vSpere IaaS 제어부 개념 및 계획

업데이트 3
VMware vSphere 8.0
VMware vCenter 8.0
VMware ESXi 8.0

vmware
by Broadcom

VMware by Broadcom 웹 사이트

https://docs.vmware.com/kr에서 최신 기술 문서를 찾을 수 있습니다.

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

목차

"vSphere IaaS 제어부 개념 및 계획"

"vSphere IaaS 제어부 개념 및 계획" 가이드에서는 vSphere IaaS control plane(이전 명칭이: vSphere with Tanzu) 주요 개념과 아키텍처, 그리고 vSphere 클러스터에서 vSphere IaaS control plane을 사용하도록 설정하고 Tanzu Kubernetes Grid 클러스터, vSphere 포드 및 VM 서비스를 사용하여 생성된 VM의 워크로드를 실행할 수 있도록 vSphere 환경이 충족해야 하는 요구 사항에 대한 정보를 제공합니다.

대상 사용자

이 정보는 vSphere에서 vSphere IaaS control plane를 사용하도록 설정하기 위한 요구 사항과 플랫폼의 주요 개념 및 아키텍처를 숙지하려는 vSphere 관리자 및 DevOps 엔지니어를 대상으로 합니다.

업데이트된 정보

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

이 표에는 "vSphere IaaS 제어부 개념 및 계획" 의 업데이트 기록이 나와 있습니다.

개정	설명
2024년 4월 18일	새 솔루션 라이센스에 대한 라이센싱 정보가 업데이트되었습니다. vSphere IaaS control plane에 대한 라이센싱의 내용을 참조하십시오.
2024년 2월 29일	클라우드에 대한 컨텐츠가 추가되었습니다. NSX Advanced Load Balancer 구성 요소의 내용을 참조하십시오.
2024년 2월 7일	감독자 네트워킹에서 링크가 업데이트되었습니다.
2023년 12월 13일	vSphere 클러스터에 참여하는 모든 ESXi 호스트를 NSX 전송 노드로 준비하는 방법에 대한 참고 사항으로 NSX 요구 사항이 업데이트되었습니다. NSX가 있는 영역 감독자 요구 사항 및 NSX를 사용한 클러스터 감독자 배포 요구 사항의 내용을 참조하십시오.
2023년 9월 29일	HAProxy 배포를 위한 로드 밸런서 요구 사항이 업데이트되었습니다. HAProxy 로드 밸런서가 있는 영역 감독자 배포 요구 사항 및 VDS 네트워킹 및 HAProxy 로드 밸런서를 사용한 클러스터 감독자 배포 요구 사항 항목을 참조하십시오.
2023년 9월 21일	NSX 및 NSX Advanced Load Balancer를 사용한 감독자 네트워킹에 대한 컨텐츠가 추가되었습니다. vSphere IaaS control plane 사용자 역할 및 워크플로 및 감독자 네트워킹의 내용을 참조하십시오.
2023년 8월 3일	부분적 개정.
2023년 6월 30일	■ 물리적 사이트 간 vSphere 영역 분포에 대한 설명이 추가되었습니다. 감독자 영역 및 클러스터 배포
22023년 6월 9일	■ vSphere IaaS control plane 보안에 다음 설명이 추가되었습니다. 각 Tanzu Kubernetes Grid 클러스터의 제어부에 설치된 데이터베이스(etcd)의 데이터에 동일한 암호화 모델이 적용됩니다. ■ Storage vMotion이 영구 볼륨에서 지원되지 않는다는 설명이 추가되었습니다. 감독자가 vSphere 스토리지와 통합되는 방식 및 Tanzu Kubernetes Grid 클러스터용 스토리지의 내용을 참조하십시오. ■ 장 5 영역 감독자배포 요구 사항 및 장 6 클러스터 감독자 배포 요구 사항에 모범 사례로 관리 도메인과 워크로드 도메인을 분리하기 위한 권장 사항이 추가되었습니다.
2023년 6월 2일	■ NSX 참조 설계 가이드에 대한 링크가 추가되었습니다. NSX가 있는 영역 감독자 요구 사항 및 NSX를 사용한 클러스터 감독자 배포 요구 사항의 내용을 참조하십시오. ■ 부분적 업데이트.
2023년 5월 30일	■ NSX 배포에 대한 GENEVE 캡슐화 지원 요구 사항이 추가되었습니다. NSX가 있는 영역 감독자 요구 사항 및 NSX를 사용한 클러스터 감독자 배포 요구 사항을 참조하십시오. ■ 부분적 업데이트.
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 영역 감독자배포 요구 사항의 내용을 참조하십시오.

개정	설명
2023년 5월 9일	■ vSphere 네임스페이스란?에 대한 별도의 항목이 추가되었습니다. ■ vSphere IaaS control plane ID 및 액세스 관리에 대한 내용이 업데이트되었습니다. ■ vSphere 포드는 NSX 네트워킹 스택에서만 지원된다는 참고 사항이 추가되었습니다. vSphere 포드란?의 내용을 참조하십시오.
2023년 5월 1일	부분적 개정.
2023년 4월 18일	vSphere 8 업데이트 1 릴리스에 대한 일반 업데이트.

vSphere IaaS control plane 개념

1

vSphere IaaS control plane을 사용하면 vSphere 클러스터를 플랫폼으로 전환하여 vSphere의 전용 리소스 풀에서 Kubernetes 워크로드를 실행할 수 있습니다. vSphere 클러스터에서 vSphere IaaS control plane가 사용되도록 설정되면 하이퍼바이저 계층에 Kubernetes 제어부가 생성됩니다. 그러면 vSphere 포드를 배포하여 Kubernetes 컨테이너를 실행하거나 VMware Tanzu™ Kubernetes Grid™를 통해 업스트림 Kubernetes 클러스터를 생성하고 이러한 클러스터 내에서 애플리케이션을 실행할 수 있습니다.

다음으로 아래 항목을 읽으십시오.

- vSphere IaaS control plane이란?
- vSphere 네임스페이스란?
- vSphere IaaS control plane 사용자 역할 및 워크플로
- vSphere IaaS control plane이 vSphere 환경을 변경하는 방식
- vSphere IaaS control plane에 대한 라이센싱
- vSphere IaaS control plane ID 및 액세스 관리
- vSphere IaaS control plane 보안

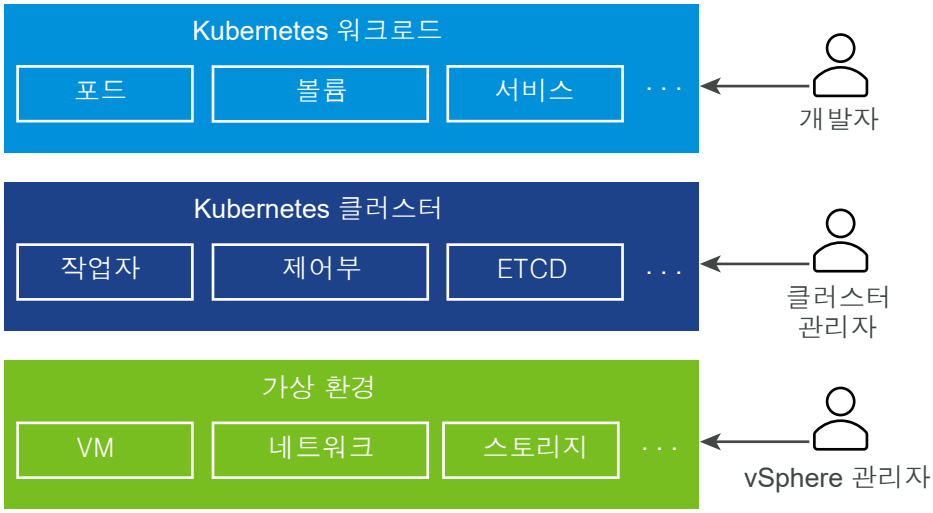
vSphere IaaS control plane이란?

vSphere IaaS control plane을 사용하여 vSphere를 하이퍼바이저 계층에서 Kubernetes 워크로드를 기본적으로 실행하는 플랫폼으로 변환할 수 있습니다. vSphere 클러스터에서 사용하도록 설정되면 vSphere IaaS control plane는 ESXi 호스트에서 직접 Kubernetes 워크로드를 실행하고 vSphere 네임스페이스라는 전용 네임스페이스 내에 업스트림 Kubernetes 클러스터를 생성하는 기능을 제공합니다.

현재 애플리케이션 스택의 과제

오늘날의 분산 시스템은 일반적으로 다수의 Kubernetes 포드 및 VM을 실행하는 여러 마이크로서비스로 구성됩니다. vSphere IaaS control plane 기반이 아닌 일반적인 스택은 VM 내부에 배포되는 Kubernetes 인프라와 이러한 VM에서 각각 실행되는 Kubernetes 포드가 있는 기본 가상 환경으로 구성됩니다. 애플리케이션 개발자, Kubernetes 클러스터 관리자 및 vSphere 관리자라는 3가지 개별 역할이 스택의 각 부분을 운영합니다.

그림 1-1. 현재 애플리케이션 스택



서로 다른 역할은 서로의 환경을 보거나 제어할 수 없습니다.

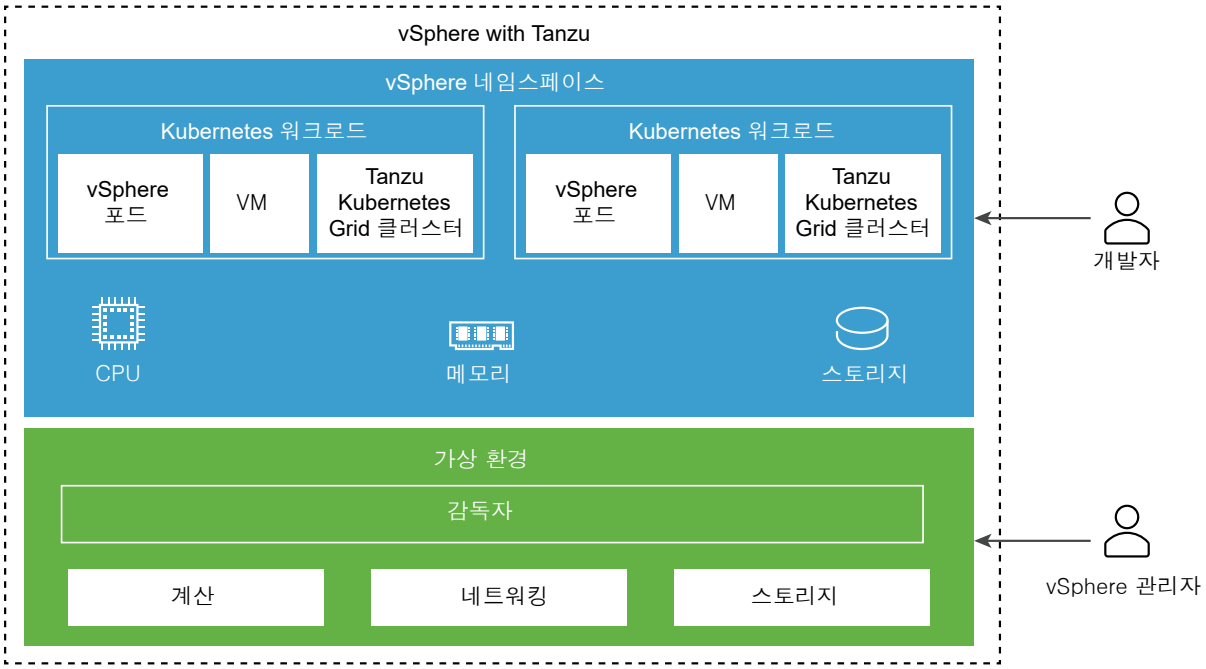
- 애플리케이션 개발자는 Kubernetes 포드를 실행하고 Kubernetes 기반 애플리케이션을 배포하고 관리할 수 있습니다. 수백 개의 애플리케이션을 실행하는 전체 스택에 대한 가시성은 없습니다.
- DevOps 엔지니어 또는 클러스터 관리자는 Kubernetes 인프라만 제어할 수 있으며, 가상 환경을 관리 또는 모니터링하고 리소스 관련 및 기타 문제를 해결하는 도구가 없습니다.
- vSphere 관리자는 기본 가상 환경을 완전히 제어할 수 있지만 Kubernetes 인프라, 가상 환경에 있는 다른 Kubernetes 개체의 배치 및 이러한 개체가 리소스를 소비하는 방식에 대한 가시성은 없습니다.

전체 스택에 대한 작업은 세 가지 역할 간에 통신이 필요하기 때문에 어려울 수 있습니다. 스택의 서로 다른 계층 간에 통합이 부족한 경우에도 문제가 발생할 수 있습니다. 예를 들어 Kubernetes 스케줄러는 vCenter Server 인벤토리에 대한 가시성을 가지고 있지 않으며 포드를 지능적으로 배치할 수 없습니다.

vSphere IaaS control plane 사용의 이점

vSphere IaaS control plane은 하이퍼바이저 계층에서 직접 Kubernetes 제어부를 생성합니다. vSphere 관리자가 vSphere IaaS control plane에 대해 기존 vSphere 클러스터를 활성화하기 때문에 클러스터의 일부인 ESXi 호스트 내에 Kubernetes 계층이 생성됩니다. vSphere IaaS control plane에 대해 활성화된 vSphere 클러스터를 감독자라고 합니다.

그림 1-2. vSphere IaaS control plane



하이퍼바이저 계층에 Kubernetes 제어부가 있으면 vSphere에서 다음과 같은 기능을 사용할 수 있습니다.

- vSphere 관리자는 감독자에서 vSphere 네임스페이스라는 네임스페이스를 생성하고 이를 지정된 양의 메모리, CPU 및 스토리지를 사용하여 구성할 수 있습니다. vSphere 네임스페이스를 DevOps 엔지니어에게 제공합니다.
- DevOps 엔지니어는 vSphere 네임스페이스 내에 공유 리소스 풀이 있는 동일한 플랫폼에서 Kubernetes 워크로드를 실행할 수 있습니다. Tanzu Kubernetes Grid를 사용하여 생성된 여러 업스트림 Kubernetes 클러스터를 배포하고 관리할 수 있습니다. vSphere 포드라는 특수한 유형의 VM 내에 있는 감독자에 Kubernetes 컨테이너를 직접 배포할 수도 있습니다. 일반 VM을 배포할 수도 있습니다.
- vSphere 관리자는 vSphere Client를 사용하여 vSphere 포드, VM 및 Tanzu Kubernetes Grid 클러스터를 관리하고 모니터링할 수 있습니다.
- vSphere 관리자는 서로 다른 네임스페이스 내에서 실행되는 vSphere 포드, VM 및 Tanzu Kubernetes Grid 클러스터, 이러한 항목의 환경 내 배치 및 리소스 소비 방식에 대한 완전한 가시성을 갖습니다.

하이퍼바이저 계층에서 Kubernetes를 실행하면 vSphere 관리자와 DevOps 팀 간의 협업이 쉬워집니다. 두 역할이 모두 동일한 개체로 작동하기 때문입니다.

워크로드란?

vSphere IaaS control plane에서 워크로드는 다음 중 한 가지 방법으로 배포되는 애플리케이션입니다.

- vSphere 포드 내에서 실행되는 컨테이너로 구성된 애플리케이션.
- VM 서비스를 통해 프로비저닝된 워크로드.

- Tanzu Kubernetes Grid를 사용하여 배포된 Tanzu Kubernetes Grid 클러스터.
- Tanzu Kubernetes Grid 클러스터 내에서 실행되는 애플리케이션.

vSphere 영역이란?

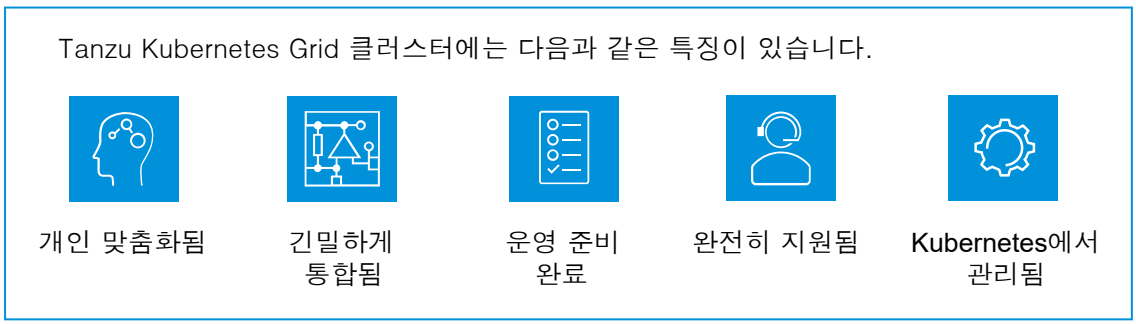
vSphere 영역은 vSphere IaaS control plane에 배포된 워크로드에 클러스터 수준 장애로부터 보호하는 고가용성을 제공합니다. vSphere 관리자는 vSphere Client에서 vSphere 영역을 생성한 다음, vSphere 클러스터를 영역에 매핑합니다. 영역을 사용하여 vSphere IaaS control plane 환경에 감독자를 배포합니다.

클러스터 수준 고가용성을 위해 세 개의 vSphere 영역에 감독자를 배포할 수 있습니다. 또는 단일 vSphere 클러스터 하나에 감독자를 배포하면 vSphere 영역이 자동으로 생성되어 클러스터에 매핑되거나, 영역에 이미 매핑된 클러스터를 사용할 수 있습니다. 자세한 내용은 감독자 아키텍처 및 감독자 영역 및 클러스터 배포 항목을 참조하십시오.

Tanzu Kubernetes Grid 클러스터란?

Tanzu Kubernetes Grid 클러스터는 VMware에서 구축, 서명 및 지원하는 Kubernetes의 전체 배포입니다. Tanzu Kubernetes Grid를 사용하여 감독자에서 업스트림 Tanzu Kubernetes Grid 클러스터를 프로비저닝하고 운영할 수 있습니다.

Tanzu Kubernetes Grid에서 프로비저닝된 Tanzu Kubernetes Grid 클러스터에는 다음과 같은 특성이 있습니다.



- Kubernetes의 개인 맞춤화된 설치. Tanzu Kubernetes Grid는 Tanzu Kubernetes Grid 클러스터 프로비저닝을 위해 vSphere에 최적화된 기본값을 제공합니다. Tanzu Kubernetes Grid를 사용하면 일반적으로 엔터프라이즈급 Kubernetes 클러스터를 배포하고 실행하는 데 필요한 시간과 노력을 줄일 수 있습니다.
- vSphere 인프라와 통합. Tanzu Kubernetes Grid 클러스터는 스토리지, 네트워킹 및 인증을 포함하여 vSphere SDDC 스택과 통합됩니다. 또한 Tanzu Kubernetes Grid 클러스터는 vSphere 클러스터에 매핑되는 감독자에 구축됩니다. 긴밀하게 통합되어 있기 때문에 Tanzu Kubernetes Grid 클러스터 실행에는 일관적인 제품 경험이 가능합니다.
- 즉시 사용 가능. Tanzu Kubernetes Grid는 운영 준비가 된 Tanzu Kubernetes Grid 클러스터를 프로비저닝합니다. 추가 구성을 수행하지 않아도 운영 워크로드를 실행할 수 있습니다. 또한 가용성을 보장하고 Kubernetes 소프트웨어 업그레이드 롤링을 허용하고 서로 다른 버전의 Kubernetes를 별도의 클러스터에 실행할 수 있습니다.

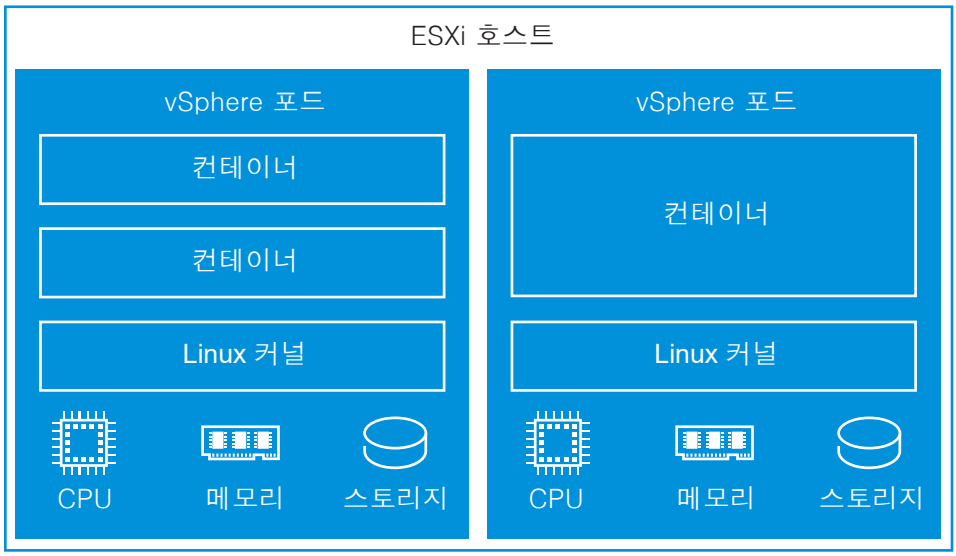
- Kubernetes 워크로드를 위한 고가용성. 3개의 vSphere 영역 감독자에 배포된 Tanzu Kubernetes Grid 클러스터는 vSphere 클러스터 수준에서 발생하는 장애로부터 보호됩니다. Tanzu Kubernetes Grid 클러스터의 워크로드 및 제어부 노드는 세 개의 vSphere 영역 모두에 분산되므로 내부에서 실행되는 Kubernetes 워크로드의 가용성을 높일 수 있습니다. 1영역 감독자에서 실행되는 Tanzu Kubernetes Grid 클러스터는 vSphere HA를 통해 ESXi 호스트 수준에서 발생하는 장애로부터 보호됩니다.
- VMware에서 완전히 지원함. Tanzu Kubernetes Grid 클러스터는 VMware의 오픈 소스 Linux 기반을 사용하며 vSphere 인프라에 배포되고 ESXi 호스트에서 실행됩니다. 하이퍼바이저에서 Kubernetes 클러스터에 이르기까지 스택의 계층에 문제가 발생하는 경우 VMware에 문의하면 그 해답을 찾을 수 있습니다.
- Kubernetes에서 관리됨. Tanzu Kubernetes Grid 클러스터는 자체적으로 Kubernetes 클러스터인 감독자 위에 구축됩니다. Tanzu Kubernetes Grid 클러스터는 사용자 지정 리소스를 사용하여 vSphere 네임스페이스에 정의됩니다. 익숙한 kubectl 명령 및 Tanzu CLI를 사용하여 셀프 서비스 방식으로 Tanzu Kubernetes Grid 클러스터를 프로비저닝합니다. 도구체인 간에는 일관성이 있습니다. 클러스터를 프로비저닝하든 워크로드를 배포하든 동일한 명령, 익숙한 YAML 및 공통 워크플로를 사용합니다.

자세한 정보는 장 3 Tanzu Kubernetes Grid 아키텍처 및 구성 요소 및 "vSphere IaaS 제어부에서 TKG 서비스 사용" 의 내용을 참조하십시오.

vSphere 포드란?

vSphere IaaS control plane에는 Kubernetes 포드와 동일한 vSphere 포드라는 구조가 도입되었습니다. vSphere 포드는 하나 이상의 Linux 컨테이너를 실행하는 설치 공간이 작은 VM입니다. 각 vSphere 포드는 수용하는 워크로드 맞게 크기가 정확하게 조정되며 해당 워크로드에 대한 명시적 리소스 예약이 있습니다. 워크로드를 실행하는 데 필요한 정확한 양의 스토리지, 메모리 및 CPU 리소스를 할당합니다. vSphere 포드는 NSX를 사용하여 네트워킹 스택으로 구성된 감독자에서만 지원됩니다.

그림 1-3. vSphere 포드

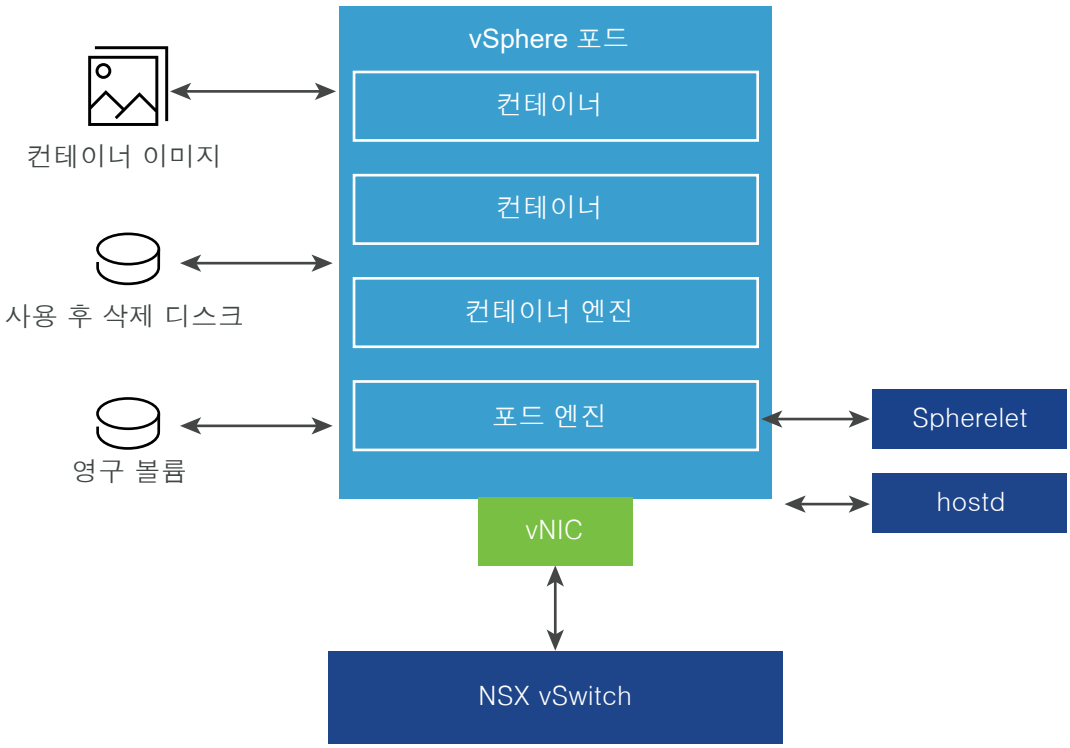


vSphere 포드는 vCenter Server의 개체이며 워크로드에 대해 다음 기능을 사용할 수 있습니다.

- 강력한 격리. vSphere 포드는 가상 시스템과 동일한 방식으로 격리됩니다. 각 vSphere 포드에는 Photon OS에 사용되는 커널을 기반으로 하는 고유한 Linux 커널이 있습니다. vSphere 포드에서는 베어메탈 구성처럼 많은 컨테이너가 커널을 공유하는 것이 아니라, 각 컨테이너에 고유한 Linux 커널이 있습니다.
- 리소스 관리. vSphere DRS는 감독자에서 vSphere 포드의 배치를 처리합니다.
- 고성능. vSphere 포드는 VM과 동일한 수준의 리소스 격리를 제공하며, 빠른 시작 시간과 낮은 컨테이너 오버헤드를 유지하면서 방해가 되는 인접 네트워크 문제를 제거합니다.
- 진단. vSphere 관리자는 vSphere에서 워크로드에 제공되는 모든 모니터링 및 검사 도구를 사용할 수 있습니다.

vSphere 포드는 OCI(Open Container Initiative)와 호환되며, 컨테이너가 OCI와 호환되는 한 모든 운영 체제에서 컨테이너를 실행할 수 있습니다.

그림 1-4. vSphere 포드 네트워킹 및 스토리지



vSphere 포드는 저장된 개체에 따라, 사용 후 삭제되는 VMDK, 영구 볼륨 VMDK 및 컨테이너 이미지 VMDK라는 세 가지 유형의 스토리지를 사용합니다. vSphere 관리자는 감독자 수준에서 컨테이너 이미지 캐시 및 사용 후 삭제되는 VMDK 배치에 대한 스토리지 정책을 구성합니다. 또한 vSphere 네임스페이스 수준에서 영구 볼륨 배치에 대한 스토리지 정책을 구성합니다. 워크로드에 대한 영구 스토리지에서 vSphere IaaS control plane의 스토리지 요구 사항 및 개념에 대한 자세한 내용을 참조하십시오.

네트워킹을 위해 vSphere 포드 및 Tanzu Kubernetes Grid 클러스터의 VM은 NSX에서 제공하는 토폴로지를 사용합니다. 자세한 내용은 감독자 네트워킹 항목을 참조하십시오.

Spherelet은 각 호스트에서 생성되는 추가 프로세스입니다. kubelet은 기본적으로 ESXi로 이식되고 ESXi 호스트가 Kubernetes 클러스터의 일부가 되도록 허용합니다.

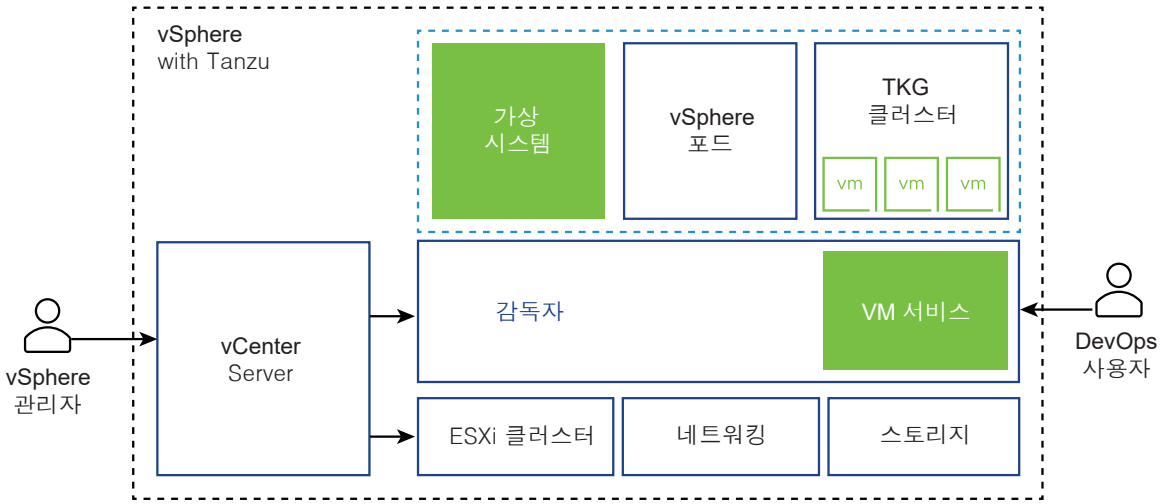
감독자에서 vSphere 포드를 사용하는 방법에 대한 자세한 내용은 "vSphere IaaS 제어부 서비스 및 워크로드" 설명서에서 vSphere 포드에 워크로드 배포를 참조하십시오.

vSphere IaaS control plane에서 가상 시스템 사용

vSphere IaaS control plane는 DevOps 엔지니어가 공통의 공유 Kubernetes 환경에서 컨테이너뿐 아니라 VM을 배포하고 실행할 수 있는 VM 서비스 기능을 제공합니다. 컨테이너와 VM 둘 다 동일한 vSphere 네임스페이스 리소스를 공유하며 단일 vSphere IaaS control plane 인터페이스를 통해 관리할 수 있습니다.

VM 서비스는 Kubernetes를 사용하지만 쉽게 컨테이너화할 수 없는 기존 VM 기반 워크로드가 있는 DevOps 팀의 요구 사항을 해결합니다. 또한 컨테이너 플랫폼과 함께 Kubernetes가 아닌 플랫폼 관리의 오버헤드를 줄이는 데에도 도움이 됩니다. Kubernetes 플랫폼에서 컨테이너와 VM을 실행하는 경우 DevOps팀은 워크로드 공간을 하나의 플랫폼으로 통합할 수 있습니다.

참고 VM 서비스는 독립형 VM 외에도 Tanzu Kubernetes Grid 클러스터를 구성하는 VM을 관리합니다. 클러스터에 대한 자세한 내용은 "vSphere IaaS 제어부에서 TKG 서비스 사용" 설명서를 참조하십시오.



VM 서비스를 통해 배포된 각 VM은 vSphere IaaS control plane 인프라를 기반으로 자체 운영 체제를 포함한 모든 구성 요소를 실행하는 완전한 시스템으로 작동합니다. VM은 감독자가 제공하는 네트워킹 및 스토리지에 액세스할 수 있으며 표준 Kubernetes `kubectl` 명령을 사용하여 관리됩니다. VM은 Kubernetes 환경에서 다른 VM 또는 워크로드의 영향을 받지 않는 완전히 분리된 시스템으로 실행됩니다.

Kubernetes 플랫폼에서 가상 시스템을 사용하는 경우

일반적으로 컨테이너 또는 VM에서 워크로드를 실행하기로 결정하는 경우는 비즈니스 요구와 목표에 따라 다릅니다. VM을 사용하는 이유 중에는 다음과 같은 경우가 있습니다.

- 애플리케이션을 컨테이너화할 수 없습니다.
- 애플리케이션이 사용자 지정 커널 또는 사용자 지정 운영 체제용으로 설계되었습니다.

- 애플리케이션이 VM에서 실행하는 데 더 적합합니다.
- 일관된 Kubernetes 환경을 유지하고 오버헤드를 방지하려고 합니다. Kubernetes가 아닌 플랫폼 및 컨테이너 플랫폼에 대해 별도의 인프라를 실행하는 대신 해당 스택을 통합하고 익숙한 `kubectl` 명령으로 관리할 있습니다.

감독자에서 독립형 가상 시스템을 배포하고 관리하는 방법에 대한 자세한 내용은 "vSphere IaaS 제어부 서비스 및 워크로드" 설명서의 가상 시스템 배포 및 관리를 참조하십시오.

vSphere IaaS control plane의 감독자 서비스

감독자 서비스는 IaaS(Infrastructure-as-a-Service) 구성 요소 및 긴밀하게 통합된 ISV(독립 소프트웨어 벤더) 서비스를 개발자에게 제공하는 vSphere 인증 Kubernetes 운영자입니다. 감독자 서비스를 Kubernetes 워크로드에서 사용할 수 있도록 vSphere IaaS control plane 환경에서 설치하고 관리할 수 있습니다. 감독자 서비스가 감독자에 설치되면 DevOps 엔지니어는 서비스 API 를 사용하여 사용자 네임스페이스의 감독자에 인스턴스를 생성할 수 있습니다. 이러한 인스턴스를 vSphere 포드 및 Tanzu Kubernetes Grid 클러스터에서 사용할 수 있습니다.

지원되는 감독자 서비스에 대해 자세한 내용 및 해당 서비스 YAML 파일을 다운로드하는 방법은 http://vmware.com/go/supervisor-service에서 참조하십시오.

감독자 서비스를 사용하는 방법에 대한 자세한 내용은 "vSphere IaaS 제어부 서비스 및 워크로드" 설명서에서 감독자 서비스 관리를 참조하십시오.

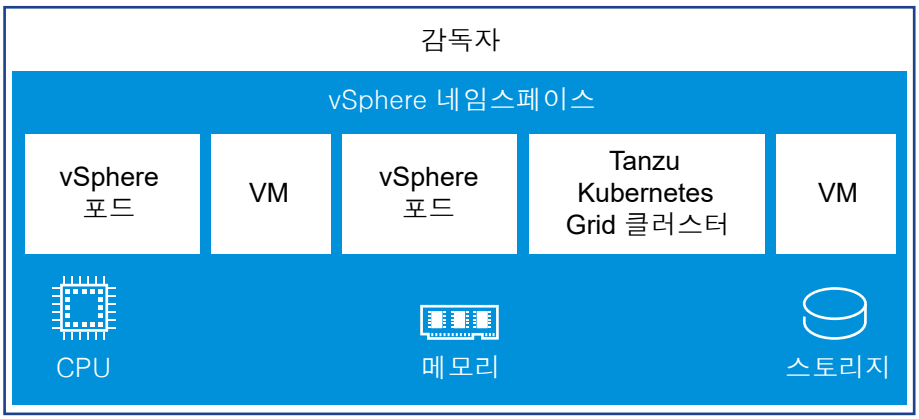
vSphere 네임스페이스란?

vSphere 네임스페이스는 vSphere 포드, VM 및 Tanzu Kubernetes Grid 클러스터가 실행될 수 있는 리소스 경계를 설정합니다. vSphere 관리자는 vSphere Client를 통해 vSphere 네임스페이스를 생성하고 구성합니다.

처음 생성되면 vSphere 네임스페이스는 감독자 내에 제한 없는 리소스가 포함됩니다. vSphere 관리자는 CPU, 메모리, 스토리지는 물론 vSphere 네임스페이스 내에서 실행할 수 있는 Kubernetes 개체의 수에 대한 제한을 설정할 수 있습니다. 스토리지 제한은 Kubernetes에서 스토리지 할당량으로 표시됩니다. 리소스 풀은 감독자의 각 vSphere 네임스페이스별로 vSphere에 생성됩니다.

vSphere 영역에서 활성화된 감독자에서 영역에 매핑된 각 vSphere 클러스터에 네임스페이스 리소스 풀이 생성됩니다. vSphere 네임스페이스는 vSphere 영역의 일부인 세 개의 vSphere 클러스터 모두에 분산됩니다. 3개 영역 감독자의 vSphere 네임스페이스에 사용되는 리소스는 기본 vSphere 클러스터 3개 모두에서 동일한 양이 사용됩니다. 예를 들어 300MHz의 CPU를 할당하면 각 vSphere 클러스터에서 100MHz가 사용됩니다.

그림 1-5. vSphere 네임스페이스



DevOps 엔지니어에게 네임스페이스에 대한 액세스를 제공하기 위해, vSphere 관리자는 vCenter Single Sign-On에 연결된 ID 소스 내에서 또는 감독자에 등록된 OIDC 제공자에서 사용 가능한 사용자나 사용자 그룹에 사용 권한을 할당합니다. 자세한 내용은 vSphere IaaS control plane ID 및 액세스 관리의 내용을 참조하십시오.

리소스 및 개체 제한은 물론 사용 권한 및 스토리지 정책으로 네임스페이스를 생성하고 구성한 후, DevOps 엔지니어가 네임스페이스에 액세스하여 Tanzu Kubernetes Grid 클러스터, vSphere 포드 및 VM 서비스를 통해 생성된 VM과 같은 워크로드를 실행할 수 있습니다.

vSphere 네임스페이스와 Kubernetes 네임스페이스의 차이점

핵심적으로 vSphere 네임스페이스는 Kubernetes 네임스페이스와 동일한 기능을 수행하지만 vSphere 네임스페이스는 vSphere IaaS control plane에만 해당됩니다. vSphere 네임스페이스를 Kubernetes 네임스페이스와 혼동해서는 안 됩니다.

vSphere 네임스페이스는 vSphere 리소스 풀에 대한 확장으로 구현되며 감독자에서 실행되는 워크로드에 리소스를 제공하는 기능을 합니다. vSphere 네임스페이스에는 Kubernetes 네임스페이스에 대한 직접 매핑이 있으며, 이를 통해 개체 및 스토리지 할당량이 워크로드에 적용됩니다.

일반 Kubernetes 네임스페이스와의 또 다른 차이점은 위에서 언급했듯이 vSphere 관리자가 vSphere 네임스페이스에 대한 사용자 액세스를 관리한다는 점입니다. vSphere 관리자는 DevOps 엔지니어가 VM을 셀프 서비스하는 데 사용할 수 있는 VM 템플릿이 포함된 컨텐츠 라이브러리와 VM 클래스를 연결할 수도 있습니다. 자세한 내용은 "vSphere IaaS 제어부 서비스 및 워크로드" 에서 가상 시스템 배포 및 관리를 참조하십시오.

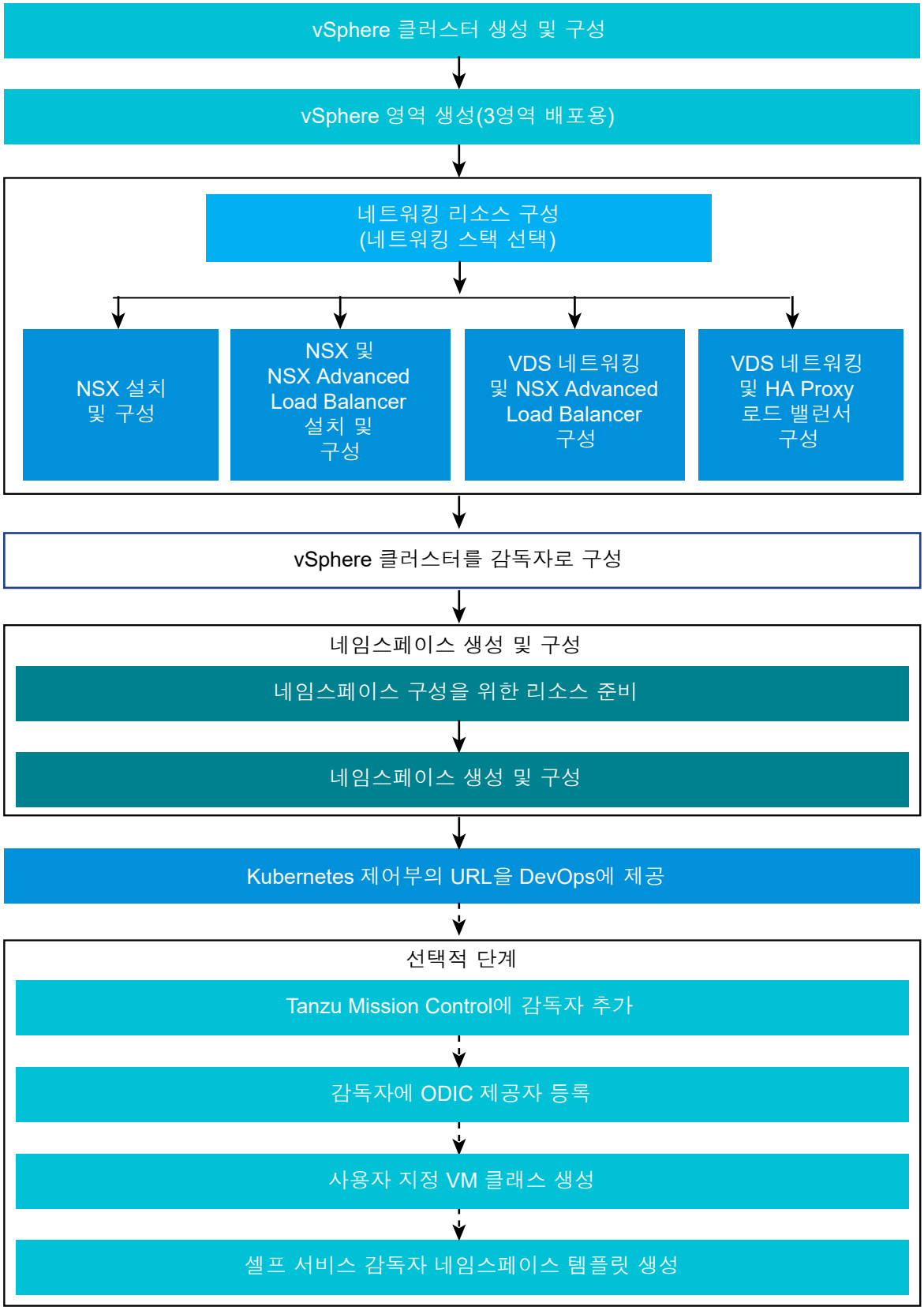
vSphere IaaS control plane 사용자 역할 및 워크플로

vSphere IaaS control plane에는 vSphere 관리자와 DevOps 엔지니어라는 두 가지 역할이 포함됩니다. DevOps 엔지니어는 DevOps, 애플리케이션 개발자 및 Kubernetes 관리자의 역할로 구성됩니다. 두 역할은 서로 다른 인터페이스를 통해 플랫폼과 상호 작용하며 vCenter Server에서 각자에 대해 정의된 사용자 또는 사용자 그룹 및 연결된 사용 권한이 있을 수 있습니다. vSphere 관리자 및 DevOps 엔지니어 역할에 대한 워크플로는 고유하며 이러한 역할에 필요한 특정 전문 기술 영역에 따라 결정됩니다.

사용자 역할 및 워크플로

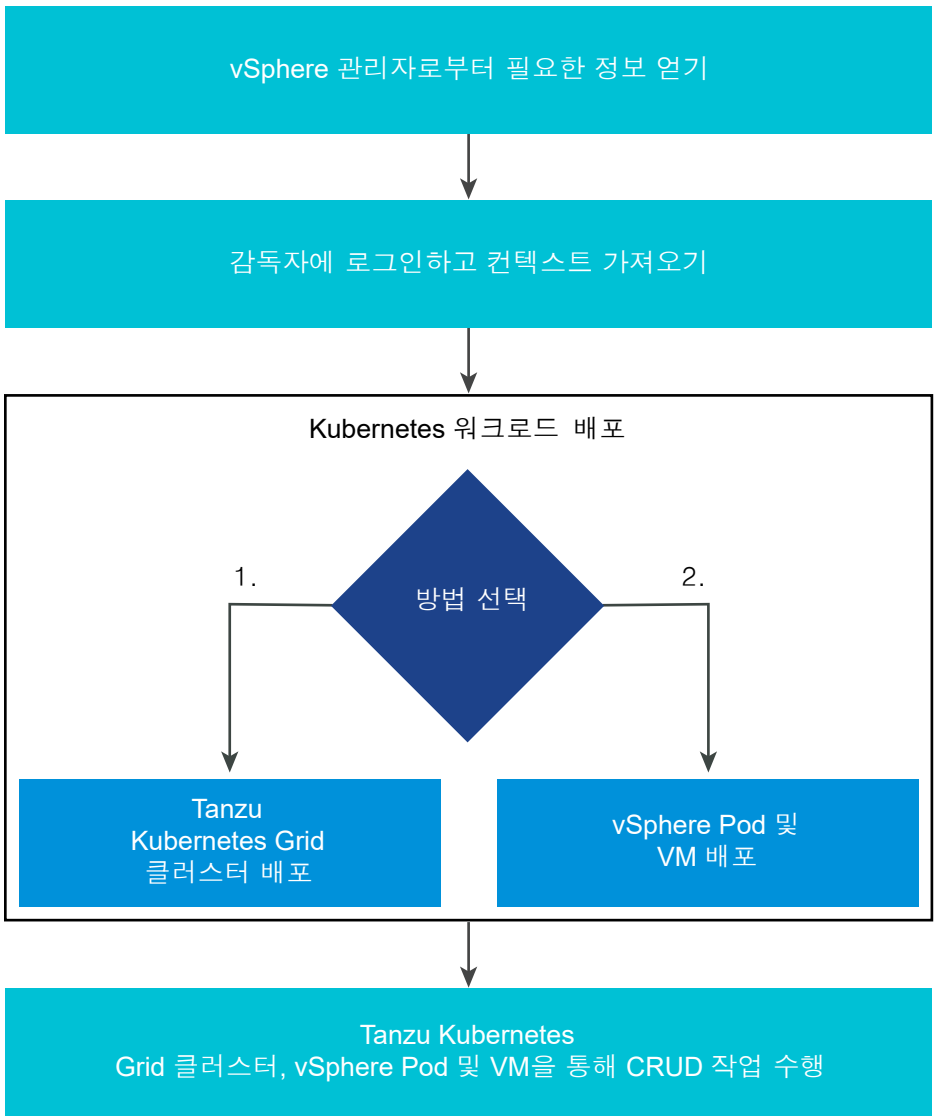
vSphere 관리자는 vSphere IaaS control plane과 상호 작용하는 기본 인터페이스가 vSphere Client입니다. 개략적으로는 DevOps 엔지니어가 Kubernetes 워크로드를 배포할 수 있는 감독자 및 네임스페이스를 구성해야 합니다. vSphere, NSX Advanced Load Balancer 또는 HAProxy 로드 밸런서, NSX(이 네트워킹 스택 선택)에 대한 지식이 풍부하고 Kubernetes에 대한 기본적인 이해가 있어야 합니다.

그림 1-6. vSphere 관리자 개략적인 워크플로



DevOps 엔지니어는 Kubernetes 개발자 및 애플리케이션 소유자, Kubernetes 관리자이거나 두 기능을 모두 결합한 것일 수 있습니다. DevOps 엔지니어는 kubectl 명령을 사용하여 기존 네임스페이스에 vSphere 포드, VM을 배포하고, kubectl 및 Tanzu CLI를 사용하여 Tanzu Kubernetes Grid 클러스터를 배포하고 관리합니다. 일반적으로 DevOps 엔지니어는 vSphere, NSX, vDS, 또는 NSX Advanced Load Balancer 및 HAProxy 전문가가 아니어도 되지만 vSphere 관리자와 보다 효율적으로 상호 작용할 수 있도록 이러한 기술과 플랫폼에 대한 기본적인 이해가 있어야 합니다.

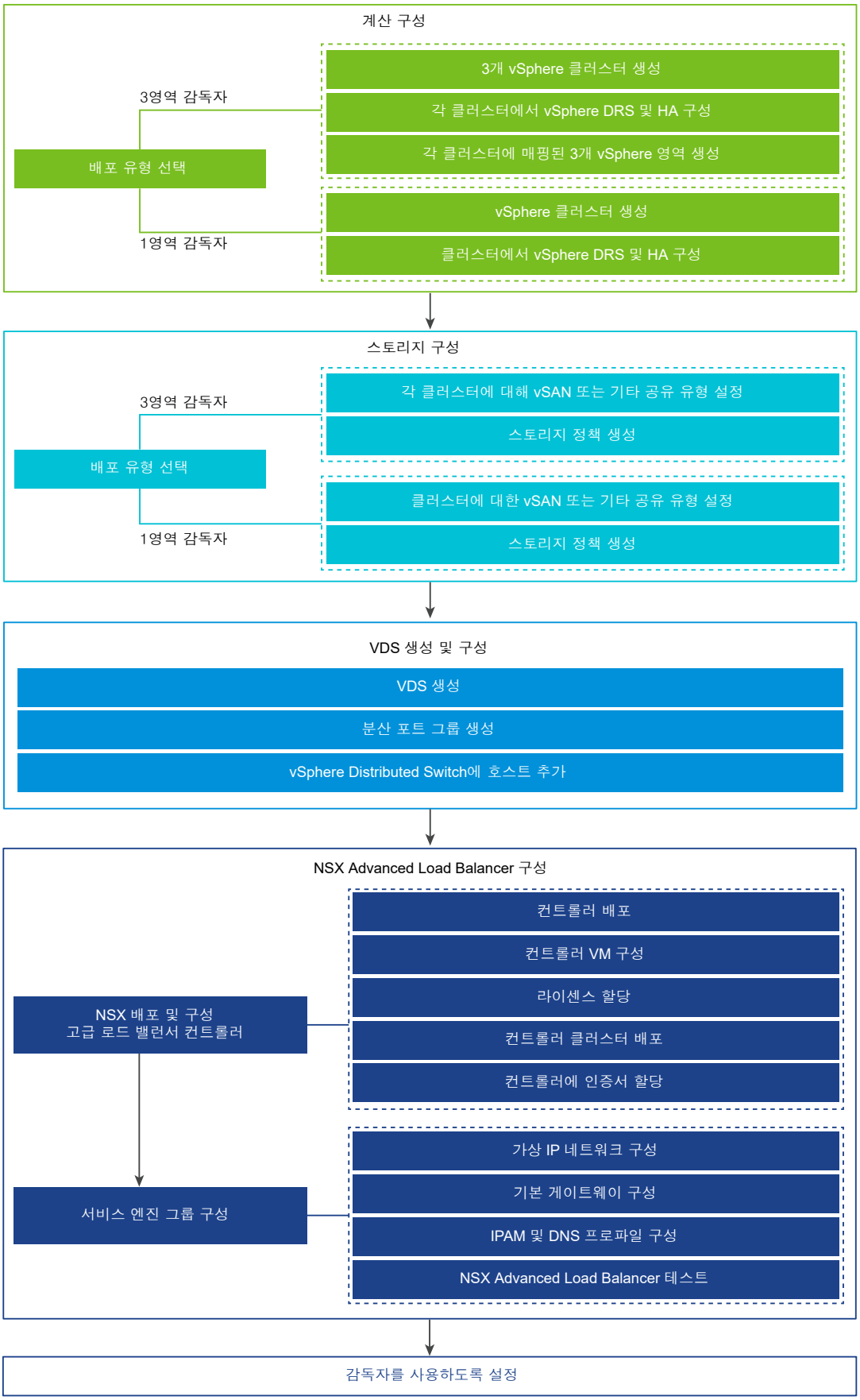
그림 1-7. DevOps 엔지니어 개략적인 워크플로



VDS 네트워킹 및 NSX Advanced Load Balancer 워크플로가 포함된 감독자

vSphere 관리자는 VDS 및 NSX Advanced Load Balancer를 통해 vSphere 네트워킹 스택이 포함된 vSphere 클러스터를 감독자로 구성할 수 있습니다. 하나의 vSphere 클러스터에 매핑된 1영역 감독자 또는 3개의 vSphere 클러스터에 매핑된 3영역 감독자를 구성할 수 있습니다. 시스템 요구 사항에 대한 자세한 내용은 NSX Advanced Load Balancer 및 VDS 네트워킹을 사용하는 클러스터 감독자 배포 요구 사항 및 NSX Advanced Load Balancer 및 VDS 네트워킹을 사용하는 영역 감독자 배포 요구 사항을 참조하십시오. VDS 네트워킹이 있는 감독자를 사용하도록 설정하는 방법에 대한 자세한 내용은 "vSphere IaaS 제어부 설치 및 구성"의 설치 및 구성을 참조하십시오.

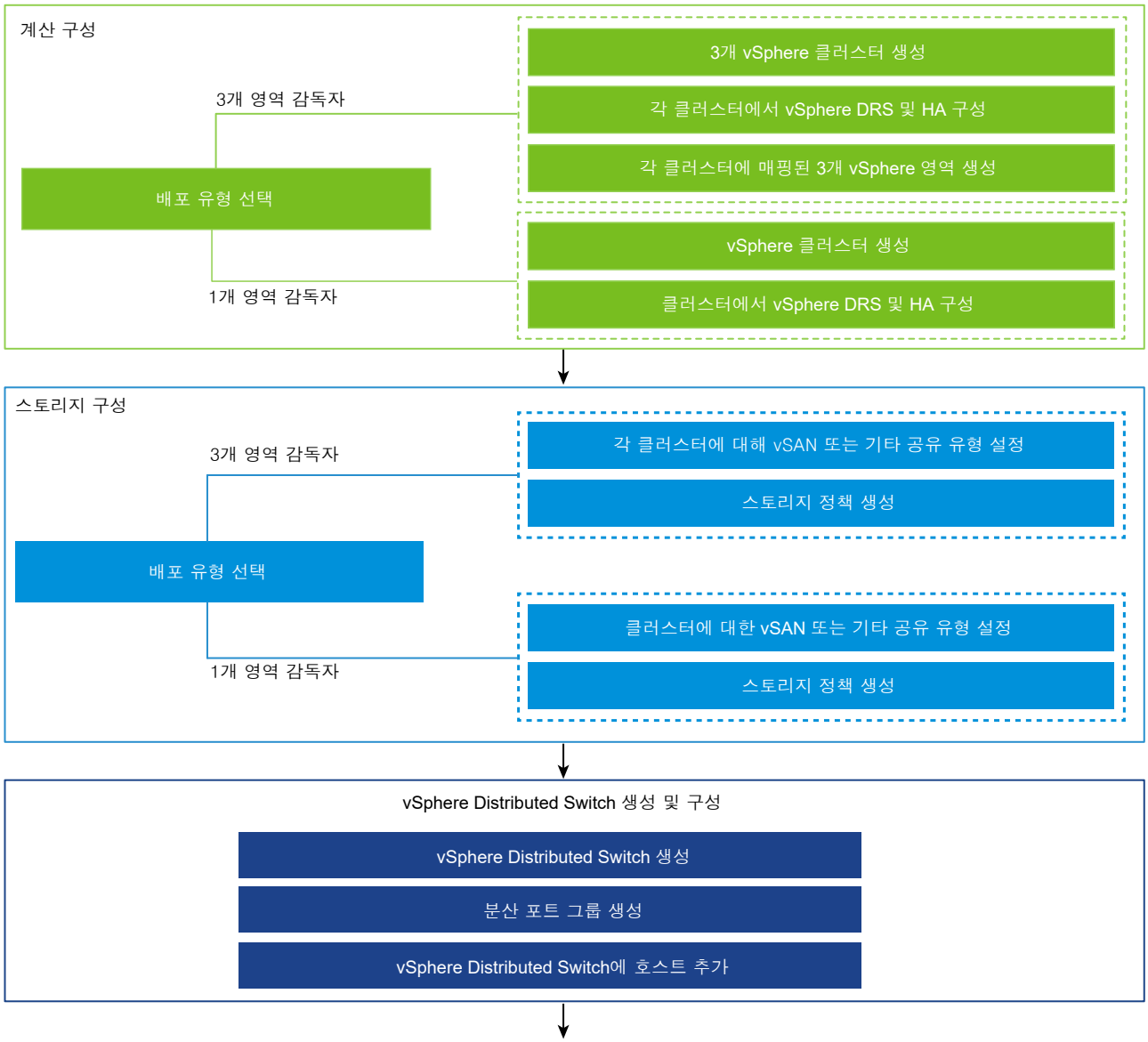
그림 1-8. VDS 네트워킹 및 NSX Advanced Load Balancer가 있는 감독자를 사용하도록 설정하는 워크플로

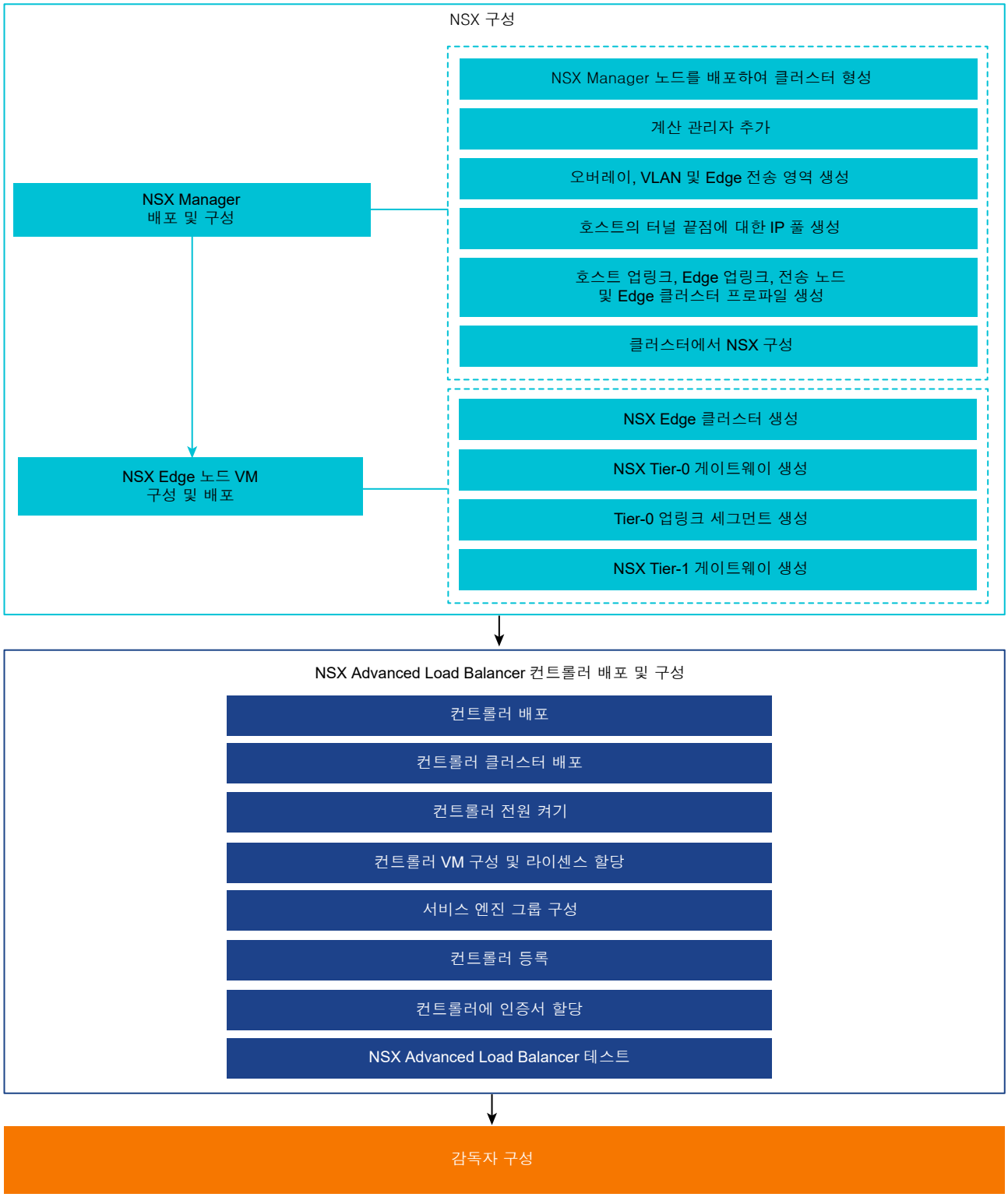


NSX 네트워킹 및 NSX Advanced Load Balancer Controller 워크플로가 포함된 감독자

NSX 네트워킹 스택 및 NSX Advanced Load Balancer Controller를 사용하여 1개 영역 또는 3개 영역 감독자를 구성할 수 있습니다. 요구 사항에 대한 자세한 내용은 NSX 및 NSX Advanced Load Balancer를 사용한 클러스터 감독자 배포 요구 사항 및 NSX 및 NSX Advanced Load Balancer가 있는 영역 감독자 요구 사항 항목을 참조하십시오. 설치 절차는 NSX 및 NSX Advanced Load Balancer 설치 및 구성을 참조하십시오.

그림 1-9. NSX 네트워킹 및 NSX Advanced Load Balancer Controller를 사용하여 감독자를 사용하도록 설정하는 워크플로

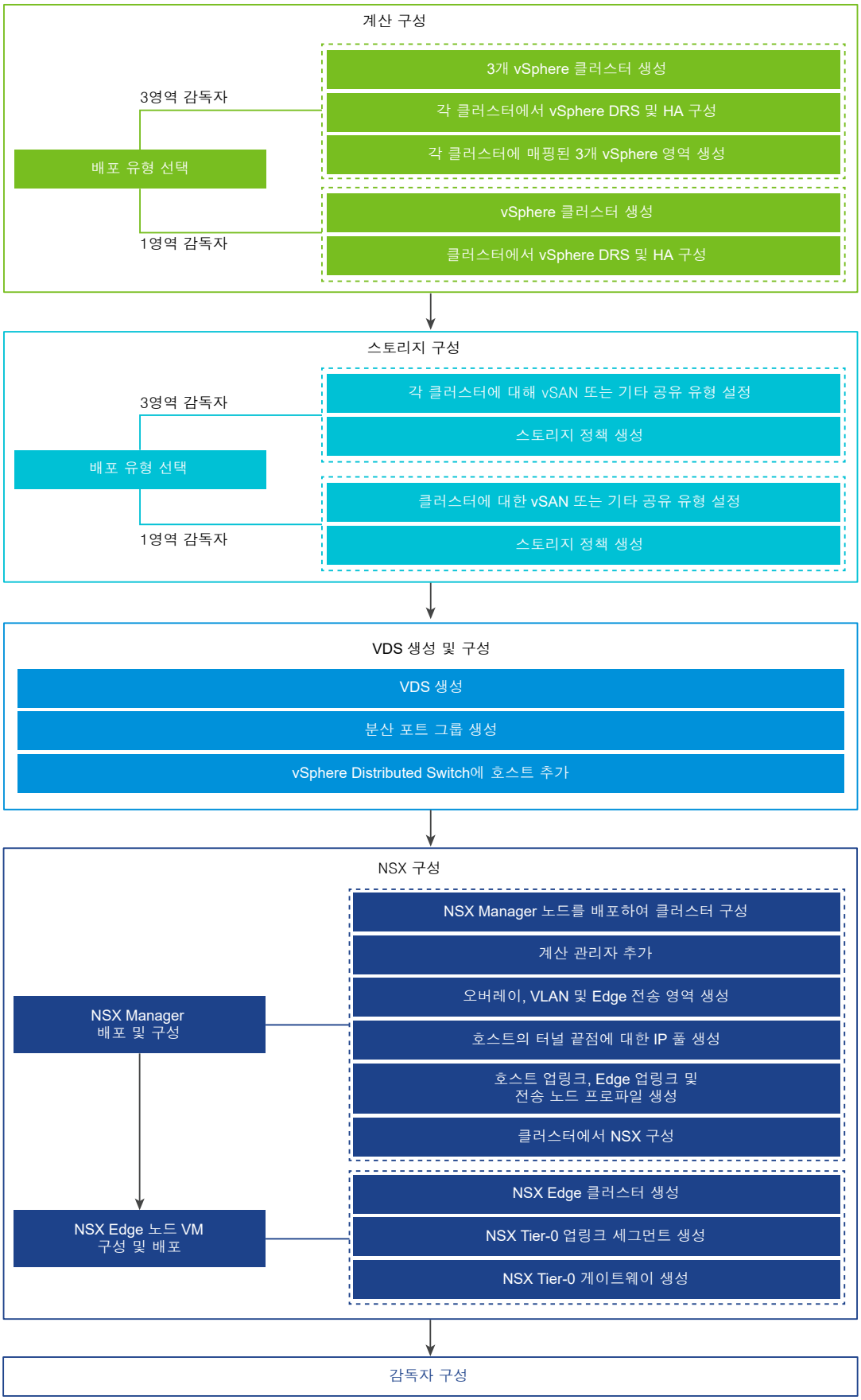



NSX 구성
NSX Manager 노드를 배포하여 클러스터 형성
계산 관리자 추가
오버레이, VLAN 및 Edge 전송 영역 생성
호스트의 터널 끝점에 대한 IP 풀 생성
호스트 업링크, Edge 업링크, 전송 노드
및 Edge 클러스터 프로파일 생성
클러스터에서 NSX 구성
NSX Manager
배포 및 구성
NSX Edge 클러스터 생성
NSX Tier-0 게이트웨이 생성
Tier-0 업링크 세그먼트 생성
NSX Tier-1 게이트웨이 생성
NSX Edge 노드 VM
구성 및 배포
NSX Advanced Load Balancer 컨트롤러 배포 및 구성
컨트롤러 배포
컨트롤러 클러스터 배포
컨트롤러 전원 켜기
컨트롤러 VM 구성 및 라이센스 할당
서비스 엔진 그룹 구성
컨트롤러 등록
컨트롤러에 인증서 할당
NSX Advanced Load Balancer 테스트
감독자 구성

NSX 네트워킹이 있는 감독자 워크플로

NSX를 네트워킹 스택으로 사용하여 1영역 또는 3영역 감독자를 구성할 수도 있습니다. 시스템 요구 사항에 대한 자세한 내용은 NSX를 사용한 클러스터 감독자 배포 요구 사항 및 NSX가 있는 영역 감독자 요구 사항을 참조하십시오. 설치 지침은 "vSphere IaaS 제어부 설치 및 구성" 의 설치 및 구성을 참조하십시오.

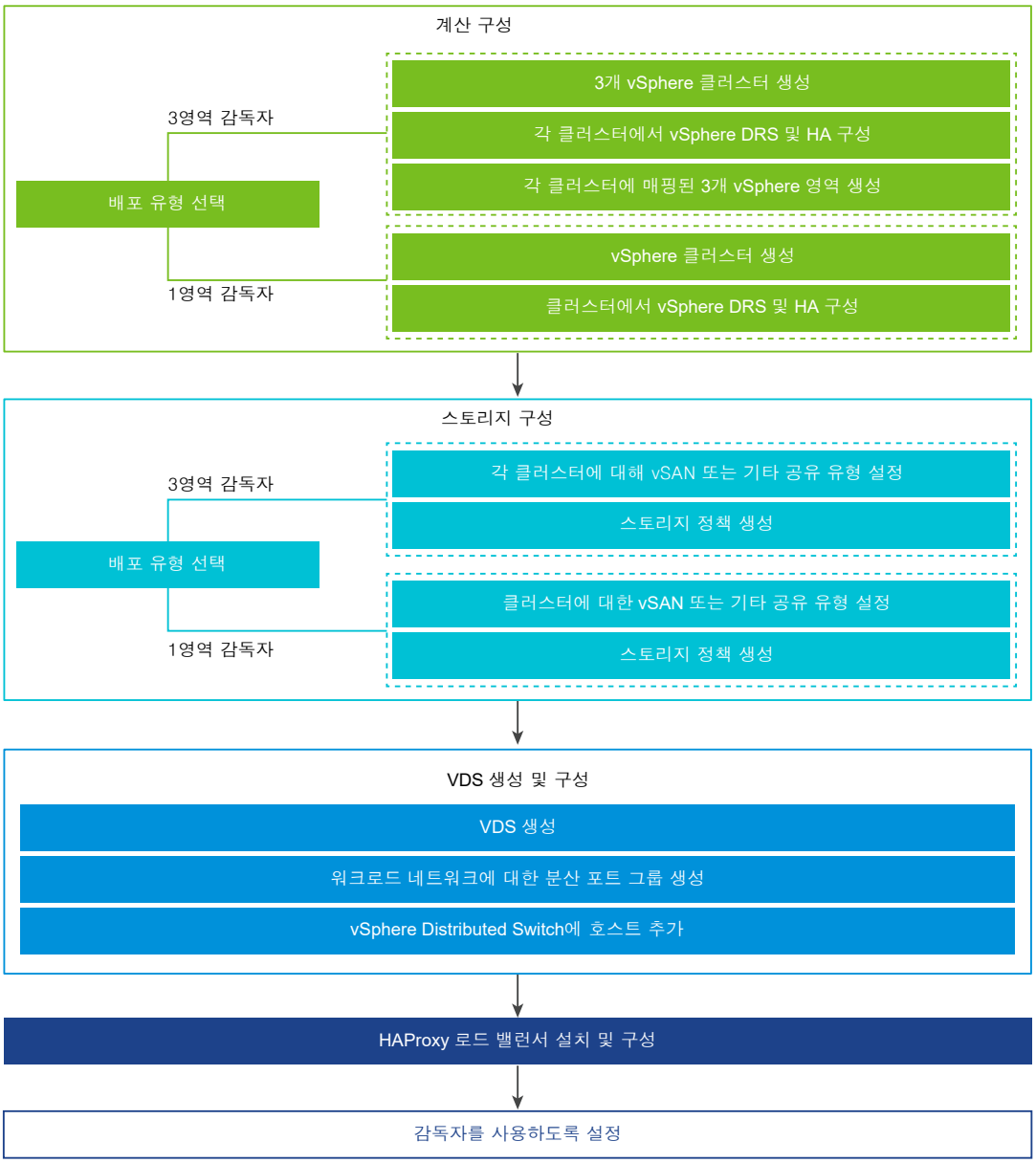
그림 1-10. NSX 네트워킹이 있는 감독자를 사용하도록 설정하는 워크플로



VDS 네트워킹 및 HAProxy 로드 밸런서가 있는 감독자 워크플로

vSphere 관리자는 VDS 네트워킹 스택 및 HAProxy 로드 밸런서를 사용하여 vSphere 클러스터에 매핑된 하나 또는 세 개의 vSphere 영역에서 감독자를 사용하도록 설정할 수 있습니다. 시스템 요구 사항에 대한 자세한 내용은 VDS 네트워킹 및 HAProxy 로드 밸런서를 사용한 클러스터 감독자 배포 요구 사항 및 HAProxy 로드 밸런서가 있는 영역 감독자 배포 요구 사항을 참조하십시오. 설치 지침은 "vSphere IaaS 제어부 설치 및 구성" 의 설치 및 구성을 참조하십시오.

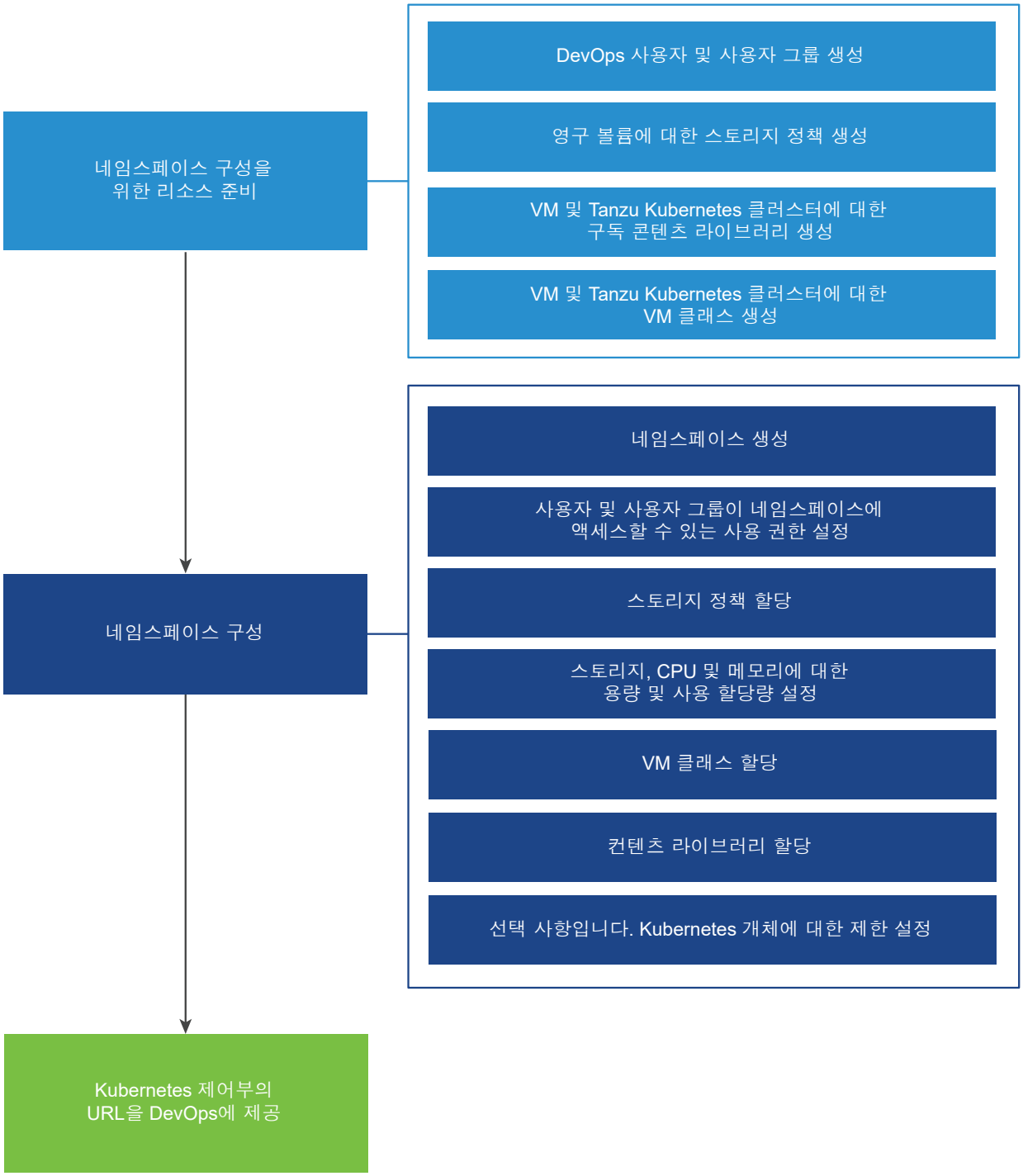
그림 1-11. VDS 네트워킹 및 HAProxy가 있는 감독자를 사용하도록 설정하는 워크플로



네임스페이스 생성 및 구성 워크플로

감독자를 사용하도록 설정하면 vSphere 관리자가 감독자에서 vSphere 네임스페이스를 생성하고 구성합니다. DevOps 엔지니어로부터 실행할 애플리케이션 및 워크로드에 대한 특정 리소스 요구 사항을 수집하고 그에 따라 네임스페이스를 구성해야 합니다. 자세한 내용은 vSphere 네임스페이스 구성 및 관리를 참조하십시오.

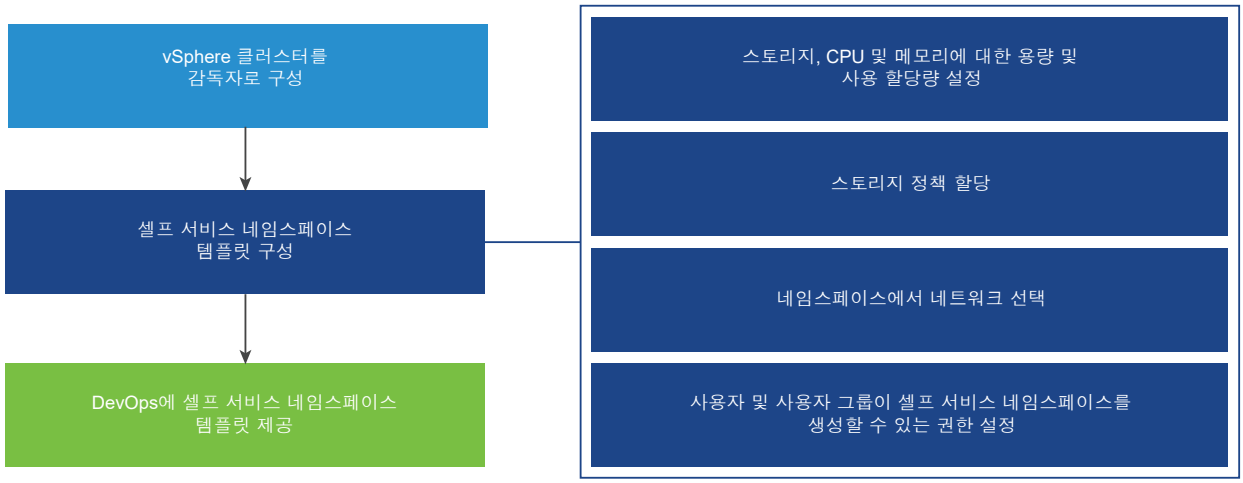
그림 1-12. vSphere 네임스페이스를 구성하는 워크플로



셀프 서비스 네임스페이스 생성 및 구성 워크플로

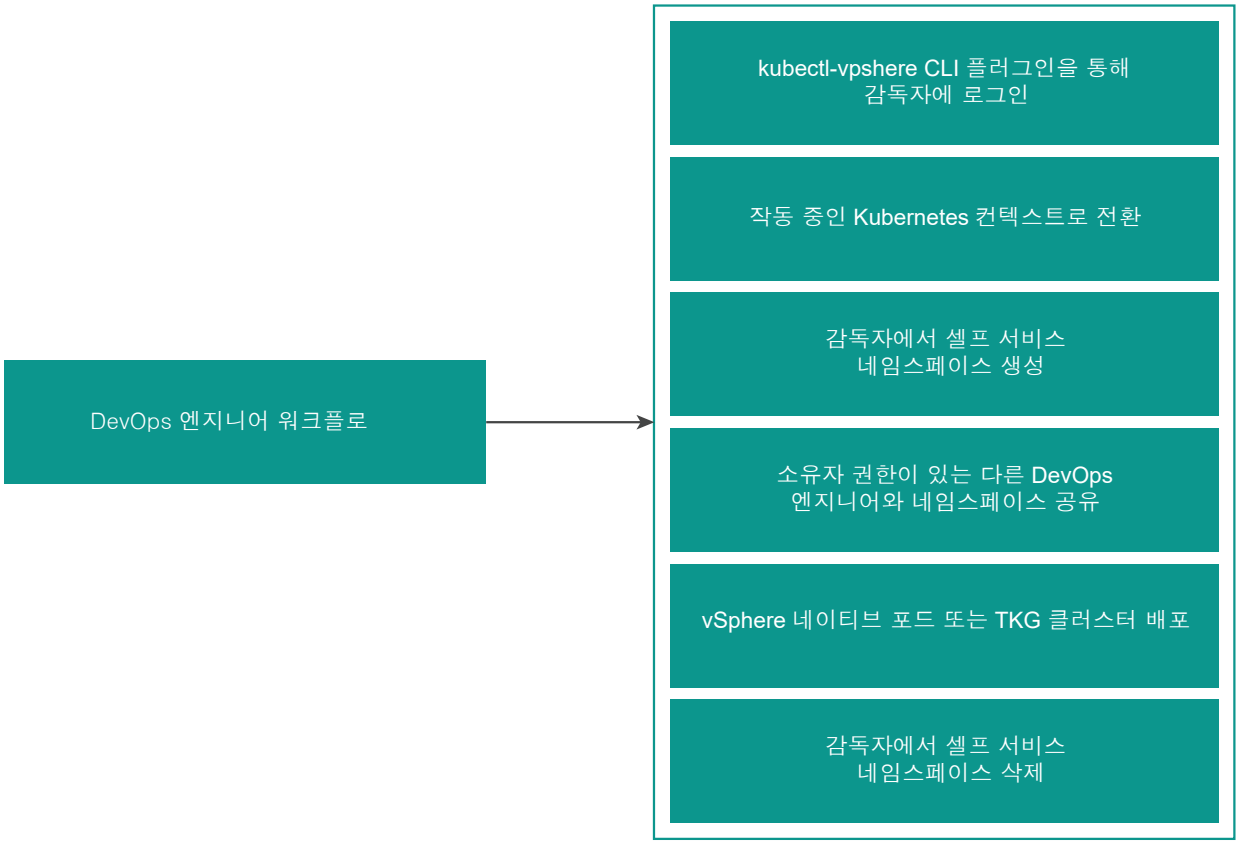
vSphere 관리자는 vSphere 네임스페이스를 생성하고, CPU, 메모리 및 스토리지 제한을 네임스페이스에 설정하고, 사용 권한을 할당하고, 클러스터에서 네임스페이스 서비스를 템플릿으로 프로비저닝 또는 활성화할 수 있습니다. 자세한 내용은 vSphere 네임스페이스 구성 및 관리를 참조하십시오.

그림 1-13. 셀프 서비스 네임스페이스 템플릿 프로비저닝 워크플로



DevOps 엔지니어는 셀프 서비스 방식으로 vSphere 네임스페이스를 생성하고 그 안에 워크로드를 배포할 수 있습니다. 다른 DevOps 엔지니어와 공유하거나 더 이상 필요하지 않으면 삭제할 수 있습니다.

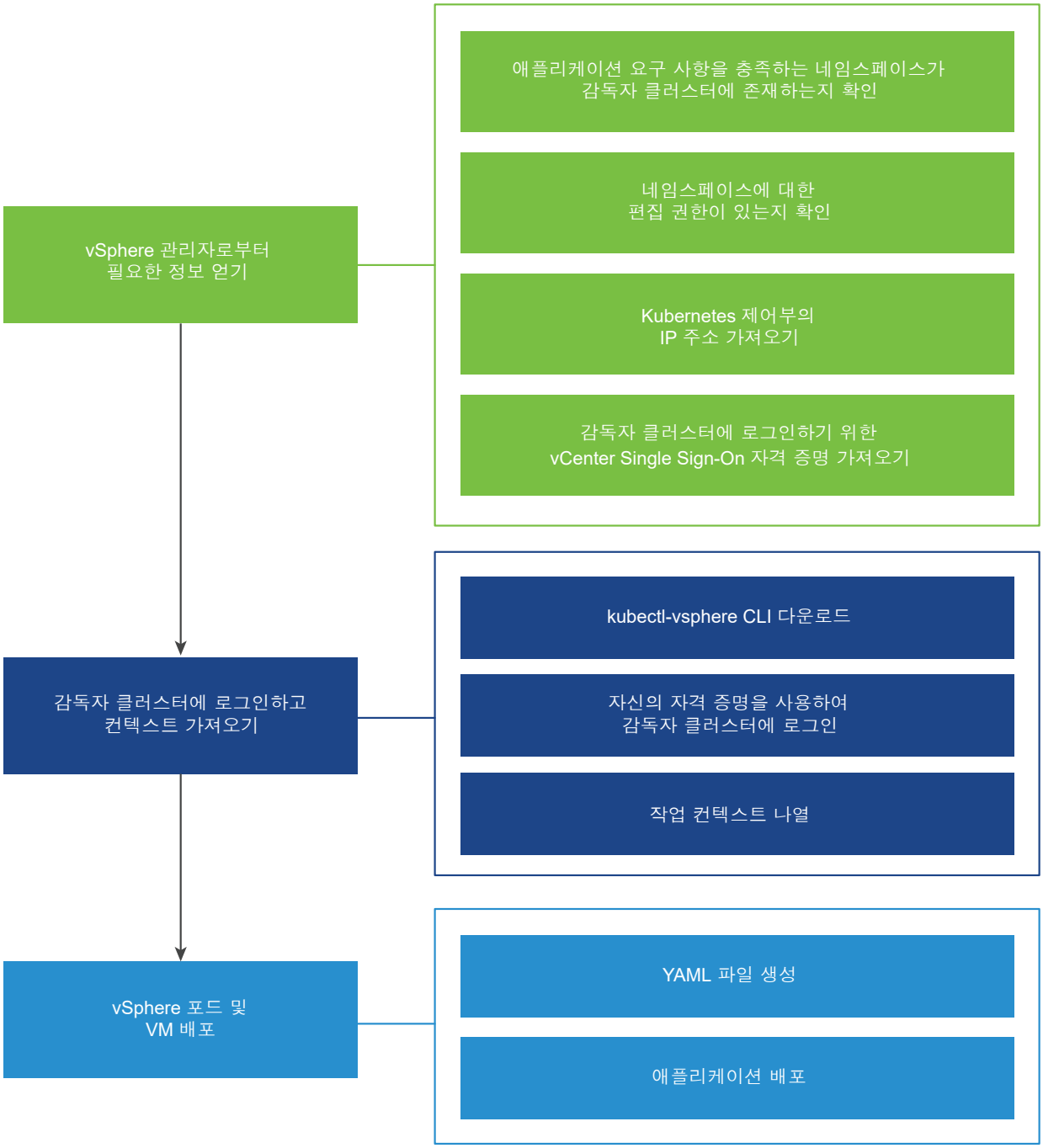
그림 1-14. 셀프 서비스 네임스페이스 생성 워크플로



vSphere 포드 및 VM 프로비저닝 워크플로

DevOps 엔지니어는 감독자에서 실행 중인 네임스페이스의 리소스 경계 내에서 vSphere 포드 및 VM을 배포할 수 있습니다. 자세한 내용은 "vSphere IaaS 제어부 서비스 및 워크로드" 의 vSphere 포드에 워크로드 배포 및 가상 시스템 배포 및 관리를 참조하십시오.

그림 1-15. vSphere 포드 및 VM 프로비저닝 워크플로



Tanzu Kubernetes Grid 클러스터 프로비저닝 워크플로

DevOps 엔지니어는 vSphere 네임스페이스에서 Tanzu Kubernetes Grid 클러스터를 생성하고 구성합니다. 자세한 내용은 "vSphere IaaS 제어부에서 TKG 서비스 사용" 가이드를 참조하십시오.

vSphere IaaS control plane이 vSphere 환경을 변경하는 방식

감독자는 네임스페이스, vSphere 포드 및 Tanzu Kubernetes Grid 클러스터와 같은 개체를 vCenter Server 인벤토리에 추가합니다.

각 감독자에서 다음을 볼 수 있습니다.

- 클러스터에서 실행 중인 논리적 애플리케이션을 나타내는 네임스페이스.
- 감독자의 각 네임스페이스에 대한 리소스 풀. 3영역 배포에서는 각 네임스페이스에 대한 리소스 풀이 영역의 각 클러스터 부분에서 생성됩니다.

모든 네임스페이스 내에서 다음을 볼 수 있습니다.

- vSphere 포드.
- Tanzu Kubernetes Grid 클러스터
- Kubernetes 제어부 VM 및 독립형 VM
- 네트워킹 및 스토리지 리소스.
- 해당 네임스페이스에 대한 사용자 권한

vSphere IaaS control plane에 대한 라이센싱

감독자에 할당할 수 있는 다양한 라이센스가 무엇인지, 라이센스 규정 준수, 평가 기간 및 라이센스 만료가 어떻게 작동하는지 알아봅니다.

감독자 라이센싱

vSphere 클러스터에서 감독자를 활성화한 후 60일 평가 기간 내에 감독자의 전체 기능 집합을 사용할 수 있습니다. 60일 평가 기간이 만료되기 전에 감독자에 유효한 라이센스를 할당해야 합니다.

VCF 및 VVF 솔루션 라이센스

vSphere 8 업데이트 2b 릴리스부터 VVF(VMware vSphere Foundation) 또는 VCF(VMware Cloud Foundation) 솔루션 라이센스를 vSphere IaaS control plane에 사용할 수 있습니다. vCenter Server를 버전 8 업데이트 2b로 업그레이드한 후에는 vSphere 환경의감독자에 VVF 또는 VCF 솔루션 라이센스를 할당할 수 있습니다.

참고 개별 구성 요소 라이센스 키는 계속 지원됩니다. 솔루션 라이센스와 함께 제공됩니다. 환경에서 솔루션 라이센스, 개별 구성 요소 라이센스 또는 두 가지 모두를 혼합하여 사용할 수 있습니다.

Tanzu Edition 라이센스

vSphere 8 업데이트 2b를 실행 중이고 감독자가 유효한 Tanzu Edition 라이센스를 이미 취득한 경우 해당 라이센스는 만료될 때까지 계속 작동합니다. Tanzu 라이센스가 만료되면 VCF 또는 VVF 솔루션 라이센스를 감독자 또는 유효한 Tanzu 라이센스에 할당해야 합니다.

라이센스 만료일

솔루션 라이센스 또는 Tanzu Edition 라이센스가 만료되면 새 라이센스를 획득할 때까지 vSphere IaaS control plane의 전체 기능 집합을 계속 사용할 수 있습니다. 하지만 새 감독자에 만료된 라이센스를 할당할 수 없습니다.

평가 기간 만료

감독자의 평가 기간이 만료되면 vSphere 관리자는 새 vSphere 네임스페이스를 생성하거나 감독자의 Kubernetes 버전을 업데이트할 수 없습니다. DevOps 엔지니어는 새 워크로드를 배포할 수 없으며 기존 Tanzu Kubernetes Grid 클러스터의 구성을 변경(예: 새 노드 추가)할 수 없습니다.

Tanzu Kubernetes Grid 클러스터에 워크로드를 계속 배포할 수 있으며 기존의 모든 워크로드는 예상대로 실행됩니다. 이미 배포된 모든 Kubernetes 워크로드는 정상적인 작업을 계속합니다.

라이센스 규정 준수

솔루션 라이센스 또는 Tanzu 라이센스 키에는 ESXi 호스트 라이센스와 유사하게 CPU당 최대 32개의 코어가 포함된 CPU당 용량이 있습니다. 이러한 라이센스 중 하나를 감독자에 할당하는 경우 사용되는 용량은 클러스터의 호스트에 있는 CPU 수와 각 CPU의 코어 수에 따라 결정됩니다. 솔루션 라이센스 또는 Tanzu Edition 라이센스 키를 한 번에 여러 감독자에 할당할 수 있지만 여러 라이센스 키를 하나의 감독자에 할당할 수는 없습니다.

예를 들어 새 호스트를 추가하여 감독자를 확장했을 때 감독자에 할당한 라이센스 키의 용량이 부족해지면 동일한 라이센스 키를 계속 사용할 수 있습니다. 하지만 EULA 준수 상태를 유지하려면 감독자의 모든 CPU 및 코어를 지원할 수 있는 충분한 용량의 새 라이센스 키를 확보해야 합니다.

vSphere IaaS control plane용 라이센스

vSphere IaaS control plane을 구성한 네트워킹 스택에 따라 제공되는 라이센스는 다음과 같이 다릅니다.

감독자 설정	vSphere 8 업데이트 2b용 라이센스	vSphere 8 업데이트 2b 이전 라이센스
VDS 네트워킹 및 NSX Advanced Load Balancer를 갖춘 감독자	■ VCF 솔루션 라이센스 ■ vSphere Enterprise+ 라이센스 ■ Tanzu Edition 라이센스 ■ NSX Advanced Load Balancer Essentials	■ vSphere Enterprise+ 라이센스 ■ Tanzu Edition 라이센스 ■ NSX Advanced Load Balancer Essentials
VDS 네트워킹 및 HAProxy 로드 밸런서가 있는 감독자	■ VVF 솔루션 라이센스 ■ vSphere Enterprise+ 라이센스 ■ Tanzu Edition 라이센스	■ vSphere Enterprise+ 라이센스 ■ Tanzu Edition 라이센스

감독자 설정	vSphere 8 업데이트 2b용 라이센스	vSphere 8 업데이트 2b 이전 라이센스
NSX를 사용한 감독자	■ VVF 솔루션 라이센스 ■ vSphere Enterprise + 라이센스 ■ Tanzu Edition 라이센스 ■ NSX Advanced 이상	■ vSphere Enterprise + 라이센스 ■ Tanzu Edition 라이센스 ■ NSX Advanced 이상
NSX 및 NSX Advanced Load Balancer를 갖춘 감독자	■ VCF 솔루션 라이센스 ■ NSX Advanced Load Balancer Enterprise ■ vSphere Enterprise+ 라이센스 ■ Tanzu Edition 라이센스 ■ NSX Advanced 이상 ■ NSX Advanced Load Balancer Enterprise	■ vSphere Enterprise+ 라이센스 ■ Tanzu Edition 라이센스 ■ NSX Advanced 이상 ■ NSX Advanced Load Balancer Enterprise

vSphere IaaS control plane ID 및 액세스 관리

vSphere 관리자는 감독자를 활성화 및 구성하고 vSphere 네임스페이스를 관리할 수 있는 권한이 필요합니다. 네임스페이스에 대한 사용 권한을 정의하여 네임스페이스에 액세스할 수 있는 DevOps 엔지니어와 개발자를 결정합니다. 외부 OIDC(OpenID Connect) 제공자로 감독자를 구성하여 다단계 인증을 사용하도록 설정할 수도 있습니다. DevOps 엔지니어 또는 개발자는 감독자에서 vSphere 관리자가 구성한 항목에 따라 vCenter Single Sign-On 자격 증명 또는 OIDC 제공자의 자격 증명을 사용하여 감독자에서 인증합니다. 사용 권한이 있는 vSphere 네임스페이스에만 액세스할 수 있습니다.

지원되는 ID 제공자

vSphere IaaS control plane는 다음과 같은 ID 제공자를 지원합니다.

- vCenter Single Sign-On. vSphere IaaS control plane 환경(감독자 및 Tanzu Kubernetes Grid 클러스터 포함)에서 인증하는 데 사용하는 기본 ID 제공자입니다. vCenter Single Sign-On은 vSphere 인프라에 대한 인증을 제공하고 AD/LDAP 시스템과 통합할 수 있습니다. vCenter Single Sign-On에 대한 자세한 내용은 vCenter Single Sign-On을 사용한 vSphere 인증을 참조하십시오.
- 외부 ID 제공자. vSphere 관리자는 OpenID Connect 프로토콜을 지원하는 외부 ID 제공자로 감독자를 구성할 수 있습니다. 외부 ID 제공자로 구성되면 감독자는 OAuth 2.0 클라이언트로 작동하며 Pinniped 인증 서비스를 사용하고 Tanzu CLI를 사용하여 Tanzu Kubernetes Grid 클러스터에 연결합니다. Tanzu CLI는 Tanzu Kubernetes Grid 클러스터의 수명 주기 관리 및 프로비저닝을 지원합니다. 각 감독자 인스턴스는 하나의 외부 ID 제공자를 지원할 수 있습니다.

감독자로 인증

vSphere IaaS control plane와 상호 작용하는 다양한 역할은 다음 방법을 사용하여 감독자로 인증할 수 있습니다.

- vSphere 관리자. vSphere 관리자는 vCenter Single Sign-On을 사용하여 vSphere Client를 통해 vSphere에서 인증합니다. kubectl용 vSphere 플러그인을 사용하여 kubectl을 통해 감독자 및 Tanzu Kubernetes Grid 클러스터에서 인증할 수도 있습니다. 자세한 내용은 vCenter Single Sign-On 사용자로 감독자에 연결을 참조하십시오.
- DevOps 엔지니어 또는 개발자. DevOps 엔지니어 또는 개발자는 vCenter Single Sign-On을 사용하여 kubectl용 vSphere 플러그인 및 kubectl을 통해 감독자에서 인증합니다. 감독자로 구성된 외부 ID 제공자의 자격 증명을 사용하여 감독자에 연결할 수도 있습니다. 자세한 내용은 외부 ID 제공자를 사용하여 감독자의 TKG 클러스터에 연결을 참조하십시오.

감독자를 사용한 로그인 세션

vCenter Single Sign-On 사용자로 감독자에 로그인하면 인증 프록시가 요청을 vCenter Single Sign-On으로 리디렉션합니다. kubectl용 vSphere 플러그인은 vCenter Server와의 세션을 설정하고 vCenter Single Sign-On에서 인증 토큰을 가져옵니다. 또한 액세스 권한이 있는 vSphere 네임스페이스 목록을 가져오고 이러한 vSphere 네임스페이스로 구성을 채웁니다. 사용자 계정의 사용 권한이 변경되면, 다음 로그인 시 vSphere 네임스페이스 목록이 업데이트됩니다.

감독자에 로그인하는 데 사용하는 계정은 자신에게 할당된 vSphere 네임스페이스에 대한 액세스만 제공합니다. vCenter Server에 로그인하려면 vSphere 관리자가 하나 이상의 vSphere 네임스페이스에서 로그인하려는 사용자의 계정에 적절한 사용 권한을 설정해야 합니다.

참고 kubectl에 대한 세션은 10시간 동안 지속됩니다. 세션이 만료된 후에는 감독자를 다시 인증해야 합니다. 토큰은 로그아웃 시 사용자 계정의 구성 파일에서 삭제되지만 세션이 종료될 때까지 유효합니다.

Tanzu Kubernetes Grid 클러스터를 사용하여 인증

DevOps 엔지니어 또는 개발자는 프로비저닝된 Tanzu Kubernetes Grid 클러스터에 연결하여 운영 및 관리합니다. Tanzu Kubernetes Grid 클러스터가 프로비저닝된 vSphere 네임스페이스에 대한 편집 또는 소유자 권한이 사용자 계정에 부여되면 계정이 `cluster-admin` 역할에 할당됩니다. 또는 `kubernetes-admin` 사용자를 사용하여 Tanzu Kubernetes Grid에 연결할 수도 있습니다. 사용자 또는 그룹을 기본 또는 사용자 지정 포드 보안 정책에 바인딩하여 개발자에게 Tanzu Kubernetes Grid 클러스터에 대한 액세스 권한을 부여할 수도 있습니다. 자세한 내용은 vCenter SSO 인증을 사용하여 감독자의 TKG 클러스터에 연결 및 외부 ID 제공자를 사용하여 감독자의 TKG 클러스터에 연결을 참조하십시오.

vSphere 네임스페이스 역할 권한

vSphere 관리자는 vSphere 네임스페이스의 DevOps 엔지니어 또는 개발자에게 보기, 편집 또는 소유자 권한을 부여합니다. 해당 사용자 또는 그룹은 vCenter Single Sign-On에서 또는 감독자로 구성된 외부 ID 제공자에서 사용할 수 있어야 합니다. 하나의 사용자 또는 그룹은 여러 vSphere 네임스페이스에 액세스할 수 있습니다. 각 vSphere 네임스페이스 역할은 다음 작업을 허용합니다.

역할	설명
볼 수 있음	사용자 또는 그룹에 대한 읽기 전용 액세스. 사용자 또는 그룹은 감독자 제어부에 로그인하고 vSphere 네임스페이스(예: vSphere 포드 및 Tanzu Kubernetes Grid 클러스터 및 VM)에서 실행 중인 워크로드를 나열할 수 있습니다.
편집할 수 있음	사용자 또는 그룹은 vSphere 포드, Tanzu Kubernetes Grid 클러스터 및 VM을 생성, 읽기, 업데이트 및 삭제할 수 있습니다. 관리자 그룹에 속한 사용자는 감독자의 모든 네임스페이스에 대한 편집 권한이 있습니다.
소유자	소유자 권한이 있는 사용자 또는 그룹은 다음을 수행할 수 있습니다. ■ vSphere 네임스페이스에서 워크로드를 배포하고 관리합니다. ■ vSphere 네임스페이스를 다른 사용자 또는 그룹과 공유합니다. ■ kubectl을 사용하여 추가 vSphere 네임스페이스를 생성하고 삭제합니다. 소유자 권한이 있는 사용자가 네임스페이스를 공유하면 다른 사용자 또는 그룹에 보기, 편집 또는 소유자 권한을 할당할 수 있습니다. **참고** 소유자 역할은 vCenter Single Sign-On에서 사용 가능한 사용자에 대해 지원됩니다. 외부 ID 제공자의 사용자 또는 그룹에는 소유자 역할을 사용할 수 없습니다.

vSphere 네임스페이스 생성 및 구성에 대한 자세한 내용은 vSphere 네임스페이스 생성 및 구성을 참조하십시오.

vSphere 관리자가 역할 사용 권한, 리소스 할당량 및 스토리지가 포함된 vSphere 네임스페이스를 구성한 후에는 감독자 제어부의 URL을 DevOps 엔지니어 및 개발자에게 제공하며, 이들은 이 URL을 사용하여 제어부에 로그인할 수 있습니다. 로그인하면 DevOps 엔지니어 및 개발자는 vCenter Server 시스템에 속한 동일한 ID 제공자로 구성된 감독자 전체에 사용 권한이 있는 vSphere 네임스페이스에 액세스할 수 있습니다. vCenter Server 시스템이 고급 연결 모드인 경우 DevOps 엔지니어 및 개발자는 링크드 모드 그룹에서 사용 가능한 모든 감독자에서 사용 권한이 있는 모든 vSphere 네임스페이스에 액세스할 수 있습니다. 감독자 제어부의 IP 주소는 NSX(VDS 네트워킹의 경우 로드 밸런서)에서 생성되는 가상 IP로, 감독자 제어부에 대한 액세스 지점으로 사용됩니다.

vSphere 관리자 사용 권한

vSphere 관리자의 사용자 계정에는 일반적으로 다음과 같은 사용 권한이 있을 수 있습니다.

개체	사용 권한
vCenter Single Sign-On user	관리자 그룹
vSphere 네임스페이스 user	관리자 그룹의 멤버에게는 모든 vSphere 네임스페이스에 대한 편집 권한이 부여됩니다.

vSphere IaaS control plane와 상호 작용하는 데 사용하는 인터페이스에 따라 부여된 사용 권한으로 다양한 작업을 수행할 수 있습니다.

인터페이스	작업
vSphere Client	vSphere Client에 관리자로 로그인하면 다음을 수행할 수 있습니다. ■ 감독자를 활성화하고 구성합니다. ■ DevOps 엔지니어 또는 개발자를 위한 역할 사용 권한 및 리소스 할당으로 vSphere 네임스페이스를 생성하고 구성합니다. kubectl을 통해 감독자 제어부에 로그인하여 워크로드 관리를 실행하려는 사용자 또는 그룹에는 vSphere 네임스페이스에 대한 역할 사용 권한이 필요합니다. ■ 감독자에서 감독자 서비스를 배포하고 관리합니다.
kubectl	vCenter Single Sign-On 관리자 계정으로 감독자 제어부에 로그인한 경우 다음을 수행할 수 있습니다. ■ 시스템 vSphere 네임스페이스(kube-system 및 모든 vmware-system-* 네임스페이스)를 포함한 모든 vSphere 네임스페이스의 리소스를 봅니다. ■ vSphere Client 또는 vCenter Server API를 통해 생성된 네임스페이스인 모든 시스템 이외 vSphere 네임스페이스의 리소스를 편집합니다. 하지만 관리자 그룹의 일부인 계정으로 감독자 제어부에 로그인한 경우 클러스터 수준 리소스를 편집하거나 kubectl을 사용하여 vSphere 네임스페이스를 생성하거나 역할 바인딩을 생성할 수 없습니다. vSphere Client를 기본 인터페이스로 사용하여 리소스 할당량을 설정하고, vSphere 네임스페이스를 생성 및 구성하고, 사용자 사용 권한을 설정해야 합니다.

DevOps 엔지니어 및 개발자 사용 권한

DevOps 엔지니어 또는 개발자의 사용자 계정에는 일반적으로 다음과 같은 사용 권한이 필요합니다.

개체	사용 권한
vSphere 네임스페이스	편집 또는 소유자
vCenter Single Sign-On user	없음 또는 읽기 전용

DevOps 엔지니어 또는 개발자는 kubectl을 기본 인터페이스로 사용하여 vSphere IaaS control plane와 상호 작용합니다. 자신에게 할당된 vSphere 네임스페이스의 워크로드를 보고 실행하고 관리하려면 kubectl용 vSphere 플러그인을 통해 감독자 제어부에 로그인할 수 있어야 합니다. 따라서 사용자 계정에는 하나 이상의 vSphere 네임스페이스에 대한 편집 또는 소유자 권한이 필요합니다.

일반적으로 vSphere Client를 통해 감독자에 대한 관리 작업을 수행할 필요가 없습니다. 단, 경우에 따라 계정에 할당된 vSphere 네임스페이스의 리소스 및 워크로드를 보기 위해 vSphere Client에 로그인해야 할 수도 있습니다. 이 경우 vSphere에 대한 읽기 전용 권한이 필요할 수 있습니다.

vSphere 네임스페이스 권한

vSphere 네임스페이스 권한은 vSphere IaaS control plane와 상호 작용하는 방식을 제어합니다. 계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

vSphere Client의 권한 이름	설명	필수	API의 권한 이름
디스크 서비스 해제 작업 허용	데이터스토어의 서비스 해제 작업이 가능합니다.	데이터스토어	Namespaces.ManageDisks
백업 워크로드 구성 요소 파일	etcd 클러스터의 컨텐츠를 백업할 수 있습니다(VMware Cloud on AWS에만 사용됨).	클러스터	Namespaces.Backup
액세스 가능한 네임스페이스 나열	액세스 가능한 vSphere 네임스페이스를 나열할 수 있습니다.	클러스터	Namespaces.ListAccess
클러스터 전체 구성 수정	감독자 구성을 수정하고 vSphere 네임스페이스를 생성 및 삭제할 수 있습니다.	클러스터	Namespaces.ManageCapabilities
클러스터 전체 네임스페이스 셀프 서비스 구성 수정	vSphere 네임스페이스 셀프 서비스 구성을 수정할 수 있습니다.	클러스터 (활성화 및 비활성화용) 템플릿 (구성 수정용) vCenter Server (템플릿 생성용)	Namespaces.SelfServiceManage
네임스페이스 구성 수정	리소스 할당, 사용자 사용 권한 및 컨텐츠 라이브러리 연결과 같은 vSphere 네임스페이스 구성 옵션을 수정할 수 있습니다.	클러스터	Namespaces.Manage
클러스터 기능 전환	클러스터 감독자 기능의 상태를 조작할 수 있습니다(VMware Cloud on AWS 경우에만 내부적으로 사용됨).	클러스터	해당 없음
최신 버전으로 클러스터 업그레이드	감독자 업그레이드를 시작할 수 있습니다.	클러스터	Namespaces.Upgrade

감독자 서비스 권한

감독자 서비스 권한은 vSphere IaaS control plane 환경에서 감독자 서비스를 생성하고 관리할 수 있는 사용자를 제어합니다.

표 1-1. 감독자 서비스 권한

vSphere Client의 권한 이름	설명	필수	API의 권한 이름
감독자 서비스 관리	감독자 서비스를 생성, 업데이트 또는 삭제할 수 있습니다. 감독자에 감독자 서비스를 설치하고, 감독자 서비스 버전을 생성하거나 삭제할 수도 있습니다.	클러스터	SupervisorServices.Manage

VM 클래스 권한

VM 클래스 권한은 vSphere 네임스페이스에서 가상 시스템 클래스를 추가하고 제거할 수 있는 사용자를 제어합니다.

표 1-2. 가상 시스템 클래스 권한

vSphere Client의 권한 이름	설명	필수	API의 권한 이름
가상 시스템 클래스 관리	감독자에서 vSphere 네임스페이스의 가상 시스템 클래스를 관리할 수 있습니다.	클러스터	VirtualMachineClasses.Manage

스토리지 보기 권한

스토리지 보기 권한이 있으면 vCenter Server에서 스토리지 정책을 볼 수 있으므로 vSphere 네임스페이스에 할당할 수 있습니다.

표 1-3. 스토리지 보기 권한

vSphere Client의 권한 이름	설명	필수	API의 권한 이름
서비스 구성	권한 있는 사용자가 모든 Storage Monitoring Service API를 사용하도록 합니다. 읽기 전용 Storage Monitoring Service API에 대한 권한에 **스토리지 보기.보기**를 사용합니다.	루트 vCenter Server	StorageViews.ConfigureService
보기	권한 있는 사용자가 읽기 전용 Storage Monitoring Service API를 사용하도록 합니다.	루트 vCenter Server	StorageViews.View

vSphere IaaS control plane 보안

vSphere IaaS control plane는 vSphere 보안 기능을 활용하며 기본적으로 안전한 클러스터 Tanzu Kubernetes Grid 클러스터를 프로비저닝합니다.

vSphere IaaS control plane는 vCenter Server 및 ESXi에 내장된 보안 기능을 활용할 수 있는 vSphere에 대한 추가 기능 모듈입니다. 자세한 내용은 vSphere 보안 설명서를 참조하십시오.

감독자는 데이터베이스(etcd)에 저장된 모든 암호를 암호화합니다. 암호는 부팅 시 vCenter Server에 의해 제공되는 로컬 암호와 키 파일을 통해 암호화됩니다. 암호 해독 키는 감독자 노드의 메모리(tempfs)와 vCenter Server 데이터베이스 내의 암호화된 형식으로 디스크에 저장됩니다. 키는 각 시스템의 루트 사용자에게 일반 텍스트로 제공됩니다. 각 워크로드 클러스터의 데이터베이스 내에 보관된 암호는 일반 텍스트로 저장됩니다. 모든 etcd 연결은 설치 시 생성되고 업그레이드 중에 순환되는 인증서를 사용하여 인증됩니다. 현재는 인증서를 수동으로 순환하거나 업데이트할 수 없습니다. 각 Tanzu Kubernetes Grid 클러스터의 제어부에 설치된 데이터베이스(etcd)의 데이터에 동일한 암호화 모델이 적용됩니다.

감독자에서는 호환되는 시스템에서 기밀 vSphere 포드를 실행할 수 있습니다. SEV-ES(Secure Encrypted Virtualization-Encrypted State)를 보안 강화 항목으로 추가하여 기밀 vSphere 포드를 생성할 수 있습니다. 자세한 내용은 "vSphere IaaS 제어부 서비스 및 워크로드" 에서 기밀 vSphere 포드 배포를 참조하십시오.

Tanzu Kubernetes Grid 클러스터는 기본적으로 안전합니다. 모든 Tanzu Kubernetes Grid 클러스터에 대해 제한적인 PSP(PodSecurityPolicy)를 사용할 수 있습니다. 개발자가 권한 있는 포드 또는 루트 컨테이너를 실행해야 하는 경우, 최소한 클러스터 관리자는 권한이 있는 기본 PSP에 대한 액세스 권한을 사용자에게 부여하는 RoleBinding을 생성해야 합니다. 자세한 내용은 "vSphere IaaS 제어부에서 TKG 서비스 사용" 의 내용을 참조하십시오.

Tanzu Kubernetes Grid 클러스터에는 인프라 자격 증명이 없습니다. Tanzu Kubernetes Grid 클러스터 내에 저장된 자격 증명은 Tanzu Kubernetes Grid 클러스터에 테넌시가 있는 vSphere 네임스페이스에만 액세스하기에 충분합니다. 따라서 클러스터 운영자 또는 사용자에 대해 권한을 에스컬레이션할 수 있는 방법은 없습니다.

Tanzu Kubernetes Grid 클러스터에 액세스하는 데 사용되는 인증 토큰은 감독자 또는 기타 Tanzu Kubernetes Grid 클러스터에 액세스하는 데 토큰을 사용할 수 없도록 범위가 지정됩니다. 이렇게 하면 클러스터 운영자 또는 클러스터를 손상시키려는 개인이 Tanzu Kubernetes Grid 클러스터에 로그인할 때 vSphere 관리자의 토큰을 캡처하기 위해 루트 수준 액세스를 사용하는 것을 방지할 수 있습니다.

감독자 아키텍처 및 구성 요소

2

vSphere IaaS control plane에서 활성화된 클러스터를 감독자라고 합니다. 3개의 vSphere 클러스터에서 하나의 감독자를 사용하도록 설정하는 3영역 배포 중에서 선택하거나 vSphere 클러스터와 감독자 간에 일대일 매핑을 선택할 수 있습니다. 감독자는 vSphere 포드, VM 및 Tanzu Kubernetes Grid 클러스터를 포함하는 워크로드를 실행하는 데 필요한 구성 요소와 리소스를 제공하는 vSphere IaaS control plane의 기반이 됩니다.

다음으로 아래 항목을 읽으십시오.

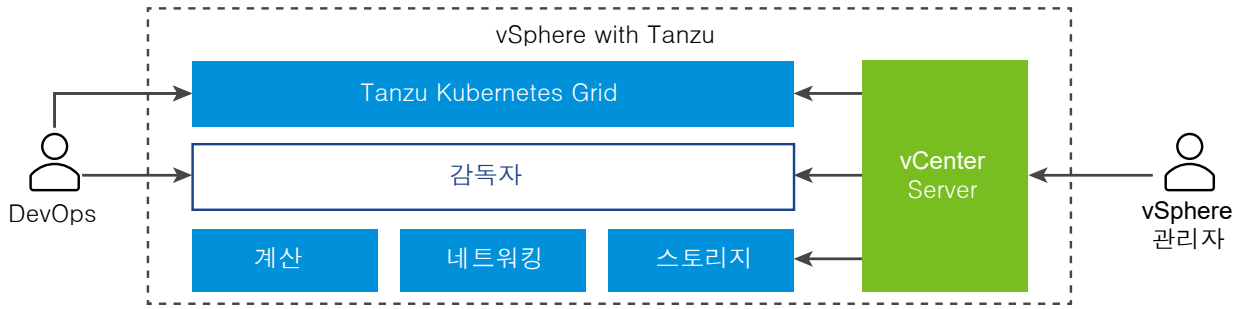
- 감독자 아키텍처
- 감독자 네트워킹
- 감독자 스토리지

감독자 아키텍처

vSphere 클러스터에서 vSphere IaaS control plane를 사용하도록 설정하고 클러스터가 감독자가 되면 하이퍼바이저 계층 내에 Kubernetes 제어부가 생성됩니다. 이 계층에는 ESXi 내에서 Kubernetes 워크로드를 실행하는 기능이 있는 특정 개체가 포함되어 있습니다.

그림 2-1. 감독자 일반 아키텍처

이 다이어그램은 vSphere IaaS control plane 상위 수준 아키텍처를 보여줍니다. 맨 위에는 Tanzu Kubernetes Grid, 중간에는 감독자, 맨 아래에는 ESXi, 네트워킹 및 스토리지가 있으며 이를 관리하는 vCenter Server가 있습니다.



감독자는 계산용 ESXi, NSX 또는 VDS 네트워킹, vSAN 또는 다른 공유 스토리지 솔루션으로 구성된 SDDC 계층의 위에서 실행됩니다. 공유 스토리지는 vSphere 포드의 영구 볼륨, 감독자 내에서 실행되는 VM, Tanzu Kubernetes Grid 클러스터의 포드에 사용됩니다. 감독자가 생성된 후에 vSphere 관리자는 감독자 내에 vSphere 네임스페이스를 생성할 수 있습니다. DevOps 엔지니어는 vSphere 포드 내에서 실행되는 컨테이너로 구성된 워크로드를 실행하고, VM 서비스를 통해 VM을 배포하고, Tanzu Kubernetes Grid 클러스터를 생성할 수 있습니다.

3개의 vSphere 영역에 감독자를 배포하여 Kubernetes 워크로드를 클러스터 수준 장애로부터 보호하는 클러스터 수준 고가용성을 제공할 수 있습니다. vSphere 영역은 독립 장애 도메인으로 설정할 수 있는 하나의 vSphere 클러스터에 매핑됩니다. 3영역 배포에서는 vSphere 클러스터 3개 모두가 하나의 감독자가 됩니다. 감독자를 하나의 vSphere 클러스터에 배포하면 vSphere 영역이 자동으로 생성되고 클러스터에 매핑됩니다. 또는 영역에 이미 매핑된 vSphere 클러스터를 사용할 수도 있습니다. 단일 클러스터 배포에서 감독자는 vSphere HA에서 제공하는 호스트 수준 고가용성만 지원합니다.

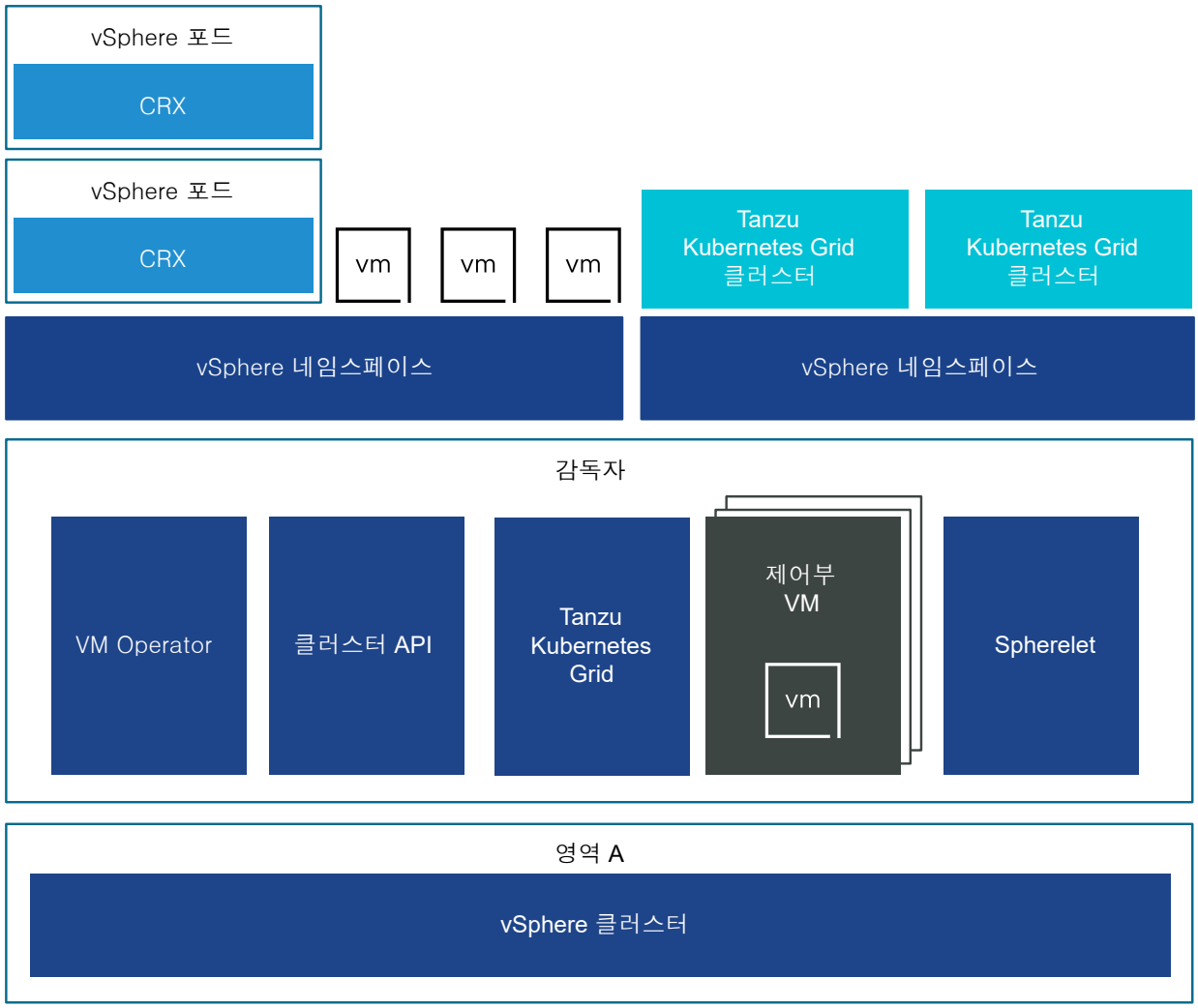
그림 2-2. 3영역 감독자 아키텍처

3영역 감독자에서는 VM 서비스를 사용하여 생성된 VM 및 Tanzu Kubernetes Grid 클러스터에서 Kubernetes 워크로드를 실행할 수 있습니다. 3영역 감독자에는 다음과 같은 구성 요소가 있습니다.

- 감독자 제어부 VM. 총 3개의 감독자제어부 VM이 감독자에 생성됩니다. 3영역 배포에서는 각 영역에 하나의 제어부 VM이 있습니다. 3개의 감독자 제어부 VM 각각에는 고유한 IP 주소가 있으므로 로드 균형이 조정됩니다. 또한 VM 중 하나에 부동 IP 주소가 할당되고 다섯 번째 IP 주소는 패치 적용 용도로 예약됩니다. vSphere DRS는 감독자의 ESXi 호스트 부분에서 제어부 VM의 정확한 배치를 결정하고 필요할 때 마이그레이션합니다.
- Tanzu Kubernetes Grid 및 클러스터 API. 감독자에서 실행되고 Tanzu Kubernetes Grid 클러스터의 프로비저닝 및 관리를 사용하도록 설정하는 모듈입니다.
- 가상 시스템 서비스와 같은 경보가 표시됩니다. 독립형 VM 및 Tanzu Kubernetes Grid 클러스터를 구성하는 VM의 배포 및 실행을 담당하는 모듈입니다.

3영역 감독자에서 영역에 매핑된 각 vSphere 클러스터에 네임스페이스 리소스 풀이 생성됩니다. 네임스페이스는 각 영역의 vSphere 클러스터 3개 모두에 분산됩니다. 3영역 감독자의 네임스페이스에 사용되는 리소스는 기본 vSphere 클러스터 3개 모두에서 동일한 양이 사용됩니다. 예를 들어 300MHz의 CPU를 할당하면 각 vSphere 클러스터에서 100MHz가 사용됩니다.

그림 2-3. 단일 클러스터 감독자 아키텍처



단일 vSphere 클러스터에 배포된 감독자에는 클러스터의 ESXi 호스트 부분에 상주하는 3개의 제어부 VM도 있습니다. 단일 클러스터 감독자에서는 Tanzu Kubernetes Grid 클러스터 및 VM 외에 vSphere 포드를 실행할 수 있습니다. vSphere DRS는 감독자 제어부 VM의 Kubernetes 스케줄러와 통합되므로 DRS가 vSphere 포드의 배치를 결정합니다. DevOps 엔지니어가 vSphere 포드을 스케줄링하는 경우, 요청은 일반 Kubernetes 워크플로를 거쳐서 DRS로 이동하여 최종 배치 결정을 내립니니다.

vSphere 포드 지원 덕분에 단일 클러스터 감독자에는 다음과 같은 추가 구성 요소가 있습니다.

- Spherelet. Spherelet이라는 추가 프로세스는 각 호스트에 생성됩니다. kubelet은 기본적으로 ESXi로 이식되고 ESXi 호스트가 Kubernetes 클러스터의 일부가 되도록 허용합니다.
- CRX(Container Runtime Executive) 구성 요소. CRX는 Hostd와 vCenter Server의 관점에서 VM과 유사합니다. CRX에는 하이퍼바이저와 함께 작동하는 반가상화 Linux 커널이 포함되어 있습니다. CRX는 VM과 동일한 하드웨어 가상화 기술을 사용하며 주변에 VM 경계가 있습니다. 직접 부팅 기술이 사용되기 때문에 CRX의 Linux 게스트가 커널 초기화를 통해 전달하지 않고도 기본 초기화 프로세스를 시작할 수 있습니다. 따라서 vSphere 포드가 거의 컨테이너만큼 빠르게 부팅할 수 있습니다.

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 라이센스가 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 네트워크로 사용합니다. 감독자의 네임스페이스에 워크로드 네트워크를 할당합니다.

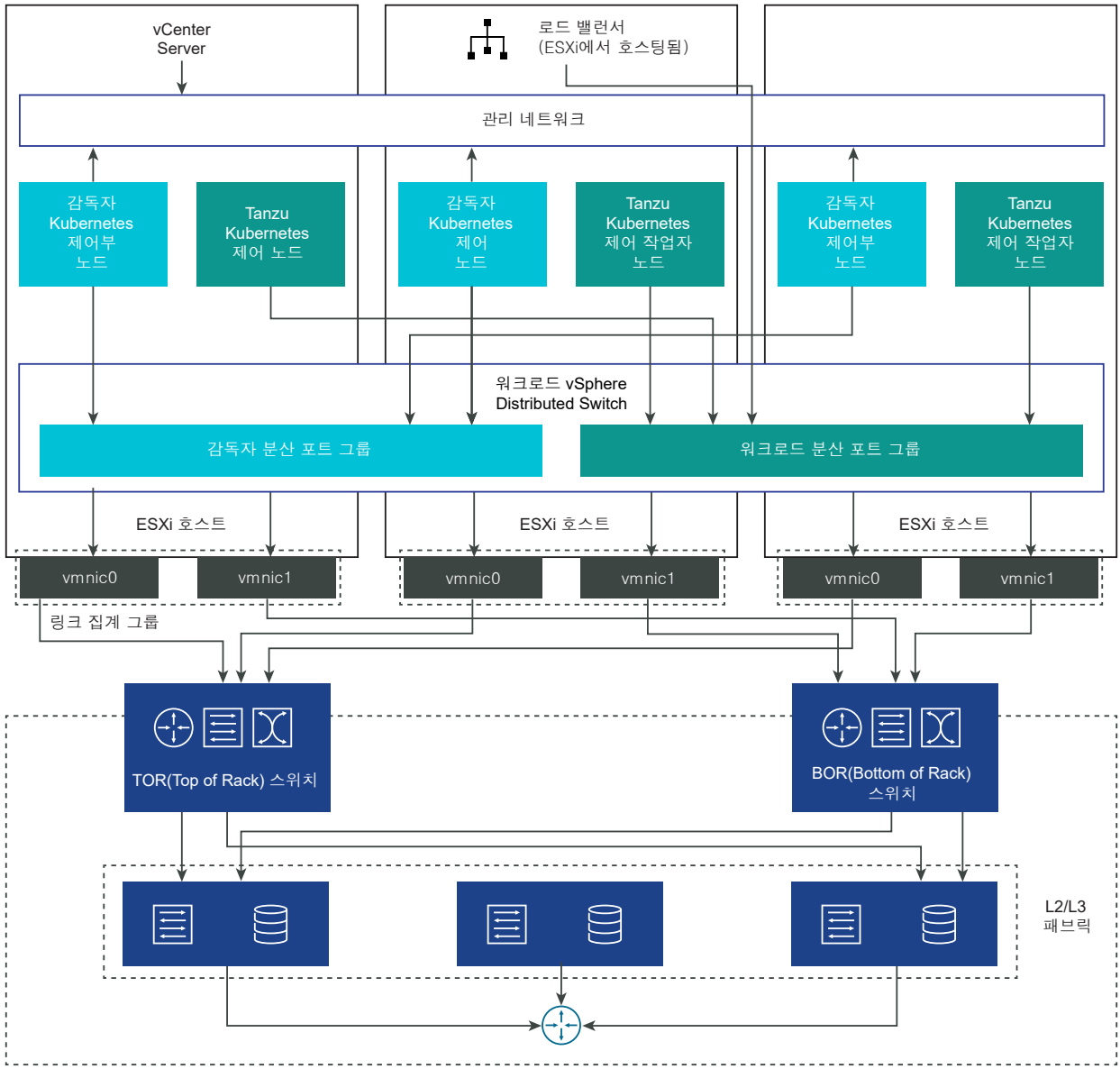
감독자에 대해 구현하는 토폴로지에 따라 하나 이상의 분산 포트 그룹을 워크로드 네트워크로 사용할 수 있습니다. 감독자 제어부 VM에 대한 연결을 제공하는 네트워크를 기본 워크로드 네트워크라고 합니다. 이 네트워크를 감독자의 모든 네임스페이스에 할당하거나 각 네임스페이스에 대해 서로 다른 네트워크를 사용할 수 있습니다. Tanzu Kubernetes Grid 클러스터는 클러스터가 상주하는 네임스페이스에 할당된 워크로드 네트워크에 연결됩니다.

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 구성을 참조하십시오.

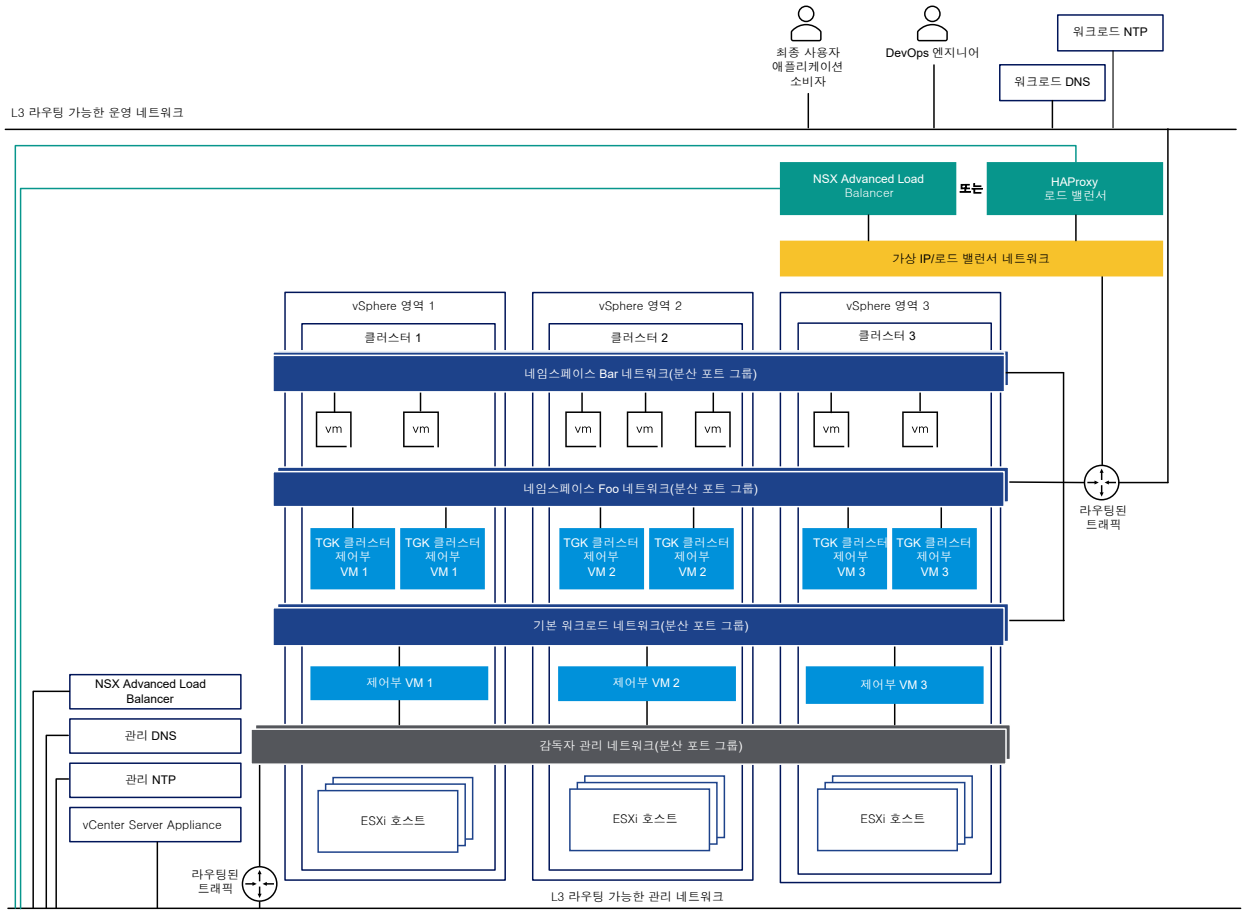
단일 클러스터 감독자 설정에서 감독자는 1개 vSphere 클러스터에서만 지원됩니다. 클러스터의 모든 호스트가 VDS에 연결되어 있어야 합니다.

그림 2-4. 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 2-5. VDS를 사용한 3개 영역 감독자 네트워킹



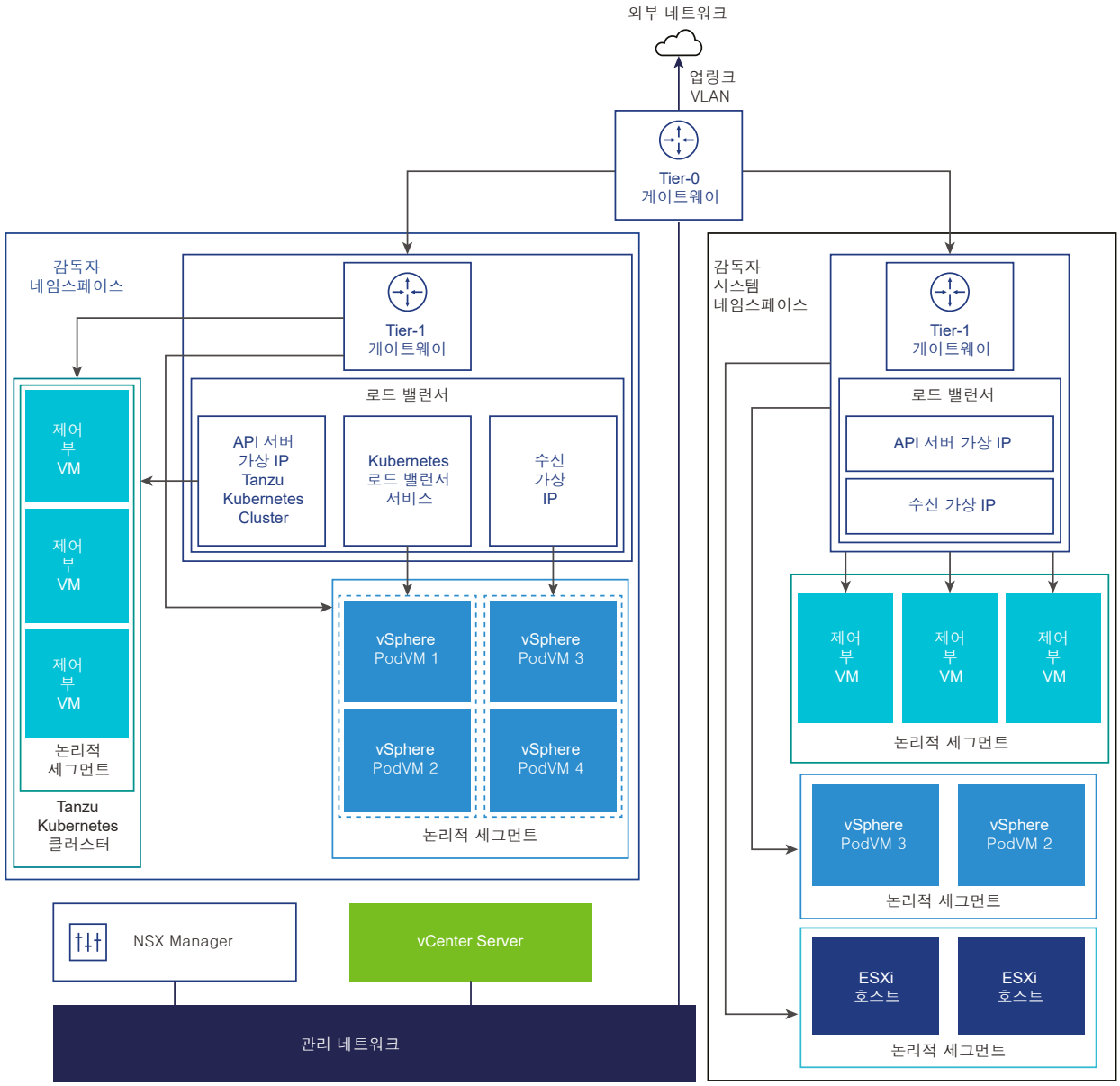
NSX를 사용한 감독자 네트워킹

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 구성을 참조하십시오.

그림 2-6. 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.

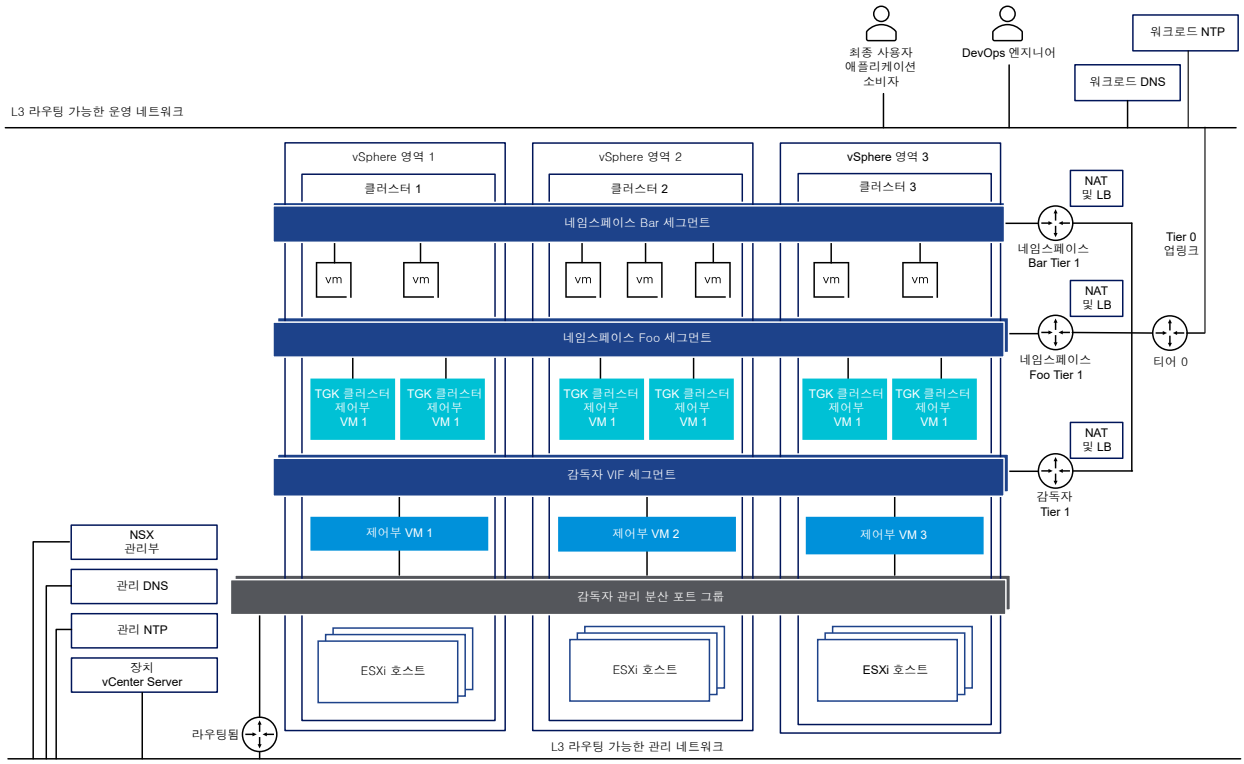
  NCP는 기본적으로 시스템 네임스페이스에 대해 하나의 공유 Tier-1 게이트웨이를 생성하고 각 네임스페이스에 대해 Tier-1 게이트웨이와 로드 밸런서를 생성합니다. Tier-1 게이트웨이는 Tier-0 게이트웨이 및 기본 세그먼트에 연결됩니다.

  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 2-7. 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 `vnic0`은 NSX Advanced Load Balancer Controller에 연결할 수 있는 관리 네트워크에 연결됩니다.
- 나머지 인터페이스인 `vnic1 - 8`은 가상 서비스가 실행되는 데이터 네트워크에 연결됩니다.

서비스 엔진 인터페이스는 올바른 vDS 포트 그룹에 자동으로 연결됩니다. 각 서비스 엔진은 가상 서비스를 1000개까지 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 포트로 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 구성을 참조하십시오.

그림 2-8. NSX 및 NSX Advanced Load Balancer Controller를 사용한 감독자 네트워킹

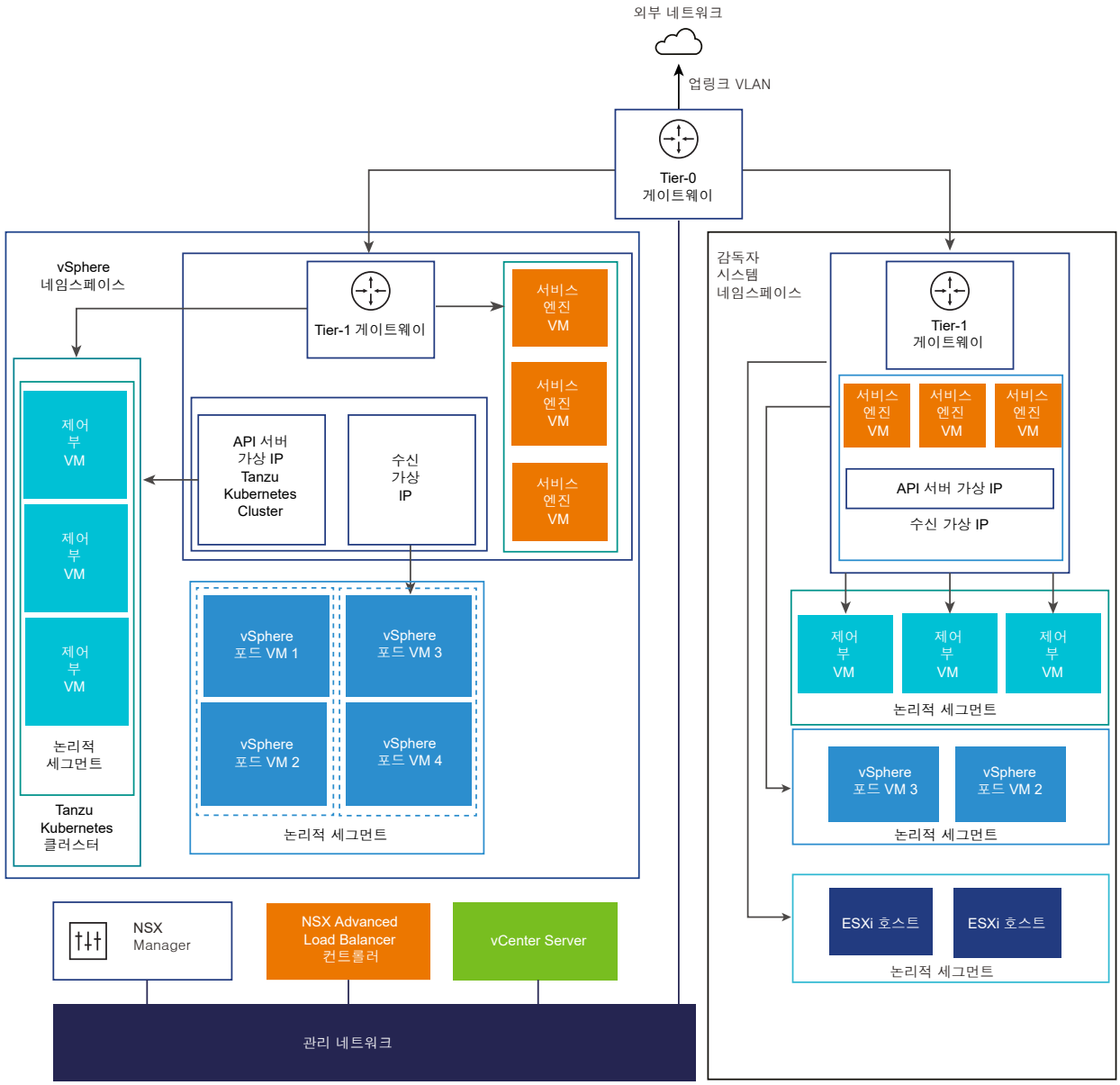
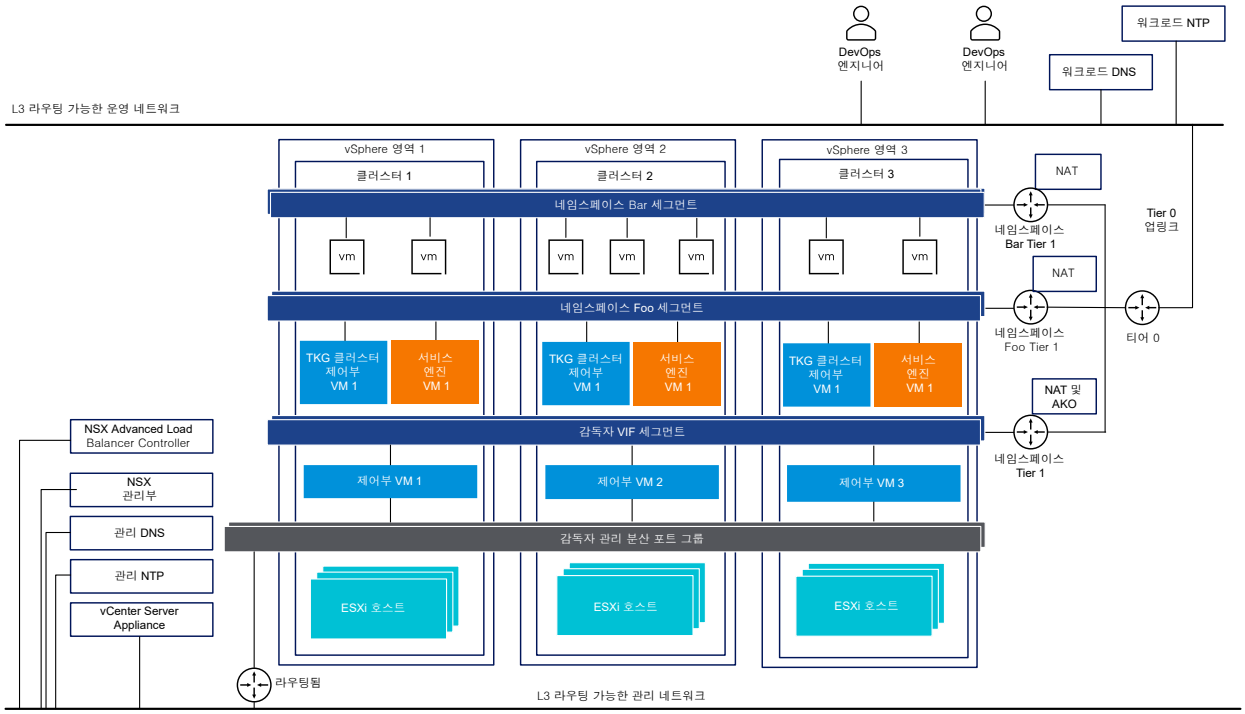


그림 2-9. NSX 및 NSX Advanced Load Balancer Controller를 사용한 3개 영역 감독자 네트워킹



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 가이드를 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 구성을 참조하십시오.

감독자 스토리지

감독자 구성 요소,애플리케이션 및 워크로드는 데이터를 저장하고 검색해야 합니다. 일시적으로 빠른 스토리지가 필요한 애플리케이션 및 개체가 있는 반면, 지속형 스토리지가 필요한 애플리케이션 및 개체도 있습니다.

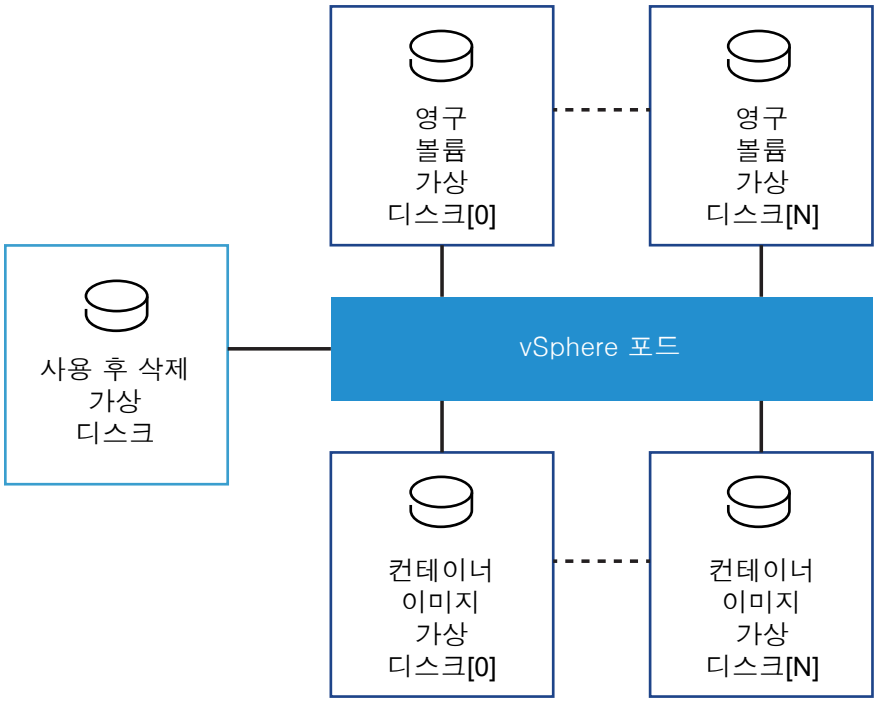
스토리지 정책 정보

감독자는 스토리지 정책을 사용하여 vSphere 환경에서 사용할 수 있는 스토리지와 통합합니다. 정책은 데이터스토어를 대표하여 제어부 VM, vSphere 포드사용 후 삭제 디스크 및 컨테이너 이미지와 같은 구성 요소 및 개체의 스토리지 배치를 관리합니다. 영구 볼륨 및 VM 컨텐츠 라이브러리의 스토리지 배치에 대한 정책도 필요할 수 있습니다. Tanzu Kubernetes Grid 클러스터를 사용하는 경우 스토리지 정책은 Tanzu Kubernetes Grid 클러스터 노드가 배포되는 방식도 지정합니다.

스토리지 정책은 VMFS, NFS, vSAN(vSAN ESA 또는 vVols 포함)과 같은 환경의 모든 공유 데이터스토어를 지원합니다.

vSphere 스토리지 환경 및 DevOps의 요구 사항에 따라 서로 다른 스토리지 클래스에 대해 여러 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.

예를 들어 vSphere 포드가 세 가지 유형의 가상 디스크를 마운트하고 vSphere 스토리지 환경에 Bronze, Silver 및 Gold의 3가지 데이터스토어 클래스가 있는 경우 모든 데이터스토어에 대한 스토리지 정책을 생성할 수 있습니다. 그런 다음 사용 후 삭제 및 컨테이너 이미지 가상 디스크에 대해 Bronze 데이터스토어를 사용하고 영구 볼륨 가상 디스크에 대해 Silver 및 Gold 데이터스토어를 사용할 수 있습니다.



스토리지 정책 생성에 대한 자세한 내용은 "vSphere IaaS 제어부 설치 및 구성" 설명서에서 스토리지 정책 생성을 참조하십시오.

스토리지 정책에 대한 일반적인 정보는 "vSphere 스토리지" 설명서의 스토리지 정책 기반 관리 장을 참조하십시오.

감독자에 대한 스토리지 정책

감독자 수준에서 감독자 제어부 VM에 대한 스토리지 정책을 구성합니다. 또한 배포에서 vSphere 포드를 지원하는 경우 스토리지 정책을 할당하고 사용 후 삭제 디스크 및 컨테이너 이미지에 대한 데이터스토어 위치를 지정합니다. 감독자를 사용하도록 설정한 경우 스토리지를 설정하는 방법에 대한 자세한 내용은 "vSphere IaaS 제어부 설치 및 구성" 설명서를 참조하십시오. 스토리지 설정을 변경하려면 감독자에서 스토리지 설정 변경을 참조하십시오.

제어부 스토리지 정책

이 정책은 정책이 나타내는 데이터스토어에 제어부 VM이 배치되도록 합니다.

사용 후 삭제 가상 디스크

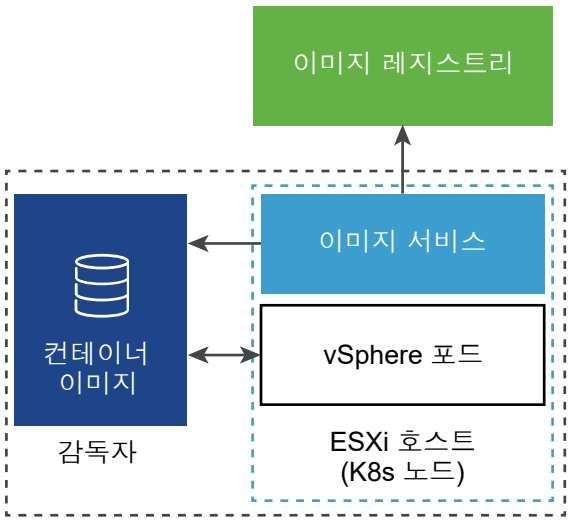
vSphere 포드은 작업 중에, 로그, `emptyDir` 볼륨 및 `ConfigMaps`와 같은 Kubernetes 개체를 저장하기 위해 사용 후 삭제되는 스토리지가 필요합니다. 이 사용 후 삭제 또는 임시 스토리지는 포드가 계속 존재하는 한 지속됩니다. 사용 후 삭제 데이터는 컨테이너를 다시 시작해도 유지되지만 사용 후 삭제 가상 디스크는 포드의 수명이 다하면 사라집니다.

각 포드에는 사용 후 삭제 가상 디스크가 하나씩 있습니다. vSphere 관리자는 감독자에 대한 스토리지를 구성할 때 스토리지 정책을 사용하여 모든 사용 후 삭제 가상 디스크에 대한 데이터스토어 위치를 정의합니다.

컨테이너 이미지 가상 디스크

vSphere 포드 내의 컨테이너는 실행할 소프트웨어가 포함된 이미지를 사용합니다. 포드는 컨테이너에서 사용하는 이미지를 이미지 가상 디스크로 마운트합니다. 포드의 수명 주기가 완료되면 이미지 가상 디스크가 포드에서 분리됩니다.

ESXi 구성 요소인 이미지 서비스는 이미지 레지스트리에서 컨테이너 이미지를 끌어와서 가상 디스크로 변환하여 포드 내에서 실행하는 작업을 담당합니다.



ESXi는 포드에서 실행 중인 컨테이너에 대해 다운로드된 이미지를 캐시할 수 있습니다. 동일한 이미지를 사용하는 후속 포드는 외부 컨테이너 레지스트리가 아닌 로컬 캐시에서 이미지를 끌어옵니다.

워크로드에 대한 영구 스토리지

DevOps가 네임스페이스에서 실행하는 특정 Kubernetes 워크로드에는 데이터를 영구적으로 저장하기 위한 영구 스토리지가 필요합니다.

영구 스토리지는 vSphere 포드, Tanzu Kubernetes Grid 클러스터, VM 및 네임스페이스에서 실행하는 기타 워크로드에서 사용할 수 있습니다. DevOps 팀이 영구 스토리지를 사용할 수 있도록 vSphere 관리자는 다양한 스토리지 요구 사항 및 서비스 클래스를 설명하는 스토리지 정책을 생성합니다. 그런 다음 관리자는 스토리지 정책을 할당하고 네임스페이스 수준에서 스토리지 제한을 구성합니다.

vSphere IaaS control plane가 영구 스토리지에서 작동하는 방식을 이해하려면 스토리지 클래스, 영구 볼륨 및 영구 볼륨 할당과 같은 필수 Kubernetes 개념을 숙지해야 합니다. 자세한 내용은 https://kubernetes.io/docs/home/에서 Kubernetes 설명서를 참조하십시오.

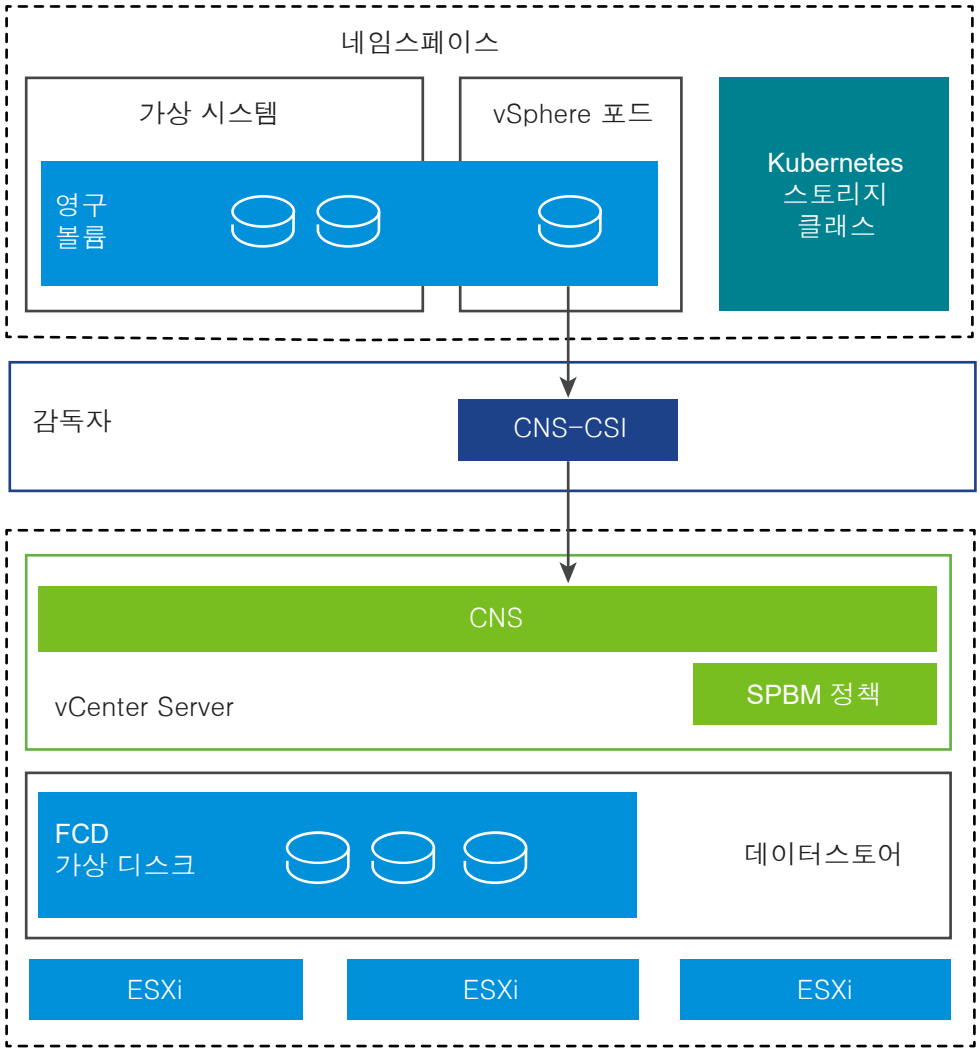
Tanzu Kubernetes Grid 클러스터용 영구 스토리지에 대한 자세한 내용은 Tanzu Kubernetes Grid 클러스터용 스토리지 항목을 참조하십시오.

영구 스토리지 사용에 대한 자세한 내용은 설명서에서 워크로드에 영구 스토리지 사용 "vSphere IaaS 제어부 서비스 및 워크로드" 을 참조하십시오.

DevOps 팀이 영구 스토리지 요구 사항을 위해 vSAN Direct를 사용하는 타사 서비스를 배포할 계획인 경우 설명서에서 vSphere with Taznu에서 상태 저장 서비스 사용 "vSphere IaaS 제어부 서비스 및 워크로드" 을 참조하십시오.

감독자가 vSphere 스토리지와 통합되는 방식

감독자는 몇 가지 구성 요소를 사용하여 vSphere 스토리지와 통합합니다.



vCenter Server의 CNS(클라우드 네이티브 스토리지)

CNS 구성 요소는 vCenter Server에 상주합니다. 이것은 영구 볼륨에 대한 수명 주기 작업과 프로비저닝을 구현하는 vCenter Server 관리의 확장입니다.

영구 볼륨을 프로비저닝할 때 이 구성 요소는 vSphere First Class Disk 기능과 상호 작용하여 볼륨을 지원하는 가상 디스크를 생성합니다. 또한 CNS 서버 구성 요소는 스토리지 정책 기반 관리와 통신하여 디스크에 필요한 서비스 수준을 보장합니다.

CNS는 vSphere 관리자가 vCenter Server를 통해 영구 볼륨 및 이를 지원하는 스토리지 개체를 관리하고 모니터링할 수 있도록 하는 쿼리 작업도 수행합니다.

First Class Disk(FCD)

향상된 가상 디스크라고도 합니다. 이러한 디스크는 데이터스토어 및 백 ReadWriteOnce 영구 볼륨에 상주합니다.

FCD를 사용하는 경우 다음 사항에 유의하십시오.

- FCD는 NFS 4.x 프로토콜을 지원하지 않습니다. 대신 NFS 3을 사용하십시오.

- vCenter Server는 동일한 FCD에서 작업을 직렬화하지 않습니다. 그 결과, 애플리케이션이 동일한 FCD에서 동시에 작업을 수행할 수 없습니다. 복제, 재배치, 삭제, 검색 등의 작업을 서로 다른 스레드에서 동시에 수행하면 예측할 수 없는 결과가 발생하게 됩니다. 문제를 방지하려면 애플리케이션이 동일한 FCD에서 순차적으로 작업을 수행해야 합니다.
- FCD는 관리되는 개체가 아니며 단일 FCD에 대한 다중 쓰기를 보호하는 글로벌 잠금을 지원하지 않습니다. 그 결과 FCD는 동일한 FCD를 관리하는 여러 vCenter Server 인스턴스를 지원하지 않습니다. FCD에서 여러 vCenter Server 인스턴스를 사용해야 하는 경우 다음 옵션이 있습니다.
  - 여러 vCenter Server 인스턴스가 서로 다른 데이터스토어를 관리할 수 있습니다.
  - 여러 vCenter Server 인스턴스가 동일한 FCD에서 작동하지 않습니다.

스토리지 정책 기반 관리

스토리지 정책 기반 관리는 스토리지 정책에 설명된 스토리지 요구 사항에 따라 영구 볼륨 및 해당 백업 가상 디스크의 프로비저닝을 지원하는 vCenter Server 서비스입니다. 프로비저닝 후에 서비스는 스토리지 정책 특성으로 볼륨의 규정 준수를 모니터링합니다. 스토리지 정책 기반 관리에 대한 자세한 내용은 "vSphere 스토리지" 설명서에서 스토리지 정책 기반 관리 장을 참조하십시오.

vSphere CNS-CSI

vSphere CNS-CSI 구성 요소는 CSI(Container Storage Interface) 규격을 준수합니다. 이것은 Kubernetes와 같은 컨테이너 Orchestrator가 영구 스토리지를 프로비저닝하는 데 사용하는 인터페이스를 제공하도록 설계된 업계 표준입니다. CNS-CSI 드라이버는 감독자에서 실행되고 네임스페이스의 Kubernetes 환경에 vSphere 스토리지를 연결합니다. vSphere CNS-CSI는 네임스페이스에서 시작된 모든 스토리지 프로비저닝 요청에 대해 CNS 구성 요소와 직접 통신합니다.

vSphere CNS-CSI에서 지원되는 기능

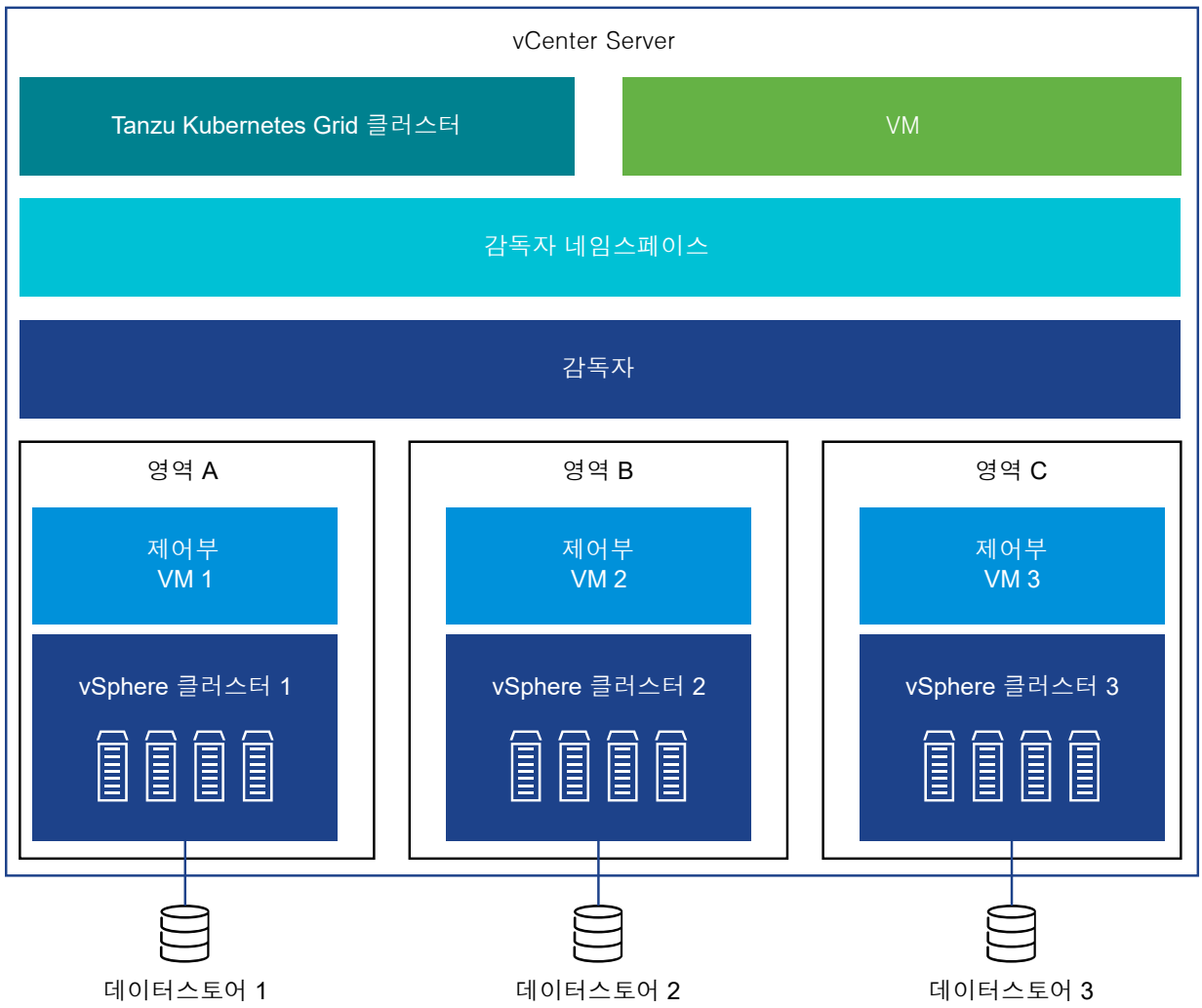
감독자에서 실행되는 vSphere CNS-CSI 구성 요소는 여러 vSphere 및 Kubernetes 스토리지 기능을 지원합니다. 하지만 특정 제한 사항이 적용됩니다.

지원되는 기능	감독자가 있는 vSphere CNS-CSI
vSphere Client의 CNS 지원	예
vSphere Client의 향상된 개체 상태	예(vSAN만)
동적 블록 영구 볼륨(ReadWriteOnce 액세스 모드)	예
동적 파일 영구 볼륨(ReadWriteMany 액세스 모드)	아니요
vSphere 데이터스토어	VMFS, NFS, vSAN(vSAN ESA 포함), vVols
정적 영구 볼륨	예
암호화	아니요
오프라인 볼륨 확장	예
온라인 볼륨 확장	예
볼륨 토폴로지 및 영역	예. 볼륨은 Tanzu Kubernetes Grid 클러스터에서만 사용할 수 있습니다.

지원되는 기능	감독자가 있는 vSphere CNS-CSI
Kubernetes 다중 제어부 인스턴스	예
WaitForFirstConsumer	아니요
VolumeHealth	예
영구 볼륨이 있는 Storage vMotion	아니요

영구 스토리지 및 vSphere 영역이 있는 감독자

3개 영역 감독자는 데이터스토어가 단일 영역의 모든 호스트에서 공유되는 영역 스토리지를 지원합니다.



3개 영역 감독자에 대한 스토리지 리소스를 준비할 때는 다음 사항을 고려하십시오.

- 세 영역 모두의 스토리지 유형이 같을 필요는 없습니다. 단, 세 클러스터 모두에 통일된 스토리지를 사용하면 일관된 성능을 얻을 수 있습니다.
- 3개 영역 감독자의 네임스페이스의 경우 각 클러스터의 공유 스토리지 규정을 준수하는 스토리지 정책을 사용합니다. 스토리지 정책은 토폴로지를 인식해야 합니다.

- 네임스페이스에 할당한 후 스토리지 정책에서 토폴로지 제약 조건을 제거하지 마십시오.
- 영역 데이터스토어를 다른 영역에 마운트하지 마십시오.
- 3개 영역 감독자는 다음 항목을 지원하지 않습니다.
  - 교차 영역 볼륨
  - vSAN 파일 볼륨(ReadWriteMany 볼륨)
  - Register Volume API를 사용한 정적 볼륨 프로비저닝
  - vSAN 데이터 지속성 플랫폼을 사용하는 워크로드
  - vSphere 포드
  - vSAN 확대 클러스터
  - vGPU 및 인스턴스 스토리지가 있는 VM

자세한 내용은 "vSphere IaaS 제어부 서비스 및 워크로드" 설명서의 3개 영역 감독자에서 영구 스토리지 사용을 참조하십시오.

Tanzu Kubernetes Grid 아키텍처 및 구성 요소

3

Tanzu Kubernetes Grid 아키텍처가 무엇이고 감독자 및 해당 구성 요소와 통합되는 방식은 무엇인지 확인하십시오. Tanzu Kubernetes Grid 클러스터에 대한 네트워킹 및 스토리지의 작동 방식과 Tanzu Kubernetes Grid의 고가용성이 무엇이며 어떤 감독자배포가 이를 지원하는지를 알아볼 수 있습니다.

다음으로 아래 항목을 읽으십시오.

- Tanzu Kubernetes Grid 아키텍처
- Tanzu Kubernetes Grid 클러스터 네트워킹
- Tanzu Kubernetes Grid 클러스터용 스토리지
- Tanzu Kubernetes Grid 클러스터를 위한 고가용성
- Tanzu Kubernetes Grid 인증

Tanzu Kubernetes Grid 아키텍처

Tanzu Kubernetes Grid는 Tanzu Kubernetes Grid 클러스터의 셀프 서비스 수명 주기 관리를 제공합니다. Tanzu Kubernetes Grid를 사용하여 Kubernetes 운영자와 개발자에게 친숙한 선언적 방식으로 Tanzu Kubernetes Grid 클러스터를 만들고 관리할 수 있습니다.

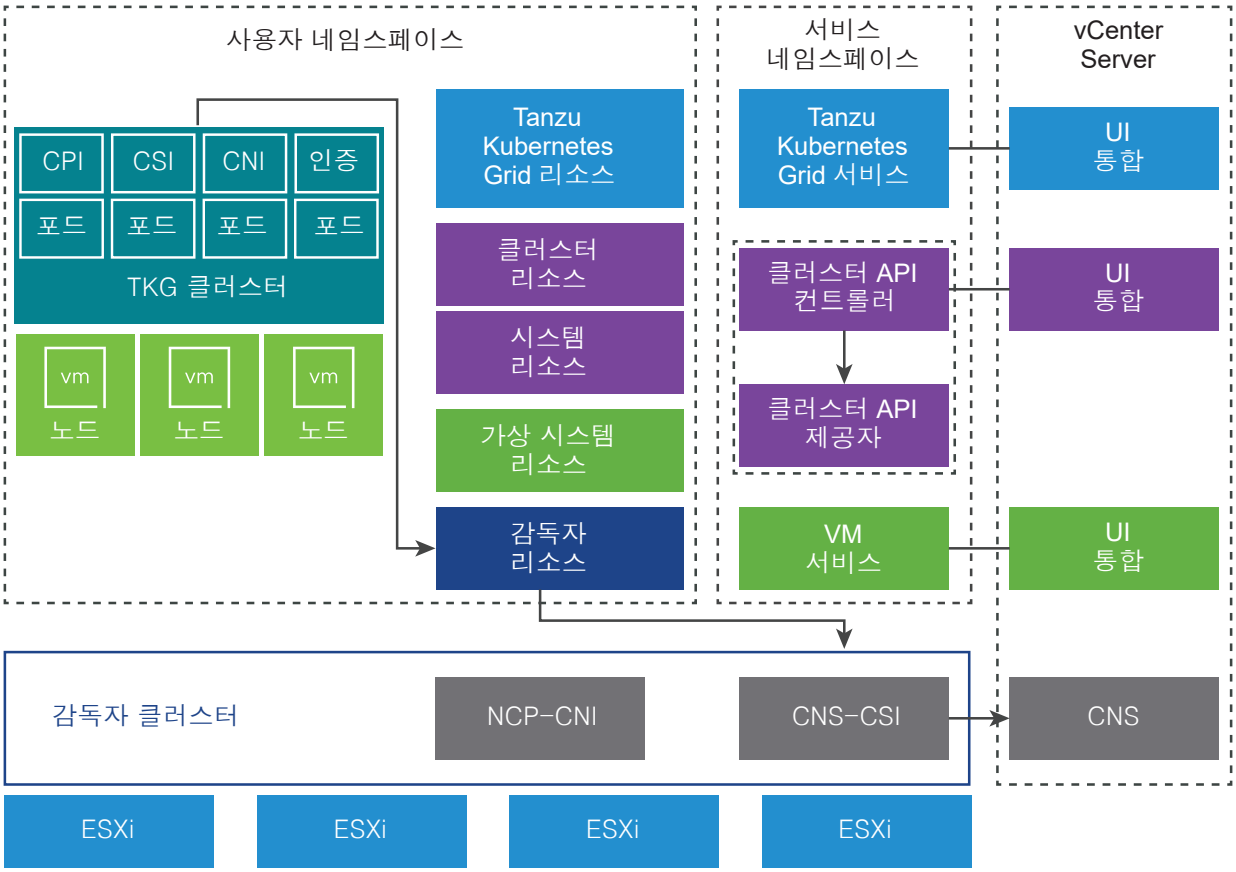
Tanzu Kubernetes Grid 구성 요소

Tanzu Kubernetes Grid는 Tanzu Kubernetes Grid 클러스터의 수명 주기를 관리하기 위한 세 계층의 컨트롤러를 노출합니다.

- Tanzu Kubernetes Grid는 기본 vSphere 네임스페이스 리소스와 통합하는 데 필요한 구성 요소를 포함하는 클러스터를 프로비저닝합니다. 이러한 구성 요소에는 감독자와 통합되는 클라우드 제공자 플러그인이 포함됩니다. 또한 Tanzu Kubernetes Grid 클러스터는 VMware CNS(클라우드 네이티브 스토리지)와 통합된 감독자에 영구 볼륨에 대한 요청을 전달합니다. 워크로드에 대한 영구 스토리지의 내용을 참조하십시오.
- 클러스터 API는 클러스터 생성, 구성 및 관리를 위한 선언적 Kubernetes 스타일의 API를 제공합니다. 클러스터 API에 대한 입력에는 클러스터를 설명하는 리소스, 클러스터를 구성하는 가상 시스템을 설명하는 리소스 집합 및 클러스터 추가 기능을 설명하는 리소스 집합이 포함됩니다.

- 가상 시스템 서비스는 VM 및 연결된 vSphere 리소스 관리를 위한 선언적 Kubernetes 스타일의 API를 제공합니다. 가상 시스템 서비스는 재사용 가능한 추상적인 하드웨어 구성을 나타내는 가상 시스템 클래스의 개념을 소개합니다. 가상 시스템 서비스에서 제공하는 기능은 Tanzu Kubernetes Grid 클러스터를 호스팅하는 제어부 및 작업자 노드 VM의 수명 주기를 관리하는 데 사용됩니다.

그림 3-1. Tanzu Kubernetes Grid 아키텍처 및 구성 요소



Tanzu Kubernetes Grid 클러스터 구성 요소

Tanzu Kubernetes Grid 클러스터에서 실행되는 구성 요소는 인증 및 권한 부여, 스토리지 통합, 포드 네트워킹 및 로드 밸런싱의 네 가지 영역에 걸쳐 있습니다.

- 인증 Webhook: 사용자 인증 토큰을 검증하기 위해 클러스터 내부의 포드로 실행되는 Webhook입니다.
- 컨테이너 스토리지 인터페이스 플러그인: 감독자를 통해 CNS와 통합되는 반가상화 CSI 플러그인입니다.
- 컨테이너 네트워크 인터페이스 플러그인: 포드 네트워킹을 제공하는 CNI 플러그인입니다.
- 클라우드 제공자 구현: Kubernetes 로드 밸런서 서비스 생성을 지원합니다.

Tanzu Kubernetes Grid API

Tanzu Kubernetes Grid API를 사용하여 Tanzu Kubernetes Grid 클러스터를 프로비저닝하고 관리할 수 있습니다. kubectl 및 YAML을 사용하여 호출하는 선언적 API입니다. 감독자 API 끝점 IP에서 VMware 확장 kubectl 실행 파일을 다운로드할 수 있습니다.

선언적 API를 사용하여 시스템에 대한 명령형 명령을 수행하는 대신 Tanzu Kubernetes Grid 클러스터의 원하는 상태(노드 수, 사용 가능한 스토리지, VM 크기, Kubernetes 소프트웨어 버전)를 지정합니다. Tanzu Kubernetes Grid는 원하는 상태와 일치하는 클러스터를 프로비저닝하는 작업을 수행합니다.

Tanzu Kubernetes Grid API를 호출하려면 YAML 파일을 사용하여 kubectl을 호출하고 이를 통해 API를 호출합니다. 클러스터가 생성되면 YAML을 업데이트하여 클러스터를 업데이트합니다.

Tanzu Kubernetes Grid 클러스터 네트워킹

Tanzu Kubernetes Grid에서 프로비저닝된 Tanzu Kubernetes Grid 클러스터는 Antrea(기본값) 및 Calico라는 두 가지 CNI 옵션을 지원합니다. 둘 다 클러스터 포드, 서비스 및 수신을 위한 네트워킹을 제공하는 오픈 소스 소프트웨어입니다.

Tanzu Kubernetes Grid에서 프로비저닝된 Tanzu Kubernetes Grid 클러스터는 다음 CNI(Container Network Interface) 옵션을 지원합니다.

- Antrea
- Calico

Antrea는 새 Tanzu Kubernetes Grid 클러스터에 대한 기본 CNI입니다. Antrea를 사용하는 경우 클러스터 프로비저닝 중에 CNI로 지정할 필요가 없습니다. Calico를 CNI로 사용하기 위해 다음 두 가지 옵션을 사용할 수 있습니다.

- 클러스터 YAML에서 직접 CNI를 지정합니다. v1alpha3 예시: 사용자 지정 네트워크가 있는 TKC를 참조하십시오.
- 기본 CNI를 변경합니다. v1beta1 예시: Calico CNI를 사용하는 클러스터를 참조하십시오.

참고 기본 CNI로 Antrea를 사용하려면 Tanzu Kubernetes Grid 클러스터에 대한 최소 버전의 OVA 파일이 필요합니다. 감독자에서 TKG 2 클러스터 업데이트를 참조하십시오.

이 표에는 Tanzu Kubernetes Grid 클러스터 네트워킹 기능과 구현이 요약되어 있습니다.

표 3-1. Tanzu Kubernetes Grid 클러스터 네트워킹

끝점	제공자	설명
포드 연결	Antrea 또는 Calico	포드용 컨테이너 네트워크 인터페이스입니다. Antrea는 Open vSwitch를 사용합니다. Calico는 BGP와 함께 Linux 브리지를 사용합니다.
서비스 유형: ClusterIP	Antrea 또는 Calico	클러스터 내에서만 액세스할 수 있는 기본 Kubernetes 서비스 유형입니다.

표 3-1. Tanzu Kubernetes Grid 클러스터 네트워킹 (계속)

끝점	제공자	설명
서비스 유형: NodePort	Antrea 또는 Calico	Kubernetes 네트워크 프록시에 의해 각 작업자 노드에 열린 포트를 통한 외부 액세스를 허용합니다.
서비스 유형: LoadBalancer	NSX-T 로드 밸런서, NSX Advanced Load Balancer, HAProxy	NSX-T의 경우, 서비스 유형 정의당 하나의 가상 서버입니다. NSX Advanced Load Balancer는 이 설명서에서 해당 섹션을 참조하십시오. **참고** 일부 로드 밸런싱 기능은 HAProxy에서 사용할 수 없습니다(예: 정적 IP 지원).
클러스터 수신	타사 수신 컨트롤러	인바운드 포드 트래픽을 위한 라우팅, Contour와 같은 타사 수신 컨트롤러를 사용할 수 있습니다.
네트워크 정책	Antrea 또는 Calico	선택한 포드 및 네트워크 끝점 사이에서 허용되는 트래픽을 제어합니다. Antrea는 Open vSwitch를 사용합니다. Calico는 Linux IP 테이블을 사용합니다.

Tanzu Kubernetes Grid 클러스터용 스토리지

Tanzu Kubernetes Grid 클러스터는 감독자 네임스페이스에서 실행되는 일부 다른 구성 요소 및 워크로드와 마찬가지로 영구 스토리지가 필요합니다.

Tanzu Kubernetes Grid 클러스터에 대한 스토리지 정책

Tanzu Kubernetes Grid 클러스터에 영구 스토리지 리소스를 제공하기 위해 vSphere 관리자는 다양한 스토리지 요구 사항을 설명하는 스토리지 정책을 구성합니다. 그런 다음 관리자는 스토리지 정책을 Tanzu Kubernetes Grid 클러스터가 배포된 네임스페이스에 추가합니다. 네임스페이스에 표시되는 스토리지 정책은 네임스페이스가 영구 스토리지에 대해 액세스하고 사용할 수 있는 데이터스토어를 결정합니다. 또한 클러스터 노드 및 워크로드가 vSphere 스토리지 환경에 배치되는 방식을 지정합니다.

네임스페이스에 할당된 스토리지 정책을 기반으로 vSphere IaaS control plane는 일치하는 Kubernetes 스토리지 클래스를 생성하고 이는 네임스페이스에 자동으로 나타납니다. 또한 이 네임스페이스의 Tanzu Kubernetes Grid 클러스터에도 전파됩니다.

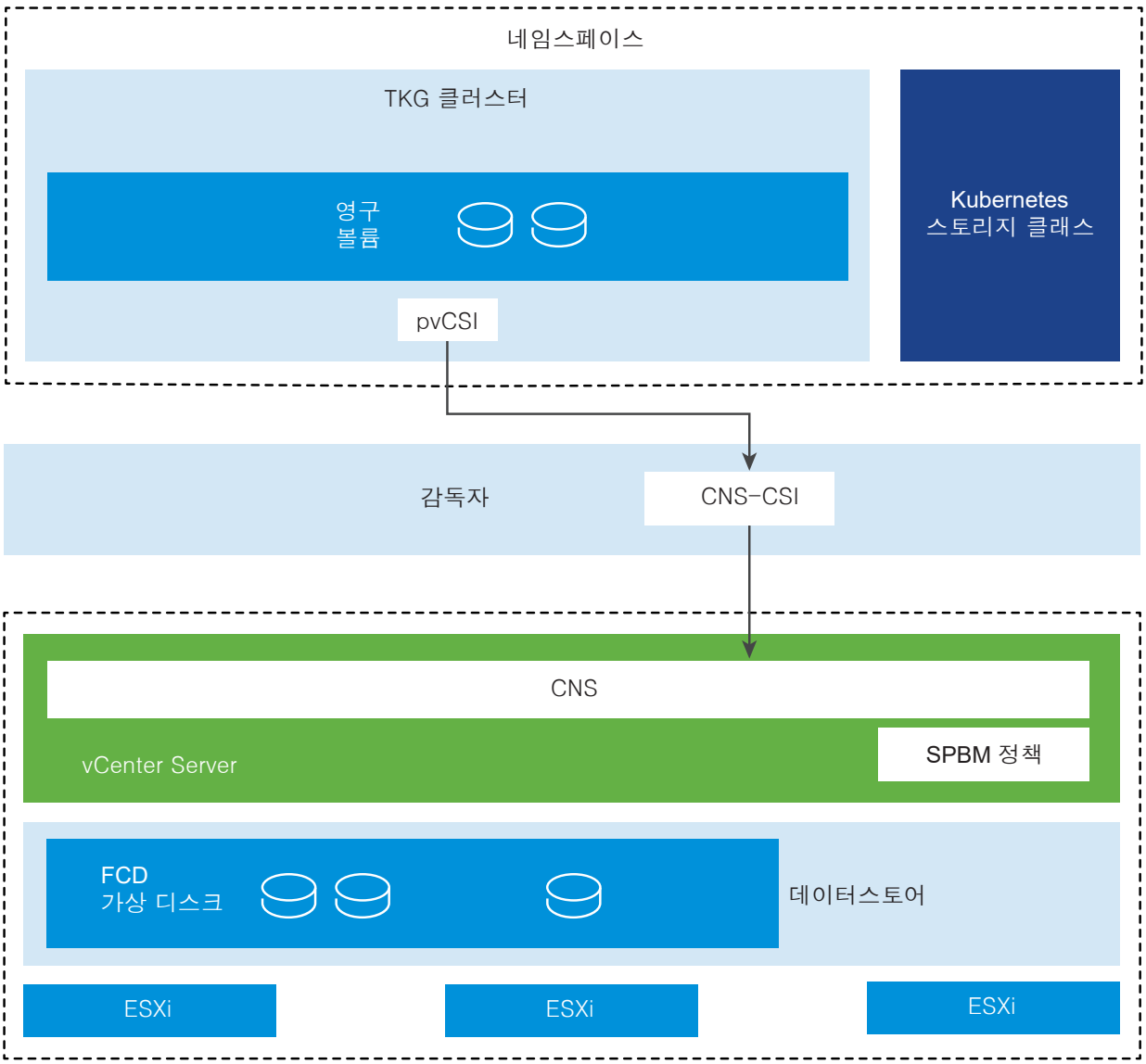
Tanzu Kubernetes Grid 클러스터에서 스토리지 클래스는 두 가지 버전(하나는 `Immediate`, 다른 하나는 `WaitForFirstConsumer` 바인딩 모드)으로 나타납니다. DevOps 팀이 선택하는 버전은 요구 사항에 따라 다릅니다.

Tanzu Kubernetes Grid 클러스터의 스토리지 클래스에 대한 자세한 내용은 영구 볼륨에 대한 스토리지 클래스 사용을 참조하십시오.

Tanzu Kubernetes Grid 클러스터가 vSphere 스토리지와 통합되는 방식

감독자 및 vSphere 스토리지와 통합하기 위해 Tanzu Kubernetes Grid 클러스터는 pvCSI(반가상화 CSI)를 사용합니다.

pvCSI는 Tanzu Kubernetes Grid 클러스터에 대해 수정된 vSphere CNS-CSI 드라이버의 버전입니다. pvCSI는 Tanzu Kubernetes Grid 클러스터에 상주하며 Tanzu Kubernetes Grid 클러스터에서 시작되는 모든 스토리지 관련 요청을 담당합니다. 요청은 CNS-CSI로 전달된 다음 vCenter Server의 CNS로 전파됩니다. 결과적으로 pvCSI는 CNS 구성 요소와 직접적으로 통신하지 않지만 대신 CNS-CSI를 통해 모든 스토리지 프로비저닝 작업을 수행합니다. CNS-CSI와 달리 pvCSI에는 인프라 자격 증명이 필요하지 않습니다. pvCSI는 네임스페이스의 서비스 계정으로 구성됩니다.

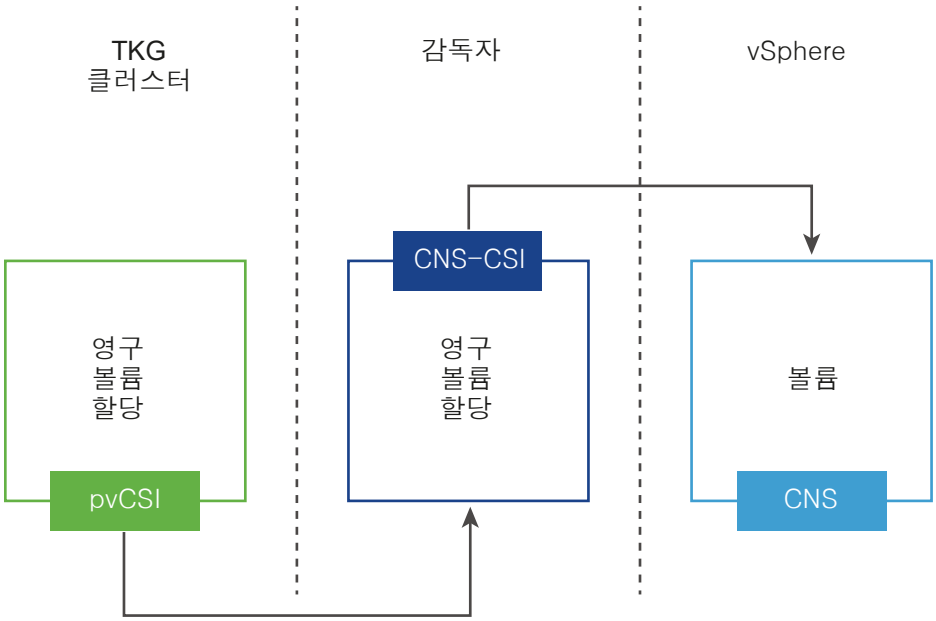


vSphere 스토리지와 통합하는 데 사용되는 감독자 구성 요소에 대한 자세한 내용은 워크로드에 대한 영구 스토리지 항목을 참조하십시오.

영구 볼륨이 생성되는 방식

다음은 DevOps 엔지니어가 Tanzu Kubernetes Grid 클러스터 내에서 스토리지 관련 작업을 수행할 때 서로 다른 구성 요소가 어떤 방식으로 상호 작용하는지 보여 줍니다. 예를 들어 PVC(영구 볼륨 할당)가 생성됩니다.

DevOps 엔지니어가 Tanzu Kubernetes Grid 클러스터에서 명령줄을 사용하여 PVC를 생성합니다. 이 작업을 수행하면 감독자에서 일치하는 PVC가 생성되고 CNS-CSI가 트리거됩니다. CNS-CSI는 CNS 볼륨 생성 API를 호출합니다.



볼륨 생성이 완료되면 작업이 감독자를 통해 Tanzu Kubernetes Grid 클러스터로 다시 전파됩니다. 이 전파의 결과로 사용자는 감독자에서 바인딩된 상태의 영구 볼륨과 영구 볼륨 할당을 볼 수 있습니다. 또한 Tanzu Kubernetes Grid 클러스터에서 바인딩된 상태의 영구 볼륨과 영구 볼륨 할당을 볼 수 있습니다.

pvCSI에서 지원되는 기능

Tanzu Kubernetes Grid 클러스터에서 실행되는 pvCSI 구성 요소는 여러 vSphere 및 Kubernetes 스토리지 기능을 지원합니다.

지원되는 기능	Tanzu Kubernetes Grid 클러스터가 있는 pvCSI
vSphere Client의 CNS 지원	예
vSphere Client의 향상된 개체 상태	예(vSAN만)
동적 블록 영구 볼륨(ReadWriteOnce 액세스 모드)	예
동적 파일 영구 볼륨(ReadWriteMany 액세스 모드)	예(vSAN 파일 서비스 사용)
vSphere 데이터스토어	VMFS/NFS/vSAN/vVols
정적 영구 볼륨	예
암호화	아니요
오프라인 볼륨 확장	예

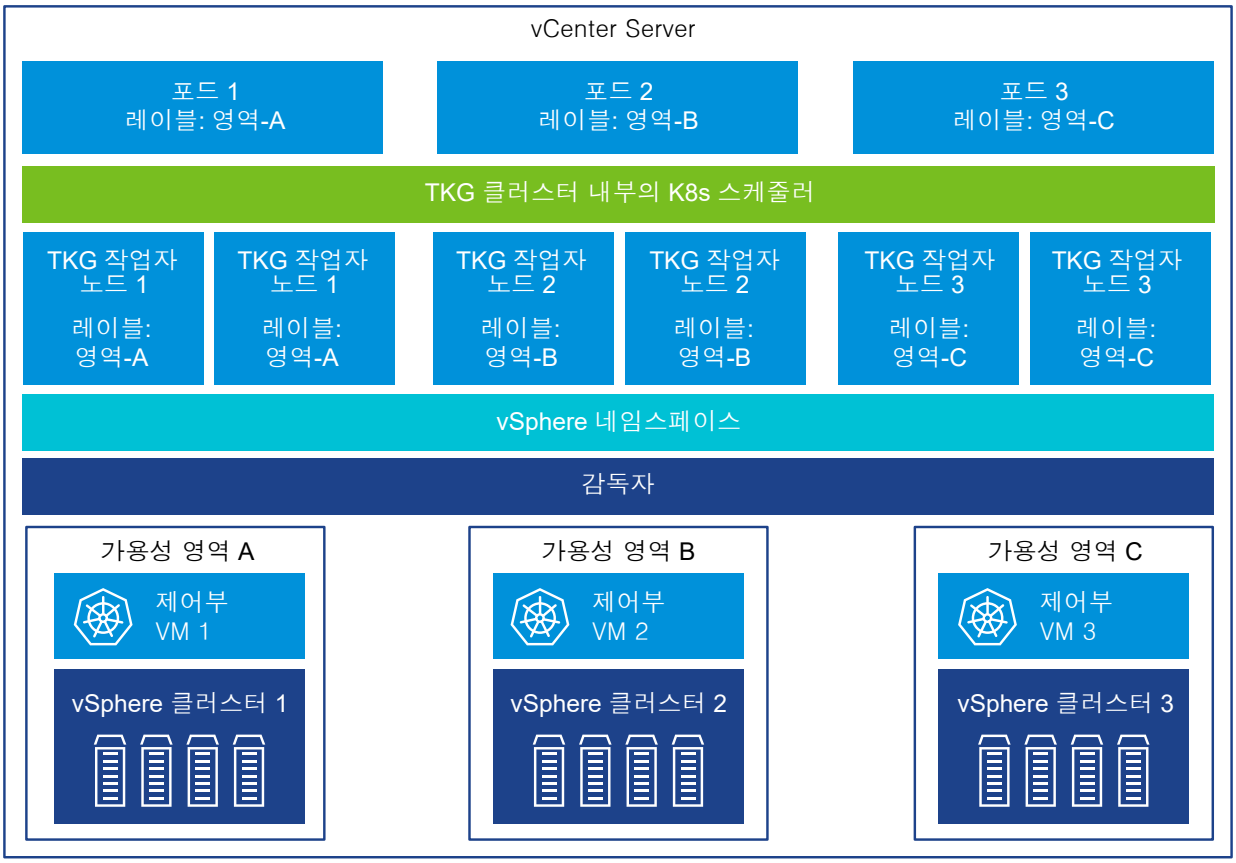
지원되는 기능	Tanzu Kubernetes Grid 클러스터가 있는 pvCSI
온라인 볼륨 확장	예
볼륨 토폴로지 및 영역	예
Kubernetes 다중 제어부 인스턴스	예
WaitForFirstConsumer	예
VolumeHealth	예
영구 볼륨이 있는 Storage vMotion	아니요

Tanzu Kubernetes Grid 클러스터를 위한 고가용성

Tanzu Kubernetes Grid 클러스터를 3개의 vSphere 영역 감독자에 배포하여 고가용성을 제공할 수 있습니다. vSphere 영역은 vSphere 클러스터에 매핑됩니다. 즉, 감독자를 3개의 vSphere 영역에 배포하면 3개의 기본 vSphere 클러스터의 리소스가 모두 활용됩니다. 이렇게 하면 Tanzu Kubernetes Grid 클러스터 내에서 실행되는 Kubernetes 워크로드를 보호하여 vSphere 클러스터 수준에서 장애가 발생하지 않도록 할 수 있습니다. 단일 영역 배포에서 Tanzu Kubernetes Grid 클러스터에 대한 고가용성은 vSphere HA에 의해 ESXi 호스트 수준에서 제공됩니다.

3개 영역 감독자에서, Tanzu Kubernetes Grid 클러스터의 제어부 노드는 vSphere 영역 전체에 자동으로 배치됩니다. 그러나 worker 노드가 영역에 분산되는 방식은 사용자가 제어할 수 있습니다. Tanzu Kubernetes Grid 클러스터의 worker 노드에 대한 노드 풀 개체를 정의하고 각 vSphere 영역을 각 노드 풀 내의 장애 도메인에 매핑할 수 있습니다. 이러한 방식으로 클러스터 API는 worker 노드를 vSphere 영역 전반에 분산합니다. 하나 또는 모든 노드 풀에 대해 장애 도메인 지정을 건너뛰면 클러스터 API가 자동으로 노드 풀을 영역 전체에 분산시킵니다.

그림 3-2. 여러 영역의 Tanzu Kubernetes Grid 클러스터에 대한 고가용성



Tanzu Kubernetes Grid 인증

다양한 인증 메커니즘에 대해 알아보고 Tanzu Kubernetes Grid 클러스터에서 사용하는 인증을 알아보십시오.

감독자에 연결

DevOps 엔지니어는 감독자에 연결하여 Tanzu Kubernetes Grid 클러스터를 프로비저닝할 수 있습니다. vSphere 관리자가 설정한 사용 권한이 있는 네임스페이스에만 액세스할 수 있습니다.

Kubernetes 제어부 IP의 감독자 또는 프로비저닝된 Tanzu Kubernetes Grid 클러스터에 연결하려면 다음 두 가지 방법을 사용할 수 있습니다.

- vCenter Single Sign-On 및 vSphere에 대한 Kubernetes CLI 도구. 이 경우 10시간마다 만료되는 인증 토큰이 생성됩니다.
- 감독자 및 Tanzu CLI에 등록된 OIDC 제공자의 자격 증명. OIDC 제공자가 있는 세션은 제공자 자체의 설정에 의해 제어됩니다.

자세한 내용은 "vSphere IaaS 제어부에서 TKG 서비스 사용" 설명서를 참조하십시오.

Tanzu Kubernetes Grid 클러스터에 연결

DevOps 엔지니어는 프로비저닝된 Tanzu Kubernetes Grid 클러스터에 연결하여 운영 및 관리할 수도 있습니다. Tanzu Kubernetes Grid 클러스터가 프로비저닝된 vSphere 네임스페이스에 대한 편집 권한이 사용자 계정에 부여되면 계정이 `cluster-admin` 역할에 할당됩니다. 또는 `kubernetes-admin` 사용자를 사용하여 Tanzu Kubernetes Grid 클러스터에 연결할 수도 있습니다. 사용자 또는 그룹을 기본 또는 사용자 지정 포드 보안 정책에 바인딩하여 개발자에게 Tanzu Kubernetes Grid 클러스터에 대한 액세스 권한을 부여할 수도 있습니다. 자세한 내용은 "vSphere IaaS 제어부에서 TKG 서비스 사용" 설명서를 참조하십시오.

감독자 배포 옵션

4

감독자 배포 및 구성을 위한 옵션을 확인하십시오. 감독자에 대해 구현하는 네트워킹 스택 또는 배포 옵션에 따라 지원되는 토폴로지와 지원되는 워크로드 유형이 다릅니다.

다음으로 아래 항목을 읽으십시오.

- 감독자 영역 및 클러스터 배포
- VDS 네트워킹 및 NSX Advanced Load Balancer를 사용하는 감독자대한 토폴로지
- 감독자를 네트워킹 스택으로 사용하는 1영역 NSX의 토폴로지
- NSX를 네트워킹 스택 및 NSX Advanced Load Balancer로 사용하는 1개 영역 감독자의 토폴로지
- HAProxy 로드 밸런서 배포를 위한 토폴로지

감독자 영역 및 클러스터 배포

vSphere 영역에 매핑된 3개의 vSphere 클러스터에 감독자를 배포하는 것과 하나의 vSphere 영역에 매핑되는 단일 감독자 클러스터 배포 간의 차이점을 알아봅니다.

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.

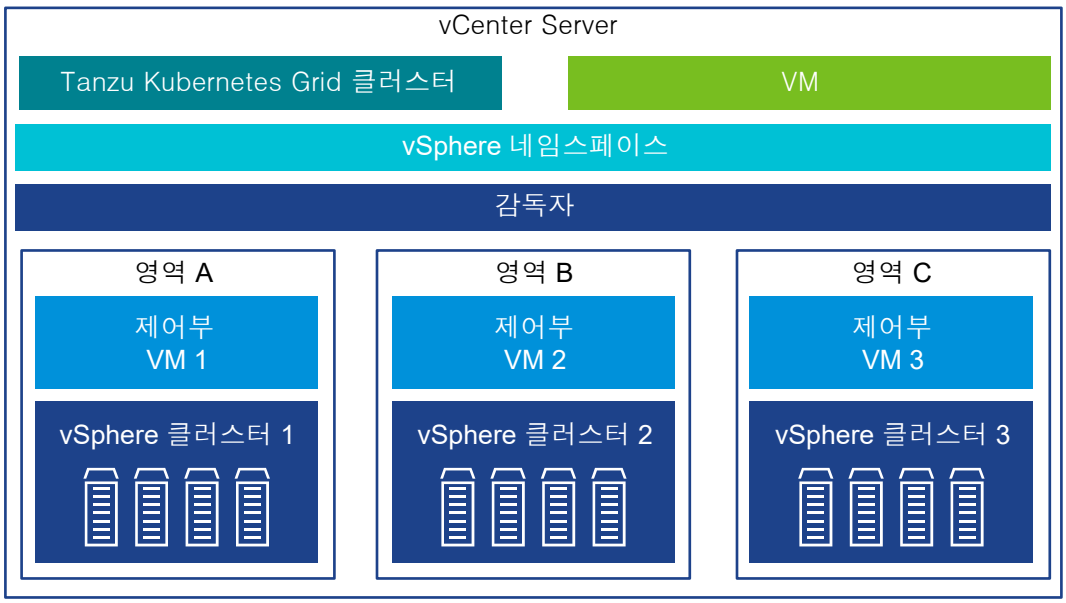
클러스터 수준 HA를 위한 3영역 감독자 배포

3개의 vSphere 영역에 매핑된 3개의 vSphere 클러스터에서 vSphere IaaS control plane를 사용하도록 설정할 수 있습니다. 각 vSphere 클러스터를 독립 장애 도메인으로 구성하고 하나의 vSphere 영역에 매핑합니다. 3영역 배포에서는 vSphere 클러스터 3개 모두가 하나의 감독자가 됩니다. 3영역 배포에서는 다음이 가능합니다.

- 각 vSphere 클러스터가 독립적인 장애 도메인이므로 감독자에 클러스터 수준의 고가용성을 제공할 수 있습니다.
- Tanzu Kubernetes Grid 클러스터의 노드를 vSphere 영역 3개 모두에 분산하여 vSphere 클러스터 수준에서 Kubernetes 워크로드에 HA를 제공할 수 있습니다.
- 3개의 vSphere 클러스터 각각에 호스트를 추가하여 감독자를 확장할 수 있습니다.

Tanzu Kubernetes Grid클러스터, vSphere 포드 및 VM을 사용하여 3영역 감독자에서 워크로드를 실행할 수 있습니다.

그림 4-1. 3영역 감독자 배포



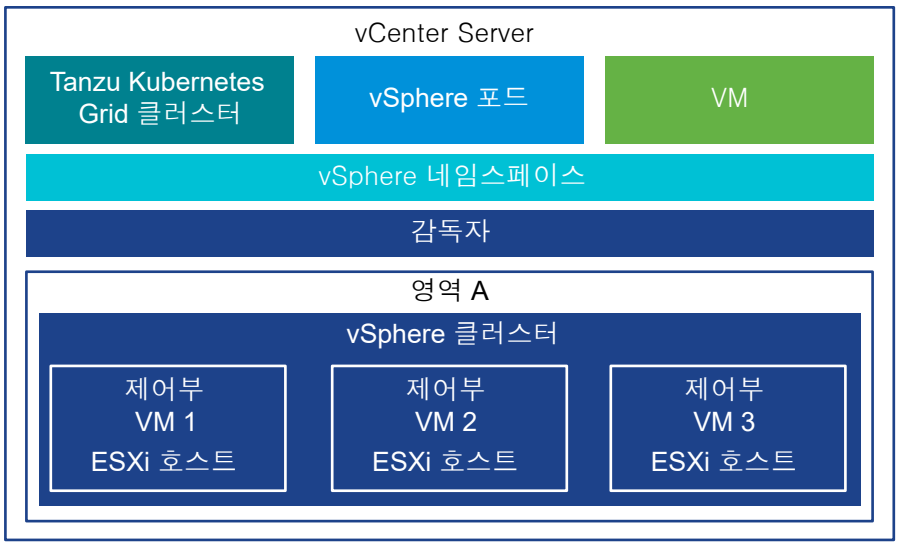
물리적 사이트 간에 vSphere 영역 배치

사이트 간의 지연 시간이 100ms를 초과하지 않는 한 여러 물리적 사이트에 vSphere 영역을 분산할 수 있습니다. 예를 들어 vSphere 영역을 두 개의 물리적 사이트(첫 번째 사이트의 vSphere 영역 하나, 두 번째 사이트의 vSphere 영역 두 개)에 분산할 수 있습니다.

감독자의 단일 클러스터 배포

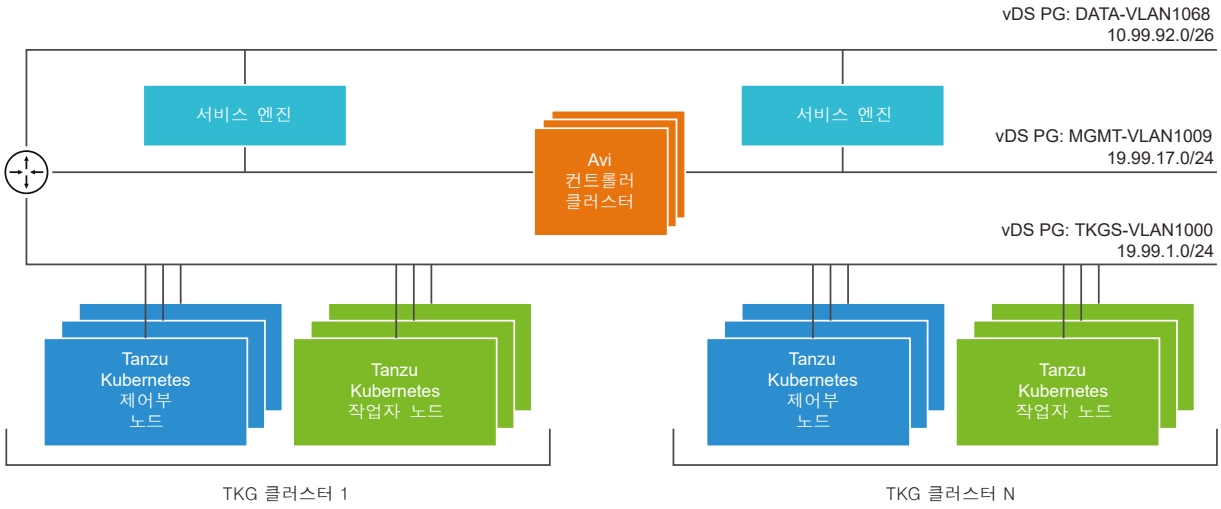
단일 vSphere 클러스터에서 감독자를 사용하도록 설정할 수 있습니다. 이 경우 감독자에 대해 단일 영역이 자동으로 생성되거나 미리 생성해둔 영역을 사용할 수 있습니다. 단일 클러스터 배포에서는 여전히 vSphere HA를 통해 클러스터 수준의 고가용성을 유지하며 감독자에 매핑되는 vSphere 클러스터에 호스트를 추가해야만 vSphere IaaS control plane 설정을 확장할 수 있습니다. 단일 클러스터 배포에서는 VM 서비스를 통해 배포된 vSphere 포드, Tanzu Kubernetes Grid 클러스터 및 VM에서 워크로드를 실행할 수 있습니다.

그림 4-2. 단일 클러스터 감독자 배포



VDS 네트워킹 및 NSX Advanced Load Balancer를 사용하는 감독자대한 토폴로지

Avi 컨트롤러는 항상 vCenter Server, ESXi 호스트 및 감독자 제어부 노드와 상호 작용할 수 있는 관리 네트워크에 배포됩니다. 서비스 엔진은 관리 네트워크 및 데이터 네트워크에 대한 인터페이스와 함께 배포됩니다.



관리 네트워크(예: `MGMT-VLAN1009`)는 컨트롤러가 상주하고 서비스 엔진의 관리 인터페이스가 연결되는 곳입니다.

데이터 네트워크(예: `DATA-VLAN1068`)는 VIP 배치를 위해 서비스 엔진 인터페이스가 연결되는 곳입니다. 클라이언트 트래픽은 VIP에 도달하고 서비스 엔진은 이 네트워크를 통해 트래픽을 워크로드 네트워크 IP로 로드 밸런싱합니다.

워크로드 네트워크(예: `TKGS-VLAN1000`)는 Tanzu Kubernetes Grid 클러스터가 실행되는 곳입니다. 서비스 엔진에는 워크로드 네트워크에 대한 인터페이스가 필요하지 않습니다.

서비스 엔진은 단일 암 모드로 실행됩니다. 서비스 엔진은 로드 밸런싱된 트래픽을 라우터를 통해 워크로드 네트워크로 라우팅합니다. 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.

이 토폴로지에서는 서비스 엔진을 단일 네트워크에 배치할 수 있습니다. 서비스 엔진 생성 및 네트워크 연결은 Avi 컨트롤러에 의해 자동화됩니다.

NSX Advanced Load Balancer 설치 및 구성에 대한 자세한 내용은 NSX Advanced Load Balancer 설치 및 구성을 참조하십시오.

NSX Advanced Load Balancer 구성 요소

Avi Load Balancer라고도 하는 NSX Advanced Load Balancer의 구성 요소에는 컨트롤러 클러스터, 서비스 엔진(데이터부) VM 및 AKO(Avi Kubernetes Operator)가 포함되어 있습니다.

NSX Advanced Load Balancer 구성 요소 설치 및 구성에 대한 자세한 내용은 NSX Advanced Load Balancer 설치 및 구성을 참조하십시오.

컨트롤러

컨트롤러라고도 하는 NSX Advanced Load Balancer 컨트롤러는 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.

vSphere에서 컨트롤러 VM을 배포하고 구성한 후 컨트롤러 클러스터를 배포하여 HA용 제어부 클러스터를 설정할 수 있는지 확인합니다.

클라우드는 NSX Advanced Load Balancer가 설치되거나 작동되는 환경을 위한 컨테이너입니다. 컨트롤러의 초기 구성 중에 이름이 **기본 클라우드**인 클라우드가 자동으로 생성됩니다. **기본 클라우드**를 **VMware vCenter** 클라우드로 사용하거나 **VMware vCenter** 유형의 사용자 지정 클라우드를 하나 이상 생성할 수 있습니다.

VMware vCenter 유형의 클라우드를 구성하면 고유한 vCenter 및 해당 vCenter 내의 데이터 센터와 연결됩니다. 해당 vCenter 및 데이터 센터에서 사용할 수 있는 모든 리소스를 클라우드에서 사용할 수 있습니다.

로드 밸런서가 여러 vCenter 서버 또는 여러 데이터 센터에 서비스를 제공할 수 있도록 하려면 각 vCenter 및 데이터 센터 조합에 대해 하나씩 **VMware vCenter** 유형의 사용자 지정 클라우드를 여러 개 생성할 수 있습니다. 그러면 로드 밸런서 인스턴스 수가 줄어들고 환경을 지원하는 데 필요한 코어 수가 줄어들기 때문에 작업 부담이 줄어듭니다. 클라우드에 대한 자세한 내용은 NSX Advanced Load Balancer 설명서를 참조하십시오.

서비스 엔진

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

서비스 엔진에는 두 가지 유형의 네트워크 인터페이스가 있습니다.

- 첫 번째 네트워크 인터페이스인 VM의 `vnic0`은 NSX Advanced Load Balancer 컨트롤러에 연결할 수 있는 관리 네트워크에 연결됩니다.
- 나머지 인터페이스인 `vnic1 - 9`은 가상 서비스가 실행되는 데이터 네트워크에 연결됩니다.

서비스 엔진 인터페이스는 올바른 vDS 포트 그룹에 자동으로 연결됩니다. 사용되지 않은 인터페이스는 연결이 끊어진 상태에서 관리 네트워크 포트 그룹에 연결되어 있습니다. 각 서비스 엔진은 가상 서비스를 1000개까지 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 포트로 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.

AVI에는 네이티브 IPAM 및 외부 IPAM 제공자 지원이 포함됩니다. vSphere에서는 AVI 네이티브 IPAM이 활용됩니다.

Avi Kubernetes Operator

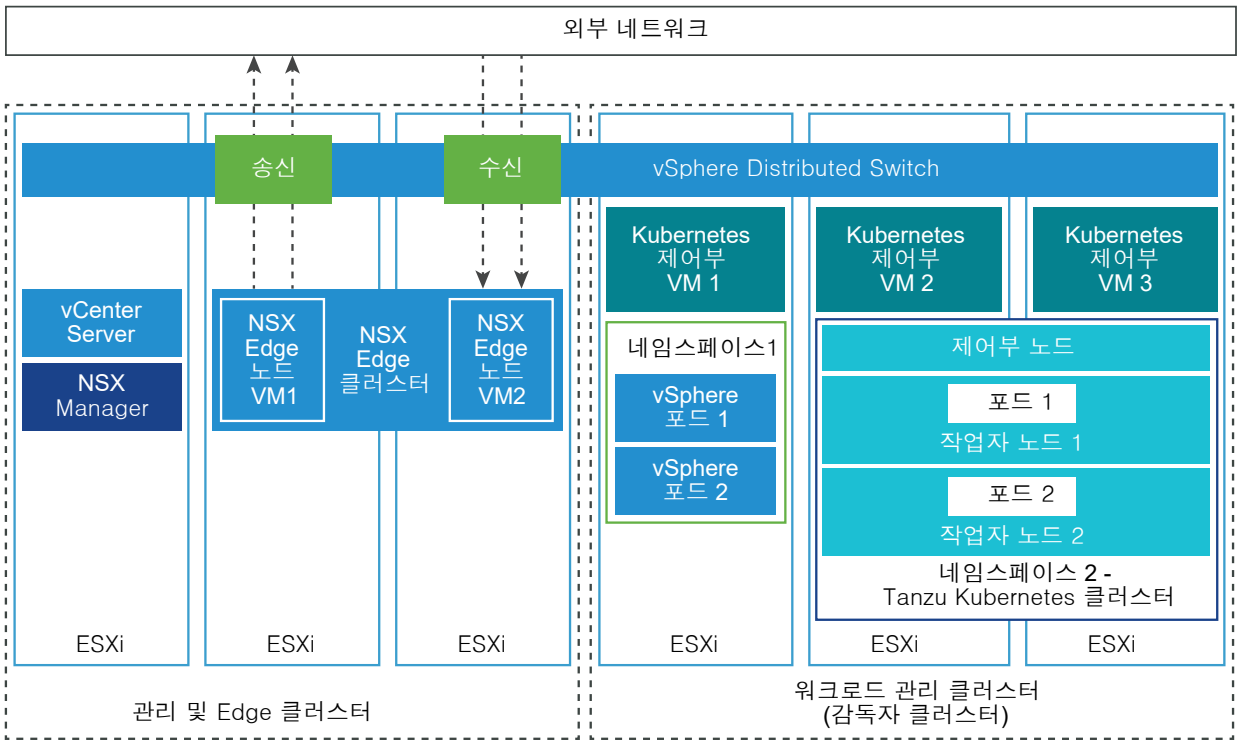
AKO(Avi Kubernetes Operator)는 Kubernetes 리소스를 감시하고 컨트롤러와 통신하여 해당 로드 밸런싱 리소스를 요청합니다.

Avi Kubernetes Operator는 사용 설정 프로세스의 일부로 감독자에 설치됩니다.

감독자를 네트워킹 스택으로 사용하는 1영역 NSX의 토폴로지

두 개의 클러스터, 즉 관리 및 Edge 기능을 위한 클러스터와 워크로드 관리 전용 클러스터에 vSphere IaaS control plane을 배포할 수 있습니다.

그림 4-3. 관리 및 Edge 및 워크로드 관리 클러스터



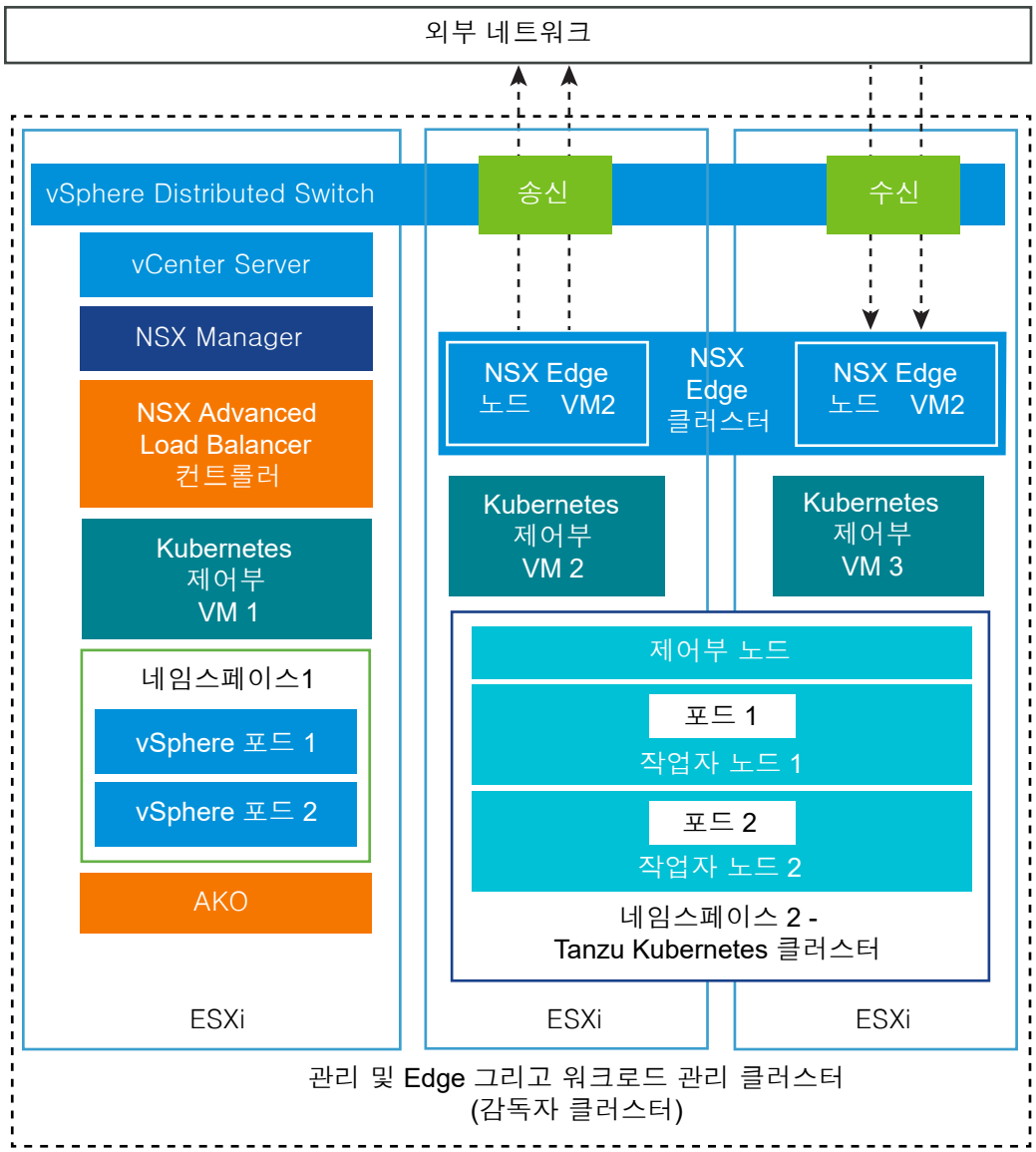
NSX를 네트워킹 스택 및 NSX Advanced Load Balancer로 사용하는 1개 영역 감독자의 토폴로지

Kubernetes 워크로드의 요구 사항 및 기본 네트워킹 인프라에 따라 감독자에 다른 토폴로지를 적용할 수 있습니다.

관리, Edge 및 워크로드 도메인 클러스터에 대한 토폴로지

단일 vSphere 클러스터에서 관리, Edge 및 워크로드 관리 기능이 결합된 vSphere IaaS control plane을 배포할 수 있습니다.

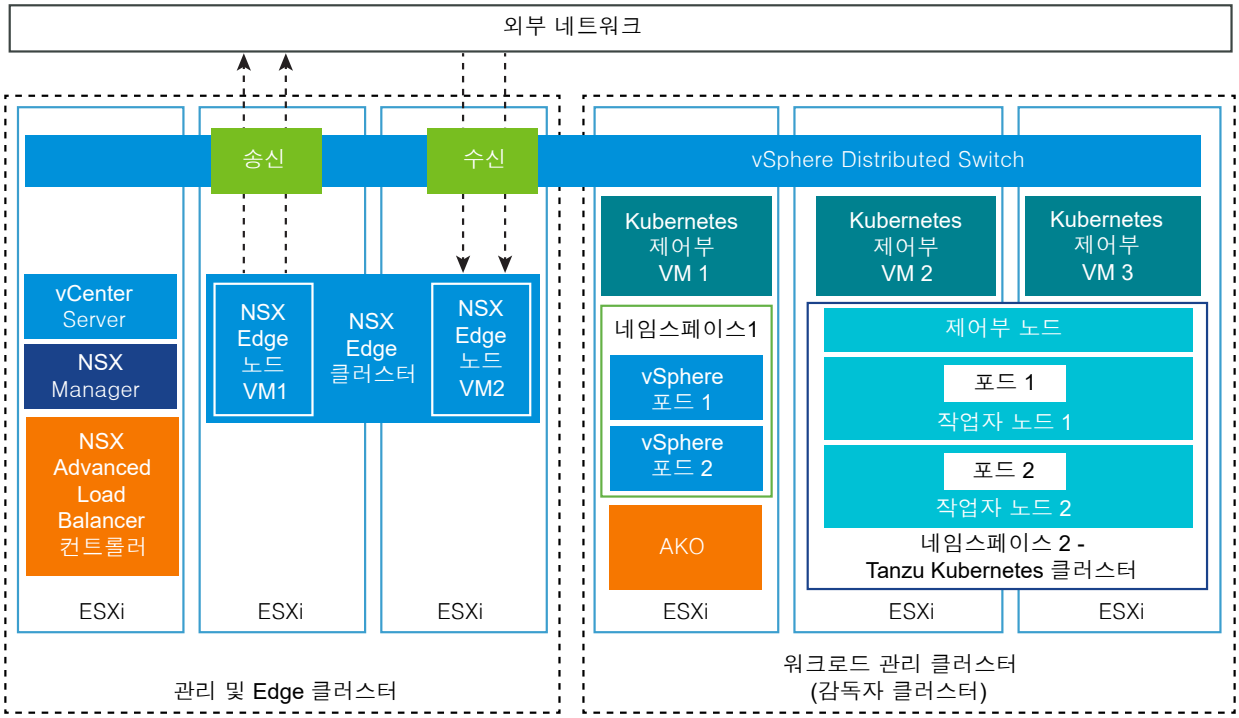
그림 4-4. 관리, Edge 및 워크로드 관리 클러스터



별도의 관리 및 Edge 클러스터 및 워크로드 관리 클러스터가 포함된 토폴로지

두 개의 클러스터, 즉 관리 및 Edge 기능을 위한 클러스터와 워크로드 관리 전용 클러스터에 vSphere IaaS control plane을 배포할 수 있습니다.

그림 4-5. 관리 및 Edge 및 워크로드 관리 클러스터



HAProxy 로드 밸런서 배포를 위한 토폴로지

VDS 네트워킹으로 구성된 감독자용 HAProxy 로드 밸런서에 대해 구현 가능한 토폴로지를 검토합니다. VDS 네트워킹에 vSphere IaaS control plane를 사용하는 경우 HAProxy는 Tanzu Kubernetes Grid 제어부에 액세스하는 개발자를 위해 그리고 로드 밸런서 유형의 Kubernetes 서비스에 대해 로드 밸런싱을 제공합니다.

감독자의 워크로드 네트워크

VDS 네트워킹을 사용하여 감독자를 구성하려면 클러스터의 모든 호스트를 VDS에 연결해야 합니다. 감독자 워크로드 네트워크에 대해 구현하는 토폴로지에 따라 하나 이상의 분산 포트 그룹을 생성합니다. 포트 그룹을 vSphere 네임스페이스에 대한 워크로드 네트워크로 지정합니다.

워크로드 네트워크는 Tanzu Kubernetes Grid 클러스터 노드 및 감독자 제어부 VM에 대한 연결을 제공합니다. Kubernetes 제어부 VM에 대한 연결을 제공하는 워크로드 네트워크를 기본 워크로드 네트워크라고 합니다. 각 감독자에는 기본 워크로드 네트워크가 하나씩 있어야 합니다. 분산 포트 그룹 중 하나를 감독자에 대한 기본 워크로드 네트워크로 지정해야 합니다.

참고 워크로드 네트워크는 감독자를 사용하도록 설정할 때만 추가되며 나중에 추가할 수 없습니다.

감독자의 Kubernetes 제어부 VM은 기본 워크로드 네트워크에 할당된 IP 주소 범위에서 3개의 IP 주소를 사용합니다. Tanzu Kubernetes Grid 클러스터의 각 노드에는 Tanzu Kubernetes Grid 클러스터가 실행되는 네임스페이스로 구성된 워크로드 네트워크의 주소 범위에서 할당된 별도의 IP 주소가 있습니다.

IP 범위 할당

HA Proxy 로드 밸런서가 있는 감독자의 네트워킹 토폴로지를 계획하는 경우 두 가지 유형의 IP 범위를 갖도록 계획합니다.

- HAProxy에 대한 가상 IP 할당 범위입니다. HAProxy의 가상 서버에 대해 구성하는 IP 범위는 로드 밸런서 장치에 의해 예약됩니다. 예를 들어 가상 IP 범위가 `192.168.1.0/24`인 경우 가상 IP 트래픽 이외의 트래픽은 해당 범위의 모든 호스트에 액세스할 수 없습니다.

  참고 해당 게이트웨이에 대한 모든 경로가 실패하기 때문에 HAProxy 가상 IP 범위 내에 게이트웨이를 구성하지 않아야 합니다.

- 감독자 및 Tanzu Kubernetes Grid 클러스터의 노드에 대한 IP 범위입니다. 감독자의 Kubernetes 제어부 VM에는 각각 하나의 IP 주소가 할당되어 총 3개의 IP 주소가 할당됩니다. 또한 Tanzu Kubernetes Grid 클러스터의 각 노드에는 별도의 IP가 할당됩니다. 네임스페이스에 구성하는 감독자의 각 워크로드 네트워크에 고유한 IP 범위를 할당해야 합니다.

하나의 /24 네트워크를 포함하는 구성 예:

- 네트워크: 192.168.120.0/24
- HAProxy VIP: 192.168.120.128/25
- HAProxy 워크로드 인터페이스에 대한 IP 주소 1개: 192.168.120.5

처음 128개 주소 내에서 사용 가능한 IP에 따라 감독자의 워크로드 네트워크에 대한 IP 범위를 정의할 수 있습니다. 예:

- 기본 워크로드 네트워크용 192.168.120.31-192.168.120.40
- 다른 워크로드 네트워크용 192.168.120.51-192.168.120.60

참고 워크로드 네트워크에 대해 정의하는 범위는 HAProxy VIP 범위와 겹치지 않아야 합니다.

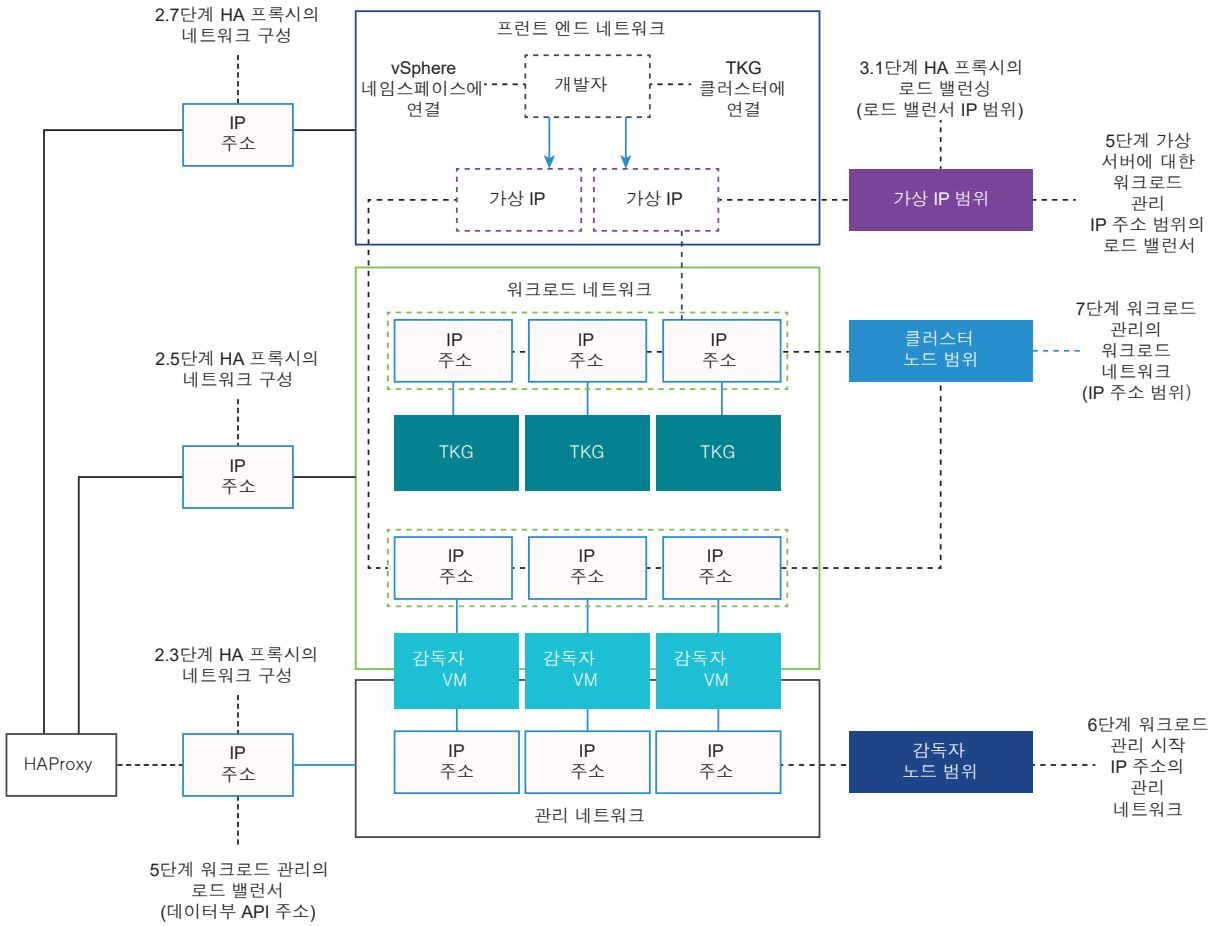
HAProxy 네트워크 토폴로지

HAProxy 배포를 위한 네트워크 구성 옵션에는 **기본** 및 **프런트 엔드**라는 두 가지가 있습니다. 기본 네트워크에는 2가지 NIC가 있으며, 하나는 관리 네트워크용이고, 다른 하나는 워크로드 네트워크용입니다. 프런트 엔드 네트워크에는 관리 네트워크, 워크로드 네트워크, 클라이언트용 프런트 엔드 네트워크라는 3가지 NIC가 있습니다. 각 네트워크의 특성은 표에 나열 및 설명되어 있습니다.

운영 설치의 경우 **프런트 엔드 네트워크** 구성을 사용하여 HAProxy 로드 밸런서를 배포하는 것이 좋습니다. **기본** 구성을 사용하여 HAProxy 로드 밸런서를 배포하는 경우에는 워크로드 네트워크에 /24 IP 주소 블록 크기를 할당하는 것이 좋습니다. 두 가지 구성 옵션 모두에서 DHCP는 권장되지 않습니다.

네트워크	특성
관리	감독자 클러스터는 관리 네트워크를 사용하여 HAProxy 로드 밸런서를 연결하고 프로그래밍합니다. ■ HAProxy 데이터부 API 끝점은 관리 네트워크에 연결된 네트워크 인터페이스에 바인딩됩니다. ■ HAProxy 제어부 VM에 할당된 관리 IP 주소는 관리 네트워크의 고정 IP여야 합니다. 그래야 감독자 클러스터가 로드 밸런서 API에 안정적으로 연결할 수 있습니다. ■ HAProxy VM의 기본 게이트웨이는 이 네트워크에 있어야 합니다. ■ 이 네트워크에서 DNS 쿼리가 발생해야 합니다.
워크로드	HAProxy 제어부 VM은 워크로드 네트워크를 사용하여 감독자 클러스터 및 Tanzu Kubernetes 클러스터 노드의 서비스에 액세스합니다. ■ HAProxy 제어부 VM은 이 네트워크에 있는 감독자 및 Tanzu Kubernetes 클러스터 노드로 트래픽을 전달합니다. ■ HAProxy 제어부 VM이 기본 모드(NIC 2개)로 배포된 경우 워크로드 네트워크는 로드 밸런서 서비스에 액세스하는 데 사용되는 논리적 네트워크를 제공해야 합니다. ■ **기본** 구성에서는 로드 밸런서 가상 IP와 Kubernetes 클러스터 노드 IP를 이 네트워크에서 가져옵니다. 네트워크 내에서 서로 겹치지 않는 별도의 범위로 정의됩니다. **참고** 워크로드 네트워크는 관리 네트워크와 다른 서브넷에 있어야 합니다. VDS 네트워킹 및 HAProxy 로드 밸런서를 사용한 클러스터 감독자 배포 요구 사항을 참조하십시오.
프런트 엔드(선택 사항)	클러스터 워크로드에 액세스하는 외부 클라이언트(예: 사용자 또는 애플리케이션)는 프런트 엔드 네트워크를 사용하여 가상 IP 주소를 사용하는 백엔드 로드 밸런싱된 서비스에 액세스합니다. ■ 프런트 엔드 네트워크는 HAProxy 제어부 VM이 3개의 NIC를 사용하여 배포된 경우에만 사용됩니다. ■ 운영 설치에 권장됩니다. ■ 프런트 엔드 네트워크는 VIP(가상 IP 주소)를 노출하는 위치입니다. HAProxy는 트래픽을 밸런싱하고 적절한 백엔드로 전달합니다.

아래 다이어그램은 **프런트 엔드 네트워크** 토폴로지를 사용하는 HAProxy 배포를 보여줍니다. 이 다이어그램은 설치 및 구성 프로세스 중에 구성 필드가 필요한 위치를 나타냅니다.



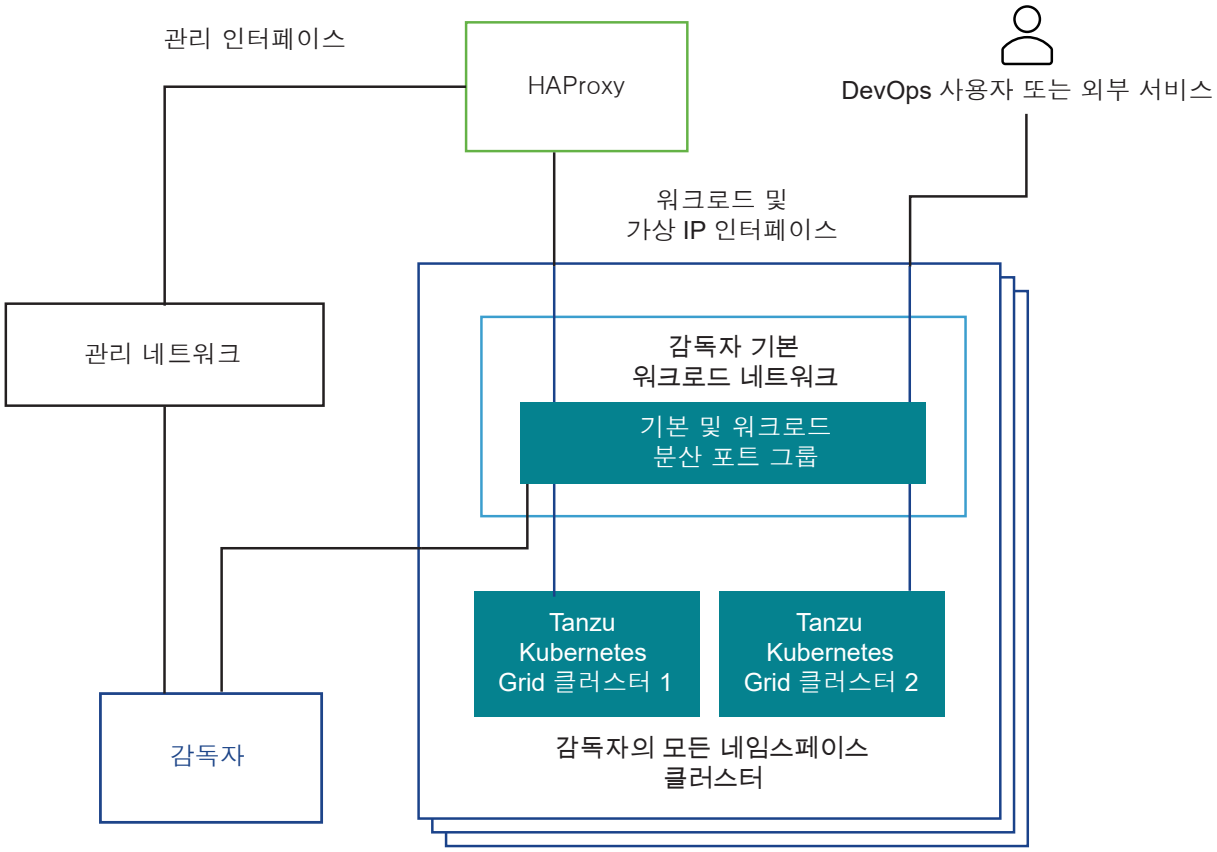
가상 NIC가 두 개인 HAProxy 및 워크로드 네트워크가 한 개인 감독자 토폴로지

이 토폴로지에서는 다음 구성 요소에 대해 워크로드 네트워크가 한 개인 감독자를 구성합니다.

- Kubernetes 제어부 VM
- Tanzu Kubernetes Grid 클러스터의 노드.
- 외부 서비스 및 DevOps 사용자가 연결되는 HAProxy 가상 IP 범위. 이 구성에서는 HAProxy가 가상 NIC 두 개(**기본** 구성)로 배포되며, 하나는 관리 네트워크에 연결되고 다른 하나는 기본 워크로드 네트워크에 연결됩니다. 기본 워크로드 네트워크와는 별도의 서브넷에 가상 IP를 할당하도록 계획해야 합니다.

하나의 포트 그룹을 감독자에 대한 기본 워크로드 네트워크로 지정한 다음, 동일한 포트 그룹을 vSphere 네임스페이스용 워크로드 네트워크로 사용합니다. 감독자, Tanzu Kubernetes Grid 클러스터, HAProxy, DevOps 사용자, 외부 서비스는 모두 기본 워크로드 네트워크로 설정된 동일한 분산 포트 그룹에 연결됩니다.

그림 4-6. 하나의 네트워크에서 지원하는 감독자



DevOps 사용자 또는 외부 애플리케이션에 대한 트래픽 경로는 다음과 같습니다.

1 DevOps 사용자 또는 외부 서비스는 분산 포트 그룹의 워크로드 네트워크 서브넷에 있는 가상 IP로 트래픽을 전송합니다.

2 HAProxy는 가상 IP 클러스터 트래픽을 Tanzu Kubernetes Grid 클러스터 노드 IP 또는 제어부 VM IP로 로드 밸런싱합니다. HAProxy는 해당 IP에서 들어오는 트래픽을 로드 밸런싱할 수 있도록 가상 IP 주소를 할당합니다.

3 제어부 VM 또는 Tanzu Kubernetes Grid 클러스터 노드는 각각 감독자 또는 Tanzu Kubernetes Grid 클러스터 내에서 실행되는 대상 포드로 트래픽을 전달합니다.

가상 NIC가 두 개인 HA 프록시 및 격리된 워크로드 네트워크가 있는 감독자 토폴로지

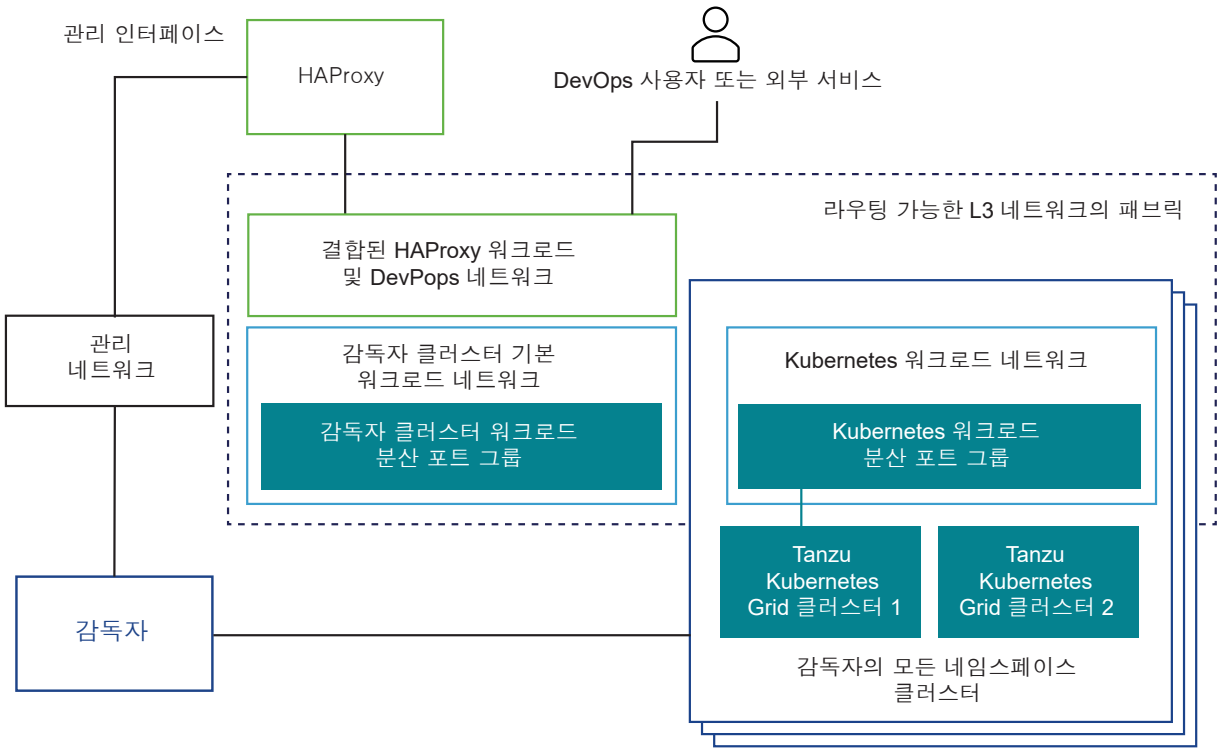
이 토폴로지에서는 다음 구성 요소에 대한 네트워크를 구성합니다.

- Kubernetes 제어부 VM. Kubernetes 제어부 VM에 대한 트래픽을 처리하기 위한 기본 워크로드 네트워크입니다.

- Tanzu Kubernetes Grid 클러스터 노드. 사용자가 감독자의 모든 네임스페이스에 할당하는 워크로드 네트워크. 이 네트워크는 Tanzu Kubernetes Grid 클러스터 노드를 연결합니다.
- HAProxy 가상 IP. 이 구성에서는 HAProxy VM이 가상 NIC 두 개(**기본** 구성)로 배포됩니다. HAProxy VM을 기본 워크로드 네트워크 또는 네임스페이스에 사용하는 워크로드 네트워크에 연결할 수 있습니다. vSphere에 이미 있으며 기본 및 워크로드 네트워크에 라우팅할 수 있는 VM 네트워크에 HAProxy를 연결할 수도 있습니다.

감독자는 기본 워크로드 네트워크를 지원하는 분산 포트 그룹에 연결되고, Tanzu Kubernetes Grid 클러스터는 워크로드 네트워크를 지원하는 분산 포트 그룹에 연결됩니다. 두 포트 그룹은 계층 3 라우팅이 가능해야 합니다. VLAN을 통해 계층 2 분리를 구현할 수 있습니다. 계층 3 트래픽 필터링은 IP 방화벽과 게이트웨이를 통해 가능합니다.

그림 4-7. 하나의 분리된 워크로드 네트워크가 있는 감독자



DevOps 사용자 또는 외부 서비스에 대한 트래픽 경로는 다음과 같습니다.

1 DevOps 사용자 또는 외부 서비스는 트래픽을 가상 IP로 전송합니다. 트래픽은 HAProxy가 연결된 네트워크로 라우팅됩니다.

2 HAProxy는 가상 IP 트래픽을 Tanzu Kubernetes Grid 노드 IP 또는 제어부 VM으로 로드 밸런싱합니다. HAProxy는 해당 IP에서 들어오는 트래픽을 로드 밸런싱할 수 있도록 가상 IP 주소를 할당합니다.

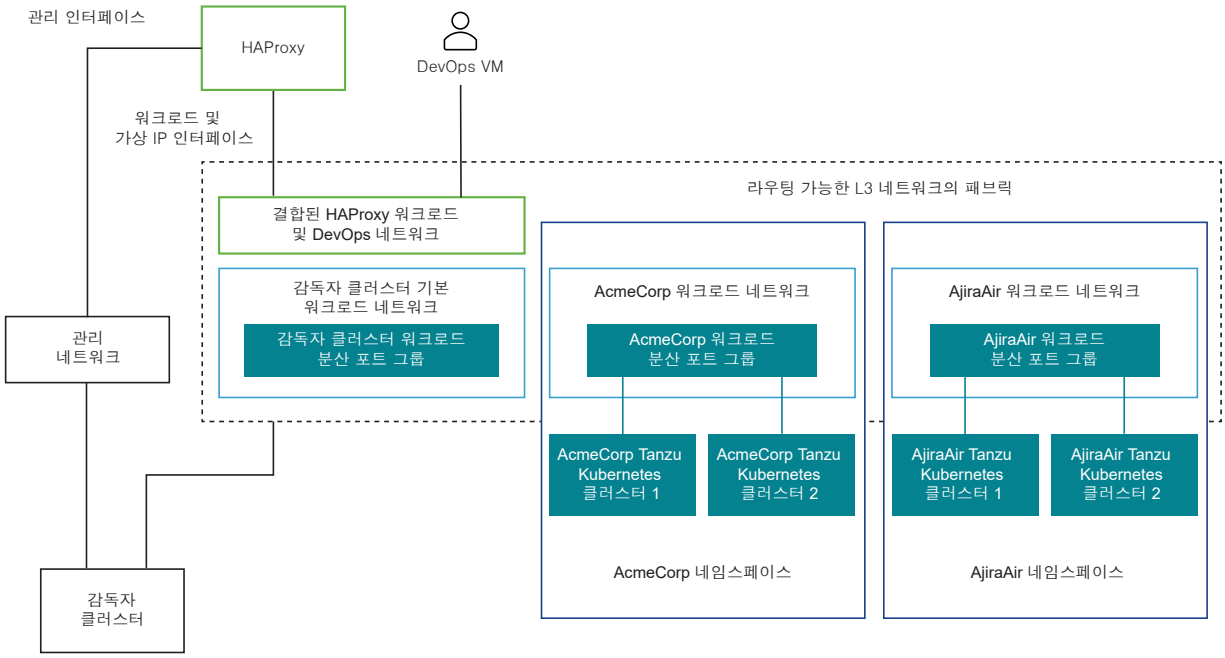
3 제어부 VM 또는 Tanzu Kubernetes Grid 클러스터 노드는 Tanzu Kubernetes Grid 클러스터 내에서 실행되는 대상 포드로 트래픽을 전달합니다.

가상 NIC가 두 개인 HA 프록시 및 다중 워크로드 네트워크가 있는 감독자 토폴로지

이 토폴로지에서는 기본 워크로드 네트워크 역할을 하는 하나의 포트 그룹과 각 네임스페이스에 대한 워크로드 네트워크 역할을 하는 전용 포트 그룹을 구성할 수 있습니다. HAProxy는 가상 NIC 두 개를 사용하여 배포되며(**기본** 구성), 기본 워크로드 네트워크 또는 임의의 워크로드 네트워크에 연결할 수 있습니다. 기본 및 워크로드 네트워크로 라우팅할 수 있는 기존 VM 네트워크를 사용할 수도 있습니다.

이 토폴로지의 DevOps 사용자 및 외부 서비스에 대한 트래픽 경로는 분리된 워크로드 네트워크 토폴로지와 동일합니다.

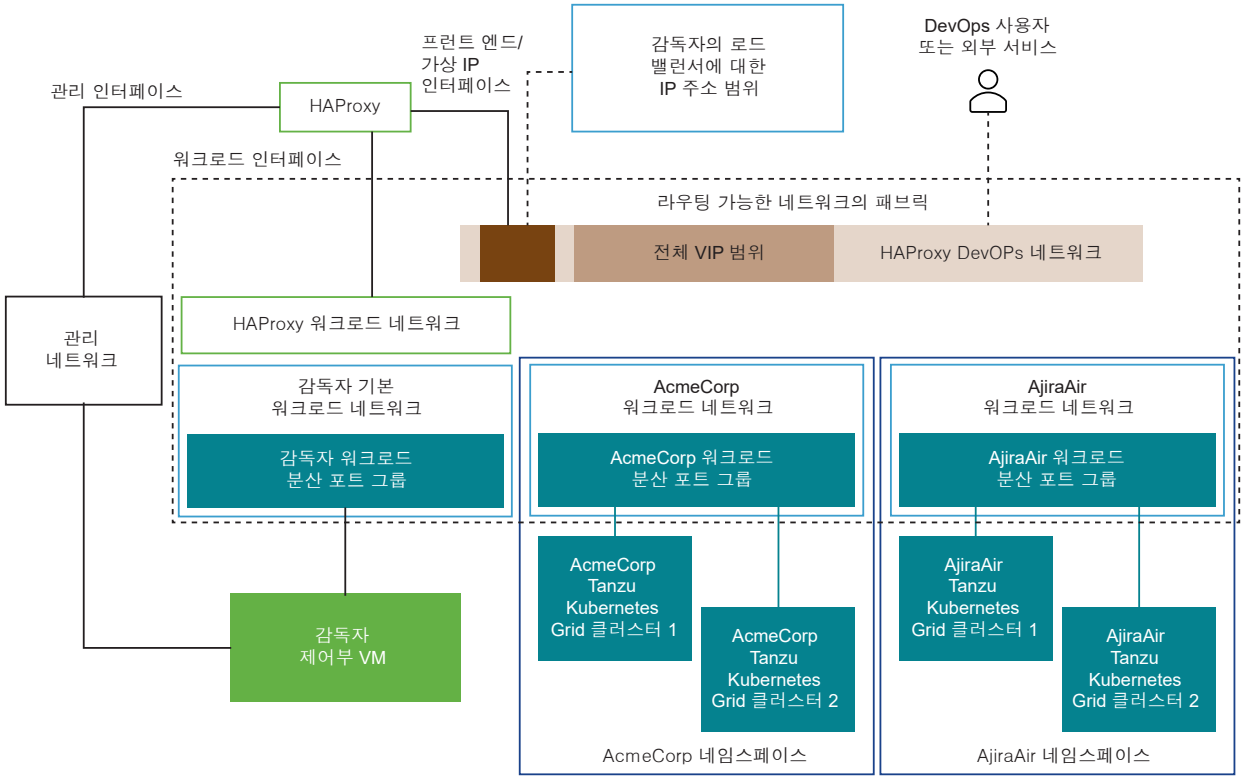
그림 4-8. 여러 개의 분리된 워크로드 네트워크에서 지원하는 감독자



가상 NIC가 세 개인 HA 프록시 및 다중 워크로드 네트워크가 있는 감독자 토폴로지

이 구성에서는 3개의 가상 NIC를 사용하여 HAProxy VM을 배포합니다. 따라서 HAProxy를 프런트 엔드 네트워크에 연결합니다. DevOps 사용자 및 외부 서비스는 프런트 엔드 네트워크의 가상 IP를 통해 HAProxy에 액세스할 수 있습니다. 운영 환경에는 가상 NIC가 세 개인 HA 프록시를 배포하는 것이 좋습니다.

그림 4-9. 3개의 가상 NIC를 사용하여 배포된 HAProxy



가능한 토폴로지 중에서 선택

가능한 각 토폴로지 중에서 선택하기 전에 해당 환경의 요구 사항을 평가합니다.

1 감독자 및 Tanzu Kubernetes Grid 클러스터 간에 계층 2 분리가 필요합니까?

   a 아니요: 모든 구성 요소를 처리하는 하나의 워크로드 네트워크를 사용하는 가장 간단한 토폴로지입니다.

   b 예: 별도의 기본 및 워크로드 네트워크를 사용하는 분리된 워크로드 네트워크 토폴로지입니다.

2 Tanzu Kubernetes Grid 클러스터 간에 추가적인 계층 2 분리가 필요합니까?

   a 아니요: 별도의 기본 및 워크로드 네트워크를 사용하는 분리된 워크로드 네트워크 토폴로지입니다.

   b 예: 각 네임스페이스 및 전용 기본 워크로드 네트워크에 별도의 워크로드 네트워크를 사용하는 다중 워크로드 네트워크 토폴로지입니다.

3 DevOps 사용자 및 외부 서비스가 Kubernetes 제어부 VM 및 Tanzu Kubernetes Grid 클러스터 노드로 직접 라우팅하지 못하도록 하시겠습니까?

   a 아니요: 2개 NIC의 HAProxy 구성입니다.

   b 예: 3개 NIC HAProxy 구성입니다. 이 구성은 운영 환경에 권장됩니다.

vSphere IaaS control plane에서 HAProxy 로드 밸런서를 사용하기 위한 고려 사항

HAProxy 로드 밸런서를 사용하여 vSphere IaaS control plane를 계획할 때는 다음 고려 사항에 유의하십시오.

- HAProxy 로드 밸런서에 대한 기술 지원을 받으려면 HAProxy와의 지원 계약이 필요합니다. VMware GSS는 HAProxy 장치에 대한 지원을 제공할 수 없습니다.
- HAProxy 장치는 고가용성 토폴로지의 가능성이 없는 싱글톤입니다. 고가용성 환경의 경우 NSX 또는 NSX Advanced Load Balancer의 전체 설치를 사용하는 것이 좋습니다.
- 나중에 프런트 엔드에 사용되는 IP 주소 범위를 확장할 수 없습니다. 즉, 향후 모든 성장에 맞게 네트워크 크기를 조정해야 합니다.

영역 감독자배포 요구 사항

5

vSphere 영역에서 감독자를 사용하도록 설정하기 위한 요구 사항을 확인하십시오. 감독자를 사용하는 vSphere 영역은 vSphere 클러스터 수준에서 Kubernetes 워크로드에 고가용성을 제공합니다.

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. vSphere IaaS control plane는 감독자를 단일 클러스터에서 3개 영역으로 변환하는 것을 지원하지 않습니다.

다음으로 아래 항목을 읽으십시오.

- NSX Advanced Load Balancer 및 VDS 네트워킹을 사용하는 영역 감독자 배포 요구 사항
- NSX가 있는 영역 감독자 요구 사항
- NSX 및 NSX Advanced Load Balancer가 있는 영역 감독자 요구 사항
- HAProxy 로드 밸런서가 있는 영역 감독자 배포 요구 사항

NSX Advanced Load Balancer 및 VDS 네트워킹을 사용하는 영역 감독자 배포 요구 사항

3개의 vSphere 영역에 매핑된 3개의 vSphere 클러스터에서 VDS 네트워킹 및 NSX Advanced Load Balancer가 있는 감독자를 사용하도록 설정하기 위한 요구 사항을 확인하십시오. Avi Load Balancer라고도 하는 NSX Advanced Load Balancer를 사용하여 vSphere IaaS control plane를 구성하려면 환경이 특정 요구 사항을 충족해야 합니다. vSphere IaaS control plane는 여러 토폴로지를 지원합니다. Avi 서비스 엔진 및 로드 밸런서 서비스를 위한 단일 VDS 네트워크를 사용할 수도 있고, Avi 관리부용 VDS와 NSX Advanced Load Balancer용 VDS를 별도로 사용할 수도 있습니다.

워크로드 네트워크

VDS 네트워킹 스택을 사용하여 감독자를 구성하려면 클러스터의 모든 호스트를 VDS에 연결해야 합니다. 감독자에 대해 구현하는 토폴로지에 따라 하나 이상의 분산 포트 그룹을 생성합니다. 포트 그룹을 vSphere 네임스페이스에 대한 워크로드 네트워크로 지정합니다.

워크로드 네트워크는 Tanzu Kubernetes Grid 클러스터 노드, 가상 시스템 서비스를 통해 생성된 VM 및 감독자 제어부 VM에 대한 연결을 제공합니다. Kubernetes 제어부 VM에 대한 연결을 제공하는 워크로드 네트워크를 기본 워크로드 네트워크라고 합니다. 각 감독자에는 기본 워크로드 네트워크가 하나씩 있어야 합니다. 분산 포트 그룹 중 하나를 감독자에 대한 기본 워크로드 네트워크로 지정해야 합니다.

감독자의 Kubernetes 제어부 VM은 기본 워크로드 네트워크에 할당된 IP 주소 범위에서 3개의 IP 주소를 사용합니다. Tanzu Kubernetes Grid 클러스터의 각 노드에는 Tanzu Kubernetes Grid 클러스터가 실행되는 네임스페이스로 구성된 워크로드 네트워크의 주소 범위에서 할당된 별도의 IP 주소가 있습니다.

네트워킹 요구 사항

NSX Advanced Load Balancer에는 라우팅 가능한 서브넷이 2개 필요합니다.

- 관리 네트워크. 관리 네트워크는 컨트롤러라고도 하는 Avi 컨트롤러가 상주하는 곳입니다. 관리 네트워크는 컨트롤러에 vCenter Server, ESXi 호스트, 감독자 제어부 노드에 대한 연결을 제공합니다. 이 네트워크에는 Avi 서비스 엔진의 관리 인터페이스가 배치됩니다. 이 네트워크에는 VDS 및 분산 포트 그룹이 필요합니다.
- 데이터 네트워크. 서비스 엔진이라고도 하는 Avi 서비스 엔진의 데이터 인터페이스가 이 네트워크에 연결됩니다. 로드 밸런서 VIP(가상 IP)는 이 네트워크에서 할당됩니다. 이 네트워크에는 VDS 및 분산 포트 그룹이 필요합니다. 로드 밸런서를 설치하기 전에 VDS 및 포트 그룹을 반드시 구성해야 합니다.

IP 주소 할당

컨트롤러와 서비스 엔진은 관리 네트워크에 연결됩니다. NSX Advanced Load Balancer를 설치하고 구성할 때 각 컨트롤러 VM에 정적, 라우팅 가능 IP 주소를 제공합니다.

서비스 엔진은 DHCP를 사용할 수 있습니다. DHCP를 사용할 수 없는 경우 서비스 엔진에 대한 IP 주소 풀을 구성할 수 있습니다.

물리적 사이트 간에 vSphere 영역 배치

사이트 간의 지연 시간이 100ms를 초과하지 않는 한 여러 물리적 사이트에 vSphere 영역을 분산할 수 있습니다. 예를 들어 vSphere 영역을 두 개의 물리적 사이트(첫 번째 사이트의 vSphere 영역 하나, 두 번째 사이트의 vSphere 영역 두 개)에 분산할 수 있습니다.

테스트 용도의 최소 계산 요구 사항

vSphere IaaS control plane 기능을 테스트하려는 경우 최소한의 테스트 베드에 플랫폼을 배포할 수 있습니다. 하지만 이러한 테스트 베드는 운영 스케일 워크로드를 실행하는 데 적합하지 않으며 클러스터 수준에서 HA를 제공하지 않는다는 점에 유의해야 합니다.

표 5-1. 테스트 용도의 최소 계산 요구 사항

시스템	최소 배포 크기	CPU	메모리	스토리지
vCenter Server 8.0	작음	2	21 GB	290GB
vSphere 클러스터	■ 3개의 vSphere 클러스터 ■ 각 vSphere 클러스터에서 vSphere DRS 및 HA가 사용되도록 설정되어 있어야 합니다. vSphere DRS는 완전히 자동화되거나 부분적으로 자동화된 모드여야 합니다. ■ 각 vSphere 클러스터에 대해 독립적으로 구성된 스토리지 및 네트워킹이 있어야 합니다.	해당 없음	해당 없음	해당 없음
ESXi 호스트 8.0	각 vSphere 클러스터에 대해 다음을 수행합니다. ■ vSAN 미포함: 호스트당 정적 IP가 1개인 ESXi 호스트 1개. ■ vSAN 포함: 클러스터당 물리적 NIC가 2개 이상인 ESXi 호스트 2개. **참고** 클러스터에 참여하는 호스트의 이름에 소문자를 사용하는지 확인합니다. 그렇지 않으면 감독자 활성화가 실패할 수 있습니다.	호스트당 8개	호스트당 64GB	해당 없음
Kubernetes 제어부 VM	3	4	16GB	16GB
NSX Advanced Load Balancer Controller	Enterprise	4(작음) 8(중간) 24(큼)	12 GB 24GB 128 GB	128 GB 128 GB 128 GB

운영을 위한 최소 계산 요구 사항

이 표에는 3개의 vSphere 영역에서 VDS 네트워킹 및 NSX Advanced Load Balancer가 있는 감독자를 사용하도록 설정하기 위한 최소 컴퓨팅 요구 사항이 나와 있습니다. 관리 도메인과 워크로드 도메인을 분리하는 것이 가장 좋습니다. 워크로드 도메인은 워크로드를 실행하는 감독자를 호스팅합니다. 관리 도메인은 vCenter Server와 같은 모든 관리 구성 요소를 호스팅합니다.

표 5-2. 최소 계산 요구 사항

시스템	최소 배포 크기	CPU	메모리	스토리지
vCenter Server 8.0	작음	2	21 GB	290GB
vSphere 클러스터	■ 3개의 vSphere 클러스터 ■ 각 vSphere 클러스터에서 vSphere DRS 및 HA가 사용되도록 설정되어 있어야 합니다. vSphere DRS는 완전히 자동화되거나 부분적으로 자동화된 모드여야 합니다. ■ 각 vSphere 클러스터에 대해 독립적으로 구성된 스토리지 및 네트워킹이 있어야 합니다.	해당 없음	해당 없음	해당 없음
ESXi 호스트 8.0	각 vSphere 클러스터에 대해 다음을 수행합니다. ■ vSAN 미포함: 호스트당 정적 IP가 1개인 ESXi 호스트 3개. ■ vSAN 포함: 클러스터당 물리적 NIC가 2개 이상인 ESXi 호스트 4개. **참고** 클러스터에 참여하는 호스트의 이름에 소문자를 사용하는지 확인합니다. 그렇지 않으면 감독자의 사용 설정이 실패할 수 있습니다.	호스트당 8개	호스트당 64GB	해당 없음
Kubernetes 제어부 VM	3	4	16GB	16GB
NSX Advanced Load Balancer 컨트롤러	Enterprise 운영 환경의 경우 3개의 컨트롤러 VM으로 구성된 클러스터를 설치하는 것이 좋습니다. HA에는 최소 2개의 서비스 엔진 VM이 필요합니다.	4(작음) 8(중간) 24(큼)	12 GB 24GB 128 GB	128 GB 128 GB 128 GB

최소 네트워크 요구 사항

이 표에는 VDS 네트워킹 및 NSX Advanced Load Balancer가 있는 감독자를 사용하도록 설정하기 위한 최소 네트워크 요구 사항이 나와 있습니다.

표 5-3. 물리적 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
계층 2 디바이스	1	감독자의 트래픽을 처리할 관리 네트워크는 감독자의 모든 클러스터 부분에 대해 동일한 계층 2 디바이스에 있어야 합니다. 기본 워크로드 네트워크도 동일한 계층 2 디바이스에 있어야 합니다.
물리적 네트워크 MTU	1500	MTU 크기는 분산 포트 그룹에서 1500 이상이어야 합니다.

표 5-4. 일반 네트워킹 요구 사항

구성 요소	최소 수량	필수 구성
지연 시간	100 ms	감독자에 함께 가입된 vSphere 영역의 일부인 각 클러스터 간의 최대 권장 지연 시간입니다.
NTP 및 DNS 서버	1	vCenter Server에서 사용할 수 있는 DNS 서버 및 NTP 서버. **참고** 모든 ESXi 호스트 및 vCenter Server에서 NTP를 구성합니다.
DHCP 서버	1	선택 사항입니다. 관리 및 워크로드 네트워크와 부동 IP에 대한 IP 주소를 자동으로 획득하도록 DHCP 서버를 구성합니다. DHCP 서버는 클라이언트 식별자를 지원하고 호환되는 DNS 서버, DNS 검색 도메인 및 NTP 서버를 제공해야 합니다. 관리 네트워크의 경우 제어부 VM IP, 부동 IP, DNS 서버, DNS, 검색 도메인 및 NTP 서버와 같은 모든 IP 주소가 DHCP 서버에서 자동으로 획득됩니다. DHCP 구성은 감독자에서 사용됩니다. 로드 밸런서에는 관리를 위한 정적 IP 주소가 필요할 수 있습니다. DHCP 범위는 이러한 정적 IP와 겹치지 않아야 합니다. DHCP는 가상 IP에 사용되지 않습니다. (VIP)

표 5-5. 관리 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
Kubernetes 제어부 VM에 대한 정적 IP	5개의 블록	관리 네트워크에서 감독자의 Kubernetes 제어부 VM으로 할당할 5개의 연속적 정적 IP 주소 블록.
관리 트래픽 네트워크	1	ESXi 호스트, vCenter Server, 감독자 및 로드 밸런서로 라우팅할 수 있는 관리 네트워크.
관리 네트워크 서브넷	1	관리 네트워크는 컨트롤러라고도 하는 NSX Advanced Load Balancer 컨트롤러가 상주하는 곳입니다. 또한 서비스 엔진 관리 인터페이스가 연결되는 위치이기도 합니다. 컨트롤러는 이 네트워크의 vCenter Server 및 ESXi 관리 IP에 연결되어야 합니다. **참고** 관리 네트워크와 워크로드 네트워크는 서로 다른 서브넷에 있어야 합니다. 관리 및 워크로드 네트워크에 동일한 서브넷을 할당하는 것은 지원되지 않으며 시스템 오류 및 문제가 발생할 수 있습니다.

표 5-6. 워크로드 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
vSphere Distributed Switch	1	vSphere 클러스터 3개 모두에 있는 모든 호스트는 VDS에 연결되어야 합니다.
워크로드 네트워크	1	기본 워크로드 네트워크로 구성한 VDS에 분산 포트 그룹을 하나 이상 생성해야 합니다. 선택한 토폴로지에 따라 네임스페이스의 워크로드 네트워크와 동일한 분산 포트 그룹을 사용하거나 더 많은 포트 그룹을 생성하고 이를 워크로드 네트워크로 구성할 수 있습니다. 워크로드 네트워크는 다음 요구 사항을 충족해야 합니다. ■ NSX Advanced Load Balancer가 가상 IP 할당에 사용하는 네트워크가 있는 모든 워크로드 네트워크 간에 라우팅이 가능해야 합니다. ■ 감독자 내의 모든 워크로드 네트워크에서 IP 주소 범위가 겹치지 않아야 합니다.
Kubernetes 서비스 CIDR 범위	/개인 IP 주소 16개	Kubernetes 서비스에 IP 주소를 할당할 개인 CIDR 범위. 각 감독자에 대해 고유한 Kubernetes 서비스 CIDR 범위를 지정해야 합니다.

표 5-7. 로드 밸런서 네트워킹 요구 사항

NTP 및 DNS 서버	1	NSX Advanced Load Balancer 컨트롤러가 vCenter Server 및 ESXi 호스트 이름을 올바르게 확인하려면 DNS 서버 IP가 필요합니다. 공용 NTP 서버가 기본적으로 사용되므로 NTP는 선택 사항입니다.
데이터 네트워크 서브넷	1	서비스 엔진이라고도 하는 서비스 엔진의 데이터 인터페이스가 이 네트워크에 연결됩니다. 서비스 엔진에 대한 IP 주소 풀을 구성합니다. 로드 밸런서 VIP(가상 IP)는 이 네트워크에서 할당됩니다.
NSX Advanced Load Balancer 컨트롤러 IP	1 또는 4	NSX Advanced Load Balancer 컨트롤러를 단일 노드로 배포하는 경우 해당 관리 인터페이스에 하나의 정적 IP가 필요합니다. 3노드 클러스터의 경우 4개의 IP 주소가 필요합니다. 각 컨트롤러 VM에 대해 1개씩 그리고 클러스터 VIP에 대해 1개입니다. 이러한 IP는 관리 네트워크 서브넷의 IP여야 합니다.
VIP IPAM 범위	-	Kubernetes 서비스에 IP 주소를 할당할 개인 CIDR 범위. IP는 데이터 네트워크 서브넷의 IP여야 합니다. 각 감독자 클러스터에 대해 고유한 Kubernetes 서비스 CIDR 범위를 지정해야 합니다.

포트 및 프로토콜

이 표에는 NSX Advanced Load Balancer, vCenter Server 및 기타 vSphere IaaS control plane 구성 요소 간의 IP 연결을 관리하는 데 필요한 프로토콜 및 포트가 나열되어 있습니다.

소스	대상	프로토콜 및 포트
NSX Advanced Load Balancer 컨트롤러	NSX Advanced Load Balancer 컨트롤러(클러스터 내)	TCP 22(SSH) TCP 443(HTTPS) TCP 8443(HTTPS)
서비스 엔진	HA의 서비스 엔진	VMware, LSC 및 NSX-T 클라우드에 대해 TCP 9001
서비스 엔진	NSX Advanced Load Balancer 컨트롤러	TCP 22(SSH) TCP 8443(HTTPS) UDP 123(NTP)
NSX Advanced Load Balancer 컨트롤러	vCenter Server, ESXi, NSX-T Manager	TCP 443(HTTPS)
감독자 제어부 노드(AKO)	NSX Advanced Load Balancer 컨트롤러	TCP 443(HTTPS)

NSX Advanced Load Balancer의 포트 및 프로토콜에 대한 자세한 내용은 https://ports.esp.vmware.com/home/NSX-Advanced-Load-Balancer 항목을 참조하십시오.

NSX가 있는 영역 감독자 요구 사항

NSX 네트워킹 스택을 사용하여 vSphere 영역에 매핑된 3개의 vSphere 클러스터에서 감독자를 사용하도록 설정하기 위한 시스템 요구 사항을 확인하십시오.

이러한 요구 사항 외에도 NSX 배포를 위한 모범 사례에 대한 자세한 내용은 NSX 참조 설계 가이드를 참조하십시오.

물리적 사이트 간에 vSphere 영역 배치

사이트 간의 지연 시간이 100ms를 초과하지 않는 한 여러 물리적 사이트에 vSphere 영역을 분산할 수 있습니다. 예를 들어 vSphere 영역을 두 개의 물리적 사이트(첫 번째 사이트의 vSphere 영역 하나, 두 번째 사이트의 vSphere 영역 두 개)에 분산할 수 있습니다.

관리 및 Edge 클러스터에 대한 최소 계산 요구 사항

시스템	최소 배포 크기	CPU	메모리	스토리지
vCenter Server 8	작음	2	21 GB	290GB
ESXi 호스트 8	ESXi 호스트 2개	8	호스트당 64GB	해당 없음
NSX Manager	중간	6	24GB	300GB
NSX Edge 1	큼	8	32GB	200GB
NSX Edge 2	큼	8	32GB	200GB

참고 vSphere IaaS control plane를 구성하려는 vSphere 클러스터에 참여하는 모든 ESXi 호스트가 NSX 전송 노드로 준비되었는지 확인합니다. 자세한 내용은 NSX 설명서에서 https://kb.vmware.com/s/article/95820 및 ESXi 호스트를 전송 노드로 준비를 참조하십시오.

워크로드 도메인 클러스터에 대한 최소 계산 요구 사항

시스템	최소 배포 크기	CPU	메모리	스토리지
vSphere 클러스터	■ 3개의 vSphere 클러스터 ■ 각 vSphere 클러스터에서 vSphere DRS 및 HA가 사용되도록 설정되어 있어야 합니다. vSphere DRS는 완전히 자동화된 모드여야 합니다. ■ 각 vSphere 클러스터에 대해 독립적으로 구성된 스토리지 및 네트워킹이 있어야 합니다.	해당 없음	해당 없음	해당 없음
ESXi 호스트 8	각 vSphere 클러스터에 대해 다음을 수행합니다. ■ vSAN 미포함: 호스트당 정적 IP가 1개인 ESXi 호스트 3개. ■ vSAN 포함: 클러스터당 물리적 NIC가 2개 이상인 ESXi 호스트 4개. **참고** 클러스터에 참여하는 호스트의 이름에 소문자를 사용하는지 확인합니다. 그렇지 않으면 감독자 활성화가 실패할 수 있습니다.	8	호스트당 64GB	해당 없음
Kubernetes 제어부 VM	3	4	16GB	16GB

네트워킹 요구 사항

참고 vSphere 8 감독자를 사용하여 IPv6 클러스터를 생성하거나 IPv6 클러스터를 Tanzu Mission Control에 등록할 수 없습니다.

지원되는 NSX 버전은 VMware 제품 상호 운용성 매트릭스를 확인하십시오.

표 5-8. 물리적 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
계층 2 디바이스	1	감독자의 트래픽을 처리할 관리 네트워크는 동일한 계층 2 디바이스에 있어야 합니다. 관리 트래픽을 처리하는 호스트당 하나 이상의 물리적 NIC가 동일한 계층 2 디바이스에 연결되어야 합니다.
물리적 네트워크 MTU	1500	MTU 크기는 모든 vSphere Distributed Switch 포트 그룹에서 1500 이상이어야 합니다.
물리적 NIC	vSAN을 사용하는 경우 호스트당 2개 이상의 물리적 NIC	Antrea CNI를 사용하고 최적의 NSX 성능을 얻으려면 참여하는 각 ESXi 호스트의 물리적 NIC 각각이 GENEVE 캡슐화를 지원하고 사용하도록 설정되어 있어야 합니다.

표 5-9. 일반 네트워킹 요구 사항

구성 요소	최소 수량	필수 구성
지연 시간	100 ms	감독자에 함께 가입된 vSphere 영역의 일부인 각 클러스터 간의 최대 권장 지연 시간입니다.
NTP 및 DNS 서버	1	vCenter Server에서 사용할 수 있는 DNS 서버 및 NTP 서버. **참고** 모든 ESXi 호스트 및 vCenter Server에서 NTP를 구성합니다.
DHCP 서버	1	선택 사항입니다. 관리 및 워크로드 네트워크와 부동 IP에 대한 IP 주소를 자동으로 획득하도록 DHCP 서버를 구성합니다. DHCP 서버는 클라이언트 식별자를 지원하고 호환되는 DNS 서버, DNS 검색 도메인 및 NTP 서버를 제공해야 합니다. 관리 네트워크의 경우 제어부 VM IP, 부동 IP, DNS 서버, DNS, 검색 도메인 및 NTP 서버와 같은 모든 IP 주소가 DHCP 서버에서 자동으로 획득됩니다. DHCP 구성은 감독자에서 사용됩니다. 로드 밸런서에는 관리를 위한 정적 IP 주소가 필요할 수 있습니다. DHCP 범위는 이러한 정적 IP와 겹치지 않아야 합니다. DHCP는 가상 IP에 사용되지 않습니다. (VIP)
이미지 레지스트리	1	서비스를 위해 레지스트리에 액세스.

표 5-10. 관리 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
Kubernetes 제어부 VM에 대한 정적 IP	5개의 블록	관리 네트워크에서 감독자의 Kubernetes 제어부 VM으로 할당할 5개의 연속적 정적 IP 주소 블록.
관리 트래픽 네트워크	1	ESXi 호스트, vCenter Server, 감독자 및 로드 밸런서로 라우팅할 수 있는 관리 네트워크.
관리 네트워크 서브넷	1	ESXi 호스트와 vCenter Server, NSX 장치 및 Kubernetes 제어부 사이의 관리 트래픽에 사용되는 서브넷. 서브넷의 크기는 다음과 같아야 합니다. ■ 호스트 VMkernel 어댑터당 IP 주소 1개. ■ vCenter Server Appliance에 대해 IP 주소 1개. ■ NSX Manager에 대해 IP 주소 1개 또는 4개. 3개 노드 및 1개 VIP(가상 IP)의 NSX Manager 클러스터링 수행 시 4개. ■ Kubernetes 제어부에 대해 IP 주소 5개. 3개 노드 각각에 대해 1개, 가상 IP에 1개, 롤링 클러스터 업그레이드에 1개. **참고** 관리 네트워크와 워크로드 네트워크는 서로 다른 서브넷에 있어야 합니다. 관리 및 워크로드 네트워크에 동일한 서브넷을 할당하는 것은 지원되지 않으며 시스템 오류 및 문제가 발생할 수 있습니다.
관리 네트워크 VLAN	1	관리 네트워크 서브넷의 VLAN ID.

표 5-11. 워크로드 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
vSphere 포드 CIDR 범위	/개인 IP 주소 23개	vSphere 포드의 IP 주소를 제공하는 개인 CIDR 범위입니다. 이러한 주소는 Tanzu Kubernetes Grid 클러스터 노드에도 사용됩니다. 각 클러스터에 대해 고유한 vSphere 포드 CIDR 범위를 지정해야 합니다. **참고** vSphere 포드 CIDR 범위와 Kubernetes 서비스 주소의 CIDR 범위는 겹치지 않아야 합니다.
Kubernetes 서비스 CIDR 범위	/개인 IP 주소 16개	Kubernetes 서비스에 IP 주소를 할당할 개인 CIDR 범위. 각 감독자에 대해 고유한 Kubernetes 서비스 CIDR 범위를 지정해야 합니다.
송신 CIDR 범위	/정적 IP 주소 27개	Kubernetes 서비스의 송신 IP를 결정하는 개인 CIDR 주석. 감독자의 각 네임스페이스에는 송신 IP 주소가 하나만 할당됩니다. 송신 IP는 외부 엔티티가 네임스페이스의 서비스와 통신하는 데 사용하는 주소입니다. 송신 IP 주소 수는 감독자가 포함할 수 있는 송신 정책의 수를 제한합니다. 최소값은 /27 이상의 CIDR입니다. 예를 들어 `10.174.4.96/27`입니다. **참고** 송신 IP 주소 및 수신 IP 주소는 겹치지 않아야 합니다.
수신 CIDR	/정적 IP 주소 27개	수신 IP 주소에 사용되는 개인 CIDR 범위. 수신을 사용하면 외부 네트워크에서 감독자로 들어오는 요청에 트래픽 정책을 적용할 수 있습니다. 수신 IP 주소 수는 클러스터가 포함할 수 있는 수신의 수를 제한합니다. 최소값은 /27 이상의 CIDR입니다. **참고** 송신 IP 주소 및 수신 IP 주소는 겹치지 않아야 합니다.
네임스페이스 네트워크 범위	1	서브넷/세그먼트를 생성하고 워크로드에 IP 주소를 할당하기 위해 하나 이상의 IP CIDR이 필요합니다.
네임스페이스 서브넷 접두사	1	네임스페이스 세그먼트용으로 예약된 서브넷의 크기를 지정하는 서브넷 접두사가 필요합니다. Default is 28.

표 5-12. NSX 요구 사항

구성 요소	최소 수량	V
VLAN	3	이러한 VLAN IP는 TEP(터널 끝점)의 IP 주소입니다. ESXi 호스트 TEP와 Edge TEP는 라우팅이 가능해야 합니다. 다음에 VLAN IP 주소가 필요합니다. ■ ESXi 호스트 VTEP ■ 정적 IP를 사용하는 Edge VTEP ■ 전송 노드에 대한 업링크 및 Tier 0 게이트웨이. **참고** ESXi 호스트 VTEP 및 Edge VTEP의 MTU 크기가 1600보다 커야 합니다. ESXi 호스트와 NSX-T Edge 노드는 터널 끝점으로 작동하며 각 호스트와 Edge 노드에 TEP(터널 끝점) IP가 할당됩니다. ESXi 호스트의 TEP IP가 Edge 노드에 TEP IP로 오버레이 터널을 생성하기 때문에 VLAN IP를 라우팅할 수 있어야 합니다. Tier-0 게이트웨이에 대한 North-South 연결을 제공하려면 추가 VLAN이 필요합니다. IP 풀은 여러 클러스터 간에 공유될 수 있습니다. 하지만 호스트 오버레이 IP 풀/VLAN은 Edge 오버레이 IP 풀/VLAN과 공유해서는 안 됩니다. **참고** 호스트 TEP와 Edge TEP가 서로 다른 물리적 NIC를 사용하는 경우 동일한 VLAN을 사용할 수 있습니다.
Tier-0 업링크 IP	/개인 IP 주소 24개	Tie-0 업링크에 사용되는 IP 서브넷. Tie-0 업링크의 IP 주소에 대한 요구 사항은 다음과 같습니다. ■ IP 1개, Edge 이중화를 사용하지 않는 경우. ■ IP 4개, BGP와 Edge 이중화를 사용하는 경우. Edge당 IP 주소 2개. ■ IP 3개, 정적 경로와 Edge 이중화를 사용하는 경우. Edge 관리 IP, 서브넷, 게이트웨이, 업링크 IP, 서브넷, 게이트웨이는 고유해야 합니다.

NSX 및 NSX Advanced Load Balancer가 있는 영역 감독자 요구 사항

NSX 네트워킹 스택 및 NSX Advanced Load Balancer를 사용하여 vSphere 영역에 매핑된 3개의 vSphere 클러스터에서 감독자를 사용하도록 설정하기 위한 시스템 요구 사항을 알아봅니다.

물리적 사이트 간에 vSphere 영역 배치

사이트 간의 지연 시간이 100ms를 초과하지 않는 한 여러 물리적 사이트에 vSphere 영역을 분산할 수 있습니다. 예를 들어 vSphere 영역을 두 개의 물리적 사이트(첫 번째 사이트의 vSphere 영역 하나, 두 번째 사이트의 vSphere 영역 두 개)에 분산할 수 있습니다.

NSX 배포 옵션

NSX 배포하는 모범 사례에 대한 자세한 내용은 NSX 참조 설계 가이드를 참조하십시오.

관리 및 Edge 클러스터에 대한 최소 계산 요구 사항

시스템	최소 배포 크기	CPU	메모리	스토리지
vCenter Server 8	작음	2	21 GB	290GB
ESXi 호스트 8	ESXi 호스트 2개	8	호스트당 64GB	해당 없음
NSX Manager	중간	6	24GB	300GB
NSX Edge 1	큼	8	32GB	200GB
NSX Edge 2	큼	8	32GB	200GB
서비스 엔진 VM	감독자당 2개 이상의 서비스 엔진 VM이 배포됩니다.	1	2GB	해당 없음

참고 vSphere IaaS control plane를 구성하려는 vSphere 클러스터에 참여하는 모든 ESXi 호스트가 NSX 전송 노드로 준비되었는지 확인합니다. 자세한 내용은 NSX 설명서에서 https://kb.vmware.com/s/article/95820 및 ESXi 호스트를 전송 노드로 준비를 참조하십시오.

컨트롤러의 시스템 용량 지정

배포 중에 컨트롤러의 시스템 용량을 지정할 수 있습니다. 시스템 용량은 CPU, RAM, 디스크와 같은 시스템 리소스 할당을 기반으로 합니다. 할당하는 리소스의 양은 컨트롤러 성능에 영향을 미칩니다.

배포 유형	노드 수	권장 할당-CPU	권장 할당-메모리	권장 할당-디스크
데모/고객 평가	1	6	24GB	128 GB

데모 배포에서는 단일 컨트롤러가 적절하며 모든 제어부 작업 및 워크플로와 분석에 사용됩니다.

운영 배포에서는 3노드 클러스터가 권장됩니다.

자세한 내용은 NSX Advanced Load Balancer 컨트롤러 크기 조정을 참조하십시오.

워크로드 도메인 클러스터에 대한 최소 계산 요구 사항

시스템	최소 배포 크기	CPU	메모리	스토리지
vSphere 클러스터	■ 3개의 vSphere 클러스터 ■ 각 vSphere 클러스터에서 vSphere DRS 및 HA가 사용되도록 설정되어 있어야 합니다. vSphere DRS는 완전히 자동화된 모드여야 합니다. ■ 각 vSphere 클러스터에 대해 독립적으로 구성된 스토리지 및 네트워킹이 있어야 합니다.	해당 없음	해당 없음	해당 없음
ESXi 호스트 8	각 vSphere 클러스터에 대해 다음을 수행합니다. ■ vSAN 미포함: 호스트당 정적 IP가 1개인 ESXi 호스트 3개. ■ vSAN 포함: 클러스터당 물리적 NIC가 2개 이상인 ESXi 호스트 4개. **참고** 클러스터에 참여하는 호스트의 이름에 소문자를 사용하는지 확인합니다. 그렇지 않으면 감독자 활성화가 실패할 수 있습니다.	8	호스트당 64GB	해당 없음
Kubernetes 제어부 VM	3	4	16GB	16GB

네트워킹 요구 사항

참고 vSphere 8 감독자를 사용하여 IPv6 클러스터를 생성하거나 IPv6 클러스터를 Tanzu Mission Control에 등록할 수 없습니다.

지원되는 NSX 버전은 VMware 제품 상호 운용성 매트릭스를 확인하십시오.

표 5-13. 물리적 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
계층 2 디바이스	1	감독자의 트래픽을 처리할 관리 네트워크는 동일한 계층 2 디바이스에 있어야 합니다. 관리 트래픽을 처리하는 호스트당 하나 이상의 물리적 NIC가 동일한 계층 2 디바이스에 연결되어야 합니다.
물리적 네트워크 MTU	1700	MTU 크기는 모든 vSphere Distributed Switch 포트 그룹에서 1700 이상이어야 합니다.
물리적 NIC	vSAN을 사용하는 경우 호스트당 2개 이상의 물리적 NIC	Antrea CNI를 사용하고 최적의 NSX 성능을 얻으려면 참여하는 각 ESXi 호스트의 물리적 NIC 각각이 GENEVE 캡슐화를 지원하고 사용하도록 설정되어 있어야 합니다.

표 5-14. 일반 네트워킹 요구 사항

구성 요소	최소 수량	필수 구성
지연 시간	100 ms	감독자에 함께 가입된 vSphere 영역의 일부인 각 클러스터 간의 최대 권장 지연 시간입니다.
NTP 및 DNS 서버	1	vCenter Server에서 사용할 수 있는 DNS 서버 및 NTP 서버. **참고** 모든 ESXi 호스트 및 vCenter Server에서 NTP를 구성합니다.
DHCP 서버	1	선택 사항입니다. 관리 및 워크로드 네트워크와 부동 IP에 대한 IP 주소를 자동으로 획득하도록 DHCP 서버를 구성합니다. DHCP 서버는 클라이언트 식별자를 지원하고 호환되는 DNS 서버, DNS 검색 도메인 및 NTP 서버를 제공해야 합니다. 관리 네트워크의 경우 제어부 VM IP, 부동 IP, DNS 서버, DNS, 검색 도메인 및 NTP 서버와 같은 모든 IP 주소가 DHCP 서버에서 자동으로 획득됩니다. DHCP 구성은 감독자에서 사용됩니다. 로드 밸런서에는 관리를 위한 정적 IP 주소가 필요할 수 있습니다. DHCP 범위는 이러한 정적 IP와 겹치지 않아야 합니다. DHCP는 가상 IP에 사용되지 않습니다. (VIP)
이미지 레지스트리	1	서비스를 위해 레지스트리에 액세스.

표 5-15. 관리 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
Kubernetes 제어부 VM에 대한 정적 IP	5개의 블록	관리 네트워크에서 감독자의 Kubernetes 제어부 VM으로 할당할 5개의 연속적 정적 IP 주소 블록.
관리 트래픽 네트워크	1	ESXi 호스트, vCenter Server, 감독자 및 로드 밸런서로 라우팅할 수 있는 관리 네트워크.
관리 네트워크 서브넷	1	ESXi 호스트와 vCenter Server, NSX 장치 및 Kubernetes 제어부 사이의 관리 트래픽에 사용되는 서브넷. 서브넷의 크기는 다음과 같아야 합니다. ■ 호스트 VMkernel 어댑터당 IP 주소 1개. ■ vCenter Server Appliance에 대해 IP 주소 1개. ■ NSX Manager에 대해 IP 주소 1개 또는 4개. 3개 노드 및 1개 VIP(가상 IP)의 NSX Manager 클러스터링 수행 시 4개. ■ Kubernetes 제어부에 대해 IP 주소 5개. 3개 노드 각각에 대해 1개, 가상 IP에 1개, 롤링 클러스터 업그레이드에 1개. **참고** 관리 네트워크와 워크로드 네트워크는 서로 다른 서브넷에 있어야 합니다. 관리 및 워크로드 네트워크에 동일한 서브넷을 할당하는 것은 지원되지 않으며 시스템 오류 및 문제가 발생할 수 있습니다.
관리 네트워크 VLAN	1	관리 네트워크 서브넷의 VLAN ID.

표 5-16. 워크로드 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
vSphere 포드 CIDR 범위	/개인 IP 주소 23개	vSphere 포드의 IP 주소를 제공하는 개인 CIDR 범위입니다. 이러한 주소는 Tanzu Kubernetes Grid 클러스터 노드에도 사용됩니다. 각 클러스터에 대해 고유한 vSphere 포드 CIDR 범위를 지정해야 합니다. **참고** vSphere 포드 CIDR 범위와 Kubernetes 서비스 주소의 CIDR 범위는 겹치지 않아야 합니다.
Kubernetes 서비스 CIDR 범위	/개인 IP 주소 16개	Kubernetes 서비스에 IP 주소를 할당할 개인 CIDR 범위. 각 감독자에 대해 고유한 Kubernetes 서비스 CIDR 범위를 지정해야 합니다.
송신 CIDR 범위	/정적 IP 주소 27개	Kubernetes 서비스의 송신 IP를 결정하는 개인 CIDR 주석. 감독자의 각 네임스페이스에는 송신 IP 주소가 하나만 할당됩니다. 송신 IP는 외부 엔티티가 네임스페이스의 서비스와 통신하는 데 사용하는 주소입니다. 송신 IP 주소 수는 감독자가 포함할 수 있는 송신 정책의 수를 제한합니다. 최소값은 /27 이상의 CIDR입니다. 예를 들어 `10.174.4.96/27`입니다. **참고** 송신 IP 주소 및 수신 IP 주소는 겹치지 않아야 합니다.
수신 CIDR	/정적 IP 주소 27개	수신 IP 주소에 사용되는 개인 CIDR 범위. 수신을 사용하면 외부 네트워크에서 감독자로 들어오는 요청에 트래픽 정책을 적용할 수 있습니다. 수신 IP 주소 수는 클러스터가 포함할 수 있는 수신의 수를 제한합니다. 최소값은 /27 이상의 CIDR입니다. **참고** 송신 IP 주소 및 수신 IP 주소는 겹치지 않아야 합니다.
네임스페이스 네트워크 범위	1	서브넷/세그먼트를 생성하고 워크로드에 IP 주소를 할당하기 위해 하나 이상의 IP CIDR이 필요합니다.
네임스페이스 서브넷 접두사	1	네임스페이스 세그먼트용으로 예약된 서브넷의 크기를 지정하는 서브넷 접두사가 필요합니다. Default is 28.

표 5-17. NSX 요구 사항

구성 요소	최소 수량	V
VLAN	3	이러한 VLAN IP는 TEP(터널 끝점)의 IP 주소입니다. ESXi 호스트 TEP와 Edge TEP는 라우팅이 가능해야 합니다. 다음에 VLAN IP 주소가 필요합니다. ■ ESXi 호스트 VTEP ■ 정적 IP를 사용하는 Edge VTEP ■ 전송 노드에 대한 업링크 및 Tier 0 게이트웨이. **참고** ESXi 호스트 VTEP 및 Edge VTEP의 MTU 크기가 1600보다 커야 합니다. ESXi 호스트와 NSX-T Edge 노드는 터널 끝점으로 작동하며 각 호스트와 Edge 노드에 TEP(터널 끝점) IP가 할당됩니다. ESXi 호스트의 TEP IP가 Edge 노드에 TEP IP로 오버레이 터널을 생성하기 때문에 VLAN IP를 라우팅할 수 있어야 합니다. Tier-0 게이트웨이에 대한 North-South 연결을 제공하려면 추가 VLAN이 필요합니다. IP 풀은 여러 클러스터 간에 공유될 수 있습니다. 하지만 호스트 오버레이 IP 풀/VLAN은 Edge 오버레이 IP 풀/VLAN과 공유해서는 안 됩니다. **참고** 호스트 TEP와 Edge TEP가 서로 다른 물리적 NIC를 사용하는 경우 동일한 VLAN을 사용할 수 있습니다.
Tier-0 업링크 IP	/개인 IP 주소 24개	Tie-0 업링크에 사용되는 IP 서브넷. Tie-0 업링크의 IP 주소에 대한 요구 사항은 다음과 같습니다. ■ IP 1개, Edge 이중화를 사용하지 않는 경우. ■ IP 4개, BGP와 Edge 이중화를 사용하는 경우. Edge당 IP 주소 2개. ■ IP 3개, 정적 경로와 Edge 이중화를 사용하는 경우. Edge 관리 IP, 서브넷, 게이트웨이, 업링크 IP, 서브넷, 게이트웨이는 고유해야 합니다.

표 5-18. 로드 밸런서 네트워킹 요구 사항

NTP 및 DNS 서버	1	NSX Advanced Load Balancer 컨트롤러가 vCenter Server 및 ESXi 호스트 이름을 올바르게 확인하려면 DNS 서버 IP가 필요합니다. 공용 NTP 서버가 기본적으로 사용되므로 NTP는 선택 사항입니다.
데이터 네트워크 서브넷	1	서비스 엔진이라고도 하는 서비스 엔진의 데이터 인터페이스가 이 네트워크에 연결됩니다. 서비스 엔진에 대한 IP 주소 풀을 구성합니다. 로드 밸런서 VIP(가상 IP)는 이 네트워크에서 할당됩니다.

표 5-18. 로드 밸런서 네트워킹 요구 사항 (계속)

NSX Advanced Load Balancer 컨트롤러 IP	1 또는 4	NSX Advanced Load Balancer 컨트롤러를 단일 노드로 배포하는 경우 해당 관리 인터페이스에 하나의 정적 IP가 필요합니다. 3노드 클러스터의 경우 4개의 IP 주소가 필요합니다. 각 컨트롤러 VM에 대해 1개씩 그리고 클러스터 VIP에 대해 1개입니다. 이러한 IP는 관리 네트워크 서브넷의 IP여야 합니다.
VIP IPAM 범위	-	Kubernetes 서비스에 IP 주소를 할당할 개인 CIDR 범위. IP는 데이터 네트워크 서브넷의 IP여야 합니다. 각 감독자 클러스터에 대해 고유한 Kubernetes 서비스 CIDR 범위를 지정해야 합니다.

포트 및 프로토콜

이 표에는 NSX Advanced Load Balancer, vCenter Server 및 기타 vSphere IaaS control plane 구성 요소 간의 IP 연결을 관리하는 데 필요한 프로토콜 및 포트가 나열되어 있습니다.

소스	대상	프로토콜 및 포트
NSX Advanced Load Balancer Controller	NSX Advanced Load Balancer 컨트롤러(클러스터 내)	TCP 22(SSH) TCP 443(HTTPS) TCP 8443(HTTPS)
서비스 엔진	HA의 서비스 엔진	VMware, LSC 및 NSX-T 클라우드에 대해 TCP 9001
서비스 엔진	NSX Advanced Load Balancer Controller	TCP 22(SSH) TCP 8443(HTTPS) UDP 123(NTP)
NSX Advanced Load Balancer Controller	vCenter Server, ESXi, NSX-T Manager	TCP 443(HTTPS)
감독자 제어부 노드(AKO)	NSX Advanced Load Balancer Controller	TCP 443(HTTPS)

NSX Advanced Load Balancer의 포트 및 프로토콜에 대한 자세한 내용은 https://ports.esp.vmware.com/home/NSX-Advanced-Load-Balancer 항목을 참조하십시오.

HAProxy 로드 밸런서가 있는 영역 감독자 배포 요구 사항

vSphere 영역에 매핑된 3개의 vSphere 클러스터에서 VDS 네트워킹 및 HAProxy 로드 밸런서가 있는 감독자를 사용하도록 설정하기 위한 요구 사항을 확인하십시오.

물리적 사이트 간에 vSphere 영역 배치

사이트 간의 지연 시간이 100ms를 초과하지 않는 한 여러 물리적 사이트에 vSphere 영역을 분산할 수 있습니다. 예를 들어 vSphere 영역을 두 개의 물리적 사이트(첫 번째 사이트의 vSphere 영역 하나, 두 번째 사이트의 vSphere 영역 두 개)에 분산할 수 있습니다.

최소 계산 요구 사항

이 표에는 3개의 vSphere 영역에서 VDS 네트워킹 및 HA Proxy 로드 밸런서가 있는 감독자를 사용하도록 설정하기 위한 최소 계산 요구 사항이 나와 있습니다. 관리 도메인과 워크로드 도메인을 분리하는 것이 가장 좋습니다. 워크로드 도메인은 워크로드를 실행하는 감독자를 호스팅합니다. 관리 도메인은 vCenter Server와 같은 모든 관리 구성 요소를 호스팅합니다.

시스템	최소 배포 크기	CPU	메모리	스토리지
vCenter Server 8.0	작음	2	21 GB	290GB
vSphere 클러스터	■ 3개의 vSphere 클러스터 ■ 각 vSphere 클러스터에서 vSphere DRS 및 HA가 사용되도록 설정되어 있어야 합니다. vSphere DRS는 완전히 자동화되거나 부분적으로 자동화된 모드여야 합니다. ■ 각 vSphere 클러스터에 대해 독립적으로 구성된 스토리지 및 네트워킹이 있어야 합니다.	해당 없음	해당 없음	해당 없음
ESXi 호스트 8.0	각 vSphere 클러스터에 대해 다음을 수행합니다. ■ vSAN 미포함: 호스트당 정적 IP가 1개인 ESXi 호스트 3개 ■ vSAN 포함: 클러스터당 물리적 NIC가 2개 이상인 ESXi 호스트 4개. **참고** 클러스터에 참여하는 호스트의 이름에 소문자를 사용하는지 확인합니다. 그렇지 않으면 감독자의 사용 설정이 실패할 수 있습니다.	8	호스트당 64GB	해당 없음
Kubernetes 제어부 VM	3	4	16GB	16GB

최소 네트워크 요구 사항

참고 vSphere 8 감독자를 사용하여 IPv6 클러스터를 생성하거나 IPv6 클러스터를 Tanzu Mission Control에 등록할 수 없습니다.

표 5-19. 물리적 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
계층 2 디바이스	1	감독자의 트래픽을 처리할 관리 네트워크는 감독자의 모든 클러스터 부분에 대해 동일한 계층 2 디바이스에 있어야 합니다. 기본 워크로드 네트워크도 동일한 계층 2 디바이스에 있어야 합니다.
물리적 네트워크 MTU	1500	MTU 크기는 분산 포트 그룹에서 1500 이상이어야 합니다.

표 5-20. 일반 네트워킹 요구 사항

구성 요소	최소 수량	필수 구성
지연 시간	100 ms	감독자에 함께 가입된 vSphere 영역의 일부인 각 클러스터 간의 최대 권장 지연 시간입니다.
NTP 및 DNS 서버	1	vCenter Server에서 사용할 수 있는 DNS 서버 및 NTP 서버. **참고** 모든 ESXi 호스트 및 vCenter Server에서 NTP를 구성합니다.
DHCP 서버	1	선택 사항입니다. 관리 및 워크로드 네트워크와 부동 IP에 대한 IP 주소를 자동으로 획득하도록 DHCP 서버를 구성합니다. DHCP 서버는 클라이언트 식별자를 지원하고 호환되는 DNS 서버, DNS 검색 도메인 및 NTP 서버를 제공해야 합니다. 관리 네트워크의 경우 제어부 VM IP, 부동 IP, DNS 서버, DNS, 검색 도메인 및 NTP 서버와 같은 모든 IP 주소가 DHCP 서버에서 자동으로 획득됩니다. DHCP 구성은 감독자에서 사용됩니다. 로드 밸런서에는 관리를 위한 정적 IP 주소가 필요할 수 있습니다. DHCP 범위는 이러한 정적 IP와 겹치지 않아야 합니다. DHCP는 가상 IP에 사용되지 않습니다. (VIP)

표 5-21. 관리 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
Kubernetes 제어부 VM에 대한 정적 IP	5개의 블록	관리 네트워크에서 감독자의 Kubernetes 제어부 VM으로 할당할 5개의 연속적 정적 IP 주소 블록.
관리 트래픽 네트워크	1	ESXi 호스트, vCenter Server, 감독자 및 로드 밸런서로 라우팅할 수 있는 관리 네트워크.

표 5-21. 관리 네트워크 요구 사항 (계속)

구성 요소	최소 수량	필수 구성
관리 네트워크 서브넷	1	ESXi 호스트, vCenter Server 및 Kubernetes 제어부 사이의 관리 트래픽에 사용되는 서브넷. 서브넷의 크기는 다음과 같아야 합니다. ■ 호스트 VMkernel 어댑터당 IP 주소 1개. ■ vCenter Server Appliance에 대해 IP 주소 1개. ■ Kubernetes 제어부에 대해 IP 주소 5개. 3개 노드 각각에 대해 1개, 가상 IP에 1개, 롤링 클러스터 업그레이드에 1개. **참고** 관리 네트워크와 워크로드 네트워크는 서로 다른 서브넷에 있어야 합니다. 관리 및 워크로드 네트워크에 동일한 서브넷을 할당하는 것은 지원되지 않으며 시스템 오류 및 문제가 발생할 수 있습니다.
관리 네트워크 VLAN	1	관리 네트워크 서브넷의 VLAN ID.

표 5-22. 워크로드 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
vSphere Distributed Switch	1	vSphere 클러스터 3개 모두에 있는 모든 호스트는 VDS에 연결되어야 합니다.
워크로드 네트워크	1	기본 워크로드 네트워크로 구성한 VDS에 분산 포트 그룹을 하나 이상 생성해야 합니다. 선택한 토폴로지에 따라 네임스페이스의 워크로드 네트워크와 동일한 분산 포트 그룹을 사용하거나 더 많은 포트 그룹을 생성하고 이를 워크로드 네트워크로 구성할 수 있습니다. 워크로드 네트워크는 다음 요구 사항을 충족해야 합니다. ■ HAProxy가 가상 IP 할당에 사용하는 네트워크가 있는 모든 워크로드 네트워크 간에 라우팅이 가능해야 합니다. ■ 감독자 내의 모든 워크로드 네트워크에서 IP 주소 범위가 겹치지 않아야 합니다. **중요** 워크로드 네트워크는 관리 네트워크와 다른 서브넷에 있어야 합니다.
Kubernetes 서비스 CIDR 범위	/개인 IP 주소 16개	Kubernetes 서비스에 IP 주소를 할당할 개인 CIDR 범위. 각 감독자에 대해 고유한 Kubernetes 서비스 CIDR 범위를 지정해야 합니다.

표 5-23. 로드 밸런서 네트워킹 요구 사항

HAProxy 로드 밸런서	1	vCenter Server 인스턴스로 구성된 HAProxy 로드 밸런서의 인스턴스입니다. ■ 동일한 HAProxy 인스턴스가 여러 감독자를 처리하는 경우 모든 감독자의 모든 워크로드 네트워크에서 트래픽을 라우팅할 수 있어야 합니다. ■ HAProxy가 서비스를 제공하는 모든 감독자의 워크로드 네트워크에서 IP 범위가 겹치지 않아야 합니다. ■ HAProxy가 가상 IP를 할당하는 데 사용하는 네트워크는 HAProxy가 연결된 모든 감독자에서 사용되는 워크로드 네트워크로 라우팅할 수 있어야 합니다.
가상 서버 IP 범위	1	가상 IP에 대한 전용 IP 범위입니다. HAProxy VM은 이 가상 IP 범위의 유일한 소유자여야 합니다. 범위는 임의의 감독자가 소유한 워크로드 네트워크에 할당된 IP 범위와 겹치지 않아야 합니다. 범위는 관리 네트워크와 동일한 서브넷에 있으면 안됩니다.

클러스터 감독자 배포 요구 사항

6

하나의 vSphere 영역에 매핑되는 단일 vSphere 클러스터에서 감독자를 사용하도록 설정하기 위한 요구 사항을 확인하십시오.

다음으로 아래 항목을 읽으십시오.

- NSX Advanced Load Balancer 및 VDS 네트워킹을 사용하는 클러스터 감독자 배포 요구 사항
- NSX를 사용한 클러스터 감독자 배포 요구 사항
- NSX 및 NSX Advanced Load Balancer를 사용한 클러스터 감독자 배포 요구 사항
- VDS 네트워킹 및 HAProxy 로드 밸런서를 사용한 클러스터 감독자 배포 요구 사항

NSX Advanced Load Balancer 및 VDS 네트워킹을 사용하는 클러스터 감독자 배포 요구 사항

vDS 네트워킹 및 NSX Advanced Load Balancer(Avi 로드 밸런서라고도 함)가 있는 vSphere 클러스터에서 감독자를 사용하도록 설정하기 위한 요구 사항을 알아봅니다. vSphere IaaS control plane는 여러 토폴로지를 지원합니다. Avi 서비스 엔진 및 로드 밸런서 서비스를 위한 단일 vDS 네트워크를 사용할 수도 있고, Avi 관리부용 vDS와 NSX Advanced Load Balancer용 vDS를 별도로 사용할 수도 있습니다.

워크로드 네트워크

vDS 네트워킹 스택을 사용하여 감독자를 구성하려면 클러스터의 모든 호스트를 vDS에 연결해야 합니다. 감독자에 대해 구현하는 토폴로지에 따라 하나 이상의 분산 포트 그룹을 생성합니다. 포트 그룹을 vSphere 네임스페이스에 대한 워크로드 네트워크로 지정합니다. 워크로드 네트워크는 Tanzu Kubernetes Grid 클러스터 노드 및 감독자 제어부 VM에 대한 연결을 제공합니다. Kubernetes 제어부 VM에 대한 연결을 제공하는 워크로드 네트워크를 기본 워크로드 네트워크라고 합니다. 각 감독자에는 기본 워크로드 네트워크가 하나씩 있어야 합니다. 분산 포트 그룹 중 하나를 감독자에 대한 기본 워크로드 네트워크로 지정해야 합니다.

감독자의 Kubernetes 제어부 VM은 기본 워크로드 네트워크에 할당된 IP 주소 범위에서 3개의 IP 주소를 사용합니다. Tanzu Kubernetes Grid 클러스터의 각 노드에는 Tanzu Kubernetes Grid 클러스터가 실행되는 네임스페이스로 구성된 워크로드 네트워크의 주소 범위에서 할당된 별도의 IP 주소가 있습니다.

네트워킹 요구 사항

NSX Advanced Load Balancer에는 라우팅 가능한 서브넷이 2개 필요합니다.

- 관리 네트워크. 관리 네트워크는 컨트롤러라고도 하는 NSX Advanced Load Balancer 컨트롤러가 상주하는 곳입니다. 관리 네트워크는 컨트롤러에 vCenter Server, ESXi 호스트, 감독자 제어부 노드에 대한 연결을 제공합니다. 이 네트워크에는 Avi 서비스 엔진의 관리 인터페이스가 배치됩니다. 이 네트워크에는 vDS 및 분산 포트 그룹이 필요합니다.
- 데이터 네트워크. 서비스 엔진이라고도 하는 Avi 서비스 엔진의 데이터 인터페이스가 이 네트워크에 연결됩니다. 로드 밸런서 VIP(가상 IP)는 이 네트워크에서 할당됩니다. 이 네트워크에는 vDS 및 분산 포트 그룹이 필요합니다. 로드 밸런서를 설치하기 전에 vDS 및 분산 포트 그룹을 반드시 구성해야 합니다.

IP 주소 할당

컨트롤러와 서비스 엔진은 관리 네트워크에 연결됩니다. NSX Advanced Load Balancer를 설치하고 구성할 때 각 컨트롤러 VM에 정적, 라우팅 가능 IP 주소를 제공합니다.

서비스 엔진은 DHCP를 사용할 수 있습니다. DHCP를 사용할 수 없는 경우 서비스 엔진에 대한 IP 주소 풀을 구성할 수 있습니다.

최소 계산 요구 사항

이 표에는 NSX Advanced Load Balancer를 사용하는 VDS 네트워킹에 대한 최소 계산 요구 사항이 나열되어 있습니다. 관리 도메인과 워크로드 도메인을 분리하는 것이 가장 좋습니다. 워크로드 도메인은 워크로드를 실행하는 감독자를 호스팅합니다. 관리 도메인은 vCenter Server와 같은 모든 관리 구성 요소를 호스팅합니다.

표 6-1. 최소 계산 요구 사항

시스템	최소 배포 크기	CPU	메모리	스토리지
vCenter Server8.0	작음	2	21 GB	290GB
ESXi 호스트 8.0	■ vSAN 미포함: 호스트당 정적 IP가 1개인 ESXi 호스트 3개. ■ vSAN 포함: 클러스터당 물리적 NIC가 2개 이상인 ESXi 호스트 4개. 호스트는 vSphere DRS 및 HA를 사용하도록 설정된 클러스터에 가입되어 있어야 합니다. vSphere DRS는 완전히 자동화되거나 부분적으로 자동화된 모드여야 합니다. **참고** 클러스터에 참여하는 호스트의 이름에 소문자를 사용하는지 확인합니다. 그렇지 않으면 감독자의 사용 설정이 실패할 수 있습니다.	8	호스트당 64GB	해당 없음
Kubernetes 제어부 VM	3	4	16GB	16GB

표 6-1. 최소 계산 요구 사항 (계속)

시스템	최소 배포 크기	CPU	메모리	스토리지
NSX Advanced Load Balancer Controller	Enterprise 운영 환경의 경우 3개의 Avi 컨트롤러 VM으로 구성된 클러스터를 설치하는 것이 좋습니다. HA에는 최소 2개의 서비스 엔진 VM이 필요합니다.	4(작음) 8(중간) 24(큼)	12 GB 24GB 128 GB	128 GB 128 GB 128 GB
서비스 엔진	HA에는 최소 2개의 서비스 엔진 VM이 필요합니다.	1	2GB	15 GB

최소 네트워크 요구 사항

이 표에는 NSX Advanced Load Balancer를 사용하는 vSphere 네트워킹에 대한 최소 네트워크 요구 사항이 나열되어 있습니다.

참고 vSphere 7 감독자를 사용하여 IPv6 클러스터를 생성하거나 IPv6 클러스터를 Tanzu Mission Control에 등록할 수 없습니다. NSX Advanced Load Balancer 서비스는 현재 IPv6을 지원하지 않습니다.

표 6-2. 물리적 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
물리적 네트워크 MTU	1500	MTU 크기는 분산 포트 그룹에서 1500 이상이어야 합니다.

표 6-3. 일반 네트워킹 요구 사항

구성 요소	최소 수량	필수 구성
NTP 및 DNS 서버	1	vCenter Server에서 사용할 수 있는 DNS 서버 및 NTP 서버. **참고** 모든 ESXi 호스트 및 vCenter Server에서 NTP를 구성합니다.
DHCP 서버	1	선택 사항입니다. 관리 및 워크로드 네트워크와 부동 IP에 대한 IP 주소를 자동으로 획득하도록 DHCP 서버를 구성합니다. DHCP 서버는 클라이언트 식별자를 지원하고 호환되는 DNS 서버, DNS 검색 도메인 및 NTP 서버를 제공해야 합니다. 관리 네트워크의 경우 제어부 VM IP, 부동 IP, DNS 서버, DNS, 검색 도메인 및 NTP 서버와 같은 모든 IP 주소가 DHCP 서버에서 자동으로 획득됩니다. DHCP 구성은 감독자에서 사용됩니다. 로드 밸런서에는 관리를 위한 정적 IP 주소가 필요할 수 있습니다. DHCP 범위는 이러한 정적 IP와 겹치지 않아야 합니다. DHCP는 가상 IP에 사용되지 않습니다. (VIP) **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.

표 6-4. 관리 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
Kubernetes 제어부 VM에 대한 정적 IP	5개의 블록	관리 네트워크에서 감독자의 Kubernetes 제어부 VM으로 할당할 5개의 연속적 정적 IP 주소 블록.
관리 트래픽 네트워크	1	ESXi 호스트, vCenter Server, 감독자 및 로드 밸런서로 라우팅할 수 있는 관리 네트워크.
관리 네트워크 서브넷	1	관리 네트워크는 컨트롤러라고도 하는 NSX Advanced Load Balancer 컨트롤러가 상주하는 곳입니다. 또한 서비스 엔진 관리 인터페이스가 연결되는 위치이기도 합니다. 컨트롤러는 이 네트워크의 vCenter Server 및 ESXi 관리 IP에 연결되어야 합니다. **참고** 관리 네트워크와 워크로드 네트워크는 서로 다른 서브넷에 있어야 합니다. 관리 및 워크로드 네트워크에 동일한 서브넷을 할당하는 것은 지원되지 않으며 시스템 오류 및 문제가 발생할 수 있습니다.

표 6-5. 워크로드 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
vSphere Distributed Switch	1	vSphere 클러스터에 있는 모든 호스트는 VDS에 연결되어야 합니다.
워크로드 네트워크	1	기본 워크로드 네트워크로 구성한 VDS에 분산 포트 그룹을 하나 이상 생성해야 합니다. 선택한 토폴로지에 따라 네임스페이스의 워크로드 네트워크와 동일한 분산 포트 그룹을 사용하거나 더 많은 포트 그룹을 생성하고 이를 워크로드 네트워크로 구성할 수 있습니다. 워크로드 네트워크는 다음 요구 사항을 충족해야 합니다. ■ NSX Advanced Load Balancer가 가상 IP 할당에 사용하는 네트워크가 있는 모든 워크로드 네트워크 간에 라우팅이 가능해야 합니다. ■ 감독자 내의 모든 워크로드 네트워크에서 IP 주소 범위가 겹치지 않아야 합니다.
Kubernetes 서비스 CIDR 범위	/개인 IP 주소 16개	Kubernetes 서비스에 IP 주소를 할당할 개인 CIDR 범위. 각 감독자에 대해 고유한 Kubernetes 서비스 CIDR 범위를 지정해야 합니다.

표 6-6. 로드 밸런서 네트워킹 요구 사항

NTP 및 DNS 서버	1	NSX Advanced Load Balancer 컨트롤러가 vCenter Server 및 ESXi 호스트 이름을 올바르게 확인하려면 DNS 서버 IP가 필요합니다. 공용 NTP 서버가 기본적으로 사용되므로 NTP는 선택 사항입니다.
데이터 네트워크 서브넷	1	서비스 엔진이라고도 하는 NSX Advanced Load Balancer 서비스 엔진의 데이터 인터페이스가 이 네트워크에 연결됩니다. 서비스 엔진에 대한 IP 주소 풀을 구성합니다. 로드 밸런서 VIP(가상 IP)는 이 네트워크에서 할당됩니다.

표 6-6. 로드 밸런서 네트워킹 요구 사항 (계속)

NSX Advanced Load Balancer 컨트롤러 IP	1 또는 4	NSX Advanced Load Balancer 컨트롤러를 단일 노드로 배포하는 경우 해당 관리 인터페이스에 하나의 정적 IP가 필요합니다. 3노드 클러스터의 경우 4개의 IP 주소가 필요합니다. 각 NSX Advanced Load Balancer 컨트롤러 VM에 대해 1개씩 그리고 클러스터 VIP에 대해 1개입니다. 이러한 IP는 관리 네트워크 서브넷의 IP여야 합니다.
VIP IPAM 범위	-	Kubernetes 서비스에 IP 주소를 할당할 개인 CIDR 범위. IP는 데이터 네트워크 서브넷의 IP여야 합니다. 각 감독자 클러스터에 대해 고유한 Kubernetes 서비스 CIDR 범위를 지정해야 합니다.

포트 및 프로토콜

이 표에는 NSX Advanced Load Balancer, vCenter 및 기타 vSphere IaaS control plane 구성 요소 간의 IP 연결을 관리하는 데 필요한 프로토콜 및 포트가 나열되어 있습니다.

소스	대상	프로토콜 및 포트
NSX Advanced Load Balancer Controller	NSX Advanced Load Balancer 컨트롤러(클러스터 내)	TCP 22(SSH) TCP 443(HTTPS) TCP 8443(HTTPS)
서비스 엔진	HA의 서비스 엔진	VMware, LSC 및 NSX-T 클라우드에 대해 TCP 9001
서비스 엔진	NSX Advanced Load Balancer 컨트롤러	TCP 22(SSH) TCP 8443(HTTPS) UDP 123(NTP)
Avi 컨트롤러	vCenter Server, ESXi, NSX-T Manager	TCP 443(HTTPS)
감독자 제어부 노드(AKO)	NSX Advanced Load Balancer 컨트롤러	TCP 443(HTTPS)

NSX Advanced Load Balancer의 포트 및 프로토콜에 대한 자세한 내용은 https://ports.esp.vmware.com/home/NSX-Advanced-Load-Balancer 항목을 참조하십시오.

NSX를 사용한 클러스터 감독자 배포 요구 사항

NSX 네트워킹 스택을 사용하여 vSphere 클러스터에서 vSphere IaaS control plane를 구성하기 위한 시스템 요구 사항을 검토합니다. vSphere 클러스터를 감독자로 사용하도록 설정하면 감독자에 대해 vSphere 영역이 자동으로 생성됩니다.

이러한 요구 사항 외에도 NSX 배포를 위한 모범 사례에 대한 자세한 내용은 NSX 참조 설계 가이드를 참조하십시오.

관리 및 Edge 클러스터에 대한 최소 계산 요구 사항

시스템	최소 배포 크기	CPU	메모리	스토리지
vCenter Server 8	작음	2	21 GB	290GB
ESXi 호스트 8	ESXi 호스트 2개	8	호스트당 64GB	해당 없음
NSX Manager	중간	6	24GB	300GB
NSX Edge 1	큼	8	32GB	200GB
NSX Edge 2	큼	8	32GB	200GB

참고 vSphere IaaS control plane를 구성하려는 vSphere 클러스터에 참여하는 모든 ESXi 호스트가 NSX 전송 노드로 준비되었는지 확인합니다. 자세한 내용은 NSX 설명서에서 https://kb.vmware.com/s/article/95820 및 ESXi 호스트를 전송 노드로 준비를 참조하십시오.

워크로드 도메인 클러스터에 대한 최소 계산 요구 사항

시스템	최소 배포 크기	CPU	메모리	스토리지
vSphere 클러스터	■ vSphere 클러스터 1개 ■ vSphere 클러스터에서 vSphere DRS 및 HA가 사용되도록 설정되어 있어야 합니다. vSphere DRS는 완전히 자동화된 모드여야 합니다.	해당 없음	해당 없음	해당 없음
ESXi 호스트 8	■ vSAN 미포함: 호스트당 정적 IP가 1개인 ESXi 호스트 3개. ■ vSAN 포함: 물리적 NIC가 2개 이상인 ESXi 호스트 4개. **참고** 클러스터에 참여하는 호스트의 이름에 소문자를 사용하는지 확인합니다. 그렇지 않으면 감독자 활성화가 실패할 수 있습니다.	8	호스트당 64GB	해당 없음
Kubernetes 제어부 VM	3	4	16GB	16GB

네트워킹 요구 사항

참고 vSphere 8 감독자를 사용하여 IPv6 클러스터를 생성하거나 IPv6 클러스터를 Tanzu Mission Control에 등록할 수 없습니다.

지원되는 NSX 버전은 VMware 제품 상호 운용성 매트릭스를 확인하십시오.

표 6-7. 물리적 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
물리적 네트워크 MTU	1500	MTU 크기는 모든 vSphere Distributed Switch 포트 그룹에서 1500 이상이어야 합니다.
물리적 NIC	vSAN을 사용하는 경우 호스트당 2개 이상의 물리적 NIC	Antrea CNI를 사용하고 최적의 NSX 성능을 얻으려면 참여하는 각 ESXi 호스트의 물리적 NIC 각각이 GENEVE 캡슐화를 지원하고 사용하도록 설정되어 있어야 합니다.

표 6-8. 일반 네트워킹 요구 사항

구성 요소	최소 수량	필수 구성
NTP 및 DNS 서버	1	vCenter Server에서 사용할 수 있는 DNS 서버 및 NTP 서버. **참고** 모든 ESXi 호스트 및 vCenter Server에서 NTP를 구성합니다.
DHCP 서버	1	선택 사항입니다. 관리 및 워크로드 네트워크와 부동 IP에 대한 IP 주소를 자동으로 획득하도록 DHCP 서버를 구성합니다. DHCP 서버는 클라이언트 식별자를 지원하고 호환되는 DNS 서버, DNS 검색 도메인 및 NTP 서버를 제공해야 합니다. 관리 네트워크의 경우 제어부 VM IP, 부동 IP, DNS 서버, DNS, 검색 도메인 및 NTP 서버와 같은 모든 IP 주소가 DHCP 서버에서 자동으로 획득됩니다. DHCP 구성은 감독자에서 사용됩니다. 로드 밸런서에는 관리를 위한 정적 IP 주소가 필요할 수 있습니다. DHCP 범위는 이러한 정적 IP와 겹치지 않아야 합니다. DHCP는 가상 IP에 사용되지 않습니다. (VIP)
이미지 레지스트리	1	서비스를 위해 레지스트리에 액세스.

표 6-9. 관리 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
Kubernetes 제어부 VM에 대한 정적 IP	5개의 블록	관리 네트워크에서 감독자의 Kubernetes 제어부 VM으로 할당할 5개의 연속적 정적 IP 주소 블록.
관리 트래픽 네트워크	1	ESXi 호스트, vCenter Server, 감독자 및 로드 밸런서로 라우팅할 수 있는 관리 네트워크.

표 6-9. 관리 네트워크 요구 사항 (계속)

구성 요소	최소 수량	필수 구성
관리 네트워크 서브넷	1	ESXi 호스트와 vCenter Server, NSX 장치 및 Kubernetes 제어부 사이의 관리 트래픽에 사용되는 서브넷. 서브넷의 크기는 다음과 같아야 합니다. ■ 호스트 VMkernel 어댑터당 IP 주소 1개. ■ vCenter Server Appliance에 대해 IP 주소 1개. ■ NSX Manager에 대해 IP 주소 1개 또는 4개. 3개 노드 및 1개 VIP(가상 IP)의 NSX Manager 클러스터링 수행 시 4개. ■ Kubernetes 제어부에 대해 IP 주소 5개. 3개 노드 각각에 대해 1개, 가상 IP에 1개, 롤링 클러스터 업그레이드에 1개. **참고** 관리 네트워크와 워크로드 네트워크는 서로 다른 서브넷에 있어야 합니다. 관리 및 워크로드 네트워크에 동일한 서브넷을 할당하는 것은 지원되지 않으며 시스템 오류 및 문제가 발생할 수 있습니다.
관리 네트워크 VLAN	1	관리 네트워크 서브넷의 VLAN ID.

표 6-10. 워크로드 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
vSphere 포드 CIDR 범위	/개인 IP 주소 23개	vSphere 포드의 IP 주소를 제공하는 개인 CIDR 범위입니다. 이러한 주소는 Tanzu Kubernetes Grid 클러스터 노드에도 사용됩니다. 각 클러스터에 대해 고유한 vSphere 포드 CIDR 범위를 지정해야 합니다. **참고** vSphere 포드 CIDR 범위와 Kubernetes 서비스 주소의 CIDR 범위는 겹치지 않아야 합니다.
Kubernetes 서비스 CIDR 범위	/개인 IP 주소 16개	Kubernetes 서비스에 IP 주소를 할당할 개인 CIDR 범위. 각 감독자에 대해 고유한 Kubernetes 서비스 CIDR 범위를 지정해야 합니다.

표 6-10. 워크로드 네트워크 요구 사항 (계속)

구성 요소	최소 수량	필수 구성
송신 CIDR 범위	/정적 IP 주소 27개	Kubernetes 서비스의 송신 IP를 결정하는 개인 CIDR 주석. 감독자의 각 네임스페이스에는 송신 IP 주소가 하나만 할당됩니다. 송신 IP는 외부 엔티티가 네임스페이스의 서비스와 통신하는 데 사용하는 주소입니다. 송신 IP 주소 수는 감독자가 포함할 수 있는 송신 정책의 수를 제한합니다. 최소값은 /27 이상의 CIDR입니다. 예를 들어 `10.174.4.96/27`입니다. **참고** 송신 IP 주소 및 수신 IP 주소는 겹치지 않아야 합니다.
수신 CIDR	/정적 IP 주소 27개	수신 IP 주소에 사용되는 개인 CIDR 범위. 수신을 사용하면 외부 네트워크에서 감독자로 들어오는 요청에 트래픽 정책을 적용할 수 있습니다. 수신 IP 주소 수는 클러스터가 포함할 수 있는 수신의 수를 제한합니다. 최소값은 /27 이상의 CIDR입니다. **참고** 송신 IP 주소 및 수신 IP 주소는 겹치지 않아야 합니다.
네임스페이스 네트워크 범위	1	서브넷/세그먼트를 생성하고 워크로드에 IP 주소를 할당하기 위해 하나 이상의 IP CIDR이 필요합니다.
네임스페이스 서브넷 접두사	1	네임스페이스 세그먼트용으로 예약된 서브넷의 크기를 지정하는 서브넷 접두사가 필요합니다. Default is 28.

표 6-11. NSX 요구 사항

구성 요소	최소 수량	필수 구성
VLAN	3	이러한 VLAN IP는 TEP(터널 끝점)의 IP 주소입니다. ESXi 호스트 TEP와 Edge TEP는 라우팅이 가능해야 합니다. 다음에 VLAN IP 주소가 필요합니다. ■ ESXi 호스트 VTEP ■ 정적 IP를 사용하는 Edge VTEP ■ 전송 노드에 대한 업링크 및 Tier 0 게이트웨이. **참고** ESXi 호스트 VTEP 및 Edge VTEP의 MTU 크기가 1600보다 커야 합니다. ESXi 호스트와 NSX-T Edge 노드는 터널 끝점으로 작동하며 각 호스트와 Edge 노드에 TEP(터널 끝점) IP가 할당됩니다. ESXi 호스트의 TEP IP가 Edge 노드에 TEP IP로 오버레이 터널을 생성하기 때문에 VLAN IP를 라우팅할 수 있어야 합니다. Tier-0 게이트웨이에 대한 North-South 연결을 제공하려면 추가 VLAN이 필요합니다. IP 풀은 여러 클러스터 간에 공유될 수 있습니다. 하지만 호스트 오버레이 IP 풀/VLAN은 Edge 오버레이 IP 풀/VLAN과 공유해서는 안 됩니다. **참고** 호스트 TEP와 Edge TEP가 서로 다른 물리적 NIC를 사용하는 경우 동일한 VLAN을 사용할 수 있습니다.
Tier-0 업링크 IP	/개인 IP 주소 24개	Tie-0 업링크에 사용되는 IP 서브넷. Tie-0 업링크의 IP 주소에 대한 요구 사항은 다음과 같습니다. ■ IP 1개, Edge 이중화를 사용하지 않는 경우. ■ IP 4개, BGP와 Edge 이중화를 사용하는 경우. Edge당 IP 주소 2개. ■ IP 3개, 정적 경로와 Edge 이중화를 사용하는 경우. Edge 관리 IP, 서브넷, 게이트웨이, 업링크 IP, 서브넷, 게이트웨이는 고유해야 합니다.

NSX 및 NSX Advanced Load Balancer를 사용한 클러스터 감독자 배포 요구 사항

NSX 네트워킹 스택을 사용하여 vSphere 클러스터에서 vSphere IaaS control plane를 구성하기 위한 시스템 요구 사항을 검토합니다. vSphere 클러스터를 감독자로 사용하도록 설정하면 감독자에 대해 vSphere 영역이 자동으로 생성됩니다.

NSX 배포 옵션

NSX 배포하는 모범 사례에 대한 자세한 내용은 NSX 참조 설계 가이드를 참조하십시오.

관리 및 Edge 클러스터에 대한 최소 계산 요구 사항

시스템	최소 배포 크기	CPU	메모리	스토리지
vCenter Server 8	작음	2	21 GB	290GB
ESXi 호스트 8	ESXi 호스트 2개	8	호스트당 64GB	해당 없음
NSX Manager	중간	6	24GB	300GB
NSX Edge 1	큼	8	32GB	200GB
NSX Edge 2	큼	8	32GB	200GB
서비스 엔진 VM	감독자당 2개 이상의 서비스 엔진 VM이 배포됩니다.	1	2GB	해당 없음

참고 vSphere IaaS control plane를 구성하려는 vSphere 클러스터에 참여하는 모든 ESXi 호스트가 NSX 전송 노드로 준비되었는지 확인합니다. 자세한 내용은 NSX 설명서에서 https://kb.vmware.com/s/article/95820 및 ESXi 호스트를 전송 노드로 준비를 참조하십시오.

컨트롤러의 시스템 용량 지정

배포 중에 컨트롤러의 시스템 용량을 지정할 수 있습니다. 시스템 용량은 CPU, RAM, 디스크와 같은 시스템 리소스 할당을 기반으로 합니다. 할당하는 리소스의 양은 컨트롤러 성능에 영향을 미칩니다.

배포 유형	노드 수	권장 할당-CPU	권장 할당-메모리	권장 할당-디스크
데모/고객 평가	1	6	24GB	128 GB

데모 배포에서는 단일 컨트롤러가 적절하며 모든 제어부 작업 및 워크플로와 분석에 사용됩니다.

운영 배포에서는 3노드 클러스터가 권장됩니다.

자세한 내용은 NSX Advanced Load Balancer 컨트롤러 크기 조정을 참조하십시오.

워크로드 도메인 클러스터에 대한 최소 계산 요구 사항

시스템	최소 배포 크기	CPU	메모리	스토리지
vSphere 클러스터	■ vSphere 클러스터 1개 ■ vSphere 클러스터에서 vSphere DRS 및 HA가 사용되도록 설정되어 있어야 합니다. vSphere DRS는 완전히 자동화된 모드여야 합니다.	해당 없음	해당 없음	해당 없음
ESXi 호스트 8	■ vSAN 미포함: 호스트당 정적 IP가 1개인 ESXi 호스트 3개. ■ vSAN 포함: 물리적 NIC가 2개 이상인 ESXi 호스트 4개. **참고** 클러스터에 참여하는 호스트의 이름에 소문자를 사용하는지 확인합니다. 그렇지 않으면 감독자 활성화가 실패할 수 있습니다.	8	호스트당 64GB	해당 없음
Kubernetes 제어부 VM	3	4	16GB	16GB

네트워킹 요구 사항

참고 vSphere 8 감독자를 사용하여 IPv6 클러스터를 생성하거나 IPv6 클러스터를 Tanzu Mission Control에 등록할 수 없습니다.

지원되는 NSX 버전은 VMware 제품 상호 운용성 매트릭스를 확인하십시오.

표 6-12. 물리적 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
물리적 네트워크 MTU	1700	MTU 크기는 모든 vSphere Distributed Switch 포트 그룹에서 1700 이상이어야 합니다.
물리적 NIC	vSAN을 사용하는 경우 호스트당 2개 이상의 물리적 NIC	Antrea CNI를 사용하고 최적의 NSX 성능을 얻으려면 참여하는 각 ESXi 호스트의 물리적 NIC 각각이 GENEVE 캡슐화를 지원하고 사용하도록 설정되어 있어야 합니다.

표 6-13. 일반 네트워킹 요구 사항

구성 요소	최소 수량	필수 구성
NTP 및 DNS 서버	1	vCenter Server에서 사용할 수 있는 DNS 서버 및 NTP 서버. **참고** 모든 ESXi 호스트 및 vCenter Server에서 NTP를 구성합니다.
DHCP 서버	1	선택 사항입니다. 관리 및 워크로드 네트워크와 부동 IP에 대한 IP 주소를 자동으로 획득하도록 DHCP 서버를 구성합니다. DHCP 서버는 클라이언트 식별자를 지원하고 호환되는 DNS 서버, DNS 검색 도메인 및 NTP 서버를 제공해야 합니다. 관리 네트워크의 경우 제어부 VM IP, 부동 IP, DNS 서버, DNS, 검색 도메인 및 NTP 서버와 같은 모든 IP 주소가 DHCP 서버에서 자동으로 획득됩니다. DHCP 구성은 감독자에서 사용됩니다. 로드 밸런서에는 관리를 위한 정적 IP 주소가 필요할 수 있습니다. DHCP 범위는 이러한 정적 IP와 겹치지 않아야 합니다. DHCP는 가상 IP에 사용되지 않습니다. (VIP)
이미지 레지스트리	1	서비스를 위해 레지스트리에 액세스.

표 6-14. 관리 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
Kubernetes 제어부 VM에 대한 정적 IP	5개의 블록	관리 네트워크에서 감독자의 Kubernetes 제어부 VM으로 할당할 5개의 연속적 정적 IP 주소 블록.
관리 트래픽 네트워크	1	ESXi 호스트, vCenter Server, 감독자 및 로드 밸런서로 라우팅할 수 있는 관리 네트워크.

표 6-14. 관리 네트워크 요구 사항 (계속)

구성 요소	최소 수량	필수 구성
관리 네트워크 서브넷	1	ESXi 호스트와 vCenter Server, NSX 장치 및 Kubernetes 제어부 사이의 관리 트래픽에 사용되는 서브넷. 서브넷의 크기는 다음과 같아야 합니다. ■ 호스트 VMkernel 어댑터당 IP 주소 1개. ■ vCenter Server Appliance에 대해 IP 주소 1개. ■ NSX Manager에 대해 IP 주소 1개 또는 4개. 3개 노드 및 1개 VIP(가상 IP)의 NSX Manager 클러스터링 수행 시 4개. ■ Kubernetes 제어부에 대해 IP 주소 5개. 3개 노드 각각에 대해 1개, 가상 IP에 1개, 롤링 클러스터 업그레이드에 1개. **참고** 관리 네트워크와 워크로드 네트워크는 서로 다른 서브넷에 있어야 합니다. 관리 및 워크로드 네트워크에 동일한 서브넷을 할당하는 것은 지원되지 않으며 시스템 오류 및 문제가 발생할 수 있습니다.
관리 네트워크 VLAN	1	관리 네트워크 서브넷의 VLAN ID.

표 6-15. 워크로드 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
vSphere 포드 CIDR 범위	/개인 IP 주소 23개	vSphere 포드의 IP 주소를 제공하는 개인 CIDR 범위입니다. 이러한 주소는 Tanzu Kubernetes Grid 클러스터 노드에도 사용됩니다. 각 클러스터에 대해 고유한 vSphere 포드 CIDR 범위를 지정해야 합니다. **참고** vSphere 포드 CIDR 범위와 Kubernetes 서비스 주소의 CIDR 범위는 겹치지 않아야 합니다.
Kubernetes 서비스 CIDR 범위	/개인 IP 주소 16개	Kubernetes 서비스에 IP 주소를 할당할 개인 CIDR 범위. 각 감독자에 대해 고유한 Kubernetes 서비스 CIDR 범위를 지정해야 합니다.

표 6-15. 워크로드 네트워크 요구 사항 (계속)

구성 요소	최소 수량	필수 구성
송신 CIDR 범위	/정적 IP 주소 27개	Kubernetes 서비스의 송신 IP를 결정하는 개인 CIDR 주석. 감독자의 각 네임스페이스에는 송신 IP 주소가 하나만 할당됩니다. 송신 IP는 외부 엔티티가 네임스페이스의 서비스와 통신하는 데 사용하는 주소입니다. 송신 IP 주소 수는 감독자가 포함할 수 있는 송신 정책의 수를 제한합니다. 최소값은 /27 이상의 CIDR입니다. 예를 들어 `10.174.4.96/27`입니다. **참고** 송신 IP 주소 및 수신 IP 주소는 겹치지 않아야 합니다.
수신 CIDR	/정적 IP 주소 27개	수신 IP 주소에 사용되는 개인 CIDR 범위. 수신을 사용하면 외부 네트워크에서 감독자로 들어오는 요청에 트래픽 정책을 적용할 수 있습니다. 수신 IP 주소 수는 클러스터가 포함할 수 있는 수신의 수를 제한합니다. 최소값은 /27 이상의 CIDR입니다. **참고** 송신 IP 주소 및 수신 IP 주소는 겹치지 않아야 합니다.
네임스페이스 네트워크 범위	1	서브넷/세그먼트를 생성하고 워크로드에 IP 주소를 할당하기 위해 하나 이상의 IP CIDR이 필요합니다.
네임스페이스 서브넷 접두사	1	네임스페이스 세그먼트용으로 예약된 서브넷의 크기를 지정하는 서브넷 접두사가 필요합니다. Default is 28.

표 6-16. NSX 요구 사항

구성 요소	최소 수량	필수 구성
VLAN	3	이러한 VLAN IP는 TEP(터널 끝점)의 IP 주소입니다. ESXi 호스트 TEP와 Edge TEP는 라우팅이 가능해야 합니다. 다음에 VLAN IP 주소가 필요합니다. ■ ESXi 호스트 VTEP ■ 정적 IP를 사용하는 Edge VTEP ■ 전송 노드에 대한 업링크 및 Tier 0 게이트웨이. **참고** ESXi 호스트 VTEP 및 Edge VTEP의 MTU 크기가 1600보다 커야 합니다. ESXi 호스트와 NSX-T Edge 노드는 터널 끝점으로 작동하며 각 호스트와 Edge 노드에 TEP(터널 끝점) IP가 할당됩니다. ESXi 호스트의 TEP IP가 Edge 노드에 TEP IP로 오버레이 터널을 생성하기 때문에 VLAN IP를 라우팅할 수 있어야 합니다. Tier-0 게이트웨이에 대한 North-South 연결을 제공하려면 추가 VLAN이 필요합니다. IP 풀은 여러 클러스터 간에 공유될 수 있습니다. 하지만 호스트 오버레이 IP 풀/VLAN은 Edge 오버레이 IP 풀/VLAN과 공유해서는 안 됩니다. **참고** 호스트 TEP와 Edge TEP가 서로 다른 물리적 NIC를 사용하는 경우 동일한 VLAN을 사용할 수 있습니다.
Tier-0 업링크 IP	/개인 IP 주소 24개	Tie-0 업링크에 사용되는 IP 서브넷. Tie-0 업링크의 IP 주소에 대한 요구 사항은 다음과 같습니다. ■ IP 1개, Edge 이중화를 사용하지 않는 경우. ■ IP 4개, BGP와 Edge 이중화를 사용하는 경우. Edge당 IP 주소 2개. ■ IP 3개, 정적 경로와 Edge 이중화를 사용하는 경우. Edge 관리 IP, 서브넷, 게이트웨이, 업링크 IP, 서브넷, 게이트웨이는 고유해야 합니다.

표 6-17. 로드 밸런서 네트워킹 요구 사항

NTP 및 DNS 서버	1	NSX Advanced Load Balancer 컨트롤러가 vCenter Server 및 ESXi 호스트 이름을 올바르게 확인하려면 DNS 서버 IP가 필요합니다. 공용 NTP 서버가 기본적으로 사용되므로 NTP는 선택 사항입니다.
데이터 네트워크 서브넷	1	서비스 엔진이라고도 하는 NSX Advanced Load Balancer 서비스 엔진의 데이터 인터페이스가 이 네트워크에 연결됩니다. 서비스 엔진에 대한 IP 주소 풀을 구성합니다. 로드 밸런서 VIP(가상 IP)는 이 네트워크에서 할당됩니다.

표 6-17. 로드 밸런서 네트워킹 요구 사항 (계속)

NSX Advanced Load Balancer 컨트롤러 IP	1 또는 4	NSX Advanced Load Balancer 컨트롤러를 단일 노드로 배포하는 경우 해당 관리 인터페이스에 하나의 정적 IP가 필요합니다. 3노드 클러스터의 경우 4개의 IP 주소가 필요합니다. 각 NSX Advanced Load Balancer 컨트롤러 VM에 대해 1개씩 그리고 클러스터 VIP에 대해 1개입니다. 이러한 IP는 관리 네트워크 서브넷의 IP여야 합니다.
VIP IPAM 범위	-	Kubernetes 서비스에 IP 주소를 할당할 개인 CIDR 범위. IP는 데이터 네트워크 서브넷의 IP여야 합니다. 각 감독자 클러스터에 대해 고유한 Kubernetes 서비스 CIDR 범위를 지정해야 합니다.

포트 및 프로토콜

이 표에는 NSX Advanced Load Balancer, vCenter 및 기타 vSphere IaaS control plane 구성 요소 간의 IP 연결을 관리하는 데 필요한 프로토콜 및 포트가 나열되어 있습니다.

소스	대상	프로토콜 및 포트
NSX Advanced Load Balancer Controller	NSX Advanced Load Balancer 컨트롤러(클러스터 내)	TCP 22(SSH) TCP 443(HTTPS) TCP 8443(HTTPS)
서비스 엔진	HA의 서비스 엔진	VMware, LSC 및 NSX-T 클라우드에 대해 TCP 9001
서비스 엔진	NSX Advanced Load Balancer Controller	TCP 22(SSH) TCP 8443(HTTPS) UDP 123(NTP)
Avi 컨트롤러	vCenter Server, ESXi, NSX-T Manager	TCP 443(HTTPS)
감독자 제어부 노드(AKO)	NSX Advanced Load Balancer Controller	TCP 443(HTTPS)

NSX Advanced Load Balancer의 포트 및 프로토콜에 대한 자세한 내용은 https://ports.esp.vmware.com/home/NSX-Advanced-Load-Balancer 항목을 참조하십시오.

VDS 네트워킹 및 HAProxy 로드 밸런서를 사용한 클러스터 감독자 배포 요구 사항

VDS 네트워킹 스택 및 HAProxy 로드 밸런서를 사용하여 vSphere 클러스터를 감독자로 설정하기 위한 시스템 요구 사항을 확인하십시오. vSphere 클러스터를 감독자로 사용하도록 설정하면 감독자에 대해 vSphere 영역이 자동으로 생성됩니다.

최소 계산 요구 사항

관리 도메인과 워크로드 도메인을 분리하는 것이 가장 좋습니다. 워크로드 도메인은 워크로드를 실행하는 감독자를 호스팅합니다. 관리 도메인은 vCenter Server와 같은 모든 관리 구성 요소를 호스팅합니다.

시스템	최소 배포 크기	CPU	메모리	스토리지
vCenter Server 8.0	작음	2	21 GB	290GB
ESXi 호스트 8.0	vSAN 미포함: 호스트당 정적 IP가 1개인 ESXi 호스트 3개. vSAN 포함: 물리적 NIC가 2개 이상인 ESXi 호스트 4개. 호스트는 vSphere DRS 및 HA를 사용하도록 설정된 클러스터에 가입되어 있어야 합니다. vSphere DRS는 완전히 자동화되거나 부분적으로 자동화된 모드여야 합니다. **참고** 클러스터에 참여하는 호스트의 이름에 소문자를 사용하는지 확인합니다. 그렇지 않으면 워크로드 관리를 위한 클러스터 사용 설정이 실패할 수 있습니다.	8	호스트당 64GB	해당 없음
Kubernetes 제어부 VM	3	4	16GB	16GB

최소 네트워크 요구 사항

참고 vSphere 8 감독자를 사용하여 IPv6 클러스터를 생성하거나 IPv6 클러스터를 Tanzu Mission Control에 등록할 수 없습니다.

표 6-18. 물리적 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
물리적 네트워크 MTU	1500	MTU 크기는 분산 포트 그룹에서 1500 이상이어야 합니다.

표 6-19. 일반 네트워킹 요구 사항

구성 요소	최소 수량	필수 구성
NTP 및 DNS 서버	1	vCenter Server에서 사용할 수 있는 DNS 서버 및 NTP 서버. **참고** 모든 ESXi 호스트 및 vCenter Server에서 NTP를 구성합니다.
DHCP 서버	1	선택 사항입니다. 관리 및 워크로드 네트워크와 부동 IP에 대한 IP 주소를 자동으로 획득하도록 DHCP 서버를 구성합니다. DHCP 서버는 클라이언트 식별자를 지원하고 호환되는 DNS 서버, DNS 검색 도메인 및 NTP 서버를 제공해야 합니다. 관리 네트워크의 경우 제어부 VM IP, 부동 IP, DNS 서버, DNS, 검색 도메인 및 NTP 서버와 같은 모든 IP 주소가 DHCP 서버에서 자동으로 획득됩니다. DHCP 구성은 감독자에서 사용됩니다. 로드 밸런서에는 관리를 위한 정적 IP 주소가 필요할 수 있습니다. DHCP 범위는 이러한 정적 IP와 겹치지 않아야 합니다. DHCP는 가상 IP에 사용되지 않습니다. (VIP) **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.

표 6-20. 관리 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
Kubernetes 제어부 VM에 대한 정적 IP	5개의 블록	관리 네트워크에서 감독자의 Kubernetes 제어부 VM으로 할당할 5개의 연속적 정적 IP 주소 블록.
관리 트래픽 네트워크	1	ESXi 호스트, vCenter Server, 감독자 및 로드 밸런서로 라우팅할 수 있는 관리 네트워크.

표 6-20. 관리 네트워크 요구 사항 (계속)

구성 요소	최소 수량	필수 구성
관리 네트워크 서브넷	1	ESXi 호스트, vCenter Server 및 Kubernetes 제어부 사이의 관리 트래픽에 사용되는 서브넷. 서브넷의 크기는 다음과 같아야 합니다. ■ 호스트 VMkernel 어댑터당 IP 주소 1개. ■ vCenter Server Appliance에 대해 IP 주소 1개. ■ Kubernetes 제어부에 대해 IP 주소 5개. 3개 노드 각각에 대해 1개, 가상 IP에 1개, 롤링 클러스터 업그레이드에 1개. **참고** 관리 네트워크와 워크로드 네트워크는 서로 다른 서브넷에 있어야 합니다. 관리 및 워크로드 네트워크에 동일한 서브넷을 할당하는 것은 지원되지 않으며 시스템 오류 및 문제가 발생할 수 있습니다.
관리 네트워크 VLAN	1	관리 네트워크 서브넷의 VLAN ID.

표 6-21. 워크로드 네트워크 요구 사항

구성 요소	최소 수량	필수 구성
vSphere Distributed Switch	1	vSphere 클러스터에 있는 모든 호스트는 VDS에 연결되어야 합니다.
워크로드 네트워크	1	기본 워크로드 네트워크로 구성한 VDS에 분산 포트 그룹을 하나 이상 생성해야 합니다. 선택한 토폴로지에 따라 네임스페이스의 워크로드 네트워크와 동일한 분산 포트 그룹을 사용하거나 더 많은 포트 그룹을 생성하고 이를 워크로드 네트워크로 구성할 수 있습니다. 워크로드 네트워크는 다음 요구 사항을 충족해야 합니다. ■ HAProxy가 가상 IP 할당에 사용하는 네트워크가 있는 모든 워크로드 네트워크 간에 라우팅이 가능해야 합니다. ■ 감독자 내의 모든 워크로드 네트워크에서 IP 주소 범위가 겹치지 않아야 합니다. **중요** 워크로드 네트워크는 관리 네트워크와 다른 서브넷에 있어야 합니다.
Kubernetes 서비스 CIDR 범위	/개인 IP 주소 16개	Kubernetes 서비스에 IP 주소를 할당할 개인 CIDR 범위. 각 감독자에 대해 고유한 Kubernetes 서비스 CIDR 범위를 지정해야 합니다.

표 6-22. 로드 밸런서 네트워킹 요구 사항

HAProxy 로드 밸런서	1	vCenter Server 인스턴스로 구성된 HAProxy 로드 밸런서의 인스턴스입니다. ■ 동일한 HAProxy 인스턴스가 여러 감독자를 처리하는 경우 모든 감독자의 모든 워크로드 네트워크에서 트래픽을 라우팅할 수 있어야 합니다. ■ HAProxy가 서비스를 제공하는 모든 감독자의 워크로드 네트워크에서 IP 범위가 겹치지 않아야 합니다. ■ HAProxy가 가상 IP를 할당하는 데 사용하는 네트워크는 HAProxy가 연결된 모든 감독자에서 사용되는 워크로드 네트워크로 라우팅할 수 있어야 합니다.
가상 서버 IP 범위	1	가상 IP에 대한 전용 IP 범위입니다. HAProxy VM은 이 가상 IP 범위의 유일한 소유자여야 합니다. 범위는 임의의 감독자가 소유한 워크로드 네트워크에 할당된 IP 범위와 겹치지 않아야 합니다. 범위는 관리 네트워크와 동일한 서브넷에 있으면 안됩니다.

구성 요소	최소 수량	필수 구성
NTP 및 DNS 서버	1	vCenter Server에서 사용할 수 있는 DNS 서버 및 NTP 서버. **참고** 모든 ESXi 호스트 및 vCenter Server에서 NTP를 구성합니다.
DHCP 서버	1	선택 사항입니다. 관리 및 워크로드 네트워크와 부동 IP에 대한 IP 주소를 자동으로 획득하도록 DHCP 서버를 구성합니다. DHCP 서버는 클라이언트 식별자를 지원하고 호환되는 DNS 서버, DNS 검색 도메인 및 NTP 서버를 제공해야 합니다. DHCP 구성은 감독자에서 사용됩니다. 로드 밸런서에는 관리를 위한 정적 IP 주소가 필요할 수 있습니다. DHCP 범위는 이러한 정적 IP와 겹치지 않아야 합니다. DHCP는 가상 IP에 사용되지 않습니다. (VIP)