

vSphere IaaS 제어부 설치 및 구성

업데이트 3

VMware vSphere 8.0

VMware vCenter 8.0

VMware ESXi 8.0

VMware by Broadcom 웹 사이트

<https://docs.vmware.com/kr>에서 최신 기술 문서를 찾을 수 있습니다.

VMware by Broadcom

3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2022-2024 Broadcom. All Rights Reserved. “Broadcom”은 Broadcom Inc. 및/또는 해당 자회사를 뜻합니다. 자세한 내용은 <https://www.broadcom.com> 페이지를 참조하십시오. 여기에서 언급된 모든 상표, 상호, 서비스 마크 및 로고는 해당 회사의 소유입니다.

목차

"vSphere IaaS 제어부 설치 및 구성" 7

업데이트된 정보 8

1 vSphere IaaS control plane 설치 및 구성 워크플로 10

vSphere 클러스터에서 vSphere IaaS control plane를 구성하기 위한 사전 요구 사항 17

2 vSphere IaaS control plane에 대한 스토리지 정책 생성 20

3 다중 영역 감독자 배포를 위한 vSphere 영역 생성 23

vSphere 영역 관리 24

4 vSphere IaaS control plane에 대한 네트워킹 25

감독자 네트워킹 25

vSphere IaaS control plane에 대한 NSX 설치 및 구성 35

vSphere Distributed Switch 생성 및 구성 37

분산 포트 그룹 생성 38

vSphere Distributed Switch에 호스트 추가 39

NSX Manager 배포 및 구성 41

NSX Manager 노드를 배포하여 클러스터 구성 42

라이선스 추가 44

계산 관리자 추가 44

전송 영역 생성 45

호스트 터널 끝점 IP 주소에 대한 IP 풀 생성 46

Edge 노드에 대한 IP 풀 생성 47

호스트 업링크 프로파일 생성 47

Edge 업링크 프로파일 생성 48

전송 노드 프로파일 생성 48

클러스터에서 NSX 구성 49

NSX Edge 전송 노드 구성 및 배포 50

NSX Edge 클러스터 생성 52

Tier-0 업링크 세그먼트 생성 52

Tier-0 게이트웨이 생성 53

NSX 및 NSX Advanced Load Balancer 설치 및 구성 55

NSX Advanced Load Balancer와 함께 사용할 감독자용 vSphere Distributed Switch 생성 58

NSX Manager 배포 및 구성 59

- NSX Manager 노드를 배포하여 클러스터 구성 61
- 라이선스 추가 62
- 계산 관리자 추가 63
- 전송 영역 생성 64
 - 호스트 터널 끝점 IP 주소에 대한 IP 풀 생성 65
 - Edge 노드에 대한 IP 풀 생성 66
- ESXi 호스트 업링크 프로파일 생성 66
 - NSX Edge 업링크 프로파일 생성 67
 - 전송 노드 프로파일 생성 68
 - NSX Edge 클러스터 프로파일 생성 69
- 클러스터에서 NSX 구성 69
 - NSX Edge 전송 노드 생성 70
 - NSX Edge 클러스터 생성 72
- Tier-0 게이트웨이 생성 73
 - Edge Tier-0 게이트웨이에서 NSX 경로 맵 구성 75
 - Tier-1 게이트웨이 생성 76
 - Tier-0 업링크 세그먼트 및 오버레이 세그먼트 생성 77
- NSX을 사용하여 vSphere IaaS control plane용 NSX Advanced Load Balancer 설치 및 구성 77
 - NSX Advanced Load Balancer OVA를 로컬 콘텐츠 라이브러리로 가져오기 78
 - NSX Advanced Load Balancer Controller 배포 79
 - NSX Advanced Load Balancer Controller 구성 81
 - 서비스 엔진 그룹 구성 84
 - NSX Advanced Load Balancer 사용에 대한 제한 사항 88
- NSX Advanced Load Balancer 설치 및 구성 88
 - NSX Advanced Load Balancer와 함께 사용할 감독자용 vSphere Distributed Switch 생성 89
 - NSX Advanced Load Balancer OVA를 로컬 콘텐츠 라이브러리로 가져오기 91
 - NSX Advanced Load Balancer 컨트롤러 배포 92
 - 컨트롤러 클러스터 배포 93
 - 컨트롤러 전원 켜기 94
 - 컨트롤러 구성 94
 - 라이선스 추가 98
 - 컨트롤러에 인증서 할당 99
 - 서비스 엔진 그룹 구성 101
 - 정적 경로 구성 102
 - 가상 IP 네트워크 구성 102
 - NSX Advanced Load Balancer 테스트 104
- HAProxy 로드 밸런서 설치 및 구성 104
 - HAProxy 로드 밸런서와 함께 사용할 감독자용 vSphere Distributed Switch 생성 104
 - HAProxy 로드 밸런서 제어부 VM 배포 105
 - HAProxy 로드 밸런서 사용자 지정 107

- 5 3개 영역 감독자 배포 110**
 - VDS 네트워킹 스택을 사용하여 3개 영역 감독자 배포 110
 - NSX 네트워킹을 사용하여 3개 영역 감독자 배포 120

- 6 1개 영역 감독자 배포 127**
 - VDS 네트워킹 스택을 사용하여 1개 영역 감독자 배포 127
 - 감독자 네트워킹을 사용하여 1개 영역 NSX 배포 137

- 7 NSX 네트워킹에 사용되는 로드 밸런서 확인 143**

- 8 감독자 구성 내보내기 144**

- 9 JSON 구성 파일을 가져와서 감독자 배포 146**

- 10 감독자에 라이선스 할당 149**

- 11 vSphere IaaS control plane 클러스터에 연결 151**
 - vSphere에 대한 Kubernetes CLI 도구 다운로드 및 설치 151
 - vSphere IaaS control plane 클러스터에 대한 보안 로그인 구성 153
 - vCenter Single Sign-On 사용자로 감독자에 연결 154
 - 개발자에게 Tanzu Kubernetes 클러스터에 대한 액세스 권한 부여 156

- 12 감독자 구성 및 관리 158**
 - VIP 인증서를 교체하여 감독자 API 끝점에 안전하게 연결 159
 - 감독자의 Tanzu Kubernetes Grid를 Tanzu Mission Control과 통합 160
 - Tanzu Kubernetes Grid 클러스터에 대한 기본 CNI 설정 162
 - 감독자의 제어부 크기 변경 164
 - VDS 네트워킹으로 구성된 감독자에서 로드 밸런서 설정 변경 165
 - VDS 네트워킹으로 구성된 감독자에 워크로드 네트워크 추가 166
 - 감독자에서 관리 네트워크 설정 변경 168
 - VDS 네트워킹으로 구성된 감독자에서 워크로드 네트워크 설정 변경 169
 - NSX로 구성된 감독자에서 워크로드 네트워크 설정 변경 170
 - vSphere IaaS control plane에서 HTTP 프록시 설정 구성 172
 - vSphere Client를 사용하여 감독자에서 HTTP프록시 설정 구성 173
 - 클러스터 관리 API 및 DCLI를 사용하여 감독자에 대한 HTTP 프록시 구성 174
 - Tanzu Mission Control을 위해 감독자 및 TKG 클러스터에서 HTTP 프록시 설정 구성 175
 - TKG 서비스 클러스터와 함께 사용할 외부 IDP 구성 176
 - 외부 IDP를 감독자에 등록 184
 - 감독자의 스토리지 설정 변경 188

- 사용자 지정 관찰 가능성 플랫폼으로 감독자 메트릭 스트리밍 189
- 감독자 제어부 DNS 이름 목록 수정 194
- 외부 모니터링 시스템에 감독자 로그 전달 194

13 기존 구성을 복제하여 감독자 배포 200

14 감독자 사용 설정 문제 해결 202

- 활성화 또는 업데이트 중 감독자 제어부 VM의 오류 상태 해결 202
- 감독자 제어부의 로그를 원격 rsyslog로 스트리밍 206
- 워크로드 관리 사용 설정 클러스터 호환성 오류 문제 해결 208
- 워크로드 관리 로그 파일에 tail 명령 사용 209

15 네트워킹 문제 해결 211

- NSX Manager에 vCenter Server 등록 211
 - NSX 장치 암호를 변경할 수 없음 212
 - 실패한 워크플로 및 불안정한 NSX Edge 문제 해결 212
 - NSX 문제 해결을 위한 지원 번들 수집 212
 - NSX에 대한 로그 파일 수집 213
 - NSX 관리 인증서, 지문 또는 IP 주소가 변경되면 WCP 서비스 다시 시작 214
- NSX Advanced Load Balancer 문제 해결을 위한 지원 번들 수집 214
 - NSX Advanced Load Balancer 구성이 적용되지 않음 215
 - ESXi 호스트를 유지 보수 모드로 전환할 수 없음 216
 - IP 주소 문제 해결 216
 - 트래픽 장애 문제 해결 218
 - NSX 백업 및 복원으로 인한 문제 해결 218
 - NSX 백업 및 복원 후 오래된 Tier-1 세그먼트 219
 - 호스트 전송 노드 트래픽에 필요한 VDS 219

16 vSphere IaaS control plane 문제 해결 221

- 스토리지 모범 사례 및 문제 해결 221
 - vSAN이 아닌 데이터스토어에서 제어부 VM에 대한 반선호도 규칙 사용 221
 - vSphere에서 제거된 스토리지 정책이 계속 Kubernetes 스토리지 클래스로 표시됨 222
 - vSAN Direct에서 외부 스토리지 사용 223
- 네트워크 토폴로지 업그레이드 문제 해결 224
 - Edge 로드 밸런서 용량이 부족하여 업그레이드 사전 검사가 실패함 225
 - 업그레이드 중에 감독자 워크로드 네임스페이스를 건너뛴 225
 - 업그레이드하는 동안 로드 밸런서 서비스를 건너뛴 225
- vSphere IaaS control plane 워크로드 도메인 종료 및 시작 226
- 감독자를 위한 지원 번들 수집 226

"vSphere IaaS 제어부 설치 및 구성"

"vSphere IaaS 제어부 설치 및 구성" 항목은 vSphere Client(이전 이름: vSphere with Tanzu)를 사용하여 vSphere IaaS control plane을 구성하고 관리하는 방법에 대한 정보를 제공합니다.

"vSphere IaaS 제어부 설치 및 구성" 항목은 기존 vSphere 클러스터에서 vSphere IaaS control plane를 사용하도록 설정하고 네임스페이스를 생성 및 관리하기 위한 지침을 제공합니다. 이 정보는 kubectl을 통해 Kubernetes 제어부와 세션을 설정하는 방법에 대한 지침도 제공합니다.

대상 사용자

"vSphere IaaS 제어부 설치 및 구성" 항목은 vSphere에서 vSphere IaaS control plane를 사용하도록 설정하고 네임스페이스를 구성하고 DevOps 팀에 제공하려는 vSphere 관리자를 대상으로 합니다. vSphere IaaS control plane를 사용하려는 vSphere 관리자는 컨테이너 및 Kubernetes에 대한 기본적인 지식이 있어야 합니다.

업데이트된 정보

이 "vSphere IaaS 제어부 설치 및 구성" 게시물은 제품의 각 릴리스에 따라 또는 필요할 때 업데이트됩니다.

이 표에는 "vSphere IaaS 제어부 설치 및 구성" 설명서의 업데이트 기록이 나와 있습니다.

개정	설명
2024년 6월 25일	vSphere 8.0 업데이트 3 릴리스에 대한 일반 업데이트 및 개선 사항입니다.
2024년 3월 18일	VIP 인증서를 교체하여 감독자 API 끝점에 안전하게 연결 항목이 전체 인증서 체인 가져오기에 대한 참고 사항으로 업데이트되었습니다.
2024년 2월 29일	<ul style="list-style-type: none"> ■ 컨트롤러의 초기 구성 중에 사용자 지정 클라우드를 생성하기 위한 단계가 추가되었습니다. 컨트롤러 구성의 내용을 참조하십시오. ■ 감독자를 배포하는 동안 클라우드를 선택하는 단계가 추가되었습니다. VDS 네트워킹 스택을 사용하여 3개 영역 감독자 배포 및 VDS 네트워킹 스택을 사용하여 1개 영역 감독자 배포의 내용을 참조하십시오. ■ 감독자를 사용하여 FQDN 로그인을 구성하는 단계가 추가되었습니다. VDS 네트워킹 스택을 사용하여 3개 영역 감독자 배포, VDS 네트워킹 스택을 사용하여 1개 영역 감독자 배포 및 감독자에서 관리 네트워크 설정 변경의 내용을 참조하십시오. ■ NSX 오버레이 세그먼트를 생성하는 단계가 추가되었습니다. Tier-0 업링크 세그먼트 및 오버레이 세그먼트 생성의 내용을 참조하십시오.
2024년 1월 24일	<ul style="list-style-type: none"> ■ NSX Advanced Load Balancer Controller를 NSX Manager에 등록 항목이 DNS 및 NTP 설정에 대한 참고 사항으로 업데이트되었습니다. ■ 사설 CA(인증 기관) 서명 인증서가 제공될 때 감독자 배포가 완료되지 않고 NSX Advanced Load Balancer 구성이 적용되지 않는 경우 수행할 단계에 대한 콘텐츠가 추가되었습니다. NSX Advanced Load Balancer 구성이 적용되지 않음의 내용을 참조하십시오.
2023년 12월 23일	<ul style="list-style-type: none"> ■ VDS 네트워킹으로 구성된 감독자에서 로드 밸런서 설정을 변경하기 위한 콘텐츠가 추가되었습니다. VDS 네트워킹으로 구성된 감독자에서 로드 밸런서 설정 변경의 내용을 참조하십시오. ■ VDS 네트워킹으로 구성된 감독자의 워크로드 네트워킹 설정을 변경하기 위한 콘텐츠가 업데이트되었습니다. VDS 네트워킹으로 구성된 감독자에서 워크로드 네트워크 설정 변경의 내용을 참조하십시오.
2023년 12월 13일	ESXi 호스트를 전송 노드로 준비하기 위한 참조가 추가되었습니다. 호스트 전송 노드 트래픽에 필요한 VDS 의 내용을 참조하십시오.
2023년 11월 21일	감독자 클러스터에서 다중 NSX가 지원되지 않음을 나타내기 위해 설명서가 업데이트되었습니다. 계산 관리자 추가 의 내용을 참조하십시오.
2023년 9월 29일	<ul style="list-style-type: none"> ■ vSphere IaaS control plane에서 HTTP 프록시 설정 구성에 대한 업데이트. ■ HAProxy 로드 밸런서를 사용자 지정하기 위한 요구 사항이 업데이트되었습니다. HAProxy 로드 밸런서 사용자 지정의 내용을 참조하십시오. <p>로드 중 오류.</p>
2023년 9월 21일	NSX를 사용하여 NSX Advanced Load Balancer 를 설치 및 구성하기 위한 정보로 네트워킹 섹션이 업데이트되었습니다. NSX 및 NSX Advanced Load Balancer 설치 및 구성 의 내용을 참조하십시오.
2023년 6월 30일	감독자 설치 항목 및 감독자의 제어부 크기 변경에 감독자 제어부 크기가 추가되었습니다.

개정	설명
2022년 6월 23일	컨텐츠 라이브러리를 생성하고 편집하기 위한 링크가 업데이트되었습니다. NSX Advanced Load Balancer OVA를 로컬 컨텐츠 라이브러리로 가져오기 의 내용을 참조하십시오.
2023년 6월 15일	다음 작업에만 HTTP 프록시를 사용할 수 있다는 참고 사항이 추가됨: Tanzu Mission Control에 감독자 등록. vSphere IaaS control plane에서 HTTP 프록시 설정 구성 의 내용을 참조하십시오.
2023년 5월 15일	감독자에 사용되는 스토리지 정책 또는 1개 영역 감독자의 네임스페이스에서 사용 도메인을 사용하도록 설정하면 안 된다는 참고 사항이 추가되었습니다. 장 2 vSphere IaaS control plane에 대한 스토리지 정책 생성 의 내용을 참조하십시오.
2023년 5월 12일	vSphere IaaS control plane 환경을 8.0 이전의 vSphere 버전에서 업그레이드했고 vSphere 영역을 사용하려는 경우에는 새로운 3개 영역 감독자를 생성해야 한다는 참고 사항이 추가되었습니다. 장 5 3개 영역 감독자 배포 의 내용을 참조하십시오.
2023년 4월 26일	vSphere 네임스페이스 구성 및 관리 가 "vSphere IaaS 제어부 서비스 및 워크로드" 로 이동되었습니다.
2023년 4월 18일	NSX Advanced Load Balancer 버전 22.1.3에 대한 지원을 포함하도록 NSX Advanced Load Balancer 설치 및 구성 섹션이 업데이트되었습니다.

vSphere IaaS control plane 설치 및 구성 워크플로

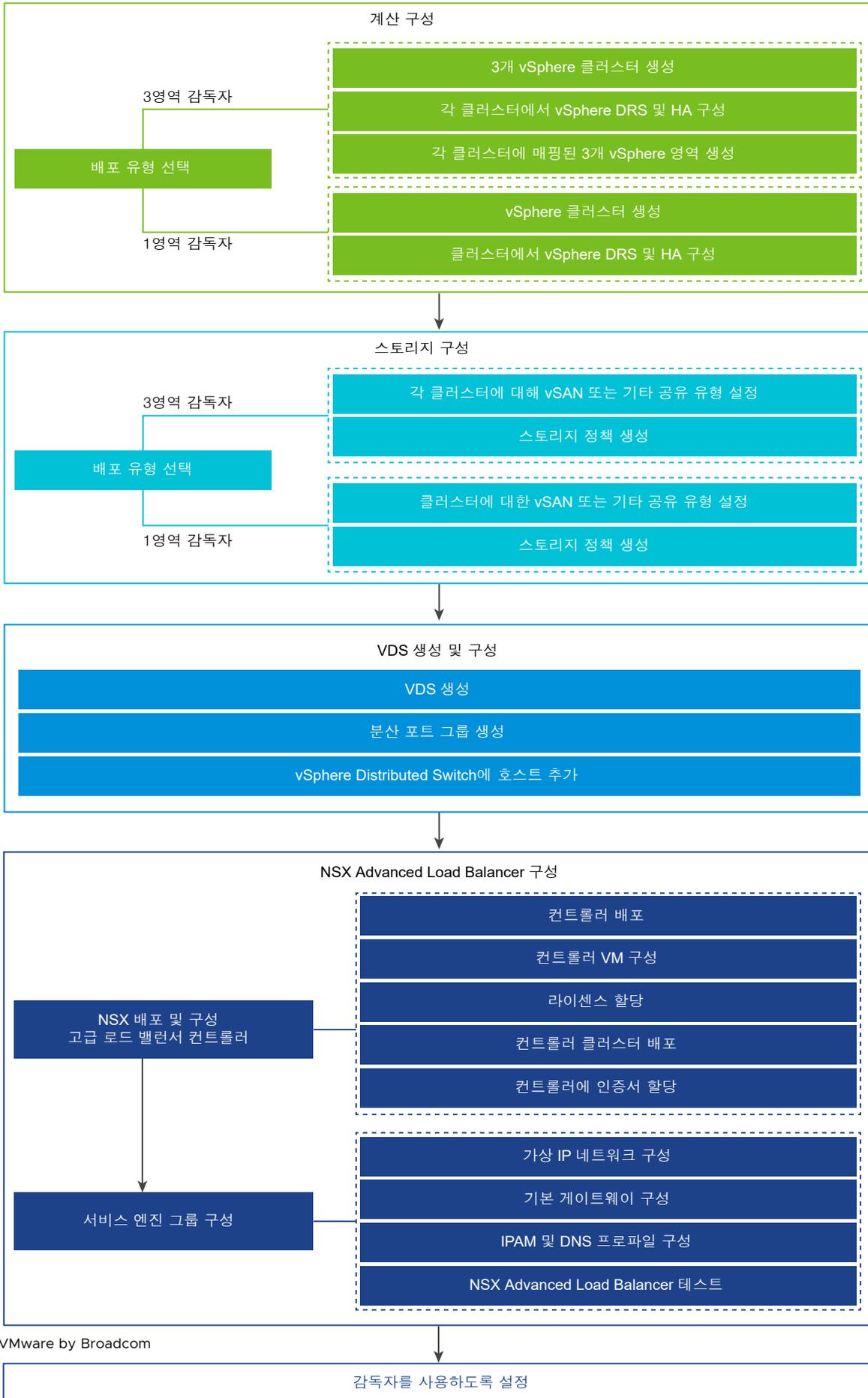
1

vSphere 클러스터를 vSphere에서 Kubernetes 워크로드를 실행하기 위한 플랫폼으로 전환하기 위한 워크플로를 검토합니다.

VDS 네트워킹 및 NSX Advanced Load Balancer를 사용하여 감독자를 배포하기 위한 워크플로

vSphere 관리자는 NSX Advanced Load Balancer를 사용하여 VDS 네트워킹을 기반으로 하는 네트워킹 스택을 사용하여 감독자를 배포할 수 있습니다.

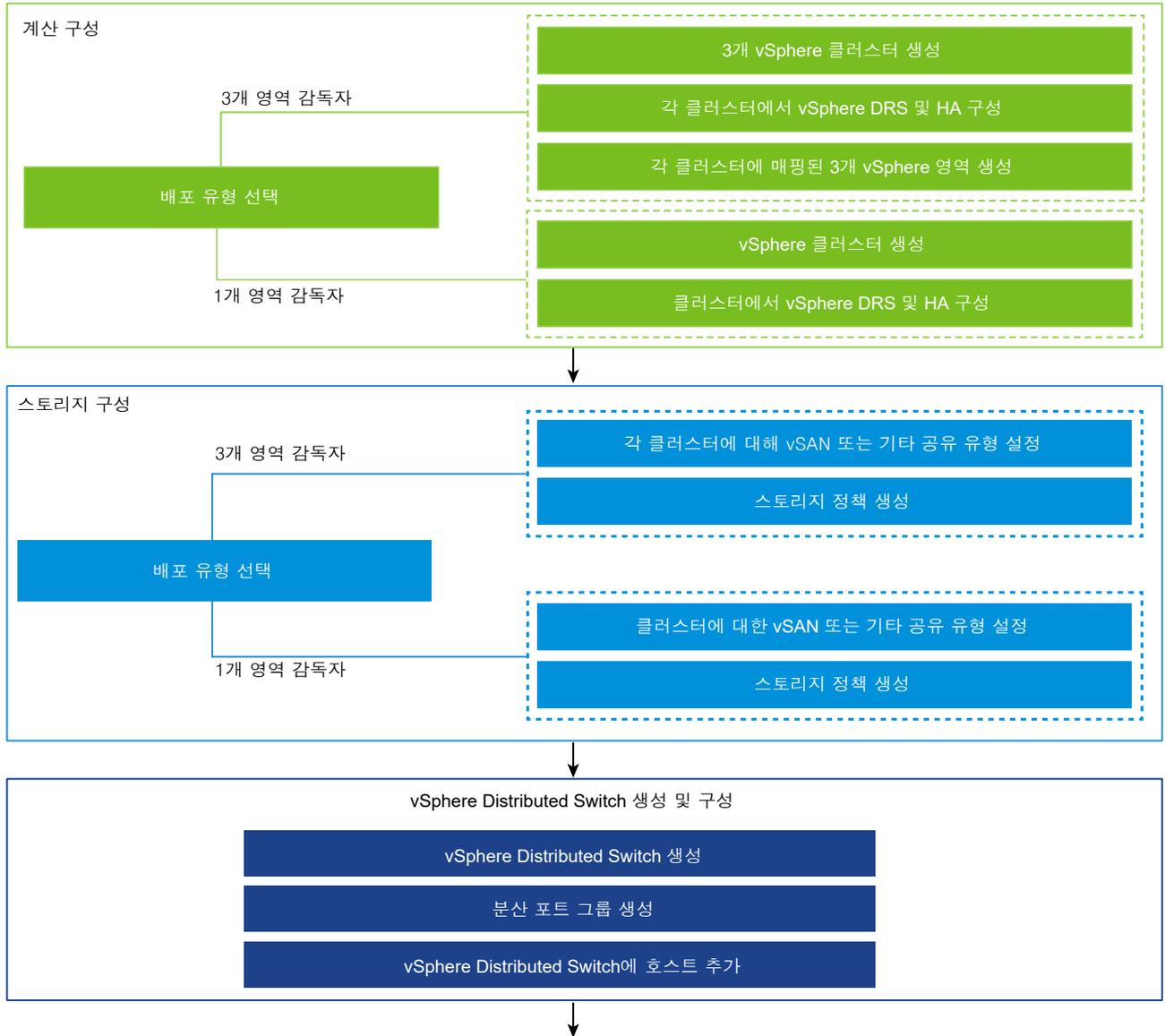
그림 1-1. NSX Advanced Load Balancer를 사용하여 감독자를 배포하기 위한 워크플로

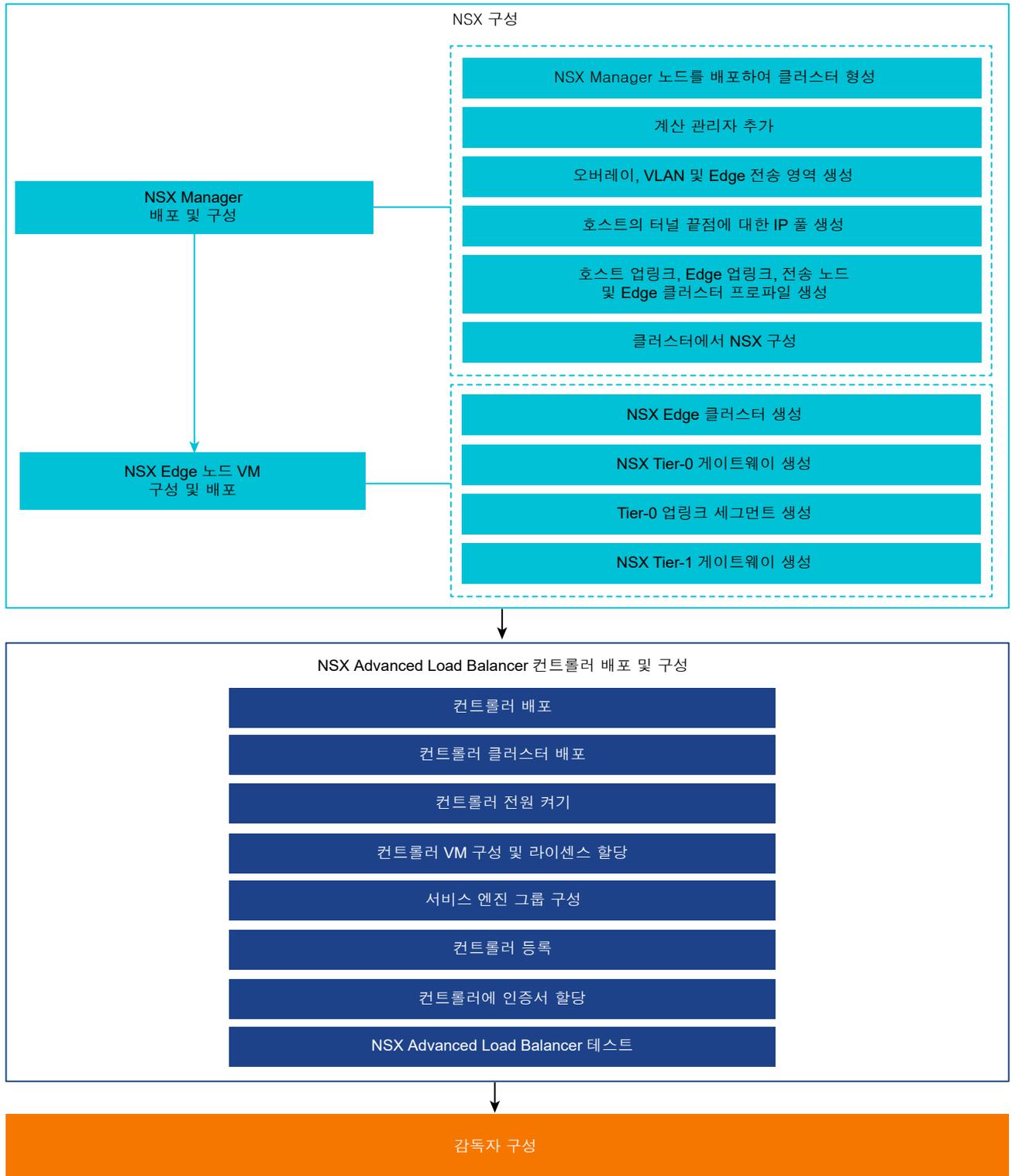


NSX 네트워킹 및 NSX Advanced Load Balancer Controller 워크플로가 포함된 감독자

vSphere 관리자는 NSX 네트워킹 스택 및 NSX Advanced Load Balancer Controller를 사용하여 감독자를 배포할 수 있습니다.

그림 1-2. NSX 네트워킹 및 NSX Advanced Load Balancer Controller를 사용하여 감독자를 배포하기 위한 워크플로

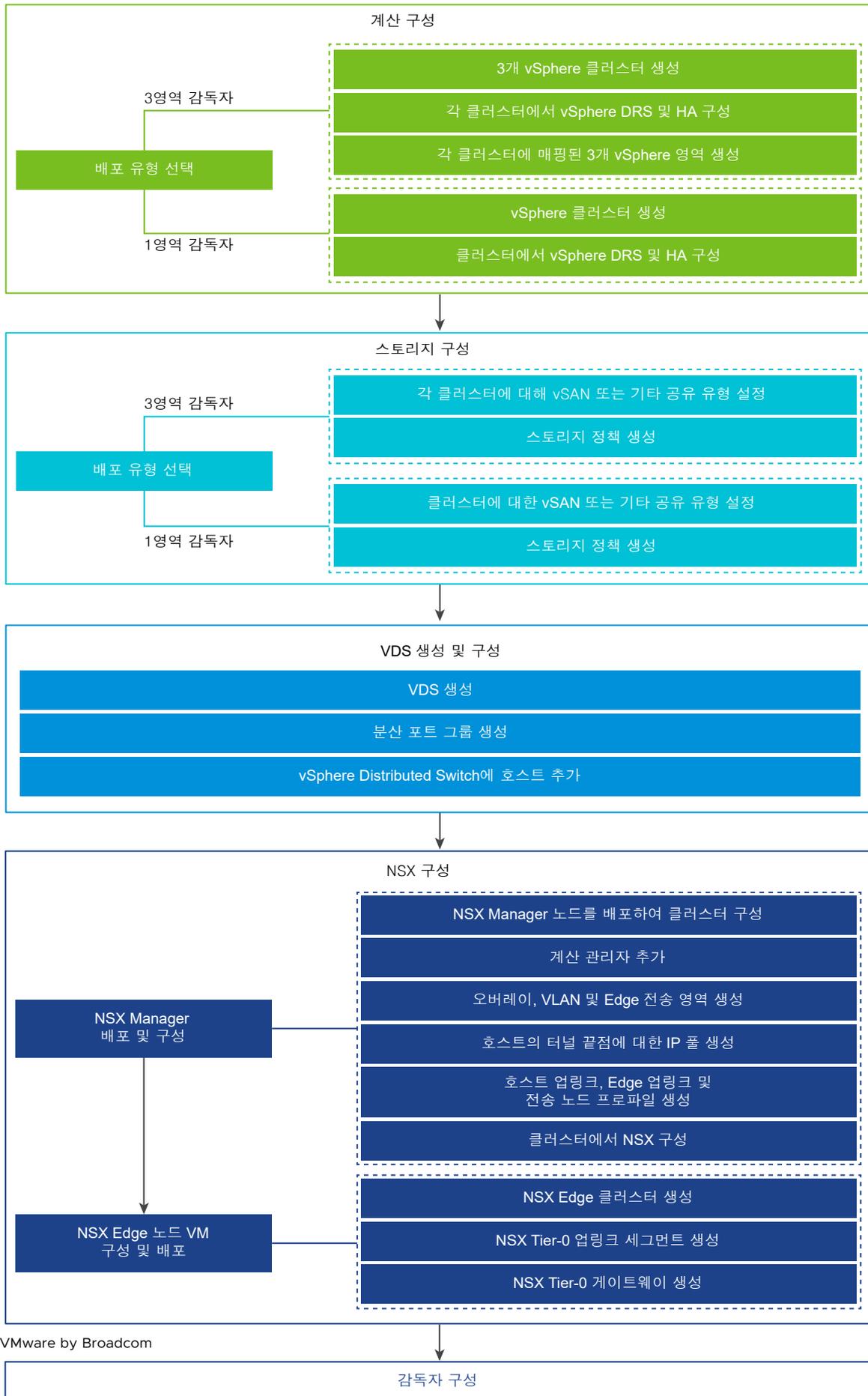




NSX 네트워킹을 사용하여 감독자를 배포하기 위한 워크플로

vSphere 관리자는 NSX 기반 네트워킹 스택을 사용하여 감독자를 배포할 수 있습니다.

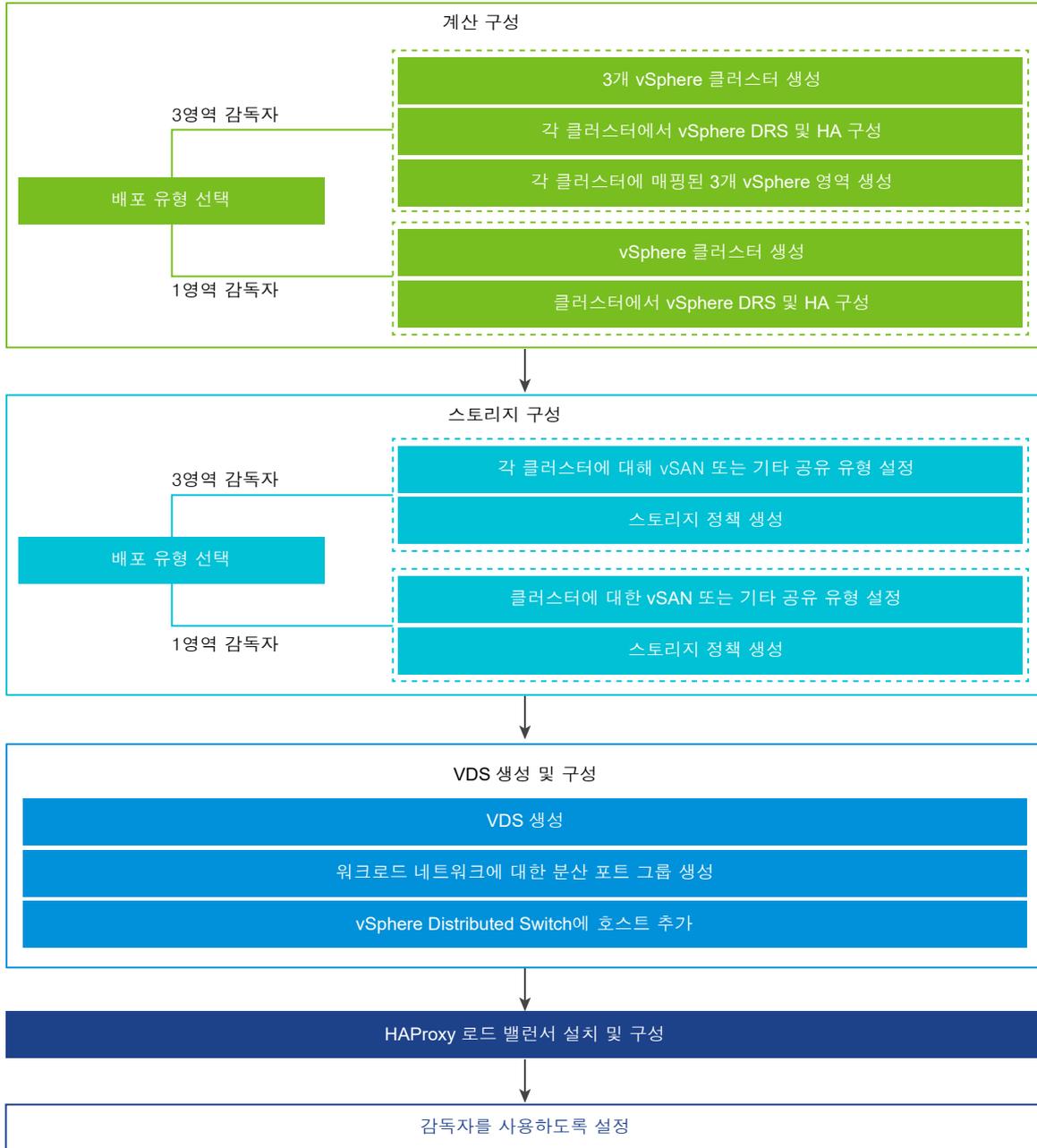
그림 1-3. NSX를 네트워킹 스택으로 사용하여 감독자를 배포하기 위한 워크플로



VDS 네트워킹 및 HAProxy 로드 밸런서를 사용하여 감독자를 배포하기 위한 워크플로

vSphere 관리자는 VDS 및 HAProxy 로드 밸런서를 기반으로 하는 네트워킹 스택을 사용하여 감독자를 배포할 수 있습니다.

그림 1-4. VDS 네트워킹 및 HAProxy를 사용하여 감독자를 배포하기 위한 워크플로



다음으로 아래 항목을 읽으십시오.

- vSphere 클러스터에서 vSphere IaaS control plane를 구성하기 위한 사전 요구 사항

vSphere 클러스터에서 vSphere IaaS control plane를 구성하기 위한 사전 요구 사항

vSphere 환경에서 vSphere IaaS control plane를 사용하도록 설정하기 위한 사전 요구 사항을 확인합니다. vSphere에서 기본적으로 컨테이너 기반 워크로드를 실행하려면 vSphere 관리자가 vSphere 클러스터를 감독자로 사용하도록 설정합니다. 감독자에는 vSphere 포드를 배포하고 Tanzu Kubernetes 클러스터 및 VM을 프로비저닝하여 vSphere에서 Kubernetes 워크로드를 실행할 수 있는 Kubernetes 계층이 있습니다.

vSphere 클러스터 생성 및 구성

감독자는 vSphere 영역과 연결된 1개 또는 3개 vSphere 클러스터에서 실행할 수 있습니다. 각 vSphere 영역은 1개 vSphere 클러스터에 매핑되며 1개 또는 3개의 영역에 감독자를 배포할 수 있습니다. 3개 영역 감독자는 Kubernetes 워크로드를 실행하기 위한 더 많은 양의 리소스를 제공하며 클러스터 장애로부터 워크로드를 보호하는 vSphere 클러스터 수준의 고가용성을 제공합니다. 1개 영역 감독자는 vSphere HA에서 제공하는 호스트 수준의 고가용성을 제공하며 Kubernetes 워크로드를 실행하는 데 1개 클러스터의 리소스만 활용합니다.

참고 한 vSphere 영역에 감독자를 배포한 후에는 감독자를 3개 영역 배포로 확장할 수 없습니다.

감독자를 배포하려는 각 vSphere 클러스터는 다음 요구 사항을 충족해야 합니다.

- ESXi 호스트가 2개 이상인 vSphere 클러스터를 생성하고 구성합니다. vSAN을 사용하는 경우 최적의 성능을 위해 클러스터에 최소 3개 호스트 또는 4개 호스트가 있어야 합니다. [클러스터 생성 및 구성](#)을 참조하십시오.
- vSAN과 같은 공유 스토리지를 사용하여 클러스터를 구성합니다. 공유 스토리지는 vSphere HA, DRS에 필요하며 영구 컨테이너 볼륨을 저장하는 데 필요합니다. [vSAN 클러스터 생성](#)을 참조하십시오.
- vSphere HA를 사용하여 클러스터를 사용하도록 설정합니다. [vSphere HA 클러스터 생성 및 사용](#)을 참조하십시오.
- 완전 자동화 모드에서 vSphere DRS를 사용하여 클러스터를 사용하도록 설정합니다. [DRS 클러스터 생성](#)을 참조하십시오.
- 감독자를 배포할 수 있도록 사용자 계정에 vSphere 클러스터의 [클러스터 전체 구성 수정](#)이 있는지 확인합니다.
- 3개 영역 감독자를 배포하려면 3개 vSphere 영역을 생성합니다. [장 3 다중 영역 감독자 배포를 위한 vSphere 영역 생성](#) 항목을 참조하십시오.
- vSphere Lifecycle Manager 이미지를 감독자에서 사용하려면 [워크로드 관리](#)를 활성화하기 전에 [워크로드 관리](#)를 활성화하려는 vSphere 클러스터를 vSphere Lifecycle Manager 이미지를 사용하도록 전환합니다. vSphere Lifecycle Manager 기준선 또는 vSphere Lifecycle Manager 이미지로 감독자의 수명 주기를 관리할 수 있습니다. 그러나 vSphere Lifecycle Manager 기준선을 사용하는 감독자를 vSphere Lifecycle Manager 이미지를 사용하는 감독자로 변환할 수는 없습니다. 따라서 [워크로드 관리](#)를 활성화하기 전에 vSphere Lifecycle Manager 이미지를 사용하도록 vSphere 클러스터를 전환해야 합니다.

스토리지 정책 생성

감독자를 배포하기 전에 감독자 제어부 VM의 데이터스토어 배치를 결정하는 스토리지 정책을 생성해야 합니다. 감독자가 vSphere 포드를 지원하는 경우 컨테이너 및 이미지에 대한 스토리지 정책도 필요합니다. 다양한 수준의 스토리지 서비스와 연결된 스토리지 정책을 생성할 수 있습니다.

[장 2 vSphere IaaS control plane에 대한 스토리지 정책 생성의 내용을 참조하십시오.](#)

네트워킹 스택 선택 및 구성

감독자를 배포하려면 이것을 사용할 네트워킹 스택을 구성해야 합니다. 사용 가능한 두 가지 옵션은 NSX 또는 로드 밸런서를 사용하는 vDS(vSphere Distributed Switch) 네트워킹입니다. NSX Advanced Load Balancer 또는 HAProxy 로드 밸런서를 구성할 수 있습니다.

감독자에 NSX 네트워킹을 사용하려면 다음을 수행합니다.

- NSX 네트워킹에 대한 시스템 요구 사항 및 토폴로지를 검토합니다. "vSphere IaaS 제어부 개념 및 계획" 에서 [NSX를 사용하여 3개 영역 감독자를 사용하도록 설정하기 위한 요구 사항](#) 및 [NSX를 사용하여 단일 클러스터 감독자를 설정하기 위한 요구 사항](#)을 참조하십시오.
- vSphere IaaS control plane에 대한 NSX를 설치 및 구성합니다. [vSphere IaaS control plane에 대한 NSX 설치 및 구성의 내용](#)을 참조하십시오.

감독자에 대해 NSX Advanced Load Balancer와 vDS 네트워킹을 사용하려면 다음을 수행합니다.

- NSX Advanced Load Balancer 요구 사항을 검토합니다. "vSphere IaaS 제어부 개념 및 계획" 에서 [NSX Advanced Load Balancer를 사용하는 3개 영역 감독자에 대한 요구 사항](#) 및 [NSX Advanced Load Balancer를 사용하여 단일 클러스터 감독자를 사용하도록 설정하기 위한 요구 사항](#)을 참조하십시오.
- vDS(vSphere Distributed Switch)를 생성하고 클러스터의 모든 ESXi 호스트를 vDS에 추가하고 워크로드 네트워크용 포트 그룹을 생성합니다. [NSX Advanced Load Balancer와 함께 사용할 감독자용 vSphere Distributed Switch 생성의 내용](#)을 참조하십시오.
- NSX Advanced Load Balancer를 배포하고 구성합니다. [NSX Advanced Load Balancer 컨트롤러 배포의 내용](#)을 참조하십시오.

참고 vSphere IaaS control plane는 vSphere 7 U2 이상에서 NSX Advanced Load Balancer를 지원합니다.

감독자에 대해 HAProxy 로드 밸런싱과 vDS 네트워킹을 사용하려면 다음을 수행합니다.

- HAProxy 로드 밸런서를 사용하는 vSphere 네트워킹에 대한 시스템 요구 사항 및 네트워크 토폴로지를 검토합니다. [HA 프록시 로드 밸런서를 사용하여 3개 영역 감독자를 사용하도록 설정하기 위한 요구 사항](#) 및 [VDS 네트워킹 및 HAProxy 로드 밸런서에서 단일 클러스터 감독자를 사용하도록 설정하기 위한 요구 사항](#) "vSphere IaaS 제어부 개념 및 계획" 을 참조하십시오.
- VDS(vSphere Distributed Switch)를 생성하고 클러스터의 모든 ESXi 호스트를 vDS에 추가하고 워크로드 네트워크용 포트 그룹을 생성합니다. [HAProxy 로드 밸런서와 함께 사용할 감독자용 vSphere Distributed Switch 생성의 내용](#)을 참조하십시오.

- 감독자를 배포하는 vSphere 클러스터에서 호스트에 연결된 vDS로 라우팅할 수 있는 HAProxy 로드 밸런서 인스턴스를 설치하고 구성합니다. HAProxy 로드 밸런서는 클라이언트 네트워크의 워크로드에 대한 네트워크 연결 및 Tanzu Kubernetes 클러스터 간에 트래픽을 로드 밸런싱을 위한 네트워크 연결을 지원합니다. [HAProxy 로드 밸런서 설치 및 구성](#)의 내용을 참조하십시오.

참고 vSphere IaaS control plane는 vSphere 7 U1 이상에서 HAProxy 로드 밸런서를 지원합니다.

vSphere IaaS control plane에 대한 스토리지 정책 생성

2

vSphere IaaS control plane을 사용하도록 설정하기 전에 감독자 및 네임스페이스에서 사용될 스토리지 정책을 생성합니다. 정책은 데이터스토어를 대표하여 감독자 제어부 VM, vSphere 포드 사용 후 삭제 디스크 및 컨테이너 이미지와 같은 구성 요소 및 개체의 스토리지 배치를 관리합니다. 영구 볼륨 및 VM 콘텐츠 라이브러리의 스토리지 배치에 대한 정책도 필요할 수 있습니다. Tanzu Kubernetes 클러스터를 사용하는 경우 스토리지 정책은 Tanzu Kubernetes 클러스터 노드가 배포되는 방식도 지정합니다.

vSphere 스토리지 환경 및 DevOps의 요구 사항에 따라 서로 다른 스토리지 클래스에 대해 여러 스토리지 정책을 생성할 수 있습니다. 예를 들어 vSphere 스토리지 환경에 Bronze, Silver 및 Gold의 3가지 데이터스토어 클래스가 있는 경우 모든 데이터스토어 유형에 대한 스토리지 정책을 생성할 수 있습니다.

감독자를 사용하도록 설정하고 네임스페이스를 설정할 때 다양한 개체, 구성 요소 및 워크로드에 사용될 서로 다른 스토리지 정책을 할당할 수 있습니다.

참고 감독자 또는 1개 영역 감독자의 네임스페이스에 대해 생성하는 스토리지 정책은 토폴로지를 인식할 필요가 없습니다. 이러한 정책에 대해 사용 도메인을 사용하도록 설정하지 마십시오.

3개 영역 감독자의 네임스페이스에 대해 생성하는 스토리지 정책은 토폴로지를 인식해야 하고 4b단계에서 사용 도메인을 사용하도록 설정해야 합니다. 3개 영역 네임스페이스는 토폴로지를 인식하지 못하는 스토리지 정책을 할당하지 못하도록 합니다.

다음 예에서는 Gold로 태그 지정된 데이터스토어에 대한 스토리지 정책을 생성합니다.

사전 요구 사항

- vSphere IaaS control plane의 스토리지 정책에 대한 정보를 숙지하려면 "vSphere IaaS 제어부 개념 및 계획" 에서 [스토리지 정책 정보](#)를 참조하십시오.
- 영구 스토리지에 vSAN 데이터 지속성 플랫폼을 사용하고 vSAN Direct 또는 vSAN SNA 데이터스토어에 대한 사용자 지정 스토리지 정책을 생성해야 하는 경우에는 "vSphere IaaS 제어부 서비스 및 워크로드" 에서 [vSAN 데이터 지속성 플랫폼에 대한 사용자 지정 스토리지 정책 생성](#)을 참조하십시오.
- 3개 영역 감독자에서 영구 스토리지에 사용할 토폴로지 인식 스토리지 정책을 생성해야 하는 경우 "vSphere IaaS 제어부 서비스 및 워크로드" 의 [3개 영역 감독자에서 영구 스토리지 사용](#)의 지침을 숙지해야 합니다.
- 스토리지 정책에서 참조하는 데이터스토어가 클러스터의 모든 ESXi 호스트 간에 공유되는지 확인합니다. VMFS, NFS, vSAN 또는 vVols를 비롯한 환경 내의 모든 공유 데이터스토어가 지원됩니다.
- 필요한 권한: [VM 스토리지 정책. 업데이트 및 VM 스토리지 정책. 보기](#).

절차

1 데이터스토어에 태그를 추가합니다.

- a 태그를 지정하려는 데이터스토어를 마우스 오른쪽 버튼으로 클릭하고 **태그 및 사용자 지정 특성 > 태그 할당**을 선택합니다.
- b **태그 추가**를 클릭하고 태그의 속성을 지정합니다.

속성	설명
이름	데이터스토어 태그의 이름을 지정합니다(예: Gold).
설명	태그에 대한 설명을 추가합니다. 예를 들어 Datastore for Kubernetes objects 라고 입력합니다.
범주	기존 범주를 선택하거나 새 범주를 생성합니다. 예를 들어 Storage for Kubernetes 라는 범주를 선택하거나 생성합니다.

2 vSphere Client에서 **VM 스토리지 정책 생성** 마법사를 엽니다.

- a **메뉴 > 정책 및 프로파일**을 클릭합니다.
- b **정책 및 프로파일**에서 **VM 스토리지 정책**을 클릭합니다.
- c **VM 스토리지 정책 생성**을 클릭합니다.

3 정책 이름 및 설명을 입력합니다.

옵션	작업
vCenter Server	vCenter Server 인스턴스를 선택합니다.
이름	스토리지 정책의 이름(예: goldsp)을 입력합니다. 참고 vSphere IaaS control plane는 네임스페이스에 할당하는 스토리지 정책을 Kubernetes 스토리지 클래스로 변환할 때 모든 대문자를 소문자로 변경하고 공백을 대시(-)로 바꿉니다. 혼동을 방지하려면 VM 스토리지 정책 이름에 소문자를 사용하고 공백을 사용하지 마십시오.
설명	스토리지 정책의 설명을 입력합니다.

4 **정책 구조** 페이지에서 다음 옵션을 선택하고 **다음**을 클릭합니다.

- a **데이터스토어별 규칙**에서 태그 기반 배치 규칙을 사용하도록 설정합니다.
- b 토폴로지 인식 정책을 생성하려면 **스토리지 토폴로지**에서 **사용 도메인 사용**을 선택합니다.

이 단계는 3개 영역 감독자의 네임스페이스에서 영구 스토리지에 사용할 토폴로지 인식 정책을 생성하는 경우에만 필요합니다.

5 태그 기반 배치 페이지에서 태그 규칙을 생성합니다.

다음 예를 사용하여 옵션을 선택합니다.

옵션	설명
태그 범주	드롭다운 메뉴에서 태그의 범주(예: Storage for Kubernetes)를 선택합니다.
사용 옵션	다음으로 태그 지정된 스토리지 사용 을 선택합니다.
태그	태그 찾아보기 를 클릭하고 데이터스토어 태그(예: Gold)를 선택합니다.

6 스토리지 토폴로지를 사용하도록 설정한 경우 **사용 도메인** 페이지에서 스토리지 토폴로지 유형을 지정합니다.

옵션	설명
영역	단일 영역의 모든 호스트에서 데이터스토어가 공유됩니다.

7 스토리지 호환성 페이지에서 이 정책과 일치하는 데이터스토어 목록을 검토합니다.

이 예에서는 Gold로 태그 지정된 데이터스토어만 표시됩니다.

8 검토 및 완료 페이지에서 스토리지 정책 설정을 검토하고 **마침**을 클릭합니다.

결과

Gold로 태그 지정된 데이터스토어에 대한 새로운 스토리지 정책이 기존 스토리지 정책의 목록에 나타납니다.

다음에 수행할 작업

스토리지 정책을 생성한 후 vSphere 관리자는 다음 작업을 수행할 수 있습니다.

- 감독자에 스토리지 정책을 할당합니다. 감독자에 구성된 스토리지 정책은 제어부 VM, 포드 사용 후 삭제 디스크 및 컨테이너 이미지가 정책이 나타내는 데이터스토어에 배치되도록 합니다.
- vSphere 네임스페이스에 스토리지 정책을 할당합니다. 네임스페이스에 표시되는 스토리지 정책은 네임스페이스가 영구 볼륨에 대해 액세스하고 사용할 수 있는 데이터스토어를 결정합니다. 스토리지 정책은 일치하는 Kubernetes 스토리지 클래스로 네임스페이스에 나타납니다. 또한 이 네임스페이스의 Tanzu Kubernetes 클러스터에도 전파됩니다. DevOps 엔지니어는 스토리지 클래스를 영구 볼륨 할당 규격에 사용할 수 있습니다. [vSphere 네임스페이스 생성 및 구성](#)을 참조하십시오.

다중 영역 감독자 배포를 위한 vSphere 영역 생성

3

감독자에서 실행되는 Kubernetes 워크로드에 클러스터 수준 고가용성을 제공하는 데 사용할 수 있는 vSphere 영역을 생성하는 방법을 알아봅니다. Kubernetes 워크로드에 클러스터 수준 고가용성을 제공하려면 3개의 vSphere 영역에 감독자를 배포합니다. 각 vSphere 영역은 호스트가 2개 이상 있는 1개 vSphere 클러스터에 매핑됩니다.

사전 요구 사항

- 각 영역에 호스트가 3개 이상 있는 3개의 vSphere 클러스터를 생성합니다. vSAN 있는 스토리지의 경우 클러스터에 4개의 호스트가 있어야 합니다.
- 각 클러스터에 대해 vSAN 또는 기타 공유 스토리지 솔루션을 사용하여 스토리지를 구성합니다.
- 완전 자동화 또는 부분 자동화 모드에서 vSphere HA 및 vSphere DRS를 사용하도록 설정합니다.
- 클러스터에 대해 NSX 또는 vDS(vSphere Distributed Switch) 네트워킹을 사용하여 네트워킹을 구성합니다.

절차

- 1 vSphere Client에서 vCenter Server로 이동합니다.
- 2 구성을 선택하고 **vSphere 영역**을 선택합니다.
- 3 새 **vSphere 영역 추가**를 클릭합니다.
- 4 영역 이름(예: **zone1**)을 지정하고 설명(선택 사항)을 추가합니다.
- 5 영역에 추가할 vSphere 클러스터를 선택하고 **마침**을 클릭합니다.
- 6 단계를 반복하여 3개의 vSphere 영역을 생성합니다.

다음에 수행할 작업

- ■ 감독자에서 사용할 네트워킹 스택을 구성합니다. [장 4 vSphere IaaS control plane에 대한 네트워킹 항목](#)을 참조하십시오.
- 생성한 3개의 vSphere 영역에서 감독자를 활성화합니다. [장 5 3개 영역 감독자 배포](#)의 내용을 참조하십시오.

vSphere 영역을 변경해야 하는 경우 해당 영역에 감독자를 배포하기 전에 변경할 수 있습니다.

vSphere 영역 관리

vSphere 영역을 변경해야 하는 경우 영역에 감독자를 배포하기 전에 변경해야 합니다. 연결된 클러스터를 변경하거나 영역을 삭제할 수 있습니다. vSphere 영역을 삭제하면 연결된 클러스터가 제거된 후 vCenter Server에서 영역이 삭제됩니다.

vSphere 영역에서 클러스터 제거

vSphere 영역에서 클러스터를 제거하려면 영역 카드에서 3개 점(...)을 클릭하고 **클러스터 제거**를 선택합니다. 클러스터가 영역에서 제거되고 다른 클러스터를 추가할 수 있습니다.

참고 vSphere 영역에서 이미 사용하도록 설정된 감독자가 있는 경우 해당 영역에서 클러스터를 제거할 수 없습니다.

vSphere 영역 삭제

vSphere 영역을 삭제하려면 영역 카드에서 3개 점(...)을 클릭하고 **영역 삭제**를 선택합니다.

참고 vSphere 영역에 이미 사용하도록 설정된 감독자가 있는 경우 해당 영역을 삭제할 수 없습니다.

vSphere IaaS control plane에 대한 네트워킹

4

감독자는 vSphere 네트워킹 스택 또는 VMware NSX®를 사용하여 Kubernetes 제어부 VM, 서비스 및 워크로드에 대한 연결을 제공할 수 있습니다. Tanzu Kubernetes Grid에서 프로비저닝된 Tanzu Kubernetes 클러스터에 사용되는 네트워킹은 클러스터 포드, 서비스 및 수신을 위한 네트워킹을 제공하는 오픈 소스 소프트웨어 및 vSphere IaaS control plane 인프라의 기반이 되는 패브릭의 조합입니다.

다음으로 아래 항목을 읽으십시오.

- 감독자 네트워킹
- vSphere IaaS control plane에 대한 NSX 설치 및 구성
- NSX 및 NSX Advanced Load Balancer 설치 및 구성
- NSX Advanced Load Balancer 설치 및 구성
- HAProxy 로드 밸런서 설치 및 구성

감독자 네트워킹

vSphere IaaS control plane 환경에서 감독자는 vSphere 네트워킹 스택 또는 NSX를 사용하여 감독자 제어부 VM, 서비스 및 워크로드에 대한 연결을 제공할 수 있습니다.

감독자가 vSphere 네트워킹 스택으로 구성되면 감독자의 모든 호스트가 워크로드 및 감독자 제어부 VM에 대한 연결을 제공하는 vDS에 연결됩니다. vSphere 네트워킹 스택을 사용하는 감독자에는 DevOps 사용자 및 외부 서비스에 대한 연결을 제공하기 위해 vCenter Server 관리 네트워크에 로드 밸런서가 필요합니다.

NSX로 구성된 감독자는 솔루션의 소프트웨어 기반 네트워크 및 NSX Edge 로드 밸런서 또는 NSX Advanced Load Balancer를 사용하여 외부 서비스 및 DevOps 사용자에 대한 연결을 제공합니다. 환경이 다음 조건을 충족하는 경우 NSX에서 NSX Advanced Load Balancer를 구성할 수 있습니다.

- NSX 버전이 4.1.1 이상입니다.
- NSX Advanced Load Balancer 버전은 엔터프라이즈 라이선스가 있는 22.1.4 이상입니다.
- 구성하려는 NSX Advanced Load Balancer Controller가 NSX에 등록되어 있습니다.
- NSX 로드 밸런서가 감독자에서 아직 구성되지 않았습니다.

VDS를 사용한 감독자 네트워킹

VDS에서 네트워킹 스택으로 지원하는 감독자에서 감독자를 지원하는 vSphere 클러스터의 모든 호스트는 동일한 VDS에 연결되어야 합니다. 감독자는 분산 포트 그룹을 Kubernetes 워크로드 및 제어부 트래픽에 대한 워크로드 네트워킹으로 사용합니다. 감독자의 네임스페이스에 워크로드 네트워킹을 할당합니다.

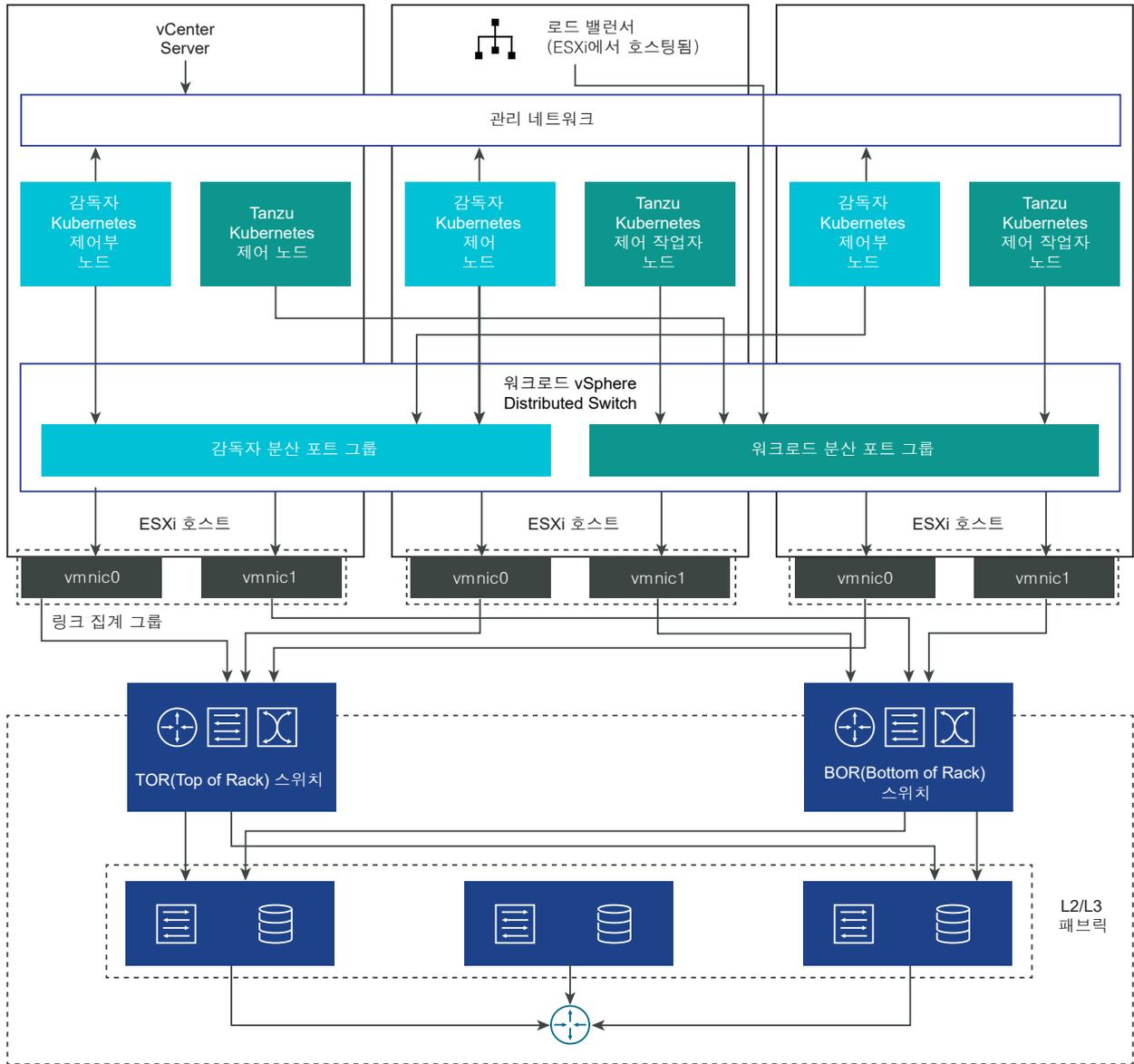
감독자에 대해 구현하는 토폴로지에 따라 하나 이상의 분산 포트 그룹을 워크로드 네트워킹으로 사용할 수 있습니다. 감독자 제어부 VM에 대한 연결을 제공하는 네트워킹을 기본 워크로드 네트워킹이라고 합니다. 이 네트워킹을 감독자의 모든 네임스페이스에 할당하거나 각 네임스페이스에 대해 서로 다른 네트워킹을 사용할 수 있습니다. Tanzu Kubernetes Grid 클러스터는 클러스터가 상주하는 네임스페이스에 할당된 워크로드 네트워킹에 연결됩니다.

VDS에서 지원되는 감독자는 DevOps 사용자 및 외부 서비스에 대한 연결을 제공하기 위해 로드 밸런서를 사용합니다. NSX Advanced Load Balancer 또는 HAProxy 로드 밸런서를 사용할 수 있습니다.

자세한 내용은 [NSX Advanced Load Balancer 설치 및 구성](#) 및 [HAProxy 로드 밸런서 설치 및 구성](#)을 참조하십시오.

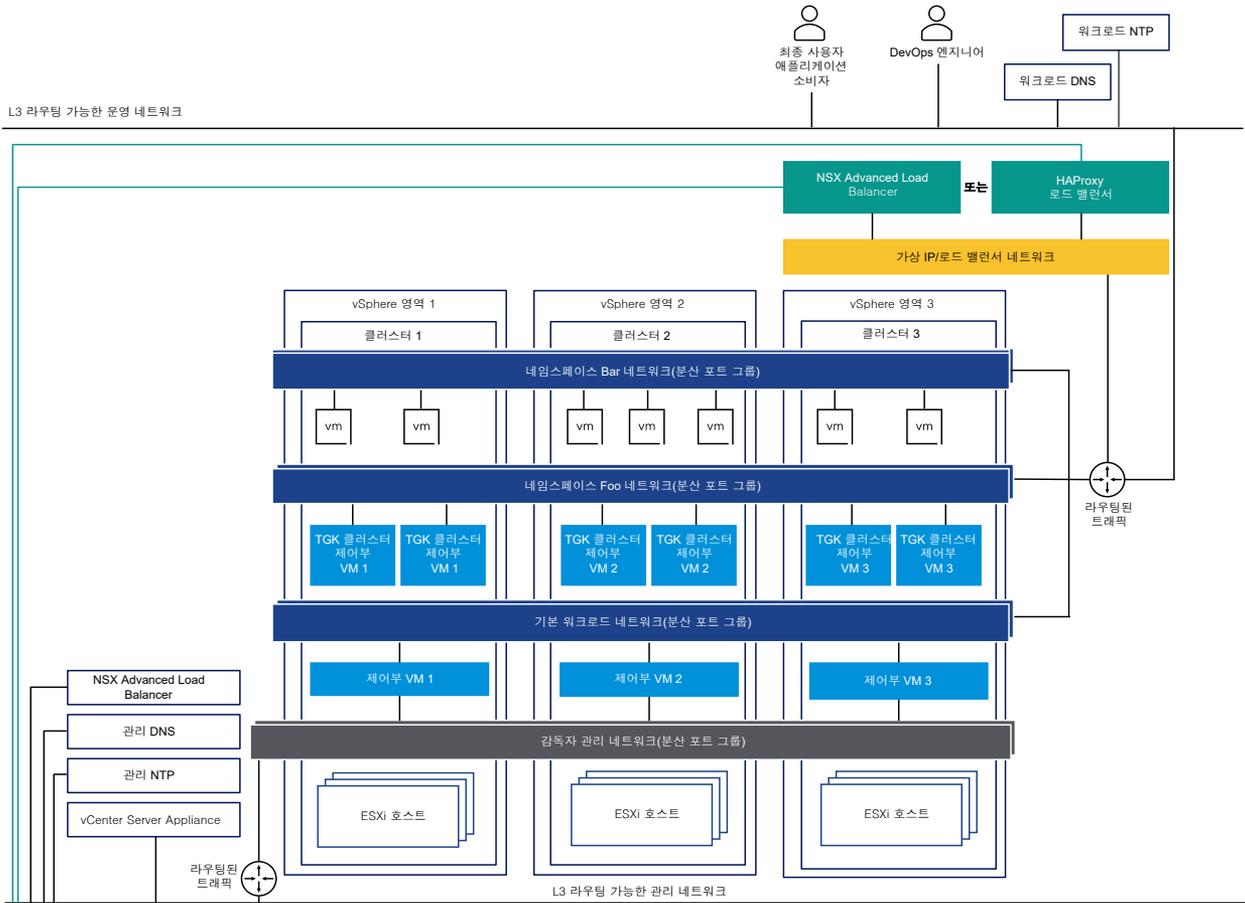
단일 클러스터 감독자 설정에서 감독자는 1개 vSphere 클러스터에서만 지원됩니다. 클러스터의 모든 호스트가 VDS에 연결되어 있어야 합니다.

그림 4-1. VDS를 사용한 단일 클러스터 감독자 네트워킹



3개 영역 감독자에서는 각각 vSphere 클러스터에 매핑된 3개 vSphere 영역에 감독자를 배포합니다. 이러한 vSphere 클러스터의 모든 호스트는 동일한 VDS에 연결되어야 합니다. 모든 물리적 서버는 L2 디바이스에 연결되어야 합니다. 네임스페이스로 구성하는 워크로드 네트워크는 3개 vSphere 영역 모두에 걸쳐 있습니다.

그림 4-2. VDS를 사용한 3개 영역 감독자 네트워킹



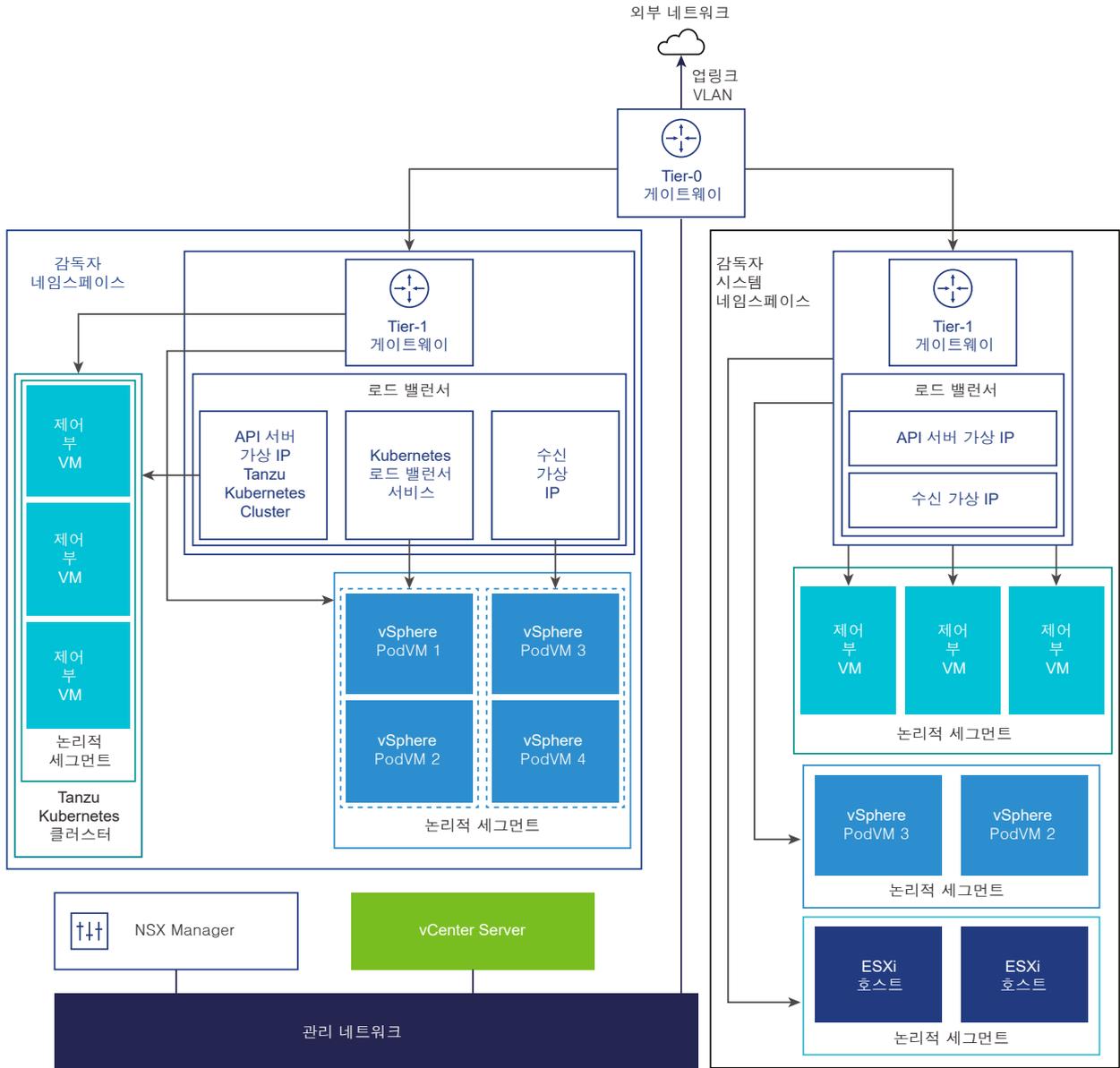
NSX를 사용한 감독자 네트워킹

NSX는 외부 네트워크 및 감독자 내부의 개체에 대한 네트워크 연결을 제공합니다. 클러스터를 구성하는 ESXi 호스트에 대한 연결은 표준 vSphere 네트워크를 통해 처리됩니다.

기존 NSX 배포를 사용하거나 NSX의 새 인스턴스를 배포하여 감독자 네트워킹을 수동으로 구성할 수도 있습니다.

자세한 내용은 [NSX for vSphere IaaS control plane 설치 및 구성](#)을 참조하십시오.

그림 4-3. NSX를 사용한 감독자 네트워킹



- NCP(NSX Container Plugin)는 NSX와 Kubernetes 간의 통합을 제공합니다. NCP의 주요 구성 요소는 컨테이너에서 실행되며 NSX Manager 및 Kubernetes 제어부와 통신합니다. NCP는 컨테이너 및 기타 리소스에 대한 변경 사항을 모니터링하고 NSX API를 호출하여 컨테이너에 대한 논리적 포트, 세그먼트, 라우터 및 보안 그룹과 같은 네트워킹 리소스를 관리합니다.

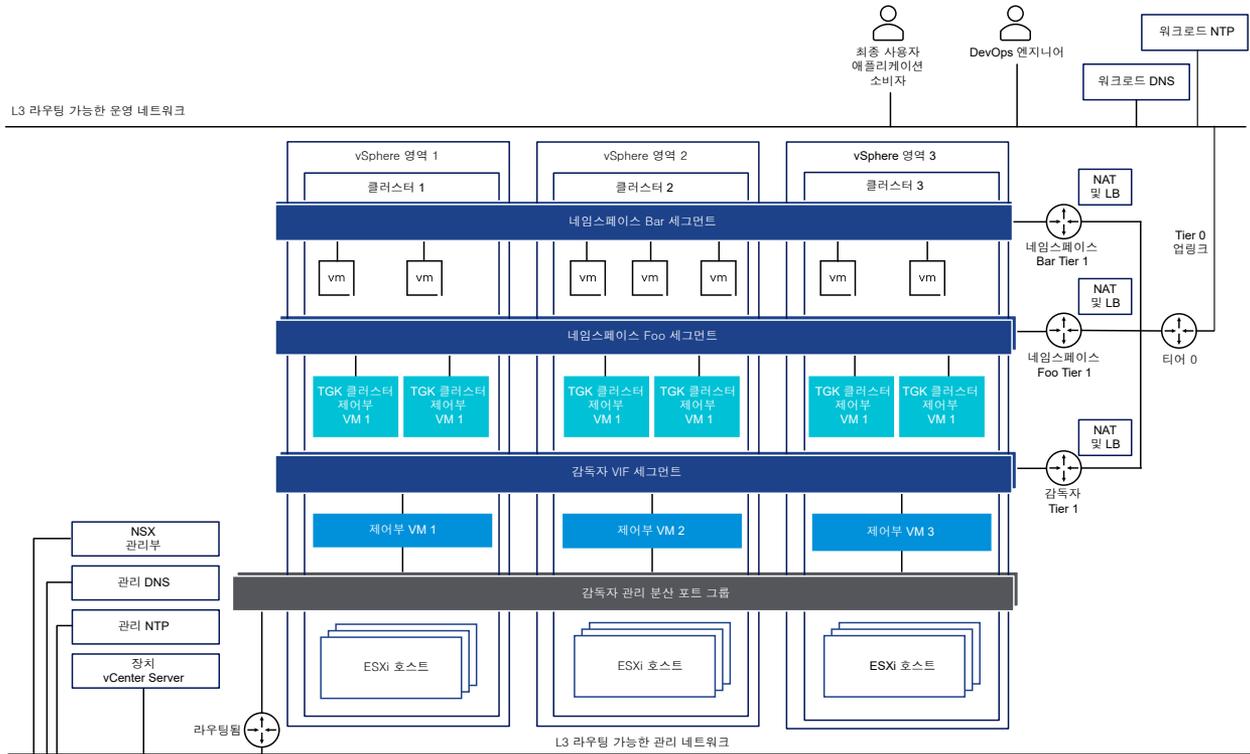
NCP는 기본적으로 시스템 네임스페이스에 대해 하나의 공유 Tier-1 게이트웨이를 생성하고 각 네임스페이스에 대해 Tier-1 게이트웨이와 로드 밸런서를 생성합니다. Tier-1 게이트웨이는 Tier-0 게이트웨이 및 기본 세그먼트에 연결됩니다.

시스템 네임스페이스는 감독자 및 Tanzu Kubernetes Grid 클러스터가 작동하는 데 필수적인 핵심 구성 요소에서 사용되는 네임스페이스입니다. Tier-1 게이트웨이, 로드 밸런서 및 SNAT IP를 포함하는 공유 네트워크 리소스는 시스템 네임스페이스에 그룹화됩니다.

- NSX Edge는 외부 네트워크에서 감독자 개체로 연결을 제공합니다. NSX Edge 클러스터에는 감독자 제어부 VM에 상주하는 Kubernetes API 서버와 감독자 외부에서 게시하고 액세스할 수 있는 모든 애플리케이션에 이중화를 제공하는 로드 밸런서가 있습니다.
- Tier-0 게이트웨이가 NSX Edge 클러스터와 연결되어 외부 네트워크에 대한 라우팅을 제공합니다. 업링크 인터페이스는 동적 라우팅 프로토콜, BGP 또는 정적 라우팅 중 하나를 사용합니다.
- 각 vSphere 네임스페이스에는 별도의 네트워크 및 네임스페이스 내의 애플리케이션이 공유하는 네트워킹 리소스 집합(예: Tier-1 게이트웨이, 로드 밸런서 서비스, SNAT IP 주소)이 있습니다.
- 동일한 네임스페이스에 있는 vSphere 포드, 일반 VM 또는 Tanzu Kubernetes Grid 클러스터에서 실행되는 워크로드는 North-South 연결에 대해 동일한 SNAT IP를 공유합니다.
- vSphere 포드 또는 Tanzu Kubernetes Grid 클러스터에서 실행되는 워크로드에는 기본 방화벽에 의해 구현되는 것과 동일한 격리 규칙이 있습니다.
- 각 Kubernetes 네임스페이스에 대해 별도의 SNAT IP가 필요하지 않습니다. 네임스페이스 간의 East-West 연결은 SNAT가 아닙니다.
- 각 네임스페이스의 세그먼트는 NSX Edge 클러스터에 연결된, 표준 모드에서 작동하는 VDS에 상주합니다. 세그먼트는 감독자에 오버레이 네트워크를 제공합니다.
- 감독자는 공유 Tier-1 게이트웨이 내에 별도의 세그먼트가 있습니다. 각 Tanzu Kubernetes Grid 클러스터에 대해 세그먼트는 네임스페이스의 Tier-1 게이트웨이 내에 정의됩니다.
- 각 ESXi 호스트의 Spherelet 프로세스는 관리 네트워크의 인터페이스를 통해 vCenter Server와 통신합니다.

NSX가 네트워킹 스택으로 구성된 3개 영역 감독자에서 영역에 매핑된 3개 vSphere 클러스터 모두의 모든 호스트는 동일한 VDS에 연결되고 동일한 NSX 오버레이 전송 영역에 참여해야 합니다. 모든 호스트는 동일한 L2 물리적 디바이스에 연결되어야 합니다.

그림 4-4. NSX를 사용한 3개 영역 감독자 네트워킹



NSX 및 NSX Advanced Load Balancer를 사용한 감독자 네트워킹

NSX는 외부 네트워크 및 감독자 내부의 개체에 대한 네트워크 연결을 제공합니다. NSX로 구성된 감독자는 NSX Edge 또는 NSX Advanced Load Balancer를 사용할 수 있습니다.

NSX Advanced Load Balancer의 구성 요소에는 NSX Advanced Load Balancer Controller 클러스터, 서비스 엔진(데이터부) VM 및 AKO(Avi Kubernetes Operator)가 포함됩니다.

NSX Advanced Load Balancer Controller는 vCenter Server와 상호 작용하여 Tanzu Kubernetes Grid 클러스터에 대한 로드 밸런싱을 자동화합니다. 컨트롤러는 서비스 엔진 프로비저닝, 서비스 엔진 전반의 리소스 조정, 서비스 엔진 메트릭 및 로깅 집계를 담당합니다. 컨트롤러는 사용자 작업 및 프로그래밍 방식 통합을 위한 API, 웹 인터페이스, 명령줄 인터페이스를 제공합니다. 컨트롤러 VM을 배포하고 구성한 후 컨트롤러 클러스터를 배포하여 HA에 대한 제어부 클러스터를 설정할 수 있습니다.

서비스 엔진은 데이터부 가상 시스템입니다. 서비스 엔진은 하나 이상의 가상 서비스를 실행합니다. 서비스 엔진은 NSX Advanced Load Balancer Controller에 의해 관리됩니다. 컨트롤러는 가상 서비스를 호스팅하는 서비스 엔진을 프로비저닝합니다.

서비스 엔진에는 두 가지 유형의 네트워크 인터페이스가 있습니다.

- 첫 번째 네트워크 인터페이스인 VM의 vnic0은 NSX Advanced Load Balancer Controller에 연결할 수 있는 관리 네트워크에 연결됩니다.
- 나머지 인터페이스인 vnic1 - 8은 가상 서비스가 실행되는 데이터 네트워크에 연결됩니다.

서비스 엔진 인터페이스는 올바른 vDS 포트 그룹에 자동으로 연결됩니다. 각 서비스 엔진은 가상 서비스를 1000 개까지 지원할 수 있습니다.

가상 서비스는 Tanzu Kubernetes Grid 클러스터 워크로드에 대한 계층 4 및 계층 7 로드 밸런싱 서비스를 제공합니다. 가상 서비스는 하나의 가상 IP와 여러 포트에 구성됩니다. 가상 서비스가 배포되면 컨트롤러는 ESX 서버를 자동으로 선택하고 서비스 엔진을 가동하여 올바른 네트워크(포트 그룹)에 연결합니다.

첫 번째 서비스 엔진은 첫 번째 가상 서비스가 구성된 후에만 생성됩니다. 후속으로 구성된 가상 서비스는 기존 서비스 엔진을 사용합니다.

각 가상 서버는 Tanzu Kubernetes Grid 클러스터에 대한 로드 밸런서 유형의 고유 IP 주소를 사용하여 계층 4 로드 밸런서를 노출합니다. 각 가상 서버에 할당된 IP 주소는 서버를 구성할 때 컨트롤러에 제공된 IP 주소 블록에서 선택됩니다.

AKO(Avi Kubernetes Operator)는 Kubernetes 리소스를 감시하고 NSX Advanced Load Balancer Controller와 통신하여 해당 로드 밸런싱 리소스를 요청합니다. Avi Kubernetes Operator는 사용 설정 프로세스의 일부로 감독자에 설치됩니다.

자세한 내용은 [NSX 및 NSX Advanced Load Balancer 설치 및 구성](#)을 참조하십시오.

그림 4-5. NSX 및 NSX Advanced Load Balancer Controller를 사용한 감독자 네트워크

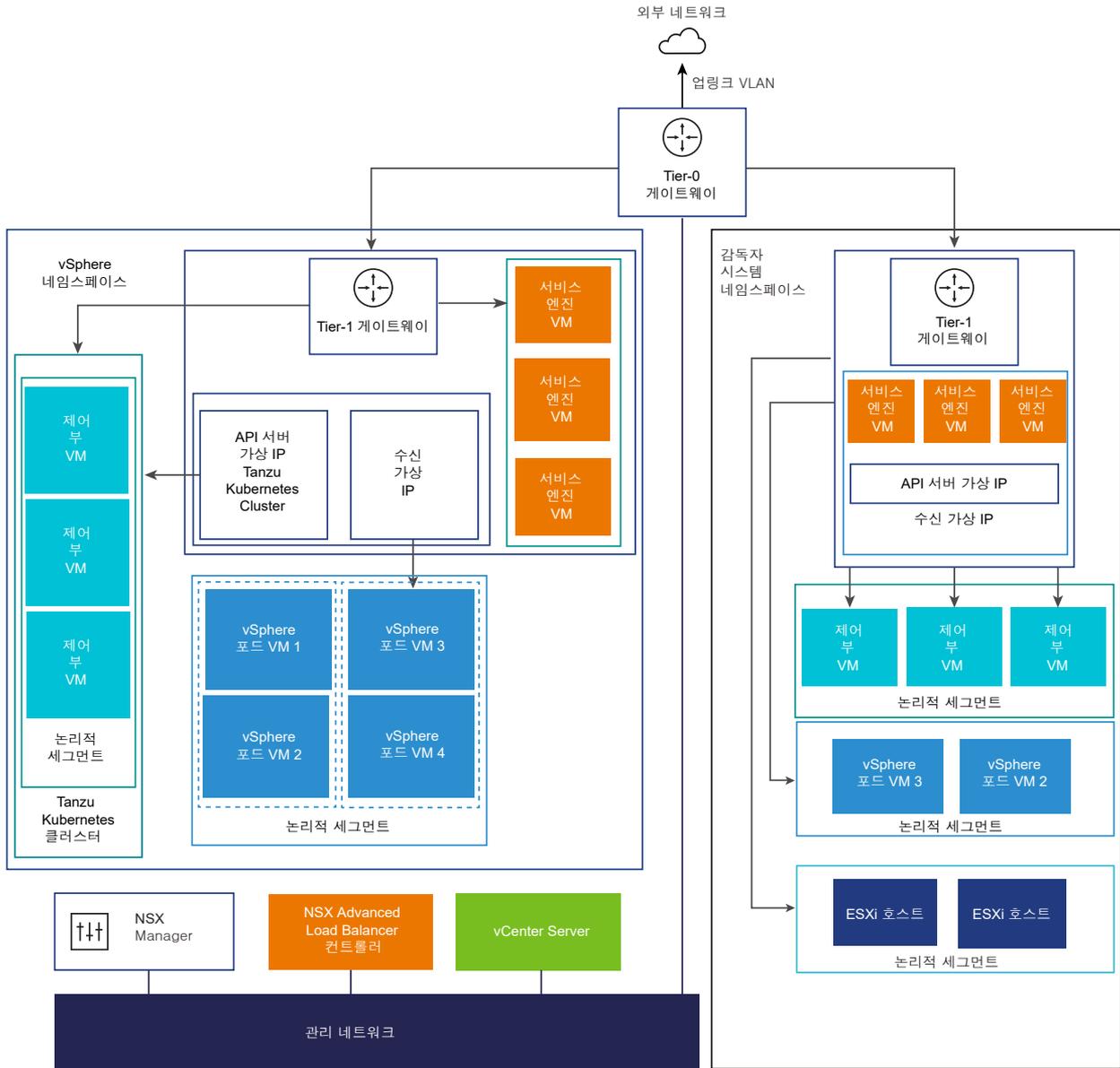
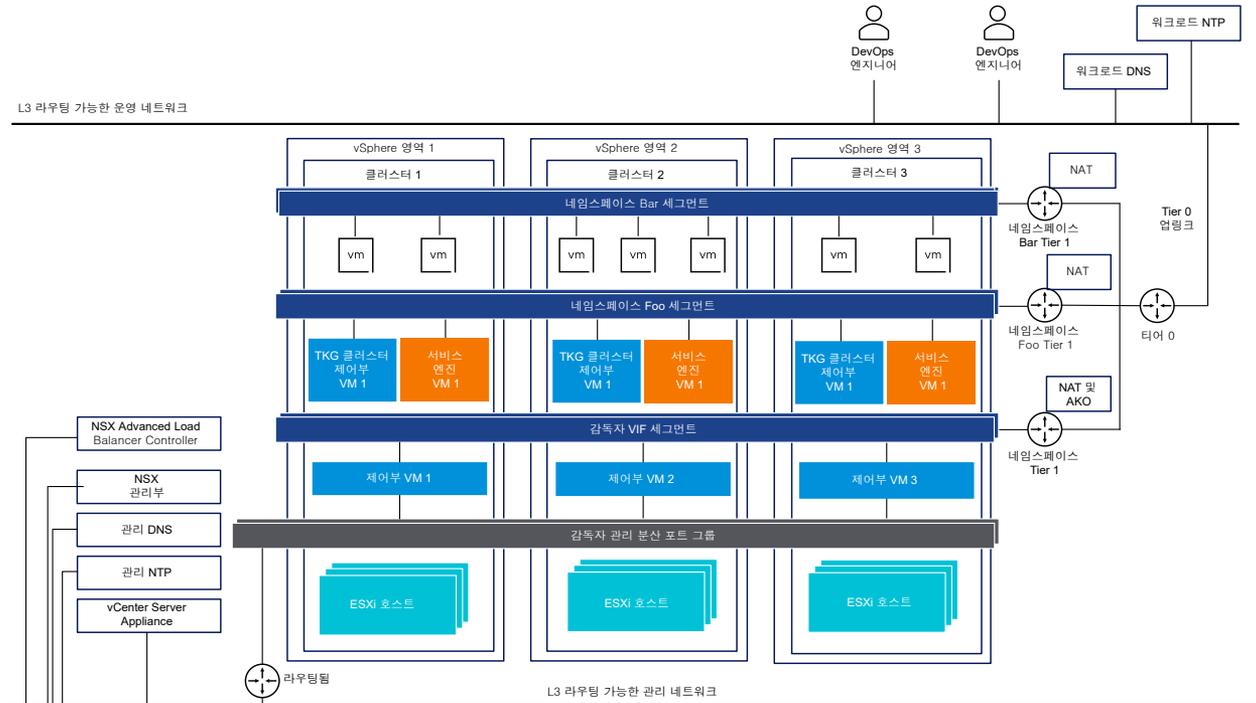


그림 4-6. NSX 및 NSX Advanced Load Balancer Controller를 사용한 3개 영역 감독자 네트워킹



중요 NSX 배포에서 NSX Advanced Load Balancer Controller를 구성할 때에는 다음 고려 사항에 유의하십시오.

- vCenter Server 고급 연결 모드 배포에서는 NSX Advanced Load Balancer Controller를 배포할 수 없습니다. 단일 vCenter Server 배포에만 NSX Advanced Load Balancer Controller를 배포할 수 있습니다. 둘 이상의 vCenter Server가 연결된 경우 NSX Advanced Load Balancer Controller를 구성하는 동안 둘 중 하나만 사용할 수 있습니다.
- 다중 계층 Tier-0 토폴로지에서는 NSX Advanced Load Balancer Controller를 구성할 수 없습니다. NSX 환경이 다중 계층 Tier-0 토폴로지로 설정된 경우 NSX Advanced Load Balancer Controller를 구성하는 동안 하나의 Tier-0 게이트웨이만 사용할 수 있습니다.

NSX를 사용한 네트워킹 구성 방법

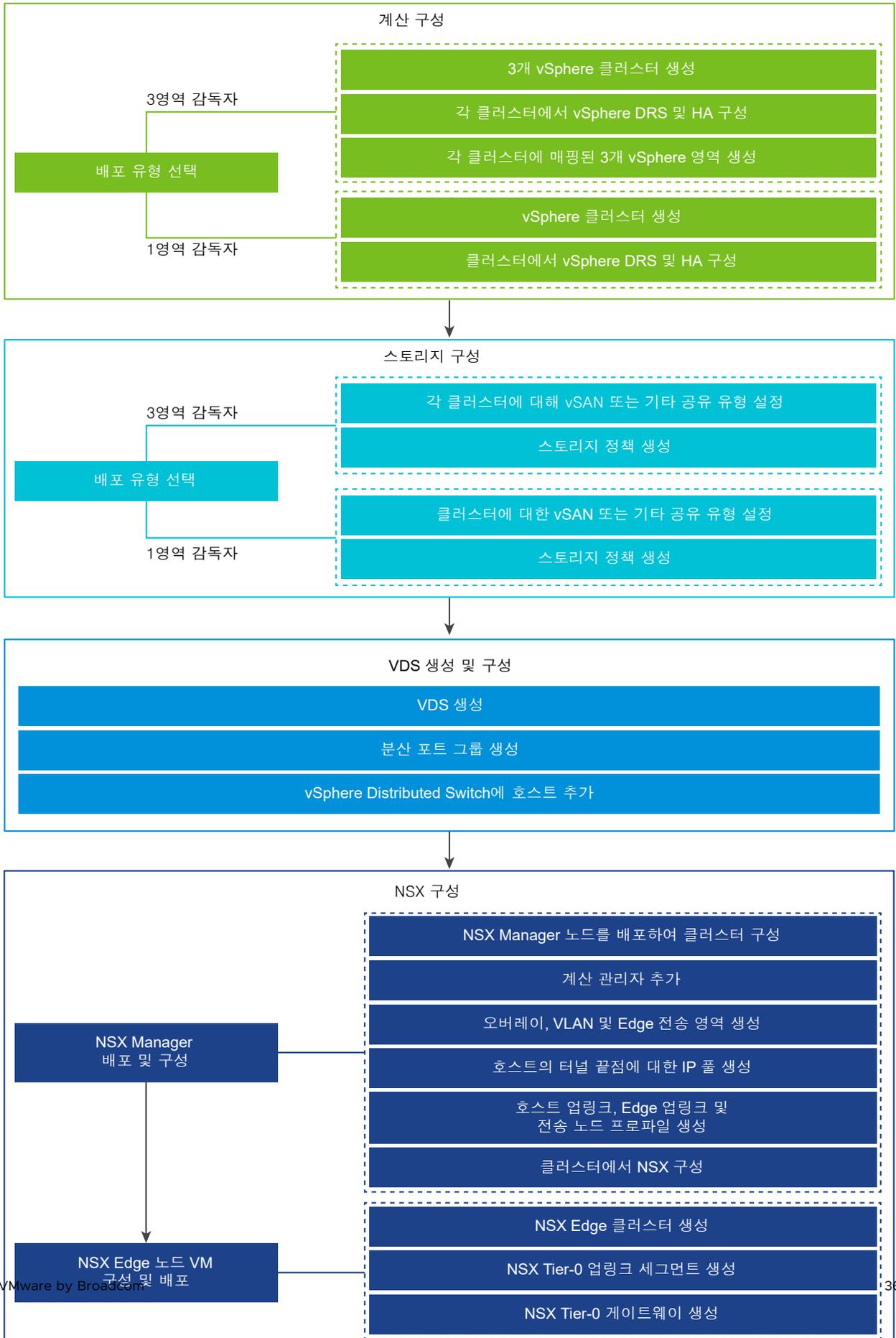
감독자는 고유한 네트워킹 구성을 사용합니다. 1개 영역 감독자에 대해 동일한 네트워킹 모델을 배포하는 NSX를 사용한 감독자 네트워킹을 구성하기 위한 두 가지 방법이 있습니다.

- 감독자 네트워킹을 구성하는 가장 간단한 방법은 VMware Cloud Foundation SDDC Manager를 사용하는 것입니다. 자세한 내용은 VMware Cloud Foundation SDDC Manager 설명서를 참조하십시오. 자세한 내용은 [VMware Cloud Foundation 관리 가이드](#)를 참조하십시오.
- 기존 NSX 배포를 사용하거나 NSX의 새 인스턴스를 배포하여 감독자 네트워킹을 수동으로 구성할 수도 있습니다. 자세한 내용은 [NSX for vSphere IaaS control plane 설치 및 구성](#)을 참조하십시오.

vSphere IaaS control plane에 대한 NSX 설치 및 구성

vSphere IaaS control plane를 사용하려면 감독자, vSphere 네임스페이스 및 네임스페이스 내에서 실행되는 모든 개체(예: vSphere 포드, VM 및 Tanzu Kubernetes 클러스터)에 대한 연결을 사용하도록 설정하기 위한 특정 네트워킹 구성이 필요합니다. vSphere 관리자는 vSphere IaaS control plane에 대한 NSX를 설치하고 구성합니다.

그림 4-7. NSX를 사용하여 감독자를 구성하기 위한 워크플로



이 섹션에서는 새 NSX 인스턴스를 배포하여 감독자 네트워킹을 구성하는 방법에 대해 설명하지만 절차는 기존 NSX 배포에 대해서도 적용됩니다. 또한 이 섹션에서는 감독자 워크로드 도메인을 설정할 때 VMware Cloud Foundation SDDC Manager가 수행하는 작업을 이해하기 위한 배경 지식을 제공합니다.

사전 요구 사항

- 사용 중인 환경이 vSphere 클러스터를 감독자로 구성하기 위한 시스템 요구 사항을 충족하는지 확인합니다. 요구 사항에 대한 자세한 내용은 "vSphere IaaS 제어부 개념 및 계획" 에서 [NSX가 있는 영역 감독자 요구 사항 및 NSX를 사용한 클러스터 감독자 배포 요구 사항](#)을 참조하십시오.
- 감독자에 Tanzu Edition 라이선스를 할당합니다.
- 제어부 VM, 포드 사용 후 삭제 디스크 및 컨테이너 이미지를 배치하기 위한 스토리지 정책을 생성합니다.
- 클러스터의 공유 스토리지를 구성합니다. 공유 스토리지는 vSphere DRS, HA 및 컨테이너의 영구 볼륨 저장에 필요합니다.
- vSphere 클러스터에서 DRS 및 HA가 사용되도록 설정되어 있고 DRS가 완전히 자동화된 모드에 있는지 확인합니다.
- 클러스터에서 [클러스터 전체 구성 수정](#) 권한이 있는지 확인합니다.

절차

1 vSphere Distributed Switch 생성 및 구성

감독자의 모든 호스트에 대한 네트워킹 구성을 처리하려면 vSphere Distributed Switch를 생성하고 분산 포트 그룹을 생성하고 호스트를 스위치와 연결합니다.

2 NSX Manager 배포 및 구성

vSphere Client를 사용하여 NSX Manager를 vSphere 클러스터에 배포하고 vSphere IaaS control plane에서 사용할 수 있습니다.

3 전송 영역 생성

전송 영역은 특정 네트워크를 사용할 수 있는 호스트 및 VM을 나타냅니다. 전송 영역은 하나 이상의 호스트 클러스터에 걸쳐 있을 수 있습니다.

4 NSX Edge 전송 노드 구성 및 배포

NSX Edge VM(가상 시스템)을 NSX 패브릭에 추가하고 이를 NSX Edge 전송 노드 VM으로 구성할 수 있습니다.

vSphere Distributed Switch 생성 및 구성

감독자의 모든 호스트에 대한 네트워킹 구성을 처리하려면 vSphere Distributed Switch를 생성하고 분산 포트 그룹을 생성하고 호스트를 스위치와 연결합니다.

절차

- 1 vSphere Client에서 데이터 센터로 이동합니다.

- 2 탐색기에서 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 **Distributed Switch > 새 Distributed Switch**를 선택합니다.
- 3 새 분산 스위치의 이름을 입력합니다.
예: DSwitch
- 4 **버전 선택**에서 Distributed Switch의 버전을 입력합니다.
8.0을 선택합니다.
- 5 **설정 구성**에서 업링크 포트 수를 입력합니다.
값 **2**를 입력합니다.
- 6 설정을 검토하고 **완료**를 클릭합니다.
- 7 생성된 분산 스위치를 마우스 오른쪽 버튼으로 클릭하고 **설정 > 설정 편집**을 선택합니다.
- 8 **고급** 탭에서 MTU(바이트) 값으로 1700을 초과하는 값을 입력하고 **확인**을 클릭합니다.
MTU 크기는 오버레이 트래픽을 전달하는 모든 네트워크에서 1700 이상이어야 합니다.
예: 9000
NSX는 글로벌 기본 MTU 값 1700을 사용합니다.

분산 포트 그룹 생성

각 NSX Edge 노드 업링크, Edge 노드 TEP, 관리 네트워크 및 공유 스토리지에 대한 분산 포트 그룹을 생성합니다.

기본 포트 그룹 및 기본 업링크는 vSphere Distributed Switch를 생성할 때 생성됩니다. 관리 포트 그룹, vSAN 포트 그룹, Edge TEP 포트 그룹 및 NSX Edge 업링크 포트 그룹을 생성해야 합니다.

사전 요구 사항

vSphere Distributed Switch를 생성했는지 확인합니다.

절차

- 1 vSphere Client에서 데이터 센터로 이동합니다.
- 2 탐색기에서 Distributed Switch를 마우스 오른쪽 버튼으로 클릭하고 **분산 포트 그룹 > 새 분산 포트 그룹**을 선택합니다.
- 3 NSX Edge 업링크에 대한 포트 그룹을 생성합니다.
예: DPortGroup-EDGE-UPLINK
- 4 **VLAN 유형**을 [VLAN 트렁킹]으로 구성합니다.
- 5 기본 VLAN 트렁크 범위(**0-4094**)를 수락합니다.
- 6 **다음**을 클릭한 다음 **마침**을 클릭합니다.

- 7 분산 스위치를 마우스 오른쪽 버튼으로 클릭하고 **작업** 메뉴에서 **분산 포트 그룹 > 분산 포트 그룹 관리**를 선택합니다.
- 8 **팀 구성 및 페일오버**를 선택하고 **다음**을 클릭합니다.
- 9 활성 및 대기 업링크를 구성합니다.
예를 들어 활성 업링크는 Uplink1이고 대기 업링크는 Uplink2입니다.
- 10 **확인**을 클릭하여 포트 그룹 구성을 완료합니다.
- 11 2~10단계를 반복하여 Edge 노드 TEP, 관리 네트워크 및 공유 스토리지에 대한 포트 그룹을 생성합니다.
예를 들어 다음과 같은 포트 그룹을 생성합니다.

포트 그룹	이름	VLAN 유형
Edge 노드 TEP	DPortGroup-EDGE-TEP	VLAN 유형 을 [VLAN 트렁킹]으로 구성합니다. 활성 업링크를 Uplink2로 구성하고 대기 업링크를 Uplink1로 구성합니다. 참고 Edge 노드 TEP에 사용되는 VLAN은 ESXi TEP에 사용되는 VLAN과 달라야 합니다.
관리	DPortGroup-MGMT	VLAN 유형 을 VLAN으로 구성하고 관리 네트워크의 VLAN ID를 입력합니다. 예: 1060
공유 스토리지 또는 vSAN	DPortGroup-VSAN	VLAN 유형 을 VLAN으로 구성하고 VLAN ID를 입력합니다. 예: 3082

- 12 다음 구성 요소에 대한 포트 그룹을 생성합니다.
 - **vSphere vMotion**. 이 포트 그룹은 감독자 업데이트에 필요합니다. vMotion에 대한 기본 포트 그룹을 구성합니다.
 - **VM 트래픽**. VM 트래픽을 처리하도록 기본 포트 그룹을 구성합니다.

vSphere Distributed Switch에 호스트 추가

vSphere Distributed Switch를 사용하여 환경의 네트워킹을 관리하려면 감독자의 호스트를 스위치와 연결해야 합니다. 호스트의 물리적 NIC, VMkernel 어댑터 및 가상 시스템 네트워크 어댑터를 Distributed Switch에 연결합니다.

사전 요구 사항

- 스위치에 연결하려는 물리적 NIC에 할당할 수 있는 업링크가 Distributed Switch에 충분히 있는지 확인합니다.
- Distributed Switch에서 하나 이상의 분산 포트 그룹을 사용할 수 있는지 확인합니다.
- 분산 포트 그룹의 팀 구성 및 페일오버 정책에 활성 업링크가 구성되어 있는지 확인합니다.

절차

- 1 vSphere Client에서 **네트워킹**을 선택하고 Distributed Switch로 이동합니다.
- 2 **작업** 메뉴에서 **호스트 추가 및 관리**를 선택합니다.
- 3 **작업 선택** 페이지에서 **호스트 추가**를 선택하고 **다음**을 클릭합니다.
- 4 **호스트 선택** 페이지에서 **새 호스트**를 클릭하고 데이터 센터에서 호스트를 선택한 후 **확인**을 클릭하고 **다음**을 클릭합니다.
- 5 **물리적 어댑터 관리** 페이지에서 Distributed Switch에 물리적 NIC를 구성합니다.
 - a **다른 스위치/할당되지 않음** 목록에서 물리적 NIC를 선택합니다.
다른 스위치에 이미 연결된 물리적 NIC를 선택하면 현재 Distributed Switch로 마이그레이션됩니다.
 - b **업링크 할당**을 클릭합니다.
 - c 업링크를 선택합니다.
 - d 클러스터의 모든 호스트에 업링크를 할당하려면 **이 업링크 할당을 나머지 호스트에 적용**을 선택합니다.
 - e **확인**을 클릭합니다.
예를 들어 Uplink 1을 vmnic0에 할당하고 Uplink 2를 vmnic1에 할당합니다.
- 6 **다음**을 클릭합니다.
- 7 **VMkernel 어댑터 관리** 페이지에서 VMkernel 어댑터를 구성합니다.
 - a VMkernel 어댑터를 선택하고 **포트 그룹 할당**을 클릭합니다.
 - b 분산 포트 그룹을 선택합니다.
예를 들어 **DPortGroup**을 선택합니다.
 - c 클러스터의 모든 호스트에 포트 그룹을 적용하려면 **이 포트 그룹 할당을 나머지 호스트에 적용**을 선택합니다.
 - d **확인**을 클릭합니다.
- 8 **다음**을 클릭합니다.
- 9 (선택 사항) **VM 네트워킹 마이그레이션** 페이지에서 **가상 시스템 네트워킹 마이그레이션** 확인란을 선택하여 가상 시스템 네트워킹을 구성합니다.
 - a 가상 시스템의 모든 네트워크 어댑터를 분산 포트 그룹에 연결하려면 가상 시스템을 선택하고, 개별 네트워크 어댑터를 연결하려면 해당 네트워크 어댑터만 선택합니다.
 - b **포트 그룹 할당**을 클릭합니다.
 - c 목록에서 분산 포트 그룹을 선택하고 **확인**을 클릭합니다.
 - d **다음**을 클릭합니다.

다음에 수행할 작업

NSX Manager를 배포하고 구성합니다. [NSX Manager 배포 및 구성](#)을 참조하십시오.

NSX Manager 배포 및 구성

vSphere Client를 사용하여 NSX Manager를 vSphere 클러스터에 배포하고 vSphere IaaS control plane에서 사용할 수 있습니다.

OVA 파일을 사용하여 NSX Manager를 배포하려면 이 절차의 단계를 수행합니다.

사용자 인터페이스 또는 CLI를 통해 NSX Manager를 배포하는 방법에 대한 자세한 내용은 "NSX 설치 가이드" 항목을 참조하십시오.

사전 요구 사항

- 환경이 네트워킹 요구 사항을 충족하는지 확인합니다. 요구 사항에 대한 자세한 내용은 "vSphere IaaS 제어부 개념 및 계획"에서 [NSX Advanced Load Balancer](#)를 사용하는 3개 영역 감독자에 대한 요구 사항 및 [NSX Advanced Load Balancer](#)를 사용하여 단일 클러스터 감독자를 사용하도록 설정하기 위한 요구 사항을 참조하십시오.
- 필수 포트가 열려 있는지 확인합니다. 포트 및 프로토콜에 대한 자세한 내용은 "NSX 설치 가이드"의 내용을 확인하십시오.

절차

- 1 VMware 다운로드 포털에서 NSX OVA 파일을 찾습니다.
다운로드 URL을 복사하거나 OVA 파일을 다운로드합니다.
- 2 마우스 오른쪽 버튼을 클릭하고 **OVF 템플릿 배포**를 선택하여 설치 마법사를 시작합니다.
- 3 **OVF 템플릿 선택** 탭에서 OVA 다운로드 URL을 입력하거나 OVA 파일로 이동합니다.
- 4 **이름 및 폴더 선택** 탭에서 NSX Manager VM(가상 시스템)의 이름을 입력합니다.
- 5 **계산 리소스 선택** 탭에서 NSX Manager를 배포할 vSphere 클러스터를 선택합니다.
- 6 **다음**을 클릭하고 세부 정보를 검토합니다.
- 7 **구성** 탭에서 NSX 배포 크기를 선택합니다.
권장되는 최소 배포 크기는 중간입니다.
- 8 **스토리지 선택** 탭에서 배포할 공유 스토리지를 선택합니다.
- 9 **가상 디스크 형식 선택**에서 **씬 프로비저닝**을 선택하여 씬 프로비저닝을 사용하도록 설정합니다.
가상 디스크는 기본적으로 씬 프로비저닝됩니다.
- 10 **네트워크 선택** 탭의 **대상 네트워크**에서 NSX Manager에 대한 대상 네트워크 또는 관리 포트 그룹을 선택합니다.

예: DPortGroup-MGMT

- 11 **템플릿 사용자 지정** 탭에서 시스템 루트, CLI 관리자 및 NSX Manager에 대한 감사 암호를 입력합니다. 암호는 암호 강도 제한을 준수 해야 합니다.
 - 12자 이상.
 - 소문자 하나 이상.
 - 대문자 하나 이상.
 - 숫자 하나 이상.
 - 특수 문자 하나 이상.
 - 5개 이상의 다른 문자.
 - 기본 암호 복잡성 규칙은 Linux PAM 모듈에 의해 적용됩니다.
- 12 기본 IPv4 게이트웨이, 관리 네트워크 IPv4, 관리 네트워크 넷마스크, DNS 서버, 도메인 검색 목록 및 NTP IP 주소를 입력합니다.
- 13 SSH를 사용하도록 설정하고 NSX Manager 명령줄에 루트 SSH 로그인을 허용합니다.
기본적으로 SSH 옵션은 보안상의 이유로 사용되지 않도록 설정됩니다.
- 14 사용자 지정 OVF 템플릿 규격이 정확한지 확인하고 **마침**을 클릭하여 설치를 시작합니다.
- 15 NSX Manager가 부팅되면 CLI에 관리자로 로그인하고 `get interface eth0` 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.
- 16 `get services` 명령을 입력하여 모든 서비스가 실행되고 있는지 확인합니다.

NSX Manager 노드를 배포하여 클러스터 구성

NSX Manager 클러스터는 고가용성을 제공합니다. vCenter Server에서 관리하는 ESXi호스트에서만 사용자 인터페이스를 사용하여 NSX Manager 노드를 배포할 수 있습니다. NSX Manager 클러스터를 생성하려면 두 개의 추가 노드를 배포하여 총 3개 노드로 이루어진 클러스터를 구성합니다. UI에서 새 노드를 배포하면 노드가 처음 배포된 노드에 연결되어 클러스터를 구성합니다. 처음 배포된 노드의 모든 저장소 세부 정보 및 암호가 새로 배포된 노드와 동기화됩니다.

사전 요구 사항

- NSX Manager 노드가 설치되었는지 확인합니다.
- 계산 관리자가 구성되어 있는지 확인합니다.
- 필수 포트가 열려 있는지 확인합니다.
- ESXi 호스트에서 데이터스토어가 구성되었는지 확인합니다.
- 사용할 NSX Manager에 대한 IP 주소 및 게이트웨이, DNS 서버 IP 주소, 도메인 검색 목록 및 NTP 서버 IP 주소가 있는지 확인합니다.
- 대상 VM 포트 그룹 네트워크가 있는지 확인합니다. NSX 장치를 관리 VM 네트워크에 배치합니다.

절차

- 1 브라우저에서 <https://<manager-ip-address>>로 이동한 후 관리자 권한으로 NSX Manager에 로그인합니다.
- 2 장치를 배포하려면 **시스템 > 장치 > NSX 장치 추가**를 선택합니다.
- 3 장치 세부 정보를 입력합니다.

옵션	설명
호스트 이름	노드에 사용할 호스트 이름 또는 FQDN을 입력합니다.
관리 IP/넷마스크	노드에 할당할 IP 주소를 입력합니다.
관리 게이트웨이	노드에서 사용할 게이트웨이 IP 주소를 입력합니다.
DNS 서버	노드에서 사용할 DNS 서버 IP 주소 목록을 입력합니다.
NTP 서버	NTP 서버 IP 주소 목록을 입력합니다.
노드 크기	옵션에서 중형(6 vCPU, 24GB RAM, 300GB 스토리지) 폼 팩터를 선택합니다.

- 4 장치 구성 세부 정보를 입력합니다.

옵션	설명
계산 관리자	계산 관리자로 구성된 vCenter Server를 선택합니다.
계산 클러스터	노드가 가입해야 하는 클러스터를 선택합니다.
데이터스토어	노드 파일에 대한 데이터스토어를 선택합니다.
가상 디스크 형식	씬 프로비저닝 형식을 선택합니다.
네트워크	네트워크 선택 을 클릭하여 노드에 대한 관리 네트워크를 선택합니다.

- 5 액세스 및 자격 증명 세부 정보를 입력합니다.

옵션	설명
SSH 사용	버튼을 전환하여 새 노드에 대한 SSH 로그인을 허용합니다.
루트 액세스 사용	버튼을 전환하여 새 노드에 대한 루트 액세스를 허용합니다.
시스템 루트 자격 증명	새 노드에 대한 루트 암호를 설정하고 확인합니다. 암호는 암호 강도 제한을 준수해야 합니다. <ul style="list-style-type: none"> ■ 12자 이상. ■ 소문자 하나 이상. ■ 대문자 하나 이상. ■ 숫자 하나 이상. ■ 특수 문자 하나 이상. ■ 5개 이상의 다른 문자. ■ 기본 암호 복잡성 규칙은 Linux PAM 모듈에 의해 적용됩니다.
관리 CLI 자격 증명 및 감사 CLI 자격 증명	루트 암호와 동일 확인란을 선택하여 루트에 대해 구성된 것과 동일한 암호를 사용하거나 확인란을 선택 취소하고 다른 암호를 설정합니다.

6 장치 설치를 클릭합니다.

새 노드가 배포됩니다. **시스템 > 장치** 페이지에서 배포 프로세스를 추적할 수 있습니다. 설치가 완료되고 클러스터가 안정화될 때까지 다른 노드를 추가하지 마십시오.

7 배포, 클러스터 구성 및 저장소 동기화가 완료될 때까지 기다립니다.

가입 및 클러스터 안정화 프로세스는 10~15분 정도 걸릴 수 있습니다. 다른 클러스터 변경 작업을 수행하기 전에 모든 클러스터 서비스 그룹의 상태가 UP인지 확인합니다.

8 노드가 부팅되면 CLI에 관리자로 로그인하고 `get interface eth0` 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

9 클러스터에 노드가 두 개만 있는 경우 다른 장치를 추가합니다. **시스템 > 장치 > NSX 장치 추가**를 선택하고 구성 단계를 반복합니다.

라이선스 추가

NSX Manager를 사용하여 라이선스를 추가합니다.

사전 요구 사항

NSX 고급 라이선스 또는 더 상위의 라이선스를 얻습니다.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **시스템 > 라이선스 > 추가**를 선택합니다.
- 3 라이선스 키를 입력합니다.
- 4 **추가**를 클릭합니다.

계산 관리자 추가

계산 관리자는 호스트 및 가상 시스템과 같은 리소스를 관리하는 애플리케이션입니다. NSX와 연결된 vCenter Server를 NSX Manager에서 계산 관리자로 구성합니다.

자세한 내용은 "NSX 관리 가이드" 를 참조하십시오.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **시스템 > 패브릭 > 계산 관리자 > 추가**를 선택합니다.
- 3 계산 관리자 세부 정보를 입력합니다.

옵션	설명
이름 및 설명	vCenter Server의 이름 및 설명을 입력합니다.
유형	기본 유형은 VMware vCenter입니다.

옵션	설명
다중 NSX	이 옵션은 선택되지 않은 상태로 둡니다. 다중 NSX 옵션을 사용하면 동일한 vCenter Server를 여러 NSX Manager에 등록할 수 있습니다. 감독자 및 vSphere Lifecycle Manager 클러스터에서는 이 옵션이 지원되지 않습니다.
FQDN 또는 IP 주소	vCenter Server의 FQDN 또는 IP 주소를 입력합니다.
역방향 프록시의 HTTPS 포트	기본 포트는 443입니다. 다른 포트를 사용하는 경우 포트가 모든 NSX Manager 장치에서 열려 있는지 확인합니다. NSX에서 계산 관리자를 등록하도록 역방향 프록시 포트를 설정합니다.
사용자 이름 및 암호	vCenter Server 로그인 자격 증명을 입력합니다.
SHA-256 지문	vCenter Server SHA-256 지문 알고리즘 값을 입력합니다.

다른 설정은 기본값을 그대로 유지할 수 있습니다.

지문 값을 비워 두면 서버에서 제공한 지문을 수락할지 묻는 메시지가 나타납니다. 지문을 수락한 후 NSX에서 vCenter 리소스를 찾아 등록하는 데 몇 초 정도 소요됩니다.

- 4 신뢰 사용을 선택하여 vCenter Server가 NSX와 통신하도록 허용합니다.
- 5 NSX Manager에 대한 지문 값을 제공하지 않으면 시스템에서 지문을 식별하여 표시합니다.
- 6 추가를 클릭하여 지문을 수락합니다.

결과

잠시 후에 계산 관리자가 vCenter Server에 등록되고 연결 상태가 접속 중으로 변경됩니다. vCenter Server의 FQDN/PNID가 변경되면 NSX Manager에 다시 등록해야 합니다. 자세한 내용은 [NSX Manager에 vCenter Server 등록](#)의 내용을 참조하십시오.

참고 vCenter Server 등록이 완료된 후 먼저 계산 관리자를 삭제하지 않은 상태에서 NSX Manager VM의 전원을 끄고 삭제하면 안 됩니다. 이 지침을 따르지 않으면 새 NSX Manager를 배포할 때 동일한 vCenter Server를 다시 등록할 수 없게 됩니다. vCenter Server가 이미 다른 NSX Manager에 등록되어 있다는 오류 메시지가 표시됩니다.

계산 관리자 이름을 클릭하여 세부 정보를 보거나, 계산 관리자를 편집하거나, 계산 관리자에 적용되는 태그를 관리할 수 있습니다.

전송 영역 생성

전송 영역은 특정 네트워크를 사용할 수 있는 호스트 및 VM을 나타냅니다. 전송 영역은 하나 이상의 호스트 클러스터에 걸쳐 있을 수 있습니다.

vSphere 관리자는 기본 전송 영역을 사용하거나 다음을 생성합니다.

- 감독자 제어부 VM에서 사용하는 오버레이 전송 영역.
- 물리적 네트워크에 대한 업링크에 사용할 NSX Edge 노드의 VLAN 전송 영역.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **시스템 > 패브릭 > 전송 영역 > 추가**를 선택합니다.
- 3 전송 영역의 이름과 필요한 경우 설명을 입력합니다.
- 4 트래픽 유형을 선택합니다.

오버레이 또는 **VLAN**을 선택할 수 있습니다.

기본적으로 다음 전송 영역이 존재합니다.

- 이름이 `nsx-vlan-transportzone`인 VLAN 전송 영역
- 이름이 `nsx-overlay-transportzone`인 오버레이 전송 영역

- 5 (선택 사항) 하나 이상의 업링크 팀 구성 정책 이름을 입력합니다.

전송 영역에 연결된 세그먼트는 이러한 명명된 팀 구성 정책을 사용합니다. 세그먼트에서 일치하는 명명된 팀 구성 정책을 찾지 못하면 기본 업링크 팀 구성 정책이 사용됩니다.

결과

전송 영역 페이지에 새 전송 영역이 나타납니다.

호스트 터널 끝점 IP 주소에 대한 IP 풀 생성

ESXi 호스트 TEP(터널 끝점)에 대한 IP 풀을 생성합니다. TEP는 외부 IP 헤더에 사용되는 소스 및 대상 IP 주소로, 오버레이 프레임의 NSX 캡슐화를 시작하고 종료하는 ESXi 호스트를 식별합니다. TEP IP 주소에 DHCP 또는 수동으로 구성된 IP 풀을 사용할 수 있습니다.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **네트워킹 > IP 주소 풀 > IP 주소 풀 추가**를 선택합니다.
- 3 다음 IP 풀 세부 정보를 입력합니다.

옵션	설명
이름 및 설명	IP 풀 이름 및 설명(선택 사항)을 입력합니다. 예: <code>ESXI-TEP-IP-POOL</code>
IP 범위	IP 할당 범위를 입력합니다. 예를 들어 <code>192.23.213.158 - 192.23.213.160</code> 입니다.
게이트웨이	게이트웨이 IP 주소를 입력합니다. 예: <code>192.23.213.253</code>
CIDR	CIDR 표기법으로 네트워크 주소를 입력합니다. 예: <code>192.23.213.0/24</code>

- 4 **추가 및 적용**을 클릭합니다.

결과

생성한 TEP IP 풀이 **IP 풀** 페이지에 나열되어 있는지 확인합니다.

Edge 노드에 대한 IP 풀 생성

Edge 노드에 대한 IP 풀을 생성합니다. TEP 주소를 라우팅할 필요는 없습니다. Edge TEP가 호스트 TEP와 통신할 수 있도록 하는 IP 주소 지정 체계를 사용할 수 있습니다.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **네트워킹 > IP 주소 풀 > IP 주소 풀 추가**를 선택합니다.
- 3 다음 IP 풀 세부 정보를 입력합니다.

옵션	설명
이름 및 설명	IP 풀 이름 및 설명(선택 사항)을 입력합니다. 예: EDGE-TEP-IP-POOL
IP 범위	IP 할당 범위를 입력합니다. 예를 들어 192.23.213.1 - 192.23.213.10.입니다.
게이트웨이	게이트웨이 IP 주소를 입력합니다. 예: 192.23.213.253
CIDR	CIDR 표기법으로 네트워크 주소를 입력합니다. 예: 192.23.213.0/24

- 4 **추가 및 적용**을 클릭합니다.

결과

생성한 IP 풀이 **IP 풀** 페이지에 나열되어 있는지 확인합니다.

호스트 업링크 프로파일 생성

호스트 업링크 프로파일은 ESXi 호스트에서 NSX 세그먼트까지의 업링크에 대한 정책을 정의합니다.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **시스템 > 패브릭 > 프로파일 > 업링크 프로파일 > 추가**를 선택합니다.
- 3 업링크 프로파일 이름을 입력하고 필요한 경우 업링크 프로파일 설명을 입력합니다.
예: ESXI-UPLINK-PROFILE
- 4 **팀 구성** 섹션에서 **추가**를 클릭하여 명명 팀 구성 정책을 추가하고 **페일오버 명령** 정책을 구성합니다.

활성 업링크 목록이 지정되고 전송 노드의 각 인터페이스가 하나의 활성 업링크에 고정됩니다. 이 구성을 사용하면 여러 활성 업링크를 동시에 사용할 수 있습니다.

5 활성 및 대기 업링크를 구성합니다.

예를 들어 활성 업링크로 `uplink-1`을 구성하고 대기 업링크로 `uplink-2`를 구성합니다.

6 전송 VLAN 값을 입력합니다.

업링크 프로파일에 설정된 전송 VLAN은 오버레이 트래픽에 태그를 지정하고 VLAN ID는 터널 끝점(TEP)에서 사용됩니다.

예: 1060

7 MTU 값을 입력합니다.

업링크 프로파일 MTU의 기본값은 1600입니다.

참고 값은 1600 이상이어야 하지만 물리적 스위치 및 vSphere Distributed Switch의 MTU 값보다 높아서 안 됩니다.

Edge 업링크 프로파일 생성

Edge 가상 시스템 오버레이 트래픽에 대해 하나의 활성 업링크가 있는 페일오버 순서 팀 구성 정책으로 업링크 프로파일을 생성합니다.

절차

1 NSX Manager에 로그인합니다.

2 **시스템 > 패브릭 > 프로파일 > 업링크 프로파일 > 추가**를 선택합니다.

3 업링크 프로파일 이름을 입력하고 필요한 경우 업링크 프로파일 설명을 추가합니다.

예: `EDGE-UPLINK-PROFILE`

4 **팀 구성** 섹션에서 **추가**를 클릭하여 명명 팀 구성 정책을 추가하고 **페일오버** 정책을 구성합니다.

활성 업링크 목록이 나열되고 전송 노드의 각 인터페이스가 하나의 활성 업링크에 고정됩니다. 이 구성을 사용하면 여러 활성 업링크를 동시에 사용할 수 있습니다.

5 활성 업링크를 구성합니다.

예를 들어 `uplink-1`을 활성 업링크로 구성합니다.

6 **업링크 프로파일** 페이지에서 업링크를 확인합니다.

전송 노드 프로파일 생성

전송 노드 프로파일은 프로파일이 연결된 특정 클러스터의 호스트에서 NSX가 설치되고 구성되는 방법을 정의합니다.

사전 요구 사항

오버레이 전송 영역을 생성했는지 확인합니다.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **시스템 > 패브릭 > 프로파일 > 전송 노드 프로파일 > 추가**를 선택합니다.
- 3 전송 노드 프로파일의 이름과 필요한 경우 설명을 입력합니다.
예: HOST-TRANSPORT-NODE-PROFILE
- 4 **새 노드 스위치** 섹션에서 **유형**을 vDS로 선택합니다.
- 5 **모드**를 Standard으로 선택합니다.
- 6 목록에서 vCenter Server 및 Distributed Switch 이름을 선택합니다.
예를 들어 DSwitch입니다.
- 7 이전에 생성된 오버레이 전송 영역을 선택합니다.
예: NSX-OVERLAY-TRANSPORTZONE
- 8 이전에 생성된 호스트 업링크 프로파일을 선택합니다.
예: ESXI-UPLINK-PROFILE
- 9 **IP 할당** 목록에서 **IP 풀 사용**을 선택합니다.
- 10 이전에 생성된 호스트 TEP 풀을 선택합니다.
예: ESXI-TEP-IP-POOL
- 11 **팀 구성 정책 스위치 매핑**에서 편집 아이콘을 클릭하고 NSX 업링크 프로파일에 정의된 업링크를 vSphere Distributed Switch 업링크에 매핑합니다.
예를 들어 uplink-1 (active)을 Uplink 1에 매핑하고 uplink-2 (standby)를 Uplink 2에 매핑합니다.
- 12 **추가**를 클릭합니다.
- 13 생성한 프로파일이 **전송 노드 프로파일** 페이지에 나열되어 있는지 확인합니다.

클러스터에서 NSX 구성

NSX를 설치하고 오버레이 TEP를 준비하려면 vSphere 클러스터에 전송 노드 프로파일을 적용합니다.

사전 요구 사항

전송 노드 프로파일을 생성했는지 확인합니다.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **시스템 > 패브릭 > 노드 > 호스트 전송 노드**를 선택합니다.

3 **관리자** 드롭다운 메뉴에서 기존 vCenter Server를 선택합니다.

페이지에 사용 가능한 vSphere 클러스터가 나열됩니다.

4 NSX를 구성하려는 계산 클러스터를 선택합니다.

5 **NSX 구성**을 클릭합니다.

6 이전에 생성한 전송 노드 프로파일을 선택하고 **적용**을 클릭합니다.

예: HOST-TRANSPORT-NODE-PROFILE

7 **호스트 전송 노드** 페이지에서 NSX 구성 상태가 `Success`이고 클러스터에 있는 호스트의 NSX Manager 연결 상태가 `Up`인지 확인합니다.

결과

이전에 생성된 전송 노드 프로파일이 vSphere 클러스터에 적용되어 NSX를 설치하고 오버레이 TEP를 준비합니다.

NSX Edge 전송 노드 구성 및 배포

NSX Edge VM(가상 시스템)을 NSX 패브릭에 추가하고 이를 NSX Edge 전송 노드 VM으로 구성할 수 있습니다.

사전 요구 사항

전송 영역, Edge 업링크 프로파일 및 Edge TEP IP 풀을 생성했는지 확인합니다.

절차

1 NSX Manager에 로그인합니다.

2 **시스템 > 패브릭 > 노드 > Edge 전송 노드 > Edge VM 추가**를 선택합니다.

3 **이름 및 설명**에서 NSX Edge의 이름을 입력합니다.

예를 들어 `nsx-edge-1`입니다.

4 vCenter Server의 호스트 이름이나 FQDN을 입력합니다.

예: `nsx-edge-1.lab.com`

5 `Large` 폼 팩터를 선택합니다.

6 **자격 증명**에서 NSX Edge에 대한 루트 암호 및 CLI를 입력합니다. 암호는 암호 강도 제한을 준수 해야 합니다.

- 12자 이상.
- 소문자 하나 이상.
- 대문자 하나 이상.
- 숫자 하나 이상.

- 특수 문자 하나 이상.
- 5개 이상의 다른 문자.
- 기본 암호 복잡성 규칙은 Linux PAM 모듈에 의해 적용됩니다.

7 CLI 및 루트 자격 증명에 대해 **SSH 로그인 허용**을 사용하도록 설정합니다.

8 **배포 구성**에서 다음 속성을 구성합니다.

옵션	설명
계산 관리자	드롭다운 메뉴에서 계산 관리자를 선택합니다. 예를 들어 vCenter를 선택합니다.
클러스터	드롭다운 메뉴에서 클러스터를 선택합니다. 예를 들어 Compute-Cluster를 선택합니다.
데이터스토어	목록에서 공유 데이터스토어를 선택합니다. 예: vsanDatastore

9 노드 설정을 구성합니다.

옵션	설명
IP 할당	[정적]을 선택합니다. 다음에 대한 값을 입력합니다. <ul style="list-style-type: none"> ■ 관리 IP: vCenter Server 관리 네트워크와 동일한 VLAN의 IP 주소를 입력합니다. 예: 10.197.79.146/24 ■ 기본 게이트웨이: 관리 네트워크의 기본 게이트웨이입니다. 예: 10.197.79.253
관리 인터페이스	인터페이스 선택 을 클릭하고 드롭다운 메뉴에서 이전에 생성한 관리 네트워크와 동일한 VLAN에 있는 vSphere Distributed Switch 포트 그룹을 선택합니다. 예: DPortGroup-MGMT

10 **NSX 구성**에서 **스위치 추가**를 클릭하여 스위치 속성을 구성합니다.

11 **Edge 스위치 이름**의 기본 이름을 사용합니다.

예: nvds1

12 전송 노드가 속하는 전송 영역을 선택합니다.

이전에 생성된 오버레이 전송 영역을 선택합니다.

예: nsx-overlay-transportzone

13 이전에 생성된 Edge 업링크 프로파일을 선택합니다.

예: EDGE-UPLINK-PROFILE

14 **IP 할당**에서 **IP 풀 사용**을 선택합니다.

15 이전에 생성된 Edge TEP IP 풀을 선택합니다.

예: EDGE-TEP-IP-POOL

16 **팀 구성 정책 스위치 매핑** 섹션에서 업링크를 이전에 생성된 Edge 업링크 프로파일에 매핑합니다.

예를 들어 Uplink1의 경우 DPortGroup-EDGE-TEP를 선택합니다.

17 10-16단계를 반복하여 새 스위치를 추가합니다.

예를 들어 다음 값을 구성합니다.

속성	값
Edge 스위치 이름	nvds2
전송 영역	nsx-vlan-transportzone
Edge 업링크 프로파일	EDGE-UPLINK-PROFILE
팀 구성 정책 스위치 매핑	DPortGroup-EDGE-UPLINK

18 **마침**을 클릭합니다.

19 두 번째 NSX Edge VM에 대해 2-18단계를 반복합니다.

20 **Edge 전송 노드** 페이지에서 연결 상태를 확인합니다.

NSX Edge 클러스터 생성

하나 이상의 NSX Edge를 항상 사용할 수 있도록 하려면 NSX Edge 클러스터를 생성합니다.

절차

1 NSX Manager에 로그인합니다.

2 **시스템 > 패브릭 > 노드 > Edge 클러스터 > 추가**를 선택합니다.

3 NSX Edge 클러스터 이름을 입력합니다.

예: EDGE-CLUSTER

4 드롭다운 메뉴에서 기본 NSX Edge 클러스터 프로파일을 선택합니다.

nsx-default-edge-high-availability-profile을 선택합니다.

5 **멤버 유형** 드롭다운 메뉴에서 **Edge 노드**를 선택합니다.

6 **사용 가능** 열에서 이전에 생성된 NSX Edge VM을 선택하고 오른쪽 화살표를 클릭하여 **선택됨** 열로 VM을 이동합니다.

7 예를 들어 nsx-edge-1 및 nsx-edge-2를 선택합니다.

8 **저장**을 클릭합니다.

Tier-0 업링크 세그먼트 생성

Tier-0 업링크 세그먼트는 NSX의 North-South 연결을 물리적 인프라에 제공합니다.

사전 요구 사항

Tier-0 게이트웨이를 생성했는지 확인합니다.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **네트워킹 > 세그먼트 > 세그먼트 추가**를 선택합니다.
- 3 세그먼트의 이름을 입력합니다.
예: TIER-0-LS-UPLINK
- 4 이전에 생성한 전송 영역을 선택합니다.
예를 들어 `nsx-vlan-transportzone`를 선택합니다.
- 5 **관리 상태**를 전환하여 사용하도록 설정합니다.
- 6 Tier-0 게이트웨이의 VLAN ID를 입력합니다.
예: 1089
- 7 **저장**을 클릭합니다.

Tier-0 게이트웨이 생성

Tier-0 게이트웨이는 NSX 논리적 네트워킹에 대한 North-South 연결을 물리적 인프라에 제공하는 NSX 논리적 라우터입니다. vSphere IaaS control plane는 동일한 전송 영역에 있는 여러 NSX Edge 클러스터에서 여러 개의 Tier-0 게이트웨이를 지원합니다.

Tier-0 게이트웨이에는 Tier-1 게이트웨이에 대한 다운링크 연결과 물리적 네트워크에 대한 외부 연결이 있습니다.

Tier-0 게이트웨이의 HA(고가용성) 모드를 **활성-활성** 또는 **활성-대기** 상태로 구성할 수 있습니다. 다음 서비스는 **활성-대기** 모드에서만 지원됩니다.

- NAT
- 로드 밸런싱
- 상태 저장 방화벽
- VPN

NAT 규칙 또는 로드 밸런서 VIP가 Tier-0 게이트웨이 외부 인터페이스의 서브넷에서 IP 주소를 사용하는 경우, 프록시 ARP가 Tier-0 게이트웨이에서 자동으로 사용하도록 설정됩니다. 프록시 ARP를 사용하도록 설정하면 오버레이 세그먼트의 호스트와 VLAN 세그먼트의 호스트가 물리적 네트워킹 패브릭에서 변경 사항을 구현하지 않고 네트워크 트래픽을 함께 교환할 수 있습니다.

NSX 3.2 이전의 경우 프록시 ARP는 **활성-대기** 구성의 Tier-0 게이트웨이에서만 지원됩니다. NSX 3.2부터 프록시 ARP는 **활성-활성** 구성의 Tier-0 게이트웨이에서도 지원됩니다.

자세한 내용은 "NSX 관리 가이드" 항목을 참조하십시오.

사전 요구 사항

NSX Edge 클러스터를 생성했는지 확인합니다.

절차

1 NSX Manager에 로그인합니다.

2 **네트워킹 > Tier-O 게이트웨이**를 선택합니다.

3 **Tier-O 게이트웨이 추가**를 클릭합니다.

4 Tier-O 게이트웨이의 이름을 입력합니다.

예: Tier-0_VWT

5 **활성-대기 HA** 모드를 선택합니다.

활성-대기 모드에서는 선택된 활성 멤버가 모든 트래픽을 처리합니다. 활성 멤버가 실패하면 새 멤버가 활성 상태로 선택됩니다.

6 이전에 생성한 NSX Edge 클러스터를 선택합니다.

예를 들어 **EDGE-CLUSTER**를 선택합니다.

7 **저장**을 클릭합니다.

Tier-O 게이트웨이가 생성됩니다.

8 **예**를 선택하여 구성을 계속합니다.

9 인터페이스를 구성합니다.

a **인터페이스**를 확장하고 **설정**을 클릭합니다.

b **인터페이스 추가**를 클릭합니다.

c 이름을 입력하십시오.

예를 들어 이름 **TIER-0_VWT-UPLINK1**을 입력합니다.

d **유형**을 **외부**로 선택합니다.

e Edge 논리적 라우터 - 업링크 VLAN에서 IP 주소를 입력합니다. IP 주소는 이전에 생성된 NSX Edge VM에 대해 구성된 관리 IP 주소와 달라야 합니다.

예: 10.197.154.1/24

f **연결 대상**에서 이전에 생성된 Tier-O 업링크 세그먼트를 선택합니다.

예를 들어 **TIER-0-LS-UPLINK**입니다.

g 목록에서 NSX Edge 노드를 선택합니다.

예: nsx-edge-1

h **저장**을 클릭합니다.

- i 두 번째 인터페이스에 대해 a - h 단계를 반복합니다.

예를 들어 nsx-edge-2 Edge 노드에 연결된 IP 주소가 10.197.154.2/24인 두 번째 업링크 TIER-0_VWT-UPLINK2를 생성합니다.

- j **닫기**를 클릭합니다.

10 고가용성을 구성하려면 **HA VIP 구성**에서 **설정**을 클릭합니다.

- a **HA VIP 구성 추가**를 클릭합니다.

- b IP 주소를 입력합니다.

예를 들어 10.197.154.3/24입니다.

- c 인터페이스를 선택합니다.

예를 들어 TIER-0_VWT-UPLINK1 및 TIER-0_VWT-UPLINK2를 선택합니다.

- d **추가 및 적용**을 클릭합니다.

11 라우팅을 구성하려면 **라우팅**을 클릭합니다.

- a 정적 경로에서 **설정**을 클릭합니다.

- b **정적 경로 추가**를 클릭합니다.

- c 이름을 입력하십시오.

예: DEFAULT-STATIC-ROUTE

- d 네트워크 IP 주소로 0.0.0.0/0을 입력합니다.

- e 다음 홉을 구성하려면 **다음 홉 설정**을 클릭한 후 **다음 홉 추가**를 클릭합니다.

- f 다음 홉 라우터의 IP 주소를 입력합니다. 일반적으로 이것은 NSX Edge 논리적 라우터 업링크 VLAN에서 관리 네트워크 VLAN의 기본 게이트웨이입니다.

예: 10.197.154.253

- g **추가 및 적용**을 클릭하고 **저장**을 클릭합니다.

- h **닫기**를 클릭합니다.

12 연결을 확인하려면 물리적 아키텍처의 외부 디바이스에서 사용자가 구성한 업링크를 ping할 수 있는지 확인합니다.

다음에 수행할 작업

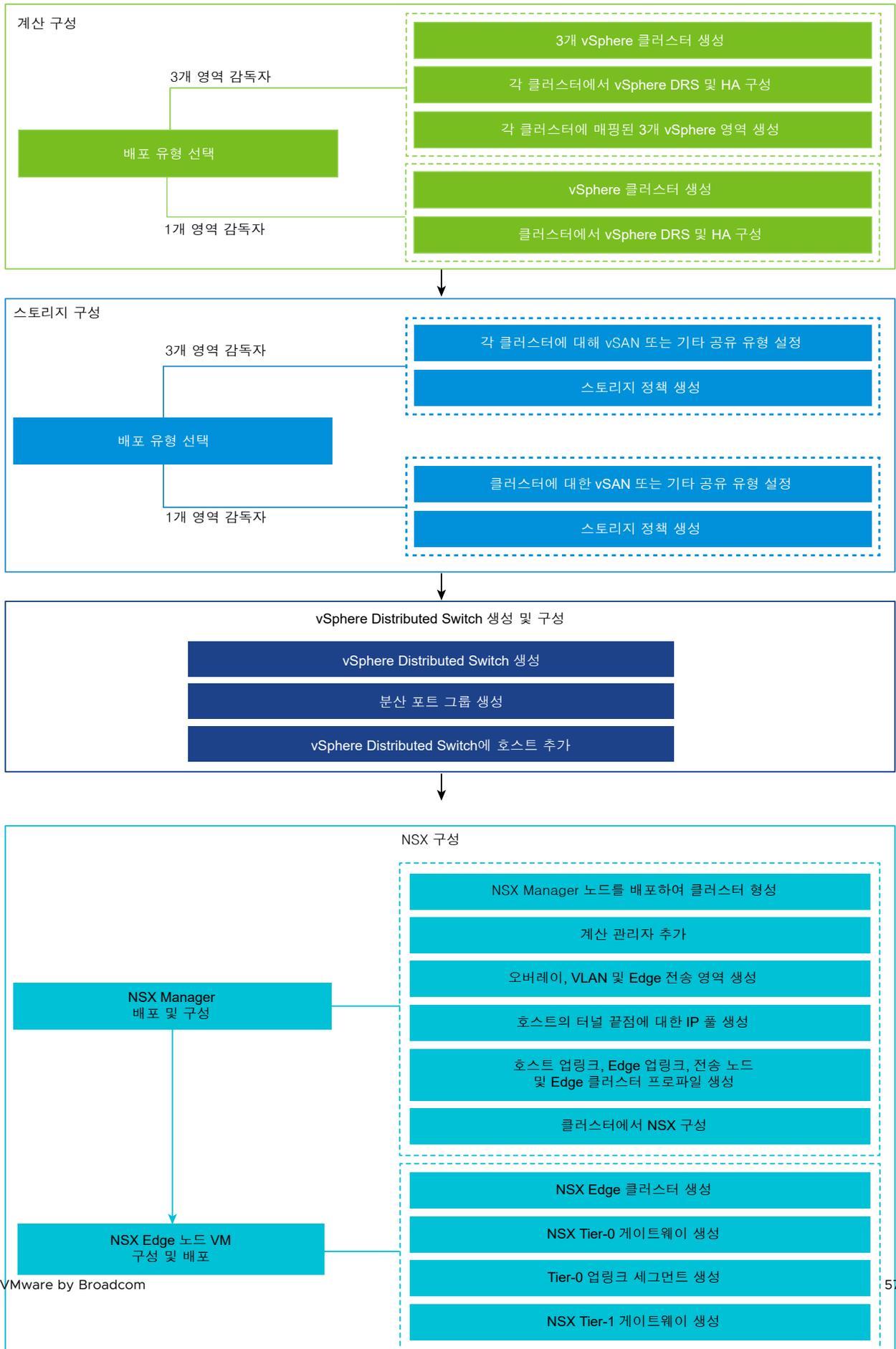
감독자를 구성합니다. [감독자 네트워킹](#)을 사용하여 1개 영역 NSX 배포 항목을 참조하십시오.

NSX 및 NSX Advanced Load Balancer 설치 및 구성

NSX를 네트워킹 스택으로 사용하는 감독자 환경에서는 로드 밸런싱 서비스에 NSX Advanced Load Balancer를 사용할 수 있습니다.

이 섹션에서는 새 NSX 인스턴스와 새 NSX Advanced Load Balancer를 배포하여 감독자 네트워킹을 구성하는 방법을 설명합니다. NSX Advanced Load Balancer를 설치 및 구성하는 절차는 기존 NSX 배포에도 적용할 수 있습니다.

그림 4-8. NSX 및 NSX Advanced Load Balancer를 사용하여 감독자를 구성하기 위한 워크플로



NSX Advanced Load Balancer와 함께 사용할 감독자용 vSphere Distributed Switch 생성

NSX 네트워킹 스택 및 NSX Advanced Load Balancer를 감독자로 사용하는 vSphere 클러스터를 구성하려면 vSphere Distributed Switch를 생성해야 합니다. 감독자에 대한 워크로드 네트워크로 구성할 수 있는 Distributed Switch에서 포트 그룹을 생성합니다. 서비스 엔진 데이터 인터페이스를 연결하려면 NSX Advanced Load Balancer에 분산 포트 그룹이 필요합니다. 포트 그룹은 서비스 엔진에 애플리케이션 VIP(가상 IP)를 배치하는 데 사용됩니다.

사전 요구 사항

NSX Advanced Load Balancer와 함께 감독자에 vSphere 네트워킹을 사용하기 위한 시스템 요구 사항 및 네트워크 토폴로지를 검토합니다. "vSphere IaaS 제어부 개념 및 계획" 에서 [NSX 및 NSX Advanced Load Balancer가 있는 영역 감독자 요구 사항](#) 및 [NSX 및 NSX Advanced Load Balancer를 사용한 클러스터 감독자 배포 요구 사항](#)을 참조하십시오.

절차

- 1 vSphere Client에서 데이터 센터로 이동합니다.
- 2 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 **Distributed Switch > 새 Distributed Switch**를 선택합니다.
- 3 스위치의 이름(예: **wcp_vds_1**)을 입력하고 **다음**을 클릭합니다.
- 4 스위치에 대해 버전 8.0을 선택하고 **다음**을 클릭합니다.
- 5 **포트 그룹 이름**에서 **Primary Workload Network**를 입력하고 **다음**을 클릭한 후 **마침**을 클릭합니다.
 하나의 포트 그룹이 포함된 새 Distributed Switch가 데이터 센터에 생성됩니다. 이 포트 그룹을 생성할 감독자에 대한 기본 워크로드 네트워크로 사용할 수 있습니다. 기본 워크로드 네트워크는 Kubernetes 제어부 VM에 대한 트래픽을 처리합니다.
- 6 워크로드 네트워크에 대한 분산 포트 그룹을 생성합니다.
 생성하는 포트 그룹의 수는 감독자에 대해 구현하려는 토폴로지에 따라 다릅니다. 하나의 분리된 워크로드 네트워크가 있는 토폴로지의 경우 감독자의 모든 네임스페이스에 대한 네트워크로 사용할 하나의 분산 포트 그룹을 생성합니다. 네임스페이스별로 분리된 네트워크가 있는 토폴로지의 경우 생성할 네임스페이스 수와 동일한 수의 포트 그룹을 생성합니다.
 - a 새로 생성된 Distributed Switch로 이동합니다.
 - b 스위치를 마우스 오른쪽 버튼으로 클릭하고 **분산 포트 그룹 > 새 분산 포트 그룹**을 선택합니다.
 - c 포트 그룹의 이름(예: **Workload Network**)을 입력하고 **다음**을 클릭합니다.
 - d 기본값을 그대로 두고 **다음**을 클릭한 다음 **마침**을 클릭합니다.

7 데이터 네트워크에 대한 포트 그룹을 생성합니다.

- 분산 스위치를 마우스 오른쪽 버튼으로 클릭하고 **분산 포트 그룹 > 새 분산 포트 그룹**을 선택합니다.
- 포트 그룹의 이름(예: **Data Network**)을 입력하고 **다음**을 클릭합니다.
- 설정 구성** 페이지에서 새 분산 포트 그룹에 대한 일반 속성을 입력하고 **다음**을 클릭합니다.

속성	설명
포트 바인딩	이 분산 포트 그룹에 연결된 가상 시스템에 포트가 할당되는 시점을 선택합니다. 가상 시스템이 분산 포트 그룹에 연결할 때 가상 시스템에 포트를 할당하려면 정적 바인딩 을 선택합니다.
포트 할당	탄력적 포트 할당을 선택합니다. 기본 포트 수는 8개입니다. 포트가 모두 할당되면 새로 여덟 개의 포트가 생성됩니다.
포트 수	기본값을 유지합니다.
네트워크 리소스 풀	드롭다운 메뉴에서 사용자 정의 네트워크 리소스 풀에 새 분산 포트 그룹을 할당합니다. 네트워크 리소스 풀을 생성하지 않은 경우 이 메뉴는 비어 있습니다.
VLAN	드롭다운 메뉴에서 VLAN 트래픽 필터링 및 표시 유형을 선택합니다. <ul style="list-style-type: none"> ■ 없음: VLAN을 사용하지 않습니다. External Switch Tagging을 사용하는 경우 이 옵션을 선택합니다. ■ VLAN: [VLAN ID] 텍스트 상자에 Virtual Switch Tagging에 대해 1-4094 사이의 값을 입력합니다. ■ VLAN 트렁킹: Virtual Guest Tagging에 대해 그리고 ID가 있는 VLAN 트래픽을 게스트 OS에 전달하려는 경우 이 옵션을 사용합니다. VLAN 트렁크 범위를 입력합니다. 쉼표로 구분된 목록을 사용하여 여러 개의 범위 또는 개별 VLAN을 설정할 수 있습니다. 예: 1702-1705, 1848-1849 ■ 전용 VLAN: 트래픽을 Distributed Switch에서 생성된 전용 VLAN과 연결합니다. 전용 VLAN을 생성하지 않은 경우에 이 메뉴는 비어 있습니다.
고급	이 옵션은 선택되지 않은 상태로 둡니다.

8 완료 준비 페이지에서 구성을 검토하고 **마침**을 클릭합니다.

결과

Distributed Switch가 생성되고 Distributed Switch 아래에 분산 포트 그룹이 표시됩니다.

NSX Manager 배포 및 구성

vSphere Client를 사용하여 vSphere 클러스터에 NSX Manager를 배포합니다. 그런 다음 NSX Manager를 구성하고 사용하여 NSX 환경을 관리합니다.

사전 요구 사항

- ■ 환경이 네트워킹 요구 사항을 충족하는지 확인합니다. 요구 사항에 대한 자세한 내용은 "vSphere IaaS 제어부 개념 및 계획"에서 **NSX 및 NSX Advanced Load Balancer가 있는 영역 감독자 요구 사항 및 NSX 및 NSX Advanced Load Balancer를 사용한 클러스터 감독자 배포 요구 사항**을 참조하십시오.

- 필수 포트가 열려 있는지 확인합니다. 포트 및 프로토콜에 대한 자세한 내용은 "NSX 설치 가이드"의 내용을 확인하십시오.

절차

- 1 VMware 다운로드 포털에서 NSX OVA 파일을 찾습니다.
다운로드 URL을 복사하거나 OVA 파일을 다운로드합니다.
- 2 마우스 오른쪽 버튼을 클릭하고 **OVF 템플릿 배포**를 선택하여 설치 마법사를 시작합니다.
- 3 **OVF 템플릿 선택** 탭에서 OVA 다운로드 URL을 입력하거나 OVA 파일로 이동합니다.
- 4 **이름 및 폴더 선택** 탭에서 NSX Manager VM(가상 시스템)의 이름을 입력합니다.
- 5 **계산 리소스 선택** 탭에서 NSX Manager를 배포할 vSphere 클러스터를 선택합니다.
- 6 **다음**을 클릭하고 세부 정보를 검토합니다.
- 7 **구성** 탭에서 NSX 배포 크기를 선택합니다.
- 8 **스토리지 선택** 탭에서 배포할 공유 스토리지를 선택합니다.
- 9 **가상 디스크 형식 선택**에서 **씬 프로비저닝**을 선택하여 씬 프로비저닝을 사용하도록 설정합니다.
가상 디스크는 기본적으로 씬 프로비저닝됩니다.
- 10 **네트워크 선택** 탭의 **대상 네트워크**에서 NSX Manager에 대한 대상 네트워크 또는 관리 포트 그룹을 선택합니다.
예: DPortGroup-MGMT
- 11 **템플릿 사용자 지정** 탭에서 시스템 루트, CLI 관리자 및 NSX Manager에 대한 감사 암호를 입력합니다. 암호는 암호 강도 제한을 준수 해야 합니다.
 - 12자 이상.
 - 소문자 하나 이상.
 - 대문자 하나 이상.
 - 숫자 하나 이상.
 - 특수 문자 하나 이상.
 - 5개 이상의 다른 문자.
 - 기본 암호 복잡성 규칙은 Linux PAM 모듈에 의해 적용됩니다.
- 12 기본 IPv4 게이트웨이, 관리 네트워크 IPv4, 관리 네트워크 넷마스크, DNS 서버, 도메인 검색 목록 및 NTP IP 주소를 입력합니다.
- 13 SSH를 사용하도록 설정하고 NSX Manager 명령줄에 루트 SSH 로그인을 허용합니다.
기본적으로 SSH 옵션은 보안상의 이유로 사용되지 않도록 설정됩니다.
- 14 사용자 지정 OVF 템플릿 규격이 정확한지 확인하고 **마침**을 클릭하여 설치를 시작합니다.

- 15 NSX Manager가 부팅되면 CLI에 관리자로 로그인하고 `get interface eth0` 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.
- 16 `get services` 명령을 입력하여 모든 서비스가 실행되고 있는지 확인합니다.

NSX Manager 노드를 배포하여 클러스터 구성

NSX Manager 클러스터는 고가용성을 제공합니다. vCenter Server에서 관리하는 ESXi호스트에서만 사용자 인터페이스를 사용하여 NSX Manager 노드를 배포할 수 있습니다. NSX Manager 클러스터를 생성하려면 두 개의 추가 노드를 배포하여 총 3개 노드로 이루어진 클러스터를 구성합니다. UI에서 새 노드를 배포하면 노드가 처음 배포된 노드에 연결되어 클러스터를 구성합니다. 처음 배포된 노드의 모든 저장소 세부 정보 및 암호가 새로 배포된 노드와 동기화됩니다.

사전 요구 사항

- NSX Manager 노드가 설치되었는지 확인합니다.
- 계산 관리자가 구성되어 있는지 확인합니다.
- 필수 포트가 열려 있는지 확인합니다.
- ESXi 호스트에서 데이터스토어가 구성되었는지 확인합니다.
- 사용할 NSX Manager에 대한 IP 주소 및 게이트웨이, DNS 서버 IP 주소, 도메인 검색 목록 및 NTP 서버 IP 주소가 있는지 확인합니다.
- 대상 VM 포트 그룹 네트워크가 있는지 확인합니다. NSX 장치를 관리 VM 네트워크에 배치합니다.

절차

- 1 브라우저에서 `https://<manager-ip-address>`로 이동한 후 관리자 권한으로 NSX Manager에 로그인합니다.
- 2 장치를 배포하려면 **시스템 > 장치 > NSX 장치 추가**를 선택합니다.
- 3 장치 세부 정보를 입력합니다.

옵션	설명
호스트 이름	노드에 사용할 호스트 이름 또는 FQDN을 입력합니다.
관리 IP/넷마스크	노드에 할당할 IP 주소를 입력합니다.
관리 게이트웨이	노드에서 사용할 게이트웨이 IP 주소를 입력합니다.
DNS 서버	노드에서 사용할 DNS 서버 IP 주소 목록을 입력합니다.
NTP 서버	NTP 서버 IP 주소 목록을 입력합니다.
노드 크기	옵션에서 중형(6 vCPU, 24GB RAM, 300GB 스토리지) 폼 팩터를 선택합니다.

4 장치 구성 세부 정보를 입력합니다.

옵션	설명
계산 관리자	계산 관리자로 구성된 vCenter Server를 선택합니다.
계산 클러스터	노드가 가입해야 하는 클러스터를 선택합니다.
데이터스토어	노드 파일에 대한 데이터스토어를 선택합니다.
가상 디스크 형식	씬 프로비저닝 형식을 선택합니다.
네트워크	네트워크 선택 을 클릭하여 노드에 대한 관리 네트워크를 선택합니다.

5 액세스 및 자격 증명 세부 정보를 입력합니다.

옵션	설명
SSH 사용	버튼을 전환하여 새 노드에 대한 SSH 로그인을 허용합니다.
루트 액세스 사용	버튼을 전환하여 새 노드에 대한 루트 액세스를 허용합니다.
시스템 루트 자격 증명	새 노드에 대한 루트 암호를 설정하고 확인합니다. 암호는 암호 강도 제한을 준수해야 합니다. <ul style="list-style-type: none"> ■ 12자 이상. ■ 소문자 하나 이상. ■ 대문자 하나 이상. ■ 숫자 하나 이상. ■ 특수 문자 하나 이상. ■ 5개 이상의 다른 문자. ■ 기본 암호 복잡성 규칙은 Linux PAM 모듈에 의해 적용됩니다.
관리 CLI 자격 증명 및 감사 CLI 자격 증명	루트 암호와 동일 확인란을 선택하여 루트에 대해 구성된 것과 동일한 암호를 사용하거나 확인란을 선택 취소하고 다른 암호를 설정합니다.

6 장치 설치를 클릭합니다.

새 노드가 배포됩니다. **시스템 > 장치** 페이지에서 배포 프로세스를 추적할 수 있습니다. 설치가 완료되고 클러스터가 안정화될 때까지 다른 노드를 추가하지 마십시오.

7 배포, 클러스터 구성 및 저장소 동기화가 완료될 때까지 기다립니다.

가입 및 클러스터 안정화 프로세스는 10~15분 정도 걸릴 수 있습니다. 다른 클러스터 변경 작업을 수행하기 전에 모든 클러스터 서비스 그룹의 상태가 UP인지 확인합니다.

8 노드가 부팅되면 CLI에 관리자로 로그인하고 `get interface eth0` 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.9 클러스터에 노드가 두 개만 있는 경우 다른 장치를 추가합니다. **시스템 > 장치 > NSX 장치 추가**를 선택하고 구성 단계를 반복합니다.

라이선스 추가

NSX Manager를 사용하여 라이선스를 추가합니다.

사전 요구 사항

NSX 고급 라이선스 또는 더 상위의 라이선스를 얻습니다.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **시스템 > 라이선스 > 추가**를 선택합니다.
- 3 라이선스 키를 입력합니다.
- 4 **추가**를 클릭합니다.

계산 관리자 추가

계산 관리자는 호스트 및 가상 시스템과 같은 리소스를 관리하는 애플리케이션입니다. NSX와 연결된 vCenter Server를 NSX Manager에서 계산 관리자로 구성합니다.

자세한 내용은 "NSX 관리 가이드" 를 참조하십시오.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **시스템 > 패브릭 > 계산 관리자 > 추가**를 선택합니다.
- 3 계산 관리자 세부 정보를 입력합니다.

옵션	설명
이름 및 설명	vCenter Server의 이름 및 설명을 입력합니다.
유형	기본 유형은 VMware vCenter입니다.
다중 NSX	이 옵션은 선택되지 않은 상태로 둡니다. 다중 NSX 옵션을 사용하면 동일한 vCenter Server를 여러 NSX Manager에 등록할 수 있습니다. 감독자 및 vSphere Lifecycle Manager 클러스터에서는 이 옵션이 지원되지 않습니다.
FQDN 또는 IP 주소	vCenter Server의 FQDN 또는 IP 주소를 입력합니다.
역방향 프록시의 HTTPS 포트	기본 포트는 443입니다. 다른 포트를 사용하는 경우 포트가 모든 NSX Manager 장치에서 열려 있는지 확인합니다. NSX에서 계산 관리자를 등록하도록 역방향 프록시 포트를 설정합니다.
사용자 이름 및 암호	vCenter Server 로그인 자격 증명을 입력합니다.
SHA-256 지문	vCenter Server SHA-256 지문 알고리즘 값을 입력합니다.

다른 설정은 기본값을 그대로 유지할 수 있습니다.

지문 값을 비워 두면 서버에서 제공한 지문을 수락할지 묻는 메시지가 나타납니다. 지문을 수락한 후 NSX에서 vCenter 리소스를 찾아 등록하는 데 몇 초 정도 소요됩니다.

- 4 **신뢰 사용**을 선택하여 vCenter Server가 NSX와 통신하도록 허용합니다.
- 5 NSX Manager에 대한 지문 값을 제공하지 않으면 시스템에서 지문을 식별하여 표시합니다.

6 **추가**를 클릭하여 지문을 수락합니다.

결과

잠시 후에 계산 관리자가 vCenter Server에 등록되고 연결 상태가 접속 중으로 변경됩니다. vCenter Server의 FQDN/PNID가 변경되면 NSX Manager에 다시 등록해야 합니다. 자세한 내용은 [NSX Manager에 vCenter Server 등록](#)의 내용을 참조하십시오.

참고 vCenter Server 등록이 완료된 후 먼저 계산 관리자를 삭제하지 않은 상태에서 NSX Manager VM의 전원을 끄고 삭제하면 안 됩니다. 이 지침을 따르지 않으면 새 NSX Manager를 배포할 때 동일한 vCenter Server를 다시 등록할 수 없게 됩니다. vCenter Server가 이미 다른 NSX Manager에 등록되어 있다는 오류 메시지가 표시됩니다.

계산 관리자 이름을 클릭하여 세부 정보를 보거나, 계산 관리자를 편집하거나, 계산 관리자에 적용되는 태그를 관리할 수 있습니다.

전송 영역 생성

전송 영역은 특정 네트워크를 사용할 수 있는 호스트 및 VM을 나타냅니다. 전송 영역은 하나 이상의 호스트 클러스터에 걸쳐 있을 수 있습니다.

기본 전송 영역을 사용하거나 다음 영역을 생성합니다.

- NSX Advanced Load Balancer Controller와 서비스 엔진 간의 관리 네트워크 연결을 위해 감독자 제어부 VM에서 사용하는 오버레이 전송 영역.
- 물리적 네트워크에 대한 업링크에 사용할 NSX Edge 노드의 VLAN 전송 영역.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **시스템 > 패브릭 > 전송 영역 > 전송 영역 추가**를 선택합니다.
- 3 전송 영역의 이름과 필요한 경우 설명을 입력합니다. 예: **overlayTZ**.
- 4 **오버레이** 트래픽 유형을 선택합니다.

기본적으로 다음 전송 영역이 존재합니다.

- 이름이 `nsx-vlan-transportzone`인 VLAN 전송 영역
- 이름이 `nsx-overlay-transportzone`인 오버레이 전송 영역

- 5 **저장**을 클릭합니다.
- 6 2~5단계를 반복하여 이름이 **vlanTZ**이고 트래픽 유형이 **VLAN**인 전송 영역을 생성합니다.
- 7 (선택 사항) 하나 이상의 업링크 팀 구성 정책 이름을 입력합니다.

전송 영역에 연결된 세그먼트는 이러한 명명된 팀 구성 정책을 사용합니다. 세그먼트에서 일치하는 명명된 팀 구성 정책을 찾지 못하면 기본 업링크 팀 구성 정책이 사용됩니다.

결과

생성한 전송 영역이 **전송 영역** 페이지에 표시됩니다.

호스트 터널 끝점 IP 주소에 대한 IP 풀 생성

ESXi 호스트 TEP(터널 끝점)에 대한 IP 풀을 생성합니다. TEP는 외부 IP 헤더에 사용되는 소스 및 대상 IP 주소로, 오버레이 프레임의 NSX 캡슐화를 시작하고 종료하는 ESXi 호스트를 식별합니다.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **네트워킹 > IP 주소 풀 > IP 주소 풀 추가**를 선택합니다.
- 3 IP 주소 풀의 이름과 설명(선택 사항)을 입력합니다. 예: `ESXI-TEP-IP-POOL`
- 4 **설정**을 클릭합니다.
- 5 **서브넷 추가** 드롭다운 메뉴에서 **IP 범위**를 선택합니다.
- 6 다음 IP 주소 풀 세부 정보를 입력합니다.

옵션	설명
IP 범위	IP 할당 범위를 입력합니다. 예를 들어 IPv4 Range - 192.168.12.1-192.168.12.60, IPv6 Range - 2001:800::0001-2001:0fff:ffff:ffff:ffff:ffff:ffff:ffff입니다.
CIDR	CIDR 표기법으로 네트워크 주소를 입력합니다. 예: 192.23.213.0/24

- 7 필요한 경우 다음과 같은 세부 정보를 입력합니다.

옵션	설명
설명	IP 범위에 대한 설명을 입력합니다.
게이트웨이 IP	게이트웨이 IP 주소를 입력합니다. 예: 192.23.213.253
DNS 서버	DNS 서버 주소를 입력합니다.
DNS 접미사	DNS 접미사를 입력합니다.

- 8 **추가 및 적용**을 클릭합니다.
- 9 **저장**을 클릭합니다.

결과

생성한 TEP IP 풀이 [IP 풀] 페이지에 나열되어 있는지 확인합니다.

Edge 노드에 대한 IP 풀 생성

Edge 노드에 대한 IP 풀을 생성합니다. TEP 주소를 라우팅할 필요는 없습니다. Edge TEP가 호스트 TEP와 통신할 수 있도록 하는 IP 주소 지정 체계를 사용할 수 있습니다.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **네트워킹 > IP 주소 풀 > IP 주소 풀 추가**를 선택합니다.
- 3 IP 주소 풀의 이름과 설명(선택 사항)을 입력합니다. 예: **EDGE-TEP-IP-POOL**.
- 4 **설정**을 클릭합니다.
- 5 다음 IP 주소 풀 세부 정보를 입력합니다.

옵션	설명
IP 범위	IP 할당 범위를 입력합니다. 예를 들어 IPv4 Range - 192.168.12.1-192.168.12.60, IPv6 Range - 2001:800::2001-2001:0fff:ffff:ffff:ffff:ffff:ffff:ffff입니다.
CIDR	CIDR 표기법으로 네트워크 주소를 입력합니다. 예: 192.23.213.0/24

- 6 필요한 경우 다음과 같은 세부 정보를 입력합니다.

옵션	설명
설명	IP 범위에 대한 설명을 입력합니다.
게이트웨이 IP	게이트웨이 IP 주소를 입력합니다. 예: 192.23.213.253
DNS 서버	DNS 서버 주소를 입력합니다.
DNS 접미사	DNS 접미사를 입력합니다.

- 7 **추가 및 적용**을 클릭합니다.
- 8 **저장**을 클릭합니다.

결과

생성한 IP 풀이 [IP 풀] 페이지에 나열되어 있는지 확인합니다.

ESXi 호스트 업링크 프로파일 생성

호스트 업링크 프로파일은 ESXi 호스트에서 NSX 세그먼트까지의 업링크에 대한 정책을 정의합니다.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **시스템 > 패브릭 > 프로파일 > 업링크 프로파일 > 프로파일 추가**를 선택합니다.

- 업링크 프로파일 이름을 입력하고 필요한 경우 업링크 프로파일 설명을 입력합니다.

예: **ESXI-UPLINK-PROFILE**.

- 팀 구성** 섹션에서 **추가**를 클릭하여 팀 구성 정책의 이름을 추가하고 **FAILOVER_ORDER** 정책을 구성합니다.

활성 업링크 목록이 지정되고 전송 노드의 각 인터페이스가 하나의 활성 업링크에 고정됩니다. 이 구성을 사용하면 여러 활성 업링크를 동시에 사용할 수 있습니다.

- 활성 및 대기 링크를 구성합니다.

예를 들어 **uplink-1**을 활성 업링크로 구성하고 **uplink-2**를 대기 업링크로 구성합니다.

- (선택 사항) 전송 VLAN 값을 입력합니다. 예: **1060**.

업링크 프로파일에 설정된 전송 VLAN은 오버레이 트래픽에 태그를 지정하고 VLAN ID는 터널 끝점(TEP)에서 사용됩니다.

- MTU 값을 입력합니다. 값은 1600 이상이어야 하지만 물리적 스위치 및 vSphere Distributed Switch의 MTU 값보다 높아서는 안 됩니다.

NSX는 글로벌 기본 MTU 값 1700을 사용합니다.

결과

업링크 프로파일 페이지에서 업링크를 봅니다.

NSX Edge 업링크 프로파일 생성

업링크는 NSX Edge 노드에서 NSX 논리적 스위치로의 링크입니다. 업링크 프로파일은 팀 구성 정책, 활성 및 대기 링크, 전송 VLAN ID 및 MTU 값을 설정하여 업링크에 대한 정책을 정의합니다.

Edge 가상 시스템 오버레이 트래픽에 대해 하나의 활성 업링크가 있는 페일오버 순서 팀 구성 정책으로 업링크 프로파일을 생성합니다.

절차

- NSX Manager에 로그인합니다.

- 시스템 > 패브릭 > 프로파일 > 업링크 프로파일 > 프로파일 추가 > 를 선택합니다..**

- 업링크 프로파일 이름을 입력하고 필요한 경우 업링크 프로파일 설명을 입력합니다.

예: **EDGE-UPLINK-PROFILE**.

- 팀 구성** 섹션에서 **추가**를 클릭하여 팀 구성 정책의 이름을 추가하고 **FAILOVER_ORDER** 정책을 구성합니다.

활성 업링크 목록이 지정되고 전송 노드의 각 인터페이스가 하나의 활성 업링크에 고정됩니다. 이 구성을 사용하면 여러 활성 업링크를 동시에 사용할 수 있습니다.

- 활성 업링크를 구성합니다.

예를 들어 **uplink-1**을 활성 업링크로 구성합니다.

결과

업링크 프로파일 페이지에서 업링크를 봅니다.

전송 노드 프로파일 생성

전송 노드 프로파일은 프로파일이 연결된 특정 클러스터의 호스트에서 NSX가 설치되고 구성되는 방법을 정의합니다. ESXi 클러스터를 전송 노드로 준비하기 전에 전송 노드 프로파일을 생성합니다.

참고 전송 노드 프로파일은 호스트에만 적용됩니다. NSX Edge 전송 노드에는 적용할 수 없습니다.

사전 요구 사항

- 클러스터를 사용할 수 있는지 확인합니다. **NSX Manager 노드**를 배포하여 클러스터 구성의 내용을 참조하십시오.
- 오버레이 전송 영역을 생성합니다. **전송 영역 생성**의 내용을 참조하십시오.
- IP 풀을 구성합니다. **호스트 터널 끝점 IP 주소에 대한 IP 풀 생성**의 내용을 참조하십시오.
- 계산 관리자를 추가합니다. **계산 관리자 추가**의 내용을 참조하십시오.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **시스템 > 패브릭 > 호스트**를 선택합니다.
- 3 **호스트** 페이지에서 **전송 노드 프로파일 > 전송 노드 프로파일 추가**를 선택합니다.
- 4 전송 노드 프로파일을 식별하는 이름을 입력합니다. 예: **HOST-TRANSPORT-NODE-PROFILE**.
필요한 경우 전송 노드 프로파일에 대한 설명을 추가합니다.
- 5 **호스트 스위치** 필드에서 **설정**을 선택합니다.
- 6 **호스트 스위치** 창에서 스위치 세부 정보를 입력합니다.

옵션	설명
vCenter	vCenter Server를 선택합니다.
유형	호스트에 구성될 스위치 유형을 선택합니다. VDS 를 선택합니다.
VDS	선택한 vCenter Server 아래에 생성된 VDS를 선택합니다. 예: wcp_vds_1 .
전송 영역	이전에 생성된 오버레이 전송 영역을 선택합니다. 예: overlayTZ .
업링크 프로파일	이전에 생성된 호스트 업링크 프로파일을 선택합니다. 예: ESXI-UPLINK-PROFILE .
IP 주소 유형	IPv4 를 선택합니다.
IPv4 할당	IP 풀 사용 을 선택합니다.

옵션	설명
IPv4 풀	이전에 생성된 호스트 TEP 풀을 선택합니다. 예: ESXI-TEP-IP-POOL .
팀 구성 정책 업링크 매핑	추가를 클릭하고 NSX 업링크 프로파일에 정의된 업링크를 vSphere Distributed Switch 업링크에 매핑합니다. 예를 들어 uplink-1 을 Uplink 1 에 매핑하고 uplink-2 를 Uplink 2 에 매핑합니다.

7 **추가 및 적용**을 클릭합니다.

8 **저장**을 클릭하여 구성을 저장합니다.

결과

생성한 프로파일이 **전송 노드 프로파일** 페이지에 나열됩니다.

NSX Edge 클러스터 프로파일 생성

NSX Edge 전송 노드에 대한 정책을 정의하는 NSX Edge 클러스터 프로파일을 생성합니다.

사전 요구 사항

NSX Edge 클러스터를 사용할 수 있는지 확인합니다.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **시스템 > 패브릭 > 프로파일 > Edge 클러스터 프로파일 > 프로파일 추가 >** 를 선택합니다..
- 3 NSX Edge 클러스터 프로파일 세부 정보를 입력합니다.
- 4 NSX Edge 클러스터 프로파일 이름을 입력합니다. 예: **Cluster Profile - 1**.
설명(선택 사항)을 입력합니다.
- 5 다른 설정은 기본값을 그대로 둡니다.
- 6 **추가**를 클릭합니다.

클러스터에서 NSX 구성

NSX를 설치하고 오버레이 TEP를 준비하려면 vSphere 클러스터에 전송 노드 프로파일을 적용합니다.

사전 요구 사항

전송 노드 프로파일을 생성했는지 확인합니다.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **시스템 > 패브릭 > 노드 > 호스트 전송 노드**를 선택합니다.

3 **관리자** 드롭다운 메뉴에서 기존 vCenter Server를 선택합니다.

페이지에 사용 가능한 vSphere 클러스터가 나열됩니다.

4 NSX를 구성하려는 계산 클러스터를 선택합니다.

5 **NSX 구성**을 클릭합니다.

6 이전에 생성한 전송 노드 프로파일을 선택하고 **적용**을 클릭합니다.

예: HOST-TRANSPORT-NODE-PROFILE

7 **호스트 전송 노드** 페이지에서 NSX 구성 상태가 `Success`이고 클러스터에 있는 호스트의 NSX Manager 연결 상태가 `Up`인지 확인합니다.

결과

이전에 생성된 전송 노드 프로파일이 vSphere 클러스터에 적용되어 NSX를 설치하고 오버레이 TEP를 준비합니다.

NSX Edge 전송 노드 생성

NSX Edge VM(가상 시스템)을 NSX 패브릭에 추가하고 이를 NSX Edge 전송 노드 VM으로 구성할 수 있습니다.

사전 요구 사항

전송 영역, Edge 업링크 프로파일 및 Edge TEP IP 풀을 생성했는지 확인합니다.

절차

1 NSX Manager에 로그인합니다.

2 **시스템 > 패브릭 > 노드 > Edge 전송 노드 > Edge 노드 추가**를 선택합니다.

3 **이름 및 설명**에 NSX Edge 노드의 이름을 입력합니다.

예를 들어 `nsx-edge-1`입니다.

4 vCenter Server의 호스트 이름이나 FQDN을 입력합니다.

예: `nsx-edge-1.lab.com`

5 NSX Edge VM 장치에 대한 폼 팩터를 선택합니다.

6 **자격 증명**에서 NSX Edge에 대한 루트 암호 및 CLI를 입력합니다. 암호는 암호 강도 제한을 준수 해야 합니다.

- 12자 이상.
- 소문자 하나 이상.
- 대문자 하나 이상.
- 숫자 하나 이상.
- 특수 문자 하나 이상.

- 5개 이상의 다른 문자.
- 기본 암호 복잡성 규칙은 Linux PAM 모듈에 의해 적용됩니다.

7 CLI 및 루트 자격 증명에 대해 **SSH 로그인 허용**을 사용하도록 설정합니다.

8 **배포 구성**에서 다음 속성을 구성합니다.

옵션	설명
계산 관리자	드롭다운 메뉴에서 계산 관리자를 선택합니다. 예를 들어 vCenter를 선택합니다.
클러스터	드롭다운 메뉴에서 클러스터를 선택합니다. 예를 들어 Compute-Cluster를 선택합니다.
데이터스토어	목록에서 공유 데이터스토어를 선택합니다. 예: vsanDatastore

9 노드 설정을 구성합니다.

옵션	설명
IP 할당	[정적]을 선택합니다. 다음에 대한 값을 입력합니다. <ul style="list-style-type: none"> ■ 관리 IP: vCenter Server 관리 네트워크와 동일한 VLAN의 IP 주소를 입력합니다. 예: 10.197.79.146/24 ■ 기본 게이트웨이: 관리 네트워크의 기본 게이트웨이입니다. 예: 10.197.79.253
관리 인터페이스	인터페이스 선택 을 클릭하고 드롭다운 메뉴에서 이전에 생성한 관리 네트워크와 동일한 VLAN에 있는 vSphere Distributed Switch 포트 그룹을 선택합니다. 예: DPortGroup-MGMT

10 **NSX 구성**에서 **스위치 추가**를 클릭하여 스위치 속성을 구성합니다.

11 **Edge 스위치 이름**의 기본 이름을 사용합니다.

예: nvds1

12 전송 노드가 속하는 전송 영역을 선택합니다.

이전에 생성된 오버레이 전송 영역을 선택합니다.

예: overlayTZ

13 이전에 생성된 Edge 업링크 프로파일을 선택합니다.

예: EDGE-UPLINK-PROFILE

14 **IP 할당**에서 **IP 풀 사용**을 선택합니다.

15 이전에 생성된 Edge TEP IP 풀을 선택합니다.

예: EDGE-TEP-IP-POOL

16 **팀 구성 정책 스위치 매핑** 섹션에서 업링크를 이전에 생성된 Edge 업링크 프로파일에 매핑합니다.

예를 들어 Uplink1의 경우 uplink-1를 선택합니다.

17 10-16단계를 반복하여 새 스위치를 추가합니다.

예를 들어 다음 값을 구성합니다.

속성	값
Edge 스위치 이름	nvds2
전송 영역	vlanTZ
Edge 업링크 프로파일	EDGE-UPLINK-PROFILE
팀 구성 정책 스위치 매핑	DPortGroup-EDGE-UPLINK

18 **마침**을 클릭합니다.

19 두 번째 NSX Edge VM에 대해 2-18단계를 반복합니다.

20 **Edge 전송 노드** 페이지에서 연결 상태를 확인합니다.

NSX Edge 클러스터 생성

하나 이상의 NSX Edge를 항상 사용할 수 있도록 하려면 NSX Edge 클러스터를 생성합니다.

절차

1 NSX Manager에 로그인합니다.

2 **시스템 > 패브릭 > 노드 > Edge 클러스터 > 추가**를 선택합니다.

3 NSX Edge 클러스터 이름을 입력합니다.

예: EDGECLUSTER1

4 **저장**을 클릭합니다.

5 드롭다운 메뉴에서 생성한 NSX Edge 클러스터 프로파일을 선택합니다. 예: **Cluster Profile - 1**.

6 **멤버 유형** 드롭다운 메뉴에서 **Edge 노드**를 선택합니다.

7 **사용 가능** 열에서 이전에 생성된 NSX Edge VM을 선택하고 오른쪽 화살표를 클릭하여 **선택됨** 열로 VM을 이동합니다.

8 예를 들어 nsx-edge-1 및 nsx-edge-2를 선택합니다.

9 **저장**을 클릭합니다.

다음에 수행할 작업

Tier-0 게이트웨이 생성

Tier-0 게이트웨이는 NSX 논리적 네트워킹에 대한 North-South 연결을 물리적 인프라에 제공하는 NSX 논리적 라우터입니다. vSphere IaaS control plane는 동일한 전송 영역에 있는 여러 NSX Edge 클러스터에서 여러 개의 Tier-0 게이트웨이를 지원합니다.

Edge Tier-0 라우터에서 NSX 경로 맵을 구성하는 방법에 대한 자세한 내용은 <https://docs.vmware.com/kr/VMware-Cloud-Foundation/4.0/vcf-40-doc.zip>에서 "VMware Cloud Foundation 운영 및 관리 가이드"를 참조하십시오.

사전 요구 사항

NSX Edge 클러스터를 생성했는지 확인합니다.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **네트워킹 > Tier-0 게이트웨이**를 선택합니다.
- 3 **게이트웨이 추가**를 클릭합니다.
- 4 Tier-0 게이트웨이의 이름을 입력합니다.

예: ContainerT0

- 5 **활성-대기 HA** 모드를 선택합니다.

기본 모드는 **액티브-액티브**입니다. **활성-대기** 모드에서는 선택된 활성 멤버가 모든 트래픽을 처리합니다. 활성 멤버가 실패하면 새 멤버가 활성 상태로 선택됩니다.

- 6 HA 모드가 **액티브-대기**인 경우 **페일오버** 모드를 선택합니다.

옵션	설명
선점	기본 노드가 실패했다가 복구되면 피어가 선점되어 활성 노드가 됩니다. 피어의 상태는 대기로 변경됩니다.
비선점	기본 노드가 실패했다가 복구되면 피어가 활성 노드인지 확인합니다. 활성 노드이면 기본 노드는 피어를 선점하지 않으며 대기 노드가 됩니다.

- 7 이전에 생성한 NSX Edge 클러스터를 선택합니다.

예를 들어 `Cluster Profile - 1`를 선택합니다.

- 8 **저장**을 클릭합니다.

Tier-0 게이트웨이가 생성됩니다.

- 9 **예**를 선택하여 구성을 계속합니다.

- 10 인터페이스를 구성합니다.

a **인터페이스**를 확장하고 **설정**을 클릭합니다.

b **인터페이스 추가**를 클릭합니다.

- c 이름을 입력하십시오.
예를 들어 이름 `TIER-0_VWT-UPLINK1`을 입력합니다.
 - d **유형**을 **외부**로 선택합니다.
 - e Edge 논리적 라우터 - 업링크 VLAN에서 IP 주소를 입력합니다. IP 주소는 이전에 생성된 NSX Edge VM에 대해 구성된 관리 IP 주소와 달라야 합니다.
예: `10.197.154.1/24`
 - f **연결 대상**에서 이전에 생성된 Tier-0 업링크 세그먼트를 선택합니다.
예를 들어 `TIER-0-LS-UPLINK`입니다.
 - g 목록에서 NSX Edge 노드를 선택합니다.
예: `nsx-edge-1`
 - h **저장**을 클릭합니다.
 - i 두 번째 인터페이스에 대해 a - h 단계를 반복합니다.
예를 들어 `nsx-edge-2` Edge 노드에 연결된 IP 주소가 `10.197.154.2/24`인 두 번째 업링크 `TIER-0_VWT-UPLINK2`를 생성합니다.
 - j **닫기**를 클릭합니다.
- 11 고가용성을 구성하려면 **HA VIP 구성**에서 **설정**을 클릭합니다.
- a **HA VIP 구성 추가**를 클릭합니다.
 - b IP 주소를 입력합니다.
예를 들어 `10.197.154.3/24`입니다.
 - c 인터페이스를 선택합니다.
예를 들어 `TIER-0_VWT-UPLINK1` 및 `TIER-0_VWT-UPLINK2`를 선택합니다.
 - d **추가 및 적용**을 클릭합니다.
- 12 라우팅을 구성하려면 **라우팅**을 클릭합니다.
- a 정적 경로에서 **설정**을 클릭합니다.
 - b **정적 경로 추가**를 클릭합니다.
 - c 이름을 입력하십시오.
예: `DEFAULT-STATIC-ROUTE`
 - d 네트워크 IP 주소로 `0.0.0.0/0`을 입력합니다.
 - e 다음 홉을 구성하려면 **다음 홉 설정**을 클릭한 후 **다음 홉 추가**를 클릭합니다.

- f 다음 홉 라우터의 IP 주소를 입력합니다. 일반적으로 이것은 NSX Edge 논리적 라우터 업링크 VLAN에서 관리 네트워크 VLAN의 기본 게이트웨이입니다.

예: 10.197.154.253

- g **추가** 및 **적용**을 클릭하고 **저장**을 클릭합니다.

- h **닫기**를 클릭합니다.

13 (선택 사항) BGP를 선택하여 BGP 로컬 및 피어 세부 정보를 구성합니다.

14 연결을 확인하려면 물리적 아키텍처의 외부 디바이스에서 사용자가 구성한 업링크를 ping할 수 있는지 확인합니다.

Edge Tier-0 게이트웨이에서 NSX 경로 맵 구성

vSphere IaaS control plane를 배포할 때 eBGP 모드의 Edge Tier-0 게이트웨이에 생성된 경로 맵에는 거부 규칙만 있는 IP 접두사가 포함됩니다. 이렇게 하면 경로가 ToR 스위치에 보급되지 않습니다.

Kubernetes - 워크로드 관리에만 Edge 클러스터를 사용하는 경우 옵션 1을 따르고 Tier-1 경로 보급을 비활성화합니다. 추가 작업에 Edge 클러스터를 사용하는 경우 옵션 2에 따라 새 허용 규칙을 생성합니다.

옵션 1: Tier-0 게이트웨이를 통해 Tier-1 연결된 네트워크의 보급 비활성화

Tier-1 게이트웨이에 연결된 네트워크는 Tier-0 게이트웨이에서 외부 네트워크로 보급되지 않습니다.

- 1 NSX Manager에 로그인합니다.
- 2 **네트워킹 > Tier-0 게이트웨이**를 선택합니다.
- 3 **편집**을 클릭합니다.
- 4 [보급된 Tier-1 서브넷] 섹션에서 **연결된 인터페이스 및 세그먼트**를 선택 취소합니다.
- 5 **적용** 및 **저장**을 차례로 클릭합니다.

옵션 2: 새 허용 규칙을 생성하여 경로 재배포에 적용

vSphere IaaS control plane를 배포하면 새 거부 규칙이 경로 맵에 추가됩니다. 따라서 IP 접두사 목록 및 경로 맵을 허용하도록 경로 맵에 새 허용 규칙을 추가하여 경로 재배포 규칙에 마지막 규칙으로 적용해야 합니다.

- 1 NSX Manager에 로그인합니다.
- 2 **네트워킹 > Tier-0 게이트웨이**를 선택합니다.
- 3 새 IP 접두사 목록을 생성합니다.
 - a **라우팅**을 확장합니다.
 - b [IP 접두사 목록] 옆에 있는 1을 클릭합니다.
 - c [IP 접두사 목록 설정] 대화상자에서 **IP 접두사 목록 추가**를 클릭합니다.
 - d 이름(예: **test**)을 입력하고 **설정**을 클릭합니다.
 - e **접두사 추가**를 클릭합니다.

- f 네트워크에서 **임의**를 클릭하고 [작업]에서 **허용**을 선택합니다.
 - g **적용 및 저장**을 차례로 클릭합니다.
- 4 3단계에서 생성된 IP 접두사 목록에 대한 경로 맵을 생성합니다.
- a [경로 맵] 옆에 있는 **설정**을 클릭합니다.
 - b **경로 맵 추가**를 클릭합니다
 - c IP 접두사로 일치 조건을 새로 추가합니다.
 - d 3단계에서 생성된 IP 접두사 및 작업 **허용**을 선택합니다.
 - e **적용 및 저장**을 차례로 클릭합니다.
- 5 경로 재배포를 위해 편집된 경로 맵을 적용합니다.
- a **Tier-0 게이트웨이** 페이지에서 **경로 재배포**를 확장하고 [편집]을 클릭합니다.
 - b [경로 맵] 열의 드롭다운 메뉴에서 4단계에서 생성한 경로 맵을 선택합니다.
 - c **적용 및 저장**을 차례로 클릭합니다.

Tier-1 게이트웨이 생성

Tier-1 게이트웨이는 일반적으로 노스바운드 방향으로 Tier-0 게이트웨이에 그리고 사우스바운드 방향으로 세그먼트에 연결됩니다.

사전 요구 사항

Tier-0 게이트웨이를 생성했는지 확인합니다.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **네트워킹 > Tier-1 게이트웨이**를 선택합니다.
- 3 **Tier-1 게이트웨이 추가**를 클릭합니다.
- 4 게이트웨이의 이름을 입력합니다. 예: **ContainerAviT1**
- 5 이 Tier-1 게이트웨이에 연결할 Tier-0 게이트웨이를 선택합니다. 예: **ContainerT0**.
- 6 NSX Edge 클러스터를 선택합니다. 예를 들어 **EDGECLUSTER1**을 선택합니다.
- 7 NSX Edge 클러스터를 선택하면 NSX Edge 노드를 선택할 수 있는 옵션으로 전환됩니다.
- 8 페일오버 모드를 선택하거나 기본 옵션인 **비선점**을 수락합니다.
- 9 나머지 설정에 대해서는 기본 옵션을 수락합니다.
- 10 **저장**을 클릭합니다.
- 11 (선택 사항) 서비스 인터페이스, 정적 경로 및 멀티캐스트 설정을 구성합니다. 기본값을 수락할 수 있습니다.

Tier-0 업링크 세그먼트 및 오버레이 세그먼트 생성

Tier-0 업링크 세그먼트는 NSX의 North-South 연결을 물리적 인프라에 제공합니다. 오버레이 세그먼트는 서비스 엔진 관리 NIC에 IP 주소를 제공합니다.

사전 요구 사항

Tier-0 게이트웨이를 생성했는지 확인합니다.

절차

- 1 NSX Manager에 로그인합니다.
- 2 **네트워킹 > 세그먼트 > 세그먼트 추가**를 선택합니다.
- 3 세그먼트의 이름을 입력합니다.
예: TIER-0-LS-UPLINK
- 4 이전에 생성한 전송 영역을 선택합니다.
예를 들어 `vlanTZ`를 선택합니다.
- 5 **관리 상태**를 전환하여 사용하도록 설정합니다.
- 6 Tier-0 게이트웨이의 VLAN ID를 입력합니다.
예: 1089
- 7 **저장**을 클릭합니다.
- 8 2-7단계를 반복하여 전송 영역 `nsx-overlay-transportzone`이 포함된 오버레이 세그먼트 `nsxoverlaysegment`를 생성합니다.

NSX을 사용하여 vSphere IaaS control plane용 NSX Advanced Load Balancer 설치 및 구성

vSphere IaaS control plane 환경에서 NSX 4.1.1 이상 버전을 사용하는 경우 NSX Advanced Load Balancer 22.1.4 이상 버전을 설치하고 구성할 수 있습니다.

- 환경이 NSX Advanced Load Balancer로 vSphere IaaS control plane를 구성하기 위한 요구 사항을 충족하는지 확인합니다. "vSphere IaaS 제어부 개념 및 계획"에서 [NSX 및 NSX Advanced Load Balancer가 있는 영역 감독자 요구 사항](#) 및 [NSX 및 NSX Advanced Load Balancer를 사용한 클러스터 감독자 배포 요구 사항](#)을 참조하십시오.
- NSX를 설치 및 구성합니다.

- NSX Advanced Load Balancer OVA를 다운로드합니다. VMware는 워크로드 관리를 사용하도록 설정할 vSphere 환경에 배포하는 NSX Advanced Load Balancer OVA 파일을 제공합니다. [VMware Customer Connect](#) 포털에서 vSphere IaaS control plane에서 지원되는 최신 버전의 OVA 파일을 다운로드합니다.

참고 이 가이드의 절차는 vSphere IaaS control plane 8.0 업데이트 2에서 지원되는 NSX Advanced Load Balancer와 관련되어 있습니다. 사용 가능한 최신 버전의 NSX Advanced Load Balancer가 있을 수 있으며 UI 워크플로가 다를 수 있습니다.

NSX Advanced Load Balancer에 대한 자세한 내용은 [VMware NSX Advanced Load Balancer 설명서](#)를 참조하십시오.

NSX Advanced Load Balancer OVA를 로컬 콘텐츠 라이브러리로 가져오기

NSX Advanced Load Balancer OVA 이미지를 저장하려면 로컬 콘텐츠 라이브러리를 생성하고 여기에 OVA를 가져옵니다.

로컬 콘텐츠 라이브러리를 생성하려면 라이브러리를 구성하고 OVA 파일을 다운로드하여 로컬 콘텐츠 라이브러리로 가져와야 합니다. 자세한 내용은 [콘텐츠 라이브러리 사용](#)을 참조하십시오.

사전 요구 사항

NSX Advanced Load Balancer OVA를 다운로드했는지 확인합니다.

로컬 콘텐츠 라이브러리를 생성합니다. [콘텐츠 라이브러리 생성 및 편집](#)을 참조하십시오.

절차

- 1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.
- 2 **메뉴 > 콘텐츠 라이브러리**를 선택합니다.
- 3 **콘텐츠 라이브러리** 목록에서 직접 생성한 로컬 콘텐츠 라이브러리의 이름 링크를 클릭합니다. 예: **NSX ALB**.
- 4 **작업**을 클릭합니다.
- 5 **항목 가져오기**를 선택합니다.
- 6 **라이브러리 항목 가져오기** 창에서 **로컬 파일**을 선택합니다.
- 7 **파일 업로드**를 클릭합니다.
- 8 다운로드한 OVA 파일을 선택합니다.
- 9 **가져오기**를 클릭합니다.
- 10 페이지 하단의 **최근 작업** 창을 나타냅니다.
- 11 **라이브러리 항목의 콘텐츠 가져오기** 작업을 모니터링하고 성공적으로 완료되었는지 확인합니다.

다음에 수행할 작업

NSX Advanced Load Balancer 컨트롤러를 배포합니다. [NSX Advanced Load Balancer 컨트롤러 배포](#)의 내용을 참조하십시오.

NSX Advanced Load Balancer Controller 배포

vSphere IaaS control plane 환경의 관리 네트워크에 NSX Advanced Load Balancer Controller VM을 배포합니다.

사전 요구 사항

- NSX Advanced Load Balancer를 배포할 관리 네트워크가 있는지 확인합니다. vDS(vSphere Distributed Switch) 또는 vSS(vSphere Standard Switch)일 수 있습니다.
- 데이터 네트워크를 위한 vDS 스위치 및 포트 그룹을 생성했는지 확인합니다. NSX Advanced Load Balancer와 함께 사용할 감독자용 vSphere Distributed Switch 생성의 내용을 참조하십시오.
- 사전 요구 사항을 완료했는지 확인합니다. "vSphere IaaS 제어부 개념 및 계획" 에서 NSX 및 NSX Advanced Load Balancer가 있는 영역 감독자 요구 사항 및 NSX 및 NSX Advanced Load Balancer를 사용한 클러스터 감독자 배포 요구 사항을 참조하십시오.

절차

- 1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.
- 2 관리 구성 요소용으로 지정된 vSphere 클러스터를 선택합니다.
- 3 **AVI-LB**라는 리소스 풀을 생성합니다.
- 4 리소스 풀을 마우스 오른쪽 버튼으로 클릭하고 **OVF 템플릿 배포**를 선택합니다.
- 5 **로컬 파일**을 선택하고 **파일 업로드**를 클릭합니다.
- 6 사전 요구 사항으로 다운로드한 `controller-VERSION.ova` 파일을 찾아서 선택합니다.
- 7 이름을 입력하고 컨트롤러의 폴더를 선택합니다.

옵션	설명
가상 시스템 이름	<code>avi-controller-1</code>
가상 시스템 위치	데이터 센터

- 8 **AVI-LB** 리소스 풀을 계산 리소스로 선택합니다.
- 9 구성 세부 정보를 검토하고 **다음**을 클릭합니다.
- 10 **VM 스토리지 정책**(예: `vsanDatastore`)을 선택합니다.
- 11 관리 네트워크(예: `network-1`)를 선택합니다.
- 12 다음과 같이 구성을 사용자 지정하고 완료되면 **다음**을 클릭합니다.

옵션	설명
관리 인터페이스 IP 주소	컨트롤러 VM의 IP 주소(예: <code>10.199.17.51</code>)를 입력합니다.
관리 인터페이스 서브넷 마스크	서브넷 마스크(예: <code>255.255.255.0</code>)를 입력합니다.
기본 게이트웨이	관리 네트워크의 기본 게이트웨이(예: <code>10.199.17.235</code>)를 입력합니다.

옵션	설명
Sysadmin 로그인 인증 키	필요한 경우 공용 키의 콘텐츠를 붙여넣습니다. 키를 비워 둘 수 있습니다.
Avi 컨트롤러의 호스트 이름	컨트롤러의 FQDN 또는 IP 주소를 입력합니다.

13 배포 설정을 검토합니다.

14 **마침**을 클릭하여 구성을 완료합니다.

15 vSphere Client를 사용하여 **작업** 패널에서 컨트롤러 VM의 프로비저닝을 모니터링합니다.

16 vSphere Client를 사용하여 컨트롤러 VM을 배포한 후 전원을 켭니다.

컨트롤러 클러스터 배포

필요한 경우 3개의 컨트롤러 노드로 구성된 클러스터를 배포할 수 있습니다. 운영 환경에서는 HA 및 재해 복구를 위해 클러스터를 구성하는 것이 좋습니다. 단일 노드 NSX Advanced Load Balancer 컨트롤러를 실행하는 경우 백업 및 복원 기능을 사용해야 합니다.

3노드 클러스터를 실행하려면 첫 번째 컨트롤러 VM을 배포한 후 두 개의 추가 컨트롤러 VM을 배포하고 전원을 켭니다. 초기 구성 마법사를 실행하거나 이러한 컨트롤러에 대한 관리자 암호를 변경하면 안 됩니다. 첫 번째 컨트롤러 VM의 구성이 두 개의 새 컨트롤러 VM에 할당됩니다.

절차

1 **관리 > 컨트롤러**로 이동합니다.

2 **노드**를 선택합니다.

3 편집 아이콘을 클릭합니다.

4 **컨트롤러 클러스터 IP**에 대한 고정 IP를 추가합니다.

이 IP 주소는 관리 네트워크의 IP 주소여야 합니다.

5 **클러스터 노드**에서 두 개의 새 클러스터 노드를 구성합니다.

옵션	설명
IP	컨트롤러 노드의 IP 주소입니다.
이름	노드의 이름입니다. 이 이름은 IP 주소일 수 있습니다.
암호	컨트롤러 노드의 암호입니다. 암호는 비워 둡니다.
공용 IP	컨트롤러 노드의 공용 IP 주소입니다. 비워 둡니다.

6 **저장**을 클릭합니다.

참고 클러스터를 배포한 후에는 추가 구성에 컨트롤러 노드 IP가 아닌 컨트롤러 클러스터 IP를 사용해야 합니다.

컨트롤러 전원 켜기

컨트롤러 VM을 배포한 후 전원을 켤 수 있습니다. 부팅 프로세스 동안 배포 중에 지정된 IP 주소가 VM에 할당됩니다.

전원을 켜 후 컨트롤러 VM의 첫 번째 부팅 프로세스에 최대 10분이 소요될 수 있습니다.

사전 요구 사항

컨트롤러를 배포합니다.

절차

- 1 vCenter Server에서, 배포한 `avi-controller-1` VM을 마우스 오른쪽 버튼으로 클릭합니다.
- 2 **전원 > 전원 켜기**를 선택합니다.
배포 중에 지정한 IP 주소가 VM에 할당됩니다.
- 3 VM의 전원이 켜져 있는지 확인하기 위해 브라우저에서 IP 주소에 액세스합니다.
VM이 온라인 상태가 되면 TLS 인증서 및 연결에 대한 주의가 표시됩니다.
- 4 **연결이 비공개가 아닙니다**. 주의에서 **세부 정보 표시**를 클릭합니다.
- 5 창이 나타나면 **이 웹 사이트 방문**을 클릭합니다.
사용자 자격 증명을 입력하라는 메시지가 표시됩니다.

NSX Advanced Load Balancer Controller 구성

사용 중인 vSphere IaaS control plane 환경에 맞게 NSX Advanced Load Balancer Controller VM을 구성합니다.

로드 밸런서 제어부를 vCenter Server 환경에 연결하려면 NSX Advanced Load Balancer Controller에 몇 가지 배포 후 구성 매개 변수가 필요합니다.

사전 요구 사항

- 사용 중인 환경이 NSX Advanced Load Balancer 구성을 위한 시스템 요구 사항을 충족하는지 확인합니다. "vSphere IaaS 제어부 개념 및 계획" 에서 [NSX 및 NSX Advanced Load Balancer가 있는 영역 감독자 요구 사항](#) 및 [NSX 및 NSX Advanced Load Balancer를 사용한 클러스터 감독자 배포 요구 사항](#)을 참조하십시오.
- 엔터프라이즈 계층 라이선스가 있는지 확인합니다. 컨트롤러는 Enterprise 버전 라이선스에 해당하는 모든 기능을 사용할 수 있는 평가 모드로 부팅됩니다. 평가 기간이 만료되기 전에 유효한 Enterprise Tier 라이선스를 컨트롤러에 할당해야 합니다.

절차

- 1 브라우저를 사용하여 NSX Advanced Load Balancer Controller를 배포할 때 지정한 IP 주소로 이동합니다.

2 관리자 계정을 생성합니다.

옵션	설명
사용자 이름	초기 구성을 위한 관리자 사용자 이름입니다. 이 필드는 편집할 수 없습니다.
암호	컨트롤러 VM의 관리자 암호를 입력합니다. 암호는 8자 이상이어야 하며 숫자, 특수 문자, 대문자 및 소문자의 조합을 포함해야 합니다.
암호 확인	관리자 암호를 다시 입력합니다.
이메일 주소(선택 사항)	관리자 이메일 주소를 입력합니다. 운영 환경에서 암호 복구를 위한 이메일 주소를 제공하는 것이 좋습니다.

3 시스템 설정을 구성합니다.

옵션	설명
암호	컨트롤러 백업을 위한 암호를 입력합니다. 컨트롤러 구성은 정기적으로 로컬 디스크에 자동으로 백업됩니다. 자세한 내용은 백업 및 복원 을 참조하십시오. 암호는 8자 이상이어야 하며 숫자, 특수 문자, 대문자 및 소문자의 조합을 포함해야 합니다.
암호 확인	백업 암호를 다시 입력합니다.
DNS 확인자	vSphere IaaS control plane 환경에서 사용하는 DNS 서버의 IP를 입력합니다. 예를 들면 10.14.7.12입니다.
DNS 검색 도메인	도메인 문자열을 입력합니다.

4 라이선스를 할당합니다.

- a **관리 > 라이선싱**을 선택합니다.
- b **설정**을 선택합니다.
- c **Enterprise Tier**를 선택하고 **저장**을 클릭합니다.
- d 라이선스를 추가하려면 **컴퓨터에서 업로드**를 선택합니다.

라이선스 파일이 업로드되면 컨트롤러 라이선스 목록에 파일이 나타납니다. 시작 날짜 및 만료 날짜를 포함하여 라이선스에 대한 정보가 표시됩니다.

- 5 NSX Advanced Load Balancer Controller가 NSX Manager와 통신할 수 있도록 NSX Manager 자격 증명을 생성합니다. NSX Advanced Load Balancer Controller 대시보드에서 **관리 > 사용자 자격 증명**을 선택합니다.

옵션	설명
이름	자격 증명의 이름입니다. 예: <code>nsxuser</code>
자격 증명 유형	NSX-T 를 선택합니다.
사용자 이름	NSX Manager 로그인에 사용할 사용자 이름을 입력합니다.
암호	NSX Manager의 암호를 입력합니다.

- 6 NSX Advanced Load Balancer Controller가 vCenter Server와 통신할 수 있도록 vCenter Server 자격 증명을 생성합니다.

옵션	설명
이름	자격 증명의 이름입니다. 예: <code>vcuser</code> .
자격 증명 유형	vCenter를 선택합니다.
사용자 이름	vCenter Server 로그인에 사용할 사용자 이름을 입력합니다.
암호	vCenter Server의 암호를 입력합니다.

- 7 자리 표시자 IPAM 프로파일을 생성합니다.

가상 서비스가 생성될 때 가상 IP 주소를 할당하려면 IPAM이 필요합니다.

- a NSX Advanced Load Balancer Controller 대시보드에서 **템플릿 > IPAM/DNS 프로파일**을 선택합니다.

새 IPAM/DNS 프로파일 페이지가 표시됩니다.

- b 프로파일의 이름을 입력합니다. 예: `default-ipam`.
- c **유형**을 **Avi Vantage IPAM**으로 선택합니다.
- d **저장**을 클릭합니다.

- 8 NSX Cloud를 구성합니다.

- a NSX Advanced Load Balancer Controller 대시보드에서 **인프라 > 클라우드**를 선택합니다.

- b 클라우드의 이름을 입력합니다. 예: `nsx-cloud`

- c 클라우드 유형으로 **NSX-T 클라우드**를 선택합니다.

- d **DHCP**를 선택합니다.

- e 서비스 엔진에 대한 **개체 이름 접두사**를 입력합니다. 접두사 문자열에는 문자, 숫자 및 밑줄만 포함해야 합니다. 클라우드가 구성된 후에는 이 필드를 변경할 수 없습니다. 예: `nsx`

- 9 NSX 자격 증명을 입력합니다.

- a NSX Manager IP 주소를 입력합니다.

- b 생성한 NSX Manager 자격 증명을 입력합니다. 예: `nsxuser`

- 10 관리 네트워크를 구성합니다. 관리 네트워크는 NSX Advanced Load Balancer Controller와 서비스 엔진 간의 통신 채널입니다.

옵션	설명
전송 영역	서비스 엔진이 배치된 전송 영역입니다. 오버레이 전송 영역을 선택합니다. 예: <code>nsx-overlay-transportzone</code> .
Tier1 논리적 라우터	Tier-1 게이트웨이를 선택합니다. 예: <code>Tier-1_VWT</code> .
오버레이 세그먼트	서비스 엔진 관리 NIC가 IP 주소를 가져오는 관리 오버레이 세그먼트입니다. 예: <code>nsxoverlaysegment</code> .

- 11 데이터 네트워크를 구성합니다.

데이터 네트워크 섹션에서 **추가**를 클릭합니다.

옵션	설명
전송 영역	오버레이 전송 영역을 선택합니다. 예: <code>nsx-overlay-transportzone</code> .
논리적 라우터	Tier-1 게이트웨이를 입력합니다. 예: <code>Tier-1_VWT</code> .
오버레이 세그먼트	오버레이 세그먼트를 선택합니다. 예: <code>nsxoverlaysegment</code> .

- 12 vCenter Server 자격 증명을 입력합니다.

vCenter Server 섹션에서 **추가**를 클릭합니다.

옵션	설명
이름	이전에 생성한 자격 증명의 이름입니다. 예: <code>vcuser</code> .
URL	vCenter Server의 IP 주소입니다.

- 13 앞서 생성한 IPAM 프로파일을 추가합니다. **IPAM 프로파일**에서 `default-ipam`을 선택합니다.

가상 서비스가 생성될 때 가상 IP 주소를 할당하려면 IPAM이 필요합니다.

결과

구성을 완료하면 NSX Advanced Load Balancer Controller **대시보드**가 보입니다. **인프라 > 클라우드**를 선택하고 **NSX Cloud**에 대한 NSX Advanced Load Balancer Controller의 상태가 녹색인지 확인합니다. 종종 NSX Advanced Load Balancer Controller가 vCenter Server 환경의 모든 포트 그룹을 검색할 때까지 상태가 잠시 노란색으로 표시되었다가 녹색으로 바뀔 수 있습니다.

다음에 수행할 작업

서비스 엔진 그룹을 구성합니다. **서비스 엔진 그룹 구성**의 내용을 참조하십시오.

서비스 엔진 그룹 구성

vSphere IaaS control plane는 **기본 그룹**을 템플릿으로 사용하여 감독자별 서비스 엔진 그룹을 구성합니다. 필요한 경우 vCenter 내 서비스 엔진 VM의 수와 배치를 정의하는 그룹 내에서 **기본 그룹** 서비스 엔진을 구성할 수

있습니다. NSX Advanced Load Balancer Controller가 Enterprise 모드에 있는 경우에도고가용성을 구성할 수 있습니다.

절차

1 NSX Advanced Load Balancer Controller 대시보드에서 **인프라 > 클라우드 리소스 > 서비스 엔진 그룹**을 선택합니다.

2 **서비스 엔진 그룹** 페이지에서 **기본 그룹**의 편집 아이콘을 클릭합니다.

일반 설정 탭이 나타납니다.

3 **고가용성 및 배치 설정** 섹션에서 고가용성 및 가상 서비스 설정을 구성합니다.

a **고가용성 모드**를 선택합니다.

기본 옵션은 N + M (buffer)입니다. 기본값을 유지하거나 다음 옵션 중 하나를 선택할 수 있습니다.

- Active/Standby

- Active/Active

b **서비스 엔진 수**를 구성합니다. 서비스 엔진 그룹 내에서 생성될 수 있는 최대 서비스 엔진 수입니다. 기본값은 10입니다.

c **서비스 엔진 전반의 가상 서비스 배치**를 구성합니다.

기본 옵션은 **컴팩트**입니다. 다음 옵션 중 하나를 선택할 수 있습니다.

- **분산**. NSX Advanced Load Balancer Controller가 새로 가동된 서비스 엔진에 가상 서비스를 지정된 최대 서비스 엔진 수까지 배치하여 성능을 최대화합니다.

- **컴팩트**. NSX Advanced Load Balancer Controller가 가능한 최소한의 서비스 엔진을 스핀 업하고 새 가상 서비스를 기존 서비스 엔진에 배치합니다. 새 서비스 엔진은 모든 서비스 엔진이 활용되는 경우에만 생성됩니다.

4 다른 설정에 대해서는 기본값을 유지할 수 있습니다.

5 **저장**을 클릭합니다.

결과

AKO는 각 vSphere IaaS control plane 클러스터에 대해 하나의 서비스 엔진 그룹을 생성합니다. 서비스 엔진 그룹 구성은 **기본 그룹** 구성에서 파생됩니다. **기본 그룹**이 필수 값으로 구성되면 AKO에서 생성된 모든 새 서비스 엔진 그룹은 동일한 설정을 갖게 됩니다. 하지만 **기본 그룹** 구성에 대한 변경 사항은 이미 생성된 서비스 엔진 그룹에 반영되지 않습니다. 기존 서비스 엔진 그룹에 대한 구성은 별도로 수정해야 합니다.

NSX Advanced Load Balancer Controller를 NSX Manager에 등록

NSX Advanced Load Balancer Controller를 NSX Manager에 등록합니다.

사전 요구 사항

NSX Advanced Load Balancer Controller를 배포하고 구성했는지 확인합니다.

절차

- 1 루트 사용자로 NSX Manager에 로그인합니다.
- 2 다음 명령을 실행합니다.

```
curl -k --location --request PUT 'https://<nsx-mgr-ip>/policy/api/v1/infra/alb-onboarding-workflow' \
--header 'X-Allow-Overwrite: True' \
--header 'Authorization: Basic <base64 encoding of username:password of NSX Mgr>' \
--header 'Content-Type: application/json' \
--data-raw '{
"owned_by": "LCM",
"cluster_ip": "<nsx-alb-controller-cluster-ip>",
"infra_admin_username" : "username",
"infra_admin_password" : "password"
}'
```

API 호출에 DNS 및 NTP 설정을 제공하는 경우 전역 설정이 재정의됩니다. 예를 들어 "dns_servers": ["<dns-servers-ips>"] 및 "ntp_servers": ["<ntp-servers-ips>"]를 선택합니다.

NSX Advanced Load Balancer Controller에 인증서 할당

NSX Advanced Load Balancer Controller는 클라이언트에 보내는 인증서를 사용하여 사이트를 인증하고 보안 통신을 설정합니다. 인증서는 NSX Advanced Load Balancer에서 자체 서명되거나 CSR(인증서 서명 요청)으로 생성될 수 있으며, 이것이 신뢰할 수 있는 CA(인증 기관)로 전송되면 신뢰할 수 있는 인증서가 생성됩니다. 자체 서명된 인증서를 생성하거나 외부 인증서를 업로드할 수 있습니다.

감독자를 사용하도록 설정하려면 사용자 지정 인증서를 제공해야 합니다. 기본 인증서는 사용할 수 없습니다. 인증서에 대한 자세한 내용은 [SSL/TLS 인증서](#)를 참조하십시오.

사실 CA(인증 기관) 서명 인증서를 사용하는 경우 감독자 배포가 완료되지 않고 NSX Advanced Load Balancer 구성이 적용되지 않을 수 있습니다. 자세한 내용은 [NSX Advanced Load Balancer 구성이 적용되지 않음](#)의 내용을 참조하십시오.

사전 요구 사항

NSX Advanced Load Balancer가 NSX Manager에 등록되어 있는지 확인합니다.

절차

- 1 컨트롤러 대시보드에서 왼쪽 상단 모서리에 있는 메뉴를 클릭하고 **템플릿 > 보안**을 선택합니다.
- 2 **SSL/TLS 인증서**를 선택합니다.
- 3 인증서를 생성하려면 **생성**을 클릭하고 **컨트롤러 인증서**를 선택합니다.
새 인증서(SSL/TLS) 창이 나타납니다.
- 4 인증서의 이름을 입력합니다.

- 5 미리 생성된 유효한 인증서가 없는 경우 **유형**을 `Self Signed`로 선택하여 자체 서명된 인증서를 추가합니다.
- a 다음과 같은 세부 정보를 입력합니다.

옵션	설명
일반 이름	사이트의 정규화된 이름을 지정합니다. 사이트가 신뢰할 수 있는 사이트로 간주되려면 이 항목이 클라이언트가 브라우저에 입력한 호스트 이름과 일치해야 합니다.
알고리즘	EC(타원 곡선) 암호화 또는 RSA를 선택합니다. EC가 권장됩니다.
키 크기	핸드셰이크에 사용할 암호화 수준을 선택합니다. <ul style="list-style-type: none"> ■ SECP256R1은 EC 인증서에 사용됩니다. ■ 2048비트는 RSA 인증서에 권장됩니다.

- b **SAN(대체 이름)**에서 **추가**를 클릭합니다.
- c NSX Advanced Load Balancer Controller가 단일 노드로 배포된 경우 이것의 클러스터 IP 주소나 FQDN 또는 둘 다를 입력합니다. IP 주소 또는 FQDN만 사용되는 경우 배포 중에 지정한 NSX Advanced Load Balancer Controller VM의 IP 주소와 일치해야 합니다.
- [NSX Advanced Load Balancer Controller 배포](#)의 내용을 참조하십시오. NSX Advanced Load Balancer Controller 클러스터가 3개의 노드로 구성된 클러스터로 배포된 경우 해당 클러스터의 IP 또는 FQDN을 입력합니다.
- d **저장**을 클릭합니다.
- 워크로드 관리 기능을 사용하도록 감독자를 구성할 때 이 인증서가 필요합니다.

- 6 생성한 자체 서명된 인증서를 다운로드합니다.

- a **보안 > SSL/TLS 인증서**를 선택합니다.
- 인증서가 표시되지 않으면 페이지를 새로 고칩니다.
- b 생성한 인증서를 선택하고 다운로드 아이콘을 클릭합니다.
- c **인증서 내보내기** 페이지가 나타나면 인증서에 대해 **클립보드에 복사**를 클릭합니다. 키를 복사하지 마십시오.
- d 나중에 워크로드 관리를 사용하도록 설정할 때 사용할 수 있도록 복사한 인증서를 저장합니다.

- 7 미리 생성된 유효한 인증서가 있는 경우 **유형**을 `Import`로 선택하여 업로드합니다.

- a **인증서**에서 **파일 업로드**를 클릭하고 인증서를 가져옵니다.
- 업로드한 인증서의 SAN 필드에는 컨트롤러의 클러스터 IP 주소 또는 FQDN이 있어야 합니다.

참고 인증서의 콘텐츠를 한 번만 업로드하거나 붙여넣어야 합니다.

- b **키(PEM) 또는 PKCS12**에서 **파일 업로드**를 클릭하고 키를 가져옵니다.
- c **유효성 검사**를 클릭하여 인증서와 키의 유효성을 검사합니다.
- d **저장**을 클릭합니다.

- 8 인증서를 변경하려면 다음 단계를 수행합니다.
 - a 컨트롤러 대시보드에서 **관리 > 시스템 설정**을 선택합니다.
 - b **편집**을 클릭합니다.
 - c **액세스** 탭을 선택합니다.
 - d **SSL/TLS 인증서**에서 기존 기본 포털 인증서를 제거합니다.
 - e 드롭다운에서 새로 생성 또는 업로드된 인증서를 선택합니다.
 - f **기본 인증**을 선택합니다.
 - g **저장**을 클릭합니다.

NSX Advanced Load Balancer 사용에 대한 제한 사항

vSphere IaaS control plane 환경에서 NSX Advanced Load Balancer를 구성하는 동안 주의 사항을 염두에 두어야 합니다.

다음과 같은 경우 수신이 NSX Advanced Load Balancer에서 외부 IP를 가져오지 않습니다.

- 수신 구성에 호스트 이름이 지정되지 않은 경우.
- 수신이 호스트 이름 대신 `defaultBackend` 구성 옵션으로 구성된 경우.

기본적으로 Kubernetes의 수신 리소스는 컨트롤러 구성에서 호스트 이름을 정의하여 외부 IP를 할당해야 합니다. 이 작업은 NSX Advanced Load Balancer가 Kubernetes 수신과 관련하여 생성된 가상 서비스의 트래픽에 대해 가상 호스팅을 사용하기 때문에 필요합니다. `defaultBackend` 구성 옵션에 관한 자세한 내용은 <https://kubernetes.io/docs/concepts/services-networking/ingress/#default-backend>의 내용을 참조하십시오.

수신이 다른 네임스페이스의 수신과 동일한 호스트 이름을 갖는 경우 NSX Advanced Load Balancer에서 외부 IP를 가져오지 않습니다. 기본적으로 NSX Advanced Load Balancer는 각 네임스페이스에 대해 고유한 VIP를 할당합니다. 즉, 단일 네임스페이스의 모든 수신이 동일한 VIP를 공유합니다. 따라서 서로 다른 네임스페이스의 두 수신에 고유한 VIP가 할당됩니다. 하지만 호스트 이름이 동일한 경우 DNS 서버는 호스트 이름을 확인할 IP 주소를 알 수 없습니다.

NSX Advanced Load Balancer 설치 및 구성

vDS(vSphere Distributed Switch) 네트워킹을 사용하는 경우 vSphere IaaS control plane 환경에 NSX Advanced Load Balancer 22.1.4를 설치하고 구성할 수 있습니다.

- 환경이 NSX Advanced Load Balancer로 vSphere IaaS control plane를 구성하기 위한 요구 사항을 충족하는지 확인합니다. "vSphere IaaS 제어부 개념 및 계획"에서 [NSX Advanced Load Balancer를 사용하는 3개 영역 감독자에 대한 요구 사항](#) 및 [NSX Advanced Load Balancer를 사용하여 단일 클러스터 감독자를 사용하도록 설정하기 위한 요구 사항](#)을 참조하십시오.

- NSX Advanced Load Balancer OVA를 다운로드합니다. VMware는 워크로드 관리를 사용하도록 설정할 vSphere 환경에 배포하는 NSX Advanced Load Balancer OVA 파일을 제공합니다. [VMware Customer Connect](#) 포털에서 vSphere IaaS control plane에서 지원되는 최신 버전의 OVA 파일을 다운로드합니다.

참고 이 가이드의 절차는 vSphere IaaS control plane 8.0 업데이트 2에서 지원되는 NSX Advanced Load Balancer와 관련되어 있습니다. 사용 가능한 최신 버전의 NSX Advanced Load Balancer가 있을 수 있으며 UI 워크플로가 다를 수 있습니다.

NSX Advanced Load Balancer에 대한 자세한 내용은 [VMware NSX Advanced Load Balancer 설명서](#)를 참조하십시오.

다음으로 읽을 항목

절차

1 NSX Advanced Load Balancer와 함께 사용할 감독자용 vSphere Distributed Switch 생성

vSphere 클러스터를 vSphere 네트워킹 스택 및 NSX Advanced Load Balancer를 사용하는 감독자로 구성하려면 vSphere Distributed Switch를 생성해야 합니다. 감독자에 대한 워크로드 네트워킹으로 구성할 수 있는 Distributed Switch에서 포트 그룹을 생성합니다. 서비스 엔진 데이터 인터페이스를 연결하려면 NSX Advanced Load Balancer에 분산 포트 그룹이 필요합니다. 포트 그룹은 서비스 엔진에 애플리케이션 VIP(가상 IP)를 배치하는 데 사용됩니다.

2 NSX Advanced Load Balancer OVA를 로컬 콘텐츠 라이브러리로 가져오기

NSX Advanced Load Balancer OVA 이미지를 저장하려면 로컬 콘텐츠 라이브러리를 생성하고 여기에 OVA를 가져옵니다.

3 NSX Advanced Load Balancer 컨트롤러 배포

vSphere IaaS control plane 환경의 관리 네트워크에 NSX Advanced Load Balancer 컨트롤러 VM을 배포합니다.

4 서비스 엔진 그룹 구성

vSphere IaaS control plane는 **기본 그룹** 서비스 엔진 그룹을 사용합니다. 필요한 경우 vCenter 내 서비스 엔진 VM의 수와 배치를 정의하는 그룹 내에서 **기본 그룹** 서비스 엔진을 구성할 수 있습니다. NSX Advanced Load Balancer 컨트롤러가 Enterprise 모드에 있는 경우에도고가용성을 구성할 수 있습니다. vSphere IaaS control plane는 **기본 그룹** 서비스 엔진만 지원합니다. 다른 서비스 엔진 그룹은 생성할 수 없습니다.

NSX Advanced Load Balancer와 함께 사용할 감독자용 vSphere Distributed Switch 생성

vSphere 클러스터를 vSphere 네트워킹 스택 및 NSX Advanced Load Balancer를 사용하는 감독자로 구성하려면 vSphere Distributed Switch를 생성해야 합니다. 감독자에 대한 워크로드 네트워킹으로 구성할 수 있는 Distributed Switch에서 포트 그룹을 생성합니다. 서비스 엔진 데이터 인터페이스를 연결하려면 NSX

Advanced Load Balancer에 분산 포트 그룹이 필요합니다. 포트 그룹은 서비스 엔진에 애플리케이션 VIP(가상 IP)를 배치하는 데 사용됩니다.

사전 요구 사항

NSX Advanced Load Balancer와 함께 감독자에 vSphere 네트워킹을 사용하기 위한 시스템 요구 사항 및 네트워크 토폴로지를 검토합니다. "vSphere IaaS 제어부 개념 및 계획" 에서 [NSX Advanced Load Balancer](#)를 사용하는 3개 영역 감독자에 대한 요구 사항 및 [NSX Advanced Load Balancer](#)를 사용하여 단일 클러스터 감독자를 사용하도록 설정하기 위한 요구 사항을 참조하십시오.

절차

- 1 vSphere Client에서 데이터 센터로 이동합니다.
- 2 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 **Distributed Switch > 새 Distributed Switch**를 선택합니다.
- 3 스위치의 이름(예: **Workload Distributed Switch**)을 입력하고 **다음**을 클릭합니다.
- 4 스위치에 대해 버전 8.0을 선택하고 **다음**을 클릭합니다.
- 5 **포트 그룹 이름**에서 **Primary Workload Network**를 입력하고 **다음**을 클릭한 후 **마침**을 클릭합니다.
 하나의 포트 그룹이 포함된 새 Distributed Switch가 데이터 센터에 생성됩니다. 이 포트 그룹을 생성할 감독자에 대한 기본 워크로드 네트워크로 사용할 수 있습니다. 기본 워크로드 네트워크는 Kubernetes 제어부 VM에 대한 트래픽을 처리합니다.
- 6 워크로드 네트워크에 대한 분산 포트 그룹을 생성합니다.
 생성하는 포트 그룹의 수는 감독자에 대해 구현하려는 토폴로지에 따라 다릅니다. 하나의 분리된 워크로드 네트워크가 있는 토폴로지의 경우 감독자의 모든 네임스페이스에 대한 네트워크로 사용할 하나의 분산 포트 그룹을 생성합니다. 네임스페이스별로 분리된 네트워크가 있는 토폴로지의 경우 생성할 네임스페이스 수와 동일한 수의 포트 그룹을 생성합니다.
 - a 새로 생성된 Distributed Switch로 이동합니다.
 - b 스위치를 마우스 오른쪽 버튼으로 클릭하고 **분산 포트 그룹 > 새 분산 포트 그룹**을 선택합니다.
 - c 포트 그룹의 이름(예: **Workload Network**)을 입력하고 **다음**을 클릭합니다.
 - d 기본값을 그대로 두고 **다음**을 클릭한 다음 **마침**을 클릭합니다.

7 데이터 네트워크에 대한 포트 그룹을 생성합니다.

- 분산 스위치를 마우스 오른쪽 버튼으로 클릭하고 **분산 포트 그룹 > 새 분산 포트 그룹**을 선택합니다.
- 포트 그룹의 이름(예: **Data Network**)을 입력하고 **다음**을 클릭합니다.
- 설정 구성** 페이지에서 새 분산 포트 그룹에 대한 일반 속성을 입력하고 **다음**을 클릭합니다.

속성	설명
포트 바인딩	이 분산 포트 그룹에 연결된 가상 시스템에 포트가 할당되는 시점을 선택합니다. 가상 시스템이 분산 포트 그룹에 연결할 때 가상 시스템에 포트를 할당하려면 정적 바인딩 을 선택합니다.
포트 할당	탄력적 포트 할당을 선택합니다. 기본 포트 수는 8개입니다. 포트가 모두 할당되면 새로 여덟 개의 포트가 생성됩니다.
포트 수	기본값을 유지합니다.
네트워크 리소스 풀	드롭다운 메뉴에서 사용자 정의 네트워크 리소스 풀에 새 분산 포트 그룹을 할당합니다. 네트워크 리소스 풀을 생성하지 않은 경우 이 메뉴는 비어 있습니다.
VLAN	드롭다운 메뉴에서 VLAN 트래픽 필터링 및 표시 유형을 선택합니다. <ul style="list-style-type: none"> ■ 없음: VLAN을 사용하지 않습니다. External Switch Tagging을 사용하는 경우 이 옵션을 선택합니다. ■ VLAN: [VLAN ID] 텍스트 상자에 Virtual Switch Tagging에 대해 1-4094 사이의 값을 입력합니다. ■ VLAN 트렁킹: Virtual Guest Tagging에 대해 그리고 ID가 있는 VLAN 트래픽을 게스트 OS에 전달하려는 경우 이 옵션을 사용합니다. VLAN 트렁크 범위를 입력합니다. 쉼표로 구분된 목록을 사용하여 여러 개의 범위 또는 개별 VLAN을 설정할 수 있습니다. 예: 1702-1705, 1848-1849 ■ 전용 VLAN: 트래픽을 Distributed Switch에서 생성된 전용 VLAN과 연결합니다. 전용 VLAN을 생성하지 않은 경우에 이 메뉴는 비어 있습니다.
고급	이 옵션은 선택되지 않은 상태로 둡니다.

8 완료 준비 페이지에서 구성을 검토하고 **마침**을 클릭합니다.

결과

Distributed Switch가 생성되고 Distributed Switch 아래에 분산 포트 그룹이 표시됩니다. 이제 생성한 포트 그룹을 NSX Advanced Load Balancer에 대한 **데이터 네트워크**로 사용할 수 있습니다.

NSX Advanced Load Balancer OVA를 로컬 콘텐츠 라이브러리로 가져오기

NSX Advanced Load Balancer OVA 이미지를 저장하려면 로컬 콘텐츠 라이브러리를 생성하고 여기에 OVA를 가져옵니다.

로컬 콘텐츠 라이브러리를 생성하려면 라이브러리를 구성하고 OVA 파일을 다운로드하여 로컬 콘텐츠 라이브러리로 가져와야 합니다. 자세한 내용은 [콘텐츠 라이브러리 사용](#)을 참조하십시오.

사전 요구 사항

NSX Advanced Load Balancer OVA를 다운로드했는지 확인합니다.

로컬 콘텐츠 라이브러리를 생성합니다. 콘텐츠 라이브러리 생성 및 편집을 참조하십시오.

절차

- 1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.
- 2 **메뉴 > 콘텐츠 라이브러리**를 선택합니다.
- 3 **콘텐츠 라이브러리** 목록에서 직접 생성한 로컬 콘텐츠 라이브러리의 이름 링크를 클릭합니다. 예: **NSX ALB**.
- 4 **작업**을 클릭합니다.
- 5 **항목 가져오기**를 선택합니다.
- 6 **라이브러리 항목 가져오기** 창에서 **로컬 파일**을 선택합니다.
- 7 **파일 업로드**를 클릭합니다.
- 8 다운로드한 OVA 파일을 선택합니다.
- 9 **가져오기**를 클릭합니다.
- 10 페이지 하단의 **최근 작업** 창을 나타냅니다.
- 11 **라이브러리 항목의 콘텐츠 가져오기** 작업을 모니터링하고 성공적으로 **완료**되었는지 확인합니다.

다음에 수행할 작업

NSX Advanced Load Balancer 컨트롤러를 배포합니다. [NSX Advanced Load Balancer 컨트롤러 배포](#)의 내용을 참조하십시오.

NSX Advanced Load Balancer 컨트롤러 배포

vSphere IaaS control plane 환경의 관리 네트워크에 NSX Advanced Load Balancer 컨트롤러 VM을 배포합니다.

사전 요구 사항

- NSX Advanced Load Balancer를 배포할 관리 네트워크가 있는지 확인합니다. vDS(vSphere Distributed Switch) 또는 vSS(vSphere Standard Switch)일 수 있습니다.
- 데이터 네트워크를 위한 vDS 스위치 및 포트 그룹을 생성했는지 확인합니다. [NSX Advanced Load Balancer와 함께 사용할 감독자용 vSphere Distributed Switch](#) 생성의 내용을 참조하십시오.
- 사전 요구 사항을 완료했는지 확인합니다. "vSphere IaaS 제어부 개념 및 계획" 에서 NSX Advanced Load Balancer를 사용하는 3개 영역 감독자에 대한 요구 사항 및 NSX Advanced Load Balancer를 사용하여 단일 클러스터 감독자를 사용하도록 설정하기 위한 요구 사항을 참조하십시오.

절차

- 1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.
- 2 관리 구성 요소용으로 지정된 vSphere 클러스터를 선택합니다.
- 3 **AVI-LB**라는 리소스 풀을 생성합니다.

- 4 리소스 풀을 마우스 오른쪽 버튼으로 클릭하고 **OVF 템플릿 배포**를 선택합니다.
- 5 **로컬 파일**을 선택하고 **파일 업로드**를 클릭합니다.
- 6 사전 요구 사항으로 다운로드한 `controller-VERSION.ova` 파일을 찾아서 선택합니다.
- 7 이름을 입력하고 컨트롤러의 폴더를 선택합니다.

옵션	설명
가상 시스템 이름	<code>avi-controller-1</code>
가상 시스템 위치	데이터 센터

- 8 **AVI-LB** 리소스 풀을 계산 리소스로 선택합니다.
- 9 구성 세부 정보를 검토하고 **다음**을 클릭합니다.
- 10 **VM 스토리지 정책**(예: `vsanDatastore`)을 선택합니다.
- 11 관리 네트워크(예: `network-1`)를 선택합니다.
- 12 다음과 같이 구성을 사용자 지정하고 완료되면 **다음**을 클릭합니다.

옵션	설명
관리 인터페이스 IP 주소	컨트롤러 VM의 IP 주소(예: <code>10.199.17.51</code>)를 입력합니다.
관리 인터페이스 서브넷 마스크	서브넷 마스크(예: <code>255.255.255.0</code>)를 입력합니다.
기본 게이트웨이	관리 네트워크의 기본 게이트웨이(예: <code>10.199.17.235</code>)를 입력합니다.
Sysadmin 로그인 인증 키	필요한 경우 공용 키의 콘텐츠를 붙여넣습니다. 키를 비워 둘 수 있습니다.
Avi 컨트롤러의 호스트 이름	컨트롤러의 FQDN 또는 IP 주소를 입력합니다.

- 13 배포 설정을 검토합니다.
- 14 **마침**을 클릭하여 구성을 완료합니다.
- 15 vSphere Client를 사용하여 **작업** 패널에서 컨트롤러 VM의 프로비저닝을 모니터링합니다.
- 16 vSphere Client를 사용하여 컨트롤러 VM을 배포한 후 전원을 켭니다.

컨트롤러 클러스터 배포

필요한 경우 3개의 컨트롤러 노드로 구성된 클러스터를 배포할 수 있습니다. 운영 환경에서는 HA 및 재해 복구를 위해 클러스터를 구성하는 것이 좋습니다. 단일 노드 NSX Advanced Load Balancer 컨트롤러를 실행하는 경우 백업 및 복원 기능을 사용해야 합니다.

3노드 클러스터를 실행하려면 첫 번째 컨트롤러 VM을 배포한 후 두 개의 추가 컨트롤러 VM을 배포하고 전원을 켭니다. 초기 구성 마법사를 실행하거나 이러한 컨트롤러에 대한 관리자 암호를 변경하면 안 됩니다. 첫 번째 컨트롤러 VM의 구성이 두 개의 새 컨트롤러 VM에 할당됩니다.

절차

- 1 **관리 > 컨트롤러**로 이동합니다.

- 2 노드를 선택합니다.
- 3 편집 아이콘을 클릭합니다.
- 4 컨트롤러 클러스터 IP에 대한 고정 IP를 추가합니다.

이 IP 주소는 관리 네트워크의 IP 주소여야 합니다.

- 5 클러스터 노드에서 두 개의 새 클러스터 노드를 구성합니다.

옵션	설명
IP	컨트롤러 노드의 IP 주소입니다.
이름	노드의 이름입니다. 이 이름은 IP 주소일 수 있습니다.
암호	컨트롤러 노드의 암호입니다. 암호는 비워 둡니다.
공용 IP	컨트롤러 노드의 공용 IP 주소입니다. 비워 둡니다.

- 6 저장을 클릭합니다.

참고 클러스터를 배포한 후에는 추가 구성에 컨트롤러 노드 IP가 아닌 컨트롤러 클러스터 IP를 사용해야 합니다.

컨트롤러 전원 켜기

컨트롤러 VM을 배포한 후 전원을 켤 수 있습니다. 부팅 프로세스 동안 배포 중에 지정된 IP 주소가 VM에 할당됩니다.

전원을 켜 후 컨트롤러 VM의 첫 번째 부팅 프로세스에 최대 10분이 소요될 수 있습니다.

사전 요구 사항

컨트롤러를 배포합니다.

절차

- 1 vCenter Server에서, 배포한 `avi-controller-1` VM을 마우스 오른쪽 버튼으로 클릭합니다.
- 2 **전원 > 전원 켜기**를 선택합니다.
배포 중에 지정한 IP 주소가 VM에 할당됩니다.
- 3 VM의 전원이 켜져 있는지 확인하기 위해 브라우저에서 IP 주소에 액세스합니다.
VM이 온라인 상태가 되면 TLS 인증서 및 연결에 대한 주의가 표시됩니다.
- 4 **연결이 비공개가 아닙니다.** 주의에서 **세부 정보 표시**를 클릭합니다.
- 5 창이 나타나면 **이 웹 사이트 방문**을 클릭합니다.
사용자 자격 증명을 입력하라는 메시지가 표시됩니다.

컨트롤러 구성

vSphere IaaS control plane 환경에 대한 컨트롤러 VM을 구성하고 클라우드를 설정합니다.

로드 밸런서 제어부를 vCenter Server 환경에 연결하려면 컨트롤러에 몇 가지 배포 후 구성 매개 변수가 필요합니다. 컨트롤러의 초기 구성 중에 첫 번째 컨트롤러가 배포되는 기본 클라우드라는 클라우드가 생성됩니다. 로드 밸런서가 여러 vCenter 서버 또는 여러 데이터 센터에 서비스를 제공할 수 있도록 하려면 각 vCenter 및 데이터 센터 조합에 대해 VMware vCenter 유형의 사용자 지정 클라우드를 생성하면 됩니다. 자세한 내용은 [NSX Advanced Load Balancer 구성 요소](#)를 참조하십시오.

사전 요구 사항

- 사용 중인 환경이 NSX Advanced Load Balancer 구성을 위한 시스템 요구 사항을 충족하는지 확인합니다. "vSphere IaaS 제어부 개념 및 계획" 에서 [NSX Advanced Load Balancer](#)를 사용하는 3개 영역 감독자에 대한 요구 사항 및 [NSX Advanced Load Balancer](#)를 사용하여 단일 클러스터 감독자를 사용하도록 설정하기 위한 요구 사항을 참조하십시오.
- 컨트롤러를 배포합니다.

절차

- 1 브라우저를 사용하여 컨트롤러를 배포할 때 지정한 IP 주소로 이동합니다.
- 2 관리자 계정을 생성합니다.

옵션	설명
사용자 이름	초기 구성을 위한 관리자 사용자 이름입니다. 이 필드는 편집할 수 없습니다.
암호	컨트롤러 VM의 관리자 암호를 입력합니다. 암호는 8자 이상이어야 하며 숫자, 특수 문자, 대문자 및 소문자의 조합을 포함해야 합니다.
암호 확인	관리자 암호를 다시 입력합니다.
이메일 주소(선택 사항)	관리자 이메일 주소를 입력합니다. 운영 환경에서 암호 복구를 위한 이메일 주소를 제공하는 것이 좋습니다.

- 3 시스템 설정을 구성합니다.

옵션	설명
암호	컨트롤러 백업을 위한 암호를 입력합니다. 컨트롤러 구성은 정기적으로 로컬 디스크에 자동으로 백업됩니다. 자세한 내용은 백업 및 복원 을 참조하십시오. 암호는 8자 이상이어야 하며 숫자, 특수 문자, 대문자 및 소문자의 조합을 포함해야 합니다.
암호 확인	백업 암호를 다시 입력합니다.
DNS 확인자	vSphere IaaS control plane 환경에서 사용하는 DNS 서버의 IP를 입력합니다. 예를 들면 10.14.7.12입니다.
DNS 검색 도메인	도메인 문자열을 입력합니다.

4 (선택 사항) 이메일/SMTP 설정을 구성합니다.

옵션	설명
SMTP 소스	없음, 로컬 호스트, SMTP 서버 또는 익명 서버 옵션 중 하나를 선택합니다. 기본값은 로컬 호스트입니다.
보낸 사람 주소	이메일 주소입니다.

5 다음을 클릭합니다.

6 다중 테넌트 설정을 구성합니다.

- a 기본 테넌트 액세스를 유지합니다.
- b 다음 이후에 클라우드 설정을 선택하고 저장을 클릭합니다.

참고 저장하기 전에 다음 이후에 클라우드 설정 옵션을 선택하지 않은 경우 초기 구성 마법사가 종료됩니다. 클라우드 구성 창이 자동으로 실행되지 않고 컨트롤러의 대시보드 보기로 연결됩니다. 이 경우 **인프라 > 클라우드**로 이동하여 클라우드를 구성합니다.

7 VMware vCenter/vSphere ESX 클라우드를 구성합니다. 생성을 클릭하고 클라우드 유형으로 VMware vCenter/vSphere ESX를 클릭합니다.

새 클라우드 설정 페이지가 표시됩니다.

8 일반 설정을 구성합니다.

옵션	설명
이름	클라우드의 이름을 입력합니다. 예: Custom-Cloud.
유형	클라우드 유형은 VMware vCenter/vSphere ESX입니다.

9 (선택 사항) vSphere 포트 그룹에서 DHCP를 사용할 수 있는 경우 기본 네트워크 IP 주소 관리 섹션에서 DHCP 사용을 선택합니다.

서비스 엔진 인터페이스에서 정적 IP 주소만 사용하도록 하려면 옵션을 선택하지 않은 상태로 둡니다. 각 네트워크에 대해 개별적으로 구성할 수 있습니다.

자세한 내용은 가상 IP 네트워크 구성의 내용을 참조하십시오.

10 가상 서비스 배치 설정을 구성합니다.

옵션	설명
가상 서비스 배치를 위해 직접 연결된 네트워크보다 정적 경로 선호	서비스 엔진 VM이 기본 게이트웨이를 통해 라우팅하여 서버 네트워크에 강제로 액세스하도록 하려면 이 옵션을 선택합니다. 기본적으로 컨트롤러는 NIC를 서버 네트워크에 직접 연결하며, 서비스 엔진이 데이터 네트워크에만 연결하고 워크로드 네트워크에 라우팅되도록 강제로 적용해야 합니다.
VIP의 네트워크 확인에 정적 경로 사용	이 옵션은 선택되지 않은 상태로 둡니다.

11 vCenter/vSphere 자격 증명을 구성합니다.

자격 증명 설정을 클릭하고 다음 세부 정보를 입력합니다.

옵션	설명
vCenter 주소	vCenter Server 환경에 대한 vSphere IaaS control plane 호스트 이름 또는 IP 주소를 입력합니다.
사용자 이름	vCenter 관리자의 사용자 이름(예: administrator@vsphere.local)을 입력합니다. 더 적은 사용 권한을 사용하려면 전용 역할을 생성합니다. 자세한 내용은 VMware 사용자 역할을 참조하십시오 .
암호	사용자 암호를 입력합니다.
액세스 권한	읽기: 서비스 엔진 VM을 직접 생성하고 관리합니다. 쓰기: 컨트롤러가 서비스 엔진 VM을 생성하고 관리합니다. [쓰기]를 선택해야 합니다.

12 데이터 센터 설정을 구성합니다.

- 워크로드 관리를 사용하도록 설정할 vSphere 데이터 센터를 선택합니다.
- 컨텐츠 라이브러리 사용 옵션을 선택하고 목록에서 로컬 컨텐츠 라이브러리를 선택합니다.

13 저장 및 다시 시작을 선택하여 구성된 설정으로 VMware vCenter/vSphere ESX 클라우드를 생성합니다.

14 네트워크 설정을 구성합니다.

옵션	설명
관리 네트워크	VM 네트워크를 선택합니다. 이 네트워크 인터페이스는 서비스 엔진이 컨트롤러와 연결하는 데 사용됩니다.
서비스 엔진	템플릿 서비스 엔진 그룹을 비워 둡니다.
관리 네트워크 IP 주소 관리	DHCP 사용을 선택합니다.

15 (선택 사항) DHCP 사용을 선택하지 않은 경우에만 다음 네트워크 설정을 구성합니다.

옵션	설명
IP 서브넷	관리 네트워크의 IP 서브넷을 입력합니다. 예: 10.199.32.0/24 참고 DHCP를 사용할 수 없는 경우에만 IP 서브넷을 입력합니다.
기본 게이트웨이	관리 네트워크의 기본 게이트웨이(예: 10.199.32.253)를 입력합니다. 참고 DHCP를 사용할 수 없는 경우에만 IP 서브넷을 입력합니다.
정적 IP 주소 풀 추가	하나 이상의 IP 주소 또는 IP 주소 범위를 입력합니다. 예: 10.99.32.62-10.199.32.65 참고 DHCP를 사용할 수 없는 경우에만 IP 서브넷을 입력합니다.

16 IPAM 프로파일을 생성하고 IPAM/DNS 설정을 구성합니다.

가상 서비스가 생성될 때 가상 IP 주소를 할당하려면 IPAM이 필요합니다.

- a **IPAM 프로파일**의 추가 작업 메뉴에서 **생성**을 선택합니다.

새 **IPAM/DNS 프로파일** 페이지가 표시됩니다.

- b **IPAM 프로파일**을 구성합니다.

옵션	설명
이름	사용자 정의 문자열(예: <code>ipam-profile</code>)
유형	AVI Vantage IPAM 선택
VRF에서 IP 할당	이 옵션을 선택 취소합니다.
클라우드	드롭다운 목록에서 Custom-Cloud 를 선택합니다.

- c **사용 가능한 네트워크**에서 **추가**를 클릭하고 구성된 가상 IP 네트워크를 선택합니다. 이 네트워크는 기본 네트워크입니다.

- d **저장**을 클릭합니다.

17 (선택 사항) 내부 NTP 서버를 사용하려면 NTP 설정을 구성합니다.

- a **관리 > 설정 > DNS/NTP**를 선택합니다.

- b 기존 NTP 서버가 있는 경우 삭제하고 사용 중인 DNS 서버의 IP 주소를 입력합니다. 예:
192.168.100.1.

결과

구성을 완료하면 컨트롤러 **대시보드**가 보입니다. **인프라 > 클라우드**를 선택하고 **Custom-Cloud**에 대한 컨트롤러의 상태가 녹색인지 확인합니다. 종종 컨트롤러가 vCenter Server 환경의 모든 포트 그룹을 검색할 때까지 상태가 잠시 노란색으로 표시되었다가 녹색으로 바뀔 수 있습니다.

라이선스 추가

NSX Advanced Load Balancer를 구성하고 나면 여기에 라이선스를 추가해야 합니다. 컨트롤러는 Enterprise 버전 라이선스에 해당하는 모든 기능을 사용할 수 있는 평가 모드로 부팅됩니다. 평가 기간이 만료되기 전에 유효한 Enterprise Tier 라이선스를 컨트롤러에 할당해야 합니다.

사전 요구 사항

Enterprise Tier 라이선스가 있는지 확인합니다.

절차

- 1 NSX Advanced Load Balancer 컨트롤러 대시보드에서 **관리 > 라이선싱**을 선택합니다.
- 2 **설정**을 선택합니다.
- 3 **Enterprise Tier**를 선택합니다.

4 **저장**을 클릭합니다.

5 라이선스를 추가하려면 **컴퓨터에서 업로드**를 선택합니다.

라이선스 파일이 업로드되면 컨트롤러 라이선스 목록에 파일이 나타납니다. 시작 날짜 및 만료 날짜를 포함하여 라이선스에 대한 정보가 표시됩니다.

컨트롤러에 인증서 할당

보안 통신을 설정하려면 컨트롤러가 클라이언트에 인증서를 보내야 합니다. 이 인증서에서 NSX Advanced Load Balancer 컨트롤러 클러스터 호스트 이름 또는 IP 주소와 일치하는 **SAN(주체 대체 이름)**이 있어야 합니다.

컨트롤러에는 기본 자체 서명된 인증서가 있습니다. 하지만 이 인증서에는 올바른 SAN이 없습니다. 이 인증서를 올바른 SAN이 있는 유효한 인증서 또는 자체 서명된 인증서로 교체해야 합니다. 자체 서명된 인증서를 생성하거나 외부 인증서를 업로드합니다.

인증서에 대한 자세한 내용은 [Avi 설명서](#)를 참조하십시오.

절차

1 컨트롤러 대시보드에서 왼쪽 상단 모서리에 있는 메뉴를 클릭하고 **템플릿 > 보안**을 선택합니다.

2 **SSL/TLS 인증서**를 선택합니다.

3 인증서를 생성하려면 **생성**을 클릭하고 **컨트롤러 인증서**를 선택합니다.

새 인증서(SSL/TLS) 창이 나타납니다.

4 인증서의 이름을 입력합니다.

5 미리 생성된 유효한 인증서가 없는 경우 **유형**을 *Self Signed*로 선택하여 자체 서명된 인증서를 추가합니다.

a 다음과 같은 세부 정보를 입력합니다.

옵션	설명
일반 이름	사이트의 정규화된 이름을 지정합니다. 사이트가 신뢰할 수 있는 사이트로 간주되려면 이 항목이 클라이언트가 브라우저에 입력한 호스트 이름과 일치해야 합니다.
알고리즘	EC(타원 곡선) 암호화 또는 RSA를 선택합니다. EC가 권장됩니다.
키 크기	핸드셰이크에 사용할 암호화 수준을 선택합니다. <ul style="list-style-type: none"> ■ SECP256R1은 EC 인증서에 사용됩니다. ■ 2048비트는 RSA 인증서에 권장됩니다.

b **SAN(대체 이름)**에서 **추가**를 클릭합니다.

- c Avi 컨트롤러가 단일 노드로 배포된 경우 클러스터 IP 주소나 FQDN 또는 둘 다를 입력합니다. IP 주소 또는 FQDN만 사용되는 경우 배포 중에 지정한 컨트롤러 VM의 IP 주소와 일치해야 합니다.

NSX Advanced Load Balancer 컨트롤러 배포의 내용을 참조하십시오.

NSX Advanced Load Balancer 컨트롤러 클러스터가 3개의 노드로 구성된 클러스터로 배포된 경우 클러스터 IP 또는 FQDN을 입력합니다. 3개의 컨트롤러 노드로 구성된 클러스터를 배포하는 방법에 대한 자세한 내용은 [컨트롤러 클러스터 배포](#) 항목을 참조하십시오.

- d **저장**을 클릭합니다.

워크로드 관리 기능을 사용하도록 감독자를 구성할 때 이 인증서가 필요합니다.

6 생성한 자체 서명된 인증서를 다운로드합니다.

- a **보안 > SSL/TLS 인증서**를 선택합니다.

인증서가 표시되지 않으면 페이지를 새로 고칩니다.

- b 생성한 인증서를 선택하고 다운로드 아이콘을 클릭합니다.

- c **인증서 내보내기** 페이지가 나타나면 인증서에 대해 **클립보드에 복사**를 클릭합니다. 키를 복사하지 마십시오.

- d 나중에 워크로드 관리를 사용하도록 설정할 때 사용할 수 있도록 복사한 인증서를 저장합니다.

7 미리 생성된 유효한 인증서가 있는 경우 유형을 Import로 선택하여 업로드합니다.

- a **인증서**에서 **파일 업로드**를 클릭하고 인증서를 가져옵니다.

업로드한 인증서의 SAN 필드에는 컨트롤러의 클러스터 IP 주소 또는 FQDN이 있어야 합니다.

참고 인증서의 콘텐츠를 한 번만 업로드하거나 붙여넣어야 합니다.

- b **키(PEM) 또는 PKCS12**에서 **파일 업로드**를 클릭하고 키를 가져옵니다.

- c **유효성 검사**를 클릭하여 인증서와 키의 유효성을 검사합니다.

- d **저장**을 클릭합니다.

8 포털 인증서를 변경하려면 다음 단계를 수행합니다.

- a 컨트롤러 대시보드에서 **관리 > 시스템 설정**을 선택합니다.

- b **편집**을 클릭합니다.

- c **액세스** 탭을 선택합니다.

- d **SSL/TLS 인증서**에서 기존 기본 포털 인증서를 제거합니다.

- e 드롭다운에서 새로 생성 또는 업로드된 인증서를 선택합니다.

- f **기본 인증**을 선택합니다.

- g **저장**을 클릭합니다.

서비스 엔진 그룹 구성

vSphere IaaS control plane는 **기본 그룹** 서비스 엔진 그룹을 사용합니다. 필요한 경우 vCenter 내 서비스 엔진 VM의 수와 배치를 정의하는 그룹 내에서 **기본 그룹** 서비스 엔진을 구성할 수 있습니다. NSX Advanced Load Balancer 컨트롤러가 Enterprise 모드에 있는 경우에도 고가용성을 구성할 수 있습니다. vSphere IaaS control plane는 **기본 그룹** 서비스 엔진만 지원합니다. 다른 서비스 엔진 그룹은 생성할 수 없습니다.

페일오버가 발생할 경우 초과 용량을 프로비저닝하는 방법에 대한 자세한 내용은 [Avi 설명서](#)를 참조하십시오.

절차

- 1 NSX Advanced Load Balancer 컨트롤러 대시보드에서 **인프라 > 클라우드 리소스 > 서비스 엔진 그룹**을 선택합니다.

- 2 **서비스 엔진 그룹** 페이지에서 **기본 그룹**의 편집 아이콘을 클릭합니다.

일반 설정 탭이 나타납니다.

vSphere IaaS control plane는 **기본 클라우드**만 지원합니다.

- 3 **배치** 섹션에서 **고가용성 모드**를 선택합니다.

기본 옵션은 N + M (buffer)입니다. 기본값을 유지하거나 다음 옵션 중 하나를 선택할 수 있습니다.

- Active/Standby
- Active/Active

- 4 **서비스 엔진** 섹션에서 서비스 엔진 그룹에 대한 초과 용량을 구성할 수 있습니다.

서비스 엔진 수 옵션은 서비스 엔진 그룹 내에서 생성될 수 있는 최대 서비스 엔진 수를 정의합니다. 기본값은 10입니다.

초과 용량을 구성하려면 **버퍼 서비스 엔진**에 값을 지정합니다. 지정하는 값은 페일오버가 발생할 경우 초과 용량을 보장하기 위해 배포되는 VM의 수입니다.

기본값은 1입니다.

- 5 **가상 서비스** 섹션에서 다음 옵션을 구성합니다.

옵션	설명
서비스 엔진당 가상 서비스	컨트롤러 클러스터가 그룹의 서비스 엔진 중 하나에 배치할 수 있는 최대 가상 서비스 수입니다. 값 1000을 입력합니다.
서비스 엔진 전반의 가상 서비스 배치	분산 을 선택합니다. 이 옵션을 선택하면 새로 가동된 서비스 엔진에 가상 서비스를 지정된 최대 서비스 엔진 수까지 배치하여 성능을 최대화합니다. 기본값은 컴팩트 입니다.

- 6 다른 설정에 대해서는 기본값을 유지할 수 있습니다.

- 7 **저장**을 클릭합니다.

정적 경로 구성

기본 게이트웨이를 사용하면 서비스 엔진이 워크로드 네트워크의 풀 서버로 트래픽을 라우팅할 수 있습니다. 데이터 네트워크 게이트웨이 IP를 기본 게이트웨이로 구성해야 합니다. 서비스 엔진은 데이터 네트워크의 DHCP에서 기본 게이트웨이 IP를 가져오지 않습니다. 서비스 엔진이 트래픽을 워크로드 네트워크 및 클라이언트 IP로 올바르게 라우팅할 수 있도록 정적 경로를 구성해야 합니다.

절차

- 1 NSX Advanced Load Balancer 컨트롤러 대시보드에서 **인프라 > 클라우드 리소스 > VRF 컨텍스트**를 선택합니다.
- 2 **생성**을 클릭합니다.
- 3 **일반** 설정에서 라우팅 컨텍스트의 이름을 입력합니다.
- 4 **정적 경로** 섹션에서 **추가**를 클릭합니다.
- 5 **게이트웨이 서브넷**에 172.16.10.0/24을 입력합니다.
- 6 **다음 홉**에 데이터 네트워크의 게이트웨이 IP 주소를 입력합니다.
예: 192.168.1.1
- 7 (선택 사항) **BGP 피어링**을 선택하여 BGP 로컬 및 피어 세부 정보를 구성합니다.
자세한 내용은 [Avi 설명서](#)를 참조하십시오.
- 8 **저장**을 클릭합니다.

가상 IP 네트워크 구성

데이터 네트워크에 대한 VIP(가상 IP) 서브넷을 구성합니다. 가상 서비스가 특정 VIP 네트워크에 배치될 때 사용할 VIP 범위를 구성할 수 있습니다. 서비스 엔진에 대해 DHCP를 구성할 수 있습니다. 필요한 경우, DHCP를 사용할 수 없으면 해당 네트워크의 서비스 엔진 인터페이스에 할당될 IP 주소 풀을 구성할 수 있습니다. vSphere IaaS control plane는 단일 VIP 네트워크만 지원합니다.

절차

- 1 NSX Advanced Load Balancer 컨트롤러 대시보드에서 **인프라 > 클라우드 리소스 > 네트워킹**을 선택합니다.
- 2 목록에서 클라우드를 선택합니다.
예를 들어 **기본 클라우드**를 선택합니다.
- 3 네트워크의 이름을 입력합니다.
예를 들면 Data Network입니다.
- 4 데이터 네트워크에서 DHCP를 사용할 수 있는 경우 **DHCP 사용**을 선택한 상태로 유지합니다.
DHCP를 사용할 수 없는 경우 이 옵션을 선택 취소합니다.

5 IPv6 자동 구성 사용을 선택합니다.

NSX Advanced Load Balancer 컨트롤러는 VM이 네트워크에서 실행 중인 경우 네트워크 CIDR을 자동으로 검색하고 **검색됨** 유형으로 표시합니다.

6 NSX Advanced Load Balancer 컨트롤러가 IP 서브넷을 자동으로 검색하는 경우 서브넷의 IP 범위를 구성합니다.

- a 설정을 편집합니다.
- b **서브넷 접두사**를 입력합니다.
- c 서비스 엔진 IP 주소에 대해 DHCP를 사용할 수 있는 경우 **VIP 및 SE에 정적 IP 주소 사용**을 선택 취소합니다.
- d 하나 이상의 IP 주소 또는 IP 주소 범위를 입력합니다.

예를 들면 10.202.35.1-10.202.35.254입니다.

참고 0으로 끝나는 IP 주소를 입력할 수 있습니다. 예를 들어 192.168.0.0를 입력하고 경고가 표시되면 무시합니다.

- e **저장**을 클릭합니다.

7 컨트롤러에서 IP 서브넷과 해당 유형이 검색되지 않으면 다음 단계를 수행합니다.

- a **추가**를 클릭합니다.
- b **서브넷 접두사**를 입력합니다.
- c **추가**를 클릭합니다.
- d 서비스 엔진 IP 주소에 대해 DHCP를 사용할 수 있는 경우 **VIP 및 SE에 정적 IP 주소 사용**을 선택 취소합니다.
- e **IP 주소**에서 가상 IP 주소를 제공하는 네트워크의 CIDR을 입력합니다.

예를 들어 10.202.35.0/22입니다.

- f 하나 이상의 IP 주소 또는 IP 주소 범위를 입력합니다.

범위는 **IP 서브넷**에 있는 네트워크 CIDR의 하위 집합이어야 합니다. 예를 들면 10.202.35.1-10.202.35.254입니다.

참고 0으로 끝나는 IP 주소를 입력할 수 있습니다. 예를 들어 192.168.0.0를 입력하고 경고가 표시되면 무시합니다.

- g **저장**을 클릭하여 서브넷 구성을 저장합니다.

네트워크 페이지에 **구성됨** 유형의 IP 서브넷과 IP 주소 풀이 나열됩니다.

8 **저장**을 클릭하여 네트워크 설정을 저장합니다.

결과

네트워크 페이지에 구성된 네트워크가 나열됩니다.

예

Primary Workload Network 네트워크는 검색된 네트워크를 10.202.32.0/22로 표시하고 구성된 서브넷을 10.202.32.0/22 [254/254]로 표시합니다. 이것은 가상 IP 주소 254개가 10.202.32.0/22에서 할당된다는 것을 나타냅니다. 요약 보기에는 IP 범위 10.202.35.1-10.202.35.254가 나열되지 않습니다.

NSX Advanced Load Balancer 테스트

NSX Advanced Load Balancer 제어부를 배포하고 구성한 후 해당 기능을 검증합니다.

절차

- 1 Avi 컨트롤러 대시보드에서 **인프라 > 클라우드**로 이동합니다.
- 2 **기본 클라우드**에 대한 컨트롤러의 상태가 녹색인지 확인합니다.

문제가 발생할 경우 해결하려면 [NSX Advanced Load Balancer 문제 해결을 위한 지원 번들 수집 항목을 참조하십시오.](#)

HAProxy 로드 밸런서 설치 및 구성

VMware는 vSphere IaaS control plane 환경에서 사용할 수 있는 오픈 소스 HAProxy 로드 밸런서의 구현을 제공합니다. **워크로드 관리**에 vDS(vSphere Distributed Switch) 네트워킹을 사용하는 경우에는 HAProxy 로드 밸런서를 설치하고 구성할 있습니다.

HAProxy 로드 밸런서와 함께 사용할 감독자용 vSphere Distributed Switch 생성

vSphere 클러스터를 vSphere 네트워킹 스택 및 HAProxy 로드 밸런서를 사용하는 감독자로 구성하려면 vSphere Distributed Switch에 호스트를 추가해야 합니다. 감독자에 대한 워크로드 네트워킹으로 구성할 Distributed Switch에서 포트 그룹을 생성해야 합니다.

클러스터에서 실행될 Kubernetes 워크로드에 제공하려는 분리 수준에 따라 감독자에 대해 서로 다른 토폴로지를 선택할 수 있습니다.

사전 요구 사항

- HAProxy 로드 밸런서와 함께 감독자에 vSphere 네트워킹을 사용하기 위한 시스템 요구 사항을 검토합니다. **HA 프록시 로드 밸런서**를 사용하여 3개 영역 감독자를 사용하도록 설정하기 위한 요구 사항 및 **VDS 네트워킹 및 HAProxy 로드 밸런서**에서 단일 클러스터 감독자를 사용하도록 설정하기 위한 요구 사항 "vSphere IaaS 제어부 개념 및 계획" 을 참조하십시오.
- 감독자에서 HAProxy를 사용하여 워크로드 네트워킹을 설정하기 위한 토폴로지를 결정합니다. "vSphere IaaS 제어부 개념 및 계획" 에서 **HAProxy 로드 밸런서 배포를 위한 토폴로지**를 참조하십시오.

절차

- 1 vSphere Client에서 데이터 센터로 이동합니다.
- 2 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 **Distributed Switch > 새 Distributed Switch**를 선택합니다.
- 3 스위치의 이름(예: **Workload Distributed Switch**)을 입력하고 **다음**을 클릭합니다.
- 4 스위치에 대해 버전 7.0을 선택하고 **다음**을 클릭합니다.
- 5 **포트 그룹 이름**에서 **Primary Workload Network**를 입력하고 **다음**을 클릭한 후 **마침**을 클릭합니다.

하나의 포트 그룹이 포함된 새 Distributed Switch가 데이터 센터에 생성됩니다. 이 포트 그룹을 생성할 감독자에 대한 기본 워크로드 네트워크로 사용할 수 있습니다. 기본 워크로드 네트워크는 Kubernetes 제어부 VM에 대한 트래픽을 처리합니다.

- 6 워크로드 네트워크에 대한 분산 포트 그룹을 생성합니다.

생성하는 포트 그룹의 수는 감독자에 대해 구현하려는 토폴로지에 따라 다릅니다. 하나의 분리된 워크로드 네트워크가 있는 토폴로지의 경우 감독자의 모든 네임스페이스에 대한 네트워크로 사용할 하나의 분산 포트 그룹을 생성합니다. 네임스페이스별로 분리된 네트워크가 있는 토폴로지의 경우 생성할 네임스페이스 수와 동일한 수의 포트 그룹을 생성합니다.

- a 새로 생성된 Distributed Switch로 이동합니다.
 - b 스위치를 마우스 오른쪽 버튼으로 클릭하고 **분산 포트 그룹 > 새 분산 포트 그룹**을 선택합니다.
 - c 포트 그룹의 이름(예: **Workload Network**)을 입력하고 **다음**을 클릭합니다.
 - d 기본값을 그대로 두고 **다음**을 클릭한 다음 **마침**을 클릭합니다.
- 7 Distributed Switch에 감독자로 구성할 vSphere 클러스터의 호스트를 추가합니다.
 - a Distributed Switch를 마우스 오른쪽 버튼으로 클릭하고 **호스트 추가 및 관리**를 선택합니다.
 - b **호스트 추가**를 선택합니다.
 - c **새 호스트**를 클릭하고 감독자로 구성할 vSphere 클러스터에서 호스트를 선택한 후 **다음**을 클릭합니다.
 - d 각 호스트에서 물리적 NIC를 선택하고 Distributed Switch에서 여기에 업링크를 할당합니다.
 - e 마법사의 나머지 화면에서 **다음**을 클릭하고 **마침**을 클릭합니다.

결과

호스트가 Distributed Switch에 추가됩니다. 이제 스위치에서 생성한 포트 그룹을 감독자의 워크로드 네트워크로 사용할 수 있습니다.

HAProxy 로드 밸런서 제어부 VM 배포

Kubernetes 워크로드에 vSphere 네트워킹 스택을 사용하려면 HAProxy 제어부 VM을 설치하여 Tanzu Kubernetes 클러스터에 로드 밸런싱 서비스를 제공합니다.

사전 요구 사항

- 환경이 HA Proxy 배포를 위한 계산 및 네트워킹 요구 사항을 충족하는지 확인합니다. HA 프록시 로드 밸런서를 사용하여 3개 영역 감독자를 사용하도록 설정하기 위한 요구 사항 및 VDS 네트워킹 및 HAProxy 로드 밸런서에서 단일 클러스터 감독자를 사용하도록 설정하기 위한 요구 사항 "vSphere IaaS 제어부 개념 및 계획" 을 참조하십시오.
- HAProxy 로드 밸런서를 배포할 vSphere Standard 또는 Distributed Switch에 관리 네트워크가 있는지 확인합니다. 감독자는 이 관리 네트워크의 HAProxy 로드 밸런서와 통신합니다.
- 워크로드 네트워크에 대한 vSphere Distributed Switch 및 포트 그룹을 생성합니다. HAProxy 로드 밸런서는 워크로드 네트워크를 통해 감독자 및 Tanzu Kubernetes 클러스터 노드와 통신합니다. HAProxy 로드 밸런서와 함께 사용할 감독자용 vSphere Distributed Switch 생성의 내용을 참조하십시오. 워크로드 네트워크에 대한 자세한 내용은 "vSphere IaaS 제어부 개념 및 계획" 에서 감독자 클러스터의 워크로드 네트워크를 참조하십시오.
- VMware-HAProxy 사이트에서 최신 버전의 VMware HAProxy OVA 파일을 다운로드합니다.
- 감독자에 HAProxy 로드 밸런서 및 워크로드 네트워크를 배포하기 위한 토폴로지를 선택합니다. "vSphere IaaS 제어부 개념 및 계획" 에서 HAProxy 로드 밸런서 배포를 위한 토폴로지를 참조하십시오.

vDS 네트워킹 및 HAProxy를 통해 vSphere IaaS control plane를 사용하는 방법에 대한 데모를 보는 것이 유용할 수 있습니다. vSphere with Tanzu 사용 시작 비디오를 확인하십시오.

절차

- 1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.
- 2 HAProxy OVA 파일에서 새 VM을 생성합니다.

옵션	설명
컨텐츠 라이브러리	OVA를 로컬 컨텐츠 라이브러리에 가져온 경우: <ul style="list-style-type: none"> ■ 메뉴 > 컨텐츠 라이브러리로 이동합니다. ■ OVA를 가져온 라이브러리를 선택합니다. ■ vmware-haproxy-vX.X.X 템플릿을 선택합니다. ■ 마우스 오른쪽 버튼을 클릭하고 이 템플릿에서 새 VM 생성을 선택합니다.
로컬 파일	OVA 파일을 로컬 호스트에 다운로드한 경우: <ul style="list-style-type: none"> ■ 워크로드 관리를 사용하도록 설정할 vCenter 클러스터를 선택합니다. ■ 마우스 오른쪽 버튼을 클릭하고 OVF 템플릿 배포를 선택합니다. ■ 로컬 파일을 선택하고 파일 업로드를 클릭합니다. ■ vmware-haproxy-vX.X.X.ova 파일을 찾아서 선택합니다.

- 3 가상 시스템 이름(예: haproxy)을 입력합니다.
- 4 HAProxy를 배포할 데이터 센터를 선택하고 다음을 클릭합니다.
- 5 워크로드 관리를 사용하도록 설정할 vCenter 클러스터를 선택하고 다음을 클릭합니다.
- 6 배포 세부 정보를 검토 및 확인하고 다음을 클릭합니다.

- 7 라이선스 계약에 동의하고 **다음**을 클릭합니다.
- 8 배포 구성을 선택합니다. 자세한 내용은 "vSphere IaaS 제어부 개념 및 계획" 에서 **HAProxy 네트워크 토폴로지**를 참조하십시오. 참조하십시오.

구성	설명
기본값	NIC가 2개(관리 네트워크 및 단일 워크로드 네트워크)인 장치를 배포하려면 이 옵션을 선택합니다.
프런트 엔드 네트워크	NIC가 3개인 장치를 배포하려면 이 옵션을 선택합니다. 프런트 엔드 서버넷은 클러스터 노드를 개발자가 클러스터 제어부에 액세스하는 데 사용하는 네트워크에서 분리하는 데 사용됩니다.

- 9 VM에 사용할 스토리지 정책을 선택하고 **다음**을 클릭합니다.
- 10 로드 밸런서에 사용할 네트워크 인터페이스를 선택하고 **다음**을 클릭합니다.

소스 네트워크	대상 네트워크
관리	관리 네트워크(예: VM 네트워크)를 선택합니다.
워크로드	워크로드 관리 를 위해 구성된 vDS 포트 그룹을 선택합니다.
프런트 엔드	프런트 엔드 서버넷에 대해 구성된 vDS 포트 그룹을 선택합니다. 프런트 엔드 구성을 선택하지 않으면 설치 중에 이 설정이 무시되므로 기본값을 그대로 둘 수 있습니다.

참고 워크로드 네트워크는 관리 네트워크와 다른 서버넷에 있어야 합니다. **HA 프록시 로드 밸런서**를 사용하여 3개 영역 감독자를 사용하도록 설정하기 위한 요구 사항 및 **VDS 네트워킹 및 HAProxy 로드 밸런서**에서 단일 클러스터 감독자를 사용하도록 설정하기 위한 요구 사항 "vSphere IaaS 제어부 개념 및 계획" 을 참조하십시오.

- 11 애플리케이션 구성 설정을 사용자 지정합니다. **장치 구성 설정**의 내용을 참조하십시오.
- 12 네트워크 구성 세부 정보를 제공합니다. **네트워크 구성**의 내용을 참조하십시오.
- 13 로드 밸런싱을 구성합니다. **로드 밸런싱 설정**의 내용을 참조하십시오.
- 14 **다음**을 클릭하여 OVA 구성을 완료합니다.
- 15 배포 구성 세부 정보를 검토하고 **마침**을 클릭하여 OVA를 배포합니다.
- 16 **작업** 패널을 사용하여 VM 배포를 모니터링합니다.
- 17 VM 배포가 완료되면 전원을 켭니다.

다음에 수행할 작업

HAProxy 로드 밸런서가 성공적으로 배포되고 전원이 켜지면 **워크로드 관리**를 사용하도록 설정합니다. **장 12 감독자 구성 및 관리**의 내용을 참조하십시오.

HAProxy 로드 밸런서 사용자 지정

구성 설정, 네트워크 설정 및 로드 밸런싱 설정을 포함하여 HAProxy 제어부 VM을 사용자 지정합니다.

장치 구성 설정

이 표에는 HAProxy 장치 구성에 대한 매개 변수가 나열 및 설명되어 있습니다.

매개 변수	설명	주석 또는 예제
루트 암호	루트 사용자의 초기 암호입니다(6~128자).	이후 암호 변경은 운영 체제에서 수행해야 합니다.
루트 로그인 허용	루트 사용자가 SSH를 통해 원격으로 VM에 로그인할 수 있는 옵션입니다.	문제 해결을 위해 루트 로그인이 필요할 수도 있지만, 루트 로그인 허용 시 보안에 미치는 영향을 염두에 두어야 합니다.
TLS CA(인증 기관)(ca.crt)	자체 서명된 CA 인증서를 사용하려면 이 필드를 비워둡니다. 자체 CA 인증서(ca.crt)를 사용하려면 해당 콘텐츠를 이 필드에 붙여넣습니다. 콘텐츠를 Base64로 인코딩해야 할 수도 있습니다. https://www.base64encode.org/	자체 서명된 CA 인증서를 사용하는 경우 인증서에서 공용 및 개인 키가 생성됩니다.
키(ca.key)	자체 서명된 인증서를 사용하는 경우에는 이 필드를 비워둡니다. CA 인증서를 제공한 경우, 인증서 개인 키의 콘텐츠를 이 필드에 붙여넣습니다.	

네트워크 구성

이 표에는 HAProxy 네트워크 구성에 대한 매개 변수가 나열 및 설명되어 있습니다.

매개 변수	설명	주석 또는 예제
호스트 이름	HAProxy 제어부 VM에 할당할 호스트 이름 (또는 FQDN)	기본값: haproxy.local
DNS	심표로 구분된 DNS 서버 IP 주소 목록입니다.	기본값: 1.1.1.1, 1.0.0.1 예제 값: 10.8.8.8
관리 IP	관리 네트워크에 있는 HAProxy 제어부 VM의 정적 IP 주소입니다.	네트워크의 접두사 길이가 있는 유효한 IPv4 주소(예: 192.168.0.2/24)입니다.
관리 게이트웨이	관리 네트워크에 대한 게이트웨이의 IP 주소입니다.	예:192.168.0.1
워크로드 IP	워크로드 네트워크에 있는 HAProxy 제어부 VM의 정적 IP 주소입니다. 이 IP 주소는 로드 밸런서 IP 주소 범위 밖에 있어야 합니다.	네트워크의 접두사 길이가 있는 유효한 IPv4 주소(예: 192.168.10.2/24)입니다.
워크로드 게이트웨이	워크로드 네트워크에 대한 게이트웨이의 IP 주소입니다.	예:192.168.10.1 프런트 엔드 구성을 선택하는 경우 게이트웨이를 입력해야 합니다. 프런트 엔드를 선택하고 게이트웨이를 지정하지 않으면 배포가 성공하지 못합니다.

매개 변수	설명	주석 또는 예제
프런트 엔드 IP	프런트 엔드 네트워크에 있는 HAProxy 장치의 정적 IP 주소입니다. 이 값은 프런트 엔드 배포 모델을 선택한 경우에만 사용됩니다.	네트워크의 접두사 길이가 있는 유효한 IPv4 주소(예: 192.168.100.2/24)입니다.
프런트 엔드 게이트웨이	프런트 엔드 네트워크에 대한 게이트웨이의 IP 주소입니다. 이 값은 프런트 엔드 배포 모델을 선택한 경우에만 사용됩니다.	예:192.168.100.1

로드 밸런싱 설정

이 표에는 HAProxy 로드 밸런서 구성에 대한 매개 변수가 나열 및 설명되어 있습니다.

매개 변수	설명	예제 또는 주석
로드 밸런서 IP 범위	이 필드에는 CIDR 형식을 사용하여 IPv4 주소의 범위를 지정합니다. 값은 유효한 CIDR 범위여야 합니다. 그렇지 않으면 설치에 실패합니다. HAProxy는 VIP(가상 IP)에 대한 IP 주소를 예약합니다. 할당되면 각 VIP 주소가 할당되고 HAProxy는 해당 주소에 대한 요청에 응답합니다. 여기서 지정하는 CIDR 범위는 vSphere Client를 사용하여 vCenter Server에서 워크로드 관리 를 사용하도록 설정할 때 가상 서버에 할당하는 IP와 겹치지 않아야 합니다. 참고 로드 밸런서 IP 범위는 관리 네트워크와 다른 서브넷에 있어야 합니다. 로드 밸런서 IP 범위를 관리 네트워크와 동일한 서브넷에 두는 것은 지원되지 않습니다.	예를 들어 네트워크 CIDR 192.168.100.0/24는 로드 밸런서에 범위가 192.168.100.0 - 192.168.100.255인 256개의 가상 IP 주소를 제공합니다. 예를 들어 네트워크 CIDR 192.168.100.0/25는 로드 밸런서에 범위가 192.168.100.0 - 192.168.100.127인 128개의 가상 IP 주소를 제공합니다.
Dataplane API 관리 포트	로드 밸런서의 API 서비스가 수신 대기하는 HAProxy VM의 포트입니다.	유효한 포트. 포트 22는 SSH용으로 예약되어 있습니다. 기본값은 5556입니다.
HAProxy 사용자 ID	로드 밸런서 API 사용자 이름	클라이언트가 로드 밸런서의 API 서비스에 인증하는 데 사용하는 사용자 이름입니다. 참고 이 사용자 이름은 감독자를 사용하도록 설정할 때 필요합니다.
HAProxy 암호	로드 밸런서 API 암호	클라이언트가 로드 밸런서의 API 서비스에 인증하는 데 사용하는 암호입니다. 참고 이 암호는 감독자를 사용하도록 설정할 때 필요합니다.

3개 영역 감독자 배포

5

3개 vSphere 영역에서 감독자를 배포하여 클러스터 수준 고가용성을 제공합니다. 각 vSphere 영역은 vSphere 클러스터에 매핑됩니다.

참고 vSphere IaaS control plane 환경을 8.0 이전의 vSphere 버전에서 업그레이드했으며 Tanzu Kubernetes Grid 클러스터와 같은 배포에 vSphere 영역을 사용하려는 경우 새로운 3개 영역 감독자를 생성해야 합니다.

다음으로 아래 항목을 읽으십시오.

- [VDS 네트워킹 스택을 사용하여 3개 영역 감독자 배포](#)
- [NSX 네트워킹을 사용하여 3개 영역 감독자 배포](#)

VDS 네트워킹 스택을 사용하여 3개 영역 감독자 배포

3개 vSphere 영역에 VDS 네트워킹 스택을 사용하여 감독자를 배포하는 방법을 알아봅니다. 각 vSphere 영역은 1개 vSphere 클러스터에 매핑됩니다. 3개 vSphere 영역에 감독자를 배포하면 클러스터 수준에서 워크로드에 고가용성을 제공할 수 있습니다. VDS 네트워킹으로 구성된 감독자는 VM 서비스를 통해 생성된 Tanzu Kubernetes Grid 클러스터 및 VM을 지원합니다. vSphere 포드는 지원하지 않습니다.

사전 요구 사항

- vSphere 클러스터를 감독자로 구성하기 위한 사전 요구 사항을 완료합니다. [vSphere 클러스터에서 vSphere IaaS control plane](#)를 구성하기 위한 사전 요구 사항의 내용을 참조하십시오.
- 3개의 vSphere 영역을 생성합니다. [장 3 다중 영역 감독자 배포를 위한 vSphere 영역 생성](#)의 내용을 참조하십시오.

절차

- 1 홈 메뉴에서 **워크로드 관리**를 선택합니다.
- 2 감독자에 대한 라이선싱 옵션을 선택합니다.
 - 유효한 Tanzu Edition 라이선스가 있는 경우 **라이선스 추가**를 클릭하여 vSphere 라이선스 인벤토리에 라이선스 키를 추가합니다.

- Tanzu Edition 라이선스가 아직 없는 경우에는 VMware에서 통신을 받을 수 있도록 연락처 세부 정보를 입력하고 **시작**을 클릭합니다.

감독자의 평가 기간은 60일 동안 지속됩니다. 이 기간 내에는 클러스터에 유효한 Tanzu Edition 라이선스를 할당해야 합니다. Tanzu Edition 라이선스 키를 추가한 경우 감독자 설정을 완료하면 60일 평가 기간 내에 해당 키를 할당할 수 있습니다.

- 3 **워크로드 관리** 화면에서 **시작**을 다시 클릭합니다.
- 4 **vCenter Server 및 네트워크** 페이지를 선택하고 감독자 배포를 위해 설정된 vCenter Server 시스템을 선택하고 네트워킹 스택으로 **VDS(vSphere Distributed Switch)**를 선택하고 **다음**을 클릭합니다.
- 5 **감독자 위치** 페이지에서 **vSphere 영역 배포**를 선택하여 3개의 vSphere 영역에 감독자를 배포합니다.
 - a 새 감독자의 이름을 입력합니다.
 - b 감독자 배포를 위해 vSphere 영역을 생성한 데이터 센터를 선택합니다.
 - c 호환되는 vSphere 영역 목록에서 3개의 영역을 선택합니다.
 - d **다음**을 클릭합니다.
- 6 **스토리지** 페이지에서 제어부 VM 배치를 위한 스토리지를 구성합니다.

옵션	설명
제어부 노드	제어부 VM 배치에 대한 스토리지 정책을 선택합니다.

7 로드 밸런서 화면에서 로드 밸런서에 대한 설정을 구성합니다.

- a 로드 밸런서의 이름을 입력합니다.
- b 로드 밸런서 유형을 선택합니다.

NSX Advanced Load Balancer 및 **HAProxy** 중에서 선택할 수 있습니다.

c 로드 밸런서에 대한 설정 구성

- NSX Advanced Load Balancer에 대해 다음 설정을 입력합니다.

옵션	설명
이름	NSX Advanced Load Balancer의 이름을 입력합니다.
NSX Advanced Load Balancer 컨트롤러 끝점	NSX Advanced Load Balancer 컨트롤러의 IP 주소입니다. 기본 포트는 443입니다.
사용자 이름	NSX Advanced Load Balancer을 사용하여 구성된 사용자 이름입니다. 이 사용자 이름을 사용하여 컨트롤러에 액세스합니다.
암호	사용자 이름에 대한 암호입니다.
서버 인증서	컨트롤러에 사용되는 인증서입니다. 구성 중에 할당한 인증서를 제공할 수 있습니다. 자세한 내용은 컨트롤러에 인증서 할당 의 내용을 참조하십시오.
클라우드 이름	설정된 사용자 지정 클라우드의 이름을 입력합니다. 클라우드는 대/소문자를 구분합니다. 기본 클라우드 를 사용하려면 이 필드를 비워 둡니다. 자세한 내용은 컨트롤러 구성 의 내용을 참조하십시오.

- HAProxy에 대한 다음 설정을 입력합니다.

옵션	설명
HAProxy 로드 밸런서 컨트롤러 끝점	HAProxy 장치의 관리 IP 주소인 HAProxy 데이터부 API의 IP 주소 및 포트입니다. 이 구성 요소는 HAProxy 서버를 제어하고 HAProxy VM 내에서 실행됩니다.
사용자 이름	HAProxy OVA 파일을 사용하여 구성된 사용자 이름입니다. 이 이름을 사용하여 HAProxy 데이터부 API를 인증합니다.
암호	사용자 이름에 대한 암호입니다.
가상 IP 범위	Tanzu Kubernetes 클러스터가 워크로드 네트워크에서 사용하는 IP 주소 범위입니다. 이 IP 범위는 HAProxy 장치 배포 중에 구성된 CIDR에 정의된 IP 목록에서 가져옵니다. HAProxy 배포에 구성된 전체 범위를 설정할 수 있지만 여러 감독자를 생성하고 해당 CIDR 범위의 IP를 사용하려는 경우

옵션	설명
	<p>해당 CIDR의 하위 집합을 설정할 수도 있습니다. 이 범위는 마법사에서 워크로드 네트워크에 대해 정의된 IP 범위와 겹치지 않아야 합니다. 또한 범위는 이 워크로드 네트워크의 DHCP 범위와 겹치지 않아야 합니다.</p>
<p>HAProxy 관리 TLS 인증서</p>	<p>데이터부 API가 제공하는 서버 인증서의 신뢰할 수 있는 루트이거나 서명된 PEM 형식의 인증서입니다.</p> <ul style="list-style-type: none"> ■ 옵션 1: 루트 액세스를 사용하도록 설정된 경우 SSH를 사용하여 HAProxy VM에 루트로 연결하고 <code>/etc/haproxy/ca.crt</code>를 서버 CA(인증 기관)에 복사합니다. <code>\n</code> 형식으로 이스케이프 줄을 사용하지 마십시오. ■ 옵션 2: HAProxy VM을 마우스 오른쪽 버튼으로 클릭하고 설정 편집을 선택합니다. 해당 필드에서 CA 인증서를 복사한 후 https://www.base64decode.org/와 같은 변환 도구를 사용하여 Base64에서 변환합니다. ■ 옵션 3: 다음 PowerCLI 스크립트를 실행합니다. <code>\$vc</code>, <code>\$vc_user</code>, <code>\$vc_password</code> 변수를 적절한 값으로 바꿉니다. <pre> \$vc = "10.21.32.43" \$vc_user = "administrator@vsphere.local" \$vc_password = "PASSWORD" Connect-VIServer -User \$vc_user -Password \$vc_password -Server \$vc \$VMname = "haproxy-demo" \$AdvancedSettingName = "guestinfo.dataplaneapi.cacert" \$Base64cert = get-vm \$VMname Get- AdvancedSetting -Name \$AdvancedSettingName while ([string]::IsNullOrEmpty(\$Base64cert .Value)) { Write-Host "Waiting for CA Cert Generation... This may take a under 5-10 minutes as the VM needs to boot and generate the CA Cert (if you haven't provided one already)." \$Base64cert = get-vm \$VMname Get-AdvancedSetting -Name \$AdvancedSettingName Start-sleep -seconds 2 } Write-Host "CA Cert Found... Converting from BASE64" \$cert = [Text.Encoding]::Utf8.GetString([Con vert]::FromBase64String(\$Base64cert. Value)) Write-Host \$cert </pre>

8 관리 네트워크 화면에서 Kubernetes 제어부 VM에 사용될 네트워크에 대한 매개 변수를 구성합니다.

a 네트워크 모드를 선택합니다.

- **DHCP 네트워크.** 이 모드에서는 관리 네트워크의 모든 IP 주소(예: 제어부 VM IP, 부동 IP, DNS 서버, DNS, 검색 도메인 및 NTP 서버)가 DHCP 서버에서 자동으로 획득됩니다. 부동 IP를 얻으려면 DHCP 서버는 클라이언트 식별자를 지원하도록 구성되어야 합니다. DHCP 모드에서 모든 제어부 VM은 안정적인 DHCP 클라이언트 식별자를 사용하여 IP 주소를 획득합니다. 이러한 클라이언트 식별자는 DHCP 서버에서 제어부 VM의 IP에 대한 정적 IP 할당을 설정하여 변경되지 않도록 하는 데 사용할 수 있습니다. 제어부 VM의 IP 및 부동 IP를 변경하는 것은 지원되지 않습니다.

이러한 설정의 텍스트 필드에 값을 입력하여 DHCP에서 상속된 일부 설정을 재정의할 수 있습니다.

옵션	설명
네트워크	감독자에 대한 관리 트래픽을 처리할 네트워크를 선택합니다.
부동 IP	다음과 같이 Kubernetes 제어부 VM에 대해 5개의 연속 IP 주소를 예약하기 위한 시작 지점을 결정하는 IP 주소를 입력합니다. <ul style="list-style-type: none"> ■ Kubernetes 제어부 VM 각각에 대한 IP 주소입니다. ■ 관리 네트워크에 대한 인터페이스로 제공할 Kubernetes 제어부 VM 중 하나에 대한 부동 IP 주소입니다. 부동 IP 주소가 할당된 제어부 VM은 세 개의 Kubernetes 제어부 VM 모두에 대해 선행 VM으로 작동합니다. 부동 IP는 Kubernetes 클러스터의 etcd 리더인 제어부 노드로 이동합니다. 그러면 네트워크 파티션 이벤트의 경우 가용성이 향상됩니다. ■ Kubernetes 제어부 VM이 실패하여 새로운 제어부 VM으로 교체하는 경우 버퍼 역할을 하는 IP 주소입니다.
DNS 서버	환경에서 사용하는 DNS 서버의 주소를 입력합니다. vCenter Server 시스템이 FQDN으로 등록되어 있으면 vSphere 환경에 사용하는 DNS 서버의 IP 주소를 입력해야 합니다. 그래야 감독자에서 FQDN을 확인할 수 있습니다.
DNS 검색 도메인	Kubernetes 제어부 노드 내에서 DNS가 검색하는 도메인 이름(예: <code>corp.local</code>)을 입력합니다. 그래야 DNS 서버가 확인할 수 있습니다.
NTP 서버	환경에서 사용하는 NTP 서버의 주소를 입력합니다(있는 경우).

- **정적.** 관리 네트워크에 대한 모든 네트워킹 설정을 수동으로 입력합니다.

옵션	설명
네트워크	감독자에 대한 관리 트래픽을 처리할 네트워크를 선택합니다.
시작 IP 주소	다음과 같이 Kubernetes 제어부 VM에 대해 5개의 연속 IP 주소를 예약하기 위한 시작 지점을 결정하는 IP 주소를 입력합니다. <ul style="list-style-type: none"> ■ Kubernetes 제어부 VM 각각에 대한 IP 주소입니다. ■ 관리 네트워크에 대한 인터페이스로 제공할 Kubernetes 제어부 VM 중 하나에 대한 부동 IP 주소입니다. 부동 IP 주소가 할당된 제어부 VM은 세 개의 Kubernetes 제어부 VM 모두에 대해 선행 VM으로 작동합니다. 부동 IP는 Kubernetes 클러스터의 etcd 리더인 제어부 노드로 이동합니다. 그러면 네트워크 파티션 이벤트의 경우 가용성이 향상됩니다. ■ Kubernetes 제어부 VM이 실패하여 새로운 제어부 VM으로 교체하는 경우 버퍼 역할을 하는 IP 주소입니다.
서브넷 마스크	정적 IP 구성에만 적용됩니다. 관리 네트워크에 대한 서브넷 마스크를 입력합니다. 예를 들어 255.255.255.0입니다.
게이트웨이	관리 네트워크의 게이트웨이를 입력합니다.
DNS 서버	환경에서 사용하는 DNS 서버의 주소를 입력합니다. vCenter Server 시스템이 FQDN으로 등록되어 있으면 vSphere 환경에 사용하는 DNS 서버의 IP 주소를 입력해야 합니다. 그래야 감독자에서 FQDN을 확인할 수 있습니다.
DNS 검색 도메인	Kubernetes 제어부 노드 내에서 DNS가 검색하는 도메인 이름(예: corp.local)을 입력합니다. 그래야 DNS 서버가 확인할 수 있습니다.
NTP 서버	환경에서 사용하는 NTP 서버의 주소를 입력합니다(있는 경우).

b 다음을 클릭합니다.

- 9 **워크로드 네트워크** 페이지에서 감독자에서 실행되는 Kubernetes 워크로드에 대한 네트워킹 트래픽을 처리하는 네트워크에 대한 설정을 입력합니다.

참고 워크로드 네트워크에 대한 네트워킹 설정을 제공하기 위해 DHCP 서버를 사용하도록 선택하는 경우 감독자 구성을 완료하면 새 워크로드 네트워크를 생성할 수 없습니다.

a 네트워크 모드를 선택합니다.

- **DHCP 네트워크.** 이 네트워크 모드에서는 워크로드 네트워크에 대한 모든 네트워킹 설정이 DHCP를 통해 획득됩니다. 다음 설정에 대한 텍스트 필드에 값을 입력하여 DHCP에서 상속된 일부 설정을 재정의할 수도 있습니다.

옵션	설명
Kubernetes 서비스를 위한 내부 네트워크	클러스터 내에서 실행되는 Tanzu Kubernetes 클러스터 및 서비스에 대한 IP 주소 범위를 결정하는 CIDR 표기법을 입력합니다.
포트 그룹	감독자에 대한 기본 워크로드 네트워크로 사용할 포트 그룹을 선택합니다. 기본 네트워크는 Kubernetes 제어부 VM 및 Kubernetes 워크로드 트래픽에 대한 트래픽을 처리합니다. 네트워킹 토폴로지에 따라, 나중에 각 네임스페이스에 네트워크로 사용할 다른 포트 그룹을 할당할 수 있습니다. 이 방법을 통해 감독자의 네임스페이스 간에 계층 2 분리를 제공할 수 있습니다. 네트워크로 할당된 다른 포트 그룹이 없는 네임스페이스는 기본 네트워크를 사용합니다. Tanzu Kubernetes 클러스터는 배포된 네임스페이스에 할당된 네트워크만 사용하거나 해당 네임스페이스에 명시적으로 할당된 네트워크가 없는 경우 기본 네트워크를 사용합니다.
네트워크 이름	네트워크 이름을 입력합니다.
DNS 서버	환경에서 사용하는 DNS 서버의 IP 주소를 입력합니다(있는 경우). 예: 10.142.7.1. DNS 서버의 IP 주소를 입력하면 각 제어부 VM에 정적 경로가 추가됩니다. 이것은 DNS 서버에 대한 트래픽이 워크로드 네트워크를 통과한다는 것을 나타냅니다. 지정하는 DNS 서버가 관리 네트워크와 워크로드 네트워크 간에 공유되는 경우에는 제어부 VM의 DNS 조회가 초기 설정 후 워크로드 네트워크를 통해 라우팅됩니다.
NTP 서버	환경에서 사용하는 NTP 서버의 주소를 입력합니다(있는 경우).

- **정적.** 워크로드 네트워크 설정을 수동으로 구성합니다.

옵션	설명
Kubernetes 서비스를 위한 내부 네트워크	클러스터 내에서 실행되는 Tanzu Kubernetes 클러스터 및 서비스에 대한 IP 주소 범위를 결정하는 CIDR 표기법을 입력합니다.
포트 그룹	<p>감독자에 대한 기본 워크로드 네트워크로 사용할 포트 그룹을 선택합니다.</p> <p>기본 네트워크는 Kubernetes 제어부 VM 및 Kubernetes 워크로드 트래픽에 대한 트래픽을 처리합니다.</p> <p>네트워킹 토폴로지에 따라, 나중에 각 네임스페이스에 네트워크로 사용할 다른 포트 그룹을 할당할 수 있습니다. 이 방법을 통해 감독자의 네임스페이스 간에 계층 2 분리를 제공할 수 있습니다. 네트워크로 할당된 다른 포트 그룹이 없는 네임스페이스는 기본 네트워크를 사용합니다. Tanzu Kubernetes 클러스터는 배포된 네임스페이스에 할당된 네트워크만 사용하거나 해당 네임스페이스에 명시적으로 할당된 네트워크가 없는 경우 기본 네트워크를 사용합니다.</p>
네트워크 이름	네트워크 이름을 입력합니다.
IP 주소 범위	<p>Kubernetes 제어부 VM 및 워크로드의 IP 주소를 할당하기 위한 IP 범위를 입력합니다.</p> <p>이 주소 범위는 감독자 노드를 연결하며, 단일 워크로드 네트워크의 경우 Tanzu Kubernetes 클러스터 노드도 연결합니다. HAProxy에 대한 기본 구성을 사용하는 경우 이 IP 범위는 로드 밸런서 VIP 범위와 겹치지 않아야 합니다.</p>
서브넷 마스크	서브넷 마스크 IP 주소를 입력합니다.
게이트웨이	기본 네트워크의 게이트웨이를 입력합니다.
NTP 서버	환경에서 사용하는 NTP 서버의 주소를 입력합니다(있는 경우).
DNS 서버	<p>환경에서 사용하는 DNS 서버의 IP 주소를 입력합니다(있는 경우).</p> <p>예: 10.142.7.1.</p>

b 다음을 클릭합니다.

- 10 검토 및 확인 페이지에서 위로 스크롤하여 지금까지 구성된 모든 설정을 검토하고 감독자 배포에 대한 고급 설정을 지정합니다.

옵션	설명
감독자 제어부 크기	<p>제어부 VM에 대한 크기 조정을 선택합니다. 제어부 VM의 크기에 따라 감독자에서 실행할 수 있는 워크로드의 양이 결정됩니다. 다음 중에서 선택할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 매우 작음 - CPU 2개, 8GB 메모리, 32GB 스토리지 ■ 작음 - CPU 4개, 16GB 메모리, 32GB 스토리지 ■ 중간- CPU 8개, 16GB 메모리, 32GB 스토리지 ■ 큼 - CPU 16개, 32GB 메모리, 32GB 스토리지 <p>참고 제어부 크기를 선택하면 스케일 업만 가능합니다. 더 작은 크기로 스케일 다운할 수 없습니다.</p>
API 서버 DNS 이름	<p>필요한 경우 감독자 제어부 IP 주소를 사용하는 대신 감독자 제어부에 액세스하는 데 사용할 FQDN을 입력합니다. 입력한 FQDN은 자동으로 생성된 인증서에 포함됩니다. 감독자에 FQDN을 사용하면 로드 밸런서 인증서에서 IP 샌드 지정을 생략할 수 있습니다.</p>
구성 내보내기	<p>입력한 감독자 구성의 값이 포함된 JSON 파일을 내보냅니다.</p> <p>감독자를 다시 배포하거나 유사한 구성으로 새 감독자를 배포하려는 경우 나중에 파일을 수정하고 가져올 수 있습니다.</p> <p>감독자 구성을 내보내면 감독자를 다시 배포할 경우 이 마법사의 모든 구성 값을 새로 입력하는 시간을 절약할 수 있습니다.</p>

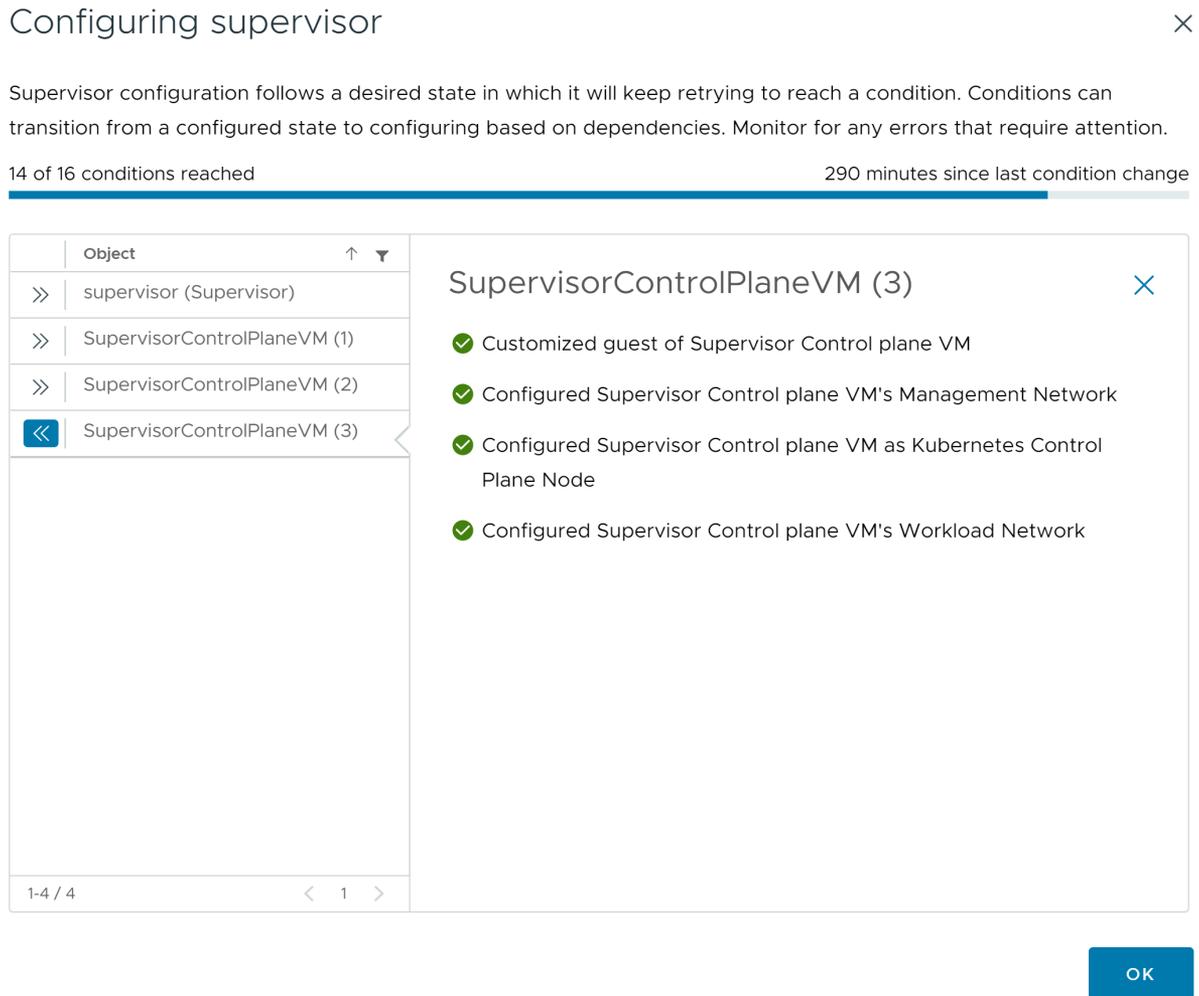
- 11 설정을 검토할 준비가 되면 **마침**을 클릭합니다.

감독자를 사용 설정하면 제어부 VM 및 기타 구성 요소의 생성 및 구성이 시작됩니다.

다음에 수행할 작업

감독자를 사용하도록 설정하는 마법사를 완료하면 활성화 프로세스를 추적하고 문제 해결이 필요한 잠재적인 문제를 관찰할 수 있습니다. **구성 상태** 열에서 **의 상태 옆에 있는** 보기감독자를 클릭합니다.

그림 5-1. 감독자 활성화 보기



배포 프로세스가 완료되려면 감독자가 원하는 상태에 도달해야 합니다. 즉 모든 조건이 충족되어야 합니다. 감독자가 사용되도록 설정하는 데 성공하면 해당 상태가 [구성 중]에서 [실행 중]으로 변경됩니다. 감독자가 [구성 중] 상태에 있는 동안 각 조건에 도달하기 위한 재시도가 계속됩니다. 조건에 도달하지 않으면 성공할 때까지 작업이 재시도됩니다. 이러한 이유로 인해 도달한 조건 수가 오락가락 변경될 수 있습니다(예: "16개 중 10개 조건에 도달" 후 "16개 중 4개 조건에 도달" 등). 매우 드문 경우지만 원하는 상태에 도달하지 못하게 하는 오류가 있는 경우 상태가 오류로 변경될 수 있습니다.

배포 오류 및 문제 해결 방법에 대한 자세한 내용은 [활성화 또는 업데이트 중 감독자 제어부 VM의 오류 상태 해결](#)을 참조하십시오.

마법사에서 입력한 구성 값을 변경하여 감독자를 다시 배포하려는 경우 [장 9 JSON 구성 파일을 가져와서 감독자 배포 항목을 확인](#)하십시오.

NSX 네트워킹을 사용하여 3개 영역 감독자 배포

3개 vSphere 영역에서 NSX를 사용하여 감독자를 배포하는 방법을 알아봅니다. 각 vSphere 영역은 1개 vSphere 클러스터에 매핑됩니다. 3개 vSphere 영역에 감독자를 배포하면 클러스터 수준에서 워크로드에 고가용성을 제공할 수 있습니다. NSX로 구성된 3개 영역 감독자는 Tanzu Kubernetes 클러스터 및 VM만 지원하며 vSphere 포드는 지원하지 않습니다.

NSX 버전 4.1.1 이상을 구성하고 NSX에서 엔터프라이즈 라이선스로 NSX Advanced Load Balancer 버전 22.1.4 이상을 설치, 구성 및 등록한 경우 NSX와 함께 사용되는 로드 밸런서는 NSX Advanced Load Balancer입니다. 4.1.1 이전 버전의 NSX를 구성한 경우 NSX 로드 밸런서가 사용됩니다. 자세한 내용은 [장 7 NSX 네트워킹에 사용되는 로드 밸런서 확인](#) 항목을 참조하십시오.

사전 요구 사항

- vSphere 클러스터를 감독자로 구성하기 위한 사전 요구 사항을 완료합니다. [vSphere 클러스터에서 vSphere IaaS control plane](#)를 구성하기 위한 [사전 요구 사항](#)의 내용을 참조하십시오.
- 3개의 vSphere 영역을 생성합니다. [장 3 다중 영역 감독자 배포를 위한 vSphere 영역 생성](#)의 내용을 참조하십시오.

절차

- 1 홈 메뉴에서 **워크로드 관리**를 선택합니다.
- 2 감독자에 대한 라이선싱 옵션을 선택합니다.
 - 유효한 Tanzu Edition 라이선스가 있는 경우 **라이선스 추가**를 클릭하여 vSphere 라이선스 인벤토리에 라이선스 키를 추가합니다.
 - Tanzu Edition 라이선스가 아직 없는 경우에는 VMware에서 통신을 받을 수 있도록 연락처 세부 정보를 입력하고 **시작**을 클릭합니다.

감독자의 평가 기간은 60일 동안 지속됩니다. 이 기간 내에는 클러스터에 유효한 Tanzu Edition 라이선스를 할당해야 합니다. Tanzu Edition 라이선스 키를 추가한 경우 감독자 설정을 완료하면 60일 평가 기간 내에 해당 키를 할당할 수 있습니다.

- 3 **워크로드 관리** 화면에서 **시작**을 다시 클릭합니다.
- 4 **vCenter Server 및 네트워크** 페이지에서 감독자 배포용으로 설정된 vCenter Server 시스템을 선택하고 **NSX**를 네트워킹 스택으로 선택합니다.
- 5 **다음**을 클릭합니다.
- 6 **감독자 위치** 페이지에서 **vSphere 영역 배포**를 선택하여 3개의 vSphere 영역에 감독자를 배포합니다.
 - a 새 감독자의 이름을 입력합니다.
 - b 감독자 배포를 위해 vSphere 영역을 생성한 데이터 센터를 선택합니다.
 - c 호환되는 vSphere 영역 목록에서 3개의 영역을 선택합니다.
 - d **다음**을 클릭합니다.

7 감독자에 대한 스토리지 정책을 선택합니다.

옵션	설명
제어부 스토리지 정책	제어부 VM 배치에 대한 스토리지 정책을 선택합니다.
사용 후 삭제 디스크 스토리지 정책	이 옵션은 사용하지 않도록 설정됩니다. 3개 영역 감독자에서는 vSphere 포드가 지원되지 않기 때문입니다.
이미지 캐시 스토리지 정책	이 옵션은 사용하지 않도록 설정됩니다. 3개 영역 감독자에서는 vSphere 포드가 지원되지 않기 때문입니다.

8 다음을 클릭합니다.

9 관리 네트워크 화면에서 Kubernetes 제어부 VM에 사용될 네트워크에 대한 매개 변수를 구성합니다.

a 네트워크 모드를 선택합니다.

- **DHCP 네트워크.** 이 모드에서는 관리 네트워크의 모든 IP 주소(예: 제어부 VM IP, 부동 IP, DNS 서버, DNS, 검색 도메인 및 NTP 서버)가 DHCP 서버에서 자동으로 획득됩니다. 부동 IP를 얻으려면 DHCP 서버는 클라이언트 식별자를 지원하도록 구성되어야 합니다. DHCP 모드에서 모든 제어부 VM은 안정적인 DHCP 클라이언트 식별자를 사용하여 IP 주소를 획득합니다. 이러한 클라이언트 식별자는 DHCP 서버에서 제어부 VM의 IP에 대한 정적 IP 할당을 설정하여 변경되지 않도록 하는 데 사용할 수 있습니다. 제어부 VM의 IP 및 부동 IP를 변경하는 것은 지원되지 않습니다.

이러한 설정의 텍스트 필드에 값을 입력하여 DHCP에서 상속된 일부 설정을 재정의할 수 있습니다.

옵션	설명
네트워크	감독자에 대한 관리 트래픽을 처리할 네트워크를 선택합니다.
부동 IP	다음과 같이 Kubernetes 제어부 VM에 대해 5개의 연속 IP 주소를 예약하기 위한 시작 지점을 결정하는 IP 주소를 입력합니다. <ul style="list-style-type: none"> ■ Kubernetes 제어부 VM 각각에 대한 IP 주소입니다. ■ 관리 네트워크에 대한 인터페이스로 제공할 Kubernetes 제어부 VM 중 하나에 대한 부동 IP 주소입니다. 부동 IP 주소가 할당된 제어부 VM은 세 개의 Kubernetes 제어부 VM 모두에 대해 선행 VM으로 작동합니다. 부동 IP는 Kubernetes 클러스터의 etcd 리더인 제어부 노드로 이동합니다. 그러면 네트워크 파티션 이벤트의 경우 가용성이 향상됩니다. ■ Kubernetes 제어부 VM이 실패하여 새로운 제어부 VM으로 교체하는 경우 버퍼 역할을 하는 IP 주소입니다.
DNS 서버	환경에서 사용하는 DNS 서버의 주소를 입력합니다. vCenter Server 시스템이 FQDN으로 등록되어 있으면 vSphere 환경에 사용하는 DNS 서버의 IP 주소를 입력해야 합니다. 그래야 감독자에서 FQDN을 확인할 수 있습니다.
DNS 검색 도메인	Kubernetes 제어부 노드 내에서 DNS가 검색하는 도메인 이름(예: <code>corp.local</code>)을 입력합니다. 그래야 DNS 서버가 확인할 수 있습니다.
NTP 서버	환경에서 사용하는 NTP 서버의 주소를 입력합니다(있는 경우).

- **정적.** 관리 네트워크에 대한 모든 네트워킹 설정을 수동으로 입력합니다.

옵션	설명
네트워크	감독자에 대한 관리 트래픽을 처리할 네트워크를 선택합니다.
시작 IP 주소	다음과 같이 Kubernetes 제어부 VM에 대해 5개의 연속 IP 주소를 예약하기 위한 시작 지점을 결정하는 IP 주소를 입력합니다. <ul style="list-style-type: none"> ■ Kubernetes 제어부 VM 각각에 대한 IP 주소입니다. ■ 관리 네트워크에 대한 인터페이스로 제공할 Kubernetes 제어부 VM 중 하나에 대한 부동 IP 주소입니다. 부동 IP 주소가 할당된 제어부 VM은 세 개의 Kubernetes 제어부 VM 모두에 대해 선행 VM으로 작동합니다. 부동 IP는 Kubernetes 클러스터의 etcd 리더인 제어부 노드로 이동합니다. 그러면 네트워크 파티션 이벤트의 경우 가용성이 향상됩니다. ■ Kubernetes 제어부 VM이 실패하여 새로운 제어부 VM으로 교체하는 경우 버퍼 역할을 하는 IP 주소입니다.
서브넷 마스크	정적 IP 구성에만 적용됩니다. 관리 네트워크에 대한 서브넷 마스크를 입력합니다. 예를 들어 255.255.255.0입니다.
게이트웨이	관리 네트워크의 게이트웨이를 입력합니다.
DNS 서버	환경에서 사용하는 DNS 서버의 주소를 입력합니다. vCenter Server 시스템이 FQDN으로 등록되어 있으면 vSphere 환경에 사용하는 DNS 서버의 IP 주소를 입력해야 합니다. 그래야 감독자에서 FQDN을 확인할 수 있습니다.
DNS 검색 도메인	Kubernetes 제어부 노드 내에서 DNS가 검색하는 도메인 이름(예: corp.local)을 입력합니다. 그래야 DNS 서버가 확인할 수 있습니다.
NTP 서버	환경에서 사용하는 NTP 서버의 주소를 입력합니다(있는 경우).

b 다음을 클릭합니다.

10 워크로드 네트워크 창에서 네임스페이스의 네트워크에 대한 설정을 구성합니다.

옵션	설명
vSphere Distributed Switch	감독자에 대한 오버레이 네트워킹을 처리하는 vSphere Distributed Switch를 선택합니다. 예를 들어 DSwitch를 선택합니다.
DNS 서버	환경에서 사용하는 DNS 서버의 IP 주소를 입력합니다(있는 경우). 예: 10.142.7.1

옵션	설명
NAT 모드	<p>NAT 모드는 기본적으로 선택되어 있습니다.</p> <p>이 옵션을 선택 취소하면 vSphere 포드, VM 및 Tanzu Kubernetes 클러스터 노드 IP 주소와 같은 모든 워크로드를 Tier-0 게이트웨이 외부에서 직접 액세스할 수 있으며 송신 CIDR을 구성할 필요가 없습니다.</p> <hr/> <p>참고 NAT 모드를 선택 취소하면 파일 볼륨 스토리지가 지원되지 않습니다.</p>
네임스페이스 네트워크	<p>하나 이상의 IP CIDR을 입력하여 서브넷/세그먼트를 생성하고 워크로드에 IP 주소를 할당합니다.</p>
수신 CIDR	<p>Kubernetes 서비스의 수신 IP 범위를 결정하는 CIDR 주석을 입력합니다. 이 범위는 로드 밸런서 및 수신 유형의 서비스에 사용됩니다.</p>
Edge 클러스터	<p>네임스페이스 네트워킹에 사용할 Tier-0 게이트웨이가 있는 NSX Edge 클러스터를 선택합니다.</p> <p>예를 들어 <code>EDGE-CLUSTER</code>를 선택합니다.</p>
Tier-0 게이트웨이	<p>클러스터 Tier-1 게이트웨이와 연결할 Tier-0 게이트웨이를 선택합니다.</p>
서브넷 접두사	<p>네임스페이스 세그먼트용으로 예약된 서브넷의 크기를 지정하는 서브넷 접두사를 입력합니다. Default is 28.</p>
서비스 CIDR	<p>Kubernetes 서비스의 IP 범위를 결정하는 CIDR 주석을 입력합니다. 기본값을 사용할 수 있습니다.</p>
송신 CIDR	<p>Kubernetes 서비스의 송신 IP를 결정하는 CIDR 주석을 입력합니다. 감독자의 각 네임스페이스에는 송신 IP 주소가 하나만 할당됩니다. 송신 IP는 특정 네임스페이스의 Kubernetes 워크로드가 NSX 외부에서 통신하는 데 사용하는 IP 주소입니다.</p>

11 다음을 클릭합니다.

- 12 검토 및 확인 페이지에서 위로 스크롤하여 지금까지 구성된 모든 설정을 검토하고 감독자 배포에 대한 고급 설정을 지정합니다.

옵션	설명
감독자 제어부 크기	<p>제어부 VM에 대한 크기 조정을 선택합니다. 제어부 VM의 크기에 따라 감독자에서 실행할 수 있는 워크로드의 양이 결정됩니다. 다음 중에서 선택할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 매우 작음 - CPU 2개, 8GB 메모리, 32GB 스토리지 ■ 작음 - CPU 4개, 16GB 메모리, 32GB 스토리지 ■ 중간- CPU 8개, 16GB 메모리, 32GB 스토리지 ■ 큼 - CPU 16개, 32GB 메모리, 32GB 스토리지 <p>참고 제어부 크기를 선택하면 스케일 업만 가능합니다. 더 작은 크기로 스케일 다운할 수 없습니다.</p>
API 서버 DNS 이름	<p>필요한 경우 감독자 제어부 IP 주소를 사용하는 대신 감독자 제어부에 액세스하는 데 사용할 FQDN을 입력합니다. 입력한 FQDN은 자동으로 생성된 인증서에 포함됩니다. 감독자에 FQDN을 사용하면 로드 밸런서 인증서에서 IP 샌드 지정을 생략할 수 있습니다.</p>
구성 내보내기	<p>입력한 감독자 구성의 값이 포함된 JSON 파일을 내보냅니다.</p> <p>감독자를 다시 배포하거나 유사한 구성으로 새 감독자를 배포하려는 경우 나중에 파일을 수정하고 가져올 수 있습니다.</p> <p>감독자 구성을 내보내면 감독자를 다시 배포할 경우 이 마법사의 모든 구성 값을 새로 입력하는 시간을 절약할 수 있습니다.</p>

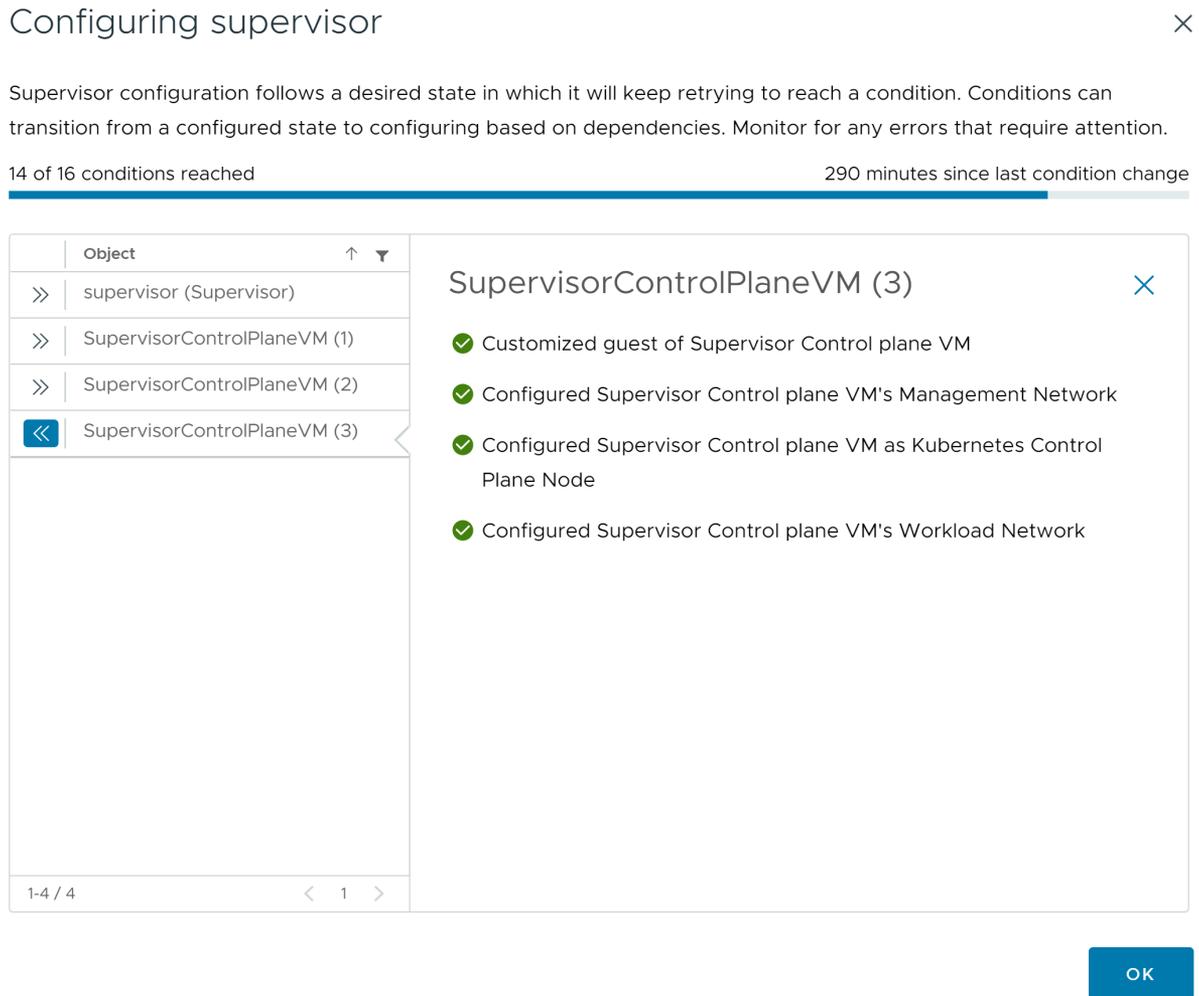
- 13 설정을 검토할 준비가 되면 **마침**을 클릭합니다.

감독자를 사용 설정하면 제어부 VM 및 기타 구성 요소의 생성 및 구성이 시작됩니다.

다음에 수행할 작업

감독자를 사용하도록 설정하는 마법사를 완료하면 활성화 프로세스를 추적하고 문제 해결이 필요한 잠재적인 문제를 관찰할 수 있습니다. **구성 상태** 열에서 **의 상태 옆에 있는** 보기감독자를 클릭합니다.

그림 5-2. 감독자 활성화 보기



배포 프로세스가 완료되려면 감독자가 원하는 상태에 도달해야 합니다. 즉 모든 조건이 충족되어야 합니다. 감독자가 사용되도록 설정하는 데 성공하면 해당 상태가 [구성 중]에서 [실행 중]으로 변경됩니다. 감독자가 [구성 중] 상태에 있는 동안 각 조건에 도달하기 위한 재시도가 계속됩니다. 조건에 도달하지 않으면 성공할 때까지 작업이 재시도됩니다. 이러한 이유로 인해 도달한 조건 수가 오락가락 변경될 수 있습니다(예: "16개 중 10개 조건에 도달" 후 "16개 중 4개 조건에 도달" 등). 매우 드문 경우지만 원하는 상태에 도달하지 못하게 하는 오류가 있는 경우 상태가 오류로 변경될 수 있습니다.

배포 오류 및 문제 해결 방법에 대한 자세한 내용은 [활성화 또는 업데이트 중 감독자 제어부 VM의 오류 상태 해결](#)을 참조하십시오.

마법사에서 입력한 구성 값을 변경하여 감독자를 다시 배포하려는 경우 [장 9 JSON 구성 파일](#)을 가져와서 감독자 배포 항목을 확인하십시오.

1개 영역 감독자 배포

6

1개 vSphere 클러스터에서 감독자를 배포합니다. 그러면 1개 vSphere 영역에 자동으로 매핑됩니다. 1개 영역 감독자에는 vSphere HA가 제공하는 호스트 수준 고가용성이 있습니다.

다음으로 아래 항목을 읽으십시오.

- VDS 네트워킹 스택을 사용하여 1개 영역 감독자 배포
- 감독자 네트워킹을 사용하여 1개 영역 NSX 배포

VDS 네트워킹 스택을 사용하여 1개 영역 감독자 배포

VDS 네트워킹 스택 및 HA Proxy 로드 밸런서 또는 NSX Advanced Load Balancer를 사용하여 1개 영역 감독자를 배포하는 방법을 알아봅니다. VDS 네트워킹으로 구성된 1개 영역 감독자는 Tanzu Kubernetes Grid를 사용하여 생성된 Tanzu Kubernetes 클러스터의 배포를 지원합니다. 감독자 서비스에서 배포한 것과 별도로 vSphere 포드를 실행하는 것은 지원하지 않습니다.

참고 단일 vSphere 클러스터에 감독자를 배포하여 1개 vSphere 영역이 생성되면 감독자를 3개 영역 배포로 확장할 수 없습니다. 1개 vSphere 영역(단일 클러스터 배포) 또는 3개 vSphere 영역에 감독자를 배포할 수 있습니다.

사전 요구 사항

- vSphere 클러스터를 감독자로 구성하기 위한 사전 요구 사항을 완료합니다. [vSphere 클러스터에서 vSphere IaaS control plane를 구성하기 위한 사전 요구 사항](#)의 내용을 참조하십시오.

절차

- 1 홈 메뉴에서 **워크로드 관리**를 선택합니다.
- 2 감독자에 대한 라이선싱 옵션을 선택합니다.
 - 유효한 Tanzu Edition 라이선스가 있는 경우 **라이선스 추가**를 클릭하여 vSphere 라이선스 인벤토리에 라이선스 키를 추가합니다.
 - Tanzu Edition 라이선스가 아직 없는 경우에는 VMware에서 통신을 받을 수 있도록 연락처 세부 정보를 입력하고 **시작**을 클릭합니다.

감독자의 평가 기간은 60일 동안 지속됩니다. 이 기간 내에는 클러스터에 유효한 Tanzu Edition 라이선스를 할당해야 합니다. Tanzu Edition 라이선스 키를 추가한 경우 감독자 설정을 완료하면 60일 평가 기간 내에 해당 키를 할당할 수 있습니다.

- 3 **워크로드 관리** 화면에서 **시작**을 다시 클릭합니다.
- 4 **vCenter Server 및 네트워크** 페이지를 선택하고 감독자 배포를 위해 설정된 vCenter Server 시스템을 선택하고 네트워킹 스택으로 **VDS(vSphere Distributed Switch)**를 선택하고 **다음**을 클릭합니다.
- 5 1개 영역 감독자를 사용하도록 설정하려면 감독자 위치 페이지에서 **클러스터 배포**를 선택합니다.
1개 영역 감독자에서 워크로드 관리를 사용하도록 설정하면 vSphere 영역이 자동으로 생성되고 클러스터가 영역에 할당됩니다.
- 6 호환되는 클러스터 목록에서 클러스터를 선택합니다.
- 7 감독자의 이름을 입력합니다.
- 8 (선택 사항) vSphere 영역의 이름을 입력하고 **다음**을 클릭합니다.
vSphere 영역의 이름을 입력하지 않으면 이름이 자동으로 할당되며 나중에 이름을 변경할 수 없습니다.
- 9 **스토리지** 페이지에서 제어부 VM 배치를 위한 스토리지를 구성합니다.

옵션	설명
제어부 노드	제어부 VM 배치에 대한 스토리지 정책을 선택합니다.

10 로드 밸런서 화면에서 로드 밸런서에 대한 설정을 구성합니다.

- a 로드 밸런서의 이름을 입력합니다.
- b 로드 밸런서 유형을 선택합니다.

NSX Advanced Load Balancer 및 **HAProxy** 중에서 선택할 수 있습니다.

c 로드 밸런서에 대한 설정 구성

- NSX Advanced Load Balancer에 대해 다음 설정을 입력합니다.

옵션	설명
이름	NSX Advanced Load Balancer의 이름을 입력합니다.
NSX Advanced Load Balancer 컨트롤러 끝점	NSX Advanced Load Balancer 컨트롤러의 IP 주소입니다. 기본 포트는 443입니다.
사용자 이름	NSX Advanced Load Balancer을 사용하여 구성된 사용자 이름입니다. 이 사용자 이름을 사용하여 컨트롤러에 액세스합니다.
암호	사용자 이름에 대한 암호입니다.
서버 인증서	컨트롤러에 사용되는 인증서입니다. 구성 중에 할당한 인증서를 제공할 수 있습니다. 자세한 내용은 컨트롤러에 인증서 할당 의 내용을 참조하십시오.
클라우드 이름	설정된 사용자 지정 클라우드의 이름을 입력합니다. 클라우드는 대/소문자를 구분합니다. 기본 클라우드 를 사용하려면 이 필드를 비워 둡니다. 자세한 내용은 컨트롤러 구성 의 내용을 참조하십시오.

- HAProxy에 대한 다음 설정을 입력합니다.

옵션	설명
HAProxy 로드 밸런서 컨트롤러 끝점	HAProxy 장치의 관리 IP 주소인 HAProxy 데이터부 API의 IP 주소 및 포트입니다. 이 구성 요소는 HAProxy 서버를 제어하고 HAProxy VM 내에서 실행됩니다.
사용자 이름	HAProxy OVA 파일을 사용하여 구성된 사용자 이름입니다. 이 이름을 사용하여 HAProxy 데이터부 API를 인증합니다.
암호	사용자 이름에 대한 암호입니다.
가상 IP 범위	Tanzu Kubernetes 클러스터가 워크로드 네트워크에서 사용하는 IP 주소 범위입니다. 이 IP 범위는 HAProxy 장치 배포 중에 구성된 CIDR에 정의된 IP 목록에서 가져옵니다. HAProxy 배포에 구성된 전체 범위를 설정할 수 있지만 여러 감독자를 생성하고 해당 CIDR 범위의 IP를 사용하려는 경우

옵션	설명
	<p>해당 CIDR의 하위 집합을 설정할 수도 있습니다. 이 범위는 마법사에서 워크로드 네트워크에 대해 정의된 IP 범위와 겹치지 않아야 합니다. 또한 범위는 이 워크로드 네트워크의 DHCP 범위와 겹치지 않아야 합니다.</p>
<p>HAProxy 관리 TLS 인증서</p>	<p>데이터부 API가 제공하는 서버 인증서의 신뢰할 수 있는 루트이거나 서명된 PEM 형식의 인증서입니다.</p> <ul style="list-style-type: none"> ■ 옵션 1: 루트 액세스를 사용하도록 설정된 경우 SSH를 사용하여 HAProxy VM에 루트로 연결하고 <code>/etc/haproxy/ca.crt</code>를 서버 CA(인증 기관)에 복사합니다. <code>\n</code> 형식으로 이스케이프 줄을 사용하지 마십시오. ■ 옵션 2: HAProxy VM을 마우스 오른쪽 버튼으로 클릭하고 설정 편집을 선택합니다. 해당 필드에서 CA 인증서를 복사한 후 https://www.base64decode.org/와 같은 변환 도구를 사용하여 Base64에서 변환합니다. ■ 옵션 3: 다음 PowerCLI 스크립트를 실행합니다. <code>\$vc</code>, <code>\$vc_user</code>, <code>\$vc_password</code> 변수를 적절한 값으로 바꿉니다. <pre> \$vc = "10.21.32.43" \$vc_user = "administrator@vsphere.local" \$vc_password = "PASSWORD" Connect-VIServer -User \$vc_user -Password \$vc_password -Server \$vc \$VMname = "haproxy-demo" \$AdvancedSettingName = "guestinfo.dataplaneapi.cacert" \$Base64cert = get-vm \$VMname Get- AdvancedSetting -Name \$AdvancedSettingName while ([string]::IsNullOrEmpty(\$Base64cert .Value)) { Write-Host "Waiting for CA Cert Generation... This may take a under 5-10 minutes as the VM needs to boot and generate the CA Cert (if you haven't provided one already)."<!-- \$Base64cert = get-vm \$VMname Get-AdvancedSetting -Name \$AdvancedSettingName Start-sleep -seconds 2 } Write-Host "CA Cert Found... Converting from BASE64" \$cert = [Text.Encoding]::Utf8.GetString([Con vert]::FromBase64String(\$Base64cert. Value)) Write-Host \$cert </pre--> </pre>

11 관리 네트워크 화면에서 Kubernetes 제어부 VM에 사용될 네트워크에 대한 매개 변수를 구성합니다.

a 네트워크 모드를 선택합니다.

- **DHCP 네트워크.** 이 모드에서는 관리 네트워크의 모든 IP 주소(예: 제어부 VM IP, 부동 IP, DNS 서버, DNS, 검색 도메인 및 NTP 서버)가 DHCP 서버에서 자동으로 획득됩니다. 부동 IP를 얻으려면 DHCP 서버는 클라이언트 식별자를 지원하도록 구성되어야 합니다. DHCP 모드에서 모든 제어부 VM은 안정적인 DHCP 클라이언트 식별자를 사용하여 IP 주소를 획득합니다. 이러한 클라이언트 식별자는 DHCP 서버에서 제어부 VM의 IP에 대한 정적 IP 할당을 설정하여 변경되지 않도록 하는 데 사용할 수 있습니다. 제어부 VM의 IP 및 부동 IP를 변경하는 것은 지원되지 않습니다.

이러한 설정의 텍스트 필드에 값을 입력하여 DHCP에서 상속된 일부 설정을 재정의할 수 있습니다.

옵션	설명
네트워크	감독자에 대한 관리 트래픽을 처리할 네트워크를 선택합니다.
부동 IP	다음과 같이 Kubernetes 제어부 VM에 대해 5개의 연속 IP 주소를 예약하기 위한 시작 지점을 결정하는 IP 주소를 입력합니다. <ul style="list-style-type: none"> ■ Kubernetes 제어부 VM 각각에 대한 IP 주소입니다. ■ 관리 네트워크에 대한 인터페이스로 제공할 Kubernetes 제어부 VM 중 하나에 대한 부동 IP 주소입니다. 부동 IP 주소가 할당된 제어부 VM은 세 개의 Kubernetes 제어부 VM 모두에 대해 선행 VM으로 작동합니다. 부동 IP는 Kubernetes 클러스터의 etcd 리더인 제어부 노드로 이동합니다. 그러면 네트워크 파티션 이벤트의 경우 가용성이 향상됩니다. ■ Kubernetes 제어부 VM이 실패하여 새로운 제어부 VM으로 교체하는 경우 버퍼 역할을 하는 IP 주소입니다.
DNS 서버	환경에서 사용하는 DNS 서버의 주소를 입력합니다. vCenter Server 시스템이 FQDN으로 등록되어 있으면 vSphere 환경에 사용하는 DNS 서버의 IP 주소를 입력해야 합니다. 그래야 감독자에서 FQDN을 확인할 수 있습니다.
DNS 검색 도메인	Kubernetes 제어부 노드 내에서 DNS가 검색하는 도메인 이름(예: <code>corp.local</code>)을 입력합니다. 그래야 DNS 서버가 확인할 수 있습니다.
NTP 서버	환경에서 사용하는 NTP 서버의 주소를 입력합니다(있는 경우).

- **정적.** 관리 네트워크에 대한 모든 네트워킹 설정을 수동으로 입력합니다.

옵션	설명
네트워크	감독자에 대한 관리 트래픽을 처리할 네트워크를 선택합니다.
시작 IP 주소	다음과 같이 Kubernetes 제어부 VM에 대해 5개의 연속 IP 주소를 예약하기 위한 시작 지점을 결정하는 IP 주소를 입력합니다. <ul style="list-style-type: none"> ■ Kubernetes 제어부 VM 각각에 대한 IP 주소입니다. ■ 관리 네트워크에 대한 인터페이스로 제공할 Kubernetes 제어부 VM 중 하나에 대한 부동 IP 주소입니다. 부동 IP 주소가 할당된 제어부 VM은 세 개의 Kubernetes 제어부 VM 모두에 대해 선행 VM으로 작동합니다. 부동 IP는 Kubernetes 클러스터의 etcd 리더인 제어부 노드로 이동합니다. 그러면 네트워크 파티션 이벤트의 경우 가용성이 향상됩니다. ■ Kubernetes 제어부 VM이 실패하여 새로운 제어부 VM으로 교체하는 경우 버퍼 역할을 하는 IP 주소입니다.
서브넷 마스크	정적 IP 구성에만 적용됩니다. 관리 네트워크에 대한 서브넷 마스크를 입력합니다. 예를 들어 255.255.255.0입니다.
게이트웨이	관리 네트워크의 게이트웨이를 입력합니다.
DNS 서버	환경에서 사용하는 DNS 서버의 주소를 입력합니다. vCenter Server 시스템이 FQDN으로 등록되어 있으면 vSphere 환경에 사용하는 DNS 서버의 IP 주소를 입력해야 합니다. 그래야 감독자에서 FQDN을 확인할 수 있습니다.
DNS 검색 도메인	Kubernetes 제어부 노드 내에서 DNS가 검색하는 도메인 이름(예: corp.local)을 입력합니다. 그래야 DNS 서버가 확인할 수 있습니다.
NTP 서버	환경에서 사용하는 NTP 서버의 주소를 입력합니다(있는 경우).

b 다음을 클릭합니다.

12 **워크로드 네트워크** 페이지에서 감독자에서 실행되는 Kubernetes 워크로드에 대한 네트워킹 트래픽을 처리하는 네트워크에 대한 설정을 입력합니다.

참고 워크로드 네트워크에 대한 네트워킹 설정을 제공하기 위해 DHCP 서버를 사용하도록 선택하는 경우 감독자 구성을 완료하면 새 워크로드 네트워크를 생성할 수 없습니다.

a 네트워크 모드를 선택합니다.

- **DHCP 네트워크.** 이 네트워크 모드에서는 워크로드 네트워크에 대한 모든 네트워킹 설정이 DHCP를 통해 획득됩니다. 다음 설정에 대한 텍스트 필드에 값을 입력하여 DHCP에서 상속된 일부 설정을 재정의할 수도 있습니다.

참고 워크로드 네트워크에 대한 DHCP 구성은 VDS 스택으로 구성된 감독자의 감독자 서비스에서 지원되지 않습니다. 감독자 서비스를 사용하려면 정적 IP 주소로 워크로드 네트워크를 구성합니다. 관리 네트워크에 DHCP를 계속 사용할 수 있습니다.

옵션	설명
Kubernetes 서비스를 위한 내부 네트워크	클러스터 내에서 실행되는 Tanzu Kubernetes 클러스터 및 서비스에 대한 IP 주소 범위를 결정하는 CIDR 표기법을 입력합니다.
포트 그룹	감독자에 대한 기본 워크로드 네트워크로 사용할 포트 그룹을 선택합니다. 기본 네트워크는 Kubernetes 제어부 VM 및 Kubernetes 워크로드 트래픽에 대한 트래픽을 처리합니다. 네트워킹 토폴로지에 따라, 나중에 각 네임스페이스에 네트워크로 사용할 다른 포트 그룹을 할당할 수 있습니다. 이 방법을 통해 감독자의 네임스페이스 간에 계층 2 분리를 제공할 수 있습니다. 네트워크로 할당된 다른 포트 그룹이 없는 네임스페이스는 기본 네트워크를 사용합니다. Tanzu Kubernetes 클러스터는 배포된 네임스페이스에 할당된 네트워크만 사용하거나 해당 네임스페이스에 명시적으로 할당된 네트워크가 없는 경우 기본 네트워크를 사용합니다.
네트워크 이름	네트워크 이름을 입력합니다.
DNS 서버	환경에서 사용하는 DNS 서버의 IP 주소를 입력합니다(있는 경우). 예: 10.142.7.1. DNS 서버의 IP 주소를 입력하면 각 제어부 VM에 정적 경로가 추가됩니다. 이것은 DNS 서버에 대한 트래픽이 워크로드 네트워크를 통과한다는 것을 나타냅니다. 지정하는 DNS 서버가 관리 네트워크와 워크로드 네트워크 간에 공유되는 경우에는 제어부 VM의 DNS 조회가 초기 설정 후 워크로드 네트워크를 통해 라우팅됩니다.
NTP 서버	환경에서 사용하는 NTP 서버의 주소를 입력합니다(있는 경우).

- **정적.** 워크로드 네트워크 설정을 수동으로 구성합니다.

옵션	설명
Kubernetes 서비스를 위한 내부 네트워크	클러스터 내에서 실행되는 Tanzu Kubernetes 클러스터 및 서비스에 대한 IP 주소 범위를 결정하는 CIDR 표기법을 입력합니다.
포트 그룹	<p>감독자에 대한 기본 워크로드 네트워크로 사용할 포트 그룹을 선택합니다.</p> <p>기본 네트워크는 Kubernetes 제어부 VM 및 Kubernetes 워크로드 트래픽에 대한 트래픽을 처리합니다.</p> <p>네트워킹 토폴로지에 따라, 나중에 각 네임스페이스에 네트워크로 사용할 다른 포트 그룹을 할당할 수 있습니다. 이 방법을 통해 감독자의 네임스페이스 간에 계층 2 분리를 제공할 수 있습니다. 네트워크로 할당된 다른 포트 그룹이 없는 네임스페이스는 기본 네트워크를 사용합니다. Tanzu Kubernetes 클러스터는 배포된 네임스페이스에 할당된 네트워크만 사용하거나 해당 네임스페이스에 명시적으로 할당된 네트워크가 없는 경우 기본 네트워크를 사용합니다.</p>
네트워크 이름	네트워크 이름을 입력합니다.
IP 주소 범위	<p>Kubernetes 제어부 VM 및 워크로드의 IP 주소를 할당하기 위한 IP 범위를 입력합니다.</p> <p>이 주소 범위는 감독자 노드를 연결하며, 단일 워크로드 네트워크의 경우 Tanzu Kubernetes 클러스터 노드도 연결합니다. HAProxy에 대한 기본 구성을 사용하는 경우 이 IP 범위는 로드 밸런서 VIP 범위와 겹치지 않아야 합니다.</p>
서브넷 마스크	서브넷 마스크 IP 주소를 입력합니다.
게이트웨이	기본 네트워크의 게이트웨이를 입력합니다.
NTP 서버	환경에서 사용하는 NTP 서버의 주소를 입력합니다(있는 경우).
DNS 서버	<p>환경에서 사용하는 DNS 서버의 IP 주소를 입력합니다(있는 경우).</p> <p>예: 10.142.7.1.</p>

b 다음을 클릭합니다.

13 검토 및 확인 페이지에서 위로 스크롤하여 지금까지 구성된 모든 설정을 검토하고 감독자 배포에 대한 고급 설정을 지정합니다.

옵션	설명
감독자 제어부 크기	<p>제어부 VM에 대한 크기 조정을 선택합니다. 제어부 VM의 크기에 따라 감독자에서 실행할 수 있는 워크로드의 양이 결정됩니다. 다음 중에서 선택할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 매우 작음 - CPU 2개, 8GB 메모리, 32GB 스토리지 ■ 작음 - CPU 4개, 16GB 메모리, 32GB 스토리지 ■ 중간- CPU 8개, 16GB 메모리, 32GB 스토리지 ■ 큼 - CPU 16개, 32GB 메모리, 32GB 스토리지 <p>참고 제어부 크기를 선택하면 스케일 업만 가능합니다. 더 작은 크기로 스케일 다운할 수 없습니다.</p>
API 서버 DNS 이름	<p>필요한 경우 감독자 제어부 IP 주소를 사용하는 대신 감독자 제어부에 액세스하는 데 사용할 FQDN을 입력합니다. 입력한 FQDN은 자동으로 생성된 인증서에 포함됩니다. 감독자에 FQDN을 사용하면 로드 밸런서 인증서에서 IP 샌드 지정을 생략할 수 있습니다.</p>
구성 내보내기	<p>입력한 감독자 구성의 값이 포함된 JSON 파일을 내보냅니다.</p> <p>감독자를 다시 배포하거나 유사한 구성으로 새 감독자를 배포하려는 경우 나중에 파일을 수정하고 가져올 수 있습니다.</p> <p>감독자 구성을 내보내면 감독자를 다시 배포할 경우 이 마법사의 모든 구성 값을 새로 입력하는 시간을 절약할 수 있습니다.</p>

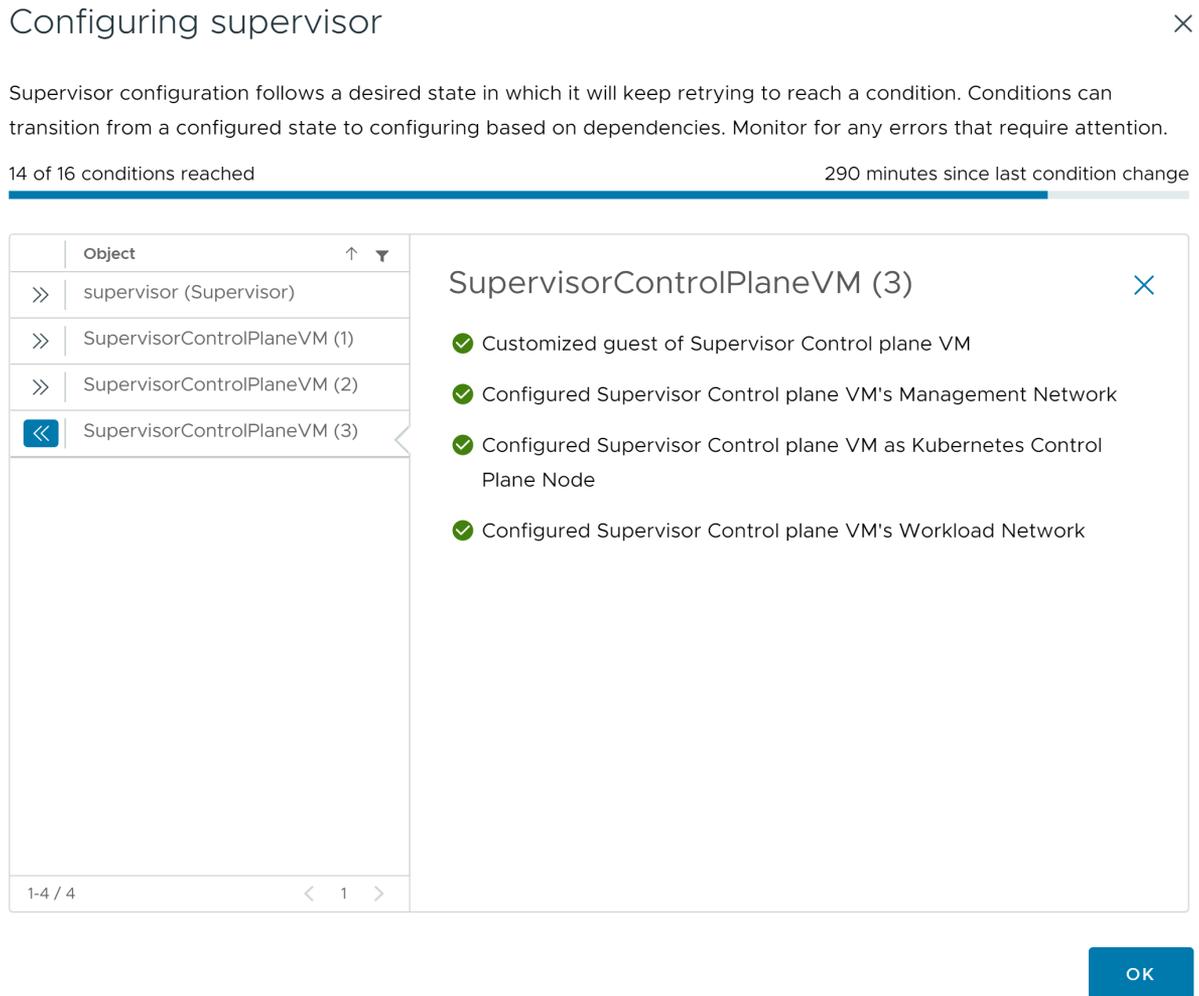
14 설정을 검토할 준비가 되면 **마침**을 클릭합니다.

감독자를 배포하면 제어부 VM 및 기타 구성 요소의 생성 및 구성이 시작됩니다.

다음에 수행할 작업

감독자를 사용하도록 설정하는 마법사를 완료하면 활성화 프로세스를 추적하고 문제 해결이 필요한 잠재적인 문제를 관찰할 수 있습니다. **구성 상태** 열에서 **의 상태 옆에 있는** 보기감독자를 클릭합니다.

그림 6-1. 감독자 활성화 보기



배포 프로세스가 완료되려면 감독자가 원하는 상태에 도달해야 합니다. 즉 모든 조건이 충족되어야 합니다. 감독자가 사용되도록 설정하는 데 성공하면 해당 상태가 [구성 중]에서 [실행 중]으로 변경됩니다. 감독자가 [구성 중] 상태에 있는 동안 각 조건에 도달하기 위한 재시도가 계속됩니다. 조건에 도달하지 않으면 성공할 때까지 작업이 재시도됩니다. 이러한 이유로 인해 도달한 조건 수가 오락가락 변경될 수 있습니다(예: "16개 중 10개 조건에 도달" 후 "16개 중 4개 조건에 도달" 등). 매우 드문 경우지만 원하는 상태에 도달하지 못하게 하는 오류가 있는 경우 상태가 오류로 변경될 수 있습니다.

배포 오류 및 문제 해결 방법에 대한 자세한 내용은 [활성화 또는 업데이트 중 감독자 제어부 VM의 오류 상태 해결](#)을 참조하십시오.

마법사에서 입력한 구성 값을 변경하여 감독자를 다시 배포하려는 경우 [장 9 JSON 구성 파일](#)을 가져와서 감독자 배포 항목을 확인하십시오.

감독자 네트워킹을 사용하여 1개 영역 NSX 배포

vSphere 영역에 매핑되는 1개 vSphere 클러스터에 NSX 네트워킹을 사용하여 감독자를 배포하는 방법을 알아 봅니다. 결과적으로 감독자는 vSphere HA에서 제공하는 호스트 수준 고가용을 갖게 됩니다. 1개 영역 감독자는 모든 Tanzu Kubernetes 클러스터, VM 및 vSphere 포드를 지원합니다.

NSX 버전 4.1.1 이상을 구성하고 NSX에서 엔터프라이즈 라이선스로 NSX Advanced Load Balancer 버전 22.1.4 이상을 설치, 구성 및 등록한 경우 NSX와 함께 사용되는 로드 밸런서는 NSX Advanced Load Balancer입니다. 4.1.1 이전 버전의 NSX를 구성한 경우 NSX 로드 밸런서가 사용됩니다. 자세한 내용은 [장 7 NSX 네트워킹에 사용되는 로드 밸런서 확인](#) 항목을 참조하십시오.

참고 단일 vSphere 클러스터에 감독자를 배포하여 1개 vSphere 영역이 생성되면 감독자를 3개 영역 배포로 확장할 수 없습니다. 1개 vSphere 영역(단일 클러스터 배포) 또는 3개 vSphere 영역에 감독자를 배포할 수 있습니다.

사전 요구 사항

사용 중인 환경이 vSphere 클러스터를 감독자로 구성하기 위한 사전 요구 사항을 충족하는지 확인합니다. 요구 사항에 대한 자세한 내용은 [vSphere 클러스터에서 vSphere IaaS control plane](#)를 구성하기 위한 [사전 요구 사항](#) 항목을 참조하십시오.

절차

- 1 홈 메뉴에서 **워크로드 관리**를 선택합니다.
- 2 감독자에 대한 라이선싱 옵션을 선택합니다.
 - 유효한 Tanzu Edition 라이선스가 있는 경우 **라이선스 추가**를 클릭하여 vSphere 라이선스 인벤토리에 라이선스 키를 추가합니다.
 - Tanzu Edition 라이선스가 아직 없는 경우에는 VMware에서 통신을 받을 수 있도록 연락처 세부 정보를 입력하고 **시작**을 클릭합니다.

감독자의 평가 기간은 60일 동안 지속됩니다. 이 기간 내에는 클러스터에 유효한 Tanzu Edition 라이선스를 할당해야 합니다. Tanzu Edition 라이선스 키를 추가한 경우 감독자 설정을 완료하면 60일 평가 기간 내에 해당 키를 할당할 수 있습니다.

- 3 **워크로드 관리** 화면에서 **시작**을 다시 클릭합니다.
- 4 **vCenter Server 및 네트워크** 페이지에서 감독자 배포용으로 설정된 vCenter Server 시스템을 선택하고 **NSX**를 네트워킹 스택으로 선택합니다.
- 5 **감독자 위치** 페이지에서 **클러스터 배포**를 선택합니다.
 - a 새 감독자의 이름을 입력합니다.
 - b 호환되는 vSphere 클러스터를 선택합니다.

- c 선택한 클러스터에 대해 자동으로 생성될 vSphere 영역의 이름을 입력합니다.
영역의 이름을 제공하지 않으면 자동으로 생성됩니다.
- d 다음을 클릭합니다.

6 감독자에 대한 스토리지 정책을 선택합니다.

다음 각 개체에 대해 선택하는 스토리지 정책은 개체가 스토리지 정책에서 참조되는 데이터스토어에 배치되도록 합니다. 개체에 대해 동일한 또는 서로 다른 스토리지 정책을 사용할 수 있습니다.

옵션	설명
제어부 스토리지 정책	제어부 VM 배치에 대한 스토리지 정책을 선택합니다.
사용 후 삭제 디스크 스토리지 정책	vSphere 포드 배치에 대한 스토리지 정책을 선택합니다.
이미지 캐시 스토리지 정책	컨테이너 이미지의 캐시 배치에 대한 스토리지 정책을 선택합니다.

7 관리 네트워크 화면에서 Kubernetes 제어부 VM에 사용될 네트워크에 대한 매개 변수를 구성합니다.

a 네트워크 모드를 선택합니다.

- **DHCP 네트워크.** 이 모드에서는 관리 네트워크의 모든 IP 주소(예: 제어부 VM IP, DNS 서버, DNS, 검색 도메인 및 NTP 서버)가 DHCP에서 자동으로 획득됩니다.
- **정적.** 관리 네트워크에 대한 모든 네트워킹 설정을 수동으로 입력합니다.

b 관리 네트워크에 대한 설정을 구성합니다.

DHCP 네트워크 모드를 선택했지만 DHCP에서 획득한 설정을 재정의하려면 **추가 설정**을 클릭하고 새 값을 입력합니다. 정적 네트워크 모드를 선택한 경우에는 관리 네트워크 설정에 대한 값을 수동으로 입력합니다.

옵션	설명
네트워크	관리 트래픽에 대해 구성된 VMkernel 어댑터가 있는 네트워크를 선택합니다.
제어 IP 주소 시작	다음과 같이 Kubernetes 제어부 VM에 대해 5개의 연속 IP 주소를 예약하기 위한 시작 지점을 결정하는 IP 주소를 입력합니다. <ul style="list-style-type: none"> ■ Kubernetes 제어부 VM 각각에 대한 IP 주소입니다. ■ 관리 네트워크에 대한 인터페이스로 제공할 Kubernetes 제어부 VM 중 하나에 대한 부동 IP 주소입니다. 부동 IP 주소가 할당된 제어부 VM은 세 개의 Kubernetes 제어부 VM 모두에 대해 선행 VM으로 작동합니다. 부동 IP는 이 Kubernetes 클러스터(감독자)의 etcd 리더인 제어부 노드로 이동합니다. 그러면 네트워크 파티션 이벤트의 경우 가용성이 향상됩니다. ■ Kubernetes 제어부 VM이 실패하여 새로운 제어부 VM으로 교체하는 경우 버퍼 역할을 하는 IP 주소입니다.
서브넷 마스크	정적 IP 구성에만 적용됩니다. 관리 네트워크에 대한 서브넷 마스크를 입력합니다. 예를 들어 255.255.255.0입니다.
DNS 서버	환경에서 사용하는 DNS 서버의 주소를 입력합니다. vCenter Server 시스템이 FQDN으로 등록되어 있으면 vSphere 환경에 사용하는 DNS 서버의 IP 주소를 입력해야 합니다. 그래야 감독자에서 FQDN을 확인할 수 있습니다.
DNS 검색 도메인	Kubernetes 제어부 노드 내에서 DNS가 검색하는 도메인 이름(예: corp.local)을 입력합니다. 그래야 DNS 서버가 확인할 수 있습니다.
NTP	환경에서 사용하는 NTP 서버의 주소를 입력합니다(있는 경우).

8 워크로드 네트워크 창에서 네임스페이스의 네트워크에 대한 설정을 구성합니다.

옵션	설명
vSphere Distributed Switch	감독자에 대한 오버레이 네트워킹을 처리하는 vSphere Distributed Switch를 선택합니다. 예를 들어 DSwitch를 선택합니다.
DNS 서버	환경에서 사용하는 DNS 서버의 IP 주소를 입력합니다(있는 경우). 예: 10.142.7.1

옵션	설명
NAT 모드	NAT 모드는 기본적으로 선택되어 있습니다. 이 옵션을 선택 취소하면 vSphere 포드, VM 및 Tanzu Kubernetes 클러스터 노드 IP 주소와 같은 모든 워크로드를 Tier-0 게이트웨이 외부에서 직접 액세스할 수 있으며 송신 CIDR을 구성할 필요가 없습니다. 참고 NAT 모드를 선택 취소하면 파일 볼륨 스토리지가 지원되지 않습니다.
네임스페이스 네트워크	하나 이상의 IP CIDR을 입력하여 서브넷/세그먼트를 생성하고 워크로드에 IP 주소를 할당합니다.
수신 CIDR	Kubernetes 서비스의 수신 IP 범위를 결정하는 CIDR 주석을 입력합니다. 이 범위는 로드 밸런서 및 수신 유형의 서비스에 사용됩니다.
Edge 클러스터	네임스페이스 네트워크에 사용할 Tier-0 게이트웨이가 있는 NSX Edge 클러스터를 선택합니다. 예를 들어 <code>EDGE-CLUSTER</code> 를 선택합니다.
Tier-0 게이트웨이	클러스터 Tier-1 게이트웨이와 연결할 Tier-0 게이트웨이를 선택합니다.
서브넷 접두사	네임스페이스 세그먼트용으로 예약된 서브넷의 크기를 지정하는 서브넷 접두사를 입력합니다. Default is 28.
서비스 CIDR	Kubernetes 서비스의 IP 범위를 결정하는 CIDR 주석을 입력합니다. 기본값을 사용할 수 있습니다.
송신 CIDR	Kubernetes 서비스의 송신 IP를 결정하는 CIDR 주석을 입력합니다. 감독자의 각 네임스페이스에는 송신 IP 주소가 하나만 할당됩니다. 송신 IP는 특정 네임스페이스의 Kubernetes 워크로드가 NSX 외부에서 통신하는 데 사용하는 IP 주소입니다.

- 9 검토 및 확인 페이지에서 위로 스크롤하여 지금까지 구성된 모든 설정을 검토하고 감독자 배포에 대한 고급 설정을 지정합니다.

옵션	설명
감독자 제어부 크기	제어부 VM에 대한 크기 조정을 선택합니다. 제어부 VM의 크기에 따라 감독자에서 실행할 수 있는 워크로드의 양이 결정됩니다. 다음 중에서 선택할 수 있습니다. <ul style="list-style-type: none"> ■ 매우 작음 - CPU 2개, 8GB 메모리, 32GB 스토리지 ■ 작음 - CPU 4개, 16GB 메모리, 32GB 스토리지 ■ 중간- CPU 8개, 16GB 메모리, 32GB 스토리지 ■ 큼 - CPU 16개, 32GB 메모리, 32GB 스토리지 참고 제어부 크기를 선택하면 스케일 업만 가능합니다. 더 작은 크기로 스케일 다운할 수 없습니다.
API 서버 DNS 이름	필요한 경우 감독자 제어부 IP 주소를 사용하는 대신 감독자 제어부에 액세스하는 데 사용할 FQDN을 입력합니다. 입력한 FQDN은 자동으로 생성된 인증서에 포함됩니다. 감독자에 FQDN을 사용하면 로드 밸런서 인증서에서 IP 샌드 지정을 생략할 수 있습니다.
구성 내보내기	입력한 감독자 구성의 값이 포함된 JSON 파일을 내보냅니다. 감독자를 다시 배포하거나 유사한 구성으로 새 감독자를 배포하려는 경우 나중에 파일을 수정하고 가져올 수 있습니다. 감독자 구성을 내보내면 감독자를 다시 배포할 경우 이 마법사의 모든 구성 값을 새로 입력하는 시간을 절약할 수 있습니다.

10 설정을 검토할 준비가 되면 **마침**을 클릭합니다.

감독자를 배포하면 제어부 VM 및 기타 구성 요소의 생성 및 구성이 시작됩니다.

11 감독자 탭에서 감독자의 배포 프로세스를 추적합니다.

- a 구성 상태 열에서 **의 상태 옆에 있는** 보기감독자를 클릭합니다.
- b 각 개체에 대한 구성 상태를 보고 문제를 해결할 잠재적인 문제를 추적합니다.

다음에 수행할 작업

감독자를 사용하도록 설정하는 마법사를 완료하면 활성화 프로세스를 추적하고 문제 해결이 필요한 잠재적인 문제를 관찰할 수 있습니다. 구성 상태 열에서 **의 상태 옆에 있는** 보기감독자를 클릭합니다.

그림 6-2. 감독자 활성화 보기

Configuring supervisor ×

Supervisor configuration follows a desired state in which it will keep retrying to reach a condition. Conditions can transition from a configured state to configuring based on dependencies. Monitor for any errors that require attention.

14 of 16 conditions reached 290 minutes since last condition change

Object	
» supervisor (Supervisor)	
» SupervisorControlPlaneVM (1)	
» SupervisorControlPlaneVM (2)	
« SupervisorControlPlaneVM (3)	<div style="border: 1px solid #ccc; padding: 5px;"> <h3 style="margin: 0;">SupervisorControlPlaneVM (3) ×</h3> <ul style="list-style-type: none"> ✔ Customized guest of Supervisor Control plane VM ✔ Configured Supervisor Control plane VM's Management Network ✔ Configured Supervisor Control plane VM as Kubernetes Control Plane Node ✔ Configured Supervisor Control plane VM's Workload Network </div>

OK

배포 프로세스가 완료되려면 감독자가 원하는 상태에 도달해야 합니다. 즉 모든 조건이 충족되어야 합니다. 감독자가 사용되도록 설정하는 데 성공하면 해당 상태가 [구성 중]에서 [실행 중]으로 변경됩니다. 감독자가 [구성 중] 상태에 있는 동안 각 조건에 도달하기 위한 재시도가 계속됩니다. 조건에 도달하지 않으면 성공할 때까지 작업이 재시도됩니다. 이러한 이유로 인해 도달한 조건 수가 오락가락 변경될 수 있습니다(예: "16개 중 10개 조건에 도달" 후 "16개 중 4개 조건에 도달" 등). 매우 드문 경우지만 원하는 상태에 도달하지 못하게 하는 오류가 있는 경우 상태가 오류로 변경될 수 있습니다.

배포 오류 및 문제 해결 방법에 대한 자세한 내용은 [활성화 또는 업데이트 중 감독자 제어부 VM의 오류 상태 해결](#)을 참조하십시오.

마법사에서 입력한 구성 값을 변경하여 감독자를 다시 배포하려는 경우 [장 9 JSON 구성 파일을 가져와서 감독자 배포 항목을 확인](#)하십시오.

NSX 네트워킹에 사용되는 로드 밸런서 확인

7

NSX 네트워킹으로 구성된 감독자는 NSX 로드 밸런서 또는 NSX Advanced Load Balancer를 사용할 수 있습니다.

NSX 버전 4.1.1 이상을 구성하고 NSX에서 엔터프라이즈 라이선스로 NSX Advanced Load Balancer 버전 22.1.4 이상을 설치, 구성 및 등록한 경우 NSX와 함께 사용되는 로드 밸런서는 NSX Advanced Load Balancer입니다. 4.1.1 이전 버전의 NSX를 구성한 경우 NSX 로드 밸런서가 사용됩니다.

NSX에 구성된 로드 밸런서를 확인하려면 다음 명령을 실행합니다.

```
kubectl get gateways.networking.x-k8s.io <gateway> -n <gateway_namespace> -oyaml
```

게이트웨이 종료자 `gateway.ako.vmware.com` 또는 수신 종료자 `ingress.ako.vmware.com/finalizer`가 규격에 있으면 NSX Advanced Load Balancer가 구성되었음을 나타냅니다.

감독자 구성 내보내기



기존 감독자의 구성을 내보내는 방법을 알아봅니다. 이 구성을 나중에 감독자 활성화 마법사에서 가져와서 유사한 구성으로 새 감독자 인스턴스를 배포할 수 있습니다. 감독자는 JSON 구성 파일 형식으로 내보내며, 이 파일을 필요에 따라 수정하고 새 감독자 인스턴스를 배포하는 데 사용할 수 있습니다.

감독자 구성을 내보내면 다음을 수행할 수 있습니다.

- 감독자 구성 유지. 이전 감독자 구성을 모두 내보내고 필요할 때 재사용할 수 있습니다.
- 보다 효율적인 문제 해결. 감독자 활성화가 실패하면 JSON 파일에 직접 감독자 구성을 조정하고 프로세스를 다시 시작할 수 있습니다. 이를 통해 JSON 파일을 가져오기 전에 JSON 파일에서 직접 설정을 수정할 수 있으므로 빠른 문제 해결이 가능합니다.
- 간소화된 관리. 내보낸 감독자 구성을 다른 관리자와 공유하여 유사한 설정으로 새 감독자를 설정할 수 있습니다.
- 일관된 형식. 내보낸 감독자 구성은 지원되는 배포 유형에 적용되는 표준화된 형식을 준수합니다.

감독자 활성화 워크플로 중에 감독자 구성을 내보낼 수도 있습니다. 자세한 내용은 [장 5 3개 영역 감독자 배포 및 장 6 1개 영역 감독자 배포](#)의 내용을 참조하십시오.

사전 요구 사항

감독자를 배포합니다.

절차

- 1 **워크로드 관리 > 감독자 > 감독자**로 이동합니다.
- 2 감독자를 선택하고 **구성 내보내기**를 선택합니다.

결과

구성은 브라우저의 기본 다운로드 폴더에 로컬로 저장되는 `wcp-config.zip`이라는 ZIP 파일에 내보내져 저장됩니다. `wcp-config.zip` 파일 내에서 다음을 찾을 수 있습니다.

- 감독자 구성이 포함된 JSON 파일(이름: `wcp-config.json`). 각 구성 설정에는 JSON 파일에 해당 이름과 위치가 있습니다. 이 JSON 파일은 계층적 데이터 구조를 따릅니다.

- 유효한 JSON 스키마 파일(이름: `wcp-config-schema.json`). 이 파일은 감독자에 대해 내보낼 수 있는 모든 설정을 간략하게 설명합니다. 여기에는 해당 유형, JSON 파일 내의 위치 및 필수 여부가 포함됩니다. 스키마 파일을 사용하여 샘플 구성 JSON 파일을 생성할 수 있으며, 이 파일을 수동으로 채우고 새로운 활성화 워크플로우로 가져올 수 있습니다.

다음에 수행할 작업

,

필요에 따라 JSON 구성을 편집하고 이를 사용하여 새 감독자를 배포합니다. [장 9 JSON 구성 파일을 가져와서 감독자 배포](#)의 내용을 참조하십시오.

JSON 구성 파일을 가져와서 감독자 배포

9

이전 감독자 배포에서 내보낸 JSON 구성 파일을 가져와서 감독자 활성화 마법사의 모든 구성 값을 자동으로 채우는 방법을 알아봅니다. 실패한 감독자 배포 문제를 해결하거나 비슷한 구성으로 새 감독자를 배포하는 경우 마법사에서 JSON 파일을 가져오기 전에 이 파일에서 직접 구성 값을 변경할 수 있습니다. 이렇게 하면 활성화 마법사의 모든 값을 수동으로 입력하는 시간을 절약하고 변경이 필요한 영역에만 집중할 수 있습니다.

감독자의 구성은 두 가지 방법으로 내보낼 수 있습니다.

- 마법사의 **완료 준비** 페이지에서 감독자를 배포하는 동안, 자세한 내용은 [장 5 3개 영역 감독자 배포 및 장 6 1개 영역 감독자 배포](#)의 내용을 참조하십시오.
- 이미 배포된 감독자의 구성을 내보냅니다. [장 8 감독자 구성 내보내기](#)의 내용을 참조하십시오.

사전 요구 사항

- vSphere 클러스터를 감독자로 구성하기 위한 사전 요구 사항을 완료합니다. [vSphere 클러스터에서 vSphere IaaS control plane를 구성하기 위한 사전 요구 사항](#)의 내용을 참조하십시오.
- 기존 감독자 배포에서 내보낸 JSON 구성 파일이 있는지 확인합니다. 파일의 기본 이름은 `wcp-config.json`입니다.

절차

- 1 다음 방법 중 하나로 감독자 배포를 시작합니다.
 - 감독자가 아직 배포되지 않은 경우 [워크로드 관리](#) 페이지에서 **시작**을 클릭합니다.
 - 환경에 추가 감독자를 배포하려면 [워크로드 관리 > 감독자 > 감독자 > 감독자 추가](#)를 선택합니다.

- 2 오른쪽 상단 모서리에서 **구성 가져오기**를 선택합니다.

vSphere Client는 JSON 파일의 값을 확인합니다. 업로드된 파일이 유효하지 않거나 JSON이 손상된 경우 오류가 표시될 수 있습니다. 마찬가지로 JSON 파일에 규격 버전이 없거나 규격 버전이 클라이언트에서 현재 지원되는 버전을 초과하는 경우 오류가 나타납니다. 따라서 구성 파일을 가져오기 전에 필요한 설정만 편집해야 합니다. 파일이 손상된 경우 JSON 스키마를 사용하여 필요한 값으로 채울 수 있는 빈 감독자 구성을 생성할 수 있습니다.

- 3 **감독자 구성 업로드** 대화상자에서 **업로드**를 클릭하고 이전에 내보낸 JSON 구성 파일을 선택합니다.

4 가져오기를 클릭합니다.

JSON 구성 파일에 기록된 값이 감독자 활성화 마법사에 채워집니다. 로드 밸런서 암호와 같은 특정 설정은 수동으로 입력해야 할 수도 있습니다.

5 마법사를 진행하면서 다음을 클릭하고 필요한 경우 값을 입력합니다.

6 검토 및 확인 페이지에서 위로 스크롤하여 지금까지 구성한 모든 설정을 검토하고 필요한 경우 최종 변경합니다.

7 설정을 검토할 준비가 되면 마침을 클릭합니다.

감독자를 활성화하면 제어부 VM 및 기타 구성 요소의 생성 및 구성이 시작됩니다.

다음에 수행할 작업

감독자를 사용하도록 설정하는 마법사를 완료하면 활성화 프로세스를 추적하고 문제 해결이 필요한 잠재적인 문제를 관찰할 수 있습니다. 구성 상태 열에서 의 상태 옆에 있는 보기감독자를 클릭합니다.

그림 9-1. 감독자 활성화 보기

Configuring supervisor ×

Supervisor configuration follows a desired state in which it will keep retrying to reach a condition. Conditions can transition from a configured state to configuring based on dependencies. Monitor for any errors that require attention.

14 of 16 conditions reached 290 minutes since last condition change

Object	↑	▼
supervisor (Supervisor)	»	
SupervisorControlPlaneVM (1)	»	
SupervisorControlPlaneVM (2)	»	
SupervisorControlPlaneVM (3)	«	

SupervisorControlPlaneVM (3) ×

- ✔ Customized guest of Supervisor Control plane VM
- ✔ Configured Supervisor Control plane VM's Management Network
- ✔ Configured Supervisor Control plane VM as Kubernetes Control Plane Node
- ✔ Configured Supervisor Control plane VM's Workload Network

1-4 / 4 < 1 >

OK

배포 프로세스가 완료되려면 감독자가 원하는 상태에 도달해야 합니다. 즉 모든 조건이 충족되어야 합니다. 감독자가 사용되도록 설정하는 데 성공하면 해당 상태가 [구성 중]에서 [실행 중]으로 변경됩니다. 감독자가 [구성 중] 상태에 있는 동안 각 조건에 도달하기 위한 재시도가 계속됩니다. 조건에 도달하지 않으면 성공할 때까지 작업이 재시도됩니다. 이러한 이유로 인해 도달한 조건 수가 오락가락 변경될 수 있습니다(예: "16개 중 10개 조건에 도달" 후 "16개 중 4개 조건에 도달" 등). 매우 드문 경우지만 원하는 상태에 도달하지 못하게 하는 오류가 있는 경우 상태가 오류로 변경될 수 있습니다.

배포 오류 및 문제 해결 방법에 대한 자세한 내용은 [활성화 또는 업데이트 중 감독자 제어부 VM의 오류 상태 해결](#)을 참조하십시오.

감독자에 라이선스 할당

10

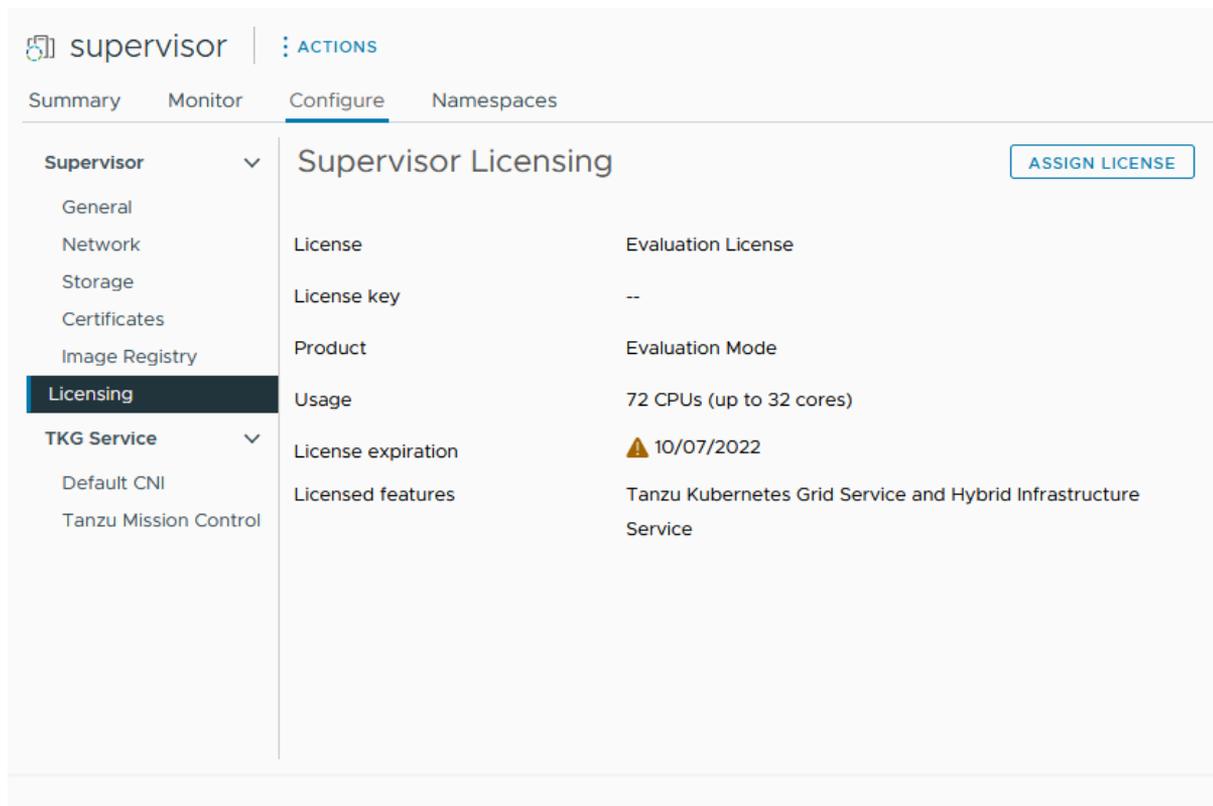
평가 모드에서 감독자를 사용하는 경우에는 60일 평가 기간이 만료되기 전에 클러스터에 솔루션 라이선스(VVF 또는 VCF) 또는 Tanzu Edition 라이선스를 할당해야 합니다.

Tanzu 라이선스의 작동 방식에 대한 자세한 내용은 [vSphere IaaS control plane에 대한 라이선싱 항목](#)을 참조하십시오.

절차

- 1 vSphere Client에서 **워크로드 관리**로 이동합니다.
- 2 **감독자**를 선택하고 목록에서 감독자를 선택합니다.
- 3 **구성 > 라이선싱**을 선택합니다.

그림 10-1. 감독자 UI에 라이선스 할당



- 4 **라이선스 할당**을 클릭합니다.
- 5 **라이선스 할당** 대화 상자에서 **새 라이선스**를 클릭합니다.
- 6 유효한 라이선스 키를 입력하고 **확인**을 클릭합니다.

vSphere IaaS control plane 클러스터에 연결

11

감독자에 연결하여 Tanzu Kubernetes 클러스터, vSphere 포드 및 VM을 프로비저닝합니다. 프로비저닝한 후에는 다양한 방법을 사용하여 Tanzu Kubernetes Grid 클러스터에 연결하고 사용자의 역할과 목표를 기반으로 인증할 수 있습니다.

다음으로 아래 항목을 읽으십시오.

- vSphere에 대한 Kubernetes CLI 도구 다운로드 및 설치
- vSphere IaaS control plane 클러스터에 대한 보안 로그인 구성
- vCenter Single Sign-On 사용자로 감독자에 연결
- 개발자에게 Tanzu Kubernetes 클러스터에 대한 액세스 권한 부여

vSphere에 대한 Kubernetes CLI 도구 다운로드 및 설치

vSphere에 대한 Kubernetes CLI 도구를 사용하여 감독자 제어부에 로그인하고, 사용 권한이 있는 vSphere 네임스페이스에 액세스하고, vSphere 포드, Tanzu Kubernetes Grid 클러스터 및 VM을 배포 및 관리할 수 있습니다.

Kubernetes CLI 도구 다운로드 패키지에는 표준 오픈 소스 kubectl 및 kubectl용 vSphere 플러그인의 두 실행 파일이 포함됩니다. kubectl CLI에는 플러그형 아키텍처가 있습니다. kubectl용 vSphere 플러그인은 vCenter Single Sign-On 자격 증명을 통해 감독자 및 Tanzu Kubernetes Grid 클러스터에 연결할 수 있도록 kubectl에 사용 가능한 명령을 확장합니다.

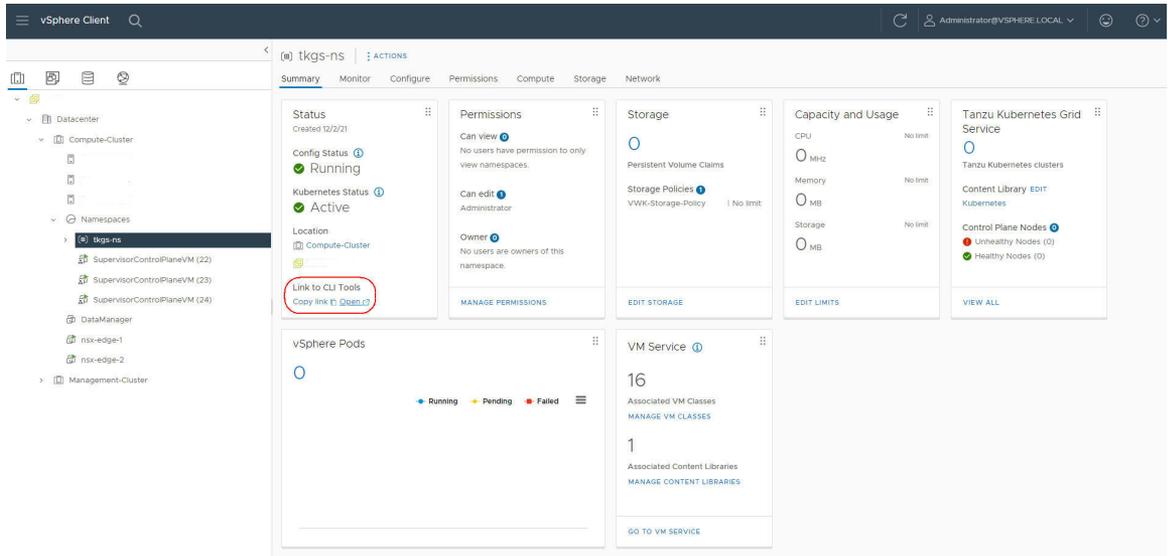
참고 vSphere 네임스페이스 업데이트를 수행하고 감독자를 업그레이드한 후 kubectl용 vSphere 플러그인을 업데이트하는 것이 가장 좋습니다. "vSphere IaaS 제어부 유지 보수" 에서 [kubectl용 vSphere 플러그인 업데이트](#)를 참조하십시오.

절차

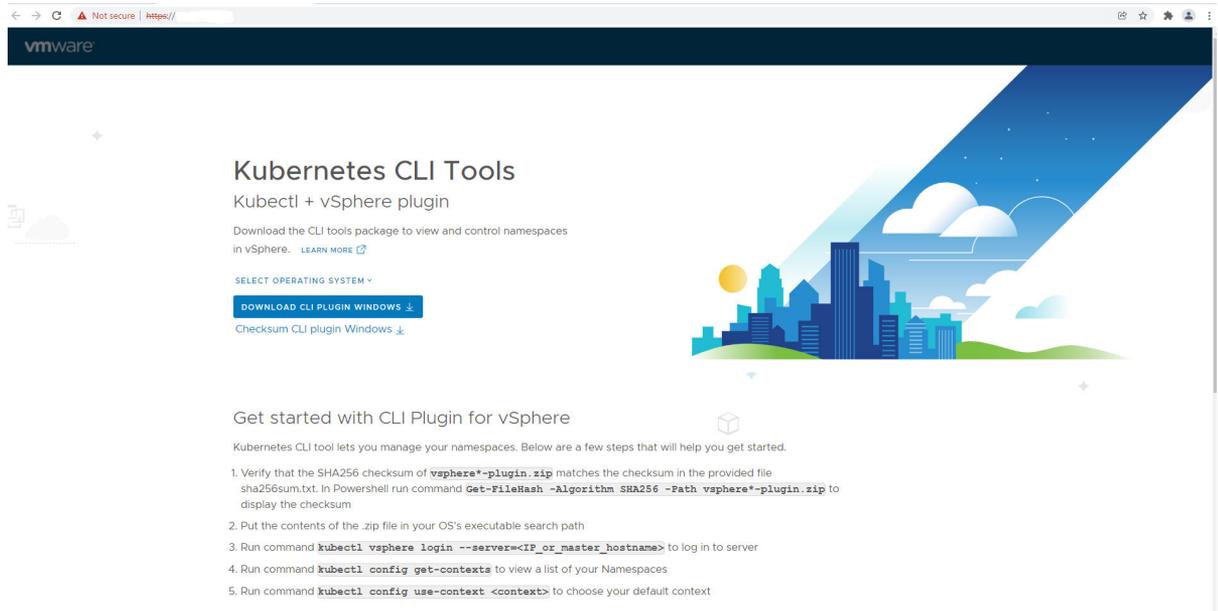
- 1 vSphere에 대한 Kubernetes CLI 도구의 다운로드 URL이기도 한 감독자 제어부의 IP 주소 또는 FQDN을 가져옵니다.

vSphere 환경에 대한 액세스 권한이 없는 DevOps 엔지니어인 경우 vSphere 관리자에게 아래 단계를 수행하도록 요청할 수 있습니다.

- a vSphere Client에서 워크로드 관리 > 네임스페이스로 이동한 후 vSphere 네임스페이스를 선택합니다.
- b 요약 탭을 선택하고 상태 창을 찾습니다.
- c CLI 도구에 연결에서 열기 또는 링크 복사를 클릭합니다.



- 2 브라우저에서 Kubernetes CLI 도구 다운로드 URL을 엽니다.



- 3 운영 체제를 선택합니다.

4 `vsphere-plugin.zip` 파일을 다운로드합니다.

5 작업 디렉토리에 ZIP 파일 콘텐츠의 압축을 풉니다.

`vsphere-plugin.zip` 패키지에는 `kubectl` 및 `kubectl`용 vSphere 플러그인의 두 실행 파일이 포함되어 있습니다. `kubectl`은 표준 Kubernetes CLI입니다. `kubectl-vsphere`는 vCenter Single Sign-On 자격 증명을 사용하여 감독자 및 Tanzu Kubernetes 클러스터로 인증하는 데 도움이 되는 `kubectl`용 vSphere 플러그인입니다.

6 두 실행 파일의 위치를 시스템의 PATH 변수에 추가합니다.

7 `kubectl` CLI의 설치를 확인하려면 셸, 터미널 또는 명령 프롬프트 세션을 시작하고 `kubectl` 명령을 실행합니다.

`kubectl` 배너 메시지 및 CLI에 대한 명령줄 옵션 목록이 표시됩니다.

8 `kubectl`용 vSphere 플러그인의 설치를 확인하려면 `kubectl vsphere` 명령을 실행합니다.

`kubectl`용 vSphere 플러그인 배너 메시지 및 플러그인에 대한 명령줄 옵션 목록이 표시됩니다.

다음에 수행할 작업

[vSphere IaaS control plane 클러스터에 대한 보안 로그인 구성](#).

vSphere IaaS control plane 클러스터에 대한 보안 로그인 구성

감독자 및 Tanzu Kubernetes Grid 클러스터에 안전하게 로그인하려면 적절한 TLS 인증서로 `kubectl`용 vSphere 플러그인을 구성하고 최신 버전의 플러그인을 실행하고 있는지 확인합니다.

감독자 CA 인증서

vSphere IaaS control plane는 `kubectl`용 vSphere 플러그인 명령인 `kubectl vsphere login ...`을 사용하여 클러스터에 액세스할 수 있도록 vCenter Single Sign-On을 지원합니다. 이 유틸리티를 설치하고 사용하려면 [vSphere에 대한 Kubernetes CLI 도구 다운로드 및 설치](#) 항목을 참조하십시오.

`kubectl`용 vSphere 플러그인은 기본적으로 보안 로그인을 사용하고 신뢰할 수 있는 인증서가 필요하며, 기본값은 vCenter Server 루트 CA에서 서명한 인증서입니다. 플러그인은 `--insecure-skip-tls-verify` 플래그를 지원하지 않지만 보안상의 이유로 이 플래그는 권장되지 않습니다.

`kubectl`용 vSphere 플러그인을 사용하여 감독자 및 Tanzu Kubernetes Grid 클러스터에 안전하게 로그인하기 위한 두 가지 옵션이 있습니다.

옵션	지침
각 클라이언트 시스템에 vCenter Server 루트 CA 인증서를 다운로드하고 설치합니다.	VMware 기술 자료 문서 vCenter Server 루트 인증서를 다운로드하고 설치하는 방법 을 참조하십시오.
감독자에 사용되는 VIP 인증서를 각 클라이언트 시스템이 신뢰하는 CA에서 서명한 인증서로 바꿉니다.	VIP 인증서를 교체하여 감독자 API 끝점에 안전하게 연결 항목을 참조하십시오.

참고 vCenter Single Sign-On, vCenter Server 인증서 관리 및 순환, 인증 문제 해결을 비롯한 vSphere 인증에 대한 추가 정보는 [vSphere 인증 설명서](#)를 참조하십시오. vSphere IaaS control plane 인증서에 대한 자세한 내용은 VMware 기술 자료 문서 [89324](#)를 참조하십시오.

Tanzu Kubernetes Grid 클러스터 CA 인증서

kubectl CLI를 사용하여 Tanzu Kubernetes 클러스터 API 서버와 안전하게 연결하려면 Tanzu Kubernetes 클러스터 CA 인증서를 다운로드합니다.

최신 버전의 kubectl용 vSphere 플러그인을 사용하는 경우에는 Tanzu Kubernetes Grid 클러스터에 처음 로그인할 때 플러그인이 Tanzu Kubernetes 클러스터 CA 인증서를 kubeconfig 파일에 등록합니다. 이 인증서는 `TANZU-KUBERNETES-CLUSTER-NAME-ca`이라는 이름의 Kubernetes 암호에 저장됩니다. 플러그인은 이 인증서를 사용하여 해당 클러스터의 CA 데이터스토어에 CA 정보를 채웁니다.

vSphere IaaS control plane를 업데이트하는 경우 최신 버전의 플러그인으로 업데이트해야 합니다. "vSphere IaaS 제어부 유지 보수"에서 [kubectl용 vSphere 플러그인 업데이트](#)를 참조하십시오.

vCenter Single Sign-On 사용자로 감독자에 연결

vSphere 포드, Tanzu Kubernetes Grid 클러스터 또는 VM을 프로비저닝하려면 kubectl용 vSphere 플러그인을 사용하여 감독자에 연결하고 vCenter Single Sign-On 자격 증명을 사용하여 인증합니다.

감독자에 로그인하면 kubectl용 vSphere 플러그인은 감독자에 대한 컨텍스트를 생성합니다. Kubernetes에서 구성 컨텍스트에는 감독자, vSphere 네임스페이스 및 사용자가 포함됩니다. `.kube/config` 파일에서 클러스터 컨텍스트를 볼 수 있습니다. 이 파일은 일반적으로 `kubeconfig` 파일이라고 합니다.

참고 기존 kubeconfig 파일이 있는 경우 각 감독자 컨텍스트에 추가됩니다. kubectl용 vSphere 플러그인은 kubectl 자체에서 사용하는 KUBECONFIG 환경 변수를 고려합니다. 필요하지 않더라도 `kubectl vsphere login ...`을 실행하기 전에 이 변수를 설정하면 정보가 현재의 kubeconfig 파일에 추가되지 않고 새 파일에 기록되므로 유용할 수 있습니다.

사전 요구 사항

- vSphere 관리자로부터 vCenter Single Sign-On 자격 증명을 얻습니다.
- vSphere 관리자로부터 감독자 제어부의 IP 주소를 얻습니다. 감독자 제어부 IP 주소는 vSphere Client의 **워크로드 관리** 아래에 있는 각 vSphere 네임스페이스의 사용자 인터페이스 아래에 연결됩니다.
- 제어부 IP 주소 대신 FQDN을 사용하여 로그인하려면 사용 설정 중에 감독자에 구성된 FQDN을 가져옵니다.
- 사용 권한이 있는 vSphere 네임스페이스의 이름을 가져옵니다.

- vSphere 네임스페이스에 대한 **편집** 권한이 있는지 확인합니다.
- vSphere에 대한 **Kubernetes CLI 도구 다운로드 및 설치**.
- 서명 CA를 신뢰 루트로 설치하거나 인증서를 신뢰 루트로 직접 추가하여 Kubernetes 제어부가 제공하는 인증서를 시스템에서 신뢰할 수 있는지 확인합니다. **vSphere IaaS control plane 클러스터에 대한 보안 로그인 구성**의 내용을 참조하십시오.

절차

- 1 로그인을 위한 명령 구문 및 옵션을 보려면 다음 명령을 실행합니다.

```
kubectl vsphere login --help
```

- 2 감독자에 연결하려면 다음 명령을 실행합니다.

```
kubectl vsphere login --server=<KUBERNETES-CONTROL-PLANE-IP-ADDRESS> --vsphere-username <VCENTER-SSO-USER>
```

및 FQDN을 사용하여 로그인할 수도 있습니다.

```
kubectl vsphere login --server <KUBERNETES-CONTROL-PLANE-FQDN> --vsphere-username <VCENTER-SSO-USER>
```

예:

```
kubectl vsphere login --server=10.92.42.13 --vsphere-username administrator@example.com
```

```
kubectl vsphere login --server wonderland.acme.com --vsphere-username administrator@example.com
```

이 작업은 Kubernetes API에 인증하기 위한 JWT(JSON Web Token)가 들어 있는 구성 파일을 생성합니다.

- 3 인증하려면 사용자 암호를 입력합니다.

감독자에 연결한 후에는 구성 컨텍스트가 액세스할 수 있는 것으로 표시됩니다. 예:

```
You have access to the following contexts:
tanzu-ns-1
tkg-cluster-1
tkg-cluster-2
```

- 4 액세스할 수 있는 구성 컨텍스트의 세부 정보를 보려면 다음 `kubectl` 명령을 실행합니다.

```
kubectl config get-contexts
```

CLI에는 사용 가능한 각 컨텍스트에 대한 세부 정보가 표시됩니다.

5 컨텍스트 간에 전환하려면 다음 명령을 사용합니다.

```
kubectl config use-context <example-context-name>
```

다음에 수행할 작업

vCenter Single Sign-On으로 Tanzu Kubernetes Grid 클러스터에 연결합니다. 자세한 내용은 "vSphere IaaS 제어부에서 TKG 서비스 사용" 에서 [vCenter Single Sign-On 사용자로 TKG 클러스터에 연결을 참조하십시오](#).

개발자에게 Tanzu Kubernetes 클러스터에 대한 액세스 권한 부여

개발자는 Kubernetes의 대상 사용자입니다. Tanzu Kubernetes 클러스터가 프로비저닝되면 vCenter Single Sign-On 인증을 사용하여 개발자에게 액세스 권한을 부여할 수 있습니다.

개발자에 대한 인증

클러스터 관리자는 개발자와 같은 다른 사용자에게 클러스터 액세스 권한을 부여할 수 있습니다. 개발자는 사용자 계정을 사용하여 직접 클러스터에 포드를 배포하거나 간접적으로 서비스 계정을 사용할 수 있습니다. 자세한 내용은 "vSphere IaaS 제어부에서 TKG 서비스 사용" 에서 [개발자에게 워크로드 클러스터에 대한 SSO 액세스 권한 부여를 참조하십시오](#).

- 사용자 계정 인증의 경우 Tanzu Kubernetes 클러스터가 vCenter Single Sign-On 사용자 및 그룹을 지원합니다. 사용자 또는 그룹은 vCenter Server에 대해 로컬이거나 지원되는 디렉토리 서버에서 동기화될 수 있습니다.
- 서비스 계정 인증의 경우 서비스 토큰을 사용할 수 있습니다. 자세한 내용은 Kubernetes 설명서를 참조하십시오.

클러스터에 개발자 사용자 추가

개발자에게 클러스터 액세스 권한을 부여하려면 다음을 수행합니다.

- 1 사용자 또는 그룹에 대한 역할 또는 ClusterRole을 정의하고 클러스터에 적용합니다. 자세한 내용은 Kubernetes 설명서를 참조하십시오.
- 2 사용자 또는 그룹에 대한 RoleBinding 또는 ClusterRoleBinding을 생성하고 클러스터에 적용합니다. 다음 예를 참조하십시오.

RoleBinding 예

vCenter Single Sign-On 사용자 또는 그룹에 액세스 권한을 부여하려면 RoleBinding의 주체에 `name` 매개 변수에 대한 다음 값 중 하나를 포함해야 합니다.

표 11-1. 지원되는 사용자 및 그룹 필드

필드	설명
<code>sso:USER-NAME@DOMAIN</code>	예를 들어 로컬 사용자 이름(예: <code>sso:joe@vsphere.local</code>)을 입력합니다.
<code>sso:GROUP-NAME@DOMAIN</code>	예를 들어 디렉토리 서버의 그룹 이름이 vCenter Server(예: <code>sso:devs@ldap.example.com</code>)와 통합되었습니다.

다음 RoleBinding 예는 이름이 Joe인 vCenter Single Sign-On 로컬 사용자를 이름이 `edit`인 기본 ClusterRole에 바인딩합니다. 이 역할은 네임스페이스에 있는 대부분의 개체(이 경우 `default` 네임스페이스)에 대한 읽기/쓰기 액세스를 허용합니다.

```
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: rolebinding-cluster-user-joe
  namespace: default
roleRef:
  kind: ClusterRole
  name: edit                                #Default ClusterRole
  apiGroup: rbac.authorization.k8s.io
subjects:
- kind: User
  name: sso:joe@vsphere.local              #sso:<username>@<domain>
  apiGroup: rbac.authorization.k8s.io
```

감독자 구성 및 관리

12

vSphere 관리자는 vSphere 클러스터를 감독자로 사용하도록 설정합니다. vSphere 네트워킹 스택 또는 VMware NSX®(NSX)를 네트워킹 솔루션으로 사용하여 감독자를 생성할 수 있습니다. NSX로 구성된 클러스터는 VMware Tanzu™ Kubernetes Grid™를 통해 생성된 vSphere 포드 및 Tanzu Kubernetes 클러스터 실행을 지원합니다. vSphere 네트워킹 스택으로 구성된 감독자는 Tanzu Kubernetes 클러스터만 지원합니다.

감독자를 사용하도록 설정한 후에는 vSphere Client를 사용하여 클러스터를 관리하고 모니터링할 수 있습니다.

다음으로 아래 항목을 읽으십시오.

- VIP 인증서를 교체하여 감독자 API 끝점에 안전하게 연결
- 감독자의 Tanzu Kubernetes Grid를 Tanzu Mission Control과 통합
- Tanzu Kubernetes Grid 클러스터에 대한 기본 CNI 설정
- 감독자의 제어부 크기 변경
- VDS 네트워킹으로 구성된 감독자에서 로드 밸런서 설정 변경
- VDS 네트워킹으로 구성된 감독자에 워크로드 네트워크 추가
- 감독자에서 관리 네트워크 설정 변경
- VDS 네트워킹으로 구성된 감독자에서 워크로드 네트워크 설정 변경
- NSX로 구성된 감독자에서 워크로드 네트워크 설정 변경
- vSphere IaaS control plane에서 HTTP 프록시 설정 구성
- TKG 서비스 클러스터와 함께 사용할 외부 IDP 구성
- 외부 IDP를 감독자에 등록
- 감독자의 스토리지 설정 변경
- 사용자 지정 관찰 가능성 플랫폼으로 감독자 메트릭 스트리밍
- 감독자 제어부 DNS 이름 목록 수정
- 외부 모니터링 시스템에 감독자 로그 전달

VIP 인증서를 교체하여 감독자 API 끝점에 안전하게 연결

vSphere 관리자는 VIP(가상 IP 주소)의 인증서를 교체하여 호스트가 이미 신뢰하는 CA에서 서명한 인증서로 감독자 API 끝점에 안전하게 연결할 수 있습니다. 이 인증서는 로그인하는 동안과 감독자와의 후속 상호 작용 동안 DevOps 엔지니어에 대한 Kubernetes 제어부를 인증합니다.

사전 요구 사항

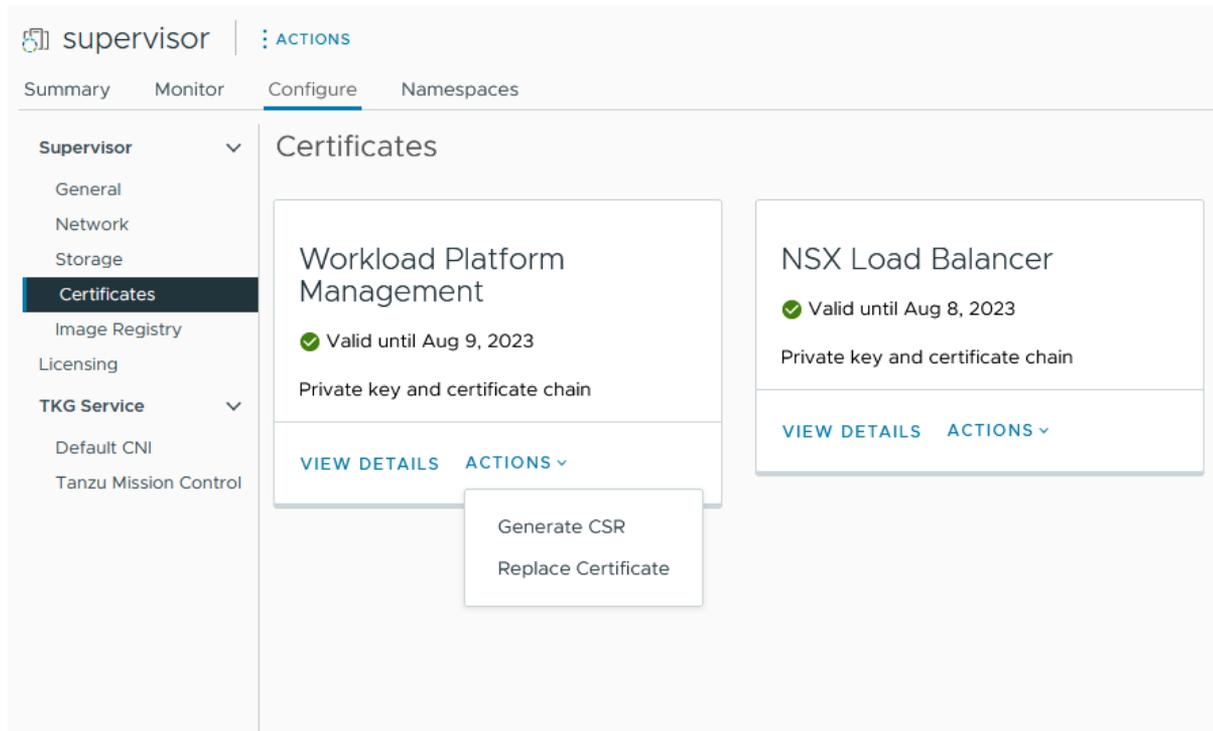
CSR에 서명할 수 있는 CA에 대한 액세스 권한이 있는지 확인합니다. DevOps 엔지니어의 경우 시스템에 CA를 신뢰할 수 있는 루트로 설치해야 합니다.

감독자 인증서에 대한 자세한 내용은 [감독자 CA 인증서](#) 항목을 참조하십시오.

절차

- 1 vSphere Client에서 **워크로드 관리**로 이동합니다.
- 2 **감독자**를 선택하고 목록에서 감독자를 선택합니다.
- 3 **구성**을 클릭하고 **인증서**를 선택합니다.
- 4 **워크로드 관리 플랫폼** 창에서 **작업 > CSR 생성**을 선택합니다.

그림 12-1. 감독자 기본 인증서 교체



- 5 인증서에 대한 세부 정보를 제공합니다.

참고 ID 제공자 서비스를 사용하는 경우 전체 인증서 체인도 포함해야 합니다. 그러나 표준 HTTPS 트래픽에는 체인이 필요하지 않습니다.

- 6 CSR이 생성되면 **복사**를 클릭합니다.
- 7 CA를 사용하여 인증서에 서명합니다.
- 8 **워크로드 플랫폼 관리** 창에서 **작업 > 인증서 바꾸기**를 선택합니다.
- 9 서명된 인증서 파일을 업로드하고 **인증서 바꾸기**를 클릭합니다.
- 10 Kubernetes 제어부의 IP 주소의 인증서를 확인합니다.

예를 들어 vSphere에 대한 Kubernetes CLI 도구 다운로드 페이지를 열고 브라우저를 사용하여 인증서가 성공적으로 바뀌었는지 확인할 수 있습니다. Linux 또는 Unix 시스템에서는 `echo | openssl s_client -connect https://ip:6443`을 사용할 수도 있습니다.

감독자의 Tanzu Kubernetes Grid를 Tanzu Mission Control과 통합

감독자에서 실행되는 Tanzu Kubernetes Grid를 Tanzu Mission Control과 통합할 수 있습니다. 이렇게 하면 Tanzu Mission Control을 사용하여 Tanzu Kubernetes 클러스터를 프로비저닝하고 관리할 수 있습니다.

Tanzu Mission Control에 대한 자세한 내용은 [Tanzu Kubernetes 클러스터 수명 주기 관리](#)를 참조하십시오. 데모를 보려면 [Tanzu Kubernetes Grid 서비스와 통합된 Tanzu Mission Control 비디오](#)를 참조하십시오.

감독자에서 Tanzu Mission Control 네임스페이스 보기

vSphere IaaS control plane v7.0.1 U1 이상에는 Tanzu Mission Control용 vSphere 네임스페이스가 제공됩니다. 이 네임스페이스는 Tanzu Mission Control 에이전트를 설치한 감독자에 있습니다. 에이전트가 설치되면 Tanzu Mission Control 웹 인터페이스를 사용하여 Tanzu Kubernetes Grid 클러스터를 프로비저닝하고 관리할 수 있습니다.

- 1 kubectl용 vSphere 플러그인을 사용하여 감독자로 인증합니다. [vCenter Single Sign-On 사용자로 감독자에 연결](#)의 내용을 참조하십시오.
- 2 컨텍스트를 감독자로 전환합니다. 예:

```
kubectl config use-context 10.199.95.59
```

- 3 다음 명령을 실행하여 네임스페이스를 나열합니다.

```
kubectl get ns
```

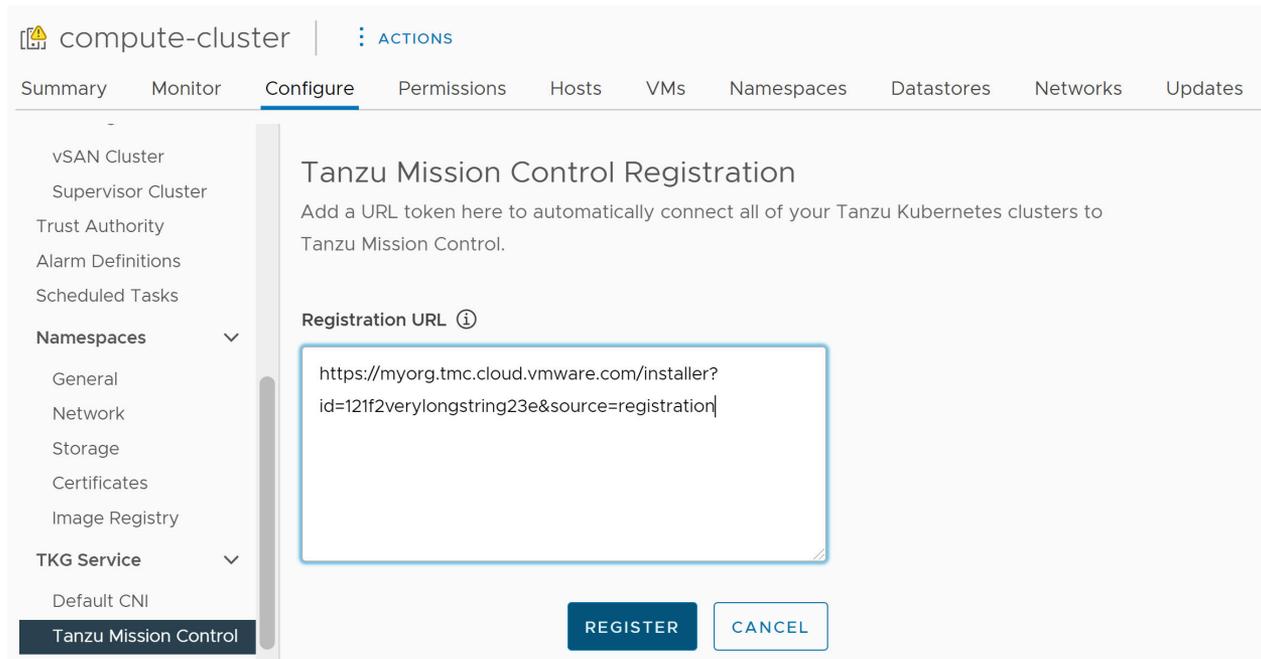
- 4 Tanzu Mission Control에 제공되는 vSphere 네임스페이스는 `svc-tmc-cXX`(여기서 XX는 숫자)로 식별됩니다.
- 5 이 네임스페이스에 Tanzu Mission Control 에이전트를 설치합니다. [감독자에 Tanzu Mission Control 에이전트 설치](#)의 내용을 참조하십시오.

감독자에 Tanzu Mission Control 에이전트 설치

Tanzu Kubernetes Grid를 Tanzu Mission Control과 통합하려면 감독자에 에이전트를 설치합니다.

참고 다음 절차를 수행하려면 감독자 버전 1.21.0 이상이 있는 vSphere 7.0 U3 이상이 필요합니다.

- 1 Tanzu Mission Control 웹 인터페이스를 사용하여 Tanzu Mission Control에 감독자를 등록합니다. [Tanzu Mission Control에 관리 클러스터 등록](#)을 참조하십시오.
- 2 Tanzu Mission Control 웹 인터페이스를 사용하여 **관리 > 관리 클러스터**로 이동하여 등록 URL을 가져옵니다.
- 3 Tanzu Mission Control에 필요한 포트(일반적으로 443)에 대해 vSphere IaaS control plane 환경에서 방화벽 포트를 엽니다. [클러스터 에이전트 확장에 의한 아웃바운드 연결](#)을 참조하십시오.
- 4 vSphere Client를 사용하여 vSphere IaaS control plane 환경에 로그인합니다.
- 5 **워크로드 관리**를 선택하고 감독자를 선택합니다.
- 6 **구성**을 선택하고 **TKG 서비스 > Tanzu Mission Control**을 선택합니다.
- 7 **등록 URL** 필드에 등록 URL을 제공합니다.
- 8 **등록**을 클릭합니다.



Tanzu Mission Control 에이전트 제거

감독자에서 Tanzu Mission Control 에이전트를 제거하려면 vSphere IaaS control plane의 감독자 클러스터에서 클러스터 에이전트를 수동으로 제거를 참조하십시오.

Tanzu Kubernetes Grid 클러스터에 대한 기본 CNI 설정

vSphere 관리자는 Tanzu Kubernetes 클러스터에 대한 기본 CNI(Container Network Interface)를 설정할 수 있습니다.

기본 CNI

Tanzu Kubernetes Grid는 Tanzu Kubernetes Grid 클러스터에 대해 **Antrea** 및 **Calico**라는 두 가지 CNI 옵션을 지원합니다.

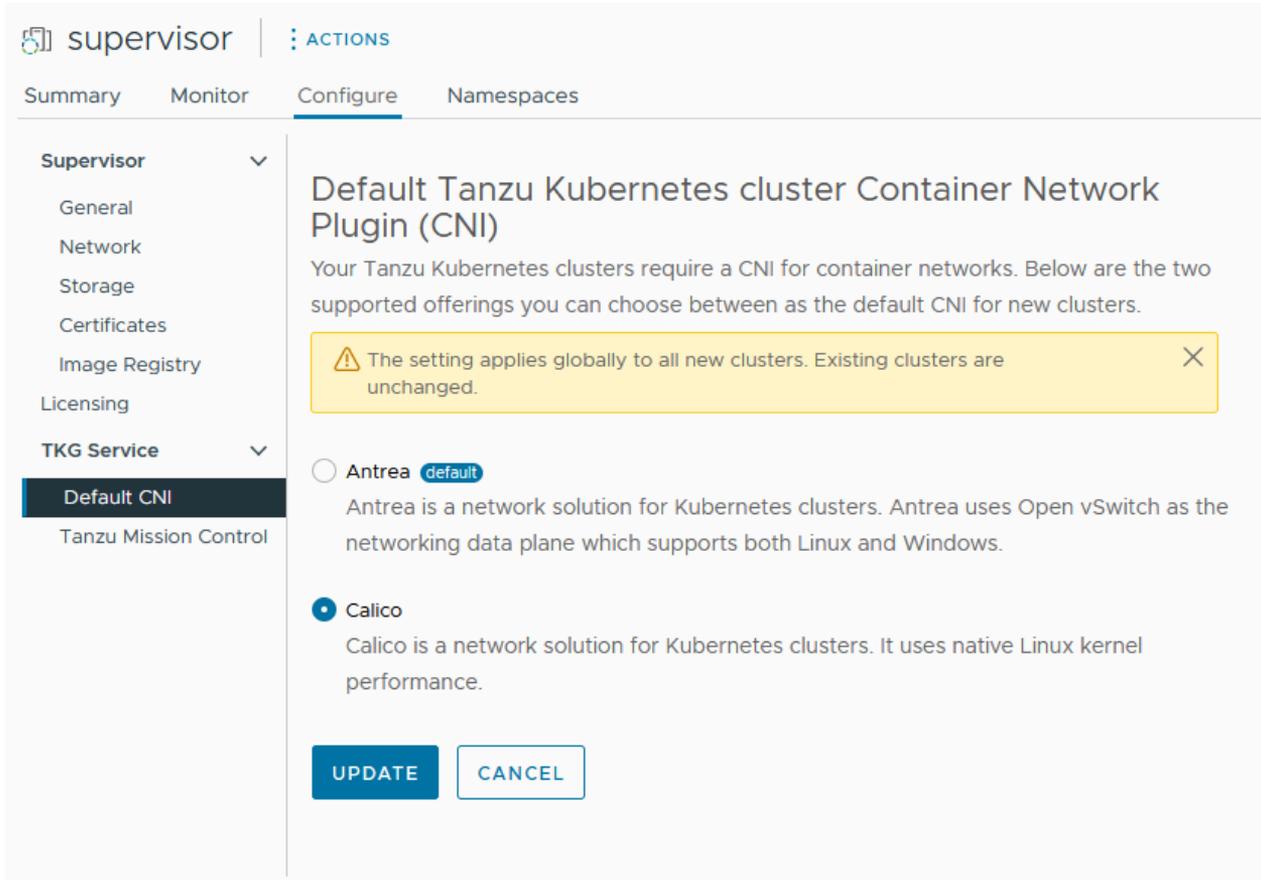
시스템 정의 기본 CNI는 Antrea입니다. 기본 CNI 설정에 대한 자세한 내용은 "vSphere IaaS 제어부에서 TKG 서비스 사용" 항목을 참조하십시오.

vSphere Client를 사용하여 기본 CNI를 변경할 수 있습니다. 기본 CNI를 설정하려면 다음 절차를 완료합니다.

경고 기본 CNI를 변경하는 것은 글로벌 작업입니다. 새로 설정된 기본값은 서비스에서 생성된 모든 새 클러스터에 적용됩니다. 기존 클러스터는 변경되지 않습니다.

- 1 vSphere Client를 사용하여 vSphere IaaS control plane 환경에 로그인합니다.
- 2 **워크로드 관리**를 선택하고 **감독자**를 선택합니다.
- 3 목록에서 감독자 인스턴스를 선택합니다.
- 4 **구성**를 선택하고 **TKG 서비스 > 기본 CNI**를 선택합니다.
- 5 새 클러스터에 대한 기본 CNI를 선택합니다.
- 6 **업데이트**를 클릭합니다.

다음 이미지는 기본 CNI 선택 항목을 보여줍니다.



다음 이미지는 CNI 선택을 Antrea에서 Calico로 변경하는 것을 보여줍니다.

supervisor | ACTIONS

Summary Monitor **Configure** Namespaces

Supervisor ▾

- General
- Network
- Storage
- Certificates
- Image Registry
- Licensing

TKG Service ▾

- Default CNI**
- Tanzu Mission Control

Default Tanzu Kubernetes cluster Container Network Plugin (CNI)

Your Tanzu Kubernetes clusters require a CNI for container networks. Below are the two supported offerings you can choose between as the default CNI for new clusters.

✔ The Tanzu Kubernetes Grid Service configuration was successfully updated! ✕

Antrea default

Antrea is a network solution for Kubernetes clusters. Antrea uses Open vSwitch as the networking data plane which supports both Linux and Windows.

Calico

Calico is a network solution for Kubernetes clusters. It uses native Linux kernel performance.

UPDATE

감독자의 제어부 크기 변경

vSphere IaaS control plane 환경에서 감독자의 Kubernetes 제어부 VM의 크기를 변경하는 방법을 알아보니다.

사전 요구 사항

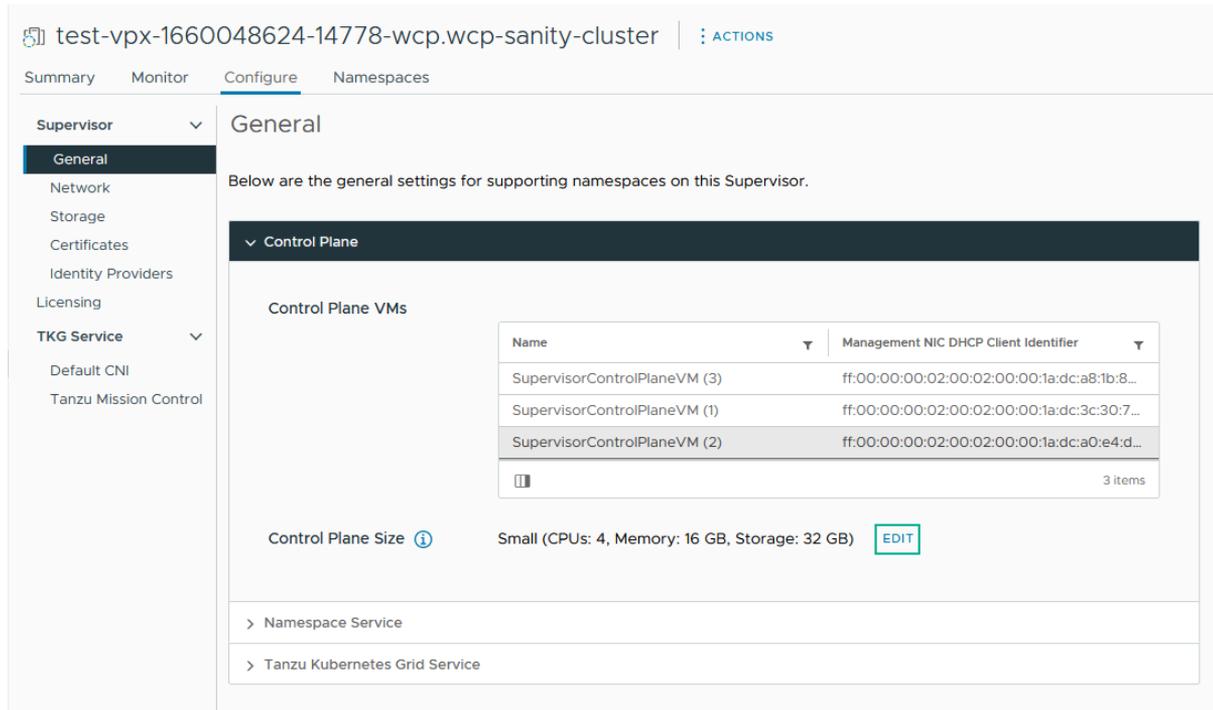
- 클러스터에서 **클러스터 전체 구성 수정** 권한이 있는지 확인합니다.

절차

- 1 vSphere Client에서 **워크로드 관리**로 이동합니다.
- 2 **감독자**에서 감독자를 선택합니다.
- 3 **구성**을 선택하고 **일반**을 선택합니다.

4 제어부 크기를 확장합니다.

그림 12-2. 감독자 제어부 설정



5 편집을 클릭하고 드롭다운 메뉴에서 새 제어부 크기를 선택합니다.

옵션	설명
매우 작음	CPU 2개, 8GB 메모리, 32GB 스토리지
작음	CPU 4개, 16GB 메모리, 32GB 스토리지
중간	CPU 8개, 16GB 메모리, 32GB 스토리지
큼	CPU 16개, 32GB 메모리, 32GB 스토리지

참고 제어부 크기를 선택하고 나면 스케일 다운할 수 없습니다. 예를 들어 감독자를 활성화하는 동안 [매우 작음] 옵션을 이미 설정한 경우에는 이 옵션에서 스케일 업만 가능합니다.

6 저장을 클릭합니다.

제어부 크기는 스케일 업만 가능합니다.

VDS 네트워킹으로 구성된 감독자에서 로드 밸런서 설정 변경

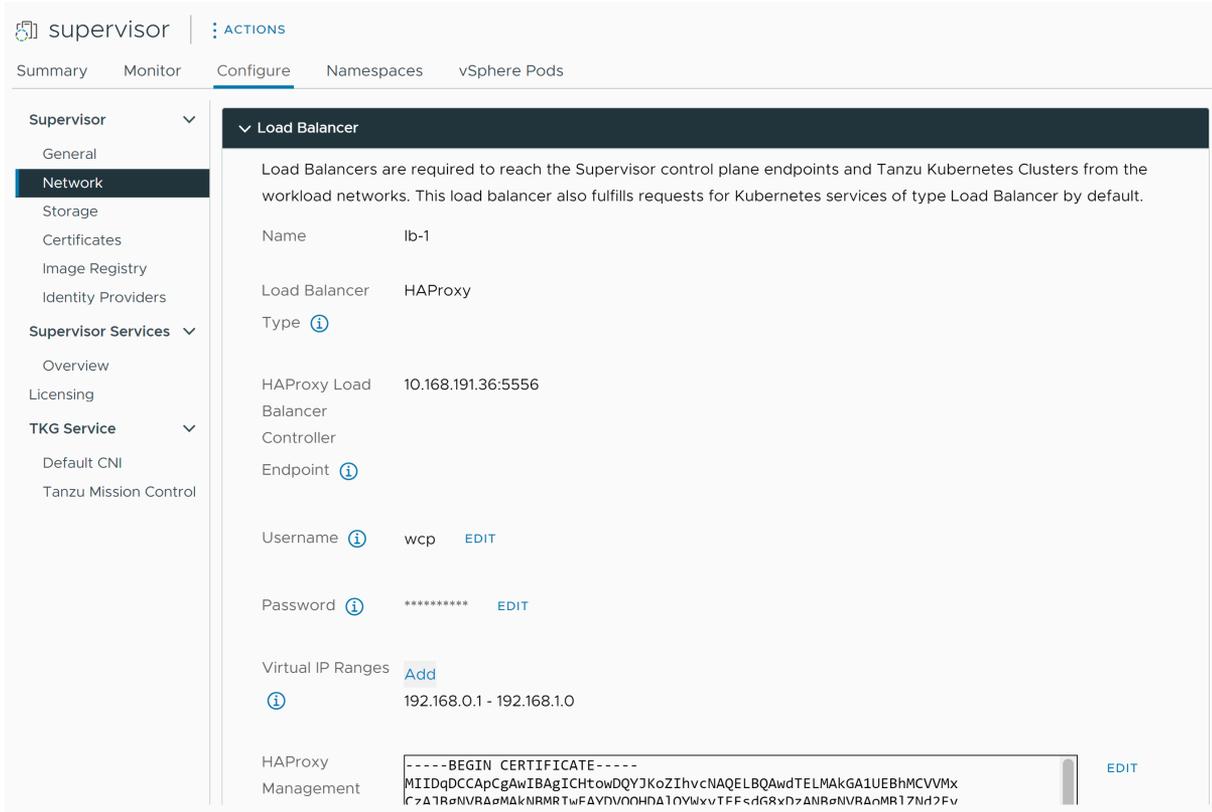
감독자에서 VDS 네트워킹 스택으로 구성된 로드 밸런서의 설정을 변경하는 방법을 확인합니다. 사용자 이름 및 암호와 같은 설정을 변경하고, 새 IP 범위를 추가하고, 로드 밸런서에 사용되는 인증서를 업데이트할 수 있습니다.

사전 요구 사항

- 클러스터에서 클러스터 전체 구성 수정 권한이 있는지 확인합니다.

절차

- 1 vSphere Client에서 워크로드 관리로 이동합니다.
- 2 감독자에서 감독자를 선택하고 구성을 선택합니다.
- 3 네트워크를 선택하고 워크로드 네트워크를 확장합니다.



옵션	설명
설정	설명
사용자 이름	감독자가 로드 밸런서 끝점에서 인증하는 데 사용하는 사용자 이름을 편집합니다.
암호	감독자가 로드 밸런서 끝점에서 인증하는 데 사용하는 암호를 변경합니다.
가상 IP 범위	로드 밸런서로 처음 구성한 가상 IP CIDR 범위의 하위 집합인 IP 범위를 추가합니다. 참고 새 IP 범위만 추가할 수 있습니다. 기존 IP 범위는 제거하거나 변경할 수 없습니다.
TLS 인증서	감독자와 로드 밸런서 간의 보안 연결을 보장하는 데 사용되는 TLS 인증서를 변경합니다.

VDS 네트워킹으로 구성된 감독자에 워크로드 네트워크 추가

vSphere 네트워킹 스택으로 구성된 감독자의 경우 워크로드 네트워크를 생성하고 이것을 네임스페이스에 할당하여 Kubernetes 워크로드에 계층 2 분리를 제공할 수 있습니다. 워크로드 네트워크는 네임스페이스의 Tanzu Kubernetes Grid 클러스터에 대한 연결을 제공하며 감독자의 호스트에 연결된 스위치의 분산 포트 그룹에서 지원됩니다.

감독자에 대해 구현할 수 있는 토폴로지에 대한 자세한 내용은 "vSphere IaaS 제어부 개념 및 계획" 에서 vSphere 네트워킹 및 NSX Advanced Load Balancer를 사용하는 감독자용 토폴로지 또는 HAProxy 로드 밸런서 배포를 위한 토폴로지를 참조하십시오.

참고 워크로드 네트워크에 대한 네트워킹 설정을 제공하는 DHCP 서버로 감독자를 구성한 경우에는 감독자 구성 후에 새 워크로드 네트워크를 생성할 수 없습니다.

사전 요구 사항

- 워크로드 네트워크를 지원할 분산 포트 그룹을 생성합니다.
- 워크로드 네트워크에 할당할 IP 범위가 환경에서 사용 가능한 모든 감독자 내에서 고유한지 확인합니다.

절차

- 1 vSphere Client에서 **워크로드 관리**로 이동합니다.
- 2 **감독자**에서 감독자를 선택합니다.
- 3 **구성**을 선택하고 **네트워크**를 선택합니다.

그림 12-3. 감독자 워크로드 네트워크 추가

The screenshot shows the vSphere Client interface for configuring a Supervisor's Network. The 'Workload Network' section is expanded, showing a table of existing networks and options to add, edit, or remove them.

Network Name	Network Mode	Port Group	IP Address Range(s)	Subnet Mask	Gateway
lifecycle-test-network	Static Mode	primary	[Redacted]	255.255.0.0	192.168.1.1
network-1	Static Mode	network-1	[Redacted]	255.255.255.0	192.168.1.1
overlapping-range-test-network	Static Mode	primary	[Redacted]	255.255.0.0	192.168.1.1
primary	Static Mode	primary	[Redacted]	255.255.0.0	192.168.1.1

4 워크로드 네트워크를 선택하고 추가를 클릭합니다.

옵션	설명
포트 그룹	이 워크로드 네트워크와 연결할 분산 포트 그룹을 선택합니다. 감독자 네트워킹에 대해 구성된 VDS(vSphere Distributed Switch)에는 포트 그룹이 포함되어 있으며 그 중에 선택할 수 있습니다.
네트워크 이름	네임스페이스에 할당된 경우 워크로드 네트워크를 식별하는 네트워크 이름입니다. 이 값은 선택한 포트 그룹의 이름에서 자동으로 채워지지만 적절히 변경할 수 있습니다.
IP 주소 범위	Tanzu Kubernetes Grid 클러스터 노드의 IP 주소 할당을 위한 IP 범위를 입력합니다. IP 범위는 서브넷 마스크로 표시된 서브넷에 있어야 합니다. 참고 각 워크로드 네트워크에 대해 고유한 IP 주소 범위를 사용해야 합니다. 여러 네트워크에 대해 동일한 IP 주소 범위를 구성하지 마십시오.
서브넷 마스크	포트 그룹의 네트워크에 대한 서브넷 마스크의 IP 주소를 입력합니다.
게이트웨이	포트 그룹의 네트워크에 대한 기본 게이트웨이를 입력합니다. 게이트웨이는 서브넷 마스크로 표시된 서브넷에 있어야 합니다. 참고 HAProxy 로드 밸런서에 할당된 게이트웨이는 사용하지 마십시오.

5 추가를 클릭합니다.

다음에 수행할 작업

새로 생성된 워크로드 네트워크를 vSphere 네임스페이스에 할당합니다.

감독자에서 관리 네트워크 설정 변경

vSphere IaaS control plane 환경의 감독자 관리 네트워크에서 DNS 및 NTP 설정을 업데이트하는 방법을 알아봅니다.

사전 요구 사항

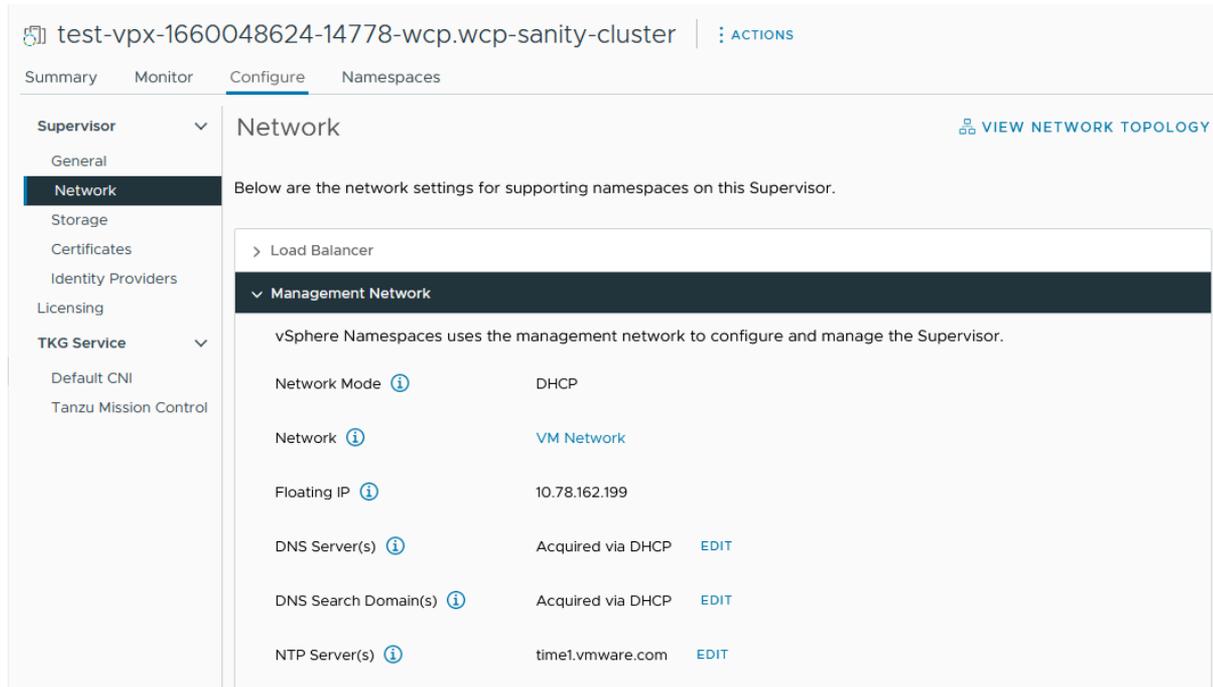
- 클러스터에서 클러스터 전체 구성 수정 권한이 있는지 확인합니다.

절차

- 1 vSphere Client에서 **워크로드 관리**를 선택합니다.
- 2 **감독자**에서 감독자를 선택하고 **구성**을 선택합니다.

3 네트워크를 선택하고 관리 네트워크를 확장합니다.

그림 12-4. 감독자 관리 네트워크 설정 업데이트



4 DNS 및 NTP 설정을 편집합니다.

옵션	설명
DNS 서버	환경에서 사용하는 DNS 서버의 주소를 입력합니다. vCenter Server 시스템이 FQDN으로 등록되어 있으면 vSphere 환경에 사용하는 DNS 서버의 IP 주소를 입력해야 합니다. 그래야 감독자에서 FQDN을 확인할 수 있습니다.
DNS 검색 도메인	Kubernetes 제어부 노드 내에서 DNS가 검색하는 도메인 이름(예: corp.local)을 입력합니다. 그래야 DNS 서버가 확인할 수 있습니다.
NTP 서버	환경에서 사용하는 NTP 서버의 주소를 입력합니다(있는 경우).

VDS 네트워킹으로 구성된 감독자에서 워크로드 네트워크 설정 변경

VDS 네트워킹 스택으로 구성된 감독자의 워크로드 네트워크에 대한 NTP 및 DNS 서버 설정을 변경하는 방법을 알아봅니다. 워크로드 네트워크에 대해 구성하는 DNS 서버는 Kubernetes 워크로드에 노출되는 외부 DNS 서버이며 감독자 외부에서 호스팅되는 기본 도메인 이름을 확인합니다.

사전 요구 사항

- 클러스터에서 클러스터 전체 구성 수정 권한이 있는지 확인합니다.

절차

- vSphere Client에서 워크로드 관리를 선택합니다.

- 2 **감독자**에서 감독자를 선택하고 **구성**을 선택합니다.
- 3 **네트워크**를 선택하고 **워크로드 네트워크**를 확장합니다.



참고 vSphere 네임스페이스에 이미 할당된 워크로드 네트워크는 제거할 수 없습니다. 워크로드 네트워크를 제거해야 하는 경우 해당 네트워크에 연결된 모든 vSphere 네임스페이스를 삭제해야 합니다. 또한 기본 워크로드 네트워크는 편집하거나 제거할 수 없습니다.

- 4 DNS 서버 설정을 편집합니다.

vSphere 관리 구성 요소의 도메인 이름을 확인할 수 있는 DNS 서버(예: vCenter Server)의 주소를 입력합니다.

예: 10.142.7.1.

DNS 서버의 IP 주소를 입력하면 각 제어부 VM에 정적 경로가 추가됩니다. 이것은 DNS 서버에 대한 트래픽이 워크로드 네트워크를 통과한다는 것을 나타냅니다.

지정하는 DNS 서버가 관리 네트워크와 워크로드 네트워크 간에 공유되는 경우에는 제어부 VM의 DNS 조회가 초기 설정 후 워크로드 네트워크를 통해 라우팅됩니다.

- 5 필요에 따라 NTP 설정을 편집합니다.
- 6 워크로드 네트워크 설정을 편집합니다.
 - a 워크로드 네트워크를 선택하고 **편집**을 클릭합니다.
 - b **IP 주소 범위** 옆에 있는 **추가**를 클릭하여 해당 네트워크의 워크로드에 사용할 새 IP 범위를 추가합니다. IP 범위는 서브넷 마스크로 표시된 서브넷에 있어야 합니다.

참고 추가하는 IP 범위는 로드 밸런서의 프론트 엔드 네트워크 구성에 대한 가상 IP와 겹치지 않아야 합니다.

NSX로 구성된 감독자에서 워크로드 네트워크 설정 변경

NSX에 대해 네트워킹 스택으로 구성된 감독자의 DNS 서버, 네임스페이스 네트워크, 수신 및 송신에 대한 네트워킹 설정을 변경하는 방법을 알아봅니다.

사전 요구 사항

- 클러스터에서 **클러스터 전체 구성 수정** 권한이 있는지 확인합니다.

절차

- 1 vSphere Client에서 워크로드 관리로 이동합니다.
- 2 감독자에서 감독자를 선택하고 구성을 선택합니다.
- 3 네트워크를 선택하고 워크로드 네트워크를 확장합니다.

그림 12-5. 감독자 워크로드 네트워크 설정 업데이트

The screenshot displays the Supervisor configuration interface for the Network section. The left sidebar shows the navigation menu with 'Network' selected under the 'Supervisor' section. The main content area is titled 'Network' and includes a 'VIEW NETWORK TOPOLOGY' link. Below the title, there is a description: 'Below are the network settings for supporting namespaces on this Supervisor.' The 'Workload Network' section is expanded, showing the following settings:

Setting	Value	Action
vSphere Distributed Switch	dc-dvs	
Edge Cluster	edge-cluster-0	
DNS Server(s)	[Redacted]	EDIT
Services CIDR	[Redacted]	
Tier-0 Gateway	60970e9d-d22c-40a9-83c8-6e81efaf3eb0	
NAT Mode	Enabled	
Namespace Network	[Redacted]	EDIT
Namespace subnet prefix	/28	
Ingress	[Redacted]	EDIT
Egress	[Redacted]	EDIT

4 필요에 따라 네트워킹 설정을 변경합니다.

옵션	설명
DNS 서버	vSphere 관리 구성 요소의 도메인 이름을 확인할 수 있는 DNS 서버(예: vCenter Server)의 주소를 입력합니다. 예: 10.142.7.1 DNS 서버의 IP 주소를 입력하면 각 제어부 VM에 정적 경로가 추가됩니다. 이것은 DNS 서버에 대한 트래픽이 워크로드 네트워크를 통과한다는 것을 나타냅니다. 지정하는 DNS 서버가 관리 네트워크와 워크로드 네트워크 간에 공유되는 경우에는 제어부 VM의 DNS 조회가 초기 설정 후 워크로드 네트워크를 통해 라우팅됩니다.
네임스페이스 네트워크	감독자의 네임스페이스 세그먼트에 연결된 Kubernetes 워크로드의 IP 범위를 변경하려면 CIDR 주석을 입력합니다. NAT 모드가 구성되지 않은 경우 이 IP CIDR 범위는 라우팅 가능한 IP 주소여야 합니다.
수신	Kubernetes 서비스의 수신 IP 범위를 변경하려면 CIDR 주석을 입력합니다. 이 범위는 로드 밸런서 및 수신 유형의 서비스에 사용됩니다. Tanzu Kubernetes Grid 클러스터의 경우 ServiceType 로드 밸런서를 통해 서비스를 게시하면 이 IP CIDR 블록의 IP 주소도 가져옵니다. 참고 수신 및 워크로드 네트워크 필드에 CIDR을 추가할 수만 있고 기존 CIDR을 편집하거나 제거할 수는 없습니다.
송신	외부 서비스에 액세스하기 위해 감독자를 나가는 트래픽에 대해 SNAT(소스 네트워크 주소 변환)의 IP 주소를 할당하기 위한 CIDR 주석을 입력합니다. 감독자의 각 네임스페이스에는 송신 IP 주소가 하나만 할당됩니다. 송신 IP는 특정 네임스페이스의 vSphere 포드가 NSX 외부에서 통신하는 데 사용하는 IP 주소입니다.

vSphere IaaS control plane에서 HTTP 프록시 설정 구성

감독자 및 TKG 클러스터에 대한 HTTP 프록시 설정을 구성하는 방법과 Tanzu Mission Control에 감독자 및 TKG 클러스터를 등록할 때 프록시를 구성하는 워크플로가 무엇인지 알아봅니다.

vSphere Client, 클러스터 관리 API 또는 DCLI 명령을 통해 감독자에 대한 프록시를 구성할 수 있습니다. 컨테이너 트래픽을 처리하거나 감독자 외부 네트워크에서 끌어오는 이미지를 처리해야 하는 경우 프록시를 사용할 수 있습니다. Tanzu Mission Control에서 관리 클러스터로 등록하는 온-프레미스 감독자의 경우 이미지 끌어오기 및 컨테이너 트래픽에 HTTP 프록시를 사용합니다.

새로 생성된 vSphere 7.0 업데이트 3 이상 감독자에서 프록시 설정 구성

vSphere 7.0 업데이트 3 이상 환경에서 새로 생성된 감독자의 경우 HTTP 프록시 설정이 vCenter Server에서 상속됩니다. vCenter Server에서 HTTP 프록시 설정을 구성하기 전이나 구성한 후에 감독자를 생성하든 상관없이 설정은 클러스터에 상속됩니다.

vCenter Server에서 HTTP 프록시 설정을 구성하는 방법에 대한 자세한 내용은 [DNS, IP 주소 및 프록시 설정 구성](#)을 참조하십시오.

vSphere Client, 클러스터 관리 API 또는 DCLI를 통해 개별 감독자에서 상속된 HTTP 프록시 구성을 재정의할 수도 있습니다.

vCenter Server 프록시 설정을 상속하는 것이 새로 생성된 vSphere 7.0.3 감독자의 기본 구성이므로 감독자에 프록시가 필요하지 않지만 vCenter Server에는 계속 필요한 경우 클러스터 관리 API 또는 DCLI를 사용하여 HTTP 프록시 설정을 상속하지 않을 수도 있습니다.

vSphere 7.0 업데이트 3 이상으로 업그레이드된 감독자에서 프록시 설정 구성

감독자를 vSphere 7.0 업데이트 3 이상으로 업그레이드한 경우 vCenter Server의 HTTP 프록시 설정이 자동으로 상속되지 않습니다. 이 경우 vSphere Client, `vcenter/namespace-management/clusters` API 또는 DCLI 명령줄을 사용하여 감독자의 프록시 설정을 구성합니다.

vSphere IaaS control plane에서 TKG 클러스터에 대한 HTTP 프록시 구성

다음 방법 중 하나를 사용하여 vSphere IaaS control plane에서 Tanzu Kubernetes 클러스터에 대한 프록시를 구성합니다.

- 개별 TKG 클러스터에 대한 프록시 설정을 구성합니다. [Tanzu Kubernetes Grid Service v1alpha2 API](#)를 사용하여 Tanzu Kubernetes 클러스터를 프로비저닝하기 위한 구성 매개 변수를 참조하십시오. 구성 YAML의 예는 [Tanzu Kubernetes Grid Service v1alpha2 API](#)를 사용하여 사용자 지정 Tanzu Kubernetes 클러스터를 프로비저닝하기 위한 예제 YAML을 참조하십시오.
- 모든 TKG 클러스터에 적용될 글로벌 프록시 구성을 생성합니다. [Tanzu Kubernetes Grid Service v1alpha2 API](#)에 대한 구성 매개 변수를 참조하십시오.

참고 Tanzu Mission Control을 사용하여 TKG 클러스터를 관리하는 경우 vSphere IaaS control plane에서 클러스터 YAML 파일을 통해 프록시 설정을 구성할 필요가 없습니다. TKG 클러스터를 Tanzu Mission Control에 워크로드 클러스터로 추가할 때 프록시 설정을 구성할 수 있습니다.

vSphere Client를 사용하여 감독자에서 HTTP프록시 설정 구성

vSphere Client를 통해 감독자에 HTTP 프록시 설정을 구성하는 방법을 확인합니다. 개별 감독자의 vCenter Server에서 상속된 프록시 설정을 재정의하거나 프록시 설정을 전혀 사용하지 않도록 선택할 수 있습니다.

사전 요구 사항

- 클러스터에서 **클러스터 전체 구성 수정** 권한이 있는지 확인합니다.

절차

- 1 vSphere Client에서 **워크로드 관리**로 이동합니다.
- 2 **감독자**에서 감독자를 선택하고 **구성**을 선택합니다.
- 3 **네트워크**를 선택하고 **프록시 구성**을 확장한 후 **편집**을 클릭합니다.

4 감독자에서 프록시 설정 구성을 선택하고 프록시 설정을 입력합니다.

옵션	설명
TLS 인증서	프록시의 인증서를 확인하는 데 사용되는 프록시 TLS 루트 CA 번들입니다. 번들을 일반 텍스트로 입력합니다.
프록시에서 제외된 호스트 및 IP 주소	프록시 서버가 필요하지 않고 직접 액세스할 수 있는 IPv4 주소, FQDN 또는 도메인 이름이 심표로 구분된 목록입니다.
HTTPS 구성	URL, 포트, 사용자 이름 및 암호와 같은 HTTPS 설정입니다.
HTTP 구성	URL, 포트, 사용자 이름 및 암호와 같은 HTTP 설정입니다.

5 확인을 클릭합니다.

결과

이 감독자에서 구성한 프록시 설정은 vCenter Server에서 상속된 설정을 재정의합니다.

클러스터 관리 API 및 DCLI를 사용하여 감독자에 대한 HTTP 프록시 구성

vcenter/namespace-management/clusters API 또는 DCLI를 통해 감독자 프록시 설정을 구성할 수 있습니다.

API는 감독자의 프록시 구성을 위한 세 가지 옵션을 제공합니다.

API 설정	새로 생성된 vSphere 7.0.3 이상 감독자	vSphere 7.0.3 이상으로 업그레이드된 감독자
VC_INHERITED	이것은 새 감독자에 대한 기본 설정이며 API를 사용하여 감독자 프록시 설정을 구성할 필요가 없습니다. vCenter Server에서 관리 인터페이스를 통해 프록시 설정을 구성할 수 있습니다.	이 설정을 사용하여 HTTP 프록시 구성을 vSphere 7.0.3 이상으로 업그레이드된 감독자에 푸시합니다.
CLUSTER_CONFIGURED	다음 중 하나의 경우 이 설정을 사용하여 vCenter Server에서 상속된 HTTP 프록시 구성을 재정의합니다. <ul style="list-style-type: none"> ■ 감독자가 vCenter Server와 다른 서브넷에 있으며 다른 프록시 서버가 필요합니다. ■ 프록시 서버가 사용자 지정 CA 번들을 사용합니다. 	다음 중 하나의 경우 이 설정을 사용하여 vSphere 7.0.3 이상으로 업그레이드된 개별 감독자에 대한 HTTP 프록시를 구성합니다. <ul style="list-style-type: none"> ■ 감독자가 vCenter Server와 다른 서브넷에 있고 다른 프록시 서버가 필요하므로 vCenter Server 프록시를 사용할 수 없습니다. ■ 프록시 서버가 사용자 지정 CA 번들을 사용합니다.
NONE	감독자가 인터넷에 직접 연결되어 있고 vCenter Server에 프록시가 필요한 경우 이 설정을 사용합니다. NONE 설정은 vCenter Server의 프록시 설정이 감독자에서 상속되는 것을 방지합니다.	

HTTP 프록시를 감독자로 설정하거나 기존 설정을 수정하려면 vCenter Server와의 SSH 세션에서 다음 명령을 사용합니다.

```
vc_address=<IP address>
cluster_id=domain-c<number>
session_id=$(curl -ksX POST --user '<SSO user name>:<password>' https://$vc_address/api/
session | xargs -t)
curl -k -X PATCH -H "vmware-api-session-id: $session_id" -H "Content-Type: application/json"
-d '{ "cluster_proxy_config": { "proxy_settings_source": "CLUSTER_CONFIGURED",
"http_proxy_config": "<proxy_url>" } }' https://$vc_address/api/vcenter/namespace-management/
clusters/$cluster_id
```

전체 클러스터 ID에서 domain_c<number>만 전달하면 됩니다. 예를 들어 클러스터 ID

ClusterComputeResource:domain-c50:5bbb510f-759f-4e43-96bd-97fd703b4edb에서 domain-c50을 가져옵니다.

VC_INHERITED 또는 NONE 설정을 사용하는 경우 명령에서 "http_proxy_config:<proxy_url>"을 생략합니다.

사용자 지정 CA 번들을 사용하려면 TLS CA 인증서를 일반 텍스트로 제공하여 명령에 "tlsRootCaBundle": "<TLS_certificate>"를 추가합니다.

HTTPS 프록시 설정의 경우 다음 명령을 사용합니다.

```
curl -k -X PATCH -H "vmware-api-session-id: $session_id"
-H "Content-Type: application/json" -d '{ "cluster_proxy_config":
{ "proxy_settings_source": "CLUSTER_CONFIGURED", "https_proxy_config": "<proxy_url>" } }'
https://$vc_address/api/vcenter/namespace-management/clusters/$cluster_id
```

DCLI를 사용하여 감독자에서 HTTP 프록시 설정 구성

다음 DCLI 명령을 사용하면 CLUSTER_CONFIGURED 설정을 사용하여 감독자에 대한 HTTP 프록시 설정을 구성할 수 있습니다.

```
<dcli> namespacemanagement clusters update --cluster domain-c57 --cluster-proxy-config-http-
proxy-config <proxy URL> --cluster-proxy-config-https-proxy-config <proxy URL> --cluster-
proxy-config-proxy-settings-source CLUSTER_CONFIGURED
```

Tanzu Mission Control을 위해 감독자 및 TKG 클러스터에서 HTTP 프록시 설정 구성

Tanzu Mission Control에서 관리 클러스터로 등록하려는 감독자에서 HTTP 프록시를 구성하려면 다음 단계를 수행합니다.

- 1 vSphere에서 vCenter Server의 HTTP 프록시 설정을 상속하거나 vSphere Client, [네임스페이스 관리 클러스터 API](#) 또는 DCLI 명령줄을 통해 개별 감독자에서 프록시 설정을 구성하여 감독자에서 HTTP 프록시를 구성합니다.

- 2 Tanzu Mission Control에서 vSphere IaaS control plane의 감독자에 구성된 프록시 설정을 사용하여 프록시 구성 개체를 생성합니다. [Tanzu Kubernetes Grid Service 클러스터에 대한 프록시 구성 개체 생성](#)을 참조하십시오.
- 3 Tanzu Mission Control에서 감독자를 관리 클러스터로 등록할 때 이 프록시 구성 개체를 사용합니다. [Tanzu Mission Control에 관리 클러스터 등록 및 감독자 클러스터 등록 완료](#)를 참조하십시오.

Tanzu Mission Control에서 워크로드 클러스터로 추가하거나 프로비저닝하는 TKG 클러스터에 HTTP 프록시를 구성하려면 다음을 수행합니다.

- 1 Tanzu Kubernetes 클러스터에 사용할 프록시 설정으로 프록시 구성 개체를 생성합니다. [Tanzu Kubernetes Grid Service 클러스터에 대한 프록시 구성 개체 생성](#)을 참조하십시오.
- 2 Tanzu Kubernetes 클러스터를 워크로드 클러스터로 추가하거나 프로비저닝할 때 해당 프록시 구성 개체를 사용합니다. [클러스터 프로비저닝 및 Tanzu Mission Control 관리에 워크로드 클러스터 추가](#)를 참조하십시오.

TKG 서비스 클러스터와 함께 사용할 외부 IDP 구성

Okta와 같은 OIDC 준수 IDP(ID 제공자)를 사용하여 감독자를 구성할 수 있습니다. 통합을 완료하려면 감독자에 대한 콜백 URL을 사용하여 IDP를 구성합니다.

지원되는 외부 OIDC 제공자

OIDC 준수 ID 제공자를 사용하여 감독자를 구성할 수 있습니다. 이 표에는 일반 항목이 나열되어 있으며 구성 지침에 대한 링크가 포함되어 있습니다.

외부 IDP	구성
Okta	Okta를 사용한 OIDC 구성 예시 Okta를 Pinniped용 OIDC 제공자로 구성 도 참조하십시오.
Workspace ONE	Workspace ONE Access를 Pinniped용 OIDC 제공자로 구성
Dex	Dex를 Pinniped용 OIDC 제공자로 구성
GitLab	GitLab을 Pinniped용 OIDC 제공자로 구성
Google OAuth	Google OAuth 2 사용

감독자의 콜백 URL을 사용하여 IDP 구성

감독자는 외부 ID 제공자에 대한 OAuth 2.0 클라이언트 역할을 합니다. 감독자 콜백 URL은 외부 IDP를 구성하는 데 사용되는 리디렉션 URL입니다. 콜백 URL은 "https://SUPERVISOR-VIP/wcp/pinniped/callback" 형식입니다.

참고 IDP 등록을 수행할 때 구성 중인 OIDC 제공자에서 콜백 URL을 "리디렉션 URL"이라고 지칭할 수 있습니다.

감독자의 TKG에서 사용할 외부 ID 제공자를 구성하는 경우 외부 ID 제공자에게 **워크로드 관리 > 감독자 > 구성 > ID 제공자** 화면의 vCenter Server에서 사용할 수 있는 **콜백 URL**을 제공합니다.

Okta를 사용한 OIDC 구성 예시

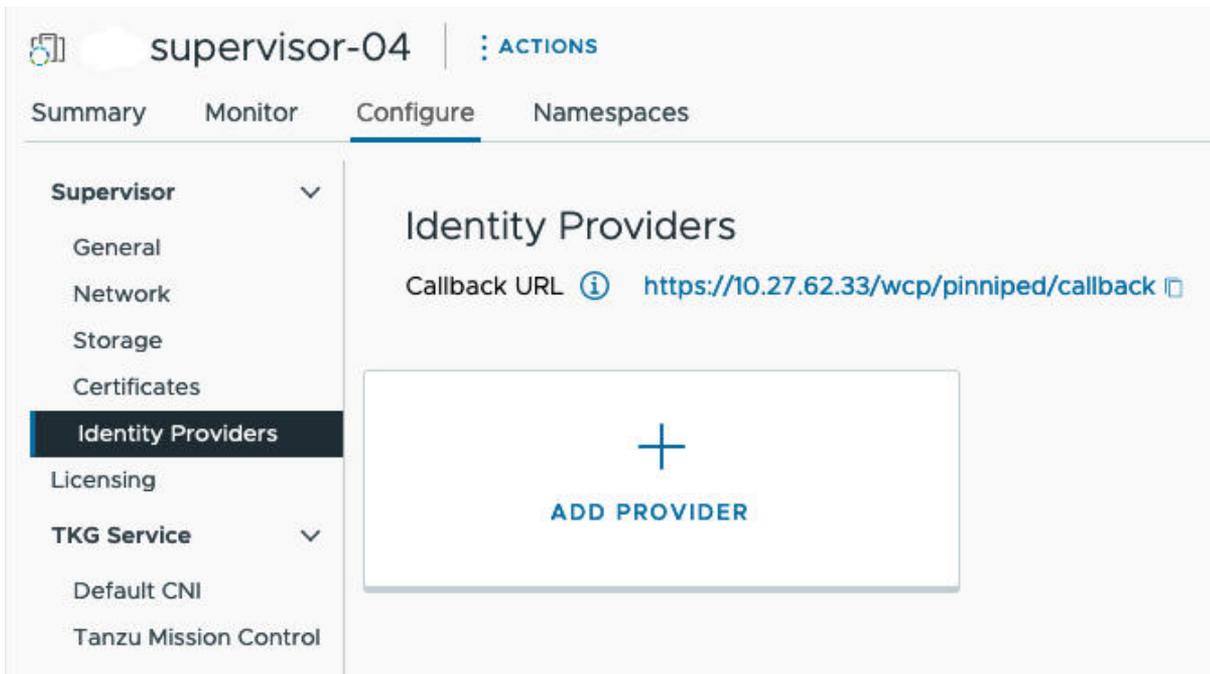
Okta를 사용하면 사용자가 **OpenID Connect** 프로토콜을 사용하여 애플리케이션에 로그인할 수 있습니다.

Okta를 감독자의 Tanzu Kubernetes Grid에 대한 외부 ID 제공자로 구성하면 감독자 및 Tanzu Kubernetes Grid 클러스터의 Pinniped 포드가 vSphere 네임스페이스 및 워크로드 클러스터 둘 다에 대한 사용자 액세스를 제어합니다.

- 1 Okta와 vCenter Server 간에 OIDC 연결을 생성하는 데 필요한 ID 제공자 콜백 URL을 복사합니다.

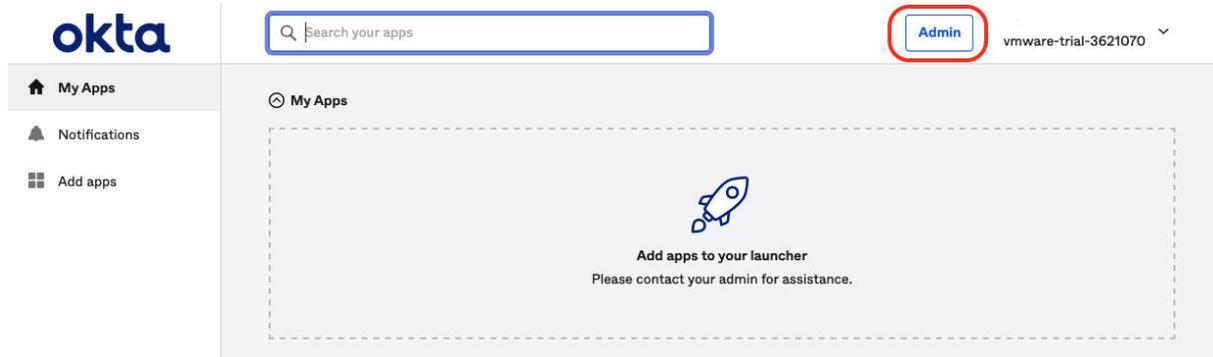
vSphere Client를 사용하여 **워크로드 관리 > 감독자 > 구성 > ID 제공자**에서 ID 제공자 콜백 URL을 가져옵니다. 이 URL을 임시 위치에 복사합니다.

그림 12-6. IDP 콜백 URL



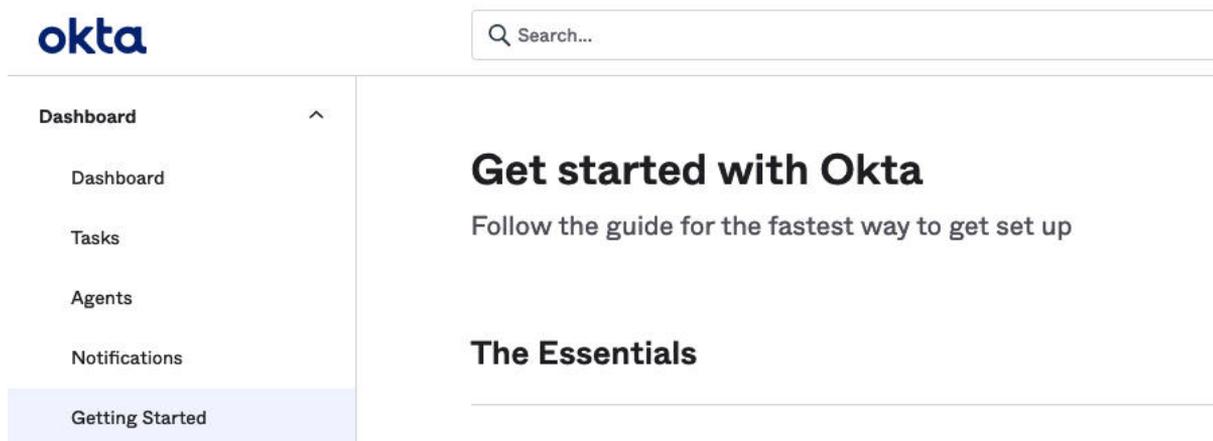
- 2 조직의 Okta 계정에 로그인하거나 <https://www.okta.com/>에서 평가판 계정을 생성합니다. **관리자** 버튼을 클릭하여 Okta 관리 콘솔을 엽니다.

그림 12-7. Okta 관리 콘솔



- 3 관리 콘솔의 Getting Started(시작) 페이지에서 **Applications(애플리케이션) > Applications(애플리케이션)**로 이동합니다.

그림 12-8. Okta Getting Started(시작)



- 4 **Create App Integration(애플리케이션 통합 생성)** 옵션을 선택합니다.

그림 12-9. Okta 애플리케이션 통합 생성

Applications



- 5 새 애플리케이션 통합을 생성합니다.
 - Sign-in method(로그인 방법)를 **OIDC - OpenID Connect**로 설정합니다.
 - Application type(애플리케이션 유형)을 **Web Application(웹 애플리케이션)**으로 설정합니다.

그림 12-10. Okta Sign-On 방법 및 애플리케이션 유형

X

Create a new app integration

Sign-in method

[Learn More](#)

- OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

- Web Application**
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)
- Single-Page Application**
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)
- Native Application**
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

[Cancel](#)
[Next](#)

6 Okta 웹 애플리케이션 통합 세부 정보를 구성합니다.

- 사용자 정의 문자열인 **App integration name**(애플리케이션 통합 이름)을 제공합니다.
- **Grant type**(권한 부여 유형) 지정: **Authorization Code**(인증 코드)를 선택하고 **Refresh Token**(새로 고침 토큰)도 선택합니다.
- Sign-in redirect URIs(로그인 리디렉션 URI): 감독자에서 복사한 ID 제공자 콜백 URL(1단계 참조)(예: <https://10.27.62.33/wcp/pinnipend/callback>)을 입력합니다.
- Sign-out redirect URIs(로그아웃 리디렉션 URI): 감독자에서 복사한 ID 제공자 콜백 URL(1단계 참조)(예: <https://10.27.62.33/wcp/pinnipend/callback>)을 입력합니다.

그림 12-11. Okta 웹 애플리케이션 통합 세부 정보

☰+ New Web App Integration

General Settings

App integration name

Logo (Optional)

Grant type [Learn More](#)

Client acting on behalf of itself

Client Credentials

Client acting on behalf of a user

Authorization Code

Interaction Code

Refresh Token

Implicit (hybrid)

Sign-in redirect URIs Allow wildcard * in sign-in URI redirect.

Okta sends the authentication response and ID token for the user's sign-in request to these URIs

Sign-out redirect URIs (Optional)

After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.

7 사용자 액세스 제어를 구성합니다.

Assignments(할당) > Controlled access(제어된 액세스) 섹션에서 조직에 존재하는 Okta 사용자 중 Tanzu Kubernetes Grid 클러스터에 액세스할 수 있는 사용자를 선택적으로 제어할 수 있습니다. 이 예시에서 조직에 정의된 모든 사람이 액세스할 수 있도록 허용합니다.

그림 12-12. Okta 액세스 제어

Trusted Origins

Base URIs (Optional)

Required if you plan to self-host the Okta Sign-In Widget. With a Trusted Origin set, the Sign-In Widget can make calls to the authentication API from this domain.

[Learn More](#) 

X

+ Add URI

Assignments

Controlled access

Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.

- Allow everyone in your organization to access
- Limit access to selected groups
- Skip group assignment for now

Enable immediate access (Recommended)

Recommended if you want to grant access to everyone without pre-assigning your app to users and use Okta only for authentication.

- Enable immediate access with **Federation Broker Mode**

i

To ensure optimal app performance at scale, Okta End User Dashboard and provisioning features are disabled. [Learn more about Federation Broker Mode.](#)

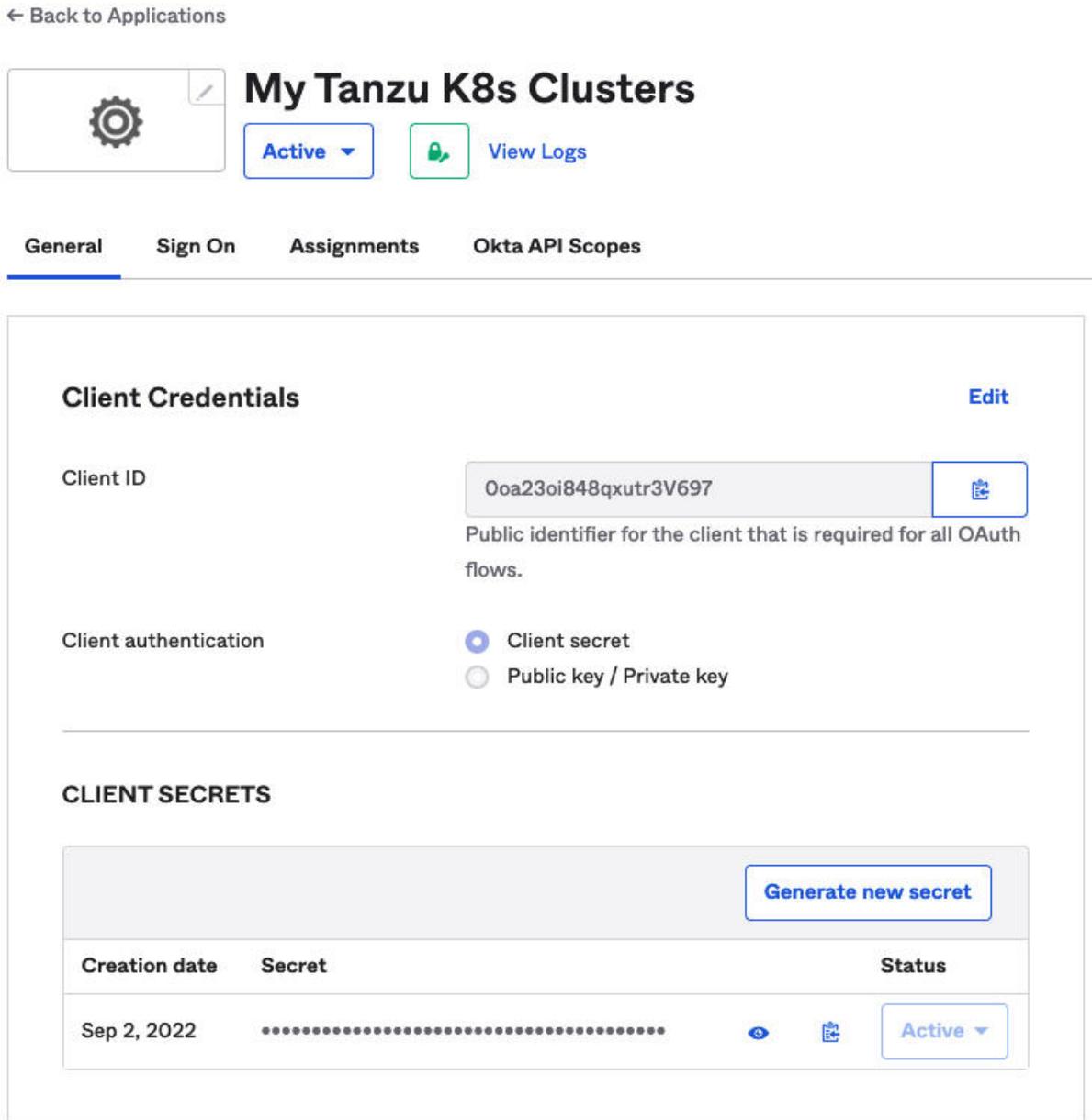
Save

Cancel

- 8 **Save(저장)**를 클릭하고 반환되는 **Client ID**(클라이언트 ID) 및 **Client Secret**(클라이언트 암호)을 복사합니다.

OKTA 구성을 저장하면 관리 콘솔에 **클라이언트 ID** 및 **클라이언트 암호**가 제공됩니다. 외부 ID 제공자를 사용하여 감독자를 구성하는 데 필요하므로 두 데이터를 모두 복사합니다.

그림 12-13. OIDC 클라이언트 ID 및 암호



9 OpenID Connect ID 토큰을 구성합니다.

Sign On(로그온) 탭을 클릭합니다. **OpenID Connect ID Token**(OpenID Connect ID 토큰) 섹션에서 **Edit**(편집) 링크를 클릭하고 **Groups claim type**(그룹 할당 유형) 필터를 입력한 후 **Save**(저장)를 클릭하여 설정을 저장합니다.

예를 들어 클레임 이름 "groups"가 모든 그룹과 일치하도록 하려면 **groups > Matches regex(정규식과 일치) > ***를 선택합니다.

그림 12-14. OpenID Connect ID 토큰

OpenID Connect ID Token Cancel

Issuer

Audience

Claims Claims for this token include all user attributes on the app profile.

Groups claim type

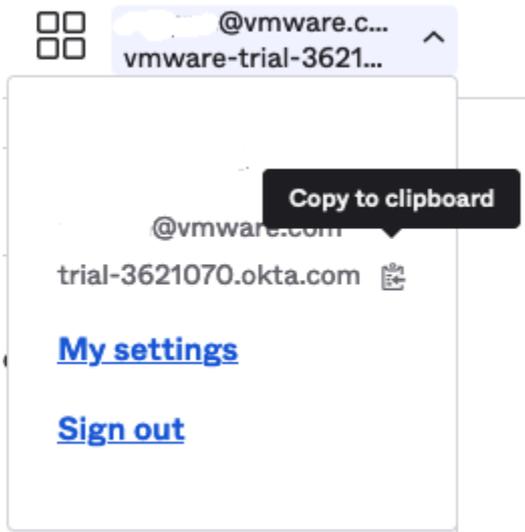
Groups claim filter
[Using Groups Claim](#)

10 Issuer URL(발급자 URL)을 복사합니다.

감독자를 구성하려면 **Client ID**(클라이언트 ID) 및 **Client Secret**(클라이언트 암호) 외에 **Issuer URL**(발급자 URL)이 필요합니다.

Okta 관리 콘솔에서 **Issuer URL**(발급자 URL)을 복사합니다.

그림 12-15. Okta 발급자 URL



외부 IDP를 감독자에 등록

Tanzu CLI를 사용하여 감독자의 Tanzu Kubernetes Grid 2.0 클러스터에 연결하려면 OIDC 제공자를 감독자에 등록합니다.

사전 요구 사항

외부 OIDC 제공자를 감독자에 등록하기 전에 다음 사전 요구 사항을 완료하십시오.

- 워크로드 관리를 사용하도록 설정하고 감독자 인스턴스를 배포합니다. [감독자에서 TKG 2.0 클러스터 실행을 참조하십시오.](#)
- 감독자 콜백 URL을 사용하여 외부 [OpenID Connect ID](#) 제공자를 구성합니다. [TKG 서비스 클러스터와 함께 사용할 외부 IDP 구성](#)의 내용을 참조하십시오.
- 외부 IDP에서 클라이언트 ID, 클라이언트 암호 및 발급자 URL을 가져옵니다. [TKG 서비스 클러스터와 함께 사용할 외부 IDP 구성](#)의 내용을 참조하십시오.

외부 IDP를 감독자에 등록

감독자는 Pinniped 감독자 및 Pinniped Concierge 구성 요소를 포드로 실행합니다. Tanzu Kubernetes Grid 클러스터는 Pinniped Concierge 구성 요소만 포드로 실행합니다. 이러한 구성 요소와 구성 요소가 상호 작용하는 방식에 대한 자세한 내용은 [Pinniped 인증 서비스 설명서](#)를 참조하십시오.

외부 ID 제공자를 감독자에 등록하면 감독자의 Pinniped 감독자 및 Pinniped Concierge 포드와 Tanzu Kubernetes Grid 클러스터의 Pinniped Concierge 포드가 시스템에서 업데이트됩니다. 해당 감독자 인스턴스에서 실행되는 모든 Tanzu Kubernetes Grid 클러스터는 동일한 외부 ID 제공자를 사용하여 자동으로 구성됩니다.

외부 OIDC 제공자를 감독자에 등록하려면 다음 절차를 완료하십시오.

- 1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.
- 2 [워크로드 관리 > 감독자 > 구성 > ID 제공자](#)를 선택합니다.
- 3 더하기 기호를 클릭하여 등록 프로세스를 시작합니다.
- 4 제공자를 구성합니다. [OIDC 제공자 구성](#)의 내용을 참조하십시오.

그림 12-16. OIDC 제공자 구성

Add Provider

- 1 Provider Configuration**
- 2 OAuth 2.0 Client Details
- 3 Additional Settings
- 4 Review and Confirm

Provider Configuration

Provider Name ⓘ

Issuer URL ⓘ

Username Claim (optional) ⓘ

Groups Claim (optional) ⓘ

- 5 OAuth 2.0 클라이언트 세부 정보를 구성합니다. [OAuth 2.0 클라이언트 세부 정보](#)의 내용을 참조하십시오.

그림 12-17. OAuth 2.0 클라이언트 세부 정보

Add Provider

- 1 Provider Configuration
- 2 OAuth 2.0 Client Details**
- 3 Additional Settings
- 4 Review and Confirm

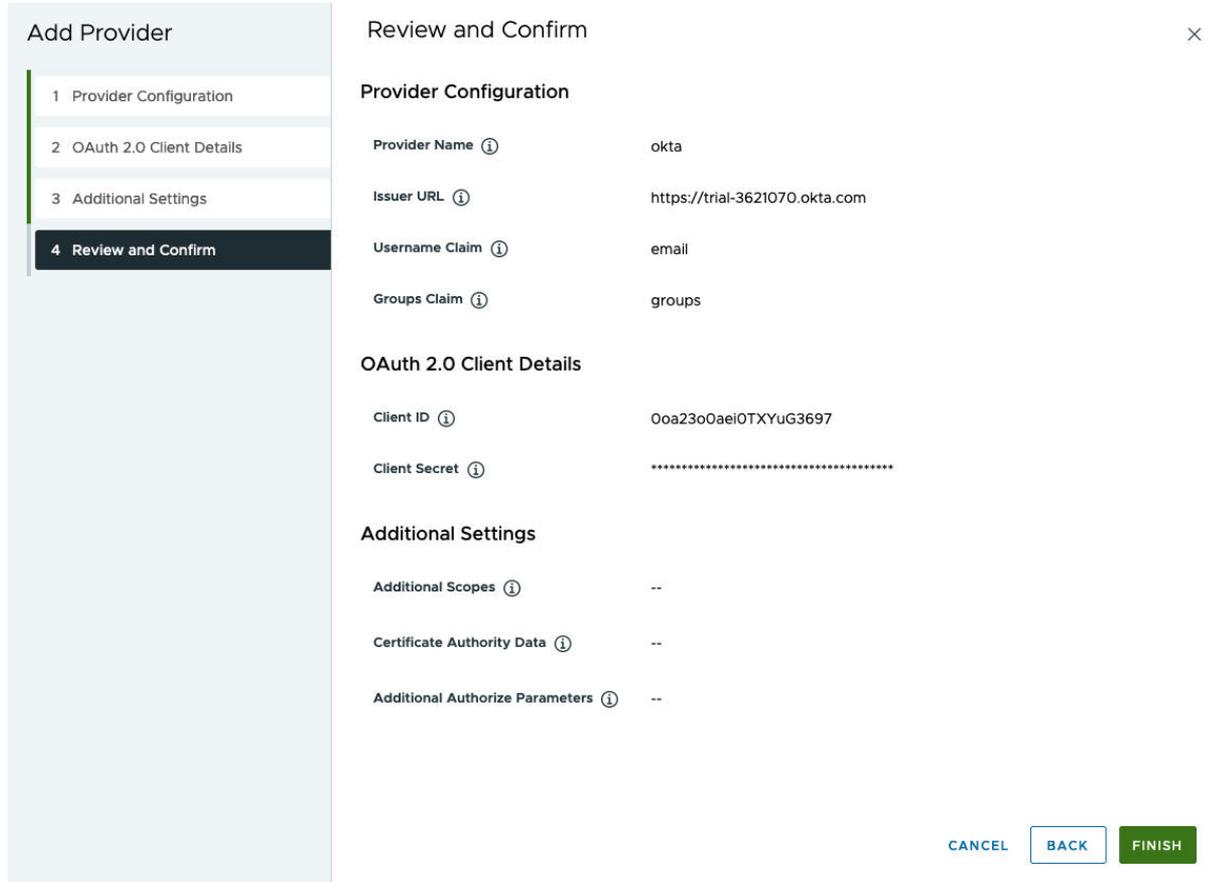
OAuth 2.0 Client Details

Client ID ⓘ

Client Secret ⓘ ⓘ

- 6 추가 설정을 구성합니다. [추가 설정](#)의 내용을 참조하십시오.
- 7 제공자 설정을 확인합니다.

그림 12-18. 제공자 설정 확인



8 **마침**을 클릭하여 OIDC 제공자 등록을 완료합니다.

OIDC 제공자 구성

외부 OIDC 제공자를 감독자에 등록할 때 다음 제공자 구성 세부 정보를 참조하십시오.

표 12-1. OIDC 제공자 구성

필드	중요도	설명
제공자 이름	필수	외부 ID 제공자에 대한 사용자 정의 이름입니다.
발급자 URL	필수	토큰을 발급하는 ID 제공자의 URL입니다. OIDC 검색 URL은 발급자 URL에서 파생됩니다. 예를 들어 Okta 발급자 URL은 다음과 같은 모양이며 관리 콘솔에서 구할 수 있습니다. "https://trial-4359939-admin.okta.com" .

표 12-1. OIDC 제공자 구성 (계속)

필드	중요도	설명
사용자 이름 할당	선택 사항	지정된 사용자의 사용자 이름을 가져오기 위해 검사할 업스트림 ID 제공자 ID 토큰 또는 사용자 정보 끝점의 할당입니다. 이 필드를 비워두면 업스트림 발급자 URL이 "sub" 할당과 연결되어 Kubernetes에서 사용할 사용자 이름이 생성됩니다. 이 필드는 Pinniped가 인증을 결정하기 위해 업스트림 ID 토큰에서 확인해야 하는 사항을 지정합니다. 제공하지 않으면 사용자 ID는 "https://IDP-ISSUER?sub=UUID" 형식으로 지정됩니다.
그룹 할당	선택 사항	지정된 사용자의 그룹을 가져오기 위해 검사할 업스트림 ID 제공자 ID 토큰 또는 사용자 정보 끝점의 할당입니다. 이 필드를 비워두면 업스트림 ID 제공자의 그룹이 사용되지 않습니다. 그룹 클레임 필드는 Pinniped가 사용자 ID를 인증하기 위해 업스트림 ID 토큰에서 확인해야 하는 사항을 지정합니다.

OAuth 2.0 클라이언트 세부 정보

외부 OIDC 제공자를 감독자에 등록할 때 다음 제공자 OAuth 2.0 클라이언트 세부 정보를 참조하십시오.

표 12-2. OAuth 2.0 클라이언트 세부 정보

OAuth 2.0 클라이언트 세부 정보	중요도	설명
클라이언트 ID	필수	외부 IDP의 클라이언트 ID
클라이언트 암호	필수	외부 IDP의 클라이언트 암호

추가 설정

외부 OIDC 제공자를 감독자에 등록할 때 다음 추가 설정을 참조하십시오.

표 12-3. 추가 설정

설정	중요도	설명
추가 범위	선택 사항	토큰에서 요청할 추가 범위
CA(인증 기관) 데이터	선택 사항	보안 외부 IDP 연결을 위한 TLS CA(인증 기관) 데이터
추가 인증 매개 변수	선택 사항	OAuth2 인증 요청 중 추가 매개 변수

감독자의 스토리지 설정 변경

감독자에 할당된 스토리지 정책은 제어부 VM, vSphere 포드 사용 후 삭제 디스크, 컨테이너 이미지 캐시와 같은 개체가 vSphere 스토리지 환경의 데이터스토어 내에 배치되는 방식을 관리합니다. vSphere 관리자는 일반적으로 감독자를 사용하도록 설정할 때 스토리지 정책을 구성합니다. 초기 감독자 구성 후 스토리지 정책 할당을 변경해야 하는 경우 이 작업을 수행합니다. 이 작업을 사용하여 TKG 클러스터의 ReadWriteMany 영구 볼륨에 대한 파일 볼륨 지원을 활성화하거나 비활성화할 수도 있습니다.

일반적으로, 스토리지 설정에 대한 변경 내용은 감독자의 새 개체에만 적용됩니다. 이 절차를 사용하여 TKG 클러스터에서 파일 볼륨 지원을 활성화하는 경우 기존 클러스터에 대해 이 작업을 수행할 수 있습니다.

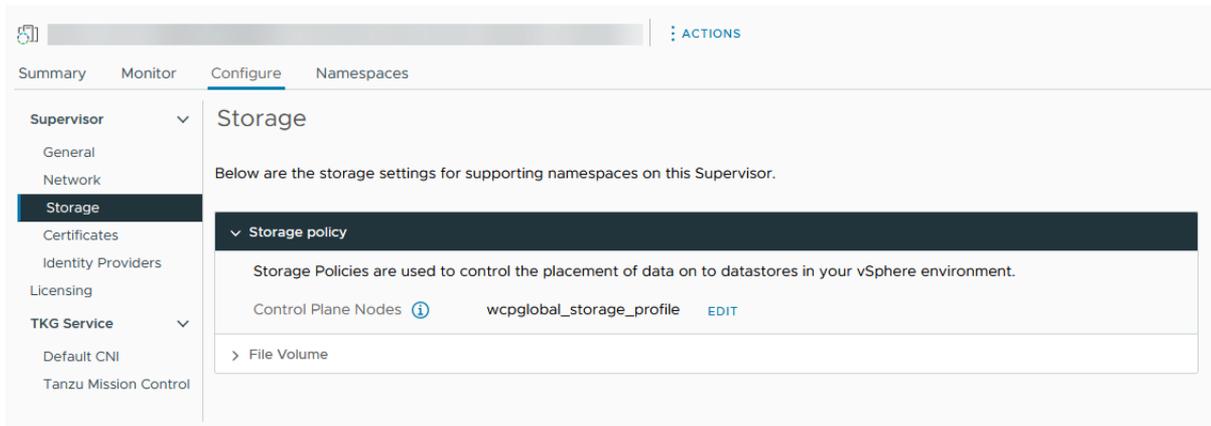
사전 요구 사항

ReadWriteMany 모드에서 영구 볼륨에 대한 TKG 클러스터의 파일 볼륨 지원을 활성화하려는 경우, "vSphere IaaS 제어부 서비스 및 워크로드" 설명서의 [vSphere IaaS control plane에서 ReadWriteMany 영구 볼륨 생성](#)에서 사전 요구 사항을 따르십시오.

절차

- 1 vSphere Client에서 **워크로드 관리**로 이동합니다.
- 2 **감독자** 탭을 클릭하고 목록에서 편집할 감독자를 선택합니다.
- 3 **구성** 탭을 클릭하고 **스토리지**를 클릭합니다.

그림 12-19. 감독자 스토리지 설정 업데이트



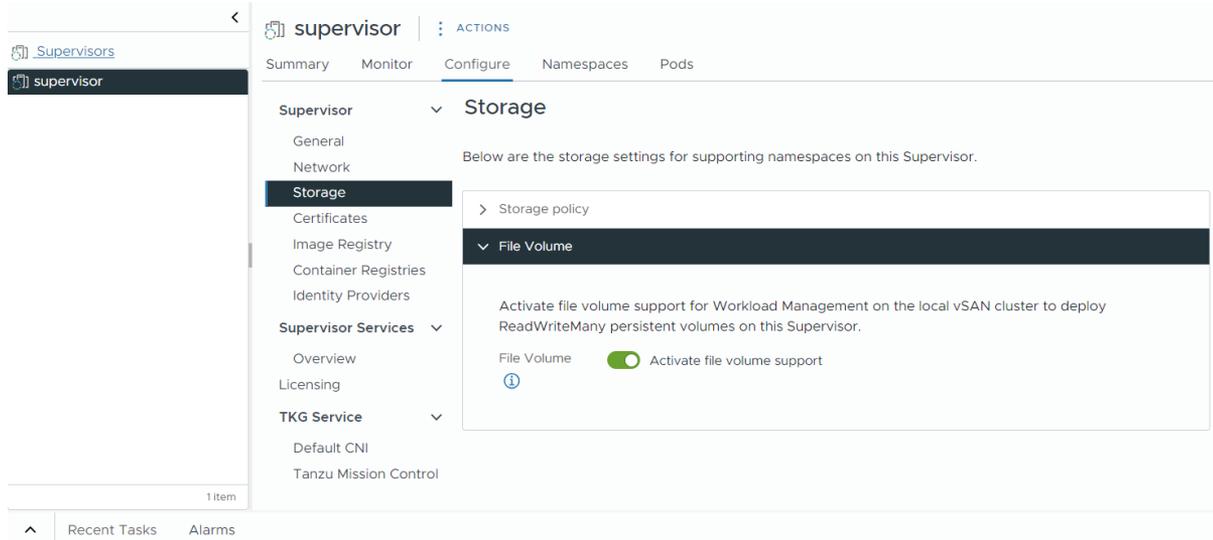
- 4 제어부 VM에 대한 스토리지 정책 할당을 변경합니다.

환경에서 vSphere 포드를 지원하는 경우 사용 후 삭제 가상 디스크 및 컨테이너 이미지 캐시에 대한 스토리지 정책을 변경할 수도 있습니다.

옵션	설명
제어부 노드	제어부 VM 배치에 대한 스토리지 정책을 선택합니다.
포드 사용 후 삭제 디스크	vSphere 포드 배치에 대한 스토리지 정책을 선택합니다.
컨테이너 이미지 캐시	컨테이너 이미지의 캐시 배치에 대한 스토리지 정책을 선택합니다.

5 파일 볼륨 지원을 사용하도록 설정하여 ReadWriteMany 영구 볼륨을 배포합니다.

이 옵션은 환경이 vSAN 파일 서비스로 구성된 경우에만 사용할 수 있습니다. [vSAN 파일 서비스 사용](#)을 참조하십시오.



사용자 지정 관찰 가능성 플랫폼으로 감독자 메트릭 스트리밍

Telegraf에서 수집한 감독자 메트릭을 사용자 지정 관찰 가능성 플랫폼으로 스트리밍하는 방법을 알아봅니다.

Telegraf는 감독자에서 기본적으로 사용하도록 설정되며 Kubernetes API 서버, VM 서비스, Tanzu Kubernetes Grid 등과 같은 감독자 구성 요소에서 Prometheus 형식의 메트릭을 수집합니다. vSphere 관리자는 수집된 감독자 메트릭을 보고 분석하도록 VMware Aria Operations for Applications, Grafana 등과 같은 관찰 가능성 플랫폼을 구성할 수 있습니다.

Telegraf는 다양한 시스템, 데이터베이스 및 IoT에서 메트릭을 수집하고 전송하기 위한 서버 기반 에이전트입니다. 각 감독자 구성 요소는 Telegraf가 연결되는 끝점을 노출합니다. 그런 다음 Telegraf는 수집된 메트릭을 원하는 관찰 가능성 플랫폼으로 전송합니다. Telegraf가 지원하는 출력 플러그인을 감독자 메트릭을 집계하고 분석하기 위한 관찰 가능성 플랫폼으로 구성할 수 있습니다. 지원되는 출력 플러그인은 [Telegraf 설명서](#)를 참조하십시오.

다음 구성 요소는 Telegraf가 연결하고 메트릭을 수집하는 끝점을 노출합니다. Kubernetes API 서버, etcd, kubelet, Kubernetes 컨트롤러 관리자, Kubernetes 스케줄러, Tanzu Kubernetes Grid, VM 서비스, VM 이미지 서비스, NCP(NSX Container Plug-in), CSI(Container Storage Interface), 인증서 관리자, NSX 및 CPU, 메모리, 스토리지와 같은 다양한 호스트 메트릭.

Telegraf 포드 및 구성 보기

Telegraf는 감독자의 `vmware-system-monitoring` 시스템 네임스페이스에서 실행됩니다. Telegraf 포드 및 ConfigMaps를 보려면:

- 1 vCenter Single Sign-On 관리자 계정으로 감독자 제어부에 로그인합니다.

```
kubectl vsphere login --server <control plane IP> --vsphere-username
administrator@vsphere.local
```

- 2 다음 명령을 사용하여 Telegraf 포드를 봅니다.

```
kubectl -n vmware-system-monitoring get pods
```

결과 포드는 다음과 같습니다.

```
telegraf-csqs1
telegraf-dkwtk
telegraf-l4nxx
```

- 3 다음 명령을 사용하여 Telegraf ConfigMaps를 봅니다.

```
kubectl -n vmware-system-monitoring get cm
```

결과 ConfigMaps는 다음과 같습니다.

```
default-telegraf-config
kube-rbac-proxy-config
kube-root-ca.crt
telegraf-config
```

`default-telegraf-config` ConfigMap은 기본 Telegraf 구성을 보유하며 읽기 전용입니다. 파일이 손상되었거나 기본값으로 복원하려는 경우 플래그 옵션으로 사용하여 `telegraf-config`의 구성을 복원할 수 있습니다. 편집할 수 있는 유일한 ConfigMap은 `telegraf-config`이며, Telegraf 에이전트에 메트릭을 전송하는 구성 요소와 플랫폼에 대해 정의합니다.

- 4 `telegraf-config` ConfigMap을 봅니다.

```
kubectl -n vmware-system-monitoring get cm telegraf-config -o yaml
```

`telegraf-config` ConfigMap의 `inputs` 섹션은 Telegraf가 메트릭은 물론 메트릭 유형을 수집하는 감독자 구성 요소의 모든 끝점을 정의합니다. 예를 들어 다음 입력은 Kubernetes API 서버를 끝점으로 정의합니다.

```
[[inputs.prometheus]]
  # APIServer
  ## An array of urls to scrape metrics from.
  alias = "kube_apiserver_metrics"
  urls = ["https://127.0.0.1:6443/metrics"]
  bearer_token = "/run/secrets/kubernetes.io/serviceaccount/token"
  # Dropping metrics as a part of short term solution to vStats integration 1MB metrics
  payload limit
```

```
# Dropped Metrics:
# apiserver_request_duration_seconds
namepass = ["apiserver_request_total", "apiserver_current_inflight_requests",
"apiserver_current_inqueue_requests", "etcd_object_counts",
"apiserver_admission_webhook_admission_duration_seconds", "etcd_request_duration_seconds"]
# "apiserver_request_duration_seconds" has _massive_cardinality, temporarily turned
off. If histogram, maybe filter the highest ones?
# Similarly, maybe filters to _only_ allow error code related metrics through?
## Optional TLS Config
tls_ca = "/run/secrets/kubernetes.io/serviceaccount/ca.crt"
```

alias 속성은 메트릭이 수집되는 구성 요소를 나타냅니다. namepass 속성은 Telegraf 에이전트에서 각각 노출되고 수집되는 구성 요소 메트릭을 지정합니다.

telegraf-config ConfigMap에는 이미 광범위한 메트릭이 포함되어 있지만 그래도 추가 메트릭을 정의할 수 있습니다. [Kubernetes 시스템 구성 요소에 대한 메트릭](#) 및 [Kubernetes 메트릭 참조](#)를 참조하십시오.

Telegraf에 대한 관찰 가능성 플랫폼 구성

telegraf-config의 outputs 섹션에서는 Telegraf가 수집한 메트릭을 스트리밍하는 위치를 구성합니다.

outputs.file, outputs.wavefront, outputs.prometheus_client 및 outputs-https와 같은 몇 가지 옵션이 있습니다. outputs-https 섹션에서는 감독자 메트릭의 집계 및 모니터링에 사용할 관찰 가능성 플랫폼을 구성할 수 있습니다. 둘 이상의 플랫폼에 메트릭을 보내도록 Telegraf를 구성할 수 있습니다. telegraf-config ConfigMap을 편집하고 감독자 메트릭을 보기 위한 관찰 가능성 플랫폼을 구성하려면 다음 단계를 수행합니다.

- 1 vCenter Single Sign-On 관리자 계정으로 감독자 제어부에 로그인합니다.

```
kubectl vsphere login --server <control plane IP> --vsphere-username
administrator@vsphere.local
```

- 2 telegraf-config ConfigMap을 로컬 kubectl 폴더에 저장합니다.

```
kubectl get cm telegraf-config -n vmware-system-monitoring -o
jsonpath="{.data['telegraf\.conf']}">telegraf.conf
```

이전 버전의 파일로 복원할 경우를 대비하여 변경하기 전에 telegraf-config ConfigMap을 버전 제어 시스템에 저장해야 합니다. 기본 구성으로 복원하려는 경우 default-telegraf-config ConfigMap의 값을 사용할 수 있습니다.

- 3 VIM과 같은 텍스트 편집기를 사용하여 선택한 관찰 가능성 플랫폼의 연결 설정으로 outputs.http 섹션을 추가합니다.

```
vim telegraf.config
```

다음 섹션의 주석 처리를 직접 제거하고 그에 따라 값을 편집하거나 필요에 따라 새 `outputs.http` 섹션을 추가할 수 있습니다.

```
#[[outputs.http]]
# alias = "prometheus_http_output"
# url = "<PROMETHEUS_ENDPOINT>"
# insecure_skip_verify = <PROMETHEUS_SKIP_INSECURE_VERIFY>
# data_format = "prometheusremotewrite"
# username = "<PROMETHEUS_USERNAME>"
# password = "<PROMETHEUS_PASSWORD>"
# <DEFAULT_HEADERS>
```

예를 들어 Grafana에 대한 `outputs.http` 구성은 다음과 같습니다.

```
[[outputs.http]]
url = "http://<grafana-host>:<grafana-metrics-port>/<prom-metrics-push-path>"
data_format = "influx"
[outputs.http.headers]
Authorization = "Bearer <grafana-bearer-token>"
```

Telegraf에서 대시보드를 구성하고 메트릭을 사용하는 방법에 대한 자세한 내용은 [Telegraf에서 Grafana로 메트릭 스트리밍](#)을 참조하십시오.

그리고 다음은 VMware Aria Operations for Applications (이전 Wavefront)의 예입니다.

```
[[outputs.wavefront]]
url = "http://<wavefront-proxy-host>:<wavefront-proxy-port>"
```

메트릭을 Aria Operations for Applications에 수집할 때 권장되는 방법은 프록시를 사용하는 것입니다. 자세한 내용은 [Wavefront 프록시](#)을 참조하십시오.

4 감독자의 기존 `telegraf-config` 파일을 로컬 폴더에서 편집한 파일로 교체합니다.

```
kubectl create cm --from-file telegraf.conf -n vmware-system-monitoring telegraf-config --dry-run=client -o yaml | kubectl replace -f -
```

5 새 구성이 성공적으로 저장되었는지 확인합니다.

- 새 `telegraf-config` ConfigMap을 살펴봅니다.

```
kubectl -n vmware-system-monitoring get cm telegraf-config -o yaml
```

- 모든 Telegraf 포드가 가동되어 실행 중인지 확인합니다.

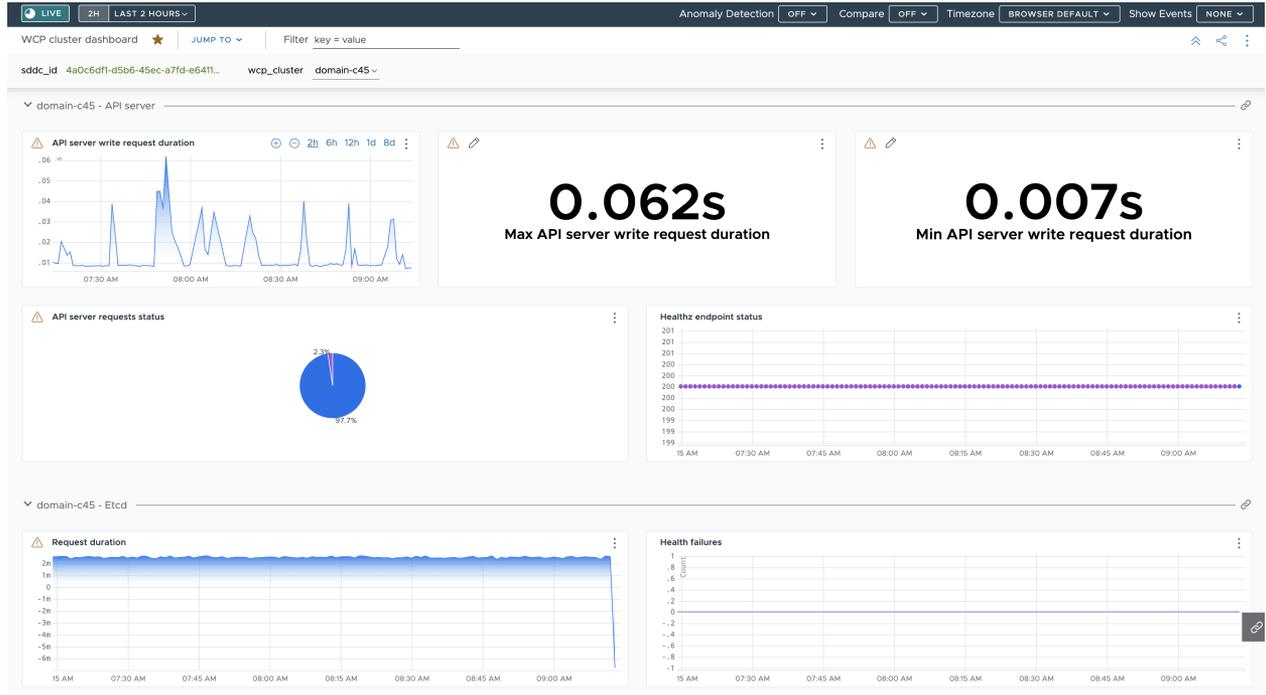
```
kubectl -n vmware-system-monitoring get pods
```

- 일부 Telegraf 포드가 실행되고 있지 않은 경우 해당 포드에 대한 Telegraf 로그를 확인하여 문제를 해결합니다.

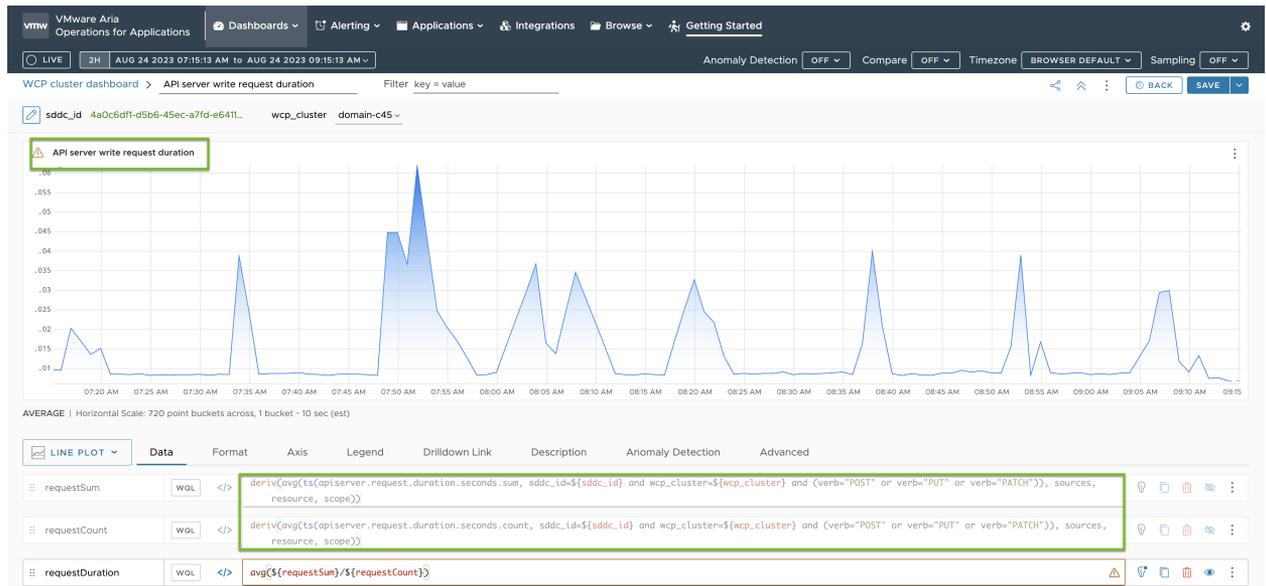
```
kubectl -n vmware-system-monitoring logs <telegraf-pod>
```

예시 Operations for Applications 대시보드

다음은 Telegraf를 통해 감독자의 API 서버 및 etcd에서 수신된 메트릭에 대한 요약을 보여주는 대시보드입니다.



API 서버 쓰기 요청 기간에 대한 메트릭은 녹색으로 강조 표시된 것처럼 telegraf-config ConfigMap에 지정된 메트릭을 기반으로 합니다.



감독자 제어부 DNS 이름 목록 수정

감독자 제어부에 액세스하기 위한 FQDN 목록을 수정하는 방법을 알아봅니다. 감독자 사용 설정 중에 감독자 FQDN 목록을 제공하고 나중에 해당 목록을 업데이트할 수 있습니다. 감독자 사용 설정 중에 FQDN을 제공하지 않은 경우 목록 감독자 FQDN을 설정할 수도 있습니다.

절차

- ◆ 다음 CLI 명령을 사용하여 감독자 제어부에 대한 FQDN 목록을 업데이트합니다.

```
dcli com vmware vcenter namespacemanagement clusters update --cluster <cluster_ID> --
master-dns-name <FQDN_1> --master-dns-name <FQDN_2>
```

- 목록에 새 FQDN을 추가하려면 기존 이름을 인수로 전달하고 새 FQDN을 추가합니다.
- 목록에서 FQDN을 제거하려면 제거하려는 FQDN을 생략하고 유지하려는 나머지 FQDN을 전달하여 update 명령을 호출합니다.

3개 영역 감독자의 경우 감독자의 일부인 클러스터의 ID를 전달할 수 있습니다.

다음 예에서는 클러스터 domain-c50에서 실행되는 감독자가 FQDN supervisor.acme.com으로 이미 구성되어 있습니다. 감독자의 DNS 이름 목록에 새 supervisor.vmware.com FQDN을 추가합니다.

```
dcli com vmware vcenter namespacemanagement clusters update --cluster domain-c50 --master-
dns-name supervisor.acme.com --master-dns-name supervisor.vmware.com
```

다음에 수행할 작업

- 감독자에 안전하게 연결하기 위한 VIP 인증서는 새 FQDN으로 자동 업데이트되지 않습니다. 따라서 수동으로 수행해야 합니다. VIP 인증서를 교체하여 감독자 API 끝점에 안전하게 연결 항목을 참조하십시오.
- 감독자에 연결하기 위한 VIP 인증서를 업데이트한 후에는 새로 추가된 FQDN을 사용하여 감독자 제어부에 로그인합니다. vCenter Single Sign-On 사용자로 감독자에 연결 항목을 참조하십시오.

외부 모니터링 시스템에 감독자 로그 전달

Fluent Bit를 사용하여 감독자 제어부 로그를 Grafana Loki 또는 Elastic Search와 같은 외부 모니터링 시스템으로 전달을 구성하는 방법을 확인합니다.

감독자 제어부 로그는 Fluent Bit를 사용하여 vCenter Server 장치에 구성된 Syslog 서버로 자동으로 전달됩니다. Fluent Bit는 다양한 로그 데이터 유형, 필터링 및 로그 태그 기능 향상을 지원하는 구성을 제공하는 오픈 소스 경량 로깅 및 메트릭 프로세서 및 전달자입니다.

감독자 활성화 또는 업그레이드 중에 부트스트랩 로그는 rsyslog를 통해 vCenter Server 장치에 구성된 Syslog 서버로 계속 전달됩니다. 감독자 제어부 VM이 가동되어 실행되면 Fluent Bit가 감독자 제어부 로그의 기본 로그 전달자가 됩니다.

vSphere 관리자는 다음에 Fluent Bit를 사용할 수 있습니다.

- 감독자 제어부 로그 및 시스템 저널 로그를 Fluent Bit에서 지원되는 Loki, Elastic Search, Grafana 및 기타 플랫폼과 같은 주요 외부 로그 모니터링 플랫폼으로 전달합니다.
- k8s API를 사용하여 감독자 제어부에 대한 로그 전달 구성을 업데이트하거나 재설정합니다.

Fluent Bit는 감독자 제어부 노드에서 DaemonSet로 실행됩니다. vSphere 관리자가 로그 서버를 정의하여 외부 플랫폼으로 로그 전달을 구성하도록 편집할 수 있는 `vmware-system-logging` 네임스페이스 아래에 `fluentbit-config-custom` ConfigMap을 노출합니다.

```
inputs-custom.conf: |
  [INPUT]
    Name          tail
    Alias         audit_apiserver_tail
    Tag           audit.apiserver.*
    Path          /var/log/vmware/audit/kube-apiserver.log
    DB            /var/log/vmware/fluentbit/flb_audit_apiserver.db
    Buffer_Max_Size 12MBb
    Mem_Buf_Limit 32MB
    Skip_Long_Lines On
    Refresh_Interval 10

filters-custom.conf: |
  [FILTER]
    Name          record_modifier
    Alias         audit_apiserver_modifier
    Match         audit.apiserver.*
    Record        hostname ${NODE_NAME}
    Record        appname audit-kube-apiserver
    Record        filename kube-apiserver.log

outputs-custom.conf: |
  [OUTPUT]
    Name          syslog
    Alias         audit_apiserver_output_syslog
    Match         audit.apiserver.*
    Host          <syslog-server-host>
    Port          <syslog-server-port>
    Mode          tcp
    Syslog_Format rfc5424
    Syslog_Message_key log
    Syslog_Hostname_key hostname
    Syslog_Appname_key appname
    Syslog_Msgid_key filename
```

Fluent Bit 로그 전달 사용자 지정

단계에 따라 Fluent Bit 로그 전달 구성을 사용자 지정합니다.

- 1 감독자 제어부에 vCenter Single Sign-On 관리자로 로그인합니다.

```
> kubectl vsphere login --server=<supervisor-cluster-vip> -u administrator@vsphere.local
> kubectl config use-context <supervisor-cluster-vip>
```

- 2 fluentbit-config-custom ConfigMap의 outputs-custom.conf 섹션에서 syslog 출력을 업데이트하거나 추가합니다. 그러면 모든 제어부 VM 시스템 로그가 외부 서버로 전달됩니다.

```
[OUTPUT]
  Name          syslog
  Alias         syslog_system
  Match         system*
  Host          <syslog-server-host>
  Port         <syslog-server-port>
  Mode         tcp
  Syslog_Format rfc5424
  Syslog_Message_key log
  Syslog_Hostname_key hostname
  Syslog_Appname_key appname
  Syslog_Msgid_key filename
  # add the following if the mode is TLS
  Tls          on
  Tls.verify   off
  Tls.ca_file  /etc/ssl/certs/vmca.pem
```

- 3 fluentbit-config-custom ConfigMap에 변경 내용을 적용합니다.

```
> kubectl -n vmware-system-logging edit cm fluentbit-config-custom

# use the below command if the change is stored in outputs-custom.conf file
> kubectl -n vmware-system-logging create configmap fluentbit-config-custom --from-
file=filters-custom.conf --from-file=inputs-custom.conf --from-file=outputs-custom.conf -o
yaml --from-file=parsers-custom.conf --dry-run | kubectl replace -f -
```

- 4 Fluent Bit 포드를 모니터링하여 구성 변경 내용을 자동으로 적용하고 Syslog 서버에서 감독자 로그를 쿼리합니다. 업데이트된 구성이 다시 로드된 후 Fluentbit DaemonSet가 오류로 실행되는 경우 fluentbit-config-custom ConfigMap의 구성을 복구하거나 재설정하여 Fluentbit DaemonSet가 정상 상태가 되도록 합니다.

```
> kubectl -n vmware-system-logging get pod
> kubectl -n vmware-system-logging logs <fluentbit-pod-name>
```

Grafana Loki 서버에 Kubernetes API 서버 감사 로그 전달

다음 단계에 따라 외부 Grafana Loki 서버로 로그 전달을 구성합니다.

- 1 감독자 제어부에 vCenter Single Sign-On 관리자로 로그인합니다.

```
> kubectl vsphere login --server=<supervisor-cluster-vip> -u administrator@vsphere.local
> kubectl config use-context <supervisor-cluster-vip>
```

- 2 fluentbit-config-custom ConfigMap의 outputs-custom.conf 섹션에서 Loki 출력을 업데이트하거나 추가합니다. 그러면 모든 제어부 VM 시스템 로그가 Loki 로그 서버로 전달됩니다.

```
[OUTPUT]
  Name loki
  Alias system_output_loki
  Match system*
  Host <loki-server-host>
  Port <loki-server-port>
  Labels $hostname,$appname,$filename,$procid,$labels
```

- 3 fluentbit-config-custom ConfigMap에 변경 내용을 적용합니다.

```
> kubectl -n vmware-system-logging edit cm fluentbit-config-custom

# use the below command if the change is stored in outputs-custom.conf file
> kubectl -n vmware-system-logging create configmap fluentbit-config-custom --from-
file=filters-custom.conf --from-file=inputs-custom.conf --from-file=outputs-custom.conf -o
yaml --from-file=parsers-custom.conf --dry-run | kubectl replace -f -
```

- 4 Fluent Bit 포드를 모니터링하여 구성 변경 내용을 자동으로 적용하고 Syslog 서버에서 감독자 로그를 쿼리합니다. 업데이트된 구성이 다시 로드된 후 Fluentbit DaemonSet가 오류로 실행되는 경우 fluentbit-config-custom ConfigMap의 구성을 복구하거나 재설정하여 Fluentbit DaemonSet가 정상 상태가 되도록 합니다.

```
> kubectl -n vmware-system-logging get pod
> kubectl -n vmware-system-logging logs <fluentbit-pod-name>
```

Elastic Search에 로그 전달

다음 단계에 따라 외부 Elastic Search 서버로 로그 전달을 구성합니다.

- 1 감독자 제어부에 vCenter Single Sign-On 관리자로 로그인합니다.

```
> kubectl vsphere login --server=<supervisor-cluster-vip> -u administrator@vsphere.local
> kubectl config use-context <supervisor-cluster-vip>
```

- 2 fluentbit-config-custom ConfigMap의 outputs-custom.conf 섹션에서 Elastic Search 출력을 업데이트하거나 추가합니다. 그러면 모든 제어부 VM 시스템 로그가 ES 로그 서버에 전달됩니다.

```
[OUTPUT]
  Name es
  Alias system_output_es
  Match system*
  Host <es-server-host>
  Port <es-server-port>
  Index supervisor
  Type controlplanevm
```

- 3 fluentbit-config-custom ConfigMap에 변경 내용을 적용합니다.

```
> kubectl -n vmware-system-logging edit cm fluentbit-config-custom

# use the below command if the change is stored in outputs-custom.conf file
> kubectl -n vmware-system-logging create configmap fluentbit-config-custom --from-file=filters-custom.conf --from-file=inputs-custom.conf --from-file=outputs-custom.conf --from-file=parsers-custom.conf --dry-run | kubectl replace -f -
```

4

- 5 Fluent Bit 포드를 모니터링하여 구성 변경 내용을 자동으로 적용하고 Syslog 서버에서 감독자 로그를 쿼리합니다.

```
> kubectl -n vmware-system-logging get pod
> kubectl -n vmware-system-logging logs <fluentbit-pod-name>
```

Syslog 서버에 Kubernetes API 감사 로그 전달

다음 단계에 따라 외부 Syslog 서버로 Kubernetes API 감사 로그 전달을 구성합니다.

- 1 kubectl-plugin-vsphere 및 authproxy 입력을 fluentbit-config ConfigMap에 추가합니다.

```
[INPUT]
  Name          tail
  Tag           auth.kubectl-plugin.*
  Path          /var/log/containers/audit/kubectl-plugin-vsphere*.log
  DB            /var/log/vmware/fluentbit/flb_auth_kubectl-plugin.db
  Skip_Long_Lines Off
  Refresh_Interval 10

[INPUT]
  Name          tail
  Tag           auth.authproxy.*
  Path          /var/log/containers/audit/wcp-authproxy*.log
  DB            /var/log/vmware/fluentbit/flb_auth_authproxy.db
  Skip_Long_Lines Off
  Refresh_Interval 10
```

- 2 `kubectl-plugin-vsphere` 및 `authproxy` 필터를 `fluentbit-config` ConfigMap에 추가합니다.

```
[FILTER]
  Name          kubernetes
  Match         auth.*
  Kube_URL      https://localhost:6443
  Tls.verify    Off
  K8S-Logging.Parser On
  K8S-Logging.Exclude On

[FILTER]
  Name          record_modifier
  Match         auth.*
  Operation     lift
  Nested_under  kubernetes

[FILTER]
  Name          modify
  Match         auth.*
  Rename       container_name appname
  Rename       host hostname
  Rename       pod_name procid
```

- 3 Syslog 서버에 `kubectl-plugin-vsphere` 출력을 `fluentbit-config` ConfigMap에 추가합니다.

```
[OUTPUT]
  Name          syslog
  Match         auth.*
  Host          <syslog-server-host>
  Port          <syslog-server-port>
  Mode          tcp
  Syslog_Format rfc5424
  Syslog_Message_key log
  Syslog_Hostname_key hostname
  Syslog_Appname_key appname
  Syslog_Msgid_key filename
```

- 4 위의 파일을 `vmware-system-logging` 네임스페이스 아래의 `fluentbit-config` ConfigMap에 포함합니다.

```
> k -n vmware-system-logging edit cm fluentbit-config
> k -n vmware-system-logging rollout restart ds fluentbit
> k -n vmware-system-logging rollout status ds fluentbit
```

기존 구성을 복제하여 감독자 배포

13

기존 감독자 인스턴스의 구성을 복제하여 감독자를 배포하는 방법을 알아봅니다. 이미 배포된 감독자와 유사한 설정을 사용하여 새 감독자 인스턴스를 배포하려는 경우 감독자를 복제합니다.

사전 요구 사항

- vSphere 클러스터를 감독자로 구성하기 위한 사전 요구 사항을 완료합니다. vSphere 클러스터에서 vSphere IaaS control plane를 구성하기 위한 사전 요구 사항의 내용을 참조하십시오.
- 감독자를 배포합니다.

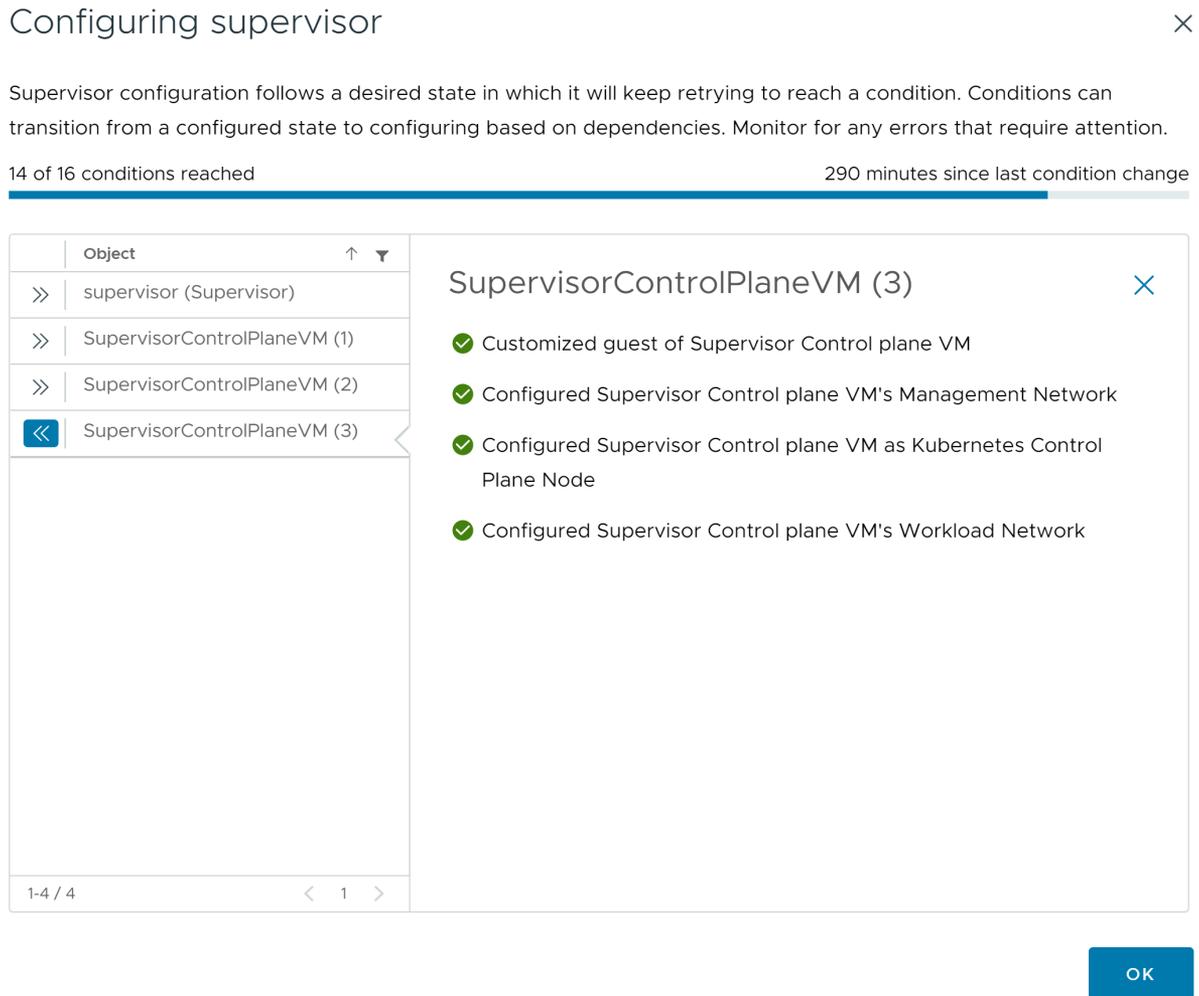
절차

- 1 **워크로드 관리 > 감독자 > 감독자**로 이동합니다.
- 2 복제할 감독자를 선택하고 **구성 복제**를 선택합니다.
선택한 감독자의 값이 미리 채워진 상태로 감독자 활성화 마법사가 열립니다.
- 3 필요에 따라 값을 수정하여 마법사를 진행합니다.
마법사 값에 대한 자세한 내용은 [장 5 3개 영역 감독자 배포](#) 및 [장 6 1개 영역 감독자 배포](#) 항목을 참조하십시오.

다음에 수행할 작업

감독자를 사용하도록 설정하는 마법사를 완료하면 활성화 프로세스를 추적하고 문제 해결이 필요한 잠재적인 문제를 관찰할 수 있습니다. **구성 상태** 열에서 **의 상태 옆에 있는** 보기감독자를 클릭합니다.

그림 13-1. 감독자 활성화 보기



배포 프로세스가 완료되려면 감독자가 원하는 상태에 도달해야 합니다. 즉 16개 조건이 모두 충족되어야 합니다. 감독자가 사용되도록 설정하는 데 성공하면 해당 상태가 [구성 중]에서 [실행 중]으로 변경됩니다. 감독자가 [구성 중] 상태에 있는 동안 16개 조건 각각에 도달하기 위한 재시도가 계속됩니다. 조건에 도달하지 않으면 성공할 때까지 작업이 재시도됩니다. 이러한 이유로 인해 도달한 조건 수가 오락가락 변경될 수 있습니다(예: "16개 중 10개 조건에 도달" 후 "16개 중 4개 조건에 도달" 등). 매우 드문 경우지만 원하는 상태에 도달하지 못하게 하는 오류가 있는 경우 상태가 오류로 변경될 수 있습니다.

배포 오류 및 문제 해결 방법에 대한 자세한 내용은 [활성화 또는 업데이트 중 감독자 제어부 VM의 오류 상태 해결](#)을 참조하십시오.

감독자 사용 설정 문제 해결

14

감독자 사용 설정 문제를 해결하여 원하는 상태에 도달하고 16개 사용 설정 조건이 모두 충족되도록 하는 방법을 알아봅니다.

다음으로 아래 항목을 읽으십시오.

- 활성화 또는 업데이트 중 감독자 제어부 VM의 오류 상태 해결
- 감독자 제어부의 로그를 원격 rsyslog로 스트리밍
- 워크로드 관리 사용 설정 클러스터 호환성 오류 문제 해결
- 워크로드 관리 로그 파일에 tail 명령 사용

활성화 또는 업데이트 중 감독자 제어부 VM의 오류 상태 해결

감독자를 활성화하거나, 감독자 Kubernetes 버전을 업데이트하거나, 기존 감독자의 설정을 편집한 후에는 구성 이 완료될 때까지 지정한 모든 설정의 유효성을 검사하고 감독자에 적용합니다. 입력한 매개 변수에 대해 상태 점검이 수행되어 구성에서 오류가 감지되면 감독자가 오류 상태가 될 수 있습니다. 이러한 오류 상태를 해결해야 감독자의 구성 또는 업데이트가 가능합니다.

표 14-1. vCenter Server 연결 오류

오류 메시지	원인	솔루션
제어부 VM <VM name>에 구성된 관리 DNS 서버로 vCenter 기본 네트워크 식별자 <FQDN>을(를) 확인할 수 없습니다. 관리 DNS 서버 <server name>에서 <network name>을(를) 확인할 수 있는지 확인합니다.	<ul style="list-style-type: none"> ■ 하나 이상의 관리 DNS 서버에 연결할 수 있습니다. ■ 하나 이상의 관리 DNS가 정적으로 제공됩니다. ■ 관리 DNS 서버에 vCenter Server PNID에 대한 호스트 이름 조회가 없습니다. ■ vCenter Server PNID는 정적 IP 주소가 아닌 도메인 이름입니다. 	<ul style="list-style-type: none"> ■ 관리 DNS 서버에 vCenter Server PNID에 대한 호스트 항목을 추가합니다. ■ 구성된 DNS 서버가 올바른지 확인합니다.
제어부 VM <VM name>의 관리 네트워크에서 DHCP를 통해 획득한 DNS 서버로 vCenter 기본 네트워크 식별자 <network name>을(를) 확인할 수 없습니다. 관리 DNS 서버에서 <network name>을(를) 확인할 수 있는지 확인합니다.	<ul style="list-style-type: none"> ■ DHCP 서버(하나 이상)에서 제공하는 관리 DNS 서버에 연결할 수 있습니다. ■ 관리 DNS 서버는 정적으로 제공됩니다. ■ 관리 DNS 서버에 vCenter Server PNID에 대한 호스트 이름 조회가 없습니다. ■ 관리 DNS 서버에 vCenter Server PNID에 대한 호스트 이름 조회가 없습니다. ■ vCenter Server PNID는 정적 IP 주소가 아닌 도메인 이름입니다. 	<ul style="list-style-type: none"> ■ 구성된 DHCP 서버에서 제공하는 관리 DNS 서버에 vCenter Server PNID에 대한 호스트 항목을 추가합니다. ■ DHCP 서버에서 제공한 DNS 서버가 올바른지 확인합니다.
구성된 관리 DNS 서버가 없기 때문에 제어부 VM <VM name>에서 호스트 <host name>을(를) 확인할 수 없습니다.	<ul style="list-style-type: none"> ■ vCenter Server PNID는 정적 IP 주소가 아닌 도메인 이름입니다. ■ 구성된 DNS 서버가 없습니다. 	관리 DNS 서버를 구성합니다.
제어부 VM <VM name>에서 호스트 <host name>을(를) 확인할 수 없습니다. 호스트 이름은 '.local' 최상위 도메인으로 끝나며, 따라서 관리 DNS 검색 도메인에 '.local'이 포함되어야 합니다.	vCenter Server PNID에 .local이 TLD(최상위 도메인)로 포함되어 있지만 구성된 검색 도메인에는 local.이 포함되지 않습니다.	관리 DNS 검색 도메인에 local을 추가합니다.

표 14-1. vCenter Server 연결 오류 (계속)

오류 메시지	원인	솔루션
제어부 VM <VM name>에서 관리 DNS 서버 <server name>에 연결할 수 없습니다. 워크로드 네트워크를 통해 연결을 시도했습니다.	<ul style="list-style-type: none"> ■ 관리 DNS 서버를 vCenter Server에 연결할 수 없습니다. ■ 제공된 <code>worker_dns</code> 값은 제공된 관리 DNS 값을 완전히 포함합니다. 즉, 트래픽은 워크로드 네트워크를 통해 라우팅됩니다. 감독자는 정적 트래픽을 이러한 IP로 전송하기 위해 하나의 네트워크 인터페이스를 선택해야 하기 때문입니다. 	<ul style="list-style-type: none"> ■ 워크로드 네트워크를 확인하여 구성된 관리 DNS 서버로 라우팅할 수 있는지 확인합니다. ■ 워크로드 네트워크의 일부 다른 서버와 DNS 서버 간에 대체 라우팅을 트리거할 수 있는 충돌하는 IP 주소가 없는지 확인합니다. ■ 구성된 DNS 서버가 실제로 DNS 서버이고 포트 53에서 해당 DNS 포트를 호스팅하고 있는지 확인합니다. ■ 워크로드 DNS 서버가 제어부 VM의 IP(워크로드 네트워크 제공 IP)로부터의 연결을 허용하도록 구성되어 있는지 확인합니다. ■ 관리 DNS 서버의 주소에 오타가 없는지 확인합니다. ■ 검색 도메인에 불필요한 '~'가 포함되어 있지 않은지 확인합니다. 그러면 호스트 이름이 잘못 확인될 수 있습니다.
제어부 VM <VM name>에서 관리 DNS 서버 <server name>에 연결할 수 없습니다.	DNS 서버에 연결할 수 없습니다.	<ul style="list-style-type: none"> ■ 관리 네트워크를 확인하여 관리 DNS 서버에 대한 경로가 존재하는지 확인합니다. ■ DNS 서버와 다른 서버 간에 대체 라우팅을 트리거할 수 있는 충돌하는 IP 주소가 없는지 확인합니다. ■ 구성된 DNS 서버가 실제로 DNS 서버이고 포트 53에서 해당 DNS 포트를 호스팅하고 있는지 확인합니다. ■ 관리 DNS 서버가 제어부 VM의 IP로부터의 연결을 허용하도록 구성되어 있는지 확인합니다. ■ 관리 DNS 서버의 주소에 오타가 없는지 확인합니다. ■ 검색 도메인에 불필요한 '~'가 포함되어 있지 않은지 확인합니다. 그러면 호스트 이름이 잘못 확인될 수 있습니다.
제어부 VM <vm name>에서 <component name> <component address>에 연결할 수 없습니다. 오류: <i>error message text</i>	<ul style="list-style-type: none"> ■ 일반 네트워크 오류가 발생했습니다. ■ vCenter Server에 실제 연결하는 동안 오류가 발생했습니다. 	<ul style="list-style-type: none"> ■ vCenter Server, HAProxy, NSX Manager 또는 NSX Advanced Load Balancer와 같은 구성된 구성 요소의 호스트 이름 또는 IP 주소가 올바른지 확인합니다. ■ 관리 네트워크에서 충돌하는 IP, 방화벽 규칙 등의 외부 네트워크 설정이 있는지 확인합니다.

표 14-1. vCenter Server 연결 오류 (계속)

오류 메시지	원인	솔루션
제어부 VM <VM name>에서 vCenter <vCenter Server name> 인증서의 유효성을 검사할 수 없습니다. vCenter Server 인증서가 잘못되었습니다.	vCenter Server에서 제공한 인증서가 잘못된 형식이므로 신뢰할 수 없습니다.	<ul style="list-style-type: none"> ■ wcpssc를 다시 시작하여 제어부 VM의 신뢰할 수 있는 루트 번들이 최신 vCenter Server 루트 인증서로 최신 상태인지 확인합니다. ■ vCenter Server 인증서가 실제로 유효한 인증서인지 확인합니다.
제어부 VM <VM name>이(가) vCenter <vCenter Server name> 인증서를 신뢰하지 않습니다.	<ul style="list-style-type: none"> ■ vCenter Server에서 제공한 vmca.pem 인증서가 제어부 VM에 구성된 것과 다릅니다. ■ 신뢰할 수 있는 루트 인증서가 vCenter Server Appliance에서 교체되었지만 wcpssc가 다시 시작되지 않았습니다. 	<ul style="list-style-type: none"> ■ wcpssc를 다시 시작하여 제어부 VM의 신뢰할 수 있는 루트 번들이 최신 vCenter Server 인증서 루트를 사용하는 최신 상태인지 확인합니다.

표 14-2. NSX Manager 연결 오류

제어부 VM <VM name>에서 NSX Server(<NSX server name>) 인증서의 유효성을 검사할 수 없습니다. 서버에서 반환된 지문(<NSX-T address>)이 vCenter에 등록된 예상 클라이언트 인증서 지문(<vCenter Server name>)과 일치하지 않습니다.	감독자에 등록된 SSL 지문이 NSX Manager에서 제공한 인증서의 SHA-1 해시와 일치하지 않습니다.	<ul style="list-style-type: none"> ■ NSX와 vCenter Server 인스턴스 간에 NSX Manager에서 신뢰를 다시 사용하도록 설정합니다. ■ vCenter Server에서 wcpssc를 다시 시작합니다.
제어부 VM <vm name>에서 <component name> <component address>에 연결할 수 없습니다. 오류: <i>error message text</i>	일반 네트워크 오류가 발생했습니다.	<ul style="list-style-type: none"> ■ NSX Manager의 관리 네트워크에서 외부 네트워크 설정, 충돌하는 IP, 방화벽 규칙 등을 확인합니다. ■ NSX 확장의 NSX Manager IP가 올바른지 확인합니다. ■ NSX Manager가 실행 중인지 확인합니다.

표 14-3. 로드 밸런서 오류

제어부 VM <vm name>이(가) 로드 밸런서(<load balancer>~<load balancer endpoint>)의 인증서를 신뢰하지 않습니다.	로드 밸런서가 제공하는 인증서가 제어부 VM에 구성된 인증서와 다릅니다.	로드 밸런서에 올바른 관리 TLS 인증서를 구성했는지 확인합니다.
제어부 VM <vm name>에서 로드 밸런서(<load balancer>~<load balancer endpoint>)의 인증서를 확인할 수 없습니다. 인증서가 잘못되었습니다.	로드 밸런서가 제공하는 인증서의 형식이 잘못되었거나 만료되었습니다.	구성된 로드 밸런서의 서버 인증서를 수정하십시오.

표 14-3. 로드 밸런서 오류 (계속)

제어부 VM <vm name>에서 사용자 이름 <user name> 및 제공된 암호를 사용하여 로드 밸런서(<load balancer>~<load balancer endpoint>)에 인증할 수 없습니다.	로드 밸런서의 사용자 이름 또는 암호가 잘 못되었습니다.	로드 밸런서에 구성된 사용자 이름 및 암호가 올바른지 확인합니다.
제어부 VM <vm name>에서 로드 밸런서 (<load balancer>~<load balancer endpoint>)에 연결하려고 시도하는 중 HTTP 오류가 발생했습니다.	제어부 VM이 로드 밸런서 끝점에 연결할 수 있지만 끝점이 성공적인(200) HTTP 응답을 반환하지 않습니다.	로드 밸런서가 정상이고 요청을 수락하는지 확인합니다.
제어부 VM <vm name>에서 <load balancer>(<load balancer endpoint>)에 연결할 수 없습니다. 오류: <error text>	<ul style="list-style-type: none"> ■ 일반 네트워크 오류가 발생했습니다. ■ 일반적으로 로드 밸런서가 작동하지 않거나 일부 방화벽이 연결을 차단한다는 의미입니다. 	<ul style="list-style-type: none"> ■ 로드 밸런서 끝점에 액세스할 수 있는지 확인합니다. ■ 로드 밸런서에 대한 연결을 차단하는 방화벽이 없는지 확인합니다.

감독자 제어부의 로그를 원격 rsyslog로 스트리밍

귀중한 로깅 데이터의 손실을 방지하기 위해 감독자 제어부 VM에서 원격 rsyslog 수신기로의 로그 스트리밍을 구성하는 방법을 알아봅니다.

감독자 제어부 VM의 구성 요소에서 생성된 로그는 VM의 파일 시스템에 로컬로 저장됩니다. 많은 양의 로그가 누적되면 로그가 높은 속도로 순환되어 다양한 문제의 근본 원인을 식별하는 데 도움이 될 수 있는 귀중한 메시지가 손실됩니다. vCenter Server 및 감독자 제어부 VM은 로컬 로그를 원격 rsyslog 수신기로 스트리밍하는 기능을 지원합니다. 이 기능은 다음 서비스 및 구성 요소에 대한 로그를 캡처하는 데 도움이 됩니다.

- vCenter Server: 워크로드 제어부 서비스, ESX Agent Manager 서비스, CA(인증 기관) 서비스 및 vCenter Server에서 실행 중인 기타 모든 서비스.
- 감독자 제어부 구성 요소 및 감독자 내장형 서비스(예: VM 서비스 및 Tanzu Kubernetes Grid).

로컬 로그 데이터를 수집하고 원격 rsyslog 수신기로 스트리밍하도록 vCenter Server Appliance를 구성할 수 있습니다. 이 구성이 vCenter Server에 적용되면 vCenter Server 내부에서 실행되는 rsyslog 발신자가 해당 vCenter Server 시스템 내부의 서비스에서 생성된 로그를 보내기 시작합니다.

감독자는 vCenter Server와 동일한 메커니즘을 사용하여 로컬 로그를 오프로드하여 구성 관리 부담을 줄여줍니다. 워크로드 제어부 서비스는 로그를 주기적으로 폴링하여 vCenter Server rsyslog 구성을 모니터링합니다. 워크로드 제어부 서비스가 원격 vCenter Server rsyslog 구성이 비어 있지 않은 것을 감지하면 서비스는 이 구성을 모든 감독자의 각 제어부 VM에 전파합니다. 이로 인해 원격 rsyslog 수신기에 부담을 줄 수 있는 대량의 rsyslog 메시지 트래픽이 생성될 수 있습니다. 따라서 수신기 시스템에는 대량의 rsyslog 메시지를 유지하기에 충분한 스토리지 용량이 있어야 합니다.

vCenter Server에서 rsyslog 구성을 제거하면 vCenter Server에서 rsyslog 메시지가 중지됩니다. 워크로드 제어부 서비스는 변경 내용을 감지하고 모든 감독자의 각 제어부 VM에 전파하여 결국 제어부 VM 스트림도 중지됩니다.

구성 단계

다음 단계를 수행하여 감독자 제어부 VM에 대한 rsyslog 스트리밍을 구성합니다.

- 1 다음에 해당하는 시스템을 프로비저닝하여 rsyslog 수신기를 구성합니다.
 - 수신기 모드에서 rsyslog 서비스를 실행합니다. rsyslog 설명서에서 [고성능으로 대량의 메시지 수신 예](#)를 참조하십시오.
 - 대량의 로그 데이터를 수용하기에 충분한 스토리지 공간이 있습니다.
 - vCenter Server 및 감독자 제어부 VM에서 데이터를 수신하기 위한 네트워크 연결이 있습니다.
- 2 "https://<vcenter server address>:5480" 에서 vCenter Server Appliance 관리 인터페이스에 루트로 로그인합니다.
- 3 vCenter Server Appliance 관리 인터페이스를 통해 rsyslog 수신기로 스트리밍하도록 vCenter Server를 구성합니다. [vCenter Server 로그 파일을 원격 Syslog 서버에 전달](#)을 참조하십시오.

vCenter Server의 rsyslog 구성이 감독자 제어부 VM에 적용되는 데 몇 분 정도 걸릴 수 있습니다. vCenter Server Appliance의 워크로드 제어부 서비스는 5분마다 장치 구성을 폴링하여 사용 가능한 모든 감독자에 전파합니다. 전파를 완료하는 데 필요한 시간은 환경의 감독자 수에 따라 다릅니다. 감독자의 제어부 VM 중 일부가 비정상 상태이거나 다른 작업을 수행하는 경우 워크로드 제어부 서비스는 성공할 때까지 rsyslog 구성 적용을 재시도합니다.

제어부 VM 구성 요소의 로그 검사

감독자 제어부 VM의 rsyslog는 이러한 로그 메시지의 소스 구성 요소를 나타내는 태그를 로그 메시지에 포함합니다.

로그 태그	설명
vns-control-plane-pods <pod_name>/<instance_number>.log	제어부 VM의 Kubernetes 포드에서 발생한 로그. 예: vns-control-plane-pods etcd/0.log 또는 vns-control-plane-pods nsx-ncp/573.log
vns-control-plane-imc	제어부 VM의 초기 구성 로그.
vns-control-plane-boostrap	Kubernetes 노드 제어부 배포의 부트스트랩 로그.
vns-control-plane-upgrade-logs	제어부 노드 패치 및 부 버전 업그레이드의 로그.
vns-control-plane-svchost-logs	제어부 VM 시스템 수준 서비스 호스트 또는 에이전트 로그.
vns-control-plane-update-controller	제어부의 원하는 상태 동기화 프로그램 및 실행 프로그램(realizer) 로그.
vns-control-plane-compact-etcd-logs	제어부 etcd 서비스 스토리지 압축을 유지하기 위한 로그.

워크로드 관리 사용 설정 클러스터 호환성 오류 문제 해결

vSphere 클러스터가 호환되지 않아서 워크로드 관리를 사용하도록 설정할 수 없다고 시스템에 표시되면, 다음 문제 해결 팁을 따르십시오.

문제

워크로드 관리를 사용하도록 설정하려고 하면 **워크로드 관리** 페이지에 vCenter 클러스터가 호환되지 않는다고 표시됩니다.

원인

여기에는 여러 가지 원인이 있을 수 있습니다. 먼저 환경이 워크로드 관리를 사용하도록 설정하기 위한 최소 요구 사항을 충족하는지 확인합니다.

- 유효한 라이선스: VMware vSphere 7 Enterprise Plus with Add-on for Kubernetes
- 둘 이상의 ESXi 호스트
- 완전히 자동화된 DRS
- vSphere HA
- vSphere Distributed Switch 7.0
- 충분한 스토리지 용량

환경이 이러한 사전 요구 사항을 충족해도 대상 vCenter 클러스터가 호환되지 않는 경우에는 VMware DCLI(Datacenter CLI)를 사용하여 문제를 식별합니다.

해결책

- 1 vCenter Server에 SSH를 실행합니다.
- 2 루트 사용자로 로그인합니다.
- 3 `dcli` 명령을 실행하여 VMware Datacenter CLI 도움말을 나열합니다.
- 4 다음 DCLI 명령을 실행하여 사용 가능한 vCenter 클러스터를 나열합니다.

```
dcli com vmware vcenter cluster list
```

예:

```
dcli +username VI-ADMIN-USER-NAME +password VI-ADMIN-PASSWORD com vmware vcenter cluster list
```

예제 결과:

```
|-----|-----|-----|-----|
|drs_enabled|cluster |name          |ha_enabled|
|-----|-----|-----|-----|
|True       |domain-d7|vSAN Cluster|True      |
|-----|-----|-----|-----|
```

- 5 다음 DCLI 명령을 실행하여 vCenter 클러스터 호환성을 확인합니다.

```
dcli com vmware vcenter namespacemanagement clustercompatibility list
```

예:

```
dcli +username VI-ADMIN-USER-NAME +password VI-ADMIN-PASSWORD com vmware vcenter
namespacemanagement clustercompatibility list
```

다음 예제 결과는 호환되는 NSX VDS 스위치가 환경에 없다는 것을 나타냅니다.

```
|-----|-----|-----|-----|
|-----|-----|-----|-----|
|cluster |compatible|
incompatibility_reasons |
|-----|-----|-----|-----|
|-----|-----|-----|-----|
|domain-d7|False      |Failed to list all distributed switches in vCenter 2b1c1fa5-
e9d4-45d7-824c-fa4176da96b8.|
|          |          |Cluster domain-d7 is missing compatible NSX
VDS.      |
|-----|-----|-----|-----|
|-----|-----|-----|-----|
```

- 6 추가 호환성 문제를 확인하려면 필요에 따라 추가 DCLI 명령을 실행합니다. NSX 오류 외에 호환되지 않는 다른 일반적인 이유는 DNS와 NTP 연결 문제입니다.
- 7 추가로 문제를 해결하려면 다음 단계를 완료하십시오.
- wcpsvc.log 파일에 tail 명령을 사용합니다. 워크로드 관리 로그 파일에 tail 명령 사용의 내용을 참조하십시오.
 - 워크로드 관리 페이지로 이동하여 사용을 클릭합니다.

워크로드 관리 로그 파일에 tail 명령 사용

워크로드 관리 로그 파일에 tail 명령을 사용하면 사용 설정 문제 및 감독자 배포 오류를 해결하는 데 유용할 수 있습니다.

해결책

- vCenter Server Appliance에 대한 SSH 연결을 설정합니다.

2 root 사용자로 로그인합니다.

3 shell 명령을 실행합니다.

다음 내용이 보입니다

```
Shell access is granted to root  
root@localhost [ ~ ]#
```

4 다음 명령을 실행하여 로그를 살펴봅니다.

```
tail -f /var/log/vmware/wcp/wcpsvc.log
```

감독자를 사용하도록 설정할 때 발생할 수 있는 네트워킹 및 로드 밸런서 문제를 해결할 수 있습니다.

다음으로 아래 항목을 읽으십시오.

- NSX Manager에 vCenter Server 등록
- NSX Advanced Load Balancer 문제 해결을 위한 지원 번들 수집
- 호스트 전송 노드 트래픽에 필요한 VDS

NSX Manager에 vCenter Server 등록

vCenter Server의 FQDN/PNID가 변경될 때와 같은 특정 상황에서 NSX Manager에 vCenter Server OIDC를 다시 등록해야 할 수 있습니다.

절차

- 1 SSH를 통해 vCenter Server Appliance에 연결합니다.
- 2 shell 명령을 실행합니다.
- 3 vCenter Server 지문을 가져오려면 다음 명령을 실행합니다.

```
- openssl s_client -connect vcenterserver-FQDN:443 </dev/null 2>/dev/null | openssl x509  
-fingerprint -sha256 -noout -in /dev/stdin
```

지문이 표시됩니다. 예를 들어

```
08:77:43:29:E4:D1:6F:29:96:78:5F:BF:D6:45:21:F4:0E:3B:2A:68:05:99:C3:A4:89:8F:F2:0B  
:EA:3A:BE:9D입니다.
```

- 4 SHA256 지문을 복사하고 콜론을 제거합니다.

```
08774329E4D16F2996785FBFD64521F40E3B2A680599C3A4898FF20BEA3ABE9D
```

- 5 vCenter Server의 OIDC를 업데이트하려면 다음 명령을 실행합니다.

```
curl --location --request POST 'https://<NSX-T_ADDRESS>/api/v1/trust-management/oidc-uris'  
\ --header 'Content-Type: application/json' \  
--header 'Authorization: Basic <AUTH_CODE>' \  
--data-raw '{  
  "oidc_type": "vcenter",
```

```
"oidc_uri": "https://<VC_ADDRESS>/openidconnect/vsphere.local/.well-known/openid-configuration",  
  "thumbprint": "<VC_THUMBPRINT>"  
}'
```

NSX 장치 암호를 변경할 수 없음

root, admin 또는 audit 사용자의 NSX 장치 암호를 변경하지 못할 수 있습니다.

문제

vSphere Client를 통해 root, admin 또는 audit 사용자의 NSX 장치 암호를 변경하려는 시도가 실패할 수 있습니다.

원인

NSX Manager를 설치하는 동안 절차는 세 가지 역할 모두에 대해 하나의 암호만 허용합니다. 나중에 이 암호를 변경하려고 하면 실패할 수 있습니다.

해결책

- ◆ 암호를 변경하려면 NSX API를 사용합니다.

자세한 내용은 <https://kb.vmware.com/s/article/70691> 및 "NSX 관리 가이드"의 내용을 참조하십시오.

실패한 워크플로 및 불안정한 NSX Edge 문제 해결

워크플로가 실패하거나 NSX Edge가 불안정한 경우 문제 해결 단계를 수행할 수 있습니다.

문제

vSphere Client에서 분산 포트 그룹 구성을 변경하면 워크플로가 실패하고 NSX Edge가 불안정해질 수 있습니다.

원인

클러스터 구성의 NSX Edge 클러스터 설정 동안 생성된 오버레이 및 업링크에 대한 분산 포트 그룹의 제거 또는 수정은 설계상 허용되지 않습니다.

해결책

NSX Edge의 VLAN 또는 IP 풀 구성을 변경해야 하는 경우 먼저 NSX의 요소 및 vSphere IaaS control plane 구성 요소를 클러스터에서 제거해야 합니다.

NSX의 요소 제거에 대한 자세한 내용은 "NSX 설치 가이드"의 내용을 참조하십시오.

NSX 문제 해결을 위한 지원 번들 수집

문제 해결을 위해 등록된 클러스터 및 패브릭 노드에 대한 지원 번들을 수집하고 번들을 시스템에 다운로드하거나 파일 서버에 업로드할 수 있습니다.

번들을 시스템에 다운로드하도록 선택하면, 각 노드에 대한 지원 번들 및 매니페스트 파일로 구성된 단일 아카이브 파일이 제공됩니다. 번들을 파일 서버에 업로드하도록 선택하면 매니페스트 파일과 개별 번들이 파일 서버에 별도로 업로드됩니다.

절차

1 브라우저에서 관리자 권한으로 NSX Manager에 로그인합니다.

2 **시스템 > 지원 번들**을 선택합니다.

3 대상 노드를 선택합니다.

사용 가능한 노드 유형은 **관리 노드**, **Edge**, **호스트** 및 **공용 클라우드 게이트웨이**입니다.

4 (선택 사항) 로그 보존 기간을 일 단위로 지정하면 지정된 일 수보다 오래된 로그를 제외할 수 있습니다.

5 (선택 사항) 코어 파일 및 감사 로그를 포함하지 아니면 제외할지를 나타내는 스위치를 전환합니다.

참고 코어 파일 및 감사 로그에는 암호나 암호화 키와 같은 중요한 정보가 포함될 수 있습니다.

6 (선택 사항) 파일 서버에 번들을 업로드하려면 이 확인란을 선택합니다.

7 지원 번들 수집을 시작하려면 **번들 수집 시작**을 클릭합니다.

각 노드의 로그 파일 수에 따라 지원 번들을 수집하는 데 걸리는 시간이 결정됩니다.

8 수집 프로세스 상태를 모니터링합니다.

상태 탭에 지원 번들 수집에 대한 진행률이 표시됩니다.

9 번들을 파일 서버로 전송하는 옵션이 설정되지 않은 경우 **다운로드**를 클릭하여 번들을 다운로드합니다.

NSX에 대한 로그 파일 수집

vSphere IaaS control plane 및 NSX 구성 요소에 있는 로그를 수집하여 오류를 감지하고 문제를 해결할 수 있습니다. 로그 파일은 VMware 지원에서 요청할 수 있습니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 다음 로그 파일을 수집합니다.

로그 파일	설명
<code>/var/log/vmware/wcp/wcpsvc.log</code>	vSphere IaaS control plane 사용 설정과 관련된 정보를 포함합니다.
<code>/var/log/vmware/wcp/nsxd.log</code>	NSX 구성 요소 구성과 관련된 정보를 포함합니다.

3 NSX Manager에 로그인합니다.

4 특정 vSphere IaaS control plane 작업이 실패하는 경우 NSX Manager가 반환하는 오류에 대한 정보는 `/var/log/proton/nsxapi.log`를 수집합니다.

NSX 관리 인증서, 지문 또는 IP 주소가 변경되면 WCP 서비스 다시 시작

vSphere IaaS control plane를 설치한 후 NSX 관리 인증서, 지문 또는 IP 주소가 변경되면 WCP 서비스를 다시 시작해야 합니다.

NSX 인증서가 변경되면 vSphere IaaS control plane 서비스 다시 시작

현재 vSphere IaaS control plane에서는 NSX 인증서, 지문 또는 NSX IP 주소가 변경되면 WCP 서비스를 다시 시작해야 변경 사항이 적용됩니다. 변경되었는데도 서비스를 다시 시작하지 않으면 vSphere IaaS control plane와 NSX 간의 통신이 실패하고 NCP가 CrashLoopBackoff 단계로 진입하거나 감독자 리소스가 배포 불가 상태가 되는 등의 특정 증상이 발생할 수 있습니다.

WCP 서비스를 다시 시작하려면 `vmon-cli`를 사용합니다.

- 1 SSH를 사용하여 vCenter Server에 연결하고 루트 사용자로 로그인합니다.
- 2 `shell` 명령을 실행합니다.
- 3 `vmon-cli -h` 명령을 실행하여 사용법 구문 및 옵션을 확인합니다.
- 4 `vmon-cli -l` 명령을 실행하여 wcp 프로세스를 봅니다.
목록 맨 아래에 wcp 서비스가 표시됩니다.
- 5 `vmon-cli --restart wcp` 명령을 실행하여 wcp 서비스를 다시 시작합니다.
Completed Restart service request 메시지가 표시됩니다.
- 6 `vmon-cli -s wcp` 명령을 실행하고 wcp 서비스가 시작되었는지 확인합니다.

예:

```
root@localhost [ ~ ]# vmon-cli -s wcp
Name: wcp
Starttype: AUTOMATIC
RunState: STARTED
RunAsUser: root
CurrentRunStateDuration(ms): 22158
HealthState: HEALTHY
FailStop: N/A
MainProcessId: 34372
```

NSX Advanced Load Balancer 문제 해결을 위한 지원 번들 수집

NSX Advanced Load Balancer 문제를 해결하기 위해 지원 번들을 수집할 수 있습니다. VMware 지원에서 지원 번들을 요청할 수도 있습니다.

지원 번들을 생성하면 디버그 로그에 대한 단일 파일이 생성되어 다운로드할 수 있습니다.

절차

- 1 NSX Advanced Load Balancer Controller 대시보드에서 왼쪽 상단 모서리에 있는 메뉴를 클릭하고 **관리**를 선택합니다.
- 2 **관리** 섹션에서 **시스템**을 선택합니다.
- 3 **시스템** 화면에서 **기술 지원**을 선택합니다.
- 4 진단 번들을 생성하려면 **기술 지원 생성**을 클릭합니다.
- 5 **기술 지원 생성** 창에서 **디버그 로그** 유형을 선택하고 **생성**을 클릭합니다.
- 6 번들이 생성되면 다운로드 아이콘을 클릭하여 시스템에 다운로드합니다.

로그 수집에 대한 자세한 내용은 <https://avinetworks.com/docs/21.1/collecting-tech-support-logs/> 항목을 참조하십시오.

NSX Advanced Load Balancer 구성이 적용되지 않음

감독자를 배포하면 배포가 완료되지 않고 NSX Advanced Load Balancer 구성이 적용되지 않습니다.

문제

사설 CA(인증 기관) 서명 인증서를 제공하는 경우 NSX Advanced Load Balancer 구성이 적용되지 않습니다.

감독자에서 실행되는 NCP 포드 중 하나의 로그 파일에 `Unable to find certificate chain` 오류 메시지가 표시될 수 있습니다.

- 1 감독자 VM에 로그인합니다.
- 2 `kubectl get pods -A XX` 명령을 사용하여 모든 Pod를 나열합니다.
- 3 감독자의 모든 NCP 포드에서 로그를 가져옵니다.

```
kubectl -n vmware-system-nsx logs nsx-ncp-<id> | grep -i alb
```

원인

Java SDK는 NCP와 NSX Advanced Load Balancer Controller 간의 통신을 설정하는 데 사용됩니다. 이 오류는 NSX 신뢰 저장소가 Java 인증서 신뢰 저장소와 동기화되지 않은 경우 발생합니다.

해결책

- 1 NSX Advanced Load Balancer에서 루트 CA 인증서를 내보내고 NSX Manager에 저장합니다.
- 2 루트 사용자로 NSX Manager에 로그인합니다.
- 3 모든 NSX Manager 노드에서 다음 명령을 순차적으로 실행합니다.

```
keytool -importcert -alias startssl -keystore /usr/lib/jvm/jre/lib/security/cacerts
-storepass changeit -file <ca-file-path>
```

경로를 찾을 수 없으면 `keytool -importcert -alias startssl -keystore /usr/java/jre/lib/security/cacerts -storepass changeit -file <ca-file-path>`를 실행합니다.

```
sudo cp <ca-file-path> /usr/local/share/ca-certificates/
sudo update-ca-certificates
service proton restart
```

참고 동일한 단계를 수행하여 중간 CA 인증서를 할당할 수 있습니다.

4 감독자 배포가 완료될 때까지 기다리거나 배포가 수행되지 않으면 다시 배포합니다.

ESXi 호스트를 유지 보수 모드로 전환할 수 없음

업그레이드를 수행하려는 경우 ESXi 호스트를 유지 보수 모드로 전환합니다.

문제

ESXi 호스트를 유지 보수 모드로 전환할 수 없으며 ESXi 및 NSX 업그레이드에 영향을 미칠 수 있습니다.

원인

이 문제는 ESXi 호스트에 전원이 켜진 상태의 서비스 엔진이 있는 경우에 발생할 수 있습니다.

해결책

- ◆ ESXi가 유지 보수 모드로 전환될 수 있도록 서비스 엔진의 전원을 끕니다.

IP 주소 문제 해결

외부 IP 할당 문제가 발생하면 다음 문제 해결 팁을 따르십시오.

IP 주소 문제는 다음과 같은 이유로 발생할 수 있습니다.

- 게이트웨이 및 수신과 같은 Kubernetes 리소스가 AKO에서 외부 IP를 가져오지 않습니다.
- Kubernetes 리소스에 할당된 외부 IP에 연결할 수 없습니다.
- 잘못 할당된 외부 IP입니다.

Kubernetes 리소스가 AKO에서 외부 IP를 가져오지 않음

이 오류는 AKO가 NSX Advanced Load Balancer Controller에서 해당 가상 서비스를 생성할 수 없을 때 발생합니다.

AKO 포드가 실행 중인지 확인합니다. 포드가 실행 중인 경우 AKO 컨테이너 로그에서 오류를 확인합니다.

Kubernetes 리소스에 할당된 외부 IP에 연결할 수 없음

이 문제는 다음과 같은 이유로 발생할 수 있습니다.

- 외부 IP를 즉시 사용할 수 없지만 생성 후 몇 분 내에 트래픽 수락이 시작됩니다. 이 문제는 가상 서비스 배치를 위해 새로운 서비스 엔진 생성이 트리거될 때 발생합니다.
- 해당 가상 서비스에 오류가 표시되어 외부 IP를 사용할 수 없습니다.

풀에 서버가 없는 경우 가상 서비스가 오류를 나타내거나 빨간색으로 나타날 수 있습니다. 이 문제는 Kubernetes 게이트웨이 또는 수신 리소스가 끝점 개체를 가리키지 않는 경우 발생할 수 있습니다.

끝점을 보려면 `kubectl get endpoints -n <service_namespace>` 명령을 실행하고 선택기 레이블 문제를 해결합니다.

상태 모니터에 풀 서버의 상태가 빨간색으로 표시되면 풀이 오류 상태로 나타날 수 있습니다.

이 문제를 해결하려면 다음 단계 중 하나를 수행하십시오.

- 풀 서버 또는 Kubernetes 포드가 구성된 포트에서 수신 대기 중인지 확인합니다.
- NSX DFW 방화벽에 서비스 엔진의 수신 또는 송신 트래픽을 차단하는 삭제 규칙이 없는지 확인합니다.
- Kubernetes 환경에 서비스 엔진의 수신 또는 송신 트래픽을 차단하는 네트워크 정책이 없는지 확인합니다.

서비스 엔진 문제에는 다음이 포함됩니다.

1 서비스 엔진 생성이 실패합니다.

서비스 엔진 생성은 다음과 같은 이유로 인해 실패할 수 있습니다.

- 리소스가 부족한 라이선스가 NSX Advanced Load Balancer Controller에서 사용됩니다.
- 서비스 엔진 그룹에서 생성된 서비스 엔진 수가 최대 제한에 도달했습니다.
- 서비스 엔진 데이터 NIC가 IP를 획득하지 못했습니다.

2 서비스 엔진 생성이 실패하고 `Insufficient licensable resources available` 오류 메시지가 표시됩니다.

이 오류는 리소스가 부족한 라이선스를 사용하여 서비스 엔진을 생성한 경우에 발생합니다.

리소스 할당량이 더 큰 라이선스를 가져와서 NSX Advanced Load Balancer Controller에 할당하십시오.

3 서비스 엔진 생성이 실패하고 `Reached configuration maximum limit` 오류 메시지가 표시됩니다.

이 오류는 서비스 엔진 그룹에서 생성된 서비스 엔진 수가 최대 제한에 도달한 경우에 발생합니다.

이 오류를 해결하려면 다음 단계를 수행하십시오.

- a NSX Advanced Load Balancer Controller 대시보드에서 **인프라 > 클라우드 리소스 > 서비스 엔진 그룹**을 선택합니다.
- b IP 트래픽 장애가 발생한 감독자와 이름이 동일한 서비스 엔진 그룹을 찾아 **편집** 아이콘을 클릭합니다.
- c **서비스 엔진 수**에 더 높은 값을 구성합니다.

4 서비스 엔진 데이터 NIC가 IP를 획득하지 못했습니다.

이 오류는 DHCP IP 풀이 다음 이유 중 하나로 인해 고갈된 경우 발생할 수 있습니다.

- 대규모 배포를 위해 너무 많은 서비스 엔진이 생성되었습니다.
- 서비스 엔진을 NSX Advanced Load Balancer UI 또는 vSphere Client에서 직접 삭제한 경우, 이렇게 삭제하면 DHCP 풀에서 DHCP 주소가 해제되지 않아서 리스 할당 실패가 발생합니다.

외부 IP가 잘못 할당됨

이 오류는 서로 다른 네임스페이스에 있는 두 개의 수신이 동일한 호스트 이름을 공유하는 경우 발생합니다. 구성을 확인하고 서로 다른 네임스페이스에 있는 두 개의 수신에 동일한 이름이 지정되지 않는지 확인합니다.

트래픽 장애 문제 해결

NSX Advanced Load Balancer를 구성한 후 트래픽 장애가 발생합니다.

문제

LB 유형의 서비스에 대한 끝점이 다른 네임스페이스에 있는 경우 트래픽 장애가 발생할 수 있습니다.

원인

NSX Advanced Load Balancer로 구성된 vSphere IaaS control plane 환경에서, 네임스페이스에 전용 Tier-1 게이트웨이가 있고 각 Tier-1 게이트웨이에는 동일한 CIDR을 가진 서비스 엔진 세그먼트가 있습니다. NSX Advanced Load Balancer 서비스가 하나의 네임스페이스에 있고 끝점이 다른 네임스페이스에 있는 경우 트래픽 장애가 발생할 수 있습니다. 이 장애는 NSX Advanced Load Balancer가 서비스에 외부 IP를 할당하고 외부 IP에 대한 트래픽이 실패하기 때문에 발생합니다.

해결책

- ◆ North-South 트래픽을 허용하려면 NSX Advanced Load Balancer 서비스 네임스페이스의 SNAT IP로 부터의 수신을 허용하는 분산 방화벽 규칙을 생성합니다.

NSX 백업 및 복원으로 인한 문제 해결

NSX 백업 및 복원으로 인해 NSX Advanced Load Balancer에서 제공된 모든 외부 IP에 대한 트래픽 장애가 발생할 수 있습니다.

문제

NSX의 백업 및 복원을 수행하면 트래픽 장애가 발생할 수 있습니다.

원인

이런 장애는 복원 후 서비스 엔진 NIC가 다시 작동하지 않아 IP 풀이 다운된 것으로 표시되기 때문에 발생합니다.

해결책

- 1 NSX Advanced Load Balancer Controller 대시보드에서 **인프라 > 클라우드**를 선택합니다.
- 2 클라우드를 선택하고 변경하지 않고 저장하고 상태가 녹색이 될 때까지 기다립니다.

3 모든 가상 서비스를 비활성화합니다.

NSX Advanced Load Balancer Controller가 모든 서비스 엔진에서 오래된 NIC를 제거할 때까지 기다립니다.

4 모든 가상 서비스를 사용하도록 설정합니다.

가상 서비스 상태가 녹색으로 표시됩니다.

트래픽 장애가 지속되면 NSX Manager에서 정적 경로를 재구성합니다.

NSX 백업 및 복원 후 오래된 Tier-1 세그먼트

NSX 백업 및 복원으로 오래된 Tier-1 세그먼트를 복원할 수 있습니다.

문제

NSX 백업 및 복원 절차 후에 서비스 엔진 NIC가 있는 오래된 Tier-1 세그먼트가 정리되지 않습니다.

원인

NSX 백업 후 네임스페이스가 삭제되면 복원 작업에서 NSX Advanced Load Balancer Controller 서비스 엔진 NIC와 연결된 오래된 Tier-1 세그먼트를 복원합니다.

해결책

- 1 NSX Manager에 로그인합니다.
- 2 **네트워킹 > 세그먼트**를 선택합니다.
- 3 삭제된 네임스페이스와 연결된 오래된 세그먼트를 찾습니다.
- 4 **포트/인터페이스** 섹션에서 오래된 서비스 엔진 NIC를 삭제합니다.

호스트 전송 노드 트래픽에 필요한 VDS

vSphere IaaS control plane에는 호스트 전송 노드 트래픽에 대해 vSphere 8.0 VDS(가상 Distributed Switch)를 사용해야 합니다. vSphere IaaS control plane에서는 호스트 전송 노드 트래픽에 대해 N-VDS(NSX VDS)를 사용할 수 없습니다.

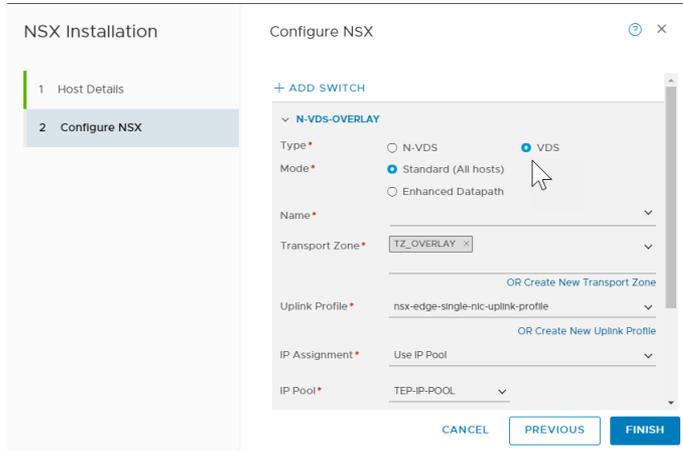
VDS가 필요함

vSphere IaaS control plane에는 동일한 VDS에서 vSphere 트래픽과 NSX 트래픽을 모두 지원하는 Converged VDS가 필요합니다. vSphere 및 NSX의 이전 릴리스에는 vSphere 트래픽을 위한 VDS(또는 VSS) 하나와 NSX 트래픽을 위한 N-VDS 하나가 있습니다. 이 구성은 vSphere IaaS control plane에서 지원되지 않습니다. N-VDS를 사용하여 워크로드 관리를 사용하도록 설정하려고 하면 시스템에서 vCenter 클러스터가 호환되지 않는 것으로 보고합니다. 자세한 내용은 [워크로드 관리 사용 설정 클러스터 호환성 오류 문제 해결의](#) 내용을 참조하십시오.

Converged VDS를 사용하려면 vCenter를 사용하여 vSphere 8.0 vDS를 생성하고 NSX에서 ESXi 호스트를 전송 노드로 준비할 때 이 VDS를 지정합니다. vCenter 측에 VDS-DSwitch를 포함하는 것만으로는 충분하지 않습니다. VDS-DSwitch 8.0은 **전송 노드 프로파일 생성** 항목에 설명되고 아래에 표시된 대로 NSX 전송 노드 프로파일로 구성해야 합니다.

ESXi 호스트를 전송 노드로 준비하는 방법에 대한 자세한 내용은 NSX 설명서에서 <https://kb.vmware.com/s/article/95820> 및 **ESXi 호스트를 전송 노드로 준비**를 참조하십시오.

그림 15-1. NSX의 VDS 구성



이전 버전에서 vSphere 8.0 및 NSX 4.x로 업그레이드한 경우에는 각 ESXi 전송 노드에서 N-VDS를 제거하고 각 호스트를 VDS로 재구성해야 합니다. 지침을 보려면 VMware 글로벌 지원 서비스에 문의하십시오.

vSphere IaaS control plane 문제 해결

16

다음과 같은 문제 해결 기법 및 모범 사례를 vSphere IaaS control plane의 인프라에 대해 사용할 수 있습니다.

다음으로 아래 항목을 읽으십시오.

- 스토리지 모범 사례 및 문제 해결
- 네트워크 토폴로지 업그레이드 문제 해결
- vSphere IaaS control plane 워크로드 도메인 종료 및 시작
- 감독자를 위한 지원 번들 수집

스토리지 모범 사례 및 문제 해결

vSphere IaaS control plane의 스토리지 환경에 대해 다음과 같은 모범 사례 및 문제 해결 방법을 사용할 수 있습니다.

vSAN이 아닌 데이터스토어에서 제어부 VM에 대한 반선호도 규칙 사용

클러스터에서 vSAN 이외의 데이터스토어를 vSphere IaaS control plane와 함께 사용하는 경우 가용성을 위해 서로 다른 데이터스토어에 3개의 제어부 VM을 배치합니다.

제어부 VM은 시스템에서 관리되므로 수동으로 마이그레이션할 수 없습니다. 데이터스토어 클러스터와 Storage DRS의 조합을 사용하여 제어부 VM을 재조정하고 별도의 데이터스토어에 배치합니다.

절차

- 1 vSphere Client에서 데이터스토어 클러스터를 생성합니다.
 - a 데이터 센터로 이동합니다.
 - b 데이터 센터 개체를 마우스 오른쪽 버튼으로 클릭하고 **새 데이터스토어 클러스터**를 선택합니다.
 - c 데이터스토어 클러스터의 이름을 지정하고 **Storage DRS 설정**을 사용하도록 설정했는지 확인합니다.
 - d 클러스터 자동화 수준을 **자동화 안 함(수동 모드)**으로 설정합니다.
 - e Storage DRS 런타임 설정을 기본값으로 둡니다.
 - f vSphere IaaS control plane와 함께 사용하도록 설정된 ESXi 클러스터를 선택합니다.

- g 데이터스토어 클러스터에 추가할 모든 공유 데이터스토어를 선택합니다.
 - h **마침**을 클릭합니다.
- 2 제어부 VM에 대한 Storage DRS 규칙을 정의합니다.
- a 데이터스토어 클러스터로 이동합니다.
 - b **구성** 탭을 클릭하고 **구성**에서 **규칙**을 클릭합니다.
 - c **추가** 아이콘을 클릭하고 규칙의 이름을 입력합니다.
 - d **규칙 사용**을 사용하도록 설정했는지 확인합니다.
 - e **규칙 유형**을 **VM 반선호도**로 설정합니다.
 - f **추가** 아이콘을 클릭하고 감독자 제어부 VM 3개를 선택합니다.
 - g **확인**을 클릭하여 구성을 마침니다.
- 3 VM 재정의 생성합니다.
- a 데이터스토어 클러스터로 이동합니다.
 - b **구성** 탭을 클릭하고 **구성**에서 **VM 재정의**를 클릭합니다.
 - c **추가** 아이콘을 클릭하고 제어부 VM 3개를 선택합니다.
 - d Storage DRS 자동화 수준을 사용하도록 설정하려면 **재정의 확인란**을 선택하고 값을 **완전히 자동화됨**으로 설정합니다.
 - e **마침**을 클릭합니다.

결과

이 작업은 제어부 VM에 대해서만 Storage DRS를 사용하도록 설정하고 VM이 서로 다른 데이터스토어에 있도록 재조정합니다.

Storage vMotion이 사용되면 SDRS 규칙 및 재정의 제거하고, Storage DRS를 사용하지 않도록 설정하고, 데이터스토어 클러스터를 제거할 수 있습니다.

vSphere에서 제거된 스토리지 정책이 계속 Kubernetes 스토리지 클래스로 표시됨

vSphere Client를 사용하여 VMware vCenter 또는 감독자의 네임스페이스에서 스토리지 정책을 제거할 경우 일치하는 스토리지 클래스는 Kubernetes 환경에 남아 있지만 사용할 수는 없습니다.

문제

`kubectl get sc` 명령을 실행하면 출력이 네임스페이스에서 사용할 수 있는 스토리지 클래스를 계속 나열합니다. 그러나 스토리지 클래스는 사용할 수 없습니다. 예를 들어 새 영구 볼륨 할당에 대해 스토리지 클래스를 사용하는 시도가 실패합니다.

스토리지 클래스가 Kubernetes 배포에서 이미 사용되고 있는 경우 배포가 예기치 않게 동작할 수 있습니다.

해결책

- 1 네임스페이스에 있는 스토리지 클래스를 확인하려면
`kubectl describe namespace namespace_name` 명령을 실행합니다.
 일치하는 스토리지 정책이 제거된 경우 이 명령의 출력은 스토리지 클래스를 나열하지 않습니다.
- 2 스토리지 클래스가 배포에서 이미 사용되고 있는 경우 스토리지 클래스를 복원합니다.
 - a vSphere Client를 사용하여 제거한 정책과 동일한 이름의 새 스토리지 정책을 생성합니다.
 예를 들어 *Gold* 정책을 삭제한 경우 새 정책의 이름을 *Gold*로 지정합니다. "vSphere IaaS 제어부 설치 및 구성" 에서 [vSphere with Tanzu에 대한 스토리지 정책 생성](#)을 참조하십시오.
 - b 네임스페이스에 정책을 할당합니다.
 "vSphere IaaS 제어부 서비스 및 워크로드" 에서 [네임스페이스의 스토리지 설정 변경](#)을 참조하십시오.
 네임스페이스에 정책을 할당한 후 vSphere IaaS control plane는 이전 스토리지 클래스를 삭제하고 동일한 이름의 일치하는 스토리지 클래스를 생성합니다.

vSAN Direct에서 외부 스토리지 사용

vSphere IaaS control plane 환경에서 vSAN Direct를 사용하는 경우 외부 공유 스토리지를 사용하여 관리 내부 VM 및 기타 메타데이터를 저장할 수 있습니다.

문제

동종 vSAN Direct 클러스터를 배포할 때는 클러스터의 각 ESXi 호스트에 복제된 vSAN 데이터스토어를 생성하여 감독자 제어부 VM 및 기타 메타데이터를 저장해야 합니다. vSAN 데이터스토어는 공간을 사용하고 각 호스트에 추가 I/O 컨트롤러가 필요하며 vSAN Direct를 지원할 수 있는 하드웨어 구성을 제한합니다.

vSAN 데이터스토어를 구성하는 대신, 외부 공유 스토리지를 사용하여 관리 내부 VM 및 기타 메타데이터를 저장할 수 있습니다.

해결책

- 1 vSAN 또는 vSAN Direct가 클러스터의 ESXi 호스트에 배포된 경우 구성에서 호스트를 지웁니다.
 - a vSAN 또는 vSAN Direct에 할당된 디스크를 제거합니다. "VMware vSAN 관리" 의 [vSAN에서 디스크 그룹 또는 디바이스 제거](#)를 참조하십시오.
 - b (선택 사항) 스크립트를 사용하여 vSAN Direct용 호스트의 디스크에 태그를 지정합니다. [스크립트를 사용하여 vSAN Direct용 스토리지 디바이스 태그 지정](#)을 참조하십시오.
- 2 VMware Cloud Foundation을 사용하여 외부 스토리지가 있는 워크로드 도메인을 생성합니다.
 NFS, vVols 또는 파이버 채널과 같은 스토리지 옵션 중 하나를 선택해야 합니다. 이러한 옵션 중 하나만 선택할 수 있습니다.
 자세한 내용은 [VMware Cloud Foundation 설명서](#)에서 "워크로드 도메인 작업" 을 참조하십시오.
 이 단계에서는 vCenter Server 및 지정된 ESXi 호스트가 있는 워크로드 도메인을 배포합니다. 외부 스토리지는 모든 호스트에 마운트되고 기본 클러스터에 추가됩니다.

3 vSAN을 사용하도록 설정합니다.

vSAN에 대해 할당된 디스크가 없는지 확인합니다.

자세한 내용은 "VMware vSAN 관리" 의 [기존 클러스터에서 vSAN 사용](#)을 참조하십시오.

이 단계에서는 vSAN 네트워크와 함께 O바이트 vSAN 데이터스토어를 생성합니다. vSAN에 로컬 디스크가 사용되지 않습니다.

4 vSAN Direct용 호스트에 로컬 디스크를 할당합니다.

자세한 내용은 "vSphere IaaS 제어부 서비스 및 워크로드" 에서 [vSAN Direct 데이터스토어 생성](#)을 참조하십시오.

할당하는 각 디바이스에 대해 vSAN Direct는 별도의 데이터스토어를 생성합니다.

5 vSAN Direct에 대한 스토리지 정책을 생성합니다.

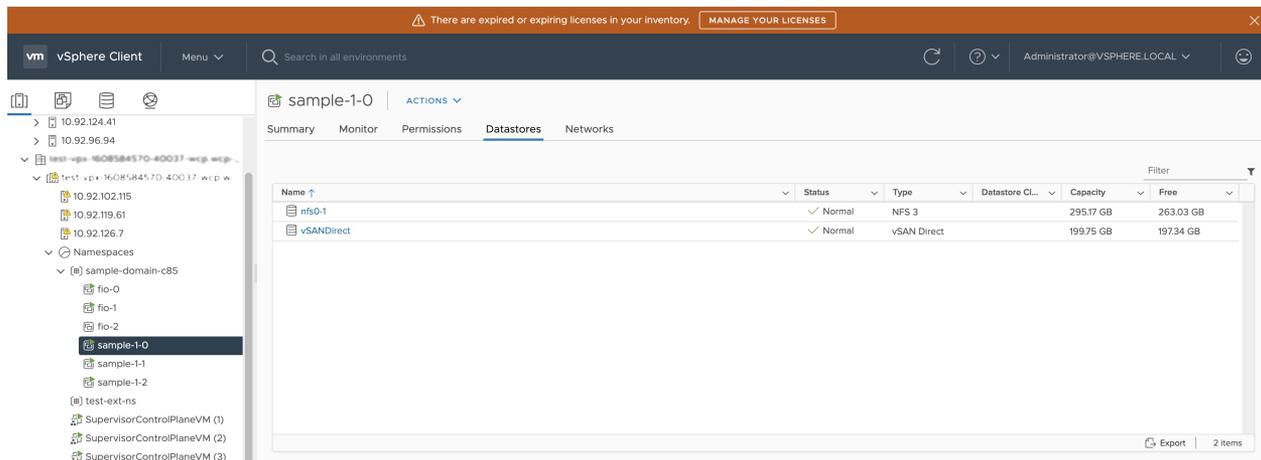
자세한 내용은 "vSphere IaaS 제어부 서비스 및 워크로드" 에서 [vSAN Direct 스토리지 정책 생성](#)을 참조하십시오.

6 감독자를 사용하도록 설정합니다.

자세한 내용은 "vSphere IaaS 제어부 설치 및 구성" 설명서를 참조하십시오.

예

이 예에서는 설정에 외부 NFS 스토리지와 vSAN Direct 데이터스토어가 포함됩니다. 제어부 VM 및 vSphere 포드는 외부 NFS 스토리지에서 실행되고 있습니다. 영구 볼륨 클레임은 vSAN Direct에서 실행됩니다.



네트워크 토폴로지 업그레이드 문제 해결

vSphere IaaS control plane 버전 7.0 업데이트 1c를 설치하거나 감독자를 버전 7.0 업데이트 1에서 버전 7.0 업데이트 1c로 업그레이드하는 경우 네트워킹 토폴로지는 단일 Tier-1 게이트웨이 토폴로지에서 감독자 내의 각 네임스페이스에 대한 Tier-1 게이트웨이가 있는 토폴로지로 업그레이드됩니다.

업그레이드 중에 발생할 수 있는 문제를 해결할 수 있습니다.

Edge 로드 밸런서 용량이 부족하여 업그레이드 사전 검사가 실패함

업그레이드 사전 검사가 실패하고 로드 밸런서 용량이 부족함을 나타내는 오류 메시지가 표시됩니다.

문제

업그레이드 사전 검사 프로세스가 실패하고 로드 밸런서 용량이 감독자에 필요한 용량 보다 적다는 오류 메시지가 표시됩니다.

해결책

이 문제를 해결하려면 다음 단계 중 하나를 수행하십시오.

- 오류 메시지에서 **강제 업그레이드** 버튼을 클릭하거나 vCenter Server 명령줄을 `--ignore-precheck-warnings true` 플래그와 함께 사용하여 강제로 업그레이드합니다.

참고 이 솔루션은 Edge 클러스터가 기존 네임스페이스 워크로드를 지원할 수 있는 경우에만 권장됩니다. 그렇지 않으면 업그레이드 중에 해당 워크로드를 건너뛸 수 있습니다.

- 사용되지 않는 워크로드를 삭제합니다.
- 클러스터에 Edge 노드를 더 추가합니다.

업그레이드 중에 감독자 워크로드 네임스페이스를 건너뛸

감독자 업그레이드 중에 일부 네임스페이스 워크로드가 업그레이드되지 않습니다.

문제

감독자 업그레이드는 성공하지만 업그레이드 중에 일부 네임스페이스 워크로드를 건너뛸니다. Kubernetes 리소스는 리소스가 부족하고 새로 생성된 Tier-1 게이트웨이가 `ERROR` 상태를 나타냅니다.

원인

로드 밸런서 용량이 부족하여 워크로드를 지원할 수 없습니다.

해결책

이 문제를 해결하려면 다음 단계 중 하나를 수행하십시오.

- 사용되지 않는 워크로드를 삭제하고 NCP를 다시 시작한 후 업그레이드를 다시 실행합니다.
- 클러스터에 Edge 노드를 더 추가하고 Tier-1 게이트웨이에 대한 재할당을 트리거합니다. NCP를 다시 시작하고 업그레이드를 다시 실행합니다.

업그레이드하는 동안 로드 밸런서 서비스를 건너뛸

감독자를 업그레이드하는 동안 일부 로드 밸런서 서비스가 업그레이드되지 않습니다.

문제

감독자 업그레이드는 성공하지만 업그레이드 중에 일부 Kubernetes 로드 밸런서 서비스를 건너뛸니다.

원인

감독자 워크로드 및 연결된 Tanzu Kubernetes 클러스터의 Kubernetes 로드 밸런서 유형 서비스 수가 NSX Edge 가상 서버 제한을 초과합니다.

해결책

사용되지 않는 워크로드를 삭제하고 NCP를 다시 시작한 후 업그레이드를 다시 실행합니다.

vSphere IaaS control plane 워크로드 도메인 종료 및 시작

데이터 손실을 방지하고 vSphere IaaS control plane 환경의 구성 요소 및 워크로드를 작동 상태로 유지하려면 구성 요소를 종료하거나 시작할 때 지정된 순서를 따라야 합니다.

일반적으로 종료 및 시작 작업은 패치를 적용하거나, 업그레이드하거나, vSphere IaaS control plane 환경을 복원한 후에 수행합니다.

Tanzu Kubernetes Grid에서 프로비저닝된 Tanzu Kubernetes 클러스터를 포함한 vSphere IaaS control plane 솔루션은 vSphere SDDC(소프트웨어 정의 데이터 센터)의 일부입니다. 따라서 vSphere IaaS control plane 환경의 종료 및 시작을 수행할 때는 전체 vSphere 인프라 스택을 고려해야 합니다. vSphere IaaS control plane를 포함한 vSphere SDDC의 종료 및 시작에 대해 검증된 다음과 같은 일련의 절차를 참조하십시오.

- vSphere IaaS control plane를 포함한 vSphere SDDC [종료 절차](#)
- vSphere IaaS control plane를 포함한 vSphere SDDC [시작 절차](#)

감독자를 위한 지원 번들 수집

감독자를 위한 지원 번들을 수집하는 방법을 알아봅니다. 감독자가 오류 또는 구성 상태인 경우에도 지원 번들을 수집할 수 있습니다.

사전 요구 사항

- 사용자 계정에 **Global.Diagnostics** 권한이 있어야 합니다.

절차

- 1 vSphere Client를 사용하여 vSphere IaaS control plane 환경에 로그인합니다.
- 2 **메뉴 > 워크로드 관리**를 선택합니다.
- 3 **감독자** 탭을 선택합니다.
- 4 대상 감독자를 선택합니다.
- 5 **로그 내보내기**를 클릭합니다.

결과

지원 번들을 수집한 후에는 KB 문서: 보안 FTP 포털을 통해 VMware에 대한 진단 정보 업로드(<http://kb.vmware.com/kb/2069559>)를 참조하십시오.