

NSX-T Data Center 설치 가이드

수정 날짜: 2021년 8월 12일
VMware NSX-T Data Center 2.5

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

<https://docs.vmware.com/kr/>

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

VMware 코리아
서울시 강남구
영동대로 517
아셈타워 13층
(우) 06164
전화: +82 2 3016 6500
팩스: +82 2 3016 6501
www.vmware.com/kr

Copyright © 2020 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

목차

NSX-T Data Center 설치 가이드 8

1 NSX-T Data Center 개요 9

핵심 개념 10

NSX Manager 개요 13

2 NSX-T Data Center 설치 워크플로 16

vSphere에 대한 NSX-T Data Center 워크플로 16

KVM에 대한 NSX-T Data Center 설치 워크플로 17

베어메탈 서버에 대한 NSX-T Data Center 구성 워크플로 18

3 설치 준비 19

시스템 요구 사항 19

NSX Manager VM 및 호스트 전송 노드 시스템 요구 사항 19

NSX Edge VM 시스템 요구 사항 23

NSX Edge 베어메탈 요구 사항 24

베어메탈 서버 시스템 요구 사항 27

베어메탈 Linux 컨테이너 요구 사항 27

포트 및 프로토콜 27

NSX Manager에서 사용되는 TCP 및 UDP 포트 28

NSX Edge에서 사용되는 TCP 및 UDP 포트 30

ESXi, KVM 호스트 및 베어메탈 서버에서 사용하는 TCP 및 UDP 포트 31

4 NSX Manager 설치 33

기본 관리자 암호 만료 수정 37

5 vSphere에 NSX-T Data Center 설치 39

NSX Manager 및 사용 가능한 장치 설치 39

명령줄 OVF 도구를 사용하여 ESXi에 NSX Manager 설치 43

부팅 시 GRUB 메뉴를 표시하도록 NSX-T Data Center 구성 48

새로 생성된 NSX Manager에 로그인 49

계산 관리자 추가 49

UI에서 클러스터를 구성하기 위해 NSX Manager 노드 배포 52

클러스터에 대해 VIP(가상 IP) 주소 구성 58

NSX-T 장치에서 스냅샷 사용 안 함 59

6 KVM에 NSX-T Data Center 설치 61

- KVM 설정 61
- KVM CLI에서 게스트 VM 관리 64
- KVM에 NSX Manager 설치 65
- 새로 생성된 NSX Manager에 로그인 69
- KVM 호스트에 타사 패키지 설치 70
- RHEL KVM 호스트의 Open vSwitch 버전 확인 71
- SUSE KVM 호스트의 Open vSwitch 버전 확인 72
- CLI를 사용하여 클러스터를 구성하기 위해 NSX Manager 노드 배포 73

7 NSX-T Data Center를 사용하도록 베어메탈 서버 구성 75

- 베어메탈 서버에 타사 패키지 설치 75
- 베어메탈 서버 워크로드를 위한 애플리케이션 인터페이스 생성 77

8 NSX Manager 클러스터 요건 78

- 단일, 이중 및 다중 사이트에 대한 NSX Manager 클러스터 요구 사항 78

9 NSX Edge 설치 82

- NSX Edge 설치 요구 사항 82
- NSX Edge 네트워킹 설정 85
- NSX Edge 설치 방법 91
- NSX Edge 전송 노드 생성 92
- NSX Edge 클러스터 생성 97
- vSphere GUI를 사용하여 ESXi에 NSX Edge 설치 98
 - 명령줄 OVF 도구를 사용하여 ESXi에 NSX Edge 설치 102
 - ISO 파일을 통해 가상 장치로 NSX Edge 설치 106
- 베어 메탈에 NSX Edge 설치 109
 - NSX Edge를 위한 PXE 서버 준비 110
 - ISO 파일을 통해 자동으로 NSX Edge 설치 115
 - ISO 파일을 통해 대화형으로 NSX Edge 설치 118
- NSX Edge를 관리부에 연결 120
- NSX Edge를 전송 노드로 구성 122

10 전송 영역 및 전송 노드 124

- 전송 영역 생성 124
- 터널 끝점 IP 주소에 대한 IP 풀 생성 126
- 고급 데이터 경로 128
- 프로파일 구성 131
 - 업링크 프로파일 생성 131

Network I/O Control 프로파일 구성	134
NSX Edge 클러스터 프로파일 추가	144
NSX Edge 브리지 프로파일 추가	144
전송 노드 프로파일 추가	145
N-VDS 스위치로 VMkernel 마이그레이션	149
VMkernel 마이그레이션 오류	154
독립형 호스트 또는 베어메탈 서비스 전송 노드 생성	157
관리 호스트 전송 노드 구성	165
링크 집계로 ESXi 호스트 전송 노드 구성	170
전송 노드 상태 확인	171
ESXi VMkernel 및 물리적 어댑터 마이그레이션	173
NSX 유지 보수 모드	174
N-VDS의 시각적 표현	175
상태 점검 VLAN ID 범위 및 MTU 설정	176
양방향 전달 감지 상태 보기	179
NSX-T Data Center 커널 모듈의 수동 설치	180
ESXi 하이퍼바이저에 수동으로 NSX-T Data Center 커널 모듈 설치	180
Ubuntu KVM 하이퍼바이저에 수동으로 NSX-T Data Center 소프트웨어 패키지 설치	183
RHEL 및 CentOS KVM 하이퍼바이저에 수동으로 NSX-T Data Center 소프트웨어 패키지 설치	184
SUSE KVM 하이퍼바이저에 수동으로 NSX-T Data Center 소프트웨어 패키지 설치	186
완전 축소형 vSphere 클러스터 NSX-T 배포	187

11 NSX-T와의 호스트 프로파일 통합 198

상태 비저장 클러스터 자동 배포	198
상태 비저장 클러스터를 자동 배포하는 상위 수준 작업	198
사전 요구 사항 및 지원되는 버전	199
상태 비저장 호스트에 대한 사용자 지정 이미지 프로파일 생성	200
사용자 지정 이미지를 참조 및 대상 호스트와 연결	201
참조 호스트에서 네트워크 구성 설정	202
참조 호스트를 NSX-T의 전송 노드로 구성	203
호스트 프로파일 추출 및 확인	206
상태 비저장 클러스터와 호스트 프로파일 간의 연결 확인	207
호스트 사용자 지정 업데이트	207
대상 호스트에서 자동 배포 트리거	208
호스트 프로파일 및 전송 노드 프로파일 문제 해결	217
상태 저장 서버	219
지원되는 NSX-T 및 ESXi 버전	219
대상 상태 저장 클러스터 준비	220
호스트 프로파일이 적용된 VMkernel 마이그레이션	221

호스트 프로파일이 적용되지 않은 VMkernel 마이그레이션 223

12 호스트 전송 노드에서 NSX-T Data Center 제거 224

제거를 위한 호스트 네트워크 매핑 확인 224

vSphere 클러스터에서 NSX-T Data Center 제거 226

vSphere 클러스터의 호스트에서 NSX-T Data Center 제거 227

독립형 호스트에서 NSX-T Data Center 제거 228

13 NSX Cloud 구성 요소 설치 230

NSX Cloud 아키텍처 및 구성 요소 230

NSX Cloud 배포 개요 232

NSX-T Data Center 온-프레미스 구성 요소 배포 232

CSM 설치 232

CSM을 NSX Manager에 연결 233

포트 및 프로토콜에 대한 액세스 사용 233

(선택 사항) 프록시 서버 구성 234

(선택 사항) Cloud Service Manager용 vIDM 설정 235

공용 클라우드 계정 추가 236

Microsoft Azure 네트워크를 온-프레미스 NSX-T Data Center 배포와 연결 236

AWS(Amazon Web Services) 네트워크를 온-프레미스 NSX-T Data Center 배포와 연결 243

NSX Public Cloud Gateway 배포 248

VNet에서 PCG 배포 250

VPC에 PCG 배포 252

전송 VPC/VNet에 연결 254

자동 생성된 논리적 엔티티 및 클라우드 기반 보안 그룹. 256

(선택 사항) 워크로드 VM에 NSX Tools 설치 260

PCG 배포 해제 또는 연결 해제 261

공용 클라우드에서 nsx.network 태그 제거 261

격리 정책 사용 안 함, 폴백 보안 그룹 제공 262

사용자 생성 논리적 엔티티 삭제 263

CSM에서 배포 해제 또는 연결 해제 263

PCG 배포 해제 문제 해결 263

14 NSX Intelligence 설치 및 구성 265

NSX Intelligence 설치 및 구성 워크플로 266

NSX Intelligence 설치 준비 266

NSX Intelligence 시스템 요구 사항 267

NSX Intelligence에서 사용되는 TCP 및 UDP 포트 268

NSX Intelligence 설치 관리자 번들 다운로드 및 압축 해제 269

NSX Intelligence 장치 설치 271

문제 해결 NSX Intelligence 장치 설치	273
자격 증명이 잘못되었거나 제공된 계정이 잠겨 있음	273
장치 배포에 대한 실패 상태가 지워지지 않음	274
NSX Intelligence 장치 제거	274

15 설치 문제 해결 275

ESXi 호스트의 부트 बैं크 공간 부족으로 설치에 실패함	275
-----------------------------------	-----

NSX-T Data Center 설치 가이드

"NSX-T Data Center 설치 가이드"에서는 VMware NSX-T™ Data Center 제품 설치 방법을 설명합니다. 또한 단계별 구성 지침 및 권장 모범 사례에 대한 정보도 수록되어 있습니다.

대상 사용자

이 정보는 NSX-T Data Center를 설치하거나 사용하려는 모든 사용자를 대상으로 합니다. 이 정보는 가상 시스템 기술과 네트워크 가상화 개념에 익숙한 숙련된 시스템 관리자를 대상으로 작성되었습니다.

기술 자료 용어집

VMware 기술 자료 사이트에서는 새로운 용어를 정리한 용어집을 제공하고 있습니다. VMware 기술 문서에 사용되는 용어의 정의를 보려면 <https://www.vmware.com/topics/glossary> 페이지로 이동하십시오.

NSX-T Data Center 개요

1

서버 가상화에서 가상 시스템을 프로그래밍 방식으로 생성 및 관리하는 것과 동일한 방법으로 NSX-T Data Center 네트워크 가상화에서도 소프트웨어 기반 가상 네트워크를 프로그래밍 방식으로 생성 및 관리합니다.

기능상 네트워크 하이퍼바이저에 해당하는 네트워크 가상화를 사용하면 소프트웨어에서 계층 2 - 계층 7 네트워킹 서비스(예: 스위칭, 라우팅, 액세스 제어, 방화벽 기능, QoS)의 모든 기능을 재현할 수 있습니다. 따라서 이런 서비스를 프로그래밍 방식을 통해 임의의 조합으로 구성함으로써 몇 초 만에 고유하고 분리된 가상 네트워크를 생성할 수 있습니다.

NSX-T Data Center는 서로 분리되어 있으나 통합된 관리부, 제어부 및 데이터부를 구현하여 작동합니다. 이러한 부분은 두 가지 유형의 노드인 NSX Manager 및 전송 노드에 상주하는 프로세스, 모듈 및 에이전트 집합으로 구현됩니다.

- 각 노드는 관리부 에이전트를 호스팅합니다.
- NSX Manager 노드는 API 서비스 및 관리부 클러스터 데몬을 호스팅합니다.
- NSX Controller 노드는 중앙 제어부 클러스터 데몬을 호스팅합니다.
- 전송 노드는 로컬 제어부 데몬 및 전달 엔진을 호스팅합니다.

NSX Manager는 노드의 클러스터에서 정책 관리자, 관리 및 중앙 제어 서비스를 병합하는 3노드 클러스터링 지원을 제공합니다. NSX Manager 클러스터링은 사용자 인터페이스 및 API의 고가용성을 제공합니다. 관리부 및 제어부 노드의 컨버전스는 NSX-T Data Center 관리자가 배포 및 관리해야 하는 가상 장치의 수를 줄입니다.

NSX Manager 장치는 서로 다른 배포 시나리오에서 세 개의 다른 크기로 사용할 수 있습니다. 소형 장치는 랩 또는 개념 증명 배포에 적합합니다. 중간 장치는 최대 64개 호스트의 배포에, 대형 장치는 대규모 환경에 배포하는 고객에 적합합니다. [NSX Manager VM 및 호스트 전송 노드 시스템 요구 사항 및 구성 최대값](#) 도구를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [핵심 개념](#)
- [NSX Manager 개요](#)

핵심 개념

설명서 및 사용자 인터페이스에서 사용되는 일반적인 NSX-T Data Center 개념입니다.

계산 관리자

계산 관리자는 호스트 및 VM과 같은 리소스를 관리하는 애플리케이션입니다. vCenter Server를 예로 들 수 있습니다.

제어부

관리부의 구성을 기준으로 런타임 상태를 계산합니다. 제어부는 데이터부 요소가 보고하는 토폴로지 정보를 전달하고, 상태 비저장 구성을 전달 엔진에 푸시합니다.

데이터부

제어부에 의해 채워진 테이블을 기준으로 패킷의 상태 비저장 전달 또는 변환을 수행합니다. 데이터부는 제어부로 토폴로지 정보를 보고하고 패킷 수준 통계를 유지 관리합니다.

외부 네트워크

NSX-T Data Center에서 관리되지 않는 물리적 네트워크 또는 VLAN입니다. 논리적 네트워크 또는 오버레이 네트워크를 NSX Edge를 통해 외부 네트워크에 연결할 수 있습니다. 예를 들어 고객 데이터 센터의 물리적 네트워크나 물리적 환경의 VLAN이 있습니다.

논리적 포트 송신

VM 또는 논리적 네트워크를 떠나는 아웃바운드 네트워크 트래픽은 트래픽이 가상 네트워크를 떠나서 데이터 센터에 진입하기 때문에 송신이라고 합니다.

논리적 포트 수신

데이터 센터를 떠나서 VM에 진입하는 인바운드 네트워크 트래픽은 수신 트래픽이라고 합니다.

논리적 라우터

NSX-T Data Center 라우팅 엔티티입니다.

논리적 라우터 포트

논리적 스위치 포트 또는 업링크 포트를 물리적 네트워크에 연결할 수 있는 논리적 네트워크 포트입니다.

논리적 스위치

VM 인터페이스 및 게이트웨이 인터페이스에 대한 가상 계층 2 스위칭을 제공하는 엔티티입니다. 논리적 스위치는 테넌트 네트워크 관리자에게 물리적 계층 2 스위치와 동급의 논리적 스위치를 제공하여 VM 집합을 일반적인 브로드캐스트 도메인에 연결할 수 있도록 합니다. 논리적 스위치는 물리적 하이퍼바이저 인프라와는 독립된 논리적 엔티티로, 여러 하이퍼바이저에 걸쳐 VM의 물리적 위치와 관계 없이 VM을 연결합니다.

다중 테넌트 클라우드에서 여러 논리적 스위치는 각 계층 2 세그먼트가 다른 세그먼트에서 분리된 상태로 동일한 하이퍼바이저 하드웨어에 나란히 존재할 수 있습니다. 논리적 스위치는 논리적 라우터를 사용하여 연결될 수 있고, 논리적 라우터는 외부 물리적 네트워크에 연결된 업링크 포트를 제공할 수 있습니다.

논리적 스위치 포트

가상 시스템 네트워크 인터페이스 또는 논리적 라우터 인터페이스에 대한 연결을 설정하기 위한 논리적 스위치 연결 지점입니다. 논리적 스위치 포트는 적용된 스위칭 프로파일, 포트 상태 및 링크 상태를 보고합니다.

관리부

시스템의 모든 관리부, 제어부 및 데이터부 노드에서 시스템에 대한 단일 API 진입점을 제공하고, 사용자 구성을 유지하고, 사용자 쿼리를 처리하고, 작업을 수행합니다. 또한 관리부는 사용자 구성의 쿼리, 수정 및 유지도 담당합니다.

NSX Edge 클러스터

고가용성 모니터링에 포함된 프로토콜과 동일한 설정을 갖는 NSX Edge 노드 장치 컬렉션입니다.

NSX Edge 노드

기능 목표가 있는 구성 요소는 IP 라우팅 및 IP 서비스 기능을 전달하기 위한 계산 능력을 제공합니다.

NSX 관리 가상 Distributed Switch 또는 KVM Open vSwitch

N-VDS(NSX 관리 가상 Distributed Switch, 이전 이름: 호스트 스위치) 또는 OVS는 공유 NSX Edge 및 계산 클러스터에 사용됩니다. 오버레이 트래픽 구성을 위해서는 N-VDS가 필요합니다.

N-VDS에는 표준 및 고급 데이터 경로라는 두 가지 모드가 있습니다. 고급 데이터 경로 N-VDS는 NFV(Network Functions Virtualization) 워크로드를 지원할 수 있는 성능을 갖추고 있습니다.

NSX Manager

API 서비스, 관리부 및 에이전트 서비스를 호스팅하는 노드입니다. NSX Manager는 NSX-T Data Center 설치 패키지에 포함된 장치입니다. NSX Manager 또는 nsx-cloud-service-manager 역할로 장치를 배포할 수 있습니다. 현재 장치는 한 번에 하나의 역할만 지원합니다.

NSX Manager 클러스터

고가용성을 제공할 수 있는 NSX Manager의 클러스터입니다.

OVS(Open vSwitch)

XenServer, Xen, KVM 및 기타 Linux 기반 하이퍼바이저 내에서 가상 스위치로 작동하는 오픈 소스 소프트웨어 스위치입니다.

오버레이 논리적 네트워크

VM에 표시되는 토폴로지가 물리적 네트워크의 토폴로지에서 분리되도록 계층 2-in-계층 3 터널링을 사용하여 구현되는 논리적 네트워크입니다.

물리적 인터페이스(pNIC)

하이퍼바이저가 설치되는 물리적 서버의 네트워크 인터페이스입니다.

세그먼트

VM 인터페이스 및 게이트웨이 인터페이스에 대한 가상 계층 2 스위칭을 제공하는 엔티티입니다. 세그먼트는 테넌트 네트워크 관리자에게 물리적 계층 2 스위치와 동급의 논리적 스위치를 제공하여 VM 집합을 일반적인 브로드캐스트 도메인에 연결할 수 있도록 합니다. 세그먼트는 물리적 하이퍼바이저 인 프라에 독립적인 논리적 엔티티로, 여러 하이퍼바이저에 걸쳐 VM의 물리적 위치와 관계없이 VM을 연결합니다. 세그먼트를 논리적 스위치라고도 합니다.

다중 테넌트 클라우드에서 여러 세그먼트는 각 계층 2 세그먼트가 다른 세그먼트에서 분리된 상태로 동일한 하이퍼바이저 하드웨어에 나란히 존재할 수 있습니다. 세그먼트는 게이트웨이를 사용하여 연결할 수 있으며 이를 통해 외부 물리적 네트워크에 대한 연결을 제공할 수 있습니다.

Tier-0 게이트웨이 또는 Tier-0 논리적 라우터

Tier-0 게이트웨이는 **고급 네트워킹 및 보안** 탭에서 Tier-0 논리적 라우터라고 합니다. Tier-0 게이트웨이는 물리적 네트워크와 상호 작용하며 활성-활성 또는 활성-대기 클러스터로 구현할 수 있습니다. Tier-0 게이트웨이는 BGP를 실행하고 물리적 라우터와 피어링됩니다. 활성-대기 모드에서 게이트웨이는 상태 저장 서비스를 제공할 수도 있습니다.

Tier-1 게이트웨이 또는 Tier-1 논리적 라우터

Tier-1 게이트웨이는 **고급 네트워킹 및 보안** 탭에서 Tier-1 논리적 라우터라고 합니다. Tier-1 게이트웨이는 노스바운드 연결을 위해 하나의 Tier-0 게이트웨이에 연결되고 사우스바운드 연결을 위해 하나 이상의 오버레이 네트워크에 연결됩니다. Tier-1 게이트웨이는 상태 저장 서비스를 제공하는 활성-대기 클러스터일 수 있습니다.

전송 영역

논리적 스위치의 최대 적용 범위를 정의하는 전송 노드 컬렉션입니다. 전송 영역은 유사하게 프로비저닝된 하이퍼바이저 및 해당 하이퍼바이저에서 VM을 연결하는 논리적 스위치 집합을 나타냅니다. 또한 NSX-T Data Center관리부에 등록되어 있고 NSX-T Data Center모듈이 설치되어 있습니다. 하이퍼바이저 호스트 또는 NSX Edge가 NSX-T Data Center 오버레이에 속하려면 이를 NSX-T Data Center전송 영역에 추가해야 합니다.

전송 노드

NSX-T Data Center 오버레이 또는 NSX-T Data Center VLAN 네트워킹에 참여할 수 있는 노드입니다. KVM 호스트의 경우 N-VDS를 미리 구성하거나 NSX Manager에서 구성이 수행되도록 할 수 있습니다. ESXi 호스트의 경우 NSX Manager에서 항상 N-VDS를 구성합니다.

업링크 프로파일

하이퍼바이저 호스트에서 NSX-T Data Center 논리적 스위치로 또는 NSX Edge 노드에서 랙 상단 스위치로 연결되는 링크에 대한 정책을 정의합니다. 업링크 프로파일에 의해 정의된 설정에는 팀 구성 정책, 활성/대기 링크, 전송 VLAN ID 및 MTU 설정이 포함될 수 있습니다. 업링크 프로파일에 설정된 전송 VLAN은 오버레이 트래픽에만 태그를 지정하고, VLAN ID가 TEP 끝점에서 사용됩니다.

VM 인터페이스(vNIC)

가상 게스트 운영 체제와 표준 vSwitch 또는 vSphere Distributed Switch 간에 연결을 제공하는 가상 시스템의 네트워크 인터페이스입니다. vNIC는 논리적 포트에 연결될 수 있습니다. UUID(고유 ID)를 기준으로 vNIC를 식별할 수 있습니다.

가상 터널 끝점

각 하이퍼바이저에는 VLAN 헤더 내부의 VM 트래픽을 캡슐화하고 추가로 처리하기 위해 대상 VTEP(가상 터널 끝점)로 패킷을 라우팅하는 VTEP가 있습니다. 트래픽을 다른 호스트의 다른 VTEP 또는 NSX Edge 게이트웨이로 라우팅하여 물리적 네트워크에 액세스할 수 있습니다.

NSX Manager 개요

NSX Manager는 NSX-T 환경을 관리할 수 있는 웹 기반 사용자 인터페이스를 제공합니다. API 호출을 처리하는 API 서버도 호스팅합니다.

NSX Manager 웹 인터페이스는 리소스를 구성하는 두 가지 방법을 제공합니다.

- 정책 인터페이스: **네트워킹, 보안, 인벤토리 및 계획 및 문제 해결** 탭.
- 고급 인터페이스: **고급 네트워킹 및 보안** 탭.

정책 또는 고급 인터페이스를 사용하는 경우

사용하는 사용자 인터페이스와 일치해야 합니다. 다른 사용자 인터페이스를 사용해야 하는 이유에는 몇 가지가 있습니다.

- NSX-T Data Center 2.4 이상이 포함된 새 환경을 배포하는 경우, 대부분의 상황에서 새로운 정책 기반 사용자 인터페이스를 사용하여 환경을 생성하고 관리하는 것이 가장 좋습니다.
 - 일부 기능은 정책 기반 사용자 인터페이스에서 사용할 수 없습니다. 이러한 기능이 필요한 경우 모든 구성에 대해 고급 사용자 인터페이스를 사용합니다.
- NSX-T Data Center 2.4 이상으로 업그레이드하는 경우 **고급 네트워킹 및 보안** 사용자 인터페이스를 사용하여 구성을 변경합니다.

표 1-1. 정책 또는 고급 인터페이스를 사용하는 경우

정책 인터페이스	고급 인터페이스
대부분의 새 배포는 정책 기반 인터페이스를 사용해야 합니다.	고급 인터페이스를 사용하여 생성된 배포(예: 정책 기반 인터페이스를 사용하기 전 버전에서 업그레이드)
NSX Cloud 배포	다른 플러그인과 통합되는 배포입니다. 예: NSX Container Plug-in, Openstack 및 기타 클라우드 관리 플랫폼

표 1-1. 정책 또는 고급 인터페이스를 사용하는 경우 (계속)

정책 인터페이스	고급 인터페이스
<p>정책 인터페이스에서만 사용할 수 있는 네트워킹 기능:</p> <ul style="list-style-type: none"> ■ DNS 서비스 및 DNS 영역 ■ VPN ■ NSX Cloud에 대한 전달 정책 	<p>고급 인터페이스에서만 사용할 수 있는 네트워킹 기능:</p> <ul style="list-style-type: none"> ■ 전달 타이머 ■ BFD 및 인터페이스(다음 홉)가 있는 정적 경로 ■ 메타데이터 프록시 ■ 격리된 세그먼트 및 정적 바인딩에 연결된 DHCP 서버
<p>정책 인터페이스에서만 사용할 수 있는 보안 기능:</p> <ul style="list-style-type: none"> ■ 끝점 보호 ■ 네트워크 검사(East-West 서비스 삼입) ■ 컨텍스트 프로파일 <ul style="list-style-type: none"> ■ L7 애플리케이션 ■ FQDN ■ 새 분산 방화벽 및 게이트웨이 방화벽 레이아웃 <ul style="list-style-type: none"> ■ 범주 ■ 자동 서비스 규칙 ■ 초안 	<p>고급 인터페이스에서만 사용할 수 있는 보안 기능:</p> <ul style="list-style-type: none"> ■ CPU와 메모리 임계값 ■ 브리지 방화벽 ■ 소스 및 대상의 IP를 기준으로 하는 분산 방화벽 규칙

정책 인터페이스 사용

정책 인터페이스를 사용하기로 결정한 경우 모든 개체를 생성하는 데 사용합니다. 고급 인터페이스를 사용하여 개체를 생성하지 마십시오.

고급 인터페이스를 사용하여 정책 인터페이스에서 생성된 개체를 수정할 수 있습니다. 정책 생성 개체에 대한 설정에 **고급 구성**에 대한 링크가 포함될 수 있습니다. 이 링크를 클릭하면 구성을 미세 조정할 수 있는 고급 인터페이스로 이동됩니다. 고급 인터페이스에서 정책 생성 개체를 직접 볼 수도 있습니다. 정책에 의해 관리되지만 고급 인터페이스에 표시되는 설정은 옆에 ⊖ 아이콘이 표시됩니다. 고급 사용자 인터페이스에서는 수정할 수 없습니다.

정책 인터페이스 및 고급 인터페이스를 찾을 수 있는 위치

정책 기반 및 고급 인터페이스는 NSX Manager 사용자 인터페이스의 서로 다른 부분에 표시되며 다른 API URI를 사용합니다.

표 1-2. 정책 인터페이스 및 고급 인터페이스

정책 인터페이스	고급 인터페이스
<ul style="list-style-type: none"> ■ 네트워킹 탭 ■ 보안 탭 ■ 인벤토리 탭 ■ 계획 및 문제 해결 탭 	고급 네트워킹 및 보안 탭
/policy/api로 시작하는 API URI	/api로 시작하는 API URI

참고 시스템 탭은 모든 환경에 사용됩니다. Edge 노드, Edge 클러스터 또는 전송 영역을 수정하는 경우 변경 사항이 정책 기반 사용자 인터페이스에 표시되는 데 최대 5분이 걸릴 수 있습니다. `POST /policy/api/v1/infra/sites/default/enforcement-points/default?action=reload`를 사용하여 즉시 동기화할 수 있습니다.

정책 API 사용에 대한 자세한 내용은 [NSX-T 정책 API 시작 가이드](#)를 참조하십시오.

정책 및 고급 인터페이스에서 생성된 개체의 이름

생성하는 개체는 해당 개체를 생성하는 데 사용된 인터페이스에 따라 달라집니다.

표 1-3. 개체 이름

정책 인터페이스를 사용하여 생성된 개체	고급 인터페이스를 사용하여 생성된 개체
세그먼트	논리적 스위치
Tier-1 게이트웨이	Tier-1 논리적 라우터
Tier-0 게이트웨이	Tier-0 논리적 라우터
그룹	NSGroup, IP 집합, MAC 집합
보안 정책	방화벽 섹션
규칙	방화벽 규칙
게이트웨이 방화벽	Edge 방화벽

NSX-T Data Center 설치 워크플로

2

NSX-T Data Center는 vSphere 또는 KVM 호스트에 설치할 수 있습니다. NSX-T Data Center를 사용하여 베어메탈 서버를 구성할 수도 있습니다.

하이퍼바이저 또는 베어메탈 중 하나를 설치하거나 구성하려면 워크플로에서 권장되는 작업을 수행합니다.

본 장은 다음 항목을 포함합니다.

- [vSphere에 대한 NSX-T Data Center 워크플로](#)
- [KVM에 대한 NSX-T Data Center 설치 워크플로](#)
- [베어메탈 서버에 대한 NSX-T Data Center 구성 워크플로](#)

vSphere에 대한 NSX-T Data Center 워크플로

체크리스트를 사용하여 vSphere 호스트에서 설치 진행률을 추적합니다.

권장되는 절차 순서를 따릅니다.

- 1 NSX Manager 설치 요구 사항을 검토합니다. [장 4 NSX Manager 설치](#)의 내용을 참조하십시오.
- 2 필요한 포트 및 프로토콜을 구성합니다. [포트 및 프로토콜](#)의 내용을 참조하십시오.
- 3 NSX Manager를 설치합니다. [NSX Manager 및 사용 가능한 장치 설치](#)의 내용을 참조하십시오.
- 4 새로 생성된 NSX Manager에 로그인합니다. [새로 생성된 NSX Manager에 로그인](#)의 내용을 참조하십시오.
- 5 계산 관리자를 구성합니다. [계산 관리자 추가](#)의 내용을 참조하십시오.
- 6 추가적인 NSX Manager 노드를 배포하여 클러스터를 구성합니다. [UI에서 클러스터를 구성하기 위해 NSX Manager 노드 배포](#)의 내용을 참조하십시오.
- 7 NSX Edge 설치 요구 사항을 검토합니다. [NSX Edge 설치 요구 사항](#)의 내용을 참조하십시오.
- 8 NSX Edge를 설치합니다. [vSphere GUI를 사용하여 ESXi에 NSX Edge 설치](#)의 내용을 참조하십시오.
- 9 NSX Edge 클러스터를 생성합니다. [NSX Edge 클러스터 생성](#)의 내용을 참조하십시오.
- 10 전송 영역을 생성합니다. [전송 영역 생성](#)의 내용을 참조하십시오.

- 11 호스트 전송 노드를 생성합니다. 독립형 호스트 또는 베어메탈 서비스 전송 노드 생성 또는 관리 호스트 전송 노드 구성의 내용을 참조하십시오.

각 호스트에 가상 스위치가 생성됩니다. 관리부는 제어부로 호스트 인증서를 전송하고, 호스트로 제어부 정보를 푸시합니다. 각 호스트는 SSL을 통해 제어부로 연결되며 해당 인증서를 제공합니다. 제어부는 관리부에서 제공한 호스트 인증서에 대해 인증서가 유효한지 검증합니다. 검증이 성공하면 컨트롤러에서 연결을 수락합니다.

설치 후

호스트가 전송 노드인 경우 언제든지 NSX Manager UI 또는 API를 통해 전송 영역, 논리적 스위치, 논리적 라우터 및 기타 네트워크 구성 요소를 생성할 수 있습니다. NSX Edge 및 호스트가 관리부에 연결되면 NSX-T Data Center 논리적 엔티티 및 구성 상태가 NSX Edge 및 호스트로 자동으로 푸시됩니다.

자세한 내용은 "NSX-T Data Center 관리 가이드"를 참조하십시오.

KVM에 대한 NSX-T Data Center 설치 워크플로

체크리스트를 사용하여 KVM 호스트에서 설치 진행률을 추적합니다.

권장되는 절차 순서를 따릅니다.

- 1 KVM 환경을 준비합니다. KVM 설정의 내용을 참조하십시오.
- 2 NSX Manager 설치 요구 사항을 검토합니다. 장 4 NSX Manager 설치의 내용을 참조하십시오.
- 3 필요한 포트 및 프로토콜을 구성합니다. 포트 및 프로토콜의 내용을 참조하십시오.
- 4 NSX Manager를 설치합니다. KVM에 NSX Manager 설치의 내용을 참조하십시오.
- 5 새로 생성된 NSX Manager에 로그인합니다. 새로 생성된 NSX Manager에 로그인의 내용을 참조하십시오.
- 6 KVM 호스트에서 타사 패키지를 구성합니다. KVM 호스트에 타사 패키지 설치의 내용을 참조하십시오.
- 7 추가적인 NSX Manager 노드를 배포하여 클러스터를 구성합니다. CLI를 사용하여 클러스터를 구성하기 위해 NSX Manager 노드 배포의 내용을 참조하십시오.
- 8 NSX Edge 설치 요구 사항을 검토합니다. NSX Edge 설치 요구 사항의 내용을 참조하십시오.
- 9 NSX Edge를 설치합니다. 베어 메탈에 NSX Edge 설치의 내용을 참조하십시오.
- 10 NSX Edge 클러스터를 생성합니다. NSX Edge 클러스터 생성의 내용을 참조하십시오.
- 11 전송 영역을 생성합니다. 전송 영역 생성의 내용을 참조하십시오.
- 12 호스트 전송 노드를 생성합니다. 독립형 호스트 또는 베어메탈 서비스 전송 노드 생성의 내용을 참조하십시오.

각 호스트에 가상 스위치가 생성됩니다. 관리부는 제어부로 호스트 인증서를 전송하고, 호스트로 제어부 정보를 푸시합니다. 각 호스트는 SSL을 통해 제어부로 연결되며 해당 인증서를 제공합니다. 제어부는 관리부에서 제공한 호스트 인증서에 대해 인증서가 유효한지 검증합니다. 검증이 성공하면 컨트롤러에서 연결을 수락합니다.

설치 후

호스트가 전송 노드인 경우 언제든지 NSX Manager UI 또는 API를 통해 전송 영역, 논리적 스위치, 논리적 라우터 및 기타 네트워크 구성 요소를 생성할 수 있습니다. NSX Edge 및 호스트가 관리부에 연결되면 NSX-T Data Center 논리적 엔티티 및 구성 상태가 NSX Edge 및 호스트로 자동으로 푸시됩니다.

자세한 내용은 "NSX-T Data Center 관리 가이드"를 참조하십시오.

베어메탈 서버에 대한 NSX-T Data Center 구성 워크플로

NSX-T Data Center를 사용하도록 베어메탈 서버를 구성할 때 체크리스트를 사용하여 진행률을 추적합니다.

권장되는 절차 순서를 따릅니다.

- 1 베어메탈 요구 사항을 검토합니다. [베어메탈 서버 시스템 요구 사항](#)의 내용을 참조하십시오.
- 2 필요한 포트 및 프로토콜을 구성합니다. [포트 및 프로토콜](#)의 내용을 참조하십시오.
- 3 NSX Manager를 설치합니다. [KVM에 NSX Manager 설치](#)의 내용을 참조하십시오.
- 4 베어메탈 서버에서 타사 패키지를 구성합니다. [베어메탈 서버에 타사 패키지 설치](#)의 내용을 참조하십시오.
- 5 호스트 전송 노드를 생성합니다. [독립형 호스트 또는 베어메탈 서비스 전송 노드 생성](#)의 내용을 참조하십시오.

각 호스트에 가상 스위치가 생성됩니다. 관리부는 제어부로 호스트 인증서를 전송하고, 호스트로 제어부 정보를 푸시합니다. 각 호스트는 SSL을 통해 제어부로 연결되며 해당 인증서를 제공합니다. 제어부는 관리부에서 제공한 호스트 인증서에 대해 인증서가 유효한지 검증합니다. 검증이 성공하면 컨트롤러에서 연결을 수락합니다.

- 6 베어메탈 서버 워크로드를 위한 애플리케이션 인터페이스를 생성합니다. [베어메탈 서버 워크로드를 위한 애플리케이션 인터페이스 생성](#)의 내용을 참조하십시오.

설치 준비

3

NSX-T Data Center를 설치하기 전에 작업 환경이 준비되었는지 확인합니다.

본 장은 다음 항목을 포함합니다.

- 시스템 요구 사항
- 포트 및 프로토콜

시스템 요구 사항

NSX-T Data Center를 설치하려면 먼저 해당 환경이 특정 하드웨어 및 리소스 요구 사항을 충족해야 합니다.

NSX Manager VM 및 호스트 전송 노드 시스템 요구 사항

NSX Manager 또는 다른 NSX-T Data Center 장치를 설치하기 전에 환경이 지원 요구 사항을 충족하는지 확인합니다.

호스트 전송 노드로 지원되는 하이퍼바이저

하이퍼바이저	버전	CPU 코어	메모리
vSphere	지원되는 vSphere 버전	4	16GB
CentOS Linux KVM	7.4, 7.5, 7.6	4	16GB
RHEL(Red Hat Enterprise Linux) KVM	7.6, 7.5 및 7.4	4	16GB
SUSE Linux Enterprise Server KVM	12 sp3, 12 sp4	4	16GB
Ubuntu KVM	16.04, 18.04.2 LTS	4	16GB

표 3-1. NSX Manager에 대해 지원되는 호스트

지원 설명	하이퍼바이저
ESXi	지원되는 호스트에 대해서는 VMware 제품 상호 운용성 매트릭스 를 참조하십시오.
KVM	RHEL 7.4 및 Ubuntu 18.04.2 LTS 참고 NSX-T Data Center 2.5부터 버전 18.04.2 LTS를 실행하는 Ubuntu 호스트는 16.04에서 업그레이드하거나 새로 설치될 수 있습니다.

ESXi 호스트의 경우 NSX-T Data Center는 vSphere 6.7 U1 이상에서 호스트 프로파일 및 Auto Deploy 기능을 지원합니다. 자세한 내용은 " " VMware ESXi 설치 및 설정에서 " " vSphere Auto Deploy 이해를 참조하십시오.

경고 RHEL 및 Ubuntu에서 `yum update` 명령은 4.14.x보다 크지 않아야 하는 커널 버전을 업데이트하며 NSX-T Data Center와 호환되지 않게 할 수 있습니다. `yum update`를 실행하는 경우에는 자동 커널 업데이트를 사용하지 않도록 설정합니다. 또한 `yum install`을 실행한 후 NSX-T Data Center가 커널 버전을 지원하는지 확인합니다.

하이퍼바이저 호스트 네트워크 요구 사항

사용된 NIC 카드는 NSX-T Data Center를 실행하는 ESXi 버전과 호환되어야 합니다. 지원되는 NIC 카드에 대해서는 [VMware 호환성 가이드](#)를 참조하십시오.

팁 호환성 가이드에서 호환되는 카드를 빠르게 식별하려면 다음 기준을 적용합니다.

- I/O 디바이스 유형에서 **네트워크**를 선택합니다.
- 경우에 따라 지원되는 GENEVE 캡슐화를 사용하려면 **기능**에서 GENEVE 옵션을 선택합니다.
- 경우에 따라 고급 데이터 경로를 사용하려면 **N-VDS 고급 데이터 경로**를 선택합니다.

고급 데이터 경로 NIC 드라이버

[My VMware](#) 페이지에서 지원되는 NIC 드라이버를 다운로드합니다.

NIC 카드	NIC 드라이버
Intel 82599	ixgben 1.1.0.26-1OEM.670.0.0.7535516
Intel(R) Ethernet Controller X710 for 10GbE SFP+	i40en 1.2.0.0-1OEM.670.0.0.8169922
Intel(R) Ethernet Controller XL710 for 40GbE QSFP+	

NSX Manager VM 리소스 요구 사항

썬 가상 디스크 크기는 3.8 GB이고 썬 가상 디스크 크기는 200GB입니다.

장치 크기	메모리	vCPU	디스크 용량	VM 하드웨어 버전
NSX Manager 초소형	8GB	2	200GB	10 이상
NSX Manager 소형 VM	16GB	4	200GB	10 이상
NSX Manager 중간 VM	24GB	6	200GB	10 이상
NSX Manager 대형 VM	48GB	12	200GB	10 이상

참고 NSX Manager는 이전에 개별 장치가 필요했던 여러 역할을 제공합니다. 여기에는 정책 역할, 관리 부 역할 및 중앙 제어부 역할이 포함됩니다. 이전에는 중앙 제어부 역할을 NSX Controller 장치에서 제공했습니다.

- 초소형 VM 리소스 크기는 Cloud Service Manager 장치(CSM)에만 사용할 수 있습니다. 필요에 따라 초소형 VM 크기 이상으로 CSM을 배포합니다. 자세한 내용은 [NSX Cloud 배포 개요](#) 항목을 참조하십시오.
- NSX Manager 소형 VM 장치 크기는 랩 및 개념 증명 배포에 적합하며 운영 환경에서는 사용하지 않아야 합니다.
- NSX Manager 중형 VM 장치 크기는 일반적인 운영 환경에 적합합니다. 이 장치 크기를 사용하여 구성된 NSX-T 관리 클러스터는 최대 64개의 하이퍼바이저를 지원할 수 있습니다.
- NSX Manager 대형 VM 장치 크기는 대규모 배포에 적합합니다. 이 장치 크기를 사용하여 구성된 NSX-T 관리 클러스터는 65개 이상의 하이퍼바이저를 지원할 수 있습니다.

NSX Manager 대형 VM 장치 크기를 사용하는 최대 규모의 경우 <https://configmax.vmware.com/guest>에서 VMware Configuration Maximums 도구로 이동한 후 제품 목록에서 NSX-T Data Center를 선택하십시오.

언어 지원

NSX Manager는 영어, 독일어, 프랑스어, 일본어, 중국어 간체자, 한국어, 중국어 번체자 및 스페인어로 현지화되었습니다.

NSX Manager 브라우저 지원

NSX Manager는 다음 브라우저에서 사용하는 것이 좋습니다.

브라우저	Windows 10	Mac OS X 10.13, 10.14	Ubuntu 18.04
Google Chrome 76	예	예	예
Mozilla Firefox 68	예	예	예

브라우저	Windows 10	Mac OS X 10.13, 10.14	Ubuntu 18.04
Microsoft Edge 44	예		
Apple Safari 12		예	

참고

- Internet Explorer는 지원되지 않습니다.
- 지원되는 브라우저 최소 해상도는 1280x800픽셀입니다.
- 언어 지원: NSX Manager는 영어, 독일어, 프랑스어, 일본어, 중국어 간체, 한국어, 중국어 번체 및 스페인어로 현지화되었습니다. 하지만 NSX Manager 현지화는 브라우저 언어 설정을 활용하기 때문에 설정이 원하는 언어와 일치하는지 확인하십시오. NSX Manager 인터페이스 자체에는 언어 기본 설정이 없습니다.

네트워크 지연 시간 요구 사항

NSX Manager 클러스터에서 NSX Manager 사이의 최대 네트워크 지연 시간은 10ms입니다.

NSX Manager와 전송 노드 간의 최대 네트워크 지연 시간은 150ms입니다.

스토리지 요구 사항

- 최대 디스크 액세스 지연 시간은 10ms 미만입니다.
 - NSX Manager는 공유 스토리지에 배치하는 것이 좋습니다.
 - 스토리지 중단을 방지하여 스토리지 장애 발생 시 모든 NSX Manager 파일 시스템을 읽기 전용 모드로 전환하기 위해서는 스토리지를 고가용성 상태로 유지해야 합니다.
- 고가용성 스토리지 솔루션을 디자인하는 최선의 방법에 대해서는 스토리지 기술 설명서를 참조하십시오.

NSX Edge VM 시스템 요구 사항

NSX Edge를 설치하기 전에 환경이 지원 요구 사항을 충족하는지 확인합니다.

참고 NSX Edge 노드의 호스트에는 다음 조건이 적용됩니다.

- NSX Edge 노드는 Intel 기반 칩셋이 있는 ESXi 기반 호스트에서만 지원됩니다.
그렇지 않으면 vSphere EVC 모드에서 NSX Edge 노드가 시작되지 못하므로 콘솔에 오류 메시지가 표시될 수 있습니다.
- vSphere EVC 모드가 NSX Edge VM의 호스트에 대해 사용되도록 설정된 경우 CPU는 Haswell 이상 세대여야 합니다.
- VMXNET3 vNIC만 NSX Edge VM에서 지원됩니다.

NSX Cloud 참고 NSX Cloud를 사용하는 경우 NSX Public Cloud Gateway(PCG)가 각각의 지원되는 공용 클라우드에 대해 단일 기본 크기로 배포됩니다. 자세한 내용은 [NSX Public Cloud Gateway 배포](#) 항목을 참조하십시오.

NSX Edge VM 리소스 요구 사항

장치 크기	메모리	vCPU	디스크 용량	VM 하드웨어 버전	참고
NSX Edge 소형	4GB	2	200GB	11 이상(vSphere 6.0 이상)	NSX Edge 소형 VM 장치 크기는 랩 및 개념 증명 배포에 적합합니다. 참고 크기가 작은 NSX Edge VM을 배포하는 경우 L7 규칙은 Tier-1 게이트웨이에서 인식되지 않습니다.
NSX Edge 중형	8GB	4	200GB	11 이상(vSphere 6.0 이상)	NSX Edge 중형 장치 크기는 일반적인 운영 환경에 적합합니다.
NSX Edge 대형	32GB	8	200GB	11 이상(vSphere 6.0 이상)	NSX Edge 대형 장치 크기는 로드 밸런싱 환경에 적합합니다. "NSX-T Data Center 관리 가이드"에서 로드 밸런서 리소스 확장 을 참조하십시오.

NSX Edge VM CPU 요구 사항

DPDK 지원을 위해서는 기본 플랫폼이 다음 요구 사항을 충족해야 합니다.

- CPU에 AESNI 기능이 있어야 합니다.
- CPU가 1GB의 Huge Page를 지원해야 합니다.

하드웨어	유형
CPU	<ul style="list-style-type: none"> ■ Intel Xeon E7-xxxx(Westmere-EX 이상 CPU 생성) ■ Intel Xeon 56xx(Westmere-EP) ■ Intel Xeon E5-xxxx(Sandy Bridge 이상 CPU 생성) ■ Intel Xeon Platinum(모든 세대) ■ Intel Xeon Gold(모든 세대) ■ Intel Xeon Silver(모든 세대) ■ Intel Xeon Bronze(모든 세대)

NSX Edge 베어메탈 요구 사항

NSX Edge 베어메탈을 구성하기 전에 환경이 지원 요구 사항을 충족하는지 확인합니다.

NSX Edge 베어메탈 메모리, CPU 및 디스크 요구 사항

최소 요구 사항

메모리	CPU 코어	디스크 용량
32GB	8	200GB

권장 요구 사항

메모리	CPU 코어	디스크 용량
256 GB	24	200GB

NSX Edge 베어메탈 DPDK CPU 요구 사항

DPDK 지원을 위해서는 기본 플랫폼이 다음 요구 사항을 충족해야 합니다.

- CPU에 AES-NI 기능이 있어야 합니다.
- CPU가 1GB의 Huge Page를 지원해야 합니다.

하드웨어	유형
CPU	<ul style="list-style-type: none"> ■ Intel Xeon E7-xxxx(Westmere-EX 이상 CPU 생성) ■ Intel Xeon 56xx(Westmere-EP) ■ Intel Xeon E5-xxxx(Sandy Bridge 이상 CPU 생성) ■ Intel Xeon Platinum(모든 세대) ■ Intel Xeon Gold(모든 세대) ■ Intel Xeon Silver(모든 세대) ■ Intel Xeon Bronze(모든 세대)

NSX Edge 베어메탈 하드웨어 요구 사항

사용 중인 베어메탈 NSX Edge 하드웨어가 URL <https://certification.ubuntu.com/server/models/?release=18.04%20LTS&category=Server>에 나열되어 있는지 확인합니다. 하드웨어가 나열되어 있지 않다면 스토리지, 비디오 어댑터 또는 마더보드 구성 요소가 NSX Edge 장치에서 작동하지 않을 수 있습니다.

NSX Edge 베어메탈 NIC 요구 사항

NIC 유형	설명	PCI 디바이스 ID	펌웨어 버전
Mellanox ConnectX-4 EN	PCI_DEVICE_ID_MELLANOX_CONNECTX4	0x1013	12.21.1000 이상
Mellanox ConnectX-4 Lx EN	PCI_DEVICE_ID_MELLANOX_CONNECTX4LX	0x1015	14.21.1000 이상
Mellanox ConnectX-5	PCI_DEVICE_ID_MELLANOX_CONNECTX5	0x1017	16.21.1000 이상
Mellanox ConnectX-5 EX	PCI_DEVICE_ID_MELLANOX_CONNECTX5EX	0x1019	16.21.1000 이상
Intel XXV710	I40E_DEV_ID_25G_B	0x158A	6.0.1
	I40E_DEV_ID_25G_SFP28	0x158B	6.0.1

NIC 유형	설명	PCI 디바이스 ID	펌웨어 버전
Intel X520/Intel 82599	IXGBE_DEV_ID_82599_KX4	0x10F7	n/a
	IXGBE_DEV_ID_82599_KX4_MEZZ	0x1514	n/a
	IXGBE_DEV_ID_82599_KR	0x1517	n/a
	IXGBE_DEV_ID_82599_COM	0x10F8	n/a
	BO_BACKPLANE	0x000C	n/a
	IXGBE_SUBDEV_ID_82599_KX4_KR_MEZZ	0x10F9	n/a
	IXGBE_DEV_ID_82599_CX4	0x10FB	n/a
	IXGBE_DEV_ID_82599_SFP	0x11A9	n/a
	IXGBE_DEV_ID_82599_SFP	0x1F72	n/a
	IXGBE_SUBDEV_ID_82599_SFP	0x17D0	n/a
	IXGBE_SUBDEV_ID_82599_SFP	0x0470	n/a
	IXGBE_SUBDEV_ID_82599_RNDC	0x1507	n/a
	IXGBE_SUBDEV_ID_82599_560FLR	0x154D	n/a
	IXGBE_SUBDEV_ID_82599_560FLR	0x154A	n/a
	IXGBE_SUBDEV_ID_82599_ECNADP	0x1558	n/a
	IXGBE_SUBDEV_ID_82599_ECNADP	0x1557	n/a
	IXGBE_DEV_ID_82599_SFP_EM	0x10FC	n/a
	IXGBE_DEV_ID_82599_SFP_SF2	0x151C	n/a
	IXGBE_DEV_ID_82599_SFP_SF_QP		
	IXGBE_DEV_ID_82599_QSFP_SF_QP		
	IXGBE_DEV_ID_82599EN_SFP		
	IXGBE_DEV_ID_82599_XAUI_LOM		
	IXGBE_DEV_ID_82599_T3_LOM		
Intel X540	IXGBE_DEV_ID_X540T	0x1528	n/a
	IXGBE_DEV_ID_X540T1	0x1560	n/a
Intel X550	IXGBE_DEV_ID_X550T	0x1563	n/a
	IXGBE_DEV_ID_X550T1	0x15D1	n/a
Intel X710	I40E_DEV_ID_SFP_X710	0x1572	6.0.1
	I40E_DEV_ID_KX_C	0x1581	6.0.1
	I40E_DEV_ID_10G_BASE_T	0x1586	6.0.1
Intel XL710	I40E_DEV_ID_KX_B	0x1580	6.0.1
	I40E_DEV_ID_QSFP_A	0x1583	6.0.1
	I40E_DEV_ID_QSFP_B	0x1584	6.0.1
	I40E_DEV_ID_QSFP_C	0x1585	6.0.1
Cisco VIC 1300 시리즈	Cisco UCS 가상 인터페이스 카드 1300	0x0043	n/a

참고 위에 나열된 모든 지원 NIC에 대해 사용하는 미디어 어댑터와 케이블이 벤더의 지원되는 미디어 유형을 따르는지 확인합니다. 공급업체에서 지원하지 않는 모든 미디어 어댑터 또는 케이블은 인식할 수 없는 미디어 어댑터로 인해 부팅 불가능을 비롯한 예기치 않은 동작을 유발할 수 있습니다. 지원되는 미디어 어댑터 및 케이블에 대한 자세한 내용은 NIC 벤더 설명서를 참조하십시오.

베어메탈 서버 시스템 요구 사항

베어메탈 서버를 구성하기 전에 서버가 지원 요구 사항을 충족하는지 확인합니다.

중요 설치를 수행하는 사용자는 일부 절차를 위해 **sudo** 명령 사용 권한이 필요할 수 있습니다. [베어메탈 서버에 타사 패키지 설치](#)의 내용을 참조하십시오.

베어메탈 서버 요구 사항

운영 체제	버전	CPU 코어	메모리
CentOS Linux	7.4(1708) 7.5	4	16GB
RHEL(Red Hat Enterprise Linux)	7.6(커널: 3.10.0-957) 7.5 7.4(커널: 3.10.0-6**)	4	16GB
SUSE Linux Enterprise Server	12 sp3, 12 sp4	4	16GB
Ubuntu	16.04.2 LTS(커널: 4.4.0-*) 18.04	4	16GB

참고 NSX-T Data Center 2.5부터 버전 18.04.2 LTS를 실행하는 Ubuntu 호스트는 버전 16.04에서 업그레이드하거나 새로 설치될 수 있습니다.

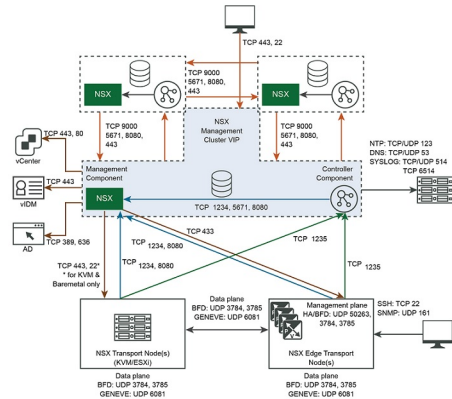
베어메탈 Linux 컨테이너 요구 사항

베어메탈 Linux 컨테이너 요구 사항에 대해서는 "OpenShift용 NSX Container Plug-in - 설치 및 관리 가이드"를 참조하십시오.

포트 및 프로토콜

포트와 프로토콜은 NSX-T Data Center에서 노드 간 통신 경로를 허용하고, 경로가 보호 및 인증되고, 자격 증명의 스토리지 위치가 상호 인증을 설정하는 데 사용됩니다.

참고 필수 포트 및 프로토콜은 물리적 및 호스트 하이퍼바이저 방화벽 둘 다에서 열려 있어야 합니다.



기본적으로 모든 인증서는 자체 서명된 인증서입니다. 노스바운드 GUI 및 API 인증서와 개인 키는 CA 서명 인증서로 대체될 수 있습니다.

루프백 또는 UNIX 도메인 소켓을 통해 통신하는 내부 데몬이 있습니다.

- KVM: MPA, netcpa, nsx-agent, OVS
- ESXi: netcpa, ESX-DP(커널에서)

참고 NSX-T Data Center 노드에 액세스하려면 이러한 노드에서 SSH를 사용하도록 설정해야 합니다.

NSX Cloud 참조 NSX Cloud 배포에 필요한 포트 목록은 [포트 및 프로토콜에 대한 액세스 사용](#) 항목을 참조하십시오.

NSX Manager에서 사용되는 TCP 및 UDP 포트

NSX Manager에서는 특정 TCP 및 UDP 포트를 사용하여 다른 구성 요소 및 제품과 통신합니다. 이러한 포트는 방화벽에서 열려 있어야 합니다.

API 호출 또는 CLI 명령을 사용하여 파일 전송을 위한 사용자 지정 포트(기본 포트 22)와 Syslog 데이터를 내보내기 위한 포트(기본 포트 514 및 6514)를 지정할 수 있습니다. 이 경우 방화벽도 지정된 포트에 따라 구성해야 합니다.

표 3-2. NSX Manager에서 사용되는 TCP 및 UDP 포트

소스	대상	포트	프로토콜	설명
NSX Manager, NSX Edge 노드, 전송 노드	NSX Manager	5671, 1234, 1235, 443	TCP	NSX 메시지
NSX Manager, NSX Edge 노드, 전송 노드, vCenter Server	NSX Manager	8080	TCP	HTTP 저장소 설치-업그레이드

표 3-2. NSX Manager에서 사용되는 TCP 및 UDP 포트 (계속)

소스	대상	포트	프로토콜	설명
NSX Manager	NSX Manager	9000 5671, 1234, 443, 8080	TCP	분산 데이터스토어
NSX Manager	DNS 서버	53	TCP	DNS
NSX Manager	DNS 서버	53	UDP	DNS
NSX Manager	관리 SCP 서버	22	TCP	SSH(지원 번들, 백업 등 업로드)
NSX Manager	NTP 서버	123	UDP	NTP
NSX Manager	SNMP 서버	161, 162	TCP	SNMP
NSX Manager	SNMP 서버	161, 162	UDP	SNMP
NSX Manager	Syslog 서버	514	TCP	Syslog
NSX Manager	Syslog 서버	514	UDP	Syslog
NSX Manager	Syslog 서버	6514	TCP	Syslog
NSX Manager	Syslog 서버	6514	UDP	Syslog
NSX Manager	중간 및 루트 CA 서버	80	TCP	Syslog(TLS를 통해 내보내기) 참고 CRL(인증서 해지 목록)을 검색하는데 사용해야 하는 TCP 포트를 확인하려면 인증 기관의 CDP(CRL 배포 지점) URI를 기준으로 확인합니다.
NSX Manager	Traceroute 대상	3343 4 - 3352 3	UDP	Traceroute
NSX Manager	vCenter Server	80	TCP	NSX Manager - 계산 관리자(vCenter Server) 통신, 구성된 경우
NSX Manager	vCenter Server	443	TCP	NSX Manager - 계산 관리자(vCenter Server) 통신, 구성된 경우
NTP 서버	NSX Manager	123	UDP	NTP
관리 클라이언트	NSX Manager	22	TCP	SSH(기본적으로 사용되지 않도록 설정됨)
관리 클라이언트	NSX Manager	443	TCP	NSX API 서버
SNMP 서버	NSX Manager	161	UDP	SNMP

NSX Edge에서 사용되는 TCP 및 UDP 포트

NSX Edge에서는 특정 TCP 및 UDP 포트를 사용하여 다른 구성 요소 및 제품과 통신합니다. 이러한 포트는 방화벽에서 열려 있어야 합니다.

API 호출 또는 CLI 명령을 사용하여 파일 전송을 위한 사용자 지정 포트(기본 포트 22)와 Syslog 데이터를 보내기 위한 포트(기본 포트 514 및 6514)를 지정할 수 있습니다. 이 경우 방화벽도 지정된 포트에 따라 구성해야 합니다.

표 3-3. NSX Edge에서 사용되는 TCP 및 UDP 포트

소스	대상	포트	프로토콜	설명
관리 클라이언트	NSX Edge 노드	22	TCP	SSH(기본적으로 사용되지 않도록 설정됨)
NSX 에이전트	NSX Edge 노드	5555	TCP	NSX Cloud - 인스턴스의 에이전트는 NSX Cloud 게이트웨이와 통신합니다.
NSX Edge 노드	DNS 서버	53	UDP	DNS
NSX Edge 노드	관리 SCP 또는 SSH 서버	22	TCP	SSH
NSX Edge 노드	NSX Manager	1235	TCP	LCP(하단 제어부)에서 CCP(중앙 제어부)로의 통신
NSX Edge 노드	NSX Edge 노드	1167	TCP	DHCP 백엔드
NSX Edge 노드	NSX Edge 노드	2480	TCP	Nestdb
NSX Edge 노드	NSX Edge 노드	6666	TCP	NSX Cloud - NSX Edge 로컬 통신.
NSX Edge 노드	NSX Edge 노드	50263	UDP	고가용성
NSX Edge 노드	NSX Manager	443	TCP	HTTPS
NSX Edge 노드	NSX Manager	1234	TCP	NSX Manager에 대한 NSX 메시징 채널
NSX Edge 노드	NSX Manager	8080	TCP	NAPI, NSX-T Data Center 업그레이드
NSX Edge 노드	NTP 서버	123	UDP	NTP
NSX Edge 노드	OpenStack Nova API 서버	3000 - 9000	TCP	메타데이터 프록시
NSX Edge 노드	SNMP 서버	161, 162	TCP	SNMP
NSX Edge 노드	SNMP 서버	161, 162	UDP	SNMP
NSX Edge 노드	Syslog 서버	514	TCP	Syslog
NSX Edge 노드	Syslog 서버	514	UDP	Syslog
NSX Edge 노드	Syslog 서버	6514	TCP	Syslog

표 3-3. NSX Edge에서 사용되는 TCP 및 UDP 포트 (계속)

소스	대상	포트	프로토콜	설명
NSX Edge 노드	Syslog 서버	6514	UDP	Syslog
NSX Edge 노드	중간 및 루트 CA 서버	80	TCP	Syslog(TLS를 통해 내보내기) 참고 CRL(인증서 해지 목록)을 검색하는 데 사용해야 하는 TCP 포트를 확인하려면 인증 기관의 CDP(CRL 배포 지점) URI를 기준으로 확인합니다.
NSX Edge 노드	Traceroute 대상	33434 - 33523	UDP	Traceroute
NSX Edge 노드, 전송 노드	NSX Edge 노드	3784, 3785	UDP	데이터의 전송 노드 TEP IP 주소 사이 BFD.
NTP 서버	NSX Edge 노드	123	UDP	NTP
SNMP 서버	NSX Edge 노드	161	UDP	SNMP

ESXi, KVM 호스트 및 베어메탈 서버에서 사용하는 TCP 및 UDP 포트

ESXi, KVM 호스트 및 베어메탈 서버를 전송 노드로 사용하는 경우에는 특정 TCP 포트와 UDP 포트를 사용할 수 있어야 합니다.

표 3-4. ESXi 및 KVM 호스트에 사용되는 TCP 및 UDP 포트

소스	대상	포트	프로토콜	설명
ESXi 호스트	NSX Manager	1235	TCP	LCP(로컬 제어부)에서 CCP(중앙 제어부)로의 통신
ESXi 호스트	NSX Manager	1234	TCP	NSX Manager에 대한 NSX 메시징 채널 NSX Manager에 대한 AMPQ 통신 채널
ESXi 호스트	NSX Manager	8080	TCP	HTTP 저장소 설치 및 업그레이드
ESXi 및 KVM 호스트	NSX Manager	443	TCP	관리 및 프로비저닝 연결
ESXi 및 KVM 호스트	NSX Manager	443	TCP	HTTP 저장소 설치 및 업그레이드
GENEVE TEP(Termination End Point)	GENEVE TEP(Termination End Point)	6081	UDP	전송 네트워크
KVM 호스트	NSX Manager	1234	TCP	NSX Manager에 대한 NSX 메시징 채널 NSX Manager에 대한 AMPQ 통신 채널

표 3-4. ESXi 및 KVM 호스트에 사용되는 TCP 및 UDP 포트 (계속)

소스	대상	포트	프로토콜	설명
베어메탈 서버 호스트	NSX Manager	5671, 1235, 1234, 8080	TCP	NSX Manager에 대한 AMQP 통신 채널
KVM 호스트	NSX Manager	1235	TCP	LCP(로컬 제어부)에서 CCP(중앙 제어부)로의 통신
KVM 호스트	NSX Manager	8080	TCP	HTTP 저장소 설치 및 업그레이드
NSX Manager	ESXi 호스트	443	TCP	관리 및 프로비저닝 연결
NSX Manager	KVM 호스트	443	TCP	관리 및 프로비저닝 연결
호스트	Syslog 서버	514	TCP	Syslog(호스트 syslog 설명서 참조)
호스트	Syslog 서버	514	UDP	Syslog(호스트 syslog 설명서 참조)
호스트	Syslog 서버	6514	TCP	Syslog(호스트 syslog 설명서 참조)
호스트	Syslog 서버	6514	UDP	Syslog(호스트 syslog 설명서 참조)
호스트	중간 및 루트 CA 서버	80	TCP	Syslog(TLS를 통해 내보내기) 참고 CRL(인증서 해지 목록)을 검색하는 데 사용해야 하는 TCP 포트를 확인하려면 인증 기관의 CDP(CRL 배포 지점) URI를 기준으로 확인합니다.
NSX-T Data Center 전송 노드	NSX-T Data Center 전송 노드	3784, 3785	UDP	TEP 인터페이스를 사용한 데이터 경로에서 TEP 간의 BFD 세션

NSX Manager 설치

4

NSX Manager는 논리적 스위치, 논리적 라우터 및 방화벽과 같은 NSX-T Data Center 구성 요소의 생성, 구성 및 모니터링을 위한 GUI(그래픽 사용자 인터페이스) 및 REST API를 제공합니다.

NSX Manager는 시스템 보기를 제공하며, NSX-T Data Center의 관리 구성 요소입니다.

고가용성을 위해 NSX-T Data Center는 3개의 NSX Manager로 구성된 관리 클러스터를 지원합니다. 운영 환경의 경우 관리 클러스터를 배포하는 것이 좋습니다. 개념 증명 환경의 경우 하나의 NSX Manager를 배포할 수 있습니다.

vSphere 환경에서는 NSX Manager는 다음 기능을 지원합니다.

- vCenter Server는 vMotion 함수를 사용하여 호스트 및 클러스터에서 NSX Manager를 실시간으로 마이그레이션할 수 있습니다.
- vCenter Server는 Storage vMotion 함수를 사용하여 호스트 및 클러스터에서 NSX Manager를 실시간으로 마이그레이션할 수 있습니다.
- vCenter Server는 Distributed Resource Scheduler 기능을 사용하여 호스트와 클러스터에서 NSX Manager를 재조정할 수 있습니다.
- vCenter Server는 반선택도 기능을 사용하여 호스트 및 클러스터에서 NSX Manager를 관리할 수 있습니다.

NSX Manager 배포, 플랫폼 및 설치 요구 사항

다음 표에서는 NSX Manager 배포, 플랫폼 및 설치 요구 사항을 자세히 설명합니다.

요구 사항	설명
지원되는 배포 방법	<ul style="list-style-type: none">■ OVA/OVF■ QCOW2
지원되는 플랫폼	NSX Manager VM 및 호스트 전송 노드 시스템 요구 사항의 내용을 참조하십시오. ESXi에서는 NSX Manager 장치를 공유 스토리지에 설치하는 것이 좋습니다.
IP 주소	NSX Manager에는 정적 IP 주소가 있어야 합니다. 설치 후에는 IP 주소를 변경할 수 없습니다.

요구 사항	설명
NSX-T Data Center 장치 암호	<ul style="list-style-type: none"> ■ 12자 이상 ■ 하나 이상의 소문자 ■ 하나 이상의 대문자 ■ 하나 이상의 숫자 ■ 하나 이상의 특수 문자 ■ 5개 이상의 다른 문자 ■ 기본 암호 복잡성 규칙은 다음 Linux PAM 모듈 인수에 의해 적용됩니다. <ul style="list-style-type: none"> ■ retry=3: 오류 결과를 반환하기 전에 새 암호를 입력할 수 있는 최대 횟수로, 이 인수의 경우 최대 3번입니다. ■ minlen=12: 새 암호에 허용되는 최소 크기입니다. 새 암호의 문자 수 외에도 다른 종류의 문자(예: 대문자, 소문자 및 숫자)에 대해 크레딧(길이에서 +1)이 지정됩니다. ■ difok=0: 새 암호에서 달라야 하는 최소 바이트 수입니다. 이전 암호와 새 암호 간 유사성을 나타냅니다. difok에 값 0을 할당하면 이전 암호 및 새 암호 바이트를 다르게 유지할 필요가 없습니다. 정확한 일치만 허용됩니다. ■ lcredit=1: 새 암호에서 소문자에 대한 최대 크레딧입니다. 1개 이하의 소문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다. ■ ucredit=1: 새 암호에서 대문자에 대한 최대 크레딧입니다. 1개 이하의 대문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다. ■ dcredit=1: 새 암호에서 숫자에 대한 최대 크레딧입니다. 1개 이하의 숫자가 있는 경우 각 숫자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다. ■ ocredit=1: 새 암호에서 다른 문자에 대한 최대 크레딧입니다. 1개 이하의 다른 문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다. ■ enforce_for_root: 암호가 루트 사용자에게 설정됩니다. <p>참고 사전 단어를 기준으로 암호를 확인하기 위한 Linux PAM 모듈에 대한 자세한 내용은 설명서 페이지를 참조하십시오.</p> <p>예를 들어 VMware123!123 또는 VMware12345와 같이 간단하고 규칙적인 암호는 사용하지 마십시오. 복잡성 표준을 충족하는 암호는 간단하고 체계적이지 않지만 문자, 알파벳, 특수 문자 및 숫자 조합(예: VMware123!45, VMware1!2345 또는 VMware@1az23x)입니다.</p>
호스트 이름	<p>NSX Manager 설치 시 밑줄과 같은 잘못된 문자 또는 점 "."과 같은 특수 문자를 포함하지 않는 호스트 이름을 지정합니다. 호스트 이름에 유효하지 않은 문자 또는 특수 문자가 포함되어 있으면 배포 후에 호스트 이름이 nsx-manager로 설정됩니다.</p> <p>호스트 이름 제한에 대한 자세한 내용은 https://tools.ietf.org/html/rfc952 및 https://tools.ietf.org/html/rfc1123을 참조하십시오.</p>
VMware Tools	<p>ESXi에서 실행되는 NSX Manager VM에는 VMTools가 설치되어 있습니다. VMTools를 제거하거나 업그레이드하지 마십시오.</p>

요구 사항	설명
시스템	<ul style="list-style-type: none"> ■ 시스템 요구 사항이 충족되었는지 확인합니다. 시스템 요구 사항의 내용을 참조하십시오. ■ 필수 포트가 열려 있는지 확인합니다. 포트 및 프로토콜의 내용을 참조하십시오. ■ 데이터스토어가 구성되었고 ESXi 호스트에서 액세스할 수 있는지 확인합니다. ■ NSX Manager에서 사용할 IP 주소와 게이트웨이, DNS 서버 IP 주소, 도메인 검색 목록 및 NTP 서버 IP 주소가 있는지 확인합니다. ■ 대상 VM 포트 그룹 네트워크가 아직 없으면 생성합니다. NSX-T Data Center 장치를 관리 VM 네트워크에 배치합니다. <p>여러 관리 네트워크가 있으면 NSX-T Data Center 장치에서 다른 네트워크로의 정적 경로를 추가할 수 있습니다.</p> <ul style="list-style-type: none"> ■ NSX Manager IPv4 IP 주소 지정 체계를 계획합니다.
OVF 권한	<p>ESXi 호스트에 OVF 템플릿을 배포하기 위한 적절한 권한이 있는지 확인합니다.</p> <p>vCenter Server 또는 vSphere Client와 같은 OVF 템플릿을 배포할 수 있는 관리 도구. OVF 배포 도구는 수동 구성을 허용하는 구성 옵션을 지원해야 합니다.</p> <p>OVF 도구 버전은 4.0 이상이어야 합니다.</p>
클라이언트 플러그인	클라이언트 통합 플러그인이 설치되어 있어야 합니다.

참고 NSX Manager 새로 설치 또는 재부팅 시나 처음 부팅할 때 **관리자** 암호를 변경한 경우 NSX Manager가 시작되는 데 몇 분 정도 걸릴 수 있습니다.

NSX Manager 설치 시나리오

중요 vSphere Client에서든 또는 명령줄에서든 OVA 또는 OVF 파일에서 NSX Manager를 설치하는 경우 OVA/OVF 속성 값(예: 사용자 이름 및 암호)은 VM 전원이 켜진 후에만 확인됩니다. 그러나 정적 IP 주소 필드는 NSX Manager를 설치하기 위한 필수 필드입니다.

- **admin** 또는 **audit** 사용자에게 대해 사용자 이름을 지정하는 경우 사용자 이름이 고유해야 합니다. 동일한 이름을 지정하면 무시되고 기본 이름(**admin** 및 **audit**)이 사용됩니다.
- **admin** 사용자에게 대한 암호가 복잡성 요구 사항을 충족하지 못하면 SSH를 통해 또는 콘솔에서 **default** 암호를 사용하여 **admin** 사용자로 NSX Manager에 로그인해야 합니다. 암호를 변경하라는 메시지가 표시됩니다.
- **audit** 사용자에게 대한 암호가 복잡성 요구 사항을 충족하지 못하면 사용자 계정이 사용되지 않도록 설정됩니다. 계정을 사용하도록 설정하려면 SSH를 통해 또는 콘솔에서 **admin** 사용자 권한으로 NSX Manager에 로그인하고 **set user audit** 명령을 실행하고 **audit** 사용자의 암호를 설정합니다(현재 암호는 빈 문자열임).

- **root** 사용자에게 대한 암호가 복잡성 요구 사항을 충족하지 못하면 SSH를 통해 또는 콘솔에서 **vmware** 암호를 사용하여 **root** 사용자 권한으로 NSX Manager에 로그인해야 합니다. 암호를 변경하라는 메시지가 표시됩니다.

경고 **root** 사용자 자격 증명으로 로그인한 상태에서 NSX-T Data Center에 대해 변경을 수행하면 시스템 오류가 발생할 수 있고 잠재적으로 네트워크에 영향을 줄 수 있습니다. VMware 지원 팀이 안내하는 경우에만 **root** 사용자 자격 증명을 사용하여 변경을 수행할 수 있습니다.

참고 장치의 핵심 서비스는 충분한 복잡도를 갖는 암호를 설정해야만 시작할 수 있습니다.

OVA 파일에서 NSX Manager를 배포한 후에는 VM 전원을 끄고 vCenter Server에서 OVA 설정을 수정하여 VM의 IP 설정을 변경할 수 없습니다.

DNS 서버에서 액세스하도록 NSX Manager 구성

기본적으로 전송 노드는 해당 IP 주소를 기준으로 NSX Manager에 액세스합니다. 그러나 NSX Manager의 DNS 이름을 기준으로 액세스할 수도 있습니다.

NSX Manager에서 FQDN 사용(DNS)을 설정하면 전송 노드에 영향을 주지 않으면서 관리자의 IP 주소를 변경할 수 있습니다.

NSX Manager의 FQDN을 게시하여 FQDN 사용을 설정합니다.

참고 다중 사이트 Lite와 NSX Cloud 및 배포에서는 NSX Manager에서 FQDN 사용(DNS)을 설정해야 합니다. (다른 모든 배포 유형에서는 선택 사항임) "NSX-T Data Center 관리 가이드"의 " " NSX-T Data Center의 다중 사이트 배포와 이 가이드의 [장 13 NSX Cloud 구성 요소 설치](#)를 참조하십시오.

NSX Manager의 FQDN 게시

NSX-T Data Center 핵심 구성 요소와 CSM를 설치한 후 FQDN을 사용하여 NAT를 사용하도록 설정하려면 DNS 서버의 관리자 노드에 대한 정방향 및 역방향 조회 항목을 설정해야 합니다.

중요 짧은 TTL(예: 600초)을 사용하여 NSX Manager의 FQDN에 대한 정방향 및 역방향 조회 항목을 모두 구성하는 것이 좋습니다.

또한 NSX-T API를 사용하여 NSX Manager FQDN 게시를 사용하도록 설정해야 합니다.

요청 예: PUT <https://<nsx-mgr>/api/v1/configs/management>

```
{
  "publish_fqdns": true,
  "_revision": 0
}
```

응답 예:

```
{
  "publish_fqdns": true,
  "_revision": 1
}
```

자세한 내용은 "NSX-T Data Center API 가이드" 항목을 참조하십시오.

참고 FQDN을 게시한 후에는 다음 섹션에 설명된 대로 전송 노드에 의한 액세스가 유효한지 검사합니다.

전송 노드의 FQDN을 통한 액세스가 유효한지 검사

NSX Manager의 FQDN을 게시한 후 전송 노드가 NSX Manager에 성공적으로 액세스하고 있는지 확인합니다.

SSH를 사용하여 하이퍼바이저 또는 Edge 노드와 같은 전송 노드에 로그인하고 `get controllers` CLI 명령을 실행합니다.

응답 예:

Controller IP	Port	SSL	Status	Is Physical Master	Session State	Controller FQDN
192.168.60.5	1235	enabled	connected	true	up	nsxmgr.corp.com

본 장은 다음 항목을 포함합니다.

■ 기본 관리자 암호 만료 수정

기본 관리자 암호 만료 수정

기본적으로 NSX Manager 및 NSX Edge 장치의 관리 암호는 90일 후에 만료됩니다. 그러나 초기 설치 및 구성 후에 만료 기간을 재설정할 수 있습니다.

암호가 만료되면 구성 요소를 로그인하고 관리할 수 없습니다. 또한 관리 암호를 실행해야 하는 작업 또는 API 호출이 실패합니다. 암호가 만료되면 기술 자료 문서 70691 [NSX-T 관리자 암호 만료됨](#)을 참조하십시오.

절차

- 1 보안 프로그램을 사용하여 NSX CLI 콘솔에 연결합니다.
- 2 만료 기간을 재설정합니다.

1에서 9999일 사이의 만료 기간을 지정할 수 있습니다.

```
nsxcli> set user admin password-expiration <1 - 9999>
```

참고 또는 API 명령을 사용하여 관리자 암호 만료 기간을 설정할 수 있습니다.

- 3** (선택 사항) 암호가 만료되지 않도록 암호 만료를 사용 안 함으로 설정할 수 있습니다.

```
nsxcli> clear user audit password-expiration
```

vSphere에 NSX-T Data Center 설치

5

UI 또는 CLI를 사용하여 NSX-T Data Center 구성 요소, NSX Manager 및 NSX Edge를 설치할 수 있습니다.

지원되는 vSphere 버전을 사용 중인지 확인해야 합니다. [vSphere 지원](#)을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [NSX Manager](#) 및 사용 가능한 장치 설치
- 클러스터에 대해 [VIP\(가상 IP\)](#) 주소 구성
- [NSX-T 장치에서 스냅샷 사용 안 함](#)

NSX Manager 및 사용 가능한 장치 설치

vSphere Client를 사용하여 NSX Manager 또는 Cloud Service Manager를 가상 장치로 배포할 수 있습니다.

Cloud Service Manager는 NSX-T Data Center 구성 요소를 사용하고 이를 공용 클라우드와 통합하는 가상 장치입니다.

사전 요구 사항

- 시스템 요구 사항이 충족되었는지 확인합니다. [시스템 요구 사항](#)의 내용을 참조하십시오.
- 필수 포트가 열려 있는지 확인합니다. [포트 및 프로토콜](#)의 내용을 참조하십시오.
- 데이터스토어가 구성되었고 ESXi 호스트에서 액세스할 수 있는지 확인합니다.
- NSX Manager에서 사용할 IP 주소와 게이트웨이, DNS 서버 IP 주소, 도메인 검색 목록 및 NTP 서버 IP 주소가 있는지 확인합니다.
- 대상 VM 포트 그룹 네트워크가 아직 없으면 생성합니다. NSX-T Data Center 장치를 관리 VM 네트워크에 배치합니다.

여러 관리 네트워크가 있으면 NSX-T Data Center 장치에서 다른 네트워크로의 정적 경로를 추가할 수 있습니다.

- NSX Manager IPv4 IP 주소 지정 체계를 계획합니다.

절차

- 1 VMware 다운로드 포털에서 NSX-T Data Center OVA 파일을 찾습니다.
다운로드 URL을 복사하거나 OVA 파일을 다운로드합니다.
- 2 마우스 오른쪽 버튼을 클릭하고 **OVF 템플릿 배포**를 선택하여 설치 마법사를 시작합니다.
- 3 OVA 다운로드 URL을 입력하거나 OVA 파일로 이동하고 **다음**을 클릭합니다.
- 4 이름을 입력하고 NSX Manager VM의 위치를 입력한 후 **다음**을 클릭합니다.
입력한 이름이 vSphere 및 vCenter Server 인벤토리에 나타납니다.
- 5 NSX Manager 장치의 계산 리소스를 선택하고 **다음**을 클릭합니다.
 - ◆ vCenter에서 관리되는 ESXi 호스트에 설치하려면 NSX Manager 장치를 배포할 호스트를 선택합니다.
 - ◆ 독립형 ESXi 호스트에 설치하려면 NSX Manager 장치를 배포할 호스트를 선택합니다.
- 6 OVF 템플릿 세부 정보를 검토하고 확인한 후 **다음**을 클릭합니다.
- 7 배포 구성 크기를 지정한 후 **다음**을 클릭합니다.
마법사의 오른쪽에 있는 [설명] 패널에 선택한 구성의 세부 정보가 표시됩니다.
- 8 구성 및 디스크 파일의 스토리지를 지정합니다.
 - a 가상 디스크 형식을 선택합니다.
 - b VM 스토리지 정책을 선택합니다.
 - c NSX Manager 장치 파일을 저장할 데이터스토어를 지정합니다.
 - d **다음**을 클릭합니다.
- 9 각 소스 네트워크의 대상 네트워크를 선택합니다.
- 10 NSX Manager에 대한 포트 그룹 또는 대상 네트워크를 선택합니다.
- 11 IP 할당 설정을 구성합니다.
 - a IP 할당의 경우 **고정 - 수동**을 지정합니다.
 - b IP 프로토콜의 경우 **IPv4**를 선택합니다.
- 12 **다음**을 클릭합니다.
다음 단계는 모두 [OVF 템플릿 배포] 마법사의 [템플릿 사용자 지정] 섹션에 있습니다.
- 13 [애플리케이션] 섹션에서 NSX Manager에 대한 시스템 루트, CLI 관리자 및 감사 암호를 입력합니다.
root 및 **admin** 자격 증명은 필수 필드입니다.
암호는 암호 길이 제한을 준수해야 합니다.
 - 12자 이상
 - 하나 이상의 소문자

- 하나 이상의 대문자
- 하나 이상의 숫자
- 하나 이상의 특수 문자
- 5개 이상의 다른 문자
- 기본 암호 복잡성 규칙은 다음 Linux PAM 모듈 인수에 의해 적용됩니다.
 - **retry=3**: 오류 결과를 반환하기 전에 새 암호를 입력할 수 있는 최대 횟수로, 이 인수의 경우 최대 3번입니다.
 - **minlen=12**: 새 암호에 허용되는 최소 크기입니다. 새 암호의 문자 수 외에도 다른 종류의 문자(예: 대문자, 소문자 및 숫자)에 대해 크레딧(길이에서 +1)이 지정됩니다.
 - **difok=0**: 새 암호에서 달라야 하는 최소 바이트 수입니다. 이전 암호와 새 암호 간 유사성을 나타냅니다. difok에 값 0을 할당하면 이전 암호 및 새 암호 바이트를 다르게 유지할 필요가 없습니다. 정확한 일치만 허용됩니다.
 - **lcredit=1**: 새 암호에서 소문자에 대한 최대 크레딧입니다. 1개 이하의 소문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다.
 - **ucredit=1**: 새 암호에서 대문자에 대한 최대 크레딧입니다. 1개 이하의 대문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다.
 - **dcredit=1**: 새 암호에서 숫자에 대한 최대 크레딧입니다. 1개 이하의 숫자가 있는 경우 각 숫자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다.
 - **ocredit=1**: 새 암호에서 다른 문자에 대한 최대 크레딧입니다. 1개 이하의 다른 문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다.
 - **enforce_for_root**: 암호가 루트 사용자에게 대해 설정됩니다.

참고 사전 단어를 기준으로 암호를 확인하기 위한 Linux PAM 모듈에 대한 자세한 내용은 설명서 페이지를 참조하십시오.

예를 들어 **VMware123!123** 또는 **VMware12345**와 같이 간단하고 규칙적인 암호는 사용하지 마십시오. 복잡성 표준을 충족하는 암호는 간단하고 체계적이지 않지만 문자, 알파벳, 특수 문자 및 숫자 조합(예: **VMware123!45**, **VMware1!2345** 또는 **VMware@1az23x**)입니다.

- 14** [선택적 매개 변수] 섹션에서 암호 필드를 비워 둡니다. vCenter Server에 액세스할 수 있는 사용자가 VMC 역할에 설정한 암호를 손상시킬 위험을 방지하기 위한 것입니다. NSX-T Data Center에 VMC를 배포할 때 이 필드는 클라우드 관리자 및 클라우드 감사 역할에 암호를 설정하기 위해 내부적으로 사용됩니다.
- 15** [네트워크 속성] 섹션에서 NSX Manager의 호스트 이름을 입력합니다.

참고 호스트 이름은 올바른 도메인 이름이어야 합니다. 점으로 구분된 호스트 이름(domain/subdomain)의 각 부분은 알파벳 문자로 시작해야 합니다.

16 장치에 대한 **역할 이름**을 선택합니다. 기본 역할은 **NSX Manager**입니다.

- NSX Manager 장치를 설치하려면 **NSX Manager** 역할을 선택합니다.
- NSX Cloud 배포를 위해 Cloud Service Manager(CSM) 장치를 설치하려면 **nsx-cloud-service-manager** 역할을 선택합니다.

자세한 내용은 [NSX Cloud 배포 개요](#) 항목을 참조하십시오.

17 (필수 필드) 기본 게이트웨이, 관리 네트워크 IPv4 및 관리 네트워크 넷마스크를 입력합니다.

중요 정적 IP 주소를 입력하지 않고 [관리 네트워크 IPv4] 필드를 비워 두면 장치를 배포하는 동안 NSX Manager에 IP 주소가 할당되지 않습니다. 전원을 켜 때 NSX Manager에 액세스할 수 없습니다. 해결 방법은 NSX Manager 장치를 다시 배포하는 것입니다.

18 [DNS] 섹션에서 DNS 서버 목록 및 도메인 검색 목록을 입력합니다.

19 [서비스 구성] 섹션에서 NTP 서버 목록을 입력합니다.

필요한 경우 SSH 서비스를 사용하도록 설정하고 루트 SSH 로그인을 허용할 수 있습니다. (권장되지 않음)

20 모든 사용자 지정 OVF 템플릿 규격이 정확한지 확인하고 **완료**를 클릭하여 설치를 시작합니다.

설치가 완료되는 데는 7-8분 정도 걸릴 수 있습니다.

21 최적의 성능을 위해 장치를 위한 메모리를 예약합니다.

NSX Manager가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정합니다. [NSX Manager VM 및 호스트 전송 노드 시스템 요구 사항](#)의 내용을 참조하십시오.

22 vSphere Client에서 VM 콘솔을 열어 노드의 부팅 프로세스를 추적합니다.

23 노드가 부팅되면 CLI에 관리자 권한으로 로그인하고 **get interface eth0** 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

24 **get services** 명령을 입력하여 모든 기본 서비스가 실행되고 있는지 확인합니다.

다음 서비스는 기본적으로 필요하지 않으며 자동으로 시작되지 않습니다.

- **liagent**
- **migration-coordinator**: 이 서비스는 마이그레이션 조정자를 실행하는 경우에만 사용됩니다. 이 서비스를 시작하기 전에 "NSX-T Data Center 마이그레이션 조정기 가이드"를 참조하십시오.
- **snmp**: SNMP 시작에 대한 자세한 내용은 "NSX-T Data Center 관리 가이드"에서 "Simple Network Management Protocol"을 참조하십시오.
- **nsx-message-bus**: 이 서비스는 NSX-T Data Center 3.0에서 사용되지 않습니다.

25 NSX Manager 또는 글로벌 관리자 노드에 필요한 연결이 있는지 확인합니다.

다음 작업을 수행할 수 있는지 확인하십시오.

- 다른 시스템에서 노드를 Ping합니다.

- 노드에서 기본 게이트웨이를 Ping할 수 있습니다.
- 노드에서 관리 인터페이스를 사용하여 동일한 네트워크에 있는 하이퍼바이저 호스트를 Ping할 수 있습니다.
- 노드에서 DNS 서버와 NTP 서버를 Ping할 수 있습니다.
- SSH를 사용하도록 설정한 경우 노드에 대해 SSH를 수행할 수 있는지 확인합니다.

연결이 설정되지 않은 경우 가상 장치의 네트워크 어댑터가 적절한 네트워크 또는 VLAN에 있는지 확인합니다.

다음에 수행할 작업

지원되는 웹 브라우저를 사용하여 NSX Manager에 로그인합니다. [새로 생성된 NSX Manager에 로그인](#) 항목을 참조하십시오.

명령줄 OVF 도구를 사용하여 ESXi에 NSX Manager 설치

NSX Manager 설치를 자동화하거나 설치를 위해 CLI를 사용하려면 명령줄 유틸리티인 VMware OVF Tool을 사용하면 됩니다.

기본적으로 `nsx_isSSHEnabled` 및 `nsx_allowSSHRootLogin`은 보안상의 이유로 둘 다 사용되지 않도록 설정됩니다. 사용되지 않도록 설정되면 SSH를 실행하거나 NSX Manager 명령줄에 로그인할 수 없습니다. `nsx_isSSHEnabled`는 사용하도록 설정하고 `nsx_allowSSHRootLogin`은 사용하지 않도록 설정하면 NSX Manager에 대해 SSH를 실행할 수 있으나 루트 권한으로 로그인할 수 없습니다.

사전 요구 사항

- 시스템 요구 사항이 충족되었는지 확인합니다. [시스템 요구 사항](#)의 내용을 참조하십시오.
- 필수 포트가 열려 있는지 확인합니다. [포트 및 프로토콜](#)의 내용을 참조하십시오.
- 데이터스토어가 구성되었고 ESXi 호스트에서 액세스할 수 있는지 확인합니다.
- NSX Manager에서 사용할 IP 주소와 게이트웨이, DNS 서버 IP 주소, 도메인 검색 목록 및 NTP 서버 IP 주소가 있는지 확인합니다.
- 대상 VM 포트 그룹 네트워크가 아직 없으면 생성합니다. NSX-T Data Center 장치를 관리 VM 네트워크에 배치합니다.

여러 관리 네트워크가 있으면 NSX-T Data Center 장치에서 다른 네트워크로의 정적 경로를 추가할 수 있습니다.

- NSX Manager IPv4 IP 주소 지정 체계를 계획합니다.

절차

1 ovftool 명령을 해당 매개 변수와 함께 실행합니다.

이 프로세스는 호스트가 독립 실행형인지 또는 vCenter Server에서 관리되는지에 따라 다릅니다.

- 독립 실행형 호스트인 경우:

- Windows 예:

```
C:\Program Files\VMware\VMware OVF Tool>ovftool \
--sourceType=OVA \
--name=nsx-manager \
--deploymentOption=medium \
--X:injectOvfEnv \
--X:logFile=<filepath>\nsxovftool.log \
--allowExtraConfig \
--datastore=<datastore name> \
--network=<network name> \
--acceptAllEulas \
--noSSLVerify \
--diskMode=thin \
--powerOn \
--prop:"nsx_role=NSX Manager" \
--prop:"nsx_ip_0=10.168.110.75" \
--prop:"nsx_netmask_0=255.255.255.0" \
--prop:"nsx_gateway_0=10.168.110.1" \
--prop:"nsx_dns1_0=10.168.110.10" \
--prop:"nsx_domain_0=corp.local" \
--prop:"nsx_ntp_0=10.168.110.10" \
--prop:"nsx_isSSHEnabled=<True|False>" \
--prop:"nsx_allowSSHRootLogin=<True|False>" \
--prop:"nsx_passwd_0=<password>" \
--prop:"nsx_cli_passwd_0=<password>" \
--prop:"nsx_cli_audit_passwd_0=<password>" \
--prop:"nsx_hostname=nsx-manager" \
<nsx-unified-appliance-release>.ova \
vi://root:<password>@10.168.110.51
```

참고 위의 Windows 코드 블록은 백슬래시(\)를 사용하여 명령줄의 연속을 나타냅니다. 실제 사용에서는 백슬래시를 생략하고 전체 명령을 한 줄에 둡니다.

참고 위의 예에서 10.168.110.51은 NSX Manager를 배포할 호스트 시스템의 IP 주소입니다.

참고 위의 예에서 --deploymentOption은 기본값인 Medium으로 설정됩니다. 지원되는 다른 크기를 확인하려면 [NSX Manager VM 및 호스트 전송 노드 시스템 요구 사항](#)을 참조하십시오.

■ Linux 예):

```

mgrformfactor="small"
ipAllocationPolicy="fixedPolicy"
mgrdatastore="QNAP-Share-VMs"
mgrnetwork="Management-VLAN-210"

mgrname01="nsx-manager-01"
mgrhostname01="nsx-manager-01"
mgrip01="192.168.210.121"

mgrnetmask="255.255.255.0"
mgrgw="192.168.210.254"
mgrdns="192.168.110.10"
mgrntp="192.168.210.254"
mgrpasswd="<password>"
mgrssh="<True|False>"
mgrroot="<True|False>"
logLevel="trivia"

mgresxhost01="192.168.110.113"

ovftool --noSSLVerify --skipManifestCheck --powerOn \
--deploymentOption=$mgrformfactor \
--diskMode=thin \
--acceptAllEulas \
--allowExtraConfig \
--ipProtocol=IPv4 \
--ipAllocationPolicy=$ipAllocationPolicy \
--datastore=$mgrdatastore \
--network=$mgrnetwork \
--name=$mgrname01 \
--prop:nsx_hostname=$mgrhostname01 \
--prop:nsx_role="NSX Manager" \
--prop:nsx_ip_0=$mgrip01 \
--prop:nsx_netmask_0=$mgrnetmask \
--prop:nsx_gateway_0=$mgrgw \
--prop:nsx_dns1_0=$mgrdns \
--prop:nsx_ntp_0=$mgrntp \
--prop:nsx_passwd_0=$mgrpasswd \
--prop:nsx_cli_passwd_0=$mgrpasswd \
--prop:nsx_cli_audit_passwd_0=$mgrpasswd \
--prop:nsx_isSSHEnabled=$mgrssh \
--prop:nsx_allowSSHRootLogin=$mgrroot \
--X:logFile=nsxt-manager-ovf.log \
--X:logLevel=$logLevel \
/home/<user/nsxt-autodeploy/<nsx-unified-appliance-release>.ova \
vi://root:<password>@$mgresxhost01

```

결과는 다음과 비슷합니다.

```

Opening OVA source: nsx-<component>.ova
The manifest validates

```

```
Source is signed and the certificate validates
Opening VI target: vi://root:<password>@10.168.110.51
Deploying to VI: vi://root:<password>@10.168.110.51
Transfer Completed
Powering on VM: NSX Manager
Task Completed
Completed successfully
```

- vCenter Server에서 관리되는 호스트의 경우:
 - Windows 예:

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-manager \
--deploymentOption=medium \
--X:injectOvfEnv \
--X:logFile=ovftool.log \
--allowExtraConfig \
--datastore=ds1 \
--network="management" \
--acceptAllEulas \
--noSSLVerify \
--diskMode=thin \
--powerOn \
--prop:"nsx_role=NSX Manager" \
--prop:"nsx_ip_0=10.168.110.75" \
--prop:"nsx_netmask_0=255.255.255.0" \
--prop:"nsx_gateway_0=10.168.110.1" \
--prop:"nsx_dns1_0=10.168.110.10" \
--prop:"nsx_domain_0=corp.local" \
--prop:"nsx_ntp_0=10.168.110.10" \
--prop:"nsx_isSshEnabled=<True|False>" \
--prop:"nsx_allowSSHRootLogin=<True|False>" \
--prop:"nsx_passwd_0=<password>" \
--prop:"nsx_cli_passwd_0=<password>" \
--prop:"nsx_cli_audit_passwd_0=$mgrpasswd" \
--prop:"nsx_hostname=nsx-manager" \
<nsx-unified-appliance-release>.ova \
vi://administrator@vsphere.local:<password>@10.168.110.24/?ip=10.168.110.51
```

참고 위의 Windows 코드 블록은 백슬래시(\)를 사용하여 명령줄의 연속을 나타냅니다. 실제 사용에서는 백슬래시를 생략하고 전체 명령을 한 줄에 둡니다.

참고 위의 예에서 --deploymentOption은 기본값인 Medium으로 설정됩니다. 지원되는 다른 크기를 확인하려면 [NSX Manager VM 및 호스트 전송 노드 시스템 요구 사항](#)을 참조하십시오.

- Linux 예:

```
mgrformfactor="small"
ipAllocationPolicy="fixedPolicy"
mgrdatastore="QNAP-Share-VMs"
```

```

mgrnetwork="Management-VLAN-210"

mgrname01="nsx-manager-01"
mgrhostname01="nsx-manager-01"
mgrip01="192.168.210.121"

mgrnetmask="255.255.255.0"
mgrgw="192.168.210.254"
mgrdns="192.168.110.10"
mgrntp="192.168.210.254"
mgrpasswd="<password>"
mgrssh="<True|False>"
mgrroot="<True|False>"
logLevel="trivia"

vadmin="administrator@vsphere.local"
vcpass="<password>"
vcip="192.168.110.151"
mgresxhost01="192.168.110.113"

ovftool --noSSLVerify --skipManifestCheck --powerOn \
--deploymentOption=$mgrformfactor \
--diskMode=thin \
--acceptAllEulas \
--allowExtraConfig \
--ipProtocol=IPv4 \
--ipAllocationPolicy=$ipAllocationPolicy \
--datastore=$mgrdatastore \
--network=$mgrnetwork \
--name=$mgrname01 \
--prop:nsx_hostname=$mgrhostname01 \
--prop:nsx_role="NSX Manager" \
--prop:nsx_ip_0=$mgrip01 \
--prop:nsx_netmask_0=$mgrnetmask \
--prop:nsx_gateway_0=$mgrgw \
--prop:nsx_dns1_0=$mgrdns \
--prop:nsx_ntp_0=$mgrntp \
--prop:nsx_passwd_0=$mgrpasswd \
--prop:nsx_cli_passwd_0=$mgrpasswd \
--prop:nsx_cli_audit_passwd_0=$mgrpasswd \
--prop:nsx_isSSHEnabled=$mgrssh \
--prop:nsx_allowSSHRootLogin=$mgrroot \
--X:logFile=nsxt-manager-ovf.log \
--X:logLevel=$logLevel \
/home/<user/nsxt-autodeploy/<nsx-unified-appliance-release>.ova \
vi://$vadmin:$vcpass@$vcip/?ip=$mgresxhost01

```

결과는 다음과 비슷합니다.

```

Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://administrator@vsphere.local@10.168.110.24:443/
Deploying to VI: vi://administrator@vsphere.local@10.168.110.24:443/

```

```
Transfer Completed
Powering on VM: NSX Manager
Task Completed
Completed successfully
```

- 2 검색 모드에서 OVF 도구를 실행하여 소스의 콘텐츠를 볼 수도 있습니다. 다른 지원되는 소스 유형 목록에서 OVA 및 OVF 패키지를 프로빙할 수 있습니다. 프로브 모드에서 반환된 정보를 사용하여 배포를 구성할 수 있습니다.

```
$> \ovftool --allowExtraConfig <OVA path or URL>
```

여기서, --allowExtraConfig는 CSM(Cloud Service Manager)에 대해 지원되는 어플라이언스 유형입니다.

- 3 최적의 성능을 위해 장치를 위한 메모리를 예약합니다.

NSX Manager가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정합니다. [NSX Manager VM 및 호스트 전송 노드 시스템 요구 사항](#)의 내용을 참조하십시오.

- 4 vSphere Client에서 VM 콘솔을 열어 노드의 부팅 프로세스를 추적합니다.
- 5 노드가 부팅되면 CLI에 관리자 권한으로 로그인하고 `get interface eth0` 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.
- 6 NSX Manager 또는 글로벌 관리자 노드에 필요한 연결이 있는지 확인합니다.

다음 작업을 수행할 수 있는지 확인하십시오.

- 다른 시스템에서 노드를 Ping합니다.
- 노드에서 기본 게이트웨이를 Ping할 수 있습니다.
- 노드에서 관리 인터페이스를 사용하여 동일한 네트워크에 있는 하이퍼바이저 호스트를 Ping할 수 있습니다.
- 노드에서 DNS 서버와 NTP 서버를 Ping할 수 있습니다.
- SSH를 사용하도록 설정한 경우 노드에 대해 SSH를 수행할 수 있는지 확인합니다.

연결이 설정되지 않은 경우 가상 장치의 네트워크 어댑터가 적절한 네트워크 또는 VLAN에 있는지 확인합니다.

다음에 수행할 작업

지원되는 웹 브라우저를 사용하여 NSX Manager에 로그인합니다. [새로 생성된 NSX Manager에 로그인](#)의 내용을 참조하십시오.

부팅 시 GRUB 메뉴를 표시하도록 NSX-T Data Center 구성

NSX-T Data Center 장치의 루트 암호를 재설정하기 위해서는 부팅 시 GRUB 메뉴가 표시되도록 NSX-T Data Center 장치를 구성해야 합니다.

중요 장치를 배포한 이후 구성 작업을 수행하지 않으면 루트, 관리자 또는 감사 암호를 잊어버린 경우에 재설정할 수 없습니다.

절차

- 1 VM에 루트로 로그인합니다.
- 2 `/etc/default/grub` 파일에서 `GRUB_HIDDEN_TIMEOUT` 매개 변수의 값을 변경합니다.
`GRUB_HIDDEN_TIMEOUT=2`
- 3 (선택 사항) `/etc/grub.d/40_custom` 파일에서 GRUB 암호를 변경합니다.
기본 암호는 `VMware1`입니다.
- 4 GRUB 구성을 업데이트합니다.
`update-grub`

새로 생성된 NSX Manager에 로그인

NSX Manager를 설치한 후 사용자 인터페이스를 사용하여 기타 설치 작업을 수행할 수 있습니다.

NSX Manager를 설치한 후 NSX-T Data Center에 대한 CEIP(고객 환경 향상 프로그램)에 참여할 수 있습니다. 프로그램의 참여 또는 해지 방법을 비롯하여 이 프로그램에 대한 자세한 내용은 "NSX-T Data Center 관리 가이드"의 고객 환경 향상 프로그램을 참조하십시오.

사전 요구 사항

NSX Manager가 설치되어 있는지 확인합니다. [NSX Manager 및 사용 가능한 장치 설치](#)의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
EULA가 표시됩니다.
- 2 EULA 약관을 읽고 동의합니다.
- 3 VMware의 CEIP(고객 환경 향상 프로그램)에 참여할지 여부를 선택합니다.
- 4 **저장**을 클릭합니다

계산 관리자 추가

예를 들어 vCenter Server와 같은 계산 관리자는 호스트 및 VM과 같은 리소스를 관리하는 애플리케이션입니다.

NSX-T Data Center는 vCenter Server에서 클러스터 정보를 수집하도록 계산 관리자를 폴링합니다.

vCenter Server 계산 관리자를 추가할 때는 vCenter Server 사용자의 자격 증명을 제공해야 합니다.

vCenter Server 관리자의 자격 증명을 제공하거나, NSX-T Data Center용의 역할 및 사용자를 생성하고 사용자의 자격 증명을 제공할 수 있습니다. 이 역할에는 다음 vCenter Server 권한이 있어야 합니다.

Extension.Register extension
Extension.Unregister extension
Extension.Update extension
Sessions.Message
Sessions.Validate session
Sessions.View and stop sessions
Host.Configuration.Maintenance
Host.Local Operations.Create virtual machine
Host.Local Operations.Delete virtual machine
Host.Local Operations.Reconfigure virtual machine
Host.Configuration.NetworkConfiguration
Tasks
Scheduled task
Global.Cancel task
Permissions.Reassign role permissions
Resource.Assign vApp to resource pool
Resource.Assign virtual machine to resource pool
Virtual Machine.Configuration
Virtual Machine.Guest Operations
Virtual Machine.Provisioning
Virtual Machine.Inventory
Network.Assign network
vApp

vCenter Server 역할 및 권한에 대한 자세한 내용은 "vSphere 보안" 문서를 참조하십시오.

사전 요구 사항

- 지원되는 vSphere 버전을 사용 중인지 확인합니다. [지원되는 vSphere 버전](#)을 참조하십시오.
- vCenter Server와의 IPv6 및 IPv4 통신.
- 권장되는 수의 계산 관리자를 사용 중인지 확인합니다. <https://configmax.vmware.com/home>의 내용을 참조하십시오.

참고 NSX-T Data Center는 둘 이상의 NSX Manager에 등록된 동일한 vCenter Server를 지원하지 않습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.

2 시스템 > 패브릭 > 계산 관리자 > 추가를 선택합니다.

3 계산 관리자 세부 정보를 완료합니다.

옵션	설명
이름 및 설명	vCenter Server를 식별하는 이름을 입력합니다. 선택적으로 vCenter Server의 클러스터 수와 같은 특별한 세부 사항을 설명할 수 있습니다.
도메인 이름/IP 주소	vCenter Server의 IP 주소를 입력합니다.
유형	기본 옵션을 그대로 둡니다.
사용자 이름 및 암호	vCenter Server 로그인 자격 증명을 입력합니다.
지문	vCenter Server SHA-256 지문 알고리즘 값을 입력합니다.

지문 값을 비워 두면 서버에서 제공한 지문을 수락할지 묻는 메시지가 나타납니다.

해당 지문을 수락하면 NSX-T Data Center에서 vCenter Server 리소스를 찾아 등록하는 데 몇 초 정도 소요됩니다.

4 진행률 아이콘이 **진행 중**에서 **등록되지 않음**으로 변경되면 다음 단계를 수행하여 오류를 해결합니다.

a 오류 메시지를 선택하고 **해결**을 클릭합니다. 가능한 오류 메시지 중 하나는 다음과 같습니다.

Extension already registered at CM <vCenter Server name> with id <extension ID>

b vCenter Server 자격 증명을 입력하고 **해결**을 클릭합니다.

기존 등록이 있으면 교체됩니다.

결과

계산 관리자를 vCenter Server에 등록하고 연결 상태가 실행 중으로 나타나려면 다소 시간이 걸립니다.

계산 관리자 이름을 클릭하여 세부 정보를 보거나, 계산 관리자를 편집하거나, 계산 관리자에게 적용되는 태그를 관리할 수도 있습니다.

vCenter Server가 성공적으로 등록되면 먼저 계산 관리자를 삭제하지 않고 NSX Manager VM의 전원을 끄지 말고 삭제하지도 마십시오. 그러지 않으면 새 NSX Manager를 배포할 때 동일한 vCenter Server를 다시 등록할 수 없게 됩니다. vCenter Server가 다른 NSX Manager에 이미 등록되었다는 오류가 발생합니다.

참고 VC(vCenter Server) 계산 관리자가 성공적으로 추가된 후에 다음 작업 중 하나를 완료했으면 제거할 수 없습니다.

- NSX 서비스 삽입을 사용하여 호스트 또는 VC의 클러스터에 배포된 서비스 VM입니다.
- NSX Manager UI를 사용하여 VC의 클러스터나 호스트에 NSX Edge, NSX Intelligence VM 또는 NSX Manager 노드를 배포합니다.

이러한 작업을 수행하려고 할 때 오류가 발생하는 경우(예: 설치 실패) 위에 나열된 작업을 성공적으로 수행하지 못했다면 VC를 제거해도 됩니다.

다음 이후에 VC를 제거할 수도 있습니다.

- 모든 전송 노드의 준비가 취소되었습니다.
- 모든 서비스 VM, NSX Intelligence VM, 모든 NSX Edge VM 및 NSX Manager 노드의 배포를 취소했습니다.

이 제한은 NSX-T Data Center 2.5.x의 새로 설치 및 업그레이드에 적용됩니다.

UI에서 클러스터를 구성하기 위해 NSX Manager 노드 배포

고가용성과 안정성을 제공하기 위해 여러 개의 NSX Manager 노드를 배포할 수 있습니다.

새 노드가 배포되면 이러한 노드가 NSX Manager 노드에 연결되어 클러스터를 구성합니다. 클러스터링된 NSX Manager 노드의 권장 개수는 3개입니다.

참고 UI를 사용한 여러 개의 NSX Manager 노드 배포는 vCenter Server에서 관리하는 ESXi 호스트에서만 지원됩니다.

처음 배포된 NSX Manager 노드의 모든 저장소 세부 정보 및 암호는 클러스터에 새로 배포된 노드와 동기화됩니다.

사전 요구 사항

- NSX Manager 노드가 설치되었는지 확인합니다. [NSX Manager 및 사용 가능한 장치 설치](#) 항목을 참조하십시오.
- 계산 관리자가 구성되어 있는지 확인합니다. [계산 관리자 추가](#) 항목을 참조하십시오.
- 시스템 요구 사항이 충족되었는지 확인합니다. [시스템 요구 사항](#)의 내용을 참조하십시오.
- 필수 포트가 열려 있는지 확인합니다. [포트 및 프로토콜](#)의 내용을 참조하십시오.
- 데이터스토어가 구성되었고 ESXi 호스트에서 액세스할 수 있는지 확인합니다.

- NSX Manager에서 사용할 IP 주소와 게이트웨이, DNS 서버 IP 주소, 도메인 검색 목록 및 NTP 서버 IP 주소가 있는지 확인합니다.
- 대상 VM 포트 그룹 네트워크가 아직 없으면 생성합니다. NSX-T Data Center 장치를 관리 VM 네트워크에 배치합니다.

여러 관리 네트워크가 있으면 NSX-T Data Center 장치에서 다른 네트워크로의 정적 경로를 추가할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 장치 > 개요 > 노드 추가**를 선택합니다.
- 3 NSX Manager 일반 특성 세부 정보를 입력합니다.

옵션	설명
계산 관리자	등록된 리소스 계산 관리자가 채워집니다.
SSH 사용	버튼을 전환하여 새 NSX Manager 노드에 대한 SSH 로그인을 허용합니다.
루트 액세스 사용	버튼을 전환하여 새 NSX Manager 노드에 대한 루트 액세스를 허용합니다.

옵션	설명
CLI 사용자 이름 및 암호 확인	<p>새 노드에 대한 CLI 암호 및 암호 확인을 설정합니다.</p> <p>암호는 암호 강도 제한을 준수해야 합니다.</p> <ul style="list-style-type: none"> ■ 12자 이상 ■ 하나 이상의 소문자 ■ 하나 이상의 대문자 ■ 하나 이상의 숫자 ■ 하나 이상의 특수 문자 ■ 5개 이상의 다른 문자 ■ 기본 암호 복잡성 규칙은 다음 Linux PAM 모듈 인수에 의해 적용됩니다. <ul style="list-style-type: none"> ■ retry=3: 오류 결과를 반환하기 전에 새 암호를 입력할 수 있는 최대 횟수로, 이 인수의 경우 최대 3번입니다. ■ minlen=12: 새 암호에 허용되는 최소 크기입니다. 새 암호의 문자 수 외에도 다른 종류의 문자(예: 대문자, 소문자 및 숫자)에 대해 크레딧(길이에서 +1)이 지정됩니다. ■ difok=0: 새 암호에서 달라야 하는 최소 바이트 수입니다. 이전 암호와 새 암호 간 유사성을 나타냅니다. difok에 값 0을 할당하면 이전 암호 및 새 암호 바이트를 다르게 유지할 필요가 없습니다. 정확한 일치만 허용됩니다. ■ lcredit=1: 새 암호에서 소문자에 대한 최대 크레딧입니다. 1개 이하의 소문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다. ■ ucredit=1: 새 암호에서 대문자에 대한 최대 크레딧입니다. 1개 이하의 대문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다. ■ dcredit=1: 새 암호에서 숫자에 대한 최대 크레딧입니다. 1개 이하의 숫자가 있는 경우 각 숫자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다. ■ ocredit=1: 새 암호에서 다른 문자에 대한 최대 크레딧입니다. 1개 이하의 다른 문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다. ■ enforce_for_root: 암호가 루트 사용자에게 대해 설정됩니다. <p>참고 사전 단어를 기준으로 암호를 확인하기 위한 Linux PAM 모듈에 대한 자세한 내용은 설명서 페이지를 참조하십시오.</p> <p>예를 들어 VMware123!123 또는 VMware12345와 같이 간단하고 규칙적인 암호는 사용하지 마십시오. 복잡성 표준을 충족하는 암호는 간단하고 체계적이지 않지만 문자, 알파벳, 특수 문자 및 숫자 조합(예: VMware123!45, VMware1!2345 또는 VMware@1az23x)입니다.</p> <p>CLI 사용자 이름은 이미 admin으로 설정되어 있습니다.</p>

옵션	설명
루트 암호 및 암호 확인	<p>새 노드에 대한 루트 암호 및 암호 확인을 설정합니다.</p> <p>암호는 암호 강도 제한을 준수해야 합니다.</p> <ul style="list-style-type: none"> ■ 12자 이상 ■ 하나 이상의 소문자 ■ 하나 이상의 대문자 ■ 하나 이상의 숫자 ■ 하나 이상의 특수 문자 ■ 5개 이상의 다른 문자 ■ 기본 암호 복잡성 규칙은 다음 Linux PAM 모듈 인수에 의해 적용됩니다. <ul style="list-style-type: none"> ■ retry=3: 오류 결과를 반환하기 전에 새 암호를 입력할 수 있는 최대 횟수로, 이 인수의 경우 최대 3번입니다. ■ minlen=12: 새 암호에 허용되는 최소 크기입니다. 새 암호의 문자 수 외에도 다른 종류의 문자(예: 대문자, 소문자 및 숫자)에 대해 크레딧(길이에서 +1)이 지정됩니다. ■ difok=0: 새 암호에서 달라야 하는 최소 바이트 수입니다. 이전 암호와 새 암호 간 유사성을 나타냅니다. difok에 값 0을 할당하면 이전 암호 및 새 암호 바이트를 다르게 유지할 필요가 없습니다. 정확한 일치만 허용됩니다. ■ lcredit=1: 새 암호에서 소문자에 대한 최대 크레딧입니다. 1개 이하의 소문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다. ■ ucredit=1: 새 암호에서 대문자에 대한 최대 크레딧입니다. 1개 이하의 대문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다. ■ dcredit=1: 새 암호에서 숫자에 대한 최대 크레딧입니다. 1개 이하의 숫자가 있는 경우 각 숫자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다. ■ ocredit=1: 새 암호에서 다른 문자에 대한 최대 크레딧입니다. 1개 이하의 다른 문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다. ■ enforce_for_root: 암호가 루트 사용자에게 대해 설정됩니다. <p>참고 사전 단어를 기준으로 암호를 확인하기 위한 Linux PAM 모듈에 대한 자세한 내용은 설명서 페이지를 참조하십시오.</p> <p>예를 들어 VMware123!123 또는 VMware12345와 같이 간단하고 규칙적인 암호는 사용하지 마십시오. 복잡성 표준을 충족하는 암호는 간단하고 체계적이지 않지만 문자, 알파벳, 특수 문자 및 숫자 조합(예: VMware123!45, VMware1!2345 또는 VMware@1az23x)입니다.</p>
DNS 서버	vCenter Server에서 사용할 수 있는 DNS 서버 IP 주소를 입력합니다.
NTP 서버	NTP 서버 IP 주소를 입력합니다.

4 NSX Manager 노드 세부 정보를 입력합니다.

옵션	설명
이름	NSX Manager 노드의 이름을 입력합니다.
클러스터	드롭다운 메뉴에서 노드가 연결될 클러스터를 지정합니다.
리소스 풀 또는 호스트	드롭다운 메뉴에서 노드에 대해 리소스 풀 또는 호스트를 할당합니다.

옵션	설명
데이터스토어	드롭다운 메뉴에서 노드 파일에 대한 데이터스토어를 선택합니다.
네트워크	드롭다운 메뉴에서 네트워크를 할당합니다.
관리 IP/넷마스크	IP 주소 및 넷마스크를 입력합니다.
관리 게이트웨이	게이트웨이 IP 주소를 입력합니다.

- 5 (선택 사항) 새 노드를 클릭하고 다른 노드를 구성합니다.

3-4단계를 반복합니다.

- 6 완료를 클릭합니다.

새 노드가 배포됩니다. 시스템 > 장치 > 개요 페이지 또는 vCenter Server에서 배포 프로세스를 추적할 수 있습니다.

- 7 배포, 클러스터 구성 및 저장소 동기화가 완료될 때까지 10-15분 동안 기다립니다.

처음 배포된 NSX Manager 노드의 모든 저장소 세부 정보 및 암호는 클러스터에 새로 배포된 노드와 동기화됩니다.

참고 새 노드의 배포가 진행 중일 때 첫 번째 노드가 재부팅되면 새 노드가 클러스터에 등록되지 않고 새 노드의 축소 이미지에 등록하지 못함 메시지가 표시됩니다. 클러스터에 노드를 수동으로 다시 배포하려면 새 노드의 축소 이미지로 이동하여 새로 줄임표를 선택하고 **다시 시도**를 클릭합니다.

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

- 9 `get services` 명령을 입력하여 모든 기본 서비스가 실행되고 있는지 확인합니다.

다음 서비스는 기본적으로 필요하지 않으며 자동으로 시작되지 않습니다.

- `liagent`

- `migration-coordinator`: 이 서비스는 마이그레이션 조정자를 실행하는 경우에만 사용됩니다. 이 서비스를 시작하기 전에 "NSX-T Data Center 마이그레이션 조정기 가이드"를 참조하십시오.

- `snmp`: SNMP 시작에 대한 자세한 내용은 "NSX-T Data Center 관리 가이드"에서 "Simple Network Management Protocol"을 참조하십시오.

- `nsx-message-bus`: 이 서비스는 NSX-T Data Center 3.0에서 사용되지 않습니다.

- 10 처음 배포된 NSX Manager 노드에 로그인하고 `get cluster status` 명령을 입력하여 노드가 클러스터에 추가되었는지 확인합니다.

- 11 NSX Manager 또는 글로벌 관리자 노드에 필요한 연결이 있는지 확인합니다.

다음 작업을 수행할 수 있는지 확인하십시오.

- 다른 시스템에서 노드를 Ping합니다.
- 노드에서 기본 게이트웨이를 Ping할 수 있습니다.

- 노드에서 관리 인터페이스를 사용하여 동일한 네트워크에 있는 하이퍼바이저 호스트를 Ping할 수 있습니다.
- 노드에서 DNS 서버와 NTP 서버를 Ping할 수 있습니다.
- SSH를 사용하도록 설정한 경우 노드에 대해 SSH를 수행할 수 있는지 확인합니다.

연결이 설정되지 않은 경우 가상 장치의 네트워크 어댑터가 적절한 네트워크 또는 VLAN에 있는지 확인합니다.

다음에 수행할 작업

NSX Edge를 구성합니다. [vSphere GUI를 사용하여 ESXi에 NSX Edge 설치](#) 항목을 참조하십시오.

CLI를 사용하여 클러스터를 구성하기 위해 NSX Manager 노드 배포

CLI를 사용하여 클러스터를 구성하기 위해 NSX Manager를 연결하면 클러스터의 모든 NSX Manager 노드가 서로 통신할 수 있습니다.

사전 요구 사항

NSX-T Data Center 구성 요소 설치가 완료되어야 합니다.

절차

- 1 처음 배포된 NSX Manager 노드에 대해 SSH 세션을 엽니다.
- 2 관리자 자격 증명으로 로그인합니다.
- 3 NSX Manager 노드에서 `get certificate api thumbprint` 명령을 실행합니다.
명령 출력은 이 NSX Manager에 고유한 숫자열입니다.
- 4 `get cluster config` 명령을 실행하여 처음 배포된 NSX Manager 클러스터 ID를 가져옵니다.
- 5 NSX Manager 노드를 클러스터에 추가합니다.

참고 새로 배포된 NSX Manager 노드에서 `join` 명령을 실행해야 합니다.

다음 NSX Manager 정보를 제공합니다.

- 연결하려는 노드의 호스트 이름 또는 IP 주소
- 클러스터 ID
- 사용자 이름
- 암호
- 인증서 지문

CLI 명령 또는 API 호출을 사용할 수 있습니다.

■ CLI 명령

```
host> join <NSX-Manager-IP> cluster-id <cluster-id> username <NSX-Manager-username> password
<NSX-Manager-password> thumbprint <NSX-Manager-thumbprint>
```

■ API 호출 POST https://<nsx-mgr>/api/v1/cluster?action=join_cluster

연결 및 클러스터 안정화 프로세스에는 10-15분이 걸릴 수 있습니다.

6 세 번째 NSX Manager 노드를 클러스터에 추가합니다.

5단계를 반복합니다.

7 호스트에서 `get cluster status` 명령을 실행하여 클러스터 상태를 확인합니다.

8 (NSX Manager UI) **시스템 > 장치 > 개요**를 선택하고 클러스터 연결을 확인합니다.

다음에 수행할 작업

전송 영역을 생성합니다. [독립형 호스트 또는 베어메탈 서비스 전송 노드 생성](#)의 내용을 참조하십시오.

클러스터에 대해 VIP(가상 IP) 주소 구성

NSX Manager 노드에 내결함성 및 고가용성을 제공하려면 NSX-T 클러스터의 멤버에 VIP(가상 IP) 주소를 할당하십시오.

클러스터의 NSX Manager는 서비스 API 및 UI 요청을 처리하기 위해 HTTPS 그룹에 속하게 됩니다. 클러스터의 리더 노드는 API 및 UI 요청을 처리하기 위해 클러스터의 집합 VIP에 대한 소유권을 갖게 됩니다. 클라이언트에서 들어오는 모든 API 및 UI 요청은 리더 노드로 전송됩니다.

참고 가상 IP를 할당할 때 클러스터의 모든 NSX Manager VM을 동일한 서브넷에서 구성해야 합니다.

VIP를 소유하는 리더 노드를 사용할 수 없게 되면 NSX-T는 새 리더를 선택합니다. 새 리더는 VIP를 소유합니다. 새 리더는 무상 ARP 패킷을 전송하고 새 VIP를 MAC 주소 매핑에 보급합니다. 새 리더 노드가 선택되면 새로운 API 및 UI 요청이 새 리더 노드로 전송됩니다.

클러스터의 새 리더 노드로의 VIP 페일오버가 수행되는 데 몇 분 정도 걸릴 수 있습니다. 이전 리더 노드가 사용할 수 없게 되어 VIP가 새 리더 노드로 페일오버될 경우 API 요청이 새 리더 노드로 전달되도록 자격 증명을 다시 인증합니다.

참고 VIP는 로드 밸런서로 작동하도록 설계되지 않았기 때문에 **시스템 > 사용자 > 구성**에서 **vIDM 외부 로드 밸런서 통합**을 사용하도록 설정한 경우에는 사용할 수 없습니다. vIDM에서 외부 로드 밸런서를 사용하려는 경우 VIP를 설정하지 마십시오. 자세한 내용은 "NSX-T Data Center 관리 가이드"에서 [VMware Identity Manager 통합 구성 구성](#)을 참조하십시오.

절차

1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.

- 2 시스템 > 개요로 이동합니다.
- 3 [가상 IP] 필드에서 **편집**을 클릭합니다.
- 4 클러스터의 VIP를 입력합니다. VIP가 다른 관리 노드와 동일한 서브넷에 속해 있는지 확인합니다.
- 5 **저장**을 클릭합니다.
- 6 HTTPS 그룹의 클러스터 상태 및 API 리더를 확인하려면 NSX Manager 콘솔 또는 SSH를 통해 NSX ManagerCLI 명령 `get cluster status verbose`을 입력합니다.

다음은 리더가 짧게 표시된 출력의 예입니다.

Group Type: HTTPS		
Group Status: STABLE		
Members:		
UUID	FQDN	IP
STATUS		
cdb93642-ccba-fdf4-8819-90bf018cd727	nsx-manager	192.196.197.84
UP		
51a13642-929b-8dfc-3455-109e6cc2a7ae	nsx-manager	192.196.198.156
UP		
d0de3642-d03f-c909-9cca-312fd22e486b	nsx-manager	192.196.198.54
UP		
Leaders:		
SERVICE	LEADER	LEASE
VERSION		
api	cdb93642-ccba-fdf4-8819-90bf018cd727	8

- 7 VIP 문제를 해결하려면 NSX Manager CLI에서 `/var/log/proxy/reverse-proxy.log`의 역방향 프록시 로그를 확인하고, `/var/log/cbm/cbm.log`의 클러스터 관리자 로그를 확인하십시오.

결과

NSX-T에 대한 모든 API 요청이 리더 노드가 소유하는 클러스터의 가상 IP 주소로 리디렉션됩니다. 그런 다음, 리더 노드는 요청을 장치의 다른 구성 요소로 전달합니다.

NSX-T 장치에서 스냅샷 사용 안 함

VM으로서 NSX Manager 및 NSX Edge를 스냅샷 생성 및 저장하도록 구성할 수 있습니다. 그러나 NSX-T 장치의 복제 및 스냅샷은 지원되지 않으며 기능 문제 및 알려지지 않은 다른 문제가 발생할 수 있습니다. 따라서 NSX-T 장치 VM의 스냅샷을 사용하지 않도록 설정하는 것이 좋습니다.

각 NSX-T 장치 VM에서 다음 절차를 수행합니다.

절차

- 1 vSphere Client에서 장치 VM 찾습니다.
- 2 VM의 전원을 끕니다.

- 3 VM을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 4 **VM 옵션** 탭을 클릭한 다음 **고급**을 확장합니다.
- 5 **구성 매개 변수** 필드에서 **구성 편집...**을 클릭합니다.
- 6 **구성 매개 변수** 창에서 **구성 매개 변수 추가**를 클릭합니다.
- 7 다음을 입력합니다.
 - 이름으로 **snapshot.MaxSnapshots**를 입력합니다.
 - 값으로 **-0**을 입력합니다.
- 8 **확인**을 클릭하여 변경 내용을 저장합니다.
- 9 VM의 전원을 다시 켭니다.

KVM에 NSX-T Data Center 설치

6

NSX-T Data Center는 두 가지 방식, 즉 호스트 전송 노드 및 NSX Manager에 대한 호스트로 KVM을 지원합니다.

지원되는 KVM 버전을 사용 중인지 확인해야 합니다. [NSX Manager VM 및 호스트 전송 노드 시스템 요구 사항](#)의 내용을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [KVM 설정](#)
- [KVM CLI에서 게스트 VM 관리](#)
- [KVM에 NSX Manager 설치](#)
- [새로 생성된 NSX Manager에 로그인](#)
- [KVM 호스트에 타사 패키지 설치](#)
- [RHEL KVM 호스트의 Open vSwitch 버전 확인](#)
- [SUSE KVM 호스트의 Open vSwitch 버전 확인](#)
- [CLI를 사용하여 클러스터를 구성하기 위해 NSX Manager 노드 배포](#)

KVM 설정

KVM을 전송 노드 또는 NSX Manager 게스트 VM에 대한 호스트로 사용하려고 하지만 KVM을 아직 설정하지 않은 경우 여기에 설명된 절차를 사용할 수 있습니다.

참고 Geneve 캡슐화 프로토콜은 UDP 포트 6081을 사용합니다. KVM 호스트의 방화벽에서 이 포트 액세스를 허용해야 합니다.

절차

- 1 (RHEL에만 해당) `/etc/yum.conf` 파일을 엽니다.
- 2 `exclude` 줄을 검색합니다.

- 3 "kernel* redhat-release*" 줄을 추가하여 지원되지 않는 RHEL 업그레이드를 피하도록 YUM을 구성합니다.

```
exclude=[existing list] kernel* redhat-release*
```

특정 호환성 요구 사항이 있는 NSX-T Data Center Container Plug-in을 실행하려는 경우 컨테이너 관련 모듈도 제외시킵니다.

```
exclude=[existing list] kernel* redhat-release* kubelet-* kubeadm-* kubectl-* docker-*
```

지원되는 RHEL 버전은 7.4 및 7.5입니다.

- 4 KVM 및 브리지 유틸리티를 설치합니다.

Linux 배포판	명령
Ubuntu	<pre>apt-get install -y qemu-kvm libvirt-bin ubuntu-vm-builder bridge-utils virtinst virt-manager virt-viewer libguestfs-tools</pre>
RHEL 또는 CentOS Linux	<pre>yum groupinstall "Virtualization Hypervisor" yum groupinstall "Virtualization Client" yum groupinstall "Virtualization Platform" yum groupinstall "Virtualization Tools"</pre>
SUSE Linux Enterprise Server	YaSt를 시작하고 가상화 > 하이퍼바이저 및 도구 설치 를 선택합니다. YaSt를 사용하면 네트워크 브리지를 자동으로 사용하도록 설정하고 구성할 수 있습니다.

- 5 NSX Manager가 KVM 호스트에 NSX 소프트웨어 패키지를 자동으로 설치하려면 업링크/데이터 인터페이스의 네트워크 구성을 준비합니다.

KVM 호스트에는 여러 네트워크 인터페이스가 있을 수 있습니다. NSX-T 용도의 업링크 인터페이스(데이터 인터페이스)로 제공할 네트워크 인터페이스의 경우, 네트워크 구성 파일을 올바르게 채우는 것이 중요합니다. NSX-T는 이러한 네트워크 구성 파일을 확인하여 NSX-T 특정 네트워크 디바이스를 생성합니다. Ubuntu에서 `/etc/network/interfaces` 파일을 채웁니다. RHEL, CentOS 또는 SUSE에서 `/etc/sysconfig/network-scripts/ifcfg-$uplinkdevice` 파일을 채웁니다.

다음 예제에서 "ens32" 인터페이스는 업링크 디바이스(데이터 인터페이스)입니다. 배포 환경에 따라 이 인터페이스는 DHCP 또는 정적 IP 설정을 사용할 수 있습니다.

참고 인터페이스 이름은 환경에 따라 다를 수 있습니다.

중요 Ubuntu의 경우 모든 네트워크 구성을 `/etc/network/interfaces`에 지정해야 합니다. `/etc/network/ifcfg-eth1`과 같은 개별 네트워크 구성 파일은 생성하지 마십시오. 이 경우 전송 노드 생성이 실패할 수 있습니다.

Linux 배포판	네트워크 구성
Ubuntu	<p>/etc/network/interfaces를 편집합니다.</p> <pre> auto eth0 iface eth0 inet manual auto ens32 iface ens32 inet manual </pre>
RHEL 또는 CentOS Linux	<p>/etc/sysconfig/network-scripts/ifcfg-ens32를 편집합니다.</p> <pre> DEVICE="ens32" TYPE="Ethernet" NAME="ens32" UUID="<something>" BOOTPROTO="none" HWADDR="<something>" ONBOOT="yes" NM_CONTROLLED="no" </pre>
SUSE Linux Enterprise Server	<p>SLES 호스트가 이미 있는 경우 데이터 인터페이스가 호스트에 이미 구성되어 있는지 확인합니다. 미리 구성된 SLES 호스트가 없는 경우 관리 및 데이터 인터페이스에 대한 참조 구성을 참조하십시오. 다음과 같이 /etc/sysconfig/network/ifcfg-ens32를 편집합니다.</p> <pre> DEVICE="ens32" NAME="ens32" UUID="<UUID>" BOOTPROTO="none" LLADDR="<HWADDR>" STARTMODE="yes" </pre>

- 6 네트워크 서비스를 다시 시작하거나(systemctl restart network) 네트워크 변경 사항이 적용되도록 Linux 서버를 재부팅합니다.
- 7 KVM 호스트가 전송 노드로 구성되면 NSX-T에서 브리지 인터페이스 'nsx-vtep0.0'을 자동으로 생성합니다.

Ubuntu에서 /etc/network/interfaces 파일에는 다음과 같은 항목이 포함됩니다.

```

iface nsx-vtep0.0 inet static
pre-up ip addr flush dev nsx-vtep0.0
address <IP_pool_address>
netmask <subnet_mask>
mtu 1600
down ifconfig nsx-vtep0.0 down
up ifconfig nsx-vtep0.0 up

```

RHEL에서 호스트 NSX 에이전트(nsxa)는 다음과 같은 항목을 포함하는 ifcfg-nsx-vtep0.0이라는 구성 파일을 생성합니다.

```

DEVICE=nsx-vtep0.0
BOOTPROTO=static
NETMASK=<IP address>
IPADDR=<subnet mask>

```

```
MTU=1600
ONBOOT=yes
USERCTL=no
NM_CONTROLLED=no
```

SUSE에서

```
DEVICE=nsx-vtep0.0
BOOTPROTO=static
NETMASK=255.255.255.0
IPADDR=192.168.13.119
MACADDR=ae:9d:b7:ca:20:4a
MTU=1600
USERCTL=no
STARTMODE=auto
```

- 8 syslog 순환 정책을 크기 기반 정책 대신 시간 기반으로 구성합니다. 크기 기반 syslog 순환 정책을 사용하면 생성된 로그 파일의 크기가 매우 클 수 있습니다.

KVM CLI에서 게스트 VM 관리

NSX Manager를 KVM VM으로 설치할 수 있습니다. 또한 KVM은 NSX-T Data Center 전송 노드에 대한 하이퍼바이저로 사용될 수 있습니다.

KVM 게스트 VM 관리는 이 가이드의 범위를 벗어납니다. 하지만 시작하는 데 도움이 되는 몇 가지 간단한 KVM CLI 명령이 다음에 나와 있습니다.

KVM CLI에서 게스트 VM을 관리하려면 **virsh** 명령을 사용합니다. 다음은 몇 가지 일반적인 **virsh** 명령입니다. 추가 정보는 KVM 설명서를 참조하십시오.

```
# List running
virsh list

# List all
virsh list --all

# Control instances
virsh start <instance>
virsh shutdown <instance>
virsh destroy <instance>
virsh undefine <instance>
virsh suspend <instance>
virsh resume <instance>

# Access an instance's CLI
virsh console <instance>
```


Linux CLI에서 `ifconfig` 명령을 실행하면 게스트 VM에 대해 생성된 인터페이스를 나타내는 `vnetX` 인터페이스를 보여줍니다. 추가 게스트 VM을 추가하는 경우 추가 `vnetX` 인터페이스도 추가됩니다.

```
ifconfig
...

vnet0    Link encap:Ethernet  HWaddr fe:54:00:b0:a0:6d
         inet6 addr: fe80::fc54:ff:feb0:a06d/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:13183 errors:0 dropped:0 overruns:0 frame:0
         TX packets:181524 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:500
         RX bytes:4984832 (4.9 MB)  TX bytes:29498709 (29.4 MB)
```

KVM에 NSX Manager 설치

NSX Manager는 KVM 호스트에 가상 장치로 설치될 수 있습니다.

QCOW2 설치 절차에서는 Linux 명령줄 도구인 `guestfish`를 사용하여 QCOW2 파일에 가상 시스템 설정을 기록합니다.

사전 요구 사항

- KVM 설정. [KVM 설정](#)의 내용을 참조하십시오.
- KVM 호스트에 QCOW2 이미지를 배포할 수 있는 권한.
- 설치 후 로그인할 수 있도록 `guestinfo`의 암호가 암호 복잡성 요구 사항을 준수하는지 확인합니다. [장 4 NSX Manager 설치](#)의 내용을 참조하십시오.
- NSX Manager 리소스 요구 사항을 숙지합니다. [NSX Manager VM 및 호스트 전송 노드 시스템 요구 사항](#) 항목을 참조하십시오.
- Ubuntu OS를 설치할 계획인 경우, KVM 호스트에 NSX Manager를 설치하기 전에 Ubuntu 버전 18.04를 설치하는 것이 좋습니다.

절차

- 1 **nsx-unified-appliance > exports > kvm** 폴더에서 NSX Manager QCOW2 이미지를 다운로드합니다.
- 2 SCP 또는 동기화를 사용하여 NSX Manager를 실행할 KVM 시스템으로 복사합니다.
- 3 (Ubuntu만 해당) 현재 로그인한 사용자를 `libvirtd` 사용자로 추가합니다.

```
adduser $USER libvirtd
```

4 QCOW2 이미지를 저장한 동일한 디렉토리에 guestinfo.xml이라는 파일을 만들고 NSX Manager VM의 속성으로 채웁니다.

속성	설명
<ul style="list-style-type: none"> ■ nsx_cli_passwd_0 ■ nsx_cli_audit_passwd_0 ■ nsx_passwd_0 	<p>암호는 암호 길이 제한을 준수해야 합니다.</p> <ul style="list-style-type: none"> ■ 12자 이상 ■ 하나 이상의 소문자 ■ 하나 이상의 대문자 ■ 하나 이상의 숫자 ■ 하나 이상의 특수 문자 ■ 5개 이상의 다른 문자 ■ 기본 암호 복잡성 규칙은 다음 Linux PAM 모듈 인수에 의해 적용됩니다. <ul style="list-style-type: none"> ■ retry=3: 오류 결과를 반환하기 전에 새 암호를 입력할 수 있는 최대 횟수로, 이 인수의 경우 최대 3번입니다. ■ minlen=12: 새 암호에 허용되는 최소 크기입니다. 새 암호의 문자 수 외에도 다른 종류의 문자(예: 대문자, 소문자 및 숫자)에 대해 크레딧(길이에서 +1)이 지정됩니다. ■ difok=0: 새 암호에서 달라야 하는 최소 바이트 수입니다. 이전 암호와 새 암호 간 유사성을 나타냅니다. difok에 값 0을 할당하면 이전 암호 및 새 암호 바이트를 다르게 유지할 필요가 없습니다. 정확한 일치만 허용됩니다. ■ lcredit=1: 새 암호에서 소문자에 대한 최대 크레딧입니다. 1개 이하의 소문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다. ■ ucredit=1: 새 암호에서 대문자에 대한 최대 크레딧입니다. 1개 이하의 대문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다. ■ dcredit=1: 새 암호에서 숫자에 대한 최대 크레딧입니다. 1개 이하의 숫자가 있는 경우 각 숫자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다. ■ ocredit=1: 새 암호에서 다른 문자에 대한 최대 크레딧입니다. 1개 이하의 다른 문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다. ■ enforce_for_root: 암호가 루트 사용자에게 대해 설정됩니다. <p>참고 사전 단어를 기준으로 암호를 확인하기 위한 Linux PAM 모듈에 대한 자세한 내용은 설명서 페이지를 참조하십시오.</p> <p>예를 들어 VMware123!123 또는 VMware12345와 같이 간단하고 규칙적인 암호는 사용하지 마십시오. 복잡성 표준을 충족하는 암호는 간단하고 체계적이지 않지만 문자, 알파벳, 특수 문자 및 숫자 조합(예: VMware123!45, VMware1!2345 또는 VMware@1az23x)입니다.</p>
nsx_hostname	NSX Manager의 호스트 이름을 입력합니다. 호스트 이름은 올바른 도메인 이름이어야 합니다. 점으로 구분된 호스트 이름(domain/subdomain)의 각 부분은 알파벳 문자로 시작해야 합니다.
nsx_role	<ul style="list-style-type: none"> ■ nsx-manager: 필수. 이 role-name은 NSX Manager 장치를 설치합니다. ■ nsx-cloud-service-manager: 선택 사항. NSX Manager를 설치한 후 이 역할 이름을 사용하여 NSX Cloud에 대한 Cloud Service Manager 장치를 설치합니다.

속성	설명
nsx_isSSHEnabled	이 속성을 사용하거나 사용하지 않도록 설정할 수 있습니다. 사용하도록 설정한 경우 SSH를 사용하여 NSX Manager에 로그인할 수 있습니다.
nsx_allowSSHRootLogin	이 속성을 사용하거나 사용하지 않도록 설정할 수 있습니다. 사용하도록 설정한 경우 SSH를 사용하여 루트 사용자 권한으로 NSX Manager에 로그인할 수 있습니다. 이 속성을 사용할 수 있으려면 nsx_isSSHEnabled 를 사용하도록 설정해야 합니다.
<ul style="list-style-type: none"> ■ nsx_dns1_0 ■ nsx_ntp_0 ■ nsx_domain_0 ■ nsx_gateway_0 ■ nsx_netmask_0 ■ nsx_ip_0 	기본 게이트웨이, 관리 네트워크 IPv4, 관리 네트워크 넷마스크, DNS 및 NTP IP 주소에 대한 IP 주소를 입력합니다.

예:

```
<?xml version="1.0" encoding="UTF-8"?>
<Environment
  xmlns="http://schemas.dmtf.org/ovf/environment/1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:oe="http://schemas.dmtf.org/ovf/environment/1">
  <PropertySection>
    <Property oe:key="nsx_cli_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_cli_audit_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_hostname" oe:value="nsx-manager1"/>
    <Property oe:key="nsx_role" oe:value="nsx-manager"/>
    <Property oe:key="nsx_isSSHEnabled" oe:value="True"/>
    <Property oe:key="nsx_allowSSHRootLogin" oe:value="True"/>
    <Property oe:key="nsx_dns1_0" oe:value="10.168.110.10"/>
    <Property oe:key="nsx_ntp_0" oe:value="10.168.110.10"/>
    <Property oe:key="nsx_domain_0" oe:value="corp.local"/>
    <Property oe:key="nsx_gateway_0" oe:value="10.168.110.83"/>
    <Property oe:key="nsx_netmask_0" oe:value="255.255.252.0"/>
    <Property oe:key="nsx_ip_0" oe:value="10.168.110.19"/>
  </PropertySection>
</Environment>
```

참고 이 예에서 **nsx_isSSHEnabled** 및 **nsx_allowSSHRootLogin**은 둘 다 사용되도록 설정됩니다. 사용되지 않도록 설정되면 SSH를 실행하거나 NSX Manager 명령줄에 로그인할 수 없습니다.

nsx_isSSHEnabled는 사용하도록 설정하고 **nsx_allowSSHRootLogin**은 사용하지 않도록 설정하면 NSX Manager에 대해 SSH를 실행할 수 있으나 루트 권한으로 로그인할 수 없습니다.

- 5 guestfish를 사용하여 QCOW2 이미지에 `guestinfo.xml` 파일을 기록합니다.

참고 `guestinfo` 정보가 QCOW2 이미지에 기록되면 정보를 덮어쓸 수 없습니다.

```
sudo guestfish --rw -i -a nsx-unified-appliance-<BuildNumber>.qcow2 upload guestinfo /config/
guestinfo
```

- 6 `virt-install` 명령을 사용하여 QCOW2 이미지를 배포합니다.

vCPU 및 RAM 값은 대규모 VM에 적합합니다. 네트워크 이름 및 포트 그룹 이름은 사용자 환경에 따라 다릅니다. 모델은 `virtio`여야 합니다.

```
sudo virt-install \
--import \
--ram 48000 \
--vcpus 12 \
--name <manager-name> \
--disk path=<manager-qcow2-file-path>,bus=virtio,cache=none \
--network network=<network-name>,portgroup=<portgroup-name>,model=virtio \
--noautoconsole \
--cpu mode=host-passthrough,cache.mode=passthrough

Starting install...
Domain installation still in progress. Waiting for installation to complete.
```

- 7 NSX Manager가 배포되었는지 확인합니다.

```
virsh list --all
```

Id	Name	State
18	nsx-manager1	running

- 8 NSX Manager 콘솔을 열고 로그인합니다.

```
virsh console 18
Connected to domain nsx-manager1
Escape character is ^]

nsx-manager1 login: admin
Password:
```

- 9 노드가 부팅되면 CLI에 관리자 권한으로 로그인하고 `get interface eth0` 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.
- 10 `get services` 명령을 실행하여 서비스가 실행되고 있는지 확인합니다.

11 NSX Manager 또는 글로벌 관리자 노드에 필요한 연결이 있는지 확인합니다.

다음 작업을 수행할 수 있는지 확인하십시오.

- 다른 시스템에서 노드를 Ping합니다.
- 노드에서 기본 게이트웨이를 Ping할 수 있습니다.
- 노드에서 관리 인터페이스를 사용하여 동일한 네트워크에 있는 하이퍼바이저 호스트를 Ping할 수 있습니다.
- 노드에서 DNS 서버와 NTP 서버를 Ping할 수 있습니다.
- SSH를 사용하도록 설정한 경우 노드에 대해 SSH를 수행할 수 있는지 확인합니다.

연결이 설정되지 않은 경우 가상 장치의 네트워크 어댑터가 적절한 네트워크 또는 VLAN에 있는지 확인합니다.

12 KVM 콘솔을 종료합니다.

`control-]`

13 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.

새로 생성된 NSX Manager에 로그인

NSX Manager를 설치한 후 사용자 인터페이스를 사용하여 기타 설치 작업을 수행할 수 있습니다.

NSX Manager를 설치한 후 NSX-T Data Center에 대한 CEIP(고객 환경 향상 프로그램)에 참여할 수 있습니다. 프로그램의 참여 또는 해지 방법을 비롯하여 이 프로그램에 대한 자세한 내용은 "NSX-T Data Center 관리 가이드"의 고객 환경 향상 프로그램을 참조하십시오.

사전 요구 사항

NSX Manager가 설치되어 있는지 확인합니다. [NSX Manager](#) 및 [사용 가능한 장치 설치](#)의 내용을 참조하십시오.

절차

1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.

EULA가 표시됩니다.

2 EULA 약관을 읽고 동의합니다.**3 VMware의 CEIP(고객 환경 향상 프로그램)에 참여할지 여부를 선택합니다.****4 저장**을 클릭합니다

KVM 호스트에 타사 패키지 설치

KVM 호스트를 패브릭 노드가 되도록 준비하려면 일부 타사 패키지를 설치해야 합니다.

사전 요구 사항

- (RHEL 및 CentOS Linux) 타사 패키지를 설치하기 전에 다음 명령을 실행하여 가상화 패키지를 설치합니다.

```
yum groupinstall "Virtualization Hypervisor"
yum groupinstall "Virtualization Client"
yum groupinstall "Virtualization Platform"
yum groupinstall "Virtualization Tools"
```

패키지를 설치할 수 없는 경우 새 설치에서 `yum install glibc.i686 nspr` 명령을 사용하여 수동으로 설치할 수 있습니다.

- (Ubuntu) 타사 패키지를 설치하기 전에 다음 명령을 실행하여 가상화 패키지를 설치합니다.

```
apt install -y \
qemu-kvm \
libvirt-bin \
virtinst \
virt-manager \
virt-viewer \
ubuntu-vm-builder \
bridge-utils
```

- (SUSE Linux Enterprise Server) 타사 패키지를 설치하기 전에 다음 명령을 실행하여 가상화 패키지를 설치합니다.

```
libcap-progs
```

절차

- ◆ Ubuntu 18.04.2 LTS에서는 `apt-get install <package_name>` 명령을 실행하여 다음 타사 패키지를 수동으로 설치합니다.

```
traceroute
python-mako
python-simplejson
python-unittest2
python-yaml
python-netaddr
dkms
libc6-dev
libelf-dev
```

- ◆ RHEL 및 CentOS Linux에서는 `yum install <package_name>` 명령을 실행하여 타사 패키지를 수동으로 설치합니다.

이미 RHEL 및 CentOS에 등록된 호스트를 수동으로 준비하는 경우에는 호스트에 타사 패키지를 설치하지 않아도 됩니다.

RHEL 7.6, 7.5 및 7.4 CentOS Linux 7.5 및 7.4

```
wget
PyYAML
libunwind
python-gevent
python-mako
python-netaddr
redhat-lsb-core
tcpdump
net-tools
```

```
wget
PyYAML
libunwind
python-gevent
python-mako
python-netaddr
redhat-lsb-core
tcpdump
```

- ◆ SUSE에서는 `zypper install <package_name>` 명령을 실행하여 타사 패키지를 수동으로 설치합니다.

SUSE Linux Enterprise Server 12.0

```
python-simplejson
python-PyYAML
python-netaddr
lsb-release
```

RHEL KVM 호스트의 Open vSwitch 버전 확인

RHEL 호스트에 OVS 패키지가 없는 경우 이 항목을 건너뛰십시오. OVS 패키지가 RHEL 호스트에 이미 있는 경우 기존 OVS 패키지를 제거하고 NSX-T 지원 OVS 패키지를 설치하거나 기존 OVS 패키지를 NSX-T 지원 패키지로 업그레이드해야 합니다.

지원되는 Open vSwitch 버전은 2.9.1.8614397-1입니다.

절차

- 1 현재 버전의 Open vSwitch가 호스트에 설치되어 있는지 확인합니다.

```
ovs-vsitchd --version
```

중요 기존 Open vSwitch 패키지가 최신 또는 이전 버전을 실행하는 경우 기존 Open vSwitch 패키지를 지원되는 버전으로 바꾸어야 합니다.

- 2 다음 Open vSwitch 패키지를 삭제합니다.

- `kmod-openvswitch` 또는 `openvswitch-kmod`
- `openvswitch`
- `openvswitch-selinux-policy`

3 또는 NSX-T Data Center에 필요한 Open vSwitch 패키지를 업그레이드합니다.

- a 관리자 권한으로 호스트에 로그인합니다.
- b nsx-lcp 파일을 다운로드한 후 /tmp 디렉토리로 복사합니다.
- c tar 패키지의 압축을 풉니다.

```
tar -zxvf nsx-lcp-<release>-rhel75_x86_64.tar.gz
```

- d 패키지 디렉토리로 이동합니다.

```
cd nsx-lcp-rhel75_x86_64/
```

- e 기존 Open vSwitch 버전을 지원되는 버전으로 교체합니다.

- 최신 Open vSwitch 버전의 경우 `--nodeps` 명령을 사용합니다.

```
rpm -Uvh openvswitch*.rpm --nodeps
```

- 이전 Open vSwitch 버전의 경우 `--force` 명령을 사용합니다.

```
rpm -Uvh openvswitch*.rpm --nodeps --force
```

SUSE KVM 호스트의 Open vSwitch 버전 확인

SUSE 호스트에 OVS 패키지가 없는 경우 이 항목을 건너뛰십시오. OVS 패키지가 SUSE 호스트에 있는 경우 기존 OVS 패키지를 제거하고 NSX-T 지원 OVS 패키지를 설치하거나 기존 OVS 패키지를 NSX-T 지원 패키지로 업그레이드해야 합니다.

지원되는 Open vSwitch 버전은 2.9.1.8614397-1입니다.

절차

- 1 현재 버전의 Open vSwitch가 호스트에 설치되어 있는지 확인합니다.

```
ovs-vswitchd --version
```

중요 기존 Open vSwitch 패키지가 최신 또는 이전 버전을 실행하는 경우 기존 Open vSwitch 패키지를 지원되는 버전으로 바꾸어야 합니다.

- 2 다음 Open vSwitch 패키지를 삭제합니다.

- kmod-openvswitch 또는 openvswitch-kmod
- openvswitch
- openvswitch-selinux-policy

- 3 또는 NSX-T Data Center에 필요한 Open vSwitch 패키지를 업그레이드합니다.

- a 관리자 권한으로 호스트에 로그인합니다.
- b nsx-lcp 파일을 다운로드한 후 /tmp 디렉토리로 복사합니다.

- c tar 패키지의 압축을 풉니다.

```
nsx-lcp-3.0.0.0.14335404-linux64-sles12sp3.tar.gz
```

- d 패키지 디렉토리로 이동합니다.

```
nsx-lcp-linux64-sles12sp3/
```

- e 기존 Open vSwitch 버전을 지원되는 버전으로 교체합니다.

- 최신 Open vSwitch 버전의 경우 `--nodeps` 명령을 사용합니다.

```
rpm -Uvh openvswitch*.rpm --nodeps
```

- 이전 Open vSwitch 버전의 경우 `--force` 명령을 사용합니다.

```
rpm -Uvh openvswitch*.rpm --nodeps --force
```

CLI를 사용하여 클러스터를 구성하기 위해 NSX Manager 노드 배포

CLI를 사용하여 클러스터를 구성하기 위해 NSX Manager를 연결하면 클러스터의 모든 NSX Manager 노드가 서로 통신할 수 있습니다.

사전 요구 사항

NSX-T Data Center 구성 요소 설치가 완료되어야 합니다.

절차

- 1 처음 배포된 NSX Manager 노드에 대해 SSH 세션을 엽니다.
- 2 관리자 자격 증명으로 로그인합니다.
- 3 NSX Manager 노드에서 `get certificate api thumbprint` 명령을 실행합니다.
명령 출력은 이 NSX Manager에 고유한 숫자열입니다.
- 4 `get cluster config` 명령을 실행하여 처음 배포된 NSX Manager 클러스터 ID를 가져옵니다.
- 5 NSX Manager 노드를 클러스터에 추가합니다.

참고 새로 배포된 NSX Manager 노드에서 `join` 명령을 실행해야 합니다.

다음 NSX Manager 정보를 제공합니다.

- 연결하려는 노드의 호스트 이름 또는 IP 주소
- 클러스터 ID
- 사용자 이름
- 암호
- 인증서 지문

CLI 명령 또는 API 호출을 사용할 수 있습니다.

■ CLI 명령

```
host> join <NSX-Manager-IP> cluster-id <cluster-id> username <NSX-Manager-username> password
<NSX-Manager-password> thumbprint <NSX-Manager-thumbprint>
```

■ API 호출 POST https://<nsx-mgr>/api/v1/cluster?action=join_cluster

연결 및 클러스터 안정화 프로세스에는 10-15분이 걸릴 수 있습니다.

6 세 번째 NSX Manager 노드를 클러스터에 추가합니다.

5단계를 반복합니다.

7 호스트에서 `get cluster status` 명령을 실행하여 클러스터 상태를 확인합니다.

8 (NSX Manager UI) **시스템 > 장치 > 개요**를 선택하고 클러스터 연결을 확인합니다.

다음에 수행할 작업

전송 영역을 생성합니다. 독립형 호스트 또는 베어메탈 서비스 전송 노드 생성의 내용을 참조하십시오.

NSX-T Data Center를 사용하도록 베어메탈 서버 구성

7

베어메탈 서버에서 NSX-T Data Center를 사용하려면 지원되는 타사 패키지를 설치해야 합니다.

NSX-T Data Center는 두 가지 방식, 즉 호스트 전송 노드 및 NSX Manager에 대한 호스트로 베어메탈 서버를 지원합니다.

지원되는 베어메탈 서버 버전을 사용 중인지 확인해야 합니다. [베어메탈 서버 시스템 요구 사항](#)의 내용을 참조하십시오.

참고 NSX Edge가 VM 폼 팩터에 있고 NSX DHCP 서비스(VLAN 기반 논리적 스위치에 배포됨)를 사용하려는 경우, NSX Edge가 배포된 베어메탈 호스트에서 위조 전송 옵션을 [수락]으로 설정해야 합니다. vSphere 제품 설명서에서 위조 전송을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [베어메탈 서버에 타사 패키지 설치](#)
- [베어메탈 서버 워크로드를 위한 애플리케이션 인터페이스 생성](#)

베어메탈 서버에 타사 패키지 설치

베어메탈 서버를 패브릭 노드가 되도록 준비하려면 타사 패키지를 설치해야 합니다.

사전 요구 사항

- 설치를 수행하는 사용자에게 다음 작업을 수행하기 위한 관리 권한이 있는지 확인합니다. 일부 사용자에게는 `sudo` 권한이 필요할 수도 있습니다.
 - 번들을 다운로드하고 압축 해제합니다.
 - NSX 구성 요소 설치/제거를 위한 `dpkg` 또는 `rpm` 명령을 실행합니다.
 - 관리부 연결 명령을 실행하기 위한 `nsxcli` 명령을 실행합니다.
- 가상화 패키지가 설치되어 있는지 확인합니다.
 - Redhat 또는 CentOS - `yum install libvirt-libs`
 - Ubuntu - `apt-get install libvirt0`
 - SUSE - `zypper install libvirt-libs`

절차

- ◆ Ubuntu의 경우 `apt-get install <package_name>`을 실행하여 타사 패키지를 설치합니다.

Ubuntu 18.04.2	Ubuntu 16.04
traceroute python-mako python-netaddr python-simplejson python-unittest2 python-yaml python-openssl dkms libvirt0 libelf-dev	libunwind8 libgflags2v5 libgoogle-perftools4 traceroute python-mako python-simplejson python-unittest2 python-yaml python-netaddr python-openssl libboost-filesystem1.58.0 libboost-chrono1.58.0 libgoogle-glog0v5 dkms libboost-date-time1.58.0 python-protobuf python-gevent libsnappy1v5 libleveldb1v5 libboost-program-options1.58.0 libboost-thread1.58.0 libboost-iostreams1.58.0 libvirt0 libelf-dev

- ◆ RHEL 또는 CentOS의 경우 `yum install`을 실행하여 타사 패키지를 설치합니다.

RHEL 7.4, 7.5 및 7.6	CentOS 7.4, 7.5 및 7.6
tcpdump boost-filesystem PyYAML boost-iostreams boost-chrono python-mako python-netaddr python-six gperftools-libs libunwind libelf-dev snappy boost-date-time c-ares redhat-lsb-core wget net-tools yum-utils lsof python-gevent libev python-greenlet libvirt-libs	tcpdump boost-filesystem PyYAML boost-iostreams boost-chrono python-mako python-netaddr python-six gperftools-libs libunwind libelf-dev snappy boost-date-time c-ares redhat-lsb-core wget net-tools yum-utils lsof python-gevent libev python-greenlet libvirt-libs

- ◆ SUSE에서는 `zypper install <package_name>` 명령을 실행하여 타사 패키지를 수동으로 설치합니다.

```
net-tools
tcpdump
python-simplejson
python-netaddr
python-PyYAML
python-six
libunwind
wget
lsof
libcap-progs
libvirt-libs
```

베어메탈 서버 워크로드를 위한 애플리케이션 인터페이스 생성

베어메탈 서버 워크로드를 위한 애플리케이션을 생성하거나 마이그레이션하려면 먼저 NSX-T Data Center를 구성하고 Linux 타사 패키지를 설치해야 합니다.

NSX-T Data Center는 Linux OS 인터페이스 결합을 지원하지 않습니다. 베어메탈 서버 전송 노드에 대해 OVS(Open vSwitch) 결합을 사용해야 합니다. 기술 자료 문서 [67835 베어메탈 서버에서 NSX-T의 전송 노드 구성에 대한 OVS 결합을 지원함](#)을 참조하십시오.

절차

- 1 필수타사 패키지를 설치합니다.

[베어메탈 서버에 타사 패키지 설치](#)의 내용을 참조하십시오.

- 2 TCP 및 UDP 포트를 구성합니다.

[ESXi, KVM 호스트 및 베어메탈 서버에서 사용하는 TCP 및 UDP 포트](#)의 내용을 참조하십시오.

- 3 베어메탈 서버를 NSX-T Data Center 패브릭에 추가하고 전송 노드를 생성합니다.

[독립형 호스트 또는 베어메탈 서비스 전송 노드 생성](#)의 내용을 참조하십시오.

- 4 Ansible 플레이북을 사용하여 애플리케이션 인터페이스를 생성합니다.

<https://github.com/vmware/bare-metal-server-integration-with-nsxt>의 내용을 참조하십시오.

NSX Manager 클러스터 요건

8

다음 하위 섹션에서는 NSX Manager 클러스터 요건을 설명하고, 특정 사이트 배포에 대한 권장 사항을 제공합니다. 또한 NSX Manager를 실행하는 호스트가 실패하는 경우 NSX-T Data Center에서 vSphere HA를 사용하여 빠르게 복구하는 방법도 설명합니다.

본 장은 다음 항목을 포함합니다.

- 단일, 이중 및 다중 사이트에 대한 NSX Manager 클러스터 요구 사항

단일, 이중 및 다중 사이트에 대한 NSX Manager 클러스터 요구 사항

NSX Manager 클러스터 구성은 배포가 단일, 이중 또는 여러 사이트에 대한 것인지에 따라 달라집니다.

NSX-T Data Center에서 vSphere HA를 사용하여 NSX Manager 노드를 실행하는 호스트 장애 시 빠른 복구를 사용하도록 설정할 수 있습니다.

참고 vSphere 제품 설명서에서 "vSphere HA 클러스터 생성 및 사용"을 참조하십시오.

클러스터 요건

- 운영 환경에서는 관리부 및 제어부의 중단을 방지하기 위해 NSX Manager 클러스터에 3개의 멤버가 있어야 합니다.

각 클러스터 멤버는 총 3개의 물리적 하이퍼바이저 호스트가 포함된 고유한 하이퍼바이저 호스트에 배치되어야 합니다. 이 작업은 NSX 제어부에 영향을 미치는 단일 물리적 하이퍼바이저 호스트 장애를 방지하기 위해 필요합니다. 반선호도 규칙을 적용하여 세 개의 클러스터 멤버가 서로 다른 호스트에서 실행되도록 하는 것이 좋습니다.

정상적인 운영 환경 상태는 3-노드 NSX Manager 클러스터입니다. 그러나 IP 주소 변경을 허용하기 위해 임시 NSX Manager 노드를 추가할 수 있습니다.

중요 NSX-T Data Center 2.4에서 NSX Manager에는 NSX 중앙 제어부 프로세스가 포함됩니다. 이 서비스는 NSX의 작동에 중요합니다. NSX Manager가 완전히 손실되거나 클러스터를 3개의 NSX Manager에서 1개의 NSX Manager로 줄인 경우 사용 환경에서 토폴로지를 변경할 수 없으며 NSX에 따라 시스템의 vMotion이 실패합니다.

- 프로덕션 워크로드가 없는 랩 및 개념 증명 배포의 경우 단일 NSX Manager를 실행하여 리소스를 절약할 수도 있습니다. ESXi 또는 KVM 중 하나에 NSX Manager 노드를 배포할 수 있습니다. 그러나 ESXi 및 KVM 둘 다에서 Manager를 혼합 배포하는 것은 지원되지 않습니다.

단일 사이트 요구 사항 및 권장 사항

다음 권장 사항은 단일 사이트 NSX-T Data Center 배포에 적용됩니다.

- 여러 관리자에게 영향을 미치는 단일 호스트 장애를 방지하기 위해서는 NSX Manager를 서로 다른 호스트에 배치하는 것이 좋습니다.
- NSX Manager 사이의 최대 지연 시간은 10ms입니다.
- NSX Manager를 서로 다른 vSphere 클러스터 또는 공통 vSphere 클러스터에 배치할 수 있습니다.
- 다른 관리 서버넷 또는 공유 관리 서버넷에 NSX Manager를 배치하는 것이 좋습니다. vSphere HA를 사용하는 경우 vSphere에서 복구한 NSX Manager가 IP 주소를 유지할 수 있도록 공유 관리 서버넷을 사용하는 것이 좋습니다.
- 공유 스토리지에도 NSX Manager를 배치하는 것이 좋습니다. vSphere HA의 경우 해당 솔루션에 대한 요구 사항을 검토하십시오.

또한 NSX-T에서 vSphere HA를 사용하여 NSX Manager가 실행 중인 호스트가 실패하는 경우 손실된 NSX Manager의 복구를 제공할 수 있습니다.

시나리오 예:

- 세 개의 모든 NSX Manager가 배포된 vSphere 클러스터.
- vSphere 클러스터는 다음 4개 이상의 호스트로 구성됩니다.
 - nsxmgr-01이 배포된 Host-01
 - nsxmgr-02이 배포된 Host-02
 - nsxmgr-03이 배포된 Host-03
 - NSX Manager가 배포되지 않은 Host-04
- vSphere HA는 손실된 NSX Manager(예: nsxmgr-01)를 임의 호스트(예: Host-01)에서 Host-04로 복구하도록 구성됩니다.

따라서 NSX Manager를 실행하는 호스트의 손실 발생 시 vSphere가 Host-04에서 손실된 NSX Manager를 복구합니다.

이중 사이트 요구 사항 및 권장 사항

다음 권장 사항은 이중 사이트(사이트 A/사이트 B) NSX-T Data Center 배포에 적용됩니다.

- vSphere HA가 없는 이중 사이트 시나리오에 NSX Manager를 배포하는 것은 권장되지 않습니다. 이 시나리오에서 한 사이트에는 2개의 NSX Manager 배포가 필요하며 해당 사이트가 손실되면 NSX-T Data Center 작업에 영향을 줍니다.

- vSphere HA가 있는 이중 사이트 시나리오에서 NSX Manager를 배포할 때는 다음 사항을 고려할 수 있습니다.
 - 확장된 단일 vSphere 클러스터에 NSX Manager에 대한 모든 호스트가 포함되어 있습니다.
 - 손실된 NSX Manager 복수 시 IP 주소 보존을 허용하도록 3개의 NSX Manager가 공통 관리 서브넷/VLAN에 배포됩니다.
 - 사이트 간 지연 시간에 대해서는 스토리지 제품 요구 사항을 참조하십시오.

시나리오 예:

- 세 개의 모든 NSX Manager가 배포된 vSphere 클러스터.
- vSphere 클러스터는 사이트 A의 3개 호스트와 사이트 B의 3개 호스트를 포함하는 6개 이상의 호스트로 구성됩니다.
- 3개의 NSX Manager는 복구된 NSX Manager 배치를 위한 추가 호스트가 있는 고유 호스트에 배포됩니다.

사이트 A:

- nsxmgr-01이 배포된 Host-01
- nsxmgr-02이 배포된 Host-02
- nsxmgr-03이 배포된 Host-03

사이트 B:

- NSX Manager가 배포되지 않은 Host-04
- NSX Manager가 배포되지 않은 Host-05
- NSX Manager가 배포되지 않은 Host-06
- vSphere HA는 손실된 NSX Manager(예: nsxmgr-01)를 사이트 A의 임의 호스트(예: Host-01)에서 사이트 B의 호스트 중 하나로 복구하도록 구성됩니다.

따라서 사이트 A가 실패하면 vSphere HA는 모든 NSX Manager를 사이트 B의 호스트로 복구합니다.

중요 NSX Manager가 동일한 공통 호스트로 복구되지 않도록 하려면 반선호도 규칙을 적절히 구성해야 합니다.

여러(3개 이상) 사이트 요구 사항 및 권장 사항

다음 권장 사항은 여러 사이트(사이트 A/사이트 B/사이트 C) NSX-T Data Center 배포에 적용됩니다.

3개 이상의 사이트가 있는 시나리오에서 vSphere HA를 포함하거나 포함하지 않은 상태로 NSX Manager를 배포할 수 있습니다.

vSphere HA를 포함하지 않고 배포하는 경우:

- 사이트별로 별도의 관리 서브넷 또는 VLAN을 사용하는 것이 좋습니다.

- NSX Manager 사이의 최대 지연 시간은 10ms입니다.

시나리오 예(3개의 사이트):

- 사이트당 별도의 3개 vSphere 클러스터
- 사이트당 NSX Manager를 실행 중인 하나 이상의 호스트:
 - nsxmgr-01이 배포된 Host-01
 - nsxmgr-02이 배포된 Host-02
 - nsxmgr-03이 배포된 Host-03

실패 시나리오:

- 단일 사이트 장애: 다른 사이트에 있는 두 개의 나머지 NSX Manager가 계속 작동합니다. NSX-T Data Center는 성능 저하 상태이지만 여전히 작동 중입니다. 손실된 클러스터 멤버를 교체하기 위해 세 번째 NSX Manager를 수동으로 배포하는 것이 좋습니다.
- 두 사이트 장애: 쿼럼이 손실되므로 NSX-T Data Center 작업에 영향을 미칩니다.

NSX Manager를 복구하는 데 CPU 속도, 디스크 성능 및 기타 배포 요소 등의 환경 조건에 따라 20분 정도 걸릴 수 있습니다.

NSX Edge 설치

9

NSX-T UI, vSphere Web Client 또는 명령줄 OVF 도구를 사용하여 ESXi에 NSX Edge를 설치합니다.

본 장은 다음 항목을 포함합니다.

- NSX Edge 설치 요구 사항
- NSX Edge 네트워킹 설정
- NSX Edge 설치 방법
- NSX Edge 전송 노드 생성
- NSX Edge 클러스터 생성
- vSphere GUI를 사용하여 ESXi에 NSX Edge 설치
- 베어 메탈에 NSX Edge 설치
- NSX Edge를 관리부에 연결
- NSX Edge를 전송 노드로 구성

NSX Edge 설치 요구 사항

NSX Edge에서는 NSX-T Data Center 배포 외부에 있는 네트워크 NSX Edge에 대해 라우팅 서비스 및 연결을 제공합니다. NAT(네트워크 주소 변환), VPN 등과 같은 상태 저장 서비스를 사용하여 Tier-0 라우터 또는 Tier-1 라우터를 배포하려는 경우 NSX Edge가 필요합니다.

참고 NSX Edge 노드당 1개의 Tier-0 라우터만 있을 수 있습니다. 하지만 여러 Tier-1 논리적 라우터를 하나의 NSX Edge 노드에 호스팅할 수 있습니다. 다른 크기의 NSX Edge VM을 동일한 클러스터에 결합할 수 있지만 권장되지는 않습니다.

표 9-1. NSX Edge 배포, 플랫폼 및 설치 요구 사항

요구 사항	설명
지원되는 배포 방법	<ul style="list-style-type: none"> ■ OVA/OVF ■ PXE를 사용하는 ISO ■ PXE를 사용하지 않는 ISO
지원되는 플랫폼	NSX Edge는 ESXi 또는 베어 메탈에서만 지원됩니다. NSX Edge는 KVM에서 지원되지 않습니다.
PXE 설치	암호 문자열은 root 및 admin 사용자 암호에 대해 sha-512 알 고리즘으로 암호화해야 합니다.
NSX-T Data Center 장치 암호	<ul style="list-style-type: none"> ■ 12자 이상 ■ 하나 이상의 소문자 ■ 하나 이상의 대문자 ■ 하나 이상의 숫자 ■ 하나 이상의 특수 문자 ■ 5개 이상의 다른 문자 ■ 사전 단어 제외 ■ 회문 제외 ■ 4자를 초과하는 단조 문자 시퀀스는 허용되지 않습니다.
호스트 이름	NSX Edge 설치 시 밑줄과 같은 잘못된 문자를 포함하지 않는 호스트 이름을 지정합니다. 호스트 이름에 유효하지 않은 문자가 포함되어 있으면 배포 후에 호스트 이름이 localhost 로 설정됩니다. 호스트 이름 제한에 대한 자세한 내용은 https://tools.ietf.org/html/rfc952 및 https://tools.ietf.org/html/rfc1123 을 참조하십시오.
VMware Tools	ESXi에서 실행되는 NSX Edge VM에는 VMTTools가 설치되어 있습니다. VMTTools를 제거하거나 업그레이드하지 마십시오.
시스템	시스템 요구 사항이 충족되었는지 확인합니다. NSX Edge VM 시스템 요구 사항 의 내용을 참조하십시오.
포트	필수 포트가 열려 있는지 확인합니다. 포트 및 프로토콜 의 내용을 참조하십시오.
IP 주소	여러 관리 네트워크가 있으면 NSX-T Data Center 장치에서 다른 네트워크로의 정적 경로를 추가할 수 있습니다. NSX Edge IPv4 또는 IPv6 IP 주소 지정 체계를 계획합니다.

표 9-1. NSX Edge 배포, 플랫폼 및 설치 요구 사항 (계속)

요구 사항	설명
OVF 템플릿	<ul style="list-style-type: none"> ■ ESXi 호스트에 OVF 템플릿을 배포하기 위한 적절한 권한이 있는지 확인합니다. ■ 호스트 이름에 밑줄이 포함되지 않았는지 확인합니다. 그렇지 않으면 호스트 이름이 <i>localhost</i>로 설정됩니다. ■ vCenter Server 또는 vSphere Client와 같은 OVF 템플릿을 배포할 수 있는 관리 도구. <p>OVF 배포 도구는 수동 구성을 허용하는 구성 옵션을 지원해야 합니다.</p> <ul style="list-style-type: none"> ■ 클라이언트 통합 플러그인이 설치되어 있어야 합니다.
NTP 서버	Edge 클러스터의 모든 NSX Edge VM 또는 베어메탈 Edge에 동일한 NTP 서버를 구성해야 합니다.

Intel 기반 칩셋

NSX Edge 노드는 Intel 기반 칩셋이 있는 ESXi 기반 호스트에서만 지원됩니다. 그렇지 않으면 vSphere VMware Enhanced vMotion Compatibility 모드에서 Edge 노드가 시작되지 못하므로 콘솔에 오류 메시지가 표시될 수 있습니다.

vSphere 무중단 업무 운영 기능의 NSX Edge 지원

NSX-T Data Center 2.5.1부터 NSX Edge 노드를 위한 vMotion, DRS 및 vSphere HA를 지원합니다.

NSX Edge 설치 시나리오

중요 vSphere 웹 클라이언트에서든 또는 명령줄에서든 OVA 또는 OVF 파일에서 NSX Edge를 설치하는 경우 OVA/OVF 속성 값(예: 사용자 이름, 암호 또는 IP 주소)은 VM 전원이 켜진 후에만 확인됩니다.

- **admin** 또는 **audit** 사용자에게 대해 사용자 이름을 지정하는 경우 사용자 이름이 고유해야 합니다. 동일한 이름을 지정하면 무시되고 기본 이름(**admin** 및 **audit**)이 사용됩니다.
- **admin** 사용자에게 대한 암호가 복잡성 요구 사항을 충족하지 못하면 SSH를 통해 또는 콘솔에서 **default** 암호를 사용하여 **admin** 사용자로 NSX Edge에 로그인해야 합니다. 암호를 변경하라는 메시지가 표시됩니다.
- **audit** 사용자에게 대한 암호가 복잡성 요구 사항을 충족하지 못하면 사용자 계정이 사용되지 않도록 설정됩니다. 계정을 사용하도록 설정하려면 SSH를 통해 또는 콘솔에서 **admin** 사용자 권한으로 NSX Edge에 로그인하고 **set user audit** 명령을 실행하고 **audit** 사용자의 암호를 설정합니다(현재 암호는 빈 문자열임).

- **root** 사용자에게 대한 암호가 복잡성 요구 사항을 충족하지 못하면 SSH를 통해 또는 콘솔에서 **vmware** 암호를 사용하여 **root** 사용자 권한으로 NSX Edge에 로그인해야 합니다. 암호를 변경하라는 메시지가 표시됩니다.

경고 **root** 사용자 자격 증명으로 로그인한 상태에서 NSX-T Data Center에 대해 변경을 수행하면 시스템 오류가 발생할 수 있고 잠재적으로 네트워크에 영향을 줄 수 있습니다. VMware 지원 팀이 안내하는 경우에만 **root** 사용자 자격 증명을 사용하여 변경을 수행할 수 있습니다.

참고 장치의 핵심 서비스는 충분한 복잡도를 갖는 암호를 설정해야만 시작할 수 있습니다.

OVA 파일에서 NSX Edge를 배포한 후에는 VM 전원을 끄고 vCenter Server에서 OVA 설정을 수정하여 VM의 IP 설정을 변경할 수 없습니다.

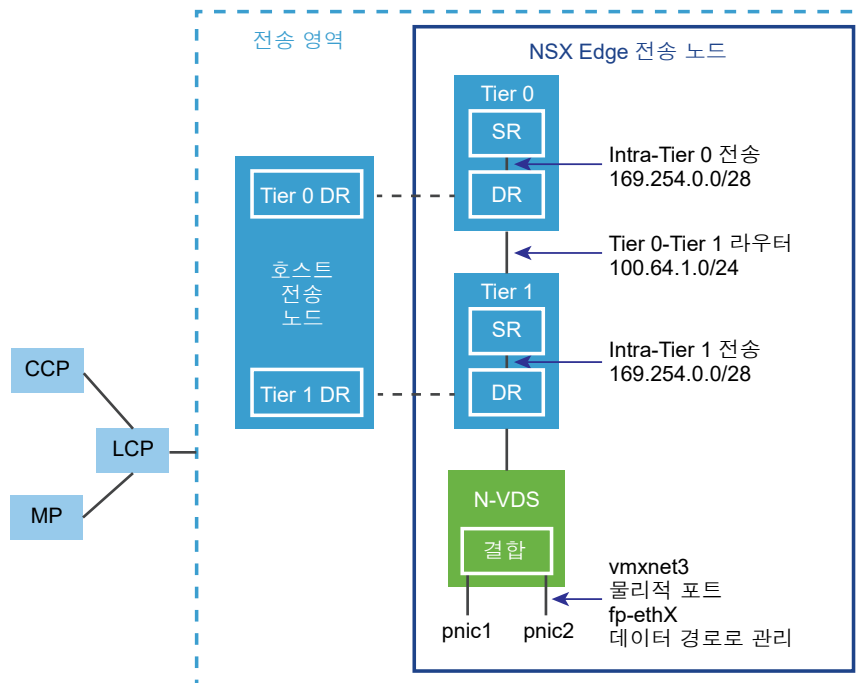
NSX Edge 네트워킹 설정

NSX Edge는 ISO, OVA/OVF 또는 PXE 시작을 통해 설치할 수 있습니다. 설치 방법과 관계없이 NSX Edge를 설치하기 전에 호스트 네트워킹이 준비되어 있도록 합니다.

전송 영역 내의 NSX Edge 간략 보기

NSX-T Data Center 간략 보기는 전송 영역에 있는 2개의 전송 노드를 표시합니다. 한 전송 노드는 호스트입니다. 다른 전송 노드는 NSX Edge입니다.

그림 9-1. NSX Edge의 상위 수준 개요



NSX Edge를 처음 배포할 때는 빈 컨테이너로 간주할 수 있습니다. NSX Edge는 논리적 라우터를 생성할 때까지 아무 작업도 수행하지 않습니다. NSX Edge에서는 Tier-0 및 Tier-1 논리적 라우터에 대한 계산 지원을 제공합니다. 각 논리적 라우터에는 SR(서비스 라우터) 및 DR(분산 라우터)이 포함되어 있습니다. 라우터가 분산된다는 것은 동일한 전송 영역에 속해 있는 모든 전송 노드에서 복제된다는 것을 의미합니다. 이 그림에서 호스트 전송 노드에는 Tier-0 및 Tier-1 라우터에 포함된 것과 동일한 DR이 포함되어 있습니다. 논리적 라우터를 NAT와 같은 서비스를 수행하도록 구성하려는 경우 서비스 라우터가 필요합니다. 모든 Tier-0 논리적 라우터에는 서비스 라우터가 있습니다. Tier-1 라우터는 설계 고려 사항에 따라 필요한 경우 서비스 라우터가 있을 수 있습니다.

기본적으로 SR 및 DR 간의 링크는 169.254.0.0/28 서브넷을 사용합니다. 이러한 라우터 내 전송 링크는 Tier-0 또는 Tier-1 논리적 라우터를 배포할 때 자동으로 생성됩니다. 169.254.0.0/28 서브넷이 배포에서 이미 사용되는 경우가 아니면 링크 구성을 구성하거나 수정할 필요가 없습니다. Tier-1 논리적 라우터에서 SR은 Tier-1 논리적 라우터를 생성할 때 NSX Edge 클러스터를 선택하는 경우에만 존재합니다.

Tier-0과 Tier-1 간의 연결에 할당되는 기본 주소 공간은 100.64.0.0/10입니다. 각 Tier-0과 Tier-1 간의 피어 연결에는 100.64.0.0/10 주소 공간 내에 /31 서브넷이 제공됩니다. Tier-1 라우터를 생성한 후 이를 Tier-0 라우터에 연결할 때 이 링크가 자동으로 생성됩니다. 100.64.0.0/10 서브넷이 배포에서 이미 사용되는 경우가 아니면 이 링크에서 인터페이스를 구성하거나 수정할 필요가 없습니다.

각 NSX-T Data Center 배포에는 MP(관리부 클러스터) 및 CCP(제어부 클러스터)가 있습니다. MP 및 CCP는 각 전송 영역의 LCP(로컬 제어부)에 구성을 푸시합니다. 호스트 또는 NSX Edge가 관리부에 연결되면 MPA(관리부 에이전트)는 호스트 또는 NSX Edge와의 연결을 설정하고 호스트 또는 NSX Edge는 NSX-T Data Center 패브릭 노드가 됩니다. 패브릭 노드가 전송 노드로 추가되면 호스트 또는 NSX Edge와의 LCP 연결이 설정됩니다.

마지막으로 이 그림은 고가용성을 제공하기 위해 결합된 2개의 물리적 NIC(물리적 NIC1 및 물리적 NIC2)의 예를 보여줍니다. 데이터 경로는 물리적 NIC를 관리합니다. 외부 네트워크에 대한 VLAN 업링크 또는 내부 NSX-T Data Center 관리 VM 네트워크에 대한 터널 끝점 링크로 작동할 수 있습니다.

VM으로 배포된 각 NSX Edge에 2개 이상의 물리적 링크를 할당하는 것이 좋습니다. 경우에 따라 다른 VLAN ID를 사용하여 동일한 물리적 NIC에서 포트 그룹을 겹칠 수 있습니다. 검색된 첫 번째 네트워크 링크는 관리에 사용됩니다. 예를 들어 NSX Edge VM에서 검색된 첫 번째 링크는 vnic1일 수 있습니다. 베어 메탈 설치에서 검색된 첫 번째 링크는 eth0 또는 em0일 수 있습니다. 나머지 링크는 업링크 및 터널에 사용됩니다. 예를 들어 하나는 NSX-T Data Center 관리 VM에서 사용되는 터널 끝점에 사용되고, 다른 하나는 외부 TOR 업링크에 대한 NSX Edge에 사용될 수 있습니다.

CLI에 관리자로 로그인하고 `get interfaces` 및 `get physical-ports` 명령을 실행하여 NSX Edge의 물리적 링크 정보를 확인할 수 있습니다. API에서 `GET fabric/nodes/<edge-node-id>/network/interfaces` API 호출을 사용할 수 있습니다. 물리적 링크는 다음 섹션에서 좀 더 자세히 설명됩니다.

NSX Edge를 VM 장치로 설치하거나 베어 메탈에 설치할 경우 배포에 따라 몇 가지 네트워크 구성 옵션이 있습니다.

전송 영역 및 N-VDS

NSX Edge 네트워킹을 이해하려면 전송 영역 및 N-VDS에 대해 알아야 할 사항이 있습니다. 전송 영역은 NSX-T Data Center의 계층 2 네트워크 도달 영역을 제어합니다. N-VDS는 전송 노드에서 생성되는 소프트웨어 스위치입니다. N-VDS는 물리적 NIC에 대한 논리적 라우터 업링크 및 다운링크를 바인딩하는 데 사용됩니다. NSX Edge가 속하는 각 전송 영역에 대해 NSX Edge에 단일 N-VDS가 설치됩니다.

전송 영역에는 두 가지 유형이 있습니다.

- 전송 노드 간의 내부 NSX-T Data Center 터널링용 오버레이
- NSX-T Data Center 외부 업링크용 VLAN

NSX Edge는 VLAN 전송 영역에 속하지 않거나 여러 전송 영역에 속할 수 있습니다. VLAN 전송 영역이 없는 경우에도 NSX Edge 업링크에서 오버레이 전송 영역에 대해 설치된 것과 동일한 N-VDS를 사용할 수 있으므로 NSX Edge에는 여전히 업링크가 있을 수 있습니다. 각 NSX Edge에 N-VDS가 하나만 있도록 하려면 이렇게 하면 됩니다. 또 다른 설계 옵션은 NSX Edge를 각 업링크에 대해 하나씩 여러 VLAN 전송 영역에 속하게 하는 것입니다.

가장 일반적인 설계 옵션은 1개의 오버레이 영역과 2개의 VLAN 전송 영역(중복 업링크용)으로 이루어진 3개의 전송 영역을 사용하는 것입니다.

VLAN 업링크의 경우처럼 오버레이 트래픽 및 기타 VLAN 트래픽에 대한 전송 네트워크에 동일한 VLAN ID를 사용하려면, 두 개의 서로 다른 N-VDS에 하나는 VLAN용, 다른 하나는 오버레이용으로 ID를 구성합니다.

가상 장치/VM NSX Edge 네트워킹

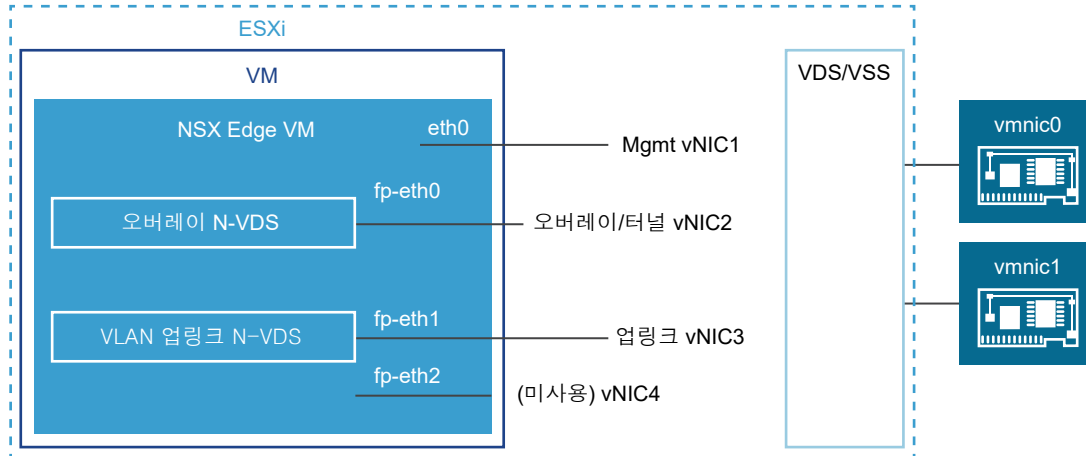
NSX Edge를 가상 장치 또는 VM으로 설치하는 경우 fp-ethX라는 내부 인터페이스가 생성됩니다. 여기서 X는 0, 1, 2, 3 등의 숫자입니다. 이러한 인터페이스는 ToR(랙 상단) 스위치로의 업링크 및 NSX-T Data Center 오버레이 터널링에 할당됩니다.

NSX Edge 전송 노드를 생성할 때 업링크 및 오버레이 터널과 연결하기 위한 fp-ethX 인터페이스를 선택할 수 있습니다. fp-ethX 인터페이스 사용 방법을 결정할 수 있습니다.

vSphere Distributed Switch 또는 vSphere Standard 스위치에서 2개 이상의 vmnic를 NSX Edge에 할당해야 합니다. 하나는 NSX Edge 관리용이고 다른 하나는 업링크 및 터널용입니다.

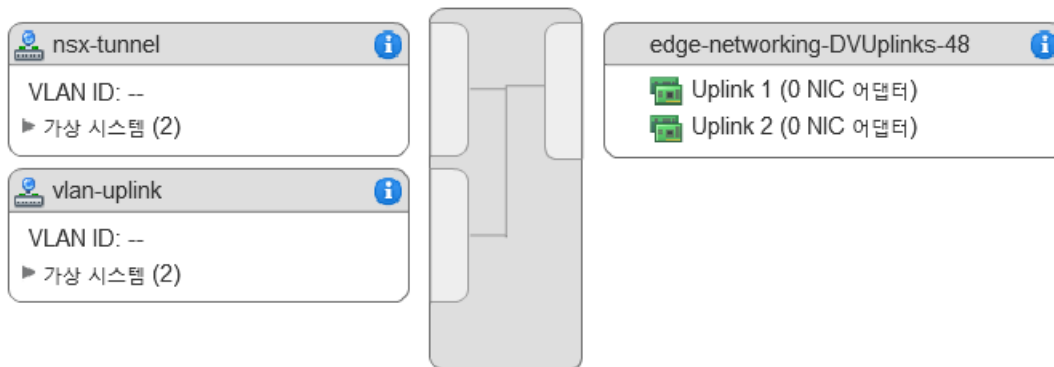
다음 샘플 물리적 토폴로지에서 fp-eth0은 NSX-T Data Center 오버레이 터널에 사용됩니다. fp-eth1은 VLAN 업링크에 사용됩니다. fp-eth2 및 fp-eth3은 사용되지 않습니다. vNIC1은 관리 네트워크에 할당되어 있습니다.

그림 9-2. NSX Edge VM 네트워킹에 대해 제안되는 한 가지 링크 설정



이 예에 나오는 NSX Edge는 2개의 전송 영역(1개의 오버레이 및 1개의 VLAN)에 속하므로 터널용 1개와 업링크 트래픽용 1개로 이루어진 2개의 N-VDS가 있습니다.

이 스크린샷은 가상 시스템 포트 그룹인 nsx-tunnel과 vlan-uplink를 보여줍니다.



배포 중에 VM 포트 그룹에 구성된 이름과 일치하는 네트워크 이름을 지정해야 합니다. 예를 들어 ovftool 을 사용하여 NSX Edge를 배포하는 경우 예에 포함된 VM 포트 그룹을 일치시키려면 네트워크 ovftool 설정을 다음과 같이 하면 됩니다.

```
--net:"Network 0-Mgmt" --net:"Network 1-nsx-tunnel" --net:"Network 2=vlan-uplink"
```

여기에 표시된 예에서는 VM 포트 그룹 이름 Mgmt, nsx-tunnel 및 vlan-uplink를 사용합니다. VM 포트 그룹에는 어떤 이름도 사용 가능합니다.

NSX Edge에 대해 구성된 터널 및 업링크 VM 포트 그룹은 VMkernel 포트 또는 지정된 IP 주소에 연결할 필요가 없습니다. 이는 계층 2에서만 사용되기 때문입니다. 배포에서 DHCP를 사용하여 관리 인터페이스에 주소를 제공하는 경우 관리 네트워크에 NIC를 하나만 할당해야 합니다.

VLAN 및 터널 포트 그룹은 트렁크 포트 그룹으로 구성됩니다. 이는 필수 작업입니다. 예를 들어 표준 vSwitch에서 트렁크 포트를 다음과 같이 구성할 수 있습니다. **호스트 > 구성 > 네트워킹 > 네트워킹 추가 > 가상 시스템 > VLAN ID 전체(4095).**

장치 기반 또는 VM NSX Edge를 사용하는 경우 표준 vSwitch 또는 vSphere Distributed Switch를 사용할 수 있습니다.

NSX Edge VM은 NSX-T Data Center 준비된 호스트에 설치되어 전송 노드로 구성될 수 있습니다. 배포에는 두 가지 유형이 있습니다.

- NSX Edge VM은 VSS/VDS 포트 그룹을 사용하여 배포할 수 있으며, VSS/VDS는 호스트에서 별도의 물리적 NIC를 사용합니다. 호스트 전송 노드는 호스트에 설치된 N-VDS에 대해 별도의 물리적 NIC를 사용합니다. 호스트 전송 노드의 N-VDS는 별도의 물리적 NIC를 사용하는 VSS 또는 VDS와 공존합니다. 호스트 TEP(Tunnel End Point)와 NSX Edge TEP는 동일하거나 다른 서브넷에 있을 수 있습니다.
- NSX Edge VM은 호스트 전송 노드의 N-VDS에 VLAN 기반 논리적 스위치를 사용하여 배포할 수 있습니다. 호스트 TEP와 NSX Edge TEP는 서로 다른 서브넷에 있어야 합니다.

경우에 따라 단일 호스트에 여러 NSX Edge 장치/VM을 설치할 수 있고, 설치된 모든 NSX Edge에서 동일한 관리, VLAN 및 터널 끝점 포트 그룹을 사용할 수 있습니다.

기본 물리적 링크가 작동되고 VM 포트 그룹이 구성되면 NSX Edge를 설치할 수 있습니다.

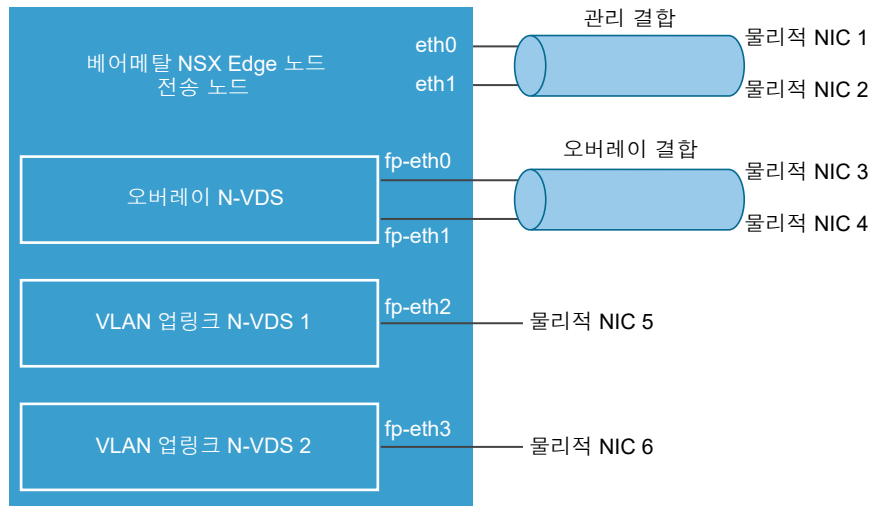
베어 메탈 NSX Edge 네트워킹

베어 메탈 NSX Edge에는 fp-ethX라는 내부 인터페이스가 포함되어 있습니다. 여기서 X는 0, 1, 2, 3 또는 4입니다. 생성되는 fp-ethX 인터페이스 수는 베어 메탈 NSX Edge에 있는 물리적 NIC의 수에 따라 다릅니다. 이러한 인터페이스를 최대 4개까지 ToR(랙 상단) 스위치 및 NSX-T Data Center 오버레이 터널링에 대한 업링크에 할당할 수 있습니다.

NSX Edge 전송 노드를 생성할 때 업링크 및 오버레이 터널과 연결하기 위한 fp-ethX 인터페이스를 선택할 수 있습니다.

fp-ethX 인터페이스 사용 방법을 결정할 수 있습니다. 다음 샘플 물리적 토폴로지에서 fp-eth0 및 fp-eth1은 결합된 후 NSX-T Data Center 오버레이 터널에 사용됩니다. fp-eth2 및 fp-eth3은 TOR에 대한 중복 VLAN 업링크로 사용됩니다.

그림 9-3. 베어 메탈 NSX Edge 네트워킹에 대해 제안되는 한 가지 링크 설정



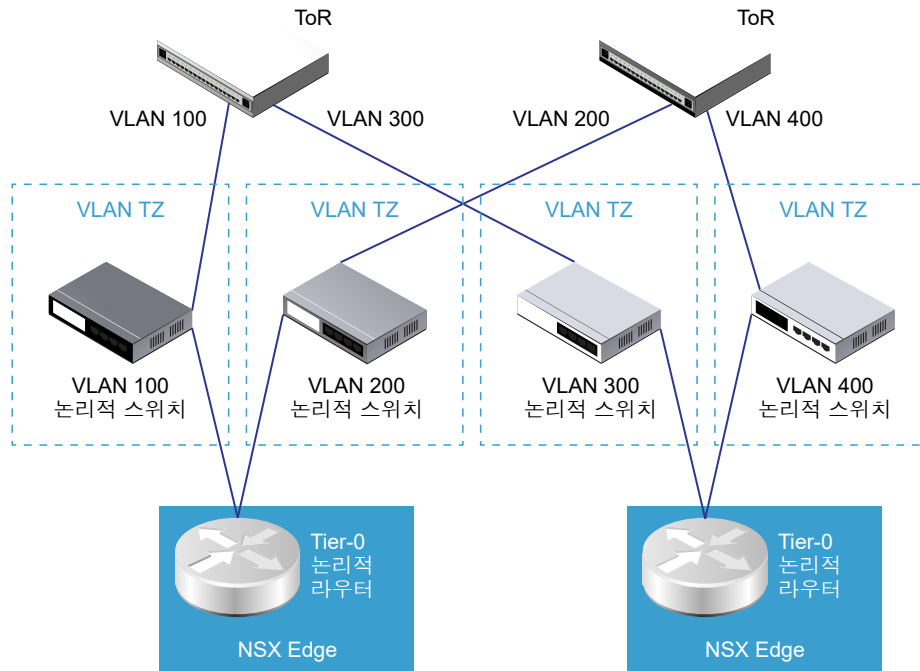
NSX Edge 업링크 이중화

NSX Edge 업링크 이중화를 통해 두 VLAN ECMP(동일 비용 다중 경로) 업링크를 NSX Edge와 외부 TOR 간의 네트워크 연결에 사용할 수 있습니다.

ECMP VLAN 업링크가 2개 있으면고가용성 및 완전 메시 연결을 위해 TOR 스위치도 2개 있어야 합니다. 각 VLAN 논리적 스위치에는 연결된 VLAN ID가 있습니다.

NSX Edge를 VLAN 전송 영역에 추가하면 새 N-VDS가 설치됩니다. 예를 들어 그림과 같이 4개의 VLAN 전송 영역에 NSX Edge 노드를 추가하면 4개의 N-VDS가 NSX Edge에 설치됩니다.

그림 9-4. TOR에 대한 NSX Edge에 권장되는 한 가지 ECMP VLAN 설정



참고 N-VDS가 아닌 vDS(vSphere Distributed Switch)가 있는 ESXi 호스트에 배포된 Edge VM의 경우 다음을 수행해야 합니다.

- DHCP 작동을 위해 위조 전송을 사용하도록 설정합니다.
- 기본적으로 MAC 학습이 사용되지 않도록 설정되어 있기 때문에 Edge VM이 알 수 없는 유니캐스트 패킷을 수신하려면 무차별 모드를 사용하도록 설정합니다. 이는 MAC 학습이 기본적으로 사용되도록 설정되어 있는 vDS 6.6 이상에 대해서는 필수가 아닙니다.

NSX Edge 설치 방법

NSX Manager UI(권장 방법), vSphere Web Client 또는 vSphere 명령줄 OVF 도구를 사용해서 ESXi 호스트에 NSX Edge를 설치합니다.

NSX Edge 설치 방법

설치 방법	지침
NSX Manager(NSX Edge VM 장치만 설치하기 위한 권장 방법)	<ul style="list-style-type: none"> ■ NSX Edge 네트워크 요구 사항을 충족하는지 확인합니다. NSX Edge 설치 요구 사항의 내용을 참조하십시오. ■ NSX Edge 전송 노드를 생성합니다. NSX Edge 전송 노드 생성 항목을 참조하십시오. ■ NSX Edge 클러스터를 생성합니다. NSX Edge 클러스터 생성 항목을 참조하십시오.
vSphere Web Client 또는 vSphere 명령줄 OVF 도구	<ul style="list-style-type: none"> ■ NSX Edge 네트워크 요구 사항을 충족하는지 확인합니다. NSX Edge 설치 요구 사항의 내용을 참조하십시오. ■ vSphere Web Client 또는 vSphere 명령줄 OVF 옵션 도구를 선택하여 NSX Edge를 설치합니다. <ul style="list-style-type: none"> ■ (Web Client) ESXi에 NSX Edge를 설치합니다. vSphere GUI를 사용하여 ESXi에 NSX Edge 설치 항목을 참조하십시오. ■ (명령줄 OVF 도구) ESXi에 NSX Edge를 설치합니다. 명령줄 OVF 도구를 사용하여 ESXi에 NSX Manager 설치 항목을 참조하십시오. ■ NSX Edge를 관리부에 연결합니다. NSX Edge를 관리부에 연결 항목을 참조하십시오. ■ NSX Edge를 전송 노드로 구성합니다. NSX Edge를 전송 노드로 구성 항목을 참조하십시오. ■ NSX Edge 클러스터를 생성합니다. NSX Edge 클러스터 생성 항목을 참조하십시오.
(베어메탈 서버) ISO(ISO 파일을 통한 자동화 또는 대화형 모드) 또는 NSX Edge VM 장치로	<p>베어메탈 서버에서 NSX Edge의 자동화 설치를 구성하거나, PXE를 사용하여 NSX Edge를 VM 장치로 설치할 수 있습니다. PXE 부팅 설치 절차는 NSX Manager에서 지원되지 않습니다.</p> <ul style="list-style-type: none"> ■ NSX Edge 네트워크 요구 사항을 충족하는지 확인합니다. NSX Edge 설치 요구 사항의 내용을 참조하십시오. ■ PXE 서버를 준비합니다. NSX Edge를 위한 PXE 서버 준비 를 참조하십시오. 지원되는 설치 방법 중에서 하나를 선택합니다. <ul style="list-style-type: none"> ■ (자동 설치) ISO 파일을 통해 베어메탈에 NSX Edge를 설치합니다. ISO 파일을 통해 자동으로 NSX Edge 설치 항목을 참조하십시오. ■ (자동 설치) ISO 파일을 통해 가상 장치로 NSX Edge를 설치합니다. ISO 파일을 통해 가상 장치로 NSX Edge 설치 항목을 참조하십시오. ■ (수동 설치) ISO 파일을 통해 NSX Edge를 수동으로 설치합니다. ISO 파일을 통해 대화형으로 NSX Edge 설치 항목을 참조하십시오. ■ NSX Edge를 관리부에 연결합니다. NSX Edge를 관리부에 연결 항목을 참조하십시오. ■ NSX Edge를 전송 노드로 구성합니다. NSX Edge를 전송 노드로 구성 항목을 참조하십시오. ■ NSX Edge 클러스터를 생성합니다. NSX Edge 클러스터 생성 항목을 참조하십시오.

NSX Edge 전송 노드 생성

NSX Edge VM을 NSX-T Data Center 패브릭에 추가하고 계속해서 NSX Edge를 전송 노드 VM으로 구성할 수 있습니다.

NSX Edge 노드는 NSX-T 데이터부를 구현하는 로컬 제어부 데몬 및 전달 엔진을 실행하는 전송 노드입니다. NSX-T 가상 Distributed Switch 또는 N-VDS라고 하는 NSX-T 가상 스위치의 인스턴스를 실행합니다. Edge 노드는 하이퍼바이저로 배포할 수 없는 중앙 집중식 네트워크 서비스 실행을 담당하는 서비스 장치입니다. 이러한 구성 요소는 베어메탈 장치 또는 가상 시스템 폼 팩터로 인스턴스화될 수 있습니다. 또한 용량 풀을 나타내는 하나 또는 여러 개의 클러스터로 그룹화됩니다.

NSX Edge는 1개의 오버레이 전송 영역과 여러 개의 VLAN 전송 영역에 속할 수 있습니다. NSX Edge는 업링크 액세스를 제공하기 위해 1개 이상의 VLAN 전송 영역에 속합니다.

참고 템플릿 VM에서 전송 노드를 생성하려는 경우 `/etc/vmware/nsx/`에서 호스트에 인증서가 없는지 확인합니다. netcpa 에이전트는 인증서가 이미 있으면 인증서를 생성하지 않습니다.

사전 요구 사항

- 전송 영역을 구성해야 합니다. [전송 영역 생성](#) 항목을 참조하십시오.
- 계산 관리자가 구성되어 있는지 확인합니다. [계산 관리자 추가](#)의 내용을 참조하십시오.
- 업링크 프로파일이 구성해야 하거나 NSX Edge 노드에 대해 기본 업링크 프로파일을 사용할 수도 있습니다. [업링크 프로파일 생성](#) 항목을 참조하십시오.
- IP 풀을 구성해야 하거나 네트워크 배포에 사용할 수 있어야 합니다. [터널 끝점 IP 주소에 대한 IP 풀 생성](#) 항목을 참조하십시오.

절차

1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.

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

3 NSX Edge의 이름을 입력합니다.

4 vCenter Server의 호스트 이름 또는 FQDN을 입력합니다.

5 최적의 성능을 위해 NSX Edge 장치를 위한 메모리를 예약합니다.

NSX Edge가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정합니다. [NSX Edge VM 시스템 요구 사항](#)의 내용을 참조하십시오.

6 NSX Edge의 CLI 및 루트 암호를 지정합니다.

암호는 암호 길이 제한을 준수해야 합니다.

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

- 5개 이상의 다른 문자
- 기본 암호 복잡성 규칙은 다음 Linux PAM 모듈 인수에 의해 적용됩니다.
 - **retry=3**: 오류 결과를 반환하기 전에 새 암호를 입력할 수 있는 최대 횟수로, 이 인수의 경우 최대 3번입니다.
 - **minlen=12**: 새 암호에 허용되는 최소 크기입니다. 새 암호의 문자 수 외에도 다른 종류의 문자(예: 대문자, 소문자 및 숫자)에 대해 크레딧(길이에 +1)이 지정됩니다.
 - **difok=0**: 새 암호에서 달라야 하는 최소 바이트 수입니다. 이전 암호와 새 암호 간 유사성을 나타냅니다. difok에 값 0을 할당하면 이전 암호 및 새 암호 바이트를 다르게 유지할 필요가 없습니다. 정확한 일치만 허용됩니다.
 - **lcredit=1**: 새 암호에서 소문자에 대한 최대 크레딧입니다. 1개 이하의 소문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다.
 - **ucredit=1**: 새 암호에서 대문자에 대한 최대 크레딧입니다. 1개 이하의 대문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다.
 - **dcredit=1**: 새 암호에서 숫자에 대한 최대 크레딧입니다. 1개 이하의 숫자가 있는 경우 각 숫자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다.
 - **ocredit=1**: 새 암호에서 다른 문자에 대한 최대 크레딧입니다. 1개 이하의 다른 문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다.
 - **enforce_for_root**: 암호가 루트 사용자에게 설정됩니다.

참고 사전 단어를 기준으로 암호를 확인하기 위한 Linux PAM 모듈에 대한 자세한 내용은 설명서 페이지를 참조하십시오.

예를 들어 **VMware123!123** 또는 **VMware12345**와 같이 간단하고 규칙적인 암호는 사용하지 마십시오. 복잡성 표준을 충족하는 암호는 간단하고 체계적이지 않지만 문자, 알파벳, 특수 문자 및 숫자 조합(예: **VMware123!45**, **VMware1!2345** 또는 **VMware@1az23x**)입니다.

7 NSX Edge 세부 정보를 입력합니다.

옵션	설명
계산 관리자	드롭다운 메뉴에서 계산 관리자를 선택합니다. 계산 관리자는 관리부에 등록된 vCenter Server입니다.
클러스터	드롭다운 메뉴에서 NSX Edge가 연결될 클러스터를 지정합니다.
리소스 풀 또는 호스트	드롭다운 메뉴에서 NSX Edge에 대해 리소스 풀 또는 특정 호스트를 할당합니다.
데이터스토어	드롭다운 메뉴에서 NSX Edge 파일에 대한 데이터스토어를 선택합니다.

8 NSX Edge 인터페이스 세부 정보를 입력합니다.

옵션	설명
IP 할당	<p>NSX Manager 및 NSX Controller와 통신하는 데 필요한 NSX Edge 노드에 할당된 IP 주소입니다.</p> <p>DHCP 또는 정적 IP를 선택합니다.</p> <p>정적을 선택하는 경우 다음 값을 입력합니다.</p> <ul style="list-style-type: none"> ■ 관리 IP: CIDR 표기법으로 NSX Edge의 IP 주소를 입력합니다. ■ 기본 게이트웨이: NSX Edge의 게이트웨이 IP 주소를 입력합니다.
관리 인터페이스	<p>드롭다운 메뉴에서 관리 네트워크 인터페이스를 선택합니다. 이 인터페이스는 NSX Manager에서 연결할 수 있거나, NSX Manager 및 NSX Controller와 동일한 관리 인터페이스에 있어야 합니다.</p> <p>NSX Edge 관리 인터페이스는 NSX Manager 관리 인터페이스와의 통신을 설정합니다.</p>

9 이 전송 노드가 속한 전송 영역을 선택합니다.

NSX Edge 전송 노드는 2개 이상의 전송 영역, 즉 NSX-T Data Center 연결용 오버레이와 업링크 연결용 VLAN에 속합니다.

참고 NSX Edge 노드는 다음과 같은 전제 조건이 충족될 때 다중 오버레이 터널(다중 TEP)을 지원합니다.

- TEP 구성은 하나의 N-VDS에서만 수행해야 합니다.
- 모든 TEP는 오버레이 트래픽에 대해 동일한 전송 VLAN을 사용해야 합니다.
- 모든 TEP IP는 동일한 서브넷에 있어야 하며 동일한 기본 게이트웨이를 사용해야 합니다.

10 N-VDS 정보를 입력합니다.

옵션	설명
Edge 스위치 이름	드롭다운 메뉴에서 VLAN 또는 오버레이 스위치를 선택합니다.
업링크 프로파일	<p>드롭다운 메뉴에서 업링크 프로파일을 선택합니다.</p> <p>사용 가능한 업링크는 선택된 업링크 프로파일의 구성에 따라 다릅니다.</p>

옵션	설명
IP 할당	<p>IP 주소가 구성된 NSX Edge 스위치에 할당됩니다. 오버레이 또는 VLAN 네트워크에서 패킷을 라우팅하는 데 사용됩니다.</p> <p>오버레이 N-VDS에 대해 IP 풀 사용 또는 정적 IP 목록 사용을 선택합니다.</p> <ul style="list-style-type: none"> ■ 정적 IP 목록 사용을 선택하는 경우 다음을 지정합니다. <ul style="list-style-type: none"> ■ 정적 IP 목록: NSX Edge 스위치에서 사용할 쉽표로 구분된 IP 주소 목록을 입력합니다. ■ 게이트웨이: 오버레이 네트워크의 NSX Edge 전송 노드 간에 패킷을 라우팅하는 데 사용되는 기본 게이트웨이 IP 주소를 입력합니다. ■ 서브넷 마스크: 구성된 게이트웨이의 서브넷 마스크를 입력합니다. ■ IP 할당에 대해 IP 풀 사용을 선택한 경우 IP 풀 이름을 지정합니다.
DPDK 빠른 경로 인터페이스/가상 NIC	<p>업링크 인터페이스에 대한 데이터 경로 인터페이스를 선택합니다.</p> <p>참고 Edge 노드에 적용된 업링크 프로파일이 명명된 팀 구성 정책을 사용하는 경우 다음 조건이 충족되어야 합니다.</p> <ul style="list-style-type: none"> ■ 명명된 팀 구성 정책을 사용하는 논리적 스위치를 통해 트래픽이 흐르려면 기본 팀 구성 정책의 모든 업링크를 Edge VM의 물리적 네트워크 인터페이스에 매핑해야 합니다.

참고

- LLDP 프로파일은 NSX Edge VM 장치에서 지원되지 않습니다.
- NSX Manager를 사용하여 또는 베어메탈 서버에 NSX Edge를 설치한 경우 업링크 인터페이스가 **DPDK 빠른 경로 인터페이스**로 표시됩니다.
- vCenter Server를 사용하여 NSX Edge를 수동으로 설치한 경우 업링크 인터페이스가 **가상 NIC**로 표시됩니다.

11 전송 노드 페이지에서 연결 상태를 확인합니다.

NSX Edge를 전송 노드로 추가하면 10-12분 후에 연결 상태가 [실행 중]으로 변경됩니다.

- (선택 사항) 다음과 같이 GET `https://<nsx-manager>/api/v1/transport-nodes/<transport-node-id>` API 호출을 사용하여 전송 노드를 확인합니다.
- (선택 사항) 상태 정보를 보려면 GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/status` API 호출을 사용합니다.
- vCenter Server를 사용하여 NSX Edge 노드를 새 호스트로 마이그레이션한 후 NSX Edge의 오래된 구성 세부 정보(계산, 데이터스토어, 네트워크, SSH, NTP, DNS, 검색 도메인)를 보고하는 NSX Manager UI를 찾을 수 있습니다. 새 호스트에서 NSX Edge의 최신 구성 세부 정보를 가져오려면 API 명령을 실행합니다.

```
POST api/v1/transport-nodes/<transport-node-id>?
action=refresh_node_configuration&resource_type=EdgeNode
```

다음에 수행할 작업

NSX Edge 클러스터에 NSX Edge 노드를 추가합니다. [NSX Edge 클러스터 생성](#)의 내용을 참조하십시오.

NSX Edge 클러스터 생성

NSX Edge의 다중 노드 클러스터를 유지하면 하나 이상의 NSX Edge를 항상 사용할 수 있습니다.

NAT, 로드 밸런서 등과 같은 상태 저장 서비스를 사용하여 Tier-0 논리적 라우터 또는 Tier-1 라우터를 생성하려면 NSX Edge 클러스터와 연결해야 합니다. 따라서 NSX Edge가 하나만 있더라도 NSX Edge 클러스터에 속해 있어야만 사용할 수 있습니다.

NSX Edge 전송 노드는 단일 NSX Edge 클러스터에만 추가할 수 있습니다.

NSX Edge 클러스터는 여러 논리적 라우터를 지원하는 데 사용할 수 있습니다.

NSX Edge 클러스터를 생성한 후에 나중에 이를 편집하여 추가 NSX Edge를 추가할 수 있습니다.

사전 요구 사항

- 하나 이상의 NSX Edge 노드를 설치합니다.
- 노드를 클러스터에 가입하기 전에 모든 서비스가 실행 중인 상태로 NSX Edge 노드가 안정적이고 모든 그룹이 안정적인지 확인합니다.
- NSX Edge를 관리부에 연결합니다.
- NSX Edge를 전송 노드로 추가합니다.
- 필요한 경우 HA(고가용성)에 대한 NSX Edge 클러스터 프로파일을 생성합니다. 기본 NSX Edge 클러스터 프로파일을 사용할 수도 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 패브릭 > 노드 > Edge 클러스터 > 추가**를 선택합니다.
- 3 NSX Edge 클러스터 이름을 입력합니다.
- 4 드롭다운 목록에서 NSX Edge 클러스터 프로파일을 선택합니다.
- 5 [멤버 유형] 드롭다운 메뉴에서 가상 시스템이 온-프레미스에 배포된 경우에는 **Edge 노드**를 선택하고, 가상 시스템이 공용 클라우드에 배포된 경우에는 **공용 클라우드 게이트웨이**를 선택합니다.
- 6 **사용 가능** 열에서 NSX Edge를 선택하고 오른쪽 화살표를 클릭하여 이를 **선택됨** 열로 이동합니다.

다음에 수행할 작업

이제 논리적 네트워크 토폴로지를 구축하고 서비스를 구성할 수 있습니다. "NSX-T Data Center 관리 가이드"의 내용을 참조하십시오.

vSphere GUI를 사용하여 ESXi에 NSX Edge 설치

vSphere Web Client 또는 vSphere Client를 사용하여 ESXi에 NSX Edge를 대화형으로 설치할 수 있습니다.

참고 NSX-T Data Center 2.5.1부터는 NSX Edge VM이 vMotion을 지원합니다.

사전 요구 사항

[NSX Edge 설치 요구 사항](#)의 NSX Edge 네트워크 요구 사항을 참조하십시오.

절차

- 1 VMware 다운로드 포털에서 NSX Edge 장치 OVA 파일을 찾습니다.
다운로드 URL을 복사하거나 OVA 파일을 컴퓨터에 다운로드합니다.
- 2 vSphere Client에서 NSX Edge 장치를 설치할 호스트를 선택합니다.
- 3 마우스 오른쪽 버튼을 클릭하고 **OVF 템플릿 배포**를 선택하여 설치 마법사를 시작합니다.
- 4 OVA 다운로드 URL을 입력하거나 저장된 OVA 파일로 이동합니다.
- 5 NSX Edge VM의 이름을 입력합니다.
입력한 이름이 인벤토리에 나타납니다.
- 6 NSX Edge 장치에 대한 계산 리소스를 선택합니다.
- 7 최적의 성능을 위해 NSX Edge 장치를 위한 메모리를 예약합니다.
NSX Edge가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정합니다. [NSX Edge VM 시스템 요구 사항](#)의 내용을 참조하십시오.
- 8 OVF 템플릿 세부 정보를 확인합니다.
- 9 NSX Edge 장치 파일을 저장할 데이터스토어를 선택합니다.
- 10 기본 소스 및 대상 네트워크 인터페이스를 수락합니다.
나머지 네트워크에 대해 기본 네트워크 대상을 수락하고 NSX Edge가 배포된 후에 네트워크 구성을 변경할 수 있습니다.
- 11 드롭다운 메뉴에서 IP 할당을 선택합니다.
- 12 NSX Edge 시스템 루트, CLI 관리자 및 감사 암호를 입력합니다.

참고 [템플릿 사용자 지정] 창에서 필드에 값을 입력하기 전에도 표시되는 메시지 모든 속성의 값이 올바른지는 무시합니다. 이 메시지는 모든 매개 변수가 선택 사항이므로 표시됩니다. 필드에 값을 입력하지 않아도 유효성 검사가 통과합니다.

암호는 암호 길이 제한을 준수해야 합니다.

- 12자 이상

- 하나 이상의 소문자
- 하나 이상의 대문자
- 하나 이상의 숫자
- 하나 이상의 특수 문자
- 5개 이상의 다른 문자
- 기본 암호 복잡성 규칙은 다음 Linux PAM 모듈 인수에 의해 적용됩니다.
 - **retry=3**: 오류 결과를 반환하기 전에 새 암호를 입력할 수 있는 최대 횟수로, 이 인수의 경우 최대 3번입니다.
 - **minlen=12**: 새 암호에 허용되는 최소 크기입니다. 새 암호의 문자 수 외에도 다른 종류의 문자 (예: 대문자, 소문자 및 숫자)에 대해 크레딧(길이에 +1)이 지정됩니다.
 - **difok=0**: 새 암호에서 달라야 하는 최소 바이트 수입니다. 이전 암호와 새 암호 간 유사성을 나타냅니다. difok에 값 0을 할당하면 이전 암호 및 새 암호 바이트를 다르게 유지할 필요가 없습니다. 정확한 일치가 허용됩니다.
 - **lcredit=1**: 새 암호에서 소문자에 대한 최대 크레딧입니다. 1개 이하의 소문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다.
 - **ucredit=1**: 새 암호에서 대문자에 대한 최대 크레딧입니다. 1개 이하의 대문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다.
 - **dcredit=1**: 새 암호에서 숫자에 대한 최대 크레딧입니다. 1개 이하의 숫자가 있는 경우 각 숫자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다.
 - **ocredit=1**: 새 암호에서 다른 문자에 대한 최대 크레딧입니다. 1개 이하의 다른 문자가 있는 경우 각 문자는 현재 minlen 값을 충족할 때까지 +1을 계산합니다.
 - **enforce_for_root**: 암호가 루트 사용자에게 대해 설정됩니다.

참고 사전 단어를 기준으로 암호를 확인하기 위한 Linux PAM 모듈에 대한 자세한 내용은 설명서 페이지를 참조하십시오.

예를 들어 **VMware123!123** 또는 **VMware12345**와 같이 간단하고 규칙적인 암호는 사용하지 마십시오. 복잡성 표준을 충족하는 암호는 간단하고 체계적이지 않지만 문자, 알파벳, 특수 문자 및 숫자 조합(예: **VMware123!45**, **VMware1!2345** 또는 **VMware@1az23x**)입니다.

- 13** (선택 사항) 사용 가능한 NSX Manager가 있고 OVA 배포 중에 NSX Edge를 관리부에 등록하려는 경우에는 Manager IP, 지문 및 토큰 필드를 완료합니다.

- a 상위 NSX Manager 노드 IP 주소 및 지문을 입력합니다.
- b API 호출 POST `https://<nsx-manager>/api/v1/aaa/registration-token`을 실행하여 NSX Manager 토큰을 검색합니다.

```
{
  "token": "4065a7c0-9658-4058-bb01-c149f20f238a",
  "roles": [
    "enterprise_admin"
  ],
  "user": "admin"
}
```

- c NSX Manager 토큰을 입력합니다.

참고 [노드 UUID] 필드는 내부용으로만 사용됩니다. 이 필드는 비워 둡니다.

- 14** NSX Edge VM의 호스트 이름을 입력합니다.
- 15** 기본 게이트웨이, 관리 네트워크 IPv4, 관리 네트워크 넷마스크, DNS 및 NTP IP 주소를 입력합니다.

참고 VMC 설정은 무시합니다. VMC 배포에 대한 값만 입력합니다.

- 16** (선택 사항) 콘솔을 사용하여 NSX Edge에 액세스하려는 경우 SSH를 사용하도록 설정하지 마십시오. 그러나 NSX Edge 명령줄에 대해 루트 SSH 로그인 및 CLI 로그인을 사용하려면 SSH 옵션을 사용하도록 설정합니다.

기본적으로 보안 때문에 SSH 액세스는 사용하지 않도록 설정됩니다.

- 17** 모든 사용자 지정 OVA 템플릿 규격이 정확한지 확인하고 **완료**를 클릭하여 설치를 시작합니다.

설치가 완료되는 데는 7-8분 정도 걸릴 수 있습니다.

- 18** NSX Edge의 콘솔을 열어 부팅 프로세스를 추적합니다.

콘솔 창이 열리지 않으면 팝업을 허용했는지 확인합니다.

- 19** NSX Edge가 시작되면 관리자 자격 증명을 사용하여 CLI에 로그인합니다.

참고 NSX Edge가 시작된 후 처음에 관리 자격 증명으로 로그인하지 않는 경우 데이터부 서비스가 NSX Edge에서 자동으로 시작되지 않습니다.

- 20** `get interface eth0`(VLAN 없음) 또는 `get interface eth0.<vlan_ID>`(VLAN 있음) 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

```
nsx-edge-1> get interface eth0.100
```

```
Interface: eth0.100
Address: 192.168.110.37/24
MAC address: 00:50:56:86:62:4d
```

```
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

참고 NSX 비관리형 호스트에서 NSX Edge VM을 작동할 때 데이터 NIC에 대한 물리적 호스트 스위치에서 MTU 설정이 1600(1500 아님)으로 설정되어 있는지 확인합니다.

21 `get managers` 명령을 실행하여 NSX Edge가 등록되었는지 확인합니다.

```
- 10.29.14.136 Standby
- 10.29.14.135 Standby
- 10.29.14.134 Connected
```

22 NSX Edge가 관리부에 등록되지 않은 경우 [NSX Edge를 관리부에 연결](#)을 참조하십시오.

23 해당 NSX Edge 장치에 필요한 연결이 있는지 확인합니다.

SSH를 사용하도록 설정한 경우 NSX Edge에 대해 SSH를 수행할 수 있는지 확인합니다.

- NSX Edge를 Ping할 수 있습니다.
- NSX Edge에서 기본 게이트웨이를 Ping할 수 있습니다.
- NSX Edge에서는 NSX Edge와 동일한 네트워크에 있는 하이퍼바이저 호스트를 Ping할 수 있습니다.
- NSX Edge에서는 DNS 서버와 해당 NTP 서버를 Ping할 수 있습니다.

24 연결 문제를 해결합니다.

참고 연결이 설정되지 않은 경우 VM 네트워크 어댑터가 적절한 네트워크 또는 VLAN에 있는지 확인합니다.

기본적으로 NSX Edge 데이터 경로는 관리 NIC(IP 주소 및 기본 경로가 있는 NIC)를 제외한 모든 가상 시스템 NIC를 할당합니다. NIC를 관리 인터페이스로 잘못 할당한 경우 다음 단계에 따라 DHCP를 사용하여 관리 IP 주소를 올바른 NIC에 할당합니다.

- a CLI에 로그인하고 `stop service dataplane` 명령을 입력합니다.
- b `set interface interface dhcp plane mgmt` 명령을 입력합니다.
- c *interface*를 DHCP 네트워크에 배치하고 IP 주소가 해당 *interface*에 할당될 때까지 기다립니다.
- d `start service dataplane` 명령을 입력합니다.

VLAN 업링크 및 터널 오버레이에 사용되는 데이터 경로 `fp-ethX` 포트가 NSX Edge의 `get interfaces` 및 `get physical-port` 명령에 표시됩니다.

다음에 수행할 작업

NSX Edge를 전송 노드로 구성합니다. [NSX Edge를 전송 노드로 구성](#) 항목을 참조하십시오.

명령줄 OVF 도구를 사용하여 ESXi에 NSX Edge 설치

NSX Edge 설치를 자동화하려면 명령줄 유틸리티인 VMware OVF Tool을 사용하면 됩니다.

사전 요구 사항

- 시스템 요구 사항이 충족되었는지 확인합니다. [시스템 요구 사항](#)의 내용을 참조하십시오.
- 필수 포트가 열려 있는지 확인합니다. [포트 및 프로토콜](#)의 내용을 참조하십시오.
- 데이터스토어가 구성되었고 ESXi 호스트에서 액세스할 수 있는지 확인합니다.
- NSX Manager에서 사용할 IP 주소와 게이트웨이, DNS 서버 IP 주소, 도메인 검색 목록 및 NTP 서버 IP 주소가 있는지 확인합니다.
- 대상 VM 포트 그룹 네트워크가 아직 없으면 생성합니다. NSX-T Data Center 장치를 관리 VM 네트워크에 배치합니다.

여러 관리 네트워크가 있으면 NSX-T Data Center 장치에서 다른 네트워크로의 정적 경로를 추가할 수 있습니다.
- NSX Manager IPv4 IP 주소 지정 체계를 계획합니다.
- [NSX Edge 설치 요구 사항](#)의 NSX Edge 네트워크 요구 사항을 참조하십시오.
- ESXi 호스트에 OVF 템플릿을 배포하기 위한 적절한 권한이 있는지 확인합니다.
- 호스트 이름에 밑줄이 포함되지 않았는지 확인합니다. 그렇지 않으면 호스트 이름이 *localhost*로 설정됩니다.
- OVF Tool 버전 4.3 이상
- NSX Edge VM을 배포하고 관리부에 가입시키는 데 사용할 수 있는 매개 변수를 확인합니다.

필드 이름	OVF 매개 변수	필드 유형
시스템 루트 암호	nsx_passwd_0	NSX Edge를 설치하는 데 필요합니다.
CLI 관리자 암호	nsx_cli_passwd_0	NSX Edge를 설치하는 데 필요합니다.
CLI 감사 암호	nsx_cli_audit_passwd_0	선택 사항
CLI 관리자 사용자 이름	nsx_cli_username	선택 사항
CLI 감사 사용자 이름	nsx_cli_audit_username	선택 사항
NSX Manager IP	mpIp	NSX Edge VM을 NSX Manager에 가입시키는 데 필요합니다.
NSX Manager 토큰	mpToken	NSX Edge VM을 NSX Manager에 가입시키는 데 필요합니다. 토큰을 검색하려면 NSX Manager에서 POST https://<nsx-manager>/api/v1/aaa/registration-token을 실행합니다.

필드 이름	OVF 매개 변수	필드 유형
NSX Manager 지문	mpThumbprint	NSX Edge VM을 NSX Manager에 가입시키는 데 필요합니다. 지문을 검색하려면 NSX Manager 노트에서 <code>get certificate api thumbprint</code> 를 실행합니다.
노드 ID	mpNodeId	내부용으로만 사용됩니다.
호스트 이름	nsx_hostname	선택 사항
기본 IPv4 게이트웨이	nsx_gateway_0	선택 사항
관리 네트워크 IP 주소	nsx_ip_0	선택 사항
관리 네트워크 넷마스크	nsx_netmask_0	선택 사항
DNS 서버	nsx_dns1_0	선택 사항
도메인 검색 접미사	nsx_domain_0	선택 사항
NTP 서버	nsx_ntp_0	선택 사항
SSH 서비스 사용	nsx_isSSHEnabled	선택 사항
루트 로그인에 SSH 사용	nsx_allowSSHRootLogin	선택 사항

절차

- ◆ 독립 실행형 호스트의 경우 해당 매개 변수를 사용하여 `ovftool` 명령을 실행합니다.

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-edge-1
--deploymentOption=medium
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net:"Network 0=Mgmt"
--net:"Network 1=nsx-tunnel"
--net:"Network 2=vlan-uplink"
--net:"Network 3=vlan-uplink"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.37
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=True
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
```

```
--prop:mpIp=<NSXManager-IP>
--prop:mpToken=<NSXManager-Token>
--prop:mpThumbprint=<NSXManager-Thumbprint>
<path/url to nsx component ova>
vi://root:<password>@192.168.110.51
```

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://root@192.168.110.24
Deploying to VI: vi://root@192.168.110.24
Transfer Completed
Powering on VM: nsx-edge-1
Task Completed
Completed successfully
```

- ◆ vCenter Server에서 관리되는 호스트의 경우 해당 매개 변수를 사용하여 **ovftool** 명령을 실행합니다.

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-edge-1
--deploymentOption=medium
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net:"Network 0=Mgmt"
--net:"Network 1=nsx-tunnel"
--net:"Network 2=vlan-uplink"
--net:"Network 3=vlan-uplink"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.37
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=True
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
--prop:mpIp=<NSXManager-IP>
--prop:mpToken=<NSXManager-Token>
```



```
--prop:mpThumbprint=<NSXManager-Thumbprint>
<path/url to nsx component ova>
vi://administrator@vsphere.local:<password>@192.168.110.24/?ip=192.168.210.53
```

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://administrator@vsphere.local@192.168.110.24:443/
Deploying to VI: vi://administrator@vsphere.local@192.168.110.24:443/
Transfer Completed
Powering on VM: nsx-edge-1
Task Completed
Completed successfully
```

- ◆ 최적의 성능을 위해 장치를 위한 메모리를 예약합니다.

NSX Manager가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정합니다. [NSX Manager VM 및 호스트 전송 노드 시스템 요구 사항](#)의 내용을 참조하십시오.

- ◆ NSX Edge의 콘솔을 열어 부팅 프로세스를 추적합니다.
- ◆ NSX Edge가 시작되면 관리자 자격 증명을 사용하여 CLI에 로그인합니다.
- ◆ `get interface eth0`(VLAN 없음) 또는 `get interface eth0.<vlan_ID>`(VLAN 있음) 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
Address: 192.168.110.37/24
MAC address: 00:50:56:86:62:4d
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

참고 NSX 비관리형 호스트에서 NSX Edge VM을 작동할 때 데이터 NIC에 대한 물리적 호스트 스위치에서 MTU 설정이 1600(1500 아님)으로 설정되어 있는지 확인합니다.

- ◆ 해당 NSX Edge 장치에 필요한 연결이 있는지 확인합니다.
- SSH를 사용하도록 설정한 경우 NSX Edge에 대해 SSH를 수행할 수 있는지 확인합니다.
- NSX Edge를 Ping할 수 있습니다.
 - NSX Edge에서 기본 게이트웨이를 Ping할 수 있습니다.
 - NSX Edge에서는 NSX Edge와 동일한 네트워크에 있는 하이퍼바이저 호스트를 Ping할 수 있습니다.
 - NSX Edge에서는 DNS 서버와 해당 NTP 서버를 Ping할 수 있습니다.

- ◆ 연결 문제를 해결합니다.

참고 연결이 설정되지 않은 경우 VM 네트워크 어댑터가 적절한 네트워크 또는 VLAN에 있는지 확인합니다.

기본적으로 NSX Edge 데이터 경로는 관리 NIC(IP 주소 및 기본 경로가 있는 NIC)를 제외한 모든 가상 시스템 NIC를 할당합니다. NIC를 관리 인터페이스로 잘못 할당한 경우 다음 단계에 따라 DHCP를 사용하여 관리 IP 주소를 올바른 NIC에 할당합니다.

- CLI에 로그인하고 **stop service dataplane** 명령을 입력합니다.
- set interface *interface* dhcp plane mgmt** 명령을 입력합니다.
- interface*를 DHCP 네트워크에 배치하고 IP 주소가 해당 *interface*에 할당될 때까지 기다립니다.
- start service dataplane** 명령을 입력합니다.

VLAN 업링크 및 터널 오버레이에 사용되는 데이터 경로 fp-ethX 포트가 NSX Edge의 **get interfaces** 및 **get physical-port** 명령에 표시됩니다.

다음에 수행할 작업

NSX Edge를 관리부에 가입시키지 않은 경우 [NSX Edge를 관리부에 연결](#)을 참조하십시오.

ISO 파일을 통해 가상 장치로 NSX Edge 설치

ISO 파일을 사용하여 수동 방식으로 NSX Edge VM을 설치할 수 있습니다.

중요 NSX-T Data Center 구성 요소 가상 시스템 설치에는 VMware Tools가 포함됩니다. NSX-T Data Center 장치의 경우 VMware Tools의 제거 또는 업그레이드가 지원되지 않습니다.

사전 요구 사항

- [NSX Edge 설치 요구 사항](#)의 NSX Edge 네트워크 요구 사항을 참조하십시오.

절차

- 1 MyVMware 계정(myvmware.com)으로 이동하고 **VMware NSX-T Data Center > 다운로드**로 이동합니다.
- 2 NSX Edge용 ISO 파일을 찾아 다운로드합니다.
- 3 vSphere Client에서 호스트 데이터스토어를 선택합니다.
- 4 **파일 > 파일 업로드 > 데이터스토어에 파일 업로드**를 선택하고 ISO 파일을 찾아서 업로드합니다.
자체 서명 인증서를 사용하는 경우 브라우저에서 IP 주소를 열고 인증서를 수락하고 ISO 파일을 다시 업로드합니다.
- 5 vSphere Client 인벤토리에서 ISO 파일을 업로드한 호스트를 선택합니다. 또는 vSphere Client에서
- 6 마우스 오른쪽 버튼을 클릭하고 **새 가상 시스템**을 선택합니다.
- 7 NSX Edge 장치에 대한 계산 리소스를 선택합니다.

- 8 NSX Edge 장치 파일을 저장할 데이터스토어를 선택합니다.
- 9 NSX Edge VM에 대한 기본 호환성을 적용합니다.
- 10 NSX Edge VM에 지원되는 ESXi 운영 체제를 선택합니다.
- 11 가상 하드웨어를 구성합니다.

- 새 하드 디스크 - **200GB**
- 새 네트워크 - **VM 네트워크**
- 새 CD/DVD 드라이브 - **데이터스토어 ISO 파일**

연결을 클릭하여 NSX Edge ISO 파일을 VM에 바인딩해야 합니다.

- 12 새 NSX Edge VM의 전원을 켭니다.
- 13 ISO 부팅 중에 VM 콘솔을 열고 **자동 설치**를 선택합니다.

Enter 키를 누른 후에 10초 동안 일시 중단될 수 있습니다.

설치하는 동안 관리 인터페이스의 VLAN ID를 입력하라는 메시지가 표시됩니다. **예**를 선택하고 VLAN ID를 입력하여 네트워크 인터페이스에 대한 VLAN 하위 인터페이스를 생성합니다. 패킷에 VLAN 태깅을 구성하지 않으려면 **아니요**를 선택하십시오.

전원이 켜지는 동안 VM은 DHCP를 통해 네트워크 구성을 요청합니다. 운영 환경에서 DHCP를 사용할 수 없으면 설치 관리자가 IP 설정을 지정하라는 메시지를 표시합니다.

기본적으로 루트 로그인 암호는 **vmware**이고 관리자 로그인 암호는 **default**입니다.

처음 로그인할 때 암호를 변경하라는 메시지가 표시됩니다. 이 암호 변경 방법은 다음을 포함하는 엄격한 복잡도 규칙을 갖습니다.

- 12자 이상
- 하나 이상의 소문자
- 하나 이상의 대문자
- 하나 이상의 숫자
- 하나 이상의 특수 문자
- 5개 이상의 다른 문자
- 사전 단어 제외
- 회문 제외
- 4자를 초과하는 단조 문자 시퀀스는 허용되지 않습니다.

중요 장치의 핵심 서비스는 충분한 복잡도를 갖는 암호를 설정해야만 시작할 수 있습니다.

- 14** 최적의 성능을 위해 NSX Edge 장치를 위한 메모리를 예약합니다.

NSX Edge가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정합니다. [NSX Edge VM 시스템 요구 사항](#)의 내용을 참조하십시오.

- 15** NSX Edge가 시작되면 관리자 자격 증명을 사용하여 CLI에 로그인합니다.

참고 NSX Edge가 시작된 후 처음에 관리 자격 증명으로 로그인하지 않는 경우 데이터부 서비스가 NSX Edge에서 자동으로 시작되지 않습니다.

- 16** 관리 인터페이스를 구성하는 방법에는 세 가지가 있습니다.

참고 서버가 Mellanox NIC 카드를 사용하는 경우 대역 내 관리 인터페이스에서 Edge를 구성하지 마십시오.

- 태그가 지정되지 않은 인터페이스. 이 인터페이스 유형은 대역외 관리 인터페이스를 생성합니다.

```
(DHCP) set interface eth0 dhcp plane mgmt
```

```
(정적) set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt
```

- 태그가 지정된 인터페이스.

```
set interface eth0 vlan <vlan_ID> plane mgmt
```

```
(DHCP)set interface eth0.<vlan_ID> dhcp plane mgmt
```

```
(정적)set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt
```

- 대역내 인터페이스.

```
set interface mac <mac_address> vlan <vlan_ID> in-band plane mgmt
```

```
(DHCP) set interface eth0.<vlan_ID> dhcp plane mgmt
```

```
(정적) set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt
```

- 17** (선택 사항) SSH 서비스를 시작합니다. `start service ssh`를 실행합니다.

- 18** `get interface eth0`(VLAN 없음) 또는 `get interface eth0.<vlan_ID>`(VLAN 있음) 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

```
nsx-edge-1> get interface eth0.100
```

```
Interface: eth0.100
```

```
Address: 192.168.110.37/24
```

```
MAC address: 00:50:56:86:62:4d
```

```
MTU: 1500
```

```
Default gateway: 192.168.110.1
```

```
Broadcast address: 192.168.110.255
```

```
...
```

참고 NSX 비관리형 호스트에서 NSX Edge VM을 작동할 때 데이터 NIC에 대한 물리적 호스트 스위치에서 MTU 설정이 1600(1500 아님)으로 설정되어 있는지 확인합니다.

- 19** (태그가 지정된 인터페이스 및 대역내 인터페이스) 인터페이스를 새로 생성하기 전에 기존 VLAN 관리 인터페이스를 먼저 제거해야 합니다.

```
Clear interface eth0.<vlan_ID>
```

새 인터페이스를 설정하려면 15 단계를 참조하십시오.

- 20** 해당 NSX Edge 장치에 필요한 연결이 있는지 확인합니다.

SSH를 사용하도록 설정한 경우 NSX Edge에 대해 SSH를 수행할 수 있는지 확인합니다.

- NSX Edge를 Ping할 수 있습니다.
- NSX Edge에서 기본 게이트웨이를 Ping할 수 있습니다.
- NSX Edge에서는 NSX Edge와 동일한 네트워크에 있는 하이퍼바이저 호스트를 Ping할 수 있습니다.
- NSX Edge에서는 DNS 서버와 해당 NTP 서버를 Ping할 수 있습니다.

- 21** 연결 문제를 해결합니다.

참고 연결이 설정되지 않은 경우 VM 네트워크 어댑터가 적절한 네트워크 또는 VLAN에 있는지 확인합니다.

기본적으로 NSX Edge 데이터 경로는 관리 NIC(IP 주소 및 기본 경로가 있는 NIC)를 제외한 모든 가상 시스템 NIC를 할당합니다. NIC를 관리 인터페이스로 잘못 할당한 경우 다음 단계에 따라 DHCP를 사용하여 관리 IP 주소를 올바른 NIC에 할당합니다.

- a CLI에 로그인하고 **stop service dataplane** 명령을 입력합니다.
- b **set interface interface dhcp plane mgmt** 명령을 입력합니다.
- c *interface*를 DHCP 네트워크에 배치하고 IP 주소가 해당 *interface*에 할당될 때까지 기다립니다.
- d **start service dataplane** 명령을 입력합니다.

VLAN 업링크 및 터널 오버레이에 사용되는 데이터 경로 fp-ethX 포트가 NSX Edge의 **get interfaces** 및 **get physical-port** 명령에 표시됩니다.

다음에 수행할 작업

NSX Edge를 관리부에 가입시키지 않은 경우 [NSX Edge를 관리부에 연결](#)의 내용을 참조하십시오.

베어 메탈에 NSX Edge 설치

PXE 서버를 사용하여 베어메탈 서버에서 NSX Edge의 설치를 자동화하거나 ISO 파일을 사용하여 NSX Edge를 VM 장치로 또는 베어메탈 서버에 설치합니다.

NSX Manager에 대해서는 PXE 부팅 설치가 지원되지 않습니다. IP 주소, 게이트웨이, 네트워크 마스크, NTP 및 DNS와 같은 네트워킹 설정도 구성할 수 없습니다.

사전 요구 사항

- NSX Edge 베어메탈 서버에서 버전 6.7u3 또는 이전 버전을 실행 중인 경우 vCenter Server에서 NSX Edge virtualHW.version을 14 이상으로 업그레이드하지 마십시오. 기본적으로 virtualHW.version은 13으로 설정되어 있습니다.
- 기본적으로, 이더넷 디바이스를 집계하여 LAG를 형성하는 NSX Edge 베어메탈 결합 디바이스는 로드 밸런싱에 맞게 최적화됩니다. 따라서, 결합 디바이스는 CPU가 패킷을 전송하는 로컬 NUMA 노드에 있는 네트워크 디바이스만 사용합니다. 결합을 형성하는 디바이스가 여러 NUMA 노드에 걸쳐 있지만 패킷 처리에 할당된 CPU가 NUMA 노드의 하위 집합에 속하는 경우 일부 디바이스만 트래픽을 전송합니다. 간단히 말해서 결합 디바이스에서 전송된 트래픽을 밸런싱하는 데 모든 디바이스가 사용되는 것은 아닙니다. 기본 최적화는 사용하지 않도록 설정할 수 없습니다.

그러나 결합의 모든 이더넷 디바이스를 사용하여 트래픽을 로드 밸런싱하려면 모든 이더넷 디바이스를 패킷 처리 CPU가 연결된 NUMA 노드로 이동해야 합니다.

참고 페일오버와 로드 밸런싱은 상호 배타적입니다. 로컬 NUMA 노드에 연결된 이더넷 디바이스가 종료된 경우, 결합 디바이스는 NUMA 로컬이 아닌 경우에도 다른 디바이스로 트래픽을 전송합니다. 로드 밸런싱 최적화는 페일오버 기능에 영향을 주지 않습니다.

NSX Edge를 위한 PXE 서버 준비

PXE는 여러 구성 요소, 즉 DHCP, HTTP 및 TFTP로 구성됩니다. 이 절차에서는 Ubuntu에서 PXE 서버를 설치하는 방법을 보여줍니다.

DHCP는 NSX Edge와 같은 NSX-T Data Center 구성 요소에 동적으로 IP 설정을 배포합니다. PXE 환경에서 DHCP 서버는 NSX Edge에서 IP 주소를 자동으로 요청하고 수신하도록 합니다.

TFTP는 파일 전송 프로토콜입니다. TFTP 서버는 항상 네트워크에서 PXE 클라이언트를 수신합니다. 이 서버는 PXE 서비스를 요청하는 네트워크 PXE 클라이언트를 감지하면 NSX-T Data Center 구성 요소 ISO 파일과 미리 시드된 파일에 포함된 설치 설정을 제공합니다.

사전 요구 사항

- 배포 환경에서 PXE 서버를 사용할 수 있어야 합니다. PXE 서버는 어떤 Linux 배포판에도 설치할 수 있습니다. PXE 서버에는 외부 통신용 인터페이스 1개와 DHCP IP 및 TFTP 서비스를 제공하는 인터페이스 1개가 있어야 합니다.
- 여러 관리 네트워크가 있으면 NSX-T Data Center 장치에서 다른 네트워크로의 정적 경로를 추가할 수 있습니다.
- 미리 시드된 구성 파일에 net.ifnames=0 및 biosdevname=0 매개 변수가 설정되어 있는지 확인하여 -- 재부팅 후에도 지속되도록 합니다.
 - **NSX Edge 설치 요구 사항**의 NSX Edge 네트워크 요구 사항을 참조하십시오.

절차

- 1 (선택 사항) kickstart 파일을 사용하여 Ubuntu 서버에서 새로운 TFTP 또는 DHCP 서비스를 설정합니다.

kickstart 파일은 첫 번째 부팅 후에 장치에서 실행하는 CLI 명령이 포함된 텍스트 파일입니다.

가리키는 PXE 서버를 기준으로 kickstart 파일의 이름을 지정합니다. 예:

```
nsxcli.install
```

파일을 웹 서버(예: /var/www/html/nsx-edge/nsxcli.install)에 복사해야 합니다.

kickstart 파일에서 CLI 명령을 추가할 수 있습니다. 예를 들어, 관리 인터페이스의 IP 주소를 구성하려면:

```
stop dataplane
set interface eth0 <ip-cidr-format> plane mgmt
start dataplane
```

관리자 암호를 변경하려면:

```
set user admin password <new_password> old-password <old-password>
```

preseed.cfg 파일에 암호를 지정하는 경우 kickstart 파일에 지정한 암호와 동일한 암호를 사용합니다. 그렇지 않을 경우 기본 암호인 "default"를 사용합니다.

NSX Edge를 관리부에 연결하려면:

```
join management-plane <manager-ip> thumbprint <manager-thumbprint> username <manager-username>
password <manager password>
```

- 2 관리용 인터페이스 1개와 DHCP 및 TFTP 서비스용 인터페이스 1개를 생성합니다.

DHCP/TFTP 인터페이스가 NSX Edge가 상주하는 동일한 서브넷에 있는지 확인합니다.

예를 들어 NSX Edge 관리 인터페이스가 192.168.210.0/24 서브넷에 배치될 예정이면 eth1도 동일한 서브넷에 배치합니다.

```
# The loopback network interface
auto lo
iface lo inet loopback

# PXE server's management interface
auto eth0
iface eth0 inet static
    address 192.168.110.81
    gateway 192.168.110.1
    netmask 255.255.255.0
    dns-nameservers 192.168.110.10

# PXE server's DHCP/TFTP interface
auto eth1
```

```

iface eth1 inet static
    address 192.168.210.82
    gateway 192.168.210.1
    netmask 255.255.255.0
    dns-nameservers 192.168.110.10

```

- 3 DHCP 서버 소프트웨어를 설치합니다.

```
sudo apt-get install isc-dhcp-server -y
```

- 4 /etc/default/isc-dhcp-server 파일을 편집하고 DHCP 서비스를 제공하는 인터페이스를 추가합니다.

```
INTERFACES="eth1"
```

- 5 (선택 사항) 이 DHCP 서버를 로컬 네트워크에 대한 공식 DHCP 서버로 지정하려면 /etc/dhcp/dhcpd.conf 파일에서 **authoritative;** 줄의 주석 처리를 해제합니다.

```

...
authoritative;
...

```

- 6 /etc/dhcp/dhcpd.conf 파일에서 PXE 네트워크에 대한 DHCP 설정을 정의합니다.

예:

```

subnet 192.168.210.0 netmask 255.255.255.0 {
    range 192.168.210.90 192.168.210.95;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 192.168.110.10;
    option routers 192.168.210.1;
    option broadcast-address 192.168.210.255;
    default-lease-time 600;
    max-lease-time 7200;
}

```

- 7 DHCP 서비스를 시작합니다.

```
sudo service isc-dhcp-server start
```

- 8 DHCP 서비스가 실행 중인지 확인합니다.

```
service --status-all | grep dhcp
```

- 9 PXE 부팅에 필요한 Apache, TFTP 및 기타 구성 요소를 설치합니다.

```
sudo apt-get install apache2 tftpd-hpa inetutils-inetd
```


10 TFTP와 Apache가 실행 중인지 확인합니다.

```
service --status-all | grep tftpd-hpa
service --status-all | grep apache2
```

11 /etc/default/tftpd-hpa 파일에 다음 줄을 추가합니다.

```
RUN_DAEMON="yes"
OPTIONS="-l -s /var/lib/tftpboot"
```

12 /etc/inetd.conf 파일에 다음 줄을 추가합니다.

```
tftp      dgram    udp      wait     root     /usr/sbin/in.tftpd /usr/sbin/in.tftpd -s /var/lib/tftpboot
```

13 TFTP 서비스를 다시 시작합니다.

```
sudo /etc/init.d/tftpd-hpa restart
```

14 NSX Edge 설치 관리자 ISO 파일을 임시 폴더에 복사하거나 다운로드합니다.**15** ISO 파일을 마운트하고 설치 구성 요소를 TFTP 서버 및 Apache 서버로 복사합니다.

```
sudo mount -o loop ~/nsx-edge.<build>.iso /mnt
cd /mnt
sudo cp -fr install/netboot/* /var/lib/tftpboot/
sudo mkdir /var/www/html/nsx-edge
sudo cp -fr /mnt/* /var/www/html/nsx-edge/
```

16 (선택 사항) `/var/www/html/nsx-edge/preseed.cfg` 파일을 편집하여 암호화된 암호를 수정합니다.

`mkpasswd`와 같은 Linux 도구를 사용하여 암호 해시를 생성할 수 있습니다.

```
sudo apt-get install whois
sudo mkpasswd -m sha-512
```

```
Password:
$6$SUFQs[...]FcoHLij0uFD
```

- a 루트 암호를 수정하고, `/var/www/html/nsx-edge/preseed.cfg`를 편집하고 다음 줄을 검색합니다.

```
d-i passwd/root-password-crypted password $6$tgmlNLMP$9BuAHhN...
```

- b 해시 문자열을 바꿉니다.

`$`, `,`, `"` 또는 `\`와 같은 특수 문자는 이스케이프할 필요가 없습니다.

- c `preseed.cfg`에 `usermod` 명령을 추가하여 루트나 관리자 또는 둘 다의 암호를 설정합니다.

예를 들어 `echo 'VMware NSX Edge'` 줄을 검색하고 다음 명령을 추가합니다.

```
usermod --password '\$6\$VS3exId0aKmw\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00b02hUF8u/' root; \
usermod --password '\$6\$VS3exId0aKmw\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00b02hUF8u/' admin; \
```

해시 문자열은 예일 뿐입니다. 모든 특수 문자는 이스케이프해야 합니다. 첫 번째 `usermod` 명령의 루트 암호는 `d-i passwd/root-password-crypted password 6tgml...`에 설정된 암호를 대신합니다.

`usermod` 명령을 사용하여 암호를 설정하는 경우 처음 로그인할 때 암호를 변경하라는 메시지가 표시되지 않습니다. 그러지 않은 경우 처음 로그인 시 암호를 변경해야 합니다.

17 `/var/lib/tftpboot/pxe/linux.cfg/default` 파일에 다음 줄을 추가합니다.

192.168.210.82를 TFTP 서버의 IP 주소로 바꿉니다.

```
label nsxedge
  kernel ubuntu-installer/amd64/linux
  ipappend 2
  append netcfg/dhcp_timeout=60 auto=true priority=critical vga=normal partman-lvm/
device_remove_lvm=true netcfg/choose_interface=auto debian-installer/allow_unauthenticated=true
preseed/url=http://192.168.210.82/nsx-edge/preseed.cfg mirror/country=manual mirror/http/
hostname=192.168.210.82 nsx-kickstart/url=http://192.168.210.82/nsx-edge/nsxcli.install mirror/
http/directory=/nsx-edge initrd=ubuntu-installer/amd64/initrd.gz mirror/suite=xenial --
```

18 /etc/dhcp/dhcpd.conf 파일에 다음 줄을 추가합니다.

192.168.210.82를 DHCP 서버의 IP 주소로 바꿉니다.

```
allow booting;
allow bootp;

next-server 192.168.210.82; #Replace this IP address
filename "pxelinux.0";
```

19 DHCP 서비스를 다시 시작합니다.

```
sudo service isc-dhcp-server restart
```

참고 오류가 반환되면(예: "중지: 알 수 없는 인스턴스: 시작: 작업 시작 실패") `sudo /etc/init.d/isc-dhcp-server stop`을 실행한 다음 `sudo /etc/init.d/isc-dhcp-server start`를 실행합니다. `sudo /etc/init.d/isc-dhcp-server start` 명령은 오류 원인에 대한 정보를 반환합니다.

다음에 수행할 작업

ISO 파일을 사용하여 베어메탈에 NSX Edge를 설치합니다. [ISO 파일을 통해 자동으로 NSX Edge 설치](#)의 내용을 참조하십시오.

ISO 파일을 통해 자동으로 NSX Edge 설치

ISO 파일을 사용하여 베어 메탈에 수동 방식으로 NSX Edge 디바이스를 설치할 수 있습니다. 여기에는 IP 주소, 게이트웨이, 네트워크 마스크, NTP 및 DNS와 같은 네트워킹 설정 구성이 포함됩니다.

사전 요구 사항

- 시스템 BIOS 모드가 레거시 BIOS로 설정되어 있는지 확인합니다.
- [NSX Edge 설치 요구 사항](#)의 NSX Edge 네트워크 요구 사항을 참조하십시오.

절차

- 1** MyVMware 계정(myvmware.com)으로 이동하고 **VMware NSX-T Data Center > 다운로드**로 이동합니다.
- 2** 베어메탈을 위한 NSX Edge용 ISO 파일을 찾아 다운로드합니다.
- 3** 베어메탈의 대역 외 관리 인터페이스(예: HP 서버의 ILO(Integrated Lights-Out))에 로그인합니다.
- 4** 가상 콘솔 미리보기에서 **시작**을 클릭합니다.
- 5** **가상 미디어 > 가상 미디어 연결**을 선택합니다.
가상 미디어가 연결될 때까지 잠시 기다립니다.
- 6** **가상 미디어 > CD/DVD 매핑**을 선택하고 ISO 파일을 찾습니다.
- 7** **다음 부팅 > 가상 CD/DVD/ISO**를 선택합니다.

8 전원 > 시스템 재설정(웜 부팅)을 선택합니다.

설치 시간은 베어메탈 환경에 따라 다릅니다.

9 자동 설치를 선택합니다.

Enter 키를 누른 후에 10초 동안 일시 중단될 수 있습니다.

10 해당하는 기본 네트워크 인터페이스를 선택합니다.

전원이 켜지는 동안 설치 관리자는 DHCP를 통해 네트워크 구성을 요청합니다. 운영 환경에서 DHCP를 사용할 수 없으면 설치 관리자가 IP 설정을 지정하라는 메시지를 표시합니다.

기본적으로 루트 로그인 암호는 **vmware**이고 관리자 로그인 암호는 **default**입니다.

11 NSX Edge의 콘솔을 열어 부팅 프로세스를 추적합니다.

콘솔 창이 열리지 않으면 팝업을 허용했는지 확인합니다.

12 NSX Edge가 시작되면 관리자 자격 증명을 사용하여 CLI에 로그인합니다.

참고 NSX Edge가 시작된 후 처음에 관리 자격 증명으로 로그인하지 않는 경우 데이터부 서비스가 NSX Edge에서 자동으로 시작되지 않습니다.

13 재부팅 후 관리 또는 루트 자격 증명으로 로그인할 수 있습니다. 기본 루트 암호는 **vmware**입니다.**14** 관리 인터페이스를 구성하는 방법에는 세 가지가 있습니다.

참고 서버가 Mellanox NIC 카드를 사용하는 경우 대역 내 관리 인터페이스에서 Edge를 구성하지 마십시오.

- 태그가 지정되지 않은 인터페이스. 이 인터페이스 유형은 대역외 관리 인터페이스를 생성합니다.

```
(DHCP) set interface eth0 dhcp plane mgmt
```

```
(정적) set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt
```

- 태그가 지정된 인터페이스.

```
set interface eth0 vlan <vlan_ID> plane mgmt
```

```
(DHCP)set interface eth0.<vlan_ID> dhcp plane mgmt
```

```
(정적)set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt
```

- 대역내 인터페이스.

```
set interface mac <mac_address> vlan <vlan_ID> in-band plane mgmt
```

```
(DHCP) set interface eth0.<vlan_ID> dhcp plane mgmt
```

```
(정적) set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt
```

- (선택 사항) 여러 인터페이스를 사용하는 관리 HA 인터페이스에 대한 **bond0** 인터페이스를 생성합니다.

다음 CLI 명령을 사용하여 NSX Edge에 대한 결합 관리 인터페이스를 구성할 수 있습니다. 결합을 생성하고 인터페이스를 추가하기 전에 콘솔을 사용하여 기존 관리 IP를 지웁니다.

참고 결합 인터페이스에는 활성 백업 모드만 허용됩니다. VLAN을 구성하는 것은 허용되지 않습니다. 따라서 물리적 스위치에 더 가까운 액세스 VLAN에 VLAN을 구성해야 합니다.

```
set interface bond0 ip x.x.x.x/mask gateway x.x.x.x plane mgmt mode active-
backup members eth0, eth1 primary eth0
```

- 15** `get interface eth0`(VLAN 없음) 또는 `get interface eth0.<vlan_ID>`(VLAN 있음) 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
Address: 192.168.110.37/24
MAC address: 00:50:56:86:62:4d
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

참고 NSX 비관리형 호스트에서 NSX Edge VM을 작동할 때 데이터 NIC에 대한 물리적 호스트 스위치에서 MTU 설정이 1600(1500 아님)으로 설정되어 있는지 확인합니다.

- 16** (태그가 지정된 인터페이스 및 대역내 인터페이스) 인터페이스를 새로 생성하기 전에 기존 VLAN 관리 인터페이스를 먼저 제거해야 합니다.

```
clear interface eth0.<vlan_ID>
```

새 인터페이스를 설정하려면 13단계를 참조하십시오.

- 17** 사용 가능한 PCI 디바이스 목록에서 NSX-T Data Center 데이터부에서 사용할 물리적 NIC를 설정합니다.

- a `get dataplace device list`
- b `set dataplane device list <NIC1>, <NIC2>, <NIC3>`
- c `restart service dataplane`
- d `get physical-port`

물리적 NIC를 선택한 후 변경 사항을 적용하려면 NSX-T Data Center 데이터부 서비스를 다시 시작하십시오.

참고 최대 16개의 물리적 NIC를 할당합니다.

- 18** 네트워크 구성 오류를 방지하려면 선택한 물리적 NIC가 전송 노드 프로파일에 구성된 NIC와 일치하는지 확인합니다.

19 NSX Edge를 전송 노드로 생성하기 전에 데이터부에서 NIC 목록을 재설정하십시오.

```
reset dataplane nic list
```

20 해당 NSX Edge 장치에 필요한 연결이 있는지 확인합니다.

SSH를 사용하도록 설정한 경우 NSX Edge에 대해 SSH를 수행할 수 있는지 확인합니다.

- NSX Edge를 Ping할 수 있습니다.
- NSX Edge에서 기본 게이트웨이를 Ping할 수 있습니다.
- NSX Edge에서는 NSX Edge와 동일한 네트워크에 있는 하이퍼바이저 호스트를 Ping할 수 있습니다.
- NSX Edge에서는 DNS 서버와 해당 NTP 서버를 Ping할 수 있습니다.

21 연결 문제를 해결합니다.

참고 연결이 설정되지 않은 경우 VM 네트워크 어댑터가 적절한 네트워크 또는 VLAN에 있는지 확인합니다.

기본적으로 NSX Edge 데이터 경로는 관리 NIC(IP 주소 및 기본 경로가 있는 NIC)를 제외한 모든 가상 시스템 NIC를 할당합니다. NIC를 관리 인터페이스로 잘못 할당한 경우 다음 단계에 따라 DHCP를 사용하여 관리 IP 주소를 올바른 NIC에 할당합니다.

- a CLI에 로그인하고 **stop service dataplane** 명령을 입력합니다.
- b **set interface interface dhcp plane mgmt** 명령을 입력합니다.
- c *interface*를 DHCP 네트워크에 배치하고 IP 주소가 해당 *interface*에 할당될 때까지 기다립니다.
- d **start service dataplane** 명령을 입력합니다.

VLAN 업링크 및 터널 오버레이에 사용되는 데이터 경로 fp-ethX 포트가 NSX Edge의 **get interfaces** 및 **get physical-port** 명령에 표시됩니다.

다음에 수행할 작업

NSX Edge를 관리부에 가입시키지 않은 경우 [NSX Edge를 관리부에 연결](#)의 내용을 참조하십시오.

ISO 파일을 통해 대화형으로 NSX Edge 설치

대화형 모드에서 ISO 파일을 사용하여 베어메탈에 NSX Edge 디바이스를 설치합니다.

사전 요구 사항

- 시스템 BIOS 모드가 레거시 BIOS로 설정되어 있는지 확인합니다.
- [NSX Edge 설치 요구 사항](#)의 NSX Edge 네트워크 요구 사항을 참조하십시오.

절차

- 1** MyVMware 계정(myvmware.com)으로 이동하고 **VMware NSX-T Data Center > 다운로드**로 이동합니다.

- 2 베어메탈을 위한 NSX Edge용 ISO 파일을 찾아 다운로드합니다.
- 3 베어메탈의 ILO에 로그인합니다.
- 4 가상 콘솔 미리보기에서 **시작**을 클릭합니다.
- 5 **가상 미디어 > 가상 미디어 연결**을 선택합니다.
가상 미디어가 연결될 때까지 잠시 기다립니다.
- 6 **가상 미디어 > CD/DVD 매핑**을 선택하고 ISO 파일을 찾습니다.
- 7 **다음 부팅 > 가상 CD/DVD/ISO**를 선택합니다.
- 8 **전원 > 시스템 재설정(원 부팅)**을 선택합니다.
설치 시간은 베어메탈 환경에 따라 다릅니다.
- 9 **대화형 설치**를 선택합니다.
Enter 키를 누른 후에 10초 동안 일시 중단될 수 있습니다.
- 10 설치 관리자가 키보드를 자동으로 감지해야 하는 경우 [키보드 구성] 창에서 **예**를 선택하고, 콘솔에서 키보드를 감지하지 않아야 하는 경우 **아니요**를 선택합니다.
- 11 언어로 [영어(미국)]를 선택합니다.
- 12 [네트워크 구성] 창에서 해당하는 기본 네트워크 인터페이스를 선택합니다.
- 13 선택한 기본 인터페이스에 연결되는 호스트 이름을 입력하고 **확인**을 클릭합니다.
전원이 켜지는 동안 설치 관리자는 DHCP를 통해 네트워크 구성을 요청합니다. 운영 환경에서 DHCP를 사용할 수 없으면 설치 관리자가 IP 설정을 지정하라는 메시지를 표시합니다.
기본적으로 루트 로그인 암호는 **vmware**이고 관리자 로그인 암호는 **default**입니다.
- 14 [킵스타트를 사용하여 NSX 장치 구성] 창:
 - 베어메탈 서버의 NSX 구성을 자동화하려면 NSX 킵스타트 구성 파일의 URL을 입력합니다.
 - 베어메탈 서버에서 NSX를 수동으로 구성하려면 이 필드를 비워 둡니다.
- 15 [디스크 분할] 창에서 다음 옵션 중 하나를 선택합니다.
 - 새 파티션을 디스크에 생성할 수 있도록 기존 파티션을 마운트 해제하려면 **예**를 선택합니다.
 - 기존 파티션을 사용하려면 **아니요**를 선택합니다.
- 16 NSX Edge가 시작되면 관리자 자격 증명을 사용하여 CLI에 로그인합니다.

참고 NSX Edge가 시작된 후 처음에 관리 자격 증명으로 로그인하지 않는 경우 데이터부 서비스가 NSX Edge에서 자동으로 시작되지 않습니다.

- 17** `get interface eth0`(VLAN 없음) 또는 `get interface eth0.<vlan_ID>`(VLAN 있음) 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
Address: 192.168.110.37/24
MAC address: 00:50:56:86:62:4d
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

참고 NSX 비관리형 호스트에서 NSX Edge VM을 작동할 때 데이터 NIC에 대한 물리적 호스트 스위치에서 MTU 설정이 1600(1500 아님)으로 설정되어 있는지 확인합니다.

- 18** 연결 문제를 해결합니다.

참고 연결이 설정되지 않은 경우 VM 네트워크 어댑터가 적절한 네트워크 또는 VLAN에 있는지 확인합니다.

기본적으로 NSX Edge 데이터 경로는 관리 NIC(IP 주소 및 기본 경로가 있는 NIC)를 제외한 모든 가상 시스템 NIC를 할당합니다. NIC를 관리 인터페이스로 잘못 할당한 경우 다음 단계에 따라 DHCP를 사용하여 관리 IP 주소를 올바른 NIC에 할당합니다.

- CLI에 로그인하고 **stop service dataplane** 명령을 입력합니다.
- set interface *interface* dhcp plane mgmt** 명령을 입력합니다.
- interface*를 DHCP 네트워크에 배치하고 IP 주소가 해당 *interface*에 할당될 때까지 기다립니다.
- start service dataplane** 명령을 입력합니다.

VLAN 업링크 및 터널 오버레이에 사용되는 데이터 경로 `fp-ethX` 포트가 NSX Edge의 **get interfaces** 및 **get physical-port** 명령에 표시됩니다.

다음에 수행할 작업

NSX Edge를 관리부에 가입시키지 않은 경우 [NSX Edge를 관리부에 연결](#)을 참조하십시오.

NSX Edge를 관리부에 연결

NSX Edge를 관리부에 연결하면 NSX Manager 및 NSX Edge가 서로 통신할 수 있게 됩니다.

사전 요구 사항

NSX Edge 및 NSX Manager 장치에 로그인할 수 있는 관리자 권한이 있는지 확인합니다.

절차

- NSX Manager 장치 중 하나에 대한 SSH 세션 또는 콘솔 세션을 엽니다.

- 2 NSX Edge 노드 VM에 대한 SSH 세션 또는 콘솔 세션을 엽니다.
- 3 NSX Manager 장치에서 `get certificate api thumbprint` 명령을 실행합니다.

명령 출력은 이 NSX Manager에 고유한 영숫자 문자열입니다.

예:

```
NSX-Manager1> get certificate api thumbprint
659442c1435350edbbc0e87ed5a6980d892b9118f851c17a13ec76a8b985f57
```

- 4 NSX Edge 노드 VM에서 `join management-plane` 명령을 실행합니다.

다음 정보를 입력합니다.

- 포트 번호(선택 사항)가 있는 NSX Manager의 호스트 이름 또는 IP 주소
- NSX Manager의 사용자 이름
- NSX Manager의 인증서 지문
- NSX Manager의 암호

```
NSX-Edge1> join management-plane <Manager-IP> thumbprint <Manager-thumbprint> username admin
```

각 NSX Edge 노드 VM에서 이 명령을 반복합니다.

- 5 NSX Edge 노드 VM에서 `get managers` 명령을 실행하여 결과를 확인합니다.

```
nsx-edge-1> get managers
- 10.173.161.17 Connected (NSX-RPC)
- 10.173.161.140 Connected (NSX-RPC)
- 10.173.160.204 Connected (NSX-RPC)
```

- 6 NSX Manager UI에서 **시스템 > 패브릭 > 노드 > Edge 전송 노드**로 이동합니다.

NSX Edge 전송 노드 페이지에서 다음을 수행합니다.

- **구성 상태** 열에 NSX 구성이 표시됩니다. 노드에 대한 구성을 시작하려면 **NSX** 구성을 클릭합니다. **NSX 버전** 열에 노드에 설치된 버전 번호가 표시되지 않는 경우 브라우저 창을 새로 고쳐 보십시오.
- NSX Edge 노드에서 NSX를 구성하기 전에 **노드 상태** 및 **터널 상태** 열은 사용할 수 없음 상태를 표시합니다. **전송 영역** 및 **N-VDS** 스위치 열은 NSX Edge 노드에 연결된 전송 영역이 없거나 구성된 N-VDS 스위치가 없음을 나타내는 0 값을 표시합니다.

다음에 수행할 작업

NSX Manager를 사용하여 NSX Edge를 설치할 경우 **NSX Edge 전송 노드 생성**을 참조하십시오.

NSX Edge를 수동으로 설치할 경우 **NSX Edge를 전송 노드로 구성**을 참조하십시오.

NSX Edge를 전송 노드로 구성

ESXi 또는 베어메탈에 NSX Edge를 수동으로 설치한 후에는 NSX Edge-NSX-T Data Center 패브릭을 전송 노드로 구성합니다.

전송 노드는 NSX-T Data Center 오버레이 또는 NSX-T Data Center VLAN 네트워킹에 참여할 수 있는 노드입니다. N-VDS가 포함된 노드는 전송 노드가 될 수 있습니다. 이러한 노드에는 NSX Edge가 포함되며 이에 국한되지 않습니다.

NSX Edge는 1개의 오버레이 전송 영역과 여러 개의 VLAN 전송 영역에 속할 수 있습니다. VM이 외부 환경에 액세스해야 할 경우 NSX Edge가 VM의 논리적 스위치가 속하는 전송 영역과 동일한 전송 영역에 속해야 합니다. 일반적으로 NSX Edge는 업링크 액세스를 제공하기 위해 1개 이상의 VLAN 전송 영역에 속합니다.

사전 요구 사항

- 전송 영역을 구성해야 합니다.
- 계산 관리자가 구성되어 있는지 확인합니다. [계산 관리자 추가](#)의 내용을 참조하십시오.
- 업링크 프로파일이 구성해야 하거나 베어메탈 NSX Edge 노드에 대해 기본 업링크 프로파일을 사용할 수도 있습니다.
- IP 풀을 구성해야 하거나 네트워크 배포에 사용할 수 있어야 합니다.
- 하나 이상의 미사용 물리적 NIC를 호스트 또는 NSX Edge 노드에서 사용할 수 있어야 합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 패브릭 > 노드 > Edge 전송 노드 > Edge 편집**을 선택합니다.
- 3 Edge 노드를 선택하고 **편집**을 클릭합니다.
- 4 이 전송 노드가 속한 전송 영역을 선택합니다.

NSX Edge 전송 노드는 2개 이상의 전송 영역, 즉 NSX-T Data Center 연결용 오버레이와 업링크 연결용 VLAN에 속합니다.

참고 전송 영역의 여러 VTEP을 동일한 네트워크 세그먼트로 구성해야 합니다. 전송 영역의 VTEP을 다른 네트워크 세그먼트로 구성하면 VTEP 간에 BFD 세션을 설정할 수 없습니다.

- 5 N-VDS 정보를 입력합니다.

옵션	설명
Edge 스위치 이름	드롭다운 메뉴에서 VLAN 스위치를 선택합니다.
업링크 프로파일	드롭다운 메뉴에서 업링크 프로파일을 선택합니다. 사용 가능한 업링크는 선택된 업링크 프로파일의 구성에 따라 다릅니다.

옵션	설명
IP 할당	<p>오버레이 N-VDS에 대해 IP 풀 사용 또는 정적 IP 목록 사용을 선택합니다. 이러한 IP 주소는 NSX Edge 전송 노드에 VTEP로 할당됩니다. NSX Edge의 여러 VTEP은 동일한 서브넷에 있어야 합니다.</p> <ul style="list-style-type: none"> ■ 정적 IP 목록 사용을 선택하면 씬프로 구분된 IP 주소 목록, 게이트웨이 및 서브넷 마스크를 지정해야 합니다. ■ IP 할당에 대해 IP 풀 사용을 선택한 경우 IP 풀 이름을 지정합니다.
DPDK 빠른 경로 인터페이스/가상 NIC	<p>업링크 인터페이스에 대한 데이터 경로 인터페이스를 선택합니다.</p> <p>참고 명명된 팀 구성 정책을 사용하여 구성된 논리적 스위치를 통해 트래픽이 흐르도록 하려면 기본 팀 구성 정책의 모든 업링크를 NSX Edge VM의 물리적 네트워크 인터페이스에 매핑합니다.</p>

6 전송 노드 페이지에서 연결 상태를 확인합니다.

NSX Edge를 전송 노드로 추가하면 10-12분 후에 연결 상태가 [실행 중]으로 변경됩니다.

- (선택 사항) 다음과 같이 GET `https://<nsx-manager>/api/v1/transport-nodes/<transport-node-id>` API 호출을 사용하여 전송 노드를 확인합니다.
- (선택 사항) 상태 정보를 보려면 GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/status` API 호출을 사용합니다.
- vCenter Server를 사용하여 NSX Edge 노드를 새 호스트로 마이그레이션한 후 NSX Edge의 오래된 구성 세부 정보(계산, 데이터스토어, 네트워크, SSH, NTP, DNS, 검색 도메인)를 보고하는 NSX Manager UI를 찾을 수 있습니다. 새 호스트에서 NSX Edge의 최신 구성 세부 정보를 가져오려면 API 명령을 실행합니다.

```
POST api/v1/transport-nodes/<transport-node-id>?
action=refresh_node_configuration&resource_type=EdgeNode
```

다음에 수행할 작업

NSX Edge 클러스터에 NSX Edge 노드를 추가합니다. [NSX Edge 클러스터 생성](#)의 내용을 참조하십시오.

전송 영역 및 전송 노드

10

전송 영역 및 전송 노드는 NSX-T Data Center에서 중요한 개념입니다.

본 장은 다음 항목을 포함합니다.

- 전송 영역 생성
- 터널 끝점 IP 주소에 대한 IP 풀 생성
- 고급 데이터 경로
- 프로파일 구성
- 독립형 호스트 또는 베어메탈 서비스 전송 노드 생성
- NSX-T Data Center 커널 모듈의 수동 설치
- 완전 축소형 vSphere 클러스터 NSX-T 배포

전송 영역 생성

전송 영역에서는 특정 네트워크 사용에 참여할 수 있는 호스트, 즉 VM을 지정합니다. 전송 영역은 논리적 스위치를 "볼 수 있는" 호스트, 즉 논리적 스위치에 연결될 수 있는 VM을 제한하여 이 작업을 수행합니다. 전송 영역은 하나 이상의 호스트 클러스터에 걸쳐 있을 수 있습니다.

NSX-T Data Center 환경에는 요구 사항에 따라 하나 이상의 전송 영역이 포함될 수 있습니다. 호스트는 여러 전송 영역에 속할 수 있습니다. 논리적 스위치는 하나의 전송 영역에만 속할 수 있습니다.

NSX-T Data Center는 계층 2 네트워크의 다른 전송 영역에 있는 VM 연결을 허용하지 않습니다. 논리적 스위치의 범위는 전송 영역으로 제한되므로 다른 전송 영역에 있는 가상 시스템이 동일한 계층 2 네트워크에 있을 수 없습니다.

오버레이 전송 영역은 호스트 전송 노드 및 NSX Edge 모두에서 사용됩니다. 호스트 또는 NSX Edge 전송 노드가 오버레이 전송 영역에 추가되면 N-VDS가 호스트 또는 NSX Edge에 설치됩니다.

VLAN 전송 영역은 VLAN 업링크를 위해 NSX Edge 및 호스트 전송 노드에서 사용됩니다. NSX Edge가 VLAN 전송 영역에 추가되면 VLAN N-VDS가 NSX Edge에 설치됩니다.

N-VDS는 논리적 라우터 업링크 및 다운링크를 물리적 NIC에 바인딩하여 가상 및 물리적 패킷 간의 흐름을 허용합니다.

전송 영역을 생성할 때는 나중에 전송 노드가 이 전송 영역에 추가될 때 해당 노드에 설치될 N-VDS의 이름을 제공해야 합니다. N-VDS 이름은 원하는 대로 지정할 수 있습니다.

절차

1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.

2 **시스템 > 패브릭 > 전송 영역 > 추가**를 선택합니다.

3 전송 영역의 이름 및 필요한 경우 설명을 입력합니다.

4 N-VDS 이름을 입력합니다.

5 N-VDS 모드를 선택합니다.

- **표준** 모드는 지원되는 모든 호스트에 적용됩니다.

- **고급 데이터 경로**는 전송 영역에 속할 수 있는 ESXi 호스트 버전 6.7 이상 유형의 전송 노드에만 적용되는 네트워킹 스택 모드입니다.

6 N-VDS 모드가 [표준]으로 설정된 경우 트래픽 유형을 선택합니다.

옵션은 **오버레이** 및 **VLAN**입니다.

7 N-VDS 모드가 [고급 데이터 경로]로 설정된 경우 트래픽 유형을 선택합니다.

옵션은 **오버레이** 및 **VLAN**입니다.

참고 고급 데이터 경로 모드에서는 특정 NIC 구성만 지원됩니다. 지원되는 NIC를 구성했는지 확인하십시오.

8 하나 이상의 업링크 팀 구성 정책 이름을 입력합니다. 이러한 명명된 팀 구성 정책은 전송 영역에 연결된 논리적 스위치에서 사용할 수 있습니다. 논리적 스위치가 일치하는 명명된 팀 구성 정책을 찾지 못하면 기본 업링크 팀 구성 정책이 사용됩니다.

9 **전송 영역** 페이지에서 새로운 전송 영역을 확인합니다.

10 (선택 사항) 또한 GET <https://<nsx-mgr>/api/v1/transport-zones> API 호출을 사용하여 새 전송 영역을 확인할 수 있습니다.

```
{
  "cursor": "00369b661aed-1eaa-4567-9408-ccbcfe50b416tz-vlan",
  "result_count": 2,
  "results": [
    {
      "resource_type": "TransportZone",
      "description": "comp overlay transport zone",
      "id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
      "display_name": "tz-overlay",
      "host_switch_name": "overlay-hostswitch",
      "transport_type": "OVERLAY",
      "transport_zone_profile_ids": [
```

```

    {
      "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
      "resource_type": "BfdHealthMonitoringProfile"
    }
  ],
  "_create_time": 1459547126454,
  "_last_modified_user": "admin",
  "_system_owned": false,
  "_last_modified_time": 1459547126454,
  "_create_user": "admin",
  "_revision": 0,
  "_schema": "/v1/schema/TransportZone"
},
{
  "resource_type": "TransportZone",
  "description": "comp vlan transport zone",
  "id": "9b661aed-1eaa-4567-9408-ccbcbfe50b416",
  "display_name": "tz-vlan",
  "host_switch_name": "vlan-uplink-hostswitch",
  "transport_type": "VLAN",
  "transport_zone_profile_ids": [
    {
      "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
      "resource_type": "BfdHealthMonitoringProfile"
    }
  ],
  "_create_time": 1459547126505,
  "_last_modified_user": "admin",
  "_system_owned": false,
  "_last_modified_time": 1459547126505,
  "_create_user": "admin",
  "_revision": 0,
  "_schema": "/v1/schema/TransportZone"
}
]
}

```

다음에 수행할 작업

경우에 따라 사용자 지정 전송 영역 프로파일을 생성한 후 이를 전송 영역에 바인딩합니다. `POST /api/v1/transportzone-profiles` API를 사용하여 사용자 지정 전송 영역 프로파일을 생성할 수 있습니다. 전송 영역 프로파일을 생성하기 위한 UI 워크플로는 없습니다. 전송 영역 프로파일이 생성된 후에는 `PUT /api/v1/transport-zones/<transport-zone-id>` API를 사용하여 전송 영역에서 찾을 수 있습니다.

전송 노드를 생성합니다. [독립형 호스트 또는 베어메탈 서비스 전송 노드 생성](#)의 내용을 참조하십시오.

터널 끝점 IP 주소에 대한 IP 풀 생성

터널 끝점에 대해 IP 풀을 사용할 수 있습니다. 터널 끝점은 외부 IP 헤더에 사용되는 소스 IP 주소와 대상 IP 주소로, 오버레이 프레임의 NSX-T Data Center 캡슐화를 시작하고 종료하는 하이퍼바이저 호스트를 식별합니다. 또한 DHCP 또는 수동으로 구성된 IP 풀을 터널 끝점 IP 주소에 사용할 수 있습니다.

ESXi 및 KVM 호스트를 둘 다 사용하는 경우 한 가지 설계 옵션은 ESXi 터널 끝점 IP 풀(sub_a) 및 KVM 터널 끝점 IP 풀(sub_b)에 대해 2개의 다른 서브넷을 사용하는 것입니다. 이 경우 KVM 호스트에서 전용 기본 게이트웨이를 사용하여 sub_a에 대한 정적 경로를 추가해야 합니다.

다음은 Ubuntu 호스트의 결과 라우팅 테이블의 예입니다. 여기서 sub_a는 192.168.140.0이고 sub_b는 192.168.150.0입니다. (예를 들어 관리 서브넷은 192.168.130.0일 수 있습니다.)

커널 IP 라우팅 테이블:

Destination	Gateway	Genmask	Iface
0.0.0.0	192.168.130.1	0.0.0.0	eth0
192.168.122.0	0.0.0.0	255.255.255.0	virbr0
192.168.130.0	0.0.0.0	255.255.255.0	eth0
192.168.140.0	192.168.150.1	255.255.255.0	nsx-vtep0.0
192.168.150.0	0.0.0.0	255.255.255.0	nsx-vtep0.0

경로는 2가지 이상의 다른 방법으로 추가할 수 있습니다. 이러한 두 방법 중에서 경로는 인터페이스를 편집하여 경로를 추가하는 경우에만 호스트 재부팅 후 유지됩니다. 경로 추가 명령을 사용하여 경로를 추가하면 호스트 재부팅 후 유지되지 않습니다.

```
route add -net 192.168.140.0 netmask 255.255.255.0 gw 192.168.150.1 dev nsx-vtep0.0
```

/etc/network/interfaces에서 "up ifconfig nsx-vtep0.0 up" 앞에 다음 정적 경로를 추가합니다.

```
post-up route add -net 192.168.140.0 netmask 255.255.255.0 gw 192.168.150.1
```

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 고급 네트워킹 및 보안 > 인벤토리 > 그룹 > IP 풀 > 추가를 선택합니다.
- 3 IP 풀 세부 정보를 입력합니다.

옵션	매개 변수 예
이름 및 설명	IP 풀 이름과 설명(선택 사항)을 입력합니다.
IP 범위	IP 할당 범위 192.168.200.100 - 192.168.200.115
게이트웨이	192.168.200.1
CIDR	CIDR 표기법으로 나타낸 네트워크 주소 192.168.200.0/24
DNS 서버	쉼표로 구분된 DNS 서버 목록 192.168.66.10
DNS 접미사	corp.local

결과

IPv4 또는 IPv6 주소 풀은 IP 풀 페이지에 나열되어 있습니다.

GET <https://<nsx-mgr>/api/v1/pools/ip-pools> API 호출을 사용하여 IP 풀 목록을 볼 수도 있습니다.

다음에 수행할 작업

업링크 프로파일을 생성합니다. [업링크 프로파일 생성](#)의 내용을 참조하십시오.

고급 데이터 경로

고급 데이터 경로는 구성 시 뛰어난 네트워크 성능을 제공하는 네트워킹 스택 모드입니다. DPDK 기능을 활용하는 성능상의 이점을 제공하는 NFV 워크로드를 주 대상으로 합니다.

ESXi 호스트에만 N-VDS 스위치를 고급 데이터 경로 모드로 구성할 수 있습니다. ENS는 Edge VM을 통과하는 트래픽도 지원합니다.

고급 데이터 경로 모드에서는 두 가지 트래픽 모드가 모두 지원됩니다.

- 오버레이 트래픽
- VLAN 트래픽

지원되는 VMkernel NIC

여러 ENS 호스트 스위치를 지원하는 NSX-T Data Center를 사용하는 경우 호스트당 지원되는 최대 VMkernel NIC의 수는 32개입니다.

고급 데이터 경로를 구성하는 상위 수준의 프로세스

네트워크 관리자는 고급 데이터 경로 모드에서 N-VDS를 지원하는 전송 영역을 생성하기 전에 지원되는 NIC 카드와 드라이버를 사용하여 네트워크를 준비해야 합니다. 네트워크 성능 향상을 위해 NUMA 노드를 인식할 수 있게 로드 밸런싱된 소스 팀 구성 정책을 사용할 수 있습니다.

상위 수준의 단계는 다음과 같습니다.

- 1 고급 데이터 경로를 지원하는 NIC 카드를 사용합니다.

고급 데이터 경로를 지원하는 NIC 카드를 확인하려면 [VMware 호환성 가이드](#)를 참조하십시오.

[VMware 호환성 가이드] 페이지의 **IO 디바이스** 범주 아래에서 **ESXi 6.7**을 선택하고, IO 디바이스 유형을 **네트워크**로, 기능을 **N-VDS 고급 데이터 경로**로 선택합니다.

- 2 [My VMware 페이지](#)에서 최신 NIC 드라이버를 다운로드하고 설치합니다.

a **드라이버 및 도구 > 드라이버 CD**로 이동합니다.

b 다음의 NIC 드라이버를 다운로드합니다.

VMware ESXi 6.7 ixgben-ens 1.1.3 NIC Driver for Intel Ethernet Controllers
82599, x520, x540, x550 및 x552 family

Intel Ethernet 컨트롤러 X710, XL710, XXV710 및 X722 제품군용 VMware ESXi 6.7 i40en-ens 1.1.3 NIC 드라이버

- c 호스트를 ENS 호스트로 사용하려면 시스템에서 하나 이상의 ENS 지원 NIC를 사용할 수 있어야 합니다. ENS 지원 NIC가 없으면 관리부에서는 호스트를 ENS 전송 영역에 추가하도록 허용하지 않습니다.

- d ENS 드라이버를 나열합니다.

```
esxcli software vib list | grep -E "i40|ixgben"
```

- e NIC가 ENS 데이터 경로 트래픽을 처리할 수 있는지 확인합니다.

```
esxcfg-nics -e
```

Name	Driver	ENS Capable	ENS Driven	MAC Address	Description
vmnic0	ixgben	True	False	e4:43:4b:7b:d2:e0	Intel(R) Ethernet Controller X550
vmnic1	ixgben	True	False	e4:43:4b:7b:d2:e1	Intel(R) Ethernet Controller X550
vmnic2	ixgben	True	False	e4:43:4b:7b:d2:e2	Intel(R) Ethernet Controller X550
vmnic3	ixgben	True	False	e4:43:4b:7b:d2:e3	Intel(R) Ethernet Controller X550
vmnic4	i40en	True	False	3c:fd:fe:7c:47:40	Intel(R) Ethernet Controller X710/X557-AT 10GBASE-T
vmnic5	i40en	True	False	3c:fd:fe:7c:47:41	Intel(R) Ethernet Controller X710/X557-AT 10GBASE-T
vmnic6	i40en	True	False	3c:fd:fe:7c:47:42	Intel(R) Ethernet Controller X710/X557-AT 10GBASE-T
vmnic7	i40en	True	False	3c:fd:fe:7c:47:43	Intel(R) Ethernet Controller X710/X557-AT 10GBASE-T

- f ENS 드라이버를 설치합니다.

```
esxcli software vib install -v file:///<DriverInstallerURL> --no-sig-check
```

- g 또는 이 드라이버를 시스템에 다운로드한 후 설치합니다.

```
wget <DriverInstallerURL>
```

```
esxcli software vib install -v file:///<DriverInstallerURL> --no-sig-check
```

- h 호스트를 재부팅하여 드라이버를 로드합니다. 다음 단계를 계속 진행합니다.

- i 드라이버를 언로드하려면 다음 단계를 수행합니다.

```
vmkload_mod -u i40en
```

```
ps | grep vmkdevmgr
```

```
kill -HUP "$(ps | grep vmkdevmgr | awk {'print $1'})"
```

```
ps | grep vmkdevmgr
```

```
kill -HUP <vmkdevmgrProcessID>
```

```
kill -HUP "$(ps | grep vmkdevmgr | awk {'print $1'})"
```

- j ENS 드라이버를 제거하려면 `esxcli software vib remove --vibname=i40en-ens --force --no-live-install`을(를) 실행합니다.

- 3 업링크 정책을 생성합니다.

[업링크 프로파일 생성](#)의 내용을 참조하십시오.

- 4 고급 데이터 경로 모드의 N-VDS를 사용하여 전송 영역을 생성합니다.

[전송 영역 생성](#)의 내용을 참조하십시오.

참고 오버레이 트래픽용으로 구성된 ENS 전송 영역: 11.0.0 버전 이전의 VMware Tools를 실행하고 vNIC 유형이 VMXNET3인 Microsoft Windows 가상 시스템의 경우 MTU를 1500으로 설정해야 합니다. vSphere 6.7 U1 및 VMware Tools 버전 11.0.0 이상을 실행하는 Microsoft Windows 가상 시스템의 경우 MTU가 8900보다 작은 값으로 설정되어 있는지 확인합니다. 지원되는 다른 OS를 실행하는 가상 시스템의 경우 가상 시스템 MTU가 8900보다 작은 값으로 설정되어 있는지 확인합니다.

- 5 호스트 전송 노드를 생성합니다. 고급 데이터 경로 N-VDS의 논리적 코어 수와 NUMA 노드 수를 구성합니다.

[독립형 호스트 또는 베어메탈 서비스 전송 노드 생성](#)의 내용을 참조하십시오.

NUMA를 인식하는 로드 밸런싱된 소스 팀 구성 정책 모드

고급 데이터 경로 N-VDS에 대해 정의된 로드 밸런싱된 소스 팀 구성 정책 모드는 다음 조건이 충족되면 NUMA를 인식할 수 있습니다.

- VM의 **지연 시간 감도가 높음**입니다.
- VMXNET3의 네트워크 어댑터 유형이 사용되고 있습니다.

VM 또는 물리적 NIC의 NUMA 노드 위치를 사용할 수 없는 경우 로드 밸런싱된 소스 팀 구성 정책에서는 VM과 NIC 정렬에 NUMA 인식을 고려하지 않습니다.

팀 구성 정책은 다음과 같은 조건에서 NUMA 인식 없이 작동합니다.

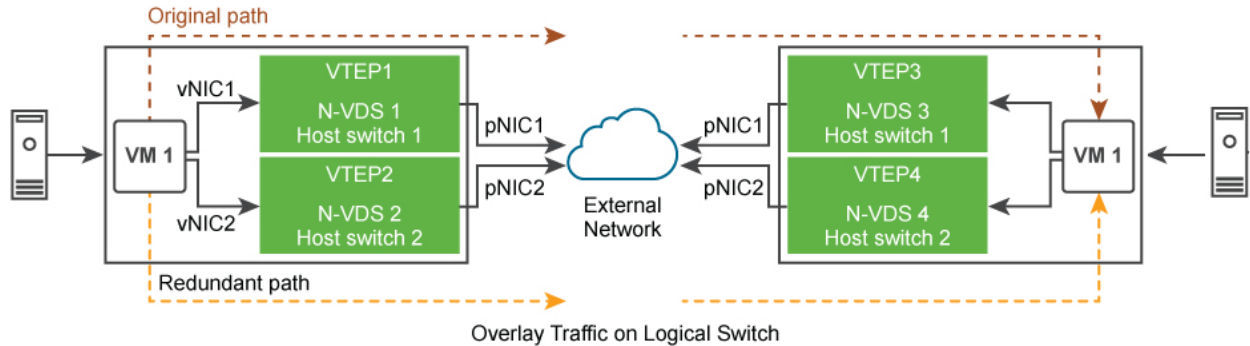
- LAG 업링크가 여러 NUMA 노드의 물리적 링크로 구성되어 있습니다.
- VM이 여러 NUMA 노드에 대한 선호도를 가집니다.
- ESXi 호스트가 VM 또는 물리적 링크에 대해 NUMA 정보를 정의하지 못했습니다.

트래픽 안정성을 필요로 하는 애플리케이션에 대한 ENS 지원

NFV 워크로드를 SCTP(Stream Control Transmission Protocol)에서 제공하는 멀티호밍 및 이중화 기능을 사용하여 애플리케이션에서 실행되는 트래픽에 대한 복원력 및 안정성을 높일 수 있습니다. 멀티호밍은 소스 VM에서 대상 VM으로 이중화 경로를 지원하는 기능입니다.

오버레이 또는 VLAN 네트워크의 업링크로 사용될 수 있는 물리적 NIC의 수에 따라 VM은 여러 이중화 네트워크 경로를 사용하여 대상 VM으로 트래픽을 전송할 수 있습니다. 이중화 경로는 논리적 스위치에 대해 고정된 물리적 NIC가 실패할 때 사용됩니다. 향상된 데이터 경로 스위치는 호스트 간에 중복 네트워크 경로를 제공합니다.

그림 10-1. ENS를 통한 트래픽의 멀티호밍 및 이중화



상위 수준의 작업은 다음과 같습니다.

- 1 호스트를 NSX-T Data Center 전송 노드로 준비합니다.
- 2 [고급 데이터 경로] 모드에서 두 개의 N-VDS 스위치를 사용하여 VLAN 또는 오버레이 전송 영역을 준비합니다.
- 3 N-VDS 1에서 첫 번째 물리적 NIC를 스위치에 고정합니다.
- 4 N-VDS 2에서 두 번째 물리적 NIC를 스위치에 고정합니다.

[고급 데이터 경로] 모드에서 N-VDS는 물리적 NIC1을 사용할 수 없게 되면 VM 1의 트래픽이 이중화 경로 (vNIC 1 → 터널 끝점 2 → pNIC 2 → VM 2)를 통해 라우팅되도록 합니다.

프로파일 구성

프로파일을 사용하면 여러 호스트 또는 노드에서 네트워크 어댑터에 대해 동일한 기능을 일관되게 구성할 수 있습니다.

프로파일은 네트워크 어댑터에 적용하려는 속성 또는 기능의 컨테이너입니다. 각 네트워크 어댑터에 대해 개별 속성 또는 기능을 구성하는 대신 프로파일에 기능을 지정한 다음 여러 호스트 또는 노드에 이를 적용할 수 있습니다.

업링크 프로파일 생성

업링크는 NSX Edge 노드에서 랙 상단 스위치 또는 NSX-T Data Center 논리적 스위치로의 링크입니다. 링크는 NSX Edge 노드의 물리적 네트워크 인터페이스에서 스위치까지 연결됩니다.

업링크 프로파일은 업링크에 대한 정책을 정의합니다. 업링크 프로파일에 의해 정의된 설정에는 팀 구성 정책, 활성/대기 링크, 전송 VLAN ID 및 MTU 설정이 포함될 수 있습니다.

VM 장치 기반 NSX Edge 노드 및 호스트 전송 노드에 대한 업링크 구성:

- 업링크 프로파일에 대해 페일오버 팀 구성 정책을 구성한 경우 팀 구성 정책에서 단일 활성 업링크만 구성할 수 있습니다. 대기 업링크는 지원되지 않으므로 페일오버 팀 구성 정책에서 설정하지 않아야 합니다. NSX Edge를 가상 장치 또는 호스트 전송 노드로 설치하는 경우 기본 업링크 프로파일을 사용합니다.
- 업링크 프로파일에 대해 로드 밸런싱 소스 팀 구성 정책을 구성한 경우 동일한 N-VDS에 여러 활성 업링크를 구성할 수 있습니다. 각 업링크는 고유 이름 및 IP 주소를 갖는 하나의 물리적 NIC에 연결됩니다. 업링크 끝점에 할당된 IP 주소는 N-VDS에 대한 IP 할당을 사용하여 구성할 수 있습니다.

트래픽 로드 밸런싱에 대해 **로드 밸런싱된 소스** 팀 구성 정책을 사용해야 합니다.

사전 요구 사항

- **NSX Edge 설치 요구 사항**의 NSX Edge 네트워크 요구 사항을 참조하십시오.
- 업링크 프로파일의 각 업링크는 하이퍼바이저 호스트 또는 NSX Edge 노드에 있는 작동되고 사용 가능한 물리적 링크와 일치해야 합니다.

예를 들어 하이퍼바이저 호스트에 작동 중인 2개의 물리적 링크 vmnic0과 vmnic1이 있습니다.

vmnic0은 관리 및 스토리지 네트워크에 사용되지만 vmnic1은 사용되지 않습니다. 즉 vmnic1은 NSX-T Data Center 업링크로 사용될 수 있지만 vmnic0은 사용될 수 없습니다. 링크 팀 구성을 수행하려면 사용 가능한 2개의 미사용 물리적 링크(예: vmnic1 및 vmnic2)가 있어야 합니다.

NSX Edge의 경우 터널 끝점 및 VLAN 업링크는 동일한 물리적 링크를 사용할 수 있습니다. 예를 들어 관리 네트워크에는 vmnic0/eth0/em0을 사용하고, fp-ethX 링크에는 vmnic1/eth1/em1을 사용할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 패브릭 > 프로파일 > 업링크 프로파일 > 추가**를 선택합니다.

3 업링크 프로파일 세부 정보를 모두 입력합니다.

옵션	설명
이름 및 설명	업링크 프로파일 이름을 입력합니다. (선택 사항) 업링크 프로파일 설명을 추가합니다.
LAG	<p>(선택 사항) LAG 섹션에서, 전송 네트워크에 대해 LACP(Link Aggregation Control Protocol)를 사용하는 LAG(링크 집계 그룹)에 대해 추가를 클릭합니다.</p> <p>참고 LACP의 경우 KVM 호스트에서 여러 LAG가 지원되지 않습니다.</p> <p>생성하는 활성 및 대기 업링크 이름은 물리적 링크를 나타내는 어떤 텍스트도 될 수 있습니다. 이러한 업링크 이름은 나중에 전송 노드를 생성할 때 참조됩니다. 전송 노드 UI/API를 사용하면 명명된 각 업링크에 상응하는 물리적 링크를 지정할 수 있습니다.</p> <p>가능한 LAG 해시 메커니즘 옵션은 다음과 같습니다.</p> <ul style="list-style-type: none"> ■ 소스 MAC 주소 ■ 대상 MAC 주소 ■ 소스 및 대상 MAC 주소 ■ 소스 및 대상 IP 주소와 VLAN ■ 소스 및 대상 MAC 주소, IP 주소 및 TCP/UDP 포트
팀 구성	<p>[팀 구성] 섹션에서 기본 팀 구성 정책을 입력하거나 명명된 팀 구성 정책을 입력하도록 선택할 수 있습니다. 추가를 클릭하여 명명된 팀 구성 정책을 추가합니다. 팀 구성 정책은 N-VDS가 이중화 및 트래픽 로드 밸런싱에 업링크를 사용하는 방법을 정의합니다. 다음 모드에서 팀 구성 정책을 구성할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 페일오버 순서: 대기 업링크의 선택적 목록과 함께 액티브 업링크를 선택합니다. 활성 업링크가 실패하는 경우 대기 목록의 다음 업링크가 활성 업링크를 대신합니다. 이 옵션을 사용하여 수행되는 실제 로드 밸런싱이 없습니다. ■ 로드 밸런싱 소스: 액티브 업링크 목록을 선택합니다. 전송 노드를 구성하면 전송 노드의 각 인터페이스를 하나의 액티브 업링크에 고정할 수 있습니다. 이 구성에서는 동시에 여러 활성 업링크를 사용할 수 있습니다. ■ 로드 밸런싱 소스 MAC 주소: 소스 이더넷의 해시를 기준으로 업링크를 선택합니다. <p>참고</p> <ul style="list-style-type: none"> ■ KVM 호스트: 페일오버 순서 팀 구성 정책만 지원되고, 로드 밸런싱 소스 및 로드 밸런싱 소스 MAC 팀 구성 정책은 지원되지 않습니다. ■ NSX Edge: 기본 팀 구성 정책에 대해 로드 밸런싱 소스 및 페일오버 순서 팀 구성 정책이 지원됩니다. 명명된 팀 구성 정책의 경우 페일오버 순서 정책만 지원됩니다. ■ ESXi 호스트: 로드 밸런싱 소스 MAC, 로드 밸런싱 소스 및 페일오버 순서 팀 구성 정책이 지원됩니다. <p>(ESXi 호스트 및 NSX Edge) 전송 영역에 대해 다음 정책을 정의할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 모든 VLAN 기반 논리적 스위치 또는 세그먼트에 대한 명명된 팀 구성 정책. ■ 전체 N-VDS에 대한 기본 팀 구성 정책.

옵션	설명
	<p>명명된 팀 구성 정책: 명명된 팀 구성 정책이란 모든 VLAN 기반 논리적 스위치 또는 세그먼트에 대해 특정 팀 구성 정책 모드와 업링크 이름을 정의할 수 있음을 의미합니다. 이 정책 유형에서는 트래픽 조절 정책(예: 대역폭 요구 사항 기준)에 따라 특정 업링크를 유연하게 선택할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 명명된 팀 구성 정책을 정의하는 경우 N-VDS는 VLAN 기반 전송 영역에 연결되고 호스트의 특정 VLAN 기반 논리적 스위치나 세그먼트용으로 최종 선택된 명명된 팀 구성 정책을 사용합니다. ■ 명명된 팀 구성 정책을 정의하지 않는 경우 N-VDS는 기본 팀 구성 정책을 사용합니다.

- 4 전송 VLAN 값을 입력합니다. 업링크 프로파일에 설정된 전송 VLAN은 오버레이 트래픽에만 태그를 지정하고, VLAN ID가 TEP 끝점에서 사용됩니다.

- 5 MTU 값을 입력합니다.

업링크 프로파일 MTU 기본값은 1600입니다.

글로벌 물리적 업링크 MTU는 NSX-T Data Center 도메인의 모든 N-VDS 인스턴스에 대한 MTU 값을 구성합니다. 글로벌 물리적 업링크 MTU 값을 지정하지 않으면, MTU 값이 구성된 경우 업링크 프로파일에 MTU가 유추되고, 구성되지 않으면 기본값인 1600이 사용됩니다. 업링크 프로파일 MTU 값은 특정 호스트의 글로벌 물리적 업링크 MTU 값을 재정의할 수 있습니다.

글로벌 논리적 인터페이스 MTU는 모든 논리적 라우터 인터페이스의 MTU 값을 구성합니다. 글로벌 논리적 인터페이스 MTU 값을 지정하지 않으면 MTU 값이 Tier-0 논리적 라우터에서 유추됩니다. 논리적 라우터 업링크 MTU 값은 특정 포트에서 글로벌 논리적 인터페이스 MTU 값을 재정의할 수 있습니다.

결과

UI 이외에도 API 호출 GET /api/v1/host-switch-profiles를 사용하여 업링크 프로파일을 확인할 수 있습니다.

다음에 수행할 작업

전송 영역을 생성합니다. [전송 영역 생성](#)의 내용을 참조하십시오.

Network I/O Control 프로파일 구성

NIOC(Network I/O Control)를 사용하여 비즈니스에 중요한 애플리케이션에 네트워크 대역폭을 할당하고 몇 가지 트래픽 유형이 공통 리소스를 얻기 위해 경쟁하는 상황을 해결합니다.

NIOC 프로파일에서는 호스트에 있는 물리적 어댑터의 용량을 기반으로 시스템 트래픽에 대한 대역폭을 예약하는 메커니즘을 사용합니다. Network I/O Control 버전 3은 향상된 네트워크 리소스 예약과 전체 스위치에 걸친 할당을 제공합니다.

NSX-T Data Center용 Network I/O Control 버전 3은 vSphere Fault Tolerance와 같은 가상 시스템 및 인프라 서비스와 관련된 시스템 트래픽의 리소스 관리를 지원합니다. 시스템 트래픽은 ESXi 호스트와 전적으로 연결되어 있습니다.

참고 NIOC 프로파일을 NSX Edge 전송 노드에 적용할 수 없습니다.

시스템 트래픽에 대한 대역폭 보장

Network I/O Control 버전 3은 공유, 예약 및 제한의 구성체를 사용하여 가상 시스템의 네트워크 어댑터에 대역폭을 프로비저닝합니다. 이러한 구성체는 NSX-T Data Center Manager UI에서 정의할 수 있습니다. 가상 시스템 트래픽에 대한 대역폭 예약은 승인 제어에서도 사용됩니다. 가상 시스템의 전원을 켜면 승인 제어 유틸리티가 리소스 용량을 제공할 수 있는 호스트에 VM을 배치하기 전에 충분한 대역폭을 사용할 수 있는지 확인합니다.

시스템 트래픽에 대한 대역폭 할당

vSphere Fault Tolerance, vSphere vMotion, 가상 시스템 등이 생성하는 트래픽에 특정 양의 대역폭을 할당하도록 Network I/O Control을 구성할 수 있습니다.

- 관리 트래픽: 호스트 관리를 위한 트래픽입니다.
- FT(Fault Tolerance) 트래픽: 페일오버 및 복구를 위한 트래픽입니다.
- NFS 트래픽: 네트워크 파일 시스템의 파일 전송과 관련된 트래픽입니다.
- vSAN 트래픽: Virtual SAN(Storage Area Network)에서 생성된 트래픽입니다.
- vMotion 트래픽: 계산 리소스 마이그레이션을 위한 트래픽입니다.
- vSphere Replication 트래픽: 복제를 위한 트래픽입니다.
- vSphere Data Protection 백업 트래픽: 데이터 백업에서 생성되는 트래픽입니다.
- 가상 시스템 트래픽: 가상 시스템에서 생성되는 트래픽입니다.
- iSCSI 트래픽: iSCSI(internet Small Computer System Interface)에 대한 트래픽입니다.

vCenter Server는 분산 스위치에서 스위치에 연결된 호스트의 각 물리적 어댑터로 할당을 전파합니다.

시스템 트래픽에 대한 대역폭 할당 매개 변수

Network I/O Control 서비스는 몇 가지 구성 매개 변수를 사용하여 기본 vSphere 시스템 기능의 트래픽에 대역폭을 할당합니다. 시스템 트래픽에 대한 할당 매개 변수.

시스템 트래픽에 대한 할당 매개 변수

- 공유: 공유(1~100)는 동일한 물리적 어댑터에서 활성인 다른 시스템 트래픽 유형에 대한 특정 시스템 트래픽 유형의 상대적 우선 순위를 반영합니다. 시스템 트래픽 유형에 할당된 상대적 공유 및 다른 시스템 기능이 전송하는 데이터 양은 해당 시스템 트래픽 유형에 대해 사용 가능한 대역폭을 결정합니다.

- **예약:** 단일 물리적 어댑터에서 보장되어야 하는 최소 대역폭(Mbps). 모든 시스템 트래픽 유형 간에 예약된 총 대역폭은 최저 용량을 가진 물리적 네트워크 어댑터가 제공할 수 있는 대역폭의 75%를 초과할 수 없습니다. 사용되지 않은 예약된 대역폭은 다른 유형의 시스템 트래픽에서 사용할 수 있게 됩니다. 하지만 Network I/O Control은 시스템 트래픽이 사용하지 않는 용량을 가상 시스템 배치로 재배포하지 않습니다.
- **제한:** 단일 물리적 어댑터에서 시스템 트래픽 유형이 소모할 수 있는 최대 대역폭(Mbps 또는 Gbps).

참고 물리적 네트워크 어댑터 대역폭의 75%까지 예약할 수 있습니다.

예를 들어 ESXi 호스트에 연결된 네트워크 어댑터가 10GbE인 경우 다양한 트래픽 유형에 7.5Gbps 대역폭만 할당할 수 있습니다. 더 많은 용량을 예약되지 않은 상태로 남겨 둘 수 있습니다. 호스트는 공유, 제한 및 사용에 따라 동적으로 예약되지 않은 대역폭을 할당할 수 있습니다. 호스트는 시스템 기능의 작동에 충분한 대역폭만 예약합니다.

N-VDS에서 시스템 트래픽에 대한 Network I/O Control 및 대역폭 할당 구성

NSX-T Data Center 호스트에서 실행 중인 시스템 트래픽에 대한 최소 대역폭을 보장하려면 N-VDS에서 네트워크 리소스 관리를 사용하도록 설정하고 구성합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 패브릭 > 프로파일 > NIOC 프로파일 > 추가**를 선택합니다.
- 3 NIOC 프로파일 세부 정보를 입력합니다.

옵션	설명
이름 및 설명	NIOC 프로파일 이름을 입력합니다. 선택적으로 프로파일 세부 정보(예: 사용하도록 설정된 트래픽 유형)를 입력할 수 있습니다.
상태	트래픽 리소스에 나열된 대역폭 할당을 사용하도록 설정하려면 전환합니다.
호스트 인프라 트래픽 리소스	나열된 기본 트래픽 리소스를 사용할 수 있습니다. 추가 를 클릭하고 트래픽 리소스를 입력하여 NIOC 프로파일을 사용자 지정합니다. (선택 사항) 기존 트래픽 유형을 선택하고 삭제 를 클릭하여 NIOC 프로파일에서 리소스를 제거합니다.

새 NIOC 프로파일이 NIOC 프로파일 목록에 추가됩니다.

API를 사용하여 N-VDS에서 시스템 트래픽에 대한 Network I/O Control 및 대역폭 할당 구성

NSX-T Data Center API를 사용하여 호스트에서 실행 중인 애플리케이션에 대한 네트워크 및 대역폭을 구성할 수 있습니다.

절차

- 1 시스템 정의 및 사용자 정의 호스트 스위치 프로파일을 모두 표시하도록 호스트를 쿼리합니다.
- 2 GET https://<nsx-mgr>/api/v1/host-switch-profiles?include_system_owned=true 항목을 참조하십시오.

호스트에 적용된 NIOC 프로파일이 샘플 응답에 표시됩니다.

```
{
  "description": "This profile is created for Network I/O Control (NIOC).",
  "extends": {
    "$ref": "BaseHostSwitchProfile"+
  },
  "id": "NiocProfile",
  "module_id": "NiocProfile",
  "polymorphic-type-descriptor": {
    "type-identifier": "NiocProfile"
  },
  "properties": {
    "_create_time": {
      "$ref": "EpochMsTimestamp"+,
      "can_sort": true,
      "description": "Timestamp of resource creation",
      "readonly": true
    },
    "_create_user": {
      "description": "ID of the user who created this resource",
      "readonly": true,
      "type": "string"
    },
    "_last_modified_time": {
      "$ref": "EpochMsTimestamp"+,
      "can_sort": true,
      "description": "Timestamp of last modification",
      "readonly": true
    },
    "_last_modified_user": {
      "description": "ID of the user who last modified this resource",
      "readonly": true,
      "type": "string"
    },
    "_links": {
      "description": "The server will populate this field when returning the resource. Ignored on PUT
and POST.",
      "items": {
        "$ref": "ResourceLink"+
      },
      "readonly": true,
      "title": "References related to this resource",
      "type": "array"
    },
  },
}
```

```

    "_protection": {
      "description": "Protection status is one of the following:
        PROTECTED – the client who retrieved the entity is not allowed to modify it.
        NOT_PROTECTED – the client who retrieved the entity is allowed to modify it
        REQUIRE_OVERRIDE – the client who retrieved the entity is a super user and can modify it,
        but only when providing the request header X-Allow-Overwrite=true.
        UNKNOWN – the _protection field could not be determined for this entity.",
      "readonly": true,
      "title": "Indicates protection status of this resource",
      "type": "string"
    },

    "_revision": {
      "description": "The _revision property describes the current revision of the resource.
        To prevent clients from overwriting each other's changes, PUT operations must include the
        current _revision of the resource,
        which clients should obtain by issuing a GET operation.
        If the _revision provided in a PUT request is missing or stale, the operation
        will be rejected.",
      "readonly": true,
      "title": "Generation of this resource config",
      "type": "int"
    },

    "_schema": {
      "readonly": true,
      "title": "Schema for this resource",
      "type": "string"
    },

    "_self": {
      "$ref": "SelfResourceLink+",
      "readonly": true,
      "title": "Link to this resource"
    },

    "_system_owned": {
      "description": "Indicates system owned resource",
      "readonly": true,
      "type": "boolean"
    },

    "description": {
      "can_sort": true,
      "maxLength": 1024,
      "title": "Description of this resource",
      "type": "string"
    },

    "display_name": {
      "can_sort": true,
      "description": "Defaults to ID if not set",
      "maxLength": 255,
      "title": "Identifier to use when displaying entity in logs or GUI",
      "type": "string"
  
```

```

    },

    "enabled": {
      "default": true,
      "description": "The enabled property specifies the status of NIOC feature.

      When enabled is set to true, NIOC feature is turned on and the bandwidth allocations
        specified for the traffic resources are enforced.
      When enabled is set to false, NIOC feature is turned off and no bandwidth allocation is
        guaranteed.

      By default, enabled will be set to true.",

      "nsx_feature": "Nioc",
      "required": false,
      "title": "Enabled status of NIOC feature",
      "type": "boolean"
    },

    "host_infra_traffic_res": {
      "description": "host_infra_traffic_res specifies bandwidth allocation for various traffic
        resources.",
      "items": {
        "$ref": "ResourceAllocation"+
      },
      "nsx_feature": "Nioc",
      "required": false,
      "title": "Resource allocation associated with NiocProfile",
      "type": "array"
    },

    "id": {
      "can_sort": true,
      "readonly": true,
      "title": "Unique identifier of this resource",
      "type": "string"
    },

    "required_capabilities": {
      "help_summary":
        "List of capabilities required on the fabric node if this profile is
        used.
        The required capabilities is determined by whether specific features are enabled in the
        profile.",
      "items": {
        "type": "string"
      },
      "readonly": true,
      "required": false,
      "type": "array"
    },

    "resource_type": {
      "$ref": "HostSwitchProfileType"+,
      "required": true
    }
  }

```

```

    },

    "tags": {
      "items": {
        "$ref": "Tag"+
      },

      "maxItems": 30,
      "title": "Opaque identifiers meaningful to the API user",
      "type": "array"
    },
    },
    "title": "Profile for Nioc",
    "type": "object"
  }
}

```

3 NIOC 프로파일이 없으면 NIOC 프로파일을 생성합니다.

POST <https://<nsx-mgr>/api/v1/host-switch-profiles>

```

{
  "description": "Specify limit, shares and reservation for all kinds of traffic.
  Values for limit and reservation are expressed in percentage. And for shares,
  the value is expressed as a number between 1-100.\n\nThe overall reservation among all traffic
  types should not exceed 75%.
  Otherwise, the API request will be rejected.",
  "id": "ResourceAllocation",
  "module_id": "NiocProfile",
  "nsx_feature": "Nioc",
  "properties": {
    "limit": {
      "default": -1.0,
      "description": "The limit property specifies the maximum bandwidth allocation for a given
      traffic type and is expressed in percentage. The default value for this
      field is set to -1 which means the traffic is unbounded for the traffic
      type. All other negative values for this property is not supported\nand will be rejected by
      the API.",
      "maximum": 100,
      "minimum": -1,
      "required": true,
      "title": "Maximum bandwidth percentage",
      "type": "number"
    },
    "reservation": {
      "default": 0.0,
      "maximum": 75,
      "minimum": 0,
      "required": true,
      "title": "Minimum guaranteed bandwidth percentage",
      "type": "number"
    },
    "shares": {

```

```

    "default": 50,
    "maximum": 100,
    "minimum": 1,
    "required": true,
    "title": "Shares",
    "type": "int"
  },

  "traffic_type": {
    "$ref": "HostInfraTrafficType+",
    "required": true,
    "title": "Resource allocation traffic type"
  }
},

"title": "Resource allocation information for a host infrastructure traffic type",
"type": "object"

```

4 새로 생성된 NIOC 프로파일의 NIOC 프로파일 ID로 전송 노드 구성을 업데이트합니다.

PUT <https://<nsx-mgr>/api/v1/transport-nodes/<TN-id>>

```

{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  "display_name": "NSX Configured TN",
  "host_switch_spec": {
    "resource_type": "StandardHostSwitchSpec",
    "host_switches": [
      {
        "host_switch_profile_ids": [
          {
            "value": "e331116d-f59e-4004-8cfd-c577aefe563a",
            "key": "UplinkHostSwitchProfile"
          },
          {
            "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
            "key": "LldpHostSwitchProfile"
          },
          {
            "value": "b0185099-8003-4678-b86f-edd47ca2c9ad",
            "key": "NiocProfile"
          }
        ],
        "host_switch_name": "nsxvswitch",
        "pnics": [
          {
            "device_name": "vmnic1",
            "uplink_name": "uplink1"
          }
        ],
        "ip_assignment_spec": {
          "resource_type": "StaticIpPoolSpec",

```

```

    "ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
  }
}
],
"transport_zone_endpoints": [
  {
    "transport_zone_id": "e14c6b8a-9edd-489f-b624-f9ef12afbd8f",
    "transport_zone_profile_ids": [
      {
        "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
        "resource_type": "BfdHealthMonitoringProfile"
      }
    ]
  }
]
},
"host_switches": [
  {
    "host_switch_profile_ids": [
      {
        "value": "e331116d-f59e-4004-8cfd-c577aefe563a",
        "key": "UplinkHostSwitchProfile"
      },
      {
        "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
        "key": "LldpHostSwitchProfile"
      }
    ],
    "host_switch_name": "nsxvswitch",
    "pnics": [
      {
        "device_name": "vmnic1",
        "uplink_name": "uplink1"
      }
    ],
    "static_ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
  }
],
"node_id": "41a4eebd-d6b9-11e6-b722-875041b9955d",
"_revision": 0
}

```

- 5** NIOC 프로파일 매개 변수가 `com.vmware.common.respools.cfg` 파일에서 업데이트되었는지 확인합니다.

```
# [root@ host:] net-dvs -l
```

```

      switch 1d 73 f5 58 99 7a 46 6a-9c cc d0 93 17 bb 2a 48 (vswitch)
max ports: 2560
global properties:

com.vmware.common.opaqueDvs = true ,      propType = CONFIG

```

```

com.vmware.nsx.kcp.enable = true ,      propType = CONFIG
com.vmware.common.alias = nsxvswitch ,   propType = CONFIG
com.vmware.common.uplinkPorts: uplink1   propType = CONFIG
com.vmware.common.portset.mtu = 1600, propType = CONFIG
com.vmware.etherswitch.cdp = LLDP, listen propType = CONFIG
com.vmware.common.respools.version = version3, propType = CONFIG
com.vmware.common.respools.cfg:
netsched.pools.persist.ft:0:50:-1:255
netsched.pools.persist.hbr:0:50:-1:255
netsched.pools.persist.vmotion:0:50:-1:255
netsched.pools.persist.vm:0:100:-1:255
netsched.pools.persist.iscsi:0:50:-1:255
netsched.pools.persist.nfs:0:50:-1:255
netsched.pools.persist.mgmt:0:50:-1:255
netsched.pools.persist.vdp:0:50:-1:255
netsched.pools.persist.vsan:0:50:-1:255
propType = CONFIG

```

6 호스트 커널에서 NIOC 프로파일을 확인합니다.

```
# [root@ host:] /get /net/portsets/DvsPortset-1/ports/50335755/nioCVnicInfo
```

```

Vnic NIOC Info
{
  Uplink reserved on:vmnic4
  Reservation in Mbps:200
  Shares:50
  Limit in Mbps:4294967295
  World ID:1001400726
  vNIC Index:0
  Respool Tag:0
  NIOC Version:3
  Active Uplink Bit Map:15
  Parent Respool ID:netsched.pools.persist.vm
}

```

7 NIOC 프로파일 정보를 확인합니다.

```
# [root@ host:] /get /net/portsets/DvsPortset-1/uplinks/vmnic4/nioCVnicInfo
```

```

Uplink NIOC Info
{
  Uplink device:vmnic4
  Link Capacity in Mbps:750
  vm respool reservation:275
  link status:1
  NetSched Ready:1
  Infrastructure reservation:0
  Total VM reservation:200
  Total vnics on this uplink:1
  NIOC Version:3
  Uplink index in BitMap:0
}

```

결과

NSX-T Data Center 호스트에서 실행 중인 애플리케이션에 대해 미리 정의된 대역폭 할당을 가진 NIOC 프로파일이 구성되었습니다.

NSX Edge 클러스터 프로파일 추가

NSX Edge 클러스터 프로파일은 NSX Edge 전송 노드에 대한 정책을 정의합니다.

사전 요구 사항

NSX Edge 클러스터를 사용할 수 있는지 확인합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 패브릭 > 프로파일 > Edge 클러스터 프로파일 > 추가**를 선택합니다.
- 3 NSX Edge 클러스터 프로파일 세부 정보를 입력합니다.

옵션	설명
이름 및 설명	NSX Edge 클러스터 프로파일 이름을 입력합니다. 필요한 경우 BFD(Bidirectional Forwarding Detection) 설정과 같은 프로파일 세부 정보를 입력할 수 있습니다.
BFD 검색 간격	기본 설정을 수락합니다. BFD는 경로 전달 실패를 식별하는 데 사용되는 프로토콜입니다. BFD가 경로 전달 실패를 감지할 간격 타이밍을 설정할 수 있습니다.
BFD 허용 홉	기본 설정을 수락합니다. 프로파일에 허용되는 다중 홉 BFD 세션의 수를 설정할 수 있습니다.
BFD에서 여러 비활성 노드 선언	기본 설정을 수락합니다. 세션을 종료 상태로 플래그 지정하기 전에 BFD 패킷을 수신하지 않을 횟수를 설정할 수 있습니다.
대기 재배치 임계값	기본 설정을 수락합니다.

NSX Edge 브리지 프로파일 추가

NSX Edge 브리지 프로파일은 ESXi 브리지 클러스터에 대한 정책을 정의합니다.

브리지 클러스터는 ESXi 호스트 전송 노드의 모음입니다.

사전 요구 사항

- NSX Edge 클러스터를 사용할 수 있는지 확인합니다.
- ESXi 브리지 클러스터를 사용할 수 있는지 확인합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 패브릭 > 프로파일 > Edge 브리지 프로파일 > 추가**를 선택합니다.
- 3 NSX Edge 클러스터 프로파일 세부 정보를 입력합니다.

옵션	설명
이름 및 설명	NSX Edge 브리지 클러스터 프로파일 이름을 입력합니다. 필요한 경우 기본 및 백업 노드 세부 정보와 같은 프로파일 세부 정보를 입력할 수 있습니다.
Edge 클러스터	사용할 NSX Edge 클러스터를 선택합니다.
기본 노드	클러스터에서 기본 NSX Edge 노드를 지정합니다.
백업 노드	기본 노드가 실패하는 경우 백업 NSX Edge 노드를 지정합니다.
케일오버 모드	선점 또는 비선점 모드 중 하나를 선택합니다. 기본 HA 모드는 선점 모드로, 기본 NSX Edge 노드가 다시 온라인 상태가 되면 트래픽 속도가 저하될 수 있습니다. 비선점 모드에서는 트래픽 속도 저하가 발생하지 않습니다.

전송 노드 프로파일 추가

전송 노드 프로파일은 전송 노드 생성에 필요한 구성을 캡처합니다. 전송 노드 프로파일을 기존 vCenter Server 클러스터에 적용하여 멤버 호스트에 대한 전송 노드를 생성할 수 있습니다. 전송 노드 프로파일은 업링크 프로파일, IP 할당, 업링크 가상 인터페이스에 대한 물리적 NIC의 매핑 등을 포함하여 N-VDS 스위치 구성, 전송 영역, 멤버 호스트를 정의합니다.

참고 전송 노드 프로파일은 NSX Edge 전송 노드에 적용할 필요가 없습니다.

전송 노드 프로파일이 vCenter Server 클러스터에 적용되면 전송 노드 생성이 시작됩니다. NSX Manager는 클러스터에서 호스트를 준비하고 모든 호스트에 NSX-T Data Center 구성 요소를 설치합니다. 호스트의 전송 노드는 전송 노드 프로파일에 지정된 구성에 따라 생성됩니다.

전송 노드 프로파일을 삭제하려면 우선 프로파일을 연결된 클러스터에서 분리해야 합니다. 기존의 전송 노드는 영향받지 않습니다. 클러스터에 추가된 새 호스트는 더 이상 전송 노드로 자동 변환되지 않습니다.

전송 노드 프로파일 생성을 위한 고려 사항:

- 각 구성에 대해 최대 4개의 N-VDS 스위치를 추가할 수 있습니다. 즉, VLAN 전송 영역용으로 생성된 고급 N-VDS, 오버레이 전송 영역용으로 생성된 고급 N-VDS가 이에 해당합니다.
- VLAN 전송 영역에 대해 생성되는 표준 N-VDS 스위치의 수에는 제한이 없습니다.

- 동일한 호스트에서 여러 개의 표준 오버레이 N-VDS 스위치 및 Edge VM을 실행하는 단일 호스트 클러스터 토폴로지에서, NSX-T Data Center는 예를 들어 첫 번째 N-VDS를 통과하는 트래픽이 두 번째 N-VDS를 통과하는 트래픽과 격리되도록 하는 방식으로 트래픽 격리를 제공합니다. 각 N-VDS의 물리적 NIC는 호스트의 Edge VM에 매핑하여 외부 환경에 대한 North-South 트래픽 연결을 허용해야 합니다. 첫 번째 전송 영역의 VM 외부로 이동하는 패킷은 외부 라우터 또는 외부 VM을 통해 두 번째 전송 영역의 VM으로 라우팅되어야 합니다.
- 각 N-VDS 스위치 이름은 고유해야 합니다. NSX-T Data Center는 중복된 스위치 이름의 사용을 허용하지 않습니다.
- 각 전송 영역 ID는 고유해야 합니다. NSX-T Data Center는 중복된 ID의 사용을 허용하지 않습니다.
- 전송 노드 프로파일에 최대 1000개의 전송 영역을 추가할 수 있습니다.
- 전송 영역을 추가하려면 전송 노드 프로파일에 있는 N-VDS에서 해당 전송 영역을 인식해야 합니다.

사전 요구 사항

- 호스트가 vCenter Server 클러스터의 일부인지 확인합니다.
- vCenter Server에는 하나 이상의 클러스터가 있어야 합니다.
- 전송 영역이 구성되어 있는지 확인합니다. [전송 영역 생성](#)의 내용을 참조하십시오.
- 클러스터를 사용할 수 있는지 확인합니다. [UI에서 클러스터를 구성하기 위해 NSX Manager 노드 배포](#)의 내용을 참조하십시오.
- IP 풀이 구성되어 있는지 확인합니다. 그렇지 않으면 네트워크 배포에서 DHCP를 사용할 수 있어야 합니다. [터널 끝점 IP 주소에 대한 IP 풀 생성](#)의 내용을 참조하십시오.
- 계산 관리자가 구성되어 있는지 확인합니다. [계산 관리자 추가](#)의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 패브릭 > 프로파일 > 전송 노드 프로파일 > 추가**를 선택합니다.
- 3 전송 노드 프로파일을 식별하는 이름을 입력합니다.
필요한 경우 전송 노드 프로파일에 대한 설명을 추가할 수 있습니다.
- 4 사용 가능한 전송 영역을 선택하고 > 버튼을 클릭하여 전송 노드 프로파일에 전송 영역을 포함시킵니다.

참고 여러 개의 전송 영역을 추가할 수 있습니다.

5 N-VDS 탭을 클릭하고 스위치 세부 정보를 입력합니다.

옵션	설명
N-VDS 이름	전송 노드가 전송 영역에 연결되었다면 N-VDS에 대해 입력한 이름이 전송 영역에 지정된 N-VDS 이름과 동일한지 확인합니다. 전송 노드는 전송 영역에 연결하지 않고도 생성할 수 있습니다.
연결된 전송 영역	연결된 호스트 스위치에서 인식된 전송 영역을 보여줍니다. 전송 노드 프로파일에 있는 N-VDS에서 인식되지 않은 전송 영역은 추가할 수 없습니다.
NIOC 프로파일	드롭다운 메뉴에서 NIOC 프로파일을 선택합니다. 트래픽 리소스의 프로파일에 지정된 대역폭 할당이 적용됩니다.
업링크 프로파일	드롭다운 메뉴에서 기존 업링크 프로파일을 선택하거나 사용자 지정 업링크 프로파일을 생성합니다. 기본 업링크 프로파일을 사용할 수도 있습니다.
LLDP 프로파일	기본적으로 NSX-T는 LLDP 인접 네트워크에서 LLDP 패킷만 수신합니다. 하지만 LLDP 인접 네트워크로 LLDP 패킷을 전송하고 인접 네트워크에서 LLDP 패킷을 수신하도록 NSX-T를 설정할 수 있습니다.
IP 할당	DHCP 사용, IP 풀 사용 또는 정적 IP 목록 사용 을 선택하여 IP 주소를 전송 노드의 VTEP(가상 터널 끝점)에 할당합니다. 정적 IP 목록 사용 을 선택하면 씬프로 구분된 IP 주소 목록, 게이트웨이 및 서브넷 마스크를 지정해야 합니다. 전송 노드의 모든 VTEP는 동일한 서브넷에 있어야 합니다. 그렇지 않으면 양방향 흐름(BFD) 세션이 설정되지 않습니다.
IP 풀	IP 할당에 대해 IP 풀 사용 을 선택한 경우 IP 풀 이름을 지정합니다.
물리적 NIC	물리적 NIC를 전송 노드에 추가합니다. 기본 업링크를 사용하거나 드롭다운 메뉴에서 기존 업링크를 할당할 수 있습니다. PNIC 추가 를 클릭하여 전송 노드에 대한 추가적인 물리적 NIC를 구성합니다. 참고 이 필드에서 추가하는 물리적 NIC의 마이그레이션은 물리적 NIC 전용 마이그레이션, 설치를 위한 네트워크 매핑 및 제거를 위한 네트워크 매핑 을 어떻게 구성하는지에 따라 결정됩니다.

- 연결된 VMkernel 매핑 없이 사용된 물리적 NIC(예를 들어 표준 vSwitch 또는 vSphere Distributed Switch에서)를 마이그레이션하려면 **물리적 NIC 전용 마이그레이션**을 사용하도록 설정했는지 확인합니다. 사용되고 있는 경우 전송 노드 상태가 **일부 성공**으로 유지되고 패브릭 노드 LCP 연결이 설정되지 않습니다.
- 연결된 VMkernel 네트워크 매핑과 함께 사용된 물리적 NIC를 마이그레이션하려면 **물리적 NIC 전용 마이그레이션**을 사용하지 않도록 설정하고 VMkernel 네트워크 매핑을 구성합니다.
- 사용 가능한 물리적 NIC를 마이그레이션하려면 **물리적 NIC 전용 마이그레이션**을 사용하도록 설정합니다.

옵션	설명
물리적 NIC 전용 마이그레이션	<p>이 필드를 설정하기 전에 다음과 같은 사항을 고려합니다.</p> <ul style="list-style-type: none"> ■ 정의된 물리적 NIC가 사용된 NIC인지 아니면 사용 가능한 NIC인지 파악합니다. ■ 호스트의 VMkernel 인터페이스를 물리적 NIC와 함께 마이그레이션해야 할지 결정합니다. <p>필드 설정:</p> <ul style="list-style-type: none"> ■ VSS 또는 DVS 스위치에서 N-VDS 스위치로 물리적 NIC만 마이그레이션하려면 물리적 NIC 전용 마이그레이션을 사용하도록 설정합니다. ■ 사용된 물리적 NIC 및 연결된 해당 VMkernel 인터페이스 매핑을 마이그레이션하려면 물리적 NIC 전용 마이그레이션을 사용하지 않도록 설정합니다. VMkernel 인터페이스 마이그레이션 매핑이 지정되면 사용 가능한 물리적 NIC가 N-VDS 스위치에 연결됩니다. <p>여러 개의 호스트 스위치가 있는 호스트에서:</p> <ul style="list-style-type: none"> ■ 모든 호스트 스위치가 물리적 NIC만 마이그레이션한다면 한 번으로 작업으로 물리적 NIC를 마이그레이션할 수 있습니다. ■ 일부 호스트 스위치가 VMkernel 인터페이스를 마이그레이션하고 나머지 호스트 스위치가 물리적 NIC만 마이그레이션하는 경우: <ol style="list-style-type: none"> 1 첫 번째 작업에서 물리적 NIC만 마이그레이션합니다. 2 두 번째 작업에서 VMkernel 인터페이스를 마이그레이션합니다. 물리적 NIC 전용 마이그레이션을 사용하지 않도록 설정했는지 확인합니다. <p>물리적 NIC 전용 마이그레이션과 VMkernel 인터페이스 마이그레이션은 여러 호스트에서 동시에 지원되지 않습니다.</p> <p>참고 관리 네트워크 NIC를 마이그레이션하려면 연결된 해당 VMkernel 네트워크 매핑을 구성하고 물리적 NIC 전용 마이그레이션을 사용하지 않도록 설정한 상태로 둡니다. 관리 NIC만 마이그레이션하면 호스트 연결이 끊어집니다.</p> <p>자세한 내용은 N-VDS 스위치로 VMkernel 마이그레이션 항목을 참조하십시오.</p>

옵션	설명
설치를 위한 네트워크 매핑	<p>설치 중에 VMkernel을 N-VDS 스위치에 마이그레이션하려면 VMkernel을 기존의 논리적 스위치에 매핑합니다. NSX Manager가 N-VDS의 매핑된 논리적 스위치에 VMkernel을 마이그레이션합니다.</p> <p>경고 관리 NIC 및 관리 VMkernel 인터페이스가 마이그레이션 전 관리 NIC가 연결되어 있던 동일한 VLAN과 연결된 논리적 스위치로 마이그레이션되었는지 확인하십시오. <code>vmnic<n></code> 및 <code>VMkernel<n></code>이 서로 다른 VLAN으로 마이그레이션되면 호스트에 대한 연결이 끊어집니다.</p> <p>경고 고정된 물리적 NIC의 경우 VMkernel 인터페이스에 대한 물리적 NIC의 호스트 스위치 매핑이 전송 노드 프로파일에 지정된 구성과 일치하는지 확인하십시오. NSX-T Data Center는 검증 절차의 일부로 매핑을 확인합니다. 검증이 통과되면 N-VDS 스위치로 VMkernel 인터페이스의 마이그레이션이 성공합니다. NSX-T Data Center는 VMkernel 인터페이스를 N-VDS 스위치로 마이그레이션한 후 호스트의 매핑 구성을 저장하지 않으므로 제거를 위한 네트워크 매핑도 구성해야 합니다. 매핑이 구성되지 않으면 VSS 또는 VDS 스위치로 다시 마이그레이션한 후 서비스(예: vSAN)에 대한 연결이 손실될 수 있습니다.</p> <p>자세한 내용은 N-VDS 스위치로 VMkernel 마이그레이션 항목을 참조하십시오.</p>
제거를 위한 네트워크 매핑	<p>제거 중에 VMkernel의 마이그레이션을 되돌리려면 VMkernel을 VSS 또는 DVS의 포트 그룹에 매핑하여 VMkernel이 다시 마이그레이션되어야 하는 VSS 또는 DVS의 포트 그룹을 NSX Manager가 알 수 있도록 합니다. DVS 스위치의 경우 포트 그룹의 유형이 사용 후 삭제인지 확인합니다.</p> <p>경고 고정된 물리적 NIC의 경우 VMkernel 인터페이스에 대한 물리적 NIC의 전송 노드 프로파일 매핑이 호스트 스위치에 지정된 구성과 일치하는지 확인하십시오. NSX-T Data Center는 VMkernel 인터페이스를 N-VDS 스위치로 마이그레이션한 후 호스트의 매핑 구성을 저장하지 않으므로 필수적으로 제거를 위한 네트워크 매핑을 구성해야 합니다. 매핑이 구성되지 않으면 VSS 또는 VDS 스위치로 다시 마이그레이션한 후 서비스(예: vSAN)에 대한 연결이 손실될 수 있습니다.</p> <p>자세한 내용은 N-VDS 스위치로 VMkernel 마이그레이션 항목을 참조하십시오.</p>

6 여러 전송 영역을 선택한 경우에는 **+ N-VDS 추가**를 다시 클릭하여 다른 전송 영역에 대해 스위치를 구성합니다.

7 완료를 클릭하여 구성을 완료합니다.

다음에 수행할 작업

기존 vSphere 클러스터에 전송 노드 프로파일을 적용합니다. [관리 호스트 전송 노드 구성](#)의 내용을 참조하십시오.

N-VDS 스위치로 VMkernel 마이그레이션

VMkernel 인터페이스를 VSS 또는 DVS 스위치에서 클러스터 수준의 N-VDS 스위치로 마이그레이션하려면, 마이그레이션에 필요한 네트워크 매핑 세부 정보를 사용하여 전송 노드 프로파일을 구성합니다 (VMkernel 인터페이스를 논리 스위치에 매핑). 마찬가지로 호스트 노드에서 VMkernel 인터페이스를 마이그레이션하려면 전송 노드 구성을 구성합니다. 마이그레이션된 VMkernel 인터페이스를 VSS 또는 DVS 스위치로 되돌리려면, 제거 중에 구현될 전송 노드 프로파일의 네트워크 매핑(논리적 포트를 VMkernel 인터페이스에 매핑) 제거를 구성합니다.

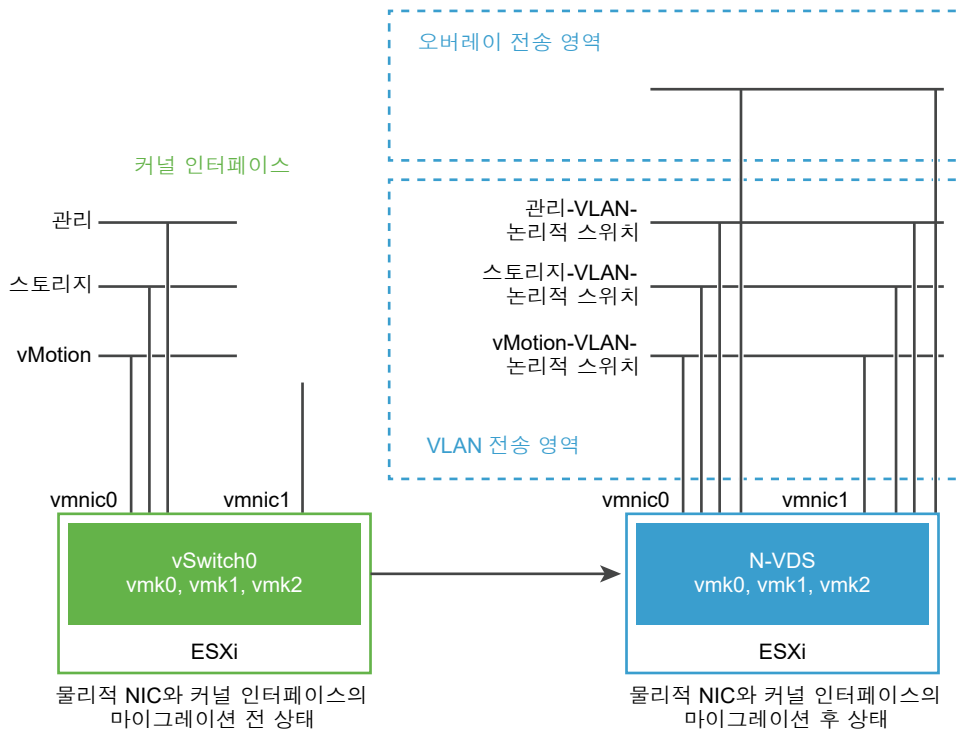
마이그레이션하는 동안 현재 사용 중인 물리적 NIC는 N-VDS 스위치로 마이그레이션되고 사용 가능한 물리적 NIC는 마이그레이션 후 N-VDS 스위치에 연결됩니다.

참고 전송 노드 프로파일은 클러스터의 모든 멤버 호스트에 적용됩니다. 하지만 특정 호스트에서 VMkernel 인터페이스의 마이그레이션을 제한하려면 호스트를 직접 구성하면 됩니다. 마이그레이션 후에 N-VDS는 N-VDS 스위치에 연결된 인터페이스에 대한 VLAN 및 오버레이 네트워크의 트래픽을 처리합니다.

중요 개별 호스트에 대해 수행된 구성에는 재정의된 플래그가 표시됩니다. 전송 노드 프로파일에 대한 이후 업데이트는 재정의된 호스트에 적용되지 않습니다. 이러한 호스트 NSX-T Data Center가 제거될 때까지 재정의된 상태로 유지됩니다.

다음 그림에서 호스트에 물리적 NIC만 두 개 있는 경우, 인터페이스가 호스트와 연결이 끊어지지 않도록 이중화를 위해 두 NIC 모두를 N-VDS에 할당하고 관련 VMkernel 인터페이스를 할당할 수 있습니다.

그림 10-2. 네트워크 인터페이스를 N-VDS로 마이그레이션하기 전과 후



마이그레이션을 수행하기 전에 ESXi 호스트에는 두 개의 물리적 포트(vmnic0 및 vmnic1)에서 파생된 두 개의 업링크가 있습니다. 여기서 vmnic0은 활성 상태로 구성되고 VSS에 연결되는 반면 vmnic1은 사용되지 않습니다. 또한 vmk0, vmk1 및 vmk2라는 세 개의 VMkernel 인터페이스가 있습니다.

NSX-T Data Center Manager UI 또는 NSX-T Data Center API를 사용하여 VMkernel 인터페이스를 마이그레이션할 수 있습니다. "NSX-T Data Center API 가이드" 항목을 참조하십시오.

마이그레이션 후, vmnic0, vmnic1 및 해당 VMkernel 인터페이스는 N-VDS 스위치로 마이그레이션됩니다. vmnic0과 vmnic1 모두는 VLAN 및 오버레이 전송 영역을 통해 연결됩니다.

VMkernel 마이그레이션에 대한 고려 사항

- PNIC 및 VMkernel 마이그레이션: 고정된 물리적 NIC 및 관련 VMkernel 인터페이스를 N-VDS 스위치로 마이그레이션하기 전에 호스트 스위치의 네트워크 매핑(물리적 NIC와 포트 그룹 매핑)을 적어둡니다.
- PNIC 전용 마이그레이션: PNIC만 마이그레이션하려는 경우 관리 VMkernel 인터페이스에 연결된 물리적 관리 NIC가 마이그레이션되지 않도록 합니다. 그렇게 되면 호스트와의 연결이 끊어집니다. 자세한 내용은 [전송 노드 프로파일 추가](#)에서 **PNIC 전용 마이그레이션** 필드를 참조하십시오.
- 마이그레이션 되돌리기: 마이그레이션된 VMkernel 인터페이스를 고정된 물리적 NIC에 대한 VSS 또는 DVS 호스트 스위치로 되돌리려면 호스트 스위치의 네트워크 매핑(물리적 NIC와 포트 그룹 매핑)을 적어둡니다. **제거를 위한 네트워크 매핑** 필드에서 호스트 스위치 매핑으로 전송 노드 프로파일을 구성하는 것은 필수입니다. 이 매핑이 없으면 NSX-T Data Center는 VMkernel 인터페이스를 다시 마이그레이션해야 하는 포트 그룹을 알 수 없습니다. 이렇게 되면 vSAN 네트워크에 대한 연결이 끊어질 수 있습니다.
- 마이그레이션 전에 vCenter Server 등록: DVS 스위치에 연결된 VMkernel 또는 PNIC를 마이그레이션하려면 vCenter Server가 NSX Manager에 등록되어 있는지 확인합니다.
- VLAN ID 일치 : 마이그레이션 후 관리 NIC 및 관리 VMkernel 인터페이스는 마이그레이션 전에 관리 NIC가 연결되었던 VLAN에 있어야 합니다. vmnic0 및 vmk0이 관리 네트워크에 연결되고 서로 다른 VLAN에 마이그레이션되면 호스트에 대한 연결이 끊어집니다.
- VSS 스위치로 마이그레이션: 두 VMkernel 인터페이스를 VSS 스위치의 동일한 포트 그룹으로 마이그레이션할 수 없습니다.
- vMotion: vMotion을 수행하여 VMkernel 및/또는 PNIC 마이그레이션 전에 VM 워크로드를 다른 호스트로 이동합니다. 마이그레이션이 실패해도 워크로드 VM은 영향을 받지 않습니다.
- vSAN: vSAN 트래픽이 호스트에서 실행 중인 경우 vCenter Server를 통해 호스트를 유지 보수 모드로 전환하고 VMkernel 및/또는 PNIC 마이그레이션 전에 vMotion 기능을 사용하여 호스트 외부로 VM을 이동합니다.
- 마이그레이션: VMkernel이 이미 대상 스위치에 연결되어 있는 경우에도 동일한 스위치로 마이그레이션하도록 선택할 수 있습니다. 이 속성은 VMK 및/또는 PNIC 마이그레이션 작업을 멍등(idempotent)으로 만듭니다. 이를 통해 PNIC만 대상 스위치로 마이그레이션할 수 있습니다. 마이그레이션에는 항상 하나 이상의 VMkernel 및 PNIC가 필요하므로, PNIC만 대상 스위치로 마이그레이션할 경우에는 이미 대상 스위치로 마이그레이션된 VMkernel을 선택합니다. VMkernel을 마이그레이션할 필요가 없으면 소스 스위치 또는 대상 스위치에서 vCenter Server를 통해 임시 VMkernel을 생성합니다. 그런 다음, PNIC와 함께 마이그레이션하고, 마이그레이션이 완료된 후 vCenter Server를 통해 임시 VMkernel을 삭제합니다.
- MAC 공유: VMkernel 인터페이스 및 PNIC가 동일한 MAC을 공유하고 동일한 스위치에 있는 경우, 마이그레이션 후 둘 다 사용하려면 동일한 대상 스위치로 함께 마이그레이션해야 합니다. 항상 vmk0 및 vmnic0를 동일한 스위치에 유지합니다.

다음 명령을 실행하여 호스트의 모든 VMK 및 PNIC에서 사용하는 MAC을 확인합니다.

```
esxcfg-vmknics -l
```

```
esxcfg-nics -l
```

- 마이그레이션 후 VIF 논리적 포트가 생성됨: VMkernel을 VSS 또는 DVS 스위치에서 N-VDS 스위치로 마이그레이션한 후에는 VIF 유형의 논리적 스위치 포트가 NSX Manager에 생성됩니다. 이러한 VIF 논리적 스위치 포트에는 분산 방화벽 규칙을 생성하면 안 됩니다.

VMkernel 인터페이스를 N-VDS 스위치로 마이그레이션

VMkernel 인터페이스를 N-VDS 스위치로 마이그레이션하는 개괄적인 워크플로:

- 1 필요한 경우 논리적 스위치를 생성합니다.
- 2 VMkernel 인터페이스와 PNIC가 N-VDS 스위치로 마이그레이션되는 호스트의 VM 전원을 끕니다.
- 3 전송 노드 생성 중에 VMkernel 인터페이스를 마이그레이션하는 데 사용되는 네트워크 매핑을 사용하여 전송 노드 프로파일을 구성합니다. 네트워크 매핑은 VMkernel 인터페이스를 논리적 스위치에 매핑하는 것을 의미합니다.

자세한 내용은 [전송 노드 프로파일 추가](#) 항목을 참조하십시오.

- 4 vCenter Server의 네트워크 어댑터 매핑이 VMkernel 스위치와 N-VDS 스위치의 새로운 연결을 반영하는지 확인합니다. 고정된 물리적 NIC의 경우, NSX-T Data Center의 매핑이 vCenter Server의 물리적 NIC에 고정된 VMkernel을 반영하는지 확인합니다.
- 5 NSX Manager에서 **고급 네트워킹 및 보안 > 네트워킹 > 스위칭**으로 이동합니다. **스위칭** 페이지에서 새로 생성된 논리적 포트를 통해 VMkernel 인터페이스가 논리적 스위치에 연결되어 있는지 확인합니다.
- 6 **시스템 > 노드 > 호스트 전송 노드**로 이동합니다. 각 전송 노드에 대해 **노드 상태** 열의 상태가 성공인지 확인하여 전송 노드 구성이 성공적으로 검증되었는지 확인합니다.
- 7 **호스트 전송 노드** 페이지에서 **구성 상태**가 성공인지 확인하여 호스트가 지정된 구성으로 성공적으로 구현되었는지 확인합니다.

NSX-T UI 또는 전송 노드 API를 사용하여 VMkernel 인터페이스 및 PNIC를 VDS에서 N-VDS 스위치로 마이그레이션한 후 vCenter Server에서 VDS에 대한 주의를 표시합니다. 호스트를 VDS에 연결해야 하는 경우 호스트를 VDS에서 제거합니다. vCenter Server는 더 이상 VDS에 대한 주의를 표시하지 않습니다.

마이그레이션 중 발생할 수 있는 오류에 대한 자세한 내용은 [VMkernel 마이그레이션 오류](#) 항목을 참조하십시오.

VMkernel 인터페이스를 VSS 또는 DVS 스위치로 마이그레이션 되돌리기

NSX-T Data Center를 제거하는 동안 VMkernel 인터페이스를 N-VDS 스위치에서 VSS 또는 DVS 스위치로 마이그레이션한 것을 되돌리는 개괄적인 워크플로입니다.

- 1 ESXi 호스트에서 마이그레이션 후 VMkernel 인터페이스를 호스팅하는 논리적 포트에 연결된 VM의 전원을 끕니다.

- 제거 프로세스 중에 VMkernel 인터페이스를 마이그레이션하는 데 사용되는 네트워크 매핑으로 전송 노드 프로파일을 구성합니다. 제거 중 네트워크 매핑은 VMkernel 인터페이스를 ESXi 호스트의 VSS 또는 DVS 스위치의 포트 그룹에 매핑합니다.

참고 VMkernel 마이그레이션을 DVS 스위치의 포트 그룹으로 되돌리려면, 포트 그룹 유형이 사용 후 삭제로 설정되어 있어야 합니다.

자세한 내용은 [전송 노드 프로파일 추가](#) 항목을 참조하십시오.

- vCenter Server의 네트워크 어댑터 매핑이 VMkernel 스위치와 DVS 스위치 또는 VSS의 포트 그룹과의 새로운 연결을 반영하는지 확인합니다.
- NSX Manager에서 **고급 네트워킹 및 보안 > 네트워킹 > 스위칭**으로 이동합니다. **스위치** 페이지에서 VMkernel 인터페이스가 포함된 논리적 스위치가 삭제되었는지 확인합니다.

마이그레이션 중 발생할 수 있는 오류에 대한 자세한 내용은 [VMkernel 마이그레이션 오류](#) 항목을 참조하십시오.

호스트 스위치 매핑 업데이트

중요

- **상태 저장 호스트:** 추가 및 업데이트 작업이 지원됩니다. 기존 매핑을 업데이트하려면 네트워크 매핑 구성에 새 VMkernel 인터페이스 항목을 추가하면 됩니다. N-VDS 스위치로 이미 마이그레이션된 VMkernel 인터페이스의 네트워크 매핑 구성을 업데이트하면 업데이트된 네트워크 매핑이 호스트에서 구현되지 않습니다.
- **상태 비저장 호스트:** 추가, 업데이트 및 제거 작업이 지원됩니다. 네트워크 매핑 구성을 변경하면 호스트가 재부팅된 후에 인식됩니다.

VMkernel 인터페이스를 새 논리적 스위치로 업데이트하려면 클러스터 수준에서 네트워크 매핑을 적용하도록 전송 노드프로파일을 편집하면 됩니다. 업데이트를 단일 호스트에만 적용하려면 호스트 수준 API를 사용하여 전송 노드를 구성합니다.

참고 개별 호스트에 대한 전송 노드 구성을 업데이트하면 전송 노드 프로파일을 통해 적용된 새 업데이트가 해당 호스트에 적용되지 않습니다. 해당 호스트 상태는 재정의됨이 됩니다.

- 클러스터의 모든 호스트를 업데이트하려면 VMkernel 매핑을 논리적 스위치로 업데이트하도록 **설치 중 네트워크 매핑** 필드를 편집합니다.

자세한 내용은 [전송 노드 프로파일 추가](#) 항목을 참조하십시오.

- 변경 내용을 저장합니다. 전송 노드 프로파일에서 변경한 내용은 재정의됨 상태로 표시된 호스트를 제외하고 클러스터의 모든 멤버 호스트에 자동으로 적용됩니다.
- 마찬가지로 개별 호스트를 업데이트하려면 전송 노드 구성에서 VMkernel 매핑을 편집합니다.

참고 **설치 중 네트워크 매핑** 필드를 새로운 VMkernel 매핑으로 업데이트하는 경우에는 **제거 중 네트워크 매핑** 필드에 동일한 VMkernel 인터페이스가 추가되어야 합니다.

마이그레이션 중 발생할 수 있는 오류에 대한 자세한 내용은 [VMkernel 마이그레이션 오류](#) 항목을 참조하십시오.

상태 비저장 클러스터에서 VMkernel 인터페이스 마이그레이션

- 1 전송 노드 API를 사용하여 호스트를 참조 호스트로 준비하고 구성합니다.
- 2 참조 호스트에서 호스트 프로파일을 추출합니다.
- 3 vCenter Server에서 상태 비저장 클러스터에 호스트 프로파일을 적용합니다.
- 4 NSX-T Data Center에서 상태 비저장 클러스터에 전송 노드 프로파일을 적용합니다.
- 5 클러스터의 각 호스트를 재부팅합니다.

클러스터 호스트에서 업데이트된 상태를 인식하는 데 몇 분 정도 걸릴 수 있습니다.

마이그레이션 실패 시나리오

- 어떤 이유로 마이그레이션이 실패하면 호스트는 물리적 NIC와 VMkernel 인터페이스를 마이그레이션하려고 세 번 시도합니다.
- 마이그레이션이 계속 실패하면 호스트는 물리적 관리 NIC인 vmnic0과의 VMkernel 연결을 유지하여 이전 구성으로 롤백합니다.
- 롤백이 실패하여 물리적 관리 NIC에 구성된 VMkernel이 손실되면 호스트를 재설정해야 합니다.

지원되지 않는 마이그레이션 시나리오

지원되는 않는 시나리오는 다음과 같습니다.

- 두 개의 서로 다른 VSS 또는 DVS 스위치의 VMkernel 인터페이스가 동시에 마이그레이션됩니다.
- 상태 저장 호스트에서는 VMkernel 인터페이스를 또 다른 논리적 스위치에 매핑하도록 네트워크 매핑이 업데이트됩니다. 예를 들어, 마이그레이션 전에 VMkernel은 논리적 스위치 1에 매핑되고 VMkernel 인터페이스는 논리적 스위치 2에 매핑됩니다.

VMkernel 마이그레이션 오류

VMkernel 인터페이스와 물리적 NIC를 VSS 또는 DVS 스위치에서 N-VDS 스위치로 마이그레이션하거나 인터페이스 마이그레이션을 VSS 또는 DVS 호스트 스위치로 되돌릴 때 오류가 발생할 수 있습니다.

표 10-1. VMkernel 마이그레이션 오류

오류 코드	문제	원인	해결 방법
8224	전송 노드 구성에 지정된 호스트 스위치를 찾을 수 없습니다.	호스트 스위치 ID를 찾을 수 없습니다.	<ul style="list-style-type: none"> ■ 호스트 스위치 이름을 사용하여 전송 영역을 생성한 후 전송 노드를 생성합니다. ■ 전송 노드 구성에 올바른 호스트 스위치를 사용합니다.
8225	VMkernel 마이그레이션이 진행 중입니다.	마이그레이션이 진행 중입니다.	다른 작업을 수행하기 전에 마이그레이션이 완료될 때까지 기다립니다.
8226	VMkernel 마이그레이션이 ESXi 호스트에서만 지원됩니다.	마이그레이션이 ESXi 호스트에 대해서만 유효합니다.	마이그레이션을 시작하기 전에 호스트가 ESXi 호스트인지 확인합니다.
8227	VMkernel 인터페이스에 호스트 스위치 이름이 추가되어 있지 않습니다.	여러 개의 호스트 스위치가 있는 호스트에서 NSX-T Data Center가 각 VMkernel 인터페이스와 해당 호스트 스위치의 연결을 식별하지 못합니다.	<p>호스트에 여러 개의 N-VDS 호스트 스위치가 있는 경우 호스트가 연결되어 있는 N-VDS의 호스트 스위치 이름이 VMkernel 인터페이스에 추가되어 있는지 확인합니다.</p> <p>예를 들어 N-VDS 호스트 스위치 이름이 nsxvswitch1 및 VMkernel1이고 다른 N-VDS 호스트 스위치 이름이 nsxvswitch2 및 VMkernel2인 호스트의 제거를 위한 네트워크 매핑은 다음과 같이 정의되어야 합니다. device_name: VMkernel1@nsxvswitch1, destination_network: DPortGroup.</p>
8228	device_name 필드에 사용된 호스트 스위치를 호스트에서 찾을 수 없습니다.	호스트 스위치 이름이 잘못되었습니다.	올바른 호스트 스위치 이름을 입력합니다.
8229	전송 노드에서 논리적 스위치의 전송 영역을 지정하지 않았습니다.	전송 영역이 추가되지 않았습니다.	전송 노드 구성에 전송 영역을 추가합니다.
8230	호스트 스위치에 물리적 NIC가 없습니다.	호스트 스위치에는 물리적 NIC가 최소 하나 있어야 합니다.	업링크 프로파일에 하나 이상의 물리적 NIC를 지정하고 논리적 스위치에 VMkernel 네트워크 매핑을 지정합니다.
8231	호스트 스위치 이름이 일치하지 않습니다.	vmk1@host_switch에 사용된 호스트 스위치 이름이 인터페이스의 대상 논리적 스위치에서 사용하는 호스트 스위치 이름과 일치하지 않습니다.	네트워크 매핑 구성에 지정된 호스트 스위치 이름이 인터페이스의 논리적 스위치에서 사용하는 이름과 일치하는지 확인합니다.
8232	호스트에서 논리적 스위치가 인식되지 않습니다.	호스트에서 논리적 스위치를 인식하지 못했습니다.	호스트를 NSX Manager와 동기화합니다.

표 10-1. VMkernel 마이그레이션 오류 (계속)

오류 코드	문제	원인	해결 방법
8233	네트워크 인터페이스 매핑에 예기치 않은 논리적 스위치가 있습니다.	설치 및 제거를 위한 네트워크 인터페이스 매핑이 논리적 스위치와 포트 그룹을 모두 나열합니다.	설치를 위한 네트워크 매핑에는 논리적 스위치만 대상으로 포함되어야 합니다. 마찬가지로, 제거를 위한 네트워크 매핑에는 포트 그룹만 대상으로 포함되어야 합니다.
8294	네트워크 인터페이스 매핑에 논리적 스위치가 없습니다.	논리적 스위치가 지정되지 않았습니다.	네트워크 인터페이스 매핑 구성에 논리적 스위치가 지정되어 있는지 확인합니다.
8296	호스트 스위치가 불일치합니다.	제거를 위한 네트워크 인터페이스 매핑이 잘못된 호스트 스위치 이름으로 구성되었습니다.	매핑 구성에 사용된 호스트 스위치 이름이 VMkernel 인터페이스가 상주하는 호스트 스위치에 입력된 이름과 일치하는지 확인합니다.
8297	VMkernel이 중복됩니다.	중복된 VMkernel을 마이그레이션하도록 지정했습니다.	설치 또는 제거 매핑 구성에 중복된 VMkernel 인터페이스를 지정하지 않아야 합니다.
8298	VMkernel 인터페이스 및 대상의 수가 불일치합니다.	구성이 잘못되었습니다.	구성에서 각 VMkernel 인터페이스에 대해 해당하는 대상을 지정했는지 확인합니다.
8299	VMkernel 인터페이스가 N-VDS의 포트를 사용 중이어서 전송 노드를 삭제할 수 없습니다.	VMkernel 인터페이스가 N-VDS 스위치의 포트를 사용 중입니다.	모든 VMkernel 인터페이스의 마이그레이션을 N-VDS 스위치에서 VSS/DVS 스위치로 되돌립니다. 그런 다음 전송 노드 삭제를 시도합니다.
9412	한 N-VDS에서 다른 N-VDS로 VMkernel을 마이그레이션할 수 없습니다.	지원되지 않는 작업입니다.	VMkernel 인터페이스의 마이그레이션을 VSS 또는 DVS 스위치로 되돌립니다. 그러면 VMkernel 인터페이스를 다른 N-VDS 스위치로 마이그레이션할 수 있습니다.
9413	VMkernel 인터페이스를 다른 논리적 스위치로 마이그레이션할 수 없습니다.	상태 저장 호스트에서, 한 논리적 스위치에 연결된 VMkernel을 다른 논리적 스위치로 마이그레이션할 수 없습니다.	VMkernel의 마이그레이션을 논리적 스위치에서 VSS/DVS 스위치로 되돌립니다. 그런 다음 VMkernel을 N-VDS의 다른 논리적 스위치로 마이그레이션합니다.
9414	VMkernel 인터페이스가 중복됩니다.	설치 및 제거 매핑 구성에 중복된 VMkernel 인터페이스가 매핑되어 있습니다.	각 VMkernel 인터페이스가 설치 및 제거 매핑에서 고유한지 확인합니다.
9415	호스트에서 VM의 전원이 켜져 있습니다.	VM의 전원이 켜져 있을 때 마이그레이션이 진행되지 않습니다.	VMkernel 인터페이스의 마이그레이션을 시작하기 전에 호스트에서 VM의 전원을 끕니다.
9416	호스트에서 VMkernel을 찾을 수 없습니다.	네트워크 매핑 구성의 호스트에 있는 VMkernel을 지정하지 않았습니다.	네트워크 매핑 구성에 있는 VMkernel을 지정합니다.
9417	포트 그룹을 찾을 수 없습니다.	네트워크 매핑 구성의 호스트에 있는 포트 그룹을 지정하지 않았습니다.	네트워크 매핑 구성에 있는 포트 그룹을 지정합니다.

표 10-1. VMkernel 마이그레이션 오류 (계속)

오류 코드	문제	원인	해결 방법
9419	마이그레이션 중에 논리적 스위치를 찾을 수 없습니다.	네트워크 인터페이스 매핑 구성에 정의된 논리적 스위치를 찾을 수 없습니다.	네트워크 인터페이스 매핑 구성에 있는 논리적 스위치를 지정합니다.
9420	마이그레이션 중에 논리적 포트를 찾을 수 없습니다.	마이그레이션 중에 NSX-T Data Center가 논리적 스위치에서 생성된 포트를 찾을 수 없습니다.	마이그레이션이 성공하려면 논리적 스위치에서 논리적 포트를 삭제하지 말아야 합니다.
9421	마이그레이션 프로세스 검증을 위한 호스트 정보가 누락되었습니다.	인벤토리에서 호스트 정보를 검색할 수 없습니다.	마이그레이션 프로세스를 다시 시도합니다.
9423	VMkernel 인터페이스에 고정된 물리적 NIC가 올바른 호스트 스위치로 마이그레이션되지 않았습니다.	환경에 고정된 물리적 NIC가 있지만 VMkernel 및 물리적 NIC가 동일한 호스트 스위치로 마이그레이션되지 않습니다.	VMkernel 인터페이스에 고정된 물리적 NIC에는 물리적 NIC를 동일한 호스트 스위치의 VMkernel에 매핑하는 전송 노드 구성이 있어야 합니다.
600	개체를 찾을 수 없습니다.	논리적 스위치에서 사용하는 지정된 전송 영역이 없습니다. VMK 매핑 대상에 있는 논리적 스위치를 찾을 수 없습니다.	<ul style="list-style-type: none"> ■ 환경에 있는 전송 영역을 지정합니다. ■ 원하는 논리적 스위치를 생성하거나 기존의 VLAN 논리적 스위치를 사용합니다.
8310	논리적 스위치 유형이 잘못되었습니다.	논리적 스위치 유형이 [오버레이]입니다.	VLAN 논리적 스위치를 생성합니다.
9424	물리적 NIC 전용 마이그레이션 및 설치 또는 제거를 위한 네트워크 매핑 설정이 동시에 구성된 경우 마이그레이션을 수행할 수 없습니다.	이러한 설정 중 하나가 구성된 경우에만 마이그레이션이 진행됩니다.	물리적 NIC 전용 마이그레이션이나 설치 또는 제거를 위한 네트워크 매핑 설정 중 하나만 구성했는지 확인합니다.

독립형 호스트 또는 베어메탈 서비스 전송 노드 생성

우선 ESXi 호스트, KVM 호스트 또는 베어메탈 서버를 NSX-T Data Center 패브릭에 추가한 다음 전송 노드를 구성해야 합니다.

패브릭 노드는 NSX-T Data Center 관리부에 등록되어 있고 NSX-T Data Center 모듈이 설치된 노드입니다. 호스트 또는 베어메탈 서버가 NSX-T Data Center 오버레이에 속하려면 먼저 이를 NSX-T Data Center 패브릭에 추가해야 합니다.

전송 노드는 NSX-T Data Center 오버레이 또는 NSX-T Data Center VLAN 네트워킹에 참여하는 노드입니다.

KVM 호스트 또는 베어메탈 서버의 경우 N-VDS를 미리 구성하거나 NSX Manager에서 구성이 수행되도록 할 수 있습니다. ESXi 호스트의 경우 NSX Manager에서 항상 N-VDS를 구성합니다.

참고 템플릿 VM에서 전송 노드를 생성하려는 경우 `/etc/vmware/nsx/`에서 호스트에 인증서가 없는지 확인합니다. netcpa 에이전트는 인증서가 있으면 인증서를 생성하지 않습니다.

베어메탈 서버는 오버레이 및 VLAN 전송 영역을 지원합니다. 관리 인터페이스를 사용하여 베어메탈 서버를 관리할 수 있습니다. 애플리케이션 인터페이스를 사용하면 베어메탈 서버의 애플리케이션에 액세스할 수 있습니다.

단일 물리적 NIC는 관리 및 애플리케이션 IP 인터페이스 모두에 대해 IP 주소를 제공합니다.

이중 물리적 NIC는 관리 인터페이스에 대해 물리적 NIC와 고유한 IP 주소를 제공합니다. 이중 물리적 NIC는 애플리케이션 인터페이스에 대해서도 물리적 NIC와 고유한 IP 주소를 제공합니다.

결합된 구성의 다중 물리적 NIC는 관리 인터페이스에 대해 이중 물리적 NIC와 고유한 IP 주소를 제공합니다. 결합된 구성의 다중 물리적 NIC는 애플리케이션 인터페이스에 대해서도 이중 물리적 NIC와 고유한 IP 주소를 제공합니다.

각 구성에 대해 최대 4개의 N-VDS 스위치를 추가할 수 있습니다. 즉, VLAN 전송 영역용으로 생성된 표준 N-VDS와 고급 N-VDS, 오버레이 전송 영역용으로 생성된 표준 N-VDS와 고급 N-VDS가 이에 해당합니다.

동일한 호스트에서 여러 개의 표준 오버레이 N-VDS 스위치 및 Edge VM을 실행하는 단일 호스트 클러스터 토폴로지에서, NSX-T Data Center는 예를 들어 첫 번째 N-VDS를 통과하는 트래픽이 두 번째 N-VDS를 통과하는 트래픽과 격리되도록 하는 방식으로 트래픽 격리를 제공합니다. 각 N-VDS의 물리적 NIC는 호스트의 Edge VM에 매핑하여 외부 환경에 대한 North-South 트래픽 연결을 허용해야 합니다. 첫 번째 전송 영역의 VM 외부로 이동하는 패킷은 외부 라우터 또는 외부 VM을 통해 두 번째 전송 영역의 VM으로 라우팅되어야 합니다.

사전 요구 사항

- 호스트는 관리부에 연결되어야 하고 연결이 [실행 중]이어야 합니다.
- 전송 영역을 구성해야 합니다.
- 업링크 프로파일을 구성해야 하며, 기본 업링크 프로파일을 사용할 수도 있습니다.
- IP 풀을 구성해야 하며, 그렇지 않은 경우 네트워크 배포에서 DHCP를 사용할 수 있어야 합니다.
- 하나 이상의 미사용 물리적 NIC를 호스트 노드에서 사용할 수 있어야 합니다.
- 호스트 이름
- 관리 IP 주소
- 사용자 이름
- 암호
- (선택 사항) (KVM) SHA-256 SSL 지문

- (선택 사항) (ESXi) SHA-256 SSL 지문
- 필요한 타사 패키지가 설치되어 있는지 확인합니다. [KVM 호스트에 타사 패키지 설치](#)의 내용을 참조하십시오.

절차

- 1 (선택 사항) 패브릭에 호스트를 추가할 때 제공할 수 있도록 하이퍼바이저 지문을 검색합니다.

- a 하이퍼바이저 지문 정보를 수집합니다.

Linux 셸을 사용합니다.

```
# echo -n | openssl s_client -connect <esxi-ip-address>:443 2>/dev/null | openssl x509 -noout -fingerprint -sha256
```

호스트에서 ESXi CLI를 사용합니다.

```
[root@host:~] openssl x509 -in /etc/vmware/ssl/rui.crt -fingerprint -sha256 -noout
SHA256
Fingerprint=49:73:F9:A6:0B:EA:51:2A:15:57:90:DE:C0:89:CA:7F:46:8E:30:15:CA:4D:5C:95:28:0A:9E:A
2:4E:3C:C4:F4
```

- b KVM 하이퍼바이저에서 SHA-256 지문을 검색하고, KVM 호스트에서 명령을 실행합니다.

```
# awk '{print $2}' /etc/ssh/ssh_host_rsa_key.pub | base64 -d | sha256sum -b | sed 's/ .*$//'  
| xxd -r -p | base64
```

- 2 시스템 > 패브릭 > 노드 > 호스트 전송 노드를 선택합니다.
- 3 [관리자] 필드에서 독립형 호스트를 선택하고 + 추가를 클릭합니다.
- 4 패브릭에 추가할 독립형 호스트 또는 베어메탈 서버 세부 정보를 입력합니다.

옵션	설명
이름 및 설명	독립형 호스트 또는 베어메탈 서버를 식별하는 이름을 입력합니다. 필요한 경우 호스트 또는 베어메탈 서버에 사용된 운영 체제에 대한 설명을 추가할 수도 있습니다.
IP 주소	호스트 또는 베어메탈 서버 IP 주소를 입력합니다.
운영 체제	드롭다운 메뉴에서 운영 체제를 선택합니다. 호스트 또는 베어메탈 서버에 따라 지원되는 운영 체제 중에서 선택할 수 있습니다. 시스템 요구 사항 의 내용을 참조하십시오. 중요 지원되는 다양한 유형의 Linux에서 Linux 배포를 실행하는 베어메탈 서버와 Linux 배포를 하이퍼바이저 호스트로 사용하는 방식 간의 차이를 알고 있어야 합니다. 예를 들어, Ubuntu Server를 운영 체제로 선택하면 Linux 서버를 실행하는 베어메탈 서버가 설정되지만, Ubuntu KVM을 선택하면 배포된 Linux 하이퍼바이저가 Ubuntu가 됩니다.

옵션	설명
사용자 이름 및 암호	호스트 사용자 이름 및 암호를 입력합니다.
SHA-256 지문	인증을 위한 호스트 지문 값을 입력합니다. 지문 값을 비워 두면 서버에서 제공한 값을 수락할지 묻는 메시지가 나타납니다. NSX-T Data Center에서 호스트를 검색하고 인증하는 데에는 몇 초가 걸립니다.

5 (필수 사항) KVM 호스트 또는 베어메탈 서버의 경우 N-VDS 유형을 선택합니다.

옵션	설명
생성된 NSX	NSX Manager가 N-VDS를 생성합니다. 이 옵션은 기본적으로 선택되어 있습니다.
사전 구성	N-VDS가 이미 구성되어 있습니다.

ESXi 호스트의 경우, N-VDS 유형은 항상 **생성된 NSX**로 설정됩니다.

6 표준 N-VDS 세부 정보를 입력합니다. 단일 호스트에 여러 개의 N-VDS 스위치를 구성할 수 있습니다.

옵션	설명
전송 영역	드롭다운 메뉴에서 이 전송 노드가 속한 전송 영역을 선택합니다.
N-VDS 이름	이 노드가 속하는 전송 영역의 N-VDS 이름과 반드시 동일해야 합니다.
NIOC 프로파일	ESXi 호스트의 경우 드롭다운 메뉴에서 NIOC 프로파일을 선택합니다.
업링크 프로파일	드롭다운 메뉴에서 기존 업링크 프로파일을 선택하거나 사용자 지정 업링크 프로파일을 생성합니다. 기본 업링크 프로파일을 사용할 수도 있습니다.
LLDP 프로파일	기본적으로 NSX-T는 LLDP 인접 네트워크에서 LLDP 패킷만 수신합니다. 하지만 LLDP 인접 네트워크로 LLDP 패킷을 전송하고 인접 네트워크에서 LLDP 패킷을 수신하도록 NSX-T를 설정할 수 있습니다.
IP 할당	DHCP 사용 , IP 풀 사용 또는 정적 IP 목록 사용 을 선택합니다. 정적 IP 목록 사용 을 선택하면 쉽표로 구분된 IP 주소 목록, 게이트웨이 및 서브넷 마스크를 지정해야 합니다.
IP 풀	IP 할당에 대해 IP 풀 사용 을 선택한 경우 IP 풀 이름을 지정합니다.

옵션	설명
물리적 NIC	<p>물리적 NIC를 전송 노드에 추가합니다. 기본 업링크를 사용하거나 드롭다운 메뉴에서 기존 업링크를 할당할 수 있습니다.</p> <p>PNIC 추가를 클릭하여 전송 노드에 대한 추가적인 물리적 NIC를 구성합니다.</p> <p>참고 이 필드에서 추가하는 물리적 NIC의 마이그레이션은 물리적 NIC 전용 마이그레이션, 설치를 위한 네트워크 매핑 및 제거를 위한 네트워크 매핑을 어떻게 구성하는지에 따라 결정됩니다.</p> <ul style="list-style-type: none"> ■ 연결된 VMkernel 매핑 없이 사용된 물리적 NIC(예를 들어 표준 vSwitch 또는 vSphere Distributed Switch에서)를 마이그레이션하려면 물리적 NIC 전용 마이그레이션을 사용하도록 설정했는지 확인합니다. 사용되고 있는 경우 전송 노드 상태가 일부 성공으로 유지되고 패브릭 노드 LCP 연결이 설정되지 않습니다. ■ 연결된 VMkernel 네트워크 매핑과 함께 사용된 물리적 NIC를 마이그레이션하려면 물리적 NIC 전용 마이그레이션을 사용하지 않도록 설정하고 VMkernel 네트워크 매핑을 구성합니다. ■ 사용 가능한 물리적 NIC를 마이그레이션하려면 물리적 NIC 전용 마이그레이션을 사용하도록 설정합니다.
물리적 NIC 전용 마이그레이션	<p>이 필드를 설정하기 전에 다음과 같은 사항을 고려합니다.</p> <ul style="list-style-type: none"> ■ 정의된 물리적 NIC가 사용된 NIC인지 아니면 사용 가능한 NIC인지 파악합니다. ■ 호스트의 VMkernel 인터페이스를 물리적 NIC와 함께 마이그레이션해야 할지 결정합니다. <p>필드 설정:</p> <ul style="list-style-type: none"> ■ VSS 또는 DVS 스위치에서 N-VDS 스위치로 물리적 NIC만 마이그레이션하려면 물리적 NIC 전용 마이그레이션을 사용하도록 설정합니다. ■ 사용된 물리적 NIC 및 연결된 해당 VMkernel 인터페이스 매핑을 마이그레이션하려면 물리적 NIC 전용 마이그레이션을 사용하지 않도록 설정합니다. <p>VMkernel 인터페이스 마이그레이션 매핑이 지정되면 사용 가능한 물리적 NIC가 N-VDS 스위치에 연결됩니다.</p> <p>여러 개의 호스트 스위치가 있는 호스트에서:</p> <ul style="list-style-type: none"> ■ 모든 호스트 스위치가 물리적 NIC만 마이그레이션한다면 한 번으로 작업으로 물리적 NIC를 마이그레이션할 수 있습니다. ■ 일부 호스트 스위치가 VMkernel 인터페이스를 마이그레이션하고 나머지 호스트 스위치가 물리적 NIC만 마이그레이션하는 경우: <ol style="list-style-type: none"> 1 첫 번째 작업에서 물리적 NIC만 마이그레이션합니다. 2 두 번째 작업에서 VMkernel 인터페이스를 마이그레이션합니다. 물리적 NIC 전용 마이그레이션을 사용하지 않도록 설정했는지 확인합니다. <p>물리적 NIC 전용 마이그레이션과 VMkernel 인터페이스 마이그레이션은 여러 호스트에서 동시에 지원되지 않습니다.</p> <p>참고 관리 네트워크 NIC를 마이그레이션하려면 연결된 해당 VMkernel 네트워크 매핑을 구성하고 물리적 NIC 전용 마이그레이션을 사용하지 않도록 설정한 상태로 둡니다. 관리 NIC만 마이그레이션하면 호스트 연결이 끊어집니다.</p> <p>자세한 내용은 N-VDS 스위치로 VMkernel 마이그레이션 항목을 참조하십시오.</p>

옵션	설명
설치를 위한 네트워크 매핑	<p>설치 중에 VMkernel을 N-VDS 스위치에 마이그레이션하려면 VMkernel을 기존의 논리적 스위치에 매핑합니다. NSX Manager가 N-VDS의 매핑된 논리적 스위치에 VMkernel을 마이그레이션합니다.</p> <p>경고 관리 NIC 및 관리 VMkernel 인터페이스가 마이그레이션 전 관리 NIC가 연결되어 있던 동일한 VLAN과 연결된 논리적 스위치로 마이그레이션되었는지 확인하십시오. <code>vmnic<n></code> 및 <code>VMkernel<n></code>이 서로 다른 VLAN으로 마이그레이션되면 호스트에 대한 연결이 끊어집니다.</p> <p>경고 고정된 물리적 NIC의 경우 VMkernel 인터페이스에 대한 물리적 NIC의 호스트 스위치 매핑이 전송 노드 프로파일에 지정된 구성과 일치하는지 확인하십시오. NSX-T Data Center는 검증 절차의 일부로 매핑을 검사합니다. 검증이 통과되면 VMkernel 인터페이스가 N-VDS 스위치로 성공적으로 마이그레이션됩니다. 동시에, NSX-T Data Center는 VMkernel 인터페이스를 N-VDS 스위치로 마이그레이션한 후 호스트의 매핑 구성을 저장하지 않으므로 필수적으로 제거를 위한 네트워크 매핑을 구성해야 합니다. 매핑이 구성되지 않으면 VSS 또는 VDS 스위치로 다시 마이그레이션한 후 서비스(예: vSAN)에 대한 연결이 손실될 수 있습니다.</p> <p>자세한 내용은 N-VDS 스위치로 VMkernel 마이그레이션 항목을 참조하십시오.</p>
제거를 위한 네트워크 매핑	<p>제거 중에 VMkernel의 마이그레이션을 되돌리려면 VMkernel을 VSS 또는 DVS의 포트 그룹에 매핑하여 VMkernel이 다시 마이그레이션되어야 하는 VSS 또는 DVS의 포트 그룹을 NSX Manager가 알 수 있도록 합니다. DVS 스위치의 경우 포트 그룹의 유형이 사용 후 삭제인지 확인합니다.</p> <p>경고 고정된 물리적 NIC의 경우 VMkernel 인터페이스에 대한 물리적 NIC의 전송 노드 프로파일 매핑이 호스트 스위치에 지정된 구성과 일치하는지 확인하십시오. NSX-T Data Center는 VMkernel 인터페이스를 N-VDS 스위치로 마이그레이션한 후 호스트의 매핑 구성을 저장하지 않으므로 필수적으로 제거를 위한 네트워크 매핑을 구성해야 합니다. 매핑이 구성되지 않으면 VSS 또는 VDS 스위치로 다시 마이그레이션한 후 서비스(예: vSAN)에 대한 연결이 손실될 수 있습니다.</p> <p>자세한 내용은 N-VDS 스위치로 VMkernel 마이그레이션 항목을 참조하십시오.</p>

- 7** 고급 데이터 경로 N-VDS 세부 정보를 입력합니다. 단일 호스트에 여러 개의 N-VDS 스위치를 구성할 수 있습니다.

옵션	설명
N-VDS 이름	이 노드가 속하는 전송 영역의 N-VDS 이름과 반드시 동일해야 합니다.
IP 할당	<p>DHCP 사용, IP 풀 사용 또는 정적 IP 목록 사용을 선택합니다.</p> <p>정적 IP 목록 사용을 선택하면 십진법으로 구분된 IP 주소 목록, 게이트웨이 및 서브넷 마스크를 지정해야 합니다.</p>
IP 풀	IP 할당에 대해 IP 풀 사용 을 선택한 경우 IP 풀 이름을 지정합니다.

옵션	설명
물리적 NIC	<p>물리적 NIC를 전송 노드에 추가합니다. 기본 업링크를 사용하거나 드롭다운 메뉴에서 기존 업링크를 할당할 수 있습니다.</p> <p>PNIC 추가를 클릭하여 전송 노드에 대한 추가적인 물리적 NIC를 구성합니다.</p> <p>참고 이 필드에서 추가하는 물리적 NIC의 마이그레이션은 물리적 NIC 전용 마이그레이션, 설치를 위한 네트워크 매핑 및 제거를 위한 네트워크 매핑을 어떻게 구성하는지에 따라 결정됩니다.</p> <ul style="list-style-type: none"> ■ 연결된 VMkernel 매핑 없이 사용된 물리적 NIC(예를 들어 표준 vSwitch 또는 vSphere Distributed Switch에서)를 마이그레이션하려면 물리적 NIC 전용 마이그레이션을 사용하도록 설정했는지 확인합니다. 사용되고 있는 경우 전송 노드 상태가 일부 성공으로 유지되고 패브릭 노드 LCP 연결이 설정되지 않습니다. ■ 연결된 VMkernel 네트워크 매핑과 함께 사용된 물리적 NIC를 마이그레이션하려면 물리적 NIC 전용 마이그레이션을 사용하지 않도록 설정하고 VMkernel 네트워크 매핑을 구성합니다. ■ 사용 가능한 물리적 NIC를 마이그레이션하려면 물리적 NIC 전용 마이그레이션을 사용하도록 설정합니다.
업링크	<p>드롭다운 메뉴에서 업링크 프로파일을 선택합니다.</p>
CPU 구성	<p>[NUMA 노드 인덱스] 드롭다운 메뉴에서 N-VDS 스위치에 할당하려는 NUMA 노드를 선택합니다. 노드에 있는 첫 번째 NUMA 노드는 값 0으로 표시됩니다.</p> <p><code>esxcli hardware memory get</code> 명령을 실행하여 호스트에서 NUMA 노드의 수를 확인할 수 있습니다.</p> <p>참고 N-VDS 스위치에 대해 선호도를 갖는 NUMA 노드의 수를 변경하려는 경우 NUMA 노드 인덱스 값을 업데이트할 수 있습니다.</p> <p>[NUMA 노드별 LCore 수] 드롭다운 메뉴에서 고급 데이터 경로에서 사용되어야 하는 논리적 코어 수를 선택합니다.</p> <p><code>esxcli network ens maxLcores get</code> 명령을 실행하여 NUMA 노드에서 생성할 수 있는 최대 논리적 코어 수를 확인할 수 있습니다.</p> <p>참고 사용 가능한 NUMA 노드와 논리적 코어를 모두 사용한 경우 전송 노드에 추가된 새 스위치를 ENS 트래픽에 사용하도록 설정할 수 없습니다.</p>

8 미리 구성된 N-VDS의 경우 다음 세부 정보를 제공합니다.

옵션	설명
N-VDS 외부 ID	이 노드가 속하는 전송 영역의 N-VDS 이름과 반드시 동일해야 합니다.
VTEP	가상 터널 끝점 이름입니다.

9 호스트 전송 노드 페이지에서 연결 상태를 확인합니다.

호스트 또는 베어메탈 서버를 전송 노드로 추가하면 3-4분 후에 NSX Manager에 대한 연결 상태가 [실행 중]으로 변경됩니다.

참고 검색 루프로 이어지는 구성 해시가 일치하지 않아 호스트 준비가 실패하는 경우 다음 옵션 중 하나를 시도합니다.

- FQDN을 false로 설정하고 호스트에서 nsx-proxy를 다시 시작합니다. 이렇게 하면 호스트와 NSX Manager가 FQDN을 사용하지 않게 됩니다.
- 또는
FQDN 모드를 사용하려는 경우에는 호스트 이름에 대해 FQDN을 사용하여 NSX Manager 장치를 배포하고, 대/소문자 구분 철자가 NSX Manager IP 주소에 대한 정방향 및 역방향 DNS 조회 둘 다와 일치하는지 확인해야 합니다. 이 설정은 모든 NSX Manager 노드에서 일관되어야 합니다.

10 또는 CLI 명령을 사용하여 연결 상태를 확인합니다.

- ◆ ESXi의 경우 `esxcli network ip connection list | grep 1234` 명령을 입력합니다.

```
# esxcli network ip connection list | grep 1234
tcp    0    0 192.168.210.53:20514 192.168.110.34:1234 ESTABLISHED 1000144459 newreno
netcpa
```

- ◆ KVM의 경우 `netstat -anp --tcp | grep 1234` 명령을 입력합니다.

```
user@host:~$ netstat -anp --tcp | grep 1234
tcp    0    0 192.168.210.54:57794 192.168.110.34:1234 ESTABLISHED -
```

11 NSX-T Data Center 모듈이 호스트 또는 베어메탈 서버에 설치되어 있는지 확인합니다.

호스트 또는 베어메탈 서버를 NSX-T Data Center 패브릭에 추가하면 NSX-T Data Center 모듈 모음이 호스트 또는 베어메탈 서버에 설치됩니다.

모듈은 호스트별로 다음과 같이 패키징되어 있습니다.

- RHEL 또는 CentOS의 KVM - RPM.
- Ubuntu의 KVM - DEB.
- ESXi에서 `esxcli software vib list | grep nsx` 명령을 입력합니다.
날짜는 설치를 수행한 날짜입니다.
- RHEL 또는 CentOS에서 `yum list installed` 또는 `rpm -qa` 명령을 입력합니다.
- Ubuntu에서 `dpkg --get-selections` 명령을 입력합니다.

12 (선택 사항) 하이퍼바이저가 500개 이상인 경우 특정 프로세스의 폴링 간격을 변경합니다.

하이퍼바이저가 500개를 초과하면 NSX Manager에서 높은 CPU 사용량 및 성능 문제가 발생할 수 있습니다.

- a NSX-T Data Center CLI 명령 `copy file` 또는 API POST `/api/v1/node/file-store/<file-name>?action=copy_to_remote_file`을 사용하여 `aggsvc_change_intervals.py` 스크립트를 호스트로 복사합니다.
- b NSX-T Data Center 파일 저장소에 있는 스크립트를 실행합니다.

```
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -i 900
```

- c (선택 사항) 폴링 간격을 다시 기본값으로 변경합니다.

```
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -r
```

결과

참고 NSX-T Data Center에서 생성한 N-VDS의 경우 전송 노드를 생성한 후 터널 끝점에 대한 IP 할당과 같은 구성을 변경하려면 호스트의 CLI가 아닌 NSX Manager GUI를 통해 변경해야 합니다.

다음에 수행할 작업

네트워크 인터페이스를 vSphere 표준 스위치에서 N-VDS로 마이그레이션합니다. [N-VDS 스위치로 VMkernel 마이그레이션](#)의 내용을 참조하십시오.

관리 호스트 전송 노드 구성

vCenter Server가 있는 경우 모든 NSX-T Data Center 호스트에서 전송 노드를 수동으로 구성하지 않고 설치 및 생성을 자동화할 수 있습니다.

전송 노드가 이미 구성된 경우 해당 노드에는 자동화된 전송 노드 생성을 적용할 수 없습니다.

사전 요구 사항

- vCenter Server에 있는 모든 호스트의 전원이 켜져 있는지 확인합니다.
- 시스템 요구 사항이 충족되었는지 확인합니다. [시스템 요구 사항](#)의 내용을 참조하십시오.
- 전송 영역을 사용할 수 있는지 확인합니다. [전송 영역 생성](#)의 내용을 참조하십시오.
- 전송 노드 프로파일이 구성되어 있는지 확인합니다. [전송 노드 프로파일 추가](#)의 내용을 참조하십시오.
- vSphere 잠금 모드에 대한 예외 목록에 만료된 사용자 계정이 포함되어 있는 경우 vSphere의 NSX-T Data Center 설치가 실패합니다. 설치를 시작하기 전에 만료된 모든 사용자 계정을 삭제했는지 확인합니다. 잠금 모드에서 액세스 권한이 있는 계정에 대한 자세한 내용은 "vSphere 보안 가이드"의 "잠금 모드에서 액세스 권한이 있는 계정 지정"을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 패브릭 > 노드 > 호스트 전송 노드**를 선택합니다.
- 3 [관리자] 드롭다운 메뉴에서 기존 vCenter Server를 선택합니다.
이 페이지는 선택한 vCenter Server에서 사용 가능한 vSphere 클러스터 및/또는 ESXi 호스트를 표시합니다. ESXi 호스트를 보기 위해 클러스터를 확장해야 할 수도 있습니다.
- 4 목록에서 단일 호스트를 선택하고 **NSX 구성**을 클릭합니다.
[NSX 구성] 대화상자가 열립니다.
 - a [호스트 세부 정보] 패널에서 호스트 이름을 확인합니다. 필요한 경우 설명을 추가할 수 있습니다.
 - b **다음**을 클릭하여 **NSX 구성** 패널로 이동합니다.
 - c 사용 가능한 전송 영역을 선택하고 **>** 버튼을 클릭하여 전송 노드 프로파일에 전송 영역을 포함시킵니다.
- 5 [호스트 세부 정보] 패널에서 호스트 이름을 확인한 후 **다음**을 클릭합니다.
필요한 경우 설명을 추가할 수 있습니다.
- 6 **NSX 구성** 패널에서 원하는 전송 영역을 선택합니다.
둘 이상의 전송 영역을 선택할 수 있습니다.
- 7 **N-VDS** 탭을 클릭하고 스위치 세부 정보를 입력합니다.

옵션	설명
N-VDS 이름	전송 노드가 전송 영역에 연결되었다면 N-VDS에 대해 입력한 이름이 전송 영역에 지정된 N-VDS 이름과 동일한지 확인합니다. 전송 노드는 전송 영역에 연결하지 않고도 생성할 수 있습니다.
연결된 전송 영역	연결된 호스트 스위치에서 인식된 전송 영역을 보여줍니다. 전송 노드 프로파일에 있는 N-VDS에서 인식되지 않은 전송 영역은 추가할 수 없습니다.
NIOC 프로파일	드롭다운 메뉴에서 NIOC 프로파일을 선택합니다. 트래픽 리소스의 프로파일에 지정된 대역폭 할당이 적용됩니다.
업링크 프로파일	드롭다운 메뉴에서 기존 업링크 프로파일을 선택하거나 사용자 지정 업링크 프로파일을 생성합니다. 기본 업링크 프로파일을 사용할 수도 있습니다.
LLDP 프로파일	기본적으로 NSX-T는 LLDP 인접 네트워크에서 LLDP 패킷만 수신합니다. 하지만 LLDP 인접 네트워크로 LLDP 패킷을 전송하고 인접 네트워크에서 LLDP 패킷을 수신하도록 NSX-T를 설정할 수 있습니다.

옵션	설명
IP 할당	<p>DHCP 사용, IP 풀 사용 또는 정적 IP 목록 사용을 선택하여 IP 주소를 전송 노드의 VTEP(가상 터널 끝점)에 할당합니다.</p> <p>정적 IP 목록 사용을 선택하면 씬프로 구분된 IP 주소 목록, 게이트웨이 및 서브넷 마스크를 지정해야 합니다. 전송 노드의 모든 VTEP는 동일한 서브넷에 있어야 합니다. 그렇지 않으면 양방향 흐름(BFD) 세션이 설정되지 않습니다.</p>
IP 풀	IP 할당에 대해 IP 풀 사용 을 선택한 경우 IP 풀 이름을 지정합니다.
물리적 NIC	<p>물리적 NIC를 전송 노드에 추가합니다. 기본 업링크를 사용하거나 드롭다운 메뉴에서 기존 업링크를 할당할 수 있습니다.</p> <p>PNIC 추가를 클릭하여 전송 노드에 대한 추가적인 물리적 NIC를 구성합니다.</p> <p>참고 이 필드에서 추가하는 물리적 NIC의 마이그레이션은 물리적 NIC 전용 마이그레이션, 설치를 위한 네트워크 매핑 및 제거를 위한 네트워크 매핑을 어떻게 구성하는지에 따라 결정됩니다.</p> <ul style="list-style-type: none"> ■ 연결된 VMkernel 매핑 없이 사용된 물리적 NIC(예를 들어 표준 vSwitch 또는 vSphere Distributed Switch에서)를 마이그레이션하려면 물리적 NIC 전용 마이그레이션을 사용하도록 설정했는지 확인합니다. 사용되고 있는 경우 전송 노드 상태가 일부 성공으로 유지되고 패브릭 노드 LCP 연결이 설정되지 않습니다. ■ 연결된 VMkernel 네트워크 매핑과 함께 사용된 물리적 NIC를 마이그레이션하려면 물리적 NIC 전용 마이그레이션을 사용하지 않도록 설정하고 VMkernel 네트워크 매핑을 구성합니다. ■ 사용 가능한 물리적 NIC를 마이그레이션하려면 물리적 NIC 전용 마이그레이션을 사용하도록 설정합니다.

옵션	설명
물리적 NIC 전용 마이그레이션	<p>이 필드를 설정하기 전에 다음과 같은 사항을 고려합니다.</p> <ul style="list-style-type: none"> ■ 정의된 물리적 NIC가 사용된 NIC인지 아니면 사용 가능한 NIC인지 파악합니다. ■ 호스트의 VMkernel 인터페이스를 물리적 NIC와 함께 마이그레이션해야 할지 결정합니다. <p>필드 설정:</p> <ul style="list-style-type: none"> ■ VSS 또는 DVS 스위치에서 N-VDS 스위치로 물리적 NIC만 마이그레이션하려면 물리적 NIC 전용 마이그레이션을 사용하도록 설정합니다. ■ 사용된 물리적 NIC 및 연결된 해당 VMkernel 인터페이스 매핑을 마이그레이션하려면 물리적 NIC 전용 마이그레이션을 사용하지 않도록 설정합니다. <p>VMkernel 인터페이스 마이그레이션 매핑이 지정되면 사용 가능한 물리적 NIC가 N-VDS 스위치에 연결됩니다.</p> <p>여러 개의 호스트 스위치가 있는 호스트에서:</p> <ul style="list-style-type: none"> ■ 모든 호스트 스위치가 물리적 NIC만 마이그레이션한다면 한 번으로 작업으로 물리적 NIC를 마이그레이션할 수 있습니다. ■ 일부 호스트 스위치가 VMkernel 인터페이스를 마이그레이션하고 나머지 호스트 스위치가 물리적 NIC만 마이그레이션하는 경우: <ol style="list-style-type: none"> 1 첫 번째 작업에서 물리적 NIC만 마이그레이션합니다. 2 두 번째 작업에서 VMkernel 인터페이스를 마이그레이션합니다. 물리적 NIC 전용 마이그레이션을 사용하지 않도록 설정했는지 확인합니다. <p>물리적 NIC 전용 마이그레이션과 VMkernel 인터페이스 마이그레이션은 여러 호스트에서 동시에 지원되지 않습니다.</p> <p>참고 관리 네트워크 NIC를 마이그레이션하려면 연결된 해당 VMkernel 네트워크 매핑을 구성하고 물리적 NIC 전용 마이그레이션을 사용하지 않도록 설정한 상태로 둡니다. 관리 NIC만 마이그레이션하면 호스트 연결이 끊어집니다.</p> <p>자세한 내용은 N-VDS 스위치로 VMkernel 마이그레이션 항목을 참조하십시오.</p>

옵션	설명
설치를 위한 네트워크 매핑	<p>설치 중에 VMkernel을 N-VDS 스위치에 마이그레이션하려면 VMkernel을 기존의 논리적 스위치에 매핑합니다. NSX Manager가 N-VDS의 매핑된 논리적 스위치에 VMkernel을 마이그레이션합니다.</p> <p>경고 관리 NIC 및 관리 VMkernel 인터페이스가 마이그레이션 전 관리 NIC가 연결되어 있던 동일한 VLAN과 연결된 논리적 스위치로 마이그레이션되었는지 확인하십시오. vmnic<n> 및 VMkernel<n>이 서로 다른 VLAN으로 마이그레이션되면 호스트에 대한 연결이 끊어집니다.</p> <p>경고 고정된 물리적 NIC의 경우 VMkernel 인터페이스에 대한 물리적 NIC의 호스트 스위치 매핑이 전송 노드 프로파일에 지정된 구성과 일치하는지 확인하십시오. NSX-T Data Center는 검증 절차의 일부로 매핑을 확인합니다. 검증이 통과되면 N-VDS 스위치로 VMkernel 인터페이스의 마이그레이션이 성공합니다. NSX-T Data Center는 VMkernel 인터페이스를 N-VDS 스위치로 마이그레이션한 후 호스트의 매핑 구성을 저장하지 않으므로 제거를 위한 네트워크 매핑도 구성해야 합니다. 매핑이 구성되지 않으면 VSS 또는 VDS 스위치로 다시 마이그레이션한 후 서비스(예: vSAN)에 대한 연결이 손실될 수 있습니다.</p> <p>자세한 내용은 N-VDS 스위치로 VMkernel 마이그레이션 항목을 참조하십시오.</p>
제거를 위한 네트워크 매핑	<p>제거 중에 VMkernel의 마이그레이션을 되돌리려면 VMkernel을 VSS 또는 DVS의 포트 그룹에 매핑하여 VMkernel이 다시 마이그레이션되어야 하는 VSS 또는 DVS의 포트 그룹을 NSX Manager가 알 수 있도록 합니다. DVS 스위치의 경우 포트 그룹의 유형이 사용 후 삭제인지 확인합니다.</p> <p>경고 고정된 물리적 NIC의 경우 VMkernel 인터페이스에 대한 물리적 NIC의 전송 노드 프로파일 매핑이 호스트 스위치에 지정된 구성과 일치하는지 확인하십시오. NSX-T Data Center는 VMkernel 인터페이스를 N-VDS 스위치로 마이그레이션한 후 호스트의 매핑 구성을 저장하지 않으므로 필수적으로 제거를 위한 네트워크 매핑을 구성해야 합니다. 매핑이 구성되지 않으면 VSS 또는 VDS 스위치로 다시 마이그레이션한 후 서비스(예: vSAN)에 대한 연결이 손실될 수 있습니다.</p> <p>자세한 내용은 N-VDS 스위치로 VMkernel 마이그레이션 항목을 참조하십시오.</p>

8 여러 전송 영역을 선택한 경우에는 **+ N-VDS 추가**를 다시 클릭하여 다른 전송 영역에 대해 스위치를 구성합니다.

9 **완료**를 클릭하여 구성을 완료합니다.

10 (선택 사항) ESXi 연결 상태를 확인합니다.

```
# esxcli network ip connection list | grep 1235
tcp 0 0 192.168.210.53:20514 192.168.110.34:1234 ESTABLISHED 1000144459 newreno netcpa
```

11 [호스트 전송 노드] 페이지에서 클러스터에 있는 호스트의 NSX Manager 연결 상태가 [실행 중]이고 NSX-T Data Center 구성 상태가 [성공]인지 확인합니다.

전송 영역이 클러스터의 호스트에 적용되어 있는 것을 볼 수도 있습니다.

12 (선택 사항) 전송 영역의 호스트에서 NSX-T Data Center 설치 및 전송 노드를 제거합니다.

a 하나 이상의 호스트를 선택하고 **작업 > NSX 제거**를 클릭합니다.

제거에는 최대 3분이 소요됩니다. NSX-T Data Center를 제거하면 호스트의 전송 노드 구성이 제거되고 호스트가 전송 영역 및 N-VDS 스위치에서 분리됩니다. 전송 노드 프로파일이 클러스터에 다시 적용될 때까지 vCenter Server 클러스터에 추가된 모든 새 호스트가 자동으로 구성되지 않습니다.

13 (선택 사항) 전송 영역에서 전송 노드를 제거합니다.

- a 단일 전송 노드를 선택하고 **작업 > 전송 영역에서 제거**를 클릭합니다.

다음에 수행할 작업

논리적 스위치를 생성하고 논리적 포트를 할당합니다. "NSX-T Data Center 관리 가이드"에서 고급 스위칭 섹션을 참조하십시오.

링크 집계로 ESXi 호스트 전송 노드 구성

이 절차에서는 링크 집계 그룹이 구성된 업링크 프로파일을 생성하는 방법과 이 업링크 프로파일을 사용하여 ESXi 호스트 전송 노드를 구성하는 방법을 설명합니다.

사전 요구 사항

- 업링크 프로파일을 생성하는 단계를 숙지합니다. [업링크 프로파일 생성](#)의 내용을 참조하십시오.
- 호스트 전송 노드를 생성하는 단계를 숙지합니다. [독립형 호스트 또는 베어메탈 서비스 전송 노드 생성](#)의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 패브릭 > 프로파일 > 업링크 프로파일 > 추가**를 선택합니다.
- 3 이름과 설명(선택 사항)을 입력합니다.
예를 들어 **uplink-profile1**을 이름으로 입력합니다.
- 4 **LAG**에서 **추가**를 클릭하여 링크 집계 그룹을 추가합니다.
예를 들어 업링크가 2개 있는 **lag1**이라는 LAG를 추가합니다.
- 5 **팀 구성**에서 **기본 팀 구성**을 선택합니다.
- 6 **액티브 업링크** 필드에 4단계에서 추가한 LAG의 이름을 입력합니다. 이 예에서 해당 이름은 **lag1**입니다.
- 7 **전송 VLAN** 및 **MTU** 값을 입력합니다.
- 8 대화 상자의 맨 아래에서 **추가**를 클릭합니다.
- 9 **팀 구성**에서 **추가**를 클릭하여 링크 집계에 대한 항목을 추가합니다.
- 10 **패브릭 > 노드 > 호스트 전송 노드 > 추가**를 선택합니다.
- 11 **호스트 세부 정보** 탭에서 호스트의 IP 주소, OS 이름, 관리 자격 증명 및 SHA 256 지문을 입력합니다.

12 N-VDS 탭에서 3단계에서 생성한 **uplink-profile1**이라는 업링크 프로파일을 선택합니다.

13 물리적 NIC 필드에서 물리적 NIC 및 업링크 드롭다운 목록에 새 NIC 및 업링크 프로파일이 반영됩니다. 특히, 4단계에서 생성한 LAG인 **lag1**에 해당하는 업링크 **lag1-0**과 **lag1-1**이 표시됩니다. **lag1-0**에 대한 물리적 NIC 및 **lag1-1**에 대한 물리적 NIC를 선택합니다.

14 다른 필드에 대한 정보를 입력합니다.

전송 노드 상태 확인

전송 노드 생성 프로세스가 올바르게 작동하는지 확인합니다.

호스트 전송 노드를 생성하면 N-VDS가 호스트에 설치됩니다.

절차

- 1 NSX-T Data Center에 로그인합니다.
- 2 [전송 노드] 페이지로 이동하고 N-VDS 상태를 확인합니다.
- 3 또는 `esxcli network ip interface list` 명령을 사용하여 ESXi에서 N-VDS를 확인합니다.

ESXi에서 명령 출력에는 전송 영역 및 전송 노드를 구성할 때 사용한 이름과 일치하는 VDS 이름을 갖는 vmk 인터페이스(예: vmk10)가 포함되어야 합니다.

```
# esxcli network ip interface list
...

vmk10
  Name: vmk10
  MAC Address: 00:50:56:64:63:4c
  Enabled: true
  Portset: DvsPortset-1
  Portgroup: N/A
  Netstack Instance: vxlan
  VDS Name: overlay-hostswitch
  VDS UUID: 18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2
  VDS Port: 10
  VDS Connection: 10
  Opaque Network ID: N/A
  Opaque Network Type: N/A
  External ID: N/A
  MTU: 1600
  TSO MSS: 65535
  Port ID: 67108895

...
```

vSphere Client를 사용하는 경우 UI에서 호스트 **구성 > 네트워크 어댑터**를 선택하여 설치된 N-VDS를 확인할 수 있습니다.

N-VDS 설치를 확인하는 KVM 명령은 `ovs-vsctl show`입니다. KVM에서 N-VDS 이름은 `nsx-switch.0`입니다. 이 이름은 전송 노드 구성의 이름과 일치하지 않습니다. 이는 설계상 의도된 동작입니다.

```
# ovs-vsctl show
...
Bridge "nsx-switch.0"
  Port "nsx-uplink.0"
    Interface "em2"
  Port "nsx-vtep0.0"
    tag: 0
    Interface "nsx-vtep0.0"
      type: internal
  Port "nsx-switch.0"
    Interface "nsx-switch.0"
      type: internal
ovs_version: "2.4.1.3340774"
```

4 전송 노드의 할당된 터널 끝점 주소를 확인합니다.

`vmk10` 인터페이스는 여기에 표시된 것처럼 NSX-T Data Center IP 풀 또는 DHCP에서 IP 주소를 수신합니다.

```
# esxcli network ip interface ipv4 get
Name    IPv4 Address    IPv4 Netmask    IPv4 Broadcast    Address Type    DHCP DNS
-----
vmk0    192.168.210.53  255.255.255.0   192.168.210.255   STATIC          false
vmk1    10.20.20.53    255.255.255.0   10.20.20.255     STATIC          false
vmk10  192.168.250.3  255.255.255.0   192.168.250.255   STATIC          false
```

KVM에서 `ifconfig` 명령을 사용하여 터널 끝점 및 IP 할당을 확인할 수 있습니다.

```
# ifconfig
...
nsx-vtep0.0 Link encap:Ethernet HWaddr ba:30:ae:aa:26:53
  inet addr:192.168.250.4 Bcast:192.168.250.255 Mask:255.255.255.0
  ...
```

5 API에서 전송 노드 상태 정보를 확인합니다.

GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state` API 호출을 사용합니다. 예:

```
{
  "state": "success",
  "host_switch_states": [
```

```
{
  "endpoints": [
    {
      "default_gateway": "192.168.250.1",
      "device_name": "vmk10",
      "ip": "192.168.250.104",
      "subnet_mask": "255.255.255.0",
      "label": 69633
    }
  ],
  "transport_zone_ids": [
    "efd7f38f-c5da-437d-af03-ac598f82a9ec"
  ],
  "host_switch_name": "overlay-hostswitch",
  "host_switch_id": "18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2"
},
"transport_node_id": "2d030569-5769-4a13-8918-0c309c63fdb9"
}
```

ESXi VMkernel 및 물리적 어댑터 마이그레이션

호스트를 전송 노드로 준비한 후에는 VMkernel 어댑터 및 물리적 어댑터의 현재 마이그레이션 구성을 변경할 수 있습니다.

사전 요구 사항

- 호스트에 하나 이상의 사용 가능한 물리적 어댑터가 있는지 확인합니다.
- VMkernel 어댑터 및 포트 그룹이 호스트에 있는지 확인합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 시스템 > 패브릭 > 호스트 전송 노드로 이동합니다.
- 3 전송 노드를 선택하고 작업 -> **ESX VMkernel 및 물리적 어댑터 마이그레이션**을 클릭합니다.

4 [ESX VMkernel 및 물리적 어댑터 마이그레이션]에서 다음 세부 정보를 입력합니다.

필드	설명
방향	선택: <ul style="list-style-type: none"> ■ 논리적 스위치로 마이그레이션: NSX-T Data Center에서 VMkernel 어댑터를 VSS 또는 VDS 스위치에서 N-VDS 스위치로 마이그레이션합니다. ■ 포트 그룹으로 마이그레이션: VMkernel 어댑터를 N-VDS 스위치에서 VSS 또는 VDS 스위치로 마이그레이션합니다.
스위치 선택	VMkernel 어댑터 및 물리적 어댑터를 마이그레이션할 스위치를 선택합니다. 사용 가능한 스위치 중에서 선택할 수 있습니다.
마이그레이션할 VMkernel 어댑터 선택	추가 를 클릭하여 VMkernel 어댑터 이름을 입력하고 마이그레이션할 위치에 따라 논리적 스위치 또는 포트 그룹으로 대상을 선택합니다.
N-VDS에서 물리적 어댑터 편집	추가 를 클릭하여 물리적 어댑터 이름을 입력하고 호스트 스위치의 업링크에 매핑합니다.

5 **저장**을 클릭하여 VMkernel 어댑터 및 물리적 어댑터의 마이그레이션을 시작합니다.

결과

업데이트된 VMkernel 어댑터 및 물리적 어댑터가 N-VDS 스위치로 마이그레이션되거나 ESXi 호스트의 VSS 또는 VDS 스위치로 반대로 마이그레이션됩니다.

NSX 유지 보수 모드

작동하지 않는 전송 노드로의 VM vMotion을 방지하려면 해당 전송 NSX 노드를 유지 보수 모드로 전환합니다.

전송 노드를 NSX 유지 보수 모드로 전환하려면 노드를 선택하고 [작업] → [NSX 유지 보수 모드]를 클릭합니다.

호스트를 NSX 유지 보수 모드로 전환하면 전송 노드가 네트워킹에 참여할 수 없습니다. 또한 N-VDS 또는 vSphere Distributed Switch가 호스트 스위치로 지정된 다른 전송 노드에서 실행되는 VM은 이 전송 노드로 vMotion할 수 없습니다. 또한 논리적 네트워크는 ESXi 또는 KVM 호스트에서 구성할 수 없습니다.

전송 노드를 NSX 유지 보수 모드로 전환하는 시나리오:

- 전송 노드가 작동하지 않습니다.
- 호스트에 NSX-T와 관련되지 않은 하드웨어 또는 소프트웨어 문제가 있지만 NSX-T에 노드와 해당 구성을 유지하려는 경우 호스트를 NSX 유지 보수 모드로 전환합니다.
- 전송 노드는 해당 전송 노드에 대한 업그레이드가 실패할 경우 자동으로 NSX 유지 보수 모드로 전환됩니다.

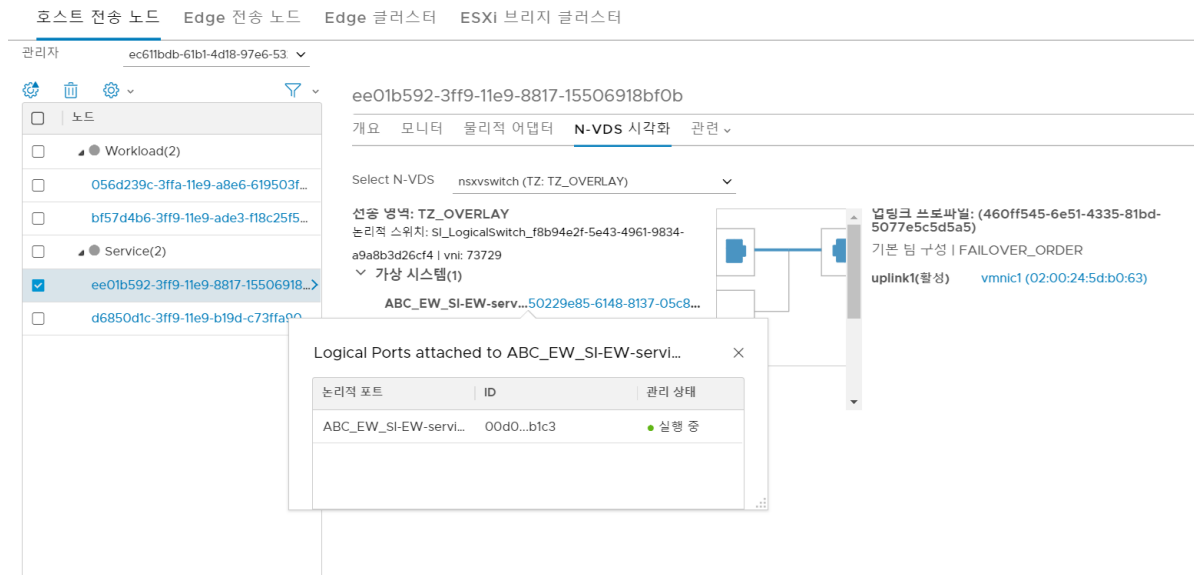
NSX 유지 보수 모드로 전환되는 전송 노드는 업그레이드되지 않습니다.

N-VDS의 시각적 표현

개별 호스트 수준에서 N-VDS의 세분화된 보기를 확인할 수 있습니다. NSX-T Data Center는 N-VDS의 업링크와 전송 영역에 연결된 VM 간 연결 상태의 시각적 표현을 제공합니다. 시각적으로 표현되는 개체에는 VM에 대한 연결을 제공하는 팀 구성 정책 - 업링크 및 물리적 NIC가 포함됩니다. 시각적으로 표현되는 다른 개체 집합에는 VM, 연결된 논리적 포트 및 스위치, VM의 상태가 있습니다. 시각적 표현을 통해 N-VDS를 더 쉽게 관리할 수 있습니다.

참고 ESXi 호스트만 N-VDS 개체의 시각화를 지원합니다.

그림 10-3. N-VDS 시각화



절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 시스템 > 패브릭 > 노드 > 호스트 전송 노드를 선택합니다.
- 3 [관리자] 필드에서 독립형 호스트 또는 계산 관리자를 선택합니다.
- 4 호스트를 선택합니다.
- 5 N-VDS 시각화 탭을 클릭합니다.
- 6 N-VDS를 선택합니다.

NSX-T에서 VM에 연결된 업링크 프로파일, VM에 연결된 논리적 포트, 전송 영역에 연결된 논리적 스위치를 시각적으로 표현합니다.

- 7 VM에 연결된 업링크 프로파일과 VM이 연결되어 있는 논리적 포트를 보려면 VM을 선택합니다.

NSX-T에서 VM과 업링크 프로파일 간 연결을 시각적으로 표현합니다.

- 8 업링크 프로파일에 연결된 VM을 보려면 업링크 프로파일을 선택합니다.

9 VM에 연결된 논리적 포트를 보려면 논리적 스위치를 확장하고 VM을 클릭합니다.

별도의 대화 상자에 논리적 포트 세부 정보가 표시됩니다.

참고 논리적 포트의 관리 상태가 대화 상자에 표시됩니다. 작업 상태가 [종료]인 경우에는 대화 상자에 표시되지 않습니다.

상태 점검 VLAN ID 범위 및 MTU 설정

상태 점검 API를 실행하여 지정한 VLAN ID 범위와 물리적 스위치의 해당 설정을 사용하는 전송 노드의 MTU 설정 간의 호환성을 확인합니다.

VLAN 또는 MTU 구성 불일치는 연결이 중단될 수 있는 일반적인 구성 오류입니다.

참고

- 상태 점검 결과는 가능한 네트워크 구성 오류를 나타낼 뿐입니다. 예를 들어, 다른 L2 도메인의 호스트에서 상태 점검을 실행하면 트렁킹되지 않은 VLAN ID가 발생합니다. 상태 점검 도구가 올바른 결과를 제공하려면 호스트가 동일한 L2 도메인에 있어야 하므로 이 결과를 구성 오류로 간주할 수 없습니다.
- 한 번에 50개의 상태 점검 작업만 진행 중일 수 있습니다.
- 한 상태 점검이 완료되면 NSX-T Data Center는 해당 결과를 24시간 동안만 시스템에 보존합니다.

상태 점검 작업에서 NSX-T Data Center opsAgent는 전송 노드의 프로브 패킷을 다른 노드로 보내 지정한 VLAN ID 범위와 물리적 스위치에서 해당 설정을 갖는 전송 노드의 MTU 값이 호환되는지 확인합니다.

확인할 VLAN ID 범위 수가 증가할수록 대기 시간이 길어집니다.

VLAN의 수	대기 시간(초)
[3073, 4095]	150
[1025, 3072]	120
[513, 1024]	80
[128, 512]	60
[64, 127]	30
[1, 63]	20

사전 요구 사항

- VLAN 및 MTU 점검이 작동하려면 N-VDS에 2개 이상의 업링크가 구성되어야 합니다.
- 동일한 L2 도메인의 전송 노드.
- v6.7U2 이상을 실행하는 ESX 호스트에서 상태 점검이 지원됩니다.

절차

1 수동 상태 점검을 생성합니다.

POST https://<NSXManager_IP>/api/v1/manual-health-checks

Example Request:

POST https://<nsx-mgr>/api/v1/manual-health-checks

```
{
  "resource_type": "ManualHealthCheck",
  "display_name": "Manual HealthCheck 002",
  "transport_zone_id": "7754341c-8f3c-443f-9c1a-2d635d5b0d1c",
  "vlangs": {
    "vlan_ranges": [{
      "start": 0,
      "end": 6
    },]
  },
}
```

Example Response:

```
{
  "operation_status": "FINISHED",
  "transport_zone_id": "7754341c-8f3c-443f-9c1a-2d635d5b0d1c",
  "vlangs": {
    "vlan_ranges": [
      {
        "start": 0,
        "end": 6
      }
    ]
  },
  "result": {
    "vlan_mtu_status": "UNTRUNKED",
    "results_per_transport_node": [
      {
        "transport_node_id": "dfcabffa-8839-11e9-b30e-6f45344d8a04",
        "result_on_host_switch": {
          "host_switch_name": "nsxvswitch",
          "results_per_uplink": [
            {
              "uplink_name": "uplink1",
              "vlan_and_mtu_allowed": [
                {
                  "start": 0,
                  "end": 0
                }
              ],
              "mtu_disallowed": [],
              "vlan_disallowed": [
                {
                  "start": 1,
                  "end": 6
                }
              ]
            }
          ]
        }
      }
    ]
  }
}
```

```

    ]
  },
  {
    "transport_node_id": "a300ea62-8839-11e9-a94e-31732bb71949",
    "result_on_host_switch": {
      "host_switch_name": "nsxvswitch",
      "results_per_uplink": [
        {
          "uplink_name": "uplink1",
          "vlan_and_mtu_allowed": [
            {
              "start": 0,
              "end": 0
            }
          ],
          "mtu_disallowed": [],
          "vlan_disallowed": [
            {
              "start": 1,
              "end": 6
            }
          ]
        }
      ]
    }
  ]
},
{
  "resource_type": "ManualHealthCheck",
  "id": "8a56ed9e-a31b-479e-987b-2dbfbde07c38",
  "display_name": "mc1",
  "_create_user": "admin",
  "_create_time": 1560149933059,
  "_last_modified_user": "system",
  "_last_modified_time": 1560149971220,
  "_system_owned": false,
  "_protection": "NOT_PROTECTED",
  "_revision": 0
}
]

```

ID가 8a56ed9e-a31b-479e-987b-2dbfbde07c38인 새 상태 점검 개체가 생성되었습니다.

- 2 시작된 모든 수동 상태 점검 작업 목록을 가져오려면 해당 API 호출을 수행합니다.

GET https://<NSXManager_IP>/api/v1/manual-health-checks

- 3 수동 상태 점검을 삭제하려면 해당 API 호출을 수행합니다.

DELETE https://<NSXManager_IP>/api/v1/manual-health-checks/<Health-check-ID>

- 4 단일 상태 점검을 수동으로 시작하려면 해당 API 호출을 수행합니다.

GET https://<NSXManager_IP>/api/v1/manual-health-checks/< Health-check-ID>

결과

API 응답 섹션에는 상태 점검 결과가 포함됩니다. NSX Ops 에이전트는 대상 전송 노드의 승인 패킷을 대기하여 물리적 스위치에서 지원되는 VLAN ID 범위를 검색합니다.

- 트렁킹되지 않음: 물리적 스위치와 호환되지 않는 VLAN ID 범위를 나열합니다. 물리적 스위치와 호환되는 VLAN ID 범위도 나열됩니다.
- 트렁킹: 물리적 스위치와 호환되는 VLAN ID 범위를 나열합니다.
- 알 수 없음: 인프라 문제 또는 지원되지 않는 플랫폼 유형(예: KVM 및 Edge) 때문에 일부 또는 모든 업링크에 대해 유효한 결과가 없습니다.

API 응답 섹션의 매개 변수:

- `vlan_and_mtu_allowed`: 호환되는 VLAN ID 범위를 나열합니다.
- `mtu_disallowed`: MTU 값이 물리적 스위치와 호환되지 않는 VLAN ID 범위를 나열합니다.
- `vlan_disallowed`: 물리적 스위치와 호환되지 않는 VLAN ID 범위를 나열합니다.

다음에 수행할 작업

- 오버레이 기반 전송 영역에서 N-VDS의 업링크 프로파일에 있는 VLAN ID 및 MTU 구성을 둘 다 업데이트합니다. 마찬가지로 물리적 스위치에서 VLAN 또는 MTU를 업데이트합니다.
- VLAN 기반 전송 영역에서 업링크 프로파일의 MTU 구성을 업데이트합니다. 또한 해당 전송 영역의 논리적 스위치에서 VLAN 구성을 업데이트합니다. 마찬가지로 물리적 스위치의 VLAN 또는 MTU를 업데이트합니다.

양방향 전달 감지 상태 보기

전송 노드 간에 BFD 상태를 봅니다. 각 전송 노드는 노드와 관련된 다른 세부 정보 중에서 BFD 상태를 표시하는 터널 상태를 통해 다른 원격 전송 노드와의 연결 상태를 감지합니다.

호스트 전송 노드(독립 실행형 및 vCenter에 등록된 호스트)와 Edge 노드 모두 터널 상태를 표시합니다. BFD 패킷은 GENEVE 및 STT 캡슐화를 둘 다 지원합니다. GENEVE는 기본 캡슐화입니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 패브릭 > 노드 > 호스트 전송 노드**로 이동합니다.
- 3 터널 열에서 표시되는 터널 번호를 클릭합니다.

[모니터] 페이지에는 터널, BFD 진단 코드, 원격 노드 UUID, BFD 패킷의 캡슐화 및 터널 이름 상태가 표시됩니다.

터널 BFD 진단 코드는 세션 상태의 변경 이유를 나타냅니다.

코드	설명
0	진단 없음
1	제어 감지 시간 만료
2	에코 기능 실패
3	인접 항목에서 세션 종료 표시
4	전달부 재설정
5	경로 종료
6	병합된 경로 종료
7	관리 목적으로 종료
8	역방향 병합된 경로 종료

결과

BFD 상태가 종료인 경우 진단 코드를 사용하여 전송 노드 간에 연결을 설정합니다.

NSX-T Data Center 커널 모듈의 수동 설치

NSX-T Data Center 패브릭 > 노드 > 호스트 > 추가 UI 또는 `POST /api/v1/fabric/nodes` API를 사용하는 대신, 하이퍼바이저 명령줄에서 NSX-T Data Center 커널 모듈을 수동으로 설치할 수 있습니다.

참고 베어메탈 서버에는 NSX-T Data Center 커널 모듈을 수동으로 설치할 수 없습니다.

ESXi 하이퍼바이저에 수동으로 NSX-T Data Center 커널 모듈 설치

호스트가 NSX-T Data Center에 참여하도록 준비하려면 ESXi 호스트에 NSX-T Data Center 커널 모듈을 설치해야 합니다. 이렇게 하면 NSX-T Data Center 제어부 및 관리부 패브릭을 구축할 수 있습니다. VIB 파일로 패키징된 NSX-T Data Center 커널 모듈은 하이퍼바이저 커널 내에서 실행되어 분산 라우팅, 분산 방화벽 및 브리징 기능과 같은 서비스를 제공합니다.

NSX-T Data Center VIB를 수동으로 다운로드한 후 이를 호스트 이미지의 일부로 만들 수 있습니다. 다운로드 경로는 NSX-T Data Center의 각 릴리스에 따라 달라질 수 있습니다. 그러므로 항상 NSX-T Data Center 다운로드 페이지를 확인하여 적합한 VIB를 가져오십시오.

절차

- 1 루트 권한 또는 관리자 권한이 있는 사용자로 호스트에 로그인합니다.
- 2 `/tmp` 디렉토리로 이동합니다.

```
[root@host:~]: cd /tmp
```

- 3 `nsx-lcp` 파일을 다운로드한 후 `/tmp` 디렉토리로 복사합니다.

4 설치 명령을 실행합니다.

```
[root@host:/tmp]: esxcli software vib install -d /tmp/nsx-lcp-<release>.zip
Installation Result
  Message: Operation finished successfully.
  Reboot Required: false
  VIBs Installed: VMware_bootbank_nsx-aggsservice-<release>, VMware_bootbank_nsx-da-<release>,
VMware_bootbank_nsx-esx-datapath-<release>, VMware_bootbank_nsx-exporter-<release>,
VMware_bootbank_nsx-host-<release>, VMware_bootbank_nsx-lldp-<release>, VMware_bootbank_nsx-
mpa-<release>, VMware_bootbank_nsx-netcpa-<release>, VMware_bootbank_nsx-python-
protobuf-<release>, VMware_bootbank_nsx-sfhc-<release>, VMware_bootbank_nsxa-<release>,
VMware_bootbank_nsxcli-<release>
  VIBs Removed:
  VIBs Skipped:
```

호스트에 이미 설치된 항목에 따라 일부 VIB가 설치되고, 일부는 제거되고, 일부는 건너뛴 수 있습니다. 명령 출력에 **Reboot Required: true**로 표시되지 않는 한 재부팅은 필요하지 않습니다.

결과

ESXi 호스트를 NSX-T Data Center 패브릭에 추가하면 호스트에 다음 VIB가 설치됩니다.

nsx-adf

(자동화된 진단 프레임워크) 성능 데이터를 수집하고 분석하여 성능 문제에 대한 로컬(호스트) 및 중앙(데이터 센터 간) 진단을 둘 다 생성합니다.

nsx-aggsservice

NSX-T Data Center 집계 서비스에 대한 호스트 측 라이브러리를 제공합니다. NSX-T Data Center 집계 서비스는 관리부 노드에서 실행되고 NSX-T Data Center 구성 요소에서 런타임 상태를 가져오는 서비스입니다.

nsx-cli-libs

하이퍼바이저 호스트에서 NSX-T Data Center CLI를 제공합니다.

nsx-common-libs

AES, SHA-1, UUID, 비트맵 등과 같은 일부 유틸리티 클래스를 제공합니다.

nsx-context-mux

NSX Guest Introspection 릴레이 기능을 제공합니다. VMware Tools 게스트 에이전트가 게스트 컨텍스트를 내부 및 등록된 타사 파트너 장치로 릴레이할 수 있도록 허용합니다.

nsx-esx-datapath

NSX-T Data Center 데이터부 패킷 처리 기능을 제공합니다.

nsx-exporter

관리부에서 실행되는 집계 서비스에 런타임 상태를 보고하는 호스트 에이전트를 제공합니다.

nsx-host

호스트에 설치되는 VIB 번들에 대한 메타데이터를 제공합니다.

nsx-metrics-libs

데몬 메트릭을 수집하기 위한 메트릭 유틸리티 클래스를 제공합니다.

nsx-mpa

NSX Manager 및 하이퍼바이저 호스트 간 통신을 제공합니다.

nsx-nestdb-libs

NestDB는 호스트와 관련된 NSX 구성(원하는 구성/런타임 상태 등)을 저장하는 데이터베이스입니다.

nsx-netcpa

중앙 제어부 및 하이퍼바이저 간 통신을 제공합니다. 중앙 제어부에서 논리적 네트워킹 상태를 수신하고 이 상태를 데이터부에서 프로그래밍합니다.

nsx-opsagent

작업 에이전트 실행(전송 노드 인식, LLDP(링크 계층 검색 프로토콜), traceflow, 패킷 캡처 등)을 관리부에 전달합니다.

nsx-platform-client

중앙 집중식 CLI 및 감사 로그 수집을 위한 일반적인 CLI 실행 에이전트를 제공합니다.

nsx-profiling-libs

데몬 프로세스 프로파일링에 사용되는 gpeftool을 기준으로 하는 프로파일링 기능을 제공합니다.

nsx-proxy

중앙 제어부 및 관리부와 통신하는 유일한 노스바운드 연락 지점 에이전트를 제공합니다.

nsx-python-gevent

Python Gevent를 포함합니다.

nsx-python-greenlet

Python Greenlet 라이브러리(타사 라이브러리)를 포함합니다.

nsx-python-logging

Python 로그를 포함합니다.

nsx-python-protobuf

프로토콜 버퍼에 대한 Python 바인딩을 제공합니다.

nsx-rpc-lib

이 라이브러리는 nsx-rpc 기능을 제공합니다.

nsx-sfhc

SFHC(서비스 패브릭 호스트 구성 요소)입니다. 관리부의 인벤토리에서 하이퍼바이저의 수명 주기를 패브릭 호스트로 관리하기 위한 호스트 에이전트를 제공합니다. 여기서는 하이퍼바이저의 NSX-T Data Center 업그레이드 및 제거와 NSX-T Data Center 모듈의 모니터링과 같은 작업을 위한 채널을 제공합니다.

nsx-shared-lib

공유 NSX 라이브러리를 포함합니다.

nsx-upm-lib

클라이언트 측 구성을 평면화하고 중복 데이터 전송을 방지하기 위한 통합된 프로파일 관리 기능을 제공합니다.

nsx-vdpi

NSX-T Data Center 분산 방화벽에 대한 심층 패킷 검사 기능을 제공합니다.

nsxcli

하이퍼바이저 호스트에서 NSX-T Data Center CLI를 제공합니다.

vsipfwlib

분산 방화벽 기능을 제공합니다.

확인하려면 ESXi 호스트에서 `esxcli software vib list | grep nsx` 및 `esxcli software vib list | grep vsipfwlib` 명령을 실행할 수 있습니다. 또는 `esxcli software vib list | grep <yyyy-mm-dd>` 명령을 실행할 수 있습니다. 여기서 날짜는 설치한 날짜입니다.

다음에 수행할 작업

NSX-T Data Center 관리부에 호스트를 추가합니다. [CLI를 사용하여 클러스터를 구성하기 위해 NSX Manager 노드 배포](#)의 내용을 참조하십시오.

Ubuntu KVM 하이퍼바이저에 수동으로 NSX-T Data Center 소프트웨어 패키지 설치

호스트가 NSX-T Data Center에 참여하도록 준비하려면 Ubuntu KVM 호스트에 NSX-T Data Center 커널 모듈을 수동으로 설치할 수 있습니다. 이렇게 하면 NSX-T Data Center 제어부 및 관리부 패브릭을 구축할 수 있습니다. DEB 파일로 패키징된 NSX-T Data Center 커널 모듈은 하이퍼바이저 커널 내에서 실행되어 분산 라우팅, 분산 방화벽 및 브리징 기능과 같은 서비스를 제공합니다.

NSX-T Data Center DEB를 수동으로 다운로드한 후 이를 호스트 이미지의 일부로 만들 수 있습니다. 다운로드 경로는 NSX-T Data Center의 각 릴리스에 따라 변경됩니다. 그러므로 항상 NSX-T Data Center 다운로드 페이지를 확인하여 적합한 DEB를 가져오십시오.

사전 요구 사항

- 필요한 타사 패키지가 설치되어 있는지 확인합니다. [KVM 호스트에 타사 패키지 설치](#)의 내용을 참조하십시오.

절차

- 1 관리자 권한을 가진 사용자로 호스트에 로그인합니다.
- 2 (선택 사항) /tmp 디렉토리로 이동합니다.

```
cd /tmp
```

- 3 nsx-lcp 파일을 다운로드한 후 /tmp 디렉토리로 복사합니다.
- 4 tar 패키지의 압축을 풉니다.

```
tar -xvf nsx-lcp-<release>-ubuntu-trusty-amd64.tar.gz
```

- 5 패키지 디렉토리로 이동합니다.

```
cd nsx-lcp-trusty-amd64/
```

- 6 패키지를 설치합니다.

```
sudo dpkg -i *.deb
```

- 7 OVS 커널 모듈을 다시 로드합니다.

```
/etc/init.d/openvswitch-switch force-reload-kmod
```

하이퍼바이저가 OVS 인터페이스에서 DHCP를 사용하는 경우 DHCP가 구성된 네트워크 인터페이스를 다시 시작합니다. 네트워크 인터페이스에서 이전 dhclient 프로세스를 수동으로 중지하고 해당 인터페이스에서 새로운 dhclient 프로세스를 다시 시작할 수 있습니다.

- 8 dpkg -l | egrep 'nsx|openvswitch' 명령을 실행하여 확인할 수 있습니다.

출력에 나열된 설치된 패키지는 nsx-lcp-trusty-amd64 디렉토리에 있는 패키지와 일치해야 합니다.

모든 오류는 불완전한 종속성으로 야기될 수 있습니다. apt-get install -f 명령은 종속성을 해결하고 NSX-T Data Center 설치를 다시 실행하려고 시도합니다.

다음에 수행할 작업

NSX-T Data Center 관리부에 호스트를 추가합니다. [CLI를 사용하여 클러스터를 구성하기 위해 NSX Manager 노드 배포](#)의 내용을 참조하십시오.

RHEL 및 CentOS KVM 하이퍼바이저에 수동으로 NSX-T Data Center 소프트웨어 패키지 설치

호스트가 NSX-T Data Center에 참여하도록 준비하기 위해 RHEL 또는 CentOS KVM 호스트에 NSX-T Data Center 커널 모듈을 수동으로 설치할 수 있습니다.

이렇게 하면 NSX-T Data Center 제어부 및 관리부 패브릭을 구축할 수 있습니다. RPM 파일로 패키징된 NSX-T Data Center 커널 모듈은 하이퍼바이저 커널 내에서 실행되어 분산 라우팅, 분산 방화벽 및 브리징 기능과 같은 서비스를 제공합니다.

NSX-T Data Center RPM을 수동으로 다운로드한 후 이를 호스트 이미지의 일부로 만들 수 있습니다. 다운로드 경로는 NSX-T Data Center의 각 릴리스에 따라 변경됩니다. 그러므로 항상 NSX-T Data Center 다운로드 페이지를 확인하여 적합한 RPM을 가져오십시오.

사전 요구 사항

RHEL 또는 CentOS 저장소에 연결하는 기능.

절차

- 1 관리자 권한으로 호스트에 로그인합니다.
- 2 nsx-lcp 파일을 다운로드한 후 /tmp 디렉토리로 복사합니다.
- 3 tar 패키지의 압축을 풉니다.

```
tar -zxvf nsx-lcp-<release>-rhel7.4_x86_64.tar.gz
```

- 4 패키지 디렉토리로 이동합니다.

```
cd nsx-lcp-rhel74_x86_64/
```

- 5 패키지를 설치합니다.

```
sudo yum install *.rpm
```

yum install 명령을 실행하면 모든 NSX-T Data Center 종속성이 해결되고 RHEL 또는 CentOS 호스트가 해당 리포지토리에 연결할 수 있다고 간주됩니다.

- 6 OVS 커널 모듈을 다시 로드합니다.

```
/usr/share/openvswitch/scripts/ovs-systemd-reload force-reload-kmod
```

하이퍼바이저가 OVS 인터페이스에서 DHCP를 사용하는 경우 DHCP가 구성된 네트워크 인터페이스를 다시 시작합니다. 네트워크 인터페이스에서 이전 dhclient 프로세스를 수동으로 중지하고 해당 인터페이스에서 새로운 dhclient 프로세스를 다시 시작할 수 있습니다.

- 7 rpm -qa | egrep 'nsx|openvswitch' 명령을 실행하여 확인할 수 있습니다.

출력에 나열된 설치된 패키지는 nsx-rhel74 또는 nsx-centos74 디렉토리에 있는 패키지과 일치해야 합니다.

다음에 수행할 작업

NSX-T Data Center 관리부에 호스트를 추가합니다. CLI를 사용하여 클러스터를 구성하기 위해 [NSX Manager 노드 배포](#)의 내용을 참조하십시오.

SUSE KVM 하이퍼바이저에 수동으로 NSX-T Data Center 소프트웨어 패키지 설치

호스트가 NSX-T Data Center에 참여하도록 준비하려면 SUSE KVM 호스트에 NSX-T Data Center 커널 모듈을 수동으로 설치할 수 있습니다.

이렇게 하면 NSX-T Data Center 제어부 및 관리부 패브릭을 구축할 수 있습니다. RPM 파일로 패키징된 NSX-T Data Center 커널 모듈은 하이퍼바이저 커널 내에서 실행되어 분산 라우팅, 분산 방화벽 및 브리징 기능과 같은 서비스를 제공합니다.

NSX-T Data Center RPM을 수동으로 다운로드한 후 이를 호스트 이미지의 일부로 만들 수 있습니다. 다운로드 경로는 NSX-T Data Center의 각 릴리스에 따라 변경됩니다. 그러므로 항상 NSX-T Data Center 다운로드 페이지를 확인하여 적합한 RPM을 가져오십시오.

사전 요구 사항

SUSE 저장소에 연결하는 기능.

절차

- 1 관리자 권한으로 호스트에 로그인합니다.
- 2 nsx-lcp 파일을 다운로드한 후 /tmp 디렉토리로 복사합니다.
- 3 tar 패키지의 압축을 풉니다.

```
tar -zxvf nsx-lcp-3.0.0.0.0.14335404-linux64-sles12sp3.tar.gz
```

- 4 패키지 디렉토리로 이동합니다.

```
cd nsx-lcp-linux64-sles12sp3
```

- 5 패키지를 설치합니다.

```
sudo zypper --no-gpg-checks install -y *.rpm
```

zypper install 명령을 실행하면 모든 NSX-T Data Center 종속성이 해결되고 SUSE 호스트가 해당 리포지토리에 연결할 수 있다고 간주됩니다.

- 6 OVS 커널 모듈을 다시 로드합니다.

```
/usr/share/openvswitch/scripts/ovs-systemd-reload force-reload-kmod
```

하이퍼바이저가 OVS 인터페이스에서 DHCP를 사용하는 경우 DHCP가 구성된 네트워크 인터페이스를 다시 시작합니다. 네트워크 인터페이스에서 이전 dhclient 프로세스를 수동으로 중지하고 해당 인터페이스에서 새로운 dhclient 프로세스를 다시 시작할 수 있습니다.

7 `zypper packages --installed-only | grep System | egrep 'openvswitch|nsx'` 명령을 실행하여 확인할 수 있습니다.

출력에 나열된 설치된 패키지는 `nsx-lcp-linux64-sles12sp3` 디렉토리에 있는 패키지와 일치해야 합니다.

다음에 수행할 작업

NSX-T Data Center 관리부에 호스트를 추가합니다. [CLI를 사용하여 클러스터를 구성하기 위해 NSX Manager 노드 배포](#)의 내용을 참조하십시오.

완전 축소형 vSphere 클러스터 NSX-T 배포

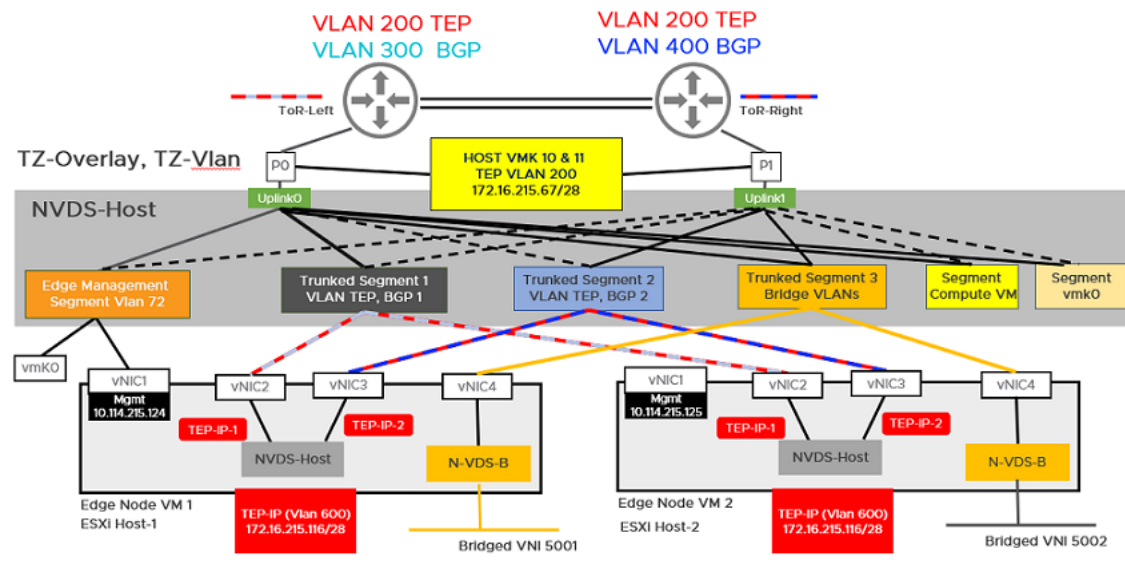
단일 클러스터에서 NSX Manager 호스트 전송 노드 및 NSX Edge VM을 구성할 수 있습니다. 클러스터의 각 호스트는 NSX-T용으로 구성된 두 개의 물리적 NIC를 제공합니다.

중요 NSX-T 2.4.2 또는 2.5 릴리스부터 완전히 축소된 단일 vSphere 클러스터 토폴로지를 배포합니다.

이 절차에서 참조하는 토폴로지는 다음을 사용합니다.

- 클러스터의 호스트로 구성된 vSAN.
- 호스트당 최소 2개의 물리적 NIC
- vMotion 및 관리 VMkernel 인터페이스.

그림 10-4. 토폴로지: NSX Edge 및 게스트 VM과의 호스트 통신을 관리하는 단일 N-VDS 스위치



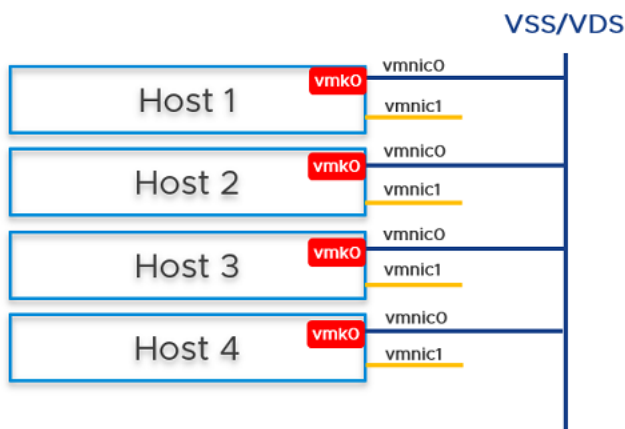
사전 요구 사항

- 모든 호스트는 vSphere 클러스터에 속해야 합니다.
- 각 호스트에는 두 개의 물리적 NIC가 사용되도록 설정되어 있습니다.

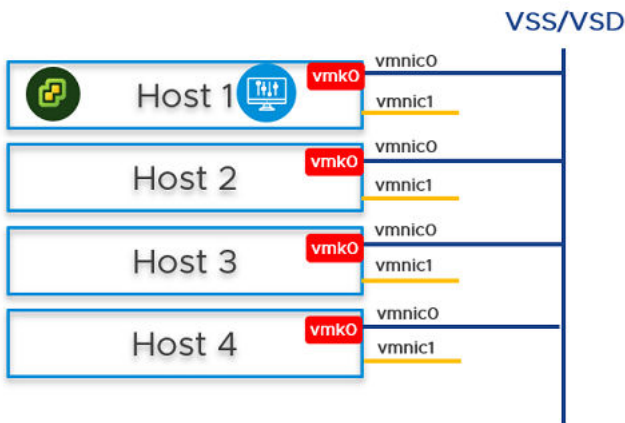
- 모든 호스트를 vCenter Server에 등록합니다.
- vCenter Server에서 호스트가 공유 스토리지를 사용할 수 있는지 확인합니다.
- 호스트 TEP IP 및 NSX Edge TEP IP는 다른 VLAN에 있어야 합니다. 호스트 워크로드의 북-남 트래픽은 GENEVE에 캡슐화되고 소스 IP가 호스트 TEP이고 대상 IP가 NSX Edge TEP인 NSX Edge 노드로 전송됩니다. 이러한 TEP는 서로 다른 VLAN 또는 서브넷에 있어야 하므로 이 트래픽은 TOR(랙 상단) 스위치를 통해 라우팅해야 합니다. 호스트에 사용되는 전송 VLAN은 VLAN 200이고 NSX Edge에 사용되는 전송 VLAN은 VLAN 600입니다.

절차

- 1 vSS 또는 vDS에서 vmnic0인 ESXi 호스트 4개를 준비합니다. vmnic1은 무료입니다.



- 2 호스트 1에서 vCenter Server를 설치하고, vSS/vDS 포트 그룹을 구성한 후 호스트에서 생성된 포트 그룹에 NSX Manager를 설치합니다.



- 3 전송 노드로 ESXi 호스트 1, 2, 3 및 4를 준비합니다.
 - a 명명된 팀 구성 정책을 사용하여 VLAN 전송 영역 및 오버레이 전송 영역을 생성합니다. [전송 영역 생성](#) 항목을 참조하십시오.

- b 호스트의 터널 끝점 IP 주소에 대해 IP 풀 또는 DHCP를 생성합니다. [터널 끝점 IP 주소에 대한 IP 풀 생성](#) 항목을 참조하십시오.
- c Edge 노드의 터널 끝점 IP 주소에 대해 IP 풀 또는 DHCP를 생성합니다. [터널 끝점 IP 주소에 대한 IP 풀 생성](#) 항목을 참조하십시오.
- d 명명된 팀 구성 정책을 사용하여 업링크 프로파일을 생성합니다. [업링크 프로파일 생성](#) 항목을 참조하십시오.
- e 전송 노드 프로파일을 적용하여 호스트를 전송 노드로 구성합니다. 이 단계에서 전송 노드 프로파일은 vmnic1(사용되지 않은 물리적 NIC)만 N-VDS 스위치로 마이그레이션합니다. 전송 노드 프로파일이 클러스터 호스트에 적용되면 N-VDS 스위치가 생성되고 vmnic1이 N-VDS 스위치에 연결됩니다. [전송 노드 프로파일 추가](#) 항목을 참조하십시오.

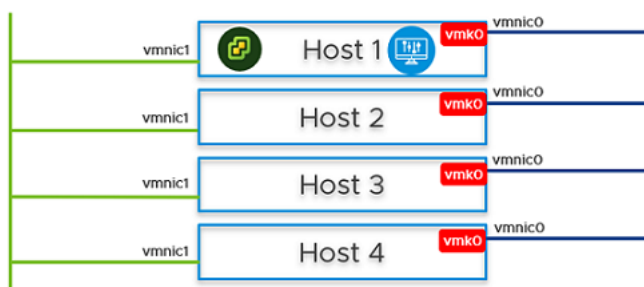
전송 노드 프로파일 편집 - TNP-host



N-VDS 이름*	vds-1	▼
연결된 전송 영역	tz	
NIOC 프로파일*	nsx-default-nioc-hostswitch-profile	▼
	또는 새 NIOC 프로파일 생성	
업링크 프로파일*	hostnodeprofile	▼
	또는 새 업링크 프로파일 생성	
LLDP 프로파일*	LLDP [Send Packet Enabled]	▼
IP 할당*	IP 풀 사용	▼
IP 풀*	ippoolhostnode	▼
	또는 새 IP 풀 생성 및 사용	
물리적 NIC	vmnic1	activeuplinkhost ▼
	물리적 NIC 추가	
물리적 NIC 전용 마이그레이션	<input checked="" type="checkbox"/> 예	
물리적 NIC에 마이그레이션용으로 선택한 vmk가 없는 경우 이 옵션을 사용하도록 설정합니다.		
설치를 위한 네트워크 매핑	매핑 추가	
제거를 위한 네트워크 매핑	매핑 추가	

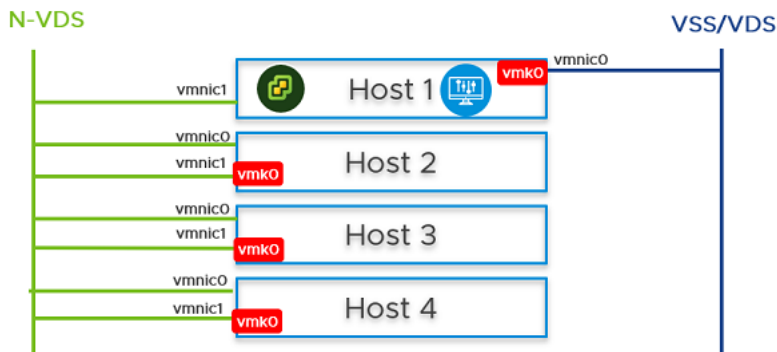
N-VDS

VSS/VDS

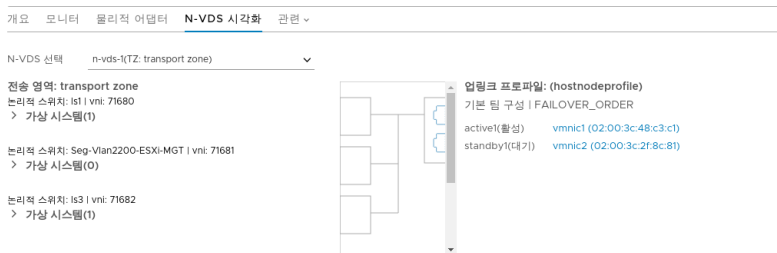


모든 호스트의 vmnic1이 N-VDS 스위치로 추가됩니다. 따라서 두 개의 물리적 NIC 중 하나가 N-VDS 스위치로 마이그레이션됩니다. vmnic0 인터페이스가 여전히 vSS 또는 vDS 스위치에 연결되어 있으므로 호스트에 대한 연결을 사용할 수 있게 됩니다.

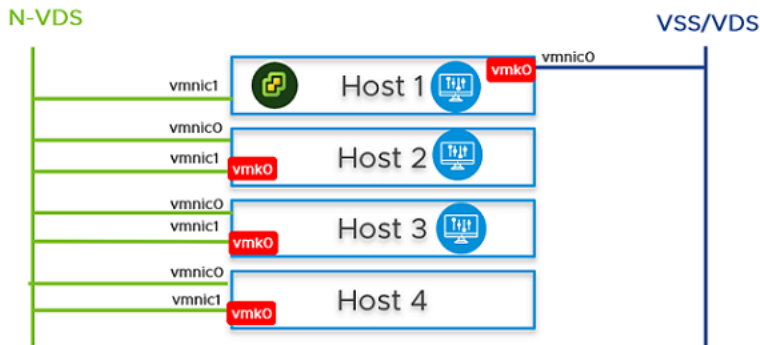
- 4 NSX Manager UI에서 NSX Manager, vCenter Server 및 NSX Edge에 대해 VLAN 지원 세그먼트를 생성합니다. 각 VLAN 지원 세그먼트에 대해 올바른 팀 구성 정책을 선택해야 합니다. VLAN 트렁크 논리적 스위치를 대상으로 사용하지 마십시오. NSX Manager UI에서 대상 세그먼트를 생성하는 경우 **VLAN 목록 입력** 필드에 VLAN 값을 하나만 입력합니다.
- 5 호스트 2, 호스트 3 및 호스트 4에서는 vmk0 어댑터와 vmnic0을 VSS/VDS에서 N-VDS 스위치로 함께 마이그레이션해야 합니다. 각 호스트에서 NSX-T 구성을 업데이트합니다. 마이그레이션하는 동안 다음을 확인합니다.
 - vmk0가 **Edge 관리 세그먼트**에 매핑되어 있습니다.
 - vmnic0은 활성 업링크인 **uplink-1**에 매핑되어 있습니다.



- 6 vCenter Server에서 호스트 2, 호스트 3 및 호스트 4로 이동하고 vmk0 어댑터가 N-VDS의 vmnic0 물리적 NIC에 연결되어 있고 연결 가능한지 확인합니다.
- 7 NSX Manager UI에서 호스트 2, 호스트 3 및 호스트 4로 이동하고, 두 물리적 NIC가 N-VDS 스위치에 있는지 확인합니다.

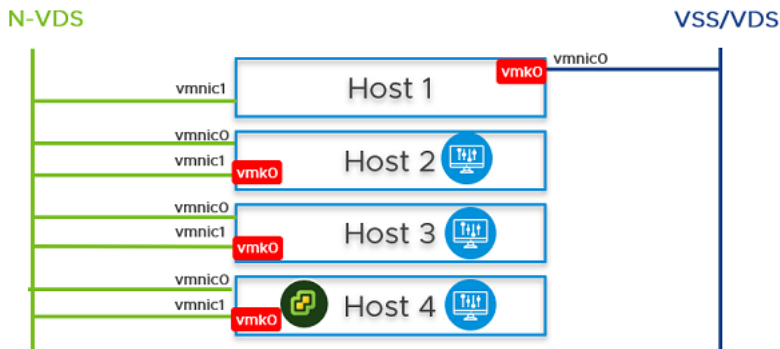


- 8 호스트 2 및 호스트 3의 NSX Manager UI에서 NSX Manager를 설치하고 NSX Manager를 세그먼트에 연결합니다. 클러스터가 형성될 때까지 약 10분 정도 기다린 후 클러스터가 구성되었는지 확인합니다.



- 9 첫 번째 NSX Manager 노드의 전원을 끕니다. 약 10분 동안 기다립니다.
- 10 NSX Manager 및 vCenter Server를 이전에 생성한 논리적 스위치에 다시 연결합니다. 호스트 4에서 NSX Manager의 전원을 켭니다. 약 10분 동안 대기하여 클러스터가 안정된 상태에 있는지 확인합니다. 첫 번째 NSX Manager의 전원이 꺼진 상태에서 콜드 vMotion을 수행하여 NSX Manager 및 vCenter Server를 호스트 1에서 호스트 4로 마이그레이션합니다.

vMotion 제한은 <https://kb.vmware.com/s/article/56991>을 참조하십시오.

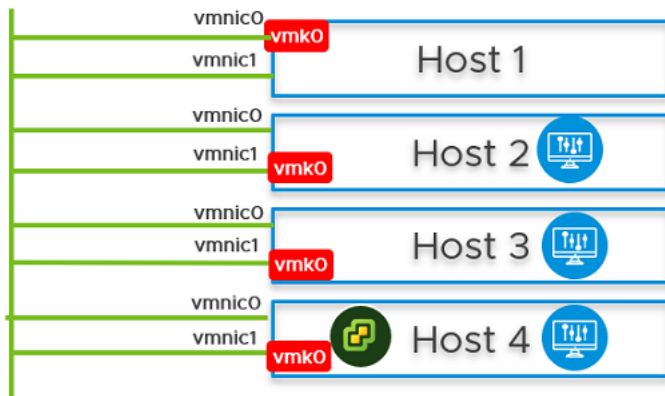


- 11 NSX Manager UI에서 호스트 1로 이동하고 vmk0 및 vmnic0를 VSS에서 N-VDS 스위치로 마이그레이션합니다.

- 12 설치를 위한 네트워크 매핑** 필드에서 vmk0 어댑터가 N-VDS 스위치의 **Edge 관리 세그먼트**에 매핑되는지 확인합니다.

The screenshot shows the 'NSX 구성' (NSX Configuration) window. On the left, a sidebar lists '1 호스트 세부 정보' and '2 NSX 구성', with '2 NSX 구성' selected. The main panel displays the '정적 IP 목록 사용' (Static IP List Usage) configuration. It includes fields for '정적 IP 목록' (Static IP List) with the value '172.16.228.36', '게이트웨이' (Gateway) with '172.16.228.33', and '서브넷 마스크' (Subnet Mask) with '255.255.255.240'. Below these, a table shows '물리적 NIC' (Physical NIC) settings: 'vmnic1' and 'vmnic2' are mapped to 'uplink-1' and 'uplink-2' respectively. A toggle for '물리적 NIC 전용 마이그레이션' (Physical NIC Dedicated Migration) is set to '아니요' (No). At the bottom, there are buttons for '취소' (Cancel), '이전' (Previous), and '완료' (Finish). A note at the bottom states: '설치를 위한 네트워크 매핑' (Network mapping for installation) and '제거를 위한 네트워크 매핑' (Network mapping for removal), both with a '매핑 추가' (Add mapping) button.

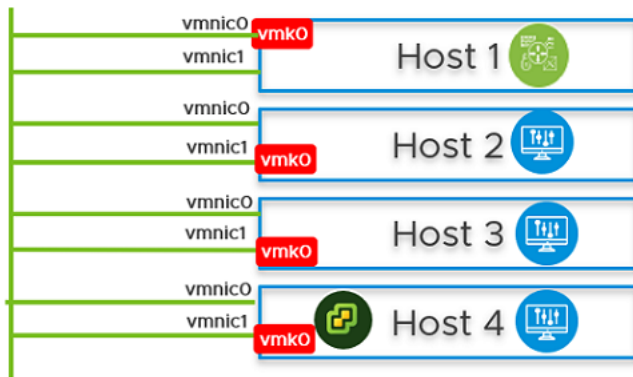
N-VDS



- 13** 호스트 1의 NSX Manager UI에서 NSX Edge VM을 설치합니다.

NSX Edge 전송 노드 생성 항목을 참조하십시오.

N-VDS



- 14 NSX Edge VM을 관리부에 연결합니다.

NSX Edge를 관리부에 연결 항목을 참조하십시오.

- 15 종방향 트래픽 연결을 설정하려면 외부 라우터를 사용하여 NSX Edge VM을 구성합니다.
- 16 NSX Edge VM과 외부 라우터 간의 북-남 트래픽 연결이 있는지 확인합니다.
- 17 전체 클러스터가 재부팅되는 전원 장애 시나리오의 경우 NSX-T 관리 구성 요소가 실행되지 않으며 N-VDS와 통신하지 못할 수 있습니다. 이러한 시나리오를 피하려면 다음 단계를 수행합니다.

경고 API 명령이 잘못 실행되면 NSX Manager와의 연결이 끊깁니다.

참고 단일 클러스터 구성에서 관리 구성 요소는 VM으로 N-VDS 스위치에 호스팅됩니다. 관리 구성 요소가 기본적으로 연결하는 N-VDS 포트는 보안 고려 사항으로 인해 차단된 포트가 초기화됩니다. 전원 장애가 발생하여 4개의 모든 호스트를 재부팅해야 하는 경우, 관리 VM 포트가 차단된 상태로 초기화됩니다. 순환 종속성을 방지하려면 차단되지 않은 상태로 N-VDS에서 포트를 생성하는 것이 좋습니다. 차단되지 않은 포트는 클러스터가 재부팅될 때 NSX-T 관리 구성 요소가 N-VDS와 통신하여 정상 기능을 재개할 수 있도록 보장합니다.

하위 작업이 끝나면 마이그레이션 명령이 다음을 가져옵니다.

- NSX Manager가 있는 호스트 노드의 UUID.
- NSX Manager VM의 UUID. 이를 차단되지 않은 상태의 정적 논리적 포트에 마이그레이션합니다.

모든 호스트의 전원을 끄거나 전원을 켜는 경우 또는 NSX Manager VM을 다른 호스트로 이동하는 경우에는 NSX Manager가 다시 실행되어 차단되지 않은 포트에 연결될 수 있으므로 NSX-T 관리 구성 요소와의 연결 끊김을 방지할 수 있습니다.

- a NSX Manager UI에서 **고급 네트워킹 및 보안** 탭(2.5.1 및 이전 릴리스)으로 이동합니다. **세그먼트 계산 VM** 세그먼트를 검색합니다. **개요** 탭을 선택하고 UUID를 찾아 복사합니다. 이 예에 사용된 UUID는 `c3fd8e1b-5b89-478e-abb5-d55603f04452`입니다.
- b 각 NSX Manager에 대한 JSON 페이로드를 생성합니다.
 - JSON 페이로드에서 `logical_switch_id`의 값을 이전에 생성한 **Edge 관리 세그먼트**의 UUID로 바꾸어 **UNBLOCKED_VLAN** 상태에서 초기화 상태의 논리적 포트를 생성합니다.
 - 각 NSX Manager의 페이로드에서 `attachment_type_id` 및 `display_name` 값은 서로 다릅니다.

중요 이 단계를 반복하여 총 4개의 JSON 파일을 생성합니다(NSX Manager용 3개, VCSA(vCenter Server Appliance)용 1개).

```
port1.json
{
  "admin_state": "UP",
  "attachment": {
    "attachment_type": "VIF",
    "id": "nsxmgr-port-147"
  },
  "display_name": "NSX Manager Node 147 Port",
  "init_state": "UNBLOCKED_VLAN",
  "logical_switch_id": "c3fd8e1b-5b89-478e-abb5-d55603f04452"
}
```

설명:

- `admin_state`: 포트의 상태입니다. 실행 중이어야 합니다.
- `attachment_type`: VIF로 설정해야 합니다. 모든 VM은 VIF ID를 사용하여 NSX-T 스위치 포트에 연결됩니다.
- `id`: VIF ID입니다. 각 NSX Manager에 대해 고유해야 합니다. 3개의 NSX Manager가 있는 경우 페이로드가 3개 있으며 각각의 VIF ID가 달라야 합니다. 고유한 UUID를 생성하려면 NSX Manager의 루트 셸에 로그인하고 `/usr/bin/uuidgen`을 실행하여 고유한 UUID를 생성합니다.
- `display_name`: NSX 관리자가 다른 NSX Manager 표시 이름에서 식별할 수 있도록 고유해야 합니다.
- `init_state`: 값이 UNBLOCKED_VLAN으로 설정된 경우 NSX Manager를 사용할 수 없는 경우에도 NSX는 NSX Manager에 대한 포트 차단을 해제합니다.
- `logical_switch_id`: **Edge 관리 세그먼트**의 논리적 스위치 ID입니다.

- c 3개의 NSX Manager가 배포된 경우 NSX Manager의 논리적 포트 각각에 대해 하나씩 3개의 페이로드를 생성해야 합니다. 예를 들면 port1.json, port2.json, port3.json과 같습니다.

다음 명령을 실행하여 페이로드를 생성합니다.

```
curl -X POST -k -u '<username>:<password>' -H 'Content-Type:application/json' -d @port1.json https://nsxmgr/api/v1/logical-ports
```

```
curl -X POST -k -u '<username>:<password>' -H 'Content-Type:application/json' -d @port2.json https://nsxmgr/api/v1/logical-ports
```

```
curl -X POST -k -u '<username>:<password>' -H 'Content-Type:application/json' -d @port3.json https://nsxmgr/api/v1/logical-ports
```

논리적 포트를 생성하기 위한 API 실행의 예입니다.

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -X POST -k -u
'<username>:<password>' -H 'Content-Type:application/json' -d @port1.json https://
localhost/api/v1/logical-ports
{
  "logical_switch_id" : "c3fd8e1b-5b89-478e-abb5-d55603f04452",
  "attachment" : {
    "attachment_type" : "VIF",
    "id" : "nsxmgr-port-147"
  },
  "admin_state" : "UP",
  "address_bindings" : [ ],
  "switching_profile_ids" : [ {
    "key" : "SwitchSecuritySwitchingProfile",
    "value" : "fbc4fb17-83d9-4b53-a286-ccdf04301888"
  }, {
    "key" : "SpoofGuardSwitchingProfile",
    "value" : "fad98876-d7ff-11e4-b9d6-1681e6b88ec1"
  }, {
    "key" : "IpDiscoverySwitchingProfile",
    "value" : "0c403bc9-7773-4680-a5cc-847ed0f9f52e"
  }, {
    "key" : "MacManagementSwitchingProfile",
    "value" : "1e7101c8-cfef-415a-9c8c-ce3d8dd078fb"
  }, {
    "key" : "PortMirroringSwitchingProfile",
    "value" : "93b4b7e8-f116-415d-a50c-3364611b5d09"
  }, {
    "key" : "QosSwitchingProfile",
    "value" : "f313290b-eba8-4262-bd93-fab5026e9495"
  } ],
  "init_state" : "UNBLOCKED_VLAN",
  "ignore_address_bindings" : [ ],
  "resource_type" : "LogicalPort",
  "id" : "02e0d76f-83fa-4839-a525-855b47ecb647",
  "display_name" : "NSX Manager Node 147 Port",
  "_create_user" : "admin",
  "_create_time" : 1574716624192,
  "_last_modified_user" : "admin",
```

```
"_last_modified_time" : 1574716624192,
"_system_owned" : false,
"_protection" : "NOT_PROTECTED",
"_revision" : 0
```

- d 논리적 포트가 생성되어 있는지 확인합니다.

스위치 포트 스위칭 프로파일						
<div> + 추가 편집 삭제 작업 <div>검색</div> </div>						
<input type="checkbox"/>	논리적 포트	ID	관리 상태	작업 상태	스위칭 프로파일	연결
<input type="checkbox"/>	1356a49d-dc33-42be-9e83-4c6...	1356...d0ee	● 실행 중	● 실행 중	nsx-default-switch-security-non...	LR:80fb...2662
<input type="checkbox"/>	61d5708b-a4ff-4954-b217-8338...	61d5...b43a	● 실행 중	● 실행 중	nsx-default-switch-security-non...	LR:42ac...ad24
<input type="checkbox"/>	NSX Manager Node 147 Port	58ad...a1cb	● 실행 중	● 종료	nsx-default-switch-security-vif...	VM:nsx-mgr-147
<input type="checkbox"/>	ubuntu12.04.1-2G-LAMP/ubuntu1...	3fb2...f698	● 실행 중	● 실행 중	nsx-default-switch-security-vif...	VM:vm1
<input type="checkbox"/>	vmknic@n-vds-1@94b323e6-1ee...	2021...4d76	● 실행 중	● 실행 중	nsx-default-switch-security-vif...	VIF:abf2...0495
<input type="checkbox"/>	worker/worker vmx@94b323e6-...	50b7...9b4c	● 실행 중	● 실행 중	nsx-default-switch-security-vif...	VM:vm3

- e 각 NSX Manager에 대한 VM 인스턴스 ID를 확인합니다. **인벤토리** → **가상 시스템**에서 인스턴스 ID를 검색하고 NSX Manager VM을 선택한 후 **개요** 탭을 선택하고 인스턴스 ID를 복사할 수 있습니다. 또는 vCenter Server의 MOB(관리 개체 브라우저)에서 인스턴스 ID를 검색합니다. NSX Manager VM의 VNIC 하드웨어 인덱스를 가져오기 위해 ID에 **:4000**을 추가합니다.

예를 들어 VM의 인스턴스 UUID가 503c9e2b-0abf-a91c-319c-1d2487245c08이면 vnic 인덱스가 503c9e2b-0abf-a91c-319c-1d2487245c08:4000이 됩니다. 세 가지 NSX Manager vnic 인덱스는 다음과 같습니다.

mgr1 vnic: 503c9e2b-0abf-a91c-319c-1d2487245c08:4000

mgr2 vnic: 503c76d4-3f7f-ed5e-2878-cffc24df5a88:4000

mgr3 vnic: 503cafd5-692e-d054-6463-230662590758:4000

- f NSX Manager를 호스팅하는 전송 노드 ID를 확인합니다. 각각 다른 전송 노드에 호스팅된 3개의 NSX Manager가 있는 경우에는 포트 노드 ID를 기록해 둡니다. 예를 들어 3개의 전송 노드 ID는 다음과 같습니다.

tn1: 12d19875-90ed-4c78-a6bb-a3b1dfe0d5ea

tn2: 4b6e182e-0ee3-403f-926a-fb7c8408a9b7

tn3: d7cec2c9-b776-4829-beea-1258d8b8d59b

- g NSX Manager를 새로 생성된 포트로 마이그레이션할 때 페이로드로 사용될 전송 노드 구성을 검색합니다.

예를 들면 다음과 같습니다.

```
curl -k -u '<user>:<password>' https://nsxmgr/api/v1/transport-nodes/
12d19875-90ed-4c78-a6bb-a3b1dfe0d5ea > tn1.json
```

```
curl -k -u '<user>:<password>' https://nsxmgr/api/v1/transport-nodes/
4b6e182e-0ee3-403f-926a-fb7c8408a9b7 > tn2.json
```

```
curl -k -u '<user>:<password>' https://nsxmgr/api/v1/transport-nodes/d7cec2c9-
b776-4829-beea-1258d8b8d59b > tn3.json
```

- h NSX Manager를 이전 포트에서 **Edge 관리 세그먼트**의 새로 생성된 차단되지 않은 논리적 포트 로 마이그레이션합니다. VIF-ID 값은 NSX Manager에 대해 이전에 생성된 포트의 연결 ID입니다.

NSX Manager를 마이그레이션하려면 다음 매개 변수가 필요합니다.

- 전송 노드 ID
- 전송 노드 구성
- NSX Manager VNIC 하드웨어 인덱스
- NSX Manager VIF ID

새로 생성된 차단되지 않은 포트 로 NSX Manager를 마이그레이션하는 API 명령은 다음과 같습니다.

```
/api/v1/transport-nodes/<TN-ID>?vnic=<VNIC-ID>&vif=<VIF-ID>
```

예를 들면 다음과 같습니다.

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -k -X PUT -u 'admin:VMware1!
VMware1!' -H 'Content-Type:application/json' -d @mgr.json 'https://
localhost/api/v1/transport-nodes/11161331-11f8-45c7-8747-34e7218b687f?
vnic=5028d756-d36f-719e-3db5-7ae24aa1d6f3:4000&vif=nsxmgr-port-147'
```

- i 정적으로 생성된 논리적 포트가 실행 중인지 확인합니다.

스위치 **포트** 스위칭 프로파일

+ 추가 편집 삭제 작업							
<input type="checkbox"/>	논리적 포트 ↑	ID	관리 상태	작업 상태	스위칭 프로파일	연결	논리적 스위치
<input type="checkbox"/>	1356a49d-dc33-42be-9e83-4c6...	1356...d0ee	● 실행 중	● 실행 중	nsx-default-switch-security-non...	LR:80fb...2662	ls3
<input type="checkbox"/>	61d5708b-a4ff-4954-b217-8338...	61d5...b43a	● 실행 중	● 실행 중	nsx-default-switch-security-non...	LR:42ac...ad24	ls1
<input type="checkbox"/>	NSX Manager Node 147 Port	58ad...alcb	● 실행 중	● 실행 중	nsx-default-switch-security-vif...	VM:nsx-mgr-147	ls1
<input type="checkbox"/>	ubuntu12.04.1-2G-LAMP/ubuntu1...	3fb2...f698	● 실행 중	● 실행 중	nsx-default-switch-security-vif...	VM:vm1	ls1
<input type="checkbox"/>	vmknic@n-vds-1@94b323e6-1ee...	2021...4d76	● 실행 중	● 실행 중	nsx-default-switch-security-vif...	VIF:abr2...0495	Seg-Vlan2200-ESXi-MGT
<input type="checkbox"/>	worker/worker.vmx@94b323e6...	50b7...9b4c	● 실행 중	● 실행 중	nsx-default-switch-security-vif...	VM:vm3	ls3

- j 클러스터의 모든 NSX Manager에 대해 위의 단계를 반복합니다.

NSX-T와의 호스트 프로파일 통합

11

ESXi 호스트에서 추출된 호스트 프로파일을 NSX-T와 통합하여 ESXi 및 NSX-T VIB를 상태 저장 및 상태 비저장 서버에 배포합니다.

본 장은 다음 항목을 포함합니다.

- 상태 비저장 클러스터 자동 배포
- 상태 저장 서버

상태 비저장 클러스터 자동 배포

상태 비저장 호스트는 구성을 유지하지 않으므로 호스트의 전원을 켤 때 필요한 시작 파일을 제공하기 위해 자동 배포 서버가 필요합니다.

이 섹션에서는 vSphere Auto Deploy 및 NSX-T 전송 노드 프로파일을 사용하여 상태 비저장 클러스터를 설정함으로써 다른 버전의 ESXi 및 NSX-T를 포함하는 새 이미지 프로파일로 호스트를 재프로비저닝할 수 있도록 도와줍니다. vSphere 자동 재배포용으로 설정된 호스트는 자동 배포 서버 및 vSphere 호스트 프로파일을 사용하여 호스트를 사용자 지정합니다. NSX-T 전송 노드 프로파일이 호스트에서 NSX-T를 구성하도록 이러한 호스트를 설정할 수도 있습니다.

따라서 vSphere 자동 배포 및 NSX-T 전송 노드 프로파일에서 사용자 지정 ESXi 및 NSX-T 버전을 사용하여 호스트를 재프로비저닝하도록 상태 비저장 호스트를 설정할 수 있습니다.

상태 비저장 클러스터를 자동 배포하는 상위 수준 작업

상태 비저장 클러스터를 자동으로 배포하는 상위 수준 작업입니다.

상태 비저장 클러스터 자동 배포를 설정하는 상위 수준 작업은 다음과 같습니다.

- 1 사전 요구 사항 및 지원되는 버전: [사전 요구 사항 및 지원되는 버전](#) 항목을 참조하십시오.
- 2 (참조 호스트) 사용자 지정 이미지 프로파일을 생성합니다. [상태 비저장 호스트에 대한 사용자 지정 이미지 프로파일 생성](#) 항목을 참조하십시오.
- 3 (참조 및 대상 호스트) 사용자 지정 이미지 프로파일을 연결합니다. [사용자 지정 이미지를 참조 및 대상 호스트와 연결](#) 항목을 참조하십시오.

- 4 (참조 호스트) ESXi에서 네트워크 구성을 설정합니다. [참조 호스트에서 네트워크 구성 설정](#) 항목을 참조하십시오.
- 5 (참조 호스트) NSX에서 전송 노드로 구성합니다. [참조 호스트를 NSX-T의 전송 노드로 구성](#) 항목을 참조하십시오.
- 6 (참조 호스트) 호스트 프로파일을 추출하고 확인합니다. [호스트 프로파일 추출 및 확인](#) 항목을 참조하십시오.
- 7 (참조 및 대상 호스트) 상태 비저장 클러스터와의 호스트 프로파일 연결을 확인합니다. [상태 비저장 클러스터와 호스트 프로파일 간의 연결 확인](#) 항목을 참조하십시오.
- 8 (참조 호스트) 호스트 사용자 지정을 업데이트합니다. [호스트 사용자 지정 업데이트](#) 항목을 참조하십시오.
- 9 (대상 호스트) 자동 배포를 트리거합니다. [대상 호스트에서 자동 배포 트리거](#) 항목을 참조하십시오.
 - a 전송 노드 프로파일 적용 전. [TNP를 적용하기 전에 호스트 재부팅](#) 항목을 참조하십시오.
 - b 전송 노드 프로파일을 적용합니다. [상태 비저장 클러스터에 TNP 적용](#) 항목을 참조하십시오.
 - c 전송 노드 프로파일 적용 후. [TNP를 적용한 후에 호스트 재부팅](#) 항목을 참조하십시오.
- 10 호스트 프로파일 및 전송 노드 프로파일 문제를 해결합니다. [호스트 프로파일 및 전송 노드 프로파일 문제 해결](#) 항목을 참조하십시오.

사전 요구 사항 및 지원되는 버전

사전 요구 사항 및 지원되는 ESXi 및 NSX-T 버전.

지원되는 워크플로

- 이미지 프로파일 및 호스트 프로파일 포함

사전 요구 사항

- 동종 클러스터(클러스터 내의 모든 호스트가 상태 비저장 또는 상태 저장이어야 함)만 지원됩니다.
- Image Builder 서비스를 사용하도록 설정해야 합니다.
- Auto Deploy 서비스를 사용하도록 설정해야 합니다.

지원되는 NSX 및 ESXi 버전

지원되는 ESXi 버전	ESXi 67ep6	ESXi 67u2	ESXi 67u3	ESXi 67ep7	ESXi 67ep15	ESXi 67ep17
NSX-T Data Center 2.4	예	예	아니요	아니요	아니요	아니요
NSX-T Data Center 2.4.1	예	예	아니요	아니요	아니요	아니요
NSX-T Data Center 2.4.2	예	예	아니요	아니요	아니요	아니요
NSX-T Data Center 2.4.3	예	예	아니요	아니요	아니요	아니요

지원되는 ESXi 버전	ESXi 67ep6	ESXi 67u2	ESXi 67u3	ESXi 67ep7	ESXi 67ep15	ESXi 67ep17
NSX-T Data Center 2.5	예	예	예	예	아니요	아니요
NSX-T Data Center 2.5.1	예	예	예	예	예	예

상태 비저장 호스트에 대한 사용자 지정 이미지 프로파일 생성

데이터 센터에서 참조 호스트로 준비할 호스트를 식별합니다.

참조 호스트가 처음 시작될 때 ESXi는 기본 규칙을 참조 호스트와 연결합니다. 이 절차에서는 사용자 지정 이미지 프로파일(ESXi 및 NSX VIB)을 추가하고 참조 호스트를 새 사용자 지정 이미지에 연결합니다.

NSX-T 이미지를 포함하는 이미지 프로파일을 사용하면 설치 시간이 현저하게 줄어듭니다. 동일한 사용자 지정 이미지가 상태 비저장 클러스터의 대상 호스트와 연결됩니다.

참고 또는 참조 및 대상 상태 비저장 클러스터에 ESXi 이미지 프로파일만 추가할 수 있습니다. 상태 비저장 클러스터에서 전송 노드 프로파일을 적용하면 NSX-T VIB가 다운로드됩니다. [소프트웨어 디포 추가](#)를 참조하십시오.

사전 요구 사항

Auto Deploy 서비스 및 Image Builder 서비스가 사용하도록 설정되어 있는지 확인합니다. [vSphere Auto Deploy](#)를 사용하여 호스트 재프로비저닝을 참조하십시오.

절차

- 1 NSX-T 패키지를 가져오려면 소프트웨어 디포를 생성합니다.
- 2 nsx-lcp 패키지를 다운로드합니다.
 - a <https://my.vmware.com>에 로그인합니다.
 - b [VMware NSX-T Data Center 다운로드] 페이지에서 NSX-T 버전을 선택합니다.
 - c [제품 다운로드] 페이지에서 특정 VMware ESXi 버전의 NSX-T 커널 모듈을 검색합니다.
 - d **지금 다운로드**를 클릭하여 nsx-lcp 패키지 다운로드를 시작합니다.
 - e nsx-lcp 패키지를 소프트웨어 디포로 가져옵니다.

NSX Kernel Module for VMware ESXi 6.7
파일 크기: 37.64 MB
파일 유형: zip

Download Now

Name: nsx-lcp-2.5.0.0.0.14663975-esx67.zip
릴리스 날짜: 2019-09-19
빌드 번호: 14663974

NSX Kernel Module for VMware ESXi 6.7
This package includes the required kernel modules to enable NSX on ESXi 6.7 if needed for a manual installation. Use esxcli to install manually or include as part of an automated deployment system of the ESXi hosts.
MD5SUM: f224a0e12fc1722ae5b5259d279bfb1
SHA1SUM: a97d3125a26a47b94ec8408acd369d42681d3027
SHA256SUM:
1ed76de6a7f22d227eb4be30a2e0aa91492a876b7b164814198de3
1eec77bc44

3 ESXi 패키지를 가져올 다른 소프트웨어 디포를 생성합니다.

vSphere Web Client는 참조 호스트에 생성된 두 개의 디포를 표시합니다.

4 이전에 가져온 ESXi 이미지 및 nsx-lcp 패키지를 복제할 사용자 지정 소프트웨어 센터를 생성합니다.

a 이전 단계에서 생성된 ESXi 소프트웨어 디포에 있는 ESXi 이미지 프로파일을 선택합니다.

b **복제**를 클릭합니다.

c [이미지 프로파일 복제] 마법사에서 생성할 사용자 지정 이미지의 이름을 입력합니다.

d 복제된 이미지(ESXi)를 사용할 수 있어야 하는 사용자 지정 소프트웨어 디포를 선택합니다.

e [소프트웨어 패키지 선택] 창에서 허용 수준을 **VMware 인증**으로 선택합니다. ESXi VIB는 미리 선택되어 있습니다.

f 패키지 목록에서 NSX-T 패키지를 식별한 후 수동으로 선택하고 **다음**을 클릭합니다.

g [완료 준비] 화면에서 세부 정보를 확인하고 **완료**를 클릭하여 ESXi 및 NSX-T 패키지를 포함하는 복제된 이미지를 사용자 지정 소프트웨어 디포에 생성합니다.

이미지 프로파일 편집

1 이름 및 세부 정보

2 소프트웨어 패키지 선택

3 완료 준비

소프트웨어 패키지 선택

수락 수준 VMware 인증됨

<input checked="" type="checkbox"/>	이름	버전	허용 수준	벤더	디포
<input checked="" type="checkbox"/>	bnxtnet	216.0.50.0-4vmw.700.1...	VMware 인증됨	VMW	esx70
<input checked="" type="checkbox"/>	bnxtroce	216.0.58.0-1vmw.700.1...	VMware 인증됨	VMW	esx70
<input checked="" type="checkbox"/>	brcmfcoe	12.0.1500.0-1vmw.700.1...	VMware 인증됨	VMW	esx70
<input checked="" type="checkbox"/>	brcmrmefc	12.4.293.2-3vmw.700.1...	VMware 인증됨	VMW	esx70
<input checked="" type="checkbox"/>	cpu-microcode	7.0.0-1.0.15735143	VMware 인증됨	VMware	esx70
<input checked="" type="checkbox"/>	crx	7.0.0-1.0.15735143	VMware 인증됨	VMware	esx70
<input checked="" type="checkbox"/>	elx-esx-ilbelixima...	12.0.1200.0-2vmw.700...	VMware 인증됨	VMware	esx70
<input checked="" type="checkbox"/>	elxiscsi	12.0.1200.0-1vmw.700.1...	VMware 인증됨	VMW	esx70
<input checked="" type="checkbox"/>	elxnet	12.0.1250.0-5vmw.700...	VMware 인증됨	VMW	esx70
<input checked="" type="checkbox"/>	esx-base	7.0.0-1.0.15735143	VMware 인증됨	VMware	esx70
<input checked="" type="checkbox"/>	esx-dvfilter-gene...	7.0.0-1.0.15735143	VMware 인증됨	VMware	esx70
<input checked="" type="checkbox"/>	esx-ui	1.34.0-15603211	VMware 인증됨	VMware	esx70
<input checked="" type="checkbox"/>	esx-update	7.0.0-1.0.15735143	VMware 인증됨	VMware	esx70
<input checked="" type="checkbox"/>	esx-xserver	7.0.0-1.0.15735143	VMware 인증됨	VMware	esx70
<input checked="" type="checkbox"/>	i40en	1.8.1.16-1vmw.700.1.0.15...	VMware 인증됨	VMW	esx70
<input checked="" type="checkbox"/>	i40iwn	1.1.2.5-1vmw.700.1.0.157...	VMware 인증됨	VMW	esx70

98개 항목 중 98개 선택됨

취소 뒤로 다음

다음에 수행할 작업

사용자 지정 이미지를 참조 및 대상 호스트와 연결합니다. [사용자 지정 이미지를 참조 및 대상 호스트와 연결](#) 항목을 참조하십시오.

사용자 지정 이미지를 참조 및 대상 호스트와 연결

ESXi 및 NSX 패키지가 포함된 새 사용자 지정 이미지를 사용하여 참조 호스트 및 대상 호스트를 시작하려면 사용자 지정 이미지 프로파일을 연결합니다.

절차의 이 시점에서 사용자 지정 이미지는 참조 및 대상 호스트에 연결되고, NSX 설치의 수행되지 않습니다.

중요 참조 및 대상 호스트 모두에서 이 사용자 지정 이미지 연결 절차를 수행합니다.

사전 요구 사항

절차

- 1 ESXi 호스트에서 **메뉴 > 자동 배포 > 배포된 호스트**로 이동합니다.
- 2 사용자 지정 이미지 프로파일을 호스트에 연결하려면 사용자 지정 이미지를 선택합니다.
- 3 **이미지 프로파일 연결 편집**을 클릭합니다.
- 4 이미지 프로파일 연결 편집 마법사에서 **찾아보기**를 클릭하고 사용자 지정 디포를 선택한 후 사용자 지정 이미지 프로파일을 선택합니다.
- 5 **이미지 프로파일 서명 확인 건너뛰기**를 사용하도록 설정합니다.
- 6 **확인**을 클릭합니다.



결과

다음에 수행할 작업

참조 호스트에서 네트워크 구성을 설정합니다. [참조 호스트에서 네트워크 구성 설정](#) 항목을 참조하십시오.

참조 호스트에서 네트워크 구성 설정

참조 호스트에서는 ESXi에서 네트워크 구성을 설정하기 위해 VMkernel 어댑터가 있는 표준 스위치가 생성됩니다.

이 네트워크 구성은 참조 호스트에서 추출된 호스트 프로파일에 캡처됩니다. 상태 비저장 배포 중에 호스트 프로파일은 각 대상 호스트에 이 네트워크 구성 설정을 복제합니다.

절차

- 1 ESXi 호스트에서 VMkernel 어댑터를 추가하여 VSS(vSphere Standard 스위치) 또는 DVS(분산 가상 스위치)를 구성합니다.

2 [VMkernel 어댑터] 페이지에 새로 추가된 VSS/DVS 스위치가 표시되는지 확인합니다.

디바이스	네트워크 레이블	스위치	IP 주소	TCP/IP 스택	vNIC
vmk0	Management N...	vSwitch0	10.192.193.193	기본값	시
vmk1	VMkernel	vSwitch2	192.163.242.185	기본값	시

다음에 수행할 작업

참조 호스트를 NSX-T의 전송 노드로 구성합니다. [참조 호스트를 NSX-T의 전송 노드로 구성](#) 항목을 참조하십시오.

참조 호스트를 NSX-T의 전송 노드로 구성

참조 호스트가 사용자 지정 이미지 프로파일에 연결되고 VSS 스위치로 구성된 후에는 참조 호스트를 NSX-T의 전송 노드로 설정합니다.

절차

- 1 브라우저에서 https://<NSXManager_IPAddress>의 NSX-T에 로그인합니다.
- 2 참조 호스트를 찾으려면 **시스템 -> 노드 -> 호스트 전송 노드**로 이동하십시오.
- 3 VLAN 전송 영역을 생성하여 가상 네트워크의 범위를 정의합니다. 범위는 전송 영역에 N-VDS 스위치를 연결하여 정의됩니다. 이 첨부 기준, N-VDS는 전송 영역 내에 정의된 세그먼트에 액세스할 수 있습니다. [전송 영역 생성](#)을 참조하십시오.
- 4 전송 영역에 VLAN 세그먼트를 생성합니다. 생성된 세그먼트는 논리적 스위치로 표시됩니다.
 - a **네트워킹 -> 세그먼트**로 이동합니다.
 - b 세그먼트를 연결할 전송 영역을 선택합니다.
 - c VLAN ID를 입력합니다.
 - d **저장**을 클릭합니다.

세그먼트 이름	연결된 게이트웨이 및 유형	서브넷	상태
Segment_autodeploy	없음 - 유연함		● 실행 중

- 5 N-VDS가 물리적 네트워크에 연결하는 방법을 정의하는 참조 호스트에 대한 업링크 프로파일을 생성합니다. [업링크 프로파일 생성](#)을 참조하십시오.

[업링크 프로파일](#) [NIOC 프로파일](#) [Edge 클러스터 프로파일](#) [Edge 브리지 프로파일](#) [구성](#) [전송 노드 프로파일](#)

+ 추가 편집 삭제 작업 ▾

<input type="checkbox"/>	업링크 프로파일	ID	팀 구성 정책	액티브 업링크	대기 업링크	전송 VLAN	MTU
<input checked="" type="checkbox"/>	Edgenodeprofile	d017...cf3b	페일오버 순서	activeuplinkedge		0	1600 (글로벌 MTU)
<input type="checkbox"/>	hostnodeprofile	1219...46fb	페일오버 순서	activeuplinkhost	standbyuplink	0	1600 (글로벌 MTU)

- 6 참조 호스트를 전송 노드로 구성합니다. [관리 호스트 전송 노드 구성](#)을 참조하십시오.
- [호스트 전송 노드] 페이지에서 참조 호스트를 선택합니다.
 - [NSX 구성]을 클릭하고 이전에 생성된 전송 영역, N-VDS, 업링크 프로파일을 선택합니다.

1 호스트 세부 정보
2 NSX 구성

전송 영역 *
tz

N-VDS 생성 *

● 생성된 NSX
○ 사전 구성

+ N-VDS 추가

새 노드 스위치

N-VDS 이름 *
vds-1

연결된 전송 영역
tz

NIOC 프로파일 *
nsx-default-nioc-hostswitch-profile

업링크 프로파일 *
nsx-default-uplink-hostswitch-profile

LLDP 프로파일 *
LLDP [Send Packet Enabled]

취소
이전
완료

VMware, Inc.

204

- 7 [설치를 위한 네트워크 매핑] 섹션에서 **매핑 추가**를 클릭하여 VMkernel을 세그먼트/논리적 스위치 매핑에 추가합니다.

설치를 위한 네트워크 매핑

X

vmnic0 및 vmk0이 마이그레이션되면 호스트 연결이 끊어질 수 있습니다.

상태 저장 호스트(독립 실행형 또는 클러스터형)에 대한 논리적 스위치를 변경해도 영향을 주지 않으며 작업이 실패합니다.

+ 추가 삭제

<input checked="" type="checkbox"/> VMkernel 어댑터 *	VLAN 세그먼트/논리적 스위치 *
<input checked="" type="checkbox"/> vmk0	segment-autodeploy

- 8 참조 호스트에서 **완료**를 클릭하여 NSX-T 설치를 시작합니다.

설치하는 동안 VMkernel 어댑터 및 물리적 NIC가 VSS 또는 DVS 스위치에서 N-VDS 스위치로 마이그레이션됩니다. 설치 후 참조 호스트의 구성 상태가 성공으로 표시됩니다.

참고 참조 호스트는 다른 호스트 아래에 나열됩니다.

호스트 전송 노드 Edge 전송 노드 Edge 클러스터 ESXi 브리지 클러스터

관리자 vc

NSX 구성 NSX 제거 작업

보기 모두

<input type="checkbox"/>	노드	ID	IP 주소	OS 유형	NSX 구성	구성 상태	노드 상태	터널	전송 영역	NSX 버전	N-VDS
<input type="checkbox"/>	Other Hosts (2) MoRef L...		1개 호스트 성능...								
<input checked="" type="checkbox"/>	hostnode	6d4c...f...	10.160.169.8...	ESXi 6.7.0	구성됨	성공	실행 중 ①	↑ 1	tz	2.5.0.0.0.14...	1
<input type="checkbox"/>	10.192.193.193	42ea...8...	10.192.193.1...	ESXi 6.7.0	구성됨	성공	성능 저하됨 ①	사용함 ...	tz	2.5.0.0.0.14...	1

- 9 vCenter Server에서 VSS 스위치의 PNIC 및 VMkernel 어댑터가 N-VDS 스위치에 마이그레이션 및 연결되었는지 확인합니다.

VMkernel 어댑터					
네트워크 추가... 새로 고침 편집... X 제거					
디바이스	네트워크 레이블	스위치	IP 주소	TCP/IP 스택	
vmk0	Management Network	vSwitch0	10.160.169.87	기본값	
vmk1	Segment_autodeploy	vds-1	169.254.171.95	기본값	

다음에 수행할 작업

호스트 프로파일을 추출하고 확인합니다. [호스트 프로파일 추출 및 확인](#) 항목을 참조하십시오.

호스트 프로파일 추출 및 확인

참조 호스트에서 호스트 프로파일을 추출한 후 호스트 프로파일에서 추출된 NSX-T 구성을 확인합니다. 이 구성은 대상 호스트에 적용되는 ESXi 및 NSX-T 구성으로 이루어집니다.

절차

- 1 호스트 프로파일을 추출하려면 참조 호스트에서 호스트 프로파일을 추출하고 구성합니다.
- 2 추출된 호스트 프로파일에서 NSX 구성을 확인합니다.

검색하기
모두

Q 필터

- > 고급 구성 설정
- > 기타
- ✓ 네트워킹 구성
 - > 표준 스위치
 - > 가상 시스템 포트 그룹
 - > 호스트 포트 그룹
 - > 물리적 NIC 구성

vSphere Distributed Switch

호스트 가상 NIC
 - ✓ NSX 호스트 vNIC:

NSX 호스트 vNIC : Segment_autodeploy
 - > Netstack 인스턴스

네트워킹 코어 덤프 설정
- > 보안 및 서비스
- > 스토리지 구성
- > 일반 시스템 설정

NSX 호스트 vNIC : Segment_autodeploy

이 가상 NIC를 연결할 LogicSwitch 결정

LogicSwitch 연결 대상을 선택하십시오.

*LogicSwitch 이름	Segment_autodeploy
-----------------	--------------------

LogicSwitch의 가상 NIC 생성 시기 결정

항상 개체 생성

LogicSwitch의 가상 NIC의 상태 비저장 부팅 속성

상태 비저장 부팅 구성 매개 변수(변경 전에 설명서 참조)

*VLAN(변경 전에 설명서 참조)	0
*팀 구성 정책(변경 전에 설명서 참조)	first uplink
사용된 출성 업링크(변경 전에 설명서 참조)	vmnic1
사용된 대기 업링크(변경 전 설명서 참조)	--
*사용된 OpaqueSwitch 이름(변경 전 설명서 참조)	vds-1

사용 가능한 서비스

vmknic의 MAC 주소 결정 방법 확인

기본값을 사용할 수 없는 경우 사용자에게 **MAC** 주소 확인

VMkernel 네트워크 어댑터 이름 정책

인터페이스 이름 할당됨

VMkernel 네트워크 어댑터	vmk1
-------------------	------

MTU 정책

지정된 MTU 할당

*MTU	1500
------	------

TCP/IP 스택:

vmknic가 연결된 Netstack 인스턴스

*이름	defaultTcpipStack
-----	-------------------

결과

호스트가 두 환경 모두에 대해 준비되었으므로 호스트 프로파일에는 ESXi 및 NSX와 관련된 구성이 포함됩니다.

다음에 수행할 작업

상태 비저장 클러스터와 호스트 프로파일 간의 연결을 확인합니다. **상태 비저장 클러스터와 호스트 프로파일 간의 연결 확인** 항목을 참조하십시오.

상태 비저장 클러스터와 호스트 프로파일 간의 연결 확인

ESXi 및 NSX 구성을 사용하여 대상 상태 비저장 클러스터를 준비하려면 참조 호스트에서 추출된 호스트 프로파일을 대상 상태 비저장 클러스터에 연결합니다.

상태 비저장 클러스터에 연결된 호스트 프로파일이 없으면 클러스터에 가입하는 새 노드를 ESXi 및 NSX VIB를 통해 자동으로 배포할 수 없습니다.

절차

- 1 호스트 프로파일을 상태 비저장 클러스터에 연결하거나 클러스터에서 분리합니다. [호스트 프로파일에 엔터티 연결 또는 분리](#)를 참조하십시오.
- 2 [배포된 호스트] 탭에서 기존 상태 비저장 호스트가 올바른 이미지와 연결되어 있고 호스트 프로파일에 연결되어 있는지 확인합니다.
- 3 호스트 프로파일 연결이 누락된 경우 대상 호스트를 선택하고 [호스트 연결에 업데이트 적용]을 클릭하여 이미지 및 호스트 프로파일을 대상 호스트로 강제로 업데이트합니다.

소프트웨어 디포	배포 규칙	배포된 호스트	검색된 호스트	스크립트 번들	구성
① Auto Deploy가 호스트에 연결한 위치, 호스트 프로파일 및 이미지 프로파일이 아래에 나열되어 있습니다. 연결은 호스트의 실제 상태와 다를 수 있습니다.					
호스트 연결 규정 준수 검사 호스트 연결에 업데이트 적용 이미지 프로파일 연결 편집					
<input type="checkbox"/>	호스트	연결된 이미지 프로파일	연결된 호스트 프로파일	연결된 위치	연결된 스크립트 번들
<input type="checkbox"/>	10.144.139.147	CustomDepot(ESXi and NSX)		1-datacenter-1964	
<input type="checkbox"/>	10.144.137.225	CustomDepot(ESXi and NSX)	Host Profile_ReferenceHost	Statless-Cluster	

다음에 수행할 작업

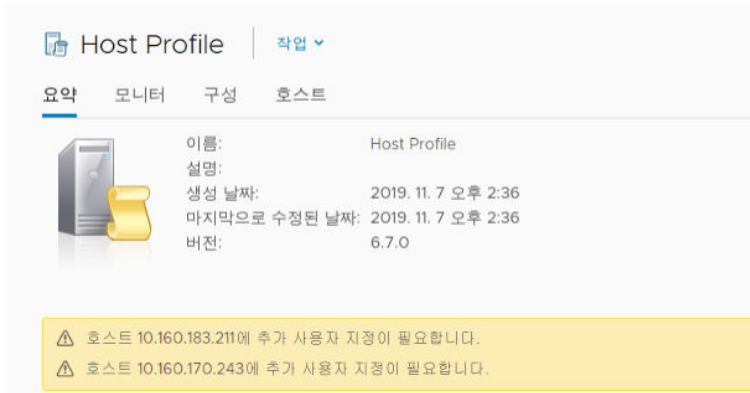
호스트 사용자 지정 업데이트. [호스트 사용자 지정 업데이트](#) 항목을 참조하십시오.

호스트 사용자 지정 업데이트

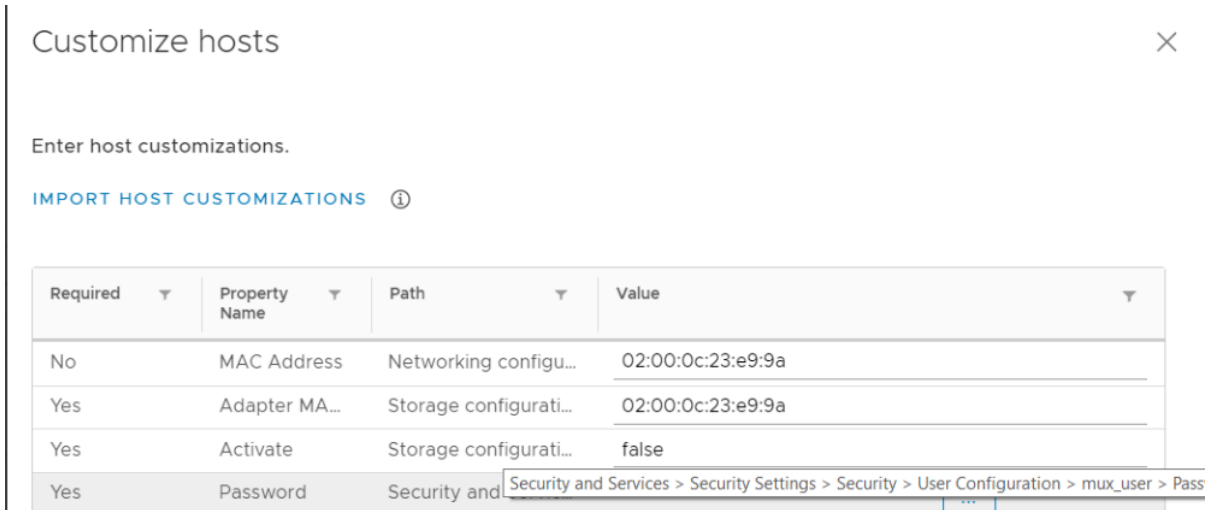
호스트 프로파일을 대상 클러스터에 연결하고 나면 호스트에 추가 사용자 지정 항목이 있어야 ESXi 및 NSX-T 패키지를 자동으로 배포할 수 있습니다.

절차

- 1 호스트 프로파일을 대상 클러스터에 연결한 후 호스트를 사용자 지정 값으로 업데이트하지 않으면 시스템에서 다음 메시지가 표시됩니다.



- 2 호스트 사용자 지정을 업데이트하려면 호스트 프로파일로 이동하고 **작업 -> 호스트 사용자 지정 편집**을 클릭합니다.
- 3 ESXi 버전 67ep6, 67ep7, 67u2의 경우 MUX 사용자 암호를 입력합니다.



- 4 모든 필수 필드가 적절한 값으로 업데이트되었는지 확인합니다.

다음에 수행할 작업

대상 호스트에서 자동 배포를 트리거합니다. [대상 호스트에서 자동 배포 트리거](#) 항목을 참조하십시오.

대상 호스트에서 자동 배포 트리거

새 노드가 클러스터에 추가되면 구성할 ESXi 및 NSX-T VIB에 대해 수동으로 재부팅해야 합니다.

참고 상태 비저장 호스트에만 적용됩니다.

호스트에서 구성할 ESXi 및 NSX-T VIB의 자동 배포를 트리거하도록 준비하는 방법에는 두 가지가 있습니다.

- 상태 비저장 클러스터에 TNP를 적용하기 전에 호스트를 재부팅합니다.
- 상태 비저장 클러스터에 TNP를 적용한 후에 호스트를 재부팅합니다.

호스트에 NSX를 설치할 때 VMkernel 어댑터를 마이그레이션하려면 다음을 참조하십시오.

- 상태 비저장 호스트가 대상 클러스터 내부에 있는 시나리오
- 상태 비저장 호스트가 대상 클러스터 외부에 있는 시나리오

다음에 수행할 작업

상태 비저장 클러스터에 TNP를 적용하기 전에 호스트를 재부팅합니다. [TNP를 적용하기 전에 호스트 재부팅](#) 항목을 참조하십시오.

TNP를 적용하기 전에 호스트 재부팅

상태 비저장 호스트에만 적용됩니다. 이 시나리오에서는 전송 노드 프로파일이 상태 비저장 클러스터에 적용되지 않으며, 이것은 대상 호스트에 NSX-T가 설치 및 구성되지 않았음을 의미합니다.

절차

1 호스트를 재부팅합니다.

대상 호스트는 ESXi 이미지로 시작합니다. 시작한 후 대상 호스트는 TNP 프로파일이 대상 호스트에 적용되고 NSX-T 설치가 완료될 때까지 유지 보수 모드를 유지합니다. 프로파일은 다음 순서로 호스트에 적용됩니다.

프로파일은 다음 순서로 호스트에 적용됩니다.

- 이미지 프로파일이 호스트에 적용됩니다.
- 호스트 프로파일 구성이 호스트에 적용됩니다.
- NSX-T 구성이 호스트에 적용됩니다.

2 호스트가 아직 전송 노드가 아니기 때문에 ESXi 호스트에서 VMkernel 어댑터가 <N-LogicalSegment>라는 임시 세그먼트에 연결됩니다. NSX-T가 설치된 후 임시 스위치가 실제 N-VDS 스위치 및 논리적 세그먼트로 바뀝니다.

요약 모니터 구성 사용 권한 VM 데이터스토어 네트워크					
VMkernel 어댑터					
네트워킹 추가... 새로 고침 편집... X 제거					
디바이스	네트워크 레이블	스위치	IP 주소	TCP/IP 스택	
vmk0	Management Network	vSwitch0	10.160.169.87	기본값	
vmk1	Segment_autodeploy	vds-1	169.254.171.95	기본값	

ESXi VIB가 재부팅된 모든 호스트에 적용됩니다. ESXi 호스트의 임시 NSX 스위치. 호스트에 TNP가 적용되면 임시 스위치가 실제 NSX-T 스위치로 교체됩니다.

다음에 수행할 작업

상태 비저장 클러스터에 TNP를 적용합니다. [상태 비저장 클러스터에 TNP 적용](#) 항목을 참조하십시오.

상태 비저장 클러스터에 TNP 적용

클러스터에 TNP가 적용된 경우 대상 호스트에서만 NSX-T 구성 및 설치가 수행됩니다.

절차

- 1 참조 호스트에서 호스트 프로파일로 추출된 설정을 기록해 둡니다. TNP 프로파일의 해당 엔티티는 값이 동일해야 합니다. 예를 들어, 호스트 프로파일 및 TNP에서 사용되는 N-VDS 이름은 동일해야 합니다.

추출된 호스트 프로파일 설정에 대한 자세한 내용은 [호스트 프로파일 추출 및 확인](#)을 참조하십시오.

- 2 TNP를 추가합니다. [전송 노드 프로파일 추가](#)를 참조하십시오.
- 3 다음 매개 변수의 값이 새 TNP 프로파일과 기존 호스트 프로파일 둘 다에서 동일한지 확인합니다.
 - N-VDS 이름: 호스트 프로파일에서 참조되는 N-VDS 이름과 TNP가 동일한지 확인합니다.
 - 업링크 프로파일: 호스트 프로파일에서 참조되는 업링크 프로파일 및 TNP가 동일한지 확인합니다.
 - PNIC: 물리적 NIC를 업링크 프로파일에 매핑할 경우 먼저 호스트 프로파일에 사용된 NIC를 확인하고 해당 물리적 NIC를 업링크 프로파일에 매핑합니다.
 - 설치를 위한 네트워크 매핑: 설치하는 동안 네트워크를 매핑하는 경우 먼저 호스트 프로파일의 VMkernel-세그먼트 매핑을 확인하고 TNP에서 동일한 매핑을 추가합니다.
 - 제거를 위한 네트워크 매핑: 제거하는 동안 네트워크를 매핑하는 경우 먼저 호스트 프로파일의 VMkernel-VSS/DVS 스위치 매핑을 확인하고 TNP에서 동일한 매핑을 추가합니다.

- 4 모든 필수 필드를 입력하여 TNP를 추가합니다. [전송 노드 프로파일 추가](#)를 참조하십시오.

다음 매개 변수의 값이 새 TNP 프로파일과 기존 호스트 프로파일 둘 다에서 동일한지 확인합니다.

- 전송 영역: 호스트 프로파일에서 참조되는 전송 영역 및 TNP가 동일한지 확인합니다.
- N-VDS 이름: 호스트 프로파일에서 참조되는 N-VDS 이름과 TNP가 동일한지 확인합니다.
- 업링크 프로파일: 호스트 프로파일에서 참조되는 업링크 프로파일 및 TNP가 동일한지 확인합니다.
- PNIC: 물리적 NIC를 업링크 프로파일에 매핑할 경우 먼저 호스트 프로파일에 사용된 NIC를 확인하고 해당 물리적 NIC를 업링크 프로파일에 매핑합니다.
- 설치를 위한 네트워크 매핑: 설치하는 동안 네트워크를 매핑하는 경우 먼저 호스트 프로파일의 VMkernel-논리적 스위치 매핑을 확인하고 TNP에서 동일한 매핑을 추가합니다.

- 제거를 위한 네트워크 매핑: 제거하는 동안 네트워크를 매핑하는 경우 먼저 호스트 프로파일의 VMkernel-VSS/DVS 스위치 매핑을 확인하고 TNP에서 동일한 매핑을 추가합니다.

N-VDS 이름 *

vds-tzvian

연결된 전송 영역

tz-33

NIOC 프로파일 *

nsx-default-nioc-hostswitch-profile

또는 새 NIOC 프로파일 생성

업링크 프로파일 *

nsx-default-uplink-hostswitch-profile

또는 새 업링크 프로파일 생성

LLDP 프로파일 *

LLDP [Send Packet Enabled]

IP 할당 *

물리적 NIC

vmnic1

uplink-1

물리적 NIC 전용 마이그레이션

☐ 아니요

물리적 NIC에 마이그레이션용으로 선택한 vmk가 없는 경우 이 옵션을 사용하도록 설정합니다.

물리적 NIC 추가

설치를 위한 네트워크 매핑

1 매핑

제거를 위한 네트워크 매핑

매핑 추가

대상 노드에 TNP를 적용한 후 TNP 구성이 호스트 프로파일 구성과 일치하지 않으면 규정 준수 오류로 인해 노드가 작동하지 않을 수 있습니다.

- 5 TNP 프로파일이 성공적으로 생성되었는지 확인합니다.
- 6 대상 클러스터에 TNP 프로파일을 적용하고 **저장**을 클릭합니다.

NSX 구성



NSX가 전송 노드 프로파일에 정의된 배포 구성을 사용하여 선택한 클러스터에 설치됩니다.

배포 프로파일 선택 * TNP_StatelessCluster

새 전송 노드 프로파일 생성

취소

저장

- 7 TNP 프로파일이 대상 클러스터에 성공적으로 적용되었는지 확인합니다. 이는 클러스터의 모든 노드에서 NSX가 구성되었음을 의미합니다.
- 8 vSphere에서 물리적 NIC 또는 VMkernel 어댑터가 N- VDS 스위치에 연결되어 있는지 확인합니다.

VMkernel 어댑터

네트워크 추가... 새로 고침 | 편집... X 제거

디바이스	네트워크 레이블	스위치	IP 주소	TCP/IP 스택
vmk0	Management Network	vSwitch0	10.160.169.87	기본값
vmk1	Segment_autodeploy	vds-1	169.254.171.95	기본값

- 9 NSX에서 ESXi 호스트가 전송 노드로 성공적으로 구성되었는지 확인합니다.

다음에 수행할 작업

또는 클러스터에 TNP를 적용한 후 대상 호스트를 재부팅할 수 있습니다. [TNP를 적용한 후에 호스트 재부팅](#) 항목을 참조하십시오.

TNP를 적용한 후에 호스트 재부팅

상태 비저장 호스트에만 적용됩니다. 새 노드가 클러스터에 추가되면 구성할 ESXi 및 NSX-T 패키지에 대한 노드를 수동으로 재부팅합니다.

절차

- 1 호스트 프로파일로 이미 준비한 상태 비저장 클러스터에 TNP를 적용합니다. [TNP 생성 및 상태 비저장 클러스터에 적용](#)을 참조하십시오.
- 2 호스트를 재부팅합니다.

상태 비저장 클러스터에 TNP 프로파일을 적용한 후 클러스터에 가입하는 새 노드를 재부팅하면 해당 노드가 자동으로 호스트에서 NSX-T로 구성됩니다.

다음에 수행할 작업

클러스터에 가입하는 새 노드를 재부팅하여 재부팅된 노드에서 ESXi 및 NSX-T를 자동으로 배포하고 구성하도록 해야 합니다.

자동 배포를 구성할 때 호스트 프로파일 및 전송 노드 프로파일 관련 문제를 해결하려면 [호스트 프로파일 및 전송 노드 프로파일 문제 해결](#)을 참조하십시오.

상태 비저장 호스트가 대상 클러스터 내부에 있는 시나리오

이 섹션에서는 상태 비저장 호스트가 대상 클러스터 내부에 있는 사용 사례에 대해 설명합니다.

중요 상태 비저장 대상 호스트에서:

- vmk0 어댑터를 VSS/DVS에서 N-VDS로 마이그레이션하는 것은 NSX-T 2.4 및 NSX-T 2.4.1에서 지원되지 않습니다.
- vmk0 어댑터를 VSS/DVS에서 N-VDS로 마이그레이션하는 것은 NSX-T 2.5에서 지원됩니다.

대상 호스트	참조 호스트 구성	대상 호스트 자동 배포 단계
대상 호스트에는 vmk0 어댑터가 구성되어 있습니다.	참조 호스트에서 추출된 호스트 프로파일의 N-VDS 스위치에 vmk0이 구성되어 있습니다. NSX-T에서 TNP에는 vmk0 마이그레이션 매핑만 구성되어 있습니다.	<ol style="list-style-type: none"> 1 호스트 프로파일을 대상 호스트에 연결합니다. vmk0 어댑터가 vSwitch에 연결됩니다. 2 필요한 경우 호스트 사용자 지정을 업데이트합니다. 3 호스트를 재부팅합니다. 호스트 프로파일이 호스트에 적용됩니다. vmk0이 임시 스위치에 연결됩니다. 4 TNP를 적용합니다. vmk0 어댑터가 N-VDS로 마이그레이션됩니다. 대상 호스트가 ESXi 및 NSX-T VIB와 함께 성공적으로 배포되었습니다.
대상 호스트에는 vmk0 어댑터가 구성되어 있습니다.	참조 호스트에서 추출된 호스트 프로파일의 vSwitch에는 vmk0이, N-VDS 스위치에는 vmk1이 구성되어 있습니다. NSX-T에서 TNP에는 vmk1 마이그레이션 매핑만 구성되어 있습니다.	<ol style="list-style-type: none"> 1 호스트 프로파일을 대상 호스트에 연결합니다. vmk0 어댑터는 vSwitch에 연결되지만 vmk1은 어떤 스위치에서도 인식되지 않습니다. 2 필요한 경우 호스트 사용자 지정을 업데이트합니다. 3 호스트를 재부팅합니다. vmk0은 vSwitch에 연결되고 vmk1은 임시 NSX 스위치에 연결됩니다. 4 TNP를 적용합니다. vmk1 어댑터가 N-VDS로 마이그레이션됩니다. 5 (옵션) 호스트가 호스트 프로파일을 준수하지 않는 상태를 유지하면 호스트를 다시 부팅하여 준수 상태로 만듭니다. 대상 호스트가 ESXi 및 NSX-T VIB와 함께 성공적으로 배포되었습니다.

대상 호스트	참조 호스트 구성	대상 호스트 자동 배포 단계
대상 호스트에는 vmk0 어댑터가 구성되어 있습니다.	참조 호스트에서 추출된 호스트 프로파일의 vSwitch에는 vmk0이, N-VDS 스위치에는 vmk1이 구성되어 있습니다. NSX-T에서 TNP에는 vmk0 및 vmk1 마이그레이션 매핑이 구성되어 있습니다.	<ol style="list-style-type: none"> 1 호스트 프로파일을 대상 호스트에 연결합니다. vmk0 어댑터는 vSwitch에 연결되지만 vmk1은 어떤 스위치에서도 인식되지 않습니다. 2 필요한 경우 호스트 사용자 지정을 업데이트합니다. 3 호스트를 재부팅합니다. vmk0 어댑터는 vSwitch에 연결되고 vmk1은 임시 NSX 스위치에 연결됩니다. 4 TNP를 적용합니다. 5 (옵션) 호스트가 호스트 프로파일을 준수하지 않는 상태를 유지하면 호스트를 다시 부팅하여 준수 상태로 만듭니다. <p>대상 호스트가 ESXi 및 NSX-T VIB와 함께 성공적으로 배포되었습니다.</p>
대상 호스트에 vmk0 및 vmk1 어댑터가 구성되어 있습니다.	참조 호스트에서 추출된 호스트 프로파일의 vSwitch에는 vmk0이, N-VDS 스위치에는 vmk1이 구성되어 있습니다. NSX-T에서 TNP에는 vmk1 마이그레이션 매핑이 구성되어 있습니다.	<ol style="list-style-type: none"> 1 호스트 프로파일을 대상 호스트에 연결합니다. vmk0 및 vmk1 어댑터는 vSwitch에 연결됩니다. 2 필요한 경우 호스트 사용자 지정을 업데이트합니다. 3 호스트를 재부팅합니다. 4 TNP를 적용합니다. vmk0 어댑터는 vSwitch에 연결되고 vmk1은 N-VDS 스위치에 연결됩니다. 5 (옵션) 호스트가 호스트 프로파일을 준수하지 않는 상태를 유지하면 호스트를 다시 부팅하여 준수 상태로 만듭니다. <p>대상 호스트가 ESXi 및 NSX-T VIB와 함께 성공적으로 배포되었습니다.</p>
대상 호스트에 vmk0 및 vmk1 어댑터가 구성되어 있습니다.	참조 호스트에서 추출된 호스트 프로파일의 N-VDS 스위치에는 vmk0 및 vmk1이 구성되어 있습니다. NSX-T에서 TNP에는 vmk0 및 vmk1 마이그레이션 매핑이 구성되어 있습니다.	<ol style="list-style-type: none"> 1 호스트 프로파일을 대상 호스트에 연결합니다. vmk0 및 vmk1 어댑터는 vSwitch에 연결됩니다. 2 필요한 경우 호스트 사용자 지정을 업데이트합니다. 3 호스트를 재부팅합니다. 4 TNP를 적용합니다. vmk0 및 vmk1은 N-VDS 스위치에 마이그레이션됩니다. <p>대상 호스트가 ESXi 및 NSX-T VIB와 함께 성공적으로 배포되었습니다.</p>

상태 비저장 호스트가 대상 클러스터 외부에 있는 시나리오

이 섹션에서는 상태 비저장 호스트가 대상 클러스터 외부에 있는 사용 사례에 대해 설명합니다.

중요 상태 비저장 호스트에서:

- vmk0 어댑터를 VSS/DVS에서 N-VDS로 마이그레이션하는 것은 NSX-T 2.4 및 NSX-T 2.4.1에서 지원되지 않습니다.
- vmk0 어댑터를 VSS/DVS에서 N-VDS로 마이그레이션하는 것은 NSX-T 2.5에서 지원됩니다.

대상 호스트 상태	참조 호스트 구성	대상 호스트 자동 배포 단계
<p>호스트가 전원이 꺼진 상태입니다 (첫 번째 시작). 나중에 클러스터에 추가됩니다.</p> <p>기본 Auto Deploy 규칙은 대상 클러스터에 대해 구성되고 호스트 프로파일에 연결됩니다.</p> <p>TNP이 클러스터에 적용됩니다.</p>	<p>참조 호스트에서 추출된 호스트 프로파일의 vSwitch에는 VMkernel 어댑터 0(vmk0)이 구성되어 있고, N-VDS 스위치에는 VMkernel 어댑터 1(vmk1)이 구성되어 있습니다.</p> <p>NSX-T에서 TNP에는 vmk1 마이그레이션 매핑만 구성되어 있습니다.</p>	<p>1 호스트 전원을 켭니다.</p> <p>호스트 전원을 켜 후</p> <ul style="list-style-type: none"> ■ 호스트가 클러스터에 추가됩니다. ■ 호스트 프로파일이 대상 호스트에 적용됩니다. ■ vmk0 어댑터는 vSwitch에 있고 vmk1 어댑터는 임시 스위치에 있습니다. ■ TNP가 트리거됩니다. ■ 클러스터에 TNP가 적용된 후 vmk0 어댑터가 vSwitch에 있고 vmk1이 N-VDS 스위치로 마이그레이션됩니다. <p>2 (옵션) 호스트가 호스트 프로파일을 준수하지 않는 상태를 유지하면 호스트를 다시 부팅하여 준수 상태로 만듭니다.</p> <p>호스트가 ESXi 및 NSX-T VIB와 함께 성공적으로 배포되었습니다.</p>
<p>호스트가 전원이 꺼진 상태입니다 (첫 번째 시작). 나중에 클러스터에 추가됩니다.</p> <p>기본 Auto Deploy 규칙은 대상 클러스터에 대해 구성되고 호스트 프로파일에 연결됩니다.</p> <p>TNP이 클러스터에 적용됩니다.</p>	<p>참조 호스트에서 추출된 호스트 프로파일의 N-VDS 스위치에는 VMkernel 어댑터 0(vmk0) 및 VMkernel 어댑터 1(vmk1)이 구성되어 있습니다.</p> <p>NSX-T에서 TNP에는 vmk0 및 vmk1 마이그레이션이 구성되어 있습니다.</p>	<p>1 호스트 전원을 켭니다.</p> <p>호스트 전원을 켜 후</p> <ul style="list-style-type: none"> ■ 호스트가 클러스터에 추가됩니다. ■ 호스트 프로파일이 대상 호스트에 적용됩니다. ■ vmk0 및 vmk1 어댑터는 임시 스위치에 있습니다. ■ TNP가 트리거됩니다. ■ 클러스터에 TNP가 적용된 후 vmk0 및 vmk1이 N-VDS 스위치로 마이그레이션됩니다. <p>호스트가 ESXi 및 NSX-T VIB와 함께 성공적으로 배포되었습니다.</p>

대상 호스트 상태	참조 호스트 구성	대상 호스트 자동 배포 단계
<p>호스트가 전원이 켜진 상태입니다. 나중에 클러스터에 추가됩니다.</p> <p>기본 Auto Deploy 규칙은 대상 클러스터에 대해 구성되고 호스트 프로파일에 연결됩니다.</p> <p>대상 호스트에는 vmkO 어댑터만 구성되어 있습니다.</p>	<p>참조 호스트에서 추출된 호스트 프로파일의 vSwitch에는 VMkernel 어댑터 O(vmkO)이 구성되어 있고, N-VDS 스위치에는 VMkernel 어댑터 1(vmk1)이 구성되어 있습니다.</p> <p>NSX-T에서 TNP에는 vmk1 마이그레이션 매핑이 구성되어 있습니다.</p>	<ol style="list-style-type: none"> 1 호스트를 클러스터의 일부가 되도록 이동합니다. 2 호스트를 재부팅합니다. <p>호스트가 재부팅되면 호스트 프로파일이 대상 호스트에 적용됩니다.</p> <ul style="list-style-type: none"> ■ vmkO 어댑터는 vSwitch에 연결되지만 vmk1 어댑터는 임시 NSX 스위치에 연결됩니다. ■ TNP가 트리거됩니다. ■ vmk1은 N-VDS 스위치로 마이그레이션됩니다. <ol style="list-style-type: none"> 3 (옵션) 호스트가 호스트 프로파일을 준수하지 않는 상태를 유지하면 호스트를 다시 부팅하여 준수 상태로 만듭니다. <p>호스트가 ESXi 및 NSX-T VIB와 함께 성공적으로 배포되었습니다.</p>
<p>호스트가 전원이 켜진 상태입니다. 나중에 클러스터에 추가됩니다.</p> <p>기본 Auto Deploy 규칙은 대상 클러스터에 대해 구성되고 호스트 프로파일에 연결됩니다.</p> <p>대상 호스트에는 vmkO 어댑터만 구성되어 있습니다.</p>	<p>참조 호스트에서 추출된 호스트 프로파일의 N-VDS에는 VMkernel 어댑터 O(vmkO) 및 VMkernel 어댑터 1(vmk1)이 구성되어 있습니다.</p> <p>NSX-T에서 TNP에는 vmkO 및 vmk1 마이그레이션이 구성되어 있습니다.</p>	<ol style="list-style-type: none"> 1 호스트를 클러스터의 일부가 되도록 이동합니다. 2 호스트를 재부팅합니다. <p>호스트를 재부팅하면 호스트 프로파일이 대상 호스트에 적용됩니다.</p> <ul style="list-style-type: none"> ■ vmkO 및 vmk1 어댑터는 임시 NSX 스위치에 연결됩니다. ■ TNP가 트리거됩니다. ■ vmkO 및 vmk1은 N-VDS 스위치에 연결됩니다. <p>호스트가 ESXi 및 NSX-T VIB와 함께 성공적으로 배포되었습니다.</p>

대상 호스트 상태	참조 호스트 구성	대상 호스트 자동 배포 단계
<p>호스트가 전원이 켜진 상태입니다. 나중에 클러스터에 추가됩니다.</p> <p>기본 Auto Deploy 규칙은 대상 클러스터에 대해 구성되고 호스트 프로파일에 연결됩니다.</p> <p>대상 호스트에 vmk0 및 vmk1 네트워크 매핑이 구성되어 있습니다.</p>	<p>참조 호스트에서 추출된 호스트 프로파일의 vSwitch에는 VMkernel 어댑터 0(vmk0)이 구성되어 있고, N-VDS 스위치에는 VMkernel 어댑터 1(vmk1)이 구성되어 있습니다.</p> <p>NSX-T에서 TNP에는 vmk1 마이그레이션이 구성되어 있습니다.</p>	<ol style="list-style-type: none"> 1 호스트를 클러스터의 일부가 되도록 이동합니다. 2 호스트를 재부팅합니다. <p>호스트가 재부팅되면 호스트 프로파일이 대상 호스트에 적용됩니다.</p> <ul style="list-style-type: none"> ■ vmk0 어댑터는 vSwitch에 연결되지만 vmk1 어댑터는 임시 NSX 스위치에 연결됩니다. ■ TNP가 트리거됩니다. ■ vmk1은 N-VDS 스위치로 마이그레이션됩니다. <ol style="list-style-type: none"> 3 (옵션) 호스트가 호스트 프로파일을 준수하지 않는 상태를 유지하면 호스트를 다시 부팅하여 준수 상태로 만듭니다. <p>호스트가 ESXi 및 NSX-T VIB와 함께 성공적으로 배포되었습니다.</p>
<p>호스트가 전원이 켜진 상태입니다. 나중에 클러스터에 추가됩니다.</p> <p>기본 Auto Deploy 규칙은 대상 클러스터에 대해 구성되고 호스트 프로파일에 연결됩니다.</p> <p>호스트에 vmk0 및 vmk1 네트워크 매핑이 구성되어 있습니다.</p>	<p>참조 호스트에서 호스트 프로파일의 N-VDS 스위치에 VMkernel 어댑터 0(vmk0) 및 VMkernel 어댑터 1(vmk1)이 구성되어 있습니다.</p> <p>NSX-T에서 TNP에는 vmk0 및 vmk1 마이그레이션이 구성되어 있습니다.</p>	<ol style="list-style-type: none"> 1 호스트를 클러스터의 일부가 되도록 이동합니다. 2 호스트를 재부팅합니다. <p>호스트가 재부팅되면 호스트 프로파일이 대상 호스트에 적용됩니다.</p> <ul style="list-style-type: none"> ■ vmk0 및 vmk1 어댑터는 임시 NSX 스위치에 연결됩니다. ■ TNP가 트리거됩니다. ■ vmk0 및 vmk1 어댑터는 N-VDS 스위치에 마이그레이션됩니다. <p>호스트가 ESXi 및 NSX-T VIB와 함께 성공적으로 배포되었습니다.</p>

호스트 프로파일 및 전송 노드 프로파일 문제 해결

상태 비저장 클러스터를 자동 배포하는 데 사용되는 호스트 프로파일 및 TNP 관련 문제를 해결합니다.

시나리오	설명
호스트 프로파일이 이식 가능하지 않습니다.	<p>문제: vCenter Server가 NSX-T 구성을 포함하는 호스트 프로파일을 사용할 수 없습니다.</p> <p>해결 방법: 없음</p>
Auto Deploy 규칙 엔진	<p>문제: Auto Deploy 규칙에서 호스트 프로파일을 사용하여 새 클러스터를 배포할 수 없습니다. 새 클러스터가 배포된 경우 호스트는 기본 네트워킹을 사용하여 배포되고 유지 보수 모드를 유지합니다.</p> <p>해결 방법: NSX-T GUI에서 각 클러스터를 준비합니다. 상태 비저장 클러스터에 TNP 적용을 참조하십시오.</p>

시나리오	설명
규정 준수 오류가 있는지 확인합니다.	<p>문제: 호스트 프로파일 업데이트 적용 중에 NSX-T 구성과 관련된 규정 준수 오류를 수정할 수 없습니다.</p> <ul style="list-style-type: none"> ■ 호스트 프로파일 및 TNP에 성 된 물리적 NIC가 서로 다릅니다. ■ vNIC에서 LS 간 매핑. 호스트 프로파일이 TNP 프로파일을 사용하여 논리적 스위치-vNIC 매핑의 불일치를 확인합니다. ■ 프로파일 및 TNP에서 N-VDS에 연결된 VMkernel 불일치 ■ 호스트 프로파일 및 TNP에서 불투명한 스위치 불일치 <p>해결 방법: 호스트 프로파일 및 TNP에서 NSX-T 구성이 일치하는지 확인합니다. 호스트를 재부팅하여 구성 변경을 실현합니다. 호스트가 작동합니다.</p>
수정	<p>문제: NSX-T 관련 규정 준수 오류가 있는 경우 해당 클러스터의 호스트 프로파일 업데이트 적용이 차단됩니다.</p> <p>구성이 잘못되었습니다.</p> <ul style="list-style-type: none"> ■ vNIC에서 LS 간 매핑 ■ 물리적 NIC 매핑 <p>해결 방법: 호스트 프로파일 및 TNP에서 NSX-T 구성이 일치하는지 확인합니다. 호스트를 재부팅하여 구성 변경을 실현합니다. 호스트가 작동합니다.</p>
연결	<p>문제: NSX-T로 구성된 클러스터에서 호스트 프로파일을 호스트 수준에서 연결할 수 없습니다.</p> <p>해결 방법: 없음</p>
분리	<p>문제: NSX-T로 구성된 클러스터에서 새 호스트 프로파일을 분리했다가 연결해도 NSX-T 구성이 제거되지 않습니다. 클러스터가 새로 연결된 호스트 프로파일을 준수하더라도, 이전 프로파일의 NSX-T 구성을 그대로 유지합니다.</p> <p>해결 방법: 없음</p>
업데이트	<p>문제: 사용자가 클러스터에서 NSX-T 구성을 변경한 경우 새 호스트 프로파일을 추출합니다. 손실된 모든 설정에 대해 호스트 프로파일을 수동으로 업데이트합니다.</p> <p>해결 방법: 없음</p>
호스트 수준 전송 노드 구성	<p>문제: anportsport 노드가 자동 배포된 후 개별 엔티티로 작동합니다. 해당 전송 노드에 대한 모든 업데이트가 TNP와 전혀 일치하지 않을 수 있습니다.</p> <p>해결 방법: 클러스터를 업데이트합니다. 독립형 전송 노드의 업데이트는 마이그레이션 규칙을 유지할 수 없습니다. 마이그레이션 중에 재부팅이 진행되지 못할 수 있습니다.</p>
mux_user 암호 정책 및 암호가 재설정되지 않았으므로 호스트 프로파일을 적용할 수 없습니다.	<p>문제: vSphere 6.7 U3보다 이전 버전을 실행하는 호스트에서만 발생하는 문제입니다. mux_user 암호를 재설정하지 않으면 호스트의 호스트 업데이트 적용 및 호스트 프로파일 애플리케이션이 실패할 수 있습니다.</p> <p>해결 방법: [정책 및 프로파일]에서 호스트 프로파일을 편집하여 mux_user 암호 정책을 수정하고 mux_user 암호를 재설정합니다.</p>
NVDS 스위치로 마이그레이션하기 위해 선택한 VMkernel 어댑터에서는 피어 DNS 구성이 지원되지 않습니다.	<p>문제: NVDS로 마이그레이션하기 위해 선택한 VMkernel 어댑터가 피어 DNS를 사용하도록 설정한 경우 호스트 프로파일 애플리케이션이 실패합니다.</p> <p>해결 방법: NVDS 스위치로 마이그레이션해야 하는 VMkernel 어댑터에서 피어 DNS 설정을 사용하지 않도록 설정하여 추출된 호스트 프로파일을 편집합니다. 또는 피어 DNS 지원 VMkernel 어댑터를 NVDS 스위치로 마이그레이션하지 않도록 하십시오.</p>

시나리오	설명
VMkernel NIC 주소의 DHCP 주소가 보존되지 않음	문제: 참조 호스트가 상태 저장인 경우 상태 저장 참조 호스트에서 추출된 프로파일을 사용하는 상태 비저장 호스트는 PXE 시작 MAC에서 파생된 VMkernel 관리 MAC 주소를 유지할 수 없습니다. 이 경우 DHCP 주소 지정 문제가 발생합니다. 해결 방법: 상태 저장 호스트의 압축되지 않은 호스트 프로파일을 편집하고 'vmknics의 MAC 주소 결정 방법 확인' 을 '시스템이 PXE 시작된 MAC 주소 사용' 으로 수정합니다.
vCenter의 호스트 프로파일 애플리케이션 오류로 인해 호스트에서 NSX 구성 오류가 발생할 수 있습니다.	문제: vCenter에서 호스트 프로파일 애플리케이션이 실패하면 NSX 구성도 실패할 수 있습니다. 해결 방법: vCenter에서 호스트 프로파일이 성공적으로 적용되었는지 확인합니다. 오류를 수정하고 다시 시도하십시오.
상태 비저장 ESXi 호스트에서는 LAG가 지원되지 않습니다.	문제: NSX에서 LAG로 구성된 업링크 프로파일이 vCenter Server 또는 NSX에서 관리되는 상태 비저장 ESXi 호스트에서 지원되지 않습니다. 해결 방법: 없음

상태 저장 서버

ESXi 호스트의 호스트 프로파일을 상태 저장 서버의 NSX-T와 통합합니다.

상태 저장 호스트는 재부팅된 후에도 모든 구성과 설치된 VIB를 유지하는 호스트입니다. 상태 비저장 호스트를 가져오는 데 필요한 부팅 파일이 자동 배포 서버에 저장되기 때문에 상태 비저장 호스트에는 자동 배포 서버가 필요하지만, 상태 저장 호스트에는 이와 유사한 인프라가 필요하지 않습니다. 이는 상태 저장 호스트를 가져오는 데 필요한 부팅 파일이 하드 드라이브에 저장되기 때문입니다.

이 절차에서는 참조 호스트가 상태 저장 클러스터와 클러스터의 대상 호스트 외부에 있습니다. 대상 호스트는 클러스터 내에 있거나 클러스터가 아닌 독립형 호스트에 있을 수 있습니다. 클러스터에 가입하는 새 대상 호스트가 NSX-T VIB로 자동 준비되도록 호스트 프로파일 및 TN 프로파일(전송 노드 프로파일)을 적용하여 클러스터를 준비합니다. 대상 호스트를 전송 노드로 구성합니다. 마찬가지로 독립형 호스트의 경우 호스트 프로파일을 적용하고 NSX-T VIB를 설치하도록 NSX-T를 구성합니다. 그러면 NSX-T 구성이 완료된 후에 전송 노드가 됩니다.

참고 NSX-T VIB는 TN 프로파일에서 설치되고 ESXi 호스트 구성은 호스트 프로파일에 의해 적용됩니다.

대상 호스트를 전송 노드로 구성하는 동안 VMkernel 어댑터 및 vmnics나 VSS 또는 VDS 스위치에 연결된 물리적 네트워크 인터페이스를 마이그레이션한 후 NSX-T 가상 분산 스위치인 N-VDS 스위치에 연결할 수 있습니다.

지원되는 NSX-T 및 ESXi 버전

상태 저장 서버의 지원되는 NSX-T 및 ESXi 버전

버전 이름	67ep6	67U2	67U3	67ep7	67U2C	6.5U3	6.5p03
NSX-T 2.4	예	아니요	아니요	아니요	아니요	아니요	예
NSX-T 2.4.1	예	예	아니요	아니요	아니요	아니요	예

버전 이름	67ep6	67U2	67U3	67ep7	67U2C	6.5U3	6.5p03
NSX-T 2.4.2	예	예	아니요	아니요	아니요	아니요	예
NSX-T 2.4.3	예	예	아니요	아니요	아니요	아니요	예
NSX-T 2.5	예	예	예	예	예	예	예
NSX-T 2.5.1	예	예	예	예	예	예	예

대상 상태 저장 클러스터 준비

대상 상태 저장 클러스터를 준비해 클러스터에 가입하는 모든 새 호스트가 ESXi 및 NSX-T VIB를 사용하여 자동으로 배포되도록 합니다.

클러스터 내에서 또는 클러스터 외부에서 참조 호스트로 사용할 호스트를 선택할 수 있습니다. 참조 호스트의 호스트 프로파일이 추출되어 대상 호스트에 적용되기 때문에 참조 호스트를 생성해야 합니다. 이 절차에서는 vmk0(관리 트래픽) 및 vmk1(vMotion 트래픽)을 N-VDS 스위치로 마이그레이션하기 위한 지침을 설명합니다.

사전 요구 사항

절차

- 1 참조 호스트에서, 지원되는 ESXi 빌드를 배포합니다.
 - a vSphere에서 vmk1 어댑터를 추가합니다. 관리 트래픽을 처리할 수 있는 vmk0이 이미 있습니다.
- 2 참조 노드를 전송 노드로 구성합니다.
 - a vmk0 및 vmk1을 마이그레이션하기 전에 vSphere Web Client를 사용하여 논리적 스위치가 NSX-T에 생성되었는지 확인합니다.
 - b (선택 사항) NSX-T Manager UI를 사용하여, NSX-T 설치 후 논리적 스위치에 매핑된 vmk1 어댑터가 N-VDS 스위치로 마이그레이션되도록 NSX를 구성합니다.
 - c (선택 사항) NSX-T Manager UI를 사용하여, NSX-T 설치 후 논리적 스위치에 매핑된 vmk0 어댑터가 N-VDS 스위치로 마이그레이션되도록 NSX-T를 구성합니다.

참고 vmk0 및 vmk1은 다른 VSS 또는 DVS 스위치에 있을 수 있습니다.

- d vSphere Web Client를 사용하여 vmk0 및 vmk1이 N-VDS 스위치의 논리적 스위치에 연결되어 있는지 확인합니다.
- 3 참조 호스트에서 호스트 프로파일을 추출합니다.
 - 4 환경에서 N-VDS 스위치에 마이그레이션해야 하는 vmkernel 어댑터가 여러 개 있을 수 있습니다. 그러나 vmk 어댑터를 VSS/DVS에서 N-VDS 스위치로 마이그레이션하기 전에 대상 호스트의 구성 매개 변수가 참조 호스트의 구성 매개 변수와 일치하는지 확인하십시오.

5 독립형 호스트인 대상 호스트에서 다음을 수행합니다.

- a 호스트 프로파일을 대상 호스트에 연결합니다.
- b 호스트에서 NSX-T를 수동으로 구성합니다. ESXi의 호스트 프로파일 때문에 호스트를 전송 노드로 구성하는 경우 다음 조건이 충족되는지 확인합니다.
- c 호스트는 동일한 전송 영역에 속해야 합니다.
- d vmk1 어댑터는 참조 호스트에서 사용하는 동일한 논리적 스위치에 연결되어야 합니다.
- e 대상 호스트는 참조 호스트에서 사용하는 것과 동일한 IP 풀을 사용해야 합니다.
- f 업링크 프로파일, LLDP, NIOC, 설치를 위한 네트워크 매핑, 대상 호스트에 구성된 N-VDS가 참조 호스트에 구성된 것과 동일해야 합니다.
- g 수동으로 VMkernel 어댑터, vmk1 및 vmnic1을 추가하여 VSS/DVS 스위치에서 N-VDS 스위치로 마이그레이션되도록 합니다. vmk1 마이그레이션 시나리오를 참조하십시오.
- h 관리 어댑터, vmk0 및 또는 vmnic0를 수동으로 추가합니다.

6 클러스터에 속하는 대상 호스트에서 다음을 수행합니다.

- a 호스트 프로파일을 상태 저장 대상 클러스터에 연결합니다.
- b TN 프로파일을 생성한 후 클러스터에서 적용합니다.
- c vmk1 및 vmnic1이 마이그레이션될 수 있도록 구성하려면 vmk1 마이그레이션 시나리오를 참조하십시오.
- d vmk0 및 vmnic0가 마이그레이션될 수 있도록 구성하려면 vmk0 마이그레이션 시나리오를 참조하십시오.
- e 클러스터에 TN 프로파일 적용하기.

다음에 수행할 작업

VMkernel 어댑터가 NSX-T에 적용된 호스트 프로파일을 사용하거나 사용하지 않고 마이그레이션되는 시나리오.

호스트 프로파일이 적용된 VMkernel 마이그레이션

이 섹션에 설명된 시나리오에서 VMkernel 1(vmk1) 어댑터는 호스트 프로파일이 NSX-T에 적용된 N-VDS 스위치로 마이그레이션됩니다. vmk1 어댑터는 vMotion, Fault Tolerance 및 기타 인프라 서비스에 대한 인프라 트래픽을 지원합니다.

시나리오	오류	해결 방법
참조 호스트 프로파일을 적용하는 독립형 대상 호스트의 vmk1 마이그레이션.	<p>대상 호스트가 전송 노드로 구성되지 않습니다. 대상 호스트가 NSX-T 개체에 대해 알 수 없으므로 호스트 프로파일 애플리케이션에 오류가 발생합니다. 대상 호스트의 호스트 프로파일 업데이트 적용이 실패합니다.</p> <p>Error: Received SOAP response fault : generate HostConfigTask Spec..</p>	<p>1 vmk1을 대상 호스트의 논리적 스위치로 마이그레이션하기 위해 참조 호스트 프로파일을 적용하기 전에, 대상 호스트를 전송 노드로 구성하여 NSX-T VIB를 설치하고, N-VDS 스위치를 생성하고, vmk1 어댑터를 VSS 스위치에서 N-VDS 스위치로 마이그레이션합니다.</p> <p>ESXi의 호스트 프로파일 때문에 호스트를 전송 노드로 구성하는 경우 다음 조건이 충족되는지 확인합니다.</p> <ul style="list-style-type: none"> ■ 호스트는 동일한 전송 영역에 속해야 합니다. ■ vmk1 어댑터는 참조 호스트에서 사용하는 동일한 논리적 스위치에 연결되어야 합니다. ■ 대상 호스트는 참조 호스트에서 사용하는 것과 동일한 IP 풀을 사용해야 합니다. ■ 업링크 프로파일, LLDP, NIOC, 설치를 위한 네트워크 매핑, 대상 호스트에 구성된 N-VDS가 참조 호스트에 구성된 것과 동일해야 합니다. <p>대상 호스트가 호스트 프로파일에 있는 동일한 논리적 스위치 이름으로 구성된 경우 호스트 프로파일 업데이트 적용이 성공적으로 수행됩니다.</p>
상태 저장 클러스터의 대상 호스트에서 vmk1 마이그레이션.	<p>호스트 프로파일을 대상 호스트에 적용하기 전에 논리적 스위치에 매핑된 vmk1으로 구성된 TN 프로파일을 적용하여 클러스터를 준비하면 vmk1 마이그레이션이 실패합니다.</p> <p>Error: vmk1 missing on the host.</p>	<p>1 참조 호스트 프로파일을 클러스터에 가입된 대상 호스트에 적용합니다.</p> <p>2 대상 호스트에서 호스트 프로파일에 업데이트를 적용하여 대상 호스트에 vmk1 어댑터를 생성합니다.</p> <p>3 TN 프로파일을 클러스터에 다시 적용하여 vmk1을 대상 클러스터로 마이그레이션합니다.</p>

시나리오	오류	해결 방법
독립형 호스트의 vmkO 및 vmk1 마이그레이션.	독립형 호스트에서 NSX-T를 구성할 때 [설치를 위한 네트워크 매핑] 필드에 vmkO 또는 vmk1 매핑이 지정되지 않으면 마이그레이션이 실패합니다.	대상 호스트에서 NSX-T를 구성할 때 [설치를 위한 네트워크 매핑] 필드가 N-VDS의 동일한 논리적 스위치에 매핑된 vmkO 및 vmk1으로 지정되어 있는지 확인합니다.
클러스터 호스트에서 vmkO 및 vmk1 마이그레이션.	클러스터에 TN 프로파일을 적용할 때 [설치를 위한 네트워크 매핑] 필드에 vmkO 또는 vmk1 매핑이 지정되지 않으면 마이그레이션이 실패합니다.	TN 프로파일을 클러스터에 적용합니다. 클러스터에 대해 TN 프로파일을 구성할 때 [설치를 위한 네트워크 매핑] 필드가 N-VDS의 논리적 스위치에 매핑된 vmkO 및 vmk1으로 지정되어 있는지 확인합니다.

호스트 프로파일이 적용되지 않은 VMkernel 마이그레이션

이 섹션에 설명된 시나리오에서 VMkernel O(vmkO) 어댑터는 호스트 프로파일이 NSX-T에 적용되지 않은 상태에서 N-VDS 스위치로 마이그레이션됩니다. vmkO 어댑터는 NSX-T에 대한 관리 트래픽을 지원합니다.

vmkO가 이미 존재하기 때문에 호스트 프로파일을 대상 호스트에 적용할 필요가 없습니다. vmkO 어댑터는 ESXi 호스트에서 관리 트래픽을 지원합니다.

시나리오	절차	결과
독립형 호스트의 vmkO 마이그레이션.	대상 호스트에서 NSX-T를 구성할 때 설치를 위한 네트워크 매핑 필드가 N-VDS의 논리적 스위치에 매핑된 vmkO로 지정되어 있는지 확인합니다.	vmkO가 대상 호스트의 논리적 스위치로 마이그레이션됩니다.
클러스터 호스트의 vmkO 마이그레이션.	TN 프로파일을 클러스터에 적용합니다. 클러스터에서 TN 프로파일을 구성할 때 설치를 위한 네트워크 매핑 필드가 N-VDS의 논리적 스위치에 매핑된 vmkO로 지정되어 있는지 확인합니다.	vmkO가 대상 호스트의 논리적 스위치로 마이그레이션됩니다.

호스트 전송 노드에서 NSX-T Data Center 제거

12

호스트 전송 노드에서 NSX-T Data Center를 제거하는 단계는 호스트 유형 및 구성 방법에 따라 다릅니다.

- 제거를 위한 호스트 네트워크 매핑 확인

ESXi 호스트에서 NSX-T Data Center를 제거하기 전에 제거를 위한 적절한 네트워크 매핑이 구성되어 있는지 확인합니다. ESXi 호스트의 VMkernel 인터페이스가 N-VDS에 연결되어 있는 경우 매핑이 필요합니다.

- vSphere 클러스터에서 NSX-T Data Center 제거

전송 노드 프로파일을 사용하여 vSphere 클러스터에 NSX-T Data Center를 설치한 경우 다음 지침에 따라 클러스터의 모든 호스트에서 NSX-T Data Center를 제거할 수 있습니다.

- vSphere 클러스터의 호스트에서 NSX-T Data Center 제거

vCenter Server에서 관리되는 단일 호스트에서 NSX-T Data Center를 제거할 수 있습니다. 클러스터의 다른 호스트는 영향을 받지 않습니다.

- 독립형 호스트에서 NSX-T Data Center 제거

독립형 호스트에서 NSX-T Data Center를 제거할 수 있습니다. 독립형 호스트는 ESXi 또는 KVM일 수 있습니다.

제거를 위한 호스트 네트워크 매핑 확인

ESXi 호스트에서 NSX-T Data Center를 제거하기 전에 제거를 위한 적절한 네트워크 매핑이 구성되어 있는지 확인합니다. ESXi 호스트의 VMkernel 인터페이스가 N-VDS에 연결되어 있는 경우 매핑이 필요합니다.

제거 매핑에 따라 제거 후 인터페이스가 연결되는 위치가 결정됩니다. 물리적 인터페이스(vmnicX) 및 VMkernel 인터페이스(vmkX)에 대한 제거 매핑이 있습니다. 제거 시 VMkernel 인터페이스가 현재 연결에서 제거 매핑에 지정된 포트 그룹으로 이동합니다. 물리적 인터페이스가 제거 매핑에 포함된 경우 물리적 인터페이스는 VMkernel 인터페이스의 대상 포트 그룹을 기준으로 적절한 vSphere Distributed Switch 또는 vSphere Standard Switch에 연결됩니다.

경고 물리적 인터페이스 또는 VMkernel 인터페이스가 N-VDS에 연결된 경우 ESXi 호스트에서 NSX-T Data Center를 제거하는 작업이 중단됩니다. 호스트나 클러스터가 vSAN과 같은 다른 애플리케이션에 참여하고 있는 경우 호스트나 클러스터를 제거하면 해당 애플리케이션도 영향을 받을 수 있습니다.

제거를 위한 네트워크 매핑을 구성할 수 있는 두 가지 위치가 있습니다.

- 전송 노드 구성: 해당 호스트에 적용됩니다.
- 전송 노드 프로파일 구성: 클러스터에 적용할 수 있습니다.

참고 전송 노드 프로파일을 클러스터에 적용하려면 계산 관리자가 구성되어 있어야 합니다.

계산 관리자가 구성된 경우 호스트에 전송 노드 구성 및 전송 노드 프로파일 구성이 둘 다 있을 수 있습니다. 가장 최근에 적용된 구성이 활성화됩니다. 제거를 위한 네트워크 매핑이 활성화 구성에 올바르게 구성되어 있는지 확인합니다.

이 예에서 클러스터 **cluster-1**에는 전송 노드 프로파일 **TNP-1**이 적용되어 있습니다. 호스트 **tn-1**에 "구성 불일치"가 표시됩니다. 이 불일치 메시지는 전송 노드 프로파일이 적용된 후에 다른 구성이 **tn-1**에 적용되었음을 나타냅니다. 전송 노드 **tn-2**는 전송 노드 프로파일의 네트워크 매핑을 사용하며 전송 노드 **tn-1**은 자체 구성을 사용합니다.

⚙️ NSX 구성
🗑️ NSX 제거
⚙️ 작업 ▼

<input type="checkbox"/>	노드	ID	IP 주소	OS 유형	NSX 구성
<input type="checkbox"/>	🔵 New Cluster (2)	MoR...			⚠️ TNP-1
<input type="checkbox"/>	🔵 tn-1	926...	10....	ESXi ...	⚠️ 구성 불일치
<input type="checkbox"/>	🔵 tn-2	901f....	10....	ESXi ...	구성됨

사전 요구 사항

- 제거 매핑에서 사용하도록 구성된 적절한 포트 그룹이 있는지 확인합니다. vSphere Distributed Switch 사용 후 삭제 포트 그룹 또는 vSphere Standard Switch 포트 그룹을 사용해야 합니다.
- 독립 실행형 ESXi 호스트에 대한 제거 매핑에서 vSphere Distributed Switch 포트 그룹을 사용하려는 경우 계산 관리자를 구성합니다. [계산 관리자 추가](#)를 참조하십시오. 구성된 계산 관리자가 없는 경우 vSphere Standard Switch 포트 그룹을 사용해야 합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 패브릭 > 노드 > 호스트 전송 노드**를 선택합니다.

- 3 제거하려는 각 호스트에 대해 제거를 위한 네트워크 매핑에 N-VDS에 있는 각 VMkernel 인터페이스에 대한 포트 그룹이 포함되어 있는지 확인합니다. 누락된 매핑을 추가합니다.

중요 제거를 위한 네트워크 매핑의 포트 그룹은 vSphere Distributed Switch 사용 후 삭제 포트 그룹 또는 vSphere Standard Switch 포트 그룹이어야 합니다.

- a VMkernel 인터페이스를 보려면 vCenter Server에 로그인하고 호스트를 선택한 다음, **구성 > VMkernel 어댑터**를 클릭합니다.
- b 전송 노드 구성이 활성 구성인 경우 호스트를 선택하고 **편집**(독립형 호스트인 경우) 또는 **NSX 구성**(관리형 호스트인 경우)을 클릭합니다. 다음을 클릭한 다음, **제거를 위한 네트워크 매핑**을 클릭합니다. **VMKNic 매핑** 및 **물리적 NIC 매핑** 탭에서 매핑을 확인합니다.
- c 전송 노드 프로파일이 활성 구성인 경우 **NSX 구성** 열에서 클러스터에 대한 전송 노드 프로파일의 이름을 클릭하고 **편집**을 클릭합니다. **N-VDS** 탭에서 **제거를 위한 네트워크 매핑**을 클릭합니다. **VMKNic 매핑** 및 **물리적 NIC 매핑** 탭에서 매핑을 확인합니다.

vSphere 클러스터에서 NSX-T Data Center 제거

전송 노드 프로파일을 사용하여 vSphere 클러스터에 NSX-T Data Center를 설치한 경우 다음 지침에 따라 클러스터의 모든 호스트에서 NSX-T Data Center를 제거할 수 있습니다.

전송 노드 프로파일에 대한 자세한 내용은 [전송 노드 프로파일 추가](#) 항목을 참조하십시오.

경고 물리적 인터페이스 또는 VMkernel 인터페이스가 N-VDS에 연결된 경우 ESXi 호스트에서 NSX-T Data Center를 제거하는 작업이 중단됩니다. 호스트나 클러스터가 vSAN과 같은 다른 애플리케이션에 참여하고 있는 경우 호스트나 클러스터를 제거하면 해당 애플리케이션도 영향을 받을 수 있습니다.

전송 노드 프로파일을 사용하여 NSX-T Data Center를 설치하지 않았거나 클러스터에 있는 호스트의 하위 집합에서 NSX-T Data Center를 제거하려는 경우에는 [vSphere 클러스터의 호스트에서 NSX-T Data Center 제거](#) 항목을 참조하십시오.

참고 클러스터에서 호스트를 제거해도 NSX-T Data Center는 제거되지 않습니다. 클러스터의 호스트에서 NSX-T Data Center를 제거하려면 [vSphere 클러스터의 호스트에서 NSX-T Data Center 제거](#)의 지침을 따르십시오.

사전 요구 사항

- 제거하려는 호스트에 네트워크 제거 매핑이 구성되어 있는지 확인합니다. [제거를 위한 호스트 네트워크 매핑 확인](#) 항목을 참조하십시오.
- 제거하려는 호스트가 vSphere에서 유지 보수 모드에 있는지 확인합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.

- 2 시스템 > 패브릭 > 노드 > **호스트 전송 노드**를 선택합니다.
- 3 관리자 드롭다운 메뉴에서 vCenter Server를 선택합니다.
- 4 제거하려는 클러스터를 선택하고 **NSX 제거**를 클릭합니다.
- 5 NSX-T Data Center 소프트웨어가 호스트에서 제거되었는지 확인합니다.
 - a 호스트의 명령줄 인터페이스에 루트 사용자로 로그인합니다.
 - b 이 명령을 실행하여 NSX-T Data Center VIB를 확인합니다.

```
esxcli software vib list | grep -E 'nsx|vsipfwlib'
```

NSX-T Data Center 소프트웨어가 성공적으로 제거되면 VIB가 나열되지 않습니다. 호스트에 NSX VIB가 남아 있는 경우 VMware 지원팀에 문의하십시오.

- 6 호스트에 NSX Intelligence도 배포된 경우 모든 전송 노드가 기본 네트워크 보안 그룹의 일부가 되기 때문에 NSX-T Data Center 제거가 실패합니다. 제거하려면:
 - a 클러스터를 선택하고 **NSX 제거**를 클릭합니다.
 - b 확인 팝업 창에서 **강제 삭제**를 선택합니다.

클러스터의 모든 호스트에서 NSX-T가 제거되었습니다.

vSphere 클러스터의 호스트에서 NSX-T Data Center 제거

vCenter Server에서 관리되는 단일 호스트에서 NSX-T Data Center를 제거할 수 있습니다. 클러스터의 다른 호스트는 영향을 받지 않습니다.

경고 물리적 인터페이스 또는 VMkernel 인터페이스가 N-VDS에 연결된 경우 ESXi 호스트에서 NSX-T Data Center를 제거하는 작업이 중단됩니다. 호스트나 클러스터가 vSAN과 같은 다른 애플리케이션에 참여하고 있는 경우 호스트나 클러스터를 제거하면 해당 애플리케이션도 영향을 받을 수 있습니다.

사전 요구 사항

- 제거하려는 호스트에 네트워크 제거 매핑이 구성되어 있는지 확인합니다. [제거를 위한 호스트 네트워크 매핑 확인](#) 항목을 참조하십시오.
- 제거하려는 호스트가 vSphere에서 유지 보수 모드에 있는지 확인합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 시스템 > 패브릭 > 노드 > **호스트 전송 노드**를 선택합니다.
- 3 관리자 드롭다운 메뉴에서 vCenter Server를 선택합니다.

- 클러스터에 전송 노드 프로파일이 적용된 경우 클러스터를 선택하고 **작업 > TN 프로파일 분리**를 클릭합니다.

클러스터에 전송 노드 프로파일이 적용된 경우 클러스터에 대한 **NSX 구성** 열에 프로파일 이름이 표시됩니다.

- 호스트를 선택하고 **NSX 제거**를 클릭합니다.
- NSX-T Data Center 소프트웨어가 호스트에서 제거되었는지 확인합니다.
 - 호스트의 명령줄 인터페이스에 루트 사용자로 로그인합니다.
 - 이 명령을 실행하여 NSX-T Data Center VIB를 확인합니다.

```
esxcli software vib list | grep -E 'nsx|vsipfwlib'
```

NSX-T Data Center 소프트웨어가 성공적으로 제거되면 VIB가 나열되지 않습니다. 호스트에 NSX VIB가 남아 있는 경우 VMware 지원팀에 문의하십시오.

- 클러스터에 전송 노드 프로파일이 적용되어 있는 경우 다시 적용하려면 클러스터를 선택하고 **NSX 구성**을 클릭한 후 **배포 프로파일 선택** 드롭다운 메뉴에서 프로파일을 선택합니다.

독립형 호스트에서 NSX-T Data Center 제거

독립형 호스트에서 NSX-T Data Center를 제거할 수 있습니다. 독립형 호스트는 ESXi 또는 KVM일 수 있습니다.

경고 물리적 인터페이스 또는 VMkernel 인터페이스가 N-VDS에 연결된 경우 ESXi 호스트에서 NSX-T Data Center를 제거하는 작업이 중단됩니다. 호스트나 클러스터가 vSAN과 같은 다른 애플리케이션에 참여하고 있는 경우 호스트나 클러스터를 제거하면 해당 애플리케이션도 영향을 받을 수 있습니다.

사전 요구 사항

독립형 ESXi 호스트에서 NSX-T Data Center를 제거하는 경우 다음 설정을 확인합니다.

- 제거하려는 호스트에 네트워크 제거 매핑이 구성되어 있는지 확인합니다. [제거를 위한 호스트 네트워크 매핑 확인](#) 항목을 참조하십시오.
- 제거하려는 호스트가 vSphere에서 유지 보수 모드에 있는지 확인합니다.

절차

- 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 시스템 > 패브릭 > 노드 > 호스트 전송 노드**를 선택합니다.
- 관리자** 드롭다운 메뉴에서 **없음: 독립형 호스트**를 선택합니다.

- 4 호스트를 선택하고 **삭제**를 클릭합니다. 표시되는 확인 대화상자에서 **NSX 구성 요소 제거**가 선택되어 있고 **강제 삭제**가 선택 취소되어 있는지 확인합니다. **삭제**를 클릭합니다.

NSX-T Data Center 소프트웨어가 호스트에서 제거됩니다. 모든 NSX-T Data Center 소프트웨어가 제거되는 데 최대 5분이 걸릴 수 있습니다.

- 5 제거에 실패하면 호스트를 선택하고 **삭제**를 다시 클릭합니다. 확인 대화상자에서 **NSX 구성 요소 제거**를 선택 취소하고 **강제 삭제**를 선택합니다.

호스트 전송 노드가 관리부에서 삭제되지만 호스트에 NSX-T Data Center 소프트웨어는 계속 설치된 상태일 수 있습니다.

- 6 NSX-T Data Center 소프트웨어가 호스트에서 제거되었는지 확인합니다.

- a 호스트의 명령줄 인터페이스에 루트 사용자로 로그인합니다.
- b 적절한 명령을 실행하여 NSX-T Data Center 소프트웨어 패키지를 확인합니다.

표 12-1. 패키지 목록 명령

호스트 운영 체제	명령
ESXi	<code>esxcli software vib list grep -E 'nsx vsipfwlib'</code>
Red Hat Enterprise Linux 및 CentOS Linux	<code>rpm -qa grep -E 'nsx vsipfwlib'</code>
Ubuntu	<code>dpkg -l grep -E 'nsx vsipfwlib'</code>
SUSE Linux Enterprise Server	<code>zypper packages --installed-only grep -E 'nsx vsipfwlib'</code>

NSX-T Data Center 소프트웨어가 성공적으로 제거되면 패키지가 나열되지 않습니다. 호스트에 NSX 소프트웨어 패키지가 남아 있는 경우 VMware 지원팀에 문의하십시오.

NSX Cloud는 공용 클라우드 네트워크를 관리할 수 있는 단일 창 방식을 제공합니다.

NSX Cloud는 공용 클라우드에서 하이퍼바이저 액세스가 필요하지 않은 공급자별 네트워킹의 대항마입니다.

여기에는 여러 가지 이점이 있습니다.

- 운영 환경에 사용되는 네트워크 및 보안 프로필과 동일한 환경을 사용하여 애플리케이션을 개발하고 테스트할 수 있습니다.
- 배포 준비가 끝날 때까지 개발자가 애플리케이션을 관리할 수 있습니다.
- 재해 복구를 통해 계획되지 않은 중단이나 공용 클라우드에 대한 보안 위협으로부터 복구가 가능합니다.
- 공용 클라우드 간에 워크로드를 마이그레이션하는 경우, NSX Cloud는 새로운 위치와 상관없이 유사한 보안 정책이 워크로드 VM에 적용되도록 합니다.

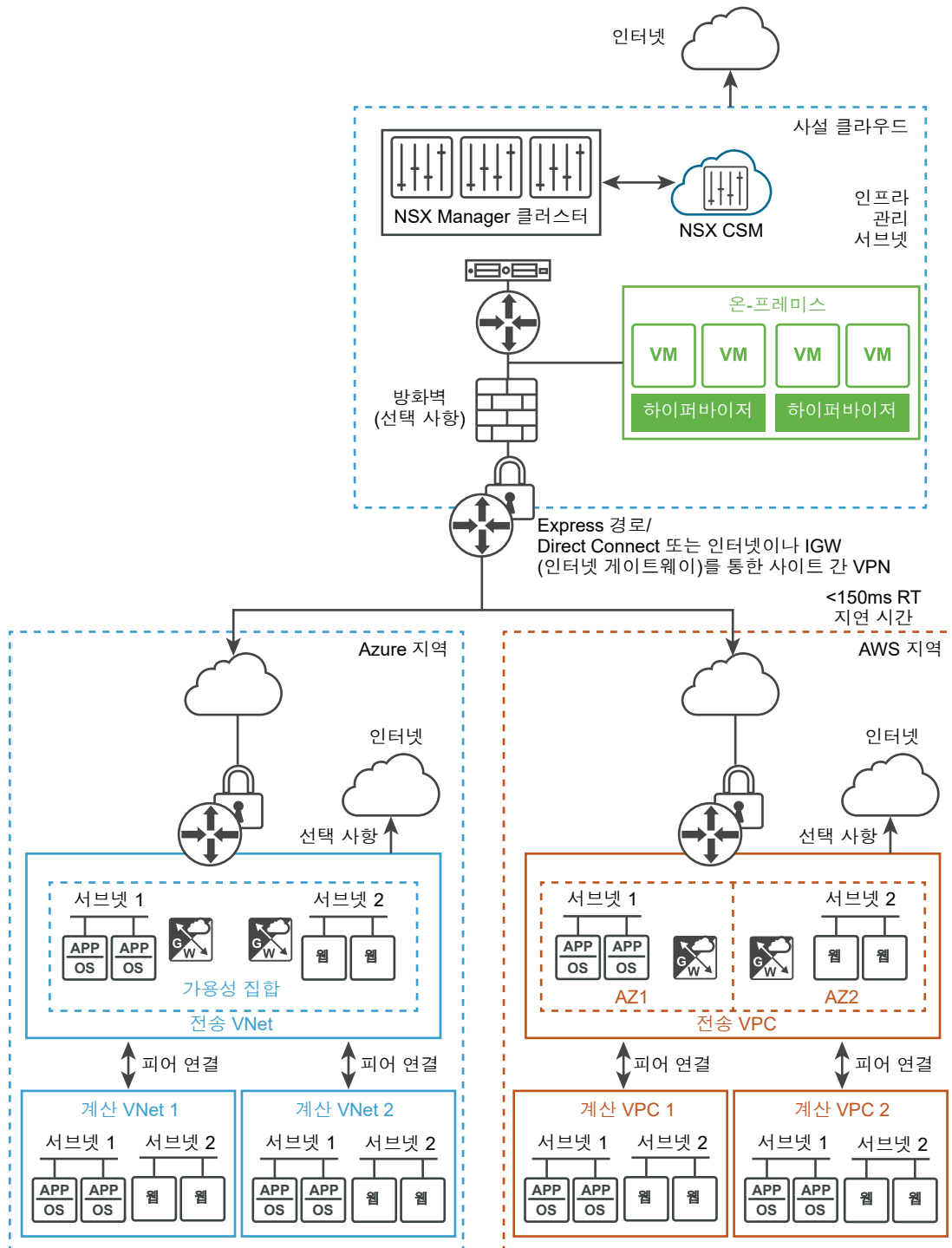
본 장은 다음 항목을 포함합니다.

- [NSX Cloud 아키텍처 및 구성 요소](#)
- [NSX Cloud 배포 개요](#)
- [NSX-T Data Center 온-프레미스 구성 요소 배포](#)
- [공용 클라우드 계정 추가](#)
- [NSX Public Cloud Gateway 배포](#)
- [\(선택 사항\) 워크로드 VM에 NSX Tools 설치](#)
- [PCG 배포 해제 또는 연결 해제](#)

NSX Cloud 아키텍처 및 구성 요소

NSX Cloud는 NSX-T Data Center 핵심 구성 요소를 공용 클라우드와 통합하여 구현 환경 전반에 네트워크 및 보안을 제공합니다.

그림 13-1. NSX Cloud 아키텍처



핵심 구성 요소

NSX Cloud의 핵심적인 구성 요소:

- **NSX Manager:** 정책 기반 라우팅, RBAC(역할 기반 액세스 제어), 제어부 및 런타임 상태가 정의되어 있는 관리부로 사용됩니다.

- **CSM(Cloud Service Manager)**: NSX Manager와 통합하여 관리부에 공용 클라우드 관련 정보 제공.
- **PCG(공용 클라우드 게이트웨이)**: NSX 관리부 및 제어부, NSX Edge Gateway 서비스와 연결 및 공용 클라우드 엔티티와 API 기반 통신.
- **NSX Tools** 기능: 워크로드 VM에 NSX 관리 데이터 경로 제공.

NSX Cloud 배포 개요

이 개요를 참조하여 NSX-T Data Center에서 공용 클라우드 워크로드 VM을 관리할 수 있도록 NSX Cloud 구성 요소를 설치 및 구성하는 전체 프로세스를 이해하십시오.



참고 배포를 계획할 때 온 프레미스 NSX-T Data Center 장치가 공용 클라우드에 배포된 PCG와 올바르게 연결되어 있고 전송 VPC/VNet이 계산 VPC/VNet과 동일한 지역에 있어야 합니다.

표 13-1. NSX Cloud 배포를 위한 워크플로

작업	지침
<input type="checkbox"/> CSM을 설치하고 NSX Manager와 연결합니다.	NSX-T Data Center 온-프레미스 구성 요소 배포의 내용을 참조하십시오.
<input type="checkbox"/> 공용 클라우드 계정 하나 이상을 CSM에 추가합니다.	공용 클라우드 계정 추가의 내용을 참조하십시오.
<input type="checkbox"/> 전송 VPC/VNet에 PCG를 배포하고 계산 VPC/VNet에 연결합니다.	NSX Public Cloud Gateway 배포의 내용을 참조하십시오.
후속 작업	"NSX-T Data Center 관리 가이드"의 NSX Cloud 사용에 나와 있는 지침을 따르십시오.

NSX-T Data Center 온-프레미스 구성 요소 배포

CSM 설치를 계속하려면 NSX Manager가 이미 설치되어 있어야 합니다.

CSM 설치

Cloud Service Manager(CSM)는 NSX Cloud의 핵심 구성 요소입니다.

NSX Manager를 설치한 후 NSX Manager 설치와 동일한 단계를 수행하고 **nsx-cloud-manager**를 VM 역할로 선택하여 CSM을 설치합니다. 지침에 대해서는 **NSX Manager 및 사용 가능한 장치 설치**를 참조하십시오.

필요에 따라 초소형 VM 크기 이상으로 CSM을 배포할 수 있습니다. 자세한 내용은 [NSX Manager VM 및 호스트 전송 노드 시스템 요구 사항](#) 항목을 참조하십시오.

CSM을 NSX Manager에 연결

구성 요소가 서로 통신할 수 있도록 하려면 CSM 장치를 NSX Manager와 연결해야 합니다.

사전 요구 사항

- NSX Manager가 설치되어 있어야 하며 관리자 계정으로 NSX Manager에 로그인할 수 있도록 사용자 이름과 암호가 있어야 합니다.
- CSM이 설치되어 있고 CSM에 엔터프라이즈 관리자 역할이 할당되어 있어야 합니다.

절차

- 1 브라우저에서 CSM에 로그인합니다.
- 2 설정 마법사에서 해당하는 메시지가 표시되면 **설정 시작**을 클릭합니다.
- 3 [NSX Manager 자격 증명] 화면에 다음 세부 정보를 입력합니다.

옵션	설명
NSX Manager 호스트 이름	가능한 경우 NSX Manager의 FQDN(정규화된 도메인 이름)을 입력합니다. NSX Manager의 IP 주소를 입력할 수도 있습니다.
관리 자격 증명	NSX Manager에 대한 엔터프라이즈 관리자 사용자 이름 및 암호를 입력합니다.
관리자 지문	필요한 경우 NSX Manager의 지문 값을 입력합니다. 이 필드를 비워 두면 시스템에서 지문을 식별하고 이를 다음 화면에 표시합니다.

- 4 (선택 사항) NSX Manager에 대한 지문 값을 제공하지 않거나 잘못된 값을 제공하면 **지문 확인** 화면이 나타납니다. 시스템에서 검색된 지문을 수락하려면 확인란을 선택합니다.
- 5 **연결**을 클릭합니다.

참고 설정 마법사에서 이 설정을 누락했거나 연결된 NSX Manager를 변경하려는 경우 CSM에 로그인하고 **시스템 > 설정**을 클릭한 다음 **연결된 NSX 노드** 패널에서 **구성**을 클릭합니다.

CSM에서 NSX Manager 지문을 확인하고 연결을 설정합니다.

- 6 (선택 사항) 프록시 서버를 설정합니다. **(선택 사항) 프록시 서버 구성**의 지침을 참조하십시오.

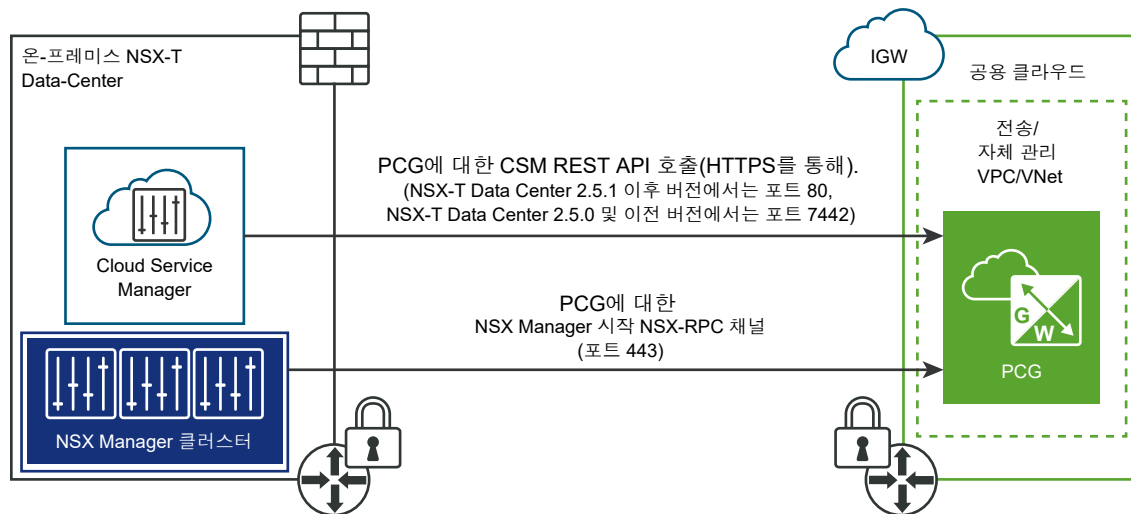
포트 및 프로토콜에 대한 액세스 사용

공용 클라우드 연결을 사용하도록 설정하려는 경우에는 NSX-T Data Center의 온-프레미스 배포에서 인바운드 포트를 열어 둘 필요가 없습니다.

다음 아웃바운드 포트가 필요합니다.

표 13-2. NSX-T Data Center와 공용 클라우드 연결에 필요한 포트 및 프로토콜

시작	끝	포트	프로토콜	다음에 필요함:
CSM	PCG	80 참고 NSX-T Data Center 버전 2.5.0을 사용하는 경우 비표준 포트 7442를 대신 열고, 방화벽에서 이 포트를 통한 SSL 트래픽을 허용하는지 확인해야 합니다.	TCP	HTTPS를 통한 CSM 구성 (예: 업그레이드 워크플로).
NSX Manager	PCG	443	TCP	NSX RPC 채널.
CSM	NSX Manager	443	TCP	NSX Manager 액세스를 위한 CSM. 온-프레미스 배포에 대한 자세한 내용은 포트 및 프로토콜 을 참조하십시오.



(선택 사항) 프록시 서버 구성

신뢰할 수 있는 HTTP 프록시를 통해 인터넷에 접속된 HTTP/HTTPS 트래픽을 모두 라우팅하고 모니터링 하려는 경우, CSM에 최대 5개의 프록시 서버를 구성할 수 있습니다.

PCG 및 CSM의 모든 공용 클라우드 통신은 선택한 프록시 서버를 통해 라우팅됩니다.

PCG에 대한 프록시 설정은 CSM에 대한 프록시 설정과 상관이 없습니다. PCG에 대해 다른 프록시 서버를 선택하거나 프록시 서버를 선택하지 않을 수 있습니다.

다음과 같은 인증 수준을 선택할 수 있습니다.

- 자격 증명 기반 인증.
- HTTPS 가로채기에 대한 자격 증명 기반 인증.
- 인증 없음.

절차

- 1 **시스템 > 설정**을 클릭합니다. 그런 다음 **프록시 서버** 패널에서 **구성**을 클릭합니다.

참고 CSM을 처음 설치할 때 사용할 수 있는 CSM 설치 마법사를 사용할 때 이러한 세부 정보를 제공할 수도 있습니다.

- 2 [프록시 서버 구성] 화면에서 다음과 같은 세부 정보를 입력합니다.

옵션	설명
기본값	이 라디오 버튼을 사용하여 기본 프록시 서버를 나타냅니다.
프로파일 이름	프록시 서버 프로파일 이름을 제공합니다. 이 항목은 필수입니다.
프록시 서버	프록시 서버의 IP 주소를 입력합니다. 이 항목은 필수입니다.
포트	프록시 서버의 포트를 입력합니다. 이 항목은 필수입니다.
인증	선택 사항입니다. 추가 인증을 설정하려면 이 확인란을 선택하고 유효한 사용자 이름과 암호를 제공합니다.
사용자 이름	이 항목은 [인증] 확인란을 선택하는 경우 필수입니다.
암호	이 항목은 [인증] 확인란을 선택하는 경우 필수입니다.
인증서	선택 사항입니다. HTTPS 가로채기에 대한 인증서를 제공하려면 이 확인란을 선택하고 나타나는 텍스트 상자에 인증서를 복사하여 붙여넣습니다.
프록시 없음	구성된 프록시 서버를 사용하지 않으려면 이 옵션을 선택합니다.

(선택 사항) Cloud Service Manager용 vIDM 설정

VMware Identity Manager를 사용하는 경우 NSX Manager 내에서 CSM에 액세스하도록 설정할 수 있습니다.

절차

- 1 NSX Manager 및 CSM에 대해 vIDM을 구성합니다. "NSX-T Data Center 관리 가이드"의 [VMware Identity Manager 통합 구성](#)에서 지침을 참조하십시오.
- 2 NSX Manager 및 CSM용 vIDM 사용자에게 동일한 역할을 할당합니다(예를 들어 **vIDM_admin** 사용자에게 **엔터프라이즈 관리자** 역할 할당). NSX Manager 및 CSM에 각각 로그인하고 동일한 사용자 이름에 동일한 역할을 할당해야 합니다. 자세한 지침은 "NSX-T Data Center 관리 가이드"에서 [역할 할당 또는 주체 ID 추가](#)를 참조하십시오.
- 3 NSX Manager에 로그인합니다. vIDM 로그인으로 리디렉션됩니다.

- 4 vIDM 사용자의 자격 증명을 입력합니다. 로그인되면 애플리케이션 아이콘을 클릭하여 NSX Manager와 CSM 간을 전환할 수 있습니다.



공용 클라우드 계정 추가

공용 클라우드 인벤토리를 추가하려면 공용 클라우드 계정을 NSX-T Data Center의 온-프레미스 배포와 연결하고, VPC/VNet에서 필수 서브넷을 생성하고, 공용 클라우드에 NSX Cloud에 대한 액세스를 허용하기 위한 역할을 생성해야 합니다.

이러한 단계는 특정 순서를 따르지 않으며 별도로 완료할 수 있습니다.

참고

- AWS용 Direct Connect, Microsoft Azure용 Express 경로, 온-프레미스에 VPN 끝점이 있는 사이트 간 VPN 및 공용 클라우드에서 VPN 끝점으로 작용하는 PCG 등, 적절한 방법을 사용하여 VPC/VNet을 온-프레미스에 연결합니다.
- 전송/계산 토폴로지를 사용하도록 선택하는 경우 전송 및 계산 VPC/VNet 간에 피어링 연결이 설정되어 있는지 확인합니다. 단일 PCG에서 여러 계산 VPC/VNet을 관리할 수 있습니다. 또한 각 VPC/VNet에 PCG 쌍이 설치된 플랫 계산 VPC/VNet 아키텍처를 유지하도록 선택할 수도 있습니다.

Microsoft Azure 네트워크를 온-프레미스 NSX-T Data Center 배포와 연결

Microsoft Azure 네트워크와 온-프레미스 NSX-T Data Center 장치 사이에 연결이 설정되어야 합니다.

참고 NSX Manager가 이미 설치되어 있고 온-프레미스 배포의 CSM과 연결되어 있어야 합니다.

개요

- Microsoft Azure 구독을 온-프레미스 NSX-T Data Center와 연결합니다.
- NSX Cloud에 필요한 CIDR 블록과 서브넷을 사용하여 VNet을 구성합니다.
- CSM 장치의 시간을 Microsoft Azure Storage 서버 또는 NTP와 동기화합니다.

Microsoft Azure 구독을 온-프레미스 NSX-T Data Center와 연결

모든 공용 클라우드는 온-프레미스 배포와 연결할 수 있는 옵션을 제공합니다. 요구 사항에 맞는 사용 가능한 연결 옵션을 선택할 수 있습니다. 자세한 내용은 **Microsoft Azure** 참조 설명서를 참조하십시오.

참고 Microsoft Azure에서 적용할 수 있는 보안 고려 사항 및 모범 사례를 검토하고 구현해야 합니다. 예를 들어 Microsoft Azure Portal 또는 API에 액세스 권한이 있는 모든 사용자 계정은 MFA(Multi Factor Authentication)를 사용하도록 설정해야 합니다. MFA는 정당한 사용자만 포털에 액세스할 수 있도록 하며 자격 증명이 도난 당하거나 유출된 경우 액세스 가능성을 줄입니다. 자세한 내용 및 권장 사항은 Microsoft Azure Security Center 설명서를 참조하십시오.

VNet 구성

Microsoft Azure에서 라우팅 가능한 CIDR 블록을 생성하고 필요한 서브넷을 설정합니다.

- 권장되는 범위가 /28 이상인 관리 서브넷 하나, 처리 대상:
 - 온-프레미스 장치에 대한 제어 트래픽
 - 클라우드 제공자 API 끝점에 대한 API 트래픽
- 워크로드 VM에 대해 권장되는 범위가 /24인 다운링크 서브넷 하나.
- VNet에서 나가고 들어오는 북-남 트래픽 라우팅을 위해, 권장되는 범위가 /24인 업링크 서브넷 하나, 또는 HA의 경우 둘.

이러한 서브넷이 사용되는 방법에 대한 자세한 내용은 **NSX Public Cloud Gateway 배포**의 내용을 참조하십시오.

Microsoft Azure 인벤토리에 대한 보안 액세스 설정

구독에서 NSX Cloud가 작동하려면 필요한 사용 권한을 부여하기 위한 서비스 사용자 그리고 CSM 및 PCG를 위한 역할을 Azure 리소스에 대한 ID를 관리하는 Microsoft Azure 기능에 따라 생성해야 합니다.

개요:

- Microsoft Azure 구독에는 NSX-T Data Center 관리 아래로 가져오려는 하나 이상의 계산 VNet이 포함되어 있습니다. VNet은 전송 모드 또는 계산 모드일 수 있습니다. 전송 VNet은 PCG가 배포되는 VNet입니다. 다른 VNet을 전송 VNet에 연결하고 해당 VNet에 호스팅된 워크로드 VM을 등록할 수 있습니다. 전송 VNet에 연결된 VNet을 계산 VNet이라고 합니다.
- NSX Cloud는 서비스 사용자 및 Microsoft Azure 자격 증명을 안전하게 유지하면서 인증 관리를 위해 Microsoft Azure의 관리 ID 기능을 사용하는 역할을 생성하는 PowerShell 스크립트를 제공합니다. 이 스크립트를 사용하면 여러 구독을 하나의 서비스 사용자에 포함할 수도 있습니다.
- 서비스 사용자를 모든 구독에 재사용하거나, 필요에 따라 새로운 서비스 사용자를 생성할 수 있습니다. 추가 구독에 대해 별도의 서비스 사용자를 생성하려는 경우에 사용할 수 있는 스크립트가 별도로 준비되어 있습니다.
- 사용하는 서비스 사용자 개수에 관계 없이 구독이 여러 개인 경우에는 CSM 및 PCG 역할에 대한 JSON 파일을 업데이트하여, 추가되는 각 구독의 이름을 *AssignableScopes* 섹션 아래에 추가해야 합니다.

- VNet에 NSX Cloud 서비스 사용자가 이미 있는 경우에는 매개 변수에서 서비스 사용자 이름을 비워둔 채로 스크립트를 다시 실행하여 업데이트할 수 있습니다.
- 서비스 사용자 이름은 Microsoft Azure Active Directory에서 고유해야 합니다. 동일한 Active Directory 도메인 아래의 서로 다른 구독에서 동일한 서비스 사용자를 사용하거나 구독별로 서로 다른 서비스 사용자를 사용할 수 있습니다. 하지만 동일한 이름으로 두 개의 서비스 사용자를 생성할 수는 없습니다.
- Microsoft Azure 구독 소유자이거나, Microsoft Azure 구독에 역할을 생성하고 할당할 수 있는 사용 권한이 있어야 합니다.
- 지원되는 시나리오는 다음과 같습니다.
 - **시나리오 1:** NSX Cloud에서 하나의 Microsoft Azure 구독 사용
 - **시나리오 2:** 동일한 Microsoft Azure Directory에 있는 여러 개의 Microsoft Azure 구독을 NSX Cloud에서 사용하되, 모든 구독에 대해 하나의 NSX Cloud 서비스 사용자 사용
 - **시나리오 3:** 동일한 Microsoft Azure Directory에 있는 여러 개의 Microsoft Azure 구독을 NSX Cloud에서 사용하되, 구독마다 서로 다른 NSX Cloud 서비스 사용자 사용

다음은 프로세스 개요입니다.

- 1 NSX Cloud PowerShell 스크립트를 사용하여 다음을 수행합니다.
 - NSX Cloud에 대한 서비스 사용자 계정을 생성합니다.
 - CSM에 대한 역할을 생성합니다.
 - PCG에 대한 역할을 생성합니다.
- 2 (선택 사항) 연결하려는 다른 구독에 사용할 서비스 사용자를 생성합니다.
- 3 CSM에서 Microsoft Azure 구독을 추가합니다.

참고 여러 개의 구독을 사용하는 경우에는 동일한 서비스 사용자를 사용하든 서로 다른 서비스 사용자를 사용하든 CSM에서 각 구독을 별도로 추가해야 합니다.

서비스 사용자 및 역할 생성

NSX Cloud는 하나 이상의 구독에 필요한 서비스 사용자 및 역할을 생성할 수 있는 PowerShell 스크립트를 제공합니다.

사전 요구 사항

- AzureRM 모듈이 설치된 PowerShell 5.0 이상이 필요합니다.
- Microsoft Azure 구독 소유자이거나, Microsoft Azure 구독에 역할을 생성하고 할당할 수 있는 사용 권한이 있어야 합니다.

참고 스크립트를 처음 실행할 때 Microsoft Azure의 응답 시간으로 인해 스크립트가 실패할 수 있습니다. 스크립트가 실패하면 다시 실행해 보십시오.

절차

- 1 Windows 데스크톱 또는 서버에서, 이름이 **CreateNSXCloudCredentials.zip**인 ZIP 파일을 NSX-T Data Center **다운로드 페이지 > 드라이버 및 도구 > NSX Cloud 스크립트 > Microsoft Azure**에서 다운로드합니다.
- 2 Windows 시스템에서 ZIP 파일의 다음 콘텐츠를 추출합니다.

스크립트/파일	설명
CreateNSXRoles.ps1	NSX Cloud 서비스 사용자와 CSM 및 PCG에 대한 관리 ID 역할을 생성하는 PowerShell 스크립트입니다. 이 스크립트에는 다음 매개 변수가 사용됩니다. <ul style="list-style-type: none"> ■ <code>-subscriptionId <the Transit_VNet's_Azure_subscription_ID></code> ■ (선택 사항) <code>-servicePrincipalName <Service_Principal_Name></code> ■ (선택 사항) <code>-useOneServicePrincipal</code>
AddServicePrincipal.ps1	구독을 여러 개 추가하고 각 구독에 서로 다른 서비스 사용자를 할당하려는 경우에 필요한 선택적 스크립트입니다. 아래의 단계에서 시나리오 3 을 참조하십시오. 이 스크립트에는 다음 매개 변수가 사용됩니다. <ul style="list-style-type: none"> ■ <code>-computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID></code> ■ <code>-transitSubscriptionId <the Transit_VNet's_Azure_Subscription_ID></code> ■ <code>-csmRoleName <CSM_Role_Name></code> ■ <code>-servicePrincipalName <Service_Principal_Name></code>
nsx_csm_role.json	CSM 역할 이름 및 사용 권한에 맞는 JSON 템플릿입니다. 이 파일은 PowerShell 스크립트에 대한 입력으로 필요하며, 스크립트와 동일한 폴더에 있어야 합니다.
nsx_pcg_role.json	PCG 역할 이름 및 사용 권한에 맞는 JSON 템플릿입니다. 이 파일은 PowerShell 스크립트에 대한 입력으로 필요하며, 스크립트와 동일한 폴더에 있어야 합니다. <p>참고 기본 PCG(게이트웨이) 역할 이름은 <code>nsx-pcg-role</code>입니다. CSM에서 구독을 추가할 때 이 값을 제공해야 합니다.</p>

3 시나리오 1: NSX Cloud에서 하나의 Microsoft Azure 구독 사용

- a PowerShell 인스턴스에서 Microsoft Azure 스크립트 및 JSON 파일을 다운로드한 디렉토리로 이동합니다.
- b 다음과 같이 `-SubscriptionId` 매개 변수를 지정하여 `CreateNSXRoles.ps1` 스크립트를 실행합니다.

```
.\CreateNSXRoles.ps1 -subscriptionId <the_single_Azure_subscription_ID>
```

참고 기본 서비스 사용자 이름인 `nsx-service-admin`을 재정의하려면 `-servicePrincipalName` 매개 변수도 함께 사용할 수 있습니다. 서비스 사용자 이름은 Microsoft Azure Active Directory에서 고유해야 합니다.

4 시나리오 2: 동일한 Microsoft Azure Directory에 있는 여러 개의 Microsoft Azure 구독을 NSX Cloud에서 사용하되, 모든 구독에 대해 하나의 NSX Cloud 서비스 사용자 사용

- a PowerShell 인스턴스에서 Microsoft Azure 스크립트 및 JSON 파일을 다운로드한 디렉토리로 이동합니다.
- b 각 JSON 파일을 편집하여 다음과 같이 **"AssignableScopes"**라는 섹션 제목 아래에 기타 구독 ID의 목록을 추가합니다.

```
"AssignableScopes": [
  "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",
  "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-ffffffffffff",
  "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-000000000000"
```

참고 이 예제에 나와 있는 형식(`"/subscriptions/<Subscription_ID>"`)을 사용하여 구독 ID를 추가해야 합니다.

- c `-subscriptionID` 및 `-useOneServicePrincipal` 매개 변수를 사용하여 이름이 `CreateNSXRoles.ps1`인 스크립트를 실행합니다.

```
.\CreateNSXRoles.ps1 -subscriptionId <the_Transit_VNet's_Azure_subscription_ID>
-useOneServicePrincipal
```

참고 기본 이름인 `nsx-service-admin`을 사용하려는 경우에는 여기에서 서비스 사용자 이름을 생략합니다. 이 서비스 사용자 이름이 Microsoft Azure Active Directory에 이미 존재하는 경우, 서비스 사용자 이름 없이 이 스크립트를 실행하면 해당 서비스 사용자가 업데이트됩니다.

5 시나리오 3: 동일한 Microsoft Azure Directory에 있는 여러 개의 Microsoft Azure 구독을 NSX Cloud에서 사용하되, 구독마다 서로 다른 NSX Cloud 서비스 사용자 사용

- a PowerShell 인스턴스에서 Microsoft Azure 스크립트 및 JSON 파일을 다운로드한 디렉토리로 이동합니다.
- b 시나리오 2의 **b** 단계와 **c** 단계를 수행하여 각 JSON 파일의 **AssignableScopes** 섹션에 여러 구독을 추가합니다.

- c -subscriptionID 매개 변수를 사용하여 이름이 **CreateNSXRoles.ps1**인 스크립트를 실행합니다.

```
.\CreateNSXRoles.ps1 -subscriptionId <One of the subscription_IDs>
```

참고 기본 이름인 **nsx-service-admin**을 사용하려는 경우에는 여기에서 서비스 사용자 이름을 생략합니다. 이 서비스 사용자 이름이 **Microsoft Azure Active Directory**에 존재하는 경우, 서비스 사용자 이름 없이 이 스크립트를 실행하면 해당 서비스 사용자가 업데이트됩니다.

- d 다음 매개 변수를 사용하여 이름이 **AddServicePrincipal.ps1**인 스크립트를 실행합니다.

매개 변수	값
-computeSubscriptionId	계산 VNet의 Azure 구독 ID
-transitSubscriptionId	전송 VNet의 Azure 구독 ID
-csmRoleName	nsx_csm_role.JSON 파일에서 이 값을 가져옵니다.
-servicePrincipalName	새 서비스 사용자 이름

```
./AddServicePrincipal.ps1 -computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID>
-transitSubscriptionId <the_Transit_VNet's_Azure_Subscription_ID>
-csmRoleName <CSM_Role_Name>
-servicePrincipalName <new_Service_Principal_Name>
```

- 6 PowerShell 스크립트를 실행한 디렉토리에서 파일을 찾습니다. 이름은 **NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name>**과 같습니다. 이 파일에는 CSM에서 Microsoft Azure 구독을 추가하는 데 필요한 정보가 포함되어 있습니다.

- 클라이언트 ID
- 클라이언트 키
- 테넌트 ID
- 구독 ID

결과

다음과 같은 항목이 생성됩니다.

- NSX Cloud에 대한 Azure AD 애플리케이션
- NSX Cloud 애플리케이션용 Azure Resource Manager 서비스 사용자
- 서비스 사용자 계정에 연결된 CSM에 대한 역할
- PCG가 공용 클라우드 인벤토리에서 작동할 수 있게 해 주는 PCG에 대한 역할.

- 이름이 `NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name>`인 파일(PowerShell 스크립트를 실행한 디렉토리에 생성됨). 이 파일에는 CSM에서 Microsoft Azure 구독을 추가하는 데 필요한 정보가 포함되어 있습니다.

참고 역할을 생성한 후 역할에서 사용할 수 있는 사용 권한의 목록을 보려면 CSM 및 PCG 역할을 생성하는 데 사용된 JSON 파일을 참조하십시오.

다음에 수행할 작업

CSM에서 Microsoft Azure 구독 추가

참고 NSX Cloud에서 여러 구독을 사용하도록 설정할 경우에는 개별 구독 각각을 CSM에 개별적으로 추가해야 합니다. 예를 들어, 구독이 총 5개라면 나머지 값은 모두 동일하고 구독 ID만 다른 Microsoft Azure 계정 5개를 CSM에 추가해야 합니다.

CSM에서 Microsoft Azure 구독 추가

NSX Cloud 서비스 사용자와 CSM 및 PCG 역할에 대한 세부 정보를 얻었다면 CSM에서 Microsoft Azure 구독을 추가할 준비가 된 것입니다.

사전 요구 사항

- NSX-T Data Center에 엔터프라이즈 관리자 역할이 있어야 합니다.
- NSX Cloud 서비스 사용자의 세부 정보가 포함된 PowerShell 스크립트 출력이 있어야 합니다.
- 역할 및 서비스 사용자를 생성하려면 PowerShell 스크립트를 실행할 때 제공한 PCG 역할의 값이 있어야 합니다. 기본값은 `nsx-pcg-role`입니다.

절차

- 1 엔터프라이즈 관리자 역할이 있는 계정을 사용하여 CSM에 로그인합니다.
- 2 **CSM > 클라우드 > Azure**로 이동합니다.
- 3 **+추가**를 클릭하고 다음 세부 정보를 입력합니다.

옵션	설명
이름	CSM에서 이 계정을 식별할 수 있는 적절한 이름을 제공합니다. 동일한 Microsoft Azure 테넌트 ID에 연결된 여러 Microsoft Azure 구독이 있을 수 있습니다. 계정 이름을 지정하고 CSM에서 적절하게 이름을 지정할 수 있습니다(예: Azure-DevOps-Account, Azure-Finance-Account 등).
클라이언트 ID	PowerShell 스크립트의 출력에서 이 값을 복사하여 붙여넣습니다.
키	PowerShell 스크립트의 출력에서 이 값을 복사하여 붙여넣습니다.
구독 ID	PowerShell 스크립트의 출력에서 이 값을 복사하여 붙여넣습니다.
테넌트 ID	PowerShell 스크립트의 출력에서 이 값을 복사하여 붙여넣습니다.

옵션	설명
게이트웨이 역할 이름	기본값은 <code>nsx-pcg-role</code> 입니다. 기본값을 변경했다면 이 값은 <code>"nsx_pcg_role.json"</code> 파일에서 확인할 수 있습니다.
클라우드 태그	기본적으로 이 옵션은 사용하도록 설정되어 있으며, 이 옵션을 사용하면 NSX Manager에서 Microsoft Azure 태그를 볼 수 있습니다.

4 저장을 클릭합니다.

CSM에 계정이 추가되면 3분 내에 **계정** 섹션에서 해당 계정을 볼 수 있습니다.

- 5 VM을 관리하려는 VNet에서 모든 VM을 화이트리스트에 추가합니다. 이 작업은 필수는 아니지만, [사용 안 함]을 [사용]으로 변경하면 격리 정책에 영향을 주므로 브라운필드 배포에 강력히 권장됩니다.

다음에 수행할 작업

[VNet에서 PCG 배포](#)

AWS(Amazon Web Services) 네트워크를 온-프레미스 NSX-T Data Center 배포와 연결

AWS(Amazon Web Services) 네트워크와 온-프레미스 NSX-T Data Center 장치 사이에 연결이 설정되어야 합니다.

참고 NSX Manager가 이미 설치되어 있고 온-프레미스 배포의 CSM과 연결되어 있어야 합니다.

개요

- 사용 가능한 옵션 중 요구 사항에 가장 적합한 옵션을 사용하여 AWS 계정을 온-프레미스 NSX Manager 장치와 연결합니다.
- NSX Cloud에 대한 서브넷 및 기타 요구 사항을 사용하여 VPC를 구성합니다.

AWS 계정을 온-프레미스 NSX-T Data Center 배포와 연결

모든 공용 클라우드 는 온-프레미스 배포와 연결할 수 있는 옵션을 제공합니다. 요구 사항에 맞는 사용 가능한 연결 옵션을 선택할 수 있습니다. 자세한 내용은 AWS 참조 설명서를 참조하십시오.

참고 AWS에서 적용할 수 있는 보안 고려 사항 및 모범 사례를 검토하고 구현해야 합니다. 자세한 내용은 AWS 보안 모범 사례를 참조하십시오.

VPC 구성

다음 구성이 필요합니다.

- 고가용성의 PCG를 지원하기 위한 6개의 서브넷
- IGW(인터넷 게이트웨이)
- 개인 및 공용 경로 테이블

- 경로 테이블과의 서브넷 연결
- 사용하도록 설정된 DNS 확인 및 DNS 호스트 이름

VPC를 구성하려면 다음 지침을 따르십시오.

- 1 VPC에서 /16 네트워크를 사용한다고 가정하면 배포가 필요한 각 게이트웨이에 대해 3개의 서브넷을 설정합니다.

중요 고가용성을 사용하는 경우라면 다른 가용성 영역에 3개의 서브넷을 추가로 설정하십시오.

- **관리 서브넷:** 이 서브넷은 온-프레미스 NSX-T Data Center 및 PCG 간 관리 트래픽에 사용됩니다. 권장 범위는 /28입니다.
- **업링크 서브넷:** 이 서브넷은 북-남 인터넷 트래픽에 사용됩니다. 권장 범위는 /24입니다.
- **다운링크 서브넷:** 이 서브넷은 워크로드 VM의 IP 주소 범위를 포함하므로 그에 따라 크기가 지정되어야 합니다. 디버깅을 위해 워크로드 VM에 추가 인터페이스를 통합해야 할 수도 있습니다.

참고 예를 들어 **management-subnet**, **uplink-subnet**, **downlink-subnet**과 같이 서브넷의 레이블을 적절하게 지정하십시오. 이 VPC에서 PCG를 배포할 때 서브넷을 선택해야 하기 때문입니다.

자세한 내용은 [NSX Public Cloud Gateway 배포](#) 항목을 참조하십시오.

- 2 VPC에 연결된 인터넷 게이트웨이(IGW)가 있는지 확인합니다.
- 3 VPC에 대한 라우팅 테이블의 대상이 0.0.0.0/0으로 설정되어 있고 대상이 VPC에 연결된 IGW인지 확인합니다.
- 4 VPC에 대해 DNS 확인 및 DNS 호스트 이름을 사용하도록 설정합니다.

AWS 인벤토리에 대한 보안 액세스 설정

NSX-T Data Center에서 관리하려는 VPC와 워크로드 VM이 있는 포함된 AWS 계정이 하나 이상 있을 수 있습니다.

개요:

- 전송/계산 VPC 토폴로지를 사용할 수 있습니다. 이는 PCG를 VPC 하나에 배포하여 전송 VPC로 만들고, 계산 VPC라고 하는 다른 VPC를 이 전송 VPC에 연결하는 방식입니다.
- NSX Cloud는 AWS 계정의 AWS CLI에서 실행하여 IAM 프로파일과 역할을 생성하고 전송 VPC와 계산 VPC 간의 신뢰 관계를 생성할 수 있는 셸 스크립트를 제공합니다.
- 지원되는 시나리오는 다음과 같습니다.
 - **시나리오 1:** NSX Cloud에서 하나의 AWS 계정 사용
 - **시나리오 2:** 마스터 AWS 계정으로 관리되는 여러 개의 AWS 하위 계정 사용
 - **시나리오 3:** NSX Cloud에서 여러 개의 AWS 계정 사용

다음은 프로세스 개요입니다.

- 1 AWS CLI가 필요한 NSX Cloud 셸 스크립트를 사용하여 다음을 수행합니다.
 - IAM 프로파일을 생성합니다.
 - PCG에 대한 역할을 생성합니다.
 - (선택 사항) 전송 VPC를 호스팅하는 AWS 계정과 계산 VPC를 호스팅하는 AWS 계정 사이에 신뢰 관계를 생성합니다.
- 2 CSM에서 AWS 계정을 추가합니다.

IAM 프로파일 및 PCG 역할 생성

NSX Cloud는 하나 이상의 AWS 계정을 설정할 수 있게 도움을 주는 셸 스크립트를 제공합니다. 이 스크립트는 IAM 프로파일 및 필요한 사용 권한을 AWS 계정에 제공하는 PCG 역할(프로파일에 연결됨)을 생성합니다.

두 개의 서로 다른 AWS 계정에 있는 여러 계산 VPC에 연결된 전송 VPC를 호스팅할 계획인 경우에는 스크립트를 사용하여 이들 계정 간에 신뢰 관계를 생성할 수 있습니다.

참고 기본적으로 PCG(게이트웨이) 역할 이름은 `nsx_pcg_service`입니다. 게이트웨이 역할 이름에 다른 값을 사용하고자 하면 스크립트에서 해당 이름을 변경할 수 있습니다. 하지만 이 값은 CSM에서 AWS 계정을 추가할 때 필요하므로 따로 기록해 두십시오.

사전 요구 사항

이 스크립트를 실행하려면 Linux 또는 호환 시스템에 다음이 설치 및 구성되어 있어야 합니다.

- AWS CLI
- jq(JSON 파서)
- openssl

참고 여러 개의 AWS 계정을 사용하는 경우에는 해당 계정을 적절한 방법으로 피어링해야 합니다.

절차

- 1 Linux나 호환되는 데스크톱 또는 서버에서, 이름이 `nsx_csm_iam_script.sh`인 셸 스크립트를 NSX-T Data Center **다운로드 페이지 > 드라이버 및 도구 > NSX Cloud 스크립트 > AWS**에서 다운로드합니다.
- 2 **시나리오 1: NSX Cloud에서 하나의 AWS 계정 사용**
 - a 스크립트를 실행합니다. 예를 들면 다음과 같습니다.

```
bash nsx_csm_iam_script.sh
```

- b Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no] 메시지가 표시되면 **yes**를 입력합니다.

- c What do you want to name the IAM User? 메시지가 표시되면 IAM 사용자의 이름을 입력합니다.

참고 IAM 사용자 이름은 AWS 계정에서 고유해야 합니다.

- d Do you want to add trust relationship for any Transit VPC account? [yes/no] 메시지가 표시되면 no를 입력합니다.

스크립트가 성공적으로 실행되면 AWS 계정에 PCG에 대한 IAM 프로파일과 역할이 생성됩니다. 값은 스크립트를 실행한 디렉토리에 있는 `aws_details.txt`라는 이름의 출력 파일에 저장됩니다. 다음으로 CSM에서 AWS 계정 추가에 나와 있는 지침을 수행한 후 VPC에 PCG 배포에 나와 있는 지침을 수행하여 전송 또는 자체 관리 VPC 설정 프로세스를 완료합니다.

3 시나리오 2: 하나의 마스터 AWS 계정으로 관리되는 여러 개의 AWS 하위 계정 사용

- a AWS 마스터 계정에서 스크립트를 실행합니다.

```
bash nsx_csm_iam_script.sh
```

- b Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no] 메시지가 표시되면 yes를 입력합니다.
- c What do you want to name the IAM User? 메시지가 표시되면 IAM 사용자의 이름을 입력합니다.

참고 IAM 사용자 이름은 AWS 계정에서 고유해야 합니다.

- d Do you want to add trust relationship for any Transit VPC account? [yes/no] 메시지가 표시되면 no를 입력합니다.

참고 마스터 AWS 계정을 사용하는 경우, 하위 계정의 계산 VPC를 볼 수 있는 권한이 전송 VPC에 있으면 하위 계정과의 신뢰 관계를 설정하지 않아도 됩니다. 그렇지 않은 경우에는 **시나리오 3**의 단계에 따라 계정을 여러 개 설정하십시오.

스크립트가 성공적으로 실행되면 AWS 마스터 계정에 IAM 프로파일 및 PCG에 대한 역할이 생성됩니다. 값은 스크립트를 실행한 디렉토리의 출력 파일에 저장됩니다. 파일 이름은 `aws_details.txt`입니다. 다음으로 CSM에서 AWS 계정 추가에 나와 있는 지침을 수행한 후 VPC에 PCG 배포에 나와 있는 지침을 수행하여 전송 또는 자체 관리 VPC 설정 프로세스를 완료합니다.

4 시나리오 3: NSX Cloud에서 여러 개의 AWS 계정 사용

참고 계속하기 전에 AWS 계정이 피어링되었는지 확인하십시오.

- a 전송 VPC를 호스팅하려는 AWS 계정의 12자리 AWS 계정 번호를 기록해 둡니다.
- b "시나리오 1"의 a-d단계에 따라 AWS 계정에 전송 VPC를 설정하고, CSM에 계정을 추가하는 프로세스를 완료합니다.

- c 계산 VPC를 호스팅하려는 다른 AWS 계정에서 Linux나 호환되는 시스템에 NSX Cloud 스크립트를 다운로드하고 실행합니다.

참고 또는 다른 계정 자격 증명을 가진 AWS를 사용하여 동일한 시스템에서 다른 AWS 계정에 대해 스크립트를 다시 실행할 수도 있습니다.

- d Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no] 메시지가 표시되면 yes를 입력합니다.

참고 이 AWS 계정을 CSM에 이미 등록한 상태에서 다른 AWS 계정에 연결하기 위해 스크립트를 다시 사용하려는 경우에는 no를 입력하여 IAM 사용자 생성을 건너뛸 수 있습니다.

- e What do you want to name the IAM User? 메시지가 표시되면 IAM 사용자의 이름을 입력합니다.

참고 IAM 사용자 이름은 AWS 계정에서 고유해야 합니다.

- f Do you want to add trust relationship for any Transit VPC account? [yes/no] 메시지가 표시되면 yes를 입력합니다.

- g What is the Transit VPC account number? 메시지가 표시되면 1단계에서 기록해 둔 12자리 AWS 계정 번호를 입력하거나 복사하여 붙여넣습니다.

스크립트를 통해 두 AWS 계정 간에 IAM 신뢰 관계가 설정되고 ExternalID가 생성됩니다.

스크립트가 성공적으로 실행되면 AWS 마스터 계정에 IAM 프로파일 및 PCG에 대한 역할이 생성됩니다. 값은 스크립트를 실행한 디렉토리의 출력 파일에 저장됩니다. 파일 이름은 `aws_details.txt`입니다. 다음으로 CSM에서 AWS 계정 추가에 나와 있는 지침을 수행한 후 전송 VPC/VNet에 연결에 나와 있는 지침을 수행하여 전송 VPC에 연결하는 프로세스를 완료합니다.

CSM에서 AWS 계정 추가

스크립트에 의해 생성된 값을 사용하여 AWS 계정을 추가합니다.

절차

- 1 엔터프라이즈 관리자 역할을 사용하여 CSM에 로그인합니다.
- 2 **CSM > 클라우드 > AWS**로 이동합니다.
- 3 **+추가**를 클릭하고 NSX Cloud 스크립트에서 생성된 출력 파일 `aws_details.txt`를 사용하여 다음 세부 정보를 입력합니다.

옵션	설명
이름	이 AWS 계정을 설명하는 이름을 입력합니다.
액세스 키	계정의 액세스 키를 입력합니다.
비밀 키	계정의 비밀 키를 입력합니다.

옵션	설명
클라우드 태그 검색	기본적으로 이 옵션은 사용하도록 설정되어 있으며, 이 옵션을 사용하면 NSX Manager에서 AWS 태그를 볼 수 있습니다.
게이트웨이 역할 이름	기본값은 <code>nsx_pcg_service</code> 입니다. "aws_details.txt" 파일의 스크립트 출력에서 이 값을 찾을 수 있습니다.

AWS 계정이 CSM에 추가됩니다.

CSM의 [VPC] 탭에서 AWS 계정의 모든 VPC를 볼 수 있습니다.

CSM의 [인스턴스] 탭에서 이 VPC의 EC2 인스턴스를 볼 수 있습니다.

- 4 VM을 관리하려는 VPC에서 모든 VM을 화이트리스트에 추가합니다. 이 작업은 필수는 아니지만, [사용 안 함]을 [사용]으로 변경하면 격리 정책에 영향을 주므로 브라운필드 배포에 강력히 권장됩니다.

다음에 수행할 작업

[VPC에 PCG 배포](#)

NSX Public Cloud Gateway 배포

NSX Public Cloud Gateway(PCG)는 공용 클라우드와 NSX-T Data Center의 온-프레미스 관리 구성 요소 간의 North-South 연결을 제공합니다.

워크로드 VM 관리를 위한 PCG의 아키텍처 및 배포 모드를 설명하는 다음 용어를 숙지하십시오.

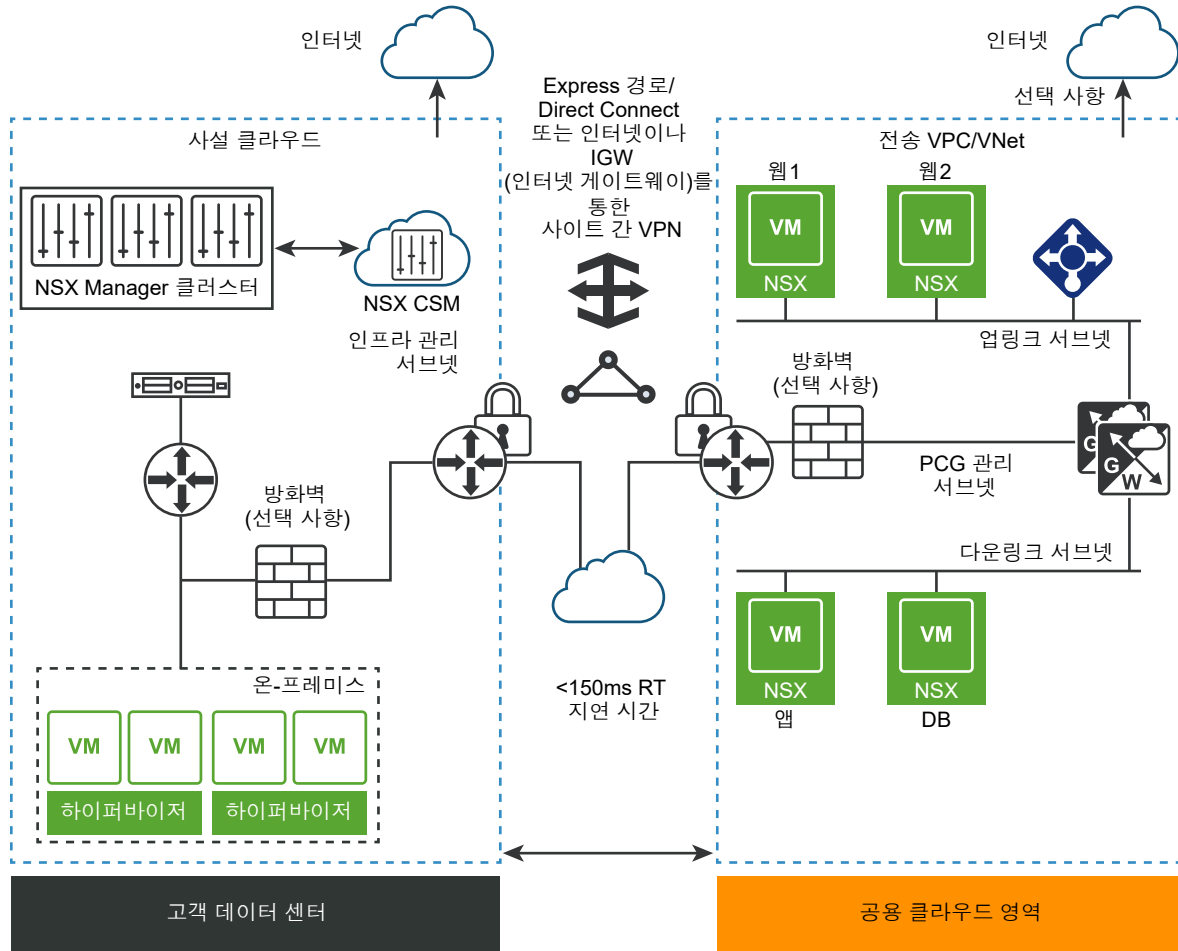
참고 PCG는 지원되는 각 공용 클라우드에 대해 단일 기본 크기로 배포됩니다.

공용 클라우드	PCG 인스턴스 유형
AWS	C4.xlarge 참고 일부 지역에서는 C4.xlarge 인스턴스 유형을 지원하지 않을 수 있습니다. 자세한 내용은 AWS 설명서를 참조하십시오.
Microsoft Azure	표준 DS3 v.2

아키텍처

PCG는 독립형 게이트웨이 장치로 사용되거나, 허브 및 스포크 토폴로지를 구축하기 위해 공용 클라우드 VPC/VNet 간에 공유될 수 있습니다.

그림 13-2. NSX Public Cloud Gateway 아키텍처



배포 모드

자체 관리 VPC/VNet: PCG를 VPC/VNet에 배포할 경우 해당 VPC/VNet은 "자체 관리" 될 수 있습니다. 즉, 이 VPC/VNet에 호스팅된 VM을 NSX에서 관리할 수 있습니다.

전송 VPC/VNet: 자체 관리 VPC/VNet은 계산 VPC/VNet에 연결하면 "전송" VPC/VNet이 됩니다.

계산 VPC/VNet: PCG가 배포되어 있지 않지만 전송 VPC/VNet에 연결하는 VPC/VNet을 "계산" VPC/VNet이라고 합니다.

VPC/VNet에서 PCG 배포에 필요한 서버넷

PCG는 VPC/VNet에서 설정한 다음 서버넷을 활용합니다. [Microsoft Azure 네트워크를 온-프레미스 NSX-T Data Center 배포와 연결](#) 또는 [AWS\(Amazon Web Services\) 네트워크를 온-프레미스 NSX-T Data Center 배포와 연결](#)의 내용을 참조하십시오.

- **관리 서버넷:** 이 서버넷은 온-프레미스 NSX-T Data Center 및 PCG 간 관리 트래픽에 사용됩니다. 권장 범위는 /28입니다.
- **업링크 서버넷:** 이 서버넷은 북-남 인터넷 트래픽에 사용됩니다. 권장 범위는 /24입니다.

- **다운링크 서브넷:** 이 서브넷은 워크로드 VM의 IP 주소 범위를 포함하므로 그에 따라 크기가 지정되어야 합니다. 디버깅을 위해 워크로드 VM에 추가 인터페이스를 통합해야 할 수도 있습니다.

PCG 배포는 네트워크 주소 지정 계획을 NSX-T Data Center 구성 요소에 대한 FQDN 및 이러한 FQDN을 확인할 수 있는 DNS 서버에 맞추어 조정합니다.

참고 PCG를 사용하여 NSX-T Data Center와 공용 클라우드를 연결할 때 IP 주소를 사용하는 것은 권장되지 않지만, IP 주소 사용을 선택하는 경우 IP 주소를 변경하지 마십시오.

VM 관리 모드

NSX 적용 모드: 이 모드에서는 AWS 또는 Microsoft Azure에서 태그 "nsx.network=default"가 적용된 후 각 워크로드 VM에 설치되어야 하는 NSX Tools를 사용하여 NSX 관리로 워크로드 VM을 가져옵니다.

기본 클라우드 적용 모드: 이 모드에서는 NSX Tools를 사용하지 않고 NSX 관리로 워크로드 VM을 가져올 수 있습니다.

격리 정책

격리 정책: 공용 클라우드 보안 그룹에서 작동하는 NSX Cloud의 위협 감지 기능입니다.

- NSX 적용 모드에서 격리 정책을 사용하거나 사용하지 않도록 설정할 수 있습니다. 워크로드 VM을 온보딩할 경우 격리 정책을 사용하지 않도록 설정하고 모든 VM을 화이트리스트에 추가하는 것이 좋습니다.
- 기본 클라우드 적용 모드 격리 정책은 항상 사용하도록 설정되며 사용하지 않도록 설정할 수 없습니다.

가능한 설계 옵션

PCG를 배포하는 모드와 관계없이, 두 모드 모두에서 계산 VPC/VNet과 연결할 수 있습니다.

표 13-3. 배포 모드가 PCG인 가능한 설계 옵션

전송 VPC/VNet의 PCG 배포 모드	계산 VPC/VNet을 이 전송 VPC/VNet에 연결할 때의 가능한 모드
NSX 적용 모드	<ul style="list-style-type: none"> ■ NSX 적용 모드 ■ 기본 클라우드 적용 모드
기본 클라우드 적용 모드	<ul style="list-style-type: none"> ■ NSX 적용 모드 ■ 기본 클라우드 적용 모드

참고 전송 또는 계산 VPC/VNet에 대해 선택한 모드는 변경할 수 없습니다. 모드를 전환하려는 경우에는 PCG의 배포를 해제하고 원하는 모드로 다시 배포해야 합니다.

VNet에서 PCG 배포

다음 지침에 따라 Microsoft Azure VNet에 PCG를 배포합니다.

PCG가 배포되는 VNet은 다른 VNet(계산 VNet이라고 함)이 연결할 수 있는 전송 VNet 역할을 할 수 있습니다. 이 VNet은 또한 VM을 관리하고 자체 관리 VNet 역할을 할 수 있습니다.

다음 지침에 따라 PCG를 배포합니다. 기존 전송 VNet에 연결하려면 [전송 VPC/VNet에 연결](#) 항목을 참조하십시오.

사전 요구 사항

- 공용 클라우드 계정이 CSM에 이미 추가되어 있어야 합니다.
- PCG를 배포 중인 VNet에 고가용성("업링크", "다운링크" 및 "관리")을 위해 필요한 서브넷이 적절하게 조정되어 있어야 합니다.

절차

- 1 엔터프라이즈 관리자 역할이 있는 계정을 사용하여 CSM에 로그인합니다.
- 2 **클라우드 > Azure**를 클릭하고 **VNet** 탭으로 이동합니다.
- 3 PCG를 배포할 VNet을 클릭합니다.
- 4 **게이트웨이 배포**를 클릭합니다. **게이트웨이 배포** 마법사가 열립니다.
- 5 일반 속성의 경우 다음 지침을 사용합니다.

옵션	설명
SSH 공용 키	PCG를 배포하는 동안 유효성을 검사할 수 있는 SSH 공용 키를 제공합니다. PCG 배포마다 필요합니다.
연결된 VNet의 격리 정책	NSX Tools(NSX 적용 모드)를 사용하여 워크로드 VM을 관리하도록 선택한 경우에만 격리 정책 설정을 변경할 수 있습니다. 격리 정책은 항상 기본 클라우드 적용 모드에서 사용하도록 설정합니다. PCG를 처음 배포할 때 기본 사용 안 함 모드를 유지합니다. 이 값은 VM을 등록한 후 변경할 수 있습니다. 자세한 내용은 "NSX-T Data Center 관리 가이드"의 격리 정책 관리 를 참조하십시오.
NSX Tools로 관리	기본값인 사용 안 함 상태를 유지하여 기본 클라우드 적용 모드에서 워크로드 VM을 온보딩합니다. NSX 적용 모드를 사용하기 위해 워크로드 VM에 NSX Tools를 설치하려는 경우 이 옵션을 사용하도록 설정합니다.
NSX Tools 자동 설치	이 기능은 [NSX Tools로 관리]를 사용하도록 설정한 경우에만 사용할 수 있습니다. 이 기능을 선택하면 <code>nsx.network=default</code> 태그를 적용한 경우 NSX Tools가 전송/자체 관리/연결된 계산 VNet의 모든 워크로드 VM에 자동으로 설치됩니다.
로컬 스토리지 계정	CSM에 Microsoft Azure 구독을 추가하면 Microsoft Azure Storage 계정 목록을 CSM에서 사용할 수 있습니다. 드롭다운 메뉴에서 스토리지 계정을 선택합니다. PCG 배포를 진행하면 CSM은 공개적으로 사용이 가능한 PCG의 VHD를 선택한 지역의 스토리지 계정으로 복사합니다.
참고 VHD 이미지가 이전 PCG 배포를 위해 이 지역의 스토리지 계정에 이미 복사된 경우에는 이후 배포 시 이 위치의 이미지가 사용되어 전체 배포 시간을 줄입니다.	

옵션	설명
VHD URL	공용 VMware 저장소에서 사용할 수 없는 다른 PCG 이미지를 사용하려면 여기에 PCG VHD의 URL을 입력하면 됩니다. VHD는 VNet이 생성된 지역 및 계정과 동일한 지역 및 계정에 있어야 합니다. 참고 VHD는 올바른 URL 형식이어야 합니다. Microsoft Azure의 클릭하여 복사 를 사용하는 것이 좋습니다.
프록시 서버	이 PCG의 인터넷 바운드 트래픽에 사용할 프록시 서버를 선택합니다. 프록시 서버는 CSM에서 구성됩니다. CSM과 동일한 프록시 서버(있는 경우)를 선택하거나, CSM과 다른 프록시 서버를 선택하거나, 프록시 서버 없음 을 선택할 수 있습니다. CSM에서 프록시 서버를 구성하는 방법에 대한 자세한 내용은 (선택 사항) 프록시 서버 구성 의 내용을 참조하십시오.
고급	고급 DNS 설정은 NSX-T Data Center 관리 구성 요소를 확인하기 위해 DNS 서버를 선택할 때 유연성을 제공합니다.
공용 클라우드 제공자의 DHCP를 통해 가져오기	Microsoft Azure DNS 설정을 사용하려면 이 옵션을 선택합니다. 이 옵션을 재정의하는 다른 옵션 중 하나를 선택하지 않는 경우 이것이 기본 DNS 설정입니다.
공용 클라우드 제공자의 DNS 서버 재정의	VNet의 워크로드 VM은 물론 NSX-T Data Center 장치를 확인하기 위해 DNS 서버 하나 이상의 IP 주소를 수동으로 제공하려면 이 옵션을 선택합니다.
NSX-T Data Center 장치에 대해서만 공용 클라우드 제공자의 DNS 서버 사용	Microsoft Azure DNS 서버를 사용하여 NSX-T Data Center 관리 구성 요소를 확인하려는 경우 이 옵션을 선택합니다. 이 설정을 사용하면 두 개의 DNS 서버를 사용할 수 있습니다. 하나는 NSX-T Data Center 장치를 확인하는 PCG용으로, 다른 하나는 VNet에서 워크로드 VM을 확인하는 VNet용입니다.

6 다음을 클릭합니다.

7 서브넷의 경우 다음 지침을 따릅니다.

옵션	설명
NSX Cloud 게이트웨이에 대해 HA 사용	고가용성을 사용하도록 설정하려면 이 옵션을 선택합니다.
서브넷	고가용성을 사용하도록 설정하려면 이 옵션을 선택합니다.
관리 NIC의 공용 IP	관리 NIC에 공용 IP 주소를 제공하려면 새 IP 주소 할당 을 선택합니다. 무료 공용 IP 주소를 다시 사용하려는 경우 공용 IP 주소를 수동으로 제공할 수 있습니다.
업링크 NIC의 공용 IP	업링크 NIC에 공용 IP 주소를 제공하려면 새 IP 주소 할당 을 선택합니다. 무료 공용 IP 주소를 다시 사용하려는 경우 공용 IP 주소를 수동으로 제공할 수 있습니다.

다음에 수행할 작업

"NSX-T Data Center 관리 가이드"의 [NSX Cloud 사용](#)에 나와 있는 지침을 따르십시오.

VPC에 PCG 배포

다음 지침에 따라 AWS VPC에 PCG를 배포합니다.

PCG가 배포되는 VPC는 다른 VPC(계산 VPC라고 함)가 연결할 수 있는 전송 VPC 역할을 할 수 있습니다. 이 VPC는 또한 VM을 관리하고 자체 관리 VPC 역할을 할 수 있습니다.

다음 지침에 따라 PCG를 배포합니다. 기존 전송 VPC에 연결하려면 [전송 VPC/VNet에 연결](#) 항목을 참조하십시오.

사전 요구 사항

- 공용 클라우드 계정이 CSM에 이미 추가되어 있어야 합니다.
- PCG를 배포 중인 VPC에고가용성("업링크", "다운링크" 및 "관리")을 위해 필요한 서브넷이 적절하게 조정되어 있어야 합니다.
- VPC의 네트워크 ACL에 대한 구성에는 허용 인바운드 규칙이 포함되어야 합니다.

절차

- 1 엔터프라이즈 관리자 역할이 있는 계정을 사용하여 CSM에 로그인합니다.
- 2 **클라우드 > AWS > <AWS_account_name>**을 클릭하고 **VPC** 탭으로 이동합니다.
- 3 **VPC** 탭에서 AWS 지역 이름을 선택합니다(예: **us-west**). AWS 지역은 계산 VPC를 생성한 지역과 동일해야 합니다.
- 4 NSX Cloud에 대해 구성된 계산 VPC를 선택합니다.
- 5 게이트웨이 배포를 클릭합니다.
- 6 일반 게이트웨이 세부 정보를 작성합니다.

옵션	설명
PEM 파일	드롭다운 메뉴에서 PEM 파일 중 하나를 선택합니다. 이 파일이 위치한 지역은 NSX Cloud가 배포된 지역 및 계산 VPC를 생성한 지역과 동일해야 합니다. 이것은 AWS 계정을 고유하게 식별합니다.
연결된 VPC의 격리 정책	NSX Tools(NSX 적용 모드)를 사용하여 워크로드 VM을 관리하도록 선택한 경우에만 격리 정책 설정을 변경할 수 있습니다. 격리 정책은 항상 기본 클라우드 적용 모드에서 사용하도록 설정합니다. PCG를 처음 배포할 때 기본 사용 안 함 모드를 유지합니다. 이 값은 VM을 등록한 후 변경할 수 있습니다. 자세한 내용은 "NSX-T Data Center 관리 가이드"의 격리 정책 관리 를 참조하십시오.
NSX Tools로 관리	기본값인 사용 안 함 상태를 유지하여 기본 클라우드 적용 모드에서 워크로드 VM을 온보딩합니다. NSX 적용 모드를 사용하기 위해 워크로드 VM에 NSX Tools를 설치하려는 경우 이 옵션을 사용하도록 설정합니다.
프록시 서버	이 PCG의 인터넷 바운드 트래픽에 사용할 프록시 서버를 선택합니다. 프록시 서버는 CSM에서 구성됩니다. CSM과 동일한 프록시 서버(있는 경우)를 선택하거나, CSM과 다른 프록시 서버를 선택하거나, 프록시 서버 없음 을 선택할 수 있습니다. CSM에서 프록시 서버를 구성하는 방법에 대한 자세한 내용은 (선택 사항) 프록시 서버 구성 의 내용을 참조하십시오.
고급	고급 설정은 필요한 경우 추가 옵션을 제공합니다.
AMI ID 재정의	AWS 계정에서 사용할 수 있는 AMI ID와 다른 AMI ID를 PCG에 제공하려면 이 고급 기능을 사용합니다.

옵션	설명
공용 클라우드 제공자의 DHCP를 통해 가져오기	AWS 설정을 사용하려면 이 옵션을 선택합니다. 이 옵션을 재정의하는 다른 옵션 중 하나를 선택하지 않는 경우 이것이 기본 DNS 설정입니다.
공용 클라우드 제공자의 DNS 서버 재정의	VPC의 워크로드 VM은 물론 NSX-T Data Center 장치를 확인하기 위해 DNS 서버 하나 이상의 IP 주소를 수동으로 제공하려면 이 옵션을 선택합니다.
NSX-T Data Center 장치에 대해서만 공용 클라우드 제공자의 DNS 서버 사용	AWS DNS 서버를 사용하여 NSX-T Data Center 관리 구성 요소를 확인하려는 경우 이 옵션을 선택합니다. 이 설정을 사용하면 두 개의 DNS 서버를 사용할 수 있습니다. 하나는 NSX-T Data Center 장치를 확인하는 PCG용으로, 다른 하나는 이 VPC에서 워크로드 VM을 확인하는 VPC용입니다.

7 다음을 클릭합니다.

8 서브넷 세부 정보를 작성합니다.

옵션	설명
공용 클라우드 게이트웨이에 대해 HA 사용	권장 설정은 [사용]으로, 예기치 않은 다운타임을 피하도록고가용성 활성/대기 쌍을 설정합니다.
기본 게이트웨이 설정	드롭다운 메뉴에서 HA를 위한 기본 게이트웨이로 us-west-1a 와 같은 가용성 영역을 선택합니다. 드롭다운 메뉴에서 업링크, 다운링크 및 관리 서브넷을 할당합니다.
보조 게이트웨이 설정	드롭다운 메뉴에서 HA를 위한 보조 게이트웨이로 us-west-1b 와 같은 다른 가용성 영역을 선택합니다. 보조 게이트웨이는 기본 게이트웨이에 장애가 발생할 때 사용됩니다. 드롭다운 메뉴에서 업링크, 다운링크 및 관리 서브넷을 할당합니다.
관리 NIC의 공용 IP	관리 NIC에 공용 IP 주소를 제공하려면 새 IP 주소 할당 을 선택합니다. 무료 공용 IP 주소를 다시 사용하려는 경우 공용 IP 주소를 수동으로 제공할 수 있습니다.
업링크 NIC의 공용 IP	업링크 NIC에 공용 IP 주소를 제공하려면 새 IP 주소 할당 을 선택합니다. 무료 공용 IP 주소를 다시 사용하려는 경우 공용 IP 주소를 수동으로 제공할 수 있습니다.

배포를 클릭합니다.

9 기본(및 선택한 경우 보조) PCG 배포의 상태를 모니터링합니다. 이 프로세스는 10-12분 정도 걸릴 수 있습니다.

10 PCG가 배포되면 완료를 클릭합니다.

다음에 수행할 작업

"NSX-T Data Center 관리 가이드"의 [NSX Cloud 사용](#)에 나와 있는 지침을 따르십시오.

전송 VPC/VNet에 연결

하나 이상의 계산 VPC/VNet을 전송 VPC/VNet에 연결할 수 있습니다.

사전 요구 사항

- PCG에 전송 VPC 또는 VNet이 있는지 확인합니다.

- 연결하려는 VPC/VNet이 VPN 또는 피어링을 통해 전송 VPC/VNet에 연결되어 있는지 확인합니다.
- 계산 VPC/VNet은 전송 VPC/VNet과 동일한 지역에 있는지 확인합니다.

참고 경로 기반 IPSec VPN 구성에서는 VTI(가상 터널 인터페이스) 포트의 IP 주소를 지정해야 합니다. 이 IP는 워크로드 VM과 다른 서브넷에 있어야 합니다. 이로 인해 워크로드 VM 인바운드 트래픽이 삭제될 VTI 포트로 전송되지 않게 됩니다.

참고 공용 클라우드에서는 보안 그룹당 인바운드/아웃바운드 규칙의 수에 대한 기본 제한이 존재하고 NSX Cloud는 기본 보안 그룹을 생성합니다. 이는 전송 VPC/VNet에 연결할 수 있는 계산 VPC/VNet의 개수에 영향을 줍니다. VPC/VNet당 1개의 CIDR 블록을 가정한다면 NSX Cloud는 전송 VPC/VNet당 10개의 계산 VPC/VNet을 지원합니다. 모든 계산 VPC/VNet에 2개 이상의 CIDR이 있는 경우 전송 VPC/VNet당 지원되는 계산 VPC/VNet 수가 줄어듭니다. 공용 클라우드 제공자에 연결하여 기본 제한을 조정할 수 있습니다.

절차

- 1 엔터프라이즈 관리자 역할이 있는 계정을 사용하여 CSM에 로그인합니다.
- 2 **클라우드 > AWS/Azure > <public cloud_account_name>**을 클릭하고 **VPC/VNet** 탭으로 이동합니다.
- 3 **VPC** 또는 **VNet** 탭에서 하나 이상의 계산 VPC/VNet을 호스팅하는 지역 이름을 선택합니다.
- 4 NSX Cloud에 대해 구성된 계산 VPC/VNet을 선택합니다.
- 5 **전송 VPC에 연결** 또는 **전송 VNet에 연결**을 클릭합니다.
- 6 **전송 VPC/VNet 연결** 창의 옵션을 완료합니다.

옵션	설명
전송 VPC/VNet	<p>드롭다운 메뉴에서 전송 VPC/VNet을 선택합니다. 선택하는 전송 VPC/VNet은 VPN 또는 피어링을 통해 이 VPC에 이미 연결되어 있어야 합니다.</p> <p>참고 전송 VNet에 연결하는 경우 해당 VNet에 DNS 전달자가 구성되어 있고 <code>nsx.dnsserver=<IP address of the DNS forwarder></code> 태그가 전송 VNet에 적용되어야 합니다. DNS 전달자 설정에 대한 자세한 내용은 Microsoft Azure 설명서를 참조하십시오.</p>
기본 격리 정책	<p>PCG를 처음 배포할 때 기본 사용 안 함 모드를 유지합니다. 이 값은 VM을 등록한 후 변경할 수 있습니다. 자세한 내용은 "NSX-T Data Center 관리 가이드"의 격리 정책 관리를 참조하십시오.</p>
NSX Tools로 관리	<p>기본값인 사용 안 함 상태를 유지하여 기본 클라우드 적용 모드에서 워크로드 VM을 온보딩합니다. NSX 적용 모드를 사용하기 위해 워크로드 VM에 NSX Tools를 설치하려는 경우 이 옵션을 사용하도록 설정합니다.</p>
NSX Tools 자동 설치	<p>이 방법은 NSX Tools를 사용해서 Microsoft Azure VNet에 대해서만 관리를 수행하도록 선택할 때만 사용할 수 있습니다. 이 기능을 선택하면 <code>nsx.network=default</code> 태그를 적용한 경우 NSX Tools가 전송/자체 관리/연결된 계산 VNet의 모든 워크로드 VM에 자동으로 설치됩니다.</p>

다음에 수행할 작업

"NSX-T Data Center 관리 가이드"의 [NSX Cloud 사용](#)에 나와 있는 지침을 따르십시오.

자동 생성된 논리적 엔티티 및 클라우드 기반 보안 그룹.

전송 VPC/VNet에 .PCG를 배포하고 여기에 계산 VPC/VNet을 연결하면 NSX-T Data Center 및 공용 클라우드에 필요한 구성이 트리거됩니다.

자동 생성된 NSX-T 논리적 엔티티

논리적 엔티티 집합은 NSX Manager에 자동 생성됩니다.

NSX Manager에 로그인하여 자동 생성된 논리적 엔티티를 확인합니다.

중요 PCG를 수동으로 배포 해제하는 경우를 제외하고 자동 생성된 엔티티는 삭제하지 마십시오. 자세한 내용은 [PCG 배포 해제 문제 해결](#) 항목을 참조하십시오.

시스템 엔티티

시스템 탭에 다음과 같은 엔티티가 표시됩니다.

표 13-4. 자동 생성된 시스템 엔티티

논리적 시스템 엔티티	생성 개수	명명법	범위
전송 영역	각 전송 VPC/VNet에 대해 2개의 전송 영역 생성	<ul style="list-style-type: none"> ■ TZ-<VPC/VNet-ID>-OVERLAY ■ TZ-<VPC/VNet-ID>-VLAN 	범위: 글로벌
Edge 전송 노드	배포된 각 PCG에 대해 1개의 Edge 전송 노드 생성(고가용성 모드로 배포된 경우 2개)	<ul style="list-style-type: none"> ■ PublicCloudGateway TN-<VPC/VNET-ID> ■ PublicCloudGateway TN-<VPC/VNET-ID>-preferred 	범위: 글로벌
Edge 클러스터	배포된 PCG당 1개의 Edge 클러스터 생성(PCG가 1개인지 고가용성 쌍인지에 관계없음)	PCG-cluster-<VPC/VNet-ID>	범위: 글로벌

인벤토리 엔티티

인벤토리 탭에서 다음 엔티티를 사용할 수 있습니다.

표 13-5. 그룹

그룹	범위
<p>다음 이름의 두 그룹:</p> <ul style="list-style-type: none"> ■ cloud-default-route ■ cloud-metadata services 	범위: 모든 PCG에서 공유
<p>계산 VPC/VNet 수준에 생성된 개별 세그먼트의 상위 그룹으로 전송 VPC/VNet 수준에 1개의 그룹이 생성됩니다. cloud-<Transit VPC/VNet ID>-all-segments</p>	범위: 모든 계산 VPC/VNet에서 공유
<p>각 Compute VPC/VNet의 두 그룹:</p> <ul style="list-style-type: none"> ■ 계산 VPC/VNet의 모든 CIDR을 위한 네트워크 CIDR 그룹: cloud-<Compute VPC/VNet ID>-cidr ■ 계산 VPC/VNet 내의 모든 관리되는 세그먼트를 위한 로컬 세그먼트 그룹: cloud-<Compute VPC/VNet ID>-local-segments 	범위: 모든 계산 VPC/VNet에서 공유
<p>현재 지원되는 공용 클라우드 서비스에 대해 다음 그룹이 생성됩니다.</p> <ul style="list-style-type: none"> ■ aws-dynamo-db-service-endpoint ■ aws-elb-service-endpoint ■ aws-rds-service-endpoint ■ aws-s3-service-endpoint ■ azure-cosmos-db-service-endpoint ■ azure-load-balancer-service-endpoint ■ azure-sql-service-endpoint ■ azure-storage-service-endpoint 	범위: 모든 PCG의 에서 공유

참고 기본 클라우드 적용 모드에 배포되었거나 연결된 PCG의 경우, VPC/VNet의 모든 워크로드 VM을 NSX Manager의 가상 시스템에서 사용할 수 있게 됩니다.

보안 엔티티

보안 탭에서 다음 엔티티를 사용할 수 있습니다.

표 13-6. 자동 생성된 보안 엔티티

논리적 보안 엔티티	생성 개수	명명법	범위
분산 방화벽(East-West)	<p>전송 VPC/VNet당 2개:</p> <ul style="list-style-type: none"> ■ 상태 비저장 ■ 상태 저장 	<ul style="list-style-type: none"> ■ cloud-stateless-<VPC/VNet ID> ■ cloud-stateful-<VPC/VNet ID> 	<ul style="list-style-type: none"> ■ 로컬로 관리되는 세그먼트 내에 트래픽을 허용하기 위한 상태 저장 규칙 ■ 관리되지 않는 VM에서 시작된 트래픽을 거부하기 위한 상태 저장 규칙
게이트웨이 방화벽(North-South)	전송 VPC/VNet당 1개	cloud-<Transit VPC/VNet ID>	

네트워킹 엔티티

다음 엔티티는 온보딩의 여러 단계에서 생성되며 **네트워킹** 탭에서 찾을 수 있습니다.

그림 13-3. PCG가 배포된 후 자동 생성된 NSX-T Data Center 네트워킹 엔티티

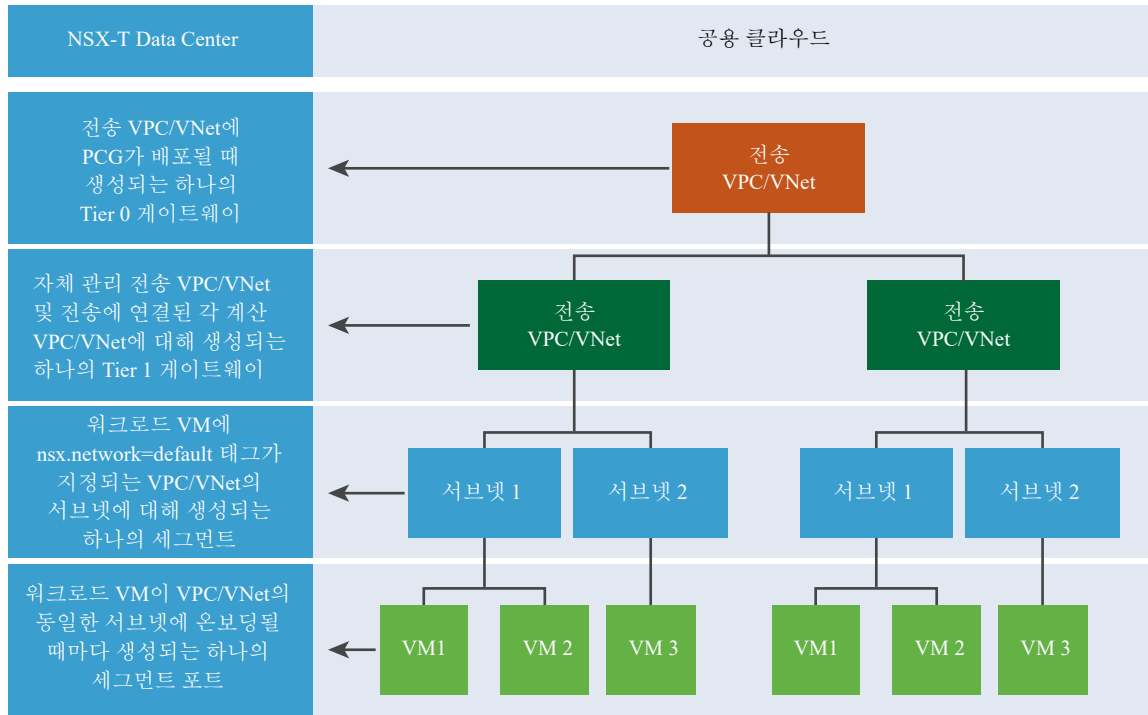


표 13-7. 자동 생성된 네트워킹 엔티티

온보딩 작업	NSX-T Data Center에 생성되는 논리적 엔티티
전송 VPC/VNet에 배포된 PCG	<ul style="list-style-type: none"> ■ Tier-0 게이트웨이 ■ 인프라 세그먼트(기본 VLAN 스위치) ■ Tier-1 라우터
전송 VPC/VNet에 연결된 계산 VPC/VNet	<ul style="list-style-type: none"> ■ Tier-1 라우터
계산 또는 자체 관리 VPC/VNet의 서브넷에서 NSX 에이전트가 설치되어 있는 워크로드 VM에는 "nsx.network:default" 키:값 태그가 지정됨	<ul style="list-style-type: none"> ■ 계산 또는 자체 관리 VPC/VNet의 이 특정 서브넷에 대해 세그먼트가 생성됨 ■ NSX 에이전트가 설치되어 있는 태그가 지정된 각 워크로드 VM에 하이브리드 포트가 생성됨
계산 또는 자체 관리 VPC/VNet의 동일 서브넷에서 더 많은 워크로드 VM에 태그가 지정됨	<ul style="list-style-type: none"> ■ NSX 에이전트가 설치되어 있는 태그가 지정된 각 워크로드 VM에 하이브리드 포트가 생성됨

전달 정책

자체 관리 전송 VPC/VNet을 포함하여, 계산 VPC/VNet에 대해 다음의 세 가지 전달 규칙이 설정됩니다.

- 동일한 계산 VPC의 모든 CIDR은 공용 클라우드의 네트워크(언더레이)를 통해 액세스합니다.
- 공용 클라우드 메타데이터 서비스와 관련된 트래픽은 공용 클라우드의 네트워크(언더레이)를 통해 라우팅합니다.
- 계산 VPC/VNet의 CIDR 블록에 포함되지 않은 모든 항목 또는 알려진 서비스는 NSX-T Data Center 네트워크(오버레이)를 통해 라우팅합니다.

자동 생성된 공용 클라우드 구성

공용 클라우드에서 일부 구성은 PCG를 배포한 후 자동으로 설정됩니다.

두 모드 NSX 적용 모드 및 기본 클라우드 적용 모드의 공용 클라우드 구성

AWS에서:

- AWS VPC에서 새로운 A 유형 레코드 집합이 `nsx-gw.vmware.local`이라는 이름으로 Amazon Route 53의 개인 호스팅된 영역에 추가됩니다. 이 레코드에 매핑되는 IP 주소는 DHCP를 사용하여 AWS가 할당하는 PCG의 관리 IP 주소와 일치하며, 각 VPC마다 다릅니다. Amazon Route 53의 개인 호스팅된 영역에 있는 이 DNS 항목은 NSX Cloud가 PCG의 IP 주소를 확인하는 데 사용됩니다.

참고 Amazon Route 53이 개인 호스팅된 영역에 정의된 사용자 지정 DNS 도메인 이름을 사용할 경우 AWS의 VPC 설정에 대해 **DNS 확인** 및 **DNS 호스트 이름** 특성을 예로 설정해야 합니다.

- PCG의 업링크 인터페이스에 대한 보조 IP가 생성됩니다. AWS Elastic IP는 이 보조 IP 주소와 연결됩니다. 이 구성은 SNAT를 위한 것입니다.

기본 클라우드 적용 모드에서 다음이 적용됩니다.

PCG가 배포될 때 다음 보안 그룹이 생성됩니다.

워크로드 VM이 NSX Manager에서 그룹 및 해당 보안 정책이 일치하면 `nsx-<GUID>`와 같은 보안 그룹이 공용 클라우드에서 일치하는 각 보안 정책에 대해 생성됩니다.

참고 AWS에서 보안 그룹이 생성됩니다. Microsoft Azure에서 NSX Manager의 그룹에 해당하는 애플리케이션 보안 그룹이 생성되고, NSX Manager의 보안 정책에 해당하는 네트워크 보안 그룹이 생성됩니다.

보안 그룹 이름	Microsoft Azure에서 사용할 수 있습니까?	AWS에서 사용할 수 있습니까?	설명
vm-quarantine-sg	예	아니요	NSX-T의 보안 정책과 일치하지 않는 VM에 할당하기 위한 Microsoft Azure의 NSX Cloud 생성 보안 그룹
기본	아니요	예	NSX-T의 보안 정책과 일치하지 않는 VM에 할당하기 위해 NSX Cloud에서 사용하는 AWS의 기존 보안 그룹
vm-overlay-sg	예	예	VM 오버레이 보안 그룹(현재 릴리스에서는 사용되지 않음)

NSX 적용 모드 사용 시 PCG 인터페이스용으로 NSX Cloud에서 생성된 공용 클라우드 보안 그룹 **gw** 보안 그룹은 각각의 PCG 인터페이스에 적용됩니다.

표 13-8. NSX Cloud에서 PCG 인터페이스용으로 생성된 공용 클라우드 보안 그룹

보안 그룹 이름	Microsoft Azure에서 사용할 수 있습니까?	AWS에서 사용할 수 있습니까?	설명
gw-mgmt-sg	예	예	게이트웨이 관리 보안 그룹
gw-uplink-sg	예	예	게이트웨이 업링크 보안 그룹
gw-vtep-sg	예	예	게이트웨이 다운링크 보안 그룹

워크로드 VM에 대해 다음과 같은 보안 그룹이 생성됩니다.

표 13-9. NSX 적용 모드로 워크로드 VM용 NSX Cloud에서 생성된 공용 클라우드 보안 그룹

보안 그룹 이름	Microsoft Azure에서 사용할 수 있습니까?	AWS에서 사용할 수 있습니까?	설명
vm-quarantine-sg	예	아니요	NSX 적용 모드의 위협 감지 워크플로에 대한 Microsoft Azure의 NSX Cloud 생성 보안 그룹
기본	아니요	예	NSX 적용 모드의 위협 감지 워크플로를 위해 NSX Cloud에서 사용하는 AWS의 기존 보안 그룹
vm-underlay-sg	예	예	VM 비오버레이 보안 그룹
vm-overlay-sg	예	예	VM 오버레이 보안 그룹(현재 릴리스에서는 사용되지 않음)

(선택 사항) 워크로드 VM에 NSX Tools 설치

NSX 적용 모드를 사용하는 경우 워크로드 VM에서 NSX Tools 설치를 계속 진행합니다.

"NSX-T Data Center 관리 가이드"의 [NSX 적용 모드에서 VM 온보딩](#)에서 지침 및 자세한 내용을 참조하십시오.

PCG 배포 해제 또는 연결 해제

PCG 배포 해제 또는 연결 해제와 관련된 단계에 대한 이 개요를 참조하십시오.

NSX 적용 모드에서

- NSX 관리 워크로드 VM에서 `nsx.network=default` 태그를 제거합니다.
- 격리 정책이 NSX 적용 모드에서 사용하도록 설정된 경우 사용하지 않도록 설정합니다.
- NSX Cloud에서 풀백 보안 그룹으로 사용할 수 있는 보안 그룹을 공용 클라우드에 제공합니다.
- PCG와 연결된 모든 사용자 생성 논리적 엔티티를 삭제합니다.

기본 클라우드 적용 모드에서

- NSX Cloud에서 풀백 보안 그룹으로 사용할 수 있는 보안 그룹을 공용 클라우드에 제공합니다.
- PCG와 연결된 모든 사용자 생성 논리적 엔티티를 삭제합니다.

절차

1 공용 클라우드에서 `nsx.network` 태그 제거

PCG를 배포 해제할 수 있으려면 모든 VM이 관리되지 않는 상태여야 합니다.

2 격리 정책 사용 안 함, 풀백 보안 그룹 제공

두 모드, NSX 적용 모드 및 기본 클라우드 적용 모드에서 공용 클라우드에 새 또는 기존 보안 그룹을 준비한 후 CSM에서 풀백 보안 그룹으로 제공하여 PCG 배포 해제 또는 VPC/VNet 연결 해제를 계속 진행해야 합니다.

3 사용자 생성 논리적 엔티티 삭제

PCG와 연결된 모든 사용자 생성 논리적 엔티티가 삭제되어야 합니다.

4 CSM에서 배포 해제 또는 연결 해제

사전 요구 사항을 완료한 후 다음 지침에 따라 PCG를 배포 해제하거나 연결 해제하십시오.

5 PCG 배포 해제 문제 해결

PCG 배포 해제가 실패하면 공용 클라우드뿐만 아니라 NSX Manager에서 모든 NSX Cloud 생성 엔티티를 수동으로 삭제해야 합니다.

공용 클라우드에서 `nsx.network` 태그 제거

PCG를 배포 해제할 수 있으려면 모든 VM이 관리되지 않는 상태여야 합니다.

참고 이 내용은 NSX 적용 모드에만 적용됩니다.

공용 클라우드에서 VPC 또는 VNet으로 이동하고 관리되는 VM에서 `nsx.network=default` 태그를 제거합니다.

격리 정책 사용 안 함, 폴백 보안 그룹 제공

두 모드, NSX 적용 모드 및 기본 클라우드 적용 모드에서 공용 클라우드에 새 또는 기존 보안 그룹을 준비한 후 CSM에서 폴백 보안 그룹으로 제공하여 PCG 배포 해제 또는 VPC/VNet 연결 해제를 계속 진행해야 합니다.

NSX 적용 모드를 사용하는 경우 격리 정책을 이전에 사용하도록 설정했으면 사용하지 않도록 설정합니다.

참고 폴백 보안 그룹은 공용 클라우드에 있는 기존의 사용자 정의 보안 그룹이어야 합니다. NSX Cloud 보안 그룹은 폴백 보안 그룹으로 사용할 수 없습니다. NSX Cloud 보안 그룹의 목록에 대해서는 [자동 생성된 논리적 엔티티 및 클라우드 기반 보안 그룹](#)의 내용을 참조하십시오.

AWS에서 `default` 보안 그룹은 NSX Cloud에서 생성되지 않았기 때문에 폴백 보안 그룹으로 구성할 수 있습니다.

이미 폴백 보안 그룹을 제공했지만 계산 VPC/VNet을 연결 해제한 후 나중에 전송 VPC/VNet에 다시 연결한 경우 다른 폴백 보안 그룹을 구성해야 합니다.

NSX 적용 모드에서 격리 정책을 사용하도록 설정한 경우

격리 정책을 사용하도록 설정한 경우 NSX Cloud에서 정의된 공용 클라우드의 보안 그룹이 VM에 할당됩니다. PCG를 배포 해제할 때에는 격리 정책을 사용하지 않도록 설정하고 VM을 NSX Cloud 보안 그룹에서 제거할 때 VM을 할당할 수 있는 폴백 보안 그룹을 지정해야 합니다.

PCG를 배포 해제하려는 VPC 또는 VNet에 대해 격리 정책을 사용하지 않도록 설정하고 폴백 보안 그룹 ID를 제공합니다.

- CSM에서 VPC 또는 VNet으로 이동합니다.
- **작업 > 구성 편집**에서 **기본 격리**에 대한 설정을 해제합니다.
- VM이 할당될 폴백 보안 그룹의 값을 입력합니다.
- 이 VPC 또는 VNet에 있는 관리되지 않는 또는 격리된 모든 VM에는 폴백 보안 그룹이 할당됩니다.
- 모든 VM이 관리되지 않는 경우 폴백 보안 그룹에 할당됩니다.
- 격리 정책을 사용하지 않도록 설정하는 동안 관리되는 VM이 있는 경우 해당 VM은 NSX Cloud에서 할당된 보안 그룹을 유지합니다. 그러한 VM을 NSX 관리에서 제거하기 위해 처음으로 `nsx.network=default` 태그를 제거하면 이러한 VM에도 폴백 보안 그룹이 할당됩니다.

기본 클라우드 적용 모드를 사용하는 경우

폴백 보안 그룹 ID를 제공합니다.

- CSM에서 VPC 또는 VNet으로 이동합니다.
- **작업 > 구성 편집**을 클릭합니다.

- AWS의 보안 그룹 ID 또는 Microsoft Azure의 네트워크 보안 그룹 리소스 ID를 PCG가 배포 해제된 후에 VM을 할당할 수 있는 풀백 보안 그룹으로 입력합니다.

참고 화이트리스트에 추가된 VM의 경우 NSX Cloud는 아무 작업도 수행하지 않으므로 VM을 풀백 보안 그룹으로 이동하지 않습니다. 화이트리스트에 추가된 VM이 NSX Cloud 할당 보안 그룹에 있는 경우 지정된 풀백 보안 그룹에 수동으로 이동해야 합니다. 격리 정책을 사용 또는 사용하지 않도록 설정하기 위한 지침과 그에 따른 영향에 대한 자세한 내용은 "NSX-T Data Center 관리 가이드"의 [NSX Cloud 격리 정책을 사용하여 위협 감지](#)를 참조하십시오.

사용자 생성 논리적 엔티티 삭제

PCG와 연결된 모든 사용자 생성 논리적 엔티티가 삭제되어야 합니다.

PCG와 연결된 엔티티를 식별한 후 삭제합니다.

참고 자동 생성된 논리적 엔티티는 삭제하지 마십시오. CSM에서 **배포 해제** 또는 **전송 VPC/VNet에서 연결 해제**를 클릭하면 이러한 엔티티가 자동으로 삭제됩니다. 자세한 내용은 [자동 생성된 논리적 엔티티 및 클라우드 기반 보안 그룹](#) 항목을 참조하십시오.

CSM에서 배포 해제 또는 연결 해제

사전 요구 사항을 완료한 후 다음 지침에 따라 PCG를 배포 해제하거나 연결 해제하십시오.

1 CSM에 로그인하고 공용 클라우드로 이동합니다.

- AWS를 사용 중인 경우 **클라우드 > AWS > VPC**로 이동합니다. 하나 또는 한 쌍의 PCG가 배포되어 실행 중인 VPC를 클릭합니다.
- Microsoft Azure를 사용 중인 경우 **클라우드 > Azure > VNet**으로 이동합니다. 하나 또는 한 쌍의 PCG가 배포되어 실행 중인 VNet을 클릭합니다.

2 **배포 해제** 또는 **전송 VPC/VNet에서 연결 해제**를 클릭합니다.

PCG를 배포 해제하거나 연결 해제하면 NSX Cloud에서 생성된 기본 엔티티가 자동으로 제거됩니다.

PCG 배포 해제 문제 해결

PCG 배포 해제가 실패하면 공용 클라우드뿐만 아니라 NSX Manager에서 모든 NSX Cloud 생성 엔티티를 수동으로 삭제해야 합니다.

- 공용 클라우드에서:
 - 전송 VPC/VNet에서 모든 PCG를 종료합니다.
 - 모든 워크로드 VM을 NSX Cloud에서 생성되지 않은 보안 그룹으로 이동합니다.
 - 다음 목록에 나와 있는 것처럼 공용 클라우드에서 NSX Cloud 생성 보안 그룹을 삭제합니다. [자동 생성된 공용 클라우드 구성](#)

- Microsoft Azure의 경우, **nsx-gw-<vnet ID>-rg**라는 NSX Cloud 생성 리소스 그룹도 삭제합니다.
- CSM에서 공용 클라우드 인벤토리를 다시 동기화합니다.
- 다음에 나열된 대로 NSX Manager에서 VPC/VNet ID가 있는 자동 생성된 엔티티를 삭제합니다. 자동 생성된 NSX-T 논리적 엔티티.

참고 자동 생성된 전역 엔티티는 삭제하지 마십시오. 이름에 VPC/VNet ID가 있는 항목만 삭제하십시오.

NSX Intelligence 설치 및 구성

14

VMware NSX® Intelligence™ 는 온 프레미스 NSX-T Data Center 환경에서 발생한 보안 상태 및 네트워크 트래픽 흐름을 시각화하는 그래픽 사용자 인터페이스를 제공합니다.

NSX Intelligence는 NSX-T Data Center 버전 2.5로 시작하는 ESXi 기반 호스트에서 사용할 수 있습니다. 이 제품은 다음과 같은 기능을 제공합니다.

- NSX-T Data Center에서 그룹, VM 및 네트워크 흐름과 같은 NSX-T 구성 요소의 그래픽 시각화. 사용되는 데이터는 지정된 기간에 집계된 네트워크 흐름을 기준으로 합니다.
- 애플리케이션의 보안 정책, 정책 보안 그룹 및 서비스에 대한 권장 사항입니다. 권장 사항은 애플리케이션 수준에서의 마이크로 크기만큼 세분화를 구현하도록 지원합니다. 이를 통해 NSX-T 데이터 센터 환경에서 VM 간에 발생하는 통신 트래픽 패턴에서 상관관계를 파악하여 보다 동적인 보안 정책을 적용할 수 있습니다.

NSX-T Data Center Enterprise Plus 라이선스가 있는 경우 또는 NSX-T Data Center 평가 라이선스가 있는 경우에는 평가 기간 중에 NSX Intelligence를 사용할 수 있습니다.

중요 NSX Intelligence를 설치, 구성 및 사용하기 위한 권한을 얻으려면 엔터프라이즈 관리자 역할이 있어야 합니다.

NSX Intelligence 장치는 두 가지 배포 시나리오에서 사용할 수 있습니다. 작은 장치는 랩 또는 개념 증명 배포 또는 소규모 운영 환경에 사용할 수 있습니다. 대규모 운영 환경에는 큰 장치를 사용할 수 있습니다.

[NSX Intelligence 시스템 요구 사항](#) 항목을 참조하십시오.

NSX Intelligence 기능을 사용하도록 설정하려면 NSX-T Data Center 장치와는 별도로 제공되는 NSX Intelligence 장치를 설치해야 합니다. NSX Manager UI(사용자 인터페이스)를 사용하여 NSX Intelligence 장치를 설치합니다. [NSX Intelligence 장치 설치](#) 항목을 참조하십시오.

NSX Intelligence 장치를 성공적으로 설치 및 구성한 후 NSX Manager UI의 **계획 및 문제 해결 > 검색 및 계획** 탭을 사용하여 NSX Intelligence 기능에 액세스합니다. "NSX-T Data Center 관리 가이드"에서 "NSX Intelligence 시작"을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [NSX Intelligence 설치 및 구성 워크플로](#)
- [NSX Intelligence 설치 준비](#)
- [NSX Intelligence 설치 관리자 번들 다운로드 및 압축 해제](#)

- [NSX Intelligence 장치 설치](#)
- [문제 해결 NSX Intelligence 장치 설치](#)
- [NSX Intelligence 장치 제거](#)

NSX Intelligence 설치 및 구성 워크플로

다음 체크리스트를 사용하여 NSX Intelligence 설치 진행률을 추적합니다.

나열된 순서대로 절차를 수행합니다.

- 1 ESXi 기반 호스트에 NSX-T Data Center 2.5 이상 버전을 설치합니다. VMware NSX® Intelligence™ 는 ESXi 기반 호스트에서만 지원됩니다. [장 2 NSX-T Data Center 설치 워크플로](#) 항목을 참조하십시오.
- 2 NSX Intelligence 시스템 요구 사항이 충족되었는지 확인합니다. [NSX Intelligence 시스템 요구 사항](#) 항목을 참조하십시오.
- 3 NSX Manager VM 및 NSX Intelligence 장치를 배포할 계산 클러스터의 시간을 동기화합니다.
- 4 로컬 웹 서버에 NSX Intelligence 설치 관리자 TAR 파일을 다운로드합니다. 이 TAR 파일에는 NSX Intelligence 장치를 설치하는 데 사용하는 NSX Intelligence OVF 파일이 포함되어 있습니다. [NSX Intelligence 설치 관리자 번들 다운로드 및 압축 해제](#) 항목을 참조하십시오.
- 5 NSX Intelligence 장치를 설치합니다. [NSX Intelligence 장치 설치](#) 항목을 참조하십시오.
- 6 NSX Manager UI에서 NSX Intelligence UI를 사용하도록 설정하려면 NSX Manager 세션에 사용 중인 웹 브라우저를 새로 고칩니다.
- 7 NSX Intelligence 기능 사용을 시작합니다. "NSX-T Data Center 관리 가이드"에서 "NSX Intelligence 시작"을 참조하십시오.

NSX Intelligence 설치 준비

NSX Intelligence를 설치하는 데 필요한 최소 시스템 요구 사항을 충족하도록 배포 환경을 준비해야 합니다.

다음 표에서는 NSX Intelligence 배포, 플랫폼 및 설치 요구 사항을 자세히 설명합니다.

요구 사항	설명
지원되는 배포 방법	OVF 계산 관리자로 추가된 VMware vCenter Server™에서 NSX Manager를 사용하여 배포됩니다. 중요 NSX Intelligence 장치는 NSX Manager만 사용하여 설치할 수 있으며, OVF가 독립적으로 설치될 때는 지원되지 않습니다.
지원되는 플랫폼	ESXi 호스트 관리자: vCenter Server
IP 주소	NSX Intelligence 장치에는 정적 IP 주소가 있어야 합니다. 설치 후에는 IP 주소를 변경할 수 없습니다.

요구 사항	설명
NSX Intelligence 장치 암호	<ul style="list-style-type: none"> ■ 12자 이상 ■ 하나 이상의 소문자 ■ 하나 이상의 대문자 ■ 하나 이상의 숫자 ■ 하나 이상의 특수 문자 ■ 5개 이상의 다른 문자 ■ 사전 단어 제외 ■ 회문 제외 ■ 4자를 초과하는 단조 문자 시퀀스는 허용되지 않습니다.
VMware Tools	ESXi 호스트에서 실행되는 NSX Intelligence VM는 VMTTools가 설치되어 있습니다. VMTTools를 제거하지 마십시오.
시스템	<ul style="list-style-type: none"> ■ 시스템 요구 사항이 충족되었는지 확인합니다. NSX Intelligence 시스템 요구 사항 항목을 참조하십시오. ■ 필수 포트가 열려 있는지 확인합니다. NSX Intelligence에서 사용되는 TCP 및 UDP 포트 항목을 참조하십시오. ■ 사용할 NSX Intelligence 장치의 관리 서브넷 및 게이트웨이에 대한 IP 주소, DNS 서버 IP 주소 및 NTP 서버 IP 주소 관련 정보를 가져옵니다. ■ SSD 기반 데이터스토어가 구성되어 있고 NSX Intelligence 장치에서 액세스 가능한지 확인합니다.

NSX Intelligence 시스템 요구 사항

NSX Intelligence 장치를 설치하기 전에 환경이 장치를 설치할 서버 호스트와 VM 시각화가 표시되는 클라이언트 모두에 대해 지원되는 최소 시스템 요구 사항을 충족하는지 확인하십시오.

NSX Intelligence 장치 리소스 요구 사항

다음 표에는 사용 가능한 NSX Intelligence 장치 크기 및 각각에 필요한 VM 리소스가 나열되어 있습니다. NSX Intelligence 작은 VM 장치 크기는 랩 및 개념 증명 배포 또는 소규모 운영 환경에 적합합니다. NSX Intelligence 대형 VM 장치 크기는 운영 환경에 적합합니다.

장치 크기	메모리	vCPU	디스크 용량
NSX Intelligence 소형	64 GB	16	2 TB
NSX Intelligence 대형	128 GB	32	2 TB

참고 NSX Manager 클러스터당 하나의 NSX Intelligence 장치만 지원됩니다.

NSX Intelligence 웹 클라이언트 메모리, CPU 및 브라우저 요구 사항

최적의 성능을 위해서 클라이언트 시스템에는 최소 2개의 1.4GHz CPU 코어와 최소 16GB RAM이 있어야 합니다.

다음 표에는 NSX Intelligence에 지원되는 웹 브라우저 버전이 나와 있습니다. 지원되는 최소 브라우저 해상도는 1280 x 800픽셀입니다.

브라우저	Windows 10	Mac OS X 10.14, 10.13	Ubuntu 18.4
Chrome 76	예	예	예
Firefox 68	예	예	예
Microsoft Edge 44	예	해당 없음	해당 없음

참고 Microsoft Edge를 사용할 때 알려진 성능 문제가 있습니다. 자세한 내용은 "NSX-T Data Center 릴리스 정보"를 참조하십시오.

NSX Intelligence에서 사용되는 TCP 및 UDP 포트

NSX Intelligence에서는 특정 TCP 및 UDP 포트를 사용하여 다른 구성 요소 및 제품과 통신합니다. 이러한 포트는 물리적 및 호스트 하이퍼바이저 방화벽 둘 다에서 열려 있어야 합니다.

중요 NSX Intelligence 노드에 원격으로 액세스하려면 해당 노드에서 SSH를 사용하도록 설정해야 합니다.

표 14-1. NSX Intelligence에서 사용되는 TCP 및 UDP 포트

소스	대상	포트	프로토콜	설명
NSX Intelligence	DNS 서버	53	TCP	DNS
NSX Intelligence	DNS 서버	53	UDP	DNS
NSX Intelligence	관리 SCP 서버	22	TCP	SSH(지원 번들, 백업 등 업로드)
NSX Intelligence	NTP 서버	123	UDP	NTP
NSX Intelligence	vCenter Server/NSX Unified Appliance	443	TCP	NSX Intelligence 계산 관리자(vCenter Server) 통신 및 NSX Unified Appliance(구성된 경우).
NSX Intelligence	NSX Unified Appliance/NSX 전송 노드	9092	TCP	NSX Unified Appliance 또는 전송 노드와의 NSX Intelligence 송신 통신
NTP 서버	NSX Intelligence	123	UDP	NTP
관리 클라이언트	NSX Intelligence	22	TCP	SSH(기본적으로 사용되지 않도록 설정됨)

표 14-1. NSX Intelligence에서 사용되는 TCP 및 UDP 포트 (계속)

소스	대상	포트	프로토콜	설명
관리 클라이언트/NSX Unified Appliance	NSX Intelligence	443	TCP	NSX API 서버
NSX Unified Appliance/전송 노드	NSX Intelligence	9092	TCP	NSX Unified Appliance 또는 전송 노드에서 NSX Intelligence 장치로 들어오는 메시지

NSX Intelligence 설치 관리자 번들 다운로드 및 압축 해제

NSX Intelligence 장치를 설치하려면 로컬 웹 서버에 NSX Intelligence 설치 관리자 번들 파일을 다운로드한 후 압축을 풉니다. 번들 파일에는 OVF 파일과 NSX Intelligence 장치를 설치하는 데 사용되는 다른 지원 파일이 포함됩니다.

사전 요구 사항

- NSX Intelligence를 사용할 권한이 있는지 확인합니다. NSX-T Data Center Enterprise Plus 라이선스가 있는 경우 또는 NSX-T Data Center 평가 라이선스가 있는 경우에는 평가 기간 중에 NSX Intelligence를 사용할 수 있습니다.
- NSX Intelligence를 설치, 구성 및 사용하려면 엔터프라이즈 관리자 역할이 있어야 합니다.
- 다운로드하는 사용자에게 .tar 파일 콘텐츠를 로컬 웹 서버에 다운로드하고 압축을 풀 수 있는 적절한 사용 권한이 있는지 확인합니다.
- NSX Intelligence 설치 관리자 번들 파일을 다운로드하는 데 사용할 로컬 웹 서버에서 HTTP에 대해 기본 포트 80을 사용하고 있는지 확인합니다.

절차

- 1 VMware 다운로드 포털에서 NSX Intelligence 설치 관리자 장치 TAR 파일을 찾습니다.
- 2 NSX Manager 사용자 인터페이스에서 액세스할 수 있는 로컬 웹 서버 위치에 NSX Intelligence 설치 관리자 번들 파일을 다운로드한 후 저장합니다.

참고 현재 지원되는 웹 서버는 Windows의 경우는 IIS이고, Linux 또는 Mac OS의 경우는 Apache입니다. 선택한 다른 웹 서버를 사용할 수 있지만 IIS 및 Apache는 이러한 운영 체제에 대해 테스트되고 지원되는 웹 서버입니다.

설치 관리자 번들 파일 이름 형식은 VMware-NSX-Intelligence-appliance-<release-number>.<build-number>.tar입니다. 예: VMware-NSX-Intelligence-appliance-1.0.0.0.14303803.tar.

3 동일한 로컬 웹 서버 위치에 TAR 파일의 압축을 풉니다.

- a 지원되는 웹 서버 중 하나에서 TAR 파일 콘텐츠의 압축을 풀려면 다음 정보를 사용하십시오.

운영 체제	웹 서버	사용할 압축 풀기 도구
Windows	IIS	<p>7-Zip 애플리케이션</p> <p>7-Zip File Manager 사용자 인터페이스를 사용하거나 명령 프롬프트 창을 사용합니다. 예를 들어, 명령 프롬프트 창을 사용하여 예제 TAR 파일의 압축을 풀려면 다운로드된 NSX Intelligence TAR 파일이 있는 위치로 이동한 후 다음 명령을 입력합니다.</p> <pre>7z x VMware-NSX-Intelligence-appliance-1.0.0.0.14303803.tar</pre>
Linux	Apache	<p>tar 명령줄 유틸리티</p> <p>예를 들어, 예제 TAR 파일의 압축을 풀려면 명령 프롬프트에서 다음을 입력합니다.</p> <pre>tar -xvf VMware-NSX-Intelligence-appliance-1.0.0.0.14303803.tar</pre>
Mac OS	Apache	<p>tar 명령줄 유틸리티</p> <p>예를 들어, 예제 TAR 파일의 압축을 풀려면 Terminal 명령줄에서 다음을 입력합니다.</p> <pre>tar -xvf VMware-NSX-Intelligence-appliance-1.0.0.0.14303803.tar</pre>

이전 단계의 예제 번들 파일 이름을 사용할 경우 압축을 푼 콘텐츠에 다음 파일이 포함됩니다.

- nsx-intelligence-appliance-1.0.0.0.14303803.cert
- nsx-intelligence-appliance-1.0.0.0.14303803.mf
- nsx-intelligence-appliance-1.0.0.0.14303803.ovf
- nsx-intelligence-appliance.vmdk

- b 설치를 계속하기 전에 압축을 푼 파일의 체크섬이 매니페스트 파일에 명시된 것과 같은지 확인합니다.

4 다음 정보를 사용하여 사용 중인 웹 서버가 각 NSX Intelligence 설치 관리자 파일 유형에 사용할 MIME 유형에 맞게 설정되어 있는지 확인합니다. 필요한 경우 웹 서버를 수동으로 업데이트합니다.

NSX Intelligence 설치 관리자 파일 유형	MIME 유형
.ovf	application/vmware
.vmdk	application/octet-stream
.mf	text/cache-manifest
.cert	application/x-x509-user-cert

5 NSX Intelligence OVF 파일의 파일 경로를 복사합니다. 예: `http://local-web-server/nsx-intelligence-appliance-1.0.0.0.14303803.ovf`. NSX Intelligence 장치 설치 프로세스 중에 이 경로를 제공합니다.

다음에 수행할 작업

NSX Intelligence 장치 설치를 계속 진행합니다. [NSX Intelligence 장치 설치](#) 항목을 참조하십시오.

NSX Intelligence 장치 설치

NSX Manager UI를 사용하여 NSX Intelligence 장치를 설치하고 구성합니다.

NSX Intelligence 기능 사용을 시작하려면 먼저 NSX Intelligence 장치를 설치하고 구성하여 NSX Intelligence 서비스 및 플러그인을 NSX Manager와 통합해야 합니다.

사전 요구 사항

- NSX-T Data Center 2.5 이상이 설치되어 있는지 확인합니다. [장 2 NSX-T Data Center 설치 워크플로](#) 항목을 참조하십시오.
- NSX Intelligence를 설치, 구성 및 사용하려면 엔터프라이즈 관리자 역할이 있어야 합니다.
- VMware 다운로드 포털에서 NSX Intelligence 설치 관리자 번들 파일을 찾은 후 로컬 웹 서버로 다운로드합니다. [NSX Intelligence 설치 관리자 번들 다운로드 및 압축 해제](#) 항목을 참조하십시오.
- NSX Intelligence 설치 관리자 번들 파일을 포함하는 로컬 웹 서버에서 HTTP에 대해 기본 포트 80을 사용하고 있는지 확인합니다.
- 구성할 NSX Intelligence 장치의 크기를 결정합니다. 작은 크기는 랩 또는 개념 증명 배포 또는 소규모 운영 환경을 위한 크기입니다. 대형 크기는 대규모 운영 환경에 적합합니다.
- NSX Intelligence 시스템 요구 사항이 설치하려는 장치 크기에 적합한지 확인합니다. [NSX Intelligence 시스템 요구 사항](#) 항목을 참조하십시오.
- NSX Intelligence 장치를 배포할 계산 클러스터의 시간을 NSX Manager 서버와 동기화합니다.
- NSX Intelligence 장치를 구성하는 데 필요한 관리 서브넷, 게이트웨이, DNS 서버 및 NTP 서버의 IP 주소를 가져옵니다.

절차

- 1 브라우저에서 엔터프라이즈 관리자 권한으로 <https://<nsx-manager-ip-address>>에서 NSX Manager에 로그인합니다.
- 2 NSX Manager에서 **시스템 > 장치**를 선택합니다.
- 3 [장치 개요] 창에서 아래로 스크롤하여 NSX Intelligence 장치 카드를 찾은 후 **NSX Intelligence 장치 추가**를 클릭합니다.
- 4 장치 추가 마법사에서 NSX Intelligence 장치 세부 정보를 입력합니다.

세부 항목	수행할 작업
OVF 파일	로컬 웹 서버에 다운로드한 NSX Intelligence OVF 파일의 URL을 입력합니다. 예: http://localhost/nsx-intelligence-appliance-1.1.0.0.13912394.ovf .
이름	NSX Intelligence 장치의 이름을 입력합니다. 이 값은 FQDN(정규화된 도메인 이름) 또는 단순한 이름(예: mytest-lab)일 수 있습니다.

세부 항목	수행할 작업
관리 서브넷	NSX Intelligence 장치에 사용할 IP 주소(범위 포함)를 입력합니다. 예: 10.11.22.33/24
게이트웨이 IP	사용할 NSX Intelligence 장치의 게이트웨이 IP 주소를 하나 입력합니다.
DNS 서버	하나 이상의 DNS 서버 IP 주소를 입력합니다.
NTP 서버	하나 이상의 NTP 서버 IP 주소를 입력합니다.
노드 크기	구성할 NSX Intelligence 장치 크기를 선택합니다. 작은 장치 크기는 랩 또는 개념 증명 환경 또는 소규모 운영 환경을 위한 크기입니다. 대형 장치 크기는 대규모 운영 환경에 적합합니다.

5 다음을 클릭합니다.

6 NSX Intelligence 장치를 배포할 위치에 대한 세부 정보를 입력합니다.

세부 항목	수행할 작업
계산 관리자	드롭다운 메뉴에서 NSX Intelligence 장치를 설치할 컴퓨터 관리자를 선택합니다.
클러스터	드롭다운 메뉴를 사용하여 사용할 클러스터를 선택합니다.
리소스 풀	(선택 사항) 드롭다운 메뉴에서 리소스 풀을 선택합니다.
호스트	<p>(선택 사항) 드롭다운 메뉴에서 호스트를 선택합니다. 여러 전송 노드가 있는 클러스터를 사용하는 경우 사용할 전송 노드를 결정합니다.</p> <p>참고 호스트를 명시적으로 선택하면 vCPU 수 검사가 재정의됩니다. 선택한 호스트에 설치하려는 NSX Intelligence 장치의 크기를 수용하는 데 vCPU 수가 충분한지 확인합니다. 호스트에 이러한 공간이 없으면 결과 NSX Intelligence 장치의 구성이 잘못될 수 있습니다. 확실치 않은 경우에는 텍스트 상자를 비워 두고 적절한 호스트가 자동으로 선택되도록 합니다.</p>
데이터스토어	드롭다운 메뉴에서 NSX Intelligence 구성 및 데이터를 저장할 데이터스토어를 선택합니다.
네트워크	드롭다운 메뉴에서 사용할 네트워크를 선택합니다.
SSH 사용 및 루트 액세스 사용	<p>NSX Intelligence 장치 CLI(명령줄 인터페이스)에 대해 SSH 액세스를 사용할지 아니면 루트 액세스를 사용할지 지정합니다.</p> <p>보안상의 이유로 이러한 옵션은 기본적으로 사용되지 않도록 설정됩니다. CLI를 사용하여 백업 파일 서버를 구성하고, NSX Intelligence 장치 구성을 백업하고, 백업을 복원합니다.</p>

7 다음을 클릭합니다.

8 관리자 자격 증명을 구성하고 NSX Intelligence 장치에 액세스합니다.

- a 루트 액세스를 사용하도록 설정하는 경우 루트 암호를 설정합니다. UI에 표시된 암호 요구 사항을 사용합니다.
- b CLI 자격 증명 및 감사 CLI 자격 증명을 구성합니다. CLI 암호 또는 감사 CLI 암호로 루트 암호를 사용하려면 **루트 암호와 동일**을 선택합니다. 그렇지 않은 경우 **CLI 암호** 및 **감사 CLI 암호**에 대한 암호를 입력합니다.

9 장치 설치를 클릭합니다.

설치 진행률이 **계획 및 문제 해결** 탭에 표시됩니다. 설치 관리자가 NSX Intelligence 장치에 필요한 모든 서비스와 플러그인을 검색하므로 설치에 5 ~ 30분이 소요될 수 있습니다.

참고 보고된 오류가 있는 경우 오류 메시지에 제공된 정보를 사용하여 보고된 문제를 해결합니다. 문제가 해결된 후에는 먼저 NSX Intelligence 장치를 제거하고 **시스템 > 장치** 탭에서 다시 설치해야 합니다. 발생할 수 있는 문제를 해결할 때 사용할 수 있는 힌트를 보려면 [NSX Intelligence 장치 제거](#) 또는 [문제 해결 NSX Intelligence 장치 설치](#) 항목도 참조하십시오.

10 NSX Intelligence 장치가 설치된 후 보기로 새로 고침을 클릭합니다.

NSX Manager UI는 NSX Intelligence 기능이 **계획 및 문제 해결 > 검색 및 계획** 탭에서 사용하도록 설정된 상태로 새로 고침됩니다.

다음에 수행할 작업

NSX Intelligence 기능 사용을 시작합니다. "NSX-T Data Center 관리 가이드"에서 "NSX Intelligence 사용"을 참조하십시오.

문제 해결 NSX Intelligence 장치 설치

이 섹션에서는 NSX Intelligence 장치를 설치할 때 발생할 수 있는 문제를 해결하기 위한 정보를 제공합니다.

자격 증명이 잘못되었거나 제공된 계정이 잠겨 있음

NSX Intelligence 장치를 배포하려고 하면 자격 증명이 잘못되었거나 지정된 계정이 잠겼습니다. 오류 메시지가 표시됩니다.

문제

NSX Intelligence 장치 설치 관리자를 실행한 후, 설치 관리자가 NSX Intelligence 서버를 NSX Manager에 등록하려고 하면 자격 증명이 잘못되었거나 지정된 계정이 잠겼습니다. 오류 메시지가 표시됩니다.

원인

다음 이유 중 하나로 인해 등록 단계가 실패할 수 있습니다.

- 관리부 토큰이 만료되었을 수 있습니다. 토큰은 30분 동안만 유효합니다.
- 시스템 시간이 NSX Intelligence 서버 호스트와 NSX Manager 호스트 간에 동기화되지 않았습니다.

해결책

- 1 시스템 시간이 NSX Intelligence 서버 호스트와 NSX Manager 호스트 간에 동기화되어 있는지 확인합니다.
- 2 시스템 시간이 동기화된 경우 네트워크 지연 시간이 있는지 확인합니다.
- 3 시스템 시간을 동기화하거나 네트워크 지연 시간이 해결되면 NSX Intelligence 장치를 제거하고 다시 설치합니다.

장치 배포에 대한 실패 상태가 지워지지 않음

NSX Intelligence 장치 배포가 성공적으로 수행되었으나 장치 배포 실패 상태가 표시됩니다.

문제

예를 들어, 리소스 부족 문제로 인해 NSX Intelligence 장치를 배포하려는 초기 시도가 실패하면 보고된 문제를 해결한 후에도 실패 배포 상태 메시지가 지워지지 않습니다.

원인

보고된 배포 문제의 근본 원인을 해결되었을 때 해당 해결 방법이 NSX Intelligence 장치 외부에서 수행되므로 NSX Intelligence 장치가 해결 사실을 알지 못합니다.

해결책

- 1 장치를 배포하려는 초기 시도 중에 보고된 문제를 해결한 후에 NSX Intelligence 장치를 제거하십시오.
- 2 **시스템 > 장치** 탭에서 NSX Intelligence 장치를 다시 설치하십시오.
- 3 (선택 사항) NSX Intelligence 장치의 업데이트된 배포 상태를 표시하려면 웹 브라우저를 새로 고치십시오.

NSX Intelligence 장치 제거

NSX Intelligence를 완전히 제거하려면 다음 단계를 사용합니다.

절차

- 1 브라우저에서 엔터프라이즈 관리자 권한으로 <https://<nsx-manager-ip-address>>에서 NSX Manager에 로그인합니다.
- 2 NSX Manager UI에서 **시스템 > 장치**를 선택합니다.
- 3 NSX Intelligence 장치 카드를 찾습니다.
- 4 **삭제**를 클릭합니다.
- 5 [장치 삭제 확인] 대화상자에서 **확인**을 클릭합니다.

NSX-T Data Center 설치 및 구성과 관련된 문제 목록

문제	솔루션
호스트 또는 클러스터에서 NSX-T를 제거한 후 vCenter Server 및/또는 ESXi 호스트가 불투명한 네트워크를 표시하고 있습니다.	https://kb.vmware.com/s/article/75234
ESXi 호스트의 부트 बैं크 공간 부족으로 설치에 실패함	https://kb.vmware.com/s/article/74864

본 장은 다음 항목을 포함합니다.

- [ESXi 호스트의 부트 बैं크 공간 부족으로 설치에 실패함](#)

ESXi 호스트의 부트 बैं크 공간 부족으로 설치에 실패함

ESXi 호스트의 부트 बैं크 또는 대체 부트 बैं크 공간이 부족하면 NSX-T Data Center 설치에 실패할 수 있습니다.

문제

ESXi 호스트에서 다음과 유사한 로그(esxupdate.log) 메시지가 표시될 수 있습니다.

```
20**-**-**T13:37:50Z esxupdate: 5557508: BootBankInstaller.pyc:
ERROR: The pending transaction requires 245 MB free space,
however the maximum supported size is 239 MB.^@
```

원인

ESXi 호스트에서 사용되지 않는 VIB의 크기가 비교적 커질 수 있습니다. 필요한 VIB를 설치할 경우 사용되지 않는 VIB로 인해 부트 बैं크 또는 대체 부트 बैं크 공간이 부족해질 수 있습니다.

해결책

- 더 이상 필요하지 않은 VIB를 제거하고 추가 디스크 공간을 확보하십시오.

사용되지 않는 VIB 삭제에 대한 자세한 내용은 <https://kb.vmware.com/s/article/74864>에서 VMware 기술 자료 문서를 참조하십시오.