

# NSX-T Data Center 관리 가이드

수정 날짜: 2019년 5월 24일  
VMware NSX-T Data Center 2.3



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](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://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](http://www.vmware.com/kr)

Copyright © 2018, 2019 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

# 목차

## VMware NSX-T Data Center 관리 정보 9

### 1 논리적 스위치 및 VM 연결 구성 10

BUM 프레임 복제 모드 이해 11

논리적 스위치 생성 12

계층 2 브리징 13

브리지 클러스터 생성 15

브리지 프로파일 생성 16

계층 2 브리지 지원 논리적 스위치 생성 16

NSX Edge 업링크에 대한 VLAN 논리적 스위치 생성 18

VM을 논리적 스위치에 연결 20

vCenter Server에 호스팅된 VM을 NSX-T Data Center 논리적 스위치에 연결 20

독립 실행형 ESXi에 호스팅된 VM을 NSX-T Data Center 논리적 스위치에 연결 22

KVM에 호스팅된 VM을 NSX-T Data Center 논리적 스위치에 연결 27

계층 2 연결 테스트 28

### 2 논리적 스위치 포트 32

논리적 스위치 포트 생성 32

논리적 스위치 포트 활동 모니터링 33

### 3 논리적 스위치 및 논리적 포트에 대한 스위칭 프로파일 34

QoS 스위칭 프로파일 이해 35

사용자 지정 QoS 스위칭 프로파일 구성 36

IP 검색 스위칭 프로파일 이해 37

IP 검색 스위칭 프로파일 구성 38

SpoofGuard 이해 39

포트 주소 바인딩 구성 40

SpoofGuard 스위칭 프로파일 구성 40

스위치 보안 스위칭 프로파일 이해 41

사용자 지정 스위치 보안 스위칭 프로파일 구성 41

MAC 관리 스위칭 프로파일 이해 42

MAC 관리 스위칭 프로파일 구성 43

사용자 지정 프로파일을 논리적 스위치에 연결 44

사용자 지정 프로파일을 논리적 포트에 연결 45

### 4 Tier-1 논리적 라우터 47

Tier-1 논리적 라우터 생성 48

Tier-1 논리적 라우터에서 다운링크 포트 추가 49

- Tier-0 또는 Tier-1 논리적 라우터에 VLAN 포트 추가 50
- Tier-1 논리적 라우터에서 경로 보급 구성 51
- Tier-1 논리적 라우터 정적 경로 구성 52
- 독립형 Tier-1 논리적 라우터 생성 54

## 5 Tier-0 논리적 라우터 56

- Tier-0 논리적 라우터 생성 58
- Tier-0과 Tier-1 연결 59
  - Tier-0 라우터에 Tier-1 라우터에서 학습된 경로가 있는지 확인 61
- NSX Edge 업링크를 위해 VLAN 논리적 스위치에 Tier-0 논리적 라우터 연결 62
  - Tier-0 논리적 라우터 및 TOR 연결 확인 63
- 루프백 라우터 포트 추가 65
- Tier-0 또는 Tier-1 논리적 라우터에 VLAN 포트 추가 66
- 정적 경로 구성 66
  - 정적 경로 확인 68
- BGP 구성 옵션 70
  - Tier-0 논리적 라우터에서 BGP 구성 71
  - Tier-0 서비스 라우터에서 BGP 연결 확인 74
- Tier-0 논리적 라우터에서 BFD 구성 75
- Tier-0 논리적 라우터에서 경로 재배포 사용 76
  - 북-남 연결 및 경로 재배포 확인 76
- ECMP 라우팅 이해 79
  - 두 번째 Edge 노드에 대한 업링크 포트 추가 79
  - 두 번째 BGP 인접 네트워크 추가 및 ECMP 라우팅 사용 81
  - ECMP 라우팅 연결 확인 82
- IP 접두사 목록 생성 83
- 커뮤니티 목록 생성 84
- 경로 맵 생성 85
- 전달 타이머 구성 86

## 6 네트워크 주소 변환 87

- Tier-1 NAT 88
  - Tier-1 라우터에서 소스 NAT 구성 88
  - Tier-1 라우터에서 대상 NAT 구성 90
  - 업스트림 Tier-0 라우터로 Tier-1 NAT 경로 보급 92
  - Tier-1 NAT 경로를 물리적 아키텍처로 보급 93
  - Tier-1 NAT 확인 94
- Tier-0 NAT 95
  - Tier-0 라우터에서 소스 및 대상 NAT 구성 95
- 재귀 NAT 96
  - Tier-0 또는 Tier-1 논리적 라우터에서 재귀 NAT 구성 98

<b>7</b>	<b>방화벽 섹션 및 방화벽 규칙</b>	<b>100</b>
	방화벽 규칙 섹션 추가	101
	방화벽 규칙 섹션 삭제	102
	섹션 규칙 사용 및 사용 안 함	102
	섹션 로그 사용 및 사용 안 함	102
	방화벽 규칙 정보	103
	방화벽 규칙 추가	104
	방화벽 규칙 삭제	106
	기본 분산 방화벽 규칙 편집	106
	방화벽 규칙 순서 변경	107
	방화벽 규칙 필터링	108
	논리 스위치 브리지 포트에 대한 방화벽 구성	108
	방화벽 제외 목록 구성	109
	방화벽 사용 및 사용 안 함	109
	논리적 라우터에 방화벽 규칙 추가 또는 삭제	109
<b>8</b>	<b>VPN(Virtual Private Network)</b>	<b>111</b>
	IPSec VPN 구성	112
	L2VPN 구성	115
<b>9</b>	<b>개체, 그룹, 서비스 및 VM 관리</b>	<b>117</b>
	IP 집합 생성	117
	IP 풀 생성	118
	MAC 집합 생성	118
	NSGroup 생성	119
	서비스 및 서비스 그룹 구성	120
	NSService 생성	121
	VM용 태그 관리	121
<b>10</b>	<b>논리적 로드 밸런서</b>	<b>123</b>
	키 로드 밸런서 개념	123
	로드 밸런서 리소스 크기 조정	124
	지원되는 로드 밸런서 기능	125
	로드 밸런서 토폴로지	126
	로드 밸런서 구성 요소 구성	127
	로드 밸런서 생성	128
	액티브 상태 모니터 구성	129
	패시브 상태 모니터 구성	132
	로드 밸런싱을 위한 서버 풀 추가	133
	가상 서버 구성 요소 구성	137

## 11 DHCP 157

- DHCP 서버 프로파일 생성 157
- DHCP 서버 생성 158
- DHCP 서버를 논리적 스위치에 연결 159
- 논리적 스위치에서 DHCP 서버 분리 159
- DHCP 릴레이 프로파일 생성 159
- DHCP 릴레이 서비스 생성 160
- 논리적 라우터 포트에 DHCP 서비스 추가 160

## 12 메타데이터 프록시 162

- 메타데이터 프록시 서버 추가 162
- 메타데이터 프록시 서버를 논리적 스위치에 연결 164
- 논리적 스위치에서 메타데이터 프록시 서버 분리 164

## 13 IP 주소 관리 165

- IP 블록 관리 165
- IP 블록에 대한 서브넷 관리 166

## 14 NSX 정책 167

- 개요 167
- 적용 지점 추가 168
- 서비스 추가 169
- 도메인 추가 169
- NSX Policy Manager의 백업 구성 170
- NSX Policy Manager 백업 171
- NSX Policy Manager 복원 171
- vIDM 호스트를 NSX Policy Manager와 연결 172
- 역할 할당 관리 173

## 15 서비스 삽입 175

- 개요 175
- 서비스 등록 176
- 서비스 인스턴스 배포 178
- 트래픽 리디렉션 구성 179
- 트래픽 리디렉션 모니터링 179

## 16 NSX Cloud 181

- Cloud Service Manager 181
  - 클라우드 182
  - 시스템 188
- 격리 정책 관리 191

격리 정책을 사용하거나 사용하지 않도록 설정하는 방법	191
격리 정책을 사용하지 않을 때의 영향	192
격리 정책을 사용할 때의 영향	193
공용 클라우드에 대한 NSX Cloud 보안 그룹	195
워크로드 VM 등록 및 관리의 개요	196
지원되는 운영 체제	196
Microsoft Azure에서 워크로드 VM을 등록하는 방법	196
AWS에서 워크로드 VM을 등록하는 방법	197
워크로드 VM 등록	198
공용 클라우드에서 VM 태그 지정	198
NSX 에이전트 설치	199
NSX 에이전트 자동 설치	204
워크로드 VM 관리	205
관리 워크로드 VM 액세스	205
NSX-T Data Center 및 공용 클라우드 태그를 사용하여 VM 그룹화	206
워크로드 VM에 대한 마이크로 세분화 설정	209
공용 클라우드에 대해 NSX-T Data Center 기능을 사용하는 방법	210
고급 NSX Cloud 기능 사용	213
Syslog 전달 사용	213
문제 해결	213
NSX Cloud 구성 요소 확인	213
문제 해결 FAQ	214

## 17 작업 및 관리 216

라이선스 키 추가	217
사용자 계정 및 역할 기반 액세스 제어 관리	217
CLI 사용자 암호 변경	217
인증 정책 설정	218
vIDM 호스트에서 인증서 지문 가져오기	219
vIDM 호스트를 NSX-T에 연결	219
NSX Manager, vIDM 및 관련 구성 요소 간의 시간 동기화	221
역할 기반 액세스 제어	222
역할 할당 관리	226
주체 ID 보기	227
인증서 설정	227
인증서 서명 요청 파일 생성	227
CA 인증서 가져오기	229
인증서 가져오기	229
자체 서명된 인증서 생성	230
인증서 교체	231
인증서 해지 목록 가져오기	231

CSR 인증서 가져오기	232
장치 구성	233
계산 관리자 추가	234
태그 관리	235
개체 검색	235
원격 서버의 SSH 지문 찾기	236
NSX Manager 백업 및 복원	237
NSX Manager 구성 백업	238
NSX Manager 구성 복원	240
NSX Controller 클러스터 복원	243
장치 및 장치 클러스터 관리	245
NSX Manager 관리	245
NSX Controller 클러스터 관리	246
NSX Edge 클러스터 관리	252
로그 메시지	257
원격 로깅 구성	258
로그 메시지 ID	259
IPFIX 구성	261
스위치 IPFIX 프로파일 구성	262
방화벽 IPFIX 수집기 구성	263
ESXi IPFIX 템플릿	264
KVM IPFIX 템플릿	268
Traceflow를 사용하여 패킷의 경로 추적	431
포트 연결 정보 보기	432
논리적 스위치 포트 활동 모니터링	433
포트 미러링 세션 모니터링	433
패브릭 노드 모니터링	436
VM에서 실행되는 애플리케이션에 대한 데이터 보기	437
지원 번들 수집	437
고객 환경 향상 프로그램	438
고객 환경 향상 프로그램 구성 편집	438



# VMware NSX-T Data Center 관리 정보

“NSX-T Data Center 관리 가이드”에서는 논리적 스위치 및 포트를 생성하는 방법과 계층화된 논리적 라우터용 네트워킹을 설정하는 방법을 비롯하여 VMware NSX-T Data Center에 대한 네트워킹을 구성하고 관리하는 방법에 대한 정보를 제공합니다. 또한 NAT, 방화벽, SpoofGuard, 그룹화 및 DHCP를 구성하는 방법도 설명합니다.

## 대상 사용자

이 정보는 NSX-T Data Center를 구성하려는 모든 사용자를 대상으로 합니다. 이 정보는 가상 시스템 기술, Networking & Security 작업에 익숙한 숙련된 Windows 또는 Linux 시스템 관리자를 대상으로 작성되었습니다.

## VMware 기술 자료 용어집

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

# 논리적 스위치 및 VM 연결 구성

# 1

NSX-T Data Center 논리적 스위치는 기본 하드웨어와 완전히 분리된 가상 환경에서 스위칭 기능, 브로드캐스트, 알 수 없는 유니캐스트, 멀티캐스트(BUM) 트래픽을 재현합니다.

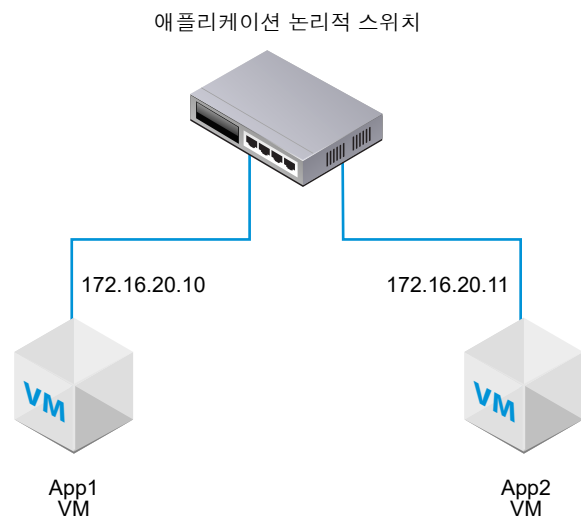
**NSX Cloud 참고** NSX Cloud를 사용 중인 경우 NSX Cloud에 필요한 구성, 지원되는 기능 및 자동 생성된 논리적 엔티티의 목록은 [공용 클라우드에 대해 NSX-T Data Center 기능을 사용하는 방법](#)의 내용을 참조하십시오.

논리적 스위치는 가상 시스템을 연결할 수 있는 네트워크 연결을 제공한다는 점에서 VLAN과 비슷합니다. VM을 동일한 논리적 스위치에 연결하면 VM이 하이퍼바이저 간의 터널을 통해 서로 통신할 수 있습니다. 각 논리적 스위치에는 VLAN ID와 같은 VNI(가상 네트워크 식별자)가 있습니다. VLAN과 달리, VNI는 VLAN ID의 한도 너머까지 잘 확장됩니다.

VNI 값 풀을 보고 편집하려면 NSX Manager에 로그인하고 **패브릭 > 프로파일**로 이동하여 **구성** 탭을 클릭합니다. 풀을 너무 작게 만들 경우, 모든 VNI 값이 사용 중이면 논리적 스위치를 생성하지 못할 수 있습니다. 논리적 스위치를 삭제하면 VNI 값이 다시 사용되지만 6시간 후에만 가능합니다.

논리적 스위치를 추가하는 경우 구축하려는 토폴로지를 계획하는 것이 중요합니다.

그림 1-1. 논리적 스위치 토폴로지



예를 들어 토폴로지는 2개의 VM에 연결된 단일 논리적 스위치를 보여줍니다. 두 개의 VM은 다른 호스트 또는 동일한 호스트에 있거나 다른 호스트 클러스터 또는 동일한 호스트 클러스터에 있을 수 있습니다. 이 예의 VM이 동일한 가상 네트워크에 있으므로 VM에 구성된 기본 IP 주소는 동일한 서브넷에 있습니다.

본 장은 다음 항목을 포함합니다.

- BUM 프레임 복제 모드 이해
- 논리적 스위치 생성
- 계층 2 브리징
- NSX Edge 업링크에 대한 VLAN 논리적 스위치 생성
- VM을 논리적 스위치에 연결
- 계층 2 연결 테스트

## BUM 프레임 복제 모드 이해

각 호스트 전송 노드는 터널 끝점입니다. 각 터널 끝점에는 IP 주소가 있습니다. 이러한 IP 주소는 전송 노드에 대한 IP 풀 또는 DHCP의 구성에 따라 동일한 서브넷 또는 다른 서브넷에 있을 수 있습니다.

다른 호스트에 있는 두 VM이 직접 통신할 경우 플러드에 대한 요구 없이, 유니캐스트 캡슐화 트래픽이 두 하이퍼바이저에 연결된 두 터널 끝점 IP 주소 사이에서 교환됩니다.

하지만 계층 2 네트워크와 마찬가지로, 경우에 따라 VM에서 시작된 트래픽을 플러딩해야 합니다. 즉, 동일한 논리적 스위치에 속하는 다른 모든 VM으로 전송해야 합니다. 이는 계층 2 브로드캐스트, 알 수 없는 유니캐스트 및 멀티캐스트 트래픽(BUM 트래픽)이 있는 경우입니다. 단일 NSX-T Data Center 논리적 스위치가 여러 하이퍼바이저에 걸쳐 있을 수 있는 경우를 생각해봅시다. 지정된 하이퍼바이저의 VM에서 시작된 BUM 트래픽은 동일한 논리적 스위치에 연결된 다른 VM을 호스팅하는 원격 하이퍼바이저로 복제되어야 합니다. 이러한 플러딩을 사용할 수 있도록 NSX-T Data Center에서는 다음 두 가지 다른 복제 모드를 지원합니다.

- 계층 구조식 2계층(경우에 따라 MTEP라고도 함)
- 헤드(경우에 따라 소스라고도 함)

계층 구조식 2계층 복제 모드는 다음 예에 나와 있습니다. VNI(가상 네트워크 식별자) 5000, 5001 및 5002에 연결된 VM을 가진 호스트 A가 있다고 가정해보겠습니다. VNI는 VLAN과 유사하지만 각 논리적 스위치에 단일 VNI가 연결되어 있다고 생각하면 됩니다. 이러한 이유로 용어 VNI와 논리적 스위치를 혼용해서 사용하는 경우가 있습니다. 호스트가 VNI에 있다고 가정하면 해당 VNI가 있는 논리적 스위치에 연결된 VM이 있는 것입니다.

터널 끝점 테이블에는 호스트와 VNI 간 연결이 표시됩니다. 호스트 A는 VNI 5000에 대한 터널 끝점 테이블을 검사하고 VNI 5000의 다른 호스트에 대해 터널 끝점 IP 주소를 확인합니다.

이러한 일부 VNI 연결은 호스트 A의 터널 끝점과 동일한 IP 서브넷(IP 세그먼트라고도 함)에 위치합니다. 이러한 각 연결에 대해 호스트 A는 모든 BUM 프레임의 별도 복사본을 생성하고 각 호스트로 직접 복사본을 전송합니다.

다른 호스트의 터널 끝점은 다른 서브넷 또는 IP 세그먼트에 있습니다. 둘 이상의 터널 끝점이 있는 각 세그먼트의 경우 호스트 A는 이러한 끝점 중 하나를 Replicator로 지명합니다.

Replicator는 호스트 A에서 VNI 5000에 대한 각 BUM 프레임 복사본을 1개 수신합니다. 이 복사본은 캡슐화된 헤더에서 로컬로 [복제]로 지정됩니다. 호스트 A는 Replicator와 같은 IP 세그먼트의 다른 호스트로 복사본을 전송하지 않습니다. VNI 5000에 있으며 해당 Replicator 호스트와 동일한 IP 세그먼트에 있는 알려진 각 호스트에 대한 BUM 프레임 복사본을 생성하는 작업은 Replicator에서 담당합니다.

이 프로세스는 VNI 5001 및 5002에 대해 복제됩니다. 터널 끝점 및 결과 Replicator 목록은 VNI마다 다를 수 있습니다.

헤드엔드 복제라고도 하는 헤드 복제를 사용하는 경우에는 Replicator가 없습니다. 호스트 A는 VNI 5000에서 알고 있는 각 터널 끝점에 대해 각 BUM 프레임 복사본을 생성한 후 전송합니다.

모든 호스트 터널 끝점이 동일한 서브넷에 있는 경우 동작이 다르지 않으므로 어떤 복제 모드를 선택해도 차이가 없습니다. 호스트 터널 끝점이 다른 서브넷에 있는 경우 계층 구조식 2계층 복제를 수행하면 여러 호스트 간에 로드를 분산하는 데 도움이 됩니다. 계층 구조식 2계층은 기본 모드입니다.

## 논리적 스위치 생성

논리적 스위치는 네트워크의 단일 또는 여러 VM에 연결됩니다. 논리적 스위치에 연결된 VM은 하이퍼바이저 간 터널을 사용하여 서로 통신할 수 있습니다.

### 사전 요구 사항

- 전송 영역이 구성되어 있는지 확인합니다. "NSX-T Data Center 설치 가이드"의 내용을 참조하십시오.
- 패브릭 노드가 NSX-T Data Center MPA(관리부 에이전트) 및 NSX-T Data Center LCP(로컬 제어부)에 연결되어 있는지 확인합니다.

GET <https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state> API 호출에서 state는 success여야 합니다. "NSX-T Data Center 설치 가이드"의 내용을 참조하십시오.

- 전송 노드가 전송 영역에 추가되어 있는지 확인합니다. "NSX-T Data Center 설치 가이드"의 내용을 참조하십시오.
- 하이퍼바이저가 NSX-T Data Center 패브릭에 추가되어 있는지와 VM이 이러한 하이퍼바이저에 호스팅되어 있는지 확인합니다.
- 논리적 스위치 토폴로지 및 BUM 프레임 복제 개념을 숙지합니다. [장 1 논리적 스위치 및 VM 연결 구성](#) 및 [BUM 프레임 복제 모드 이해](#)를 참조하십시오.
- NSX Controller 클러스터가 안정적인지 확인합니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 **스위칭 > 스위치**를 선택합니다.

**3 추가**를 클릭합니다.**4** 논리적 스위치 이름 및 필요한 경우 설명을 입력합니다.**5** 논리적 스위치에 대한 전송 영역을 선택합니다.

동일한 전송 영역에 있는 논리적 스위치에 연결된 VM은 서로 통신할 수 있습니다.

**6** 업링크 팀 구성 정책의 이름을 입력합니다.**7 관리 상태를 실행** 또는 **종료**로 설정합니다.**8** 논리적 스위치에 대한 복제 모드를 선택합니다.

오버레이 논리적 스위치에는 복제 모드(계층 구조식 2계층 또는 헤드)가 필요하지만 VLAN 기반 논리적 스위치에는 필요하지 않습니다.

복제 모드	설명
계층 구조식 2계층	Replicator는 동일한 VNI 내의 다른 호스트로 BUM 트래픽의 복제를 수행하는 호스트입니다. 각 호스트는 모든 VNI에서 하나의 호스트 터널 끝점을 Replicator로 지명합니다. 이 작업은 각 VNI에 대해 수행됩니다.
HEAD	호스트는 각 BUM 프레임의 복사본을 생성하고 이를 각 VNI에 대해 알고 있는 각 터널 끝점으로 전송합니다.

**9** (선택 사항) VLAN 태그 지정을 위해 VLAN ID 또는 VLAN ID 범위를 지정합니다.

이 스위치에 연결된 VM에 게스트 VLAN 태그 지정을 지원하려면 트렁크 VLAN ID 범위라고도 하는 VLAN ID 범위를 지정해야 합니다. 논리적 포트는 트렁크 VLAN ID 범위를 기반으로 패킷을 필터링하며 게스트 VM은 트렁크 VLAN ID 범위에 기반한 자체 VLAN ID로 패킷에 태그를 지정할 수 있습니다.

**10** (선택 사항) **스위칭 프로파일** 탭을 클릭하고 스위칭 프로파일을 선택합니다.**11 저장**을 클릭합니다.

NSX Manager UI에서 새 논리적 스위치는 클릭할 수 있는 링크입니다.

## 다음에 수행할 작업

논리적 스위치에 VM을 연결합니다. [VM을 논리적 스위치에 연결](#)의 내용을 참조하십시오.

## 계층 2 브리징

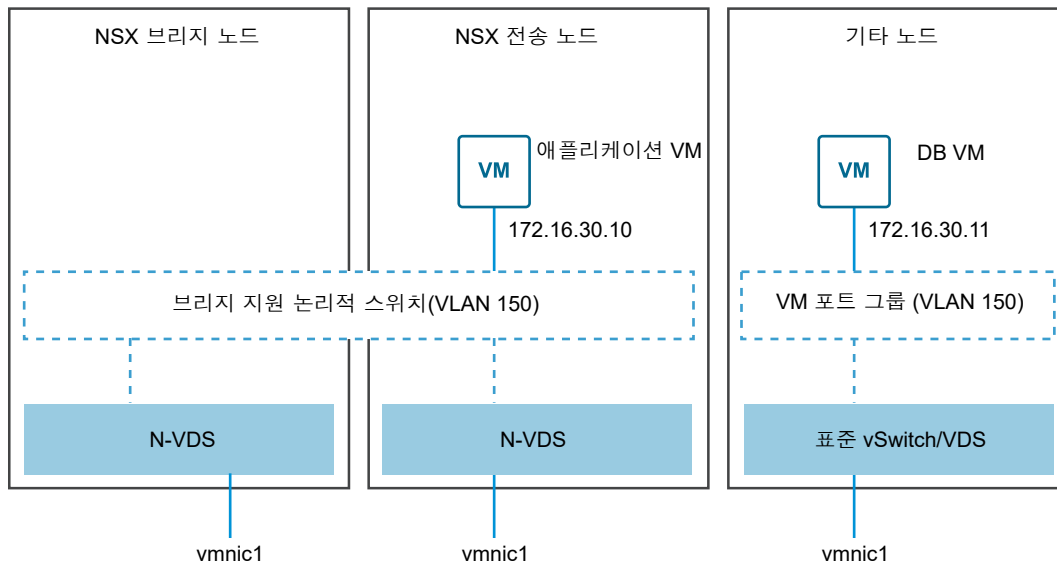
NSX-T Data Center 논리적 스위치에 VLAN 지원 포트 그룹에 대한 계층 2 연결이 필요하거나 NSX-T Data Center 배포 외부에 있는 게이트웨이 등의 다른 디바이스에 연결해야 할 경우 NSX-T Data Center 계층 2 브리징을 사용할 수 있습니다. 이는 물리적 및 가상 워크로드에서 서버넷을 분할해야 하는 마이그레이션 시나리오에서 특히 유용합니다.

계층 2 브리징에 관련된 NSX-T Data Center 개념은 브리지 클러스터, 브리지 끝점 및 브리지 노드입니다. 브리지 클러스터는 브리지 노드의 HA(고가용성) 모음입니다. 브리지 노드는 브리징을 수행하는 전송 노드입니다. 가상 및 물리적 배포를 브리징하는 데 사용되는 각 논리적 스위치에는 연결된 VLAN ID가 있습니다. 브리지 끝점은 브리지 클러스터 ID 및 연결된 VLAN ID와 같은 브리지의 물리적 특성을 식별합니다.

ESXi 호스트 전송 노드 또는 NSX Edge 전송 노드를 사용하여 계층 2 브리징을 구성할 수 있습니다. 브리징에 ESXi 호스트 전송 노드를 사용하려면 브리지 클러스터를 생성합니다. 브리징에 NSX Edge 전송 노드를 사용하려면 브리지 프로파일을 생성합니다.

다음 예에서 2개의 NSX-T Data Center 전송 노드는 동일한 오버레이 전송 영역에 속합니다. 따라서 NSX 관리 가상 분산 스위치(N-VDS, 이전 이름: 호스트 스위치)를 동일한 브리지 지원 논리적 스위치에 연결할 수 있습니다.

그림 1-2. 브리지 토폴로지



왼쪽의 전송 노드는 브리지 클러스터에 속하므로 브리지 노드입니다.

논리적 스위치는 브리지 클러스터에 연결되므로 브리지 지원 논리적 스위치라고 합니다. 브리지 지원이 가능하려면 논리적 스위치가 VLAN 전송 영역이 아닌 오버레이 전송 영역에 있어야 합니다.

중간 전송 노드는 브리지 클러스터에 속하지 않습니다. 이는 일반적인 전송 노드입니다. KVM 또는 ESXi 호스트일 수 있습니다. 다이어그램에서 이 노드의 "애플리케이션 VM"이라고 하는 VM은 브리지 지원 논리적 스위치에 연결됩니다.

오른쪽의 노드는 NSX-T Data Center 오버레이에 속하지 않습니다. VM이 있는 하이퍼바이저(다이어그램에 표시됨) 또는 물리적 네트워크 노드일 수 있습니다. 비 NSX-T Data Center 노드가 ESXi 호스트이면 포트 연결을 위해 표준 vSwitch 또는 vSphere Distributed Switch를 사용할 수 있습니다. 한 가지 요구 사항은 포트 연결의 VLAN ID가 브리지 지원 논리적 스위치에 있는 VLAN ID와 일치해야 한다는 것입니다. 또한 통신이 계층 2를 통해 진행되므로, 2개의 엔드 디바이스의 IP 주소가 동일한 서브넷에 있어야 합니다.

설명된 것처럼 브리지의 용도는 두 VM 간의 계층 2 통신을 사용하도록 설정하는 것입니다. 두 VM 간에 트래픽이 전송되면 트래픽은 브리지 노드를 이동합니다.

**참고** ESXi 호스트에서 실행 중인 Edge VM을 사용하여 계층 2 브리징을 제공하는 경우 VLAN 측에서 트래픽을 송수신하는 표준 또는 분산 스위치의 포트 그룹이 무차별 모드여야 합니다. 최적의 성능을 위해 다음 내용에 유의하십시오.

- 동일한 호스트에 있는 무차별 모드의 다른 포트 그룹이 동일한 VLAN 집합을 공유하지 않도록 합니다.
- 활성 및 대기 Edge VM은 서로 다른 호스트에 있어야 합니다. 동일한 호스트에 있으면 VLAN 트래픽을 무차별 모드로 두 VM 모두에 전달해야 하기 때문에 처리량이 7Gbps로 떨어질 수 있습니다.

## 브리지 클러스터 생성

브리지 클러스터는 논리적 스위치에 계층 2 브리징을 제공할 수 있는 ESXi 호스트 전송 노드의 모음입니다.

브리지 클러스터는 최대 2개의 ESXi 호스트 전송 노드를 브리지 노드로 사용할 수 있습니다. 브리지 노드가 두 개이면 브리지 클러스터가 활성-대기 모드에서 고가용성을 제공합니다. 브리지 노드가 하나 필요하다더라도 브리지 클러스터를 생성해야 합니다. 브리지 클러스터를 생성하면 나중에 브리지 노드를 더 추가할 수 있습니다.

### 사전 요구 사항

- 브리지 노드로 사용할 하나 이상의 NSX-T Data Center 전송 노드를 생성합니다.
- 브리지 노드로 사용되는 전송 노드는 ESXi 호스트여야 합니다. KVM은 브리지 노드에서 지원되지 않습니다.
- 브리지 노드에는 호스팅된 VM이 없도록 하는 것을 권장합니다.
- 전송 노드는 하나의 브리지 클러스터에만 추가할 수 있습니다. 동일한 전송 노드를 여러 브리지 클러스터에 추가할 수 없습니다.

### 절차

- 1 탐색 패널에서 **패브릭 > 노드**를 선택합니다.
- 2 **ESXi 브리지 클러스터** 탭을 클릭합니다.
- 3 **추가**를 클릭합니다.
- 4 이름과 설명(선택 사항)을 입력합니다.
- 5 브리지 클러스터에 대한 전송 영역을 선택합니다.
- 6 **사용 가능** 열에서 전송 노드를 선택하고 오른쪽 화살표를 클릭하여 이를 **선택됨** 열로 이동합니다.
- 7 **추가** 버튼을 클릭합니다.

## 다음에 수행할 작업

이제 논리적 스위치를 브리지 클러스터에 연결할 수 있습니다.

## 브리지 프로파일 생성

브리지 프로파일을 사용하면 NSX Edge 클러스터에서 논리적 스위치에 계층 2 브리징을 제공할 수 있습니다.

### 사전 요구 사항

- NSX Edge 전송 노드가 두 개인 NSX Edge 클러스터가 있는지 확인합니다.

### 절차

- 1 탐색 패널에서 **패브릭 > 프로파일**을 선택합니다.
- 2 **Edge 브리지 프로파일** 탭을 클릭합니다.
- 3 **추가**를 클릭합니다.
- 4 이름과 설명(선택 사항)을 입력합니다.
- 5 NSX Edge 클러스터를 선택합니다.
- 6 기본 노드를 선택합니다.
- 7 백업 노드를 선택합니다.
- 8 페일오버 모드를 선택합니다.  
옵션은 **선점** 및 **비선점**입니다.
- 9 **추가** 버튼을 클릭합니다.

## 다음에 수행할 작업

이제 논리적 스위치를 브리지 프로파일에 연결할 수 있습니다.

## 계층 2 브리지 지원 논리적 스위치 생성

NSX-T Data Center 오버레이에 연결된 VM이 있는 경우 NSX-T Data Center 배포 외부에 있는 다른 디바이스 또는 VM과의 계층 2 연결을 제공하기 위해 브리지 지원 논리적 스위치를 구성할 수 있습니다.

토폴로지 예를 보려면 [그림 1-2. 브리지 토폴로지](#)를 참조하십시오.

### 사전 요구 사항

- 브리지 클러스터 또는 브리지 프로파일이 있는지 확인합니다.
- 일반 전송 노드 역할을 하는 하나 이상의 ESXi 또는 KVM 호스트. 이 노드에는 NSX-T Data Center 배포 외부의 디바이스와의 연결이 필요한 호스팅된 VM이 있습니다.
- NSX-T Data Center 배포 외부의 VM 또는 다른 엔드 디바이스. 이 엔드 디바이스는 브리지 지원 논리적 스위치의 VLAN ID와 일치하는 VLAN 포트에 연결되어야 합니다.



- 브리지 지원 논리적 스위치 역할을 하는 오버레이 전송 영역의 단일 논리적 스위치.

## 절차

- 1 브라우저에서 `https://<nsx-mgr>`의 NSX Manager에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 스위칭**을 선택합니다.
- 3 오버레이 스위치(트래픽 유형: 오버레이)의 이름을 클릭합니다.
- 4 **관련 > ESXi 브리지 클러스터** 또는 **관련 > Edge 브리지 프로파일**을 클릭합니다.
- 5 **연결**을 클릭합니다.
- 6 브리지 클러스터에 연결하려면,
  - a 브리지 클러스터를 선택합니다.
  - b VLAN ID를 입력합니다.
  - c **VLAN의 HA**를 사용하거나 사용하지 않도록 설정합니다.
  - d **연결**을 클릭합니다.
- 7 브리지 프로파일에 연결하려면,
  - a 브리지 프로파일을 선택합니다.
  - b 전송 영역을 선택합니다.
  - c VLAN ID를 입력합니다.
  - d **저장**을 클릭합니다.
- 8 아직 연결하지 않은 경우 VM을 논리적 스위치에 연결합니다.

VM은 브리지 클러스터나 브리지 프로파일과 동일한 전송 영역의 전송 노드에 있어야 합니다.

## 결과

NSX-T Data Center 내부 VM에서 NSX-T Data Center 외부 노드로 ping을 전송하여 브리지의 기능을 테스트할 수 있습니다. 예를 들어 [그림 1-2. 브리지 토폴로지](#)에서 NSX-T Data Center 전송 노드의 애플리케이션 VM은 외부 노드의 DB VM을 ping하고 그 반대로도 수행할 수 있어야 합니다.

**모니터** 탭을 클릭하여 브리지 스위치의 트래픽을 모니터링할 수 있습니다.

GET `https://192.168.110.31/api/v1/bridge-endpoints/<endpoint-id>/statistics` API 호출을 사용하여 브리지 트래픽을 볼 수도 있습니다.

```
{
  "tx_packets": {
    "total": 134416,
    "dropped": 0,
    "multicast_broadcast": 0
  },
  "rx_bytes": {
    "total": 22164,
    "multicast_broadcast": 0
  }
}
```

```

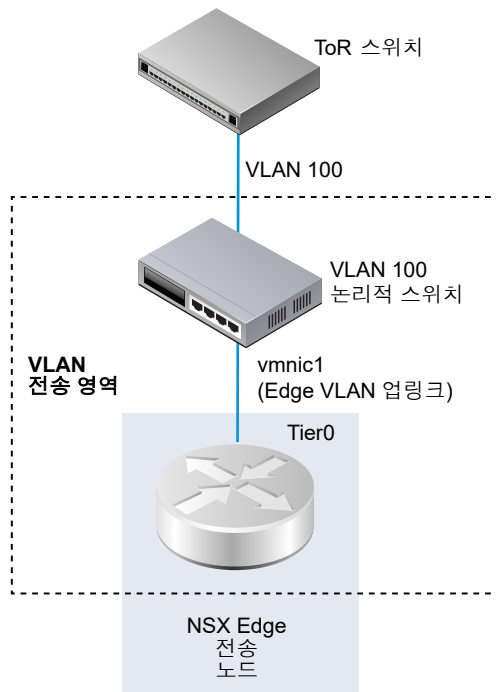
},
"tx_bytes": {
  "total": 8610134,
  "multicast_broadcast": 0
},
"rx_packets": {
  "total": 230,
  "dropped": 0,
  "multicast_broadcast": 0
},
"last_update_timestamp": 1454979822860,
"endpoint_id": "ba5ba59d-22f1-4a02-b6a0-18ef0e37ef31"
}

```

## NSX Edge 업링크에 대한 VLAN 논리적 스위치 생성

Edge 업링크는 VLAN 논리적 스위치를 통과합니다.

VLAN 논리적 스위치를 생성하는 경우 구축하려는 특정 토폴로지를 고려하는 것이 중요합니다. 예를 들어 다음의 간단한 토폴로지는 VLAN 전송 영역 내부의 단일 VLAN 논리적 스위치를 보여줍니다. VLAN 논리적 스위치는 VLAN ID 100을 갖습니다. 이 값은 Edge의 VLAN 업링크에 사용되는 하이퍼 바이저 호스트 포트에 연결된 TOR 포트의 VLAN ID와 일치합니다.



### 사전 요구 사항

- VLAN 논리적 스위치를 생성하려면 먼저 VLAN 전송 영역을 생성해야 합니다.

- NSX-T Data Center vSwitch를 NSX Edge에 추가해야 합니다. Edge를 확인하려면 `get host-switches` 명령을 실행합니다. 예:

```
nsx-edge1> get host-switches

Host Switch      : c0a78378-1c20-432a-9e23-ddb34f1c80c9
Switch Name      : hs1
Transport Zone   : c46dcd72-808a-423d-b4cc-8752c33f6b2c
Transport Zone   : 73def985-d122-4b7b-ab6a-a58176dfc32d
Physical Port    : fp-eth0
Uplink Name      : uplink-1
Transport VLAN   : 4096
Default Gateway  : 192.168.150.1
Subnet Mask      : 255.255.255.0
Local VTEP Device : fp-eth0
Local VTEP IP    : 192.168.150.102
```

- NSX Controller 클러스터가 안정적인지 확인합니다.
- 패브릭 노드가 NSX-T Data Center MPA(관리부 에이전트) 및 NSX-T Data Center LCP(로컬 제어부)에 연결되어 있는지 확인합니다.

GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state` API 호출에서 `state`는 `success`여야 합니다. "NSX-T Data Center 설치 가이드"의 내용을 참조하십시오.

## 절차

- 1 브라우저에서 `https://<nsx-mgr>`의 NSX Manager에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 스위칭**을 선택합니다.
- 3 **추가**를 클릭합니다.
- 4 논리적 스위치의 이름을 입력합니다.
- 5 논리적 스위치에 대한 전송 영역을 선택합니다.
- 6 업링크 팀 구성 정책을 선택합니다.
- 7 관리 상태의 경우 **실행** 또는 **종료**를 선택합니다.
- 8 VLAN ID를 입력합니다.  
물리적 TOR로의 업링크에 대한 VLAN ID가 없으면 VLAN 필드에 0을 입력합니다.
- 9 (선택 사항) **스위칭 프로파일** 탭을 클릭하고 스위칭 프로파일을 선택합니다.

## 결과

**참고** VLAN ID가 동일한 VLAN 논리적 스위치 두 개를 동일한 Edge N-VDS(이전 이름: 호스트 스위치)에 연결할 수 없습니다. VLAN 논리적 스위치와 오버레이 논리적 스위치가 있고, VLAN 논리적 스위치의 VLAN ID가 오버레이 논리적 스위치의 전송 VLAN ID와 같은 경우에도 두 스위치를 동일한 Edge N-VDS에 연결할 수 없습니다.

다음에 수행할 작업

논리적 라우터를 추가합니다.

## VM을 논리적 스위치에 연결

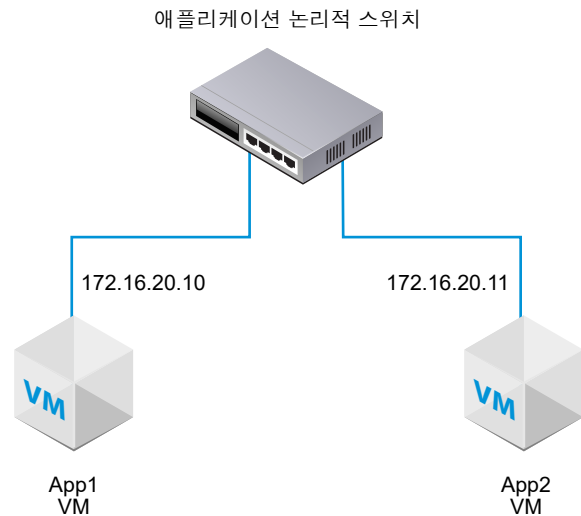
호스트에 따라 VM을 논리적 스위치에 연결하기 위한 구성이 다를 수 있습니다.

논리적 스위치에 연결될 수 있는 지원되는 호스트는 vCenter Server, 독립 실행형 ESXi 호스트 및 KVM 호스트에서 관리되는 ESXi 호스트입니다.

### vCenter Server에 호스팅된 VM을 NSX-T Data Center 논리적 스위치에 연결

vCenter Server에서 관리하는 ESXi 호스트가 있는 경우 웹 기반 vSphere Web Client를 통해 호스트 VM에 액세스할 수 있습니다. 이 경우 다음 절차를 사용하여 VM을 NSX-T Data Center 논리적 스위치에 연결할 수 있습니다.

이 절차에 표시된 예는 app-vm이라는 VM을 app-switch라는 논리적 스위치에 연결하는 방법을 보여줍니다.



설치 기반 vSphere Client 애플리케이션은 VM을 NSX-T Data Center 논리적 스위치에 연결하는 것은 지원하지 않습니다. (웹 기반) vSphere Web Client가 없는 경우 [독립 실행형 ESXi에 호스팅된 VM을 NSX-T Data Center 논리적 스위치에 연결](#)을 참조하십시오.

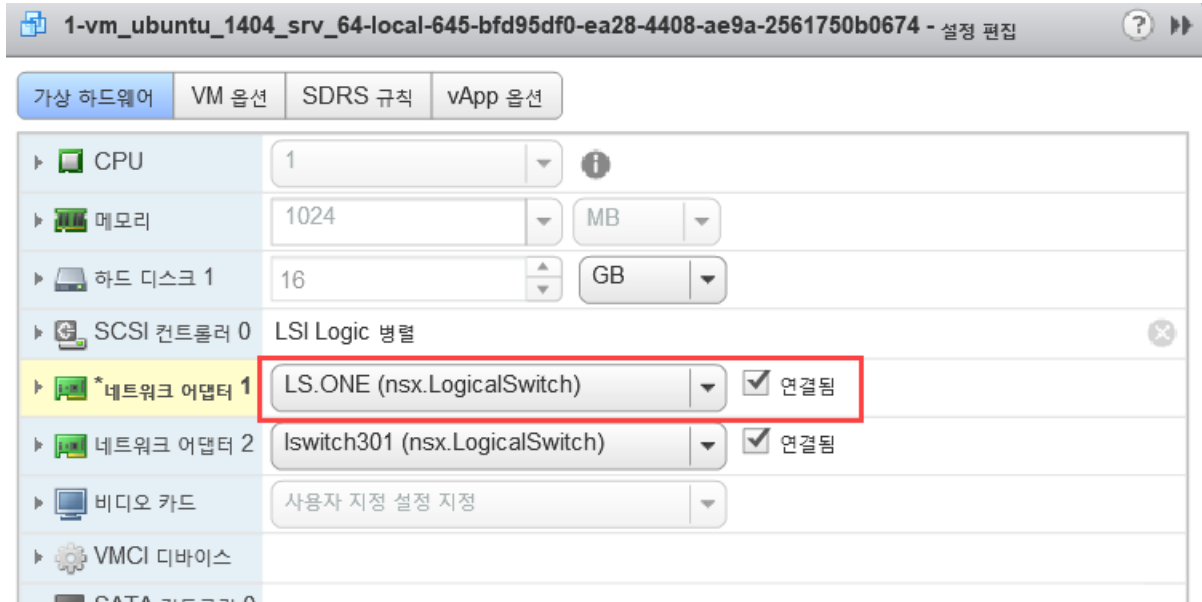
#### 사전 요구 사항

- VM은 NSX-T Data Center 패브릭에 추가된 하이퍼바이저에 호스팅되어야 합니다.
- 패브릭 노드는 NSX-T Data Center 관리부(MPA) 및 NSX-T Data Center 제어부(LCP)에 연결할 수 있어야 합니다.
- 패브릭 노드는 전송 영역에 추가되어야 합니다.
- 논리적 스위치를 생성해야 합니다.

## 절차

- 1 vSphere Web Client에서 VM 설정을 편집하고, VM을 NSX-T Data Center 논리적 스위치에 연결합니다.

예:



- 2 **확인**을 클릭합니다.

## 결과

VM을 논리적 스위치에 연결한 후 논리적 스위치 포트가 논리적 스위치에 추가됩니다. NSX Manager의 **스위칭 > 포트**에서 논리적 스위치 포트를 볼 수 있습니다.

NSX-T Data Center API에서 GET <https://<nsx-mgr>/api/v1/fabric/virtual-machines> API 호출을 사용하여 NSX-T Data Center 연결 VM을 볼 수 있습니다.

NSX-T Data Center Manager UI의 **스위칭 > 포트**에서 VIF 연결 ID가 API 호출에서 찾은 ExternalID와 일치하는 항목을 찾습니다. VM의 ExternalID와 일치하는 VIF 연결 ID를 찾고 관리자 및 작업 상태가 둘 다 [실행]인지 확인합니다.

두 VM이 동일한 논리적 스위치에 연결되어 있고 동일한 서브넷에 IP 주소가 구성된 경우 서로 간에 ping할 수 있어야 합니다.

## 다음에 수행할 작업

논리적 라우터를 추가합니다.

논리적 스위치 포트에서의 활동을 모니터링하여 문제를 해결할 수 있습니다. 자세한 내용은 "NSX-T Data Center 관리 가이드"의 "논리적 스위치 포트 활동 모니터링"을 참조하십시오.

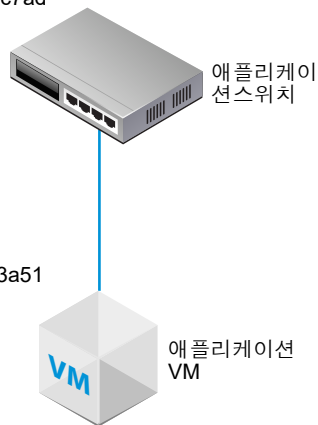
## 독립 실행형 ESXi에 호스팅된 VM을 NSX-T Data Center 논리적 스위치에 연결

독립 실행형 ESXi 호스트가 있는 경우 웹 기반 vSphere Web Client를 통해 호스트 VM에 액세스할 수 없습니다. 이 경우 다음 절차를 사용하여 VM을 NSX-T Data Center 논리적 스위치에 연결할 수 있습니다.

이 절차에 표시된 예는 app-vm이라는 VM을 app-switch라는 논리적 스위치에 연결하는 방법을 보여줍니다.

스위치의 불투명 네트워크 ID:  
22b22448-38bc-419b-bea8-b51126bec7ad

VM의 외부 ID:  
50066bae-0f8a-386b-e62e-b0b9c6013a51



### 사전 요구 사항

- VM은 NSX-T Data Center 패브릭에 추가된 하이퍼바이저에 호스팅되어야 합니다.
- 패브릭 노드는 NSX-T Data Center 관리부(MPA) 및 NSX-T Data Center 제어부(LCP)에 연결할 수 있어야 합니다.
- 패브릭 노드는 전송 영역에 추가되어야 합니다.
- 논리적 스위치를 생성해야 합니다.
- NSX Manager API에 액세스할 수 있어야 합니다.
- VM의 VMX 파일에 대해 쓰기 액세스 권한이 있어야 합니다.

## 절차

- 1 (설치 기반) vSphere Client 애플리케이션 또는 일부 다른 VM 관리 도구를 사용하여 VM을 편집하고 VMXNET 3 이더넷 어댑터를 추가합니다.

명명된 네트워크를 임의로 선택합니다. 이후 단계에서 네트워크 연결을 변경하게 됩니다.

## 하드웨어 사용자 지정

가상 시스템 하드웨어를 구성합니다.

The screenshot shows the 'Hardware' tab in the vSphere Client. The 'New Network' section is highlighted. The configuration is as follows:

Component	Value
CPU	1
메모리	4096 MB
새 하드 디스크	40 GB
새 SCSI 컨트롤러	LSI Logic SAS
새 네트워크	VM Network
실행 상태	<input checked="" type="checkbox"/> 전원을 켤 때 연결
어댑터 유형	VMXNET 3
DirectPath I/O	<input type="checkbox"/> 사용
MAC 주소	자동
새 CD/DVD 드라이브	클라이언트 디바이스
새 플로피 드라이브	클라이언트 디바이스

At the bottom, there is a 'New Device' section with a dropdown set to 'Network' and a 'Add' button.

- 2 NSX-T Data Center API를 사용하여 GET <https://<nsx-mgr>/api/v1/fabric/virtual-machines/<VM-ID>> API 호출을 실행합니다.

결과에서 VM의 externalId를 찾습니다.

예 :

```
GET https://<nsx-mgr>/api/v1/fabric/virtual-machines/60a5a5d5-ea2b-407e-a806-4fdc8468f735
```

```
{
  "resource_type": "VirtualMachine",
  "id": "60a5a5d5-ea2b-407e-a806-4fdc8468f735",
  "display_name": "app-vm",
  "compute_ids": [
    "instanceUid:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "moldOnHost:5",
    "externalId:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "hostLocalId:5",
    "locationId:564dc020-1565-e3f4-f591-ee3953eef3ff",
    "biosUid:4206f47d-fe7-08c5-5bf7-ea26a4c6b18d"
  ],
  "external_id": "50066bae-0f8a-386b-e62e-b0b9c6013a51",
  "type": "REGULAR",
}
```

```
"host_id": "cb82b0fa-a8f1-11e5-92a9-6b7d1f8661fa",
"local_id_on_host": "5"
}
```

### 3 전원을 끄고 호스트에서 VM을 등록 취소합니다.

여기에 표시된 것처럼 VM 관리 도구 또는 ESXi CLI를 사용할 수 있습니다.

```
[user@host:~] vim-cmd /vmsvc/getallvms
Vmid    Name      File           Guest OS      Version  Annotation
5       app-vm    [ds2] app-vm/app-vm.vmx  ubuntuGuest   vmx-08
8       web-vm    [ds2] web-vm/web-vm.vmx   ubuntu64Guest  vmx-08

[user@host:~] vim-cmd /vmsvc/power.off 5
Powering off VM:

[user@host:~] vim-cmd /vmsvc/unregister 5
```

### 4 NSX Manager UI에서 논리적 스위치 ID를 가져옵니다.

예 :



## app-switch

개요   모니터   관리 ▾   관련 ▾

▽ 요약   편집

이름	app-switch
ID	b68e7ac3-877a-420e-af47-53e974c17915
위치	
설명	lswitch202 (created through automation)
관리 상태	● 실행 중
복제 모드	헤드 복제
VLAN	해당 없음
VNI	71681
논리적 포트	1
트래픽 유형	오버레이
전송 영역	transportzone1
업링크 팀 구성 정책 이름	[Use Default]
N-VDS 모드	STANDARD
생성일	9/10/2018, 12:20:46 PM(기준: admin)
마지막 업데이트 날짜	9/26/2018, 2:01:14 PM(기준: admin)

## 5 VM의 VMX 파일을 수정합니다.

**ethernet1.networkName** = "<이름>" 필드를 삭제하고 다음 필드를 추가합니다.

- ethernet1.opaqueNetwork.id = "<논리적 스위치의 ID>"
- ethernet1.opaqueNetwork.type = "nsx.LogicalSwitch"
- ethernet1.externalId = "<VM의 externalId>"
- ethernet1.connected = "TRUE"
- ethernet1.startConnected = "TRUE"

예 :

## 이전

```
ethernet1.pciSlotNumber = "224"
ethernet1.virtualDev = "vmxnet3"
ethernet1.networkName = "VM Network"
ethernet1.addressType = "vpx"
```

```

ethernet1.generatedAddress = "00:50:56:86:7b:d7"
ethernet1.uptCompatibility = "true"
ethernet1.present = "TRUE"

```

#### 신규

```

ethernet1.pciSlotNumber = "224"
ethernet1.virtualDev = "vmxnet3"
ethernet1.addressType = "vpx"
ethernet1.generatedAddress = "00:50:56:86:7b:d7"
ethernet1.uptCompatibility = "true"
ethernet1.present = "TRUE"
ethernet1.opaqueNetwork.id = "22b22448-38bc-419b-bea8-b51126bec7ad"
ethernet1.opaqueNetwork.type = "nsx.LogicalSwitch"
ethernet1.externalId = "50066bae-0f8a-386b-e62e-b0b9c6013a51"
ethernet1.connected = "TRUE"
ethernet1.startConnected = "TRUE"

```

- 6 NSX Manager UI에서 논리적 스위치 포트를 추가하고 VIF 첨부에 대해 VM의 externalId를 사용합니다.
- 7 VM을 다시 등록하고 전원을 켭니다.

여기에 표시된 것처럼 VM 관리 도구 또는 ESXi CLI를 사용할 수 있습니다.

```

[user@host:~] vim-cmd /solo/register /path/to/file.vmx

For example:
[user@host:~] vim-cmd solo/registervm /vmfs/volumes/355f2049-6c704347/app-vm/app-vm.vmx
9

[user@host:~] vim-cmd /vmsvc/power.on 9
Powering on VM:

```

## 결과

NSX Manager UI의 **스위칭 > 포트**에서 VM의 externalId와 일치하는 VIF 첨부 ID를 찾은 후 관리 및 작업 상태가 [실행]/[실행]인지 확인합니다.

두 VM이 동일한 논리적 스위치에 연결되어 있고 동일한 서브넷에 IP 주소가 구성된 경우 서로 간에 ping할 수 있어야 합니다.

## 다음에 수행할 작업

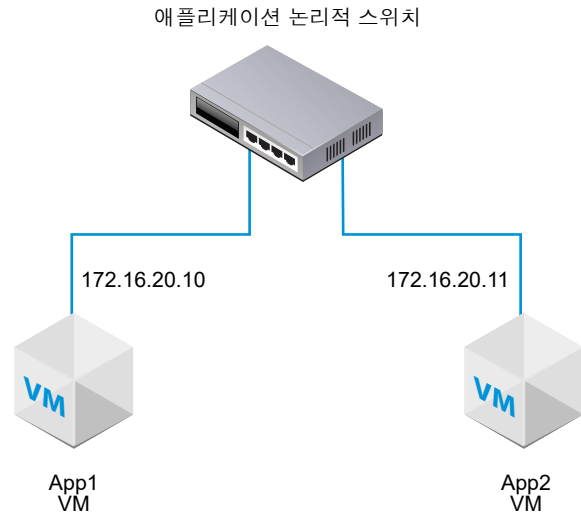
논리적 라우터를 추가합니다.

논리적 스위치 포트에서의 활동을 모니터링하여 문제를 해결할 수 있습니다. 자세한 내용은 "NSX-T Data Center 관리 가이드"의 "논리적 스위치 포트 활동 모니터링"을 참조하십시오.

## KVM에 호스팅된 VM을 NSX-T Data Center 논리적 스위치에 연결

KVM 호스트가 있는 경우 다음 절차를 사용하여 VM을 NSX-T Data Center 논리적 스위치에 연결할 수 있습니다.

이 절차에 표시된 예는 app-vm이라는 VM을 app-switch라는 논리적 스위치에 연결하는 방법을 보여줍니다.



### 사전 요구 사항

- VM은 NSX-T Data Center 패브릭에 추가된 하이퍼바이저에 호스팅되어야 합니다.
- 패브릭 노드는 NSX-T Data Center 관리부(MPA) 및 NSX-T Data Center 제어부(LCP)에 연결할 수 있어야 합니다.
- 패브릭 노드는 전송 영역에 추가되어야 합니다.
- 논리적 스위치를 생성해야 합니다.

### 절차

- 1 KVM CLI에서 `virsh dumpxml <your vm> | grep interfaceid` 명령을 실행합니다.
- 2 NSX Manager UI에서 논리적 스위치 포트를 추가하고 VIF 연결에 대해 VM의 인터페이스 ID를 사용합니다.

### 결과

NSX Manager UI의 **스위칭 > 포트**에서 VIF 연결 ID를 찾고 관리자 및 작동 상태가 둘 다 [실행]인지 확인합니다.

두 VM이 동일한 논리적 스위치에 연결되어 있고 동일한 서브넷에 IP 주소가 구성된 경우 서로 간에 ping할 수 있어야 합니다.

### 다음에 수행할 작업

논리적 라우터를 추가합니다.

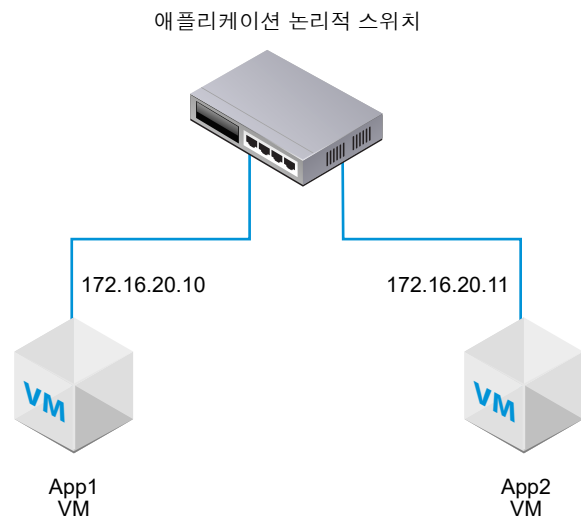
논리적 스위치 포트에서의 활동을 모니터링하여 문제를 해결할 수 있습니다. 자세한 내용은 "NSX-T Data Center 관리 가이드"의 "논리적 스위치 포트 활동 모니터링"을 참조하십시오.

## 계층 2 연결 테스트

논리적 스위치를 설정하고 VM을 논리적 스위치에 연결한 후 연결된 VM의 네트워크 연결을 테스트할 수 있습니다.

네트워크 환경이 제대로 구성된 경우 토폴로지에 따라 App2 VM이 App1 VM을 ping할 수 있습니다.

그림 1-3. 논리적 스위치 토폴로지



### 절차

- 1 SSH 또는 VM 콘솔을 사용하여 논리적 스위치에 연결된 VM 중 하나에 로그인합니다.

예: App2 VM 172.16.20.11

- 2 논리적 스위치에 연결된 두 번째 VM에 ping을 수행하여 연결을 테스트합니다.

```

$ ping -c 2 172.16.20.10
PING 172.16.20.10 (172.16.20.10) 56(84) bytes of data.
64 bytes from 172.16.20.10: icmp_seq=1 ttl=63 time=0.982 ms
64 bytes from 172.16.20.10: icmp_seq=2 ttl=63 time=0.654 ms
64 bytes from 172.16.20.10: icmp_seq=3 ttl=63 time=0.791 ms

--- 172.16.20.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1990ms
rtt min/avg/max/mdev = 0.654/0.809/0.902/0.104 ms
  
```

- 3 (선택 사항) ping 실패를 야기하는 문제를 식별합니다.
  - a VM 네트워크 설정이 올바른지 확인합니다.
  - b VM 네트워크 어댑터가 올바른 논리적 스위치에 연결되어 있는지 확인합니다.
  - c 논리적 스위치 관리 상태가 [작동]인지 확인합니다.

- d NSX Manager에서 **스위칭 > 스위치**를 선택합니다.

- e 논리적 스위치를 클릭하고 UUID 및 VNI 정보를 적어 둡니다.
- f NSX Controller에서 다음 명령을 실행하여 문제를 해결합니다.

명령	설명
<b>get logical-switch &lt;VNI 또는 UUID&gt; arp-table</b>	지정된 논리적 스위치에 대한 ARP 테이블을 표시합니다. 샘플 출력 <div> <pre>nsx-controller1&gt; get logical-switch 41866 arp-table VNI      IP          MAC          Connection-ID 41866 172.16.20.11 00:50:56:b1:70:5e 295422</pre> </div>
<b>get logical-switch &lt;VNI 또는 UUID&gt; connection-table</b>	지정된 논리적 스위치에 대한 연결을 표시합니다. 샘플 출력 <div> <pre>nsx-controller1&gt; get logical-switch 41866 connection-table Host-IP      Port  ID 192.168.110.37 36923 295420 192.168.210.53 37883 295421 192.168.210.54 57278 295422</pre> </div>
<b>get logical-switch &lt;VNI 또는 UUID&gt; mac-table</b>	지정된 논리적 스위치에 대한 MAC 테이블을 표시합니다. 샘플 출력 <div> <pre>nsx-controller1&gt; get logical-switch 41866 mac-table VNI      MAC          VTEP-IP      Connection-ID 41866 00:50:56:86:f2:b2 192.168.250.102 295421 41866 00:50:56:b1:70:5e 192.168.250.101 295422</pre> </div>
<b>get logical-switch &lt;VNI 또는 UUID&gt; stats</b>	지정된 논리적 스위치에 대한 통계 정보를 표시합니다. 샘플 출력 <div> <pre>nsx-controller1&gt; get logical-switch 41866 stats update.member 11 update.vtep 11 update.mac 4 update.mac.invalidate 0 update.arp 7 update.arp.duplicate 0 query.mac 2 query.mac.miss 0 query.arp 9 query.arp.miss 6</pre> </div>
<b>get logical-switch &lt;VNI 또는 UUID&gt; stats-sample</b>	시간에 따른 모든 논리적 스위치 통계의 요약을 표시합니다. 샘플 출력 <div> <pre>nsx-controller1&gt; get logical-switch 41866 stats-sample 21:00:00 21:10:00 21:20:00 21:30:00 21:40:00 update.member 0 0 0 0 0 update.vtep 0 0 0 0 0 update.mac 0 0 0 0 0 update.mac.invalidate 0 0 0 0 0 update.arp 0 0 0 0 0 update.arp.duplicate 0 0 0 0 0</pre> </div>

명령	설명
	<pre>query.mac 0 0 0 0 0 query.mac.miss 0 0 0 0 0 query.arp 0 0 0 0 0 query.arp.miss 0 0 0 0 0</pre>
<b>get logical-switch &lt;VNI 또는 UUID&gt; vtep</b>	<p>지정된 논리적 스위치와 관련된 모든 가상 터널 끝점을 표시합니다. 샘플 출력</p> <pre>nsx-controller1&gt; get logical-switch 41866 vtep VNI      IP          LABEL      Segment      MAC Connection-ID 41866 192.168.250.102 0x8801 192.168.250.0 00:50:56:65:f5:fc 295421 41866 192.168.250.100 0x1F801 192.168.250.0 02:50:56:00:00:00 295420 41866 192.168.250.101 0x16001 192.168.250.0 00:50:56:64:7c:28 295422</pre>

## 결과

논리적 스위치에 연결된 첫 번째 VM은 두 번째 VM으로 패킷을 전송할 수 있습니다.

# 논리적 스위치 포트

## 2

논리적 스위치에는 여러 스위치 포트가 있습니다. 라우터, VM 또는 컨테이너 같은 엔티티는 논리적 스위치 포트를 통해 논리적 스위치에 연결할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 논리적 스위치 포트 생성
- 논리적 스위치 포트 활동 모니터링

## 논리적 스위치 포트 생성

논리적 스위치 포트를 사용하면 다른 네트워크 구성 요소, VM 또는 컨테이너를 논리적 스위치에 연결할 수 있습니다.

VM을 논리적 스위치에 연결하는 방법에 대한 자세한 내용은 [VM을 논리적 스위치에 연결](#)을 참조하십시오. 컨테이너를 논리적 스위치에 연결하는 방법에 대한 자세한 내용은 "Kubernetes용 NSX-T Container Plug-in - 설치 및 관리 가이드"를 참조하십시오.

---

**참고** 컨테이너의 논리적 스위치 포트에 바인딩되는 IP 주소와 MAC 주소는 NSX Manager가 할당합니다. 주소 바인딩을 수동으로 변경하지 마십시오.

---

### 사전 요구 사항

논리적 스위치 포트가 생성되어 있는지 확인합니다. [장 1 논리적 스위치 및 VM 연결 구성](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 스위칭**을 선택합니다.
- 3 **포트** 탭을 클릭합니다.
- 4 **추가**를 클릭합니다.



## 5 일반 탭에서 포트 세부 정보를 완료합니다.

옵션	설명
이름 및 설명	이름과 설명(선택 사항)을 입력합니다.
논리적 스위치	드롭다운 목록에서 논리적 스위치를 선택합니다.
관리 상태	실행 또는 종료를 선택합니다.
연결 유형	없음 또는 VIF를 선택합니다.
연결 ID	연결 유형이 VIF이면 연결 ID를 입력합니다.

## 6 (선택 사항) 스위칭 프로파일 탭에서 스위칭 프로파일을 선택합니다.

## 7 저장을 클릭합니다.

# 논리적 스위치 포트 활동 모니터링

네트워크 정체 및 패킷 삭제 문제를 해결하려는 경우 등에 논리적 포트 활동을 모니터링할 수 있습니다.

## 사전 요구 사항

논리적 스위치 포트가 구성되어 있는지 확인합니다. [VM을 논리적 스위치에 연결](#)의 내용을 참조하십시오.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
  - 2 탐색 패널에서 **네트워킹 > 스위칭**을 선택합니다.
  - 3 **포트** 탭을 클릭합니다.
  - 4 포트의 이름을 클릭합니다.
  - 5 **모니터** 탭을 클릭합니다.
- 포트 상태 및 통계가 표시됩니다.
- 6 호스트에서 학습한 MAC 주소의 CSV 파일을 다운로드하려면 **MAC 테이블 다운로드**를 클릭합니다.
  - 7 포트의 작업을 모니터링하려면 **추적 시작**을 클릭합니다.

포트 추적 페이지가 열립니다. 양방향 포트 트래픽을 보고 삭제된 패킷을 식별할 수 있습니다. 포트 추적기 페이지에는 논리적 스위치 포트에 연결된 스위칭 프로파일도 나열됩니다.

## 결과

네트워크 정체로 인해 삭제된 패킷이 있는 경우 기본 패킷의 데이터 손실을 방지하도록 논리적 스위치 포트에 대한 QoS 스위칭 프로파일을 구성할 수 있습니다. [QoS 스위칭 프로파일 이해](#)의 내용을 참조하십시오.

# 논리적 스위치 및 논리적 포트에 대한 스위칭 프로파일

## 3

스위칭 프로파일에는 논리적 스위치 및 논리적 포트에 대한 계층 2 네트워킹 구성 세부 정보가 포함됩니다. NSX Manager는 몇 가지 유형의 스위칭 프로파일을 지원하고, 각 프로파일 유형에 대해 하나 이상의 시스템 정의 기본 스위칭 프로파일을 유지 관리합니다.

다음 유형의 스위칭 프로파일을 사용할 수 있습니다.

- QoS(서비스 품질)
- IP 검색
- SpoofGuard
- 스위치 보안
- MAC 관리

---

**참고** NSX Manager에서 기본 스위칭 프로파일은 편집하거나 삭제할 수 없습니다. 대신 사용자 지정 스위칭 프로파일을 생성할 수 있습니다.

---

각 기본 또는 사용자 지정 스위칭 프로파일에는 예약된 고유 식별자가 있습니다. 이 식별자를 사용하여 스위칭 프로파일을 논리적 스위치 또는 논리적 포트에 연결합니다. 예를 들어 기본 QoS 스위칭 프로파일 ID는 f313290b-eba8-4262-bd93-fab5026e9495입니다.

논리적 스위치 또는 논리적 포트를 각 유형의 스위칭 프로파일 하나에 연결할 수 있습니다. 예를 들어 2개의 다른 QoS 스위칭 프로파일을 하나의 논리적 스위치나 논리적 포트에 연결할 수 없습니다.

논리적 스위치를 생성하거나 업데이트하는 동안 스위칭 프로파일 유형을 연결하지 않으면 NSX Manager는 해당 기본 시스템 정의 스위칭 프로파일을 연결합니다. 하위 논리적 포트는 상위 논리적 스위치에서 기본 시스템 정의 스위칭 프로파일을 상속합니다.

논리적 스위치나 논리적 포트를 생성 또는 업데이트할 때 기본 또는 사용자 지정 스위칭 프로파일을 연결하도록 선택할 수 있습니다. 스위칭 프로파일이 논리적 스위치에 연결되거나 연결이 해제될 때 하위 논리적 포트에 대한 스위칭 프로파일이 다음 조건에 따라 적용됩니다.

- 상위 논리적 스위치에 연결된 프로파일이 있으면 하위 논리적 포트가 상위에서 스위칭 프로파일을 상속합니다.
- 상위 논리적 스위치에 연결된 스위칭 프로파일이 없으면 기본 스위칭 프로파일이 논리적 스위치에 할당되고 논리적 포트는 해당 기본 스위칭 프로파일을 상속합니다.

- 사용자 지정 프로파일을 논리적 포트에 명시적으로 연결하는 경우 이 사용자 지정 프로파일이 기존 스위칭 프로파일을 재정의합니다.

**참고** 사용자 지정 스위칭 프로파일을 논리적 스위치에 연결했으나 하위 논리적 포트 중 하나에 대해 기본 스위칭 프로파일을 유지하려면 기본 스위칭 프로파일의 복사본을 만든 후 이를 특정 논리적 포트에 연결해야 합니다.

논리적 스위치 또는 논리적 포트에 연결되어 있는 사용자 지정 스위칭 프로파일은 삭제할 수 없습니다. [요약] 보기의 [할당 대상] 섹션으로 이동하고 나열된 논리적 스위치 및 논리적 포트를 클릭하여 논리적 스위치 및 논리적 포트가 사용자 지정 스위칭 프로파일에 연결되어 있는지 확인할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- QoS 스위칭 프로파일 이해
- IP 검색 스위칭 프로파일 이해
- SpoofGuard 이해
- 스위치 보안 스위칭 프로파일 이해
- MAC 관리 스위칭 프로파일 이해
- 사용자 지정 프로파일을 논리적 스위치에 연결
- 사용자 지정 프로파일을 논리적 포트에 연결

## QoS 스위칭 프로파일 이해

QoS는 높은 대역폭을 요구하는 기본 트래픽에 고품질 및 전용 네트워크 성능을 제공합니다. QoS 메커니즘은 네트워크 정체가 발생하더라도 충분한 대역폭에 우선 순위를 지정하고, 지연 시간 및 지터를 제어하고, 기본 패킷의 데이터 손실을 줄임으로써 이러한 효과를 구현합니다. 이러한 네트워크 서비스 수준은 기존 네트워크 리소스를 효율적으로 사용하여 제공됩니다.

이 릴리스의 경우 조절 및 트래픽 표시, 즉 CoS 및 DSCP가 지원됩니다. 계층 2 CoS(서비스 클래스)를 사용하여 트래픽이 정체로 인해 논리적 스위치에서 버퍼링될 때 데이터 패킷의 우선 순위를 지정할 수 있습니다. 계층 3 DSCP(Differentiated Services Code Point)는 DSCP 값을 기준으로 패킷을 감지합니다. CoS는 신뢰 모드와 관계없이 데이터 패킷에 항상 적용됩니다.

NSX-T Data Center는 가상 시스템에 의해 적용된 DSCP 설정을 신뢰하거나 논리적 스위치 수준에서 DSCP 값을 수정 및 설정합니다. 각 경우 DSCP 값은 캡슐화 프레임의 외부 IP 헤더로 전파됩니다. 이를 통해 외부 물리적 네트워크는 외부 헤더의 DSCP 설정에 따라 트래픽의 우선 순위를 지정할 수 있습니다. DSCP가 신뢰 모드인 경우 DSCP 값이 내부 헤더에서 복사됩니다. 신뢰할 수 없는 모드에서는 내부 헤더에 대해 DSCP 값이 보존되지 않습니다.

**참고** DSCP 설정은 터널링된 트래픽에서만 작동합니다. 이러한 설정은 동일한 하이퍼바이저 내의 트래픽에는 적용되지 않습니다.

QoS 스위칭 프로파일을 사용하여 전송 제한 속도를 설정하기 위한 평균 수신 및 송신 대역폭 값을 구성할 수 있습니다. 버스트 트래픽을 지원하기 위해 최대 대역폭 속도를 사용하면 논리적 스위치가 노스바운드 네트워크 링크의 정체를 방지하도록 허용됩니다. 이러한 설정은 대역폭을 보장하지는 않지만 네트워크 대역폭의 사용을 제한하는 데 도움이 됩니다. 관찰되는 실제 대역폭은 포트의 연결 속도 또는 스위칭 프로파일의 값 중 더 낮은 값에 따라 결정됩니다.

QoS 스위칭 프로파일 설정은 논리적 스위치에 적용되고, 하위 논리적 스위치 포트에 상속됩니다.

## 사용자 지정 QoS 스위칭 프로파일 구성

DSCP 값을 정의하고 수신 및 송신 설정을 구성하여 사용자 지정 QoS 스위칭 프로파일을 생성할 수 있습니다.

### 사전 요구 사항

- QoS 스위칭 프로파일 개념을 숙지합니다. [QoS 스위칭 프로파일 이해](#)의 내용을 참조하십시오.
- 우선 순위를 지정하려는 네트워크 트래픽을 식별합니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 스위칭**을 선택합니다.
- 3 **스위칭 프로파일** 탭을 클릭합니다.
- 4 **추가**를 클릭하고 **QoS**를 선택합니다.
- 5 QoS 스위칭 프로파일 세부 정보 입력을 완료합니다.

옵션	설명
<b>이름 및 설명</b>	사용자 지정 QoS 스위칭 프로파일에 이름을 할당합니다. 필요한 경우 프로파일에서 수정한 설정에 대한 설명을 입력할 수 있습니다.
<b>모드</b>	<p>[모드] 드롭다운 메뉴에서 <b>신뢰함</b> 또는 <b>신뢰하지 않음</b> 옵션을 선택합니다.</p> <p>[신뢰함] 모드를 선택하면 내부 헤더 DSCP 값이 IP/IPv6 트래픽에 대한 외부 IP 헤더에 적용됩니다. IP/IPv6 이외 트래픽의 경우 외부 IP 헤더에 기본값이 적용됩니다. [신뢰함] 모드는 오버레이 기반 논리적 포트에서 지원됩니다. 기본값은 0입니다.</p> <p>[신뢰하지 않음] 모드는 오버레이 기반 및 VLAN 기반 논리적 포트에서 지원됩니다. 오버레이 기반 논리적 포트의 경우 아웃바운드 IP 헤더의 DSCP 값이 논리적 포트에 대한 내부 패킷 유형과 관계없는 구성된 값으로 설정됩니다. VLAN 기반 논리적 포트의 경우 IP/IPv6 패킷의 DSCP 값이 구성된 값으로 설정됩니다. [신뢰하지 않음] 모드에 대한 DSCP 값 범위는 0~63입니다.</p> <p><b>참고</b> DSCP 설정은 터널링된 트래픽에서만 작동합니다. 이러한 설정은 동일한 하이퍼바이저 내의 트래픽에는 적용되지 않습니다.</p>
<b>우선 순위</b>	<p>CoS 우선 순위 값을 설정합니다.</p> <p>우선 순위 값의 범위는 0부터 63까지이며, 0이 우선 순위가 가장 높습니다.</p>

옵션	설명
서비스 클래스	<p>CoS 값을 설정합니다.</p> <p>CoS는 VLAN 기반 논리적 포트에서 지원됩니다. CoS는 네트워크에서 비슷한 유형의 트래픽을 그룹화하며, 각 트래픽 유형은 자체 서비스 우선 순위 수준을 갖는 하나의 클래스로 취급됩니다. 우선 순위가 낮은 트래픽은 우선 순위가 높은 트래픽에 더 나은 처리량을 제공하기 위해 느려지거나 경우에 따라 삭제됩니다. 패킷이 0인 VLAN ID에 대해서도 CoS를 구성할 수 있습니다.</p> <p>CoS 값의 범위는 0~7이며, 여기서 0은 최선의 서비스를 나타냅니다.</p>
수신	<p>VM에서 논리적 네트워크의 아웃바운드 네트워크 트래픽에 대한 사용자 지정 값을 설정합니다.</p> <p>평균 대역폭을 사용하여 네트워크 정체를 줄일 수 있습니다. 최대 대역폭 속도는 버스트 트래픽을 지원하는 데 사용되고, 버스트 기간은 버스트 크기 설정에서 설정됩니다. 대역폭은 보장할 수 없습니다. 하지만 설정을 사용하여 네트워크 대역폭을 제한할 수 있습니다. 기본값은 0이며, 수신 트래픽이 사용되지 않도록 설정됩니다.</p> <p>예를 들어 논리적 스위치에 대한 평균 대역폭을 30Mbps로 설정하면 정책에서 대역폭을 제한합니다. 20바이트 기간 동안 버스트 트래픽을 100Mbps로 제한할 수 있습니다.</p>
수신 브로드캐스트	<p>브로드캐스트를 기준으로 VM에서 논리적 네트워크의 아웃바운드 네트워크 트래픽에 대한 사용자 지정 값을 설정합니다.</p> <p>기본값은 0이며, 수신 브로드캐스트 트래픽이 사용되지 않도록 설정됩니다.</p> <p>예를 들어 논리적 스위치에 대한 평균 대역폭을 50Kbps로 설정하면 정책에서 대역폭을 제한합니다. 60바이트 기간 동안 버스트 트래픽을 400Kbps로 제한할 수 있습니다.</p>
송신	<p>논리적 네트워크에서 VM으로의 인바운드 네트워크 트래픽에 대한 사용자 지정 값을 설정합니다.</p> <p>기본값은 0이며, 송신 트래픽이 사용되지 않도록 설정됩니다.</p>

수신, 수신 브로드캐스트 및 송신 옵션이 구성되지 않으면 기본값이 프로토콜 버퍼로 사용됩니다.

## 6 저장을 클릭합니다.

### 결과

사용자 지정 QoS 스위칭 프로파일이 링크로 표시됩니다.

### 다음에 수행할 작업

스위칭 프로파일의 수정된 매개 변수가 네트워크 트래픽에 적용되도록 이 QoS 사용자 지정된 스위칭 프로파일을 논리적 스위치 또는 논리적 포트에 연결합니다. [사용자 지정 프로파일을 논리적 스위치에 연결](#) 또는 [사용자 지정 프로파일을 논리적 포트에 연결](#)의 내용을 참조하십시오.

## IP 검색 스위칭 프로파일 이해

IP 검색은 DHCP 스누핑, ARP 스누핑 또는 VM Tools를 사용하여 VM MAC 및 IP 주소를 학습합니다. MAC 및 IP 주소가 학습되면 항목이 NSX Controller와 공유되므로 ARP가 억제됩니다. ARP 억제는 동일한 논리적 스위치에 연결된 VM 내의 ARP 트래픽 플러딩을 최소화합니다.

DHCP 스누핑은 VM DHCP 클라이언트와 DHCP 서버 간에 교환되는 DHCP 패킷을 조사하여 VM IP 및 MAC 주소를 학습합니다.

ARP 스누핑은 VM의 송신 ARP 및 GARP를 조사하여 IP 및 MAC 주소를 학습합니다.

VM Tools는 ESXi 호스팅 VM에서 실행되며 VM의 구성 정보(MAC 및 IP 주소 포함)를 제공할 수 있는 소프트웨어입니다. 이 IP 검색 방법은 ESXi 호스트에서 실행되는 VM에서만 사용할 수 있습니다.

**참고** Linux VM에서는 ARP flux 문제 때문에 ARP 스누핑이 잘못된 정보를 가져올 수 있습니다. ARP 필터를 사용하면 이 문제를 방지할 수 있습니다. 자세한 내용은 <http://linux-ip.net/html/ether-arp.html#ether-arp-flux> 항목을 참조하십시오.

## IP 검색 스위칭 프로파일 구성

ARP 스누핑, DHCP 스누핑 또는 VM Tools를 사용하도록 설정하여 IP 및 MAC 주소를 학습하는 사용자 지정 IP 검색 스위칭 프로파일을 생성함으로써 논리적 스위치의 IP 무결성을 보장할 수 있습니다. VM Tools IP 검색 방법은 ESXi 호스팅 VM에서만 사용할 수 있습니다.

### 사전 요구 사항

IP 검색 스위칭 프로파일 개념을 숙지합니다. [IP 검색 스위칭 프로파일 이해](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 스위칭**을 선택합니다.
- 3 **스위칭 프로파일** 탭을 클릭합니다.
- 4 **추가**를 클릭하고 **IP 검색**을 선택합니다.
- 5 IP 검색 스위칭 프로파일 세부 정보 입력을 완료합니다.

옵션	설명
<b>이름 및 설명</b>	이름과 설명(선택 사항)을 입력합니다.
<b>ARP 스누핑</b>	<b>ARP 스누핑</b> 버튼을 전환하여 기능을 사용하도록 설정합니다. ARP 스누핑은 VM 송신 ARP 및 GARP를 조사하여 VM MAC 및 IP 주소를 학습합니다. ARP 스누핑은 VM이 DHCP 대신 정적 IP 주소를 사용하는 경우에 적용 가능합니다.
<b>ARP 바인딩 제한</b>	1~128의 ARP 바인딩 제한을 지정합니다.
<b>DHCP 스누핑</b>	<b>DHCP 스누핑</b> 버튼을 전환하여 해당 기능을 사용하도록 설정합니다. DHCP 스누핑은 VM DHCP 클라이언트와 DHCP 서버 간에 교환되는 DHCP 패킷을 조사하여 VM MAC 및 IP 주소를 학습합니다.
<b>VM Tools</b>	<b>VM Tools</b> 버튼을 전환하여 기능을 사용하도록 설정합니다. 이 옵션은 ESXi 호스팅 VM에서만 사용할 수 있습니다. VM Tools는 ESXi 호스팅 VM에서 실행되며 VM의 MAC 및 IP 주소를 제공할 수 있는 소프트웨어입니다.

- 6 **저장**을 클릭합니다.

## 결과

사용자 지정 IP 검색 스위칭 프로파일은 링크로 표시됩니다.

## 다음에 수행할 작업

스위칭 프로파일의 수정된 매개 변수가 네트워크 트래픽에 적용되도록 이 IP 검색 사용자 지정된 스위칭 프로파일을 논리적 스위치 또는 논리적 포트에 연결합니다. [사용자 지정 프로파일을 논리적 스위치에 연결](#) 또는 [사용자 지정 프로파일을 논리적 포트에 연결](#)의 내용을 참조하십시오.

# SpoofGuard 이해

SpoofGuard는 "웹 스푸핑" 또는 "피싱"이라고 하는 악의적인 공격 형태를 방지하는 데 도움이 됩니다. SpoofGuard 정책은 스푸핑으로 확인된 트래픽을 차단합니다.

SpoofGuard는 작업 환경의 가상 시스템이 트래픽을 끝낼 권한이 없는 IP 주소를 사용하여 트래픽을 전송하지 못하게 하도록 설계된 도구입니다. 가상 시스템의 IP 주소가 SpoofGuard의 해당 논리적 포트 및 스위치 주소 바인딩에 있는 IP 주소와 일치하지 않을 경우 가상 시스템의 vNIC는 네트워크에 전혀 액세스하지 못합니다. SpoofGuard는 포트 또는 스위치 수준에서 구성할 수 있습니다. 작업 환경에서 SpoofGuard를 사용하는 이유에는 다음과 같은 몇 가지가 있습니다.

- 악성 가상 시스템이 기존 VM의 IP 주소를 가정하지 못하도록 방지합니다.
- 가상 시스템의 IP 주소를 개입 없이 변경할 수 없도록 합니다. 일부 환경에서는 가상 시스템이 적절한 변경 제어 검토 없이 IP 주소를 변경할 수 없도록 하는 것이 좋습니다. SpoofGuard는 가상 시스템 소유자가 IP 주소를 변경하고 방해 없이 계속 작업하지 못하도록 하여 이러한 작동을 용이하게 합니다.
- DFW(분산 방화벽) 규칙이 실수로(또는 고의로) 우회되지 않도록 보장합니다. IP 집합을 소스 또는 대상으로 활용하여 생성한 DFW 규칙의 경우 가상 시스템이 패킷 헤더에서 IP 주소를 위조하여 문제의 규칙을 우회할 가능성이 항상 존재합니다.

NSX-T Data Center SpoofGuard 구성에는 다음이 포함됩니다.

- MAC SpoofGuard - 패킷의 MAC 주소를 인증합니다.
- IP SpoofGuard - 패킷의 MAC 및 IP 주소를 인증합니다.
- 동적 ARP(Address Resolution Protocol) 검사 즉, ARP 및 GARP(Gratuitous Address Resolution Protocol) SpoofGuard와 ND(Neighbor Discovery) SpoofGuard 유효성 검사는 모두 ARP/GARP/ND 페이로드의 MAC 소스, IP 소스 및 IP-MAC 소스 매핑에 대해 수행됩니다.

포트 수준에서 허용되는 MAC/VLAN/IP 화이트리스트는 포트의 [주소 바인딩] 속성을 통해 제공됩니다. 가상 시스템이 트래픽을 전송할 경우 해당 IP/MAC/VLAN이 포트의 IP/MAC/VLAN 속성과 일치하지 않으면 트래픽이 삭제됩니다. 포트 수준 SpoofGuard는 트래픽 인증을 처리합니다. 즉, 트래픽이 VIF 구성과 일치하는지 확인합니다.

스위치 수준에서 허용되는 MAC/VLAN/IP 화이트리스트는 스위치의 [주소 바인딩] 속성을 통해 제공됩니다. 이는 일반적으로 스위치에 대해 허용되는 IP 범위/서브넷이며, 스위치 수준 SpoofGuard는 트래픽 인증을 처리합니다.

트래픽은 스위치로 들어가도록 허용되기 전에 먼저 포트 수준 및 스위치 수준 SpoofGuard에서 허용되어야 합니다. 포트 및 스위치 수준 SpoofGuard를 사용하거나 사용하지 않도록 설정하는 작업은 SpoofGuard 스위치 프로파일을 사용하여 제어할 수 있습니다.

## 포트 주소 바인딩 구성

주소 바인딩은 논리적 포트의 IP 및 MAC 주소를 지정하고 SpoofGuard의 포트 화이트리스트를 지정하는 데 사용됩니다.

포트 주소 바인딩을 사용하여 IP 및 MAC 주소를 지정하고, 해당되는 경우 논리적 포트의 VLAN을 지정합니다. SpoofGuard를 사용하도록 설정하면 SpoofGuard가 지정된 주소 바인딩이 데이터 경로에 적용되도록 합니다. SpoofGuard 외에 포트 주소 바인딩이 DFW 규칙 변환에 사용됩니다.

### 절차

- 1 NSX Manager에서 **네트워킹 > 스위칭**으로 이동합니다.
- 2 **포트** 탭을 클릭합니다.
- 3 주소 바인딩을 적용하려는 논리적 포트를 클릭합니다.  
논리적 포트 요약이 표시됩니다.
- 4 **개요** 탭에서 **주소 바인딩**을 확장합니다.
- 5 **추가**를 클릭합니다.  
[주소 바인딩 추가] 대화상자가 표시됩니다.
- 6 주소 바인딩을 적용하려는 논리적 포트의 IP 및 MAC 주소를 지정합니다. VLAN ID를 지정할 수도 있습니다.
- 7 **추가**를 클릭합니다.

다음에 수행할 작업

[SpoofGuard 스위칭 프로파일 구성](#) 시 포트 주소 바인딩을 사용합니다.

## SpoofGuard 스위칭 프로파일 구성

SpoofGuard가 구성되면 가상 시스템의 IP 주소가 변경될 경우 구성된 해당 포트/스위치 주소 바인딩이 새 IP 주소로 업데이트될 때까지 가상 시스템의 트래픽이 차단될 수 있습니다.

게스트를 포함하는 포트 그룹에 대해 SpoofGuard를 사용하도록 설정합니다. 각 네트워크 어댑터에 대해 SpoofGuard를 사용하도록 설정하면 지정된 MAC 및 해당 IP 주소에 대한 패킷이 조사됩니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 스위칭**을 선택합니다.
- 3 **스위칭 프로파일** 탭을 클릭합니다.



- 4 **추가**를 클릭하고 **Spoof Guard**를 선택합니다.
- 5 이름과 설명(선택 사항)을 입력합니다.
- 6 포트 수준 SpoofGuard를 사용하도록 설정하려면 **포트 바인딩**을 **사용**으로 설정합니다.
- 7 **추가**를 클릭합니다.

## 결과

새 스위칭 프로파일이 SpoofGuard 프로파일을 사용하여 생성되었습니다.

## 다음에 수행할 작업

SpoofGuard 프로파일을 논리적 스위치 또는 논리적 포트에 연결합니다. [사용자 지정 프로파일을 논리적 스위치에 연결](#) 또는 [사용자 지정 프로파일을 논리적 포트에 연결](#)의 내용을 참조하십시오.

## 스위치 보안 스위칭 프로파일 이해

스위치 보안은 논리적 스위치에 대한 수신 트래픽을 확인하고 일치하는 IP 주소, MAC 주소 및 프로토콜을 찾아 VM에서 허용되는 주소 및 프로토콜 집합으로 전송되는 인증되지 않은 패킷을 삭제하여 상태 비저장 계층 2 및 계층 3 보안을 제공합니다. 스위치 보안을 사용하여 네트워크의 VM에서 발생하는 악의적인 공격을 필터링하여 논리적 스위치 무결성을 보호할 수 있습니다.

BPDU(Bridge Protocol Data Unit) 필터, DHCP 스누핑, DHCP 서버 차단 및 속도 제한 옵션을 구성하여 논리적 스위치의 스위치 보안 스위칭 프로파일을 사용자 지정할 수 있습니다.

## 사용자 지정 스위치 보안 스위칭 프로파일 구성

허용되는 BPDU 목록의 MAC 대상 주소로 사용자 지정 스위치 보안 스위칭 프로파일을 생성하고 속도 제한을 구성할 수 있습니다.

## 사전 요구 사항

스위치 보안 스위칭 프로파일 개념을 숙지합니다. [스위치 보안 스위칭 프로파일 이해](#)의 내용을 참조하십시오.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 스위칭**을 선택합니다.
- 3 **스위칭 프로파일** 탭을 클릭합니다.
- 4 **추가**를 클릭하고 **스위치 보안**을 선택합니다.

## 5 스위치 보안 프로파일 세부 정보 입력을 완료합니다.

옵션	설명
이름 및 설명	사용자 지정 스위치 보안 프로파일에 이름을 할당합니다. 필요한 경우 프로파일에서 수정한 설정에 대한 설명을 입력할 수 있습니다.
BPDU 필터	<b>BPDU 필터</b> 버튼을 전환하여 BPDU 필터링을 사용하도록 설정합니다. BPDU 필터가 사용되도록 설정되면 BPDU 대상 MAC 주소로의 모든 트래픽이 차단됩니다. 또한 BPDU 필터가 사용되도록 설정되면 논리적 스위치 포트는 STP에 참여할 것으로 예상되지 않으므로 이러한 포트에서 STP가 사용되지 않도록 설정됩니다.
BPDU 필터 허용 목록	BPDU 대상 MAC 주소 목록에서 대상 MAC 주소를 클릭하여 허용되는 대상으로의 트래픽을 허용합니다.
DHCP 필터	<b>서버 차단</b> 버튼 및 <b>클라이언트 차단</b> 버튼을 전환하여 DHCP 필터링을 사용하도록 설정합니다. DHCP 서버 차단은 DHCP 서버에서 DHCP 클라이언트로의 트래픽을 차단합니다. DHCP 서버에서 DHCP 릴레이 에이전트로의 트래픽은 차단하지 않습니다. DHCP 클라이언트 차단은 DHCP 요청을 차단하여 VM이 DHCP IP 주소를 획득하지 못하게 합니다.
비 IP 트래픽 차단	<b>비 IP 트래픽 차단</b> 버튼을 전환하여 IPv4, IPv6, ARP, GARP 및 BPDU 트래픽만 허용합니다. 나머지 비 IP 트래픽은 차단됩니다. 허용되는 IPv4, IPv6, ARP, GARP 및 BPDU 트래픽은 주소 바인딩 및 SpoofGuard 구성에 설정된 다른 정책을 기준으로 합니다. 기본적으로 이 옵션은 비 IP 트래픽이 일반 트래픽으로 처리되도록 허용하기 위해 사용되지 않도록 설정됩니다.
속도 제한	수신 또는 송신 브로드캐스트 및 멀티캐스트 트래픽에 대한 속도 제한을 설정합니다. 논리적 스위치 또는 VM을 브로드캐스트 트래픽 스톰 등으로부터 보호하도록 속도 제한을 구성합니다. 연결 문제를 방지하려면 최소 속도 제한 값을 10pps 이상으로 설정해야 합니다.

## 6 추가를 클릭합니다.

### 결과

사용자 지정 스위치 보안 프로파일이 링크로 표시됩니다.

### 다음에 수행할 작업

스위칭 프로파일의 수정된 매개 변수가 네트워크 트래픽에 적용되도록 이 스위치 보안 사용자 지정된 스위칭 프로파일을 논리적 스위치 또는 논리적 포트에 연결합니다. [사용자 지정 프로파일을 논리적 스위치에 연결](#) 또는 [사용자 지정 프로파일을 논리적 포트에 연결](#)의 내용을 참조하십시오.

## MAC 관리 스위칭 프로파일 이해

MAC 관리 스위칭 프로파일은 MAC 학습 및 MAC 주소 변경의 두 가지 기능을 지원합니다.

MAC 주소 변경 기능을 사용하면 VM에서 MAC 주소를 변경할 수 있습니다. 포트에 연결된 VM은 관리 명령을 실행하여 vNIC의 MAC 주소를 변경하고, 해당 vNIC에서 계속 트래픽을 송수신할 수 있습니다. 이 기능은 ESXi에서만 지원되고 KVM에서는 지원되지 않습니다. 이 속성은 기본적으로 사용되지 않도록 설정되어 있습니다.

MAC 학습은 여러 MAC 주소가 단일 vNIC 뒤에서 구성되는 배포에 대해 네트워크 연결을 제공합니다 (예: ESXi VM이 ESXi 호스트에서 실행되고 여러 VM이 ESXi VM 내에서 실행되는 중첩된 하이퍼바이저 배포의 경우). MAC 학습을 사용하지 않을 경우 ESXi VM의 vNIC가 스위치 포트에 연결되면 해당 MAC 주소는 정적입니다. ESXi VM 내에서 실행되는 VM은 해당 패킷이 다른 소스 MAC 주소를 가지므로 네트워크 연결이 없습니다. MAC 학습을 사용할 경우 vSwitch는 vNIC에서 들어오는 모든 패킷의 소스 MAC 주소를 조사하고, MAC 주소를 학습하고, 패킷이 통과되도록 합니다. 학습된 MAC 주소는 특정 기간 동안 사용되지 않으면 제거됩니다. 이러한 에이징 속성은 구성할 수 없습니다.

MAC 학습 또는 MAC 주소 변경을 사용하도록 설정하는 경우 보안을 향상하려면 SpoofGuard도 구성합니다.

## MAC 관리 스위칭 프로파일 구성

MAC 관리 스위칭 프로파일을 생성하여 MAC 주소를 관리할 수 있습니다.

### 사전 요구 사항

MAC 관리 스위칭 프로파일 개념을 숙지합니다. [MAC 관리 스위칭 프로파일 이해](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 스위칭**을 선택합니다.
- 3 **스위칭 프로파일** 탭을 클릭합니다.
- 4 **추가**를 클릭하고 **MAC 관리**를 선택합니다.
- 5 MAC 관리 프로파일 세부 사항을 완료합니다.

옵션	설명
이름 및 설명	MAC 관리 프로파일에 이름을 할당합니다. 필요한 경우 프로파일에서 수정한 설정에 대한 설명을 입력할 수 있습니다.
MAC 변경	MAC 주소 변경 기능을 사용하거나 사용하지 않도록 설정합니다.
상태	MAC 학습 기능을 사용하거나 사용하지 않도록 설정합니다.

- 6 **추가**를 클릭합니다.

### 결과

MAC 관리 프로파일이 링크로 표시됩니다.

다음에 수행할 작업

스위칭 프로파일을 논리적 스위치 또는 논리적 포트에 연결합니다. [사용자 지정 프로파일을 논리적 스위치에 연결](#) 또는 [사용자 지정 프로파일을 논리적 포트에 연결](#)의 내용을 참조하십시오.

## 사용자 지정 프로파일을 논리적 스위치에 연결

프로파일이 스위치의 모든 포트에 적용되도록 사용자 지정 스위칭 프로파일을 논리적 스위치에 연결할 수 있습니다.

사용자 지정 스위칭 프로파일이 논리적 스위치에 연결되면 기존의 기본 스위칭 프로파일을 재정의합니다. 사용자 지정 스위칭 프로파일은 하위 논리적 스위치 포트에서 상속됩니다.

---

**참고** 사용자 지정 스위칭 프로파일을 논리적 스위치에 연결했으나 하위 논리적 스위치 포트 중 하나에 대해 기본 스위칭 프로파일을 유지하려면 기본 스위칭 프로파일의 복사본을 만든 후 특정 논리적 스위치 포트에 연결해야 합니다.

---

### 사전 요구 사항

- 논리적 스위치가 구성되어 있는지 확인합니다. [논리적 스위치 생성](#)의 내용을 참조하십시오.
- 사용자 지정 스위칭 프로파일이 구성되어 있는지 확인합니다. [장 3 논리적 스위치 및 논리적 포트에 대한 스위칭 프로파일](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 스위칭**을 선택합니다.
- 3 **스위치** 탭을 클릭합니다.
- 4 사용자 지정 스위칭 프로파일을 적용할 논리적 스위치를 클릭합니다.
- 5 **관리** 탭을 클릭합니다.
- 6 드롭다운 메뉴에서 사용자 지정 스위칭 프로파일 유형을 선택합니다.
  - QoS
  - 포트 미러링
  - IP 검색
  - SpoofGuard
  - 스위치 보안
  - MAC 관리
- 7 **변경**을 클릭합니다.
- 8 드롭다운 메뉴에서 이전에 생성한 사용자 지정 스위칭 프로파일을 선택합니다.

## 9 저장을 클릭합니다.

이제 논리적 스위치가 사용자 지정 스위칭 프로파일에 연결됩니다.

## 10 관리 탭 아래에 구성이 수정된 새로운 사용자 지정 스위칭 프로파일이 나타나는지 확인합니다.

## 11 (선택 사항) 관련 탭을 클릭하고 드롭다운 메뉴에서 **포트**를 선택하여 사용자 지정 스위칭 프로파일 이 하위 논리적 포트에 적용되었는지 확인합니다.

### 다음에 수행할 작업

논리적 스위치에서 상속된 스위칭 프로파일을 사용하지 않으려면 사용자 지정 스위칭 프로파일을 하위 논리적 스위치 포트에 적용할 수 있습니다. [사용자 지정 프로파일을 논리적 포트에 연결](#)의 내용을 참조하십시오.

## 사용자 지정 프로파일을 논리적 포트에 연결

논리적 포트는 VIF에 대한 논리적 연결 지점, 라우터에 대한 패치 연결 또는 외부 네트워크에 대한 계층 2 게이트웨이 연결을 제공합니다. 또한 논리적 포트는 스위칭 프로파일, 포트 통계 카운터 및 논리적 링크 상태를 표시합니다.

상속된 스위칭 프로파일을 논리적 스위치에서 하위 논리적 포트에 대한 다른 사용자 지정 스위칭 프로파일로 변경할 수 있습니다.

### 사전 요구 사항

- 논리적 포트가 구성되어 있는지 확인합니다. [VM을 논리적 스위치에 연결](#)의 내용을 참조하십시오.
- 사용자 지정 스위칭 프로파일이 구성되어 있는지 확인합니다. [장 3 논리적 스위치 및 논리적 포트에 대한 스위칭 프로파일](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 스위칭**을 선택합니다.
- 3 **포트** 탭을 클릭합니다.
- 4 사용자 지정 스위칭 프로파일을 적용할 논리적 포트를 클릭합니다.
- 5 **관리** 탭을 클릭합니다.
- 6 드롭다운 메뉴에서 사용자 지정 스위칭 프로파일 유형을 선택합니다.
  - QoS
  - 포트 미러링
  - IP 검색
  - SpoofGuard
  - 스위치 보안

## ■ MAC 관리

**7 변경**을 클릭합니다.

**8** 드롭다운 메뉴에서 이전에 생성한 사용자 지정 스위칭 프로파일을 선택합니다.

**9 저장**을 클릭합니다.

이제 논리적 포트가 사용자 지정 스위칭 프로파일에 연결됩니다.

**10 관리** 탭 아래에 구성이 수정된 새로운 사용자 지정 스위칭 프로파일이 나타나는지 확인합니다.

다음에 수행할 작업

논리적 스위치 포트에서의 활동을 모니터링하여 문제를 해결할 수 있습니다. 자세한 내용은 "NSX-T Data Center 관리 가이드"의 "논리적 스위치 포트 활동 모니터링"을 참조하십시오.

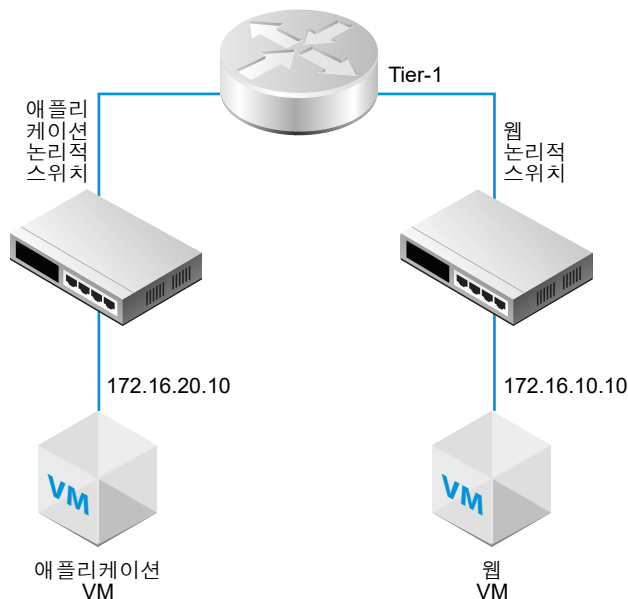
# Tier-1 논리적 라우터

# 4

NSX-T Data Center 논리적 라우터는 기본 하드웨어에서 완전히 분리된 가상 환경에서 라우팅 기능을 재현합니다. Tier-1 논리적 라우터에는 NSX-T Data Center 논리적 스위치에 연결하기 위한 다운링크 포트와 NSX-T Data Center Tier-0 논리적 라우터에 연결하기 위한 업링크 포트가 있습니다.

논리적 라우터를 추가하는 경우 구축하려는 네트워킹 토폴로지를 계획하는 것이 중요합니다.

그림 4-1. Tier-1 논리적 라우터 토폴로지



예를 들어 이 간단한 토폴로지는 Tier-1 논리적 라우터에 연결된 2개의 논리적 스위치를 보여줍니다. 각 논리적 스위치에는 단일 VM이 연결되어 있습니다. 두 개의 VM은 다른 호스트 또는 동일한 호스트에 있거나 다른 호스트 클러스터 또는 동일한 호스트 클러스터에 있을 수 있습니다. 논리적 라우터가 VM을 분리하지 않을 경우 VM에 구성된 기본 IP 주소는 같은 서브넷에 있는 것입니다. 논리적 라우터가 VM을 분리하는 경우 VM의 IP 주소가 다른 서브넷에 있는 것입니다.

본 장은 다음 항목을 포함합니다.

- Tier-1 논리적 라우터 생성
- Tier-1 논리적 라우터에서 다운링크 포트 추가

- Tier-0 또는 Tier-1 논리적 라우터에 VLAN 포트 추가
- Tier-1 논리적 라우터에서 경로 보급 구성
- Tier-1 논리적 라우터 정적 경로 구성
- 독립형 Tier-1 논리적 라우터 생성

## Tier-1 논리적 라우터 생성

노스바운드 물리적 라우터 액세스 권한을 얻으려면 Tier-1 논리적 라우터를 Tier-0 논리적 라우터에 연결해야 합니다.

### 사전 요구 사항

- 논리적 스위치가 구성되어 있는지 확인합니다. [논리적 스위치 생성](#)의 내용을 참조하십시오.
- NAT(네트워크 주소 변환) 구성을 수행하려면 NSX Edge 클러스터가 배포되었는지 확인합니다. "NSX-T Data Center 설치 가이드"의 내용을 참조하십시오.
- Tier-1 논리적 라우터 토폴로지를 숙지합니다. [장 4 Tier-1 논리적 라우터](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 **추가**를 클릭하고 **Tier-1 라우터**를 선택합니다.
- 4 논리적 라우터 이름 및 필요한 경우 설명을 입력합니다.
- 5 (선택 사항) 이 Tier-1 논리적 라우터에 연결할 Tier-0 논리적 라우터를 선택합니다.  
아직 구성된 Tier-0 논리적 라우터가 없으면 지금은 이 필드를 비워 두고 나중에 라우터 구성을 편집하면 됩니다.
- 6 (선택 사항) 이 Tier-1 논리적 라우터에 연결할 NSX Edge 클러스터를 선택합니다.  
Tier-1 논리적 라우터를 NAT 구성에 사용하려는 경우 이를 NSX Edge 클러스터에 연결해야 합니다. 아직 구성된 NSX Edge 클러스터가 없으면 지금은 이 필드를 비워 두고 나중에 라우터 구성을 편집하면 됩니다.
- 7 (선택 사항) NSX Edge 클러스터를 선택한 경우 페일오버 모드를 선택합니다.

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

- 8 (선택 사항) **고급** 탭을 클릭하고 **Tier-1 내부 전송 서브넷**에 대한 값을 입력합니다.



## 9 추가를 클릭합니다.

NSX Manager UI에서 새 논리적 라우터는 클릭 가능한 링크입니다.

### 결과

이 논리적 라우터가 5000개가 넘는 VM을 지원하는 경우 NSX Edge 클러스터의 각 노드에서 다음 명령을 실행하여 ARP 테이블의 크기를 늘려야 합니다.

```
set debug-mode
set dataplane neighbor max-arp-logical-router 10000
```

변경 사항은 지속적이지 않으므로 데이터부가 다시 시작되거나 노드가 재부팅된 후에는 명령을 다시 실행해야 합니다.

### 다음에 수행할 작업

Tier-1 논리적 라우터에 대한 다운링크 포트를 생성합니다. [Tier-1 논리적 라우터에서 다운링크 포트 추가](#)의 내용을 참조하십시오.

## Tier-1 논리적 라우터에서 다운링크 포트 추가

Tier-1 논리적 라우터에 다운링크 포트를 생성하면 포트는 같은 서브넷에 있는 VM의 기본 게이트웨이로 사용됩니다.

### 사전 요구 사항

Tier-1 논리적 라우터가 구성되어 있는지 확인합니다. [Tier-1 논리적 라우터 생성](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 라우터의 이름을 클릭합니다.
- 4 **구성** 탭을 클릭하고 **라우터 포트**를 선택합니다.
- 5 **추가**를 클릭합니다.
- 6 라우터 포트 이름 및 필요한 경우 설명을 입력합니다.
- 7 **유형** 필드에서 **다운링크**를 선택합니다.
- 8 **URPF 모드**의 경우 **엄격** 또는 **없음**을 선택합니다.  
URPF(유니캐스트 역방향 경로 전달)는 보안 기능입니다.
- 9 (선택 사항) 논리적 스위치를 선택합니다.

**10** 이 연결이 스위치 포트를 생성할지 또는 기존 스위치 포트를 업데이트할지 선택합니다.

기존 스위치 포트를 사용하여 연결하는 경우, 드롭다운 메뉴에서 포트를 선택합니다.

**11** CIDR 표기법으로 라우터 포트 IP 주소를 입력합니다.

예를 들어 IP 주소는 172.16.10.1/24가 될 수 있습니다.

**12** (선택 사항) DHCP 릴레이 서비스를 선택합니다.

**13** **추가**를 클릭합니다.

다음에 수행할 작업

경로 보급을 사용하도록 설정하여 VM과 외부 물리적 네트워크 간 또는 같은 Tier-0 논리적 라우터에 연결된 서로 다른 Tier-1 논리적 라우터 간 북-남 연결을 제공합니다. [Tier-1 논리적 라우터에서 경로 보급 구성](#)의 내용을 참조하십시오.

## Tier-0 또는 Tier-1 논리적 라우터에 VLAN 포트 추가

VLAN 지원 논리적 스위치만 있는 경우 NSX-T Data Center가 계층-3 서비스를 제공할 수 있도록 Tier-0 또는 Tier-1 라우터의 VLAN 포트에 스위치를 연결할 수 있습니다.

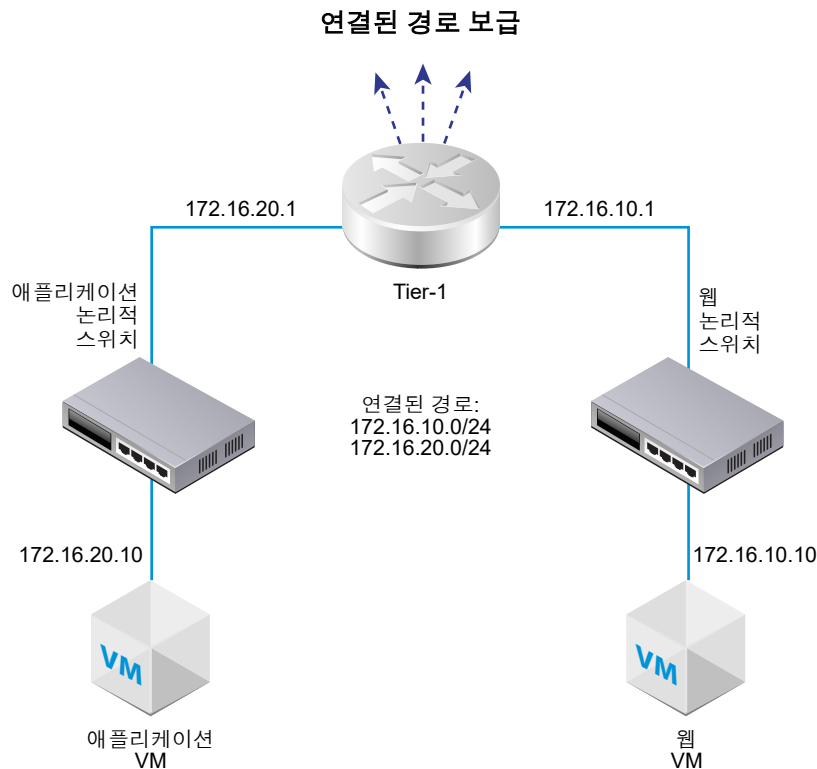
절차

- 1** 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2** 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3** 라우터의 이름을 클릭합니다.
- 4** **구성** 탭을 클릭하고 **라우터 포트**를 선택합니다.
- 5** **추가**를 클릭합니다.
- 6** 라우터 포트 이름 및 필요한 경우 설명을 입력합니다.
- 7** **유형** 필드에서 **중앙 집중식**을 선택합니다.
- 8** **URPF 모드**의 경우 **엄격** 또는 **없음**을 선택합니다.  
URPF(유니캐스트 역방향 경로 전달)는 보안 기능입니다.
- 9** (필수 사항) 논리적 스위치를 선택합니다.
- 10** 이 연결이 스위치 포트를 생성할지 또는 기존 스위치 포트를 업데이트할지 선택합니다.  
기존 스위치 포트를 사용하여 연결하는 경우, 드롭다운 메뉴에서 포트를 선택합니다.
- 11** CIDR 표기법으로 라우터 포트 IP 주소를 입력합니다.
- 12** **추가**를 클릭합니다.

## Tier-1 논리적 라우터에서 경로 보급 구성

다른 Tier-1 논리적 라우터에 연결된 논리적 스위치에 연결된 VM 간에 계층 3 연결을 제공하려면 Tier-0 쪽으로 Tier-1 경로 보급을 사용하도록 설정해야 합니다. Tier-1 및 Tier-0 논리적 라우터 간에 라우팅 프로토콜 또는 정적 경로를 구성할 필요는 없습니다. NSX-T Data Center는 경로 보급을 사용하도록 설정하면 NSX-T Data Center 정적 경로를 자동으로 생성합니다.

예를 들어 다른 피어 라우터를 통해 VM과의 연결을 제공하려면 Tier-1 논리적 라우터에 연결된 경로에 대한 경로 보급이 구성되어야 합니다. 연결된 모든 경로를 보급하려는 경우가 아니면 보급할 경로를 지정할 수 있습니다.



### 사전 요구 사항

- VM이 논리적 스위치에 연결되어 있는지 확인합니다. [장 1 논리적 스위치 및 VM 연결 구성](#)의 내용을 참조하십시오.
- Tier-1 논리적 라우터에 대한 다운링크 포트가 구성되어 있는지 확인합니다. [Tier-1 논리적 라우터에서 다운링크 포트 추가](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 Tier-1 라우터의 이름을 클릭합니다.

4 **라우팅** 드롭다운 메뉴에서 **경로 보급**을 선택합니다.

5 **편집**을 클릭하여 경로 보급 구성을 편집합니다.

다음 스위치를 전환할 수 있습니다.

- **상태**
- **모든 NSX 연결 경로 보급**
- **모든 NAT 경로 보급**
- **모든 정적 경로 보급**
- **모든 LB VIP 경로 보급**
- **모든 LB SNAT IP 경로 보급**

a **저장**을 클릭합니다.

6 **추가**를 클릭하여 경로를 보급합니다.

- a 이름과 설명(선택 사항)을 입력합니다.
- b 경로 접두사를 CIDR 형식으로 입력합니다.
- c **필터 적용**을 클릭하여 다음 옵션을 설정합니다.

<b>작업</b>	허용 또는 거부를 지정합니다.
<b>경로 유형 일치</b>	다음 중 하나 이상을 선택합니다. <ul style="list-style-type: none"> <li>■ 임의</li> <li>■ NSX 연결됨</li> <li>■ Tier-1 LB VIP</li> <li>■ 정적</li> <li>■ Tier-1 NAT</li> <li>■ Tier-1 LB SNAT</li> </ul>
<b>접두사 연산자</b>	GE 또는 EQ를 선택합니다.

d **추가**를 클릭합니다.

다음에 수행할 작업

Tier-0 논리적 라우터 토폴로지를 숙지하고 Tier-0 논리적 라우터를 생성합니다. [장 5 Tier-0 논리적 라우터](#)의 내용을 참조하십시오.

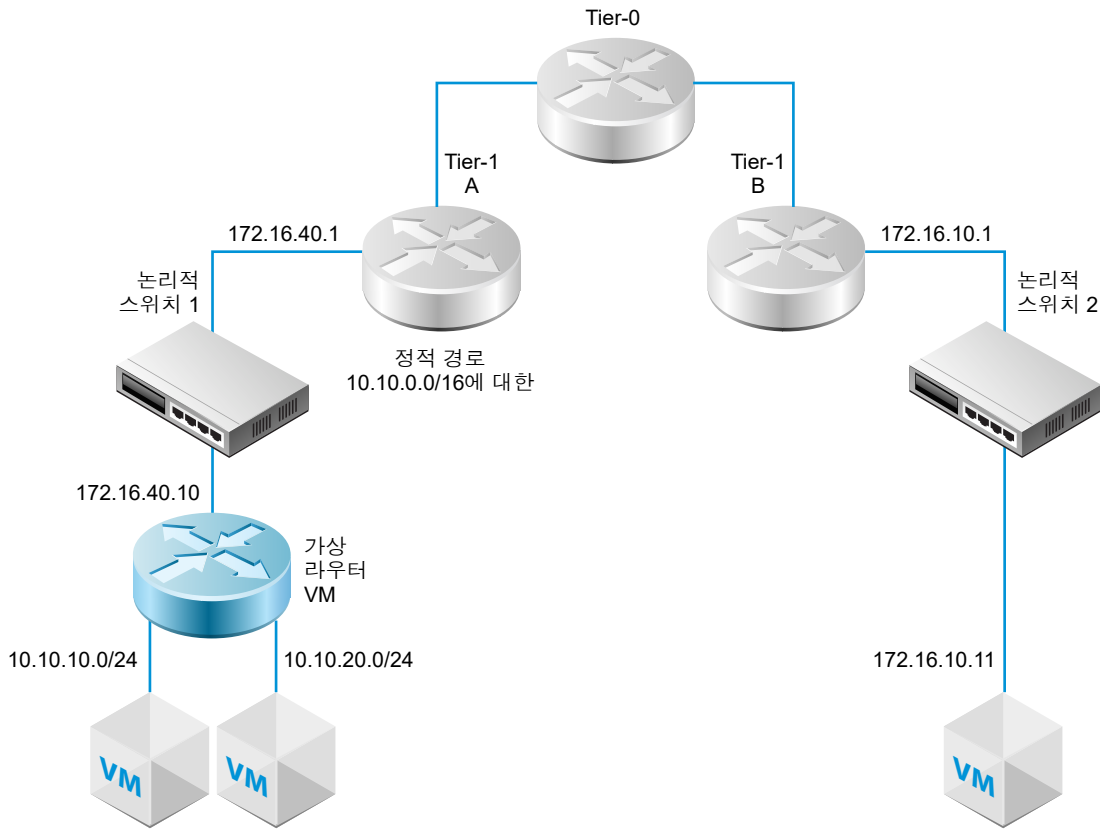
Tier-0 논리적 라우터가 Tier-1 논리적 라우터에 이미 연결된 경우 Tier-0 라우터가 Tier-1 라우터 연결 경로를 학습하고 있는지 확인할 수 있습니다. [Tier-0 라우터에 Tier-1 라우터에서 학습된 경로가 있는지 확인](#)의 내용을 참조하십시오.

## Tier-1 논리적 라우터 정적 경로 구성

NSX-T Data Center에서 가상 라우터를 통해 액세스할 수 있는 네트워크 집합으로의 연결을 제공하도록 Tier-1 논리적 라우터에서 정적 경로를 구성할 수 있습니다.

예를 들어 다음 다이어그램에서 Tier-1 A 논리적 라우터에는 NSX-T Data Center 논리적 스위치에 대한 다운링크 포트가 있습니다. 이 다운링크 포트(172.16.40.1)는 가상 라우터 VM에 대한 기본 게이트웨이 역할을 합니다. 가상 라우터 VM 및 Tier-1 A는 동일한 NSX-T Data Center 논리적 스위치를 통해 연결됩니다. Tier-1 논리적 라우터에는 가상 라우터를 통해 사용할 수 있는 네트워크를 요약하는 정적 경로 10.10.0.0/16이 있습니다. 그러면 Tier-1 A에서는 Tier-1 B에 정적 경로를 보급하도록 구성된 경로 보급이 생성됩니다.

그림 4-2. Tier-1 논리적 라우터 정적 경로 토폴로지



#### 사전 요구 사항

다운링크 포트가 구성되어 있는지 확인합니다. Tier-1 논리적 라우터에서 다운링크 포트 추가의 내용을 참조하십시오.

#### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 Tier-1 라우터의 이름을 클릭합니다.
- 4 **라우팅** 탭을 클릭하고 드롭다운 메뉴에서 **정적 경로**를 선택합니다.
- 5 **추가**를 클릭합니다.

**6** 네트워크 주소를 CIDR 형식으로 입력합니다.

예: 10.10.10.0/16

**7** **추가**를 클릭하여 다음 홉 IP 주소를 추가합니다.

예를 들면 172.16.40.10과 같습니다. 연필 아이콘을 클릭하고 드롭다운에서 **NULL**을 선택하여 null 경로를 지정할 수도 있습니다. 다른 다음 홉 주소를 추가하려면 **추가**를 다시 클릭합니다.

**8** 대화 상자의 맨 아래에서 **추가**를 클릭합니다.

새로 생성된 정적 경로 네트워크 주소가 행에 표시됩니다.

**9** Tier-1 논리적 라우터에서 **라우팅 > 경로 보급**을 선택합니다.**10** **편집**을 클릭하고 **모든 정적 경로 보급**을 선택합니다.**11** **저장**을 클릭합니다.

정적 경로는 NSX-T Data Center 오버레이를 거쳐 전파됩니다.

## 독립형 Tier-1 논리적 라우터 생성

독립형 Tier-1 논리적 라우터에는 다운링크가 없으며 Tier-0 라우터에 대한 연결이 없습니다. 서비스 라우터가 있고 분산 라우터는 없습니다. 서비스 라우터는 활성-대기 모드에서 하나의 NSX Edge 노드 또는 두 개의 NSX Edge 노드에 배포할 수 있습니다.

독립형 Tier-1 논리적 라우터:

- Tier-0 논리적 라우터에 연결되어 있지 않아야 합니다.
- 다운링크가 없어야 합니다.
- LB(로드 밸런서) 서비스를 연결하는 데 사용되는 경우 하나의 CSP(중앙 집중식 서비스 포트)만 포함할 수 있습니다.
- 오버레이 논리적 스위치 또는 VLAN 논리적 스위치에 연결될 수 있습니다.
- 로드 밸런싱 및 NAT 서비스만 지원합니다.

일반적으로 독립형 Tier-1 논리적 라우터는 일반 Tier-1 논리적 라우터도 연결된 논리적 스위치에 연결되어 있습니다. 독립형 Tier-1 논리적 라우터는 정적 경로 및 경로 보급이 구성된 후 일반 Tier-1 논리적 라우터를 통해 다른 디바이스와 통신할 수 있습니다.

### 절차

- 1** 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2** 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3** **추가**를 클릭하고 **Tier-1 라우터**를 선택합니다.
- 4** 논리적 라우터 이름 및 필요한 경우 설명을 입력합니다.
- 5** (필수 사항) 이 Tier-1 논리적 라우터에 연결할 NSX Edge 클러스터를 선택합니다.

**6** (필수 사항) 페일오버 모드 및 클러스터 멤버를 선택합니다.

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

**7** **추가**를 클릭합니다.**8** 방금 생성한 라우터의 이름을 클릭합니다.**9** **구성** 탭을 클릭하고 **라우터 포트**를 선택합니다**10** **추가**를 클릭합니다.**11** 라우터 포트 이름 및 필요한 경우 설명을 입력합니다.**12** **유형** 필드에서 **중앙 집중식**을 선택합니다.**13** **URPF 모드**의 경우 **엄격** 또는 **없음**을 선택합니다.

URPF(유니캐스트 역방향 경로 전달)는 보안 기능입니다.

**14** (필수 사항) 논리적 스위치를 선택합니다.**15** 이 연결이 스위치 포트를 생성할지 또는 기존 스위치 포트를 업데이트할지 선택합니다.**16** CIDR 표기법으로 라우터 포트 IP 주소를 입력합니다.**17** **추가**를 클릭합니다.**결과**

독립형 Tier-1 논리적 라우터를 사용하기 전에 다음에 유의하십시오.

- 독립형 Tier-1 논리적 라우터에 대한 기본 게이트웨이를 지정하려면 정적 경로를 추가해야 합니다. 서브넷은 0.0.0.0/0이어야 하며 다음 홉은 동일한 스위치에 연결된 일반 Tier-1 라우터의 IP 주소입니다.
- 독립형 라우터에 대한 ARP 프로키는 지원되지 않습니다. 따라서 CSP IP를 사용하는 경우가 아니면 CSP의 서브넷에서 LB 가상 서버 IP 또는 LB SNAT IP를 구성하지 않아야 합니다. 예를 들어 CSP IP가 1.1.1.1/24인 경우 가상 IP는 1.1.1.1 또는 일부 다른 서브넷 IP 주소여야 합니다. 1.1.1.1/24 서브넷의 다른 주소일 수 없습니다.
- NSX Edge VM의 경우 동일한 VLAN 지원 논리적 스위치 또는 동일한 VLAN ID가 있는 다른 VLAN 지원 논리적 스위치에 연결된 둘 이상의 CSP를 포함할 수 없습니다.

# Tier-0 논리적 라우터

## 5

NSX-T Data Center 논리적 라우터는 기본 하드웨어에서 완전히 분리된 가상 환경에서 라우팅 기능을 재현합니다. Tier-0 논리적 라우터는 논리적 및 물리적 네트워크 간의 게이트웨이를 켜고 끌 수 있는 서비스를 제공합니다.

---

**NSX Cloud 참고** NSX Cloud를 사용 중인 경우 NSX Cloud에 필요한 구성, 지원되는 기능 및 자동 생성된 논리적 엔티티의 목록은 [공용 클라우드에 대해 NSX-T Data Center 기능을 사용하는 방법](#)의 내용을 참조하십시오.

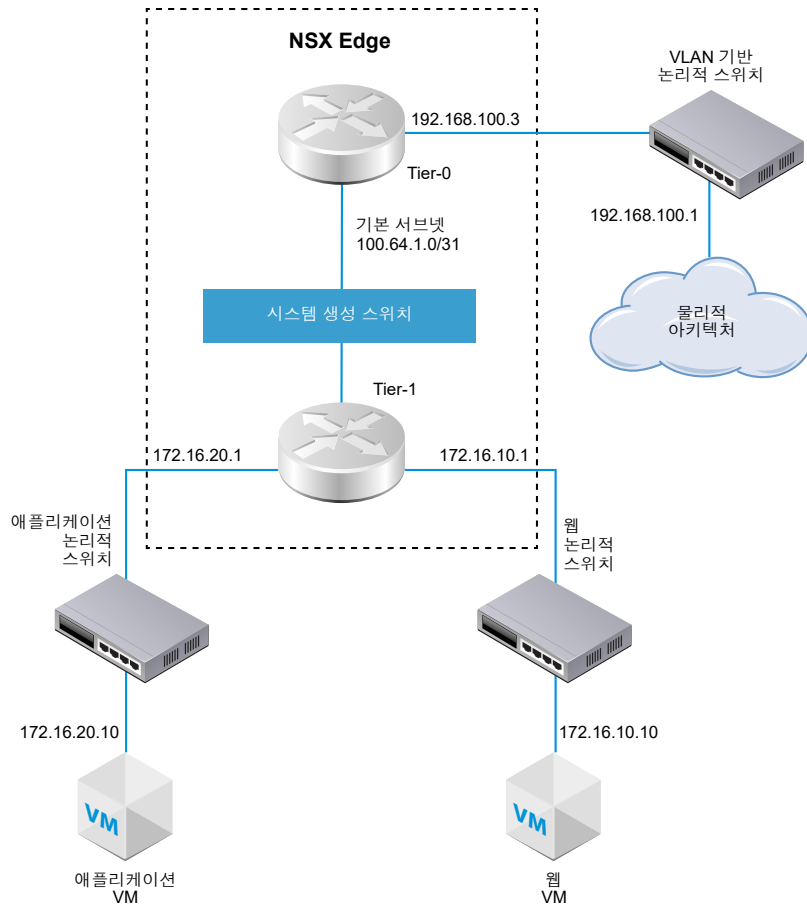
---

NSX Edge 클러스터는 여러 Tier-0 논리적 라우터를 지원할 수 있습니다. Tier-0 라우터는 BGP 동적 라우팅 프로토콜 및 ECMP를 지원합니다.

Tier-0 논리적 라우터를 추가하는 경우 구축하려는 네트워킹 토폴로지를 계획하는 것이 중요합니다.



그림 5-1. Tier-0 논리적 라우터 토폴로지



단순화를 위해 샘플 토폴로지에서는 단일 NSX Edge 노드에 호스팅된 단일 Tier-0 논리적 라우터에 연결된 단일 Tier-1 논리적 라우터를 보여줍니다. 이는 권장되는 토폴로지가 아닙니다. 논리적 라우터 설계를 완전히 활용하는 가장 이상적인 방법은 최소 2개의 NSX Edge 노드를 갖추고 있는 것입니다.

Tier-1 논리적 라우터에는 해당 VM이 연결된 웹 논리적 스위치와 애플리케이션 논리적 스위치가 있습니다. Tier-1 라우터를 Tier-0 라우터에 연결할 때 Tier-1 라우터와 Tier-0 라우터 간의 라우터-링크 스위치가 자동으로 생성됩니다. 따라서 이 스위치에는 시스템 생성이라는 레이블이 지정됩니다.

본 장은 다음 항목을 포함합니다.

- Tier-0 논리적 라우터 생성
- Tier-0과 Tier-1 연결
- NSX Edge 업링크를 위해 VLAN 논리적 스위치에 Tier-0 논리적 라우터 연결
- 루프백 라우터 포트 추가
- Tier-0 또는 Tier-1 논리적 라우터에 VLAN 포트 추가
- 정적 경로 구성
- BGP 구성 옵션

- Tier-0 논리적 라우터에서 BFD 구성
- Tier-0 논리적 라우터에서 경로 재배포 사용
- ECMP 라우팅 이해
- IP 접두사 목록 생성
- 커뮤니티 목록 생성
- 경로 맵 생성
- 전달 타이머 구성

## Tier-0 논리적 라우터 생성

Tier-0 논리적 라우터에는 NSX-T Data Center Tier-1 논리적 라우터에 연결하기 위한 다운링크 포트와 외부 네트워크에 연결하기 위한 업링크 포트가 있습니다.

### 사전 요구 사항

- 하나 이상의 NSX Edge가 설치되어 있는지 확인합니다. "NSX-T Data Center 설치 가이드"를 참조하십시오.
- NSX Controller 클러스터가 안정적인지 확인합니다.
- NSX Edge 클러스터가 구성되었는지 확인합니다. "NSX-T Data Center 설치 가이드"의 내용을 참조하십시오.
- Tier-0 논리적 라우터의 네트워킹 토폴로지를 숙지합니다. [장 5 Tier-0 논리적 라우터](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 **추가**를 클릭하여 Tier-0 논리적 라우터를 생성합니다.
- 4 드롭다운 메뉴에서 **Tier-0 라우터**를 선택합니다.
- 5 Tier-0 논리적 라우터에 이름을 할당합니다.
- 6 드롭다운 메뉴에서 이 Tier-0 논리적 라우터를 지원할 기존 NSX Edge 클러스터를 선택합니다.
- 7 (선택 사항) 고가용성 모드를 선택합니다.

기본적으로 활성-활성 모드가 사용됩니다. 활성-활성 모드에서 트래픽이 모든 멤버에서 로드 밸런싱됩니다. 활성-대기 모드에서 모든 트래픽은 선택된 활성 멤버에 의해 처리됩니다. 활성 멤버에 오류가 발생하면 새 멤버가 활성 멤버로 선택됩니다.

- 8** (선택 사항) **고급** 탭을 클릭하여 Tier-0 내부 전송 서브넷에 대한 서브넷을 입력합니다.

이는 Tier-0 서비스 라우터를 분산 라우터에 연결하는 서브넷입니다. 이 항목을 비워 두면 기본 169.0.0.0/28 서브넷이 사용됩니다.

- 9** (선택 사항) **고급** 탭을 클릭하여 Tier-0과 Tier-1 간 전송 서브넷에 대한 서브넷을 입력합니다.

이는 Tier-0 라우터를 이 Tier-0 라우터에 연결되는 임의의 Tier-1 라우터에 연결하는 서브넷입니다. 이 항목을 비워 두면 이러한 Tier-0과 Tier-1 간의 연결에 할당된 기본 주소 공간은 100.64.0.0/10입니다. 각 Tier-0과 Tier-1 간의 피어 연결에는 100.64.0.0/10 주소 공간 내에 /31 서브넷이 제공됩니다.

- 10 저장**을 클릭합니다.

새 Tier-0 논리적 라우터가 링크로 표시됩니다.

- 11** (선택 사항) Tier-0 논리적 라우터 링크를 클릭하여 요약을 검토합니다.

#### 다음에 수행할 작업

Tier-1 논리적 라우터를 이 Tier-0 논리적 라우터에 연결합니다.

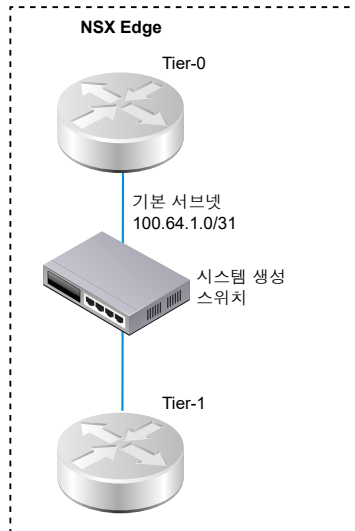
Tier-0 논리적 라우터를 구성하여 이를 VLAN 논리적 스위치에 연결하고 외부 네트워크에 대한 업링크를 생성합니다. [NSX Edge 업링크를 위해 VLAN 논리적 스위치에 Tier-0 논리적 라우터 연결](#)의 내용을 참조하십시오.

## Tier-0과 Tier-1 연결

Tier-0 논리적 라우터를 Tier-1 논리적 라우터에 연결하면 Tier-1 논리적 라우터가 노스바운드 및 동서 네트워크 연결을 할 수 있습니다.

Tier-1 논리적 라우터를 Tier-0 논리적 라우터에 연결하면 두 라우터 간의 라우터-링크 스위치가 생성됩니다. 이 스위치는 토폴로지에서 시스템 생성이라고 레이블이 지정되어 있습니다. 이러한 Tier-0과 Tier-1 간의 연결에 할당된 기본 주소 공간은 100.64.0.0/10입니다. 각 Tier-0과 Tier-1 간의 피어 연결에는 100.64.0.0/10 주소 공간 내에 /31 서브넷이 제공됩니다. (선택 사항) Tier-0의 **요약 > 고급** 구성에서 주소 공간을 구성할 수 있습니다.

다음 그림은 샘플 토폴로지를 보여줍니다.



## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 Tier-1 논리적 라우터를 선택합니다.
- 4 **요약** 탭에서 **편집**을 클릭합니다.
- 5 드롭다운 메뉴에서 Tier-0 논리적 라우터를 선택합니다.
- 6 (선택 사항) 드롭다운 목록에서 NSX Edge 클러스터를 선택합니다.  
 라우터가 NAT와 같은 서비스에 사용될 경우 Edge 디바이스가 Tier-1 라우터를 지원해야 합니다. NSX Edge 클러스터를 선택하지 않으면 Tier-1 라우터가 NAT를 수행할 수 없습니다.
- 7 멤버 및 기본 멤버를 지정합니다.  
 NSX Edge 클러스터를 선택하고 멤버 및 기본 멤버 필드를 비워 두면 NSX-T Data Center가 지정된 클러스터에서 지원 Edge 디바이스를 설정합니다.
- 8 **저장**을 클릭합니다.
- 9 Tier-1 라우터의 **구성** 탭을 클릭하여 지점 간 연결된 새로운 포트 IP 주소가 생성되었는지 확인합니다.  
 예를 들어 연결된 포트의 IP 주소는 100.64.1.1/31이 될 수 있습니다.
- 10 탐색 패널에서 Tier-0 논리적 라우터를 선택합니다.
- 11 Tier-0 라우터의 **구성** 탭을 클릭하여 지점 간 연결된 새로운 포트 IP 주소가 생성되었는지 확인합니다.  
 예를 들어 연결된 포트의 IP 주소는 100.64.1.1/31이 될 수 있습니다.

## 다음에 수행할 작업

Tier-0 라우터에서 Tier-1 라우터가 보급한 경로를 학습하는지 확인합니다.

## Tier-0 라우터에 Tier-1 라우터에서 학습된 경로가 있는지 확인

Tier-1 논리적 라우터는 Tier-0 논리적 라우터로 경로를 보급할 때 경로가 Tier-0 라우터의 라우팅 테이블에 NSX-T Data Center 정적 경로로 표시됩니다.

### 절차

- 1 NSX Edge에서 `get logical-routers` 명령을 실행하여 Tier-0 서비스 라우터의 VRF 번호를 찾습니다.

```
nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf        : 7
type       : SERVICE_ROUTER_TIER1

Logical Router
UUID       : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf        : 8
type       : DISTRIBUTED_ROUTER
```

- 2 `vrf <number>` 명령을 실행하여 Tier-0 서비스 라우터 컨텍스트를 시작합니다.

```
nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>
```

- 3 Tier-0 서비스 라우터에서 `get route` 명령을 실행하고 라우팅 테이블에 예상된 경로가 표시되는지 확인합니다.

Tier-1 라우터가 경로를 보급하고 있으므로 NSX-T Data Center NS(정적 경로)가 Tier-0 라우터에서 학습됩니다.

```
nsx-edge1(tier0_sr)> get route
```

Flags: c - connected, s - static, b - BGP, ns - nsx\_static

nc - nsx\_connected, rl - router\_link, t0n: Tier0-NAT, t1n: Tier1-NAT

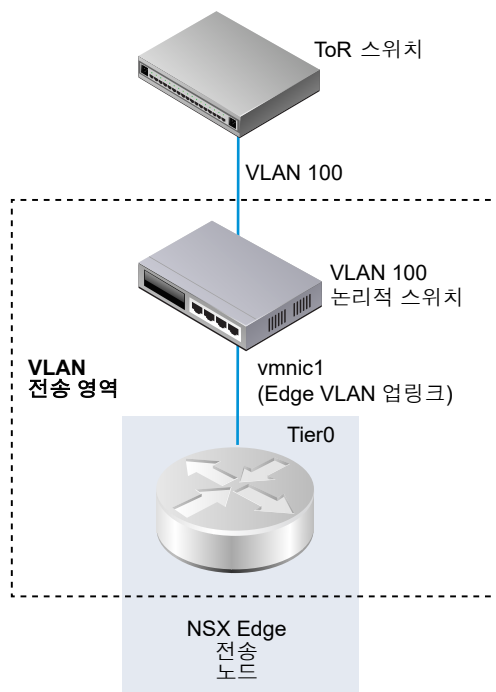
Total number of routes: 7

b	10.10.10.0/24	[20/0]	via 192.168.100.254
rl	100.91.176.0/31	[0/0]	via 169.254.0.1
c	169.254.0.0/28	[0/0]	via 169.254.0.2
ns	172.16.10.0/24 [3/3]	via 169.254.0.1	ns 172.16.20.0/24 [3/3] via 169.254.0.1
c	192.168.100.0/24	[0/0]	via 192.168.100.2

## NSX Edge 업링크를 위해 VLAN 논리적 스위치에 Tier-0 논리적 라우터 연결

NSX Edge 업링크를 생성하려면 Tier-0 라우터를 VLAN 스위치에 연결합니다.

다음의 간단한 토폴로지는 VLAN 전송 영역 내부의 VLAN 논리적 스위치를 보여줍니다. VLAN 논리적 스위치는 Edge의 VLAN 업링크에 대한 TOR 포트의 VLAN ID와 일치하는 VLAN ID를 갖습니다.



## 사전 요구 사항

VLAN 논리적 스위치를 생성합니다. [NSX Edge 업링크에 대한 VLAN 논리적 스위치 생성](#)의 내용을 참조하십시오.

Tier-0 라우터를 생성합니다.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 Tier-0 논리적 라우터를 선택합니다.
- 4 **구성** 탭에서 새 논리적 라우터 포트를 추가합니다.
- 5 포트의 이름(예: 업링크)을 입력합니다.
- 6 **업링크** 유형을 선택합니다.
- 7 Edge 전송 노드를 선택합니다.
- 8 VLAN 논리적 스위치를 선택합니다.
- 9 TOR 스위치에 연결된 포트와 같은 서브넷에 CIDR 형식으로 IP 주소를 입력합니다.

## 결과

Tier-0 라우터에 대해 새 업링크 포트가 추가됩니다.

## 다음에 수행할 작업

BGP 또는 정적 경로를 구성합니다.

## Tier-0 논리적 라우터 및 TOR 연결 확인

Tier-0 라우터에서 업링크에 라우팅하려면 랙 상단 디바이스와 연결되어 있어야 합니다.

## 사전 요구 사항

- Tier-0 논리적 라우터가 VLAN 논리적 스위치에 연결되어 있는지 확인합니다. [NSX Edge 업링크를 위해 VLAN 논리적 스위치에 Tier-0 논리적 라우터 연결](#)의 내용을 참조하십시오.

## 절차

- 1 NSX Manager CLI에 로그인합니다.
- 2 NSX Edge에서 `get logical-routers` 명령을 실행하여 Tier-0 서비스 라우터의 VRF 번호를 찾습니다.

```
nsx-edge-1> get logical-routers
Logical Router
UUID          : 736a80e3-23f6-5a2d-81d6-bbefb2786666
```

```

vrf      : 0
type     : TUNNEL

Logical Router
UUID     : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type     : SERVICE_ROUTER_TIER0

Logical Router
UUID     : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf      : 6
type     : DISTRIBUTED_ROUTER

Logical Router
UUID     : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf      : 7
type     : SERVICE_ROUTER_TIER1

Logical Router
UUID     : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf      : 8
type     : DISTRIBUTED_ROUTER

```

- 3** vrf <number> 명령을 실행하여 Tier-0 서비스 라우터 컨텍스트를 시작합니다.

```

nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>

```

- 4** Tier-0 서비스 라우터에서 get route 명령을 실행하여 예상되는 경로가 라우팅 테이블에 나타나는지 확인합니다.

TOR에 대한 경로는 연결됨(c)으로 나타납니다.

```

nsx-edge1(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

Total number of routes: 7

b  10.10.10.0/24      [20/0]      via 192.168.100.254
rl 100.91.176.0/31   [0/0]      via 169.254.0.1
c  169.254.0.0/28    [0/0]      via 169.254.0.2
ns 172.16.10.0/24    [3/3]      via 169.254.0.1
ns 172.16.20.0/24    [3/3]      via 169.254.0.1
c 192.168.100.0/24 [0/0] via 192.168.100.2

```



## 5 TOR에 ping을 수행합니다.

```
nsx-edge1(tier0_sr)> ping 192.168.100.254
PING 192.168.100.254 (192.168.100.254): 56 data bytes
64 bytes from 192.168.100.254: icmp_seq=0 ttl=64 time=2.822 ms
64 bytes from 192.168.100.254: icmp_seq=1 ttl=64 time=1.393 ms
^C
nsx-edge1>
--- 192.168.100.254 ping statistics ---
3 packets transmitted, 2 packets received, 33.3% packet loss
round-trip min/avg/max/stddev = 1.393/2.107/2.822/0.715 ms
```

### 결과

연결을 확인하기 위해 Tier-0 논리적 라우터 및 물리적 라우터 간에 패킷이 전송됩니다.

### 다음에 수행할 작업

네트워크 요구 사항에 따라 정적 경로 또는 BGP를 구성할 수 있습니다. [정적 경로 구성](#) 또는 [Tier-0 논리적 라우터에서 BGP 구성](#)의 내용을 참조하십시오.

## 루프백 라우터 포트 추가

Tier-0 논리적 라우터에 루프백 포트를 추가할 수 있습니다.

루프백 포트는 다음 용도로 사용할 수 있습니다.

- 라우팅 프로토콜의 라우터 ID
- NAT
- BFD
- 라우팅 프로토콜의 소스 주소

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 Tier-0 논리적 라우터를 선택합니다.
- 4 **구성 > 라우터 포트**를 선택합니다.
- 5 **추가**를 클릭합니다.
- 6 이름과 설명(선택 사항)을 입력합니다.
- 7 **루프백** 유형을 선택합니다.
- 8 Edge 전송 노드를 선택합니다.

## 9 IP 주소를 CIDR 형식으로 입력합니다.

### 결과

Tier-0 라우터에 대해 새 포트가 추가됩니다.

## Tier-0 또는 Tier-1 논리적 라우터에 VLAN 포트 추가

VLAN 지원 논리적 스위치만 있는 경우 NSX-T Data Center가 계층-3 서비스를 제공할 수 있도록 Tier-0 또는 Tier-1 라우터의 VLAN 포트에 스위치를 연결할 수 있습니다.

### 절차

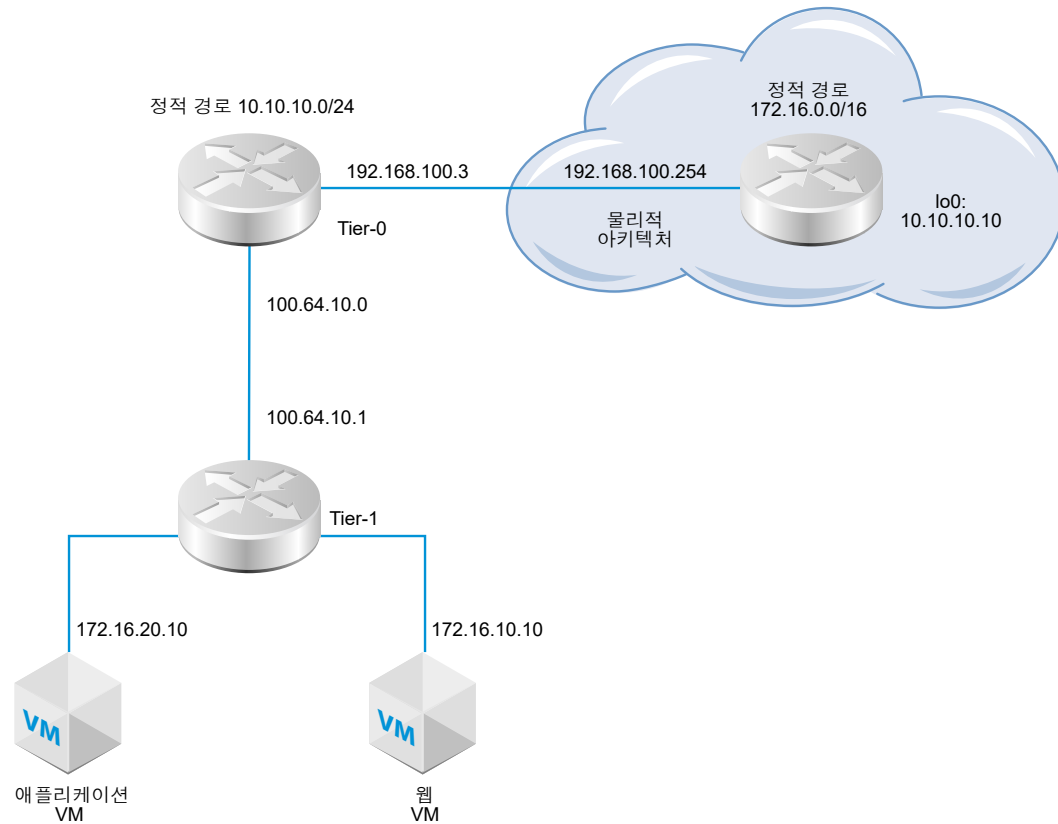
- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 라우터의 이름을 클릭합니다.
- 4 **구성** 탭을 클릭하고 **라우터 포트**를 선택합니다.
- 5 **추가**를 클릭합니다.
- 6 라우터 포트 이름 및 필요한 경우 설명을 입력합니다.
- 7 **유형** 필드에서 **중앙 집중식**을 선택합니다.
- 8 **URPF 모드**의 경우 **엄격** 또는 **없음**을 선택합니다.  
URPF(유니캐스트 역방향 경로 전달)는 보안 기능입니다.
- 9 (필수 사항) 논리적 스위치를 선택합니다.
- 10 이 연결이 스위치 포트를 생성할지 또는 기존 스위치 포트를 업데이트할지 선택합니다.  
기존 스위치 포트를 사용하여 연결하는 경우, 드롭다운 메뉴에서 포트를 선택합니다.
- 11 CIDR 표기법으로 라우터 포트 IP 주소를 입력합니다.
- 12 **추가**를 클릭합니다.

## 정적 경로 구성

Tier-0 라우터에 외부 네트워크에 대한 정적 경로를 구성할 수 있습니다. 정적 경로를 구성한 후에 Tier-0에서 Tier-1로의 경로를 보급할 필요가 없습니다. Tier-1 라우터에는 연결된 Tier-0 라우터를 향하는 정적 기본 경로가 자동으로 형성되기 때문입니다.

정적 경로 토폴로지는 물리적 아키텍처에 10.10.10.0/24 접두사에 대한 정적 경로가 있는 Tier-0 논리적 라우터를 표시합니다. 테스트를 위해 외부 라우터 루프백 인터페이스에 10.10.10.10/32 주소가 구성됩니다. 외부 라우터에는 애플리케이션 및 웹 VM에 도달하기 위해 172.16.0.0/16 접두사에 대한 정적 경로가 있습니다.

그림 5-2. 정적 경로 토폴로지



### 사전 요구 사항

- 물리적 라우터 및 Tier-0 논리적 라우터가 연결되어 있는지 확인합니다. [Tier-0 논리적 라우터 및 TOR 연결 확인](#)의 내용을 참조하십시오.
- 연결된 경로를 보급하기 위해 Tier-1 라우터가 구성되어 있는지 확인합니다. [Tier-1 논리적 라우터 생성](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 Tier-0 논리적 라우터를 선택합니다.
- 4 **라우팅** 탭을 클릭하고 드롭다운 메뉴에서 **정적 경로**를 선택합니다.
- 5 **추가**를 선택합니다.
- 6 네트워크 주소를 CIDR 형식으로 입력합니다.

예: 10.10.10.0/24

**7 + 추가**를 클릭하여 다음 홉 IP 주소를 추가합니다.

예를 들면 192.168.100.254와 같습니다. 연필 아이콘을 클릭하고 드롭다운에서 **NULL**을 선택하여 null 경로를 지정할 수도 있습니다.

**8** 관리 거리를 지정합니다.

**9** 드롭다운 목록에서 논리적 라우터 포트를 선택합니다.

목록에는 IPsec VTI(가상 터널 인터페이스) 포트가 포함됩니다.

**10 추가** 버튼을 클릭합니다.

다음에 수행할 작업

정적 경로가 제대로 구성되어 있는지 확인합니다. [정적 경로 확인](#)의 내용을 참조하십시오.

## 정적 경로 확인

CLI를 사용하여 정적 경로가 연결되어 있는지 확인합니다. 또한 외부 라우터가 내부 VM을 ping하고 외부 VM이 외부 라우터를 ping할 수 있는지도 확인해야 합니다.

사전 요구 사항

정적 경로가 구성되어 있는지 확인합니다. [정적 경로 구성](#)의 내용을 참조하십시오.

절차

**1** NSX Manager CLI에 로그인합니다.

## 2 정적 경로를 확인합니다.

- a 서비스 라우터 UUID 정보를 가져옵니다.

```
get logical-routers
```

```
nsx-edge1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 2
type       : TUNNEL

Logical Router
UUID       : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf        : 4
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf        : 5
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : a6ee6316-2212-4171-99cc-930c98bcad7f
vrf        : 6
type       : DISTRIBUTED_ROUTER
```

- b 출력에서 UUID 정보를 찾습니다.

```
Logical Router
UUID       : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf        : 4
type       : SERVICE_ROUTER_TIER0
```

- c 정적 경로가 작동되는지 확인합니다.

```
get logical-router d40bbfa4-3e3d-4178-8615-6f42ea335037 static
```

```
Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

s   10.10.10.0/24      [1/1]      via 192.168.100.254
rl  100.64.1.0/31      [0/0]      via 169.0.0.1
ns  172.16.10.0/24     [3/3]      via 169.0.0.1
ns  172.16.20.0/24     [3/3]      via 169.0.0.1
```

### 3 외부 라우터에서 내부 VM을 ping하여 NSX-T Data Center 오버레이를 통해 연결할 수 있는지 확인합니다.

#### a 외부 라우터에 연결합니다.

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=62 time=127 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=62 time=1.96 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.966/64.793/127.620/62.827 ms
```

#### b 네트워크 연결을 테스트합니다.

tracert 172.16.10.10

```
tracert to 172.16.10.10 (172.16.10.10), 30 hops max, 60 byte packets
 1 192.168.100.3 (192.168.100.3) 0.640 ms 0.575 ms 0.696 ms
 2 100.64.1.1 (100.64.1.1) 0.656 ms 0.604 ms 0.578 ms
 3 172.16.10.10 (172.16.10.10) 3.397 ms 3.703 ms 3.790 ms
```

### 4 VM에서 외부 IP 주소를 ping합니다.

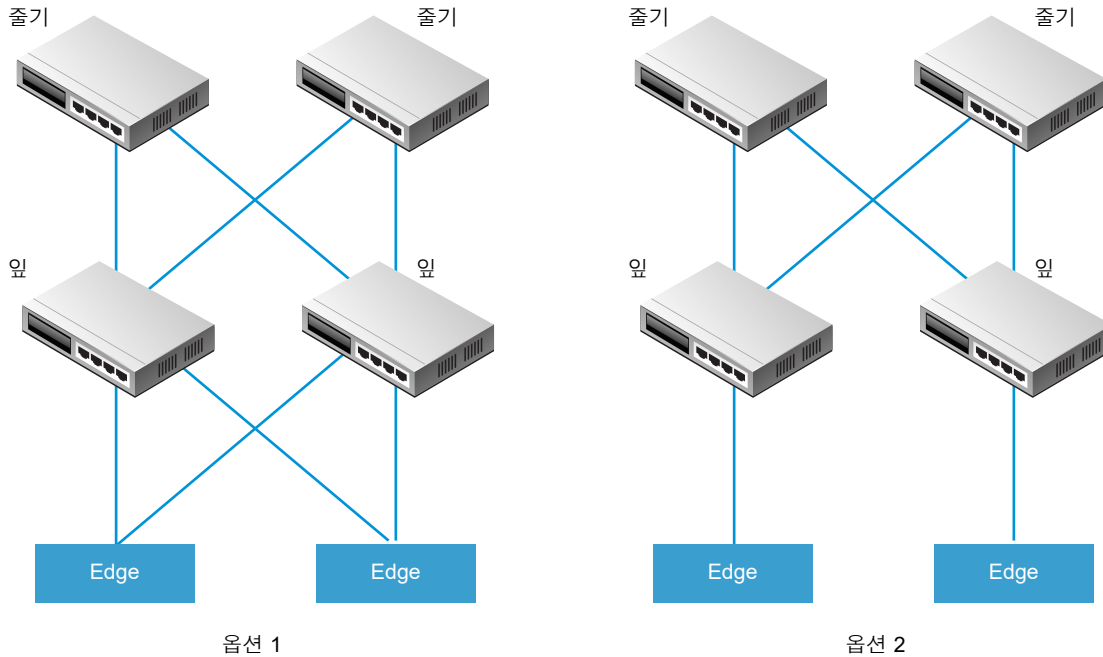
ping 10.10.10.10

```
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_req=1 ttl=62 time=119 ms
64 bytes from 10.10.10.10: icmp_req=2 ttl=62 time=1.93 ms
^C
--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.936/60.865/119.795/58.930 ms
```

## BGP 구성 옵션

Tier-0 논리적 라우터를 최대한 활용하려면 토폴로지가 Tier-0 라우터와 외부 Top-of-Rack 피어 간 BGP와의 이중화 및 대칭으로 구성되어야 합니다. 이러한 설계는 링크 및 노드 실패 시 연결을 보장하는 데 도움이 됩니다.

구성에는 활성-활성과 활성-대기 두 가지 모드가 있습니다. 다음 다이어그램은 대칭 구성의 두 가지 옵션을 나타냅니다. 표시된 각 토폴로지에는 두 개의 NSX Edge 노드가 있습니다. 활성-활성 구성의 경우 Tier-0 업링크 포트를 생성하면 각 업링크 포트를 최대 8개의 NSX Edge 전송 노드와 연결할 수 있습니다. 각 NSX Edge 노드는 두 개의 업링크를 가질 수 있습니다.



첫 번째 옵션의 경우 물리적 리프 노드 라우터가 구성되면 NSX Edge와 BGP 인접성을 가져야 합니다. 경로 재배포는 모든 BGP 인접 네트워크에 대해 동일한 BGP 메트릭을 가진 같은 네트워크 접두사를 포함해야 합니다. Tier-0 논리적 라우터 구성에서 모든 리프 노드 라우터는 BGP 인접 네트워크로 구성되어야 합니다.

Tier-0 라우터의 BGP 인접 네트워크를 구성할 때 로컬 주소(소스 IP 주소)를 지정하지 않으면 BGP 인접 네트워크 구성이 Tier-0 논리적 라우터 업링크와 연결된 모든 NSX Edge 노드에 전송됩니다. 로컬 주소를 구성하면 구성이 해당 IP 주소를 소유하고 있는 업링크와 함께 NSX Edge 노드로 이동합니다.

첫 번째 옵션의 경우 업링크가 NSX Edge 노드와 같은 서브넷에 있으면 로컬 주소를 생략하는 것이 적절합니다. NSX Edge 노드의 업링크가 다른 서브넷에 있으면 로컬 주소가 Tier-0 라우터의 BGP 인접 네트워크 구성에 지정되어 있어야 구성이 모든 연결된 NSX Edge 노드로 이동하는 것을 방지할 수 있습니다.

두 번째 옵션의 경우 Tier-0 논리적 라우터 구성이 Tier-0 서비스 라우터의 로컬 IP 주소를 포함하는지 확인합니다. 리프 노드 라우터는 BGP 인접 네트워크로 서로 직접 연결된 NSX Edge로만 구성됩니다.

## Tier-0 논리적 라우터에서 BGP 구성

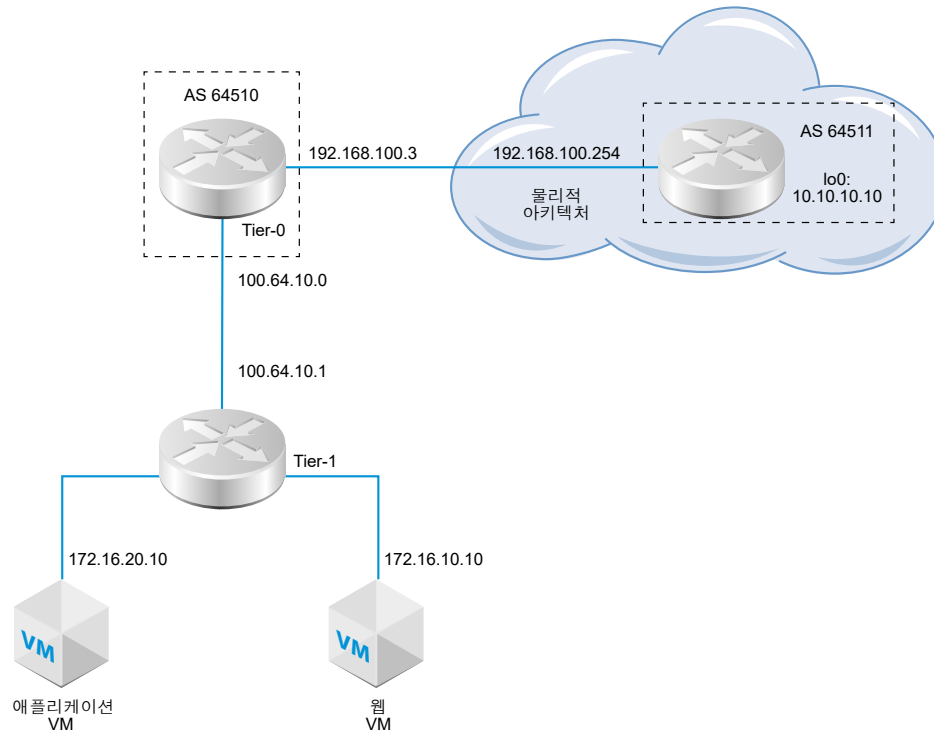
VM과 외부 환경 간에 액세스를 사용하도록 설정하려면 Tier-0 논리적 라우터와 물리적 인프라의 라우터 간에 eBGP(외부 BGP) 연결을 구성하면 됩니다.

BGP를 구성할 때 Tier-0 논리적 라우터에 대해 로컬 AS(자치 시스템) 번호를 구성해야 합니다. 예를 들어 다음 토폴로지는 로컬 AS 번호가 64510임을 나타냅니다. 또한 물리적 라우터의 원격 AS 번호도 구성해야 합니다. 이 예에서 원격 AS 번호는 64511입니다. 원격 인접 네트워크 IP 주소는 192.168.100.254입니다. 인접 네트워크는 Tier-0 논리적 라우터에 있는 업링크와 동일한 IP 서브넷에 있어야 합니다. BGP 다중 홉이 지원됩니다.

테스트를 위해 외부 라우터 루프백 인터페이스에 10.10.10.10/32 주소가 구성됩니다.

**참고** Edge 노드의 BGP 세션 형성에 사용되는 라우터 ID는 Tier-0 논리적 라우터의 업링크에 구성된 IP 주소 중에서 자동으로 선택됩니다. Edge 노드의 BGP 세션은 라우터 ID가 변경될 때 플래핑될 수 있습니다. 이러한 현상은 라우터 ID에 대해 자동으로 선택된 IP 주소가 삭제되거나 이 IP가 할당된 로컬 라우터 포트가 삭제될 때 발생할 수 있습니다.

그림 5-3. BGP 연결 토폴로지



### 사전 요구 사항

- 연결된 경로를 보급하기 위해 Tier-1 라우터가 구성되어 있는지 확인합니다. [Tier-1 논리적 라우터에서 경로 보급 구성](#)의 내용을 참조하십시오. 엄격히 말해서 이 단계는 BGP 구성에 대한 사전 요구 사항은 아니지만 2계층 토폴로지가 있고 Tier-1 네트워크를 BGP에 재배포하려는 경우 이를 수행해야 합니다.
- Tier-0 라우터가 구성되어 있는지 확인합니다. [Tier-0 논리적 라우터 생성](#)의 내용을 참조하십시오.
- Tier-0 논리적 라우터가 Tier-1 논리적 라우터의 경로를 학습했는지 확인합니다. [Tier-0 라우터에 Tier-1 라우터에서 학습된 경로가 있는지 확인](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 Tier-0 논리적 라우터를 선택합니다.



**4 라우팅** 탭을 클릭하고 드롭다운 메뉴에서 **BGP**를 선택합니다.

**5 편집**을 클릭합니다.

a 로컬 AS 번호를 구성합니다.

예: 64510

b **상태** 전환 버튼을 클릭하여 BGP를 사용하도록 설정합니다.

[상태] 버튼에 사용 [사용]이라고 표시됩니다.

c (선택 사항) **ECMP** 토글 버튼을 클릭하여 ECMP를 사용하도록 설정합니다.

d (선택 사항) **정상적인 다시 시작** 토글 버튼을 클릭하여 정상적으로 다시 시작하도록 할 수 있습니다.

e (선택 사항) 경로 집계를 구성하고, 정상적인 다시 시작을 사용하도록 설정하고, ECMP를 사용하도록 설정합니다.

정상적인 다시 시작은 Tier-0 라우터와 연결된 NSX Edge 클러스터에 하나의 Edge 노드가 있을 때만 지원됩니다.

f **저장**을 클릭합니다.

**6 추가**를 클릭하여 BGP 인접 네트워크를 추가합니다.

**7** 인접 네트워크 IP 주소를 입력합니다.

예: 192.168.100.254

**8** (선택 사항) 최대 홉 한계를 지정합니다.

기본값은 1입니다.

**9** 원격 AS 번호를 입력합니다.

예: 64511

**10** (선택 사항) 타이머(연결 유지 시간 및 보류 시간) 및 암호를 구성합니다.

**11** (선택 사항) **로컬 주소** 탭을 클릭하여 로컬 주소를 선택합니다.

a (선택 사항) **모든 업링크**를 선택 취소하여 루프백 포트와 업링크 포트를 둘 다 확인합니다.

**12** (선택 사항) **주소 패밀리** 탭을 클릭하여 주소 패밀리를 추가합니다.

**13** (선택 사항) **BFD 구성** 탭을 클릭하여 BFD를 사용하도록 설정합니다.

**14 저장**을 클릭합니다.

다음에 수행할 작업

BGP가 제대로 작동하는지 테스트합니다. [Tier-0 서비스 라우터에서 BGP 연결 확인](#)의 내용을 참조하십시오.

## Tier-0 서비스 라우터에서 BGP 연결 확인

CLI를 사용하여 Tier-0 서비스 라우터에서 인접 네트워크에 대한 BGP 연결이 설정되어 있는지 확인합니다.

### 사전 요구 사항

BGP가 구성되어 있는지 확인합니다. [Tier-0 논리적 라우터에서 BGP 구성](#)의 내용을 참조하십시오.

### 절차

- 1 NSX Manager CLI에 로그인합니다.
- 2 NSX Edge에서 `get logical-routers` 명령을 실행하여 Tier-0 서비스 라우터의 VRF 번호를 찾습니다.

```
nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf        : 7
type       : SERVICE_ROUTER_TIER1

Logical Router
UUID       : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf        : 8
type       : DISTRIBUTED_ROUTER
```

- 3 `vrf <number>` 명령을 실행하여 Tier-0 서비스 라우터 컨텍스트를 시작합니다.

```
nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>
```

#### 4 BGP 상태가 Established, up인지 확인합니다.

```
get bgp neighbor
```

```
BGP neighbor: 192.168.100.254 Remote AS: 64511
BGP state: Established, up
Hold Time: 180s Keepalive Interval: 60s
Capabilities:
    Route Refresh: advertised and received
    Address Family: IPv4 Unicast:advertised and received
    Graceful Restart: none
    Restart Remaining Time: 0
Messages: 28 received, 31 sent
Minimum time between advertisements: 30s (default)
For Address Family IPv4 Unicast:advertised and received
    Route Refresh: 0 received, 0 sent
    Prefixes: 2 received, 2 sent, 2 advertised
1 Connections established, 2 dropped
Local host: 192.168.100.3, Local port: 179
Remote host: 192.168.100.254, Remote port: 33044
```

다음에 수행할 작업

외부 라우터에서 BGP 연결을 확인합니다. [북-남 연결 및 경로 재배포 확인](#)의 내용을 참조하십시오.

## Tier-0 논리적 라우터에서 BFD 구성

BFD(Bidirectional Forwarding Detection)는 경로 전달 실패를 감지할 수 있는 프로토콜입니다.

**참고** 이 릴리스에서 VTI(가상 터널 인터페이스) 포트를 통한 BFD는 지원되지 않습니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 Tier-0 논리적 라우터를 선택합니다.
- 4 **라우팅** 탭을 클릭하고 드롭다운 메뉴에서 **BFD**를 선택합니다.
- 5 **편집**을 클릭하여 BFD를 구성합니다.
- 6 **상태** 전환 버튼을 클릭하여 BFD를 사용하도록 설정합니다.

필요한 경우 글로벌 BFD 속성인 **수신 간격**, **전송 간격** 및 **비활성 간격 선언**을 변경할 수 있습니다.

- 7 (선택 사항) BFD 피어를 추가하려면 [정적 경로 다음 홉에 대한 BFD 피어]에서 **추가**를 클릭합니다.

피어 IP 주소를 지정하고 관리 상태를 **사용**으로 설정합니다. 필요한 경우 글로벌 BFD 속성인 **수신 간격**, **전송 간격** 및 **비활성 간격 선언**을 재정의할 수 있습니다.

## Tier-0 논리적 라우터에서 경로 재배포 사용

경로 재배포를 사용하도록 설정하면 Tier-0 논리적 라우터는 지정된 경로를 노스바운드 라우터와 공유하기 시작합니다.

### 사전 요구 사항

- Tier-1 논리적 라우터 네트워크를 보급하여 Tier-0 논리적 라우터에 재배포할 수 있도록 Tier-0 및 Tier-1 논리적 라우터가 연결되어 있는지 확인합니다. [Tier-0과 Tier-1 연결](#)의 내용을 참조하십시오.
- 경로 재배포에서 특정 IP 주소를 필터링하려면 경로 맵이 구성되어 있는지 확인합니다. [경로 맵 생성](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 Tier-0 논리적 라우터를 선택합니다.
- 4 **라우팅** 탭을 클릭하고 드롭다운 메뉴에서 **경로 재배포**를 선택합니다.
- 5 **추가**를 클릭하여 경로 재배포 조건을 완료합니다.

옵션	설명
<b>이름 및 설명</b>	경로 재배포에 이름을 할당합니다. 필요한 경우 설명을 제공할 수 있습니다. 이름의 예로 advertise-to-bgp-neighbor를 들 수 있습니다.
<b>소스</b>	재배포하려는 소스 경로 확인란을 선택합니다. 정적 - Tier-0 정적 경로. NSX 연결됨 - Tier-1 연결된 경로. NSX 정적 - Tier-1 정적 경로. 다음 정적 경로가 자동으로 생성됩니다. Tier-0 NAT - NAT가 Tier-0 논리적 라우터에 구성되는 경우 생성된 경로 Tier-1 NAT - NAT가 Tier-1 논리적 라우터에 구성되는 경우 생성된 경로
<b>경로 맵</b>	(선택 사항) 경로 맵을 할당하여 경로 재배포에서 IP 주소 시퀀스를 필터링합니다.

- 6 **저장**을 클릭합니다.
- 7 **상태** 토글 버튼을 클릭하여 경로 재배포를 사용하도록 설정합니다.  
[상태] 버튼이 [사용]으로 나타납니다.

## 북-남 연결 및 경로 재배포 확인

CLI를 사용하여 BGP 경로가 학습되었는지 확인합니다. 외부 라우터에서 NSX-T Data Center 연결 VM에 연결할 수 있는지를 확인할 수도 있습니다.

## 사전 요구 사항

- BGP가 구성되어 있는지 확인합니다. [Tier-0 논리적 라우터에서 BGP 구성](#)의 내용을 참조하십시오.
- NSX-T Data Center 정적 경로가 재배포되도록 설정되어 있는지 확인합니다. [Tier-0 논리적 라우터에서 경로 재배포 사용](#)의 내용을 참조하십시오.

## 절차

- 1 NSX Manager CLI에 로그인합니다.
- 2 외부 BGP 인접 네트워크에서 학습된 경로를 확인합니다.

```
nsx-edge1(tier0_sr)> get route bgp
```

```
Flags: c - connected, s - static, b - BGP, ns - nsx_static
```

```
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT
```

```
b    10.10.10.0/24      [20/0]      via 192.168.100.254
```

### 3 외부 라우터에서 BGP 경로가 학습되었는지와 NSX-T Data Center 오버레이를 통해 VM에 연결할 수 있는지 확인합니다.

#### a BGP 경로를 나열합니다.

```
user@router# run show ip route bgp
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 172.16.10.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
B>* 172.16.20.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
B>* 172.16.30.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
```

#### b 외부 라우터에서 NSX-T Data Center 연결 VM을 ping합니다.

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=62 time=127 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=62 time=1.96 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.966/64.793/127.620/62.827 ms
```

#### c NSX-T Data Center 오버레이를 통한 경로를 확인합니다.

traceroute 172.16.10.10

```
traceroute to 172.16.10.10 (172.16.10.10), 30 hops max, 60 byte packets
 1 192.168.100.3 (192.168.100.3) 0.640 ms 0.575 ms 0.696 ms
 2 100.91.176.1 (100.91.176.1) 0.656 ms 0.604 ms 0.578 ms
 3 172.16.10.10 (172.16.10.10) 3.397 ms 3.703 ms 3.790 ms
```

### 4 내부 VM에서 외부 IP 주소를 ping합니다.

ping 10.10.10.10

```
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_req=1 ttl=62 time=119 ms
64 bytes from 10.10.10.10: icmp_req=2 ttl=62 time=1.93 ms
^C
--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.936/60.865/119.795/58.930 ms
```

#### 다음에 수행할 작업

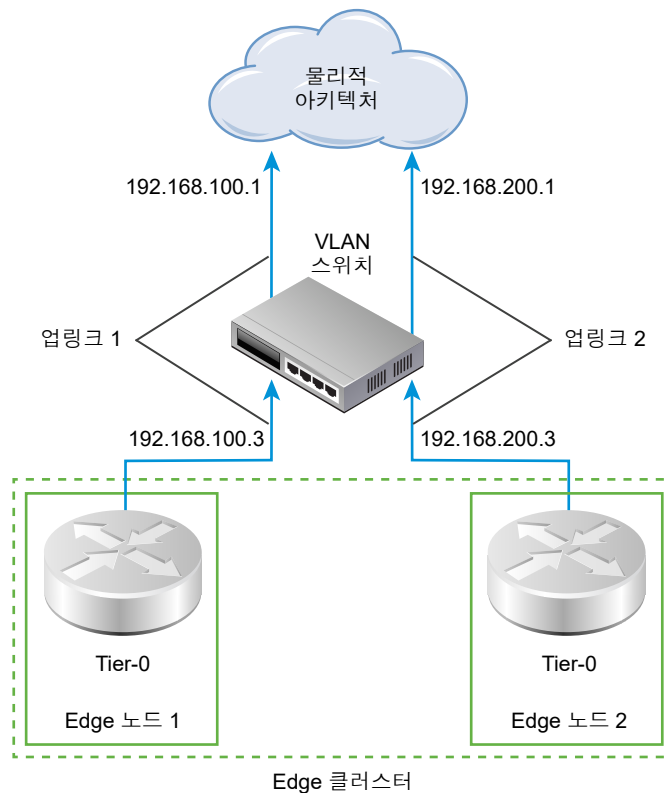
ECMP와 같은 추가 라우팅 기능을 구성합니다.

## ECMP 라우팅 이해

ECMP(Equal Cost Multi-Path) 라우팅 프로토콜은 Tier-0 논리적 라우터에 업링크를 추가하여 북-남 통신 대역폭을 늘리고, NSX Edge 클러스터의 각 Edge 노드에 맞게 이를 구성합니다. ECMP 라우팅 경로는 트래픽을 로드 밸런싱하는 데 사용되며 실패한 경로에 대해 Fault Tolerance를 제공합니다.

ECMP 경로는 자동으로 논리적 스위치에 연결된 VM에서 Tier-0 논리적 라우터가 인스턴스화되는 Edge 노드로 생성됩니다. 최대 8개의 ECMP 경로가 지원됩니다.

그림 5-4. ECMP 라우팅 토폴로지



예를 들어 토폴로지는 NSX Edge 클러스터의 Tier-0 논리적 라우터 2개를 보여줍니다. 각 Tier-0 논리적 라우터는 Edge 노드에 있고 이러한 노드는 클러스터에 속합니다. 업링크 포트 192.168.100.3 및 198.168.200.3은 전송 노드가 논리적 스위치에 연결되어 물리적 네트워크에 대한 액세스 권한을 얻는 방식을 정의합니다. ECMP 라우팅 경로가 사용되도록 설정되면 이러한 경로는 논리적 스위치에 연결된 VM 및 NSX Edge 클러스터에 있는 2개의 Edge 노드를 연결합니다. 다중 ECMP 라우팅 경로는 네트워크 처리량 및 복원력을 높입니다.

## 두 번째 Edge 노드에 대한 업링크 포트 추가

ECMP를 사용하도록 설정하기 전에 업링크를 구성하여 Tier-0 논리적 라우터를 VLAN 논리적 스위치에 연결해야 합니다.

## 사전 요구 사항

- 전송 영역 및 두 개의 전송 노드가 구성되어 있는지 확인합니다. "NSX-T Data Center 설치 가이드"의 내용을 참조하십시오.
- 두 개의 Edge 노드 및 Edge 클러스터가 구성되어 있는지 확인합니다. "NSX-T Data Center 설치 가이드"의 내용을 참조하십시오.
- 업링크에 대해 VLAN 논리적 스위치를 사용할 수 있는지 확인합니다. [NSX Edge 업링크에 대한 VLAN 논리적 스위치 생성](#)의 내용을 참조하십시오.
- Tier-0 논리적 라우터가 구성되어 있는지 확인합니다. [Tier-0 논리적 라우터 생성](#)의 내용을 참조하십시오.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 Tier-0 논리적 라우터를 선택합니다.
- 4 **구성** 탭을 클릭하여 라우터 포트를 추가합니다.
- 5 **추가**를 클릭합니다.
- 6 라우터 포트 세부 정보의 입력을 완료합니다.

옵션	설명
이름	라우터 포트의 이름을 할당합니다.
설명	포트가 ECMP 구성에 사용된다는 추가 설명을 제공합니다.
유형	기본 유형 <b>업링크</b> 를 수락합니다.
전송 노드	드롭다운 메뉴에서 호스트 전송 노드를 할당합니다.
논리적 스위치	드롭다운 메뉴에서 VLAN 논리적 스위치를 할당합니다.
논리적 스위치 포트	새로운 스위치 포트 이름을 할당합니다. 기존 스위치 포트를 사용할 수도 있습니다.
IP 주소/마스크	ToR 스위치에 연결된 포트와 같은 서브넷에 있는 IP 주소를 입력합니다.

- 7 **저장**을 클릭합니다.

## 결과

Tier-0 라우터 및 VLAN 논리적 스위치에 새 업링크 포트가 추가됩니다. Tier-0 논리적 라우터는 두 Edge 노드에서 구성됩니다.

## 다음에 수행할 작업

두 번째 인접 네트워크에 대해 BGP 연결을 생성하고 ECMP 라우팅을 사용하도록 설정합니다. [두 번째 BGP 인접 네트워크 추가 및 ECMP 라우팅 사용](#)의 내용을 참조하십시오.



## 두 번째 BGP 인접 네트워크 추가 및 ECMP 라우팅 사용

ECMP 라우팅을 사용하도록 설정하기 전에 BGP 인접 네트워크를 추가하고 새로 추가된 업링크 정보로 이를 구성해야 합니다.

### 사전 요구 사항

두 번째 Edge 노드에 업링크 포트가 구성되어 있는지 확인합니다. [두 번째 Edge 노드에 대한 업링크 포트 추가](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 Tier-0 논리적 라우터를 선택합니다.
- 4 **라우팅** 탭을 클릭하고 드롭다운 메뉴에서 **BGP**를 선택합니다.
- 5 [인접 네트워크] 섹션 아래의 **추가**를 클릭하여 BGP 인접 네트워크를 추가합니다.
- 6 인접 네트워크 IP 주소를 입력합니다.  
예: 192.168.200.254
- 7 (선택 사항) 최대 홉 한계를 지정합니다.  
기본값은 1입니다.
- 8 원격 AS 번호를 입력합니다.  
예: 64511
- 9 (선택 사항) **로컬 주소** 탭을 클릭하여 로컬 주소를 선택합니다.  
a (선택 사항) **모든 업링크**를 선택 취소하여 루프백 포트와 업링크 포트를 둘 다 확인합니다.
- 10 (선택 사항) **주소 패밀리** 탭을 클릭하여 주소 패밀리를 추가합니다.
- 11 (선택 사항) **BFD 구성** 탭을 클릭하여 BFD를 사용하도록 설정합니다.
- 12 **저장**을 클릭합니다.  
새로 추가된 BGP 인접 네트워크가 나타납니다.
- 13 [BGP 구성] 섹션 옆에 있는 **편집**을 클릭합니다.
- 14 **ECMP** 토글 버튼을 클릭하여 ECMP를 사용하도록 설정합니다.  
[상태] 버튼에 사용 [사용]이라고 표시됩니다.
- 15 **저장**을 클릭합니다.

### 결과

여러 ECMP 라우팅 경로가 논리적 스위치에 연결된 VM과 Edge 클러스터에 있는 두 개의 Edge 노드를 연결합니다.

## 다음에 수행할 작업

ECMP 라우팅 연결이 제대로 작동하는지 테스트합니다. [ECMP 라우팅 연결 확인](#)의 내용을 참조하십시오.

## ECMP 라우팅 연결 확인

CLI를 사용하여 인접 네트워크에 대한 ECMP 라우팅 연결이 설정되어 있는지 확인합니다.

### 사전 요구 사항

ECMP 라우팅이 구성되어 있는지 확인합니다. [두 번째 Edge 노드에 대한 업링크 포트 추가](#) 및 [두 번째 BGP 인접 네트워크 추가 및 ECMP 라우팅 사용](#)을 참조하십시오.

### 절차

- 1 NSX Manager CLI에 로그인합니다.
- 2 분산 라우터 UUID 정보를 가져옵니다.

```
get logical-routers
```

```
Logical Router
UUID          : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf           : 2
type          : TUNNEL
```

```
Logical Router
UUID          : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf           : 4
type          : SERVICE_ROUTER_TIER0
```

```
Logical Router
UUID          : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf           : 5
type          : DISTRIBUTED_ROUTER
```

```
Logical Router
UUID          : a6ee6316-2212-4171-99cc-930c98bcad7f
vrf           : 6
type          : DISTRIBUTED_ROUTER
```

- 3 출력에서 UUID 정보를 찾습니다.

```
Logical Router
UUID          : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf           : 5
type          : DISTRIBUTED_ROUTER
```

- 4 Tier-0 분산 라우터에 대한 VRF를 입력합니다.

```
vrf 5
```

- 5 Tier-0 분산 라우터가 Edge 노드에 연결되어 있는지 확인합니다.

```
get forwarding
```

예: edge-node-1 및 edge-node-2

- 6 **exit**를 입력하여 vrf 컨텍스트를 종료합니다.

- 7 Tier-0 논리적 라우터에 대한 활성 컨트롤러를 엽니다.

- 8 컨트롤러 노드의 Tier-0 분산 라우터가 연결되어 있는지 확인합니다.

```
get logical-router <UUID> route
```

UUID의 경로 유형은 NSX\_CONNECTED로 표시됩니다.

- 9 두 Edge 노드에서 SSH 세션을 시작합니다.

- 10 패킷을 캡처하기 위한 세션을 시작합니다.

```
set capture session 0 interface fp-eth1 dir tx
```

```
set capture session 0 expression src net <IP_Address>
```

- 11 제어 센터로 이동한 후 httpdata11.bat 및 httpdata12.bat 스크립트를 두 번 클릭합니다.

두 웹 VM에 대한 많은 수의 HTTP 요청이 전송되고, Edge 노드를 사용하여 두 경로로 트래픽이 해시되므로 ECMP가 작동하고 있음을 알 수 있습니다.

- 12 캡처 세션을 중지합니다.

```
del capture session 0
```

- 13 bat 스크립트를 제거합니다.

## IP 접두사 목록 생성

IP 접두사 목록에는 경로 보급을 위한 액세스 권한이 할당된 단일 또는 여러 IP 주소가 포함됩니다. 이 목록의 IP 주소는 순차적으로 처리됩니다. IP 접두사 목록은 BGP 인접 네트워크 필터 또는 경로 맵을 통해 내부 또는 외부 방향으로 참조됩니다.

예를 들어 IP 접두사 목록에 IP 주소 192.168.100.3/27을 추가하고 경로가 노스바운드 라우터로 재배포되지 못하게 거부합니다. le(less-than-or-equal-to) 및 ge(greater-than-or-equal-to) 수정자를 IP 주소에 추가하여 경로 재배포를 허용하거나 제한할 수도 있습니다. 예를 들어 192.168.100.3/27 ge 24 le 30 수정자는 길이가 24비트보다 크거나 같고, 30비트보다 작거나 같은 서브넷 마스크를 검색합니다.

---

**참고** 경로에 대한 기본 작업은 **거부**입니다. 특정 경로를 거부하거나 허용하기 위한 접두사 목록을 생성할 때, 다른 모든 경로를 허용하려는 경우에는 특정 네트워크 주소를 포함하지 않는 IP 접두사를 생성(드롭다운 목록에서 **임의** 선택)하고 **허용** 작업을 선택하십시오.

---

### 사전 요구 사항

Tier-0 논리적 라우터가 구성되어 있는지 확인합니다. [Tier-0 논리적 라우터 생성](#)의 내용을 참조하십시오.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 Tier-0 논리적 라우터를 선택합니다.
- 4 **라우팅** 탭을 클릭하고 드롭다운 메뉴에서 **IP 접두사 목록**을 선택합니다.
- 5 **추가**를 클릭합니다.
- 6 IP 접두사 목록의 이름을 입력합니다.
- 7 접두사를 지정하려면 **추가**를 클릭합니다.
  - a IP 주소를 CIDR 형식으로 입력합니다.  
예: 192.168.100.3/27
  - b 드롭다운 메뉴에서 **거부** 또는 **허용**을 선택합니다.
  - c (선택 사항) **le** 또는 **ge** 수정자로 IP 주소 번호의 범위를 설정합니다.  
예를 들어 **le**를 30으로, **ge**를 24로 설정합니다.
- 8 접두사를 추가로 지정하려면 이전 단계를 반복합니다.
- 9 창의 맨 아래에서 **추가**를 클릭합니다.

## 커뮤니티 목록 생성

커뮤니티 목록을 기반으로 경로 맵을 구성할 수 있도록 BGP 커뮤니티 목록을 생성할 수 있습니다.

### 사전 요구 사항

Tier-0 논리적 라우터가 구성되어 있는지 확인합니다. [Tier-0 논리적 라우터 생성](#)의 내용을 참조하십시오.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 Tier-0 논리적 라우터를 선택합니다.
- 4 **라우팅** 탭을 클릭하고 드롭다운 메뉴에서 **커뮤니티 목록**을 선택합니다.
- 5 **추가**를 클릭합니다.
- 6 커뮤니티 목록의 이름을 입력합니다.

- 7 aa:nn 형식(예: 300:500)을 사용하여 커뮤니티를 지정하고 Enter 키를 누릅니다. 커뮤니티를 더 추가하려면 반복합니다.

또한 드롭다운 화살표를 클릭하고 다음 중 하나 이상을 선택할 수 있습니다.

- NO\_EXPORT\_SUBCONFED - EBGp 피어로 보급하지 마십시오.
- NO\_ADVERTISE - 어떤 피어로도 보급하지 마십시오.
- NO\_EXPORT - BGP 연합 외부로 보급하지 마십시오.

- 8 **추가**를 클릭합니다.

## 경로 맵 생성

경로 맵은 IP 접두사 목록, BGP 경로 특성 및 연결된 작업 순서로 구성됩니다. 라우터는 이 순서에서 일치하는 IP 주소를 검색합니다. 일치하는 주소가 있으면 라우터는 작업을 수행하고 검색을 더 이상 하지 않습니다.

경로 맵은 BGP 인접 네트워크 수준 및 경로 재배포에서 참조될 수 있습니다. IP 접두사 목록이 경로 맵에서 참조되고, 경로 맵의 허용 또는 거부 작업이 적용되면 경로 맵 순서에 지정된 작업이 IP 접두사 목록 내의 사양을 재정의합니다.

### 사전 요구 사항

IP 접두사 목록이 구성되어 있는지 확인합니다. [IP 접두사 목록 생성](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 Tier-0 논리적 라우터를 선택합니다.
- 4 **라우팅 > 경로 맵**을 선택합니다.
- 5 **추가**를 클릭합니다.
- 6 경로 맵에 대한 이름 및 설명(선택 사항)을 입력합니다.
- 7 **추가**를 클릭하여 경로 맵에 항목을 추가합니다.
- 8 **IP 접두사 목록/커뮤니티 목록 일치** 열을 편집하여 IP 접두사 목록 또는 커뮤니티 목록 중 하나를 선택합니다. 둘 다 선택할 수는 없습니다.
- 9 (선택 사항) BGP 특성을 설정합니다.

BGP 특성	설명
AS 경로 추가	하나 이상의 AS(자치 시스템) 번호를 경로 앞에 추가함으로써 경로를 더 길게 만들어 덜 선호되게 합니다.
MED	Multi-Exit Discriminator는 AS에 대해 선호되는 경로를 외부 피어에 알려줍니다.

BGP 특성	설명
가중치	가중치를 설정하여 경로 선택에 영향을 줍니다. 범위는 0 - 65535입니다.
커뮤니티	<p>aa:nn 형식을 사용하여 커뮤니티를 지정합니다(예: 300:500). 또는 드롭다운 메뉴를 사용하여 다음 중 하나를 선택합니다.</p> <ul style="list-style-type: none"> <li>■ NO_EXPORT_SUBCONFED - EBGp 피어로 보급하지 마십시오.</li> <li>■ NO_ADVERTISE - 어떤 피어로도 보급하지 마십시오.</li> <li>■ NO_EXPORT - BGP 연합 외부로 보급하지 마십시오.</li> </ul>

**10 [작업] 열에서 허용 또는 거부를 선택합니다.**

IP 접두사 목록의 IP 주소 보급을 허용하거나 거부할 수 있습니다.

**11 저장**을 클릭합니다.

## 전달 타이머 구성

Tier-0 논리적 라우터에 대한 전달 타이머를 구성할 수 있습니다.

전달 타이머는 라우터가 첫 번째 BGP 세션이 설정된 후 알림을 보내기 전에 기다려야 하는 시간(초)을 정의합니다. 이 타이머(이전 이름: 전달 지연)는 동적 라우팅(BGP)을 사용하는 NSX Edge에서 논리적 라우터의 활성-활성 또는 활성-대기 구성에 대한 페일오버가 발생할 경우 다운타임을 최소화합니다. 외부 라우터(TOR)가 첫 번째 BGP/BFD 세션 이후에 이 라우터에 대한 모든 경로를 보급하는데 소요되는 시간(초)으로 설정해야 합니다. 이 타이머 값은 라우터가 학습해야 하는 노스바운드 동적 경로 수에 직접 비례해야 합니다. 이 타이머는 단일 Edge 노드 설정에서 0으로 설정되어야 합니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 Tier-0 논리적 라우터를 선택합니다.
- 4 **라우팅 > 글로벌 구성**을 선택합니다.
- 5 **편집**을 클릭합니다.
- 6 전달 타이머 값을 입력합니다.
- 7 **저장**을 클릭합니다.

# 네트워크 주소 변환

## 6

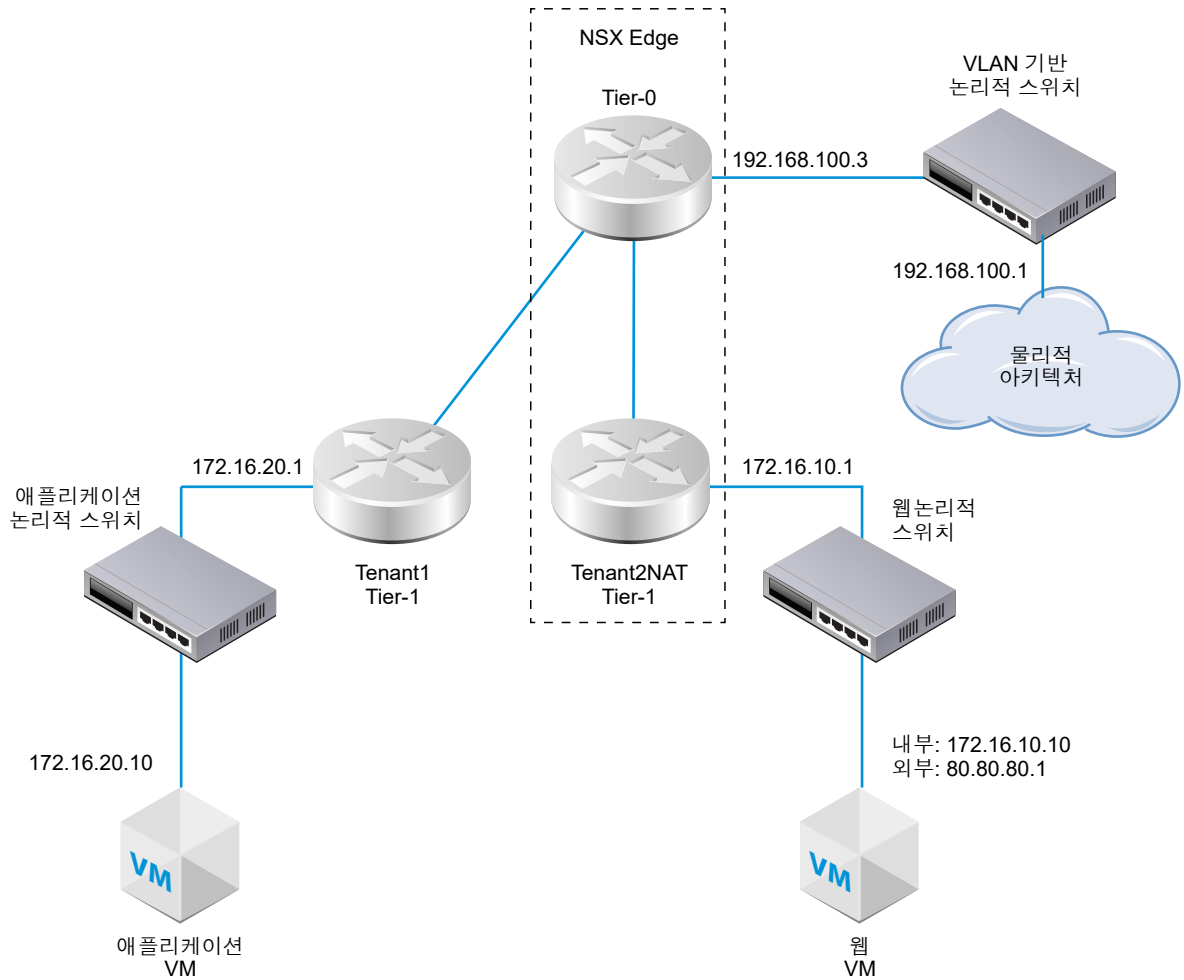
NSX-T Data Center의 NAT(네트워크 주소 변환)를 Tier-0 및 Tier-1 논리적 라우터에서 구성할 수 있습니다.

예를 들어 다음 다이어그램은 Tenant2NAT에 구성된 NAT가 있는 2개의 Tier-1 논리적 라우터를 보여줍니다. 웹 VM은 간편하게 IP 주소로 172.16.10.10을 사용하고, 기본 게이트웨이로 172.16.10.1을 사용하도록 구성되어 있습니다.

NAT는 Tier-0 논리적 라우터에 대한 연결에서 Tenant2NAT 논리적 라우터의 업링크에 적용됩니다.

NAT 구성을 사용하도록 설정하려면 Tenant2NAT의 서비스 구성 요소가 NSX Edge 클러스터에 있어야 합니다. 따라서 Tenant2NAT는 NSX Edge 내부에 표시됩니다. 비교를 위해 Tenant1을 NSX Edge 외부에 배치할 수 있습니다. 이 테넌트는 Edge 서비스를 사용하지 않기 때문입니다.

그림 6-1. NAT 토폴로지



본 장은 다음 항목을 포함합니다.

- Tier-1 NAT
- Tier-0 NAT
- 채워 NAT

## Tier-1 NAT

Tier-1 논리적 라우터는 소스 NAT 및 대상 NAT를 지원합니다.

### Tier-1 라우터에서 소스 NAT 구성

SNAT(소스 NAT)는 패킷의 IP 헤더에서 소스 주소를 변경합니다. 또한 TCP/UDP 헤더에서 소스 포트를 변경할 수도 있습니다. 일반적인 용도는 네트워크를 나가는 패킷에 대해 개인(rfc1918) 주소/포트를 공용 주소/포트로 변경하는 것입니다.

소스 NAT를 사용하거나 사용하지 않도록 설정하는 규칙을 생성할 수 있습니다.



이 예에서는 웹 VM에서 패킷이 수신될 때 Tenant2NAT Tier-1 라우터는 패킷의 소스 IP 주소를 172.16.10.10에서 80.80.80.1로 변경합니다. 공용 소스 IP 주소를 사용하면 개인 네트워크 외부의 대상이 원래 소스에 다시 라우팅되도록 할 수 있습니다.

### 사전 요구 사항

- Tier-0 라우터에는 VLAN 기반 논리적 스위치에 연결된 1개의 업링크가 있어야 합니다. [NSX Edge 업링크를 위해 VLAN 논리적 스위치에 Tier-0 논리적 라우터 연결](#)의 내용을 참조하십시오.
- Tier-0 라우터는 물리적 아키텍처에 대한 업링크에 라우팅(정적 또는 BGP) 및 경로 재배포가 구성되어 있어야 합니다. [정적 경로 구성](#), [Tier-0 논리적 라우터에서 BGP 구성](#) 및 [Tier-0 논리적 라우터에서 경로 재배포 사용](#)을 참조하십시오.
- Tier-1 라우터 각각에는 Tier-0 라우터에 대한 업링크가 구성되어 있어야 합니다. Tenant2NAT는 NSX Edge 클러스터에서 지원해야 합니다. [Tier-0과 Tier-1 연결](#)의 내용을 참조하십시오.
- Tier-1 라우터에는 다운링크 포트 및 경로 보급이 구성되어 있어야 합니다. [Tier-1 논리적 라우터에서 다운링크 포트 추가](#) 및 [Tier-1 논리적 라우터에서 경로 보급 구성](#)을 참조하십시오.
- VM은 올바른 논리적 스위치에 연결되어야 합니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 NAT를 구성하려는 Tier-1 논리적 라우터를 클릭합니다.
- 4 **서비스 > NAT**를 선택합니다.
- 5 **추가**를 클릭합니다.
- 6 우선 순위 값을 지정합니다.  
값이 낮을수록 이 규칙의 우선 순위가 높다는 것을 의미합니다.
- 7 **작업**에 대해 소스 NAT를 사용하도록 설정하려면 **SNAT**를 선택하고 소스 NAT를 사용하지 않도록 설정하려면 **NO\_SNAT**를 선택합니다.
- 8 프로토콜 유형을 선택합니다.  
기본적으로 **임의 프로토콜**이 선택됩니다.
- 9 (선택 사항) **소스 IP**에 대해 IP 주소 또는 CIDR 형식의 IP 주소 범위를 지정합니다.  
이 필드를 비워 두면 라우터의 다운링크 포트의 모든 소스가 변환됩니다. 이 예에서 소스 IP 주소는 172.16.10.10입니다.
- 10 (선택 사항) **대상 IP**에 대해 IP 주소 또는 CIDR 형식의 IP 주소 범위를 지정합니다.  
이 필드를 비워 두면 로컬 서브넷 외부의 모든 대상에 NAT가 적용됩니다.
- 11 작업이 **SNAT**인 경우 **변환된 IP**에 대해 IP 주소 또는 CIDR 형식의 IP 주소 범위를 지정합니다.  
이 예에서 변환된 IP 주소는 80.80.80.1입니다.

**12** (선택 사항) **적용 대상**에 대해 라우터 포트를 선택합니다.

**13** (선택 사항) 규칙의 상태를 설정합니다.

이 규칙은 기본적으로 사용하도록 설정됩니다.

**14** (선택 사항) 로깅 상태를 변경합니다.

로깅은 기본적으로 사용하지 않도록 설정됩니다.

**15** (선택 사항) 방화벽 우회 설정을 변경합니다.

이 설정은 기본적으로 사용하도록 설정됩니다.

## 결과

새 규칙은 [NAT] 아래에 표시됩니다. 예:

Tenant2NAT

개요 구성 라우팅 서비스

NAT 새로 고침

수집된 통계가 없습니다.

+ 추가 편집 삭제

ID	작업	일치				변환됨		적용 대상	통계
		프로토콜	소스 IP	소스 포트	대상 IP	대상 포트	IP		
우선 순위: 1024									
1033	SNAT	임의	172.16.10.10	임의	임의	임의	80.80.80.1	임의	

## 다음에 수행할 작업

Tier-1 라우터가 NAT 경로를 보급하도록 구성합니다.

Tier-0 라우터에서 물리적 아키텍처로의 NAT 경로 업스트림을 보급하려면 Tier-0 라우터가 Tier-1 NAT 경로를 보급하도록 구성합니다.

## Tier-1 라우터에서 대상 NAT 구성

대상 NAT는 패킷의 IP 헤더에서 대상 주소를 변경합니다. 또한 TCP/UDP 헤더에서 대상 포트를 변경할 수도 있습니다. 이 기능의 일반적인 용도는 대상으로 공용 주소/포트를 갖는 수신 패킷을 네트워크 내부의 개인 IP 주소/포트로 리디렉션하는 것입니다.

대상 NAT를 사용하거나 사용하지 않도록 설정하는 규칙을 생성할 수 있습니다.

이 예에서는 애플리케이션 VM에서 패킷이 수신될 때 Tenant2NAT Tier-1 라우터가 패킷의 대상 IP 주소를 172.16.10.10에서 80.80.80.1로 변경합니다. 공용 대상 IP 주소를 사용하면 개인 네트워크 외부로부터 개인 네트워크 내의 대상으로 연결할 수 있습니다.

## 사전 요구 사항

- Tier-0 라우터에는 VLAN 기반 논리적 스위치에 연결된 1개의 업링크가 있어야 합니다. [NSX Edge 업링크를 위해 VLAN 논리적 스위치에 Tier-0 논리적 라우터 연결](#)의 내용을 참조하십시오.

- Tier-0 라우터는 물리적 아키텍처에 대한 업링크에 라우팅(정적 또는 BGP) 및 경로 재배포가 구성되어 있어야 합니다. [정적 경로 구성](#), [Tier-0 논리적 라우터에서 BGP 구성](#) 및 [Tier-0 논리적 라우터에서 경로 재배포 사용](#)을 참조하십시오.
- Tier-1 라우터 각각에는 Tier-0 라우터에 대한 업링크가 구성되어 있어야 합니다. Tenant2NAT는 NSX Edge 클러스터에서 지원해야 합니다. [Tier-0과 Tier-1 연결](#)의 내용을 참조하십시오.
- Tier-1 라우터에는 다운링크 포트 및 경로 보급이 구성되어 있어야 합니다. [Tier-1 논리적 라우터에서 다운링크 포트 추가](#) 및 [Tier-1 논리적 라우터에서 경로 보급 구성](#)을 참조하십시오.
- VM은 올바른 논리적 스위치에 연결되어야 합니다.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 NAT를 구성하려는 Tier-1 논리적 라우터를 클릭합니다.
- 4 **서비스 > NAT**를 선택합니다.
- 5 **추가**를 클릭합니다.
- 6 우선 순위 값을 지정합니다.  
값이 낮을수록 이 규칙의 우선 순위가 높다는 것을 의미합니다.
- 7 **작업**에 대해 대상 NAT를 사용하도록 설정하려면 **DNAT**를 선택하고 대상 NAT를 사용하지 않도록 설정하려면 **NO\_DNAT**를 선택합니다.
- 8 프로토콜 유형을 선택합니다.  
기본적으로 **임의 프로토콜**이 선택됩니다.
- 9 (선택 사항) **소스 IP**에 대해 IP 주소 또는 CIDR 형식의 IP 주소 범위를 지정합니다.  
[소스 IP]를 비워 두면 NAT가 로컬 서브넷 외부의 모든 소스에 적용됩니다.
- 10 **대상 IP**에 대해 IP 주소 또는 CIDR 형식의 IP 주소 범위를 지정합니다.  
이 예에서 대상 IP 주소는 80.80.80.1입니다.
- 11 작업이 **DNAT**인 경우 **변환된 IP**에 대해 IP 주소 또는 CIDR 형식의 IP 주소 범위를 지정합니다.  
이 예에서 내부/변환된 IP 주소는 172.16.10.10입니다.
- 12 (선택 사항) 작업이 **DNAT**인 경우 **변환된 포트**에 대해 변환된 포트를 지정합니다.
- 13 (선택 사항) **적용 대상**에 대해 라우터 포트를 선택합니다.
- 14 (선택 사항) 규칙의 상태를 설정합니다.  
이 규칙은 기본적으로 사용하도록 설정됩니다.
- 15 (선택 사항) 로깅 상태를 변경합니다.  
로깅은 기본적으로 사용하지 않도록 설정됩니다.

**16** (선택 사항) 방화벽 우회 설정을 변경합니다.

이 설정은 기본적으로 사용하도록 설정됩니다.

## 결과

새 규칙은 [NAT] 아래에 표시됩니다. 예:

Tenant2NAT

개요 구성 라우팅 서비스

NAT 새로 고침

수집된 통계가 없습니다.

+ 추가 편집 삭제

ID	작업	일치					변환됨		적용 대상	통계
		프로토콜	소스 IP	소스 포트	대상 IP	대상 포트	IP	포트		
우선 순위: 1024										
1034	DNAT	임의	임의	임의	80.80.80.1	임의	172.16.10.10	임의		

## 다음에 수행할 작업

Tier-1 라우터가 NAT 경로를 보급하도록 구성합니다.

Tier-0 라우터에서 물리적 아키텍처로의 NAT 경로 업스트림을 보급하려면 Tier-0 라우터가 Tier-1 NAT 경로를 보급하도록 구성합니다.

## 업스트림 Tier-0 라우터로 Tier-1 NAT 경로 보급

Tier-1 NAT 경로를 보급하면 업스트림 Tier-0 라우터가 이러한 경로를 학습할 수 있습니다.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 NAT가 구성된 Tier-1 논리적 라우터를 클릭합니다.
- 4 Tier-1 라우터에서 **라우팅 > 경로 보급**을 선택합니다.
- 5 경로 보급 규칙을 편집하여 NAT 경로 보급을 사용하도록 설정합니다.

## 결과

Tenant2NAT	
개요	구성 ▾ 라우팅 ▾ 서비스 ▾
<b>경로 보급</b>   편집	
상태	● 사용
모든 NSX 연결 경로 보급	● 예
모든 NAT 경로 보급	● 예
모든 정적 경로 보급	● 아니요
모든 LB VIP 경로 보급	● 아니요
모든 LB SNAT IP 경로 보급	● 아니요
보급된 네트워크	5 네트워크

다음에 수행할 작업

Tier-0 라우터에서 온 Tier-1 NAT 경로를 업스트림 물리적 아키텍처로 보급합니다.

## Tier-1 NAT 경로를 물리적 아키텍처로 보급

Tier-0 라우터에서 온 Tier-1 NAT 경로를 보급하면 업스트림 물리적 아키텍처가 이러한 경로를 학습할 수 있습니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 **라우팅**을 선택합니다.
- 3 NAT가 구성된 Tier-1 라우터에 연결된 Tier-0 논리적 라우터를 클릭합니다.
- 4 Tier-0 라우터에서 **라우팅 > 경로 재배포**를 선택합니다.
- 5 경로 보급 규칙을 편집하여 Tier-1 NAT 경로 보급을 사용하도록 설정합니다.

## 결과

## 재배포 조건 편집 - rule1



이름 \*

rule1

설명

Rule

소스 \*

☐ 정적☒ Tier-1 NAT☒ NSX 연결됨☐ Tier-1 LB VIP☒ NSX 정적☐ Tier-1 LB SNAT☐ Tier-0 NAT

경로 맵



취소

저장

다음에 수행할 작업

NAT가 예상대로 작동되는지 확인합니다.

## Tier-1 NAT 확인

SNAT 및 DNAT 규칙이 제대로 작동하는지 확인합니다.

## 절차

- 1 NSX Edge에 로그인합니다.
- 2 `get logical-routers`를 실행하여 Tier-0 서비스 라우터에 대한 VRF 번호를 확인합니다.
- 3 `vrf <number>` 명령을 실행하여 Tier-0 서비스 라우터 컨텍스트를 시작합니다.
- 4 `get route` 명령을 실행하고 Tier-1 NAT 주소가 표시되는지 확인합니다.

```
nsx-edge(tier0_sr)> get route
```

```
Flags: c - connected, s - static, b - BGP, ns - nsx_static
```

```
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

Total number of routes: 8

t1n 80.80.80.1/32      [3/3]      via 169.0.0.1
...
```

- 5 웹 VM이 [웹] 페이지를 제공하도록 설정된 경우 <http://80.80.80.1>에서 [웹] 페이지를 열 수 있습니다.
- 6 물리적 아키텍처에 있는 Tier-0 라우터의 업스트림 인접 네트워크가 80.80.80.1을 ping할 수 있는지 확인합니다.
- 7 Ping이 여전히 실행 중인 경우 DNAT 규칙의 통계 열을 확인합니다.  
활성 세션이 하나만 있어야 합니다.

## Tier-0 NAT

Tier-0 논리적 라우터는 소스 NAT, 대상 NAT 및 재귀 NAT를 지원합니다.

### Tier-0 라우터에서 소스 및 대상 NAT 구성

활성-대기 모드에서 실행 중인 Tier-0 라우터에서 소스 및 대상 NAT를 구성할 수 있습니다.

IP 주소 또는 주소 범위에 대해 NAT를 사용하지 않도록 설정하도록 NAT 없음, NO\_SNAT 또는 NO\_DNAT를 구성할 수도 있습니다. 여러 NAT 규칙이 주소에 적용되는 경우 우선 순위가 가장 높은 규칙이 적용됩니다.

#### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 Tier-0 논리적 라우터를 클릭합니다.
- 4 **서비스 > NAT**를 선택합니다.
- 5 **추가**를 클릭하여 NAT 규칙을 추가합니다.
- 6 우선 순위 값을 지정합니다.  
값이 낮을수록 우선 순위가 더 높습니다.
- 7 작업의 경우 **SNAT**, **DNAT**, **NAT 없음**, **NO\_SNAT** 또는 **NO\_DNAT**를 선택합니다.
- 8 프로토콜 유형을 선택합니다.  
기본적으로 **임의 프로토콜**이 선택됩니다.
- 9 (필수 사항) **소스 IP**에 대해 IP 주소 또는 CIDR 형식의 IP 주소 범위를 지정합니다.  
이 필드를 비워 두면 로컬 서브넷 외부의 모든 소스에 이 NAT 규칙이 적용됩니다.

**10 대상 IP**에 대해 IP 주소 또는 CIDR 형식의 IP 주소 범위를 지정합니다.

**11 변환된 IP**에 대해 IP 주소 또는 CIDR 형식의 IP 주소 범위를 지정합니다.

**12 (선택 사항) 작업이 DNAT인 경우 변환된 포트**에 대해 변환된 포트를 지정합니다.

**13 (선택 사항) 적용 대상**에 대해 라우터 포트를 선택합니다.

**14 (선택 사항) 규칙의 상태를 설정**합니다.

이 규칙은 기본적으로 사용하도록 설정됩니다.

**15 (선택 사항) 로깅 상태를 변경**합니다.

로깅은 기본적으로 사용하지 않도록 설정됩니다.

**16 (선택 사항) 방화벽 우회 설정을 변경**합니다.

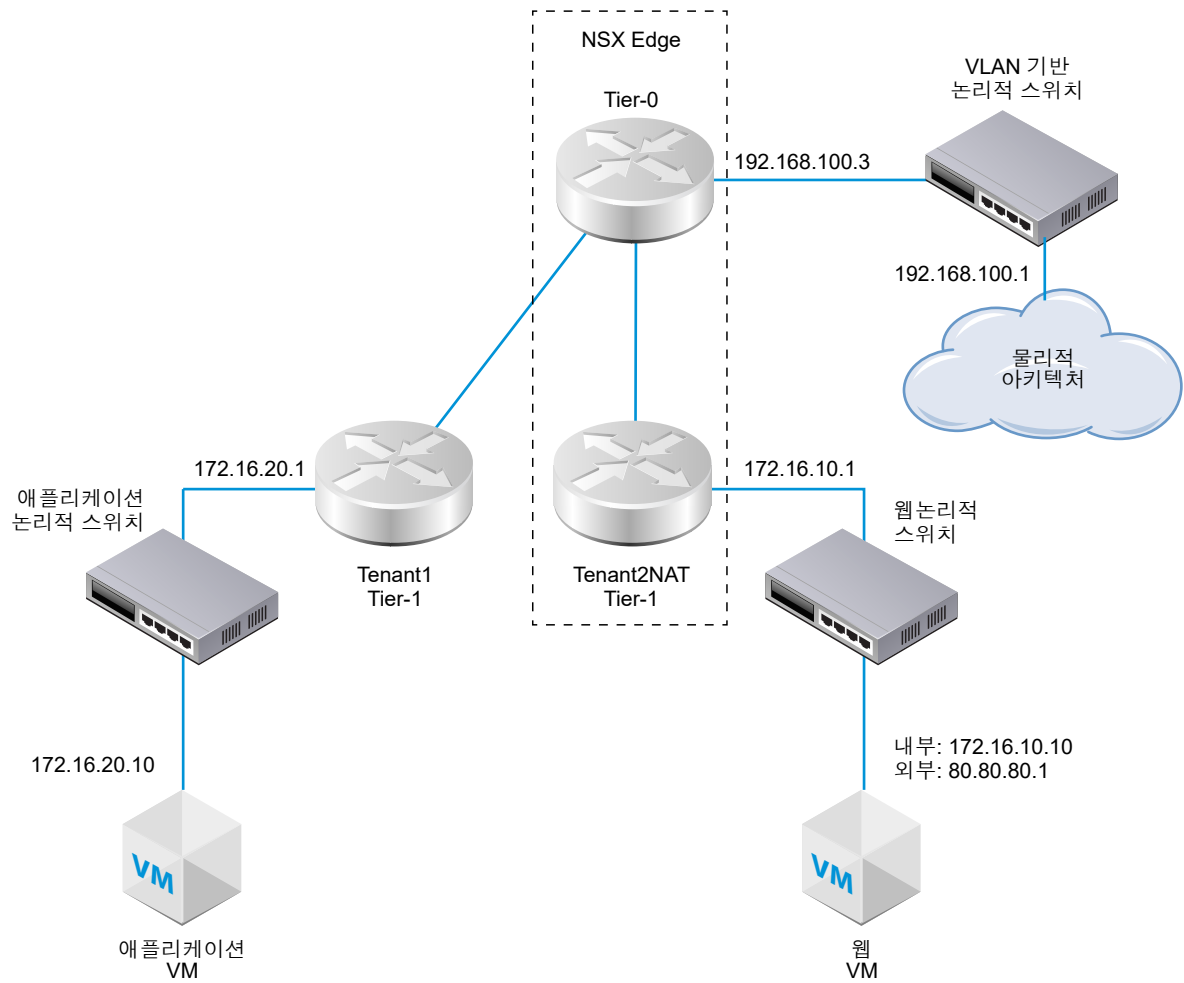
이 설정은 기본적으로 사용하도록 설정됩니다.

## 재귀 NAT

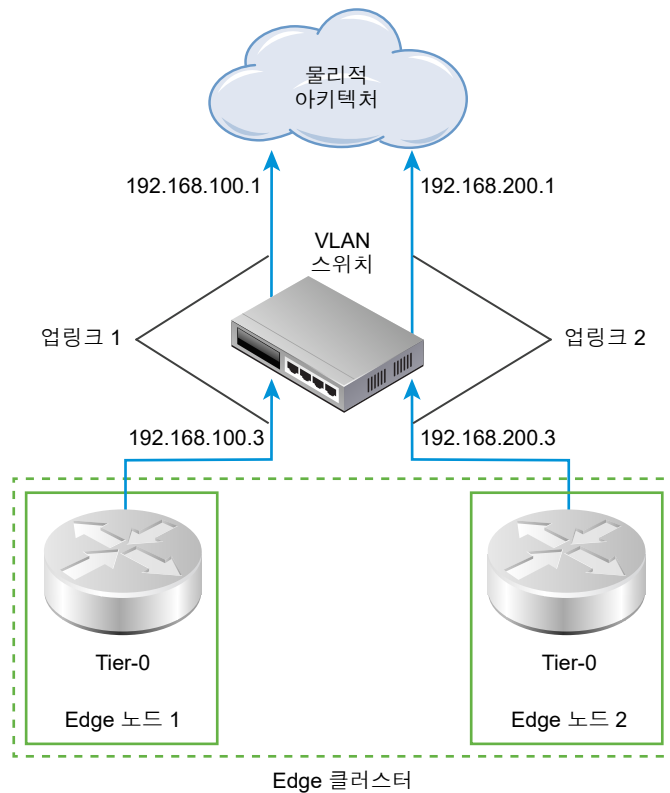
Tier-0 또는 Tier-1 논리적 라우터가 활성-활성 모드에서 실행될 때 비대칭 경로가 문제를 유발할 수 있는 상태 저장 NAT를 구성할 수 없습니다. 활성-활성 라우터의 경우 재귀 NAT(경우에 따라 상태 비저장 NAT라고도 함)를 사용할 수 있습니다.

이 예에서는 웹 VM에서 패킷이 수신될 때 Tenant2NAT Tier-1 라우터는 패킷의 소스 IP 주소를 172.16.10.10에서 80.80.80.1로 변경합니다. 공용 소스 IP 주소를 사용하면 개인 네트워크 외부의 대상이 원래 소스에 다시 라우팅되도록 할 수 있습니다.





여기에 표시된 것처럼 2개의 활성-활성 Tier-0 라우터가 사용될 경우 재귀 NAT를 구성해야 합니다.



## Tier-0 또는 Tier-1 논리적 라우터에서 재귀 NAT 구성

Tier-0 또는 Tier-1 논리적 라우터가 활성-활성 모드에서 실행될 때 비대칭 경로가 문제를 유발할 수 있는 상태 저장 NAT를 구성할 수 없습니다. 활성-활성 라우터의 경우 재귀 NAT(경우에 따라 상태 비저장 NAT라고도 함)를 사용할 수 있습니다.

재귀 NAT에 대해 변환할 단일 소스 주소 또는 주소 범위를 구성할 수 있습니다. 소스 주소의 범위를 구성하는 경우 변환된 주소의 범위도 구성해야 합니다. 두 가지 범위의 크기는 동일해야 합니다. 주소 변환은 결정되어 있습니다. 즉, 소스 주소 범위의 첫 번째 주소는 변환된 주소 범위의 첫 번째 주소로 변환되고, 소스 범위의 두 번째 주소는 변환된 범위의 두 번째 주소로 변환됩니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 재귀 NAT를 구성하려는 Tier-0 또는 Tier-1 논리적 라우터를 클릭합니다.
- 4 **서비스 > NAT**를 선택합니다.
- 5 **추가**를 클릭합니다.
- 6 우선 순위 값을 지정합니다.

값이 낮을수록 이 규칙의 우선 순위가 높다는 것을 의미합니다.

7 작업에 대해 **재귀**를 선택합니다.

8 **소스 IP**에 대해 IP 주소 또는 CIDR 형식의 IP 주소 범위를 지정합니다.

9 **변환된 IP**에 대해 IP 주소 또는 CIDR 형식의 IP 주소 범위를 지정합니다.

10 (선택 사항) 규칙의 상태를 설정합니다.

이 규칙은 기본적으로 사용하도록 설정됩니다.

11 (선택 사항) 로깅 상태를 변경합니다.

로깅은 기본적으로 사용하지 않도록 설정됩니다.

12 (선택 사항) 방화벽 우회 설정을 변경합니다.

이 설정은 기본적으로 사용하도록 설정됩니다.

## 결과

새 규칙은 [NAT] 아래에 표시됩니다. 예:

Tier0-LR-1 ✕

개요 구성 라우팅 서비스

NAT | 새로 고침

총 규칙 통계 | 마지막 업데이트 날짜: 2019년 3월 6일 오후 6:21:12

☒ 액티브 세션    ☐ 패킷 수    ☐ 바이트 데이터

[+ 추가](#)   [✎ 편집](#)   [🗑 삭제](#)

ID	작업	일치					변환됨		적용 대상	통계
		프로토콜	소스 IP	소스 포트	대상 IP	대상 포트	IP	포트		
▼ 우선 순위: 1024										
✓ 2048	재귀	임의	80.80.80.1	임의	임의	임의	172.16.10.10	임의		

# 방화벽 섹션 및 방화벽 규칙

## 7

방화벽 섹션은 방화벽 규칙의 집합을 그룹화하는 데 사용됩니다.

방화벽 섹션은 하나 이상의 개별 방화벽 규칙으로 구성됩니다. 각 개별 방화벽 규칙에는 패킷이 허용 또는 차단되는지와 어떤 프로토콜 및 포트가 사용되도록 허용되는지 등을 결정하는 지점이 포함되어 있습니다. 판매 및 엔지니어링 부서에 대한 특정 규칙이 별도의 섹션에 있는 경우처럼, 섹션은 다중 테넌 시에 사용됩니다.

섹션은 상태 저장 또는 상태 비저장 규칙 적용으로 정의할 수 있습니다. 상태 비저장 규칙은 기존의 상태 비저장 ACL로 취급됩니다. 상태 비저장 섹션에 대해서는 재귀 ACL이 지원되지 않습니다. 단일 논리적 스위치 포트에 상태 비저장 및 상태 저장 규칙이 혼합되어 있는 것은 권장되지 않으며 정의되지 않은 동작을 야기할 수 있습니다.

규칙을 섹션 내에서 위아래로 이동할 수 있습니다. 방화벽을 통과하려는 모든 트래픽의 경우 패킷 정보는 규칙이 섹션에 표시된 순서에 따라(맨 위에서 시작하여 맨 아래의 기본 규칙으로 내려감) 달라집니다. 패킷과 일치하는 첫 번째 규칙이 있으면 구성된 작업이 적용되고, 규칙의 구성된 옵션에 지정된 모든 처리가 수행되며, 후속 규칙은 모두 무시됩니다(후속 규칙이 더 잘 일치되더라도 무시됨). 따라서 구체적인 규칙을 더 일반적인 규칙보다 상위에 배치하여 해당 규칙이 무시되지 않도록 해야 합니다. 규칙 테이블의 맨 밑에 있는 기본 규칙은 "포괄적인" 규칙으로, 다른 규칙에 해당되지 않는 패킷은 기본 규칙에 의해 적용됩니다.

---

**참고** 논리적 스위치에는 N-VDS 모드라는 속성이 있습니다. 이 속성은 스위치가 속한 전송 영역에서 가져옵니다. N-VDS 모드가 ENS(다른 이름: Enhanced Datapath)인 경우에는 Source, Destination 또는 Applied To 필드에 스위치 또는 포트가 있는 방화벽 규칙 또는 섹션을 생성할 수 없습니다.

---

본 장은 다음 항목을 포함합니다.

- 방화벽 규칙 섹션 추가
- 방화벽 규칙 섹션 삭제
- 섹션 규칙 사용 및 사용 안 함
- 섹션 로그 사용 및 사용 안 함
- 방화벽 규칙 정보
- 방화벽 규칙 추가
- 방화벽 규칙 삭제

- 기본 분산 방화벽 규칙 편집
- 방화벽 규칙 순서 변경
- 방화벽 규칙 필터링
- 논리 스위치 브리지 포트에 대한 방화벽 구성
- 방화벽 제외 목록 구성
- 방화벽 사용 및 사용 안 함
- 논리적 라우터에 방화벽 규칙 추가 또는 삭제

## 방화벽 규칙 섹션 추가

방화벽 규칙 섹션은 독립적으로 편집 및 저장되며 별도의 방화벽 구성을 테넌트에 적용시키는 데 사용됩니다.

### 절차

- 1 탐색 패널에서 **보안 > 분산 방화벽**을 선택합니다.
- 2 계층 3(L3) 규칙에 대해 **일반** 탭을 클릭하거나 계층 2(L2) 규칙에 대해 **이더넷** 탭을 클릭합니다.
- 3 기존 섹션이나 규칙을 클릭합니다.
- 4 메뉴 모음에서 섹션 아이콘을 클릭하고 **위에 섹션 추가** 또는 **아래에 섹션 추가**를 선택합니다.

---

**참고** 방화벽을 통과하려는 모든 트래픽의 경우 패킷 정보는 규칙이 [규칙] 테이블에 표시된 순서에 따라(맨 위에서 시작하여 맨 아래의 기본 규칙으로 내려감) 달라집니다. 일부 경우 두 개 이상의 규칙 우선 순위는 패킷의 배치를 결정하는 데 중요할 수 있습니다.

---

- 5 섹션 이름을 입력합니다.
- 6 방화벽에 상태 비저장을 사용하려면 **상태 비저장 방화벽 사용**을 선택합니다. 이 옵션은 L3에만 적용됩니다.

상태 비저장 방화벽은 네트워크 트래픽을 관찰하며 소스 및 대상 주소 또는 기타 정적 값에 따라 패킷을 제한하거나 차단합니다. 상태 저장 방화벽은 트래픽 스트림을 처음부터 끝까지 관찰할 수 있습니다. 상태 비저장 방화벽은 트래픽 부하가 심한 경우에 일반적으로 더 빠르고 성능이 더 좋습니다. 상태 저장 방화벽은 승인되지 않았으며 위조된 통신을 더 잘 식별합니다. 한 번 정의된 이후에는 상태 저장과 상태 비저장 간에 전환할 수 없습니다.

- 7 섹션을 적용할 개체를 하나 이상 선택합니다.

개체 유형은 논리적 포트, 논리적 스위치 및 NSGroup입니다. NSGroup을 선택할 경우, 개체에 논리적 스위치나 논리적 포트가 하나 이상 포함되어 있어야 합니다. NSGroup에 IP 집합 또는 MAC 집합만 포함되어 있으면 해당 개체는 무시됩니다.

---

**참고** 섹션의 **적용 대상**은 해당 섹션에 있는 규칙의 모든 **적용 대상** 설정을 재정의합니다.

---

- 8 **확인**을 클릭합니다.

다음에 수행할 작업

섹션에 방화벽 규칙을 추가합니다.

## 방화벽 규칙 섹션 삭제

방화벽 규칙 섹션은 더 이상 사용되지 않을 때 삭제할 수 있습니다.

방화벽 규칙 섹션을 삭제하면 해당 섹션의 모든 규칙이 삭제됩니다. 섹션을 삭제한 후 방화벽 테이블의 다른 위치에 다시 추가할 수는 없습니다. 이렇게 하려면 섹션을 삭제하고 구성을 게시해야 합니다. 그런 다음 삭제한 섹션을 방화벽 테이블에 추가하고 구성을 다시 게시하면 됩니다.

절차

- 1 탐색 패널에서 **보안 > 분산 방화벽**을 선택합니다.
- 2 L3 규칙에 대해 **일반** 탭을 클릭하거나 L2 규칙에 대해 **이더넷** 탭을 클릭합니다.
- 3 섹션의 첫 번째 열에 있는 메뉴 아이콘을 클릭하고 **섹션 삭제**를 선택합니다.

섹션을 선택하고 메뉴 모음에서 삭제 아이콘을 클릭할 수도 있습니다.

## 섹션 규칙 사용 및 사용 안 함

방화벽 규칙 섹션의 모든 규칙을 사용하거나 사용하지 않도록 설정할 수 있습니다.

절차

- 1 탐색 패널에서 **보안 > 분산 방화벽**을 선택합니다.
- 2 L3 규칙에 대해 **일반** 탭을 클릭하거나 L2 규칙에 대해 **이더넷** 탭을 클릭합니다.
- 3 섹션의 첫 번째 열에 있는 메뉴 아이콘을 클릭하고 **모든 규칙 사용** 또는 **모든 규칙 사용 안 함**을 선택합니다.
- 4 **게시**를 클릭합니다.

## 섹션 로그 사용 및 사용 안 함

섹션 규칙에 대한 로그를 사용하도록 설정하면 섹션의 모든 규칙에 대해 패킷의 정보가 기록됩니다. 섹션의 규칙 수에 따라 일반적인 방화벽 섹션은 대량의 로그 정보를 생성하고 성능에 영향을 미칠 수 있습니다.

로그는 vSphere ESXi 및 KVM 호스트의 /var/log/dfwpgtlogs.log 파일에 저장됩니다.

절차

- 1 탐색 패널에서 **보안 > 분산 방화벽**을 선택합니다.
- 2 L3 규칙에 대해 **일반** 탭을 클릭하거나 L2 규칙에 대해 **이더넷** 탭을 클릭합니다.
- 3 섹션의 첫 번째 열에 있는 메뉴 아이콘을 클릭하고 **로그 사용** 또는 **로그 사용 안 함**을 선택합니다.

#### 4 계시를 클릭합니다.

## 방화벽 규칙 정보

NSX-T Data Center는 방화벽 규칙을 사용하여 네트워크 내부 및 외부에서의 트래픽 처리를 지정합니다.

방화벽은 구성 가능한 규칙의 집합인 계층 3 규칙(일반 탭)과 계층 2 규칙(이더넷 탭)을 제공합니다. 계층 2 방화벽 규칙이 계층 3 규칙보다 먼저 처리됩니다. 방화벽 적용에서 제외할 논리적 스위치, 논리적 포트 또는 그룹이 포함된 제외 목록을 구성할 수 있습니다.

방화벽 규칙은 다음과 같이 적용됩니다.

- 규칙은 위에서 아래로 처리됩니다.
- 각 패킷은 규칙 테이블의 맨 위에 있는 규칙에 대하여 확인된 후 테이블의 다음 규칙 순서에 따라 확인됩니다.
- 테이블에서 트래픽 매개 변수와 일치하는 첫 번째 규칙이 적용됩니다.

그러면 해당 패킷에 대한 검색이 종료되므로 그다음 규칙은 적용할 수 없습니다. 이러한 동작 때문에 항상 가장 세분화된 정책을 규칙 테이블의 맨 위에 배치하도록 권장됩니다. 이를 통해 이러한 규칙이 특정 규칙보다 우선하여 적용되도록 할 수 있습니다.

규칙 테이블의 맨 밑에 있는 기본 규칙은 포괄적인 규칙으로, 다른 규칙에 해당되지 않는 패킷은 기본 규칙에 의해 적용됩니다. 호스트 준비 작업 이후 기본 규칙은 작업을 허용하도록 설정됩니다. 이를 통해 스테이징 또는 마이그레이션 단계 동안 VM 간의 통신이 끊어지지 않습니다. 그런 다음 이 기본 규칙을 변경하여 작업을 차단하고 포지티브 제어 모델을 통한 액세스 제어를 적용하도록(예: 방화벽 규칙에 정의된 트래픽만 네트워크로 허용함) 하는 것이 가장 좋습니다.

**참고** TCP 프로토콜의 경우 상태 저장 규칙에 대해 TCP 엄격 검사가 자동으로 사용됩니다. 즉, SYN 패킷을 사용하여 네트워크 연결을 시작한 경우에만 패킷이 TCP 규칙에 대해 일치 여부가 확인됩니다.

표 7-1. 방화벽 규칙의 속성

속성	설명
이름	방화벽 규칙 이름입니다.
ID	각 규칙에 대해 생성된 고유 시스템 ID입니다.
소스	규칙의 소스는 IP나 MAC 주소 또는 IP 주소가 아닌 다른 개체가 될 수 있습니다. 소스가 정의되지 않은 경우 임의로 일치하는 항목을 찾습니다. IPv6은 소스나 대상 범위에 대해 지원되지 않습니다.
대상	규칙에 영향을 받는 연결의 대상 IP 또는 MAC 주소/넷마스크입니다. 대상이 정의되지 않은 경우 임의로 일치하는 항목을 찾습니다. IPv6은 소스나 대상 범위에 대해 지원되지 않습니다.
서비스	서비스는 L3에 대해 미리 정의된 포트 프로토콜 조합일 수 있습니다. L2의 경우 이더넷 유형일 수 있습니다. L2 및 L3의 경우 새로운 서비스 또는 서비스 그룹을 수동으로 정의할 수 있습니다. 서비스가 정의되지 않은 경우 임의로 일치하는 항목을 찾습니다.
적용 대상	이 규칙이 적용되는 범위를 정의합니다. 정의되지 않은 경우 범위는 모든 논리적 포트입니다. 섹션에 [적용 대상]을 추가한 경우 규칙이 덮어쓰입니다.
로그	로그는 끄거나 켤 수 있습니다. 로그는 ESX와 KVM 호스트의 /var/log/dfwptlogs.log 파일에 저장됩니다.

표 7-1. 방화벽 규칙의 속성 (계속)

속성	설명
작업	규칙이 적용하는 작업은 <b>허용</b> , <b>삭제</b> 또는 <b>거절</b> 입니다. 기본값은 <b>허용</b> 입니다.
IP 프로토콜	옵션은 <b>IPv4</b> , <b>IPv6</b> 및 <b>IPv4_IPv6</b> 입니다. 기본값은 <b>IPv4_IPv6</b> 입니다. 이 속성에 액세스하려면 <b>고급 설정</b> 아이콘을 클릭합니다.
방향	옵션은 <b>수신</b> , <b>송신</b> 및 <b>수신/송신</b> 입니다. 기본값은 <b>수신/송신</b> 입니다. 이 필드는 대상 개체의 관점에서 트래픽 방향을 나타냅니다. <b>수신</b> 은 개체로 들어오는 트래픽만 확인하고, <b>송신</b> 은 개체에서 나가는 트래픽만 확인하며, <b>수신/송신</b> 은 양쪽 방향 트래픽 모두 확인함을 의미합니다. 이 속성에 액세스하려면 <b>고급 설정</b> 아이콘을 클릭합니다.
규칙 태그	규칙에 추가된 태그입니다. 이 속성에 액세스하려면 <b>고급 설정</b> 아이콘을 클릭합니다.
흐름 통계	바이트, 패킷 수 및 세션을 표시하는 읽기 전용 필드입니다. 이 속성에 액세스하려면 그래프 아이콘을 클릭합니다.

**참고** SpoofGuard를 사용하지 않도록 설정하면 악의적인 가상 컴퓨터가 다른 가상 컴퓨터의 주소를 요청할 수 있기 때문에, 자동으로 검색된 주소 바인딩을 신뢰할 수 있는 것으로 보장할 수 없습니다. SpoofGuard를 사용하도록 설정하면 승인된 바인딩만 존재하도록 검색된 각 바인딩을 확인합니다.

## 방화벽 규칙 추가

방화벽은 미리 지정된 방화벽 규칙에 따라 들어오고 나가는 네트워크 트래픽을 모니터링하고 제어하는 네트워크 보안 시스템입니다.

방화벽 규칙은 NSX Manager 범위에서 추가됩니다. [적용 대상] 필드를 사용하면 규칙을 적용할 범위를 좁힐 수 있습니다. 각 규칙에 대해 소스 및 대상 수준에서 여러 개체를 추가할 수 있어 추가해야 할 총 방화벽 규칙 수가 줄어듭니다.

**참고** 기본적으로 규칙은 소스, 대상 및 서비스 규칙 요소의 기본값과 일치하는지 확인하며, 모든 인터페이스 및 트래픽 방향이 일치하는지 확인합니다. 규칙의 효과를 특정 인터페이스 또는 트래픽 방향으로 제한하려면 규칙에 제한을 지정해야 합니다.

### 사전 요구 사항

주소 그룹을 사용하려면 먼저 각 VM의 IP 및 MAC 주소를 해당 논리적 스위치에 수동으로 연결합니다.

### 절차

- 1 탐색 패널에서 **보안 > 분산 방화벽**을 선택합니다.
- 2 L3 규칙에 대해 **일반** 탭을 클릭하거나 L2 규칙에 대해 **이더넷** 탭을 클릭합니다.
- 3 기존 섹션이나 규칙을 클릭합니다.



- 4 규칙의 첫 번째 열에 있는 메뉴 아이콘을 클릭하고 **위에 규칙 추가** 또는 **아래에 규칙 추가**를 선택합니다.

방화벽 규칙을 정의할 수 있는 새로운 행이 나타납니다.

**참고** 방화벽을 통과하려는 모든 트래픽의 경우 패킷 정보는 규칙이 [규칙] 테이블에 표시된 순서에 따라(맨 위에서 시작하여 맨 아래의 기본 규칙으로 내려감) 달라집니다. 일부 경우 두 개 이상의 규칙 우선 순위는 패킷의 배치를 결정하는 데 중요할 수 있습니다.

- 5 이름 열에 규칙 이름을 입력합니다.

- 6 소스 열에서 편집 아이콘을 클릭하고 규칙의 소스를 선택합니다. 소스가 정의되지 않은 경우 임의로 일치하는 항목을 찾습니다.

옵션	설명
IP 주소	쉼표로 구분된 목록에 여러 IP 또는 MAC 주소를 입력합니다. 목록에는 최대 255자가 포함될 수 있습니다. IPv4 및 IPv6 형식이 둘 다 지원됩니다.
컨테이너 개체	사용 가능한 개체는 IP 집합, 논리적 포트, 논리적 스위치 및 NS 그룹입니다. 개체를 선택하고 <b>확인</b> 을 클릭합니다.

- 7 대상 열에서 편집 아이콘을 클릭하고 대상을 선택합니다. 대상이 정의되지 않은 경우 임의로 일치하는 항목을 찾습니다.

옵션	설명
IP 주소	쉼표로 구분된 목록에 IP 또는 MAC 주소를 여러 개 입력할 수 있습니다. 목록에는 최대 255자가 포함될 수 있습니다. IPv4 및 IPv6 형식이 둘 다 지원됩니다.
컨테이너 개체	사용 가능한 개체는 IP 집합, 논리적 포트, 논리적 스위치 및 NS 그룹입니다. 개체를 선택하고 <b>확인</b> 을 클릭합니다.

- 8 서비스 열에서 편집 아이콘을 클릭하고 서비스를 선택합니다. 서비스가 정의되지 않은 경우 임의로 일치하는 항목을 찾습니다.

- 9 미리 정의된 서비스를 선택하려면 하나 이상의 사용 가능한 서비스를 선택합니다.

- 10 새 서비스를 정의하려면 **원시 포트-프로토콜** 탭을 클릭하고 **추가**를 클릭합니다.

옵션	설명
서비스 유형	<ul style="list-style-type: none"> <li>■ ALG</li> <li>■ ICMP</li> <li>■ IGMP</li> <li>■ IP</li> <li>■ L4 포트 집합</li> </ul>
프로토콜	사용 가능한 프로토콜 중 하나를 선택합니다.
소스 포트	소스 포트를 입력합니다.
대상 포트	대상 포트를 선택합니다.

- 11 적용 대상 열에서 편집 아이콘을 클릭하고 개체를 선택합니다.

## 12 로그 열에서 로깅 옵션을 설정합니다.

로그는 ESXi 및 KVM 호스트의 /var/log/dfwpktlogs.log 파일에 있습니다. 로깅을 사용하도록 설정하면 성능에 영향을 줄 수 있습니다.

## 13 작업 열에서 작업을 선택합니다.

옵션	설명
허용	지정된 소스, 대상 및 프로토콜을 가진 모든 L3 또는 L2 트래픽이 현재 방화벽 컨텍스트를 통과하도록 허용합니다. 규칙과 일치하고 허용된 패킷은 방화벽이 존재하지 않을 때와 동일하게 시스템을 이동합니다.
삭제	지정된 소스, 대상 및 프로토콜을 가진 패킷을 삭제합니다. 패킷 삭제는 소스 또는 대상 시스템에 알림을 보내지 않는 작업입니다. 패킷을 삭제하면 재시도 임계값에 도달할 때까지 연결이 재시도됩니다.
거절	지정된 소스, 대상 및 프로토콜을 가진 패킷을 거절합니다. 패킷 거절은 보낸 사람에게 대상에 접속할 수 없다는 메시지를 보내는 패킷 거부 방식입니다. 프로토콜이 TCP인 경우 TCP RST 메시지가 전송됩니다. UDP, ICMP 및 기타 IP 연결에 대해 관리 목적으로 금지된 코드가 포함된 ICMP 메시지가 전송됩니다. [거절] 기능의 장점 중 하나는 단 한 차례의 시도에서 연결이 설정되지 않으면 전송 애플리케이션에 알림이 보내진다는 점입니다.

## 14 고급 설정 아이콘을 클릭하여 IP 프로토콜, 방향, 규칙 태그 및 주석을 지정합니다.

## 15 계시를 클릭합니다.

# 방화벽 규칙 삭제

방화벽은 미리 지정된 방화벽 규칙에 따라 들어오고 나가는 네트워크 트래픽을 모니터링하고 제어하는 네트워크 보안 시스템입니다. 사용자 정의된 규칙을 추가하고 삭제할 수 있습니다.

### 절차

- 1 탐색 패널에서 **보안 > 분산 방화벽**을 선택합니다.
- 2 L3 규칙에 대해 **일반** 탭을 클릭하거나 L2 규칙에 대해 **이더넷** 탭을 클릭합니다.
- 3 규칙의 첫 번째 열에 있는 메뉴 아이콘을 클릭하고 **규칙 삭제**를 선택합니다.
- 4 계시를 클릭합니다.

# 기본 분산 방화벽 규칙 편집

사용자 정의 방화벽 규칙과 일치하지 않는 트래픽에 적용되는 기본 방화벽 설정을 편집할 수 있습니다.

기본 방화벽 규칙은 사용자 정의 방화벽 규칙과 일치하지 않는 트래픽에 적용됩니다. 기본 계층 3 규칙은 **일반** 탭 아래에 있고, 기본 계층 2 규칙은 **이더넷** 탭 아래에 있습니다.

기본 방화벽 규칙은 모든 L3 및 L2 트래픽이 인프라의 모든 준비된 클러스터를 통과하도록 허용합니다. 기본 규칙은 항상 규칙 테이블의 맨 아래에 있으며 삭제할 수 없습니다. 하지만 규칙의 **작업** 요소를 **허용**에서 **삭제** 또는 **거절**로 변경하고(권장되지 않음) 해당 규칙에 대해 트래픽이 로깅되어야 하는지 여부를 지정할 수 있습니다.

기본 계층 3 방화벽 규칙은 DHCP를 포함한 모든 트래픽에 적용됩니다. **작업**을 **삭제**나 **거절**로 변경하면 DHCP 트래픽이 차단됩니다. DHCP 트래픽을 허용하는 규칙을 만들어야 합니다.

#### 절차

- 1 탐색 패널에서 **보안 > 분산 방화벽**을 선택합니다.
- 2 L3 규칙에 대해 **일반** 탭을 클릭하거나 L2 규칙에 대해 **이더넷** 탭을 클릭합니다.
- 3 **이름** 열에 새 이름을 입력합니다.
- 4 **작업** 열에서 옵션 중 하나를 선택합니다.
  - 허용 - 지정된 소스, 대상 및 프로토콜을 가진 모든 L3 또는 L2 트래픽이 현재 방화벽 컨텍스트를 통과하도록 허용합니다. 규칙과 일치하고 허용된 패킷은 방화벽이 존재하지 않을 때와 동일하게 시스템을 이동합니다.
  - 삭제 - 지정된 소스, 대상 및 프로토콜을 가진 패킷을 삭제합니다. 패킷 삭제는 소스 또는 대상 시스템에 알림을 보내지 않는 작업입니다. 패킷을 삭제하면 재시도 임계값에 도달할 때까지 연결이 재시도됩니다.
  - 거절 - 지정된 소스, 대상 및 프로토콜을 가진 패킷을 거절합니다. 패킷 거절은 보낸 사람에게 대상에 접속할 수 없다는 메시지를 보내는 패킷 거부 방식입니다. 프로토콜이 TCP인 경우 TCP RST 메시지가 전송됩니다. UDP, ICMP 및 기타 IP 연결에 대해 관리 목적으로 금지된 코드가 포함된 ICMP 메시지가 전송됩니다. [거절] 기능의 장점 중 하나는 단 한 차례의 시도에서 연결이 설정되지 않으면 전송 애플리케이션에 알림이 보내진다는 점입니다.

---

**참고** 기본 규칙에 대한 작업으로 **거절**을 선택하는 것은 권장되지 않습니다.

---

- 5 **로그**에서 로깅을 사용하거나 사용하지 않도록 설정합니다.  
로깅을 사용하도록 설정하면 성능에 영향을 줄 수 있습니다.
- 6 **계시**를 클릭합니다.

## 방화벽 규칙 순서 변경

규칙은 위에서 아래로 처리됩니다. 목록의 규칙 순서를 변경할 수 있습니다.

방화벽을 통과하려는 모든 트래픽의 경우 패킷 정보는 규칙이 [규칙] 테이블에 표시된 순서에 따라(맨 위에서 시작하여 맨 아래의 기본 규칙으로 내려감) 달라집니다. 일부 경우 두 개 이상의 규칙 우선 순위는 트래픽 흐름을 결정하는 데 중요할 수 있습니다.

사용자 지정 규칙을 테이블에서 위나 아래로 이동할 수 있습니다. 기본 규칙은 항상 테이블의 맨 아래에 있으며 이동할 수 없습니다.

#### 절차

- 1 탐색 패널에서 **보안 > 분산 방화벽**을 선택합니다.
- 2 L3 규칙에 대해 **일반** 탭을 클릭하거나 L2 규칙에 대해 **이더넷** 탭을 클릭합니다.
- 3 규칙을 선택하고 메뉴 모음에서 **위로 이동** 또는 **아래로 이동** 아이콘을 클릭합니다.

#### 4 계시를 클릭합니다.

## 방화벽 규칙 필터링

방화벽 섹션으로 이동하면 처음에는 모든 규칙이 표시됩니다. 필터를 적용하여 규칙 하위 집합만 보이도록 표시되는 내용을 제어할 수 있습니다. 이렇게 하면 규칙을 보다 쉽게 관리할 수 있습니다.

#### 절차

- 1 탐색 패널에서 **보안 > 분산 방화벽**을 선택합니다.
- 2 L3 규칙에 대해 **일반** 탭을 클릭하거나 L2 규칙에 대해 **이더넷** 탭을 클릭합니다.
- 3 메뉴 모음의 오른쪽에 있는 검색 텍스트 필드에서, 개체를 선택하거나 개체 이름의 시작 문자를 입력하여 선택할 개체 목록의 범위를 좁힙니다.  
  
개체를 선택하면 필터가 적용되고 규칙 목록이 업데이트되어 해당 개체를 포함하는 규칙만 다음 열에 표시됩니다.
  - 소스
  - 대상
  - 적용 대상
  - 서비스
- 4 필터를 제거하려면 텍스트 필드에서 개체 이름을 삭제합니다.

## 논리 스위치 브리지 포트에 대한 방화벽 구성

계층 2 브리지 기반 논리적 스위치의 브리지 포트에 대해 방화벽 섹션과 방화벽 규칙을 구성할 수 있습니다. 브리지는 NSX Edge 노드를 사용하여 생성해야 합니다.

#### 사전 요구 사항

스위치가 브리지 프로파일에 연결되어 있는지 확인합니다. [계층 2 브리지 지원 논리적 스위치 생성](#)의 내용을 참조하십시오.

#### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **보안 > 브리지 방화벽**을 선택합니다.
- 3 논리적 스위치를 선택합니다.  
  
스위치는 브리지 프로파일에 연결되어야 합니다.
- 4 이전 섹션에서 계층 2 또는 계층 3 방화벽을 구성하는 단계와 동일한 단계를 수행합니다.

## 방화벽 제외 목록 구성

논리적 포트, 논리적 스위치 또는 NSGroup을 방화벽 규칙에서 제외할 수 있습니다.

방화벽 규칙으로 섹션을 생성한 후에 방화벽 규칙에서 NSX-T Data Center 장치 포트를 제외할 수 있습니다.

### 절차

- 1 탐색 패널에서 **보안 > 분산 방화벽**을 선택합니다.
- 2 **제외 목록** 탭을 클릭합니다.
- 3 **추가**를 클릭합니다.
- 4 유형 및 개체를 선택합니다.  
사용 가능한 유형에는 **논리적 포트**, **논리적 스위치** 및 **NSGroup**이 있습니다.
- 5 **확인**을 클릭합니다.
- 6 제외 목록에서 개체를 제거하려면 개체를 선택하고 메뉴 모음에서 **삭제**를 클릭합니다.

## 방화벽 사용 및 사용 안 함

분산 방화벽 기능을 사용하거나 사용하지 않도록 설정할 수 있습니다. 사용되지 않도록 설정하면 규칙이 적용되지 않습니다.

### 절차

- 1 탐색 패널에서 **보안 > 분산 방화벽**을 선택합니다.
- 2 **설정** 탭을 클릭합니다.
- 3 **편집**을 클릭합니다.
- 4 대화 상자에서 방화벽 상태를 녹색(사용) 또는 회색(사용 안 함)으로 설정합니다.
- 5 **저장**을 클릭합니다.

## 논리적 라우터에 방화벽 규칙 추가 또는 삭제

계층 0 또는 계층 1 논리적 라우터에 방화벽 규칙을 추가하여 라우터와의 통신을 제어할 수 있습니다.

### 사전 요구 사항

방화벽 규칙의 매개 변수를 숙지하십시오. [방화벽 규칙 추가](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.

- 3 **라우터** 탭을 아직 선택하지 않았으면 클릭합니다.
- 4 논리적 라우터의 이름을 클릭합니다.
- 5 **서비스 > Edge 방화벽**을 선택합니다.
- 6 기존 섹션이나 규칙을 클릭합니다.
- 7 규칙을 추가하려면 메뉴 모음에서 **규칙 추가**를 클릭하고 **위에 규칙 추가** 또는 **아래에 규칙 추가**를 선택하거나 규칙의 첫 번째 열에 있는 메뉴 아이콘을 클릭하고 **위에 규칙 추가** 또는 **아래에 규칙 추가**를 선택한 후 규칙 매개 변수를 지정합니다.  
  
이 규칙은 논리적 라우터에만 적용되기 때문에 [적용 대상] 필드가 표시되지 않습니다.
- 8 규칙을 삭제하려면 해당 규칙을 선택하고 메뉴 모음에서 **삭제**를 클릭하거나 첫 번째 열의 메뉴 아이콘을 클릭하고 **삭제**를 선택합니다.

## 결과

---

**참고** Tier-0 논리적 라우터에 방화벽 규칙을 추가하고 라우터를 지원하는 NSX Edge 클러스터가 활성-활성 모드에서 실행 중인 경우 방화벽은 상태 비저장 모드에서만 실행될 수 있습니다. HTTP, SSL, TCP 등과 같은 상태 저장 서비스로 방화벽 규칙을 구성하면 방화벽 규칙이 예상대로 작동하지 않습니다. 이 문제를 방지하려면 NSX Edge 클러스터가 활성-대기 모드에서 실행되도록 구성합니다.

---

# VPN(Virtual Private Network)



NSX-T Data Center는 NSX Edge에서 IPsec VPN 및 L2VPN(계층 2 VPN)을 지원합니다.

---

**참고** NSX-T Data Center 수출 제한 릴리스에서는 IPsec VPN 및 L2VPN이 지원되지 않습니다.

---

## IPsec VPN

IPsec VPN은 끝점이라는 IPsec 게이트웨이를 통과하는 공용 네트워크를 통해 연결된 두 네트워크 간에 트래픽 흐름을 보호합니다. NSX Edge는 ESP(Encapsulating Security Payload)와 함께 IP 터널링을 사용하는 터널 모드만 지원합니다.

IPsec VPN은 IKE 프로토콜을 사용하여 보안 매개 변수를 협상합니다. 기본 UDP 포트는 500으로 설정됩니다. 게이트웨이에서 NAT가 감지되면 포트는 4500으로 설정됩니다.

---

**참고** IPsec VPN은 Tier-0 논리 라우터에서만 지원됩니다.

---

NSX Edge는 정책 기반 VPN과 경로 기반 VPN이라는 두 가지 유형의 VPN을 지원합니다.

정책 기반 VPN에서는 IPsec 서비스로 전달되는 패킷에 정책을 적용해야 합니다. 이런 유형의 VPN은 로컬 네트워크 토폴로지 및 구성이 변경될 때 변경 사항을 수용하기 위해 정책 설정도 업데이트해야 하기 때문에 정적으로 간주됩니다.

경로 기반 VPN은 BGP 등을 프로토콜로 사용하여 VTI(가상 터널 인터페이스)라는 특수 인터페이스를 통해 동적으로 학습된 경로를 기반으로 트래픽을 터널링합니다. IPsec는 VTI(가상 터널 인터페이스)를 통과하는 모든 트래픽을 보호합니다.

## L2VPN

L2VPN 연결을 사용하면 온-프레미스 데이터 센터의 계층 2 네트워크를 VMware Cloud on Amazon(VMC)과 같은 클라우드로 확장할 수 있습니다. 이 연결은 경로 기반 IPsec 터널로 보호됩니다.

확장된 네트워크는 단일 브로드캐스트 도메인이 있는 단일 서브넷이므로 IP 주소를 변경하지 않고도 온-프레미스 데이터 센터와 공용 클라우드 간에 VM을 마이그레이션할 수 있습니다.

데이터 센터 마이그레이션을 지원하는 것 외에도, L2VPN으로 확장된 온-프레미스 네트워크는 재해 복구와 수요 증가("클라우드 버스팅"이라고도 함)를 충족시키기 위한 오프-프레미스 계산 리소스의 동적 활용에 유용합니다.

각 L2VPN 세션에는 GRE 터널이 하나 있습니다. 터널 이중화는 지원되지 않습니다. L2VPN 세션은 최대 4094개의 계층 2 네트워크로 확장할 수 있습니다.

**참고** L2VPN은 NSX Data Center for vSphere에서 비관리형 또는 관리형인 NSX Edge와 NSX-T Data Center 사이에서 지원됩니다.

본 장은 다음 항목을 포함합니다.

- [IPSec VPN 구성](#)
- [L2VPN 구성](#)

## IPSec VPN 구성

경로 기반 VPN 및 정책 기반 VPN 세션은 API만을 사용하여 생성할 수 있습니다.

**참고** NSX-T Data Center 수출 제한 릴리스에서는 IPSec VPN이 지원되지 않습니다.

동일한 네트워크 프로파일에서 NAT와 IPSec VPN을 함께 사용할 수 없습니다. NAT와 IPSec VPN을 다른 네트워크 프로파일에 배치해야 합니다.

### 사전 요구 사항

IPSec VPN을 숙지합니다. [IPSec VPN](#)의 내용을 참조하십시오.

### 절차

- 1 Tier-0 논리적 라우터에서 IPSec VPN 서비스를 구성합니다.

POST /api/v1/vpn/ipsec/services 호출을 사용합니다.

```
POST /api/v1/vpn/ipsec/services
{
  "display_name": "IPSec VPN service",
  "logical_router_id": "f81f220f-3072-4a6e-9f53-ad3b8bb8af57"
}
```

- 2 DPD(Dead Peer Detection) 프로파일을 구성합니다.

POST /api/v1/vpn/ipsec/dpd-profiles 호출을 사용합니다.

기본 프로파일은 60초 DPD 프로브 간격으로 프로비저닝됩니다.

```
POST /api/v1/vpn/ipsec/dpd-profiles
{
  "enabled": "true",
  "dpd_probe_interval": 60,
  "description": "DPD profile",
  "display_name": "DPD profile"
}
```



### 3 IKE 프로파일 매개 변수를 구성합니다.

POST /api/v1/vpn/ipsec/ike-profiles 호출을 사용합니다.

```
POST /api/v1/vpn/ipsec/ike-profiles
{
  "digest_algorithms": ["SHA2_256"],
  "description": "IKEProfile for site1",
  "display_name": "IKEProfile site1",
  "encryption_algorithms": ["AES_128"],
  "ike_version": "IKE_V2",
  "dh_groups": ["GROUP14"],
  "sa_life_time": 21600
}
```

### 4 IPSec VPN에 대한 터널 프로파일을 구성합니다.

POST /api/v1/vpn/ipsec/tunnel-profiles 호출을 사용합니다.

```
POST /api/v1/vpn/ipsec/tunnel-profiles/
{
  "digest_algorithms": ["SHA1", "SHA2_256"],
  "description": "Tunnel Profile for site 1",
  "display_name": "Tunnel Profile for site 1",
  "encapsulation_mode": "TUNNEL_MODE",
  "encryption_algorithms": ["AES_128", "AES_256"],
  "enable_perfect_forward_secrecy": true,
  "dh_groups": ["GROUP14"],
  "transform_protocol": "ESP",
  "sa_life_time": 3600,
  "df_policy": "CLEAR"
}
```

### 5 IPSec VPN 피어와 통신하도록 피어 끝점을 구성합니다.

POST /api/v1/vpn/ipsec/peer-endpoints 호출을 사용합니다.

```
POST /api/v1/vpn/ipsec/peer-endpoints
{
  "display_name": "Peer endpoint for site 1",
  "connection_initiation_mode": "INITIATOR",
  "authentication_mode": "PSK",
  "ipsec_tunnel_profile_id": "640607f3-bb83-4e54-a153-57939965881c",
  "dpd_profile_id": "4808d04e-572d-480d-8182-61ddaa146461",
  "psk": "6721b9f1f5936956c0a8b4ed95286b452db04dae721edd0f264f0fcc6e94882b",
  "ike_profile_id": "a4db6863-b6f0-45bd-967e-a2e22c260329",
  "peer_address": "10.14.24.4",
  "peer_id": "10.14.24.4"
}
```

**6** VPN 끝점에 대한 로컬 끝점을 구성합니다.

POST /api/v1/vpn/ipsec/local-endpoints 호출을 사용합니다.

```
POST /api/v1/vpn/ipsec/local-endpoints
{
  "local_address": "1.1.1.12",
  "local_id": "1.1.1.12",
  "display_name": "Local endpoint",
  "ipsec_vpn_service_id": {
    "target_id" : "81388ec0-b5e3-4a9e-b551-e372e700772c"
  }
}
```

**7** 경로 기반 VPN 세션을 구성합니다.

POST /api/v1/vpn/ipsec/sessions 호출을 사용합니다.

```
POST /api/v1/vpn/ipsec/sessions
{
  "resource_type": "RouteBasedIPSecVPNSession",
  "display_name": "RouteSession1",
  "ipsec_vpn_service_id": "657bcb55-48ce-4e0f-bfc7-a5a91b2990ae",
  "peer_endpoint_id": "cfc70ab5-16d1-4292-9391-fcee23ccea96",
  "local_endpoint_id": "9d4b44f1-0bfa-4705-ac67-09244a17d42e",
  "enabled": true,
  "tunnel_ports": [
    {
      "ip_subnets": [
        {
          "ip_addresses" : [
            "192.168.50.1"
          ],
          "prefix_length" : 24
        }
      ]
    }
  ]
}
```

**8** 정책 기반 VPN 세션을 구성합니다.

POST /api/v1/vpn/ipsec/sessions 호출을 사용합니다.

```
POST /api/v1/vpn/ipsec/sessions
{
  "resource_type": "PolicyBasedIPSecVPNSession",
  "display_name": "PolicySession1",
  "ipsec_vpn_service_id": "ea071856-9e91-4826-a841-9ec7ee9ea534",
  "peer_endpoint_id": "0c2447d2-8890-4b55-bf02-8c6b1a94d1ce",
  "local_endpoint_id": "161acb63-c3f2-438d-9e5c-cb655e6a1099",
  "enabled": true,
  "policy_rules": [
    {
      "sources": [
```

```

    {
      "subnet": "2.2.2.0/24"
    }
  ],
  "logged": true,
  "destinations": [
    {
      "subnet": "3.3.3.0/24"
    }
  ],
  "action": "PROTECT",
  "enabled": true
}
]
}

```

## L2VPN 구성

L2VPN 서비스 및 세션은 API만을 사용하여 생성할 수 있습니다.

---

**참고** NSX-T Data Center 수출 제한 릴리스에서는 L2VPN이 지원되지 않습니다.

---

### 사전 요구 사항

- L2VPN을 숙지합니다. [L2VPN](#)의 내용을 참조하십시오.
- Tier-0 논리적 라우터가 업링크 프로파일로 구성되었는지 확인합니다. "NSX-T Data Center 설치 가이드"의 내용을 참조하십시오.
- 논리적 스위치가 구성되어 있는지 확인합니다. [논리적 스위치 생성](#)의 내용을 참조하십시오.
- NSX Data Center for vSphere에서 관리되지 않는 NSX Edge를 사용할 수 있는지 확인합니다.
- IPSec VPN이 구성되었는지 확인합니다. [IPSec VPN 구성](#)

### 절차

#### 1 L2VPN 서비스를 구성합니다.

POST /api/v1/vpn/l2vpn/services 호출을 사용합니다.

```

POST /api/v1/vpn/l2vpn/services
{
  "logical_router_id": "b6fe5455-619b-4030-b5f8-8575749f4404",
  "logical_tap_ip_pool" : [ "169.254.64.0/28" ],
  "enable_full_mesh" : true
}

```

## 2 L2VPN 세션을 구성합니다.

POST /api/v1/vpn/l2vpn/sessions 호출을 사용합니다.

```
POST /api/v1/vpn/l2vpn/sessions
{
  "l2vpn_service_id" : "421de3a2-c6ec-4c42-a891-5bde3b5feb68",
  "transport_tunnels" : [
    {
      "target_id" : "801e5140-6da8-4e78-ab44-f966de75f311"
    }
  ]
}
```

## 3 연결(attachment)을 사용하여 논리적 포트를 구성합니다.

POST /api/v1/vpn/logical-ports 호출을 사용합니다.

```
POST /api/v1/logical-ports/
{
  "resource_type": "LogicalPort",
  "display_name": "Extend logicalSwitch, port for service",
  "logical_switch_id": "f52abcee-27a7-426c-a128-037db2283582",
  "admin_state" : "UP",
  "attachment": {
    "attachment_type": "L2VPN_SESSION",
    "id": "6806c4ea-3b77-4b8a-8af2-ccc47b1ba8a9",
    "context" : {
      "resource_type" : "L2VpnAttachmentContext",
      "tunnel_id" : 10
    }
  }
}
```

## 4 L2VPN 피어 코드 구성을 다운로드합니다.

GET /api/v1/vpn/l2vpn/sessions/<L2VPN-session-ID>/peer-codes

## 5 온-프레미스 NSX Data Center for vSphere 관리되지 않는 NSX Edge CLI에 로그인합니다.

## 6 L2VPN 피어 코드 구성을 붙여넣습니다.

## 7 (선택 사항) L2VPN 세션을 모니터링합니다.

- L2VPN 세션 요약 GET /api/v1/vpn/l2vpn/sessions/summary.
- L2VPN 세션 통계 GET /api/v1/vpn/l2vpn/sessions/<L2VPN-session-ID>/statistics.

# 개체, 그룹, 서비스 및 VM 관리

# 9

IP 집합, IP 풀, MAC 집합, NSGroup 및 NSService를 생성할 수 있습니다. 또한 VM용 태그를 관리할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- IP 집합 생성
- IP 풀 생성
- MAC 집합 생성
- NSGroup 생성
- 서비스 및 서비스 그룹 구성
- VM용 태그 관리

## IP 집합 생성

IP 집합은 방화벽 규칙에서 소스 및 대상으로 사용할 수 있는 IP 주소 그룹입니다.

IP 집합은 개별 IP 주소, IP 범위 및 서브넷 조합을 포함할 수 있습니다. IPv4 또는 IPv6 주소 중 하나 또는 둘 다를 지정할 수 있습니다. IP 집합은 NSGroup의 멤버일 수 있습니다.

---

**참고** IPv6은 방화벽 규칙에 대한 소스 또는 대상 범위에 대해 지원되지 않습니다.

---

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **인벤토리 > 그룹**을 선택합니다.
- 3 기본 패널의 맨 위에 있는 **IP 집합**을 선택합니다.
- 4 **추가**를 클릭합니다.
- 5 이름을 입력합니다.
- 6 (선택 사항) 설명을 입력합니다.
- 7 개별 주소 또는 주소 범위를 입력합니다.

## 8 저장을 클릭합니다.

# IP 풀 생성

L3 서브넷을 생성할 때 IP 풀을 사용하여 IP 주소 또는 서브넷을 할당할 수 있습니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **인벤토리 > 그룹**을 선택합니다.
- 3 기본 패널의 맨 위에 있는 **IP 풀**을 선택합니다.
- 4 **추가**를 클릭합니다.
- 5 이름을 입력합니다.
- 6 (선택 사항) 설명을 입력합니다.
- 7 **추가**를 클릭합니다.
- 8 IP 범위를 입력합니다.  
셀의 오른쪽 상단 모서리로 마우스를 가져간 후 연필 아이콘을 클릭하여 편집합니다.
- 9 (선택 사항) 게이트웨이를 입력합니다.
- 10 CIDR IP 주소와 접미사를 입력합니다.
- 11 (선택 사항) DNS 서버를 입력합니다.
- 12 (선택 사항) DNS 접미사를 입력합니다.
- 13 **저장**을 클릭합니다.

# MAC 집합 생성

MAC 집합은 계층 2 방화벽 규칙에서 소스 및 대상으로 사용하고 NSGroup의 멤버로 사용할 수 있는 MAC 주소 그룹입니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **인벤토리 > 그룹**을 선택합니다.
- 3 기본 패널의 맨 위에 있는 **MAC 집합**을 선택합니다.
- 4 **추가**를 클릭합니다.
- 5 이름을 입력합니다.
- 6 (선택 사항) 설명을 입력합니다.

7 MAC 주소를 입력합니다.

8 **저장**을 클릭합니다.

## NSGroup 생성

NSGroup을 구성하여 IP 집합, MAC 집합, 논리적 포트, 논리적 스위치 및 기타 NSGroup 조합을 포함할 수 있습니다. Applied To 필드뿐 아니라 방화벽 규칙에 소스 및 대상으로 NSGroup을 지정할 수 있습니다.

---

**NSX Cloud 참고** NSX Cloud를 사용 중인 경우 NSX Cloud에 필요한 구성, 지원되는 기능 및 자동 생성된 논리적 엔티티의 목록은 [공용 클라우드에 대해 NSX-T Data Center 기능을 사용하는 방법](#)의 내용을 참조하십시오.

---

NSGroup은 다음과 같은 특성을 갖습니다.

- IP 집합, MAC 집합, 논리적 스위치, 논리적 포트 및 NSGroup이 될 수 있는 직접 멤버를 지정할 수 있습니다.
- 논리적 스위치, 논리적 포트 또는 VM에 적용되는 최대 5개의 멤버 자격 기준을 지정할 수 있습니다. 논리적 스위치 또는 논리적 포트에 적용되는 기준의 경우 태그 및 범위(선택 사항)를 지정할 수 있습니다. VM에 적용되는 기준의 경우 특정 문자열로 시작하거나, 특정 문자열과 같거나, 특정 문자열을 포함하는 이름을 지정할 수 있습니다.
- NSGroup에는 직접 멤버와 유효한 멤버가 있습니다. 유효한 멤버에는 이 NSGroup의 멤버에 속하는 직접 및 유효한 멤버뿐 아니라 멤버 자격 기준을 사용하여 지정하는 멤버가 포함됩니다. 예를 들어 NSGroup-1에 직접 멤버 LogicalSwitch-1이 있다고 가정해보겠습니다. NSGroup-2를 추가하고 NSGroup-1 및 LogicalSwitch-2를 멤버로 지정합니다. 이제 NSGroup-2에는 직접 멤버 NSGroup-1 및 LogicalSwitch-2와 유효한 멤버 LogicalSwitch-1이 있습니다. 다음에는 NSGroup-3을 추가하고 멤버로 NSGroup-2를 지정합니다. 이제 NSGroup-3에는 직접 멤버 NSGroup-2가 있고 유효한 멤버 LogicalSwitch-1 및 LogicalSwitch-2가 있습니다.
- NSGroup에는 최대 500개의 직접 멤버가 있을 수 있습니다.
- NSGroup에서 권장되는 유효한 멤버 수 제한은 5000개입니다. 이 제한을 초과해도 기능에는 영향이 없으나 성능이 저하될 수 있습니다. NSX Manager에서 NSGroup에 대한 유효한 멤버 수가 5000개의 80%를 초과하면 경고 메시지 `NSGroup xyz is about to exceed the maximum member limit. Total number in NSGroup is ...`가 로그 파일에 표시되고, 이 수가 5000을 초과하면 경고 메시지 `NSGroup xyz has reached the maximum numbers limit. Total number in NSGroup = ...`이 표시됩니다. NSX Controller에서 NSGroup의 변환된 VIF/IP/MAC 수가 5000개를 초과하면 경고 메시지 `Container xyz has reached the maximum IP/MAC/VIF translations limit. Current translations count in Container - IPs:..., MACs:..., VIFs:...`가 로그 파일에 표시됩니다. NSX Manager 및 NSX Controller는 하루에 2번, 즉 오전 7시와 오후 7시에 NSGroup에서 해당 제한을 확인합니다.
- 지원되는 최대 VM 수는 10,000개입니다.

NSGroup에 멤버로 추가할 수 있는 모든 개체(즉, 논리적 스위치, 논리적 포트, IP 집합, MAC 집합, VM 및 NSGroup)의 경우 개체에 대한 화면으로 이동한 후 **관련 > NSGroup**을 선택하여 직간접적으로 이 개체를 멤버로 갖고 있는 모든 NSGroup을 표시합니다. 예를 들어 위의 예에서 LogicalSwitch-1에 대한 화면으로 이동한 후 **관련 > NSGroup**을 선택하면 NSGroup-1, NSGroup-2 및 NSGroup-3이 표시됩니다. 이 세 항목이 모두 직접 또는 간접 멤버로 LogicalSwitch-1을 포함하기 때문입니다.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **인벤토리 > 그룹**을 선택합니다.
- 3 **그룹** 탭을 아직 선택하지 않았으면 클릭합니다.
- 4 **추가**를 클릭합니다.
- 5 NSGroup의 이름을 입력합니다.
- 6 (선택 사항) 설명을 입력합니다.
- 7 (선택 사항) **멤버 자격 조건**을 클릭합니다

기준은 논리적 스위치, 논리적 포트 또는 VM에 적용될 수 있습니다. 각 기준의 경우 논리적 AND 연산자로 조합된 최대 5개의 규칙을 지정할 수 있습니다. 논리적 스위치 또는 논리적 포트에 적용되는 규칙의 경우 태그 및 범위(선택 사항)를 지정할 수 있습니다. VM에 적용되는 규칙의 경우 특정 문자열로 시작하거나, 특정 문자열과 같거나, 특정 문자열을 포함하는 이름을 지정할 수 있습니다.

논리적 OR 연산자로 조합된 최대 5개의 기준을 지정할 수 있습니다.

- 8 (선택 사항) **멤버**를 클릭하여 멤버를 선택합니다.

사용 가능한 유형은 **IP 집합**, **MAC 집합**, **논리적 스위치**, **논리적 포트** 및 **NSGroup**입니다.

- 9 **저장**을 클릭합니다.

## 서비스 및 서비스 그룹 구성

NSService를 구성하고 일치하는 네트워크 트래픽에 대해 포트 및 프로토콜 연결과 같은 매개 변수를 지정할 수 있습니다. NSService를 사용하여 방화벽 규칙에서 특정 유형의 트래픽을 허용하거나 차단할 수도 있습니다.

NSService 유형은 다음과 같습니다.

- 이더넷
- IP
- IGMP
- ICMP
- ALG



## ■ L4 포트 집합

L4 포트 집합은 소스 포트 및 대상 포트의 식별을 지원합니다. 최대 15개의 포트 범위 내에서 개별 포트 또는 포트 범위를 지정할 수 있습니다.

NSService는 다른 NSService의 그룹일 수도 있습니다. 그룹에 해당하는 NSService는 다음 유형일 수 있습니다.

- 계층 2
- 계층 3 이상

NSService를 생성한 후에는 유형을 변경할 수 없습니다. 일부 NSService는 미리 정의됩니다. 이를 수정하거나 삭제할 수는 없습니다.

## NSService 생성

NSService를 생성하여 일치하는 네트워크 검색에 사용하는 특성을 지정하거나 방화벽 규칙에서 차단하거나 허용할 트래픽 유형을 정의할 수 있습니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **인벤토리 > 서비스**를 선택합니다.
- 3 **추가**를 클릭합니다.
- 4 이름을 입력합니다.
- 5 (선택 사항) 설명을 입력합니다.
- 6 **프로토콜 지정**을 선택하여 개별 서비스를 구성하거나 **기존 서비스 그룹화**를 선택하여 NSService 그룹을 구성합니다.
- 7 개별 서비스에 대해 유형 및 프로토콜을 선택합니다.  
사용 가능한 유형은 **이더넷**, **IP**, **IGMP**, **ICMP**, **ALG** 및 **L4 포트 집합**입니다.
- 8 서비스 그룹에 대해 그룹의 유형 및 멤버를 선택합니다.  
사용 가능한 유형은 **계층 2** 및 **계층 3 이상**입니다.
- 9 **저장**을 클릭합니다.

## VM용 태그 관리

인벤토리에서 VM 목록을 볼 수 있습니다. VM에 태그를 추가하여 보다 쉽게 검색할 수도 있습니다.

### 절차

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

**2** 탐색 패널에서 **인벤토리 > 가상 시스템**을 선택합니다.

가상 시스템, 외부 ID, 소스 및 태그라는 4개의 열로 구성된 VM 목록이 표시됩니다. 처음 3개 열의 머리글에 있는 필터 아이콘을 클릭하여 목록을 필터링할 수 있습니다. 문자열을 입력하여 부분 일치 항목을 찾을 수 있습니다. 입력한 문자열이 열의 문자열에 포함되어 있으면 해당 항목이 표시됩니다. 큰따옴표로 묶은 문자열을 입력하여 정확히 일치하는 항목을 찾을 수 있습니다. 입력한 문자열이 열의 문자열과 정확하게 일치하면 해당 항목이 표시됩니다.

**3** VM을 선택합니다.**4** **태그 관리**를 클릭합니다.**5** 태그를 추가하거나 삭제합니다.

옵션	작업
태그 추가	<b>추가</b> 를 클릭하여 태그 및 범위(선택 사항)를 지정합니다.
태그 삭제	기존 태그를 선택하고 <b>삭제</b> 를 클릭합니다.

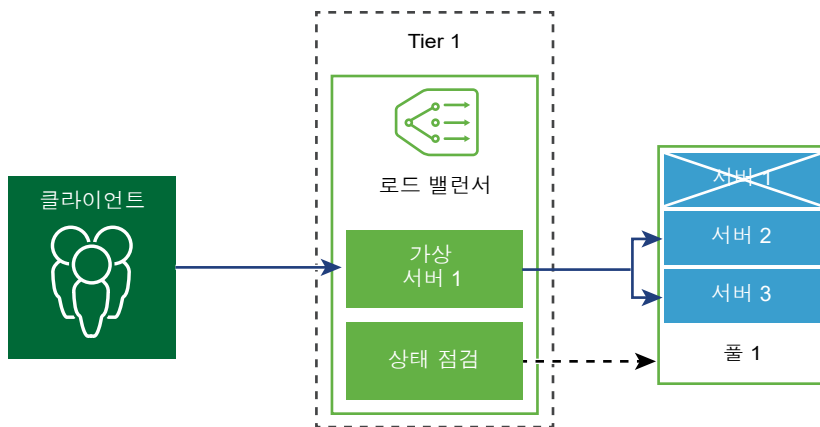
VM은 최대 15개의 태그를 가질 수 있습니다.

**6** **저장**을 클릭합니다.

# 논리적 로드 밸런서

# 10

NSX-T Data Center 논리적 로드 밸런서는 애플리케이션에 고가용성 서비스를 제공하고 네트워크 트래픽 로드를 여러 서버로 분산합니다.



로드 밸런서는 들어오는 서비스 요청을 로드 분산이 사용자에게 투명해지는 방식으로 여러 서버에 고르게 분산합니다. 로드 밸런싱은 리소스 활용도를 최적화하고, 처리량을 극대화하며, 응답 시간을 최소화하고, 오버로드를 방지하는 데 도움이 됩니다.

로드 밸런싱을 위해 가상 IP 주소를 풀 서버 집합에 매핑할 수 있습니다. 로드 밸런서는 가상 IP 주소에 대한 TCP, UDP, HTTP 또는 HTTPS 요청을 수락하고 사용할 풀 서버를 결정합니다.

환경 요구 사항에 따라 과도한 네트워크 트래픽 로드를 처리하도록 기존 가상 서버와 풀 멤버를 늘려서 로드 밸런서 성능을 확장 할 수 있습니다.

**참고** 논리적 로드 밸런서는 Tier-1 논리적인 라우터에만 지원됩니다. 하나의 로드 밸런서는 하나의 Tier-1 논리적 라우터에만 연결할 수 있습니다.

본 장은 다음 항목을 포함합니다.

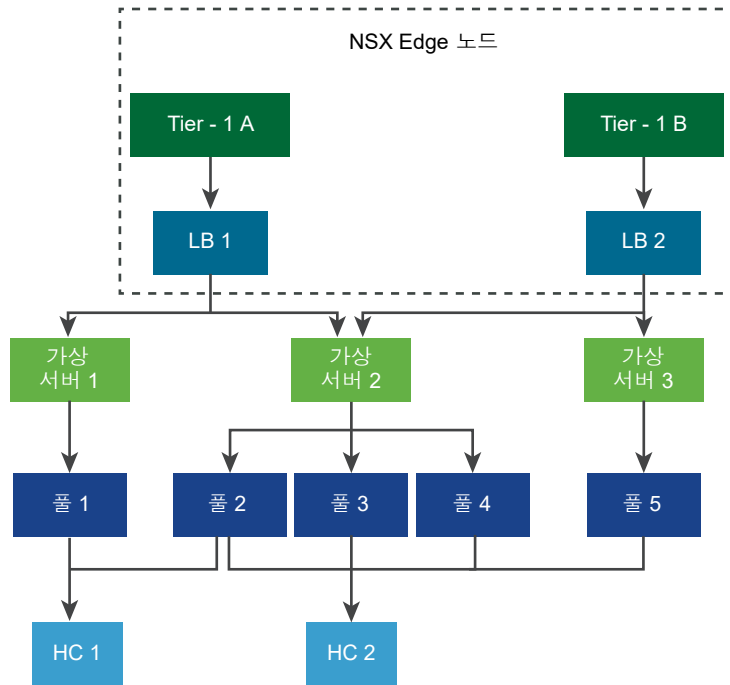
- [키 로드 밸런서 개념](#)
- [로드 밸런서 구성 요소 구성](#)

## 키 로드 밸런서 개념

로드 밸런서에는 가상 서버, 서버 풀 및 상태 점검 모니터가 포함됩니다.

로드 밸런서는 Tier-1 논리적 라우터에 연결됩니다. 로드 밸런서는 하나 이상의 가상 서버를 호스팅합니다. 가상 서버는 IP, 포트 및 프로토콜의 고유 한 조합으로 표시되는 애플리케이션 서비스의 추상적인 개념입니다. 가상 서버는 하나 이상의 서버 풀로 연결됩니다. 서버 풀은 서버 그룹으로 구성됩니다. 서버 풀에는 개별 서버 풀 멤버가 포함됩니다.

각 서버가 애플리케이션을 올바르게 실행하는지 테스트하려면 서버의 상태를 점검하는 상태 점검 모니터를 추가하십시오.



## 로드 밸런서 리소스 크기 조정

로드 밸런서는 소형, 중형 및 대형 크기로 제공됩니다. 로드 밸런서는 로드 밸런서 크기를 기반으로 다양한 가상 서버 및 풀 멤버를 호스팅할 수 있습니다.

하나의 로드 밸런서는 하나의 Tier-1 논리적 라우터에 연결됩니다. 이 Tier-1 논리적 라우터는 NSX Edge 노드에서 호스팅됩니다. NSX Edge에는 폼 팩터 베어 메탈, 소형, 중형 및 대형 VM 장치가 있습니다. 폼 팩터를 기반으로 NSX Edge 노드는 다른 수의 로드 밸런서를 호스팅할 수 있습니다.

표 10-1. 로드 밸런서 서비스에 대한 로드 밸런서 규모

로드 밸런서 서비스	소형 로드 밸런서	중형 로드 밸런서	대형 로드 밸런서
로드 밸런서당 가상 서버 수	10	100	1000
로드 밸런서당 풀 수	20	200	2000
로드 밸런서당 풀 멤버 수	200	2000	10,000

표 10-2. NSX Edge 노드에 대한 로드 밸런서 규모

NSX Edge 노드 당 로드 밸런서	소형 로드 밸런서	중형 로드 밸런서	대형 로드 밸런서	최대 풀 멤버
NSX Edge VM - 소형	해당 없음	해당 없음	해당 없음	해당 없음
NSX Edge VM - 중형	1	해당 없음	해당 없음	200
NSX Edge VM - 대형	40	4	해당 없음	5000
NSX Edge VM - 베어 메탈	750	75	7	20,000

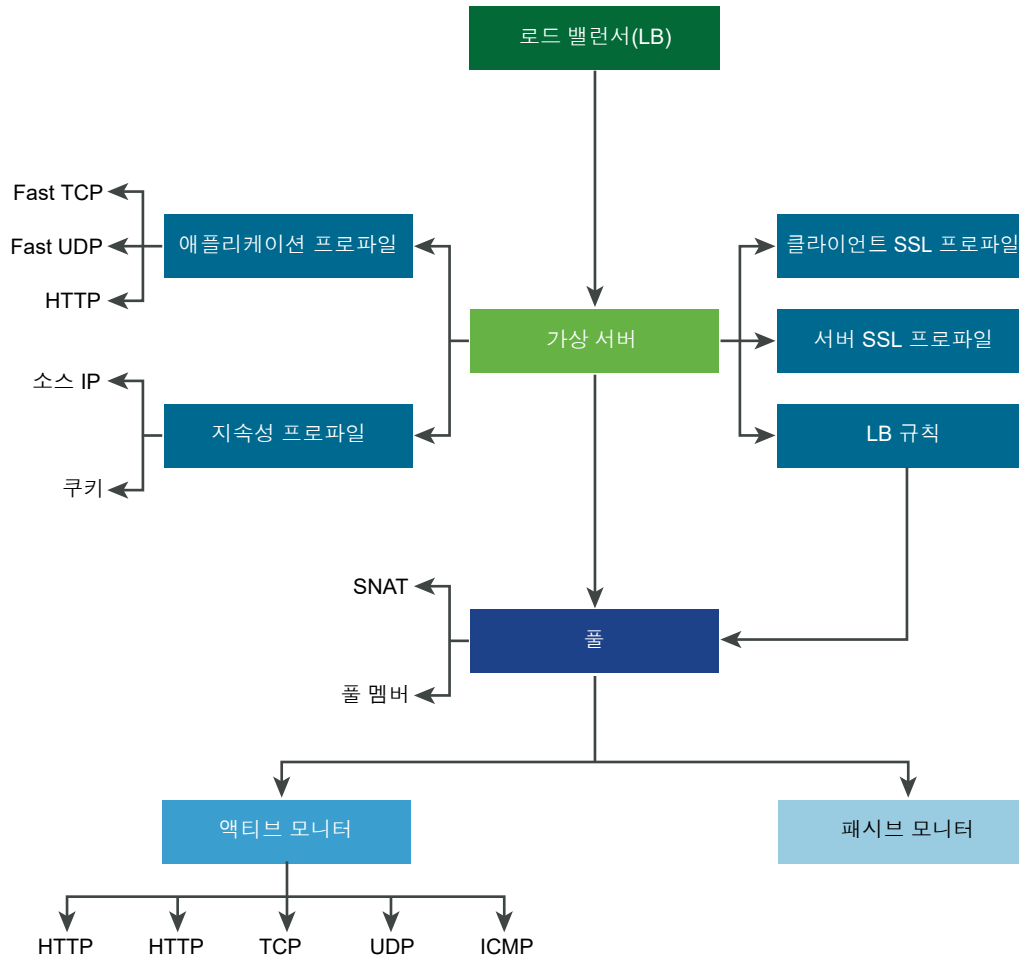
## 지원되는 로드 밸런서 기능

NSX-T Data Center 로드 밸런서는 다음 기능을 지원합니다.

- 계층 4 - TCP 및 UDP
- 계층 7 - HTTP 및 HTTPS(로드 밸런서 규칙 지원)
- 서버 풀 - 정적 및 동적(NSGroup 포함)
- 지속성 - 소스 IP 및 쿠키 지속성 모드
- 상태 점검 모니터 - HTTP, HTTPS, TCP, UDP 및 ICMP를 포함하는 액티브 모니터 및 패시브 모니터
- SNAT - 투명, 자동 맵 및 IP 목록
- HTTP 업그레이드 - WebSocket과 같은 HTTP 업그레이드를 사용하는 응용 프로그램의 경우 클라이언트 또는 서버가 HTTP 업그레이드를 요청하며 이는 지원됩니다. 기본적으로 NSX-T Data Center는 HTTP 응용 프로그램 프로파일을 사용하여 HTTPS 업그레이드 클라이언트 요청을 지원하고 허용합니다.

비활성 클라이언트 또는 서버 통신을 감지하기 위해 로드 밸런서는 60초로 설정된 HTTP 응용 프로그램 프로파일 응답 시간 초과 기능을 사용합니다. 서버가 60초 간격으로 트래픽을 보내지 않으면 NSX-T Data Center는 클라이언트와 서버 측에서 연결을 종료합니다.

참고: SSL 종료 모드 및 프록시 모드는 NSX-T Data Center 2.2 Limited Export 릴리스에서 지원되지 않습니다.

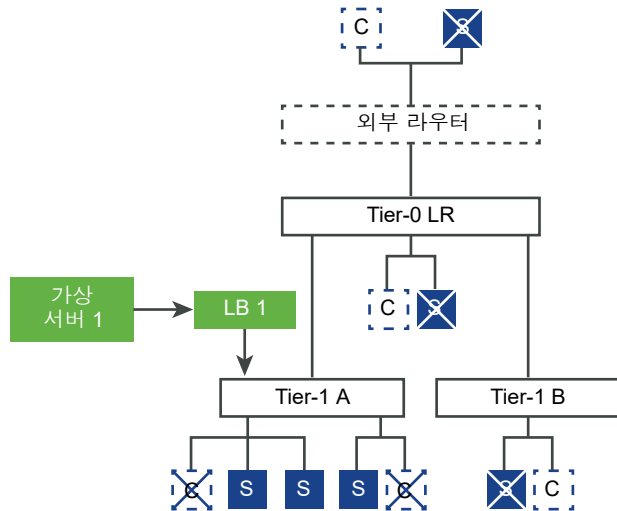


## 로드 밸런서 토폴로지

로드 밸런서는 일반적으로 인라인 또는 단일 암 모드로 배포됩니다.

### 인라인 토폴로지

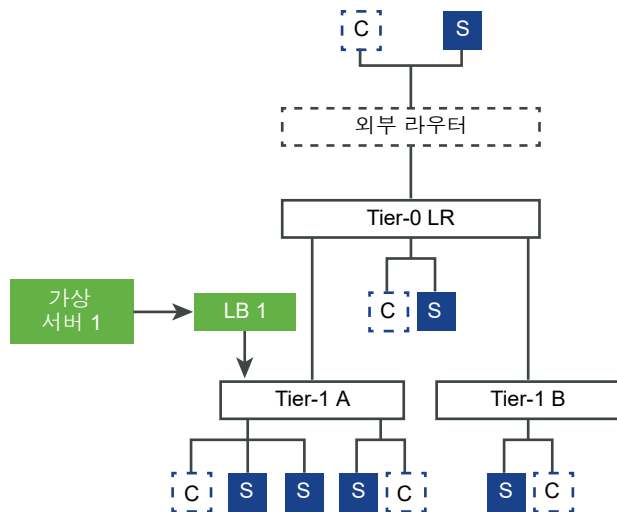
인라인 모드에서 로드 밸런서는 클라이언트와 서버 사이의 트래픽 경로에 있습니다. 클라이언트와 서버는 동일한 Tier-1 논리적 라우터에 연결되지 말아야 합니다. 이 토폴로지에는 가상 서버 SNAT가 필요하지 않습니다.



## 단일 홉 토폴로지

단일 홉 모드에서는 로드 밸런서가 클라이언트와 서버 사이의 트래픽 경로에 있지 않습니다. 이 모드에서는 클라이언트와 서버가 어디에나 있을 수 있습니다. 로드 밸런서는 소스 NAT(SNAT)를 수행하여 로드 밸런서를 통과하는 클라이언트로 향하는 서버의 반환 트래픽을 강제 실행합니다. 이 토폴로지에서는 가상 서버 SNAT를 사용하도록 설정해야 합니다.

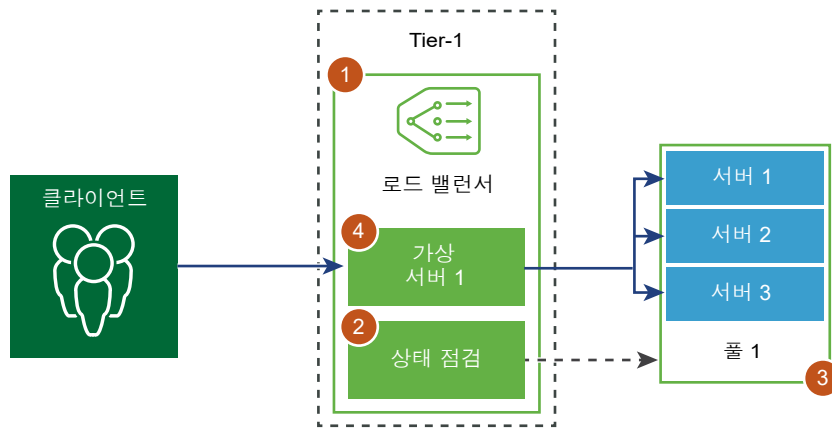
로드 밸런서가 가상 IP 주소에 대한 클라이언트 트래픽을 수신하면 로드 밸런서는 서버 풀 멤버를 선택하고 여기로 클라이언트 트래픽을 전달합니다. 단일 홉 모드에서 로드 밸런서는 서버 응답이 로드 밸런서로 항상 전송되고 로드 밸런서가 서버로 응답을 전달하도록 클라이언트 IP 주소를 로드 밸런서 IP 주소로 바꿉니다.



## 로드 밸런서 구성 요소 구성

논리적 로드 밸런서를 사용하려면 먼저 로드 밸런서를 구성하여 Tier-1 논리적 라우터에 연결해야 합니다.

그런 다음 서버에 대한 상태 점검 모니터링을 설정할 수 있습니다. 그 후, 로드 밸런서에 대한 서버 풀을 구성해야 합니다. 마지막으로 로드 밸런서에 대해 계층 4 또는 계층 7 가상 서버를 생성해야 합니다.

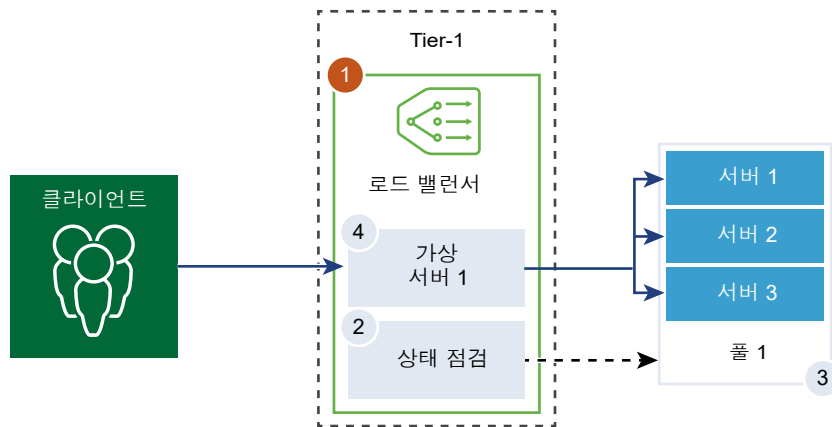


## 로드 밸런서 생성

로드 밸런서는 생성되어 Tier-1 논리적 라우터에 연결됩니다.

로드 밸런서가 오류 로그에 추가할 오류 메시지의 수준을 구성할 수 있습니다.

**참고** 트래픽이 많은 로드 밸런서에서 로그 수준을 DEBUG로 설정하지 마십시오. 로그에 인쇄되는 메시지 수가 많아서 성능에 영향을 줍니다.



### 사전 요구 사항

Tier-1 논리적 라우터가 구성되어 있는지 확인합니다. [Tier-1 논리적 라우터 생성](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 **네트워킹 > 로드 밸런서 > 추가**를 선택합니다.



- 3 로드 밸런서의 이름과 설명을 입력합니다.
- 4 사용 가능한 리소스를 기반으로 로드 밸런서 가상 서버 크기와 풀 멤버의 수를 선택합니다.
- 5 드롭다운 메뉴에서 오류 로그의 심각도 수준을 정의합니다.

로드 밸런서는 다양한 심각도 수준의 발생한 문제에 대한 정보를 오류 로그에 수집합니다.

- 6 **확인**을 클릭합니다.
- 7 새로 생성된 로드 밸런서를 가상 서버에 연결합니다.
  - a 로드 밸런서 선택하고 **작업 > 가상 서버에 연결**을 클릭합니다.
  - b 드롭다운 메뉴에서 기존 가상 서버를 선택합니다.
  - c **확인**을 클릭합니다.
- 8 새로 생성된 로드 밸런서를 Tier-1 논리적 라우터에 연결합니다.
  - a 로드 밸런서를 선택하고 **작업 > 논리적 라우터에 연결**을 클릭합니다.
  - b 드롭다운 메뉴에서 기존 Tier-1 논리적 라우터를 선택합니다.

Tier-1 라우터는 활성-대기 모드여야 합니다.

  - c **확인**을 클릭합니다.
- 9 (선택 사항) 로드 밸런서를 삭제합니다.

로드 밸런서를 더 이상 사용하지 않으려면, 먼저 가상 서버와 Tier-1 논리적 라우터에서 로드 밸런서를 분리해야 합니다.

## 액티브 상태 모니터 구성

액티브 상태 모니터는 서버가 사용 가능한지 여부를 테스트하는 데 사용됩니다. 액티브 상태 모니터는 서버에 기본 ping을 보내거나 애플리케이션 상태를 모니터링하기 위해 고급 HTTP 요청을 보내는 등 여러 유형의 테스트를 사용합니다.

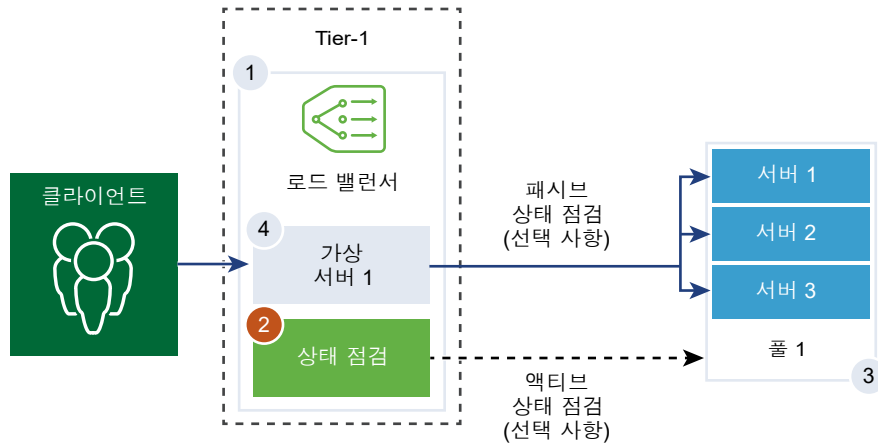
특정 기간 내에 응답하지 못하거나 오류로 응답하는 서버는 후속 정기 상태 점검에서 해당 서버가 정상으로 확인될 때까지 향후 연결 처리에서 제외됩니다.

풀 멤버가 가상 서버에 연결되고 이 가상 서버가 Tier-1 논리적 라우터에 연결된 후 서버 풀 멤버에 액티브 상태 점검이 수행됩니다. Tier-1 업링크 IP 주소는 상태 점검에 사용됩니다.

---

**참고** 서버 풀마다 하나의 액티브 상태 모니터를 구성할 수 있습니다.

---



### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 **로드 밸런서 > 네트워킹 > 모니터 > 액티브 상태 모니터 > 추가**를 선택합니다.
- 3 액티브 상태 모니터에 대한 설명과 이름을 입력합니다.
- 4 드롭다운 메뉴에서 서버의 상태 점검 프로토콜을 선택합니다.

NSX Manager; http-monitor, https-monitor, icmp-monitor, Tcp-monitor 및 Udp-monitor에서 미리 정의된 프로토콜을 사용할 수도 있습니다.

- 5 모니터링 포트의 값을 설정합니다.
- 6 서비스 풀을 모니터링할 값을 구성합니다.

액티브 상태 모니터 기본값을 수락할 수도 있습니다.

옵션	설명
모니터링 간격	모니터가 서버에 또 다른 연결 요청을 보내는 시간을 초 단위로 설정합니다.
하락 카운트	값을 설정합니다. 연속 실패가 이 값에 도달하면 서버를 일시적으로 사용할 수 없는 것으로 간주됩니다.
상승 카운트	숫자를 설정합니다. 이 숫자에 해당하는 시간 초과 기간이 지나면 서버가 사용 가능한지 확인하기 위해 서버에 새 연결을 다시 시도합니다.
시간 초과 기간	서버를 [종료] 상태로 간주하기 전에 테스트할 시간을 설정합니다.

예를 들어 모니터링 간격을 5초 설정하고, 시간 초과를 15초로 설정하면 로드 밸런서가 5초마다 서버에 요청을 보냅니다. 각 탐색에서 예상된 응답이 15초 내에 서버에서 수신되면 상태 점검 결과는 [정상]입니다. 그렇지 않으면 결과는 [위험]입니다. 최근 3개의 상태 점검 결과가 모두 [실행 중]이면 서버는 [실행 중]으로 표시됩니다.

## 7 HTTP를 상태 점검 프로토콜로 선택한 경우, 다음 세부 정보를 모두 입력합니다.

옵션	설명
<b>HTTP 메서드</b>	드롭다운 메뉴에서 서버 상태를 감지할 메서드를 GET, OPTIONS, POST, HEAD 및 PUT 중에 선택합니다.
<b>HTTP 요청 URL</b>	메서드에 대한 요청 URI를 입력합니다.
<b>HTTP 요청 버전</b>	드롭다운 메뉴에서 지원되는 요청 버전을 선택합니다. 기본 버전인 HTTP_VERSION_1_1을 수락할 수도 있습니다.
<b>HTTP 요청 본문</b>	요청 본문을 입력합니다. POST 및 PUT 메서드에 유효합니다.
<b>HTTP 응답 코드</b>	모니터가 HTTP 응답 본문의 상태 줄에서 일치할 것으로 예상하는 문자열을 입력합니다. 응답 코드는 쉼표로 구분된 목록입니다. 예: 200,301,302,401.
<b>HTTP 응답 본문</b>	HTTP 응답 본문 문자열과 HTTP 상태 점검 응답 본문이 일치하면 서버는 정상으로 간주됩니다.

## 8 HTTPS를 상태 점검 프로토콜로 선택한 경우, 다음 세부 정보를 모두 입력합니다.

### a SSL 프로토콜 목록을 선택합니다.

TLS 버전 TLS1.1 및 TLS1.2는 기본적으로 지원되고 사용하도록 설정됩니다. TLS1.0은 지원되지만 기본적으로 사용되지 않도록 설정됩니다.

### b 화살표를 클릭하고 프로토콜을 선택한 섹션으로 이동합니다.

### c 기본 SSL 암호를 할당하거나 사용자 지정 SSL 암호를 생성합니다.

### d 상태 점검 프로토콜로 HTTP에 대한 다음 세부 정보를 완료합니다.

옵션	설명
<b>HTTP 메서드</b>	드롭다운 메뉴에서 서버 상태를 감지할 메서드를 GET, OPTIONS, POST, HEAD 및 PUT 중에 선택합니다.
<b>HTTP 요청 URL</b>	메서드에 대한 요청 URI를 입력합니다.
<b>HTTP 요청 버전</b>	드롭다운 메뉴에서 지원되는 요청 버전을 선택합니다. 기본 버전인 HTTP_VERSION_1_1을 수락할 수도 있습니다.
<b>HTTP 요청 본문</b>	요청 본문을 입력합니다. POST 및 PUT 메서드에 유효합니다.
<b>HTTP 응답 코드</b>	모니터가 HTTP 응답 본문의 상태 줄에서 일치할 것으로 예상하는 문자열을 입력합니다. 응답 코드는 쉼표로 구분된 목록입니다. 예: 200,301,302,401.
<b>HTTP 응답 본문</b>	HTTP 응답 본문 문자열과 HTTP 상태 점검 응답 본문이 일치하면 서버는 정상으로 간주됩니다.

## 9 ICMP를 상태 점검 프로토콜로 선택한 경우 ICMP 상태 점검 패킷의 데이터 크기를 바이트 단위로 할당합니다.

**10** TCP를 상태 점검 프로토콜로 선택한 경우 매개 변수를 비워둘 수 있습니다.

전송되는 데이터와 예상되는 데이터가 모두 나열되지 않으면 서버 상태를 검사하기 위해 3방향 핸드셰이크 TCP 연결이 설정됩니다. 데이터가 전송되지 않습니다. 예상되는 데이터가 나열되는 경우 문자열이어야 하며 응답의 어느 위치에나 있을 수 있습니다. 정규식은 지원되지 않습니다.

**11** UDP를 상태 점검 프로토콜로 선택한 경우, 다음 세부 정보를 모두 입력합니다.

필수 옵션	설명
전송된 UDP 데이터	연결이 설정된 후 서버에 보낼 문자열을 입력합니다.
예상 UDP 데이터	서버에서 수신할 것으로 예상되는 문자열을 입력합니다. 수신된 문자열이 이 정의와 일치할 때에만 서버가 작동 상태인 것으로 간주됩니다.

**12** 완료 버튼을 클릭합니다.

다음에 수행할 작업

액티브 상태 모니터를 서버 풀과 연결합니다. [로드 밸런싱을 위한 서버 풀 추가](#)의 내용을 참조하십시오.

## 패시브 상태 모니터 구성

로드 밸런서는 패시브 상태 점검을 수행하여 클라이언트 연결 중 오류를 모니터링하고 일관된 장애를 유발하는 서버를 [종료] 상태로 표시합니다.

패시브 상태 점검은 로드 밸런서를 통과하는 클라이언트 트래픽에 장애가 있는지 모니터링합니다. 예를 들어 풀 멤버가 클라이언트 연결에 대한 응답으로 TCP Reset(RST)을 보내면 로드 밸런서는 해당 장애를 감지합니다. 다수의 연속된 장애가 발생하면 로드 밸런서는 해당 서버 풀 멤버를 일시적으로 사용할 수 없다고 간주하고 얼마 동안 해당 풀 멤버에 연결 요청 보내기를 중지합니다. 어느 정도 시간이 지나면 로드 밸런서는 풀 멤버가 복구되었는지 확인하기 위해 연결 요청을 보냅니다. 연결이 성공하면 풀 멤버가 정상으로 간주됩니다. 그렇지 않으면 로드 밸런서가 잠시 기다렸다가 다시 시도합니다.

패시브 상태 점검은 다음 시나리오를 클라이언트 트래픽의 장애로 간주합니다.

- 계층 7 가상 서버와 연결된 서버 풀에서, 풀 멤버에 연결이 실패하는 경우. 예를 들어 로드 밸런서가 로드 밸런서 사이에 SSL 핸드셰이크를 수행하거나 연결하려고 할 때 풀 멤버가 TCP RST를 보내면 풀 멤버에 장애가 발생합니다.
- 계층 4 TCP 가상 서버와 연결된 서버 풀에서, 풀 멤버가 클라이언트 TCP SYN에 대한 응답으로 TCP RST를 보내거나 전혀 응답하지 않는 경우.
- 계층 4 UDP 가상 서버와 연결된 서버 풀에서, 포트에 도달할 수 없거나 클라이언트 UDP 패킷에 대한 응답으로 대상에 도달할 수 없는 ICMP 오류 메시지가 수신되는 경우.

계층 7 가상 서버와 연결된 서버 풀, 실패한 연결 수는 TCP 연결 오류(예: TCP RST 데이터 전송 실패 또는 SSL 핸드셰이크 실패)가 있으면 증가합니다.

계층 4 가상 서버와 연결된 서버 풀, 서버 풀 멤버에 보낸 TCP SYN에 응답이 수신되지 않거나 TCP SYN에 대한 응답으로 TCP RST가 수신되면 서버 풀 멤버가 [종료] 상태로 간주됩니다. 실패 수가 증가합니다.

계층 4 UDP 가상 서버의 경우, ICMP 오류(예: 클라이언트 트래픽에 대한 응답으로 포트나 대상에 도달할 수 없는 메시지)가 수신되면 [종료] 상태로 간주됩니다.

**참고** 서버 풀마다 하나의 패시브 상태 모니터를 구성할 수 있습니다.

#### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 **네트워킹 > 로드 밸런서 > 모니터 > 패시브 상태 모니터 > 추가**를 선택합니다.
- 3 패시브 상태 모니터에 대한 설명과 이름을 입력합니다.
- 4 서비스 풀을 모니터링할 값을 구성합니다.  
액티브 상태 모니터 기본값을 수락할 수도 있습니다.

옵션	설명
하락 카운트	값을 설정합니다. 연속 실패가 이 값에 도달하면 서버를 일시적으로 사용할 수 없는 것으로 간주됩니다.
시간 초과 기간	서버를 [종료] 상태로 간주하기 전에 테스트할 시간을 설정합니다.

예를 들어 연속 실패가 구성된 값 5에 도달하면 해당 멤버는 5초 동안 일시적으로 사용할 수 없는 것으로 간주됩니다. 이 시간이 지나면 해당 멤버에 새 연결을 다시 시도하여 사용이 가능한지 확인합니다. 연결이 성공하면 멤버는 사용이 가능한 것으로 간주되고 실패 수는 0으로 설정됩니다. 하지만 연결에 실패하면 시간 초과 간격인 5초 동안 추가적으로 사용되지 않습니다.

#### 5 확인을 클릭합니다.

#### 다음에 수행할 작업

패시브 상태 모니터를 서버 풀과 연결합니다. [로드 밸런싱을 위한 서버 풀 추가](#)의 내용을 참조하십시오.

## 로드 밸런싱을 위한 서버 풀 추가

서버 풀은 동일한 응용 프로그램을 구성하고 실행하는 하나 이상의 서버로 구성됩니다. 하나의 풀은 계층 4 및 계층 7 가상 서버 모두에 연결할 수 있습니다.

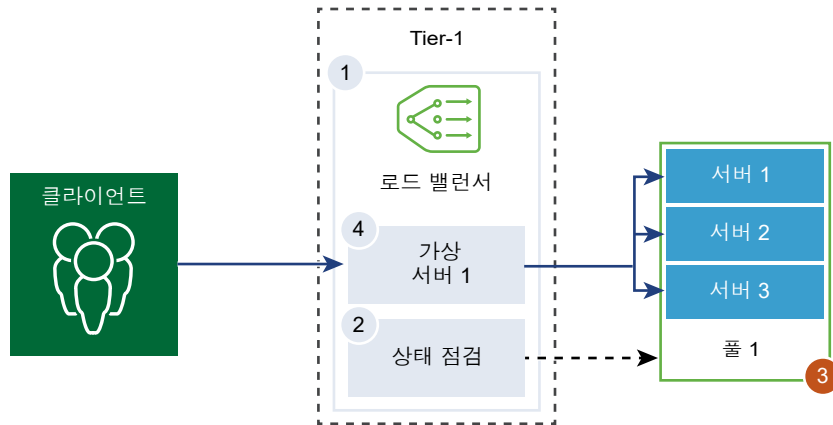
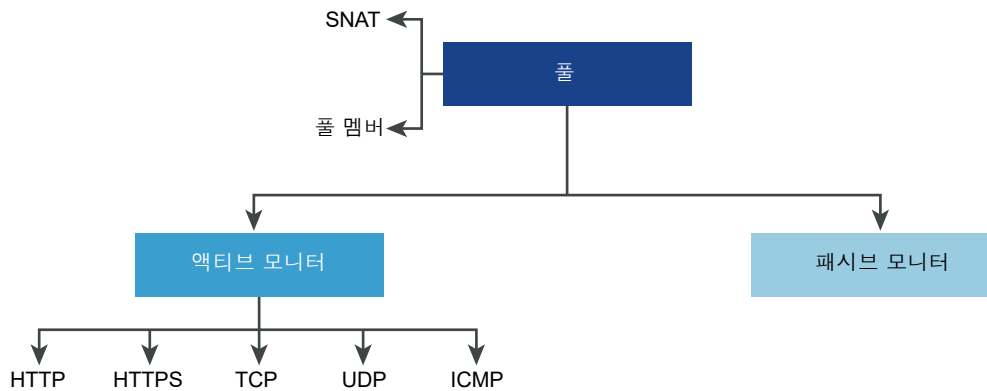


그림 10-1. 서버 풀 매개 변수 구성



#### 사전 요구 사항

- 동적 풀 멤버를 사용하는 경우 NSGroup을 구성해야 합니다. [NSGroup 생성](#)의 내용을 참조하십시오.
- 사용하는 모니터링에 따라 액티브 또는 패시브 상태 모니터가 구성되어 있는지 확인합니다. [액티브 상태 모니터 구성](#) 또는 [패시브 상태 모니터 구성](#)의 내용을 참조하십시오.

#### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 **네트워킹 > 로드 밸런서 > 서버 풀 > 추가**를 선택합니다.
- 3 로드 밸런서 풀에 대한 설명과 이름을 입력합니다.  
선택적으로 서버 풀에서 관리하는 연결을 설명할 수 있습니다.
- 4 서버 풀에 대한 알고리즘 밸런싱 메서드를 선택합니다.  
로드 밸런싱 알고리즘은 들어오는 연결이 멤버 사이에 분산되는 방식을 제어합니다. 이 알고리즘은 서버 풀이나 서버에서 직접 사용할 수 있습니다.

모든 로드 밸런싱 알고리즘은 다음 조건 중 하나라도 충족하는 서버를 건너뛵니다.

- 관리 상태가 [사용 안 함]으로 설정되어 있음
- 관리 상태가 [정상적으로 사용 안 함]으로 설정되어 있고 일치하는 지속성 항목이 없음
- 액티브 또는 패시브 상태 점검 상태가 [종료]임
- 서버 풀 최대 동시 연결에 대한 연결 제한에 도달했습니다.

옵션	설명
<b>ROUND_ROBIN</b>	들어오는 클라이언트 요청이 요청을 처리할 수 있는 사용 가능한 서버 목록을 통해 순환됩니다. 서버 풀 멤버 가중치가 구성되어 있어도 무시합니다.
<b>WEIGHTED_ROUND_ROBIN</b>	각 서버에 풀의 다른 서버에 비해 해당 서버가 어떻게 수행하는지를 나타내는 가중치 값이 할당됩니다. 이 값은 풀에 있는 다른 서버에 비해 서버에 전송되는 클라이언트 요청 수를 결정합니다. 이 로드 밸런싱 알고리즘은 사용 가능한 서버 리소스간에로드를 균등하게 분산하는 데 중점을 둡니다.
<b>LEAST_CONNECTION</b>	서버에 이미 있는 연결 수를 기반으로 하여 클라이언트 요청을 여러 서버로 분산합니다. 새 연결은 연결 수가 가장 적은 서버로 전송됩니다. 서버 풀 멤버 가중치가 구성되어 있어도 무시합니다.
<b>WEIGHTED_LEAST_CONNECTION</b>	각 서버에 풀의 다른 서버에 비해 해당 서버가 어떻게 수행하는지를 나타내는 가중치 값이 할당됩니다. 이 값은 풀에 있는 다른 서버에 비해 서버에 전송되는 클라이언트 요청 수를 결정합니다. 이 로드 밸런싱 알고리즘은 가중치 값을 사용하여 사용 가능한 서버 리소스 간에로드를 균등하게 분산하는 데 중점을 둡니다. 기본적으로 가중치 값은 해당 값이 구성되지 않았으며 느린 시작이 사용되도록 설정된 경우 1입니다.
<b>IP-HASH</b>	소스 IP 주소의 해시와 실행 중인 모든 서버의 총 가중치에 따라 서버를 선택합니다.

## 5 [TCP 멀티플렉싱] 버튼을 전환하여 이 메뉴 항목을 사용하도록 설정합니다.

TCP 멀티플렉싱을 통해 로드 밸런서와 서버 간에 동일한 TCP 연결을 사용하여 서로 다른 클라이언트 TCP 연결에서 여러 클라이언트 요청을 보낼 수 있습니다.

## 6 나중에 클라이언트 요청을 보내기 위해 활성으로 유지되는 풀당 최대 TCP 멀티플렉싱 연결 수를 설정합니다.

## 7 SNAT(소스 NAT) 모드를 선택합니다.

토폴로지에 따라, 로드 밸런서가 클라이언트로 향하는 서버의 트래픽을 수신하기 위해 SNAT가 필요할 수 있습니다. SNAT는 서버 풀별로 사용하도록 설정할 수 있습니다.

모드	설명
투명 모드	로드 밸런서는 서버에 연결을 설정하는 동안 클라이언트 IP 주소 및 포트 스누핑을 사용합니다. SNAT가 필요하지 않습니다.
자동 맵 모드	로드 밸런서는 인터페이스 IP 주소 및 사용 후 삭제 포트를 사용하여 서버의 설정된 수신 포트 중 하나에 처음에 연결된 클라이언트와 통신을 계속합니다. SNAT가 필요합니다. SNAT 프로세스가 수행된 후 튜플(소스 IP, 소스 포트, 대상 IP, 대상 포트 및 IP 프로토콜)이 고유한 경우 동일한 SNAT IP 및 포트를 여러 연결에 사용할 수 있도록 포트 오버로드를 사용하도록 설정합니다. 또한 포트 오버로드 팩터를 설정하여 여러 연결에 동시에 포트를 사용할 수 있는 최대 횟수를 허용할 수 있습니다.
IP 목록 모드	풀의 서버 중 하나에 연결할 때 SNAT에 사용할 단일 IP 주소 범위(예: 1.1.1.1-1.1.1.10)를 지정합니다. 기본적으로 4000~64000 포트 범위는 구성된 모든 SNAT IP 주소에 사용됩니다. 1000~4000 포트 범위는 Linux 애플리케이션에서 시작된 연결 및 상태 점검과 같은 용도로 예약되어 있습니다. IP 주소가 여러 개 있으면 라운드 로빈 방식으로 선택됩니다. SNAT 프로세스가 수행된 후 튜플(소스 IP, 소스 포트, 대상 IP, 대상 포트 및 IP 프로토콜)이 고유한 경우 동일한 SNAT IP 및 포트를 여러 연결에 사용할 수 있도록 포트 오버로드를 사용하도록 설정합니다. 또한 포트 오버로드 팩터를 설정하여 여러 연결에 동시에 포트를 사용할 수 있는 최대 횟수를 허용할 수 있습니다.

## 8 서버 풀 멤버를 선택합니다.

서버 풀은 단일 또는 여러 풀 멤버로 구성됩니다. 각 풀 멤버에는 IP 주소와 포트가 있습니다.

각 서버 풀 멤버에는 로드 밸런싱 알고리즘에 사용할 가중치를 구성할 수 있습니다. 가중치는 동일한 풀에 있는 다른 구성원에 비해 지정된 풀 멤버가 처리 할 수 있는 로드 양을 나타냅니다.

백업 멤버로 풀 멤버 지정은 상태 모니터와 작동하여 액티브/대기 상태를 제공합니다. 트래픽 폐일 오버는 활성 멤버가 상태 점검을 실패하는 경우 백업 멤버에 대해 발생합니다.

옵션	설명
정적	추가를 클릭하여 정적 풀 멤버를 포함합니다. 기존의 정적 풀 멤버를 복제할 수도 있습니다.
동적	드롭다운 메뉴에서 NSGroup을 선택합니다. 서버 풀 멤버 자격 조건이 그룹에 정의됩니다. 선택적으로 최대 그룹 IP 주소 목록을 정의할 수 있습니다.

## 9 서버 풀이 항상 유지해야 하는 활성 멤버의 최소 수를 입력합니다.

## 10 드롭다운 메뉴에서 서버 풀에 대한 액티브 및 패시브 상태 모니터를 선택합니다.



11 완료를 클릭합니다.

## 가상 서버 구성 요소 구성

가상 서버에는 구성할 수 있는 구성 요소(예: 애플리케이션 프로파일, 영구 프로파일 및 로드 밸런서 규칙)가 몇 가지 있습니다.

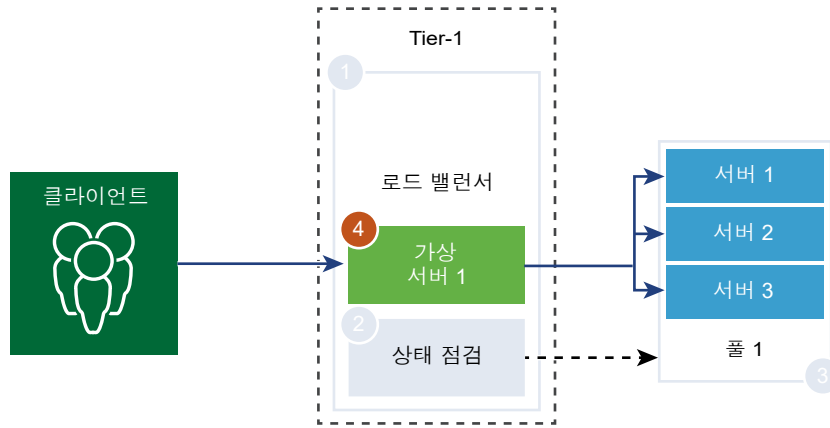
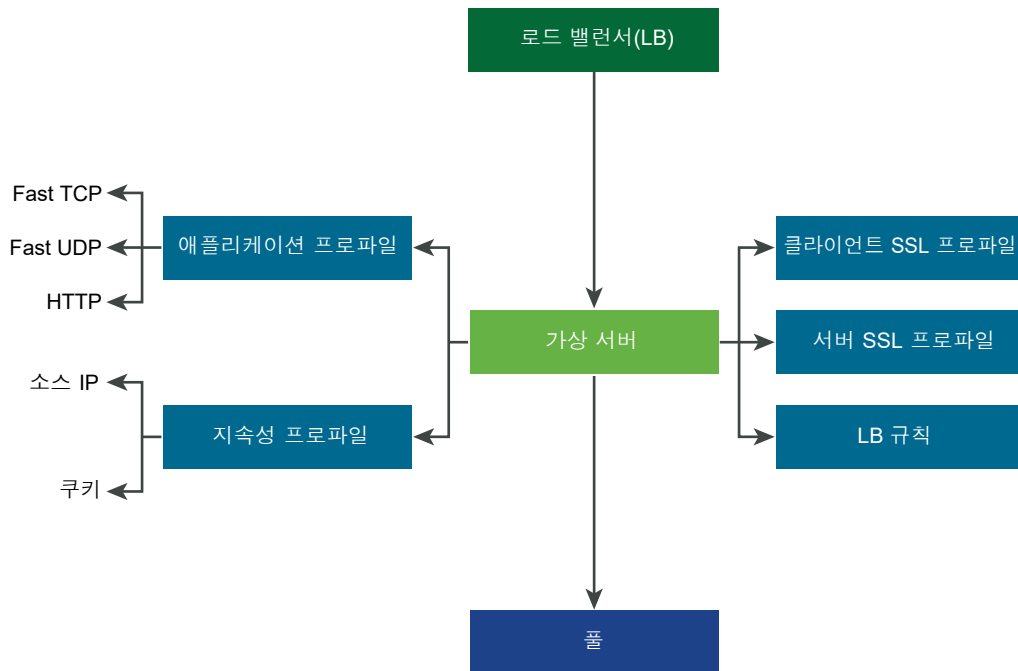


그림 10-2. 가상 서버 구성 요소



## 애플리케이션 프로파일 구성

애플리케이션 프로파일은 가상 서버와 연결되어 로드 밸런싱 네트워크 트래픽을 향상시키고 트래픽 관리 작업을 간소화합니다.

애플리케이션 프로파일은 특정 유형의 네트워크 트래픽 동작을 정의합니다. 연결된 가상 서버는 애플리케이션 프로파일에 지정된 값에 따라 네트워크 트래픽을 처리합니다. 빠른 TCP, 빠른 UDP 및 HTTP 애플리케이션 프로파일은 지원되는 프로파일 유형입니다.

TCP 애플리케이션 프로파일은 가상 서버에 연결된 애플리케이션 프로파일이 없는 경우 기본적으로 사용됩니다. TCP 및 UDP 애플리케이션 프로파일은 TCP나 UDP 프로토콜에서 애플리케이션이 실행 중이고 HTTP URL 로드 밸런싱과 같은 애플리케이션 수준의 로드 밸런싱이 필요하지 않은 경우에 사용됩니다. 이러한 프로파일은 성능이 빠르고 연결 미러링을 지원하는 계층 4 로드 밸런싱만 필요한 경우에도 사용됩니다.

HTTP 애플리케이션 프로파일은 로드 밸런서가 계층 7을 기반으로 작업을 수행해야 하는 경우(예: 모든 이미지 요청을 특정 서버 풀 멤버에 로드 밸런싱하거나 풀 멤버에서 SSL을 오프로드하기 위해 HTTPS를 종료하는 경우) HTTP 및 HTTPS 애플리케이션 모두에 사용됩니다. TCP 애플리케이션 프로파일과 달리 HTTP 애플리케이션 프로파일은 서버 풀 멤버를 선택하기 전에 클라이언트 TCP 연결을 종료합니다.

그림 10-3. 계층 4 TCP 및 UDP 애플리케이션 프로파일

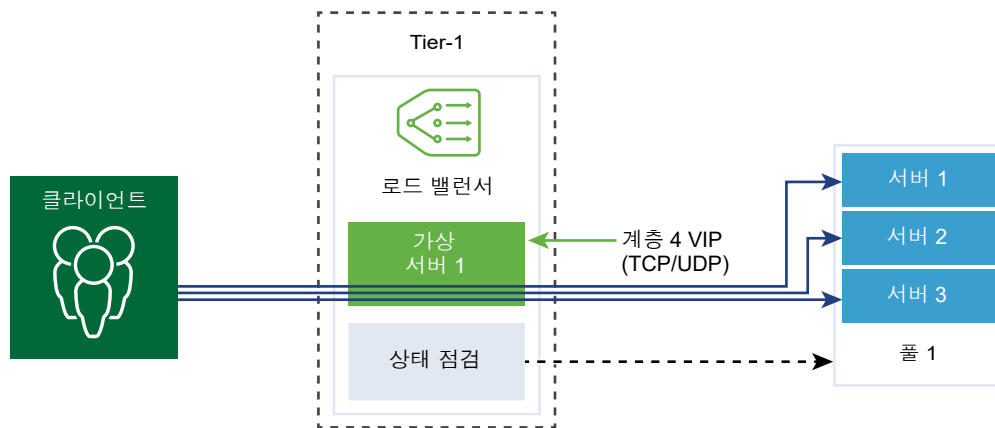
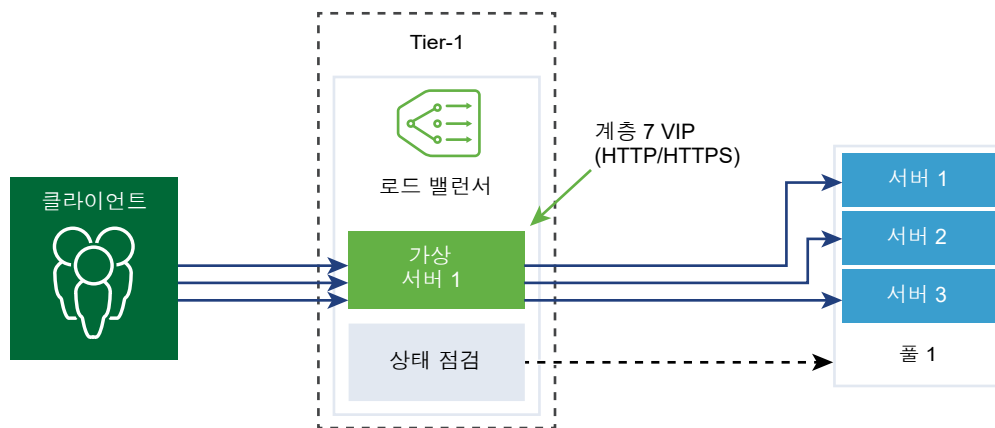


그림 10-4. 계층 7 HTTPS 애플리케이션 프로파일



#### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 **네트워킹 > 로드 밸런서 > 프로파일 > 애플리케이션 프로파일**을 선택합니다.

**3 빠른 TCP 애플리케이션 프로파일을 생성합니다.**

- 드롭다운 메뉴에서 **추가 > 빠른 TCP 프로파일**을 선택합니다.
- 빠른 TCP 애플리케이션 프로파일에 대한 설명과 이름을 입력합니다.
- 애플리케이션 프로파일 세부 정보를 모두 입력합니다.

빠른 TCP 프로파일 설정 기본값을 수락할 수도 있습니다.

옵션	설명
<b>연결 유휴 시간 제한</b>	TCP 연결이 설정된 후 서버가 유휴 상태로 유지될 수 있는 시간을 초 단위로 입력합니다.  유휴 시간을 실제 애플리케이션 유휴 시간에 몇 초를 더 추가한 값으로 설정하여 애플리케이션이 연결을 닫기 전에 로드 밸런서가 연결을 닫지 않도록 합니다.
<b>연결 닫기 시간 제한</b>	연결을 닫기 전에 TCP 연결(두 핀 또는 RST)이 애플리케이션에 대해 유지되어야 하는 시간을 초 단위로 입력합니다.  빠른 연결 속도를 지원하려면 닫기 시간 제한이 짧아야 할 수 있습니다.
<b>HA 흐름 미러링</b>	버튼을 전환하여 연결된 가상 서버에 대한 모든 흐름을 HA 대기 노드로 미러링합니다.

- 확인**을 클릭합니다.

**4 빠른 UDP 애플리케이션 프로파일을 생성합니다.**

UDP 프로파일 설정 기본값을 수락할 수도 있습니다.

- 드롭다운 메뉴에서 **추가 > 빠른 UDP 프로파일**을 선택합니다.
- 빠른 UDP 애플리케이션 프로파일에 대한 설명과 이름을 입력합니다.
- 애플리케이션 프로파일 세부 정보를 모두 입력합니다.

옵션	설명
<b>유휴 시간 제한</b>	UDP 연결이 설정된 후 서버가 유휴 상태로 유지될 수 있는 시간을 초 단위로 입력합니다.  UDP는 연결이 없는 프로토콜입니다. 로드 밸런싱을 위해 흐름 서명이 동일한 모든 UDP 패킷(예: 유휴 시간 제한 기간 내에 수신한 소스 및 대상 IP 주소 또는 포트 및 IP 프로토콜)은 동일한 연결에 속하는 것으로 간주되고 동일한 서버로 전송됩니다.  유휴 시간 제한 기간 동안 패킷이 수신되지 않으면, 흐름 서명과 선택된 서버 간의 연결이 닫힙니다.
<b>HA 흐름 미러링</b>	버튼을 전환하여 연결된 가상 서버에 대한 모든 흐름을 HA 대기 노드로 미러링합니다.

- 확인**을 클릭합니다.

**5 HTTP 애플리케이션 프로파일을 생성합니다.**

HTTP 프로파일 설정 기본값을 수락할 수도 있습니다.

HTTP 애플리케이션 프로파일은 HTTP 및 HTTPS 애플리케이션 모두에 사용됩니다.

- a 드롭다운 메뉴에서 **추가 > 빠른 HTTP 프로파일**을 선택합니다.
- b HTTP 애플리케이션 프로파일에 대한 설명과 이름을 입력합니다.

## C 애플리케이션 프로파일 세부 정보를 모두 입력합니다.

옵션	설명
<b>리디렉션</b>	<ul style="list-style-type: none"> <li>■ 없음 - 웹 사이트가 일시적으로 다운된 경우 페이지를 찾을 수 없음 오류 메시지가 사용자에게 표시됩니다.</li> <li>■ HTTP 리디렉션 - 웹 사이트가 일시적으로 다운되었거나 이동된 경우 해당 가상 서버에 들어오는 요청이 여기에 지정된 URL로 일시적으로 리디렉션될 수 있습니다. 정적 리디렉션만 지원됩니다.</li> </ul> <p>예를 들어 HTTP 리디렉션이 <code>http://sitedown.abc.com/sorry.html</code>로 설정되면 실제 요청(예: <code>http://original_app.site.com/home.html</code> 또는 <code>http://original_app.site.com/somepage.html</code>)에 관계없이, 원래 웹 사이트가 다운되었을 때 들어오는 요청은 지정된 URL로 리디렉션됩니다.</p> <ul style="list-style-type: none"> <li>■ HTTP에서 HTTPS로 리디렉션 - 특정 보안 애플리케이션은 SSL을 통한 통신을 강제 적용할 수 있지만 비 SSL 연결을 거부하는 대신 SSL을 사용하도록 클라이언트 요청을 리디렉션할 수 있습니다. HTTP에서 HTTPS로 리디렉션을 사용하면 호스트와 URI 경로를 모두 보존하고 SSL을 사용하도록 클라이언트 요청을 리디렉션할 수 있습니다.</li> </ul> <p>HTTP에서 HTTPS로 리디렉션의 경우, HTTPS 가상 서버에 포트 443이 있어야 하며 동일한 로드 밸런서에 동일한 가상 서버 IP 주소를 구성해야 합니다.</p> <p>예를 들어 <code>http://app.com/path/page.html</code>에 대한 클라이언트 요청은 <code>https://app.com/path/page.html</code>로 리디렉션됩니다. 리디렉션하는 동안 호스트 이름이나 URI를 수정해야 하는 경우(예: <code>https://secure.app.com/path/page.html</code>로 리디렉션), 로드 밸런싱 규칙이 사용되어야 합니다.</p>
<b>XFF(X-Forwarded-For)</b>	<ul style="list-style-type: none"> <li>■ 삽입 - 들어오는 요청에 XFF HTTP 헤더가 없으면 로드 밸런서가 클라이언트 IP 주소로 새 XFF 헤더를 삽입합니다.</li> <li>■ 바꾸기 - 들어오는 요청에 XFF HTTP 헤더가 이미 있으면 로드 밸런서가 헤더를 바꿀 수 있습니다.</li> </ul> <p>웹 서버는 요청하는 클라이언트 IP 주소로 처리하는 각 요청을 기록합니다. 이러한 로그는 디버깅 및 분석 용도로 사용됩니다. 배포 토폴로지로 인해 로드 밸런서에 SNAT가 필요한 경우, 서버는 로깅 목적을 무효화하는 클라이언트 SNAT IP 주소를 사용합니다.</p> <p>한 가지 해결 방법으로, 원래 클라이언트 IP 주소로 XFF HTTP 헤더를 삽입하도록 로드 밸런서를 구성할 수 있습니다. 연결의 소스 IP 주소 대신 XFF 헤더의 IP 주소를 기록하도록 서버를 구성할 수 있습니다.</p>
<b>연결 유휴 시간 제한</b>	TCP 애플리케이션 프로파일에 구성해야 하는 TCP 소켓 설정 대신 HTTP 애플리케이션이 유휴 상태로 유지될 수 있는 시간을 초 단위로 입력합니다.
<b>요청 헤더 크기</b>	HTTP 요청 헤더를 저장하는 데 사용되는 최대 버퍼 크기를 바이트 단위로 지정합니다.
<b>NTLM 인증</b>	<p>TCP 멀티플렉싱을 끄고 HTTP 연결을 유지하도록 로드 밸런서 버튼을 전환합니다.</p> <p>NTLM은 HTTP를 통해 사용할 수 있는 인증 프로토콜입니다. NTLM 인증을 사용한 로드 밸런싱의 경우, NTLM 기반 애플리케이션을 호스팅하는 서버 풀에 대해 TCP 멀티플렉싱을 사용하지 않도록 설정해야 합니다. 그렇지 않으면 한 클라이언트의 자격 증명으로 설정된 서버 측 연결이 다른 클라이언트의 요청을 제공하는 데 잠재적으로 사용될 수 있습니다.</p>

옵션	설명
	<p>프로파일에 NTLM을 사용하도록 설정되어 있고 NTLM이 가상 서버에 연결되어 있고 서버 풀에 TCP 멀티플렉싱을 사용하도록 설정되어 있는 경우에는 NTLM이 우선합니다. 해당 가상 서버에 대해 TCP 멀티플렉싱이 수행되지 않습니다. 하지만 동일한 풀이 또 다른 비 NTLM 가상 서버에 연결되어 있으면 해당 가상 서버에 대한 연결에 TCP 멀티플렉싱을 사용할 수 있습니다.</p> <p>클라이언트에서 HTTP/1.0을 사용하면 로드 밸런서는 HTTP/1.1 프로토콜로 업그레이드되고 HTTP 연결 유지가 설정됩니다. 동일한 클라이언트 측 TCP 연결에서 수신된 모든 HTTP 요청은 재 인증이 필요하지 않도록 단일 TCP 연결을 통해 동일한 서버로 전송됩니다.</p>

d **확인**을 클릭합니다.

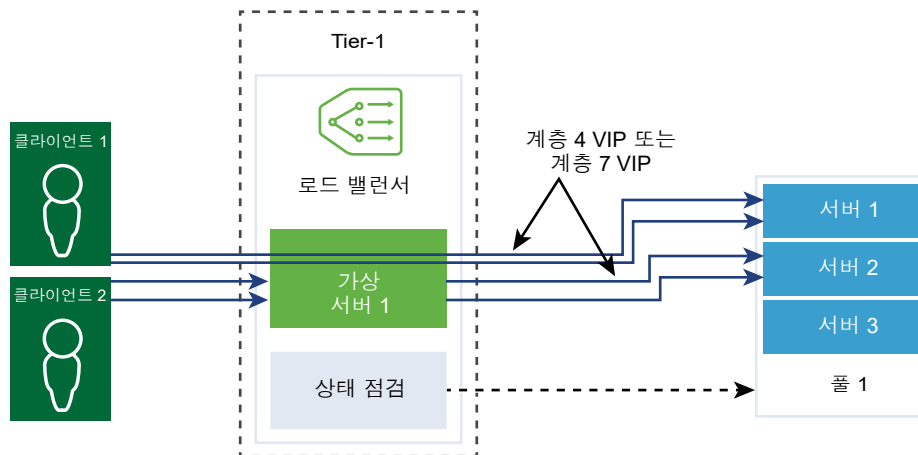
## 영구 프로파일 구성

상태 저장 애플리케이션의 안정성을 보장하기 위해 로드 밸런서는 관련된 모든 연결을 동일한 서버로 보내는 지속성을 구현합니다. 다양한 유형의 애플리케이션 요구 사항을 해결하기 위해 다양한 유형의 지속성이 지원됩니다.

일부 애플리케이션은 서버 상태(예: 쇼핑 카트)를 유지 보수합니다. 이러한 상태는 클라이언트마다 있을 수 있으며 클라이언트 IP 주소 또는 HTTP 세션별로 식별될 수 있습니다. 애플리케이션은 HTTP 세션 또는 동일한 클라이언트와 관련된 후속 연결을 처리하는 동안 이 상태에 액세스하거나 수정할 수 있습니다.

소스 IP 지속성 프로파일은 소스 IP 주소를 기반으로 세션을 추적합니다. 클라이언트가 소스 주소 지속성을 사용하는 가상 서버에 대한 연결을 요청하면, 로드 밸런서는 해당 클라이언트가 이전에 연결되었는지 확인하여 연결한 적이 있으면 클라이언트를 동일한 서버에 반환합니다. 그렇지 않으면 풀 로드 밸런싱 알고리즘을 기반으로 서버 풀 멤버를 선택할 수 있습니다. 소스 IP 지속성 프로파일은 계층 4 및 계층 7 가상 서버에 사용됩니다.

쿠키 지속성 프로파일은 클라이언트가 사이트에 처음 액세스할 때 세션을 식별하기 위해 고유한 쿠키를 삽입합니다. HTTP 쿠키는 후속 요청에서 클라이언트에 의해 전달되며 로드 밸런서는 해당 정보를 사용하여 쿠키 지속성을 제공합니다. 쿠키 지속성 프로파일은 계층 7 가상 서버에서만 사용할 수 있습니다.



## 절차

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

2 **네트워킹 > 로드 밸런서 > 프로파일 > 지속성 프로파일**을 선택합니다.

3 소스 IP 지속성 프로파일을 생성합니다.

- a 드롭다운 메뉴에서 **추가 > 소스 IP 지속성**을 선택합니다.
- b 소스 IP 지속성 프로파일에 대한 설명과 이름을 입력합니다.
- c 지속성 프로파일 세부 정보를 모두 입력합니다.

기본적인 소스 IP 프로파일 설정을 수락할 수도 있습니다.

옵션	설명
<b>지속성 공유</b>	이 프로파일과 연결된 모든 가상 서버가 지속성 테이블을 공유할 수 있도록 버튼을 전환하여 지속성을 공유합니다. 가상 서버와 연결된 소스 IP 지속성 프로파일에 지속성 공유를 사용하도록 설정되어 있지 않으면 프로파일이 연결되어 있는 각각의 가상 서버는 개인 지속성 테이블을 유지 보수합니다.
<b>지속성 항목 시간 초과</b>	지속성 만료 시간(초)을 입력합니다. 로드 밸런서 지속성 테이블은 클라이언트 요청이 동일한 서버로 전송되는 것을 기록하는 항목을 유지합니다. <ul style="list-style-type: none"> <li>■ 새 연결 요청이 시간 초과 기간 내에 동일한 클라이언트에서 수신되면 지속성 항목이 만료되어 삭제됩니다.</li> <li>■ 시간 초과 기간 내에 동일한 클라이언트의 새 연결 요청이 수신되면 타이머가 재설정되고 클라이언트 요청이 고정 풀 멤버로 전송됩니다.</li> </ul> 시간 초과 기간이 만료되면 로드 밸런싱 알고리즘에 의해 할당된 서버에 새 연결 요청이 전송됩니다. L7 로드 밸런싱 TCP 소스 IP 지속성 시나리오의 경우 기존 연결이 여전히 활성 상태라도 얼마간 새 TCP 연결이 생성되지 않으면 지속성 항목은 시간 초과됩니다.
<b>HA 지속성 미러링</b>	버튼을 전환하여 지속성 항목을 HA 피어와 동기화합니다.
<b>가득 차면 항목 제거</b>	지속성 테이블이 가득 차면 항목을 제거합니다. 시간 초과 값이 크면 트래픽이 과도할 경우 지속성 테이블이 빠르게 채워질 수 있습니다. 지속성 테이블이 채워지면 최신 항목을 수용하기 위해 가장 오래된 항목부터 삭제됩니다.

- d **확인**을 클릭합니다.

4 쿠키 지속성 프로파일을 생성합니다.

- a 드롭다운 메뉴에서 **추가 > 쿠키 지속성**을 선택합니다.
- b 쿠키 지속성 프로파일에 대한 설명과 이름을 입력합니다.

- c **지속성 공유** 버튼을 전환하여 동일한 풀 멤버와 연결된 여러 가상 서버에서 지속성을 공유합니다.

쿠키 지속성 프로파일은 `<name>.<profile-id>.<pool-id>` 형식으로 쿠키를 삽입합니다.

가상 서버와 연결된 쿠키 지속성 프로파일에서 공유된 지속성을 사용하도록 설정하지 않은 경우, 각 가상 서버에 대한 개인 쿠키 지속성이 사용되며 풀 멤버에 의해 자격이 부여됩니다. 로드 밸런서는 `<name>.<virtual_server_id>.<pool_id>` 형식으로 쿠키를 삽입합니다.

- d **다음**을 클릭합니다.
- e 지속성 프로파일 세부 정보를 모두 입력합니다.

옵션	설명
<b>쿠키 모드</b>	드롭다운 메뉴에서 모드를 선택합니다. <ul style="list-style-type: none"> <li>■ 삽입 - 세션을 식별하는 고유한 쿠키를 추가합니다.</li> <li>■ 접두사 - 기존 HTTP 쿠키 정보에 추가합니다.</li> <li>■ 재작성 - 기존 HTTP 쿠키 정보를 재작성합니다.</li> </ul>
<b>쿠키 이름</b>	쿠키 이름을 입력합니다.
<b>쿠키 도메인</b>	도메인 이름을 입력합니다. HTTP 쿠키 도메인은 삽입 모드에서만 구성 할 수 있습니다.
<b>쿠키 경로</b>	쿠키 URL 경로를 입력합니다. HTTP 쿠키 경로는 삽입 모드에서만 설정할 수 있습니다.
<b>쿠키 왜곡</b>	쿠키 서버 IP 주소 및 포트 정보를 암호화합니다. 버튼을 전환하여 암호화를 사용하지 않도록 설정합니다. 왜곡을 사용하지 않도록 설정하면 쿠키 서버 IP 주소 및 포트 정보가 일반 텍스트 형식입니다.
<b>쿠키 대체</b>	쿠키가 [사용 안 함] 또는 [종료] 상태인 서버를 가리키는 경우 클라이언트 요청을 처리할 새 서버를 선택합니다. 쿠키가 [사용 안 함] 또는 [종료] 상태인 서버를 가리키는 경우 클라이언트 요청이 거부되도록 버튼을 전환합니다.

- f 쿠키 만료 세부 정보를 모두 입력합니다.

옵션	설명
<b>쿠키 시간 유형</b>	드롭다운 메뉴에서 쿠키 시간 유형을 선택합니다. 브라우저가 닫히면 세션 쿠키 및 지속성 쿠키 유형 모두가 만료됩니다.
<b>최대 유효 시간</b>	쿠키가 만료되기 전에 쿠키가 유효 상태일 수 있는 시간(초 단위)을 입력합니다.

- g **완료**를 클릭합니다.



## SSL 프로파일 구성

SSL 프로파일은 애플리케이션 독립적인 SSL 속성(예: 암호 목록)을 구성하고 이 목록을 여러 애플리케이션에 재사용합니다. SSL 속성은 로드 밸런서가 클라이언트로 작동할 때와 서버로 작동할 때가 다르기 때문에 클라이언트 측 SSL 프로파일과 서버 측 SSL 프로파일이 별도로 지원됩니다.

**참고** NSX-T Data Center Limited Export 릴리스에서는 SSL 프로파일이 지원되지 않습니다.

클라이언트 측 SSL 프로파일은 SSL 서버로 작동하면서 클라이언트 SSL 연결을 종료하는 로드 밸런서를 나타냅니다. 서버 측 SSL 프로파일은 클라이언트로 작동하면서 서버에 대한 연결을 설정하는 로드 밸런서를 나타냅니다.

클라이언트 측 SSL 프로파일 및 서버 측 SSL 프로파일 모두에 암호 목록을 지정할 수 있습니다.

SSL 세션 캐싱을 사용하면 SSL 클라이언트와 서버가 이전에 협상된 보안 매개 변수를 재사용할 수 있어 SSL 핸드셰이크 중에 비용이 높은 공용 키 작업을 방지할 수 있습니다. SSL 세션 캐싱은 클라이언트 측과 서버 측에서 모두에서 기본적으로 사용하지 않도록 설정됩니다.

SSL 세션 티켓은 SSL 클라이언트와 서버가 이전에 협상된 세션 매개 변수를 재사용할 수 있도록 하는 대체 메커니즘입니다. SSL 세션 티켓에서 클라이언트와 서버는 핸드셰이크를 교환하는 동안 SSL 세션 티켓을 지원하는지 여부를 협상합니다. 둘 다 지원하는 경우 서버는 암호화된 SSL 세션 매개 변수가 포함된 SSL 티켓을 클라이언트에 보낼 수 있습니다. 클라이언트는 후속 연결에서 해당 티켓을 사용하여 세션을 재사용할 수 있습니다. SSL 세션 티켓은 클라이언트 쪽에서 사용하도록 설정되고 서버 쪽에서 사용하지 않도록 설정됩니다.

그림 10-5. SSL 오프로딩

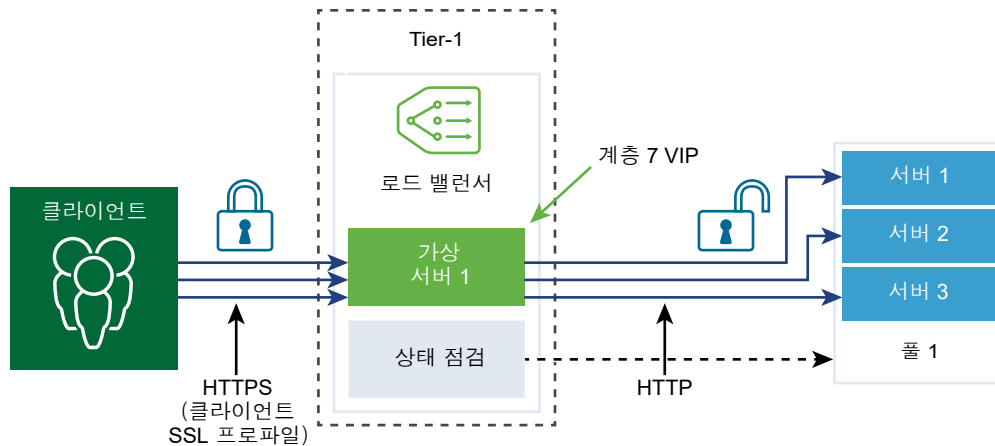
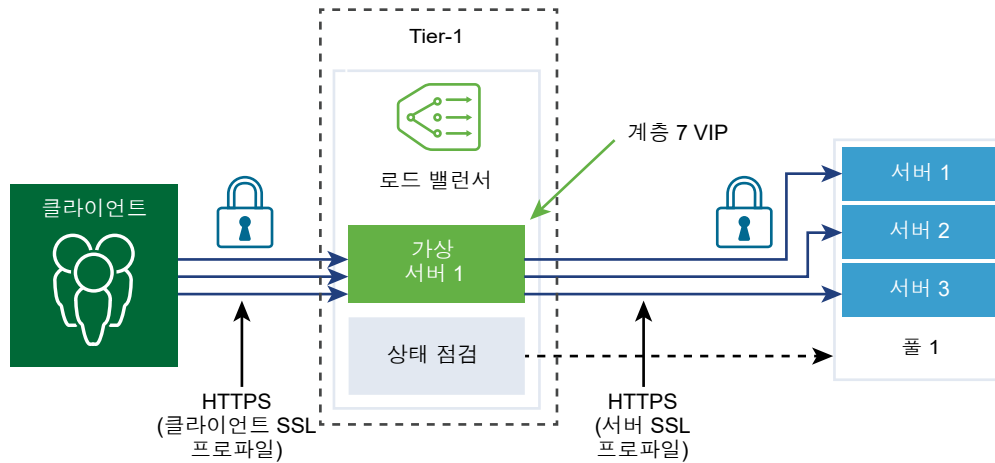


그림 10-6. 종단 간 SSL



## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 **네트워킹 > 로드 밸런서 > 프로파일 > SSL 프로파일**을 선택합니다.
- 3 클라이언트 SSL 프로파일을 생성합니다.
  - a 드롭다운 메뉴에서 **추가 > 클라이언트 측 SSL**을 선택합니다.
  - b 클라이언트 SSL 프로파일에 대한 설명과 이름을 입력합니다.
  - c 클라이언트 SSL 프로파일에 포함할 SSL 암호를 할당합니다.  
사용자 지정 SSL 암호를 생성할 수도 있습니다.
  - d 화살표를 클릭하여 암호를 [선택됨] 섹션으로 이동합니다.
  - e **프로토콜 및 세션** 탭을 클릭합니다.
  - f 클라이언트 SSL 프로파일에 포함할 SSL 프로토콜을 선택합니다.  
SSL 프로토콜 버전 TLS1.1 및 TLS1.2는 기본적으로 사용하도록 설정됩니다. TLS1.0도 지원되지만 기본적으로 사용하지 않도록 설정됩니다.
  - g 화살표를 클릭하여 프로토콜을 [선택됨] 섹션으로 이동합니다.

- h SSL 프로토콜 세부 정보를 모두 입력합니다.

SSL 프로파일 설정 기본값을 수락할 수도 있습니다.

옵션	설명
세션 캐싱	SSL 세션 캐싱을 사용하면 SSL 클라이언트와 서버가 이전에 협상된 보안 매개 변수를 재사용할 수 있어 SSL 핸드셰이크 중에 비용이 높은 공용 키 작업을 방지할 수 있습니다.
세션 캐시 항목 시간 초과	캐시 시간 초과를 초 단위로 입력하여 SSL 세션 매개 변수를 얼마나 오래 유지해야 하고 재사용할 수 있는지를 지정합니다.
기본 서버 암호	서버가 지원할 수 있는 목록에서 첫 번째로 지원되는 암호를 선택할 수 있도록 버튼을 전환합니다.  SSL 핸드셰이크 중에 클라이언트는 지원되는 암호의 순서가 지정된 목록을 서버에 전송합니다.

- i **확인**을 클릭합니다.

#### 4 서버 SSL 프로파일을 생성합니다.

- a 드롭다운 메뉴에서 **추가 > 서버 측 SSL**을 선택합니다.

- b 서버 SSL 프로파일에 대한 설명과 이름을 입력합니다.

- c 서버 SSL 프로파일에 포함할 SSL 암호를 선택합니다.

사용자 지정 SSL 암호를 생성할 수도 있습니다.

- d 화살표를 클릭하여 암호를 [선택됨] 섹션으로 이동합니다.

- e **프로토콜 및 세션** 탭을 클릭합니다.

- f 서버 SSL 프로파일에 포함할 SSL 프로토콜을 선택합니다.

SSL 프로토콜 버전 TLS1.1 및 TLS1.2는 기본적으로 사용하도록 설정됩니다. TLS1.0도 지원되지만 기본적으로 사용하지 않도록 설정됩니다.

- g 화살표를 클릭하여 프로토콜을 [선택됨] 섹션으로 이동합니다.

- h 세션 캐싱 설정 기본값을 수락합니다.

SSL 세션 캐싱을 사용하면 SSL 클라이언트와 서버가 이전에 협상된 보안 매개 변수를 재사용할 수 있어 SSL 핸드셰이크 중에 비용이 높은 공용 키 작업을 방지할 수 있습니다.

- i **확인**을 클릭합니다.

## 계층 4 가상 서버 구성

가상 서버는 모든 클라이언트 연결을 수신하여 서버에 배포합니다. 가상 서버에는 IP 주소, 포트 및 프로토콜이 있습니다. 계층 4 가상 서버의 경우, 단일 TCP 또는 UDP 포트 대신 포트 범위 목록을 지정하여 동적 포트에 복잡한 프로토콜을 지원할 수 있습니다.

계층 4 가상 서버는 기본 풀이라고도 하는 기본 서버 풀에 연결되어 있어야 합니다.

가상 서버 상태가 사용 안 함인 경우, 가상 서버에 대한 새로운 연결 시도는 TCP 연결에 대해 TCP RST 또는 UDP에 대해 ICMP 오류 메시지를 보내서 거부됩니다. 새 연결은 일치하는 지속성 항목이 있어도 거부됩니다. 활성 연결은 계속 처리됩니다. 가상 서버가 삭제되거나 로드 밸런서에서 연결이 끊어지면 해당 가상 서버에 대한 활성 연결이 실패합니다.

### 사전 요구 사항

- 애플리케이션 프로파일을 사용할 수 있는지 확인합니다. [애플리케이션 프로파일 구성](#)의 내용을 참조하십시오.
- 영구 프로파일을 사용할 수 있는지 확인합니다. [영구 프로파일 구성](#)의 내용을 참조하십시오.
- 클라이언트와 서버에 대한 SSL 프로파일을 사용할 수 있는지 확인합니다. [SSL 프로파일 구성](#)의 내용을 참조하십시오.
- 서버 풀을 사용할 수 있는지 확인합니다. [로드 밸런싱을 위한 서버 풀 추가](#)의 내용을 참조하십시오.

### 절차

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

- 2 **네트워킹 > 로드 밸런서 > 가상 서버 > 추가**를 선택합니다.

- 3 계층 4 가상 서버에 대한 설명과 이름을 입력합니다.

- 4 드롭다운 메뉴에서 계층 4 프로토콜을 선택합니다.

계층 4 가상 서버는 Fast TCP 또는 Fast UDP 프로토콜 중 하나를 지원하지만 둘 다 지원하지는 않습니다. 동일한 IP 주소 및 포트에 Fast TCP 또는 Fast UDP 프로토콜을 지원하려면(예: DNS) 각 프로토콜에 대해 가상 서버가 생성되어야 합니다.

프로토콜 유형을 기반으로, 기존 애플리케이션 프로파일이 자동으로 채워집니다.

- 5 액세스 로그 버튼을 전환하여 계층 4 가상 서버에 대한 로깅을 사용하도록 설정합니다.

- 6 **다음**을 클릭합니다.

- 7 가상 서버 IP 주소 및 포트 번호를 입력합니다.

가상 서버 포트 번호나 포트 범위를 입력할 수 있습니다.

- 8 고급 속성 세부 정보를 모두 입력합니다.

옵션	설명
<b>최대 동시 연결</b>	가상 서버가 동일한 로드 밸런서에서 호스팅되는 다른 애플리케이션의 리소스를 고갈시키지 않도록 가상 서버에 허용되는 최대 동시 연결 수를 설정합니다.
<b>최대 새 연결 속도</b>	가상 서버가 리소스를 고갈시키지 않도록 서버 풀 멤버에 대한 최대 새 연결을 설정합니다.
<b>기본 풀 멤버 포트</b>	가상 서버에 대한 풀 멤버 포트가 정의되지 않은 경우 기본 풀 멤버 포트를 입력합니다.  예를 들어, 가상 서버가 포트 범위 2000-2999로 정의되고 기본 풀 멤버 포트 범위가 8000-8999로 설정되면 가상 서버 포트 2500에 대해 들어오는 클라이언트 연결은 대상 포트가 8500으로 설정된 풀 멤버로 전송됩니다.

**9** 드롭다운 메뉴에서 기존 서버 풀을 선택합니다.

서버 풀은 유사하게 구성되고 동일한 애플리케이션을 실행하는 하나 이상의 서버로 구성되며, 이러한 서버를 풀 멤버라고도 합니다.

**10** 드롭다운 메뉴에서 기존 장애 서버 풀을 선택합니다.

장애 서버 풀은 로드 밸런서가 기본 풀에서의 요청을 처리할 백엔드 서버를 선택할 수 없는 경우 해당 요청을 처리합니다.

**11** 다음을 클릭합니다.**12** 드롭다운 메뉴에서 기존 지속성 프로파일을 선택합니다.

지속성 프로파일은 가상 서버에서 사용하도록 설정되어 관련 클라이언트 연결을 동일한 서버로 전송하도록 허용합니다.

**13** 완료를 클릭합니다.

## 계층 7 가상 서버 구성

가상 서버는 모든 클라이언트 연결을 수신하여 서버에 배포합니다. 가상 서버에는 IP 주소, 포트 및 TCP 프로토콜이 있습니다.

로드 밸런서 규칙은 HTTP 애플리케이션 프로파일인 계층 7 가상 서버에만 지원됩니다. 서로 다른 로드 밸런서 서비스는 로드 밸런서 규칙을 사용할 수 있습니다.

각 로드 밸런서 규칙은 단일 또는 여러 일치 조건 및 단일 또는 여러 작업으로 구성됩니다. 일치 조건을 지정하지 않으면 로드 밸런서 규칙이 항상 일치하여 기본 규칙을 정의하는 데 사용됩니다. 일치 조건이 둘 이상 지정되면 일치 전략은 로드 밸런서 규칙이 일치하는 것으로 간주되기 위해 모든 조건이 일치해야 하는지 또는 조건이 하나라도 일치해야 하는지를 결정해야 합니다.

각 로드 밸런서 규칙은 로드 밸런싱 프로세스의 특정 단계(HTTP 요청 재작성, HTTP 요청 전달 및 HTTP 응답 재작성)에서 구현됩니다. 모든 일치 조건과 작업이 각 단계에 적용될 수 있는 것은 아닙니다.

가상 서버 상태가 사용 안 함인 경우, 가상 서버에 대한 새로운 연결 시도는 TCP 연결에 대해 TCP RST 또는 UDP에 대해 ICMP 오류 메시지를 보내서 거부됩니다. 새 연결은 일치하는 지속성 항목이 있어도 거부됩니다. 활성 연결은 계속 처리됩니다. 가상 서버가 삭제되거나 로드 밸런서에서 연결이 끊어지면 해당 가상 서버에 대한 활성 연결이 실패합니다.

### 사전 요구 사항

- 애플리케이션 프로파일을 사용할 수 있는지 확인합니다. [애플리케이션 프로파일 구성](#)의 내용을 참조하십시오.
- 영구 프로파일을 사용할 수 있는지 확인합니다. [영구 프로파일 구성](#)의 내용을 참조하십시오.
- 클라이언트와 서버에 대한 SSL 프로파일을 사용할 수 있는지 확인합니다. [SSL 프로파일 구성](#)의 내용을 참조하십시오.
- 서버 풀을 사용할 수 있는지 확인합니다. [로드 밸런싱을 위한 서버 풀 추가](#)의 내용을 참조하십시오.
- CA 및 클라이언트 인증서를 사용할 수 있는지 확인합니다. [인증서 서명 요청 파일 생성](#)의 내용을 참조하십시오.

- CRL(인증 해지 목록)을 사용할 수 있는지 확인합니다. [인증서 해지 목록 가져오기](#)의 내용을 참조하십시오.
- **계층 7 가상 서버 풀 및 규칙 구성**  
계층 7 가상 서버를 사용하면 조건 또는 작업 규칙을 사용하여 로드 밸런서 규칙을 선택적으로 구성하고 로드 밸런싱 동작을 사용자 지정할 수 있습니다.
- **계층 7 가상 서버 로드 밸런싱 프로파일 구성**  
계층 7 가상 서버를 사용하면 로드 밸런서 지속성, 클라이언트 측 SSL 및 서버 측 SSL 프로파일을 선택적으로 구성할 수 있습니다.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 **네트워킹 > 로드 밸런서 > 가상 서버 > 추가**를 선택합니다.
- 3 계층 7 가상 서버에 대한 설명과 이름을 입력합니다.
- 4 계층 7 메뉴 항목을 선택합니다.  
계층 7 가상 서버는 HTTP 및 HTTPS 프로토콜을 지원합니다.  
기존 HTTP 애플리케이션 프로파일은 자동으로 채워집니다.
- 5 (선택 사항) **다음**을 클릭하여 서버 풀 및 로드 밸런싱 프로파일을 구성합니다.
- 6 **완료**를 클릭합니다.

## 계층 7 가상 서버 풀 및 규칙 구성

계층 7 가상 서버를 사용하면 조건 또는 작업 규칙을 사용하여 로드 밸런서 규칙을 선택적으로 구성하고 로드 밸런싱 동작을 사용자 지정할 수 있습니다.

로드 밸런서 규칙은 일치 유형에 대해 정규식을 지원합니다. PCRE 스타일 REGEX 패턴이 지원되지만 고급 사용 사례에 대한 몇 가지 제한 사항이 있습니다. REGEX가 일치 조건에서 사용되면 명명된 캡처링 그룹이 지원됩니다.

REGEX 제한에는 다음이 포함됩니다.

- 문자 공용 구조체 및 교차가 지원되지 않습니다. 예를 들어, `[a-z[0-9]]`와 `[a-z&&[aeiou]]` 대신 `[a-z0-9]`와 `[aeiou]`를 각각 사용하십시오.
- 9개의 역참조만 지원되며 참조를 위해 `\1`부터 `\9`까지 사용할 수 있습니다.
- `\ddd` 형식이 아닌 `\0dd` 형식을 사용하여 8진수 문자와 일치시킵니다.
- 내장형 플래그는 최상위 레벨에서 지원되지 않으며 그룹 내에서만 지원됩니다. 예를 들어 `"Case(?:s)ensitive"` 대신 `"Case((?:s)ensitive)"`를 사용하십시오.
- 전처리 작업 `\l`, `\u`, `\L`, `\U`가 지원되지 않습니다. 여기서 `\l` - 다음 문자 소문자, `\u` - 다음 문자 대문자, `\L` - `\E`까지 소문자, `\U` - `\E`까지 대문자입니다.
- `(?(condition)X)`, `(?{code})`, `(?{Code})` 및 `(?#comment)`는 지원되지 않습니다.

- 미리 정의된 유니코드 문자 클래스 \X는 지원되지 않습니다.
- 명명된 문자 구성을 유니 코드 문자에 사용하는 것이 지원되지 않습니다. 예를 들어 \N{name} 대신 \u2018을 사용합니다.

REGEX가 일치 조건에서 사용되면 명명된 캡처링 그룹이 지원됩니다. 예를 들어 REGEX 일치 패턴 `/news/(?<year>\d+)-(?(<month>\d+)-(?(<day>\d+))/(?(<article>.*))`을 사용하여 `/news/2018-06-15/news1234.html`과 같은 URI를 일치시킬 수 있습니다.

변수는 다음과 같이 설정됩니다. `$year = "2018" $month = "06" $day = "15" $article = "news1234.html"`. 변수가 설정된 후에는 이러한 변수를 로드 밸런서 규칙 작업에 사용할 수 있습니다. 예를 들어 `/news.py?year=$year&month=$month&day=$day&article=$article`과 같이 일치된 변수를 사용하여 URI를 다시 작성할 수 있습니다. 그러면 URI가 `/news.py?year=2018&month=06&day=15&article=news1234.html`로 다시 작성됩니다.

재작성 작업에는 명명된 캡처링 그룹과 기본 제공 변수의 조합을 사용할 수 있습니다. 예를 들어 URI가 `/news.py?year=$year&month=$month&day=$day&article=$article&user_ip=$_remote_addr`로 작성될 수 있습니다. 그러면 예제 URI가 `/news.py?year=2018&month=06&day=15&article=news1234.html&user_ip=1.1.1.1`로 재작성됩니다.

---

**참고** 명명된 캡처링 그룹의 경우 `_` 문자로 이름을 시작할 수 없습니다.

---

명명된 캡처링 그룹 외에도 다음과 같은 기본 제공 변수를 재작성 작업에 사용할 수 있습니다. 모든 기본 제공 변수 이름은 `_`로 시작합니다.

- `$_args` - 요청의 인수
- `$_cookie_<name>` - <name> 쿠키의 값
- `$_host` - 우선 순위에 따라 - 요청 라인의 호스트 이름 또는 "Host" 요청 헤더 필드의 호스트 이름 또는 요청과 일치하는 서버 이름
- `$_hostname` - 호스트 이름
- `$_http_<name>` - 임의 요청 헤더 필드이며 <name>은 소문자로 변환된 필드 이름이고 대시는 밑줄로 대체됨
- `$_https` - SSL 모드에서 연결이 작동하면 "on", 그렇지 않으면 ""
- `$_is_args` - 요청 라인에 인수가 있으면 "?", 그렇지 않으면 ""
- `$_query_string` - `$_args`와 동일
- `$_remote_addr` - 클라이언트 주소
- `$_remote_port` - 클라이언트 포트
- `$_request_uri` - 원래 요청 URI 전체(인수 포함)
- `$_scheme` - 요청 체계, "http" 또는 "https"
- `$_server_addr` - 요청을 수락한 서버의 주소
- `$_server_name` - 요청을 수락한 서버의 이름

- `$_server_port` - 요청을 수락한 서버의 포트
- `$_server_protocol` - 요청 프로토콜, 일반적으로 “HTTP/1.0” 또는 “HTTP/1.1”
- `$_ssl_client_cert` - 설정된 SSL 연결에 대한 PEM 형식의 클라이언트 인증서를 반환하며, 첫 줄을 제외한 각 줄 앞에 탭 문자가 추가됨
- `$_ssl_server_name` - SNI를 통해 요청된 서버 이름을 반환함
- `$_uri` - 요청의 URI 경로

## 사전 요구 사항

계층 7 가상 서버를 사용할 수 있는지 확인합니다. [계층 7 가상 서버 구성](#)의 내용을 참조하십시오.

## 절차

- 1 계층 7 가상 서버를 엽니다.
- 2 [가상 서버 식별자] 페이지로 건너웁니다.
- 3 가상 서버 IP 주소 및 포트 번호를 입력합니다.  
가상 서버 포트 번호나 포트 범위를 입력할 수 있습니다.
- 4 고급 속성 세부 정보를 모두 입력합니다.

옵션	설명
최대 동시 연결	가상 서버가 동일한 로드 밸런서에서 호스팅되는 다른 애플리케이션의 리소스를 고갈시키지 않도록 가상 서버에 허용되는 최대 동시 연결 수를 설정합니다.
최대 새 연결 속도	가상 서버가 리소스를 고갈시키지 않도록 서버 풀 멤버에 대한 최대 새 연결을 설정합니다.
기본 풀 멤버 포트	가상 서버에 대한 풀 멤버 포트가 정의되지 않은 경우 기본 풀 멤버 포트를 입력합니다. 예를 들어, 가상 서버가 포트 범위 2000-2999로 정의되고 기본 풀 멤버 포트 범위가 8000-8999로 설정되면 가상 서버 포트 2500에 대해 들어오는 클라이언트 연결은 대상 포트가 8500으로 설정된 풀 멤버로 전송됩니다.

- 5 (선택 사항) 드롭다운 메뉴에서 기존 기본 서버 풀을 선택합니다.

서버 풀은 유사하게 구성되고 동일한 애플리케이션을 실행하는 하나 이상의 서버로 구성되며, 이러한 서버를 풀 멤버라고 합니다.

- 6 **추가**를 클릭하여 HTTP 요청 재작성 단계에 대한 로드 밸런서 규칙을 구성합니다.

지원되는 일치 유형은 REGEX, STARTS\_WITH, ENDS\_WITH 및 반전 옵션입니다.

지원되는 일치 조건	설명
HTTP 요청 메서드	HTTP 요청 메서드를 일치시킵니다. <code>http_request.method</code> - 일치시킬 값
HTTP 요청 URI	쿼리 인수 없이 HTTP 요청 URI를 일치시킵니다. <code>http_request.uri</code> - 일치시킬 값



지원되는 일치 조건	설명
HTTP 요청 URI 인수	HTTP 요청 URI 쿼리 인수를 일치시킵니다. http_request.uri_arguments - 일치시킬 값
HTTP 요청 버전	HTTP 요청 버전을 일치시킵니다. http_request.version - 일치시킬 값
HTTP 요청 헤더	HTTP 요청 헤더를 일치시킵니다. http_request.header_name - 일치시킬 헤더 이름 http_request.header_value - 일치시킬 값
HTTP 요청 페이로드	HTTP 요청 본문 콘텐츠를 일치시킵니다. http_request.body_value - 일치시킬 값
TCP 헤더 필드	TCP 소스 또는 대상 포트를 일치시킵니다. tcp_header.source_port - 일치시킬 소스 포트 tcp_header.destination_port - 일치시킬 대상 포트
IP 헤더 필드	IP 소스 또는 대상 주소를 일치시킵니다. ip_header.source_address - 일치시킬 소스 주소 ip_header.destination_address - 일치시킬 대상 주소
작업	설명
HTTP 요청 URI 재작성	URI를 수정합니다. http_request.uri - 작성할 URI(쿼리 인수 없음) http_request.uri_args - 작성할 URI 쿼리 인수
HTTP 요청 헤더 재작성	HTTP 헤더의 값을 수정합니다. http_request.header_name - 헤더 이름 http_request.header_value - 작성할 값

## 7 추가를 클릭하여 HTTP 요청 전달에 대한 로드 밸런서 규칙을 구성합니다.

모든 일치 값은 정규식을 허용합니다.

지원되는 일치 조건	설명
HTTP 요청 메서드	HTTP 요청 메서드를 일치시킵니다. http_request.method - 일치시킬 값
HTTP 요청 URI	HTTP 요청 URI를 일치시킵니다. http_request.uri - 일치시킬 값
HTTP 요청 URI 인수	HTTP 요청 URI 쿼리 인수를 일치시킵니다. http_request.uri_args - 일치시킬 값
HTTP 요청 버전	HTTP 요청 버전을 일치시킵니다. http_request.version - 일치시킬 값
HTTP 요청 헤더	HTTP 요청 헤더를 일치시킵니다. http_request.header_name - 일치시킬 헤더 이름 http_request.header_value - 일치시킬 값
HTTP 요청 페이로드	HTTP 요청 본문 콘텐츠를 일치시킵니다. http_request.body_value - 일치시킬 값

지원되는 일치 조건	설명
<b>TCP 헤더 필드</b>	TCP 소스 또는 대상 포트를 일치시킵니다. tcp_header.source_port - 일치시킬 소스 포트 tcp_header.destination_port - 일치시킬 대상 포트
<b>IP 헤더 필드</b>	IP 소스 주소를 일치시킵니다. ip_header.source_address - 일치시킬 소스 주소
작업	설명
<b>거절</b>	예를 들면 상태를 5xx로 설정하여 요청을 거부합니다. http_forward.reply_status - 거부하는 데 사용되는 HTTP 상태 코드 http_forward.reply_message - HTTP 거부 메시지
<b>리디렉션</b>	요청을 리디렉션합니다. 상태 코드를 3xx로 설정해야 합니다. http_forward.redirect_status - 리디렉션을 위한 HTTP 상태 코드 http_forward.redirect_url - HTTP 리디렉션 URL
<b>풀 선택</b>	요청을 특정 서버 풀에 강제 적용합니다. 지정된 풀 멤버의 구성된 알고리즘(예: 측자)은 서버 풀 내에서 서버를 선택하는 데 사용됩니다. http_forward.select_pool - 서버 풀 UUID

## 8 추가를 클릭하여 HTTP 응답 재작성에 대한 로드 밸런서 규칙을 구성합니다.

모든 일치 값은 정규식을 허용합니다.

지원되는 일치 조건	설명
<b>HTTP 응답 헤더</b>	HTTP 응답 헤더를 일치시킵니다. http_response.header_name - 일치시킬 헤더 이름 http_response.header_value - 일치시킬 값
작업	설명
<b>HTTP 응답 헤더 다시 쓰기</b>	HTTP 응답 헤더의 값을 수정합니다. http_response.header_name - 헤더 이름 http_response.header_value - 작성할 값

## 9 (선택 사항) 다음을 클릭하여 로드 밸런싱 프로파일을 구성합니다.

## 10 완료

### 계층 7 가상 서버 로드 밸런싱 프로파일 구성

계층 7 가상 서버를 사용하면 로드 밸런서 지속성, 클라이언트 측 SSL 및 서버 측 SSL 프로파일을 선택적으로 구성할 수 있습니다.

**참고** NSX-T Data Center 2.2 Limited Export 릴리스에서는 SSL 프로파일이 지원되지 않습니다.

클라이언트 측 SSL 프로파일 바인딩이 서버 측 SSL 프로파일 바인딩이 아닌 가상 서버에 구성되면 가상 서버는 SSL 종료 모드에서 작동합니다. 여기에는 클라이언트에 대한 암호화된 연결과 서버에 대한 일반 텍스트 연결이 있습니다. 클라이언트 측 및 서버 측 SSL 프로파일 바인딩이 모두 구성되면 가상 서버는 SSL 프록시 모드에서 작동합니다. 여기에는 클라이언트와 서버 모두에 암호화된 연결이 있습니다.

클라이언트 측 SSL 프로파일 바인딩과 연결하지 않고 서버 측 SSL 프로파일 바인딩을 연결하는 것은 현재 지원되지 않습니다. 클라이언트 측 및 서버 측 SSL 프로파일 바인딩이 가상 서버와 연결되어 있지 않고 애플리케이션이 SSL 기반인 경우에는 가상 서버가 SSL 비 인식 모드로 작동합니다. 이런 경우 계층 4에 대해 가상 서버를 구성해야 합니다. 예를 들어, 가상 서버를 빠른 TCP 프로파일에 연결할 수 있습니다.

## 사전 요구 사항

계층 7 가상 서버를 사용할 수 있는지 확인합니다. [계층 7 가상 서버 구성](#)의 내용을 참조하십시오.

## 절차

**1** 계층 7 가상 서버를 엽니다.

**2** [로드 밸런싱 프로파일] 페이지로 건너뛵니다.

**3** [지속성] 버튼을 전환하여 프로파일을 사용하도록 설정합니다.

지속성 프로파일을 사용하면 관련 클라이언트 연결을 동일한 서버로 보낼 수 있습니다.

**4** 소스 IP 지속성 또는 쿠키 지속성 프로파일을 선택합니다.

**5** 드롭다운 메뉴에서 기존 지속성 프로파일을 선택합니다.

**6** 다음을 클릭합니다.

**7** [클라이언트 측 SSL] 버튼을 전환하여 프로파일을 사용하도록 설정합니다.

클라이언트 측 SSL 프로파일 바인딩을 사용하면 서로 다른 호스트 이름이 동일한 가상 서버에 연결될 수 있도록 여러 인증서가 허용됩니다.

연결된 클라이언트 측 SSL 프로파일은 자동으로 채워집니다.

**8** 드롭다운 메뉴에서 기본 인증서를 선택합니다.

이 인증서는 서버가 동일한 IP 주소에서 여러 호스트 이름을 호스팅하지 않거나 클라이언트가 SNI(서버 이름 표시) 확장을 지원하지 않는 경우 사용됩니다.

**9** 사용 가능한 SNI 인증서를 선택하고 화살표를 클릭하여 인증서를 [선택됨] 섹션으로 이동합니다.

**10** (선택 사항) [필수 클라이언트 인증]을 전환하여 이 메뉴 항목을 사용하도록 설정합니다.

**11** 사용 가능한 CA 인증서를 선택하고 화살표를 클릭하여 인증서를 [선택됨] 섹션으로 이동합니다.

**12** 인증서 체인 수준을 설정하여 서버 인증서 체인의 수준을 확인합니다.

**13** 사용 가능한 CRL을 선택하고 화살표를 클릭하여 인증서를 [선택됨] 섹션으로 이동합니다.

CRL은 손상된 서버 인증서를 허용하지 않도록 구성할 수 있습니다.

**14** 다음을 클릭합니다.

**15** [서버 측 SSL] 버튼을 전환하여 프로파일을 사용하도록 설정합니다.

연결된 서버 측 SSL 프로파일은 자동으로 채워집니다.

**16** 드롭다운 메뉴에서 클라이언트 인증서를 선택합니다.

클라이언트 인증서는 서버가 동일한 IP 주소에서 여러 호스트 이름을 호스팅하지 않거나 클라이언트가 SNI(서버 이름 표시) 확장을 지원하지 않는 경우 사용됩니다.

**17** 사용 가능한 SNI 인증서를 선택하고 화살표를 클릭하여 인증서를 [선택됨] 섹션으로 이동합니다.

**18** (선택 사항) [서버 인증]을 전환하여 이 메뉴 항목을 사용하도록 설정합니다.

서버 측 SSL 프로파일 바인딩은 SSL 핸드셰이크 중에 로드 밸런서에 제공되는 서버 인증서의 유효성을 검사해야 할지 여부를 지정합니다. 유효성 검사를 사용하도록 설정된 경우, 자체 서명된 인증서가 동일한 서버 측 SSL 프로파일 바인딩에 지정되어 있는 신뢰할 수 있는 CA 중 하나가 서버 인증서에 서명해야 합니다.

**19** 사용 가능한 CA 인증서를 선택하고 화살표를 클릭하여 인증서를 [선택됨] 섹션으로 이동합니다.

**20** 인증서 체인 수준을 설정하여 서버 인증서 체인의 수준을 확인합니다.

**21** 사용 가능한 CRL을 선택하고 화살표를 클릭하여 인증서를 [선택됨] 섹션으로 이동합니다.

CRL은 손상된 서버 인증서를 허용하지 않도록 구성할 수 있습니다. OCSP 및 OCSP 스테이플링은 서버 측에서 지원되지 않습니다.

**22 완료**를 클릭합니다.

# DHCP

# 11

DHCP(Dynamic Host Configuration Protocol)를 사용하면 클라이언트는 IP 주소, 서브넷 마스크, 기본 게이트웨이 및 DNS 구성과 같은 네트워크 구성을 DHCP 서버에서 자동으로 가져올 수 있습니다.

DHCP 서버를 생성하여 DHCP 요청을 처리하고 DHCP 릴레이 서비스를 생성하여 DHCP 트래픽을 외부 DHCP 서버로 릴레이할 수 있습니다. 그러나 DHCP 서버를 논리적 스위치에 구성하고, 이 논리적 스위치가 연결되어 있는 라우터 포트에 DHCP 릴레이 서비스까지 구성하면 안 됩니다. 이와 같은 시나리오에서는 DHCP 요청이 DHCP 릴레이 서비스에만 전송됩니다.

DHCP 서버를 구성하는 경우 보안을 향상하기 위해 유효한 DHCP 서버 IP 주소에 대해서만 UDP 포트 67 및 68의 트래픽을 허용하도록 DFW 규칙을 구성합니다.

---

**참고** 소스가 Logical Switch/Logical Port/NSGroup이고, 대상이 Any이며 포트 67 및 68에 대해 DHCP 패킷을 삭제하도록 구성된 DFW 규칙은 DHCP 트래픽을 차단하지 못합니다. DHCP 트래픽을 차단하려면 소스 및 대상으로 Any를 구성합니다.

---

본 장은 다음 항목을 포함합니다.

- DHCP 서버 프로파일 생성
- DHCP 서버 생성
- DHCP 서버를 논리적 스위치에 연결
- 논리적 스위치에서 DHCP 서버 분리
- DHCP 릴레이 프로파일 생성
- DHCP 릴레이 서비스 생성
- 논리적 라우터 포트에 DHCP 서비스 추가

## DHCP 서버 프로파일 생성

DHCP 서버 프로파일은 NSX Edge 클러스터 또는 NSX Edge 클러스터의 멤버를 지정합니다. 이 프로파일이 있는 DHCP 서버는 프로파일에 지정된 NSX Edge 노드에 연결되어 있는 논리 스위치에서 VM의 DHCP 요청을 처리합니다.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > DHCP**를 선택합니다.
- 3 **서버 프로파일**을 클릭하고 **추가**를 클릭합니다.
- 4 이름과 설명(선택 사항)을 입력합니다.
- 5 드롭다운 목록에서 NSX Edge 클러스터를 선택합니다.
- 6 (선택 사항) NSX Edge 클러스터의 멤버를 선택합니다.  
최대 2개의 멤버를 지정할 수 있습니다.

## 다음에 수행할 작업

DHCP 서버를 생성합니다. [DHCP 서버 생성](#)의 내용을 참조하십시오.

## DHCP 서버 생성

논리적 스위치에 연결되어 있는 VM의 DHCP 요청을 처리하는 DHCP 서버를 생성할 수 있습니다.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > DHCP**를 선택합니다.
- 3 **서버**를 클릭하고 **추가**를 클릭합니다.
- 4 이름과 설명(선택 사항)을 입력합니다.
- 5 DHCP 서버의 IP 주소와 해당 서브넷 마스크를 CIDR 형식으로 입력합니다.  
예: 192.168.1.2/24
- 6 (필수 사항) 드롭다운 메뉴에서 DHCP 프로파일을 선택합니다.
- 7 (선택 사항) 도메인 이름, 기본 게이트웨이, DNS 서버 및 서브넷 마스크와 같은 일반 옵션을 입력합니다.
- 8 (선택 사항) 클래스 없는 정적 경로 옵션을 입력합니다.
- 9 (선택 사항) 기타 옵션을 입력합니다.
- 10 **저장**을 클릭합니다.
- 11 새로 생성된 DHCP 서버를 선택합니다.
- 12 [IP 풀] 섹션을 확장합니다.
- 13 **추가**를 클릭하여 IP 범위, 기본 게이트웨이, 리스 기간, 주의 임계값, 오류 임계값, 클래스 없는 정적 경로 옵션 및 기타 옵션을 추가합니다.

**14** [정적 바인딩] 섹션을 확장합니다.

**15 추가**를 클릭하여 MAC 주소와 IP 주소 간 정적 바인딩, 기본 게이트웨이, 호스트 이름, 리스 기간, 클래스 없는 정적 경로 옵션 및 기타 옵션을 추가합니다.

다음에 수행할 작업

DHCP 서버를 논리적 스위치에 연결합니다. [DHCP 서버를 논리적 스위치에 연결](#)의 내용을 참조하십시오.

## DHCP 서버를 논리적 스위치에 연결

DHCP 서버가 스위치에 연결된 VM의 DHCP 요청을 처리하기 전에 DHCP 서버를 논리적 스위치에 연결해야 합니다. VLAN 논리적 스위치에서는 DHCP 서버가 지원되지 않습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 스위칭**을 선택합니다.
- 3 DHCP 서버를 연결하려는 논리적 스위치를 클릭합니다.
- 4 **작업 > DHCP 서버 연결**을 클릭합니다.

## 논리적 스위치에서 DHCP 서버 분리

논리적 스위치에서 DHCP 서버를 분리하여 환경을 재구성할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 스위칭**을 선택합니다.
- 3 DHCP 서버를 분리하려는 논리적 스위치를 클릭합니다.
- 4 **작업 > DHCP 서버 분리**를 클릭합니다.

## DHCP 릴레이 프로파일 생성

DHCP 릴레이 프로파일은 하나 이상의 외부 DHCP 서버를 지정합니다. DHCP 릴레이 서비스를 생성할 때 DHCP 릴레이 프로파일을 지정해야 합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > DHCP**를 선택합니다.

- 3 릴레이 프로파일을 클릭하고 **추가**를 클릭합니다.
- 4 이름과 설명(선택 사항)을 입력합니다.
- 5 하나 이상의 외부 DHCP 서버 주소를 입력합니다.

다음에 수행할 작업

DHCP 릴레이 서비스를 생성합니다. [DHCP 릴레이 서비스 생성](#)의 내용을 참조하십시오.

## DHCP 릴레이 서비스 생성

DHCP 릴레이 서비스를 생성하여 NSX-T Data Center에서 생성되지 않은 DHCP 클라이언트 및 DHCP 서버 간에 트래픽을 릴레이할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > DHCP**를 선택합니다.
- 3 **릴레이 서비스**를 클릭하고 **추가**를 클릭합니다.
- 4 이름과 설명(선택 사항)을 입력합니다.
- 5 드롭다운 메뉴에서 DHCP 릴레이 프로파일을 선택합니다.

다음에 수행할 작업

논리적 라우터 포트에 DHCP 서비스를 추가합니다. [논리적 라우터 포트에 DHCP 서비스 추가](#)의 내용을 참조하십시오.

## 논리적 라우터 포트에 DHCP 서비스 추가

논리적 라우터 포트에 DHCP 릴레이 서비스를 추가하면 해당 포트에 연결된 논리적 스위치의 VM이 릴레이 서비스에 구성된 DHCP 서버와 통신할 수 있습니다.

사전 요구 사항

- DHCP 릴레이 서비스가 구성되어 있는지 확인합니다. [DHCP 릴레이 서비스 생성](#)의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > 라우팅**을 선택합니다.
- 3 원하는 논리적 스위치에 연결된 라우터를 선택하고 **구성** 탭을 클릭합니다.
- 4 원하는 논리적 스위치에 연결된 라우터 포트를 선택하고 **편집**을 클릭합니다.



- 5 **DHCP 서비스** 드롭다운 목록에서 DHCP 릴레이 서비스를 선택하고 **저장**을 클릭합니다.  
논리적 라우터 포트는 **DHCP 서비스** 열에서 DHCP 릴레이 서비스를 표시합니다.  
또한 새 논리적 라우터 포트를 추가할 때 DHCP 릴레이 서비스를 선택할 수 있습니다.

# 메타데이터 프록시

# 12

메타데이터 프록시 서버를 사용하면 VM 인스턴스는 OpenStack Nova API 서버에서 인스턴스별 메타데이터를 검색할 수 있습니다.

다음 단계에서는 메타데이터 프록시가 작동하는 방식을 설명합니다.

- 1 VM은 `http://169.254.169.254:80`으로 HTTP GET을 전송하여 일부 메타데이터를 요청합니다.
- 2 VM과 동일한 논리적 스위치에 연결된 메타데이터 프록시 서버는 요청을 읽고, 헤더를 적절히 변경하고, Nova API 서버에 요청을 전달합니다.
- 3 Nova API 서버는 Neutron 서버에서 VM에 대한 정보를 요청하고 수신합니다.
- 4 Nova API 서버는 메타데이터를 찾은 후 이를 메타데이터 프록시 서버로 전송합니다.
- 5 메타데이터 프록시 서버는 VM에 메타데이터를 전달합니다.

메타데이터 프록시 서버는 NSX Edge 노드에서 실행됩니다. 고가용성을 위해 NSX Edge 클러스터에 있는 둘 이상의 NSX Edge 노드에서 실행되도록 메타데이터 프록시를 구성할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 메타데이터 프록시 서버 추가
- 메타데이터 프록시 서버를 논리적 스위치에 연결
- 논리적 스위치에서 메타데이터 프록시 서버 분리

## 메타데이터 프록시 서버 추가

메타데이터 프록시 서버를 사용하면 VM은 OpenStack Nova API 서버에서 메타데이터를 검색할 수 있습니다.

### 사전 요구 사항

NSX Edge 클러스터를 생성했는지 확인합니다. 자세한 내용은 "NSX-T Data Center 설치 가이드"를 참조하십시오.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > DHCP**를 선택합니다.
- 3 **메타데이터 프록시** 탭을 클릭합니다.
- 4 **추가**를 클릭합니다.
- 5 메타데이터 프록시 서버의 이름을 입력합니다.
- 6 (선택 사항) 설명을 입력합니다.
- 7 Nova 서버의 URL 및 포트를 입력합니다.  
유효한 포트 범위는 3000 - 9000입니다.
- 8 **암호**에 대한 값을 입력합니다.
- 9 드롭다운 목록에서 NSX Edge 클러스터를 선택합니다.
- 10 (선택 사항) NSX Edge 클러스터의 멤버를 선택합니다.

예

예 :

**New Metadata Proxy Server** ? ×

<b>Name *</b>	metadata-proxy-1
<b>Description</b>	
<b>Nova Server URL *</b>	https://123.1.1.1:8775
<b>Secret *</b>	*****
<b>Edge Cluster *</b>	edge_cluster_p1r1 <span>▼</span>
<b>Members</b>	53524616-c67f-11e8-837f-020046520048 <span>×</span> <span>▼</span>

CANCEL ADD

다음에 수행할 작업

메타데이터 프록시 서버를 논리적 스위치에 연결합니다.

## 메타데이터 프록시 서버를 논리적 스위치에 연결

논리적 스위치에 연결된 VM에 메타데이터 프록시 서비스를 제공하려면 메타데이터 프록시 서버를 스위치에 연결해야 합니다.

### 사전 요구 사항

논리적 스위치를 생성했는지 확인합니다. 자세한 내용은 [논리적 스위치 생성](#) 항목을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > DHCP**를 선택합니다.
- 3 **메타데이터 프록시** 탭을 클릭합니다.
- 4 메타데이터 프록시 서버를 선택합니다.
- 5 메뉴 옵션 **작업 > 논리적 스위치에 연결**을 선택합니다.
- 6 드롭다운 목록에서 논리적 스위치를 선택합니다.

### 결과

또한 **스위칭 > 스위치**로 이동한 후, 스위치를 선택하고 메뉴 옵션 **작업 > 메타데이터 프록시 연결**을 선택하여 메타데이터 프록시 서버를 논리적 스위치에 연결할 수 있습니다.

## 논리적 스위치에서 메타데이터 프록시 서버 분리

논리적 스위치에 연결된 VM에 메타데이터 프록시 서비스를 제공하지 못하게 하거나 다른 메타데이터 프록시 서버를 사용하려면 논리적 스위치에서 메타데이터 프록시 서버를 분리할 수 있습니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > DHCP**를 선택합니다.
- 3 **메타데이터 프록시** 탭을 클릭합니다.
- 4 메타데이터 프록시 서버를 선택합니다.
- 5 메뉴 옵션 **작업 > 논리적 스위치에서 분리**를 선택합니다.
- 6 드롭다운 목록에서 논리적 스위치를 선택합니다.

### 결과

**스위칭 > 스위치**로 이동하고 스위치를 선택한 후 메뉴 옵션 **작업 > 메타데이터 프록시 분리**를 선택하여 논리적 스위치에서 메타데이터 프록시 서버를 분리할 수도 있습니다.

# IP 주소 관리

# 13

IPAM(IP 주소 관리)을 사용하면 NCP(NSX-T Container Plug-in)를 지원하는 IP 블록을 생성할 수 있습니다. NCP에 대한 자세한 내용은 “Kubernetes용 NSX-T Container Plug-in - 설치 및 관리 가이드”를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- IP 블록 관리
- IP 블록에 대한 서브넷 관리

## IP 블록 관리

NSX-T Container Plug-in을 설치하려면 컨테이너용 IP 블록을 생성해야 합니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > IPAM**을 선택합니다.
- 3 IP 블록을 추가하려면 **추가**를 클릭합니다.
  - a 이름과 설명(선택 사항)을 입력합니다.
  - b IP 블록을 CIDR 형식으로 입력합니다. 예: 10.10.10.0/24
- 4 IP 블록을 편집하려면 IP 블록의 이름을 클릭합니다.
  - a **개요** 탭에서 **편집**을 클릭합니다.  
이름, 설명 또는 IP 블록 값을 변경할 수 있습니다.
- 5 IP 블록의 태그를 관리하려면 IP 블록의 이름을 클릭합니다.
  - a **개요** 탭에서 **관리**를 클릭합니다.  
태그를 추가하거나 삭제할 수 있습니다.

- 6 하나 이상의 IP 블록을 삭제하려면 블록을 선택합니다.
  - a **삭제**를 클릭합니다.  
서브넷이 할당된 IP 블록은 삭제할 수 없습니다.

## IP 블록에 대한 서브넷 관리

IP 블록에 대한 서브넷을 추가하거나 삭제할 수 있습니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **네트워킹 > IPAM**을 선택합니다.
- 3 IP 블록의 이름을 클릭합니다.
- 4 **서브넷** 탭을 클릭합니다.
- 5 서브넷을 추가하려면 **추가**를 클릭합니다.
  - a 이름과 설명(선택 사항)을 입력합니다.
  - b 서브넷의 크기를 입력합니다.
- 6 하나 이상의 서브넷을 삭제하려면 서브넷을 선택합니다.
  - a **삭제**를 클릭합니다.

정책은 규칙과 서비스의 조합이며 규칙은 리소스 액세스 및 사용량에 대한 기준을 정의합니다. NSX 정책을 사용하면 낮은 수준의 세부 정보에 대한 걱정 없이 리소스 액세스 및 사용량을 관리할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 개요
- 적용 지점 추가
- 서비스 추가
- 도메인 추가
- NSX Policy Manager의 백업 구성
- NSX Policy Manager 백업
- NSX Policy Manager 복원
- vIDM 호스트를 NSX Policy Manager와 연결
- 역할 할당 관리

## 개요

NSX 정책을 사용하면 규칙 메커니즘에 대한 걱정 없이 VM, 논리적 포트, IP 주소 및 MAC 주소와 같은 개체에 대한 규칙을 지정할 수 있습니다. 정책은 NSX Manager가 아닌 NSX Policy Manager에서 관리합니다.

정책을 구성하기 전에 NSX Policy Manager를 설치해야 합니다. 자세한 내용은 “NSX-T 설치 가이드”를 참조하십시오. NSX Policy Manager에서 적용 지점을 하나 이상 추가하여 정책이 적용될 NSX Manager에 대한 정보도 제공해야 합니다.

다음 예에서는 정책을 사용하여 애플리케이션에 대한 네트워킹을 관리하는 방법을 보여줍니다.

애플리케이션에 3가지 계층(웹, 애플리케이션 및 데이터베이스)이 있으며 다음 규칙을 애플리케이션의 VM에 적용해야 합니다.

- 웹 계층과 애플리케이션 계층 간의 트래픽을 허용합니다.
- 애플리케이션 계층과 데이터베이스 계층 간의 트래픽을 허용합니다.

- 모든 시스템과 웹 계층 간의 트래픽을 허용합니다.

NSX Manager에서 다음 단계를 수행합니다.

- 웹 VM의 워크로드 이름을 Web 뒤에 식별 문자열이 붙도록 설정합니다.
- 애플리케이션 VM의 워크로드 이름을 App 뒤에 식별 문자열이 붙도록 설정합니다.
- 데이터베이스 VM의 워크로드 이름을 DB 뒤에 식별 문자열이 붙도록 설정합니다.

NSX Policy Manager에서 다음 단계를 수행합니다.

- 도메인을 생성하고 다음을 지정합니다.
  - 워크로드 이름이 Web으로 시작하는 VM으로 구성된 WebGroup이라는 그룹을 생성합니다.
  - 워크로드 이름이 App으로 시작하는 VM으로 구성된 AppGroup이라는 그룹을 생성합니다.
  - 워크로드 이름이 DB으로 시작하는 VM으로 구성된 DBGroup이라는 그룹을 생성합니다.
  - 그룹 간의 통신을 제어하는 보안 정책을 지정합니다.
- 도메인 구성에서 오류가 없는지 확인합니다.
- 적용 지점을 선택합니다.

적용 지점을 선택하면 NSX Policy Manager가 적용 지점에서 NSX Manager와 통신하여 보안 정책이 구현됩니다.

## 역할 기반 액세스 제어

NSX Policy Manager에는 admin과 audit이라는 두 가지 기본 제공 사용자가 있습니다. NSX Policy Manager를 vIDM(VMware Identity Manager)과 통합하고 vIDM이 관리하는 사용자를 위해 RBAC(역할 기반 액세스 제어)를 구성 할 수 있습니다.

vIDM이 관리하는 사용자에게는 admin과 audit에게만 적용되는 NSX Policy Manager의 인증 정책이 아니라 vIDM 관리자가 구성한 인증 정책이 적용됩니다.

## 적용 지점 추가

적용 지점은 정책의 규칙을 적용할 지점입니다. 이 릴리스에서 적용 지점은 NSX-T 설치여야 하며 NSX Policy Manager는 적용 지점을 하나만 지원합니다.

### 절차

- 1 브라우저에서 NSX Policy Manager(<https://nsx-policy-manager-IP-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 적용 지점**을 선택합니다.
- 3 **추가**를 클릭합니다.



#### 4 다음 정보를 제공합니다.

매개 변수	설명
이름	적용 지점의 이름입니다.
자격 증명	NSX Manager에 로그인하기 위한 사용자 이름과 암호입니다.
적용 주소	NSX Manager의 IP 주소입니다.
지문	NSX Manager의 인증서 지문입니다.

#### 5 저장을 클릭합니다.

## 서비스 추가

서비스는 사용자 환경의 프로토콜 또는 소프트웨어 구성 요소입니다. 정책은 서비스에 적용되는 규칙을 포함합니다.

서비스의 예로는 FTP, HTTP, AD 서버, DHCP 서버, Oracle 데이터베이스 등이 있습니다.

#### 절차

- 1 브라우저에서 NSX Policy Manager(<https://nsx-policy-manager-IP-address>)에 로그인합니다.
- 2 탐색 패널에서 **인프라 > 서비스**를 선택합니다.
- 3 **새 서비스 추가**를 클릭합니다.
- 4 서비스의 이름을 입력합니다.
- 5 **서비스 항목 설정**을 클릭하여 서비스 항목을 추가합니다.
  - a **새 서비스 항목 추가**를 클릭합니다.
  - b 서비스 유형을 선택합니다.  
사용 가능한 유형은 **IP, IGMP, ICMP, ALG, TCP 및 UDP**입니다.
  - c **추가 속성** 드롭다운 목록을 클릭하여 속성을 선택합니다.  
항목을 더 추가하거나, 항목을 편집 또는 삭제할 수 있습니다.
- 6 **저장**을 클릭합니다.

## 도메인 추가

도메인은 일반적인 비즈니스 목표를 수행하고 정책을 적용해야 하는 워크로드의 논리적 모음입니다. 여기에는 그룹 집합과 해당 통신 요구 사항이 들어 있습니다.

여러 개의 대규모 도메인(각각 200개 이상의 결과 규칙이 있는)을 생성하려는 경우, 순차적으로 적용 지점에 배포하고 다음 도메인으로 진행하기 전에 각 도메인의 인식을 기다려야 합니다. API를 사용하여 이러한 도메인을 배포하는 경우 도메인이 적용 지점에 배포되기 전에 통신 항목을 생성하는 것이 좋습니다.

## 절차

- 1 브라우저에서 NSX Policy Manager(<https://nsx-policy-manager-IP-address>)에 로그인합니다.
- 2 탐색 패널에서 **인프라 > 도메인**을 선택합니다.
- 3 **도메인 추가**를 클릭하여 도메인을 추가합니다.
- 4 도메인의 이름을 지정하고 선택적으로 설명을 지정합니다.
- 5 **다음**을 클릭하여 [워크로드 그룹] 단계로 이동합니다.
- 6 **그룹 추가**를 클릭하여 하나 이상의 워크로드 그룹을 추가합니다. 각 워크로드 그룹에 대해,
  - a 이름을 지정합니다.
  - b **멤버 유형** 필드를 클릭하여 멤버 유형을 선택합니다.  
선택 가능한 항목에는 **가상 시스템**, **IP 주소** 및 **멤버 자격 조건**이 있습니다.
  - c **가상 시스템** 및 **IP 주소**의 경우 값을 지정합니다.
  - d **멤버 자격 조건**의 경우 **멤버 자격 조건 설정**을 클릭하여 멤버 선택 방식을 지정합니다.
- 7 **다음**을 클릭하여 [보안] 단계로 이동합니다.
- 8 **새 섹션 추가**를 클릭하여 방화벽 섹션을 추가하거나 **새 규칙 추가**를 클릭하여 방화벽 규칙을 추가합니다.  
여러 섹션과 규칙을 추가할 수 있습니다.
- 9 **다음**을 클릭하여 [도메인 구성 확인] 단계로 이동합니다.  
도메인에 대한 그래픽 표현이 표시됩니다.
- 10 **다음**을 클릭하여 [적용 지점 선택] 단계로 이동합니다.
- 11 하나 이상의 적용 지점을 선택합니다.
- 12 **완료**를 클릭하여 도메인을 배포합니다.

## NSX Policy Manager의 백업 구성

Policy Manager가 저장하는 데이터를 보호하기 위해 NSX Policy Manager를 백업할 수 있습니다. 백업을 수행하려면, 먼저 백업 속성을 구성해야 합니다.

### 사전 요구 사항

백업 파일 서버의 SSH 지문이 있는지 확인합니다. SHA256 해시 ECDSA 키만 지문으로 허용됩니다. [원격 서버의 SSH 지문 찾기](#)의 내용을 참조하십시오.

## 절차

- 1 브라우저에서 NSX Policy Manager(<https://nsx-policy-manager-IP-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 유틸리티**를 선택합니다.

- 3 구성을 클릭합니다.
- 4 자동 백업 토글을 클릭하여 자동 백업을 사용하거나 사용하지 않도록 설정합니다.
- 5 백업 파일 서버의 IP 주소 또는 호스트 이름을 입력합니다.
- 6 필요한 경우 기본 포트를 편집합니다.
- 7 백업 파일 서버에 로그인하는 데 필요한 사용자 이름 및 암호를 입력합니다.
- 8 대상 디렉토리 필드에서 백업이 저장될 절대 디렉토리 경로를 입력합니다.  
디렉토리가 이미 존재해야 합니다.
- 9 백업 데이터를 암호화하는 데 사용되는 암호를 입력합니다.  
백업을 복원하려면 이 암호가 필요합니다. 백업 암호를 잊어버리면 백업을 복원할 수 없습니다.
- 10 백업을 저장하는 서버의 SSH 지문을 입력합니다. [원격 서버의 SSH 지문 찾기](#)의 내용을 참조하십시오.
- 11 스케줄 탭을 클릭합니다.
- 12 빈도를 선택합니다.  
매주를 선택하는 경우, 요일과 시간을 지정합니다. 간격을 선택하는 경우 간격을 지정합니다.
- 13 저장을 클릭합니다.

## NSX Policy Manager 백업

NSX Policy Manager는 자동 또는 수동으로 백업할 수 있습니다.

자동 백업을 구성한 경우 자동으로 백업이 수행됩니다. 이 절차는 수동으로 백업을 시작하는 절차입니다.

### 사전 요구 사항

백업 속성을 구성했는지 확인합니다. [NSX Policy Manager의 백업 구성](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 NSX Policy Manager(<https://nsx-policy-manager-IP-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 유틸리티**를 선택합니다.
- 3 **지금 백업**을 클릭합니다.

## NSX Policy Manager 복원

백업을 통해 NSX Policy Manager를 과거 상태로 복원할 수 있습니다.

## 사전 요구 사항

백업 파일 서버의 SSH 지문이 있는지 확인합니다. SHA256 해시 ECDSA 키만 지문으로 허용됩니다. [원격 서버의 SSH 지문 찾기](#)의 내용을 참조하십시오.

## 절차

- 1 브라우저에서 NSX Policy Manager(<https://nsx-policy-manager-IP-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 유틸리티**를 선택합니다.
- 3 **지금 복원**을 클릭합니다.
- 4 필수 조건 및 위험 요소에 대한 메시지를 확인하고 **다음**을 클릭합니다.
- 5 백업 서버의 IP 주소 또는 호스트 이름을 입력합니다.
- 6 필요한 경우 포트 번호를 변경합니다.  
기본값은 22입니다.
- 7 사용자 이름과 암호를 입력하여 서버에 로그인합니다.
- 8 **백업 디렉토리** 필드에 백업이 저장될 절대 디렉토리 경로를 입력합니다.
- 9 백업 데이터를 암호화하는 데 사용된 암호를 입력합니다.
- 10 백업 서버의 SSH 지문을 입력합니다.
- 11 **다음**을 클릭합니다.
- 12 백업을 선택합니다.
- 13 **복원**을 클릭합니다.

복원 작업의 상태가 표시됩니다. 백업 이후에 패브릭 노드 또는 전송 노드를 삭제하거나 추가한 경우 특정 작업(예 : 노드에 로그인 및 스크립트 실행)을 수행하라는 메시지가 표시됩니다.

복원 작업이 완료되면 [복원 완료] 화면이 표시되고 복원 결과, 백업 파일의 타임 스탬프, 복원 작업의 시작 및 종료 시간이 표시됩니다. 복원에 실패하면 화면에 오류가 발생한 단계가 표시됩니다. 복원 작업을 다시 시도하려면 실패가 발생한 장치가 아닌 새 정책 관리자 장치를 사용해야 합니다.

## vIDM 호스트를 NSX Policy Manager와 연결

NSX Policy Manager와 vIDM을 통합하려면 vIDM 호스트에 대한 정보를 제공해야 합니다.

CA(인증 기관)에서 서명한 인증서가 vIDM 서버에 있어야 합니다. 그렇지 않으면 NSX Policy Manager에서 vIDM에 로그인하는 것이 Microsoft Edge나 Internet Explorer 11과 같은 특정 브라우저에서 작동하지 않을 수 있습니다. vIDM에 CA 서명된 인증서 설치에 대한 자세한 내용은 <https://docs.vmware.com/kr/VMware-Identity-Manager/3.1/vidm-install/GUID-B76761BF-4B12-4CD5-9366-B0A1A2BF2A8B.html> 항목을 참조하십시오.

vIDM에 NSX Policy Manager를 등록할 때 정책 관리자를 가리키는 리디렉션 URI를 지정합니다. FQDN(정규화된 도메인 이름) 또는 IP 주소를 제공할 수 있습니다. FQDN 또는 IP 주소를 사용하는지 여부를 기억하는 것이 중요합니다. vIDM을 통해 정책 관리자에 로그인하려고 하는 경우 동일한 방식으로 URL에서 호스트 이름을 지정해야 합니다. 즉, vIDM에 관리자를 등록할 때 FQDN을 사용하는 경우 URL에서 해당 FQDN을 사용해야 하며, vIDM에 관리자를 등록할 때 IP 주소를 사용하는 경우 URL에서 해당 IP 주소를 사용해야 합니다. 그렇지 않으면 로그인이 실패합니다.

### 사전 요구 사항

- vIDM 호스트의 인증서 지문이 있는지 확인합니다. [vIDM 호스트에서 인증서 지문 가져오기](#)의 내용을 참조하십시오.
- NSX Policy Manager가 vIDM 호스트에 대한 OAuth 클라이언트로 등록되어 있는지 확인합니다. 등록 프로세스 중에 클라이언트 ID와 클라이언트 암호를 적어두십시오. 자세한 내용은 <https://www.vmware.com/support/pubs/identitymanager-pubs.html>에서 VMware Identity Manager 설명서를 참조하십시오.

### 절차

- 1 브라우저에서 NSX Policy Manager(<https://nsx-policy-manager-IP-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 사용자**를 선택합니다.
- 3 **구성** 탭을 클릭합니다.
- 4 **편집**을 클릭합니다.
- 5 **VMware Identity Manager 통합** 토글을 클릭하여 **사용**으로 설정합니다.
- 6 다음 정보를 제공합니다.

매개 변수	설명
<b>VMware Identity Manager 장치</b>	vIDM 호스트의 FQDN(정규화된 도메인 이름)입니다.
<b>OAuth 클라이언트 ID</b>	NSX Policy Manager를 vIDM 호스트에 등록할 때 생성되는 ID입니다.
<b>OAuth 클라이언트 암호</b>	NSX Policy Manager를 vIDM 호스트에 등록할 때 생성되는 암호입니다.
<b>SHA-256 지문</b>	vIDM 호스트의 인증서 지문입니다.
<b>NSX 정책 장치</b>	NSX Policy Manager의 IP 주소 또는 FQDN(정규화된 도메인 이름)입니다. FQDN을 지정하는 경우에는 URL에 관리자의 FQDN을 사용하여 브라우저에서 NSX Policy Manager에 액세스해야 하고, IP 주소를 지정하는 경우에는 URL에 IP 주소를 사용해야 합니다. 또는 FQDN 또는 IP 주소를 사용하여 연결할 수 있도록 vIDM 관리자가 NSX Policy Manager 클라이언트를 구성할 수 있습니다.

- 7 **저장**을 클릭합니다.

## 역할 할당 관리

VMware Identity Manager가 NSX Policy Manager와 통합된 경우 사용자 또는 사용자 그룹에 대해 역할 할당을 추가, 변경 및 삭제할 수 있습니다.

다음 역할은 미리 정의됩니다. 새 역할을 추가할 수는 없습니다.

- 엔터프라이즈 관리자
- 감사자
- 사이트 안정성 엔지니어(VMware Cloud 배포에서 사용 가능)
- 클라우드 서비스 관리자(VMware Cloud 배포에서 사용 가능)
- 클라우드 서비스 감사자(VMware Cloud 배포에서 사용 가능)

#### 사전 요구 사항

- vIDM 호스트가 NSX Policy Manager와 연결되어 있는지 확인합니다. 자세한 내용은 [vIDM 호스트를 NSX Policy Manager와 연결](#) 항목을 참조하십시오.

#### 절차

- 1 브라우저에서 NSX Policy Manager(<https://nsx-policy-manager-IP-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 사용자**를 선택합니다.
- 3 **역할 할당** 탭을 아직 선택하지 않았으면 클릭합니다.
- 4 역할 할당을 추가, 변경 또는 삭제합니다.

옵션	작업
역할 할당 추가	<b>추가</b> 를 클릭하고 사용자 또는 사용자 그룹을 선택한 후 역할을 선택합니다.
역할 할당 변경	사용자 또는 사용자 그룹을 선택하고 <b>편집</b> 을 클릭합니다.
역할 할당 삭제	사용자 또는 사용자 그룹을 선택하고 <b>삭제</b> 를 클릭합니다.

서비스 삽입을 사용하면 타사 서비스를 라우터를 통해 통과하는 동-서 트래픽을 비롯한 북-남 트래픽에 적용할 수 있습니다. 서비스는 일반적으로 IDS(침입 탐지 시스템) 또는 IPS(침입 방지 시스템)와 같은 고급 보안 기능을 제공합니다.

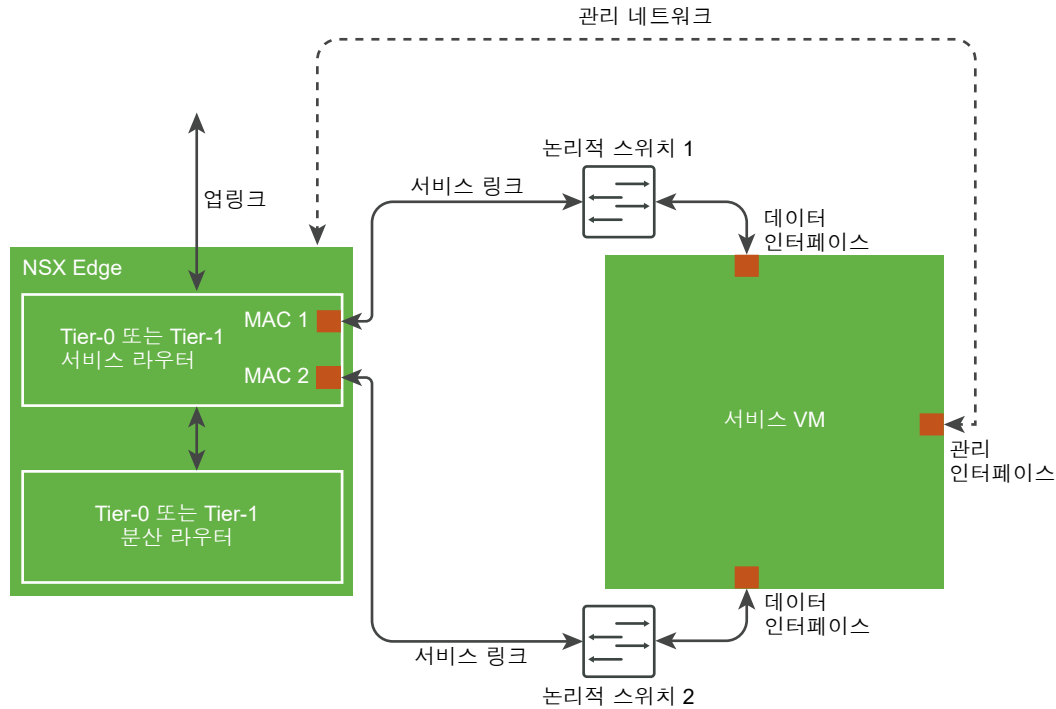
본 장은 다음 항목을 포함합니다.

- 개요
- 서비스 등록
- 서비스 인스턴스 배포
- 트래픽 리디렉션 구성
- 트래픽 리디렉션 모니터링

## 개요

Tier-0 라우터에서 북-남 트래픽 또는 Tier-1 라우터에서 동-서 트래픽을 VM으로 리디렉션하도록 서비스 삽입을 설정할 수 있습니다. VM에서 실행 중인 서비스는 트래픽을 처리하고 적절한 조치를 취할 수 있습니다.

다음 아키텍처 다이어그램은 서비스 삽입이 구성된 데이터의 흐름을 보여 줍니다.



서비스 삽입은 2개의 Edge 노드 및 2개의 서비스 VM이 포함된 액티브-대기 모드에서 HA(고가용성)를 지원합니다. 서비스 삽입은 액티브-액티브 모드에서 HA를 지원하지 않습니다. 라우터는 하나의 서비스만 지원할 수 있습니다.

서비스 삽입 설정은 다음 단계를 포함합니다.

- 서비스를 등록합니다.
- 서비스 인스턴스를 배포합니다.
- 트래픽 리디렉션을 구성합니다.

## 서비스 등록

서비스 등록에는 API 호출이 필요합니다. 서비스가 등록된 후 NSX Manager UI에서 확인할 수 있습니다.

API 호출 및 입력 매개 변수에 대한 세부 정보는 "NSX-T Data Center API 참조"에 있습니다.

### 절차

- 1 서비스를 등록하려면 다음 API 호출을 수행합니다.

```
POST /api/v1/serviceinsertion/services
```



예를 들면 다음과 같습니다.

```
POST https://<nsx-mgr>/api/v1/serviceinsertion/services
{
  "display_name": "NS Service for ABC partner",
  "description": "This service is inserted at T0 router and it provides advanced security",
  "attachment_point": [
    "TIER0_LR"
  ],
  "functionalities": [
    "NG_FW"
  ],
  "implementations": [
    "NORTH_SOUTH"
  ],
  "transports": [
    "L2_BRIDGE"
  ],
  "vendor_id": "ABC_Partner",
  "on_failure_policy": "ALLOW",
  "service_deployment_spec": {
    "deployment_specs": [{
      "ovf_url": "http://server.com/dir1/ABC-Company-HA-OVF/ABC-VM-ESX-2.0.ovf",
      "name": "NS_DepSpec",
      "host_type": "ESXI",
      "service_form_factor": "MEDIUM"
    }],
    "nic_metadata_list": [
      {
        "interface_label": "eth",
        "interface_index": 0,
        "interface_type": "MANAGEMENT"
      },
      {
        "interface_label": "eth",
        "interface_index": 1,
        "interface_type": "DATA1"
      },
      {
        "interface_label": "eth",
        "interface_index": 2,
        "interface_type": "DATA2"
      }
    ],
    "deployment_template": [{
      "name": "NS_DepTemp",
      "attributes": [{
        "attribute_type": "STRING",
        "display_name": "License",
        "key": "LicenseKey"
      }]
    }]
  }
}
```

- 2 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 3 탐색 패널에서 **파트너 서비스**를 선택합니다.
- 4 **카탈로그** 탭을 클릭하고 서비스가 등록되었는지 확인합니다.

다음에 수행할 작업

서비스의 인스턴스를 배포합니다. [서비스 인스턴스 배포](#)의 내용을 참조하십시오.

## 서비스 인스턴스 배포

서비스를 등록한 후 서비스가 네트워크 트래픽 처리를 시작하려면 서비스의 인스턴스를 배포해야 합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **파트너 서비스**를 선택합니다.
- 3 **배포**를 클릭합니다.
- 4 인스턴스 이름과 설명(선택 사항)을 입력합니다.
- 5 **파트너 서비스** 필드를 클릭하고 서비스를 선택합니다.
- 6 **배포 규격**을 선택합니다.
- 7 논리적 라우터를 선택합니다.  
서비스 삽입이 구성되지 않은 라우터만 표시됩니다.
- 8 **다음**을 클릭합니다.
- 9 **계산 관리자** 필드를 클릭하고 계산 관리자를 선택합니다.
- 10 **클러스터** 필드를 클릭하고 클러스터를 선택합니다.
- 11 (선택 사항) **리소스 풀** 필드를 클릭하고 vCenter Server에서 구성된 경우 리소스 풀을 선택합니다.
- 12 **데이터스토어** 필드를 클릭하고 데이터스토어를 선택합니다.
- 13 **배포 모드**를 선택합니다.  
선택 항목은 **독립형** 또는 **고가용성**입니다.
- 14 **실패 정책**을 선택합니다.  
선택 항목은 **허용** 또는 **차단**입니다.
- 15 VM의 IP 주소를 입력합니다.
- 16 VM의 IP 주소에 대한 기본 게이트웨이를 입력합니다.

**17** VM의 IP 주소에 대한 서브넷 마스크를 입력합니다.

**18** 다음을 클릭합니다.

**19** 배포 템플릿을 선택합니다.

**20** 파트너 서비스에 대한 라이선스를 입력합니다.

**21** 완료를 클릭합니다.

## 결과

벤더의 구현에 따라 배포 프로세스에 시간이 다소 걸릴 수 있습니다. 관리자 UI에서 상태를 볼 수 있습니다. 배포가 성공할 경우 상태는 배포 성공이 됩니다.

## 다음에 수행할 작업

서비스 인스턴스에 대한 트래픽 리디렉션을 구성합니다. [트래픽 리디렉션 구성](#)의 내용을 참조하십시오.

# 트래픽 리디렉션 구성

서비스 인스턴스를 배포한 후 라우터가 서비스로 리디렉션하는 트래픽의 유형을 구성할 수 있습니다. 트래픽 리디렉션 구성은 방화벽 구성과 유사합니다.

방화벽 구성에 대한 자세한 내용은 [장 7 방화벽 섹션 및 방화벽 규칙](#)을 참조하십시오.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **파트너 서비스**를 선택합니다.
- 3 서비스 인스턴스의 이름을 클릭합니다.
- 4 **트래픽 리디렉션** 탭을 클릭합니다.
- 5 섹션 및 규칙을 추가하거나 제거합니다.

# 트래픽 리디렉션 모니터링

서비스 인스턴스를 배포하고 트래픽 리디렉션을 구성한 후 서비스 인스턴스 안팎으로 이동하는 트래픽 양을 모니터링할 수 있습니다.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **파트너 서비스**를 선택합니다.
- 3 서비스 인스턴스의 이름을 클릭합니다.

**개요** 탭에는 서비스 인스턴스의 구성 및 상태가 표시됩니다.

**4 통계** 탭을 클릭합니다.

서비스 인스턴스 안팎으로 이동하는 데이터 양 및 패킷 수에 대한 정보가 표시됩니다.

**5 새로 고침**을 클릭하여 통계를 업데이트합니다.

NSX Cloud에서는 NSX-T Data Center를 사용하여 공용 클라우드 인벤토리를 관리하고 보호할 수 있습니다.

NSX Cloud 구성 요소의 목록 및 설명은 "NSX-T Data Center 설치 가이드"의 [NSX Cloud 아키텍처 및 구성 요소](#)를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [Cloud Service Manager](#)
- [격리 정책 관리](#)
- [워크로드 VM 등록 및 관리의 개요](#)
- [워크로드 VM 등록](#)
- [워크로드 VM 관리](#)
- [고급 NSX Cloud 기능 사용](#)
- [문제 해결](#)

## Cloud Service Manager

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

CSM 인터페이스는 다음과 같은 범주로 나뉩니다.

- **검색:** 검색 텍스트 상자를 사용하여 공용 클라우드 계정 또는 관련 구성체를 찾을 수 있습니다.
- **클라우드:** 공용 클라우드 인벤토리는 이 범주 아래의 섹션을 통해 관리됩니다.
- **시스템:** 이 범주에서 Cloud Service Manager에 대한 **설정**, **유틸리티** 및 **사용자**에 액세스할 수 있습니다.

CSM의 **클라우드** 하위 섹션으로 이동하면 모든 공용 클라우드 작업을 수행할 수 있습니다.

백업, 복원, 업그레이드, 사용자 관리와 같은 시스템 기반 작업을 수행하려면 **시스템** 하위 섹션으로 이동합니다.

## 클라우드

다음은 **클라우드** 아래의 섹션입니다.

### 클라우드 > 개요

**클라우드**를 클릭하여 공용 클라우드 계정에 액세스합니다.

**개요:** 이 화면의 각 타일은 공용 클라우드 계정과 여기에 포함된 계정, 지역, VPC 또는 VNet 및 인스턴스(워크로드 VM)의 수를 나타냅니다.

다음 작업을 수행할 수 있습니다.

공용 클라우드 계정 또는 구독 추가	<p>하나 이상의 공용 클라우드 계정 또는 구독을 추가할 수 있습니다. 그러면 CSM에서 공용 클라우드 인벤토리를 볼 수 있으며 NSX-T Data Center 및 해당 상태로 관리되는 VM 수를 나타냅니다.</p> <p>자세한 지침은 "NSX-T Data Center 설치 가이드"의 <b>공용 클라우드 계정 추가</b>를 참조하십시오.</p>
NSX Public Cloud Gateway 배포/배포 해제	<p>하나 또는 두 개(HA의 경우)의 PCG를 배포하거나 배포 해제할 수 있습니다. 또한 CSM에서 PCG를 배포 해제할 수도 있습니다.</p> <p>자세한 지침은 "NSX-T Data Center 설치 가이드"의 <b>PCG 배포</b> 또는 <b>PCG 배포 해제</b>를 참조하십시오.</p>
격리 정책을 사용하거나 사용하지 않도록 설정	<p>격리 정책을 사용하거나 사용하지 않도록 설정할 수 있습니다. 자세한 내용은 <a href="#">격리 정책 관리</a> 항목을 참조하십시오.</p>
그리드 및 카드 보기 사이 전환	<p>카드에는 인벤토리 개요가 표시됩니다. 그리드에 더 자세한 내용이 표시됩니다. 보기 유형을 전환하려면 아이콘을 클릭하십시오.</p>

CSM에서는 공용 클라우드 인벤토리를 다양한 방식으로 표현하기 때문에 NSX Cloud와 연결된 모든 공용 클라우드 계정을 전체적으로 볼 수 있습니다.

- 운영 중인 지역의 수를 볼 수 있습니다.
- 지역별 전용 네트워크의 수를 볼 수 있습니다.
- 전용 네트워크당 워크로드 VM의 수를 볼 수 있습니다.

**클라우드** 아래에는 4개의 탭이 있습니다.

UI 요소에 대한 설명은 [CSM 차트 및 아이콘](#)의 내용을 참조하십시오.

### 클라우드 > {공용 클라우드} > 계정

CSM의 [계정] 섹션에는 이미 추가한 공용 클라우드 계정에 대한 정보가 제공됩니다.

각 카드는 클라우드에서 선택한 클라우드 제공자의 공용 클라우드 계정을 나타냅니다.

이 섹션에서 다음 작업을 수행할 수 있습니다.

- 계정 추가
- 계정 편집

- 계정 삭제
- 계정 다시 동기화

## 클라우드 > {공용 클라우드} > 지역

[지역] 섹션에는 선택한 지역의 인벤토리가 표시됩니다.

지역은 공용 클라우드 계정별로 필터링할 수 있습니다. 각 지역에는 VPC 또는 VNet 및 인스턴스가 있습니다. PCG를 배포한 경우 해당 PCG가 여기에서 PCG 상태 표시기가 있는 게이트웨이로 표시됩니다.

## 클라우드 > {공용 클라우드} > VPC 또는 VNet

[VPC] 또는 [VNet] 섹션에는 사설 클라우드 인벤토리가 표시됩니다.

인벤토리는 계정 및 지역별로 필터링할 수 있습니다.

- 각 카드는 하나의 VPC 또는 VNet을 나타냅니다.
- 각 VPC 또는 VNet에 하나 또는 두 개(HA의 경우)의 PCG를 배포할 수 있습니다.
- 그리드 보기로 전환하면 각 VPC 또는 VNet에 대한 자세한 정보를 볼 수 있습니다.
- 다음에 액세스하려면 **작업**을 클릭하십시오.
  - **구성 편집:**
    - 격리 정책을 사용하거나 사용하지 않도록 설정합니다.
    - 프록시 서버 선택을 변경합니다.
  - **NSX Cloud 게이트웨이 배포:** 이 VPC 또는 VNet에서 PCG 배포를 시작하려면 이 옵션을 클릭하십시오. PCG 또는 PCG의고가용성 쌍이 이미 배포된 경우 이 옵션은 사용할 수 없습니다. 자세한 지침은 "NSX-T Data Center 설치 가이드"의 **PCG 배포**를 참조하십시오.

## 클라우드 > {공용 클라우드} > 인스턴스

[인스턴스] 섹션에는 VPC 또는 VNet에 있는 인스턴스의 세부 정보가 표시됩니다.

인스턴스 인벤토리는 계정, 지역 및 VPC 또는 VNet별로 필터링할 수 있습니다.

각 카드는 인스턴스(워크로드 VM)를 나타내며 요약을 표시합니다.

인스턴스에 대한 자세한 내용을 보려면 카드를 클릭하거나 그리드 보기로 전환합니다.

---

**참고** CSM은 NSX로 관리되는 VM에 대해 OS 릴리스 값을 표시하지만 NSX에서 관리되지 않는 VM의 경우 표시되는 OS의 유형은 클라우드 제공자 API에서 가져오므로 세부 정보가 최소화됩니다.

---

## CSM 차트 및 아이콘

CSM은 알아보기 쉬운 직관적인 아이콘을 사용하여 공용 클라우드 구성의 상태를 표시합니다.

---

**참고** 격리 워크플로는 **격리 사용** 설정이 켜져 있는 경우에만 적용됩니다. 이 설정은 기본적으로 꺼져 있습니다.

---

## VNet

그림 16-1. 정상 상태의 NSX Cloud에서 관리되는 VM이 있는 VNet

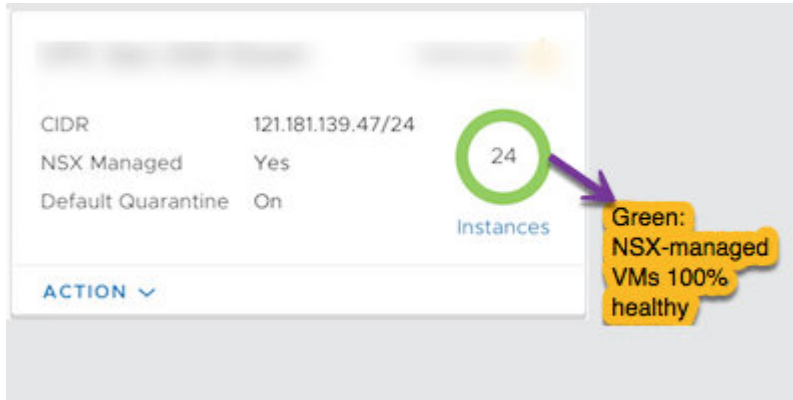


그림 16-2. 오류가 있는 NSX Cloud에서 관리되는 VM이 있는 VNet

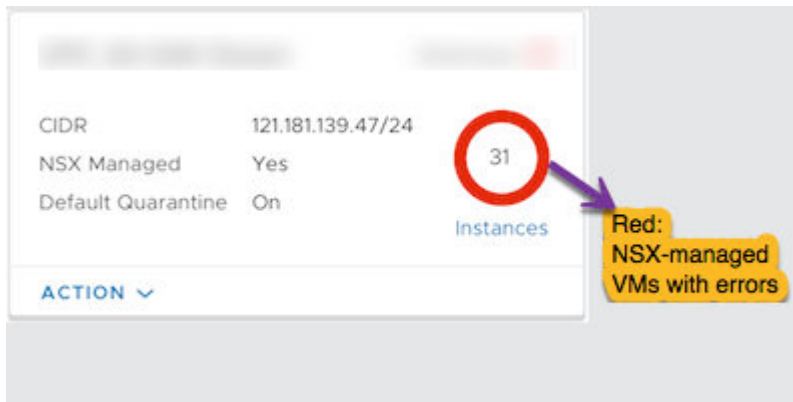


그림 16-3. 전원이 꺼진 VM이 있는 VNet

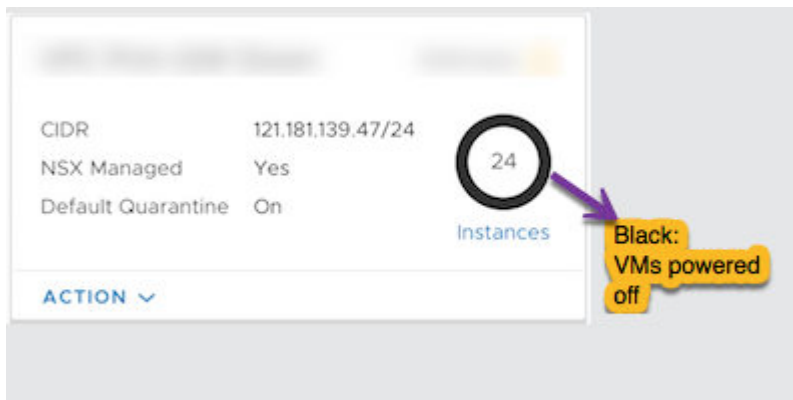




그림 16-4. 기본 격리 상태를 표시하는 VNet

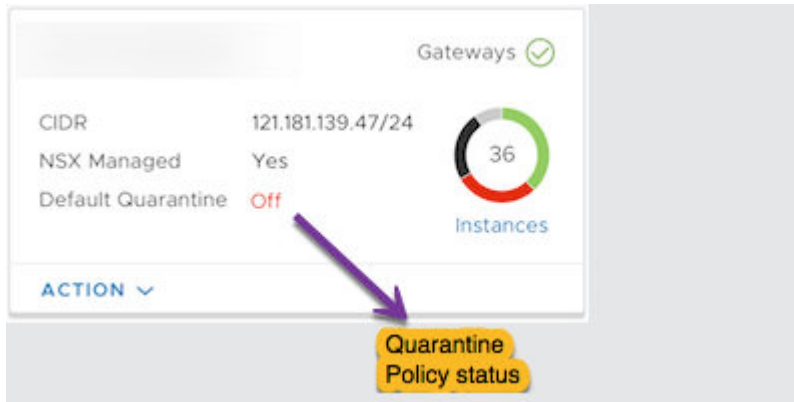
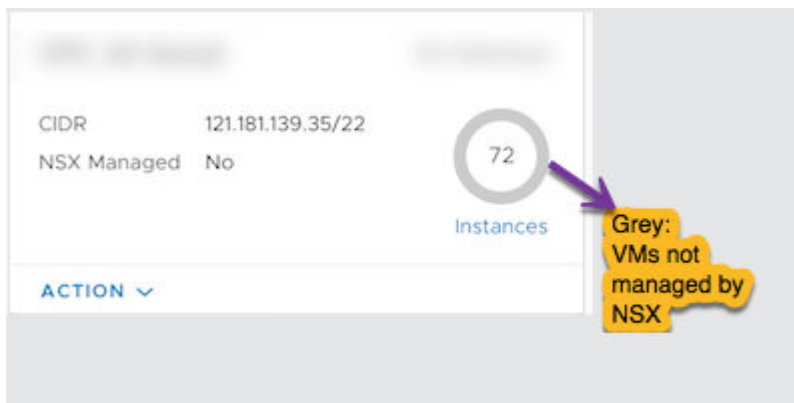


그림 16-5. NSX Cloud에서 관리되지 않는 VM이 있는 VNet



## 인스턴스

### 관리되는 인스턴스

그림 16-6. 정상 상태의 NSX Cloud에서 관리되는 인스턴스

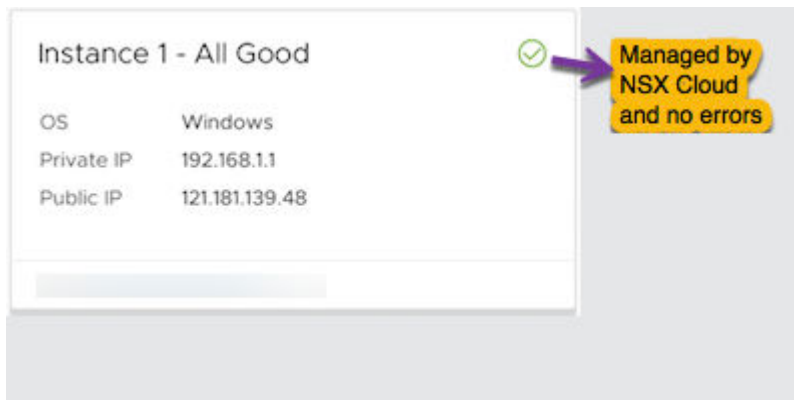


그림 16-7. 오류가 있는 NSX Cloud에서 관리되는 인스턴스

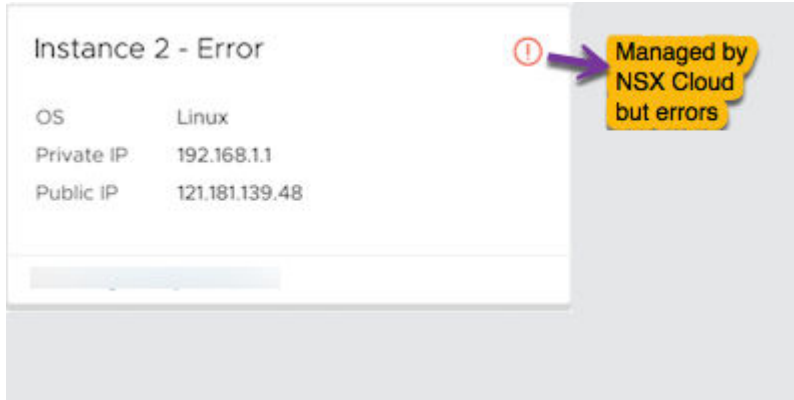


그림 16-8. 오류가 있고 격리된 NSX Cloud에서 관리되는 인스턴스

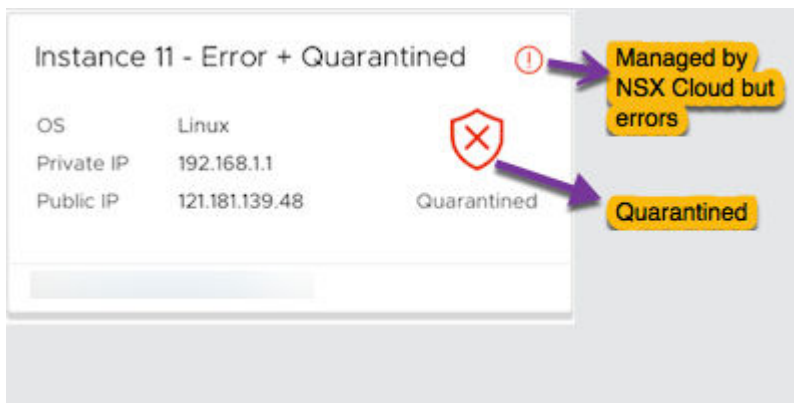


그림 16-9. 격리되었지만 **vm-override-sg** 네트워크 보안 그룹을 적용하여 화이트리스트에 포함된 NSX Cloud에서 관리되는 인스턴스

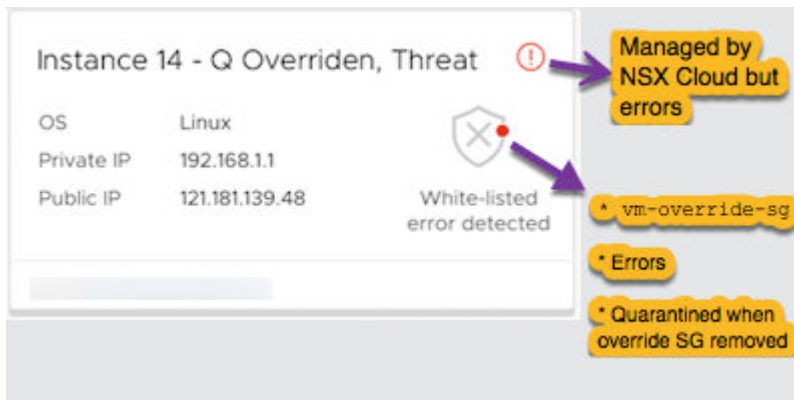
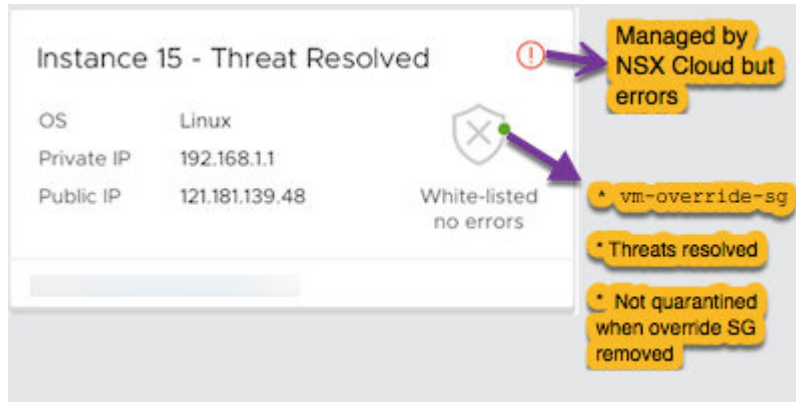


그림 16-10. 격리되고 오류가 해결되어 화이트리스트에 추가된 NSX Cloud에서 관리되는 인스턴스



### 관리되지 않는 인스턴스

그림 16-11. NSX Cloud에서 관리되지 않고 기본적으로 격리된 VM

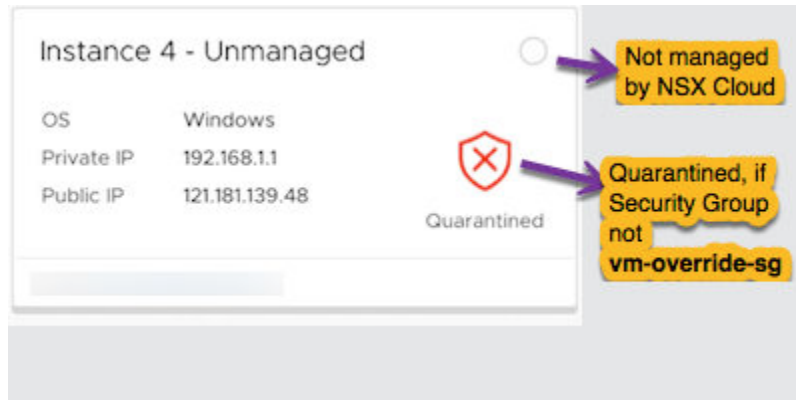
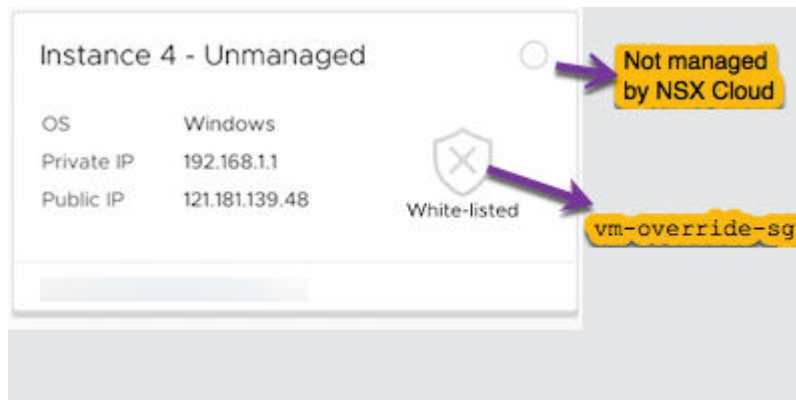


그림 16-12. NSX Cloud에서 관리되지 않지만 **vm-override-sg**를 적용하여 화이트리스트에 추가된 VM



## 공용 클라우드 게이트웨이(PCG)

그림 16-13. 기본 및 보조 PCG가 모두 실행 중인 VNet

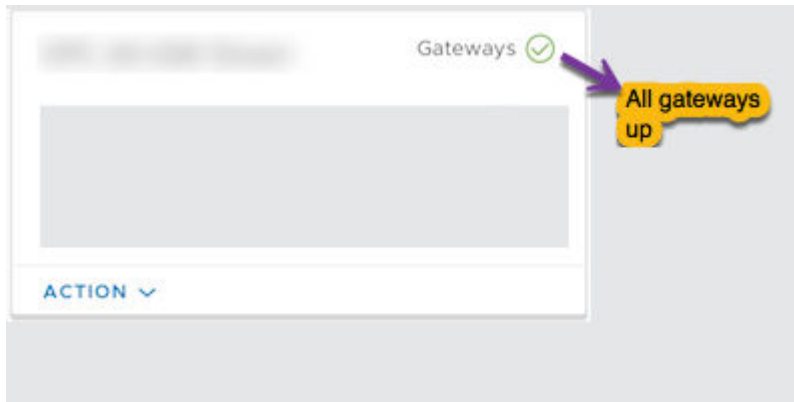


그림 16-14. 기본 또는 보조 PCG 중 하나가 다운된 VNet

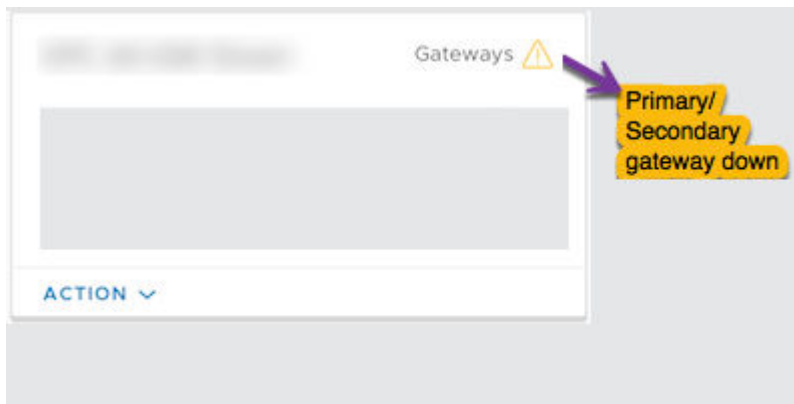
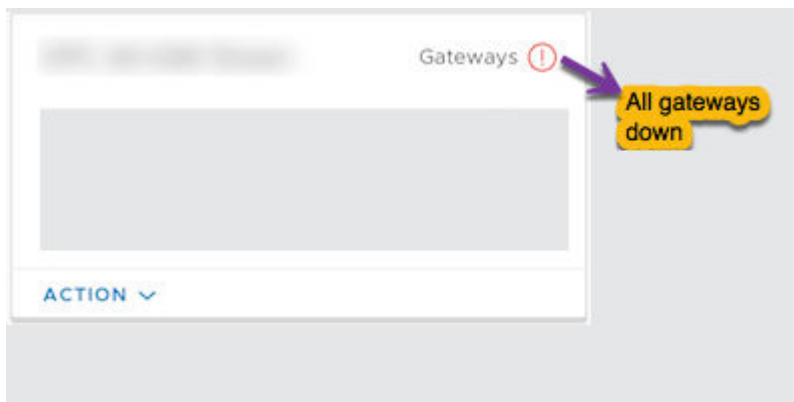


그림 16-15. 기본 및 보조 PCG가 모두 다운된 VNet



## 시스템

다음은 **시스템** 아래의 섹션입니다.

## 시스템 > 설정

이러한 설정은 CSM을 설치할 때 처음 구성됩니다. 나중에 이를 편집할 수 있습니다.

### CSM을 NSX Manager에 연결

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

#### 사전 요구 사항

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

#### 절차

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

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

명령의 출력은 NSX Manager에 고유한 숫자열입니다.

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

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

- 5 NSX Manager의 세부 정보를 입력합니다.

옵션	설명
<b>NSX Manager 호스트 이름</b>	가능한 경우 NSX Manager의 FQDN(정규화된 도메인 이름)을 입력합니다. NSX Manager의 IP 주소를 입력할 수도 있습니다.
<b>관리 자격 증명</b>	엔터프라이즈 관리자 역할이 있는 사용자 이름과 암호를 입력합니다.
<b>관리자 지문</b>	2단계에서 확보한 NSX Manager의 지문 값을 입력합니다.

- 6 **연결**을 클릭합니다.

CSM에서 NSX Manager 지문을 확인하고 연결을 설정합니다.

#### (선택 사항) 프록시 서버 구성

신뢰할 수 있는 HTTP 프록시를 통해 인터넷에 접속된 HTTP/HTTPS 트래픽을 모두 라우팅하고 모니터링하려는 경우, CSM에 최대 5개의 프록시 서버를 구성할 수 있습니다.

PCG 및 CSM의 모든 공용 클라우드 통신은 선택한 프록시 서버를 통해 라우팅됩니다.

PCG에 대한 프록시 설정은 CSM에 대한 프록시 설정과 상관이 없습니다. PCG에 대해 다른 프록시 서버를 선택하거나 프록시 서버를 선택하지 않을 수 있습니다.

다음과 같은 인증 수준을 선택할 수 있습니다.

- 자격 증명 기반 인증.
- HTTPS 가로채기에 대한 자격 증명 기반 인증.
- 인증 없음.

## 절차

- 1 **시스템 > 설정**을 클릭합니다. 그런 다음 **프록시 서버** 패널에서 **구성**을 클릭합니다.

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

- 2 [프록시 서버 구성] 화면에서 다음과 같은 세부 정보를 입력합니다.

옵션	설명
기본값	이 라디오 버튼을 사용하여 기본 프록시 서버를 나타냅니다.
프로파일 이름	프록시 서버 프로파일 이름을 제공합니다. 이 항목은 필수입니다.
프록시 서버	프록시 서버의 IP 주소를 입력합니다. 이 항목은 필수입니다.
포트	프록시 서버의 포트를 입력합니다. 이 항목은 필수입니다.
인증	선택 사항입니다. 추가 인증을 설정하려면 이 확인란을 선택하고 유효한 사용자 이름과 암호를 제공합니다.
사용자 이름	이 항목은 [인증] 확인란을 선택하는 경우 필수입니다.
암호	이 항목은 [인증] 확인란을 선택하는 경우 필수입니다.
인증서	선택 사항입니다. HTTPS 가로채기에 대한 인증서를 제공하려면 이 확인란을 선택하고 나타나는 텍스트 상자에 인증서를 복사하여 붙여넣습니다.
프록시 없음	구성된 프록시 서버를 사용하지 않으려면 이 옵션을 선택합니다.

## 시스템 > 유틸리티

다음 유틸리티를 사용할 수 있습니다.

### 백업 및 복원

CSM 백업 및 복원은 NSX Manager 백업 및 복원에 사용한 것과 동일한 지침을 따릅니다. 자세한 내용은 [NSX Manager 백업 및 복원](#) 항목을 참조하십시오.

### 지원 번들

CSM용 지원 번들을 검색하려면 **다운로드**를 클릭합니다. 이것은 문제 해결에 사용됩니다. 자세한 내용은 "NSX-T Data Center 문제 해결 가이드"를 참조하십시오.

## 시스템 > 사용자

사용자는 RBAC(역할 기반 액세스 제어)를 통해 관리됩니다.

자세한 내용은 [사용자 계정 및 역할 기반 액세스 제어 관리](#) 항목을 참조하십시오.

## 격리 정책 관리

격리 정책을 사용하거나 사용하지 않도록 설정하는 방법을 알아 보고 이것이 워크로드 VM에 미치는 영향을 이해합니다.

NSX Cloud는 공용 클라우드 보안 그룹을 사용하여 위협을 감지합니다. 예를 들어 격리 정책을 사용하도록 설정하는 경우 NSX 에이전트가 악의적인 의도를 가진 관리되는 VM에서 강제로 중지되면 quarantine(Microsoft Azure의 경우) 또는 default(AWS의 경우) 보안 그룹을 사용하여 손상된 VM을 격리합니다.

### 일반 권장 사항:

**브라운필드** 배포에 대해 “사용 안 함” 으로 시작: 격리 정책은 기본적으로 사용하지 않도록 설정됩니다. 공용 클라우드 환경에 VM이 이미 설정되어 있는 경우 워크로드 VM을 등록할 때까지 격리 정책에 대해 사용 안 함 모드를 사용합니다. 이렇게 하면 기존 VM이 자동으로 격리되지 않습니다.

**그린필드** 배포에 대해 “사용” 으로 시작: 그린필드 배포의 경우 VM에 대한 위협 감지를 NSX Cloud에서 관리할 수 있도록 격리 정책을 사용하는 것이 좋습니다.

**참고** 격리 정책을 사용하도록 설정하는 경우 워크로드 VM을 등록할 수 있도록 워크로드 VM에 대해 vm\_override\_sg를 적용하고 NSX Cloud에 의해 관리되는 상태가 되면 이 보안 그룹을 제거하십시오. 2분 내로 적절한 보안 그룹이 VM에 적용됩니다.

## 격리 정책을 사용하거나 사용하지 않도록 설정하는 방법

PCG를 배포할 때 격리 정책을 설정하거나 해제할 수 있습니다. 다음 단계에 따라 이후에 격리 정책을 사용하거나 사용하지 않도록 설정하십시오.

### 사전 요구 사항

VPC 또는 VNet에 하나 또는 한 쌍의 PCG를 배포해야 합니다.

### 절차

- CSM에 로그인하고 공용 클라우드로 이동합니다.
  - AWS를 사용 중인 경우 **클라우드 > AWS > VPC**로 이동합니다. 하나 또는 한 쌍의 PCG가 배포되어 실행 중인 VPC를 클릭합니다.
  - Microsoft Azure를 사용 중인 경우 **클라우드 > Azure > VNet**으로 이동합니다. 하나 또는 한 쌍의 PCG가 배포되어 실행 중인 VNet을 클릭합니다.
- 다음 중 하나를 사용하여 옵션을 사용하도록 설정합니다.

- 타일 보기에서 **작업 > 구성 편집**을 클릭합니다.



- 그리드 보기에 있는 경우 VPC 또는 VNet 옆의 확인란을 선택하고 **작업 > 구성 편집**을 클릭합

니다.

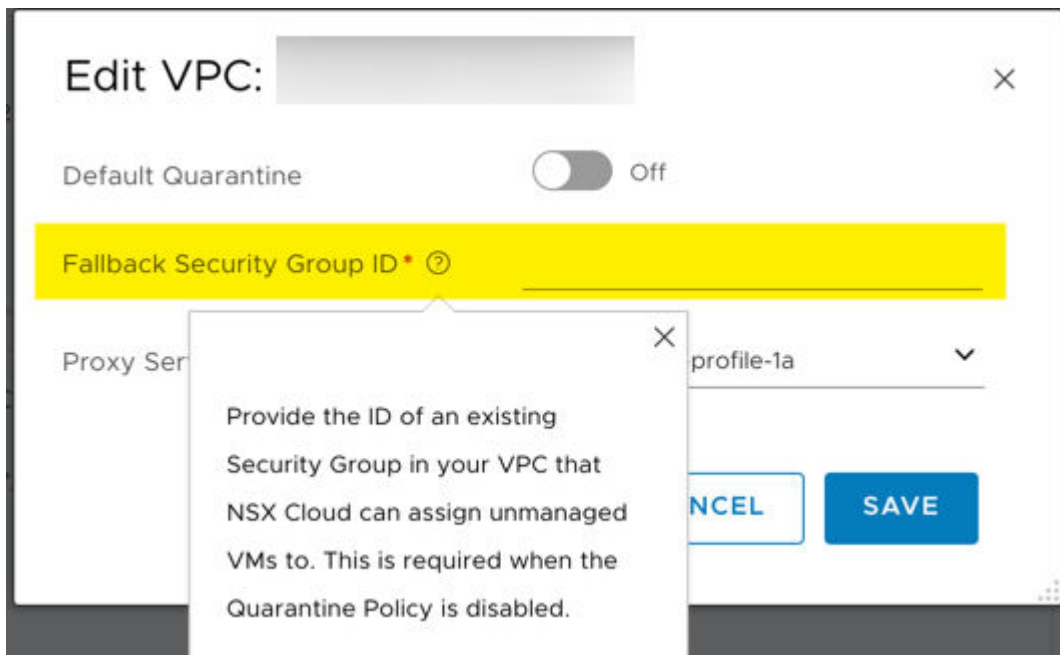


- ◆ VPC 또는 VNet의 페이지에 있는 경우 작업 아이콘을 클릭하여 **구성 편집**으로 이동합니다.



- 3 기본 격리를 설정 또는 해제하여 격리를 사용하거나 사용하지 않도록 설정합니다.
- 4 격리 정책을 사용하지 않도록 설정하는 경우에는 폴백 보안 그룹을 제공해야 합니다.

**참고** 폴백 보안 그룹은 공용 클라우드에 있는 기존의 사용자 정의 보안 그룹이어야 합니다. NSX Cloud 보안 그룹은 폴백 보안 그룹으로 사용할 수 없습니다. NSX Cloud 보안 그룹의 목록에 대해서는 [공용 클라우드에 대한 NSX Cloud 보안 그룹](#)의 내용을 참조하십시오.



- 이 VPC 또는 VNet에 있는 관리되지 않는 또는 격리된 모든 VM은 격리 정책을 사용하지 않도록 설정할 때 폴백 보안 그룹이 할당됩니다.
- 관리되는 모든 VM은 NSX Cloud에서 할당된 보안 그룹을 유지합니다. 격리 정책을 사용하지 않도록 설정한 후 그러한 VM이 처음으로 태그 해제되고 관리되지 않게 되는 경우에도 폴백 보안 그룹이 할당됩니다.

- 5 **저장**을 클릭합니다.

## 격리 정책을 사용하지 않을 때의 영향



## 격리 정책: 사용 안 함

격리 정책을 사용하지 않도록 설정하면:

- NSX Cloud가 이 VPC 또는 VNet에서 시작된 VM에 보안 그룹을 할당하지 않습니다. 위협 감지를 사용하도록 설정하려면 VM에 적절한 NSX Cloud 보안 그룹을 할당해야 합니다.

Microsoft Azure 포털 또는 AWS 콘솔에서:

- ■ Microsoft Azure 또는 AWS에서 제공하는 언더레이 네트워크를 사용하려는 VM에 `vm-underlay-sg`를 할당합니다.

## 격리 정책: 사용에서 사용 안 함으로 변경됨

다음 표에는 격리 정책이 사용되도록 설정되었다가 사용되지 않도록 설정된 경우 보안 그룹 할당에 대한 영향이 캡처되어 있습니다.

표 16-1. 격리 정책 사용 안 함의 보안 그룹 영향

VM-ID	관리됨?	보안 그룹	격리 정책을 사용하지 않도록 설정한 후 VM에 대한 보안 그룹
VM1	예	vm_underlay_sg	vm_underlay_sg . 이 VM에서 nsx.network 태그를 제거하면 NSX 관리에서 이를 제거하기 위해 이 VM에도 풀백 보안 그룹이 할당됩니다.
VM 2	예	default (AWS) 또는 quarantine (Microsoft Azure)	격리 정책을 사용하지 않도록 설정할 때 지정하는 풀백 보안 그룹. 자세한 내용은 <a href="#">격리 정책을 사용하거나 사용하지 않도록 설정하는 방법</a> 항목을 참조하십시오.
VM 3	아니요	vm_override_sg	격리 정책을 사용하지 않도록 설정할 때 지정하는 풀백 보안 그룹.
VM 4	아니요	default (AWS) 또는 quarantine (Microsoft Azure)	격리 정책을 사용하지 않도록 설정할 때 지정하는 풀백 보안 그룹.

**참고** 격리 정책 사용 안 함은 PCG 배포 해제에 필요합니다. 자세한 내용은 "NSX-T Data Center 설치 가이드"의 **PCG 배포 해제**를 참조하십시오.

## 격리 정책을 사용할 때의 영향

## 격리 정책: 사용

격리 정책을 사용하도록 설정하면:

- 이 VPC 또는 VNet에 속하는 워크로드 VM의 모든 인터페이스에 대한 SG(보안 그룹) 또는 NSG(네트워크 보안 그룹) 할당이 다음과 같은 조건 하에 NSX Cloud에서 관리됩니다.
  - 관리되지 않는 VM은 Microsoft Azure에서 quarantine NSG 및 AWS에서 default 보안 그룹이 할당되고 격리됩니다. 이렇게 하면 아웃바운드 트래픽이 제한되고 해당 VM에 대한 모든 인바운드 트래픽이 중지됩니다.
  - 관리되지 않는 VM에 NSX 에이전트를 설치하고 공용 클라우드에서 nsx.network 태그를 지정하면 해당 VM이 NSX로 관리되는 VM이 될 수 있습니다. 기본 시나리오에서 NSX Cloud는 적절한 인바운드/아웃바운드 트래픽 허용하기 위해 vm-underlay-sg를 할당합니다.
  - VM에서 위협이 감지되면(예: NSX 에이전트가 VM에서 중지됨) NSX로 관리되는 VM에도 quarantine 또는 default 보안 그룹을 할당하고 격리할 수 있습니다.
  - 보안 그룹이 수동으로 변경되면 2분 내에 NSX 결정 보안 그룹으로 되돌려집니다.
  - VM을 격리 구역 외부로 이동하려면 vm-override-sg를 이 VM에 대한 유일한 보안 그룹으로 할당합니다. NSX Cloud는 vm-override-sg 보안 그룹을 자동으로 변경하지 않으며 VM에 대한 SSH 및 RDP 액세스를 허용합니다. vm-override-sg를 제거하면 VM 보안 그룹이 NSX 결정 보안 그룹으로 다시 되돌려집니다.

---

**참고** 격리 정책을 사용하도록 설정하는 경우 VM에 NSX 에이전트를 설치하기 전에 vm-override-sg를 할당합니다. NSX 에이전트를 설치하고 VM에 언더레이로 태그를 지정하는 프로세스를 수행한 후에 VM에서 vm-override-sg NSG를 제거합니다. NSX Cloud는 그런 다음 NSX로 관리되는 VM에 적절한 보안 그룹을 자동으로 할당합니다. 이 단계는 NSX Cloud에 대해 VM을 준비하는 동안 VM에 quarantine 또는 default 보안 그룹이 할당되지 않도록 하기 때문에 필요합니다.

---

## 격리 정책: 사용 안 함에서 사용으로 변경됨

다음 표에는 격리 정책이 사용되지 않도록 설정되었다가 사용되도록 설정된 경우 보안 그룹 할당에 대한 영향이 캡처되어 있습니다.

표 16-2. 격리 정책 사용의 보안 그룹 영향

VM-ID	관리됨?	위협 감지됨?	격리 정책 사용 후 보안 그룹
VM1	예	아니요	vm_underlay_sg
VM 2	예	예	default (AWS) 또는 quarantine (Microsoft Azure)
<b>참고</b> 수동으로 vm_override_sg를 관리되는 VM에 할당할 수 있습니다. 이 경우 격리 모드가 종료되고 SSH 또는 RDP를 통해 해당 VM에 액세스하여 문제를 복원할 수 있습니다. <b>격리 정책: 사용</b> 항목을 참조하십시오.			
VM 3	아니요	해당 없음	default (AWS) 또는 quarantine (Microsoft Azure)

## 공용 클라우드에 대한 NSX Cloud 보안 그룹

다음 보안 그룹은 PCG 배포 시 NSX Cloud에서 생성됩니다.

**gw** 보안 그룹은 각각의 PCG 인터페이스에 적용됩니다.

표 16-3. NSX Cloud에서 PCG 인터페이스용으로 생성된 공용 클라우드 보안 그룹

보안 그룹 이름	Microsoft Azure에서 사용할 수 있습니까?	AWS에서 사용할 수 있습니까?	전체 이름
gw-mgmt-sg	예	예	게이트웨이 관리 보안 그룹
gw-uplink-sg	예	예	게이트웨이 업링크 보안 그룹
gw-vtep-sg	예	예	게이트웨이 다운링크 보안 그룹

표 16-4. 워크로드 VM용 NSX Cloud에서 생성된 공용 클라우드 보안 그룹

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

표 16-4. 워크로드 VM용 NSX Cloud에서 생성된 공용 클라우드 보안 그룹 (계속)

보안 그룹 이름	Microsoft Azure에서 사용할 수 있습니까?	AWS에서 사용할 수 있습니까?	설명
vm-outbound-bypass-sg	예	예	VM 아웃바운드 바이패스 보안 그룹(현재 릴리스에서는 사용되지 않음)
vm-inbound-bypass-sg	예	예	VM 인바운드 바이패스 보안 그룹(현재 릴리스에서는 사용되지 않음)

## 워크로드 VM 등록 및 관리의 개요

공용 클라우드의 등록 워크플로의 개요는 순서도를 참조하십시오.

Day-0 워크플로는 "NSX-T Data Center 설치 가이드"의 [NSX Cloud 구성 요소 설치](#)를 참조하십시오.

## 지원되는 운영 체제

워크로드 VM에 대해 NSX Cloud에서 현재 지원되는 운영 체제 목록입니다.

현재 다음 운영 체제가 지원됩니다.

**참고** 예외는 "NSX-T Data Center 릴리스 정보"의 NSX Cloud 알려진 문제 섹션을 참조하십시오.

- Red Hat Enterprise Linux(RHEL) 7.2, 7.3, 7.4, 7.5
- CentOS 7.2, 7.3, 7.4, 7.5
- Oracle Enterprise Linux 7.2, 7.3, 7.4(Unbreakable Enterprise Kernel 버전은 지원되지 않음).

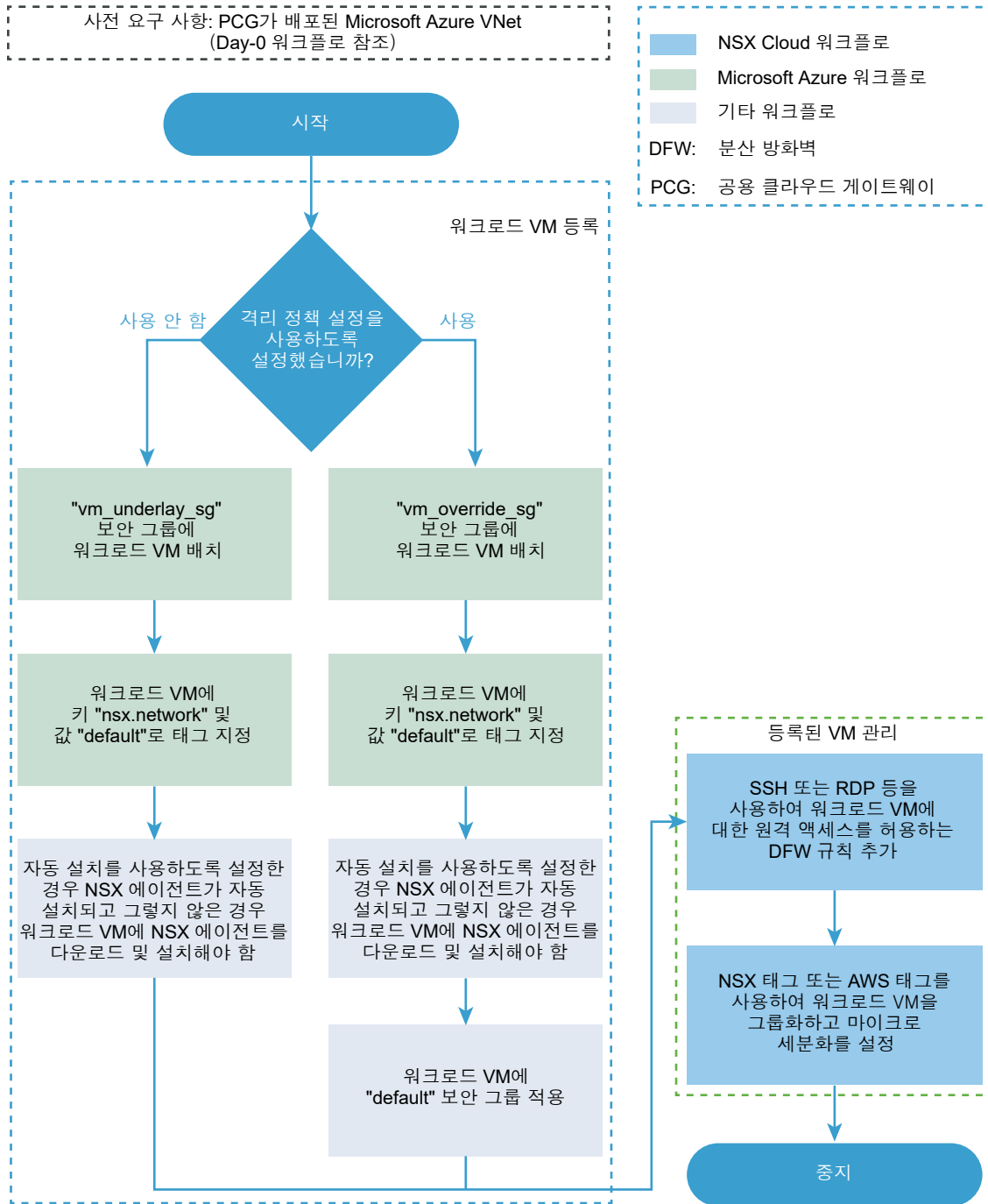
**참고** SE Linux는 Oracle Enterprise Linux, Red Hat Enterprise Linux 및 CentOS에 대해 지원되지 않음

- Ubuntu 14.04, 16.04
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

## Microsoft Azure에서 워크로드 VM을 등록하는 방법

Microsoft Azure에서 워크로드 VM을 등록하는 단계에 대한 개요는 이 순서도를 참조하십시오.

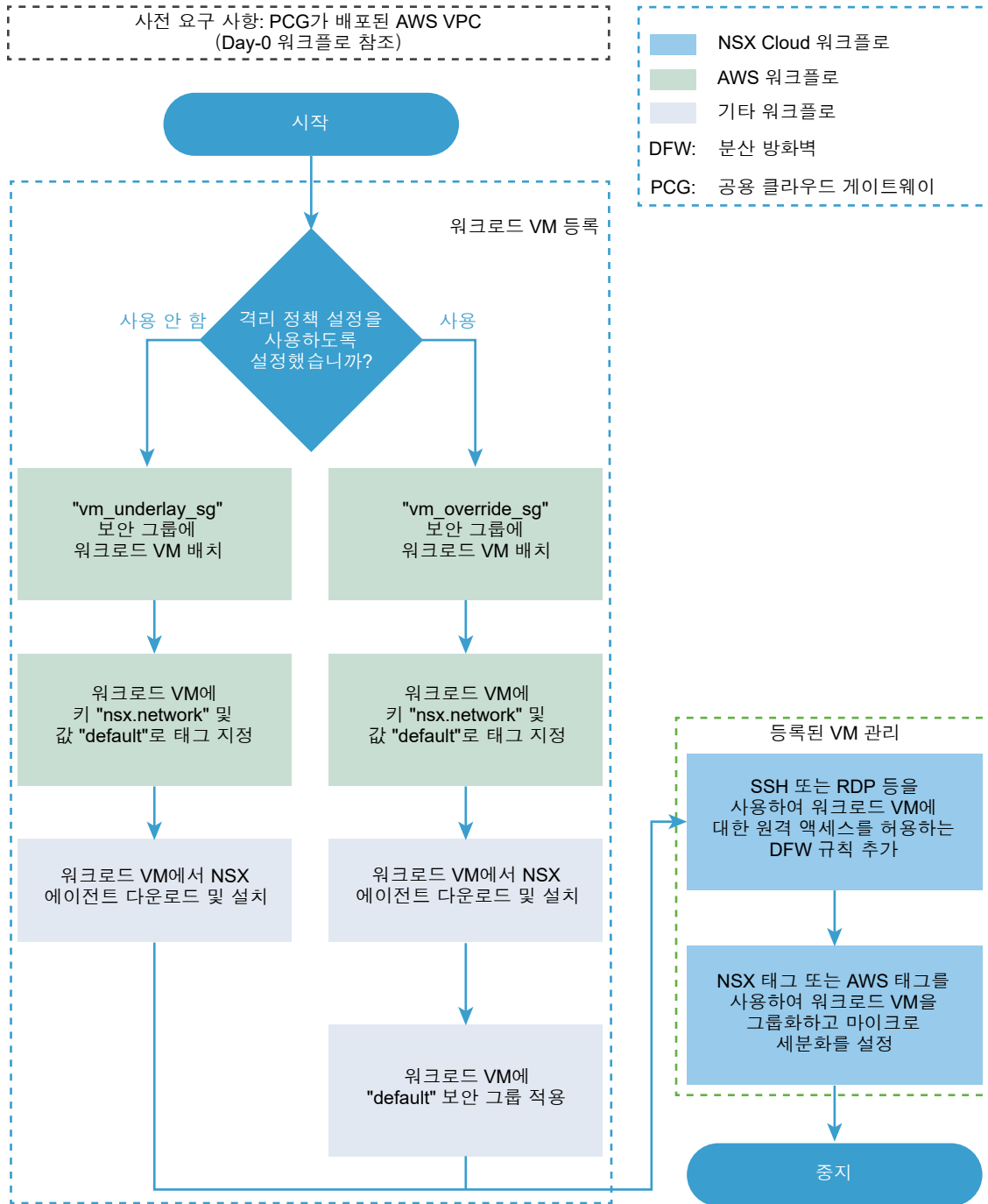
그림 16-16. Microsoft Azure에 대한 Day-N 등록 워크플로



## AWS에서 워크로드 VM을 등록하는 방법

AWS에서 워크로드 VM을 등록하는 단계에 대한 개요는 이 순서도를 참조하십시오.

그림 16-17. AWS에 대한 Day-N 등록 워크플로



## 워크로드 VM 등록

NSX-T Data Center를 사용하여 워크로드 VM을 관리하려면 워크로드 VM을 등록합니다.

## 공용 클라우드에서 VM 태그 지정

NSX-T Data Center를 사용하여 관리하려는 VM에 **nsx.network** 태그를 적용합니다.

## 사전 요구 사항

워크로드 VM이 호스팅되는 VPC 또는 VNet이 NSX Cloud에 등록되어 있어야 합니다. 자세한 내용은 “NSX-T Data Center 설치 가이드”의 **공용 클라우드 인벤토리 추가**를 참조하십시오.

## 절차

- 1 공용 클라우드 계정에 로그인하고 NSX Cloud에 등록된 VPC 또는 VNet으로 이동합니다.
- 2 NSX-T Data Center를 사용하여 관리하려는 VM을 선택합니다.
- 3 VM에 대한 태그 세부 정보를 추가하고 변경 내용을 저장합니다.

```
Name: nsx.network
Value: default
```

**참고** 이 태그는 VM 수준 또는 인터페이스 수준에서 동일한 효과를 적용할 수 있습니다.

## 예

### 다음에 수행할 작업

이러한 VM에 NSX 에이전트를 설치합니다. [NSX 에이전트 설치](#)의 내용을 참조하십시오.

Microsoft Azure를 사용하는 경우 태그 지정된 VM에 NSX 에이전트를 자동으로 설치할 수 있습니다. 자세한 내용은 [NSX 에이전트 자동 설치](#) 항목을 참조하십시오.

## NSX 에이전트 설치

워크로드 VM에 NSX 에이전트 설치

### Windows VM에 NSX 에이전트 설치

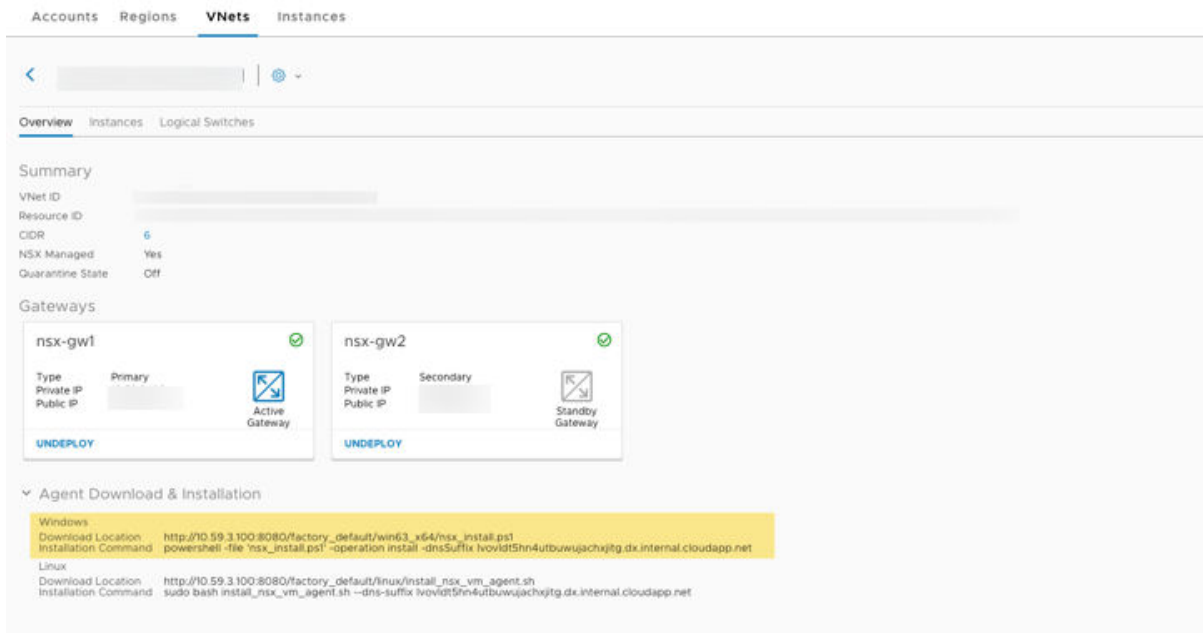
다음 지침에 따라 Windows 워크로드 VM에 NSX 에이전트를 설치합니다.

현재 지원되는 Microsoft Windows 버전 목록은 [지원되는 운영 체제](#)를 참조하십시오.

## 절차

- 1 CSM에 로그인하고 공용 클라우드로 이동합니다.
  - a AWS를 사용 중인 경우 **클라우드 > AWS > VPC**로 이동합니다. 하나 또는 한 쌍의 PCG가 배포되어 실행 중인 VPC를 클릭합니다.
  - b Microsoft Azure를 사용 중인 경우 **클라우드 > Azure > VNet**으로 이동합니다. 하나 또는 한 쌍의 PCG가 배포되어 실행 중인 VNet을 클릭합니다.

- 2 화면의 **에이전트 다운로드 및 설치** 섹션에서 **Windows** 아래에 있는 **다운로드 위치** 및 **설치 명령**을 적어 둡니다.



**참고** 설치 명령의 DNS 접미사는 PCG를 배포할 때 선택한 DNS 설정과 일치하도록 동적으로 생성됩니다.

- 3 Windows 워크로드 VM에 관리자 권한으로 연결합니다.
- 4 CSM에서 확인한 **다운로드 위치**에서 Windows VM에 대한 설치 스크립트를 다운로드합니다. 원하는 브라우저(예: Internet Explorer)를 사용하여 스크립트를 다운로드할 수 있습니다. 브라우저의 기본 다운로드 디렉토리(예: "C:\Downloads")에 다운로드됩니다.
- 5 PowerShell 프롬프트를 열어서 다운로드한 스크립트가 포함된 디렉토리로 이동합니다.
- 6 CSM에서 확인한 **설치 명령**을 사용하여 다운로드한 스크립트를 실행합니다.

예:

```
c:\W> powershell -file 'nsx_install.ps1' -operation install -dnsSuffix <>
```

**참고** 동일한 디렉토리에 있거나 PowerShell 스크립트가 해당 경로에 이미 있는 경우가 아니면 파일 인수에 전체 경로가 필요합니다. 예를 들어 스크립트를 C:\Downloads에 다운로드한 경우 현재 이 디렉토리에 있지 않으면 스크립트에 `powershell -file 'C:\Downloads\nsx_install.ps1'` ... 위치를 포함해야 합니다.

- 7 스크립트가 실행되고 완료되면 NSX 에이전트가 성공적으로 설치되었는지 여부를 나타내는 메시지가 표시됩니다.

**참고** 스크립트는 기본 네트워크 인터페이스를 기본값으로 간주합니다.



모든 스크립트 옵션 목록 및 제거 지침은 [Windows VM용 NSX 에이전트 설치 스크립트 옵션](#) 항목을 참조하십시오.

다음에 수행할 작업

[위크로드 VM 관리](#)

## Linux VM에 NSX 에이전트 설치

다음 지침에 따라 Linux 위크로드 VM에 NSX 에이전트를 설치합니다.

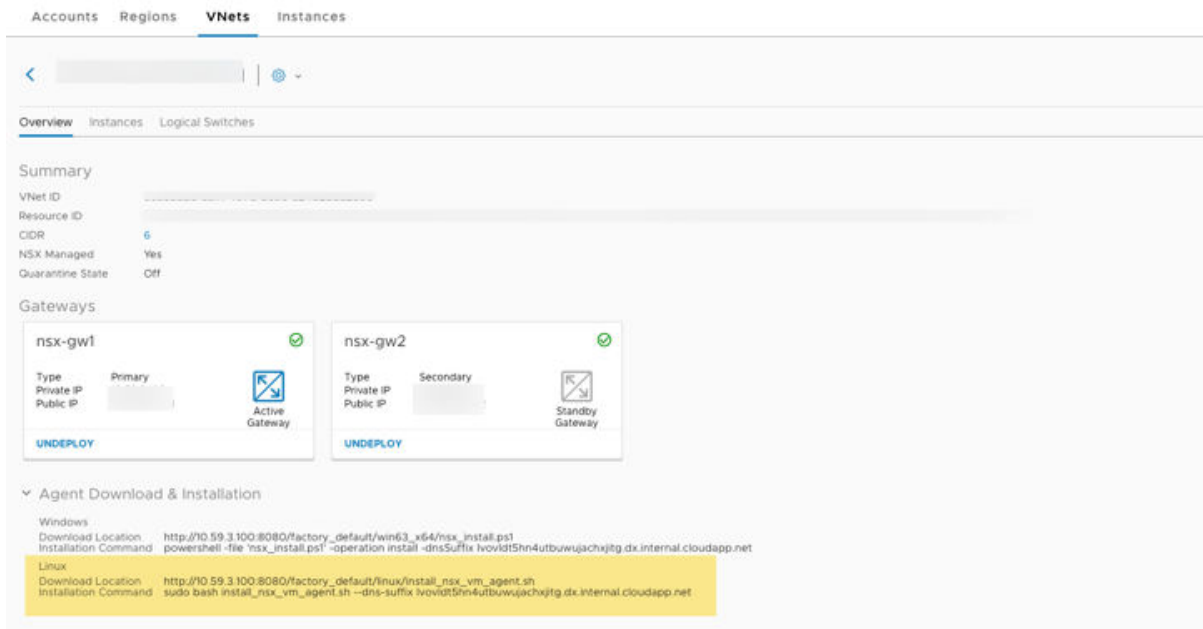
현재 지원되는 Linux 배포 목록은 [지원되는 운영 체제](#) 항목을 참조하십시오.

사전 요구 사항

NSX 에이전트 설치 스크립트를 실행하려면 **wget** 및 **nslookup** 명령이 필요합니다.

절차

- 1 CSM에 로그인하고 공용 클라우드로 이동합니다.
  - a AWS를 사용 중인 경우 **클라우드 > AWS > VPC**로 이동합니다. 하나 또는 한 쌍의 PCG가 배포되어 실행 중인 VPC를 클릭합니다.
  - b Microsoft Azure를 사용 중인 경우 **클라우드 > Azure > VNet**으로 이동합니다. 하나 또는 한 쌍의 PCG가 배포되어 실행 중인 VNet을 클릭합니다.
- 2 화면의 **에이전트 다운로드 및 설치** 섹션에서 **Linux** 아래에 있는 **다운로드 위치** 및 **설치 명령**을 적어둡니다.



**참고** 설치 명령의 DNS 접미사는 PCG를 배포할 때 선택한 DNS 설정과 일치하도록 동적으로 생성됩니다.

- 3 슈퍼유저 권한으로 Linux 위크로드 VM에 로그인합니다.

- 4 `wget` 또는 동급을 사용하여 CSM에서 확인한 **다운로드 위치**에서 Linux VM에 대한 설치 스크립트를 다운로드합니다. 설치 스크립트는 `wget` 명령을 실행한 디렉토리에 다운로드됩니다.
- 5 필요한 경우 설치 스크립트에 대한 권한을 실행이 가능하도록 변경하고 실행합니다.

```
$ sudo chmod +x install_nsx_vm_agent.sh
$ sudo bash install_nsx_vm_agent.sh --dns-suffix <>
```

**참고:** Red Hat Enterprise Linux 및 해당 파생 제품에서 SELinux가 지원되지 않습니다. NSX 에이전트를 설치하려면 SELinux를 사용하지 않도록 설정합니다.

- 6 NSX 에이전트 설치가 시작되면 Linux VM에 대한 연결이 끊어집니다. 화면에 다음과 같은 메시지가 표시됩니다. `Installation completed!!! Starting NSX Agent service. SSH connection will now be lost.` VM에 다시 연결하여 온보딩 프로세스를 완료합니다.

## 결과

NSX 에이전트는 워크로드 VM에 설치됩니다.

## 참고

- NSX 에이전트가 설치된 후 포트 8888은 VM에서 열린 상태로 표시되지만 언더레이 모드에서 VM에 대해 차단되어 있으며 고급 문제 해결에 필요한 경우에만 사용해야 합니다.
- 스크립트는 `eth0`을 기본 인터페이스로 사용합니다. 스크립트 옵션 목록 및 제거 지침은 [Linux VM용 NSX 에이전트 설치 스크립트 옵션](#) 항목을 참조하십시오.

다음에 수행할 작업

## 워크로드 VM 관리

## NSX 에이전트 설치 스크립트 옵션 및 제거

NSX 에이전트 설치 스크립트는 구성 가능한 옵션을 제공합니다. 아래 표에는 이러한 옵션이 나열되어 있습니다.

## Windows VM용 NSX 에이전트 설치 스크립트 옵션

표 16-5.

옵션	설명
-gateway <ip dns>	<p>NSX Public Cloud Gateway IP 또는 DNS 이름. PCG에 IP 주소를 사용하려면 이 옵션을 지정합니다. 이 매개 변수가 지정되지 않은 경우 PCG의 기본 DNS 이름이 사용됩니다.</p> <ul style="list-style-type: none"> <li>■ AWS의 PCG DNS 이름: nsx-gw.vmware.local</li> <li>■ Microsoft Azure의 PCG DNS 이름: nsx-gw</li> </ul> <p><b>참고</b> PCG의 HA 모드에서 Microsoft Azure VM 등에서 두 PCG 이름을 사용하여 "--gateway" 옵션을 지정합니다. --gateway "nsx-gw1;nsx-gw2"</p>
-noStart true	NSX 에이전트가 설치된 후에 VM의 VHD를 생성할 수 있습니다. 이 옵션을 사용하여 설치 스크립트를 실행합니다. 그런 다음 Microsoft Azure Portal에서 이 VM의 VHD를 생성합니다.
-downloadPath <path>	<p>파일을 다운로드해야 하는 디렉토리의 경로입니다. 경로에 이스케이프 문자가 포함된 경우 작은 따옴표로 묶습니다.</p> <p>기본 = %temp%</p>
-silentInstall <true/false>	<p>true로 설정되면 스크립트가 자동 설치를 실행합니다.</p> <p>기본값은 false입니다.</p>
-noSigCheck <true/false>	<p>바이너리의 서명을 검사할지 여부를 지정할 수 있습니다.</p> <p>기본값 = false</p>
-logLevel <value>	<p>NSX 구성 요소의 로그 수준을 지정할 수 있습니다.</p> <p>기본값 = 1</p> <p>세부 정보 표시 = 3</p>
-operation <install/uninstall>	<p>install 또는 uninstall 중에서 수행할 작업을 지정할 수 있습니다.</p> <p>기본값 = install</p>
-bundlePath <path>	<p>NSX VM 에이전트 번들에 대한 로컬 경로 지정할 수 있습니다.</p> <p>기본 옵션은 PCG에서 번들을 다운로드하는 것입니다.</p>

## Windows VM에서 NSX 에이전트 제거

- 1 RDP를 사용하여 VM에 원격 로그인합니다.
- 2 설치 스크립트를 제거 옵션과 함께 실행합니다.

```
Wnsx_install.ps1 -operation uninstall
```

## Linux VM용 NSX 에이전트 설치 스크립트 옵션

표 16-6.

옵션	설명
--gateway <ip dns>	<p>NSX Public Cloud Gateway IP 또는 DNS 이름. PCG에 IP 주소를 사용하려면 이 옵션을 지정합니다. 이 매개 변수가 지정되지 않은 경우 PCG의 기본 DNS 이름이 사용됩니다.</p> <ul style="list-style-type: none"> <li>■ AWS의 PCG DNS 이름: nsx-gw.vmware.local</li> <li>■ Microsoft Azure의 PCG DNS 이름: nsx-gw</li> </ul> <p><b>참고</b> PCG의 HA 모드에서 Microsoft Azure VM 등에서 두 PCG 이름을 사용하여 "--gateway" 옵션을 지정합니다. --gateway "nsx-gw1;nsx-gw2"</p>
--no-start	<p>NSX 에이전트가 설치된 후에 VM의 VHD를 생성할 수 있습니다. 이 옵션을 사용하여 설치 스크립트를 실행합니다. 그런 다음 Microsoft Azure Portal에서 이 VM의 VHD를 생성합니다.</p>
--uninstall	<p>NSX 에이전트를 제거하려면 이 옵션과 함께 스크립트를 실행합니다.</p>

## NSX 에이전트 자동 설치

현재 Microsoft Azure에 대해서만 지원됩니다.

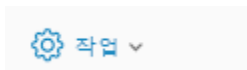
Microsoft Azure에서 다음 기준이 충족되는 경우 NSX 에이전트가 자동으로 설치됩니다.

- VNet의 VM에 설치된 Azure VM 확장이 NSX Cloud에 추가되었습니다. 자세한 내용은 [VM 확장에 대한 Microsoft Azure 설명서](#)를 참조하십시오.
- VM에 nsx.network 및 값 default를 사용하여 태그가 지정되었습니다.

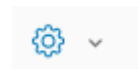
이 기능을 사용하도록 설정하려면 다음과 같이 하십시오.

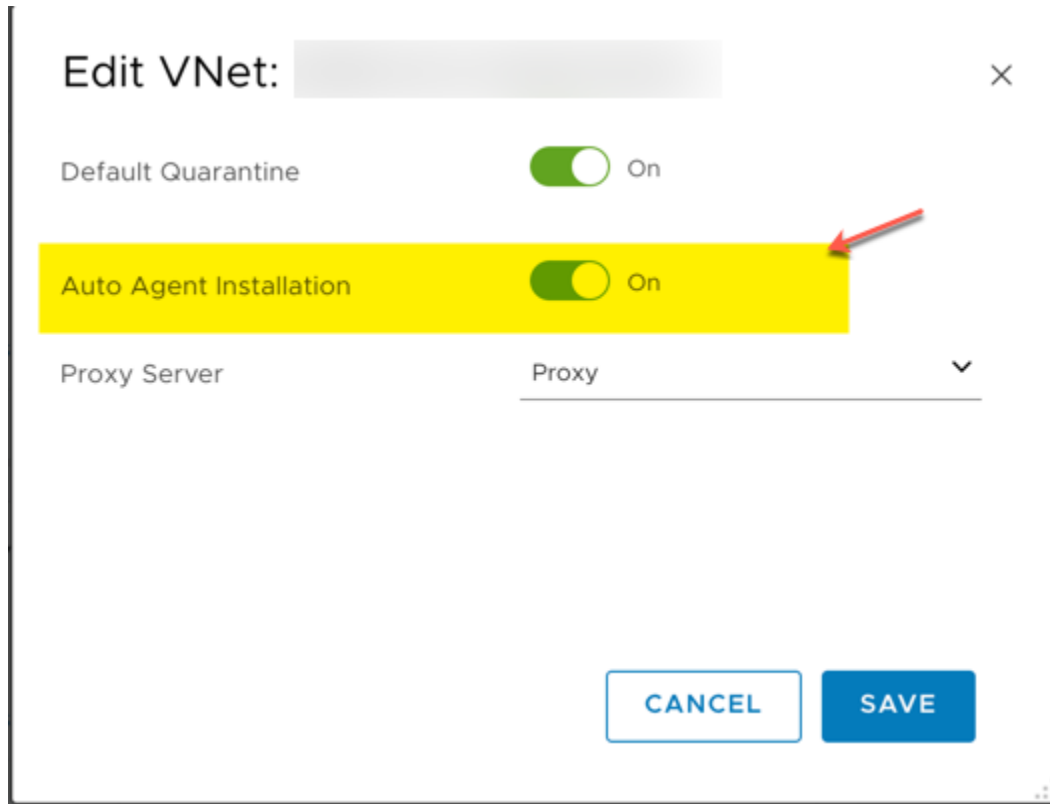
- 1 **클라우드 > Azure > VNet**으로 이동합니다.
- 2 NSX 에이전트를 자동 설치할 VM의 VNet을 선택합니다.
- 3 다음 중 하나를 사용하여 옵션을 사용하도록 설정합니다.

- 타일 보기에서 **작업 > 구성 편집**을 클릭합니다.
- 그리드 보기에 있는 경우 VNet 옆의 확인란을 선택하고 **작업 > 구성 편집**을 클릭합니다.



- VNet의 페이지에 있는 경우 작업 아이콘을 클릭하여 **구성 편집**으로 이동합니다.





## 워크로드 VM 관리

워크로드 VM을 성공적으로 등록한 후 NSX-T Data Center를 사용하여 관리할 수 있습니다.

### 관리 워크로드 VM 액세스

이 워크플로에 따라 언더레이 모드에서 관리 VM에 액세스합니다.

VPC 또는 VNet에서 PCG를 배포할 때 NSX Cloud는 워크로드 VM의 보안을 강화하기 위한 기본 방화벽 규칙을 생성합니다.

언더레이 모드에서 관리 워크로드 VM에 액세스하려면 VM에 대한 액세스를 여는 DFW(분산 방화벽) 규칙을 추가해야 합니다.

다음을 수행합니다.

- 1 NSX Manager 콘솔을 엽니다.
- 2 **방화벽 > 일반 > 규칙 추가**로 이동합니다.

3 다음 구성으로 규칙을 추가합니다. 자세한 지침은 [방화벽 규칙 추가](#) 항목을 참조하십시오.

표 16-7.

옵션	설명
이름	규칙의 용도를 정의하는 이름(예: <code>AllowRemoteAccessToUnderlay</code> )을 제공합니다.
소스	임의를 선택합니다.
대상	VM이 연결되거나 소속되어 있는 논리적 스위치 또는 포트 또는 NSGroup을 선택합니다.
서비스	워크로드 VM에 대한 원격 액세스 서비스(예: Linux의 경우 SSH, Windows의 경우 RDP)를 선택합니다.
작업	허용을 선택합니다.

## NSX-T Data Center 및 공용 클라우드 태그를 사용하여 VM 그룹화

NSX Cloud를 사용하면 워크로드 VM에 할당된 공용 클라우드 태그를 사용할 수 있습니다.

공용 클라우드와 마찬가지로 NSX Manager는 태그를 사용하여 VM을 그룹화합니다. 따라서 NSX Cloud는 쉽게 VM을 그룹화할 수 있도록 미리 정의된 크기와 예약어 조건을 충족하는 경우 워크로드 VM에 적용된 공용 클라우드 태그를 NSX Manager로 가져옵니다.

### 태그 용어

NSX Manager에서 **태그**란 공용 클라우드 컨텍스트에서 값으로 알려진 것을 말합니다. 공용 클라우드 태그의 **키**는 NSX Manager에서 **범위**라고 합니다.

태그 구성 요소 위치: NSX Manager	공용 클라우드의 태그에 해당하는 구성 요소
범위	키
태그	값

### 태그 유형 및 제한 사항

NSX Cloud는 NSX 관리 공용 클라우드 VM에 대해 세 가지 유형의 태그를 허용합니다.

- **시스템 태그:** 이러한 태그는 시스템 정의 항목이며 추가, 편집 또는 삭제할 수 없습니다. NSX Cloud는 다음과 같은 시스템 태그를 사용합니다.
  - azure:subscription\_id
  - azure:region
  - azure:vm\_rg
  - azure:vnet\_name
  - azure:vnet\_rg
  - aws:vpc

- aws:availabilityzone

- **검색된 태그:** 공용 클라우드의 VM에 추가한 태그는 NSX Cloud에서 자동으로 검색되고 NSX Manager 인벤토리의 워크로드 VM에 대해 표시됩니다. 이러한 태그는 NSX Manager 내에서 편집할 수 없습니다. 검색된 태그의 수에는 제한이 없습니다. 이러한 태그 앞에는 Microsoft Azure에서 검색되었음을 나타내기 위해 접두사 **dis:azure:**가 붙습니다.

공용 클라우드의 태그를 변경하면 변경 내용이 2분 내에 NSX Manager에 반영됩니다.

기본적으로 이 기능은 사용하도록 설정되어 있습니다. Microsoft Azure 구독 또는 AWS 계정을 추가할 때 Microsoft Azure 또는 AWS 태그의 검색을 사용 또는 사용하지 않도록 설정할 수 있습니다.

- **사용자 태그:** 사용자 태그는 최대 25개까지 생성할 수 있습니다. 사용자 태그에 대한 추가, 편집, 삭제 권한이 있습니다. 사용자 태그 관리에 대한 자세한 내용은 [VM용 태그 관리](#)의 내용을 참조하십시오.

표 16-8. 태그 유형 및 제한 사항 요약

태그 유형	태그 범위 또는 미리 결정된 접두사	제한 사항	엔터프라이즈 관리자 권한	감사자 권한
시스템 정의	전체 시스템 태그: <ul style="list-style-type: none"> <li>■ azure:subscription_id</li> <li>■ azure:region</li> <li>■ azure:vm_rg</li> <li>■ azure:vnet_name</li> <li>■ azure:vnet_rg</li> <li>■ aws:vpc</li> <li>■ aws:availabilityzone</li> </ul>	범위(키): 20자 태그(값): 65자 최대 허용: 5	읽기 전용	읽기 전용
검색됨	VNet에서 가져온 Microsoft Azure 태그에 대한 접두사: <b>dis:azure:</b> VPC에서 가져온 AWS 태그에 대한 접두사: <b>dis:aws:</b>	범위(키): 20자 태그(값): 65자 최대 허용: 무제한  <a href="#">참고</a> 문자에 대한 제한에서 접두사 <b>dis:&lt;공용 클라우드 이름&gt;</b> 은 제외됩니다. 이러한 제한을 초과하는 태그는 NSX Manager에 반영되지 않습니다.  접두사 <b>nsx</b> 가 있는 태그는 무시됩니다.	읽기 전용	읽기 전용
사용자	사용자 태그에는 허용된 문자 수 내에서 원하는 범위(키) 및 값을 사용할 수 있습니다. 단, 다음 항목은 제외됩니다. <ul style="list-style-type: none"> <li>■ 범위(키) 접두사 <b>dis:azure:</b> 또는 <b>dis:aws:</b></li> <li>■ 시스템 태그와 동일한 범위(키)</li> </ul>	범위(키): 30자 태그(값): 65자 최대 허용: 25	추가/편집/삭제	읽기 전용

## 검색된 태그의 예

**참고** 태그는 공용 클라우드의 경우 **키=값** 형식이고 NSX Manager의 경우 **범위=태그** 형식입니다.



표 16-9.

워크로드 VM에 대한 공용 클라우드 태그	NSX Cloud에서 검색되었습니까?	워크로드 VM에 해당하는 NSX Manager 태그
Name = Developer	예	dis:azure:Name = Developer
ValidDisTagKeyLength = ValidDisTagValue	예	dis:azure:ValidDisTagKeyLength = ValidDisTagValue
Abcdefghijklmnopqrstuvwxyz = value 2	아니요 (키가 20자를 초과함)	없음
tag3 = Abcdefghijklmnopqrstuvwxyz Ab23690hgjguytreswqacvbcdefghij klmnopqrstuvwxyz	아니요 (값이 65자를 초과함)	없음
nsx.name = Tester	아니요 (키에 접두사 <b>nsx</b> 가 있음)	없음

## NSX Manager에서 태그를 사용하는 방법

- [VM용 태그 관리](#)의 내용을 참조하십시오.
- [개체 검색](#)의 내용을 참조하십시오.
- [워크로드 VM에 대한 마이크로 세분화 설정](#)의 내용을 참조하십시오.

## 워크로드 VM에 대한 마이크로 세분화 설정

관리 워크로드 VM에 대한 마이크로 세분화를 설정할 수 있습니다.

온보드된 워크로드 VM에 분산 방화벽 규칙을 적용하려면 다음을 수행합니다.

- 1 VM 이름이나 태그 또는 다른 멤버 자격 조건(예: **웹**, **앱**, **DB** 계층)을 사용하여 NSGroup을 생성합니다. 자세한 내용은 [NSGroup 생성](#) 항목을 참조하십시오.

**참고** 멤버 자격 조건에 다음 태그 중 원하는 태그를 사용할 수 있습니다. 자세한 내용은 [NSX-T Data Center 및 공용 클라우드 태그를 사용하여 VM 그룹화](#) 항목을 참조하십시오.

- 시스템 정의 태그
- NSX Cloud에서 검색된 VPC 또는 VNet의 태그
- 또는 자신의 사용자 지정 태그

- 2 필요한 경우 방화벽 규칙 섹션을 생성하고 NSGroup에 적용합니다. [방화벽 규칙 섹션 추가](#)의 내용을 참조하십시오.
- 3 보안 정책에 따라 방화벽 규칙을 생성하고 소스 및 대상에 NSGroup을 사용합니다. [방화벽 규칙 추가](#)의 내용을 참조하십시오.

이 마이크로 세분화는 인벤토리가 CSM에서 수동으로 다시 동기화되거나 공용 클라우드에서 CSM으로 변경 사항을 가져올 때 약 2분 이내에 적용됩니다.

## 공용 클라우드에 대해 NSX-T Data Center 기능을 사용하는 방법

NSX Cloud는 공용 클라우드의 네트워크 토폴로지를 생성하므로 자동 생성된 NSX-T Data Center 논리적 엔티티를 편집하거나 삭제해서는 안 됩니다.

이 목록을 자동 생성되는 항목과 공용 클라우드에 적용할 때 NSX-T Data Center 기능을 사용하는 방법에 대한 빠른 참조로 사용하십시오.

### NSX Manager 구성

다음 엔티티는 NSX Manager에서 자동으로 생성됩니다.

---

**중요** 이러한 자동 생성된 엔티티를 편집하거나 삭제하지 마십시오.

---

- PCG(**공용 클라우드 게이트웨이**)라는 Edge 노드가 생성됩니다.
- PCG가 Edge 클러스터에 추가됩니다. 고가용성 배포에서는 2개의 PCG가 있습니다.
- PCGPCG는 2개의 전송 영역이 생성된 전송 노드로 등록됩니다.
- 두 개의 기본 논리적 스위치가 생성됩니다.
- Tier-0 논리적 라우터가 하나 생성됩니다.
- IP 검색 프로파일이 생성됩니다. 이것은 오버레이 논리적 스위치에 사용됩니다.
- DHCP 프로파일이 생성됩니다. 이것은 DHCP 서버에 사용됩니다.

---

**참고** DHCP 프로파일이 생성되기는 하지만 오버레이 네트워킹에 사용되므로 현재 릴리스에서는 지원되지 않습니다.

---

- 이름이 **PublicCloudSecurityGroup**인 기본 NSGroup이 생성되며 다음과 같은 멤버가 포함됩니다.
  - 기본 VLAN 논리적 스위치
  - HA를 사용하도록 설정한 경우 논리적 포트, PCG 업링크 포트마다 각각 하나씩
  - IP 주소
- 세 가지 기본 분산 방화벽 규칙이 생성됩니다.
  - LogicalSwitchToLogicalSwitch
  - LogicalSwitchToAnywhere
  - AnywhereToLogicalSwitch

---

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

---

NSX Manager에서 다음 구성을 확인하십시오.

- 1 NSX Cloud 대시보드에서 **NSX Manager**를 클릭합니다.

- 2 **패브릭 > 노드 > Edge**로 이동합니다. Edge 노드로 **PCG-<your-VPC-or-VNet-name>**이 표시되어야 합니다.

**참고** 배포 상태, 관리자 연결 및 컨트롤러 연결이 연결되어 있는지 확인합니다(상태가 녹색점이 있는 **실행**을 표시함).

- 3 **패브릭 > 노드 > Edge 클러스터**로 이동하여 **PCG-Cluster-<your-VPC-or-VNet-name>**이 추가되었는지 확인합니다.
- 4 **패브릭 > 노드 > 전송 노드**로 이동하고 PCG가 전송 노드로 등록되었는지 그리고 PCG를 배포하는 동안 자동 생성된 2개의 전송 영역에 연결되었는지 확인합니다.
- VLAN 트래픽 유형 -- 이것은 PCG 업링크에 연결됩니다.
  - 오버레이 트래픽 유형 -- 이것은 오버레이 논리적 네트워킹을 위한 것입니다.

**참고** 오버레이는 현재 릴리스에서 지원되지 않습니다.

- 5 논리적 스위치와 Tier-0 논리적 라우터가 생성되었고 논리적 라우터가 Edge 클러스터에 추가되었는지 확인합니다.
- **네트워킹 > 스위칭 > 스위치**로 이동합니다. 자동 생성된 **DefaultSwitch-Overlay-<your-VPC-or-VNet-name>** 및 **DefaultSwitch-VLAN-<your-VPC-or-VNet-name>** 스위치가 표시되어야 합니다.
  - **네트워킹 > 라우팅 > 라우터**로 이동합니다. 자동 생성된 **PCG-Tier0-LR-<your-VPC-or-VNet-name>** 라우터가 표시되어야 합니다.

## 논리적 스위칭 FAQ

표 16-10.

질문	응답
PCG가 배포될 때 NSX Cloud에서 기본 스위치를 생성합니까?	예. NSX Cloud는 PCG를 배포하는 각 VPC 또는 VNet에 대해 2개의 기본 스위치를 생성합니다. 해당 스위치는 다음과 같이 명명됩니다.  <b>DefaultSwitch-Overlay-&lt;vpc-or-vnet-name&gt;</b> <b>DefaultSwitch-VLAN-&lt;vpc-or-vnet-name&gt;</b>
NSX Cloud에서 생성된 기본 논리적 스위치 외에도 VLAN 논리적 스위치를 생성할 수 있습니까?	아니요. VLAN 논리적 스위치를 생성하면 안 됩니다.
NSX Cloud에서 생성된 기본 논리적 스위치를 편집하거나 삭제할 수 있습니까?	UI를 사용하여 기본 논리적 엔티티를 편집하거나 삭제할 수 있지만 NSX Cloud에서 자동 생성된 엔티티를 편집하거나 삭제하면 안 됩니다.
포트를 생성해야 합니까?	아니요. 포트를 생성하지 않아도 됩니다. NSX Cloud는 AWS 또는 Microsoft Azure의 VM에 태그를 지정할 때 포트를 생성합니다. NSX Cloud에서 자동 생성된 포트를 편집하거나 삭제하면 안 됩니다.

## 표 16-10. (계속)

질문	응답
스위칭 프로파일을 생성해야 하나요?	아니요. 스위칭 프로파일을 생성하지 않아도 됩니다. <b>PublicCloud-Global-SpoofGuardProfile</b> 을 사용합니다. 기본 스위칭 프로파일을 편집하거나 삭제하면 안 됩니다.
어디에서 논리적 스위치에 대한 세부 정보를 찾을 수 있습니까?	<a href="#">장 1 논리적 스위치 및 VM 연결 구성</a> 의 내용을 참조하십시오.

## 논리적 라우터 FAQ

## 표 16-11.

질문	응답
PCG가 배포될 때 NSX Cloud에서 논리적 라우터가 자동 생성됩니까?	예. PCG가 VPC 또는 VNet에서 배포될 때 NSX Cloud에서 Tier-0 논리적 라우터가 자동 생성됩니다.
어디에서 논리적 라우터에 대한 자세한 정보를 찾을 수 있습니까?	<a href="#">장 5 Tier-0 논리적 라우터</a> 의 내용을 참조하십시오.

## IPFIX FAQ

## 표 16-12.

질문	응답
IPFIX가 공용 클라우드에서 작동하기 위해 필요한 특정 구성이 있습니까?	예. <ul style="list-style-type: none"> <li>■ IPFIX는 NSX Cloud의 UDP 포트 4739에서만 지원됩니다.</li> <li>■ 수집기는 IPFIX 프로파일이 적용된 VM과 동일한 VPC 또는 VNet에 있어야 합니다.</li> <li>■ <b>스위치 및 DFW IPFIX</b>: 수집기가 IPFIX 프로파일이 적용된 Windows VM과 동일한 서브넷에 있는 경우 ARP 항목을 찾을 수 없을 때 Windows가 자동으로 UDP 패킷을 삭제하기 때문에 Windows VM에 해당 수집기에 대한 정적 ARP 항목이 필요합니다.</li> </ul>
어디에서 IPFIX에 대한 자세한 정보를 찾을 수 있습니까?	<a href="#">IPFIX 구성</a> 의 내용을 참조하십시오.

## 포트 미러링 FAQ

## 표 16-13.

질문	응답
공용 클라우드의 포트 미러링에 필요한 특정 구성이 있습니까?	포트 미러링은 현재 릴리스의 AWS에서만 지원됩니다. <ul style="list-style-type: none"> <li>■ NSX Cloud의 경우, <b>도구 &gt; 포트 미러링 세션</b>에서 포트 미러링을 구성합니다.</li> <li>■ L3SPAN 포트 미러링만 지원됩니다.</li> <li>■ 수집기가 소스 워크로드 VM과 동일한 VPC에 있어야 합니다.</li> </ul>
어디에서 포트 미러링에 대한 자세한 정보를 찾을 수 있습니까?	<a href="#">포트 미러링 세션 모니터링</a> 의 내용을 참조하십시오.

## 기타 FAQ

표 16-14.

질문	응답
공용 클라우드의 워크로드 VM에 적용하는 태그를 NSX-T Data Center에서 사용할 수 있습니까?	예. 자세한 내용은 <a href="#">NSX-T Data Center 및 공용 클라우드 태그를 사용하여 VM 그룹화</a> 항목을 참조하십시오.
NSX-T Data Center에서 관리하는 워크로드 VM에 대해 마이크로 세분화를 설정하려면 어떻게 해야 하나요?	<a href="#">워크로드 VM에 대한 마이크로 세분화 설정</a> 의 내용을 참조하십시오.

## 고급 NSX Cloud 기능 사용

### Syslog 전달 사용

NSX Cloud는 syslog 전달을 지원합니다.

관리 VM에서 DFW(분산 방화벽) 패킷에 대한 Syslog 전달을 사용하도록 설정할 수 있습니다. 자세한 내용은 "NSX-T Data Center 문제 해결 가이드"의 [원격 로깅 구성](#)을 참조하십시오.

다음은 수행합니다.

#### 절차

- 1 점프 호스트를 사용하여 PCG에 로그인합니다.
- 2 `nsxcli`를 입력하여 NSX-T Data Center CLI를 엽니다.
- 3 다음 명령을 입력하여 DFW 로그 전달을 사용하도록 설정합니다.

```
nsx-public-cloud-gateway> set gw-controller vm-log-forwarding enabled
nsx-public-cloud-gateway> set logging-server <서버-IP-주소> proto udp level info messageid FIREWALL-PKTLOG
```

이 설정이 완료되면 PCG의 `/var/log/syslog`에서 NSX 에이전트 DFW 패킷 로그를 사용할 수 있습니다.

- 4 VM마다 로그 전달을 사용하도록 설정하려면 다음 명령을 입력합니다.

```
nsx-public-cloud-gateway> set gw-controller vm-log-forwarding enabled <vm-id>
```

## 문제 해결

NSX Cloud에서 사용 가능한 검증 및 문제 해결 옵션을 이해합니다.

### NSX Cloud 구성 요소 확인

운영 환경에 배포하기 전에 모든 구성 요소가 실행되고 있는지 확인하는 것이 좋습니다.

## NSX 에이전트가 PCG에 연결되어 있는지 확인

워크로드 VM의 NSX 에이전트가 PCG에 연결되어 있는지 확인하려면 다음을 수행합니다.

- 1 `nsxcli` 명령을 입력하여 NSX-T Data Center CLI를 엽니다.
- 2 다음 명령을 입력하여 게이트웨이 연결 상태를 가져옵니다. 예를 들면 다음과 같습니다.

```
get gateway connection status
Public Cloud Gateway : nsx-gw.vmware.com:5555 Connection Status : ESTABLISHED
```

## VM의 인터페이스/네트워크 모드 확인

NSX 에이전트가 설치되어 있는 인터페이스를 다음과 같이 확인합니다.

- 1 `nsxcli` 명령을 입력하여 NSX-T Data Center CLI를 엽니다.
- 2 다음 명령을 입력하여 전환 모드를 확인합니다. 예를 들면 다음과 같습니다.

```
get vm-network-mode
VM-Network-Mode : underlay Interface : eth0
```

## AWS 또는 Microsoft Azure에서 VM 인터페이스 태그 확인

워크로드 VM에 올바른 태그가 있어야 PCG에 연결할 수 있습니다.

- 1 AWS 콘솔 또는 Microsoft Azure 포털에 로그인합니다.
- 2 VM의 eth0 또는 인터페이스 태그를 확인합니다.

`nsx.network` 키의 값은 `default`여야 합니다.

## 문제 해결 FAQ

여기에는 몇 가지 질문과 대답이 있습니다.

VM에 태그를 올바르게 지정하고 에이전트를 설치했지만 VM이 격리되었습니다. 어떻게 해야 하나요?

이 문제가 발생하면 다음을 시도해 보십시오.

- NSX Cloud 태그 `nsx.managed` 및 해당 값 `default`를 올바르게 입력했는지 확인합니다. 이것은 대/소문자를 구분합니다.
- CSM에서 AWS 또는 Microsoft Azure 계정을 다시 동기화합니다.
  - CSM에 로그인합니다.
  - **클라우드 > AWS/Azure > 계정**으로 이동합니다.
  - 공용 클라우드 계정 타일에서 **작업**을 클릭하고 **계정 다시 동기화**를 클릭합니다.

## 워크로드 VM에 액세스할 수 없는 경우 어떻게 해야 하나요?

특정 조건에서 드물게 관리 Linux 또는 Windows 워크로드 VM에 대한 연결이 끊어질 수 있습니다. 다음 단계를 시도합니다.

### 공용 클라우드에서(AWS 또는 Microsoft Azure)

- NSX Cloud에서 관리되는 포트를 포함한 VM의 모든 포트, OS 방화벽(Microsoft Windows 또는 IPTables) 및 NSX-T Data Center가 트래픽을 허용하도록 올바르게 구성되었는지 확인합니다. 예를 들어 VM에 대한 ping을 허용하려면 다음을 올바르게 구성해야 합니다.
  - AWS 또는 Microsoft Azure의 보안 그룹. 자세한 내용은 [격리 정책 관리](#) 항목을 참조하십시오.
  - NSX-T Data Center DFW 규칙. 자세한 내용은 [관리 워크로드 VM 액세스](#) 항목을 참조하십시오.
  - Windows Firewall 또는 Linux의 IPTables
- SSH 또는 다른 방법(예: Microsoft Azure의 직렬 콘솔)을 사용하여 VM에 로그인하고 문제에 대한 해결을 시도합니다.
- 잠겨 있는 VM을 재부팅할 수 있습니다.
- 그래도 VM에 액세스할 수 없으면 보조 NIC를 워크로드 VM에 연결하여 이 NIC에서 해당 워크로드 VM에 액세스합니다.

# 작업 및 관리

# 17

라이선스 및 인증서 추가와 암호 변경과 같이 설치한 장치의 구성을 변경해야 할 수 있습니다. 또한 백업 실행을 비롯하여 수행해야 하는 일상적인 유지 보수 작업도 있습니다. 그뿐 아니라 원격 시스템 로그인, Traceflow 및 포트 연결을 비롯하여 NSX-T Data Center에서 생성되는 NSX-T Data Center 인프라 및 논리적 네트워크에 속하는 장치에 대한 정보를 찾는 데 도움이 되는 도구도 있습니다.

본 장은 다음 항목을 포함합니다.

- 라이선스 키 추가
- 사용자 계정 및 역할 기반 액세스 제어 관리
- 인증서 설정
- 장치 구성
- 계산 관리자 추가
- 태그 관리
- 개체 검색
- 원격 서버의 SSH 지문 찾기
- NSX Manager 백업 및 복원
- 장치 및 장치 클러스터 관리
- 로그 메시지
- IPFIX 구성
- Traceflow를 사용하여 패킷의 경로 추적
- 포트 연결 정보 보기
- 논리적 스위치 포트 활동 모니터링
- 포트 미러링 세션 모니터링
- 패브릭 노드 모니터링
- VM에서 실행되는 애플리케이션에 대한 데이터 보기
- 지원 번들 수집



## ■ 고객 환경 향상 프로그램

# 라이선스 키 추가

NSX Manager UI를 사용하여 하나 이상의 라이선스 키를 추가할 수 있습니다.

다음의 비평가판 라이선스 유형을 사용할 수 있습니다.

- 표준
- 고급
- 엔터프라이즈

NSX Manager를 설치하면 미리 설치한 평가판 라이선스가 활성화되고 60일 동안 유효합니다. 평가판 라이선스는 엔터프라이즈 라이선스의 모든 기능을 제공합니다. 평가판 라이선스는 설치하거나 할당 취소할 수 없습니다.

하나 이상의 비평가판 라이선스를 설치할 수 있지만 각 유형에 대해 하나의 키만 설치할 수 있습니다. 표준, 고급 또는 엔터프라이즈 라이선스를 설치할 때 평가판 라이선스는 더 이상 사용할 수 없습니다. 비평가판 라이선스를 할당 취소할 수도 있습니다. 모든 비평가판 라이선스를 할당 취소하면 평가판 라이선스가 복원됩니다.

동일한 라이선스 유형의 키가 여러 개 있고 키를 조합하려면 <https://my.vmware.com>으로 이동한 후 키 조합 기능을 사용해야 합니다. NSX Manager UI는 이 기능을 제공하지 않습니다.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 구성 > 라이선스**를 선택합니다.
- 3 **추가**를 클릭하여 라이선스 키를 입력합니다.
- 4 **저장**을 클릭합니다.

# 사용자 계정 및 역할 기반 액세스 제어 관리

NSX-T Data Center 장치에는 admin 및 audit이라는 두 가지 기본 제공 사용자가 있습니다. NSX-T Data Center를 VMware Identity Manager(vIDM)와 통합하고 vIDM이 관리하는 사용자에게 대해 RBAC(역할 기반 액세스 제어)를 구성할 수 있습니다.

vIDM이 관리하는 사용자에게는 admin 사용자와 audit 사용자에게만 적용되는 NSX-T Data Center의 인증 정책이 아니라 vIDM 관리자가 구성한 인증 정책이 적용됩니다.

## CLI 사용자 암호 변경

각 장치에는 로그인하고 CLI 명령을 실행하는 데 사용할 수 있는 admin 및 audit이라는 두 가지 기본 제공 사용자가 있습니다. 이러한 사용자의 암호는 변경할 수 있지만 사용자를 추가하거나 삭제할 수는 없습니다.

## 절차

- 1 장치의 CLI에 로그인합니다.
- 2 `set user` 명령을 실행합니다. 예를 들면 다음과 같습니다.

```
nsx> set user admin
Current password:
New password:
Confirm new password:
nsx>
```

암호는 다음과 같은 복잡성 요구 사항을 충족해야 합니다.

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

## 인증 정책 설정

CLI를 통해 인증 정책 설정을 보거나 변경할 수 있습니다.

다음 명령을 사용하여 최소 암호 길이를 보거나 설정할 수 있습니다.

```
get auth-policy minimum-password-length
set auth-policy minimum-password-length <password-length>
```

다음 명령은 NSX Manager UI로의 로그인 또는 API 호출에 적용됩니다.

```
get auth-policy api lockout-period
get auth-policy api lockout-reset-period
get auth-policy api max-auth-failures
set auth-policy api lockout-period <lockout-period>
set auth-policy api lockout-reset-period <lockout-reset-period>
set auth-policy api max-auth-failures <auth-failures>
```

다음 명령은 NSX Manager, NSX Controller 또는 NSX Edge 노드에서 CLI로의 로그인에 적용됩니다.

```
get auth-policy cli lockout-period
get auth-policy cli max-auth-failures
set auth-policy cli lockout-period <lockout-period>
set auth-policy cli max-auth-failures <auth-failures>
```

CLI 명령에 대한 자세한 내용은 “NSX-T 명령줄 인터페이스 참조”를 참조하십시오.

기본적으로 NSX Manager UI에 대한 로그인 시도가 연속해서 5회 실패하면 관리자 계정이 15분 동안 잠깁니다. 다음 명령을 사용하여 계정 잠금을 사용하지 않도록 설정할 수 있습니다.

```
set auth-policy api lockout-period 0
```

마찬가지로 다음 명령을 사용하여 CLI에 대한 계정 잠금을 사용하지 않도록 설정할 수 있습니다.

```
set auth-policy cli lockout-period 0
```

## vIDM 호스트에서 인증서 지문 가져오기

vIDM과 NSX-T의 통합을 구성하기 전에 vIDM 호스트에서 인증서 지문을 가져와야 합니다.

### 절차

- 1 vIDM 호스트에 대해 SSH를 수행하고 **sshuser** 권한으로 로그인합니다.
- 2 다음 명령을 실행하여 **root** 사용자가 됩니다.

```
su root
```

- 3 /etc/ssh/sshd\_config 파일을 편집하고 PermitRootLogin 값을 yes로, StrictModes 값을 no로 변경합니다.

```
PermitRootLogin yes
StrictModes no
```

- 4 다음 명령을 실행하여 sshd 서비스를 다시 시작합니다.

```
service sshd restart
```

- 5 로그아웃한 후 **root** 권한으로 로그인합니다.
- 6 다음 명령을 실행하여 디렉토리를 변경합니다.

```
cd /usr/local/horizon/conf
```

- 7 다음 명령을 실행하여 지문을 가져옵니다.

```
openssl s_client -connect <FQDN of vIDM host>:443 < /dev/null 2>/dev/null | openssl x509 -sha256 -
fingerprint -noout -in /dev/stdin
```

예:

```
openssl s_client -connect vidm.corp.local:443 < /dev/null 2>/dev/null | openssl x509 -sha256 -
fingerprint -noout -in /dev/stdin
```

## vIDM 호스트를 NSX-T에 연결

NSX-T와 vIDM을 통합하려면 vIDM 호스트에 대한 정보를 제공해야 합니다.

CA(인증 기관)에서 서명한 인증서가 vIDM 서버에 있어야 합니다. 그렇지 않으면 NSX Manager에서 vIDM에 로그인하는 것이 Microsoft Edge나 Internet Explorer 11과 같은 특정 브라우저에서 작동하지 않을 수 있습니다. vIDM에 CA 서명된 인증서 설치에 대한 자세한 내용은 <https://docs.vmware.com/kr/VMware-Identity-Manager/3.1/vidm-install/GUID-B76761BF-4B12-4CD5-9366-B0A1A2BF2A8B.html> 항목을 참조하십시오.

vIDM에 NSX Manager를 등록할 때 NSX Manager를 가리키는 리디렉션 URI를 지정합니다. FQDN(정규화된 도메인 이름) 또는 IP 주소를 제공할 수 있습니다. FQDN 또는 IP 주소를 사용하는지 여부를 기억하는 것이 중요합니다. vIDM을 통해 NSX Manager에 로그인하려고 하는 경우 동일한 방식으로 URL에서 호스트 이름을 지정해야 합니다. 즉, vIDM에 관리자를 등록할 때 FQDN을 사용하는 경우 URL에서 해당 FQDN을 사용해야 하며, vIDM에 관리자를 등록할 때 IP 주소를 사용하는 경우 URL에서 해당 IP 주소를 사용해야 합니다. 그렇지 않으면 로그인이 실패합니다.

### 사전 요구 사항

- vIDM 호스트의 인증서 지문이 있는지 확인합니다. [vIDM 호스트에서 인증서 지문 가져오기](#)의 내용을 참조하십시오.
- NSX Manager가 vIDM 호스트에 대한 OAuth 클라이언트로 등록되어 있는지 확인합니다. 등록 프로세스 중에 클라이언트 ID와 클라이언트 암호를 적어두십시오. 자세한 내용은 <https://www.vmware.com/support/pubs/identitymanager-pubs.html>에서 VMware Identity Manager 설명서를 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 사용자**를 선택합니다.
- 3 **구성** 탭을 클릭합니다.
- 4 **편집**을 클릭합니다.
- 5 다음 정보를 제공합니다.

매개 변수	설명
<b>VMware Identity Manager 장치</b>	vIDM 호스트의 FQDN(정규화된 도메인 이름)입니다.
<b>클라이언트 ID</b>	NSX Manager를 vIDM 호스트에 등록할 때 생성되는 ID입니다.
<b>클라이언트 암호</b>	NSX Manager를 vIDM 호스트에 등록할 때 생성되는 암호입니다.
<b>지문</b>	vIDM 호스트의 인증서 지문입니다.
<b>NSX 장치</b>	NSX Manager의 IP 주소 또는 FQDN(정규화된 도메인 이름)입니다. FQDN을 지정하는 경우에는 URL에 관리자의 FQDN을 사용하여 브라우저에서 NSX Manager에 액세스해야 하고, IP 주소를 지정하는 경우에는 URL에 IP 주소를 사용해야 합니다. 또는 FQDN 또는 IP 주소를 사용하여 연결할 수 있도록 vIDM 관리자가 NSX Manager 클라이언트를 구성할 수 있습니다.

- 6 **저장**을 클릭합니다.

## NSX Manager, vIDM 및 관련 구성 요소 간의 시간 동기화

인증이 올바르게 작동하려면 NSX Manager, vIDM 및 Active Directory 같은 다른 서비스 제공자의 시간을 모두 동기화해야 합니다. 이 섹션에서는 이러한 구성 요소의 시간을 동기화하는 방법을 설명합니다.

### VMware Infrastructure

ESXi 호스트를 동기화하려면 다음 KB 문서에 나와 있는 지침을 따릅니다.

- <https://kb.vmware.com/kb/1003736>
- <https://kb.vmware.com/kb/2012069>

VM 및 호스트 동기화에 대한 자세한 내용은 [https://docs.vmware.com/kr/VMware-vSphere/6.0/com.vmware.vsphere.vm\\_admin.doc/GUID-C0D8326A-B6E7-4E61-8470-6C173FDDF656.html](https://docs.vmware.com/kr/VMware-vSphere/6.0/com.vmware.vsphere.vm_admin.doc/GUID-C0D8326A-B6E7-4E61-8470-6C173FDDF656.html) 페이지를 참조하십시오. VM이 NSX Manager, vIDM, Active Directory 또는 다른 서비스 제공자를 실행 중일 수 있습니다.

### 타사 인프라

VM 및 호스트를 동기화하는 방법은 벤더의 설명서를 따르십시오.

### vIDM 서버에 NTP 구성(권장되지 않음)

호스트 간에 시간을 동기화할 수 없는 경우에는 호스트에 동기화하지 않도록 설정하고 vIDM 서버에 NTP를 구성할 수 있습니다. 그러기 위해서는 vIDM 서버에서 UDP 포트 123을 열어야 하기 때문에 이 방법은 권장되지 않습니다.

- vIDM 서버의 클럭이 올바른지 확인합니다.

```
# hwclock
Tue May 9 12:08:43 2017 -0.739213 seconds
```

- 아직 없는 경우, /etc/ntp.conf를 편집하여 다음 항목을 추가합니다.

```
server server time.nist.gov
server server pool.ntp.org
server server time.is dynamic
```

- UDP 포트 123을 엽니다.

```
# iptables -A INPUT -p udp --dport 123 -j ACCEPT
```

다음 명령을 실행하여 포트가 열려 있는지 확인합니다.

```
# iptables -L -n
```

- NTP 서비스를 시작합니다.

```
/etc/init.d/ntp start
```

- 재부팅 후 NTP가 자동으로 실행되도록 구성합니다.

```
# chkconfig --add ntp
# chkconfig ntp on
```

- NTP 서버에 연결할 수 있는지 확인합니다.

```
# ntpq -p
```

reach 열에 0이 표시되면 안 됩니다. st 열에 16 이외의 숫자가 표시되어야 합니다.

## 역할 기반 액세스 제어

RBAC(역할 기반 액세스 제어)를 사용하면 시스템 액세스를 허가된 사용자로 제한할 수 있습니다. 사용자에게는 역할이 할당되고 각 역할은 특정 사용 권한을 가집니다.

사용 권한 유형은 다음 네 가지로 구분됩니다.

- 전체 액세스 권한
- 실행
- 읽기
- 없음

전체 액세스 권한은 사용자에게 모든 사용 권한을 부여합니다. 실행 사용 권한에는 읽기 권한이 포함됩니다.

NSX-T Data Center에는 다음과 같은 기본 제공 역할이 있습니다. 새 역할을 추가할 수는 없습니다.

- 엔터프라이즈 관리자
- 감사자
- 네트워크 엔지니어
- 네트워크 작업
- 보안 엔지니어
- 보안 작업
- 클라우드 서비스 관리자
- 클라우드 서비스 감사자
- 로드 밸런서 관리자
- 로드 밸런서 감사자

AD(Active Directory) 사용자에게 역할이 할당된 후 AD 서버에서 사용자 이름이 변경되면 새 사용자 이름을 사용하여 역할을 다시 할당해야 합니다.

## 역할 및 사용 권한

표 17-1. 역할 및 사용 권한에서는 각 역할이 여러 작업에 대해 갖는 사용 권한을 보여 줍니다. 다음과 같은 약어가 사용됩니다.

- EA - 엔터프라이즈 관리자
- A - 감사자
- NE - 네트워크 엔지니어
- NO - 네트워크 작업
- SE - 보안 엔지니어
- SO - 보안 작업
- CS Adm - 클라우드 서비스 관리자
- CS Aud - 클라우드 서비스 감사자
- LB Adm - 로드 밸런서 관리자
- LB Aud - 로드 밸런서 감사자
- FA - 전체 액세스 권한
- E - 실행
- R - 읽기

표 17-1. 역할 및 사용 권한

작업	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
도구 > 포트 연결	E	R	E	E	E	E	E	R	E	E
도구> 흐름 추적	E	R	E	E	E	E	E	R	E	E
도구 > 포트 미러링	FA	R	FA	FA	FA	FA	FA	R	없음	없음
도구 > IPFIX	FA	R	FA	R	FA	R	FA	R	없음	없음
방화벽 > 일반	FA	R	R	R	FA	R	FA	R	없음	없음
방화벽 > 구성	FA	R	R	R	FA	R	FA	R	없음	없음
암호화	FA	R	FA	R	FA	FA	없음	없음	없음	없음
라우팅 > 라우터	FA	R	FA	R	R	R	FA	R	R	R
라우팅 > NAT	FA	R	FA	R	FA	R	FA	R	R	R
DHCP > 서버 프로파일	FA	R	FA	R	FA	없음	FA	R	없음	없음
DHCP > 서버	FA	R	FA	R	FA	없음	FA	R	없음	없음

표 17-1. 역할 및 사용 권한 (계속)

작업	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
DHCP > 릴레이 프로파일	FA	R	FA	R	FA	없음	FA	R	없음	없음
DHCP > 릴레이 서비스	FA	R	FA	R	FA	없음	FA	R	없음	없음
DHCP > 메타데이터 프로кси	FA	R	FA	R	FA	없음	없음	없음	없음	없음
IPAM	FA	R	FA	R	FA	없음	없음	없음	없음	없음
스위칭 > 스위치	FA	R	FA	FA	R	R	FA	R	R	R
스위칭 > 포트	FA	R	FA	FA	R	R	FA	R	R	R
스위칭 > 스위칭 프로파일	FA	R	FA	FA	FA	FA	FA	R	R	R
로드 밸런싱 > 로드 밸런서	FA	R	없음	없음	없음	없음	FA	R	FA	R
로드 밸런싱 > 가상 서버	FA	R	없음	없음	없음	없음	FA	R	FA	R
로드 밸런싱 > 프로파일 > 애플리케이션 프로파일	FA	R	없음	없음	없음	없음	FA	R	FA	R
로드 밸런싱 > 프로파일 > 지속성 프로파일	FA	R	없음	없음	없음	없음	FA	R	FA	R
로드 밸런싱 > 프로파일 > SSL 프로파일	FA	R	없음	없음	FA	R	FA	R	FA	R
로드 밸런싱 > 서버 풀	FA	R	없음	없음	없음	없음	FA	R	FA	R
로드 밸런싱 > 모니터	FA	R	없음	없음	없음	없음	FA	R	FA	R
인벤토리 > 그룹	FA	R	FA	R	FA	R	FA	R	R	R
인벤토리 > IP 집합	FA	R	FA	R	FA	R	FA	R	R	R
인벤토리 > IP 풀	FA	R	FA	R	없음	R	없음	없음	R	R
인벤토리 > MAC 집합	FA	R	FA	R	FA	R	FA	R	R	R
인벤토리 > 서비스	FA	R	FA	R	FA	R	FA	R	R	R



표 17-1. 역할 및 사용 권한 (계속)

작업	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
인벤토리 > 가상 시스템	R	R	R	R	R	R	R	R	R	R
인벤토리 > VM > 태그 생성 및 할당	FA	R	FA	FA	FA	FA	FA	R	R	R
인벤토리 > VM > 태그 구성	FA	없음	없음	없음	FA	없음	없음	없음	없음	없음
패브릭 > 노드 > 호스트	FA	R	R	R	R	R	R	R	없음	없음
패브릭 > 노드 > 노드	FA	R	FA	R	FA	R	R	R	없음	없음
패브릭 > 노드 > Edge	FA	R	FA	R	R	R	R	R	없음	없음
패브릭 > 노드 > Edge 클러스터	FA	R	FA	R	R	R	R	R	없음	없음
패브릭 > 노드 > 브리지	FA	R	FA	R	R	R	없음	없음	R	R
패브릭 > 노드 > 전송 노드	FA	R	R	R	R	R	R	R	R	R
패브릭 > 노드 > 터널	R	R	R	R	R	R	R	R	R	R
패브릭 > 프로파일 > 업링크 프로파일	FA	R	R	R	R	R	R	R	R	R
패브릭 > 프로파일 > Edge 클러스터 프로파일	FA	R	FA	R	R	R	R	R	R	R
패브릭 > 프로파일 > 구성	FA	R	없음	없음	없음	없음	R	R	없음	없음
패브릭 > 전송 영역 > 전송 영역	FA	R	R	R	R	R	R	R	R	R
패브릭 > 전송 영역 > 전송 영역 프로파일	FA	R	R	R	R	R	R	R	R	R
패브릭 > 계산 관리자	FA	R	R	R	R	R	R	R	없음	없음
시스템 > 신뢰	FA	R	없음	없음	FA	R	없음	없음	FA	R
시스템 > 구성	E	R	R	R	R	R	없음	없음	없음	없음

표 17-1. 역할 및 사용 권한 (계속)

작업	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
시스템 > 유틸리티 > 지원 변들	FA	R	R	R	R	R	R	R	없음	없음
시스템 > 유틸리티 > 백업	FA	R	없음	없음	없음	없음	없음	없음	없음	없음
시스템 > 유틸리티 > 복원	FA	R	없음	없음	없음	없음	없음	없음	없음	없음
시스템 > 유틸리티 > 업그레이드	FA	R	R	R	R	R	없음	없음	없음	없음
시스템 > 사용자 > 역할 할당	FA	R	없음	없음	없음	없음	없음	없음	없음	없음
시스템 > 사용자 > 구성	FA	R	없음	없음	없음	없음	없음	없음	없음	없음

## 역할 할당 관리

VMware Identity Manager가 NSX-T Data Center와 통합된 경우 사용자 또는 사용자 그룹에 대해 역할 할당을 추가, 변경 및 삭제할 수 있습니다.

### 사전 요구 사항

- vIDM 호스트가 NSX-T와 연결되어 있는지 확인합니다. 자세한 내용은 [vIDM 호스트를 NSX-T에 연결](#)을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 사용자**를 선택합니다.
- 3 **역할 할당** 탭을 아직 선택하지 않았으면 클릭합니다.
- 4 역할 할당을 추가, 변경 또는 삭제합니다.

옵션	작업
역할 할당 추가	<b>추가</b> 를 클릭하고 사용자 또는 사용자 그룹을 선택한 후 역할을 선택합니다.
역할 할당 변경	사용자 또는 사용자 그룹을 선택하고 <b>편집</b> 을 클릭합니다.
역할 할당 삭제	사용자 또는 사용자 그룹을 선택하고 <b>삭제</b> 를 클릭합니다.

## 주체 ID 보기

주체는 NSX-T Data Center 구성 요소 또는 OpenStack 제품과 같은 타사 애플리케이션일 수 있습니다. 주체 ID를 사용하면 주체가 ID 이름을 사용하여 개체를 생성하고, ID 이름이 동일한 엔티티만 개체를 수정하거나 삭제할 수 있도록 합니다.

주체 ID는 다음과 같은 속성을 포함합니다.

- 이름
- 노드 ID
- 인증서
- 주체의 액세스 권한을 나타내는 RBAC 역할
- 이 주체가 생성한 개체가 보호되는지 여부를 나타내는 플래그

엔터프라이즈 관리자 역할이 있는 사용자(로컬, 원격 또는 주체 ID)는 주체 ID가 소유하는 개체를 수정하거나 삭제할 수 있습니다. 엔터프라이즈 관리자 역할이 없는 사용자(로컬, 원격 또는 주체 ID)는 주체 ID가 소유하는 보호된 개체를 수정하거나 삭제할 수 없지만 보호되지 않는 개체는 수정하거나 삭제할 수 있습니다. 엔터프라이즈 관리자 사용자는 NSX Manager UI가 아닌 NSX-T Data Center API를 사용해야만 보호된 개체를 삭제할 수 있습니다.

주체 ID는 NSX-T API를 사용해야만 생성 또는 삭제할 수 있습니다. 자세한 내용은 “NSX-T Data Center API 참조”를 참조하십시오. 하지만, NSX Manager UI 통해 주체 ID를 볼 수 있습니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 사용자**를 선택합니다.
- 3 **역할 할당** 탭을 클릭합니다.

사용자, 사용자 그룹 및 주체 ID가 표시됩니다.

## 인증서 설정

NSX Manager에서 CSR(인증서 서명 요청)을 생성한 후 이를 CA(인증 기관)로 보내 서버 인증서를 가져올 수 있습니다.

또한 CSR을 사용하여 자체 서명된 인증서를 생성할 수도 있습니다. 기존 인증서 또는 CA 인증서가 있는 경우 사용하기 위해 이를 가져올 수 있습니다. 해지된 인증서가 포함된 CRL(인증서 해지 목록)을 가져올 수도 있습니다.

## 인증서 서명 요청 파일 생성

CSR(인증서 서명 요청)은 조직 이름, 일반 이름, 구/군/시 및 국가와 같은 특정 정보를 포함하는 암호화된 텍스트입니다. CA(인증 기관)에 CSR 파일을 전송하여 디지털 ID 인증서를 신청합니다.

## 사전 요구 사항

- CSR 파일에 기입해야 하는 정보를 수집합니다. 서버의 FQDN, 조직 구성 단위, 조직, 구/군/시, 시/도 및 국가를 알아야 합니다.
- 공용 및 개인 키 쌍을 사용할 수 있는지 확인합니다.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 신뢰**를 선택합니다.
- 3 **CSRS** 탭을 클릭합니다.
- 4 **CSR 생성**을 클릭합니다.
- 5 CSR 파일 세부 정보 입력을 완료합니다.

옵션	설명
<b>이름</b>	인증서에 이름을 할당합니다.
<b>일반 이름</b>	서버의 FQDN(정규화된 도메인 이름)을 입력합니다. 예: test.vmware.com
<b>조직 이름</b>	해당 접미사를 포함하여 조직 이름을 입력합니다. 예: VMware Inc.
<b>조직 구성 단위</b>	이 인증서를 처리하는 조직의 부서를 입력합니다. 예: IT 부서
<b>인접성</b>	조직이 위치한 구/군/시를 추가합니다. 예: Palo Alto
<b>상태</b>	조직이 위치한 시/도를 추가합니다. 예: California
<b>국가</b>	조직이 위치한 국가를 추가합니다. 예: US(United States)
<b>메시지 알고리즘</b>	인증서에 대한 암호화 알고리즘을 설정합니다.  RSA 암호화 - 디지털 서명 및 메시지의 암호화에 사용됩니다. 따라서 암호화된 토큰을 생성할 때는 DSA보다 더 느리지만 이 토큰을 분석하고 유효성을 검사할 때는 더 빠릅니다. 이 암호화의 해독 시간은 더 느리고 암호화 시간은 더 빠릅니다.  DSA 암호화 - 디지털 서명에 사용됩니다. 따라서 암호화된 토큰을 생성할 때는 RSA보다 더 빠르지만 이 토큰을 분석하고 유효성을 검사할 때는 더 느립니다. 이 암호화의 해독 시간은 더 빠르고 암호화 시간은 더 느립니다.
<b>키 크기</b>	암호화 알고리즘의 키 비트 크기를 설정합니다.  기본값인 2048은 다른 키 크기가 필요한 경우가 아니면 적절합니다. 많은 CA에는 최솟값으로 2048이 필요합니다. 키 크기가 더 크면 더 안전하지만 성능에는 더 큰 영향을 미칩니다.
<b>설명</b>	나중에 이 인증서를 식별하는 데 도움이 되는 특정 세부 정보를 입력합니다.

**6 저장**을 클릭합니다.

사용자 지정 CSR이 링크로 표시됩니다.

**7 CSR**을 선택하고 **작업**을 클릭합니다.**8** 드롭다운 메뉴에서 **CSR PEM 다운로드**를 선택합니다.

기록 보관 및 CA 제출을 위해 CSR PEM 파일을 저장할 수 있습니다.

**9** CSR 파일의 콘텐츠를 사용하여 CA 등록 프로세스에 따라 CA에 인증서 요청을 제출합니다.**결과**

CA는 CSR 파일의 정보에 따라 서버 인증서를 생성하고, 개인 키를 사용하여 서명하고, 인증서를 사용자에게 전송합니다. 또한 CA는 사용자에게 루트 CA 인증서도 전송합니다.

## CA 인증서 가져오기

서명된 CA 인증서를 가져와 회사의 임시 CA가 될 수 있습니다. 인증서를 가져오면 자체 인증서에 서명할 권한을 갖게 됩니다.

**사전 요구 사항**

CA 인증서를 사용할 수 있는지 확인합니다.

**절차**

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 신뢰**를 선택합니다.
- 3 **인증서** 탭을 클릭합니다.
- 4 **가져오기 > CA 인증서 가져오기**를 선택하고 인증서 세부 정보를 입력합니다.

옵션	설명
이름	CA 인증서에 이름을 할당합니다.
인증서 콘텐츠	컴퓨터의 CA 인증서 파일을 찾은 후 해당 파일을 추가합니다.
설명	이 CA 인증서에 포함된 내용의 요약을 입력합니다.

**5 저장**을 클릭합니다.**결과**

이제 사용자 본인의 인증서에 서명할 수 있습니다.

## 인증서 가져오기

개인 키를 사용하여 인증서를 가져와 자체 서명된 인증서를 생성할 수 있습니다.

## 사전 요구 사항

인증서를 사용할 수 있는지 확인합니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 신뢰**를 선택합니다.
- 3 **인증서** 탭을 클릭합니다.
- 4 **가져오기 > 인증서 가져오기**를 선택하고 인증서 세부 정보를 입력합니다.

옵션	설명
이름	CA 인증서에 이름을 할당합니다.
인증서 콘텐츠	컴퓨터의 인증서 파일을 찾은 후 해당 파일을 추가합니다.
개인 키	컴퓨터의 개인 키 파일을 찾은 후 해당 파일을 추가합니다.
암호	이 인증서에 대한 암호를 추가합니다.
설명	이 인증서에 포함된 내용의 요약을 입력합니다.

- 5 **저장**을 클릭합니다.

### 결과

이제 자체 서명된 인증서를 생성할 수 있습니다.

## 자체 서명된 인증서 생성

자체 서명된 인증서를 사용하는 것은 신뢰할 수 있는 인증서를 사용하는 것보다 덜 안전합니다.

자체 서명된 인증서를 사용할 경우 클라이언트 사용자는 잘못된 보안 인증서와 같은 경고 메시지를 수신합니다. 그런 다음 클라이언트 사용자는 계속 진행하기 위해 서버에 처음 연결할 때 자체 서명된 인증서를 수락해야 합니다. 클라이언트 사용자가 이 옵션을 선택하면 다른 인증 방법보다 보안이 약화됩니다.

## 사전 요구 사항

CSR을 사용할 수 있는지 확인합니다. [인증서 서명 요청 파일 생성](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 신뢰**를 선택합니다.
- 3 **CSRS** 탭을 클릭합니다.
- 4 기존 CSR을 선택합니다.

- 5 작업을 클릭하고 드롭다운 메뉴에서 **CSR에 대한 자체 서명된 인증서**를 선택합니다.
- 6 자체 서명된 인증서가 유효한 일 수를 입력합니다.  
기본 기간은 10년입니다.
- 7 **저장**을 클릭합니다.

## 결과

자체 서명된 인증서는 **인증서** 목록에 표시됩니다. 인증서 유형은 자체 서명된 것으로 지정됩니다.

## 인증서 교체

인증서가 곧 만료되는 경우처럼 인증서를 교체해야 할 때 API 호출을 수행하여 기존 인증서를 교체할 수 있습니다.

### 사전 요구 사항

NSX Manager에서 인증서를 사용할 수 있는지 확인합니다. [자체 서명된 인증서 생성 및 인증서 가져오기](#)를 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 신뢰**를 선택합니다.
- 3 **인증서** 탭을 클릭합니다.
- 4 사용하려는 인증서의 ID를 클릭하고 팝업 창에서 인증서 ID를 복사합니다.
- 5 `POST /api/v1/node/services/http?action=apply_certificate` API 호출을 사용하여 기존 인증서를 교체합니다. 예를 들면 다음과 같습니다.

```
POST https://<nsx-mgr>/api/v1/node/services/http?
action=apply_certificate&certificate_id=e61c7537-3090-4149-b2b6-19915c20504f
```

자세한 내용은 "NSX-T API 참조"를 참조하십시오.

## 결과

HTTP 서비스가 새 인증서를 사용할 수 있도록 API 호출은 해당 서비스를 다시 시작합니다. POST 요청이 성공하면 응답 코드는 200 Accepted입니다.

## 인증서 해지 목록 가져오기

CRL(인증서 해지 목록)은 구독자 및 해당 인증서 상태의 목록입니다. 잠재적 사용자가 서버에 액세스하려고 하면 서버가 해당 특정 사용자의 CRL 항목을 기준으로 액세스를 거부합니다.

인증서 해지 목록에는 다음 항목이 포함됩니다.

- 해지된 인증서와 해지 이유
- 인증서가 발급된 날짜
- 인증서를 발급한 단체
- 제안된 다음 릴리스 날짜

## 사전 요구 사항

CRL을 사용할 수 있는지 확인합니다.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 신뢰**를 선택합니다.
- 3 **CRLS** 탭을 클릭합니다.
- 4 **가져오기**를 클릭하고 CRL 세부 정보를 추가합니다.

옵션	설명
이름	CRL에 이름을 할당합니다.
인증서 콘텐츠	CRL의 모든 항목을 복사한 후 이 섹션에 붙여 넣습니다. 샘플 CRL <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <pre>-----BEGIN X509 CRL----- MIIB0DCB4zANBgkqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTEEMMAoGA1UECBMD UUxEEMRkwFwYDVQQKEwBNaW5jb20gUHR5LjBmdGQuMQswCQYDVQQLEwJDUzEbMBKg A1UEAxMSU1NMZW51GR1bW8gc2VydMVFw0wMTAxMTUxNjI2NTdaFw0wMTAyMTQx NjI2NTdaMF1wEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEwMTAwMDBa MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMAOGCSqG SIb3DQEBAUAA0EAHPjQ3M93Q0j8Ufi+jZM7Y78TfAzG4jJn/E6MYBPFVQFY0/Gp UZexfjSVo5CIyyS0tYscz8o07avwBxTiMpDEQg== -----END X509 CRL--</pre> </div>
설명	이 CRL에 포함된 항목의 요약을 입력합니다.

- 5 **저장**을 클릭합니다.

## 결과

가져온 CRL이 링크로 나타납니다.

## CSR 인증서 가져오기

CSR에 대한 서명된 인증서를 가져올 수 있습니다.



자체 서명된 인증서를 사용할 경우 클라이언트 사용자는 잘못된 보안 인증서와 같은 경고 메시지를 수신합니다. 그런 다음 클라이언트 사용자는 계속 진행하기 위해 서버에 처음 연결할 때 자체 서명된 인증서를 수락해야 합니다. 클라이언트 사용자가 이 옵션을 선택하면 다른 인증 방법보다 보안이 약화됩니다.

### 사전 요구 사항

CSR을 사용할 수 있는지 확인합니다. [인증서 서명 요청 파일 생성](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 신뢰**를 선택합니다.
- 3 **CSRS** 탭을 클릭합니다.
- 4 기존 CSR을 선택합니다.
- 5 **작업**을 클릭하고 드롭다운 메뉴에서 **CSR에 대한 인증서 가져오기**를 선택합니다.
- 6 컴퓨터의 서명된 인증서 파일을 찾은 후 해당 파일을 추가합니다.
- 7 **저장**을 클릭합니다.

### 결과

자체 서명된 인증서는 **인증서** 목록에 표시됩니다. 인증서 유형은 자체 서명된 것으로 지정됩니다.

## 장치 구성

일부 시스템 구성 작업은 명령줄 또는 API를 사용하여 수행해야 합니다.

전체 명령줄 인터페이스 정보를 보려면 "NSX-T Data Center 명령줄 인터페이스 참조"를 참조하십시오. 전체 API 정보를 보려면 "NSX-T Data Center API 가이드"를 참조하십시오.

표 17-2. 시스템 구성 명령 및 API 요청

작업	명령줄 (NSX Manager, NSX Controller, NSX Edge)	API 요청 (NSX Manager만 해당)
시스템 시간대 설정	set timezone <timezone>	PUT <a href="https://&lt;nsx-mgr&gt;/api/v1/node">https://&lt;nsx-mgr&gt;/api/v1/node</a>
NTP 서버 설정	set ntp-server <ntp-server>	PUT <a href="https://&lt;nsx-mgr&gt;/api/v1/node/services/ntp">https://&lt;nsx-mgr&gt;/api/v1/node/services/ntp</a>
DNS 서버 설정	set name-servers <dns-server>	PUT <a href="https://&lt;nsx-mgr&gt;/api/v1/node/network/name-servers">https://&lt;nsx-mgr&gt;/api/v1/node/network/name-servers</a>
DNS 검색 도메인 설정	set search-domains <domain>	PUT <a href="https://&lt;nsx-mgr&gt;/api/v1/node/network/search-domains">https://&lt;nsx-mgr&gt;/api/v1/node/network/search-domains</a>

## 계산 관리자 추가

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

이 릴리스에서 이 기능은 다음을 지원합니다.

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

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 탐색 패널에서 **패브릭 > 계산 관리자**를 선택합니다.
- 3 **추가**를 클릭합니다.
- 4 계산 관리자 세부 정보를 완료합니다.

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

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

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

- 5 진행률 아이콘이 **진행 중**에서 **등록되지 않음**으로 변경되면 다음 단계를 수행하여 오류를 해결합니다.
  - a 오류 메시지를 선택하고 **해결**을 클릭합니다. 가능한 오류 메시지 중 하나는 다음과 같습니다.

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

- b vCenter Server 자격 증명을 입력하고 **해결**을 클릭합니다.  
기존 등록이 있으면 교체됩니다.

## 결과

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

## 태그 관리

개체에 태그를 추가하여 보다 쉽게 검색할 수 있습니다. 태그를 지정할 때 범위도 지정할 수 있습니다.

**NSX Cloud 참고** NSX Cloud를 사용 중인 경우 NSX Cloud에 필요한 구성, 지원되는 기능 및 자동 생성된 논리적 엔티티의 목록은 [공용 클라우드에 대해 NSX-T Data Center 기능을 사용하는 방법](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 개체 범주로 이동합니다.  
예를 들어 **스위칭 > 스위치**로 이동합니다.
- 3 스위치의 이름을 클릭합니다.
- 4 메뉴 옵션 **작업 > 태그 관리**를 선택하거나 태그 옆의 **관리**를 클릭합니다.
- 5 태그를 추가하거나 삭제합니다.

옵션	작업
태그 추가	<b>추가</b> 를 클릭하여 태그 및 범위(선택 사항)를 지정합니다.
태그 삭제	기존 태그를 선택하고 <b>삭제</b> 를 클릭합니다.

하나의 개체는 최대 30개의 태그를 가질 수 있습니다. 태그의 최대 길이는 256자입니다. 범위의 최대 길이는 128자입니다.

- 6 **저장**을 클릭합니다.

## 개체 검색

다양한 기준을 사용하여 NSX-T Data Center 인벤토리 전체에서 개체를 검색할 수 있습니다.

검색 결과는 관련성에 따라 정렬되며 검색 쿼리를 기준으로 이러한 결과를 필터링할 수 있습니다.

**참고** 검색 쿼리에 연산자로도 작동하는 특수 문자가 있는 경우 앞에 백슬래시를 추가해야 합니다. 연산자로 작동하는 문자는 +, -, =, & &, ||, <, >, !, (, ), {, }, [, ], ^, ', ~, ?, :, /, \입니다.

### 절차

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


- 2 홈 페이지에서 개체 또는 개체 유형에 대한 검색 패턴을 입력합니다.

검색 패턴을 입력할 때 검색 기능은 해당하는 키워드를 표시하여 지원을 제공합니다.

검색	검색 쿼리
이름 또는 속성에 <b>Logical</b> 이 들어 있는 개체	Logical
정확한 논리적 스위치 이름	display_name:LSP-301
!와 같은 특수 문자를 포함하는 이름	Logical\!

모든 관련 검색 결과가 각기 다른 탭의 리소스 유형별로 나열되고 그룹화됩니다.

리소스 유형에 대한 특정 검색 결과에 대한 탭을 클릭할 수 있습니다.

- 3 (선택 사항) 검색 창에서 저장 아이콘을 클릭하여 세부적인 검색 기준을 저장합니다.
- 4 검색 창에서  아이콘을 클릭하여 검색 범위를 좁힐 수 있는 고급 검색 열을 엽니다.
- 5 하나 이상의 조건을 지정하여 검색 범위를 좁힙니다.
- 이름
  - 리소스 유형
  - 설명
  - ID
  - 생성자
  - 수정한 사용자
  - 태그
  - 생성 날짜
  - 수정된 날짜
- 최근 검색 결과 및 저장된 검색 기준을 볼 수도 있습니다.
- 6 (선택 사항) 고급 검색 기준을 재설정하려면 **모두 지우기**를 클릭합니다.

## 원격 서버의 SSH 지문 찾기

원격 서버로 또는 원격 서버에서의 파일 복사와 관련된 일부 API 요청에서는 요청 본문에 원격 서버에 대한 SSH 지문을 제공해야 합니다. SSH 지문은 원격 서버의 호스트 키에서 파생됩니다.

SSH를 통해 연결하려면 NSX Manager 및 원격 서버가 공통된 호스트 키 유형을 가져야 합니다. 공통된 호스트 키 유형이 여러 개 있으면 NSX Manager의 HostKeyAlgorithm 구성에 따라 선호되는 유형이 사용됩니다.

원격 서버에 대한 지문이 있으면 올바른 서버에 연결할 수 있고 메시지 가로채기 공격으로부터 보호됩니다. 서버의 SSH 지문을 제공할 수 있는지를 원격 서버의 관리자에게 문의할 수 있습니다. 또는 원격 서버에 연결하여 지문을 찾을 수도 있습니다. 콘솔을 통해 서버에 연결하는 것이 네트워크를 통해 연결하는 것보다 더 안전합니다.

다음 표에는 NSX Manager에서 지원되는 키가 선호되는 순서부터 나열되어 있습니다.

표 17-3. 선호 순서대로 나타낸 NSX Manager 호스트 키

NSX Manager에서 지원되는 호스트 키 유형	키의 기본 위치
ECDSA(256비트)	/etc/ssh/ssh_host_ecdsa_key.pub
ED25519	/etc/ssh/ssh_host_ed25519_key.pub

## 절차

- 1 원격 서버에 루트 권한으로 로그인합니다.

콘솔을 사용하여 로그인하는 것이 네트워크를 사용하는 것보다 더 안전합니다.

- 2 /etc/ssh 디렉토리의 공용 키 파일을 나열합니다.

```
$ ls -al /etc/ssh/*pub
-rw-r--r-- 1 root root 601 Apr  8 18:10 ssh_host_dsa_key.pub
-rw-r--r-- 1 root root 93 Apr  8 18:10 ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root 393 Apr  8 18:10 ssh_host_rsa_key.pub
```

- 3 사용 가능한 키를 NSX Manager에서 지원되는 키와 비교해 보십시오.

이 예제에서는 ED25519가 유일하게 허용되는 키입니다.

- 4 키의 지문을 가져옵니다.

```
# awk '{print $2}' /etc/ssh/ssh_host_ed25519_key.pub | base64 -d | sha256sum -b | sed 's/ .*$//' | xxd -r -p | base64 | sed 's/./44g' | awk '{print "SHA256:"$1}'
SHA256:KemgftCfsd/hn7EEf1hJ4m1698rRhMmNN2IW8y9iq2A
```

## NSX Manager 백업 및 복원

NSX Manager가 작동 불가능 상태가 될 경우 백업에서 복원할 수 있습니다. NSX Manager를 작동할 수 없는 동안 데이터부는 영향을 받지 않지만 구성을 변경할 수는 없습니다.

백업 유형은 세 가지로 구분됩니다.

### 클러스터 백업

이 백업에는 가상 네트워크의 원하는 상태가 포함됩니다.

### 노드 백업

NSX Manager 노드의 백업입니다.

### 인벤토리 백업

이 백업에는 ESX 및 KVM 호스트/Edge 집합이 포함됩니다. 이 정보는 복원 작업 중에 관리부의 원하는 상태와 이러한 호스트 간의 불일치를 감지하고 해결하는 데 사용됩니다.

백업 방법으로는 다음 두 가지가 있습니다.

**수동 NSX Manager 노드 백업 및 클러스터 백업** 수동 노드 및 클러스터 백업은 언제든지 필요할 때 실행할 수 있습니다.

**자동 NSX Manager 노드 백업, 클러스터 백업 및 인벤토리 백업** 자동 백업은 설정된 스케줄에 따라 실행됩니다. 자동 백업을 사용하는 것을 적극 권장합니다. [자동 백업 스케줄링](#)의 내용을 참조하십시오.

최신 백업 상태를 유지하려면 자동 백업을 구성해야 합니다. 클러스터 및 인벤토리 백업을 정기적으로 실행하는 것이 중요합니다.

NSX-T Data Center 구성을 클러스터 백업에 캡처된 상태로 다시 복원할 수 있습니다. 백업을 복원할 때는 백업된 장치와 동일한 NSX Manager 버전이 실행되는 새 NSX Manager 장치로 복원해야 합니다.

## NSX Manager 구성 백업

NSX Manager 구성 백업은 NSX Manager 노드 백업, 클러스터 백업 및 인벤토리 백업으로 구성됩니다.

### 절차

#### 1 백업 위치 구성

백업은 NSX Manager에서 액세스할 수 있는 파일 서버에 저장됩니다. 백업이 진행되려면 먼저 이 서버의 위치를 구성해야 합니다.

#### 2 자동 백업 스케줄링

작동 불가능한 NSX Manager 및 해당 구성 데이터를 복원할 수 있도록 주기적인 백업을 스케줄링합니다. 자동 백업은 기본적으로 사용되지 않도록 설정되어 있습니다. 특정 요일 또는 지정된 간격으로 자동 백업이 수행되도록 스케줄링할 수 있습니다. 스케줄링된 백업을 사용하는 것을 적극 권장합니다.

### 백업 위치 구성

백업은 NSX Manager에서 액세스할 수 있는 파일 서버에 저장됩니다. 백업이 진행되려면 먼저 이 서버의 위치를 구성해야 합니다.

---

**참고** 설계상, NSX Manager는 백업 파일 서버에서 백업 파일을 삭제하지 않습니다. 백업 순환을 관리하고 서버에 백업을 위한 충분한 디스크 공간이 있는지 확인해야 합니다. 이전 백업을 자동으로 삭제하는 스크립트를 실행하는 것을 고려할 수 있습니다.

---

### 사전 요구 사항

백업 파일 서버의 SSH 지문이 있는지 확인합니다. SHA256 해시 ECDSA 키만 지문으로 허용됩니다. [원격 서버의 SSH 지문 찾기](#)의 내용을 참조하십시오.

## 절차

- 1 브라우저에서 NSX Manager(<https://<nsx-manager-ip-address>>)에 관리자로 로그인합니다.
- 2 **시스템 > 유틸리티 > 백업**을 클릭합니다.
- 3 백업 위치에 대한 액세스 자격 증명을 제공하려면 페이지 오른쪽 상단에 있는 **편집**을 클릭합니다.
- 4 **자동 백업** 토글을 클릭하여 자동 백업을 사용하도록 설정합니다.
- 5 백업 파일 서버의 IP 주소 또는 호스트 이름을 입력합니다.
- 6 필요한 경우 기본 포트를 편집합니다.
- 7 백업 파일 서버에 로그인하는 데 필요한 사용자 이름 및 암호를 입력합니다.
- 8 **대상 디렉토리** 필드에서 백업이 저장될 절대 디렉토리 경로를 입력합니다.  
디렉토리가 이미 존재해야 합니다. 여러 NSX-T Data Center 배포가 있는 경우 각 배포에 대해 다른 디렉토리를 사용합니다.
- 9 백업 데이터를 암호화하는 데 사용되는 암호를 입력합니다.  
백업을 복원하려면 이 암호가 필요합니다. 백업 암호를 잊어버리면 백업을 복원할 수 없습니다.
- 10 백업을 저장하는 서버의 SSH 지문을 입력합니다. [원격 서버의 SSH 지문 찾기](#)의 내용을 참조하십시오.
- 11 **저장**을 클릭합니다.
- 12 페이지 아래쪽의 **지금 백업**을 클릭하여 백업 파일 서버에 파일을 쓸 수 있음을 확인합니다.

## 다음에 수행할 작업

자동 백업을 스케줄링합니다.

## 자동 백업 스케줄링

작동 불가능한 NSX Manager 및 해당 구성 데이터를 복원할 수 있도록 주기적인 백업을 스케줄링합니다. 자동 백업은 기본적으로 사용되지 않도록 설정되어 있습니다. 특정 요일 또는 지정된 간격으로 자동 백업이 수행되도록 스케줄링할 수 있습니다. 스케줄링된 백업을 사용하는 것을 적극 권장합니다.

### 사전 요구 사항

- 해당 백업 위치를 확인합니다. 단일 실패 지점에 대해 보호를 제공하는 위치를 선택합니다. 예를 들어 장치와 동일한 파일 저장소에 백업을 두지 마십시오. 해당 파일 저장소에서 장애가 발생하면 장치와 해당 백업이 모두 영향을 받을 수 있습니다.
- 백업을 저장하는 서버의 ssh 지문을 찾습니다. [원격 서버의 SSH 지문 찾기](#)의 내용을 참조하십시오. 백업 및 복원 API 요청에서는 SSH 지문에 콜론이 포함되지 않아야 합니다.

## 절차

- 1 브라우저에서 NSX Manager(<https://<nsx-manager-ip-address>>)에 관리자로 로그인합니다.
- 2 **시스템 > 유틸리티 > 백업**을 클릭합니다.

- 3 페이지 상단 오른쪽 모서리에 있는 **편집**을 클릭합니다.
- 4 **파일 서버**를 클릭한 다음 [자동 백업]이 사용되도록 설정되어 있는지 확인합니다.
- 5 페이지 상단의 **스케줄**을 클릭합니다.
- 6 [노드/클러스터 백업]에서 **매주**를 클릭한 다음 SFTP 서버에 대한 백업 요일 및 시간을 설정하거나 **간격**을 클릭하고 백업 시간을 설정합니다.
- 7 인벤토리 백업은 기본적으로 5분 간격으로 발생하도록 설정되며 자주 발생해야 합니다. 기본 설정을 적용하거나 필요에 따라 변경하십시오.
- 8 **저장**을 클릭합니다.

## 결과

**참고** 첫 번째 주별 스케줄 백업은 지정된 요일 및 시간에 발생합니다. 첫 번째 간격 스케줄 백업은 자동 백업을 사용하도록 설정하여 백업 구성을 저장한 직후에 발생합니다.

NSX Manager는 노드 수준, 클러스터 수준 및 인벤토리의 세 가지 개별 백업 파일을 저장합니다. 백업 파일은 백업 구성에 지정된 SFTP 서버의 디렉토리에 저장됩니다. 해당 디렉토리 내에서 파일은 다음 디렉토리에 저장됩니다.

- /<user specified directory>/cluster-node-backups(클러스터 및 노드 백업)
- /<user specified directory>/inventory-summary(인벤토리 백업)

## NSX Manager 구성 복원

NSX Manager가 작동 불가능 상태가 될 경우 백업에서 복원할 수 있습니다. 백업이 생성되었을 때 지정된 암호가 필요합니다.

**참고** 백업이 생성된 동일한 NSX Manager 장치에서 백업을 복원하는 것은 지원되지 않습니다.

## 절차

### 1 NSX Manager 백업 복원 준비

NSX Manager 백업을 복원하기 전에 새 NSX Manager 장치를 설치해야 합니다. 새 NSX Manager는 이전 NSX Manager와 동일한 관리 IP 주소를 사용해서 배포해야 합니다.

### 2 백업 복원

백업을 복원하면 백업 당시의 네트워크 상태가 복원되고, NSX Manager에서 유지 보수되는 구성이 복원되고, 백업을 수행한 후 패브릭에 대해 수행된 노드 추가 또는 삭제와 같은 모든 변경 사항이 조정됩니다.

### 3 vCenter Server에서 NSX-T Data Center 확장 제거

계산 관리자를 추가하면 NSX Manager는 자체 ID를 확장으로 vCenter Server에 추가합니다. 이 vCenter Server를 NSX-T Data Center 설치에 등록하지 않으려면 vCenter Server의 MOB(Managed Object Browser)를 통해 확장을 제거할 수 있습니다.



## NSX Manager 백업 복원 준비

NSX Manager 백업을 복원하기 전에 새 NSX Manager 장치를 설치해야 합니다. 새 NSX Manager는 이전 NSX Manager와 동일한 관리 IP 주소를 사용해서 배포해야 합니다.

---

**참고** 백업이 생성된 동일한 NSX Manager 장치에서 백업을 복원하는 것은 지원되지 않습니다.

---

### 사전 요구 사항

- 백업을 생성하는 데 사용된 NSX Manager 버전을 알고 있는지와 동일한 버전의 설치 파일(OVA, OVF 또는 QCOW2)을 사용할 수 있는지 확인합니다.
- 노드 백업을 생성하는 데 사용된 NSX Manager에 할당된 IP 주소를 알고 있는지 확인합니다.
- 복원 프로세스가 완료될 때까지 NSX Manager의 구성을 변경하려고 하는 사람이 없도록 합니다.

### 절차

- 1 이전 NSX Manager 장치가 여전히 실행 중인 경우(예를 들어 업그레이드 시도를 롤백하기 위해 복원하는 경우) 장치를 종료합니다.
- 2 새 NSX Manager 장치를 설치합니다.
  - 새 NSX Manager 장치의 버전은 백업을 생성하는 데 사용된 장치의 버전과 같아야 합니다.
  - 관리자 백업에 해당하는 IP 주소를 사용하여 이 장치를 구성해야 합니다.
 이러한 단계에 대한 정보 및 지침을 보려면 “NSX-T Data Center 설치 가이드”를 참조하십시오.

### 다음에 수행할 작업

백업을 복원합니다.

## 백업 복원

백업을 복원하면 백업 당시의 네트워크 상태가 복원되고, NSX Manager에서 유지 보수되는 구성이 복원되고, 백업을 수행한 후 패브릭에 대해 수행된 노드 추가 또는 삭제와 같은 모든 변경 사항이 조정됩니다.

---

**참고** 백업이 생성된 동일한 NSX Manager 장치에서 백업을 복원하는 것은 지원되지 않습니다.

---

### 사전 요구 사항

- 백업 파일 서버의 SSH 지문이 있는지 확인합니다. SHA256 해시 ECDSA 키만 지문으로 허용됩니다. [원격 서버의 SSH 지문 찾기](#)의 내용을 참조하십시오.
- 노드 및 클러스터 백업 파일의 암호가 있는지 확인합니다.
- 구성된 개체가 없는 NSX Manager가 새로 설치되어 있는지 확인합니다. [NSX Manager 백업 복원 준비](#)의 내용을 참조하십시오.

### 절차

- 1 브라우저에서 새로 설치된 NSX Manager에 로그인합니다.

- 2 탐색 패널에서 **시스템 > 유틸리티**를 선택합니다.
- 3 **복원** 탭을 클릭합니다.
- 4 **편집**을 클릭하여 백업 파일 서버를 구성합니다.
- 5 IP 주소 또는 호스트 이름을 입력합니다.
- 6 필요한 경우 포트 번호를 변경합니다.  
기본값은 22입니다.
- 7 사용자 이름과 암호를 입력하여 서버에 로그인합니다.
- 8 **대상 디렉토리** 필드에서 백업이 저장될 절대 디렉토리 경로를 입력합니다.
- 9 백업 데이터를 암호화하는 데 사용된 암호를 입력합니다.
- 10 백업을 저장하는 서버의 SSH 지문을 입력합니다.
- 11 **저장**을 클릭합니다.
- 12 백업을 선택합니다.
- 13 **복원**을 클릭합니다.

복원 작업의 상태가 표시됩니다. 백업 이후에 패브릭 노드 또는 전송 노드를 삭제하거나 추가한 경우 특정 작업(예 : 노드에 로그인 및 스크립트 실행)을 수행하라는 메시지가 표시됩니다.

복원 작업이 완료되면 [복원 완료] 화면이 표시되고 복원 결과, 백업 파일의 타임 스탬프, 복원 작업의 시작 및 종료 시간이 표시됩니다. 복원에 실패하면 오류가 발생한 단계(예: Current Step: Restoring Cluster (DB) 또는 Current Step: Restoring Node)가 표시됩니다. 클러스터 복원 또는 노드 복원이 실패하면 해당 오류는 일시적일 수 있습니다. 이 경우 **재시도**를 클릭할 필요가 없습니다. 관리자를 다시 시작하거나 재부팅하면 복원이 계속됩니다.

다음 CLI 명령을 실행하여 시스템 로그 파일을 보고 문자열 클러스터 복원 실패 및 노드 복원 실패를 검색하여 클러스터 복원 또는 노드 복원 오류가 발생했는지 확인할 수도 있습니다.

```
get log-file syslog
```

관리자를 다시 시작하려면 다음 CLI 명령을 실행합니다.

```
restart service manager
```

관리자를 재부팅하려면 다음 CLI 명령을 실행합니다.

```
reboot
```

## 결과

**참고** 백업 후 계산 관리자를 추가한 경우, 복원 후 계산 관리자를 다시 추가하려고 하면 등록이 실패했다는 오류 메시지가 표시됩니다. 이 오류를 해결하고 계산 관리자를 추가할 수 있습니다. 자세한 내용은 [계산 관리자 추가](#)의 5단계를 참조하십시오. vCenter Server에 저장된 NSX-T Data Center에 대한 정보를 제거하려면 [vCenter Server에서 NSX-T Data Center 확장 제거](#)의 단계를 수행합니다.

## vCenter Server에서 NSX-T Data Center 확장 제거

계산 관리자를 추가하면 NSX Manager는 자체 ID를 확장으로 vCenter Server에 추가합니다. 이 vCenter Server를 NSX-T Data Center 설치에 등록하지 않으려면 vCenter Server의 MOB(Managed Object Browser)를 통해 확장을 제거할 수 있습니다.

### 절차

- 1 vSphere Web Client에 관리자로 로그인합니다.
- 2 ESXi 호스트를 선택합니다.
- 3 **관리 > 설정** 탭을 클릭합니다.
- 4 메뉴에서 **고급 시스템 설정**을 선택합니다.
- 5 **Config.HostAgent.plugins.solo.enableMob** 옵션을 사용하도록 설정합니다.
- 6 MOB에 로그인합니다.
- 7 속성 테이블에서 **content** 속성에 대한 값인 **content** 링크를 클릭합니다.
- 8 속성 테이블에서 **extensionManager** 속성에 대한 값인 **ExtensionManager** 링크를 클릭합니다.
- 9 메서드 테이블에서 **UnregisterExtension** 링크를 클릭합니다.
- 10 값 텍스트 필드에 **com.vmware.nsx.management.nsxt**를 입력합니다.
- 11 페이지 오른쪽에서 매개 변수 테이블 아래에 있는 **메서드 호출** 링크를 클릭합니다.

메서드 결과에 void가 표시되지만 확장은 제거됩니다.

- 12 확장이 제거되었는지 확인하려면 이전 페이지에서 **FindExtension** 메서드를 클릭하고 확장에 대해 동일한 값을 입력하여 호출합니다.

결과는 void여야 합니다.

## NSX Controller 클러스터 복원

NSX Controller 클러스터를 복구할 수 없거나 클러스터 멤버 자격 변경 때문에 하나 이상의 컨트롤러를 바꿔야 할 경우 전체 컨트롤러 클러스터를 복원해야 합니다.

컨트롤러 클러스터를 복원하기 전에 먼저 관리부에서 알려져 있는 멤버 자격과 컨트롤러 자체에 알려져 있는 실제 멤버 자격 간에 변경된 사항이 있는지 확인합니다. 백업 후에 변경이 수행되었으면 멤버 자격이 달라질 수 있습니다.

- 전체 클러스터를 복구할 수 없는 경우 [NSX Controller 클러스터 다시 배포](#)를 참조하십시오.
- 아래 단계에 따라 클러스터 멤버 자격이 변경되었는지 확인하고 변경되었으면 백업에서 복원하십시오.

### 사전 요구 사항

- 최근 백업이 있는지 확인합니다.
- 복원을 수행합니다. [백업 복원](#)의 내용을 참조하십시오.

## 절차

- 1 NSX Manager의 CLI에 로그인하고 `get management-cluster status` 명령을 실행합니다.
- 2 NSX Controller의 CLI에 로그인하고 `get managers` 명령을 실행하여 Controller가 Manager에 등록되었는지 확인합니다.
- 3 `get control-cluster status` 명령을 실행합니다.
- 4 멤버 자격이 변경되었는지 확인하려면 `get management-cluster status` 명령 출력의 IP 주소와 `get control-cluster status` 명령 출력을 비교합니다.  
  
IP 주소 집합이 동일하면 수행할 작업이 없습니다. IP 주소가 다르면 나머지 단계를 계속 진행하여 전체 컨트롤러 클러스터를 복원합니다.
- 5 NSX Controller의 CLI에 로그인하고 `get control-cluster status` 명령을 실행하여 마스터 컨트롤러를 확인합니다.  
  
마스터 컨트롤러 출력에는 `is master: true`가 표시됩니다.
- 6 특정 비마스터 컨트롤러에 대해 `stop service <controller>` 명령을 실행합니다.
- 7 마스터 컨트롤러에 로그인한 다음 `detach control-cluster <ip-address[:port]>` 명령을 실행하여 이전 단계의 비마스터 컨트롤러를 분리합니다.
- 8 (선택 사항) `get management-cluster status` 명령이 NSX Manager에서 이 컨트롤러를 표시하는 경우에만 NSX Manager에 대해 `detach controller <uuid>` 명령을 실행합니다.
- 9 NSX Controller의 CLI에 로그인하고 `deactivate control-cluster` 명령을 실행합니다.
- 10 `rm -r /opt/vmware/etc/bootstrap-config` 및 `rm -r /config/vmware/node-uuid` 명령을 사용하여 부트스트랩 파일 및 UUID 파일을 제거합니다.
- 11 나머지 비마스터 컨트롤러에 대해 6-10 단계를 수행합니다.
- 12 마스터 컨트롤러의 CLI에 로그인하고 `stop service <controller>` 명령을 실행합니다.
- 13 NSX Manager에 대해 `detach controller <uuid>` 명령을 실행하여 이 컨트롤러를 분리합니다.
- 14 마스터 컨트롤러의 CLI에 로그인하고 `deactivate control-cluster` 명령을 실행합니다.
- 15 `rm -r /opt/vmware/etc/bootstrap-config` 및 `rm -r /config/vmware/node-uuid` 명령을 사용하여 부트스트랩 파일 및 UUID 파일을 제거합니다.
- 16 NSX Manager에서 `get management-cluster status` 명령을 실행합니다. 출력에 표시되는 컨트롤러가 여전히 있으면 `detach controller <uuid>` 명령을 실행하여 나머지 컨트롤러를 분리합니다.

## 다음에 수행할 작업

다음 작업을 나열된 순서대로 완료하십시오.

- 1 복원을 완료합니다.
- 2 "NSX-T 설치 가이드"에 설명된 대로 NSX Controller를 관리부에 연결합니다.
- 3 "NSX-T 설치 가이드"에 설명된 대로 NSX Controller 클러스터를 다시 배포합니다.

## 장치 및 장치 클러스터 관리

각 NSX-T Data Center 설치에는 하나의 NSX Manager 인스턴스만 필요하며 하나의 NSX Manager 인스턴스만 지원합니다. NSX Controller 클러스터에 3개의 멤버가 있어야 합니다. NSX Edge 클러스터에는 2개 이상의 멤버가 있어야 합니다.

NSX Controller 또는 NSX Edge 클러스터의 장치가 작동 불가능해지거나 어떤 이유로 이를 제거해야 할 경우 새 장치로 교체할 수 있습니다.

**중요** NSX Controller 또는 NSX Edge 클러스터 멤버 자격을 변경하면 나중에 새 구성을 지원할 클러스터 백업을 생성해야 합니다. [NSX Manager 백업 및 복원](#)의 내용을 참조하십시오.

## NSX Manager 관리

NSX Manager의 상태를 확인하고 작동 불가능 상태가 될 경우 재부팅합니다.

### NSX Manager 상태 가져오기

NSX Manager UI를 통해 NSX Manager의 상태를 확인하거나 CLI 명령을 사용하여 상태를 가져올 수 있습니다.

#### 절차

- 1 브라우저에서 NSX Manager(<http://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 구성 요소**를 선택합니다.  
NSX Manager의 상태가 표시됩니다.
- 3 또는 NSX Manager의 CLI에 로그인합니다.
- 4 `get management-cluster status` 명령을 실행합니다. 예를 들면 다음과 같습니다.

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 10.172.121.217 (UUID 42191561-79dc-710a-74f1-d15f10cd2c40) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 10.172.121.91 (UUID ab35851f-e616-4760-8d7a-c4386c537382)
- 10.172.122.187 (UUID d159b758-c320-411f-aa67-1e2fd35f5ef2)
- 10.172.122.138 (UUID 12a3b19d-26a0-492e-836e-e9a3cc25e799)

Control cluster status: DEGRADED
```

**참고** 결과에 관리 클러스터라고 표시되더라도 NSX Manager의 인스턴스가 하나만 있을 수 있습니다.

## NSX Manager 재부팅

CLI 명령을 통해 NSX Manager를 재부팅하여 위험 오류에서 복구할 수 있습니다.

## 절차

- 1 NSX Manager의 CLI에 로그인합니다.
- 2 reboot 명령을 실행합니다. 예를 들면 다음과 같습니다.

```
nsx-manager> reboot
Are you sure you want to reboot (yes/no): y
```

## NSX Controller 클러스터 관리

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

NSX Controller 클러스터는 정상적으로 작동하려면 과반수 조건을 충족해야 합니다. 3개 멤버 중 2개가 온라인 상태이면 클러스터는 여전히 과반수 조건을 충족합니다. 오프라인 NSX Controller를 가져와 3멤버 클러스터를 복원해야 합니다. 가져올 수 없는 경우에는 바꿀 수 있습니다. [NSX Controller 클러스터의 멤버 교체](#)의 내용을 참조하십시오.

세 멤버 중 하나만 온라인 상태이면 클러스터는 과반수 조건을 충족하지 않으므로 정상적으로 작동하지 못합니다. 오프라인 멤버 중 하나를 가져올 수 경우, 실패한 NSX Controller를 바꾸거나 NSX Controller 클러스터를 다시 배포할 수 있습니다. [NSX Controller 클러스터 다시 배포](#)의 내용을 참조하십시오.

### 사전 요구 사항

장치를 복구할 수 없는 문제를 해결하는 방법을 확인합니다. 예를 들어 이러한 단계를 수행하면 장치를 교체하지 않고도 복구할 수 있습니다.

- 장치에 네트워크 연결이 있는지 확인하고 없는 경우 네트워크 연결이 되도록 합니다.
- 장치를 재부팅합니다.

### 다음에 수행할 작업

NSX Controller 클러스터 상태를 가져옵니다. [NSX Controller 클러스터 상태 가져오기](#)의 내용을 참조하십시오.

## NSX Controller 클러스터 상태 가져오기

NSX Manager에서 NSX Controller 클러스터의 상태를 확인할 수 있습니다. 해당 명령줄 인터페이스에서 각 NSX Controller의 상태를 확인할 수도 있습니다.

NSX Controller 클러스터의 상태 및 클러스터 멤버를 가져오면 NSX Controller 클러스터의 문제 원인을 파악하는 데 도움이 될 수 있습니다.

표 17-4. NSX Controller 클러스터 상태

	하나 이상의 컨트롤러 가 NSX Manager에 등록되어 있습니까?	NSX Controller 클러스터가 과 반수가 됩니까?	다운된 NSX Controller 클러스터 멤버가 있습니까?
NO_CONTROLLERS	아니요	해당 없음	해당 없음
UNAVAILABLE	알 수 없음	알 수 없음	알 수 없음
STABLE	예	예	아니요
DEGRADED	예	예	예
UNSTABLE	예	아니요	아니요

## 절차

- 1 NSX Manager CLI에 로그인합니다.
- 2 `get management-cluster status` 명령을 실행합니다.

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)

Control cluster status: STABLE
```

- 3 NSX Controller CLI에 로그인합니다.
- 4 `get control-cluster status` 명령을 실행합니다.

```
nsx-controller-1> get control-cluster status
uuid: 03fad907-612f-4068-8109-efdf73002038
is master: true
in majority: true
uuid                address                status
03fad907-612f-4068-8109-efdf73002038 192.168.110.51        active
1228c336-3932-4b5b-b87e-9f66259cebcd 192.168.110.52        active
f5348a2e-2d59-4edc-9618-2c05ac073fd8 192.168.110.53        active
```

## NSX Controller 클러스터 멤버 재부팅

NSX Controller 클러스터의 여러 멤버를 재부팅해야 하는 경우 한 번에 한 멤버를 재부팅해야 합니다. 3멤버 클러스터는 한 멤버가 오프라인 상태일 경우 과반수 조건을 충족합니다. 두 멤버가 오프라인 상태가 되면 클러스터는 과반수 조건을 충족하지 못하므로 정상적으로 작동하지 않습니다.

## 절차

- 1 NSX Manager의 CLI에 로그인합니다.
- 2 관리 및 제어 클러스터의 상태를 가져옵니다.

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)

Control cluster status: STABLE
```

- 3 재부팅해야 하는 NSX Controller의 CLI에 로그인한 후 재부팅합니다.

```
nsx-controller-2> reboot
Are you sure you want to reboot (yes/no): y
```

- 4 관리 및 제어 클러스터의 상태를 다시 가져옵니다. 추가 멤버를 재부팅하기 전에 제어 클러스터 상태가 STABLE이 될 때까지 기다립니다.

이 예에서 NSX Controller 192.168.110.53이 재부팅되고 제어 클러스터의 상태는 DEGRADED입니다. 즉, 클러스터는 과반수 조건을 충족하지만 멤버 중 하나는 다운된 상태입니다. NSX Controller 클러스터 상태에 대한 자세한 내용은 [NSX Controller 클러스터 상태 가져오기](#)를 참조하십시오.

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)

Control cluster status: DEGRADED
```

NSX Controller 클러스터가 STABLE 상태이면 추가 멤버를 재부팅하는 것이 안전합니다.

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
```



```
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)
```

```
Control cluster status: STABLE
```

- 5 개별 NSX Controller 장치 상태에 대한 정보가 필요한 경우 NSX Controller에 로그인하고 `get control-cluster status` 명령을 실행할 수 있습니다.

```
nsx-controller-1> get control-cluster status
uuid: 03fad907-612f-4068-8109-efdf73002038
is master: true
in majority: true
uuid          address          status
03fad907-612f-4068-8109-efdf73002038 192.168.110.51    active
1228c336-3932-4b5b-b87e-9f66259cebcd 192.168.110.52    active
f5348a2e-2d59-4edc-9618-2c05ac073fd8 192.168.110.53    not active
```

- 6 필요한 경우 추가 NSX Controller 장치를 재부팅하는 단계를 반복합니다.

## NSX Controller 클러스터의 멤버 교체

NSX Controller 클러스터에는 3개 이상의 멤버가 있어야 합니다. NSX Controller 장치가 작동 불가능한 상태가 되거나 다른 이유로 장치를 클러스터에서 제거하려는 경우에는 먼저 새 NSX Controller 장치를 추가하여 4멤버 클러스터를 만들어야 합니다. 네 번째 멤버가 추가되면 클러스터에서 NSX Controller 장치를 제거할 수 있습니다.

### 사전 요구 사항

- 장치를 복구할 수 없는 문제를 해결하는 방법을 확인합니다. 예를 들어 이러한 단계를 수행하면 장치를 교체하지 않고도 복구할 수 있습니다.
  - 장치에 네트워크 연결이 있는지 확인하고 없는 경우 네트워크 연결이 되도록 합니다.
  - 장치를 재부팅합니다.
- 교체하려는 NSX Controller 버전을 알고 있는지와 동일한 버전의 설치 파일(OVA, OVF 또는 QCOW2)을 사용할 수 있는지 확인합니다.

### 절차

- 1 새 NSX Controller를 설치하고 구성합니다.

이러한 단계에 대한 정보 및 지침을 보려면 "NSX-T Data Center 설치 가이드"를 참조하십시오.

- a 새 NSX Controller 장치를 설치합니다.

새 NSX Controller의 버전은 교체하려는 NSX Controller의 버전과 같아야 합니다.

- b 새 NSX Controller를 관리부에 연결합니다.

- c 새 NSX Controller를 제어 클러스터에 연결합니다.

- 2 클러스터에서 제거하려는 NSX Controller를 종료합니다.

- 3 다른 NSX Controller에 로그인하고 제거하려는 NSX Controller가 not active 상태인지 확인합니다.

```
nsx-controller-1> get control-cluster status
uuid: e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b
is master: true
in majority: true
```

uuid	address	status
06996547-f50c-43c0-95c1-8bb644dea498	192.168.110.53	active
471e5ac0-194b-437c-9359-564cea845333	192.168.110.54	active
e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b	192.168.110.51	active
863f9669-509f-4eba-b0ac-61a9702a242b	192.168.110.52	not active

- 4 클러스터에서 컨트롤러를 분리합니다.

```
nsx-controller-1> detach control-cluster 192.168.110.52
Successfully detached node from the control cluster.
```

- 5 관리부에서 컨트롤러를 분리합니다.

```
nsx-manager-1> detach controller 863f9669-509f-4eba-b0ac-61a9702a242b
The detach operation completed successfully
```

- 6 컨트롤러가 활성 상태인지와 제어 클러스터가 안정적인 상태인지 확인합니다.

NSX Controller:

```
nsx-controller-1> get control-cluster status
uuid: e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b
is master: true
in majority: true
```

uuid	address	status
06996547-f50c-43c0-95c1-8bb644dea498	192.168.110.53	active
471e5ac0-194b-437c-9359-564cea845333	192.168.110.54	active
e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b	192.168.110.51	active

NSX Manager:

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 4213216E-F93A-71B2-DA20-AFE5E714644F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.51 (UUID e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b)
- 192.168.110.53 (UUID 06996547-f50c-43c0-95c1-8bb644dea498)
- 192.168.110.54 (UUID 471e5ac0-194b-437c-9359-564cea845333)

Control cluster status: STABLE
```

## 결과

**참고** detach 명령을 사용하여 제거한 컨트롤러에는 일부 구성 정보가 유지됩니다. 컨트롤러를 다른 컨트롤러 클러스터에 다시 연결하려면 다음 CLI 명령을 컨트롤러에서 실행하여 오래된 정보를 제거해야 합니다.

```
deactivate control-cluster
```

## NSX Controller 클러스터 다시 배포

한 컨트롤러를 교체해도 NSX Controller 클러스터 문제가 해결되지 않거나 여러 NSX Controller 장치를 복구할 수 없는 경우 전체 클러스터를 다시 배포할 수 있습니다. NSX Manager에는 원하는 모든 구성 상태가 포함되며, NSX Controller 클러스터를 다시 생성하는 데 사용할 수 있습니다.

NSX Controller 클러스터 복원 중에 데이터 경로 연결이 중단되지 않습니다.

### 사전 요구 사항

- 장치를 복구할 수 없는 문제를 해결하는 방법을 확인합니다. 예를 들어 이러한 단계를 수행하면 장치를 교체하지 않고도 복구할 수 있습니다.
  - 장치에 네트워크 연결이 있는지 확인하고 없는 경우 네트워크 연결이 되도록 합니다.
  - 장치를 재부팅합니다.
- 교체하려는 NSX Controller 버전을 알고 있는지와 동일한 버전의 설치 파일(OVA, OVF 또는 QCOW2)을 사용할 수 있는지 확인합니다.
- NSX Controller 장치에 할당된 IP 주소를 알고 있는지 확인합니다.

### 절차

- 1 NSX Controller 클러스터의 모든 컨트롤러를 종료합니다.

## 2 NSX Manager에서 컨트롤러를 분리합니다.

- a NSX Manager CLI에 로그인합니다.
- b `get management-cluster status` 명령을 사용하여 컨트롤러 목록을 가져옵니다.

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 422EC8D8-B43F-D206-5048-781A5AECDC6) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID c28d0ac7-3107-4548-817a-50d76db007ab)
- 192.168.110.51 (UUID 4a0916c7-2f4d-48c2-81b6-29b7b3758ef4)
- 192.168.110.52 (UUID 1a409f24-9b9a-431e-a03a-1929db74bf00)

Control cluster status: UNSTABLE
```

- c `detach controller` 명령을 사용하여 컨트롤러를 분리합니다.

```
nsx-manager-1> detach controller 1a409f24-9b9a-431e-a03a-1929db74bf00
The detach operation completed successfully
nsx-manager-1> detach controller 4a0916c7-2f4d-48c2-81b6-29b7b3758ef4
The detach operation completed successfully
nsx-manager-1> detach controller c28d0ac7-3107-4548-817a-50d76db007ab
The detach operation completed successfully
```

## 3 세 개의 NSX Controller 장치를 설치하고 새 NSX Controller 클러스터를 생성합니다.

이러한 단계에 대한 정보 및 지침을 보려면 "NSX-T Data Center 설치 가이드"를 참조하십시오.

- a 세 개의 NSX Controller 장치를 설치합니다.
  - 새 NSX Controller 장치의 버전은 교체하려는 NSX Controller 장치의 버전과 같아야 합니다.
  - 이전 컨트롤러에 사용된 것과 동일한 IP 주소를 새 컨트롤러에 할당합니다.
- b NSX Controller 장치를 관리부에 연결합니다.
- c NSX Controller 장치 중 하나에서 제어 클러스터를 초기화합니다.
- d 다른 두 컨트롤러를 제어 클러스터에 연결합니다.

## NSX Edge 클러스터 관리

NSX Edge가 작동 불가능해지거나 하드웨어를 변경해야 할 경우 NSX Edge를 교체할 수 있습니다. 새 NSX Edge를 설치하고 새 전송 노드를 생성한 후에 NSX Edge 클러스터를 수정하여 이전 전송 노드를 새 전송 노드로 교체할 수 있습니다.

**참고** Tier-1 NSX Edge 클러스터를 제거하면 Tier-1 DR(분산 라우터) 인스턴스가 잠시 서비스 불가 상태가 됩니다.

## 절차

- 1 교체하려는 NSX Edge가 여전히 작동 중이면 유지 보수 모드로 전환하여 다운타임을 최소화할 수 있습니다. 연결된 논리적 라우터에서 고가용성이 사용되도록 설정될 경우 유지 보수 모드로 전환하면 논리적 라우터에서 다른 NSX Edge 클러스터 멤버가 사용됩니다. NSX Edge가 작동 불가능한 경우에는 이 작업을 수행할 필요가 없습니다.

- a 실패한 패브릭 노드의 패브릭 노드 ID를 가져옵니다.

```
https://192.168.110.201/api/v1/fabric/nodes
...
  "resource_type": "EdgeNode",
  "id": "a0f4fa74-e77c-11e5-8701-005056aeed61",
  "display_name": "edgenode-02a",
  ...
```

- b 실패한 NSX Edge 노드를 유지 보수 노드로 전환합니다.

```
POST https://192.168.110.201/api/v1/fabric/nodes/a0f4fa74-e77c-11e5-8701-005056aeed61?
action=enter_maintenance_mode
```

- 2 새 NSX Edge를 설치합니다.

이러한 단계에 대한 정보 및 지침을 보려면 "NSX-T Data Center 설치 가이드"를 참조하십시오.

- 3 join management-plane 명령을 사용하여 새 NSX Edge를 관리부에 연결합니다.

이러한 단계에 대한 정보 및 지침을 보려면 "NSX-T Data Center 설치 가이드"를 참조하십시오.

- 4 NSX Edge를 전송 노드로 구성합니다.

이러한 단계에 대한 정보 및 지침을 보려면 "NSX-T Data Center 설치 가이드"를 참조하십시오.

API에서 실패한 NSX Edge 장치의 전송 노드 구성을 가져오고 이 정보를 사용하여 새 전송 노드를 생성할 수 있습니다.

- a 새 패브릭 노드의 패브릭 노드 ID를 가져옵니다.

```
https://192.168.110.201/api/v1/fabric/nodes
...
  "resource_type": "EdgeNode",
  "id": "d61c8d86-f4b8-11e5-b1b2-005056ae3c10",
  "display_name": "edgenode-03a",
...
```

- b 실패한 전송 노드의 전송 노드 ID를 가져옵니다.

```
GET https://192.168.110.201/api/v1/transport-nodes
...
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
...
}
```

- c 실패한 전송 노드의 전송 노드 구성을 가져옵니다.

```
GET https://192.168.110.201/api/v1/transport-nodes/73cb00c9-70d0-4808-abfe-a12a43251133
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
  "tags": [],
  "transport_zone_endpoints": [
    ...
  ],
  "host_switches": [
    ...
  ],
  "node_id": "a0f4fa74-e77c-11e5-8701-005056aeed61",
  "_create_time": 1457696199196,
  "_last_modified_user": "admin",
  "_last_modified_time": 1457696225606,
  "_create_user": "admin",
  "_revision": 2
}
```

- d POST /api/v1/transport-nodes를 사용하여 새 전송 노드를 생성합니다.

요청 본문에서 새 전송 노드에 대한 다음 정보를 제공합니다.

- 새 전송 노드에 대한 description(선택 사항)
- 새 전송 노드의 display\_name
- 새 전송 노드를 생성하는 데 사용되는 패브릭 노드의 node\_id

요청 본문에서 실패한 전송 노드의 다음 정보를 복사합니다.

- transport\_zone\_endpoints
- host\_switches
- tags(선택 사항)

```
POST https://192.168.110.201/api/v1/transport-nodes
{
  "description": "",
  "display_name": "TN-edgenode-03a",
  "tags": [
    ...
  ],
  "transport_zone_endpoints": [
    ...
  ],
  "host_switches": [
    ...
  ],
  "node_id": "d61c8d86-f4b8-11e5-b1b2-005056ae3c10"
}
```

## 5 NSX Edge 클러스터를 편집하여 실패한 전송 노드를 새 전송 노드로 교체합니다.

- a 새 전송 노드 및 실패한 전송 노드의 ID를 가져옵니다. id 필드에는 전송 노드 ID가 포함됩니다.

```
GET https://192.168.110.201/api/v1/transport-nodes
```

```
...
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
  ...
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "890f0e3c-aa81-46aa-843b-8ac25fe30bd3",
  "display_name": "TN-edgenode-03a",
  ...
```

- b NSX Edge 클러스터의 ID를 가져옵니다. id 필드에는 NSX Edge 클러스터 ID가 포함됩니다. members 어레이에서 NSX Edge 클러스터의 멤버를 가져옵니다.

```
GET https://192.168.110.201/api/v1/edge-clusters
```

```
....
{
  "resource_type": "EdgeCluster",
  "description": "",
  "id": "9a302df7-0833-4237-af1f-4d826c25ad78",
  "display_name": "Edge-Cluster-1",
  ...
  "members": [
    {
      "member_index": 0,
      "transport_node_id": "73cb00c9-70d0-4808-abfe-a12a43251133"
    },
    {
      "member_index": 1,
      "transport_node_id": "e5d17b14-cdeb-4e63-b798-b23a0757463b"
    }
  ],
  ...
```

- c NSX Edge 클러스터를 편집하여 실패한 전송 노드를 새 전송 노드로 교체합니다. member\_index는 실패한 전송 노드의 인덱스와 일치해야 합니다.

---

**경고** NSX Edge가 여전히 작동 중일 때 이 작업을 수행하면 지장이 있습니다. 이렇게 하면 실패한 전송 노드의 모든 논리적 라우터 포트가 새 전송 노드로 이동됩니다.

---



이 예에서는 전송 노드 TN-edgenode-01a(73cb00c9-70d0-4808-abfe-a12a43251133)가 실패했으며 NSX Edge 클러스터 Edge-Cluster-1(9a302df7-0833-4237-af1f-4d826c25ad78)의 전송 노드 TN-edgenode-03a(890f0e3c-aa81-46aa-843b-8ac25fe30bd3)로 교체됩니다.

```
POST http://192.168.110.201/api/v1/edge-clusters/9a302df7-0833-4237-af1f-4d826c25ad78?
action=replace_transport_node
{
  "member_index": 0,
  "transport_node_id" : "890f0e3c-aa81-46aa-843b-8ac25fe30bd3"
}
```

**6** (선택 사항) 실패한 전송 노드 및 NSX Edge 노드를 삭제합니다.

## 로그 메시지

ESXi에서 실행되는 항목을 비롯한 모든 NSX-T Data Center 구성 요소의 로그 메시지는 RFC 5424에 명시된 syslog 형식을 준수합니다. KVM 호스트의 로그 메시지는 RFC 3164 형식입니다. 이 로그 파일은 /var/log 디렉토리에 있습니다.

NSX-T Data Center 장치에서 다음 NSX-T Data Center CLI 명령을 실행하여 로그를 확인할 수 있습니다.

```
get log-file <auth.log | http.log | kern.log | manager.log | node-mgmt.log | syslog> [follow]
```

하이퍼바이저에서 tac, tail, grep 및 more와 같은 Linux 명령을 사용하여 로그를 확인할 수 있습니다. 또한 NSX-T Data Center 장치에서 이러한 명령을 사용할 수 있습니다.

RFC 5424에 대한 자세한 내용은 <https://tools.ietf.org/html/rfc5424>를 참조하십시오. RFC 3164에 대한 자세한 내용은 <https://tools.ietf.org/html/rfc3164>를 참조하십시오.

RFC 5424는 로그 메시지에 대해 다음 형식을 정의합니다.

```
<facility * 8 + severity> version UTC-TZ hostname APP-NAME procid MSGID [structured-data] msg
```

샘플 로그 메시지:

```
<187>1 2016-03-15T22:53:00.114Z nsx-manager NSX - SYSTEM [nsx@6876 comp="nsx-manager" errorCode="MP4039"
subcomp="manager"] Connection verification failed for broker '10.160.108.196'. Marking broker unhealthy.
```

모든 메시지에는 메시지의 소스를 식별하는 데 도움이 되는 구성 요소(comp) 및 하위 구성 요소(subcomp) 정보가 있습니다.

NSX-T Data Center는 일반 로그(숫자 값이 22인 시설 local6) 및 감사 로그(숫자 값이 23인 시설 local7)를 생성합니다. 모든 API 호출은 감사 로그를 트리거합니다.

API 호출에 연결된 감사 로그에는 다음 정보가 있습니다.

- API의 개체를 식별하기 위한 엔티티 ID 매개 변수 entId.
- 특정 API 호출을 식별하기 위한 요청 ID 매개 변수 req-id.

- API 호출에 X-NSX-EREQID:<string> 머릿글이 포함된 경우 외부 요청 ID 매개 변수 `ereqId`.
- API 호출에 X-NSX-EUSER:<string> 머릿글이 포함된 경우 외부 사용자 매개 변수 `euser`.

RFC 5424는 다음과 같은 심각도 수준을 정의합니다.

심각도 수준	설명
0	긴급: 시스템을 사용할 수 없음
1	경고: 작업을 즉시 수행해야 함
2	위험: 위험한 상태
3	오류: 오류 상태
4	경고: 경고 상태
5	알림: 일반적이지만 중요한 상태
6	정보: 정보용 메시지
7	디버그: 디버그 수준 메시지

심각도가 긴급, 경고, 위험 또는 오류인 모든 로그에는 로그 메시지의 구조화된 데이터 부분에 고유한 오류 코드가 포함되어 있습니다. 오류 코드는 문자열과 10진수로 구성됩니다. 문자열은 특정 모듈을 나타냅니다.

MSGID 필드는 메시지 유형을 식별합니다. 메시지 ID 목록은 [로그 메시지 ID](#)의 내용을 참조하십시오.

## 원격 로깅 구성

원격 로깅 서버로 로그 메시지를 전송하도록 NSX-T Data Center 장치 및 하이퍼바이저를 구성할 수 있습니다.

원격 로깅은 NSX Manager, NSX Controller, NSX Edge 및 하이퍼바이저에서 지원됩니다. 각 노드에서 개별적으로 원격 로깅을 구성해야 합니다.

KVM 호스트에서는 NSX-T Data Center 설치 패키지가 구성 파일을 `/etc/rsyslog.d` 디렉토리에 배치하여 자동으로 rsyslog 데몬을 구성합니다.

### 사전 요구 사항

- 로그를 수신하도록 로깅 서버를 구성합니다.

## 절차

**1** NSX-T Data Center 장치에서 원격 로깅을 구성하려면 다음을 수행합니다.

- a 다음 명령을 실행하여 로그 서버로 전송할 메시지 유형 및 로그 서버를 구성합니다. 여러 시설 또는 메시지 ID는 공백 없이 쉼표로 구분된 목록으로 지정할 수 있습니다.

```
set logging-server <hostname-or-ip-address[:port]> proto <proto> level <level> [facility <facility>]
[messageid <messageid>] [certificate <filename>] [structured-data <structured-data>]
```

이 명령에 대한 자세한 내용은 "NSX-T CLI 참조"를 참조하십시오. 명령을 여러 번 실행하여 여러 로깅 서버 구성을 추가할 수 있습니다. 예:

```
nsx> set logging-server 192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
nsx> set logging-server 192.168.110.60 proto udp level info facility auth,user
```

- b get logging-server 명령으로 로깅 구성을 확인할 수 있습니다. 예를 들면 다음과 같습니다.

```
nsx> get logging-servers
192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
192.168.110.60 proto udp level info facility auth,user
```

**2** ESXi 호스트에서 원격 로깅을 구성하려면 다음을 수행합니다.

- a 다음 명령을 실행하여 Syslog를 구성하고 테스트 메시지를 전송합니다.

```
esxcli network firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
esxcli system syslog mark -s "This is a test message"
```

- b 다음 명령을 실행하여 구성을 표시할 수 있습니다.

```
esxcli system syslog config get
```

**3** KVM 호스트에서 원격 로깅을 구성하려면 다음을 수행합니다.

- a 환경에 대한 /etc/rsyslog.d/10-vmware-remote-logging.conf 파일을 편집합니다.  
b 파일에 다음 줄을 추가합니다.

```
*.* @<ip>:514;RFC5424fmt
```

- c 다음 명령을 실행합니다.

```
service rsyslog restart
```

## 로그 메시지 ID

로그 메시지에서 메시지 ID 필드는 메시지 유형을 식별합니다. set logging-server 명령의 messageid 매개 변수를 사용하여 로깅 서버로 보낼 로그 메시지를 필터링할 수 있습니다.

표 17-5. 로그 메시지 ID

메시지 ID	예
FABRIC	호스트 노드 호스트 준비 Edge 노드 전송 영역 전송 노드 업링크 프로파일 클러스터 프로파일 Edge 클러스터 브리지 클러스터 및 끝점
SWITCHING	논리적 스위치 논리적 스위치 포트 스위칭 프로파일 스위치 보안 기능
ROUTING	논리적 라우터 논리적 라우터 포트 정적 라우팅 동적 라우팅 NAT
FIREWALL	방화벽 규칙 방화벽 규칙 섹션
FIREWALL-PKTLOG	방화벽 연결 로그 방화벽 패킷 로그
GROUPING	IP 집합 MAC 집합 NSGroup NSService NSService 그룹 VNI 풀 IP 풀
DHCP	DHCP 릴레이
SYSTEM	장치 관리(원격 syslog, ntp 등) 클러스터 관리 신뢰 관리 라이선싱 사용자 및 역할 작업 관리 설치(NSX Manager, NSX Controller) 업그레이드(NSX Manager, NSX Controller, NSX Edge 및 호스트 패키지 업그레이드) 인식 태그

표 17-5. 로그 메시지 ID (계속)

메시지 ID	예
MONITORING	SNMP 포트 연결 Traceflow
-	다른 모든 로그 메시지

## IPFIX 구성

IPFIX(Internet Protocol Flow Information Export)는 네트워크 흐름 정보의 형식 및 내보내기에 대한 표준입니다. 스위치 및 방화벽에 대해 IPFIX를 구성할 수 있습니다. 스위치의 경우 VIF(가상 인터페이스) 및 pNIC(물리적 NIC)의 네트워크 흐름이 내보내집니다. 방화벽의 경우 분산 방화벽 구성 요소가 관리하는 네트워크 흐름이 내보내집니다.

**NSX Cloud 참고** NSX Cloud를 사용 중인 경우 NSX Cloud에 필요한 구성, 지원되는 기능 및 자동 생성된 논리적 엔티티의 목록은 [공용 클라우드에 대해 NSX-T Data Center 기능을 사용하는 방법](#)의 내용을 참조하십시오.

IPFIX를 사용하도록 설정하면 구성된 모든 호스트 전송 노드가 포트 4739를 사용하여 IPFIX 메시지를 IPFIX 수집기로 보냅니다. ESXi의 경우 NSX-T Data Center는 포트 4739를 자동으로 엽니다. KVM의 경우 방화벽이 사용되지 않도록 설정되면 포트 4739가 열리지만 방화벽이 사용되도록 설정되면 NSX-T Data Center가 포트를 자동으로 열지 않으므로 포트가 열려 있는지 확인해야 합니다.

ESXi 및 KVM의 IPFIX는 여러 가지 방법으로 터널 패킷을 샘플링합니다. ESXi에서 터널 패킷은 다음과 같은 두 가지 레코드로 샘플링됩니다.

- 일부 내부 패킷 정보를 포함하는 외부 패킷 레코드
  - SrcAddr, DstAddr, SrcPort, DstPort 및 Protocol은 외부 패킷을 나타냅니다.
  - 내부 패킷을 설명하기 위한 일부 엔터프라이즈 항목을 포함합니다.
- 내부 패킷 레코드
  - SrcAddr, DstAddr, SrcPort, DstPort 및 Protocol은 내부 패킷을 나타냅니다.

KVM에서 터널 패킷은 다음 한 가지 레코드로 샘플링됩니다.

- 일부 외부 터널 정보를 포함하는 내부 패킷 레코드
  - SrcAddr, DstAddr, SrcPort, DstPort 및 Protocol은 내부 패킷을 나타냅니다.
  - 외부 패킷을 설명하기 위한 일부 엔터프라이즈 항목을 포함합니다.

### 사전 요구 사항

- 하나 이상의 IPFIX 수집기를 설치합니다.
- IPFIX 수집기가 네트워크를 통해 하이퍼바이저에 연결되는지 확인합니다.
- ESXi 방화벽을 비롯한 모든 관련 방화벽이 IPFIX 수집기 포트의 트래픽을 허용하는지 확인합니다.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **도구 > IPFIX**를 선택합니다.
- 3 스위치 IPFIX를 구성하려면 **스위치 IPFIX 수집기** 탭을 클릭합니다.
- 4 **추가**를 클릭합니다.
- 5 이름과 설명(선택 사항)을 입력합니다.
- 6 **추가**를 클릭하고 수집기의 IP 주소와 포트를 입력합니다.  
최대 4개의 수집기를 추가할 수 있습니다.
- 7 **저장**을 클릭합니다.

## 스위치 IPFIX 프로파일 구성

스위치의 IPFIX 프로파일을 구성할 수 있습니다.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **도구 > IPFIX**를 선택합니다.
- 3 **스위치 IPFIX 프로파일** 탭을 클릭합니다.
- 4 **추가**를 클릭하여 프로파일을 추가합니다.

설정	설명
이름 및 설명	이름과 설명(선택 사항)을 입력합니다.
활성 시간 초과(초)	흐름과 연결된 추가 패킷이 수신되는 경우라도 흐름이 시간 초과되기까지의 시간입니다. 기본값은 300입니다.
유희 시간 초과(초)	흐름과 연결된 추가 패킷이 수신되지 않고 흐름이 시간 초과되기까지의 시간입니다(ESXi만 해당, KVM은 활성 시간 초과를 기준으로 모든 흐름을 시간 초과함). 기본값은 300입니다.
최대 흐름 수	브리지에 캐시되는 최대 흐름입니다(KVM만 해당, ESXi에서 구성 가능하지 않음). 기본값은 16384입니다.
샘플링 확률(%)	샘플링되는 패킷의 비율(근사치)입니다. 이 설정을 증가시키면 하이퍼바이저 및 수집기의 성능에 영향을 미칠 수 있습니다. 모든 하이퍼바이저가 수집기에 더 많은 IPFIX 패킷을 전송하는 경우 수집기가 모든 패킷을 수집하지 못할 수 있습니다. 확률을 기본값인 0.1%로 설정하면 성능에 미치는 영향이 낮게 유지됩니다.
관찰 도메인 ID	관찰 도메인 ID는 네트워크 흐름이 시작되는 관찰 도메인을 식별합니다. 특정 관찰 도메인을 지정하지 않으려면 0을 입력합니다.
수집기 프로파일	이전 단계에서 구성한 스위치 IPFIX 수집기를 선택합니다.
우선 순위	이 매개 변수는 여러 프로파일이 적용되는 경우 충돌을 해결합니다. IPFIX 내보내기는 우선 순위가 가장 높은 프로파일만 사용합니다. 값이 낮을수록 우선 순위가 더 높습니다.

## 5 적용 대상을 클릭하여 하나 이상의 개체에 프로파일을 적용합니다.

개체 유형은 논리적 포트, 논리적 스위치 및 NSGroup입니다. NSGroup을 선택할 경우, 개체에 논리적 스위치나 논리적 포트가 하나 이상 포함되어 있어야 합니다. NSGroup에 IP 집합 또는 MAC 집합만 포함되어 있으면 해당 개체는 무시됩니다.

## 6 저장을 클릭합니다.

# 방화벽 IPFIX 수집기 구성

방화벽의 IPFIX 수집기를 구성할 수 있습니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **도구 > IPFIX**를 선택합니다.
- 3 **방화벽 IPFIX 수집기** 탭을 클릭합니다.
- 4 이름과 설명(선택 사항)을 입력합니다.
- 5 **추가**를 클릭하고 수집기의 IP 주소와 포트를 입력합니다.  
최대 4개의 수집기를 추가할 수 있습니다.

## 6 저장을 클릭합니다.

# 방화벽 IPFIX 프로파일 구성

방화벽의 IPFIX 프로파일을 구성할 수 있습니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **도구 > IPFIX**를 선택합니다.
- 3 **방화벽 IPFIX 프로파일** 탭을 클릭합니다.
- 4 **추가**를 클릭하여 프로파일을 추가합니다.

설정	설명
이름 및 설명	이름과 설명(선택 사항)을 입력합니다.
수집기 구성	드롭다운 목록에서 수집기를 선택합니다.
활성화된 흐름 내보내기 시간 초과(분)	흐름과 연결된 추가 패킷이 수신되는 경우라도 흐름이 시간 초과되기까지의 시간입니다. 기본값은 1입니다.
우선 순위	이 매개 변수는 여러 프로파일이 적용되는 경우 충돌을 해결합니다. IPFIX 내보내기는 우선 순위가 가장 높은 프로파일만 사용합니다. 값이 낮을수록 우선 순위가 더 높습니다.
관찰 도메인 ID	이 매개 변수는 네트워크 흐름이 시작되는 관찰 도메인을 식별합니다. 기본값은 0이며 특정 관찰 도메인이 없음을 나타냅니다.

**5 적용 대상**을 클릭하여 하나 이상의 개체에 프로파일을 적용합니다.

개체 유형은 논리적 포트, 논리적 스위치 및 NSGroup입니다. NSGroup을 선택할 경우, 개체에 논리적 스위치나 논리적 포트가 하나 이상 포함되어 있어야 합니다. NSGroup에 IP 집합 또는 MAC 집합만 포함되어 있으면 해당 개체는 무시됩니다.

**6 저장**을 클릭합니다.

## ESXi IPFIX 템플릿

ESXi 호스트 전송 노드는 8개의 IPFIX 흐름 템플릿을 지원합니다.

### IPv4 템플릿

템플릿 ID: 256

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsId, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

### IPv4 캡슐화된 템플릿

템플릿 ID: 257

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
```



```

IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port - Uplink Port, Access port, N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_END()

```

## IPv4 ICMP 템플릿

템플릿 ID: 258

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
// Specify the Interface port - Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()

```

## IPv4 ICMP 캡슐화된 템플릿

템플릿 ID: 259

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsId, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

## IPv6 템플릿

템플릿 ID: 260

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
```

```
// Specify the Interface port - Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

## IPv6 캡슐화된 템플릿

템플릿 ID: 261

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
//ENCAP specific
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port - Uplink Port, Access Port, or NA
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_END()
```

## IPv6 ICMP 템플릿

템플릿 ID: 262

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
```

```

IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
// Specify the Interface port - Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsId, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()

```

## IPv6 ICMP 캡슐화된 템플릿

템플릿 ID: 263

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_VMW_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
//ENCAP Specific
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port - Uplink Port, Access Port, or NA
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsId, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

## KVM IPFIX 템플릿

KVM 호스트 전송 노드는 88개의 IPFIX 흐름 템플릿 및 하나의 옵션 템플릿을 지원합니다.

## KVM 이더넷 IPFIX 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 KVM 이더넷 IPFIX 템플릿이 있습니다.

### 이더넷 수신

템플릿 ID: 256. 필드 수: 27.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)

- flowEndReason(길이: 1)

## 이더넷 송신

템플릿 ID: 257. 필드 수: 31.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 8)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)

- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)

## 터널을 통한 이더넷 수신

템플릿 ID: 258. 필드 수: 34.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)

- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)

### 터널을 통한 이더넷 송신

템플릿 ID: 259. 필드 수: 38.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 8)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))



- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)

## KVM IPv4 IPFIX 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 KVM IPv4 IPFIX 템플릿이 있습니다.

### IPv4 수신

템플릿 ID: 276. 필드 수: 45.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)

- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)

- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## IPv4 송신

템플릿 ID: 277. 필드 수: 49.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)

- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## 터널을 통한 IPv4 수신

템플릿 ID: 278. 필드 수: 52.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)

- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## 터널을 통한 IPv4 송신

템플릿 ID: 279. 필드 수: 56.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)

- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)

- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## IPv4 IPFIX를 통한 KVM TCP 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 IPv4 IPFIX를 통한 KVM TCP 템플릿이 있습니다.

### IPv4를 통한 TCP 수신

템플릿 ID: 280. 필드 수: 53.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)



- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)

- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)
- tcpAckTotalCount(길이: 8)
- tcpFinTotalCount(길이: 8)
- tcpPshTotalCount(길이: 8)
- tcpRstTotalCount(길이: 8)
- tcpSynTotalCount(길이: 8)
- tcpUrgTotalCount(길이: 8)

## IPv4를 통한 TCP 송신

템플릿 ID: 281. 필드 수: 57.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)

- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)

- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)
- tcpAckTotalCount(길이: 8)
- tcpFinTotalCount(길이: 8)
- tcpPshTotalCount(길이: 8)
- tcpRstTotalCount(길이: 8)
- tcpSynTotalCount(길이: 8)
- tcpUrgTotalCount(길이: 8)

## 터널을 통해 IPv4를 통한 TCP 수신

템플릿 ID: 282. 필드 수: 60.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)

- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)

- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)
- tcpAckTotalCount(길이: 8)
- tcpFinTotalCount(길이: 8)
- tcpPshTotalCount(길이: 8)
- tcpRstTotalCount(길이: 8)
- tcpSynTotalCount(길이: 8)
- tcpUrgTotalCount(길이: 8)

터널을 통해 IPv4를 통한 TCP 송신

템플릿 ID: 283. 필드 수: 64.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)

- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)

- postMcastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMcastOctetTotalCount(길이: 8)
- tcpAckTotalCount(길이: 8)
- tcpFinTotalCount(길이: 8)
- tcpPshTotalCount(길이: 8)
- tcpRstTotalCount(길이: 8)
- tcpSynTotalCount(길이: 8)
- tcpUrgTotalCount(길이: 8)

## IPv4 IPFIX를 통한 KVM UDP 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 IPv4 IPFIX를 통한 KVM UDP 템플릿이 있습니다.

### IPv4를 통한 UDP 수신

템플릿 ID: 284. 필드 수: 47.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)



- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)

- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

#### IPv4를 통한 UDP 송신

템플릿 ID: 285. 필드 수: 51.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)

- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)

- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## 터널을 통해 IPv4를 통한 UDP 수신

템플릿 ID: 286. 필드 수: 54.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))

- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

터널을 통해 IPv4를 통한 UDP 송신

템플릿 ID: 287. 필드 수: 58.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))

- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP LENGTH MINIMUM(길이: 8)
- IP LENGTH MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## IPv4 IPFIX를 통한 KVM SCTP 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 IPv4 IPFIX를 통한 KVM SCTP 템플릿이 있습니다.

## IPv4를 통한 SCTP 수신

템플릿 ID: 288. 필드 수: 47.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)



- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## IPv4를 통한 SCTP 송신

템플릿 ID: 289. 필드 수: 51.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)

- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)

- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

### 터널을 통해 IPv4를 통한 SCTP 수신

템플릿 ID: 290. 필드 수: 54.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)

- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)

- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## 터널을 통해 IPv4를 통한 SCTP 송신

템플릿 ID: 291. 필드 수: 58.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)

- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)

- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## KVM ICMPv4 IPFIX 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 KVM ICMPv4 IPFIX 템플릿이 있습니다.

### ICMPv4 수신

템플릿 ID: 292. 필드 수: 47.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- ICMP\_IPv4\_TYPE(길이: 1)
- ICMP\_IPv4\_CODE(길이: 1)
- 898(길이: 가변, PEN: VMware Inc.(6876))

- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## ICMPv4 송신

템플릿 ID: 293. 필드 수: 51.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)



- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- ICMP\_IPv4\_TYPE(길이: 1)
- ICMP\_IPv4\_CODE(길이: 1)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)

- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## 터널을 통한 ICMPv4 수신

템플릿 ID: 294. 필드 수: 54.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)

- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- ICMP\_IPv4\_TYPE(길이: 1)
- ICMP\_IPv4\_CODE(길이: 1)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)

- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

### 터널을 통한 ICMPv4 송신

템플릿 ID: 295. 필드 수: 58.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)

- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- ICMP\_IPv4\_TYPE(길이: 1)
- ICMP\_IPv4\_CODE(길이: 1)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)

- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## KVM IPv6 IPFIX 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 KVM IPv6 IPFIX 템플릿이 있습니다.

### IPv6 수신

템플릿 ID: 296. 필드 수: 46.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)

- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)

- postMCastOctetTotalCount(길이: 8)

## IPv6 송신

템플릿 ID: 297. 필드 수: 50.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)



- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## 터널을 통한 IPv6 수신

템플릿 ID: 298. 필드 수: 53.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)

- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)

- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## 터널을 통한 IPv6 송신

템플릿 ID: 299. 필드 수: 57.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)

- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)

- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## IPv6 IPFIX를 통한 KVM TCP 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 IPv6 IPFIX를 통한 KVM TCP 템플릿이 있습니다.

### IPv6을 통한 TCP 수신

템플릿 ID: 300. 필드 수: 54.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)

- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)

- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)
- tcpAckTotalCount(길이: 8)
- tcpFinTotalCount(길이: 8)
- tcpPshTotalCount(길이: 8)
- tcpRstTotalCount(길이: 8)
- tcpSynTotalCount(길이: 8)
- tcpUrgTotalCount(길이: 8)

#### IPv6을 통한 TCP 송신

템플릿 ID: 301. 필드 수: 58.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)

- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)



- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)
- tcpAckTotalCount(길이: 8)
- tcpFinTotalCount(길이: 8)
- tcpPshTotalCount(길이: 8)
- tcpRstTotalCount(길이: 8)
- tcpSynTotalCount(길이: 8)
- tcpUrgTotalCount(길이: 8)

### 터널을 통해 IPv6을 통한 TCP 수신

템플릿 ID: 302. 필드 수: 61.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)

- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)

- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)
- tcpAckTotalCount(길이: 8)
- tcpFinTotalCount(길이: 8)
- tcpPshTotalCount(길이: 8)
- tcpRstTotalCount(길이: 8)
- tcpSynTotalCount(길이: 8)
- tcpUrgTotalCount(길이: 8)

#### 터널을 통해 IPv6을 통한 TCP 송신

템플릿 ID: 303. 필드 수: 65.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)

- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)

- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)
- tcpAckTotalCount(길이: 8)
- tcpFinTotalCount(길이: 8)
- tcpPshTotalCount(길이: 8)
- tcpRstTotalCount(길이: 8)
- tcpSynTotalCount(길이: 8)
- tcpUrgTotalCount(길이: 8)

## IPv6 IPFIX를 통한 KVM UDP 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 IPv6 IPFIX를 통한 KVM UDP 템플릿이 있습니다.

### IPv6을 통한 UDP 수신

템플릿 ID: 304. 필드 수: 48.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)

- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)

- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

#### IPv6을 통한 UDP 송신

템플릿 ID: 305. 필드 수: 52.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)

- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)



- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## 터널을 통해 IPv6을 통한 UDP 수신

템플릿 ID: 306. 필드 수: 55.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))

- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)

- postMCastOctetTotalCount(길이: 8)

## 터널을 통해 IPv6을 통한 UDP 송신

템플릿 ID: 307. 필드 수: 59.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))

- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)

- postMCastOctetTotalCount(길이: 8)

## IPv6 IPFIX를 통한 KVM SCTP 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 IPv6 IPFIX를 통한 KVM SCTP 템플릿이 있습니다.

### IPv6을 통한 SCTP 수신

템플릿 ID: 308. 필드 수: 48.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)

- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## IPv6을 통한 SCTP 송신

템플릿 ID: 309. 필드 수: 52.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)

- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)

- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

#### 터널을 통해 IPv6을 통한 SCTP 수신

템플릿 ID: 310. 필드 수: 55.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)



- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)

- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## 터널을 통해 IPv6을 통한 SCTP 송신

템플릿 ID: 311. 필드 수: 59.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)

- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)

- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## KVM ICMPv6 IPFIX 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 KVM ICMPv6 IPFIX 템플릿이 있습니다.

### ICMPv6 수신

템플릿 ID: 312. 필드 수: 48.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)

- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- ICMP\_IPv6\_TYPE(길이: 1)
- ICMP\_IPv6\_CODE(길이: 1)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)

- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## ICMPv6 송신

템플릿 ID: 313. 필드 수: 52.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- ICMP\_IPv6\_TYPE(길이: 1)

- ICMP\_IPv6\_CODE(길이: 1)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

터널을 통한 ICMPv6 수신

템플릿 ID: 314. 필드 수: 55.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- ICMP\_IPv6\_TYPE(길이: 1)
- ICMP\_IPv6\_CODE(길이: 1)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)



- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

### 터널을 통한 ICMPv6 송신

템플릿 ID: 315. 필드 수: 59.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)

- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- ICMP\_IPv6\_TYPE(길이: 1)
- ICMP\_IPv6\_CODE(길이: 1)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)

- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## KVM 이더넷 VLAN IPFIX 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 KVM 이더넷 VLAN IPFIX 템플릿이 있습니다.

### 이더넷 VLAN 수신

템플릿 ID: 316. 필드 수: 30.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)

## 이더넷 VLAN 송신

템플릿 ID: 317. 필드 수: 34.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 8)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)

- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)

## 터널을 통한 이더넷 VLAN 수신

템플릿 ID: 318. 필드 수: 37.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)

- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)

## 터널을 통한 이더넷 VLAN 송신

템플릿 ID: 319. 필드 수: 41.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 8)
- IF\_NAME(길이: 가변)

- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)

## KVM IPv4 VLAN IPFIX 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 KVM IPv4 VLAN IPFIX 템플릿이 있습니다.



## IPv4 VLAN 수신

템플릿 ID: 336. 필드 수: 48.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)

- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## IPv4 VLAN 송신

템플릿 ID: 337. 필드 수: 52.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)

- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)

- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## 터널을 통한 IPv4 VLAN 수신

템플릿 ID: 338. 필드 수: 55.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)

- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)

- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

### 터널을 통한 IPv4 VLAN 송신

템플릿 ID: 339. 필드 수: 59.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)

- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)

- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## IPv4 VLAN IPFIX를 통한 KVM TCP 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 IPv4 VLAN IPFIX를 통한 KVM TCP 템플릿이 있습니다.

### IPv4 VLAN을 통한 TCP 수신

템플릿 ID: 340. 필드 수: 56.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)



- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)

- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)
- tcpAckTotalCount(길이: 8)
- tcpFinTotalCount(길이: 8)
- tcpPshTotalCount(길이: 8)
- tcpRstTotalCount(길이: 8)
- tcpSynTotalCount(길이: 8)
- tcpUrgTotalCount(길이: 8)

### IPv4 VLAN을 통한 TCP 송신

템플릿 ID: 341. 필드 수: 60.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)

- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)

- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)
- tcpAckTotalCount(길이: 8)
- tcpFinTotalCount(길이: 8)
- tcpPshTotalCount(길이: 8)
- tcpRstTotalCount(길이: 8)
- tcpSynTotalCount(길이: 8)
- tcpUrgTotalCount(길이: 8)

터널을 통해 IPv4 VLAN을 통한 TCP 수신

템플릿 ID: 342. 필드 수: 63.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)

- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)

- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)
- tcpAckTotalCount(길이: 8)
- tcpFinTotalCount(길이: 8)
- tcpPshTotalCount(길이: 8)
- tcpRstTotalCount(길이: 8)
- tcpSynTotalCount(길이: 8)
- tcpUrgTotalCount(길이: 8)

터널을 통해 IPv4 VLAN을 통한 TCP 송신

템플릿 ID: 343. 필드 수: 67.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)

- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)

- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)
- tcpAckTotalCount(길이: 8)
- tcpFinTotalCount(길이: 8)
- tcpPshTotalCount(길이: 8)
- tcpRstTotalCount(길이: 8)
- tcpSynTotalCount(길이: 8)
- tcpUrgTotalCount(길이: 8)

## IPv4 VLAN IPFIX를 통한 KVM UDP 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 IPv4 VLAN IPFIX를 통한 KVM UDP 템플릿이 있습니다.

### IPv4 VLAN을 통한 UDP 수신

템플릿 ID: 344. 필드 수: 50.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)



- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)

- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

#### IPv4 VLAN을 통한 UDP 송신

템플릿 ID: 345. 필드 수: 54.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)

- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)

- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

터널을 통해 IPv4 VLAN을 통한 UDP 수신

템플릿 ID: 346. 필드 수: 57.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)

- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)

- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

터널을 통해 IPv4 VLAN을 통한 UDP 송신

템플릿 ID: 347. 필드 수: 61.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)

- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)

- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## IPv4 VLAN IPFIX를 통한 KVM SCTP 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 IPv4 VLAN IPFIX를 통한 KVM SCTP 템플릿이 있습니다.

### IPv4 VLAN을 통한 SCTP 수신

템플릿 ID: 348. 필드 수: 50.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)



- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)

- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## IPv4 VLAN을 통한 SCTP 송신

템플릿 ID: 349. 필드 수: 54.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)

- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## 터널을 통해 IPv4 VLAN을 통한 SCTP 수신

템플릿 ID: 350. 필드 수: 57.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))

- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

터널을 통해 IPv4 VLAN을 통한 SCTP 송신

템플릿 ID: 351. 필드 수: 61.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))

- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## KVM ICMPv4 VLAN IPFIX 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 KVM ICMPv4 VLAN IPFIX 템플릿이 있습니다.

### ICMPv4 VLAN 수신

템플릿 ID: 352. 필드 수: 50.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- ICMP\_IPv4\_TYPE(길이: 1)
- ICMP\_IPv4\_CODE(길이: 1)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)



- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## ICMPv4 VLAN 송신

템플릿 ID: 353. 필드 수: 54.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)

- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- ICMP\_IPv4\_TYPE(길이: 1)
- ICMP\_IPv4\_CODE(길이: 1)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)

- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## 터널을 통한 ICMPv4 VLAN 수신

템플릿 ID: 354. 필드 수: 57.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)

- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- ICMP\_IPv4\_TYPE(길이: 1)
- ICMP\_IPv4\_CODE(길이: 1)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)

- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## 터널을 통한 ICMPv4 VLAN 송신

템플릿 ID: 355. 필드 수: 61.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)

- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IP\_SRC\_ADDR(길이: 4)
- IP\_DST\_ADDR(길이: 4)
- ICMP\_IPv4\_TYPE(길이: 1)
- ICMP\_IPv4\_CODE(길이: 1)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)

- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## KVM IPv6 VLAN IPFIX 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 KVM IPv6 VLAN IPFIX 템플릿이 있습니다.

### IPv6 VLAN 수신

템플릿 ID: 356. 필드 수: 49.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)

- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)



- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## IPv6 VLAN 송신

템플릿 ID: 357. 필드 수: 53.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)

- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)

- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## 터널을 통한 IPv6 VLAN 수신

템플릿 ID: 358. 필드 수: 56.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)

- FLOW\_LABEL(길이: 4)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)

- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## 터널을 통한 IPv6 VLAN 송신

템플릿 ID: 359. 필드 수: 60.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)

- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)

- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## IPv6 VLAN IPFIX를 통한 KVM TCP 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 IPv6 VLAN IPFIX를 통한 KVM TCP 템플릿이 있습니다.

### IPv6 VLAN을 통한 TCP 수신

템플릿 ID: 360. 필드 수: 57.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)

- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)



- tcpAckTotalCount(길이: 8)
- tcpFinTotalCount(길이: 8)
- tcpPshTotalCount(길이: 8)
- tcpRstTotalCount(길이: 8)
- tcpSynTotalCount(길이: 8)
- tcpUrgTotalCount(길이: 8)

## IPv6 VLAN을 통한 TCP 송신

템플릿 ID: 361. 필드 수: 61.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)

- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)

- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)
- tcpAckTotalCount(길이: 8)
- tcpFinTotalCount(길이: 8)
- tcpPshTotalCount(길이: 8)
- tcpRstTotalCount(길이: 8)
- tcpSynTotalCount(길이: 8)
- tcpUrgTotalCount(길이: 8)

### 터널을 통해 IPv6 VLAN을 통한 TCP 수신

템플릿 ID: 362. 필드 수: 64.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)

- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)

- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)
- tcpAckTotalCount(길이: 8)
- tcpFinTotalCount(길이: 8)
- tcpPshTotalCount(길이: 8)
- tcpRstTotalCount(길이: 8)
- tcpSynTotalCount(길이: 8)
- tcpUrgTotalCount(길이: 8)

#### 터널을 통해 IPv6 VLAN을 통한 TCP 송신

템플릿 ID: 363. 필드 수: 68.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)

- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)

- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)
- tcpAckTotalCount(길이: 8)
- tcpFinTotalCount(길이: 8)
- tcpPshTotalCount(길이: 8)
- tcpRstTotalCount(길이: 8)
- tcpSynTotalCount(길이: 8)
- tcpUrgTotalCount(길이: 8)

## IPv6 VLAN IPFIX를 통한 KVM UDP 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 IPv6 VLAN IPFIX를 통한 KVM UDP 템플릿이 있습니다.

### IPv6 VLAN을 통한 UDP 수신

템플릿 ID: 364. 필드 수: 51.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)

- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)



- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

#### IPv6 VLAN을 통한 UDP 송신

템플릿 ID: 365. 필드 수: 55.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)

- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)

- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

터널을 통해 IPv6 VLAN을 통한 UDP 수신

템플릿 ID: 366. 필드 수: 58.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)

- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)

- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

터널을 통해 IPv6 VLAN을 통한 UDP 송신

템플릿 ID: 367. 필드 수: 62.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)

- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)

- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## IPv6 VLAN IPFIX를 통한 KVM SCTP 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 IPv6 VLAN IPFIX를 통한 KVM SCTP 템플릿이 있습니다.

### IPv6 VLAN을 통한 SCTP 수신

템플릿 ID: 368. 필드 수: 51.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)

- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)



- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

### IPv6 VLAN을 통한 SCTP 송신

템플릿 ID: 369. 필드 수: 55.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)

- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)

- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

터널을 통해 IPv6 VLAN을 통한 SCTP 수신

템플릿 ID: 370. 필드 수: 58.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)

- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)

- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

터널을 통해 IPv6 VLAN을 통한 SCTP 송신

템플릿 ID: 371. 필드 수: 62.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)

- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- L4\_SRC\_PORT(길이: 2)
- L4\_DST\_PORT(길이: 2)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)

- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## KVM ICMPv6 VLAN IPFIX 템플릿

수신, 송신, 터널을 통한 수신 및 터널을 통한 송신의 4개의 KVM ICMPv6 IPFIX 템플릿이 있습니다.

### ICMPv6 수신

템플릿 ID: 372. 필드 수: 51.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)

- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- ICMP\_IPv6\_TYPE(길이: 1)
- ICMP\_IPv6\_CODE(길이: 1)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)



- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## ICMPv6 송신

템플릿 ID: 373. 필드 수: 55.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)

- ICMP\_IPv6\_TYPE(길이: 1)
- ICMP\_IPv6\_CODE(길이: 1)
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

## 터널을 통한 ICMPv6 수신

템플릿 ID: 374. 필드 수: 58.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- ICMP\_IPv6\_TYPE(길이: 1)
- ICMP\_IPv6\_CODE(길이: 1)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))
- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))

- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)
- postMCastOctetTotalCount(길이: 8)

터널을 통한 ICMPv6 송신

템플릿 ID: 375. 필드 수: 62.

필드는 다음과 같습니다.

- observationPointId(길이: 4)
- DIRECTION(길이: 1)
- SRC\_MAC(길이: 6)
- DESTINATION\_MAC(길이: 6)
- ethernetType(길이: 2)
- ethernetHeaderLength(길이: 1)
- INPUT\_SNMP(길이: 4)
- Unknown(368)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- OUTPUT\_SNMP(길이: 4)
- Unknown(369)(길이: 4)
- IF\_NAME(길이: 가변)
- IF\_DESC(길이: 가변)
- SRC\_VLAN(길이: 2)
- dot1qVlanId(길이: 2)
- dot1qPriority(길이: 1)
- IP\_PROTOCOL\_VERSION(길이: 1)
- IP\_TTL(길이: 1)
- PROTOCOL(길이: 1)
- IP\_DSCP(길이: 1)
- IP\_PRECEDENCE(길이: 1)
- IP\_TOS(길이: 1)
- IPV6\_SRC\_ADDR(길이: 4)
- IPV6\_DST\_ADDR(길이: 4)
- FLOW\_LABEL(길이: 4)
- ICMP\_IPv6\_TYPE(길이: 1)
- ICMP\_IPv6\_CODE(길이: 1)
- 893(길이: 4, PEN: VMware Inc.(6876))
- 894(길이: 4, PEN: VMware Inc.(6876))

- 895(길이: 1, PEN: VMware Inc.(6876))
- 896(길이: 2, PEN: VMware Inc.(6876))
- 897(길이: 2, PEN: VMware Inc.(6876))
- 891(길이: 1, PEN: VMware Inc.(6876))
- 892(길이: 가변, PEN: VMware Inc.(6876))
- 898(길이: 가변, PEN: VMware Inc.(6876))
- flowStartDeltaMicroseconds(길이: 4)
- flowEndDeltaMicroseconds(길이: 4)
- DROPPED\_PACKETS(길이: 8)
- DROPPED\_PACKETS\_TOTAL(길이: 8)
- PKTS(길이: 8)
- PACKETS\_TOTAL(길이: 8)
- Unknown(354)(길이: 8)
- Unknown(355)(길이: 8)
- Unknown(356)(길이: 8)
- Unknown(357)(길이: 8)
- Unknown(358)(길이: 8)
- MUL\_DPKTS(길이: 8)
- postMCastPacketTotalCount(길이: 8)
- Unknown(352)(길이: 8)
- Unknown(353)(길이: 8)
- flowEndReason(길이: 1)
- DROPPED\_BYTES(길이: 8)
- DROPPED\_BYTES\_TOTAL(길이: 8)
- BYTES(길이: 8)
- BYTES\_TOTAL(길이: 8)
- BYTES\_SQUARED(길이: 8)
- BYTES\_SQUARED\_PERMANENT(길이: 8)
- IP\_LENGTH\_MINIMUM(길이: 8)
- IP\_LENGTH\_MAXIMUM(길이: 8)
- MUL\_DOCTETS(길이: 8)

- postMCastOctetTotalCount(길이: 8)

## KVM 옵션 IPFIX 템플릿

IETF RFC 7011, 섹션 3.4.2를 기반으로 하나의 KVM 옵션 템플릿이 있습니다.

### 옵션 템플릿

템플릿 ID: 462. 범위 수: 1. 데이터 수: 1.

## Traceflow를 사용하여 패킷의 경로 추적

Traceflow를 사용하여 논리적 네트워크의 한 논리적 포트에서 같은 네트워크의 다른 논리적 포트에 이동하는 패킷의 경로를 조사합니다. Traceflow는 논리적 포트에 삽입된 패킷의 전송 노드 수준 경로를 추적합니다. 추적 패킷은 논리적 스위치 오버레이를 이동하지만 논리적 스위치에 연결된 인터페이스에는 보이지 않습니다. 즉, 실제로 테스트 패킷의 의도된 수신자에게 전달되는 패킷은 없습니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 [Traceflow] 화면으로 이동합니다. 다음 두 가지 옵션 중에서 선택할 수 있습니다.
  - 탐색 패널에서 **도구 > Traceflow**를 선택합니다.
  - 탐색 패널에서 **스위칭**을 선택하고 **포트** 탭을 클릭한 후 VIF 연결 포트를 선택하고 **작업 > Traceflow**를 클릭합니다.
- 3 트래픽 유형을 선택합니다.
 

[유니캐스트], [멀티캐스트] 및 [브로드캐스트] 중에서 선택할 수 있습니다.
- 4 트래픽 유형에 따라 소스 및 대상 정보를 지정합니다.

트래픽 유형	소스 정보 지정	대상 정보 지정
유니캐스트	<p>VM 및 가상 인터페이스를 선택합니다.</p> <p>VMware Tools가 VM에 설치되거나 VM이 OpenStack 플러그인을 사용하여 배포되면(이 경우 주소 바인딩 사용) IP 주소 및 MAC 주소가 표시됩니다. VM에 둘 이상의 IP 주소가 있으면 드롭다운 메뉴에서 하나를 선택합니다.</p> <p>IP 주소 및 MAC 주소가 표시되지 않으면 텍스트 상자에 IP 주소 및 MAC 주소를 입력합니다.</p> <p>이 작업은 [멀티캐스트] 및 [브로드캐스트]에도 적용됩니다.</p>	<p>[유형] 드롭다운 메뉴에서 [VM 이름] 또는 [IP-MAC]을 선택합니다.</p> <ul style="list-style-type: none"> <li>■ [VM 이름]을 선택한 경우 VM 및 가상 인터페이스를 선택합니다. IP 주소 및 MAC 주소를 선택하거나 입력합니다.</li> <li>■ [IP-MAC]을 선택한 경우 추적 유형([계층 2] 또는 [계층 3])을 선택합니다. 추적 유형이 [계층 2]이면 IP 주소 및 MAC 주소를 입력합니다. 추적 유형이 [계층 3]이면 IP 주소를 입력합니다.</li> </ul>
멀티캐스트	위와 동일합니다.	IP 주소를 입력합니다. 224.0.0.0 - 239.255.255.255 범위의 멀티캐스트 주소여야 합니다.
브로드캐스트	위와 동일합니다.	서브넷 접두사 길이를 입력합니다.

- 5 (선택 사항) **고급**을 클릭하여 고급 옵션을 표시합니다.
- 6 (선택 사항) 왼쪽 열에서 다음 필드에 대해 원하는 값 또는 입력을 넣습니다.

옵션	설명
프레임 크기	예: 128
TTL	예: 64
시간 초과(밀리초)	예: 10000
Ethertype	예: 2048
페이로드 유형	드롭다운 메뉴에서 옵션을 선택합니다.
페이로드 데이터	선택한 페이로드 유형(Base64, Hex, Plaintext, Binary 또는 Decimal)에 따라 형식이 지정된 페이로드

- 7 (선택 사항) 왼쪽 열의 [프로토콜] 아래에서 [유형] 드롭다운 메뉴에 있는 프로토콜을 선택합니다.
- 8 (선택 사항) 선택한 프로토콜에 따라 다음 표의 관련 단계를 완료합니다.

프로토콜	1단계	2단계	3단계
TCP	소스 포트를 입력합니다.	대상 포트를 입력합니다.	드롭다운 메뉴에서 원하는 [TCP 플래그]를 선택합니다.
UDP	소스 포트를 입력합니다.	대상 포트를 입력합니다.	해당 없음
ICMP	ICMP ID를 입력합니다.	순서 값을 입력합니다.	해당 없음

## 9 추적을 클릭합니다.

연결, 구성 요소 및 계층에 대한 정보가 표시됩니다. 출력에는 [관찰 유형]([전송됨], [삭제됨], [수신됨], [전달됨]), [전송 노드] 및 [구성 요소]를 표시하는 테이블과 대상으로 유니캐스트 및 논리적 스위치가 선택된 토폴로지의 그래픽 맵이 포함됩니다. 표시되는 관찰에 필터(**모두**, **전송됨**, **삭제됨**)를 적용할 수 있습니다. 삭제된 관찰이 있으면 기본적으로 **삭제됨** 필터가 적용됩니다. 그렇지 않으면 **모두** 필터가 적용됩니다. 그래픽 맵에 백플레인 및 라우터 링크가 표시됩니다. 브리징 정보는 표시되지 않습니다.

## 포트 연결 정보 보기

포트 연결 도구를 사용하여 두 VM 간에 연결을 빠르게 시각화하고 문제를 해결할 수 있습니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **도구 > 포트 연결**을 선택합니다.
- 3 **소스 가상 시스템** 드롭다운 메뉴에서 VM을 선택합니다.
- 4 **대상 가상 시스템** 드롭다운 메뉴에서 VM을 선택합니다.



## 5 이동을 클릭합니다.

포트 연결 토폴로지의 시각적 맵이 표시됩니다. 시각적 출력에서 구성 요소를 클릭하여 해당 구성 요소에 대한 세부 정보를 확인할 수 있습니다.

# 논리적 스위치 포트 활동 모니터링

네트워크 정체 및 패킷 삭제 문제를 해결하려는 경우 등에 논리적 포트 활동을 모니터링할 수 있습니다.

## 사전 요구 사항

논리적 스위치 포트가 구성되어 있는지 확인합니다. [VM을 논리적 스위치에 연결](#)의 내용을 참조하십시오.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
  - 2 탐색 패널에서 **네트워킹 > 스위칭**을 선택합니다.
  - 3 **포트** 탭을 클릭합니다.
  - 4 포트의 이름을 클릭합니다.
  - 5 **모니터** 탭을 클릭합니다.
- 포트 상태 및 통계가 표시됩니다.
- 6 호스트에서 학습한 MAC 주소의 CSV 파일을 다운로드하려면 **MAC 테이블 다운로드**를 클릭합니다.
  - 7 포트의 작업을 모니터링하려면 **추적 시작**을 클릭합니다.

포트 추적 페이지가 열립니다. 양방향 포트 트래픽을 보고 삭제된 패킷을 식별할 수 있습니다. 포트 추적기 페이지에는 논리적 스위치 포트에 연결된 스위칭 프로파일도 나열됩니다.

## 결과

네트워크 정체로 인해 삭제된 패킷이 있는 경우 기본 패킷의 데이터 손실을 방지하도록 논리적 스위치 포트에 대한 QoS 스위칭 프로파일을 구성할 수 있습니다. [QoS 스위칭 프로파일 이해](#)의 내용을 참조하십시오.

# 포트 미러링 세션 모니터링

문제 해결 및 기타 목적으로 포트 미러링 세션을 모니터링할 수 있습니다.

---

**NSX Cloud 참고** NSX Cloud를 사용 중인 경우 NSX Cloud에 필요한 구성, 지원되는 기능 및 자동 생성된 논리적 엔티티의 목록은 [공용 클라우드에 대해 NSX-T Data Center 기능을 사용하는 방법](#)의 내용을 참조하십시오.

---

이 기능에는 다음과 같은 제한 사항이 있습니다.

- 소스 미러 포트는 둘 이상의 미러 세션일 수 없습니다.
- 대상 포트는 미러 트래픽만 수신할 수 있습니다.
- KVM을 사용하면 여러 NIC가 동일한 OVS 포트에 연결될 수 있습니다. 미러링은 OVS 업링크 포트에서 발생합니다. 즉, OVA 포트에 연결된 모든 물리적 NIC의 트래픽이 미러링됩니다.
- 미러 세션 소스 및 대상 포트는 동일한 호스트 vSwitch에 있어야 합니다. 따라서 소스 또는 대상 포트를 갖고 있는 VM을 다른 호스트로 vMotion하면 해당 포트의 트래픽을 더 이상 미러링할 수 없습니다.
- ESXi에서 업링크에 미러링을 사용하도록 설정하면 VDL2에 의해 Geneve 프로토콜을 사용하여 원시 프로덕션 TCP 패킷이 UDP 패킷으로 캡슐화됩니다. TSO(TCP 세분화 오프로드)를 지원하는 물리적 NIC는 패킷을 변경하고 MUST\_TSO 플래그로 패킷을 표시할 수 있습니다. VMXNET3 또는 E1000 vNIC가 있는 모니터 VM에서 드라이버는 패킷을 일반 UDP 패킷으로 취급하며 MUST\_TSO 플래그를 처리할 수 없으므로 해당 패킷을 삭제합니다.

많은 트래픽이 모니터 VM으로 미러링되면 드라이버의 버퍼 링이 꽉 차서 패킷이 삭제될 수 있습니다. 이 문제를 완화하기 위해 다음 작업 중 하나 이상을 수행할 수 있습니다.

- rx 버퍼 링 크기를 늘립니다.
- VM에 더 많은 CPU 리소스를 할당합니다.
- DPDK(Data Plane Development Kit)를 사용하여 패킷 처리 성능을 향상합니다.

**참고** 모니터 VM의 MTU 설정(KVM의 경우 하이퍼바이저의 가상 NIC 디바이스의 MTU 설정도 해당)이 패킷을 처리할 만큼 충분히 큰지 확인합니다. 캡슐화를 수행하면 패킷 크기가 커지므로 캡슐화된 패킷에서는 이러한 확인 작업이 특히 중요합니다. 그러지 않으면 패킷이 삭제될 수 있습니다. 이는 VMXNET3 NIC가 있는 ESXi VM의 문제가 아니며, ESXi 및 KVM VM 둘 다에 있는 다른 유형의 NIC에서 발생할 수 있는 문제입니다.

**참고** VM을 KVM 호스트에 포함하는 L3 포트 미러링 세션에서 캡슐화에 필요한 추가 바이트를 처리하는 데 충분한 크기로 MTU를 설정해야 합니다. 미러 트래픽은 OVS 인터페이스 및 OVS 업링크를 통과합니다. OVS 인터페이스의 MTU를 원래 패킷보다 적어도 100바이트 더 크게 설정해야 합니다(캡슐화 및 미러링 전에). 삭제된 패킷을 확인한 경우 호스트의 가상 NIC 및 OVS 인터페이스에 대한 MTU 설정을 늘립니다. 다음 명령을 사용하여 OVS 인터페이스에 대한 MTU를 설정합니다.

```
ovs-vsctl -- set interface <ovs_Interface> mtu_request=<MTU>
```

**참고** VM의 논리적 포트와 VM이 상주하는 호스트의 업링크 포트를 모니터링하면 호스트가 ESXi인지 또는 KVM인지에 따라 다른 동작이 나타납니다. ESXi의 경우 논리적 포트 미러 패킷 및 업링크 미러 패킷에 동일한 VLAN ID가 태그로 지정되어 모니터 VM에서 동일한 것으로 나타납니다. KVM의 경우 논리적 포트 미러 패킷에 VLAN ID가 태그로 지정되지 않으나 업링크 미러 패킷에는 이 태그가 지정되므로 두 패킷이 모니터 VM에 다른 것으로 나타납니다.

## 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **도구 > 포트 미러링 세션**을 선택합니다.
- 3 **추가**를 클릭하고 세션 유형을 선택합니다.  
사용 가능한 유형은 **로컬 SPAN**, **원격 SPAN**, **원격 L3 SPAN** 및 **논리적 SPAN**입니다.
- 4 세션 이름과 설명(선택 사항)을 입력합니다.
- 5 추가 매개 변수를 제공합니다.

세션 유형	매개 변수
로컬 SPAN	<ul style="list-style-type: none"> <li>■ <b>전송 노드</b> - 전송 노드를 선택합니다.</li> <li>■ <b>방향</b> - 양방향, 수신 또는 송신을 선택합니다.</li> <li>■ <b>패킷 잘림</b> - 패킷 잘림 값을 선택합니다.</li> </ul>
원격 SPAN	<ul style="list-style-type: none"> <li>■ <b>세션 유형</b> - RSPAN 소스 세션 또는 RSPAN 대상 세션을 선택합니다.</li> <li>■ <b>전송 노드</b> - 전송 노드를 선택합니다.</li> <li>■ <b>방향</b> - 양방향, 수신 또는 송신을 선택합니다.</li> <li>■ <b>패킷 잘림</b> - 패킷 잘림 값을 선택합니다.</li> <li>■ <b>VLAN ID 캡슐화</b> - 캡슐화 VLAN ID를 지정합니다.</li> <li>■ <b>원본 VLAN 유지</b> - 원본 VLAN ID 유지 여부를 선택합니다.</li> </ul>
원격 L3 SPAN	<ul style="list-style-type: none"> <li>■ <b>캡슐화</b> - GRE, ERSPAN 2, 또는 ERSPAN 3를 선택합니다.</li> <li>■ <b>GRE 키</b> - 캡슐화가 GRE인 경우 GRE 키를 지정합니다.</li> <li>■ <b>전송 노드</b> - 캡슐화가 ERSPAN 2 또는 ERSPAN 3인 경우 전송 노드를 지정합니다.</li> <li>■ <b>ERSPAN ID</b> - 캡슐화가 ERSPAN 2 또는 ERSPAN 3인 경우 ERSPAN ID를 지정합니다.</li> <li>■ <b>방향</b> - 양방향, 수신 또는 송신을 선택합니다.</li> <li>■ <b>패킷 잘림</b> - 패킷 잘림 값을 선택합니다.</li> </ul>
논리적 SPAN	<ul style="list-style-type: none"> <li>■ <b>논리적 스위치</b> - 논리적 스위치를 선택합니다.</li> <li>■ <b>방향</b> - 양방향, 수신 또는 송신을 선택합니다.</li> <li>■ <b>패킷 잘림</b> - 패킷 잘림 값을 선택합니다.</li> </ul>

- 6 다음을 클릭합니다.

- 7 소스 정보를 제공합니다.

세션 유형	매개 변수
로컬 SPAN	<ul style="list-style-type: none"> <li>■ N-VDS를 선택합니다.</li> <li>■ 물리적 인터페이스를 선택합니다.</li> <li>■ 캡슐화된 패킷을 사용하거나 사용하지 않도록 설정합니다.</li> <li>■ 가상 시스템을 선택합니다.</li> <li>■ 가상 인터페이스를 선택합니다.</li> </ul>
원격 SPAN	<ul style="list-style-type: none"> <li>■ 가상 시스템을 선택합니다.</li> <li>■ 가상 인터페이스를 선택합니다.</li> </ul>

세션 유형	매개 변수
원격 L3 SPAN	<ul style="list-style-type: none"> <li>■ 가상 시스템을 선택합니다.</li> <li>■ 가상 인터페이스를 선택합니다.</li> <li>■ 논리적 스위치를 선택합니다.</li> </ul>
논리적 SPAN	<ul style="list-style-type: none"> <li>■ 논리적 포트를 선택합니다.</li> </ul>

**8 다음**을 클릭합니다.

**9 대상 정보**를 제공합니다.

세션 유형	매개 변수
로컬 SPAN	<ul style="list-style-type: none"> <li>■ 가상 시스템을 선택합니다.</li> <li>■ 가상 인터페이스를 선택합니다.</li> </ul>
원격 SPAN	<ul style="list-style-type: none"> <li>■ N-VDS를 선택합니다.</li> <li>■ 물리적 인터페이스를 선택합니다.</li> </ul>
원격 L3 SPAN	<ul style="list-style-type: none"> <li>■ IPv4 주소를 지정합니다.</li> </ul>
논리적 SPAN	<ul style="list-style-type: none"> <li>■ 논리적 포트를 선택합니다.</li> </ul>

**10 저장**을 클릭합니다.

포트 미러링 세션을 저장한 후에는 소스나 대상을 변경할 수 없습니다.

## 패브릭 노드 모니터링

NSX Manager UI에서 호스트, Edge, NSX Edge 클러스터, 브리지 및 전송 노드와 같은 패브릭 노드를 모니터링할 수 있습니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **패브릭 > 노드**를 선택합니다.
- 3 다음 탭 중 하나를 선택합니다.
  - 호스트
  - Edge
  - Edge 클러스터
  - 브리지
  - 전송 노드

### 결과

**참고** [호스트] 화면에서 호스트의 [MPA 연결] 상태가 [다운] 또는 [알 수 없음]이면 [LCP 연결] 상태가 정확하지 않을 수 있으므로 무시합니다.

## VM에서 실행되는 애플리케이션에 대한 데이터 보기

NSGroup의 멤버인 VM에서 실행되는 애플리케이션에 대한 정보를 볼 수 있습니다. 이는 기술 미리보기 기능입니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **인벤토리 > 그룹**을 선택합니다.
- 3 NSGroup의 이름을 클릭합니다.
- 4 **애플리케이션** 탭을 클릭합니다.
- 5 **애플리케이션 데이터 수집**을 클릭합니다.

이 프로세스에는 몇 분 정도 소요될 수 있습니다. 프로세스가 완료되면 다음 정보가 표시됩니다.

- 프로세스의 총 수
- 다양한 계층(예: 웹 계층, 데이터베이스 계층 및 애플리케이션 계층)을 나타내는 원 또한 각 계층의 프로세스 수도 표시됩니다.

- 6 해당 계층의 프로세스에 대한 자세한 내용을 보려면 원을 클릭합니다.

## 지원 번들 수집

등록된 클러스터 및 패브릭 노드의 지원 번들을 수집하고 번들을 시스템에 다운로드하거나 파일 서버에 업로드할 수 있습니다.

번들을 시스템에 다운로드할 경우 각 노드에 대해 매니페스트 파일 및 지원 번들로 구성된 단일 아카이브 파일을 받게 됩니다. 번들을 파일 서버에 업로드할 경우 매니페스트 파일과 개별 번들은 파일 서버에 별도로 업로드됩니다.

---

**NSX Cloud 참고** CSM에 대한 지원 번들을 수집하려면 CSM에 로그인하고 **시스템 > 유틸리티 > 지원 번들**로 이동한 다음 **다운로드**를 클릭하십시오. PCG에 대한 지원 번들은 다음 지침을 사용하여 NSX Manager에서 사용할 수 있습니다. PCG에 대한 지원 번들에는 모든 워크로드 VM에 대한 로그도 포함되어 있습니다.

---

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 탐색 패널에서 **시스템 > 유틸리티**를 선택합니다.
- 3 **지원 번들** 탭을 클릭합니다.

**4 대상 노드를 선택합니다.**

사용 가능한 노드 유형은 관리 노드, 컨트롤러 노드, Edge, 호스트 및 공용 클라우드 게이트웨이입니다.

**5 (선택 사항) 로그 수명(일)을 지정하여 지정된 일 수보다 오래된 로그를 제외합니다.****6 (선택 사항) 코어 파일 및 감사 로그를 포함 또는 제외할지를 나타내는 스위치를 전환합니다.**

**참고** 코어 파일 및 감사 로그에는 암호 또는 암호화 키와 같은 중요한 정보가 포함될 수 있습니다.

**7 (선택 사항) 확인란을 선택하여 번들을 파일 서버에 업로드합니다.****8 번들 수집 시작**을 클릭하여 지원 번들 수집을 시작합니다.

존재하는 로그 파일의 개수에 따라 노드마다 몇 분 정도 걸릴 수 있습니다.

**9 수집 프로세스 상태를 모니터링합니다.**

상태 필드에는 지원 번들 수집을 완료한 노드의 백분율이 표시됩니다.

**10 번들을 파일 서버로 전송하는 옵션이 설정되지 않은 경우 다운로드**를 클릭하여 번들을 다운로드합니다.

## 고객 환경 향상 프로그램

NSX-T Data Center는 VMware의 CEIP(고객 환경 향상 프로그램)에 참여합니다.

CEIP를 통해 수집되는 데이터에 대한 세부 정보와 VMware에서 해당 정보를 사용하는 목적은 신뢰 및 보장 센터(<https://www.vmware.com/solutions/trustvmware/ceip.html>)에 명시되어 있습니다.

NSX-T Data Center에 대한 CEIP에 참여하거나 탈퇴하려는 경우 또는 프로그램 설정을 편집하려는 경우에는 [고객 환경 향상 프로그램 구성 편집](#) 항목을 참조하십시오.

## 고객 환경 향상 프로그램 구성 편집

NSX Manager를 설치하거나 업그레이드할 때 CEIP 참여를 결정하고 데이터 수집 설정 구성할 수 있습니다.

또한 기존 CEIP 구성을 편집하여 프로그램에 참여하거나 탈퇴하고, 정보 수집 빈도 및 기간(일)과 프록시 서버 구성을 정의할 수도 있습니다.

### 사전 요구 사항

- NSX Manager가 연결되어 있고 하이퍼바이저와 동기화할 수 있는지 확인합니다.
- NSX-T Data Center가 데이터 업로드를 위해 공용 네트워크에 연결되어 있는지 확인합니다.

### 절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
- 2 **시스템 > 구성 > 속성**을 선택합니다.

- 3 상태 및 통계 섹션에서 **편집**을 클릭합니다.
- 4 **데이터 수집** 메뉴 항목을 전환합니다.
- 5 [고객 환경 향상 프로그램] 섹션에서 **편집**을 클릭합니다.
- 6 **VMware 고객 환경 향상 프로그램 참여** 메뉴 항목을 전환합니다.
- 7 (선택 사항) 데이터 수집을 구성하고 되풀이 설정을 업로드합니다.
- 8 (선택 사항) **프록시** 탭을 클릭합니다.
- 9 **프록시** 메뉴 항목 전환하여 데이터를 전송하도록 프록시 서버 설정을 구성합니다.

옵션	설명
<b>호스트 이름</b>	프록시 서버 FQDN 또는 IP 주소를 입력합니다.
<b>포트</b>	프록시 서버 포트를 입력합니다.
<b>사용자 이름</b>	(선택 사항) 프록시 서버 인증에 사용되는 사용자 이름을 입력합니다.
<b>암호</b>	(선택 사항) 프록시 서버 인증에 사용되는 암호를 입력합니다.
<b>체계</b>	드롭다운 메뉴에서 프록시 서버가 허용하는 HTTP 또는 HTTPS 체계를 설정합니다.

- 10 **저장**을 클릭합니다.