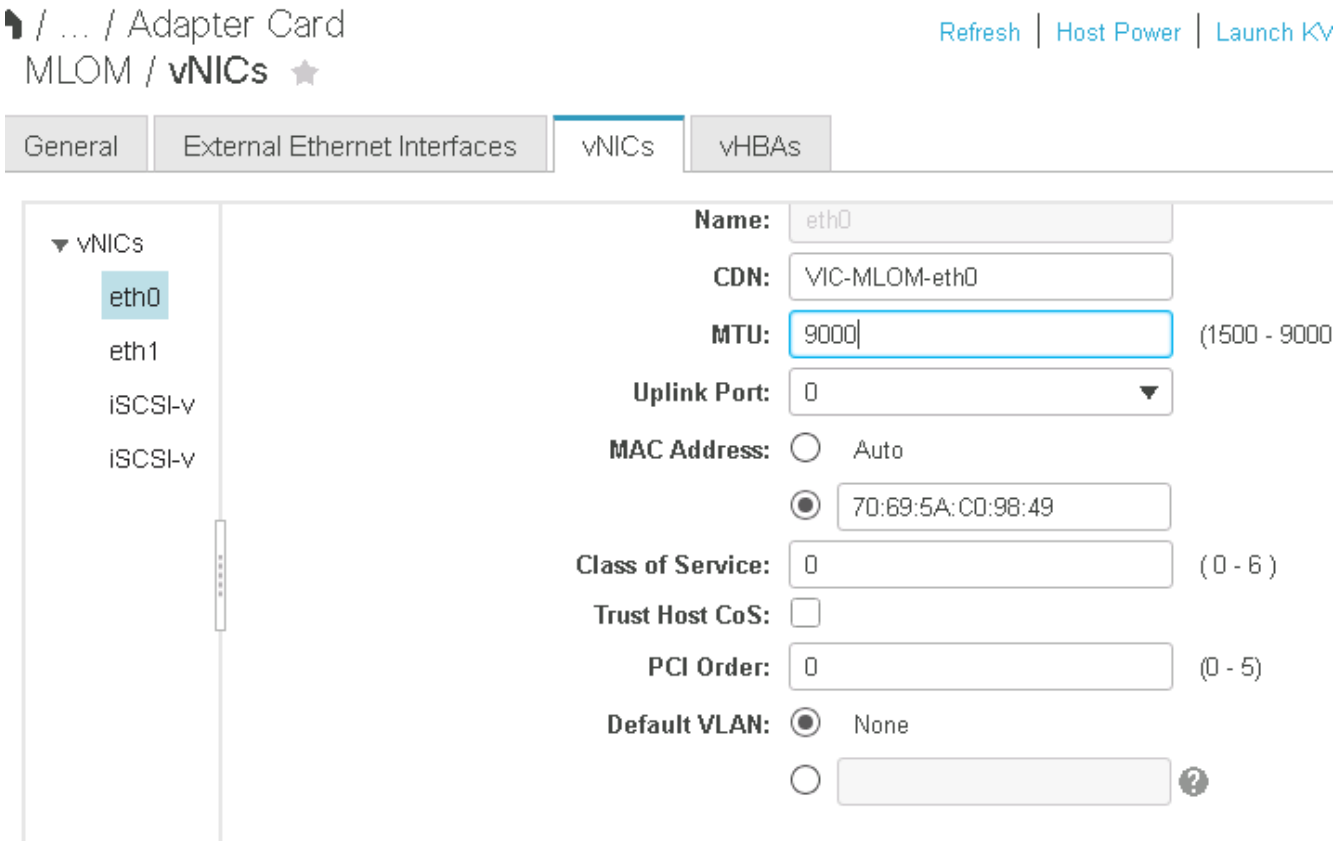
    각 vNIC의 IQN 이름을 기록해야 합니다. 나중에 필요한 단계일 수 있습니다.
15. Configure iSCSI 를 클릭합니다.
16. 이 프로세스를 반복하여 Cisco UCS 서버 B에 대한 iSCSI 부팅을 구성합니다

ESXi용 vNIC를 구성합니다

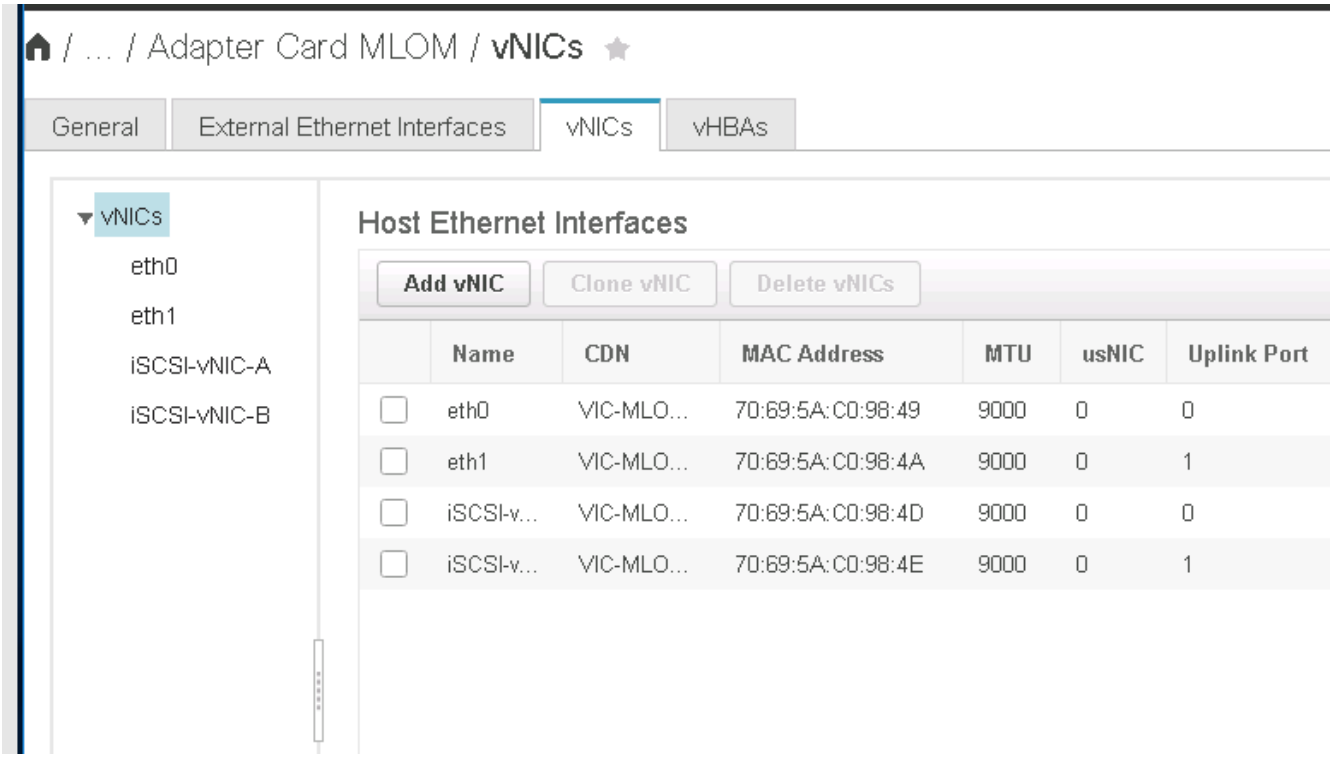
1. CIMC 인터페이스 브라우저 창에서 인벤토리 를 클릭한 다음 오른쪽 창에서 Cisco VIC 어댑터 를 클릭합니다.
2. 어댑터 카드 아래에서 Cisco UCS VIC 1387을 선택한 다음 아래에서 vNIC를 선택합니다.



3. eth0 을 선택하고 속성 을 클릭합니다.
4. MTU를 9000으로 설정합니다. 변경 내용 저장 을 클릭합니다.



5. eth1에 대해 3단계와 4단계를 반복하여 업링크 포트가 eth1에 대해 "1"로 설정되어 있는지 확인합니다.



이 절차는 각 초기 Cisco UCS 서버 노드 및 환경에 추가된 각 추가 Cisco UCS 서버 노드에 대해 반복해야 합니다.

"다음: NetApp AFF 스토리지 구현 절차(2부)"

NetApp AFF 스토리지 구현 절차(2부)

ONTAP SAN 부팅 스토리지 설정

iSCSI igroup을 생성합니다

Igroup을 생성하려면 다음 단계를 완료하십시오.

이 단계를 위해서는 서버 구성에서 iSCSI 이니시에이터 IQN이 필요합니다.

1. 클러스터 관리 노드의 SSH 연결에서 다음 명령을 실행합니다. 이 단계에서 생성한 3개의 igroup을 보려면 igroup show 명령을 실행합니다.

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-A –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_a_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-B –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_b_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```

Cisco UCS C-Series 서버를 추가할 때는 이 단계를 완료해야 합니다.

부팅 LUN을 igroup에 매핑합니다

부트 LUN을 igroup에 매핑하려면 클러스터 관리 SSH 연결에서 다음 명령을 실행합니다.

```
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra- A –igroup
VM-Host-Infra- A –lun-id 0
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra- B –igroup
VM-Host-Infra- B –lun-id 0
```

Cisco UCS C-Series 서버를 추가할 때는 이 단계를 완료해야 합니다.

"다음: VMware vSphere 6.7 구축 절차."

VMware vSphere 6.7 구축 절차

이 섹션에서는 FlexPod Express 구성에 VMware ESXi 6.7을 설치하는 절차를 자세히 설명합니다. 다음 구현 절차는 이전 섹션에서 설명한 환경 변수를 포함하도록 커스터마이징되었습니다.

이러한 환경에 VMware ESXi를 설치하는 방법은 여러 가지가 있습니다. 이 절차에서는 Cisco UCS C-Series 서버용 CIMC 인터페이스의 가상 KVM 콘솔과 가상 미디어 기능을 사용하여 원격 설치 미디어를 각 개별 서버에 매핑합니다.

이 절차는 Cisco UCS 서버 A 및 Cisco UCS 서버 B에 대해 완료되어야 합니다

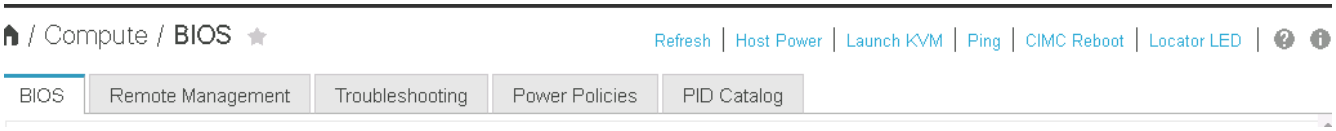
클러스터에 추가된 노드에 대해 이 절차를 완료해야 합니다.

Cisco UCS C-Series 독립 실행형 서버에 대한 CIMC 인터페이스에 로그인합니다

다음 단계에서는 Cisco UCS C-Series 독립 실행형 서버의 CIMC 인터페이스에 로그인하는 방법을 자세히 설명합니다. CIMC 인터페이스에 로그인하여 가상 KVM을 실행해야 관리자가 원격 미디어를 통해 운영 체제 설치를 시작할 수 있습니다.

모든 호스트

1. 웹 브라우저로 이동하고 Cisco UCS C-Series의 CIMC 인터페이스에 대한 IP 주소를 입력합니다. 이 단계에서는 CIMC GUI 애플리케이션이 시작됩니다.
2. 관리자의 사용자 이름과 자격 증명을 사용하여 CIMC UI에 로그인합니다.
3. 주 메뉴에서 서버 탭을 선택합니다.
4. Launch KVM Console을 클릭합니다.



5. 가상 KVM 콘솔에서 Virtual Media 탭을 선택합니다.
6. CD/DVD 매핑 을 선택합니다.

먼저 가상 디바이스 활성화 를 클릭해야 할 수도 있습니다. 메시지가 표시되면 이 세션 수락 을 선택합니다.

7. VMware ESXi 6.7 설치 관리자 ISO 이미지 파일을 찾아 이동하고 Open을 클릭합니다. 장치 매핑 을 클릭합니다.
8. Power 메뉴를 선택하고 Power Cycle System (Cold Boot) 을 선택합니다. 예 를 클릭합니다.

VMware ESXi를 설치합니다

다음 단계에서는 각 호스트에 VMware ESXi를 설치하는 방법을 설명합니다.

ESXi 6.7 Cisco 사용자 지정 이미지를 다운로드합니다

1. 로 이동합니다 "VMware vSphere 다운로드 페이지" 사용자 정의 ISO의 경우.
2. Cisco Custom Image for ESXi 6.7 GA Install CD(ESXi 6.7 GA 설치 CD용 Cisco 사용자 지정 이미지) 옆의 Go to Downloads(다운로드로 이동) 를 클릭합니다.
3. ESXi 6.7 GA 설치 CD(ISO)용 Cisco Custom Image를 다운로드합니다.

모든 호스트

1. 시스템이 부팅되면 VMware ESXi 설치 미디어의 존재 여부가 자동으로 감지됩니다.
2. 나타나는 메뉴에서 VMware ESXi 설치 프로그램을 선택합니다.

설치 프로그램이 로드됩니다. 이 작업은 몇 분 정도 걸립니다.

3. 설치 프로그램 로드가 완료된 후 Enter 키를 눌러 설치를 계속합니다.
4. 최종 사용자 사용권 계약을 읽은 후 동의하고 F11 키를 눌러 설치를 계속합니다.
5. 이전에 ESXi용 설치 디스크로 설정된 NetApp LUN을 선택하고 Enter 키를 눌러 설치를 계속합니다.



6. 적절한 자판 배열을 선택하고 Enter 키를 누릅니다.
7. 루트 암호를 입력 및 확인하고 Enter 키를 누릅니다.
8. 볼륨에서 기존 파티션이 제거된다는 경고 메시지가 표시됩니다. F11 키를 눌러 설치를 계속합니다. ESXi 설치 후 서버가 재부팅됩니다.

VMware ESXi 호스트 관리 네트워킹을 설정합니다

다음 단계에서는 각 VMware ESXi 호스트의 관리 네트워크를 추가하는 방법을 설명합니다.

모든 호스트

1. 서버 재부팅이 완료된 후 F2 키를 눌러 시스템 커스터마이징 옵션을 시작합니다.
2. root라는 로그인 이름과 이전에 설치 과정에서 입력한 루트 암호를 사용하여 로그인합니다.
3. Configure Management Network 옵션을 선택합니다.
4. Network Adapters 를 선택하고 Enter 키를 누릅니다.
5. vSwitch0에 대해 원하는 포트를 선택합니다. Enter 키를 누릅니다.

> CIMC의 eth0 및 eth1에 해당하는 포트를 선택합니다.



6. VLAN (optional)을 선택하고 Enter 키를 누릅니다.
7. VLAN ID '<<mgmt_vlan_id>>'를 입력합니다. Enter 키를 누릅니다.
8. Configure Management Network 메뉴에서 IPv4 Configuration을 선택하여 관리 인터페이스의 IP 주소를 구성합니다. Enter 키를 누릅니다.
9. 화살표 키를 사용하여 Set Static IPv4 address(정적 IPv4 주소 설정) 를 강조 표시하고 스페이스바를 사용하여 이 옵션을 선택합니다.
10. VMware ESXi 호스트 "\< ESXi_host_mgmt_ip>>"를 관리하기 위한 IP 주소를 입력합니다.
11. VMware ESXi 호스트 "\< ESXi_host_mgmt_netmask>>의 서브넷 마스크를 입력합니다
12. VMware ESXi 호스트 '\< ESXi_host_mgmt_gateway>'의 기본 게이트웨이를 입력합니다.
13. Enter 키를 눌러 IP 구성의 변경 사항을 적용합니다.
14. IPv6 구성 메뉴로 들어갑니다.
15. 스페이스바를 사용하여 IPv6 사용(재시작 필요) 옵션을 선택 취소하여 IPv6을 사용하지 않도록 설정합니다. Enter 키를 누릅니다.
16. DNS 설정을 구성하는 메뉴로 들어갑니다.
17. IP 주소는 수동으로 할당되므로 DNS 정보도 수동으로 입력해야 합니다.
18. Primary DNS 서버의 IP 주소를 입력합니다[nameserver_ip]".
19. (선택 사항) 보조 DNS 서버의 IP 주소를 입력합니다.
20. VMware ESXi 호스트 이름:'에 대한 FQDN을 입력합니다[esxi_host_fqdn]".
21. Enter 키를 눌러 DNS 구성의 변경 사항을 적용합니다.
22. Esc 키를 눌러 Configure Management Network 하위 메뉴를 종료합니다.
23. Y 를 눌러 변경 사항을 확인하고 서버를 재부팅합니다.
24. Esc 키를 눌러 VMware 콘솔에서 로그아웃합니다.

ESXi 호스트를 구성합니다

각 ESXi 호스트를 구성하려면 다음 표의 정보가 필요합니다.

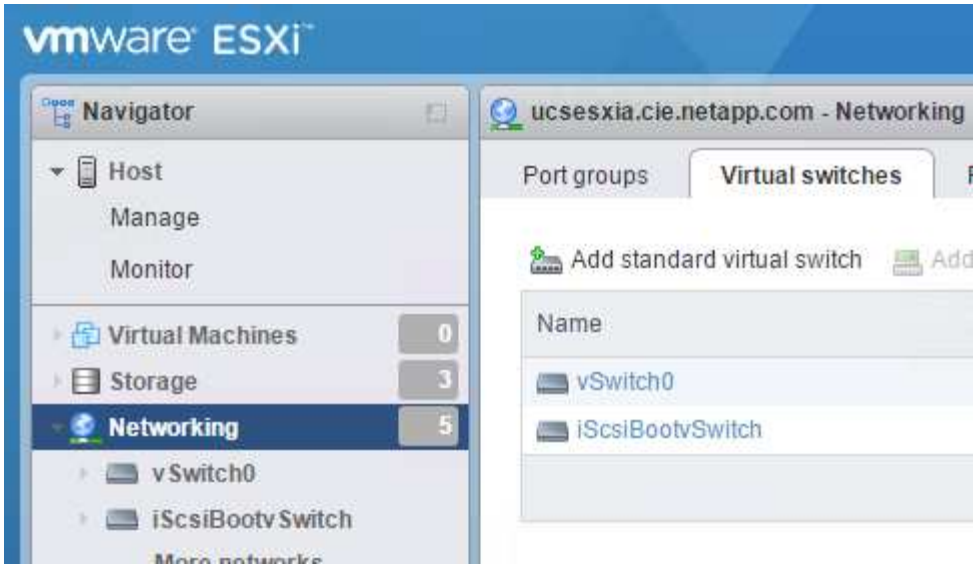
세부 정보	값
ESXi 호스트 이름입니다	
ESXi 호스트 관리 IP입니다	
ESXi 호스트 관리 마스크입니다	
ESXi 호스트 관리 게이트웨이	
ESXi 호스트 NFS IP입니다	
ESXi 호스트 NFS 마스크입니다	
ESXi 호스트 NFS 게이트웨이	
ESXi 호스트 vMotion IP입니다	
ESXi 호스트 vMotion 마스크	
ESXi 호스트 vMotion 게이트웨이	
ESXi 호스트 iSCSI - A IP	
ESXi 호스트 iSCSI - 마스크	
ESXi 호스트 iSCSI - 게이트웨이	
ESXi 호스트 iSCSI-B IP	
ESXi 호스트 iSCSI-B 마스크	
ESXi 호스트 iSCSI-B 게이트웨이	

ESXi 호스트에 로그인합니다

1. 웹 브라우저에서 호스트의 관리 IP 주소를 엽니다.
2. 설치 프로세스 중에 지정한 암호 및 루트 계정을 사용하여 ESXi 호스트에 로그인합니다.
3. VMware 사용자 환경 개선 프로그램에 대한 설명을 읽어 보십시오. 적절한 응답을 선택한 후 OK(확인) 를 클릭합니다.

iSCSI 부트를 구성합니다

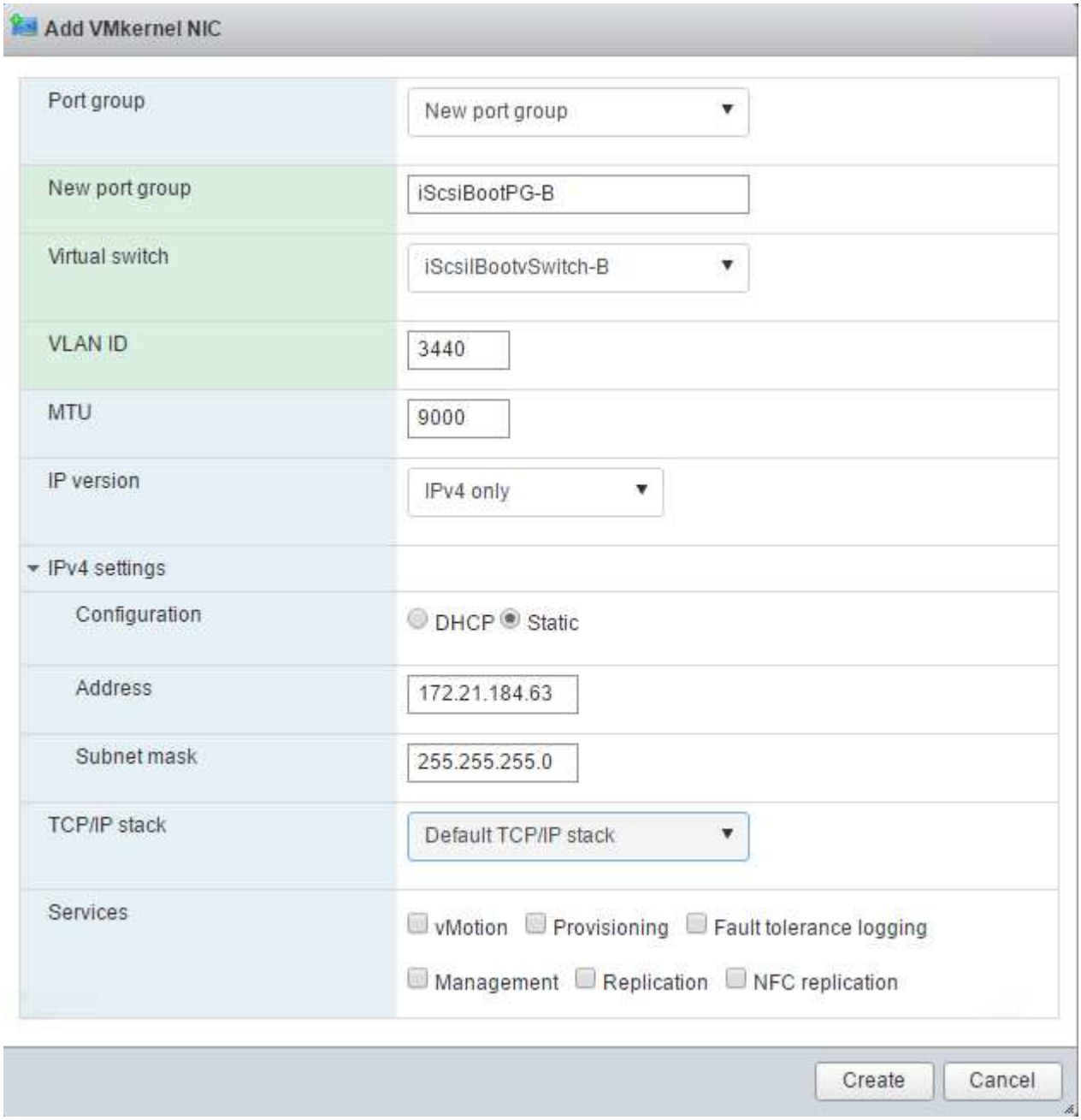
1. 왼쪽에서 네트워킹 을 선택합니다.
2. 오른쪽에서 Virtual Switches 탭을 선택합니다.



3. iSciBootvSwitch 를 클릭합니다.
4. 설정 편집 을 선택합니다.
5. MTU를 9000으로 변경하고 저장 을 클릭합니다.
6. 가상 스위치 탭으로 돌아가려면 왼쪽 탐색 창에서 네트워킹 을 클릭합니다.
7. 표준 가상 스위치 추가를 클릭합니다.
8. vSwitch 이름에 iSciBootvSwitch-B라는 이름을 입력합니다.
   - MTU를 9000으로 설정합니다.
   - 업링크 1 옵션에서 vmnic3을 선택합니다.
   - 추가 를 클릭합니다.

> 이 구성에서는 Vmnic2 및 vmnic3이 iSCSI 부팅에 사용됩니다. ESXi 호스트에 추가 NIC가 있는 경우 vmnic 번호가 다를 수 있습니다. iSCSI 부트에 사용되는 NIC를 확인하려면 CIMC의 iSCSI vNIC의 MAC 주소를 ESXi의 vmnics와 일치시킵니다.

9. 가운데 창에서 VMkernel NIC 탭을 선택합니다.
10. Add VMkernel NIC 를 선택합니다.
    - iScosibootPG-B의 포트 그룹 이름을 새로 지정합니다.
    - 가상 스위치에 대해 iSciBootvSwitch-B를 선택합니다.
    - VLAN ID에 '<<iscsib_vlan_id>>'를 입력합니다.
    - MTU를 9000으로 변경합니다.
    - IPv4 설정 을 확장합니다.
    - 정적 설정을 선택합니다.
    - Address 에 "<<var_hosta_iscsib_ip>>"를 입력합니다.
    - 서브넷 마스크에 '<<var_hosta_iscsib_mask>>'를 입력합니다.
    - 생성 을 클릭합니다.

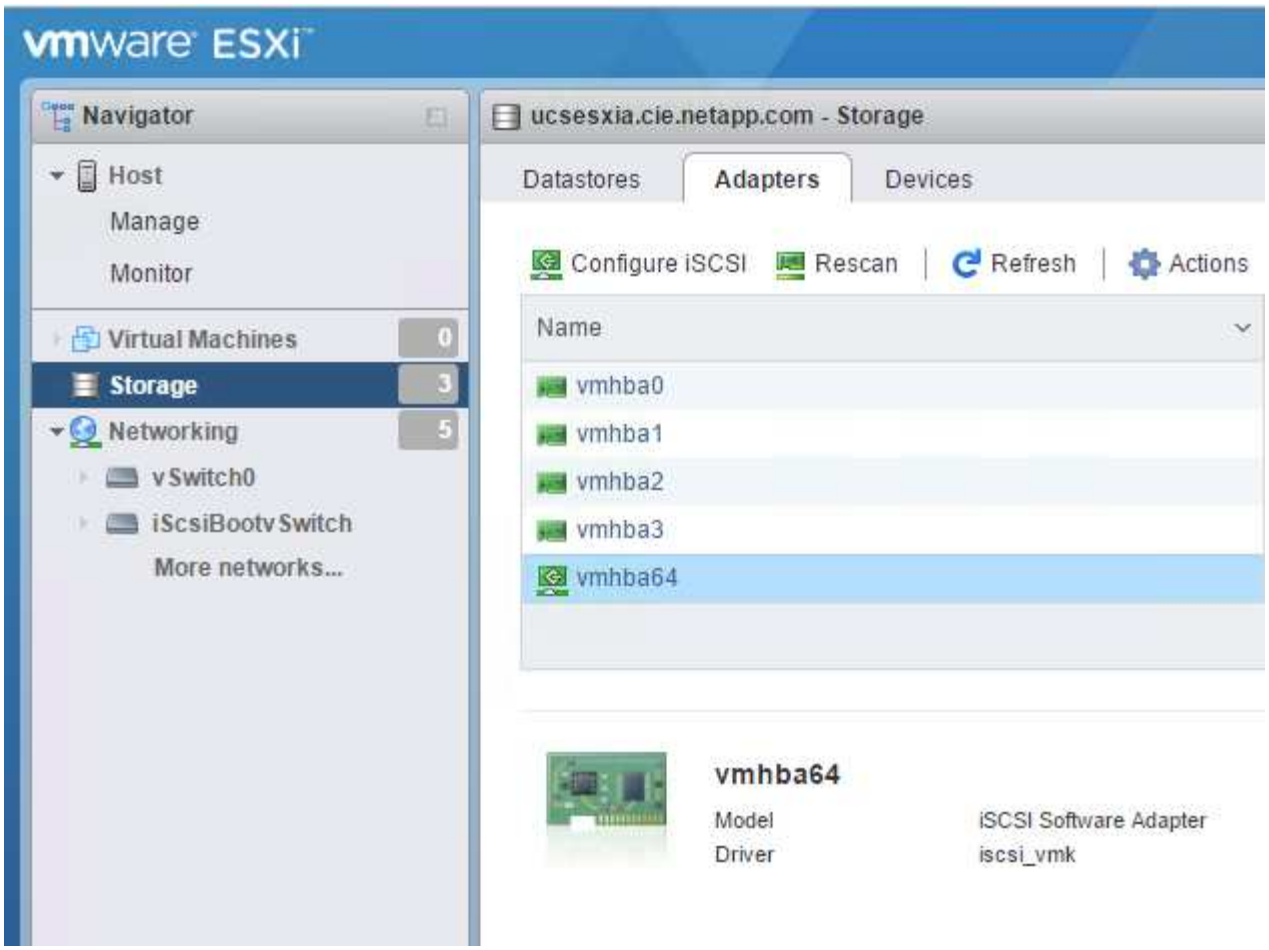


iSciBootPG-A에서 MTU를 9000으로 설정합니다

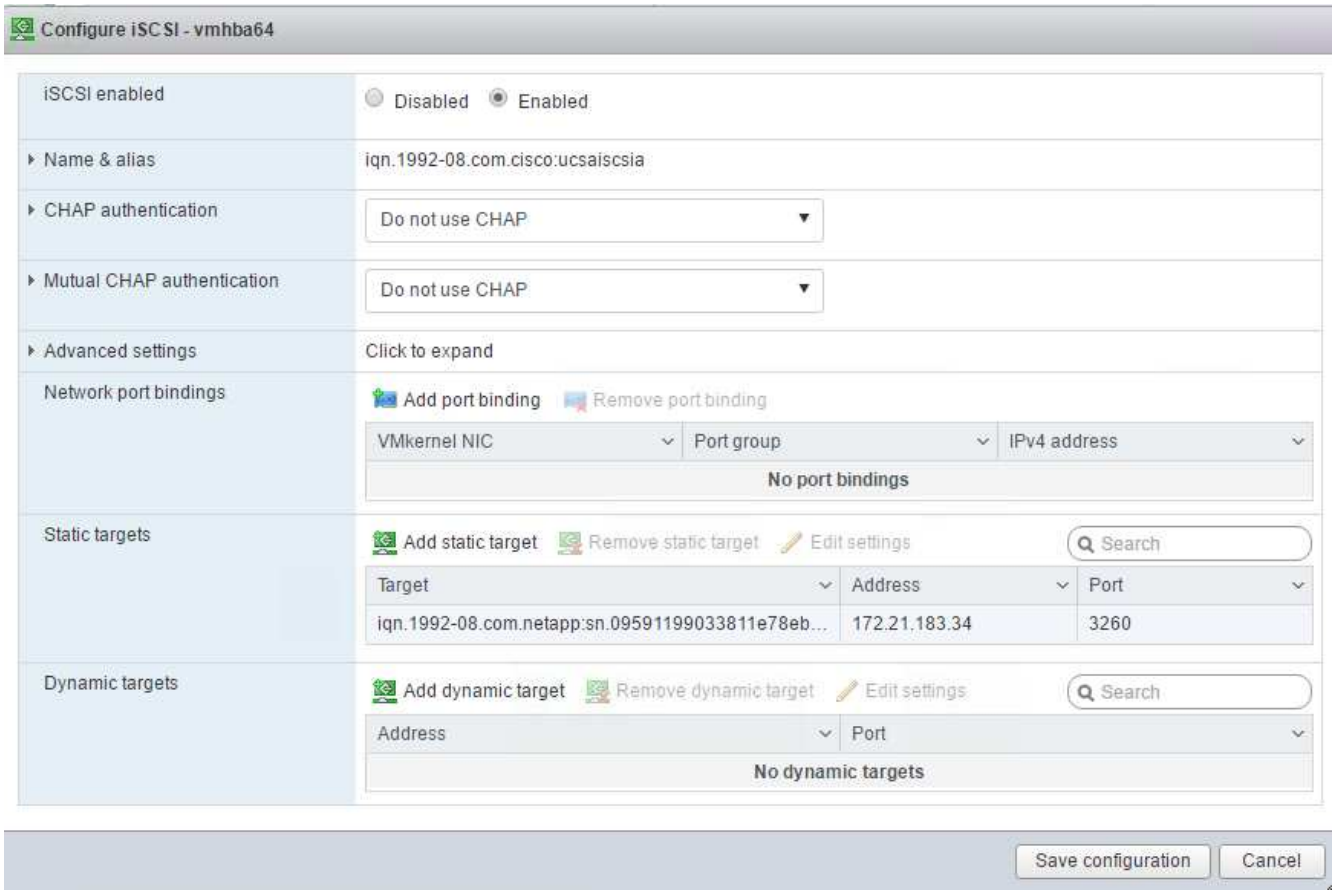
iSCSI 다중 경로를 구성합니다

ESXi 호스트에 iSCSI 다중 경로를 설정하려면 다음 단계를 수행하십시오.

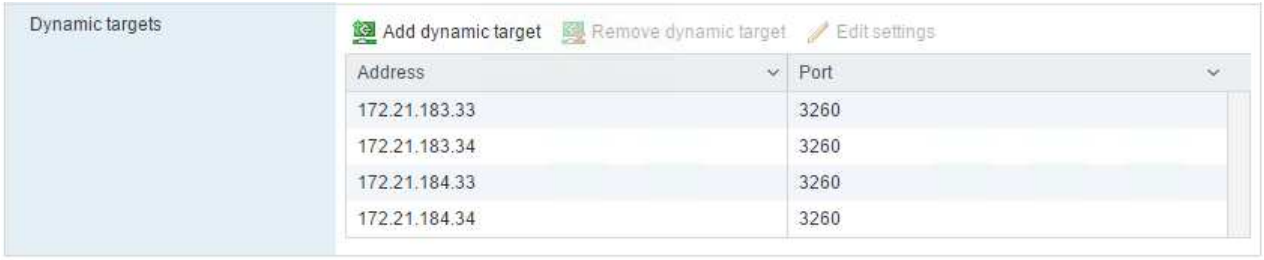
1. 왼쪽 탐색 창에서 스토리지 를 선택합니다. 어댑터를 클릭합니다.
2. iSCSI 소프트웨어 어댑터를 선택하고 iSCSI 구성 을 클릭합니다.



3. 동적 대상에서 동적 대상 추가를 클릭합니다.



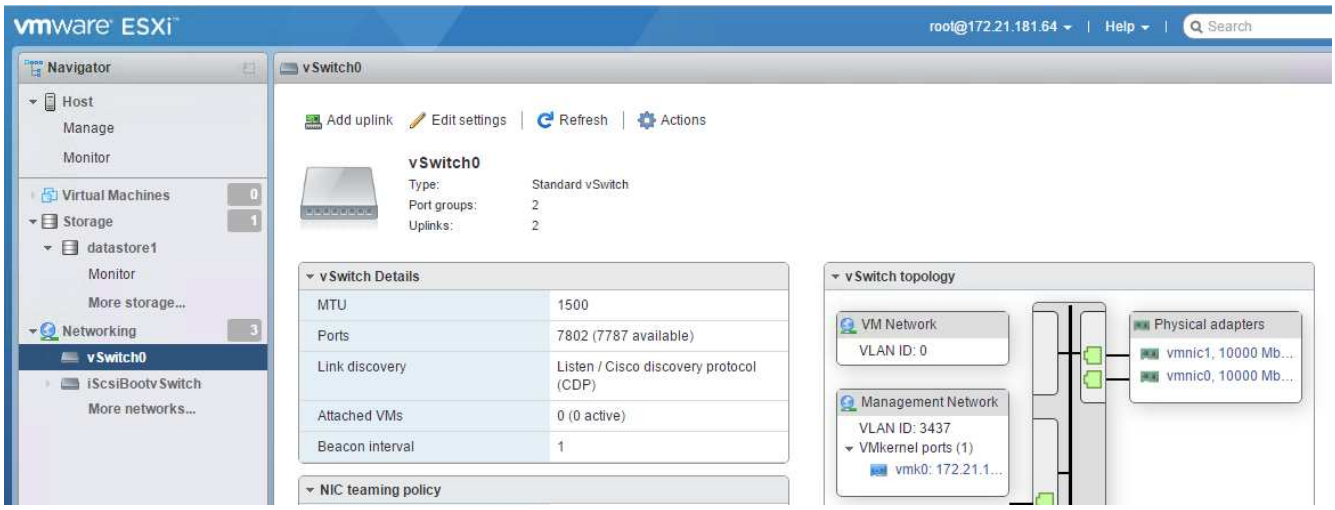
4. IP 주소 'iscsi_lif01a'를 입력합니다.
   - IP 주소 iscsi_liff 01b, iscsi_liff 02a, iscsi_liff 02b와 함께 이 과정을 반복합니다.
   - 구성 저장 을 클릭합니다.



NetApp 클러스터에서 'network interface show' 명령을 실행하거나 OnCommand System Manager에서 네트워크 인터페이스 탭을 확인하여 iSCSI LIF IP 주소를 찾을 수 있습니다.

ESXi 호스트를 구성합니다

1. 왼쪽 탐색 창에서 네트워킹 을 선택합니다.
2. vSwitch0을 선택합니다.



3. 설정 편집 을 선택합니다.
4. MTU를 9000으로 변경합니다.
5. NIC 티밍을 확장하고 vmnic0 및 vmnic1이 모두 활성으로 설정되어 있는지 확인합니다.

포트 그룹 및 **VMkernel NIC**를 구성합니다

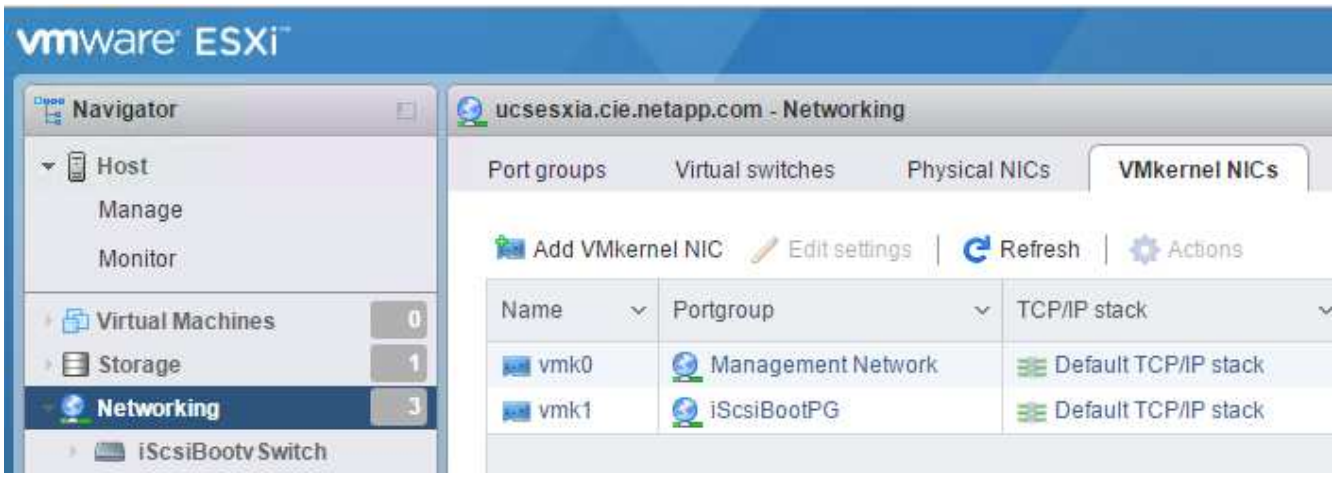
1. 왼쪽 탐색 창에서 네트워킹 을 선택합니다.
2. 포트 그룹 탭을 마우스 오른쪽 단추로 클릭합니다.



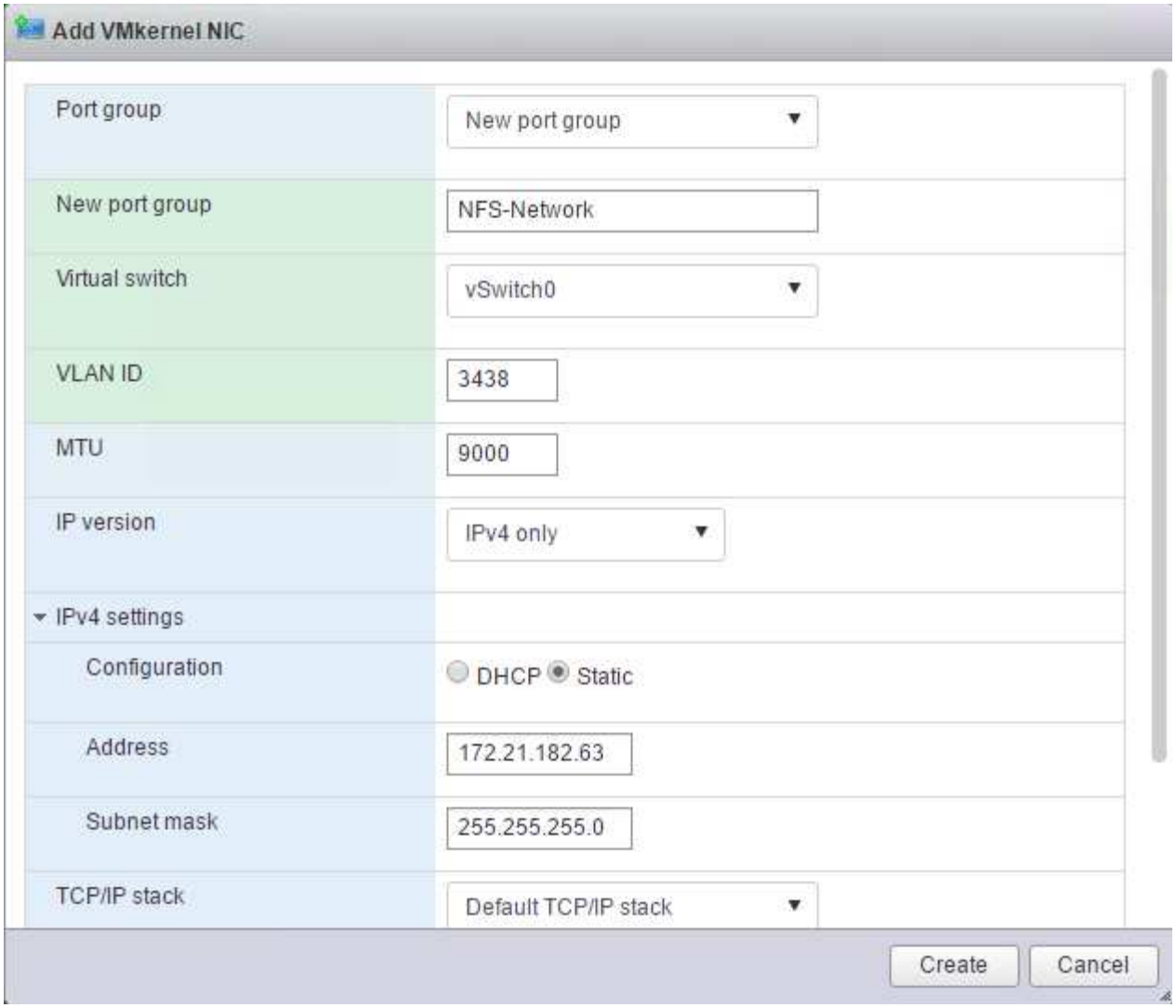
3. VM Network를 마우스 오른쪽 버튼으로 클릭하고 Edit를 선택합니다. VLAN ID를 '<<var_vm_traffic_vlan>>'로 변경합니다.
4. 포트 그룹 추가 를 클릭합니다.
   - 포트 그룹의 이름을 MGMT-Network로 지정합니다.
   - VLAN ID에 '<<mgmt_vlan>>'를 입력합니다.
   - vSwitch0이 선택되어 있는지 확인합니다.

◦ 추가 를 클릭합니다.

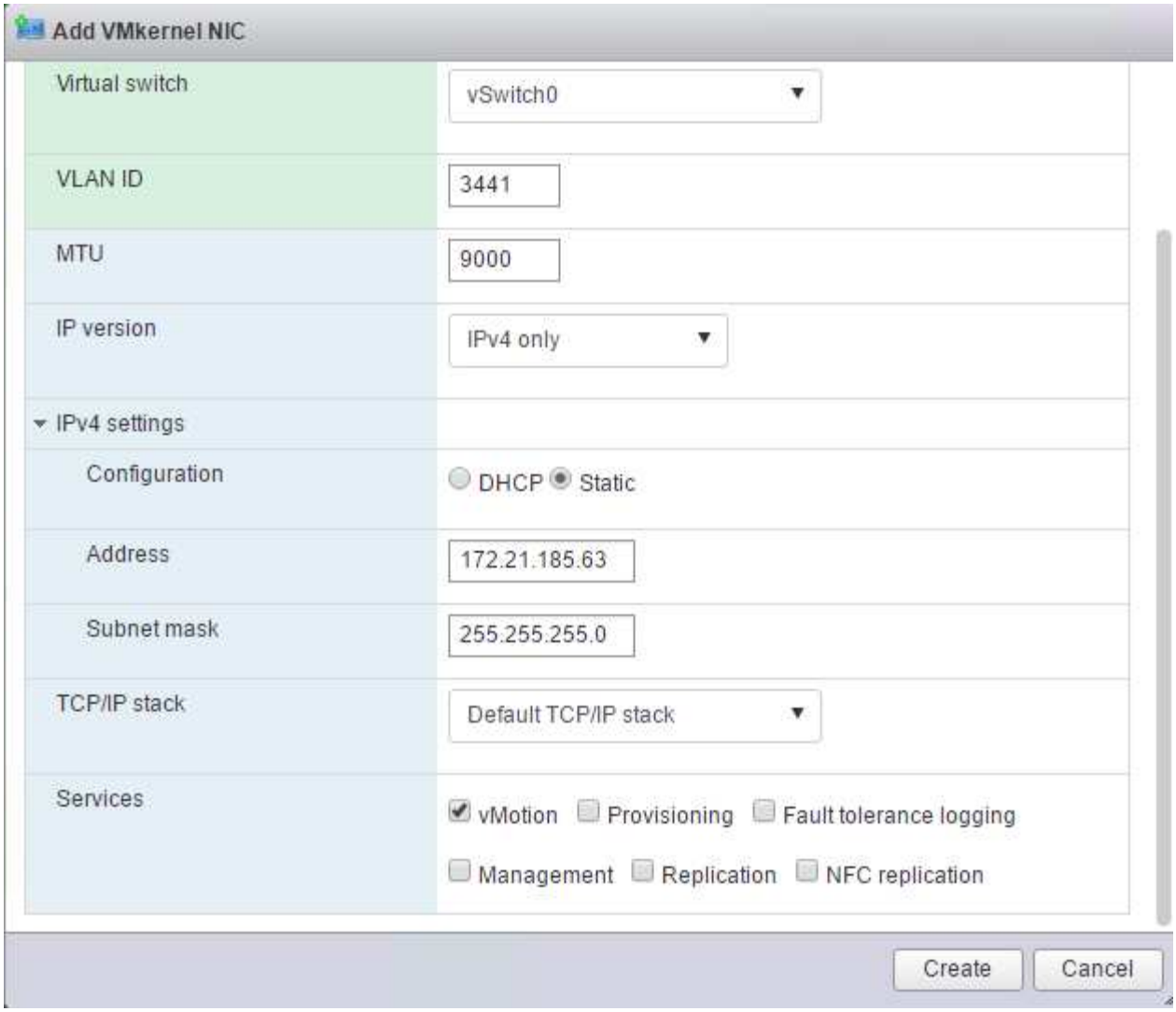
5. VMkernel NIC 탭을 클릭합니다.



6. Add VMkernel NIC 를 선택합니다.
   ◦ 새 포트 그룹을 선택합니다.
   ◦ 포트 그룹의 이름을 NFS-Network로 지정합니다.
   ◦ VLAN ID에 '<<nfs_vlan_id>>'를 입력합니다.
   ◦ MTU를 9000으로 변경합니다.
   ◦ IPv4 설정 을 확장합니다.
   ◦ 정적 설정을 선택합니다.
   ◦ Address 에 "<<var_hosta_nfs_ip>>"를 입력합니다.
   ◦ 서브넷 마스크에 '<<var_hosta_nfs_mask>>'를 입력합니다.
   ◦ 생성 을 클릭합니다.



7. 이 프로세스를 반복하여 vMotion VMkernel 포트를 생성합니다.
8. Add VMkernel NIC 를 선택합니다.
    a. 새 포트 그룹을 선택합니다.
    b. 포트 그룹의 이름을 vMotion으로 지정합니다.
    c. VLAN ID에 '\< vMotion_vlan_id>>'를 입력합니다.
    d. MTU를 9000으로 변경합니다.
    e. IPv4 설정 을 확장합니다.
    f. 정적 설정을 선택합니다.
    g. Address 에 "<<var_hosta_vmotion_ip>>"를 입력합니다.
    h. 서브넷 마스크에 '<<var_hosta_vmotion_mask>>'를 입력합니다.
    i. IPv4 설정 후 vMotion 확인란이 선택되어 있는지 확인합니다.

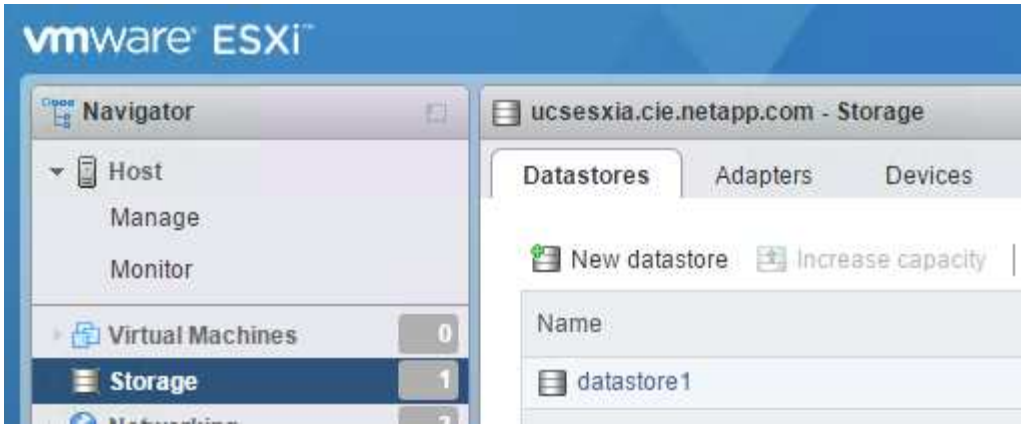


라이센싱에서 허용하는 경우 VMware vSphere 분산 스위치를 사용하는 등 여러 가지 방법으로 ESXi 네트워킹을 구성할 수 있습니다. 비즈니스 요구 사항을 충족하는 데 필요한 경우 FlexPod Express에서 대체 네트워크 구성이 지원됩니다.

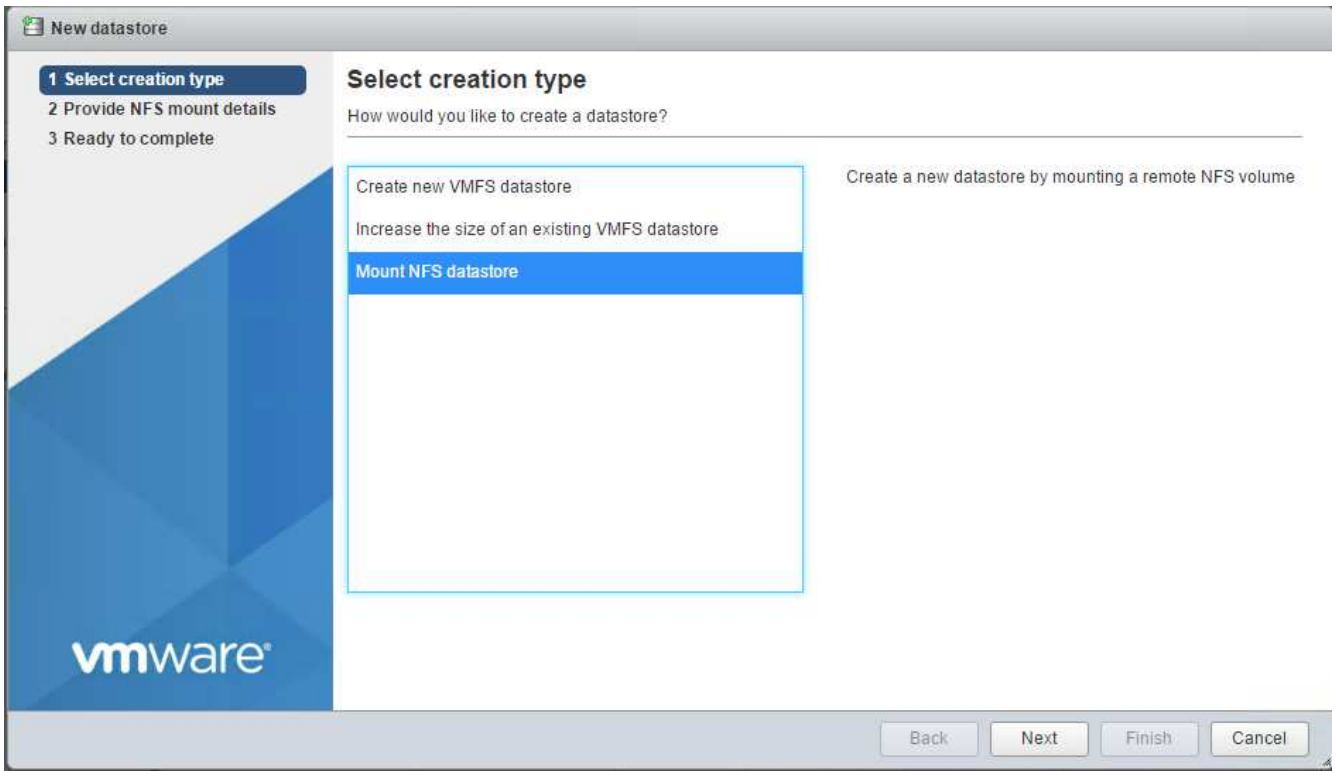
첫 번째 데이터 저장소를 마운트합니다

마운트할 첫 번째 데이터 저장소는 가상 머신용 infra_datastore_1 데이터 저장소와 가상 머신 스왑 파일용 infra_swap 데이터 저장소입니다.

1. 왼쪽 탐색 창에서 스토리지 를 클릭한 다음 새 데이터 저장소 를 클릭합니다.



2. Mount NFS Datastore를 선택합니다.



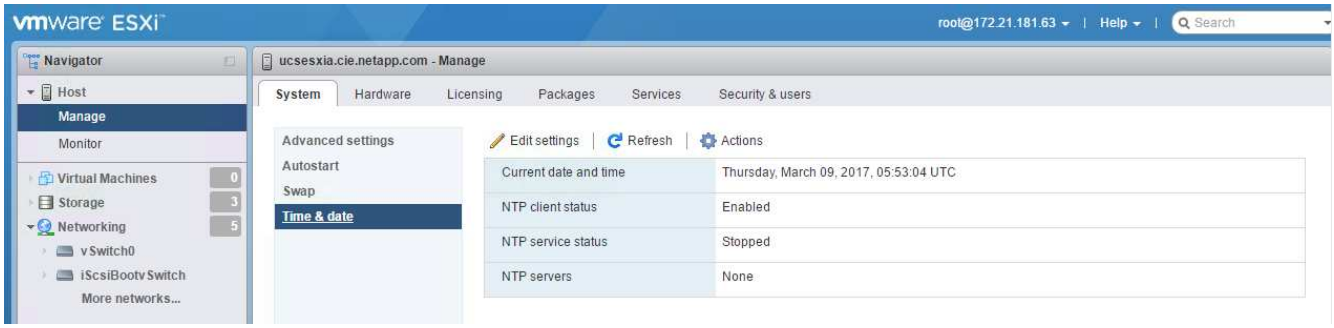
3. 그런 다음 NFS 마운트 세부 정보 제공 페이지에 다음 정보를 입력합니다.
   - 이름: 'infra_datastore_1'
   - NFS 서버:\<<var_NodeA_nfs_lif>'
   - 공유:/infra_datastore_1
   - NFS 3이 선택되어 있는지 확인합니다.
4. 마침 을 클릭합니다. 최근 작업 창에서 작업이 완료된 것을 볼 수 있습니다.
5. 다음 프로세스를 반복하여 infra_swap 데이터 저장소를 마운트합니다.
   - 이름: infra_swap
   - NFS 서버:\<<var_NodeA_nfs_lif>'
   - 공유: '/infra_swap'

◦ NFS 3이 선택되어 있는지 확인합니다.

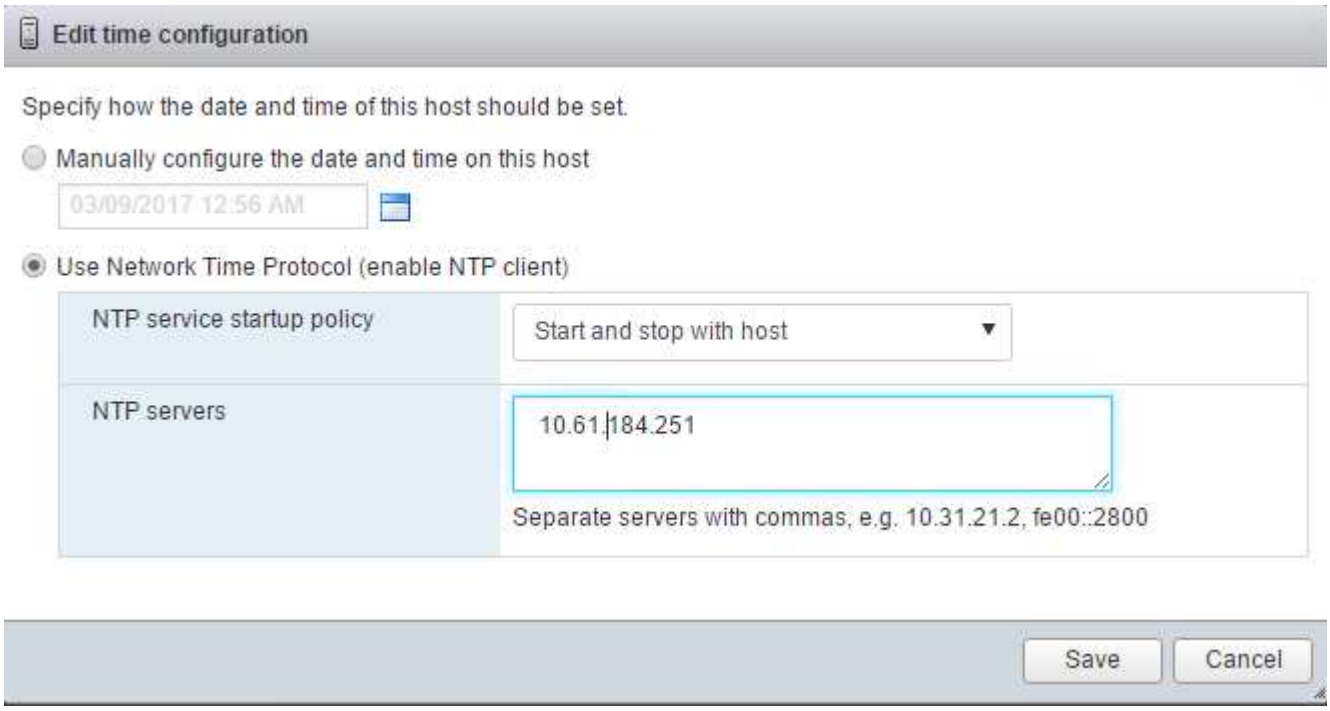
NTP를 구성합니다

ESXi 호스트에 대해 NTP를 구성하려면 다음 단계를 수행하십시오.

1. 왼쪽 탐색 창에서 관리 를 클릭합니다. 오른쪽 창에서 시스템 을 선택한 다음 시간 및 날짜 를 클릭합니다.



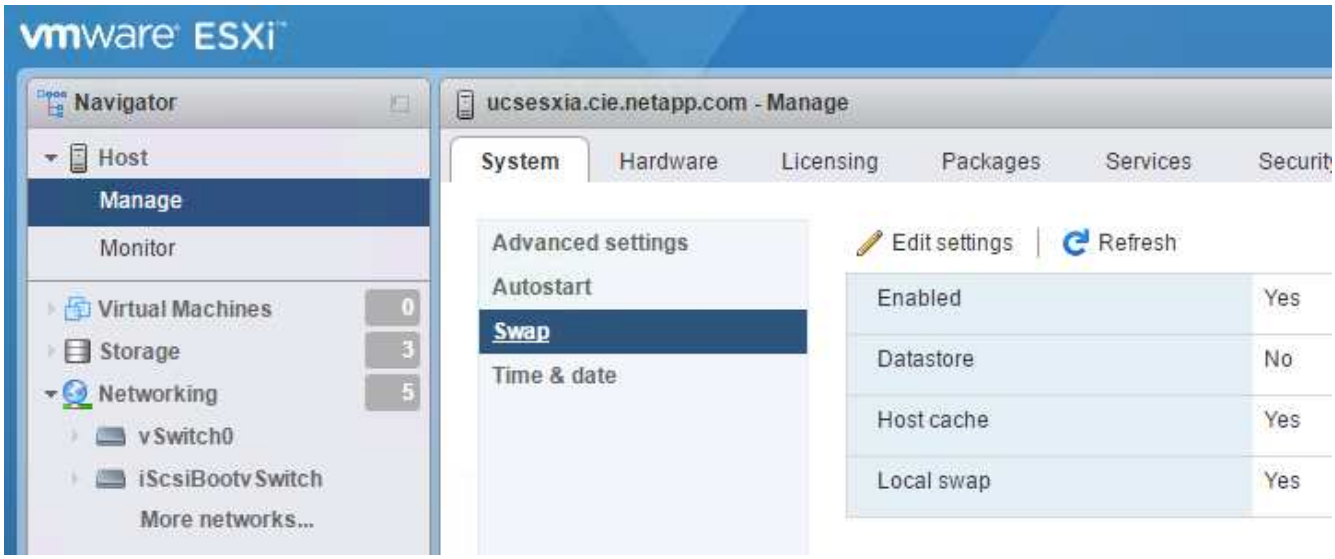
2. Use Network Time Protocol (Enable NTP Client) 을 선택합니다.
3. Start and Stop with Host 를 NTP 서비스 시작 정책으로 선택합니다.
4. NTP 서버로 '<<var_ntp>>'를 입력합니다. 여러 NTP 서버를 설정할 수 있습니다.
5. 저장 을 클릭합니다.



가상 머신 스왑 파일 위치를 이동합니다

다음 단계에서는 가상 머신 스왑 파일 위치를 이동하는 방법을 자세히 설명합니다.

1. 왼쪽 탐색 창에서 관리 를 클릭합니다. 오른쪽 창에서 시스템을 선택한 다음 바꾸기를 클릭합니다.



2. 설정 편집 을 클릭합니다. Datastore 옵션에서 infra_swap을 선택합니다.



3. 저장 을 클릭합니다.

VMware VAAI용 **NetApp NFS** 플러그인 **1.0.20**을 설치합니다

VMware VAAI용 NetApp NFS 플러그인 1.0.20을 설치하려면 다음 단계를 완료하십시오.

1. 다음 명령을 입력하여 VAAI가 활성화되었는지 확인합니다.

```
esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
```

VAAI가 활성화된 경우 다음 명령을 실행하면 다음 출력이 생성됩니다.

```
~ #  esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
~ # esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
```

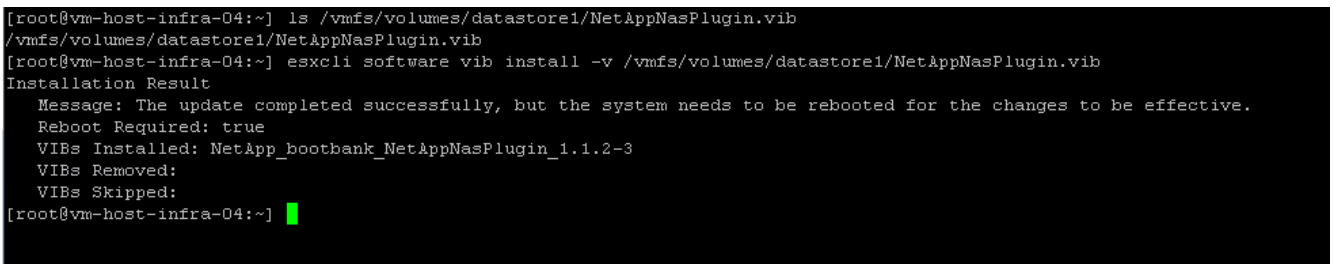
2. VAAI가 설정되어 있지 않으면 다음 명령을 입력하여 VAAI를 사용하도록 설정합니다.

```
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedInit
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
```

이러한 명령은 다음과 같은 출력을 생성합니다.

```
~ # esxcfg-advcfg -s 1 /Data Mover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
~ #  esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
```

3. NetApp NFS Plug-in for VMware VAAI 다운로드:
   a. 로 이동합니다 "소프트웨어 다운로드 페이지".
   b. 아래로 스크롤하여 VMware VAAI용 NetApp NFS 플러그인 을 클릭합니다.
   c. ESXi 플랫폼을 선택합니다.
   d. 최신 플러그인의 오프라인 번들(.zip) 또는 온라인 번들(.vib)을 다운로드합니다.
4. ESX CLI를 사용하여 ESXi 호스트에 플러그인을 설치합니다.
5. ESXi 호스트를 재부팅합니다.



"다음: VMware vCenter Server 6.7을 설치합니다"

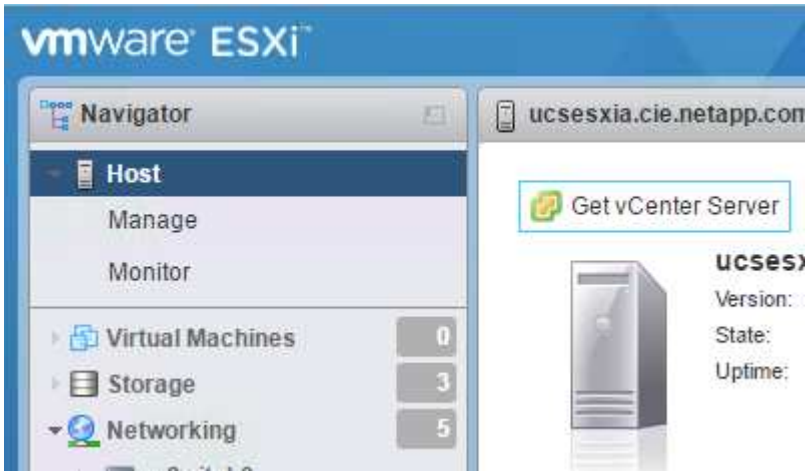
VMware vCenter Server 6.7을 설치합니다

이 섹션에서는 FlexPod Express 구성에 VMware vCenter Server 6.7을 설치하는 절차를 자세히 설명합니다.

FlexPod Express는 VCSA(VMware vCenter Server Appliance)를 사용합니다.

VMware vCenter Server 어플라이언스를 다운로드합니다

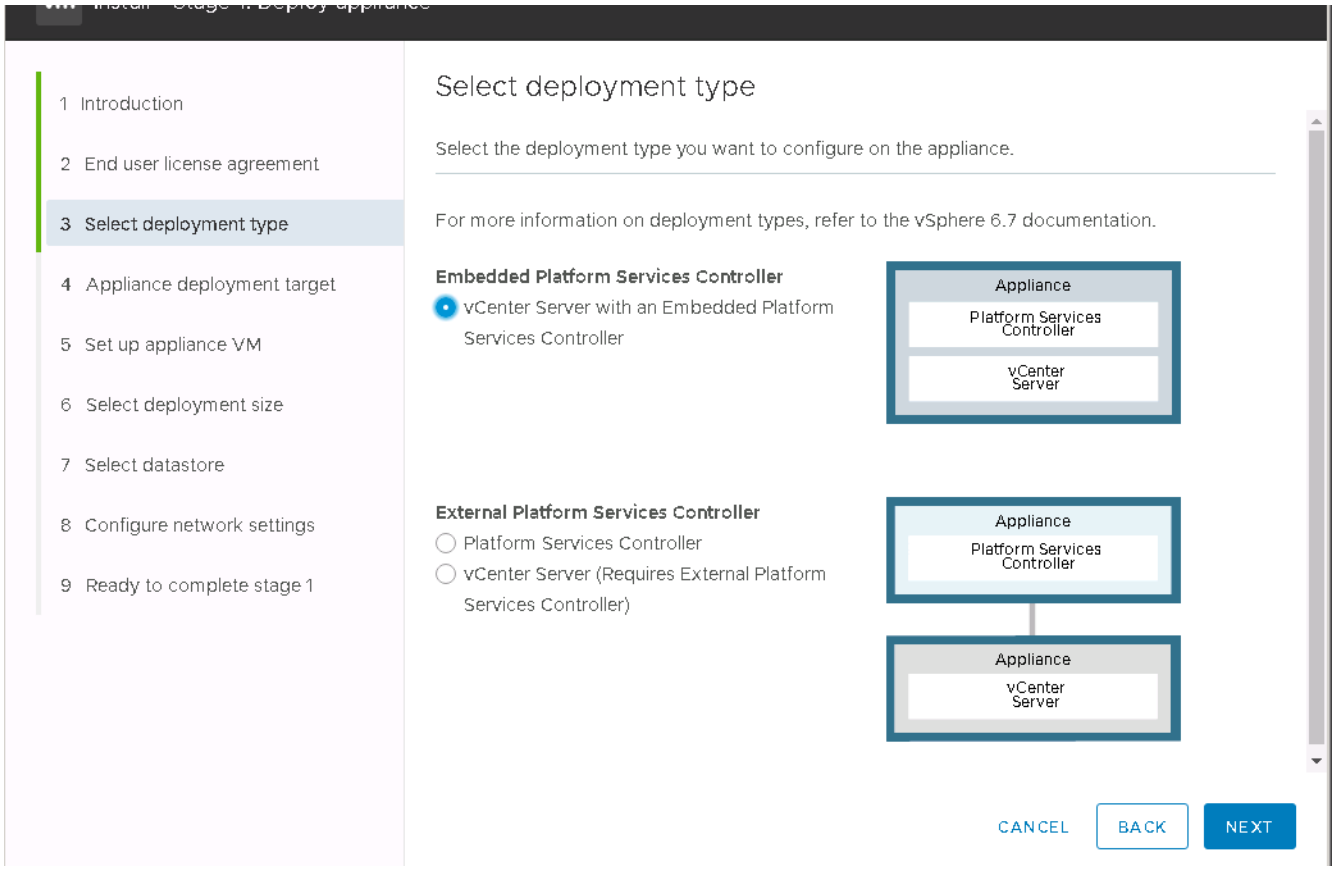
1. VCSA를 다운로드합니다. ESXi 호스트를 관리할 때 vCenter Server 가져오기 아이콘을 클릭하여 다운로드 링크를 액세스합니다.



2. VMware 사이트에서 VCSA를 다운로드합니다.

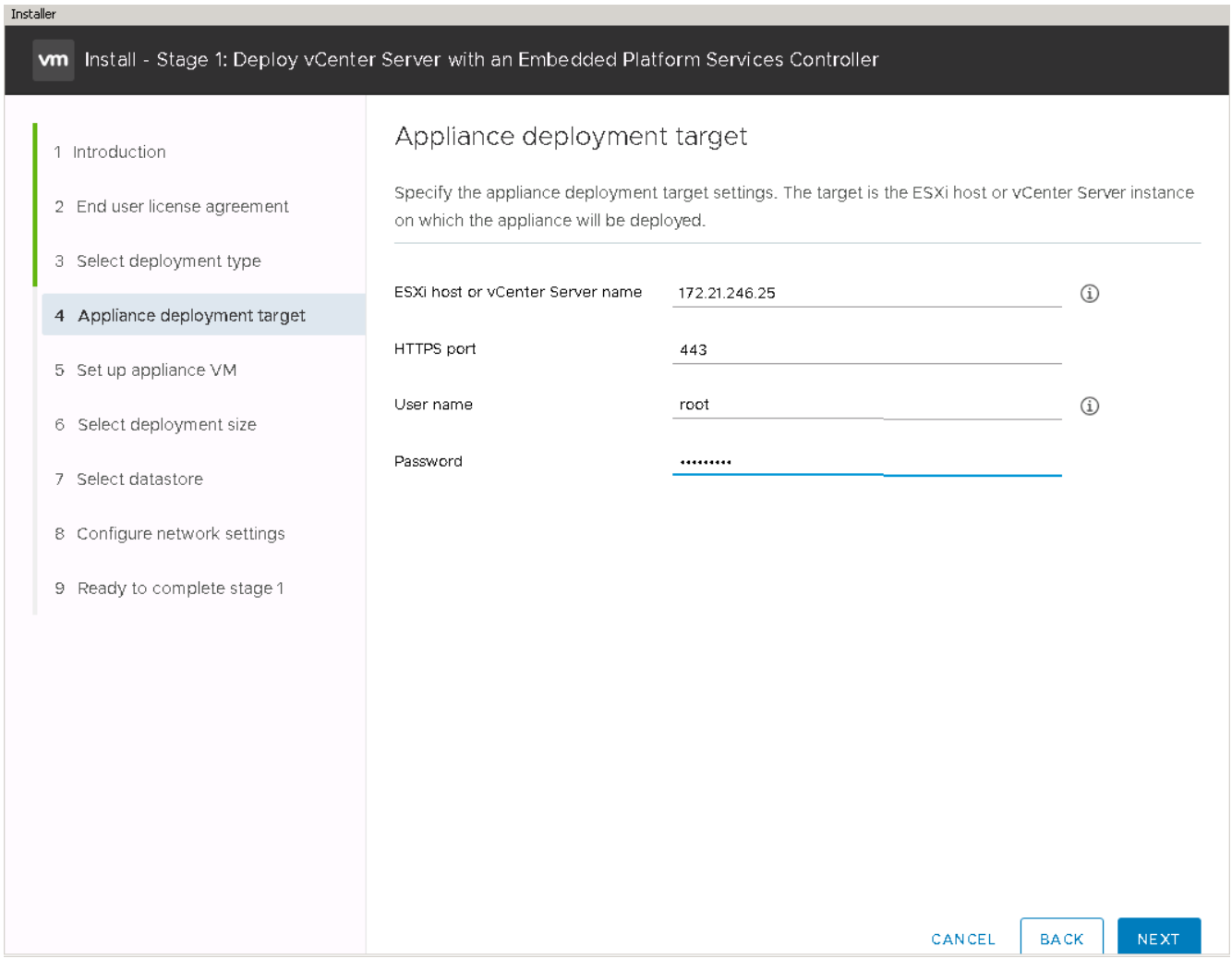
> Microsoft Windows vCenter Server 설치 가능한 가 지원되지만 VMware는 새로운 구축에 VCSA를 권장합니다.

3. ISO 이미지를 마운트합니다.
4. vcsa-UI-installer> Win32 디렉터리로 이동합니다. installer.exe를 두 번 클릭합니다.
5. 설치 를 클릭합니다.
6. 소개 페이지에서 다음 을 클릭합니다.
7. 최종 사용자 라이센스 계약에 동의합니다.
8. 배포 유형으로 임베디드 플랫폼 서비스 컨트롤러 를 선택합니다.

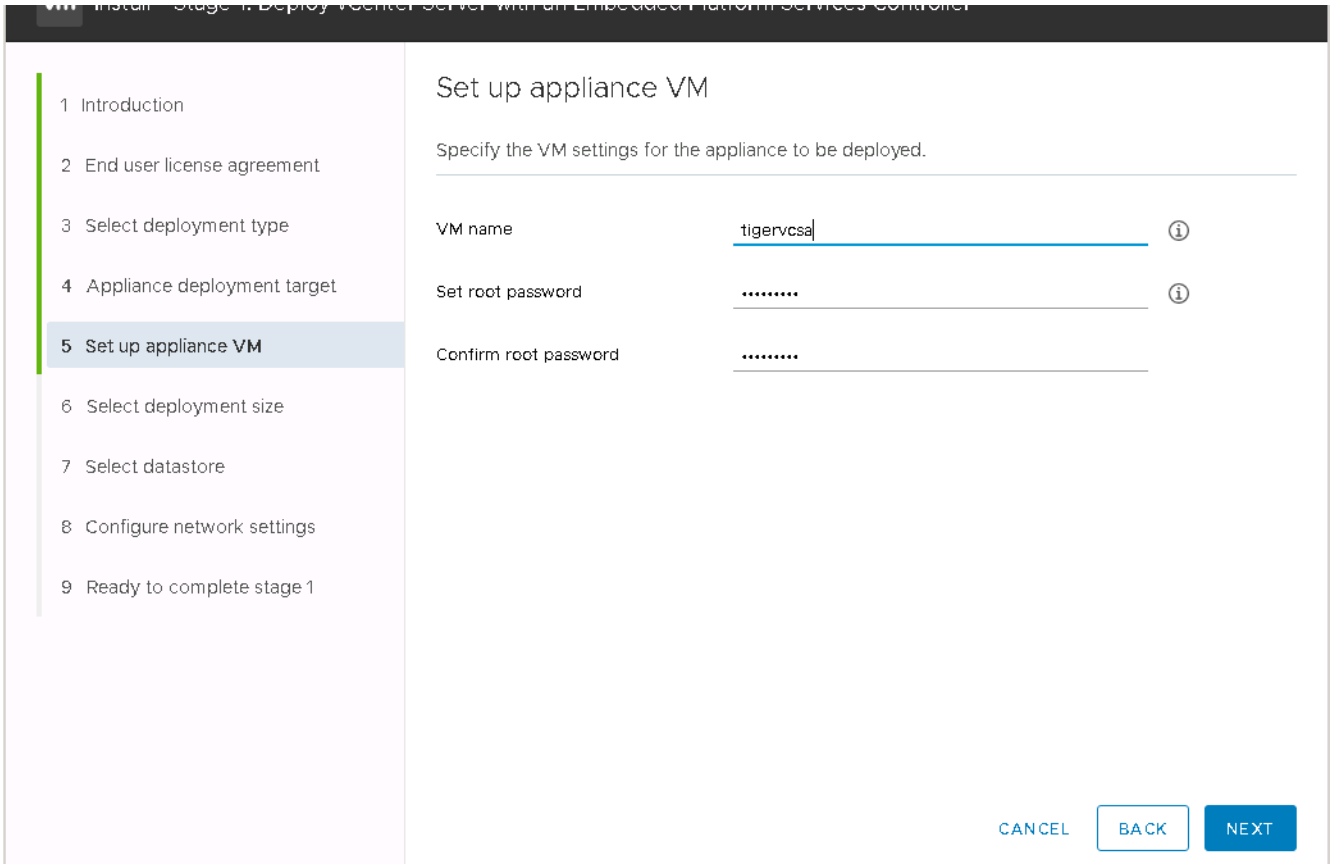


필요한 경우 외부 플랫폼 서비스 컨트롤러 배포도 FlexPod Express 솔루션의 일부로 지원됩니다.

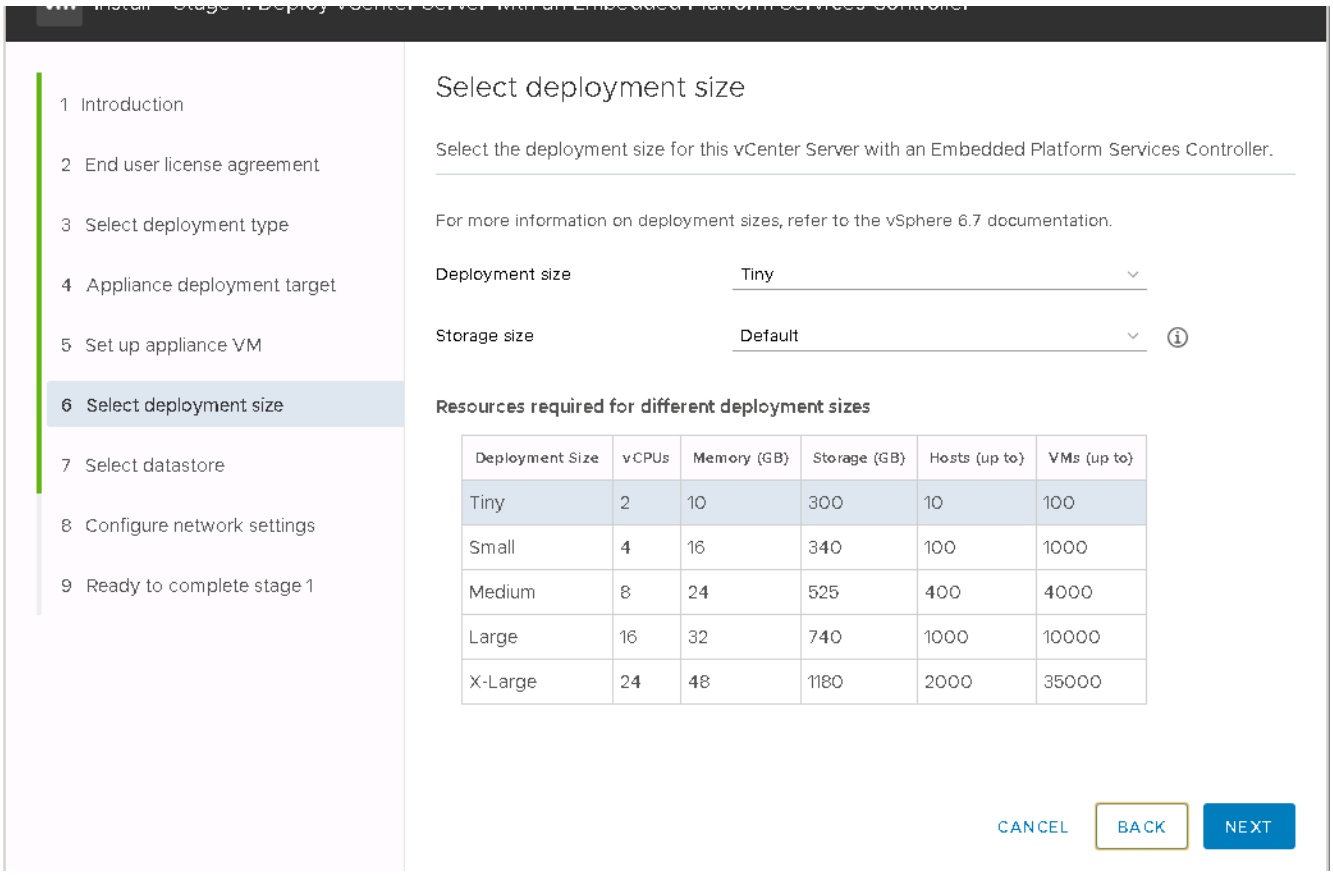
9. Appliance Deployment Target에서 구축한 ESXi 호스트의 IP 주소와 루트 사용자 이름 및 루트 암호를 입력합니다.



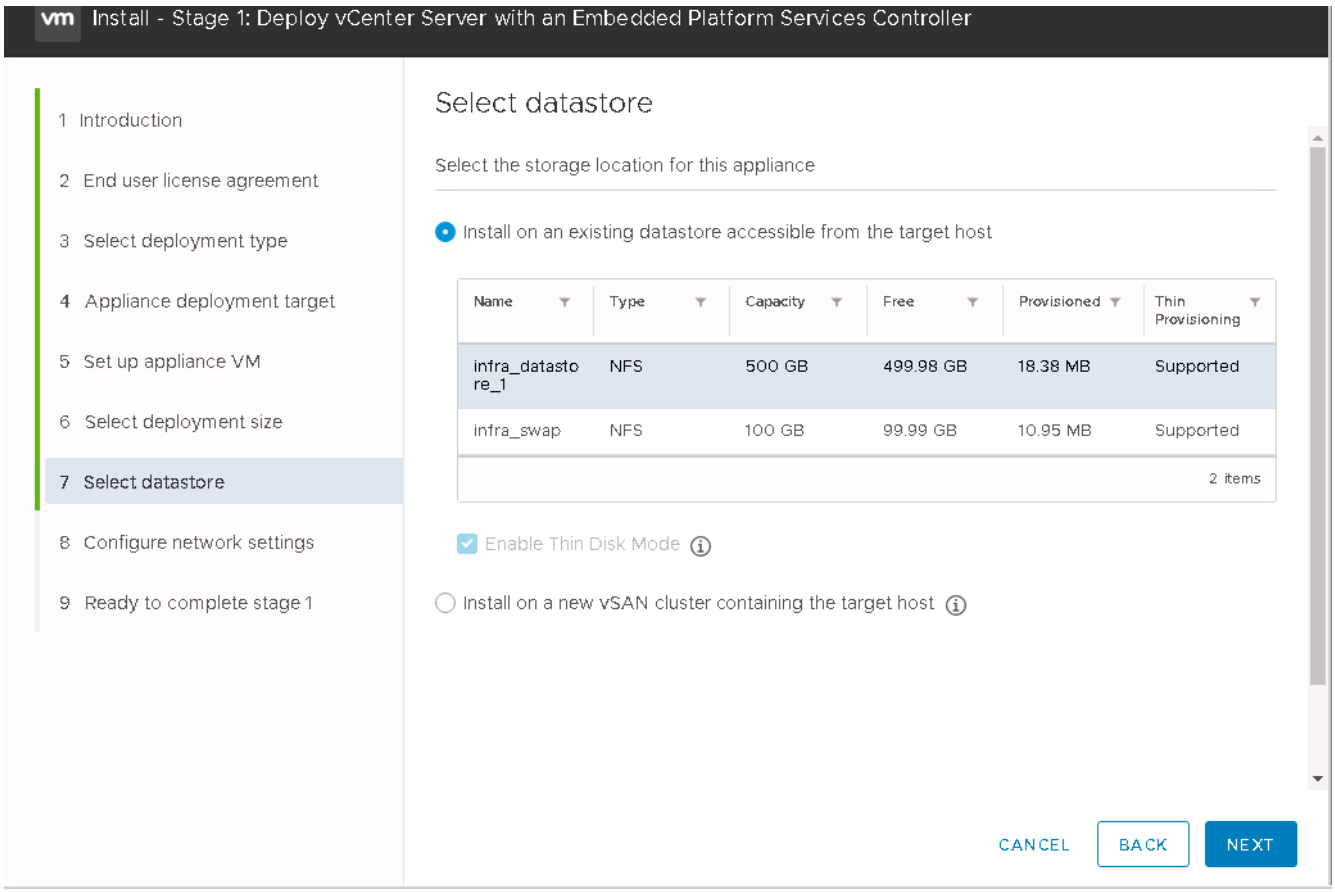
10. VCSA에 사용할 VM 이름과 루트 암호를 VCSA로 입력하여 어플라이언스 VM을 설정합니다.



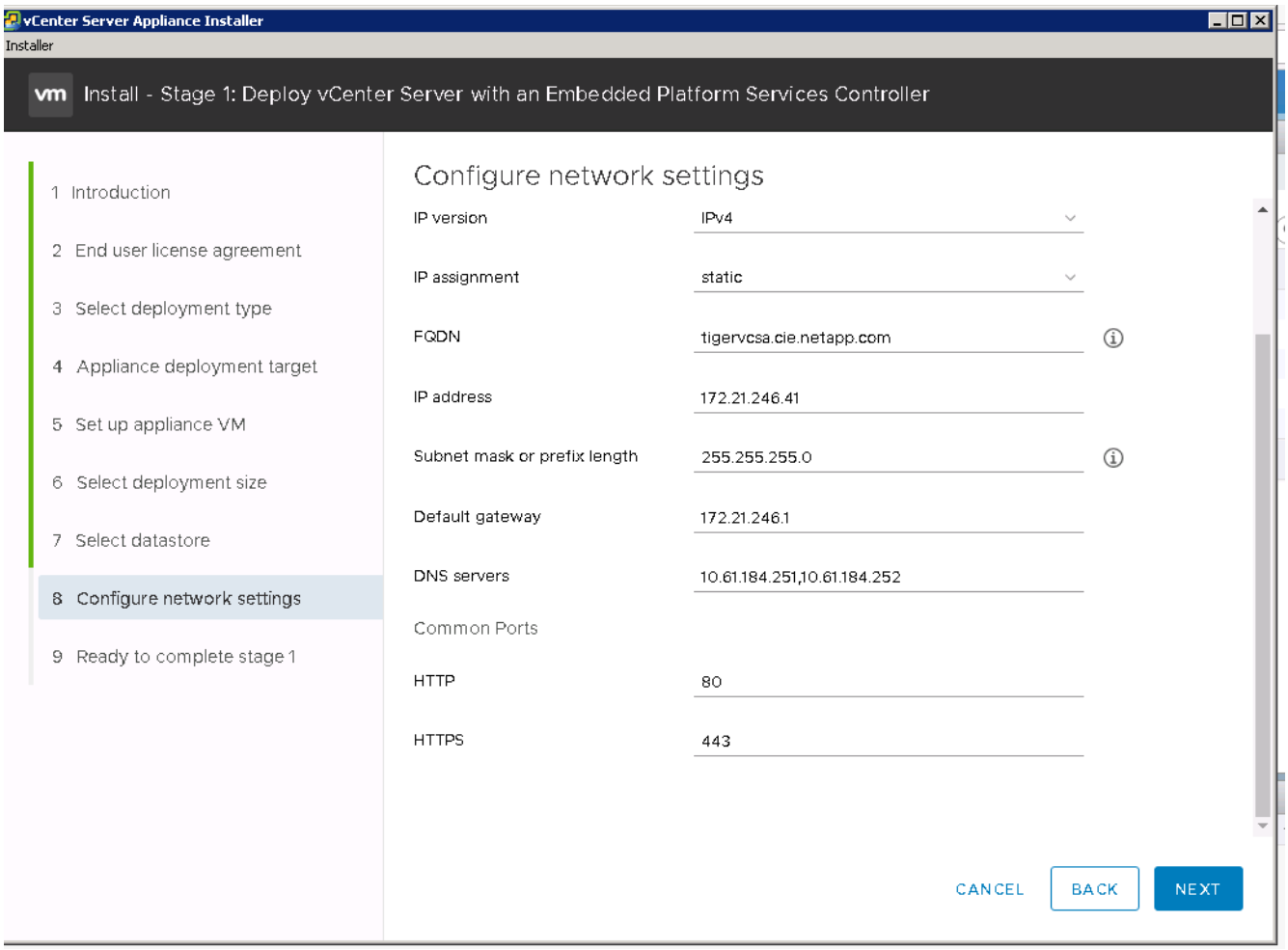
11. 환경에 가장 적합한 구축 크기를 선택합니다. 다음 을 클릭합니다.



12. infra_datastore_1 데이터 저장소를 선택합니다. 다음 을 클릭합니다.

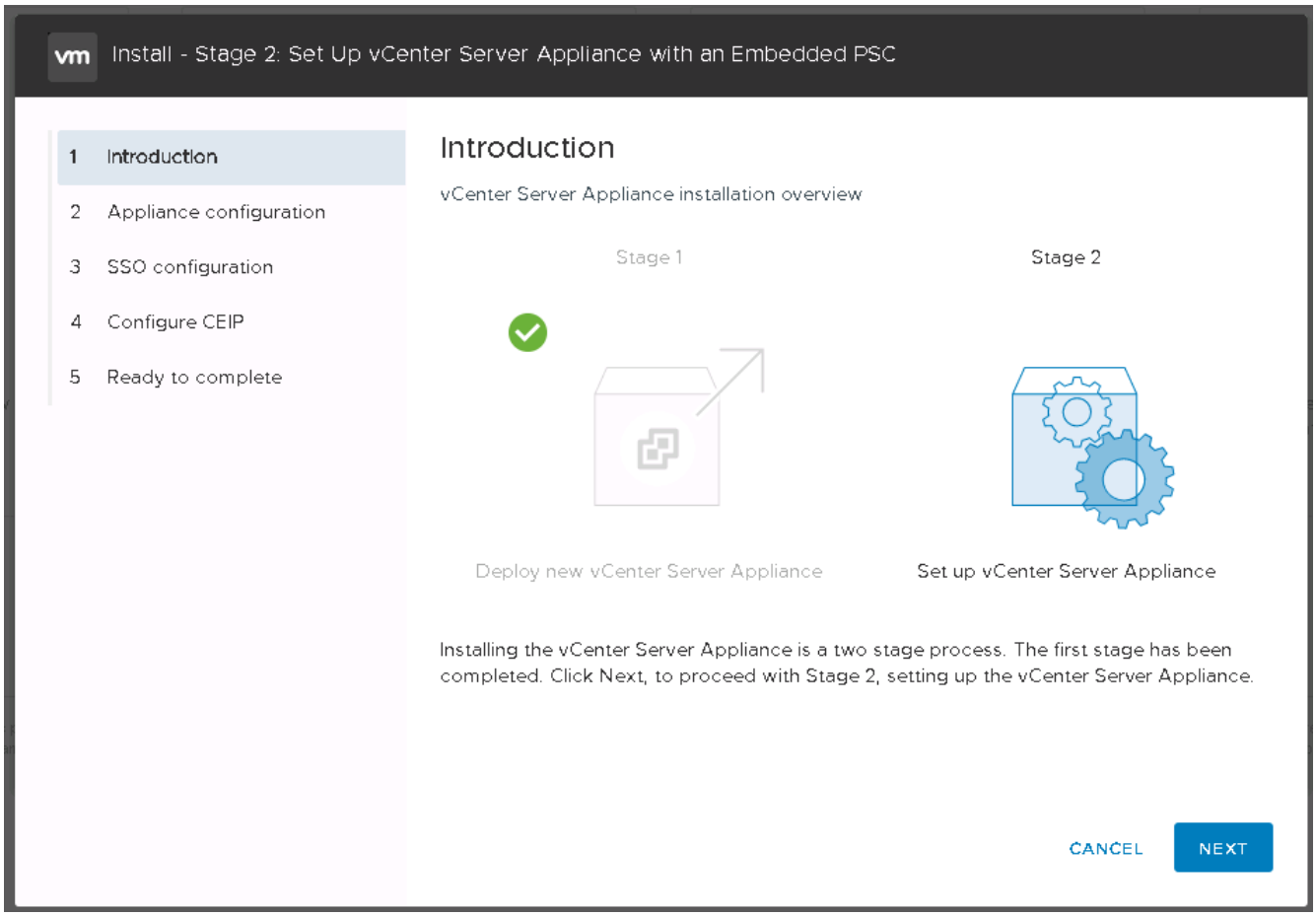


13. 네트워크 설정 구성 페이지에 다음 정보를 입력하고 다음 을 클릭합니다.
    a. Network 에서 MGMT-Network 를 선택합니다.
    b. VCSA에 사용할 FQDN 또는 IP를 입력합니다.
    c. 사용할 IP 주소를 입력합니다.
    d. 사용할 서브넷 마스크를 입력합니다.
    e. 기본 게이트웨이를 입력합니다.
    f. DNS 서버를 입력합니다.
14. 1단계 완료 준비 페이지에서 입력한 설정이 올바른지 확인합니다. 마침 을 클릭합니다.



VCSA가 지금 설치됩니다. 이 과정은 몇 분 정도 소요됩니다.

15. 1단계가 완료되면 완료되었다는 메시지가 나타납니다. 계속 을 클릭하여 2단계 구성을 시작합니다.
16. 2단계 소개 페이지에서 다음 을 클릭합니다.



17. NTP 서버 주소에 대해 '<<var_ntp_id>>'를 입력합니다. 여러 NTP IP 주소를 입력할 수 있습니다.

    vCenter Server HA(고가용성)를 사용하려는 경우 SSH 액세스가 설정되어 있는지 확인합니다.

18. SSO 도메인 이름, 암호 및 사이트 이름을 구성합니다. 다음 을 클릭합니다.

    특히 vSphere.local 도메인 이름을 벗어난 경우 이러한 값을 참조로 기록합니다.

19. 원하는 경우 VMware 고객 경험 프로그램에 참여하십시오. 다음 을 클릭합니다.
20. 설정 요약을 봅니다. 마침 을 클릭하거나 뒤로 단추를 사용하여 설정을 편집합니다.
21. 설치가 시작된 후 설치를 일시 중지하거나 중지할 수 없다는 메시지가 나타납니다. 계속하려면 확인을 클릭하십시오.

    어플라이언스 설정이 계속됩니다. 이 작업은 몇 분 정도 걸립니다.

    설정이 성공했음을 나타내는 메시지가 나타납니다.

    vCenter Server에 액세스하기 위해 설치 관리자가 제공하는 링크를 클릭할 수 있습니다.

"다음: VMware vCenter Server 6.7 및 vSphere 클러스터링을 구성합니다."

VMware vCenter Server 6.7 및 **vSphere** 클러스터링 구성

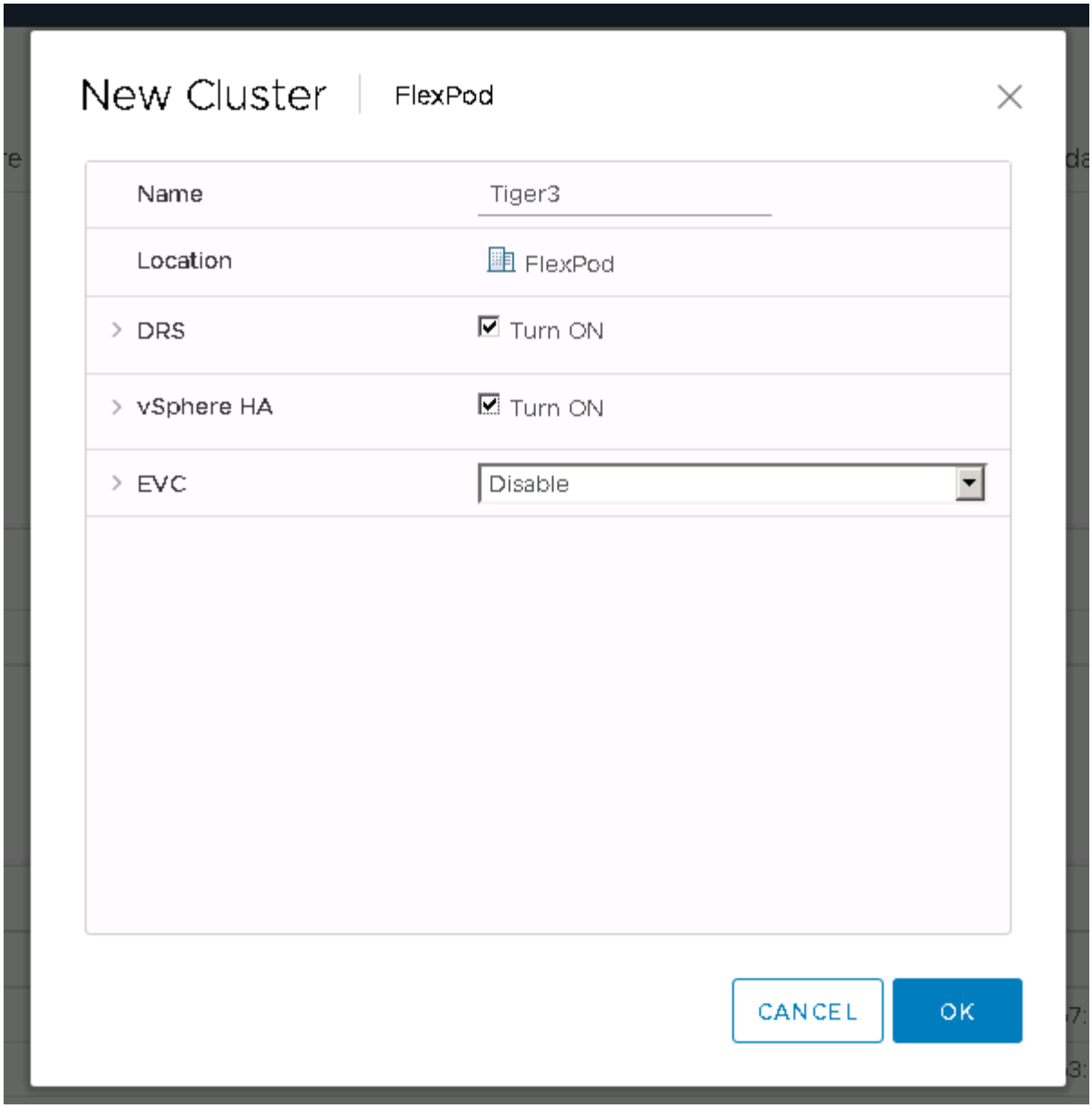
VMware vCenter Server 6.7 및 vSphere 클러스터링을 구성하려면 다음 단계를 수행하십시오.

1. https://\<<FQDN 또는 vCenter의 IP >>/vSphere-client/로 이동합니다.
2. vSphere Client 시작 을 클릭합니다.
3. 사용자 이름 mailto:administrator@vspehre.loca l[administrator@vsphere.loca l^]과 VCSA 설정 프로세스 중에 입력한 SSO 암호를 사용하여 로그인합니다.
4. vCenter 이름을 마우스 오른쪽 버튼으로 클릭하고 New Datacenter를 선택합니다.
5. 데이터 센터의 이름을 입력하고 확인 을 클릭합니다.

vSphere 클러스터를 생성합니다

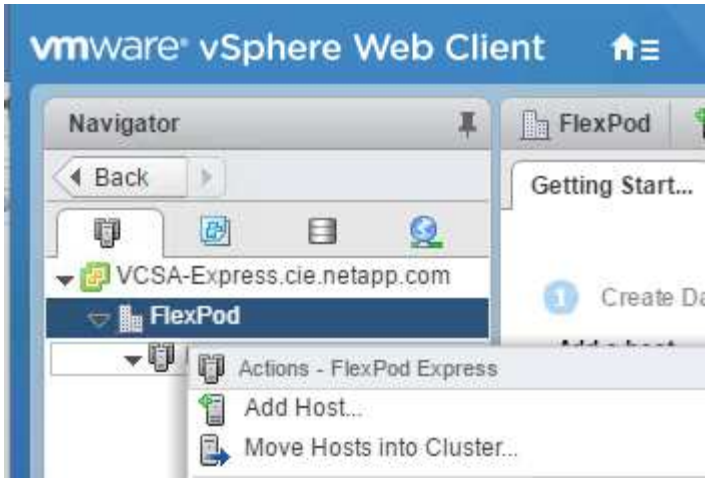
vSphere 클러스터를 생성하려면 다음 단계를 수행하십시오.

1. 새로 생성된 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 New Cluster를 선택합니다.
2. 클러스터의 이름을 입력합니다.
3. 확인란을 선택하여 DR 및 vSphere HA를 설정합니다.
4. 확인 을 클릭합니다.



클러스터에 **ESXi** 호스트를 추가합니다

1. 클러스터를 마우스 오른쪽 버튼으로 클릭하고 Add Host를 선택합니다.



2. 클러스터에 ESXi 호스트를 추가하려면 다음 단계를 수행하십시오.
   a. 호스트의 IP 또는 FQDN을 입력합니다. 다음 을 클릭합니다.
   b. 루트 사용자 이름과 암호를 입력합니다. 다음 을 클릭합니다.
   c. 예를 클릭하여 호스트의 인증서를 VMware 인증서 서버에서 서명한 인증서로 바꿉니다.
   d. 호스트 요약 페이지에서 다음 을 클릭합니다.
   e. 녹색 + 아이콘을 클릭하여 vSphere 호스트에 라이센스를 추가합니다.

      이 단계는 원할 경우 나중에 완료할 수 있습니다.

   f. 다음 을 클릭하여 잠금 모드를 해제합니다.
   g. VM 위치 페이지에서 다음 을 클릭합니다.
   h. 완료 준비 페이지를 검토합니다. 뒤로 단추를 사용하여 변경하거나 마침 을 선택합니다.
3. Cisco UCS 호스트 B에 대해 1단계와 2단계를 반복합니다 FlexPod Express 구성에 추가된 모든 호스트에 대해 이 프로세스를 완료해야 합니다.

ESXi 호스트에서 코어 덤프를 구성합니다

1. SSH를 사용하여 관리 IP ESXi 호스트에 연결하고 사용자 이름에 root를 입력한 다음 루트 암호를 입력합니다.
2. 다음 명령을 실행합니다.

```
esxcli system coredump network set -i ip_address_of_core_dump_collector
-v vmk0 -o 6500
esxcli system coredump network set --enable=true
esxcli system coredump network check
```

3. 최종 명령어를 입력하면 확인된 netdump server가 실행 중인 것으로 확인되었다는 메시지가 나타난다.

FlexPod Express에 추가된 모든 호스트에 대해 이 프로세스를 완료해야 합니다.

결론

FlexPod Express는 업계 최고의 구성요소를 사용하는 검증된 설계를 통해 간단하고 효율적인 솔루션을 제공합니다. FlexPod Express는 추가 구성요소를 추가하여 특정 비즈니스 요구사항에 맞게 확장할 수 있습니다. FlexPod Express는 전용 솔루션이 필요한 중소기업, ROBO 및 기타 기업을 염두에 두고 설계되었습니다.

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대한 자세한 내용은 다음 문서 및/또는 웹 사이트를 참조하십시오.

- NetApp 제품 설명서

  "http://docs.netapp.com"

- FlexPod Express with VMware vSphere 6.7 및 NetApp AFF A220 설계 가이드 를 참조하십시오

  "https://www.netapp.com/us/media/nva-1125-design.pdf"

직접 연결 IP 기반 스토리지를 사용하는 VMware vSphere 6.7U1 및 NetApp AFF A220을 지원하는 FlexPod Express

NVA-1131-deploy: VMware vSphere 6.7U1 및 NetApp AFF A220을 지원하는 FlexPod Express(직접 연결 IP 기반 스토리지 포함

NetApp, 스리랑카 Sree Lakshmi

업계 동향에 따르면 많은 데이터 센터가 공유 인프라 및 클라우드 컴퓨팅으로 전환하고 있습니다. 또한 기업에서는 데이터 센터에 친숙한 기술을 활용하여 원격 사무소 및 지사를 위한 간편하고 효율적인 솔루션을 찾고 있습니다.

FlexPod Express는 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 스위치 제품군, NetApp 스토리지 기술을 기반으로 사전 설계되며 모범 사례 아키텍처입니다. FlexPod 익스프레스 시스템의 구성요소는 FlexPod 데이터 센터와 비슷하기 때문에 더 작은 규모로 전체 IT 인프라 환경에서 관리 시너지 효과를 실현할 수 있습니다. FlexPod 데이터 센터와 FlexPod Express는 가상화와 베어 메탈 OS와 엔터프라이즈 워크로드를 위한 최적의 플랫폼입니다.

FlexPod 데이터 센터 및 FlexPod 익스프레스 는 기본 구성을 제공하며 다양한 사용 사례와 요구 사항을 수용할 수 있도록 크기를 조정할 수 있는 다기능성을 제공합니다. 기존 FlexPod 데이터 센터 고객은 익숙한 툴을 사용하여 FlexPod 익스프레스 시스템을 관리할 수 있습니다. 새로운 FlexPod Express 고객은 환경 확장에 따라 FlexPod 데이터 센터 관리에 쉽게 적응할 수 있습니다.

FlexPod Express는 원격 사무소 및 지사(ROBO)와 중소 기업 및 중견 기업을 위한 최적의 인프라 기반입니다. 전용 워크로드에 대한 인프라를 제공하려는 고객에게 최적의 솔루션입니다.

FlexPod Express는 거의 모든 워크로드에 적합한 관리하기 쉬운 인프라를 제공합니다.

솔루션 개요

이 FlexPod Express 솔루션은 FlexPod 통합 인프라 프로그램의 일부입니다.

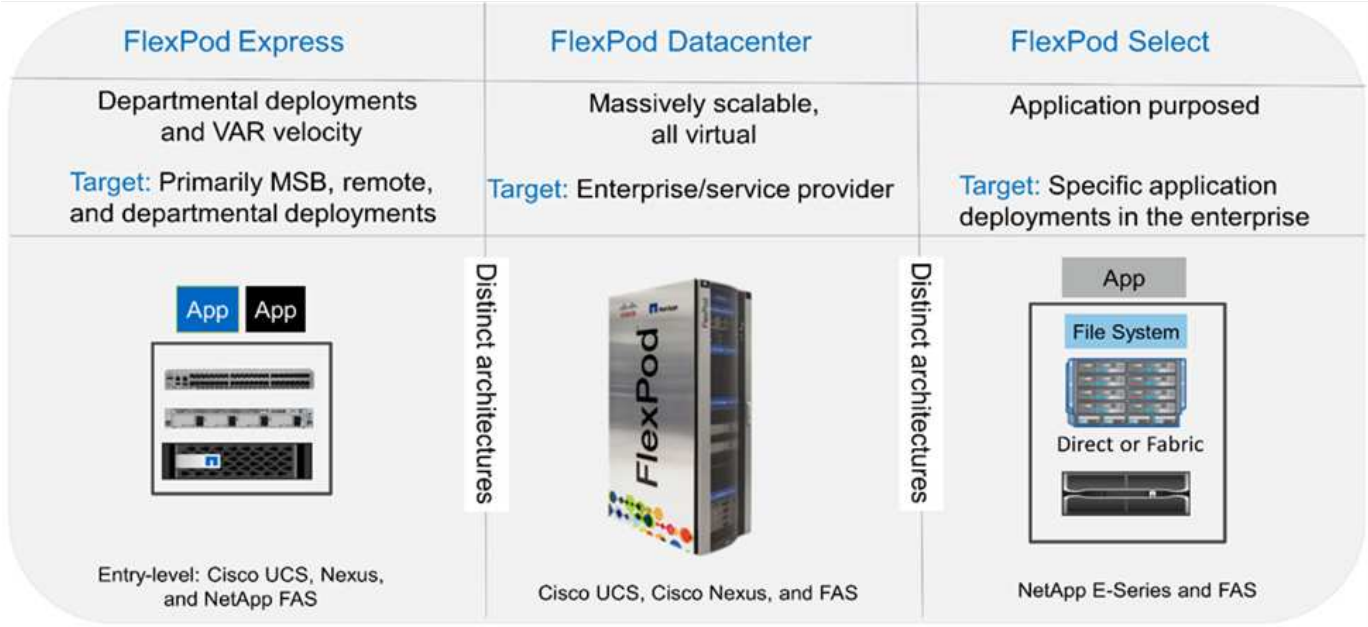
FlexPod 통합 인프라 프로그램

FlexPod 참조 아키텍처는 CVD(Cisco Validated Design) 또는 NVA(NetApp Verified Architecture)로 제공됩니다. 지정된 CVD 또는 NVA의 고객 요구 사항에 따른 편차는 이러한 변형으로 지원되지 않는 구성이 생성되지는 않을 경우 허용됩니다.

아래 그림과 같이 FlexPod 프로그램에는 FlexPod 익스프레스, FlexPod 데이터 센터, FlexPod 선택의 세 가지 솔루션이 포함되어 있습니다.

- * FlexPod 익스프레스 * 는 Cisco 및 NetApp의 기술을 갖춘 엔트리 레벨 솔루션을 고객에게 제공합니다.
- * FlexPod 데이터 센터 * 는 다양한 워크로드 및 애플리케이션을 위한 최적의 다목적 토대를 제공합니다.
- * FlexPod Select * 는 FlexPod 데이터 센터의 최고 기능을 통합하고 인프라를 특정 애플리케이션에 맞게 조정합니다.

다음 그림은 솔루션의 기술 구성요소를 보여 줍니다.



NetApp 검증 아키텍처 프로그램

NVA 프로그램은 NetApp 솔루션을 위한 검증된 아키텍처를 고객에게 제공합니다. NVA는 NetApp 솔루션 아키텍처의 다음과 같은 특징을 제공합니다.

- 철저한 테스트를 거친 아키텍처
- 기본적으로 규범적인 아키텍처
- 구축 위험 최소화
- 출시 시기를 단축합니다

이 가이드는 직접 연결 NetApp 스토리지를 사용하는 FlexPod Express의 설계에 대해 자세히 설명합니다. 다음 섹션에서는 이 솔루션 설계에 사용되는 구성 요소를 나열합니다.

하드웨어 구성 요소

- NetApp AFF A220을 참조하십시오
- Cisco UCS Mini를 참조하십시오
- Cisco UCS B200 M5
- Cisco UCS VIC 1440/1480.
- Cisco Nexus 3000 시리즈 스위치

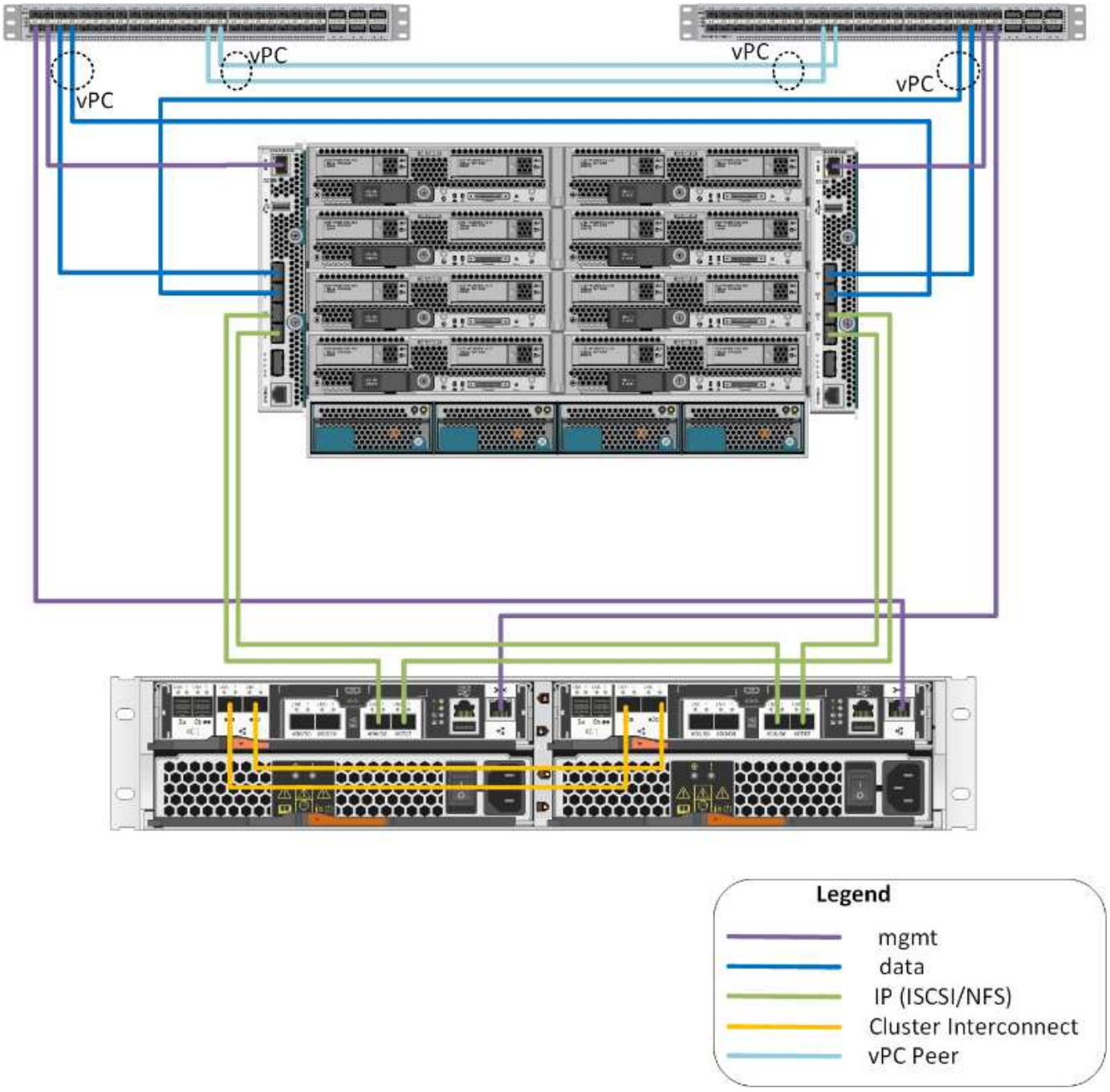
소프트웨어 구성 요소

- NetApp ONTAP 9. 5
- VMware vSphere 6.7U1
- Cisco UCS Manager 4.0(1b)
- Cisco NXOS 펌웨어 7.0(3) I6(1)

솔루션 기술

이 솔루션은 NetApp, Cisco 및 VMware의 최신 기술을 활용합니다. ONTAP 9.5, 이중 Cisco Nexus 31108PCV 스위치를 실행하는 새로운 NetApp AFF A220과 VMware vSphere 6.7U1을 실행하는 Cisco UCS B200 M5 서버를 특징으로 합니다. 이 검증된 솔루션은 10GbE 기술을 통한 Direct Connect IP 스토리지를 사용합니다.

다음 그림에서는 VMware vSphere 6.7U1 IP 기반 직접 연결 아키텍처를 지원하는 FlexPod Express를 보여 줍니다.



사용 사례 요약

FlexPod 익스프레스 솔루션은 다음과 같은 여러 사용 사례에 적용할 수 있습니다.

- ROBO
- 중소기업
- 비용 효율적인 전용 솔루션이 필요한 환경

FlexPod Express는 가상화된 혼합 워크로드에 가장 적합합니다.

기술 요구 사항

FlexPod 익스프레스 시스템에는 하드웨어 및 소프트웨어 구성 요소의 조합이 필요합니다. 또한 FlexPod Express는 하이퍼바이저 노드를 시스템에 추가하는 데 필요한 하드웨어 구성요소를 2개 단위로 설명합니다.

하드웨어 요구 사항

선택한 하이퍼바이저에 관계없이 모든 FlexPod Express 구성은 동일한 하드웨어를 사용합니다. 따라서 비즈니스 요구사항이 변경되더라도 두 하이퍼바이저 중 하나를 동일한 FlexPod Express 하드웨어에서 실행할 수 있습니다.

다음 표에는 모든 FlexPod Express 구성에 필요한 하드웨어 구성요소가 나와 있습니다.

하드웨어	수량
AFF A220 HA 쌍	1
Cisco UCS B200 M5 서버	2
Cisco Nexus 31108PCV 스위치	2
Cisco UCS B200 M5 서버용 Cisco UCS VIC(Virtual Interface Card) 1440	2
2개의 통합 UCS-Fi-M-6324 패브릭 인터커넥트를 지원하는 Cisco UCS Mini	1

소프트웨어 요구 사항

다음 표에는 FlexPod 익스프레스 솔루션의 아키텍처를 구현하는 데 필요한 소프트웨어 구성 요소가 나열되어 있습니다.

소프트웨어	버전	세부 정보
Cisco UCS Manager를 참조하십시오	4.0(1b)	Cisco UCS Fabric Interconnect Fi - 6324UP
Cisco Blade 소프트웨어	4.0(1b)	Cisco UCS B200 M5 서버용
Cisco nenic 드라이버	1.0.25.0	Cisco VIC 1440 인터페이스 카드용
Cisco NX-OS입니다	7.0(3) I6(1)	Cisco Nexus 31108PCV 스위치의 경우
NetApp ONTAP를 참조하십시오	9.5	AFF A220 컨트롤러

다음 표에는 FlexPod Express의 모든 VMware vSphere 구축에 필요한 소프트웨어가 나와 있습니다.

소프트웨어	버전
VMware vCenter Server 어플라이언스	6.7U1
VMware vSphere ESXi 하이퍼바이저	6.7U1

FlexPod 익스프레스 케이블 연결 정보

참조 검증 케이블 연결은 다음 표에 설명되어 있습니다.

다음 표에는 Cisco Nexus 스위치 31108PCV A의 케이블 연결 정보가 나열되어 있습니다

로컬 장치	로컬 포트	원격 장치	원격 포트
Cisco Nexus 스위치 31108PCV A	eth1/1	NetApp AFF A220 스토리지 컨트롤러 A입니다	e0M
	eth1/2	Cisco UCS-미니 FI-A	mgmt0
	eth1/3	Cisco UCS-미니 FI-A	eth1/1
	eth 1/4입니다	Cisco UCS-미니 FI-B를 지원합니다	eth1/1
	eth 1/13	Cisco NX 31108PCV B	eth 1/13
	eth 1/14	Cisco NX 31108PCV B	eth 1/14

다음 표에는 Cisco Nexus 스위치 31108PCV B의 케이블 연결 정보가 나와 있습니다

로컬 장치	로컬 포트	원격 장치	원격 포트
Cisco Nexus 스위치 31108PCV B	eth1/1	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0M
	eth1/2	Cisco UCS-미니 FI-B를 지원합니다	mgmt0
	eth1/3	Cisco UCS-미니 FI-A	eth1/2
	eth 1/4입니다	Cisco UCS-미니 FI-B를 지원합니다	eth1/2
	eth 1/13	Cisco NX 31108PCV A	eth 1/13
	eth 1/14	Cisco NX 31108PCV A	eth 1/14

다음 표에서는 NetApp AFF A220 스토리지 컨트롤러 A의 케이블 연결 정보를 보여 줍니다

로컬 장치	로컬 포트	원격 장치	원격 포트
NetApp AFF A220 스토리지 컨트롤러 A입니다	e0a	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0a
	e0b	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0b
	e0e	Cisco UCS-미니 FI-A	eth1/3
	e0f	Cisco UCS-미니 FI-B를 지원합니다	eth1/3
	e0M	Cisco NX 31108PCV A	eth1/1

다음 표에서는 NetApp AFF A220 스토리지 컨트롤러 B의 케이블 연결 정보를 보여 줍니다

로컬 장치	로컬 포트	원격 장치	원격 포트
NetApp AFF A220 스토리지 컨트롤러 B입니다	e0a	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0a
	e0b	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0b
	e0e	Cisco UCS-미니 FI-A	eth1/4
	e0f	Cisco UCS-미니 FI-B를 지원합니다	eth1/4
	e0M	Cisco NX 31108PCV B	eth1/1

다음 표에는 Cisco UCS Fabric Interconnect A의 케이블 연결 정보가 나와 있습니다

로컬 장치	로컬 포트	원격 장치	원격 포트
Cisco UCS 6120 패브릭 인터커넥트 A	eth1/1	Cisco NX 31108PCV A	eth1/3
	eth1/2	Cisco NX 31108PCV B	eth1/3
	eth1/3	NetApp AFF A220 스토리지 컨트롤러 A입니다	e0e
	eth1/4	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0e
	mgmt0	Cisco NX 31108PCV A	eth1/2

다음 표에는 Cisco UCS Fabric Interconnect B의 케이블 연결 정보가 나와 있습니다

로컬 장치	로컬 포트	원격 장치	원격 포트
Cisco UCS 6120 패브릭 인터커넥트 B	eth1/1	Cisco NX 31108PCV A	eth1/4
	eth1/2	Cisco NX 31108PCV B	eth1/4
	eth1/3	NetApp AFF A220 스토리지 컨트롤러 A입니다	e0f
	eth1/4	NetApp AFF A220 스토리지 컨트롤러 B입니다	e0f
	mgmt0	Cisco NX 31108PCV B	eth1/2

구현 절차

이 문서에서는 완전히 이중화된 고가용성 FlexPod Express 시스템을 구성하는 방법에 대해 자세히 설명합니다. 이러한 이중화를 반영하기 위해 각 단계에서 구성 요소를 구성 요소 A 또는 구성 요소 B라고 합니다 예를 들어 컨트롤러 A와 컨트롤러 B는 이 문서에 프로비저닝된 NetApp 스토리지 컨트롤러 2개를 식별합니다. 스위치 A와 스위치 B는 Cisco Nexus 스위치 쌍을 나타냅니다. 패브릭 인터커넥트 A와 패브릭 인터커넥트 B는 통합 Nexus 패브릭 인터커넥트 2개입니다.

또한 서버 A, 서버 B 등으로 순차적으로 구분되는 여러 Cisco UCS 호스트를 프로비저닝하는 단계도 설명합니다.

사용자 환경과 관련된 정보를 단계별로 포함해야 함을 나타내기 위해 명령 구조의 일부로 '<<text>>'이 표시됩니다. 'VLAN create' 명령은 다음 예를 참조하십시오.

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

이 문서를 사용하여 FlexPod Express 환경을 완전히 구성할 수 있습니다. 이 프로세스에서 다양한 단계를 수행하려면 고객별 명명 규칙, IP 주소 및 VLAN(Virtual Local Area Network) 스키마를 삽입해야 합니다. 아래 표에는 이 가이드에 설명된 대로 구축에 필요한 VLAN이 설명되어 있습니다. 이 표는 특정 사이트 변수를 기반으로 완료할 수 있으며 문서 구성 단계를 구현하는 데 사용할 수 있습니다.

별도의 대역내 및 대역외 관리 VLAN을 사용하는 경우 이 VLAN 사이에 계층 3 라우트를 생성해야 합니다. 이 검증에서는 공통 관리 VLAN이 사용되었습니다.

VLAN 이름입니다	**VLAN**의 용도	이 문서의 유효성을 검사하는 데 사용되는 **ID**입니다
관리 VLAN	관리 인터페이스용 VLAN	18
네이티브 VLAN	태그가 지정되지 않은 프레임이 할당되는 VLAN입니다	2
NFS VLAN	NFS 트래픽용 VLAN	104
VMware vMotion VLAN	가상 머신(VM)을 하나의 물리적 호스트에서 다른 물리적 호스트로 이동하도록 지정된 VLAN	103
VM 트래픽 VLAN	VM 애플리케이션 트래픽용 VLAN	102
iSCSI-A-VLAN	패브릭 A의 iSCSI 트래픽용 VLAN	124를 참조하십시오
iSCSI-B-VLAN	패브릭 B의 iSCSI 트래픽용 VLAN	125

FlexPod Express를 구성하는 동안 VLAN 번호가 필요합니다. VLAN은 "<<var_xxxx_vlan>>"라고 하며, 여기서 "xxxx"는 VLAN의 목적(예: iSCSI-A)입니다.

다음 표에는 생성된 VMware VM이 나와 있습니다.

VM 설명	호스트 이름
VMware vCenter Server를 참조하십시오	Seahawks-vcsa.cie.netapp.com

Cisco Nexus 31108PCV 전개 절차

이 섹션에서는 FlexPod 익스프레스 환경에서 사용되는 Cisco Nexus 31308PCV 스위치 구성에 대해 자세히 설명합니다.

Cisco Nexus 31108PCV 스위치의 초기 설정

이 절차에서는 기본 FlexPod Express 환경에서 사용할 Cisco Nexus 스위치를 구성하는 방법에 대해 설명합니다.

이 절차에서는 NX-OS 소프트웨어 릴리즈 7.0(3) I6(1)을 실행하는 Cisco Nexus 31108PCV를 사용하고 있다고 가정합니다.

1. 초기 부팅이 완료되고 스위치의 콘솔 포트에 연결되면 Cisco NX-OS 설정이 자동으로 시작됩니다. 이 초기 구성에서는 스위치 이름, mgmt0 인터페이스 구성, SSH(Secure Shell) 설정과 같은 기본 설정을 지정합니다.
2. FlexPod 익스프레스 관리 네트워크는 여러 가지 방법으로 구성할 수 있습니다. 31108PCV 스위치의 mgmt0 인터페이스를 기존 관리 네트워크에 연결하거나, 31108PCV 스위치의 mgmt0 인터페이스를 연속 구성으로 연결할 수 있습니다. 하지만 이 링크는 SSH 트래픽과 같은 외부 관리 액세스에 사용할 수 없습니다.

   이 구축 가이드에서는 FlexPod Express Cisco Nexus 31108PCV 스위치가 기존 관리 네트워크에 연결되어 있습니다.
3. Cisco Nexus 31108PCV 스위치를 구성하려면, 스위치의 전원을 켜고 화면에 표시되는 메시지에 따라 두 스위치를 초기 설정하고 스위치 관련 정보에 해당하는 값을 대체합니다.

```
This setup utility will guide you through the basic configuration of the
system. Setup configures only enough connectivity for management of the
system.
```

```
*Note: setup is mainly used for configuring the system initially, when
no configuration is present. So setup always assumes system defaults and
not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip
the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
Create another login account (yes/no) [n]: n
Configure read-only SNMP community string (yes/no) [n]: n
Configure read-write SNMP community string (yes/no) [n]: n
Enter the switch name : 31108PCV-A
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
Configure the default gateway? (yes/no) [y]: y
IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
Configure advanced IP options? (yes/no) [n]: n
Enable the telnet service? (yes/no) [n]: n
Enable the ssh service? (yes/no) [y]: y
Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
Number of rsa key bits <1024-2048> [1024]: <enter>
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address : <<var_ntp_ip>>
Configure default interface layer (L3/L2) [L2]: <enter>
Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]:
<enter>
```

4. 구성 요약이 표시되고 구성을 편집할지 묻는 메시지가 표시됩니다. 구성이 올바르면 n을 입력합니다.

```
Would you like to edit the configuration? (yes/no) [n]: no
```

5. 그런 다음 이 구성을 사용하고 저장할지 묻는 메시지가 표시됩니다. 그렇다면 y를 입력합니다.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Cisco Nexus 스위치 B에 대해 1단계부터 5단계까지 반복합니다

고급 기능을 활성화합니다

추가 구성 옵션을 제공하려면 Cisco NX-OS에서 특정 고급 기능을 사용하도록 설정해야 합니다.

1. Cisco Nexus 스위치 A와 스위치 B에서 적절한 기능을 활성화하려면 '(config t)' 명령을 사용하여 구성 모드를 시작하고 다음 명령을 실행합니다.

```
feature interface-vlan
feature lacp
feature vpc
```

> 기본 포트 채널 로드 밸런싱 해쉬는 소스 및 타깃 IP 주소를 사용하여 포트 채널의 인터페이스에 대한 로드 밸런싱 알고리즘을 결정합니다. 소스 및 타깃 IP 주소보다 많은 입력을 해쉬 알고리즘에 제공하면 포트 채널 멤버 전체에 걸쳐 더 효율적으로 분산될 수 있습니다. 동일한 이유로 소스 및 타깃 TCP 포트를 해쉬 알고리즘에 추가하는 것이 좋습니다.

2. 구성 모드 '(config t)에서 다음 명령을 실행하여 Cisco Nexus 스위치 A 및 스위치 B의 글로벌 포트 채널 로드 밸런싱 구성을 설정하십시오.

```
port-channel load-balance src-dst ip-l4port
```

글로벌 스패닝 트리 구성을 수행합니다

Cisco Nexus 플랫폼은 브리지 보장이라는 새로운 보호 기능을 사용합니다. 브리지 보장은 스패닝 트리 알고리즘을 더 이상 실행하지 않는 장치에서 데이터 트래픽을 계속 전달하는 단방향 링크 또는 기타 소프트웨어 장애를 방지합니다. 플랫폼에 따라 네트워크 또는 가장자리를 포함한 여러 상태 중 하나에 포트를 배치할 수 있습니다.

기본적으로 모든 포트가 네트워크 포트로 간주되도록 브리지 보장을 설정하는 것이 좋습니다. 이 설정은 네트워크 관리자가 각 포트의 구성을 검토하도록 합니다. 또한 확인되지 않은 에지 포트 또는 브리지 보장 기능이 활성화되지 않은 인접 장치와 같은 가장 일반적인 구성 오류도 표시됩니다. 또한 스패닝 트리에서 너무 적은 포트가 아니라 많은 포트를 차단하는 편이 더 안전합니다. 그러면 기본 포트 상태를 통해 네트워크의 전반적인 안정성을 향상할 수 있습니다.

특히 브리지 보장을 지원하지 않는 서버, 스토리지 및 업링크 스위치를 추가할 때는 스패닝 트리 상태에 세심한 주의를 기울여야 합니다. 이러한 경우 포트를 활성화하려면 포트 유형을 변경해야 할 수 있습니다.

브리지 프로토콜 데이터 단위(BPDU) 보호대는 기본적으로 다른 보호 계층으로 에지 포트에서 활성화됩니다. 네트워크의 루프를 방지하기 위해 이 기능은 다른 스위치의 BPDU가 이 인터페이스에 표시되는 경우 포트를 종료합니다.

구성 모드('config t')에서 다음 명령을 실행하여 Cisco Nexus 스위치 A 및 스위치 B에서 기본 포트 유형과 BPDU 가드를 포함한 기본 스패닝 트리 옵션을 구성하십시오.

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

VLAN을 정의합니다

VLAN이 서로 다른 개별 포트를 구성하기 전에 스위치에서 레이어 2 VLAN을 정의해야 합니다. 향후 문제 해결이 용이하도록 VLAN 이름을 지정하는 것도 좋은 방법입니다.

구성 모드('config t')에서 다음 명령을 실행하여 Cisco Nexus 스위치 A 및 스위치 B의 계층 2 VLAN을 정의하고 설명하십시오.

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

액세스 및 관리 포트 설명을 구성합니다

레이어 2 VLAN에 이름을 할당하는 경우와 마찬가지로, 모든 인터페이스에 대한 설정 설명은 프로비저닝과 문제 해결에 도움이 될 수 있습니다.

각 스위치의 구성 모드('config t')에서 FlexPod Express 대규모 구성에 대한 다음 포트 설명을 입력합니다.

Cisco Nexus 스위치 **A**

```
int eth1/1
  description AFF A220-A e0M
int eth1/2
  description Cisco UCS FI-A mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/1
int eth1/4
  description Cisco UCS FI-B eth1/1
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

Cisco Nexus 스위치 **B**

```
int eth1/1
  description AFF A220-B e0M
int eth1/2
  description Cisco UCS FI-B mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/2
int eth1/4
  description Cisco UCS FI-B eth1/2
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

서버 및 스토리지 관리 인터페이스를 구성합니다

서버와 스토리지 모두의 관리 인터페이스는 일반적으로 단일 VLAN만 사용합니다. 따라서 관리 인터페이스 포트를 액세스 포트로 구성합니다. 각 스위치에 대한 관리 VLAN을 정의하고 스패닝 트리 포트 유형을 에지로 변경합니다.

구성 모드('config t')에서 다음 명령을 실행하여 서버와 스토리지 모두의 관리 인터페이스에 대한 포트 설정을 구성하십시오.

Cisco Nexus 스위치 **A**

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Cisco Nexus 스위치 **B**

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

NTP 배포 인터페이스를 추가합니다

Cisco Nexus 스위치 **A**

글로벌 구성 모드에서 다음 명령을 실행합니다.

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-a-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-b-ntp-ip> use-vrf default
```

Cisco Nexus 스위치 **B**

글로벌 구성 모드에서 다음 명령을 실행합니다.

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch- b-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-a-ntp-ip> use-vrf default
```

가상 포트 채널 글로벌 구성을 수행합니다

가상 포트 채널(vPC)을 사용하면 물리적으로 두 개의 서로 다른 Cisco Nexus 스위치에 연결된 링크가 세 번째 장치에 단일 포트 채널로 표시될 수 있습니다. 세 번째 장치는 스위치, 서버 또는 다른 네트워킹 장치일 수 있습니다. vPC는 계층 2 다중 경로를 제공할 수 있으므로 대역폭을 높이고, 노드 간에 여러 개의 병렬 경로를 활성화하고, 대체 경로가 있는 로드 밸런싱 트래픽을 통해 이중화를 생성할 수 있습니다.

vPC는 다음과 같은 이점을 제공합니다.

- 단일 장치에서 두 업스트림 장치에 걸쳐 포트 채널을 사용하도록 설정
- 스패닝 트리 프로토콜 차단 포트 제거
- 루프 없는 토폴로지 제공
- 사용 가능한 모든 업링크 대역폭 사용
- 링크 또는 디바이스에 장애가 발생할 경우 빠른 컨버전스를 제공합니다
- 링크 레벨의 복원력 제공
- 고가용성 제공 지원

vPC 기능이 제대로 작동하려면 두 Cisco Nexus 스위치 간의 몇 가지 초기 설정이 필요합니다. 연속 인접 mgmt0 구성을 사용하는 경우에는 인터페이스에 정의된 주소를 사용하고 ping "<<switch_a/B_mgmt0_ip_addr>>VRF" 관리 명령을 사용하여 통신 가능 여부를 확인해야 합니다.

구성 모드('config t')에서 다음 명령을 실행하여 두 스위치에 대한 vPC 글로벌 구성을 설정하십시오.

Cisco Nexus 스위치 **A**

```
vpc domain 1
 role priority 10
peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10description vPC peer-link
switchport
switchport mode trunkswitchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
  channel-group 14 mode active
copy run start
```

Cisco Nexus 스위치 B

```
vpc domain 1
peer-switch
role priority 20
peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10
description vPC peer-link
switchport
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
```

```
  channel-group 14 mode active
copy run start
```

이 솔루션 검증에서 MTU(Maximum Transmission Unit) 9000이 사용되었습니다. 그러나 애플리케이션 요구 사항에 따라 MTU의 적절한 값을 구성할 수 있습니다. FlexPod 솔루션에서 동일한 MTU 값을 설정하는 것이 중요합니다. 구성 요소 간의 MTU 구성이 잘못되면 패킷이 삭제됩니다.

기존 네트워크 인프라로 업링크

사용 가능한 네트워크 인프라에 따라 여러 가지 방법과 기능을 사용하여 FlexPod 환경을 업링크할 수 있습니다. 기존 Cisco Nexus 환경이 존재하는 경우, NetApp은 vPC를 사용하여 FlexPod 환경에 포함된 Cisco Nexus 31108PVC 스위치를 인프라로 업링크하는 것을 권장합니다. 업링크는 10GbE 인프라스트럭처 솔루션의 경우 10GbE 업링크, 필요한 경우 1GbE 인프라스트럭처 솔루션의 경우 1GbE가 될 수 있습니다. 앞서 설명한 절차를 사용하여 기존 환경에 대한 업링크 vPC를 생성할 수 있습니다. 구성이 완료된 후 각 스위치에 대한 구성을 저장하려면 copy run start를 실행해야 합니다.

NetApp 스토리지 구축 절차(1부)

이 섹션에서는 NetApp AFF 스토리지 구축 절차를 설명합니다.

NetApp 스토리지 컨트롤러 AFF2xx 시리즈 설치

NetApp Hardware Universe를 참조하십시오

를 클릭합니다 "NetApp Hardware Universe를 참조하십시오" (HWU) 애플리케이션은 특정 ONTAP 버전에 대해 지원되는 하드웨어 및 소프트웨어 구성요소를 제공합니다. 현재 ONTAP 소프트웨어가 지원하는 모든 NetApp 스토리지 어플라이언스에 대한 구성 정보를 제공합니다. 구성요소 호환성 표도 제공합니다.

사용하려는 하드웨어 및 소프트웨어 구성 요소가 설치하려는 ONTAP 버전에서 지원되는지 확인합니다.

1. 에 액세스합니다 "HWU" 응용 프로그램 - 시스템 구성 가이드를 봅니다. 스토리지 시스템 비교 탭을 선택하여 ONTAP 소프트웨어의 다른 버전과 원하는 사양이 있는 NetApp 스토리지 어플라이언스 간의 호환성을 확인하십시오.
2. 또는 스토리지 어플라이언스별로 구성 요소를 비교하려면 스토리지 시스템 비교 를 클릭합니다.

컨트롤러 AFF2XX 시리즈 사전 요구 사항
스토리지 시스템의 물리적 위치를 계획하려면 다음 섹션을 참조하십시오. 전기 요구 사항 지원되는 전원 코드 온보드 포트 및 케이블

스토리지 컨트롤러

의 컨트롤러에 대한 물리적 설치 절차를 따릅니다 "AFF A220 문서".

NetApp ONTAP 9.5

구성 워크시트

설치 스크립트를 실행하기 전에 제품 설명서에서 구성 워크시트를 작성하십시오. 구성 워크시트는 에서 사용할 수 있습니다 "ONTAP 9.5 소프트웨어 설치 안내서" (에서 사용 가능 "ONTAP 9 문서 센터")를 클릭합니다. 아래 표에는 ONTAP 9.5 설치 및 구성 정보가 나와 있습니다.

이 시스템은 스위치가 없는 2노드 클러스터 구성에서 설정됩니다.

클러스터 세부 정보	클러스터 세부 정보 값입니다
클러스터 노드 A IP 주소입니다	<<var_NodeA_mgmt_ip>> 를 입력합니다
클러스터 노드 A 넷마스크	<<var_NodeA_mgmt_mask>> 를 입력합니다
클러스터 노드 A 게이트웨이	<<var_NodeA_mgmt_gateway>> 를 참조하십시오
클러스터 노드 A 이름	<<var_NodeA>> 를 참조하십시오
클러스터 노드 B IP 주소입니다	<<var_NodeB_mgmt_ip>> 를 입력합니다
클러스터 노드 B 넷마스크	<<var_NodeB_mgmt_mask>> 를 입력합니다
클러스터 노드 B 게이트웨이	<<var_NodeB_mgmt_gateway>> 를 참조하십시오
클러스터 노드 B 이름	<<var_NodeB>> 를 참조하십시오
ONTAP 9.5 URL	<<var_url_boot_software>>
클러스터의 이름입니다	<<var_clustername>> 를 클릭합니다
클러스터 관리 IP 주소입니다	<<var_clustermgmt_ip>> 를 입력합니다
클러스터 B 게이트웨이	<<var_clustermgmt_gateway>> 를 클릭합니다
클러스터 B 넷마스크	<<var_clustermgmt_mask>> 를 입력합니다
도메인 이름	<<var_domain_name>>
DNS 서버 IP(둘 이상 입력할 수 있음)	<<var_dns_server_ip>> 를 참조하십시오
NTP 서버 A IP입니다	스위치-A-NTP-IP>>
NTP 서버 B IP입니다	switch-b-ntp-ip>>

노드 **A**를 구성합니다

노드 A를 구성하려면 다음 단계를 완료하십시오.

1. 스토리지 시스템 콘솔 포트에 연결합니다. Loader-A 메시지가 표시됩니다. 하지만 스토리지 시스템이 재부팅 루프 상태인 경우 다음 메시지가 표시될 때 Ctrl-C를 눌러 자동 부팅 루프를 종료합니다.

```
Starting AUTOBOOT press Ctrl-C to abort...
```

2. 시스템이 부팅되도록 합니다.

```
autoboot
```

3. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.

   ONTAP 9인 경우 5는 부팅 중인 소프트웨어 버전이 아닙니다. 새 소프트웨어를 설치하려면 다음 단계를 계속 수행하십시오. ONTAP 9인 경우 5는 부팅 중인 버전이며 옵션 8과 y를 선택하여 노드를 재부팅합니다. 그런 다음 14단계를 계속합니다.

4. 새 소프트웨어를 설치하려면 옵션 '7'을 선택합니다.
5. 업그레이드를 수행하려면 y를 입력하십시오.
6. 다운로드에 사용할 네트워크 포트로 e0M 을 선택합니다.
7. 지금 재부팅하려면 y를 입력하십시오.
8. 각 위치에 e0M의 IP 주소, 넷마스크 및 기본 게이트웨이를 입력합니다.

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

9. 소프트웨어를 찾을 수 있는 URL을 입력합니다.

   이 웹 서버는 Ping할 수 있어야 합니다.

10. 사용자 이름에 대해 Enter 키를 눌러 사용자 이름이 없음을 나타냅니다.
11. 새로 설치한 소프트웨어를 이후 재부팅에 사용할 기본값으로 설정하려면 'y'를 입력합니다.
12. 노드를 재부팅하려면 y를 입력합니다.

    새 소프트웨어를 설치할 때 시스템이 BIOS 및 어댑터 카드에 대한 펌웨어 업그레이드를 수행할 수 있으며, 이로 인해 LOADER-A 프롬프트에서 재부팅되고 중지될 수 있습니다. 이러한 작업이 발생하면 시스템이 이 절차를 벗어날 수 있습니다.

13. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.
14. Clean Configuration 및 Initialize All Disks 옵션을 4로 선택합니다.
15. 디스크를 제로화하려면 y를 입력하고 구성을 재설정한 다음 새 파일 시스템을 설치합니다.
16. 디스크에 있는 모든 데이터를 지우려면 'y'를 입력합니다.

    연결된 디스크의 수와 유형에 따라 루트 애그리게이트의 초기화 및 생성을 완료하는 데 90분 이상이 걸릴 수 있습니다. 초기화가 완료되면 스토리지 시스템이 재부팅됩니다. SSD를 초기화하는 데 걸리는 시간은 상당히 줄어듭니다. 노드 A용 디스크가 제로화하는 동안 노드 B 구성을 계속할 수 있습니다.

17. 노드 A를 초기화하는 동안 노드 B를 구성합니다

노드 **B**를 구성합니다

노드 B를 구성하려면 다음 단계를 완료하십시오.

1. 스토리지 시스템 콘솔 포트에 연결합니다. Loader-A 메시지가 표시됩니다. 하지만 스토리지 시스템이 재부팅 루프 상태인 경우 다음 메시지가 표시될 때 Ctrl-C를 눌러 자동 부팅 루프를 종료합니다.

```
Starting AUTOBOOT press Ctrl-C to abort...
```

2. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.

```
autoboot
```

3. 메시지가 나타나면 Ctrl-C를 누릅니다.

   ONTAP 9인 경우 5는 부팅 중인 소프트웨어 버전이 아닙니다. 새 소프트웨어를 설치하려면 다음 단계를 계속 수행하십시오. ONTAP 9.4가 부팅 중인 버전인 경우 옵션 8 및 y를 선택하여 노드를 재부팅합니다. 그런 다음 14단계를 계속합니다.

4. 새 소프트웨어를 설치하려면 옵션 7을 선택합니다.
5. 업그레이드를 수행하려면 y를 입력하십시오.
6. 다운로드에 사용할 네트워크 포트로 e0M 을 선택합니다.
7. 지금 재부팅하려면 y를 입력하십시오.
8. 각 위치에 e0M의 IP 주소, 넷마스크 및 기본 게이트웨이를 입력합니다.

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. 소프트웨어를 찾을 수 있는 URL을 입력합니다.

   이 웹 서버는 Ping할 수 있어야 합니다.

```
<<var_url_boot_software>>
```

10. 사용자 이름에 대해 Enter 키를 눌러 사용자 이름이 없음을 나타냅니다
11. 새로 설치한 소프트웨어를 이후 재부팅에 사용할 기본값으로 설정하려면 'y'를 입력합니다.
12. 노드를 재부팅하려면 y를 입력합니다.

    새 소프트웨어를 설치할 때 시스템이 BIOS 및 어댑터 카드에 대한 펌웨어 업그레이드를 수행할 수 있으며, 이로 인해 LOADER-A 프롬프트에서 재부팅되고 중지될 수 있습니다. 이러한 작업이 발생하면 시스템이 이 절차를 벗어날 수 있습니다.

13. Ctrl-C를 눌러 부팅 메뉴로 들어갑니다.
14. Clean Configuration(구성 정리) 및 Initialize All Disks(모든 디스크 초기화) 에 대해 옵션 4 를 선택합니다.
15. 디스크를 제로화하려면 y를 입력하고 구성을 재설정한 다음 새 파일 시스템을 설치합니다.
16. 디스크에 있는 모든 데이터를 지우려면 'y'를 입력합니다.

    연결된 디스크의 수와 유형에 따라 루트 애그리게이트의 초기화 및 생성을 완료하는 데 90분 이상이 걸릴 수 있습니다. 초기화가 완료되면 스토리지 시스템이 재부팅됩니다. SSD를 초기화하는 데 걸리는 시간은 상당히 줄어듭니다.

연속 노드 구성 및 클러스터 구성

스토리지 컨트롤러 A(노드 A) 콘솔 포트에 연결된 콘솔 포트 프로그램에서 노드 설정 스크립트를 실행합니다. 이

스크립트는 ONTAP 9.5가 노드에서 처음 부팅될 때 나타납니다.

ONTAP 9.5에서 노드 및 클러스터 설정 절차가 약간 변경되었습니다. 이제 클러스터 설정 마법사를 사용하여 클러스터의 첫 번째 노드를 구성하고 System Manager를 사용하여 클러스터를 구성할 수 있습니다.

1. 프롬프트에 따라 노드 A를 설정합니다

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. 노드의 관리 인터페이스의 IP 주소로 이동합니다.

> CLI를 사용하여 클러스터를 설정할 수도 있습니다. 이 문서에서는 NetApp System Manager의 안내에 따라 설정을 사용하는 클러스터 설정에 대해 설명합니다.

3. Guided Setup(안내식 설정) 을 클릭하여 클러스터를 구성합니다.
4. 클러스터 이름은 <<var_clustername>>'을, 구성 중인 각 노드에 대해서는 <<var_NodeA>>'와 <<var_NodeB>>를 입력합니다. 스토리지 시스템에 사용할 암호를 입력합니다. 클러스터 유형으로 Switchless Cluster를 선택합니다. 클러스터 기본 라이센스를 입력합니다.
5. 클러스터, NFS 및 iSCSI에 대한 기능 라이센스도 입력할 수 있습니다.

6. 클러스터를 생성 중임을 나타내는 상태 메시지가 표시됩니다. 이 상태 메시지는 여러 상태를 순환합니다. 이 과정은 몇 분 정도 소요됩니다.
7. 네트워크를 구성합니다.
   a. IP 주소 범위 옵션을 선택 취소합니다.
   b. Cluster Management IP Address 필드(<<var_clustermgmt_ip>>)에 넷마스크 필드(<<var_clustermgmt_mask>>)에 <<var_clustermgmt_gateway>>)를 입력합니다. 포트 필드의… 선택기를 사용하여 노드 A의 e0M을 선택합니다
   c. 노드 A의 노드 관리 IP가 이미 채워져 있습니다. 노드 B에 대해 '<<var_NodeA_mgmt_ip>>'를 입력합니다
   d. DNS Domain Name 필드에 '<<var_domain_name>>'을 입력합니다. DNS 서버 IP 주소 필드에 '<<var_dns_server_ip>>'를 입력합니다.

      여러 DNS 서버 IP 주소를 입력할 수 있습니다.

   e. Primary NTP Server 필드에 '<<switch-a-ntp-ip>>'를 입력합니다.

      대체 NTP 서버를 "<<switch-b-ntp-ip>>"로 입력할 수도 있습니다.
8. 지원 정보를 구성합니다.
   a. 환경에 AutoSupport에 액세스하기 위한 프록시가 필요한 경우 프록시 URL에 URL을 입력합니다.
   b. 이벤트 알림에 대한 SMTP 메일 호스트 및 이메일 주소를 입력합니다.

      계속하려면 이벤트 알림 방법을 설정해야 합니다. 방법 중 하나를 선택할 수 있습니다.
9. 클러스터 구성이 완료되었으면 클러스터 관리 를 클릭하여 스토리지를 구성합니다.

스토리지 클러스터 구성의 연속

스토리지 노드 및 기본 클러스터를 구성한 후에는 스토리지 클러스터 구성을 계속할 수 있습니다.

모든 스페어 디스크를 제로합니다

클러스터의 모든 스페어 디스크를 제로하려면 다음 명령을 실행합니다.

```
disk zerospares
```

온보드 **UTA2** 포트 속성을 설정합니다

1. ucadmin show 명령을 실행하여 현재 모드와 포트의 현재 유형을 확인합니다.

```
AFFA220-Clus::> ucadmin show
                      Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFFA220-Clus-01
              0c       cna      target     -        -          offline
AFFA220-Clus-01
              0d       cna      target     -        -          offline
AFFA220-Clus-01
              0e       cna      target     -        -          offline
AFFA220-Clus-01
              0f       cna      target     -        -          offline
AFFA220-Clus-02
              0c       cna      target     -        -          offline
AFFA220-Clus-02
              0d       cna      target     -        -          offline
AFFA220-Clus-02
              0e       cna      target     -        -          offline
AFFA220-Clus-02
              0f       cna      target     -        -          offline
8 entries were displayed.
```

2. 사용 중인 포트의 현재 모드가 CNA인지, 현재 유형이 'target'으로 설정되어 있는지 확인합니다. 그렇지 않은 경우 다음 명령을 실행하여 포트 속성을 변경합니다.

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

이전 명령을 실행하려면 포트가 오프라인 상태여야 합니다. 포트를 오프라인으로 전환하려면 다음 명령을 실행합니다.

```
network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down
```

포트 속성을 변경한 경우 변경 사항을 적용하려면 각 노드를 재부팅해야 합니다.

Cisco Discovery Protocol을 활성화합니다

NetApp 스토리지 컨트롤러에서 CDP(Cisco Discovery Protocol)를 활성화하려면 다음 명령을 실행합니다.

```
node run -node * options cdpd.enable on
```

모든 이더넷 포트에서 링크 계층 검색 프로토콜을 활성화합니다

다음 명령을 실행하여 스토리지와 네트워크 스위치 간에 LLDP(Link-layer Discovery Protocol) 인접 정보 교환을 활성화합니다. 이 명령을 실행하면 클러스터에 있는 모든 노드의 모든 포트에 LLDP가 설정됩니다.

```
node run * options lldp.enable on
```

관리 논리 인터페이스의 이름을 바꿉니다

관리 논리 인터페이스(LIF)의 이름을 변경하려면 다음 단계를 수행하십시오.

1. 현재 관리 LIF 이름을 표시합니다.

   ```
   network interface show –vserver <<clustername>>
   ```

2. 클러스터 관리 LIF의 이름을 바꿉니다.

   ```
   network interface rename –vserver <<clustername>> –lif
   cluster_setup_cluster_mgmt_lif_1 –newname cluster_mgmt
   ```

3. 노드 B 관리 LIF의 이름을 바꿉니다.

   ```
   network interface rename -vserver <<clustername>> -lif
   cluster_setup_node_mgmt_lif_AFF A220_A_1 - newname AFF A220-01_mgmt1
   ```

클러스터 관리에서 자동 되돌리기 설정

클러스터 관리 인터페이스에서 자동 되돌리기 매개 변수를 설정합니다.

```
network interface modify –vserver <<clustername>> -lif cluster_mgmt –auto-
revert true
```

서비스 프로세서 네트워크 인터페이스를 설정합니다

각 노드의 서비스 프로세서에 정적 IPv4 주소를 할당하려면 다음 명령을 실행합니다.

```
system service-processor network modify -node <<var_nodeA>> -address
-family IPv4 -enable true - dhcp none -ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify -node <<var_nodeB>> -address
-family IPv4 -enable true - dhcp none -ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

ⓘ 서비스 프로세서 IP 주소는 노드 관리 IP 주소와 동일한 서브넷에 있어야 합니다.

ONTAP에서 스토리지 페일오버 설정

스토리지 페일오버가 설정되었는지 확인하려면 페일오버 쌍에서 다음 명령을 실행합니다.

1. 스토리지 페일오버 상태를 확인합니다.

   ```
   storage failover show
   ```

   '<<var_NodeA>>'와 '<<var_NodeB>>'는 모두 테이크오버를 수행할 수 있어야 합니다. 노드가 테이크오버 수행 가능한 경우 3단계로 이동하십시오.

2. 두 노드 중 하나에서 페일오버가 사용되도록 설정합니다.

   ```
   storage failover modify -node <<var_nodeA>> -enabled true
   ```

3. 2노드 클러스터의 HA 상태를 확인합니다.

   ⓘ 2개 이상의 노드가 있는 클러스터에는 이 단계를 적용할 수 없습니다.

   ```
   cluster ha show
   ```

4. 고가용성이 구성된 경우 6단계로 이동합니다. 고가용성이 구성된 경우 명령을 실행하면 다음 메시지가 표시됩니다.

   ```
   High Availability Configured: true
   ```

5. 2노드 클러스터에만 HA 모드를 사용하도록 설정합니다.

   2개 이상의 노드가 있는 클러스터에서는 페일오버에 문제가 발생하므로 이 명령을 실행하지 마십시오.

   ```
   cluster ha modify -configured true
   Do you want to continue? {y|n}: y
   ```

6. 하드웨어 지원이 올바르게 구성되어 있는지 확인하고 필요한 경우 파트너 IP 주소를 수정합니다.

```
storage failover hwassist show
```

"Keep Alive Status: Error: whwassist keep alive alert from partner(활성 상태 유지: 오류: 파트너의 hwassist keep alive 경고를 수신하지 못했습니다)" 메시지는 하드웨어 지원이 구성되지 않았음을 나타냅니다. 다음 명령을 실행하여 하드웨어 지원을 구성합니다.

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

ONTAP에서 점보 프레임 **MTU** 브로드캐스트 도메인을 생성합니다

MTU가 9000인 데이터 브로드캐스트 도메인을 생성하려면 다음 명령을 실행합니다.

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

기본 브로드캐스트 도메인에서 데이터 포트를 제거합니다

10GbE 데이터 포트는 iSCSI/NFS 트래픽에 사용되며 이러한 포트는 기본 도메인에서 제거해야 합니다. 포트 e0e 및 e0f는 사용되지 않으며 기본 도메인에서도 제거해야 합니다.

브로드캐스트 도메인에서 포트를 제거하려면 다음 명령을 실행합니다.

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

UTA2 포트에서 흐름 제어를 사용하지 않도록 설정합니다

외부 장치에 연결된 모든 UTA2 포트에서 흐름 제어를 사용하지 않도록 설정하는 것이 NetApp의 모범 사례입니다. 흐름 제어를 사용하지 않도록 설정하려면 다음 명령을 실행합니다.

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
```

ONTAP에 대한 Cisco UCS Mini 직접 연결은 LACP를 지원하지 않습니다.

NetApp ONTAP에서 점보 프레임을 구성합니다

ONTAP 네트워크 포트에서 점보 프레임(일반적으로 9,000바이트 MTU 사용)을 사용하도록 구성하려면 클러스터 쉘에서 다음 명령을 실행합니다.

```
AFF A220::> network port modify -node node_A -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_A -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
```

ONTAP에서 **VLAN**을 생성합니다

ONTAP에서 VLAN을 생성하려면 다음 단계를 수행하십시오.

1. NFS VLAN 포트를 생성하여 데이터 브로드캐스트 도메인에 추가합니다.

```
network port vlan create –node <<var_nodeA>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeA>> -vlan-name e0f-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0f-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>: e0e- <<var_nfs_vlan_id>>, <<var_nodeB>>: e0e-
<<var_nfs_vlan_id>> , <<var_nodeA>>:e0f- <<var_nfs_vlan_id>>,
<<var_nodeB>>:e0f-<<var_nfs_vlan_id>>
```

2. iSCSI VLAN 포트를 생성하여 데이터 브로드캐스트 도메인에 추가합니다.

```
network port vlan create –node <<var_nodeA>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>: e0e- <<var_iscsi_vlan_A_id>>,<<var_nodeB>>: e0e-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>: e0f- <<var_iscsi_vlan_B_id>>,<<var_nodeB>>: e0f-
<<var_iscsi_vlan_B_id>>
```

3. MGMT-VLAN 포트를 생성합니다.

```
network port vlan create –node <<var_nodeA>> -vlan-name e0m-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0m-
<<mgmt_vlan_id>>
```

ONTAP에서 애그리게이트를 생성합니다

ONTAP 설정 프로세스 중에 루트 볼륨이 포함된 애그리게이트가 생성됩니다. 추가 애그리게이트를 생성하려면 애그리게이트 이름, 애그리게이트를 생성할 노드, 애그리게이트에 포함된 디스크 수를 결정합니다.

Aggregate를 생성하려면 다음 명령을 실행합니다.

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

구성에 최소 하나의 디스크(가장 큰 디스크 선택)를 스페어로 보관합니다. 모범 사례는 각 디스크 유형 및 크기에 대해 하나 이상의 스페어를 두는 것입니다.

5개의 디스크로 시작합니다. 스토리지를 추가해야 할 때 디스크를 애그리게이트에 추가할 수 있습니다.

디스크 비우기가 완료될 때까지 애그리게이트를 생성할 수 없습니다. 집계 생성 상태를 표시하려면 'aggr show' 명령을 실행합니다. aggr1_NodeA가 온라인이 될 때까지 진행하지 마십시오.

ONTAP에서 시간대를 구성합니다

시간 동기화를 구성하고 클러스터에서 표준 시간대를 설정하려면 다음 명령을 실행합니다.

```
timezone <<var_timezone>>
```

예를 들어, 미국 동부의 시간대는 '아메리카/뉴욕'입니다. 표준 시간대 이름을 입력하기 시작하면 Tab 키를 눌러 사용 가능한 옵션을 확인합니다.

ONTAP에서 SNMP를 구성합니다

SNMP를 구성하려면 다음 단계를 수행하십시오.

1. 위치 및 연락처와 같은 SNMP 기본 정보를 구성합니다. 이 정보는 SNMP에서 'SysLocation', 'SysContact' 변수로 표시됩니다.

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_snmp_location>>"
snmp init 1
options snmp.enable on
```

2. 원격 호스트에 보낼 SNMP 트랩을 구성합니다.

```
snmp traphost add <<var_snmp_server_fqdn>>
```

ONTAP에서 SNMPv1을 구성합니다

SNMPv1을 구성하려면 커뮤니티라는 공유 암호 일반 텍스트 암호를 설정합니다.

```
snmp community add ro <<var_snmp_community>>
```

NMP community delete all 명령을 주의하여 사용한다. 다른 모니터링 제품에 커뮤니티 문자열을 사용하는 경우 이 명령은 해당 문자열을 제거합니다.

ONTAP에서 SNMPv3을 구성합니다

SNMPv3을 사용하려면 인증을 위해 사용자를 정의하고 구성해야 합니다. SNMPv3을 구성하려면 다음 단계를 수행하십시오.

1. Security snmpusers 명령을 실행하여 엔진 ID를 조회한다.
2. 'snmpv3user'라는 사용자를 생성합니다.

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. 신뢰할 수 있는 엔터티의 엔진 ID를 입력하고 인증 프로토콜로 md5 를 선택한다.
4. 메시지가 나타나면 인증 프로토콜에 사용할 최소 길이 8자로 된 암호를 입력합니다.
5. 개인 정보 보호 프로토콜로 'des'를 선택합니다.
6. 메시지가 나타나면 개인 정보 보호 프로토콜에 사용할 최소 길이 8자로 된 암호를 입력합니다.

ONTAP에서 **AutoSupport HTTPS**를 구성합니다

NetApp AutoSupport 툴은 HTTPS를 통해 지원 요약 정보를 NetApp에 보냅니다. AutoSupport를 구성하려면 다음 명령을 실행합니다.

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

스토리지 가상 머신을 생성합니다

인프라 스토리지 가상 시스템(SVM)을 생성하려면 다음 단계를 완료하십시오.

1. 'vserver create' 명령을 실행합니다.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume- security-style unix
```

2. NetApp VSC를 위한 인프라-SVM 애그리게이트 목록에 데이터 애그리게이트를 추가합니다.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. NFS와 iSCSI를 남겨두고 SVM에서 사용하지 않는 스토리지 프로토콜을 제거합니다.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. 인프라 SVM에서 NFS 프로토콜을 사용하고 실행합니다.

```
nfs create -vserver Infra-SVM -udp disabled
```

5. NetApp NFS VAAI 플러그인에 대한 'VM vStorage' 매개 변수를 설정합니다. 그런 다음 NFS가 구성되었는지 확인합니다.

```
vserver nfs modify -vserver Infra-SVM -vstorage enabled
vserver nfs show
```

SVM은 이전에 서버라고 불렸던 것이기 때문에 명령행에서 'vserver'가 명령을 앞에 표시합니다

ONTAP에서 **NFSv3**을 구성합니다

아래 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
ESXi 호스트 NFS IP 주소입니다	<<var_esxi_hostA_nfs_ip>> 를 참조하십시오
ESXi 호스트 B NFS IP 주소입니다	<<var_esxi_hostB_nfs_ip>> 를 참조하십시오

SVM에서 NFS를 구성하려면 다음 명령을 실행합니다.

1. 기본 엑스포트 정책에서 각 ESXi 호스트에 대한 규칙을 생성합니다.
2. 생성 중인 각 ESXi 호스트에 대해 규칙을 할당합니다. 각 호스트에는 고유한 규칙 인덱스가 있습니다. 첫 번째 ESXi 호스트에는 규칙 인덱스 1이 있고 두 번째 ESXi 호스트에는 규칙 인덱스 2가 있습니다.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid falsevserver export-
policy rule create –vserver Infra-SVM -policyname default –ruleindex 2
-protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>> -rorule sys –rwrule
sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. 인프라 SVM 루트 볼륨에 엑스포트 정책을 할당합니다.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

vSphere를 설정한 후 NetApp VSC는 엑스포트 정책을 자동으로 처리합니다. 설치하지 않은 경우 Cisco UCS B-Series 서버를 추가할 때 엑스포트 정책 규칙을 생성해야 합니다.

ONTAP에서 **iSCSI** 서비스를 생성합니다

iSCSI 서비스를 생성하려면 다음 단계를 완료하십시오.

1. SVM에서 iSCSI 서비스를 생성합니다. 또한 이 명령은 iSCSI 서비스를 시작하고 SVM에 대한 IQN(iSCSI Qualified Name)을 설정합니다. iSCSI가 구성되었는지 확인합니다.

```
iscsi create -vserver Infra-SVM
iscsi show
```

ONTAP에서 SVM 루트 볼륨의 로드 공유 미러를 생성합니다

ONTAP에서 SVM 루트 볼륨의 로드 공유 미러를 생성하려면 다음 단계를 수행하십시오.

1. 각 노드에서 인프라 SVM 루트 볼륨의 로드 공유 미러가 될 볼륨을 생성합니다.

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
aggr1_nodeA –size 1GB –type DPvolume create –vserver Infra_Vserver
–volume rootvol_m02 –aggregate aggr1_nodeB –size 1GB –type DP
```

2. 15분마다 루트 볼륨 미러 관계를 업데이트하는 작업 스케줄을 생성합니다.

```
job schedule interval create -name 15min -minutes 15
```

3. 미러링 관계를 생성합니다.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. 미러링 관계를 초기화하고 미러링 관계가 만들어졌는지 확인합니다.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol snapmirror
show
```

ONTAP에서 HTTPS 액세스를 구성합니다

스토리지 컨트롤러에 대한 보안 액세스를 구성하려면 다음 단계를 수행하십시오.

1. 인증서 명령에 액세스할 수 있도록 권한 수준을 높입니다.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. 일반적으로 자체 서명된 인증서가 이미 있습니다. 다음 명령을 실행하여 인증서를 확인합니다.

```
security certificate show
```

3. 표시된 각 SVM에서 인증서 공통 이름은 SVM의 DNS FQDN(정규화된 도메인 이름)과 일치해야 합니다. 네 개의 기본 인증서를 삭제하고 자체 서명된 인증서 또는 인증 기관의 인증서로 대체해야 합니다.

   인증서를 만들기 전에 만료된 인증서를 삭제하는 것이 좋습니다. 만료된 인증서를 삭제하려면 보안 인증서 삭제 명령을 실행합니다. 다음 명령에서 Tab completion을 사용하여 각 기본 인증서를 선택하고 삭제합니다.

```
security certificate delete [TAB] ...
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM - type server -serial 552429A6
```

4. 자체 서명된 인증서를 생성하고 설치하려면 다음 명령을 일회성 명령으로 실행합니다. 인프라 SVM 및 클러스터 SVM에 대한 서버 인증서를 생성합니다. 다시 한 번 탭 완료 기능을 사용하면 이러한 명령을 쉽게 완료할 수 있습니다.

```
security certificate create [TAB] ...
Example: security certificate create -common-name infra-svm.netapp.com
-type server -size 2048 - country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email- addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. 다음 단계에서 필요한 매개 변수 값을 얻으려면 'security certificate show' 명령을 실행합니다.
6. '–server-enabled true' 및 '–client-enabled false' 매개 변수를 사용하여 방금 만든 각 인증서를 활성화합니다. 다시 탭 완료를 사용합니다.

```
security ssl modify [TAB] ...
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. SSL 및 HTTPS 액세스를 구성 및 활성화하고 HTTP 액세스를 비활성화합니다.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
System services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

명령 실행 중 일부에서 항목이 존재하지 않는다는 오류 메시지가 반환되는 것은 정상입니다.

8. 관리 권한 수준으로 되돌아가며 SVM을 웹에서 사용할 수 있도록 설정을 생성합니다.

```
set -privilege admin
vserver services web modify -name spi|ontapi|compat -vserver * -enabled
true
```

ONTAP에서 **NetApp FlexVol** 볼륨을 생성합니다

NetApp FlexVol ® 볼륨을 생성하려면 볼륨 이름, 크기 및 해당 볼륨을 입력합니다. 2개의 VMware 데이터 저장소 볼륨과 서버 부팅 볼륨을 생성합니다.

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB - state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent- snapshot-space 0
volume create -vserver Infra-SVM -volume infra_datastore_2 -aggregate
aggr1_nodeB -size 500GB - state online -policy default -junction-path
/infra_datastore_2 -space-guarantee none -percent- snapshot-space 0
```

```
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -juntion-path /infra_swap -space
-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

ONTAP에서 중복 제거를 설정합니다

하루에 한 번 적절한 볼륨에서 중복 제거를 설정하려면 다음 명령을 실행합니다.

```
volume efficiency modify -vserver Infra-SVM -volume esxi_boot -schedule
sun-sat@0
volume efficiency modify -vserver Infra-SVM -volume infra_datastore_1
-schedule sun-sat@0
volume efficiency modify -vserver Infra-SVM -volume infra_datastore_2
-schedule sun-sat@0
```

ONTAP에서 **LUN**을 생성합니다

두 개의 부팅 논리 유닛 번호(LUN)를 생성하려면 다음 명령을 실행합니다.

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware - space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware - space-reserve disabled
```

Cisco UCS C-Series 서버를 더 추가할 때는 부팅 LUN을 더 생성해야 합니다.

ONTAP에서 **iSCSI LIF**를 생성합니다

아래 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
스토리지 노드 A iSCSI LIF01A	<<var_NodeA_iscsi_lif01a_ip>> 를 참조하십시오
스토리지 노드 A iSCSI LIF01A 네트워크 마스크입니다	<<var_NodeA_iscsi_lif01a_mask>>
스토리지 노드 A iSCSI LIF01B	<<var_NodeA_iscsi_liff 01b_ip>> 를 참조하십시오
스토리지 노드 A iSCSI LIF01B 네트워크 마스크입니다	<<var_NodeA_iscsi_liff 01b_mask>>
스토리지 노드 B iSCSI LIF01A	<<var_NodeB_iscsi_liff 01a_ip>>
스토리지 노드 B iSCSI LIF01A 네트워크 마스크입니다	<<var_NodeB_iscsi_liff 01a_mask>>
스토리지 노드 B iSCSI LIF01B	<<var_NodeB_iscsi_liff 01b_ip>>
스토리지 노드 B iSCSI LIF01B 네트워크 마스크입니다	<<var_NodeB_iscsi_liff 01b_mask>>

1. 각 노드에 2개의 iSCSI LIF를 4개 생성합니다.

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface show
```

ONTAP에서 **NFS LIF**를 생성합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
스토리지 노드 A NFS LIF 01 A IP	<<var_NodeA_nfs_lif_01_a_ip>>
스토리지 노드 A NFS LIF 01 네트워크 마스크입니다	<<var_NodeA_nfs_lif_01_a_mask>>
스토리지 노드 A NFS LIF 01 b IP입니다	<<var_NodeA_nfs_lif_01_b_ip>>
스토리지 노드 A NFS LIF 01 b 네트워크 마스크	<<var_NodeA_nfs_lif_01_b_mask>>
스토리지 노드 B NFS LIF 02 A IP	<<var_NodeB_nfs_lif_02_a_ip>>
스토리지 노드 B NFS LIF 02 A 네트워크 마스크	<<var_NodeB_nfs_lif_02_a_mask>>
스토리지 노드 B NFS LIF 02 b IP	<<var_NodeB_nfs_lif_02_b_ip>>
스토리지 노드 B NFS LIF 02 b 네트워크 마스크	<<var_NodeB_nfs_lif_02_b_mask>>

1. NFS LIF를 생성합니다.

```
network interface create -vserver Infra-SVM -lif nfs_lif01_a -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0e-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_a_ip>> - netmask <<
var_nodeA_nfs_lif_01_a_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif01_b -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0f-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_b_ip>> - netmask <<
var_nodeA_nfs_lif_01_b_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_a -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0e-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_a_ip>> - netmask <<
var_nodeB_nfs_lif_02_a_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_b -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0f-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_b_ip>> - netmask <<
var_nodeB_nfs_lif_02_b_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface show
```

인프라 **SVM** 관리자를 추가합니다

다음 표에는 이 구성을 완료하는 데 필요한 정보가 나와 있습니다.

세부 정보	상세 값
Vsmgmt IP	<<var_svm_mgmt_ip>> 를 입력합니다
Vsmgmt 네트워크 마스크	<<var_svm_mgmt_mask>>
Vsmgmt 기본 게이트웨이	<<var_svm_mgmt_gateway>>

인프라 SVM 관리자 및 SVM 관리 LIF를 관리 네트워크에 추가하려면 다음 단계를 완료하십시오.

1. 다음 명령을 실행합니다.

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data
–data-protocol none –home-node <<var_nodeB>> -home-port e0M –address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> - status-admin up
–failover-policy broadcast-domain-wide –firewall-policy mgmt –auto-
revert true
```

ⓘ 여기서 SVM 관리 IP는 스토리지 클러스터 관리 IP와 동일한 서브넷에 있어야 합니다.

2. 기본 경로를 생성하여 SVM 관리 인터페이스가 외부 환경에 도달할 수 있도록 합니다.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_svm_mgmt_gateway>> network route show
```

3. SVM 'vsadmin' 사용자의 비밀번호를 설정하고 사용자 잠금을 해제합니다.

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock –username vsadmin –vserver
```

Cisco UCS 서버 구성

FlexPod Cisco UCS 기반

FlexPod 환경을 위한 Cisco UCS 6324 패브릭 인터커넥트를 초기 설정합니다.

이 섹션에서는 Cisco UCS Manger를 사용하여 FlexPod ROBO 환경에서 Cisco UCS를 사용하도록 구성하는 절차를 자세히 설명합니다.

Cisco UCS 패브릭 인터커넥트 6324 A

Cisco UCS는 액세스 계층 네트워킹 및 서버를 사용합니다. 이 고성능 차세대 서버 시스템은 데이터 센터에 높은 수준의 워크로드 민첩성 및 확장성을 제공합니다.

Cisco UCS Manager 4.0(1b)은 패브릭 인터커넥트를 Cisco UCS 섀시에 통합하고 더 작은 구축 환경을 위한 통합 솔루션을 제공하는 6324 패브릭 인터커넥트를 지원합니다. Cisco UCS Mini는 시스템 관리를 단순화하고 저렴한 배포 비용을 절감해 줍니다.

하드웨어 및 소프트웨어 구성 요소는 단일 통합 네트워크 어댑터를 통해 여러 유형의 데이터 센터 트래픽을 실행하는 Cisco의 통합 패브릭을 지원합니다.

초기 시스템 설치

Cisco UCS 도메인에서 패브릭 인터커넥트에 처음 액세스할 때 설정 마법사가 시스템을 구성하는 데 필요한 다음 정보를 묻습니다.

- 설치 방법(GUI 또는 CLI)
- 설정 모드(전체 시스템 백업 또는 초기 설정에서 복원)
- 시스템 구성 유형(독립 실행형 또는 클러스터 구성)
- 시스템 이름입니다
- 관리자 암호입니다
- 관리 포트 IPv4 주소 및 서브넷 마스크, 또는 IPv6 주소 및 접두어
- 기본 게이트웨이 IPv4 또는 IPv6 주소입니다

- DNS 서버 IPv4 또는 IPv6 주소입니다
- 기본 도메인 이름입니다

다음 표에는 Fabric Interconnect A에서 Cisco UCS 초기 구성을 완료하는 데 필요한 정보가 나와 있습니다

세부 정보	상세/값
시스템 이름	<<var_UCS_clustername>>
관리자 암호	<<var_password>> 를 참조하십시오
관리 IP 주소: 패브릭 인터커넥트 A	<<var_ucsa_mgmt_ip>> 를 입력합니다
관리 넷마스크: Fabric Interconnect A	<<var_ucsa_mgmt_mask>>
기본 게이트웨이: Fabric Interconnect A	<<var_ucsa_mgmt_gateway>>
클러스터 IP 주소입니다	<<var_UCS_cluster_ip>> 를 참조하십시오
DNS 서버 IP 주소입니다	<<var_nameserver_ip>> 를 참조하십시오
도메인 이름	<<var_domain_name>>

FlexPod 환경에서 사용할 Cisco UCS를 구성하려면 다음 단계를 완료하십시오.

1. 첫 번째 Cisco UCS 6324 Fabric Interconnect A의 콘솔 포트에 연결합니다

```
Enter the configuration method. (console/gui) ? console

  Enter the setup mode; setup newly or restore from backup.
(setup/restore) ? setup

  You have chosen to setup a new Fabric interconnect. Continue? (y/n): y

  Enforce strong password? (y/n) [y]: Enter

  Enter the password for "admin":<<var_password>>
  Confirm the password for "admin":<<var_password>>

  Is this Fabric interconnect part of a cluster(select 'no' for
standalone)? (yes/no) [n]: yes

  Enter the switch fabric (A/B) []: A

  Enter the system name: <<var_ucs_clustername>>

  Physical Switch Mgmt0 IP address : <<var_ucsa_mgmt_ip>>

  Physical Switch Mgmt0 IPv4 netmask : <<var_ucsa_mgmt_mask>>

  IPv4 address of the default gateway : <<var_ucsa_mgmt_gateway>>

  Cluster IPv4 address : <<var_ucs_cluster_ip>>

  Configure the DNS Server IP address? (yes/no) [n]: y

       DNS IP address : <<var_nameserver_ip>>

  Configure the default domain name? (yes/no) [n]: y
Default domain name: <<var_domain_name>>

  Join centralized management environment (UCS Central)? (yes/no) [n]:
no

 NOTE: Cluster IP will be configured only after both Fabric
Interconnects are initialized. UCSM will be functional only after peer
FI is configured in clustering mode.

  Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. 콘솔에 표시된 설정을 검토합니다. 맞으면 yes로 답하여 설정을 적용하고 저장합니다.
3. 로그인 프롬프트가 구성을 저장했는지 확인할 때까지 기다립니다.

다음 표에는 Fabric Interconnect B에서 Cisco UCS 초기 구성을 완료하는 데 필요한 정보가 나와 있습니다

세부 정보	상세/값
시스템 이름	<<var_UCS_clustername>>
관리자 암호	<<var_password>> 를 참조하십시오
관리 IP 주소 - FI B	<<var_ucsb_mgmt_ip>> 를 입력합니다
관리 넷마스크 - FI B	<<var_ucsb_mgmt_mask>>
기본 게이트웨이 - FI B	<<var_ucsb_mgmt_gateway>>
클러스터 IP 주소입니다	<<var_UCS_cluster_ip>> 를 참조하십시오
DNS 서버 IP 주소입니다	<<var_nameserver_ip>> 를 참조하십시오
도메인 이름	<<var_domain_name>>

1. 두 번째 Cisco UCS 6324 Fabric Interconnect B의 콘솔 포트에 연결합니다

```
 Enter the configuration method. (console/gui) ? console

  Installer has detected the presence of a peer Fabric interconnect.
This Fabric interconnect will be added to the cluster. Continue (y/n) ?
y

  Enter the admin password of the peer Fabric
interconnect:<<var_password>>
    Connecting to peer Fabric interconnect... done
    Retrieving config from peer Fabric interconnect... done
    Peer Fabric interconnect Mgmt0 IPv4 Address: <<var_ucsb_mgmt_ip>>
    Peer Fabric interconnect Mgmt0 IPv4 Netmask: <<var_ucsb_mgmt_mask>>
    Cluster IPv4 address: <<var_ucs_cluster_address>>

    Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric
Interconnect Mgmt0 IPv4 Address

  Physical Switch Mgmt0 IP address : <<var_ucsb_mgmt_ip>>


  Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. 로그인 프롬프트가 구성을 저장했는지 확인할 때까지 기다립니다.

Cisco UCS Manager에 로그인합니다

Cisco UCS(Unified Computing System) 환경에 로그인하려면 다음 단계를 수행하십시오.

1. 웹 브라우저를 열고 Cisco UCS Fabric Interconnect 클러스터 주소로 이동합니다.

   Cisco UCS Manager가 나타날 수 있도록 두 번째 패브릭 인터커넥트를 구성한 후 5분 이상 기다려야 할 수 있습니다.

2. Cisco UCS Manager 실행 링크를 클릭하여 Cisco UCS Manager를 시작합니다.
3. 필요한 보안 인증서를 수락합니다.
4. 메시지가 표시되면 사용자 이름으로 admin 을 입력하고 관리자 암호를 입력합니다.
5. Cisco UCS Manager에 로그인하려면 로그인을 클릭합니다.

Cisco UCS Manager 소프트웨어 버전 **4.0(1b)**

이 문서에서는 Cisco UCS Manager 소프트웨어 버전 4.0(1b)을 사용한다고 가정합니다. Cisco UCS Manager 소프트웨어 및 Cisco UCS 6324 Fabric Interconnect 소프트웨어를 업그레이드하려면 을 참조하십시오 "Cisco UCS Manager 설치 및 업그레이드 가이드:"

Cisco UCS Call Home을 구성합니다

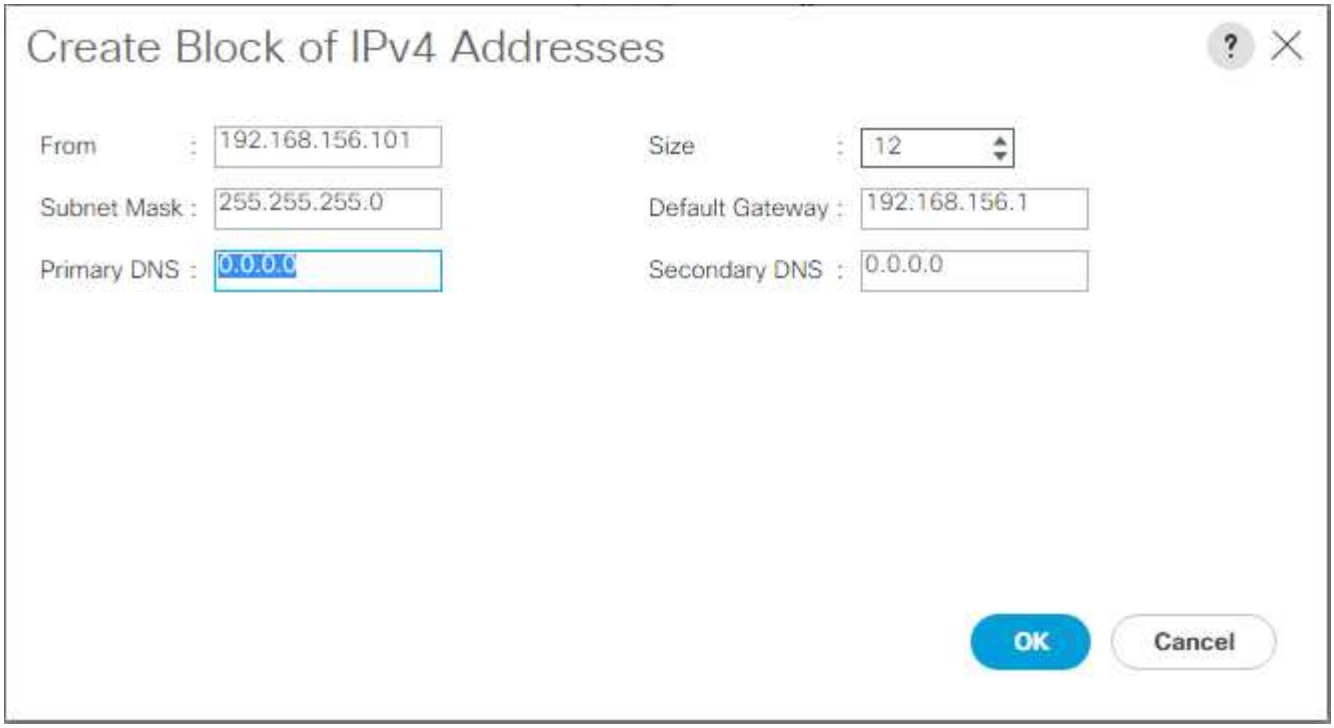
Cisco UCS Manager에서 Call Home을 구성하는 것이 좋습니다. Call Home을 구성하면 지원 케이스의 해결 속도가 빨라집니다. Call Home을 구성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에서 관리 를 클릭합니다.
2. 모두 > 통신 관리 > Call Home을 선택합니다.
3. 상태를 켜짐 으로 변경합니다.
4. Management(관리) 기본 설정에 따라 모든 필드를 입력하고 Save Changes(변경 사항 저장) 및 OK(확인) 를 클릭하여 Call Home 구성을 완료합니다.

키보드, 비디오, 마우스 액세스를 위한 **IP** 주소 블록을 추가합니다

Cisco UCS 환경에서 대역내 서버 키보드, 비디오, 마우스(KVM) 액세스를 위한 IP 주소 블록을 만들려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 LAN을 클릭합니다.
2. Pools > root > IP Pools 를 확장합니다.
3. IP Pool ext-mgmt 를 마우스 오른쪽 단추로 클릭하고 IPv4 주소 블록 만들기 를 선택합니다.
4. 블록의 시작 IP 주소, 필요한 IP 주소 수, 서브넷 마스크 및 게이트웨이 정보를 입력합니다.



5. 확인 을 클릭하여 블럭을 작성합니다.
6. 확인 메시지에서 확인 을 클릭합니다.

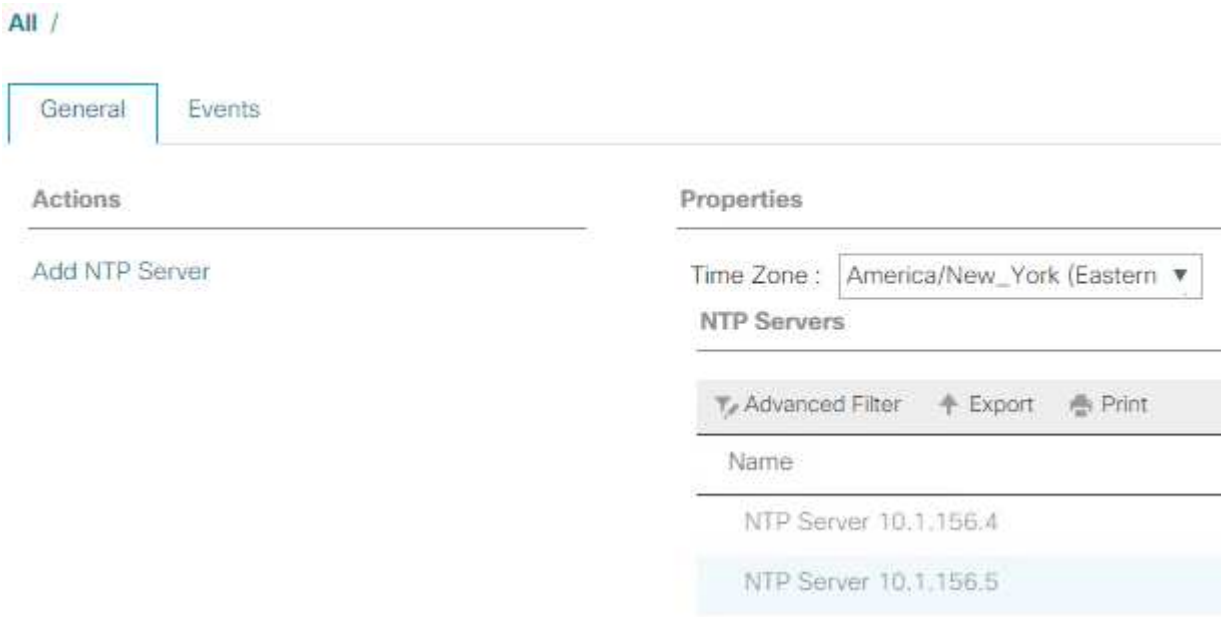
Cisco UCS를 NTP에 동기화합니다

Cisco UCS 환경을 Nexus 스위치의 NTP 서버와 동기화하려면 다음 단계를 완료하십시오.

1. Cisco UCS Manager의 경우 왼쪽에서 관리 를 클릭합니다.
2. 모두 > 시간대 관리 를 확장합니다.
3. 시간대 를 선택합니다.
4. 속성 창의 표준 시간대 메뉴에서 적절한 시간대를 선택합니다.
5. 변경 내용 저장 을 클릭하고 확인 을 클릭합니다.
6. NTP 서버 추가를 클릭합니다.
7. '<switch-a-ntp-ip> 또는 <Nexus-a-mgmt-ip>'를 입력하고 확인을 클릭합니다. 확인 을 클릭합니다.



8. NTP 서버 추가를 클릭합니다.
9. '<switch-b-ntp-ip>' 또는 <Nexus-B-mgmt-ip>'를 입력하고 확인을 클릭합니다. 확인 창에서 확인 을 클릭합니다.



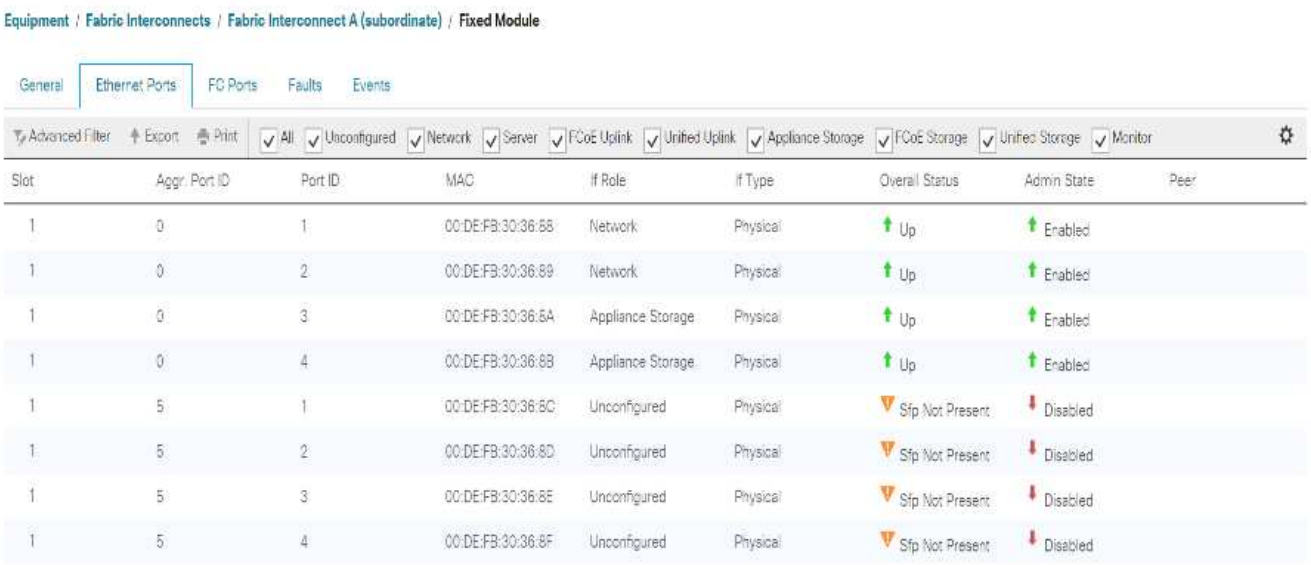
섀시 검색 정책을 편집합니다

검색 정책을 설정하면 Cisco UCS B-Series 섀시와 추가 패브릭 익스텐더를 간편하게 추가하여 Cisco UCS C-Series에 연결할 수 있습니다. 섀시 검색 정책을 수정하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 왼쪽에서 장비 를 클릭하고 두 번째 목록에서 장비 를 선택합니다.
2. 오른쪽 창에서 Policies 탭을 선택합니다.
3. 글로벌 정책에서 섀시/FEX 검색 정책을 섀시 또는 패브릭 익스텐더(FEX)와 패브릭 인터커넥트 간에 케이블로 연결된 최소 업링크 포트 수와 일치하도록 설정합니다.
4. 링크 그룹화 기본 설정을 포트 채널로 설정합니다. 설정 중인 환경에 많은 양의 멀티캐스트 트래픽이 포함된 경우 멀티캐스트 하드웨어 해시 설정을 사용으로 설정합니다.
5. 변경 내용 저장 을 클릭합니다.
6. 확인 을 클릭합니다.

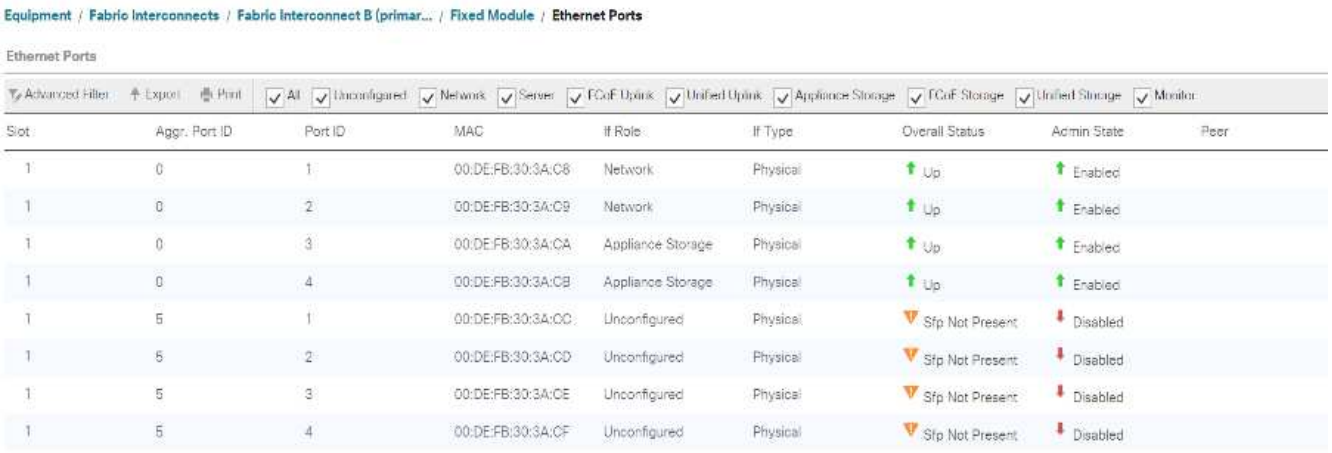
서버 및 업링크 포트를 활성화하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 탐색 창에서 장비 탭을 선택합니다.
2. 장비 > 패브릭 인터커넥트 > 패브릭 인터커넥트 A > 고정 모듈 을 확장합니다.
3. 이더넷 포트 를 확장합니다.
4. Cisco Nexus 31108 스위치에 연결된 포트 1과 2를 선택하고 마우스 오른쪽 단추를 클릭한 다음 업링크 포트로 구성 을 선택합니다.
5. 업링크 포트를 확인하려면 예를 클릭하고 확인을 클릭하십시오.
6. NetApp 스토리지 컨트롤러에 연결된 포트 3 및 4를 선택하고 마우스 오른쪽 버튼을 클릭한 다음 Configure as Appliance Port를 선택합니다.
7. 예 를 클릭하여 어플라이언스 포트를 확인합니다.
8. Configure as Appliance Port 창에서 OK를 클릭합니다.
9. 확인을 클릭하여 확인합니다.
10. 왼쪽 창에서 Fabric Interconnect A 아래에서 고정 모듈을 선택합니다
11. 이더넷 포트 탭의 IF 역할 열에서 포트가 올바르게 구성되었는지 확인합니다. 확장 포트에서 포트 C-Series 서버가 구성된 경우 해당 포트를 클릭하여 포트 연결을 확인합니다.



12. 장비 > 패브릭 인터커넥트 > 패브릭 인터커넥트 B > 고정 모듈 을 확장합니다.
13. 이더넷 포트 를 확장합니다.
14. Cisco Nexus 31108 스위치에 연결된 이더넷 포트 1과 2를 선택하고 마우스 오른쪽 버튼을 클릭한 다음 업링크 포트로 구성 을 선택합니다.
15. 업링크 포트를 확인하려면 예를 클릭하고 확인을 클릭하십시오.
16. NetApp 스토리지 컨트롤러에 연결된 포트 3 및 4를 선택하고 마우스 오른쪽 버튼을 클릭한 다음 Configure as Appliance Port를 선택합니다.
17. 예 를 클릭하여 어플라이언스 포트를 확인합니다.

18. Configure as Appliance Port 창에서 OK를 클릭합니다.
19. 확인을 클릭하여 확인합니다.
20. 왼쪽 창에서 Fabric Interconnect B 아래에서 고정 모듈을 선택합니다
21. 이더넷 포트 탭의 IF 역할 열에서 포트가 올바르게 구성되었는지 확인합니다. 확장 포트에서 포트 C-Series 서버가 구성된 경우 이를 클릭하여 포트 연결을 확인합니다.



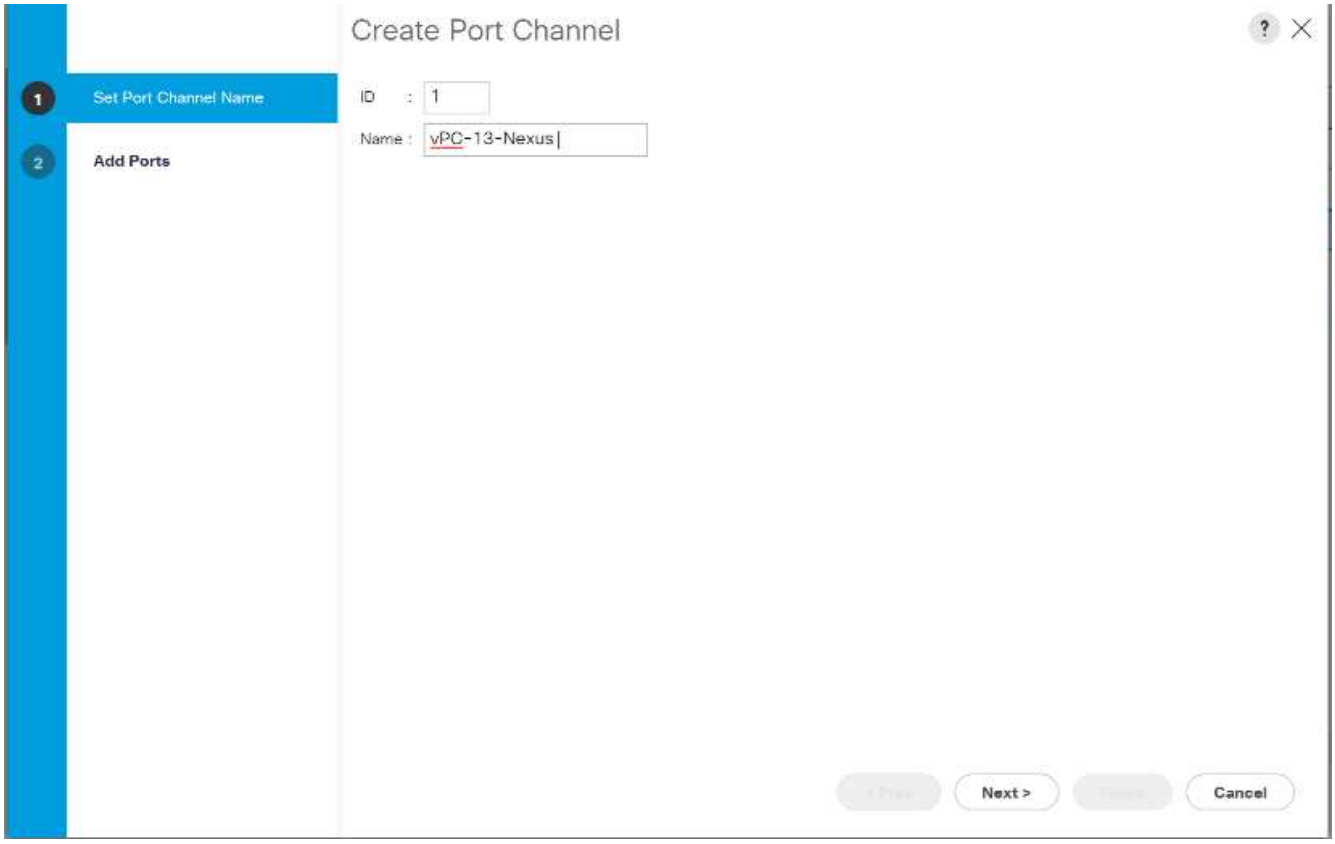
Cisco Nexus 31108 스위치에 업링크 포트 채널을 생성합니다

Cisco UCS 환경에서 필요한 포트 채널을 구성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 탐색 창에서 LAN 탭을 선택합니다.

> 이 절차에서는 패브릭 A에서 Cisco Nexus 31108 스위치 두 개, 그리고 패브릭 B에서 Cisco Nexus 31108 스위치 두 개로 포트 채널 두 개가 생성됩니다. 표준 스위치를 사용하는 경우 이 절차를 적절히 수정합니다. 패브릭 인터커넥트에 1기가비트 이더넷(1GbE) 스위치 및 GLC-T SFP를 사용하는 경우 패브릭 상호 연결의 이더넷 포트 1/1 및 1/2의 인터페이스 속도를 1Gbps로 설정해야 합니다.

2. LAN > LAN 클라우드 에서 패브릭 A 트리를 확장합니다.
3. 포트 채널 을 마우스 오른쪽 단추로 클릭합니다.
4. 포트 채널 생성 을 선택합니다.
5. 포트 채널의 고유 ID로 13을 입력합니다.
6. 포트 채널 이름으로 vPC-13-Nexus를 입력합니다.
7. 다음 을 클릭합니다.



8. 포트 채널에 추가할 다음 포트를 선택합니다.
   a. 슬롯 ID 1 및 포트 1
   b. 슬롯 ID 1 및 포트 2
9. 포트 채널에 포트를 추가하려면 >> 를 클릭합니다.
10. 마침 을 클릭하여 포트 채널을 생성합니다. 확인 을 클릭합니다.
11. 포트 채널 에서 새로 생성된 포트 채널을 선택합니다.

    포트 채널은 전체 상태가 UP 이어야 합니다.

12. 탐색 창의 LAN > LAN Cloud 아래에서 패브릭 B 트리를 확장합니다.
13. 포트 채널 을 마우스 오른쪽 단추로 클릭합니다.
14. 포트 채널 생성 을 선택합니다.
15. 포트 채널의 고유 ID로 14를 입력합니다.
16. 포트 채널 이름으로 vPC-14-Nexus를 입력합니다. 다음 을 클릭합니다.
17. 포트 채널에 추가할 다음 포트를 선택합니다.
   a. 슬롯 ID 1 및 포트 1
   b. 슬롯 ID 1 및 포트 2
18. 포트 채널에 포트를 추가하려면 >> 를 클릭합니다.
19. 마침 을 클릭하여 포트 채널을 생성합니다. 확인 을 클릭합니다.
20. 포트 채널 에서 새로 생성된 포트 채널을 선택합니다.

21. 포트 채널은 전체 상태가 UP 이어야 합니다.

조직 만들기(선택 사항)

조직은 리소스를 구성하고 IT 조직 내의 다양한 그룹에 대한 액세스를 제한하여 컴퓨팅 리소스에 대한 멀티 테넌시를 활성화하는 데 사용됩니다.

> 이 문서에서는 조직의 사용을 전제로 하지 않지만 이 절차에서는 조직을 만드는 방법에 대한 지침을 제공합니다.

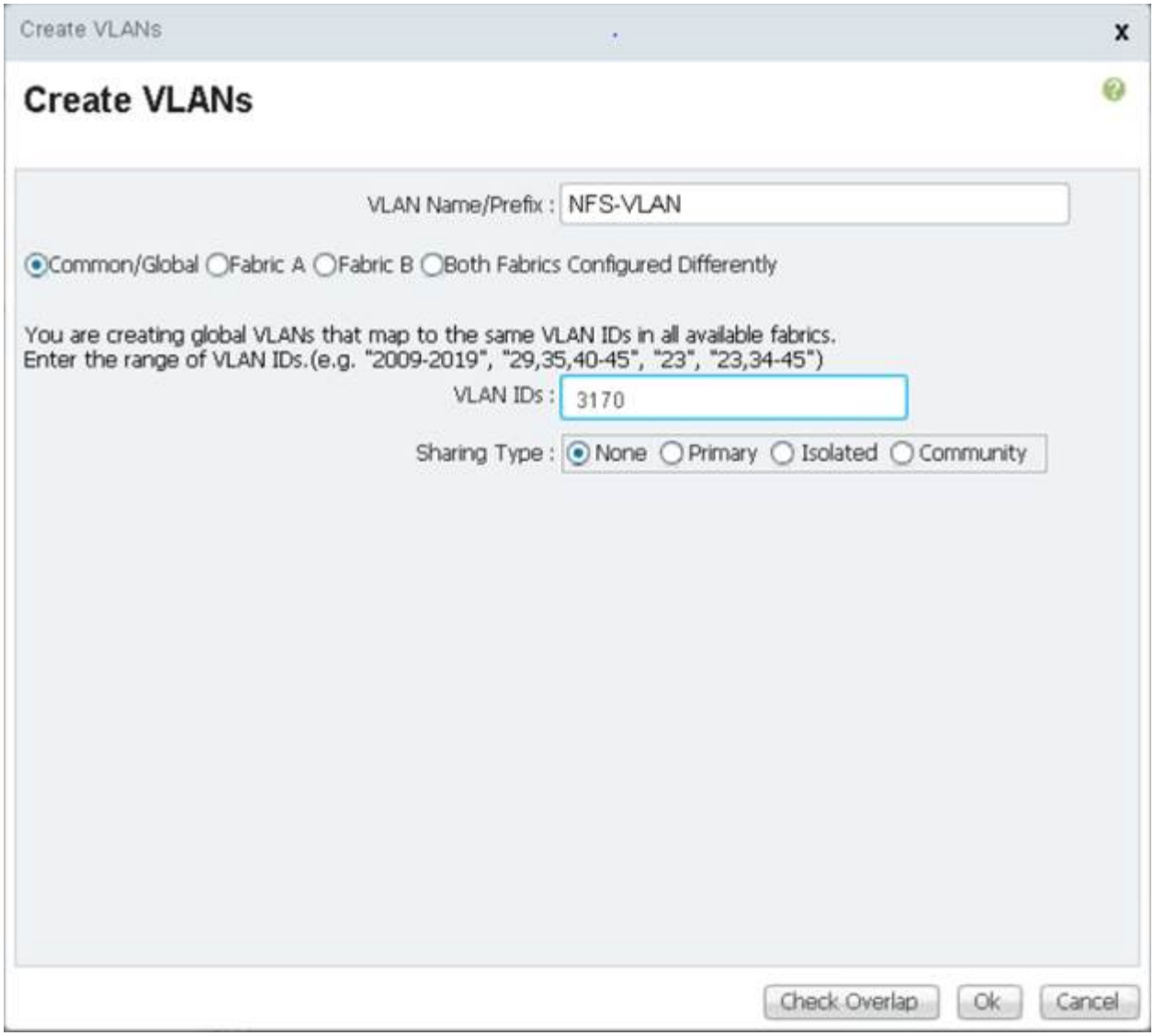
Cisco UCS 환경에서 조직을 구성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 창 맨 위에 있는 도구 모음의 새로 만들기 메뉴에서 조직 만들기 를 선택합니다.
2. 조직의 이름을 입력합니다.
3. 선택 사항: 조직에 대한 설명을 입력합니다. 확인 을 클릭합니다.
4. 확인 메시지에서 확인 을 클릭합니다.

스토리지 어플라이언스 포트 및 스토리지 **VLAN**을 구성합니다

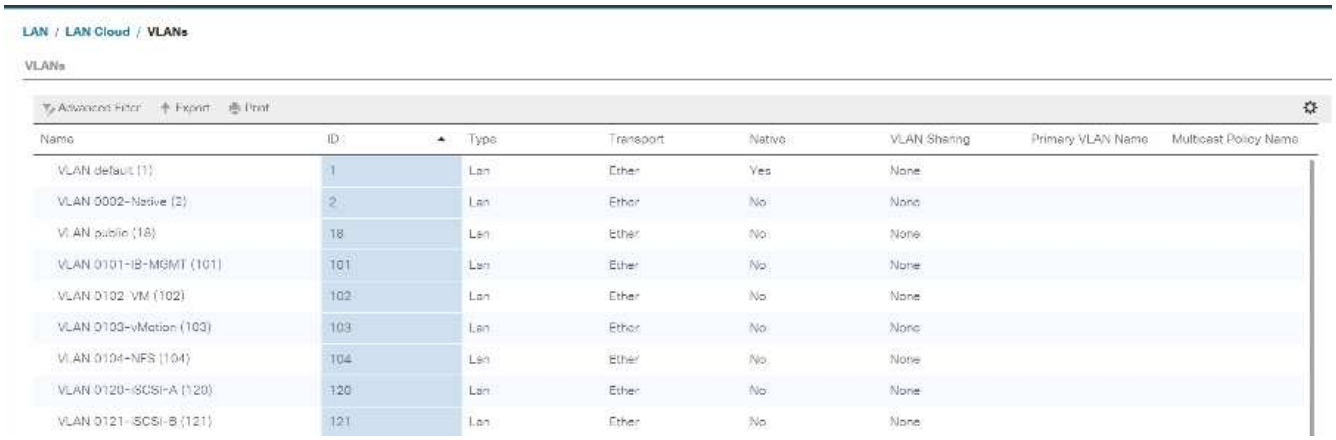
스토리지 어플라이언스 포트 및 스토리지 VLAN을 구성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager에서 LAN 탭을 선택합니다.
2. 어플라이언스 클라우드 확장
3. Appliances Cloud 아래에서 VLAN을 마우스 오른쪽 버튼으로 클릭합니다.
4. VLAN 생성을 선택합니다.
5. 인프라스트럭처 NFS VLAN의 이름으로 NFS-VLAN을 입력합니다.
6. 공통/전체 를 선택한 상태로 둡니다.
7. VLAN ID에 '<<var_nfs_vlan_id>>'를 입력합니다.
8. 공유 유형을 없음으로 둡니다.

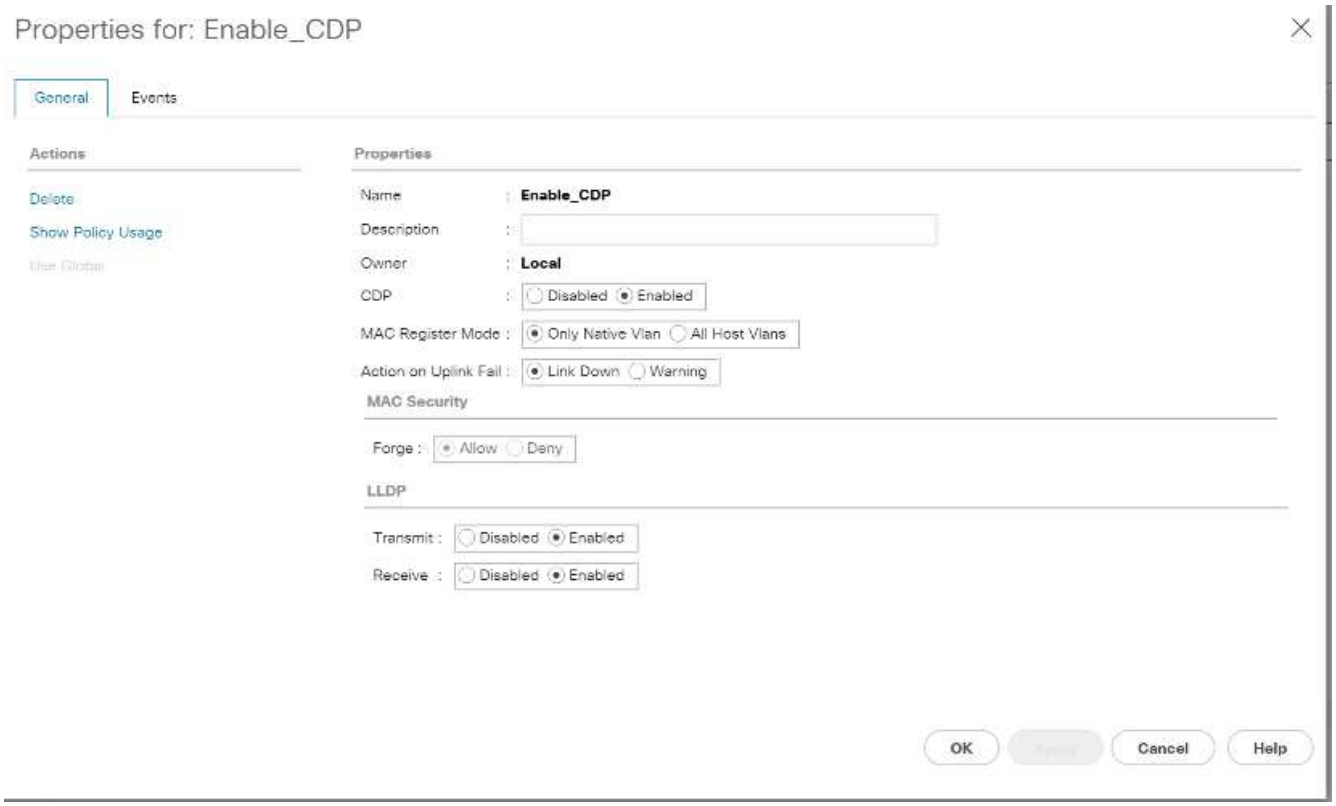


9. 확인을 클릭한 다음 확인을 다시 클릭하여 VLAN을 만듭니다.
10. Appliances Cloud 아래에서 VLAN을 마우스 오른쪽 버튼으로 클릭합니다.
11. VLAN 생성을 선택합니다.
12. 인프라 iSCSI 패브릭 A VLAN의 이름으로 iSCSI-A-VLAN을 입력합니다.
13. 공통/전체 를 선택한 상태로 둡니다.
14. VLAN ID에 '<<var_iscsi-a_vlan_id>>'를 입력합니다.
15. 확인을 클릭한 다음 확인을 다시 클릭하여 VLAN을 만듭니다.
16. Appliances Cloud 아래에서 VLAN을 마우스 오른쪽 버튼으로 클릭합니다.
17. VLAN 생성을 선택합니다.
18. 인프라 iSCSI 패브릭 B VLAN의 이름으로 iSCSI-B-VLAN을 입력합니다.
19. 공통/전체 를 선택한 상태로 둡니다.
20. VLAN ID에 '<<var_iscsi-b_vlan_id>>'를 입력합니다.
21. 확인을 클릭한 다음 확인을 다시 클릭하여 VLAN을 만듭니다.

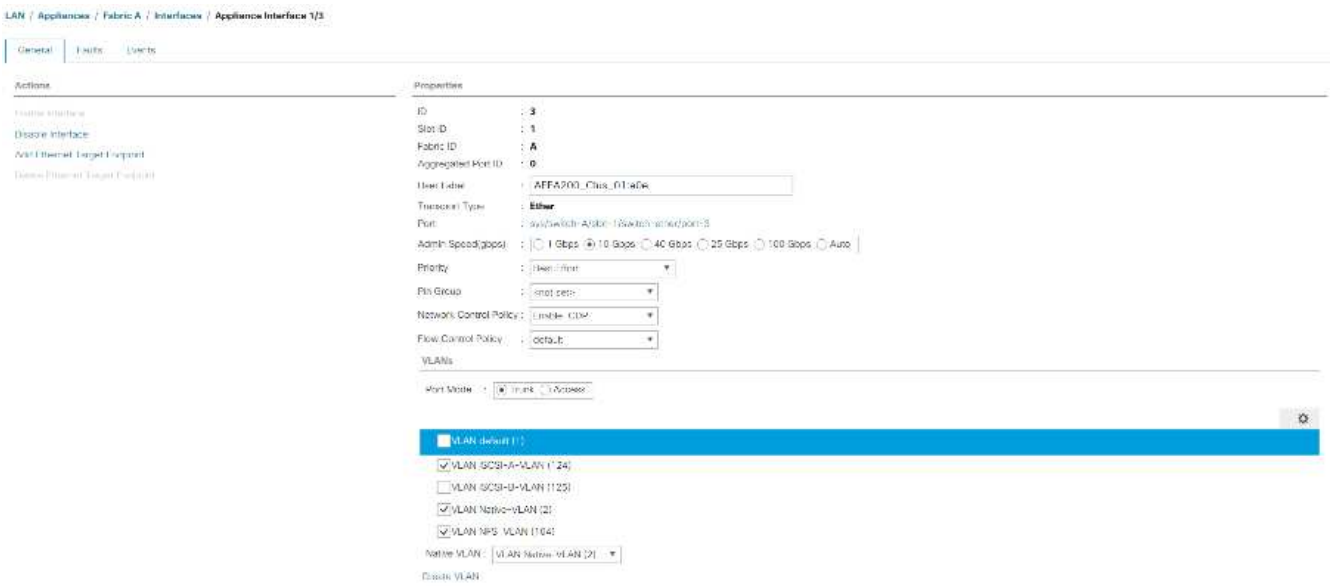
22. Appliances Cloud 아래에서 VLAN을 마우스 오른쪽 버튼으로 클릭합니다.
23. VLAN 생성을 선택합니다.
24. Native VLAN의 이름으로 Native-VLAN을 입력한다.
25. 공통/전체 를 선택한 상태로 둡니다.
26. VLAN ID에 '<<var_native_vlan_id>>'를 입력합니다.
27. 확인을 클릭한 다음 확인을 다시 클릭하여 VLAN을 만듭니다.



28. 탐색 창의 LAN > 정책 에서 어플라이언스 를 확장하고 네트워크 제어 정책 을 마우스 오른쪽 단추로 클릭합니다.
29. 네트워크 제어 정책 생성 을 선택합니다.
30. 정책 이름을 "Enable_CDP_LLPD"로 지정하고 CDP 옆에 있는 Enabled를 선택합니다.
31. LLDP의 전송 및 수신 기능을 활성화합니다.

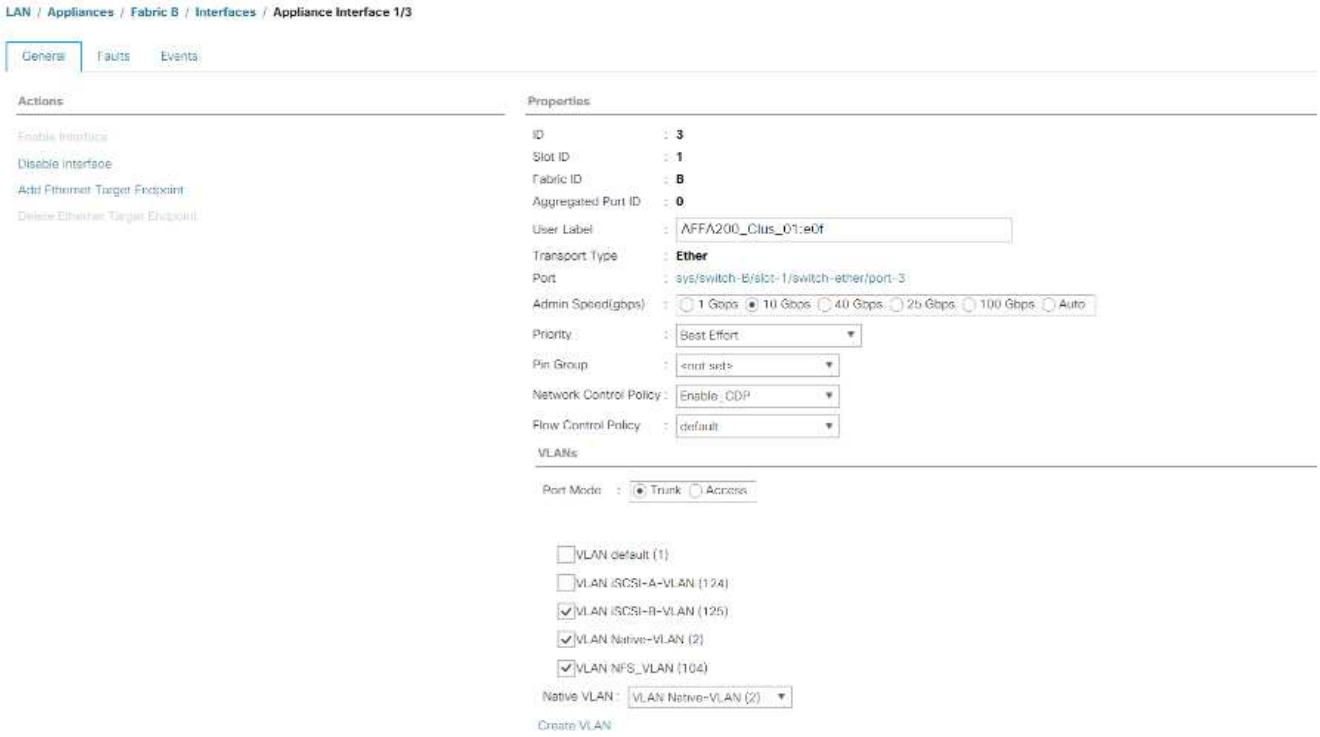


32. 확인 을 클릭한 다음 확인 을 다시 클릭하여 정책을 만듭니다.
33. 탐색 창의 LAN > 어플라이언스 클라우드 에서 Fabric A 트리를 확장합니다.
34. Interfaces를 확장합니다.
35. 어플라이언스 인터페이스 1/3을 선택합니다.
36. User Label 필드에 '<storage_controller_01_name>:e0e'와 같은 스토리지 컨트롤러 포트를 나타내는 정보를 입력합니다. 변경 내용 저장 및 확인 을 클릭합니다.
37. Enable_CDP Network Control Policy를 선택하고 Save Changes and OK를 선택합니다.
38. VLAN에서 iSCSI-A-VLAN, NFS VLAN 및 기본 VLAN을 선택합니다. Native-VLAN을 Native VLAN으로 설정한다. 기본 VLAN 선택을 취소합니다.
39. 변경 내용 저장 및 확인 을 클릭합니다.



40. Fabric A 아래에서 Appliance Interface 1/4를 선택합니다
41. User Label 필드에 '<storage_controller_02_name>:e0e'와 같은 스토리지 컨트롤러 포트를 나타내는 정보를 입력합니다. 변경 내용 저장 및 확인 을 클릭합니다.
42. Enable_CDP Network Control Policy를 선택하고 Save Changes and OK를 선택합니다.
43. VLAN에서 iSCSI-A-VLAN, NFS VLAN 및 기본 VLAN을 선택합니다.
44. Native-VLAN을 Native VLAN으로 설정한다.
45. 기본 VLAN 선택을 취소합니다.
46. 변경 내용 저장 및 확인 을 클릭합니다.
47. 탐색 창의 LAN > 어플라이언스 클라우드 에서 Fabric B 트리를 확장합니다.
48. Interfaces를 확장합니다.
49. 어플라이언스 인터페이스 1/3을 선택합니다.
50. User Label 필드에 '<storage_controller_01_name>:e0f'와 같은 스토리지 컨트롤러 포트를 나타내는 정보를 입력합니다. 변경 내용 저장 및 확인 을 클릭합니다.

51. Enable_CDP Network Control Policy를 선택하고 Save Changes and OK를 선택합니다.
52. VLAN에서 iSCSI-B-VLAN, NFS VLAN 및 기본 VLAN을 선택합니다. Native-VLAN을 Native VLAN으로 설정한다. 기본 VLAN을 선택 취소합니다.

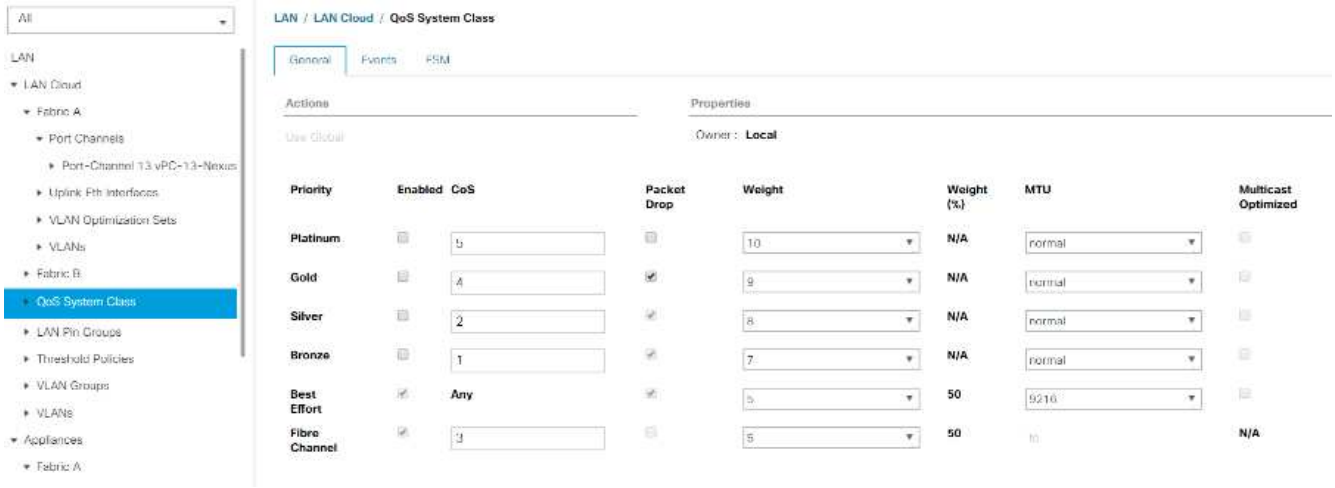


53. 변경 내용 저장 및 확인 을 클릭합니다.
54. Fabric B 아래에서 Appliance Interface 1/4를 선택합니다
55. User Label 필드에 '<storage_controller_02_name>:e0f'와 같은 스토리지 컨트롤러 포트를 나타내는 정보를 입력합니다. 변경 내용 저장 및 확인 을 클릭합니다.
56. Enable_CDP Network Control Policy를 선택하고 Save Changes and OK를 선택합니다.
57. VLAN에서 iSCSI-B-VLAN, NFS VLAN 및 기본 VLAN을 선택합니다. Native-VLAN을 Native VLAN으로 설정한다. 기본 VLAN을 선택 취소합니다.
58. 변경 내용 저장 및 확인 을 클릭합니다.

Cisco UCS 패브릭에서 점보 프레임을 설정합니다

Cisco UCS 패브릭에서 점보 프레임을 구성하고 서비스 품질을 설정하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 탐색 창에서 LAN 탭을 클릭합니다.
2. LAN > LAN Cloud > QoS System Class 를 선택합니다.
3. 오른쪽 창에서 일반 탭을 클릭합니다.
4. Best Effort 행의 MTU 열 아래에 있는 상자에 9216을 입력합니다.



5. 변경 내용 저장 을 클릭합니다.
6. 확인 을 클릭합니다.

Cisco UCS 섀시를 확인합니다

모든 Cisco UCS 섀시를 확인하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager에서 장비 탭을 선택한 다음 오른쪽의 장비 탭을 확장합니다.
2. 장비 > 섀시를 확장합니다.
3. 섀시 1에 대한 작업에서 섀시 승인 을 선택합니다.
4. 확인을 클릭한 다음 확인을 클릭하여 섀시 확인을 완료합니다.
5. 닫기 를 클릭하여 속성 창을 닫습니다.

Cisco UCS 4.0(1b) 펌웨어 이미지를 로드합니다

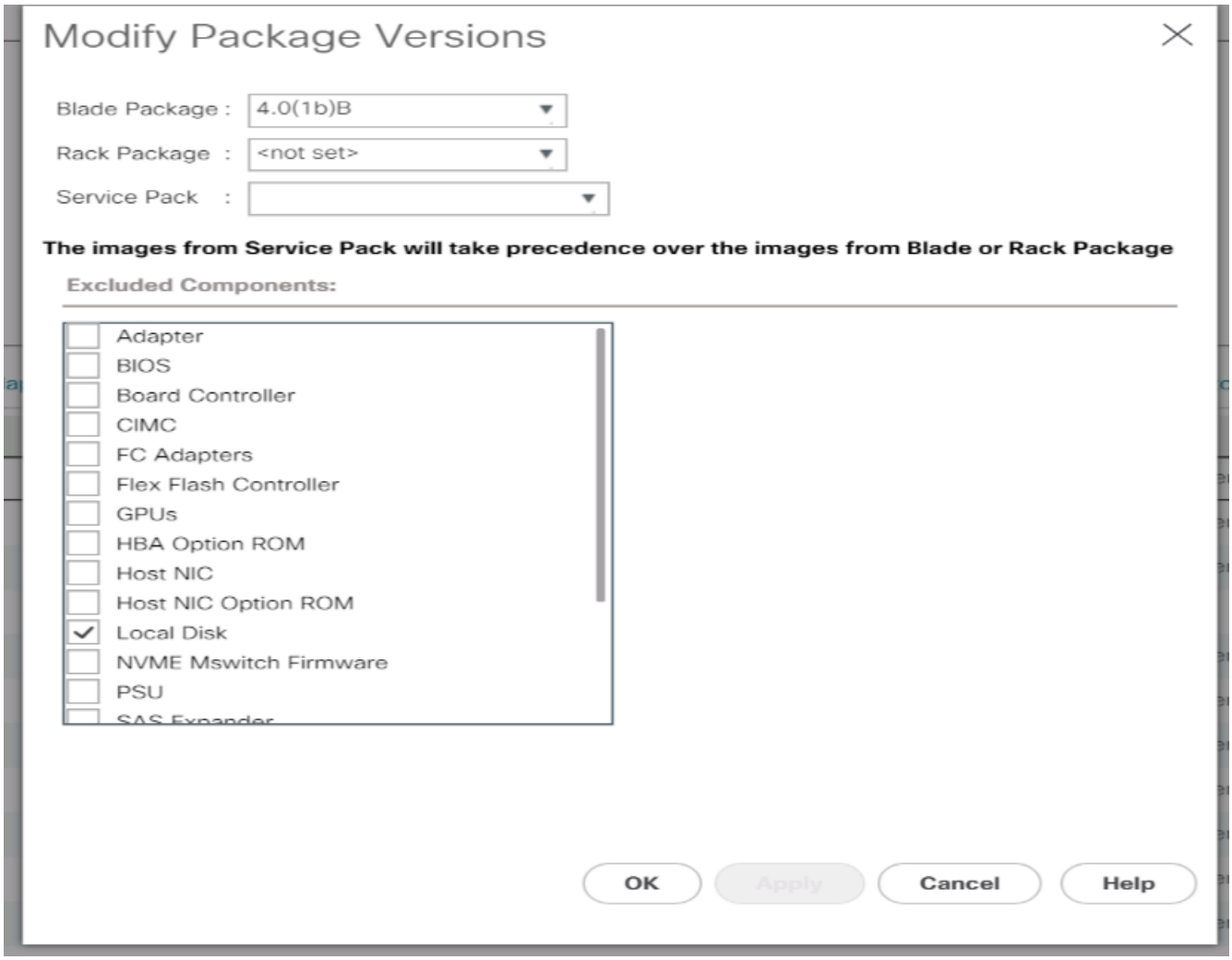
Cisco UCS Manager 소프트웨어 및 Cisco UCS Fabric Interconnect 소프트웨어를 버전 4.0(1b)으로 업그레이드하려면 을 참조하십시오 "Cisco UCS Manager 설치 및 업그레이드 가이드".

호스트 펌웨어 패키지를 생성합니다

관리자는 펌웨어 관리 정책을 사용하여 지정된 서버 구성에 해당하는 패키지를 선택할 수 있습니다. 이러한 정책에는 종종 어댑터, BIOS, 보드 컨트롤러, FC 어댑터, HBA(호스트 버스 어댑터) 옵션 ROM 및 스토리지 컨트롤러 속성에 대한 패키지가 포함됩니다.

Cisco UCS 환경에서 지정된 서버 구성에 대한 펌웨어 관리 정책을 생성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 서버 를 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. 호스트 펌웨어 패키지를 확장합니다.
4. 기본값을 선택합니다.
5. 작업 창에서 패키지 버전 수정을 선택합니다.
6. 두 블레이드 패키지 모두에 대해 버전 4.0(1b)을 선택합니다.



7. OK(확인) 를 클릭한 다음 OK(확인) 를 다시 클릭하여 호스트 펌웨어 패키지를 수정합니다.

MAC 주소 풀을 생성합니다

Cisco UCS 환경에 필요한 MAC 주소 풀을 구성하려면 다음 단계를 수행하십시오.

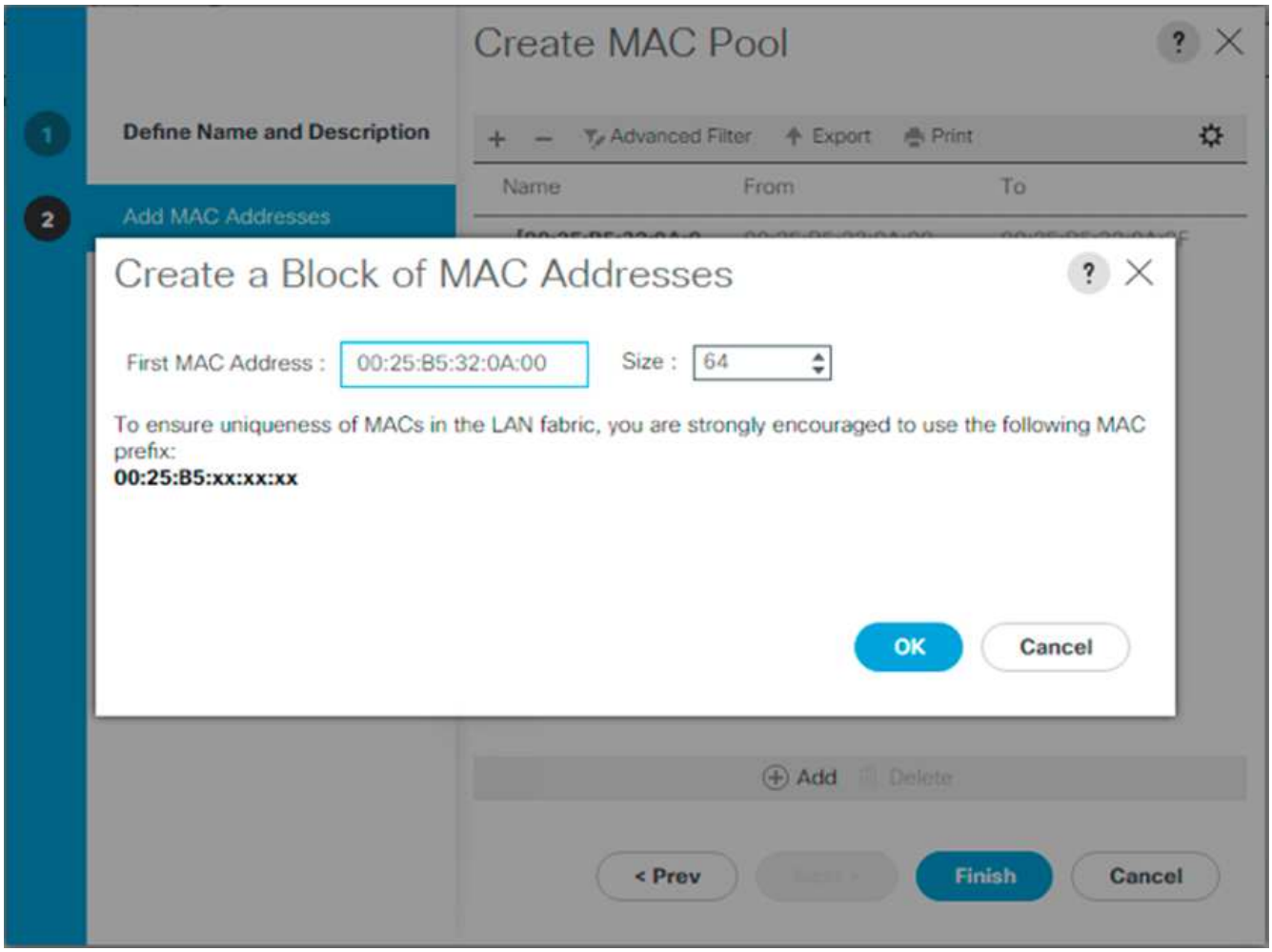
1. Cisco UCS Manager의 경우 왼쪽에 있는 LAN을 클릭합니다.
2. Pools > root 를 선택합니다.

   이 절차에서는 각 스위칭 패브릭에 대해 하나씩 두 개의 MAC 주소 풀이 생성됩니다.

3. 루트 조직 아래에서 MAC Pools 를 마우스 오른쪽 단추로 클릭합니다.
4. MAC 주소 풀을 생성하려면 MAC 풀 생성 을 선택합니다.
5. MAC-Pool-A를 MAC 풀의 이름으로 입력합니다.
6. 선택 사항: MAC 풀에 대한 설명을 입력합니다.
7. 할당 순서 옵션으로 Sequential(순차)을 선택합니다. 다음 을 클릭합니다.
8. 추가 를 클릭합니다.
9. 시작 MAC 주소를 지정합니다.

FlexPod 솔루션의 경우 모든 MAC 주소를 패브릭 A 주소로 식별하기 위해 시작 MAC 주소의 마지막 옥텟에 0A를 배치하는 것이 좋습니다. 이 예에서는 첫 번째 MAC 주소로 00:25:B5:32:0A:00을 제공하는 Cisco UCS 도메인 번호 정보도 포함하는 예를 전달했습니다.

10. 사용 가능한 블레이드 또는 서버 리소스를 지원하기에 충분한 MAC 주소 풀의 크기를 지정합니다. 확인 을 클릭합니다.



11. 마침 을 클릭합니다.
12. 확인 메시지에서 확인 을 클릭합니다.
13. 루트 조직 아래에서 MAC Pools 를 마우스 오른쪽 단추로 클릭합니다.
14. MAC 주소 풀을 생성하려면 MAC 풀 생성 을 선택합니다.
15. MAC-Pool-B를 MAC 풀의 이름으로 입력합니다.
16. 선택 사항: MAC 풀에 대한 설명을 입력합니다.
17. 할당 순서 옵션으로 Sequential(순차)을 선택합니다. 다음 을 클릭합니다.
18. 추가 를 클릭합니다.
19. 시작 MAC 주소를 지정합니다.

FlexPod 솔루션의 경우, 이 풀의 모든 MAC 주소를 패브릭 B 주소로 식별하기 위해 시작 MAC 주소의 마지막 옥텟에 0B를 배치하는 것이 좋습니다. 다시 한 번, 첫 번째 MAC 주소로 00:25:B5:32:0B:00을 제공하는 Cisco UCS 도메인 번호 정보를 포함하는 예를 들어보겠습니다.

20. 사용 가능한 블레이드 또는 서버 리소스를 지원하기에 충분한 MAC 주소 풀의 크기를 지정합니다. 확인 을 클릭합니다.
21. 마침 을 클릭합니다.
22. 확인 메시지에서 확인 을 클릭합니다.

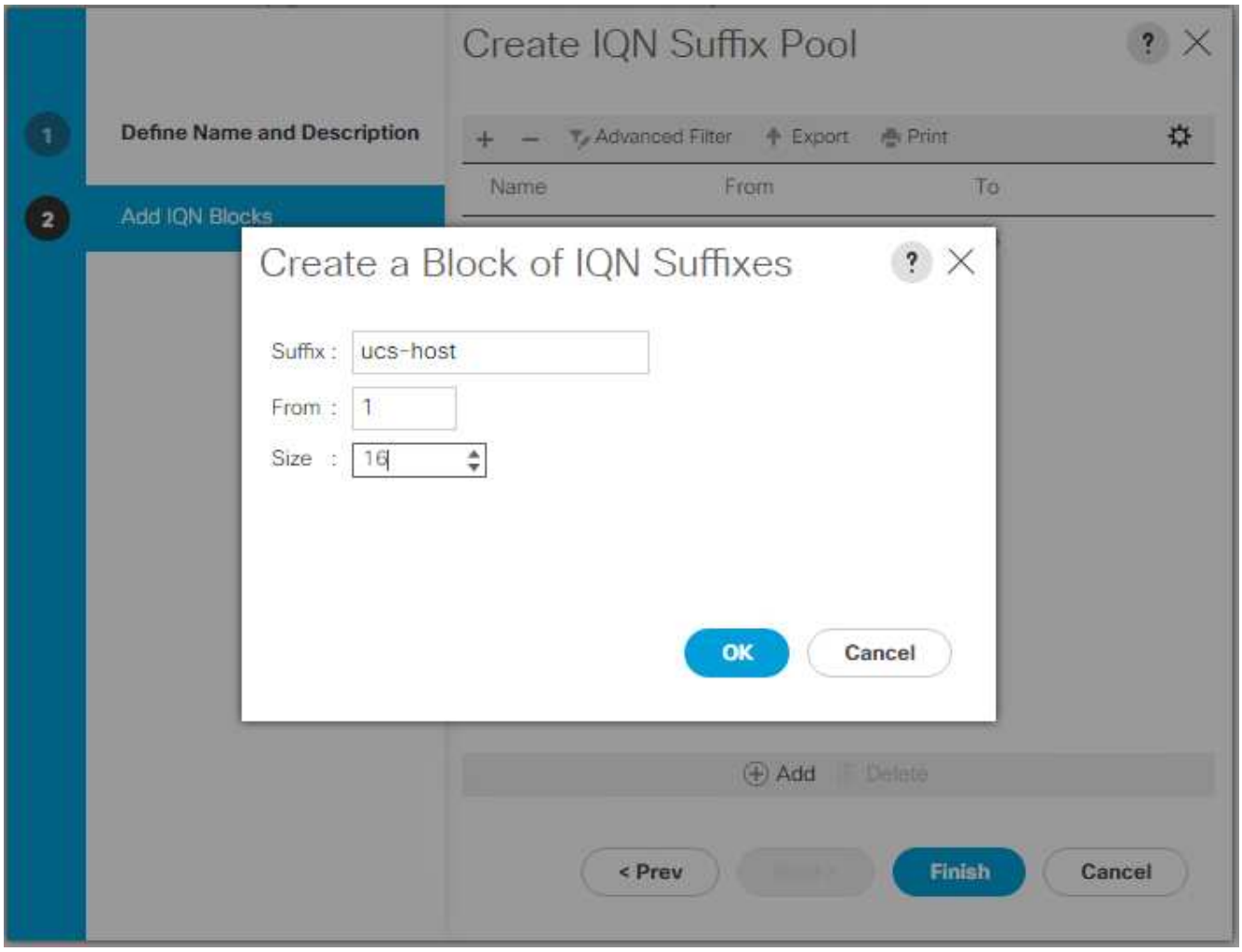
iSCSI IQN 풀을 생성합니다

Cisco UCS 환경에 필요한 IQN 풀을 구성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에서 SAN을 클릭합니다.
2. Pools > root 를 선택합니다.
3. IQN Pools 를 마우스 오른쪽 버튼으로 클릭합니다.
4. IQN 접미사 풀 생성 을 선택하여 IQN 풀을 생성합니다.
5. IQN 풀의 이름에 IQN-Pool을 입력합니다.
6. 선택 사항: IQN 풀에 대한 설명을 입력합니다.
7. 접두사로 iqn.1992-08.com.cisco` 를 입력합니다.
8. 할당 순서에서 순차적 을 선택합니다. 다음 을 클릭합니다.
9. 추가 를 클릭합니다.
10. 접미사로 UCS-host를 입력합니다.

여러 Cisco UCS 도메인을 사용 중인 경우 보다 구체적인 IQN 접미사를 사용해야 할 수 있습니다.

11. 보낸 사람 필드에 1을 입력합니다.
12. 사용 가능한 서버 리소스를 지원하기에 충분한 IQN 블록 크기를 지정합니다. 확인 을 클릭합니다.



13. 마침 을 클릭합니다.

iSCSI 이니시에이터 **IP** 주소 풀을 생성합니다

Cisco UCS 환경에 필요한 IP 풀 iSCSI 부트를 구성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 LAN을 클릭합니다.
2. Pools > root 를 선택합니다.
3. IP Pools 를 마우스 오른쪽 버튼으로 클릭합니다.
4. Create IP Pool 을 선택합니다.
5. IP 풀 이름으로 iSCSI-IP-Pool-A를 입력합니다.
6. 선택 사항: IP 풀에 대한 설명을 입력합니다.
7. 할당 순서에 대해 Sequential(순차) 을 선택합니다. 다음 을 클릭합니다.
8. 추가 를 클릭하여 IP 주소 블록을 추가합니다.
9. From(보낸 사람) 필드에 iSCSI IP 주소로 할당할 범위의 시작 부분을 입력합니다.
10. 서버 수용 가능한 주소 크기로 설정합니다. 확인 을 클릭합니다.
11. 다음 을 클릭합니다.

12. 마침 을 클릭합니다.
13. IP Pools 를 마우스 오른쪽 버튼으로 클릭합니다.
14. Create IP Pool 을 선택합니다.
15. IP 풀 이름으로 iSCSI-IP-Pool-B를 입력합니다.
16. 선택 사항: IP 풀에 대한 설명을 입력합니다.
17. 할당 순서에 대해 Sequential(순차) 을 선택합니다. 다음 을 클릭합니다.
18. 추가 를 클릭하여 IP 주소 블록을 추가합니다.
19. From(보낸 사람) 필드에 iSCSI IP 주소로 할당할 범위의 시작 부분을 입력합니다.
20. 서버 수용 가능한 주소 크기로 설정합니다. 확인 을 클릭합니다.
21. 다음 을 클릭합니다.
22. 마침 을 클릭합니다.

UUID 접미사 풀을 생성합니다

Cisco UCS 환경에 필요한 UUID(Universally Unique Identifier) 접미사 풀을 구성하려면 다음 단계를 완료하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 서버 를 클릭합니다.
2. Pools > root 를 선택합니다.
3. UUID 접미사 풀 을 마우스 오른쪽 버튼으로 클릭합니다.
4. UUID 접미사 풀 생성 을 선택합니다.
5. UUID 접미사 풀의 이름으로 UUID-Pool을 입력합니다.
6. 선택 사항: UUID 접미사 풀에 대한 설명을 입력합니다.
7. 원본에 구속되는 옵션에서 접두어를 유지합니다.
8. 할당 순서에 대해 Sequential(순차) 을 선택합니다.
9. 다음 을 클릭합니다.
10. 추가 를 클릭하여 UUID 블록을 추가합니다.
11. 보낸 사람 필드를 기본 설정으로 유지합니다.
12. 사용 가능한 블레이드 또는 서버 리소스를 지원하기에 충분한 UUID 블록의 크기를 지정합니다. 확인 을 클릭합니다.
13. 마침 을 클릭합니다.
14. 확인 을 클릭합니다.

서버 풀을 생성합니다

Cisco UCS 환경에 필요한 서버 풀을 구성하려면 다음 단계를 수행하십시오.



사용자 환경에 필요한 세분화 수준을 달성하려면 고유한 서버 풀을 생성하는 것이 좋습니다.

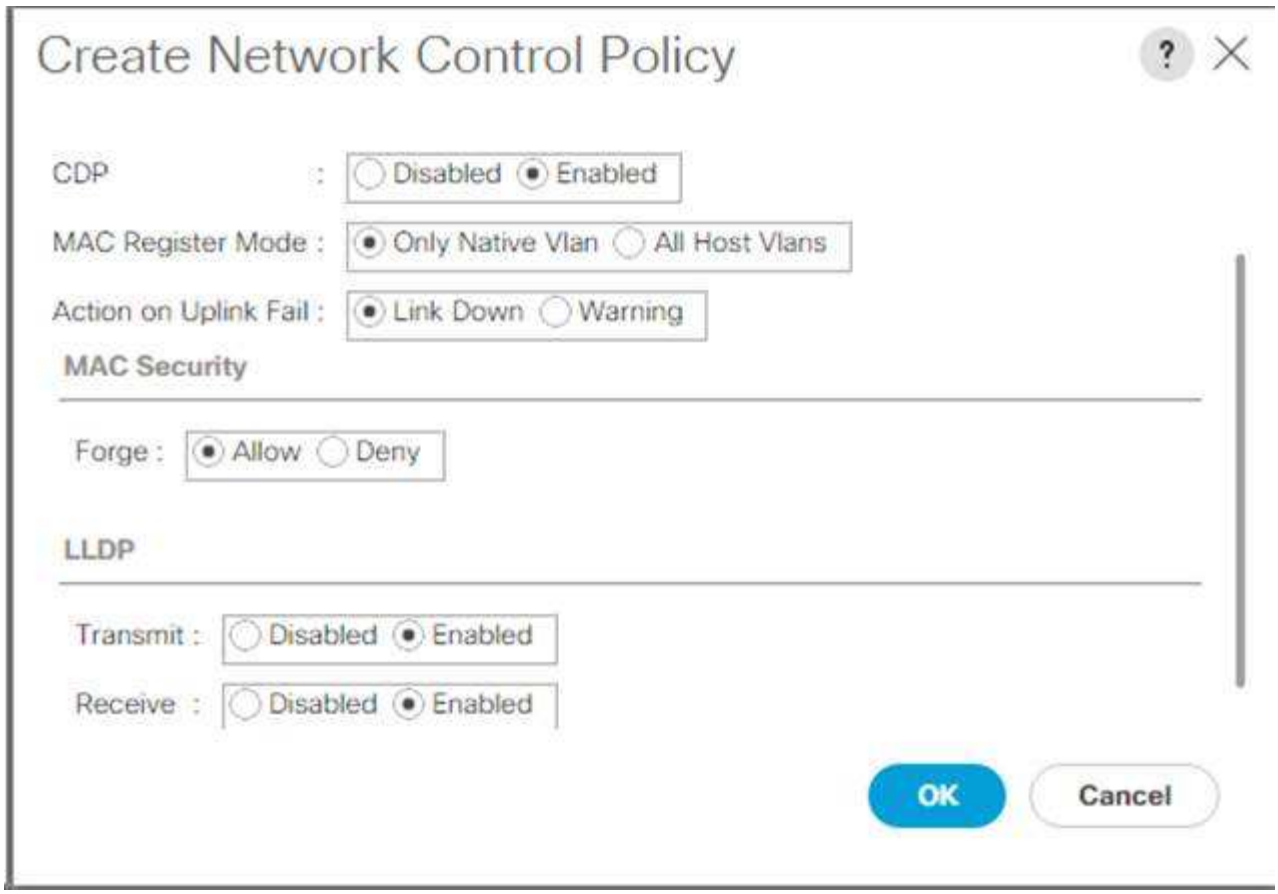
1. Cisco UCS Manager의 경우 왼쪽에 있는 서버 를 클릭합니다.
2. Pools > root 를 선택합니다.

3. 서버 풀 을 마우스 오른쪽 단추로 클릭합니다.
4. Create Server Pool 을 선택합니다.
5. 서버 풀의 이름으로 Infra-Pool을 입력합니다.
6. 선택 사항: 서버 풀에 대한 설명을 입력합니다. 다음 을 클릭합니다.
7. VMware 관리 클러스터에 사용할 서버를 두 개 이상 선택하고 >> 를 클릭하여 Infra-Pool의 서버 풀에 추가합니다.
8. 마침 을 클릭합니다.
9. 확인 을 클릭합니다.

Cisco Discovery Protocol 및 Link Layer Discovery Protocol에 대한 네트워크 제어 정책을 생성합니다

CDP(Cisco Discovery Protocol) 및 LLDP(Link Layer Discovery Protocol)에 대한 네트워크 제어 정책을 만들려면 다음 단계를 수행하십시오.

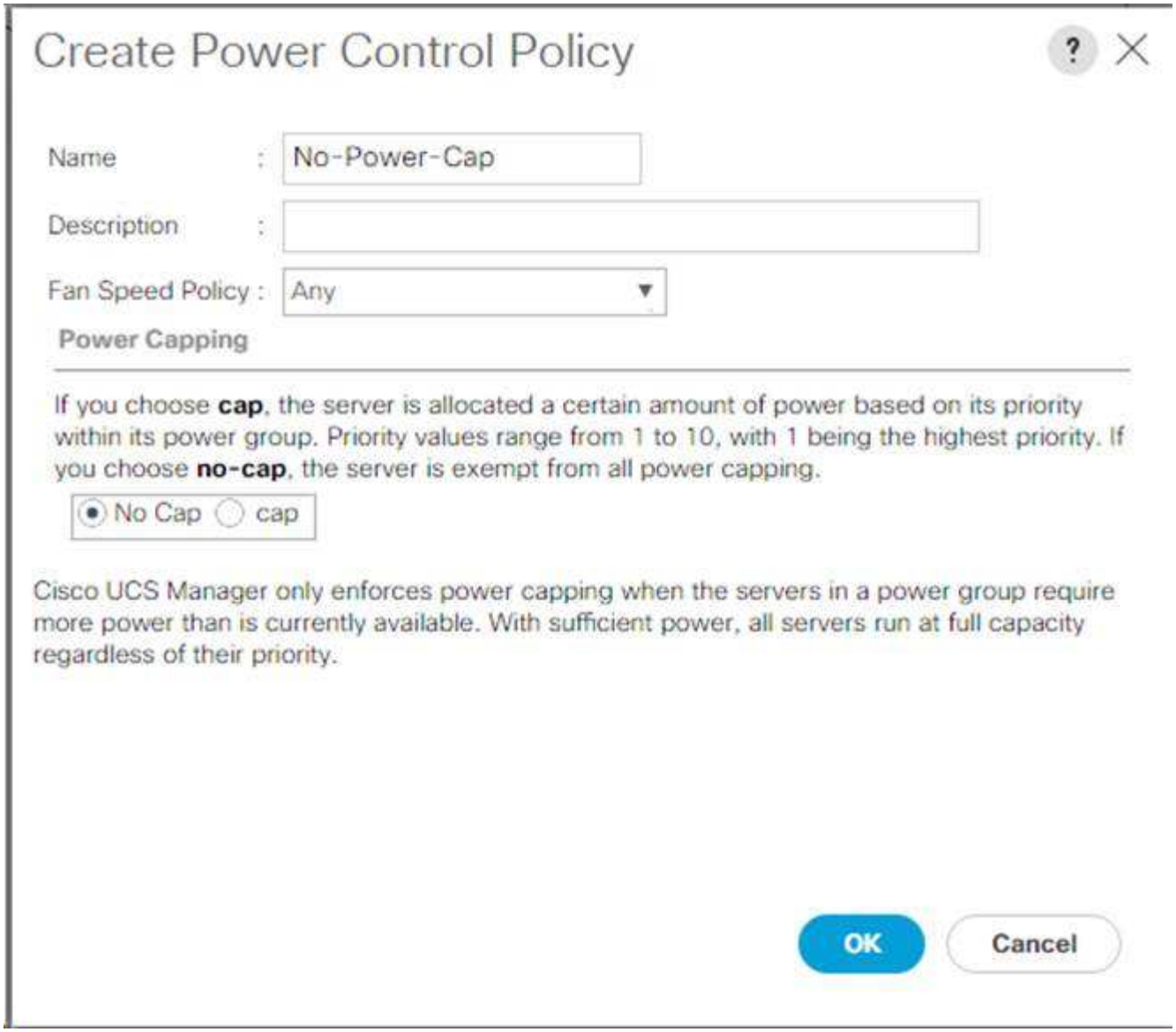
1. Cisco UCS Manager의 경우 왼쪽에 있는 LAN을 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. 네트워크 제어 정책 을 마우스 오른쪽 단추로 클릭합니다.
4. 네트워크 제어 정책 생성 을 선택합니다.
5. Enable-CDP-LLDP 정책 이름을 입력합니다.
6. CDP의 경우 사용 옵션을 선택합니다.
7. LLDP의 경우 아래로 스크롤하여 전송 및 수신 모두에 대해 사용 을 선택합니다.
8. 확인 을 클릭하여 네트워크 제어 정책을 생성합니다. 확인 을 클릭합니다.



전원 제어 정책을 생성합니다

Cisco UCS 환경에 대한 전원 제어 정책을 생성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에서 서버 탭을 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. 전원 제어 정책 을 마우스 오른쪽 단추로 클릭합니다.
4. 전원 제어 정책 생성 을 선택합니다.
5. 전원 제어 정책 이름으로 No-Power-Cap을 입력합니다.
6. 전력 제한 설정을 캡 없음 으로 변경합니다.
7. 확인 을 클릭하여 전원 제어 정책을 만듭니다. 확인 을 클릭합니다.



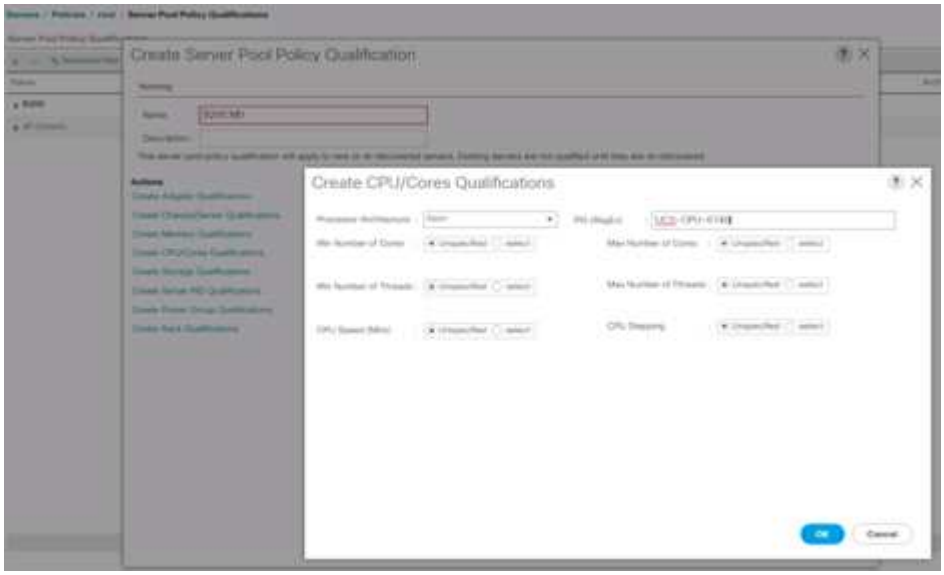
서버 풀 검증 정책 생성(선택 사항)

Cisco UCS 환경에 대해 선택적인 서버 풀 검증 정책을 생성하려면 다음 단계를 완료하십시오.

이 예에서는 Intel E2660 v4 Xeon Broadwell 프로세서를 사용하는 Cisco UCS B-Series 서버에 대한 정책을 생성합니다.

1. Cisco UCS Manager의 경우 왼쪽에 있는 서버 를 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. 서버 풀 정책 자격 을 선택합니다.
4. Create Server Pool Policy Qualification 또는 Add를 선택합니다.
5. 정책 이름을 인텔 으로 지정합니다.
6. Create CPU/Cores Qualifications(CPU/코어 자격 생성) 를 선택합니다.
7. 프로세서/아키텍처로 제온을 선택합니다.

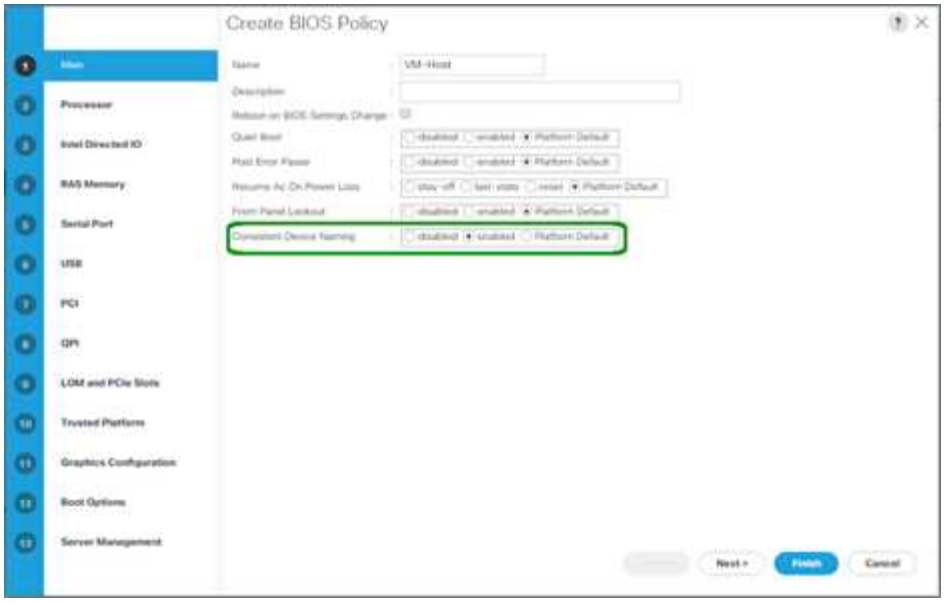
8. 프로세스 ID(PID)로 '<UCS-CPU-PID>'를 입력합니다.
9. 확인 을 클릭하여 CPU/코어 조건을 만듭니다.
10. 확인 을 클릭하여 정책을 생성한 다음 확인 을 클릭합니다.



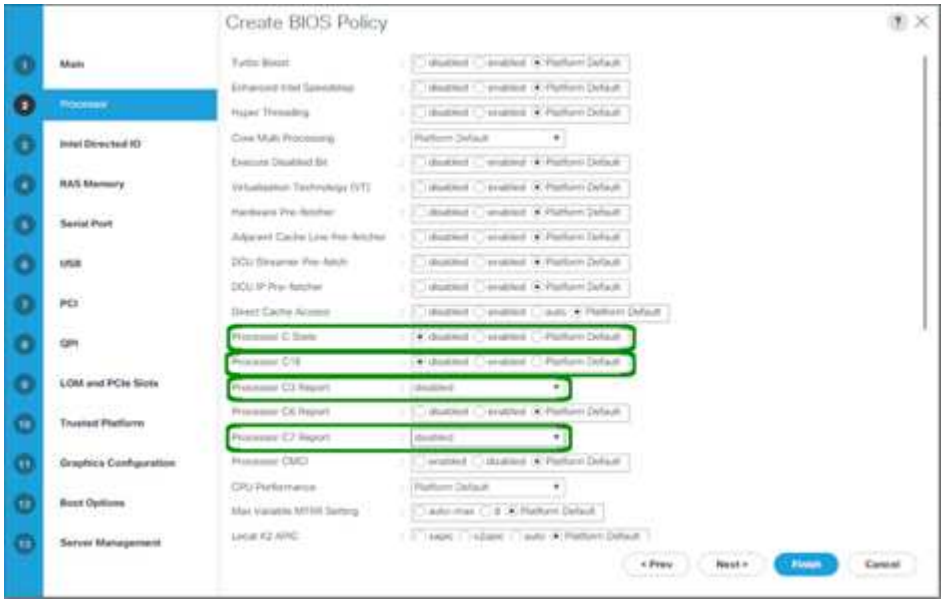
서버 **BIOS** 정책을 만듭니다

Cisco UCS 환경에 대한 서버 BIOS 정책을 생성하려면 다음 단계를 수행하십시오.

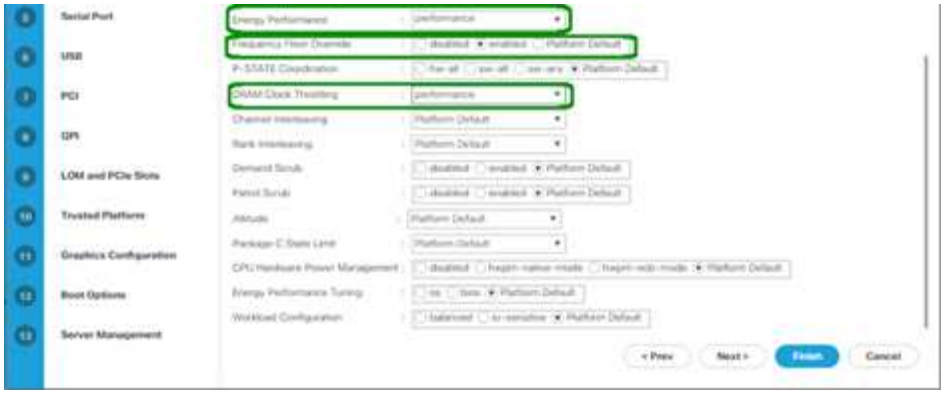
1. Cisco UCS Manager의 경우 왼쪽에 있는 서버 를 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. BIOS 정책을 마우스 오른쪽 단추로 클릭합니다.
4. BIOS 정책 생성 을 선택합니다.
5. BIOS 정책 이름으로 VM-Host를 입력합니다.
6. 자동 부팅 설정을 사용 안 함으로 변경합니다.
7. 정합성 보장 장치 이름을 사용으로 변경합니다.



8. 프로세서 탭을 선택하고 다음 매개 변수를 설정합니다.
   - 프로세서 C 상태: 비활성화됨
   - 처리기 C1E: 비활성화
   - 프로세서 C3 보고서: 사용 안 함
   - 프로세서 C7 보고서: 사용 안 함



9. 나머지 프로세서 옵션까지 아래로 스크롤하여 다음 매개변수를 설정합니다.
   - 에너지 성능: 성능
   - Frequency Floor Override: enabled(주파수 플로어 재설정
   - DRAM 클럭 제한: 성능



10. RAS 메모리 를 클릭하고 다음 매개변수를 설정합니다.
    - LV DDR 모드: 성능 모드

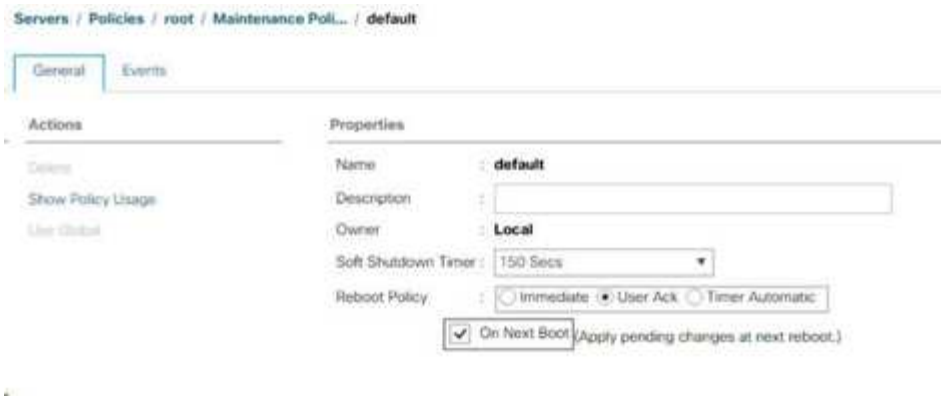


11. 마침 을 클릭하여 BIOS 정책을 만듭니다.
12. 확인 을 클릭합니다.

기본 유지 관리 정책을 업데이트합니다

기본 유지 관리 정책을 업데이트하려면 다음 단계를 완료하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 서버 를 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. Maintenance Policies > default 를 선택합니다.
4. 재부팅 정책을 사용자 승인 으로 변경합니다.
5. 다음 부팅 시 를 선택하여 유지 관리 창을 서버 관리자에게 위임합니다.



6. 변경 내용 저장 을 클릭합니다.
7. 확인 을 클릭하여 변경 사항을 적용합니다.

vNIC 템플릿을 생성합니다

Cisco UCS 환경에 대한 vNIC(Virtual Network Interface Card) 템플릿을 여러 개 생성하려면 이 섹션에 설명된 절차를 완료하십시오.

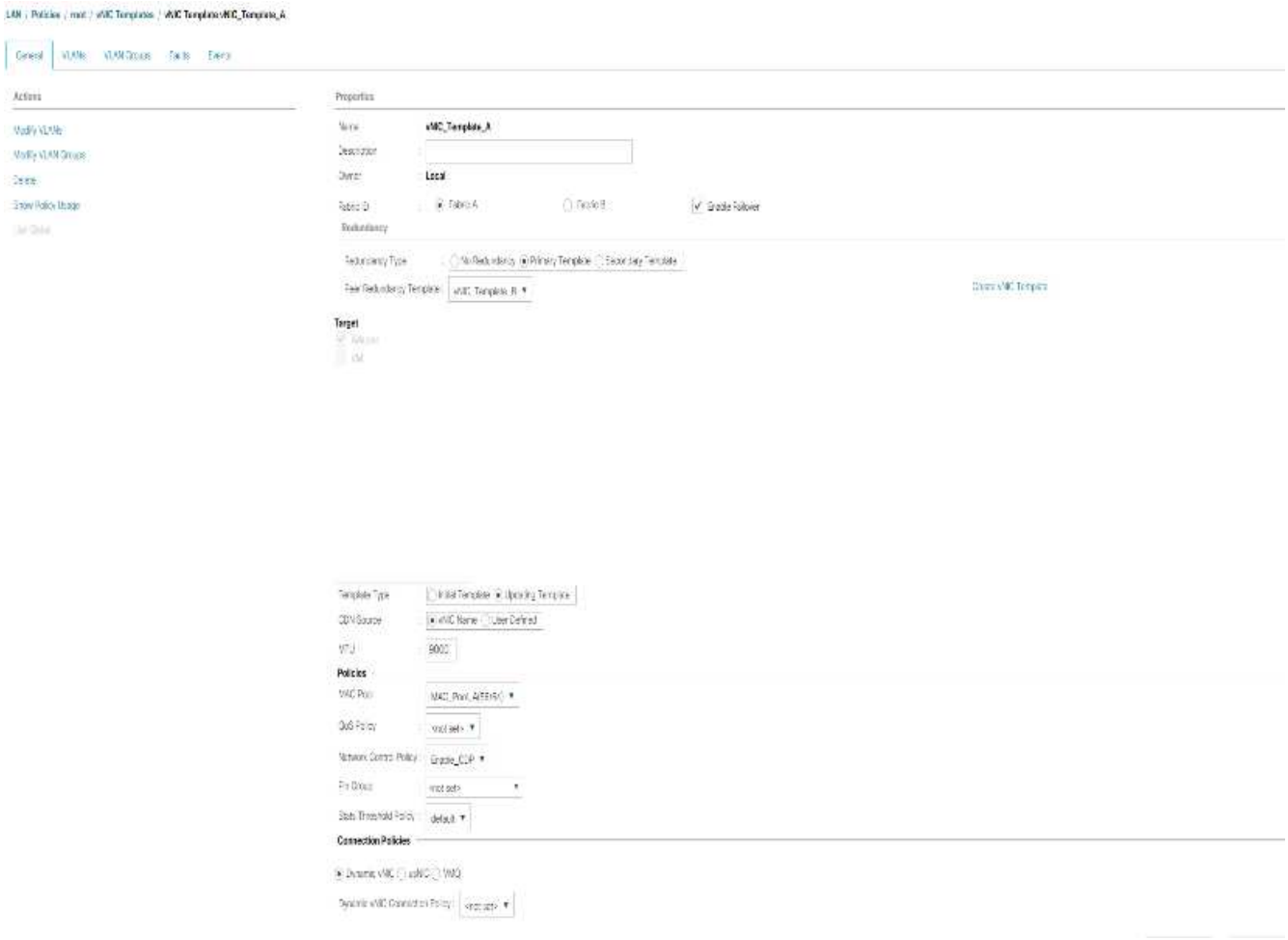
총 4개의 vNIC 템플릿이 생성됩니다.

인프라 vNIC를 생성합니다

인프라 vNIC를 생성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 LAN을 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. vNIC 템플릿을 마우스 오른쪽 버튼으로 클릭합니다.
4. vNIC 템플릿 생성 을 선택합니다.
5. vNIC 템플릿 이름으로 Site-XX-vNIC_A를 입력합니다.
6. 템플릿 유형으로 Update-template(업데이트-템플릿) 을 선택합니다.
7. Fabric ID로 Fabric A를 선택합니다
8. Enable Failover 옵션이 선택되지 않았는지 확인합니다.
9. 중복 유형으로 기본 템플릿을 선택합니다.
10. 피어 중복 템플릿은 "<설정되지 않음>"으로 설정된 상태로 둡니다.
11. 대상에서 어댑터 옵션만 선택되어 있는지 확인합니다.
12. Native-VLAN을 native VLAN으로 설정한다.
13. CDN 소스로 vNIC 이름 을 선택합니다.
14. MTU의 경우 9000을 입력합니다.
15. 허용된 VLAN에서 'Native-VLAN, Site-XX-IB-MGMT, Site-XX-NFS, Site-XX-VM-Traffic'을 선택합니다. 및 Site-XX-vMotion을 참조하십시오. Ctrl 키를 사용하여 이 항목을 여러 개 선택합니다.
16. 선택 을 클릭합니다. 이제 이러한 VLAN이 선택한 VLAN 아래에 나타납니다.

17. MAC Pool 목록에서 MAC_Pool_A를 선택합니다.
18. 네트워크 제어 정책 목록에서 Pool-A를 선택합니다
19. 네트워크 제어 정책 목록에서 Enable-CDP-LLDP 를 선택합니다.
20. 확인 을 클릭하여 vNIC 템플릿을 생성합니다.
21. 확인 을 클릭합니다.

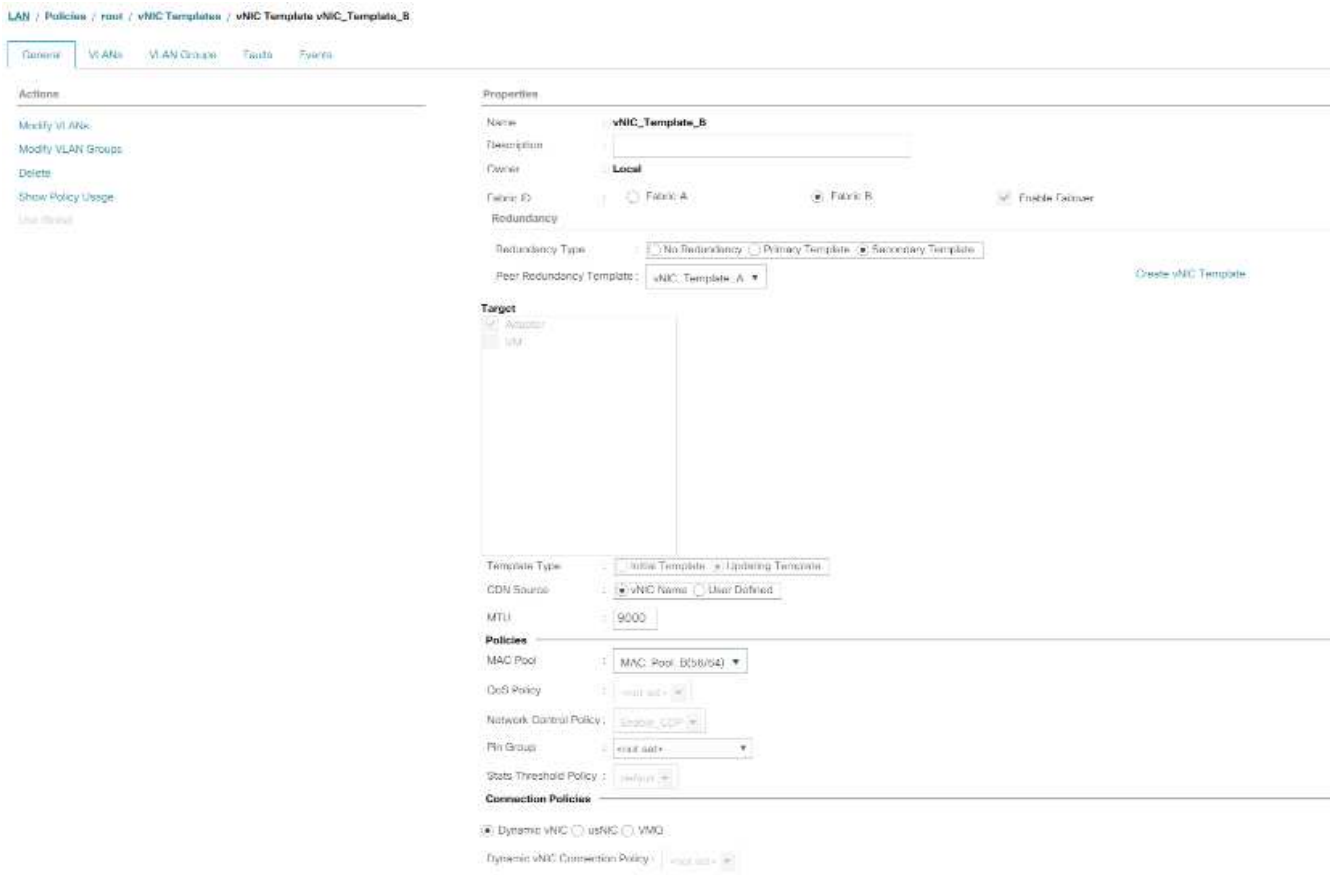


보조 중복 템플릿 Infra-B를 생성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 LAN을 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. vNIC 템플릿을 마우스 오른쪽 버튼으로 클릭합니다.
4. vNIC 템플릿 생성 을 선택합니다.
5. vNIC 템플릿 이름으로 Site-XX-vNIC_B를 입력합니다.
6. 템플릿 유형으로 Update-template(업데이트-템플릿) 을 선택합니다.
7. Fabric ID로 Fabric B를 선택합니다
8. Enable Failover 옵션을 선택합니다.

페일오버를 선택하는 것은 하드웨어 레벨에서 이를 처리하고 가상 스위치에서 NIC 장애가 감지되지 않을 가능성을 방지함으로써 링크 페일오버 시간을 개선하는 중요한 단계입니다.

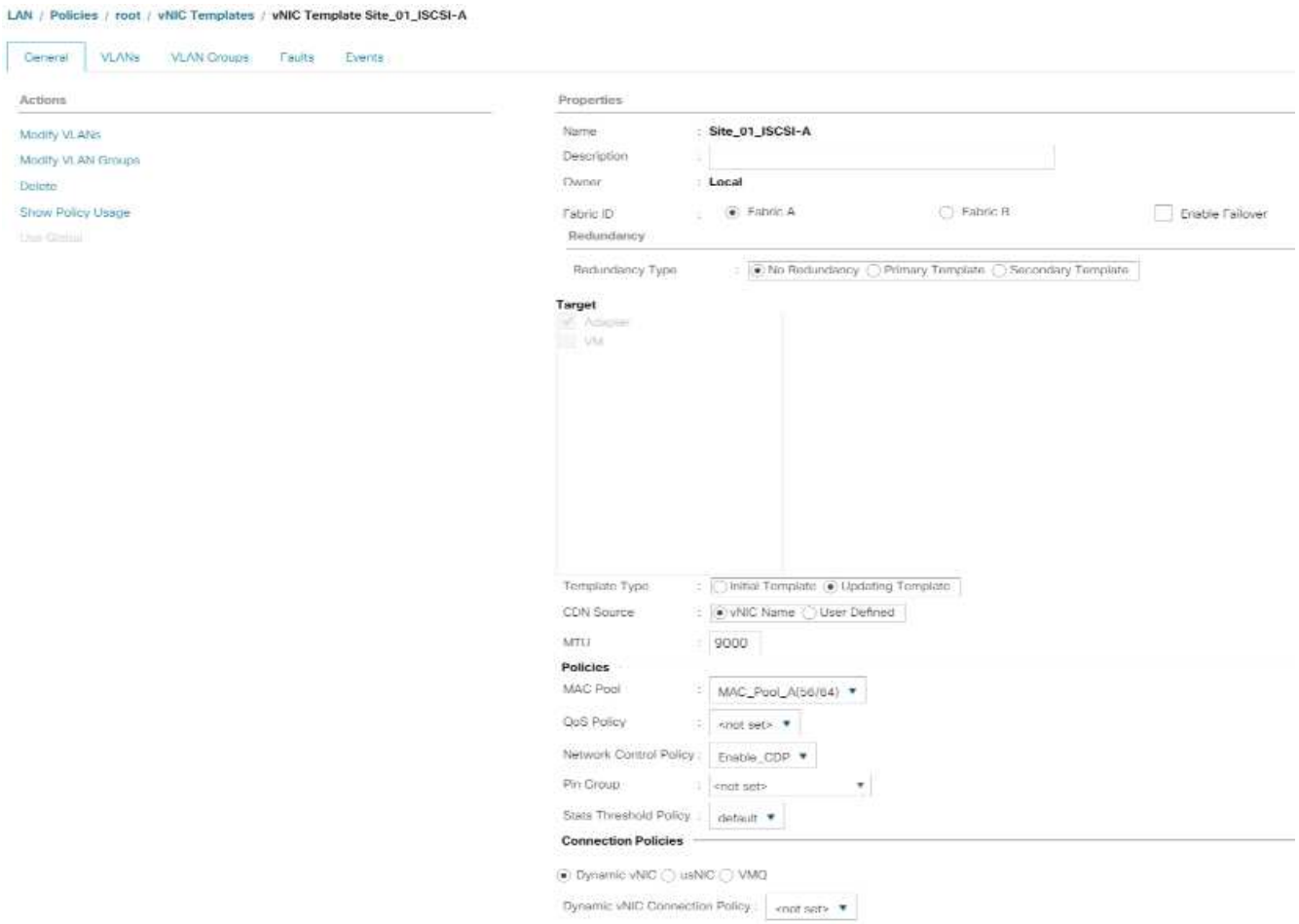
9. 중복 유형으로 기본 템플릿을 선택합니다.
10. 피어 이중화 템플릿은 "vNIC_Template_A"로 설정된 상태로 둡니다.
11. 대상에서 어댑터 옵션만 선택되어 있는지 확인합니다.
12. Native-VLAN을 native VLAN으로 설정한다.
13. CDN 소스로 vNIC 이름 을 선택합니다.
14. MTU의 경우 '9000'을 입력합니다.
15. 허용된 VLAN에서 'Native-VLAN, Site-XX-IB-MGMT, Site-XX-NFS, Site-XX-VM-Traffic'을 선택합니다. 및 Site-XX-vMotion을 참조하십시오. Ctrl 키를 사용하여 이 항목을 여러 개 선택합니다.
16. 선택 을 클릭합니다. 이제 이러한 VLAN이 선택한 VLAN 아래에 나타납니다.
17. MAC Pool 목록에서 MAC_Pool_B를 선택합니다.
18. 네트워크 제어 정책 목록에서 Pool-B를 선택합니다
19. 네트워크 제어 정책 목록에서 Enable-CDP-LLDP 를 선택합니다.
20. 확인 을 클릭하여 vNIC 템플릿을 생성합니다.
21. 확인 을 클릭합니다.



iSCSI vNIC를 생성합니다

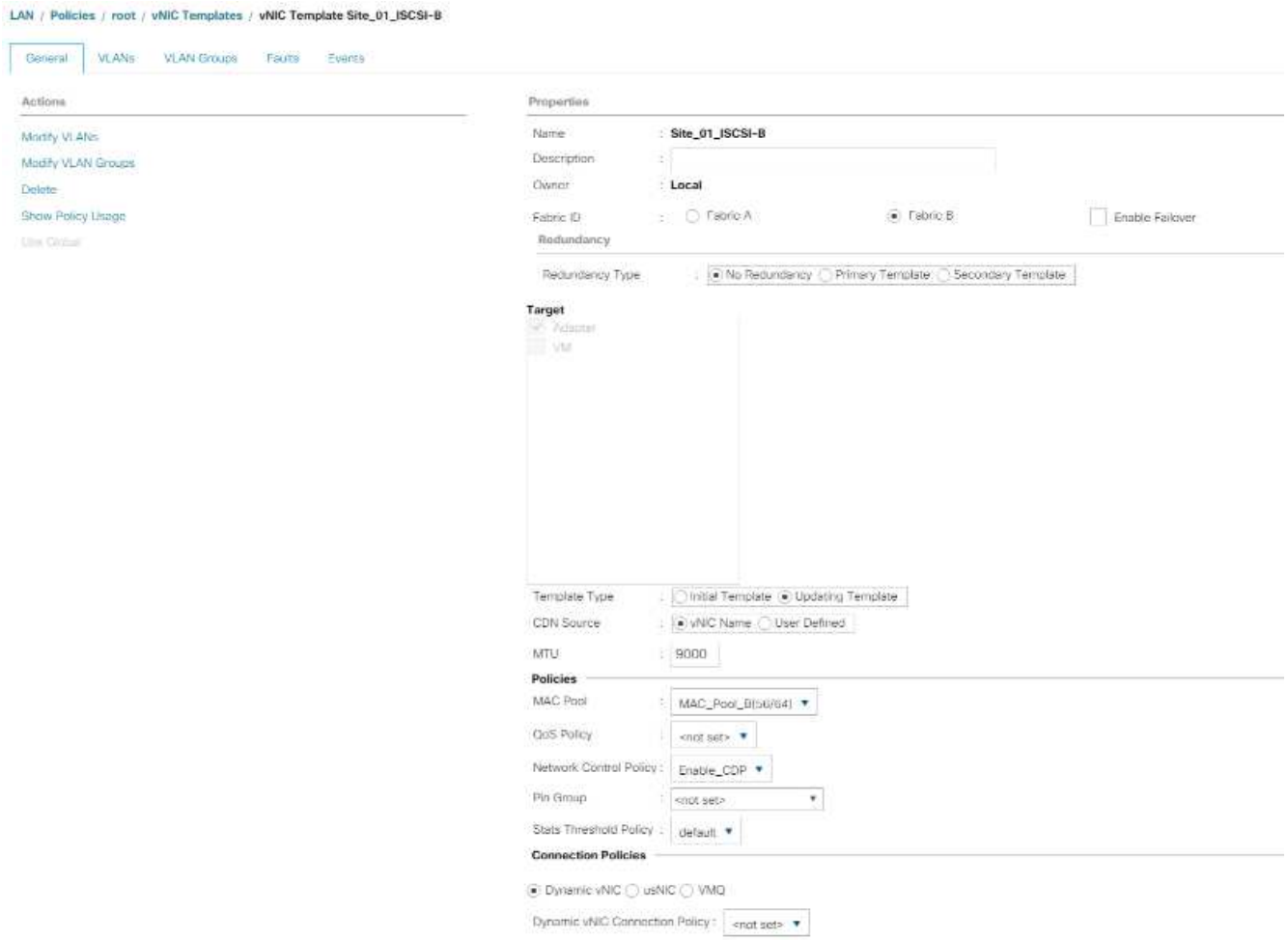
iSCSI vNIC를 생성하려면 다음 단계를 수행하십시오.

1. 왼쪽에서 LAN 을 선택합니다.
2. 정책 > 루트를 선택합니다.
3. vNIC 템플릿을 마우스 오른쪽 버튼으로 클릭합니다.
4. vNIC 템플릿 생성 을 선택합니다.
5. vNIC 템플릿 이름으로 Site-01-iscsi_a를 입력합니다.
6. 패브릭 A 를 선택합니다 Enable Failover 옵션을 선택하지 마십시오.
7. 중복성 유형을 중복되지 않음 으로 설정합니다.
8. 대상에서 어댑터 옵션만 선택되어 있는지 확인합니다.
9. 템플릿 유형으로 템플릿 업데이트를 선택합니다.
10. VLAN에서 Site-01-iSCSI_A_VLAN만 선택합니다.
11. Site-01-iscsi_a_vlan을 기본 VLAN으로 선택합니다.
12. CDN 소스에 대해 vNIC 이름을 설정된 상태로 둡니다.
13. MTU에서 9000을 입력합니다.
14. MAC Pool 목록에서 MAC-Pool-A를 선택합니다
15. 네트워크 제어 정책 목록에서 Enable-CDP-LLDP 를 선택합니다.
16. 확인 을 클릭하여 vNIC 템플릿 생성을 완료합니다.
17. 확인 을 클릭합니다.



18. 왼쪽에서 LAN 을 선택합니다.
19. 정책 > 루트를 선택합니다.
20. vNIC 템플릿을 마우스 오른쪽 버튼으로 클릭합니다.
21. vNIC 템플릿 생성 을 선택합니다.
22. vNIC 템플릿 이름으로 Site-01-ISCSI_B를 입력합니다.
23. Fabric B를 선택합니다 Enable Failover 옵션을 선택하지 마십시오.
24. 중복성 유형을 중복되지 않음 으로 설정합니다.
25. 대상에서 어댑터 옵션만 선택되어 있는지 확인합니다.
26. 템플릿 유형으로 템플릿 업데이트를 선택합니다.
27. VLAN에서 'ite-01-iscsi_B_vlan'만 선택합니다.
28. 네이티브 VLAN으로 Site-01-ISCSI_B_VLAN을 선택한다.
29. CDN 소스에 대해 vNIC 이름을 설정된 상태로 둡니다.
30. MTU에서 9000을 입력합니다.
31. MAC Pool 목록에서 MAC-Pool-B를 선택합니다.
32. Network Control Policy 목록에서 Enable-CDP-LLDP를 선택합니다.
33. 확인 을 클릭하여 vNIC 템플릿 생성을 완료합니다.

34. 확인 을 클릭합니다.



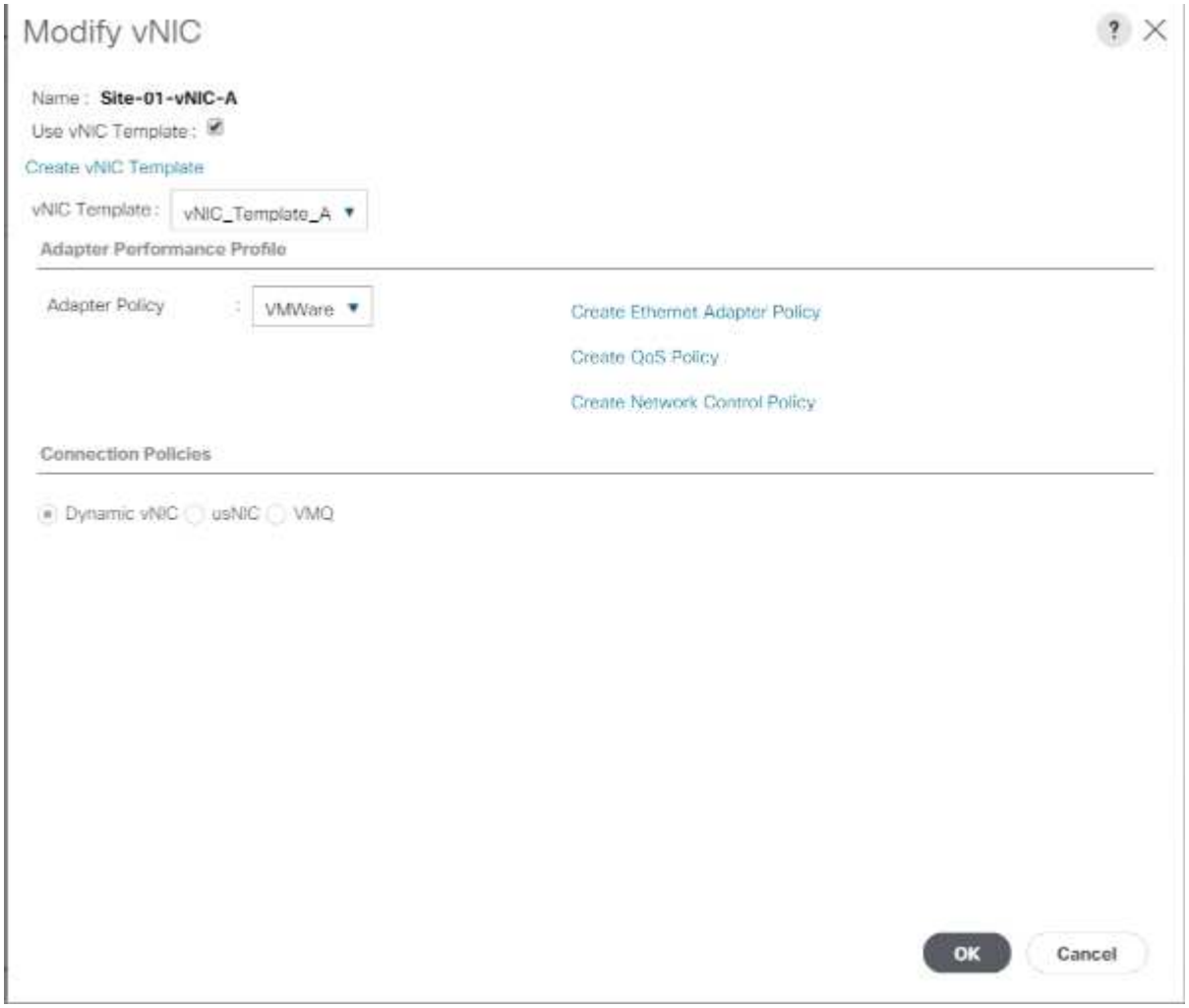
iSCSI 부트에 대한 **LAN** 연결 정책을 생성합니다

이 절차는 두 개의 iSCSI LIF가 클러스터 노드 1('iSCSI_liff 01a' 및 'iscsi_liff 01b')에 있고 두 개의 iSCSI LIF가 클러스터 노드 2('iscsi_liff 02a' 및 'iscsi_liff')에 있는 Cisco UCS 환경에 적용됩니다. 또한, LIF가 패브릭 A(Cisco UCS 6324 A)에 연결되고 B LIF가 패브릭 B(Cisco UCS 6324 B)에 연결된 것으로 가정합니다.

필요한 인프라 LAN 연결 정책을 구성하려면 다음 단계를 수행하십시오.

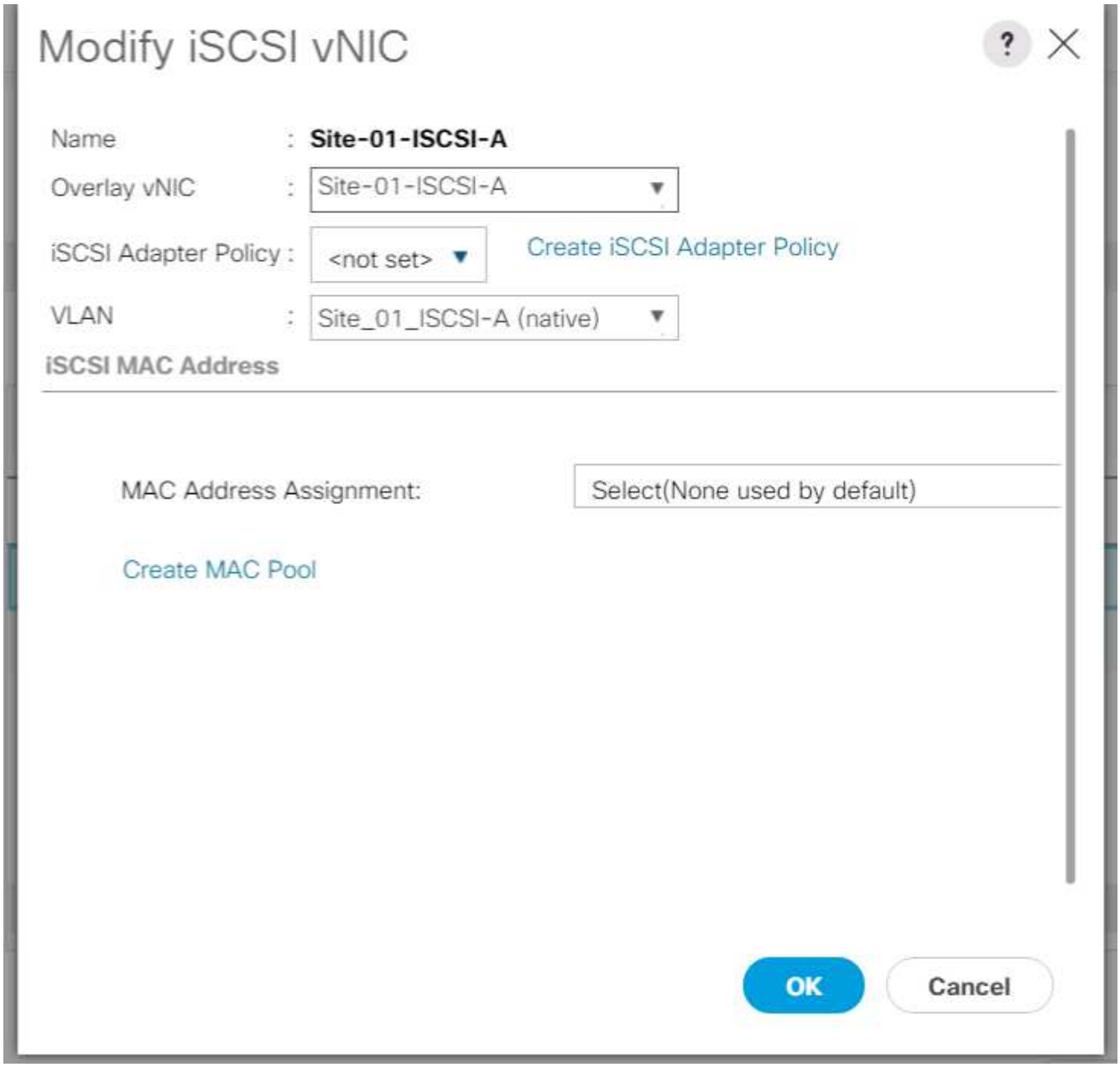
1. Cisco UCS Manager의 경우 왼쪽에 있는 LAN을 클릭합니다.
2. LAN > 정책 > 루트를 선택합니다.
3. LAN 연결 정책을 마우스 오른쪽 단추로 클릭합니다.
4. LAN 연결 정책 생성 을 선택합니다.
5. 정책 이름으로 사이트 XX-Fabric-A를 입력합니다.
6. vNIC를 추가하려면 상단 추가 옵션을 클릭합니다.
7. vNIC 생성 대화 상자에서 vNIC 이름으로 'ite-01-vNIC-A'를 입력합니다.
8. vNIC 템플릿 사용 옵션을 선택합니다.

9. vNIC 템플릿 목록에서 'vNIC_Template_A'를 선택합니다.
10. 어댑터 정책 드롭다운 목록에서 VMware 를 선택합니다.
11. 확인 을 클릭하여 이 vNIC를 정책에 추가합니다.

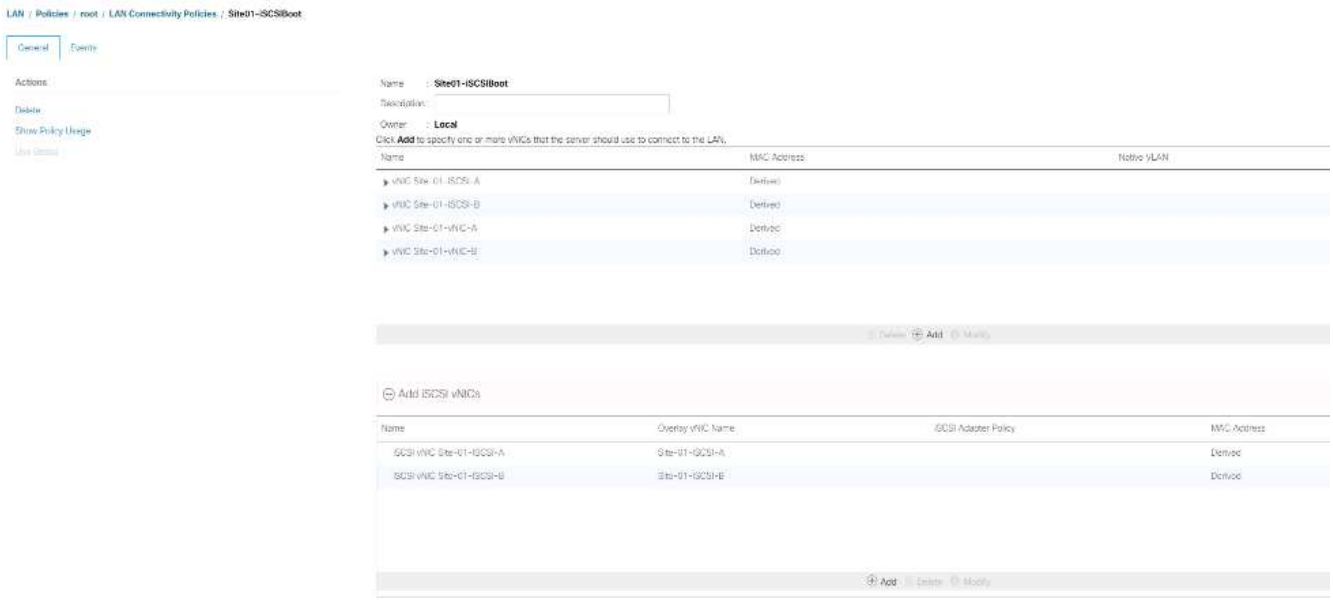


12. vNIC를 추가하려면 상단 추가 옵션을 클릭합니다.
13. vNIC 생성 대화 상자에서 vNIC 이름으로 'ite-01-vNIC-B'를 입력합니다.
14. vNIC 템플릿 사용 옵션을 선택합니다.
15. vNIC 템플릿 목록에서 'vNIC_Template_B'를 선택합니다.
16. 어댑터 정책 드롭다운 목록에서 VMware 를 선택합니다.
17. 확인 을 클릭하여 이 vNIC를 정책에 추가합니다.
18. vNIC를 추가하려면 상단 추가 옵션을 클릭합니다.
19. vNIC 생성 대화 상자에서 vNIC 이름으로 Site-01-iscsi-A를 입력합니다.
20. vNIC 템플릿 사용 옵션을 선택합니다.
21. vNIC 템플릿 목록에서 '사이트-01-iSCSI-A'를 선택합니다.
22. 어댑터 정책 드롭다운 목록에서 VMware 를 선택합니다.
23. 확인 을 클릭하여 이 vNIC를 정책에 추가합니다.

24. vNIC를 추가하려면 상단 추가 옵션을 클릭합니다.
25. vNIC 생성 대화 상자에서 vNIC 이름으로 Site-01-iscsi-B를 입력합니다.
26. vNIC 템플릿 사용 옵션을 선택합니다.
27. vNIC 템플릿 목록에서 '사이트-01-iSCSI-B'를 선택합니다.
28. 어댑터 정책 드롭다운 목록에서 VMware 를 선택합니다.
29. 확인 을 클릭하여 이 vNIC를 정책에 추가합니다.
30. iSCSI vNIC 추가 옵션을 확장합니다.
31. iSCSI vNIC 공간 추가 에서 아래쪽 추가 옵션을 클릭하여 iSCSI vNIC를 추가합니다.
32. iSCSI vNIC 생성 대화 상자에서 vNIC 이름으로 Site-01-iscsi-A를 입력합니다.
33. 오버레이 vNIC를 'ite-01-iscsi-a'로 선택합니다.
34. iSCSI 어댑터 정책 옵션을 Not Set로 둡니다.
35. VLAN을 Site-01-ISCSI-Site-A(NATIVE)로 선택합니다.
36. MAC 주소 할당으로 없음(기본값: 사용)을 선택합니다.
37. 확인 을 클릭하여 iSCSI vNIC를 정책에 추가합니다.



38. iSCSI vNIC 공간 추가 에서 아래쪽 추가 옵션을 클릭하여 iSCSI vNIC를 추가합니다.
39. iSCSI vNIC 생성 대화 상자에서 vNIC 이름으로 Site-01-iscsi-B를 입력합니다.
40. 오버레이 vNIC를 Site-01-iSCSI-B로 선택합니다
41. iSCSI 어댑터 정책 옵션을 Not Set로 둡니다.
42. VLAN을 Site-01-iSCSI-Site-B(NATIVE)로 선택합니다.
43. MAC 주소 할당으로 없음(기본값: 사용)을 선택합니다.
44. 확인 을 클릭하여 iSCSI vNIC를 정책에 추가합니다.
45. 변경 내용 저장 을 클릭합니다.



VMware ESXi 6.7U1 설치 부팅에 대한 **vMedia** 정책을 생성합니다

NetApp Data ONTAP 설정 단계에서는 NetApp Data ONTAP 및 VMware 소프트웨어를 호스팅하는 데 사용되는 HTTP 웹 서버가 필요합니다. 여기서 생성된 vMedia 정책은 VMware ESXi 6을 매핑합니다. 7U1 ISO를 클릭하여 ESXi 설치를 부팅합니다. 이 정책을 만들려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에서 서버 를 선택합니다.
2. 정책 > 루트를 선택합니다.
3. vMedia 정책 을 선택합니다.
4. 추가 를 클릭하여 새 vMedia 정책을 생성합니다.
5. 정책 이름을 ESXi-6.7U1-HTTP 로 지정합니다.
6. 설명 필드에 ESXi 6.7U1의 마운트 ISO를 입력합니다.
7. 마운트 실패 시 재시도를 위해 예를 선택하십시오.
8. 추가 를 클릭합니다.
9. 마운트 ESXi-6.7U1-HTTP의 이름을 지정합니다.
10. CDD Device Type을 선택한다.
11. HTTP 프로토콜을 선택합니다.
12. 웹 서버의 IP 주소를 입력합니다.

> DNS 서버 IP가 이전에 KVM IP에 입력되지 않았으므로 호스트 이름 대신 웹 서버의 IP를 입력해야 합니다.

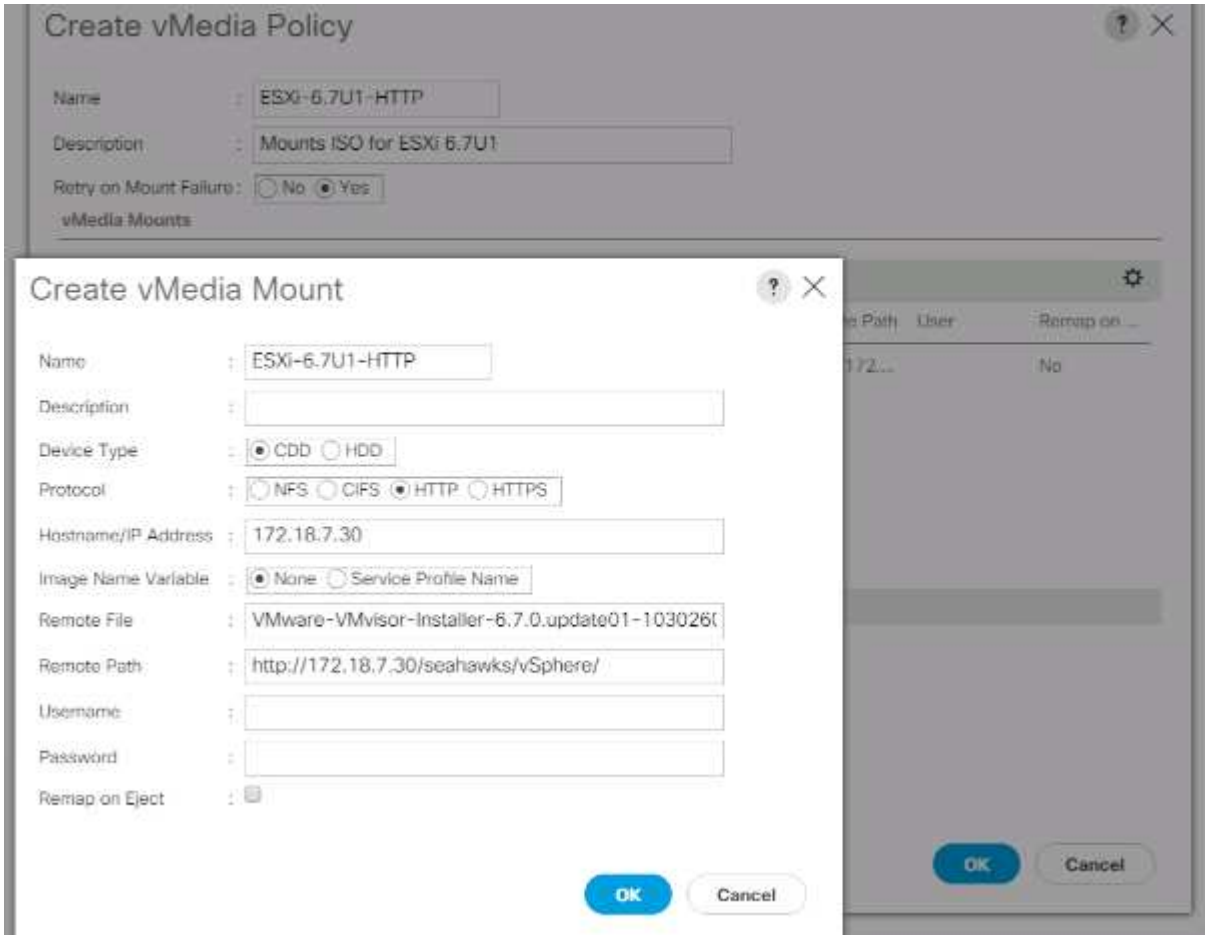
13. 원격 파일 이름으로 VMware-VMvisor-Installer-6.7.0.update01-10302608.x86_64.iso를 입력합니다.

    이 VMware ESXi 6.7U1 ISO는 에서 다운로드할 수 있습니다 "VMware 다운로드".

14. 원격 경로 필드에 ISO 파일의 웹 서버 경로를 입력합니다.

15. OK를 클릭하여 vMedia Mount를 생성합니다.
16. 확인 을 클릭한 다음 확인 을 다시 클릭하여 vMedia 정책 생성을 완료합니다.

Cisco UCS 환경에 추가된 새 서버의 경우 vMedia 서비스 프로필 템플릿을 사용하여 ESXi 호스트를 설치할 수 있습니다. SAN 마운트 디스크가 비어 있기 때문에 첫 번째 부팅 시 호스트가 ESXi 설치 프로그램으로 부팅됩니다. ESXi가 설치된 후에는 부팅 디스크에 액세스할 수 있는 한 vMedia가 참조되지 않습니다.



iSCSI 부트 정책을 생성합니다

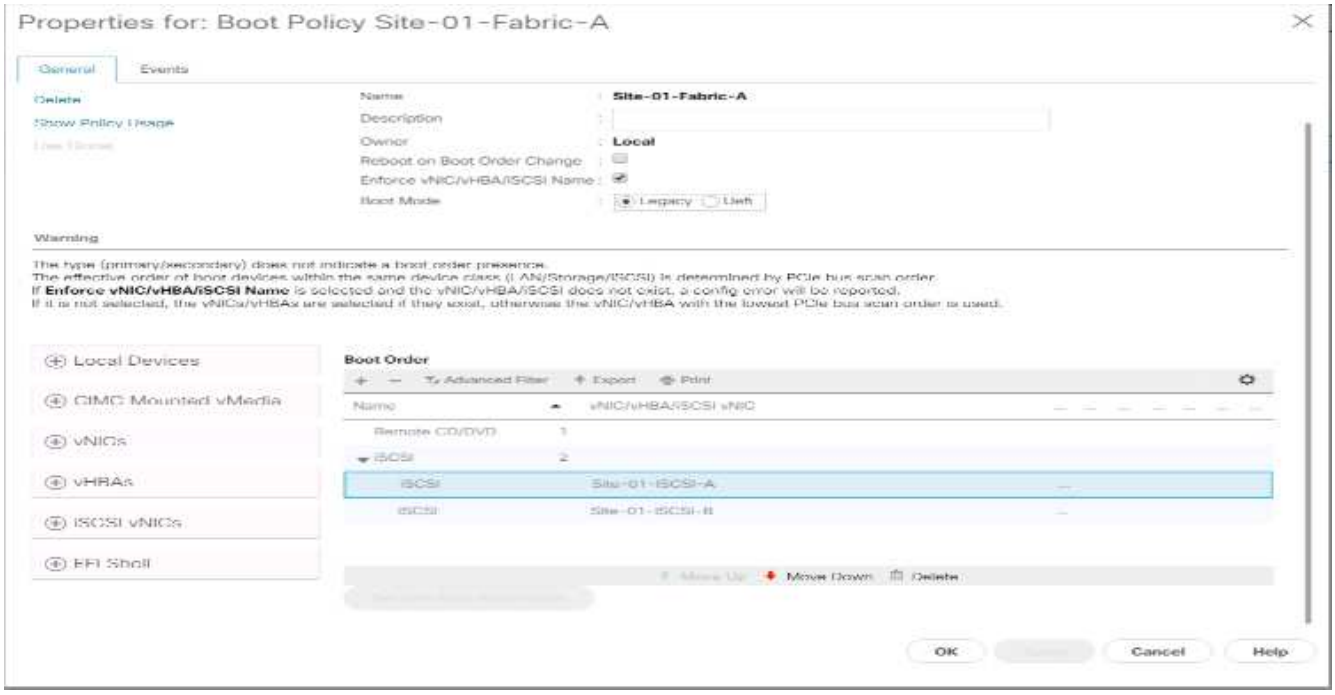
이 섹션의 절차는 두 개의 iSCSI 논리 인터페이스(LIF)가 클러스터 노드 1('iSCSI_liff 01a' 및 'iSCSI_liff')에 있고 두 개의 iSCSI LIF가 클러스터 노드 2('iscsi_liff 02a' 및 'iscsi_liff')에 있는 Cisco UCS 환경에 적용됩니다. 또한, LIF가 패브릭 A(Cisco UCS Fabric Interconnect A)에 연결되고 B LIF는 패브릭 B(Cisco UCS Fabric Interconnect B)에 연결되어 있다고 가정합니다.

이 절차에서 하나의 부팅 정책이 구성됩니다. 이 정책은 기본 대상을 "iscsi_liff 01a"로 구성합니다.

Cisco UCS 환경에 대한 부팅 정책을 생성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 서버 를 클릭합니다.
2. 정책 > 루트를 선택합니다.
3. Boot Policies 를 마우스 오른쪽 버튼으로 클릭합니다.
4. Create Boot Policy를 선택합니다.

5. 부팅 정책의 이름으로 '사이트-01-Fabric-A'를 입력합니다.
6. 선택 사항: 부팅 정책에 대한 설명을 입력합니다.
7. Boot Order Change(부팅 순서 변경) 옵션의 Reboot(재부팅) 옵션을 선택하지 않은 상태로 유지합니다.
8. 부팅 모드가 레거시입니다.
9. 로컬 장치 드롭다운 메뉴를 확장하고 원격 CD/DVD 추가 를 선택합니다.
10. iSCSI vNIC 드롭다운 메뉴를 확장하고 iSCSI 부팅 추가 를 선택합니다.
11. Add iSCSI Boot 대화 상자에서 'ite-01-iscsi-a'를 입력합니다. 확인 을 클릭합니다.
12. Add iSCSI Boot 를 선택합니다.
13. Add iSCSI Boot 대화 상자에서 'ite-01-iscsi-B'를 입력합니다. 확인 을 클릭합니다.
14. 확인 을 클릭하여 정책을 생성합니다.



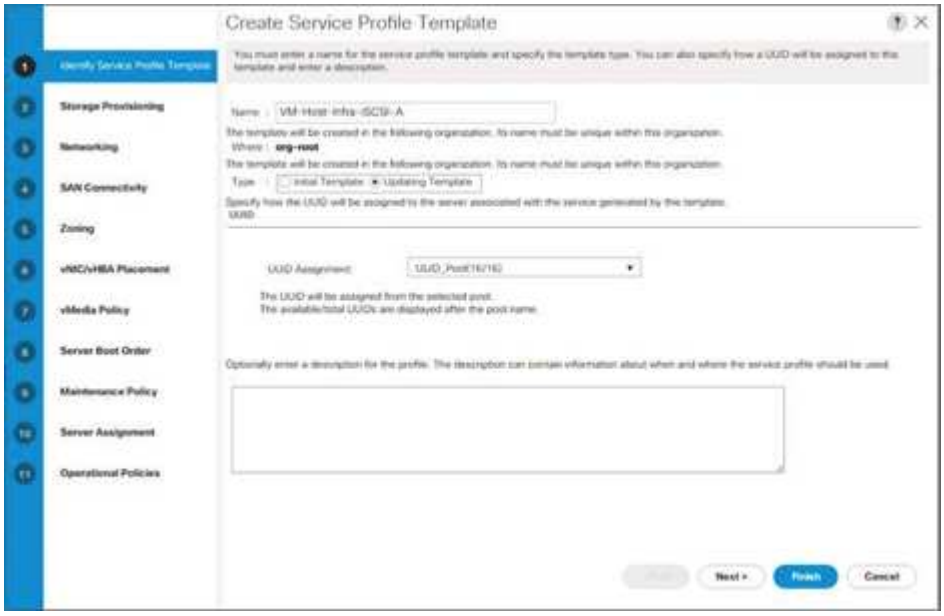
서비스 프로필 템플릿을 생성합니다

이 절차에서는 Fabric A 부팅을 위해 인프라스트럭처 ESXi 호스트에 대한 서비스 프로필 템플릿 하나가 생성됩니다.

서비스 프로필 템플릿을 생성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager의 경우 왼쪽에 있는 서버 를 클릭합니다.
2. 서비스 프로필 템플릿 > 루트 를 선택합니다.
3. root 를 마우스 오른쪽 단추로 클릭합니다.
4. 서비스 프로필 템플릿 생성 을 선택하여 서비스 프로필 템플릿 생성 마법사를 엽니다.
5. 서비스 프로필 템플릿의 이름으로 VM-Host-Infra-iSCSI-A를 입력합니다. 이 서비스 프로필 템플릿은 패브릭 A의 스토리지 노드 1에서 부팅하도록 구성됩니다
6. 템플릿 업데이트 옵션을 선택합니다.

7. UUID에서 UUID 풀로 UUID_Pool을 선택합니다. 다음 을 클릭합니다.



스토리지 프로비저닝을 구성합니다

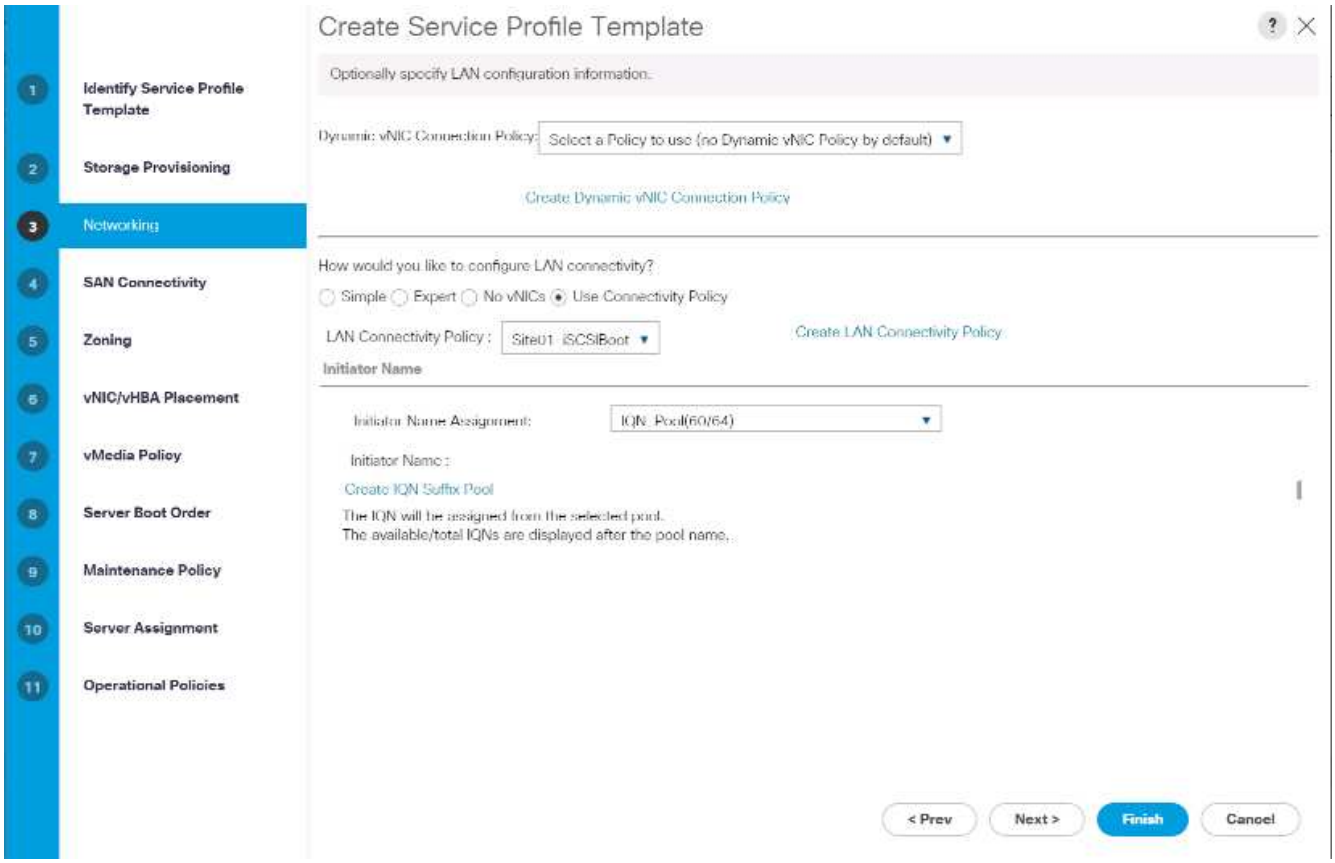
스토리지 프로비저닝을 구성하려면 다음 단계를 수행하십시오.

1. 물리적 디스크가 없는 서버가 있는 경우 로컬 디스크 구성 정책 을 클릭하고 SAN 부팅 로컬 스토리지 정책 을 선택합니다. 그렇지 않으면 기본 로컬 스토리지 정책을 선택합니다.
2. 다음 을 클릭합니다.

네트워킹 옵션을 구성합니다

네트워킹 옵션을 구성하려면 다음 단계를 수행하십시오.

1. 동적 vNIC 연결 정책의 기본 설정을 유지합니다.
2. 연결 정책 사용 옵션을 선택하여 LAN 연결을 구성합니다.
3. LAN 연결 정책 드롭다운 메뉴에서 iSCSI - 부팅 을 선택합니다.
4. 이니시에이터 이름 할당에서 IQN_Pool을 선택합니다. 다음 을 클릭합니다.



SAN 연결을 구성합니다

SAN 연결을 구성하려면 다음 단계를 수행하십시오.

1. vHBA의 경우 SAN 연결을 어떻게 구성하시겠습니까? 에서 아니요 를 선택합니다. 옵션을 선택합니다.
2. 다음 을 클릭합니다.

조닝을 구성합니다

조닝을 구성하려면 다음을 클릭합니다.

vNIC/HBA 배치를 구성합니다

vNIC/HBA 배치를 구성하려면 다음 단계를 수행하십시오.

1. Select Placement(배치 선택) 드롭다운 목록에서 배치 정책을 Let System Perform Placement(배치 수행) 로 둡니다.
2. 다음 을 클릭합니다.

vMedia 정책을 구성합니다

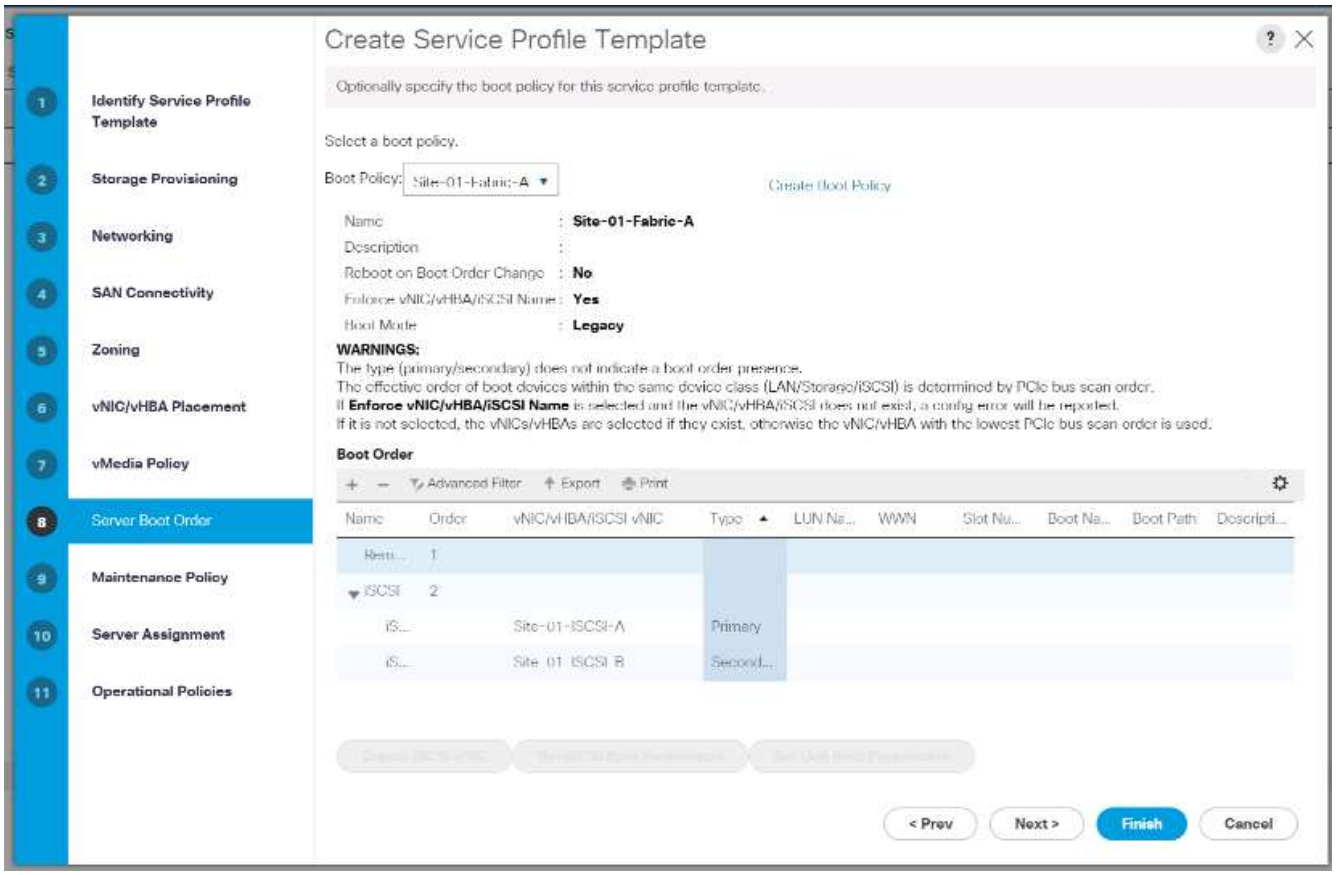
vMedia 정책을 구성하려면 다음 단계를 수행하십시오.

1. vMedia 정책을 선택하지 마십시오.
2. 다음 을 클릭합니다.

서버 부팅 순서를 구성합니다

서버 부팅 순서를 구성하려면 다음 단계를 수행하십시오.

1. Boot Policy에서 Boot-Fabric-A를 선택합니다.



2. 보or 순서에서 '사이트-01-iSCSI-A'를 선택합니다.
3. Set iSCSI Boot Parameters(iSCSI 부팅 매개변수 설정) 를 클릭합니다.
4. iSCSI 부트 매개 변수 설정 대화 상자에서 환경에 적합한 인증 프로파일을 별도로 만들지 않은 경우 인증 프로파일 옵션을 설정하지 않음 으로 둡니다.
5. 이전 단계에서 정의한 단일 서비스 프로필 이니시에이터 이름을 사용하려면 이니시에이터 이름 할당 대화 상자를 Not Set로 두십시오.
6. "iscsi_ip_Pool_a"를 초기자 IP 주소 정책으로 설정합니다.
7. iSCSI 정적 타겟 인터페이스 옵션을 선택합니다.
8. 추가 를 클릭합니다.
9. iSCSI 타겟 이름을 입력합니다. Infra-SVM의 iSCSI 대상 이름을 얻으려면 스토리지 클러스터 관리 인터페이스에 로그인하고 "iscsi show" 명령을 실행합니다.

```
bb04-aff300::> iscsi show
          Target                          Target                          Status
Vserver   Name                            Alias                           Admin
--------- ------------------------------- ------------------------------- ------
Infra-SVM iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                          Infra-SVM                       up
```

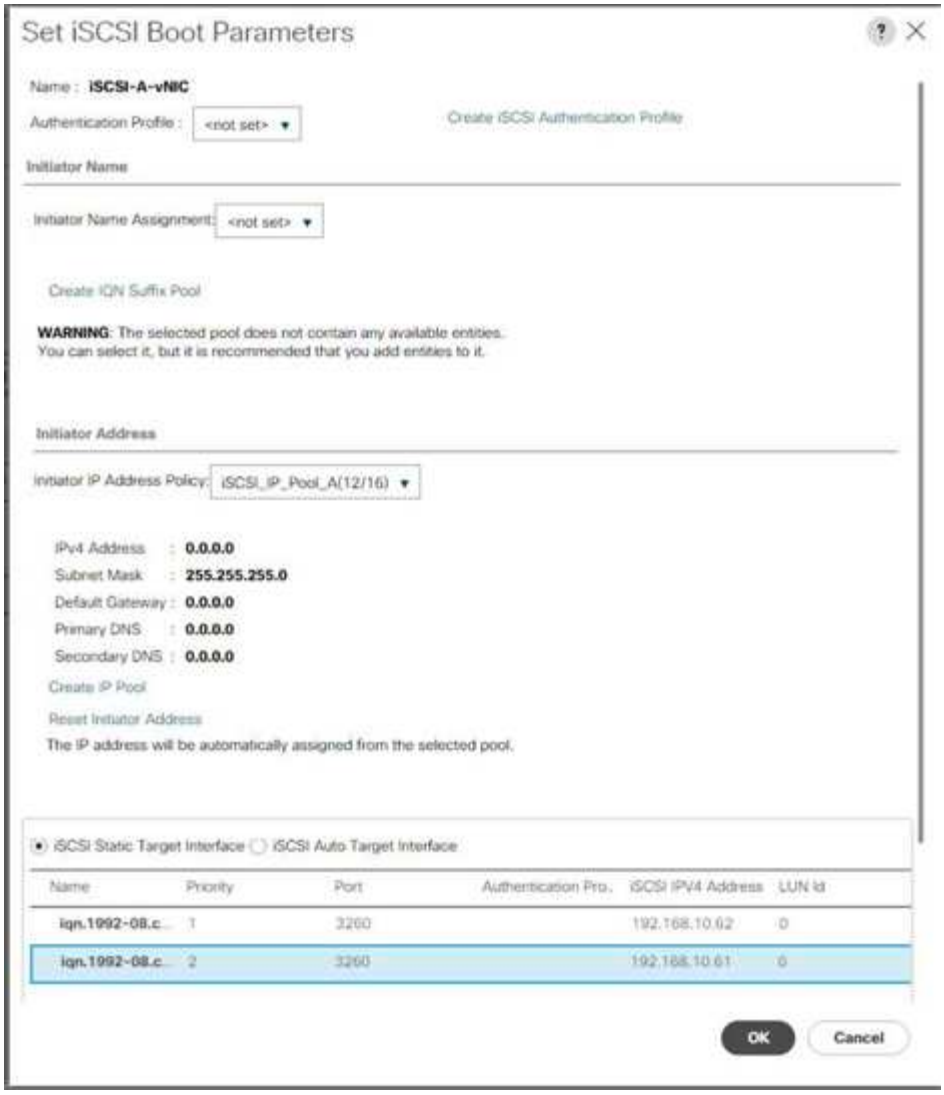
10. IPv4 Address 필드에 iSCSI_lif_02a IP 주소를 입력합니다.



11. 확인 을 클릭하여 iSCSI 정적 대상을 추가합니다.
12. 추가 를 클릭합니다.
13. iSCSI 타겟 이름을 입력합니다.
14. IPv4 Address 필드에 iSCSI_lif_01A IP 주소를 입력합니다.



15. 확인 을 클릭하여 iSCSI 정적 대상을 추가합니다.



타겟 IP는 스토리지 노드 02 IP를 먼저, 스토리지 노드 01 IP와 함께 배치되었습니다. 부팅 LUN이 노드 01에 있다고 가정합니다. 이 절차의 순서가 사용되는 경우 호스트는 노드 01의 경로를 사용하여 부팅됩니다.

16. 부팅 순서에서 iSCSI-B-vNIC를 선택합니다.
17. Set iSCSI Boot Parameters(iSCSI 부팅 매개변수 설정) 를 클릭합니다.
18. iSCSI 부트 매개 변수 설정 대화 상자에서 환경에 적합한 인증 프로파일을 별도로 만들지 않은 경우 인증 프로파일 옵션을 설정되지 않음 으로 둡니다.
19. 이전 단계에서 정의한 단일 서비스 프로필 이니시에이터 이름을 사용하려면 이니시에이터 이름 할당 대화 상자를 Not Set로 두십시오.
20. ISCSI_IP_Pool_B를 초기자 IP 주소 정책으로 설정합니다.
21. iSCSI 정적 타겟 인터페이스 옵션을 선택합니다.
22. 추가 를 클릭합니다.
23. iSCSI 타겟 이름을 입력합니다. Infra-SVM의 iSCSI 대상 이름을 얻으려면 스토리지 클러스터 관리 인터페이스에 로그인하고 "iscsi show" 명령을 실행합니다.

```
bb04-aff300::> iscsi show
          Target                          Target                          Status
Vserver   Name                            Alias                           Admin
--------- ------------------------------- ------------------------------- ------
Infra-SVM  iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                          Infra-SVM                       up
```

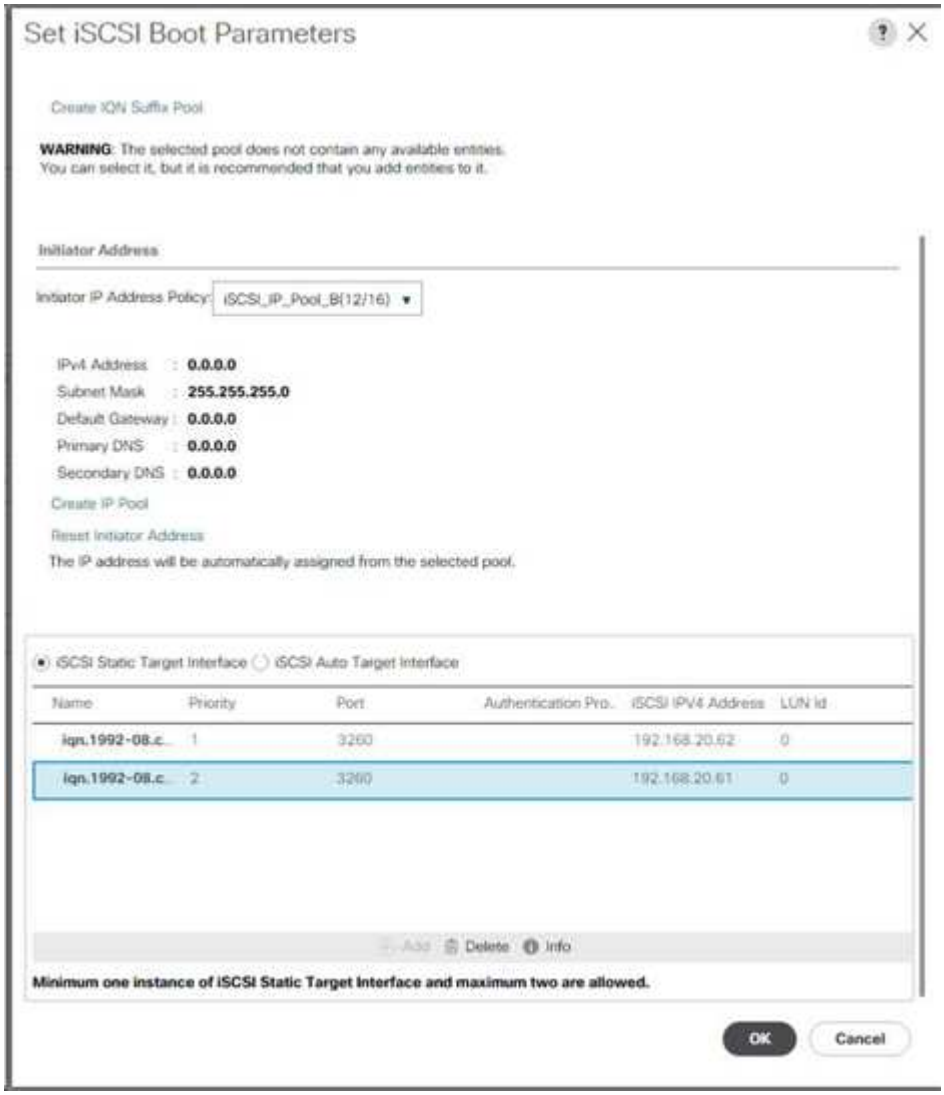
24. IPv4 Address 필드에 iSCSI_lif_02B의 IP 주소를 입력합니다.



25. 확인 을 클릭하여 iSCSI 정적 대상을 추가합니다.
26. 추가 를 클릭합니다.
27. iSCSI 타겟 이름을 입력합니다.
28. IPv4 Address 필드에 iSCSI_lif_01B IP 주소를 입력합니다.



29. 확인 을 클릭하여 iSCSI 정적 대상을 추가합니다.

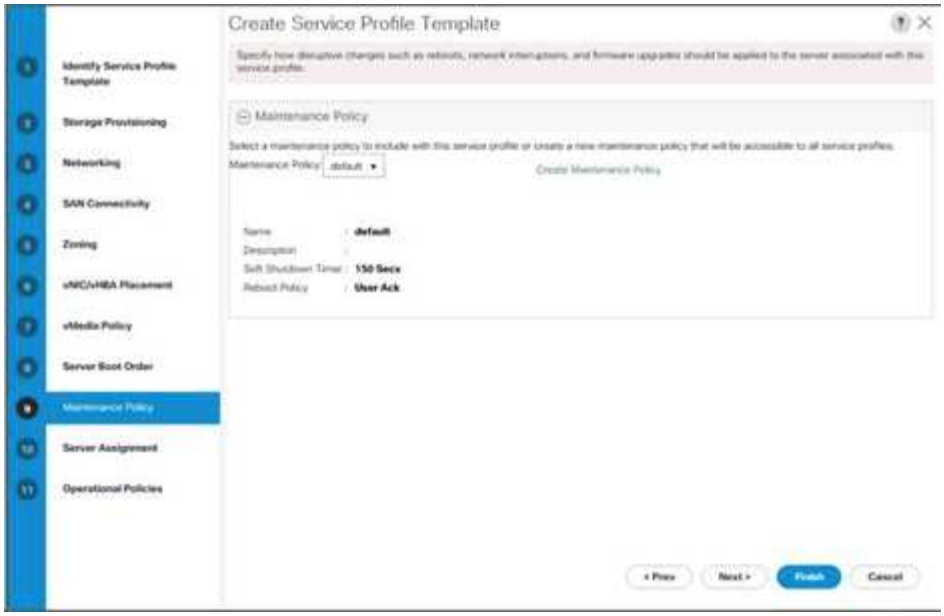


30. 다음 을 클릭합니다.

유지 관리 정책을 구성합니다

유지보수 정책을 구성하려면 다음 단계를 완료하십시오.

1. 유지보수 정책을 기본값으로 변경합니다.

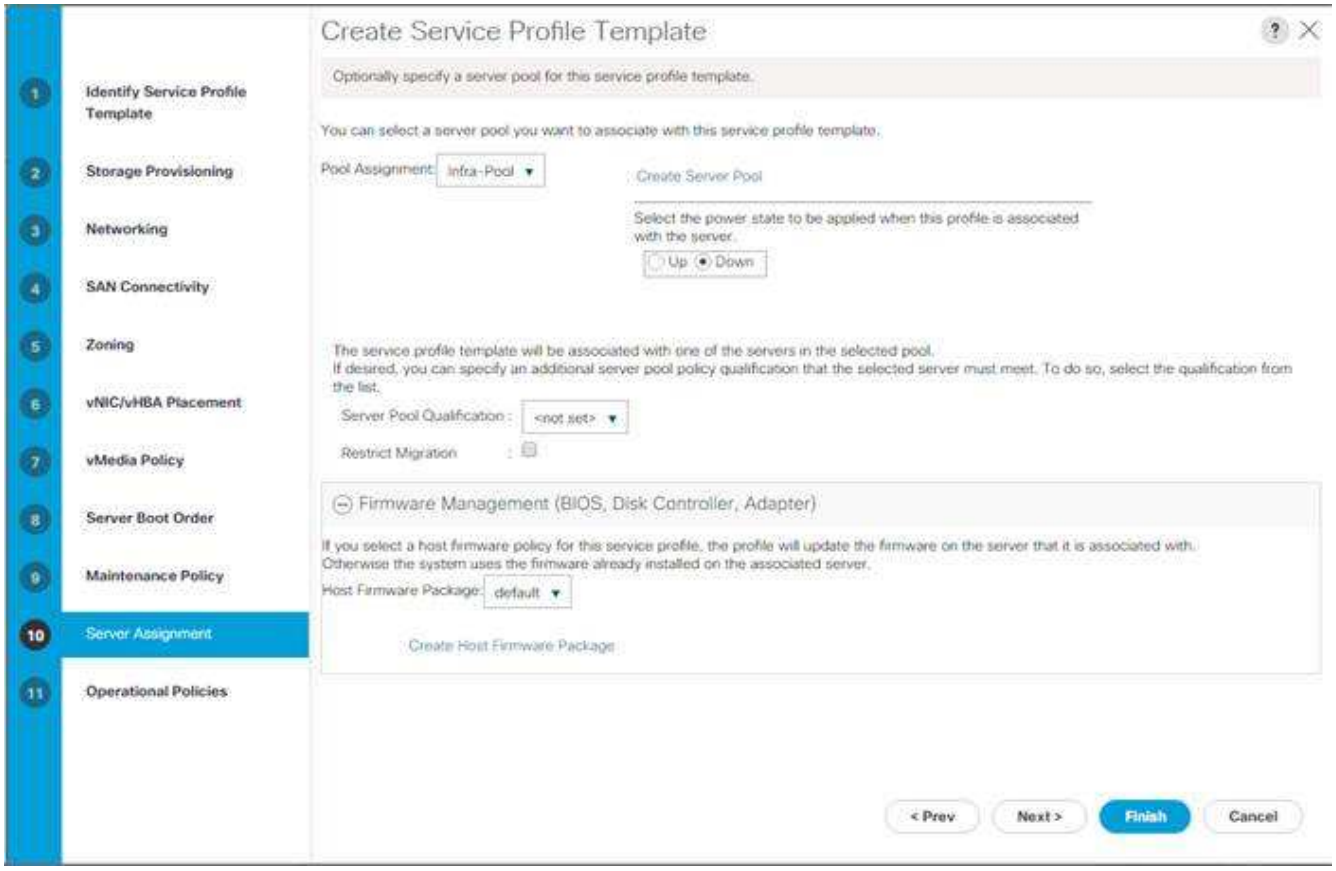


2. 다음 을 클릭합니다.

서버 할당을 구성합니다

서버 할당을 구성하려면 다음 단계를 완료하십시오.

1. 풀 할당 목록에서 Infra-Pool을 선택합니다.
2. 프로파일이 서버에 연결될 때 적용될 전원 상태로 down(끄기)을 선택합니다.
3. 페이지 하단의 펌웨어 관리 를 확장하고 기본 정책을 선택합니다.

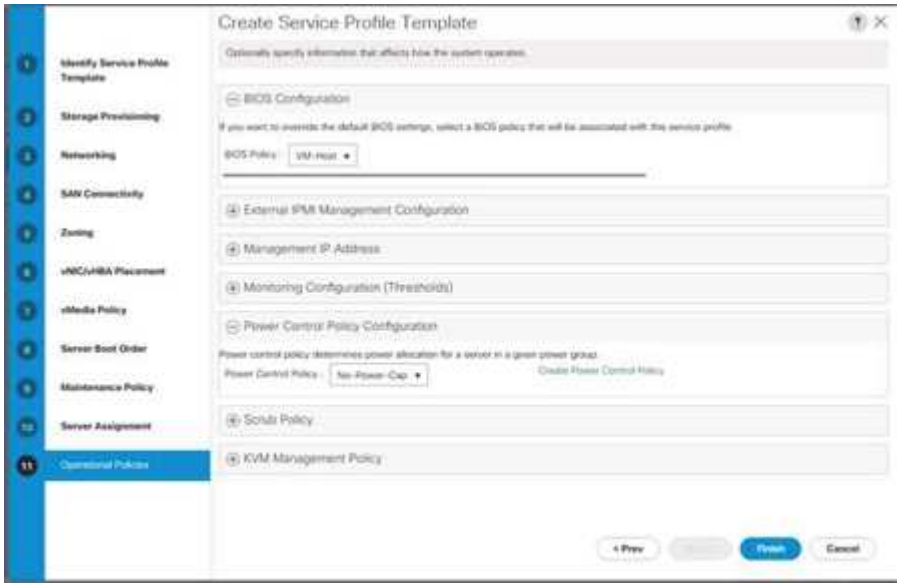


4. 다음 을 클릭합니다.

운영 정책을 구성합니다

운영 정책을 구성하려면 다음 단계를 완료하십시오.

1. BIOS 정책 드롭다운 목록에서 VM-호스트 를 선택합니다.
2. 전원 제어 정책 구성 을 확장하고 전원 제어 정책 드롭다운 목록에서 전원이 들어오지 않음(No Power-Cap) 을 선택합니다.



3. 마침 을 클릭하여 서비스 프로필 템플릿을 생성합니다.
4. 확인 메시지에서 확인 을 클릭합니다.

vMedia 지원 서비스 프로필 템플릿을 생성합니다

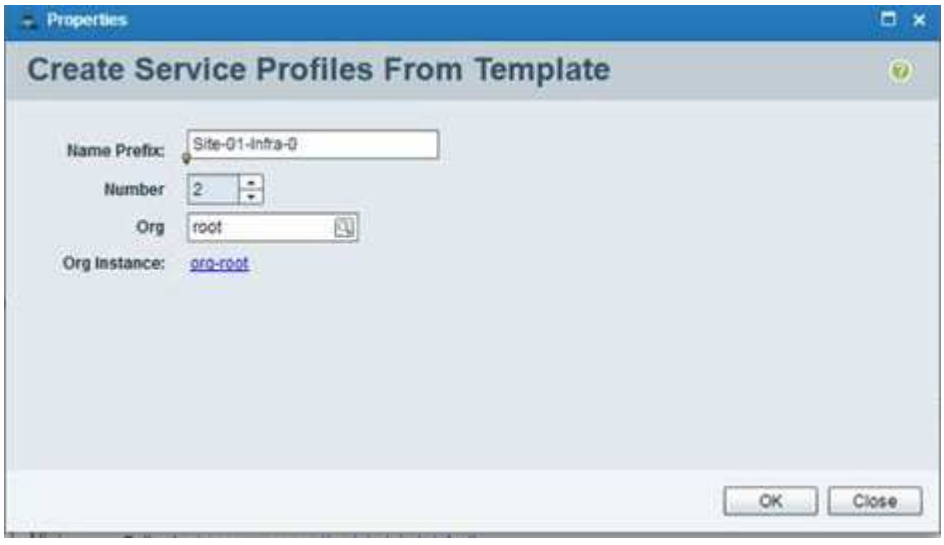
vMedia가 활성화된 서비스 프로필 템플릿을 생성하려면 다음 단계를 수행하십시오.

1. UCS Manager에 연결하고 왼쪽에서 서버 를 클릭합니다.
2. 서비스 프로필 템플릿 > 루트 > 서비스 템플릿 VM-호스트-인프라스트럭처-iSCSI-A를 선택합니다
3. VM-Host-Infra-iSCSI-A를 마우스 오른쪽 버튼으로 클릭하고 Create a Clone을 선택합니다.
4. 클론 이름을 VM-Host-Infra-iSCSI-A-VM으로 지정합니다.
5. 새로 생성된 VM-Host-Infra-iSCSI-A-VM을 선택하고 오른쪽에서 vMedia Policy 탭을 선택합니다.
6. vMedia 정책 수정을 클릭합니다.
7. ESXi-6을 선택합니다. 7U1-HTTP vMedia 정책 을 클릭하고 확인 을 클릭합니다.
8. 확인을 클릭하여 확인합니다.

서비스 프로필을 생성합니다

서비스 프로필 템플릿에서 서비스 프로필을 생성하려면 다음 단계를 수행하십시오.

1. Cisco UCS Manager에 연결하고 왼쪽에서 서버 를 클릭합니다.
2. Servers > Service Profile Templates > root > Service Template <name> 을 확장합니다.
3. 동작에서 템플릿으로부터 서비스 프로필 만들기를 클릭하고 다음 단계를 경쟁합니다.
   a. 이름 접두사로 'ite-01-infra-0'을 입력합니다.
   b. 생성할 인스턴스 수로 2를 입력합니다.
   c. ORG로 root를 선택합니다.
   d. 확인 을 클릭하여 서비스 프로필을 만듭니다.



4. 확인 메시지에서 확인 을 클릭합니다.

5. 서비스프로필 ite-01-Infra-01과 Site-01-Infra-02가 만들어졌는지 확인한다.

   서비스 프로필은 할당된 서버 풀의 서버와 자동으로 연결됩니다.

스토리지 구성 2부: 부팅 LUN 및 이니시에이터 그룹

ONTAP 부팅 저장소 설정

이니시에이터 그룹을 생성합니다

이니시에이터 그룹(igroup)을 생성하려면 다음 단계를 완료합니다.

1. 클러스터 관리 노드의 SSH 연결에서 다음 명령을 실행합니다.

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-01 –protocol
iscsi –ostype vmware –initiator <vm-host-infra-01-iqn>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-02 –protocol
iscsi –ostype vmware –initiator <vm-host-infra-02-iqn>
igroup create –vserver Infra-SVM –igroup MGMT-Hosts –protocol iscsi
–ostype vmware –initiator <vm-host-infra-01-iqn>, <vm-host-infra-02-iqn>
```

   IQN 정보에 대해서는 표 1 및 표 2에 나열된 값을 사용합니다.

2. 방금 작성한 3개 igroup을 보려면 'igroup show' 명령을 실행합니다.

부팅 LUN을 igroup에 매핑합니다

부팅 LUN을 igroup에 매핑하려면 다음 단계를 완료하십시오.

1. 스토리지 클러스터 관리 SSH 연결에서 다음 명령을 실행합니다.

```
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra- A
–igroup VM-Host-Infra-01 –lun-id 0lun map –vserver Infra-SVM –volume
esxi_boot –lun VM-Host-Infra- B –igroup VM-Host-Infra-02 –lun-id 0
```

VMware vSphere 6.7U1 구축 절차

이 섹션에서는 FlexPod Express 구성에 VMware ESXi 6.7U1을 설치하는 절차를 자세히 설명합니다. 절차가 완료된 후 부팅된 ESXi 호스트 2개가 프로비저닝됩니다.

VMware 환경에 ESXi를 설치하는 방법은 여러 가지가 있습니다. 이 절차에서는 Cisco UCS Manager에 내장된 KVM 콘솔과 가상 미디어 기능을 사용하여 원격 설치 미디어를 개별 서버에 매핑하고 부팅 LUN에 연결하는 방법에 초점을 맞춥니다.

ESXi 6.7U1용 **Cisco** 사용자 지정 이미지를 다운로드합니다

VMware ESXi 사용자 지정 이미지를 다운로드하지 않은 경우 다음 단계를 수행하여 다운로드를 완료합니다.

1. https://my.vmware.com/group/vmware/details?downloadGroup=OEM-ESXI67U1-CISCO&productId=742[VMware vSphere 하이퍼바이저(ESXi) 6.7U1.^ 링크를 클릭합니다.
2. 에 사용자 ID와 암호가 필요합니다 "VMware.com" 를 눌러 이 소프트웨어를 다운로드합니다.
3. ISO 파일을 다운로드합니다.

Cisco UCS Manager를 참조하십시오

Cisco UCS IP KVM을 사용하면 관리자가 원격 미디어를 통해 OS 설치를 시작할 수 있습니다. IP KVM을 실행하려면 Cisco UCS 환경에 로그인해야 합니다.

Cisco UCS 환경에 로그인하려면 다음 단계를 수행하십시오.

1. 웹 브라우저를 열고 Cisco UCS 클러스터 주소의 IP 주소를 입력합니다. 이 단계에서는 Cisco UCS Manager 애플리케이션을 시작합니다.
2. HTML에서 UCS Manager 실행 링크를 클릭하여 HTML 5 UCS Manager GUI를 시작합니다.
3. 보안 인증서를 수락하라는 메시지가 나타나면 필요에 따라 수락하십시오.
4. 메시지가 나타나면 사용자 이름으로 admin을 입력하고 관리자 암호를 입력합니다.
5. Cisco UCS Manager에 로그인하려면 로그인을 클릭합니다.
6. 기본 메뉴에서 왼쪽에 있는 서버 를 클릭합니다.
7. Servers > Service Profiles > root > VM-Host-Infra-01’을 선택합니다.
8. VM-Host-Infra-01을 마우스 오른쪽 버튼으로 클릭하고 KVM Console을 선택합니다.
9. 표시되는 메시지에 따라 Java 기반 KVM 콘솔을 실행합니다.
10. Servers > Service Profiles > root > VM-Host-Infra-02’를 선택합니다.
11. VM-Host-Infra-02를 마우스 오른쪽 버튼으로 클릭합니다. KVM 콘솔을 선택합니다.
12. 표시되는 메시지에 따라 Java 기반 KVM 콘솔을 실행합니다.

VMware ESXi 설치를 설정합니다

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

OS 설치를 위해 서버를 준비하려면 각 ESXi 호스트에서 다음 단계를 수행하십시오.

1. KVM 창에서 가상 미디어를 클릭합니다.
2. 가상 장치 활성화 를 클릭합니다.
3. 암호화되지 않은 KVM 세션을 수락하라는 메시지가 표시되면 필요에 따라 수락하십시오.
4. 가상 미디어 를 클릭하고 CD/DVD 매핑 을 선택합니다.
5. ESXi 설치 관리자 ISO 이미지 파일을 찾아 이동하고 Open을 클릭합니다.
6. 장치 매핑 을 클릭합니다.
7. KVM 탭을 클릭하여 서버 부팅을 모니터링합니다.

◦ ESXi * 설치

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

호스트의 iSCSI 부팅 가능 LUN에 VMware ESXi를 설치하려면 각 호스트에서 다음 단계를 수행하십시오.

1. Boot Server를 선택하고 OK를 클릭하여 서버를 부팅합니다. 그런 다음 확인을 다시 클릭합니다.
2. 재부팅 시 ESXi 설치 미디어의 존재 여부가 자동으로 감지됩니다. 표시되는 부팅 메뉴에서 ESXi 설치 프로그램을 선택합니다.
3. 설치 프로그램 로드가 완료된 후 Enter 키를 눌러 설치를 계속합니다.
4. 최종 사용자 사용권 계약(EULA)을 읽고 동의합니다. F11 키를 눌러 동의하고 계속합니다.
5. 이전에 ESXi용 설치 디스크로 설정된 LUN을 선택하고 Enter 키를 눌러 설치를 계속합니다.
6. 적절한 자판 배열을 선택하고 Enter 키를 누릅니다.
7. 루트 암호를 입력 및 확인하고 Enter 키를 누릅니다.
8. 설치 프로그램에서 선택한 디스크가 다시 분할된다는 경고를 표시합니다. F11 키를 눌러 설치를 계속합니다.
9. 설치가 완료되면 Virtual Media 탭을 선택하고 ESXi 설치 미디어 옆에 있는 P 표시를 지웁니다. 예 를 클릭합니다.



설치 프로그램이 아닌 ESXi로 서버를 재부팅하도록 ESXi 설치 이미지를 매핑 해제해야 합니다.

10. 설치가 완료되면 Enter 키를 눌러 서버를 재부팅합니다.
11. Cisco UCS Manager에서 현재 서비스 프로필을 비 vMedia 서비스 프로필 템플릿에 바인딩하여 HTTP를 통해 ESXi 설치 ISO가 마운트되지 않도록 합니다.

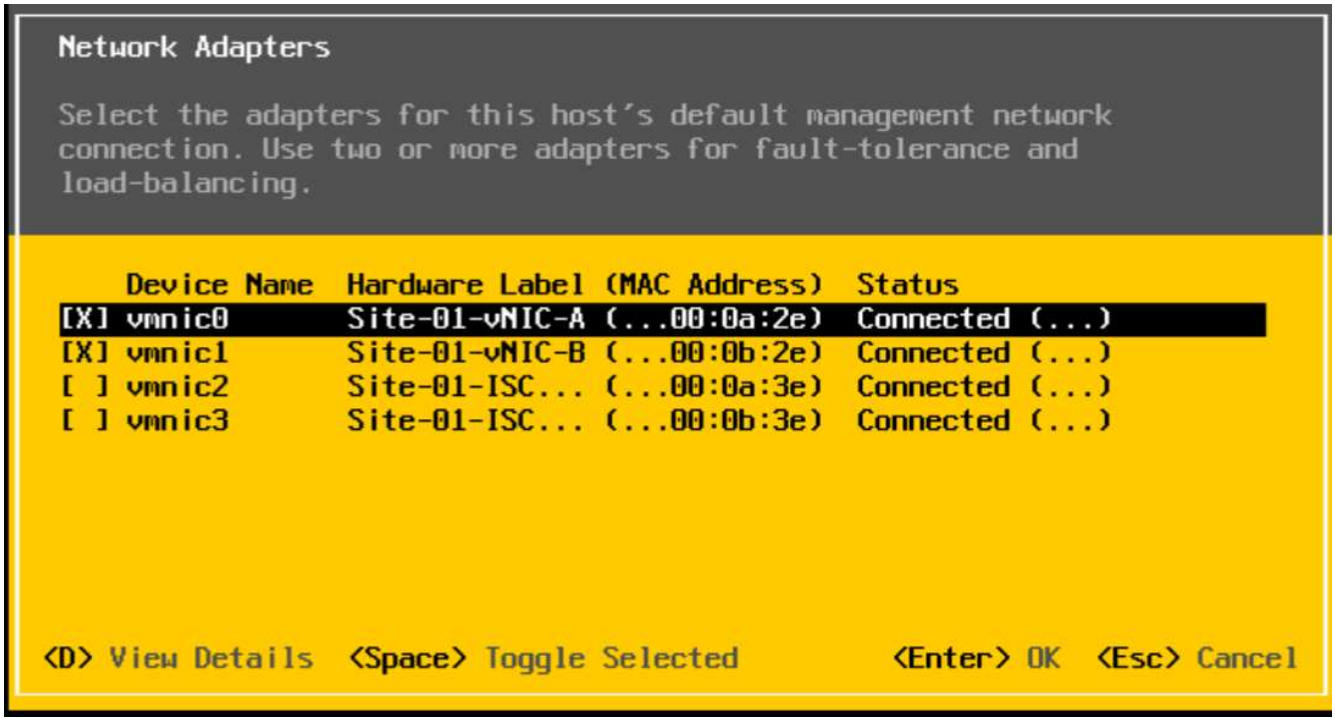
ESXi 호스트에 대한 관리 네트워킹을 설정합니다

호스트를 관리하려면 각 VMware 호스트에 대한 관리 네트워크를 추가해야 합니다. VMware 호스트에 대한 관리 네트워크를 추가하려면 각 ESXi 호스트에서 다음 단계를 수행합니다.

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

관리 네트워크에 액세스할 수 있도록 각 ESXi 호스트를 구성하려면 다음 단계를 수행하십시오.

1. 서버 재부팅이 완료된 후 F2 키를 눌러 시스템을 사용자 정의합니다.
2. root로 로그인하여 해당 비밀번호를 입력한 후 Enter를 눌러 로그인합니다.
3. 문제 해결 옵션을 선택하고 Enter 키를 누릅니다.
4. ESXi 셸 활성화 를 선택하고 Enter 키를 누릅니다.
5. SSH 활성화 를 선택하고 Enter 키를 누릅니다.
6. Esc 키를 눌러 문제 해결 옵션 메뉴를 종료합니다.
7. Configure Management Network 옵션을 선택하고 Enter 키를 누릅니다.
8. Network Adapters 를 선택하고 Enter 키를 누릅니다.
9. 하드웨어 레이블 필드의 숫자가 장치 이름 필드의 번호와 일치하는지 확인합니다.
10. Enter 키를 누릅니다.



11. VLAN (Optional) 옵션을 선택하고 Enter 키를 누릅니다.
12. '<IB-mgmt-vlan-id>'를 입력하고 Enter 키를 누릅니다.
13. IPv4 구성 을 선택하고 Enter 키를 누릅니다.
14. 스페이스바를 사용하여 정적 IPv4 주소 설정 및 네트워크 구성 옵션을 선택합니다.
15. 첫 번째 ESXi 호스트를 관리하기 위한 IP 주소를 입력합니다.
16. 첫 번째 ESXi 호스트의 서브넷 마스크를 입력합니다.
17. 첫 번째 ESXi 호스트의 기본 게이트웨이를 입력합니다.
18. Enter 키를 눌러 IP 구성의 변경 사항을 적용합니다.
19. DNS 구성 옵션을 선택하고 Enter 키를 누릅니다.

    IP 주소는 수동으로 할당되므로 DNS 정보도 수동으로 입력해야 합니다.

20. 기본 DNS 서버의 IP 주소를 입력합니다.
21. 선택 사항: 보조 DNS 서버의 IP 주소를 입력합니다.
22. 첫 번째 ESXi 호스트의 FQDN을 입력합니다.
23. Enter 키를 눌러 DNS 구성의 변경 사항을 적용합니다.
24. Esc를 눌러 Configure Management Network 메뉴를 종료합니다.
25. 관리 네트워크 테스트 를 선택하여 관리 네트워크가 올바르게 설정되어 있는지 확인하고 Enter 키를 누릅니다.
26. Enter 키를 눌러 테스트를 실행하고 테스트가 완료되면 Enter 키를 다시 누릅니다. 오류가 발생하면 환경을 검토합니다.
27. Configure Management Network를 다시 선택하고 Enter 키를 누릅니다.
28. IPv6 구성 옵션을 선택하고 Enter 키를 누릅니다.

29. 스페이스바를 사용하여 Disable IPv6 (restart required) 를 선택하고 Enter 키를 누릅니다.
30. Esc 키를 눌러 Configure Management Network 하위 메뉴를 종료합니다.
31. Y 를 눌러 변경 사항을 확인하고 ESXi 호스트를 재부팅합니다.

VMware ESXi 호스트 **VMkernel** 포트 **vmk0 MAC** 주소 재설정**(**선택 사항**)**

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

기본적으로 관리 VMkernel 포트 vmk0의 MAC 주소는 관리 VMkernel 포트가 배치된 이더넷 포트의 MAC 주소와 동일합니다. ESXi 호스트의 부팅 LUN이 다른 MAC 주소를 가진 다른 서버에 다시 매핑되면 ESXi 시스템 구성이 재설정되지 않는 한 vmk0이 할당된 MAC 주소를 유지하므로 MAC 주소 충돌이 발생합니다. vmk0의 MAC 주소를 임의의 VMware 할당 MAC 주소로 재설정하려면 다음 단계를 수행하십시오.

1. ESXi 콘솔 메뉴 기본 화면에서 Ctrl-Alt-F1을 눌러 VMware 콘솔 명령줄 인터페이스에 액세스합니다. UCSM KVM에서 Ctrl-Alt-F1이 정적 매크로 목록에 나타납니다.
2. 루트로 로그인합니다.
3. 인터페이스 vmk0의 세부 목록을 보려면 esxcfg-vmknic –l을 입력하십시오. vmk0은 Management Network 포트 그룹에 속해야 합니다. vmk0의 IP 주소와 넷마스크를 기록해 둡니다.
4. vmk0을 제거하려면 다음 명령을 입력합니다.

```
esxcfg-vmknic –d “Management Network”
```

5. 임의의 MAC 주소를 사용하여 vmk0을 다시 추가하려면 다음 명령을 입력합니다.

```
esxcfg-vmknic –a –i <vmk0-ip> -n <vmk0-netmask> “Management Network””.
```

6. 임의의 MAC 주소를 사용하여 vmk0이 다시 추가되었는지 확인합니다

```
esxcfg-vmknic –l
```

7. 명령줄 인터페이스에서 로그아웃하려면 "exit"를 입력합니다.
8. Ctrl-Alt-F2를 눌러 ESXi 콘솔 메뉴 인터페이스로 돌아갑니다.

VMware 호스트 클라이언트를 사용하여 **VMware ESXi** 호스트에 로그인합니다

ESXi 호스트 VM-Host-Infra-01

VMware 호스트 클라이언트를 사용하여 VM-Host-Infra-01 ESXi 호스트에 로그인하려면 다음 단계를 수행하십시오.

1. 관리 워크스테이션에서 웹 브라우저를 열고 VM-Host-Infra-01 관리 IP 주소로 이동합니다.
2. VMware 호스트 클라이언트 열기 를 클릭합니다.
3. 사용자 이름으로 root를 입력합니다.

4. 루트 암호를 입력합니다.
5. Login을 클릭하여 연결합니다.
6. 이 과정을 반복하여 별도의 브라우저 탭이나 창에서 VM-Host-Infra-02에 로그인합니다.

VIC(Cisco Virtual Interface Card)용 VMware 드라이버 설치

다음 VMware VIC 드라이버에 대한 오프라인 번들을 다운로드하여 관리 워크스테이션에 압축을 풉니다.

- nenic 드라이버 버전 1.0.25.0

ESXi는 VM-Host-Infra-01 및 VM-Host-Infra-02를 호스팅합니다

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02에 VMware VIC 드라이버를 설치하려면 다음 단계를 수행하십시오.

1. 각 호스트 클라이언트에서 스토리지를 선택합니다.
2. datastore1을 마우스 오른쪽 단추로 클릭하고 찾아보기 를 선택합니다.
3. 데이터 저장소 브라우저에서 업로드 를 클릭합니다.
4. 다운로드한 VIC 드라이버의 저장된 위치로 이동하고 VMW-ESX-6.7.0-nenic-1.0.25.0-offline_bundle-11271332.zip을 선택합니다.
5. 데이터 저장소 브라우저에서 업로드 를 클릭합니다.
6. 열기 를 클릭하여 파일을 datastore1에 업로드합니다.
7. 파일이 두 ESXi 호스트에 모두 업로드되었는지 확인합니다.
8. 각 호스트를 유지 관리 모드로 전환합니다(아직 없는 경우).
9. 셸 연결 또는 putty 터미널에서 ssh를 통해 각 ESXi 호스트에 연결합니다.
10. 루트 암호를 사용하여 루트로 로그인합니다.
11. 각 호스트에서 다음 명령을 실행합니다.

```
esxcli software vib update -d /vmfs/volumes/datastore1/VMW-ESX-6.7.0-
nenic-1.0.25.0-offline_bundle-11271332.zip
reboot
```

12. 재부팅이 완료되면 각 호스트의 호스트 클라이언트에 로그인하고 유지 관리 모드를 종료합니다.

VMkernel 포트 및 가상 스위치를 설정합니다

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

ESXi 호스트에서 VMkernel 포트 및 가상 스위치를 설정하려면 다음 단계를 수행하십시오.

1. 호스트 클라이언트 의 왼쪽에서 네트워킹 을 선택합니다.
2. 가운데 창에서 가상 스위치 탭을 선택합니다.
3. vSwitch0을 선택합니다.

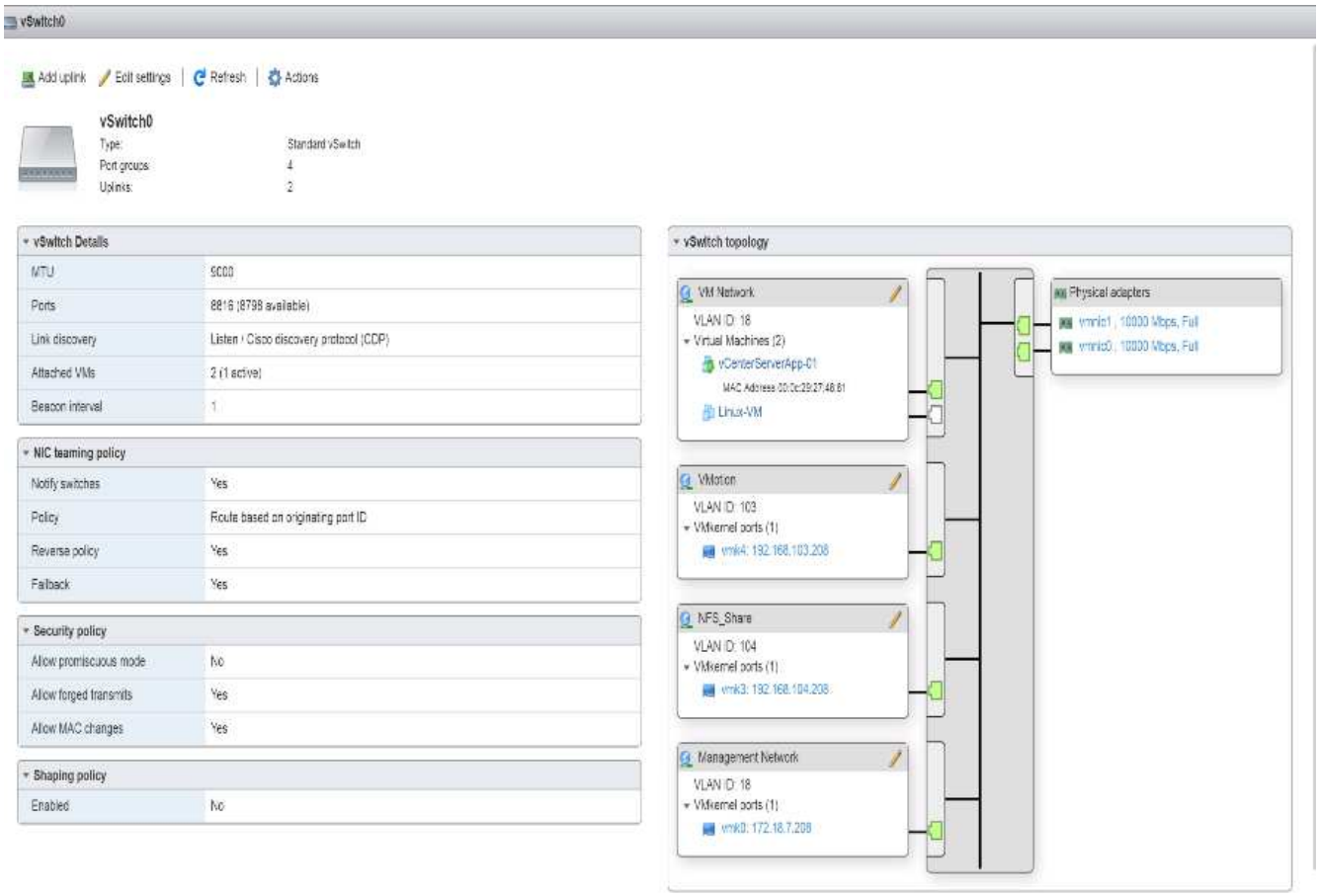
4. 설정 편집 을 선택합니다.
5. MTU를 9000으로 변경합니다.
6. NIC 팀 구성을 확장합니다.
7. 페일오버 순서 섹션에서 vmnic1을 선택하고 활성 상태로 표시를 클릭합니다.
8. vmnic1의 상태가 활성인지 확인합니다.
9. 저장 을 클릭합니다.
10. 왼쪽에서 네트워킹 을 선택합니다.
11. 가운데 창에서 가상 스위치 탭을 선택합니다.
12. iSciBootvSwitch 를 선택합니다.
13. 설정 편집 을 선택합니다.
14. MTU를 9000으로 변경합니다
15. 저장 을 클릭합니다.
16. VMkernel NIC 탭을 선택합니다.
17. vmk1 iSciBootPG 를 선택합니다.
18. 설정 편집 을 선택합니다.
19. MTU를 9000으로 변경합니다.
20. IPv4 설정을 확장하고 IP 주소를 UCS iSCSI-IP-Pool-A 외부의 주소로 변경합니다

> Cisco UCS iSCSI IP 풀 주소를 재할당해야 하는 경우 IP 주소 충돌을 방지하려면 iSCSI VMkernel 포트에 대해 동일한 서브넷에 있는 다른 IP 주소를 사용하는 것이 좋습니다.

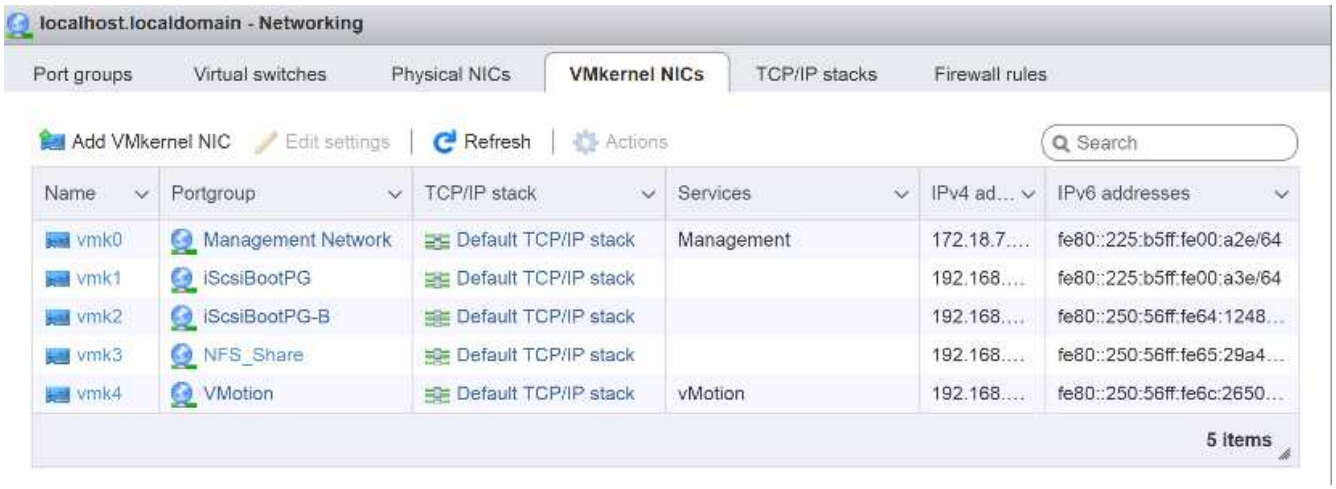
21. 저장 을 클릭합니다.
22. 가상 스위치 탭을 선택합니다.
23. Add standard virtual 스위치를 선택합니다.
24. vSwitch Name에 대한 iSciSciBootvSwitch-B의 이름을 입력합니다.
25. MTU를 9000으로 설정합니다.
26. 업링크 1 드롭다운 메뉴에서 vmnic3 을 선택합니다.
27. 추가 를 클릭합니다.
28. 가운데 창에서 VMkernel NIC 탭을 선택합니다.
29. Add VMkernel NIC 를 선택합니다
30. iSciBootPG-B의 새 포트 그룹 이름을 지정합니다
31. 가상 스위치용 iSciSciBootvSwitch-B를 선택합니다.
32. MTU를 9000으로 설정합니다. VLAN ID를 입력하지 마십시오.
33. IPv4 설정에 대해 정적 을 선택하고 옵션을 확장하여 구성 내에서 주소 및 서브넷 마스크를 제공합니다.

IP 주소 충돌을 피하기 위해 Cisco UCS iSCSI IP 풀 주소를 재할당해야 하는 경우 iSCSI VMkernel 포트에 대해 동일한 서브넷에 있는 다른 IP 주소를 사용하는 것이 좋습니다.

34. 생성 을 클릭합니다.
35. 왼쪽에서 네트워킹 을 선택한 다음 포트 그룹 탭을 선택합니다.
36. 가운데 창에서 VM Network를 마우스 오른쪽 버튼으로 클릭하고 Remove를 선택합니다.
37. 제거를 클릭하여 포트 그룹 제거를 완료합니다.
38. 가운데 창에서 포트 그룹 추가를 선택합니다.
39. 포트 그룹 관리 네트워크의 이름을 지정하고 VLAN ID 필드에 '<IB-mgmt-vlan-id>'를 입력한 다음 가상 스위치 vSwitch0이 선택되어 있는지 확인합니다.
40. 추가 를 클릭하여 IB-MGMT Network에 대한 편집을 마칩니다.
41. 맨 위에서 VMkernel NIC 탭을 선택합니다.
42. Add VMkernel NIC를 클릭합니다.
43. 새 포트 그룹의 경우 VMotion을 입력합니다.
44. 가상 스위치의 경우 vSwitch0 선택됨 을 선택합니다.
45. VLAN ID에 '<vMotion-vlan-id>'를 입력합니다.
46. MTU를 9000으로 변경합니다.
47. 정적 IPv4 설정을 선택하고 IPv4 설정을 확장합니다.
48. ESXi 호스트 vMotion IP 주소와 넷마스크를 입력합니다.
49. vMotion 스택 TCP/IP 스택을 선택합니다.
50. Services 아래에서 vMotion을 선택합니다.
51. 생성 을 클릭합니다.
52. Add VMkernel NIC를 클릭합니다.
53. 새 포트 그룹에 NFS_Share를 입력합니다.
54. 가상 스위치의 경우 vSwitch0 선택됨 을 선택합니다.
55. VLAN ID에 '<infra-nfs-vlan-id>'를 입력합니다
56. MTU를 9000으로 변경합니다.
57. 정적 IPv4 설정을 선택하고 IPv4 설정을 확장합니다.
58. ESXi 호스트 인프라스트럭처 NFS IP 주소와 넷마스크를 입력합니다.
59. 서비스를 선택하지 마십시오.
60. 생성 을 클릭합니다.
61. 가상 스위치 탭을 선택한 다음 vSwitch0을 선택합니다. vSwitch0 VMkernel NIC의 속성은 다음 예와 유사해야 합니다.



62. VMkernel NIC 탭을 선택하여 구성된 가상 어댑터를 확인합니다. 나열된 어댑터는 다음 예와 비슷해야 합니다.



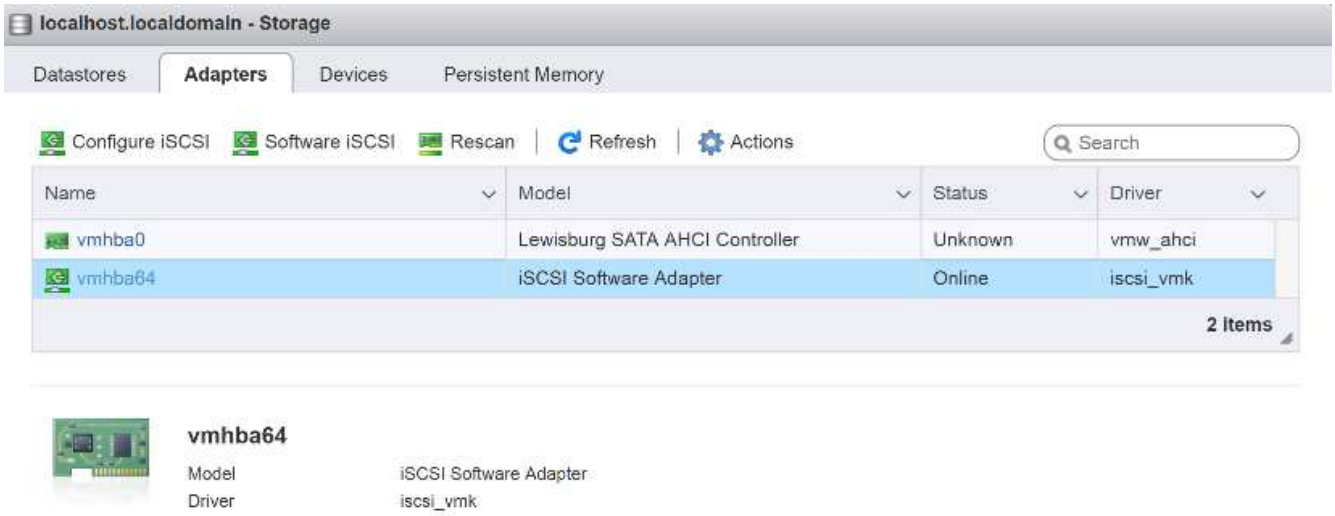
iSCSI 다중 경로를 설정합니다

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

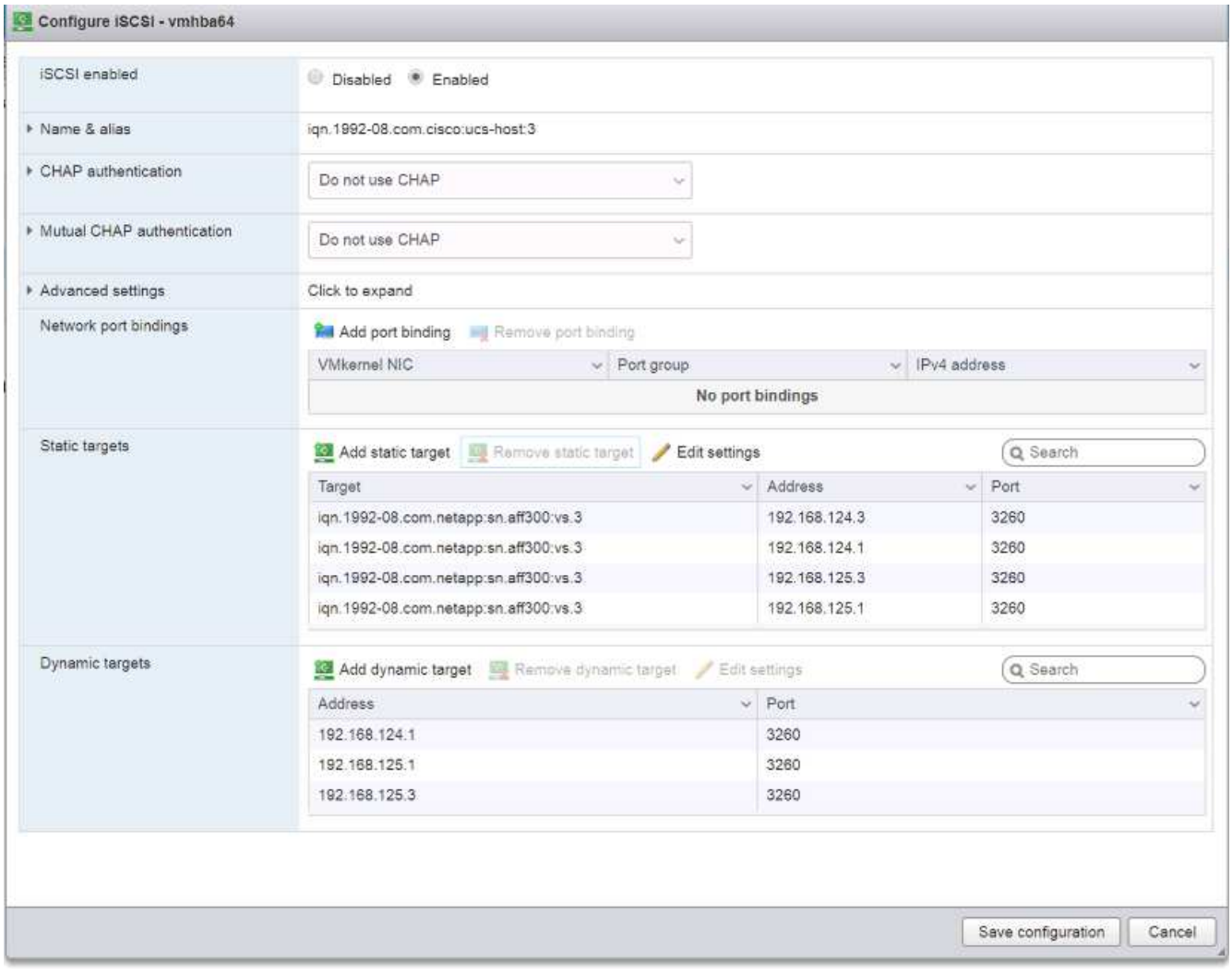
ESXi 호스트에서 iSCSI 다중 경로를 설정하려면 VM-Host-Infra-01 및 VM-Host-Infra-02를 수행하고 다음 단계를 수행하십시오.

1. 각 호스트 클라이언트에서 왼쪽의 Storage 를 선택합니다.

2. 가운데 창에서 어댑터를 클릭합니다.
3. iSCSI 소프트웨어 어댑터를 선택하고 iSCSI 구성 을 클릭합니다.



4. 동적 대상 아래에서 동적 대상 추가를 클릭합니다.
5. ISCSI_liff 01a IP Address를 입력한다.
6. iSCSI_liff 01b, iSCSI_liff 02a, iSCSI_liff 02b 등의 IP 주소를 다시 입력합니다.
7. 구성 저장 을 클릭합니다.



모든 "iscsi_lif" IP 주소를 얻으려면 NetApp 스토리지 클러스터 관리 인터페이스에 로그인하고 "network interface show" 명령을 실행하십시오.

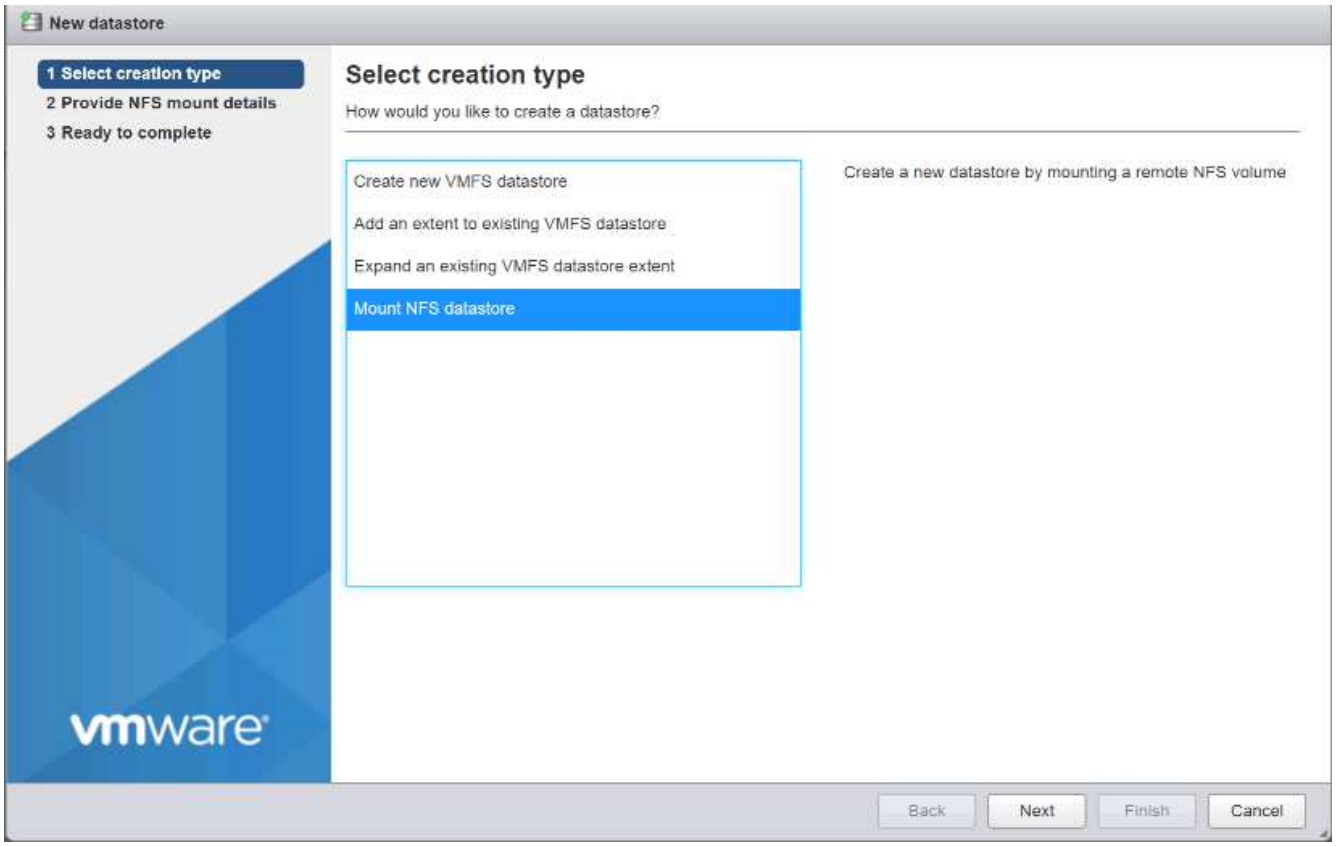
호스트가 스토리지 어댑터를 자동으로 다시 검사하며 대상은 정적 대상에 추가됩니다.

필수 데이터 저장소를 마운트합니다

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

필요한 데이터 저장소를 마운트하려면 각 ESXi 호스트에서 다음 단계를 수행합니다.

1. 호스트 클라이언트 에서 왼쪽에 있는 스토리지 를 선택합니다.
2. 가운데 창에서 데이터 저장소 를 선택합니다.
3. 가운데 창에서 새 데이터 저장소 를 선택하여 새 데이터 저장소를 추가합니다.
4. 새 데이터 저장소 대화 상자에서 NFS 데이터 저장소 마운트 를 선택하고 다음 을 클릭합니다.



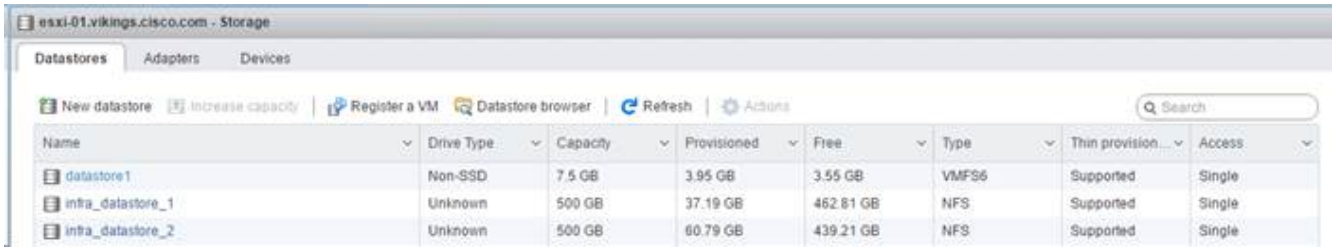
5. NFS 마운트 세부 정보 제공 페이지에서 다음 단계를 완료합니다.
   a. 데이터 저장소 이름에 'infra_datastore_1'을 입력합니다.
   b. NFS 서버에 대한 NFS_liff 01_a LIF의 IP 주소를 입력합니다.
   c. NFS 공유에 대해 '/infra_datastore_1'을 입력합니다.
   d. NFS 버전은 NFS 3으로 설정된 상태로 둡니다.
   e. 다음 을 클릭합니다.



6. 마침 을 클릭합니다. 이제 데이터 저장소가 데이터 저장소 목록에 표시됩니다.
7. 가운데 창에서 새 데이터 저장소 를 선택하여 새 데이터 저장소를 추가합니다.
8. New Datastore 대화 상자에서 Mount NFS Datastore를 선택하고 Next를 클릭합니다.
9. NFS 마운트 세부 정보 제공 페이지에서 다음 단계를 완료합니다.

a. 데이터 저장소 이름에 infra_datastore_2 를 입력합니다.
b. NFS 서버에 대한 NFS_liff 02_a LIF의 IP 주소를 입력합니다.
c. NFS 공유에 대해 '/infra_datastore_2'를 입력합니다.
d. NFS 버전은 NFS 3으로 설정된 상태로 둡니다.
e. 다음 을 클릭합니다.

10. 마침 을 클릭합니다. 이제 데이터 저장소가 데이터 저장소 목록에 표시됩니다.



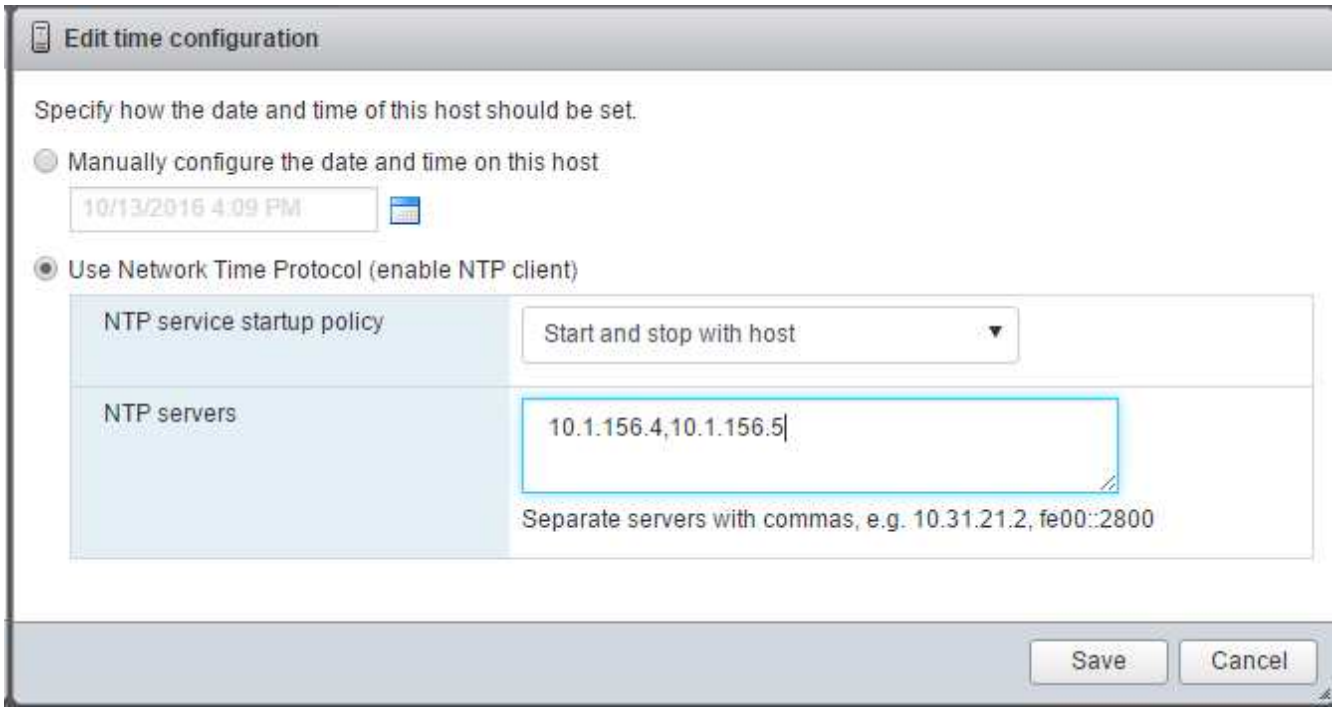
11. 두 ESXi 호스트에 두 데이터 저장소를 모두 마운트합니다.

ESXi 호스트에서 **NTP**를 구성합니다

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

ESXi 호스트에서 NTP를 구성하려면 각 호스트에서 다음 단계를 수행합니다.

1. Host Client의 왼쪽에 있는 Manage를 선택합니다.
2. 가운데 창에서 시간 및 날짜 탭을 선택합니다.
3. 설정 편집 을 클릭합니다.
4. Use Network Time Protocol (enable NTP client)(네트워크 시간 프로토콜 사용(NTP 클라이언트 활성화)) 이 선택되어 있는지 확인합니다.
5. 드롭다운 메뉴를 사용하여 Start and Stop with Host 를 선택합니다.
6. NTP 서버 상자에 두 개의 Nexus 스위치 NTP 주소를 쉼표로 구분하여 입력합니다.



7. 저장 을 클릭하여 구성 변경 사항을 저장합니다.
8. Actions > NTP Service > Start 를 선택합니다.
9. 이제 NTP 서비스가 실행되고 있으며 시계가 대략 올바른 시간으로 설정되어 있는지 확인합니다

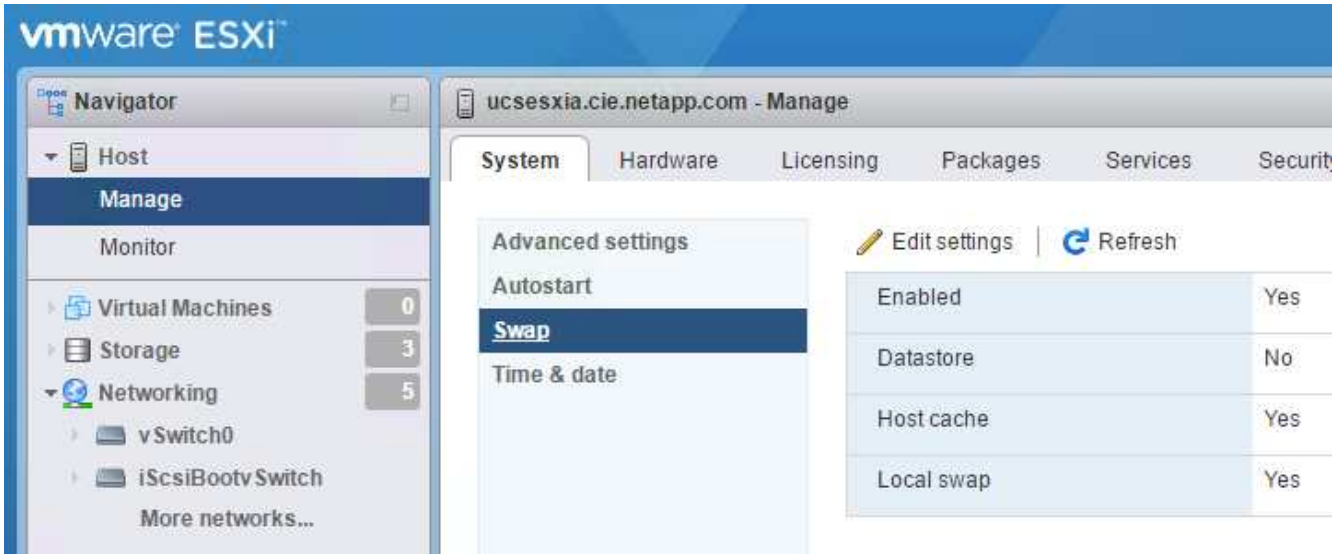
NTP 서버 시간은 호스트 시간과 약간 다를 수 있습니다.

ESXi 호스트 스왑을 구성합니다

ESXi 호스트 VM-Host-Infra-01 및 VM-Host-Infra-02

ESXi 호스트에서 호스트 스왑을 구성하려면 각 호스트에서 다음 단계를 수행합니다.

1. 왼쪽 탐색 창에서 관리 를 클릭합니다. 오른쪽 창에서 System을 선택하고 Swap을 클릭합니다.



2. 설정 편집 을 클릭합니다. Datastore 옵션에서 infra_swap을 선택합니다.



3. 저장 을 클릭합니다.

VMware VAAI용 NetApp NFS 플러그인 1.1.2를 설치합니다

NetApp NFS 플러그인 1을 설치합니다. 1.2 VMware VAAI의 경우 다음 단계를 완료합니다.

1. NetApp NFS Plug-in for VMware VAAI 다운로드:
   a. 로 이동합니다 "NetApp 소프트웨어 다운로드 페이지".
   b. 아래로 스크롤하여 VMware VAAI용 NetApp NFS 플러그인 을 클릭합니다.
   c. ESXi 플랫폼을 선택합니다.
   d. 최신 플러그인의 오프라인 번들(.zip) 또는 온라인 번들(.vib)을 다운로드합니다.
2. VMware VAAI용 NetApp NFS 플러그인은 ONTAP 9.5에서 IMT 자격 평가를 보류 중이며, 상호 운용성 세부 정보가 곧 NetApp IMT에 게시될 예정입니다.
3. ESX CLI를 사용하여 ESXi 호스트에 플러그인을 설치합니다.
4. ESXi 호스트를 재부팅합니다.

VMware vCenter Server 6.7을 설치합니다

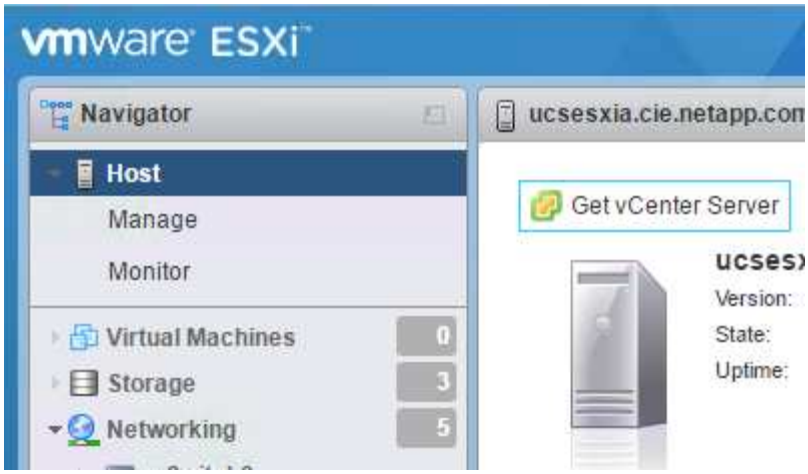
이 섹션에서는 FlexPod Express 구성에 VMware vCenter Server 6.7을 설치하는 절차를 자세히 설명합니다.

FlexPod Express는 VCSA(VMware vCenter Server Appliance)를 사용합니다.

VMware vCenter Server 어플라이언스를 설치합니다

VCSA를 설치하려면 다음 단계를 완료하십시오.

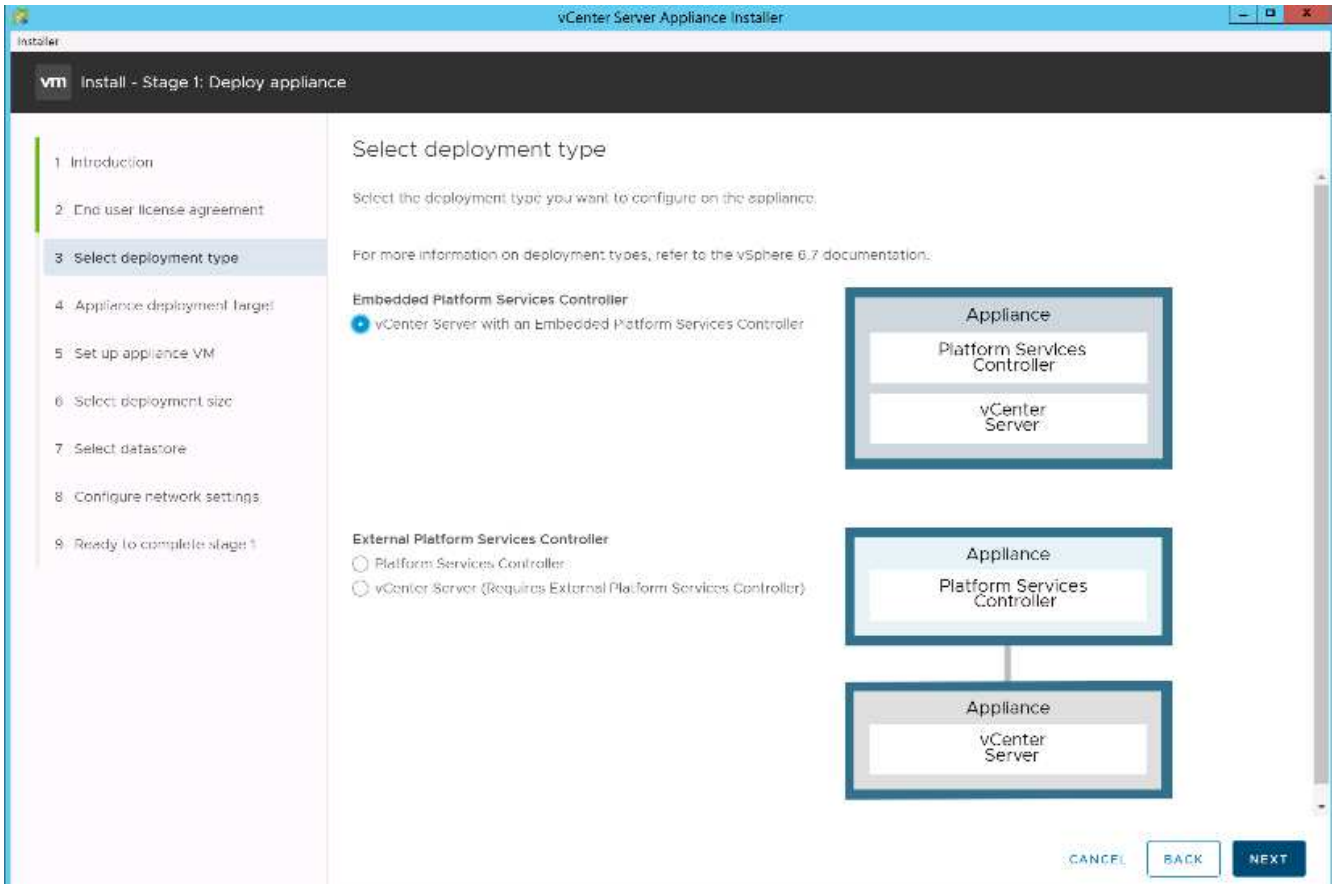
1. VCSA를 다운로드합니다. ESXi 호스트를 관리할 때 vCenter Server 가져오기 아이콘을 클릭하여 다운로드 링크를 액세스합니다.



2. VMware 사이트에서 VCSA를 다운로드합니다.

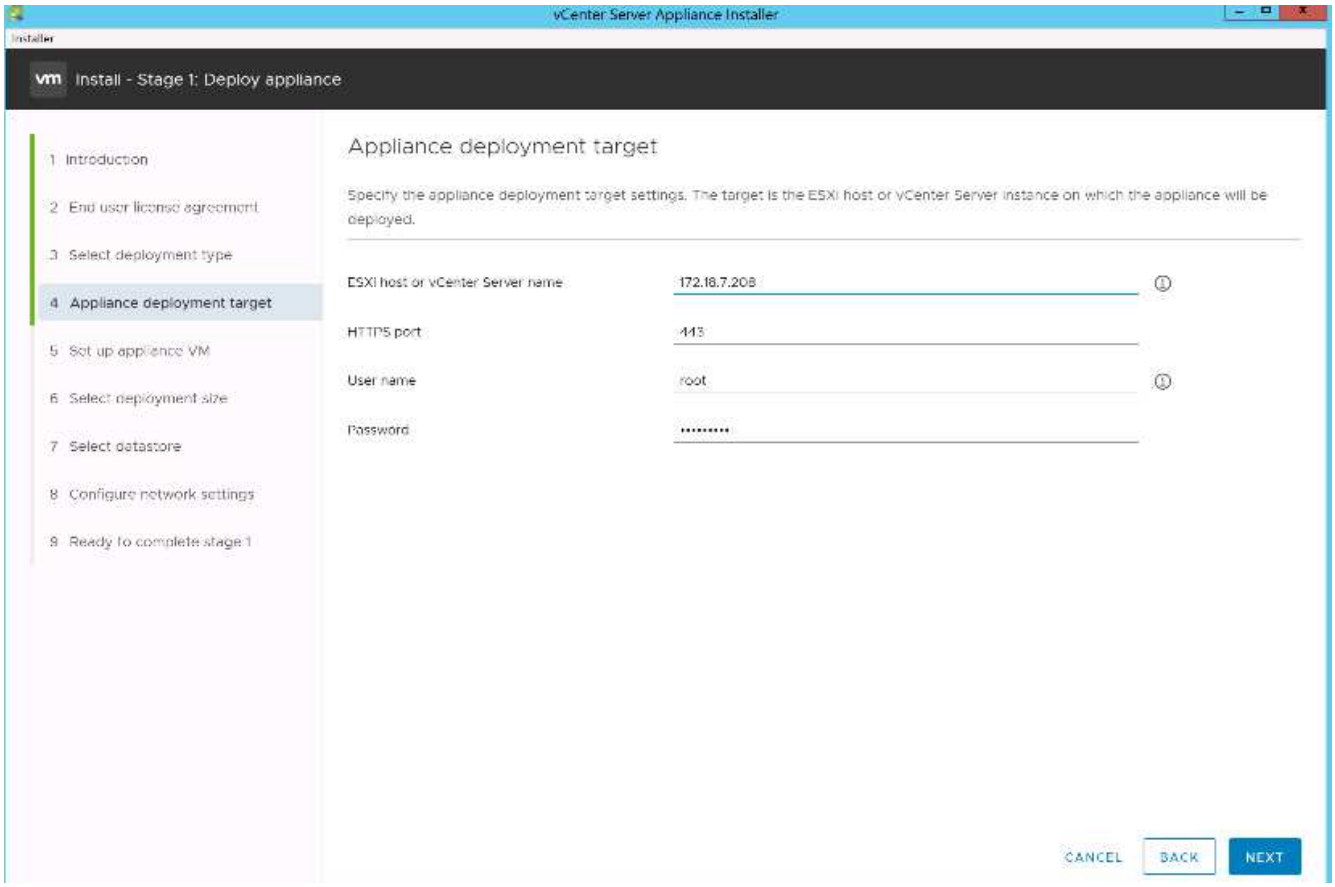
> Microsoft Windows vCenter Server 설치 가능한 가 지원되지만 VMware는 새로운 구축에 VCSA를 권장합니다.

3. ISO 이미지를 마운트합니다.
4. vcsa-UI-installer>'Win32' 디렉토리로 이동합니다. installer.exe를 두 번 클릭합니다.
5. 설치 를 클릭합니다.
6. 소개 페이지에서 다음 을 클릭합니다.
7. EULA에 동의합니다.
8. 배포 유형으로 임베디드 플랫폼 서비스 컨트롤러 를 선택합니다.

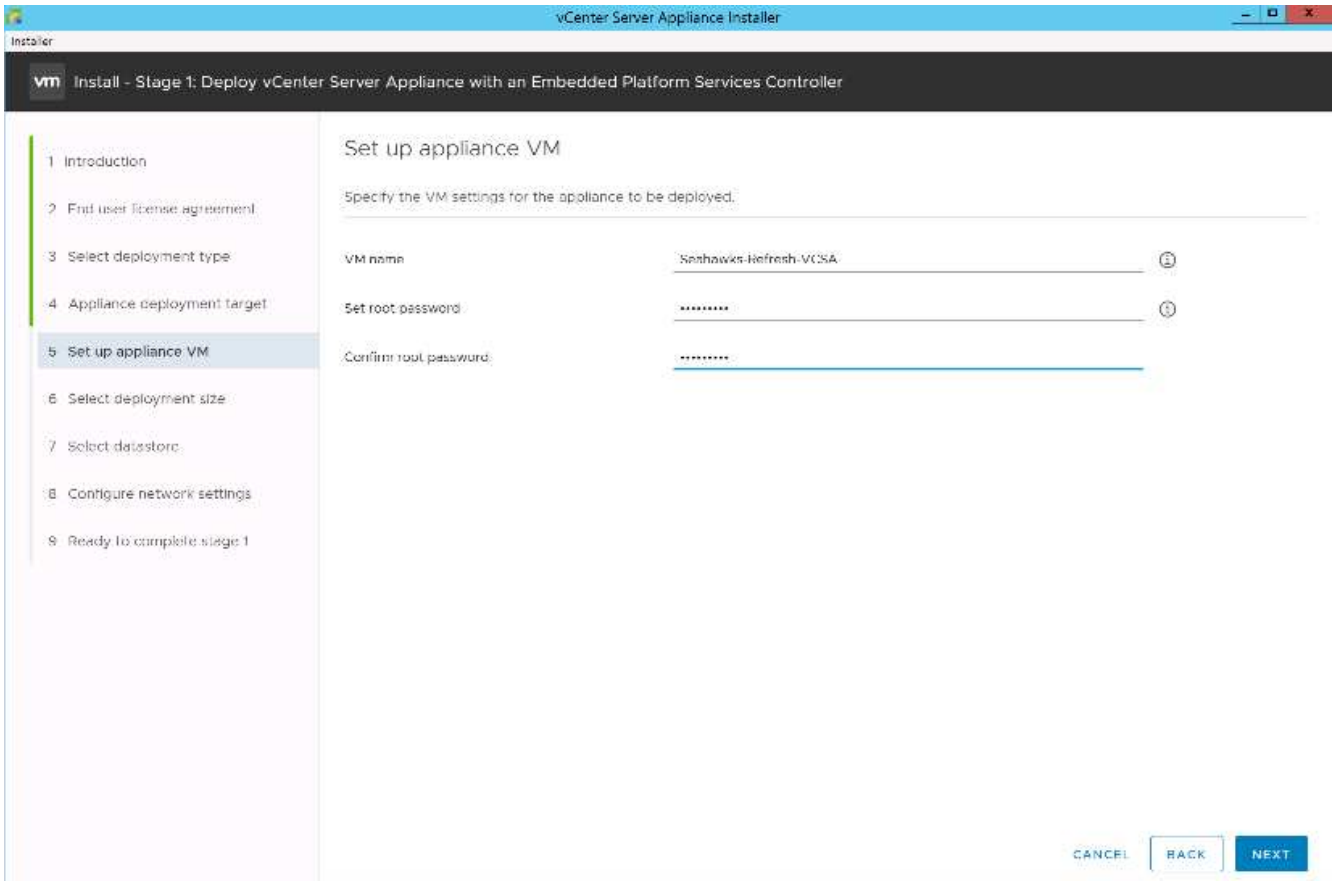


필요한 경우 외부 플랫폼 서비스 컨트롤러 배포도 FlexPod Express 솔루션의 일부로 지원됩니다.

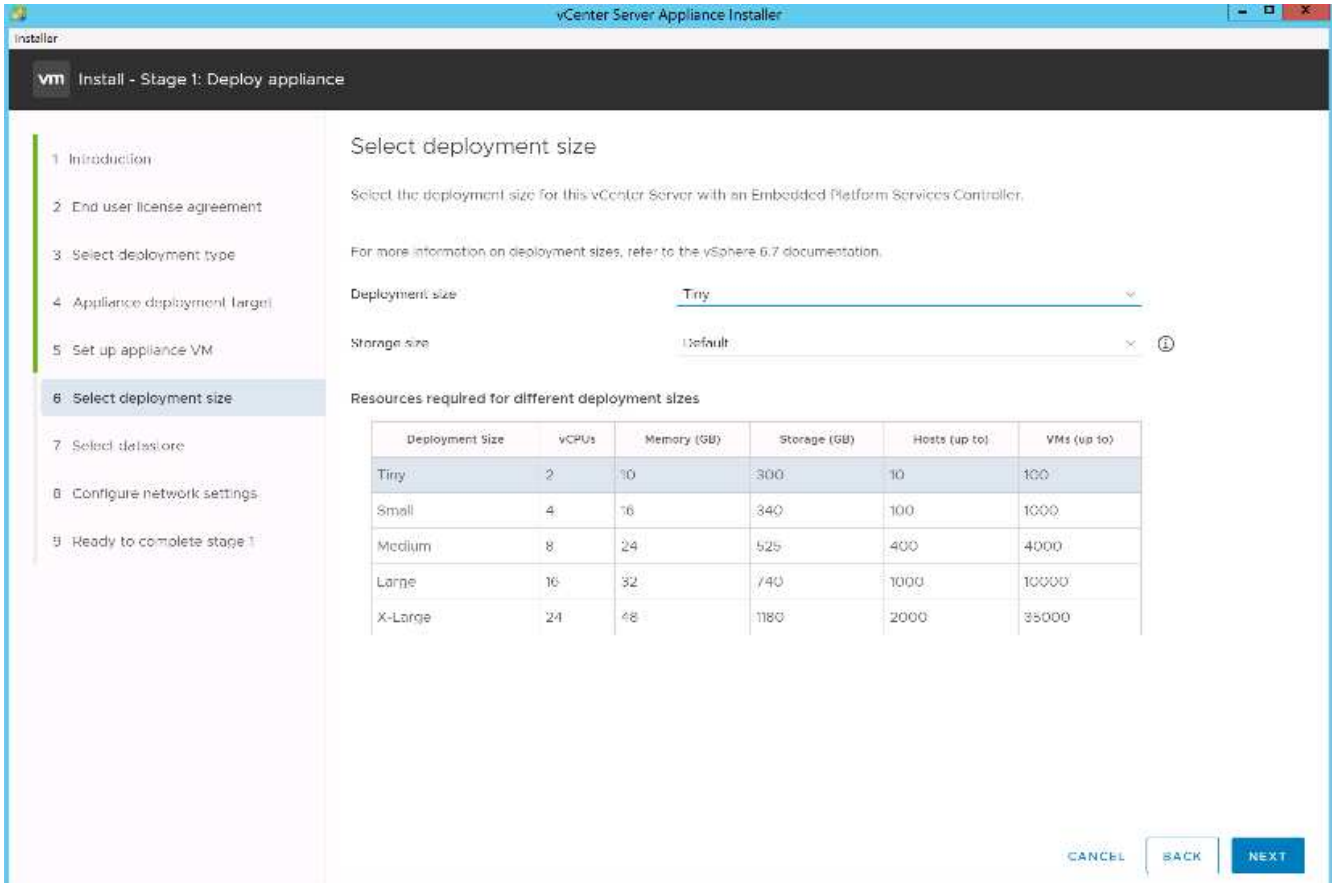
9. 어플라이언스 배포 대상 페이지에서 배포한 ESXi 호스트의 IP 주소, 루트 사용자 이름 및 루트 암호를 입력합니다. 다음 을 클릭합니다.



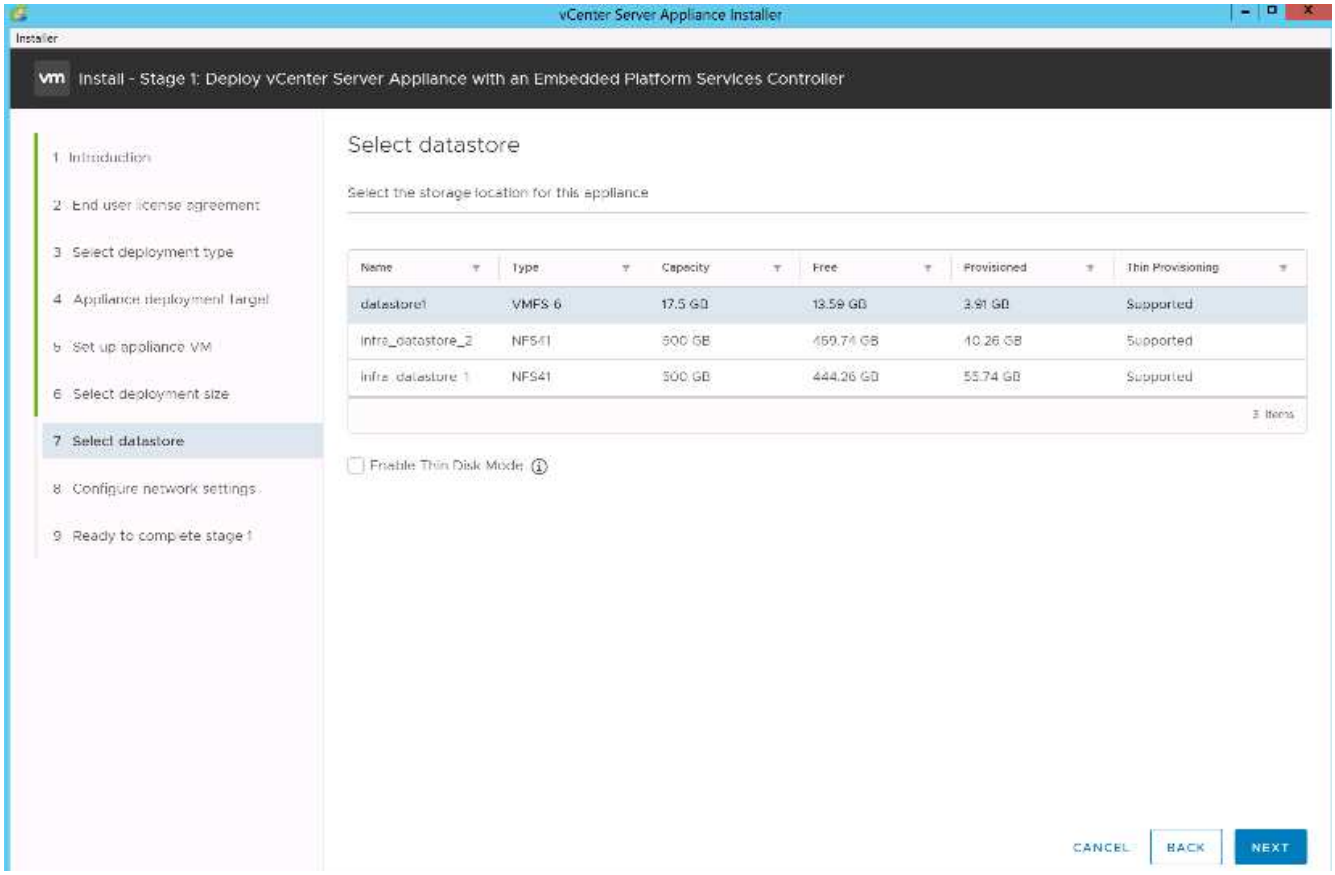
10. VCSA를 VM 이름으로 입력하고 VCSA에 사용할 루트 암호를 입력하여 어플라이언스 VM을 설정합니다. 다음 을 클릭합니다.



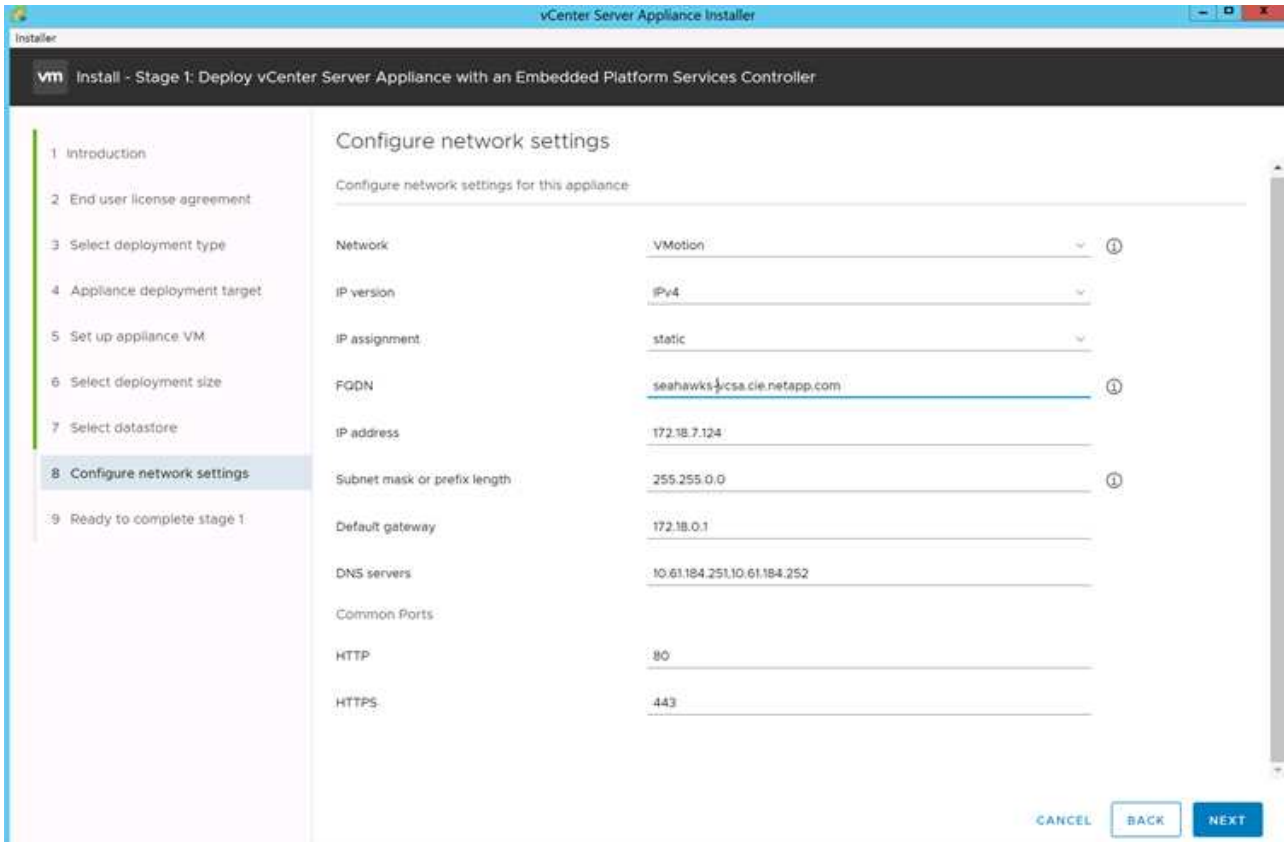
11. 환경에 가장 적합한 구축 크기를 선택합니다. 다음 을 클릭합니다.



12. 'infra_datastore_1' 데이터 저장소를 선택합니다. 다음 을 클릭합니다.



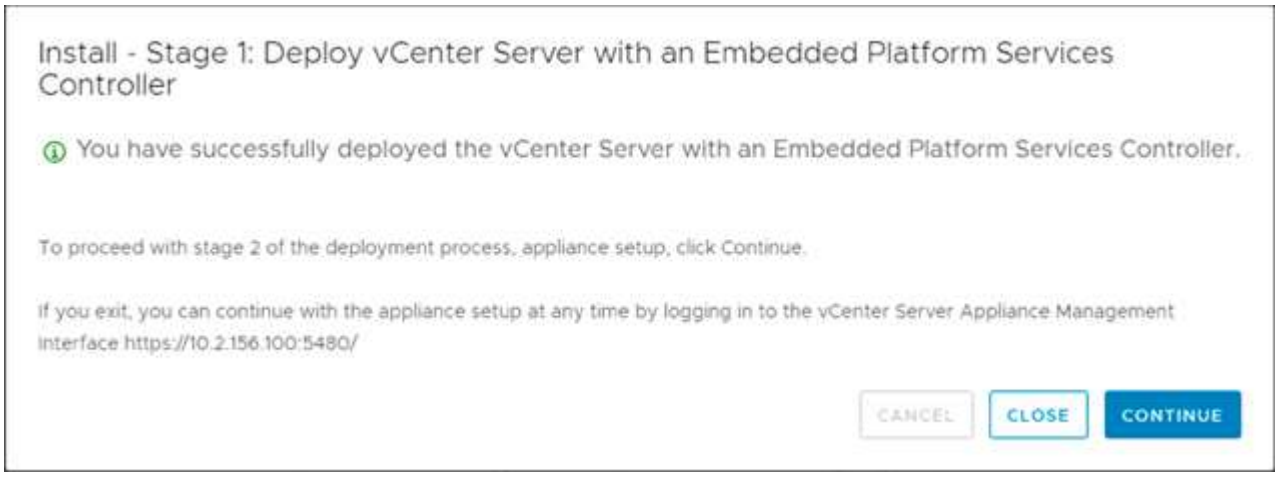
13. 네트워크 설정 구성 페이지에서 다음 정보를 입력하고 다음 을 클릭합니다.
    a. MGMT-Network를 네트워크로 선택합니다.
    b. VCSA에 사용할 FQDN 또는 IP를 입력합니다.
    c. 사용할 IP 주소를 입력합니다.
    d. 사용할 서브넷 마스크를 입력합니다.
    e. 기본 게이트웨이를 입력합니다.
    f. DNS 서버를 입력합니다.



14. 1단계 완료 준비 페이지에서 입력한 설정이 올바른지 확인합니다. 마침 을 클릭합니다.

    VCSA가 지금 설치됩니다. 이 과정은 몇 분 정도 소요됩니다.

15. 1단계가 완료되면 완료되었다는 메시지가 나타납니다. 계속 을 클릭하여 2단계 구성을 시작합니다.



16. 2단계 소개 페이지에서 다음 을 클릭합니다.
17. NTP 서버 주소에 대해 '<<var_ntp_id>>'를 입력합니다. 여러 NTP IP 주소를 입력할 수 있습니다.

    vCenter Server 고가용성을 사용하려는 경우 SSH 액세스가 설정되어 있는지 확인합니다.

18. SSO 도메인 이름, 암호 및 사이트 이름을 구성합니다. 다음 을 클릭합니다.

특히 "vsphere.local" 도메인 이름을 벗어나는 경우 이러한 값을 참조로 기록합니다.

19. 원하는 경우 VMware 고객 경험 프로그램에 참여하십시오. 다음 을 클릭합니다.
20. 설정 요약을 봅니다. 마침 을 클릭하거나 뒤로 단추를 사용하여 설정을 편집합니다.
21. 설치가 시작된 후 설치를 일시 중지하거나 중지할 수 없다는 메시지가 나타납니다. 계속하려면 확인을 클릭하십시오.

    어플라이언스 설정이 계속됩니다. 이 작업은 몇 분 정도 걸립니다.

    설정이 성공했음을 나타내는 메시지가 나타납니다.

    vCenter Server에 액세스하기 위해 설치 관리자가 제공하는 링크를 클릭할 수 있습니다.

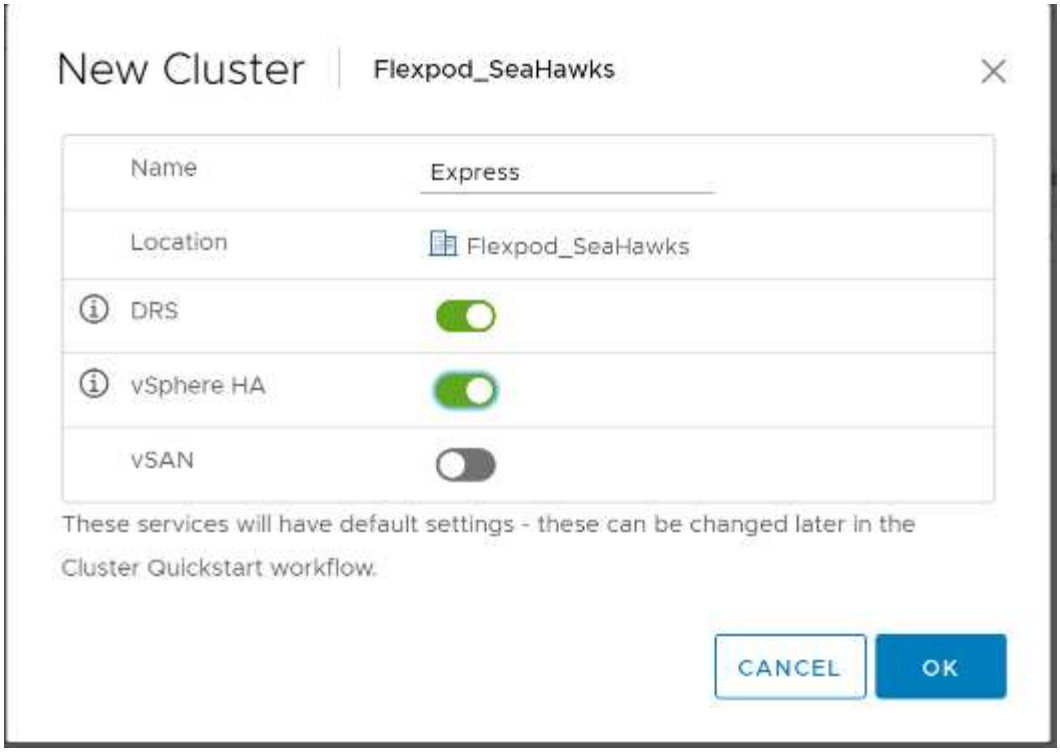
VMware vCenter Server 6.7 및 **vSphere** 클러스터링 구성

VMware vCenter Server 6.7 및 vSphere 클러스터링을 구성하려면 다음 단계를 수행하십시오.

1. https://\<<FQDN 또는 vCenter의 IP >>/vSphere-client/로 이동합니다.
2. vSphere Client 시작 을 클릭합니다.
3. 사용자 이름 administrator@vsphere.loca l 과 VCSA 설정 프로세스 중에 입력한 SSO 암호를 사용하여 로그인합니다.
4. vCenter 이름을 마우스 오른쪽 버튼으로 클릭하고 New Datacenter를 선택합니다.
5. 데이터 센터의 이름을 입력하고 확인 을 클릭합니다.
    - vSphere 클러스터를 생성합니다. *

vSphere 클러스터를 생성하려면 다음 단계를 수행하십시오.

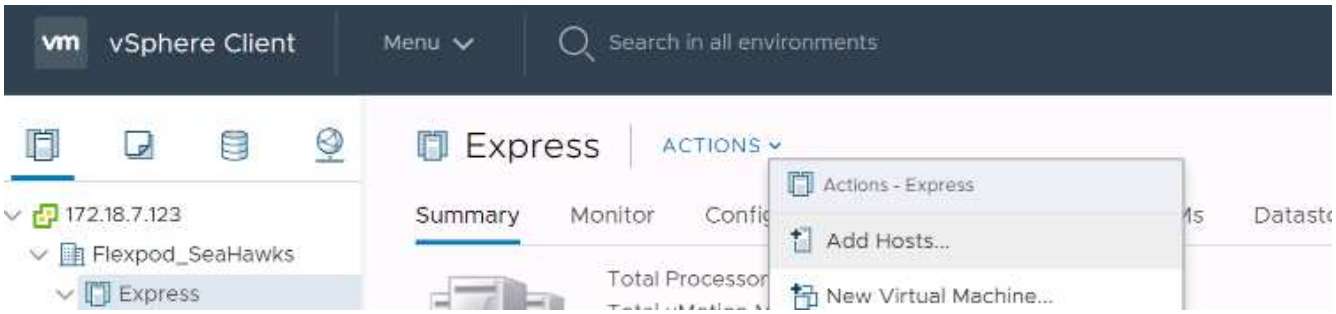
1. 새로 생성된 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 New Cluster를 선택합니다.
2. 클러스터의 이름을 입력합니다.
3. DRS 및 vSphere HA 옵션을 선택하고 설정합니다.
4. 확인 을 클릭합니다.



◦ 클러스터에 ESXi 호스트 추가 *

클러스터에 ESXi 호스트를 추가하려면 다음 단계를 수행하십시오.

1. 클러스터의 Actions 메뉴에서 Add Host를 선택합니다.



2. 클러스터에 ESXi 호스트를 추가하려면 다음 단계를 수행하십시오.
   a. 호스트의 IP 또는 FQDN을 입력합니다. 다음 을 클릭합니다.
   b. 루트 사용자 이름과 암호를 입력합니다. 다음 을 클릭합니다.
   c. 예를 클릭하여 호스트의 인증서를 VMware 인증서 서버에서 서명한 인증서로 바꿉니다.
   d. 호스트 요약 페이지에서 다음 을 클릭합니다.
   e. 녹색 + 아이콘을 클릭하여 vSphere 호스트에 라이센스를 추가합니다.

      이 단계는 원할 경우 나중에 완료할 수 있습니다.

   f. 다음 을 클릭하여 잠금 모드를 해제합니다.
   g. VM 위치 페이지에서 다음 을 클릭합니다.

h. 완료 준비 페이지를 검토합니다. 뒤로 단추를 사용하여 변경하거나 마침 을 선택합니다.

3. Cisco UCS 호스트 B에 대해 1단계와 2단계를 반복합니다

   FlexPod Express 구성에 추가된 모든 호스트에 대해 이 프로세스를 완료해야 합니다.

ESXi 호스트에서 코어 덤프를 구성합니다

iSCSI 부팅 호스트에 대한 ESXi Dump Collector 설정

VMware iSCSI 소프트웨어 이니시에이터를 사용하여 iSCSI로 부팅된 ESXi 호스트는 vCenter의 일부인 ESXi 덤프 수집기로 코어 덤프를 수행하도록 구성해야 합니다. 덤프 수집기는 vCenter 어플라이언스에서 기본적으로 사용되지 않습니다. 이 절차는 vCenter 구축 섹션의 마지막에 실행해야 합니다. ESXi 덤프 수집기를 설정하려면 다음 단계를 수행하십시오.

1. vSphere Web Client에 mailto:administrator@vsphere.loca l[administrator@vsphere.loca l^]으로 로그인하고 Home을 선택합니다.
2. 가운데 창에서 시스템 구성 을 클릭합니다.
3. 왼쪽 창에서 서비스를 선택합니다.
4. 서비스 에서 VMware vSphere ESXi Dump Collector 를 클릭합니다.
5. 중앙 창에서 녹색 시작 아이콘을 클릭하여 서비스를 시작합니다.
6. 작업 메뉴에서 시작 유형 편집을 클릭합니다.
7. 자동을 선택합니다.
8. 확인 을 클릭합니다.
9. SSH를 루트로 사용하여 각 ESXi 호스트에 연결합니다.
10. 다음 명령을 실행합니다.

```
esxcli system coredump network set –v vmk0 –j <vcenter-ip>
esxcli system coredump network set –e true
esxcli system coredump network check
```

최종 명령어를 실행하면 Verified the configured netdump server is running 메시지가 나타난다.

FlexPod Express에 추가된 모든 호스트에 대해 이 프로세스를 완료해야 합니다.

결론

FlexPod Express는 업계 최고의 구성요소를 사용하는 검증된 설계를 통해 간단하고 효율적인 솔루션을 제공합니다. FlexPod Express는 추가 구성요소를 추가하여 특정 비즈니스 요구사항에 맞게 확장할 수 있습니다. FlexPod Express는 전용 솔루션이 필요한 중소기업, ROBO 및 기타 기업을 염두에 두고 설계되었습니다.

추가 정보

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

- NVA-1130-design:VMware vSphere 6.7U1 및 NetApp AFF A220을 포함하는 FlexPod Express with Direct-Attached IP = 기반 스토리지 NVA Design

  "https://www.netapp.com/us/media/nva-1130-design.pdf"

- AFF and FAS 시스템 설명서 센터 를 참조하십시오

  "http://docs.netapp.com/platstor/index.jsp"

- ONTAP 9 문서 센터

  "http://docs.netapp.com/ontap-9/index.jsp"

- NetApp 제품 설명서

  "https://docs.netapp.com"

FlexPod Express for VMware vSphere 7.0 with Cisco UCS Mini 및 NetApp AFF/FAS-NVA-Deployment

Jyh-shing Chen, NetApp

Cisco UCS Mini 및 NetApp AFF/FAS 솔루션이 포함된 VMware vSphere 7.0용 FlexPod Express는 B200 M5 블레이드 서버, Cisco UCS 6324 섀시 내 패브릭 인터커넥트, Cisco Nexus 31108PC-V 스위치 또는 기타 호환 스위치, NetApp AFF A220, C190 또는 FAS2700 시리즈 컨트롤러 HA 쌍을 지원하는 Cisco UCS Mini를 활용합니다. NetApp ONTAP 9.7 데이터 관리 소프트웨어를 실행합니다. 이 NVA(NetApp Verified Architecture) 구축 문서는 인프라 구성 요소를 구성하고 VMware vSphere 7.0 및 관련 툴을 구축하여 매우 안정적이고 가용성이 높은 FlexPod Express 기반 가상 인프라를 구축하는 데 필요한 세부 단계를 제공합니다.

"FlexPod Express for VMware vSphere 7.0 with Cisco UCS Mini 및 NetApp AFF/FAS-NVA-Deployment"

FlexPod 및 보안

FlexPod, 랜섬웨어에 대한 솔루션

TR-4802: FlexPod, 랜섬웨어에 대한 솔루션

NetApp의 Arvind Ramakrishnan

파트너 후원:

랜섬웨어를 이해하려면 먼저 암호화에 대한 몇 가지 핵심 사항을 이해해야 합니다. 암호화 그래픽 방법을 사용하면 공유 비밀 키(대칭 키 암호화) 또는 키 쌍(비대칭 키 암호화)으로 데이터를 암호화할 수 있습니다. 이러한 키 중 하나는 널리 사용되는 공개 키이고 다른 하나는 비공개 개인 키입니다.

랜섬웨어는 암호화 바이러스 를 기반으로 하는 맬웨어의 한 유형으로, 암호화를 사용하여 악성 소프트웨어를 작성합니다. 이 맬웨어는 대칭 키 암호화와 비대칭 키 암호화를 모두 사용하여 피해자의 데이터를 잠그고 피해자의 데이터를 해독할 키를 제공하는 대가로 금전을 요구합니다.

랜섬웨어의 작동 방식

다음 단계에서는 랜섬웨어가 암호화를 사용하여 피해자의 암호 해독 또는 복구 범위 없이 피해자의 데이터를 암호화하는 방법을 설명합니다.

1. 공격자는 비대칭 키 암호화에서와 같이 키 쌍을 생성합니다. 생성된 공개 키는 맬웨어 내에 배치되고 맬웨어는 해제됩니다.
2. 맬웨어가 피해자의 컴퓨터 또는 시스템에 침입한 후 pseudorandom 숫자 생성기(PRNG) 또는 기타 실행 가능한 임의의 숫자 생성 알고리즘을 사용하여 임의의 대칭 키를 생성합니다.
3. 맬웨어는 이 대칭 키를 사용하여 피해자의 데이터를 암호화합니다. 결과적으로 맬웨어에 포함된 공격자의 공개 키를 사용하여 대칭 키를 암호화합니다. 이 단계의 출력은 암호화된 대칭 키의 비대칭 암호문과 피해자 데이터의 대칭 암호문입니다.
4. 맬웨어는 피해자의 데이터와 데이터를 암호화하는 데 사용된 대칭 키를 제로(삭제)하여 복구 범위를 남기지 않습니다.
5. 피해자는 이제 대칭 키의 비대칭 암호문과 데이터를 암호화하는 데 사용된 대칭 키를 얻기 위해 지불해야 하는 랜섬 값을 표시합니다.
6. 피해자는 몸값을 지불하고 비대칭 암호문을 공격자와 공유합니다. 공격자는 개인 키로 암호문을 해독하여 대칭 키를 만듭니다.
7. 공격자는 이 대칭 키를 피해자와 공유합니다. 이 키를 사용하여 모든 데이터를 해독하고 공격에서 복구할 수 있습니다.

당면 과제

개인 및 조직은 랜섬웨어의 공격을 받을 때 다음과 같은 문제에 직면해 있습니다.

- 가장 중요한 과제는 조직 또는 개인의 생산성을 즉각적으로 저하시키는 것입니다. 모든 중요 파일을 다시 확보하고 시스템을 안전하게 보호해야 하므로 정상 상태로 복원하는 데 시간이 걸립니다.
- 고객 또는 고객에 속하는 중요한 기밀 정보가 포함된 데이터 유출로 인해 조직이 분명히 피하고 싶어 하는 위기 상황이 발생할 수 있습니다.
- 데이터가 잘못 유출되거나 완전히 삭제될 가능성이 매우 높습니다. 이로 인해 조직과 개인에게 재앙이 될 수 있는 무리턴 지점이 될 수 있습니다.
- 랜섬을 지불한 후에는 공격자가 데이터를 복원할 키를 제공할 것이라는 보장이 없습니다.
- 공격자는 대가를 지불하더라도 중요한 데이터의 브로드캐스트를 삼가한다는 보장은 없습니다.
- 대규모 엔터프라이즈에서 랜섬웨어 공격으로 이어받은 허점을 식별하는 일은 지루한 작업이며, 모든 시스템을 보호하는 데는 많은 노력이 필요합니다.

누가 위험에 처합니까?

개인 및 대규모 조직을 포함하여 모든 사람이 랜섬웨어의 공격을 받을 수 있습니다. 잘 정의된 보안 수단과 관행을 구현하지 않는 조직은 이러한 공격에 훨씬 더 취약합니다. 대규모 조직에 가해지는 공격의 결과는 개인이 견딜 수 있는 것보다 몇 배 더 클 수 있습니다.

랜섬웨어는 모든 맬웨어 공격의 약 28%를 차지합니다. 다시 말해, 4개 맬웨어 사고 중 2개 이상이 랜섬웨어 공격입니다. 랜섬웨어는 인터넷을 통해 자동으로 무차별적으로 확산될 수 있으며, 보안 문제가 발생할 경우 피해자의 시스템에 진입하여 연결된 다른 시스템으로 계속 확산될 수 있습니다. 공격자들은 많은 파일 공유를 수행하거나, 많은 중요한 데이터를 보유하고 있거나, 공격에 대한 부적절한 보호를 유지하는 사람 또는 조직을 표적으로 삼는 경향이 있습니다.

공격자들은 다음과 같은 잠재적 표적에 집중하는 경향이 있습니다.

- 대학 및 학생 커뮤니티
- 정부 기관 및 기관
- 있습니다
- 은행

이것은 전체 대상 목록이 아닙니다. 이러한 범주 중 하나를 벗어나는 경우 공격으로부터 자신을 보호할 수 없습니다.

랜섬웨어는 시스템에 어떻게 들어가거나 확산됩니까?

랜섬웨어가 시스템에 들어오거나 다른 시스템으로 확산되는 방법에는 여러 가지가 있습니다. 오늘날의 세계에서 거의 모든 시스템은 인터넷, LAN, WAN 등을 통해 서로 연결되어 있습니다. 이러한 시스템 간에 생성 및 교환되는 데이터의 양은 증가만 되고 있습니다.

랜섬웨어가 확산되는 가장 일반적인 방법 중 일부에는 매일 데이터를 공유 또는 액세스하기 위해 사용하는 방법이 포함됩니다.

- 이메일
- P2P 네트워크
- 파일 다운로드
- 소셜 네트워킹
- 모바일 장치
- 안전하지 않은 공용 네트워크에 연결

- 웹 URL 액세스

데이터 손실의 결과

데이터 손실의 결과 또는 효과는 조직이 예상하는 것보다 훨씬 더 클 수 있습니다. 이러한 영향은 다운타임 기간 또는 조직이 데이터에 액세스할 수 없는 기간에 따라 달라질 수 있습니다. 공격이 지속되는 기간이 길수록 조직의 매출, 브랜드, 평판에 미치는 영향이 커집니다. 또한 조직은 법적 문제와 급격한 생산성 저하에 직면할 수 있습니다.

이러한 문제는 시간이 지나면서 계속 지속되기 때문에 공격이 어떻게 반응하는지에 따라 조직 문화가 확대되고 결국 조직 문화가 변하게 될 수 있습니다. 오늘날의 세계에서 정보가 빠른 속도로 퍼지고 조직에 대한 부정적인 뉴스가 퍼지면 회사의 명성에 영구적인 손상을 줄 수 있습니다. 조직은 데이터 손실에 대해 막대한 처벌을 받을 수 있으며, 이로 인해 결과적으로 비즈니스가 종료될 수 있습니다.

재무적 영향

최근 에 따르면 "McAfee 보고서"사이버 범죄로 인해 발생하는 글로벌 비용은 약 6천억 달러로, 이는 전 세계 GDP의 약 0.8%입니다. 이 액수가 전 세계적으로 4조2000억 달러에 이르는 인터넷 경제 성장세에 비해 14%의 세금에 해당한다.

랜섬웨어는 이러한 재무 비용의 상당 부분을 차지합니다. 2018년에 랜섬웨어 공격으로 인해 발생한 비용은 약 80억 달러이며, 2019년에는 115억 달러에 이를 것으로 예측됩니다.

솔루션이 무엇입니까**?**

최소한의 다운타임으로 랜섬웨어 공격에서 복구하려면 사전 예방적 재해 복구 계획을 구현해야만 합니다. 공격에서 복구할 수 있는 기능을 갖추는 것이 좋지만 공격을 한 번에 차단하는 것이 좋습니다.

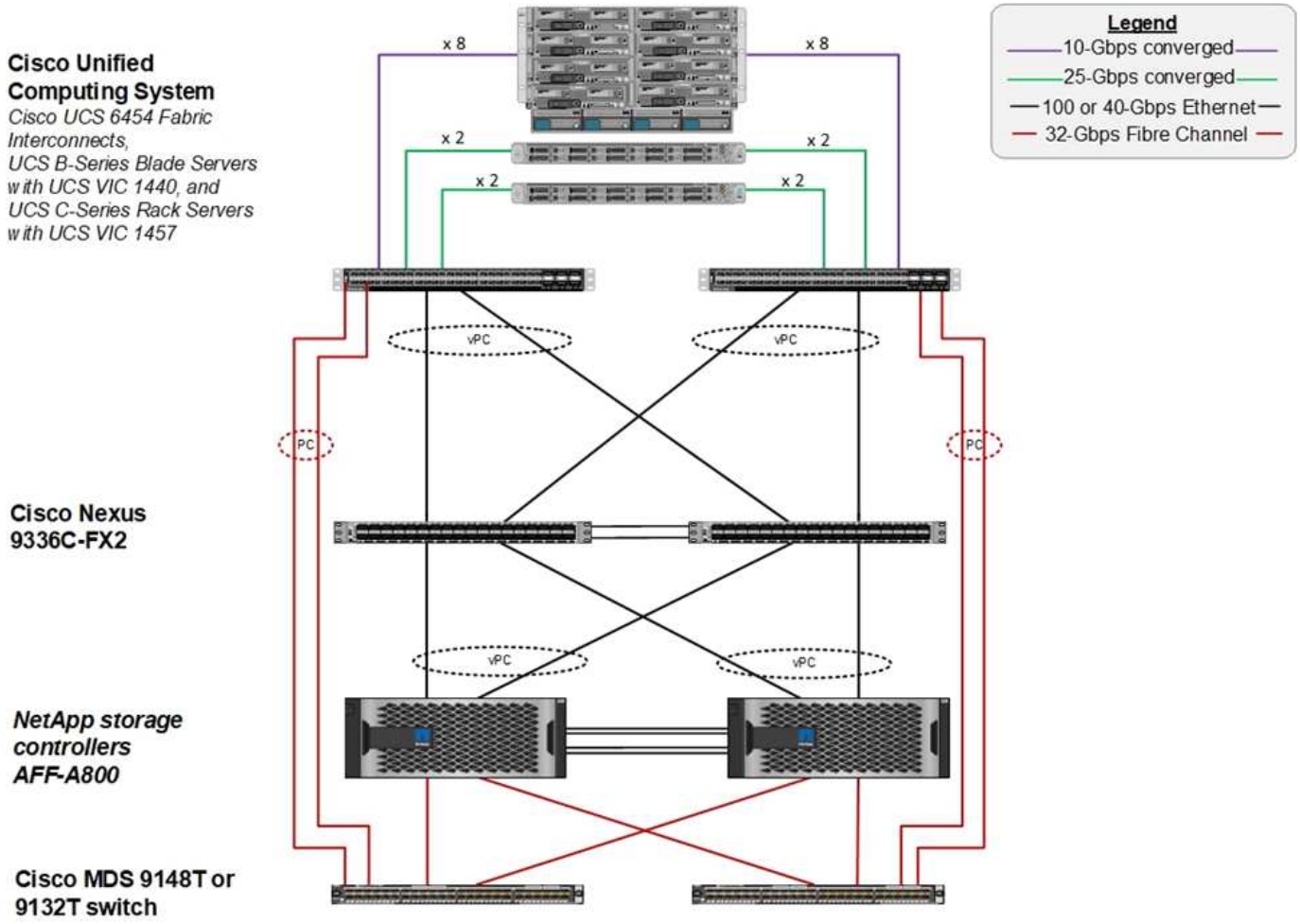
공격을 방지하기 위해 몇 가지 프런트 엔드를 검토하고 수정해야 하지만 공격을 막거나 공격으로부터 복구할 수 있는 핵심 구성 요소는 데이터 센터입니다.

네트워크, 컴퓨팅 및 스토리지 엔드 포인트의 보안을 위해 데이터 센터가 제공하는 설계와 기능은 일상적인 운영을 위한 안전한 환경을 구축하는 데 중요한 역할을 합니다. 이 문서에서는 FlexPod 하이브리드 클라우드 인프라의 기능이 공격 시 데이터를 빠르게 복구하는 데 어떤 도움이 되며 공격을 한 번에 차단하는 데에도 어떤 도움이 되는지를 보여 줍니다.

FlexPod 개요

FlexPod는 Cisco UCS(Unified Computing System) 서버, Cisco Nexus 스위치 제품군, Cisco MDS 패브릭 스위치 및 NetApp 스토리지 어레이를 유연한 단일 아키텍처로 결합하는 사전 설계, 통합 및 검증된 아키텍처입니다. FlexPod 솔루션은 단일 장애 지점 없이 고가용성을 지원하도록 설계되었으며, 비용 효율성과 설계 유연성을 유지하여 다양한 워크로드를 지원합니다. FlexPod 설계는 다양한 하이퍼바이저와 베어 메탈 서버를 지원할 수 있으며 고객의 워크로드 요구사항에 따라 규모 조정 및 최적화할 수 있습니다.

아래 그림은 FlexPod 아키텍처를 보여 주며 스택의 모든 계층에서 고가용성을 보여 줍니다. 스토리지, 네트워크 및 컴퓨팅의 인프라 구성요소는 구성요소 중 하나에 장애가 발생할 경우 정상 작동하는 파트너에게 즉시 페일오버할 수 있도록 구성됩니다.



FlexPod 시스템의 가장 큰 장점은 여러 워크로드를 위해 사전 설계, 통합 및 검증된다는 것입니다. 모든 솔루션 검증에 대한 자세한 설계 및 배포 가이드가 게시되었습니다. 이러한 문서에는 FlexPod에서 원활하게 워크로드를 실행하기 위해 채택해야 하는 모범 사례가 포함되어 있습니다. 이러한 솔루션은 동급 최고의 컴퓨팅, 네트워크 및 스토리지 제품과 전체 인프라의 보안 및 강화를 위한 다양한 기능을 토대로 구축되었습니다.

"IBM의 X-Force 위협 인텔리전스 지수" "과거 424%의 잘못 구성된 클라우드 인프라 점프를 포함하여 손상된 기록의 3분의 2를 책임지는 사람의 실수"

FlexPod 시스템을 사용하면 CVD(Cisco Validated Design)와 NVA(NetApp Verified Architecture)에 설명된 모범 사례에 따라 인프라를 엔드 투 엔드 방식으로 설정하는, Ansible 플레이북을 통해 자동화를 통해 인프라 구성 오류를 방지할 수 있습니다.

랜섬웨어 차단 조치

이 섹션에서는 랜섬웨어 공격을 효과적으로 보호하고 복구할 수 있는 NetApp ONTAP 데이터 관리 소프트웨어의 주요 기능과 Cisco UCS 및 Cisco Nexus용 툴에 대해 설명합니다.

스토리지**: NetApp ONTAP**

ONTAP 소프트웨어는 데이터 보호에 유용한 여러 기능을 제공하며, 대부분의 기능은 ONTAP 시스템을 사용하는 고객에게 무료로 제공됩니다. 다음 기능을 항상 사용하여 공격으로부터 데이터를 보호할 수 있습니다.

- * NetApp 스냅샷 기술. * 스냅샷 복사본은 특정 시점의 파일 시스템 상태를 캡처하는 볼륨의 읽기 전용

이미지입니다. 이러한 복사본은 시스템 성능에 영향을 주지 않고 데이터를 보호하면서 많은 스토리지 공간을 차지하지 않습니다. 스냅샷 복사본을 생성하기 위한 일정을 생성하는 것이 좋습니다. 또한 일부 맬웨어가 휴면 상태가 된 후 감염 후 몇 주 또는 몇 개월 후에 다시 활성화될 수 있기 때문에 보존 기간을 길게 유지해야 합니다. 공격이 발생할 경우 감염 전에 생성된 스냅샷 복사본을 사용하여 볼륨을 롤백할 수 있습니다.

- * NetApp SnapRestore 기술. * SnapRestore 데이터 복구 소프트웨어는 데이터 손상을 복구하거나 파일 내용만 되돌리는 데 매우 유용합니다. SnapRestore은 볼륨의 특성을 되돌리지 않으며 스냅샷 복사본에서 액티브 파일 시스템으로 파일을 복사하여 관리자가 달성할 수 있는 것보다 훨씬 빠릅니다. 많은 파일을 최대한 빨리 복구해야 하는 경우 데이터를 복구할 수 있는 속도가 유용합니다. 이러한 매우 효율적인 복구 프로세스를 통해 공격이 발생할 경우 비즈니스를 신속하게 온라인 상태로 되돌릴 수 있습니다.
- * NetApp SnapCenter 기술. * SnapCenter 소프트웨어는 NetApp 스토리지 기반 백업 및 복제 기능을 사용하여 애플리케이션 정합성을 보장하는 데이터 보호를 제공합니다. 이 소프트웨어는 엔터프라이즈 애플리케이션과 통합되며 애플리케이션, 데이터베이스 및 가상 인프라 관리자의 요구사항에 부합하는 애플리케이션별 워크플로우 및 데이터베이스별 워크플로우를 제공합니다. SnapCenter은 사용하기 쉬운 엔터프라이즈 플랫폼을 제공하여 애플리케이션, 데이터베이스 및 파일 시스템 전반에서 데이터 보호를 안전하게 조율하고 관리합니다. 애플리케이션을 더욱 신속하게 일관된 상태로 복원할 수 있으므로 데이터 복구 중에도 애플리케이션 정합성이 보장된 데이터 보호를 제공하는 기능은 매우 중요합니다.
- NetApp SnapLock 기술 * SnapLock은 파일을 저장한 후 지우거나 쓰기가 불가능한 상태로 커밋하는 특수한 용도의 볼륨을 제공합니다. FlexVol 볼륨에 상주하는 사용자의 운영 데이터는 NetApp SnapMirror 또는 SnapVault 기술을 통해 SnapLock 볼륨으로 미러링하거나 저장할 수 있습니다. SnapLock 볼륨의 파일, 볼륨 자체 및 해당 호스팅 애그리게이트는 보존 기간이 끝날 때까지 삭제할 수 없습니다.
- * NetApp FPolicy 기술. * FPolicy 소프트웨어를 사용하여 특정 확장명의 파일에 대한 작업을 허용하지 않도록 함으로써 공격을 방지하십시오. FPolicy 이벤트는 특정 파일 작업에 대해 트리거될 수 있습니다. 이 이벤트는 정책에 연결되어 있어야 하는 엔진을 호출합니다. 랜섬웨어를 포함할 수 있는 파일 확장자 세트로 정책을 구성할 수 있습니다. 허용되지 않는 확장명을 가진 파일이 무단 작업을 수행하려고 하면 FPolicy가 해당 작업이 실행되지 않도록 합니다.

네트워크**: Cisco Nexus**

Cisco NX OS 소프트웨어는 네트워크 이상 현상 및 보안을 더욱 강화하는 NetFlow 기능을 지원합니다. NetFlow는 네트워크의 모든 대화 메타데이터, 통신 관련 당사자, 사용 중인 프로토콜 및 트랜잭션 기간을 캡처합니다. 정보를 집계 및 분석한 후에는 정상적인 동작에 대한 통찰력을 제공할 수 있습니다.

또한 수집된 데이터를 통해 네트워크를 통해 확산되는 맬웨어와 같은 의심스러운 활동 패턴을 식별할 수 있으며, 그렇지 않을 경우 이를 간과할 수 있습니다.

NetFlow는 흐름을 사용하여 네트워크 모니터링에 대한 통계를 제공합니다. 흐름은 소스 인터페이스(또는 VLAN)에 도착하고 키에 대해 동일한 값을 갖는 패킷의 단방향 스트림입니다. 키는 패킷 내의 필드에 대해 식별된 값입니다. 유동 레코드를 사용하여 유동의 고유 키를 정의하는 유동을 만듭니다. 흐름 내보내기를 사용하여 Cisco Stealthwatch와 같은 원격 NetFlow 수집기로 플로우에 대해 NetFlow에서 수집하는 데이터를 내보낼 수 있습니다. Stealthwatch는 이 정보를 사용하여 네트워크를 지속적으로 모니터링하고 랜섬웨어 발생 시 실시간 위협 탐지 및 사고 대응 법의학 조사를 제공합니다.

컴퓨팅**: Cisco UCS**

Cisco UCS는 FlexPod 아키텍처의 컴퓨팅 엔드포인트입니다. 운영 체제 수준에서 스택의 이 계층을 보호하는 데 도움이 되는 여러 Cisco 제품을 사용할 수 있습니다.

컴퓨팅 또는 애플리케이션 계층에서 다음 주요 제품을 구현할 수 있습니다.

- * 끝점용 Cisco AMP(Advanced Malware Protection).* Microsoft Windows 및 Linux 운영 체제에서 지원되는 이 솔루션은 예방, 검색 및 응답 기능을 통합합니다. 이 보안 소프트웨어는 침입을 방지하고 진입 지점에서 맬웨어를

차단하며 파일 및 프로세스 활동을 지속적으로 모니터링 및 분석하여 일선 방어를 우회할 수 있는 위협을 신속하게 탐지, 억제 및 해결합니다.

AMP의 MAP(Malicious Activity Protection) 구성 요소는 모든 엔드포인트 활동을 지속적으로 모니터링하고 엔드포인트에서 실행 중인 프로그램의 비정상적인 동작을 런타임 감지 및 차단합니다. 예를 들어, 엔드포인트 동작에 랜섬웨어가 표시되면 문제가 되는 프로세스가 종료되어 엔드포인트 암호화가 예방되고 공격이 중지됩니다.

- * Cisco Advanced Malware Protection for Email Security. * 이메일은 맬웨어를 유포하고 사이버 공격을 수행하는 주요 수단으로 자리 잡았습니다. 평균적으로 하루 동안 약 1,000억 개의 이메일이 교환되며, 이를 통해 공격자들은 사용자 시스템에 대한 탁월한 침투 벡터를 얻을 수 있습니다. 따라서 이 공격 라인을 방어하는 것이 절대적으로 중요합니다.

  AMP는 제로 데이 익스플로잇(zero-day exploit) 및 악성 첨부 파일에 숨겨진 악성 맬웨어와 같은 위협에 대한 이메일을 분석합니다. 또한 업계 최고의 URL 인텔리전스를 사용하여 악성 링크를 차단합니다. 스피어 피싱, 랜섬웨어 및 기타 정교한 공격에 대한 고급 보호 기능을 제공합니다.

- * NGIPS(Next-Generation Intrusion Prevention System). * Cisco firepower NGIPS는 데이터 센터에서 물리적 어플라이언스로 구축하거나 VMware(NGIPSv for VMware)에서 가상 어플라이언스로 구축할 수 있습니다. 이 고효율 침입 방지 시스템은 안정적인 성능과 낮은 총 소유 비용을 제공합니다. AMP, 애플리케이션 가시성 및 제어, URL 필터링 기능을 제공하기 위해 선택적 구독 라이센스로 위협 보호를 확장할 수 있습니다. 가상화된 NGIPS는 VM(가상 시스템) 간의 트래픽을 검사하고 리소스가 제한된 사이트에서 NGIPS 솔루션을 쉽게 배포 및 관리할 수 있도록 하여 물리적 자산과 가상 자산 모두의 보호를 강화합니다.

FlexPod에서 데이터 보호 및 복구

이 섹션에서는 공격 발생 시 최종 사용자의 데이터를 복구하는 방법과 FlexPod 시스템을 사용하여 공격을 방지하는 방법을 설명합니다.

테스트 베드 개요

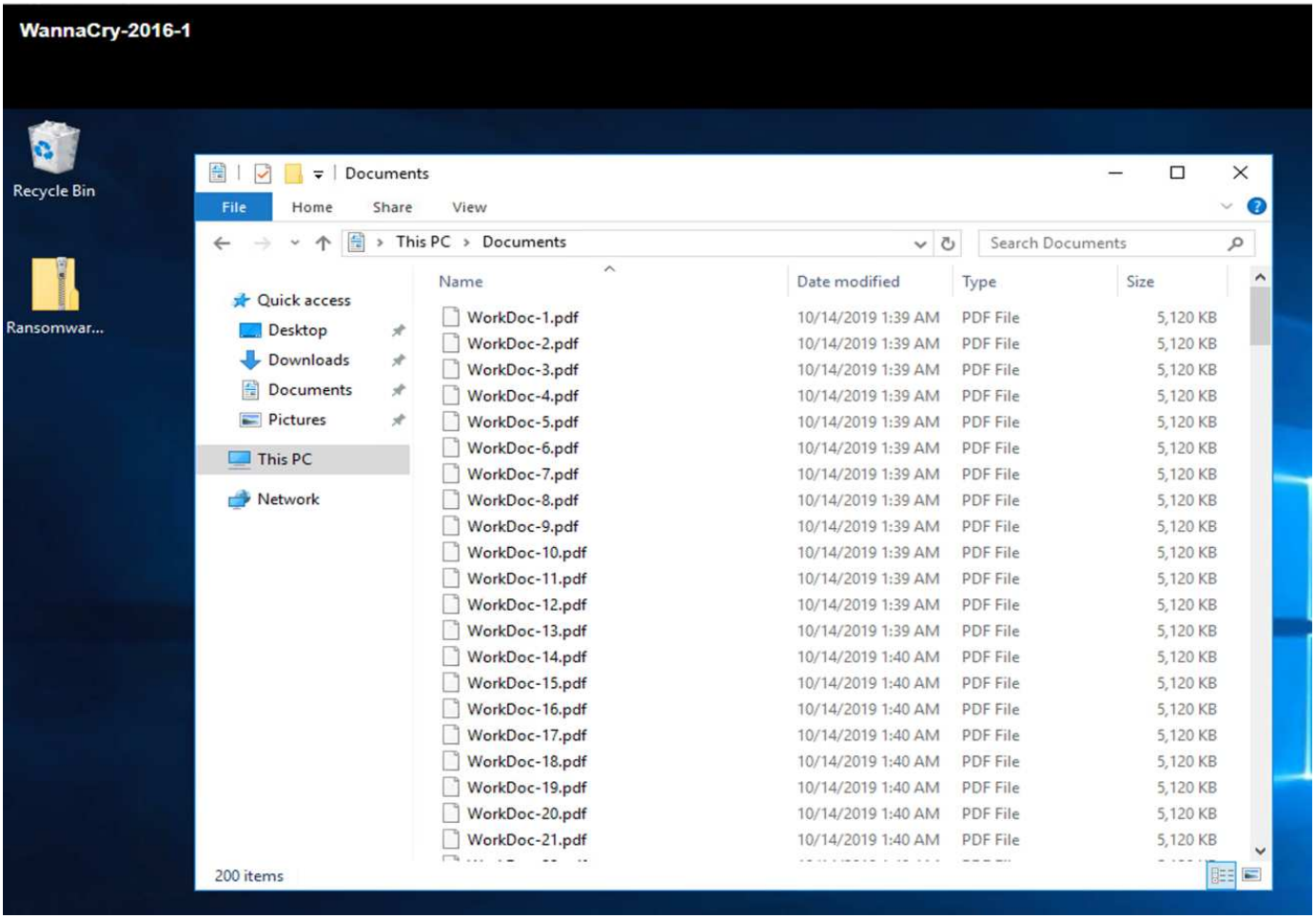
FlexPod 감지, 개선 및 예방을 보여주기 위해 이 문서가 작성된 시점에 제공되는 최신 플랫폼 CVD에 지정된 지침에 따라 테스트베드가 구축되었습니다. "VMware vSphere 6.7 U1, Cisco UCS 4세대 및 NetApp AFF A-Series CVD를 지원하는 FlexPod 데이터 센터".

NetApp ONTAP 소프트웨어의 CIFS 공유를 제공하는 Windows 2016 VM이 VMware vSphere 인프라에 구축했습니다. 그런 다음 CIFS 공유에서 NetApp FPolicy를 구성하여 특정 확장 유형의 파일이 실행되지 않도록 했습니다. 또한 NetApp SnapCenter 소프트웨어는 애플리케이션 정합성을 보장하는 스냅샷 복사본을 제공하기 위해 인프라에서 VM의 스냅샷 복사본을 관리하기 위해 구축되었습니다.

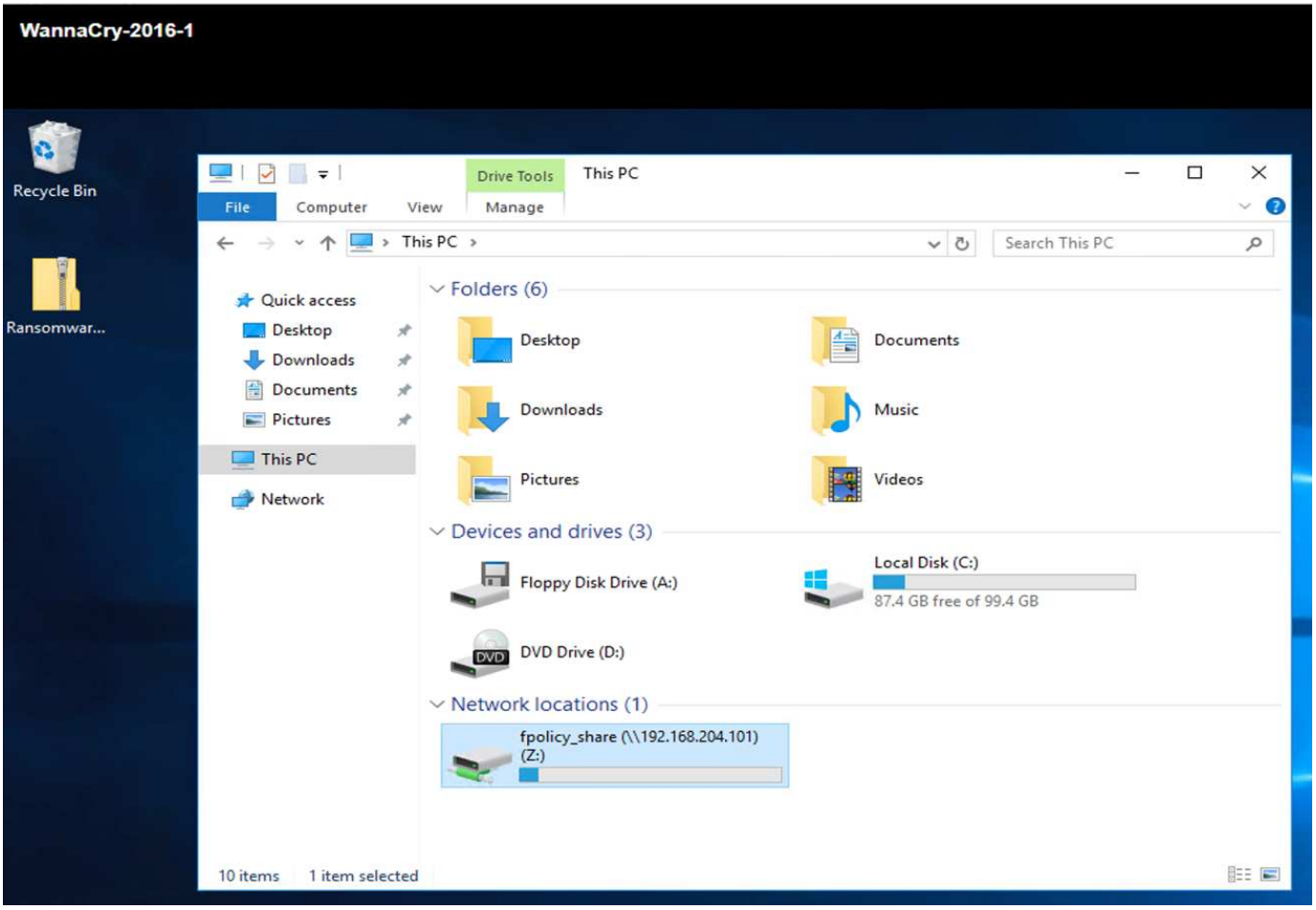
공격 전의 **VM** 및 파일 상태

이 섹션에서는 VM에 대한 공격 전의 파일 상태와 매핑된 CIFS 공유를 보여 줍니다.

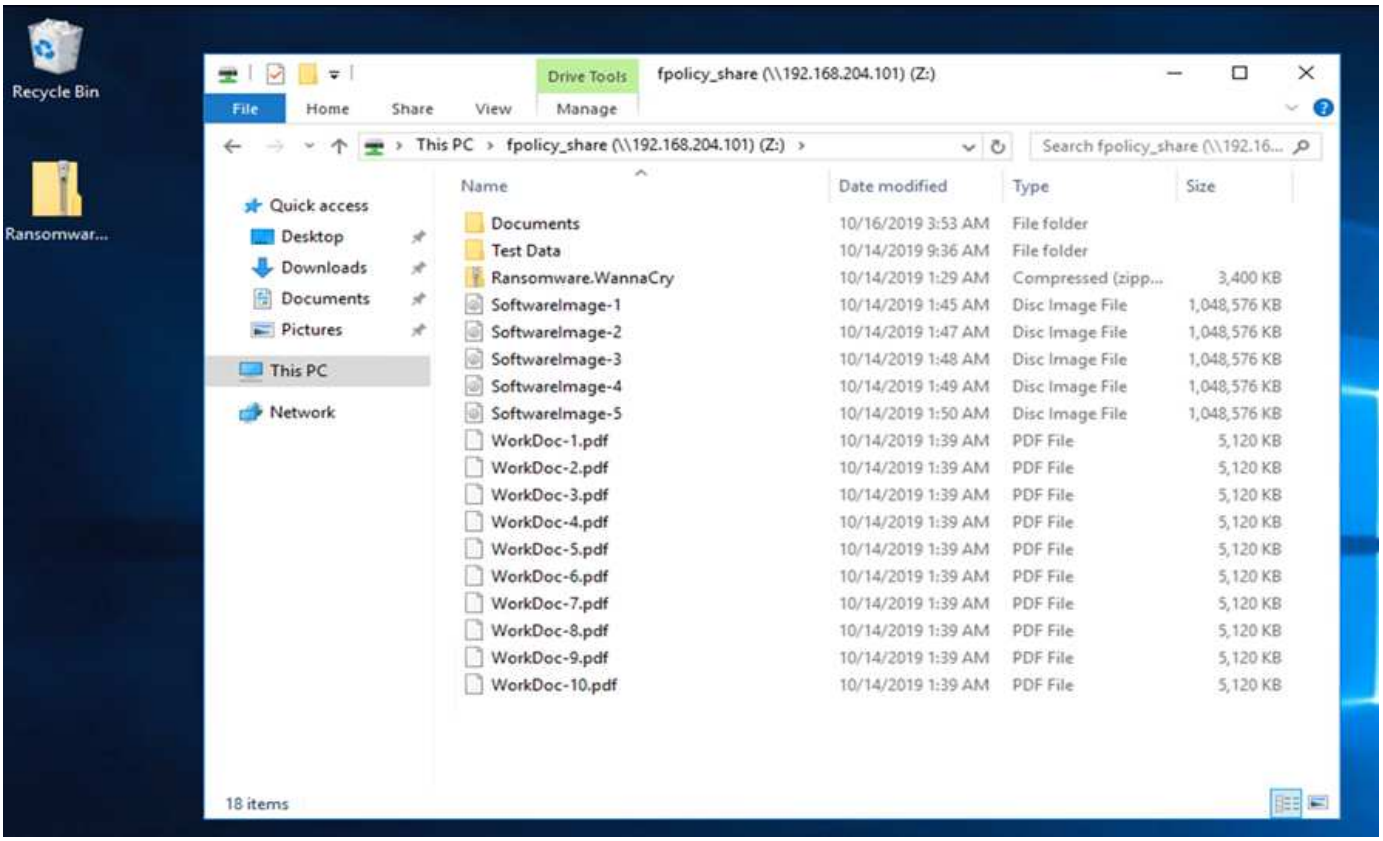
VM의 Documents 폴더에는 WannaCry 맬웨어에 의해 아직 암호화되지 않은 PDF 파일 세트가 있습니다.



다음 스크린샷은 VM에 매핑된 CIFS 공유를 보여 줍니다.



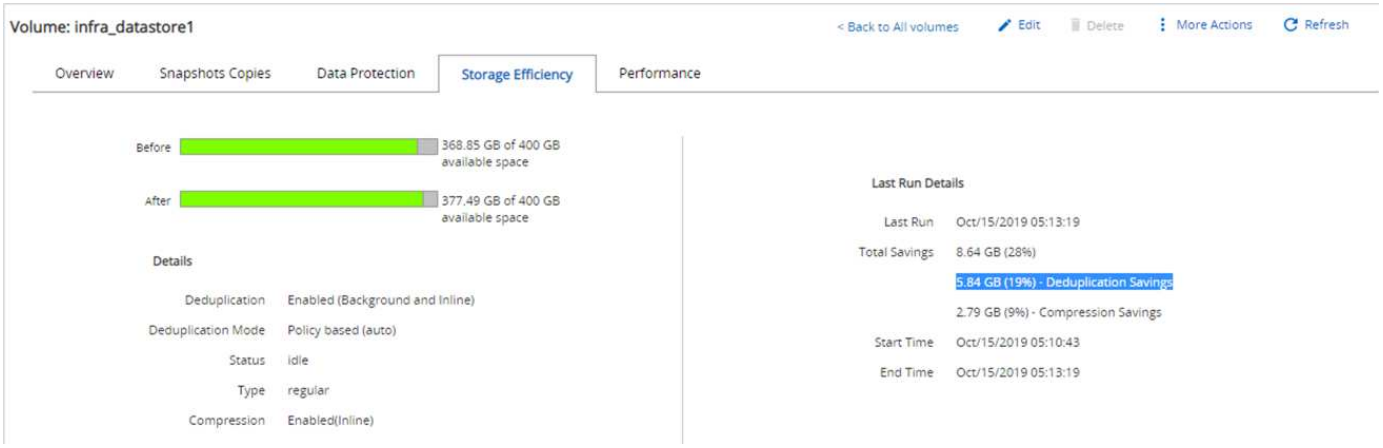
다음 스크린샷은 WannaCry 맬웨어가 아직 암호화하지 않은 CIFS 공유 'FPolicy_share'의 파일을 보여 줍니다.



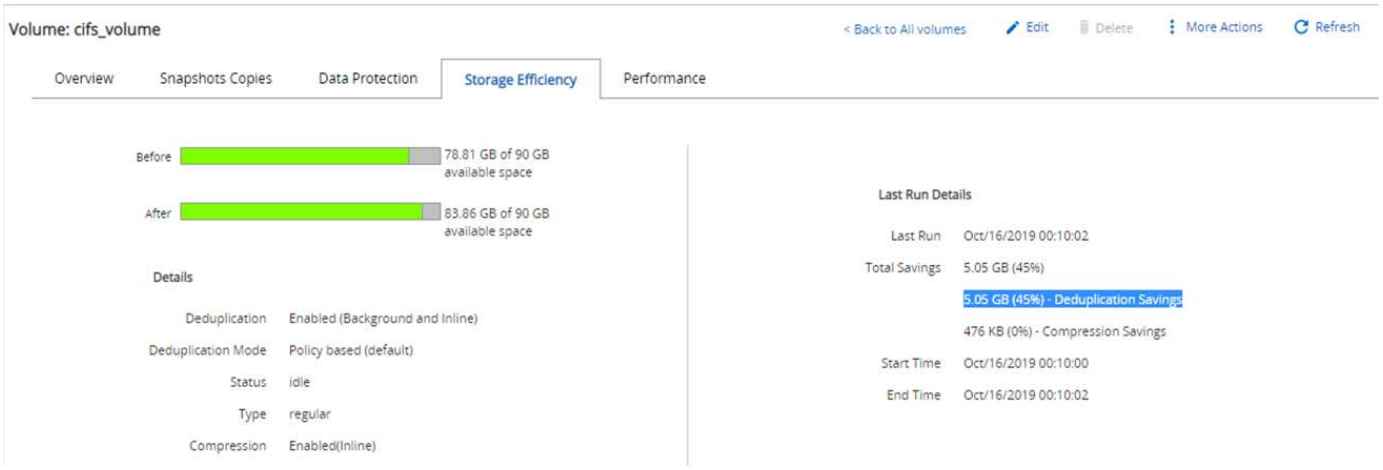
공격 전에 데이터 중복 제거 및 스냅샷 정보

공격 전의 스냅샷 복사본의 스토리지 효율성 세부 정보와 크기는 검색 단계 중에 참조로 표시되고 사용됩니다.

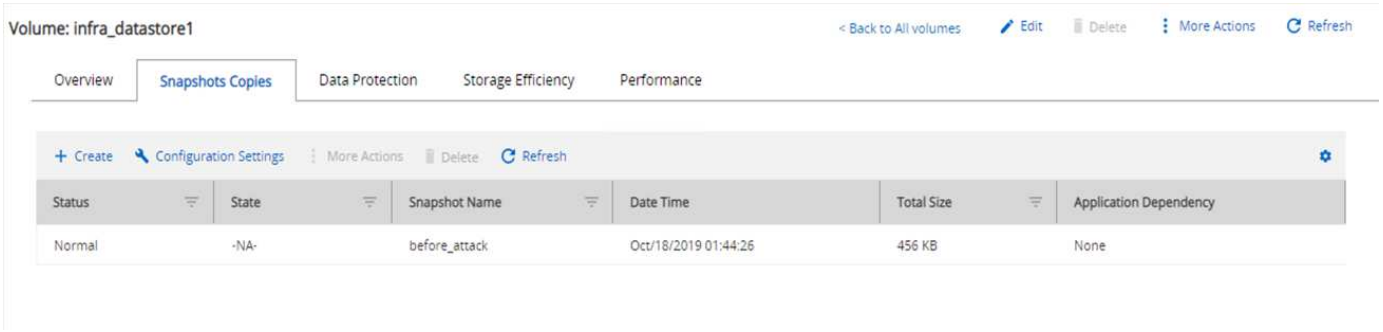
VM을 호스팅하는 볼륨에서 중복 제거를 통해 스토리지를 19%나 절감할 수 있었습니다.



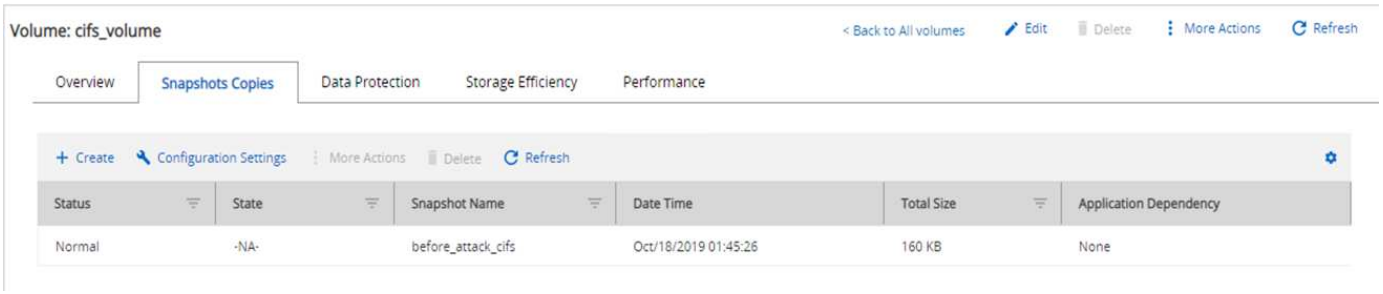
CIFS 공유 'FPolicy_share'의 중복제거 기능으로 스토리지를 45% 절약할 수 있었습니다.



VM을 호스팅하는 볼륨에서 456KB의 스냅샷 복사본 크기가 관찰되었습니다.



CIFS 공유 'FPolicy_share'에 대해 160KB의 스냅샷 복사본 크기가 관찰되었습니다.



VM 및 **CIFS** 공유에서 **WannaCry** 감염

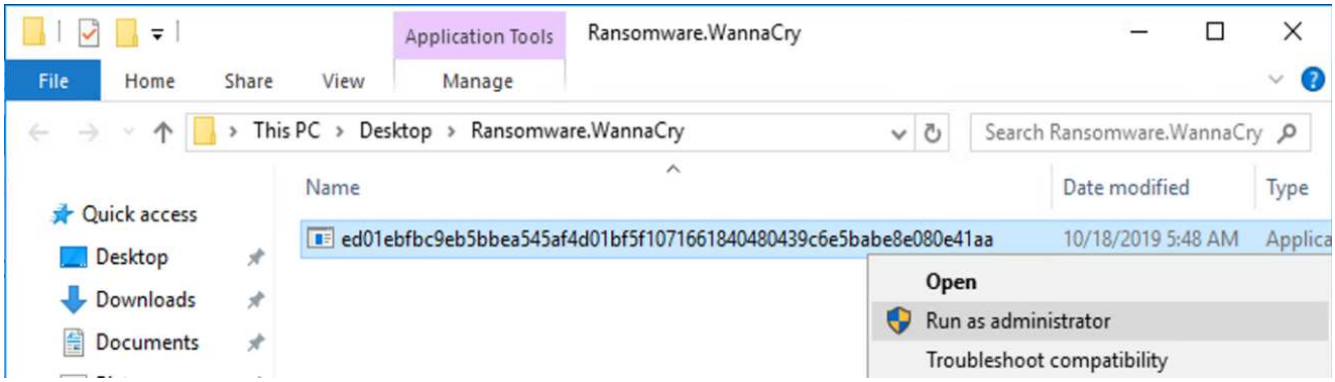
이 섹션에서는 WannaCry 맬웨어가 FlexPod 환경에 도입된 방식과 관찰된 시스템에 대한 후속 변경 사항을 보여 줍니다.

다음 단계에서는 WannaCry 맬웨어 바이너리가 VM에 도입된 방법을 보여 줍니다.

1. 보안 맬웨어가 추출되었습니다.



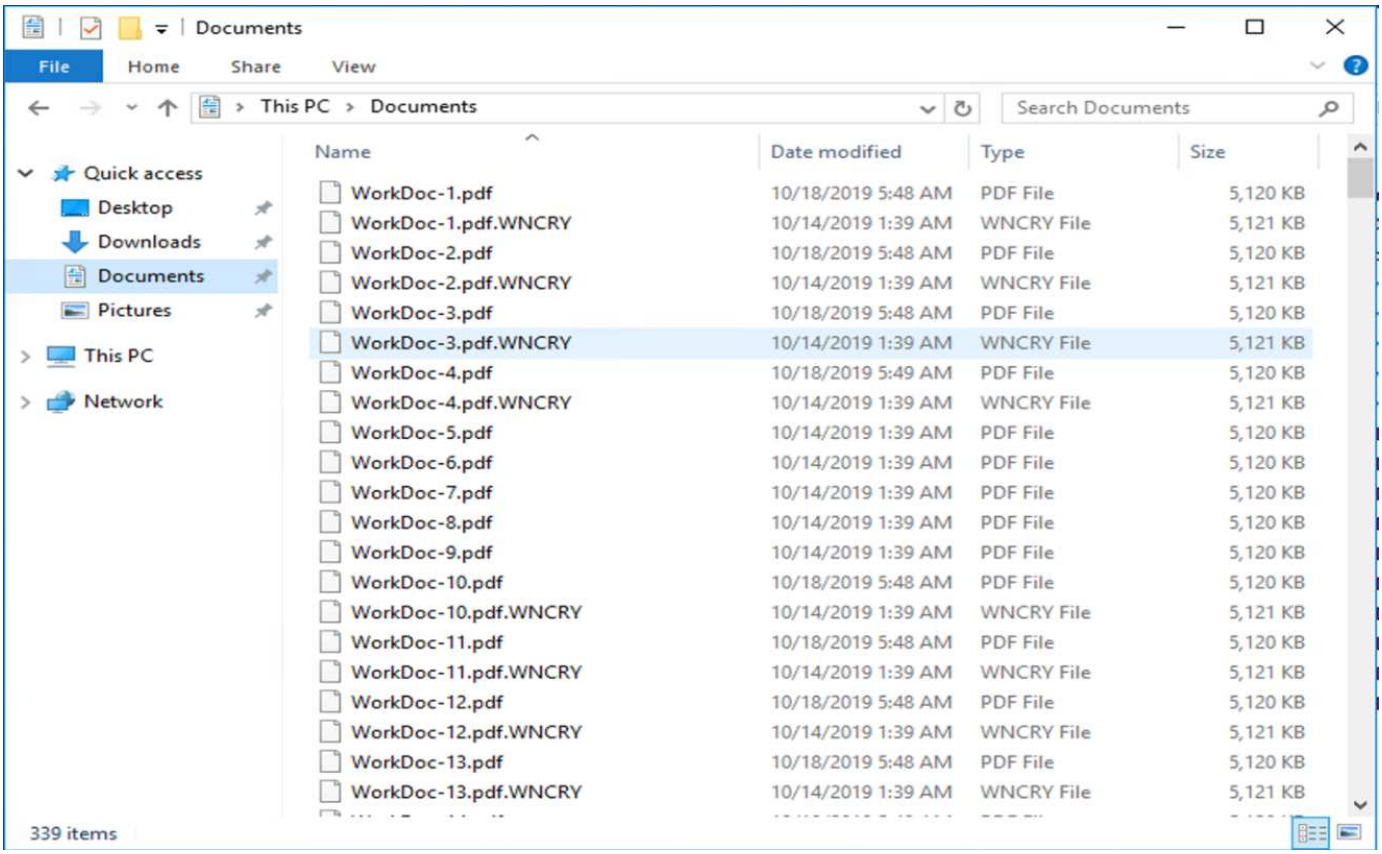
2. 바이너리가 실행되었습니다.



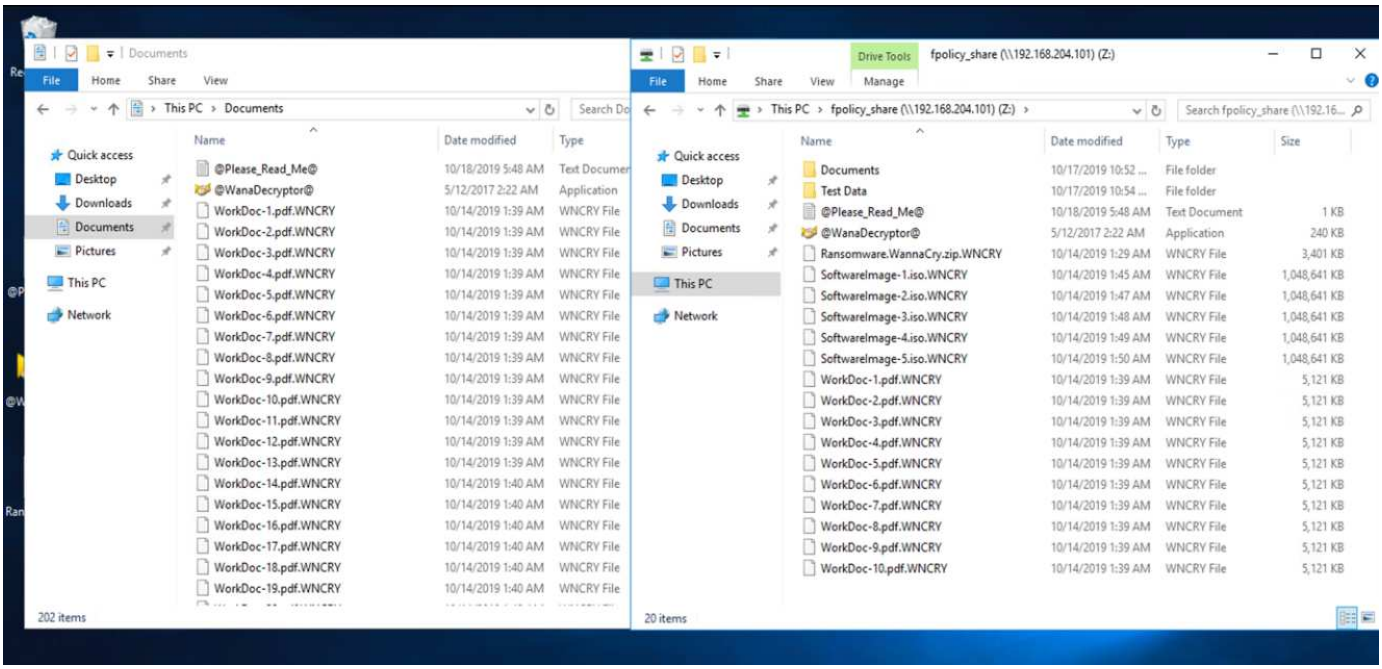
사례 **1: WannaCry**는 **VM** 및 매핑된 **CIFS** 공유 내의 파일 시스템을 암호화합니다

로컬 파일 시스템과 매핑된 CIFS 공유는 WannaCry 멀웨어에 의해 암호화되었습니다.

맬웨어가 WNCRY 확장명으로 파일을 암호화하기 시작합니다.



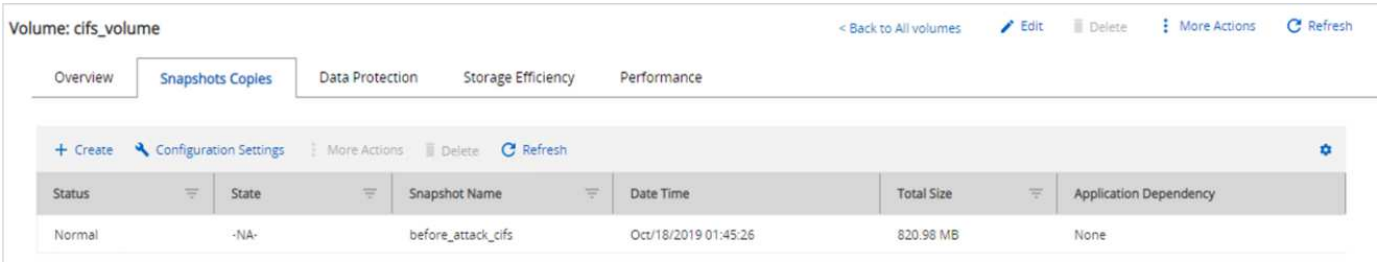
맬웨어는 로컬 VM 및 매핑된 공유의 모든 파일을 암호화합니다.



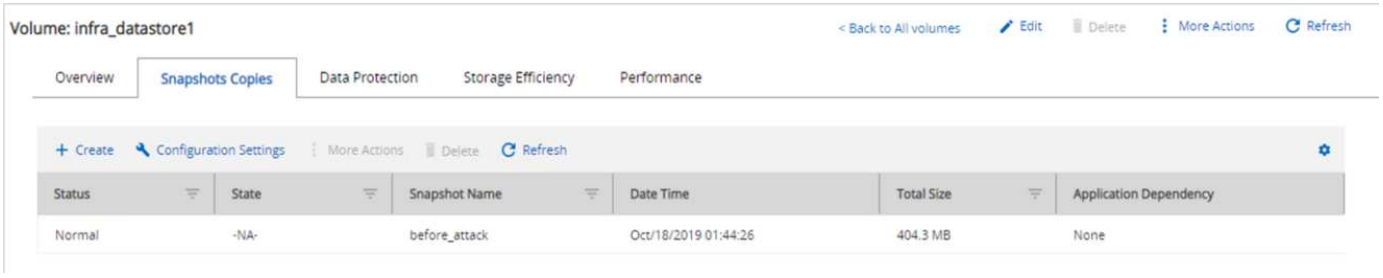
탐지

맬웨어가 파일을 암호화하기 시작한 순간부터 스냅샷 복사본의 크기가 기하급수적으로 증가하고 스토리지 효율성 백분율이 기하급수적으로 감소하게 되었습니다.

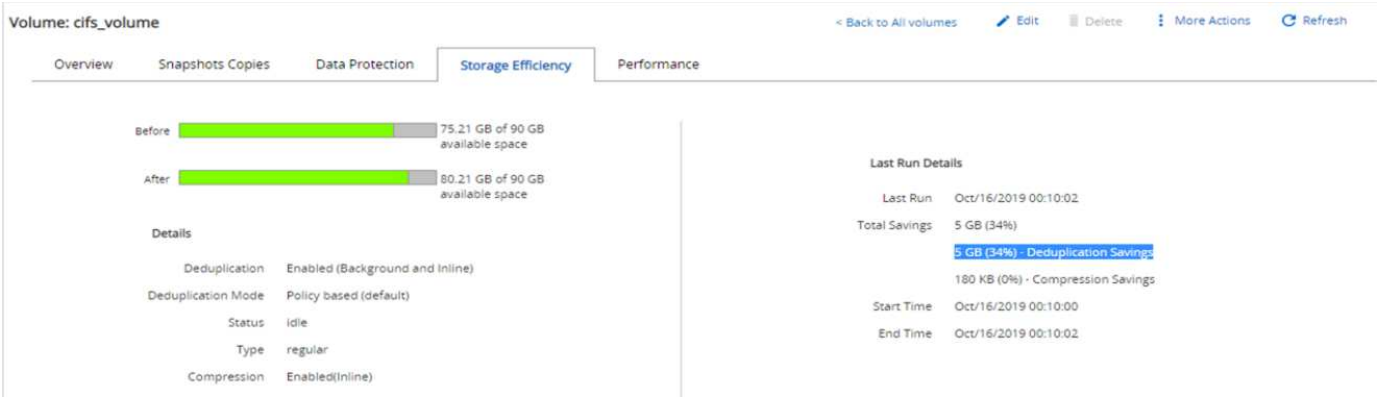
공격 중에 CIFS 공유를 호스팅하는 볼륨에서 스냅샷 크기가 820.98MB로 대폭 증가되는 것을 발견했습니다.



VM을 호스팅하는 볼륨에서 스냅샷 복사본 크기가 404.3MB로 증가되는 것을 발견했습니다.



CIFS 공유를 호스팅하는 볼륨의 스토리지 효율성이 34%로 감소했습니다.



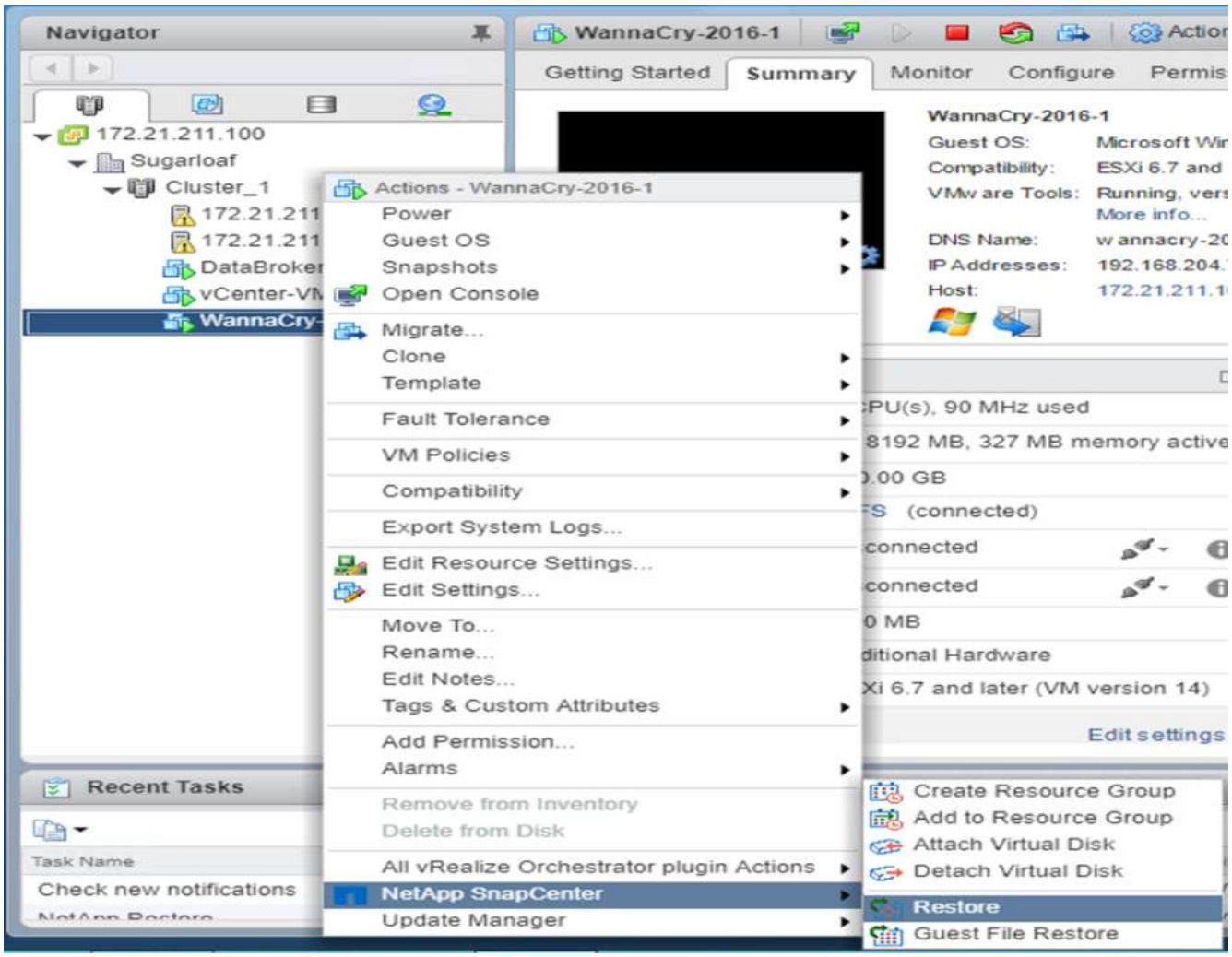
해결

공격 전에 생성된 클린 스냅샷 복사본을 사용하여 VM 및 매핑된 CIFS 공유를 복구합니다.

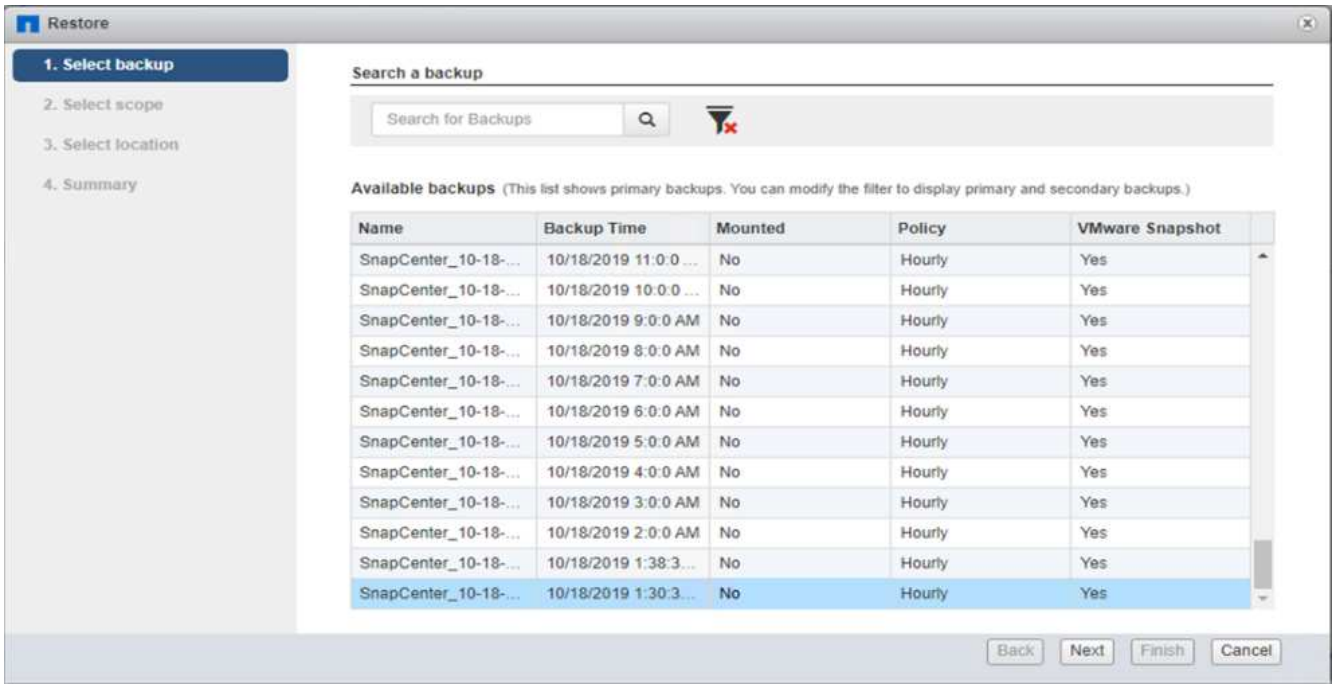
- VM 복원 *

VM을 복원하려면 다음 단계를 완료하십시오.

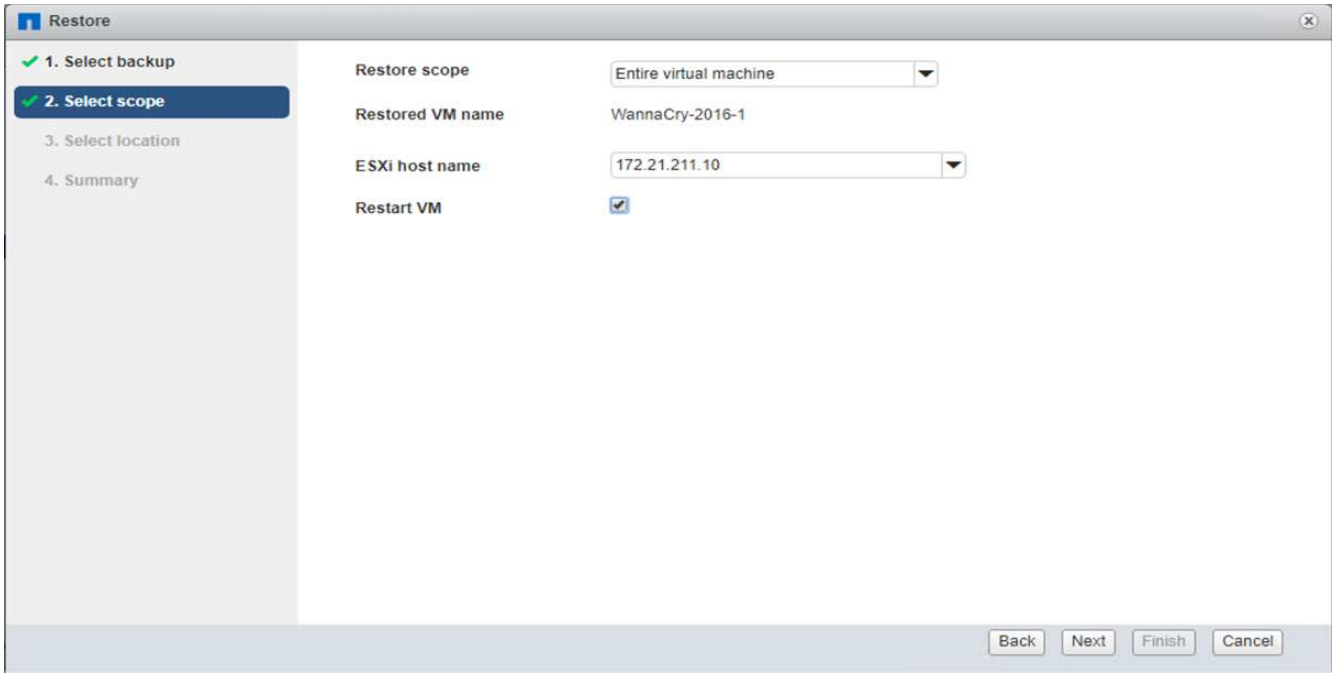
1. SnapCenter에서 생성한 스냅샷 복사본을 사용하여 VM을 복원합니다.



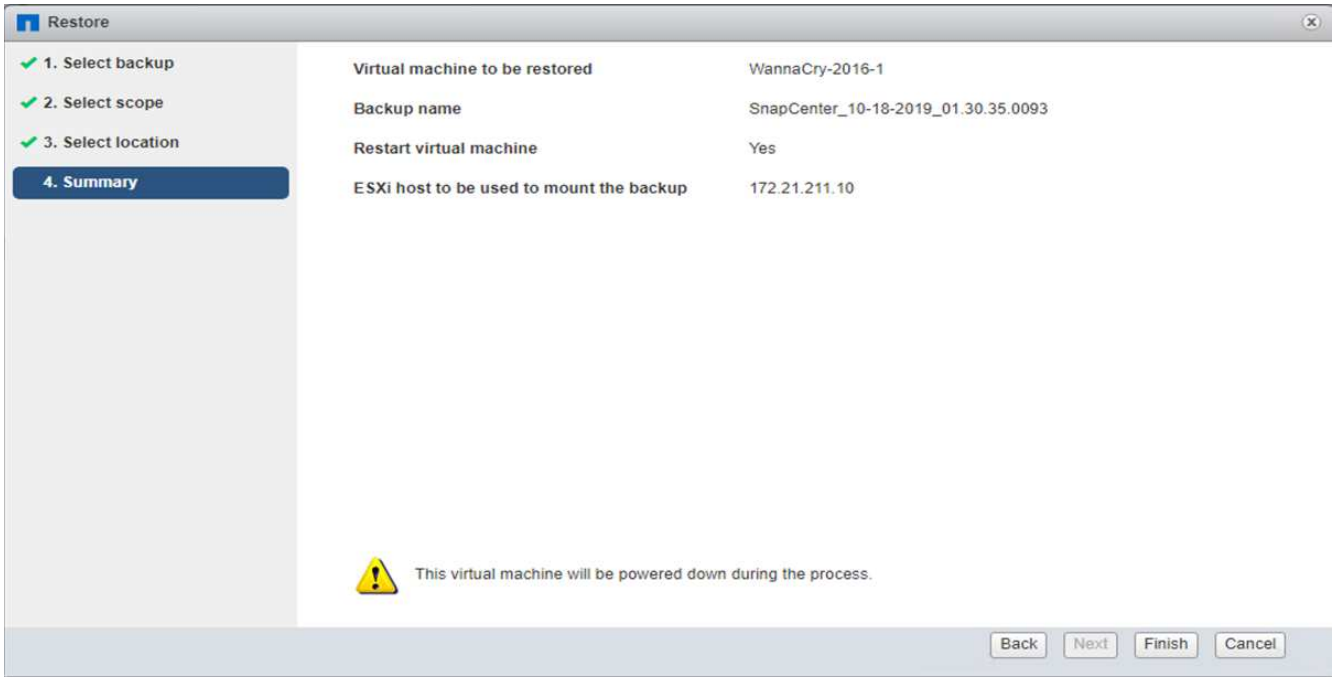
2. 복구할 VMware 정합성 보장 스냅샷 복사본을 선택합니다.



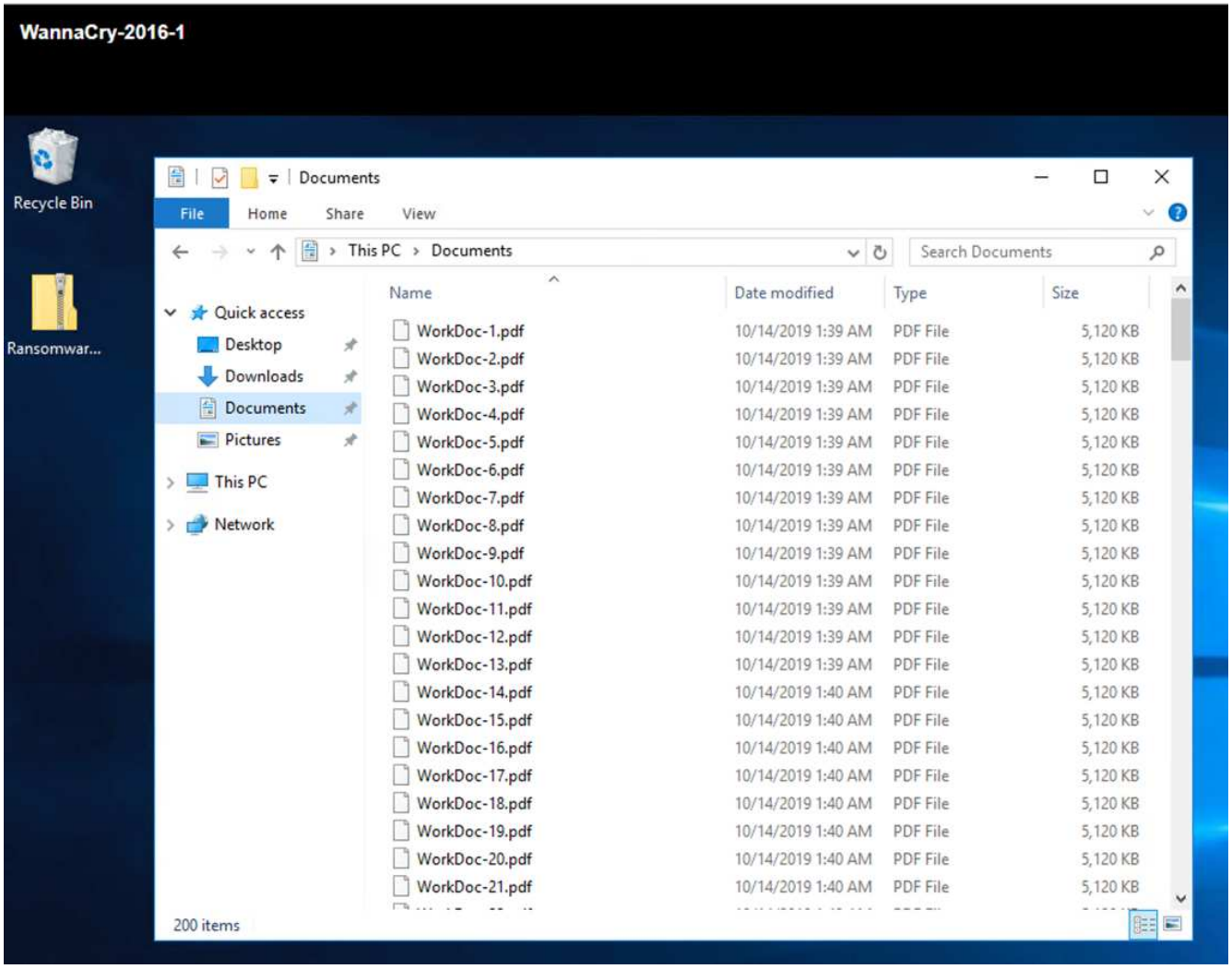
3. 전체 VM이 복원되고 다시 시작됩니다.



4. 마침 을 클릭하여 복원 프로세스를 시작합니다.



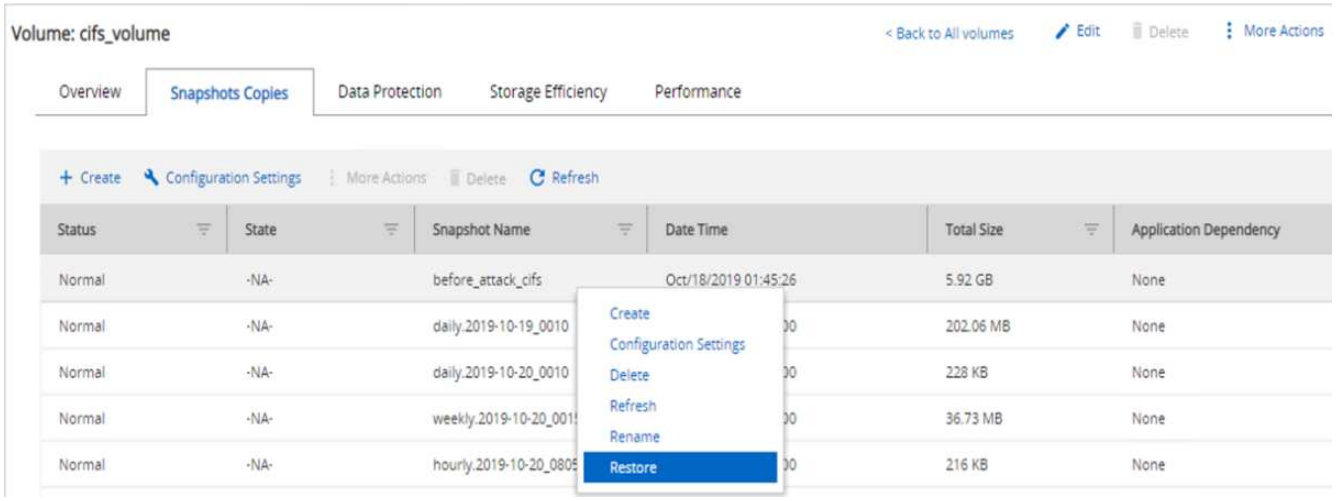
5. VM 및 해당 파일이 복원됩니다.



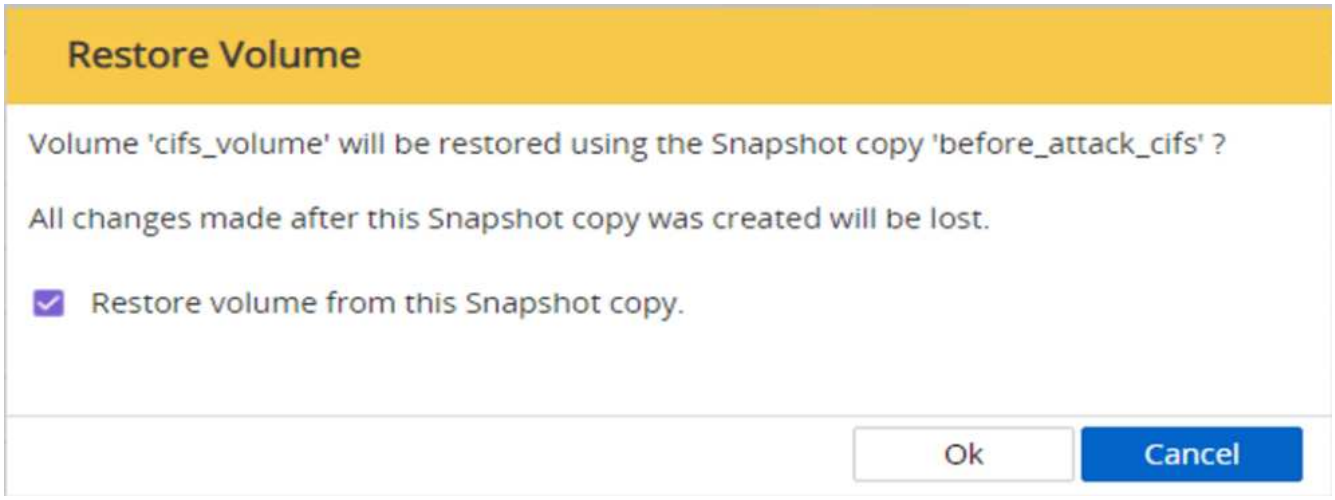
◦ CIFS 공유 복원 *

CIFS 공유를 복구하려면 다음 단계를 수행하십시오.

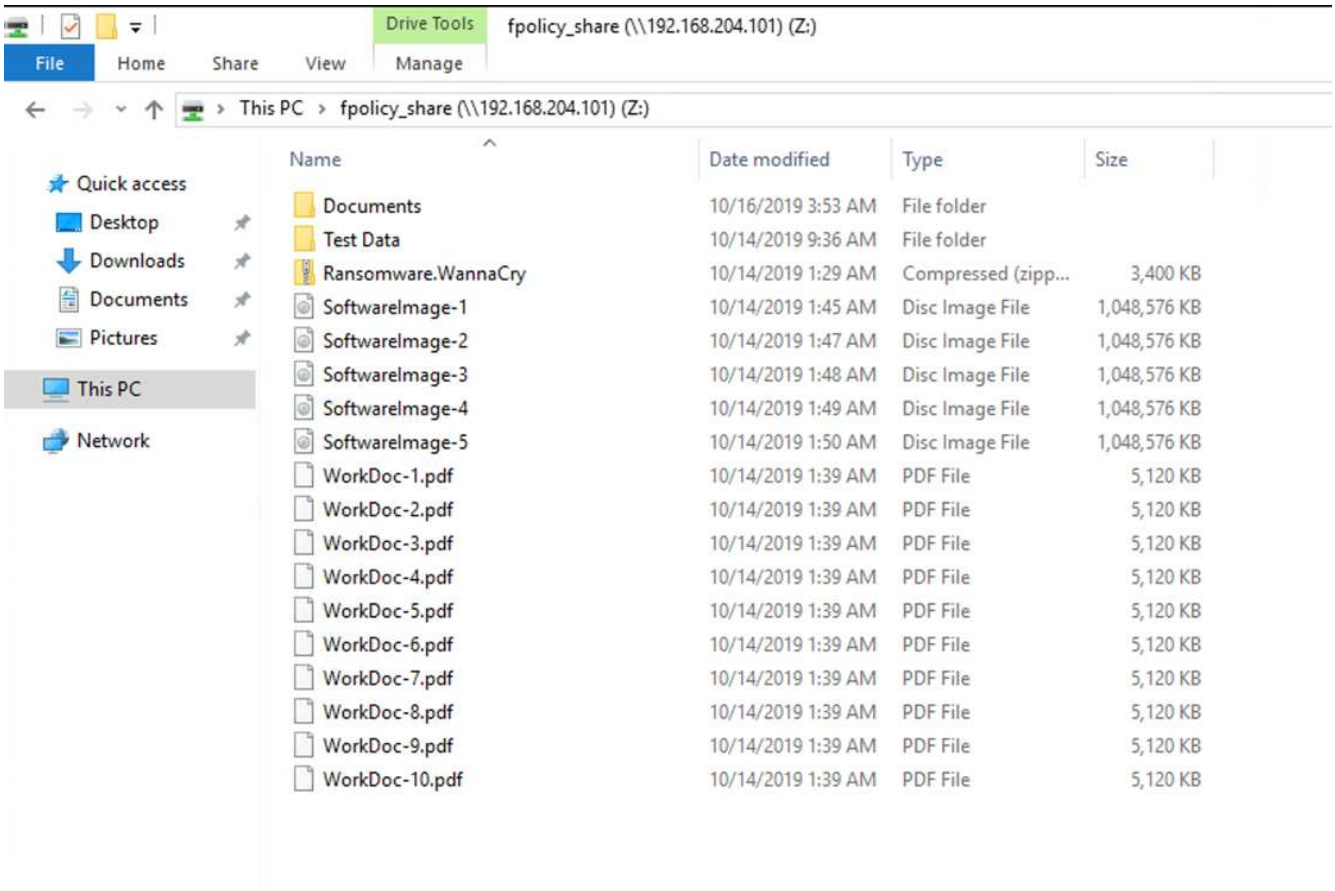
1. 공격 전에 생성된 볼륨의 스냅샷 복사본을 사용하여 공유를 복구합니다.



2. 확인 을 클릭하여 복원 작업을 시작합니다.



3. 복구 후 CIFS 공유를 봅니다.



사례 **2: WannaCry**는 **VM** 내의 파일 시스템을 암호화하고 **FPolicy**를 통해 보호되는 매핑된 **CIFS** 공유를 암호화합니다

예방

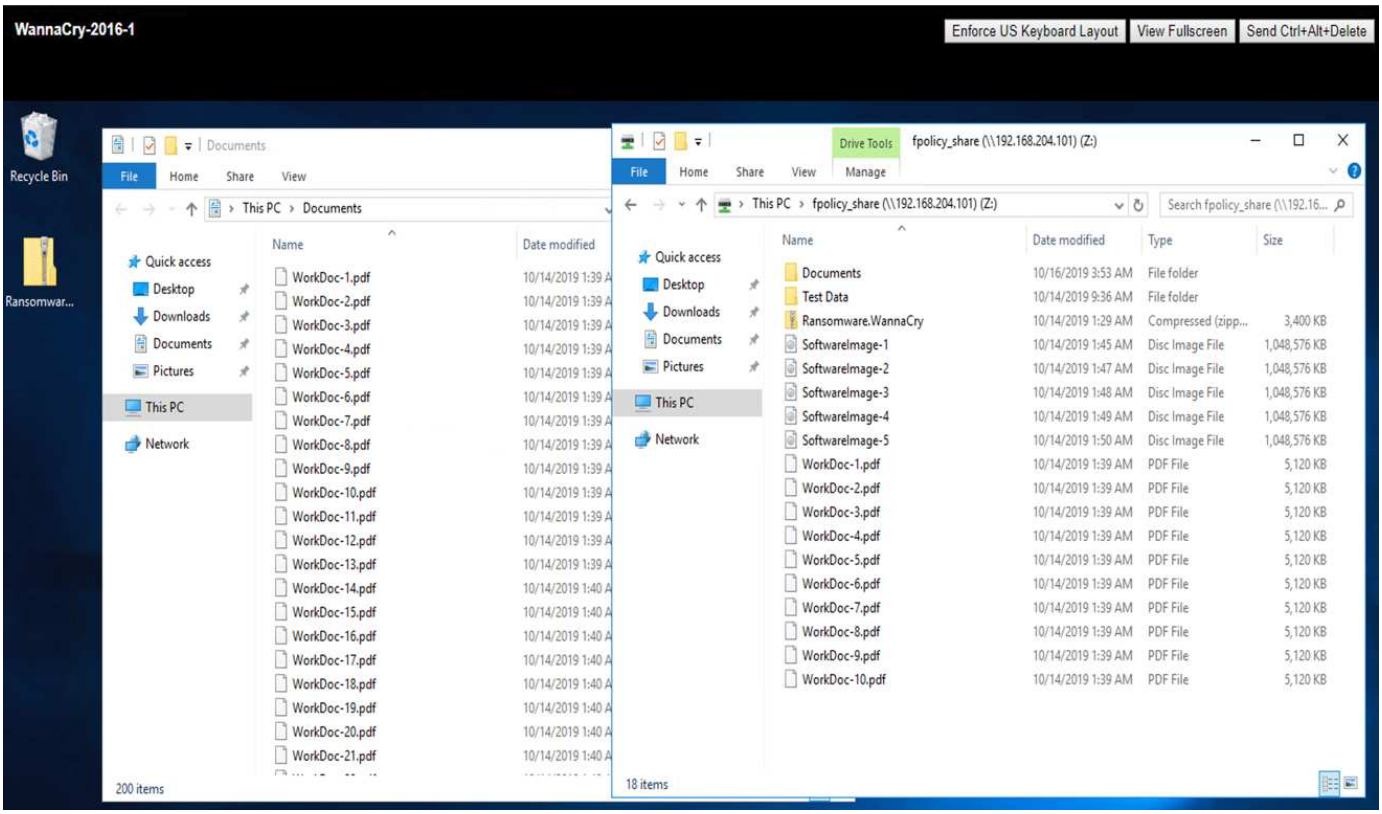
- FPolicy 구성 * 을 참조하십시오

CIFS 공유에서 FPolicy를 구성하려면 ONTAP 클러스터에서 다음 명령을 실행하십시오.

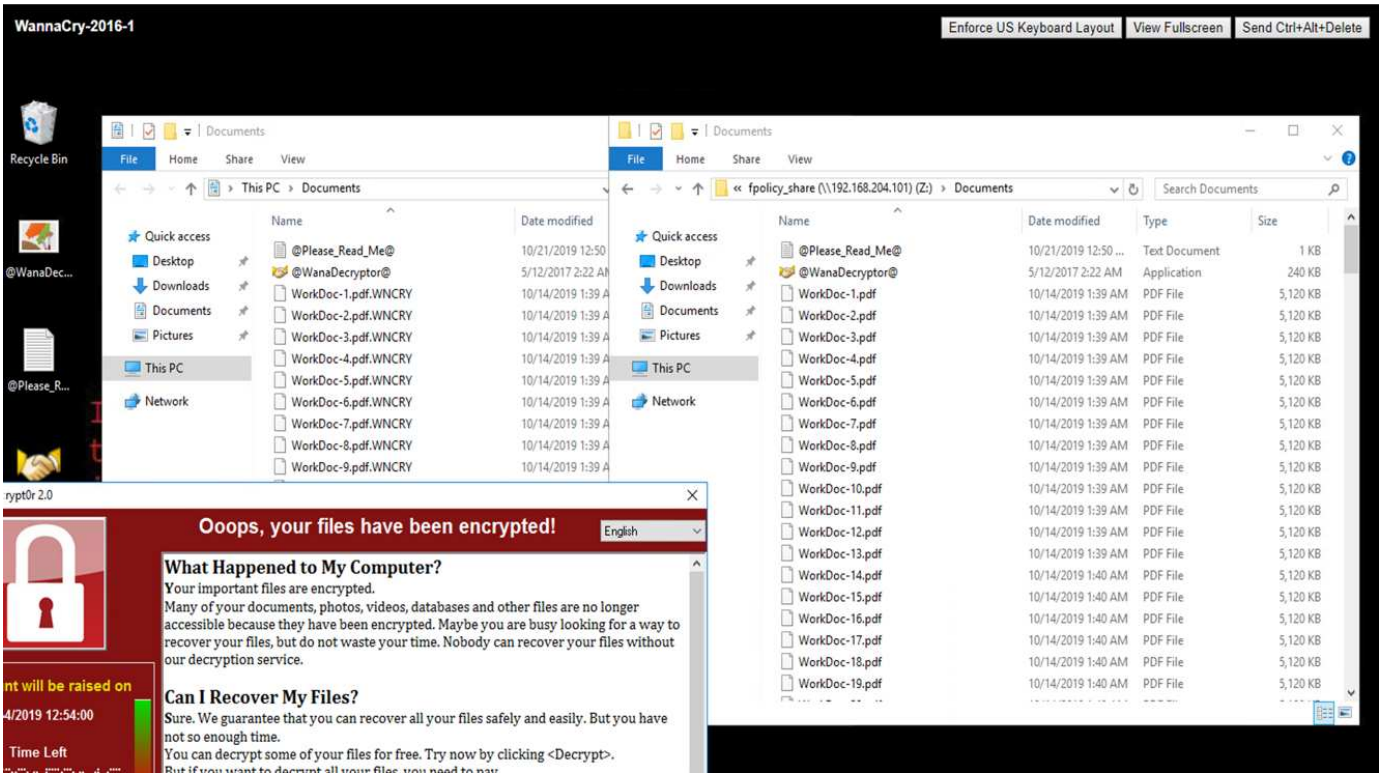
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -vserver infra_svm -policy-name
Ransomware_policy -shares-to-include fpolicy_share -file-extensions-to
-include WNCRY,Locky,ad4c
vserver fpolicy enable -vserver infra_svm -policy-name Ransomware_policy
-sequence-number 1
```

이 정책을 사용하면 WNCRY, Locky 및 ad4c 확장명을 가진 파일은 파일 생성, 이름 바꾸기, 쓰기 또는 열기 작업을 수행할 수 없습니다.

공격하기 전에 파일의 상태를 확인합니다. 암호화되지 않은 상태로 깨끗한 시스템에 있습니다.



VM의 파일은 암호화됩니다. WannaCry 맬웨어는 CIFS 공유의 파일을 암호화하려고 하지만 FPolicy는 파일이 영향을 받지 않도록 합니다.



대가를 지불하지 않고 비즈니스 운영을 지속하십시오

이 문서에 설명된 NetApp 기능은 공격 후 몇 분 내에 데이터를 복구하고 공격을 차단함으로써 비즈니스 운영을 방해받지 않고 계속할 수 있도록 합니다.

원하는 RPO(복구 시점 목표)를 충족하도록 스냅샷 복사본 스케줄을 설정할 수 있습니다. 스냅샷 복사본 기반 복원 작업은 매우 빠르게 수행되므로 RTO(복구 시간 목표)를 매우 짧게 달성할 수 있습니다.

무엇보다, 공격으로 인한 대가를 지불하지 않아도 되며, 신속하게 정상 운영으로 돌아갈 수 있습니다.

결론

랜섬웨어는 조직 범죄의 산물이며 공격자는 윤리적으로 행동하지 않습니다. 이들은 돈을 받은 후에도 암호 해독 키를 제공하지 않을 수 있습니다. 피해자는 데이터를 잃을 뿐만 아니라 상당한 금액의 돈까지 잃게 되고 운영 데이터의 손실로 인한 결과에 직면하게 됩니다.

에 따르면 "Forbes 기사를 참조하십시오"랜섬웨어 피해자 중 오직 19%만 대가를 지불한 후 데이터를 돌려받습니다. 따라서 공격자는 공격 시 대가를 지불하지 않는 것이 좋습니다. 대가를 지불하면 비즈니스 모델에 대한 믿음을 강화할 수 있기 때문입니다.

데이터 백업 및 복원 작업은 랜섬웨어 복구의 중요한 부분입니다. 따라서 비즈니스 계획의 필수 요소로 포함되어야 합니다. 이러한 작업의 구현 예산을 책정하여 공격 발생 시 복구 기능에 영향을 주지 않도록 해야 합니다.

중요한 것은 이 과정에서 올바른 기술 파트너를 선택하는 것입니다. FlexPod은 기본적으로 All-Flash FAS 시스템에서 추가 비용 없이 필요한 기능을 대부분 제공합니다.

감사의 말

저자는 이 문서 작성에 도움을 주신 다음 분들께 감사 드립니다.

- Jorge Gomez Navarrete, NetApp
- NetApp, Ganesh Kamath

추가 정보

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

- NetApp Snapshot 소프트웨어

  "https://www.netapp.com/us/products/platform-os/snapshot.aspx"

- SnapCenter 백업 관리

  "https://www.netapp.com/us/products/backup-recovery/snapcenter-backup-management.aspx"

- SnapLock 데이터 규정 준수

  "https://www.netapp.com/us/products/backup-recovery/snaplock-compliance.aspx"

- NetApp 제품 설명서

  "https://www.netapp.com/us/documentation/index.aspx"

- Cisco AMP(Advanced Malware Protection)

  "https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html"

- Cisco Stealthwatch

  "https://www.cisco.com/c/en_in/products/security/stealthwatch/index.html"

FIPS 140-2 Security-호환 FlexPod 솔루션을 통한 의료 서비스 지원

TR-4892: FIPS 140-2 Security-compliant FlexPod solution for healthcare

Cisco의 NetApp John McAbel, JayaKishore Esanakula

경제 및 임상 보건법(HITECH)을 위한 의료 정보 기술(Health Information Technology for Economic and Clinical Health Act, HITECH)에는 전자 보호 건강 정보(ePHI)에 대한 FIPS(Federal Information Processing Standard) 140-2의 검증된 암호화가 필요합니다. Hit(Health Information Technology) 애플리케이션 및 소프트웨어는 FIPS 140-2를 준수하여 프로모션 상호 운용성 프로그램(이전의 의미 있는 사용 인센티브 프로그램) 인증을 취득해야 합니다. 자격을 갖춘 제공자 및 병원은 Medicare 및 Medicaid 인센티브를 받을 때 FIPS 140-2(Level 1) 준수 히트(Hit)를 사용하고 중앙 의료보험 및 메디케이드(Center for Medicare and

Medicaid, CMS)에서 보상금 부과를 방지해야 합니다. FIPS 140-2 인증 암호화 알고리즘은 에 따라 필요한 기술 보호 수단으로서 제공됩니다 "보안 규칙" HIPAA(Health Information Portability and Accountability Act).

FIPS 140-2는 미국 중요한 정보를 보호하는 하드웨어, 소프트웨어 및 펌웨어의 암호화 모듈에 대한 보안 요구 사항을 설정하는 정부 표준입니다. 표준 준수는 미국 정부가 사용하도록 규정하고 있습니다 금융 서비스 및 의료와 같은 규제 대상 산업에서도 자주 사용됩니다. 이 기술 보고서를 통해 독자는 FIPS 140-2 보안 표준을 높은 수준에서 이해할 수 있습니다. 또한 의료 기관이 직면한 다양한 위협을 청중이 이해하는 데 도움이 됩니다. 마지막으로, 기술 보고서를 통해 FlexPod 통합 인프라에 FIPS 140-2 규격 FlexPod 시스템을 구축하여 의료 자산을 보호하는 방법을 파악할 수 있습니다.

범위

이 문서는 FIPS 140-2 보안 규정을 준수해야 하는 하나 이상의 의료 IT 애플리케이션 또는 솔루션을 호스팅하기 위한 Cisco Unified Computing System(Cisco UCS), Cisco Nexus, Cisco MDS 및 NetApp ONTAP 기반 FlexPod 인프라의 기술 개요입니다.

대상

이 문서는 의료 산업의 기술 리더 및 Cisco와 NetApp 파트너 솔루션 엔지니어 및 프로페셔널 서비스 직원을 위한 것입니다. NetApp은 사용자가 컴퓨팅 및 스토리지 사이징 개념을 잘 이해하고 있을 뿐만 아니라 의료 위협, 의료 보안, 의료 IT 시스템, Cisco UCS 및 NetApp 스토리지 시스템에 대한 기술적 지식을 갖추고 있다고 가정합니다.

"다음은 의료 분야의 사이버 보안 위협입니다."

의료 분야의 사이버 보안 위협

"이전: 소개."

모든 문제는 새로운 기회를 제공합니다. COVID 범세계적 확산으로 인해 이러한 기회 중 하나가 발생할 수 있습니다. 에 따르면 "보고서" HHS(Department of Health and Human Services) 사이버 보안 프로그램을 통해 COVID 대응은 랜섬웨어 공격 횟수를 늘렸습니다. 2020년 3월 셋째 주에 등록된 새로운 인터넷 도메인은 6,000개에 달했습니다. 도메인 중 50% 이상이 맬웨어를 호스팅했습니다. 랜섬웨어 공격은 2020년 전체 의료 데이터 침해의 거의 50%를 차지하여 630개 이상의 의료 조직과 약 2,900만 개의 의료 기록에 영향을 주었습니다. 19개의 침공자/현장은 갈취의 두 배가 되었습니다. 24.5%에 의료 산업에서는 2020년에 데이터 유출 사고가 가장 많이 발생하였습니다.

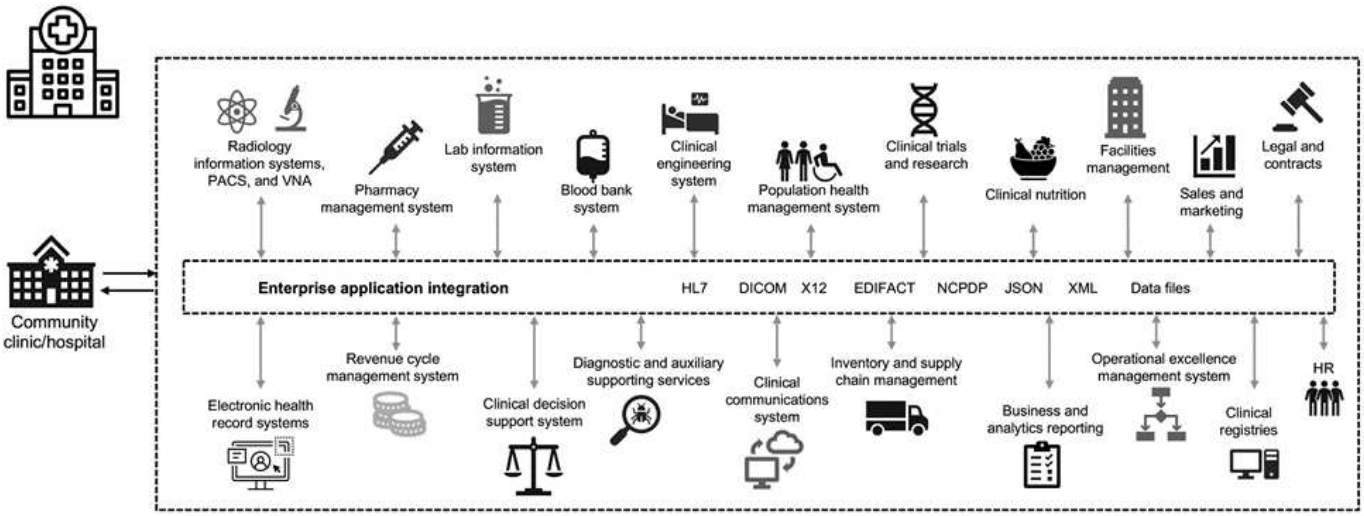
악의적인 요원들이 정보를 판매하거나 이를 파괴하거나 노출시키겠다고 위협하여 PHI(Protected Health Information)의 보안 및 개인 정보를 침해하려고 시도했습니다. ePHI에 대한 무단 접근을 위해 대상 및 대량 방송 시도가 자주 이루어집니다. 2020년 하반기에 노출된 환자 기록의 약 75%는 업무 관계자가 피해를 본 덕분이었습니다.

다음 의료 조직 목록은 악의적인 에이전트의 표적이 되었습니다.

- 병원 시스템
- 생명 과학 연구소
- 연구 랩
- 재활 시설

- 지역 병원 및 클리닉

의료 기관을 구성하는 애플리케이션의 다양성은 부인할 수 없으며 복잡성이 증가하고 있습니다. 정보 보안 사무소는 방대한 IT 시스템 및 자산에 대한 거버넌스를 제공해야 하는 과제를 안고 있습니다. 다음 그림은 일반적인 병원 시스템의 임상적 기능을 보여줍니다.



환자 데이터가 이 영상의 중심에 있습니다. 환자 데이터 손실 및 민감한 의학적 상태와 관련된 오인은 매우 현실적입니다. 기타 중요한 문제로는 사회적 부담보, 협박메일, 프로파일링, 대상 마케팅, 악용, 지불자의 특권 이외의 의료 정보에 대한 지불자에 대한 잠재적인 재정적 책임 등이 있습니다.

의료에 대한 위협은 본질적으로 다차원적이며 영향을 줍니다. 전 세계 정부들은 ePHI를 보호하기 위해 다양한 규정을 제정했습니다. 의료 위협 요소의 해로운 영향과 진화하는 특성으로 인해 의료 기관은 모든 위협을 방어하기가 어렵습니다.

다음은 의료 분야에서 확인된 일반적인 위협 목록입니다.

- 랜섬웨어 공격
- 민감한 정보가 있는 장비 또는 데이터의 손실 또는 도난
- 피싱 공격
- 환자 안전에 영향을 줄 수 있는 연결된 의료 기기에 대한 공격
- 전자 메일 피싱 공격
- 장비 또는 데이터의 손실 또는 도난
- 원격 데스크톱 프로토콜 손상
- 소프트웨어 취약점

의료 조직은 디지털 에코시스템과 같이 복잡한 법률 및 규정 환경에서 사업을 운영하고 있습니다. 이 환경에는 다음이 포함되지만 이에 국한되지는 않습니다.

- 국립보건조정관(의료 기술용) ONC 인증 전자보건정보기술상호운용성 표준
- Medicare 액세스 및 아동 건강 보험 프로그램 재허가 법(MACRA)/의미 있는 사용
- FDA(Food and Drug Administration)에 따른 다수의 의무
- 공동 위원회 인증 프로세스

- HIPAA 요구 사항
- HITECH 요구 사항
- 지불자의 최소 허용 위험 기준
- 개인 정보 보호 및 보안 규칙
- 연방 정보 보안 현대화 법안 요구 사항 연방 계약 및 연구 보조금은 국가 보건원 등의 기관을 통해 통합됩니다
- PCI-DSS(Payment Card Industry Data Security Standard)
- 약물 남용 및 정신 건강 서비스 관리(SAMHSA) 요건
- 재무 처리를 위한 Gramm-Leach-Bliley Act
- Stark 법률은 제휴 조직에 서비스를 제공하는 것과 관련이 있습니다
- 고등 교육에 참여하는 기관을 위한 가족교육권 및 개인정보보호법(FERPA)
- 유전정보차별금지법(GINA)
- EU의 새로운 GDPR(General Data Protection Regulation)

악의적 행위자가 의료 정보 시스템에 영향을 주지 않도록 보안 아키텍처 표준이 빠르게 발전하고 있습니다. 이러한 표준 중 하나는 NIST(National Institute of Standards and Technology)에서 정의한 FIPS 140-2입니다. FIPS 140-2 은 미국에 대해 자세히 설명합니다 암호화 모듈에 대한 정부 요구 사항 보안 요구 사항은 암호화 모듈의 보안 설계 및 구현과 관련된 영역을 다루며, 보안 요구 사항을 적용하여 보안 기능을 강화할 수 있습니다. 잘 정의된 암호화 경계를 통해 암호화 모듈을 최신 상태로 유지하면서 보안 관리를 쉽게 수행할 수 있습니다. 이러한 경계는 악의적인 행위자가 쉽게 악용할 수 있는 약한 암호화 모듈을 방지하는 데 도움이 됩니다. 또한 표준 암호화 모듈을 관리할 때 인적 오류를 방지할 수 있습니다.

NIST는 CSE(Communications Security Establishment)와 함께 FIPS 140-2 검증 수준에 대한 암호화 모듈을 인증하기 위해 CMVP(Cryptographic Module Validation Program)를 설립했습니다. FIPS 140-2 인증 모듈을 사용하는 연방 조직은 이동 중에도 기밀 또는 가치 있는 데이터를 보호해야 합니다. 민감하거나 중요한 정보를 보호하는 데 성공했기 때문에 많은 의료 시스템이 법적으로 요구되는 최소 보안 수준 이상으로 FIPS 140-2 암호화 모듈을 사용하여 ePHI를 암호화하기로 결정했습니다.

FlexPod FIPS 140-2 기능을 활용하여 구현하는 데 몇 시간(며칠이 아님)만 걸립니다. FIPS를 준수하는 것은 규모와 관계없이 대부분의 의료 조직에서 가능합니다. 암호화 경계가 명확하게 정의되고 문서화되고 간단한 구현 단계를 통해 FIPS 140-2 규격 FlexPod 아키텍처는 인프라를 위한 견고한 보안 기반을 마련하고 보안 위협에 대한 보호 수준을 더욱 높이기 위해 간단한 개선 기능을 제공할 수 있습니다.

"다음: FIPS 140-2의 개요"

FIPS 140-2 개요

"이전: 의료 분야의 사이버 보안 위협"

"FIPS 140-2" 컴퓨터 및 통신 시스템의 중요한 정보를 보호하는 보안 시스템 내에서 사용되는 암호화 모듈에 대한 보안 요구 사항을 지정합니다. 암호화 모듈은 하드웨어, 소프트웨어, 펌웨어 또는 조합 세트여야 합니다. FIPS는 암호화 경계 내에 포함된 암호화 알고리즘, 키 생성 및 키 관리자에 적용됩니다. FIPS 140-2는 제품, 아키텍처, 데이터 또는 에코시스템이 아닌 암호화 모듈에 특히 적용된다는 점을 이해하는 것이 중요합니다. 이 문서의 뒷부분에 나오는 주요 용어로 정의된 암호화 모듈은 승인된 보안 기능을 구현하는 특정 구성 요소(하드웨어, 소프트웨어 및 /또는 펌웨어)입니다. 또한 FIPS 140-2는 네 가지 레벨을 지정합니다. 승인된 암호화 알고리즘은

모든 수준에 공통적입니다. 각 보안 수준의 주요 요소 및 요구 사항은 다음과 같습니다.

- * 보안 수준 1 *
  - 암호화 모듈에 대한 기본 보안 요구 사항을 지정합니다(하나 이상의 승인된 알고리즘 또는 보안 기능이 필요함).
  - 운영 등급 구성 요소의 기본 요구 사항을 초과하는 수준 1에는 지정된 물리적 보안 메커니즘이 필요하지 않습니다.
- * 보안 수준 2 *
  - 코팅 또는 봉인, 탈착식 커버 또는 암호화 모듈의 도어에 잠금 장치와 같은 변조 방지 솔루션을 사용하여 변조 증거에 대한 요구 사항을 추가하여 물리적 보안 메커니즘을 강화합니다.
  - 최소한 역할 기반 액세스 제어(RBAC)가 필요하며, 이 경우 암호화 모듈은 운영자 또는 관리자의 권한을 인증하여 특정 역할을 수행하고 해당 기능 세트를 수행해야 합니다.
- * 보안 수준 3 *
  - 레벨 2의 변조 가능한 요구 사항을 기반으로 암호화 모듈 내의 중요 보안 매개 변수(CSP)에 대한 추가 액세스를 방지합니다.
  - 수준 3에 필요한 물리적 보안 메커니즘은 물리적 액세스 시도 또는 암호화 모듈의 사용 또는 수정 시도를 감지하고 이에 대응할 가능성이 높은 것을 목적으로 합니다. 암호화 모듈의 이동식 덮개가 열릴 때 모든 일반 텍스트 CSP를 제로화하는 강력한 인클로저, 변조 감지 및 응답 회로가 이러한 예에 포함될 수 있습니다.
  - 레벨 2에 지정된 RBAC 메커니즘의 보안을 강화하기 위해 ID 기반 인증 메커니즘이 필요합니다. 암호화 모듈은 운영자의 ID를 인증하고 운영자가 역할을 사용하고 역할의 기능을 수행할 권한이 있는지 확인합니다.
- * 보안 수준 4 *
  - FIPS 140-2의 최고 보안 수준.
  - 물리적으로 보호되지 않는 환경에서 작업을 수행하는 데 가장 유용한 레벨입니다.
  - 이 수준에서 물리적 보안 메커니즘은 물리적 액세스에서 승인되지 않은 시도를 감지하고 대응하는 책임을 지고 암호화 모듈에 대한 완벽한 보호를 제공하기 위한 것입니다.
  - 암호화 모듈의 침투 또는 노출은 감지 가능성이 높으며 모든 비보안 또는 일반 텍스트 CSP의 즉각적인 제로로 이어질 수 있습니다.

"다음: 컨트롤 플레인 대 데이터 플레인"

컨트롤 플레인 대 데이터 플레인

"이전: FIPS 140-2의 개요"

FIPS 140-2 전략을 구현할 때는 어떤 것이 보호되고 있는지 이해하는 것이 중요합니다. 컨트롤 플레인과 데이터 플레인의 두 영역으로 쉽게 나눌 수 있습니다. 제어 계층이란 FlexPod 시스템 내에서 구성 요소의 제어 및 운영에 영향을 미치는 측면, 예를 들어 NetApp 스토리지 컨트롤러, Cisco Nexus 스위치, Cisco UCS 서버에 대한 관리 액세스 권한을 말합니다. 이 계층의 보호는 관리자가 장치에 연결하고 변경할 때 사용할 수 있는 프로토콜과 암호화 사이퍼를 제한함으로써 제공됩니다. 데이터 플레인은 FlexPod 시스템 내의 PHI와 같은 실제 정보를 나타냅니다. 이는 저장된 데이터를 암호화하고 FIPS를 위해 다시 암호화하여 보호하므로 사용 중인 암호화 모듈이 표준을 충족하도록 합니다.

"다음으로, FlexPod Cisco UCS 컴퓨팅 및 FIPS 140-2를 살펴보겠습니다."

FlexPod Cisco UCS 컴퓨팅 및 FIPS 140-2

"이전: 컨트롤 플레인 대 데이터 플레인"

FlexPod 아키텍처는 FIPS 140-2를 준수하는 Cisco UCS 서버로 설계할 수 있습니다. 미국 S. NIST, Cisco UCS 서버는 FIPS 140-2 레벨 1 준수 모드에서 작동할 수 있습니다. FIPS 호환 Cisco 구성 요소의 전체 목록은 을 참조하십시오 "Cisco의 FIPS 140 페이지". Cisco UCS Manager는 FIPS 140-2 검증을 거쳤습니다.

Cisco UCS 및 패브릭 인터커넥트

Cisco UCS Manager는 Cisco Fabric Interconnect(FI)에서 구축 및 실행됩니다.

Cisco UCS 및 FIPS 활성화 방법에 대한 자세한 내용은 를 참조하십시오 "Cisco UCS Manager 설명서".

각 패브릭 A 및 B의 Cisco 패브릭 인터커넥트에서 FIPS 모드를 활성화하려면 다음 명령을 실행합니다.

```
fp-health-fabric-A# connect local-mgmt
fp-health-fabric-A(local-mgmt)# enable fips-mode
FIPS mode is enabled
```

Cisco UCS Manager 릴리즈 3.2(3)의 클러스터에서 Cisco UCS Manager 릴리즈 3.2(3) 이전 릴리즈의 FI로 FI를 교체하려면 교체 FI를 클러스터에 추가하기 전에 기존 FI에서 FIPS 모드(FIPS 모드 비활성화)를 비활성화하십시오. Cisco UCS Manager의 부팅 과정에서 클러스터가 구성되면 FIPS 모드가 자동으로 설정됩니다.

Cisco는 컴퓨팅 또는 애플리케이션 계층에서 구현할 수 있는 다음과 같은 주요 제품을 제공합니다.

- * 엔드포인트용 Cisco AMP(Advanced Malware Protection).* Microsoft Windows 및 Linux 운영 체제에서 지원되는 이 솔루션은 예방, 검색 및 응답 기능을 통합합니다. 이 보안 소프트웨어는 침입을 방지하고 진입 지점에서 맬웨어를 차단하며 파일 및 프로세스 활동을 지속적으로 모니터링 및 분석하여 일선 방어를 우회할 수 있는 위협을 신속하게 탐지, 억제 및 해결합니다. AMP의 MAP(Malicious Activity Protection) 구성 요소는 모든 엔드포인트 활동을 지속적으로 모니터링하고 엔드포인트에서 실행 중인 프로그램의 비정상적인 동작을 런타임 감지 및 차단합니다. 예를 들어, 엔드포인트 동작에 랜섬웨어가 표시되면 문제가 되는 프로세스가 종료되어 엔드포인트 암호화가 예방되고 공격이 중지됩니다.
- 이메일 보안을 위한 * AMP. * 이메일은 맬웨어를 유포하고 사이버 공격을 수행하는 주요 수단으로 자리 잡았습니다. 평균적으로 하루 동안 약 1,000억 개의 이메일이 교환되며, 이를 통해 공격자들은 사용자 시스템에 대한 탁월한 침투 벡터를 얻을 수 있습니다. 따라서 이 공격 라인을 방어하는 것이 절대적으로 중요합니다. AMP는 제로 데이 익스플로잇(zero-day exploit) 및 악성 첨부 파일에 숨겨진 악성 맬웨어와 같은 위협에 대한 이메일을 분석합니다. 또한 업계 최고의 URL 인텔리전스를 사용하여 악성 링크를 차단합니다. 스피어 피싱, 랜섬웨어 및 기타 정교한 공격에 대한 고급 보호 기능을 제공합니다.
- * NGIPS(Next-Generation Intrusion Prevention System). * Cisco firepower NGIPS는 데이터 센터에서 물리적 어플라이언스로 구축하거나 VMware(NGIPSv for VMware)에서 가상 어플라이언스로 구축할 수 있습니다. 이 고효율 침입 방지 시스템은 안정적인 성능과 낮은 총 소유 비용을 제공합니다. AMP, 애플리케이션 가시성 및 제어, URL 필터링 기능을 제공하기 위해 선택적 구독 라이센스로 위협 보호를 확장할 수 있습니다. 가상화된 NGIPS는 VM(가상 시스템) 간의 트래픽을 검사하고 리소스가 제한된 사이트에서 NGIPS 솔루션을 쉽게 배포 및 관리할 수 있도록 하여 물리적 자산과 가상 자산 모두의 보호를 강화합니다.

"다음으로, FlexPod Cisco 네트워킹 및 FIPS 140-2가 있습니다."

FlexPod Cisco 네트워킹 및 FIPS 140-2

"이전: FlexPod Cisco UCS 컴퓨팅 및 FIPS 140-2가 지원됩니다."

Cisco MDS를 참조하십시오

소프트웨어 8.4.x가 포함된 Cisco MDS 9000 시리즈 플랫폼은 "FIPS 140-2 규격 준수". Cisco MDS는 SNMPv3 및 SSH에 대해 암호화 모듈 및 다음 서비스를 구현합니다.

- 각 서비스를 지원하는 세션 설정
- 각 서비스 키 파생 기능을 지원하는 모든 기본 암호화 알고리즘
- 각 서비스에 대한 해싱입니다
- 각 서비스의 대칭 암호화

FIPS 모드를 활성화하기 전에 MDS 스위치에서 다음 작업을 완료합니다.

1. 암호의 길이는 최소 8자 이상이어야 합니다.
2. 텔넷을 비활성화합니다. 사용자는 SSH만 사용하여 로그인해야 합니다.
3. RADIUS/TACACS+를 통해 원격 인증을 비활성화합니다. 스위치에 로컬로 있는 사용자만 인증을 받을 수 있습니다.
4. SNMP v1 및 v2를 비활성화합니다. SNMPv3에 대해 구성된 스위치의 기존 사용자 계정은 인증을 위해 SHA 와 개인 정보 보호를 위해 AES/3DES 로만 구성해야 합니다.
5. VRRP를 비활성화합니다.
6. 인증을 위해 MD5가 있거나 암호화를 위해 DES가 있는 모든 IKE 정책을 삭제합니다. 인증에 SHA를 사용하고 암호화에 3DES/AES를 사용하도록 정책을 수정합니다.
7. 모든 SSH 서버 RSA1 키 쌍을 삭제합니다.

FIPS 모드를 활성화하고 MDS 스위치에 FIPS 상태를 표시하려면 다음 단계를 수행하십시오.

1. FIPS 상태를 표시합니다.

```
MDSSwitch# show fips status
FIPS mode is disabled
MDSSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. 2048비트 SSH 키를 설정합니다.

```
MDSSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
MDSSwitch(config)# no ssh key
MDSSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
MDSSwitch(config)# ssh key
dsa   rsa
MDSSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. FIPS 모드를 활성화합니다.

```
MDSSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
```

4. FIPS 상태를 표시합니다.

```
MDSSwitch(config)# show fips status
FIPS mode is enabled
MDSSwitch(config)# feature ssh
MDSSwitch(config)# show feature | grep ssh
sshServer            1        enabled
```

5. 실행 중인 구성에 구성을 저장합니다.

```
MDSSwitch(config)# copy ru st
[##################################################] 100%
exitCopy complete.
MDSSwitch(config)# exit
```

6. MDS 스위치를 다시 시작합니다

```
MDSSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

7. FIPS 상태를 표시합니다.

```
Switch(config)# fips mode enable
Switch(config)# show fips status
```

자세한 내용은 을 참조하십시오 "FIPS 모드 활성화".

Cisco Nexus를 참조하십시오

Cisco Nexus 9000 시리즈 스위치(버전 9.3)는 "FIPS 140-2 규격 준수". Cisco Nexus는 SNMPv3 및 SSH에 대해 암호화 모듈 및 다음 서비스를 구현합니다.

- 각 서비스를 지원하는 세션 설정
- 각 서비스 키 파생 기능을 지원하는 모든 기본 암호화 알고리즘
- 각 서비스에 대한 해싱입니다
- 각 서비스의 대칭 암호화

FIPS 모드를 활성화하기 전에 Cisco Nexus 스위치에서 다음 작업을 완료하십시오.

1. 텔넷을 비활성화합니다. 사용자는 SSH(Secure Shell)만 사용하여 로그인해야 합니다.
2. SNMPv1 및 v2를 비활성화합니다. SNMPv3에 대해 구성된 장치의 기존 사용자 계정은 인증을 위해 SHA 와 개인 정보 보호를 위해 AES/3DES 로만 구성해야 합니다.
3. 모든 SSH 서버 RSA1 키 쌍을 삭제합니다.
4. Cisco TrustSec 보안 연결 프로토콜(SAP) 협상 중에 사용할 HMAC-SHA1 메시지 무결성 검사(MIC)를 활성화합니다. 이렇게 하려면 CTS-MANUAL 또는 CTS-dot1x 모드에서 SAP hash-algorithm HMAC-SHA-1 명령을 입력한다.

Nexus 스위치에서 FIPS 모드를 활성화하려면 다음 단계를 수행하십시오.

1. 2048비트 SSH 키를 설정합니다.

```
NexusSwitch# show fips status
FIPS mode is disabled
NexusSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. 2048비트 SSH 키를 설정합니다.

```
NexusSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
NexusSwitch(config)# no ssh key
NexusSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
NexusSwitch(config)# ssh key
dsa   rsa
NexusSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. FIPS 모드를 활성화합니다.

```
NexusSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
Show fips status
NexusSwitch(config)# show fips status
FIPS mode is enabled
NexusSwitch(config)# feature ssh
NexusSwitch(config)# show feature | grep ssh
sshServer             1        enabled
Save configuration to the running configuration
NexusSwitch(config)# copy ru st
[########################################] 100%
exitCopy complete.
NexusSwitch(config)# exit
```

4. Nexus 스위치를 다시 시작합니다.

```
NexusSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

5. FIPS 상태를 표시합니다.

```
NexusSwitch(config)# fips mode enable
NexusSwitch(config)# show fips status
```

또한 Cisco NX OS 소프트웨어는 네트워크 이상 및 보안 검색을 향상시키는 NetFlow 기능을 지원합니다. NetFlow는 네트워크의 모든 대화 메타데이터, 통신 관련 당사자, 사용 중인 프로토콜 및 트랜잭션 기간을 캡처합니다. 정보를 집계 및 분석한 후에는 정상적인 동작에 대한 통찰력을 제공할 수 있습니다. 또한 수집된 데이터를 통해 네트워크를 통해 확산되는 맬웨어와 같은 의심스러운 활동 패턴을 식별할 수 있으며, 그렇지 않을 경우 이를 간과할 수 있습니다. NetFlow는 흐름을 사용하여 네트워크 모니터링에 대한 통계를 제공합니다. 흐름은 소스 인터페이스(또는 VLAN)에 도착하고 키에 대해 동일한 값을 갖는 패킷의 단방향 스트림입니다. 키는 패킷 내의 필드에 대해 식별된 값입니다. 유동 레코드를 사용하여 유동의 고유 키를 정의하는 유동을 만듭니다. 흐름 내보내기를 사용하여 Cisco Stealthwatch와 같은 원격 NetFlow 수집기로 플로우에 대해 NetFlow에서 수집하는 데이터를 내보낼 수 있습니다. Stealthwatch는 이 정보를 사용하여 네트워크를 지속적으로 모니터링하고 랜섬웨어 발생 시 실시간 위협 탐지 및 사고 대응 법의학 조사를 제공합니다.

"다음으로, FlexPod NetApp ONTAP 스토리지와 FIPS 140-2를 살펴보겠습니다."

FlexPod NetApp ONTAP 스토리지 및 FIPS 140-2

"이전: FlexPod Cisco 네트워킹 및 FIPS 140-2."

NetApp은 다양한 하드웨어, 소프트웨어 및 서비스를 제공하며, 여기에는 표준에 따라 검증된 암호화 모듈의 다양한 구성요소가 포함될 수 있습니다. 따라서 NetApp은 제어 플레인 및 데이터 플레인을 위해 FIPS 140-2 규정 준수를 위한 다양한 접근 방식을 사용합니다.

- NetApp에는 전송 중인 데이터 및 유휴 데이터의 암호화에 대한 레벨 1 검증을 획득한 암호화 모듈이 포함되어 있습니다.
- NetApp은 FIPS 140-2 검증을 거친 하드웨어 및 소프트웨어 모듈을 모두 인수합니다. 예를 들어, NetApp Storage Encryption 솔루션은 FIPS 레벨 2 인증 드라이브를 활용합니다.
- NetApp 제품은 제품 또는 기능이 검증 범위 내에 있지 않더라도 표준을 준수하는 방법으로 검증된 모듈을 사용할 수 있습니다. 예를 들어, NetApp Volume Encryption(NVE)은 FIPS 140-2 규정을 준수합니다. 이 솔루션은 개별적으로 검증되지 않았지만 레벨 1의 검증된 NetApp 암호화 모듈을 활용합니다. 사용 중인 ONTAP 버전에 대한 규정 준수 사항을 자세히 알아보려면 FlexPod SME에게 문의하십시오.
- NetApp 암호화 모듈은 FIPS 140-2 레벨 1의 검증을 거쳤습니다 *
- NetApp CSM(Cryptographic Security Module)은 FIPS 140-2 레벨 1의 검증을 거쳤습니다.
- NetApp 자체 암호화 드라이브는 FIPS 140-2 레벨 2의 검증을 거쳤습니다 *

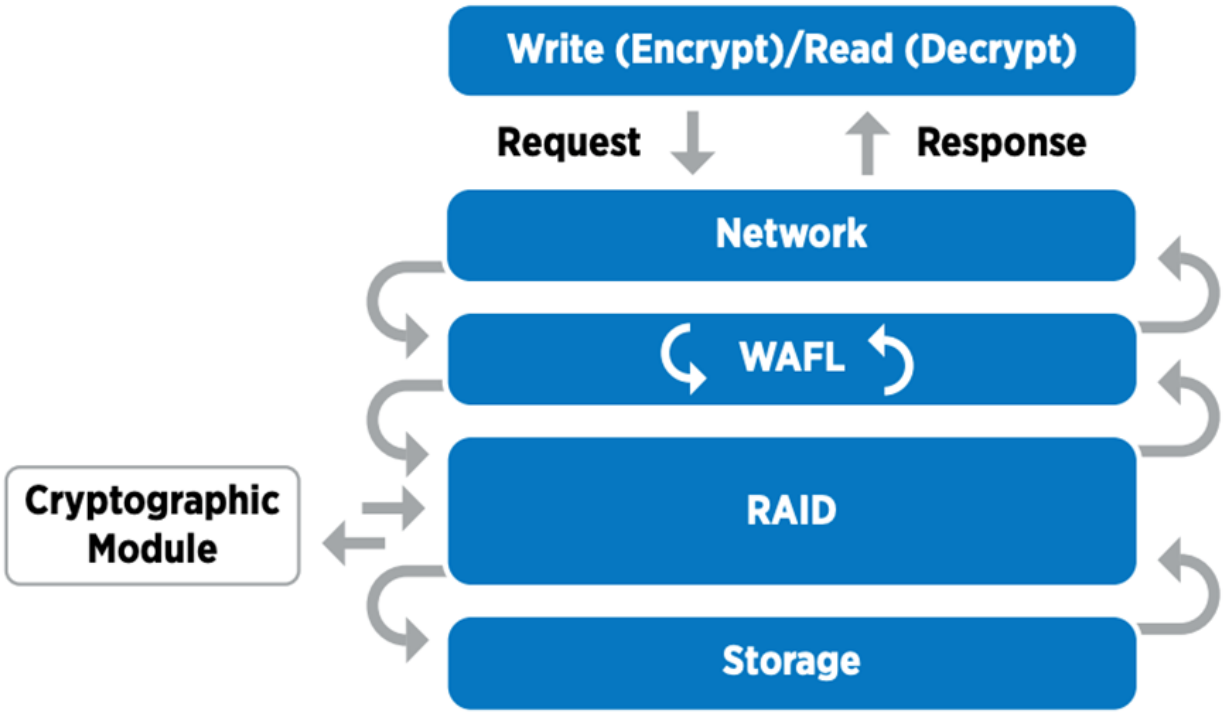
NetApp은 FIPS 140-2 검증을 거친 SED(자체 암호화 드라이브)를 OEM(Original Equipment Manufacturer)에서 구입합니다. 이러한 드라이브를 찾는 고객은 주문 시 드라이브를 지정해야 합니다. 드라이브는 레벨 2에서 검증됩니다. 다음 NetApp 제품은 검증된 SED를 활용할 수 있습니다.

- AFF A-Series 및 FAS 스토리지 시스템
- E-Series 및 EF-Series 스토리지 시스템을 구축합니다
- NetApp 애그리게이트 암호화 및 NetApp 볼륨 암호화 *

NVE 및 NetApp Aggregate Encryption(NAE) 기술을 사용하면 볼륨 및 애그리게이트 레벨에서 데이터를 암호화할 수 있으므로 솔루션이 물리적 드라이브에 제한되지 않습니다.

NVE는 ONTAP 9.1부터 사용 가능한 소프트웨어 기반의 유휴 데이터 암호화 솔루션이며 ONTAP 9.2 이후 FIPS 140-2를 준수합니다. NVE를 사용하면 ONTAP가 각 볼륨의 데이터를 세부적으로 암호화할 수 있습니다. ONTAP 9.6과 함께 제공되는 NAE는 NVE의 성장이 앞서며, ONTAP가 각 볼륨의 데이터를 암호화할 수 있으며 볼륨이 애그리게이트 전체에서 키를 공유할 수 있습니다. NVE와 NAE는 모두 AES 256비트 암호화를 사용합니다. SED가 없는 디스크에도 데이터를 저장할 수 있습니다. NVE와 NAE를 사용하면 암호화가 사용되는 경우에도 스토리지 효율성 기능을 사용할 수 있습니다. 애플리케이션 계층만 암호화하면 스토리지 효율성의 모든 이점을 누릴 수 없습니다. NVE와 NAE를 사용하면 데이터가 NetApp WAFL를 통해 네트워크에서 RAID 계층으로 전송되기 때문에 스토리지 효율성이 유지되고 데이터의 암호화 여부가 결정됩니다. 스토리지 효율성을 높이기 위해 NAE에서 애그리게이트 중복제거를 사용할 수 있습니다. NVE 볼륨과 NAE 볼륨이 동일한 NAE 애그리게이트에 공존할 수 있습니다. NAE 애그리게이트는 암호화되지 않은 볼륨을 지원하지 않습니다.

프로세스는 다음과 같이 진행됩니다. 데이터가 암호화되면 FIPS 140-2 레벨 1의 유효성이 검증된 암호화 모듈로 전송됩니다. 암호화 모듈은 데이터를 암호화하고 RAID 계층으로 다시 전송합니다. 그런 다음 암호화된 데이터가 디스크로 전송됩니다. 따라서 NVE와 NAE를 결합하여 데이터를 디스크로 이미 암호화할 수 있습니다. 읽기는 반대 경로를 따릅니다. 즉, 데이터가 암호화된 상태로 남아 RAID로 전송되고 암호화 모듈에 의해 해독되며 다음 그림과 같이 스택의 나머지 부분까지 전송됩니다.



NVE는 FIPS 140-2 레벨 1의 검증된 소프트웨어 암호화 모듈을 사용합니다.

NVE에 대한 자세한 내용은 를 "NVE 데이터시트"참조하십시오.

NVE는 클라우드의 데이터를 보호합니다. Cloud Volumes ONTAP 및 Azure NetApp Files는 FIPS 140-2 규격 데이터 암호화를 유휴 상태에서 제공할 수 있습니다.

ONTAP 9.7부터 NVE 라이센스와 온보드 또는 외부 키 관리가 있을 때 새로 생성된 애그리게이트 및 볼륨이 기본적으로 암호화됩니다. ONTAP 9.6부터 애그리게이트 레벨 암호화를 사용하여 암호화할 볼륨의 포함된 애그리게이트에 키를 할당할 수 있습니다. Aggregate에서 생성한 볼륨은 기본적으로 암호화됩니다. 볼륨을 암호화할 때 기본값을 재정의할 수 있습니다.

ONTAP NAE CLI 명령

다음 CLI 명령을 실행하기 전에 클러스터에 필요한 NVE 라이센스가 있는지 확인하십시오.

Aggregate를 생성하여 암호화하려면 다음 명령을 실행합니다(ONTAP 9.6 이상의 클러스터 CLI에서 실행 시).

```
fp-health::> storage aggregate create -aggregate aggregatename -encrypt
-with-aggr-key true
```

NAE가 아닌 애그리게이트를 NAE A aggregate로 변환하려면 다음 명령을 실행합니다(ONTAP 9.6 및 이후 클러스터 CLI에서 실행되는 경우).

```
fp-health::> storage aggregate modify -aggregate aggregatename  -node
svmname -encrypt-with-aggr-key true
```

NAE 애그리게이트를 NAE가 아닌 aggregate로 변환하려면 다음 명령을 실행하십시오(ONTAP 9.6 이상의 클러스터 CLI에서 실행되는 경우).

```
fp-health::> storage aggregate modify -aggregate aggregatename -node
svmname -encrypt-with-aggr-key false
```

ONTAP NVE CLI 명령

ONTAP 9.6부터 애그리게이트 레벨 암호화를 사용하여 암호화할 볼륨의 포함된 애그리게이트에 키를 할당할 수 있습니다. Aggregate에서 생성한 볼륨은 기본적으로 암호화됩니다.

NAE가 활성화된 애그리게이트에서 볼륨을 생성하려면 다음 명령을 실행합니다(ONTAP 9.6 및 이후 클러스터 CLI에서 실행되는 경우).

```
fp-health::> volume create -vserver svmname -volume volumename -aggregate
aggregatename -encrypt true
```

볼륨 이동 없이 기존 볼륨 "제자리에" 암호화를 활성화하려면 다음 명령을 실행합니다(ONTAP 9.6 이상 클러스터 CLI에서 실행 시).

```
fp-health::> volume encryption conversion start -vserver svmname -volume
volumename
```

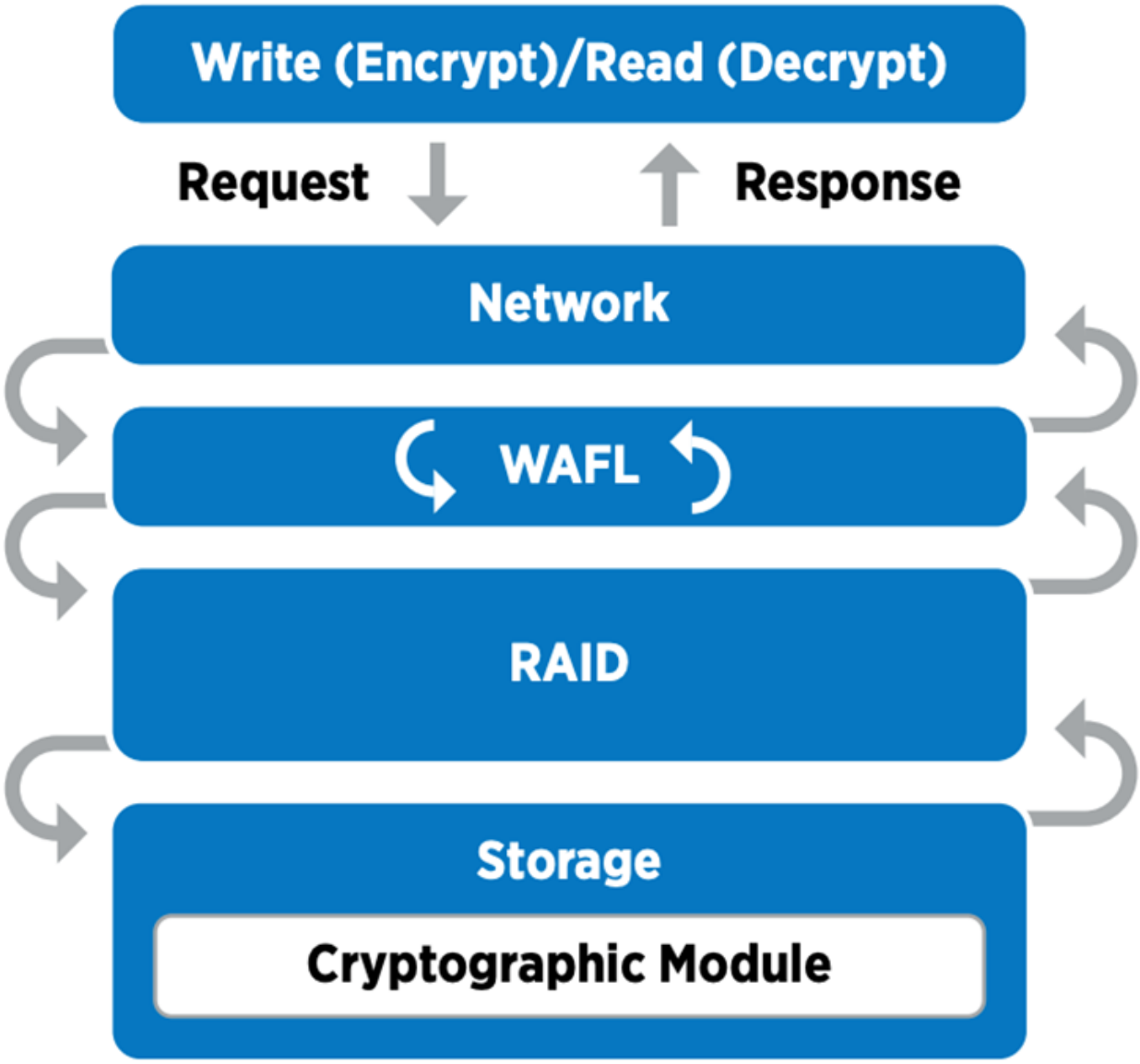
볼륨에 암호화가 설정되어 있는지 확인하려면 다음 CLI 명령을 실행합니다.

```
fp-health::> volume show -is-encrypted true
```

NSE를 선택합니다

NSE는 SED를 사용하여 하드웨어 가속 메커니즘을 통해 데이터 암호화를 수행합니다.

NSE는 AES 256비트 투명 디스크 암호화를 통해 유휴 데이터를 보호하여 규정 준수 및 스페어 반환을 지원하도록 FIPS 140-2 레벨 2 자체 암호화 드라이브를 구성합니다. 드라이브는 암호화 키 생성을 포함하여 다음 그림에 설명된 대로 내부적으로 모든 데이터 암호화 작업을 수행합니다. 데이터에 대한 무단 액세스를 방지하기 위해 스토리지 시스템은 드라이브를 처음 사용할 때 설정된 인증 키를 사용하여 드라이브에서 자체적으로 인증해야 합니다.



NSE는 FIPS 140-2 레벨 2의 검증된 각 드라이브에서 하드웨어 암호화를 사용합니다.

NSE에 대한 자세한 내용은 를 "NSE 데이터시트"참조하십시오.

키 관리

FIPS 140-2 표준은 다음 그림과 같이 경계에서 정의한 암호화 모듈에 적용됩니다.

2.1.1 Cryptographic Boundary

The logical cryptographic boundary of the CryptoMod module is the cryptomod_fips.ko component of ONTAP OS kernel. The logical boundary is depicted in the block diagram below. The Approved DRBG is used to supply the module's cryptographic keys. The physical boundary for the module is the enclosure of the NetApp controller.

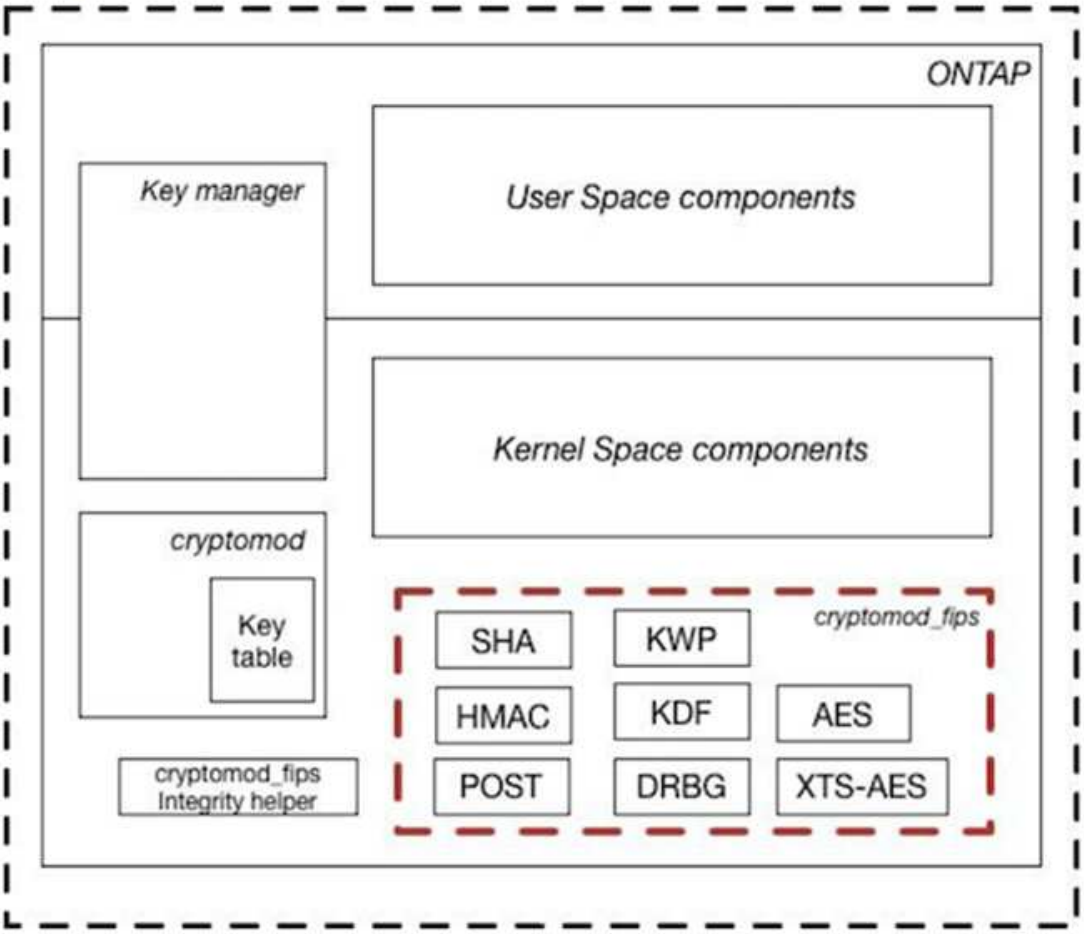


Figure 1 - Block Diagram

키 관리자는 ONTAP에서 사용하는 모든 암호화 키를 추적합니다. NSE SED는 키 관리자를 사용하여 NSE SED의 인증 키를 설정합니다. 키 관리자를 사용할 때 NVE와 NAE의 결합된 솔루션은 소프트웨어 암호화 모듈, 암호화 키 및 키 관리자로 구성됩니다. NVE는 각 볼륨에 대해 키 관리자가 저장하는 고유한 XTS-AES 256 데이터 암호화 키를 사용합니다. 데이터 볼륨에 사용되는 키는 해당 클러스터의 데이터 볼륨에 고유하며 암호화된 볼륨이 생성될 때 생성됩니다. 마찬가지로 NAE 볼륨은 집합당 고유한 XTS-AES 256 데이터 암호화 키를 사용하며 키 관리자도 이 암호화 키를 저장합니다. NAE 키는 암호화된 Aggregate가 생성될 때 생성됩니다. ONTAP는 키를 미리 생성하거나 다시 사용하거나 일반 텍스트로 표시하지 않습니다. 키는 키 관리자에 의해 저장 및 보호됩니다.

외부 키 관리자 지원

ONTAP 9.3부터 외부 키 관리자는 NVE 솔루션과 NSE 솔루션 모두에서 지원됩니다. FIPS 140-2 표준은 특정 공급업체의 구현에 사용되는 암호화 모듈에 적용됩니다. 대부분의 경우 FlexPod 및 ONTAP 고객은 에 따라 다음 검증 중 하나를 사용합니다 "NetApp 상호 운용성 매트릭스") 주요 관리자:

- Gemalto 또는 SafeNet AT
- 보메트릭(목요일)

- IBM SKLM
- Utimaco(이전의 Microfocus, HPE)

NSE 및 NVMe SED 인증 키는 업계 표준 OASIS KMIP(Key Management Interoperability Protocol)를 사용하여 외부 키 관리자에 백업됩니다. 스토리지 시스템, 드라이브 및 키 관리자만이 키에 액세스할 수 있으며, 보안 도메인 외부로 드라이브를 이동하면 드라이브 잠금을 해제할 수 없으므로 데이터 유출을 방지할 수 있습니다. 외부 키 관리자는 NVE 볼륨 암호화 키와 NAE 애그리게이트 암호화 키도 저장합니다. 컨트롤러와 디스크가 더 이상 외부 키 관리자에 액세스할 수 없는 경우, NVE 및 NAE 볼륨은 액세스할 수 없으며 해독할 수 없습니다.

다음 명령 예에서는 외부 키 관리자가 SVM(Store Virtual Machine)의 vmname1"에 사용하는 서버 목록에 두 개의 키 관리 서버를 추가합니다.

```
fp-health::> security key-manager external add-servers -vserver svmname1
-key-servers 10.0.0.20:15690, 10.0.0.21:15691
```

ONTAP는 멀티테넌시 시나리오에서 FlexPod 데이터 센터를 사용 중인 경우 SVM 레벨에서 보안상의 이유로 테넌시를 제공하여 사용자를 지원합니다.

외부 키 관리자 목록을 확인하려면 다음 CLI 명령을 실행합니다.

```
fp-health::> security key-manager external show
```

이중 암호화를 위한 암호화 결합(계층화된 방어)

데이터에 대한 액세스를 격리하고 데이터를 항상 보호해야 하는 경우 NSE SED를 네트워크 또는 패브릭 수준 암호화와 결합할 수 있습니다. NSE SED는 관리자가 상위 수준 암호화를 구성하거나 잘못 구성하는 경우 백스톱처럼 작동합니다. 두 개의 개별 암호화 계층의 경우 NSE SED를 NVE 및 NAE와 결합할 수 있습니다.

NetApp ONTAP 클러스터 전체에서 데이터 제어 플레인 **FIPS** 모드를 지원합니다

NetApp ONTAP 데이터 관리 소프트웨어에는 고객을 위해 추가 보안 수준을 인스턴스화하는 FIPS 모드 구성이 있습니다. 이 FIPS 모드는 컨트롤 평면에만 적용됩니다. FIPS 모드가 활성화되면 FIPS 140-2의 주요 요소에 따라 전송 계층 보안 v1(TLSv1) 및 SSLv3이 비활성화되고 TLS v1.1 및 TLS v1.2만 활성화됩니다.

FIPS 모드의 ONTAP 클러스터 전체 제어 창은 FIPS 140-2 레벨 1을 준수합니다. 클러스터 전체 FIPS 모드는 NCSM에서 제공하는 소프트웨어 기반 암호화 모듈을 사용합니다.

클러스터 전체 컨트롤 플레인을 위한 FIPS 140-2 규정 준수 모드는 ONTAP의 모든 제어 인터페이스를 보호합니다. 기본적으로 FIPS 140-2 전용 모드는 비활성화되어 있지만 '보안 구성 수정' 명령에 대해 'is-FIPS-enabled' 매개 변수를 'true'로 설정하여 이 모드를 활성화할 수 있습니다.

ONTAP 클러스터에서 FIPS 모드를 활성화하려면 다음 명령을 실행합니다.

```
fp-health::> security config modify -interface SSL -is-fips-enabled true
```

SSL FIPS 모드가 활성화되면 ONTAP에서 외부 클라이언트 또는 ONTAP 외부의 서버 구성 요소로의 SSL 통신은 SSL을 위해 FIPS 컴플레인 암호화를 사용합니다.

전체 클러스터에 대해 FIPS 상태를 표시하려면 다음 명령을 실행합니다.

```
fp-health::> set advanced
fp-health::*> security config modify -interface SSL -is-fips-enabled true
```

"다음으로, FlexPod 통합 인프라의 솔루션 이점에 대해 알아보십시오."

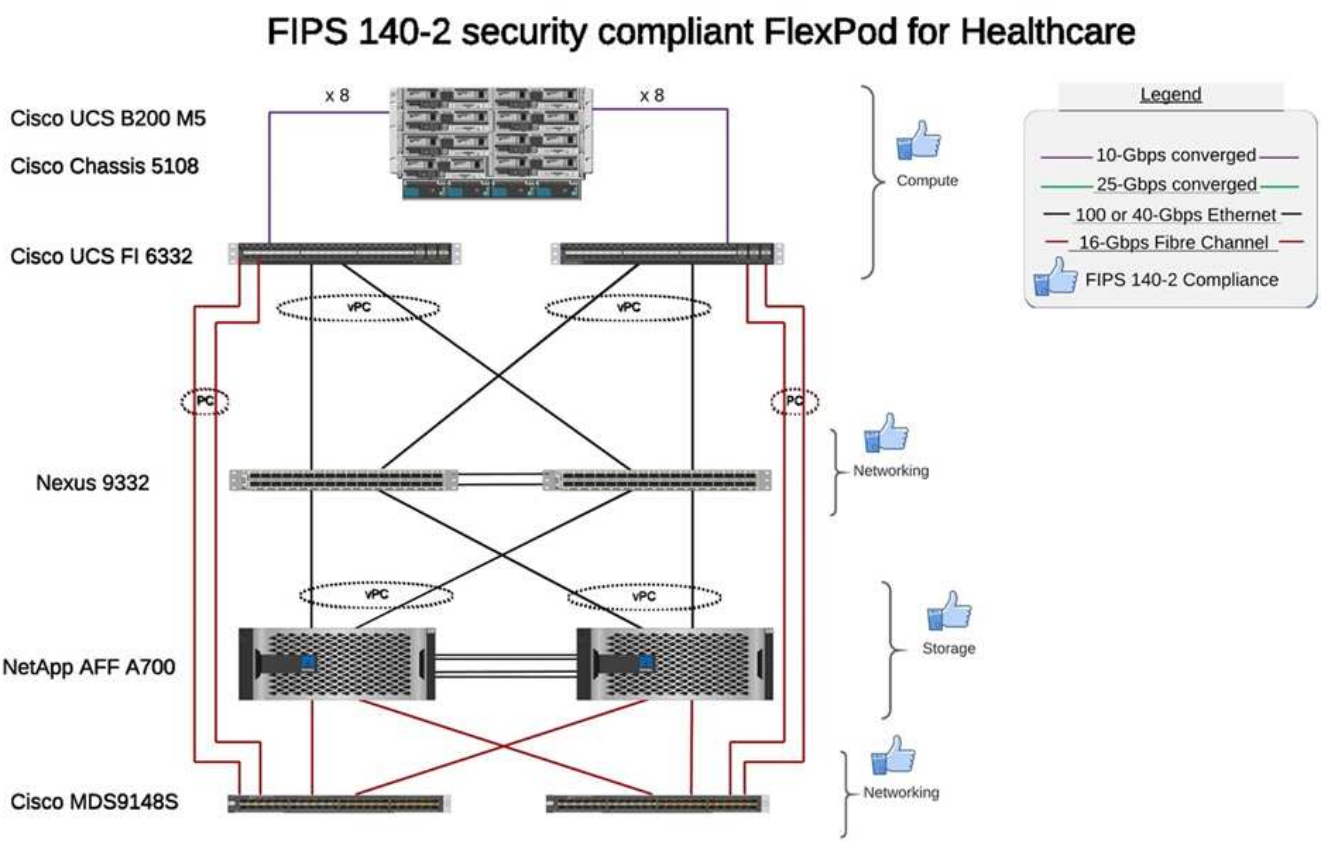
FlexPod 통합 인프라의 솔루션 이점

"이전:FlexPod NetApp ONTAP 스토리지 및 FIPS 140-2가 있습니다."

의료 조직에는 몇 가지 미션 크리티컬 시스템이 있습니다. 가장 중요한 시스템 두 가지는 EHR(전자 건강 기록) 시스템과 의료 영상 시스템입니다. FlexPod 시스템에서 FIPS 설정을 시연하기 위해 FlexPod 시스템에서 랩 설정 및 워크로드 검증을 위해 오픈 소스 EHR과 오픈 소스 사진 아카이빙 및 통신 시스템(PACS) 시스템을 사용했습니다. EHR 기능, EHR 논리적 애플리케이션 구성 요소 및 EHR 시스템을 FlexPod 시스템에 구현할 경우 EHR 시스템이 어떤 이점을 누릴 수 있는지 보려면 을 참조하십시오 "TR-4881: 전자 건강 기록 시스템용 FlexPod". 의료 영상 시스템 기능, 논리적 응용 프로그램 구성 요소 및 의료 영상 시스템이 FlexPod에 구현될 때 어떤 이점을 얻을 수 있는지 전체 목록은 를 참조하십시오 "TR-4865: 의료 영상용 FlexPod".

FIPS 설정 및 워크로드 검증 과정에서 NetApp은 일반적인 의료 기관을 대표하는 워크로드 특성을 실행했습니다. 예를 들어, 오픈 소스 EHR 시스템을 사용하여 현실적인 환자 데이터 액세스 및 변경 시나리오를 포함했습니다. 또한 ' * 에서 디지털 이미징 및 의료(DICOM) 개체 통신 등의 의료 영상 작업 부하를 행사했습니다. DCM의 파일 형식입니다. 메타데이터가 있는 DICOM 객체가 파일 및 블록 스토리지에 모두 저장되었습니다. 또한 가상화된 RedHat Enterprise Linux(RHEL) 서버 내에서 다중 경로 기능을 구현했습니다. NFS에 DICOM 객체, iSCSI를 사용하여 마운트된 LUN 및 FC를 사용하여 마운트된 LUN을 저장했습니다. FIPS 설정 및 검증 중에 FlexPod 통합 인프라가 당사의 기대치를 초과하고 원활하게 수행된다는 것을 확인했습니다.

다음 그림은 FIPS 설정 및 검증에 사용되는 FlexPod 시스템을 보여 줍니다. 우리는 을 활용했습니다 "VMware vSphere 7.0 및 NetApp ONTAP 9.7을 사용하는 FlexPod 데이터 센터 CVD(Cisco Validated Design)" 설치 프로세스 중



솔루션 인프라 하드웨어 및 소프트웨어 구성 요소

다음 두 그림은 FlexPod에서 FIPS 테스트를 수행할 때 각각 사용되는 하드웨어 및 소프트웨어 구성 요소를 나열합니다. 이러한 표의 권장사항은 예이며, NetApp SME와 협력하여 해당 구성요소가 귀사에 적합한지 확인해야 합니다. 또한 에서 구성 요소 및 버전이 지원되는지 확인합니다 "NetApp 상호 운용성 매트릭스 툴" (IMT) 및 "Cisco HCL(하드웨어 호환 목록)".

레이어	제품군	수량 및 모델	세부 정보
컴퓨팅	Cisco UCS 5108 섀시	1 또는 2	
	Cisco UCS 블레이드 서버	3 B200 M5	각각 20개 이상의 코어, 2.7GHz 및 128-384GB RAM이 있습니다
	Cisco UCS 가상 인터페이스 카드(VIC)	Cisco UCS 1440	를 참조하십시오
	Cisco UCS Fabric 인터커넥트 2개	6332	-
네트워크	Cisco Nexus 스위치	2x Cisco Nexus 9332	-
스토리지 네트워크	SMB/CIFS, NFS 또는 iSCSI 프로토콜을 통한 스토리지 액세스를 위한 IP 네트워크	위와 동일한 네트워크 스위치	-
	FC를 통한 스토리지 액세스	Cisco MDS 9148S 2개	-

레이어	제품군	수량 및 모델	세부 정보
스토리지	NetApp AFF A700 All-Flash 스토리지 시스템	클러스터 1개	2개의 노드로 클러스터
	디스크 쉘프	DS224C 또는 NS224 디스크 쉘프 1개	24개 드라이브로 완전히 채워집니다
	SSD를 지원합니다	>24, 1.2TB 이상의 용량	-

소프트웨어	제품군	버전 또는 릴리스	세부 정보
다양하다	리눅스	RHEL 7.X를 참조하십시오	-
	Windows	Windows Server 2012 R2(64비트)	-
	NetApp ONTAP를 참조하십시오	ONTAP 9.7 이상	-
	Cisco UCS 6120 패브릭 인터커넥트	Cisco UCS Manager 4.1 이상	-
	Cisco 이더넷 3000 또는 9000 시리즈 스위치	9000 시리즈, 7.0(3) i7(7) 이상(3000 시리즈, 9.2(4) 이상	-
	Cisco FC: Cisco MDS 9132T	8.4(1a) 이상	-
	하이퍼바이저	VMware vSphere ESXi 6.7 U2 이상	-
스토리지	하이퍼바이저 관리 시스템	VMware vCenter Server 6.7 U3(vCSA) 이상	-
네트워크	NetApp 가상 스토리지 콘솔(VSC)	VSC 9.7 이상	-
	NetApp SnapCenter를 참조하십시오	SnapCenter 4.3 이상	-
	Cisco UCS Manager를 참조하십시오	4.1(1c) 이상	
하이퍼바이저	ESXi		
관리	하이퍼바이저 관리 시스템 VMware vCenter Server 6.7 U3(vCSA) 이상		
	NetApp 가상 스토리지 콘솔(VSC)	VSC 9.7 이상	
	NetApp SnapCenter를 참조하십시오	SnapCenter 4.3 이상	
	Cisco UCS Manager를 참조하십시오	4.1(1c) 이상	

"다음: 추가 FlexPod 보안 고려 사항."

추가 **FlexPod** 보안 고려 사항

"이전: FlexPod 통합 인프라의 솔루션 이점"

FlexPod 인프라는 모듈식, 컨버지드, 선택적으로 가상화, 확장 가능(스케일아웃 및 스케일업) 및 비용 효율적인 플랫폼입니다. FlexPod 플랫폼을 사용하면 컴퓨팅, 네트워크, 스토리지를 독립적으로 확장하여 애플리케이션 구축을 가속할 수 있습니다. 모듈식 아키텍처를 사용하므로 시스템 스케일아웃 및 업그레이드 작업 중에도 무중단으로 운영할 수 있습니다.

HIT 시스템의 여러 구성 요소는 SMB/CIFS, NFS, ext4 및 NTFS 파일 시스템에 데이터를 저장해야 합니다. 즉, 인프라가 NFS, CIFS 및 SAN 프로토콜을 통해 데이터 액세스를 제공해야 합니다. 단일 NetApp 스토리지 시스템에서 이러한 모든 프로토콜을 지원하여 프로토콜 관련 스토리지 시스템의 기존 관행을 제거할 수 있습니다. 또한, 단일 NetApp 스토리지 시스템은 EHR, PACS 또는 VNA, 유전체학, VDI 등 다양한 HIT 워크로드를 지원할 수 있습니다.
보장된 구성 가능한 성능 수준

HIT는 FlexPod 시스템에 배포되면 의료 산업에만 해당되는 여러 가지 이점을 제공합니다. 다음 목록은 이러한 이점에 대한 자세한 설명입니다.

- * FlexPod 보안 *. 보안은 FlexPod 시스템의 기초가 됩니다. 지난 몇 년 동안 랜섬웨어는 위협이 되었습니다. 랜섬웨어는 암호화 바이러스, 암호화를 사용하여 악성 소프트웨어를 빌드하는 일종의 맬웨어입니다. 이 맬웨어는 대칭 키 암호화와 비대칭 키 암호화를 모두 사용하여 피해자의 데이터를 잠그고 데이터 암호를 해독할 키를 제공하는 대가로 금전을 요구합니다. FlexPod 솔루션이 랜섬웨어와 같은 위협을 완화하는 데 어떤 도움이 되는지 알아보려면 를 참조하십시오. "TR-4802: 랜섬웨어에 대한 솔루션" FlexPod 인프라 구성 요소도 "FIPS 140-2를 준수합니다"있습니다.
- Cisco Intersight. * Cisco Intersight는 혁신적인 클라우드 기반의 서비스형 관리 플랫폼으로, 전체 스택 FlexPod 관리 및 오케스트레이션을 위한 단일 창을 제공합니다. Intersight 플랫폼은 FIPS 140-2 보안 호환 암호화 모듈을 사용합니다. 플랫폼의 대역 외 관리 아키텍처는 HIPAA와 같은 일부 표준 또는 감사 범위를 벗어납니다. 네트워크에서 개인 식별 가능한 건강 정보는 Intersight 포털에 전송되지 않습니다.
- * NetApp FPolicy 기술. * 이름 파일 정책의 진화된 FPolicy는 NFS 또는 SMB/CIFS 프로토콜을 통한 파일 액세스를 모니터링하고 관리하기 위한 파일 액세스 알림 프레임워크입니다. 이 기술은 10년 이상 ONTAP 데이터 관리 소프트웨어의 일부였습니다. 랜섬웨어의 탐지에 유용합니다. 이 제로 트러스트 엔진은 ACL(액세스 제어 목록)의 사용 권한 외에 추가적인 보안 조치를 제공합니다. FPolicy는 두 가지 운영 모드, 즉 기본 및 외부 모드를 사용합니다.
  - 기본 모드는 파일 확장명의 블랙리스트와 화이트리스팅을 모두 제공합니다.
  - 외부 모드는 네이티브 모드와 동일한 기능을 제공하지만, ONTAP 시스템 외부에서 실행되는 FPolicy 서버와 SIEM(보안 정보 및 이벤트 관리) 시스템과도 통합됩니다. 랜섬웨어에 대항하는 방법에 대한 자세한 내용은 를 참조하십시오 "랜섬웨어에 대항하기: 3부 – 강력한 기본(무료) 툴인 ONTAP FPolicy" 블로그:
- * 저장된 데이터 *. ONTAP 9 이상에서는 FIPS 140-2를 준수하는 세 가지 유휴 데이터 암호화 솔루션이 있습니다.
  - NSE는 자체 암호화 드라이브를 사용하는 하드웨어 솔루션입니다.
  - NVE는 각 볼륨의 고유 키를 사용해 활성화된 모든 드라이브 유형의 모든 데이터 볼륨을 암호화할 수 있는 소프트웨어 솔루션입니다.
  - NAE는 각 애그리게이트의 고유 키를 사용하여 활성화된 모든 드라이브 유형의 모든 데이터 볼륨을 암호화할 수 있는 소프트웨어 솔루션입니다.

ONTAP 9.7부터 NAE와 NVE는 VE라는 이름의 NetApp NVE 라이센스 패키지가 설치된 경우 기본적으로 활성화됩니다.

- * 비행 중인 데이터 *. ONTAP 9.8부터 IPsec(인터넷 프로토콜 보안)은 클라이언트와 ONTAP SVM 사이의 모든 IP 트래픽에 엔드 투 엔드 암호화 지원을 제공합니다. 모든 IP 트래픽에 대한 IPsec 데이터 암호화에는 NFS, iSCSI 및 SMB/CIFS 프로토콜이 포함됩니다. IPsec은 iSCSI 트래픽에 대해 전송 중인 유일한 암호화 옵션을 제공합니다.
- * 하이브리드 멀티 클라우드 Data Fabric * 에서 엔드 투 엔드 데이터 암호화 데이터 복제 트래픽에 NSE 또는 NVE, CPE(Cluster 피어링 암호화)와 같은 유휴 데이터 암호화 기술을 사용하는 고객은 이제 ONTAP 9.8 이상으로 업그레이드하고 IPsec을 사용하여 하이브리드 멀티 클라우드 데이터 패브릭 전체에서 클라이언트와 스토리지 간의 엔드 투 엔드 암호화를 사용할 수 있습니다. ONTAP 9부터는 클러스터 차원의 제어 평면 인터페이스를 위해 FIPS 140-2 규정 준수 모드를 활성화할 수 있습니다. 기본적으로 FIPS 140-2 전용 모드는 비활성화되어 있습니다. ONTAP 9.6부터 CPE는 ONTAP SnapMirror, NetApp SnapVault 및 NetApp FlexCache 기술과 같은 데이터 복제 기능에 TLS 1.2 AES-256 GCM 암호화 지원을 제공합니다. 암호화는 두 클러스터 피어 간에 미리 공유된 키(PSK)를 통해 설정됩니다.
- * 보안 멀티 테넌시 *. 가상화된 서버 및 스토리지 공유 인프라의 증가하는 요구 사항을 지원하여 특히 데이터베이스 및 소프트웨어의 여러 인스턴스를 호스팅할 때 시설별 정보의 안전한 멀티 테넌시를 지원합니다.

"다음: 결론."

결론

"이전: 추가 FlexPod 보안 고려 사항."

FlexPod 플랫폼에서 의료 애플리케이션을 실행하면 FIPS 140-2를 지원하는 플랫폼을 통해 의료 조직을 더욱 안전하게 보호할 수 있습니다. FlexPod은 컴퓨팅, 네트워크, 스토리지 등 모든 단일 구성 요소에서 다계층 보호를 제공합니다. FlexPod 데이터 보호 기능은 사용되지 않는 데이터나 사용 중인 데이터를 보호하고, 필요할 때 백업을 안전하게 보호합니다.

Cisco와 NetApp의 전략적 파트너십을 통해 엄격한 테스트를 거친 FlexPod 사전 검증된 설계를 활용하여 사람의 실수를 방지합니다. FlexPod 시스템은 FIPS 140-2를 컴퓨팅, 네트워킹 및 스토리지 계층에서 사용할 수 있는 경우에도 성능에 거의 영향을 주지 않으면서 예측 가능하고 낮은 대기 시간의 시스템 성능과 고가용성을 제공하도록 엔지니어링 및 설계되었습니다. 이러한 접근 방식은 사용자의 사용 환경이 뛰어나고 사용자의 HIT 시스템 사용자에게 최적의 응답 시간을 제공합니다.

"다음: 감사의 말, 버전 기록 및 추가 정보를 찾을 위치."

감사의 말, 버전 기록 및 추가 정보를 찾을 수 있는 위치

"이전: 결론."

이 문서에 설명된 정보에 대한 자세한 내용은 다음 문서 및 웹 사이트를 참조하십시오.

- Cisco MDS 9000 제품군 NX-OS 보안 구성 가이드

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/security/cisco_mds9000_security_config_guide_8x/configuring_fips.html#task_1188151

- Cisco Nexus 9000 시리즈 NX-OS 보안 구성 가이드, 릴리즈 9.3(x)

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/security/configuration/guide/b-cisco-nexus-9000-nx-os-security-configuration-guide-93x/m-configuring-fips.html

- NetApp 및 FIPS(Federal Information Processing Standard) 간행물 140-2

https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- FIPS 140-2

  https://fieldportal.netapp.com/content/902303

- NetApp ONTAP 9 강화 가이드

  https://www.netapp.com/pdf.html?item=/media/10674-tr4569pdf.pdf

- NetApp 암호화 기능 가이드 를 참조하십시오

  https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-nve%2Fhome.html

- NVE 및 NAE 데이터시트

  https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- NSE 데이터시트

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- ONTAP 9 문서 센터

  http://docs.netapp.com

- NetApp 및 FIPS(Federal Information Processing Standard) 간행물 140-2

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- Cisco 및 FIPS 140-2 규정 준수

  https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html

- NetApp 암호화 보안 모듈

  https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2648.pdf

- 중대형 의료 조직을 위한 사이버 보안 사례

  https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf

- Cisco 및 CMVP(Cryptographic Module Validation Program)

  https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=cisco&CertificateStatus=Active&ValidationYear=0

- NetApp 스토리지 암호화, NVMe 자체 암호화 드라이브, NetApp 볼륨 암호화 및 NetApp 애그리게이트 암호화

  https://www.netapp.com/pdf.html?item=/media/17073-ds-3898.pdf

- NetApp 볼륨 암호화 및 NetApp 애그리게이트 암호화

https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- NetApp 스토리지 암호화

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- 전자 건강 기록 시스템용 FlexPod

  https://www.netapp.com/pdf.html?item=/media/22199-tr-4881.pdf

- Data Now:클라우드 연결 플래시 기술로 Epic EHR 환경의 성능 향상

  https://www.netapp.com/media/10809-cloud-connected-flash-wp.pdf

- Epic EHR 인프라용 FlexPod Datacenter

  https://www.netapp.com/pdf.html?item=/media/17061-ds-3683.pdf

- Epic EHR용 FlexPod 데이터 센터 구축 가이드 를 참조하십시오

  https://www.netapp.com/media/10658-tr-4693.pdf

- MEDITECH 소프트웨어용 FlexPod 데이터 센터 인프라

  https://www.netapp.com/media/8552-flexpod-for-meditech-software.pdf

- FlexPod 표준은 MEDITECH 소프트웨어로 확장됩니다

  https://blog.netapp.com/the-flexpod-standard-extends-to-meditech-software/

- MEDITECH 방향 사이징 가이드용 FlexPod

  https://www.netapp.com/pdf.html?item=/media/12429-tr4774.pdf

- 의료 영상 촬영용 FlexPod

  https://www.netapp.com/media/19793-tr-4865.pdf

- 의료 부문의 AI

  https://www.netapp.com/pdf.html?item=/media/7393-na-369pdf.pdf

- 의료 분야의 혁신을 지원하는 FlexPod

  https://flexpod.com/solutions/verticals/healthcare/

- Cisco와 NetApp의 FlexPod

  https://flexpod.com/

감사의 말

- Abhinav Singh, NetApp 기술 마케팅 엔지니어

- Brian O는 NetApp의 솔루션 설계자 Healthcare(Epic) 입니다
- Brian Pruitt, NetApp 비즈니스 개발 매니저
- Arvind Ramakrishnan, NetApp 수석 솔루션 설계자
- Michael Hommer, NetApp의 FlexPod 글로벌 현장 CTO

버전 기록

버전	날짜	문서 버전 기록
버전 1.0	2021년 4월	최초 릴리스

NetApp ONTAP 스토리지와 Cisco Intersight

Cisco Intersight with NetApp Storage 빠른 시작 가이드 를 참조하십시오

파트너 후원:

소개

NetApp과 Cisco는 협력 관계를 맺고 FlexPod 에코시스템을 위한 단일 창 방식으로 제공하는 Cisco Intersight를 제공하고 있습니다. 이처럼 간소한 통합으로 FlexPod 인프라 및 FlexPod 솔루션의 모든 구성요소를 위한 통합 관리 플랫폼이 생성됩니다. Cisco Intersight를 사용하면 NetApp 스토리지, Cisco 컴퓨팅 및 VMware 인벤토리를 모니터링할 수 있습니다. 또한 워크플로우를 조율하거나 자동화하여 스토리지 및 가상화 작업을 동시에 수행할 수 있습니다.

관련 정보

자세한 내용은 다음 문서 및 웹 사이트를 참조하십시오.

"TR 4883: ONTAP 9.8을 지원하는 FlexPod 데이터 센터, Cisco Intersight용 ONTAP 스토리지 커넥터, Cisco Intersight 관리 모드"

"Cisco Intersight 도움말 센터"

"Cisco Intersight 시작하기 개요"

"Intersight Appliance 설치 및 업그레이드 가이드"

새로운 기능

이 섹션에서는 NetApp ONTAP 스토리지와 Cisco Intersight에 사용할 수 있는 새로운 기능에 대해 설명합니다.

2024년 1월

- 참조 워크플로우를 사용한 NetApp 스토리지 오케스트레이션은 이제 를 통해 GitHub에서 다운로드할 수 있습니다 "FlexPod Intersight 워크플로 저장소". GitHub의 새로운 참조 워크플로에 대한 자세한 내용은 을 참조하십시오 "사용 사례 2: 참조 워크플로우를 사용하는 NetApp 스토리지 오케스트레이션".

2023년 11월

- 사용자 인터페이스의 인벤토리 섹션에 NVMe 네임스페이스 페이지가 추가되었습니다.

2023년 8월

NetApp Active IQ Unified Manager 9.13GA 업그레이드는 최신 릴리스와 호환되고 모든 기능을 보장하기 위해 필요합니다.

- 새 이니시에이터 그룹을 생성하거나 기존 이니시에이터 그룹을 선택하는 데 사용할 수 있는 선택 옵션을 명확하게 표시하도록 새 NetApp 스마트 LUN 작업을 개선했습니다. 이제 사용자가 새 이니시에이터 그룹을 생성하기 위한 상자를 선택하면 기존 이니시에이터 그룹을 선택하는 데 필요한 매개 변수를 더 이상 사용할 수 없습니다. 새 이니시에이터 그룹을 생성하기 위해 확인란을 선택 취소하면 기존 이니시에이터 그룹 매개 변수를 사용할 수 있습니다.
- 새 NetApp LUN 매핑 및 NetApp LUN 매핑 제거 작업이 개선되었습니다. 이제 LUN과 이니시에이터 그룹 간의 새로운 관계가 업데이트됩니다. 작업 실행 시 LUN과 이니시에이터 그룹의 UI 인벤토리가 즉시 업데이트됩니다.
- 이제 사용자가 처음 로그인할 때 검사 페이지가 올바르게 로드되고 더 이상 새로 고칠 필요가 없습니다.

2023년 7월

NetApp Active IQ Unified Manager 9.13GA 업그레이드는 최신 릴리스와 호환되고 모든 기능을 보장하기 위해 필요합니다.

- NetApp 스토리지 작업의 이름이 업데이트되었습니다. 이름이 바뀐 작업의 전체 목록은 디자이너가 없는 양식을 사용하는 사용자 지정 워크플로 사용 사례 3 을 참고하세요.
- NFS 인터페이스 IP 주소가 새 NetApp NAS 스마트 볼륨 작업의 출력으로 추가되었습니다.
- ASUP 전송이 검사 탭에 추가되었는지 확인합니다.
- 이제 모든 계층의 올바른 계층 유형이 계층 사용자 인터페이스 아래에 올바르게 표시됩니다.
- 이제 모든 호환 라이센스가 라이센스 페이지 아래에 올바르게 표시됩니다.
- 이제 홈 디렉토리가 없거나 없는 CIFS 공유에 대한 정확한 값이 공유 페이지에 표시됩니다.
- 이제 LUN 페이지에서 매핑된 열에 대해 정렬 및 필터링이 설정되었습니다.
- 이제 정렬 및 필터링을 통해 NTP 서버 페이지에서 인증 설정 열을 사용할 수 있게 되었습니다.
- 검사 탭에 새 검사 및 다음 해당 범주를 추가했습니다.
  - 보안
  - 랜섬웨어 방지
  - 가용성
  - 기타
- 재고 세부 정보 보기에서 물리적 사용된 용량 대신 사용 중인 보고서를 표시합니다.

2023년 6월

NetApp Active IQ Unified Manager 9.13RC1로 업그레이드하여 최신 릴리스와 완벽하게 호환되도록 해야 합니다.

- NetApp 스토리지 작업의 이름이 업데이트되었습니다. 을 참조하십시오 "사용 사례 3 디자이너가 없는 양식을 사용하는 사용자 지정 워크플로" 이름이 바뀐 작업의 전체 목록을 표시합니다.

2023년 4월

- 사용자 인터페이스의 인벤토리 섹션에 있는 정책 페이지 아래에 보호 정책(SnapMirror) 및 스냅샷 정책 탭이 추가되었습니다.
- 사용자 인터페이스의 Inventory 섹션 아래에 NFS Clients 페이지가 추가되었습니다.
- 사용자 인터페이스의 Inventory 섹션 아래에 있는 Storage VMs 페이지에 Protected 열이 추가되었습니다.
- 데이터 축소 정보가 보고 표시되는 방식을 수정했습니다.
- 사용자 인터페이스의 Inventory 섹션에 있는 Tiers 페이지 아래에 Local Tier 및 Cloud Tier 탭이 추가되었습니다.
- 이제 사용자 인터페이스의 인벤토리 섹션에 있는 포트 페이지의 이름 열 뒤에 노드 열이 표시됩니다.

2023년 1월

ⓘ 최신 릴리즈와의 호환성 및 모든 기능을 사용하려면 NetApp Active IQ Unified Manager 9.12 GA로 업그레이드해야 합니다. 이 릴리스와 관련된 알려진 문제 목록은 를 참조하십시오 알려진 문제.

- Intersight 상호 운용성 점검은 이제 호환성 검사를 수행할 때 UCSM 및 IMM 펌웨어 모드를 구분할 수 있습니다.
- ONTAP 9.7의 경우 Intersight에는 보호 관계가 표시되지 않습니다. 이 문제는 ONTAP 9.8RC1에서 해결되었습니다.

2022년 8월

ⓘ 최신 릴리스와의 호환성 및 모든 기능을 보장하려면 NetApp Active IQ Unified Manager 9.11 GA로 업그레이드해야 합니다. 이 릴리스와 관련된 알려진 문제 목록은 를 참조하십시오 알려진 문제.

- System Manager와 일치하도록 클러스터 가용 용량 계산을 업데이트했습니다
- 성능 데이터가 채워질 때까지 성능 메트릭 요약을 숨기려면 클러스터 일반 페이지를 업데이트했습니다
- 간혹 페이지가 중단되는 원인이 되는 클러스터 일반 페이지 UI 문제를 해결했습니다
- 백엔드 인벤토리에 CIFS 공유, CIFS 서비스, Qtree, SVM SnapMirror 정책 추가
- Logical Inventory 섹션의 UI 탐색 메뉴에 공유 및 qtree가 추가되었습니다
- 선택한 스토리지 VM에서 공유를 탭으로 추가했습니다
- 스토리지 VM이 CIFS 설정된 경우 스토리지 VM 일반 탭에 CIFS 서비스 정보가 추가되었습니다
- 사용자가 NetApp 스토리지 시스템의 구성을 확인할 수 있도록 클러스터 점검 페이지가 추가되었으며 모범 사례를 준수합니다

2022년 7월

- 이제 Capacity 위젯에서 클러스터 데이터 축소율에 대한 향상된 시각 자료를 사용할 수 있습니다
- 네트워크 인터페이스 페이지에 FC 인터페이스 탭이 추가되었습니다
- 일반 "새 저장소 볼륨" 작업을 사용하여 새 볼륨을 생성하면 볼륨 공간 보장이 없음으로 설정되고 스냅숏 예비 공간 비율은 0%로 설정됩니다
- 이제 스냅샷 정책 편집 작업 아래에 주석 필드가 선택 사항이므로 더 이상 필수가 아닙니다

- UI 인벤토리 및 오케스트레이션 일관성 향상
- 이제 System Manager와 일치하는 클러스터 용량 아래의 Intersight 용량 정보
- 사용 편의성을 높이기 위해 새 관리 인터페이스를 생성할 때 모든 매개 변수를 표시하는 New Storage Virtual Machine 작업 아래에 확인란이 추가되었습니다
- 클라이언트 일치 아래 프로토콜을 이동했으므로 이제 System Manager와 일치합니다
- 이제 액세스 프로토콜을 표시하는 엑스포트 정책 일반 페이지
- iGroup 제거가 이제 조건부로 기록되었습니다
- 새 스토리지 NAS 데이터 인터페이스 및 새 스토리지 iSCSI 데이터 인터페이스 아래에 NAS에 대한 "페일오버 정책" 및 "자동 변환" 매개 변수가 추가되었습니다
- 새 저장소 NAS에 대한 롤백 Smart Volume 작업은 연결된 다른 볼륨이 없는 경우 엑스포트 정책을 제거합니다
- Smart Volume 및 Smart LUN 작업을 위한 향상된 기능을 제공합니다

2022년 4월

> 향후 릴리스와 호환성 및 완벽한 기능을 보장하기 위해 NetApp Active IQ Unified Manager를 버전 9.10P1로 업그레이드하는 것이 좋습니다.

- 이더넷 포트 세부 정보 페이지에 브로드캐스트 도메인 추가
- 사용자 인터페이스 내에서 애그리게이트 및 SVM을 위한 “Aggregate”라는 용어를 “계층”으로 변경했습니다
- "클러스터 상태"를 "어레이 상태"로 변경했습니다.
- 이제 MTU 필터가 <, >, =, ⇐, >= 문자에 대해 작동합니다
- 클러스터 인벤토리에 네트워크 인터페이스 페이지가 추가되었습니다
- 클러스터 인벤토리에 AutoSupport가 추가되었습니다
- 노드에 CDPD.ENABLE 옵션이 추가되었습니다
- CDP 인접 항목 객체 추가
- Cisco Intersight에서 NetApp 워크플로우 스토리지 작업을 추가했습니다. 을 참조하십시오 "사용 사례 3 디자이너가 없는 양식을 사용하는 사용자 지정 워크플로" NetApp 스토리지 작업의 전체 목록을 확인하십시오.

2022년 1월

- NetApp Active IQ Unified Manager 9.10 이상에 대한 이벤트 기반 Intersight 알람이 추가되었습니다.

> 향후 릴리스와 호환성 및 완벽한 기능을 보장하기 위해 NetApp Active IQ Unified Manager를 버전 9.10으로 업그레이드하는 것이 좋습니다.

- 스토리지 가상 시스템에 대해 활성화된 각 프로토콜(참 또는 거짓)을 명시적으로 설정합니다
- 매핑된 클러스터 상태 상태 정상 - 억제된 상태로 OK
- 이름이 클러스터 목록 페이지의 클러스터 상태 열로 바뀌었습니다
- 클러스터가 다운되었거나 연결할 수 없는 경우 스토리지 배열에 "접속할 수 없음"이 표시됩니다
- 클러스터 일반 페이지 아래의 스토리지 상태 열로 이름이 변경되었습니다

- 이제 SVM에는 SVM의 모든 볼륨을 표시하는 "볼륨" 탭이 있습니다
- 볼륨에 스냅샷 용량 섹션이 있습니다
- 이제 라이센스가 올바르게 표시됩니다

2021년 10월

- Cisco Intersight에서 사용 가능한 NetApp 스토리지 작업 목록이 업데이트되었습니다. 을 참조하십시오 "사용 사례 3 디자이너가 없는 양식을 사용하는 사용자 지정 워크플로" NetApp 스토리지 작업의 전체 목록을 확인하십시오.
- 클러스터 목록 페이지 아래에 상태 열이 추가되었습니다.
- 이제 선택한 클러스터의 일반 페이지에서 확장된 세부 정보를 사용할 수 있습니다.
- 이제 탐색 창을 통해 NTP 서버 테이블에 액세스할 수 있습니다.
- 스토리지 가상 머신에 대한 일반 페이지가 포함된 새 센서 탭이 추가되었습니다.
- 이제 Port General 페이지에서 VLAN 및 Link Aggregation 그룹 요약을 사용할 수 있습니다.
- Volume Total Capacity 테이블 아래에 추가된 Total Data Capacity 열
- 평균 볼륨 통계, 평균 LUN 통계, 평균 집계 통계, 평균 스토리지 VM 통계 및 평균 노드 통계 테이블에 추가된 지연 시간, IOPS 및 처리량 열

> 위의 성능 메트릭은 NetApp Active IQ Unified Manager 9.9 이상을 통해 모니터링되는 스토리지 어레이에만 사용할 수 있습니다.

알려진 문제

- AIQUM 9.11 이하 버전을 사용하는 경우 Storage List(저장소 목록) 페이지에 표시된 값과 Storage general(저장소 일반) 페이지의 capacity bar(용량 표시줄) 차트 간에 불일치가 발생합니다. 이 문제를 해결하려면 표시된 용량 값의 정확성을 보장하기 위해 AIQUM 9.12 이상으로 업그레이드하십시오.
- AIQUM 9.11 이전 버전을 사용하는 경우 "Integrated Systems" 페이지 아래의 "Interoperability" 탭에서 수행한 검사는 IMM과 UCSM Cisco 구성 요소를 정확하게 구분하지 못합니다. 이 문제를 해결하려면 AIQUM 9.12로 업그레이드하여 모든 구성 요소가 올바르게 식별되었는지 확인하십시오.
- 데이터 수집 프로세스 중에 Intersight 저장소 인벤토리 데이터가 영향을 받지 않도록 하려면 지원되지 않는 ONTAP 클러스터(예: ONTAP 9.7P1 이하 버전)를 AIQUM(Active IQ Unified Manager)에서 제거해야 합니다.
- 청구된 모든 대상은 FlexPod 통합 시스템 상호 운용성 쿼리를 성공적으로 완료하려면 최소 AIQUM 버전 9.11이 필요합니다.
- FQDN을 사용하여 AIQUM에 ONTAP 클러스터를 추가하면 스토리지 인벤토리 검사 페이지가 채워지지 않습니다. 사용자는 IP 주소를 사용하여 AIQUM에 ONTAP 클러스터를 추가해야 합니다.

요구 사항

NetApp ONTAP 스토리지를 Cisco Intersight와 통합하기 위한 하드웨어, 소프트웨어 및 라이센스 요구사항을 충족하는지 확인합니다.

하드웨어 및 소프트웨어 요구 사항

이러한 구성 요소는 솔루션을 구축하는 데 필요한 최소 하드웨어 및 소프트웨어 구성 요소입니다. 솔루션의 특정 구현에 사용되는 구성 요소는 고객의 요구 사항에 따라 다를 수 있습니다.

구성 요소	요구사항 세부 정보
NetApp ONTAP를 참조하십시오	ONTAP 9.7P1 이상
NetApp Active IQ Unified Manager를 참조하십시오	최신 버전의 NetApp Active IQ Unified Manager가 필요합니다(현재 9.14RC1).
NetApp 스토리지 어레이	ONTAP 9.7P1 이상에서 모든 ONTAP ASA, AFF 및 FAS 스토리지 어레이를 지원합니다
가상화 하이퍼바이저	vSphere 7.0 이상



을 참조하십시오 "Cisco Intersight 지원 시스템" Cisco UCS Compute Components 및 UCSM 버전의 최소 요구 사항

Cisco Intersight 라이센스 요구 사항

Cisco Intersight는 물리적 스토리지(NetApp 스토리지)를 관리, 자동화, 최적화하는 인프라 서비스 및 Cloud Orchestrator 서비스와 같은 서비스를 제공합니다. 이 서비스를 사용하여 Cisco UCS 서버 및 Cisco HyperFlex 시스템을 관리할 수 있습니다. Infrastructure Service 및 Cloud Orchestrator 서비스는 여러 계층의 구독 기반 라이센스 모델을 사용합니다. 선택한 구독 기간에 필요한 Cisco UCS Server 볼륨 계층을 선택할 수 있습니다.

라이센스 모델

Cisco Intersight Infrastructure Services 라이센스 모델이 간소화되었으며, 이제 다음 두 개의 계층을 제공합니다.

- * Cisco Intersight Infrastructure Services Essentials * - Essentials 라이센스 계층은 글로벌 상태 모니터링 기능, 인벤토리, Cisco TAC 통합을 통한 사전 지원, 다중 요소 인증, SDK 및 API 액세스를 제공하는 등의 서버 관리를 제공합니다.
- * Cisco Intersight Infrastructure Services Advantage * - Advantage 라이센스 계층은 확장된 가시성, 에코시스템 통합, Cisco 및 타사 하드웨어 및 소프트웨어 자동화와 다중 도메인 솔루션을 제공하는 고급 서버 관리를 제공합니다.

다양한 라이센스 계층에서 지원하는 기능에 대한 자세한 내용은 를 참조하십시오 "인프라 서비스 라이센스".

시작하기 전에

Cisco Intersight에서 NetApp 스토리지를 모니터링 및 오케스트레이션하려면 vCenter 환경에 NetApp Active IQ Unified Manager 및 Cisco Intersight Assist 가상 어플라이언스가 설치되어 있어야 합니다.

NetApp Active IQ Unified Manager 설치 또는 업그레이드

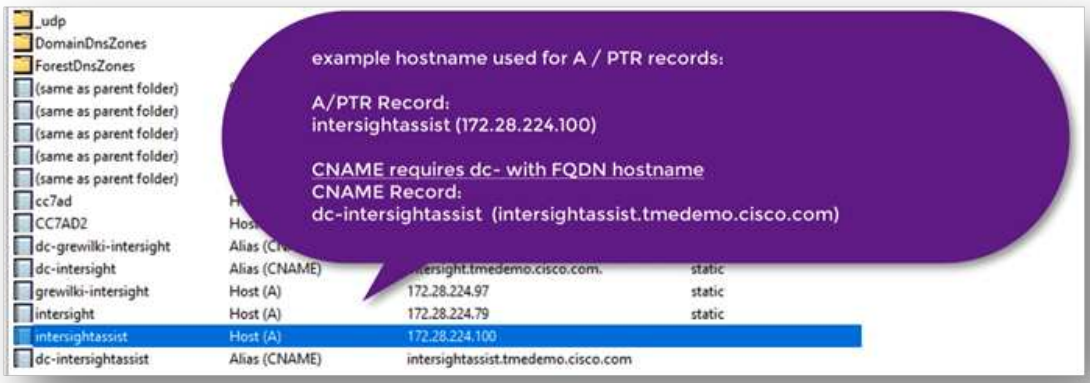
설치하지 않은 경우 Active IQ Unified Manager(최신 버전 필요, 현재 9.14RC1) 설치 또는 업그레이드합니다. 자세한 내용은 로 이동하십시오 "NetApp Active IQ Unified Manager 문서".

Cisco Intersight Assist 가상 어플라이언스를 설치합니다

을(를) 충족하는지 확인합니다 "Cisco Intersight 가상 어플라이언스 라이센스, 시스템 및 네트워크 요구 사항".

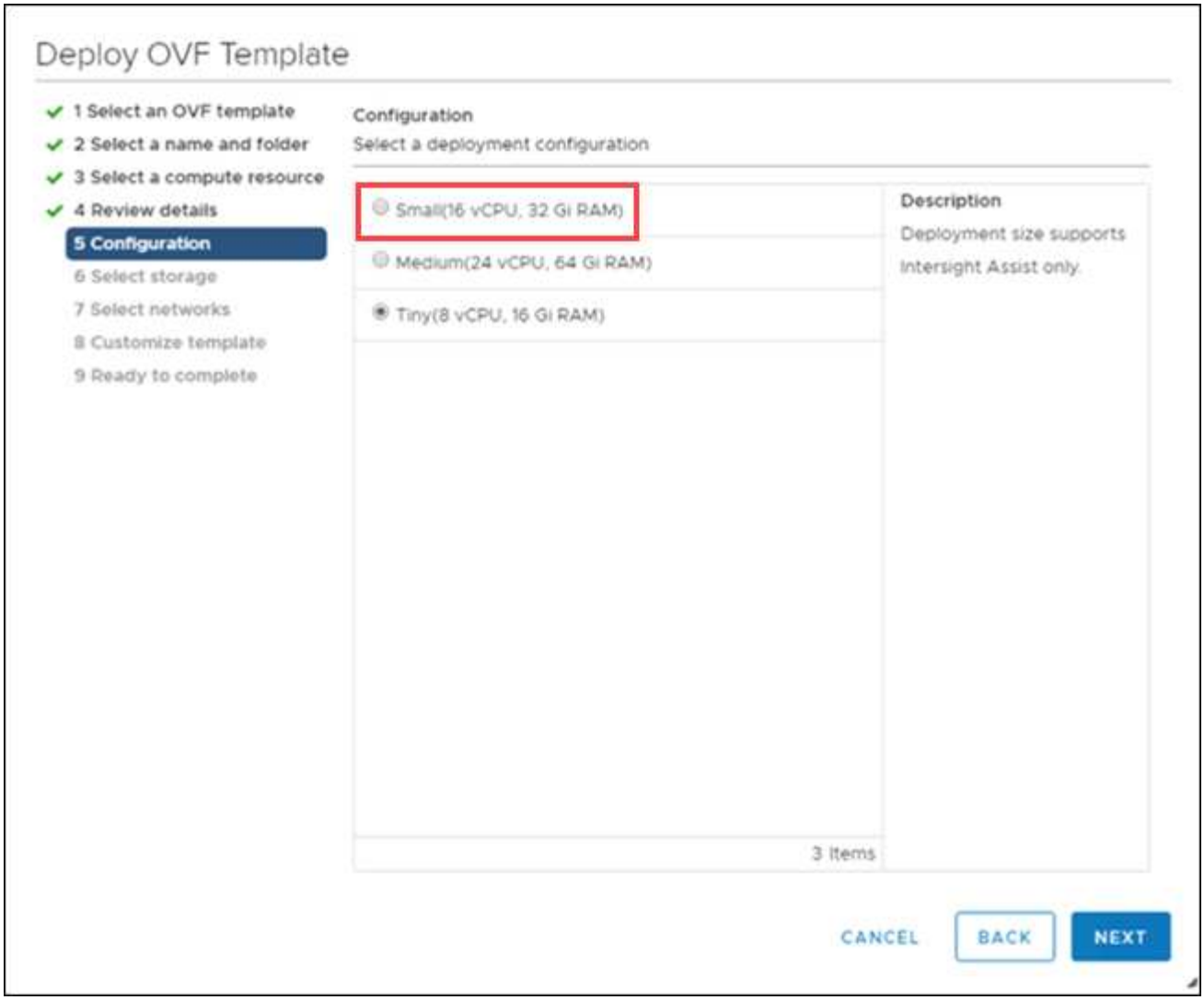
- 단계 *

1. Cisco Intersight 계정을 만듭니다. 를 방문하십시오 "https://intersight.com/" Intersight 계정을 생성합니다. Cisco Intersight 계정을 만들려면 유효한 Cisco ID가 있어야 합니다.
2. Intersight Virtual Appliance는 에서 다운로드할 수 있습니다 "software.cisco.com". 자세한 내용은 를 참조하십시오 "Intersight Appliance 설치 및 업그레이드 가이드".
3. OVA를 배포합니다. OVA를 구축하려면 DNS와 NTP가 필요합니다.
   a. OVA를 배포하기 전에 A/PTR 및 CNAME 별칭 레코드로 DNS를 구성합니다. 아래 예를 참조하십시오.

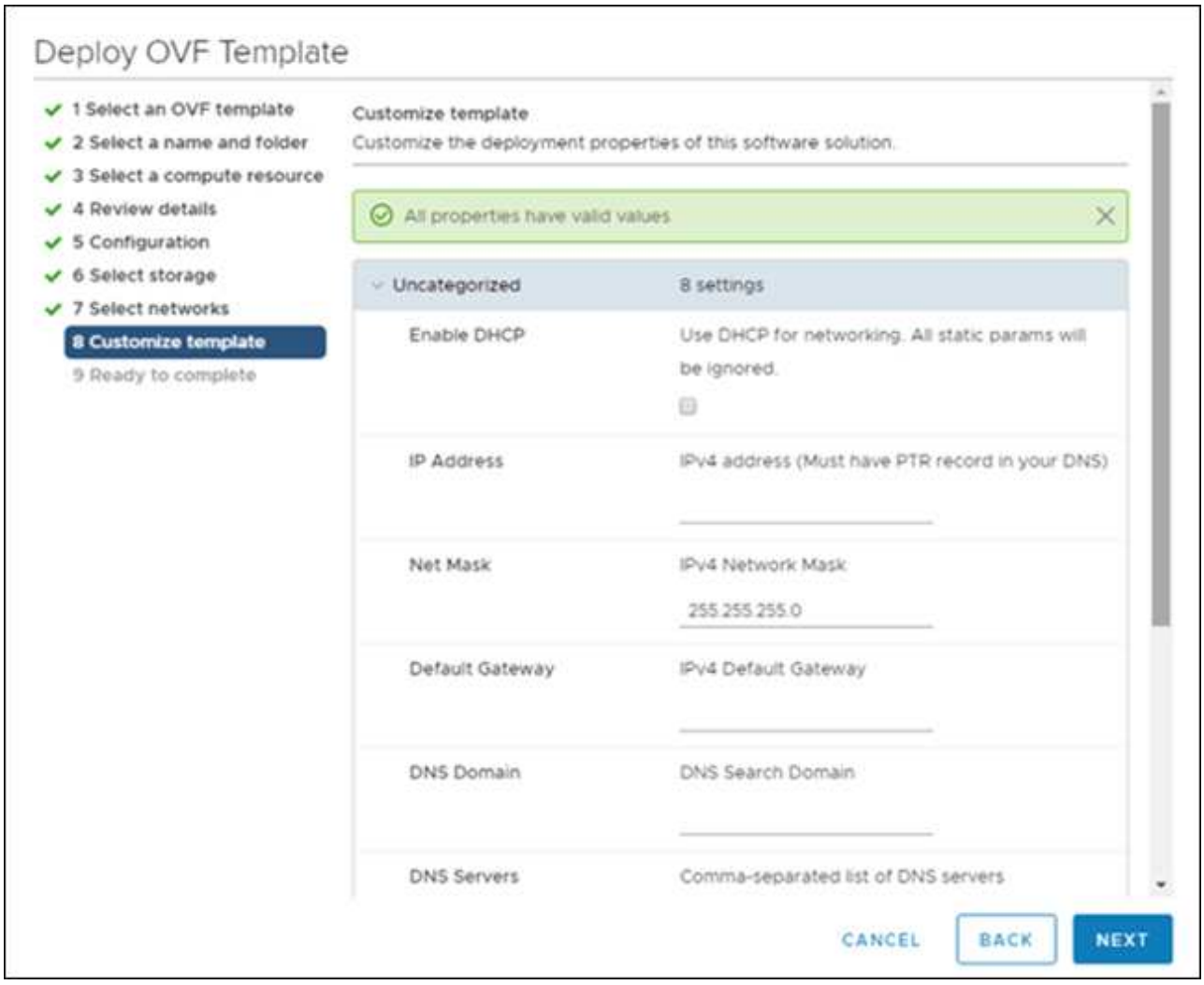


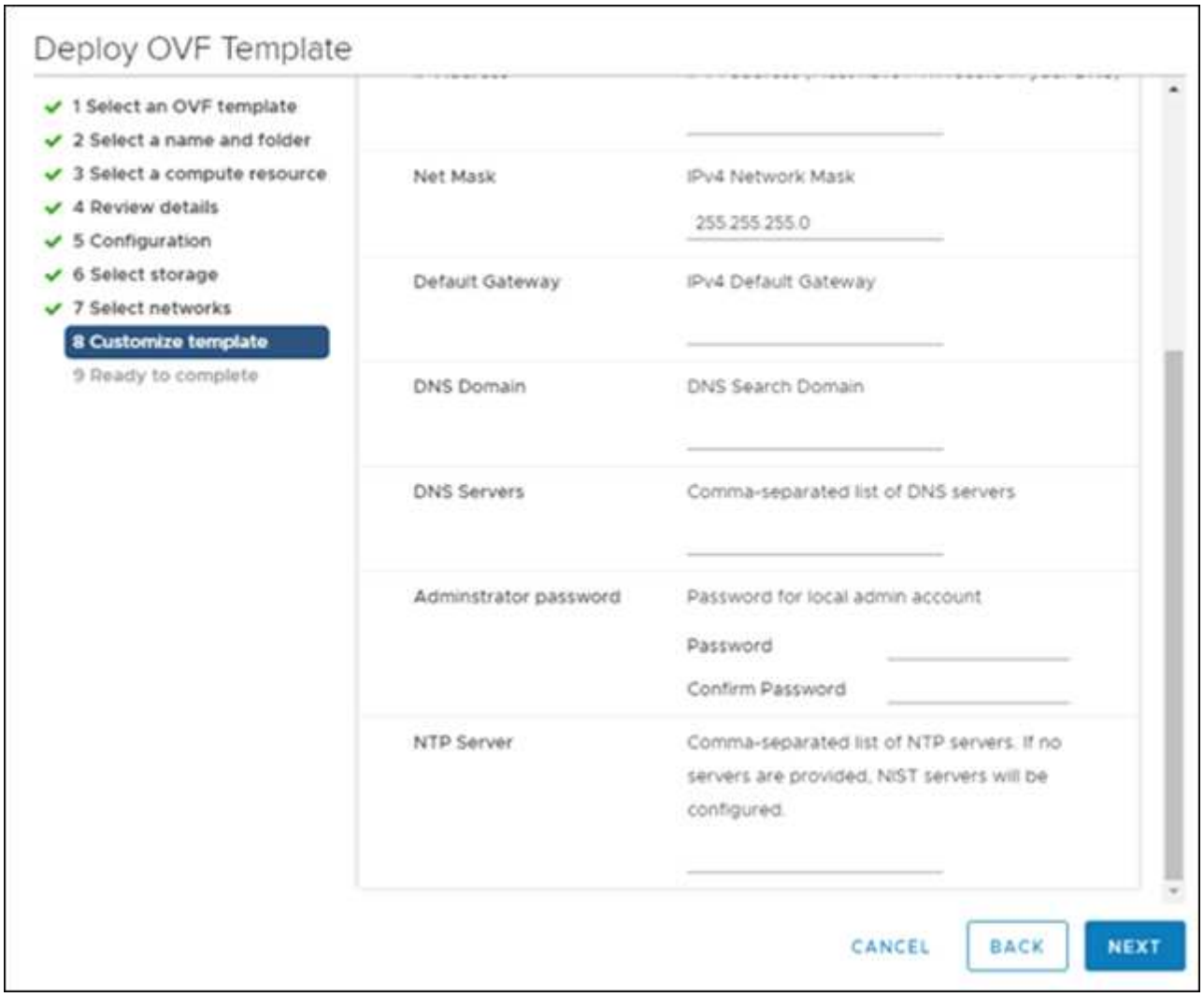
   b. Intersight Virtual Appliance에 대한 OVA 배포 요구 사항에 따라 적절한 구성 크기(Tiny, Small 또는 Medium)를 선택합니다.

- 팁: * 스토리지 객체가 많은 2노드 ONTAP 클러스터의 경우 Small (16 vCPU, 32 Gi RAM) 옵션을 사용하는 것이 좋습니다.



a. Customize Template * 페이지에서 OVF 템플릿의 배포 속성을 사용자 지정합니다. 관리자 암호는 admin('WebUI/CLI/ssh')에 사용됩니다.


Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Configuration
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Customize template
Customize the deployment properties of this software solution.
All properties have valid values
Uncategorized
8 settings
Enable DHCP
Use DHCP for networking. All static params will be ignored.
IP Address
IPv4 address (Must have PTR record in your DNS)
Net Mask
IPv4 Network Mask
255.255.255.0
Default Gateway
IPv4 Default Gateway
DNS Domain
DNS Search Domain
DNS Servers
Comma-separated list of DNS servers
CANCEL
BACK
NEXT



b. 다음 * 을 클릭합니다.

   1. Intersight Assist 어플라이언스 구축 후

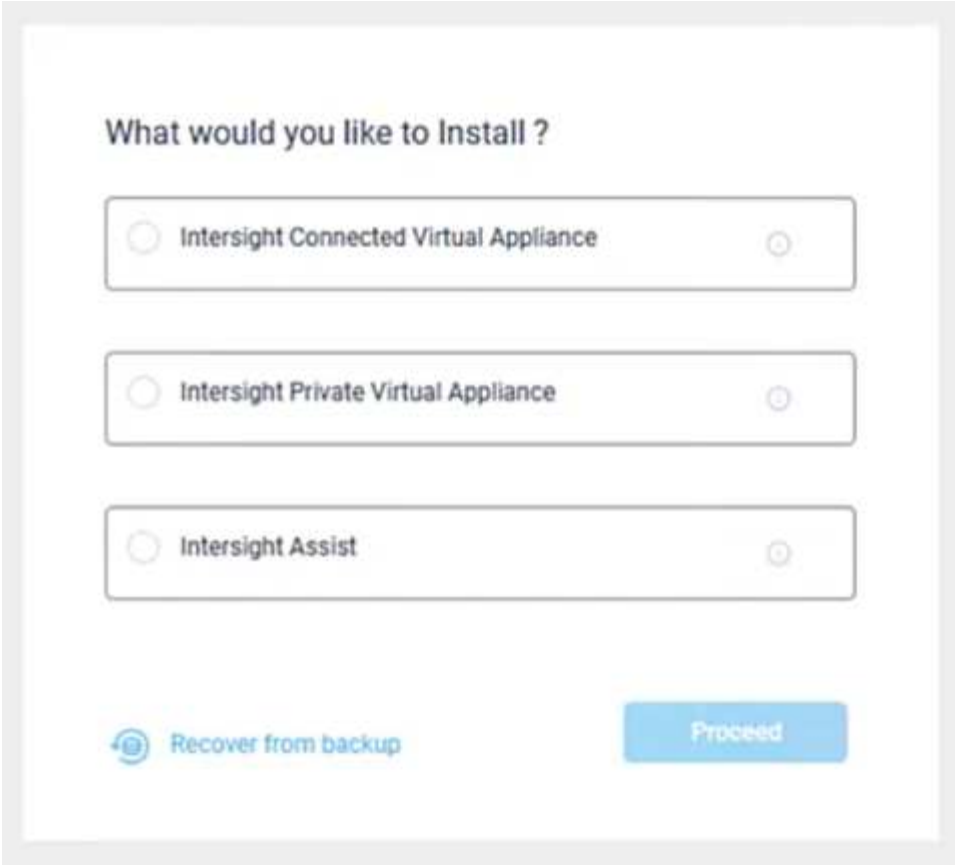
c. 로 이동합니다 https://FQDN-of-your-appliance 제품의 설치 후 설정을 완료합니다.

   설치 프로세스가 자동으로 시작됩니다. Intersight.com 대역폭에 따라 최대 1시간이 소요될 수 있습니다. 또한 VM의 전원을 켜면 보안 사이트가 작동하는 데 몇 초 정도 걸릴 수 있습니다.

d. 배포 후 프로세스 중에 다음 옵션을 선택합니다.

   - * Intersight Assist. * 이 배포를 통해 SaaS 모델을 Cisco Intersight에 연결할 수 있습니다.

     Intersight Assist를 선택할 때 계속하기 전에 장치 ID 및 클레임 코드를 기록해 두십시오.



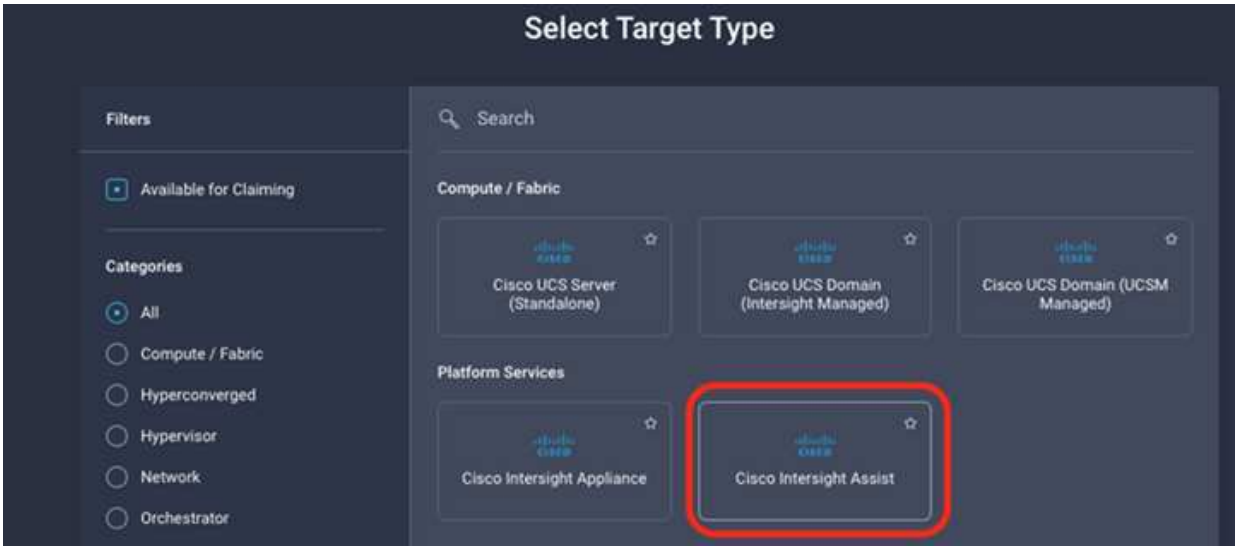
a. Proceed * 를 클릭합니다.

b. Intersight Assist * 를 선택하고 다음 단계를 완료합니다.

   i. 에서 SaaS Intersight 계정으로 이동합니다 "https://intersight.com".

   ii. Targets *, * Cisco Intersight Assist * 를 클릭한 다음 * Start * 를 클릭합니다.

   iii. 새로 배포된 Intersight Assist 가상 어플라이언스에서 장치 ID 및 클레임 코드를 복사하여 붙여넣어 * Cisco Intersight Assist * 어플라이언스를 신청하십시오.



   iv. Cisco Intersight Assist* 어플라이언스로 돌아가 * Continue(계속) * 를 클릭합니다. * 브라우저를 새로 고쳐야 할 수 있습니다.

다운로드 및 설치 프로세스가 시작됩니다. 바이너리는 Intersight Cloud에서 사내 어플라이언스로 전송됩니다. 완료 시간은 Intersight Cloud에 대한 대역폭에 따라 다릅니다.

IMT 서비스용 AIQ UM 프록시 서버를 구성합니다

NetApp ONTAP 스토리지와 Cisco Intersight를 위해 AIQ UM이 포함된 프록시 서버를 사용하는 경우 IMT(상호 운용성 매트릭스 툴 서비스)를 활용하려면 CLI(Command Line Interface)를 통해 설정을 구성해야 합니다. IMT 서비스는 * 통합 시스템 * 페이지의 * 상호 운용성 * 탭에서 사용할 수 있습니다. AIQ UM 프록시 서버 설정을 구성하려면 OVA(Active IQ Unified Manager 가상 머신) 진단 셸을 사용해야 합니다.

AIQ UM 진단 셸에 액세스하는 방법에 대한 자세한 내용은 을 참조하십시오 "OVA(Active IQ Unified Manager Virtual Machine) DIAG 셸에 액세스하는 방법"

- 단계 *

1. AIQ UM 터미널에 로그인하고 다음 명령을 실행하여 um에 로그인합니다.

```
um cli login -u <um maintenance user name>
```

- 예 *

```
um cli login -u admin
```

1. 다음 명령어를 실행해 IMT_PROXY_HOST와 IMT_PROXY_PORT를 설정한다.

IMT 프록시는 AutoSupport(ASUP) 프록시 구성과 별도의 구성입니다.

```
um option set imt.https.proxy.host=<IMT_PROXY_HOST>
um option set imt.https.proxy.port=<IMT_PROXY_PORT>
```

- 예 *

```
um option set imt.https.proxy.host=example-proxy.cls.eng.com
um option set imt.https.proxy.port=8200
```

IMT 프록시 서버 구성은 인증을 지원하지 않습니다.

1. IMT 프록시 세부 정보를 확인하여 다음 명령어를 통해 proxy_host와 proxy_port 설정을 확인한다.

```
um option list |grep imt
```

청구 대상

Cisco Intersight Assist를 설치한 후에는 NetApp 스토리지 및 가상화 장치를 요청할 수 있습니다. Intersight Targets * 페이지로 돌아가서 vCenter 및 NetApp Active IQ Unified Manager 타겟을 추가합니다.

NetApp AIQ UM(Active IQ Unified Manager) API 게이트웨이가 활성화되어 있는지 확인하십시오.

NetApp IQ Unified Manager에서 * 설정 > 일반 > 기능 설정 * 으로 이동합니다.



다음 예제는 Cisco Intersight에서 청구되는 NetApp AIQ UM 대상을 보여줍니다.

NetApp AIQ UM 타겟을 요청할 경우 Active IQ Unified Manager에서 관리하는 모든 클러스터가 Intersight에 자동으로 추가됩니다.

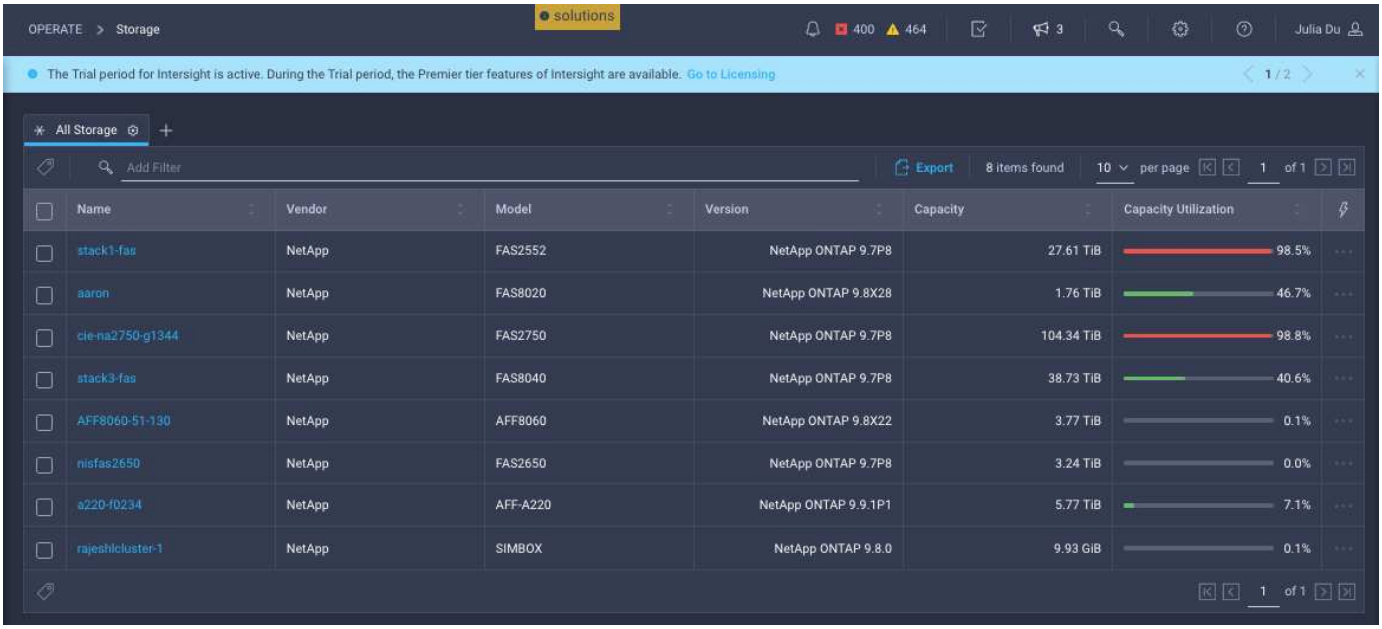


Cisco Intersight에서 NetApp 스토리지 모니터링

대상이 확보되면 Advantage 계층 라이센스가 있는 경우 NetApp 스토리지 위젯, 스토리지 인벤토리 및 가상화 탭을 사용할 수 있습니다. 프리미어 계층 라이센스가 있는 경우 오케스트레이션 탭을 사용할 수 있습니다.

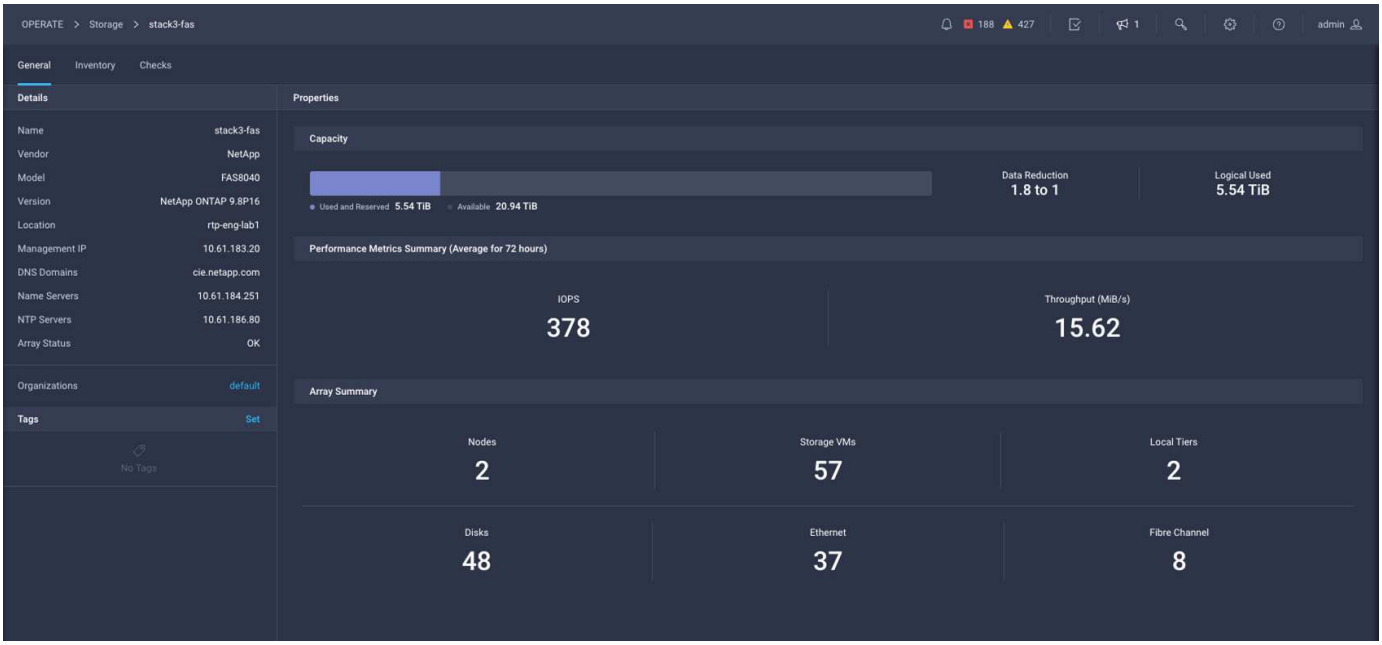
스토리지 인벤토리 개요

다음 스크린샷은 * Operate > Storage * 화면을 표시합니다.



다음 스크린샷은 스토리지 클러스터 개요를 보여 줍니다.

다음 성능 메트릭 요약 정보는 NetApp Active IQ Unified Manager 9.9 이상을 통해 스토리지 어레이를 모니터링하는 경우에만 표시됩니다.



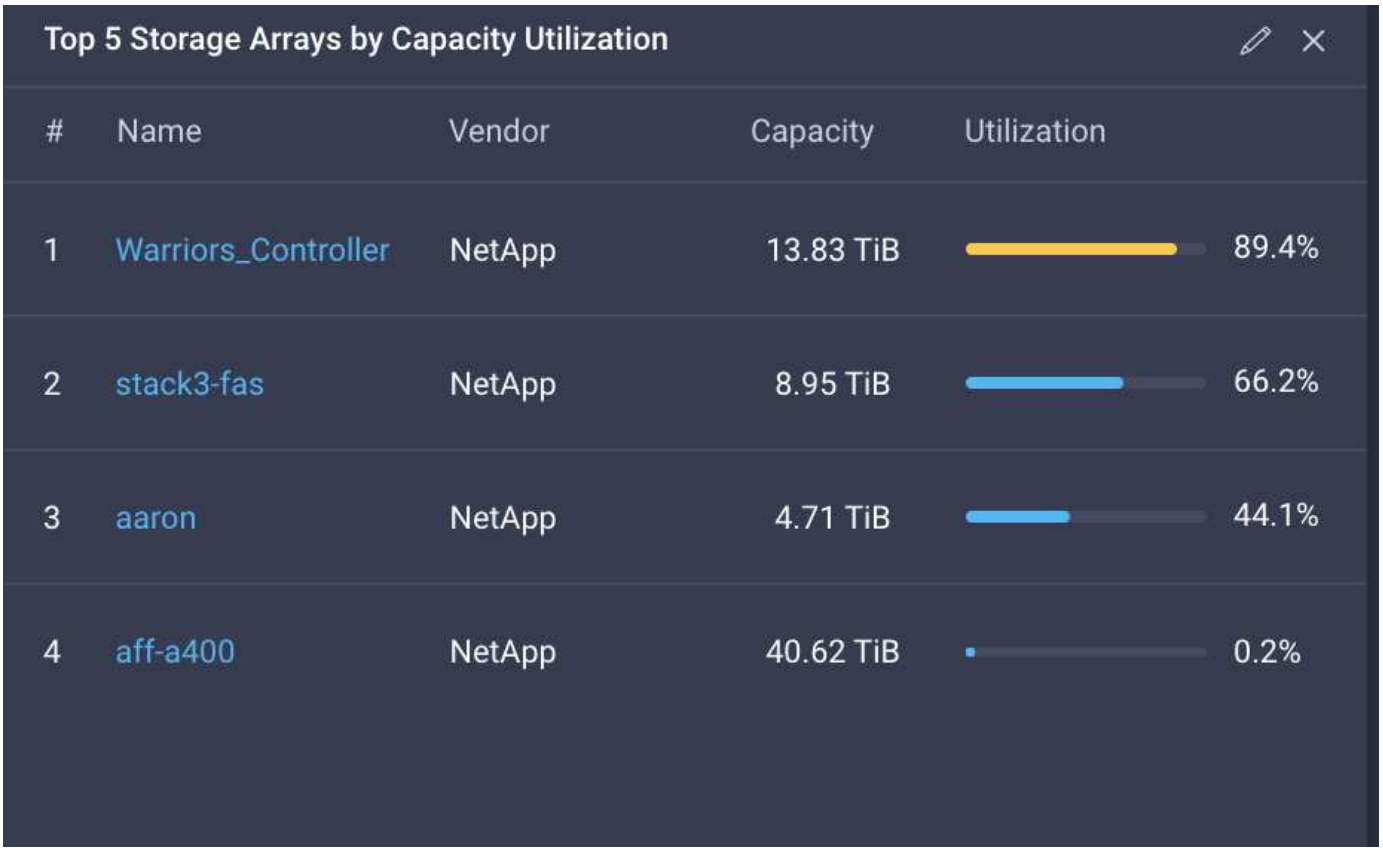
스토리지 위젯

스토리지 위젯을 보려면 * 모니터링 > 대시보드 > NetApp 스토리지 위젯 보기 * 로 이동합니다.

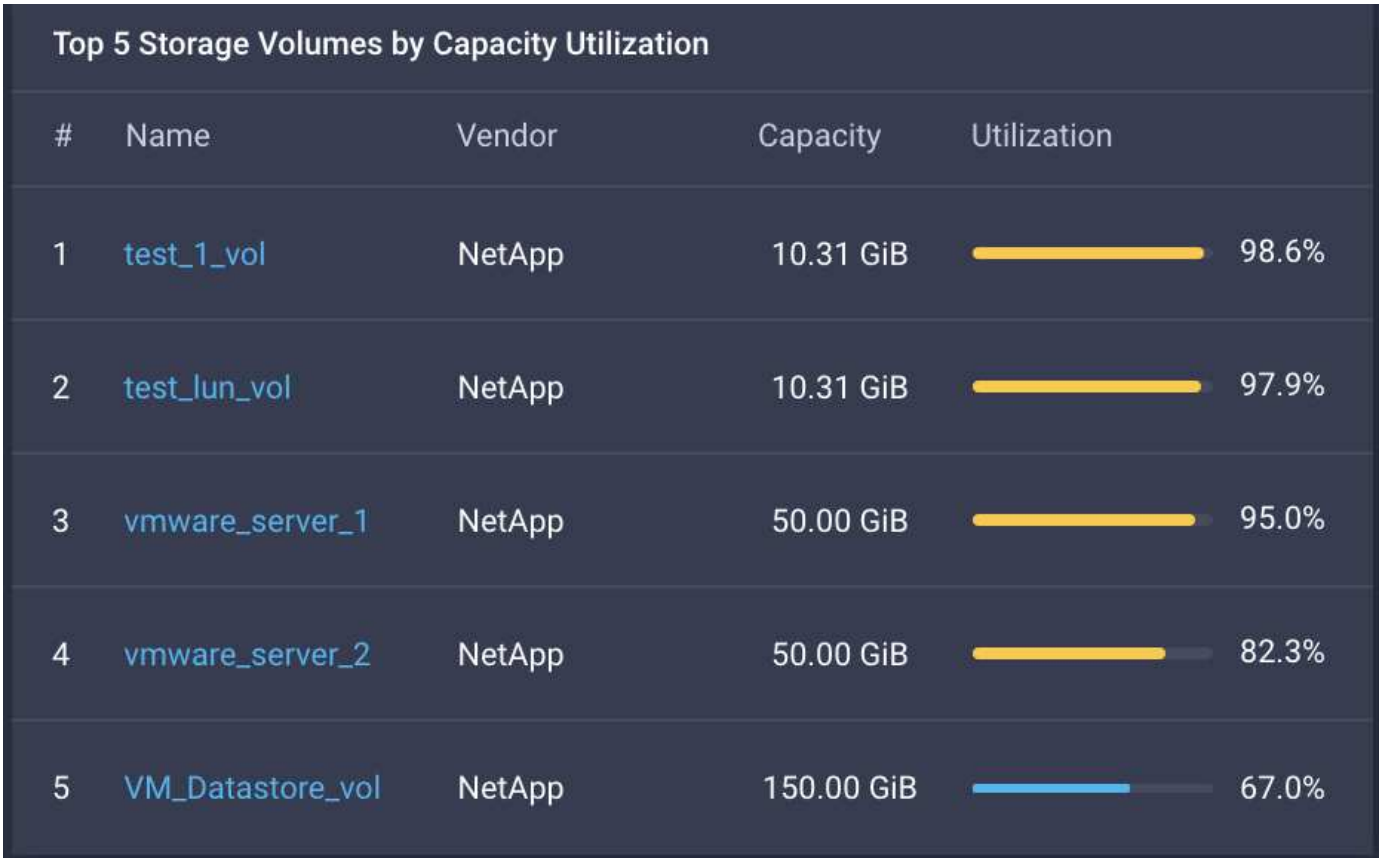
- 다음 스크린샷은 Storage Version Summary 위젯을 보여 줍니다.



- 이 스크린샷은 용량 활용률별 상위 5개 스토리지 어레이를 보여 줍니다.



- 이 스크린샷은 용량 활용률별 상위 5개 스토리지 볼륨을 보여 줍니다.



사용 사례

다음은 Cisco Intersight에서 NetApp 스토리지를 모니터링 및 오케스트레이션한 몇 가지 사용 사례 사례입니다.

사용 사례 **1: NetApp** 스토리지 인벤토리 및 위젯 모니터링

NetApp 스토리지 환경을 Cisco Intersight에서 사용할 수 있으면 NetApp 스토리지 객체를 스토리지 인벤토리에서 자세히 모니터링하고 스토리지 위젯에서 개요를 볼 수 있습니다.

1. Intersight Assist OVA 구축(vCenter 환경의 Onprem 작업)
2. Intersight Assist에 NetApp AIQ UM 장치를 추가합니다.
3. 스토리지 * 로 이동하여 NetApp 스토리지 인벤토리를 탐색할 수 있습니다.
4. NetApp 스토리지의 * 위젯 * 을 * 모니터 대시보드 * 에 추가합니다.

사용 사례 **2:** 참조 워크플로우를 사용하여 **NetApp** 스토리지 오케스트레이션

NetApp 스토리지 및 vCenter 환경을 Cisco Intersight에서 사용할 수 있으면 를 통해 GitHub에서 제공되는 엔드 투 엔드 참조 워크플로를 사용할 수 있습니다 "FlexPod Intersight 워크플로 저장소".

참조 워크플로에는 스토리지 및 가상화 작업이 포함됩니다. 리포지토리의 README 파일은 워크플로 실행에 필요한 필수 조건, 유용한 리소스에 대한 링크(워크플로 가져오기 방법에 대한 문서 포함) 및 각 참조 워크플로에 대한 문서 링크를 제공합니다.

각 워크플로에는 두 개의 파일이 들어 있는 리포지토리의 폴더가 있습니다.

- JSON 파일을 다운로드하여 Intersight로 가져옵니다.
- 워크플로의 작업, 워크플로 입력 및 워크플로 실행 예를 보여 주는 문서 파일입니다.

참조 워크플로를 가져오고 사용하려면 다음을 수행합니다.

1. Intersight Assist OVA 구축(vCenter 환경의 Onprem 작업)
2. Intersight Assist에 NetApp AIQ UM 장치를 추가합니다.
3. Intersight Assist를 통해 Intersight에 vCenter 타겟을 추가합니다.
4. FlexPod-Intersight-Workflow 저장소에서 참조 워크플로우용 JSON 파일을 다운로드하십시오.
5. 워크플로우를 Intersight로 가져온 다음 워크플로우를 실행합니다.

다음은 GitHub FlexPod-Intersight - 워크플로 저장소에서 사용할 수 있는 워크플로 목록입니다.

- NetApp 이니시에이터 그룹에 이니시에이터를 추가합니다
- NetApp 볼륨에 대한 새로운 내보내기 정책
- NetApp 스마트 볼륨을 사용하는 새 NAS 데이터 저장소입니다
- 새로운 NetApp FC 데이터 인터페이스
- 새 NetApp 이니시에이터 그룹

- 새로운 NetApp iSCSI 데이터 인터페이스
- 새로운 NetApp NAS 데이터 인터페이스
- 새로운 NetApp 스토리지 가상 시스템
- NetApp Smart LUN을 사용하는 새 VMFS 데이터 저장소입니다
- NetApp 이니시에이터 그룹에서 이니시에이터를 제거합니다
- NetApp 스마트 볼륨을 사용하여 NAS 데이터 저장소를 제거합니다
- NetApp 내보내기 정책을 제거합니다
- NetApp 이니시에이터 그룹을 제거합니다
- NetApp 스마트 LUN을 사용하여 VMFS 데이터 저장소를 제거합니다
- NetApp 스마트 볼륨을 사용하여 NAS 데이터 저장소를 업데이트합니다
- NetApp Smart LUN을 사용하여 VMFS 데이터 저장소를 업데이트합니다

사용 사례 **3:** 디자이너가 필요 없는 양식을 사용하는 사용자 지정 워크플로

Cisco Intersight에서 NetApp 스토리지 및 vCenter 환경을 사용할 수 있는 경우 NetApp 스토리지 및 가상화 작업을 사용하여 맞춤형 워크플로우를 구축할 수 있습니다.

1. Intersight Assist OVA 구축(vCenter 환경의 내부 작업)
2. Intersight Assist에 NetApp AIQ UM 장치를 추가합니다.
3. Intersight Assist를 통해 Intersight에 vCenter 타겟을 추가합니다.
4. Intersight에서 * Orchestration * 탭으로 이동합니다.
5. 워크플로 만들기 * 를 선택합니다.
6. 워크플로우에 스토리지 및 가상화 작업을 추가할 수 있습니다.

   다음은 Cisco Intersight에서 사용할 수 있는 NetApp 스토리지 작업입니다.

   - NetApp CIFS 공유에 ACL을 추가합니다
   - NetApp 내보내기 정책 규칙에 클라이언트 일치 항목을 추가합니다
   - NetApp 볼륨에 내보내기 정책을 추가합니다
   - NetApp 이니시에이터 그룹에 이니시에이터를 추가합니다
   - NetApp 내보내기 정책에 규칙을 추가합니다
   - NetApp 스냅샷 정책에 스케줄을 추가합니다
   - NetApp 라이센스 상태를 확인합니다
   - NetApp 스토리지 가상 머신 FCP 프로토콜 상태 확인
   - 스토리지 가상 시스템에 대한 NetApp 애그리게이트를 편집합니다
   - NetApp 비동기식 SnapMirror 정책을 편집합니다
   - NetApp CIFS 공유 ACL 권한을 편집합니다
   - NetApp 엑스포트 정책 규칙을 편집합니다

- NetApp 스냅샷 정책을 편집합니다
- NetApp 스냅샷 정책 일정을 편집합니다
- NetApp 볼륨 보안 스타일을 편집합니다
- NetApp 볼륨 스냅샷 정책을 편집합니다
- NetApp CIFS 서비스를 설정합니다
- NetApp LUN 을 확장합니다
- 새로운 NetApp 비동기식 SnapMirror 정책
- 새 NetApp CIFS 서버
- 새로운 NetApp CIFS 공유
- NetApp 이니시에이터 그룹 LUN 매핑을 찾습니다
- ID별로 NetApp LUN을 찾습니다
- ID별로 NetApp 볼륨을 찾습니다
- 새 NetApp 내보내기 정책
- 새로운 NetApp FC 데이터 인터페이스
- 새 NetApp 이니시에이터 그룹
- 새로운 NetApp iSCSI 데이터 인터페이스
- SVM 루트 볼륨용 새 NetApp 로드 공유 미러
- 새로운 NetApp LUN
- 새로운 NetApp LUN 매핑
- 새로운 NetApp NAS 데이터 인터페이스
- 새로운 NetApp NAS 스마트 볼륨
- 새로운 NetApp 스마트 LUN
- 볼륨에 대한 새로운 NetApp SnapMirror 관계
- 새로운 NetApp 스냅샷 정책
- 새로운 NetApp 스토리지 가상 시스템
- 새 NetApp 볼륨
- 새로운 NetApp 볼륨 스냅샷
- NetApp 스토리지 가상 머신용 DNS를 등록합니다
- NetApp CIFS 공유에서 ACL을 제거합니다
- NetApp 엑스포트 정책 규칙에서 클라이언트 일치 제거
- NetApp 볼륨에서 엑스포트 정책을 제거합니다
- NetApp 이니시에이터 그룹에서 이니시에이터를 제거합니다
- NetApp CIFS 서버를 제거합니다
- NetApp CIFS 공유를 제거합니다

- NetApp 내보내기 정책을 제거합니다
- NetApp FC 데이터 인터페이스를 제거합니다
- NetApp 이니시에이터 그룹을 제거합니다
- NetApp IP 인터페이스를 제거합니다
- SVM 루트 볼륨에 대한 NetApp 로드 공유 미러를 제거합니다
- NetApp LUN을 제거합니다
- NetApp LUN 매핑을 제거합니다
- NetApp NAS 스마트 볼륨을 제거합니다
- NetApp 스마트 LUN을 제거합니다
- 볼륨에 대한 NetApp SnapMirror 관계를 제거합니다
- NetApp SnapMirror 정책을 제거합니다
- NetApp 스냅샷 정책을 제거합니다
- NetApp 스토리지 가상 머신을 제거합니다
- NetApp 볼륨을 제거합니다
- NetApp 볼륨 스냅샷을 제거합니다
- NetApp 내보내기 정책에서 규칙을 제거합니다
- NetApp 스냅샷 정책에서 일정을 제거합니다
- NetApp 볼륨 스냅샷의 이름을 바꿉니다
- SVM 루트 볼륨에 대한 NetApp 로드 공유 미러를 업데이트합니다
- NetApp 볼륨 용량을 업데이트합니다

검토할 수 있습니다

Cisco UCSM, VMware vSphere 7.0 및 NetApp ONTAP 9를 사용하는 FlexPod용 엔드 투 엔드 NVMe

TR-4914: Cisco UCSM, VMware vSphere 7.0 및 NetApp ONTAP 9를 사용하는 FlexPod용 엔드 투 엔드 NVMe

Chris Schmitt와 Kamini Singh, NetApp

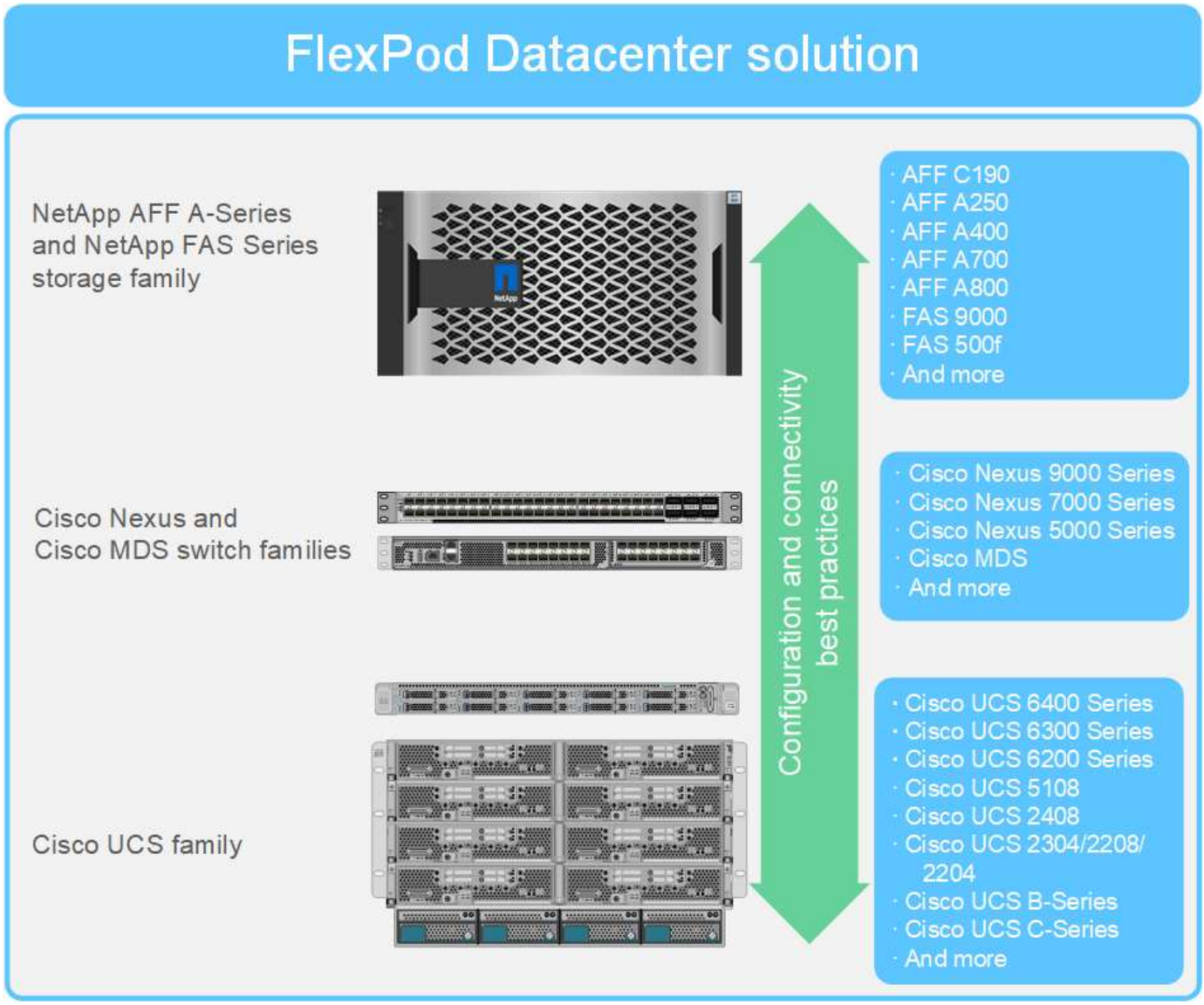
파트너 후원:

새로운 핵심 기술인 NVMe 데이터 스토리지 표준은 현재 및 미래 메모리 기술에 매우 높은 대역폭과 매우 짧은 지연 시간의 스토리지 액세스를 제공하여 엔터프라이즈 데이터 스토리지 액세스 및 전송을 변화시키고 있습니다. NVMe는 SCSI 명령 세트를 NVMe 명령 세트로 대체합니다.

NVMe는 비휘발성 플래시 드라이브, 멀티 코어 CPU 및 수 기가바이트의 메모리와 작동하도록 설계되었습니다. 또한 1970년대 이후 컴퓨터 과학의 상당한 발전을 활용하여 데이터를 보다 효율적으로 구문 분석하고 조작할 수 있는 효율적인 명령 집합을 지원합니다. 또한 엔드 투 엔드 NVMe 아키텍처를 통해 데이터 센터 관리자는 가상화된 컨테이너식 환경과 트랜잭션 중심 데이터베이스에서 지원할 수 있는 확장성을 재고할 수 있습니다.

FlexPod는 Cisco UCS(Cisco Unified Computing System), Cisco Nexus 스위치, Cisco MDS 스위치, NetApp AFF 시스템을 포함하는 모범 사례 데이터 센터 아키텍처입니다. 이러한 구성요소는 Cisco와 NetApp의 모범 사례에 따라 연결 및 구성되었으므로 다양한 엔터프라이즈 워크로드를 안심하고 실행할 수 있는 훌륭한 플랫폼을 제공합니다. FlexPod는 성능 및 용량을 늘리기 위해(필요에 따라 컴퓨팅, 네트워크 또는 스토리지 리소스를 개별적으로 추가) 스케일업하거나, 여러 개의 일관된 구축(예: 추가 FlexPod 스택 스케일아웃)이 필요한 환경을 위해 스케일아웃할 수 있습니다.

다음 그림에서는 FlexPod 구성 요소 제품군을 보여 줍니다.



FlexPod는 FC-NVMe를 도입하는 데 이상적인 플랫폼입니다. 기존 Cisco UCS B200 M5 또는 M6 서버 또는 Cisco UCS C-Series M5 또는 M6 랙 서버에 Cisco UCS VIC 1400 Series 및 Port Expander를 추가하여 지원할 수 있으며, Cisco UCS 시스템, Cisco MDS 32Gbps 스위치로 간단하고 중단 없는 소프트웨어 업그레이드를 수행할 수 있습니다. 및 NetApp AFF 스토리지 어레이를 모두 지원합니다. 지원되는 하드웨어 및 소프트웨어를 배치한 후 FC-NVMe의 구성은 FCP 구성과 비슷합니다.

NetApp ONTAP 9.5 이상은 전체 FC-NVMe 솔루션을 제공합니다. AFF A300, AFF A400, AFF A700, AFF A700s 및 AFF A800 어레이에 대한 무중단 ONTAP 소프트웨어 업데이트를 통해 이러한 장치에서 엔드-투-엔드 NVMe 스토리지 스택을 지원할 수 있습니다. 따라서 6세대 HBA(호스트 버스 어댑터) 및 NVMe 드라이버를 지원하는 서버는 네이티브 NVMe를 사용하여 이러한 어레이와 통신할 수 있습니다.

목표

이 솔루션은 FlexPod 기반의 VMware vSphere 7을 사용한 FC-NVMe 성능의 상위 수준 요약을 제공합니다. 이 솔루션은 FC-NVMe 트래픽을 성공적으로 전달하는 것으로 확인되었으며 다양한 데이터 블록 크기의 FC-NVMe에 성능 메트릭이 캡처되었습니다.

솔루션 이점

엔드 투 엔드 NVMe for FlexPod는 다음과 같은 솔루션 이점을 제공하는 고객에게 탁월한 가치를 제공합니다.

- NVMe는 SCSI, SAS 및 SATA와 같은 이전 표준보다 훨씬 빠른 고속 및 고대역폭 하드웨어 프로토콜인 PCIe를 사용합니다. 대부분의 까다로운 애플리케이션을 위해 Cisco UCS Server와 NetApp 스토리지 어레이 간에 높은 대역폭과 매우 짧은 지연 시간을 지원합니다.
- FC-NVMe 솔루션은 무손실 솔루션이며 차세대 애플리케이션의 확장성 요구사항을 처리할 수 있습니다. 새로운 기술에는 인공 지능(AI), 머신 러닝(ML), 딥 러닝(DL), 실시간 분석 및 기타 미션 크리티컬 애플리케이션이 포함됩니다.
- 전체 스택에서 모든 리소스를 효율적으로 사용하여 IT 비용을 절감합니다.
- 응답 시간을 대폭 단축하고 애플리케이션 성능을 향상하여 IOPS 및 처리량을 높이고 지연 시간을 줄여 줍니다. 이 솔루션은 기존 워크로드에 대해 최대 60% 더 높은 성능을 제공하며 지연 시간을 최대 50% 줄여줍니다.
- FC-NVMe는 뛰어난 큐 처리 기능을 갖춘 간소화된 프로토콜로, 특히 IOPS가 더 많은 초당 I/O 작업(트랜잭션 수 증가)과 병렬 활동이 더 많은 경우에 유용합니다.
- Cisco UCS, Cisco MDS, NetApp AFF 스토리지 어레이와 같은 FlexPod 구성요소의 무중단 소프트웨어 업그레이드를 제공합니다. 응용 프로그램을 수정할 필요가 없습니다.

"다음: 테스트 접근 방식."

테스트 접근 방식

"이전: 소개."

이 섹션에서는 FC-NVMe on FlexPod 검증 테스트에 대한 간략한 개요를 제공합니다. 여기에는 VMware vSphere 7을 사용하는 FlexPod용 FC-NVMe와 관련하여 워크로드 테스트를 수행하기 위해 채택된 테스트 환경/구성 및 테스트 계획이 모두 포함됩니다.

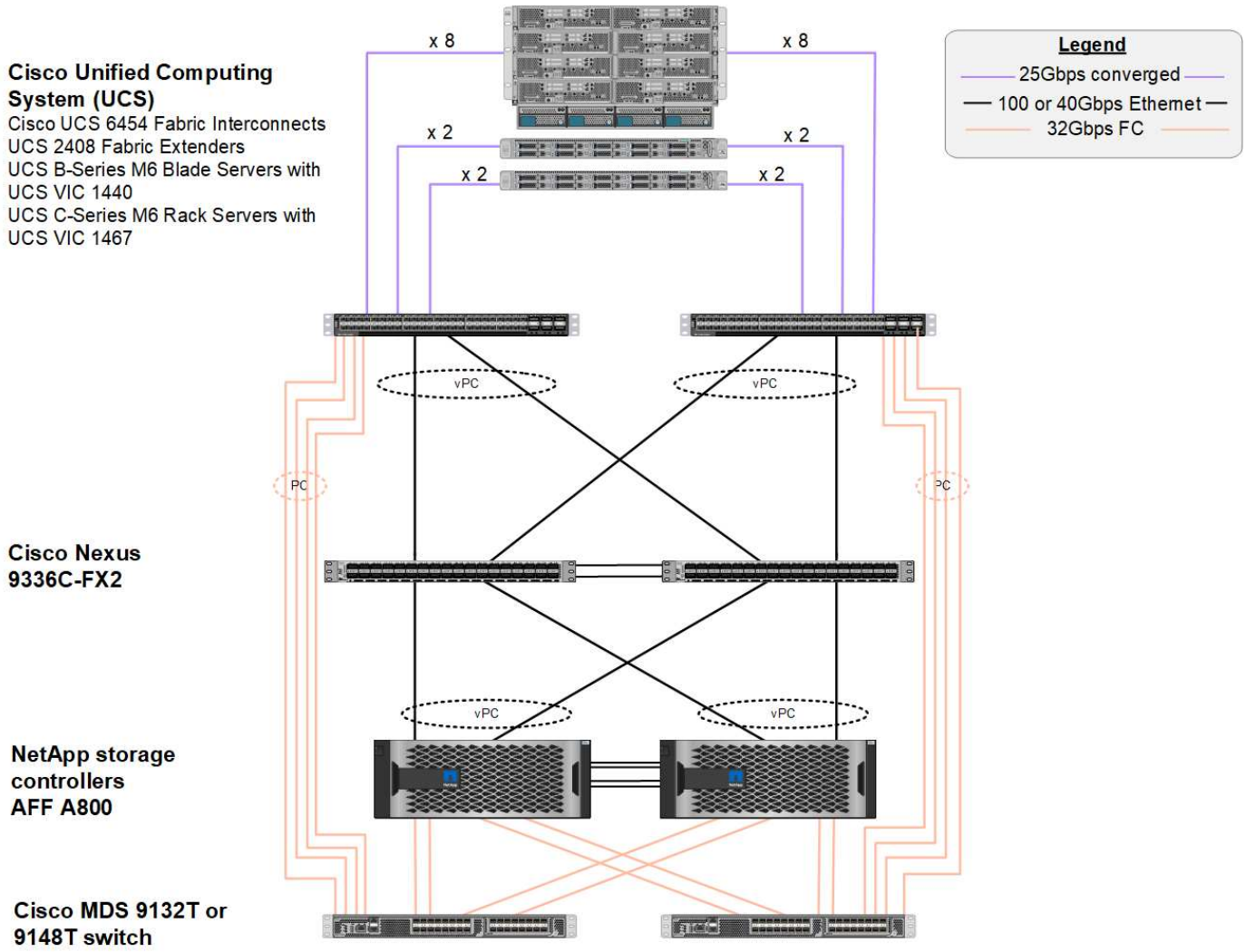
테스트 환경

Cisco Nexus 9000 시리즈 스위치는 2가지 운영 모드를 지원합니다.

- NX-OS 독립 실행형 모드, Cisco NX-OS 소프트웨어 사용
- Cisco ACI(Application Centric Infrastructure) 플랫폼을 사용하는 ACI 패브릭 모드

독립 실행형 모드에서 스위치는 일반적인 Cisco Nexus 스위치와 마찬가지로 높은 포트 밀도, 짧은 지연 시간, 40GbE 및 100GbE 연결을 지원합니다.

NX-OS가 포함된 FlexPod는 컴퓨팅, 네트워크 및 스토리지 계층에서 완전히 이중화되도록 설계되었습니다. 디바이스 또는 트래픽 경로 관점에서 단일 장애 지점이 없습니다. 아래 그림은 FC-NVMe의 이 검증에 사용된 최신 FlexPod 설계의 다양한 요소를 보여줍니다.



FC SAN 관점에서 볼 때 이 설계는 최신 4세대 Cisco UCS 6454 패브릭 상호 연결 및 서버에 포트 확장기가 있는 Cisco UCS VICS 1400 플랫폼을 사용합니다. Cisco UCS 섀시의 Cisco UCS B200 M6 블레이드 서버는 Cisco UCS 2408 Fabric Extender IOM에 연결된 포트 확장기가 있는 Cisco UCS VIC 1440을 사용하며, 각 FCoE(Fibre Channel over Ethernet) vHBA(Virtual Host Bus Adapter)의 속도는 40Gbps입니다. Cisco UCS가 관리하는 Cisco UCS C220 M5 랙 서버는 Cisco UCS VIC 1457을 사용하며, 각 Fabric Interconnect에 2개의 25Gbps 인터페이스가 제공됩니다. 각 C220 M5 FCoE vHBA의 속도는 50Gbps입니다.

Fabric 상호 연결은 32Gbps SAN 포트 채널을 통해 최신 세대 Cisco MDS 9148T 또는 9132T FC 스위치에 연결됩니다. Cisco MDS 스위치와 NetApp AFF A800 스토리지 클러스터 간의 연결도 32Gbps FC입니다. 이 구성은 스토리지 클러스터와 Cisco UCS 사이의 파이버 채널 프로토콜(FCP)과 FC-NVMe 스토리지를 위해 32Gbps FC를 지원합니다. 이 검증을 위해 각 스토리지 컨트롤러에 대한 FC 연결 4개가 사용됩니다. 각 스토리지 컨트롤러에서 FC 포트 4개가 FCP 및 FC-NVMe 프로토콜 모두에 사용됩니다.

Cisco Nexus 스위치와 최신 세대 NetApp AFF A800 스토리지 클러스터 간의 연결은 스토리지 컨트롤러의 포트 채널 및 스위치의 vPC에서도 100Gbps입니다. NetApp AFF A800 스토리지 컨트롤러는 고속 PCIe(Peripheral Connect Interface Express) 버스에 NVMe 디스크를 장착하고 있습니다.

이 검증에 사용된 FlexPod 구현은 를 기반으로 합니다 "UCS 관리 모드, VMware vSphere 7.0U2 및 NetApp ONTAP 9.9의 Cisco UCS 4.2(1)가 설치된 FlexPod 데이터 센터".

검증된 하드웨어 및 소프트웨어

다음 표에는 솔루션 검증 프로세스 중에 사용되는 하드웨어 및 소프트웨어 버전이 나와 있습니다. Cisco와 NetApp은 상호 운용성 매트릭스를 보유하고 있으며, 이러한 매트릭스는 FlexPod의 특정 구현 지원을 결정하는 데 참조되어야 합니다. 자세한 내용은 다음 리소스를 참조하십시오.

- "NetApp 상호 운용성 매트릭스 툴"
- "Cisco UCS 하드웨어 및 소프트웨어 상호 운용성 툴"

레이어	장치	이미지	설명
없습니다	• Cisco UCS 6454 패브릭 인터커넥트 2개 • 2개의 Cisco UCS 2408 I/O 모듈이 있는 1개의 Cisco UCS 5108 블레이드 섀시 • Cisco UCS B200 M6 블레이드 4개, 각각 Cisco UCS VIC 1440 어댑터 및 포트 확장기 카드 1개 포함	릴리스 4.2(1f)	Cisco UCS Manager, Cisco UCS VIC 1440 및 포트 확장기를 포함합니다
CPU	2.0GHz의 Intel Xeon Gold 6330 CPU 2개, 42MB Layer 3 캐시 및 CPU당 28코어	–	–
메모리	1024GB(3200MHz로 작동하는 16x 64GB DIMM)	–	–
네트워크	NX-OS 독립 실행형 모드의 Cisco Nexus 9336C-FX2 스위치 2개	릴리스 9.3(8)	–
스토리지 네트워크	Cisco MDS 9132T 32Gbps 32포트 FC 스위치 2개	릴리즈 8.4(2c)	FC-NVMe SAN 분석 지원
스토리지	24x 1.8TB NVMe SSD가 장착된 NetApp AFF A800 스토리지 컨트롤러 2개	NetApp ONTAP 9.9.1P1	–
소프트웨어	Cisco UCS Manager를 참조하십시오	릴리스 4.2(1f)	–
	VMware vSphere를 참조하십시오	7.0U2	–
	VMware ESXi	7.0.2	–
	VMware ESXi 네이티브 파이버 채널 NIC 드라이버(NFNIC)	5.0.12	VMware에서 FC-NVMe 지원

레이어	장치	이미지	설명
	VMware ESXi 네이티브 이더넷 NIC 드라이버(NENIC)	1.0.35.0	–
테스트 툴	FiO	3.19	–

테스트 계획

우리는 가상 워크로드를 사용하여 FlexPod에서 NVMe를 검증하기 위한 성능 테스트 계획을 개발했습니다. 이 워크로드를 통해 8KB 랜덤 읽기 및 쓰기와 64KB 읽기 및 쓰기를 실행할 수 있었습니다. VMware ESXi 호스트를 사용하여 AFF A800 스토리지에 대해 테스트 사례를 실행했습니다.

우리는 성능 측정에 사용할 수 있는 오픈 소스 합성 I/O 도구인 FIO를 사용하여 가상 워크로드를 생성했습니다.

성능 테스트를 완료하기 위해 스토리지와 서버 모두에서 몇 가지 구성 단계를 수행했습니다. 다음은 구현을 위한 세부 단계입니다.

1. 스토리지 측면에 4개의 스토리지 가상 시스템(SVM, 이전의 vserver), SVM당 8개의 볼륨 및 볼륨당 1개의 네임스페이스를 생성했습니다. 1TB 볼륨 및 960GB 네임스페이스가 생성되었습니다. NetApp은 SVM당 4개의 LIF와 SVM당 1개의 하위 시스템을 생성했습니다. SVM LIF는 클러스터에 있는 8개의 사용 가능한 FC 포트에 균등하게 분산되었습니다.
2. 서버 측에서 각 ESXi 호스트에 총 4개의 VM에 대해 단일 가상 머신(VM)을 생성했습니다. 가상 워크로드를 실행하기 위해 서버에 FIO를 설치했습니다.
3. 스토리지 및 VM을 구성한 후에는 ESXi 호스트에서 스토리지 네임스페이스에 연결할 수 있었습니다. 덕분에 네임스페이스를 기반으로 데이터 저장소를 생성한 다음 이러한 데이터 저장소를 기반으로 VMDK(가상 머신 디스크)를 생성할 수 있었습니다.

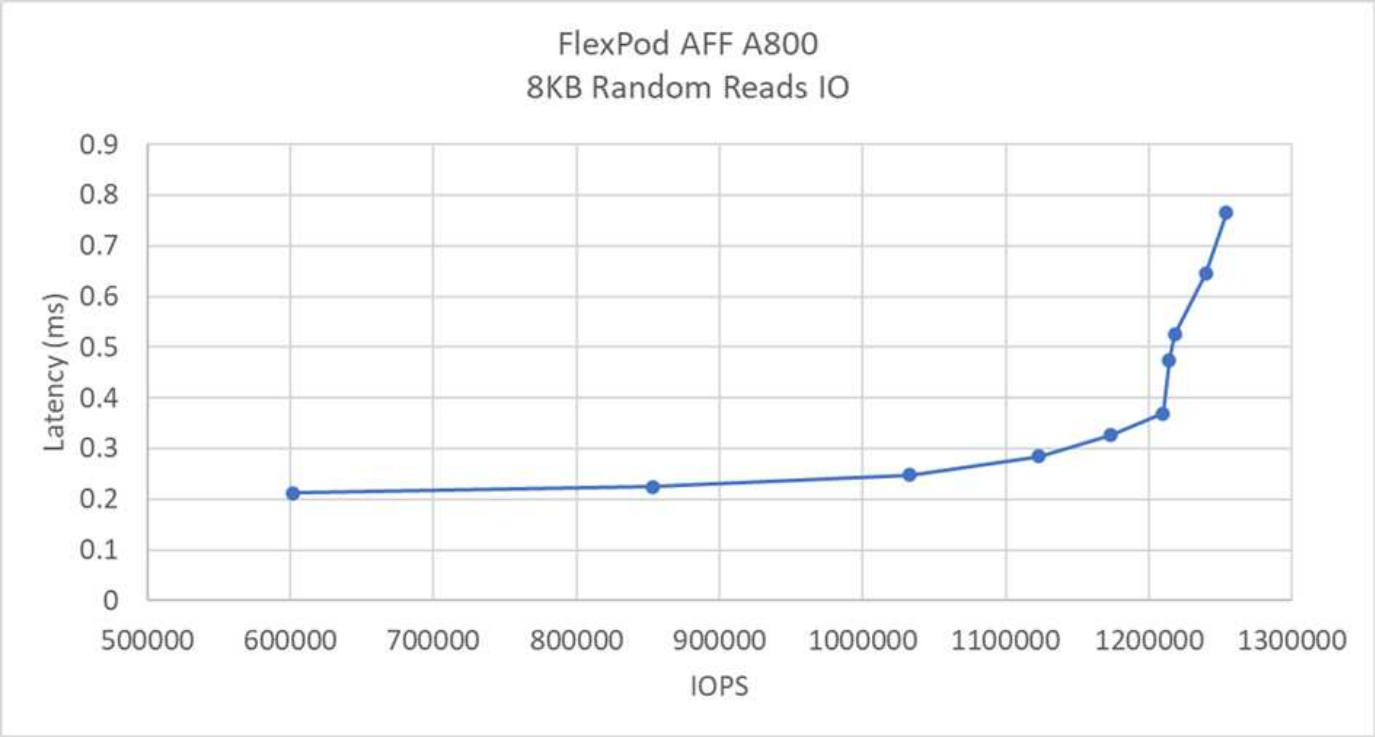
"다음: 테스트 결과."

테스트 결과

"이전: 테스트 접근 방식."

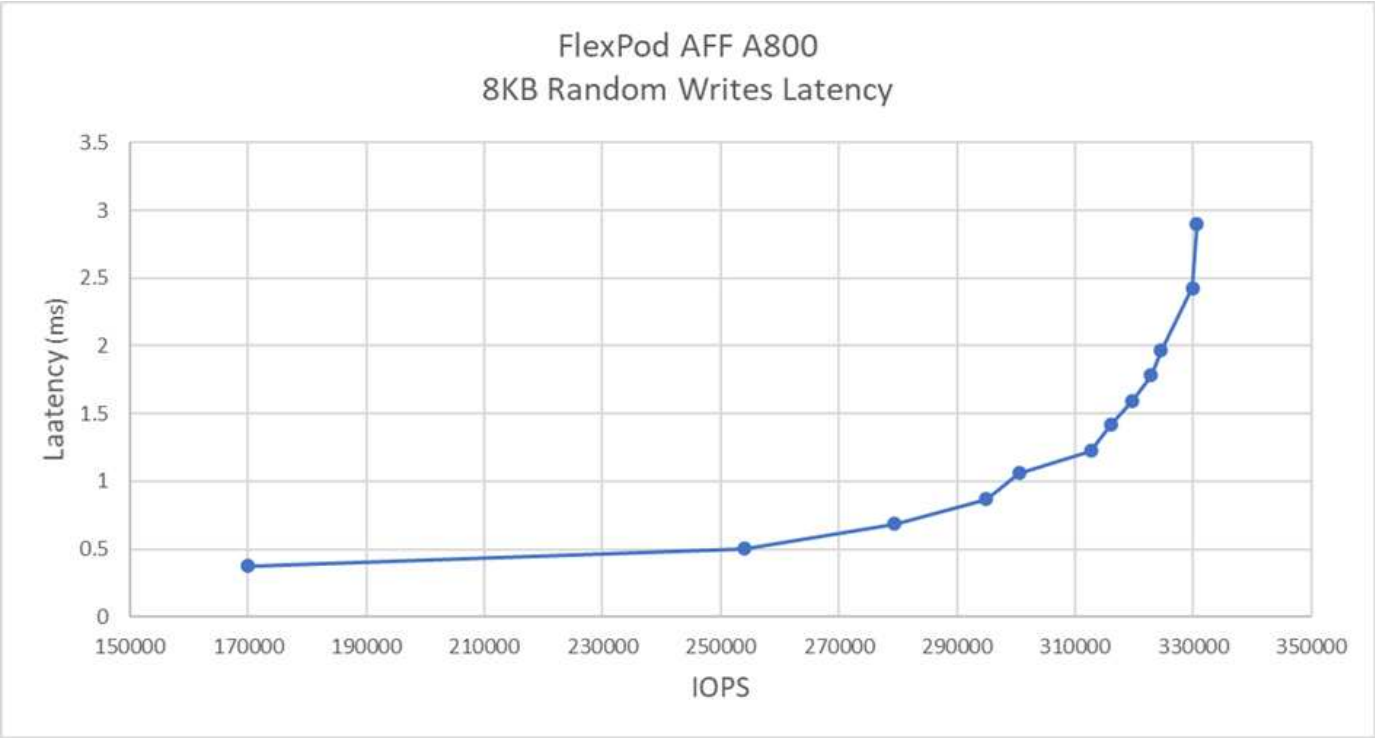
테스트는 IOPS 및 지연 시간 측면에서 FC-NVMe 성능을 측정하기 위해 FIO 워크로드를 실행하는 것으로 구성되었습니다.

다음 그래프는 8KB 블록 크기를 사용하여 100% 랜덤 읽기 워크로드를 실행할 때의 결과를 보여줍니다.



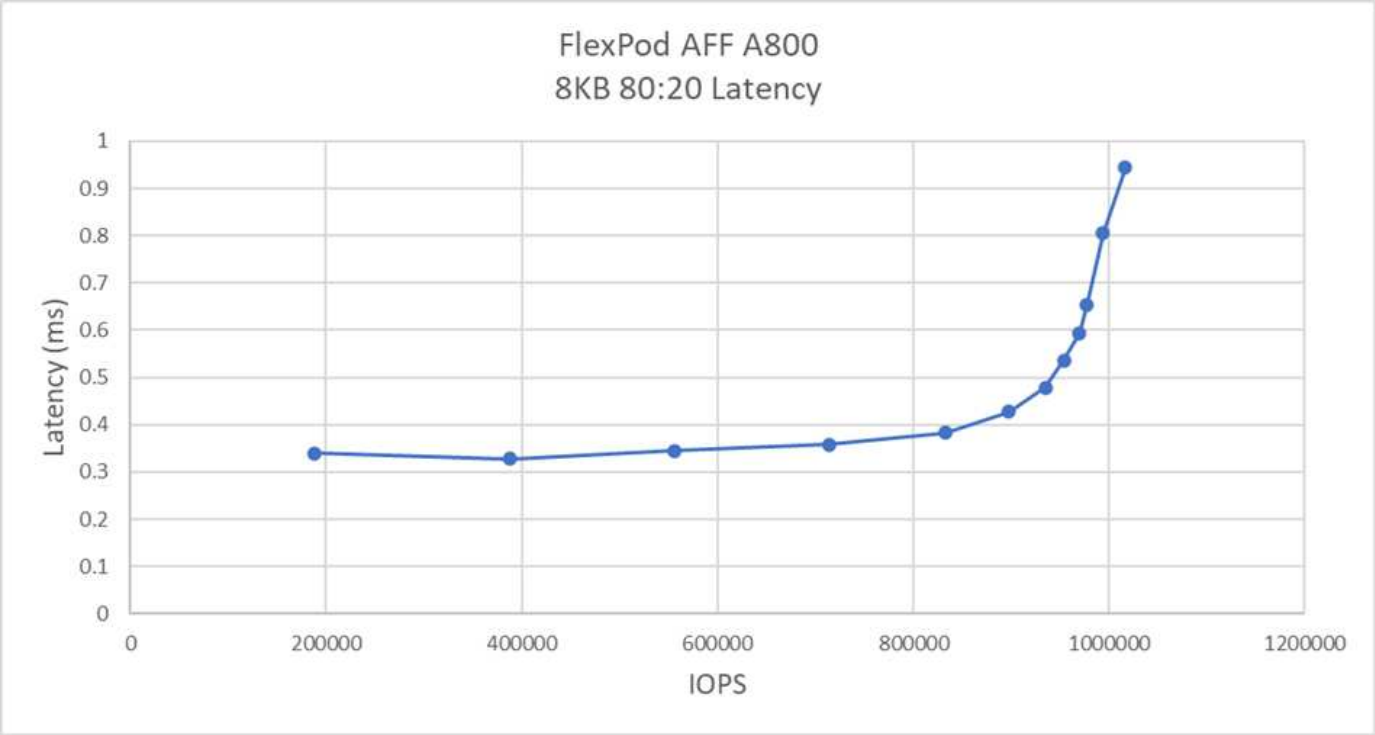
이 테스트에서는 서버 측 지연 시간이 0.35ms 미만으로 유지하면서 시스템이 120만 IOPS 이상을 달성하는 것을 발견했습니다.

다음 그래프는 8KB 블록 크기를 사용하여 100% 랜덤 쓰기 워크로드를 실행할 때 얻은 결과를 보여 줍니다.



이 테스트에서는 약 300,000 IOPS를 달성했지만 1ms 미만의 서버 측 지연 시간만 유지된다는 사실을 발견했습니다.

8KB 블록 크기, 80% 랜덤 읽기 및 20% 쓰기의 경우 다음과 같은 결과를 확인했습니다.



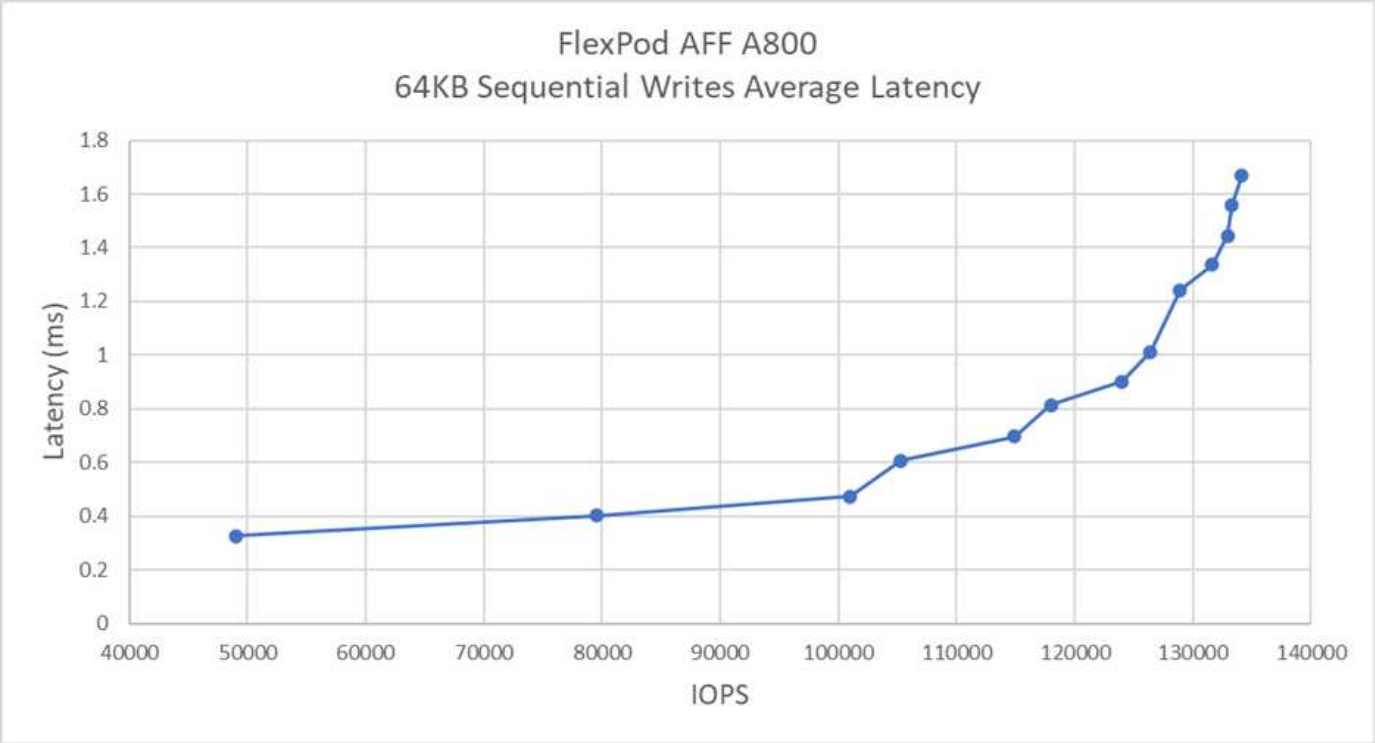
테스트에서는 시스템이 1백만 IOPS 이상을 달성하는 동시에 1ms 미만의 서버 측 지연 시간을 유지한다는 사실을 발견했습니다.

64KB 블록 크기 및 100% 순차적 읽기의 경우 다음 결과가 관찰되었습니다.



이번 테스트에서 시스템은 지연 시간이 1ms 미만인 동시에 약 250,000 IOPS를 실현했다는 사실을 확인했습니다.

64KB 블록 크기 및 100% 순차적 쓰기의 경우 다음 결과가 관찰되었습니다.



이 테스트에서는 약 120k IOPS를 달성하면서 1ms 미만의 서버 측 지연 시간을 유지하던 시스템이 나타났습니다.

"다음: 결론."

결론

"이전: 테스트 결과."

이 솔루션에서 관찰된 처리량은 1ms의 지연 시간 미만의 순차 읽기 워크로드를 위한 14GBps 및 220k IOPS입니다. 랜덤 읽기 워크로드의 경우 9.5GBps 및 1.25M IOPS의 처리량을 기록했습니다. FlexPod의 FC-NVMe로 이러한 성능을 제공하면 모든 미션 크리티컬 애플리케이션의 요구사항을 해결할 수 있습니다.

VMware vSphere 7.0 U2를 사용하는 FlexPod 데이터 센터는 다양한 IT 워크로드에 FC-NVMe를 구축하여 이를 필요로 하는 애플리케이션에 고성능 스토리지 액세스를 제공하는 최적의 공유 인프라 기반입니다. FC-NVMe가 고가용성, 다중 경로, 추가 운영 체제 지원을 포함하는 방향으로 발전함에 따라, FlexPod은 이러한 기능을 지원하는 데 필요한 확장성과 안정성을 제공하는 엄선된 플랫폼에 적합합니다.

Cisco와 NetApp은 FlexPod를 통해 다양한 사용 사례 및 애플리케이션에 맞게 유연하고 확장 가능한 플랫폼을 개발했습니다. FC-NVMe를 통해 FlexPod은 동일한 공유 인프라에서 동시에 실행되는 비즈니스 크리티컬 애플리케이션을 효율적이고 효과적으로 지원할 수 있는 또 다른 기능을 추가합니다. 또한 FlexPod의 유연성과 확장성을 통해 고객은 변화하는 비즈니스 요구사항에 맞게 성장하고 조정할 수 있는 적정 규모의 인프라로 시작할 수 있습니다.

추가 정보

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

- Cisco UCS(Unified Computing System)

  "http://www.cisco.com/en/US/products/ps10265/index.html"

- Cisco UCS 6400 Series Fabric Interconnect 데이터 시트

  "https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/datasheet-c78-741116.html"

- Cisco UCS 5100 시리즈 블레이드 서버 섀시

  "http://www.cisco.com/en/US/products/ps10279/index.html"

- Cisco UCS B-Series 블레이드 서버

  "http://www.cisco.com/en/US/partner/products/ps10280/index.html"

- Cisco UCS C-Series 랙 서버

  "http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html"

- Cisco Unified Computing System 어댑터

  "http://www.cisco.com/en/US/products/ps10277/prod_module_series_home.html"

- Cisco UCS Manager를 참조하십시오

  "http://www.cisco.com/en/US/products/ps10281/index.html"

- Cisco Nexus 9000 시리즈 스위치

  "http://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html"

- Cisco MDS 9000 Multilayer Fabric 스위치

  "http://www.cisco.com/c/en/us/products/storage-networking/mds-9000-series-multilayer-switches/index.html"

- Cisco MDS 9132T 32Gbps 32포트 파이버 채널 스위치

  "https://www.cisco.com/c/en/us/products/collateral/storage-networking/mds-9100-series-multilayer-fabric-switches/datasheet-c78-739613.html"

- NetApp ONTAP 9

  "http://www.netapp.com/us/products/platform-os/ontap/index.aspx"

- NetApp AFF A 시리즈

  "http://www.netapp.com/us/products/storage-systems/all-flash-array/aff-a-series.aspx"

- VMware vSphere를 참조하십시오

  "https://www.vmware.com/products/vsphere"

- VMware vCenter Server를 참조하십시오

  "http://www.vmware.com/products/vcenter-server/overview.html"

- 최신 SAN에 대한 모범 사례

  "https://www.netapp.com/us/media/tr-4080.pdf"

- FlexPod용 엔드 투 엔드 NVMe 소개

  "https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/whitepaper-c11-741907.html"

상호 운용성 매트릭스

- NetApp 상호 운용성 매트릭스 툴

  "http://support.netapp.com/matrix/"

- Cisco UCS 하드웨어 호환성 매트릭스

  "https://ucshcltool.cloudapps.cisco.com/public/"

- VMware 호환성 가이드 를 참조하십시오

  "http://www.vmware.com/resources/compatibility"

감사의 말

저자는 이 프로젝트 실행 중에 제공된 지원 및 지침에 대해 Cisco의 John George와 NetApp의 Scott Lane과 Bobby Oommen에게 감사를 전합니다.

법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

저작권

"https://www.netapp.com/company/legal/copyright/"

상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

"https://www.netapp.com/company/legal/trademarks/"

특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

개인 정보 보호 정책

"https://www.netapp.com/company/legal/privacy-policy/"

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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