

NSX-T Data Center 설치 가이드

수정 날짜: 2019년 4월 23일

VMware NSX-T Data Center 2.3



vmware®

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

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

VMware 웹 사이트에서는 최신 제품 업데이트도 제공합니다.

본 문서에 대한 의견이 있으시면 다음 주소로 피드백을 보내주십시오.

docfeedback@vmware.com

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

목차

NSX-T Data Center 설치 가이드 5

1 NSX-T Data Center 개요 6

관리부 7

제어부 9

데이터부 10

논리적 스위치 11

논리적 라우터 11

핵심 개념 12

2 설치 준비 16

시스템 요구 사항 16

포트 및 프로토콜 20

NSX-T Data Center 설치 상위 수준 작업 26

3 KVM 사용 28

KVM 설정 28

KVM CLI에서 게스트 VM 관리 33

4 NSX Manager 설치 35

NSX Manager 및 사용 가능한 장치 설치 37

명령줄 OVF 도구를 사용하여 ESXi에 NSX Manager 설치 39

KVM에 NSX Manager 설치 42

새로 생성된 NSX Manager 에 로그인 44

5 NSX Controller 설치 및 클러스터링 46

NSX Manager 에서 컨트롤러 및 클러스터의 자동화된 설치 48

GUI를 사용하여 ESXi에 NSX Controller 설치 55

명령줄 OVF 도구를 사용하여 ESXi에 NSX Controller 설치 57

KVM에 NSX Controller 설치 59

NSX Controller 를 NSX Manager 에 연결 62

제어 클러스터를 초기화하여 제어 클러스터 마스터 생성 63

클러스터 마스터에 추가 NSX Controller 연결 65

6 NSX Edge 설치 68

NSX Edge 네트워킹 설정 70

NSX Manager 에서 NSX Edge VM의 자동 배포 75

vSphere GUI를 사용하여 ESXi에 NSX Edge 설치 77

- 명령줄 OVF 도구를 사용하여 ESXi에 NSX Edge 설치 79
- PXE 서버와 ISO 파일을 사용하여 NSX Edge 설치 82
- NSX Edge 를 관리부에 연결 94

7 호스트 준비 96

- KVM 호스트 또는 베어메탈 서버에 타사 패키지 설치 96
- RHEL KVM 호스트의 Open vSwitch 버전 확인 99
- NSX-T Data Center 패브릭에 하이퍼바이저 호스트 또는 베어메탈 서버 추가 100
- NSX-T Data Center 커널 모듈의 수동 설치 104
- 하이퍼바이저 호스트를 관리부에 연결 108

8 전송 영역 및 전송 노드 111

- 전송 영역 정보 111
- 고급 데이터 경로 113
- 터널 끝점 IP 주소에 대한 IP 풀 생성 114
- 업링크 프로파일 생성 117
- 전송 영역 생성 121
- 호스트 전송 노드 생성 123
- 베어메탈 서버 워크로드를 위한 애플리케이션 인터페이스 생성 141
- Network I/O Control 프로파일 구성 142
- NSX Edge 전송 노드 생성 151
- NSX Edge 클러스터 생성 154

9 NSX Cloud 구성 요소 설치 156

- NSX Cloud 아키텍처 및 구성 요소 156
- NSX Cloud 구성 요소 설치 개요 157
- CSM 을 설치하고 NSX Manager 와 연결 159
- 공용 클라우드를 온-프레미스 배포와 연결 162
- 공용 클라우드 계정 추가 165
- PCG 배포 170
- PCG 배포 해제 175

10 NSX-T Data Center 제거 180

- NSX-T Data Center 오버레이 구성 해제 180
- NSX-T Data Center 에서 호스트 제거 또는 NSX-T Data Center 를 완전히 제거 180

NSX-T Data Center 설치 가이드

NSX-T Data Center 설치 가이드에서는 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.

VMware 기술 자료 용어집

VMware 기술 자료 사이트에서는 새로운 용어를 정리한 용어집을 제공하고 있습니다. VMware 기술 설명서에 사용된 용어에 대한 정의를 보려면 <http://www.vmware.com/support/pubs>를 참조하십시오.

NSX-T Data Center 개요

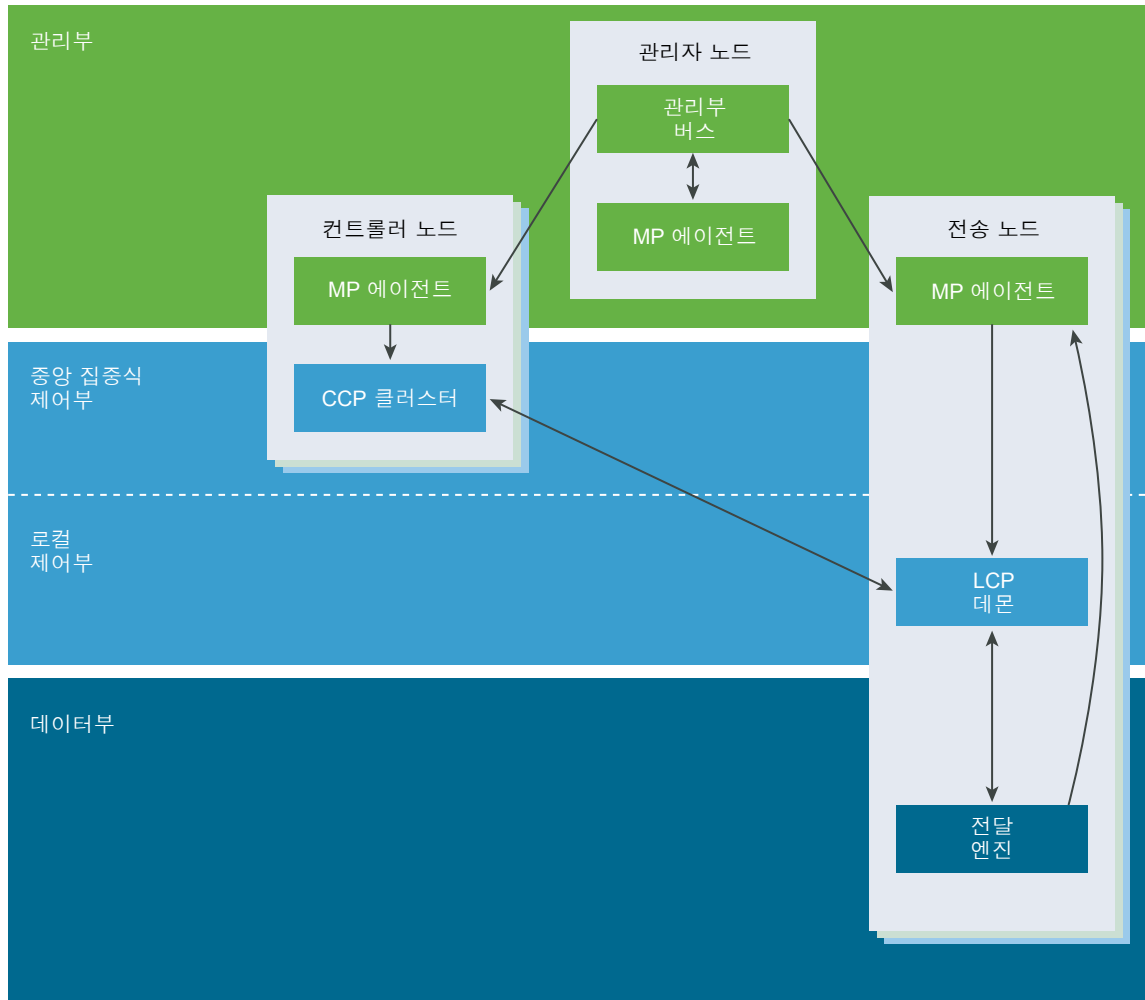
서버 가상화에서 소프트웨어 기반 VM(가상 시스템)을 프로그래밍 방식으로 생성, 스냅샷 생성, 삭제 및 복원하는 것과 상당히 동일한 방법으로 NSX-T Data Center 네트워크 가상화에서도 소프트웨어 기반 가상 네트워크를 프로그래밍 방식으로 생성, 삭제 및 복원합니다.

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 임의 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. 이 세 가지 부분은 세 가지 유형의 노드인 관리자, 컨트롤러 및 전송 노드에 상주하는 프로세스, 모듈 및 에이전트 집합으로 구현됩니다.

- 각 노드는 관리부 에이전트를 호스팅합니다.
- NSX Manager 노드는 API 서비스를 호스팅합니다. 각 NSX-T Data Center 설치에 단일 NSX Manager 노드를 지원합니다.
- NSX Controller 노드는 중앙 제어부 클러스터 데몬을 호스팅합니다.
- NSX Manager 및 NSX Controller 노드는 동일한 물리적 서버에 함께 호스팅될 수 있습니다.

- 전송 노드는 로컬 제어부 데몬 및 전달 엔진을 호스팅합니다.



본 장은 다음 항목을 포함합니다.

- 관리부
- 제어부
- 데이터부
- 논리적 스위치
- 논리적 라우터
- 핵심 개념

관리부

관리부는 시스템의 모든 관리부, 제어부 및 데이터부 노드에서 시스템에 대한 단일 API 진입점을 제공하고, 사용자 구성을 유지하고, 사용자 쿼리를 처리하고, 작업을 수행합니다.

NSX-T Data Center의 경우 사용자 구성을 쿼리, 수정 및 유지하는 일은 관리부에서 담당하지만, 해당 구성을 데이터부 요소의 올바른 하위 집합으로 전달하는 것은 제어부에서 담당합니다. 즉, 일부 데이터는 어느 단계에 있는지를 기준으로 여러 부에 속합니다. 또한 관리부는 제어부 및 경우에 따라 데이터부에서 직접 최근 상태 및 통계에 대한 쿼리를 처리합니다.

관리부는 사용자가 구성을 통해 관리하는 구성된 (논리적) 시스템의 유일한 소스입니다. RESTful API 또는 NSX-T Data Center UI를 사용하여 변경이 수행됩니다.

NSX에는 모든 컨트롤러 클러스터 및 전송 노드에서 실행되는 MPA(관리부 에이전트)도 있습니다. MPA는 로컬로도 원격으로도 액세스가 가능합니다. 전송 노드에서는 데이터부 관련 작업도 수행될 수 있습니다.

관리부에서 발생하는 작업에는 다음이 포함됩니다.

- 구성 지속성(원하는 논리적 상태)
- 입력 검증
- 사용자 관리 -- 역할 할당
- 정책 관리
- 백그라운드 작업 추적

NSX Manager

NSX Manager는 논리적 스위치 및 NSX Edge Services Gateway와 같은 NSX-T Data Center 구성 요소의 생성, 구성 및 모니터링을 위한 GUI(그래픽 사용자 인터페이스) 및 REST API를 제공하는 가상 장치입니다.

NSX Manager는 NSX-T Data Center 에코시스템을 위한 관리부입니다. NSX Manager는 종합적인 시스템 보기를 제공하며, NSX-T Data Center의 중앙 집중식 네트워크 관리 구성 요소입니다. 또한 다음의 구성 및 오케스트레이션을 제공합니다.

- 논리적 네트워킹 구성 요소 - 논리적 스위칭 및 라우팅
- 네트워킹 및 Edge 서비스
- 보안 서비스 및 분산 방화벽

NSX Manager는 NSX-T Data Center에 의해 생성된 가상 네트워크에 연결되는 워크로드를 모니터링하고 문제를 해결하는 방법을 제공합니다. 이는 기본 제공 및 외부 서비스의 원활한 오케스트레이션을 허용합니다. 기본 제공 방식이나 타사에서 제공하는 모든 보안 서비스는 NSX-T Data Center 관리부에 의해 배포되고 구성됩니다. 관리부는 서비스 가용성을 확인하기 위한 단일 창을 제공합니다. 또한 정책 기반 서비스 체인, 컨텍스트 공유 및 서비스 간 이벤트 처리를 용이하게 합니다. 이를 통해 보안 상태 감사가 단순화되고 ID 기반 제어 애플리케이션을 간소화합니다(예: AD 및 모빌리티 프로파일).

또한 NSX Manager는 사용을 자동화하기 위한 REST API 진입점도 제공합니다. 이러한 유연한 아키텍처는 클라우드 관리 플랫폼, 보안 벤더 플랫폼 또는 자동화 프레임워크를 통해 모든 구성 및 모니터링 측면의 자동화를 가능하게 합니다.

NSX-T Data Center MPA(관리부 에이전트)는 각 노드(하이퍼바이저)에 있는 NSX Manager 구성 요소입니다. MPA는 원하는 시스템 상태를 유지하고 전송 노드와 관리부 간에 구성, 통계, 상태 및 실시간 데이터와 같은 NFC(non-flow-controlling) 메시지를 전달하는 일을 담당합니다.

NSX Policy Manager

NSX Policy Manager는 NSX-T Data Center 서비스의 사용을 단순화하기 위한 의도 기반 시스템을 제공하는 가상 장치입니다.

NSX Policy Manager는 네트워킹, 보안 및 가용성과 관련된 의도를 지정하도록 GUI(그래픽 사용자 인터페이스) 및 REST API를 제공합니다.

NSX Policy Manager는 트리 기반 데이터 모델의 형태로 사용자의 의도를 수용하고 NSX Manager가 해당 의도를 인식하도록 구성합니다. NSX Policy Manager는 NSX Manager에 분산 방화벽을 구성하는 통신 의도 규격을 지원합니다.

Cloud Service Manager

Cloud Service Manager(CSM)는 모든 공용 클라우드 구성체에 대한 단일 창 방식 관리 끝점을 제공합니다.

CSM은 공용 클라우드 인벤토리 등록 구성 및 모니터링을 위한 GUI(그래픽 사용자 인터페이스) 및 REST API를 제공하는 가상 장치입니다.

제어부

관리부의 구성에 따라 모든 사용 후 삭제 런타임 상태를 계산하고, 데이터부 요소에서 보고한 토폴로지 정보를 전달하고, 상태 비저장 구성을 전달 엔진으로 푸시합니다.

제어부는 NSX-T Data Center에서 두 부분, 즉 NSX Controller 클러스터 노드에서 실행되는 CCP(중앙 제어부)와 전송 노드에서 실행되는 LCP(로컬 제어부)(여기서 제어하는 데이터부에 인접) 부분으로 분할됩니다. 중앙 제어부는 관리부의 구성에 따라 일부 사용 후 삭제 런타임 상태를 계산하고, 로컬 제어부를 통해 데이터부 요소에서 보고하는 정보를 전달합니다. 로컬 제어부는 로컬 링크 상태를 모니터링하고, 데이터부 및 CCP의 업데이트에 따라 대부분의 사용 후 삭제 런타임 상태를 계산하고, 상태 비저장 구성을 전달 엔진으로 푸시합니다. LCP는 LCP를 호스팅하는 데이터부 요소에 따라 작동됩니다.

NSX Controller

CCP(중앙 제어부)라고 하는 NSX Controller는 가상 네트워크 및 오버레이 전송 터널을 제어하는 고급 분산 상태 관리 시스템입니다.

NSX Controller는 전체 NSX-T Data Center 아키텍처에서 가상 네트워크의 프로그래밍 방식 배포를 담당하는 고가용성의 가상 장치 클러스터로 배포됩니다. NSX-T Data Center CCP는 모든 데이터부 트래픽에서 논리적으로 분리되므로 제어부의 장애가 기존 데이터부 작업에 영향을 미치지 않습니다. 트래픽은 컨트롤러를 통과하지 않으며, 대신 컨트롤러가 논리적 스위치, 논리적 라우터 및 Edge 등의 구성을 다른 NSX Controller 구성 요소에 제공합니다. 데이터 전송의 안정성 및 신뢰성은 네트워크에서 핵심적인 문제입니다. 고가용성 및 확장성을 좀 더 향상하기 위해 NSX Controller가 3개의 인스턴스 클러스터에 배포됩니다.

데이터부

제어부에 의해 채워진 테이블을 기준으로 패킷의 상태 비저장 전달/변환을 수행하고, 제어부에 토폴로지 정보를 보고하고, 패킷 수준 통계를 유지 관리합니다.

데이터부는 물리적 토폴로지 및 상태에 대한 데이터 소스(예: VIF 위치, 터널 상태 등)입니다. 한 위치에서 다른 위치로의 패킷 이동을 처리하는 경우 사용자는 데이터부에 위치해 있는 것입니다. 또한 데이터부는 여러 링크/터널의 상태를 유지 관리하고 여러 링크/터널 간 패일오버를 처리합니다. 패킷 기준 성능은 아주 엄격한 지연 시간 또는 불규칙 신호 요구 사항에서 가장 중요합니다. 데이터부는 커널, 드라이버, 사용자 공간 또는 특정 사용자 공간 프로세스에 반드시 완전히 포함된 것은 아닙니다. 데이터부는 제어부에 의해 채워진 테이블/규칙을 기준으로 하는 완전한 상태 비저장 전달로 제한됩니다.

또한 데이터부에는 TCP 종료와 같은 기능에 대해 특정 수준의 상태를 유지 관리하는 구성 요소도 포함되어 있을 수 있습니다. 이는 MAC:IP 터널 매핑과 같은 제어부 관리 상태와는 다릅니다. 제어부에서 관리하는 상태는 패킷 전달 방법과 관련이 있지만 데이터부에서 관리하는 상태는 페이로드를 조작하는 방법으로 제한되기 때문입니다.

NSX Edge

NSX Edge에서는 NSX-T Data Center 배포 외부에 있는 네트워크에 대해 라우팅 서비스 및 연결을 제공합니다.

NSX Edge는 베어 메탈 노드 또는 VM으로 배포할 수 있습니다.

NSX Edge는 BGP 또는 정적 라우팅을 거쳐 Tier-0 라우터를 통해 NSX-T Data Center 도메인에서 외부 연결을 설정하는 데 필요합니다. 또한 Tier-0 또는 Tier-1 논리적 라우터에서 NAT(네트워크 주소 변환) 서비스가 필요한 경우 NSX Edge를 배포해야 합니다.

NSX Edge 게이트웨이는 NAT 및 동적 라우팅과 같은 공용 게이트웨이 서비스를 제공하여 분리된 스텝 네트워크를 공유(업링크) 네트워크에 연결합니다. 일반적인 NSX Edge 배포는 NSX Edge가 각 테넌트에 대해 가상 경계를 생성하는 DMZ 및 다중 테넌트 클라우드 환경에 포함됩니다.

전송 영역

전송 노드는 논리적 스위치가 도달할 수 있는 호스트를 제어하는 논리적 구성체입니다. 전송 영역은 하나 이상의 호스트 클러스터에 걸쳐 있을 수 있습니다. 전송 영역에서는 특정 네트워크 사용에 참여할 수 있는 호스트, 즉 VM을 지정합니다.

전송 영역은 물리적 네트워크 인프라에서 서로 통신할 수 있는 호스트 컬렉션을 정의합니다. 이 통신은 VTEP(가상 터널 끝점)로 정의된 하나 이상의 인터페이스에서 발생합니다.

전송 노드는 로컬 제어부 데몬을 실행하고 NSX-T Data Center 데이터부를 구현하는 엔진을 전달하는 호스트입니다. 전송 노드는 사용 가능한 네트워크 서비스의 구성에 따라 패킷 스위칭을 담당하는 N-VDS(NSX-T Data Center 가상 Distributed Switch)로 구성됩니다.

두 전송 노드가 동일한 전송 영역에 있으면 해당 전송 노드에 호스팅된 VM은 해당 전송 영역에 함께 있는 NSX-T Data Center 논리적 스위치를 “볼 수 있고” 여기에 연결될 수 있습니다. VM에 계층 2/계층 3 접근성이 있다면 이러한 연결을 통해 VM은 서로 통신할 수 있게 됩니다. VM이 다른 전송 영역에 있는 스위치에 연결되면 VM은 서로 통신할 수 없습니다. 전송 영역은 계층 2/계층 3 접근성 요구를 대체하지 않으나 접근성을 제한합니다. 즉, 동일한 전송 영역에 속하는 것이 연결을 위한 전제 조건입니다. 이러한 전제 조건이 충족되면 연결이 가능해지지만 자동으로 이루어지지 않습니다. 실제 접근성을 얻으려면 계층 2 및 (다른 서브넷용) 계층 3 네트워킹이 작동해야 합니다.

호스트가 하나 이상의 N-VDS(NSX 관리 가상 Distributed Switch, 이전 이름: 호스트 스위치)를 포함하는 경우 전송 노드로 작동할 수 있습니다. 호스트 전송 노드를 생성한 후 해당 노드를 전송 영역에 추가하면 NSX-T Data Center는 호스트에 N-VDS를 설치합니다. 호스트가 속하는 각 전송 영역에 대해 별도의 N-VDS가 설치됩니다. N-VDS는 VM을 NSX-T Data Center 논리적 스위치에 연결하고 NSX-T Data Center 논리적 라우터 업링크 및 다운링크를 생성하는 데 사용됩니다.

논리적 스위치

NSX-T Data Center 플랫폼의 논리적 스위칭 기능은 가상 시스템에 대해 존재하는 것과 동일한 유연성 및 민첩성으로 분리된 논리적 L2 네트워크를 스핀업하는 기능을 제공합니다.

논리적 스위치는 계층 3 IP 연결이 가능한 여러 호스트 간에 계층 2 스위칭 연결을 표시합니다. 일부 논리적 네트워크를 제한된 호스트 집합으로 제한하거나 연결을 사용자 지정해야 하는 경우 추가 논리적 스위치를 생성하는 것이 필요할 수 있습니다.

이러한 애플리케이션과 테넌트는 보안 및 장애 분리의 목적과 IP 주소 겹침 문제를 방지하기 위해 서로 분리되어야 합니다. 가상 및 물리적 끝점은 논리적 세그먼트에 연결될 수 있으며 데이터 센터 네트워크의 물리적 위치와는 별도로 연결을 설정할 수 있습니다. 이는 NSX-T Data Center 네트워크 가상화를 통해 제공되는 논리적 네트워크(예: 오버레이 네트워크의 기본 네트워크)에서 네트워크 인프라를 분리하여 수행할 수 있습니다.

논리적 라우터

NSX-T Data Center 논리적 라우터는 북-남 연결을 제공하므로, 테넌트가 공용 네트워크에 액세스할 수 있도록 하고, 동일한 테넌트 내의 다른 네트워크 간 동-서 연결을 허용합니다. 동-서 연결의 경우 논리적 라우터가 호스트의 커널 전체에 분산됩니다.

NSX-T Data Center를 사용하면 2계층 논리적 라우터 토폴로지를 생성할 수 있습니다. 즉, 상위 계층 논리적 라우터는 Tier-0이고, 하위 계층 논리적 라우터는 Tier-1입니다. 이 구조는 제공자 관리자와 테넌트 관리자가 해당 서비스 및 정책을 완전히 제어할 수 있도록 합니다. 관리자는 Tier-0 라우팅 및 서비스를 제어 및 구성하고, 테넌트 관리자는 Tier-1을 제어 및 구성합니다. Tier-0의 북쪽 끝은 물리적 네트워크에 연결되고, 여기에서 동적 라우팅 프로토콜이 물리적 라우터와 라우팅 정보를 교환하도록 구성할 수 있습니다. Tier-0의 남쪽 끝은 여러 Tier-1 라우팅 계층에 연결되고 이러한 계층으로부터 라우팅 정보를 수신합니다. 리소스 사용을 최적화하기 위해 Tier-0 계층은 물리적 네트워크에서 들어오는 모든 경로를 Tier-1 쪽으로 푸시하지 않고 기본 정보를 제공합니다.

사우스바운드에서 Tier-1 라우팅 계층은 테넌트 관리자가 정의하는 논리적 스위치에 연결되고 둘 간에 단일 홉 라우팅 기능을 제공합니다. 물리적 네트워크에서 Tier-1 연결 서브넷에 연결되도록 하려면 Tier-0 계층 쪽의 경로 재배포가 사용되도록 설정되어야 합니다. 하지만 Tier-1 계층과 Tier-0 계층 사이에 실행되는 기존 라우팅 프로토콜(예: OSPF 또는 BGP)은 없으며 모든 경로는 NSX-T Data Center 제어부를 통과합니다. 2계층 라우팅 토폴로지는 필수가 아닙니다. 제공자와 테넌트를 분리할 필요가 없으면 단일 계층 토폴로지를 생성할 수 있고, 이 시나리오의 경우 논리적 스위치는 Tier-0 계층에 직접 연결되고 Tier-1 계층은 없습니다.

논리적 라우터는 하나의 DR(분산 라우터)과 하나 이상의 SR(서비스 라우터)로 구성된 두 부분(선택 사항)으로 이루어집니다.

DR은 논리적 라우터가 바인딩된 Edge 노드뿐만 아니라 VM이 이 논리적 라우터에 연결되어 있는 하이퍼바이저에 걸쳐 있습니다. 기능적으로 DR은 논리적 스위치 및/또는 이 논리적 라우터에 연결된 논리적 라우터 간의 단일 홉 분산 라우팅을 담당합니다. SR은 현재 분산 방식으로 구현되지 않은 서비스를 전달합니다(예: 상태 저장 NAT).

논리적 라우터에는 항상 DR이 있고 다음 조건이 충족될 경우 SR도 있습니다.

- 상태 저장 서비스가 구성되지 않더라도 논리적 라우터는 Tier-0 라우터입니다.
- 논리적 라우터는 Tier-0 라우터에 연결된 Tier-1 라우터이고, 분산 구현이 없는 서비스가 구성되어 있습니다(예: NAT, LB, DHCP).

NSX-T Data Center MP(관리부)는 서비스 라우터를 분산 라우터에 연결하는 구조를 자동으로 생성합니다. MP는 전송 논리적 스위치를 생성한 후 VNI를 할당한 다음, 각 SR 및 DR에 포트를 생성하고, 전송 논리적 스위치에 연결한 후 SR 및 DR에 대해 IP 주소를 할당합니다.

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.

패브릭 노드	NSX-T Data Center 관리부에 등록되어 있고 NSX-T Data Center 모듈이 설치된 호스트입니다. 하이퍼바이저 호스트 또는 NSX Edge가 NSX-T Data Center 오버레이에 속하려면 이를 NSX-T Data Center 패브릭에 추가해야 합니다.
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	<p>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 관계없이 VM을 연결합니다.</p> <p>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.</p>
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 사용 구성의 쿼리, 수정 및 유지도 담당합니다.
NSX Controller 클러스터	전체 NSX-T Data Center 아키텍처에서 가상 네트워크의 프로그래밍 방식 배포를 담당하는 고가용성의 가상 장치 클러스터로 배포됩니다.
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**

하이퍼바이저에서 실행되고 트래픽 전달을 제공하는 소프트웨어입니다. N-VDS(NSX 관리 가상 Distributed Switch, 이전 이름: 호스트 스위치) 또는 OVS는 테넌트 네트워크 관리자에게 보이지 않으며 각 논리적 스위치에 필요한 기본 전달 서비스를 제공합니다. 네트워크 가상화를 수행하기 위해 네트워크 컨트롤러는 테넌트 관리자가 논리적 스위치를 생성 및 구성할 때 정의한 논리적 브로드캐스트 도메인을 형성하는 네트워크 흐름 테이블로 하이퍼바이저 가상 스위치를 구성해야 합니다.

각 논리적 브로드캐스트 도메인은 터널 캡슐화 메커니즘인 Geneve를 사용하여 VM과 VM 간의 트래픽 및 VM과 논리적 라우터 간의 트래픽을 터널링하여 구현됩니다. 네트워크 컨트롤러는 데이터 센터의 글로벌 뷰를 제공하고, VM이 생성, 이동 또는 제거될 때 하이퍼바이저 가상 스위치 흐름 테이블이 업데이트되도록 합니다.

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-T Data Center
통합 장치**

NSX-T Data Center 통합 장치는 NSX-T Data Center 설치 패키지에 포함된 장치입니다. NSX Manager, Policy Manager 또는 Cloud Service Manager 역할로 장치를 배포할 수 있습니다. 현재 장치는 한 번에 하나의 역할만 지원합니다.

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 토폴로지에서도 분리되도록 계층 2-in-계층 3 터널링을 사용하여 구현되는 논리적 네트워크입니다.

**물리적 인터페이스
(pNIC)**

하이퍼바이저가 설치되는 물리적 서버의 네트워크 인터페이스입니다.

Tier-0 논리적 라우터

공급자 논리적 라우터를 물리적 네트워크가 포함된 Tier-0 논리적 라우터 인터페이스라고도 합니다. Tier-0 논리적 라우터는 상위 계층 라우터로, 서비스 라우터의 활성-활성 또는 활성-대기 클러스터로 구현할 수 있습니다. 논리적 라우터는 BGP를 실행하고 물리적 라우터와 피어링됩니다. 활성-대기 모드에서 논리적 라우터는 상태 저장 서비스를 제공할 수도 있습니다.

Tier-1 논리적 라우터

Tier-1 논리적 라우터는 노스바운드 연결을 위해 하나의 Tier-0 논리적 라우터에 연결되고 사우스바운드 연결을 위해 하나 이상의 오버레이 네트워크에 연결되는 두 번째 계층 라우터입니다. Tier-1 논리적 라우터는 상태 저장 서비스를 제공하는 서비스 라우터의 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.
전송 노드	NSX-T Data Center 오버레이 또는 NSX-T Data Center VLAN 네트워크에 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.
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	하이퍼바이저 호스트를 NSX-T Data Center 오버레이에 참여하도록 할 수 있습니다. NSX-T Data Center 오버레이는 패킷 내부에 프레임을 캡슐화하고 기본 전송 네트워크를 통해 패킷을 전송하여 기존 계층 3 네트워크 패브릭 위에 계층 2 네트워크를 배포합니다. 기본 전송 네트워크는 다른 계층 2 네트워크이거나 계층 3 경계를 가로지를 수 있습니다. VTEP는 캡슐화 및 캡슐화 해제가 발생하는 연결 지점입니다.

설치 준비

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

본 장은 다음 항목을 포함합니다.

- 시스템 요구 사항
- 포트 및 프로토콜
- NSX-T Data Center 설치 상위 수준 작업

시스템 요구 사항

NSX-T Data Center에는 하드웨어 리소스 및 소프트웨어 버전에 대한 특정 요구 사항이 있습니다.

하이퍼바이저 요구 사항

하이퍼바이저	버전	CPU 코어	메모리
vSphere	지원되는 vSphere 버전	4	16GB
RHEL KVM	7.5 및 7.4	4	16GB
Ubuntu KVM	16.04.2 LTS	4	16GB
CentOS KVM	7.4	4	16GB

NSX-T Data Center는 RHEL 7.5, RHEL 7.4, Ubuntu 16.04 및 CentOS 7.4에서 호스트 준비를 지원합니다. NSX Manager 및 NSX Controller 배포는 RHEL 7.5 및 CentOS 7.4에서 지원되지 않습니다. NSX Edge 노드 배포는 vSphere에서만 지원됩니다.

ESXi 호스트의 경우 NSX-T Data Center는 vSphere 6.7 U1 이상에서 호스트 프로파일 및 Auto Deploy 기능을 지원합니다.



경고 RHEL에서 yum update 명령은 커널 버전을 업데이트하고 NSX-T Data Center와의 호환성을 중단할 수 있습니다. yum update를 실행하는 경우에는 자동 커널 업데이트를 사용하지 않도록 설정합니다. 또한 yum install을 실행한 후 NSX-T Data Center가 커널 버전을 지원하는지 확인합니다.

베어메탈 서버 요구 사항

운영 체제	버전	CPU 코어	메모리
RHEL	7.5 및 7.4	4	16GB
Ubuntu	16.04.2 LTS	4	16GB
CentOS	7.4	4	16GB

NSX Manager 리소스 요구 사항

썬 가상 디스크 크기는 3.1GB이고 썬 가상 디스크 크기는 200GB입니다.

장치	메모리	vCPU	스토리지	VM 하드웨어 버전
NSX Manager 소형 VM	8GB	2	200GB	10 이상
NSX Manager 중간 VM	16GB	4	200GB	10 이상
NSX Manager 중대형 VM	24GB	6	200GB	10 이상
NSX Manager 대형 VM	32GB	8	200GB	10 이상
NSX Manager 초대형 VM	48GB	12	200GB	10 이상

참고 NSX Manager 소형 VM은 랩 및 개념 증명 배포에 사용해야 합니다.

NSX Manager 리소스 요구 사항이 NSX Policy Manager 및 Cloud Service Manager에 적용됩니다.

NSX Controller 리소스 요구 사항

장치	메모리	vCPU	디스크 용량	배포 유형
NSX Controller 소형 VM	8GB	2	120GB	랩 및 개념 증명 배포
NSX Controller 중간 VM	16GB	4	120GB	중간 규모 배포에 권장
NSX Controller 대형 VM	32GB	8	120GB	대규모 배포에 필요

참고 고가용성을 보장하고 NSX-T Data Center 제어부의 중단을 방지하기 위해 세 개의 NSX Controller를 배포합니다.

하나의 물리적 하이퍼바이저 호스트 장애가 NSX-T Data Center 제어부에 영향을 주지 않도록 하려면 각 NSX Controller 클러스터가 3개의 개별적인 물리적 하이퍼바이저 호스트에 있어야 합니다. NSX-T Data Center 참조 설계 가이드를 참조하십시오.

프로덕션 워크로드가 없는 랩 및 개념 증명 배포의 경우 단일 NSX Controller를 사용하여 리소스를 절약할 수 있습니다.

vSphere OVF 배포 사용자 인터페이스에서 소형 및 대형 VM 폼 팩터만 배포할 수 있습니다.

NSX Edge VM 리소스 요구 사항

배포 크기	메모리	vCPU	디스크 용량	VM 하드웨어 버전
소형	4GB	2	120GB	10 이상(vSphere 5.5 이상)
중간	8GB	4	120GB	10 이상(vSphere 5.5 이상)
대형	16GB	8	120GB	10 이상(vSphere 5.5 이상)

참고 NSX Manager 및 NSX Edge의 경우 소형 장치는 개념 증명 배포용입니다. 중간 장치는 일반적인 운영 환경에 적합하며 최대 64개의 하이퍼바이저를 지원할 수 있습니다. 대형 장치는 65개 이상의 하이퍼바이저가 있는 대규모 배포용입니다.

참고 VMXNET 3 vNIC은 NSX Edge VM에서만 지원됩니다.

NSX Edge VM 및 베어메탈 NSX Edge CPU 요구 사항

참고 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.

DPDK 지원을 위해서는 기본 플랫폼이 다음 요구 사항을 충족해야 합니다.

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

참고 NSX-T Data Center 데이터부는 Intel의 DPDK(데이터부 개발 키트)의 네트워크 기능을 사용하므로 intel 기반 CPU만 지원됩니다.

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

베어메탈 NSX Edge 하드웨어 요구 사항

사용 중인 베어메탈 NSX Edge 하드웨어가 URL

[https://certification.ubuntu.com/server/models/?](https://certification.ubuntu.com/server/models/?release=16.04%20LTS&category=Server)

[release=16.04%20LTS&category=Server](https://certification.ubuntu.com/server/models/?release=16.04%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.

베어메탈 NSX Edge 특정 NIC 요구 사항

NIC 유형	설명	PCI 디바이스 ID
Intel X520/Intel 82599	IXGBE_DEV_ID_82599_KX4	0x10F7
	IXGBE_DEV_ID_82599_KX4_MEZ	0x1514
	Z	0x1517
	IXGBE_DEV_ID_82599_KR	0x10F8
	IXGBE_DEV_ID_82599_COMBO_B	0x000C
	ACKPLANE	0x10F9
	IXGBE_SUBDEV_ID_82599_KX4_	0x10FB
	KR_MEZZ	0x11A9
	IXGBE_DEV_ID_82599_CX4	0x1F72
	IXGBE_DEV_ID_82599_SFP	0x17D0
	IXGBE_SUBDEV_ID_82599_SFP	0x0470
	IXGBE_SUBDEV_ID_82599_RNDC	0x1507
	IXGBE_SUBDEV_ID_82599_560FL	0x154D
	R	0x154A
	IXGBE_SUBDEV_ID_82599_ECNA	0x1558
	_DP	0x1557
	IXGBE_DEV_ID_82599_SFP_EM	0x10FC
	IXGBE_DEV_ID_82599_SFP_SF2	0x151C
	IXGBE_DEV_ID_82599_SFP_SF_Q	
	P	
Intel X540	IXGBE_DEV_ID_82599_QSFP_SF_	
	QP	
	IXGBE_DEV_ID_82599EN_SFP	
	IXGBE_DEV_ID_82599_XAUI_LO	
	M	
Intel X540	IXGBE_DEV_ID_82599_T3_LOM	
Intel X540	IXGBE_DEV_ID_X540T	0x1528
	IXGBE_DEV_ID_X540T1	0x1560
Intel X550	IXGBE_DEV_ID_X550T	0x1563
	IXGBE_DEV_ID_X550T1	0x15D1
Intel X710	I40E_DEV_ID_SFP_X710	0x1572
	I40E_DEV_ID_KX_C	0x1581
	I40E_DEV_ID_10G_BASE_T	0x1586
Intel XL710	I40E_DEV_ID_KX_B	0x1580
	I40E_DEV_ID_QSFP_A	0x1583
	I40E_DEV_ID_QSFP_B	0x1584
	I40E_DEV_ID_QSFP_C	0x1585
Cisco VIC 1387	Cisco UCS 가상 인터페이스 카드 1387	0x0043

베어메탈 NSX Edge 메모리, CPU 및 디스크 요구 사항

메모리	CPU 코어	디스크 용량
32GB	8	200GB

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 1.1.3-1OEM.670.0.0.8169922
Intel(R) Ethernet Controller XL710 for 40GbE QSFP+	

NSX Manager 브라우저 지원

브라우저	Windows 10	Windows 8.1	Ubuntu 14.04	Mac OS X 10.11 및 10.12
Internet Explorer 11	예	예		
Firefox 55			예	예
Chrome 60	예	예		예
Safari 10				예
Microsoft Edge 40	예			

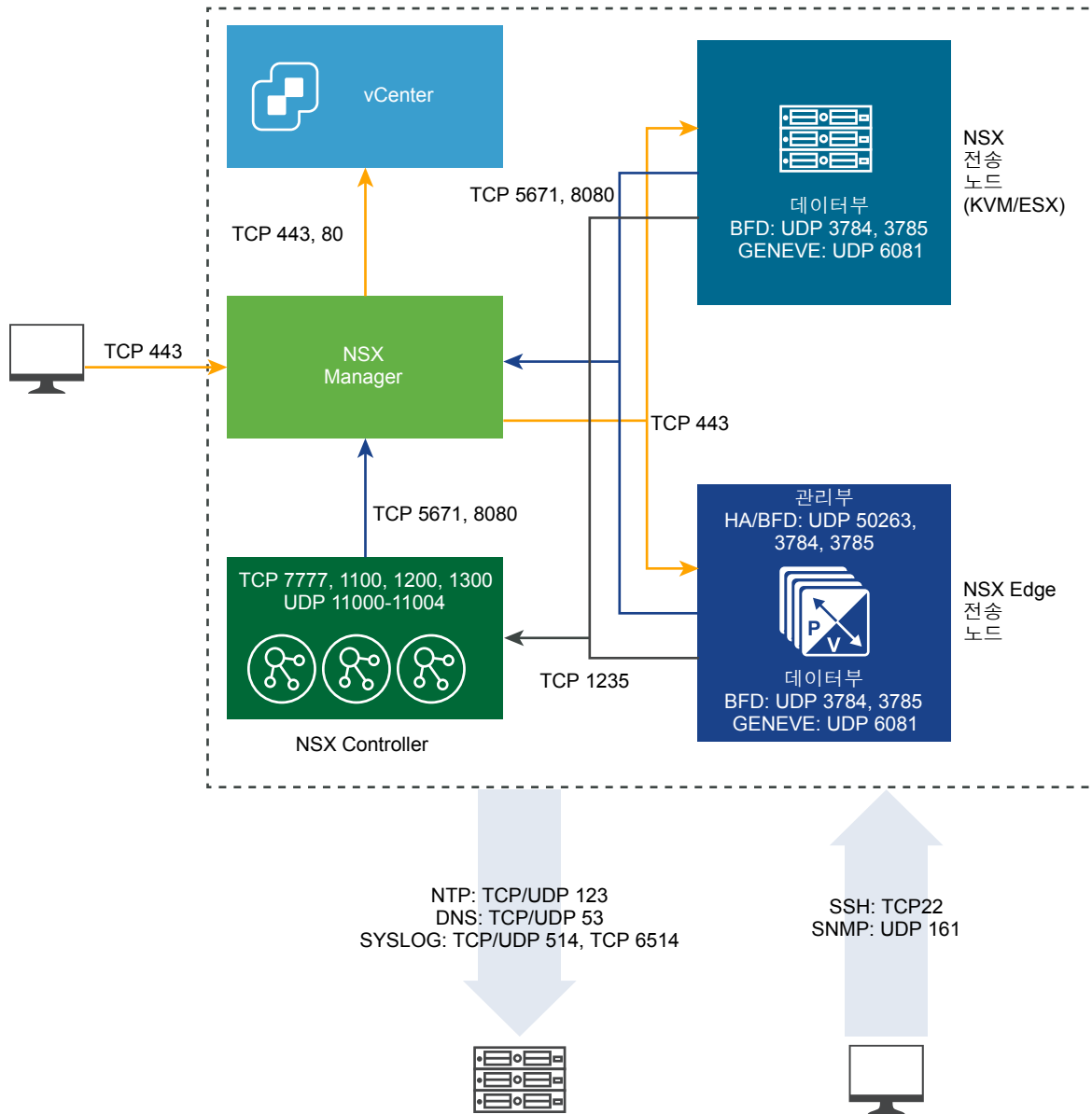
참고 호환성 모드의 Internet Explorer 11은 지원되지 않습니다.

지원되는 브라우저 최소 해상도는 1280x800픽셀입니다.

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.

그림 2-1. NSX-T Data Center 포트 및 프로토콜



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
- ESX: netcpa, ESX-DP(커널에서)

RMQ 사용자 데이터베이스(db)에서 암호는 복구 불가능한 해시 함수로 해시됩니다. 즉 h(p1)는 암호 p1의 해시입니다.

CCP 중앙 제어부

LCP 로컬 제어부


MP

관리부

MPA

관리부 에이전트

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

 **NSX Cloud 참조** NSX Cloud 배포에 필요한 포트 목록은 [하이브리드 연결을 위해 CSM의 포트 및 프로토콜에 액세스할 수 있도록 설정](#) 항목을 참조하십시오.

NSX Manager 에서 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 2-1. NSX Manager 에서 사용되는 TCP 및 UDP 포트

소스	대상	포트	프로토콜	설명
관리 클라이언트	NSX Manager	22	TCP	SSH(기본적으로 사용되지 않도록 설정됨)
NTP 서버	NSX Manager	123	UDP	NTP
관리 클라이언트	NSX Manager	443	TCP	NSX API 서버
SNMP 서버	NSX Manager	161	UDP	SNMP
NSX Controller, NSX Edge 노드, 전송 노드, vCenter Server	NSX Manager	8080	TCP	HTTP 저장소 설치-업그레이드
NSX Controller, NSX Edge 노드, 전송 노드	NSX Manager	5671	TCP	NSX 메시징
NSX Manager	관리 SCP 서버	22	TCP	SSH(지원 번들, 백업 등 업로드)
NSX Manager	DNS 서버	53	TCP	DNS
NSX Manager	DNS 서버	53	UDP	DNS
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

표 2-1. NSX Manager 에서 사용되는 TCP 및 UDP 포트 (계속)

소스	대상	포트	프로토콜	설명
NSX Manager	Syslog 서버	6514	UDP	Syslog
NSX Manager	LogInsight 서버	9000	TCP	Log Insight 에이전트
NSX Manager	Traceroute 대상	33434 - 33523	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

NSX Controller에서 사용되는 TCP 및 UDP 포트

NSX Controller에서는 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 2-2. NSX Controller 에서 사용되는 TCP 및 UDP 포트

소스	대상	포트	프로토콜	설명
관리 클라이언트	NSX Controller	22	TCP	SSH(기본적으로 사용되지 않도록 설정됨)
DNS 서버	NSX Controller	53	UDP	DNS
NTP 서버	NSX Controller	123	UDP	NTP
SNMP 서버	NSX Controller	161	UDP	SNMP
NSX Controller	NSX Controller	1100	TCP	Zookeeper 쿼럼
NSX Controller	NSX Controller	1200	TCP	Zookeeper 리더 선택
NSX Controller	NSX Controller	1300	TCP	Zookeeper 서버
NSX Edge 노드, 전송 노드	NSX Controller	1235	TCP	CCP-netcpa 통신
NSX Controller	NSX Controller	7777	TCP	Moot RPC
NSX Controller	NSX Controller	11000 - 11004	UDP	다른 클러스터 노드에 대한 터널. 클러스터에 6개 이상의 노드가 있으면 추가 포트를 열어야 합니다.
Traceroute 대상	NSX Controller	33434 - 33523	UDP	Traceroute
NSX Controller	SSH 대상	22	TCP	SSH(기본적으로 사용되지 않도록 설정됨)
NSX Controller	DNS 서버	53	UDP	DNS

표 2-2. NSX Controller 에서 사용되는 TCP 및 UDP 포트 (계속)

소스	대상	포트	프로토콜	설명
NSX Controller	DNS 서버	53	TCP	DNS
NSX Controller	NTP 서버	123	UDP	NTP
NSX Controller	NSX Manager	5671	TCP	NSX 메시징
NSX Controller	LogInsight 서버	9000	TCP	Log Insight 에이전트
NSX Controller	NSX Controller	11000 - 11004	TCP	다른 클러스터 노드에 대한 터널. 클러스터에 6개 이상의 노드가 있으면 추가 포트를 열어 야 합니다.
NSX Controller	NSX Manager	8080	TCP	NSX 업그레이드
NSX Controller	Traceroute 대상	33434 - 33523	UDP	Traceroute
NSX Controller	Syslog 서버	514	UDP	Syslog
NSX Controller	Syslog 서버	514	TCP	Syslog
NSX Controller	Syslog 서버	6514	TCP	Syslog

NSX Edge 에서 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 내보내기 위한 포트(기본 포트 514 및 6514)를 지정할 수 있습니다. 이 경우 방화벽도 지정된 포트에 따라 구성해야 합니다.

표 2-3. NSX Edge 에서 사용되는 TCP 및 UDP 포트

소스	대상	포트	프로토콜	설명
관리 클라이언트	NSX Edge 노드	22	TCP	SSH(기본적으로 사용되지 않도록 설정됨)
NTP 서버	NSX Edge 노드	123	UDP	NTP
SNMP 서버	NSX Edge 노드	161	UDP	SNMP
NSX Edge 노드	NSX Edge 노드	1167	TCP	DHCP 백엔드
NSX Edge 노드, 전송 노드	NSX Edge 노드	3784, 3785	UDP	데이터의 전송 노드 TEP IP 주소 사이 BFD.
NSX 에이전트	NSX Edge 노드	5555	TCP	NSX Cloud - 인스턴스의 에이전트는 NSX Cloud 게이트웨이와 통신합니다.
NSX Edge 노드	NSX Edge 노드	6666	TCP	NSX Cloud - NSX Edge 로컬 통신.
NSX Edge 노드	NSX Manager	8080	TCP	NAPI, NSX-T Data Center 업그레이드

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

소스	대상	포트	프로토콜	설명
NSX Edge 노드	NSX Edge 노드	2480	TCP	Nestdb
NSX Edge 노드	관리 SCP 또는 SSH 서버	22	TCP	SSH
NSX Edge 노드	DNS 서버	53	UDP	DNS
NSX Edge 노드	NTP 서버	123	UDP	NTP
NSX Edge 노드	SNMP 서버	161, 162	UDP	SNMP
NSX Edge 노드	SNMP 서버	161, 162	TCP	SNMP
NSX Edge 노드	NSX Manager	443	TCP	HTTPS
NSX Edge 노드	Syslog 서버	514	TCP	Syslog
NSX Edge 노드	Syslog 서버	514	UDP	Syslog
NSX Edge 노드	NSX Edge 노드	1167	TCP	DHCP 백엔드
NSX Edge 노드	NSX Controller	1235	TCP	netcpa
NSX Edge 노드	OpenStack Nova API 서버	3000 - 9000	TCP	메타데이터 프록시
NSX Edge 노드	NSX Manager	5671	TCP	NSX 메시징
NSX Edge 노드	Syslog 서버	6514	TCP	TLS를 통한 Syslog
NSX Edge 노드	Traceroute 대상	3343 - 33523	UDP	Traceroute
NSX Edge 노드	NSX Edge 노드	50263	UDP	고가용성

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

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

표 2-4. vSphere ESXi 및 KVM 호스트에 사용되는 TCP 및 UDP 포트

소스	대상	포트	프로토콜	설명
NSX Manager	vSphere ESXi 호스트	443	TCP	관리 및 프로비저닝 연결
NSX Manager	KVM 호스트	443	TCP	관리 및 프로비저닝 연결

표 2-4. vSphere ESXi 및 KVM 호스트에 사용되는 TCP 및 UDP 포트 (계속)

소스	대상	포트	프로토콜	설명
vSphere ESXi 호스트	NSX Manager	567 1	TCP	NSX Manager에 대한 AMQP 통신 채널
vSphere ESXi 호스트	NSX Controller	123 5	TCP	제어부 - LCP와 CCP 간의 통신
KVM 호스트	NSX Manager	567 1	TCP	NSX Manager에 대한 AMQP 통신 채널
KVM 호스트	NSX Controller	123 5	TCP	제어부 - LCP와 CCP 간의 통신
vSphere ESXi 호스트	NSX Manager	808 0	TCP	HTTP 저장소 설치 및 업그레이드
KVM 호스트	NSX Manager	808 0	TCP	HTTP 저장소 설치 및 업그레이드
GENEVE TEP(Termination End Point)	GENEVE TEP(Termination End Point)	608 1	UDP	전송 네트워크
NSX-T Data Center 전송 노드	NSX-T Data Center 전송 노드	378 4, 378 5	UDP	TEP 인터페이스를 사용한 데이터 경로에서 TEP 간의 BFD 세션

NSX-T Data Center 설치 상위 수준 작업

체크리스트를 사용하여 설치 진행률을 추적합니다.

권장되는 절차 순서를 따릅니다.

- 1 NSX Manager를 설치합니다. [장4NSX Manager 설치](#)를 참조하십시오.
- 2 NSX Controller를 설치합니다. [장5NSX Controller 설치 및 클러스터링](#)을 참조하십시오.
- 3 NSX Controller를 관리부에 연결합니다. [NSX Controller를 NSX Manager에 연결](#)을 참조하십시오.
- 4 마스터 NSX Controller를 생성하여 제어 클러스터를 초기화합니다. [제어 클러스터를 초기화하여 제어 클러스터 마스터 생성](#)을 참조하십시오.
- 5 NSX Controller를 제어 클러스터에 연결합니다. [클러스터 마스터에 추가 NSX Controller 연결](#)을 참조하십시오.

NSX Manager는 하이퍼바이저 호스트가 추가된 후 NSX-T Data Center 모듈을 설치합니다.

참고 NSX-T Data Center 모듈이 설치될 때 하이퍼바이저 호스트에 인증서가 생성됩니다.

- 6 하이퍼바이저 호스트를 관리부에 연결합니다. [하이퍼바이저 호스트를 관리부에 연결](#)을 참조하십시오.

호스트는 관리부로 호스트 인증서를 보냅니다.

- 7 NSX Edge를 설치합니다. [장6NSX Edge 설치](#)를 참조하십시오.
- 8 NSX Edge를 관리부에 연결합니다. [NSX Edge를 관리부에 연결](#)을 참조하십시오.
- 9 전송 영역 및 전송 노드를 생성합니다. [장8전송 영역 및 전송 노드](#)를 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.

일반적인 설치 순서는 다음과 같습니다.

- 1 NSX Manager가 먼저 설치됩니다.
- 2 NSX Controller를 설치하고 관리부에 연결할 수 있습니다.
- 3 관리부에 연결하기 전에 NSX-T Data Center 모듈을 하이퍼바이저 호스트에 설치할 수도 있고, **패브릭 > 호스트 > 추가** UI를 사용하여 두 절차를 동시에 진행할 수도 있습니다.
- 4 NSX Controller, NSX Edge 및 호스트(NSX-T Data Center 모듈 포함)는 언제든지 관리부에 연결될 수 있습니다.

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 Controller, NSX Edge 및 호스트가 관리부에 연결되면 NSX-T Data Center 논리적 엔티티 및 구성 상태가 NSX Controller, NSX Edge 및 호스트로 자동으로 푸시됩니다.

자세한 내용은 NSX-T Data Center 관리 가이드를 참조하십시오.

KVM 사용

NSX-T Data Center에서는 KVM을 호스트 전송 노드 및 NSX Manager와 NSX Controller에 대한 호스트로 지원합니다.

표 3-1. 지원되는 KVM 버전

요구 사항	설명
지원되는 플랫폼	<ul style="list-style-type: none"> ■ RHEL 7.5 ■ RHEL 7.4 ■ Ubuntu 16.04.2 LTS ■ CentOS 7.4

본 장은 다음 항목을 포함합니다.

- [KVM 설정](#)
- [KVM CLI에서 게스트 VM 관리](#)

KVM 설정

KVM을 전송 노드 또는 NSX Manager 및 NSX Controller 게스트 VM에 대한 호스트로 사용하고 있지만 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 (Red Hat에만 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 Container Plug-in을 실행하려는 경우 컨테이너 관련 모듈도 제외시킵니다.

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

지원되는 RHEL 버전은 7.4입니다.

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	<pre>yum groupinstall "Virtualization Hypervisor" yum groupinstall "Virtualization Client" yum groupinstall "Virtualization Platform" yum groupinstall "Virtualization Tools"</pre>

5 하드웨어 가상화 기능을 확인합니다.

```
cat /proc/cpuinfo | egrep "vmx|svm"
```

출력에는 vmx가 포함되어야 합니다.

6 KVM 모듈이 설치되어 있는지 확인합니다.

Linux 배포판	명령
Ubuntu	<pre>kvm-ok INFO: /dev/kvm exists KVM acceleration can be used</pre>
RHEL	<pre>lsmod grep kvm kvm_intel 53484 6 kvm 316506 1 kvm_intel</pre>

7 KVM을 NSX Manager 또는 NSX Controller에 대한 호스트로 사용하려면 브리지 네트워크, 관리 인터페이스 및 NIC 인터페이스를 준비합니다.

다음 예에서 첫 번째 이더넷 인터페이스(eth0 또는 ens32)는 Linux 시스템 자체로 연결하는 데 사용됩니다. 배포 환경에 따라 이 인터페이스는 DHCP 또는 정적 IP 설정을 사용할 수 있습니다. 업링크 인터페이스를 NSX-T 호스트에 할당하기 전에 이러한 업링크에 사용되는 인터페이스 스크립트가 이미 구성되었는지 확인합니다. 시스템에 이러한 인터페이스 파일이 없으면 호스트 전송 노드를 성공적으로 생성할 수 없습니다.

참고 인터페이스 이름은 환경에 따라 다를 수 있습니다.

Linux 배포판	네트워크 구성
Ubuntu	<p>/etc/network/interfaces를 편집합니다.</p> <pre> auto lo iface lo inet loopback auto eth0 iface eth0 inet manual auto br0 iface br0 inet static address 192.168.110.51 netmask 255.255.255.0 network 192.168.110.0 broadcast 192.168.110.255 gateway 192.168.110.1 dns-nameservers 192.168.3.45 dns-search example.com bridge_ports eth0 bridge_stp off bridge_fd 0 bridge_maxwait 0 </pre> <p>브리지에 대한 네트워크 정의 xml 파일을 생성합니다. 예를 들어 다음 줄을 사용하여 /tmp/bridge.xml을 생성합니다.</p> <pre> <network> <name>bridge</name> <forward mode='bridge' /> <bridge name='br0' /> </network> </pre> <p>다음 명령을 사용하여 브리지 네트워크를 정의하고 시작합니다.</p> <pre> virsh net-define bridge.xml virsh net-start bridge virsh net-autostart bridge </pre>

Linux 배포판**네트워크 구성**

다음 명령을 사용하여 브리지 네트워크의 상태를 확인할 수 있습니다.

```
virsh net-list --all
```

Name	State	Autostart	Persistent
bridge	active	yes	yes
default	active	yes	yes

RHEL

/etc/sysconfig/network-scripts/ifcfg-*management_interface*를 편집합니다.

```
DEVICE="ens32"
TYPE="Ethernet"
NAME="ens32"
UUID="<UUID>"
BOOTPROTO="none"
HWADDR="<HWADDR>"
ONBOOT="yes"
NM_CONTROLLED="no"
BRIDGE="br0"
```

/etc/sysconfig/network-scripts/ifcfg-eth1을 편집합니다.

```
DEVICE="eth1"
TYPE="Ethernet"
NAME="eth1"
UUID="<UUID>"
BOOTPROTO="none"
HWADDR="<HWADDR>"
ONBOOT="yes"
NM_CONTROLLED="no"
```

/etc/sysconfig/network-scripts/ifcfg-eth2를 편집합니다.

```
DEVICE="eth2"
TYPE="Ethernet"
NAME="eth2"
UUID="<UUID>"
BOOTPROTO="none"
HWADDR="<HWADDR>"
ONBOOT="yes"
NM_CONTROLLED="no"
```

/etc/sysconfig/network-scripts/ifcfg-br0을 편집합니다.

```
DEVICE="br0"
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE="Bridge"
```

8 KVM을 전송 노드로 사용하려면 네트워크 브리지를 준비합니다.

다음 예에서 첫 번째 이더넷 인터페이스(eth0 또는 ens32)는 Linux 시스템 자체로 연결하는 데 사용됩니다. 배포 환경에 따라 이 인터페이스는 DHCP 또는 정적 IP 설정을 사용할 수 있습니다.

참고 인터페이스 이름은 환경에 따라 다를 수 있습니다.

Linux 배포판	네트워크 구성
Ubuntu	<p>/etc/network/interfaces를 편집합니다.</p> <pre> auto lo iface lo inet loopback auto eth0 iface eth0 inet manual auto eth1 iface eth1 inet manual auto br0 iface br0 inet dhcp bridge_ports eth0 </pre>
RHEL	<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" BRIDGE="br0" </pre> <p>/etc/sysconfig/network-scripts/ifcfg-ens33을 편집합니다.</p> <pre> DEVICE="ens33" TYPE="Ethernet" NAME="ens33" UUID="<something>" BOOTPROTO="none" HWADDR="<something>" ONBOOT="yes" NM_CONTROLLED="no" </pre> <p>/etc/sysconfig/network-scripts/ifcfg-br0을 편집합니다.</p> <pre> DEVICE="br0" BOOTPROTO="dhcp" NM_CONTROLLED="no" ONBOOT="yes" TYPE="Bridge" </pre>

중요 Ubuntu의 경우 모든 네트워크 구성을 /etc/network/interfaces에 지정해야 합니다. /etc/network/ifcfg-eth1과 같은 개별 네트워크 구성 파일은 생성하지 마십시오. 이 경우 전송 노드 생성이 실패할 수 있습니다.

이 단계 이후 KVM 호스트가 전송 노드로 구성되면 브리지 인터페이스 "nsx-vtep0.0"이 생성됩니다. Ubuntu에서 /etc/network/interfaces에는 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
```

- 9 네트워크 변경 사항을 적용하려면 네트워크 서비스 systemctl restart network를 다시 시작하거나 Linux 서버를 재부팅합니다.

KVM CLI에서 게스트 VM 관리

NSX Manager 및 NSX Controller를 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 사용할 수 있습니다. 다음은 몇 가지 일반적인 virsh 명령입니다. 추가 정보에 대해서는 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)
```

NSX Manager 설치

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.

NSX-T Data Center 배포에는 NSX Manager 인스턴스가 하나만 있을 수 있습니다.

NSX Manager가 ESXi 호스트에 배포되는 경우 vSphere HA(High Availability) 기능을 사용하여 NSX Manager의 가용성을 보장할 수 있습니다.

표 4-1. NSX Manager 배포, 플랫폼 및 설치 요구 사항

요구 사항	설명
지원되는 배포 방법	<ul style="list-style-type: none"> ■ OVA/OVF ■ QCOW2
지원되는 플랫폼	<p>시스템 요구 사항의 내용을 참조하십시오.</p> <p>ESXi에서는 NSX Manager 장치를 공유 스토리지에 설치하는 것이 좋습니다. vSphere HA를 보장하려면 공유 스토리지가 필요합니다. 그래야 원래 호스트에 장애가 발생할 경우 다른 호스트에서 VM을 다시 시작할 수 있습니다.</p>
IP 주소	NSX Manager에는 정적 IP 주소가 있어야 합니다. 설치 후에는 IP 주소를 변경할 수 없습니다.
NSX-T Data Center 장치 암호	<ul style="list-style-type: none"> ■ 8자 이상의 문자 ■ 하나 이상의 소문자 ■ 하나 이상의 대문자 ■ 하나 이상의 숫자 ■ 하나 이상의 특수 문자 ■ 5개 이상의 다른 문자 ■ 사전 단어 제외 ■ 회문 제외
호스트 이름	<p>NSX Manager 설치 시 밑줄과 같은 잘못된 문자를 포함하지 않는 호스트 이름을 지정합니다. 호스트 이름에 유효하지 않은 문자가 포함되어 있으면 배포 후에 호스트 이름이 nsx-manager로 설정됩니다. 호스트 이름 제한에 대한 자세한 내용은 https://tools.ietf.org/html/rfc952 및 https://tools.ietf.org/html/rfc1123을 참조하십시오.</p>
VMware Tools	ESXi에서 실행되는 NSX Manager VM에는 VMTTools가 설치되어 있습니다. VMTTools를 제거하거나 업그레이드하지 마십시오.

표 4-1. NSX Manager 배포, 플랫폼 및 설치 요구 사항 (계속)

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. ■ 대상 VM 포트 그룹 네트워크가 아직 없으면 생성합니다. NSX-T Data Center 장치를 관리 VM 네트워크에 배치하는 것이 좋습니다. <p>여러 관리 네트워크가 있으면 NSX-T Data Center 장치에서 다른 네트워크로의 정적 경로를 추가할 수 있습니다.</p> <ul style="list-style-type: none"> ■ IPv4 IP 주소 체계를 계획합니다. 이 NSX-T Data Center 릴리스에서는 IPv6가 지원되지 않습니다.
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 웹 클라이언트에서든 또는 명령줄에서든 OVA 또는 OVF 파일에서 NSX Manager를 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 **admin** 사용자 권한으로 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.

본 장은 다음 항목을 포함합니다.

- [NSX Manager 및 사용 가능한 장치 설치](#)
- [명령줄 OVF 도구를 사용하여 ESXi에 NSX Manager 설치](#)
- [KVM에 NSX Manager 설치](#)
- [새로 생성된 NSX Manager에 로그인](#)

NSX Manager 및 사용 가능한 장치 설치

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

NSX Policy Manager는 정책을 관리할 수 있는 가상 장치입니다. 논리적 포트, IP 주소, VM 등과 같은 NSX-T Data Center 구성 요소에 대한 규칙을 지정하는 정책을 구성할 수 있습니다.

NSX Policy Manager 규칙을 사용하면 정확한 세부 정보를 지정하지 않아도 적용되는 높은 수준의 사용량 및 리소스 액세스 규칙을 설정할 수 있습니다.

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

참고 vSphere Client 대신 vSphere Web Client를 사용하는 것을 권장합니다. 운영 환경에 vCenter Server가 없는 경우 ovftool을 사용하여 NSX Manager를 배포합니다. [명령줄 OVF 도구를 사용하여 ESXi에 NSX Manager 설치](#)의 내용을 참조하십시오.

절차

- 1 NSX-T Data Center 통합 장치 OVA 또는 OVF 파일을 찾습니다.
다운로드 URL을 복사하거나 OVA 파일을 컴퓨터에 다운로드합니다.
- 2 vSphere Web Client에서 **OVF 템플릿 배포** 마법사를 실행하고 .ova 파일을 찾거나 이 파일을 연결합니다.

- 3 NSX Manager의 이름을 입력하고 폴더 또는 데이터센터를 선택합니다.
입력한 이름이 인벤토리에 나타납니다.
선택한 폴더는 NSX Manager에 사용 권한을 적용하는 데 사용됩니다.
- 4 NSX Manager 가상 장치 파일을 저장할 데이터스토어를 선택합니다.
- 5 vCenter에서 설치하는 경우 NSX Manager 장치를 배포할 호스트 또는 클러스터를 선택합니다.
- 6 NSX Manager에 대한 포트 그룹 또는 대상 네트워크를 선택합니다.
- 7 NSX Manager 암호 및 IP 설정을 지정합니다.
- 8 **nsx-manager** 역할을 수락합니다.
 - 드롭다운 메뉴에서 **nsx-policy-manager** 역할을 선택하여 NSX Policy Manager 장치를 설치합니다.
 - 드롭다운 메뉴에서 **nsx-cloud-service-manager** 역할을 선택하여 NSX Cloud 장치를 설치합니다.

참고 **nsx-manager nsx-cloud-service-manager (multi-role)** 역할은 지원되지 않습니다.

- 9 (선택 사항) 최적의 성능을 위해서는 NSX-T Data Center 구성 요소용 메모리를 예약합니다.
메모리 예약은 메모리가 오버 커밋되더라도 호스트가 가상 시스템을 위해 예약하는 물리적 메모리 양에 대해 보장되는 하한 값입니다. NSX-T Data Center 구성 요소가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정합니다. [시스템 요구 사항](#)의 내용을 참조하십시오.
- 10 NSX-T Data Center 구성 요소의 콘솔을 열어 부팅 프로세스를 추적합니다.
- 11 NSX-T Data Center 구성 요소가 부팅되면 CLI에 관리자 권한으로 로그인하고 `get interface eth0` 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

- 12 NSX-T Data Center 구성 요소에 필요한 연결이 있는지 확인합니다.
다음 작업을 수행할 수 있는지 확인하십시오.
 - 다른 시스템에서 NSX-T Data Center 구성 요소를 Ping합니다.
 - NSX-T Data Center 구성 요소에서 기본 게이트웨이를 Ping할 수 있습니다.
 - NSX-T Data Center 구성 요소에서 관리 인터페이스를 사용하여 NSX-T Data Center 구성 요소와 동일한 네트워크에 있는 하이퍼바이저 호스트를 Ping할 수 있습니다.

- NSX-T Data Center 구성 요소에서는 DNS 서버와 NTP 서버를 Ping할 수 있습니다.
- SSH를 사용하도록 설정한 경우 NSX-T Data Center 구성 요소에 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 브라우저에서 NSX Manager GUI에 연결합니다.

URL은 https://<NSX Manager의 IP 주소>입니다. 예를 들어 https://10.16.176.10 같은 주소를 입력합니다.

참고 HTTPS를 사용해야 합니다. HTTP는 지원되지 않습니다.

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_allowSSHRootLogin은 보안상의 이유로 둘 다 사용되지 않도록 설정됩니다. 사용되지 않도록 설정되면 SSH를 실행하거나 NSX Manager 명령줄에 로그인할 수 없습니다. nsx_isSSHEnabled는 사용하도록 설정하고 nsx_allowSSHRootLogin은 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.
- 대상 VM 포트 그룹 네트워크가 아직 없으면 생성합니다. NSX-T Data Center 장치를 관리 VM 네트워크에 배치하는 것이 좋습니다.

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

- IPv4 IP 주소 체계를 계획합니다. 이 NSX-T Data Center 릴리스에서는 IPv6가 지원되지 않습니다.

절차

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

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-manager
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
```

```
--net="management"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_role=nsx-manager
--prop:nsx_ip_0=192.168.110.75
--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|False>
--prop:nsx_allowSSHRootLogin=<True|False>
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-manager
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:<password>@192.168.110.51
Deploying to VI: vi://root:<password>@192.168.110.51
Transfer Completed
Powering on VM: nsx-manager
Task Completed
Completed successfully
```

- vCenter Server에서 관리되는 호스트의 경우 해당 매개 변수를 사용하여 ovftool 명령을 실행합니다. 예를 들면 다음과 같습니다.

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-manager
--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=192.168.110.75
--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|False>
--prop:nsx_allowSSHRootLogin=<True|False>
```



```
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-manager
nsx-<component>.ova
vi://administrator@vsphere.local:<password>@192.168.110.24/?ip=192.168.110.51
```

```
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-manager
Task Completed
Completed successfully
```

- (선택 사항) 최적의 성능을 위해서는 NSX-T Data Center 구성 요소용 메모리를 예약합니다.
메모리 예약은 메모리가 오버 커밋되더라도 호스트가 가상 시스템을 위해 예약하는 물리적 메모리 양에 대해 보장되는 하한 값입니다. NSX-T Data Center 구성 요소가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정합니다. [시스템 요구 사항](#)의 내용을 참조하십시오.
- NSX-T Data Center 구성 요소의 콘솔을 열어 부팅 프로세스를 추적합니다.
- NSX-T Data Center 구성 요소가 부팅되면 CLI에 관리자 권한으로 로그인하고 `get interface eth0` 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

- NSX-T Data Center 구성 요소에 필요한 연결이 있는지 확인합니다.
다음 작업을 수행할 수 있는지 확인하십시오.
 - 다른 시스템에서 NSX-T Data Center 구성 요소를 Ping합니다.
 - NSX-T Data Center 구성 요소에서 기본 게이트웨이를 Ping할 수 있습니다.
 - NSX-T Data Center 구성 요소에서 관리 인터페이스를 사용하여 NSX-T Data Center 구성 요소와 동일한 네트워크에 있는 하이퍼바이저 호스트를 Ping할 수 있습니다.
 - NSX-T Data Center 구성 요소에서는 DNS 서버와 NTP 서버를 Ping할 수 있습니다.
 - SSH를 사용하도록 설정한 경우 NSX-T Data Center 구성 요소에 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 브라우저에서 NSX Manager GUI에 연결합니다.

URL은 `https://<NSX Manager의 IP 주소>`입니다. 예를 들어 `https://10.16.176.10` 같은 주소를 입력합니다.

참고 HTTPS를 사용해야 합니다. HTTP는 지원되지 않습니다.

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. [장4NSX Manager 설치](#)의 내용을 참조하십시오.

절차

- 1 NSX Manager QCOW2 이미지를 다운로드한 다음, SCP 또는 동기화를 사용하여 NSX Manager를 실행하는 KVM 시스템으로 복사합니다.
- 2 (Ubuntu만 해당) 현재 로그인한 사용자를 `libvirtd` 사용자로 추가합니다.

```
adduser $USER libvirtd
```

- 3 QCOW2 이미지를 저장한 동일한 디렉토리에 `guestinfo`(파일 확장명 없음)라는 파일을 만들고 NSX Manager VM의 속성으로 채웁니다.

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_role" oe:value="nsx-manager"/>
    <Property oe:key="nsx_allowSSHRootLogin" oe:value="True"/>
    <Property oe:key="nsx_cli_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_dns1_0" oe:value="192.168.110.10"/>
    <Property oe:key="nsx_domain_0" oe:value="corp.local"/>
    <Property oe:key="nsx_gateway_0" oe:value="192.168.110.1"/>
    <Property oe:key="nsx_hostname" oe:value="nsx-manager1"/>
    <Property oe:key="nsx_ip_0" oe:value="192.168.110.19"/>
  </PropertySection>
</Environment>
```

```
<Property oe:key="nsx_isSSHEnabled" oe:value="True"/>
<Property oe:key="nsx_netmask_0" oe:value="255.255.255.0"/>
<Property oe:key="nsx_ntp_0" oe:value="192.168.110.10"/>
<Property oe:key="nsx_passwd_0" oe:value="<password>"/>
</PropertySection>
</Environment>
```

이 예에서 nsx_isSSHEnabled 및 nsx_allowSSHRootLogin은 둘 다 사용되도록 설정됩니다. 사용되지 않도록 설정되면 SSH를 실행하거나 NSX Manager 명령줄에 로그인할 수 없습니다. nsx_isSSHEnabled는 사용하도록 설정하고 nsx_allowSSHRootLogin은 사용하지 않도록 설정하면 NSX Manager에 대해 SSH를 실행할 수 있으나 루트 권한으로 로그인할 수 없습니다.

4 guestfish를 사용하여 QCOW2 이미지에 guestinfo 파일을 기록합니다.

guestinfo 정보가 QCOW2 이미지에 기록되면 정보를 덮어쓸 수 없습니다.

```
sudo guestfish --rw -i -a nsx-manager1-build.qcow2 upload guestinfo /config/guestinfo
```

5 virt-install 명령을 사용하여 QCOW2 이미지를 배포합니다.

```
user@ubuntu1604:/var/lib/libvirt/images$ sudo virt-install --import --name nsx-manager1 --ram 16348 --vcpus 4
--network=bridge:br0,model=e1000 --disk path=/var/lib/libvirt/images/nsx-
manager-1.1.0.0.4446302.qcow2,format=qcow2 --nographics

Starting install...
Creating domain...      |  0 B    00:01
Connected to domain nsx-manager1
Escape character is ^]

nsx-manager1 login:
```

NSX Manager가 부팅된 후에 NSX Manager 콘솔이 나타납니다.

6 (선택 사항) 최적의 성능을 위해서는 NSX-T Data Center 구성 요소용 메모리를 예약합니다.

메모리 예약은 메모리가 오버 커밋되더라도 호스트가 가상 시스템을 위해 예약하는 물리적 메모리 양에 대해 보장되는 하한 값입니다. NSX-T Data Center 구성 요소가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정합니다. [시스템 요구 사항](#)의 내용을 참조하십시오.

7 NSX-T Data Center 구성 요소의 콘솔을 열어 부팅 프로세스를 추적합니다.

8 NSX-T Data Center 구성 요소가 부팅되면 CLI에 관리자 권한으로 로그인하고 get interface eth0 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
```

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

9 NSX-T Data Center 구성 요소에 필요한 연결이 있는지 확인합니다.

다음 작업을 수행할 수 있는지 확인하십시오.

- 다른 시스템에서 NSX-T Data Center 구성 요소를 Ping합니다.
- NSX-T Data Center 구성 요소에서 기본 게이트웨이를 Ping할 수 있습니다.
- NSX-T Data Center 구성 요소에서 관리 인터페이스를 사용하여 NSX-T Data Center 구성 요소와 동일한 네트워크에 있는 하이퍼바이저 호스트를 Ping할 수 있습니다.
- NSX-T Data Center 구성 요소에서는 DNS 서버와 NTP 서버를 Ping할 수 있습니다.
- SSH를 사용하도록 설정한 경우 NSX-T Data Center 구성 요소에 대해 SSH를 수행할 수 있는지 확인합니다.

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

10 KVM 콘솔을 종료합니다.

```
control-]
```

다음에 수행할 작업

지원되는 웹 브라우저에서 NSX Manager GUI에 연결합니다.

URL은 `https://<NSX Manager의 IP 주소>`입니다. 예를 들어 `https://10.16.176.10` 같은 주소를 입력합니다.

참고 HTTPS를 사용해야 합니다. HTTP는 지원되지 않습니다.

새로 생성된 NSX Manager 에 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 가이드의 고객 환경 향상 프로그램을 참조하십시오.

사전 요구 사항

NSX Manager가 설치되어 있는지 확인합니다.

절차

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

EULA가 표시됩니다.

- 2 EULA의 맨 아래로 스크롤하고 EULA 조건을 수락합니다.
- 3 VMware의 CEIP(고객 환경 향상 프로그램)에 참여할지 여부를 선택합니다.
- 4 **저장**을 클릭합니다

NSX Controller 설치 및 클러스터링

5

NSX Controller는 NSX-T Data Center 논리적 스위칭 및 라우팅 기능에 대한 제어부 기능을 제공하는 고급 분산 상태 관리 시스템입니다.

NSX Controller는 네트워크 내의 모든 논리적 스위치에 대한 중앙 제어 지점으로 작동하고 모든 호스트, 논리적 스위치 및 논리적 라우터에 대한 정보를 유지합니다. NSX Controller는 패킷 전달을 수행하는 디바이스를 제어합니다. 이러한 전달 디바이스를 가상 스위치라고 합니다.

N-VDS(NSX 관리 가상 Distributed Switch, 이전 이름: 호스트 스위치) 및 OVS(Open vSwitch)와 같은 가상 스위치는 ESXi 및 KVM과 같은 다른 하이퍼바이저에 상주합니다.

운영 환경에서는 NSX 제어부에 대한 중단을 방지하기 위해 세 개의 멤버가 있는 NSX Controller 클러스터가 있어야 합니다. 하나의 물리적 하이퍼바이저 호스트에 장애가 발생하여 NSX 제어부에 영향을 미치지 않도록, 각 컨트롤러를 고유한 하이퍼바이저 호스트(총 3개의 물리적 하이퍼바이저 호스트)에 배치해야 합니다. 프로덕션 워크로드가 없는 랩 및 개념 증명 배포의 경우 단일 컨트롤러를 실행하여 리소스를 절약할 수도 있습니다.

표 5-1. NSX Controller 배포, 플랫폼 및 설치 요구 사항

요구 사항	설명
지원되는 배포 방법	<ul style="list-style-type: none"> ■ OVA/OVF ■ QCOW2 <p>참고 PXE 부팅 배포 방법은 지원되지 않습니다.</p>
지원되는 플랫폼	<p>시스템 요구 사항의 내용을 참조하십시오.</p> <p>NSX Controller는 ESXi에서 VM 및 KVM으로 지원됩니다.</p> <p>참고 PXE 부팅 배포 방법은 지원되지 않습니다.</p>
IP 주소	<p>NSX Controller에는 정적 IP 주소가 있어야 합니다. 설치 후에는 IP 주소를 변경할 수 없습니다.</p> <p>IPv4 IP 주소 체계를 계획합니다. 이 NSX-T Data Center 릴리스에서는 IPv6가 지원되지 않습니다.</p>

표 5-1. NSX Controller 배포, 플랫폼 및 설치 요구 사항 (계속)

요구 사항	설명
NSX-T Data Center 장치 암호	<ul style="list-style-type: none"> ■ 8자 이상의 문자 ■ 하나 이상의 소문자 ■ 하나 이상의 대문자 ■ 하나 이상의 숫자 ■ 하나 이상의 특수 문자 ■ 5개 이상의 다른 문자 ■ 사전 단어 제외 ■ 회문 제외
호스트 이름	NSX Controller 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 Controller VM에는 VMTTools가 설치되어 있습니다. VMTTools를 제거하거나 업그레이드하지 마십시오.
시스템	시스템 요구 사항이 충족되었는지 확인합니다. 시스템 요구 사항 의 내용을 참조하십시오.
포트	필수 포트가 열려 있는지 확인합니다. 포트 및 프로토콜 의 내용을 참조하십시오.

NSX Controller 설치 시나리오

중요 vSphere 웹 클라이언트에서든 또는 명령줄에서든 OVA 또는 OVF 파일에서 NSX Controller를 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 **admin** 사용자 권한으로 NSX Controller에 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 Controller에 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 Controller에 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

- 루트 권한을 사용하여 데몬이나 애플리케이션을 설치하지 마십시오. 데몬이나 애플리케이션을 설치하기 위해 루트 권한을 사용하면 지원 계약이 무효화될 수 있습니다. 루트 권한은 VMware 지원 팀에서 요청하는 경우에만 사용하십시오.
- 장치의 핵심 서비스는 충분한 복잡도를 갖는 암호를 설정해야만 시작할 수 있습니다.
OVA 파일에서 NSX Controller를 배포한 후에는 VM 전원을 끄고 vCenter Server에서 OVA 설정을 수정하여 VM의 IP 설정을 변경할 수 없습니다.

본 장은 다음 항목을 포함합니다.

- [NSX Manager에서 컨트롤러 및 클러스터의 자동화된 설치](#)
- [GUI를 사용하여 ESXi에 NSX Controller 설치](#)
- [명령줄 OVF 도구를 사용하여 ESXi에 NSX Controller 설치](#)
- [KVM에 NSX Controller 설치](#)
- [NSX Controller를 NSX Manager에 연결](#)
- [제어 클러스터를 초기화하여 제어 클러스터 마스터 생성](#)
- [클러스터 마스터에 추가 NSX Controller 연결](#)

NSX Manager 에서 컨트롤러 및 클러스터의 자동화된 설치

vSphere ESXi 호스트에 컨트롤러를 자동으로 설치하도록 NSX Manager를 구성할 수 있습니다. 배포 후에는 이러한 컨트롤러가 vCenter Server에서 관리되는 해당 vSphere ESXi 호스트의 컨트롤러 클러스터에 자동으로 추가됩니다. 또는 NSX Manager REST API를 사용하여 컨트롤러 클러스터를 자동으로 설치할 수도 있습니다.

NSX Manager에서는 수동으로 배포된 기존 클러스터에 추가 컨트롤러를 자동으로 배포할 수 있습니다. 단, 수동으로 추가된 컨트롤러를 클러스터에서 삭제하려면 클러스터에서 컨트롤러를 수동으로 제거해야 합니다.

지원되는 사용 사례

- 단일 노드 클러스터 생성
- 다중 노드 클러스터 생성

- 기존 클러스터에 노드 추가
- 기능 클러스터에서 자동으로 배포된 컨트롤러 삭제

NSX Manager UI를 사용하여 컨트롤러 및 클러스터의 자동화된 설치 구성

vCenter Server에서 관리되는 vSphere ESXi 호스트에 컨트롤러를 자동으로 설치하도록 NSX Manager를 구성합니다. 설치 후에는 이러한 컨트롤러가 vSphere ESXi 호스트의 컨트롤러 클러스터에 자동으로 추가됩니다.

사전 요구 사항

- NSX Manager를 배포합니다.
- vCenter Server 및 vSphere ESXi 호스트를 배포합니다.
- vSphere ESXi 호스트를 vCenter Server에 등록합니다.
- vSphere ESXi 호스트에는 12개의 vCPU, 48GB RAM 및 360GB 스토리지를 지원하기 위한 충분한 CPU, 메모리 및 하드 디스크 리소스가 있어야 합니다.

절차

- 1 NSX Manager(<https://<nsxmanagerIPAddress>/>)에 로그인합니다.
- 2 NSX Manager UI에서 등록된 vCenter가 없는 경우 **패브릭** 패널로 이동하고, **계산 관리자**를 클릭하고, 계산 관리자를 추가합니다.
- 3 [시스템] 페이지에서 **컨트롤러 추가**를 클릭합니다.
- 4 [일반 특성] 페이지에서 필수 값을 입력합니다.
- 5 **계산 관리자**를 선택합니다.
- 6 (선택 사항) SSH를 사용하도록 설정할 수 있습니다.
- 7 (선택 사항) 루트 액세스를 사용하도록 설정할 수 있습니다.
- 8 (선택 사항) 기존 클러스터에 노드를 추가하는 경우 [기존 클러스터 연결]을 사용하도록 설정합니다.
- 9 클러스터를 초기화하고 형성하는 데 필요한 공유 암호 키를 입력 및 확인합니다.

참고 이 클러스터에 추가된 모든 컨트롤러 노드가 동일한 공유 암호 키를 사용해야 합니다.

- 10 컨트롤러 자격 증명을 입력합니다.
- 11 **다음**을 클릭합니다.
- 12 [컨트롤러] 페이지에서 **컨트롤러 추가**를 클릭합니다.
- 13 컨트롤러 노드에 대한 올바른 호스트 이름 또는 정규화된 도메인 이름을 입력합니다.
- 14 클러스터를 선택합니다.

15 (선택 사항) 리소스 풀을 선택합니다. 리소스 풀은 컨트롤러 노드를 배포하기 위한 계산 리소스 풀만 제공합니다. 특정 스토리지 리소스를 할당합니다.

16 (선택 사항) 호스트를 선택합니다.

17 데이터스토어를 선택합니다.

18 호스트가 호스트 자체 내의 다른 구성 요소와 통신하는 데 사용되는 관리 인터페이스를 선택합니다.

19 포트 세부 정보 (<IPAddress>/<PortNumber>) 및 넷 마스크가 포함된 정적 IP 주소를 입력합니다.

20 여러 컨트롤러를 추가할 수 있습니다. 배포 시작 전에 + 버튼을 클릭하고 컨트롤러 세부 정보를 입력합니다.

21 완료를 클릭합니다.

자동화된 컨트롤러 설치가 시작됩니다. 컨트롤러는 클러스터를 형성하거나 기존 클러스터를 연결하기 전에 NSX Manager에 처음 등록됩니다.

22 컨트롤러가 NSX Manager에 등록되었는지 확인합니다.

a NSX Manager 콘솔에 로그인합니다.

b # get management-cluster status를 입력합니다.

관리 클러스터 상태는 STABLE이어야 합니다.

c 또는 NSX Manager UI에서 관리자 연결이 UP인지 확인합니다.

23 제어 클러스터 상태를 확인합니다.

a 컨트롤러 CLI 콘솔에 로그인합니다.

b # get control-cluster status를 입력합니다.

컨트롤러 클러스터 상태는 STABLE이어야 합니다.

c 또는 NSX Manager UI에서 클러스터 연결이 UP인지 확인합니다.

다음에 수행할 작업

API를 사용하여 컨트롤러와 클러스터를 자동으로 설치하도록 NSX Manager를 구성합니다. [API를 사용하여 컨트롤러 및 클러스터의 자동화된 설치 구성](#)의 내용을 참조하십시오.

API를 사용하여 컨트롤러 및 클러스터의 자동화된 설치 구성

API를 사용하여 vCenter Server에서 관리되는 vSphere ESXi 호스트에 컨트롤러를 자동으로 설치하도록 NSX Manager를 구성할 수 있습니다. 컨트롤러를 설치하면 컨트롤러가 vSphere ESXi 호스트의 컨트롤러 클러스터에 자동으로 추가됩니다.

절차

1 컨트롤러 클러스터의 자동 생성을 트리거하기 전에 POST API의 페이로드로 필요한 vCenter Server ID, 계산 ID, 스토리지 ID 및 네트워크 ID를 가져와야 합니다.

2 vCenter Server에 로그인합니다.

`https://<vCenterServer_IPAddress>/mob.`

3 [값] 열에서 **컨텐츠**를 클릭합니다.**4** [컨텐츠 속성] 페이지에서 [값] 열로 이동하고 데이터 센터를 검색한 후 그룹 링크를 클릭합니다.**5** [그룹 속성] 페이지에서 [값] 열로 이동하고 데이터 센터 링크를 클릭합니다.**6** [데이터 센터 속성] 페이지에서 컨트롤러 클러스터를 생성하는 데 사용할 데이터스토어 값, 네트워크 값을 복사합니다.**7** **HostFolder** 링크를 클릭합니다.**8** [그룹 속성] 페이지에서 컨트롤러 클러스터를 생성하는 데 사용할 클러스터 값을 복사합니다.**9** vCenter Server ID를 가져오려면 NSX Manager UI로 이동하고 [계산 관리자] 페이지에서 해당 ID를 복사합니다.**10** POST `https://<nsx-manager>/api/v1/cluster/nodes/deployments`

```

REQUEST
{
  "deployment_requests": [
    {
      "roles": ["CONTROLLER"],
      "user_settings": {
        "cli_password": "CLIp4$$w4rd",
        "root_password": "R00Tp4$$w4rd"
      },
      "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
        "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
        "management_network_id": "network-13",
        "hostname": "controller-0",
        "compute_id": "domain-s9",
        "storage_id": "datastore-12",
        "default_gateway_addresses": [
          "10.33.79.253"
        ],
        "management_port_subnets": [
          {
            "ip_addresses": [
              "10.33.79.64"
            ],
            "prefix_length": "22"
          }
        ]
      }
    },
    {
      "roles": ["CONTROLLER"],
      "user_settings": {
        "cli_password": "VMware$123",
        "root_password": "VMware$123"
      }
    }
  ]
}

```

```

    },
    "deployment_config": {
      "placement_type": "VsphereClusterNodeVMDeploymentConfig",
      "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
      "management_network_id": "network-13",
      "hostname": "controller-1",
      "compute_id": "domain-s9",
      "storage_id": "datastore-12"
      "default_gateway_addresses": [
        "10.33.79.253"
      ],
      "management_port_subnets": [
        {
          "ip_addresses": [
            "10.33.79.65"
          ],
          "prefix_length": "22"
        }
      ]
    }
  }
},
    "deployment_config": {
      "placement_type": "VsphereClusterNodeVMDeploymentConfig",
      "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
      "management_network_id": "network-13",
      "hostname": "controller-0",
      "compute_id": "domain-s9",
      "storage_id": "datastore-12",
      "default_gateway_addresses": [
        "10.33.79.253"
      ],
      "management_port_subnets": [
        {
          "ip_addresses": [
            "10.33.79.66"
          ],
          "prefix_length": "22"
        }
      ]
    }
  },
    "clustering_config": {
      "clustering_type": "ControlClusteringConfig",
      "shared_secret": "123456",
      "join_to_existing_cluster": false
    }
  }
}

Response
{
  "result_count": 2,
  "results": [

```

```

{
  "user_settings": {
    "cli_password": "[redacted]",
    "root_password": "[redacted]",
    "cli_username": "admin"
  },
  "vm_id": "71f02260-644f-4482-aa9a-ab8570bb49a3",
  "roles": [
    "CONTROLLER"
  ],
  "deployment_config": {
    "placement_type": "VsphereClusterNodeVMDeploymentConfig",
    "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
    "management_network_id": "network-13",
    "default_gateway_addresses": [
      "10.33.79.253"
    ],
    "hostname": "controller-0",
    "compute_id": "domain-s9",
    "storage_id": "datastore-12",
    "management_port_subnets": [
      {
        "ip_addresses": [
          "10.33.79.64"
        ],
        "prefix_length": 22
      }
    ]
  },
  "form_factor": "SMALL"
},

{
  "user_settings": {
    "cli_password": "[redacted]",
    "root_password": "[redacted]",
    "cli_username": "admin"
  },
  "vm_id": "38029a2b-b9bc-467f-8138-aef784e802cc",
  "roles": [
    "CONTROLLER"
  ],
  "deployment_config": {
    "placement_type": "VsphereClusterNodeVMDeploymentConfig",
    "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
    "management_network_id": "network-13",
    "hostname": "controller-1",
    "compute_id": "domain-s9",
    "storage_id": "datastore-12"
  },

```

```

    "form_factor": "MEDIUM"
  }
]
}

```

11 API 호출을 사용하여 배포의 상태를 확인할 수 있습니다. GET <https://<nsx-manager>/api/v1/cluster/nodes/deployments>

```

{
  "result_count": 2,
  "results": [
    {
      "user_settings": {
        "cli_password": "[redacted]",
        "root_password": "[redacted]"
      },
      "vm_id": "12f563af-af9f-48f3-848e-e9257c8740b0",
      "roles": [
        "CONTROLLER"
      ],
      "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
        "vc_id": "15145422-47a1-4c55-81da-01d953151d1f",
        "management_network_id": "network-158",
        "hostname": "controller-0",
        "compute_id": "domain-c154",
        "storage_id": "datastore-157"
      },
      "form_factor": "SMALL",
    },
    {
      "user_settings": {
        "cli_password": "[redacted]",
        "root_password": "[redacted]"
      },
      "vm_id": "cc21854c-265b-42de-af5f-05448c00777a",
      "roles": [
        "CONTROLLER"
      ],
      "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
        "vc_id": "feb17651-49a7-4ce6-88b4-41d3f624e53b",
        "management_network_id": "network-158",
        "hostname": "controller-0",
        "compute_id": "domain-c154",
        "storage_id": "datastore-157"
      },
      "form_factor": "MEDIUM",
    }
  ]
}

```

```
}
]
}
```

다음에 수행할 작업

클러스터를 삭제합니다. [NSX Controller 삭제](#)의 내용을 참조하십시오.

NSX Controller 삭제

클러스터에서 NSX Controller를 삭제합니다.

절차

- 1 <https://<nsx-manager-ip>/>에 로그인합니다.
- 2 시스템 > 구성 요소를 클릭합니다.
- 3 [컨트롤러 클러스터]에서 NSX Controller를 식별합니다.
- 4 설정 아이콘을 클릭하고 삭제를 클릭합니다.
- 5 확인을 클릭합니다.

NSX-T Data Center는 클러스터에서 NSX Controller를 분리하고 NSX Manager에서 등록 취소하고 전원을 끈 후 NSX Controller를 삭제합니다.

다음에 수행할 작업

GUI를 사용하여 vSphere ESXi 호스트에 NSX Controller를 설치합니다. [GUI를 사용하여 ESXi에 NSX Controller 설치](#)의 내용을 참조하십시오.

GUI를 사용하여 ESXi에 NSX Controller 설치

대화형 NSX Controller 설치를 원할 경우 vCenter Server에 연결된 vSphere Client와 같은 UI 기반 VM 관리 도구를 사용할 수 있습니다.

암호가 요구 사항을 충족하지 않아도 설치 성공합니다. 하지만 처음 로그인할 때 암호를 변경하라는 메시지가 표시됩니다.

중요 장치의 핵심 서비스는 충분한 복잡도를 갖는 암호를 설정해야만 시작할 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

- 시스템 요구 사항이 충족되었는지 확인합니다. [시스템 요구 사항](#)의 내용을 참조하십시오.
- 필수 포트가 열려 있는지 확인합니다. [포트 및 프로토콜](#)의 내용을 참조하십시오.

- 대상 VM 포트 그룹 네트워크가 아직 없으면 생성합니다. NSX-T Data Center 장치를 관리 VM 네트워크에 배치하는 것이 좋습니다.
여러 관리 네트워크가 있으면 NSX-T Data Center 장치에서 다른 네트워크로의 정적 경로를 추가할 수 있습니다.
- IPv4 IP 주소 체계를 계획합니다. 이 NSX-T Data Center 릴리스에서는 IPv6가 지원되지 않습니다.
- ESXi 호스트에 OVF 템플릿을 배포하기 위한 적절한 권한이 있는지 확인합니다.
- 호스트 이름에 밑줄이 포함되지 않았는지 확인합니다. 그렇지 않으면 호스트 이름이 nsx-controller로 설정됩니다.
- vCenter Server 또는 vSphere Client와 같은 OVF 템플릿을 배포할 수 있는 관리 도구. OVF 배포 도구는 수동 구성을 허용하는 구성 옵션을 지원해야 합니다.
- 클라이언트 통합 플러그인이 설치되어 있어야 합니다.

절차

- 1 NSX Controller OVA 또는 OVF 파일을 찾습니다.
다운로드 URL을 복사하거나 OVA 파일을 컴퓨터에 다운로드합니다.
- 2 관리 도구에서 **OVF 템플릿 배포** 마법사를 실행하고 .ova 파일을 찾거나 이 파일을 연결합니다.
- 3 NSX Controller의 이름을 입력하고 폴더 또는 데이터센터를 선택합니다.
입력한 이름이 인벤토리에 나타납니다.
선택한 폴더는 NSX Controller에 사용 권한을 적용하는 데 사용됩니다.
- 4 NSX Controller 가상 장치 파일을 저장할 데이터스토어를 선택합니다.
- 5 vCenter에서 사용하는 경우 NSX Controller 장치를 배포할 호스트 또는 클러스터를 선택합니다.
- 6 NSX Controller에 대한 포트 그룹 또는 대상 네트워크를 선택합니다.
- 7 NSX Controller 암호 및 IP 설정을 지정합니다.
- 8 (선택 사항) 최적의 성능을 위해서는 NSX-T Data Center 구성 요소용 메모리를 예약합니다.
메모리 예약은 메모리가 오버 커밋되더라도 호스트가 가상 시스템을 위해 예약하는 물리적 메모리 양에 대해 보장되는 하한 값입니다. NSX-T Data Center 구성 요소가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정합니다. [시스템 요구 사항](#)의 내용을 참조하십시오.
- 9 NSX-T Data Center 구성 요소의 콘솔을 열어 부팅 프로세스를 추적합니다.
- 10 NSX-T Data Center 구성 요소가 부팅되면 CLI에 관리자 권한으로 로그인하고 get interface eth0 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
```



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

11 NSX-T Data Center 구성 요소에 필요한 연결이 있는지 확인합니다.

다음 작업을 수행할 수 있는지 확인하십시오.

- 다른 시스템에서 NSX-T Data Center 구성 요소를 Ping합니다.
- NSX-T Data Center 구성 요소에서 기본 게이트웨이를 Ping할 수 있습니다.
- NSX-T Data Center 구성 요소에서 관리 인터페이스를 사용하여 NSX-T Data Center 구성 요소와 동일한 네트워크에 있는 하이퍼바이저 호스트를 Ping할 수 있습니다.
- NSX-T Data Center 구성 요소에서는 DNS 서버와 NTP 서버를 Ping할 수 있습니다.
- SSH를 사용하도록 설정한 경우 NSX-T Data Center 구성 요소에 대해 SSH를 수행할 수 있는지 확인합니다.

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

다음에 수행할 작업

NSX Controller를 관리부에 연결합니다. [NSX Controller를 NSX Manager에 연결](#)의 내용을 참조하십시오.

명령줄 OVF 도구를 사용하여 ESXi에 NSX Controller 설치

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

기본적으로 nsx_isSSHEnabled 및 nsx_allowSSHRootLogin은 보안상의 이유로 둘 다 사용되지 않도록 설정됩니다. 사용되지 않도록 설정되면 SSH를 실행하거나 NSX Controller 명령줄에 로그인할 수 없습니다. nsx_isSSHEnabled는 사용하도록 설정하고 nsx_allowSSHRootLogin은 사용하지 않도록 설정하면 NSX Controller에 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.
- 대상 VM 포트 그룹 네트워크가 아직 없으면 생성합니다. NSX-T Data Center 장치를 관리 VM 네트워크에 배치하는 것이 좋습니다.
여러 관리 네트워크가 있으면 NSX-T Data Center 장치에서 다른 네트워크로의 정적 경로를 추가할 수 있습니다.
- IPv4 IP 주소 체계를 계획합니다. 이 NSX-T Data Center 릴리스에서는 IPv6가 지원되지 않습니다.
- OVF Tool 버전 4.0 이상

절차

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

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-controller
--X: injectOvfEnv
--X: logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--network="management"
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.210
--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|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-controller
<path/url to nsx component ova>
vi://root:<password>@192.168.110.51
```

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

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-controller
--X: injectOvfEnv
--X: logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--network="management"
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.210
--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|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-controller
<path/url to nsx component ova>
vi://administrator@vsphere.local:<vcenter_password>@192.168.110.24/?ip=192.168.110.51
```

- (선택 사항) 최적의 성능을 위해서는 NSX-T Data Center 구성 요소용 메모리를 예약합니다.

메모리 예약은 메모리가 오버 커밋되더라도 호스트가 가상 시스템을 위해 예약하는 물리적 메모리 양에 대해 보장되는 하한 값입니다. NSX-T Data Center 구성 요소가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정합니다. [시스템 요구 사항](#)의 내용을 참조하십시오.

- NSX-T Data Center 구성 요소의 콘솔을 열어 부팅 프로세스를 추적합니다.
- NSX-T Data Center 구성 요소가 부팅되면 CLI에 관리자 권한으로 로그인하고 get interface eth0 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

- NSX-T Data Center 구성 요소에 필요한 연결이 있는지 확인합니다.

다음 작업을 수행할 수 있는지 확인하십시오.

- 다른 시스템에서 NSX-T Data Center 구성 요소를 Ping합니다.
- NSX-T Data Center 구성 요소에서 기본 게이트웨이를 Ping할 수 있습니다.
- NSX-T Data Center 구성 요소에서 관리 인터페이스를 사용하여 NSX-T Data Center 구성 요소와 동일한 네트워크에 있는 하이퍼바이저 호스트를 Ping할 수 있습니다.
- NSX-T Data Center 구성 요소에서는 DNS 서버와 NTP 서버를 Ping할 수 있습니다.
- SSH를 사용하도록 설정한 경우 NSX-T Data Center 구성 요소에 대해 SSH를 수행할 수 있는지 확인합니다.

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

다음에 수행할 작업

NSX Controller를 관리부에 연결합니다. [NSX Controller를 NSX Manager에 연결](#)의 내용을 참조하십시오.

KVM에 NSX Controller 설치

NSX Controller는 네트워크 내의 모든 논리적 스위치에 대한 중앙 제어 지점으로서 모든 호스트, 논리적 스위치 및 논리적 분산 라우터에 대한 정보를 유지 관리합니다.

QCOW2 설치 절차에서는 Linux 명령줄 도구인 guestfish를 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.

절차

- 1 NSX Controller QCOW2 이미지를 /var/lib/libvirt/images 디렉토리에 다운로드합니다.
- 2 (Ubuntu만 해당) 현재 로그인한 사용자를 libvirtd 사용자로 추가합니다.

```
adduser $USER libvirtd
```

- 3 QCOW2 이미지를 저장한 동일한 디렉토리에 guestinfo(파일 확장명 없음)라는 파일을 만들고 NSX Controller VM의 속성으로 채웁니다.

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_allowSSHRootLogin" oe:value="True"/>
    <Property oe:key="nsx_cli_audit_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_cli_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_dns1_0" oe:value="192.168.110.10"/>
    <Property oe:key="nsx_domain_0" oe:value="corp.local"/>
    <Property oe:key="nsx_gateway_0" oe:value="192.168.110.1"/>
    <Property oe:key="nsx_hostname" oe:value="nsx-Controller1"/>
    <Property oe:key="nsx_ip_0" oe:value="192.168.110.34"/>
    <Property oe:key="nsx_isSSHEnabled" oe:value="True"/>
    <Property oe:key="nsx_netmask_0" oe:value="255.255.255.0"/>
    <Property oe:key="nsx_ntp_0" oe:value="192.168.110.10"/>
    <Property oe:key="nsx_passwd_0" oe:value="<password>"/>
  </PropertySection>
</Environment>
```

이 예에서 nsx_isSSHEnabled 및 nsx_allowSSHRootLogin은 둘 다 사용되도록 설정됩니다. 사용되지 않도록 설정되면 SSH를 실행하거나 NSX Controller 명령줄에 로그인할 수 없습니다. nsx_isSSHEnabled는 사용하도록 설정하고 nsx_allowSSHRootLogin은 사용하지 않도록 설정하면 NSX Controller에 대해 SSH를 실행할 수 있으나 루트 권한으로 로그인할 수 없습니다.

4 guestfish를 사용하여 QCOW2 이미지에 guestinfo 파일을 기록합니다.

여러 NSX Controller를 만드는 경우 각 컨트롤러에 대해 별도 QCOW2 이미지 사본을 만듭니다. guestinfo 정보가 QCOW2 이미지에 기록되면 정보를 덮어쓸 수 없습니다.

```
sudo guestfish --rw -i -a nsx-controller1-build.qcow2 upload guestinfo /config/guestinfo
```

5 virt-install 명령을 사용하여 QCOW2 이미지를 배포합니다.

```
user@ubuntu1604:/var/lib/libvirt/images$ sudo virt-install --import --name nsx-controller1 --ram 16384 --vcpus 2 --network=bridge:br0,model=e1000 --disk path=/var/lib/libvirt/images/nsx-controller-release_version_number.qcow2,format=qcow2 --nographics --noautoconsole
```

NSX Controller가 부팅된 후에 NSX Controller 콘솔이 나타납니다.

6 (선택 사항) 최적의 성능을 위해서는 NSX-T Data Center 구성 요소용 메모리를 예약합니다.

메모리 예약은 메모리가 오버 커밋되더라도 호스트가 가상 시스템을 위해 예약하는 물리적 메모리 양에 대해 보장되는 하한 값입니다. NSX-T Data Center 구성 요소가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정합니다. [시스템 요구 사항](#)의 내용을 참조하십시오.

7 NSX-T Data Center 구성 요소의 콘솔을 열어 부팅 프로세스를 추적합니다.

8 NSX-T Data Center 구성 요소가 부팅되면 CLI에 관리자 권한으로 로그인하고 get interface eth0 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

9 NSX-T Data Center 구성 요소에 필요한 연결이 있는지 확인합니다.

다음 작업을 수행할 수 있는지 확인하십시오.

- 다른 시스템에서 NSX-T Data Center 구성 요소를 Ping합니다.
- NSX-T Data Center 구성 요소에서 기본 게이트웨이를 Ping할 수 있습니다.
- NSX-T Data Center 구성 요소에서 관리 인터페이스를 사용하여 NSX-T Data Center 구성 요소와 동일한 네트워크에 있는 하이퍼바이저 호스트를 Ping할 수 있습니다.
- NSX-T Data Center 구성 요소에서는 DNS 서버와 NTP 서버를 Ping할 수 있습니다.
- SSH를 사용하도록 설정한 경우 NSX-T Data Center 구성 요소에 대해 SSH를 수행할 수 있는지 확인합니다.

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

다음에 수행할 작업

NSX Controller를 관리부에 연결합니다. [NSX Controller를 NSX Manager에 연결](#)의 내용을 참조하십시오.

NSX Controller 를 NSX Manager 에 연결

NSX Controller를 NSX Manager에 연결하면 NSX Manager 및 NSX Controller가 서로 통신할 수 있습니다.

사전 요구 사항

- NSX Manager가 설치되어 있는지 확인합니다.
- NSX Manager 및 NSX Controller 장치에 로그인할 수 있는 관리자 권한이 있는지 확인합니다.

절차

- 1 NSX Manager에 대해 SSH 세션을 엽니다.
- 2 각 NSX Controller 장치에 대해 SSH 세션을 엽니다.
예: NSX-Controller1, NSX-Controller2, NSX-Controller3.
- 3 NSX Manager에서 `get certificate api thumbprint` 명령을 실행합니다.

```
NSX-Manager> get certificate api thumbprint
...
```

- 4 각 NSX Controller 장치에서 **join management-plane** 명령을 실행합니다.

```
NSX-Controller1> join management-plane NSX-Manager-IP-address username admin thumbprint <NSX-Manager-thumbprint>

Password for API user: <NSX-Manager-password>
Node successfully registered and controller restarted
```

배포된 각 NSX Controller 노드에서 다음 명령을 실행합니다.

다음 정보를 입력합니다.

- 포트 번호(선택 사항)가 있는 NSX Manager의 IP 주소
 - NSX Manager의 사용자 이름
 - NSX Manager의 인증서 지문
 - NSX Manager의 암호
- 5 NSX Controller에서 `get managers` 명령을 실행하여 결과를 확인합니다.

```
NSX-Controller1> get managers
- 192.168.110.47 Connected
```

- 6 NSX Manager 장치에서 `get management-cluster status` 명령을 실행하고 NSX Controller가 나열되는지 확인합니다.

```

NSX-Manager> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.47 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.201 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
- 192.168.110.202 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
- 192.168.110.203 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)

```

다음에 수행할 작업

제어 컨트롤러를 초기화합니다. [제어 클러스터를 초기화하여 제어 클러스터 마스터 생성](#)의 내용을 참조하십시오.

제어 클러스터를 초기화하여 제어 클러스터 마스터 생성

NSX-T Data Center 배포에서 첫 번째 NSX Controller를 설치한 후에 제어 클러스터를 초기화할 수 있습니다. 제어 클러스터를 초기화하는 작업은 컨트롤러 노드가 하나만 있는 소규모 개념 증명 환경을 설정하는 경우에도 필요합니다. 제어 클러스터를 초기화하지 않으면 컨트롤러가 하이퍼바이저 호스트와 통신할 수 없습니다. 클러스터에서 하나의 컨트롤러만 초기화해야 합니다.

사전 요구 사항

- 하나 이상의 NSX Controller를 설치합니다.
- NSX Controller를 관리부에 연결합니다.
- NSX Controller 장치에 로그인할 수 있는 관리자 권한이 있는지 확인합니다.
- 공유 암호를 할당합니다. 공유 암호는 사용자 정의 공유 암호(예: "secret123")입니다.

절차

- 1 NSX Controller의 SSH 세션을 엽니다.
- 2 `set control-cluster security-model shared-secret secret <secret>` 명령을 실행하고 공유 암호를 입력하라는 메시지가 표시되면 입력합니다.
- 3 `initialize control-cluster` 명령을 실행합니다.

이 명령을 실행하면 이 컨트롤러가 제어 클러스터 마스터가 됩니다.

예:

```

NSX-Controller1> initialize control-cluster
Control cluster initialization successful.

```

4 get control-cluster status verbose 명령을 실행합니다.

is master 및 in majority가 true인지, 상태가 active이고 Zookeeper Server IP가 reachable, ok 인지 확인합니다.

```
nsx-controller1> get control-cluster status verbose
NSX Controller Status:

uuid: 78d5b561-4f66-488d-9e53-089735eac1c1
is master: true
in majority: true

```

uuid	address	status
78d5b561-4f66-488d-9e53-089735eac1c1	192.168.110.34	active

```
Cluster Management Server Status:


```

uuid	address	status	rpc address	rpc port	global id	vpn
557a911f-41fd-4977-9c58-f3ef55b3efe7	192.168.110.34	connected	192.168.110.34	7777	1	
169.254.1.1						

```
Zookeeper Ensemble Status:

Zookeeper Server IP: 10.0.0.1, reachable, ok
Zookeeper version: 3.5.1-alpha--1, built on 03/08/2016 01:18 GMT
Latency min/avg/max: 0/0/1841
Received: 212095
Sent: 212125
Connections: 5
Outstanding: 0
Zxid: 0x10000017a
Mode: leader
Node count: 33
Connections: /10.0.0.1:51726[1]
(queueued=0,recved=60324,sent=60324,sid=0x100000f14a10003,lop=PING,est=1459376913497,to=30000,lcid=0x8,lzcid=0x10000017a,lresp=604617273,llat=0,minlat=0,avglat=0,maxlat=1088)
/10.0.0.1:35462[0](queued=0,recved=1,sent=0)
/10.0.0.1:51724[1]
(queueued=0,recved=45786,sent=45803,sid=0x100000f14a10001,lop=GETC,est=1459376911226,to=40000,lcid=0x21e,lzcid=0x10000017a,lresp=604620658,llat=0,minlat=0,avglat=0,maxlat=1841)
/10.0.0.1:51725[1]
(queueued=0,recved=60328,sent=60333,sid=0x100000f14a10002,lop=PING,est=1459376913455,to=30000,lcid=0xc,lzcid=0x10000017a,lresp=604618294,llat=0,minlat=0,avglat=0,maxlat=1356)
/10.0.0.1:51730[1]
(queueued=0,recved=45315,sent=45324,sid=0x100000f14a10006,lop=PING,est=1459376914516,to=40000,lcid=0x49,lzcid=0x10000017a,lresp=604623243,llat=0,minlat=0,avglat=0,maxlat=1630)
```

다음에 수행할 작업

추가 NSX Controller를 제어 클러스터에 추가합니다. [클러스터 마스터에 추가 NSX Controller 연결의 내용을 참조하십시오.](#)

클러스터 마스터에 추가 NSX Controller 연결

NSX Controller의 다중 노드 클러스터를 유지하면 하나 이상의 NSX Controller를 항상 사용할 수 있습니다.

사전 요구 사항

- 최소 3개의 NSX Controller 장치를 설치합니다.
- NSX Controller 장치에 로그인할 수 있는 관리자 권한이 있는지 확인합니다.
- NSX Controller 노드가 관리부에 연결되어 있는지 확인합니다. [NSX Controller를 NSX Manager에 연결](#)의 내용을 참조하십시오.
- 제어 클러스터를 초기화하여 제어 클러스터 마스터를 생성합니다. 첫 번째 컨트롤러만 초기화해야 합니다.
- `join control-cluster` 명령에서는 도메인 이름이 아닌 IP 주소를 사용해야 합니다.
- vCenter를 사용하고 NSX-T Data Center 컨트롤러를 동일한 클러스터에 배포하려면 DRS 반선택도 규칙을 구성해야 합니다. 반선택도 규칙이 있으면 DRS가 둘 이상의 노드를 단일 호스트로 마이그레이션할 수 없습니다.

절차

- 1 각 NSX Controller 장치에 대해 SSH 세션을 엽니다.

예: NSX-Controller1, NSX-Controller2, NSX-Controller3. 이 예에서 NSX-Controller1은 제어 클러스터를 이미 초기화했으며 제어 클러스터 마스터입니다.

- 2 비마스터 NSX Controller에서 공유 암호를 사용하여 `set control-cluster security-model` 명령을 실행합니다. NSX-Controller2 및 NSX-Controller3에 대해 입력된 공유 암호는 NSX-Controller1에 입력한 공유 암호와 일치해야 합니다.

예:

```
NSX-Controller2> set control-cluster security-model shared-secret secret <NSX-Controller1' s-shared-secret-password>
```

```
Security secret successfully set on the node.
```

```
NSX-Controller3> set control-cluster security-model shared-secret secret <NSX-Controller1' s-shared-secret-password>
```

```
Security secret successfully set on the node.
```

- 3 비마스터 NSX Controller에서 `get control-cluster certificate thumbprint` 명령을 실행합니다.

명령 출력은 각 NSX Controller에 고유한 숫자열입니다.

예:

```
NSX-Controller2> get control-cluster certificate thumbprint
...
```

```
NSX-Controller3> get control-cluster certificate thumbprint
...
```

- 4 마스터 NSX Controller에서 `join control-cluster` 명령을 실행합니다.

다음 정보를 입력합니다.

- 비마스터 NSX Controller의 포트 번호(선택 사항)와 함께 IP 주소(이 예에서는 NSX-Controller2 및 NSX-Controller3)
- 비마스터 NSX Controller의 인증서 지문

여러 컨트롤러에 대해 `join` 명령을 동시에 실행하지 마십시오. 다른 컨트롤러를 연결하기 전에 각 연결을 완료해야 합니다.

```
NSX-Controller1> join control-cluster <NSX-Controller2-IP> thumbprint <nsx-controller2's-thumbprint>
Node 192.168.210.48 has successfully joined the control cluster.
Please run 'activate control-cluster' command on the new node.
```

`get control-cluster status` 명령을 실행하여 NSX-Controller2가 클러스터에 연결되었는지 확인합니다.

```
NSX-Controller1> join control-cluster <NSX-Controller3-IP> thumbprint <nsx-controller3's-thumbprint>
Node 192.168.210.49 has successfully joined the control cluster.
Please run 'activate control-cluster' command on the new node.
```

`get control-cluster status` 명령을 실행하여 NSX-Controller3가 클러스터에 연결되었는지 확인합니다.

- 5 제어 클러스터 마스터에 연결된 두 NSX Controller 노드에서 `activate control-cluster` 명령을 실행합니다.

참고 여러 NSX Controller에 대해 `activate` 명령을 병렬로 실행하지 마십시오. 다른 컨트롤러를 활성화하기 전에 각 활성화를 완료해야 합니다.

예:

```
NSX-Controller2> activate control-cluster
Control cluster activation successful.
```

NSX-Controller2에서 `get control-cluster status verbose` 명령을 실행하고 Zookeeper Server IP가 reachable, ok인지 확인합니다.

```
NSX-Controller3> activate control-cluster
Control cluster activation successful.
```

NSX-Controller3에서 `get control-cluster status verbose` 명령을 실행하고 Zookeeper Server IP가 reachable, ok인지 확인합니다.

6 get control-cluster status 명령을 실행하여 결과를 확인합니다.

```
NSX-Controller1> get control-cluster status
uuid: db4aa77a-4397-4d65-ad33-9fde79ac3c5c
is master: true
in majority: true
  uuid                                address                status
  ---                                -
0cfe232e-6c28-4fea-8aa4-b3518baef00d 192.168.210.47         active
bd257108-b94e-4e6d-8b19-7fa6c012961d 192.168.210.48         active
538be554-1240-40e4-8e94-1497e963a2aa 192.168.210.49         active
```

표시된 첫 번째 UUID는 전체 제어 클러스터에 대한 것입니다. 각 NSX Controller 노드도 UUID를 갖습니다.

컨트롤러를 클러스터에 연결하려고 하는데 명령 `set control-cluster security-model` 또는 `join control-cluster`가 실패하는 경우 클러스터 구성 파일이 일관되지 못한 상태에 있을 수 있습니다.

이 문제를 해결하려면 다음 단계를 수행합니다.

- 클러스터에 연결하려는 NSX Controller에서 `deactivate control-cluster` 명령을 실행합니다.
- 마스터 컨트롤러에서 명령 `get control-cluster status` 또는 `get control-cluster status verbose`가 실패한 컨트롤러에 대한 정보를 표시하면 `detach control-cluster <IP address of failed controller>` 명령을 실행합니다.

다음에 수행할 작업

NSX Edge를 배포합니다. [장6NSX Edge 설치](#)의 내용을 참조하십시오.

NSX Edge 설치

NSX Edge에서는 NSX-T Data Center 배포 외부에 있는 네트워크에 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.

표 6-1. 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 알고리즘으로 암호화해야 합니다.
NSX-T Data Center 장치 암호	<ul style="list-style-type: none"> ■ 8자 이상의 문자 ■ 하나 이상의 소문자 ■ 하나 이상의 대문자 ■ 하나 이상의 숫자 ■ 하나 이상의 특수 문자 ■ 5개 이상의 다른 문자 ■ 사전 단어 제외 ■ 회문 제외
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. 시스템 요구 사항 의 내용을 참조하십시오.

표 6-1. NSX Edge 배포, 플랫폼 및 설치 요구 사항 (계속)

요구 사항	설명
NSX 포트	필수 포트가 열려 있는지 확인합니다. 포트 및 프로토콜 의 내용을 참조하십시오. 대상 VM 포트 그룹 네트워크가 아직 없으면 생성합니다. NSX-T Data Center 장치를 관리 VM 네트워크에 배치하는 것이 좋습니다.
IP 주소	여러 관리 네트워크가 있으면 NSX-T Data Center 장치에서 다른 네트워크로의 정적 경로를 추가할 수 있습니다. IPv4 IP 주소 체계를 계획합니다. 이 NSX-T Data Center 릴리스에서는 IPv6가 지원되지 않습니다. IPv6 형식은 지원되지 않습니다.
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 <code>nsx-manager</code>로 설정됩니다. vCenter Server 또는 vSphere Client와 같은 OVF 템플릿을 배포할 수 있는 관리 도구. OVF 배포 도구는 수동 구성을 허용하는 구성 옵션을 지원해야 합니다. 클라이언트 통합 플러그인이 설치되어 있어야 합니다.
NTP 서버	Edge 클러스터의 모든 NSX Edge 서버에 동일한 NTP 서버를 구성해야 합니다.

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 **vmware** 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** 사용자에 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.

본 장은 다음 항목을 포함합니다.

- [NSX Edge 네트워킹 설정](#)
- [NSX Manager에서 NSX Edge VM의 자동 배포](#)
- [vSphere GUI를 사용하여 ESXi에 NSX Edge 설치](#)
- [명령줄 OVF 도구를 사용하여 ESXi에 NSX Edge 설치](#)
- [PXE 서버와 ISO 파일을 사용하여 NSX Edge 설치](#)
- [NSX Edge를 관리부에 연결](#)

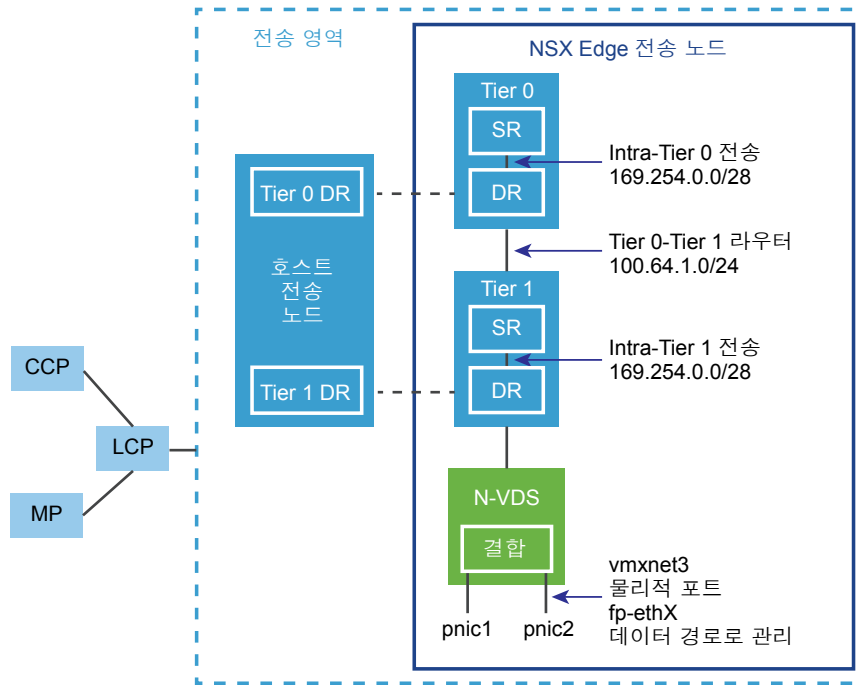
NSX Edge 네트워킹 설정

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 Edge 노드는 실행 중인 네트워크 서비스 전용으로, 하이퍼바이저에 배포할 수 없는 용량 풀을 사용하는 서비스 장치입니다. Edge 노드는 처음 배포될 때 빈 컨테이너로 보일 수 있습니다.

그림 6-1. NSX Edge 의 상위 수준 개요



NSX Edge 노드는 물리적 인프라에 연결하기 위해 물리적 NIC를 제공하는 장치입니다. 이러한 기능에는 다음이 포함됩니다.

- 물리적 인프라에 연결
- NAT
- DHCP 서버
- 메타데이터 프로кси
- Edge 방화벽

이러한 서비스 중 하나가 구성되거나 논리적 라우터에서 물리적 인프라에 연결하기 위한 업링크가 정의된 경우, SR은 NSX Edge 노드에서 인스턴스화됩니다. NSX Edge 노드는 또한 NSX-T Data Center의 계산 노드와 마찬가지로 전송 노드이기도 하며, 계산 노드와 유사합니다. NSX Edge는 둘 이상의 전송 영역(오버레이용 1개, 외부 디바이스와의 북-남 피어링용 1개)에 연결될 수 있습니다. NSX Edge에는 전송 영역이 두 개 있습니다.

오버레이 전송 영역 - NSX-T Data Center 도메인에 참가하는 VM에서 발생한 모든 트래픽이 처리하려면 외부 디바이스 또는 네트워크에 연결되어야 할 수 있습니다. 일반적으로 외부 북-남 트래픽으로 설명됩니다. NSX Edge 노드는 계산 노드에서 수신되는 오버레이 트래픽의 캡슐화를 해제하고 계산 노드로 전송된 트래픽을 캡슐화하는 역할을 합니다.

VLAN 전송 영역 - 트래픽 캡슐화 또는 캡슐화 해제 기능 외에, NSX Edge 노드에는 물리적 인프라에 대한 업링크 연결을 제공하기 위한 VLAN 전송 영역도 필요합니다.

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 Edge를 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.

NSX Edge의 고급 개요 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 가장 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.

베어메탈 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.

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

전송 영역 및 N-VDS

전송 영역은 NSX-T Data Center의 계층 2 네트워크 도달 영역을 제어합니다. N-VDS는 전송 노드에서 생성되는 소프트웨어 스위치입니다. 전송 노드의 데이터부에 포함되는 기본 구성 요소는 N-VDS입니다. N-VDS는 전송 노드에서 실행되는 구성 요소 간(예: 가상 시스템 간 또는 내부 구성 요소와 물리적 네트워크 간)에 트래픽을 전달합니다. 후자의 경우 N-VDS는 전송 노드에서 하나 이상의 물리적 인터페이스(pNIC)를 소유해야 합니다. 다른 가상 스위치와 마찬가지로 N-VDS는 다른 N-VDS와 물리적 인터페이스를 공유할 수 없습니다. 별도의 pNIC 집합을 사용하는 경우 다른 N-VDS와 공존할 수 있습니다.

전송 영역에는 두 가지 유형이 있습니다.

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

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.

전송 영역에 대한 자세한 내용은 [전송 영역 정보](#)를 참조하십시오.

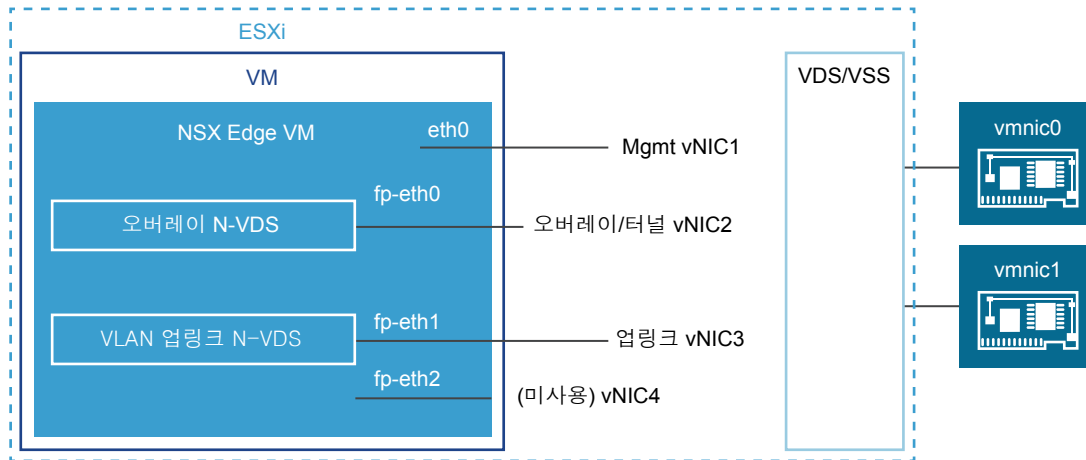
가상 장치/VM NSX Edge 네트워킹

NSX Edge VM에는 4개의 내부 인터페이스, 즉 eth0, fp-eth0, fp-eth1 및 fp-eth2가 있습니다. Eth0은 관리를 위해 예약되어 있지만 나머지 인터페이스는 DPDK 빠른 경로에 할당됩니다. 이러한 인터페이스는 TOR 스위치로의 업링크 및 NSX-T Data Center 오버레이 터널링에 할당됩니다. 인터페이스 할당은 업링크 또는 오버레이에서 유연하게 진행됩니다. 예를 들어, fp-eth0은 오버레이 트래픽용으로 할당할 수 있고, fp-eth1, fp-eth2 또는 둘 다를 업링크 트래픽용으로 할당할 수 있습니다.

vSphere 분산 스위치 또는 vSphere 표준 스위치에서 이중화를 위해 2개 이상의 vmnic를 NSX Edge에 할당해야 합니다.

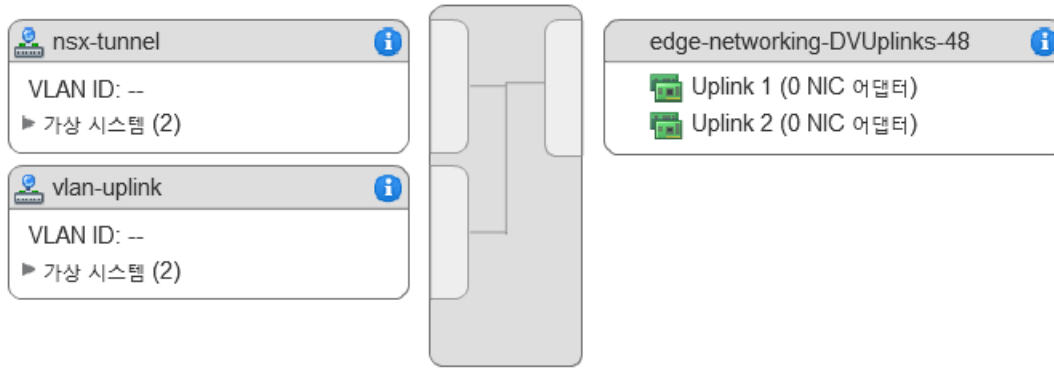
다음 샘플 물리적 토폴로지에서 eth0는 관리 네트워크에 사용되고, fp-eth0는 NSX-T Data Center 오버레이 트래픽에 사용되며, fp-eth1은 VLAN 업링크에 사용되고, fp-eth2는 사용되지 않습니다. fp-eth2가 사용되지 않는 경우 연결을 끊어야 합니다.

그림 6-2. 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 ovftool을 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.

예를 들어 표준 vSwitch에서는 트렁크 포트를 다음과 같이 구성할 수 있습니다. **호스트 > 구성 > 네트워크 > 네트워킹 추가 > 가상 시스템 > VLAN ID 전체(4095)**.

NSX Edge VM을 vSphere 분산 스위치 또는 vSphere 표준 스위치에 설치할 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.

동일한 관리, VLAN 및 오버레이 포트 그룹을 활용하여 단일 호스트에 여러 개의 NSX Edge VM을 설치할 수 있습니다.

N-VDS가 아닌 vSphere가 있는 ESXi 호스트에 배포된 NSX Edge VM의 경우 다음을 수행해야 합니다.

- 이 NSX Edge에서 실행 중인 DHCP 서버에 대해 위조 전송을 사용하도록 설정합니다.
- 기본적으로 MAC 학습이 사용되지 않도록 설정되어 있기 때문에 NSX 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.

베어 메탈 NSX Edge 네트워킹

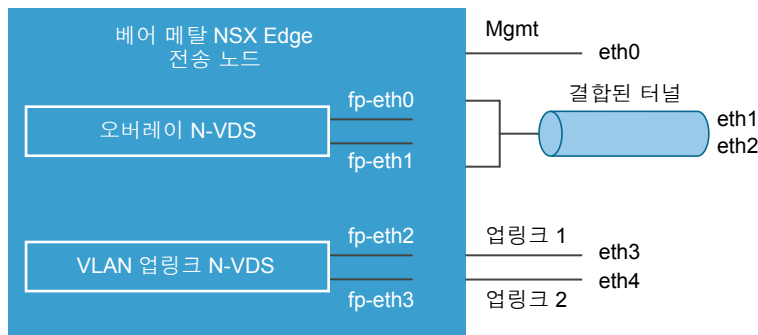
NSX-T Data Center 베어메탈 NSX Edge는 물리적 서버에서 실행되며 ISO 파일 또는 PXE 부팅을 사용하여 설치됩니다. 베어메탈 NSX Edge는 계층 3 유니캐스트 전달 외에 NAT, 방화벽 및 로드 밸런서와 같은 서비스가 필요한 운영 환경에서 권장됩니다. 베어메탈 NSX Edge는 성능 측면에서 VM 폼 팩터 NSX Edge와 다릅니다. 초단위 이하의 빠른 컨버전스, 신속한 페일오버 및 더 높은 처리량을 제공합니다.

베어메탈 NSX Edge 노드가 설치되면 관리를 위해 전용 인터페이스가 유지됩니다. 이중화가 필요한 경우 관리부 고가용성을 위해 두 개의 NIC를 사용할 수 있습니다. 이러한 관리 인터페이스는 1G일 수도 있습니다.

베어메탈 NSX Edge 노드는 TOR(랙 상단) 스위치로의 오버레이 트래픽 및 업링크 트래픽을 위해 최대 8개의 물리적 NIC를 지원합니다. 서버에 있는 이러한 8개의 각 물리적 NIC에 대해 이름 지정 체계 "fp-ethX"에 따라 내부 인터페이스가 생성됩니다. 이러한 내부 인터페이스는 DPDK 빠른 경로에 할당됩니다. 오버레이 또는 업링크 연결에 대해 fp-eth 인터페이스를 할당할 경우 유연하게 작업할 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 6-3. 베어 메탈 NSX Edge 네트워킹에 대해 제안되는 한 가지 링크 설정



NSX Manager 에서 NSX Edge VM의 자동 배포

NSX Manager UI에서 NSX Edge를 구성하고 vCenter Server에서 NSX Edge를 자동으로 배포할 수 있습니다.

사전 요구 사항

- [NSX Edge 네트워킹 설정](#)의 NSX Edge 네트워크 요구 사항을 참조하십시오.
- vCenter Server가 NSX-T Data Center에서 계산 관리자로 등록된 경우 NSX Manager UI를 사용하여 호스트를 NSX Edge 노드로 구성하고 vCenter Server에 자동으로 배포할 수 있습니다.
- NSX Edge를 설치 중인 vCenter Server의 데이터스토어에서 최소 120GB가 사용 가능한지 확인합니다.

- vCenter Server 클러스터 또는 호스트에서 구성의 지정된 네트워크 및 데이터스토어에 액세스할 수 있는지 확인합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **패브릭 > 노드 > Edge > Edge VM 추가**를 선택합니다.
- 3 NSX Edge의 이름을 입력합니다.
- 4 vCenter Server의 호스트 이름 또는 FQDN을 입력합니다.
- 5 작음, 중간 또는 큼 중에서 구성 크기를 선택합니다.
시스템 요구 사항은 구성 크기에 따라 다릅니다.
- 6 시스템의 CLI 및 루트 암호를 지정합니다.
루트 및 CLI 관리자 암호에 대한 제한 사항은 자동 배포에도 적용됩니다.
- 7 드롭다운 메뉴에서 [계산 관리자]를 선택합니다.
계산 관리자는 관리부에 등록된 vCenter Server입니다.
- 8 계산 관리자의 경우 드롭다운 메뉴에서 클러스터를 선택하거나 리소스 풀을 할당합니다.
- 9 NSX Edge 가상 시스템 파일을 저장할 데이터스토어를 선택합니다.
- 10 NSX Edge VM을 배포할 클러스터를 선택합니다.
네트워크 관리 유틸리티를 제공하는 클러스터에 NSX Edge를 추가하는 것이 좋습니다.
- 11 호스트 또는 리소스 풀을 선택합니다. 한 번에 하나의 호스트만 추가할 수 있습니다.
- 12 IP 주소를 선택하고 NSX Edge 인터페이스를 배치할 관리 네트워크 IP 주소 및 경로를 입력합니다. 입력된 IP 주소는 CIDR 형식이어야 합니다.
관리 네트워크에서 NSX Manager에 액세스할 수 있어야 합니다. DHCP 서버에서 IP 주소를 수신해야 합니다. NSX Edge가 배포된 후에 네트워크를 변경할 수 있습니다.
- 13 관리 네트워크 IP 주소가 NSX Manager 네트워크와 동일한 계층 2에 속하지 않는 경우 기본 게이트웨이를 추가합니다.
NSX Manager와 NSX Edge 관리 네트워크 간에 계층 3 연결을 사용할 수 있는지 확인합니다.

NSX Edge 배포를 완료하는 데 1 ~ 2분이 소요됩니다. UI에서 배포의 실시간 상태를 추적할 수 있습니다.

다음에 수행할 작업

NSX Edge 배포가 실패하면 `/var/log/cm-inventory/cm-inventory.log` 및 `/var/log/proton/nsxapi.log` 파일로 이동하여 문제를 해결합니다.

NSX Edge를 NSX Edge 클러스터에 추가하거나 전송 노드로 구성하기 전에 새로 생성된 NSX Edge 노드가 [노드 준비 완료]로 표시되는지 확인합니다.

vSphere GUI를 사용하여 ESXi에 NSX Edge 설치

대화형 NSX Edge 설치를 원할 경우 vCenter Server에 연결된 vSphere Client와 같은 UI 기반 VM 관리 도구를 사용할 수 있습니다.

이 NSX-T Data Center 릴리스에서는 IPv6가 지원되지 않습니다.

사전 요구 사항

- [NSX Edge 네트워킹 설정](#)의 NSX Edge 네트워크 요구 사항을 참조하십시오.

절차

- 1 NSX Edge OVA 또는 OVF 파일을 찾습니다.
다운로드 URL을 복사하거나 OVA 파일을 컴퓨터에 다운로드합니다.
- 2 관리 도구에서 **OVF 템플릿 배포** 마법사를 실행하고 .ova 파일을 찾거나 이 파일을 연결합니다.
- 3 NSX Edge의 이름을 입력하고 폴더 또는 vCenter Server 데이터센터를 선택합니다.
입력한 이름이 인벤토리에 나타납니다.
선택한 폴더는 NSX Edge에 사용 권한을 적용하는 데 사용됩니다.
- 4 작음, 중간 또는 큼 중에서 구성 크기를 선택합니다.
시스템 요구 사항은 구성 NSX Edge 배포 크기에 따라 다릅니다. [시스템 요구 사항](#)의 내용을 참조하십시오.
- 5 NSX Edge 가상 장치 파일을 저장할 데이터스토어를 선택합니다.
- 6 vCenter Server에서 설치하는 경우 NSX Edge 장치를 배포할 호스트 또는 클러스터를 선택합니다.
- 7 NSX Edge 인터페이스를 배치할 네트워크를 선택합니다.
NSX Edge가 배포된 후에 네트워크를 변경할 수 있습니다.
- 8 NSX Edge 암호 및 IP 설정을 지정합니다.
- 9 (선택 사항) 최적의 성능을 위해서는 NSX-T Data Center 구성 요소용 메모리를 예약합니다.
메모리 예약은 메모리가 오버 커밋되더라도 호스트가 가상 시스템을 위해 예약하는 물리적 메모리 양에 대해 보장되는 하한 값입니다. NSX-T Data Center 구성 요소가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정합니다. [시스템 요구 사항](#)의 내용을 참조하십시오.
- 10 NSX Edge의 콘솔을 열어 부팅 프로세스를 추적합니다.
콘솔 창이 열리지 않으면 팝업을 허용했는지 확인합니다.
- 11 NSX Edge가 시작된 후 관리자 권한으로 CLI에 로그인합니다. 사용자 이름은 **admin**이고 암호는 **default**입니다.

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

12 재부팅 후 관리 또는 루트 자격 증명으로 로그인할 수 있습니다. 기본 루트 암호는 **vmware**입니다.

13 `get interface eth0` 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

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

Interface: eth0
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
...
```

필요한 경우 `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` 명령을 실행하여 관리 인터페이스를 업데이트합니다. 경우에 따라 `start service ssh` 명령을 사용하여 SSH 서비스를 시작할 수 있습니다.

14 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.

15 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. DHCP가 잘못된 NIC를 관리로 지정하면 작업을 완료하여 문제를 해결합니다.

- a CLI에 로그인하고 `stop service dataplane` 명령을 입력합니다.
- b `set interface eth0 dhcp plane mgmt` 명령을 입력합니다.
- c eth0를 DHCP 네트워크에 배치하고 IP 주소가 eth0에 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 연결합니다. [NSX Edge를 관리부에 연결](#)의 내용을 참조하십시오.

명령줄 OVF 도구를 사용하여 ESXi에 NSX Edge 설치

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

이 NSX-T Data Center 릴리스에서는 IPv6가 지원되지 않습니다.

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.
- 대상 VM 포트 그룹 네트워크가 아직 없으면 생성합니다. NSX-T Data Center 장치를 관리 VM 네트워크에 배치하는 것이 좋습니다.

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

- IPv4 IP 주소 체계를 계획합니다. 이 NSX-T Data Center 릴리스에서는 IPv6가 지원되지 않습니다.
- [NSX Edge 네트워킹 설정](#)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 localhost로 설정됩니다.
- OVF Tool 버전 4.0 이상

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_isSSEnabled=True
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
<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_isSSEnabled=True
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
```



```
--prop:nsx_hostname=nsx-edge
<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
```

- (선택 사항) 최적의 성능을 위해서는 NSX-T Data Center 구성 요소용 메모리를 예약합니다.
메모리 예약은 메모리가 오버 커밋되더라도 호스트가 가상 시스템을 위해 예약하는 물리적 메모리 양에 대해 보장되는 하한 값입니다. NSX-T Data Center 구성 요소가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정합니다. [시스템 요구 사항](#)의 내용을 참조하십시오.
- NSX Edge의 콘솔을 열어 부팅 프로세스를 추적합니다.
- NSX Edge가 시작된 후 관리자 권한으로 CLI에 로그인합니다. 사용자 이름은 **admin**이고 암호는 **default**입니다.
- `get interface eth0` 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

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

Interface: eth0
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
...
```

필요한 경우 `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` 명령을 실행하여 관리 인터페이스를 업데이트합니다. 경우에 따라 `start service ssh` 명령을 사용하여 SSH 서비스를 시작할 수 있습니다.

- 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. DHCP가 잘못된 NIC를 관리로 지정하면 작업을 완료하여 문제를 해결합니다.

- CLI에 로그인하고 **stop service dataplane** 명령을 입력합니다.
- set interface eth0 dhcp plane mgmt** 명령을 입력합니다.
- eth0를 DHCP 네트워크에 배치하고 IP 주소가 eth0에 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 연결합니다. [NSX Edge를 관리부에 연결](#)의 내용을 참조하십시오.

PXE 서버와 ISO 파일을 사용하여 NSX Edge 설치

베어 메탈에서 자동화 방식으로 또는 PXE를 사용하여 VM으로 NSX Edge 디바이스를 설치할 수 있습니다.

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

NSX Edge 설치를 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 네트워킹 설정**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 <mgr-ip> thumbprint <mgr-thumbprint> username <mgr-username> password <mgr 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. mkpasswd와 같은 Linux 도구를 사용하여 암호 해시를 생성할 수 있습니다.

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

Password:
$6$SUFQqs[...]FcoHLijOuFD
```

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

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

- b 해시 문자열을 바꿉니다.
\$, ', " 또는 \와 같은 특수 문자는 이스케이프할 필요가 없습니다.
- c preseed.cfg에 usermod 명령을 추가하여 루트나 관리자 또는 둘 다의 암호를 설정합니다.
예를 들어 echo 'VMware NSX Edge' 줄을 검색하고 다음 명령을 추가합니다.

```
usermod --password '$6$W$VS3exld0aKmzWW$U3g0V7BF0DXlmRI.LR0v/VgIoxVotEDp00b02hUF8u/' root; W
usermod --password '$6$W$VS3exld0aKmzWW$U3g0V7BF0DXlmRI.LR0v/VgIoxVotEDp00b02hUF8u/' admin; W
```

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

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/pxelinux.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 stop을 실행한 다음 sudo /etc/init.d/isc-dhcp-server start를 실행합니다. sudo /etc/init.d/isc-dhcp-server start 명령은 오류 원인에 대한 정보를 반환합니다.

다음에 수행할 작업

베어메탈 또는 ISO 파일을 사용하여 NSX Edge를 설치합니다. [베어 메탈에 NSX Edge 설치](#) 또는 [ISO 파일을 통해 가상 장치로 NSX Edge 설치](#)의 내용을 참조하십시오.

베어 메탈에 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 네트워킹 설정](#)의 NSX Edge 네트워크 요구 사항을 참조하십시오.

절차

- 1 NSX Edge ISO 파일을 사용하여 부팅 가능 디스크를 생성합니다.
- 2 디스크에서 물리적 시스템을 부팅합니다.
- 3 **자동 설치**를 선택합니다.

Enter 키를 누른 후에 10초 동안 일시 중단될 수 있습니다.

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.

- 4 NSX Edge의 콘솔을 열어 부팅 프로세스를 추적합니다.

콘솔 창이 열리지 않으면 팝업을 허용했는지 확인합니다.

- 5 NSX Edge가 시작된 후 관리자 권한으로 CLI에 로그인합니다. 사용자 이름은 **admin**이고 암호는 **default**입니다.

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

- 6 재부팅 후 관리 또는 루트 자격 증명으로 로그인할 수 있습니다. 기본 루트 암호는 **vmware**입니다.
- 7 `get interface eth0` 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

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

Interface: eth0
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
...
```

필요한 경우 `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` 명령을 실행하여 관리 인터페이스를 업데이트합니다. 경우에 따라 `start service ssh` 명령을 사용하여 SSH 서비스를 시작할 수 있습니다.

- 8 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.

- 9 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. DHCP가 잘못된 NIC를 관리로 지정하면 작업을 완료하여 문제를 해결합니다.

- a CLI에 로그인하고 `stop service dataplane` 명령을 입력합니다.
- b `set interface eth0 dhcp plane mgmt` 명령을 입력합니다.

c eth0를 DHCP 네트워크에 배치하고 IP 주소가 eth0에 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 연결합니다. [NSX Edge를 관리부에 연결](#)의 내용을 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 네트워킹 설정](#)의 NSX Edge 네트워크 요구 사항을 참조하십시오.

절차

- 1 독립 실행형 호스트 또는 vCenter Web Client에서 VM을 생성하고 다음 리소스를 할당합니다.
 - 게스트 운영 체제: 기타(64비트)
 - 3개의 VMXNET3 NIC. NSX Edge는 e1000 NIC 드라이버를 지원하지 않습니다.
 - NSX-T Data Center 배포에 필요한 해당 시스템 리소스.

2 NSX Edge ISO 파일을 VM에 바인딩합니다.

CD/DVD 드라이브 디바이스 상태가 **전원을 켤 때 연결**로 설정되어 있는지 확인합니다.

3 ISO 부팅 중에 VM 콘솔을 열고 **자동 설치**를 선택합니다.

Enter 키를 누른 후에 10초 동안 일시 중단될 수 있습니다.

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.

- 8자 이상의 문자
- 하나 이상의 소문자
- 하나 이상의 대문자
- 하나 이상의 숫자
- 하나 이상의 특수 문자

- 5개 이상의 다른 문자
- 사전 단어 제외
- 회문 제외

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

- 4 (선택 사항) 최적의 성능을 위해서는 NSX-T Data Center 구성 요소용 메모리를 예약합니다.

메모리 예약은 메모리가 오버 커밋되더라도 호스트가 가상 시스템을 위해 예약하는 물리적 메모리 양에 대해 보장되는 하한 값입니다. NSX-T Data Center 구성 요소가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정합니다. [시스템 요구 사항](#)의 내용을 참조하십시오.

- 5 NSX Edge의 콘솔을 열어 부팅 프로세스를 추적합니다.

콘솔 창이 열리지 않으면 팝업을 허용했는지 확인합니다.

- 6 NSX Edge가 시작된 후 관리자 권한으로 CLI에 로그인합니다. 사용자 이름은 **admin**이고 암호는 **default**입니다.

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

- 7 재부팅 후 관리 또는 루트 자격 증명으로 로그인할 수 있습니다. 기본 루트 암호는 **vmware**입니다.

- 8 `get interface eth0` 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

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

Interface: eth0
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
...
```

필요한 경우 `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` 명령을 실행하여 관리 인터페이스를 업데이트합니다. 경우에 따라 `start service ssh` 명령을 사용하여 SSH 서비스를 시작할 수 있습니다.

- 9 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.

10 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. DHCP가 잘못된 NIC를 관리로 지정하면 작업을 완료하여 문제를 해결합니다.

- a CLI에 로그인하고 **stop service dataplane** 명령을 입력합니다.
- b **set interface eth0 dhcp plane mgmt** 명령을 입력합니다.
- c eth0를 DHCP 네트워크에 배치하고 IP 주소가 eth0에 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 연결합니다. [NSX Edge를 관리부에 연결](#)의 내용을 참조하십시오.

NSX Edge 설치 액세스 및 확인

NSX-T Data Center VM 또는 NSX-T Data Center 베어메탈 호스트에 로그인하여 설치에 성공했는지 확인하고 필요한 경우 문제를 해결할 수 있습니다.

사전 요구 사항

- PXE 서버가 설치용으로 구성되었는지 확인합니다. [NSX Edge 설치를 위한 PXE 서버 준비](#)의 내용을 참조하십시오.
- NSX Edge가 베어메탈을 사용하여 설치되었는지 아니면 ISO 파일을 사용하여 설치되었는지 확인합니다. [베어 메탈에 NSX Edge 설치](#) 또는 [ISO 파일을 통해 가상 장치로 NSX Edge 설치](#)의 내용을 참조하십시오.

절차

- 1 NSX-T Data Center VM 또는 NSX-T Data Center 베어메탈 호스트의 전원을 켭니다.
- 2 부팅 메뉴에서 **nsxedge**를 선택합니다.

네트워크가 구성되고, 파티션이 생성되고, NSX Edge 구성 요소가 설치됩니다.

NSX Edge 로그인 프롬프트가 표시되면 관리자 또는 루트 권한으로 로그인할 수 있습니다.

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

- 3 (선택 사항) 최적의 성능을 위해서는 NSX-T Data Center 구성 요소용 메모리를 예약합니다.

메모리 예약은 메모리가 오버 커밋되더라도 호스트가 가상 시스템을 위해 예약하는 물리적 메모리 양에 대해 보장되는 하한 값입니다. NSX-T Data Center 구성 요소가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정합니다. [시스템 요구 사항](#)의 내용을 참조하십시오.

4 NSX Edge의 콘솔을 열어 부팅 프로세스를 추적합니다.

콘솔 창이 열리지 않으면 팝업을 허용했는지 확인합니다.

5 NSX Edge가 시작된 후 관리자 권한으로 CLI에 로그인합니다. 사용자 이름은 **admin**이고 암호는 **default**입니다.

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

6 채부팅 후 관리 또는 루트 자격 증명으로 로그인할 수 있습니다. 기본 루트 암호는 **vmware**입니다.

7 `get interface eth0` 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

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

Interface: eth0
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
...
```

필요한 경우 `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` 명령을 실행하여 관리 인터페이스를 업데이트합니다. 경우에 따라 `start service ssh` 명령을 사용하여 SSH 서비스를 시작할 수 있습니다.

8 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.

9 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. DHCP가 잘못된 NIC를 관리로 지정하면 작업을 완료하여 문제를 해결합니다.

a CLI에 로그인하고 `stop service dataplane` 명령을 입력합니다.

b `set interface eth0 dhcp plane mgmt` 명령을 입력합니다.

- c eth0를 DHCP 네트워크에 배치하고 IP 주소가 eth0에 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 연결합니다. [NSX Edge를 관리부에 연결](#)의 내용을 참조하십시오.

NSX Edge 를 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

- 1 NSX Manager 장치에 대해 SSH 세션을 엽니다.
- 2 NSX Edge에 대해 SSH 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
...
```

- 4 NSX Edge에서 **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 NSX-Manager1 username admin thumbprint <NSX-Manager1's-thumbprint>
Password for API user: <NSX-Manager1's-password>
Node successfully registered and Edge restarted
```

각 NSX Edge 노드에서 다음 명령을 반복합니다.

NSX Edge에서 get managers 명령을 실행하여 결과를 확인합니다.

```
nsx-edge-1> get managers
- 192.168.110.47    Connected
```

NSX Manager UI에서 NSX Edge가 **패브릭 > 노드 > Edge** 페이지에 나타납니다.

NSX Manager 연결은 [실행] 상태여야 합니다. NSX Manager 연결이 [실행] 상태가 아니면 브라우저 화면을 새로 고쳐 봅니다.

다음에 수행할 작업

NSX Edge를 전송 노드로 추가합니다. [NSX Edge 전송 노드 생성](#)의 내용을 참조하십시오.

호스트 준비

NSX-T Data Center에서 작동할 수 있게 하이퍼바이저 호스트가 준비되면 이는 패브릭 노드로 알려 집니다. 패브릭 노드인 호스트에는 NSX-T Data Center 모듈이 설치되어 있고 NSX-T Data Center 관리부에 등록됩니다.

본 장은 다음 항목을 포함합니다.

- KVM 호스트 또는 베어메탈 서버에 타사 패키지 설치
- RHEL KVM 호스트의 Open vSwitch 버전 확인
- NSX-T Data Center 패브릭에 하이퍼바이저 호스트 또는 베어메탈 서버 추가
- NSX-T Data Center 커널 모듈의 수동 설치
- 하이퍼바이저 호스트를 관리부에 연결

KVM 호스트 또는 베어메탈 서버에 타사 패키지 설치

KVM 호스트 또는 베어메탈 서버를 패브릭 노드가 되도록 준비하려면 타사 패키지를 설치해야 합니다.

사전 요구 사항

- (Red Hat 및 CentOS) 타사 패키지를 설치하기 전에 가상화 패키지를 설치합니다. 호스트에서 다음 명령을 실행합니다.

```
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 수동으 로 설치할 수 있습니다.

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

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

- (베어메탈 서버) 타사 패키지 설치를 위한 가상화 사전 요구 사항은 없습니다.

절차

- Ubuntu 16.04.2 LTS에서 다음 타사 패키지가 호스트에 설치되어 있는지 확인합니다.

```
libunwind8
libgflags2v5
libgoogle-perftools4
traceroute
python-mako
python-simplejson
python-unittest2
python-yaml
python-netaddr
libprotobuf9v5
libboost-chrono1.58.0
libgoogle-glog0v5
dkms
libboost-date-time1.58.0
libleveldb1v5
libsnappy1v5
python-gevent
python-protobuf
ieee-data
libyaml-0-2
python-linecache2
python-traceback2
libtcmalloc-minimal4
python-greenlet
python-markupsafe
libboost-program-options1.58.0
```

Ubuntu 16.04.2 LTS에 종속성 패키지가 설치되지 않은 경우에는 `apt-get install <package>`를 실행하여 패키지를 수동으로 설치합니다.

- Red Hat 및 CentOS 호스트가 등록되어 있고 해당 리포지토리에 액세스할 수 있는지 확인합니다.

참고 NSX-T Data Center UI를 사용하여 호스트를 준비하는 경우 호스트에 다음 종속성을 설치해야 합니다.

RHEL 7.4 및 CentOS 7.4에 타사 패키지를 설치합니다.

```
yum-utils
wget
redhat-lsb-core
tcpdump
boost-filesystem
PyYAML
boost-iostreams
boost-chrono
python-mako
python-netaddr
python-six
gperftools-libs
libunwind
snappy
boost-date-time
c-ares
libev
python-gevent
python-greenlet
```

RHEL 7.5에 타사 패키지를 설치합니다.

```
PyYAML
c-ares
libev
libunwind
libyaml
python-beaker
python-gevent
python-greenlet
python-mako
python-markupsafe
python-netaddr
python-paste
python-tempita
```

- 이미 RHEL 및 CentOS에 등록된 호스트를 수동으로 준비하는 경우에는 호스트에 종속성을 설치하지 않아도 됩니다. 호스트가 등록되어 있지 않으면 `yum install <package>`를 사용하여 나열된 종속성을 수동으로 설치합니다.
- 베어메탈 서버에 타사 패키지를 설치합니다.
 - a 작업 환경에 따라, 이 항목의 나열된 Ubuntu, RHEL 또는 CentOS 타사 패키지를 설치합니다.
 - b 베어메탈 서버별 타사 패키지를 설치합니다.

Ubuntu - `apt-get install libvirt-libs`

RHEL 또는 CentOS - `yum install libvirt-libs`

RHEL KVM 호스트의 Open vSwitch 버전 확인

OVS 패키지가 호스트에 있는 경우 기존 패키지를 제거하고 지원되는 패키지를 설치해야 합니다.

지원되는 Open vSwitch 버전은 2.9.1.8614397-1입니다.

절차

- 1 현재 버전의 Open vSwitch가 호스트에 설치되어 있는지 확인합니다.

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

Open vSwitch 최신 버전 또는 이전 버전을 사용하는 경우 해당 Open vSwitch 버전을 지원되는 버전으로 교체해야 합니다

- a 다음 Open vSwitch 패키지를 삭제합니다.

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

- b NSX Manager에서 또는 수동 설치 절차에 따라 NSX-T Data Center를 설치합니다.

- 2 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>-rhel74_x86_64.tar.gz
```

- d 패키지 디렉토리로 이동합니다.

```
cd nsx-lcp-rhel74_x86_64/
```

- e 기존 Open vSwitch 버전을 지원되는 버전으로 교체합니다.

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

```
예: rpm -Uvh kmod-openvswitch-<new version>.e17.x86_64.rpm --nodeps
rpm -Uvh openvswitch-*.rpm --nodeps
```

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

```
예: rpm -Uvh kmod-openvswitch-<new version>.e17.x86_64.rpm --nodeps
--force
rpm -Uvh openvswitch-*.rpm --nodeps --force
```

다음에 수행할 작업

NSX-T Data Center 패브릭에 하이퍼바이저 호스트를 추가합니다. [NSX-T Data Center 패브릭에 하이퍼바이저 호스트 또는 베어메탈 서버 추가](#)의 내용을 참조하십시오.

NSX-T Data Center 패브릭에 하이퍼바이저 호스트 또는 베어메탈 서버 추가

패브릭 노드는 NSX-T Data Center 관리부에 등록되어 있고 NSX-T Data Center 모듈이 설치된 노드입니다. 하이퍼바이저 호스트 또는 베어메탈 서버가 NSX-T Data Center 오버레이에 속하려면 먼저 이를 NSX-T Data Center 패브릭에 추가해야 합니다.

CLI를 사용하여 호스트에 수동으로 모듈을 설치하고 호스트를 관리부에 연결했으면 이 절차를 건너뛰어도 됩니다.

참고 RHEL의 KVM 호스트의 경우 `sudo` 자격 증명을 사용하여 호스트 준비 활동을 수행할 수 있습니다.

사전 요구 사항

- NSX-T Data Center 패브릭에 추가하려는 각 호스트에 대해 먼저 다음 호스트 정보를 수집합니다.
 - 호스트 이름
 - 관리 IP 주소
 - 사용자 이름
 - 암호
 - (선택 사항) (KVM) SHA-256 SSL 지문
 - (선택 사항) (ESXi) SHA-256 SSL 지문
- Ubuntu의 경우 필요한 타사 패키지가 설치되어 있는지 확인합니다. [KVM 호스트 또는 베어메탈 서버에 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 vSphere 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:A2:4E:
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 NSX Manager CLI에서 install-upgrade 서비스가 실행되고 있는지 확인합니다.

```
nsx-manager-1> get service install-upgrade
```

```
Service name: install-upgrade
Service state: running
Enabled: True
```

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

- 4 **패브릭 > 노드 > 호스트**를 선택하고 **추가**를 클릭합니다.

- 5 호스트 이름, IP 주소, 사용자 이름, 암호 및 지문(선택 사항)을 입력합니다.

예:

호스트 추가



이름 *	comp-02b
IP 주소 *	192.168.210.54 ×
운영 체제 *	ESXi ▼
사용자 이름 *	root
암호 *	●●●●●●
SHA-256 지문	

취소

추가

베어메탈 서버의 경우 [운영 체제] 드롭다운 메뉴에서 **RHEL 서버**, **Ubuntu 서버** 또는 **CentOS 서버**를 선택할 수 있습니다.

호스트 지문을 입력하지 않으면 NSX-T Data Center UI에 호스트에서 검색된 기본 지문을 일반 텍스트 형식으로 사용하라는 메시지가 표시됩니다.

예 :

잘못된 지문



입력한 지문이 잘못되었습니다.

이 서버에서 제공된 지문을 사용하시겠습니까?

fa984ff00d4856c1e8db1be005ff908a3f2335bcd67776447e926aba71a006b8

아니요

추가



호스트가 NSX-T Data Center 패브릭에 추가되면 NSX Manager **호스트** 페이지에 **배포 상태: 설치 성공** 및 **MPA 연결: 실행**이 표시됩니다.

LCP 연결은 패브릭 노드를 전송 노드로 만들 때까지 사용할 수 없습니다.

- 6 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.

vSphere ESXi에서 모듈은 VIB로 패키징됩니다. RHEL의 KVM 또는 베어메탈 서버의 경우 RPM으로 패키징됩니다. Ubuntu의 KVM 또는 베어메탈 서버의 경우 DEB로 패키징됩니다.

- ESXi에서 `esxcli software vib list | grep nsx` 명령을 입력합니다.

날짜는 설치를 수행한 날짜입니다.

- RHEL에서 `yum list installed` 또는 `rpm -qa` 명령을 입력합니다.

- Ubuntu에서 `dpkg --get-selections` 명령을 입력합니다.

- 7 (선택 사항) 다음과 같이 GET `https://<nsx-mgr>/api/v1/fabric/nodes/<node-id>` API 호출을 사용하여 패브릭 노드를 확인합니다.

- 8 (선택 사항) GET `https://<nsx-mgr>/api/v1/fabric/nodes/<node-id>/status` API 호출을 사용하여 API에서 상태를 모니터링합니다.

- 9 (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 Manager IP address>' -u 'admin' -p '<password>' -i 900
```

- c (선택 사항) 폴링 간격을 다시 기본값으로 변경합니다.

```
python aggsvc_change_intervals.py -m '<NSX Manager IP address>' -u 'admin' -p '<password>' -r
```

다음에 수행할 작업

전송 영역을 생성합니다. [전송 영역 정보](#)의 내용을 참조하십시오.

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-aggservice_<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_nsx_<release>, VMware_bootbank_nsxcli_<release>
  VIBs Removed:
  VIBs Skipped:
```

호스트에 이미 설치된 항목에 따라 일부 VIB가 설치되고, 일부는 제거되고, 일부는 건너뛸 수 있습니다. 명령 출력에 `Reboot Required: true`로 표시되지 않는 한 재부팅은 필요하지 않습니다.

ESXi 호스트를 NSX-T Data Center 패브릭에 추가하면 호스트에 다음 VIB가 설치됩니다.

- `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-da`—하이퍼바이저 OS 버전, 가상 시스템 및 네트워크 인터페이스에 대한 DA(검색 에이전트) 데이터를 수집합니다. 문제 해결 도구에서 사용할 데이터를 관리부에 제공합니다.
- `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-lldp`—LAN에서 ID, 기능 및 인접 네트워크를 보급하기 위해 네트워크 디바이스에서 사용하는 링크 계층 프로토콜인 LLDP(Link Layer Discovery Protocol)를 지원합니다.
- `nsx-mpa`—NSX Manager 및 하이퍼바이저 호스트 간 통신을 제공합니다.
- `nsx-netcpa`—중앙 제어부 및 하이퍼바이저 간 통신을 제공합니다. 중앙 제어부에서 논리적 네트워크 상태를 수신하고 이 상태를 데이터부에서 프로그래밍합니다.
- `nsx-python-protobuf`—프로토콜 버퍼에 대한 Python 바인딩을 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.
- `nsxa`—N-VDS 생성 및 업링크 구성과 같은 호스트 수준 구성을 수행합니다.
- `nsxcli`—하이퍼바이저 호스트에서 NSX-T Data Center CLI를 제공합니다.
- `nsx-support-bundle-client`—지원 번들을 수집하는 기능을 제공합니다.

확인하려면 ESXi 호스트에서 **`esxcli software vib list | grep nsx`** 또는 **`esxcli software vib list | grep <yyyy-mm-dd>`** 명령을 실행하면 됩니다. 여기서 날짜는 설치를 수행한 날입니다.

다음에 수행할 작업

NSX-T Data Center 관리부에 호스트를 추가합니다. [하이퍼바이저 호스트를 관리부에 연결](#)의 내용을 참조하십시오.

Ubuntu KVM 하이퍼바이저에 수동으로 NSX-T Data Center 커널 모듈 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 호스트 또는 베어메탈 서버에 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 | grep nsx 명령을 실행하여 확인할 수 있습니다.

```
user@host:~$ dpkg -l | grep nsx
```

ii	nsx-agent	<release>	amd64	NSX Agent
ii	nsx-aggservice	<release>	all	NSX Aggregation Service Lib
ii	nsx-cli	<release>	all	NSX CLI
ii	nsx-da	<release>	amd64	NSX Inventory Discovery Agent
ii	nsx-host	<release>	all	NSX host meta package
ii	nsx-host-node-status-reporter	<release>	amd64	NSX Host Status Reporter for Aggregation Service
ii	nsx-lldp	<release>	amd64	NSX LLDP Daemon
ii	nsx-logical-exporter	<release>	amd64	NSX Logical Exporter

ii	nsx-mpa	<release>	amd64	NSX Management Plane Agent Core
ii	nsx-netcpa	<release>	amd64	NSX Netcpa
ii	nsx-sfhc	<release>	amd64	NSX Service Fabric Host Component
ii	nsx-transport-node-status-reporter	<release>	amd64	NSX Transport Node Status Reporter
ii	nsxa	<release>	amd64	NSX L2 Agent

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. [하이퍼바이저 호스트를 관리부에 연결](#)의 내용을 참조하십시오.

RHEL 및 CentOS KVM 하이퍼바이저에 수동으로 NSX-T Data Center 커널 모듈 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.

```
/etc/init.d/openvswitch 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|nicira' 명령을 실행하여 확인할 수 있습니다.

출력에 나열된 설치된 패키지는 nsx-rhel74 또는 nsx-centos74 디렉토리에 있는 패키지와 일치해야 합니다.

다음에 수행할 작업

NSX-T Data Center 관리부에 호스트를 추가합니다. [하이퍼바이저 호스트를 관리부에 연결](#)의 내용을 참조하십시오.

하이퍼바이저 호스트를 관리부에 연결

하이퍼바이저 호스트를 관리부에 연결하면 NSX Manager 및 호스트가 서로 통신할 수 있게 됩니다.

사전 요구 사항

NSX-T Data Center 모듈 설치가 완료되어야 합니다.

절차

- 1 NSX Manager 장치에 대해 SSH 세션을 엽니다.
- 2 관리자 자격 증명으로 로그인합니다.
- 3 하이퍼바이저 호스트에 대해 SSH 세션을 엽니다.
- 4 NSX Manager 장치에서 get certificate api thumbprint cli 명령을 실행합니다.

명령 출력은 이 NSX Manager에 고유한 숫자열입니다.

예:

```
NSX-Manager1> get certificate api thumbprint
...
```

5 하이퍼바이저 호스트에서 nsxcli 명령을 실행하여 NSX-T Data Center CLI를 시작합니다.

참고 KVM의 경우 다음 명령을 슈퍼유저(sudo) 권한으로 실행합니다.

```
[user@host:~] nsxcli
host>
```

프롬프트가 변경됩니다.

6 하이퍼바이저 호스트에서 **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

```
host> join management-plane NSX-Manager1 username admin thumbprint <NSX-Manager1's-thumbprint>
Password for API user: <NSX-Manager1's-password>
Node successfully joined
```

호스트에서 `get managers` 명령을 실행하여 결과를 확인합니다.

```
host> get managers
- 192.168.110.47 Connected
```

NSX Manager UI의 **패브릭 > 노드 > 호스트**에서 호스트의 MPA 연결이 **실행** 상태인지 확인합니다.

또한 **GET https://<nsx-mgr>/api/v1/fabric/nodes/<패브릭 노드 ID>/state** API 호출을 사용하여 패브릭 호스트의 상태를 확인할 수 있습니다.

```
{
  "details": [],
  "state": "success"
}
```

관리부는 제어부로 호스트 인증서를 전송하고, 제어부는 호스트로 제어부 정보를 푸시합니다.

각 ESXi 호스트에서 `/etc/vmware/nsx/controller-info.xml`의 NSX Controller 주소를 확인하거나 `get controllers`를 사용하여 CLI에 액세스해야 합니다.

```
[root@host:~] cat /etc/vmware/nsx/controller-info.xml
<?xml version="1.0" encoding="utf-8"?>
<config>
  <connectionList>
    <connection id="0">
      <server>10.143.1.47</server>
      <port>1234</port>
      <sslEnabled>true</sslEnabled>
      <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
    <connection id="1">
      <server>10.143.1.45</server>
      <port>1234</port>
      <sslEnabled>true</sslEnabled>
      <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
    <connection id="2">
      <server>10.143.1.46</server>
```

```

    <port>1234</port>
    <sslEnabled>true</sslEnabled>
    <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
  </connection>
</connectionList>
</config>

```

NSX-T Data Center에 대한 호스트 연결이 시작되고 호스트가 전송 노드로 승격될 때까지 "CLOSE_WAIT" 상태가 유지됩니다. 이 사항은 **esxcli network ip connection list | grep 1234** 명령을 실행하여 확인할 수 있습니다.

```

# esxcli network ip connection list | grep 1234
tcp          0      0 192.168.210.53:45823      192.168.110.34:1234  CLOSE_WAIT    37256  newreno  netcpa

```

KVM의 경우 해당 명령은 `netstat -anp --tcp | grep 1234`입니다.

```

user@host:~$ netstat -anp --tcp | grep 1234
tcp  0  0 192.168.210.54:57794  192.168.110.34:1234  CLOSE_WAIT -

```

다음에 수행할 작업

전송 영역을 생성합니다. [전송 영역 정보](#)의 내용을 참조하십시오.

전송 영역 및 전송 노드

전송 영역 및 전송 노드는 NSX-T Data Center에서 중요한 개념입니다.

본 장은 다음 항목을 포함합니다.

- 전송 영역 정보
- 고급 데이터 경로
- 터널 끝점 IP 주소에 대한 IP 풀 생성
- 업링크 프로파일 생성
- 전송 영역 생성
- 호스트 전송 노드 생성
- 베어메탈 서버 워크로드를 위한 애플리케이션 인터페이스 생성
- Network I/O Control 프로파일 구성
- NSX Edge 전송 노드 생성
- NSX Edge 클러스터 생성

전송 영역 정보

전송 영역은 전송 노드의 잠재적 도달 범위를 정의하는 컨테이너입니다. 전송 노드는 하이퍼바이저 호스트와 NSX-T Data Center 오버레이에 참여하는 NSX Edge입니다. 하이퍼바이저 호스트의 경우는 NSX-T Data Center 논리적 스위치를 통해 통신하는 VM을 호스팅하는 것을 의미합니다.

NSX Edge의 경우에는 논리적 라우터 업링크 및 다운링크가 존재하게 됨을 의미합니다.

전송 영역을 생성하는 경우 **표준** 또는 **고급 데이터 경로**일 수 있는 N-VDS 모드를 지정해야 합니다. 전송 노드를 전송 영역에 추가하는 경우 전송 영역과 연결된 N-VDS가 전송 노드에 설치됩니다. 각 전송 영역은 단일 N-VDS를 지원합니다. 고급 데이터 경로 N-VDS는 NFV(네트워크 기능 가상화) 워크로드를 지원하기 위한 성능 기능을 제공하고, VLAN과 오버레이 네트워크를 지원하며, 고급 데이터 경로 N-VDS를 지원하는 ESXi 호스트가 필요합니다.

전송 노드는 다음에 속할 수 있습니다.

- 여러 VLAN 전송 영역
- 표준 N-VDS가 포함된 최대 하나의 오버레이 전송 영역

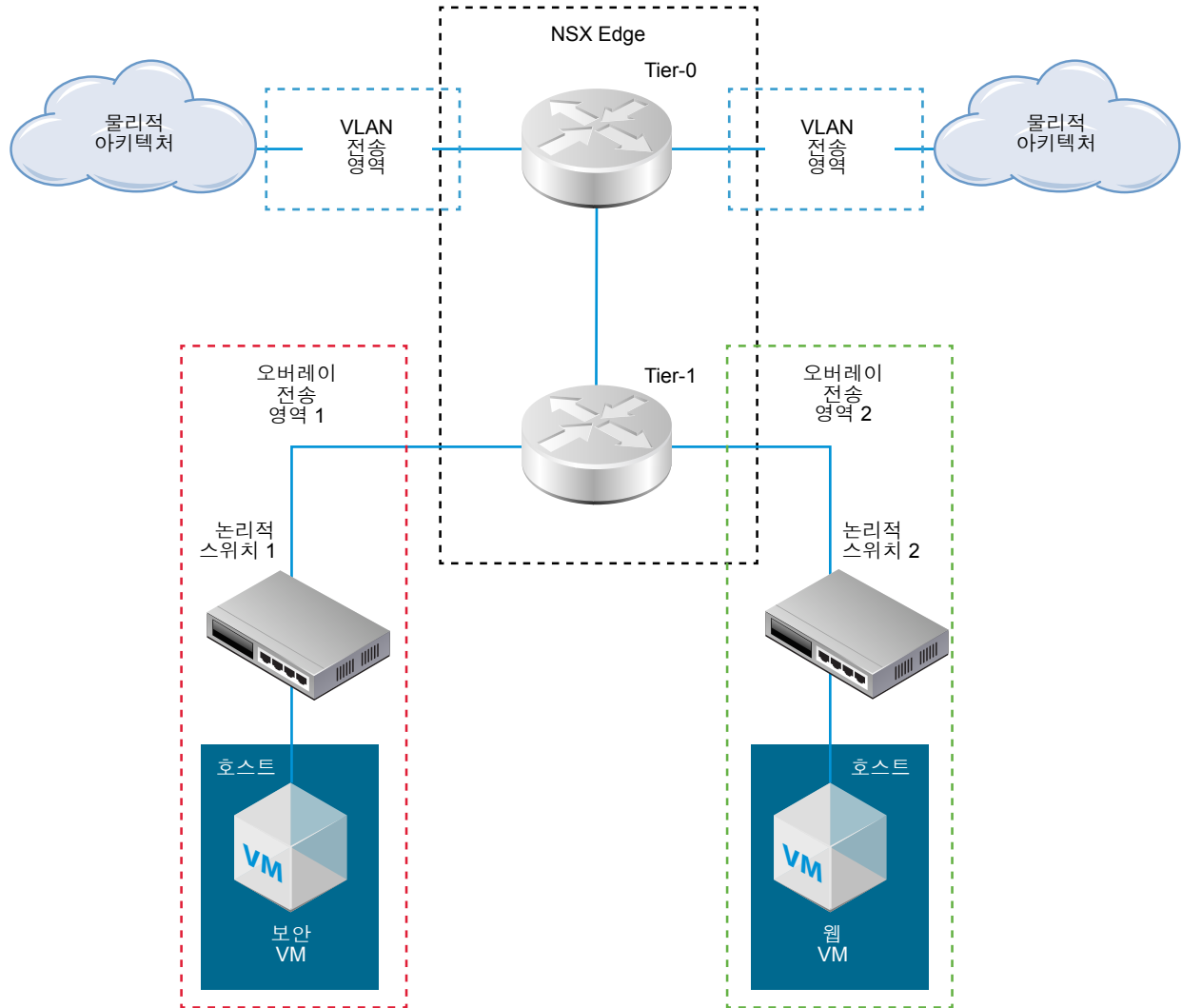
- 전송 노드가 ESXi 호스트에서 실행되고 있는 경우 고급 데이터 경로 N-VDS가 포함된 여러 오버레이 전송 영역

두 전송 노드가 동일한 전송 영역에 있으면 해당 전송 노드에 호스팅된 VM은 해당 전송 영역에 함께 있는 NSX-T Data Center 논리적 스위치에 연결될 수 있습니다. VM에 계층 2/계층 3 접근성이 있다면 이러한 연결을 통해 VM은 서로 통신할 수 있게 됩니다. VM이 다른 전송 영역에 있는 스위치에 연결되면 VM은 서로 통신할 수 없습니다. 전송 영역은 계층 2/계층 3 언더레이 접근성 요구를 대체하지 않으나 접근성을 제한합니다. 즉, 동일한 전송 영역에 속하는 것이 연결을 위한 전제 조건입니다. 이러한 전제 조건이 충족되면 연결이 가능해지지만 자동으로 이루어지지 않습니다. 실제 접근성을 얻으려면 계층 2 및 (다른 서브넷용) 계층 3 언더레이 네트워킹이 작동해야 합니다.

단일 전송 노드에 일반 VM과 높은 보안의 VM이 모두 포함되어 있다고 가정해보십시오. 네트워크 설계에서 일반 VM은 서로 연결되어야 하지만 높은 보안의 VM에 연결되어서는 안 됩니다. 이 목표를 달성하려면 secure-tz라는 한 전송 영역에 속하는 호스트에 보안 VM을 배치하면 됩니다. 일반 VM과 보안 VM은 동일한 전송 노드에 있을 수 없습니다. 그러면 일반 VM은 general-tz라는 다른 전송 영역에 위치하게 됩니다. 일반 VM은 마찬가지로 general-tz에 있는 NSX-T Data Center 논리적 스위치에 연결됩니다. 높은 보안의 VM은 secure-tz에 있는 NSX-T Data Center 논리적 스위치에 연결됩니다. 다른 전송 영역에 있는 VM은 같은 서브넷에 있더라도 서로 통신할 수 없습니다. VM과 논리적 스위치 간의 연결은 궁극적으로 VM 접근성을 제어합니다. 따라서 두 논리적 스위치가 별도의 전송 영역에 있으므로 "웹 VM" 및 "보안 VM"은 서로 연결될 수 없습니다.

예를 들어 다음 그림에서는 3개의 전송 영역, 즉 2개의 VLAN 전송 영역과 오버레이 전송 영역 2에 속하는 NSX Edge를 보여줍니다. 오버레이 전송 영역 1에는 호스트, NSX-T Data Center 논리적 스위치 및 보안 VM이 포함됩니다. NSX Edge는 오버레이 전송 영역 1에 속하지 않으므로 보안 VM은 물리적 아키텍처로 또는 물리적 아키텍처로부터 액세스할 수 없습니다. 반대로 오버레이 전송 영역 2의 웹 VM은 NSX Edge가 오버레이 전송 영역 2에 속하므로 물리적 아키텍처와 통신할 수 있습니다.

그림 8-1. NSX-T Data Center 전송 영역



고급 데이터 경로

고급 데이터 경로는 구성 시 뛰어난 네트워크 성능을 제공하는 네트워킹 스택 모드입니다. 고급 데이터 경로는 기본적으로 NFV 워크로드를 대상으로 하므로 이 모드에서 제공하는 성능 이점이 필요합니다.

ESXi 호스트에만 N-VDS 스위치를 고급 데이터 경로 모드로 구성할 수 있습니다.

고급 데이터 경로 모드에서는 다음을 구성할 수 있습니다.

- 오버레이 트래픽
- VLAN 트래픽

고급 데이터 경로를 구성하는 간략한 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 NIC 드라이버를 다운로드하고 설치합니다.

- 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.

- 5 호스트 전송 노드를 생성합니다. 고급 데이터 경로 N-VDS의 논리적 코어 수와 NUMA 노드 수를 구성합니다.

[호스트 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.

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 고유하게 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 **인벤토리 > 그룹 > IP 풀**을 선택하고 **추가**를 클릭합니다.
- 3 IP 풀의 이름, 설명(선택 사항) 및 네트워크 설정을 입력합니다.

네트워크 설정에는 다음이 포함됩니다.

- IP 주소 범위
- 게이트웨이
- CIDR 표기법으로 나타낸 네트워크 주소
- (선택 사항) 쉽표로 구분된 DNS 서버 목록

■ (선택 사항) DNS 접미사

예 :


새 IP 풀 추가

?

이름 *

설명

서브넷

+ 추가  삭제

<input checked="" type="checkbox"/> IP 범위 *	게이트웨이	CIDR *	DNS 서버	DNS 접미사
<input checked="" type="checkbox"/> 192.168.250.100 - 192.168.250.200	192.168.210.1	192.168.250.0/24		corp.local

또한 다음과 같이 GET <https://<nsx-mgr>/api/v1/pools/ip-pools> API 호출을 사용하여 IP 풀을 확인할 수 있습니다.

```
{
  "cursor": "0036e2d8c2e8-f6d7-498e-821b-b7e44d2650a9ip-pool-1",
  "sort_by": "displayName",
  "sort_ascending": true,
  "result_count": 1,
  "results": [
    {
      "id": "e2d8c2e8-f6d7-498e-821b-b7e44d2650a9",
      "display_name": "comp-tep",
      "resource_type": "IpPool",
      "subnets": [
        {
          "dns_nameservers": [
            "192.168.110.10"
          ],
          "allocation_ranges": [
            {
              "start": "192.168.250.100",
              "end": "192.168.250.200"
            }
          ],
          "gateway_ip": "192.168.250.1",
          "cidr": "192.168.250.0/24",
          "dns_suffix": "corp.local"
        }
      ]
    }
  ]
}
```

```

    }
  ],
  "_last_modified_user": "admin",
  "_last_modified_time": 1443649891178,
  "_create_time": 1443649891178,
  "_system_owned": false,
  "_create_user": "admin",
  "_revision": 0
}
]
}

```

다음에 수행할 작업

업링크 프로파일을 생성합니다. [업링크 프로파일 생성](#)의 내용을 참조하십시오.

업링크 프로파일 생성

업링크 프로파일은 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 프로파일을 사용하면 여러 호스트 또는 노드에서 네트워크 어댑터에 대해 동일한 기능을 일관되게 구성할 수 있습니다. 업링크 프로파일은 네트워크 어댑터에 적용하려는 속성 또는 기능의 컨테이너입니다. 각 네트워크 어댑터에 대해 개별 속성 또는 기능을 구성하는 대신, 업링크 프로파일에 기능을 지정한 다음 NSX-T Data Center 전송 노드를 생성할 때 이를 적용할 수 있습니다.

대기 업링크는 VM/장치 기반 NSX Edge에서 지원되지 않습니다. NSX Edge를 가상 장치로 설치할 때 기본 업링크 프로파일을 사용합니다. VM 기반 NSX Edge에 대해 생성된 각 업링크 프로파일의 경우 1개의 활성 업링크만 지정하면 되며 대기 업링크는 필요하지 않습니다.

참고 각 업링크에 대해 서로 다른 VLAN을 사용하여 별도의 N-VDS를 생성하는 경우 NSX Edge VM은 여러 업링크를 허용합니다. 각 업링크에는 별도의 VLAN 전송 영역이 필요합니다. 이는 여러 TOR 스위치로 연결되는 단일 NSX Edge 노드를 지원하기 위한 것입니다.

사전 요구 사항

- NSX Edge 네트워킹을 숙지하십시오. [NSX Edge 네트워킹 설정](#)의 내용을 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 **패브릭 > 프로파일 > 업링크 프로파일**을 선택하고 **추가**를 클릭합니다.
- 3 업링크 프로파일 세부 정보를 모두 입력합니다.

옵션	설명
이름	업링크 프로파일 이름을 입력합니다.
설명	(선택 사항) 업링크 프로파일 설명을 추가합니다.

옵션	설명
LAG	<p>(선택 사항) 전송 네트워크에 대해 LACP(Link Aggregation Control Protocol)를 사용하는 LAG(링크 집계 그룹).</p> <p>참고 LACP의 경우 KVM 호스트에서 여러 LAG가 지원되지 않습니다.</p> <p>섬표로 구분된 활성 업링크 이름 목록을 추가합니다.</p> <p>섬표로 구분된 대기 업링크 이름 목록을 추가합니다. 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 옵션입니다.</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 추가를 클릭하고 세부 정보를 입력합니다. 팀 구성 정책은 N-VDS가 이중화 및 트래픽 로드 밸런싱에 업링크를 사용하는 방법을 정의합니다. 팀 구성 정책을 구성하기 위한 2개의 팀 구성 정책 모드가 있습니다.</p> <ul style="list-style-type: none"> ■ 페일오버 순서: 활성 업링크가 대기 업링크의 선택적 목록과 함께 지정됩니다. 활성 업링크가 실패하는 경우 대기 목록의 다음 업링크가 활성 업링크를 대신합니다. 이 옵션을 사용하여 수행되는 실제 로드 밸런싱이 없습니다. ■ 로드 밸런싱된 소스: 활성 업링크의 목록이 지정되고 전송 노드의 각 인터페이스가 하나의 활성 업링크에 고정됩니다. 이 구성에서는 동시에 여러 활성 업링크를 사용할 수 있습니다. <p>참고 KVM 호스트에서는 페일오버 순서 팀 구성 정책만 지원됩니다. 로드 밸런싱 소스 팀 구성 정책은 지원되지 않습니다.</p> <p>(ESXi 호스트만 해당) 전송 영역에 대해 다음 정책을 정의할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 스위치에 구성된 모든 논리적 스위치에 대한 명명된 팀 구성 정책. ■ 전체 스위치에 대한 기본 팀 구성 정책. <p>명명된 팀 구성 정책: 명명된 팀 구성 정책이란 모든 논리적 스위치에 대해 특정 팀 구성 정책 모드와 업링크를 정의할 수 있음을 의미합니다. 이 정책 유형은 대역폭 요구 사항에 따라 업링크를 선택할 수 있는 유연성을 제공합니다.</p> <ul style="list-style-type: none"> ■ 명명된 팀 구성 정책을 정의하는 경우 N-VDS는 호스트의 연결된 전송 영역 및 논리적 스위치에서 지정한 명명된 팀 구성 정책을 사용합니다. ■ 명명된 팀 구성 정책을 정의하지 않는 경우 N-VDS는 기본 팀 구성 정책을 사용합니다.

4 전송 VLAN 값을 입력합니다.

5 MTU 값을 입력합니다.

기본값은 1600입니다.

UI 이외에도 GET /api/v1/host-switch-profiles API 호출을 사용하여 업링크 프로파일을 확인할 수 있습니다.

```
{
  "result_count": 2,
  "results": [
    {
      "resource_type": "UplinkHostSwitchProfile",
      "id": "16146a24-122b-4274-b5dd-98b635e4d52d",
      "display_name": "comp-uplink",
      "transport_vlan": 250,
      "teaming": {
        "active_list": [
          {
            "uplink_type": "PNIC",
            "uplink_name": "uplink-1"
          }
        ],
        "standby_list": [ {
          "uplink_name": "uplink-2",
          "uplink_type": "PNIC"
        } ],
        "policy": "FAILOVER_ORDER"
      },
      "mtu": 1600,
      "_last_modified_time": 1457984399526,
      "_create_time": 1457984399526,
      "_last_modified_user": "admin",
      "_system_owned": false,
      "_create_user": "admin",
      "_revision": 0
    },
    {
      "resource_type": "UplinkHostSwitchProfile",
      "id": "c9e35cec-e9d9-4c51-b52e-17a5c1bd9a38",
      "display_name": "vlan-uplink",
      "transport_vlan": 100,
      "teaming": {
        "active_list": [
          {
            "uplink_type": "PNIC",
            "uplink_name": "uplink-1"
          }
        ],
        "standby_list": [],
        "policy": "FAILOVER_ORDER"
      },
      "named_teamings": [
        {
          "active_list": [
            {
              "uplink_type": "PNIC",
              "uplink_name": "uplink-2"
            }
          ]
        }
      ]
    }
  ]
}
```



```

    ],
    "standby_list": [
    {
        "uplink_type": "PNIC",
        "uplink_name": "uplink-1"
    }
    ],
    "policy": "FAILOVER_ORDER",
    "name": "named teaming policy"
  }
]

  "mtu": 1600,
  "_last_modified_time": 1457984399574,
  "_create_time": 1457984399574,
  "_last_modified_user": "admin",
  "_system_owned": false,
  "_create_user": "admin",
  "_revision": 0
}
]
}

```

다음에 수행할 작업

전송 영역을 생성합니다. [전송 영역 생성](#)의 내용을 참조하십시오.

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 Edge에서 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 **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.
옵션은 **표준** 및 **고급 데이터 경로**입니다.
- 6 N-VDS 모드가 [표준]인 경우 트래픽 유형을 선택합니다.
옵션은 **오버레이** 및 **VLAN**입니다.
- 7 N-VDS 모드가 [고급 데이터 경로]인 경우 트래픽 유형을 선택합니다.
옵션은 **오버레이** 및 **VLAN**입니다.

참고 고급 데이터 경로 모드에서는 특정 NIC 구성만 지원됩니다. 지원되는 NIC를 구성하십시오.

- 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-ccbcfe50b416",
    "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. [호스트 전송 노드 생성](#)의 내용을 참조하십시오.

호스트 전송 노드 생성

전송 노드는 NSX-T Data Center 오버레이 또는 NSX-T Data Center VLAN 네트워킹에 참여하는 노드입니다.

KVM 호스트의 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 이미 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.

사전 요구 사항

- 호스트는 관리부에 연결되어야 하고 **패브릭 > 호스트** 페이지에서 MPA 연결이 [작동] 상태여야 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.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **패브릭 > 노드 > 전송 노드 > 추가**를 선택합니다.
- 3 전송 노드의 이름을 입력합니다.
- 4 드롭다운 메뉴에서 노드를 선택합니다.
- 5 이 전송 노드가 속한 전송 영역을 선택합니다.
- 6 **N-VDS** 탭을 클릭합니다.
- 7 KVM 노드의 경우 N-VDS 유형을 선택합니다.

옵션	설명
표준	NSX Manager가 N-VDS를 생성합니다. 이 옵션은 기본적으로 선택되어 있습니다.
사전 구성	N-VDS가 이미 구성되어 있습니다.

비 KVM 노드의 경우 N-VDS 유형은 항상 **표준** 또는 **고급 데이터 경로**입니다.

- 8 표준 N-VDS의 경우 다음 세부 정보를 제공합니다.

옵션	설명
N-VDS 이름	이 노드가 속하는 전송 영역의 N-VDS 이름과 반드시 동일해야 합니다.
NIOC 프로파일	드롭다운 메뉴에서 NIOC 프로파일을 선택합니다.

옵션	설명
업링크 프로파일	드롭다운 메뉴에서 업링크 프로파일을 선택합니다.
IP 할당	DHCP 사용, IP 풀 사용 또는 정적 IP 목록 사용 을 선택합니다. 정적 IP 목록 사용 을 선택하면 씬표로 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.
물리적 NIC	물리적 NIC가 아직 사용되고 있지 않은지 확인합니다(예: 표준 vSwitch 또는 vSphere Distributed Switch에서). 사용되고 있는 경우 전송 노드 상태가 일부 성공 으로 유지되고 패브릭 노드 LCP 연결이 설정되지 않습니다. 베어메탈 서버의 경우 업링크-1 포트로 구성할 수 있는 물리적 NIC를 선택합니다. 업링크-1 포트는 업링크 프로파일에 정의됩니다. 베어메탈 서버에 네트워크 어댑터가 하나만 있는 경우에는 해당 물리적 NIC를 선택하여 업링크-1 포트가 관리 및 애플리케이션 인터페이스 둘 다에 할당되도록 합니다.

9 고급 데이터 경로 N-VDS의 경우 다음 세부 정보를 제공합니다.

옵션	설명
N-VDS 이름	이 노드가 속하는 전송 영역의 N-VDS 이름과 반드시 동일해야 합니다.
IP 할당	DHCP 사용, IP 풀 사용 또는 정적 IP 목록 사용 을 선택합니다. 정적 IP 목록 사용 을 선택하면 씬표로 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.
물리적 NIC	고급 데이터 경로를 지원하는 물리적 NIC를 선택합니다. 물리적 NIC가 아직 사용되고 있지 않은지 확인합니다(예: 표준 vSwitch 또는 vSphere Distributed Switch에서). 사용되고 있는 경우 전송 노드 상태가 일부 성공 으로 유지되고 패브릭 노드 LCP 연결이 설정되지 않습니다.
업링크	드롭다운 메뉴에서 업링크 프로파일을 선택합니다.
CPU 구성	[NUMA 노드 인덱스] 드롭다운 메뉴에서 N-VDS 스위치에 할당하려는 NUMA 노드를 선택합니다. 노드에 있는 첫 번째 NUMA 노드는 값 0으로 표시됩니다. esxcli hardware memory get 명령을 실행하여 호스트에서 NUMA 노드의 수를 확인할 수 있습니다. 참고 N-VDS 스위치에 대해 선호도를 갖는 NUMA 노드의 수를 변경하려는 경우 NUMA 노드 인덱스 값을 업데이트할 수 있습니다. [NUMA 노드별 LCore 수] 드롭다운 메뉴에서 고급 데이터 경로에서 사용되어야 하는 논리적 코어 수를 선택합니다. esxcli network ens maxLcores get 명령을 실행하여 NUMA 노드에서 생성할 수 있는 최대 논리적 코어 수를 확인할 수 있습니다. 참고 사용 가능한 NUMA 노드와 논리적 코어를 모두 사용한 경우 전송 노드에 추가된 새 스위치를 ENS 트래픽에 사용하도록 설정할 수 없습니다.

10 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.

호스트를 전송 노드로 추가하면 NSX Controller에 대한 호스트 연결이 [실행] 상태로 변경됩니다.

11 전송 노드 페이지에서 연결 상태를 확인합니다.

12 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 -
```

13 (선택 사항) 다음과 같이 GET `https://<nsx-mgr>/api/v1/transport-nodes/<node-id>` API 호출을 사용하여 전송 노드를 확인합니다.

```
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "95c8ce77-f895-43de-adc4-03a3ae2565e2",
  "display_name": "node-comp-01b",
  "tags": [],
  "transport_zone_endpoints": [
    {
      "transport_zone_id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ]
    }
  ],
  "host_switches": [
    {
      "host_switch_profile_ids": [
        {
          "value": "8abdb6c0-db83-4e69-8b99-6cd85bfcc61d",
          "key": "UplinkHostSwitchProfile"
        }
      ],
    }
  ]
}
```

```

    "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
    "key": "LldpHostSwitchProfile"
  }
],
"host_switch_name": "overlay-hostswitch",
"pnics": [
  {
    "device_name": "vmnic1",
    "uplink_name": "uplink-1"
  }
],
"static_ip_pool_id": "c78ac522-2a50-43fe-816a-c459a210127e"
}
],
"node_id": "c551290a-f682-11e5-ae84-9f8726e1de65",
"_create_time": 1460051753373,
"_last_modified_user": "admin",
"_system_owned": false,
"_last_modified_time": 1460051753373,
"_create_user": "admin",
"_revision": 0
}

```

14 새로 생성된 전송 노드를 전송 영역에 추가합니다.

- a 전송 노드를 선택합니다.
- b **작업 > 전송 영역에 추가**를 선택합니다.
- c 드롭다운 메뉴에서 전송 영역을 선택합니다.

다른 모든 필드는 채워져 있습니다.

참고 표준 N-VDS의 경우 전송 노드를 생성한 후 IP 할당과 같은 구성을 터널 끝점으로 변경하려면 호스트의 CLI가 아닌 NSX Manager GUI를 통해 변경해야 합니다.

다음에 수행할 작업

vSphere 표준 스위치에서 NSX-T 가상 Distributed Switch로 네트워크 인터페이스를 마이그레이션합니다. [N-VDS 스위치로 VMkernel 마이그레이션](#)의 내용을 참조하십시오.

자동 전송 노드 생성 구성

vCenter Server 클러스터가 있는 경우 단일 또는 다중 클러스터의 모든 NSX-T Data Center 호스트에서 전송 노드를 수동으로 구성하지 않고 설치 및 생성을 자동화할 수 있습니다.

참고 자동화된 NSX-T Data Center 전송 노드 생성은 vCenter Server 6.5 업데이트 1, 6.5 업데이트 2 및 6.7에서만 지원됩니다.

전송 노드가 이미 구성된 경우 해당 노드에는 자동화된 전송 노드 생성을 적용할 수 없습니다.

사전 요구 사항

- 호스트는 vCenter Server 클러스터에 속해야 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.
- vCenter Server에는 하나 이상의 클러스터가 있어야 합니다.
- 계산 관리자를 구성해야 합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **패브릭 > 노드 > 호스트**를 선택합니다.
- 3 [관리자] 드롭다운 메뉴에서 기존 계산 관리자를 선택합니다.
- 4 클러스터를 선택하고 **클러스터 구성**을 클릭합니다.
- 5 클러스터 구성 세부 사항을 완료합니다.

옵션	설명
NSX 자동 설치	vCenter Server 클러스터의 모든 호스트에서 NSX-T Data Center 설치를 사용하려면 이 버튼을 전환합니다.
전송 노드 자동 생성	vCenter Server 클러스터의 모든 호스트에서 전송 노드 생성을 사용하려면 이 버튼을 전환합니다. 이는 필수 설정입니다. 참고 사전 구성된 전송 노드가 클러스터에 있거나 다른 클러스터로 이동한 경우 NSX-T Data Center가 클러스터의 전송 노드 템플릿에 정의된 구성을 사용하여 사전 구성된 전송 노드를 업데이트하지 않습니다. 모든 노드에 동일한 구성이 포함되도록 하려면 사전 구성된 전송 노드를 삭제하고 해당 호스트를 클러스터에 추가합니다.
전송 영역	드롭다운 메뉴에서 기존 전송 노드를 선택합니다.
업링크 프로파일	드롭다운 메뉴에서 기존 업링크 프로파일을 선택하거나 사용자 지정 업링크 프로파일을 생성합니다. 참고 클러스터의 호스트는 업링크 프로파일이 동일해야 합니다. 기본 업링크 프로파일을 사용할 수도 있습니다.

옵션	설명
IP 할당	드롭다운 메뉴에서 DHCP 사용 또는 IP 풀 사용 을 선택합니다. IP 풀 사용 을 선택하는 경우 드롭다운 메뉴에서 네트워크의 기존 IP 풀을 할당해야 합니다.
물리적 NIC	물리적 NIC가 아직 사용되고 있지 않은지 확인합니다(예: 표준 vSwitch 또는 vSphere Distributed Switch에서). 사용되고 있는 경우 전송 노드 상태가 부분적으로만 성공이며, 패브릭 노드 LCP 연결이 설정되지 않습니다. 기본 업링크를 사용하거나 드롭다운 메뉴에서 기존 업링크를 할당할 수 있습니다. PNIC 추가 를 클릭하여 구성에서 NIC 수를 늘립니다.

클러스터의 각 호스트에서 NSX-T Data Center 설치 및 전송 노드 생성은 병렬로 시작됩니다. 전체 프로세스는 클러스터의 호스트 수에 따라 다릅니다.

새 호스트가 vCenter Server 클러스터에 추가되면 NSX-T Data Center 설치 및 전송 노드 생성은 자동으로 발생합니다.

6 (선택 사항) ESXi 연결 상태를 확인합니다.

```
# esxcli network ip connection list | grep 1234
tcp 0 0 192.168.210.53:20514 192.168.110.34:1234 ESTABLISHED 1000144459 newreno netcpa
```

7 (선택 사항) 클러스터의 호스트에서 NSX-T Data Center 설치 및 전송 노드를 제거합니다.

- 클러스터를 선택하고 **클러스터 구성**을 클릭합니다.
- [NSX 자동 설치] 버튼을 전환하여 해당 옵션을 사용하지 않도록 설정합니다.
- 하나 이상의 호스트를 선택하고 **NSX 제거**를 클릭합니다.

제거에는 최대 3분이 소요됩니다.

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. [호스트 전송 노드 생성](#)의 내용을 참조하십시오.

절차

- 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 패브릭 > 프로파일 > 업링크 프로파일**을 선택하고 **추가**를 클릭합니다.
- 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** 항목을 선택합니다.

6 **액티브 업링크** 필드에 4단계에서 추가한 LAG의 이름을 입력합니다. 이 예에서 해당 이름은 **lag1**입니다.

7 대화 상자의 맨 아래에서 **추가**를 클릭합니다.

8 **전송 VLAN** 및 **MTU** 값을 입력합니다.

9 창의 맨 아래에서 **추가**를 클릭합니다.

10 **패브릭 > 노드 > 전송 노드 > 추가**를 선택합니다.

11 **일반** 탭에 정보를 입력합니다.

12 **N-VDS** 탭에서 3단계에서 생성한 **uplink-profile1**이라는 업링크 프로파일을 선택합니다.

13 **물리적 NIC** 필드에 물리적 NIC의 드롭다운 목록과 업링크 프로파일을 만들 때 지정한 업링크의 드롭다운 목록이 표시됩니다. 특히, 4단계에서 생성한 LAG인 **lag1**에 해당하는 업링크 **lag1-0**과 **lag1-1**을 볼 수 있습니다. **lag1-0**에 대한 물리적 NIC 및 **lag1-1**에 대한 물리적 NIC를 선택합니다.

14 다른 필드에 대한 정보를 입력합니다.

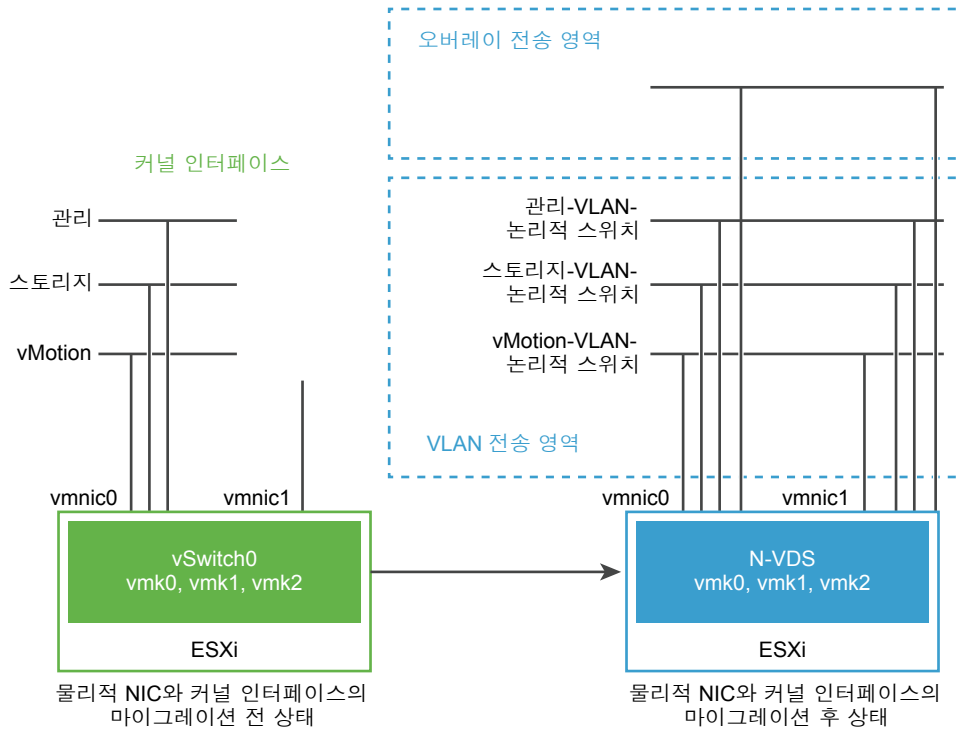
N-VDS 스위치로 VMkernel 마이그레이션

전송 노드를 생성할 때 물리적 NIC와 커널 인터페이스를 vSphere 표준 스위치(VSS) 또는 VDS에서 NSX-T Data Center 가상 Distributed Switch(N-VDS)로 마이그레이션해야 할 수 있습니다. 마이그레이션 후에는 N-VDS에서 VLAN 네트워크의 트래픽을 처리합니다.

물리적 NIC와 VMkernel 인터페이스는 처음에 vSphere ESXi 호스트의 VSS 또는 VDS에 연결됩니다. 이러한 호스트에 커널 인터페이스가 정의되어 관리 인터페이스, 스토리지 및 기타 인터페이스에 대한 연결을 제공합니다. 마이그레이션한 후 VMkernel 인터페이스 및 이와 연결된 물리적 NIC가 N-VDS에 연결되고 VLAN 및 오버레이 전송 영역에서 트래픽을 처리합니다.

다음 그림에서 호스트에 물리적 NIC가 두 개만 있는 경우 이중화를 위해 두 NIC 모두를 N-VDS에 할당할 수 있습니다.

그림 8-2. 네트워크 인터페이스를 N-VDS로 마이그레이션하기 전과 후



마이그레이션을 수행하기 전에 vSphere ESXi 호스트에는 두 개의 물리적 포트(vmnic0 및 vmnic1)에서 파생된 두 개의 업링크가 있습니다. 여기서 vmnic0은 활성 상태로 구성되고 VSS 또는 VDS에 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 마이그레이션합니다. 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.

NSX-T Data Center Manager UI를 사용하여 VMkernel 인터페이스를 N-VDS 스위치로 마이그레이션

NSX-T Data Center Manager UI를 사용하면 관리 인터페이스를 포함한 모든 커널 인터페이스를 VSS 또는 VDS에서 N-VDS 스위치로 마이그레이션 할 수 있습니다.

이 예에서는 vmnic0과 vmnic1이라는 두 개의 물리적 어댑터가 있는 vSphere ESXi 호스트를 고려합니다. 호스트의 기본 VSS 또는 VDS 스위치는 vmnic0에 매핑된 단일 업링크로 구성됩니다. VMkernel 인터페이스 vmk0도 노드에서 관리 트래픽을 실행하도록 VSS 또는 VDS에 구성됩니다. 목표는 vmnic0 및 vmk0을 N-VDS 스위치로 마이그레이션하는 것입니다.

호스트 준비의 일환으로 VLAN 및 오버레이 전송 영역이 생성되어 관리 및 VM 트래픽이 각각 실행됩니다. N-VDS 스위치도 생성되어 vmnic1에 매핑된 업링크를 사용하여 구성됩니다. 마이그레이션 후에 NSX-T Data Center는 vmnic0과 vmk0 모두를 VSS 또는 VDS 스위치에서 노드의 N-VDS 스위치로 마이그레이션합니다.

사전 요구 사항

- 물리적 네트워크 인프라가 vmnic1 및 vmnic0에 동일한 LAN 연결을 제공하는지 확인합니다.
- 사용하지 않는 물리적 NIC인 vmnic1이 vmnic0과 계층 2 연결이 있는지 확인합니다.
- 이 마이그레이션에 포함된 모든 VMkernel 인터페이스가 동일한 네트워크에 속하는지 확인합니다. VMkernel 인터페이스를 다른 네트워크에 연결된 업링크로 마이그레이션하면 호스트에 연결할 수 없거나 호스트가 작동하지 않을 수 있습니다.

절차

- 1 NSX Manager UI에서 **패브릭** -> **프로파일** -> **업링크 프로파일**로 이동합니다.
- 2 vmnic0을 활성 업링크로 사용하고 vmnic1을 패시브 업링크로 사용하여 업링크 프로파일을 생성합니다.
- 3 **패브릭** -> **전송 영역** -> **추가**로 이동합니다.
- 4 VM 트래픽과 관리 트래픽을 각각 처리할 오버레이 및 VLAN 전송 영역을 생성합니다.

참고 VLAN 전송 영역 및 오버레이 전송 영역에 사용되는 N-VDS 이름은 동일해야 합니다.

- 5 **패브릭** -> **노드** -> **전송 노드**로 이동합니다.
- 6 전송 노드에 두 전송 영역을 모두 추가합니다.
- 7 N-VDS 탭에서 N-VDS에 사용될 물리적인 어댑터, 업링크를 정의하여 N-VDS를 추가합니다.
전송 노드는 단일 업링크를 통해 전송 영역에 연결됩니다.
- 8 마이그레이션 후에 vmk0과 vmnic0이 VLAN 전송 영역에 연결될 수 있도록, 적절한 VLAN 전송 영역에 대한 논리적 스위치를 생성합니다.
- 9 전송 노드를 선택하고 **작업** -> **ESX VMkernel 및 물리적 어댑터 마이그레이션**을 클릭합니다.
- 10 **논리적 스위치로 마이그레이션**을 선택합니다.
- 11 N-VDS 스위치를 선택합니다.
- 12 VMkernel 어댑터 및 연결된 논리적 스위치를 추가합니다.
- 13 VMkernel 인터페이스에 해당하는 물리적 어댑터를 추가합니다. 하나 이상의 물리적 어댑터가 VSS 또는 VDS 스위치에 남아 있도록 합니다.
- 14 **저장**을 클릭합니다.
- 15 **계속**을 클릭하여 마이그레이션을 시작합니다.
- 16 NSX Manager에서 vmnic0 및 vmk0에 대한 연결을 테스트합니다.
- 17 또는 vCenter Server에서 VMkernel 어댑터가 NSX-T Data Center 스위치와 연결되어 있는지 확인합니다.

VMkernel 인터페이스와 해당하는 물리적 어댑터가 N-VDS로 마이그레이션됩니다.

다음에 수행할 작업

VMkernel 마이그레이션을 VSS 또는 VDS 스위치로 되돌릴 수 있습니다.

NSX-T Data Center Manager UI를 사용하여 VMkernel 인터페이스 마이그레이션을 VSS 또는 VDS 스위치로 되돌리기

VMkernel 인터페이스의 마이그레이션을 VSS 또는 VDS 스위치로 되돌리려면 ESXi 호스트에 포트 그룹이 있는지 확인합니다.

VMkernel 인터페이스를 N-VDS 스위치에서 VSS 또는 VDS 스위치로 마이그레이션하려면 NSX-T Data Center에 포트 그룹이 필요합니다. 포트 그룹은 이러한 인터페이스를 VSS 또는 VDS 스위치로 마이그레이션하기 위한 네트워크 요청을 수락합니다. 이 마이그레이션에 참여하는 포트 멤버는 대역폭 및 정책 구성에 따라 결정됩니다.

VMkernel을 VSS 또는 VDS 스위치로 다시 마이그레이션을 시작하기 전에, VMkernel 인터페이스가 작동하고 N-VDS 스위치에 연결되어 있는지 확인합니다.

사전 요구 사항

- 포트 그룹이 vSphere ESXi 서버에 존재합니다.

절차

- 1 NSX Manager UI에서 **패브릭** -> **노드** -> **전송 노드**로 이동합니다.
- 2 전송 노드를 선택하고 **작업** -> **ESX VMkernel 및 물리적 어댑터 마이그레이션**을 클릭합니다.
- 3 **포트 그룹으로 마이그레이션**을 선택합니다.
- 4 N-VDS 스위치를 선택합니다.
- 5 VMkernel 어댑터 및 연결된 논리적 스위치를 추가합니다.
- 6 VMkernel 인터페이스에 해당하는 물리적 어댑터를 추가합니다. 하나 이상의 물리적 어댑터가 VSS 또는 VDS 스위치에 연결된 상태로 유지되도록 합니다.
- 7 **저장**을 클릭합니다.
- 8 **계속**을 클릭하여 마이그레이션을 시작합니다.
- 9 NSX Manager에서 vmnic0 및 vmk0에 대한 연결을 테스트합니다.
- 10 또는 vCenter Server에서 VMkernel 어댑터가 VSS 또는 VDS 스위치와 연결되어 있는지 확인합니다.

VMkernel 인터페이스와 해당하는 물리적 어댑터가 N-VDS로 마이그레이션됩니다.

다음에 수행할 작업

API를 사용하여 VMkernel 인터페이스를 마이그레이션하는 것이 좋습니다. [API를 사용하여 커널 인터페이스를 N-VDS로 마이그레이션](#)의 내용을 참조하십시오.

API를 사용하여 커널 인터페이스를 N-VDS로 마이그레이션

NSX-T Data Center API를 사용하는 경우 관리 인터페이스를 마이그레이션하기 전에 모든 커널 인터페이스를 먼저 마이그레이션해야 합니다.

각각의 물리적 NIC에 연결된 업링크가 두 개 있는 호스트를 고려해 보겠습니다. 이 절차에서는 스토리지 커널 인터페이스 vmk1을 N-VDS로 마이그레이션하는 것부터 시작할 수 있습니다. 이 커널 인터페이스가 N-VDS로 성공적으로 마이그레이션되면 관리 커널 인터페이스를 마이그레이션할 수 있습니다.

NSX-T Data Center API 가이드 항목을 참조하십시오.

사전 요구 사항

- 물리적 네트워크 인프라가 vmnic1 및 vmnic0에 동일한 LAN 연결을 제공하는지 확인합니다.
- 사용하지 않는 물리적 NIC인 vmnic1이 vmnic0과 계층 2 연결이 있는지 확인합니다.
- 이 마이그레이션에 포함된 모든 VMkernel 인터페이스가 동일한 네트워크에 속하는지 확인합니다. VMkernel 인터페이스를 다른 네트워크에 연결된 업링크로 마이그레이션하면 호스트에 연결할 수 없거나 호스트가 작동하지 않을 수 있습니다.

절차

- 1 오버레이 전송 영역에서 사용하는 N-VDS의 host_switch_name으로 VLAN 전송 영역을 생성합니다.
- 2 VSS 또는 VDS에서 vmk1이 사용하는 VLAN ID와 일치하는 VLAN ID로 VLAN 전송 영역에 VLAN 지원 논리적 스위치를 생성합니다.
- 3 VLAN 전송 영역에 vSphere ESXi 전송 노드를 추가합니다.
- 4 vSphere ESXi 전송 노드 구성을 검색합니다.

```
GET /api/v1/transport-nodes/<transportnode-id>
```

여기에서 <transportnode-id>는 전송 노드의 UUID입니다.

- 5 vmk1을 N-VDS로 마이그레이션합니다.

```
PUT https://<NSXmgr>/api/v1/transport-nodes/<transportnode-id> ?
if_id=<vmk>&esx_mgmt_if_migration_dest=<network>
```

여기에서 <transportnode-id>는 전송 노드의 UUID입니다. <vmk>는 VMkernel 인터페이스 vmk1의 이름입니다. <network>는 대상 논리적 스위치의 UUID입니다.

- 6 마이그레이션이 완료되었는지 확인합니다.

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

마이그레이션 상태가 성공으로 표시될 때까지 기다립니다. vCenter Server에서 VMkernel 인터페이스의 마이그레이션 상태를 확인할 수도 있습니다.

VMkernel 인터페이스가 VSS 또는 VDS에서 N-VDS 스위치로 마이그레이션됩니다.

다음에 수행할 작업

나머지 VMkernel 인터페이스 및 VSS 또는 VDS의 관리 커널 인터페이스를 N-VDS로 마이그레이션할 수 있습니다.

API를 사용하여 VSS 또는 VDS에서 N-VDS로 관리 커널 인터페이스 마이그레이션

다른 모든 커널 인터페이스를 마이그레이션한 후에, 관리 커널 인터페이스를 마이그레이션합니다. 관리 커널 인터페이스를 마이그레이션하는 경우 vmnic0 및 vmk0을 VSS 또는 VDS에서 N-VDS로 이동합니다.

그러면 물리적 업링크 vmnic0 및 vmk0을 N-VDS로 한 번에 같이 마이그레이션할 수 있습니다. vmnic0이 현재 업링크 중 하나로 구성되도록 전송 노드 구성을 수정합니다.

참고 업링크 vmnic0 및 커널 인터페이스 vmk0을 별도로 마이그레이션하려면 먼저 vmk0을 마이그레이션한 다음 vmnic0을 마이그레이션합니다. vmnic0을 먼저 마이그레이션하면 vmk0이 백업 업링크 없이 VSS 또는 VDS에 남게 되어 호스트에 대한 연결이 끊어집니다.

사전 요구 사항

- 이미 마이그레이션된 vmknics에 대한 연결을 확인합니다. [API를 사용하여 커널 인터페이스를 N-VDS로 마이그레이션](#)을 참조하십시오.
- vmk0과 vmk1이 서로 다른 VLAN을 사용하는 경우 두 VLAN을 모두 지원하려면 물리적 NIC vmnic0 및 vmnic1에 연결된 물리적 스위치에 트렁크 VLAN을 구성해야 합니다.
- 외부 디바이스가 스토리지 VLAN 지원 논리적 스위치의 vmk1 인터페이스와 vMotion VLAN 지원 논리적 스위치의 vmk2 인터페이스에 연결할 수 있는지 확인합니다.

절차

- 1 (선택 사항) VSS 또는 VDS에 두 번째 관리 커널 인터페이스를 생성하고 새로 생성한 이 인터페이스를 N-VDS로 마이그레이션합니다.
- 2 (선택 사항) 외부 장치에서 테스트 관리 인터페이스에 대한 연결을 확인합니다.
- 3 vmk0(관리 인터페이스)이 vmk1(스토리지 인터페이스)과 다른 VLAN을 사용하는 경우 VSS 또는 VDS에서 vmk0이 사용하는 VLAN ID와 일치하는 VLAN ID로 VLAN 전송 영역에 VLAN 지원 논리적 스위치를 생성합니다.
- 4 vSphere ESXi 전송 노드 구성을 검색합니다.

```
GET /api/v1/transport-nodes/<transportnode-id>
```

여기에서 <transportnode-id>는 전송 노드의 UUID입니다.

- 5 구성의 `host_switch_spec:host_switches` 요소에서 물리적 NIC 테이블에 `vmnic0`을 추가하고 이것을 전용 업링크, 업링크-2에 할당합니다.

참고 VM 커널 인터페이스를 마이그레이션하는 동안 `vmnic1`을 업링크-1에 할당했습니다. 마이그레이션을 성공적으로 수행하고 마이그레이션한 후 호스트에 연결할 수 있으려면 `vmnic0`, 관리 인터페이스를 전용 업링크에 할당해야 합니다.

```
"pnics": [
  {
    "device_name": "vmnic0",
    "uplink_name": "uplink-2"
  },
  {
    "device_name": "vmnic1",
    "uplink_name": "uplink-1"
  }
],
```

- 6 업데이트된 구성을 사용하여 관리 커널 인터페이스인 `vmk0`을 N-VDS로 마이그레이션합니다.

```
PUT /api/v1/transport-nodes/<transportnode-id>?if_id=<vmk>&esx_mgmt_if_migration_dest=<network>
```

여기에서 `<transportnode-id>`는 전송 노드의 UUID입니다. `<vmk>`는 VMkernel 관리 인터페이스 `vmk0`의 이름입니다. `<network>`는 대상 논리적 스위치의 UUID입니다.

- 7 마이그레이션이 완료되었는지 확인합니다.

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

마이그레이션 상태가 성공으로 표시될 때까지 기다립니다. vCenter Server에서 커널 어댑터가 새 논리적 스위치 이름을 표시하도록 구성되었는지 확인할 수 있습니다.

다음에 수행할 작업

N-VDS에서 VSS 또는 VDS 스위치로 커널 인터페이스 및 관리 인터페이스의 마이그레이션을 되돌리도록 선택할 수 있습니다.

API를 사용하여 VMkernel 인터페이스 마이그레이션을 N-VDS 스위치에서 VSS 또는 VDS 스위치로 되돌리기

VMkernel 인터페이스를 되돌리는 경우 관리 커널 인터페이스의 마이그레이션부터 시작해야 합니다. 그런 다음, 다른 커널 인터페이스를 N-VDS에서 VSS 또는 VDS 스위치로 마이그레이션합니다.

절차

- 1 전송 노드 상태가 성공적인지 확인합니다.

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```


- 2 vSphere ESXi 전송 노드 구성을 검색하여 "host_switch_spec":"host_switches"요소 내에 정의된 물리적 NIC를 찾습니다.

GET /api/v1/transport-nodes/<transportnode-id>

```
"pnics": [
  { "device_name": "vmnic0",
    "uplink_name": "uplink-2"
  },
  { "device_name": "vmnic1",
    "uplink_name": "uplink-1"
  }
],
```

- 3 전송 노드 구성의 "host_switch_spec":"host_switches" 요소에서 vmnic0을 제거하고 마이그레이션을 위한 관리 인터페이스를 준비합니다.

```
"pnics": [
  { "device_name": "vmnic1",
    "uplink_name": "uplink-1"
  }
],
```

- 4 수정된 구성을 사용하여 관리 인터페이스, vmnic0 및 vmk0을 N-VDS에서 VSS 또는 VDS로 마이그레이션합니다.

PUT api/v1/transport-nodes/<transportnode-id>?

if_id=vmk0&esx_mgmt_if_migration_dest=<vmk0_port_group_name>

여기서 <vmk0_port_group>은 논리적 스위치로 마이그레이션하기 전에 vmk0에 할당된 포트 그룹 이름입니다.

- 5 마이그레이션 상태를 확인합니다.

GET /api/v1/transport-nodes/<transportnode-id>/state

상태가 "성공"으로 표시될 때까지 기다립니다.

- 6 vSphere ESXi 전송 노드 구성을 검색합니다.

GET /api/v1/transport-nodes/<transportnode-id>

- 7 이전 전송 노드 구성을 사용하여 N-VDS에서 VSS 또는 VDS로 vmk1을 마이그레이션합니다.

PUT api/v1/transport-nodes/<transportnode-id>?

if_id=vmk1&esx_mgmt_if_migration_dest=<vmk1_port_group>

여기서 <vmk1_port_group>은 논리적 스위치로 마이그레이션하기 전에 vmk1에 할당된 포트 그룹 이름입니다.

참고 VSS 또는 VDS에 연결된 물리적 NIC가 없기 때문에 하나 이상의 물리적 NIC를 사용하여 vmk0 또는 vmk1을 VSS 또는 VDS로 마이그레이션해야 합니다.

8 전송 노드 상태가 성공적인지 확인합니다.

```
GET /api/v1/transport-nodes/<transportnode-id>/state.
```

9 문제를 방지하기 위해 사후 마이그레이션 확인을 수행합니다.

- a VSS 또는 VDS에 연결된 업링크 인터페이스가 있기 전에 관리 커널 인터페이스, vmk0을 마이그레이션하면 안 됩니다.
- b vmk0이 vmnic0에서 IP 주소를 수신하는지 확인합니다. 그렇지 않으면 IP가 변경될 수 있으며 VC와 같은 다른 구성 요소에서 이전 IP를 통해 호스트에 대한 연결이 끊어질 수 있습니다.

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 그렇게 설계된 것입니다.

```
# 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 상태 정보에 대해서는 API를 확인하십시오.

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": "over lay-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"
}

```

계산 관리자 추가

예를 들어 vCenter Server와 같은 계산 관리자는 호스트 및 VM과 같은 리소스를 관리하는 애플리케이션입니다. NSX-T Data Center는 계산 관리자를 폴링하여 호스트 또는 VM의 추가 또는 제거 같은 변경 사항을 확인하고 그에 따라 인벤토리를 업데이트합니다. NSX-T는 계산 관리자 없이도 독립 실행형 호스트 및 VM과 같은 인벤토리 정보를 가져오기 때문에 계산 관리자를 추가하는 것은 선택 사항입니다.

이 릴리스에서 이 기능은 다음을 지원합니다.

- vCenter Server 버전 6.5 업데이트 1, 6.5 업데이트 2 및 6.7
- vCenter Server와의 IPv6 및 IPv4 통신
- 최대 5개의 계산 관리자

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 탐색 패널에서 **패브릭 > 계산 관리자**를 선택합니다.
- 3 **추가**를 클릭합니다.
- 4 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.

옵션	설명
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.

- 5 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.

계산 관리자 패널에 계산 관리자 목록이 표시됩니다. 관리자 이름을 클릭하여 관리자에 대한 세부 정보를 보거나 편집할 수 있고, 관리자에게 적용되는 태그를 관리할 수도 있습니다.

베어메탈 서버 워크로드를 위한 애플리케이션 인터페이스 생성

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

절차

- 1 필수타사 패키지를 설치합니다.

[KVM 호스트 또는 베어메탈 서버에 타사 패키지 설치](#)의 내용을 참조하십시오.

- 2 TCP 및 UDP 포트를 구성합니다.

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

- 3 베어메탈 서버를 NSX-T Data Center 패브릭에 추가합니다.

[NSX-T Data Center 패브릭에 하이퍼바이저 호스트 또는 베어메탈 서버 추가](#)의 내용을 참조하십시오.

- 4 KVM 호스트 전송 노드를 생성합니다.

[호스트 전송 노드 생성](#)의 내용을 참조하십시오.

- 5 Ansible 플레이북을 사용하여 애플리케이션 인터페이스를 생성합니다.

<https://github.com/vmware/bare-metal-server-integration-with-nsxt>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 Center를 위한 Network I/O Control 버전 3은 vSphere Fault Tolerance 등과 같은 가상 시스템 및 인프라 서비스와 관련된 시스템 트래픽의 리소스 관리를 지원합니다. 시스템 트래픽은 vSphere ESXi 호스트와 전적으로 연결되어 있습니다.

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. 승인 제어에서는 가상 시스템 트래픽에 대한 대역폭 예약도 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 스위치에 연결된 호스트의 각 물리적 어댑터로 Distributed Switch의 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-VDS 스위치에서 시스템 트래픽에 대한 Network I/O Control 및 대역폭 할당 구성

NSX-T 호스트에서 실행 중인 시스템 트래픽에 대한 최소 대역폭을 보장하려면 NSX-T Distributed Switch에서 네트워크 리소스 관리를 사용하도록 설정 및 구성합니다.

절차

- 1 NSX Manager Manager(<https://<nsx-manager-IP-address>>)에 로그인합니다.
 - 2 **네트워킹 > 프로파일**로 이동합니다.
 - 3 **NIOC 프로파일**을 선택합니다.
 - 4 **+** **추가**를 클릭합니다.
 - 5 [새 NIOC 프로파일] 화면에서 필수 세부 정보를 입력합니다.
 - a NIOC 프로파일의 이름을 입력합니다.
 - b 상태를 **사용**으로 전환합니다.
 - c [호스트 인프라 트래픽 리소스] 섹션에서 트래픽 유형을 선택하고 제한, 공유 및 예약에 대한 값을 입력합니다.
 - 6 **추가**를 클릭합니다.
- 새 NIOC 프로파일이 NIOC 프로파일의 목록에 추가됩니다.

API를 사용하여 N-VDS 스위치에서 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 구성합니다.

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.

아래의 샘플 응답에 호스트에 적용된 NIOC 프로파일이 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 새 NIOC 프로파일을 만듭니다.

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. When the 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 and 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-4004-8cf-d-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 섹션에서 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/nicVnicInfo
```

```

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 # [root@ host:] /get /net/portsets/DvsPortset-1/uplinks/vmnic4/nicVnicInfo

```

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
}

```

NIOC 프로파일은 NSX-T Data Center 호스트에서 실행 중인 애플리케이션에 대한 사전 구성된 대역폭 할당을 사용하여 구성됩니다.

NSX Edge 전송 노드 생성

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 Edge도 포함될 수 있습니다. 다음 절차에서는 NSX Edge를 전송 노드로 추가하는 방법을 보여줍니다.

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.

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

사전 요구 사항

- NSX Edge는 관리부에 연결되어야 하고 **패브릭 > Edge** 페이지에서 MPA 연결이 [작동] 상태여야 합니다. [NSX Edge를 관리부에 연결](#)의 내용을 참조하십시오.
- 전송 영역을 구성해야 합니다.
- 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 **패브릭 > 노드 > 전송 노드 > 추가**를 선택합니다.
- 3 NSX Edge 전송 노드의 이름을 입력합니다.
- 4 드롭다운 목록에서 NSX Edge 패브릭 노드를 선택합니다.
- 5 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.

6 N-VDS 탭을 클릭하고 N-VDS 정보를 제공합니다.

옵션	설명
N-VDS 이름	전송 영역을 생성할 때 구성한 이름과 반드시 일치해야 합니다.
업링크 프로파일	드롭다운 메뉴에서 업링크 프로파일을 선택합니다. 사용 가능한 업링크는 선택된 업링크 프로파일의 구성에 따라 다릅니다.
IP 할당	오버레이 N-VDS에 대해 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.
물리적 NIC	vmnicX를 물리적 NIC로 사용하는 호스트 전송 노드와 달리, NSX Edge 전송 노드는 fp-ethX를 사용합니다.

7 (선택 사항) 다음과 같이 GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>` API 호출을 사용하여 전송 노드를 확인합니다.

GET `https://<nsx-mgr>/api/v1/transport-nodes/78a03020-a3db-44c4-a8fa-f68ad4be6a0c`

```
{
  "resource_type": "TransportNode",
  "id": "78a03020-a3db-44c4-a8fa-f68ad4be6a0c",
  "display_name": "node-comp-01b",
  "transport_zone_endpoints": [
    {
      "transport_zone_id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ]
    }
  ],
  "host_switches": [
    {
      "host_switch_profile_ids": [
        {
          "value": "8abdb6c0-db83-4e69-8b99-6cd85bfcc61d",
          "key": "UplinkHostSwitchProfile"
        },
        {
          "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
          "key": "LldpHostSwitchProfile"
        }
      ],
      "host_switch_name": "overlay-hostswitch",
      "pnics": [
        {
          "device_name": "vmnic1",
          "uplink_name": "uplink-1"
        }
      ]
    }
  ],
}
```



```

    "static_ip_pool_id": "c78ac522-2a50-43fe-816a-c459a210127e"
  }
],
"node_id": "c551290a-f682-11e5-ae84-9f8726e1de65",
"_create_time": 1459547122893,
"_last_modified_user": "admin",
"_last_modified_time": 1459547126740,
"_create_user": "admin",
"_revision": 1
}

```

- 8 (선택 사항)** 상태 정보를 보려면 GET <https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/status> API 호출을 사용합니다.

```

{
  "control_connection_status": {
    "degraded_count": 0,
    "down_count": 0,
    "up_count": 1,
    "status": "UP"
  },
  "tunnel_status": {
    "down_count": 0,
    "up_count": 0,
    "status": "UNKNOWN",
    "bfd_status": {
      "bfd_admin_down_count": 0,
      "bfd_up_count": 0,
      "bfd_init_count": 0,
      "bfd_down_count": 0
    },
    "bfd_diagnostic": {
      "echo_function_failed_count": 0,
      "no_diagnostic_count": 0,
      "path_down_count": 0,
      "administratively_down_count": 0,
      "control_detection_time_expired_count": 0,
      "forwarding_plane_reset_count": 0,
      "reverse_concatenated_path_down_count": 0,
      "neighbor_signaled_session_down_count": 0,
      "concatenated_path_down_count": 0
    }
  },
  "pnic_status": {
    "degraded_count": 0,
    "down_count": 0,
    "up_count": 4,
    "status": "UP"
  },
  "mgmt_connection_status": "UP",

```

```

"node_uuid": "cd4a8501-0ffc-44cf-99cd-55980d3d8aa6",
"status": "UNKNOWN"
}

```

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.
- NSX Edge를 관리부에 연결합니다.
- NSX Edge를 전송 노드로 추가합니다.
- 경우에 따라 **패브릭 > 프로파일 > Edge 클러스터 프로파일**에서 HA(고가용성)를 위한 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 **패브릭 > 노드 > Edge 클러스터 > 추가**로 이동합니다.
- 3 NSX Edge 클러스터 이름을 입력합니다.
- 4 NSX Edge 클러스터 프로파일을 선택합니다.
- 5 **편집**을 클릭하고 **물리적 시스템** 또는 **가상 시스템**을 선택합니다.

[물리적 시스템]은 베어 메탈에 설치되는 NSX Edge를 나타냅니다. [가상 시스템]은 가상 시스템/장치로 설치되는 NSX Edge를 나타냅니다.

- 6 가상 시스템의 경우 [멤버 유형] 드롭다운 메뉴에서 NSX Edge 노드 또는 **공용 클라우드 게이트웨이 노드**를 선택합니다.

가상 시스템이 공용 클라우드 환경에 배포된 경우에는 [공용 클라우드 게이트웨이]를 선택하고 그렇지 않으면 NSX Edge 노드를 선택합니다.

- 7 **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 가이드의 내용을 참조하십시오.

NSX Cloud 구성 요소 설치

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 프로파일과 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.

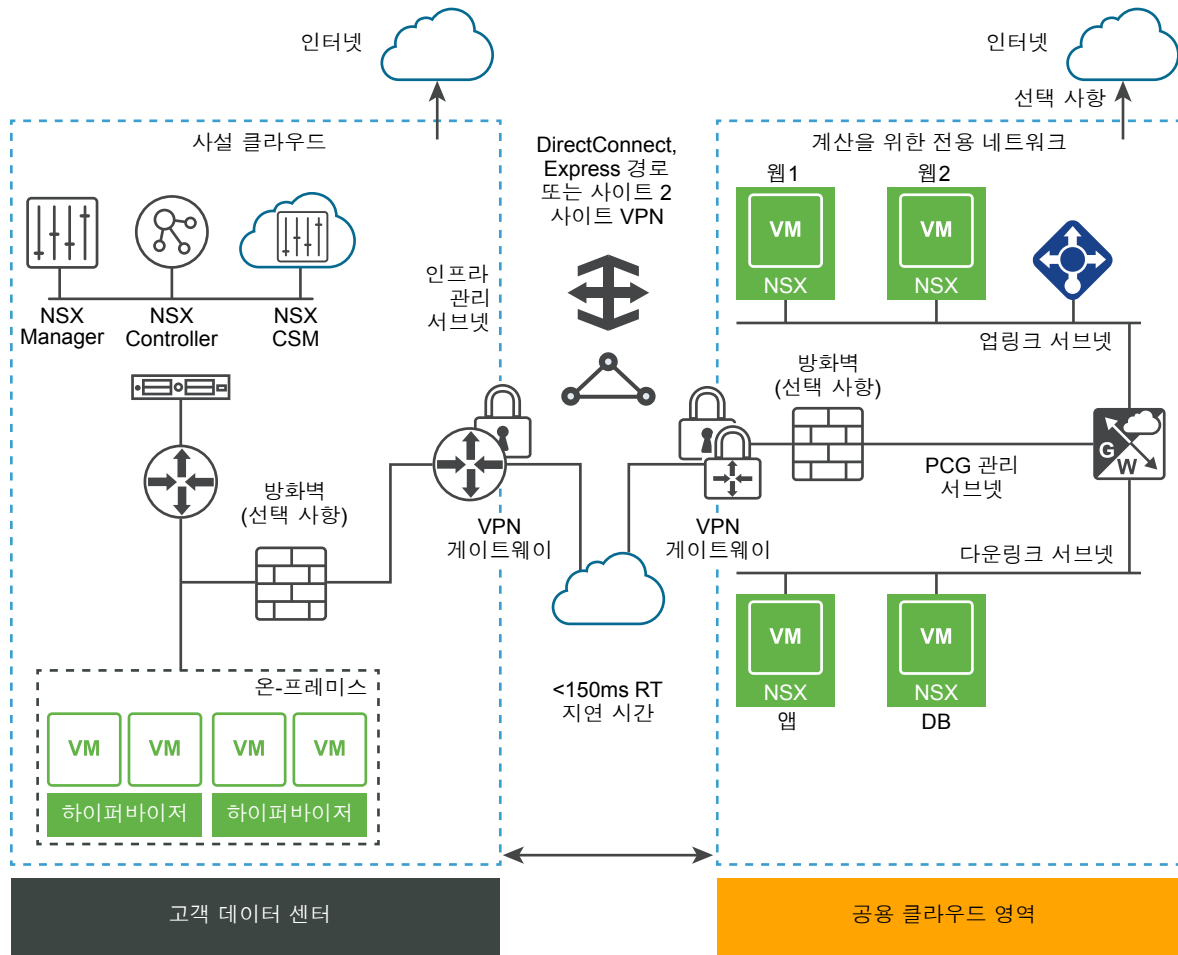
본 장은 다음 항목을 포함합니다.

- [NSX Cloud 아키텍처 및 구성 요소](#)
- [NSX Cloud 구성 요소 설치 개요](#)
- [CSM을 설치하고 NSX Manager와 연결](#)
- [공용 클라우드를 온-프레미스 배포와 연결](#)
- [공용 클라우드 계정 추가](#)
- [PCG 배포](#)
- [PCG 배포 해제](#)

NSX Cloud 아키텍처 및 구성 요소

NSX Cloud는 NSX-T Data Center 핵심 구성 요소인 NSX Manager와 NSX Controller를 공용 클라우드와 통합하여 구현 환경 전반에 네트워크 및 보안을 제공합니다.

그림 9-1. NSX Cloud 아키텍처



NSX Cloud의 핵심적인 구성 요소:

- NSX Manager: RBAC(역할 기반 액세스 제어)가 정의된 관리부.
- NSX Controller : 제어부 및 런타임 상태.
- Cloud Service Manager: 관리부에 공용 클라우드 관련 정보를 제공하기 위해 NSX Manager와 통합.
- NSX Public Cloud Gateway : NSX 관리부 및 제어부, NSX Edge Gateway 서비스와 연결 및 공용 클라우드 엔티티와 API 기반 통신.
- NSX 에이전트 기능: 워크로드 VM에 NSX 관리 데이터 경로 제공.

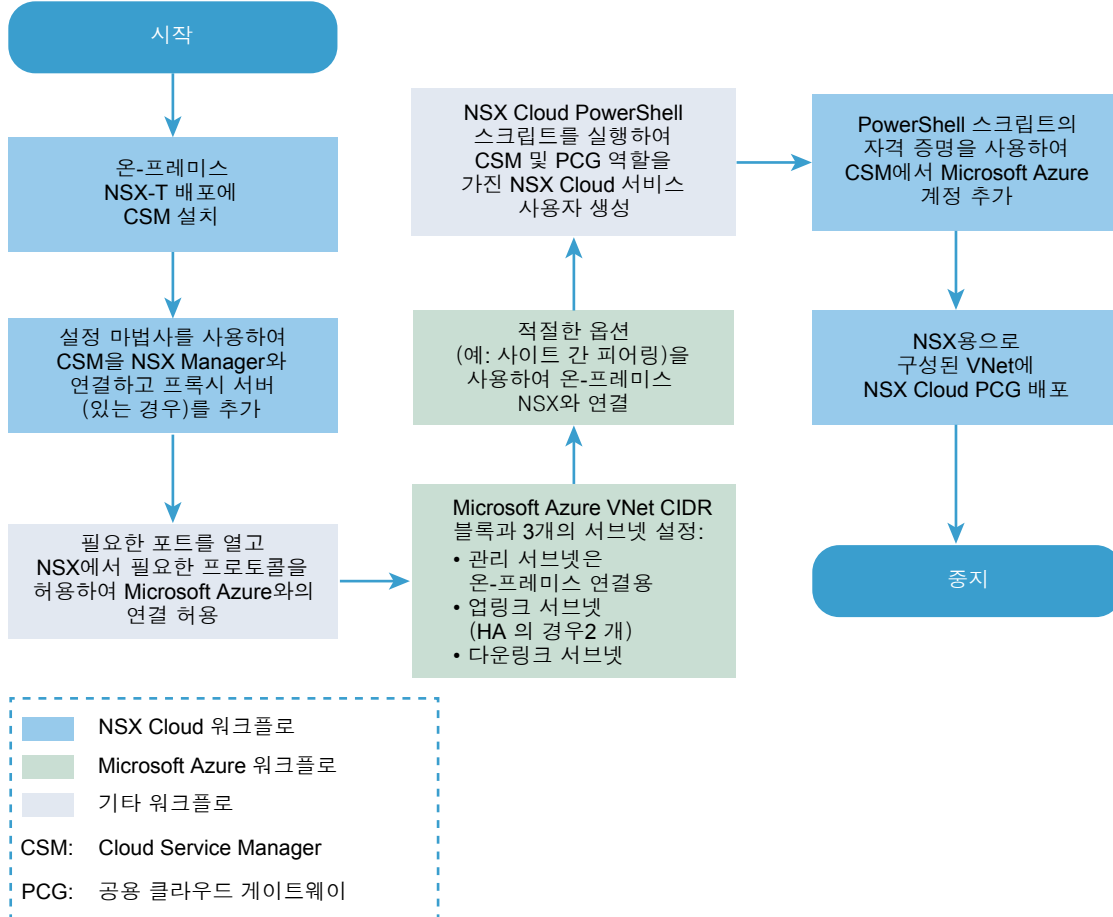
NSX Cloud 구성 요소 설치 개요

다음 순서도에서 NSX-T Data Center가 공용 클라우드에서 워크로드 VM을 관리할 수 있도록 설정하는 Day-0 작업에 대한 개요를 참조하십시오.

Microsoft Azure에 대한 Day-0 워크플로

이 순서도에는 Microsoft Azure VNet을 NSX Cloud에 추가하는 단계에 대한 개요가 표시됩니다.

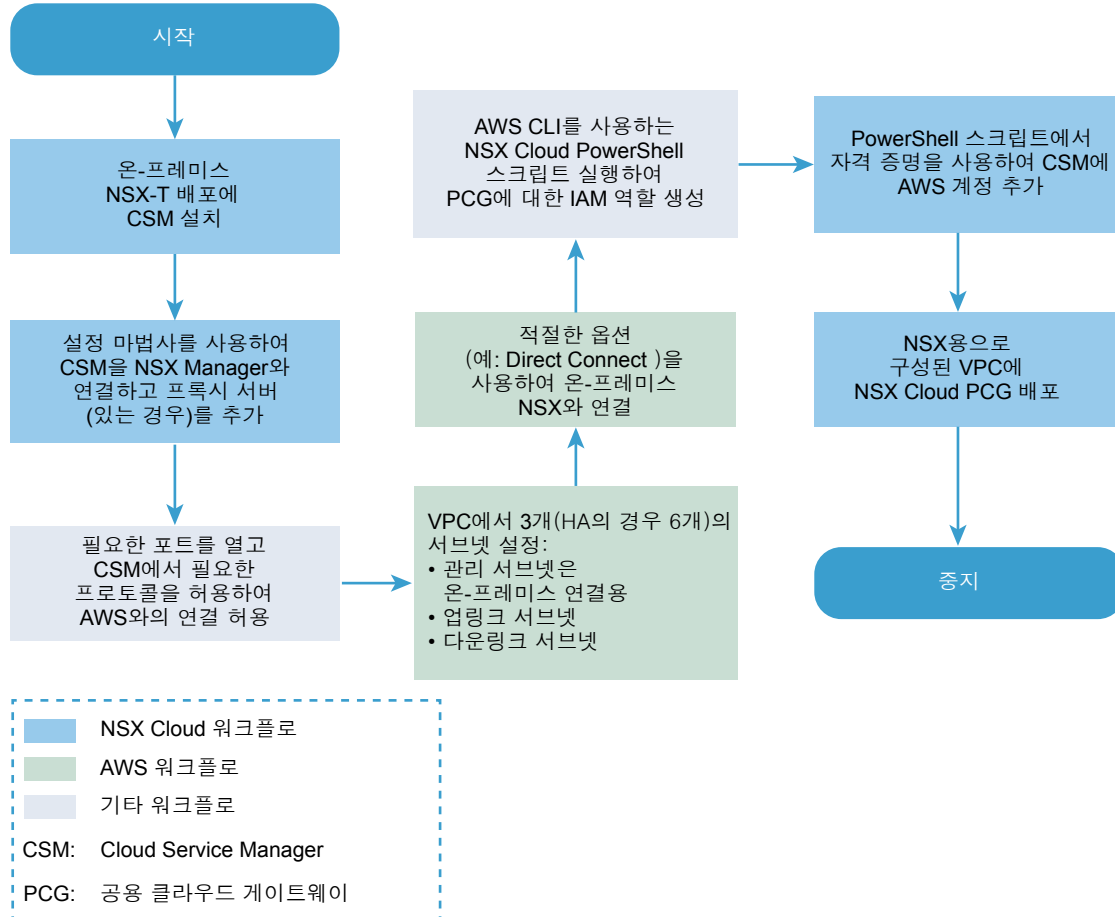
그림 9-2. Microsoft Azure에 대한 NSX Cloud Day-0 워크플로



AWS에 대한 Day-0 워크플로

이 순서도는 AWS VPC를 NSX Cloud에 추가하는 단계에 대한 개요를 제공합니다.

그림 9-3. AWS에 대한 NSX Cloud Day-0 워크플로



CSM 을 설치하고 NSX Manager 와 연결

설정 마법사를 사용하여 CSM을 NSX Manager와 연결하고 프록시 서버(있는 경우)를 설정합니다.

CSM 설치

Cloud Service Manager(CSM)는 NSX Cloud의 필수 구성 요소입니다.

핵심 NSX-T Data Center 구성 요소를 설치한 후 CSM을 설치합니다.

자세한 지침은 [NSX Manager 및 사용 가능한 장치 설치](#) 항목을 참조하십시오.

NSX Manager의 FQDN 게시

NSX-T Data Center 핵심 구성 요소와 CSM을 설치한 다음 FQDN을 사용하여 NAT를 사용하도록 설정하려면 배포의 NSX-T DNS 서버에서 조회 및 역방향 조회 항목을 설정해야 합니다.

또한 NSX-T API를 사용하여 NSX Manager의 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.

CSM 을 NSX Manager 에 연결

구성 요소가 서로 통신할 수 있도록 하려면 CSM 장치를 NSX Manager와 연결해야 합니다.

사전 요구 사항

- NSX Manager가 설치되어 있고 NSX Manager에 로그인할 수 있는 관리자 권한이 있어야 합니다.
- CSM이 설치되어 있고 CSM에 엔터프라이즈 관리자 역할이 할당되어 있어야 합니다.

절차

- 1 NSX Manager에 대해 SSH 세션을 엽니다.
- 2 NSX Manager에서 get certificate api thumbprint 명령을 실행합니다.

```
NSX-Manager> get certificate api thumbprint
```

명령의 출력은 NSX Manager에 고유한 숫자열입니다.

- 3 엔터프라이즈 관리자 역할로 CSM에 로그인합니다.
- 4 **시스템 > 설정**을 클릭합니다. 그런 다음 **연결된 NSX 노드** 패널에서 **구성**을 클릭합니다.

참고 CSM을 처음 설치할 때 사용할 수 있는 CSM 설치 마법사를 사용할 때 이러한 세부 정보를 제공할 수도 있습니다.

5 NSX Manager의 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	엔터프라이즈 관리자 역할이 있는 사용자 이름과 암호를 입력합니다.
관리자 지문	2단계에서 확보한 NSX Manager의 지문 값을 입력합니다.

6 연결을 클릭합니다.

CSM에서 NSX Manager 지문을 확인하고 연결을 설정합니다.

(선택 사항) 프록시 서버 구성

실행할 수 있는 HTTP 프록시를 통해 인터넷에 접속된 HTTP/HTTPS 트래픽을 모두 라우팅하고 모니터링하려는 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 > 설정을 클릭합니다. 그런 다음 **프록시 서버** 패널에서 **구성**를 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.

옵션	설명
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.

공용 클라우드를 온-프레미스 배포와 연결

온-프레미스 배포를 공용 클라우드 계정 또는 구독과 연결하려면 적절한 연결 옵션을 사용해야 합니다.

하이브리드 연결을 위해 CSM 의 포트 및 프로토콜에 액세스할 수 있도록 설정

필요한 네트워크 포트를 열고 NSX Manager에서 공용 클라우드 연결을 사용하도록 설정하는 데 필요한 프로토콜을 허용합니다.

공용 클라우드의 NSX Manager 에 대한 액세스 허용

온-프레미스 NSX Manager 배포와의 연결을 허용하도록 다음 네트워크 포트 및 프로토콜을 엽니다.

표 9-1.

시작	끝	프로토콜/포트	설명
PCG	NSX Manager	TCP/5671	공용 클라우드에서 온-프레미스 NSX-T Data Center로 관리부 통신을 위한 인바운드 트래픽
PCG	NSX Manager	TCP/8080	공용 클라우드에서 온-프레미스 NSX-T Data Center로 업그레이드를 위한 인바운드 트래픽
PCG	NSX Controller	TCP/1234, TCP/1235	공용 클라우드에서 온-프레미스 NSX-T Data Center로 제어부 통신을 위한 인바운드 트래픽
PCG	DNS	UDP/53	공용 클라우드에서 온-프레미스 NSX-T Data Center DNS로 인바운드 트래픽 (온-프레미스 DNS 서버를 사용하는 경우)
CSM	PCG	TCP/7442	CSM 구성 푸시

표 9-1. (계속)

시작	끝	프로토콜/포트	설명
입의	NSX Manager	TCP/443	NSX Manager UI
입의	CSM	TCP/443	CSM UI

중요 모든 NSX-T Data Center 인프라 통신은 SSL 기반 암호화를 활용합니다. 방화벽에서 비표준 포트를 통한 SSL 트래픽을 허용하는지 확인하십시오.

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 Center 와 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 설명서](#)를 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 [Azure Security Center 설명서](#)를 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.

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 클라우드에는 온-프레미스 배포와 연결할 수 있는 옵션을 제공합니다. 요구 사항에 맞는 사용 가능한 연결 옵션을 선택할 수 있습니다. 자세한 내용은 [AWS 참조 설명서](#)를 참조하십시오.

참고 AWS에서 적용할 수 있는 보안 고려 사항 및 모범 사례를 검토하고 구현해야 합니다. [AWS 보안 모범 사례](#)를 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.

- 2 VPC에 연결된 인터넷 게이트웨이(IGW)가 있는지 확인합니다.
- 3 VPC에 대한 라우팅 테이블의 대상이 `0.0.0.0/0`으로 설정되어 있고 대상이 VPC에 연결된 IGW인지 확인합니다.
- 4 VPC에 대해 DNS 확인 및 DNS 호스트 이름을 사용하도록 설정합니다.

공용 클라우드 계정 추가

공용 클라우드 인벤토리를 추가하려면 공용 클라우드에서 역할을 생성하여 NSX Cloud에 대한 액세스를 허용한 다음 CSM에서 필요한 정보를 추가해야 합니다.

Microsoft Azure 인벤토리 액세스를 위해 CSM 사용

Microsoft Azure 구독에는 NSX-T Data Center 관리 아래로 가져오려는 하나 이상의 계산 VNet이 포함되어 있습니다.

참고 CSM에 AWS 계정을 이미 추가한 경우에는 Microsoft Azure 계정을 추가하기 전에 **NSX Manager > 패브릭 > 프로파일 > 업링크 프로파일 > PCG-Uplink-HostSwitch-Profile**에서 MTU를 1500으로 업데이트하십시오. 이 작업은 NSX Manager REST API를 사용하여 수행할 수도 있습니다.

구독에서 NSX Cloud가 작동하려면 NSX-T Data Center에 필요한 액세스 권한을 부여하기 위해 새로운 서비스 사용자를 생성해야 합니다. 또한 CSM 및 PCG에 대한 MSI 역할도 생성해야 합니다.

NSX Cloud는 서비스 사용자를 생성하는 PowerShell 스크립트를 제공합니다.

이 과정은 두 단계입니다.

- 1 NSX Cloud PowerShell 스크립트를 사용합니다.
 - NSX Cloud에 대한 서비스 사용자 계정을 생성합니다.
 - CSM에 대한 역할을 생성하고 이를 서비스 사용자에게 연결합니다.
 - PCG에 대한 역할을 생성하고 이를 서비스 사용자에게 연결합니다.
- 2 CSM에서 Microsoft Azure 구독을 추가합니다.

필요한 역할 생성

NSX Cloud는 Microsoft Azure의 MSI(Managed Service Identity) 기능을 활용하여 Microsoft 자격 증명을 안전하게 유지하면서 인증을 관리합니다.

Microsoft Azure 구독에서 NSX Cloud가 작동하려면 CSM 및 PCG에 대한 MSI 역할과 NSX Cloud에 대한 서비스 사용자를 생성해야 합니다.

이 작업은 NSX Cloud PowerShell 스크립트를 실행하여 수행할 수 있습니다. 또한 JSON 형식의 파일 두 개가 매개 변수로 필요합니다. 필요한 매개 변수와 함께 PowerShell 스크립트를 실행하면 다음 구성체가 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.

참고 스크립트를 처음 실행할 때 Microsoft Azure의 응답 시간으로 인해 스크립트가 실패할 수 있습니다. 스크립트가 실패하면 다시 실행해 보십시오.

사전 요구 사항

- AzureRM 모듈이 설치된 PowerShell 5.0 이상이 필요합니다.
- NSX Cloud 서비스 사용자를 생성하기 위해 스크립트를 실행하려는 Microsoft Azure 구독의 소유자여야 합니다.

절차

- 1 Windows 데스크톱 또는 서버에서, 이름이 CreateNSXCloudCredentials.zip인 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.

파일 이름	설명
CreateNSXRoles.ps1	이것은 CSM 및 PCG에 대한 NSX Cloud 서비스 사용자 및 MSI 역할을 생성하는 PowerShell 스크립트입니다.
nsx_csm_role.json	이 파일에는 CSM 역할 이름과 Microsoft Azure에서 이 역할의 사용 권한이 포함되어 있습니다. 이것은 PowerShell 스크립트에 대한 입력으로, 스크립트와 동일한 폴더에 있어야 합니다.
nsx_pcg_role.json	이 파일에는 PCG 역할 이름과 Microsoft Azure에서 이 역할의 사용 권한이 포함되어 있습니다. 이것은 PowerShell 스크립트에 대한 입력으로, 스크립트와 동일한 폴더에 있어야 합니다. 기본 PCG(게이트웨이) 역할 이름은 nsx-pcg-role입니다.

참고 Microsoft Azure Active Directory에서 여러 구독에 대한 역할을 생성 중인 경우라면 각각의 JSON 파일에서 각 구독에 대한 CSM 및 PCG 역할 이름을 변경한 후 스크립트를 다시 실행해야 합니다.

- 3 Microsoft Azure 구독 ID를 매개 변수로 사용하여 스크립트를 실행합니다. 매개 변수 이름은 subscriptionId입니다.

예를 들면 다음과 같습니다.

```
.\CreateNSXRoles.ps1 -subscriptionId <your_subscription_ID>
```

이것은 NSX Cloud에 대한 서비스 사용자와 CSM 및 PCG에 대해 적절한 권한을 가진 역할을 생성하고 CSM 및 PCG 역할을 NSX Cloud 서비스 사용자에게 연결합니다.

- 4 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

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](#)

CSM 에서 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.

절차

- 1 엔터프라이즈 관리자 역할이 있는 계정을 사용하여 CSM에 로그인합니다.
- 2 **CSM > 클라우드 > Azure**로 이동합니다.

3 + 추가를 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.
게이트웨이 역할 이름	기본값은 nsx-pcg-role입니다. 기본값을 변경했다면 이 값은 nsx_pcg_role.json 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 몇 분 내에 **계정** 섹션에서 해당 계정을 볼 수 있습니다.

다음에 수행할 작업

[Microsoft Azure VNet에 PCG 배포](#)

AWS 인벤토리 액세스를 위해 CSM 사용

AWS 계정에는 NSX-T Data Center 관리 아래로 가져오려는 하나 이상의 계산 VPC가 포함되어 있습니다.

이 과정은 세 단계입니다.

1 AWS CLI가 필요한 NSX Cloud 스크립트를 사용하여 다음을 수행합니다.

- IAM 프로파일을 생성합니다.
- PCG에 대한 역할을 생성합니다.

2 CSM에서 AWS 계정을 추가합니다.

필요한 역할 생성

NSX Cloud는 AWS IAM을 활용하여 AWS 계정 액세스에 필요한 사용 권한을 PCG에 제공하는 NSX Cloud 프로파일에 연결된 역할을 생성합니다.

AWS 계정에서 NSX Cloud가 작동하려면 PCG에 대한 IAM 프로파일 및 역할을 생성해야 합니다.

이 작업은 AWS CLI를 사용하여 다음 구성체를 생성하는 NSX Cloud PowerShell 스크립트를 실행하여 수행할 수 있습니다.

- NSX Cloud에 대한 IAM 프로파일.

- PCG가 공용 클라우드 인벤토리에서 작동할 수 있게 해 주는 PCG에 대한 역할.

사전 요구 사항

- AWS 계정의 액세스 키 및 비밀 키를 사용하여 AWS CLI를 설치하고 구성해야 합니다.
- 스크립트에 제공할 고유한 IAM 프로파일 이름을 선택해야 합니다. 게이트웨이 역할 이름이 이 IAM 프로파일에 연결됩니다.
-

절차

- 1 Linux나 호환되는 데스크톱 또는 서버에서, 이름이 AWS_create_credentials.sh인 PowerShell 스크립트를 NSX-T Data Center **다운로드 페이지 > 드라이버 및 도구 > NSX Cloud 스크립트 > AWS**에서 다운로드합니다.
- 2 스크립트를 실행하고 메시지가 표시되면 IAM 프로파일의 이름을 입력합니다. 예를 들면 다음과 같습니다.

```
bash AWS_create_NSXCloud_credentials.sh
```

- 3 스크립트가 성공적으로 실행되면 AWS 계정에 PCG에 대한 IAM 프로파일과 역할이 생성됩니다. 값은 스크립트를 실행한 디렉토리의 출력 파일에 저장됩니다. 파일 이름은 aws_details.txt입니다.

참고 기본적으로 PCG(게이트웨이) 역할 이름은 nsx_pcg_service입니다. 게이트웨이 역할 이름으로 다른 값을 원하는 경우 스크립트에서 이를 변경할 수 있습니다. 이 값은 CSM에서 AWS 계정을 추가하는 데 필요하므로 기본값을 변경하는 경우 해당 값을 기록해 두어야 합니다.

다음에 수행할 작업

CSM에서 [AWS 계정 추가](#)

CSM 에서 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.txt를 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	기본적으로 이 옵션은 사용하도록 설정되어 있으며, 이 옵션을 사용하면 NSX Manager에서 AWS 태그를 볼 수 있습니다.
게이트웨이 역할 이름	기본값은 nsx_pcg_service입니다. 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.

다음에 수행할 작업

[AWS VPC에 PCG 배포](#)

PCG 배포

NSX Public Cloud Gateway(PCG)는 공용 클라우드와 NSX-T Data Center 온-프레미스 관리 구성 요소 간의 북-남 연결을 제공합니다.

사전 요구 사항

- 공용 클라우드 계정이 CSM에 이미 추가되어 있어야 합니다.
- PCG를 배포 중인 VPC 또는 VNet에 고가용성(업링크, 다운링크 및 관리)을 위해 필요한 서브넷이 적절하게 조정되어 있어야 합니다.

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.

Microsoft Azure VNet에 PCG 배포

다음 지침에 따라 Microsoft Azure 구독에 PCG를 배포합니다.

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. **기본 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	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 가이드의 격리 정책 관리 를 참조하십시오.
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.
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.
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.

옵션	설명
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

워크로드 VM을 등록합니다. Day-N 워크플로에 대한 자세한 내용은 NSX-T Data Center 관리 가이드의 **워크로드 VM 등록 및 관리**를 참조하십시오.

AWS VPC에 PCG 배포

다음 지침에 따라 AWS 계정에 PCG를 배포합니다.

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 배포**를 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	기본 선택 항목은 [사용]입니다. 이것은 그린필드 배포에 권장됩니다. VPC에서 이미 VM을 시작했다면 격리 정책을 사용하지 않도록 설정하십시오. 자세한 내용은 NSX-T Data Center 관리 가이드의 격리 정책 관리 를 참조하십시오.
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.
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.

옵션	설명
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 상태를 설정합니다.
기본 게이트웨이 설정	드롭다운 메뉴에서 HA를 위한 기본 게이트웨이로 us-west-1a와 같은 가용성 영역을 선택합니다. 드롭다운 메뉴에서 업링크, 다운링크 및 관리 서브넷을 할당합니다.
보조 게이트웨이 설정	드롭다운 메뉴에서 HA를 위한 보조 게이트웨이로 us-west-1b와 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 **완료**를 클릭합니다.

다음에 수행할 작업

워크로드 VM을 등록합니다. Day-N 워크플로에 대한 자세한 내용은 NSX-T Data Center 관리 가이드의 **워크로드 VM 등록 및 관리**를 참조하십시오.

PCG 배포 후 생성되는 구성체

PCG가 성공적으로 배포된 후 NSX Manager에 중요한 NSX-T Data Center 엔티티가 생성 및 구성되고 공용 클라우드에 보안 그룹이 생성됩니다.

NSX Manager 구성

다음 엔티티는 NSX Manager에서 자동으로 생성됩니다.

- PCG(공용 클라우드 게이트웨이)라는 Edge 노드가 생성됩니다.

- PCG가 Edge 클러스터에 추가됩니다. 고가용성 배포에서는 2개의 PCG가 있습니다.
- PCGPCG는 2개의 전송 영역이 생성된 전송 노드로 등록됩니다.
- 두 개의 기본 논리적 스위치가 생성됩니다.
- Tier-0 논리적 라우터가 하나 생성됩니다.
- IP 검색 프로파일이 생성됩니다. 이것은 오버레이 논리적 스위치에 사용됩니다.
- DHCP 프로파일이 생성됩니다. 이것은 DHCP 서버에 사용됩니다.
- 이름이 **PublicCloudSecurityGroup**인 기본 NSGroup이 생성되며 다음과 같은 멤버가 포함됩니다.
 - 기본 VLAN 논리적 스위치
 - HA를 사용하도록 설정한 경우 논리적 포트, PCG 업링크 포트마다 각각 하나씩
 - IP 주소
- 세 가지 기본 분산 방화벽 규칙이 생성됩니다.
 - LogicalSwitchToLogicalSwitch
 - LogicalSwitchToAnywhere
 - AnywhereToLogicalSwitch

참고 이러한 DFW 규칙은 모든 트래픽을 차단하므로 해당 요구 사항에 따라 조정해야 합니다.

NSX Manager에서 다음 구성을 확인하십시오.

- 1 NSX Cloud 대시보드에서 **NSX Manager**를 클릭합니다.
- 2 **패브릭 > 노드 > Edge**로 이동합니다. 공용 클라우드 게이트웨이가 Edge 노드로 나열되어야 합니다.
- 3 배포 상태, 관리자 연결 및 컨트롤러 연결이 연결되어 있는지 확인합니다(상태가 녹색점이 있는 **실행**을 표시함).
- 4 **패브릭 > 노드 > Edge 클러스터**로 이동하고 Edge 클러스터와 PCG가 이 클러스터의 일부로 추가되었는지 확인합니다.
- 5 **패브릭 > 노드 > 전송 노드**로 이동하고 PCG가 전송 노드로 등록되었는지 그리고 PCG를 배포하는 동안 자동 생성된 2개의 전송 영역에 연결되었는지 확인합니다.
 - VLAN 트래픽 유형 -- 이것은 PCG 업링크에 연결됩니다.
 - 오버레이 트래픽 유형 -- 이것은 오버레이 논리적 네트워킹을 위한 것입니다.
- 6 논리적 스위치와 Tier-0 논리적 라우터가 생성되었고 논리적 라우터가 Edge 클러스터에 추가되었는지 확인합니다.

중요 NSX 생성 엔티티를 삭제하지 마십시오.

공용 클라우드 구성

AWS에서:

- AWS VPC에서 새로운 A 유형 레코드 집합이 `nsx-gw.vmware.local`이라는 이름으로 추가됩니다. 이 레코드에 매핑된 IP 주소는 PCG의 관리 IP 주소와 일치합니다. 이것은 AWS에서 DHCP를 사용하여 할당하며 VPC별로 다릅니다.
- PCG의 업링크 인터페이스에 대한 보조 IP가 생성됩니다. AWS Elastic IP는 이 보조 IP 주소와 연결됩니다. 이 구성은 SNAT를 위한 것입니다.

AWS 및 Microsoft Azure에서:

gw 보안 그룹은 각각의 PCG 인터페이스에 적용됩니다.

표 9-2. NSX Cloud 에서 PCG 인터페이스용으로 생성된 공용 클라우드 보안 그룹

보안 그룹 이름	Microsoft Azure에서 사용할 수 있습니까?	AWS에서 사용할 수 있습니까?	전체 이름
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

표 9-3. 워크로드 VM용 NSX Cloud 에서 생성된 공용 클라우드 보안 그룹

보안 그룹 이름	Microsoft Azure에서 사용할 수 있습니까?	AWS에서 사용할 수 있습니까?	설명
격리	예	아니요	Microsoft Azure에 대한 격리 보안 그룹
기본	아니요	예	AWS에 대한 격리 보안 그룹
vm-underlay-sg	예	예	VM 비오버레이 보안 그룹
vm-override-sg	예	예	VM 재정의의 보안 그룹
vm-overlay-sg	예	예	VM 오버레이 보안 그룹(현재 릴리스에서는 사용되지 않음)
vm-outbound-bypass-sg	예	예	VM 아웃바운드 바이패스 보안 그룹(현재 릴리스에서는 사용되지 않음)
vm-inbound-bypass-sg	예	예	VM 인바운드 바이패스 보안 그룹(현재 릴리스에서는 사용되지 않음)

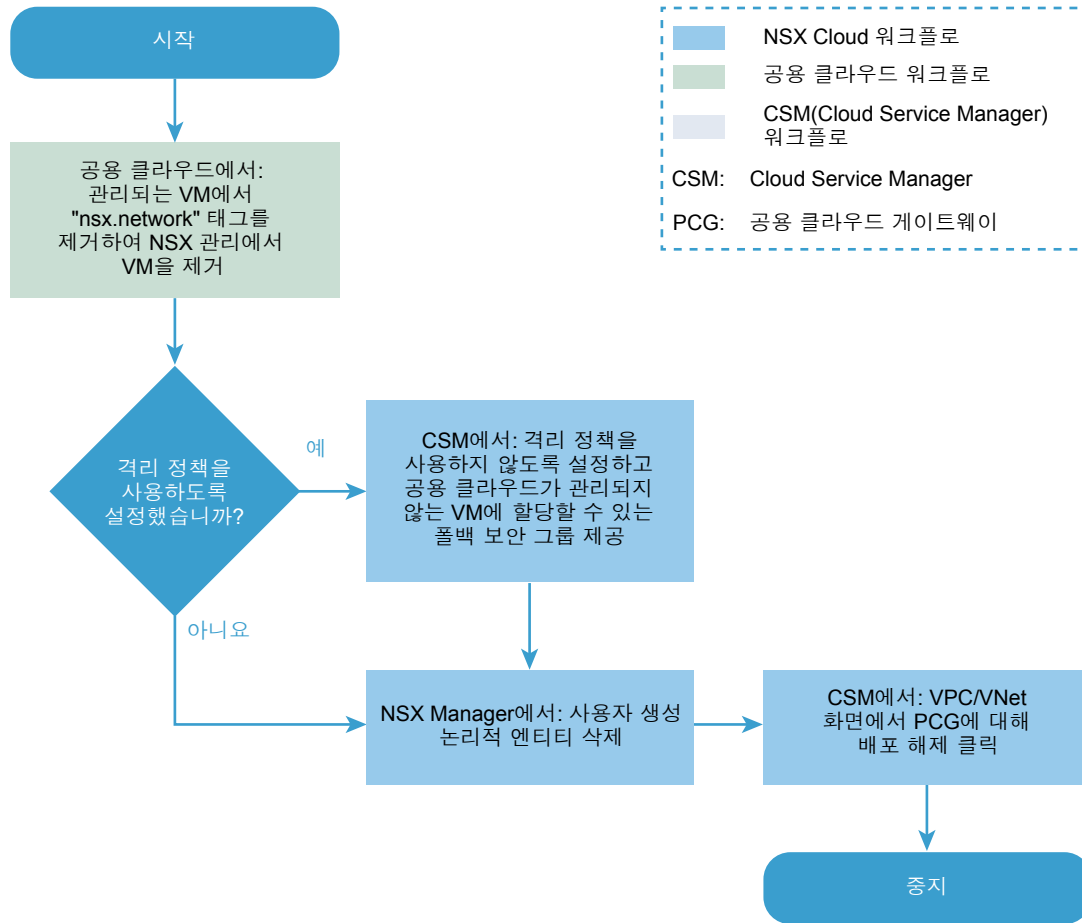
PCG 배포 해제

PCG를 배포 해제하는 단계는 이 순서도를 참조하십시오.

- PCG를 배포해제하려면 다음 조건이 충족되어야 합니다. VPC 또는 VNet에 NSX로 관리되는 워크로드 VM이 없어야 합니다.

- 격리 정책을 사용하지 않도록 설정해야 합니다.
- PCG와 연결된 모든 사용자 생성 논리적 엔티티가 삭제되어야 합니다.

그림 9-4. PCG 배포 해제



1 공용 클라우드에서 VM 태그 해제

PCG를 배포 해제할 수 있으려면 모든 VM이 관리되지 않는 상태여야 합니다.

2 격리 정책이 사용되도록 설정된 경우 사용되지 않도록 설정

이전에 격리 정책이 사용되도록 설정된 경우 사용되지 않도록 설정해야 PCG를 배포해제 할 수 있습니다.

3 사용자 생성 논리적 엔티티 삭제

NSX Manager에서 생성한 논리적 엔티티를 모두 삭제합니다.

4 CSM에서 배포 해제

사전 요구 사항을 완료한 후 PCG를 배포 해제하려면 CSM에서 **클라우드 > <Public_Cloud> > <VNet/VPC>**로 이동하고 **게이트웨이 배포 해제**를 클릭합니다.

공용 클라우드에서 VM 태그 해제

PCG를 배포 해제할 수 있으려면 모든 VM이 관리되지 않는 상태여야 합니다.

공용 클라우드에서 VPC 또는 VNet으로 이동하고 관리되는 VM에서 `nsx.network` 태그를 제거합니다.

격리 정책이 사용되도록 설정된 경우 사용되지 않도록 설정

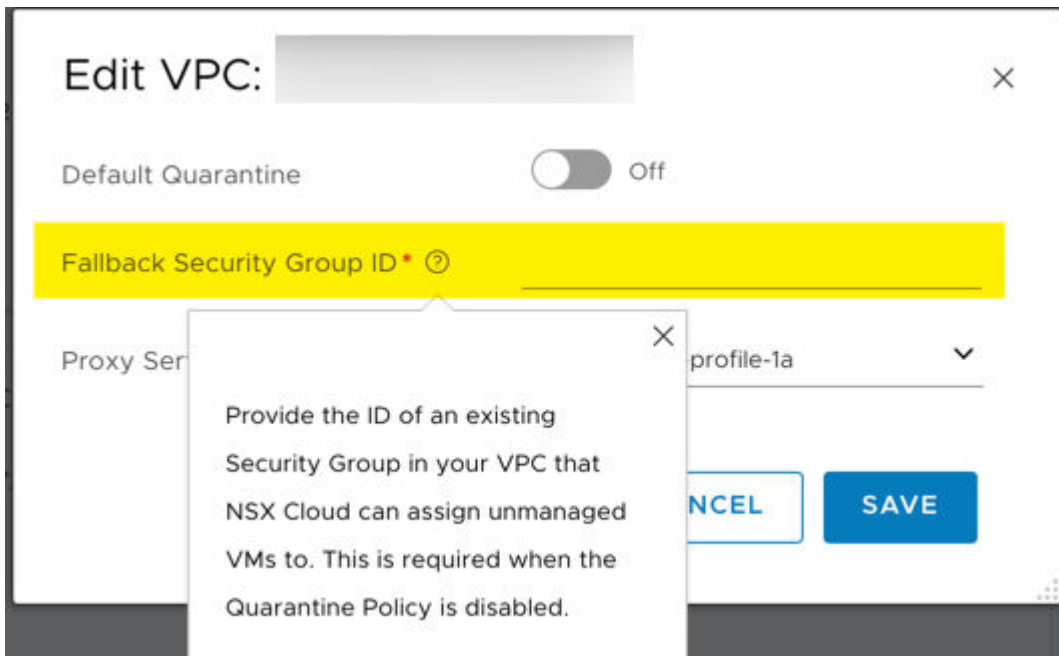
이전에 격리 정책이 사용되도록 설정된 경우 사용되지 않도록 설정해야 PCG를 배포해제 할 수 있습니다.

격리 정책이 사용되도록 설정되면 NSX Cloud에서 정의된 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.

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 [PCG 배포 후 생성되는 구성체](#)의 내용을 참조하십시오.

PCG를 배포 해제하는 VPC 또는 VNet에 대해 격리 정책을 사용하지 않도록 설정합니다.

- 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 태그를 제거하면 이러한 VM에도 폴백 보안 그룹이 할당됩니다.

참고 격리 정책을 사용 또는 사용하지 않도록 설정하기 위한 지침과 그에 따른 영향에 대한 자세한 내용은 NSX-T Data Center 관리 가이드의 **격리 정책 관리**를 참조하십시오.

사용자 생성 논리적 엔티티 삭제

NSX Manager에서 생성한 논리적 엔티티를 모두 삭제합니다.

삭제할 엔티티를 찾으려면 아래 목록을 참조하십시오.

참고 PCG를 배포할 때 자동으로 생성된 논리적 엔티티는 삭제하지 마십시오. **PCG 배포 후 생성되는 구성체** 항목을 참조하십시오.

- 공용 클라우드 DNS 항목
- DDI: DHCP 프로파일
- 라우팅: SNAT 규칙
- 라우팅: 정적 라우터
- 라우팅: 논리적 라우터 포트
- 라우팅: 논리적 라우터
- 패브릭 노드: Edge클러스터
- 패브릭 노드: 전송 노드
- 패브릭 노드: Edges
- 패브릭 프로파일: PCG-Uplink-HostSwitch-Profile
- 스위칭: 논리적 스위치 포트
- 스위칭: 논리적 스위치
- 패브릭 전송 영역: 전송 영역
- 스위칭: PublicCloud-Global-SpoofGuardProfile

CSM 에서 배포 해제

사전 요구 사항을 완료한 후 PCG를 배포 해제하려면 CSM에서 **클라우드 > <Public_Cloud> > <VNet/VPC>**로 이동하고 **게이트웨이 배포 해제**를 클릭합니다.

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 게이트웨이 배포 해제를 클릭합니다.

PCG를 배포 해제하면 NSX Cloud에서 생성된 기본 엔터티가 자동으로 제거됩니다.

NSX-T Data Center 제거

NSX-T Data Center 오버레이의 요소를 제거하거나, NSX-T Data Center에서 하이퍼바이저 호스트를 제거하거나, NSX-T Data Center를 완전히 제거할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- [NSX-T Data Center 오버레이 구성 해제](#)
- [NSX-T Data Center에서 호스트 제거 또는 NSX-T Data Center를 완전히 제거](#)

NSX-T Data Center 오버레이 구성 해제

오버레이를 삭제하려고 하지만 전송 노드를 원래 상태로 유지하려면 다음 단계를 따르십시오.

절차

- 1 vSphere Client에 로그인합니다.
- 2 VM 관리 도구를 사용하여 논리적 스위치에서 모든 VM을 분리하고 VM을 비 NSX-T Data Center 네트워크에 연결합니다.
- 3 KVM 호스트의 경우 SSH를 사용하여 호스트에 연결하고 VM의 전원을 끕니다.
`shutdown -h now`
- 4 NSX Manager UI 또는 API에서 모든 논리적 라우터를 삭제합니다.
- 5 NSX Manager UI 또는 API에서 모든 논리적 스위치 포트를 삭제한 다음 모든 논리적 스위치를 삭제합니다.
- 6 NSX Manager UI 또는 API에서 모든 NSX Edge를 삭제한 다음 모든 NSX Edge 클러스터를 삭제합니다.
- 7 필요에 따라 새 NSX-T Data Center 오버레이를 구성합니다.

NSX-T Data Center 에서 호스트 제거 또는 NSX-T Data Center 를 완전히 제거

NSX-T Data Center를 완전히 제거하거나 호스트가 NSX-T Data Center 오버레이에 더 이상 참여할 수 없도록 NSX-T Data Center에서 하이퍼바이저 호스트만 제거하려면 다음 단계를 따르십시오.

다음 절차에서는 NSX-T Data Center의 완전 제거를 수행하는 방법을 설명합니다.

사전 요구 사항

VM 관리 도구가 vCenter Server이면 vSphere 호스트를 유지 보수 모드로 설정합니다.

절차

- 1 NSX Manager에서 **패브릭 > 노드 > 전송 노드**를 선택하고 호스트 전송 노드를 삭제합니다.

전송 노드를 삭제하면 N-VDS가 호스트에서 제거됩니다. 다음 명령을 실행하여 이 동작을 수행할 수 있습니다.

```
[root@host:~] esxcli network vswitch dvs vmware list
```

KVM에서 해당 명령은 다음과 같습니다.

```
ovs-vsctl show
```

- 2 NSX Manager CLI에서 NSX-T Data Center install-upgrade 서비스가 실행되고 있는지 확인합니다.

```
nsx-manager-1> get service install-upgrade
Service name: install-upgrade
Service state: running
Enabled: True
```

- 3 관리부에서 호스트를 제거하고 NSX-T Data Center 모듈을 제거합니다.

모든 NSX-T Data Center 모듈이 제거되는 데 최대 5분이 걸릴 수 있습니다.

NSX-T Data Center 모듈을 제거하는 데 다음 몇 가지 방법을 사용할 수 있습니다.

- NSX Manager에서 **패브릭 > 노드 > 호스트 > 삭제**를 선택합니다.

NSX 구성 요소 제거가 선택되었는지 확인합니다. 이 옵션이 선택되면 NSX-T Data Center 모듈이 호스트에서 제거됩니다.

RHEL 7.4 종속성 패키지(json_spirit, python-greenlet, libev, protobuf, leveldb, python-gevent, python-simplejson, glog)를 제거합니다.

Ubuntu 16.04.x 종속성 패키지(nicira-ovs-hypervisor-node, openvswitch-switch, openvswitch-datapath-dkms, openvswitch-pki, python-openvswitch, openvswitch-common, libjson-spirit)를 제거합니다.

또한 **NSX 구성 요소 제거** 옵션을 선택하지 않은 상태로 **패브릭 > 노드 > 호스트 > 삭제**를 사용하는 방식은 호스트를 등록 취소하는 데 사용되는 방식이 아닙니다. 이 방식은 잘못된 상태의 호스트에 대한 해결 방법입니다.

- (계산 관리자에서 관리되는 호스트) NSX Manager에서 **패브릭 > 노드 > 호스트 > 전송 노드 > 호스트 삭제**를 선택합니다.

NSX Manager에서 **패브릭 > 노드 > 호스트 > 계산 관리자 > 클러스터 관리자 구성**을 선택하고 **자동으로 NSX 설치**의 선택을 취소합니다. 노드를 선택하고 **NSX 제거**를 클릭합니다.

NSX 구성 요소 제거가 선택되었는지 확인합니다. 이 옵션이 선택되면 NSX-T Data Center 모듈이 호스트에서 제거됩니다.

- DELETE /api/v1/fabric/nodes/<node-id> API를 사용합니다.

참고 이 API는 nsx-lcp 번들에서 종속성 패키지를 제거하지 않습니다.

RHEL 7.4 종속성 패키지(json_spirit, python-greenlet, libev, protobuf, leveldb, python-gevent, python-simplejson, glog)를 제거합니다.

Ubuntu 16.04.x 종속성 패키지(nicira-ovs-hypervisor-node, openvswitch-switch, openvswitch-datapath-dkms, openvswitch-pki, python-openvswitch, openvswitch-common, libjson-spirit)를 제거합니다.

- vSphere용 CLI를 사용합니다.

- a 관리자 지문을 가져옵니다.

```
manager> get certificate api thumbprint
```

- b 호스트의 NSX-T Data Center CLI에서 다음 명령을 실행하여 관리부에서 호스트를 분리합니다.

```
host> detach management-plane <MANAGER> username <ADMIN-USER> password <ADMIN-PASSWORD> thumbprint <MANAGER-THUMBPRINT>
```

- c 호스트에서 다음 명령을 실행하여 필터를 제거합니다.

```
[root@host:~] vsipioctl clearallfilters
```

- d 호스트에서 다음 명령을 실행하여 netcpa를 중지합니다.

```
[root@host:~] /etc/init.d/netcpad stop
```

- e 호스트에서 VM의 전원을 끄거나 다른 호스트로 마이그레이션합니다.

- f 호스트에서 다음 명령을 실행하여 NSX-T Data Center 구성 및 모듈을 수동으로 제거합니다. 이 명령은 모든 호스트 유형에서 지원됩니다.

```
[root@host:~] clear management-plane
```

다음에 수행할 작업

이렇게 변경하면 호스트가 관리부에서 제거되고 NSX-T Data Center 오버레이에 더 이상 참여할 수 없습니다.

NSX-T Data Center를 완전히 제거하려는 경우 VM 관리 도구에서 NSX Manager, NSX Controller 및 NSX Edge를 종료하고 디스크에서 삭제합니다.