

NSX 설치 가이드

업데이트 9

수정 날짜: 2020년 2월 21일

VMware NSX Data Center for vSphere 6.3



vmware®

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

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

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

Copyright © 2010 - 2020 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

목차

NSX 설치 가이드 5

1 NSX for vSphere 개요 6

NSX for vSphere 구성 요소 7

데이터부 8

제어부 9

관리부 10

소비 플랫폼 10

NSX Edge 10

NSX Services 13

2 설치 준비 15

NSX의 시스템 요구 사항 15

NSX for vSphere에 필요한 포트 및 프로토콜 17

NSX와 vSphere Distributed Switch 20

예: vSphere Distributed Switch 작업 22

복제 모드 파악하기 29

NSX 설치 워크플로 및 샘플 토폴로지 31

크로스 vCenter NSX 및 고급 연결 모드 33

3 NSX Manager 가상 장치 설치 35

4 NSX Manager에 vCenter Server 등록 40

5 Single Sign On 구성 43

6 NSX Manager에 대한 Syslog 서버 구성 45

7 NSX for vSphere 라이선스 설치 및 할당 47

8 NSX Controller 클러스터 배포 49

9 방화벽 보호 대상에서 가상 시스템 제외 53

10 NSX에 사용할 수 있도록 호스트 클러스터 준비 55

11 준비된 클러스터에 호스트 추가 59

- 12 NSX 준비된 클러스터에서 호스트 제거 60**
- 13 VXLAN 전송 매개 변수 구성 62**
- 14 세그먼트 ID 풀 및 멀티캐스트 주소 범위 할당 66**
- 15 전송 영역 추가 68**
- 16 논리적 스위치 추가 73**
- 17 논리적 분산 라우터 추가 79**
- 18 Edge Services Gateway 추가 92**
- 19 논리적 (분산) 라우터에서 OSPF 구성 103**
- 20 Edge Services Gateway에서 OSPF 구성 109**
- 21 호스트 클러스터에 Guest Introspection 설치 116**
- 22 NSX 구성 요소 제거 119**
 - Guest Introspection 모듈 제거 119
 - NSX Edge Services Gateway 또는 논리적 분산 라우터 제거 120
 - 논리적 스위치 제거 120
 - 호스트 클러스터에서 NSX 제거 120
 - 안전한 방법으로 NSX 설치 제거 122

NSX 설치 가이드

이 "NSX 설치 가이드"에서는 NSX Manager 사용자 인터페이스 및 vSphere Web Client를 사용하여 VMware NSX[®] for vSphere[®] 시스템을 설치하는 방법을 설명합니다. 또한 단계별 구성 지침 및 권장 모범 사례에 대한 정보도 수록되어 있습니다.

대상 사용자

이 설명서는 VMware vCenter 환경에서 NSX를 설치하거나 사용하려는 모든 사용자를 대상으로 합니다. 이 설명서의 정보는 가상 시스템 기술 및 가상 데이터 센터 작업에 익숙한 숙련된 시스템 관리자를 대상으로 작성되었으며, 이 설명서에서는 VMware ESXi, vCenter Server 및 vSphere Web Client를 포함하는 VMware vSphere에 익숙하다고 가정합니다.

VMware 기술 자료 용어집

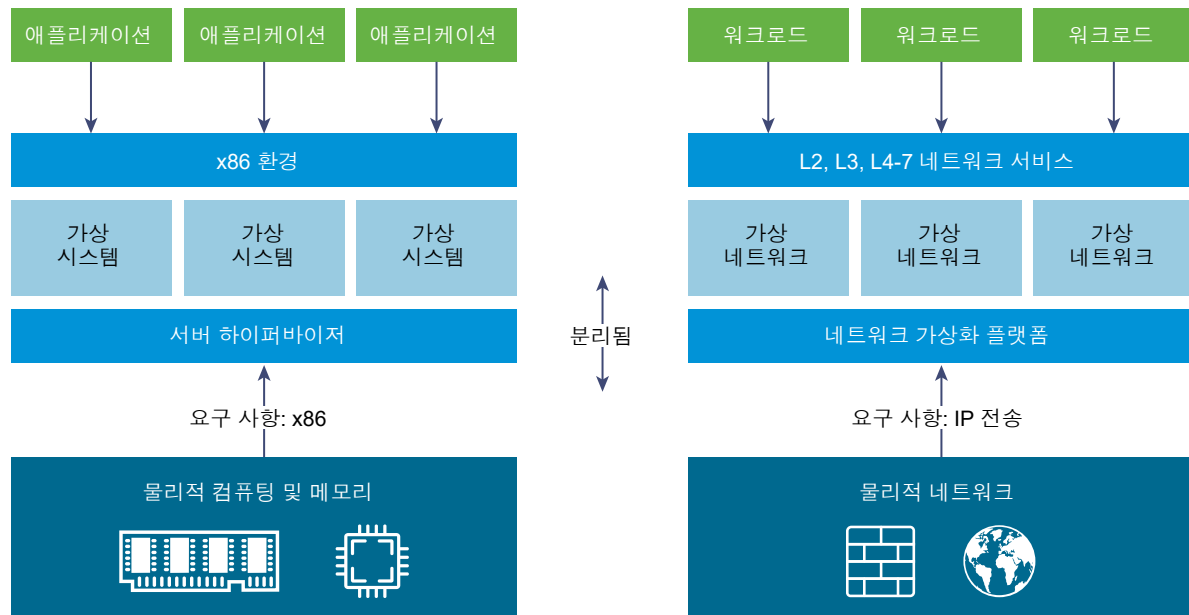
VMware 기술 자료 사이트에서는 새로운 용어를 정리한 용어집을 제공하고 있습니다. VMware 기술 설명서에 사용된 용어에 대한 정의를 보려면 <http://www.vmware.com/support/pubs>를 참조하십시오.

NSX for vSphere 개요

1

IT 조직은 서버 가상화의 직접적인 결과로 많은 혜택을 얻고 있습니다. 서버 통합으로 물리적인 복잡도는 줄어들고, 운영 효율성 및 기본 리소스를 동적으로 용도 변경할 수 있는 기능은 증가하여 점점 더 동적인 비즈니스 애플리케이션의 요구 사항을 신속하게 최적으로 충족할 수 있습니다.

현재 VMware의 SDDC(소프트웨어 정의 데이터센터) 아키텍처는 전체 물리적 데이터센터 인프라에서 가상화 기술을 확장하고 있습니다. NSX for vSphere는 SDDC 아키텍처의 핵심 제품입니다. NSX for vSphere를 사용한 가상화를 통해 계산 및 스토리지 부문에서 이미 구현된 뛰어난 성능을 네트워킹에서도 제공할 수 있게 되었습니다. 서버 가상화에서 소프트웨어 기반 VM(가상 시스템)을 프로그래밍 방식으로 생성, 스냅샷 생성, 삭제 및 복원하는 것과 상당히 동일한 방법으로 NSX for vSphere 네트워크 가상화에서도 소프트웨어 기반 가상 네트워크를 프로그래밍 방식으로 생성, 스냅샷 생성, 삭제 및 복원합니다. 그 결과 데이터 센터 관리자는 민첩성과 경제성 면에서 상당한 개선을 달성할 수 있을 뿐만 아니라 기본 물리적 네트워크의 운영 모델도 크게 단순화할 수 있는, 네트워킹에 대한 혁신된 접근 방식이 탄생했습니다. 기존의 네트워킹 모델과 모든 벤더의 차세대 패브릭 아키텍처를 포함한 모든 IP 네트워크에서 배포할 수 있는 기능을 제공하는 NSX for vSphere는 무중단 솔루션입니다. 실제로 NSX for vSphere를 사용하면 이미 구축된 물리적 네트워크 인프라에서도 소프트웨어 정의 데이터 센터를 배포하기만 하면 됩니다.



위 그림에서는 계산 및 네트워크 가상화 간의 유사점을 보여줍니다. 서버 가상화를 사용하면 소프트웨어 추상화 계층(서버 하이퍼바이저)에서 x86 물리적 서버(예: CPU, RAM, 디스크, NIC)의 익숙한 특성을 재현하고 이들 특성을 임의 조합으로 프로그래밍 방식을 통해 구성할 수 있기 때문에 몇 초 만에 고유한 VM을 생성할 수 있습니다.

기능상 네트워크 하이퍼바이저에 해당하는 네트워크 가상화를 사용하면 소프트웨어에서 계층 2 - 계층 7 네트워킹 서비스(예: 스위칭, 라우팅, 액세스 제어, 방화벽 기능, QoS 및 로드 밸런싱)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.

네트워크 가상화를 사용하면 서버 가상화와 유사한 이점을 얻을 수 있습니다. 예를 들어, VM은 기본 x86 플랫폼과 상관이 없고 VM을 통해 IT가 물리적 호스트를 계산 용량의 풀로 처리할 수 있는 것처럼, 가상 네트워크는 기본 IP 네트워크 하드웨어와 상관이 없고 가상 네트워크를 통해 IT는 물리적 네트워크를 요청 시 사용하고 용도 변경할 수 있는 전송 용량 풀로 처리할 수 있습니다. 레거시 아키텍처와 달리 기본 물리적 하드웨어 또는 토폴로지를 재구성하지 않고도 가상 네트워크를 프로그래밍 방식으로 프로비저닝, 변경, 저장, 삭제 및 복원할 수 있습니다. 널리 사용되는 서버 및 스토리지 가상화 솔루션의 기능 및 이점을 동등한 수준으로 제공하는 네트워킹에 대한 이러한 혁신적인 접근 방식은 소프트웨어 정의 데이터센터의 모든 잠재력을 발휘하게 만들 것입니다.

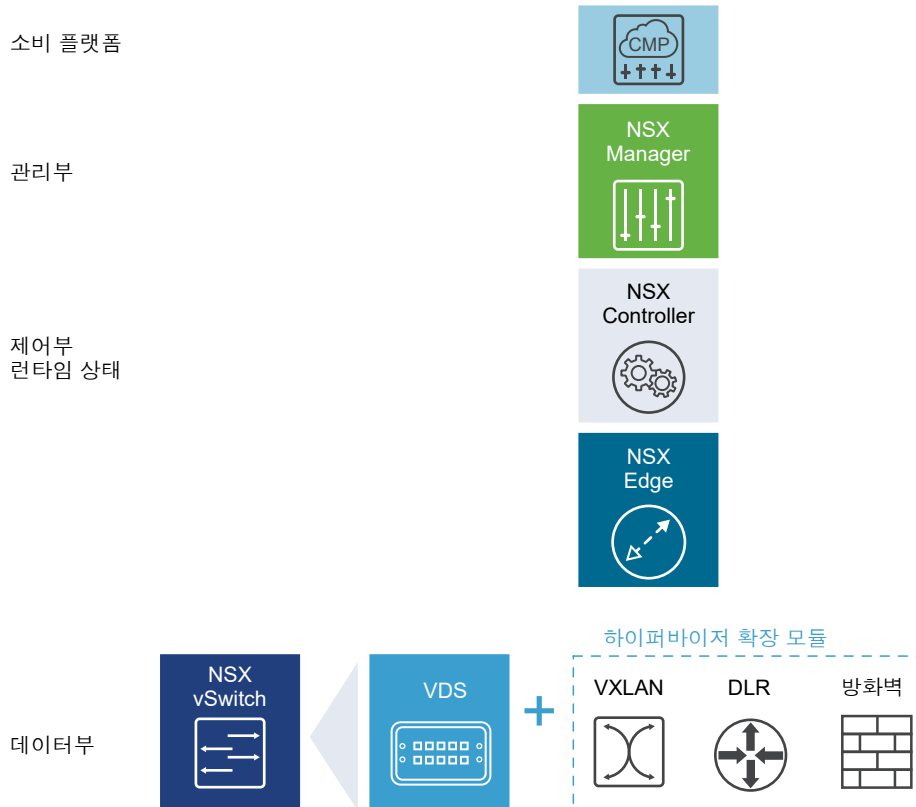
NSX for vSphere는 vSphere Web Client, CLI(명령줄 인터페이스) 및 REST API를 통해 구성할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- [NSX for vSphere 구성 요소](#)
- [NSX Edge](#)
- [NSX Services](#)

NSX for vSphere 구성 요소

이 섹션에서는 NSX for vSphere 솔루션의 구성 요소에 대해 설명합니다.



CMP(Cloud Management Platform)는 NSX for vSphere 구성 요소가 아니지만 NSX for vSphere는 REST API를 통한 거의 모든 CMP로의 통합과 VMware CMP와의 기본 통합을 제공합니다.

데이터부

NSX 데이터부는 서비스를 사용하도록 설정하는 추가 구성 요소가 포함된 VDS(vSphere Distributed Switch) 기반의 NSX vSwitch로 구성됩니다. NSX 커널 모듈, 사용자 공간 에이전트, 구성 파일 및 설치 스크립트가 VIB에 패키징되어 있고 하이퍼바이저 커널 내에서 실행됨으로써 분산 라우팅 및 논리적 방화벽 같은 서비스를 제공하고 VXLAN 브리징 기능을 사용하도록 설정합니다.

NSX vSwitch(vDS 기반)는 물리적 네트워크를 추상화하고 하이퍼바이저에서 액세스 수준에 따른 스위칭 기능을 제공합니다. 이는 VLAN 같은 물리적 구성체와 상관없이 논리적 네트워크를 사용하도록 하므로 네트워크 가상화의 중심입니다. vSwitch의 일부 이점은 다음과 같습니다.

- 프로토콜(예: VXLAN) 및 중앙 집중식 네트워크 구성을 사용하여 오버레이 네트워킹을 지원합니다. 오버레이 네트워킹을 통해 다음 기능을 제공합니다.
 - 물리적 네트워크에서 VLAN ID 사용을 줄입니다.
 - 데이터센터 네트워크를 다시 구축하지 않고도 기존 물리적 인프라의 기존 IP 네트워크에서 유연한 논리적 계층 2(L2) 오버레이를 생성할 수 있습니다.
 - 테넌트 간 분리를 유지하면서 통신(동-서/남-북)을 제공할 수 있습니다.
 - 애플리케이션 워크로드 및 가상 시스템이 오버레이 네트워크를 인지하지 않고도 물리적 L2 네트워크에 연결된 것처럼 작동합니다.

- 하이퍼바이저의 방대한 확장을 용이하게 합니다.
- 여러 기능(예: 포트 미러링, NetFlow/IPFIX, 구성 백업 및 복원, 네트워크 상태 점검, QoS 및 LACP)을 통해 가상 네트워크 내 트래픽 관리, 모니터링 및 문제 해결을 위한 종합적인 툴킷을 제공합니다.

논리적 라우터는 논리적 네트워킹 공간(VXLAN)에서 물리적 네트워크(VLAN)로 L2 브리징을 제공할 수 있습니다.

게이트웨이 디바이스는 일반적으로 NSX Edge 가상 장치입니다. NSX Edge는 L2, L3, 경계 방화벽, 로드 밸런싱 및 기타 서비스(예: SSL VPN 및 DHCP)를 제공합니다.

제어부

NSX 제어부는 NSX Controller 클러스터에서 실행됩니다. NSX Controller는 NSX 논리적 스위칭 및 라우팅 기능에 대한 제어부 기능을 제공하는 고급 분산 상태 관리 시스템입니다. 이 컨트롤러는 네트워크 내 모든 논리적 스위치에 대한 중앙 제어 지점이며 모든 호스트, 논리적 스위치(VXLAN) 및 논리적 분산 라우터에 대한 정보를 유지 관리합니다.

컨트롤러 클러스터는 하이퍼바이저에서 분산 스위칭 및 라우팅 모듈을 관리합니다. 컨트롤러를 통과하는 데이터부 트래픽은 없습니다. 컨트롤러 노드는 3개 멤버의 클러스터에 배포되어고가용성 및 확장을 사용하도록 설정합니다. 컨트롤러 노드가 실패해도 데이터부 트래픽에는 영향을 미치지 않습니다.

NSX CONTROLLER는 네트워크 정보를 호스트로 분산하는 방식으로 작동합니다. 높은 수준의 복원력을 달성할 수 있도록 NSX Controller는 스케일 아웃과 HA를 위해 클러스터링됩니다. NSX CONTROLLER를 3노드 클러스터에 배포해야 합니다. 세 개의 가상 장치는 NSX 도메인 내에서 작동하는 모든 네트워크의 상태를 제공, 유지 및 업데이트합니다. NSX Manager는 NSX Controller 노드를 배포하는 데 사용됩니다.

세 개의 NSX Controller 노드가 하나의 컨트롤러 클러스터를 구성합니다. "분할 브레인" 시나리오를 방지하려면 컨트롤러 클러스터에 쿼럼(과반수라고도 함)이 필요합니다. 분할 브레인 시나리오에서는 서로 겹치는 두 데이터 집합의 유지 보수로 인해 데이터 불일치가 발생합니다. 이러한 불일치는 실패 상태 및 데이터 동기화 문제로 인해 야기될 수 있습니다. 컨트롤러 노드를 세 개 사용할 경우 NSX Controller 노드 중 하나가 실패해도 데이터 중복성이 보장됩니다.

컨트롤러 클러스터에는 다음을 포함한 몇 가지 역할이 있습니다.

- API 제공자
- 지속성 서버
- 스위치 관리자
- 논리적 관리자
- 디렉토리 서버

각 역할에는 마스터 컨트롤러 노드가 있습니다. 특정 역할의 마스터 컨트롤러 노드가 실패하면 클러스터는 사용 가능한 NSX Controller 노드 중에서 해당 역할의 새로운 마스터를 선택합니다. 해당 역할의 새 마스터 NSX Controller 노드는 작업의 손실된 부분을 나머지 NSX Controller 노드 간에 재할당합니다.

NSX는 세 가지 논리적 스위치 제어부 모드를 지원하는데, 멀티캐스트, 유니캐스트 및 하이브리드입니다. 컨트롤러 클러스터를 사용하여 VXLAN 기반 논리적 스위치를 관리할 경우 물리적 네트워크 인프라에서 멀티캐스트를 지원할 필요가 없습니다. 멀티캐스트 그룹 IP 주소를 제공할 필요가 없고, 물리적 스위치 또는 라우터에서 PIM 라우팅 또는 IGMP 스누핑 기능을 사용하도록 설정할 필요가 없습니다. 따라서 유니캐스트 및 하이브리드 모드는 물리적 네트워크에서 NSX를 분리합니다. 유니캐스트 제어부 모드의 VXLAN은 더 이상 물리적 네트워크가 논리적 스위치 내의 BUM(브로드캐스트, 알 수 없는 유니캐스트 및 멀티캐스트) 트래픽을 처리하기 위한 멀티캐스트를 지원하도록 요구하지 않습니다. 유니캐스트 모드에서는 모든 BUM 트래픽을 호스트에서 로컬로 복제하므로 물리적 네트워크 구성이 필요 없습니다. 하이브리드 모드에서는 성능 개선을 위해 일부 BUM 트래픽 복제가 첫 번째 홉 물리적 스위치로 오프로드됩니다. 하이브리드 모드에서는 첫 번째 홉 스위치에서 IGMP 스누핑과 각 VTEP 서브넷의 IGMP 쿼리 발송기에 대한 액세스 권한이 필요합니다.

관리부

NSX 관리부는 NSX의 중앙화된 네트워크 관리 구성 요소인 NSX Manager에 의해 구성됩니다. 여기에서는 단일 구성 지점 및 REST API 진입 지점을 제공합니다.

NSX Manager는 vCenter Server 환경의 모든 ESX™ 호스트에 가상 장치로 설치됩니다. NSX Manager와 vCenter는 일대일 관계에 있습니다. NSX Manager 인스턴스마다 하나의 vCenter Server가 있습니다. 이는 크로스 vCenter NSX 환경에서도 적용됩니다.

크로스 vCenter NSX 환경에는 기본 NSX Manager와 하나 이상의 보조 NSX Manager가 모두 있습니다. 기본 NSX Manager에서는 범용 논리적 스위치, 범용 논리적(분산) 라우터 및 범용 방화벽 규칙을 생성하고 관리할 수 있습니다. 보조 NSX Manager는 해당 NSX Manager의 로컬 네트워킹 서비스를 관리하는 데 사용됩니다. 크로스 vCenter NSX 환경에는 기본 NSX Manager와 연결된 보조 NSX Manager가 최대 7개 있을 수 있습니다.

소비 플랫폼

vSphere Web Client에서 사용할 수 있는 NSX Manager 사용자 인터페이스를 통해 NSX의 소비량을 직접 유도할 수 있습니다. 일반적으로 최종 사용자는 네트워크 가상화를 자신의 Cloud Management Platform에 연결하여 애플리케이션을 배포합니다. NSX는 REST API를 통해 실질적으로 모든 CMP에 다양한 통합을 제공합니다. VMware vCloud Automation Center, vCloud Director 및 NSX용 Neutron 플러그인이 포함된 OpenStack을 통해 기본 제공되는 통합 기능을 사용할 수도 있습니다.

NSX Edge

NSX Edge를 ESG(Edge Services Gateway) 또는 DLR(논리적 분산 라우터)로 설치할 수 있습니다.

Edge Services Gateway

ESG는 방화벽, NAT, DHCP, VPN, 로드 밸런싱 및 고가용성 같은 모든 NSX Edge 서비스에 대해 액세스를 제공합니다. 데이터 센터에 여러 ESG 가상 장치를 설치할 수 있습니다. 각 ESG 가상 장치는 총 10개의 업링크 및 내부 네트워크 인터페이스를 사용할 수 있습니다. 트렁크를 통해 ESG에는 최대 200개의 하위 인터페이스가 있을 수 있습니다. 내부 인터페이스는 보안 포트 그룹에 연결하여 포트 그룹에 있는 모든 보호된 가상 시스템의 게이트웨이 역할을 합니다. 내부 인터페이스에 할당된 서브넷은 라우팅된 공용 IP 공간이거나 NAT가 적용된/라우팅된 RFC 1918 전용 공간일 수 있습니다. 네트워크 인터페이스 간의 트래픽에는 방화벽 규칙 및 기타 NSX Edge 서비스가 적용됩니다.

ESG의 업링크 인터페이스는 업링크 포트 그룹에 연결하여 액세스 계층 네트워킹을 제공하는 서비스나 공유 회사 네트워크에 액세스할 수 있습니다. 로드 밸런서, 사이트 간 VPN 및 NAT 서비스에는 외부 IP 주소를 여러 개 구성할 수 있습니다.

논리적 분산 라우터

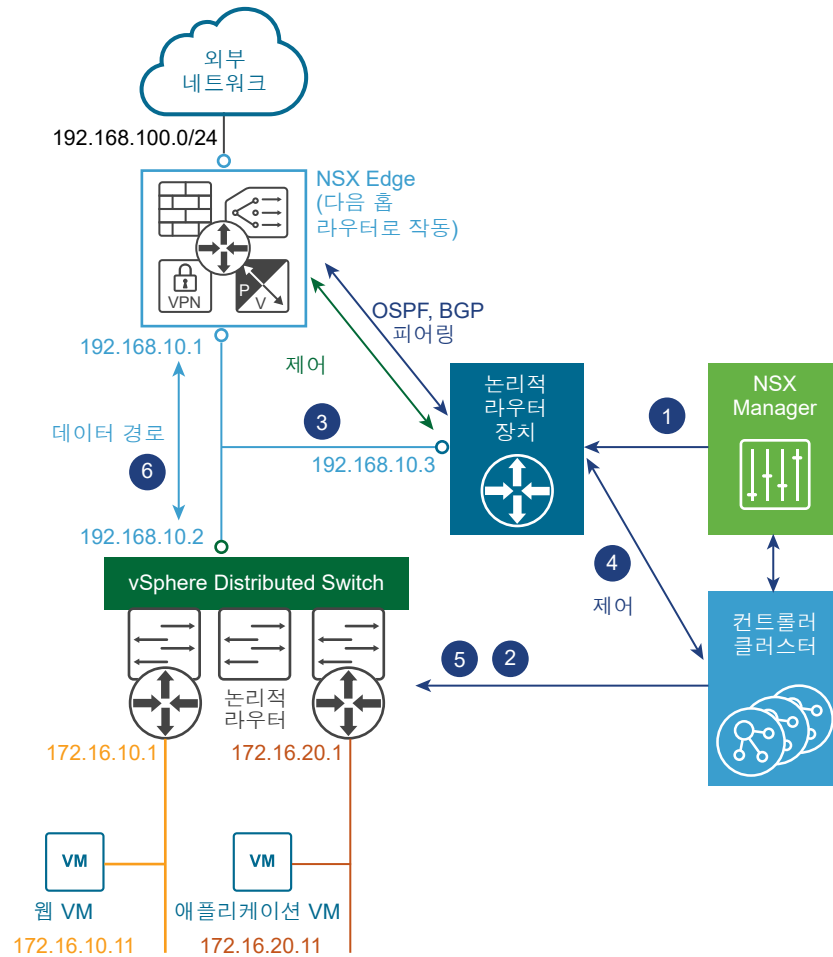
DLR은 테넌트 IP 주소 공간 및 데이터 경로 분리를 지원하는 동-서 분산 라우팅을 제공합니다. 서로 다른 서브넷의 동일한 호스트에 상주하는 가상 시스템 또는 워크로드는 기존 라우팅 인터페이스를 이동하지 않고도 서로 통신할 수 있습니다.

논리적 라우터에는 8개의 업링크 인터페이스와 최대 1,000개의 내부 인터페이스가 있을 수 있습니다. DLR의 업링크 인터페이스는 일반적으로 DLR과 ESG 사이에 개입하는 계층 2 논리적 전송 스위치를 통해, ESG와 피어 관계를 이룹니다. DLR의 내부 인터페이스는 가상 시스템과 DLR 사이에 개입하는 논리적 스위치를 통해, ESXi 하이퍼바이저에 호스트되는 가상 시스템과 피어 관계를 이룹니다.

DLR에는 두 개의 기본 구성 요소가 있습니다.

- DLR 제어부는 DLR 가상 장치에서 제공되며 제어 VM이라고도 합니다. 이 VM은 동적 라우팅 프로토콜(BGP 및 OSPF)을 지원하고 라우팅 업데이트를 다음 계층 3 홉 장치(대개 Edge Services Gateway)와 교환하며 NSX Manager 및 NSX Controller 클러스터와 통신합니다. DLR 가상 장치의 고가용성은 활성-대기 구성을 통해 제공됩니다. 즉, HA를 사용하도록 설정한 DLR을 생성할 경우 활성/대기 모드에서 작동하는 가상 시스템 쌍이 제공됩니다.
- 데이터부 수준에서는 NSX 도메인의 일부인 ESXi 호스트에 설치되는 DLR 커널 모듈(VIB)이 있습니다. 커널 모듈은 계층 3 라우팅을 지원하는 모듈식 새시의 라인 카드와 비슷합니다. 커널 모듈에는 컨트롤러 클러스터에서 푸시되고 라우팅 테이블이라고도 하는 RIB(Routing Information Base)가 있습니다. 경로 조회 및 ARP 항목 조회의 데이터부 기능은 커널 모듈에서 수행됩니다. 커널 모듈에는 다양한 논리적 스위치 및 VLAN 지원 포트 그룹에 연결하는 LIF라는 논리적 인터페이스가 장착되어 있습니다. 각 LIF에는 해당 LIF가 연결하는 논리적 L2 세그먼트의 기본 IP 게이트웨이를 나타내는 IP 주소와 vMAC 주소가 할당되어 있습니다. IP 주소는 LIF별로 고유하지만 모든 정의된 LIF에는 동일한 vMAC가 할당됩니다.

그림 1-1. 논리적 라우팅 구성 요소



- 1 DLR 인스턴스는 NSX Manager UI 또는 API 호출을 통해 생성되고 OSPF 또는 BGP를 사용하여 라우팅이 사용되도록 설정됩니다.
- 2 NSX Controller는 ESXi 호스트와 제어부를 사용하여 LIF 및 연결된 해당 IP 주소와 vMAC 주소를 비롯한 새로운 DLR 구성을 푸시합니다.
- 3 라우팅 프로토콜이 다음 홉 장치(이 예에서는 NSX Edge [ESG])에서도 사용되도록 설정된다고 가정하면 ESG와 DLR 제어 VM 사이에 OSPF 또는 BGP 피어링이 설정됩니다. 그러면 ESG와 DLR이 라우팅 정보를 교환할 수 있습니다.
 - 모든 연결된 논리적 네트워크(이 예에서는 172.16.10.0/24 및 172.16.20.0/24)에 대해 IP 접두사를 OSPF로 재배포하도록 DLR 제어 VM을 구성할 수 있습니다. 그러면 이 VM이 이러한 경로 알림을 NSX Edge에 푸시합니다. 이와 같은 접두사의 다음 홉은 제어 VM에 할당된 IP 주소(192.168.10.3)가 아니지만 DLR의 데이터부 구성 요소를 식별하는 IP 주소(192.168.10.2)입니다. 전자를 DLR "프로토콜 주소"라고 하고 후자를 "전달 주소"라고 합니다.
 - NSX Edge는 제어 VM에 접두사를 푸시하여 외부 네트워크의 IP 네트워크에 연결합니다. 대부분의 경우 NSX Edge에서 단일 기본 경로가 전송되는데, 이 경로는 물리적 네트워크 인프라로의 단일 출구 지점을 나타내기 때문입니다.

- 4 DLR 제어 VM은 NSX Edge에서 얻은 IP 경로를 컨트롤러 클러스터에 푸시합니다.
- 5 컨트롤러 클러스터는 DLR 제어 VM에서 얻은 경로를 하이퍼바이저로 배포합니다. 클러스터의 각 컨트롤러 노드는 특정 논리적 라우터 인스턴스에 대해 정보를 배포합니다. 여러 논리적 라우터 인스턴스가 배포된 배포 환경에서는 컨트롤러 노드 간에 로드가 분산됩니다. 일반적으로 별개의 논리적 라우터 인스턴스가 배포된 각 테넌트와 연결됩니다.
- 6 호스트의 DLR 라우팅 커널 모듈은 NSX Edge를 통한 외부 네트워크와의 통신에 대한 데이터-경로 트래픽을 처리합니다.

NSX Services

NSX 구성 요소는 함께 작동하여 다음의 기능 서비스를 제공합니다.

논리적 스위치

클라우드 배포 환경 또는 가상 데이터센터에는 여러 테넌트에 분산된 다양한 애플리케이션이 있습니다. 이러한 애플리케이션과 테넌트는 보안, 장애 분리 및 겹치지 않는 IP 주소를 위해 서로 분리되어야 합니다.

NSX에서는 각각 하나의 논리적 브로드캐스트 도메인에 해당하는 논리적 스위치를 여러 개 생성할 수 있습니다. 애플리케이션 또는 테넌트 가상 시스템은 논리적 스위치에 논리적으로 연결될 수 있습니다. 이 기능은 배포 유연성과 속도를 향상시킬 뿐 아니라 물리적 계층 2 확장 또는 스페닝 트리 문제 없이 물리적 네트워크의 브로드캐스트 도메인(VLAN)이 가진 모든 특성도 제공합니다.

논리적 스위치는 분산되며 vCenter의 모든 호스트(또는 크로스 vCenter NSX 환경의 모든 호스트)에 분산될 수 있습니다. 이러한 특성은 물리적 계층 2(VLAN) 경계의 제한 없이 데이터센터 내에서 가상 시스템의 이동성(vMotion)을 지원합니다. 소프트웨어의 논리적 스위치에 브로드캐스트 도메인이 포함되므로 물리적 인프라는 MAC/FIB 테이블 제한의 제약을 받지 않습니다.

논리적 라우터

라우팅은 계층 2 브로드캐스트 도메인 간에 필요한 정보 전달 기능을 제공하므로 계층 2 브로드캐스트 도메인의 크기를 줄이고 네트워크 효율성 및 확장성을 개선할 수 있습니다. NSX는 워크로드가 상주하는 위치로 이 인텔리전스 기능을 확장하여 동-서 라우팅을 수행합니다. 따라서 코스트나 시간을 들여 홉을 확장할 필요 없이 가상 시스템 간의 직접적인 통신이 가능합니다. 이와 동시에 NSX 논리적 라우터는 북-남 연결도 제공하므로 테넌트가 공용 네트워크에 액세스할 수 있습니다.

논리적 방화벽

논리적 방화벽은 동적 가상 데이터센터에 대한 보안 메커니즘을 제공합니다. 논리적 방화벽의 분산 방화벽 구성 요소를 이용하면 VM 이름과 특성, 사용자 ID, 데이터센터와 같은 vCenter 개체, 호스트 그리고 IP 주소나 VLAN 등과 같은 전통적 네트워킹 특성에 기반하여 가상 시스템과 같은 가상 데이터센터 엔티티를 분류할 수 있습니다. Edge Firewall 구성 요소는 IP/VLAN 구성에 기반한 DMZ 구성 및 멀티 테넌트 가상 데이터센터에서 테넌트 간 분리와 같은 주요 경계 보안 요구 사항을 충족하는 데 도움이 됩니다.

Flow Monitoring 기능은 애플리케이션 프로토콜 수준에서 가상 시스템 간의 네트워크 작업을 표시합니다. 이 정보를 사용하여 네트워크 트래픽을 감사하고, 방화벽 정책을 정의 및 구체화하며, 네트워크에 대한 위협을 식별할 수 있습니다.

논리적 VPN(Virtual Private Network)

SSL VPN-Plus를 통해 원격 사용자는 회사 전용 애플리케이션에 액세스할 수 있습니다. IPSec VPN은 NSX 또는 타사 벤더의 하드웨어 라우터/VPN 게이트웨이를 사용하여 NSX Edge 인스턴스와 원격 사이트 간에 사이트 대 사이트 연결을 제공합니다. L2 VPN을 사용하면 가상 시스템에서 지리적 경계를 넘어 동일한 IP 주소를 유지하면서 네트워크 연결을 유지할 수 있으므로 데이터센터를 확장할 수 있습니다.

논리적 로드 밸런서

NSX Edge 로드 밸런서는 단일 VIP(가상 IP 주소)로 방향 지정된 클라이언트 연결을 로드 밸런싱 풀의 구성원으로 구성된 여러 대상으로 분산합니다. 즉, 로드 분산이 사용자에게 투명하게 진행되도록 들어오는 서비스 요청을 여러 서버 간에 균일하게 분산합니다. 따라서 로드 밸런싱은 리소스 활용도를 최적화하고, 처리량을 극대화하며, 응답 시간을 최소화하고, 오버로드를 방지하는 데 도움이 됩니다.

Service Composer

Service Composer는 네트워크 및 보안 서비스를 가상 인프라의 애플리케이션에 프로비저닝하고 할당하는 데 도움이 됩니다. 이러한 서비스를 보안 그룹에 매핑하면 보안 정책을 사용하여 보안 그룹의 가상 시스템에 서비스가 적용됩니다.

NSX 확장성

타사 솔루션 제공자는 각자의 솔루션을 NSX 플랫폼에 통합할 수 있으므로 VMware 제품 및 파트너 솔루션 전체에서 통합된 환경을 고객에게 제공할 수 있습니다. 데이터센터 운영자는 복잡한 다중 계층 가상 네트워크를 기본 네트워크 토폴로지 또는 구성 요소와는 상관없이 몇 초 안에 프로비저닝할 수 있습니다.

설치 준비

2

이 섹션에서는 NSX for vSphere의 시스템 요구 사항과 열어 두어야 하는 포트를 설명합니다.

본 장은 다음 항목을 포함합니다.

- NSX의 시스템 요구 사항
- NSX for vSphere에 필요한 포트 및 프로토콜
- NSX와 vSphere Distributed Switch
- 예: vSphere Distributed Switch 작업
- 복제 모드 파악하기
- NSX 설치 워크플로 및 샘플 토폴로지
- 크로스 vCenter NSX 및 고급 연결 모드

NSX의 시스템 요구 사항

NSX를 설치하거나 업그레이드하기 전에 네트워크 구성 및 리소스를 고려합니다. vCenter Server별로 NSX Manager 하나, ESXi™ 호스트별로 Guest Introspection 인스턴스를 하나 설치하고 데이터센터별로 NSX Edge 인스턴스를 여러 개 설치할 수 있습니다.

하드웨어

이 표에는 NSX 장치에 대한 하드웨어 요구 사항이 설명되어 있습니다.

표 2-1. 장치에 대한 하드웨어 요구 사항

장치	메모리	vCPU	디스크 용량
NSX Manager	16GB(더 큰 NSX 배포의 경우 24GB)	4(더 큰 NSX 배포의 경우 8)	60 GB
NSX Controller	4GB	4	28 GB

표 2-1. 장치에 대한 하드웨어 요구 사항 (계속)

장치	메모리	vCPU	디스크 용량
NSX Edge	소형: 512MB	소형: 1	소형, 중형: 584MB 디스크 1개 + 512MB 디스크 1개
	중형: 1GB	중형: 2	
	대형: 2GB	대형: 4	대형: 584MB 디스크 1개 + 512MB 디스크 2개
	초대형: 8GB	초대형: 6	초대형: 584 MB 디스크 1개 + 2 GB 디스크 1개 + 512 MB 디스크 1개
Guest Introspection	2 GB	2	5GB(프로비저닝된 공간: 6.26GB)

일반적인 지침에 따라 NSX 관리 환경에 256개가 넘는 하이퍼바이저 또는 2000개가 넘는 VM이 포함되어 있는 경우 NSX Manager 리소스를 vCPU 8개 및 24GB RAM으로 늘립니다.

특정 크기 조정 세부 정보는 VMware 지원팀에 문의하십시오.

가상 장치에 대한 메모리 및 vCPU 할당을 늘리는 방법에 대한 자세한 내용은 "vSphere 가상 시스템 관리"에서 메모리 리소스 할당 및 가상 CPU의 수 변경을 참조하십시오.

Guest Introspection 장치에 대한 프로비저닝된 공간은 Guest Introspection에 대해 6.26GB로 표시됩니다. 이는 클러스터의 여러 호스트가 스토리지를 공유할 때 vSphere ESX Agent Manager가 빠른 복제를 생성하기 위해 서비스 VM의 스냅샷을 생성하기 때문입니다. ESX Agent Manager를 통해 이 옵션을 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 *ESX Agent Manager* 설명서를 참조하십시오.

네트워크 지연 시간

구성 요소 간 네트워크 지연 시간이 설명된 최대 지연 시간 이하인지 확인해야 합니다.

표 2-2. 구성 요소 간 최대 네트워크 지연 시간

구성 요소	최대 지연 시간
NSX Manager 및 NSX Controller	150ms RTT
NSX Manager 및 ESXi 호스트	150ms RTT
NSX Manager 및 vCenter Server 시스템	150ms RTT
NSX Manager 및 크로스 vCenter NSX 환경의 NSX Manager	150ms RTT
NSX Controller 및 ESXi 호스트	150ms RTT

소프트웨어

최신 상호 운용성 정보는 제품 상호 운용성 매트릭스(http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php)를 참조하십시오.

NSX, vCenter Server 및 ESXi의 권장 버전에 대해서는 업그레이드하려는 NSX 버전에 대한 릴리스 정보를 참조하십시오. 릴리스 정보는 다음 NSX for vSphere 설명서 사이트에서 확인할 수 있습니다. <https://docs.vmware.com/kr/VMware-NSX-for-vSphere/index.html>

NSX Manager가 크로스 vCenter NSX 배포에 참여하려면 다음과 같은 조건이 필요합니다.

구성 요소	버전
NSX Manager	6.2 이상
NSX Controller	6.2 이상
vCenter Server	6.0 이상
ESXi	<ul style="list-style-type: none"> ■ ESXi 6.0 이상 ■ NSX 6.2 이상 VIB를 사용하여 준비된 호스트 클러스터

크로스 vCenter NSX 배포 환경에서 단일 vSphere Web Client를 통해 모든 NSX Manager를 관리하려면 고급 연결 모드에서 vCenter Server를 연결해야 합니다. vCenter Server 및 호스트 관리에서 "" 고급 연결 모드 사용을 참조하십시오.

NSX와의 파트너 솔루션 호환성을 확인하려면 <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>에서 네트워킹 및 보안에 대한 VMware 호환성 가이드를 참조하십시오.

클라이언트 및 사용자 액세스

다음 항목은 NSX 환경을 관리하는 데 필요합니다.

- 정방향 및 역방향 이름 확인. ESXi 호스트를 이름으로 vSphere 인벤토리에 추가한 경우에 필요합니다. 그렇지 않은 경우 NSX Manager는 IP 주소를 확인할 수 없습니다.
- 가상 시스템을 추가하고 가상 시스템의 전원을 켤 수 있는 권한이 필요합니다.
- 가상 시스템 파일을 저장하는 데이터스토어에 대한 액세스 권한과 해당 데이터스토어에 파일을 복사할 계정 사용 권한이 있어야 합니다.
- NSX Manager 사용자 인터페이스에 액세스할 수 있도록 웹 브라우저에서 쿠키를 사용하도록 설정해야 합니다.
- 포트 443은 NSX Manager와 ESXi 호스트, vCenter Server 및 배포할 NSX 장치 간에 열려 있어야 합니다. 이 포트는 배포할 OVF 파일을 ESXi 호스트에 다운로드하는 데 필요합니다.
- 사용 중인 vSphere Web Client 버전에서 지원되는 웹 브라우저. 자세한 내용은 "vCenter Server 및 호스트 관리" 설명서에서 vSphere Web Client 사용을 참조하십시오.

NSX for vSphere에 필요한 포트 및 프로토콜

NSX for vSphere가 올바르게 작동하려면 다음 포트가 열려 있어야 합니다.

참고 크로스 vCenter NSX 환경 및 vCenter Server 시스템이 고급 연결 모드인 경우, vCenter Server 시스템에서 NSX Manager를 관리하려면 각 NSX Manager 장치가 환경의 각 vCenter Server 시스템과 필요로 하는 연결이 되어 있어야 합니다.

표 2-3. NSX for vSphere에 필요한 포트 및 프로토콜

소스	대상	포트	프로토콜	용도	민감도	TLS	인증
클라이언트 PC	NSX Manager	443	TCP	NSX Manager 관리 인터페이스	아니요	예	PAM 인증
클라이언트 PC	NSX Manager	443	TCP	NSX Manager VIB 액세스	아니요	아니요	PAM 인증
ESXi 호스트	vCenter Server	443	TCP	ESXi 호스트 준비	아니요	아니요	
vCenter Server	ESXi 호스트	443	TCP	ESXi 호스트 준비	아니요	아니요	
ESXi 호스트	NSX Manager	5671	TCP	RabbitMQ	아니요	예	RabbitMQ 사용자/암호
ESXi 호스트	NSX Controller	1234	TCP	사용자 월드 에이전트 연결	아니요	예	
NSX Controller	NSX Controller	2878, 2888, 3888	TCP	컨트롤러 클러스터 - 상태 동기화	아니요	예	IPsec
NSX Controller	NSX Controller	7777	TCP	컨트롤러 간 RPC 포트	아니요	예	IPsec
NSX Controller	NSX Controller	30865	TCP	컨트롤러 클러스터 - 상태 동기화	아니요	예	IPsec
NSX Manager	NSX Controller	443	TCP	컨트롤러와 Manager 간 통신	아니요	예	사용자/암호
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	아니요	예	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	아니요	예	
NSX Manager	ESXi 호스트	443	TCP	관리 및 프로비저닝 연결	아니요	예	
NSX Manager	ESXi 호스트	902	TCP	관리 및 프로비저닝 연결	아니요	예	
NSX Manager	DNS 서버	53	TCP	DNS 클라이언트 연결	아니요	아니요	
NSX Manager	DNS 서버	53	UDP	DNS 클라이언트 연결	아니요	아니요	
NSX Manager	Syslog 서버	514	TCP	Syslog 연결	아니요	아니요	
NSX Manager	Syslog 서버	514	UDP	Syslog 연결	아니요	아니요	
NSX Manager	NTP 시간 서버	123	TCP	NTP 클라이언트 연결	아니요	예	
NSX Manager	NTP 시간 서버	123	UDP	NTP 클라이언트 연결	아니요	예	
vCenter Server	NSX Manager	80	TCP	호스트 준비	아니요	예	
REST 클라이언트	NSX Manager	443	TCP	NSX Manager REST API	아니요	예	사용자/암호

표 2-3. NSX for vSphere에 필요한 포트 및 프로토콜 (계속)

소스	대상	포트	프로토콜	용도	민감도	TLS	인증
VTEP(VXLAN Tunnel End Point)	VTEP(VXLAN Tunnel End Point)	8472(NSX 6.2.3 이전의 기본 값) 또는 4789(NSX 6.2.3 이상 새 설치의 기본 값)	UDP	VTEP 간 전송 네트워크 캡슐화	아니요	예	
ESXi 호스트	ESXi 호스트	6999	UDP	VLAN LIF의 ARP	아니요	예	
ESXi 호스트	NSX Manager	8301, 8302	UDP	DVS 동기화	아니요	예	
NSX Manager	ESXi 호스트	8301, 8302	UDP	DVS 동기화	아니요	예	
Guest Introspection VM	NSX Manager	5671	TCP	RabbitMQ	아니요	예	RabbitMQ 사용자/암호
기본 NSX Manager	보조 NSX Manager	443	TCP	크로스 vCenter NSX 범용 동기화 서비스	아니요	예	
기본 NSX Manager	vCenter Server	443	TCP	vSphere API	아니요	예	
보조 NSX Manager	vCenter Server	443	TCP	vSphere API	아니요	예	
기본 NSX Manager	NSX 범용 컨트롤러 클러스터	443	TCP	NSX Controller REST API	아니요	예	사용자/암호
보조 NSX Manager	NSX 범용 컨트롤러 클러스터	443	TCP	NSX Controller REST API	아니요	예	사용자/암호
ESXi 호스트	NSX 범용 컨트롤러 클러스터	1234	TCP	NSX 제어부 프로토콜	아니요	예	
ESXi 호스트	기본 NSX Manager	5671	TCP	RabbitMQ	아니요	예	RabbitMQ 사용자/암호
ESXi 호스트	보조 NSX Manager	5671	TCP	RabbitMQ	아니요	예	RabbitMQ 사용자/암호

NSX와 vSphere Distributed Switch

NSX 도메인에서 NSX vSwitch는 서버와 물리적 네트워크 간에 소프트웨어 추상화 계층을 형성할 수 있도록 서버 하이퍼바이저에서 작동하는 소프트웨어입니다.

NSX vSwitch는 VDS(vSphere Distributed Switch)에 기반하며 ToR(Top-of-Rack) 물리적 스위치에 대한 호스트 연결용 업링크를 제공합니다. 가장 좋은 방법은 NSX for vSphere를 설치하기 전에 vSphere Distributed Switch를 계획하고 준비하는 것입니다.

NSX 서비스는 vSphere Standard Switch에서 지원되지 않습니다. NSX 서비스 및 기능을 사용하려면 VM 워크로드가 vSphere Distributed Switch에 연결되어야 합니다.

단일 호스트를 여러 VDS에 연결할 수 있습니다. 단일 VDS는 여러 클러스터에 있는 여러 호스트에 걸쳐 있을 수 있습니다. NSX에 참여할 각 호스트 클러스터에 대해 클러스터 내의 호스트를 공용 VDS에 연결해야 합니다.

예를 들어 클러스터에 Host1과 Host2가 있다고 가정해 보겠습니다. Host1은 VDS1과 VDS2에 연결되어 있고 Host2는 VDS1과 VDS3에 연결되어 있습니다. NSX에 대한 클러스터를 준비할 때 사용자는 NSX를 클러스터의 VDS1에만 연결할 수 있습니다. 다른 호스트(Host3)를 클러스터에 추가하고 Host3을 VDS1에 연결하지 않으면 구성이 올바르지 않아 Host3에서 NSX 기능을 사용할 수 없게 됩니다.

일부 VDS가 여러 클러스터에 걸쳐 있다 하더라도 호스트의 각 클러스터를 하나의 VDS에만 연결하여 배포를 간소화하는 경우도 있습니다. 예를 들어 사용자의 vCenter에 다음 호스트 클러스터가 있다고 가정합니다.

- 애플리케이션 계층 호스트에 대한 계산 클러스터 A
- 웹 계층 호스트에 대한 계산 클러스터 B
- 관리 및 Edge 호스트에 대한 관리 및 Edge 클러스터

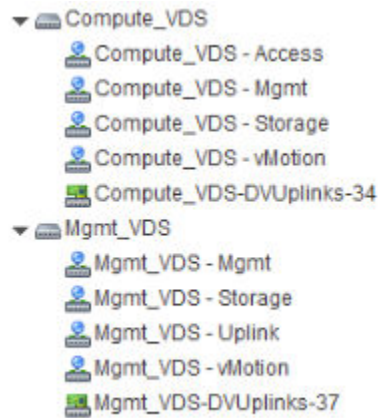
다음 화면은 이러한 클러스터가 vCenter에 어떻게 표시되는지를 보여 줍니다.



이와 같은 클러스터 설계에서는 Compute_VDS와 Mgmt_VDS라고 하는 두 개의 VDS가 있을 수 있습니다. Compute_VDS는 두 개의 계산 클러스터에 걸쳐 있고 Mgmt_VDS는 관리 및 Edge 클러스터에만 연결됩니다.

각 VDS에는 전달할 서로 다른 유형의 트래픽에 대한 분산 포트 그룹이 포함됩니다. 일반적인 트래픽 유형으로는 관리, 스토리지 및 vMotion이 있습니다. 업링크 및 액세스 포트도 일반적으로 필요합니다. 보통은 각 VDS에 트래픽 유형별로 하나의 포트 그룹이 생성됩니다.

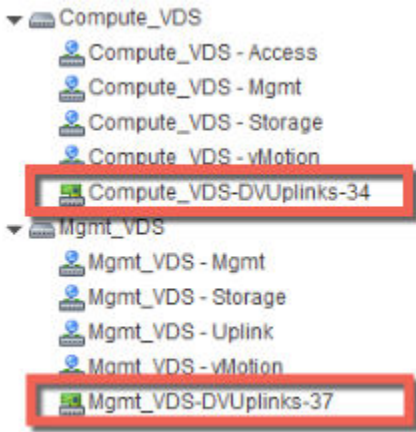
예를 들어 다음 화면은 이러한 **Distributed Switch**와 포트가 **vCenter**에 어떻게 표시되는지를 보여 줍니다.



필요할 경우 각 포트 그룹을 **VLAN ID**로 구성할 수 있습니다. 다음 목록은 **VLAN**을 분산 포트 그룹에 연결하여 서로 다른 트래픽 유형 간에 논리적으로 분리하는 방법을 보여 줍니다.

- Compute_VDS - Access---VLAN 130
- Compute_VDS - Mgmt---VLAN 210
- Compute_VDS - Storage---VLAN 520
- Compute_VDS - vMotion---VLAN 530
- Mgmt_VDS - Uplink---VLAN 100
- Mgmt_VDS - Mgmt---VLAN 110
- Mgmt_VDS - Storage---VLAN 420
- Mgmt_VDS - vMotion---VLAN 430

DVUplinks 포트 그룹은 **VDS**를 생성할 때 자동으로 생성된 **VLAN** 트렁크입니다. 이 포트 그룹은 트렁크 포트로서 태그가 지정된 프레임을 보내고 받으며, 기본적으로 모든 **VLAN ID(0-4094)**를 전달합니다. 즉, **VLAN ID**가 있는 모든 트래픽은 **DVUplink** 슬롯에 연결된 **vmnic** 네트워크 어댑터를 통과할 수 있고 **Distributed Switch**가 트래픽을 수신해야 하는 포트 그룹을 지정하면 하이퍼바이저 호스트에서 필터링될 수 있습니다.



기존 vCenter 환경에 Distributed Switch가 아닌 표준 vSwitch가 포함된 경우 호스트를 Distributed Switch로 마이그레이션할 수 있습니다.

예: vSphere Distributed Switch 작업

이 예에서는 VDS(vSphere Distributed Switch)를 새로 만드는 방법, 관리, 스토리지 및 vMotion 트래픽 유형을 위한 포트 그룹을 만드는 방법 및 표준 vSwitch의 호스트를 새로운 Distributed Switch로 마이그레이션하는 방법을 보여 줍니다.

이는 절차를 보여 주기 위해 사용된 하나의 예일 뿐입니다. VDS의 물리적 및 논리적 업링크에 대한 자세한 고려 사항은 "VMware NSX for vSphere 네트워크 가상화 설계 가이드" (<https://communities.vmware.com/docs/DOC-27683>)를 참조하십시오.

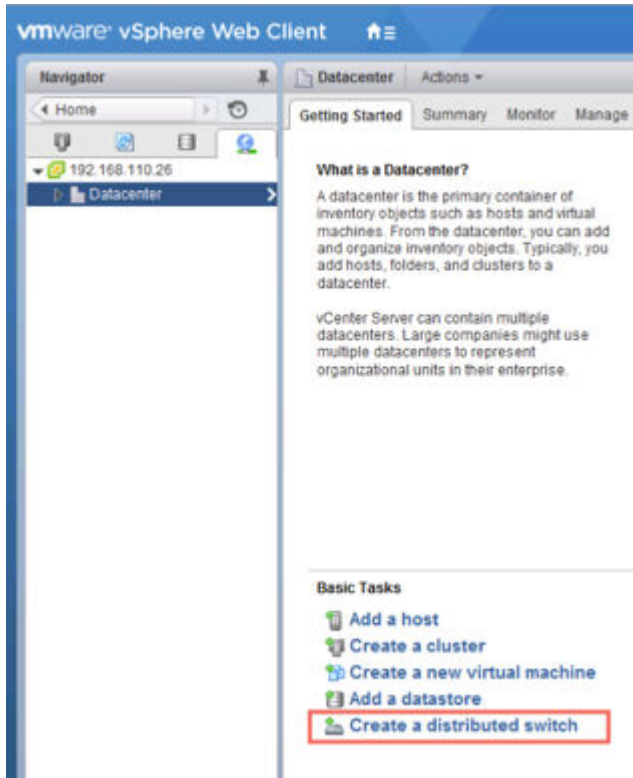
사전 요구 사항

이 예는 새 VDS(vSphere Distributed Switch)를 생성하고 관리, 스토리지 및 vMotion 트래픽 유형에 대한 포트 그룹을 추가하고 표준 vSwitch의 호스트를 새 Distributed Switch로 마이그레이션하는 방법을 보여 줍니다. 이 업링크는 Distributed Switch 및 NSX VXLAN 트래픽에 사용될 수 있습니다.

절차

- 1 vSphere Web Client에서 데이터 센터로 이동합니다.

2 Distributed Switch 생성(Create a Distributed Switch)을 클릭합니다.



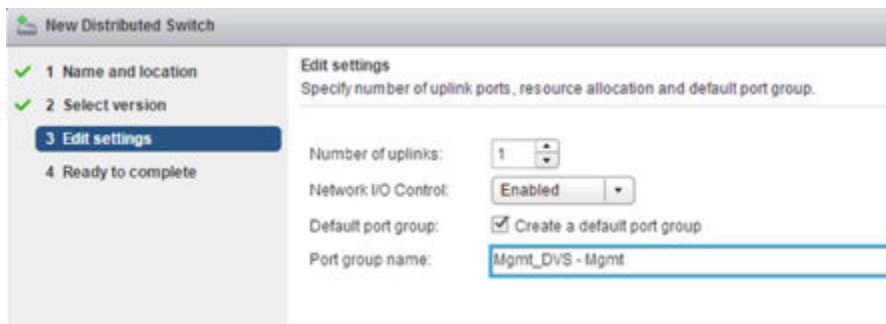
3 이 스위치에 연결할 호스트 클러스터에 따라 스위치에 의미 있는 이름을 지정합니다.

예를 들어 데이터 센터 관리 호스트의 클러스터를 Distributed Switch에 연결하려는 경우 스위치 이름을 VDS_Mgmt로 지정할 수 있습니다.

4 Distributed Switch에 대한 1개 이상의 업링크를 제공하고 IO 제어를 사용하도록 설정한 상태로 유지하며 기본 포트 그룹에 의미 있는 이름을 입력합니다. 기본 포트 그룹 생성은 꼭 필요한 작업은 아닙니다. 나중에 수동으로 포트 그룹을 생성할 수 있습니다.

기본적으로 4개의 업링크가 생성됩니다. VDS 설계에 따라 업링크 수를 조정하십시오. 필요한 업링크 수는 일반적으로 VDS에 할당하는 물리적 NIC의 수와 같습니다.

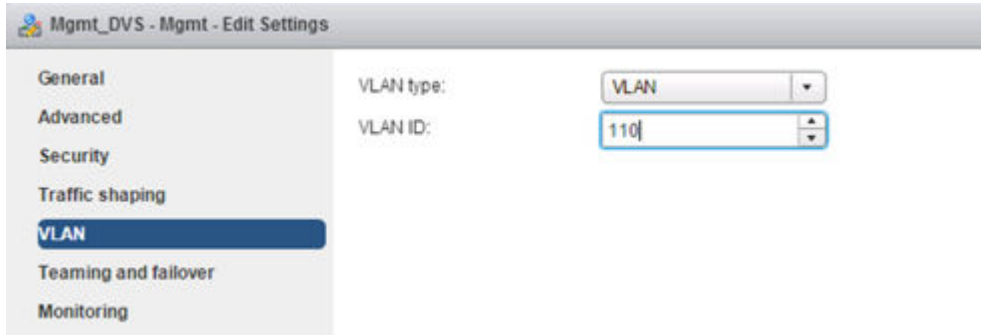
다음 화면은 관리 호스트 클러스터의 관리 트래픽에 대한 설정의 예를 보여 줍니다.



기본 포트 그룹은 이 스위치에 포함될 포트 그룹 중 하나입니다. 스위치를 생성한 후 다른 트래픽 유형에 대한 포트 그룹을 추가할 수 있습니다. 필요한 경우 새 VDS를 생성할 때 **기본 포트 그룹 생성(Create a default port group)** 옵션의 선택을 취소할 수 있습니다. 포트 그룹을 생성할 때는 분명한 것이 좋으므로 사실 이 옵션을 취소하는 것이 모범 사례입니다.

- 5 (선택 사항) 새 Distributed Switch 마법사를 완료한 후 기본 포트 그룹의 설정을 편집하여 관리 트래픽에 대한 올바른 VLAN에 기본 포트 그룹을 배치합니다.

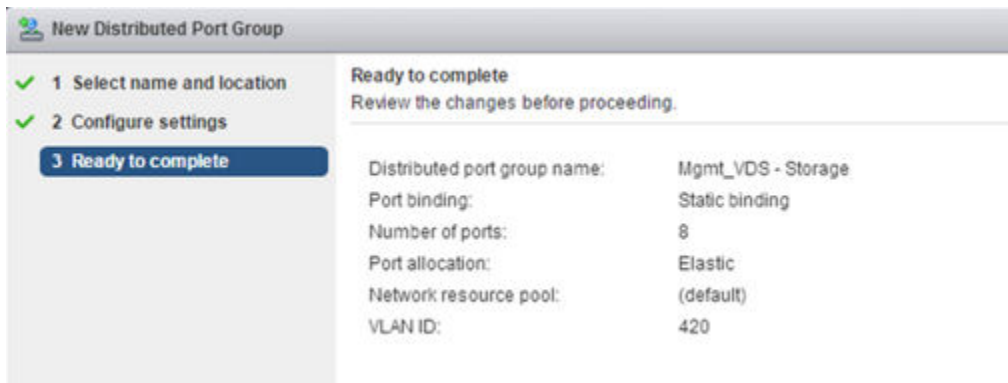
예를 들어 호스트 관리 인터페이스가 VLAN 110에 있는 경우 기본 포트 그룹을 VLAN 110에 배치합니다. 호스트 관리 인터페이스가 VLAN에 없는 경우 이 단계를 건너뛰니다.



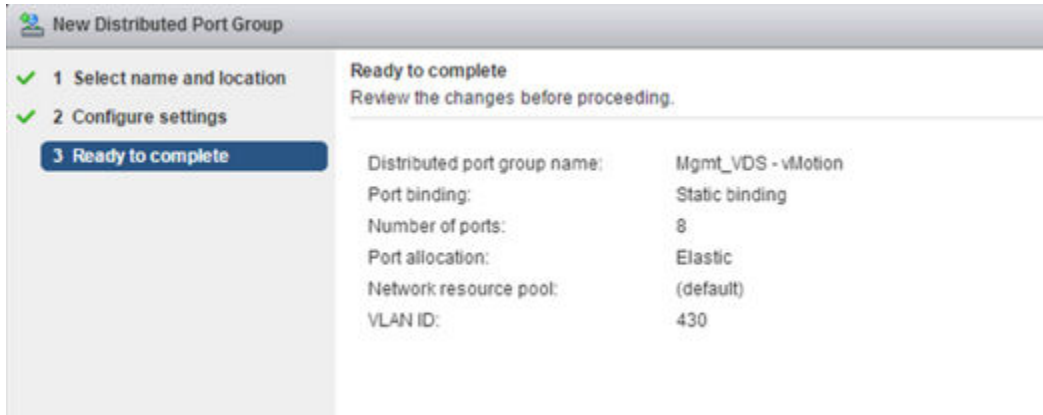
- 6 새 Distributed Switch 마법사를 완료한 후 Distributed Switch를 마우스 오른쪽 버튼으로 클릭하고 **새 분산 포트 그룹(New Distributed Port Group)**을 선택합니다.

각 트래픽 유형에 대해 이 단계를 반복하면서 각 포트 그룹에 의미 있는 이름을 지정하고 사용 중인 배포의 트래픽 분리 요구 사항에 따라 올바른 VLAN ID를 구성합니다.

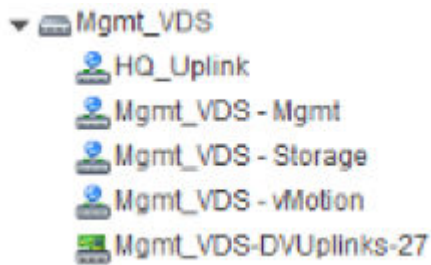
스토리지에 대한 그룹 설정 예입니다.



vMotion 트래픽에 대한 그룹 설정 예입니다.

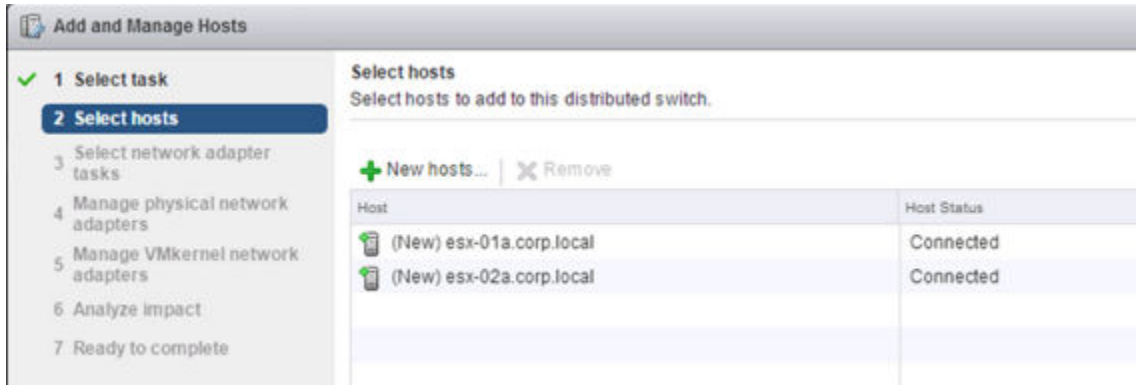


완료된 Distributed Switch와 포트 그룹은 다음과 같이 표시됩니다.

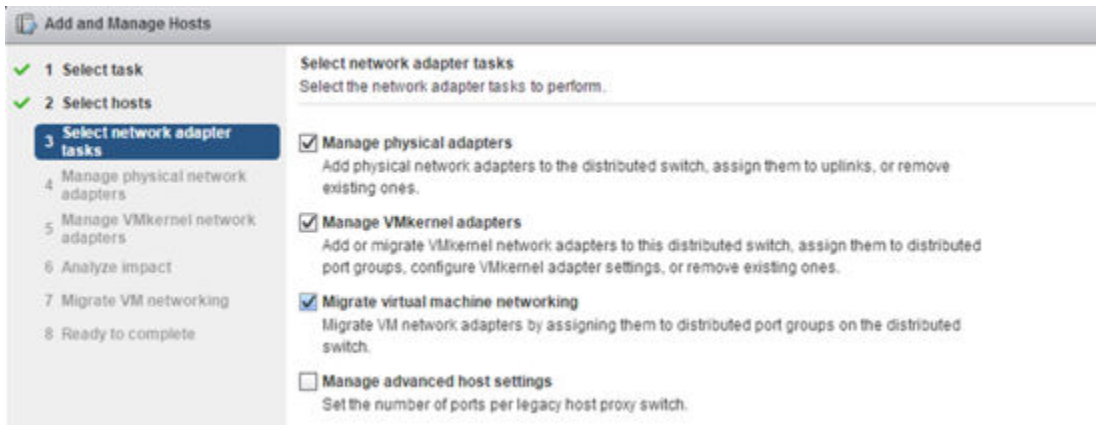


- 7 Distributed Switch를 마우스 오른쪽 버튼으로 클릭하고 **호스트 추가 및 관리(Add and Manage Hosts)**를 선택한 다음 **호스트 추가(Add Hosts)**를 선택합니다.

연결된 클러스터에 있는 모든 호스트를 연결합니다. 예를 들어 해당 Distributed Switch가 관리 호스트에 대한 스위치인 경우 관리 클러스터에 있는 모든 호스트를 선택합니다.

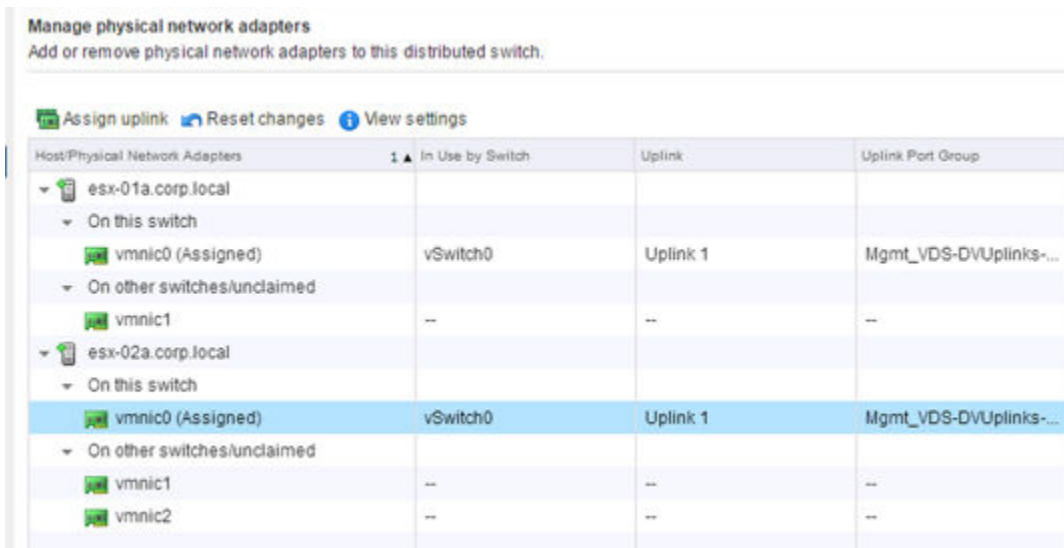


- 8 물리적 어댑터, VMkernel 어댑터 및 가상 시스템 네트워킹을 마이그레이션하는 옵션을 선택합니다.



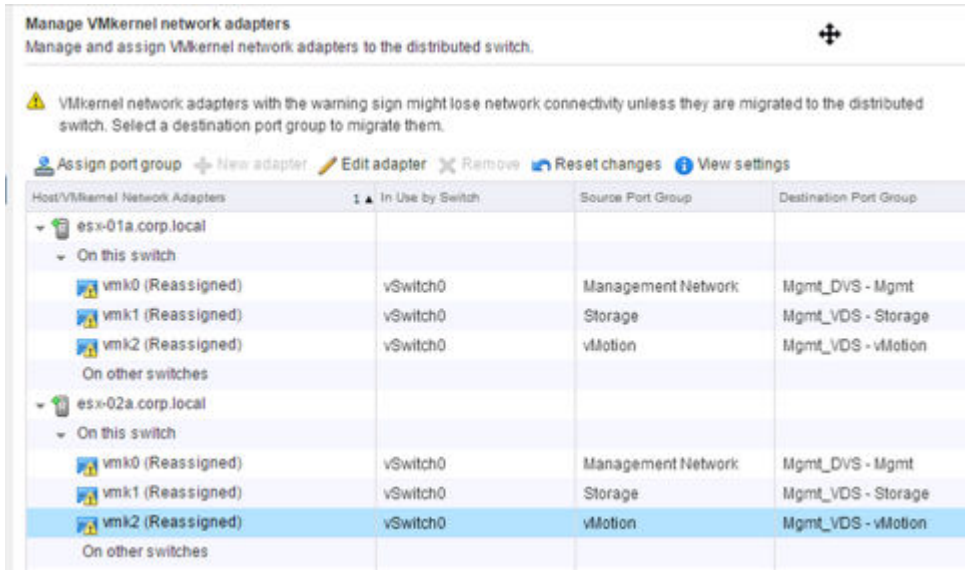
- 9 vmnic를 선택하고 **업링크 할당(Assign uplink)**을 클릭하여 표준 vSwitch의 vmnic을 Distributed Switch로 마이그레이션합니다. 분산 vSwitch에 연결하는 각 호스트에 대해 이 단계를 반복합니다.

예를 들어 이 화면에서는 호스트 2개의 vmnic0 업링크가 각각의 표준 vSwitch에서 분산된 Mgmt_VDS-DVUplinks 포트 그룹(모든 VLAN ID를 전달할 수 있는 트렁크 포트)으로 마이그레이션되도록 구성되어 있습니다.



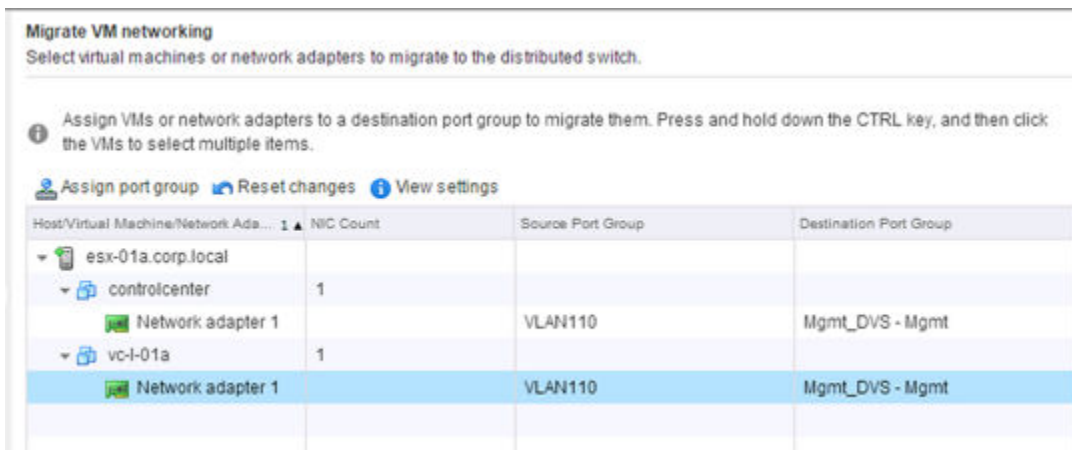
- 10 VMkernel 네트워크 어댑터를 선택하고 **포트 그룹 할당(Assign port group)**을 클릭합니다. 분산 vSwitch에 연결하는 모든 호스트의 모든 네트워크 어댑터에 대해 이 단계를 반복합니다.

예를 들어 이 화면에서는 호스트 2개에 있는 vmk 네트워크 어댑터 3개가 표준 포트 그룹에서 새 분산 포트 그룹으로 마이그레이션되도록 구성되어 있습니다.



11 호스트에 있는 모든 VM을 분산 포트 그룹으로 이동합니다.

예를 들어 이 화면에서는 호스트 1개에 있는 VM 2개가 표준 포트 그룹에서 새 분산 포트 그룹으로 마이그레이션되도록 구성되었습니다.



결과

절차가 완료되면 호스트 CLI에서 다음 명령을 실행하여 결과를 확인할 수 있습니다.

```

■ ~ # esxcli network vswitch dvs vmware list
Mgmt_VDS
  Name: Mgmt_VDS
  VDS ID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
  Class: etherswitch
  Num Ports: 1862
  Used Ports: 5
  Configured Ports: 512
  MTU: 1600
  CDP Status: listen
  Beacon Timeout: -1
  Uplinks: vmnic0

```

```

VMware Branded: true
DVPort:
    Client: vmnic0
    DVPortgroup ID: dvportgroup-306
    In Use: true
    Port ID: 24

    Client: vmk0
    DVPortgroup ID: dvportgroup-307
    In Use: true
    Port ID: 0

    Client: vmk2
    DVPortgroup ID: dvportgroup-309
    In Use: true
    Port ID: 17

    Client: vmk1
    DVPortgroup ID: dvportgroup-308
    In Use: true
    Port ID: 9

```

```

■ ~ # esxcli network ip interface list
vmk2
    Name: vmk2
    MAC Address: 00:50:56:6f:2f:26
    Enabled: true
    Portset: DvsPortset-0
    Portgroup: N/A
    Netstack Instance: defaultTcpipStack
    VDS Name: Mgmt_VDS
    VDS UUID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
    VDS Port: 16
    VDS Connection: 1235399406
    MTU: 1500
    TSO MSS: 65535
    Port ID: 50331650

vmk0
    Name: vmk0
    MAC Address: 54:9f:35:0b:dd:1a
    Enabled: true
    Portset: DvsPortset-0
    Portgroup: N/A
    Netstack Instance: defaultTcpipStack
    VDS Name: Mgmt_VDS
    VDS UUID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
    VDS Port: 2
    VDS Connection: 1235725173
    MTU: 1500
    TSO MSS: 65535
    Port ID: 50331651

vmk1
    Name: vmk1

```

```

MAC Address: 00:50:56:6e:a4:53
Enabled: true
Portset: DvsPortset-0
Portgroup: N/A
Netstack Instance: defaultTcpipStack
VDS Name: Mgmt_VDS
VDS UUID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
VDS Port: 8
VDS Connection: 1236595869
MTU: 1500
TSO MSS: 65535
Port ID: 50331652

```

다음에 수행할 작업

모든 vSphere Distributed Switch에 대해 마이그레이션 프로세스를 반복합니다.

복제 모드 파악하기

전송 영역 또는 논리적 스위치를 생성하려면 복제 모드를 선택해야 합니다. 다양한 모드를 파악해 두면 사용 중인 환경에 가장 적합한 모드를 결정할 수 있습니다.

NSX용으로 마련된 각 ESXi 호스트는 VTEP(VXLAN 터널 엔드포인트)로 구성됩니다. 각 VXLAN 터널 엔드포인트에는 IP 주소가 할당되어 있습니다. 이러한 IP 주소는 동일한 서브넷에서 이용하거나 여러 서브넷에서 이용할 수 있습니다.

여러 ESXi 호스트에 있는 두 VM이 직접 통신하면 두 VTEP IP 주소 간에 플러딩할 필요 없이 유니캐스트 캡슐화 트래픽이 교환됩니다. 그러나 다른 계층 2 네트워크와 마찬가지로, VM의 트래픽을 플러딩하거나 동일한 논리적 스위치에 속한 기타 모든 VM으로 전송해야 하는 경우도 있습니다. 계층 2 브로드캐스트, 알 수 없는 유니캐스트 및 멀티캐스트 트래픽을 통틀어 BUM 트래픽이라고 합니다. 지정된 호스트의 VM에서 발생한 BUM 트래픽은 VM이 동일한 논리적 스위치에 연결되어 있는 다른 모든 호스트로 복제되어야 합니다. NSX for vSphere는 다음 세 가지 다른 복제 모드를 지원합니다.

- 유니캐스트 복제 모드
- 멀티캐스트 복제 모드
- 하이브리드 복제 모드

복제 모드의 요약

표 2-4. 복제 모드의 요약

복제 모드	동일한 서브넷의 VTEP에 대한 BUM 복제 방법	다른 서브넷의 VTEP에 대한 BUM 복제 방법	물리적 네트워크 요구 사항
유니캐스트	유니캐스트	유니캐스트	<ul style="list-style-type: none"> ■ VTEP 서브넷 간 라우팅
멀티캐스트	계층 2 멀티캐스트	계층 3 멀티캐스트	<ul style="list-style-type: none"> ■ VTEP 서브넷 간 라우팅 ■ 계층 2 멀티캐스트, IGMP ■ 계층 3 멀티캐스트, PIM ■ 논리적 스위치에 멀티캐스트 그룹 할당
하이브리드	계층 2 멀티캐스트	유니캐스트	<ul style="list-style-type: none"> ■ VTEP 서브넷 간 라우팅 ■ 계층 2 멀티캐스트, IGMP

유니캐스트 복제 모드

유니캐스트 복제 모드를 사용하면 논리적 스위치 내의 **BUM** 트래픽을 처리하기 위해 물리적 네트워크에서 계층 2 또는 계층 3 멀티캐스트를 지원할 필요가 없습니다. 유니캐스트 모드를 사용하면 물리적 네트워크에서 논리적 네트워크가 완전히 분리됩니다. 유니캐스트 모드는 소스 호스트에서 로컬로 모든 **BUM** 트래픽을 복제하고 유니캐스트 패킷의 **BUM** 트래픽을 원격 호스트로 전달합니다. 유니캐스트 모드에서는 모든 **VTEP**를 하나의 서브넷에 두거나 여러 서브넷에 둘 수 있습니다.

단일 서브넷 시나리오: 모든 호스트 **VTEP** 인터페이스가 단일 서브넷에 속하는 경우 소스 **VTEP**는 모든 원격 **VTEP**에 **BUM** 트래픽을 전달합니다. 이를 헤드-엔드 복제라고 합니다. 헤드-엔드 복제는 원치 않는 호스트 오버헤드를 일으키고 대역폭 사용을 늘릴 수 있습니다. 그 영향은 **BUM** 트래픽의 양과 서브넷 내의 호스트 및 **VTEP** 수에 따라 달라집니다.

다중 서브넷 시나리오: 호스트 **VTEP** 인터페이스가 여러 IP 서브넷으로 그룹화된 경우 소스 호스트는 **BUM** 트래픽을 두 부분으로 처리합니다. 소스 **VTEP**는 동일한 서브넷의 각 **VTEP**에 **BUM** 트래픽을 전달합니다 (단일 서브넷 시나리오와 동일함). 원격 서브넷의 **VTEP**의 경우 소스 **VTEP**는 각 원격 **VTEP** 서브넷에 있는 하나의 호스트에 **BUM** 트래픽을 전달하고, 이 패킷을 로컬 복제용으로 표시하기 위해 복제 비트를 설정합니다. 원격 서브넷의 호스트가 이 패킷을 수신하고 복제 비트 집합을 찾으면, 논리적 스위치가 있는 해당 서브넷의 다른 모든 **VTEP**로 패킷을 전송합니다.

따라서 많은 **VTEP IP** 서브넷이 있는 네트워크 아키텍처에서는 로드가 여러 호스트에 분산되므로 유니캐스트 복제 모드가 원활하게 확장됩니다.

멀티캐스트 복제 모드

멀티캐스트 복제 모드를 사용하려면 물리적 인프라에서 계층 3 및 계층 2 멀티캐스트 모두를 사용하도록 설정해야 합니다. 네트워크 관리자는 멀티캐스트 모드를 구성하기 위해 각 논리적 스위치를 IP 멀티캐스트 그룹에 연결합니다. 특정 논리적 스위치에서 VM을 호스팅하는 ESXi 호스트의 경우 연결된 VTEP는 IGMP를 사용하여 멀티캐스트 그룹에 연결합니다. 라우터는 IGMP 연결을 추적하고 멀티캐스트 라우팅 프로토콜을 사용하여 해당 연결 간에 멀티캐스트 분산 트리를 생성합니다.

호스트는 동일한 IP 서브넷의 VTEP에 BUM 트래픽을 복제할 때 계층 2 멀티캐스트를 사용합니다. 호스트는 다른 IP 서브넷의 VTEP에 BUM 트래픽을 복제할 때 계층 3 멀티캐스트를 사용합니다. 두 경우 모두 원격 VTEP에 대한 BUM 트래픽 복제 작업을 물리적 인프라에서 처리합니다.

IP 멀티캐스트는 잘 알려진 기술이지만 데이터 센터의 IP 멀티캐스트 배포는 종종 다른 기술, 운영 또는 관리상의 이유로 인해 장애물로 간주되는 경우가 많습니다. 네트워크 관리자가 논리적 스위치와 멀티캐스트 그룹 간에 일대일 매핑을 사용하도록 설정하려면 물리적 인프라에서 지원하는 최대 멀티캐스트 상태에 유의해야 합니다. 가상화의 이점 중 하나는 추가 상태를 물리적 인프라에 노출하지 않으면서 가상 인프라로 확장할 수 있다는 것입니다. "물리적" 멀티캐스트 그룹으로 논리적 스위치를 매핑하면 이 모델이 손상됩니다.

참고 멀티캐스트 복제 모드에서는 NSX Controller 클러스터가 논리적 스위칭에 사용되지 않습니다.

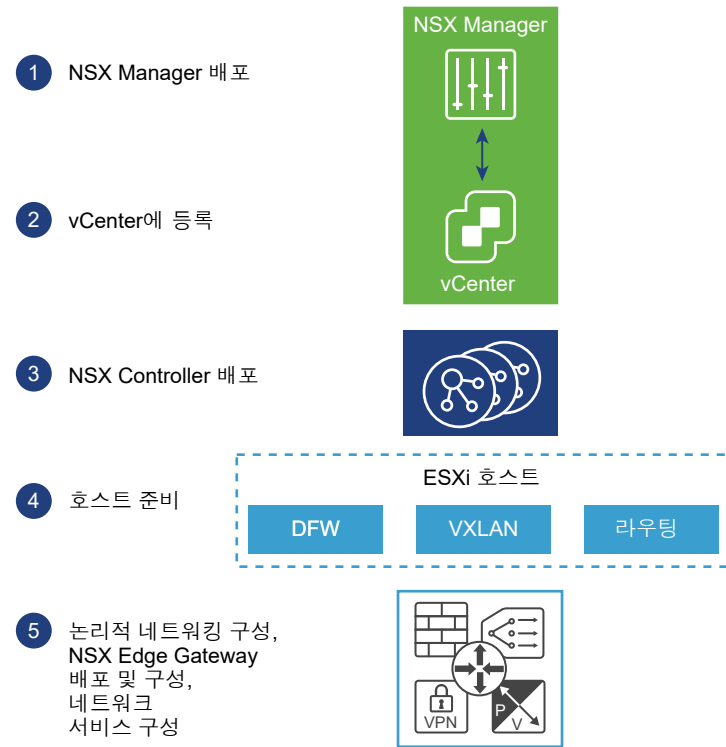
하이브리드 복제 모드

하이브리드 모드는 유니캐스트 및 멀티캐스트 복제 모드를 모두 사용할 수 있는 모드입니다. 하이브리드 복제 모드에서 호스트 VTEP는 계층 2 멀티캐스트를 사용하여 동일한 서브넷의 피어 VTEP로 BUM 트래픽을 분산합니다. 호스트 VTEP는 다른 서브넷의 VTEP로 BUM 트래픽을 복제할 때 VTEP 서브넷당 하나의 호스트에 유니캐스트 패킷으로 트래픽을 전달합니다. 그러면 트래픽을 수신하는 호스트가 계층 2 멀티캐스트를 사용하여 해당 서브넷의 다른 VTEP로 패킷을 전송합니다.

계층 2 멀티캐스트는 일반적으로 배포하기 쉽다는 특성 때문에 계층 3 멀티캐스트보다 고객 네트워크에서 더 많이 사용됩니다. 동일한 서브넷에 있는 여러 VTEP로의 복제는 물리적 네트워크에서 처리됩니다. 동일한 서브넷에 많은 피어 VTEP가 있는 경우 하이브리드 복제를 사용하면 소스 호스트의 BUM 트래픽을 획기적으로 줄일 수 있습니다. 하이브리드 복제를 사용하면 세분화를 거의 또는 전혀 거치지 않고 고밀도 환경으로 확장할 수 있습니다.

NSX 설치 워크플로 및 샘플 토폴로지

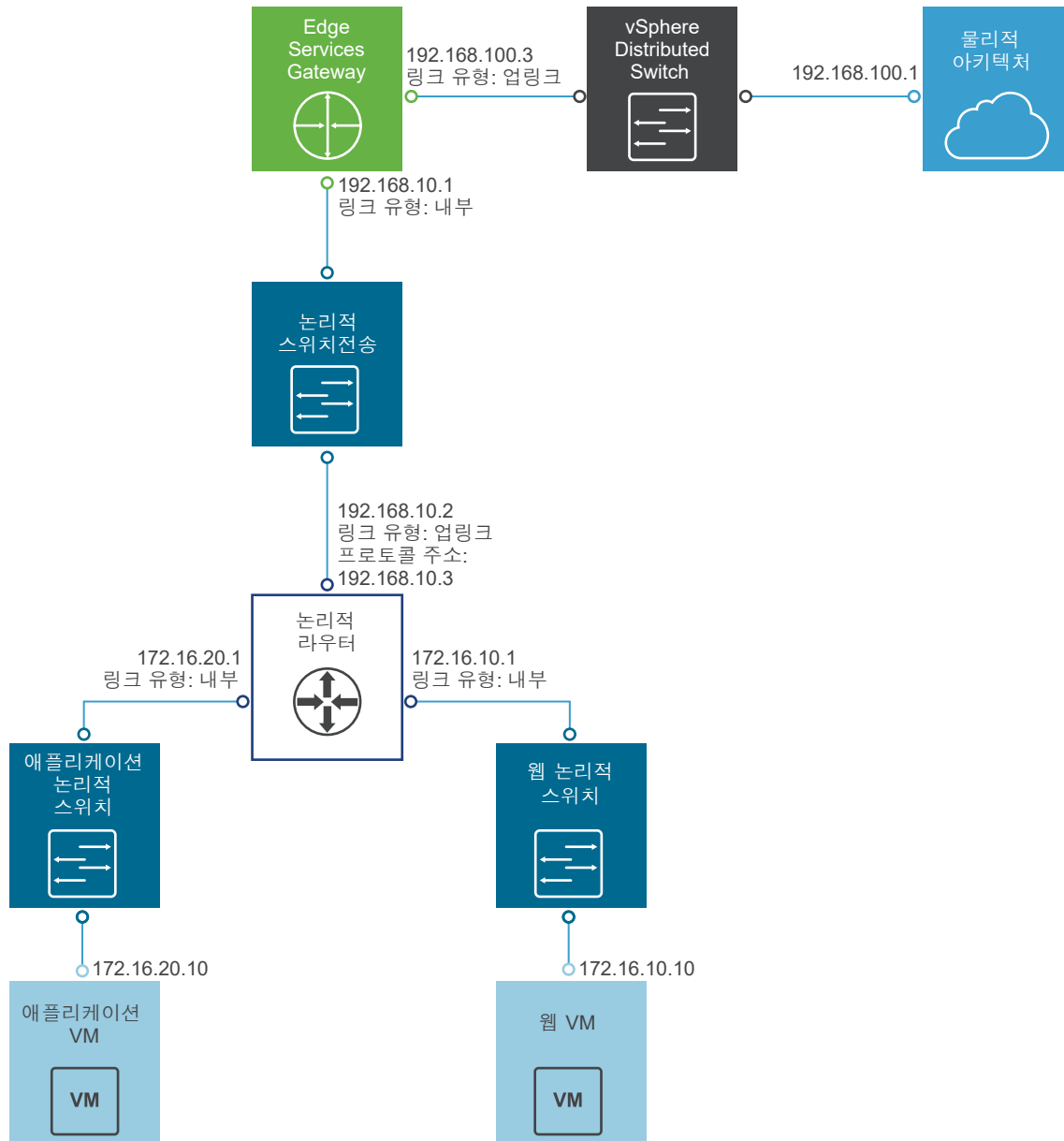
NSX 설치에는 여러 가상 장치의 배포, 몇 가지 ESX 호스트 준비 사항 및 물리적 장치와 가상 장치 전체의 통신을 가능하게 하는 몇 가지 구성 작업이 포함됩니다.



설치 프로세스는 먼저 **NSX Manager OVF/OVA** 템플릿을 배포하고 **NSX Manager**가 관리 대상 **ESX** 호스트의 관리 인터페이스에 연결할 수 있는지 확인하는 것으로 시작합니다. 그 후에는 **NSX Manager**와 **vCenter** 인스턴스를 등록 프로세스를 통해 서로 연결해야 합니다. 그런 다음 **NSX CONTROLLER**의 클러스터를 배포할 수 있습니다. **NSX CONTROLLER**는 **NSX Manager**와 마찬가지로 **ESX** 호스트에서 가상 장치로 실행됩니다. 다음 단계는 **NSX**가 작동할 수 있도록 **ESX** 호스트에 여러 **VIB**를 설치하여 **ESX** 호스트를 준비하는 것입니다. 이러한 **VIB**는 계층 2 **VXLAN** 기능, 분산 라우팅 및 분산 방화벽을 사용할 수 있도록 설정합니다. **VXLAN**을 구성하고, **VNI**(가상 네트워크 인터페이스) 범위를 지정하고, 전송 영역을 생성한 후에 **NSX** 오버레이 토폴로지를 구축할 수 있습니다.

이 설치 가이드에서는 설치 프로세스의 각 단계를 자세히 설명합니다.

이 가이드는 모든 **NSX** 배포 환경에 적용할 수 있지만 연습, 지침 및 참조용으로 사용할 수 있는 샘플 **NSX** 오버레이 토폴로지를 생성하는 과정도 안내합니다. 샘플 오버레이에는 단일 **NSX** 논리적 분산 라우터(**DLR**이라고도 함), **ESG**(Edge Services Gateway) 및 **NSX** 라우팅 디바이스 2개에 연결되는 **NSX** 논리적 전송 스위치가 포함됩니다. 샘플 토폴로지에는 샘플 가상 시스템 2개를 포함하여 언더레이 요소도 포함됩니다. 이 두 가상 시스템은 각각 **NSX** 논리적 라우터(**DLR**)를 통한 연결을 가능하게 하는 개별적인 **NSX** 논리적 스위치에 연결됩니다.



크로스 vCenter NSX 및 고급 연결 모드

vSphere 6.0에는 하나 이상의 Platform Services Controller를 사용하여 여러 vCenter Server 시스템을 연결하는 고급 연결 모드가 도입되었습니다. 이 기능을 통해 vSphere Web Client 내에서 연결된 모든 vCenter Server 시스템의 인벤토리를 보고 검색할 수 있습니다. 크로스 vCenter NSX 환경에서 고급 연결 모드를 사용하여 단일 vSphere Web Client에서 모든 NSX Manager를 관리할 수 있습니다.

vCenter Server가 여러 개 있는 대규모 배포에서 vCenter에 크로스 vCenter NSX와 고급 연결 모드를 사용하는 것이 적절할 수 있습니다. 이 두 기능은 상호 보완적이지만 서로 별개입니다.

고급 연결 모드와 함께 크로스 vCenter NSX 사용

크로스 vCenter NSX에서 기본 NSX Manager와 여러 보조 NSX Manager를 사용할 수 있습니다. 이와 같은 각각의 NSX Manager는 별개의 vCenter Server에 연결됩니다. 기본 NSX Manager에서 범용 NSX 구성 요소(예: 스위치 및 라우터)를 생성하면 보조 NSX Manager에서 볼 수가 있습니다.

개별 vCenter Server가 고급 연결 모드로 배포되면 단일 창이라고도 하는 단일 vCenter Server에서 모든 vCenter Server를 보고 관리할 수 있습니다.

따라서 vCenter에 대해 크로스 vCenter NSX와 고급 연결 모드를 결합하면 연결된 vCenter Server에서 NSX Manager 및 모든 범용 NSX 구성 요소를 보고 관리할 수 있습니다.

고급 연결 모드 없이 크로스 vCenter NSX 사용

고급 연결 모드는 크로스 vCenter NSX를 위한 사전 요구 사항이 아닙니다. 고급 연결 모드를 사용하지 않는 경우 크로스 vCenter 범용 전송 영역, 범용 스위치, 범용 라우터 및 범용 방화벽 규칙을 만들 수 있습니다. 하지만 고급 연결 모드가 없을 경우 각 NSX Manager 인스턴스에 액세스하려면 개별 vCenter Server에 로그인해야 합니다.

vSphere 및 고급 연결 모드에 대한 추가 정보

고급 연결 모드를 사용하려는 경우 "vSphere 설치 및 설정 가이드" 또는 "vSphere 업그레이드 가이드"에서 vSphere 및 고급 연결 모드에 대한 최신 요구 사항을 참조하십시오.

NSX Manager 가상 장치 설치

3

NSX Manager는 vCenter 환경의 모든 ESX 호스트에 가상 장치로 설치됩니다.

NSX Manager는 컨트롤러, 논리적 스위치 및 Edge Services Gateway와 같은 NSX 구성 요소의 생성, 구성 및 모니터링을 위한 GUI(그래픽 사용자 인터페이스) 및 REST API를 제공합니다. 시스템에 대한 종합적인 정보를 제공하는 NSX Manager는 NSX의 중앙 집중식 네트워크 관리 구성 요소입니다. NSX Manager 가상 시스템은 OVA 파일로 패키징되므로 vSphere Web Client를 사용하여 NSX Manager를 데이터스토어 및 가상 시스템 인벤토리로 가져올 수 있습니다.

고가용성을 보장하려면 NSX Manager를 HA 및 DRS로 구성된 클러스터에 배포하는 것이 좋습니다. 필요한 경우 NSX Manager와 상호 운용할 vCenter 이외의 다른 vCenter에 NSX Manager를 설치할 수 있습니다. 단일 NSX Manager는 단일 vCenter Server 환경에 서비스를 제공합니다.

크로스 vCenter NSX 설치 환경에서는 각 NSX Manager의 UUID가 고유해야 합니다. OVA 파일에서 배포된 NSX Manager 인스턴스에는 고유한 UUID가 지정됩니다. 템플릿(가상 시스템을 템플릿으로 변환한 경우)에서 배포된 NSX Manager에는 템플릿을 생성할 때 사용된 원래 NSX Manager와 동일한 UUID가 지정되므로 이 두 NSX Manager를 동일한 크로스 vCenter NSX 설치 환경에 사용할 수 없습니다. 다시 말해 각 NSX Manager에 대해 이 절차에 요약된 대로 새 장치를 처음부터 설치해야 합니다.

NSX Manager 가상 시스템 설치에는 VMware Tools가 포함됩니다. NSX Manager에서 VMware Tools를 업그레йд하거나 설치하지 마십시오.

설치 중에 NSX에 대해 CEIP(고객 환경 향상 프로그램)에 참여할 수 있습니다. 프로그램의 참여 또는 해지 방법을 비롯하여 이 프로그램에 대한 자세한 내용은 "NSX 관리 가이드"의 고객 환경 향상 프로그램을 참조하십시오.

사전 요구 사항

- NSX Manager를 설치하기 전에 필요한 포트가 열려 있는지 확인합니다. [NSX for vSphere에 필요한 포트 및 프로토콜](#)을 참조하십시오.
- 데이터스토어가 구성되었고 대상 ESX 호스트에서 액세스할 수 있는지 확인합니다. 공유 스토리지를 사용하는 것이 좋습니다. HA를 보장하려면 공유 스토리지가 필요합니다. 그래야 원래 호스트에 장애가 발생할 경우 다른 호스트에서 NSX Manager 장치를 다시 시작할 수 있습니다.
- NSX Manager에서 사용할 IP 주소/게이트웨이, DNS 서버 IP 주소, 도메인 검색 목록 및 NTP 서버 IP 주소를 알고 있는지 확인하십시오.

- NSX Manager에서 IPv4 주소 또는 IPv6 주소만 사용할지, 아니면 이중 스택 네트워크 구성을 사용할지를 결정합니다. NSX Manager의 호스트 이름은 다른 엔터티에 의해 사용됩니다. 따라서 NSX Manager 호스트 이름은 해당 네트워크에서 사용되는 DNS 서버의 올바른 IP 주소에 매핑되어야 합니다.
- NSX Manager에서 통신할 관리 트래픽 분산 포트 그룹을 준비합니다. 예: [vSphere Distributed Switch 작업](#) 항목을 참조하십시오. NSX Guest Introspection 인스턴스에서 NSX Manager 관리 인터페이스, vCenter Server 및 ESXi 호스트 관리 인터페이스에 연결할 수 있어야 합니다.
- 클라이언트 통합 플러그인이 설치되어 있어야 합니다. OVF 템플릿 배포 마법사는 Firefox 웹 브라우저에서 가장 잘 작동합니다. Chrome 웹 브라우저에서는 플러그인이 이미 성공적으로 설치된 경우에도 클라이언트 통합 플러그인 설치에 대한 오류 메시지가 가끔 표시됩니다. 클라이언트 통합 플러그인을 설치하려면
 - a 웹 브라우저를 열고 vSphere Web Client의 URL을 입력합니다.
 - b vSphere Web Client 로그인 페이지의 아래쪽에서 [클라이언트 통합 플러그인 다운로드]를 클릭합니다.

클라이언트 통합 플러그인이 시스템에 이미 설치되어 있으면 플러그인 다운로드 링크가 표시되지 않습니다. 클라이언트 통합 플러그인을 제거하면 vSphere Web Client 로그인 페이지에 플러그인 다운로드 링크가 표시됩니다.

절차

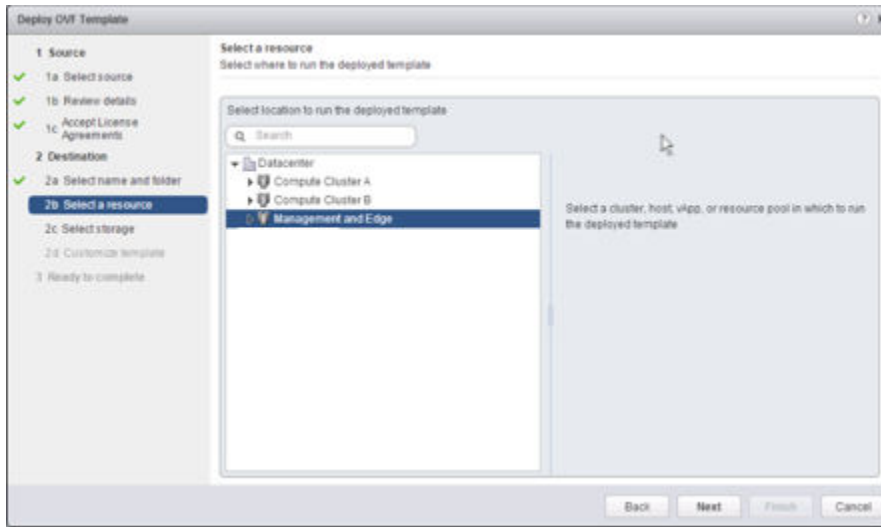
- 1 NSX Manager OVA(Open Virtualization Appliance) 파일을 찾습니다.
다운로드 URL을 복사하거나 OVA 파일을 컴퓨터에 다운로드합니다.
- 2 Firefox에서 vCenter를 엽니다.
- 3 VM 및 템플릿(VMs and Templates)을 선택하고 데이터 센터를 마우스 오른쪽 버튼으로 클릭한 다음 OVF 템플릿 배포(Deploy OVF Template)를 선택합니다.
- 4 다운로드 URL을 붙여 넣거나 **찾아보기(Browse)**를 클릭하여 컴퓨터에서 파일을 선택합니다.

참고 작업 시간 초과 오류로 인해 설치가 실패하면 스토리지 및 네트워크 디바이스에 연결 문제가 있는지 확인하십시오. 이 문제는 물리적 인프라에 스토리지 디바이스와의 연결 끊김 또는 물리적 NIC 또는 스위치의 연결 문제와 같은 문제가 물리적 인프라에 있을 때 발생합니다.

- 5 **추가 구성 옵션 수락(Accept extra configuration options)** 확인란을 선택합니다.
이를 통해 설치 후에 이러한 설정을 수동으로 구성하는 것이 아니라 설치 중에 IPv4 및 IPv6 주소, 기본 게이트웨이, DNS, NTP 및 SSH 속성을 설정할 수 있습니다.
- 6 VMware 라이선스 계약에 동의합니다.
- 7 필요한 경우 NSX Manager 이름을 편집하고 배포된 NSX Manager의 위치를 선택합니다.
입력한 이름이 vCenter 인벤토리에 나타납니다.
선택한 폴더는 NSX Manager에 사용 권한을 적용하는 데 사용됩니다.

8 NSX Manager 장치를 배포할 호스트 또는 클러스터를 선택합니다.

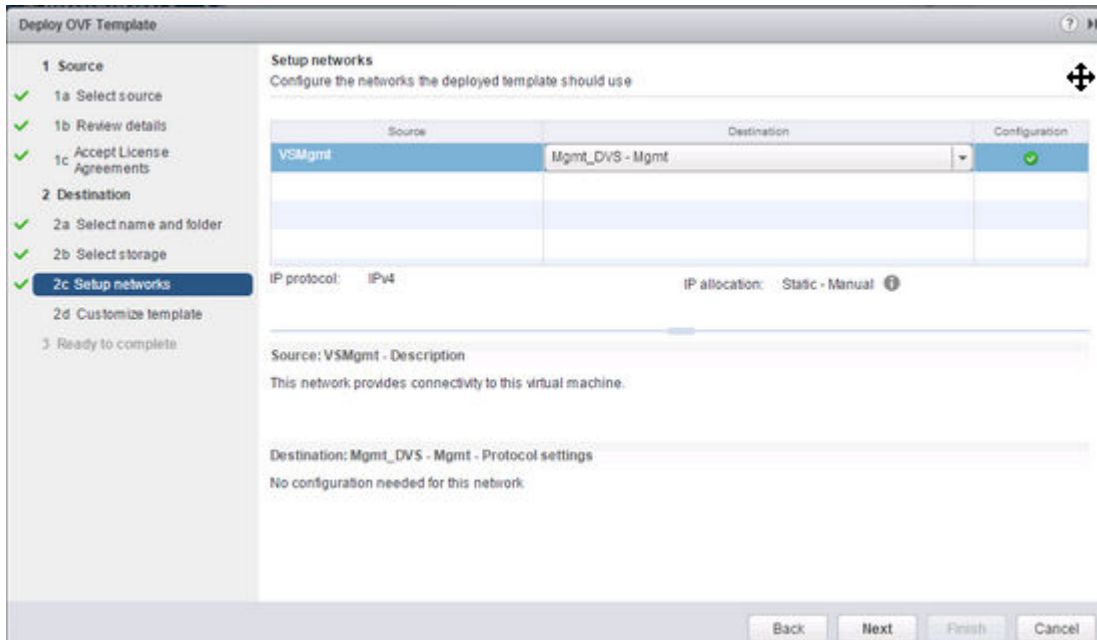
예:



9 가상 디스크 형식을 **썸 프로비저닝(Thick Provision)**으로 변경하고 가상 시스템 구성 파일 및 가상 디스크에 대한 대상 데이터스토어를 선택합니다.

10 NSX Manager에 대한 포트 그룹을 선택합니다.

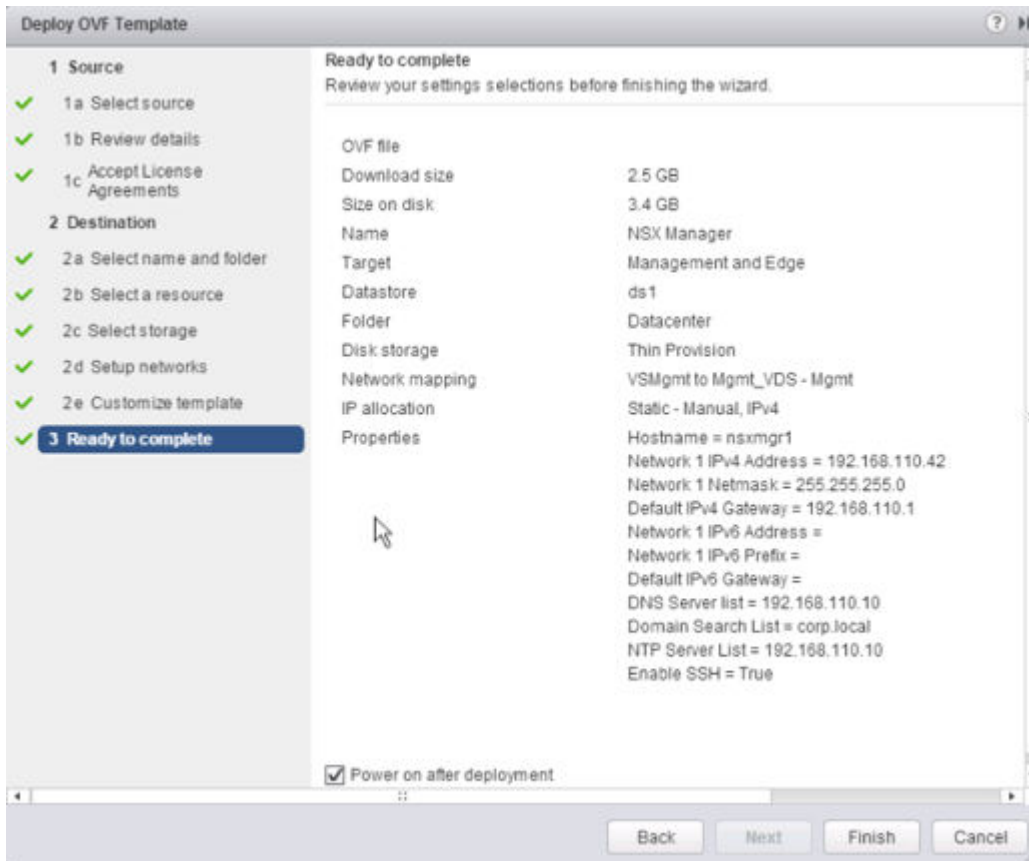
예를 들어 이 화면에서는 **Mgmt_DVS - Mgmt** 포트 그룹이 선택되었습니다.



11 (선택 사항) 고객 환경 향상 프로그램 참여(Join the Customer Experience Improvement Program) 확인란을 선택합니다.

12 NSX Manager 추가 구성 옵션을 설정합니다.

예를 들어 이 화면에는 IPv4 전용 배포에서 모든 옵션을 구성한 후의 최종 검토 화면이 표시되어 있습니다.



결과

NSX Manager의 콘솔을 열어 부팅 프로세스를 추적합니다.

NSX Manager가 완전히 부팅되면 CLI에 로그인하고 `show interface` 명령을 실행하여 IP 주소가 예상대로 적용되었는지 확인합니다.

```
nsxmgr1> show interface
Interface mgmt is up, line protocol is up
index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
HWaddr: 00:50:56:8e:c7:fa
inet 192.168.110.42/24 broadcast 192.168.110.255
inet6 fe80::250:56ff:fe8e:c7fa/64
Full-duplex, 0Mb/s
input packets 1370858, bytes 389455808, dropped 50, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 1309779, bytes 2205704550, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
```

NSX Manager에서 기본 게이트웨이, NTP 서버, vCenter Server 및 NSX Manager가 관리할 모든 하이퍼바이저 호스트의 관리 인터페이스 IP 주소를 ping할 수 있는지 확인합니다.

웹 브라우저를 열고 NSX Manager IP 주소 또는 호스트 이름으로 이동하여 NSX Manager 장치 GUI에 연결합니다.

설치 중에 설정한 암호를 사용하여 **관리자(admin)**로 로그인한 후에 홈 페이지에서 **요약 보기(View Summary)**를 클릭하여 다음 서비스가 실행되고 있는지 확인하십시오.

- vPostgres
- RabbitMQ
- NSX 관리 서비스

성능을 최적화하려면 NSX Manager 가상 장치를 위한 메모리를 예약하는 것이 좋습니다. 메모리 예약은 메모리가 오버 커밋되더라도 호스트가 가상 시스템을 위해 예약하는 물리적 메모리 양에 대해 보장되는 하한 값입니다. NSX Manager가 효율적으로 실행되는 데 충분한 메모리를 갖도록 예약 수준을 설정하십시오.

다음에 수행할 작업

NSX Manager에 vCenter Server를 등록합니다.

NSX Manager에 vCenter Server 등록

4

NSX Manager와 vCenter Server는 일대일 관계에 있습니다. 크로스 vCenter NSX 환경의 경우에도 NSX Manager의 모든 인스턴스에 하나의 vCenter Server가 있습니다.

vCenter Server 시스템에는 NSX Manager를 하나만 등록할 수 있습니다. 구성된 NSX Manager의 vCenter 등록 변경이 지원되지 않습니다.

기존 NSX Manager의 vCenter 등록을 변경하려는 경우 먼저 모든 NSX for vSphere 구성을 제거하고 vCenter Server 시스템에서 NSX Manager 플러그인을 제거해야 합니다. 지침은 [안전한 방법으로 NSX 설치 제거](#) 항목을 참조하십시오. 또는 새 NSX Manager 장치를 배포하여 새 vCenter Server 시스템에 등록할 수도 있습니다.

필요한 경우 NSX Manager에 등록하는 데 사용되는 vCenter Server 사용자 계정을 변경할 수 있습니다. 등록에 사용되는 vCenter Server 사용자 계정은 vCenter Single Sign-On **관리자** 그룹의 멤버여야 합니다.

사전 요구 사항

- NSX 관리 서비스가 실행 중이어야 합니다. <https://<nsx-manager-ip>>의 NSX Manager 웹 인터페이스에서 **홈(Home) > 요약 보기(View Summary)**를 클릭하여 서비스 상태를 확인하십시오.
- vCenter Single Sign-On **관리자** 그룹의 멤버인 vCenter Server 사용자 계정을 사용하여 NSX Manager를 vCenter Server 시스템과 동기화해야 합니다. 계정 암호에 ASCII가 아닌 문자가 포함된 경우 NSX Manager를 vCenter Server 시스템과 동기화하기 전에 암호를 변경해야 합니다. 루트 계정은 사용하지 마십시오.

사용자 추가 방법에 대한 내용은 "Platform Services Controller 관리" 설명서에서 "vCenter Single Sign-On 사용자 및 그룹 관리"를 참조하십시오.

- 정방향 및 역방향 이름 확인이 작동하는지, 그리고 다음 시스템이 서로의 DNS 이름을 확인할 수 있는지 확인합니다.
 - NSX Manager 장치
 - vCenter Server 시스템
 - Platform Services Controller 시스템
 - ESXi 호스트

절차

1 NSX Manager 가상 장치에 로그인합니다.

웹 브라우저에서 <https://<nsx-manager-ip>> 또는 <https://<nsx-manager-hostname>>의 NSX Manager 장치 GUI로 이동한 후 **관리자** 또는 **엔터프라이즈 관리자** 역할을 가진 계정으로 로그인합니다.

2 홈 페이지에서 **vCenter 등록 관리(Manage vCenter Registration)**를 클릭합니다.

3 vCenter Server 시스템의 IP 주소 또는 호스트 이름을 가리키도록 vCenter Server 요소를 편집하고 vCenter Server 시스템의 사용자 이름과 암호를 입력합니다.

4 인증서 지문이 vCenter Server 시스템의 인증서와 일치하는지 확인합니다.

vCenter Server 시스템에 CA 서명된 인증서를 설치한 경우 CA 서명된 인증서의 지문이 제공됩니다. 그렇지 않은 경우 자체 서명된 인증서가 제공됩니다.

5 NSX Manager가 방화벽 유형의 마스킹 디바이스로 보호되는 경우 외에는 **플러그인 스크립트 다운로드 위치 수정(Modify plugin script download location)**을 선택하지 마십시오.

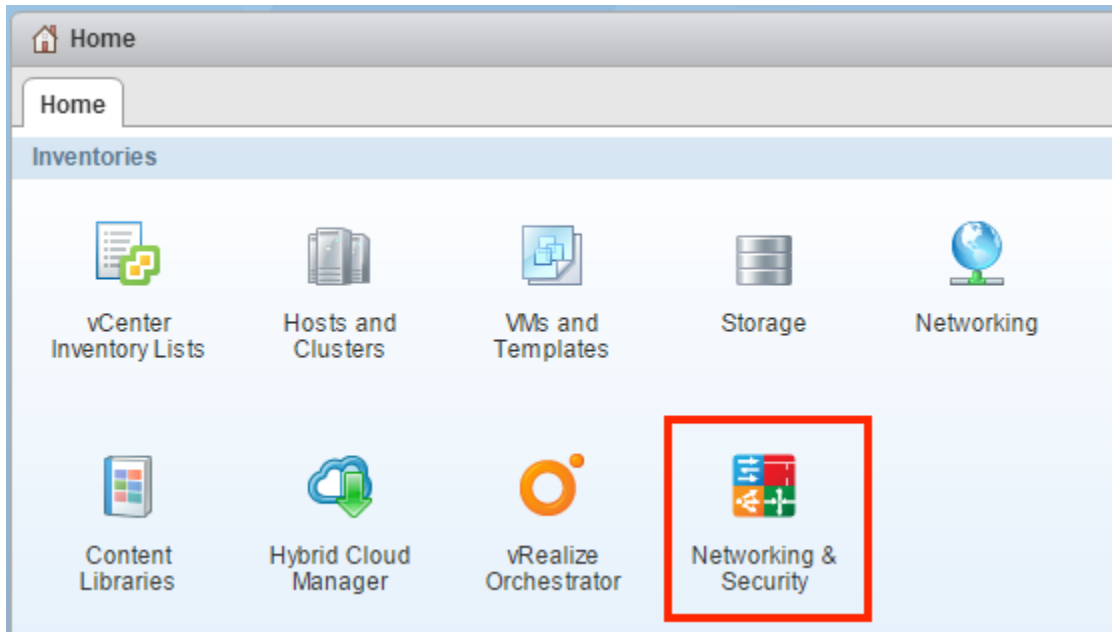
이 옵션을 선택하면 NSX Manager에 대한 대체 IP 주소를 입력할 수 있습니다. 이 유형의 방화벽 뒤에 NSX Manager를 배치하는 것은 바람직하지 않습니다.

6 vCenter Server 시스템 상태가 **연결됨(Connected)**인지 확인합니다.

7 vSphere Web Client가 이미 열려 있는 경우 로그아웃했다가 NSX Manager를 vCenter Server에 등록하는 데 사용된 계정으로 다시 로그인하십시오.

로그아웃했다가 다시 로그인하지 않으면 vSphere Web Client는 **홈(Home)** 탭에 **네트워킹 및 보안(Networking & Security)** 아이콘을 표시하지 않습니다.

네트워킹 및 보안(Networking & Security) 아이콘을 클릭하고 새로 배포된 NSX Manager가 표시되는지 확인합니다.



다음에 수행할 작업

NSX Manager를 설치한 후 즉시 NSX Manager 데이터의 백업을 예약합니다. "NSX 관리 가이드"에서 "NSX 백업 및 복원"을 참조하십시오.

NSX for vSphere 파트너 솔루션이 있는 경우 NSX Manager에 파트너 콘솔을 등록하는 방법에 대한 자세한 내용은 파트너 설명서를 참조하십시오.

이제 NSX for vSphere 구성 요소를 설치하고 구성할 수 있습니다.

Single Sign On 구성

5

SSO를 사용하면 각 구성 요소가 사용자를 개별적으로 인증할 필요 없이 다양한 구성 요소가 보안 토큰 교환 메커니즘을 통해 서로 통신할 수 있어 vSphere와 NSX의 보안이 한층 강화됩니다.

NSX Manager에서 Lookup Service를 구성하고 SSO 관리자 자격 증명을 제공하여 NSX 관리 서비스를 SSO 사용자로 등록할 수 있습니다. SSO(Single Sign On) 서비스를 NSX와 통합하면 vCenter 사용자의 사용자 인증 보안이 강화되며 NSX가 AD, NIS, LDAP 등 다른 ID 서비스의 사용자를 인증할 수 있습니다. SSO를 사용하면 NSX가 REST API 호출을 통해 신뢰할 수 있는 소스의 인증된 SAML(Security Assertion Markup Language) 토큰을 사용하여 인증을 지원합니다. 또한 NSX Manager는 다른 VMware 솔루션에 사용할 인증 SAML 토큰을 획득할 수도 있습니다.

NSX는 SSO 사용자를 위한 그룹 정보를 캐시합니다. 그룹 멤버 자격에 대한 변경 사항이 ID 제공자(예: Active Directory)에서 NSX로 전파되는 데 최대 60분이 걸립니다.

사전 요구 사항

- NSX Manager에서 SSO(Single Sign-On)를 사용하려면 vCenter Server 5.5 이상을 사용하고 vCenter Server에 SSO 인증 서비스가 설치되어 있어야 합니다. 이는 내장된 SSO에 해당하는 요건입니다. 대신 해당 배포 환경에서 외부 중앙 SSO 서버를 사용 중일 수 있습니다.

vSphere에서 제공되는 SSO 서비스에 대한 자세한 내용은 <http://kb.vmware.com/kb/2072435> 및 <http://kb.vmware.com/kb/2113115> 항목을 참조하십시오.

- SSO 서버 시간과 NSX Manager 시간이 동기화되도록 NTP 서버를 지정해야 합니다.

예:

Time Settings Unconfigure NTP Servers Edit

Specify NTP server below. For SSO configuration to work correctly it is required that the time on this virtual appliance and NTP server should be in sync. It is recommended to use the same NTP server used by the SSO server.

NTP Server	192.168.110.10
Timezone	UTC
Date/Time	12/28/2016 21:31:49

절차

1 NSX Manager 가상 장치에 로그인합니다.

웹 브라우저에서 `https://<nsx-manager-ip>` 또는 `https://<nsx-manager-hostname>`의 NSX Manager 장치 GUI로 이동한 후 **관리자** 또는 **엔터프라이즈 관리자** 역할을 가진 계정으로 로그인합니다.

2 NSX Manager 가상 장치에 로그인합니다.

3 홈 페이지에서 **장치 설정 관리(Manage Appliance Settings) > NSX 관리 서비스(NSX Management Service)**를 클릭합니다.4 [Lookup Service URL] 섹션에서 **편집(Edit)**을 클릭합니다.

5 Lookup Service가 있는 호스트의 이름 또는 IP 주소를 입력합니다.

6 포트 번호를 입력합니다.

vSphere 6.0을 사용하는 경우 포트 443을 입력합니다. vSphere 5.5의 경우 포트 번호 7444를 사용합니다.

지정된 호스트 및 포트를 기준으로 Lookup Service URL이 표시됩니다.

7 SSO 관리자 사용자 이름 및 암호를 입력하고 **확인(OK)**을 클릭합니다.



SSO 서버의 인증서 지문이 표시됩니다.

8 인증서 지문이 SSO 서버의 인증서와 일치하는지 확인합니다.

CA 서버에 CA 서명된 인증서를 설치한 경우 CA 서명된 인증서의 지문이 제공됩니다. 그렇지 않은 경우 자체 서명된 인증서가 제공됩니다.

9 Lookup Service 상태가 **연결됨(Connected)**인지 확인합니다.

예:

Lookup Service URL:	<code>https://psc-01a.corp.local:443/lookupservice/sdk</code>
SSO Administrator User Name:	<code>administrator@vsphere.local</code>
Status:	 Connected 

다음에 수행할 작업

"NSX 관리 가이드"에서 vCenter 사용자에게 역할 할당을 참조하십시오.

NSX Manager에 대한 Syslog 서버 구성

6

Syslog 서버를 지정할 경우 NSX Manager는 모든 감사 로그 및 시스템 이벤트를 Syslog 서버로 보냅니다.

Syslog 데이터는 설치와 구성 작업 중의 문제 해결과 기록된 데이터 검토에 유용합니다.

NSX Edge는 2개의 Syslog 서버를 지원합니다. NSX Manager 및 NSX Controller는 하나의 Syslog 서버를 지원합니다.

절차

- 1 NSX Manager 가상 장치에 로그인합니다.

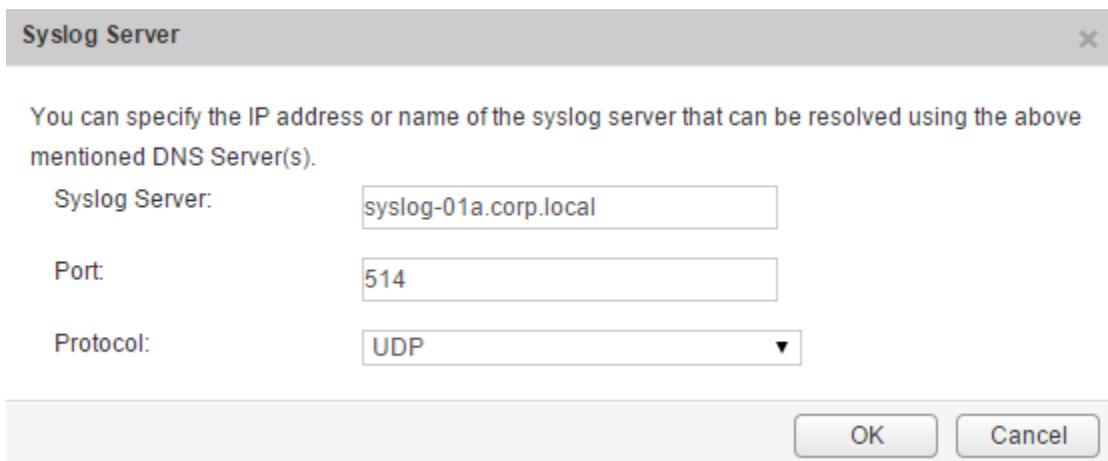
웹 브라우저에서 <https://<nsx-manager-ip>> 또는 <https://<nsx-manager-hostname>>의 NSX Manager 장치 GUI로 이동한 후 관리자 또는 엔터프라이즈 관리자 역할을 가진 계정으로 로그인합니다.

- 2 홈 페이지에서 장치 설정 관리(Manage Appliance Settings) > 일반(General)을 클릭합니다.

- 3 Syslog 서버(Syslog Server) 옆의 편집(Edit)을 클릭합니다.

- 4 syslog 서버의 IP 주소 또는 호스트 이름, 포트 및 프로토콜을 입력합니다.

예:



Syslog Server

You can specify the IP address or name of the syslog server that can be resolved using the above mentioned DNS Server(s).

Syslog Server:

Port:

Protocol:

OK Cancel

- 5 확인(OK)을 클릭합니다.

결과

NSX Manager 원격 로깅은 사용하도록 설정되어 있고, 로그는 독립형 **syslog** 서버에 저장되어 있습니다.

NSX for vSphere 라이선스 설치 및 할당

7

NSX Manager 설치가 완료된 후 vSphere Web Client를 사용하여 NSX for vSphere 라이선스를 설치하고 할당할 수 있습니다.

NSX 6.2.3부터 설치 시의 기본 라이선스는 vShield Endpoint용 NSX입니다. 이 라이선스가 있으면 바이러 스 백신 오프로드 기능용으로만 vShield Endpoint를 배포하고 관리하기 위한 NSX를 사용할 수 있으며 호 스트 준비 및 NSX Edge 생성을 차단하여 VXLAN, 방화벽 및 Edge 서비스의 사용을 제한하는 엄격한 적용 기능도 사용할 수 있습니다.

논리적 스위치, 논리적 라우터, 분산 방화벽을 포함하는 다른 NSX 기능이나 NSX Edge가 필요한 경우 NSX 라이선스를 구입하여 이러한 기능을 사용하거나 단기간의 기능 평가가 필요한 경우에는 평가판 라이 센스를 요청하십시오.

NSX 라이선싱 버전 및 관련 기능에 대한 자세한 내용은 <https://kb.vmware.com/kb/2145269>를 참조하십시오.

절차

- ◆ vSphere 5.5에서 다음 단계를 완료하여 NSX에 대한 라이선스를 추가합니다.
 - a vSphere Web Client에 로그인합니다.
 - b 시스템 관리(Administration)를 클릭하고 라이선스(Licenses)를 클릭합니다.
 - c 솔루션(Solutions) 탭을 클릭합니다.
 - d [솔루션] 목록에서 [NSX for vSphere]를 선택합니다. 라이선스 키 할당(Assign a license key)을 클릭합니다.
 - e 드롭다운 메뉴에서 새 라이선스 키 할당(Assign a new license key)을 선택합니다.
 - f 라이선스 키를 입력하고 새 키의 레이블(선택 사항)을 입력합니다.
 - g 디코딩(Decode)을 클릭합니다.

라이선스 키가 올바른 형식인지, 자산에 라이선스를 부여하기에 충분한 용량이 있는지 확인하려면 해당 라이선스 키를 디코딩합니다.
 - h 확인(OK)을 클릭합니다.

- ◆ vSphere 6.0에서 다음 단계를 완료하여 NSX에 대한 라이선스를 추가합니다.
 - a vSphere Web Client에 로그인합니다.
 - b 시스템 관리(Administration)를 클릭하고 라이선스(Licenses)를 클릭합니다.
 - c 자산(Assets) 탭을 클릭하고 솔루션(Solutions) 탭을 클릭합니다.
 - d [솔루션] 목록에서 [NSX for vSphere]를 선택합니다. 모든 작업(All Actions) 드롭다운 메뉴에서 라이선스 할당...(Assign license...)을 선택합니다.
 - e 추가(Add)(+) 아이콘을 클릭합니다. 라이선스 키를 입력하고 다음(Next)을 클릭합니다. 라이선스의 이름을 입력하고 다음(Next)을 클릭합니다. 완료(Finish)를 클릭하여 라이선스를 추가합니다.
 - f 새 라이선스를 선택합니다.
 - g (선택 사항) 기능 보기(View Features) 아이콘을 클릭하여 이 라이선스로 사용할 수 있는 기능을 확인합니다. 용량(Capacity) 열에서 라이선스의 용량을 확인합니다.
 - h 확인(OK)을 클릭하여 NSX에 새 라이선스를 할당합니다.

다음에 수행할 작업

NSX 라이선싱에 대한 자세한 내용은 <http://www.vmware.com/files/pdf/vmware-product-guide.pdf>를 참조하십시오.

NSX Controller 클러스터 배포

8

NSX Controller는 NSX 논리적 스위칭 및 라우팅 기능에 대한 제어부 기능을 제공하는 고급 분산 상태 관리 시스템입니다. 네트워크 내의 모든 논리적 스위치에 대한 중앙 제어 지점으로서 모든 호스트, 논리적 스위치(VXLAN) 및 논리적 분산 라우터에 대한 정보를 유지하는 역할을 합니다. 1) 논리적 분산 라우터 또는 2) VXLAN을 유니캐스트 또는 하이브리드 모드로 배포하려는 경우 컨트롤러가 필요합니다.

NSX 배포의 규모에 관계없이 VMware를 사용하려면 각 NSX Controller 클러스터에 세 개의 컨트롤러 노드가 있어야 합니다. 다른 개수의 컨트롤러 노드를 포함하는 경우는 지원되지 않습니다.

각 컨트롤러의 디스크 스토리지 시스템의 최대 쓰기 지연 시간은 300ms보다 작고 평균 쓰기 지연 시간은 100ms보다 작아야 합니다. 스토리지 시스템이 이러한 요구 사항을 충족하지 못하면 클러스터가 불안정해지며 시스템 다운타임이 발생할 수 있습니다.

경고 컨트롤러 상태가 **배포 중(Deploying)**인 동안에는 논리적 스위치 또는 분산 라우팅을 환경에 추가하거나 수정하지 마십시오. 또한 호스트 준비 절차로 진행하지 마십시오. 새 컨트롤러를 컨트롤러 클러스터에 추가한 후에는 모든 컨트롤러가 잠시(5분 이하) 비활성화됩니다. 이 중단 시간 동안 컨트롤러 관련 작업(예: 호스트 준비)에서 예상치 않은 결과가 나타날 수 있습니다. 호스트 준비가 성공적으로 완료된 것처럼 보여도 SSL 인증이 올바르게 설정되지 않을 수 있기 때문에 VXLAN 네트워크에서 문제가 발생합니다.

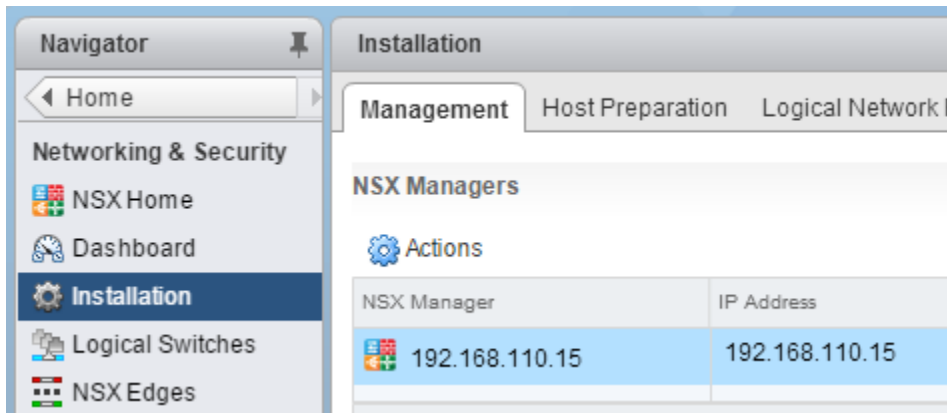
사전 요구 사항

- NSX Controller를 배포하기 전에 NSX Manager 장치를 배포하고 vCenter를 NSX Manager에 등록해야 합니다.
- 게이트웨이 및 IP 주소 범위 등 컨트롤러 클러스터의 IP 풀 설정을 지정합니다. DNS 설정은 선택 사항입니다. NSX Controller IP 네트워크는 NSX Manager와 ESXi 호스트의 관리 인터페이스에 연결되어야 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **홈 > Networking & Security > 설치(Home > Networking & Security > Installation)**로 이동하여 **관리(Management)** 탭을 선택합니다.

예:



- 3 NSX Controller 노드 섹션에서 **노드 추가(Add Node)**(+) 아이콘을 클릭합니다.
- 4 환경에 맞게 NSX Controller 설정을 입력합니다.

NSX Controller는 VXLAN을 기반으로 하지 않으면서 IPv4를 통해 NSX Manager, 기타 컨트롤러와 호스트에 연결되어 있는 vSphere 표준 스위치 또는 vSphere Distributed Switch 포트 그룹으로 배포해야 합니다.

예:

Add Controller ?

Name:

*

NSX Manager:

* ▼

Datacenter:

* ▼

Cluster/Resource Pool:

* ▼

Datastore:

* ▼

Host:

▼

Folder

▼

Connected To:

* Change Remove

IP Pool:

* Select

Password:

*

Confirm password:

*

- 5 아직 컨트롤러 클러스터에 대한 IP 풀을 구성하지 않은 경우 **새 IP 풀(New IP Pool)**을 클릭하여 구성합니다.

필요할 경우 개별 컨트롤러를 개별 IP 서브넷에 배치할 수 있습니다.

예:

Add Static IP Pool

Name: * controller-pool

Gateway: * 192.168.110.1
A gateway can be any IPv4 or IPv6 address.

Prefix Length: * 24

Primary DNS:

Secondary DNS:

DNS Suffix:

Static IP Pool: * 192.168.110.31-192.168.110.35
for example 192.168.1.2-192.168.1.100 or
abcd:87:87::10-abcd:87:87::20

OK Cancel

- 6 컨트롤러의 암호를 입력하고 다시 입력합니다.

참고 암호 안에 사용자 이름 문자열을 포함할 수 없습니다. 또한 동일한 문자가 3회 이상 연속적으로 반복될 수 없습니다.

암호는 최소 12자여야 하고 다음 4개 규칙 중 3개를 준수해야 합니다.

- 하나 이상의 대문자
- 하나 이상의 소문자
- 숫자 1개 이상
- 하나 이상의 특수 문자

- 7 첫 번째 컨트롤러가 완전하게 배포되면 컨트롤러 두 개를 추가적으로 배포합니다.

컨트롤러는 반드시 3개를 배포해야 합니다. 컨트롤러가 동일한 호스트에 놓이지 않도록 DRS 반선택도 규칙을 구성하는 것이 좋습니다.

결과

성공적으로 배포되면 컨트롤러 상태가 **연결됨(Connected)**이 되고 녹색 확인 표시가 표시됩니다.

배포에 실패하면 "NSX 문제 해결 가이드"에서 NSX Controller 배포를 참조하십시오.

NSX Controller 노드가 먼저 배포된 호스트에서는 NSX가 자동 VM 시작/종료를 사용하도록 설정합니다. 컨트롤러 노드 VM이 나중에 다른 호스트로 마이그레이션되는 경우 새 호스트가 자동 VM 시작/종료를 사용하도록 설정하지 않을 수도 있습니다. 따라서 클러스터의 모든 호스트에서 자동 VM 시작/종료가 사용되도록 설정되었는지 확인하는 것이 좋습니다. http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-5FE08AC7-4486-438E-AF88-80D6C7928810.html를 참조하십시오.

예

방화벽 보호 대상에서 가상 시스템 제외

9

NSX 분산 방화벽으로 보호되는 대상에서 가상 시스템 집합을 제외할 수 있습니다.

NSX Manager, NSX Controller 및 NSX Edge 가상 시스템은 NSX 분산 방화벽 보호 대상에서 자동으로 제외됩니다. 또한 다음 서비스 가상 시스템은 제외 목록에 배치하여 트래픽의 자유로운 흐름을 허용하는 것이 좋습니다.

- **vCenter Server.** 방화벽으로 보호되는 클러스터로 vCenter Server를 이동할 수는 있지만, 연결 문제를 방지하려면 해당 vCenter Server가 이미 제외 목록에 있는 상태여야 합니다.

참고 "any any" 기본 규칙을 허용에서 차단으로 변경하기 전에 vCenter Server를 제외 목록에 추가하는 것이 중요합니다. 이렇게 하지 못하면 모두 거부 규칙을 생성(또는 작업을 차단하도록 기본 규칙 수정)한 후에 vCenter Server에 대한 액세스가 차단됩니다. 이 경우 다음 API 명령을 실행하여 DFW를 기본 방화벽 규칙 집합으로 롤백합니다. https://NSX_Manager_IP/api/4.0/firewall/globalroot-0/config. 요청은 상태 204를 반환해야 합니다. 이렇게 하면 DFW에 대한 기본 규칙(허용 기본 규칙)이 복원되고 vCenter Server 및 vSphere Web Client에 대한 액세스가 다시 사용되도록 설정됩니다.

- 파트너 서비스 가상 시스템.
- 비규칙 모드가 필요한 가상 시스템. NSX 분산 방화벽에서 이 가상 시스템을 보호하는 경우 성능에 부정적인 영향을 줄 수 있습니다.
- Windows 기반 vCenter에서 사용하는 SQL Server.
- vCenter 웹 서버(별도로 실행할 경우).

절차

- 1 vSphere Web Client에서 **Networking & Security**를 클릭합니다.
- 2 **Networking & Security 인벤토리(Networking & Security Inventory)**에서 **NSX Manager(NSX Managers)**를 클릭합니다.
- 3 **이름(Name)** 열에서 NSX Manager를 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **제외 목록(Exclusion List)** 탭을 클릭합니다.
- 5 **추가(Add)**(+) 아이콘을 클릭합니다.
- 6 제외하려는 가상 시스템을 선택하고 **추가(Add)**를 클릭합니다.

7 확인(OK)을 클릭합니다.

결과

가상 시스템에 여러 vNIC가 있는 경우에는 모두 보호 대상에서 제외됩니다. 가상 시스템을 제외 목록에 추가한 후 vNIC를 가상 시스템에 추가한 경우 새로 추가된 vNIC에서 방화벽이 자동으로 배포됩니다. 이 vNIC를 방화벽 보호 대상에서 제외하려면 제외 목록에서 가상 시스템을 제거한 다음, 가상 시스템을 제외 목록에 다시 추가해야 합니다. 다른 해결 방법은 가상 시스템의 전원을 껐다가 다시 켜는 것입니다. 그러나 첫 번째 옵션이 지장을 적게 줍니다.

NSX에 사용할 수 있도록 호스트 클러스터 준비

10

호스트 준비는 NSX Manager가 1) vCenter 클러스터의 멤버인 ESXi 호스트에 커널 모듈을 설치하고 2) 제어부 및 관리부 패브릭을 구축하는 프로세스입니다. VIB 파일로 패키징된 NSX for vSphere 커널 모듈은 하이퍼바이저 커널 내에서 실행되어 분산 라우팅, 분산 방화벽 및 VXLAN 브리징 기능과 같은 서비스를 제공합니다.

네트워크 가상화를 위한 환경을 준비하려면 각 vCenter Server의 클러스터 수준별로 필요한 위치에 네트워크 인프라 구성 요소를 설치해야 합니다. 이렇게 해야 클러스터의 모든 호스트에 필요한 소프트웨어가 배포됩니다. 해당 클러스터에 새 호스트가 추가되면 필요한 소프트웨어가 새로 추가된 호스트에 자동으로 설치됩니다.

ESXi를 상태 비저장 모드에서 사용하는 경우 ESXi가 재부팅 과정에서 상태를 유지하지 않으므로 NSX VIB를 수동으로 다운로드하고 호스트 이미지에 포함시켜야 합니다. NSX VIB의 다운로드 경로는 `https://<NSX_MANAGER_IP>/bin/vdn/nwfabric.properties` 페이지에서 찾을 수 있습니다. 다운로드 경로는 NSX 릴리스에 따라 변경되니 유의하시기 바랍니다. 항상 `https://<NSX_MANAGER_IP>/bin/vdn/nwfabric.properties` 페이지를 확인하여 적절한 VIB를 다운로드하십시오. 자세한 내용은 "자동 배포를 통해 VXLAN 배포" <https://kb.vmware.com/kb/2041972>를 참조하십시오.

사전 요구 사항

- vCenter Server를 NSX Manager에 등록하고 NSX Controller를 배포합니다.
- NSX Manager의 IP 주소로 쿼리할 때 DNS 역방향 조회에서 정규화된 도메인 이름을 반환하는지 확인합니다. 예:

```
C:\Users\Administrator>nslookup 192.168.110.42
Server: localhost
Address: 127.0.0.1

Name: nsxmgr-1-01a.corp.local
Address: 192.168.110.42
```

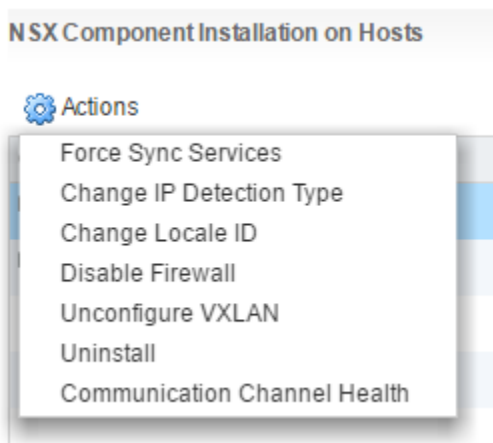
- 호스트가 vCenter Server의 DNS 이름을 확인할 수 있는지 확인합니다.
- 호스트가 포트 80을 사용하여 vCenter Server에 연결할 수 있는지 확인합니다.

- vCenter Server와 ESXi 호스트의 네트워크 시간이 동기화되었는지 확인합니다.
- NSX에 참여할 각 호스트 클러스터에 대해 클러스터 내의 호스트가 공용 VDS(vSphere Distributed Switch)에 연결되었는지 확인합니다.

예를 들어 클러스터에 Host1과 Host2가 있다고 가정해 보겠습니다. Host1은 VDS1과 VDS2에 연결되어 있고 Host2는 VDS1과 VDS3에 연결되어 있습니다. NSX에 대한 클러스터를 준비할 때 사용자는 NSX를 클러스터의 VDS1에만 연결할 수 있습니다. 다른 호스트(Host3)를 클러스터에 추가하고 Host3을 VDS1에 연결하지 않으면 구성이 올바르지 않아 Host3에서 NSX 기능을 사용할 수 없게 됩니다.

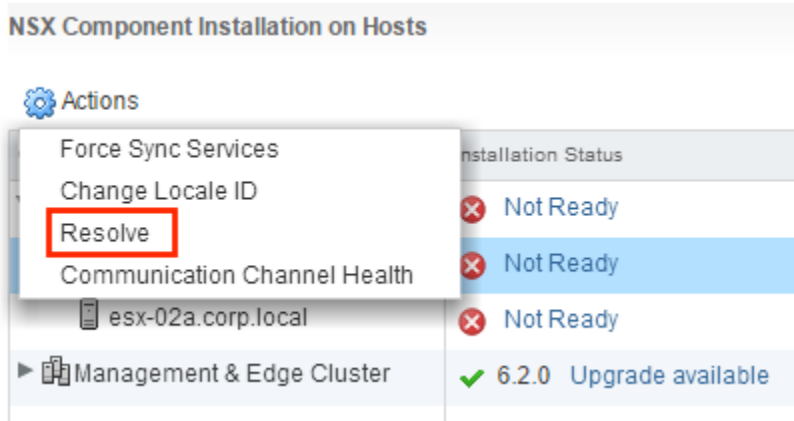
- 환경에 VUM(vSphere Update Manager)이 있는 경우 네트워크 가상화를 위한 클러스터를 준비하기 전에 VUM을 사용하지 않도록 설정해야 합니다. VUM이 사용하도록 설정되어 있는지 여부를 확인하는 방법과 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 <http://kb.vmware.com/kb/2053782>를 참조하십시오.
- NSX 호스트 준비 프로세스를 시작하기 전에 항상 클러스터가 해결된 상태에 있는지 확인하십시오. 즉, **해결(Resolve)** 옵션이 클러스터의 **작업(Actions)** 목록에 나타나지 않아야 합니다.

예:




해결(Resolve) 옵션은 클러스터에서 하나 이상의 호스트를 재부팅해야 할 때 나타날 수 있습니다.

또한 해결해야 하는 오류 조건이 있을 경우에도 **해결(Resolve)** 옵션이 나타납니다. **준비 안 됨(Not Ready)** 링크를 클릭하면 오류가 표시됩니다. 가능한 경우 오류 조건을 제거합니다. 클러스터에서 오류 조건을 제거할 수 없는 경우 호스트를 새 클러스터나 다른 클러스터로 이동한 후 이전 클러스터를 삭제하는 방법을 시도할 수 있습니다.



해결(Resolve) 옵션으로 문제가 해결되지 않으면 "NSX 문제 해결 가이드"를 참조하십시오. **해결(Resolve)** 옵션을 통해 해결된 문제 목록을 보려면 "NSX 로깅 및 시스템 이벤트"를 참조하십시오.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **홈 > Networking & Security > 설치(Home > Networking & Security > Installation)**로 이동하여 **호스트 준비(Host Preparation)** 탭을 선택합니다.
- 3 NSX 논리적 스위칭, 라우팅 및 방화벽이 필요한 모든 클러스터에 대해 **작업(Actions)**()과 **설치(Install)**를 차례대로 클릭합니다.

페이로드 클러스터라고도 하는 계산 클러스터는 애플리케이션 VM(웹, 데이터베이스 등)이 포함된 클러스터입니다. 계산 클러스터에서 NSX 스위칭, 라우팅 또는 방화벽을 사용할 예정인 경우에는 해당 계산 클러스터에 대해 **설치(Install)**를 클릭해야 합니다.

공유 "관리 및 Edge" 클러스터(예 참조)에서는 NSX Manager 및 컨트롤러 VM이 DRL(논리적 분산 라우터) 및 ESG(Edge Services Gateway) 등의 Edge 디바이스와 클러스터를 공유합니다. 이 경우에는 공유 클러스터에 대해 **설치(Install)**를 클릭하는 것이 중요합니다.

하지만 반대로 관리 및 Edge 각각이 운영 환경에서 권장되는 것처럼 서로 공유되지 않는 전용 클러스터를 사용하는 경우에는 관리 클러스터는 제외하고 Edge 클러스터에 대해 **설치(Install)**를 클릭해야 합니다.

참고 설치가 진행 중인 동안 서비스 또는 구성 요소를 배포하거나 업그레이드하거나 제거하지 마십시오.

- 4 **설치 상태(Installation Status)** 열에 녹색 확인 표시가 나타날 때까지 설치를 모니터링합니다.

설치 상태(Installation Status) 열에 빨간색 경고 아이콘이 나타나고 **준비 안 됨(Not Ready)**이라고 표시되면 **해결(Resolve)**을 클릭합니다. **해결(Resolve)**을 클릭하면 호스트를 재부팅해야 할 수 있습니다. 여전히 설치가 실패하면 경고 아이콘을 클릭합니다. 그러면 모든 오류가 표시됩니다. 필요한 조치를 취하고 **해결(Resolve)**을 다시 클릭합니다.

설치가 완료되면 **설치 상태(Installation Status)** 열에는 설치된 NSX의 버전 및 빌드가 표시되고 **방화벽(Firewall)** 열에는 **사용(Enabled)**이 표시됩니다. 또한 두 열에 녹색 확인 표시가 나타납니다. **설치 상태(Installation Status)** 열에 [해결]이라고 표시되면 [해결]을 클릭하고 브라우저 창을 새로 고칩니다.

결과

준비된 클러스터 내의 모든 호스트에 VIB가 설치 및 등록됩니다. 설치되는 VIB는 설치된 NSX 및 ESXi 버전에 따라 다릅니다.

ESXi 버전	NSX 버전	설치된 VIB
5.5	모든 6.3.x	<ul style="list-style-type: none"> ■ esx-vsip ■ esx-vxlan
6.0 이상	6.3.2 또는 이전 버전	<ul style="list-style-type: none"> ■ esx-vsip ■ esx-vxlan
6.0 이상	6.3.3 이상 버전	<ul style="list-style-type: none"> ■ esx-nsxv

확인하려면 SSH를 통해 각 호스트에 연결하고 `esxcli software vib list` 명령을 실행한 후 관련 VIB를 확인합니다. 이 명령을 실행하면 VIB 및 설치된 VIB의 버전이 표시됩니다.

```
[root@host:~] esxcli software vib list | grep esx
esx-XXXX      6.0.0-0.0.XXXXXXX  VMware  VMwareCertified  2016-12-29
```

호스트를 준비된 클러스터에 추가하면 NSX VIB가 자동으로 해당 호스트에 설치됩니다.

호스트를 준비되지 않은 클러스터로 이동하면 해당 호스트에서 NSX VIB가 자동으로 제거됩니다.

준비된 클러스터에 호스트 추가

11

이 섹션에서는 네트워크 가상화를 위해 준비된 클러스터에 호스트를 추가하는 방법을 설명합니다.

절차

- 1 vCenter Server에 독립형 호스트로 호스트를 추가합니다.

자세한 내용은 "ESXi 및 vCenter Server 설명서" 를 참조하십시오.

- 2 호스트를 추가하려는 클러스터에 매핑된 vSphere Distributed Switch에 호스트를 추가합니다.

클러스터의 모든 호스트는 NSX에서 사용하는 vSphere Distributed Switch에 있어야 합니다.

- 3 대상 호스트를 마우스 오른쪽 버튼으로 클릭하고 **유지 보수 모드(Maintenance Mode) > 유지 보수 모드 설정(Enter Maintenance Mode)**을 선택합니다.

- 4 대상 호스트를 기존 NSX 지원 클러스터로 끌어서 놓습니다.

준비된 클러스터이므로 새로 추가된 호스트에 필요한 소프트웨어가 자동으로 설치됩니다.

- 5 호스트를 마우스 오른쪽 버튼으로 클릭하고 **유지 보수 모드(Maintenance Mode) > 유지 보수 모드 종료(Exit Maintenance Mode)**를 선택합니다.

DRS가 가상 시스템을 호스트에 분산합니다.

NSX 준비된 클러스터에서 호스트 제거

12

이 섹션에서는 네트워크 가상화를 위해 준비된 클러스터에서 호스트를 제거하는 방법을 설명합니다. 예를 들어 특정 호스트를 NSX에 참여시키지 않으려는 경우 이 절차를 수행할 수 있습니다.

중요 NSX 6.3.0 이상 및 ESXi 6.0 이상이 있는 호스트에서는 VIB를 제거하기 위해 호스트를 재부팅할 필요가 없습니다. 이전 버전의 NSX 및 ESXi에서는 VIB 제거를 완료하기 위해 재부팅이 필요합니다.

절차

- 1 호스트를 유지 보수 모드로 전환하고 DRS에서 호스트를 제거할 때까지 기다리거나 호스트에서 실행 중인 VM에 수동으로 vMotion을 수행합니다.
- 2 호스트를 준비되지 않은 클러스터로 이동하거나 클러스터 외부의 독립형 호스트로 만들어 준비된 클러스터에서 호스트를 제거합니다.

NSX가 네트워크 가상화 구성 요소 및 서비스 가상 시스템을 호스트에서 제거합니다.

- 3 호스트에 NSX 6.2.x 이전 버전 또는 ESXi 5.5가 설치되어 있으면 호스트를 재부팅합니다.
- 4 VIB 제거가 완료되었는지 확인하십시오.
 - a vSphere Web Client에서 [최근 작업] 창을 확인합니다.
 - b **호스트 준비(Host Preparation)** 탭에서 호스트가 제거된 클러스터의 [설치 상태]에 녹색 확인 표시가 있는지 확인하십시오.

[설치 상태]가 설치 중이면 제거 작업이 여전히 진행 중인 것입니다.

- 5 제거가 완료되면 유지 보수 모드에서 호스트를 제거하십시오.

결과

NSX VIB가 호스트에서 제거됩니다. 확인하려면 SSH를 통해 호스트에 연결하고 `esxcli software vib list | grep esx` 명령을 실행합니다. 호스트에 다음 VIB가 없는지 확인합니다.

- esx-vsip
- esx-vxlan

호스트에 VIB가 남아 있는 경우 자동 VIB 제거가 수행되지 않은 이유를 로그에서 확인할 수 있습니다.

다음 명령을 실행하면 VIB를 수동으로 제거할 수 있습니다.

- `esxcli software vib remove --vibname=esx-vxlan`
- `esxcli software vib remove --vibname=esx-vsip`

VXLAN 전송 매개 변수 구성

13

VXLAN 네트워크는 호스트 간의 계층 2 논리적 스위칭에 사용되며 다수의 기본 계층 3 도메인으로 확장될 수 있습니다. VXLAN은 NSX에 참여하는 각 클러스터를 VDS(vSphere Distributed Switch)에 매핑하여 클러스터 단위로 구성할 수 있습니다. 클러스터를 Distributed Switch에 매핑하면 해당 클러스터 내의 각 호스트가 논리적 스위치를 사용하도록 설정됩니다. 여기에서 선택한 설정은 VMkernel 인터페이스를 생성하는데 사용됩니다.

논리적 라우팅 및 스위칭이 필요한 경우 호스트에 NSX VIB가 설치된 모든 클러스터에는 VXLAN 전송 매개 변수도 구성되어야 합니다. 분산 방화벽만 배포하려는 경우에는 VXLAN 전송 매개 변수를 구성하지 않아도 됩니다.

VXLAN 네트워킹을 구성할 때 vSphere Distributed Switch, VLAN ID, MTU 크기, IP 주소 지정 메커니즘(DHCP 또는 IP 풀) 및 NIC 팀 구성 정책을 제공해야 합니다.

각 스위치의 MTU는 1550 이상으로 설정해야 합니다. 기본적으로는 1600으로 설정되어 있습니다.

vSphere Distributed Switch MTU 크기가 VXLAN MTU보다 큰 경우 vSphere Distributed Switch MTU가 하향 조정되지 않습니다. 값을 낮게 설정한 경우에는 VXLAN MTU와 일치하도록 조정됩니다. 예를 들어 vSphere Distributed Switch MTU를 2000으로 설정하고 VXLAN MTU의 기본값인 1600을 사용하는 경우 vSphere Distributed Switch MTU는 변경되지 않습니다. vSphere Distributed Switch MTU가 1500이고 VXLAN MTU가 1600이면 vSphere Distributed Switch MTU는 1600으로 변경됩니다.

VTEP에는 연결된 VLAN ID가 있습니다. 그러나 프레임에 태그를 지정하지 않으려는 경우 VTEP의 VLAN ID를 0으로 지정할 수 있습니다.

관리 클러스터 및 계산 클러스터에 대해 다른 IP 주소 설정을 사용할 수도 있습니다. 이는 물리적 네트워크의 설계 방식에 따라 다르며 소규모 배포에는 해당되지 않습니다.

사전 요구 사항

- 클러스터의 모든 호스트가 공통 vSphere Distributed Switch에 연결되어 있어야 합니다.
- NSX Manager가 설치되어 있어야 합니다.
- 멀티캐스트 복제 모드를 제어부에 사용하는 경우가 아니라면 NSX Controller가 설치되어 있어야 합니다.
- NIC 팀 구성 정책을 계획합니다. NIC 팀 구성 정책은 vSphere Distributed Switch의 로드 밸런싱 및 페일오버 설정을 결정합니다.

일부는 이더넷 채널이나 LACPv1 또는 LACPv2를 사용하고 다른 일부는 다른 팀 구성 정책을 사용하는 vSphere Distributed Switch에서는 여러 포트 그룹에 대해 다양한 팀 구성 정책을 함께 사용하지 않아야 합니다. 서로 다른 팀 구성 정책에서 업링크를 공유하면 트래픽이 중단됩니다. 논리적 라우터가 있으면 라우팅 문제가 발생합니다. 이러한 구성은 지원되지 않으며 사용하지 않아야 합니다.

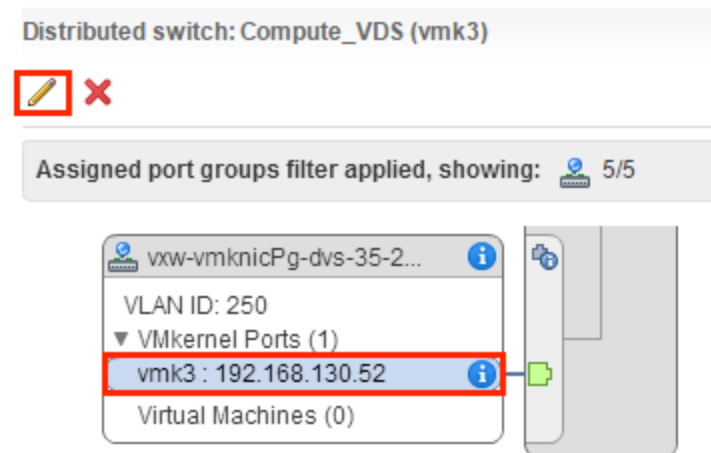
IP 해시 기반 팀 구성(이더넷 채널, LACPv1 또는 LACPv2)에 대한 모범 사례에서는 팀의 vSphere Distributed Switch에서 모든 업링크를 사용하며, 해당 vSphere Distributed Switch에 다른 팀 구성 정책을 사용하는 포트 그룹이 없습니다. 자세한 내용 및 지침은 "VMware® NSX for vSphere 네트워크 가상화 설계 가이드" (<https://communities.vmware.com/docs/DOC-27683>)를 참조하십시오.

- VTEP(VXLAN Tunnel End Point)의 IP 주소 지정 체계를 계획합니다. VTEP는 외부 IP 헤더에 사용되는 소스 IP 주소와 대상 IP 주소로, VXLAN에서 프레임 캡슐화를 시작하고 종료하는 ESX 호스트를 고유하게 식별합니다. DHCP 또는 수동으로 구성된 IP 풀을 VTEP IP 주소에 사용할 수 있습니다.

특정 IP 주소를 VTEP에 할당하려는 경우 1) MAC 주소를 DHCP 서버의 특정 IP 주소로 매핑하는 DHCP 고정 주소 또는 예약을 사용하거나 2) IP 풀을 사용한 다음 **호스트 및 클러스터(Hosts and Clusters) > 호스트(host) > 관리(Manage) > 네트워킹(Networking) > 가상 스위치(Virtual Switches)**에서 vmknic에 할당된 VTEP IP 주소를 수동으로 편집할 수 있습니다.

참고 IP 주소를 수동으로 편집하는 경우 IP 주소가 원래 IP 풀 범위와 비슷하지 않도록 확인합니다.

예:



- 동일한 VDS의 멤버인 클러스터의 경우 VTEP의 VLAN ID와 NIC 팀 구성의 VLAN ID가 동일해야 합니다.
- VXLAN에 사용할 수 있도록 클러스터를 준비하기 전에 vSphere Distributed Switch 구성을 내보내는 것이 좋습니다. <http://kb.vmware.com/kb/2034602>를 참조하십시오.

절차

- 1 vSphere Web Client에 로그인합니다.

- 2 **홈 > Networking & Security > 설치(Home > Networking & Security > Installation)**로 이동하여 **호스트 준비(Host Preparation)** 탭을 선택합니다.
- 3 **VXLAN(Not Configured)** 열에서 **구성되지 않음(VXLAN)**을 클릭합니다.
- 4 논리적 네트워킹을 설정합니다.

설정 시 vSphere Distributed Switch, VLAN ID, MTU 크기, IP 주소 지정 메커니즘 및 NIC 팀 구성 정책을 선택합니다.

아래의 예제 화면은 IP 풀 주소 범위가 182.168.150.1부터 192.168.150.100까지이고 VLAN 150을 통해 지원되며 페일오버 NIC 팀 구성 정책이 있는 관리 클러스터의 구성을 보여 줍니다.

Configure VXLAN networking

Configuring all hosts in cluster "Management and Edge" for VXLAN networking.

Switch: * Mgmt_VDS

VLAN: * 150

MTU: * 1600

VMKNic IP Addressing: * ☐ Use DHCP
☒ Use IP Pool

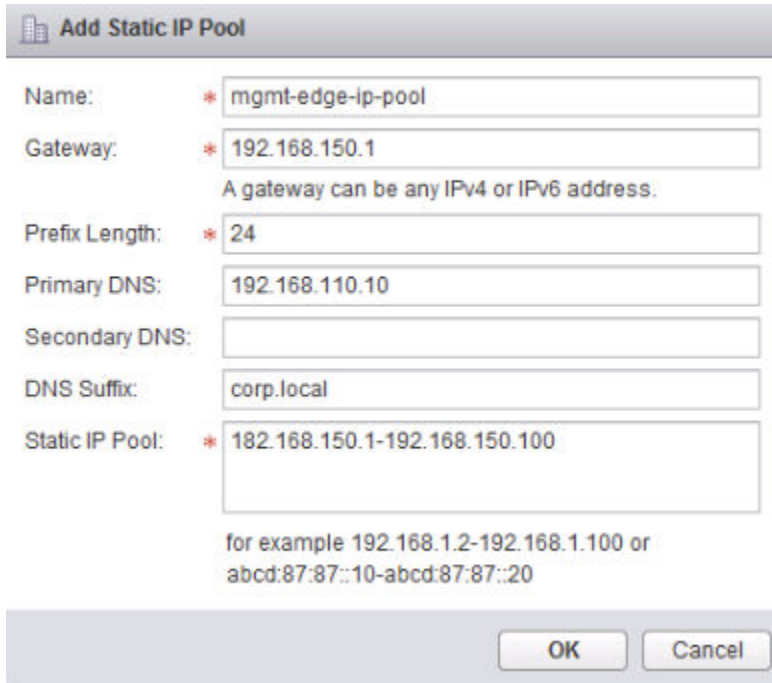
IP Pool: New IP Pool...

VMKNic Teaming Policy: * Fail Over

VTEP: * 1

OK Cancel

VTEP의 수는 UI에서 편집할 수 없습니다. VTEP 수는 준비되는 vSphere Distributed Switch의 dvUplink 수와 일치하도록 설정됩니다.



Add Static IP Pool

Name: * mgmt-edge-ip-pool

Gateway: * 192.168.150.1
A gateway can be any IPv4 or IPv6 address.

Prefix Length: * 24

Primary DNS: 192.168.110.10

Secondary DNS:

DNS Suffix: corp.local

Static IP Pool: * 192.168.150.1-192.168.150.100

for example 192.168.1.2-192.168.1.100 or
abcd:87:87::10-abcd:87:87::20

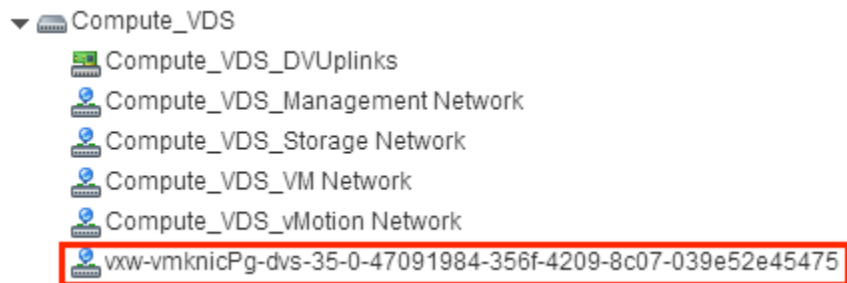
OK Cancel

계산 클러스터에는 다른 IP 주소 설정을 사용할 수 있습니다(예: 192.168.250.0/24 및 VLAN 250). 이는 물리적 네트워크의 설계 방식에 따라 다르며 소규모 배포에는 해당되지 않습니다.

결과

VXLAN을 구성하면 지정된 vSphere Distributed Switch에 새 분산 포트 그룹이 생성됩니다.

예:



VXLAN 문제 해결에 대한 자세한 내용은 "NSX 문제 해결 가이드"를 참조하십시오.

세그먼트 ID 풀 및 멀티캐스트 주소 범위 할당

14

VXLAN 세그먼트는 VTEP(VXLAN Tunnel End Point) 사이에 구축됩니다. 하이퍼바이저 호스트는 일반적인 VTEP의 예입니다. 각 VXLAN 터널은 세그먼트 ID를 갖습니다. 네트워크 트래픽을 분리하기 위해 각 NSX Manager에 대해 세그먼트 ID 풀을 지정해야 합니다. NSX Controller가 현재 환경에 배포되지 않았을 경우 전체 네트워크에서 트래픽을 분산시키고 단일 멀티캐스트 주소가 오버로드되지 않도록 멀티캐스트 주소 범위를 추가해야 합니다.

각 세그먼트 ID 풀의 크기를 결정할 때는 세그먼트 ID 범위에 따라 생성할 수 있는 논리적 스위치의 수가 달라진다는 점을 유념해야 합니다. 사용할 수 있는 1,600만 개의 VNI 중에서 적은 양의 일부를 선택합니다. vCenter는 dvPortgroup의 수를 10,000개로 제한하므로 단일 vCenter에 10,000개가 넘는 VNI를 구성할 수 없습니다.

VXLAN이 다른 NSX 배포에 있는 경우 이미 사용 중인 VNI를 확인하여 VNI가 겹치지 않도록 하십시오. 단일 NSX Manager 및 vCenter 환경에서는 비겹침 VNI가 자동으로 적용됩니다. 로컬 VNI 범위는 겹칠 수 없습니다. 그러나 개별 NSX 배포에서 VNI가 겹치지 않는지 확인하는 것이 중요합니다. 비겹침 VNI는 추적 목적으로 사용하기에 유용하며 크로스 vCenter 환경에 대한 배포 준비를 용이하게 합니다.

전송 영역에서 멀티캐스트 또는 하이브리드 복제 모드를 사용하려는 경우 멀티캐스트 주소 또는 멀티캐스트 주소 범위를 추가해야 합니다.

멀티캐스트 주소 범위를 통해 네트워크에 트래픽을 분산하면 단일 멀티캐스트 주소의 오버로드가 방지되고 BUM 복제가 효과적으로 억제됩니다.

239.0.0.0/24 또는 239.128.0.0/24는 멀티캐스트 주소 범위로 사용하지 마십시오. 이러한 네트워크는 로컬 서브넷 제어에 사용되므로 물리적 스위치가 이 주소를 사용하는 모든 트래픽을 플러딩합니다. 사용할 수 없는 멀티캐스트 주소에 대한 자세한 내용은 <https://tools.ietf.org/html/draft-ietf-mboned-ipv4-mcast-unusable-01> 페이지를 참조하십시오.

VXLAN 멀티캐스트 및 하이브리드 복제 모드가 구성되고 올바르게 작동하는 경우 멀티캐스트 트래픽의 복사본은 IGMP 가입 메시지를 전송한 호스트에만 전송됩니다. 그렇지 않은 경우 물리적 네트워크가 동일한 브로드캐스트 도메인 내의 모든 호스트로 전송되는 모든 멀티캐스트 트래픽을 플러딩합니다. 이러한 플러딩을 방지하려면 다음을 수행해야 합니다.

- 기본 물리적 스위치의 MTU가 1,600 이상으로 구성되었는지 확인합니다.
- 기본 물리적 스위치에 IGMP 스누핑이 올바르게 구성되고 VTEP 트래픽을 전송하는 네트워크 세그먼트에 IGMP 쿼리 발송기가 올바르게 구성되었는지 확인합니다.

- 전송 영역이 권장 멀티캐스트 주소 범위로 구성되었는지 확인합니다. 권장 멀티캐스트 주소 범위는 239.0.1.0/24에서 시작하며 239.128.0.0/24는 제외됩니다.

vSphere Web Client 인터페이스를 사용하여 단일 세그먼트 ID 범위 및 단일 멀티캐스트 주소나 멀티캐스트 주소 범위를 구성할 수 있습니다. 여러 세그먼트 ID 범위 또는 여러 멀티캐스트 주소 값을 구성하려면 NSX API를 사용하여 이 작업을 수행할 수 있습니다. 자세한 내용은 "NSX API 가이드" 항목을 참조하십시오.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **홈 > Networking & Security > 설치(Home > Networking & Security > Installation)**로 이동하고 **논리적 네트워크 준비(Logical Network Preparation)** 탭을 선택합니다.
- 3 **세그먼트 ID > 편집(Segment ID > Edit)**을 클릭합니다.
- 4 세그먼트 ID 범위를 입력합니다(예: 5000–5999).
- 5 (선택 사항) 전송 영역에서 멀티캐스트 또는 하이브리드 복제 모드를 사용하려는 경우 멀티캐스트 주소 또는 멀티캐스트 주소 범위를 추가해야 합니다.
 - a **멀티캐스트 주소 지정 사용(Enable Multicast addressing)** 확인란을 선택합니다.
 - b 멀티캐스트 주소 또는 멀티캐스트 주소 범위(예: 239.0.0.0–239.255.255.255)를 입력합니다.

결과

논리적 스위치를 구성하면 각 논리적 스위치는 풀에서 세그먼트 ID를 수신합니다.

전송 영역 추가

15

전송 영역은 논리적 스위치가 연결할 수 있는 호스트를 제어합니다. 전송 영역은 하나 이상의 **vSphere** 클러스터에 걸쳐 있을 수 있습니다. 전송 영역에서 클러스터를 지정하므로 특정 네트워크 사용에 참여할 수 있는 **VM**도 지정합니다.

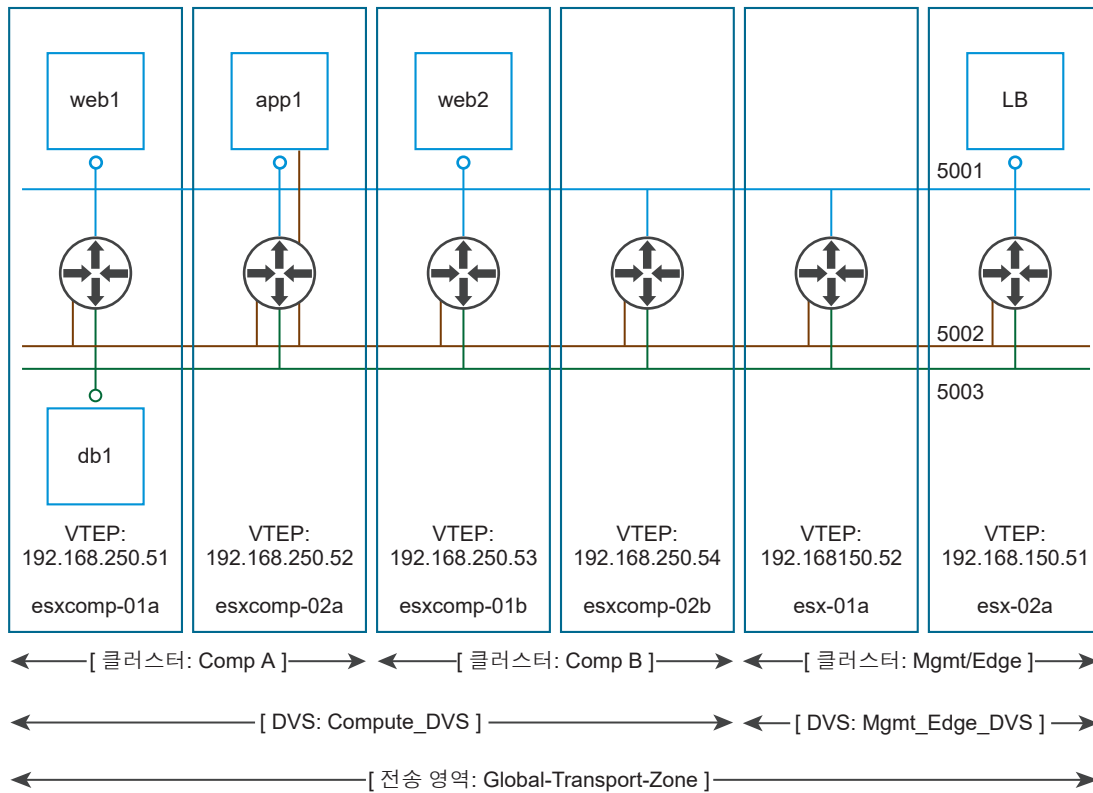
NSX 환경에는 요구 사항에 따라 하나 이상의 전송 영역이 포함될 수 있습니다. 호스트 클러스터는 여러 전송 영역에 속할 수 있습니다. 논리적 스위치는 하나의 전송 영역에만 속할 수 있습니다.

NSX는 다른 전송 영역에 있는 **VM**의 연결을 허용하지 않습니다. 논리적 스위치의 범위는 전송 영역으로 제한되므로 다른 전송 영역에 있는 가상 시스템이 동일한 계층 2 네트워크에 있을 수 없습니다. 논리적 분산 라우터는 다른 전송 영역에 있는 논리적 스위치에 연결할 수 없습니다. 첫 번째 논리적 스위치를 연결하면 동일한 전송 영역에 있는 논리적 스위치만 추가로 선택할 수 있도록 제한됩니다.

전송 영역을 설계하는 데 다음 지침이 도움이 될 수 있습니다.

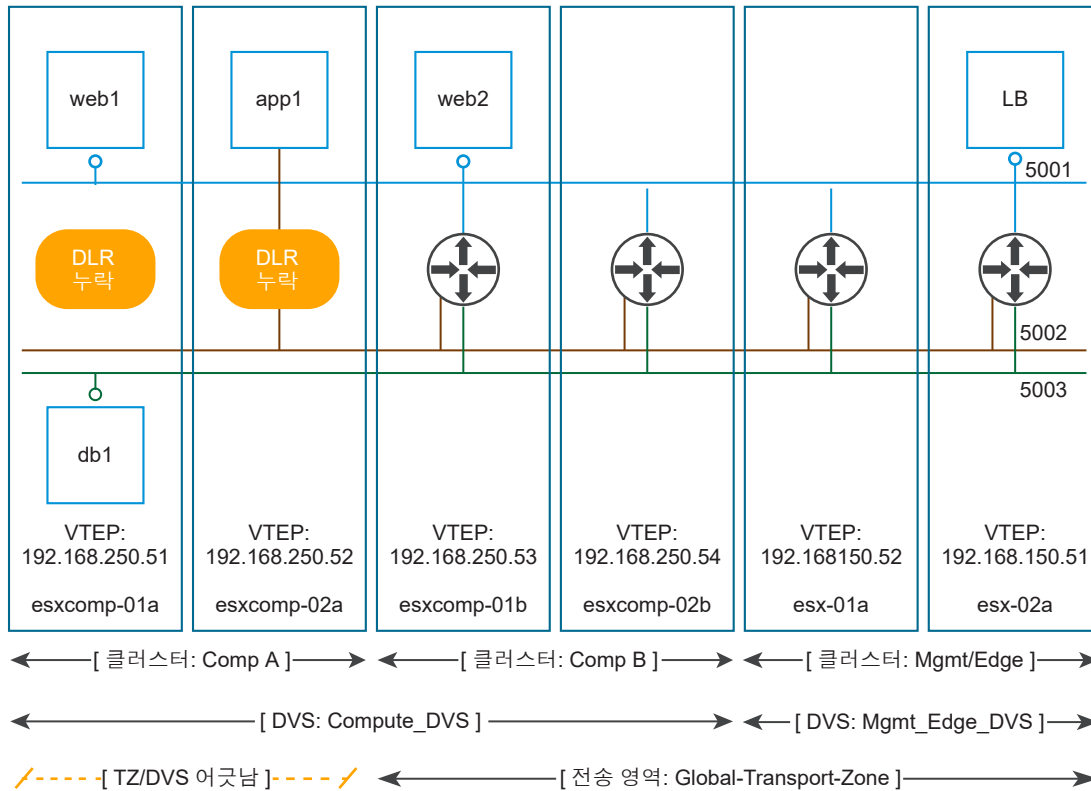
- 클러스터에 계층 3 연결이 필요한 경우 클러스터가 **Edge** 클러스터를 포함하는 전송 영역에 있어야 합니다. **Edge** 클러스터는 계층 3 **Edge** 디바이스(논리적 분산 라우터 및 **ESG(Edge Services Gateway)**)가 있는 클러스터를 의미합니다.
- 2개의 클러스터가 있는데 하나는 웹 서비스용이고 다른 하나는 애플리케이션 서비스용이라고 가정합니다. 이 두 클러스터에 있는 **VM** 간에 **VXLAN** 연결을 생성하려면 두 클러스터가 모두 전송 영역에 포함되어야 합니다.
- 전송 영역에 포함된 모든 논리적 스위치가 전송 영역에 포함된 클러스터 내 모든 **VM**에게 표시되고 이들 **VM**이 사용할 수 있습니다. 클러스터에 보안 환경이 포함된 경우 다른 클러스터의 **VM**이 사용할 수 없도록 만들고자 할 수 있습니다. 대신 더 격리된 전송 영역에 보안 클러스터를 배치할 수 있습니다.
- **vSphere Distributed Switch(VDS 또는 DVS)**의 범위는 전송 영역 범위와 일치해야 합니다. 다중 클러스터 **VDS** 구성에서 전송 영역을 생성할 경우 선택된 **VDS**의 모든 클러스터가 전송 영역에 포함되어 있는지 확인하십시오. 이는 **VDS dvPortgroup**이 사용 가능한 모든 클러스터에서 **DLR**을 사용할 수 있는지 확인하는 것입니다.

다음 다이어그램에서는 **VDS** 경계에 맞게 정렬된 전송 영역을 보여줍니다.



이 모범 사례를 따르지 않는다면 VDS가 둘 이상의 호스트 클러스터에 걸쳐 있고 전송 영역에 이 클러스터 중 하나(또는 하위 집합)만 포함된 경우 이 전송 영역에 포함된 모든 논리적 스위치가 VDS 범위의 모든 클러스터 내 VM에 액세스할 수 있습니다. 즉, 전송 영역에서 논리적 스위치 범위를 클러스터의 하위 집합으로 제한할 수 없습니다. 이 논리적 스위치가 나중에 DLR에 연결할 경우 계층 3 문제를 방지하기 위해 전송 영역에 포함된 클러스터에만 라우터 인스턴스가 생성되는지 확인해야 합니다.

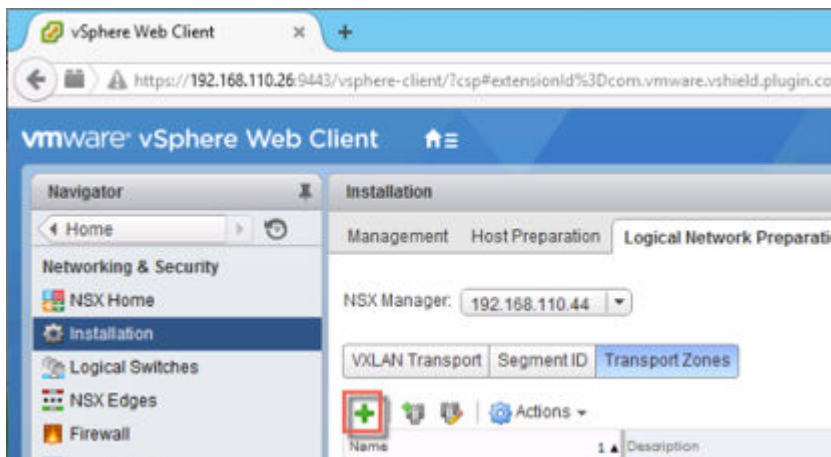
예를 들어 전송 영역이 VDS 경계에 맞춰지지 않은 경우 논리적 스위치의 범위(5001, 5002 및 5003) 및 이 논리적 스위치가 연결된 DLR 인스턴스가 연결 해제되기 때문에 Comp A 클러스터의 VM이 DLR 논리적 인터페이스(LIF)에 액세스할 수 없게 됩니다.



절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **홈 > Networking & Security > 설치(Home > Networking & Security > Installation)**로 이동하고 **논리적 네트워크 준비(Logical Network Preparation)** 탭을 선택합니다.
- 3 **전송 영역(Transport Zones)**을 클릭하고 새 전송 영역(New Transport Zone)(+) 아이콘을 클릭합니다.

예:



- 4 새 전송 영역 대화상자에서 전송 영역의 이름과 설명(선택 사항)을 입력합니다.

5 해당 환경에 컨트롤러 노드가 있는지 또는 멀티캐스트 주소를 사용할지 여부에 따라 제어부 모드를 선택합니다.

- **멀티캐스트(Multicast):** 물리적 네트워크의 멀티캐스트 IP 주소가 제어부에 사용됩니다. 이 모드는 이전 버전의 VXLAN 배포에서 업그레이드하는 경우에만 권장됩니다. 물리적 네트워크에서 PIM/IGMP가 필요합니다.
- **유니캐스트(Unicast):** 제어부가 NSX Controller에서 처리됩니다. 모든 유니캐스트 트래픽에서 최적화된 헤드엔드 복제를 사용합니다. 멀티캐스트 IP 주소 또는 특별한 네트워크 구성이 필요하지 않습니다.
- **하이브리드(Hybrid):** 로컬 트래픽 복제를 물리적 네트워크(L2 멀티캐스트)로 오프로드합니다. 이 모드를 사용하려면 첫 번째 홉 스위치에서 IGMP 스누핑과 각 VTEP 서브넷의 IGMP 쿼리 발송기에 대한 액세스 권한이 필요하지만 PIM은 필요하지 않습니다. 첫 번째 홉 스위치에서 서브넷의 트래픽 복제를 처리합니다.

6 전송 영역에 추가할 클러스터를 선택합니다.

예:

New Transport Zone

Name:

Description:

Replication mode:

- ☐ Multicast
Multicast on Physical network used for VXLAN control plane.
- ☒ Unicast
VXLAN control plane handled by NSX Controller Cluster.
- ☐ Hybrid
Optimized Unicast mode. Offloads local traffic replication to physical network.

Select clusters that will be part of the Transport Zone

	Name	NSX vSwitch	Status
<input checked="" type="checkbox"/>	Compute Cluster A	Compute_DVS	✓ Normal
<input checked="" type="checkbox"/>	Compute Cluster B	Compute_DVS	✓ Normal
<input checked="" type="checkbox"/>	Management and Edge Clust...	Mgmt_VDS	✓ Normal
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			

OK Cancel

다음에 수행할 작업

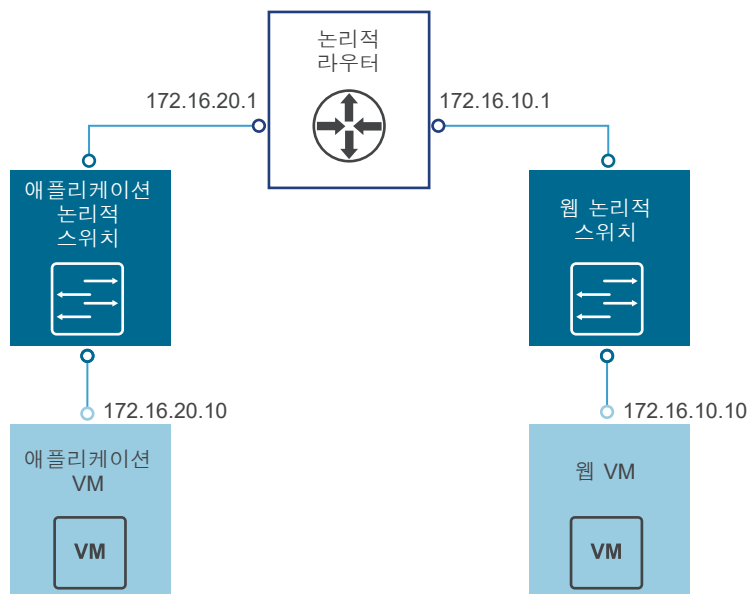
이제 전송 영역이 있고 논리적 스위치를 추가할 수 있습니다.

논리적 스위치 추가

16

NSX for vSphere 논리적 스위치는 기본 하드웨어와 완전히 분리된 가상 환경에서 스위칭 기능(유니캐스트, 멀티캐스트, 브로드캐스트)을 재현합니다. 논리적 스위치는 가상 시스템을 연결할 수 있는 네트워크 연결을 제공한다는 점에서 VLAN과 비슷합니다. VM을 동일한 논리적 스위치에 연결하면 VM이 VXLAN을 통해 다른 VM과 통신할 수 있습니다. 각 논리적 스위치에는 VLAN ID와 같은 세그먼트 ID가 있습니다. 세그먼트 ID는 VLAN ID와 달리 최대 1,600만 개까지 만들 수 있습니다.

논리적 스위치를 추가할 경우 구성하는 특정 토폴로지를 고려해야 합니다. 예를 들어, 다음과 같은 간단한 토폴로지에서는 단일 논리적 분산 라우터(DLR)에 연결된 2개의 논리적 스위치를 보여줍니다. 이 다이어그램에서 각각의 논리적 스위치는 단일 VM에 연결되어 있습니다. 두 개의 VM은 다른 호스트 또는 동일한 호스트에 있거나 다른 호스트 클러스터 또는 동일한 호스트 클러스터에 있을 수 있습니다. DLR에서 VM을 구분하지 않을 경우 VM에 구성된 기본 IP 주소가 동일한 서브넷에 있을 수 있습니다. DLR에서 VM을 구분할 경우 이 예제에 표시된 대로 VM의 IP 주소가 다른 서브넷에 있어야 합니다.



논리적 스위치를 생성할 때 전송 영역 및 복제 모드를 선택하는 것 외에, 2가지 옵션인 IP 검색 및 MAC 학습을 구성합니다.



IP 검색은 개별 VXLAN 세그먼트 내에서, 즉 동일한 논리적 스위치에 연결된 VM 간에 ARP 트래픽 플러딩을 최소화합니다. IP 검색은 기본적으로 사용하도록 설정되어 있습니다.

MAC 학습은 각 vNIC에 VLAN/MAC 쌍 학습 테이블을 구성합니다. 이 테이블은 **dvfilter** 데이터의 일부로 저장됩니다. vMotion 동안 **dvfilter**는 새 위치에서 테이블을 저장하고 복원합니다. 그런 다음 스위치가 테이블의 모든 VLAN/MAC 항목에 대해 RARP를 발급합니다. VLAN을 트렁킹하는 가상 NIC를 사용하는 경우 MAC 학습을 사용하도록 설정하는 것이 좋습니다.

사전 요구 사항

- vSphere Distributed Switch를 구성해야 합니다.
- NSX Manager가 설치되어 있어야 합니다.
- 컨트롤러를 배포해야 합니다.
- NSX용 호스트 클러스터를 준비해야 합니다.
- VXLAN을 구성해야 합니다.
- 세그먼트 ID 풀을 구성해야 합니다.
- 전송 영역을 생성해야 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **홈 > 네트워킹 및 보안 > 논리적 스위치(Home > Networking & Security > Logical Switches)**로 이동합니다.
- 3 **새 논리적 스위치(New Logical Switch)()**를 클릭합니다.
- 4 논리적 스위치의 이름과 설명(선택 사항)을 입력합니다.
- 5 논리적 스위치를 생성할 전송 영역을 선택합니다.
기본적으로 논리적 스위치는 전송 영역에서 제어부 복제 모드를 상속합니다.
- 6 (선택 사항) 전송 영역으로 결정되는 복제 모드를 재정의합니다.
이 모드를 다른 사용 가능한 모드 중 하나로 변경할 수 있습니다. 사용 가능한 모드는 유니캐스트, 하이브리드 및 멀티캐스트입니다.
각각의 논리적 스위치에 대해 상속된 전송 영역의 제어부 복제 모드를 재정의하려고 하는 경우는 생성하는 논리적 스위치가 전송하는 BUM 트래픽의 양적인 면에서 크게 다른 특성이 있을 때입니다. 이 경우 유니캐스트 모드로 사용하는 전송 영역을 생성하고, 각각의 논리적 스위치에 대해 하이브리드 또는 멀티캐스트 모드를 사용할 수 있습니다.
- 7 (선택 사항) ARP 억제를 사용하도록 설정하려면 **IP 검색 사용(Enable IP Discovery)**을 클릭합니다.
- 8 (선택 사항) **MAC 학습 사용(Enable MAC learning)**을 클릭합니다.
- 9 스위치를 선택하고 **가상 시스템 추가(Add Virtual Machine) ()**를 클릭하여 논리적 스위치에 가상 시스템을 연결합니다.

10 하나 이상의 가상 시스템을 선택하고 오른쪽 화살표 버튼 (→)을 클릭합니다.

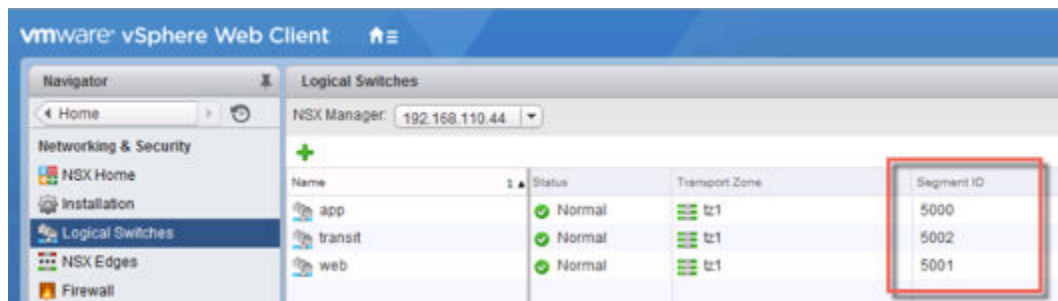
가상 시스템이 [사용 가능한 개체]에서 [선택한 개체]로 이동됩니다.

11 다음(Next)을 클릭하고 각 가상 시스템에 대한 vNIC를 선택합니다. 완료(Finish)를 클릭합니다.

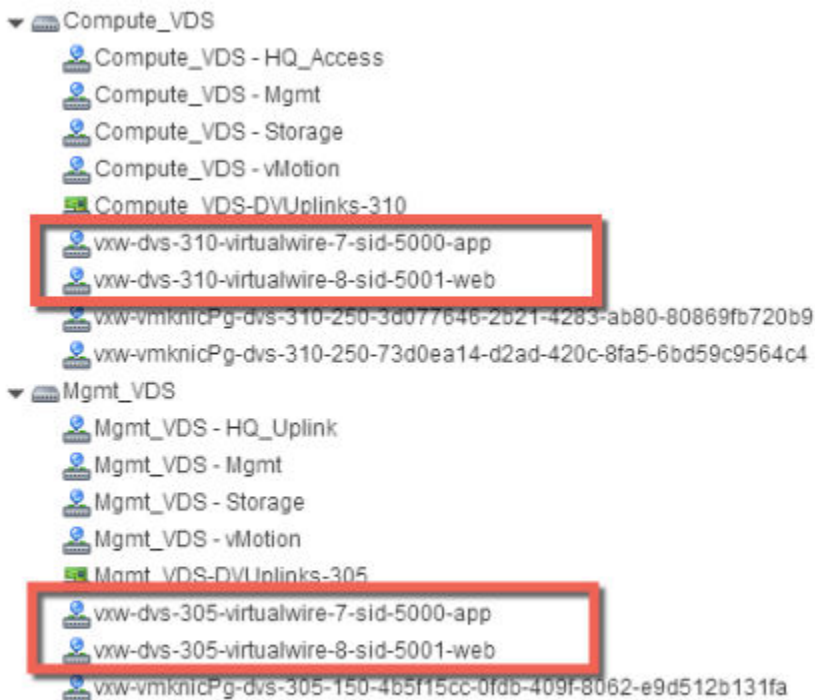
결과

사용자가 생성하는 각각의 논리적 스위치가 세그먼트 ID 풀에서 ID를 수신하고, 가상 와이어가 생성됩니다. 가상 와이어는 각 vSphere Distributed Switch에 생성되는 dvPortgroup입니다. 가상 와이어 설명자에는 논리적 스위치의 이름과 논리적 스위치의 세그먼트 ID가 포함됩니다. 다음 예제에 표시된 것처럼, 할당된 세그먼트 ID가 여러 위치에 표시됩니다.

홈 > 네트워킹 및 보안 > 논리적 스위치(Home > Networking & Security > Logical Switches):

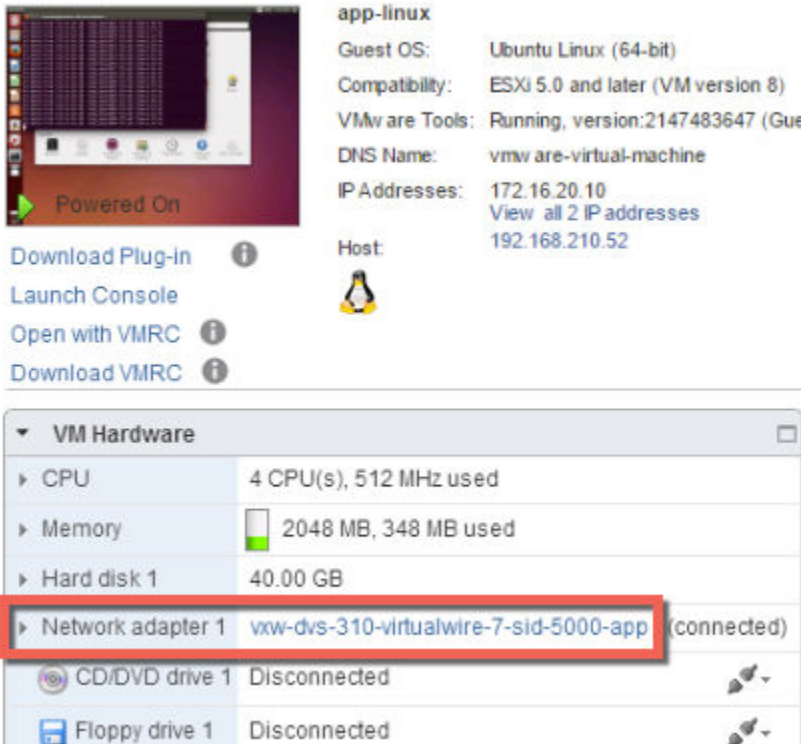


홈 > 네트워킹(Home > Networking):



vSphere Distributed Switch인 Compute_VDS 및 Mgmt_VDS 둘 다에 가상 와이어가 생성됩니다. 이 vSphere Distributed Switch 둘 다가 Web 및 App 논리적 스위치와 연결된 전송 영역의 멤버이기 때문입니다.

홈 > 호스트 및 클러스터 > VM > 요약(Home > Hosts and Clusters > VM > Summary):



논리적 스위치에 연결된 VM을 실행 중인 호스트에서 로그인하고 다음 명령을 실행하여 로컬 VXLAN 구성 및 상태 정보를 조회합니다.

- 호스트별 VXLAN 세부 정보를 표시합니다.

```
~ # esxcli network vswitch dvs vmware vxlan list
```

VDS ID	VDS Name	MTU	Segment ID	Gateway IP
88 eb 0e 50 96 af 1d f1-36 fe c1 ef a1 51 51 49 ff:ff:ff:ff:ff:ff	Compute_VDS	1600	192.168.250.0	192.168.250.1

참고 esxcli network vswitch dvs vmware vxlan 명령에서 "알 수 없는 명령 또는 네임스페이스" 오류 메시지를 생성할 경우 호스트에서 /etc/init.d/hostd restart 명령을 실행한 다음 다시 시도하십시오.

VDS 이름에서 호스트가 연결된 vSphere Distributed Switch를 표시합니다.

세그먼트 ID가 VXLAN에서 사용한 IP 네트워크입니다.

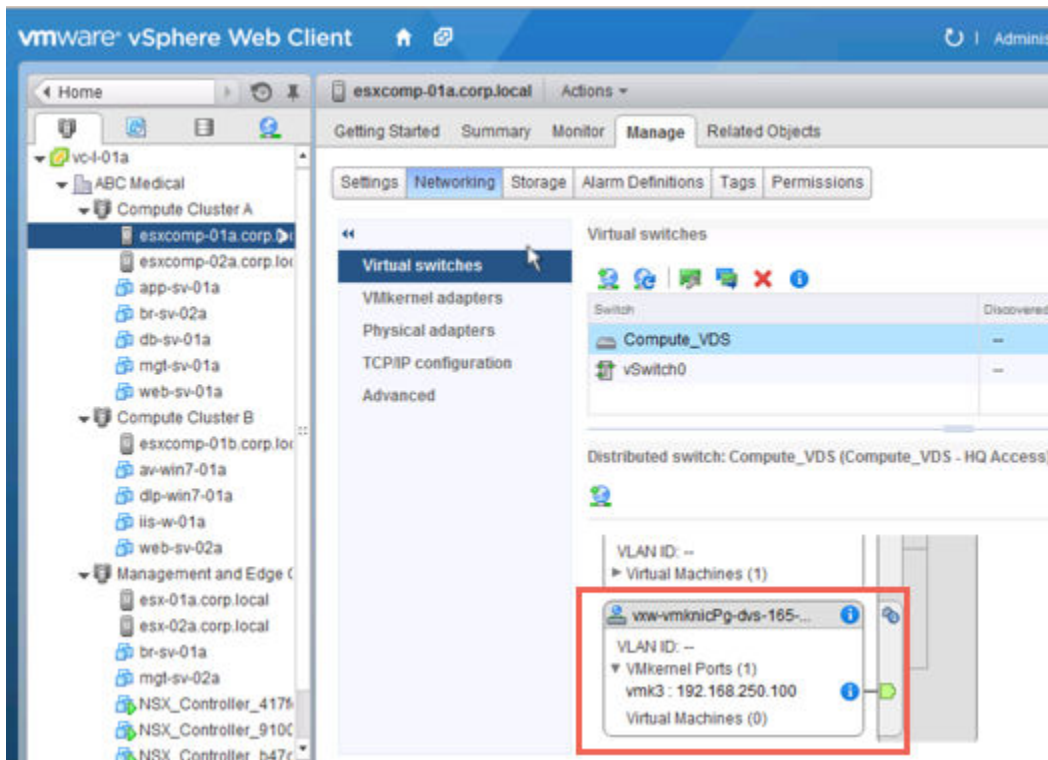
게이트웨이 IP가 VXLAN에서 사용한 게이트웨이 IP 주소입니다.

게이트웨이 MAC 주소는 ff:ff:ff:ff:ff:ff로 남아 있습니다.

DLR이 논리적 스위치에 연결되지 않은 경우 네트워크 수는 0으로 남아 있습니다.

Vmknics 수는 논리적 스위치에 연결된 VM 수와 일치해야 합니다.

- IP VTEP 인터페이스 연결을 테스트하고, VXLAN 캡슐화를 지원하도록 MTU를 늘렸는지 확인합니다. vCenter Web Client에서 호스트의 **관리 > 네트워킹 > 가상 스위치(Manage > Networking > Virtual switches)** 페이지에 있는 vmknics 인터페이스 IP 주소를 Ping합니다.



-d 플래그는 IPv4패킷에서 DF(don't-fragment) 비트를 설정합니다. -s 플래그는 패킷 크기를 설정합니다.

```
root@esxcomp-02a ~ # vmkping ++netstack=vxlan -d -s 1570 192.168.250.100
PING 192.168.250.100 (192.168.250.100): 1570 data bytes
1578 bytes from 192.168.250.100: icmp_seq=0 ttl=64 time=1.294 ms
1578 bytes from 192.168.250.100: icmp_seq=1 ttl=64 time=0.686 ms
1578 bytes from 192.168.250.100: icmp_seq=2 ttl=64 time=0.758 ms

--- 192.168.250.100 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.686/0.913/1.294 ms
~ #
```

```
root@esxcomp-01a ~ # vmkping ++netstack=vxlan -d -s 1570 192.168.250.101
PING 192.168.250.101 (192.168.250.101): 1570 data bytes
1578 bytes from 192.168.250.101: icmp_seq=0 ttl=64 time=0.065 ms
1578 bytes from 192.168.250.101: icmp_seq=1 ttl=64 time=0.118 ms
```

```
--- 192.168.250.101 ping statistics ---  
2 packets transmitted, 2 packets received, 0% packet loss  
round-trip min/avg/max = 0.065/0.091/0.118 ms
```

다음에 수행할 작업

다른 논리적 스위치에 연결된 가상 시스템 간 연결을 사용하도록 설정하려면 논리적(분산) 라우터를 생성하여 논리적 스위치에 연결합니다.

논리적 분산 라우터 추가

17

DLR(논리적 분산 라우터)은 커널 모듈의 데이터부를 각 하이퍼바이저 호스트로 분산하는 한편 라우팅 제어부를 포함하는 가상 장치입니다. DLR 제어부 기능은 NSX Controller 클러스터를 사용하여 라우팅 업데이트를 커널 모듈로 푸시합니다.

새 논리적 라우터를 배포하는 경우 다음을 고려하십시오.

- NSX 버전 6.2 이상에서는 논리적 라우터로 라우팅된 논리적 인터페이스(LIF)를 VLAN에 브리징되는 VXLAN에 연결할 수 있습니다.
- VLAN ID를 0으로 설정한 상태에서 논리적 라우터 인터페이스와 브리징 인터페이스를 dvPortgroup에 연결할 수 없습니다.
- 지정한 논리적 라우터 인스턴스는 다른 전송 영역에 있는 논리적 스위치에 연결할 수 없습니다. 이를 통해 모든 논리적 스위치와 논리적 라우터 인스턴스가 정렬됩니다.
- 논리적 라우터가 둘 이상의 VDS(vSphere Distributed Switch)에 걸쳐 있는 논리적 스위치에 연결된 경우 VLAN 지원 포트 그룹에 연결할 수 없습니다. 따라서 논리적 라우터 인스턴스가 여러 호스트에 있는 논리적 스위치 dvPortgroups에 올바르게 매핑될 수 있습니다.
- 두 개의 네트워크가 동일한 vSphere Distributed Switch에 있는 경우 동일한 VLAN ID를 가진 두 개의 다른 분산 포트 그룹(dvPortgroups)에서 논리적 라우터 인터페이스를 생성하면 안 됩니다.
- 두 개의 네트워크가 다른 vSphere Distributed Switch에 있지만 두 개의 vSphere Distributed Switch가 동일한 호스트를 공유할 경우 동일한 VLAN ID를 가진 두 개의 다른 dvPortgroups에서 논리적 라우터 인터페이스를 생성하면 안 됩니다. 즉 두 개의 dvPortgroups이 두 개의 다른 vSphere Distributed Switch에 있는 경우 vSphere Distributed Switch가 호스트를 공유하지 않는 한 동일한 VLAN ID를 가진 두 개의 다른 네트워크에서 논리적 라우터 인터페이스를 생성할 수 있습니다.
- VXLAN이 구성된 경우, 논리적 라우터 인터페이스를 vSphere VXLAN이 구성된 vSphere Distributed Switch의 분산 포트 그룹에 연결해야 합니다. 논리적 라우터 인터페이스를 다른 vSphere Distributed Switch의 포트 그룹에 연결하지 마십시오.

다음 목록에서는 논리적 라우터의 인터페이스 유형(업링크 및 내부)별로 지원되는 기능을 설명합니다.

- 동적 라우팅 프로토콜(BGP 및 OSPF)은 업링크 인터페이스에서만 지원됩니다.
- 방화벽 규칙은 업링크 인터페이스에서만 적용 가능하고 Edge 가상 장치로 전송되는 제어 및 관리 트래픽으로 제한됩니다.

- DLR 관리 인터페이스에 대한 자세한 내용은 기술 자료 문서 "관리 인터페이스 가이드: DLR 제어 VM - NSX" <http://kb.vmware.com/kb/2122060>을 참조하십시오.

사전 요구 사항

- **엔터프라이즈 관리자** 또는 **NSX 관리자** 역할을 할당받아야 합니다.
- NSX 논리적 스위치를 생성할 계획이 없어도 로컬 세그먼트 ID 풀을 생성해야 합니다.
- 논리적 라우터 구성을 생성하거나 변경하기 전에 컨트롤러 클러스터가 최신 상태이고 사용 가능한지 확인하십시오. 논리적 라우터는 NSX Controller를 사용하지 않으면 라우팅 정보를 호스트에 배포할 수 없습니다. 논리적 라우터는 NSX Controller를 사용하여 작동하는 반면, ESG(Edge Services Gateway)는 NSX Controller를 사용하지 않습니다.
- 논리적 라우터가 VLAN dvPortgroup에 연결될 경우 논리적 라우터 장치가 설치된 모든 하이퍼바이저 호스트가 UDP 포트 6999에서 서로 연결할 수 있는지 확인하십시오. 논리적 라우터 VLAN 기반 ARP 프로세스가 작동하려면 이 포트에서 통신할 수 있어야 합니다.
- 논리적 라우터 장치를 배포할 위치를 확인합니다.
 - 대상 호스트는 새 논리적 라우터의 인터페이스에 연결된 논리적 스위치와 동일한 전송 영역에 속해야 합니다.
 - ECMP 설정에서 ESG를 사용하는 경우 하나 이상의 업스트림 ESG와 동일한 호스트에 배치하지 않도록 합니다. DRS 반선회도 규칙을 사용하여 이를 적용함으로써 논리적 라우터 전달에 대한 호스트 실패의 영향을 줄일 수 있습니다. 업스트림 ESG가 하나 있거나 HA 모드인 경우 이 지침이 적용되지 않습니다. 자세한 내용은 <https://communities.vmware.com/docs/DOC-27683>에 있는 "VMware NSX for vSphere 네트워크 가상화 설계 가이드"를 참조하십시오.
- 논리적 라우터 장치를 설치하는 호스트 클러스터에서 NSX 사용 준비가 되었는지 확인하십시오. "NSX 설치 가이드"에서 "NSX에 대한 호스트 클러스터 준비"를 참조하십시오.

절차

- 1 vSphere Web Client에서 **홈 > 네트워킹 및 보안 > NSX Edge(Home > Networking & Security > NSX Edges)**로 이동합니다.
- 2 **추가(Add)(+)** 아이콘을 클릭합니다.
- 3 **논리적 (분산) 라우터(Logical (Distributed) Router)**를 선택하고 디바이스 이름을 입력합니다.

이 이름은 vCenter 인벤토리에 나타납니다. 단일 테넌트 내의 모든 논리적 라우터에서 고유한 이름을 사용하십시오.

필요한 경우 호스트 이름을 입력할 수도 있습니다. 이 이름이 CLI에 표시됩니다. 호스트 이름을 입력하지 않으면 자동으로 생성되는 Edge ID가 CLI에 표시됩니다.

필요한 경우 설명과 테넌트를 입력할 수 있습니다.

예:

Name and description

Install Type: ☐ Edge Services Gateway
Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.

☒ Logical (Distributed) Router
Provides Distributed Routing and Bridging capabilities.

Name: * logical-distributed-router1

Hostname:

Description:

Tenant:

☒ Deploy Edge Appliance
Deploys NSX Edge Appliance to support Firewall and Dynamic routing.

☐ Enable High Availability
Enable HA, for enabling and configuring High Availability.

4 (선택 사항) Edge Appliance를 배포합니다.

Edge Appliance 배포(Deploy Edge Appliance)가 기본적으로 선택됩니다. 논리적 라우터 ping, SSH 액세스 및 동적 라우팅 트래픽에 적용되는 동적 라우팅 및 논리적 라우터 장치의 방화벽에는 Edge Appliance(논리적 라우터 가상 장치라고도 함)가 필요합니다.

정적 경로만 필요하고 Edge Appliance를 배포하지 않을 경우 Edge Appliance 옵션을 선택 취소할 수 있습니다. 논리적 라우터를 생성한 후 Edge Appliance를 논리적 라우터에 추가할 수 없습니다.

5 (선택 사항) 고가용성을 사용하도록 설정합니다.

고가용성 사용(Enable High Availability)은 기본적으로 선택되어 있지 않습니다. HA(고가용성)를 사용하도록 설정하고 구성하려면 **고가용성 사용(Enable High Availability)** 확인란을 선택합니다. 동적 라우팅 수행을 계획하는 경우 고가용성이 필요합니다.

6 논리적 라우터의 암호를 입력하고 다시 입력합니다.

암호는 12 ~ 255자여야 하고 다음을 포함해야 합니다.

- 하나 이상의 대문자
- 하나 이상의 소문자
- 숫자 1개 이상
- 하나 이상의 특수 문자

7 (선택 사항) SSH를 사용하도록 설정합니다.

기본적으로 **SSH**는 사용하지 않도록 설정되어 있습니다. **SSH**를 사용하도록 설정하지 않은 경우 가상 장치 콘솔을 열어 논리적 라우터에 액세스할 수 있습니다. 여기서 **SSH**를 사용하도록 설정하면 **SSH** 프로세스가 논리적 라우터 가상 장치에서 실행됩니다. 논리적 라우터의 프로토콜 주소에 대한 **SSH** 액세스를 허용하려면 논리적 라우터 방화벽 구성을 수동으로 조정해야 합니다. 논리적 라우터에서 동적 라우팅을 구성할 때 프로토콜 주소가 구성됩니다.

8 (선택 사항) FIPS 모드를 사용하도록 설정하고 로그 수준을 설정합니다.

기본적으로 **FIPS** 모드는 사용하지 않도록 설정되어 있습니다. **FIPS 모드 사용(Enable FIPS mode)** 확인란을 선택하여 **FIPS** 모드를 사용하도록 설정합니다. **FIPS** 모드를 사용하도록 설정하면 **NSX Edge**와의 모든 보안 통신에 **FIPS**에서 허용하는 암호화 알고리즘 또는 프로토콜이 사용됩니다.

기본적으로 로그 수준은 긴급입니다.

예:

The screenshot shows the 'Settings' page for the NSX Edge appliance. It includes a warning about CLI credentials being set on the appliance. Below this, there are input fields for 'User Name' (set to 'admin'), 'Password', and 'Confirm password'. There are two checkboxes: 'Enable SSH access' and 'Enable FIPS mode', both of which are currently unchecked. At the bottom, there is a dropdown menu for 'Edge Control Level Logging' set to 'EMERGENCY', with a link below it that says 'Set the Edge Control Level Logging'.

9 배포를 구성합니다.

- ◆ **Edge Appliance 배포(Deploy Edge Appliance)**를 선택하지 않은 경우 **추가(Add)(+)** 아이콘이 회색으로 표시됩니다. 구성을 계속하려면 **다음(Next)**을 클릭합니다.
- ◆ **Edge Appliance 배포(Deploy Edge Appliance)**를 선택한 경우 논리적 라우터 가상 장치에 대한 설정을 입력합니다.

예:

Add NSX Edge Appliance

Specify placement parameters for the NSX Edge appliance.

Cluster/Resource Pool:	*	Management & Edge ...	▼
Datastore:	*	ds-1	▼
Host:		esxmgt-01a.corp.local	▼
Folder:		Discovered virtual mac...	▼

10 인터페이스를 구성합니다. 논리적 라우터에서는 IPv4 주소 지정만 지원됩니다.

- a HA 인터페이스 연결을 구성하고 필요한 경우 IP 주소도 구성합니다.

Edge Appliance 배포(Deploy Edge Appliance)를 선택한 경우 HA 인터페이스를 분산 포트 그룹 또는 논리적 스위치에 연결해야 합니다. 이 인터페이스를 HA 인터페이스로만 사용하는 경우 논리적 스위치를 사용합니다. /30 서브넷이 링크 로컬 범위 169.254.0.0/16에서 할당되고 두 NSX Edge 장치 각각의 IP 주소를 제공하는 데 사용됩니다.

필요에 따라 이 인터페이스를 사용하여 NSX Edge에 연결할 경우 HA 인터페이스에 대한 추가 IP 주소 및 접두사를 지정할 수 있습니다.

참고 NSX 6.2 이전에는 HA 인터페이스를 관리 인터페이스라고 지칭했습니다. HA 인터페이스와 동일한 IP 서브넷에 없는 모든 위치에서 HA 인터페이스로 SSH할 수 없습니다. HA 인터페이스를 가리키는 정적 경로를 구성할 수 없으므로, RPF가 들어오는 트래픽을 삭제하게 됩니다. 이론상 RPF를 사용하지 않도록 설정할 수 있지만 이런 경우 고가용성에는 역효과를 낼 수 있습니다. SSH 액세스의 경우 동적 라우팅을 구성할 때 나중에 구성되는 논리적 라우터의 프로토콜 주소를 사용할 수도 있습니다.

NSX 6.2 이상에서는 논리적 라우터의 HA 인터페이스가 경로 재배포에서 자동으로 제외됩니다.

- b 이 NSX Edge의 인터페이스를 구성합니다.

이 NSX Edge의 인터페이스 구성(Configure interfaces of this NSX Edge)에서 내부 인터페이스는 VM 대 VM 통신(때로 동-서 통신이라고도 함)을 허용하는 스위치에 연결하기 위한 것입니다. 논리적 라우터 가상 장치에서 내부 인터페이스가 유사 vNIC로 생성됩니다. 업링크 인터페이스는 북-남 통신용입니다. 논리적 라우터 업링크 인터페이스는 Edge Services Gateway 또는 타사 라우터 VM에 연결할 수 있습니다. 동적 라우팅이 작동하려면 업링크 인터페이스가 하나 이상 있어야 합니다. 논리적 라우터 가상 장치에서 업링크 인터페이스가 vNIC로 생성됩니다.

여기서 입력하는 인터페이스 구성을 나중에 수정할 수 있습니다. 논리적 라우터가 배포된 후 인터페이스를 추가, 제거 및 수정할 수 있습니다.

다음 예제에서는 관리 분산 포트 그룹에 연결된 HA 인터페이스를 보여줍니다. 또한 2개의 내부 인터페이스(app 및 web)와 업링크 인터페이스(to-ESG)를 보여줍니다.

New NSX Edge

1 Name and description

2 Settings

3 Configure deployment

4 Configure interfaces

5 Default gateway settings

6 Ready to complete

Configure interfaces

HA interface Configuration

Connected To: [Change](#) [Remove](#)

+

x

IP Address	Subnet Prefix Length
192.168.110.60*	24

HA interface is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.

Configure interfaces of this NSX Edge

+

x

Name	IP Address	Subnet Prefix Length	Connected To
app	172.16.20.1*	24	app
web	172.16.10.1*	24	web
to-ESG	192.168.10.2*	29	transit

Back

Next

Finish

Cancel

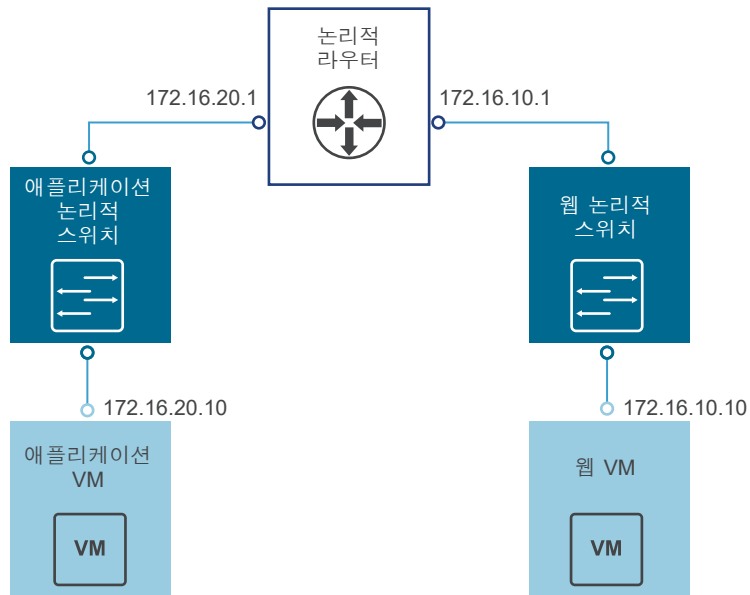
11 기본 게이트웨이를 구성합니다.

예:

12 논리적 스위치에 연결된 VM의 기본 게이트웨이가 논리적 라우터 인터페이스 IP 주소로 올바르게 설정되어 있는지 확인하십시오.

결과

다음 예제 토폴로지에서 App VM의 기본 게이트웨이는 172.16.20.1이고 웹 VM의 기본 게이트웨이는 172.16.10.1입니다. VM이 해당 기본 게이트웨이 및 서로를 Ping할 수 있는지 확인하십시오.



SSH 또는 콘솔을 사용하여 NSX Manager에 연결하고 다음 명령을 실행합니다.

- 모든 논리적 라우터 인스턴스 정보를 나열합니다.

```

nsxmgr-l-01a> show logical-router list all
Edge-id          Vdr Name          Vdr id          #Lifs
edge-1           default+edge-1    0x00001388      3
  
```

- 컨트롤러 클러스터에서 논리적 라우터에 대한 라우팅 정보를 수신한 호스트를 나열합니다.

```

nsxmgr-l-01a> show logical-router list dlr edge-1 host
ID              HostName
host-25         192.168.210.52
host-26         192.168.210.53
host-24         192.168.110.53
  
```

지정한 논리적 라우터(이 예제에서는 **edge-1**)에 연결된 논리적 스위치를 소유하는 전송 영역의 멤버로 구성된 모든 호스트 클러스터의 모든 호스트가 출력에 포함됩니다.

- 논리적 라우터가 호스트에 전달하는 라우팅 테이블 정보를 나열합니다. 모든 호스트에서 라우팅 테이블 항목이 일치해야 합니다.

```

nsx-mgr-l-01a> show logical-router host host-25 dlr edge-1 route
  
```

VDR default+edge-1 Route Table

Legend: [U: Up], [G: Gateway], [C: Connected], [I: Interface]

Legend: [H: Host], [F: Soft Flush] [!: Reject] [E: ECMP]

Destination	GenMask	Gateway	Flags	Ref	Origin	UpTime	Interface
0.0.0.0	0.0.0.0	192.168.10.1	UG	1	AUTO	4101	138800000002

172.16.10.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10195	13880000000b
172.16.20.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10196	13880000000a
192.168.10.0	255.255.255.248	0.0.0.0	UCI	1	MANUAL	10196	138800000002
192.168.100.0	255.255.255.0	192.168.10.1	UG	1	AUTO	3802	138800000002

- 호스트 중 하나의 관점에서 라우터에 대한 추가 정보를 나열합니다. 이 출력은 호스트와 통신하고 있는 컨트롤러를 확인하는 데 유용합니다.

```
nsx-mgr-l-01a> show logical-router host host-25 dlr edge-1 verbose
```

VDR Instance Information :

```
-----
Vdr Name:                default+edge-1
Vdr Id:                  0x00001388
Number of Lifs:          3
Number of Routes:        5
State:                   Enabled
Controller IP:           192.168.110.203
Control Plane IP:        192.168.210.52
Control Plane Active:     Yes
Num unique nexthops:     1
Generation Number:       0
Edge Active:             No
```

show logical-router host host-25 dlr edge-1 verbose 명령의 출력에서 컨트롤러 IP 필드를 확인합니다.

컨트롤러에 SSH하고, 다음 명령을 실행하여 컨트롤러의 확인된 VNI, VTEP, MAC 및 ARP 테이블 상태 정보를 표시합니다.

- 192.168.110.202 # show control-cluster logical-switches vni 5000
- | VNI | Controller | BUM-Replication | ARP-Proxy | Connections |
|------|-----------------|-----------------|-----------|-------------|
| 5000 | 192.168.110.201 | Enabled | Enabled | 0 |

VNI 5000에 대한 출력에서 제로 연결을 표시하고 컨트롤러 192.168.110.201을 VNI 5000의 소유자로 나열합니다. 해당 컨트롤러에 로그인하여 VNI 5000에 대한 추가 정보를 수집합니다.

```
192.168.110.201 # show control-cluster logical-switches vni 5000
```

VNI	Controller	BUM-Replication	ARP-Proxy	Connections
5000	192.168.110.201	Enabled	Enabled	3

192.168.110.201에 대한 출력에서 세 개 연결을 표시합니다. 추가 VNI를 확인합니다.

```
192.168.110.201 # show control-cluster logical-switches vni 5001
```

VNI	Controller	BUM-Replication	ARP-Proxy	Connections
5001	192.168.110.201	Enabled	Enabled	3

```
192.168.110.201 # show control-cluster logical-switches vni 5002
```

VNI	Controller	BUM-Replication	ARP-Proxy	Connections
5002	192.168.110.201	Enabled	Enabled	3

192.168.110.201에서 3개의 VNI 연결을 모두 소유하기 때문에 다른 컨트롤러 192.168.110.203에서 연결이 표시되지 않을 것입니다.

```
192.168.110.203 # show control-cluster logical-switches vni 5000
VNI      Controller      BUM-Replication ARP-Proxy Connections
5000     192.168.110.201 Enabled             Enabled      0
```

- MAC 및 ARP 테이블을 확인하기 전에 하나의 VM에서 다른 VM으로 ping합니다.

App VM에서 웹 VM으로:

```
vmware@app-vm$ ping 172.16.10.10
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=64 time=2.605 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=64 time=1.490 ms
64 bytes from 172.16.10.10: icmp_req=3 ttl=64 time=2.422 ms
```

MAC 테이블을 확인합니다.

```
192.168.110.201 # show control-cluster logical-switches mac-table 5000
VNI      MAC                  VTEP-IP      Connection-ID
5000     00:50:56:a6:23:ae 192.168.250.52 7
```

```
192.168.110.201 # show control-cluster logical-switches mac-table 5001
VNI      MAC                  VTEP-IP      Connection-ID
5001     00:50:56:a6:8d:72 192.168.250.51 23
```

ARP 테이블을 확인합니다.

```
192.168.110.201 # show control-cluster logical-switches arp-table 5000
VNI      IP                   MAC                  Connection-ID
5000     172.16.20.10        00:50:56:a6:23:ae 7
```

```
192.168.110.201 # show control-cluster logical-switches arp-table 5001
VNI      IP                   MAC                  Connection-ID
5001     172.16.10.10        00:50:56:a6:8d:72 23
```

논리적 라우터 정보를 확인합니다. 각 논리적 라우터 인스턴스를 컨트롤러 노드 중 하나가 사용합니다.

`show control-cluster logical-routers` 명령의 `instance` 하위 명령에서 이 컨트롤러에 연결된 논리적 라우터 목록을 표시합니다.

`interface-summary` 하위 명령에서 컨트롤러가 NSX Manager에서 확인한 LIF를 표시합니다. 전송 영역에서 관리되는 호스트 클러스터에 있는 호스트로 이 정보가 전송됩니다.

routes 하위 명령에서 논리적 라우터의 가상 장치(컨트롤 VM이라고도 함)가 이 컨트롤러에 전송한 라우팅 테이블을 표시합니다. ESXi 호스트에서와 달리 이 라우팅 테이블에는 직접 연결된 서브넷은 포함되지 않습니다. 이 정보는 LIF 구성에서 제공하기 때문입니다. ESXi 호스트에 대한 경로 정보에는 직접 연결된 서브넷이 포함됩니다. 이 경우 ESXi 호스트의 데이터 경로에서 사용한 전달 테이블이기 때문입니다.

- 이 컨트롤러에 연결된 모든 논리적 라우터를 나열합니다.

```
controller # show control-cluster logical-routers instance all
LR-Id      LR-Name      Universal Service-Controller Egress-Locale
0x1388     default+edge-1  false      192.168.110.201  local
```

LR-Id를 기록하고 이를 다음 명령에서 사용하십시오.

- controller # show control-cluster logical-routers interface-summary 0x1388

Interface	Type	Id	IP[]
13880000000b	vxlan	0x1389	172.16.10.1/24
13880000000a	vxlan	0x1388	172.16.20.1/24
138800000002	vxlan	0x138a	192.168.10.2/29

- controller # show control-cluster logical-routers routes 0x1388

Destination	Next-Hop[]	Preference	Locale-Id	Source
192.168.100.0/24	192.168.10.1	110	00000000-0000-0000-0000-000000000000	CONTROL_VM
0.0.0.0/0	192.168.10.1	0	00000000-0000-0000-0000-000000000000	CONTROL_VM

```
[root@comp02a:~] esxcfg-route -l
```

VMkernel Routes:

Network	Netmask	Gateway	Interface
10.20.20.0	255.255.255.0	Local Subnet	vmk1
192.168.210.0	255.255.255.0	Local Subnet	vmk0
default	0.0.0.0	192.168.210.1	vmk0

- 특정 VNI에 대한 컨트롤러 연결을 표시합니다.

```
192.168.110.203 # show control-cluster logical-switches connection-table 5000
Host-IP      Port  ID
192.168.110.53 26167 4
192.168.210.52 27645 5
192.168.210.53 40895 6
```

```
192.168.110.202 # show control-cluster logical-switches connection-table 5001
Host-IP      Port  ID
192.168.110.53 26167 4
192.168.210.52 27645 5
192.168.210.53 40895 6
```

이 호스트-IP 주소는 VTEP가 아니라 vmk0 인터페이스입니다. ESXi 호스트와 컨트롤러 간의 연결이 관리 네트워크에 생성됩니다. 여기서 포트 번호는 호스트가 컨트롤러와 연결을 설정할 때 ESXi 호스트 IP 스택에서 할당하는 사용 후 삭제 TCP 포트입니다.

- 호스트에서 포트 번호와 일치하는 컨트롤러 네트워크 연결을 확인할 수 있습니다.

```
[root@192.168.110.53:~] #esxcli network ip connection list | grep 26167
tcp          0      0 192.168.110.53:26167      192.168.110.101:1234    ESTABLISHED
96416 newreno netcpa-worker
```

- 호스트의 활성 VNI를 표시합니다. 호스트에서 출력이 어떻게 다른지 관찰합니다. 모든 VNI가 모든 호스트에서 활성화되어 있는 것은 아닙니다. 논리적 스위치에 연결된 VM이 호스트에 있는 경우 VNI가 호스트에서 활성화되어 있습니다.

```
[root@192.168.210.52:~] # esxcli network vswitch dvs vmware vxlan network list --vds-name
Compute_VDS
```

VXLAN ID	Multicast IP	Control Plane	Controller Connection
Port Count	MAC Entry Count	ARP Entry Count	VTEP Count
5000	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.203
(up)	1	0	0
5001	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.202
(up)	1	0	0

참고 vSphere 6.0 이상에서 vxlan 네임스페이스를 사용하도록 설정하려면 `/etc/init.d/hostd restart` 명령을 실행하십시오.

하이브리드 모드나 유니캐스트 모드에 있는 논리적 스위치의 경우 `esxcli network vswitch dvs vmware vxlan network list --vds-name <vds-name>` 명령에 다음 출력이 포함됩니다.

- 제어부는 사용하도록 설정되어 있습니다.
- 멀티캐스트 프록시 및 ARP 프록시가 나열됩니다. IP 검색을 사용하지 않도록 설정한 경우에도 AARP 프록시가 나열됩니다.
- 유효한 컨트롤러 IP 주소가 나열되고 연결이 실행 중입니다.
- 논리적 라우터가 ESXi 호스트에 연결된 경우 논리적 스위치에 연결된 호스트에 VM이 없더라도 포트 수는 최소 1입니다. 이 포트는 ESXi 호스트의 논리적 라우터 커널 모듈에 연결된 특수한 dvPort 인 vdrPort입니다.

- 먼저 VM에서 다른 서브넷의 다른 VM으로 Ping한 다음, MAC 테이블을 표시합니다. 내부 MAC은 VM 항목이고, 외부 MAC과 외부 IP는 VTEP를 참조합니다.

```
~ # esxcli network vswitch dvs vmware vxlan network mac list --vds-name=Compute_VDS --vxlan-id=5000
```

Inner MAC	Outer MAC	Outer IP	Flags
00:50:56:a6:23:ae	00:50:56:6a:65:c2	192.168.250.52	00000111

```
~ # esxcli network vswitch dvs vmware vxlan network mac list --vds-name=Compute_VDS --vxlan-id=5001
```

Inner MAC	Outer MAC	Outer IP	Flags
02:50:56:56:44:52	00:50:56:6a:65:c2	192.168.250.52	00000101
00:50:56:f0:d7:e4	00:50:56:6a:65:c2	192.168.250.52	00000111

다음에 수행할 작업

NSX Edge 장치를 설치할 때 vSphere HA가 클러스터에서 사용되지 않도록 설정되어 있으면 NSX는 호스트에서 자동 VM 시작/종료를 사용하도록 설정합니다. 장치 VM이 나중에 클러스터의 다른 호스트로 마이그레이션되는 경우 새 호스트가 자동 VM 시작/종료를 사용하도록 설정하지 않을 수도 있습니다. 이러한 이유로 vSphere HA가 사용되지 않도록 설정된 클러스터에서 NSX Edge 장치를 설치할 때는 클러스터의 모든 호스트를 점검하여 자동 VM 시작/종료가 사용되도록 설정되어 있는지 확인해야 합니다. "vSphere 가상 시스템 관리"에서 "가상 시스템 시작 및 종료 설정 편집"을 참조하십시오.

논리적 라우터가 배포된 후 논리적 라우터 ID를 두 번 클릭하여 인터페이스, 라우팅, 방화벽, 브리징 및 DHCP 릴레이 같은 추가 설정을 구성합니다.

Edge Services Gateway 추가

18

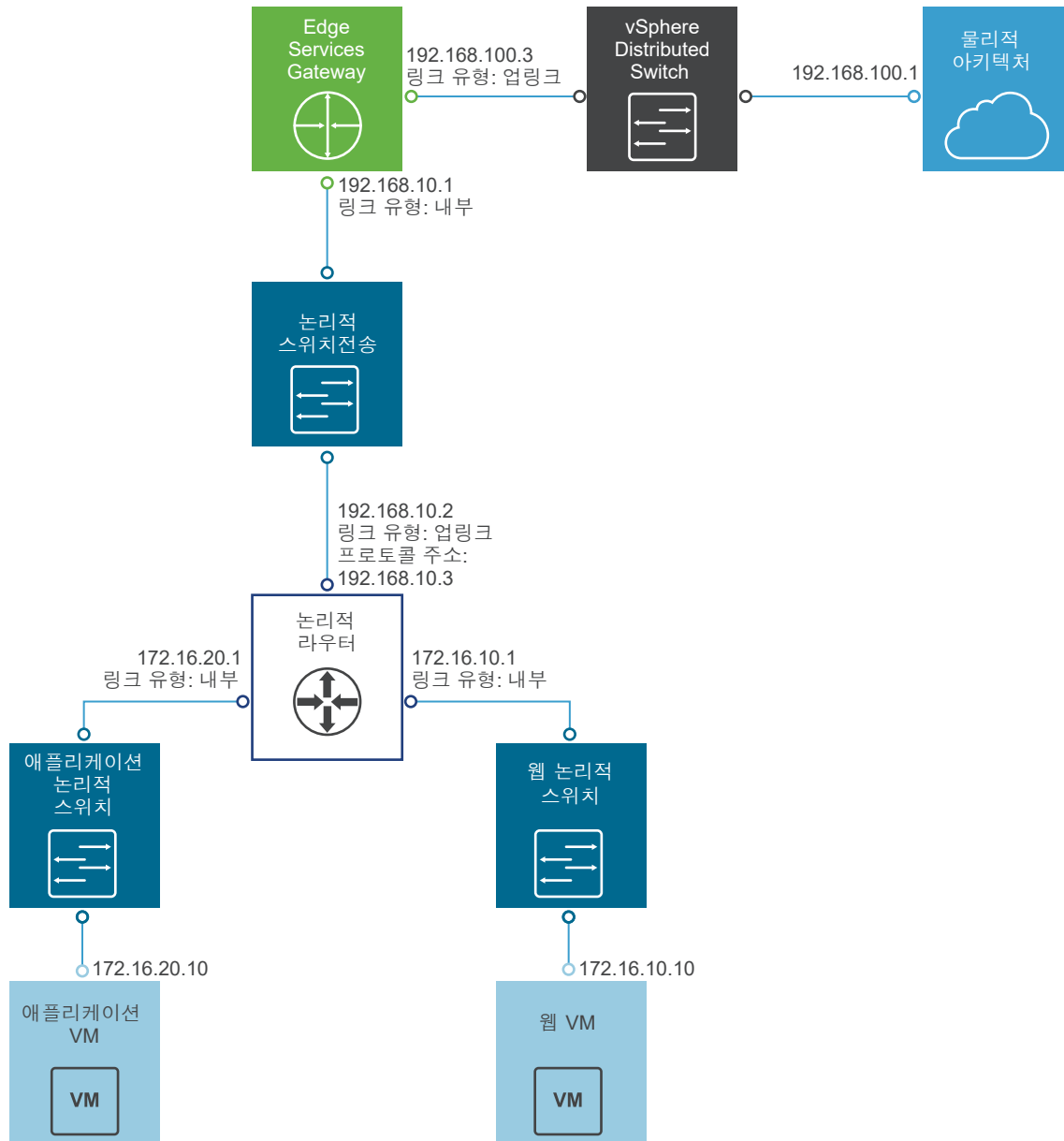
데이터 센터에 여러 **NSX Edge Services Gateway** 가상 장치를 설치할 수 있습니다. 각 **NSX Edge** 가상 장치는 총 **10**개의 업링크 및 내부 네트워크 인터페이스를 사용할 수 있습니다. 내부 인터페이스는 보안 포트 그룹에 연결하여 포트 그룹에 있는 모든 보호된 가상 시스템의 게이트웨이 역할을 합니다. 내부 인터페이스에 할당된 서브넷은 라우팅된 공용 **IP** 주소 공간이거나 **NAT**가 적용된/라우팅된 **RFC 1918** 전용 공간일 수 있습니다. 인터페이스 간의 트래픽에는 방화벽 규칙 및 기타 **NSX Edge** 서비스가 적용됩니다.

ESG의 업링크 인터페이스는 업링크 포트 그룹에 연결하여 액세스 계층 네트워킹을 제공하는 서비스나 공유 회사 네트워크에 액세스할 수 있습니다.

다음 목록에서는 **ESG**에서 인터페이스 유형(내부 및 업링크)별로 지원되는 기능을 설명합니다.

- **DHCP**: 업링크 인터페이스에서 지원되지 않습니다.
- **DNS 전달자**: 업링크 인터페이스에서 지원되지 않습니다.
- **HA**: 업링크 인터페이스에서 지원되지 않고, 하나 이상의 내부 인터페이스가 필요합니다.
- **SSL VPN**: 수신기 **IP**가 업링크 인터페이스에 속해야 합니다.
- **IPSec VPN**: 로컬 사이트 **IP**가 업링크 인터페이스에 속해야 합니다.
- **L2 VPN**: 내부 네트워크만 확장할 수 있습니다.

다음 그림에서는 **vSphere Distributed Switch**를 통해 물리적 인프라에 연결된 **ESG**의 업링크 인터페이스와 **NSX** 논리적 전송 스위치를 통해 **NSX** 논리적 라우터에 연결된 **ESG**의 내부 인터페이스가 포함된 샘플 토폴로지를 보여줍니다.



로드 밸런싱, 사이트 간 VPN 및 NAT 서비스에는 외부 IP 주소를 여러 개 구성할 수 있습니다.

사전 요구 사항

- 엔터프라이즈 관리자 또는 NSX 관리자 역할을 할당받아야 합니다.
- 리소스 풀에 ESG(Edge Services Gateway) 가상 장치를 배포하기에 충분한 용량이 있는지 확인합니다. [NSX의 시스템 요구 사항](#)을 참조하십시오.
- NSX Edge 장치가 설치될 호스트 클러스터가 NSX용으로 준비되어 있는지 확인합니다. "NSX 설치 가이드"에서 "NSX에 대한 호스트 클러스터 준비"를 참조하십시오.

절차

- 1 vCenter에서 **홈 > Networking & Security > NSX Edge(Home > Networking & Security > NSX Edges)**로 이동하고 **추가(Add) (+)** 아이콘을 클릭합니다.

- 2 **Edge Services Gateway**를 선택하고 디바이스 이름을 입력합니다.

이 이름은 vCenter 인벤토리에 나타납니다. 이 이름은 단일 테넌트 내의 모든 ESG에서 고유해야 합니다.

필요한 경우 호스트 이름을 입력할 수도 있습니다. 이 이름이 CLI에 표시됩니다. 호스트 이름을 지정하지 않으면 자동으로 생성되는 Edge ID가 CLI에 표시됩니다.

필요한 경우 설명과 테넌트를 입력하고 HA(고가용성)를 사용하도록 설정할 수 있습니다.

예:

New NSX Edge

1 Name and description

2 Settings

3 Configure deployment

4 Configure interfaces

5 Default gateway settings

6 Firewall and HA

7 Ready to complete

Name and description

Install Type: ☒ Edge Services Gateway
Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.

☐ Logical (Distributed) Router
Provides Distributed Routing and Bridging capabilities.

Name:

Hostname:

Description:

Tenant:

☒ Deploy NSX Edge
Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.

☐ Enable High Availability
Enable HA, for enabling and configuring High Availability.

Back Next Finish Cancel

- 3 ESG의 암호를 입력하고 다시 입력합니다.

암호는 최소 12자여야 하고 다음 4개 규칙 중 3개를 준수해야 합니다.

- 하나 이상의 대문자

- 하나 이상의 소문자
- 하나 이상의 숫자
- 하나 이상의 특수 문자

4 (선택 사항) SSH, 고가용성, 자동 규칙 생성 및 FIPS 모드를 사용하도록 설정하고 로그 수준을 설정합니다.

자동 규칙 생성을 사용하도록 설정하지 않을 경우 로드 밸런싱, VPN 등의 NSX Edge 서비스에 대한 제어 트래픽을 허용하도록 방화벽, NAT 및 라우팅 구성을 수동으로 추가해야 합니다. 자동 규칙 생성을 사용해도 데이터 채널 트래픽에 대한 규칙은 생성되지 않습니다.

기본적으로 SSH 및 HA는 사용하지 않도록 설정되어 있고, 자동 규칙 생성은 사용하도록 설정되어 있습니다.

기본적으로 FIPS 모드는 사용하지 않도록 설정되어 있습니다.

기본적으로 로그 수준은 긴급입니다.

예:

New NSX Edge

1 Name and description
2 Settings
 3 Configure deployment
 4 Configure interfaces
 5 Default gateway settings
 6 Firewall and HA
 7 Ready to complete

Settings

CLI credentials will be set on the NSX Edge appliance(s). These credentials can be used to login to the read only command line interface of the appliance.

User Name: * admin

Password: * [masked]

Confirm password: * [masked]

☒ Enable SSH access

☒ Enable FIPS mode

☒ Enable auto rule generation
 Enable auto rule generation, to automatically generate service rules to allow flow of control traffic.

Edge Control Level Logging: EMERGENCY

Set the Edge Control Level Logging

Back Next Finish Cancel

5 시스템 리소스에 따라 NSX Edge 인스턴스의 크기를 선택합니다.

중형(Large) NSX Edge에는 **소형(Compact)** NSX Edge보다 CPU, 메모리 및 디스크 공간이 더 많이 있으므로 지원하는 동시 **SSL VPN-Plus** 사용자 수가 더 많습니다. **초대형(X-Large)** NSX Edge는 수백만 개의 동시 세션에서 로드 밸런서를 사용하는 환경에 적합합니다. 처리량이 많고 속도가 빠른 연결이 필요할 경우 대형 NSX Edge가 적합합니다.

NSX의 시스템 요구 사항을 참조하십시오.

6 Edge 장치를 생성합니다.

vCenter 인벤토리에 추가되는 **ESG** 가상 장치에 대한 설정을 입력합니다. 장치를 추가하지 않은 상태로 NSX Edge를 설치하면 장치를 추가할 때까지 NSX Edge가 오프라인 모드로 유지됩니다.

HA를 사용하도록 설정한 경우 두 개 장치를 추가할 수 있습니다. 한 장치만 추가하면 NSX Edge가 대기 장치를 위해 해당 구성을 복제합니다. 이는 DRS 및 vMotion을 사용한 후에도 두 HA NSX Edge 가상 시스템이 동일한 ESX 호스트에 있지 않도록 보장하기 위해서입니다(단, 수동으로 vMotion을 통해 동일한 호스트로 이동하는 경우는 제외). HA가 올바르게 작동하려면 공유 데이터스토어에 두 장치를 모두 배포해야 합니다.

예:

Add NSX Edge Appliance

Specify placement parameters for the NSX Edge appliance.

Cluster/Resource Pool: * Management & Edge ... ▼

Datastore: * ds-1 ▼

Host: esxmgt-01a.corp.local ▼

Folder: Discovered virtual mac... ▼

7 Edge를 배포 모드에서 추가하려면 NSX Edge 배포(Deploy NSX Edge)를 선택합니다. Edge를 배포하려면 먼저 Edge에 대한 장치 및 인터페이스를 구성해야 합니다.

8 인터페이스를 구성합니다.

ESG에서 IPv4 및 IPv6 주소가 모두 지원됩니다.

HA가 작동하려면 내부 인터페이스를 하나 이상 추가해야 합니다.

인터페이스에는 겹치지 않는 서브넷이 여러 개 포함될 수 있습니다.

인터페이스에 대한 IP 주소를 둘 이상 입력하는 경우 기본 IP 주소를 선택할 수 있습니다. 인터페이스는 하나의 기본 IP 주소와 여러 개의 보조 IP 주소를 사용할 수 있습니다. NSX Edge는 기본 IP 주소를 로컬에서 생성된 트래픽(예: 원격 syslog 및 운영자가 시작한 ping)의 소스 주소로 간주합니다.

IP 주소를 기능 구성에 사용하기 전 인터페이스에 추가해야 합니다.

필요한 경우 인터페이스에 대한 **MAC** 주소를 입력할 수 있습니다.

나중에 **API** 호출을 사용하여 **MAC** 주소를 변경하는 경우 **MAC** 주소를 변경한 후에 **Edge**를 다시 배포해야 합니다.

HA를 사용하도록 설정한 경우 두 개의 관리 **IP** 주소를 **CIDR** 형식으로 입력할 수도 있습니다. 두 **NSX Edge HA** 가상 시스템의 하트비트가 이러한 관리 **IP** 주소를 통해 통신합니다. 관리 **IP** 주소는 동일한 **L2/서브넷**에 있어야 하며 서로 통신할 수 있어야 합니다.

필요한 경우 **MTU**를 수정할 수 있습니다.

ESG가 다른 시스템을 대상으로 한 **ARP** 요청에 응답할 수 있도록 허용하려면 프록시 **ARP**를 사용하도록 설정합니다. 예를 들어, **WAN** 연결의 양쪽에 동일한 서브넷이 있는 경우 유용합니다.

라우팅 정보를 호스트에 전달하려면 **ICMP** 리디렉션을 사용하도록 설정합니다.

역방향 경로 필터링을 사용하도록 설정하여 전달될 패킷의 소스 주소가 연결되는지 확인합니다. 사용 모드에서는 라우터가 반환 패킷을 전달하는 데 사용할 인터페이스에서 패킷을 수신해야 합니다. 소프트 모드에서는 소스 주소가 라우팅 테이블에 나타나야 합니다.

서로 다른 **fence** 환경에서 **IP** 및 **MAC** 주소를 다시 사용할 경우 **fence** 매개 변수를 구성합니다. 예를 들어, **CMP(Cloud Management Platform)**에서 **Fence**를 사용하면 완전히 분리되거나 "**fence**"된 동일한 **IP** 및 **MAC** 주소를 사용하여 여러 클라우드 인스턴스를 동시에 실행할 수 있습니다.

예:

Edit NSX Edge Interface ?

VNIC#: 1

Name: * Internal

Type: ☒ Internal ☐ Uplink

Connected To: transit-switch Change Remove

Connectivity Status: ☒ Connected ☐ Disconnected

Configure subnets

+ / - / ✕

IP Address	Subnet Prefix Length
192.168.10.1*	29

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU:

Options: ☐ Enable Proxy ARP ☐ Send ICMP Redirect Reverse Path Filter Disable ▾

Fence Parameters:

Example: ethernet0.filter1.param1=1

OK Cancel

다음 예제에서 두 개 인터페이스를 보여주는데 하나는 vSphere Distributed Switch에서 업링크 포트 그룹을 통해 ESG를 외부에 연결하고 있고, 다른 하나는 논리적 분산 라우터가 연결되어 있는 논리적 전송 스위치에 ESG를 연결하고 있습니다.

New NSX Edge

✓ 1 Name and description
 ✓ 2 Settings
 ✓ 3 Configure deployment
 ✓ 4 **Configure interfaces**
 5 Default gateway settings
 6 Firewall and HA
 7 Ready to complete

Configure interfaces

Configure interfaces of this NSX Edge

+ ✎ ✕

vNIC#	Name	IP Address	Subnet Prefix Length	Connected To
0	uplink	192.168.100.3	24	Mgmt_VDS - HQ_Uplink
1	internal	192.168.10.1*	29	transit-switch

Back Next Finish Cancel

9 기본 게이트웨이를 구성합니다.

MTU 값을 편집할 수 있지만, 인터페이스에 구성된 MTU보다 클 수는 없습니다.

예:

New NSX Edge

✓ 1 Name and description
 ✓ 2 Settings
 ✓ 3 Configure deployment
 ✓ 4 Configure interfaces
5 Default gateway settings
 6 Firewall and HA
 7 Ready to complete

Default gateway settings

☒ Configure Default Gateway

vNIC: * uplink

Gateway IP: * 192.168.100.2

MTU: 1500

Back Next Finish Cancel

10 방화벽 정책, 로깅 및 HA 매개 변수를 구성합니다.

경고 방화벽 정책을 구성하지 않을 경우 모든 트래픽을 거부하도록 기본 정책이 설정됩니다.

기본적으로 모든 새 **NSX Edge** 장치에서 로그가 사용되도록 설정되어 있습니다. 기본 로깅 수준은 [알림]입니다. 로그가 **ESG**에 로컬로 저장된 경우 로깅을 수행하면 너무 많은 로그가 생성되고 **NSX Edge**의 성능에 영향을 줄 수 있습니다. 이러한 이유로 원격 **Syslog** 서버를 구성하고, 분석 및 모니터링을 위해 모든 로그를 중앙 수집기로 전달하는 것이 좋습니다.

HA를 사용하도록 설정한 경우 **HA** 섹션을 완료하십시오. 기본적으로 **HA**에서는 자동으로 내부 인터페이스를 선택하고 링크-로컬 **IP** 주소를 할당합니다. **NSX Edge**는 고가용성을 위해 두 개의 가상 시스템을 지원하며 둘 다 사용자 구성으로 최신으로 유지됩니다. 기본 가상 시스템에서 하트비트 오류가 발생하면 보조 가상 시스템이 활성 상태로 변경됩니다. 따라서 네트워크에서 **NSX Edge** 가상 시스템 하나는 항상 활성 상태입니다. **NSX Edge**는 대기 장치를 위해 기본 장치의 구성을 복제하며, **DRS** 및 **vMotion**을 사용한 후에도 두 **HA NSX Edge** 가상 시스템이 동일한 **ESX** 호스트에 있지 않도록 보장합니다. 두 가상 시스템은 구성된 장치와 동일한 리소스 풀 및 데이터스토어의 **vCenter**에 배포됩니다. 서로 통신할 수 있도록 **NSX Edge HA**의 **HA** 가상 시스템에 로컬 링크 **IP** 주소가 할당됩니다. **HA** 매개 변수

수를 구성할 내부 인터페이스를 선택합니다. 인터페이스에 대해 [임의]를 선택하지만 구성된 내부 인터페이스가 없는 경우 UI에서 오류를 표시합니다. 두 개의 Edge 장치가 생성되지만 구성된 내부 인터페이스가 없기 때문에 새 Edge는 대기 상태를 유지하고 HA는 사용하지 않도록 설정됩니다. 내부 인터페이스가 구성되면 Edge 장치에서 HA가 사용하도록 설정됩니다. 지정한 시간 내에 백업 장치가 기본 장치로부터 하트비트 신호를 받지 못하면 기본 장치를 비활성 상태로 간주하여 백업 장치가 작업을 맡도록 할 기간(초)을 입력합니다. 기본 간격은 15초입니다. 필요한 경우 HA 가상 시스템에 할당된 로컬 링크 IP 주소를 재정의하려면 관리 IP 주소 두 개를 CIDR 형식으로 입력할 수 있습니다. 관리 IP 주소가 다른 인터페이스에서 사용되는 IP 주소와 겹치지 않고 트래픽 라우팅을 방해하지 않는지 확인합니다. 네트워크가 NSX Edge에 직접 연결되어 있지 않은 경우에도 해당 네트워크상의 어딘가에 존재하는 IP 주소를 사용해서는 안 됩니다.

예:

New NSX Edge

- ✓ 1 Name and description
- ✓ 2 Settings
- ✓ 3 Configure deployment
- ✓ 4 Configure interfaces
- ✓ 5 Default gateway settings
- 6 Firewall and HA**
- 7 Ready to complete

Firewall and HA

☒ **Configure Firewall default policy**

Default Traffic Policy: ☒ Accept ☐ Deny

Logging: ☐ Enable ☒ Disable

Configure HA parameters

Configuring HA parameters is mandatory for HA to work.

vNIC: * internal

Declare Dead Time: 15 (seconds)

Management IPs:

You can specify pair of IPs (in CIDR format) with /30 subnet. Management IPs must not overlap with any vnic subnets.

Back Next Finish Cancel

결과

ESG가 배포된 후 호스트 및 클러스터 보기로 이동하고 Edge 가상 장치의 콘솔을 엽니다. 콘솔에서 연결된 인터페이스를 Ping할 수 있는지 확인합니다.

다음에 수행할 작업

NSX Edge 장치를 설치할 때 vSphere HA가 클러스터에서 사용되지 않도록 설정되어 있으면 NSX는 호스트에서 자동 VM 시작/종료를 사용하도록 설정합니다. 장치 VM이 나중에 클러스터의 다른 호스트로 마이그레이션되는 경우 새 호스트가 자동 VM 시작/종료를 사용하도록 설정하지 않을 수도 있습니다. 이러한 이유로 vSphere HA가 사용되지 않도록 설정된 클러스터에서 NSX Edge 장치를 설치할 때는 클러스터의 모든 호스트를 점검하여 자동 VM 시작/종료가 사용되도록 설정되어 있는지 확인해야 합니다. "vSphere 가상 시스템 관리"에서 "가상 시스템 시작 및 종료 설정 편집"을 참조하십시오.

이제 외부 디바이스에서 VM으로 연결을 허용하도록 라우팅을 구성할 수 있습니다.

논리적 (분산) 라우터에서 OSPF 구성

19

논리적 라우터에서 OSPF를 구성하면 논리적 라우터 전체에서 VM을 연결하고 논리적 라우터에서 ESG(Edge Services Gateway)로 VM을 연결할 수 있습니다.

OSPF 라우팅 정책은 동일한 코스트의 경로 간에 트래픽 로드 밸런싱의 동적 프로세스를 제공합니다.

OSPF 네트워크가 라우팅 영역으로 구분되어 트래픽 흐름을 최적화하고 라우팅 테이블의 크기를 제한합니다. 영역은 동일한 영역 ID를 가진 OSPF 네트워크, 라우터 및 링크의 논리적 모음입니다.

영역은 영역 ID로 식별됩니다.

사전 요구 사항

논리적 (분산) 라우터에 구성된 OSPF에 표시된 대로 라우터 ID를 구성해야 합니다.

라우터 ID를 사용하도록 설정한 경우 기본적으로 논리적 라우터의 업링크 인터페이스로 필드가 채워집니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 논리적 라우터를 두 번 클릭합니다.
- 4 **라우팅(Routing)**을 클릭하고 **OSPF**를 클릭합니다.
- 5 OSPF를 사용하도록 설정합니다.
 - a 창의 오른쪽 상단에서 **편집(Edit)**을 클릭하고 **OSPF 사용(Enable OSPF)**을 클릭합니다.
 - b **전달 주소(Forwarding Address)**에서 호스트의 라우터 데이터 경로 모듈이 데이터 경로 패킷을 전달하기 위해 사용할 IP 주소를 입력합니다.
 - c **프로토콜 주소(Protocol Address)**에서 **전달 주소(Forwarding Address)**와 동일한 서브넷 내의 고유한 IP 주소를 입력합니다. 프로토콜에서 프로토콜 주소를 사용하여 피어와의 인접성을 형성합니다.
- 6 OSPF 영역을 구성합니다.
 - a 선택에 따라 기본적으로 구성되는 NSSA(not-so-stubby 영역) 51을 삭제합니다.
 - b **영역 정의(Area Definitions)**에서 **추가(Add)** 아이콘을 클릭합니다.

- c 영역 ID를 입력합니다. NSX Edge는 십진수 형식의 영역 ID를 지원합니다. 올바른 값은 0~4294967295입니다.
- d **유형(Type)**에서 **보통(Normal)** 또는 **NSSA**를 선택합니다.

NSSA는 AS 외부 LSA(링크 상태 알림)가 NSSA로 플러딩되는 것을 방지합니다. NSSA는 외부 대상에 대한 기본 라우팅을 사용합니다. 따라서 NSSA는 OSPF 라우팅 도메인의 종단에 있어야 합니다. NSSA는 외부 경로를 OSPF 라우팅 도메인에 가져올 수 있으므로 OSPF 라우팅 도메인에 포함되지 않은 소규모 라우팅 도메인에 전송 서비스를 제공할 수 있습니다.

7 (선택 사항) 인증(Authentication) 유형을 선택합니다. OSPF가 영역 수준에서 인증을 수행합니다.

영역 내 모든 라우터에는 동일한 인증 및 해당하는 암호가 구성되어 있어야 합니다. MD5 인증이 작동하려면 수신 라우터와 전송 라우터가 동일한 MD5 키를 가지고 있어야 합니다.

- a **없음(None)**: 인증이 필요하지 않으며 기본값입니다.
- b **암호>Password**: 이 인증 방법을 사용할 경우 전송된 패킷에 암호가 포함됩니다.
- c **MD5**: 이 인증 방법은 MD5(메시지 다이제스트 유형 5) 암호화를 사용합니다. 전송된 패킷에 MD5 체크섬이 포함됩니다.
- d **암호>Password** 또는 **MD5** 인증 유형을 선택한 경우 암호나 MD5 키를 입력합니다.

중요

- NSX Edge가 OSPF의 정상적인 다시 시작이 사용되도록 설정된 HA에 대해 구성되어 있고 MD5가 인증에 사용될 경우 OSPF는 정상적으로 다시 시작되지 못합니다. OSPF 도우미 노드에서 유예 기간이 만료된 후에만 인접성이 형성됩니다.
- FIPS 모드가 사용되도록 설정되어 있으면 **MD5** 인증을 구성할 수 없습니다.
- NSX for vSphere는 항상 키 ID 값으로 1을 사용합니다. Edge Services Gateway 또는 논리적 분산 라우터와 연결되는 NSX for vSphere에서 관리되지 않는 모든 디바이스는 MD5 인증이 사용될 때 값이 1인 키 ID를 사용하도록 구성해야 합니다. 그렇지 않으면 OSPF 세션을 설정할 수 없습니다.

8 인터페이스를 영역에 매핑합니다.

- a **영역-인터페이스 매핑(Area to Interface Mapping)**에서 **추가(Add)** 아이콘을 클릭하여 OSPF 영역에 속한 인터페이스를 매핑합니다.
- b 매핑할 인터페이스를 선택하고 인터페이스를 매핑할 OSPF 영역을 선택합니다.

9 (선택 사항) 필요한 경우 기본 OSPF 설정을 편집합니다.

대부분의 경우 기본 OSPF 설정을 유지하는 것이 좋습니다. 설정을 변경할 경우 OSPF 피어에서 동일한 설정을 사용하는지 확인하십시오.

- a **Hello 간격(Hello Interval)**은 인터페이스에서 전송되는 hello 패킷 간의 기본 간격을 표시합니다.
- b **비활성 간격(Dead Interval)**은 인접 네트워크가 중단되었음을 라우터가 선언하기 전에 인접 네트워크로부터 하나 이상의 hello 패킷이 수신되어야 하는 기본 간격을 표시합니다.

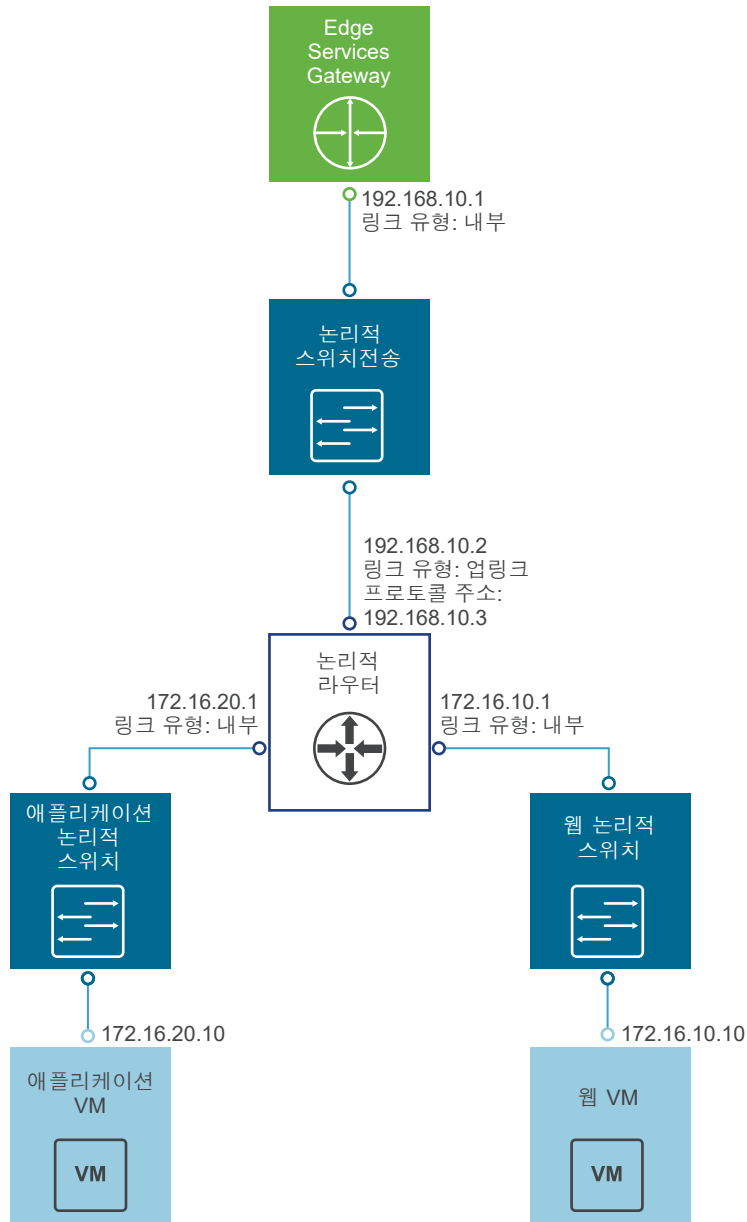
- c **우선 순위(Priority)**는 인터페이스의 기본 우선 순위를 표시합니다. 우선 순위가 가장 높은 인터페이스는 지정 라우터입니다.
- d 인터페이스 **코스트(Cost)**는 해당 인터페이스 전체에서 패킷을 보내는 데 필요한 기본 오버헤드를 표시합니다. 인터페이스 코스트는 인터페이스 대역폭과 반비례합니다. 대역폭이 클수록 코스트가 적어집니다.

10 변경 내용 게시(Publish Changes)를 클릭합니다.

예제: 논리적 (분산) 라우터에 구성된 OSPF

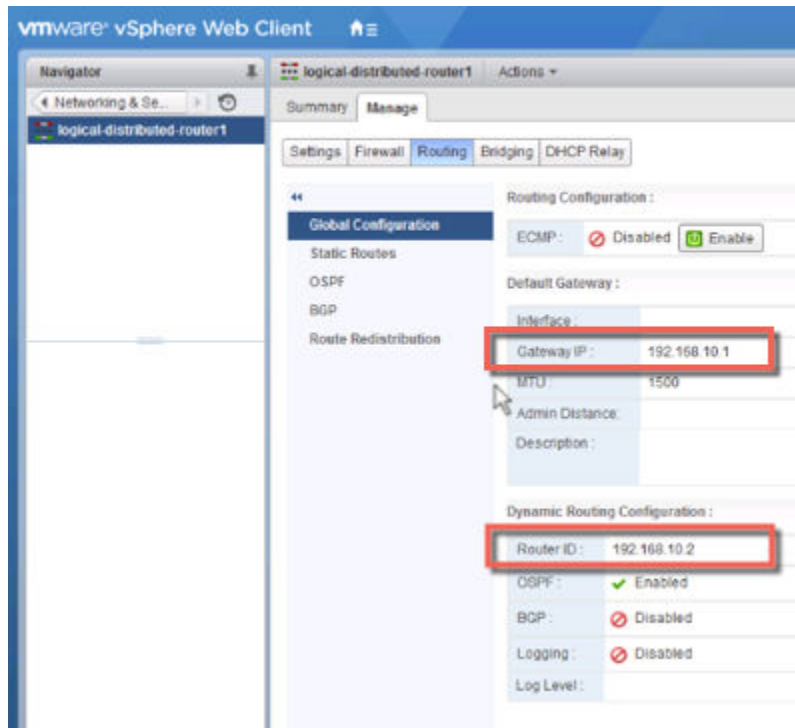
여기에 표시된 OSPF를 사용하는 간단한 NSX for vSphere 시나리오에서는 DLR(논리적 라우터) 및 ESG(Edge Services Gateway)가 OSPF 인접 네트워크입니다.

그림 19-1. NSX for vSphere 토폴로지

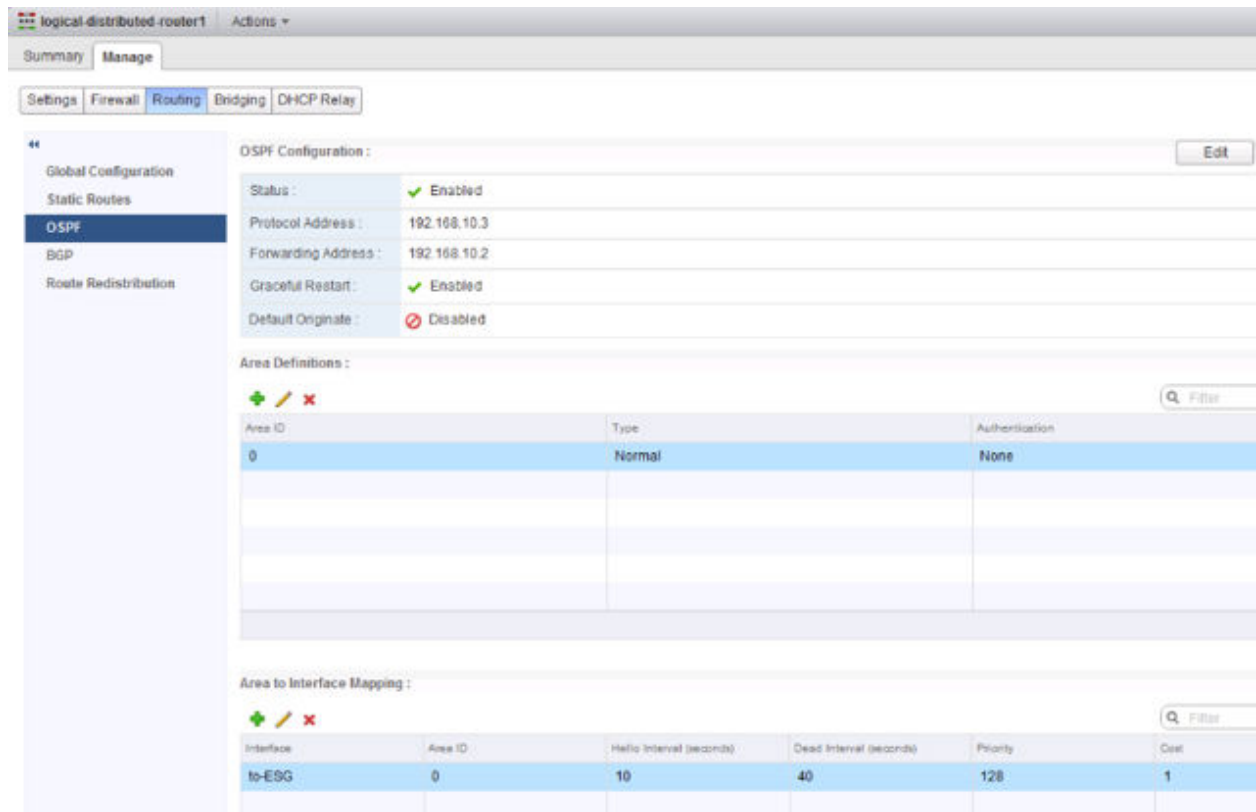


다음 화면에서 논리적 라우터의 기본 게이트웨이는 ESG의 내부 인터페이스 IP 주소(192.168.10.1)입니다.

라우터 ID는 논리적 라우터의 업링크 인터페이스입니다. 즉 ESG에 연결되는 IP 주소입니다 (192.168.10.2).



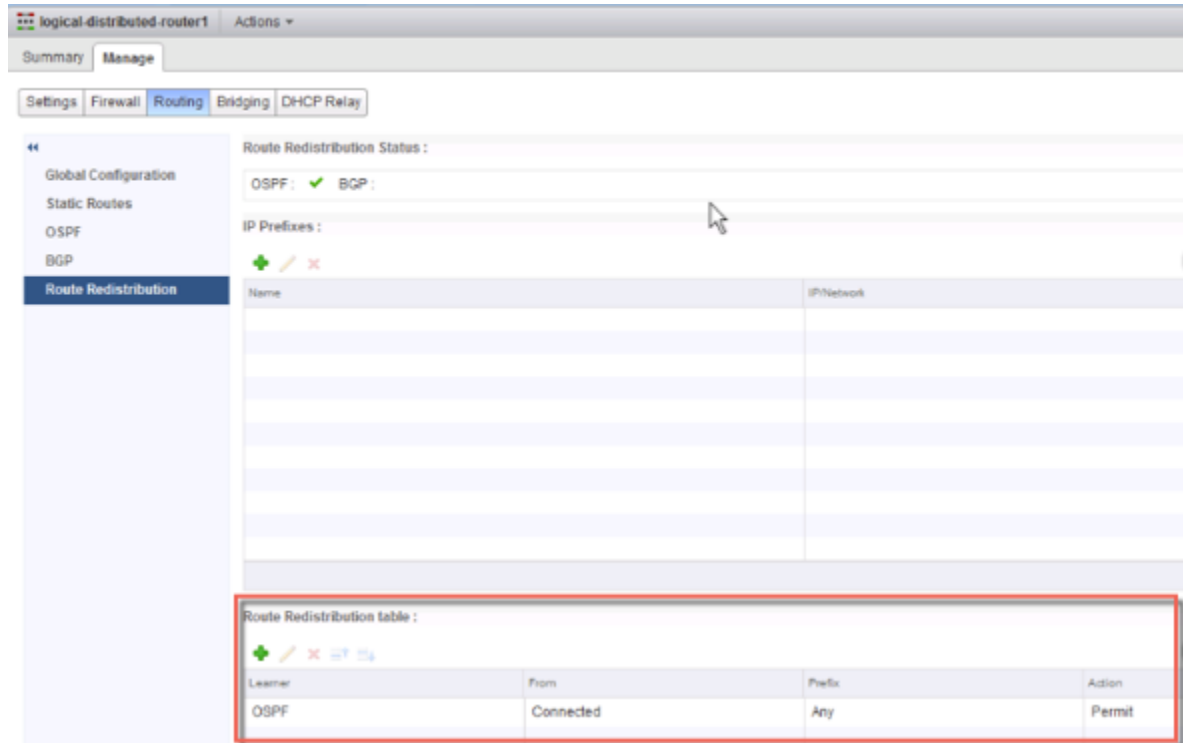
논리적 라우터 구성에서는 192.168.10.2를 전달 주소로 사용합니다. 동일한 서브넷에 있고 다른 곳에서 사용되지 않은 IP 주소가 프로토콜 주소가 될 수 있습니다. 이 경우 192.168.10.3이 구성됩니다. 구성된 영역 ID는 0이고 업링크 인터페이스(ESG에 연결되는 인터페이스)가 영역에 매핑됩니다.



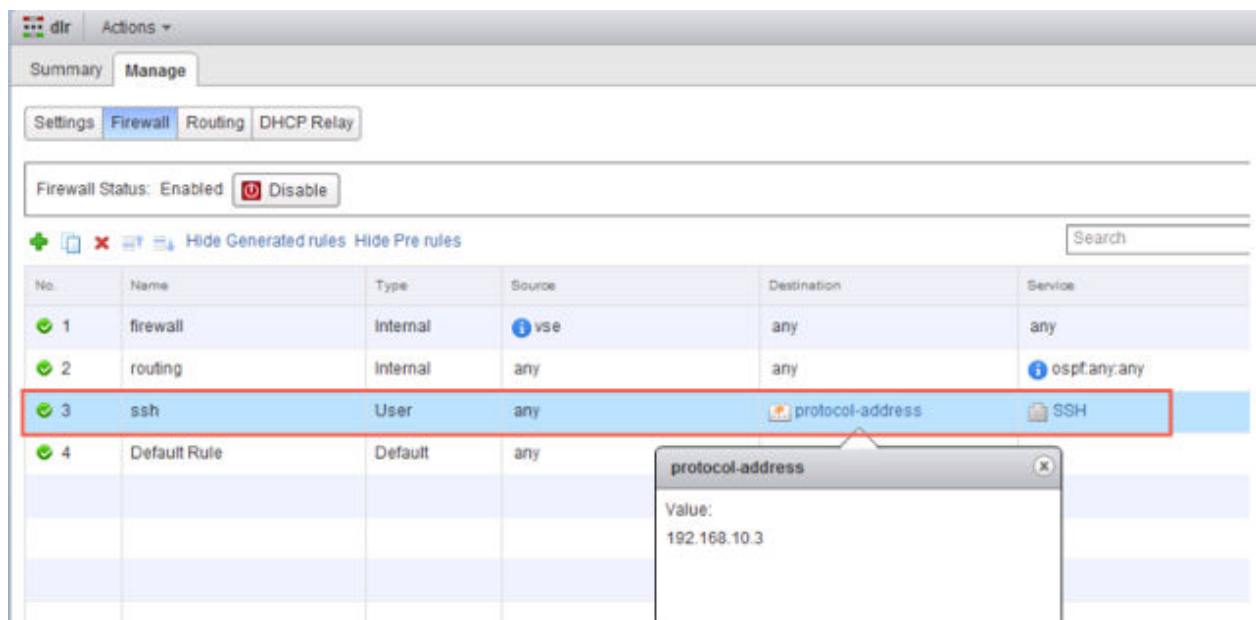
다음에 수행할 작업

경로 재배포 및 방화벽 구성에서 올바른 경로가 보급되도록 허용하는지 확인합니다.

이 예제에서는 논리적 라우터의 연결된 경로(172.16.10.0/24 및 172.16.20.0/24)가 OSPF에 보급됩니다.



논리적 라우터를 생성할 때 SSH를 사용하도록 설정한 경우 SSH를 논리적 라우터의 프로토콜 주소에 허용하는 방화벽 필터도 구성해야 합니다. 예:



Edge Services Gateway에서 OSPF 구성

20

ESG(Edge Services Gateway)에서 OSPF를 구성하면 ESG가 경로를 인식 및 보급할 수 있습니다. ESG에서 OSPF의 가장 일반적인 애플리케이션은 ESG와 논리적 (분산) 라우터 간의 링크에 있습니다. 이를 통해 ESG가 논리적 라우터에 연결된 LIFS(논리적 인터페이스)를 인식할 수 있습니다. OSPF, IS-IS, BGP 또는 정적 라우팅을 사용하여 이 목적을 달성할 수 있습니다.

OSPF 라우팅 정책은 동일한 코스트의 경로 간에 트래픽 로드 밸런싱의 동적 프로세스를 제공합니다.

OSPF 네트워크가 라우팅 영역으로 구분되어 트래픽 흐름을 최적화하고 라우팅 테이블의 크기를 제한합니다. 영역은 동일한 영역 ID를 가진 OSPF 네트워크, 라우터 및 링크의 논리적 모음입니다.

영역은 영역 ID로 식별됩니다.

사전 요구 사항

Edge Services Gateway에 구성된 OSPF에 표시된 대로 라우터 ID를 구성해야 합니다.

라우터 ID를 사용하도록 설정할 경우 기본적으로 ESG의 업링크 인터페이스 IP 주소로 필드가 채워집니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 ESG를 두 번 클릭합니다.
- 4 **라우팅(Routing)**을 클릭하고 **OSPF**를 클릭합니다.
- 5 OSPF를 사용하도록 설정합니다.
 - a 창의 오른쪽 상단에서 **편집(Edit)**을 클릭하고 **OSPF 사용(Enable OSPF)**을 클릭합니다.
 - b (선택 사항) OSPF 서비스를 다시 시작하는 중에 패킷 전달이 중단되지 않도록 하려면 **정상적인 다시 시작 사용(Enable Graceful Restart)**을 클릭합니다.
 - c (선택 사항) ESG가 자신을 기본 게이트웨이로 피어에 보급할 수 있도록 허용하려면 **기본 시작 사용(Enable Default Originate)**을 클릭합니다.
- 6 OSPF 영역을 구성합니다.
 - a (선택 사항) 기본적으로 구성되는 NSSA(not-so-stubby 영역) 51을 삭제합니다.
 - b **영역 정의(Area Definitions)**에서 **추가(Add)** 아이콘을 클릭합니다.

- c 영역 ID를 입력합니다. NSX Edge는 IP 주소 또는 십진수 형식의 영역 ID를 지원합니다.
- d **유형(Type)**에서 **보통(Normal)** 또는 **NSSA**를 선택합니다.

NSSA는 AS 외부 LSA(링크 상태 알림)가 NSSA로 플러딩되는 것을 방지합니다. NSSA는 외부 대상에 대한 기본 라우팅을 사용합니다. 따라서 NSSA는 OSPF 라우팅 도메인의 종단에 있어야 합니다. NSSA는 외부 경로를 OSPF 라우팅 도메인에 가져올 수 있으므로 OSPF 라우팅 도메인에 포함되지 않은 소규모 라우팅 도메인에 전송 서비스를 제공할 수 있습니다.

- 7 (선택 사항) 유형으로 **NSSA**를 선택하면 **NSSA 변환기 역할(NSSA Translator Role)** 필드가 나타납니다. **항상(Always)** 확인란을 선택하여 Type-7 LSA를 Type-5 LSA로 변환합니다. 모든 Type-7 LSA는 NSSA에 의해 Type-5 LSA로 변환됩니다.

- 8 (선택 사항) **인증(Authentication)** 유형을 선택합니다. OSPF가 영역 수준에서 인증을 수행합니다.

영역 내 모든 라우터에는 동일한 인증 및 해당하는 암호가 구성되어 있어야 합니다. MD5 인증이 작동하려면 수신 라우터와 전송 라우터가 동일한 MD5 키를 가지고 있어야 합니다.

- a **없음(None)**: 인증이 필요하지 않으며 기본값입니다.
- b **암호>Password**: 이 인증 방법을 사용할 경우 전송된 패킷에 암호가 포함됩니다.
- c **MD5**: 이 인증 방법은 MD5(메시지 다이제스트 유형 5) 암호화를 사용합니다. 전송된 패킷에 MD5 체크섬이 포함됩니다.
- d **암호>Password** 또는 **MD5** 인증 유형을 선택한 경우 암호나 MD5 키를 입력합니다.

참고

- FIPS 모드가 사용되도록 설정되어 있으면 **MD5** 인증을 구성할 수 없습니다.
 - NSX는 항상 키 ID 값으로 1을 사용합니다. NSX Edge 또는 논리적 분산 라우터와 피어로 연결된 모든 비 NSX 디바이스는 MD5 인증이 사용될 때 키 ID로 값 1을 사용하도록 구성되어야 합니다. 그렇지 않으면 OSPF 세션이 설정되지 않습니다.
-

- 9 인터페이스를 영역에 매핑합니다.

- a **영역-인터페이스 매핑(Area to Interface Mapping)**에서 **추가(Add)** 아이콘을 클릭하여 OSPF 영역에 속한 인터페이스를 매핑합니다.
- b 매핑할 인터페이스를 선택하고 인터페이스를 매핑할 OSPF 영역을 선택합니다.

- 10 (선택 사항) 기본 OSPF 설정을 편집합니다.

대부분의 경우 기본 OSPF 설정을 유지하는 것이 좋습니다. 설정을 변경할 경우 OSPF 피어에서 동일한 설정을 사용하는지 확인하십시오.

- a **Hello 간격(Hello Interval)**은 인터페이스에서 전송되는 hello 패킷 간의 기본 간격을 표시합니다.
- b **비활성 간격(Dead Interval)**은 인접 네트워크가 중단되었음을 라우터가 선언하기 전에 인접 네트워크로부터 하나 이상의 hello 패킷이 수신되어야 하는 기본 간격을 표시합니다.
- c **우선 순위(Priority)**는 인터페이스의 기본 우선 순위를 표시합니다. 우선 순위가 가장 높은 인터페이스는 지정 라우터입니다.

- d 인터페이스 **코스트(Cost)**는 해당 인터페이스 전체에서 패킷을 보내는 데 필요한 기본 오버헤드를 표시합니다. 인터페이스 코스트는 인터페이스 대역폭과 반비례합니다. 대역폭이 클수록 코스트가 적어집니다.

11 변경 내용 게시(Publish Changes)를 클릭합니다.

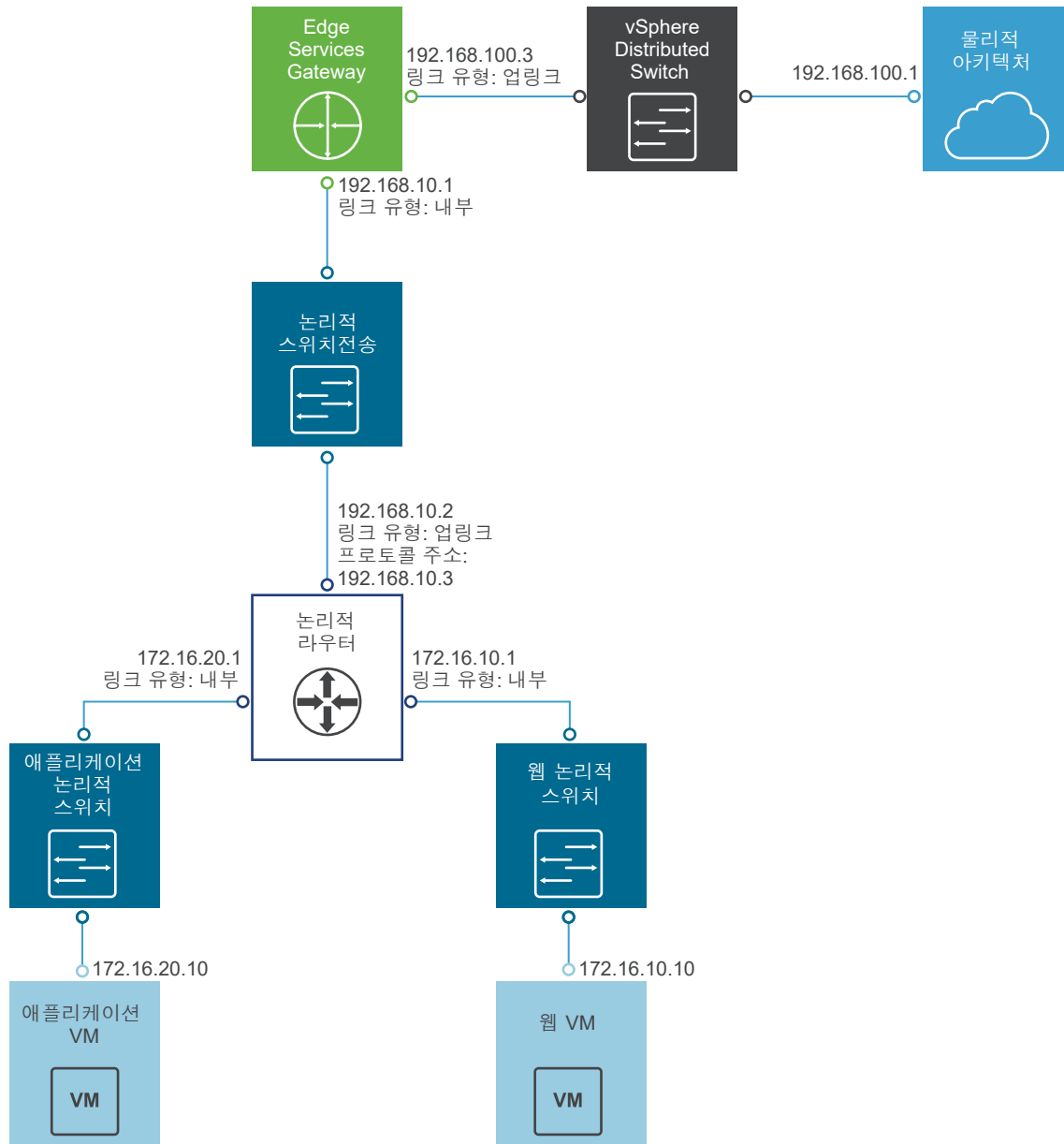
12 경로 재배포 및 방화벽 구성에서 올바른 경로가 보급되도록 허용하는지 확인합니다.

예제: Edge Services Gateway에 구성된 OSPF

여기에 표시된 OSPF를 사용하는 간단한 NSX 시나리오에서는 논리적 라우터 및 Edge Services Gateway가 OSPF 인접 네트워크입니다.

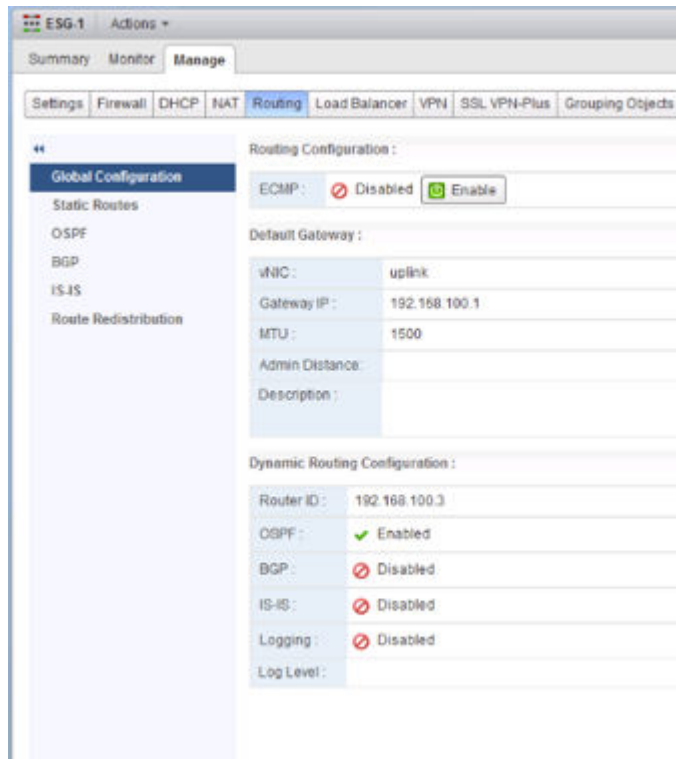
ESG는 브리지 또는 물리적 라우터를 통해 외부에 연결되거나 여기에 표시된 대로 vSphere Distributed Switch의 업링크 포트 그룹을 통해 외부에 연결할 수 있습니다.

그림 20-1. NSX 토폴로지

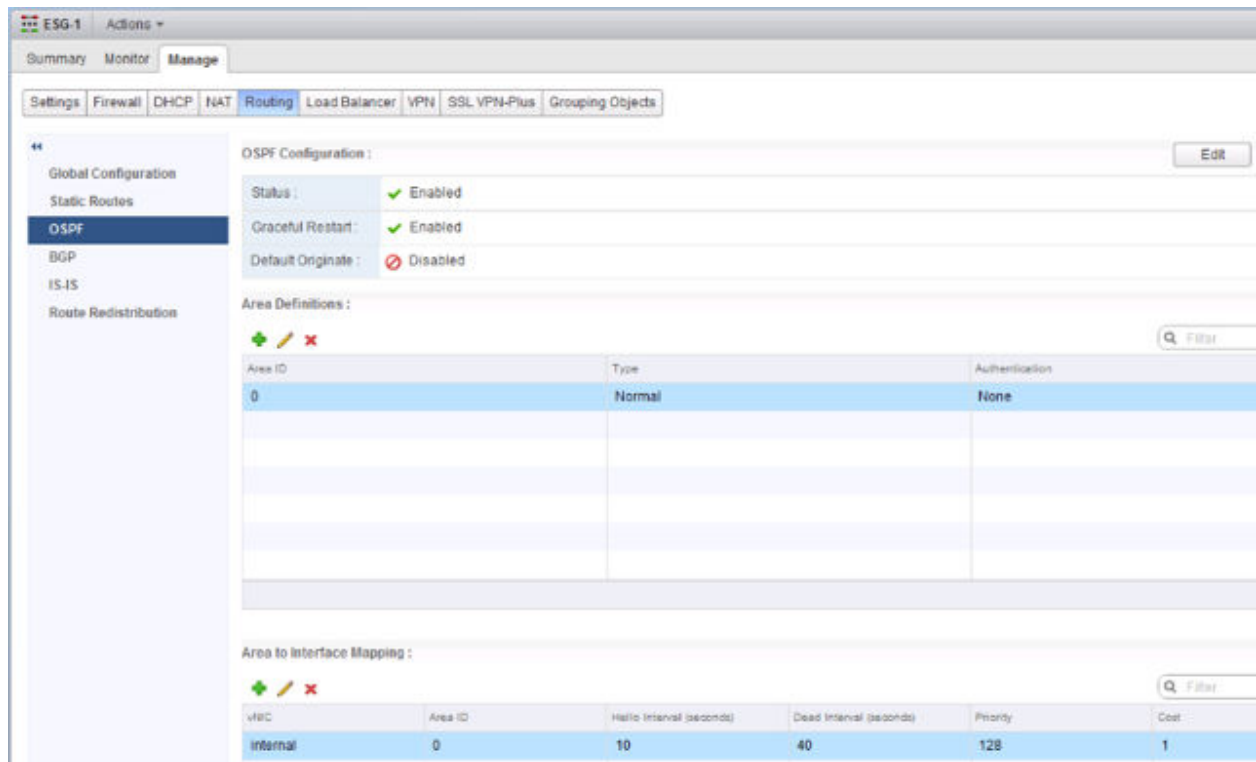


다음 화면에서 ESG의 기본 게이트웨이는 외부 피어에 대한 ESG의 업링크 인터페이스입니다.

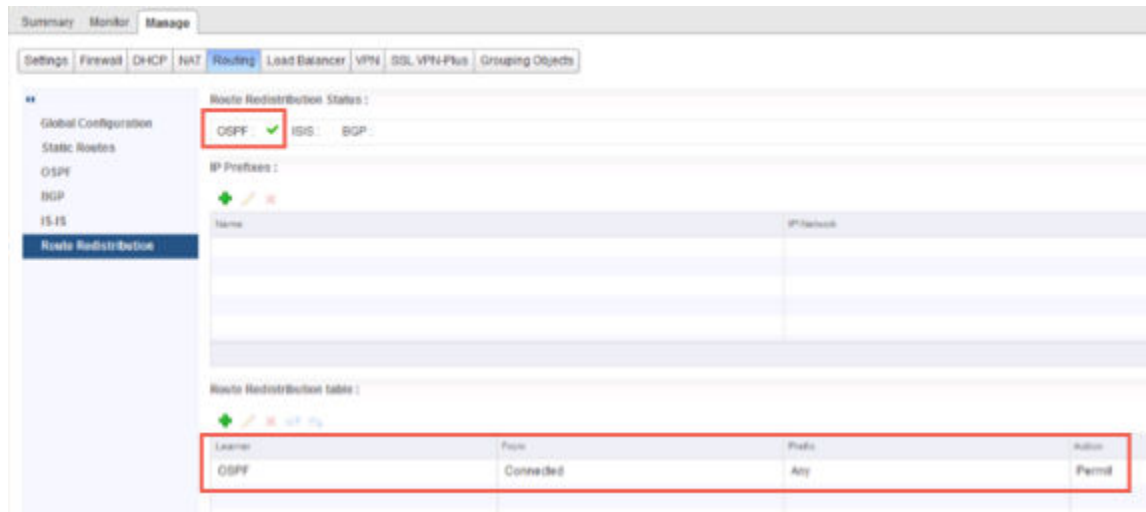
라우터 ID는 ESG의 업링크 인터페이스 IP 주소입니다. 즉 외부 피어에 연결하는 IP 주소입니다.



구성된 영역 ID는 0이고 내부 인터페이스(논리적 라우터에 연결되는 인터페이스)가 영역에 매핑됩니다.



연결된 경로가 OSPF에 재배포되므로 OSPF 인접 네트워크(논리적 라우터)가 ESG의 업링크 네트워크를 인식할 수 있습니다.



참고 그리고 ESG와 해당 외부 피어 라우터 간에 OSPF를 구성할 수 있지만 경로 보급을 위해 이 링크에서 BGP를 사용하는 것이 더 일반적입니다.

ESG가 논리적 라우터에서 OSPF 외부 경로를 인식하는지 확인하십시오.

```
NSX-edge-7-0> show ip route

Codes: 0 - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 5

S      0.0.0.0/0          [0/0]          via 192.168.100.1
0 E2 172.16.10.0/24      [110/1]        via 192.168.10.2
0 E2 172.16.20.0/24      [110/1]        via 192.168.10.2
C      192.168.10.0/29    [0/0]          via 192.168.10.1
C      192.168.100.0/24   [0/0]          via 192.168.100.3
```

연결을 확인하려면 물리적 아키텍처의 외부 디바이스가 VM을 ping할 수 있는지 확인하십시오.

예:

```
PS C:\Users\Administrator> ping 172.16.10.10
```

Pinging 172.16.10.10 with 32 bytes of data:

Reply from 172.16.10.10: bytes=32 time=5ms TTL=61

Reply from 172.16.10.10: bytes=32 time=1ms TTL=61

Ping statistics for 172.16.10.10:

Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 5ms, Average = 3ms

```
PS C:\Users\Administrator> ping 172.16.20.10
```

Pinging 172.16.20.10 with 32 bytes of data:

Reply from 172.16.20.10: bytes=32 time=2ms TTL=61

Reply from 172.16.20.10: bytes=32 time=1ms TTL=61

Ping statistics for 172.16.20.10:

Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 2ms, Average = 1ms

호스트 클러스터에 Guest Introspection 설치

21

Guest Introspection을 설치하면 클러스터의 각 호스트에 새 VIB 및 서비스 가상 시스템이 자동으로 설치됩니다. Activity Monitoring, 여러 타사 보안 솔루션을 사용하려면 Guest Introspection이 필요합니다.

참고 vMotion/SvMotion을 사용하여 SVM(서비스 VM)을 마이그레이션할 수 없습니다. SVM이 올바르게 작동하려면 배포된 호스트에 유지되어야 합니다.

사전 요구 사항

수행할 설치 지침에서는 사용자가 다음 시스템을 갖추고 있는 것으로 간주합니다.

- 지원되는 버전의 vCenter Server 및 ESXi가 클러스터의 각 호스트에 설치되어 있는 데이터센터.
- 클러스터의 호스트가 vCenter Server 버전 5.0에서 5.5로 업그레이드된 경우 해당 호스트에서 포트 80 및 443을 열어야 합니다.
- Guest Introspection을 설치하려는 클러스터의 호스트는 NSX 준비가 완료되어 있습니다. "NSX 설치 가이드"에서 "NSX에 대한 호스트 클러스터 준비"를 참조하십시오. 독립형 호스트에는 Guest Introspection을 설치할 수 없습니다. 바이러스 백신 오프로드 기능 전용 Guest Introspection을 배포 및 관리하기 위해 NSX를 사용하는 경우에는 NSX를 위해 호스트를 준비할 필요가 없습니다. NSX for vShield Endpoint 라이선스에서 허용하지 않기 때문입니다.
- NSX Manager가 설치되어 실행되고 있습니다.
- NSX Manager 및 Guest Introspection 서비스를 실행할 준비된 호스트가 동일한 NTP 서버에 연결되었고 시간이 동기화되었는지 확인합니다. 확인하지 않으면 클러스터의 상태가 Guest Introspection 및 타사 서비스에 대해 녹색으로 표시되어도 VM이 바이러스 백신 서비스로 보호되지 않을 수 있습니다.

NTP 서버가 추가되면 Guest Introspection 및 타사 서비스를 다시 배포하는 것이 좋습니다.

NSX Guest Introspection 서비스 가상 시스템에 IP 풀의 IP 주소를 할당하려면 NSX Guest Introspection을 설치하기 전에 IP 풀을 생성합니다. "NSX 관리 가이드"에서 IP 풀 사용을 참조하십시오.

경고 Guest Introspection은 169.254.x.x 서브넷을 사용하여 GI 서비스에 대해 내부적으로 IP 주소를 할당합니다. ESXi 호스트의 VMkernel 인터페이스에 169.254.1.1 IP 주소를 할당하면 Guest Introspection 설치가 실패합니다. GI 서비스는 내부 통신용으로 이 IP 주소를 사용합니다.

vSphere Fault Tolerance가 Guest Introspection에서는 작동하지 않습니다.

절차

- 1 **설치(Installation)** 탭에서 **서비스 배포(Service Deployments)**를 클릭합니다.
- 2 **새 서비스 배포(New Service Deployment)**() 아이콘을 클릭합니다.
- 3 네트워크 및 보안 서비스 배포 대화상자에서 **Guest Introspection**을 선택합니다.
- 4 대화상자 아래쪽의 **스케줄 지정(Specify schedule)**에서 **지금 배포(Deploy now)**를 선택하여 Guest Introspection을 설치 즉시 배포하거나 배포 날짜 및 시간을 선택합니다.
- 5 **다음(Next)**을 클릭합니다.
- 6 Guest Introspection을 설치할 데이터센터 및 클러스터를 선택하고 **다음(Next)**을 클릭합니다.
- 7 [스토리지 및 관리 네트워크 선택] 페이지에서 서비스 가상 시스템 스토리지를 추가할 데이터스토어를 선택하거나 **지정된 호스트(Specified on host)**를 선택합니다. "지정된 호스트" 대신 공유 데이터스토어 및 네트워크를 사용하여 배포 워크플로우를 자동화하는 것이 좋습니다.

선택한 데이터스토어는 선택한 클러스터의 모든 호스트에서 사용할 수 있어야 합니다.

지정된 호스트(Specified on host)를 선택했을 경우 클러스터의 각 호스트에 대해 아래의 단계를 수행합니다.

- a vSphere Web Client 홈 페이지에서 **vCenter**를 클릭하고 **호스트(Hosts)**를 클릭합니다.
 - b **이름(Name)** 열에서 호스트를 클릭하고 **관리(Manage)** 탭을 클릭합니다.
 - c **에이전트 VM(Agent VMs)**을 클릭하고 **편집(Edit)**을 클릭합니다.
 - d 데이터스토어를 선택하고 **확인(OK)**을 클릭합니다.
- 8 관리 인터페이스를 호스팅할 분산 가상 포트 그룹을 선택합니다. 데이터스토어가 **지정된 호스트(Specified on host)**로 설정된 경우 네트워크도 **지정된 호스트(Specified on host)**로 설정해야 합니다.

선택한 포트 그룹이 NSX Manager의 포트 그룹에 액세스할 수 있어야 하고 선택한 클러스터의 모든 호스트에서 사용 가능해야 합니다.

지정된 호스트(Specified on host)를 선택했을 경우 7단계의 하위 단계를 수행하여 호스트의 네트워크를 선택합니다. 호스트(또는 다중 호스트)를 클러스터에 추가할 경우 호스트가 클러스터에 추가되기 전에 데이터스토어와 네트워크를 설정해야 합니다.

9 IP 할당에서 다음 중 하나를 선택합니다.

선택	끝
DHCP	DHCP(Dynamic Host Configuration Protocol)를 통해 IP 주소를 NSX Guest Introspection 서비스 가상 시스템에 할당합니다. 호스트가 다른 서브넷에 있는 경우 이 옵션을 선택합니다.
IP 풀	선택한 IP 풀의 IP 주소를 NSX Guest Introspection 서비스 가상 시스템에 할당합니다.

10 다음(Next)을 클릭한 후 [완료 준비] 페이지에서 **완료(Finish)**를 클릭합니다.

11 설치 상태(Installation Status) 열이 **성공(Succeeded)**으로 표시될 때까지 배포를 모니터링합니다.

12 설치 상태(Installation Status) 열에 **실패(Failed)**가 표시되면 실패 옆의 아이콘을 클릭합니다. 그러면 모든 배포 오류가 표시됩니다. **해결(Resolve)**을 클릭하여 오류를 해결합니다. 경우에 따라 오류를 해결하면 다른 오류가 표시됩니다. 필요한 조치를 취하고 **해결(Resolve)**을 다시 클릭합니다.

이 장에서는 vCenter 인벤토리에서 NSX 구성 요소를 제거하는 데 필요한 단계를 자세히 설명합니다.

참고 NSX(예: 컨트롤러 및 Edge)에서 배포한 장치를 vCenter에서 직접 제거하지 마십시오. 항상 vSphere Web Client의 **Networking & Security** 탭을 사용하여 NSX 장치를 관리 및 제거하십시오.

본 장은 다음 항목을 포함합니다.

- **Guest Introspection** 모듈 제거
- **NSX Edge Services Gateway** 또는 논리적 분산 라우터 제거
- 논리적 스위치 제거
- 호스트 클러스터에서 **NSX** 제거
- 안전한 방법으로 **NSX** 설치 제거

Guest Introspection 모듈 제거

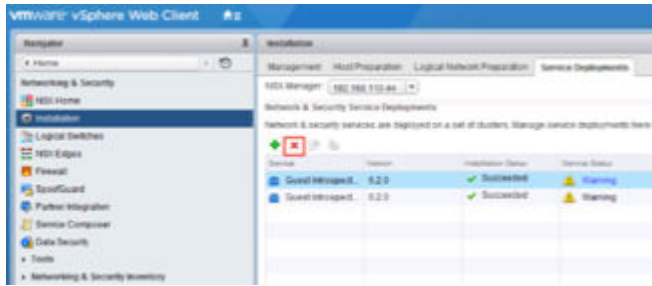
Guest Introspection을 제거하면 클러스터 내의 호스트에서 VIB가 제거되며 클러스터 내의 각 호스트에서 서비스 가상 시스템이 제거됩니다. ID 방화벽, 끝점 모니터링, 여러 타사 보안 솔루션을 사용하려면 Guest Introspection이 필요합니다. Guest Introspection 모듈 제거는 폭넓은 영향을 미칠 수 있습니다.

경고 클러스터에서 Guest Introspection 모듈을 제거하기 전에 해당 클러스터의 호스트에서 Guest Introspection을 사용하는 모든 타사 제품을 제거해야 합니다. 솔루션 제공자의 지침을 따르십시오.

NSX 클러스터의 VM에 대한 보호가 손실됩니다. 제거하기 전에 클러스터의 VM에 대해 vMotion을 수행해야 합니다.

Guest Introspection을 제거하기 위해서는,

- 1 vCenter에서 **홈 > Networking & Security > 설치(Home > Networking & Security > Installation)** 로 이동하고 **서비스 배포(Service Deployments)** 탭을 선택합니다.
- 2 Guest Introspection 인스턴스를 선택하고 삭제 아이콘을 클릭합니다.
- 3 지금 삭제하거나 추후 삭제를 예약합니다.



NSX Edge Services Gateway 또는 논리적 분산 라우터 제거

vSphere Web Client를 사용하여 NSX Edge를 제거할 수 있습니다.

사전 요구 사항

엔터프라이즈 관리자 또는 NSX 관리자 역할을 할당받아야 합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 선택하고 **삭제(Delete)(X)** 아이콘을 클릭합니다.

논리적 스위치 제거

논리적 스위치를 제거하기 전에 논리적 스위치에서 모든 가상 시스템을 제거해야 합니다.

사전 요구 사항

엔터프라이즈 관리자 또는 NSX 관리자 역할을 할당받아야 합니다.

절차

- 1 vSphere Web Client에서 **홈 > 네트워킹 및 보안 > 논리적 스위치(Home > Networking & Security > Logical Switches)**로 이동합니다.
- 2 논리적 스위치에서 모든 가상 시스템을 제거합니다.
 - a 논리적 스위치를 선택하고 [가상 시스템 제거] 아이콘 (X)을 클릭합니다.
 - b [사용 가능한 개체]의 모든 가상 시스템을 [선택한 개체]로 이동하고 **확인(OK)**을 클릭합니다.
- 3 논리적 스위치를 선택한 상태에서 **삭제(Delete)(X)** 아이콘을 클릭합니다.

호스트 클러스터에서 NSX 제거

클러스터의 모든 호스트에서 NSX를 제거할 수 있습니다.

전체 클러스터가 아닌 개별 호스트에서 NSX를 제거하려는 경우 [장 12 NSX 준비된 클러스터에서 호스트 제거](#)를 참조하십시오.

사전 요구 사항


- 논리적 스위치의 클러스터에서 VM 연결을 끊습니다.

절차

- 1 전송 영역에서 클러스터를 제거합니다.

논리적 네트워크 준비 > 전송 영역(Logical Network Preparation > Transport Zones)으로 이동하고 전송 영역에서 클러스터의 연결을 끊습니다.

클러스터가 회색으로 표시되고 전송 영역에서 클러스터 연결을 끊을 수 없는 경우 1) 클러스터의 호스트 연결이 끊겼거나 전원이 꺼졌거나 2) 전송 영역에 연결된 하나 이상의 가상 시스템 또는 장치가 클러스터에 포함되었기 때문일 수 있습니다. 예를 들어 호스트가 관리 클러스터에 있고 NSX Controller가 호스트에 설치되어 있는 경우 먼저 컨트롤러를 제거하거나 이동합니다.

- 2 NSX VIB를 제거합니다. vCenter Web Client에서 **Networking & Security > 설치 > 호스트 준비(Networking & Security > Installation > Host Preparation)**로 이동합니다. 클러스터를 선택하고 **작업(Actions)**() , **제거(Uninstall)**를 차례대로 선택합니다.

[설치 상태]에 **준비 안 됨(Not Ready)**이 표시됩니다. **준비 안 됨(Not Ready)**을 클릭하면 대화 상자에 에이전트 VIB 설치를 완료하려면 호스트가 유지 보수 모드에 있어야 됨 메시지가 표시됩니다.

- 3 클러스터를 선택하고 **해결(Resolve)** 작업을 클릭하여 제거를 완료합니다.

- 호스트에 NSX 6.2.x 이전 버전 또는 ESXi 5.5가 있으면 제거를 완료하기 위해 재부팅해야 합니다. 클러스터에 DRS가 사용하도록 설정된 경우 DRS가 VM의 실행을 중단하지 않는 제어된 방식으로 호스트 재부팅을 시도합니다. 어떤 이유로 DRS의 재부팅이 실패할 경우 **해결(Resolve)** 작업이 중단됩니다. 이 경우에는 VM을 수동으로 이동한 다음 **해결(Resolve)** 작업을 다시 실행하거나 호스트를 수동으로 재부팅해야 합니다.
- NSX 6.3.0 이상 및 ESXi 6.0 이상이 있는 호스트의 경우 제거를 완료하기 위해 호스트를 유지 보수 모드로 전환해야 합니다. 클러스터에 DRS가 사용하도록 설정된 경우 DRS가 VM의 실행을 중단하지 않는 제어된 방식으로 호스트를 유지 보수 모드로 전환합니다. 어떤 이유로 DRS의 재부팅이 실패할 경우 **해결(Resolve)** 작업이 중단됩니다. 이 경우에는 VM을 수동으로 이동한 다음 **해결(Resolve)** 작업을 다시 실행하거나 호스트를 수동으로 유지 보수 모드로 전환해야 합니다.

중요 호스트를 수동으로 유지 보수 모드로 전환한 경우 먼저 호스트 VIB 제거가 완료되었는지 확인한 후에 호스트의 유지 보수 모드 설정을 해제해야 합니다.

- a vSphere Web Client에서 [최근 작업] 창을 확인합니다.
- b **호스트 준비(Host Preparation)** 탭에서 호스트가 제거된 클러스터의 [설치 상태]에 녹색 확인 표시가 있는지 확인하십시오.

[설치 상태]가 설치 중이면 제거 작업이 여전히 진행 중인 것입니다.

안전한 방법으로 NSX 설치 제거

NSX를 완전히 제거하면 호스트 VIB, NSX Manager, 컨트롤러, 모든 VXLAN 구성, 논리적 스위치, 논리적 라우터, NSX 방화벽, Guest Introspection 및 vCenter NSX 플러그인이 제거됩니다. 클러스터의 모든 호스트에 대해 해당 단계를 따라야 합니다. vCenter Server에서 NSX 플러그인을 제거하기 전에 클러스터에서 네트워크 가상화 구성 요소를 제거하는 것이 좋습니다.

참고 NSX(예: 컨트롤러 및 Edge)에서 배포한 장치를 vCenter에서 직접 제거하지 마십시오. 항상 vSphere Web Client의 **Networking & Security** 탭을 사용하여 NSX 장치를 관리 및 제거하십시오.

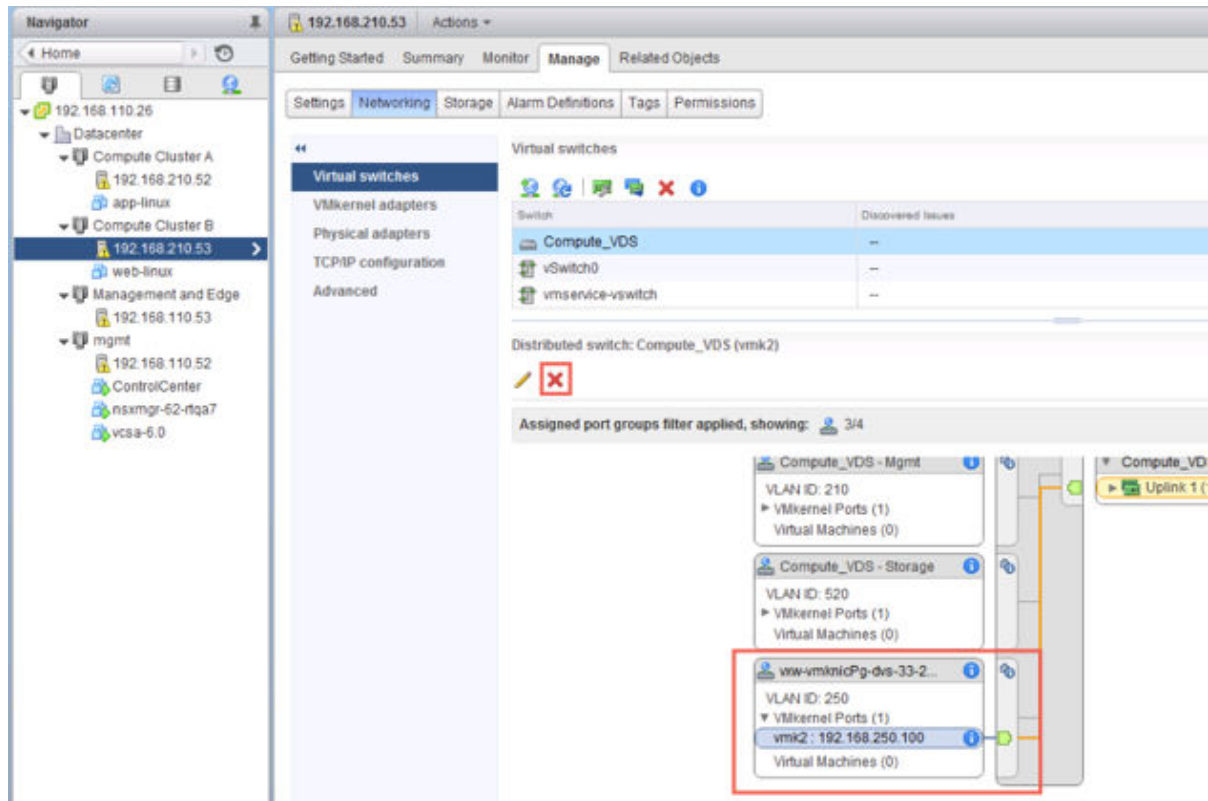
사전 요구 사항

- 엔터프라이즈 관리자 또는 NSX 관리자 역할을 할당받아야 합니다.
- 호스트 준비 상태를 되돌리기 전에 등록된 모든 파트너 솔루션과 끝점 서비스를 제거해야 클러스터의 서비스 VM이 정상적으로 제거됩니다.
- 모든 NSX Edge를 삭제합니다. [NSX Edge Services Gateway](#) 또는 [논리적 분산 라우터 제거](#)를 참조하십시오.
- 전송 영역에 있는 가상 시스템을 논리적 스위치로부터 분리하고 논리적 스위치를 삭제합니다. [논리적 스위치 제거](#)를 참조하십시오.
- 호스트 클러스터에서 NSX를 제거합니다. [호스트 클러스터에서 NSX 제거](#)를 참조하십시오.

절차

- 1 전송 영역을 삭제합니다.
- 2 NSX Manager 장치 및 모든 NSX Controller 장치 VM을 디스크에서 삭제합니다.
- 3 남아 있는 모든 VTEP vmkernel 인터페이스를 제거합니다.

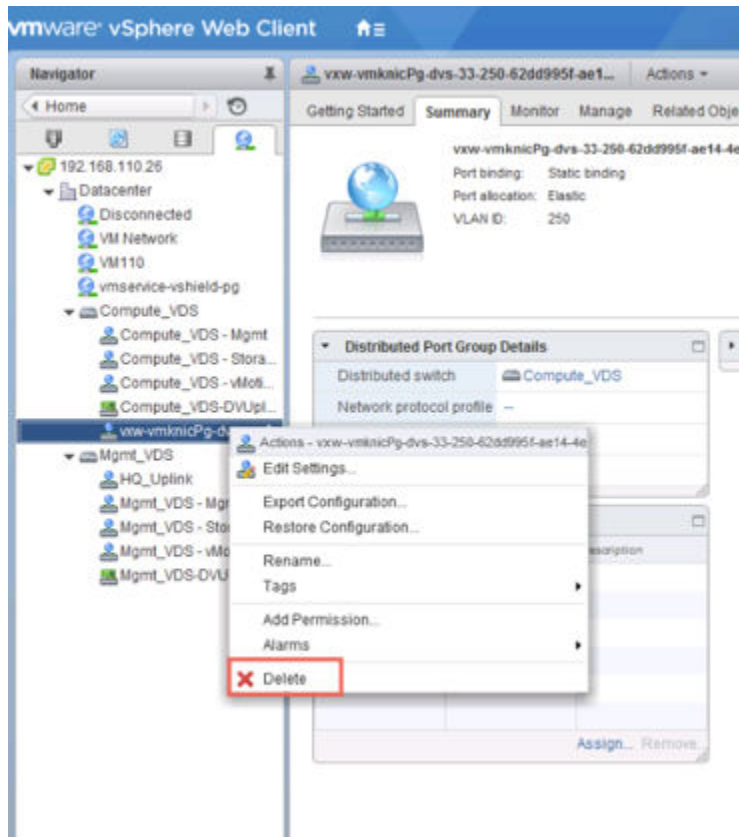
예:



일반적으로 VTEP vmkernel 인터페이스는 앞서 수행한 제거 작업의 결과로 이미 삭제된 상태입니다.

4 VTEP에 사용되는 나머지 dvPortgroup을 모두 제거합니다.

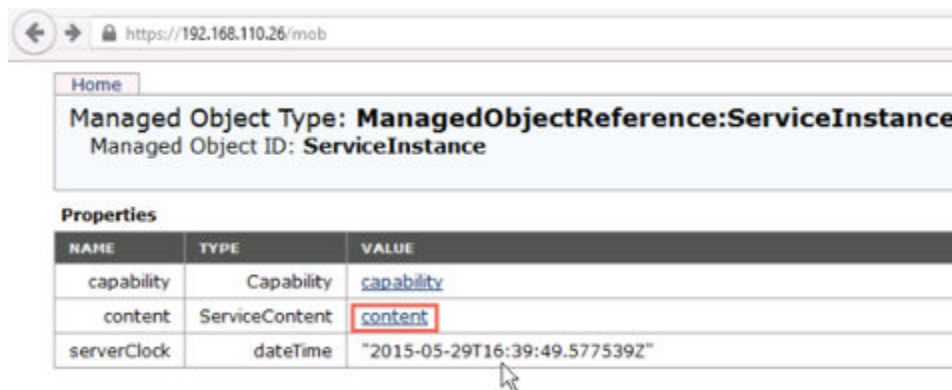
예:



일반적으로 VTEP에 사용되는 dvPortgroup은 앞서 수행한 제거 작업의 결과로 이미 삭제된 상태입니다.

- 5 VTEP vmkernel 인터페이스 또는 dvPortgroup을 제거한 경우 호스트를 재부팅하십시오.
- 6 NSX Manager 플러그인을 제거할 vCenter에 대해 https://your_vc_server/mob의 MOB(Managed Object Browser)에 로그인합니다.
- 7 콘텐츠(Content)를 클릭합니다.

예:



8 ExtensionManager를 클릭합니다.

← → <https://192.168.110.26/mob/?moid=ServiceInstance&doPath=content>

[Home](#)

Data Object Type: ServiceContent
Parent Managed Object ID: **ServiceInstance**
Property Path: **content**

Properties

NAME	TYPE	VALUE
about	AboutInfo	about
accountManager	ManagedObjectReference:HostLocalAccountManager	Unset
alarmManager	ManagedObjectReference:AlarmManager	AlarmManager
authorizationManager	ManagedObjectReference:AuthorizationManager	AuthorizationManager
certificateManager	ManagedObjectReference:CertificateManager	certificateManager
clusterProfileManager	ManagedObjectReference:ClusterProfileManager	ClusterProfileManager
complianceManager	ManagedObjectReference:ProfileComplianceManager	MoComplianceManager
customFieldsManager	ManagedObjectReference:CustomFieldsManager	CustomFieldsManager
customizationSpecManager	ManagedObjectReference:CustomizationSpecManager	CustomizationSpecManager
datastoreNamespaceManager	ManagedObjectReference:DatastoreNamespaceManager	DatastoreNamespaceManager
diagnosticManager	ManagedObjectReference:DiagnosticManager	DiagMgr
dvSwitchManager	ManagedObjectReference:DistributedVirtualSwitchManager	DVSManager
eventManager	ManagedObjectReference:EventManager	EventManager
extensionManager	ManagedObjectReference:ExtensionManager	ExtensionManager
fileManager	ManagedObjectReference:FileManager	FileManager
guestOperationsManager	ManagedObjectReference:GuestOperationsManager	questOperationsManager
hostProfileManager	ManagedObjectReference:HostProfileManager	HostProfileManager

9 UnregisterExtension을 클릭합니다.

Methods

RETURN TYPE	NAME
Extension	FindExtension
string	GetPublicKey
ExtensionManagerIpAllocationUsage[]	QueryExtensionIpAllocationUsage
ManagedObjectReference:ManagedEntity[]	QueryManagedBy
void	RegisterExtension
void	SetExtensionCertificate
void	SetPublicKey
void	UnregisterExtension
void	UpdateExtension

- 10 `com.vmware.vShieldManager` 문자열을 입력하고 **메서드 호출(Invoke Method)**을 클릭합니다.

Managed Object Type:
ManagedObjectReference:ExtensionManager
 Managed Object ID: `ExtensionManager`
 Method: `UnregisterExtension`

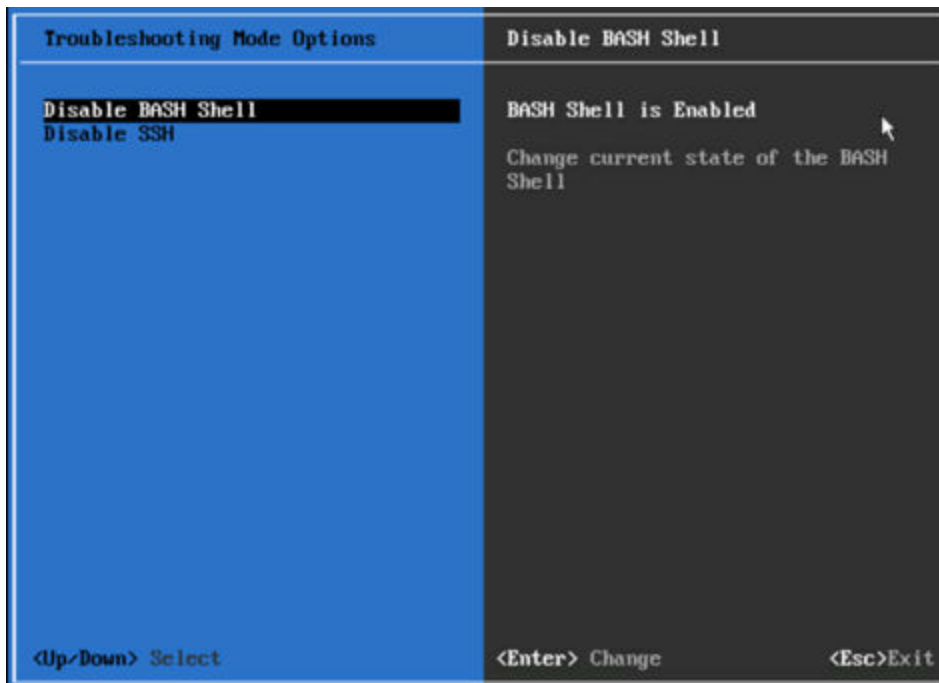
void UnregisterExtension

Parameters

NAME	TYPE	VALUE
<code>extensionKey</code> (required)	string	<code>com.vmware.vShieldManager</code>

[Invoke Method](#)

- 11 vSphere 6 vCenter Appliance를 실행 중이면 콘솔을 시작하고 **문제 해결 모드 옵션(Troubleshooting Mode Options)**에서 BASH 셸을 사용하도록 설정합니다.



BASH 셸을 사용하도록 설정하는 또 다른 방법은 루트로 로그인한 후 `shell.set --enabled true` 명령을 실행하는 것입니다.

- 12 NSX용 vSphere Web Client 디렉토리를 삭제한 다음 Web Client 서비스를 다시 시작합니다.

NSX용 vSphere Web Client 디렉토리의 이름은 `com.vmware.vShieldManager.**`이고 위치는 다음과 같습니다.

- Windows용 VMware vCenter Server – `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity\`

- VMware vCenter Server Appliance - /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/

vCenter Server Appliance를 다시 시작합니다.

- vCenter Server Appliance 6.0에서 vCenter Server 셸에 루트 사용자 자격으로 로그인한 후 다음 명령을 실행합니다.

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

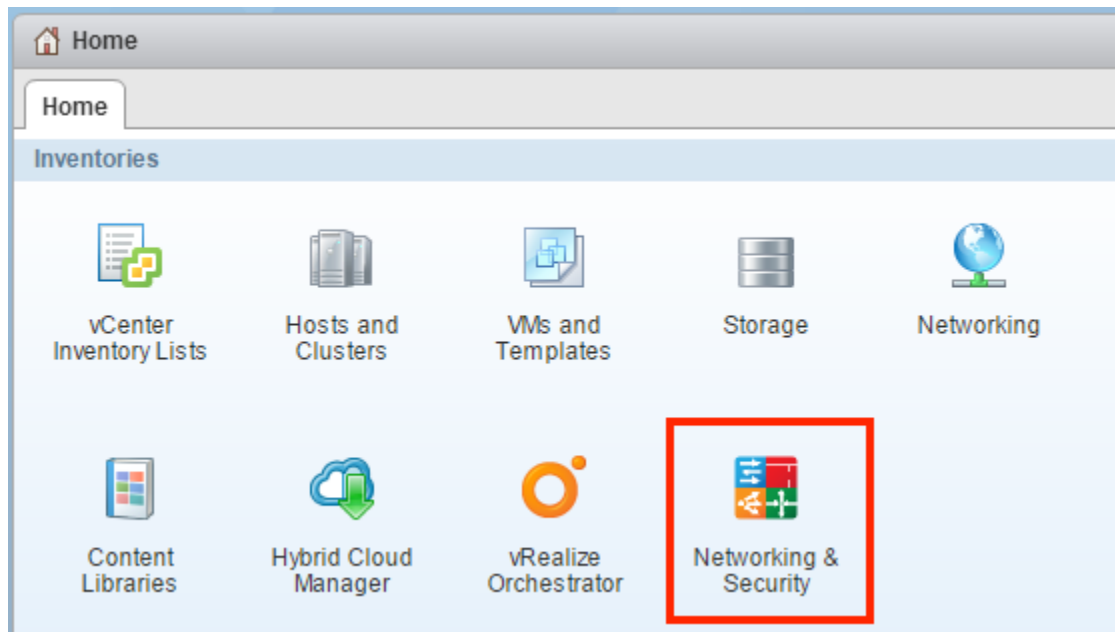
- Windows의 vCenter Server 6.0에서는 다음 명령을 실행하여 이 작업을 수행할 수 있습니다.

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

결과

NSX Manager 플러그인이 vCenter에서 제거됩니다. 확인하려면 vCenter에서 로그아웃하고 다시 로그인합니다.

NSX Manager 플러그인 **Networking & Security** 아이콘이 더 이상 vCenter Web Client 홈 화면에 나타나지 않습니다.



관리 > 클라이언트 플러그인(Administration > Client Plug-Ins)으로 이동하고 플러그인 목록에 **NSX 사용자 인터페이스 플러그인(NSX User Interface plugin)**이 없는지 확인합니다.

