

NSX-T Data Center 관리 가이드

수정 날짜: 2022년 5월 6일
VMware NSX-T Data Center 2.5

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

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

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

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

Copyright © 2022 VMware, Inc. All rights reserved. 저작권 및 상표 정보

목차

VMware NSX-T Data Center 관리 정보 13

- 1 NSX Manager 개요 14**
- 2 Tier-0 게이트웨이 17**
 - Tier-0 게이트웨이 추가 17
 - IP 접두사 목록 생성 21
 - 커뮤니티 목록 생성 22
 - 정적 경로 구성 23
 - 경로 맵 생성 24
 - 경로 맵을 추가할 때 정규식을 사용하여 커뮤니티 목록과 일치 26
 - BGP 구성 26
 - BFD 구성 30
 - IPv6 계층 3 전달 구성 30
 - IPv6 주소 할당을 위한 SLAAC 및 DAD 프로파일 생성 31
- 3 Tier-1 게이트웨이 33**
 - Tier-1 게이트웨이 추가 33
- 4 세그먼트 36**
 - 세그먼트 프로파일 36
 - QoS 세그먼트 프로파일 이해 37
 - IP 검색 세그먼트 프로파일 이해 39
 - SpoofGuard 세그먼트 프로파일 이해 41
 - 세그먼트 보안 세그먼트 프로파일 이해 43
 - MAC 검색 세그먼트 프로파일 이해 44
 - 세그먼트 추가 46
- 5 VPN(Virtual Private Network) 49**
 - IPSec VPN 이해 50
 - 정책 기반 IPSec VPN 사용 50
 - 경로 기반 IPSec VPN 사용 51
 - 계층 2 VPN 이해 53
 - VPN 서비스 추가 54
 - IPSec VPN 서비스 추가 55
 - L2 VPN 서비스 추가 56

- IPSec VPN 세션 추가 59
 - 정책 기반 IPSec 세션 추가 59
 - 경로 기반 IPSec 세션 추가 62
 - 지원되는 규정 준수 제품군 정보 66
 - TCP MSS 클램핑 이해 67
- L2 VPN 세션 추가 68
 - L2 VPN 서버 세션 추가 68
 - L2 VPN 클라이언트 세션 추가 70
 - 원격 측 L2 VPN 구성 파일 다운로드 71
- 로컬 끝점 추가 72
- 프로파일 추가 74
 - IKE 프로파일 추가 74
 - IPSec 프로파일 추가 77
 - DPD 프로파일 추가 79
- 자치 Edge를 L2 VPN 클라이언트로 추가 80
- IPSec VPN 세션의 인식된 상태 확인 82
- VPN 세션 모니터링 및 문제 해결 85

- 6 네트워크 주소 변환 87**
 - 게이트웨이에서 NAT 구성 87

- 7 로드 밸런싱 89**
 - 키 로드 밸런서 개념 90
 - 로드 밸런서 리소스 크기 조정 90
 - 지원되는 로드 밸런서 기능 91
 - 로드 밸런서 토폴로지 92
 - 로드 밸런서 구성 요소 설정 94
 - 로드 밸런서 추가 94
 - 액티브 모니터 추가 96
 - 패시브 모니터 추가 99
 - 서버 풀 추가 100
 - 가상 서버 구성 요소 설정 104
 - 서버 풀 및 가상 서버에 대해 생성되는 그룹 126

- 8 전달 정책 128**
 - 전달 정책 추가 또는 편집 129

- 9 IPAM(IP 주소 관리) 131**
 - DNS 영역 추가 131
 - DNS 전달자 서비스 추가 132

- DHCP 서버 추가 133
- Tier-0 또는 Tier-1 게이트웨이에 대한 DHCP 릴레이 서버 구성 134
- IP 주소 풀 추가 135
- IP 주소 블록 추가 136

10 보안 137

- 보안 구성 개요 137
- 보안 용어 138
- ID 기반 방화벽 138
 - ID 방화벽 워크플로 139
- 계층 7 컨텍스트 프로필 141
 - 계층 7 방화벽 규칙 워크플로 143
 - 특성 144
- 분산 방화벽 147
 - 방화벽 초안 148
 - 분산 방화벽 추가 150
 - 분산 방화벽 패킷 로그 153
 - 기본 연결 전략 선택 156
 - 방화벽 제외 목록 관리 156
 - 특정 도메인 필터링(FQDN/URL) 157
 - 물리적 워크로드에 대한 보안 정책 확장 158
 - 공유 주소 집합 165
- East-West 네트워크 보안 - 타사 서비스 연결 165
 - 네트워크 보호 East-West의 핵심 개념 165
 - East-West 트래픽에 대한 NSX-T Data Center 요구 사항 166
 - East-West 네트워크 보안에 대한 상위 수준 작업 167
 - East-West 트래픽 검사를 위한 서비스 배포 167
 - 서비스 프로필 추가 169
 - 서비스 체인 추가 169
 - East-West 트래픽에 대한 리디렉션 규칙 추가 170
- 게이트웨이 방화벽 구성 172
 - 게이트웨이 방화벽 정책 및 규칙 추가 173
- 종방향 네트워크 보안 - 타사 서비스 삽입 176
 - 종방향 네트워크 보안에 대한 상위 수준 작업 176
 - North-South 트래픽 검사를 위한 서비스 배포 176
 - 트래픽 리디렉션 구성 178
 - North-South 트래픽에 대한 리디렉션 규칙 추가 179
 - 트래픽 리디렉션 모니터링 180
- 끝점 보호 181
 - 끝점 보호 이해 181

- 끝점 보호 구성 185
- 끝점 보호 관리 200
- 보안 프로파일 212
 - 세션 타이머 생성 212
 - 플러드 보호 214
 - DNS 보안 구성 216
 - 그룹-프로파일 우선 순위 관리 217

11 인벤토리 219

- 서비스 추가 219
- 그룹 추가 220
- 컨텍스트 프로파일 추가 222

12 모니터링 224

- 방화벽 IPFIX 프로파일 추가 224
- 스위치 IPFIX 프로파일 추가 225
- IPFIX 수집기 추가 226
- 포트 미러링 프로파일 추가 227
- SNMP(단순 네트워크 관리 프로토콜) 228
- 시스템 모니터링에 vRealize Log Insight 사용 228
- 시스템 모니터링에 vRealize Operations Manager 사용 229
- 시스템 모니터링에 vRealize Network Insight Cloud 사용 233
- 고급 모니터링 도구 244
 - 포트 연결 정보 보기 244
 - Traceflow 244
 - 포트 미러링 세션 모니터링 247
 - 포트 미러링 세션에 대한 필터 구성 250
 - IPFIX 구성 251
 - 논리적 스위치 포트 활동 모니터링 430

13 논리적 스위치 432

- BUM 프레임 복제 모드 이해 433
- 논리적 스위치 생성 434
- VM을 논리적 스위치에 연결 436
 - vCenter Server에 호스팅된 VM을 NSX-T Data Center 논리적 스위치에 연결 436
 - 독립 실행형 ESXi에 호스팅된 VM을 NSX-T Data Center 논리적 스위치에 연결 438
 - KVM에 호스팅된 VM을 NSX-T Data Center 논리적 스위치에 연결 443
- 논리적 스위치 포트 생성 444
- 계층 2 연결 테스트 445
- NSX Edge 업링크에 대한 VLAN 논리적 스위치 생성 448

- 논리적 스위치 및 논리적 포트에 대한 스위칭 프로파일 450
 - QoS 스위칭 프로파일 이해 451
 - 포트 미러링 스위칭 프로파일 이해 454
 - IP 검색 스위칭 프로파일 이해 456
 - SpoofGuard 이해 458
 - 스위치 보안 스위칭 프로파일 이해 461
 - MAC 관리 스위칭 프로파일 이해 462
 - 사용자 지정 프로파일을 논리적 스위치에 연결 464
 - 사용자 지정 프로파일을 논리적 포트에 연결 465
- 향상된 네트워킹 스택 466
 - ENS 논리적 코어 자동 할당 466
 - 게스트 VLAN 간 라우팅 구성 467
- 계층 2 브리징 469
 - Edge 브리징 프로파일 생성 470
 - Edge 기반 브리징 구성 470
 - 계층 2 브리징 지원 논리적 스위치 생성 473

14 논리적 라우터 476

- Tier-1 논리적 라우터 476
 - Tier-1 논리적 라우터 생성 478
 - Tier-1 논리적 라우터에서 다운링크 포트 추가 479
 - Tier-0 또는 Tier-1 논리적 라우터에 VLAN 포트 추가 480
 - Tier-1 논리적 라우터에서 경로 보급 구성 481
 - Tier-1 논리적 라우터 정적 경로 구성 483
 - 독립형 Tier-1 논리적 라우터 생성 484
- Tier-0 논리적 라우터 486
 - Tier-0 논리적 라우터 생성 487
 - Tier-0과 Tier-1 연결 488
 - NSX Edge 업링크를 위해 VLAN 논리적 스위치에 Tier-0 논리적 라우터 연결 491
 - 루프백 라우터 포트 추가 494
 - Tier-0 또는 Tier-1 논리적 라우터에 VLAN 포트 추가 495
 - 정적 경로 구성 495
 - BGP 구성 옵션 499
 - Tier-0 논리적 라우터에서 BFD 구성 505
 - Tier-0 논리적 라우터에서 경로 재배포 사용 506
 - ECMP 라우팅 이해 509
 - IP 접두사 목록 생성 513
 - 커뮤니티 목록 생성 514
 - 경로 맵 생성 515
 - 전달 타이머 구성 516

15 고급 NAT 517

네트워크 주소 변환 517

Tier-1 NAT 519

Tier-0 NAT 525

재귀 NAT 526

16 고급 그룹 개체 530

IP 집합 생성 530

IP 풀 생성 531

MAC 집합 생성 531

NSGroup 생성 532

서비스 및 서비스 그룹 구성 534

NSService 생성 534

VM용 태그 관리 535

17 고급 DHCP 536

DHCP 536

DHCP 서버 프로파일 생성 536

DHCP 서버 생성 537

DHCP 서버를 논리적 스위치에 연결 538

논리적 스위치에서 DHCP 서버 분리 538

DHCP 릴레이 프로파일 생성 538

DHCP 릴레이 서비스 생성 539

논리적 라우터 포트에 DHCP 릴레이 서비스 추가 539

DHCP 리스 삭제 540

메타데이터 프록시 540

메타데이터 프록시 서버 추가 540

메타데이터 프록시 서버를 논리적 스위치에 연결 541

논리적 스위치에서 메타데이터 프록시 서버 분리 542

18 고급 IP 주소 관리 543

IP 블록 관리 543

IP 블록에 대한 서브넷 관리 544

19 고급 로드 밸런싱 545

키 로드 밸런서 개념 546

로드 밸런서 구성 요소 구성 546

로드 밸런서 생성 547

액티브 상태 모니터 구성 548

- 패시브 상태 모니터 구성 551
- 로드 밸런싱을 위한 서버 풀 추가 552
- 가상 서버 구성 요소 구성 556

20 고급 방화벽 577

- 논리적 라우터에 방화벽 규칙 추가 또는 삭제 577
- 논리 스위치 브리지 포트에 대한 방화벽 구성 578
- 방화벽 섹션 및 방화벽 규칙 578
 - 분산 방화벽 사용 및 사용 안 함 579
 - 방화벽 규칙 섹션 추가 579
 - 방화벽 규칙 섹션 삭제 580
 - 섹션 규칙 사용 및 사용 안 함 581
 - 섹션 로그 사용 및 사용 안 함 581
 - 방화벽 제외 목록 구성 581
- 방화벽 규칙 정보 582
 - 방화벽 규칙 추가 583
 - 방화벽 규칙 삭제 585
 - 기본 분산 방화벽 규칙 편집 585
 - 방화벽 규칙 순서 변경 586
 - 방화벽 규칙 필터링 587

21 작업 및 관리 588

- 모니터링 대시보드 보기 589
- 개체 범주의 사용량 및 용량 보기 591
- 구성 변경의 인식된 상태 확인 592
- 개체 검색 596
- 개체 특성별 필터링 597
- 계산 관리자 추가 598
- Active Directory 추가 600
- LDAP 서버 추가 601
- Active Directory 동기화 602
- 사용자 계정 및 역할 기반 액세스 제어 관리 603
 - 사용자의 암호 관리 603
 - 장치의 암호 재설정 604
 - 인증 정책 설정 606
 - vIDM 호스트에서 인증서 지문 가져오기 607
 - VMware Identity Manager 통합 구성 607
 - VMware Identity Manager 기능 검증 609
 - NSX Manager, vIDM 및 관련 구성 요소 간의 시간 동기화 611
 - 역할 기반 액세스 제어 612

- 역할 할당 또는 주체 ID 추가 620
- NSX Manager 백업 및 복원 622
 - 백업 구성 623
 - 이전 백업 제거 624
 - 사용 가능한 백업 나열 625
 - 백업 복원 626
 - 업그레이드 중 백업 및 복원 628
- vCenter Server에서 NSX-T Data Center 확장 제거 629
- NSX Manager 클러스터 관리 629
 - NSX Manager 클러스터의 상태 및 구성 보기 629
 - NSX Manager 클러스터 종료 및 전원 켜기 632
 - NSX Manager 재부팅 633
 - NSX Manager의 IP 주소 변경 633
 - NSX Manager 노드 크기 조정 635
 - vCenter Server에서 ESXi 호스트 전송 노드 추가 및 제거 635
- NSX Edge 클러스터에서 NSX Edge 전송 노드 교체 636
 - NSX Manager UI를 사용하여 NSX Edge 전송 노드 교체 636
 - API를 사용하여 NSX Edge 전송 노드 교체 637
- vCenter Server가 손실되어 복구할 수 없는 경우 NSX-T 복구 639
- NSX-T Data Center 다중 사이트 배포 640
- 장치 구성 648
- 라이선스 키 추가 및 라이선스 사용량 보고서 생성 649
- 인증서 설정 650
 - 인증서 가져오기 650
 - 인증서 서명 요청 파일 생성 651
 - CA 인증서 가져오기 652
 - 자체 서명된 인증서 생성 653
 - NSX Manager 노드 또는 NSX Manager 클러스터 가상 IP에 대한 인증서 바꾸기 653
 - 인증서 해지 목록 가져오기 654
 - 인증서 해지 목록을 검색하도록 NSX Manager 구성 655
 - CSR 인증서 가져오기 656
 - 공용 인증서 및 개인 키 스토리지 656
- 규정 준수 기반 구성 657
 - 준수 상태 보고서 보기 657
 - 규정 준수 상태 보고서 코드 658
 - 로드 밸런서에 대한 글로벌 FIPS 규정 준수 모드 구성 660
- 지원 번들 수집 663
- 로그 메시지 및 오류 코드 664
 - 원격 로깅 구성 666
 - 로그 메시지 ID 673

- Syslog 문제 해결 674
- 장치 VM에서 직렬 로깅 구성 675
- 고객 환경 향상 프로그램 675
 - 고객 환경 향상 프로그램 구성 편집 676
- 개체에 태그 추가 676
- 원격 서버의 SSH 지문 찾기 678
- VM에서 실행되는 애플리케이션에 대한 데이터 보기 678
- 외부 로드 밸런서 구성 679

22 NSX Cloud 사용 681

- Cloud Service Manager의 빠른 둘러보기 681
 - 클라우드 682
 - 시스템 687
- NSX Cloud 격리 정책을 사용한 위협 감지 689
 - NSX 적용 모드의 격리 정책 690
 - 기본 클라우드 적용 모드의 격리 정책 696
 - VM을 화이트리스트에 추가 696
- NSX 적용 모드 697
 - 현재 워크로드 VM에 대해 지원되는 운영 체제 697
 - NSX 적용 모드에서 VM 온보딩 698
 - NSX 적용 모드에서 VM 관리 707
- 기본 클라우드 적용 모드 708
 - 기본 클라우드 적용 모드에서 VM 관리 708
- NSX Cloud에서 지원되는 NSX-T Data Center 기능 712
 - NSX-T Data Center 및 공용 클라우드 태그를 사용하여 VM 그룹화 713
 - 기본 클라우드 서비스 사용 717
 - 공용 클라우드에 대한 서비스 삽입 718
 - NSX 관리 VM에서 NAT를 사용하도록 설정 725
 - Syslog 전달 사용 725
 - NSX 적용 모드에서 VPN 설정 726
- FAQ(질문과 대답) 730

23 NSX Intelligence 사용 733

- NSX Intelligence 시작 733
 - NSX Intelligence 홈 페이지 둘러보기 733
 - NSX Intelligence 그래픽 요소 사용해 보기 736
- NSX Intelligence 보기 및 흐름 이해 738
 - 그룹 보기 사용 738
 - VM 보기 사용 743
 - 트래픽 흐름 사용 745

NSX Intelligence 권장 사항 사용	747
NSX Intelligence 권장 사항 이해	747
새 NSX Intelligence 권장 사항 생성	748
생성된 권장 사항 검토 및 게시	749
NSX Intelligence 백업 및 복원	751
NSX Intelligence 백업 구성	752
NSX Intelligence 백업	752
NSX Intelligence 백업 복원	753
NSX Intelligence 문제 해결	754
NSX Intelligence 장치의 상태 확인	754
NSX Intelligence 지원 번들 수집	759

VMware NSX-T Data Center 관리 정보

"NSX-T Data Center 관리 가이드"에서는 논리적 스위치 및 포트를 생성하는 방법과 계층화된 논리적 라우터용 네트워킹을 설정하고, NAT, 방화벽, SpoofGuard, 그룹화 및 DHCP를 설정하는 방법을 비롯하여 VMware NSX-T Data Center에 대한 네트워킹을 구성하고 관리하는 방법에 대한 정보를 제공합니다. 또한 NSX Cloud를 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 문서에 사용되는 용어의 정의를 보려면 <https://www.vmware.com/topics/glossary>로 이동하십시오.

NSX Manager 개요

1

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

NSX Manager 웹 인터페이스는 리소스를 구성하는 두 가지 방법을 제공합니다.

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

정책 또는 고급 인터페이스를 사용하는 경우

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

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

표 1-1. 정책 또는 고급 인터페이스를 사용하는 경우

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

표 1-1. 정책 또는 고급 인터페이스를 사용하는 경우 (계속)

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

정책 인터페이스 사용

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

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

정책 인터페이스 및 고급 인터페이스를 찾을 수 있는 위치

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

표 1-2. 정책 인터페이스 및 고급 인터페이스

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

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

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

정책 및 고급 인터페이스에서 생성된 개체의 이름

생성하는 개체는 해당 개체를 생성하는 데 사용된 인터페이스에 따라 달라집니다.

표 1-3. 개체 이름

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

Tier-0 게이트웨이

2

Tier-0 게이트웨이는 Tier-0 논리적 라우터의 기능을 수행합니다. 논리적 네트워크와 물리적 네트워크 사이의 트래픽을 처리합니다.

NSX Cloud 참고 NSX Cloud를 사용하는 경우 NSX Cloud에서 지원되는 NSX-T Data Center 기능에서 자동 생성된 논리적 엔티티, 지원되는 기능 및 NSX Cloud에 필요한 구성 목록을 확인하십시오.

Edge 노드는 하나의 Tier-0 게이트웨이 또는 논리적 라우터만 지원할 수 있습니다. Tier-0 게이트웨이 또는 논리적 라우터를 생성할 때 NSX Edge 클러스터에 Edge 노드 수보다 더 많은 Tier-0 게이트웨이 또는 논리적 라우터를 생성하지 않아야 합니다.

참고 고급 네트워킹 및 보안 탭에서 Tier-0 논리적 라우터 용어는 Tier-0 게이트웨이를 나타내는 데 사용됩니다.

본 장은 다음 항목을 포함합니다.

- Tier-0 게이트웨이 추가
- IP 접두사 목록 생성
- 커뮤니티 목록 생성
- 정적 경로 구성
- 경로 맵 생성
- 경로 맵을 추가할 때 정규식을 사용하여 커뮤니티 목록과 일치
- BGP 구성
- BFD 구성
- IPv6 계층 3 전달 구성
- IPv6 주소 할당을 위한 SLAAC 및 DAD 프로파일 생성

Tier-0 게이트웨이 추가

Tier-0 게이트웨이에는 Tier-1 게이트웨이에 대한 다운링크 연결과 물리적 네트워크에 대한 업링크 연결이 있습니다.

Tier-0 게이트웨이의 HA(고가용성) 모드를 액티브-액티브 또는 액티브-대기 상태로 구성할 수 있습니다. 다음 서비스는 액티브-대기 모드에서만 지원됩니다.

- NAT
- 로드 밸런싱
- 상태 저장 방화벽
- VPN

Tier-0 및 Tier-1 게이트웨이는 단일 계층 및 다중 계층 토폴로지의 모든 인터페이스(업링크, 서비스 포트 및 다운링크)에 다음과 같은 주소 지정 구성을 지원합니다.

- IPv4 전용
- IPv6 전용
- 이중 스택 - IPv4 및 IPv6 둘 다

IPv6 또는 이중 스택 주소 지정을 사용하려면 **네트워킹 > 네트워킹 설정 > 글로벌 네트워킹 구성**에서 L3 전달 모드로 **IPv4 및 IPv6**를 사용하도록 설정합니다.

Tier-0 게이트웨이에 대한 경로 재배포를 구성하는 경우 두 개의 소스 그룹인 Tier-0 서브넷 및 보급된 Tier-1 서브넷 중에서 선택할 수 있습니다. Tier-0 서브넷 그룹의 소스는 다음과 같습니다.

소스 유형	설명
연결된 인터페이스 및 세그먼트	여기에는 외부 인터페이스 서브넷, 서비스 인터페이스 서브넷 및 Tier-0 게이트웨이에 연결된 세그먼트 서브넷이 포함됩니다.
정적 경로	Tier-0 게이트웨이에 구성된 정적 경로입니다.
NAT IP	Tier-0 게이트웨이에서 소유하고 Tier-0 게이트웨이에 구성된 NAT 규칙에서 검색되는 NAT IP 주소입니다.
IPSec 로컬 IP	VPN 세션을 설정하기 위한 로컬 IPSEC 끝점 IP 주소입니다.
DNS 전달자 IP	클라이언트의 DNS 쿼리에 대한 수신기 IP로, DNS 쿼리를 업스트림 DNS 서버로 전달하는 데 사용되는 소스 IP로도 사용됩니다.

보급된 Tier-1 서브넷 그룹의 소스는 다음과 같습니다.

소스 유형	설명
연결된 인터페이스 및 세그먼트	여기에는 Tier-1 게이트웨이에 연결된 세그먼트 서브넷과 Tier-1 게이트웨이에 구성된 서비스 인터페이스 서브넷이 포함됩니다.
정적 경로	Tier-1 게이트웨이에 구성된 정적 경로입니다.
NAT IP	Tier-1 게이트웨이에서 소유하고 Tier-1 게이트웨이에 구성된 NAT 규칙에서 검색되는 NAT IP 주소입니다.
LB VIP	로드 밸런싱 가상 서버의 IP 주소입니다.
LB SNAT IP	로드 밸런서가 소스 NAT에 사용하는 IP 주소 또는 IP 주소 범위입니다.

소스 유형	설명
DNS 전달자 IP	클라이언트의 DNS 쿼리에 대한 수신기 IP로, DNS 쿼리를 업스트림 DNS 서버로 전달하는 데 사용되는 소스 IP로도 사용됩니다.
IPSec 로컬 끝점	IPSec 로컬 끝점의 IP 주소입니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > Tier-0 게이트웨이**를 선택합니다.
- 3 **Tier-0 게이트웨이 추가**를 클릭합니다.
- 4 게이트웨이의 이름을 입력합니다.
- 5 HA(고가용성) 모드를 선택합니다.

기본 모드는 액티브-액티브입니다. 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.

중요 게이트웨이를 생성한 후에는 HA 모드를 변경할 수 없습니다.

- 6 HA 모드가 액티브-대기인 경우 페일오버 모드를 선택합니다.

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

- 7 (선택 사항) NSX Edge 클러스터를 선택합니다.
- 8 (선택 사항) 하나 이상의 태그를 추가합니다.

9 (선택 사항) 추가 설정을 클릭합니다.

a 내부 전송 서브넷 필드에 서브넷을 입력합니다.

이러한 서브넷은 이 게이트웨이 내 구성 요소 간 통신에 사용됩니다. 기본값은 169.254.0.0/28입니다.

b TO-T1 전송 서브넷 필드에 하나 이상의 서브넷을 입력합니다.

이러한 서브넷은 이 게이트웨이 및 연결된 모든 Tier-1 게이트웨이 간 통신에 사용됩니다. 이 게이트웨이를 생성하고 Tier-1 게이트웨이에 연결하면 Tier-O 게이트웨이 측 및 Tier-1 게이트웨이 측의 링크에 할당된 실제 IP 주소가 표시됩니다. 이 주소는 Tier-O 게이트웨이 페이지 및 Tier-1 게이트웨이 페이지의 **추가 설정 > 라우터 링크**에 표시됩니다. 기본값은 100.64.0.0/16입니다.

c IPv6 주소 구성에 대해 ND 프로파일 및 DAD 프로파일을 선택합니다.

이러한 프로파일은 IPv6 주소에 대한 SLAAC(상태 비저장 주소 자동 구성) 및 DAD(중복 주소 감지)를 구성하는 데 사용됩니다. 기본 프로파일이 생성됩니다.

10 저장을 클릭합니다.

11 경로 재배포를 구성하려면 경로 재배포와 설정을 클릭합니다.

하나 이상의 소스를 선택합니다.

- Tier-O 서브넷: 정적 경로, NAT IP, IPSec 로컬 IP, DNS 전달자 IP, 연결된 인터페이스 및 세그먼트.

연결된 인터페이스 및 세그먼트에서 서비스 인터페이스 서브넷, 외부 인터페이스 서브넷, 루프백 인터페이스 서브넷, 연결된 세그먼트 중 하나 이상을 선택할 수 있습니다.

- 보급된 Tier-1 서브넷: DNS 전달자 IP, 정적 경로, LB VIP, NAT IP, LB SNAT IP, IPSec 로컬 끝점, 연결된 인터페이스 및 세그먼트.

연결된 인터페이스 및 세그먼트에서 서비스 인터페이스 서브넷 및/또는 연결된 세그먼트를 선택할 수 있습니다.

12 인터페이스를 구성하려면 인터페이스와 설정을 클릭합니다.

a 인터페이스 추가를 클릭합니다.

b 이름을 입력합니다.

c 유형을 선택합니다.

HA 모드가 액티브-대기인 경우 선택 항목은 외부, 서비스 및 루프백입니다. HA 모드가 액티브-액티브인 경우 선택 항목은 외부 및 루프백입니다.

d IP 주소를 CIDR 형식으로 입력합니다.

e 세그먼트를 선택합니다.

f 인터페이스 유형이 서비스가 아닌 경우 NSX Edge 노드를 선택합니다.

- g (선택 사항) 인터페이스 유형이 **루프백**이 아닌 경우 MTU 값을 입력합니다.
 - h (선택 사항) 태그를 추가하고 ND 프로파일을 선택합니다.
- 13 (선택 사항) HA 모드가 액티브-대기인 경우 HA VIP 구성 옆에 있는 설정을 클릭하여 HA VIP를 구성합니다.**
- HA VIP를 구성하면 하나의 업링크가 종료된 경우에도 Tier-0 게이트웨이가 작동합니다. 물리적 라우터는 HA VIP하고만 상호 작용합니다. HA VIP는 BGP가 아닌 고정 라우팅에서 작동하기 위한 것입니다.
- a **HA VIP 구성 추가**를 클릭합니다.
 - b IP 주소와 서브넷 마스크를 입력합니다.
HA VIP 서브넷은 바인딩된 인터페이스의 서브넷과 동일해야 합니다.
 - c 두 개의 서로 다른 Edge 노드에서 두 개의 인터페이스를 선택합니다.
- 14 라우팅**을 클릭하여 IP 접두사 목록, 커뮤니티 목록, 정적 경로 및 경로 맵을 추가합니다.
- 15 BGP**를 클릭하여 BGP를 구성합니다.
- 16 고급 구성**을 클릭하여 **고급 네트워킹 및 보안 > 라우터** 페이지로 이동하고 추가 구성을 수행합니다.
- a 계층 3 전달 모드를 구성하려면 **글로벌 구성** 탭을 클릭합니다.
 - b **편집**을 클릭합니다.
 - c **IPv4** 또는 **IPv4 및 IPv6**를 선택하십시오.
기본값은 IPv4 전용입니다. IPv6 전용은 지원되지 않습니다. IPv6을 사용하도록 설정하려면 **IPv4 및 IPv6**을 선택합니다.
 - d **저장**을 클릭합니다.

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 게이트웨이가 구성되어 있는지 확인합니다. Tier-0 논리적 라우터 생성의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > Tier-0 게이트웨이**를 선택합니다.
- 3 Tier-0 게이트웨이를 편집하려면 메뉴 아이콘(3개의 점)을 클릭하고 **편집**을 선택합니다.
- 4 **라우팅**을 클릭합니다.
- 5 **IP 접두사 목록** 옆에 있는 **설정**을 클릭합니다.
- 6 **IP 접두사 목록 추가**를 클릭합니다.
- 7 IP 접두사 목록의 이름을 입력합니다.
- 8 **설정**을 클릭하여 IP 접두사를 추가합니다.
- 9 **접두사 추가**를 클릭합니다.
 - a IP 주소를 CIDR 형식으로 입력합니다.
예: 192.168.100.3/27
 - b (선택 사항) **le** 또는 **ge** 수정자로 IP 주소 번호의 범위를 설정합니다.
예를 들어 **le**를 30으로, **ge**를 24로 설정합니다.
 - c 드롭다운 메뉴에서 **거부** 또는 **허용**을 선택합니다.
 - d **추가**를 클릭합니다.
- 10 접두사를 추가로 지정하려면 이전 단계를 반복합니다.
- 11 **저장**을 클릭합니다.

커뮤니티 목록 생성

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

커뮤니티 목록은 커뮤니티 특성 값의 사용자 정의 목록입니다. 이러한 목록은 BGP 업데이트 메시지의 커뮤니티 특성을 일치 또는 조작하는 데 사용할 수 있습니다.

BGP 커뮤니티 특성(RFC 1997) 및 BGP 대규모 커뮤니티 특성(RFC 8092)이 모두 지원됩니다. BGP 커뮤니티 특성은 2개의 16비트 값으로 분할되는 32비트 값입니다. BGP 대규모 커뮤니티 특성에는 3개의 구성 요소가 있으며 길이는 각각 4개의 옥텟입니다.

경로 맵에서 BGP 커뮤니티 또는 대규모 커뮤니티 특성을 일치 또는 설정할 수 있습니다. 이 기능을 사용하여 네트워크 운영자는 BGP 커뮤니티 특성을 기반으로 네트워크 정책을 구현할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > Tier-0 게이트웨이**를 선택합니다.
- 3 Tier-0 게이트웨이를 편집하려면 메뉴 아이콘(3개의 점)을 클릭하고 **편집**을 선택합니다.
- 4 **라우팅**을 클릭합니다.
- 5 **커뮤니티 목록** 옆의 **설정**을 클릭합니다.
- 6 **커뮤니티 목록 추가**를 클릭합니다.
- 7 커뮤니티 목록의 이름을 입력합니다.
- 8 커뮤니티 목록을 지정합니다. aa:nn 형식을 사용하여 일반 커뮤니티를 지정합니다(예: 300:500). 대규모 커뮤니티의 경우 aa:bb:cc 형식(예: 11:22:33)을 사용합니다. 목록에 일반 커뮤니티와 대규모 커뮤니티를 둘 다 포함할 수는 없습니다. 일반 커뮤니티 또는 대규모 커뮤니티 중 하나만 포함해야 합니다.
또한 다음 중 하나 이상의 일반 커뮤니티를 선택할 수 있습니다. 목록에 대규모 커뮤니티가 포함된 경우에는 추가할 수 없습니다.
 - NO_EXPORT_SUBCONFED - EBGp 피어로 보급하지 마십시오.
 - NO_ADVERTISE - 어떤 피어로도 보급하지 마십시오.
 - NO_EXPORT - BGP 연합 외부로 보급하지 마십시오.
- 9 **저장**을 클릭합니다.

정적 경로 구성

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

재귀 정적 경로가 지원됩니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > Tier-0 게이트웨이**를 선택합니다.
- 3 Tier-0 게이트웨이를 편집하려면 메뉴 아이콘(3개의 점)을 클릭하고 **편집**을 선택합니다.
- 4 **라우팅**을 클릭합니다.
- 5 **정적 경로** 옆의 **설정**을 클릭합니다.
- 6 **정적 경로 추가**를 클릭합니다.

- 7 이름 및 네트워크 주소를 CIDR 형식으로 입력합니다. IPv6 기반의 정적 경로가 지원됩니다. IPv6 접두사에는 IPv6 다음 홉만 포함될 수 있습니다.
- 8 **다음 홉 설정**을 클릭하여 다음 홉 정보를 추가합니다.
- 9 **다음 홉 추가**를 클릭합니다.
- 10 IP 주소를 입력합니다.
- 11 관리 거리를 지정합니다.
- 12 드롭다운 목록에서 인터페이스를 선택합니다.
- 13 **추가** 버튼을 클릭합니다.

다음에 수행할 작업

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

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.

사전 요구 사항

- IP 접두사 목록 또는 커뮤니티 목록이 구성되어 있는지 확인합니다. [IP 접두사 목록 생성 또는 커뮤니티 목록 생성](#)을 참조하십시오.
- 정규식을 사용하여 커뮤니티 목록의 경로 맵 일치 기준을 정의하는 방법에 대한 자세한 내용은 [경로 맵을 추가할 때 정규식을 사용하여 커뮤니티 목록과 일치를 참조하십시오](#).

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > Tier-0 게이트웨이**를 선택합니다.
- 3 Tier-0 게이트웨이를 편집하려면 메뉴 아이콘(3개의 점)을 클릭하고 **편집**을 선택합니다.
- 4 **라우팅**을 클릭합니다.
- 5 **경로 맵 옆의 설정**을 클릭합니다.
- 6 **경로 맵 추가**를 클릭합니다.
- 7 이름을 입력하고 **설정**을 클릭하여 일치 조건을 추가합니다.
- 8 **일치 조건 추가**를 클릭하여 일치 조건을 하나 이상 추가합니다.

9 각 조건에 대해 **IP 접두사** 또는 **커뮤니티 목록**을 선택하고 **설정**을 클릭하여 일치하는 식을 하나 이상 지정합니다.

a **커뮤니티 목록**을 선택한 경우 커뮤니티 목록의 멤버를 일치시킬 방법을 정의하는 일치 식을 지정합니다. 각 커뮤니티 목록에 대해 다음과 같은 일치 옵션을 사용할 수 있습니다.

- **임의 항목 일치** - 커뮤니티 목록의 커뮤니티가 하나라도 일치하는 경우 경로 맵에서 설정한 작업을 수행합니다.
- **모든 항목 일치** - 커뮤니티 목록의 모든 커뮤니티가 순서에 관계없이 일치하는 경우 경로 맵에서 설정한 작업을 수행합니다.
- **정확한 일치** - 커뮤니티 목록의 모든 커뮤니티가 정확히 동일한 순서대로 일치하는 경우 경로 맵에서 설정한 작업을 수행합니다.
- **커뮤니티 정규식 일치** - NRLI에 연결된 모든 일반 커뮤니티가 정규식과 일치하는 경우 경로 맵에서 설정한 작업을 수행합니다.
- **대규모 커뮤니티 정규식 일치** - NRLI에 연결된 모든 대규모 커뮤니티가 정규식과 일치하는 경우 경로 맵에서 설정한 작업을 수행합니다.

일치 조건 `MATCH_COMMUNITY_REGEX`를 사용하여 표준 커뮤니티에 대한 경로를 일치시키고, 일치 조건 `MATCH_LARGE_COMMUNITY_REGEX`를 사용하여 대규모 커뮤니티에 대한 경로를 일치시켜야 합니다. 표준 커뮤니티 또는 대규모 커뮤니티 값이 포함된 경로를 허용하려면 다음과 같은 두 가지 일치 조건을 생성해야 합니다. 동일한 일치 조건의 일치 표현식이 지정된 경우 표준 및 대규모 커뮤니티를 둘 다 포함하는 경로만 허용됩니다.

임의 일치 조건의 경우 일치 표현식이 **AND** 작업에 적용되므로 일치가 발생하려면 일치하는 모든 표현식이 충족되어야 합니다. 일치 조건이 여러 개 있는 경우 **OR** 작업에 적용되므로 일치 조건 중 하나라도 충족하면 일치가 발생합니다.

10 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.
가중치	가중치를 설정하여 경로 선택에 영향을 줍니다. 범위는 0 - 65535입니다.
커뮤니티	커뮤니티 목록을 지정합니다. <code>aa:nn</code> 형식을 사용하여 일반 커뮤니티를 지정합니다(예: <code>300:500</code>). 대규모 커뮤니티의 경우 <code>aa:bb:cc</code> 형식(예: <code>11:22:33</code>)을 사용합니다. 또는 드롭다운 메뉴를 사용하여 다음 중 하나를 선택합니다. <ul style="list-style-type: none"> ■ <code>NO_EXPORT_SUBCONFED</code> - EBGp 피어로 보급하지 마십시오. ■ <code>NO_ADVERTISE</code> - 어떤 피어로도 보급하지 마십시오. ■ <code>NO_EXPORT</code> - BGP 연합 외부로 보급하지 마십시오.
로컬 기본 설정	아웃바운드 외부 BGP 경로를 선택하려면 이 값을 사용합니다. 가장 높은 값이 있는 경로가 선호됩니다.

11 [작업] 열에서 **허용** 또는 **거부**를 선택합니다.

IP 접두사 목록 또는 커뮤니티 목록과 일치하는 IP 주소의 보급을 허용하거나 거부할 수 있습니다.

12 **저장**을 클릭합니다.

경로 맵을 추가할 때 정규식을 사용하여 커뮤니티 목록과 일치

정규식을 사용하여 커뮤니티 목록에 대한 경로 맵 일치 조건을 정의할 수 있습니다. BGP 정규식은 POSIX 1003.2 정규식을 기준으로 합니다.

다음 표현식은 POSIX 정규식의 하위 집합입니다.

표현식	설명
.	임의의 단일 문자를 일치시킵니다.
*	0개 이상의 패턴 발생을 일치시킵니다.
+	1개 이상의 패턴 발생을 일치시킵니다.
?	0개 또는 1개의 패턴 발생을 일치시킵니다.
^	줄 맨 처음을 일치시킵니다.
\$	줄의 맨 끝을 일치시킵니다.
-	이 문자는 BGP 정규식에서 특별한 의미가 있습니다. 이 값은 공백, 쉼표, AS 설정 구분 기호 { 및 }, AS 통합 구분 기호 (및)에 일치됩니다. 줄의 시작과 끝에도 일치됩니다. 따라서 이 문자는 AS 경계 일치에 사용할 수 있습니다. 이 문자는 기술적으로 (^ [{}()]\$)로 평가됩니다.

다음은 경로 맵에서 정규식을 사용하기 위한 몇 가지 예입니다.

표현식	설명
^101	101로 시작하는 커뮤니티 특성이 있는 경로를 일치시킵니다.
^[0-9]+	0-9 사이의 숫자로 시작하며 이러한 숫자의 인스턴스를 하나 이상 포함하는 커뮤니티 특성이 있는 경로를 일치시킵니다.
.	커뮤니티 특성이 있거나 없는 경로를 일치시킵니다.
+	커뮤니티 값이 있는 경로를 일치시킵니다.
^\$	커뮤니티 값이 없거나 Null인 경로를 일치시킵니다.

BGP 구성

VM과 외부 환경 간에 액세스를 사용하도록 설정하려면 Tier-0 게이트웨이와 물리적 인프라의 라우터 간에 eBGP 또는 iBGP(외부 또는 내부 BGP) 연결을 구성하면 됩니다.

BGP를 구성할 때 Tier-0 게이트웨이에 대해 로컬 AS(자치 시스템) 번호를 구성해야 합니다. 또한 원격 AS 번호도 구성해야 합니다. EBGP 인접 네트워크는 직접 연결되어야 하고 Tier-0 업링크와 동일한 서브넷에 있어야 합니다. 동일한 서브넷에 있지 않으면 BGP 다중 홉을 사용해야 합니다.

BGPv6은 단일 홉 및 다중 홉에 대해 지원됩니다. BGPv6 인접 항목은 IPv6 주소만 지원합니다. 재배포, 접두사 목록 및 경로 맵은 IPv6 접두사에서 지원됩니다.

액티브-액티브 모드의 Tier-0 게이트웨이는 SR(서비스 라우터) 간 iBGP를 지원합니다. 게이트웨이 #1이 노스바운드 물리적 라우터와 통신할 수 없는 경우 트래픽은 액티브-액티브 클러스터의 게이트웨이 #2로 다시 라우팅됩니다. 게이트웨이 #2가 물리적 라우터와 통신할 수 없는 경우 게이트웨이 #1과 물리적 라우터 간 트래픽은 영향을 받지 않습니다.

NSX Edge의 ECMP 구현은 프로토콜 번호의 5-튜플, 소스 및 대상 주소, 소스 및 대상 포트를 기준으로 합니다.

iBGP 기능에는 다음과 같은 기능 및 제한 사항이 있습니다.

- 재배포, 접두사 목록 및 경로 맵이 지원됩니다.
- 경로 리플렉터가 지원되지 않습니다.
- BGP 연합이 지원되지 않습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > Tier-0 게이트웨이**를 선택합니다.
- 3 Tier-0 게이트웨이를 편집하려면 메뉴 아이콘(3개의 점)을 클릭하고 **편집**을 선택합니다.
- 4 **BGP**를 클릭합니다.
 - a 로컬 AS 번호를 입력합니다.

액티브-액티브 모드에서는 기본 ASN 값 65000이 이미 채워져 있습니다. 액티브-대기 모드에는 기본 ASN 값이 없습니다.
 - b **BGP** 토글 버튼을 클릭하여 BGP를 사용하거나 사용하지 않도록 설정합니다.

액티브-액티브 모드에서는 **BGP**가 기본적으로 사용하도록 설정됩니다. 액티브-대기 모드에서는 **BGP**가 기본적으로 사용하지 않도록 설정됩니다.
 - c 게이트웨이가 액티브-액티브 모드인 경우 **SR 간 iBGP** 토글 버튼을 클릭하여 SR 간 iBGP를 사용하거나 사용하지 않도록 설정합니다. 기본적으로 사용하도록 설정됩니다.

게이트웨이가 액티브-대기 모드에 있는 경우에는 이 기능을 사용할 수 없습니다.
 - d **ECMP** 토글 버튼을 클릭하여 ECMP를 사용하거나 사용하지 않도록 설정합니다.

- e **다중 경로 완화** 토글 버튼을 클릭하여 AS-path 특성 값만 다르게 AS-path 길이는 동일한 다중 경로에서 로드 공유를 사용하거나 사용하지 않도록 설정합니다.

참고 다중 경로 완화가 작동하려면 ECMP를 사용하도록 설정해야 합니다.

- f **정상 다시 시작** 필드에서 **사용 안 함**, **도우미만** 또는 **정상 다시 시작 및 도우미**를 선택합니다.

필요한 경우 **정상 다시 시작 타이머** 및 **정상 다시 시작 부실 타이머**를 변경할 수 있습니다.

기본적으로 정상 다시 시작 모드는 **도우미만**으로 설정됩니다. 도우미 모드는 정상 다시 시작이 가능한 인접 항목 환경에서 학습된 경로에 연결된 트래픽의 중단을 해소 및/또는 줄이는 데 유용합니다. 인접 항목은 다시 시작되는 동안 자신의 전달 테이블을 보존할 수 있어야 합니다.

모든 게이트웨이의 BGP 피어링이 항상 액티브 상태이기 때문에 정상 다시 시작 기능을 Tier-0 게이트웨이에서는 사용하도록 설정하지 않는 것이 좋습니다. 페일오버 시, 정상 다시 시작 기능은 원격 인접 항목에서 대체 Tier-0 게이트웨이를 선택하는 데 소요되는 시간을 늘립니다. 이로 인해 BFD 기반 컨버전스가 지연됩니다.

참고: 인접 항목 관련 구성에 의해 재정의되지 않는 한, Tier-0 구성은 모든 BGP 인접 항목에 적용됩니다.

- 5 IP 주소 접두사를 추가하여 **경로 집계**를 구성합니다.

- a **접두사 추가**를 클릭합니다.
- b IP 주소 접두사를 CIDR 형식으로 입력합니다.
- c **요약만** 옵션에 대해 **예** 또는 **아니요**를 선택합니다.

- 6 **저장**을 클릭합니다.

BGP 인접 네트워크를 구성하려면 먼저 글로벌 BGP 구성을 저장해야 합니다.

- 7 **BGP 인접 항목**을 구성합니다.

- a 인접 항목의 IP 주소를 입력합니다.
- b **BFD**를 사용하거나 사용하지 않도록 설정합니다.
- c **원격 AS 번호** 값을 입력합니다.

iBGP의 경우 4a단계에 있는 AS 번호와 동일한 숫자를 입력합니다. eBGP의 경우에는 물리적 라우터의 AS 번호를 입력합니다.

- d **송신 필터**를 구성합니다.
- e **수신 필터**를 구성합니다.
- f **Allowas-in** 기능을 사용하거나 사용하지 않도록 설정합니다.

이 기능은 기본적으로 사용하지 않도록 설정됩니다. 이 기능을 사용하도록 설정하는 경우 BGP 인접 항목은 예를 들어 동일한 서비스 제공자를 사용하여 서로 연결된 두 위치가 있을 때 동일한 AS를 가진 경로를 수신할 수 있습니다. 이 기능은 모든 주소 패밀리에 적용되며 특정 주소 패밀리에만 적용할 수는 없습니다.

- g **소스 주소** 필드에서 소스 주소를 선택하여 이 특정 소스 주소를 사용하는 인접 라우터와의 피어링 세션을 설정할 수 있습니다. 아무것도 선택하지 않으면 게이트웨이가 자동으로 하나를 선택합니다.
- h **IP 주소 패밀리** 필드에서 **IPv4**, **IPv6** 또는 **사용 안 함**을 선택합니다.
- i **최대 홉 제한** 값을 입력합니다.
- j **정상 다시 시작** 필드에서 필요에 따라 **사용 안 함**, **도우미만** 또는 **정상 다시 시작 및 도우미**를 선택할 수 있습니다.

옵션	설명
선택한 항목 없음	이 인접 항목에 대한 정상 다시 시작은 Tier-0 게이트웨이 BGP 구성을 따릅니다.
사용 안 함	<ul style="list-style-type: none"> ■ Tier-0 게이트웨이 BGP가 사용 안 함으로 구성되면 이 인접 항목에 대해 정상 다시 시작이 사용되지 않도록 설정됩니다. ■ Tier-0 게이트웨이 BGP가 도우미만으로 구성되면 이 인접 항목에 대해 정상 다시 시작이 사용되지 않도록 설정됩니다. ■ Tier-0 게이트웨이 BGP가 정상 다시 시작 및 도우미로 구성되면 이 인접 항목에 대해 정상 다시 시작이 사용되지 않도록 설정됩니다.
도우미만	<ul style="list-style-type: none"> ■ Tier-0 게이트웨이 BGP가 사용 안 함으로 구성되면 이 인접 항목에 대해 정상 다시 시작이 도우미만으로 구성됩니다. ■ Tier-0 게이트웨이 BGP가 도우미만으로 구성되면 이 인접 항목에 대해 정상 다시 시작이 도우미만으로 구성됩니다. ■ Tier-0 게이트웨이 BGP가 정상 다시 시작 및 도우미로 구성되면 이 인접 항목에 대해 정상 다시 시작이 도우미만으로 구성됩니다.
정상 다시 시작 및 도우미	<ul style="list-style-type: none"> ■ Tier-0 게이트웨이 BGP가 사용 안 함으로 구성되면 이 인접 항목에 대해 정상 다시 시작이 정상 다시 시작 및 도우미로 구성됩니다. ■ Tier-0 게이트웨이 BGP가 도우미만으로 구성되면 이 인접 항목에 대해 정상 다시 시작이 정상 다시 시작 및 도우미로 구성됩니다. ■ Tier-0 게이트웨이 BGP가 정상 다시 시작 및 도우미로 구성되면 이 인접 항목에 대해 정상 다시 시작이 정상 다시 시작 및 도우미로 구성됩니다.

- k **타이머 및 암호**를 클릭합니다.
- l **BFD 간격** 값을 입력합니다.
단위는 밀리초입니다. VM에서 실행되는 Edge 노드의 경우 최소값은 1000입니다. 베어메탈 Edge 노드의 경우 최소값은 300입니다.
- m **BFD 승수** 값을 입력합니다.
- n **보류 시간** 값을 입력합니다.
- o **연결 유지 시간** 값을 입력합니다.
- p 암호를 입력합니다.
이것은 BGP 피어 간 MD5 인증을 구성하는 경우 필수입니다.

8 **저장**을 클릭합니다.

BFD 구성

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

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > Tier-0 게이트웨이**를 선택합니다.
- 3 Tier-0 게이트웨이를 편집하려면 메뉴 아이콘(3개의 점)을 클릭하고 **편집**을 선택합니다.
- 4 **고급 구성**을 클릭합니다.

이 경우 **고급 네트워킹 및 보안 > 라우터** 페이지로 이동됩니다. 게이트웨이는 논리적 라우터 중 하나로 표시됩니다. Tier-0 논리적 라우터에서 BFD 구성의 지침을 따르십시오.

IPv6 계층 3 전달 구성

IPv4 계층 3 전달은 기본적으로 사용하도록 설정됩니다. 또한 IPv6 계층 3 전달을 구성할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > Tier-0 게이트웨이**를 선택합니다.
- 3 메뉴 아이콘(3개의 점)을 클릭하고 **편집**을 선택하여 Tier-0 게이트웨이를 편집합니다.
- 4 **고급 구성**을 클릭합니다.

이 경우 **고급 네트워킹 및 보안 > 라우터** 페이지로 이동됩니다. 게이트웨이는 논리적 라우터 중 하나로 표시됩니다.

- 5 **글로벌 구성** 탭을 클릭합니다.
- 6 **L3 전달 모드** 필드에서 **IPv4 및 IPv6**을 선택합니다.
IPv6 전용은 지원되지 않습니다.
- 7 **네트워킹** 탭으로 이동하여 게이트웨이를 다시 편집합니다.
- 8 **추가 설정**으로 이동합니다.
 - a **내부 전송 서브넷**에 대한 구성 가능한 IPv6 주소가 없습니다. 시스템은 자동으로 IPv6 링크 로컬 주소를 사용합니다.
 - b **T0-T1 전송 서브넷**에 대한 IPv6 서브넷을 입력하십시오.
- 9 **인터페이스**로 이동하고 IPv6에 대한 인터페이스를 추가하십시오.

IPv6 주소 할당을 위한 SLAAC 및 DAD 프로파일 생성

논리적 라우터 인터페이스에서 IPv6을 사용하는 경우 IP 주소 할당에 대해 SLAAC(상태 비저장 주소 자동 구성)을 설정할 수 있습니다. SLAAC를 사용하면 라우터 보급을 통해 로컬 네트워크 라우터에서 보급된 네트워크 접두사를 기준으로 호스트의 주소를 지정할 수 있습니다. DAD(중복 주소 감지)는 IP 주소의 고유성을 보장합니다.

사전 요구 사항

고급 네트워킹 및 보안 > 라우터 > 글로벌 구성으로 이동한 후 **L3 전달 모드**로 **IPv4** 및 **IPv6**을 선택합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > Tier-0 게이트웨이**를 선택합니다.
- 3 Tier-0 게이트웨이를 편집하려면 메뉴 아이콘(3개의 점)을 클릭하고 **편집**을 선택합니다.
- 4 **추가 설정**을 클릭합니다.
- 5 **ND 프로파일(SLAAC 프로파일)**을 생성하려면 메뉴 아이콘(점 3개)을 클릭하고 **새로 생성**을 선택합니다.
 - a 프로파일의 이름을 입력합니다.
 - b 다음과 같이 모드를 선택합니다.
 - **사용 안 함** - 라우터 보급 메시지가 사용되지 않도록 설정되었습니다.
 - **RA를 통한 SLAAC(DNS 포함)** - 주소 및 DNS 정보가 라우터 보급 메시지로 생성됩니다.
 - **DHCP를 통한 SLAAC(DNS 포함)** - 주소가 라우터 보급 메시지로 생성되고 DNS 정보가 DHCP 서버에 의해 생성됩니다.
 - **DHCP를 통한 DHCP(주소 및 DNS 포함)** - 주소 및 DNS 정보가 DHCP 서버에서 생성됩니다.
 - **DHCP를 통한 SLAAC(주소 및 DNS 포함)** - 주소 및 DNS 정보가 DHCP 서버에서 생성됩니다. 이 옵션은 KVM 호스트 또는 ESXi 호스트가 아닌 NSX Edge에서만 지원됩니다.
 - c 라우터 보급 메시지에 대해 연결할 수 있는 시간 및 재전송 간격을 입력합니다.
 - d 도메인 이름을 입력하고 도메인 이름의 수명을 지정합니다. **RA를 통한 SLAAC (DNS 포함)** 모드에 대해서만 이러한 값을 입력하십시오.

- e DNS 서버를 입력하고 DNS 서버의 수명을 지정합니다. **RA를 통한 SLAAC (DNS 포함)** 모드에 대해서만 이러한 값을 입력하십시오.
 - f 라우터 보급에 대해 다음 값을 입력합니다.
 - **RA 간격** - 연속되는 라우터 보급 메시지 전송 사이의 시간 간격입니다.
 - **홉 제한** - 보급 경로의 수명입니다.
 - **라우터 수명** - 라우터의 수명입니다.
 - **접두사 수명** - 접두사의 수명(초)입니다.
 - **접두사 기본 설정 시간** - 유효한 주소가 기본 설정된 시간입니다.
- 6 DAD 프로파일을 생성하려면 메뉴 아이콘(점 3개)을 클릭하고 새로 만들기를 선택합니다.**
- a 프로파일의 이름을 입력합니다.
 - b 다음과 같이 모드를 선택합니다.
 - **소프트** - 중복된 주소 알림이 수신되지만 중복된 주소가 감지될 때 아무 작업도 수행되지 않습니다.
 - **엄격** - 중복된 주소 알림이 수신되고 중복된 주소는 더 이상 사용되지 않습니다.
 - c NS 패킷 간의 시간 간격을 지정하는 **대기 시간(초)**을 입력합니다.
 - d **대기 시간(초)**에 정의된 간격으로 중복 주소를 검색할 NS 패킷 수를 지정하는 **NS 재시도 횟수**를 입력합니다.

Tier-1 게이트웨이

3

Tier-1 게이트웨이는 Tier-1 논리적 라우터의 기능을 수행합니다. 여기에는 세그먼트에 대한 다운링크 연결과 Tier-0 게이트웨이에 대한 업링크 연결이 있습니다.

참고 고급 네트워킹 및 보안 탭에서 Tier-1 논리적 라우터라는 용어는 Tier-1 게이트웨이를 언급하는 데 사용됩니다.

Tier-1 게이트웨이에서 경로 보급 및 정적 경로를 구성할 수 있습니다. 재귀 정적 경로가 지원됩니다.

본 장은 다음 항목을 포함합니다.

- Tier-1 게이트웨이 추가

Tier-1 게이트웨이 추가

Tier-1 게이트웨이는 일반적으로 노스바운드 방향으로 Tier-0 게이트웨이에 그리고 사우스바운드 방향으로 세그먼트에 연결됩니다.

Tier-0 및 Tier-1 게이트웨이는 단일 계층 및 다중 계층 토폴로지의 모든 인터페이스(업링크, 서비스 포트 및 다운링크)에 다음과 같은 주소 지정 구성을 지원합니다.

- IPv4 전용
- IPv6 전용
- 이중 스택 - IPv4 및 IPv6 둘 다

IPv6 또는 이중 스택 주소 지정을 사용하려면 **네트워킹 > 네트워킹 설정 > 글로벌 네트워킹 구성**에서 L3 전달 모드로 **IPv4 및 IPv6**를 사용하도록 설정합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > Tier-1 게이트웨이**를 선택합니다.
- 3 **Tier-1 게이트웨이 추가**를 클릭합니다.
- 4 게이트웨이의 이름을 입력합니다.

- 5 (선택 사항) 이 Tier-1 게이트웨이에 연결할 Tier-0 게이트웨이를 선택하여 멀티 Tier 토폴로지를 생성합니다.
- 6 페일오버 모드를 선택합니다.

옵션	설명
선택점	기본 NSX Edge 노드가 실패했다가 복구되면 피어가 선택되어 활성 노드가 됩니다. 피어의 상태는 대기로 변경됩니다.
비선택점	기본 NSX Edge 노드가 실패했다가 복구되면 피어가 활성 노드인지 확인합니다. 활성 노드이면 기본 노드는 피어를 선택하지 않으며 대기 노드가 됩니다. 이는 기본 옵션입니다.

- 7 (선택 사항) 이 Tier-1 게이트웨이가 상태 저장 서비스(NAT, 로드 밸런서 또는 방화벽)를 호스팅하도록 하려면 NSX Edge 클러스터를 선택합니다.

NSX Edge 클러스터를 선택하면 서비스 라우터가 항상 생성되고(상태 저장 서비스를 구성하지 않아도) 북/남 트래픽 패턴에 영향을 미칩니다.

- 8 (선택 사항) NSX Edge 노드를 선택합니다.
- 9 (선택 사항) 대기 재배치 사용 토글 버튼을 클릭하여 대기 재배치를 사용하거나 사용하지 않도록 설정합니다.

대기 재배치는 활성 또는 대기 논리적 라우터가 실행되고 있는 Edge 노드가 실패하는 경우고가용성을 유지하기 위해 다른 Edge 노드에서 새 대기 논리적 라우터가 생성됨을 의미합니다. 실패한 Edge 노드가 활성 논리적 라우터를 실행 중인 경우 원래의 대기 논리적 라우터가 활성 논리적 라우터가 되고 새 대기 논리적 라우터가 생성됩니다. 실패하는 Edge 노드에서 대기 논리적 라우터가 실행 중인 경우 새 대기 논리적 라우터가 대신 사용됩니다.

- 10 **저장**을 클릭합니다.
- 11 (선택 사항) **경로 보급**을 클릭합니다.

다음 중 하나 이상을 선택합니다.

- 모든 고정 경로
- 모든 NAT IP
- 모든 DNS 전달자 경로
- 모든 LB VIP 경로
- 모든 연결된 세그먼트 및 서비스 포트
- 모든 LB SNAT IP 경로
- 모든 IPSec 로컬 끝점

경로 보급 규칙 설정 필드에서 **설정**을 클릭하여 경로 보급 규칙을 추가합니다.

- 12** (선택 사항) **서비스 인터페이스** 및 **설정**을 클릭하여 세그먼트에 대한 연결을 구성합니다. VLAN 지원 세그먼트 또는 단일 압 로드 밸런싱 같은 일부 토폴로지에서 필요합니다.
- a **인터페이스 추가**를 클릭합니다.
 - b 이름 및 IP 주소를 CIDR 형식으로 입력합니다.
 - c 세그먼트를 선택합니다.
 - d **MTU** 필드에서 64와 9000 사이의 숫자를 입력합니다.
 - e **ND 프로파일** 필드에서 프로파일을 선택합니다.
 - f **저장**을 클릭합니다.
- 13** (선택 사항) **고정 경로** 및 **설정**을 클릭하여 고정 경로를 구성합니다.
- a **고정 경로 추가**를 클릭합니다.
 - b 이름 및 네트워크 주소를 CIDR 또는 IPv6 CIDR 형식으로 입력합니다.
 - c **다음 홉 설정**을 클릭하여 다음 홉 정보를 추가합니다.
 - d **저장**을 클릭합니다.

세그먼트는 논리적 스위치의 기능을 수행합니다.

참고 고급 네트워크 및 보안 탭에서 논리적 스위치라는 용어는 세그먼트를 가리키는 데 사용됩니다.

본 장은 다음 항목을 포함합니다.

- 세그먼트 프로파일
- 세그먼트 추가

세그먼트 프로파일

세그먼트 프로파일에는 세그먼트 및 세그먼트 포트에 대한 계층 2 네트워크 구성 세부 정보가 포함됩니다. NSX Manager는 여러 유형의 세그먼트 프로파일을 지원합니다.

다음 유형의 세그먼트 프로파일을 사용할 수 있습니다.

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

참고 기본 세그먼트 프로파일은 편집하거나 삭제할 수 없습니다. 기본 세그먼트 프로파일과는 다른 설정이 필요한 경우 사용자 지정 세그먼트 프로파일을 생성할 수 있습니다. 기본적으로 세그먼트 보안 프로파일을 제외한 모든 사용자 지정 세그먼트 프로파일은 해당 기본 세그먼트 프로파일의 설정을 상속합니다. 예를 들어 기본적으로 사용자 지정 IP 검색 세그먼트 프로파일은 기본 IP 검색 세그먼트 프로파일과 동일한 설정을 갖습니다.

각 기본 또는 사용자 지정 세그먼트 프로파일에는 고유 식별자가 있습니다. 이 식별자를 사용하여 세그먼트 프로파일을 세그먼트 또는 세그먼트 포트에 연결합니다.

세그먼트 또는 세그먼트 포트는 유형별로 하나의 프로파일에만 연결할 수 있습니다. 예를 들어 2개의 QoS 세그먼트 프로파일을 하나의 세그먼트 또는 세그먼트 포트에 연결할 수 없습니다.

세그먼트를 생성할 때 세그먼트 프로파일을 연결하지 않으면 NSX Manager가 해당하는 기본 시스템 정의 세그먼트 프로파일을 연결합니다. 하위 세그먼트 포트는 상위 세그먼트에서 기본 시스템 정의 세그먼트 프로파일을 상속합니다.

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

- 상위 세그먼트에 연결된 프로파일이 있으면 하위 세그먼트 포트가 상위에서 세그먼트 프로파일을 상속합니다.
- 상위 세그먼트에 연결된 세그먼트 프로파일이 없으면 기본 세그먼트 프로파일이 세그먼트에 할당되고 세그먼트 포트는 해당 기본 세그먼트 프로파일을 상속합니다.
- 사용자 지정 프로파일을 세그먼트 포트에 명시적으로 연결하는 경우 이 사용자 지정 프로파일이 기존 세그먼트 프로파일을 재정의합니다.

참고 사용자 지정 세그먼트 프로파일을 세그먼트에 연결했으나 하위 세그먼트 포트 중 하나에 대해 기본 세그먼트 프로파일을 유지하려면 기본 세그먼트 프로파일의 복사본을 만든 후 이를 특정 세그먼트 포트에 연결해야 합니다.

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

QoS 세그먼트 프로파일 이해

QoS는 높은 대역폭을 요구하는 기본 트래픽에 고품질 및 전용 네트워크 성능을 제공합니다. QoS 메커니즘은 네트워크 정체 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 세그먼트에서 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 세그먼트 수준에서 DSCP 값을 수정 및 설정합니다. 각각의 경우 DSCP 값은 캡슐화된 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 세그먼트가 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 세그먼트에 적용되고, 하위 세그먼트 포트에 상속됩니다.

QoS 세그먼트 프로파일 생성

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 **네트워킹 > 세그먼트 > 세그먼트 프로파일**을 선택합니다.
- 3 **세그먼트 프로파일 추가**를 클릭하고 **QoS**를 선택합니다.
- 4 QoS 스위칭 프로파일 세부 정보 입력을 완료합니다.

옵션	설명
이름	프로파일의 이름입니다.
모드	<p>[모드] 드롭다운 메뉴에서 신뢰함 또는 신뢰하지 않음 옵션을 선택합니다.</p> <p>[신뢰함] 모드를 선택하면 내부 헤더 DSCP 값이 IP/IPv6 트래픽에 대한 외부 IP 헤더에 적용됩니다. IP/IPv6 이외의 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>참고 DSCP 설정은 터널링된 트래픽에서만 작동합니다. 이러한 설정은 동일한 하 이퍼바이저 내의 트래픽에는 적용되지 않습니다.</p>
우선 순위	<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 크기는 대역폭이 최대인 기간을 기준으로 결정됩니다. 버스트 크기 설정에서 버스트 기간을 설정합니다. 대역폭은 보장할 수 없습니다. 그러나 평균, 최대 크기 및 버스트 크기 설정을 사용하여 네트워크 대역폭을 제한할 수 있습니다.</p> <p>예를 들어, 평균 대역폭이 30Mbps이고 최대 대역폭이 60Mbps이고 허용된 기간이 0.1초이면 버스트 크기는 $60 * 1000000 * 0.10/8 = 750000$바이트입니다.</p> <p>기본값은 0이며, 수신 트래픽에 대한 속도 제한이 사용되지 않도록 설정됩니다.</p>
수신 브로드캐스트	<p>브로드캐스트를 기준으로 VM에서 논리적 네트워크의 아웃바운드 네트워크 트래픽에 대한 사용자 지정 값을 설정합니다.</p> <p>예를 들어, 논리적 스위치에 대한 평균 대역폭을 3,000Kbps로 설정하고, 최대 대역폭이 6,000Kbps이고, 허용되는 기간은 0.1초이면 버스트 크기는 $6000 * 1000 * 0.10/8 = 75,000$바이트입니다.</p> <p>기본값은 0이며, 수신 브로드캐스트 트래픽에 대한 속도 제한이 사용되지 않도록 설정됩니다.</p>
송신	<p>논리적 네트워크에서 VM으로의 인바운드 네트워크 트래픽에 대한 사용자 지정 값을 설정합니다.</p> <p>기본값은 0이며, 송신 트래픽에 대한 속도 제한이 사용되지 않도록 설정됩니다.</p>

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

5 저장을 클릭합니다.

IP 검색 세그먼트 프로파일 이해

IP 검색은 DHCP 및 DHCPv6 스누핑, ARP(주소 확인 프로토콜) 스누핑, ND(Neighbor Discovery) 스누핑 및 VM Tools를 사용하여 MAC 및 IP 주소를 학습합니다.

참고 IPv6의 IP 검색 방법은 기본 IP 검색 세그먼트 프로파일에서 사용하지 않도록 설정됩니다. 세그먼트의 IPv6에 대해 IP 검색을 사용하도록 설정하려면 IPv6 옵션을 사용하도록 설정한 상태로 IP 검색 프로파일을 생성하고 세그먼트에 프로파일을 연결해야 합니다. 또한 분산 방화벽이 모든 워크로드 간에 IPv6 인접 항목 검색 패킷을 허용하는지 확인합니다(기본적으로 허용됨).

검색된 MAC 및 IP 주소는 ARP/ND 역제를 달성하는 데 사용되며 이는 동일한 세그먼트에 연결된 VM 사이의 트래픽을 최소화합니다. 이 주소는 SpoofGuard 및 DFW(분산 방화벽) 구성 요소에도 사용됩니다. DFW는 주소 바인딩을 사용하여 방화벽 규칙에 있는 개체의 IP 주소를 확인합니다.

DHCP/DHCPv6 스누핑은 DHCP/DHCPv6 클라이언트와 서버 간에 교환되는 DHCP/DHCPv6 패킷을 조사하여 IP 및 MAC 주소를 학습합니다.

ARP 스누핑은 VM의 송신 ARP 및 GARP(Gratuitous ARP) 패킷을 조사하여 IP 및 MAC 주소를 학습합니다.

VM Tools는 ESXi 호스팅 VM에서 실행되며 VM의 구성 정보(MAC 및 IP 또는 IPv6 주소 포함)를 제공할 수 있는 소프트웨어입니다. 이 IP 검색 방법은 ESXi 호스트에서 실행되는 VM에서만 사용할 수 있습니다.

ND 스누핑은 IPv6 형태의 ARP 스누핑입니다. NS(인접 라우터 요청) 및 NA(Neighbor Advertisement) 메시지를 조사하여 IP 및 MAC 주소를 학습합니다.

중복 주소 감지는 새로 검색된 IP 주소가 다른 포트에 대한 인식된 바인딩 목록에 이미 있는지 여부를 확인합니다. 이 확인은 동일한 세그먼트의 포트에 대해 수행됩니다. 중복 주소가 감지되면 새로 검색된 주소는 검색된 목록에 추가되지만 인식된 바인딩 목록에는 추가되지 않습니다. 모든 중복 IP에는 연결된 검색 타임스탬프가 있습니다. 인식되는 바인딩 목록에 있는 IP가 바인딩 무시 목록에 추가되거나 스누핑을 사용하지 않도록 설정하여 제거되면 가장 오래된 타임스탬프가 있는 중복 IP가 인식되는 바인딩 목록으로 이동됩니다. 중복 주소 정보는 API 호출을 통해 사용할 수 있습니다.

기본적으로 검색 방법 ARP 스누핑과 ND 스누핑은 TOFU(최초 사용 시 신뢰)라는 모드에서 작동합니다. TOFU 모드에서 주소가 검색되고 인식된 바인딩 목록에 추가되면 해당 바인딩은 인식된 목록에 계속 남아 있게 됩니다. TOFU는 ARP/ND 스누핑을 사용하여 검색된 처음 'n'개의 고유한 <IP, MAC, VLAN> 바인딩에 적용됩니다. 여기서 'n'은 구성할 수 있는 바인딩 제한입니다. ARP/ND 스누핑에 대해 TOFU를 사용하지 않도록 설정할 수 있습니다. 그러면 메시드가 모든 사용(TOEU) 모드에서 신뢰 모드로 작동합니다. TOEU 모드에서 주소가 검색되면 인식된 바인딩 목록에 추가되며, 삭제 또는 만료되면 인식된 바인딩 목록에서 제거됩니다. DHCP 스누핑 및 VM Tools는 항상 TOEU 모드에서 작동합니다.

참고 TOFU는 SpoofGuard와 동일하지 않으며 SpoofGuard와 같은 방식으로 트래픽을 차단하지 않습니다. 자세한 내용은 [SpoofGuard 세그먼트 프로파일 이해](#)를 참조하십시오.

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.

각 포트에 대해 NSX Manager는 포트에 바인딩할 수 없는 IP 주소를 포함하는 바인딩 무시 목록을 유지합니다. **고급 네트워킹 및 보안 > 스위칭 > 포트**로 이동한 후 포트를 선택하여 검색된 바인딩을 [바인딩 무시] 목록에 추가할 수 있습니다. 또한 기존의 검색되었거나 인식되는 바인딩을 **바인딩 무시**로 복사하여 삭제할 수도 있습니다.

IP 검색 세그먼트 프로파일 생성

NSX-T Data Center에는 여러 기본 IP 검색 스위칭 프로파일이 있습니다. 추가 항목을 생성할 수도 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 **네트워킹 > 세그먼트 > 세그먼트 프로파일**을 선택합니다.
- 3 **세그먼트 프로파일 추가**를 클릭하고 **IP 검색**을 선택합니다.
- 4 IP 검색 스위칭 프로파일 세부 정보를 지정합니다.

옵션	설명
이름	이름을 입력합니다.
ARP 스누핑	IPv4 환경의 경우, VM에 정적 IP 주소가 있는 경우에 해당합니다.
ARP 바인딩 제한	포트에 바인딩할 수 있는 최대 IPv4 IP 주소 수입니다. 허용되는 최소값은 1(기본값)이고 최대값은 256입니다.
ARP ND 바인딩 제한 시간 초과	TOFU가 사용되지 않도록 설정된 경우 ARP/ND 바인딩 테이블의 IP 주소에 대한 시간 초과 값(분)입니다. 주소 시간이 초과되면 새로 검색된 주소로 대체됩니다.
DHCP 스누핑	IPv4 환경의 경우, VM에 IPv4 주소가 있는 경우에 해당합니다.
DHCP V6 스누핑	IPv6 환경의 경우, VM에 IPv6 주소가 있는 경우에 해당합니다.
VM Tools	ESXi 호스팅 VM에만 사용할 수 있습니다.
IPv6용 VM Tools	ESXi 호스팅 VM에만 사용할 수 있습니다.
인접 항목 검색 스누핑	IPv6 환경의 경우, VM에 정적 IP 주소가 있는 경우에 해당합니다.
인접 항목 검색 바인딩 제한	포트에 바인딩할 수 있는 최대 IPv6 주소 수입니다.
최초 사용 시 신뢰	ARP 및 ND 스누핑에 적용됩니다.
중복 IP 감지	모든 스누핑 방법 및 IPv4 환경과 IPv6 환경의 경우.

- 5 **저장**을 클릭합니다.

SpooGuard 세그먼트 프로파일 이해

SpooGuard는 "웹 스푸핑" 또는 "피싱"이라고 하는 악의적인 공격 형태를 방지하는 데 도움이 됩니다. SpooGuard 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 세그먼트 주소 바인딩에 있는 IP 주소와 일치하지 않을 경우 가상 시스템의 vNIC는 네트워크에 전혀 액세스하지 못합니다. SpoofGuard는 포트 또는 세그먼트 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.

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

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

SpoofGuard 세그먼트 프로파일 생성

SpoofGuard가 구성되면 가상 시스템의 IP 주소가 변경될 경우 구성된 해당 포트/세그먼트 주소 바인딩이 새 IP 주소로 업데이트될 때까지 가상 시스템에서 나가는 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 **네트워킹 > 세그먼트 > 세그먼트 프로파일**을 선택합니다.
- 3 **세그먼트 프로파일 추가**를 클릭하고 **Spoof Guard**를 선택합니다.
- 4 이름을 입력합니다.
- 5 포트 수준 SpoofGuard를 사용하도록 설정하려면 **포트 바인딩을 사용**으로 설정합니다.
- 6 **저장**을 클릭합니다.

세그먼트 보안 세그먼트 프로파일 이해

세그먼트 보안은 세그먼트에 대한 수신 트래픽을 확인하고 IP 주소, MAC 주소 및 프로토콜을 허용된 주소 및 프로토콜 집합과 일치하는지 확인하고 VM에서 보낸 인증되지 않은 패킷을 삭제하여 상태 비저장 계층 2 및 계층 3 보안을 제공합니다. 세그먼트 보안을 사용하면 네트워크의 VM에서 악의적인 공격을 필터링하여 세그먼트 무결성을 보호할 수 있습니다.

기본 세그먼트 보안 프로파일은 DHCP 설정 Server Block 및 Server Block - IPv6를 사용하도록 설정되어 있습니다. 즉, 기본 세그먼트 보안 프로파일을 사용하는 세그먼트는 DHCP 서버에서 DHCP 클라이언트로 전송되는 트래픽을 차단합니다. DHCP 서버 트래픽을 허용하는 세그먼트를 원하는 경우에는 세그먼트에 대한 사용자 지정 세그먼트 보안 프로파일을 생성해야 합니다.

세그먼트 보안 세그먼트 프로파일 생성

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

사전 요구 사항

세그먼트 보안 세그먼트 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 **네트워킹 > 세그먼트 > 세그먼트 프로파일**을 선택합니다.
- 3 **세그먼트 프로파일 추가**를 클릭하고 **세그먼트 보안**을 선택합니다.

4 세그먼트 보안 프로파일 세부 정보 입력을 완료합니다.

옵션	설명
이름	프로파일의 이름입니다.
BPDU 필터	<p>BPDU 필터 버튼을 전환하여 BPDU 필터링을 사용하도록 설정합니다. 기본적으로 사용하지 않도록 설정됩니다.</p> <p>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.</p>
BPDU 필터 허용 목록	BPDU 대상 MAC 주소 목록에서 대상 MAC 주소를 클릭하여 허용되는 대상으로의 트래픽을 허용합니다. BPDU 필터 를 목록에서 선택할 수 있도록 설정해야 합니다.
DHCP 필터	<p>서버 차단 버튼 및 클라이언트 차단 버튼을 전환하여 DHCP 필터링을 사용하도록 설정합니다. 둘 다 기본적으로 사용하지 않도록 설정되어 있습니다.</p> <p>DHCP 서버 차단은 DHCP 서버에서 DHCP 클라이언트로의 트래픽을 차단합니다. DHCP 서버에서 DHCP 릴레이 에이전트로의 트래픽은 차단하지 않습니다.</p> <p>DHCP 클라이언트 차단은 DHCP 요청을 차단하여 VM이 DHCP IP 주소를 획득하지 못하게 합니다.</p>
DHCPv6 필터	<p>서버 차단 - IPv6 버튼 및 클라이언트 차단 - IPv6 버튼을 전환하여 DHCP 필터링을 사용하도록 설정합니다. 둘 다 기본적으로 사용하지 않도록 설정되어 있습니다.</p> <p>DHCPv6 서버 차단은 DHCPv6 서버에서 DHCPv6 클라이언트로의 트래픽을 차단합니다. DHCP 서버에서 DHCP 릴레이 에이전트로의 트래픽은 차단하지 않습니다. UDP 소스 포트 번호가 547인 패킷이 필터링됩니다.</p> <p>DHCPv6 클라이언트 차단은 DHCP 요청을 차단하여 VM이 DHCP IP 주소를 획득하지 못하게 합니다. UDP 소스 포트 번호가 546인 패킷이 필터링됩니다.</p>
비 IP 트래픽 차단	<p>비 IP 트래픽 차단 버튼을 전환하여 IPv4, IPv6, ARP 및 BPDU 트래픽만 허용합니다.</p> <p>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.</p>
RA 가드	RA 가드 버튼을 전환하여 수신 IPv6 라우터 알림을 필터링합니다. ICMPv6 유형 134 패킷이 필터링됩니다. 이 옵션은 기본적으로 사용하도록 설정되어 있습니다.
속도 제한	<p>브로드캐스트 및 멀티캐스트 트래픽에 대한 속도 제한을 설정합니다. 이 옵션은 기본적으로 사용하도록 설정되어 있습니다.</p> <p>속도 제한은 브로드캐스트 스톱과 같은 이벤트에서 논리적 스위치 또는 VM을 보호하는 데 사용될 수 있습니다.</p> <p>연결 문제를 방지하려면 최소 속도 제한 값을 10pps 이상으로 설정해야 합니다.</p>

5 저장을 클릭합니다.

MAC 검색 세그먼트 프로파일 이해

MAC 관리 세그먼트 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 세그먼트 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. 이 기간은 구성 가능하지 않습니다. **MAC 학습 에이징 시간** 필드에 미리 정의된 값(600)이 표시됩니다.

또한 MAC 학습은 알 수 없는 유니캐스트 플러딩을 지원합니다. 일반적으로 포트에서 수신된 패킷에 알 수 없는 대상 MAC 주소가 있으면 패킷이 삭제됩니다. 알 수 없는 유니캐스트 플러딩이 사용되도록 설정되면 포트는 MAC 학습 및 알 수 없는 유니캐스트 플러딩이 사용되도록 설정된 스위치의 모든 포트에 알 수 없는 유니캐스트 트래픽을 플러딩합니다. 이 속성은 기본적으로 사용되도록 설정되어 있지만 MAC 학습이 사용되도록 설정된 경우에만 사용할 수 있습니다.

학습할 수 있는 MAC 주소 수는 구성 가능합니다. 최대값은 4096(기본값)입니다. 제한에 도달하는 경우에 대해 이 정책을 설정할 수도 있습니다. 옵션은 다음과 같습니다.

- **삭제** - 알 수 없는 소스 MAC 주소의 패킷이 삭제됩니다. 이 MAC 주소로의 인바운드 패킷은 알 수 없는 유니캐스트로 처리됩니다. 포트는 알 수 없는 유니캐스트 플러딩을 사용하도록 설정한 경우에만 패킷을 수신합니다.
- **허용** - 주소가 학습되지 않더라도 알 수 없는 소스 MAC 주소의 패킷이 전달됩니다. 이 MAC 주소로의 인바운드 패킷은 알 수 없는 유니캐스트로 처리됩니다. 포트는 알 수 없는 유니캐스트 플러딩을 사용하도록 설정한 경우에만 패킷을 수신합니다.

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

MAC 검색 세그먼트 프로파일 생성

MAC 검색 세그먼트 프로파일을 생성하여 MAC 주소를 관리할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > 세그먼트 > 세그먼트 프로파일**을 선택합니다.
- 3 **세그먼트 프로파일 추가**를 클릭하고 **MAC 검색**을 선택합니다.

4 MAC 검색 프로파일 세부 정보 입력을 완료합니다.

옵션	설명
이름	프로파일의 이름입니다.
MAC 변경	MAC 주소 변경 기능을 사용하거나 사용하지 않도록 설정합니다. 기본값은 사용 안 함입니다.
MAC 학습	MAC 학습 기능을 사용하거나 사용하지 않도록 설정합니다. 기본값은 사용 안 함입니다.
MAC 제한 정책	허용 또는 삭제 를 선택합니다. 기본값은 허용 입니다. 이 옵션은 MAC 학습을 사용하도록 설정한 경우 사용할 수 있습니다.
알 수 없는 유니캐스트 플러딩	알 수 없는 유니캐스트 플러딩 기능을 사용하거나 사용하지 않도록 설정합니다. 기본값은 사용입니다. 이 옵션은 MAC 학습을 사용하도록 설정한 경우 사용할 수 있습니다.
MAC 제한	최대 MAC 주소 개수를 설정합니다. 기본값은 4096입니다. 이 옵션은 MAC 학습을 사용하도록 설정한 경우 사용할 수 있습니다.
MAC 학습 에이징 시간	정보를 위해서만 사용됩니다. 이 옵션은 구성할 수 없습니다. 미리 정의된 값은 600입니다.

5 저장을 클릭합니다.

세그먼트 추가

세그먼트는 게이트웨이 및 VM에 연결됩니다. 세그먼트는 논리적 스위치의 기능을 수행합니다.

VM의 VIF ID를 찾는 방법에 대한 자세한 내용은 [VM을 논리적 스위치에 연결](#)의 내용을 참조하십시오.

참고 향상된 데이터 경로 모드에서 구성된 N-VDS 스위치는 IP 검색, SpoofGuard 및 IPFIX 프로파일을 지원하지 않습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(https://<nsx-manager-ip-address>)에 로그인합니다.
- 2 **네트워킹 > 세그먼트**를 선택합니다.
- 3 **세그먼트 추가**를 클릭합니다.
- 4 세그먼트의 이름을 입력합니다.
- 5 연결된 게이트웨이를 선택합니다.

기존 Tier-0 또는 Tier-1 게이트웨이를 선택하거나 **없음**을 선택할 수 있습니다. 기본값은 **없음**이며, 이는 세그먼트가 단순히 논리적 스위치임을 의미합니다. 서브넷이 구성된 경우 Tier-0 또는 Tier-1 게이트웨이에 연결될 수 있습니다.

- 6 연결된 게이트웨이가 Tier-1 게이트웨이인 경우 유형을 **유연함** 또는 **고정됨** 중에서 선택합니다.

유연한 세그먼트는 게이트웨이에서 연결 해제될 수 있습니다. 고정된 세그먼트는 삭제될 수 있지만 게이트웨이에서 연결 해제될 수 없습니다.

- 7 서브넷을 지정하려면 **서브넷 설정**을 클릭합니다.

- 8 오버레이 또는 VLAN이 될 수 있는 전송 영역을 선택합니다.

- 9 전송 영역이 VLAN 유형인 경우 VLAN ID 목록을 지정합니다.

- 10 계층 2 VPN을 사용하여 세그먼트를 확장하려면 **L2 VPN** 텍스트 상자를 클릭하고 L2 VPN 서버 또는 클라이언트 세션을 선택합니다.

두 개 이상 선택할 수 있습니다.

- 11 **VPN 터널 ID**에서 세그먼트를 식별하는 데 사용되는 고유한 값을 입력합니다.

- 12 **저장**을 클릭합니다.

- 13 세그먼트 포트를 추가하려면 세그먼트 구성을 계속할지 묻는 메시지가 표시될 때 **예**를 클릭합니다.

a **포트 및 설정**을 클릭합니다.

b **세그먼트 포트 추가**를 클릭합니다.

c 포트 이름을 입력합니다.

d ID의 경우 이 포트에 연결되는 VM 또는 서버의 VIF UUID를 입력합니다.

e **상위**, **하위** 또는 **독립** 유형을 선택합니다.

컨테이너 또는 VMware HCX와 같은 사용 사례를 제외하고 이 텍스트 상자를 비워 둡니다. 이 포트가 VM의 컨테이너용인 경우 **하위**를 선택합니다. 이 포트가 컨테이너 호스트 VM용인 경우 **상위**를 선택합니다. 이 포트가 베어메탈 컨테이너 또는 서버용인 경우 **독립**을 선택합니다.

f 컨텍스트 ID를 입력합니다.

유형이 하위인 경우 상위 VIF ID를 입력하거나 **유형이 독립**인 경우 전송 노드 ID를 입력합니다.

g 트래픽 태그를 입력합니다.

컨테이너 및 기타 사용 사례에서 VLAN ID를 입력합니다.

h 주소 할당 방법을 **IP 풀**, **MAC 풀**, **둘 다** 또는 **없음** 중에서 선택합니다.

i 태그를 지정합니다.

j IP(IPv4 주소, IPv6 주소 또는 IPv6 서브넷) 및 주소 바인딩을 적용하려는 논리적 포트의 MAC 주소를 지정하여 주소 바인딩을 적용합니다. 예를 들어 IPv6의 경우, 2001::/64가 IPv6가 서브넷이고 2001::1이 호스트 IP이며, 2001::1/64는 잘못된 입력입니다. VLAN ID를 지정할 수도 있습니다.

수동 주소 바인딩은 지정된 경우 자동 검색된 주소 바인딩을 재정의합니다.

k 이 포트에 대한 세그먼트 프로파일을 선택합니다.

- 14 세그먼트 프로파일을 선택하려면 **세그먼트 프로파일**을 클릭합니다.

15 저장을 클릭합니다.

VPN(Virtual Private Network)

5

NSX-T Data Center는 NSX Edge 노드에서 IPsec VPN(IPsec Virtual Private Network) 및 L2 VPN(계층 2 VPN)을 지원합니다. IPsec VPN은 NSX Edge 노드와 원격 사이트 사이에서 사이트 간 연결을 제공합니다. L2 VPN을 사용하면 가상 시스템이 동일한 IP 주소를 사용하면서 지리적 경계를 넘어 네트워크 연결을 유지하도록 허용함으로써 데이터 센터를 확장할 수 있습니다.

참고 NSX-T Data Center Limited Export 릴리스에서는 IPsec VPN 및 L2 VPN이 지원되지 않습니다.

VPN 서비스를 구성하려면 Tier-0 또는 Tier-1 게이트웨이가 하나 이상 구성되어 있고 작동 중인 NSX Edge 노드가 있어야 합니다. 자세한 내용은 "NSX-T Data Center 설치 가이드"의 "NSX Edge 설치"를 참조하십시오. "

NSX-T Data Center 2.4부터는 NSX Manager 사용자 인터페이스를 사용하여 새로운 VPN 서비스를 구성할 수도 있습니다. 이전 릴리스의 NSX-T Data Center에서는 REST API 호출을 사용하여 VPN 서비스만 구성할 수 있습니다.

중요 NSX-T Data Center 2.4 이상을 사용하여 VPN 서비스를 구성하는 경우 NSX-T Data Center 2.4 이상 릴리스에 포함된 NSX Manager UI 또는 정책 API를 사용하여 생성된 Tier-0 게이트웨이와 같은 새로운 개체를 사용해야 합니다. NSX-T Data Center 2.4 릴리스 전에 구성된 기존 Tier-0 또는 Tier-1 논리적 라우터를 사용하려면 계속해서 API 호출을 사용하여 VPN 서비스를 구성해야 합니다.

VPN 서비스 구성 중에 사전 정의된 값 및 설정이 포함된 시스템 기본 구성 프로파일을 사용할 수 있습니다. 다른 설정이 포함된 새로운 프로파일을 정의하고 VPN 서비스 구성 중에 선택할 수도 있습니다.

본 장은 다음 항목을 포함합니다.

- IPsec VPN 이해
- 계층 2 VPN 이해
- VPN 서비스 추가
- IPsec VPN 세션 추가
- L2 VPN 세션 추가
- 로컬 끝점 추가
- 프로파일 추가
- 자치 Edge를 L2 VPN 클라이언트로 추가

- IPsec VPN 세션의 인식된 상태 확인
- VPN 세션 모니터링 및 문제 해결

IPsec VPN 이해

IPsec(인터넷 프로토콜 보안) 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. ESP는 IP 프로토콜 번호 50을 사용하여 IP 위에서 직접 작동합니다.

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

NSX Edge는 정책 기반 또는 경로 기반 IPsec VPN을 지원합니다.

Active-Standby 고가용성 모드에 있어야 하는 Tier-0 게이트웨이에서 IPsec VPN 서비스가 지원됩니다. 자세한 내용은 [Tier-0 게이트웨이 추가](#)의 내용을 참조하십시오. NSX-T Data Center 2.5부터 IPsec VPN은 Tier-1 게이트웨이에서도 지원됩니다. IPsec VPN 서비스를 구성할 때 Tier-0 또는 Tier-1 게이트웨이에 연결된 세그먼트를 사용할 수 있습니다.

NSX-T Data Center의 IPsec VPN 서비스는 게이트웨이 수준 페일오버 기능을 사용하여 고가용성 서비스를 지원합니다. 터널이 페일오버 시 재설정되고 VPN 구성 데이터가 동기화됩니다. 터널이 재설정될 때 IPsec VPN 상태는 동기화되지 않습니다.

NSX Edge 노드와 원격 VPN 사이트 간에 사전 공유 키 모드 인증 및 IP 유니캐스트 트래픽이 지원됩니다. 또한 NSX-T Data Center 2.4부터 인증서 인증이 지원됩니다. 다음 서명 해시 알고리즘 중 하나에서 서명한 인증서 유형만 지원됩니다.

- SHA256withRSA
- SHA384withRSA
- SHA512withRSA

정책 기반 IPsec VPN 사용

정책 기반 IPsec VPN을 사용하려면 VPN 터널을 통과하기 전에 IPsec으로 보호되는 트래픽을 확인하기 위해 패킷에 VPN 정책을 적용해야 합니다.

이런 유형의 VPN은 로컬 네트워크 토폴로지 및 구성이 변경될 때 변경 사항을 수용하기 위해 VPN 정책 설정도 업데이트해야 하기 때문에 정적으로 간주됩니다.

NSX-T Data Center와 함께 정책 기반 IPsec VPN을 사용하는 경우 IPsec 터널을 사용하여 NSX Edge 노드 뒤에 있는 하나 이상의 로컬 서브넷을 원격 VPN 사이트의 피어 서브넷과 연결합니다.

NAT 디바이스 뒤에 NSX Edge 노드를 배포할 수 있습니다. 이 배포에서 NAT 디바이스는 NSX Edge 노드의 VPN 주소를 인터넷에 연결하는 공용 액세스 가능 주소로 변환합니다. 원격 VPN 사이트는 이 공용 주소를 사용하여 NSX Edge 노드에 액세스합니다.

NAT 디바이스 뒤에 원격 VPN 사이트를 배치할 수도 있습니다. IPSec 터널을 설정하려면 원격 VPN 사이트의 공용 IP 주소 및 해당 ID(FQDN 또는 IP 주소)를 제공해야 합니다. 양쪽 끝점에서 VPN 주소에 대해 정적 일대일 NAT가 필요합니다.

참고 정책 기반 IPSec VPN이 구성된 Tier-1 게이트웨이에서는 DNAT가 지원되지 않습니다.

다음 표에 표시된 것처럼 NSX Edge 노드의 크기는 지원되는 터널의 최대 수를 결정합니다.

표 5-1. 지원되는 IPSec 터널 수

Edge 노드 크기	VPN 세션(정책 기반)당 IPSec 터널 수	VPN 서비스당 세션 수	VPN 서비스당 IPSec 터널 수 (세션당 터널 16개)
소형	해당 없음(POC/Lab 전용)	해당 없음(POC/Lab 전용)	해당 없음(POC/Lab 전용)
중간	128	128	2048
대형	128(소프트 한도)	256	4096
베어메탈	128(소프트 한도)	512	6000

제한 사항 정책 기반 IPSec VPN의 기본 아키텍처로 인해 VPN 터널 이중화를 설정할 수 없습니다.

정책 기반 IPSec VPN을 구성하는 방법에 대한 내용은 [IPSec VPN 서비스 추가](#) 항목을 참조하십시오.

경로 기반 IPSec VPN 사용

경로 기반 IPSec VPN은 BGP 등을 프로토콜로 사용하여 VTI(가상 터널 인터페이스)라는 특수 인터페이스를 통해 정적 경로 또는 동적으로 학습된 경로를 기준으로 트래픽을 터널링합니다. IPSec은 VTI를 통과하는 모든 트래픽을 보호합니다.

참고

- IPSec VPN 터널을 통한 라우팅에 대해서는 OSPF 동적 라우팅이 지원되지 않습니다.
- VTI에 대한 동적 라우팅은 Tier-1 게이트웨이를 기준으로 하는 VPN에서는 지원되지 않습니다.

경로 기반 IPSec VPN은 IPSec 처리를 적용하기 전에 패킷에 추가 캡슐화가 추가되지 않는다는 점을 제외하고 IPSec을 통한 GRE(일반 라우팅 캡슐화)와 비슷합니다.

이 VPN 터널링 방식에서는 NSX Edge 노드에 VTI가 생성됩니다. 각 VTI는 IPSec 터널과 연결됩니다. 암호화된 트래픽은 VTI 인터페이스를 통해 한 사이트에서 다른 사이트로 라우팅됩니다. IPSec 처리는 VTI에서만 발생합니다.

VPN 터널 이중화

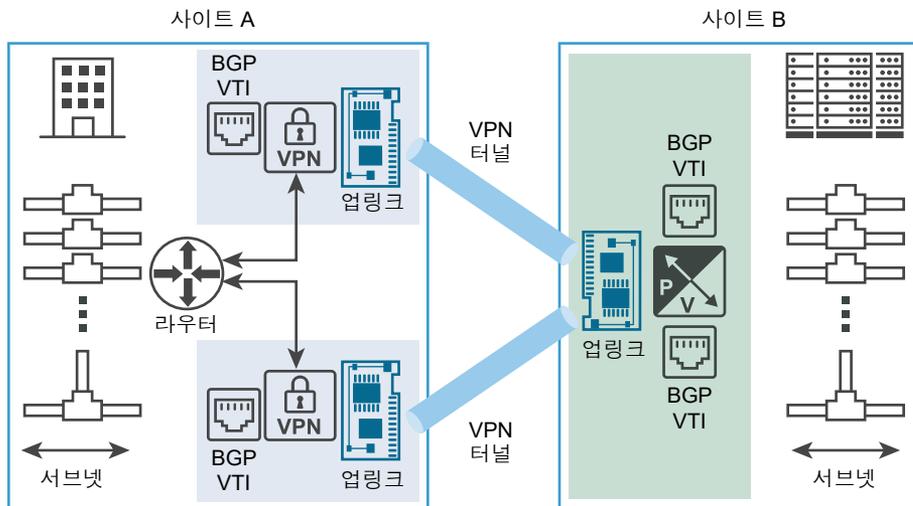
Tier-0 게이트웨이에 구성된 경로 기반 IPsec VPN 세션을 사용하여 VPN 터널 이중화를 구성할 수 있습니다. 터널 이중화를 사용하면 두 사이트 간에 여러 개의 터널을 설정할 수 있습니다. 이중 하나의 터널을 기본 터널을 사용할 수 없을 때 다른 터널로의 페일오버를 통해 기본 터널로 사용합니다. 이 기능은 링크 이중화에 대해 다른 ISP를 사용하는 것과 같은 여러 연결 옵션이 있는 경우에 가장 유용합니다.

중요

- NSX-T Data Center에서 IPsec VPN 터널 이중화는 BGP를 사용해야만 지원됩니다.
- VPN 터널 이중화를 달성하려면 경로 기반 IPsec VPN 터널에 대해 정적 라우팅을 사용하지 마십시오.

다음 그림은 두 사이트 간의 IPsec VPN 터널 이중화를 논리적으로 보여 줍니다. 이 그림에서 사이트 A와 사이트 B는 2개의 데이터 센터를 나타냅니다. 이 예의 경우 NSX-T Data Center가 사이트 A에서 Edge VPN 게이트웨이를 관리하고 있지 않으며 NSX-T Data Center가 사이트 B에서 Edge Gateway 가상 장치를 관리하고 있다고 가정합니다.

그림 5-1. 경로 기반 IPsec VPN의 터널 이중화



그림에 나와 있는 것처럼 VTI를 사용하여 두 개의 독립 IPsec VPN 터널을 구성할 수 있습니다. 동적 라우팅은 터널 이중화를 달성하기 위해 BGP 프로토콜을 사용하여 구성됩니다. 두 IPsec VPN 터널을 사용할 수 있는 경우 서비스에 남아 있습니다. NSX Edge 노드를 통해 사이트 A에서 사이트 B로 경로가 지정된 모든 트래픽은 VTI를 통해 라우팅됩니다. 데이터 트래픽은 IPsec 처리를 거치고 연결된 NSX Edge 노드 업링크 인터페이스에서 벗어납니다. NSX Edge 노드 업링크 인터페이스의 사이트 B VPN 게이트웨이에서 수신된 모든 들어오는 IPsec 트래픽이 암호 해독 후에 VTI로 전달되면 일반적인 라우팅이 발생합니다.

필요한 페일오버 시간 내에 피어와의 연결 끊김을 감지하도록 BGP 보류 타이머 및 연결 유지 타이머 값을 구성해야 합니다. BGP 구성의 내용을 참조하십시오.

계층 2 VPN 이해

계층 2 VPN(L2 VPN)을 사용하면 동일한 브로드캐스트 도메인의 여러 사이트에 계층 2 네트워크(VNI 또는 VLAN)를 확장할 수 있습니다. 이 연결은 L2 VPN 서버 및 L2 VPN 클라이언트 간의 경로 기반 IPSec 터널로 보호됩니다.

참고 이 L2 VPN 기능은 NSX-T Data Center에서만 사용할 수 있으며 타사 상호 운용성은 없습니다.

확장된 네트워크는 단일 브로드캐스트 도메인이 있는 단일 서브넷이므로 사이트 간에 VM을 이동하더라도 VM은 동일한 서브넷에 남아 있으며 IP 주소는 변경되지 않습니다. 따라서 기업은 네트워크 사이트 간에 VM을 원활하게 마이그레이션할 수 있습니다. VM은 VNI 기반 네트워크 또는 VLAN 기반 네트워크에서 실행될 수 있습니다. 클라우드 제공자의 경우 L2 VPN은 테넌트 워크로드 및 애플리케이션에서 사용하는 기존 IP 주소를 수정하지 않고 해당 테넌트를 온보딩하는 메커니즘을 제공합니다.

데이터 센터 마이그레이션을 지원하는 것 외에도, L2 VPN으로 확장된 온-프레미스 네트워크는 재해 복구 계획 및 수요 증가를 충족시키기 위한 오프-프레미스 계산 리소스의 동적 활용에 유용합니다.

각 L2 VPN 세션에는 하나의 GRE(Generic Routing Encapsulation) 터널이 있습니다. 터널 이중화는 지원되지 않습니다. L2 VPN 세션은 최대 4094개의 L2 세그먼트로 확장할 수 있습니다.

NSX-T Data Center L2 VPN 서비스는 Tier-0 게이트웨이에서만 지원됩니다. 세그먼트는 Tier-0 또는 Tier-1 게이트웨이에 연결될 수 있으며 L2 VPN 서비스를 사용할 수 있습니다.

NSX-T Data Center 2.5 릴리스부터 VLAN 기반 세그먼트는 NSX-T Data Center 환경에서 관리되는 NSX Edge에서 L2 VPN 서비스를 사용하여 확장할 수 있습니다. 이 지원을 통해 VLAN에서 VNI, VLAN에서 VLAN 및 VNI에서 VNI로의 L2 네트워크 확장을 허용할 수 있습니다.

또한 ESX N-VDS(NSX 관리형 가상 분산 스위치)를 사용하는 VLAN 트렁킹도 지원됩니다. 계산 및 I/O 리소스에서 허용하는 경우 VLAN 트렁킹은 한 개의 NSX Edge 클러스터가 단일 인터페이스를 통해 여러 VLAN 네트워크를 확장할 수 있도록 합니다.

L2 VPN 서비스 지원은 다음과 같은 시나리오에서 제공됩니다.

- NSX Data Center for vSphere 환경에서 관리되는 NSX Edge에서 호스팅되는 L2 VPN 클라이언트 및 NSX-T Data Center L2 VPN 서버 사이. 관리되는 L2 VPN 클라이언트는 VLAN과 VNI를 모두 지원합니다.
- 독립형 또는 관리되지 않는 NSX Edge에서 호스팅되는 L2 VPN 클라이언트 및 NSX-T Data Center L2 VPN 서버 사이. 관리되지 않는 L2 VPN 클라이언트는 VLAN만 지원합니다.
- 자치 NSX Edge에서 호스팅되는 L2 VPN 클라이언트 및 NSX-T Data Center L2 VPN 서버 사이. 자치 L2 VPN 클라이언트는 VLAN만 지원합니다.
- NSX-T Data Center 2.4 릴리스부터, NSX-T Data Center L2 VPN 서버 및 NSX-T Data Center L2 VPN 클라이언트 간에 L2 VPN 서비스 지원을 사용할 수 있습니다. 이 시나리오에서는 두 개의 온-프레미스 SDDC(소프트웨어 정의 데이터 센터) 간에 논리적 L2 세그먼트를 확장할 수 있습니다.

VPN 서비스 추가

NSX Manager UI(사용자 인터페이스)를 사용하여 IPsec VPN(정책 기반 또는 경로 기반) 또는 L2 VPN을 추가할 수 있습니다.

다음 섹션에서는 필요한 VPN 서비스를 설정하는 데 필요한 워크플로에 대한 정보를 제공합니다. 이 섹션 다음에 나오는 항목에서는 NSX Manager 사용자 인터페이스를 사용하여 IPsec VPN 또는 L2 VPN을 추가하는 방법에 대해 자세히 설명합니다.

정책 기반 IPsec VPN 구성 워크플로

정책 기반 IPsec VPN 서비스 워크플로를 구성하려면 다음과 같은 개괄적인 단계가 필요합니다.

- 1 기존 Tier-0 또는 Tier-1 게이트웨이를 사용하여 IPsec VPN 서비스를 생성하고 사용하도록 설정합니다. [IPsec VPN 서비스 추가](#)의 내용을 참조하십시오.
- 2 시스템 기본값을 사용하지 않으려는 경우, DPD(Dead Peer Detection) 프로파일을 생성합니다. [DPD 프로파일 추가](#)의 내용을 참조하십시오.
- 3 시스템 기본값이 아닌 IKE 프로파일을 사용하려면 IKE(Internet Key Exchange) 프로파일을 정의합니다. [IKE 프로파일 추가](#)의 내용을 참조하십시오.
- 4 [IPsec 프로파일 추가](#) 작업을 수행하여 IPsec 프로파일을 구성합니다.
- 5 로컬 끝점 추가를 사용하여 NSX Edge에서 호스팅되는 VPN 서버를 생성합니다.
- 6 정책 기반 IPsec VPN 세션을 구성하고, 프로파일을 적용하고, 여기에 로컬 끝점을 연결합니다. [정책 기반 IPsec 세션 추가](#)의 내용을 참조하십시오. 터널에 사용할 로컬 및 피어 서브넷을 지정합니다. 로컬 서브넷에서 피어 서브넷으로 향하는 트래픽은 세션에 정의된 터널을 사용하여 보호됩니다.

경로 기반 IPsec VPN 구성 워크플로

경로 기반 IPsec VPN 구성 워크플로에는 다음과 같은 개괄적인 단계가 필요합니다.

- 1 기존 Tier-0 또는 Tier-1 게이트웨이를 사용하여 IPsec VPN 서비스를 구성하고 사용하도록 설정합니다. [IPsec VPN 서비스 추가](#)의 내용을 참조하십시오.
- 2 기본 IKE 프로파일을 사용하지 않으려면 IKE 프로파일을 정의합니다. [IKE 프로파일 추가](#)의 내용을 참조하십시오.
- 3 시스템 기본 IPsec 프로파일을 사용하지 않으려는 경우, [IPsec 프로파일 추가](#) 작업을 수행하여 생성합니다.
- 4 기본 DPD 프로파일을 사용하지 않으려면 DPD 프로파일을 생성합니다. [DPD 프로파일 추가](#)의 내용을 참조하십시오.
- 5 로컬 끝점 추가 작업을 수행하여 로컬 끝점을 추가합니다.
- 6 경로 기반 IPsec VPN 세션을 구성하고, 프로파일을 적용하고, 세션에 로컬 끝점을 연결합니다. 구성에 VTI IP를 제공하고 동일한 IP를 사용하여 라우팅을 구성합니다. 경로는 정적 또는 동적일 수 있습니다(BGP 사용). [경로 기반 IPsec 세션 추가](#)의 내용을 참조하십시오.

L2 VPN 구성 워크플로

L2 VPN을 구성하려면 서버 모드에서 L2 VPN 서비스를 구성한 다음 클라이언트 모드에서 또 다른 L2 VPN 서비스를 구성해야 합니다. L2 VPN 서버에 의해 생성된 피어 코드를 사용하여 L2 VPN 서버 및 L2 VPN 클라이언트에 대한 세션도 구성해야 합니다. 다음은 L2 VPN 서비스를 구성하는 개괄적인 워크플로입니다.

- 1 서버 모드에서 L2 VPN 서비스를 생성합니다.
 - a Tier-0 게이트웨이를 사용하는 경로 기반 IPsec 터널을 구성하고 이 경로 기반 IPsec VPN 터널을 사용하여 L2 VPN 서버 서비스를 구성합니다. [L2 VPN 서버 서비스 추가](#)의 내용을 참조하십시오.
 - b 새로 생성된 경로 기반 IPsec VPN 서비스와 L2 VPN 서버 서비스를 바인딩하는 L2 VPN 서버 세션을 구성하고 GRE IP 주소를 자동으로 할당합니다. [L2 VPN 서버 세션 추가](#)의 내용을 참조하십시오.
 - c L2 VPN 서버 세션에 세그먼트를 추가합니다. 이 단계는 [L2 VPN 서버 세션 추가](#)에도 설명되어 있습니다.
 - d 원격 측 [L2 VPN 구성 파일 다운로드](#) 작업을 수행하여 L2 VPN 서버 서비스 세션에 대한 피어 코드를 확보합니다. 이 피어 코드를 원격 사이트에 적용하고, L2 VPN 클라이언트 세션을 자동으로 구성하는 데 사용해야 합니다.
- 2 클라이언트 모드에서 L2 VPN 서비스를 생성합니다.
 - a 다른 Tier-0 게이트웨이를 사용하여 또 다른 경로 기반 IPsec VPN 서비스를 구성하고 방금 구성한 Tier-0 게이트웨이를 사용하여 L2 VPN 클라이언트 서비스를 구성합니다. 자세한 내용은 [L2 VPN 클라이언트 서비스 추가](#)의 내용을 참조하십시오.
 - b L2 VPN 서버 서비스에서 생성된 피어 코드를 가져와서 L2 VPN 클라이언트 세션을 정의합니다. [L2 VPN 클라이언트 세션 추가](#)의 내용을 참조하십시오.
 - c 이전 단계에서 정의된 L2 VPN 클라이언트 세션에 세그먼트를 추가합니다. 이 단계는 [L2 VPN 클라이언트 세션 추가](#)에 설명되어 있습니다.

IPsec VPN 서비스 추가

NSX-T Data Center는 Tier-0 또는 Tier-1 게이트웨이와 원격 사이트 사이에서 사이트 간 IPsec VPN 서비스를 지원합니다. 정책 기반 또는 경로 기반 IPsec VPN 서비스를 생성할 수 있습니다. 정책 기반 또는 경로 기반 IPsec VPN 세션을 구성하려면 먼저 IPsec VPN 서비스를 생성해야 합니다.

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

IPsec VPN은 로컬 끝점 IP 주소가 IPsec VPN 세션이 구성된 동일한 논리적 라우터에서 NAT를 통과할 때는 지원되지 않습니다.

사전 요구 사항

- IPsec VPN을 숙지합니다. [IPsec VPN 이해](#)의 내용을 참조하십시오.

- Tier-0 또는 Tier-1 게이트웨이가 하나 이상 구성되어 있고 사용할 수 있어야 합니다. 자세한 내용은 Tier-0 게이트웨이 추가 또는 Tier-1 게이트웨이 추가를 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(https://<nsx-manager-ip-address>)에 로그인합니다.
- 2 **네트워킹 > VPN > VPN 서비스**로 이동합니다.
- 3 **서비스 추가 > IPSec**를 선택합니다.
- 4 IPSec 서비스의 이름을 입력합니다.
이 이름은 필수입니다.
- 5 **게이트웨이** 드롭다운 메뉴에서 이 IPSec VPN 서비스와 연결할 Tier-0 또는 Tier-1 게이트웨이를 선택합니다.
- 6 **관리 상태**를 사용하거나 사용하지 않도록 설정합니다.
기본적으로 이 값은 Enabled로 설정됩니다. 즉, 새 IPSec VPN 서비스가 구성된 후 IPSec VPN 서비스가 Tier-0 또는 Tier-1 게이트웨이에서 사용하도록 설정됩니다.
- 7 **IKE 로그 수준**에 대한 값을 설정합니다.
기본값은 Info 수준으로 설정됩니다.
- 8 이 서비스를 태그 그룹에 포함시키려면 **태그**에 대한 값을 입력합니다.
- 9 IPSec 세션 규칙에 IP 주소가 지정된 경우에도 임의의 IPSec 보호 없이 지정된 로컬 및 원격 IP 주소 간에 데이터 패킷을 교환할 수 있도록 허용하려면 **글로벌 바이패스 규칙**을 클릭합니다. **로컬 네트워크 및 원격 네트워크** 텍스트 상자에 바이패스 규칙이 적용되는 로컬 및 원격 서브넷 목록을 입력합니다.
기본값은 로컬 사이트와 원격 사이트 간에 데이터를 교환할 때 IPSec 보호를 사용하는 것입니다. 이 규칙은 이 IPSec VPN 서비스 내에서 생성된 모든 IPSec VPN 세션에 적용됩니다. ""
- 10 **저장**을 클릭합니다.
새 IPSec VPN 서비스가 성공적으로 만들어지면 나머지 IPSec VPN 구성을 계속할지 묻는 메시지가 나타납니다. **예**를 클릭하면 [IPSec VPN 서비스 추가] 패널로 되돌아갑니다. 이제 **세션** 링크가 활성화되어 있고, 이것을 클릭하여 IPSec VPN 세션을 추가할 수 있습니다.

다음에 수행할 작업

IPSec VPN 세션 추가의 정보를 사용하여 IPSec VPN 세션을 추가하는 과정을 안내합니다. IPSec VPN 구성을 마치는 데 필요한 프로파일 및 로컬 끝점에 대한 정보도 제공합니다.

L2 VPN 서비스 추가

L2 VPN 서비스를 Tier-0 게이트웨이에서 구성합니다. L2 VPN 서비스를 사용하도록 설정하려면 Tier-0 게이트웨이에 IPSec VPN 서비스가 아직 없으면 생성해야 합니다. 그런 다음, L2 VPN 서버(대상 게이트웨이)와 L2 VPN 클라이언트(소스 게이트웨이) 간에 L2 VPN 터널을 구성합니다.

L2 VPN 서비스를 구성하려면 이 섹션 뒤에 나오는 항목의 정보를 참조하십시오.

사전 요구 사항

- IPsec VPN 및 L2 VPN을 숙지합니다. **IPSec VPN 이해** 및 **계층 2 VPN 이해**를 참조하십시오.
- Tier-0 게이트웨이가 하나 이상 구성되어 있고 사용할 수 있어야 합니다. **Tier-0 게이트웨이 추가**의 내용을 참조하십시오.

절차

1 L2 VPN 서버 서비스 추가

L2 VPN 서버 서비스를 구성하려면 L2 VPN 클라이언트가 연결될 대상 NSX Edge에서 서버 모드로 L2 VPN 서비스를 구성해야 합니다.

2 L2 VPN 클라이언트 서비스 추가

L2 VPN 서버 서비스를 구성한 후에는 다른 NSX Edge 인스턴스에서 클라이언트 모드로 L2 VPN 서비스를 구성합니다.

L2 VPN 서버 서비스 추가

L2 VPN 서버 서비스를 구성하려면 L2 VPN 클라이언트가 연결될 대상 NSX Edge에서 서버 모드로 L2 VPN 서비스를 구성해야 합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 (선택 사항) L2 VPN 서버로 구성하려는 IPsec VPN 서비스가 Tier-0 게이트웨이에 아직 없는 경우 다음 단계를 사용하여 생성합니다.
 - a **네트워킹 > VPN > VPN 서비스** 탭으로 이동하여 **서비스 추가 > IPsec**을 선택합니다.
 - b IPsec VPN 서비스의 이름을 입력합니다.
 - c **Tier-0 게이트웨이** 드롭다운 메뉴에서 L2 VPN 서버에 사용할 Tier-0 게이트웨이를 선택합니다.
 - d 시스템 기본값과 다른 값을 사용하려면 필요에 따라 [IPsec 서비스 추가] 창에서 나머지 속성을 설정합니다.
 - e **저장**을 클릭하고 IPsec VPN 서비스를 계속 구성할지 묻는 메시지가 나타나면 **아니요**를 선택합니다.
- 3 **네트워킹 > VPN > VPN 서비스** 탭으로 이동하고 **서비스 추가 > L2 VPN 서버**를 선택하여 L2 VPN 서버를 생성합니다.
- 4 L2 VPN 서버의 이름을 입력합니다.
- 5 **Tier-0 게이트웨이** 드롭다운 메뉴에서 잠시 전에 만든 IPsec 서비스에 사용한 것과 동일한 Tier-0 게이트웨이를 선택합니다.
- 6 이 L2 VPN 서버에 대한 설명(선택 사항)을 입력합니다.

7 이 서비스를 태그 그룹에 포함시키려면 **태그**에 대한 값을 입력합니다.

8 **허브 및 스포크** 속성을 사용하거나 사용하지 않도록 설정합니다.

기본적으로 이 값은 Disabled으로 설정됩니다. 즉, L2 VPN 클라이언트에서 받은 트래픽이 L2 VPN 서버에 연결된 세그먼트로만 복제됩니다. 이 속성이 Enabled로 설정되면, L2 VPN 클라이언트의 트래픽이 다른 모든 L2 VPN 클라이언트에 복제됩니다.

9 **저장**을 클릭합니다.

새 L2 VPN 서버가 성공적으로 생성되면 나머지 L2 VPN 서비스 구성을 계속할지 묻는 메시지가 표시됩니다. **예**를 클릭하면, [L2 VPN 서버 추가] 창으로 되돌아가고 **세션** 링크가 활성화됩니다. 이 링크를 사용하여 L2 VPN 서버 세션을 생성하거나 **네트워킹 > VPN > L2 VPN 세션** 탭을 사용할 수 있습니다.

다음에 수행할 작업

L2 VPN 서버 세션 추가의 정보를 가이드로 사용하여 구성된 L2 VPN 서버에 대한 L2 VPN 서버 세션을 구성합니다.

L2 VPN 클라이언트 서비스 추가

L2 VPN 서버 서비스를 구성한 후에는 다른 NSX Edge 인스턴스에서 클라이언트 모드로 L2 VPN 서비스를 구성합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 (선택 사항) L2 VPN 클라이언트 서비스에 대한 IPSec VPN 서비스가 아직 없는 경우 다음 단계를 사용하여 생성합니다.
 - a **네트워킹 > VPN > VPN 서비스** 탭으로 이동하여 **서비스 추가 > IPSec**을 선택합니다.
 - b IPSec VPN 서비스의 이름을 입력합니다.
 - c **Tier-0 게이트웨이** 드롭다운 메뉴에서 L2 VPN 클라이언트에 사용할 Tier-0 게이트웨이를 선택합니다.
 - d 시스템 기본값과 다른 값을 사용하려면 필요에 따라 [IPSec 서비스 추가] 창에서 나머지 속성을 설정합니다.
 - e **저장**을 클릭하고 IPSec VPN 서비스를 계속 구성할지 묻는 메시지가 나타나면 **아니요**를 선택합니다.
- 3 **네트워킹 > VPN > VPN 서비스** 탭으로 이동하여 **서비스 추가 > L2 VPN 클라이언트**을 선택합니다.
- 4 L2 VPN 클라이언트 서비스의 이름을 입력합니다.
- 5 **Tier-0 게이트웨이** 드롭다운 메뉴에서 이전에 생성한 경로 기반 IPSec 터널과 함께 사용한 것과 동일한 Tier-0 게이트웨이를 선택합니다.
- 6 필요한 경우 **설명** 및 **태그**에 대한 값을 설정합니다.

7 저장을 클릭합니다.

새 L2 VPN 클라이언트 서비스가 성공적으로 생성된 후 나머지 L2 VPN 클라이언트 구성을 계속할지 여부를 확인합니다. 예를 클릭하는 경우 [L2 VPN 클라이언트 추가] 창으로 되돌아가고 **세션** 링크가 사용되도록 설정됩니다. 해당 링크를 사용하여 L2 VPN 클라이언트 세션을 생성하거나 **네트워킹 > VPN > L2 VPN 세션** 탭을 사용할 수 있습니다.

다음에 수행할 작업

구성한 L2 VPN 클라이언트 서비스에 대한 L2 VPN 클라이언트 세션을 구성합니다. **L2 VPN 클라이언트 세션 추가**의 정보를 가이드로 사용합니다.

IPSec VPN 세션 추가

IPSec VPN 서비스를 구성한 후에는 구성할 IPSec VPN 유형에 따라 정책 기반 IPSec VPN 세션 또는 경로 기반 IPSec VPN 세션을 추가해야 합니다. IPSec VPN 서비스 구성을 마치는 데 사용할 로컬 끝점 및 프로파일에 대한 정보도 제공합니다.

정책 기반 IPSec 세션 추가

정책 기반 IPSec VPN을 추가할 때 IPSec 터널이 NSX Edge 노드 뒤의 다중 로컬 서브넷을 원격 VPN 사이트의 피어 서브넷과 연결하는 데 사용됩니다.

다음 단계에서는 NSX Manager UI의 **IPSec 세션** 탭을 사용하여 정책 기반 IPSec 세션을 만듭니다. 또한 터널, IKE 및 DPD 프로파일에 대한 정보를 추가하고 정책 기반 IPSec VPN에 사용할 기존 로컬 끝점을 선택합니다.

참고 IPSec VPN 서비스를 구성한 직후에 IPSec VPN 세션을 추가할 수도 있습니다. IPSec VPN 서비스 구성을 계속할지 묻는 메시지가 표시되면 **예**를 클릭하고 [IPSec 세션 추가] 패널에서 **세션 > 세션 추가**를 선택합니다. 다음 절차의 처음 몇 개 단계는 IPSec VPN 서비스 구성을 계속할지 묻는 메시지에서 **아니오**를 선택한 경우를 가정한 것입니다. **예**를 선택하면, 다음 단계의 3단계로 진행하여 나머지 정책 기반 IPSec VPN 세션 구성을 안내합니다.

사전 요구 사항

- 계속하기 전에 IPSec VPN 서비스를 구성해야 합니다. **IPSec VPN 서비스 추가**의 내용을 참조하십시오.
- 추가하려는 정책 기반 IPSec VPN 세션에서 사용할 로컬 끝점, 피어 사이트의 IP 주소, 로컬 네트워크 서브넷 및 원격 네트워크 서브넷에 대한 정보를 확보합니다. 로컬 끝점을 생성하려면 **로컬 끝점 추가**의 내용을 참조하십시오.
- 인증에 PSK(사전 공유 키)를 사용 중이면 PSK 값을 가져옵니다.
- 인증에 인증서를 사용 중이라면 필요한 서버 인증서와 해당하는 CA 서명된 인증서를 이미 가져왔는지 확인합니다. **인증서 설정**의 내용을 참조하십시오.

- NSX-T Data Center에서 제공하는 IPSec 터널, IKE 또는 DPD(Dead Peer Detection) 프로파일의 기본값을 사용하지 않으려면, 사용하려는 프로파일을 대신 구성합니다. 자세한 내용은 [프로파일 추가](#)의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > VPN > IPSec 세션** 탭으로 이동합니다.
- 3 **IPSec 세션 추가 > 정책 기반**를 선택합니다.
- 4 정책 기반 IPSec VPN 세션의 이름을 입력합니다.
- 5 **VPN 서비스** 드롭다운 메뉴에서, 이 새로운 IPSec 세션을 추가할 IPSec VPN 서비스를 선택합니다.

참고 IPSec 세션 추가 대화 상자에서 이 IPSec 세션을 추가하는 경우에는 **IPSec 세션 추가** 버튼 위에 VPN 서비스 이름이 이미 표시되어 있습니다.

- 6 드롭다운 메뉴에서 기존의 로컬 끝점을 선택합니다.
이 로컬 끝점 값은 필수이며 로컬 NSX Edge 노드를 식별합니다. 다른 로컬 끝점을 생성하려는 경우 3개의 점으로 표시된 메뉴(⋮)를 클릭하고 **로컬 끝점 추가**를 선택합니다.
- 7 **원격 IP** 텍스트 상자에 원격 사이트의 필수 IP주소를 입력합니다.
이 값은 필수입니다.
- 8 이 정책 기반 IPSec VPN 세션에 대한 설명(선택 사항)을 입력합니다.
최대 길이는 1024자입니다.
- 9 IPSec VPN 세션을 사용하거나 사용하지 않도록 설정하려면 **관리 상태**를 클릭합니다.
기본적으로 값은 Enabled으로 설정됩니다. 즉, IPSec VPN 세션이 NSX Edge 노드로 구성됩니다.
- 10 (선택 사항) **규정 준수 제품군** 드롭다운 메뉴에서 보안 규정 준수 제품군을 선택합니다.

참고 규정 준수 제품군 지원은 NSX-T Data Center 2.5부터 제공됩니다. 자세한 내용은 [지원되는 규정 준수 제품군 정보](#)를 참조하십시오.

선택된 기본값은 None입니다. 규정 준수 제품군을 선택하는 경우 **인증 모드**가 Certificate로 설정되고 **고급 속성** 섹션에서 **IKE 프로파일** 및 **IPSec 프로파일**의 값이 선택한 보안 규정 준수 제품군에 대한 시스템 정의 프로파일로 설정됩니다. 이러한 시스템 정의 프로파일은 편집할 수 없습니다.

- 11 **규정 준수 제품군**을 None으로 설정하면 **인증 모드** 드롭다운 메뉴에서 모드를 선택합니다.
사용되는 기본 인증 모드는 PSK입니다. 이것은 NSX Edge와 원격 사이트 간에 공유되는 비밀 키가 IPSec VPN 세션에 사용됨을 의미합니다. Certificate를 선택하면 로컬 끝점을 구성하는 데 사용된 사이트 인증서가 인증에 사용됩니다.

- 12 로컬 네트워크 및 원격 네트워크 텍스트 상자에 이 정책 기반 IPsec VPN 세션에 사용할 IP 서브넷 주소를 하나 이상 입력합니다.

이러한 서브넷은 CIDR 형식이어야 합니다.

- 13 인증 모드가 PSK로 설정되면 사전 공유 키 텍스트 상자에 키 값을 입력합니다.

비밀 키는 최대 길이가 128자인 문자열일 수 있습니다.

경고 PSK 값에는 일부 민감한 정보가 포함되어 있으므로 공유하거나 저장할 때 주의해야 합니다.

- 14 피어 사이트를 식별하려면 원격 ID에 값을 입력합니다.

PSK 인증을 사용하는 피어 사이트의 경우 이 ID 값은 공용 IP 주소이거나 피어 사이트의 FQDN이어야 합니다. 인증서 인증을 사용하는 피어 사이트의 경우 이 ID 값은 피어 사이트 인증서에서 사용되는 CN(일반 이름) 또는 DN(고유 이름)이어야 합니다.

참고 피어 사이트의 인증서에는 DN 문자열의 이메일 주소가 포함되어 있습니다. 예를 들어 다음과 같습니다.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123/emailAddress=user1@mycompany.com
```

그런 다음, 예에서처럼 다음 형식을 사용하여 원격 ID 값을 입력합니다.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, MAILTO=user1@mycompany.com"
```

로컬 사이트의 인증서에 DN 문자열의 이메일 주소가 포함되어 있고 피어 사이트에서 strongSwan IPsec 구현을 사용하는 경우, 해당 피어 사이트에 로컬 사이트의 ID 값을 입력합니다. 예제는 다음과 같습니다.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, E=user1@mycompany.com"
```

- 15 정책 기반 IPsec VPN 세션에서 사용되는 프로파일, 초기 모드, TCP MSS 클램핑 모드 및 태그를 변경하려면 고급 속성을 클릭합니다.

기본적으로 시스템에서 생성한 프로파일이 사용됩니다. 기본 프로파일을 사용하지 않으려면 사용할 수 있는 다른 프로파일을 선택합니다. 아직 구성되지 않은 프로파일을 사용하려는 경우에는 3개의 점으로 표시된 메뉴(⋮)를 클릭하고 다른 프로파일을 생성합니다. [프로파일 추가](#)의 내용을 참조하십시오.

- IKE 프로파일** 드롭다운 메뉴가 사용하도록 설정되면 IKE 프로파일을 선택합니다.
- IPsec 프로파일** 드롭다운 메뉴를 사용하도록 설정한 경우 IPsec 터널 프로파일을 선택합니다.
- DPD 프로파일** 드롭다운 메뉴를 사용하도록 설정한 경우 기본 DPD 프로파일을 선택합니다.

- d **연결 시작 모드** 드롭다운 메뉴에서 기본 모드를 선택합니다.

연결 시작 모드는 터널 생성 프로세스 중에 로컬 끝점에서 사용하는 정책을 정의합니다. 기본값은 **이니시에이터**입니다. 다음 표에서는 사용 가능한 서로 다른 연결 시작 모드에 대해 설명합니다.

표 5-2. 연결 시작 모드

연결 시작 모드	설명
Initiator	기본값입니다. 이 모드에서 로컬 끝점은 IPsec VPN 터널 생성을 시작하고 피어 게이트웨이로부터 들어오는 터널 설정 요청에 응답합니다.
On Demand	이 모드에서 로컬 끝점은 정책 규칙과 일치하는 첫 번째 패킷이 수신된 이후 IPsec VPN 터널 생성을 시작합니다. 또한 들어오는 시작 요청에도 응답합니다.
Respond Only	IPsec VPN은 연결을 시작하지 않습니다. 항상 피어 사이트에서 연결 요청을 시작하고 로컬 끝점은 해당 연결 요청에 응답합니다.

- e IPsec 연결 동안 TCP 세션의 MSS(최대 세그먼트 크기) 페이로드를 줄이려면 **TCP MSS 클램핑**을 사용하도록 설정하고 **TCP MSS 방향** 값을 선택한 후, 필요에 따라 **TCP MSS 값**을 설정합니다.

자세한 내용은 **TCP MSS 클램핑 이해** 항목을 참조하십시오.

- f 특정 그룹의 일부로 이 세션을 포함하려는 경우 **태그**에 태그 이름을 입력합니다.

16 저장을 클릭합니다.

결과

새 정책 기반 IPsec VPN 세션이 성공적으로 구성되면 사용 가능한 IPsec VPN 세션 목록에 추가됩니다. 이것은 읽기 전용 모드입니다.

다음에 수행할 작업

- IPsec VPN 터널 상태가 [실행 중]인지 확인합니다. 자세한 내용은 **VPN 세션 모니터링 및 문제 해결**의 내용을 참조하십시오.
- 필요한 경우 세션 행의 왼쪽에서 3개의 점으로 표시된 메뉴(⋮)를 클릭하여 IPsec VPN 세션 정보를 관리합니다. 수행할 수 있는 작업 중 하나를 선택합니다.

경로 기반 IPsec 세션 추가

경로 기반 IPsec VPN을 추가하면 BGP와 같은 기본 프로토콜을 사용하여 VTI(가상 터널 인터페이스)를 통해 동적으로 학습된 경로를 기반으로 트래픽에 터널링이 제공됩니다. IPsec은 VTI를 통과하는 모든 트래픽을 보호합니다.

이 항목에 설명된 단계에서는 **IPSec 세션** 탭을 사용하여 경로 기반 IPSec 세션을 생성합니다. 터널, IKE 및 DPD 프로파일에 대한 정보를 추가하고 경로 기반 IPSec VPN에서 사용할 기존의 로컬 끝점을 선택합니다.

참고 IPSec VPN 서비스를 구성한 직후에 IPSec VPN 세션을 추가할 수도 있습니다. IPSec VPN 서비스 구성을 계속할지 묻는 메시지가 표시되면 **예**를 클릭하고 [IPSec 세션 추가] 패널에서 **세션 > 세션 추가**를 선택합니다. 다음 절차의 처음 몇 개 단계는 IPSec VPN 서비스 구성을 계속할지 묻는 메시지에서 **아니오**를 선택한 경우를 가정한 것입니다. **예**를 선택했다면 3단계로 진행합니다. 이후 단계에서는 경로 기반 IPSec VPN 세션 구성의 나머지 작업들을 안내합니다.

사전 요구 사항

- 계속하기 전에 IPSec VPN 서비스를 구성해야 합니다. **IPSec VPN 서비스 추가**의 내용을 참조하십시오.
- 추가하려는 경로 기반 IPSec 세션에서 사용할 터널 서비스 IP 서브넷 주소, 피어 사이트의 IP 주소 및 로컬 끝점에 대한 정보를 가져옵니다. 로컬 끝점을 생성하려면 **로컬 끝점 추가**의 내용을 참조하십시오.
- 인증에 PSK(사전 공유 키)를 사용 중이면 PSK 값을 가져옵니다.
- 인증에 인증서를 사용 중이라면 필요한 서버 인증서와 해당하는 CA 서명된 인증서를 이미 가져왔는지 확인합니다. **인증서 설정**의 내용을 참조하십시오.
- NSX-T Data Center에서 제공된 IPSec 터널, IKE 또는 DPD(Dead Peer Detection) 프로파일에 대해 기본값을 사용하지 않으려는 경우에는 대신 사용할 프로파일을 구성합니다. 자세한 내용은 **프로파일 추가**의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(https://<nsx-manager-ip-address>)에 로그인합니다.
- 2 **네트워킹 > VPN > IPSec 세션**로 이동합니다.
- 3 **IPSec 세션 추가 > 경로 기반**를 선택합니다.
- 4 경로 기반 IPSec 세션의 이름을 입력합니다.
- 5 **VPN 서비스** 드롭다운 메뉴에서, 이 새로운 IPSec 세션을 추가할 IPSec VPN 서비스를 선택합니다.

참고 **IPSec 세션 추가** 대화 상자에서 이 IPSec 세션을 추가하는 경우에는 **IPSec 세션 추가** 버튼 위에 VPN 서비스 이름이 이미 표시되어 있습니다.

- 6 드롭다운 메뉴에서 기존의 로컬 끝점을 선택합니다.
이 로컬 끝점 값은 필수이며 로컬 NSX Edge 노드를 식별합니다. 다른 로컬 끝점을 생성하려는 경우 3개의 점으로 표시된 메뉴()를 클릭하고 **로컬 끝점 추가**를 선택합니다.
- 7 **원격 IP** 텍스트 상자에 원격 사이트의 IP 주소를 입력합니다.
이 값은 필수입니다.

- 8 이 경로 기반 IPsec VPN 세션에 대한 설명(선택 사항)을 입력합니다.
최대 길이는 1024자입니다.
- 9 IPsec 세션을 사용 또는 사용하지 않도록 설정하려면 **관리 상태**를 클릭합니다.
기본적으로 값은 Enabled으로 설정됩니다. 즉, IPsec 세션이 NSX Edge 노드로 구성됩니다.
- 10 (선택 사항) **규정 준수 제품군** 드롭다운 메뉴에서 보안 규정 준수 제품군을 선택합니다.

참고 규정 준수 제품군 지원은 NSX-T Data Center 2.5부터 제공됩니다. 자세한 내용은 [지원되는 규정 준수 제품군 정보](#)를 참조하십시오.

기본값은 None으로 설정됩니다. 규정 준수 제품군을 선택하는 경우 **인증 모드**가 Certificate로 설정되고 **고급 속성** 섹션에서 **IKE 프로파일** 및 **IPsec 프로파일**의 값이 선택한 규정 준수 제품군에 대한 시스템 정의 프로파일로 설정됩니다. 이러한 시스템 정의 프로파일은 편집할 수 없습니다.

- 11 터널 인터페이스에 CIDR 표기법으로 IP 서브넷 주소를 입력합니다.
이 주소는 필수입니다.
- 12 **규정 준수 제품군**을 None으로 설정하면 **인증 모드** 드롭다운 메뉴에서 모드를 선택합니다.
사용되는 기본 인증 모드는 PSK입니다. 이것은 NSX Edge와 원격 사이트 간에 공유되는 비밀 키가 IPsec VPN 세션에 사용됨을 의미합니다. Certificate를 선택하면 로컬 끝점을 구성하는 데 사용된 사이트 인증서가 인증에 사용됩니다.
- 13 인증 모드로 PSK를 선택했다면 **사전 공유 키** 텍스트 상자에 키 값을 입력합니다.
비밀 키는 최대 길이가 128자인 문자열일 수 있습니다.

경고 PSK 값에는 일부 민감한 정보가 포함되어 있으므로 공유하거나 저장할 때 주의해야 합니다.

14 원격 ID에 값을 입력합니다.

PSK 인증을 사용하는 피어 사이트의 경우 이 ID 값은 공용 IP 주소이거나 피어 사이트의 FQDN이어야 합니다. 인증서 인증을 사용하는 피어 사이트의 경우 이 ID 값은 피어 사이트 인증서에서 사용되는 CN(일반 이름) 또는 DN(고유 이름)이어야 합니다.

참고 피어 사이트의 인증서에는 DN 문자열의 이메일 주소가 포함되어 있습니다. 예를 들어 다음과 같습니다.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123/emailAddress=user1@mycompany.com
```

그런 다음, 예에서처럼 다음 형식을 사용하여 **원격 ID** 값을 입력합니다.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, MAILTO=user1@mycompany.com"
```

로컬 사이트의 인증서에 DN 문자열의 이메일 주소가 포함되어 있고 피어 사이트에서 strongSwan IPsec 구현을 사용하는 경우, 해당 피어 사이트에 로컬 사이트의 ID 값을 입력합니다. 예제는 다음과 같습니다.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, E=user1@mycompany.com"
```

- 15 특정 그룹 태그의 일부로 이 IPsec 세션을 포함하려는 경우 **태그**에 태그 이름을 입력합니다.
- 16 경로 기반 IPsec VPN 세션에서 사용되는 프로파일, 초기 모드, TCP MSS 클램핑 모드 및 태그를 변경하려면 **고급 속성**을 클릭합니다.

기본적으로 시스템에서 생성한 프로파일이 사용됩니다. 기본 프로파일을 사용하지 않으려면 사용 가능한 다른 프로파일을 선택합니다. 아직 구성되지 않은 프로파일을 사용하려는 경우에는 3개의 점으로 표시된 메뉴()를 클릭하고 다른 프로파일을 생성합니다. **프로파일 추가**의 내용을 참조하십시오.

- a **IKE 프로파일** 드롭다운 메뉴가 사용하도록 설정되면 IKE 프로파일을 선택합니다.
- b **IPsec 프로파일** 드롭다운 메뉴를 사용하도록 설정한 경우 IPsec 터널 프로파일을 선택합니다.

- c **DPD 프로파일** 드롭다운 메뉴를 사용하도록 설정한 경우 기본 DPD 프로파일을 선택합니다.
- d **연결 시작 모드** 드롭다운 메뉴에서 기본 모드를 선택합니다.

연결 시작 모드는 터널 생성 프로세스 중에 로컬 끝점에서 사용하는 정책을 정의합니다. 기본값은 **이니시에이터**입니다. 다음 표에서는 사용 가능한 서로 다른 연결 시작 모드에 대해 설명합니다.

표 5-3. 연결 시작 모드

연결 시작 모드	설명
Initiator	기본값입니다. 이 모드에서 로컬 끝점은 IPsec VPN 터널 생성을 시작하고 피어 게이트웨이로부터 들어오는 터널 설정 요청에 응답합니다.
On Demand	경로 기반 VPN에서는 사용하지 마십시오. 이 모드는 정책 기반 VPN에만 적용됩니다.
Respond Only	IPsec VPN은 연결을 시작하지 않습니다. 항상 피어 사이트에서 연결 요청을 시작하고 로컬 끝점은 해당 연결 요청에 응답합니다.

- 17 IPsec 연결 동안 TCP 세션의 MSS(최대 세그먼트 크기) 페이로드를 줄이려면 **TCP MSS 클램핑**을 사용하도록 설정하고 **TCP MSS 방향** 값을 선택한 후, 필요에 따라 **TCP MSS 값**을 설정합니다. []

자세한 내용은 [TCP MSS 클램핑 이해](#)를 참조하십시오.

- 18 특정 그룹 태그의 일부로 이 IPsec 세션을 포함하려는 경우 **태그**에 태그 이름을 입력합니다.

- 19 **저장**을 클릭합니다.

결과

새로운 경로 기반 IPsec VPN 세션이 성공적으로 구성되면 사용 가능한 IPsec VPN 세션 목록에 추가됩니다. 이것은 읽기 전용 모드입니다.

다음에 수행할 작업

- IPsec VPN 터널 상태가 [실행 중]인지 확인합니다. 자세한 내용은 [VPN 세션 모니터링 및 문제 해결](#)의 내용을 참조하십시오.
- 정적 경로 또는 BGP를 사용하여 라우팅을 구성합니다. 정적 경로 구성 또는 [BGP 구성](#)을 참조하십시오.
- 필요한 경우 세션 행의 왼쪽에서 3개의 점으로 표시된 메뉴(⋮)를 클릭하여 IPsec VPN 세션 정보를 관리합니다. 수행할 수 있는 작업 중 하나를 선택합니다.

지원되는 규정 준수 제품군 정보

NSX-T Data Center 2.5부터 IPsec VPN 세션에 사용되는 보안 프로파일을 구성하는 데 사용할 보안 규정 준수 제품군을 지정할 수 있습니다.

보안 규정 준수 제품군에는 여러 보안 매개 변수에 사용되고 수정할 수 없는 미리 정의된 값이 있습니다. 규정 준수 제품군을 선택하면 미리 정의된 값이 구성 중인 IPSec VPN 세션의 보안 프로파일에 자동으로 사용됩니다.

다음 표에는 NSX-T Data Center의 IKE 프로파일에 대해 지원되는 규정 준수 제품군과 각각에 대한 미리 정의된 값이 나열되어 있습니다.

규정 준수 제품군 이름	IKE 버전	암호화 알고리즘	다이제스트 알고리즘	Diffie Hellman 그룹
CNSA	IKEv2	AES 256	SHA2 384	그룹 15, 그룹 20
FIPS	IKE-Flex	AES 128	SHA2 256	그룹 20
기본	IKEv1	AES 128	SHA2 256	그룹 14
PRIME	IKEv2	AES GCM 128	설정되지 않음	그룹 19
Suite-B-GCM-128	IKEv2	AES 128	SHA2 256	그룹 19
Suite-B-GCM-256	IKEv2	AES 256	SHA2 384	그룹 20

다음 표에는 NSX-T Data Center의 IPSec 프로파일에 대해 지원되는 규정 준수 제품군과 각각에 대한 미리 정의된 값이 나열되어 있습니다.

규정 준수 제품군 이름	암호화 알고리즘	다이제스트 알고리즘	PFS 그룹	Diffie-Hellman 그룹
CNSA	AES 256	SHA2 384	사용	그룹 15, 그룹 20
FIPS	AES GCM 128	설정되지 않음	사용	그룹 20
기본	AES 128	SHA2 256	사용	그룹 14
PRIME	AES GCM 128	설정되지 않음	사용	그룹 19
Suite-B-GCM-128	AES GCM 128	설정되지 않음	사용	그룹 19
Suite-B-GCM-256	AES GCM 256	설정되지 않음	사용	그룹 20

TCP MSS 클램핑 이해

TCP MSS 클램핑을 사용하면 IPSec 터널을 통한 연결 설정 중에 TCP 세션에서 사용되는 MSS(최대 세그먼트 크기) 값을 줄일 수 있습니다. 이 기능은 NSX-T Data Center 2.5부터 지원됩니다.

TCP MSS는 호스트가 단일 TCP 세그먼트에서 수락할 수 있는 최대 데이터 양(바이트)입니다. TCP 연결의 각 끝은 3방향 핸드셰이크 동안 원하는 MSS 값을 해당 피어 끝에 전송합니다. 여기서 MSS는 TCP SYN 패킷에서 사용되는 TCP 헤더 옵션 중 하나입니다. TCP MSS는 보낸 사람 호스트의 송신 인터페이스에 대한 MTU(최대 전송 단위)를 기준으로 계산됩니다.

TCP 트래픽이 IPSec VPN 또는 임의 종류의 VPN 터널을 통과하면 보안을 유지하기 위해 추가 헤더가 원래 패킷에 추가됩니다. IPSec 터널 모드인 경우 추가 헤더는 IP, ESP 및 선택적으로 UDP(포트 변환이 네트워크에 있는 경우)입니다. 이러한 추가 헤더 때문에 캡슐화된 패킷의 크기가 VPN 인터페이스의 MTU를 초과합니다. 패킷은 DF 정책에 따라 조각나거나 삭제될 수 있습니다.

패킷 조각화 또는 삭제를 방지하려면 TCP MSS 클램핑 기능을 사용하도록 설정하여 IPsec 세션의 MSS 값을 조정할 수 있습니다. **네트워킹 > VPN > IPsec 세션**으로 이동합니다. IPsec 세션을 추가하거나 기존 항목을 편집할 때 **고급 속성** 섹션을 확장하고 **TCP MSS 클램핑**을 사용하도록 설정합니다.

TCP MSS 방향 및 **TCP MSS 값**을 설정하여 IPsec 세션에 적합한 미리 계산된 MSS 값을 구성할 수 있습니다. 구성된 MSS 값은 MSS 클램핑에 사용됩니다. **TCP MSS 방향**을 설정하고 **TCP MSS 값**을 비워 두어 동적 MSS 계산을 사용하도록 선택할 수 있습니다. MSS 값은 VPN 인터페이스 MTU, VPN 오버헤드 및 PMTU(경로 MTU)(미리 결정된 경우)를 기준으로 자동 계산됩니다. MTU 또는 PMTU 변경 사항을 동적으로 처리하기 위해 각 TCP 핸드셰이크 동안 유효 MSS가 다시 계산됩니다.

L2 VPN 세션 추가

L2 VPN 서버와 L2 VPN 클라이언트를 구성한 후 모두에 대해 L2 VPN 세션을 추가하여 L2 VPN 서비스 구성을 완료해야 합니다.

L2 VPN 서버 세션 추가

L2 VPN 서버 서비스를 생성한 후에는 L2 VPN 세션을 추가하고 이 세션을 기존 세그먼트에 연결해야 합니다.

다음 단계에서는 NSX Manager UI의 **L2 VPN 세션** 탭을 사용하여 L2 VPN 서버 세션을 생성합니다. 또한 L2 VPN 서버 세션에 연결할 기존 로컬 끝점 및 세그먼트를 선택합니다.

참고 L2 VPN 서버 서비스를 구성한 직후에 L2 VPN 서버 세션을 추가할 수도 있습니다. L2 VPN 서버 구성을 계속할지 묻는 메시지가 표시되면 **예**를 클릭하고 [L2 VPN 서버 추가] 패널에서 **세션 > 세션 추가**를 선택합니다. 다음 절차의 처음 몇 개 단계는 L2 VPN 서버 구성을 계속할지 묻는 메시지에서 **아니오**를 선택한 경우를 가정한 것입니다. **예**를 선택했다면 3단계로 진행합니다. 이후 단계에서는 L2 VPN 서버 세션 구성의 나머지 작업들을 안내합니다.

사전 요구 사항

- 계속하기 전에 L2 VPN 서버 서비스를 구성해야 합니다. **L2 VPN 서버 서비스 추가**의 내용을 참조하십시오.
- 추가 중인 L2 VPN 서버 세션에서 사용할 로컬 끝점 및 원격 IP에 대한 정보를 가져옵니다. 로컬 끝점을 생성하려면 **로컬 끝점 추가**의 내용을 참조하십시오.
- L2 VPN 서버 세션에서 사용할 PSK(사전 공유 키) 및 터널 인터페이스 서브넷에 대한 값을 가져옵니다.
- 생성 중인 L2 VPN 서버 세션에 연결하려는 기존 세그먼트의 이름을 가져옵니다. 자세한 내용은 **세그먼트 추가**의 내용을 참조하십시오.

절차

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

- 2 **네트워킹 > VPN > L2 VPN 세션** 탭으로 이동합니다.
- 3 **L2 VPN 세션 추가 > L2 VPN 서버**를 선택합니다.
- 4 L2 VPN 서버 세션의 이름을 입력합니다.
- 5 **L2 VPN 서비스** 드롭다운 메뉴에서 L2 VPN 세션을 생성할 L2 VPN 서버 서비스를 선택합니다.

참고 이 L2 VPN 서버 세션을 [L2VPN 서버 세션 설정] 대화 상자에서 추가하는 중이라면 L2 VPN 서버 서비스가 이미 **L2 세션 추가** 버튼 위에 표시됩니다.

- 6 드롭다운 메뉴에서 기존의 로컬 끝점을 선택합니다.
 다른 로컬 끝점을 생성하려는 경우 3개의 점으로 표시된 메뉴(⋮)를 클릭하고 **로컬 끝점 추가**를 선택합니다.
- 7 원격 사이트의 IP 주소를 입력합니다.
- 8 L2 VPN 서버 세션을 사용하거나 사용하지 않도록 설정하려면 **관리 상태**를 클릭합니다.
 기본적으로 값은 **사용**으로 설정됩니다. 즉, L2 VPN 서버 세션이 NSX Edge 노드로 구성됩니다.
- 9 **사전 공유 키**에 비밀 키 값을 입력합니다.

경고 PSK 값은 중요한 정보로 간주되므로 공유하거나 저장할 때 주의해야 합니다.

- 10 **터널 인터페이스**에 CIDR 표기법을 사용하여 IP 서브넷 주소를 입력합니다.
 예: 4.5.6.6/24 이 서브넷 주소는 필수입니다.
- 11 **원격 ID**에 값을 입력합니다.
 인증서 인증을 사용하는 피어 사이트의 경우 이 ID는 피어 사이트 인증서의 일반 이름이어야 합니다. PSK 피어의 경우에는 이 ID가 임의의 문자열일 수 있습니다. 가능하면 VPN 서비스의 FQDN 또는 VPN의 공용 IP 주소를 Remote ID로 사용하는 것이 좋습니다.
- 12 특정 그룹의 일부로 이 세션을 포함하려는 경우 **태그**에 태그 이름을 입력합니다.
- 13 **저장**을 클릭하고 VPN 서비스 구성을 계속할 것인지 묻는 메시지가 표시되면 **예**를 클릭합니다.
 [L2VPN 세션 추가] 패널로 돌아오면 이제 **세그먼트** 링크를 사용할 수 있습니다.
- 14 기존 세그먼트를 L2 VPN 서버 세션에 연결합니다.
 - a **세그먼트 > 세그먼트 설정**을 클릭합니다.
 - b **세그먼트 설정** 대화 상자에서 **세그먼트 설정**을 클릭하여 기존 세그먼트를 L2 VPN 서버 세션에 연결합니다.
 - c **세그먼트** 드롭다운 메뉴에서 세션에 연결할 VNI 기반 또는 VLAN 기반 세그먼트를 선택합니다.

d 선택한 세그먼트를 식별하는 데 사용되는 **VPN 터널 ID**에 고유한 값을 입력합니다.

e **저장**을 클릭한 다음 **닫기**를 클릭합니다.

[L2VPN 세션 설정] 창 또는 대화 상자에서 시스템이 L2 VPN 서버 세션에 대해 **세그먼트** 수를 증가시킵니다.

15 L2 VPN 서버 세션 구성을 완료하려면 **편집 닫기**를 클릭합니다.

결과

VPN 서비스 탭에서 시스템이 사용자가 구성한 L2 VPN 서버 서비스에 대해 **세션** 수를 증가시킵니다.

다음에 수행할 작업

L2 VPN 서비스 구성을 완료하려면 L2 VPN 서비스([클라이언트] 모드)와 L2 VPN 클라이언트 세션도 생성해야 합니다. **L2 VPN 클라이언트 서비스 추가** 및 **L2 VPN 클라이언트 세션 추가**를 참조하십시오.

L2 VPN 클라이언트 세션 추가

L2 VPN 클라이언트 서비스를 생성한 후에 L2 VPN 클라이언트 세션을 추가하고 기존 세그먼트에 연결해야 합니다.

다음 단계에서는 NSX Manager UI의 **L2 VPN 세션** 탭을 사용하여 L2 VPN 클라이언트 세션을 생성합니다. L2 VPN 클라이언트 세션에 연결할 기존 로컬 끝점 및 세그먼트도 선택합니다.

참고 L2 VPN 클라이언트 서비스를 성공적으로 구성한 후 바로 L2 VPN 클라이언트 세션을 추가할 수도 있습니다. L2 VPN 클라이언트 구성을 계속할지 묻는 메시지가 표시되면 **예**를 클릭하고 [L2 VPN 클라이언트 추가] 패널에서 **세션 > 세션 추가**를 선택합니다. 다음 절차의 처음 몇 단계에서는 L2 VPN 클라이언트 구성을 계속할지 묻는 메시지에서 **아니오**를 선택했다고 가정합니다. **예**를 선택하면 다음 단계의 3단계로 진행하여 나머지 L2 VPN 클라이언트 세션 구성을 안내합니다.

사전 요구 사항

- 계속하기 전에 L2 VPN 클라이언트 서비스를 구성해야 합니다. **L2 VPN 클라이언트 서비스 추가**의 내용을 참조하십시오.
- 추가하려는 L2 VPN 클라이언트 세션에 사용할 로컬 IP 및 원격 IP에 대한 IP 주소 정보를 확보합니다.
- L2 VPN 서버 구성 중에 생성된 피어 코드를 확보합니다. **원격 측 L2 VPN 구성 파일 다운로드**의 내용을 참조하십시오.
- 생성하려는 L2 VPN 클라이언트 세션에 연결할 기존 세그먼트의 이름을 확보합니다. **세그먼트 추가**의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(https://<nsx-manager-ip-address>)에 로그인합니다.
- 2 **네트워킹 > VPN > L2 VPN 세션**을 선택합니다.

- 3 **L2 VPN 세션 추가 > L2 VPN 클라이언트**를 선택합니다.
- 4 L2 VPN 클라이언트 세션에 대한 이름을 입력합니다.
- 5 **VPN 서비스** 드롭다운 메뉴에서 L2 VPN 세션을 연결할 L2 VPN 클라이언트 서비스를 선택합니다.

참고 [L2 VPN 클라이언트 세션 설정] 대화상자에서 이 L2 VPN 클라이언트 세션을 추가하는 경우, L2 VPN 클라이언트 서비스가 **L2 세션 추가** 버튼 위에 이미 표시되어 있습니다.

- 6 **로컬 IP 주소** 텍스트 상자에 L2 VPN 클라이언트 세션의 IP 주소를 입력합니다. ""
- 7 L2 VPN 클라이언트 세션에 사용할 IPsec 터널의 원격 IP 주소를 입력합니다. ""
- 8 **피어 구성** 텍스트 상자에 L2 VPN 서버 서비스를 구성할 때 생성된 피어 코드를 입력합니다.
- 9 **관리 상태**를 사용하거나 사용하지 않도록 설정합니다.
기본적으로 값은 **사용**으로 설정됩니다. 즉, L2 VPN 서버 세션이 NSX Edge 노드로 구성됩니다.
- 10 **저장**을 클릭하고 VPN 서비스 구성을 계속할 것인지 묻는 메시지가 표시되면 **예**를 클릭합니다.
- 11 기존 세그먼트를 L2 VPN 클라이언트 세션에 연결합니다.
 - a **세그먼트 > 세그먼트 추가**를 선택합니다.
 - b **세그먼트 설정** 대화상자에서 **세그먼트 추가**를 클릭합니다.
 - c **세그먼트** 드롭다운 메뉴에서 L2 VPN 클라이언트 세션에 연결할 VNI 기반 또는 VLAN 기반 세그먼트를 선택합니다.
 - d 선택한 세그먼트를 식별하는 데 사용되는 **VPN 터널 ID**에 고유한 값을 입력합니다.
 - e **닫기**를 클릭합니다.
- 12 L2 VPN 클라이언트 세션 구성을 마치려면 **편집 닫기**를 클릭합니다.

결과

VPN 서비스 탭에, 구성된 L2 VPN 클라이언트 서비스에 대한 세션 수가 업데이트됩니다.

원격 측 L2 VPN 구성 파일 다운로드

L2 VPN 클라이언트 세션을 구성하려면 L2 VPN 서버 세션을 구성했을 때 생성된 피어 코드를 가져와야 합니다.

사전 요구 사항

- 계속하기 전에 L2 VPN 서버 서비스 및 세션이 구성되어 있어야 합니다. **L2 VPN 서버 서비스 추가**의 내용을 참조하십시오.

절차

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

- 2 **네트워크 > VPN > L2 VPN 세션** 탭으로 이동합니다.
- 3 L2 VPN 세션 테이블에서 L2 VPN 클라이언트 세션 구성에 대해 사용하려는 L2 VPN 서버 세션에 대한 행을 확장합니다.
- 4 **구성 다운로드**를 클릭하고 [경고] 대화상자에서 **예**를 클릭합니다.

이름이 L2VPNSession_<name-of-L2-VPN-server-session>_config.txt인 텍스트 파일이 다운로드됩니다. 원격 측 L2 VPN 구성에 대한 피어 코드가 포함됩니다.

경고 피어 코드에는 중요한 정보로 간주되는 PSK 값이 포함되어 있으므로 저장 및 공유할 때 주의하십시오.

예를 들어 L2VPNSession_L2VPNServer_config.txt에는 다음 구성이 포함됩니다.

```
[
  {
    "transport_tunnel_path": "/infra/tier-0s/ServerT0_AS/locale-services/1-policyconnectivity-693/ipsec-vpn-services/IpsecService1/sessions/Routebase1",
    "peer_code":
    "MCw3ZjBjYzdjLHsic210ZU5hbWUiOiJSb3V0ZWJhc2UxIiwic3JjVGFwSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYXBjCjE2OS4yNTQuNjQuMSIsImVlbnR1bm5lbHMlOlR1ImxvY2FzSWQiOiI2MC42MC42MC4xIiwicGVlcklkIjoiaU50NTAuNTAuMSIsImxvY2FzVnRpsXAiOiIxNjkuMi4yLjMvMzEifV19"
  }
]
```

- 5 L2 VPN 클라이언트 서비스 및 세션을 구성하는 데 사용하는 피어 코드를 복사합니다.

앞의 구성 파일 예제를 사용하여 L2 VPN 클라이언트 구성에서 사용할 수 있게 다음 피어 코드를 복사합니다.

```
MCw3ZjBjYzdjLHsic210ZU5hbWUiOiJSb3V0ZWJhc2UxIiwic3JjVGFwSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYXBjCjE2OS4yNTQuNjQuMSIsImVlbnR1bm5lbHMlOlR1ImxvY2FzSWQiOiI2MC42MC42MC4xIiwicGVlcklkIjoiaU50NTAuNTAuMSIsImxvY2FzVnRpsXAiOiIxNjkuMi4yLjMvMzEifV19
```

다음에 수행할 작업

L2 VPN 클라이언트 서비스 및 세션을 구성합니다. L2 VPN 클라이언트 서비스 추가 및 L2 VPN 클라이언트 세션 추가를 참조하십시오.

로컬 끝점 추가

구성 중인 IPSec VPN에서 사용할 로컬 끝점을 구성해야 합니다.

다음 단계에서는 NSX Manager UI의 **로컬 끝점** 탭을 사용합니다. IPsec VPN 세션을 추가하는 동안 3개의 점으로 표시된 메뉴(☰)를 클릭하고 **로컬 끝점 추가**를 선택하여 로컬 끝점을 생성할 수도 있습니다. 현재 IPsec VPN 세션을 구성하는 중이라면 3단계로 진행하십시오. 여기에서 새 로컬 끝점 생성 과정을 안내합니다.

사전 요구 사항

- 구성 중인 로컬 끝점을 사용할 IPsec VPN 세션에 대해 인증서 기반 인증 모드를 사용 중인 경우 로컬 끝점에서 사용해야 하는 인증서에 대한 정보를 가져옵니다.
- 이 로컬 끝점이 연결될 IPsec VPN 서비스를 구성했는지 확인합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > VPN > 로컬 끝점**로 이동하고 **로컬 끝점 추가**를 클릭합니다.
- 3 로컬 끝점의 이름을 입력합니다.
- 4 **VPN 서비스** 드롭다운 메뉴에서 이 로컬 끝점을 연결할 IPsec VPN 서비스를 선택합니다.
- 5 로컬 끝점의 IP 주소를 입력합니다.

Tier-0 게이트웨이에서 실행되는 IPsec VPN 서비스의 경우 로컬 끝점 IP 주소는 Tier-0 게이트웨이의 업링크 인터페이스 IP 주소와 달라야 합니다. 제공하는 로컬 끝점 IP 주소는 Tier-0 게이트웨이의 루프백 인터페이스에 연결되며 업링크 인터페이스를 통해 라우팅할 수 있는 IP 주소로도 게시됩니다. Tier-1 게이트웨이에서 실행되는 IPsec VPN 서비스의 경우 로컬 끝점 IP 주소를 라우팅할 수 없으면 IPsec 로컬 끝점에 대한 경로 보급이 Tier-1 게이트웨이 구성에서 사용되도록 설정되어야 합니다. 자세한 내용은 **Tier-1 게이트웨이 추가** 항목을 참조하십시오.

- 6 IPsec VPN 세션에 대해 인증서 기반 인증 모드를 사용 중인 경우 **사이트 인증서** 드롭다운 메뉴에서 로컬 끝점이 사용할 인증서를 선택합니다.
- 7 (선택 사항) 필요에 따라 **설명**에 설명을 추가합니다.
- 8 로컬 NSX Edge 인스턴스를 식별하는 데 사용되는 **로컬 ID** 값을 입력합니다.

이 로컬 ID는 원격 사이트의 피어 ID입니다. 로컬 ID는 원격 사이트의 공용 IP 주소이거나 FQDN이어야 합니다. 로컬 끝점을 사용하여 정의된 인증서 기반 VPN 세션의 경우 로컬 ID는 로컬 끝점과 연결된 인증서에서 파생됩니다. **로컬 ID** 텍스트 상자에 지정된 ID는 무시됩니다. VPN 세션의 인증서에서 파생된 로컬 ID는 인증서에 있는 확장에 따라 다릅니다.

- X509v3 확장 X509v3 Subject Alternative Name이 인증서에 없으면 DN(고유 이름)이 로컬 ID 값으로 사용됩니다.
- X509v3 확장 X509v3 Subject Alternative Name이 인증서에 있으면 주체 대체 이름 중 하나가 로컬 ID 값으로 사용됩니다.

- 9 신뢰할 수 있는 CA 인증서 및 인증서 해지 목록 드롭다운 메뉴에서 로컬 끝점에 필요한 적절한 인증서를 선택합니다.
- 10 필요하다면 태그를 지정합니다.
- 11 저장을 클릭합니다.

프로파일 추가

NSX-T Data Center는 IPsec VPN 또는 L2 VPN 서비스를 구성할 때 기본적으로 할당되는 시스템 생성 IPsec 터널 프로파일과 IKE 프로파일을 제공합니다. IPsec VPN 구성을 위해 시스템 생성 DPD 프로파일이 생성됩니다.

IKE 및 IPsec 프로파일은 네트워크 사이트 간에 공유 암호를 인증, 암호화 및 설정하는 데 사용되는 알고리즘에 대한 정보를 제공합니다. DPD 프로파일은 프로브 간 대기 시간(초)에 대한 정보를 제공합니다.

NSX-T Data Center에서 제공하는 기본 프로파일을 사용하지 않으려는 경우, 이 섹션에 나오는 항목의 정보를 사용하여 프로파일을 직접 구성할 수 있습니다.

IKE 프로파일 추가

IKE(Internet Key Exchange) 프로파일은 IKE 터널을 설정할 때 네트워크 사이트 간에 공유 암호를 인증, 암호화 및 설정하는 데 사용되는 알고리즘에 대한 정보를 제공합니다.

NSX-T Data Center는 IPsec VPN이나 L2 VPN 서비스를 구성할 때 기본적으로 할당되는 시스템 생성 IKE 프로파일을 제공합니다. 다음 표에는 제공된 기본 프로파일이 나열되어 있습니다.

표 5-4. IPsec VPN 또는 L2 VPN 서비스에 사용되는 기본 IKE 프로파일

기본 IKE 프로파일 이름	설명
nsx-default-l2vpn-ike-profile	<ul style="list-style-type: none"> ■ L2 VPN 서비스 구성에 사용됩니다. ■ IKE V2, AES 128 암호화 알고리즘, SHA2 256 알고리즘 및 Diffie-Hellman 그룹 14 키 교환 알고리즘을 사용하여 구성됩니다.
nsx-default-l3vpn-ike-profile	<ul style="list-style-type: none"> ■ IPsec VPN 서비스 구성에 사용됩니다. ■ IKE V2, AES 128 암호화 알고리즘, SHA2 256 알고리즘 및 Diffie-Hellman 그룹 14 키 교환 알고리즘을 사용하여 구성됩니다.

사용된 기본 IKE 프로파일 대신, NSX-T Data Center 2.5부터 지원되는 규정 준수 제품군 중 하나를 선택할 수도 있습니다. 자세한 내용은 지원되는 규정 준수 제품군 정보를 참조하십시오.

제공된 기본 IKE 프로파일 또는 규정 준수 제품군을 사용하지 않으려는 경우 다음 단계를 사용하여 고유한 IKE 프로파일을 구성할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > VPN > 프로파일** 탭을 클릭합니다.
- 3 **IKE 프로파일** 프로파일 유형을 선택하고 **IKE 프로파일 추가**를 클릭합니다.
- 4 IKE 프로파일의 이름을 입력합니다.
- 5 **IKE 버전** 드롭다운 메뉴에서 IPsec 프로토콜 집합에서 **SA(보안 연결)**를 설정하는 데 사용할 IKE 버전을 선택합니다.

표 5-5. IKE 버전

IKE 버전	설명
IKEv1	이 옵션을 선택하면 IPsec VPN이 시작되고 IKEv1 프로토콜에만 응답합니다.
IKEv2	이 버전은 기본값입니다. 이 옵션을 선택하면 IPsec VPN이 시작되고 IKEv2 프로토콜에만 응답합니다.
IKE-Flex	이 버전을 선택하고 IKEv2 프로토콜을 사용한 터널 설정이 실패하는 경우 소스 사이트는 폴백되지 않고 IKEv1 프로토콜을 사용한 연결이 시작됩니다. 대신, 원격 사이트가 IKEv1 프로토콜을 통해 연결을 시작하면 연결이 허용됩니다.

- 6 드롭다운 메뉴에서 암호화, 다이제스트 및 Diffie-Hellman 그룹 알고리즘을 선택합니다. 여러 알고리즘을 선택하여 적용하거나 적용하고 **않을** 알고리즘을 선택 취소할 수 있습니다.

표 5-6. 사용되는 알고리즘

알고리즘 유형	유효한 값	설명
암호화	<ul style="list-style-type: none"> ■ AES 128(기본값) ■ AES 256 ■ AES GCM 128 ■ AES GCM 192 ■ AES GCM 256 	<p>IKE(Internet Key Exchange) 협상 중 사용되는 암호화 알고리즘입니다.</p> <p>AES-GCM 알고리즘은 IKEv2에서 사용되도록 지원됩니다. IKEv1에서는 사용할 수 없습니다.</p>
다이제스트	<ul style="list-style-type: none"> ■ SHA2 256(기본값) ■ SHA 1 ■ SHA2 384 ■ SHA2 512 	<p>IKE 협상 중에 사용되는 보안 해싱 알고리즘입니다.</p> <p>AES-GCM이 암호화 알고리즘 텍스트 상자에서 선택한 유일한 암호화 알고리즘인 경우 RFC 5282의 섹션 8에 따라 다이제스트 알고리즘 텍스트 상자에 해시 알고리즘을 지정할 수 없습니다. 또한 PRF(Pseudo-Random Function) 알고리즘, PRF-HMAC-SHA2-256은 IKE SA(보안 연결) 협상에서 암시적으로 선택되고 사용됩니다. IKE SA 협상의 1단계가 성공하려면 피어 게이트웨이에 대해 PRF-HMAC-SHA2-256 알고리즘도 구성해야 합니다.</p> <p>암호화 알고리즘 텍스트 상자에 AES-GCM 알고리즘 외의 추가 알고리즘을 지정한 경우 다이제스트 알고리즘 텍스트 상자에서 하나 이상의 해시 알고리즘을 선택할 수 있습니다. 또한 IKE SA 협상에 사용되는 PRF 알고리즘은 구성된 해시 알고리즘에 따라 암시적으로 결정됩니다. IKE SA 협상의 1단계가 성공하려면 피어 게이트웨이에 대해 하나 이상의 일치하는 PRF 알고리즘도 구성해야 합니다. 예를 들어 암호화 알고리즘 텍스트 상자에 AES 128 및 AES GCM 128이 포함되어 있고, SHA1이 다이제스트 알고리즘 텍스트 상자에 지정된 경우, PRF-HMAC-SHA1 알고리즘이 IKE SA 협상 중에 사용됩니다. 이를 피어 게이트웨이에서도 구성해야 합니다.</p>
Diffie-Hellman 그룹	<ul style="list-style-type: none"> ■ 그룹 14(기본값) ■ 그룹 2 ■ 그룹 5 ■ 그룹 15 ■ 그룹 16 ■ 그룹 19 ■ 그룹 20 ■ 그룹 21 	<p>피어 사이트와 NSX Edge가 비보안 통신 채널을 통해 공유 암호를 설정하는 데 사용되는 암호화 체계입니다.</p>

참고 2개의 암호화 알고리즘 또는 2개의 다이제스트 알고리즘을 사용하여 GUARD VPN 클라이언트 (이전의 QuickSec VPN 클라이언트)와의 IPsec VPN 터널을 설정하려고 하면 GUARD VPN 클라이언트는 제안된 협상 목록에 추가 알고리즘을 추가합니다. 예를 들어 IPsec VPN 터널을 설정하는 데 사용하는 IKE 프로파일에 사용할 암호화 알고리즘으로 AES 128 및 AES 256을 지정하고, 다이제스트 알고리즘으로 SHA2 256 및 SHA2 512를 지정한 경우 GUARD VPN 클라이언트는 협상 목록에 AES 192 및 SHA2 384도 제안합니다. 이 경우 NSX-T Data Center는 IPsec VPN 터널을 설정할 때 선택한 첫 번째 암호화 알고리즘을 사용합니다.

- 7 기본값 86,400초(24시간)와 다르게 설정하려면 SA(보안 연결) 수명 값을 초 단위로 입력합니다.
- 8 설명을 제공하고 필요에 따라 태그를 추가합니다.
- 9 **저장**을 클릭합니다.

결과

새로운 행이 사용 가능한 IKE 프로파일 테이블에 추가됩니다. 시스템 이외에서 생성된 프로파일을 편집하거나 삭제하려면 점 3개 메뉴(*)를 클릭하고 사용 가능한 작업 목록에서 선택합니다.

IPsec 프로파일 추가

IPsec(인터넷 프로토콜 보안) 프로파일은 IPsec 터널을 설정할 때 네트워크 사이트 간에 공유 암호를 인증, 암호화 및 설정하는 데 사용되는 알고리즘에 대한 정보를 제공합니다.

NSX-T Data Center는 IPsec VPN이나 L2 VPN 서비스를 구성할 때 기본적으로 할당되는 시스템 생성 IPsec 프로파일을 제공합니다. 다음 표에는 제공된 기본 IPsec 프로파일이 나열되어 있습니다.

표 5-7. IPsec VPN 또는 L2 VPN 서비스에 사용되는 기본 IPsec 프로파일

기본 IPsec 프로파일의 이름	설명
nsx-default-l2vpn-tunnel-profile	<ul style="list-style-type: none"> ■ L2 VPN에 사용됩니다. ■ AES GCM 128 암호화 알고리즘 및 Diffie-Hellman 그룹 14 키 교환 알고리즘을 사용하여 구성됩니다.
nsx-default-l3vpn-tunnel-profile	<ul style="list-style-type: none"> ■ IPsec VPN에 사용됩니다. ■ AES GCM 128 암호화 알고리즘 및 Diffie-Hellman 그룹 14 키 교환 알고리즘을 사용하여 구성됩니다.

기본 IPsec 프로파일 대신, NSX-T Data Center 2.5부터 지원되는 규정 준수 제품군 중 하나를 선택할 수도 있습니다. 자세한 내용은 [지원되는 규정 준수 제품군 정보](#)를 참조하십시오.

제공된 기본 IPsec 프로파일 또는 규정 준수 제품군을 사용하지 않으려는 경우 다음 단계를 사용하여 직접 구성할 수 있습니다.

절차

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

- 2 **네트워킹 > VPN > 프로파일** 탭으로 이동합니다.
- 3 **IPSec 프로파일** 프로파일 유형을 선택하고 **IPSec 프로파일 추가**를 클릭합니다.
- 4 IPSec 프로파일의 이름을 입력합니다.
- 5 드롭다운 메뉴에서 암호화, 다이제스트 및 Diffie-Hellman 알고리즘을 선택합니다. 적용할 알고리즘을 여러 개 선택할 수 있습니다.
사용하지 않으려는 항목은 선택을 취소합니다.

표 5-8. 사용되는 알고리즘

알고리즘 유형	유효한 값	설명
암호화	<ul style="list-style-type: none"> ■ AES GCM 128(기본값) ■ AES 128 ■ AES 256 ■ AES GCM 192 ■ AES GCM 256 ■ 암호화 인증 AES GMAC 128 없음 ■ 암호화 인증 AES GMAC 192 없음 ■ 암호화 인증 AES GMAC 256 없음 ■ 암호화 없음 	IPSec(인터넷 프로토콜 보안) 협상 중 사용되는 암호화 알고리즘입니다.
다이제스트	<ul style="list-style-type: none"> ■ SHA 1 ■ SHA2 256 ■ SHA2 384 ■ SHA2 512 	IPSec 협상 중에 사용되는 보안 해싱 알고리즘입니다.
Diffie-Hellman 그룹	<ul style="list-style-type: none"> ■ 그룹 14(기본값) ■ 그룹 2 ■ 그룹 5 ■ 그룹 15 ■ 그룹 16 ■ 그룹 19 ■ 그룹 20 ■ 그룹 21 	피어 사이트와 NSX Edge가 비보안 통신 채널을 통해 공유 암호를 설정하는데 사용되는 암호화 체계입니다.

- 6 VPN 서비스에서 PFS 그룹 프로토콜을 사용하지 않으려면 **PFS 그룹** 선택을 취소합니다.
이 항목은 기본적으로 선택됩니다.
- 7 **SA 수명** 텍스트 상자에서 IPSec 터널을 다시 설정해야 하는 기본 경과 시간(초)을 수정합니다.
기본적으로 SA 수명은 24시간(86,400초)이 사용됩니다.
- 8 IPSec 터널에 사용할 **DF 비트**의 값을 선택합니다.
이 값은 수신된 데이터 패킷에 포함된 DF(Don't Fragment) 비트를 처리하는 방법을 결정합니다. 허용되는 값은 다음 표에 설명되어 있습니다.

표 5-9. DF 비트 값

DF 비트 값	설명
COPY	기본값입니다. 이 값을 선택하면 NSX-T Data Center는 수신된 패킷의 DF 비트 값을 전달된 패킷으로 복사합니다. 이 값은 수신된 데이터 패킷에 DF 비트가 설정되어 있으면 암호화 후 패킷에도 DF 비트가 설정되어 있음을 의미합니다.
CLEAR	이 값을 선택하면 NSX-T Data Center는 수신된 데이터 패킷의 DF 비트 값을 무시하고 암호화된 패킷에서 DF 비트는 항상 0입니다.

9 설명을 제공하고 필요한 경우 태그를 추가합니다.

10 **저장**을 클릭합니다.

결과

새로운 행이 사용 가능한 IPsec 프로파일 테이블에 추가됩니다. 시스템 이외에서 생성된 프로파일을 편집하거나 삭제하려면 점 3개 메뉴(⋮)를 클릭하고 사용 가능한 작업 목록에서 선택합니다.

DPD 프로파일 추가

DPD(Dead Peer Detection) 프로파일은 IPsec 피어의 활성 여부를 감지하기 위한 검색 간 대기 시간(초)에 대한 정보를 제공합니다.

NSX-T Data Center는 IPsec VPN 서비스를 구성할 때 기본적으로 할당되는 이름이 nsx-default-13vpn-dpd-profile인 시스템 생성 DPD 프로파일을 제공합니다.

제공된 기본 DPD 프로파일을 사용하지 않으려면 다음 단계에 따라 고유한 항목을 구성할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > VPN > 프로파일**로 이동합니다.
- 3 **DPD 프로파일** 프로파일 유형을 선택하고 **DPD 프로파일 추가**를 클릭합니다.
- 4 DPD 프로파일의 이름을 입력합니다.
- 5 **DPD 검색 간격** 텍스트 상자에 다음 DPD 검색을 보내기 전에 NSX-T Data Center에서 대기할 시간(초)을 입력합니다. 기본값은 60초입니다.

NSX Edge 노드가 원격 피어 사이트의 응답을 수신하는 경우 DPD 검색 간격 타이머가 다시 시작됩니다. NSX Edge 노드가 다음 DPD 검색이 전송되고 0.5초 내에 피어 사이트에서 응답을 다시 수신하지 못하면 재전송 타이머가 0.5초로 설정됩니다. NSX Edge 노드는 재전송 타이머에 도달한 후 다음 DPD 검색을 재전송합니다. 원격 피어 사이트가 계속 응답하지 않으면 재전송 타이머는 최대 제한 6초가 될 때까지 급격히 증가합니다. NSX Edge 노드는 재전송 타이머가 만료될 때마다 계속해서 DPD 검색을 재전송합니다. NSX Edge 노드는 피어 사이트를 비활성 상태로 선언하기 전에 최대 30회까지 재전송하며, 비활성 피어의 링크에서 SA(보안 연결)를 끊습니다. DPD 검색을 30회 재전송하는 데 소요되는 총 시간은 약 2분 45초입니다.

- 6 설명을 제공하고 필요에 따라 태그를 추가합니다.
- 7 **저장**을 클릭합니다.

결과

사용 가능한 DPD 프로파일의 테이블에 새 행이 추가됩니다. 시스템 이외에서 생성된 프로파일을 편집하거나 삭제하려면 점 3개 메뉴(⋮)를 클릭하고 사용 가능한 작업 목록에서 선택합니다.

자치 Edge를 L2 VPN 클라이언트로 추가

L2 VPN을 사용하여 계층 2 네트워크를 NSX-T Data Center에서 관리하지 않는 사이트로 확장할 수 있습니다. 자치 NSX Edge를 사이트에 L2 VPN 클라이언트로서 배포할 수 있습니다. 자치 NSX Edge는 배포가 간단하며, 쉽게 프로그래밍할 수 있고 고성능 VPN을 제공합니다. 자치 NSX Edge는 NSX-T Data Center에서 관리되지 않는 호스트에서 OVF 파일을 사용하여 배포됩니다. 기본 및 보조 자치 L2 VPN Edge 클라이언트를 배포하여 VPN 이중화를 위해 HA를 사용하도록 설정할 수도 있습니다.

사전 요구 사항

- 포트 그룹을 생성하고 호스트의 vSwitch에 바인딩합니다.
- 내부 L2 확장 포트에 대한 포트 그룹을 생성합니다.
- 추가하려는 L2 VPN 클라이언트 세션에 사용할 로컬 IP 및 원격 IP에 대한 IP 주소를 확보합니다.
- L2 VPN 서버 구성 중에 생성된 피어 코드를 확보합니다.

절차

- 1 vSphere Web Client를 사용하여 비 NSX 환경을 관리하는 vCenter Server에 로그인합니다.
- 2 **호스트 및 클러스터**를 선택하고 클러스터를 확장하여 사용 가능한 호스트를 표시합니다.
- 3 자치 NSX Edge를 설치할 호스트를 마우스 오른쪽 버튼으로 클릭하고 **OVF 템플릿 배포**를 선택합니다.
- 4 인터넷에서 OVF 파일을 다운로드하고 설치할 URL을 입력하거나 **찾아보기**를 클릭하여 컴퓨터에서 자치 NSX Edge OVF 파일이 있는 폴더를 찾은 후 **다음**을 클릭합니다.
- 5 **이름 및 폴더 선택** 페이지에서 자치 NSX Edge 이름을 입력하고 배포할 폴더 또는 데이터 센터를 선택합니다. **다음**을 클릭합니다.
- 6 **계산 리소스 선택** 페이지에서 계산 리소스의 대상을 선택합니다.
- 7 [OVF 템플릿 세부 정보] 페이지에서 템플릿 세부 정보를 검토하고 **다음**을 클릭합니다.
- 8 **구성** 페이지에서 배포 구성 옵션을 선택합니다.
- 9 **스토리지 선택** 페이지에서 구성 파일 및 디스크 파일을 저장할 위치를 선택합니다.

10 네트워크 선택 페이지에서 배포한 템플릿이 사용해야 할 네트워크를 구성합니다. 업링크 인터페이스에 대해 생성한 포트 그룹, L2 확장 포트에 대해 생성한 포트 그룹을 선택하고 HA 인터페이스를 시작합니다. 다음을 클릭합니다.

11 템플릿 사용자 지정 페이지에서 다음 값을 입력하고 다음을 클릭합니다.

- a CLI 관리자 암호를 입력하고 한 번 더 입력합니다.
- b CLI 사용 암호를 입력하고 한 번 더 입력합니다.
- c CLI 루트 암호를 입력하고 한 번 더 입력합니다.
- d 관리 네트워크의 IPv4 주소를 입력합니다.
- e 종료 인터페이스가 업링크 인터페이스의 포트 그룹을 사용하여 네트워크에 매핑되도록 VLAN ID, 종료 인터페이스, IP 주소 및 IP 접두사 길이에 대한 **외부 포트** 세부 정보를 입력합니다.

종료 인터페이스가 트렁크 포트 그룹에 연결된 경우 VLAN ID를 지정합니다. 예:

20,eth2,192.168.5.1,24. VLAN ID를 사용하여 포트 그룹을 구성하고 **외부 포트**에 대해 VLAN 0을 사용할 수도 있습니다.

- f (선택 사항) 고가용성을 구성하려면 종료 인터페이스가 해당 HA 네트워크에 매핑되는 **HA 포트** 세부 정보를 입력합니다.
- g (선택 사항) 자치 NSX Edge를 HA를 위한 보조 노드로 배포하는 경우 **이 자치 Edge를 보조 노드로 배포**를 선택합니다.

기본 노드와 동일한 OVF 파일을 사용하고 기본 노드의 IP 주소, 사용자 이름, 암호 및 지문을 입력합니다.

기본 노드의 지문을 검색하려면 기본 노드에 로그인하고 다음 명령을 실행합니다.

```
get certificate api thumbprint
```

기본 노드와 보조 노드의 VTEP IP 주소가 동일한 서브넷에 있고 동일한 포트 그룹에 연결되어 있는지 확인합니다. 배포를 완료하고 보조 Edge를 시작하면 기본 노드에 연결되어 Edge 클러스터를 구성합니다.

12 완료 준비 페이지에서 자치 Edge 설정을 검토하고 **완료**를 클릭합니다.

참고 배포 중에 오류가 발생하면 해당 날의 메시지가 CLI에 표시됩니다. API 호출을 사용하여 오류를 확인할 수도 있습니다.

```
GET https://<nsx-mgr>/api/v1/node/status
```

오류는 소프트 오류 및 하드 오류로 분류됩니다. API 호출을 사용하여 필요에 따라 소프트 오류를 해결합니다. API 호출을 사용하여 해당 날의 메시지를 지울 수 있습니다.

```
POST /api/v1/node/status?action=clear_bootup_error
```

13 자치 NSX Edge 장치의 전원을 켭니다.

- 14 자치 NSX Edge 클라이언트에 로그인합니다.
- 15 **L2VPN > 세션 추가**를 선택하고 다음 값을 입력합니다.
 - a 세션 이름을 입력합니다.
 - b 로컬 IP 주소와 원격 IP 주소를 입력합니다.
 - c L2VPN 서버에서 피어 코드를 입력합니다. 피어 코드 가져오기에 대한 자세한 내용은 [원격 측 L2 VPN 구성 파일 다운로드](#)를 참조하십시오.
- 16 **저장**을 클릭합니다.
- 17 **포트 > 포트 추가**를 선택하여 L2 확장 포트를 생성합니다.
- 18 이름, VLAN을 입력하고 종료 인터페이스를 선택합니다.
- 19 **저장**을 클릭합니다.
- 20 **L2VPN > 포트 연결**을 선택하고 다음 값을 입력합니다.
 - a 생성한 L2 VPN 세션을 선택합니다.
 - b 생성한 L2 확장 포트를 선택합니다.
 - c 터널 ID를 입력합니다.
- 21 **연결**을 클릭합니다.

여러 L2 네트워크를 확장해야 하는 경우 추가 L2 확장 포트를 생성하고 이를 세션에 연결할 수 있습니다.
- 22 브라우저를 사용하여 자치 NSX Edge에 로그인하거나 API 호출을 사용하여 L2VPN 세션의 상태를 확인합니다.

참고 L2VPN 서버 구성이 변경되면 피어 코드를 다시 다운로드하고 새 피어 코드로 세션을 업데이트해야 합니다.

IPSec VPN 세션의 인식된 상태 확인

IPSec VPN 세션에 대한 구성 업데이트 요청을 전송한 후 요청된 상태가 전송 노드의 NSX-T Data Center 로컬 제어부에서 처리되었는지 확인할 수 있습니다.

IPSec VPN 세션을 생성하면 IKE 프로파일, DPD 프로파일, 터널 프로파일, 로컬 끝점, IPSec VPN 서비스 및 IPSec VPN 세션과 같은 여러 엔티티가 생성됩니다. 이러한 엔티티는 모두 동일한 IPsecVPNSession 범위를 공유하므로 동일한 GET API 호출을 사용하여 IPSec VPN 세션의 모든 엔티티의 인식 상태를 가져올 수 있습니다. API만 사용하여 인식 상태를 확인할 수 있습니다.

사전 요구 사항

- IPSec VPN을 숙지합니다. [IPSec VPN 이해](#)의 내용을 참조하십시오.
- IPSec VPN이 구성되었는지 확인합니다. [IPSec VPN 서비스 추가](#)의 내용을 참조하십시오.

- NSX Manager API에 액세스할 수 있어야 합니다.

절차

- 1 POST, PUT 또는 DELETE 요청 API 호출을 전송합니다.

"""

예:

```
PUT https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/8dd1c386-9b2c-4448-85b8-51ff649fae4f
{
  "resource_type": "PolicyBasedIPSecVPNSession",
  "id": "8dd1c386-9b2c-4448-85b8-51ff649fae4f",
  "display_name": "Test RZ_UPDATED",
  "ipsec_vpn_service_id": "7adfa455-a6fc-4934-a919-f5728957364c",
  "peer_endpoint_id": "17263ca6-dce4-4c29-bd8a-e7d12bd1a82d",
  "local_endpoint_id": "91ebfa0a-820f-41ab-bd87-f0fb1f24e7c8",
  "enabled": true,
  "policy_rules": [
    {
      "id": "1026",
      "sources": [
        {
          "subnet": "1.1.1.0/24"
        }
      ],
      "logged": true,
      "destinations": [
        {
          "subnet": "2.1.4..0/24"
        }
      ],
      "action": "PROTECT",
      "enabled": true,
      "_revision": 1
    }
  ]
}
```

- 2 반환된 응답 헤더에서 x-nsx-requestid의 값을 찾아 복사합니다.

예:

```
x-nsx-requestid e550100d-f722-40cc-9de6-cf84d3da3ccb
```

- 3 다음 GET 호출을 사용하여 IPsec VPN 세션의 인식 상태를 요청합니다.

```
GET https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/<ipsec-vpn-session-id>/state?request_id=<request-id>
```

다음 API 호출은 이전 단계에서 사용된 예의 id 및 x-nsx-requestid 값을 사용합니다.

```
GET https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/8dd1c386-9b2c-4448-85b8-51ff649fae4f/state?
request_id=e550100d-f722-40cc-9de6-cf84d3da3ccb
```

다음은 인식 상태가 `in_progress`일 때 수신한 응답의 예입니다.

```
{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "fe651e63-04bd-43a4-a8ec-45381a3b71b9",
      "state": "in_progress",
      "failure_message": "CCP Id:ab5958df-d98a-468e-a72b-d89dcdae5346, Message:State realization is in progress at the node."
    },
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "ebeb174ac-e4f1-4135-ba72-3dd2eb7099e3",
      "state": "in_sync"
    }
  ],
  "state": "in_progress",
  "failure_message": "The state realization is in progress at transport nodes."
}
```

다음은 인식 상태가 `in_sync`일 때 수신한 응답의 예입니다.

```
{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "7046e8f4-a680-11e8-9bc3-020020593f59",
      "state": "in_sync"
    }
  ],
  "state": "in_sync"
}
```

다음은 인식 상태가 `unknown`일 때 수신한 가능한 응답의 예입니다.

```
{
  "state": "unknown",
  "failure_message": "Unable to get response from any CCP node. Please retry operation after some time."
}
```

```
{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "3e643776-5def-11e8-94ae-020022e7749b",
      "state": "unknown",
      "failure_message": "CCP Id:ab5958df-d98a-468e-a72b-d89dcdae5346, Message: Unable to get response from the node. Please retry operation after some time."
    },
    {
      "sub_system_type": "TransportNode",
```

```

        "sub_system_id": "4784ca0a-5def-11e8-93be-020022f94b73",
        "state": "in_sync"
    }
  ],
  "state": "unknown",
  "failure_message": "The state realization is unknown at transport nodes"
}

```

엔티티 DELETE 작업을 수행한 후 다음 예에서 표시된 대로 NOT_FOUND의 상태를 수신할 수 있습니다.

```

{
  "http_status": "NOT_FOUND",
  "error_code": 600,
  "module_name": "common-services",
  "error_message": "The operation failed because object identifier LogicalRouter/61746f54-7ab8-4702-93fe-6ddeb804 is missing: Object identifiers are case sensitive.."
}

```

세션과 연결된 IPsec VPN 서비스가 사용되지 않도록 설정된 경우 다음 예에 표시된 대로 BAD_REQUEST 응답이 수신됩니다.

```

{
  "httpStatus": "BAD_REQUEST",
  "error_code": 110199,
  "module_name": "VPN",
  "error_message": "VPN service f9cfe508-05e3-4e1d-b253-fed096bb2b63 associated with the session 8dd1c386-9b2c-4448-85b8-51ff649fae4f is disabled. Can not get the realization status."
}

```

VPN 세션 모니터링 및 문제 해결

IPsec 또는 L2 VPN 세션을 구성한 후 VPN 터널 상태를 모니터링하고 NSX Manager 사용자 인터페이스를 사용하여 보고된 터널 문제를 해결할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > VPN > IPsec 세션** 또는 **네트워킹 > VPN > L2 VPN 세션** 탭으로 이동합니다.
- 3 모니터링하거나 문제를 해결할 VPN 세션에 대한 행을 확장합니다.
- 4 VPN 터널 상태를 보려면 정보 아이콘을 클릭합니다.
[상태] 대화상자가 나타나고 사용 가능한 상태가 표시됩니다.
- 5 VPN 터널 트래픽 통계를 보려면 [상태] 열의 **통계 보기**를 클릭합니다.
[통계] 대화상자에 VPN 터널에 대한 트래픽 통계가 표시됩니다.
- 6 오류 통계를 보려면 [통계] 대화상자의 **더 보기** 링크를 클릭합니다.

7 통계 대화상자를 닫으려면 **닫기**를 클릭합니다.

네트워크 주소 변환

6

NAT(네트워크 주소 변환)는 하나의 IP 주소 공간을 다른 주소 공간에 매핑합니다. Tier-0 및 Tier-1 게이트웨이에서 NAT를 구성할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 게이트웨이에서 NAT 구성

게이트웨이에서 NAT 구성

Tier-0 또는 Tier-1 게이트웨이에서 SNAT(소스 NAT), DNAT(대상 NAT) 또는 재귀 NAT를 구성할 수 있습니다.

Tier-0 게이트웨이가 활성-활성 모드에서 실행 중인 경우 비대칭 경로가 문제를 유발할 수 있기 때문에 SNAT 또는 DNAT를 구성할 수 없습니다. 재귀 NAT(경우에 따라 상태 비저장 NAT라고도 함)만 구성할 수 있습니다. Tier-0 게이트웨이가 활성-대기 모드에서 실행 중인 경우 SNAT, DNAT 또는 재귀 NAT를 구성할 수 있습니다.

IP 주소 또는 주소 범위에 대해 SNAT 또는 DNAT를 사용하지 않도록 설정할 수도 있습니다. 주소에 여러 NAT 규칙이 있는 경우 우선 순위가 가장 높은 규칙이 적용됩니다.

참고 정책 기반 IPsec VPN이 구성된 Tier-1 게이트웨이에서는 DNAT가 지원되지 않습니다.

Tier-0 게이트웨이의 외부 인터페이스에서 구성된 SNAT는 Tier-1 게이트웨이에서 나가는 트래픽은 물론 Tier-0 게이트웨이의 다른 외부 인터페이스에서 나가는 트래픽을 처리합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > NAT**를 선택합니다.
- 3 게이트웨이를 선택합니다.
- 4 **NAT 규칙 추가**를 클릭합니다.
- 5 작업을 선택합니다.

Tier-1 게이트웨이의 경우 사용 가능한 작업은 **SNAT**, **DNAT**, **재귀**, **SNAT 없음** 및 **DNAT 없음**입니다.

활성-대기 모드의 Tier-0 게이트웨이의 경우 사용 가능한 작업은 **SNAT, DNAT, SNAT 없음** 및 **DNAT 없음**입니다.

활성-활성 모드의 Tier-0 게이트웨이의 경우 사용 가능한 작업은 **재귀**입니다.

6 서비스 열에서 **설정**을 클릭하여 서비스를 선택합니다.

7 (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.

8 **대상 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 **변환된 포트**에 대한 값을 입력합니다.

11 다음 옵션에서 방화벽 설정을 선택합니다.

- **외부 주소와 일치** - 패킷은 변환된 IP 주소와 변환된 포트의 조합과 일치하는 방화벽 규칙에 의해 처리됩니다.
 - SNAT의 경우 외부 주소는 NAT가 완료된 후 변환된 소스 주소입니다.
 - DNAT의 경우 외부 주소는 NAT가 완료되기 전의 원래 대상 주소입니다.
 - REFLEXIVE의 경우 트래픽을 송신하기 위해 NAT가 완료된 후 방화벽이 변환된 소스 주소에 적용됩니다. 수신 트래픽의 경우 NAT가 완료되기 전에 방화벽이 원래 대상 주소에 적용됩니다.
- **내부 주소와 일치** - 패킷은 원래 IP 주소와 원래 포트의 조합과 일치하는 방화벽 규칙에 의해 처리됩니다.
 - SNAT의 경우 내부 주소는 NAT가 완료되기 전에 원본 소스 주소입니다.
 - DNAT의 경우 외부 주소는 NAT가 완료된 후의 변환된 대상 주소입니다.
 - REFLEXIVE의 경우 송신 트래픽에서 NAT가 완료되기 전에 방화벽이 원래 소스 주소에 적용됩니다. 수신 트래픽의 경우 NAT가 완료된 후 방화벽이 변환된 대상 주소에 적용됩니다.
- **우회** - 패킷은 방화벽 규칙을 우회합니다.

12 (필수 사항) 로깅 상태를 변경합니다.

13 (필수 사항) **적용 대상**의 경우 이 규칙이 적용되는 개체를 선택합니다.

사용 가능한 개체는 **Tier-0 게이트웨이, 인터페이스, 레이블, 서비스 인스턴스 끝점** 및 **가상 끝점**입니다.

14 우선 순위 값을 지정합니다.

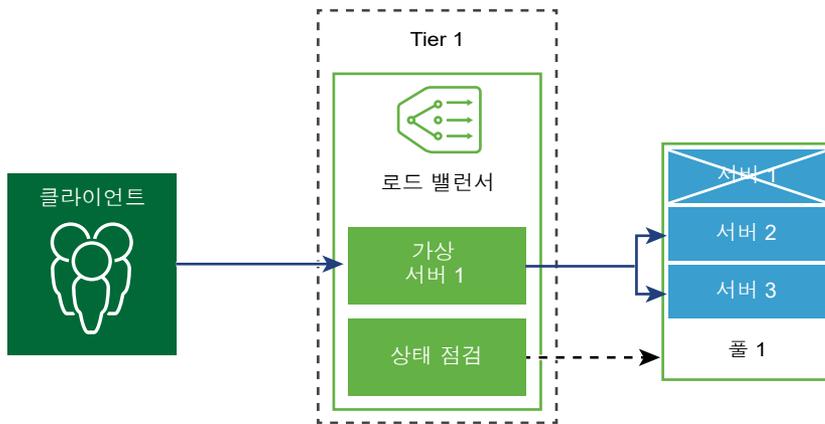
값이 낮을수록 우선 순위가 더 높습니다. 기본값은 100입니다.

15 **저장**을 클릭합니다.

로드 밸런싱

7

NSX-T Data Center 논리적 로드 밸런서는 애플리케이션에고가용성 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 게이트웨이에만 지원됩니다. 하나의 로드 밸런서는 하나의 Tier-1 게이트웨이에만 연결할 수 있습니다.

본 장은 다음 항목을 포함합니다.

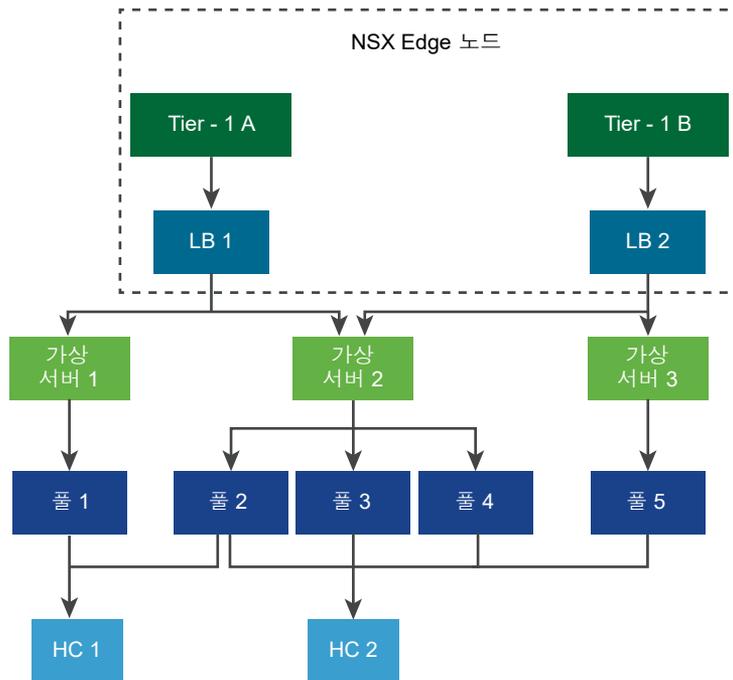
- 키 로드 밸런서 개념
- 로드 밸런서 구성 요소 설정
- 서버 풀 및 가상 서버에 대해 생성되는 그룹

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 밸런서를 구성할 때 크기(소형, 중형 또는 대형)를 지정할 수 있습니다. 크기는 로드 밸런서가 지원할 수 있는 가상 서버, 서버 풀 및 풀 멤버의 수를 결정합니다.

로드 밸런서는 활성-대기 모드에 있어야 하는 Tier-1 게이트웨이에서 실행됩니다. 게이트웨이는 NSX Edge 노드에서 실행됩니다. NSX Edge 노드의 폼 팩터(베어메탈, 소형, 중형 또는 대형)는 NSX Edge 노드가 지원할 수 있는 로드 밸런서의 수를 결정합니다. **고급 네트워킹 및 보안** 탭에서 논리적 라우터라는 용어는 게이트웨이를 가리키는 데 사용됩니다.

다양한 로드 밸런싱 크기 및 NSX Edge 폼 팩터 지원에 대한 자세한 내용은 <https://configmax.vmware.com>을 참조하십시오.

운영 환경에서는 소형 NSX Edge 노드를 사용하여 소형 로드 밸런서를 실행하지 않는 것이 좋습니다.

NSX Edge 노드의 로드 밸런서 사용량 정보를 가져오기 위해 API를 호출할 수 있습니다. **네트워킹** 탭을 사용하여 로드 밸런싱을 구성하는 경우 다음 명령을 실행합니다.

```
GET /policy/api/v1/infra/lb-node-usage?node_path=<node-path>
```

고급 네트워킹 및 보안 탭을 사용하여 로드 밸런싱을 구성하는 경우 다음 명령을 실행합니다.

```
GET /api/v1/loadbalancer/usage-per-node/<node-id>
```

사용량 정보에는 노드에 구성된 로드 밸런서 개체(로드 밸런서 서비스, 가상 서버, 서버 풀 및 풀 멤버) 수가 포함됩니다. 자세한 정보는 "NSX-T Data Center API 가이드" 를 참조하십시오.

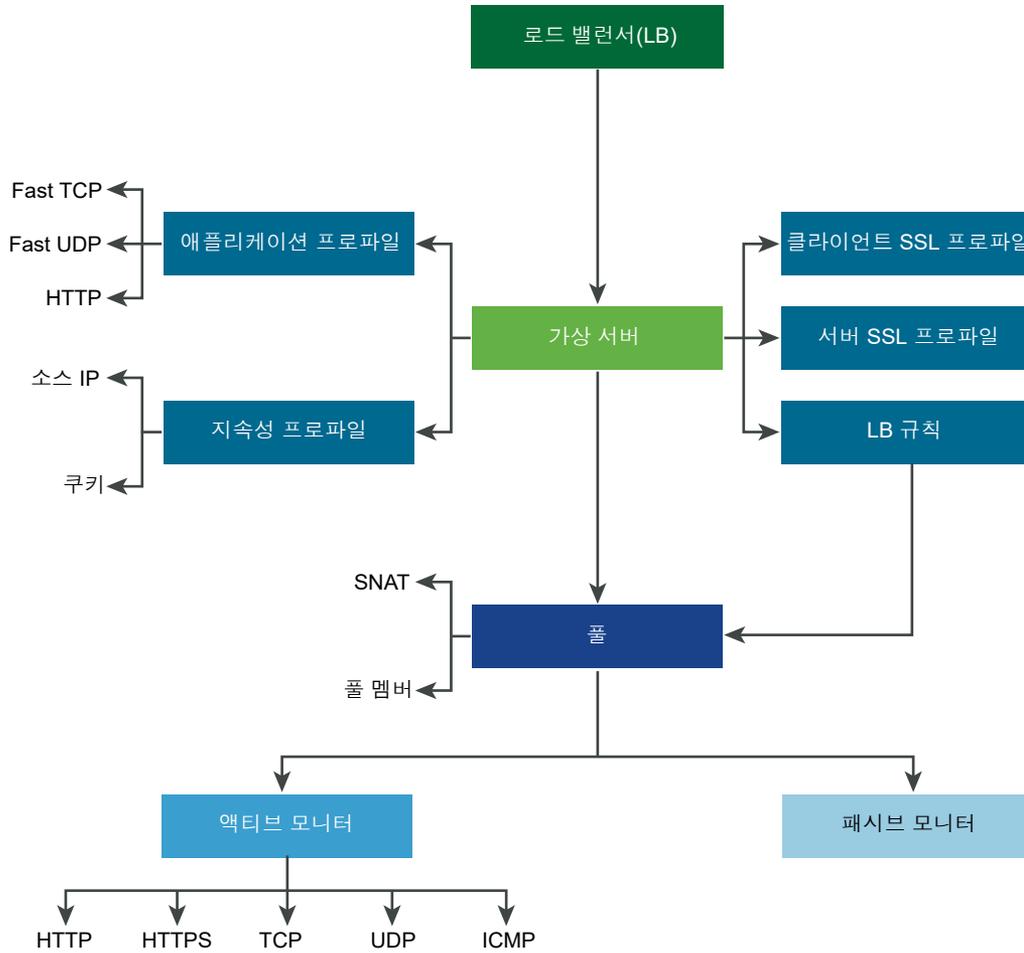
지원되는 로드 밸런서 기능

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 Limited Export 릴리스에서 지원되지 않습니다.

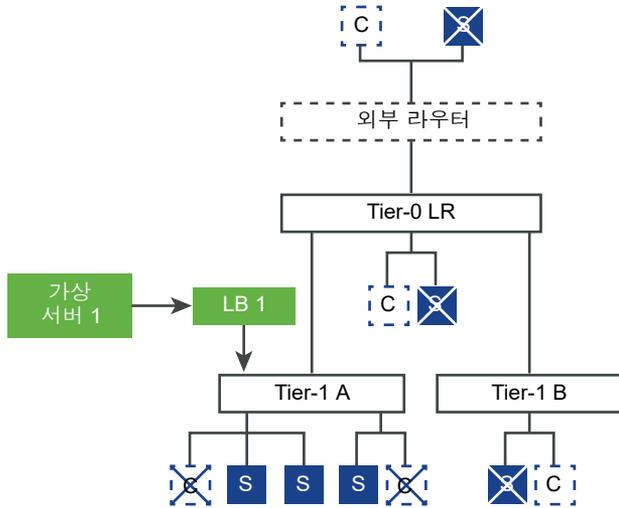


로드 밸런서 토폴로지

로드 밸런서는 일반적으로 인라인 또는 단일 암 모드로 배포됩니다. 단일 암 모드에는 가상 서버 SNAT(소스 NAT) 구성이 필요하지만 인라인 모드에서는 그렇지 않습니다.

인라인 토폴로지

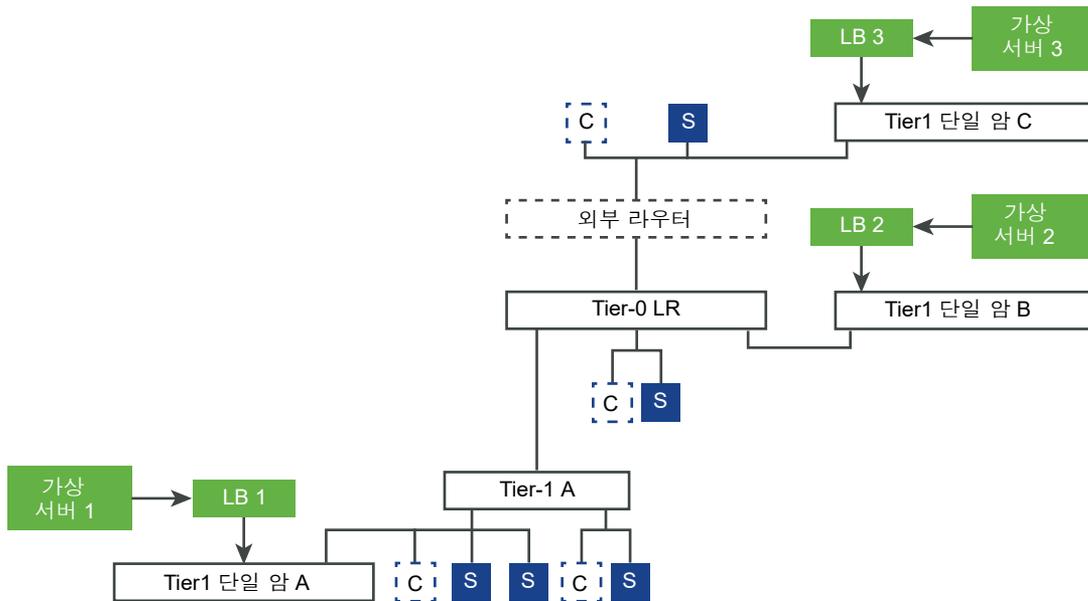
인라인 모드에서 로드 밸런서는 클라이언트와 서버 사이의 트래픽 경로에 있습니다. 로드 밸런서에서 SNAT를 사용하지 않으려는 경우 클라이언트 및 서버를 동일한 Tier-1 논리적 라우터의 오버레이 세그먼트에 연결하면 안 됩니다. 클라이언트와 서버가 동일한 Tier-1 논리적 라우터의 오버레이 세그먼트에 연결된 경우 SNAT가 필요합니다.



단일 암 토폴로지

단일 암 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 암 모드에서 로드 밸런서는 서버 응답이 로드 밸런서로 항상 전송되도록 클라이언트 IP 주소를 로드 밸런서 IP 주소로 바꿉니다. 로드 밸런서는 클라이언트로 응답을 전달합니다.



Tier-1 서비스 체인

Tier-1 게이트웨이 또는 논리적 라우터가 NAT, 방화벽 및 로드 밸런서 등의 여러 다른 서비스를 호스팅하는 경우 서비스는 다음과 같은 순서로 적용됩니다.

- 수신

DNAT - 방화벽 - 로드 밸런서

참고: DNAT가 방화벽 우회로 구성된 경우에는 방화벽을 건너뛰고 로드 밸런서는 건너뛰지 않습니다.

- 송신

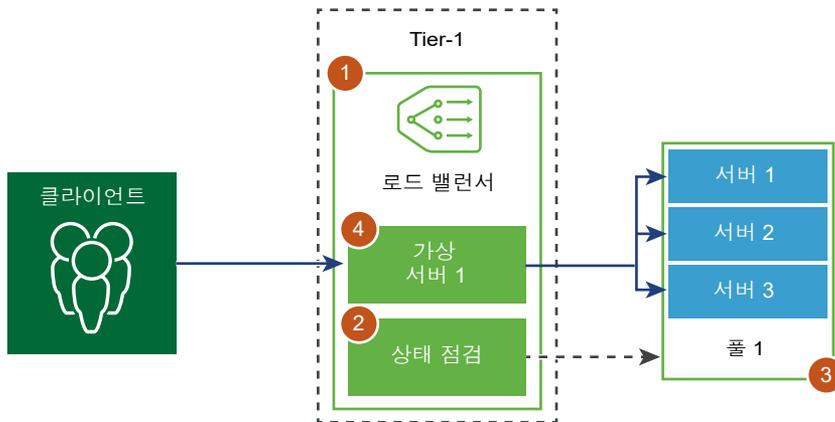
로드 밸런서 - 방화벽 - SNAT

로드 밸런서 구성 요소 설정

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

참고 고급 및 보안 탭에서 Tier-1 논리적 라우터라는 용어는 Tier-1 게이트웨이를 가리키는 데 사용됩니다.

그런 다음 서버에 대한 상태 점검 모니터링을 설정합니다. 그 후, 로드 밸런서에 대한 서버 풀을 구성해야 합니다. 마지막으로 로드 밸런서에 대한 계층 4 또는 계층 7 가상 서버를 생성하고 새로 생성된 가상 서버를 로드 밸런서에 연결해야 합니다.



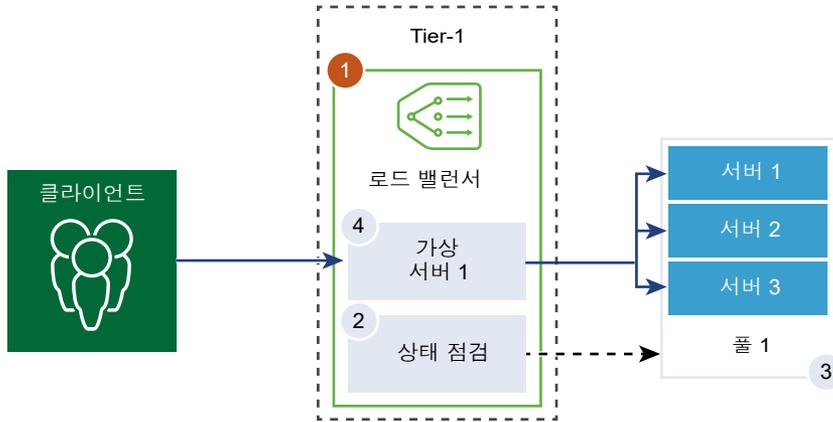
로드 밸런서 추가

로드 밸런서는 생성되어 Tier-1 게이트웨이에 연결됩니다.

참고 고급 및 보안 탭에서 Tier-1 논리적 라우터라는 용어는 Tier-1 게이트웨이를 가리키는 데 사용됩니다.

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 게이트웨이가 구성되어 있는지 확인합니다. [장 3 Tier-1 게이트웨이의 내용을 참조하십시오.](#)

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > 로드 밸런싱 > 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 이 로드 밸런서에 연결할 이미 구성된 Tier-1 게이트웨이를 선택합니다.
Tier-1 게이트웨이는 활성-대기 모드여야 합니다.
- 6 드롭다운 메뉴에서 오류 로그의 심각도 수준을 정의합니다.
로드 밸런서는 다양한 심각도 수준의 발생한 문제에 대한 정보를 오류 로그에 수집합니다.
- 7 (선택 사항) 더 쉬운 검색을 위해 태그를 입력합니다.
태그를 지정하여 태그의 범위를 설정할 수 있습니다.
- 8 **저장**을 클릭합니다.
로드 밸런서 생성 및 Tier-1 게이트웨이에 로드 밸런서 연결은 약 3분이 소요되며 구성 상태가 녹색이고 [실행 중]으로 표시됩니다.
상태가 [종료됨]인 경우 계속하기 전에 정보 아이콘을 클릭하여 오류를 해결합니다.
- 9 (선택 사항) 로드 밸런서를 삭제합니다.
 - a 가상 서버 및 Tier-1 게이트웨이에서 로드 밸런서를 분리합니다.
 - b 로드 밸런서를 선택합니다.

- c 세로 말줄임표 버튼을 클릭합니다.
- d 삭제를 선택합니다.

액티브 모니터 추가

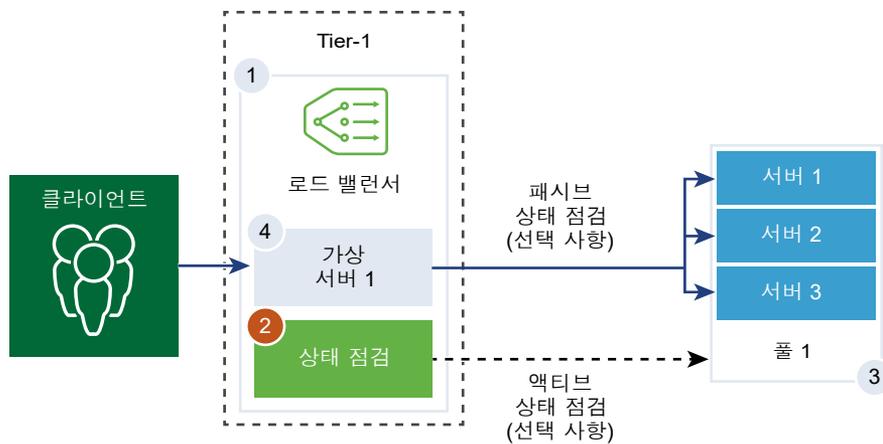
액티브 상태 모니터는 서버가 사용 가능한지 여부를 테스트하는 데 사용됩니다. 액티브 상태 모니터는 서버에 기본 ping을 보내거나 애플리케이션 상태를 모니터링하기 위해 고급 HTTP 요청을 보내는 등 여러 유형의 테스트를 사용합니다.

참고 고급 및 보안 탭에서 Tier-1 논리적 라우터라는 용어는 Tier-1 게이트웨이를 가리키는 데 사용됩니다.

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 게이트웨이에 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 **네트워킹 > 로드 밸런싱 > 모니터 > 액티브 > 액티브 모니터 추가**를 선택합니다.
- 3 드롭다운 메뉴에서 서버의 프로토콜을 선택합니다.

NSX Manager에 대해 HTTP, HTTPS, ICMP, TCP 및 UDP와 같은 미리 정의된 프로토콜을 사용할 수도 있습니다.

- 4 **HTTP** 프로토콜을 선택합니다.

5 서비스 폴을 모니터링할 값을 구성합니다.

액티브 상태 모니터 기본값을 수락할 수도 있습니다.

옵션	설명
이름 및 설명	액티브 상태 모니터에 대한 설명과 이름을 입력합니다.
모니터링 포트	모니터링 포트의 값을 설정합니다.
모니터링 간격	모니터가 서버에 또 다른 연결 요청을 보내는 시간을 초 단위로 설정합니다.
시간 초과 기간	서버를 [중요] 상태로 간주하기 전에 테스트할 시간을 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.
태그	더 쉬운 검색을 위해 태그를 입력합니다. 태그를 지정하여 태그의 범위를 설정할 수 있습니다.

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.

6 구성을 클릭합니다.

7 HTTP 요청 및 응답 구성 세부 정보를 입력합니다.

옵션	설명
HTTP 메서드	드롭다운 메뉴에서 서버 상태를 감지할 메서드를 GET, OPTIONS, POST, HEAD 및 PUT 중에서 선택합니다.
HTTP 요청 URL	메서드에 대한 요청 URI를 입력합니다.
HTTP 요청 버전	드롭다운 메뉴에서 지원되는 요청 버전을 선택합니다. 기본 버전인 HTTP_VERSION_1을 수락할 수도 있습니다.
HTTP 응답 헤더	추가를 클릭하고 HTTP 응답 헤더 이름과 해당 값을 입력합니다. 기본 헤더 값은 4000입니다. 최대 헤더 값은 64000입니다.
HTTP 요청 본문	요청 본문을 입력합니다. POST 및 PUT 메서드에 유효합니다.
HTTP 응답 코드	모니터가 HTTP 응답 본문의 상태 줄에서 일치할 것으로 예상하는 문자열을 입력합니다. 응답 코드는 쉼표로 구분된 목록입니다. 예: 200,301,302,401.
HTTP 응답 본문	HTTP 응답 본문 문자열과 HTTP 상태 점검 응답 본문이 일치하면 서버는 정상으로 간주됩니다.

8 HTTPS 프로토콜을 선택합니다.

- 9 5단계를 완료합니다.
- 10 구성을 클릭합니다.
- 11 HTTP 요청 및 응답, SSL 구성 세부 정보를 입력합니다.

옵션	설명
이름 및 설명	액티브 상태 모니터에 대한 설명과 이름을 입력합니다.
HTTP 메서드	드롭다운 메뉴에서 서버 상태를 감지할 메서드를 GET, OPTIONS, POST, HEAD 및 PUT 중에서 선택합니다.
HTTP 요청 URL	메서드에 대한 요청 URI를 입력합니다.
HTTP 요청 버전	드롭다운 메뉴에서 지원되는 요청 버전을 선택합니다. 기본 버전인 HTTP_VERSION_1을 수락할 수도 있습니다.
HTTP 응답 헤더	추가 를 클릭하고 HTTP 응답 헤더 이름과 해당 값을 입력합니다. 기본 헤더 값은 4000입니다. 최대 헤더 값은 64000입니다.
HTTP 요청 본문	요청 본문을 입력합니다. POST 및 PUT 메서드에 유효합니다.
HTTP 응답 코드	모니터가 HTTP 응답 본문의 상태 줄에서 일치할 것으로 예상하는 문자열을 입력합니다. 응답 코드는 쉼표로 구분된 목록입니다. 예: 200,301,302,401.
HTTP 응답 본문	HTTP 응답 본문 문자열과 HTTP 상태 점검 응답 본문이 일치하면 서버는 정상으로 간주됩니다.
서버 SSL	버튼을 전환하여 SSL 서버를 사용하도록 설정합니다.
클라이언트 인증서	(선택 사항) 서버가 동일한 IP 주소에서 여러 호스트 이름을 호스팅하지 않거나 클라이언트가 SNI 확장을 지원하지 않는 경우 사용할 인증서를 드롭다운 메뉴에서 선택합니다.
서버 SSL 프로파일	(선택 사항) 재사용 가능하고 애플리케이션 독립적인 클라이언트 측 SSL 속성을 정의하는 기본 SSL 프로파일을 드롭다운 메뉴에서 할당합니다. 세로 줄임표를 클릭하고 사용자 지정 SSL 프로파일을 생성합니다.
신뢰할 수 있는 CA 인증서	(선택 사항) 클라이언트가 인증을 위해 CA 인증서를 가지도록 요청할 수 있습니다.
필수 서버 인증	(선택 사항) 버튼을 전환하여 서버 인증을 사용하도록 설정합니다.
인증서 체인 수준	(선택 사항) 클라이언트 인증서 체인에 대한 인증 깊이를 설정합니다.
인증서 해지 목록	(선택 사항) 손상된 클라이언트 인증서를 거부하도록 클라이언트 측 SSL 프로파일에서 CRL(인증서 해지 목록)을 설정합니다.

- 12 ICMP 프로토콜을 선택합니다.
- 13 5단계를 완료하고 ICMP 상태 점검 패킷의 데이터 크기를 바이트 단위로 할당합니다.
- 14 TCP 프로토콜을 선택합니다.

15 5단계를 완료하고 TCP 데이터 매개 변수를 비워 둘 수 있습니다.

전송되는 데이터와 예상되는 데이터가 모두 나열되지 않으면 서버 상태를 검사하기 위해 3방향 핸드셰이크 TCP 연결이 설정됩니다. 데이터가 전송되지 않습니다.

예상되는 데이터(나열된 경우)는 문자열이어야 합니다. 정규식은 지원되지 않습니다.

16 UDP 프로토콜을 선택합니다.

17 5단계를 완료하고 UDP 데이터를 구성합니다.

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.

다음에 수행할 작업

액티브 상태 모니터를 서버 풀과 연결합니다. 서버 풀 추가의 내용을 참조하십시오.

패시브 모니터 추가

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 밸런싱 > 모니터 > 패시브 > 패시브 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.
태그	더 쉬운 검색을 위해 태그를 입력합니다. 태그를 지정하여 태그의 범위를 설정할 수 있습니다.

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.

다음에 수행할 작업

패시브 상태 모니터를 서버 풀과 연결합니다. **서버 풀 추가**의 내용을 참조하십시오.

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.

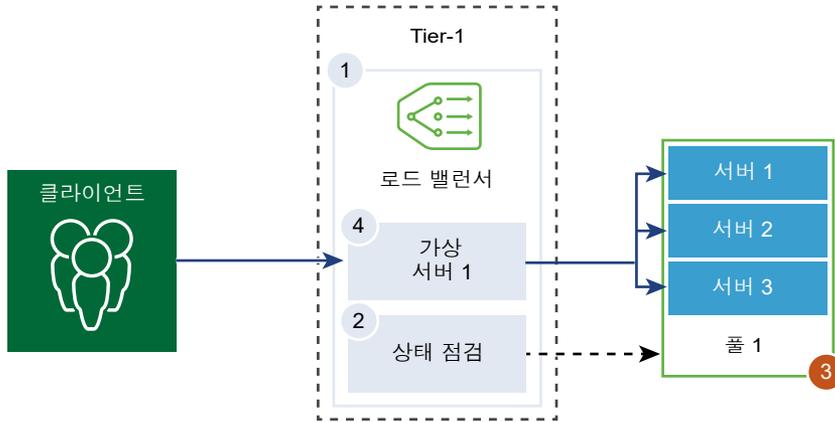
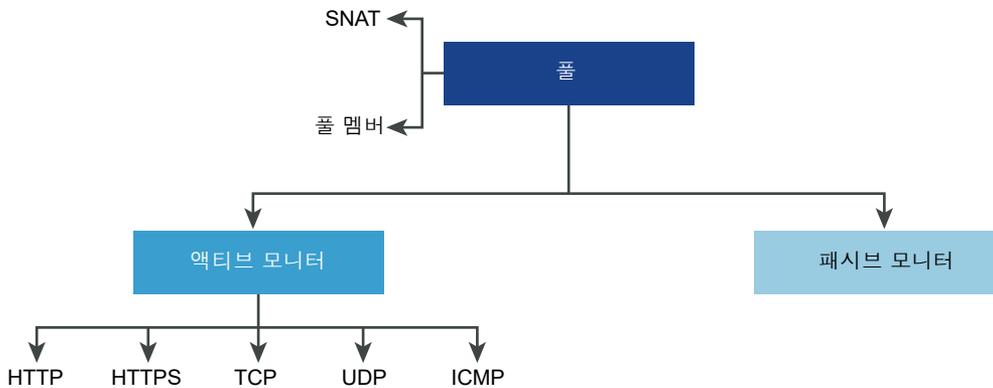


그림 7-1. 서버 풀 매개 변수 구성



사전 요구 사항

- 동적 풀 멤버를 사용하는 경우 NSGroup을 구성해야 합니다. NSGroup 생성의 내용을 참조하십시오.
- 패시브 상태 모니터가 구성되어 있는지 확인합니다. 패시브 모니터 추가의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(https://<nsx-manager-ip-address>)에 로그인합니다.
- 2 **네트워킹 > 로드 밸런싱 > 서버 풀 > 서버 풀 추가**를 선택합니다.
- 3 로드 밸런서 서버 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 건너뛸니다.
 - 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
ROUND_ROBIN	들어오는 클라이언트 요청이 요청을 처리할 수 있는 사용 가능한 서버 목록을 통해 순환됩니다. 서버 풀 멤버 가중치가 구성되어 있어도 무시합니다.
WEIGHTED_ROUND_ROBIN	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 리소스간에 로드를 균등하게 분산하는 데 중점을 둡니다.
LEAST_CONNECTION	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.
WEIGHTED_LEAST_CONNECTION	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 간에 로드를 분산하는 데 중점을 둡니다. 기본적으로 가중치 값은 해당 값이 구성되지 않았으며 느린 시작이 사용되도록 설정된 경우 1입니다.
IP-HASH	소스 IP 주소의 해시와 실행 중인 모든 서버의 총 가중치에 따라 서버를 선택합니다.

5 서버 풀 멤버를 선택합니다.

서버 풀은 단일 또는 여러 풀 멤버로 구성됩니다.

옵션	설명
<p>개별 멤버 입력</p>	<p>풀 멤버 이름, IP주소 및 포트를 입력합니다.</p> <p>각 서버 풀 멤버에는 로드 밸런싱 알고리즘에 사용할 가중치를 구성할 수 있습니다. 가중치는 동일한 풀에 있는 다른 구성원에 비해 지정된 풀 멤버가 처리할 수 있는 로드의 양을 나타냅니다.</p> <p>서버 풀 관리 상태를 설정할 수 있습니다. 기본적으로 서버 풀 멤버가 추가되면 이 옵션은 사용하도록 설정됩니다.</p> <p>이 옵션을 사용하지 않도록 설정하면 활성 연결이 처리되고 새 연결에 대해 서버 풀 멤버가 선택되지 않습니다. 새 연결은 풀의 다른 멤버에 할당됩니다.</p> <p>정상적으로 사용하지 않도록 설정되면, 유지 보수를 위해 서버를 제거할 수 있습니다. 이 상태의 서버 풀에 포함된 멤버에 대한 기존 연결은 계속 처리됩니다.</p> <p>버튼을 전환하여 풀 멤버를 백업 멤버로 지정하고 상태 모니터를 사용하여 액티브-대기 상태를 제공합니다. 트래픽 페일오버는 활성 멤버가 상태 점검을 실패하는 경우 백업 멤버에 대해 발생합니다. 서버 선택 중에 백업 멤버는 건너뛴니다. 서버 풀이 비활성 상태이면, 수신 연결은 애플리케이션을 사용할 수 없음을 나타내는 장애 페이지로 구성된 백업 멤버에게만 전송됩니다.</p> <p>[최대 동시 연결 수] 값은 서버 선택 시 서버 풀 멤버가 오버로드되지 않고 건너뛰도록 연결 최대 값을 지정합니다. 값을 지정하지 않으면 연결에 제한이 없습니다.</p>
<p>그룹 선택</p>	<p>미리 구성된 서버 풀 멤버 그룹을 선택합니다.</p> <p>그룹 이름과 설명(선택 사항)을 입력합니다.</p> <p>기존 목록에서 계산 멤버를 설정하거나 새로 만듭니다. 멤버 자격 조건을 지정하고, 그룹 멤버를 선택하고, IP 및 MAC 주소를 그룹 멤버로 추가하고, Active Directory 그룹을 추가할 수 있습니다. ID 멤버는 계산 멤버와 교차하여 그룹의 멤버 자격을 정의합니다.</p> <p>더 쉬운 검색을 위해 태그를 입력합니다. 태그를 지정하여 태그의 범위를 설정할 수 있습니다.</p> <p>선택적으로 최대 그룹 IP 주소 목록을 정의할 수 있습니다.</p>

6 드롭다운 메뉴에서 서버 풀에 대한 액티브 상태 점검 모니터를 선택합니다.

로드 밸런서는 주기적으로 서버에 ICMP ping을 전송하여 데이터 트래픽과 독립적으로 상태를 확인합니다. 서버 풀 마다 액티브 상태 점검 모니터를 하나만 구성할 수 있습니다.

7 SNAT(소스 NAT) 변환 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
자동 맵 모드	<p>로드 밸런서는 인터페이스 IP 주소 및 사용 후 삭제 포트를 사용하여 서버의 설정된 수신 포트 중 하나에 처음에 연결된 클라이언트와 통신을 계속합니다.</p> <p>SNAT가 필요합니다.</p> <p>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.</p> <p>또한 포트 오버로드 팩터를 설정하여 여러 연결에 동시에 포트를 사용할 수 있는 최대 횟수를 허용할 수 있습니다.</p>
사용 안 함	SNAT 변환 모드를 사용하지 않도록 설정합니다.
IP 풀	<p>풀의 서버 중 하나에 연결할 때 SNAT에 사용할 단일 IP 주소 범위(예: 1.1.1.1-1.1.1.10)를 지정합니다.</p> <p>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.</p> <p>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.</p> <p>또한 포트 오버로드 팩터를 설정하여 여러 연결에 동시에 포트를 사용할 수 있는 최대 횟수를 허용할 수 있습니다.</p>

8 버튼을 전환하여 TCP 멀티플렉싱을 사용하도록 설정합니다.

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

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

10 서버 풀이 항상 유지해야 하는 활성 멤버의 최소 수를 입력합니다.

11 드롭다운 메뉴에서 서버 풀에 대한 패시브 상태 모니터를 선택합니다.

12 더 쉬운 검색을 위해 태그를 입력합니다.

태그를 지정하여 태그의 범위를 설정할 수 있습니다.

가상 서버 구성 요소 설정

계층 4 및 계층 7 가상 서버를 설정하고 애플리케이션 프로파일, 영구 프로파일 및 로드 밸런서 규칙과 같은 몇 가지 가상 서버 구성 요소를 구성할 수 있습니다.

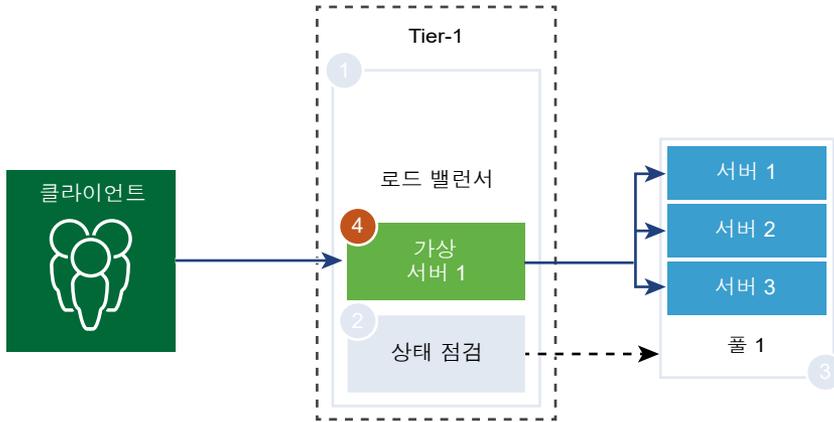
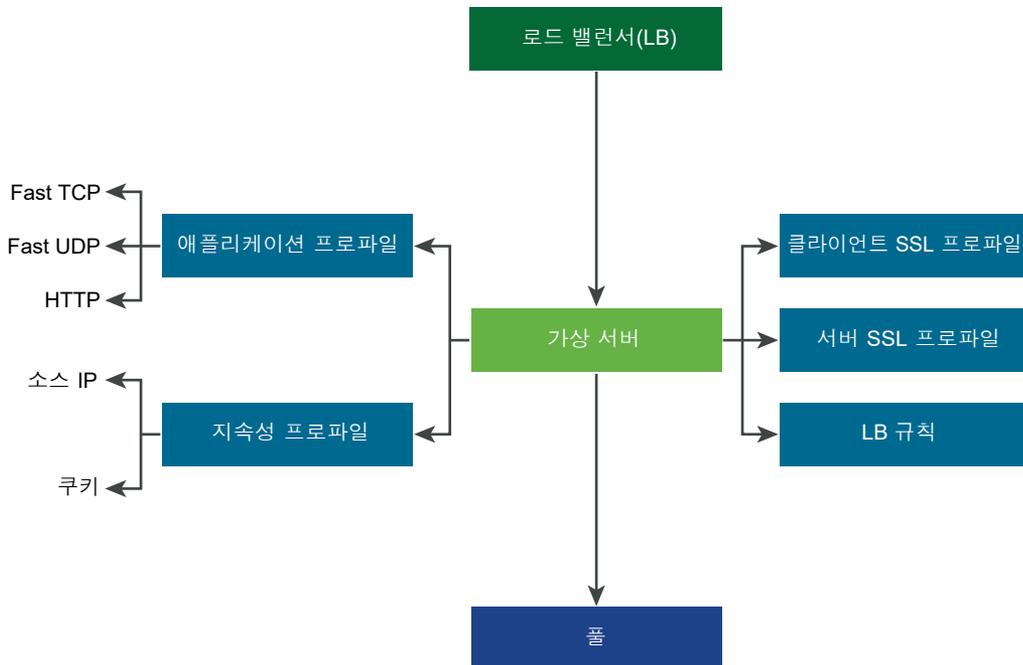


그림 7-2. 가상 서버 구성 요소



애플리케이션 프로파일 추가

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 중지하는 경우) HTTP 및 HTTPS 애플리케이션 모두에 사용됩니다. TCP 애플리케이션 프로파일과 달리 HTTP 애플리케이션 프로파일은 서버 풀 멤버를 선택하기 전에 클라이언트 TCP 연결을 중지합니다.

그림 7-3. 계층 4 TCP 및 UDP 애플리케이션 프로파일

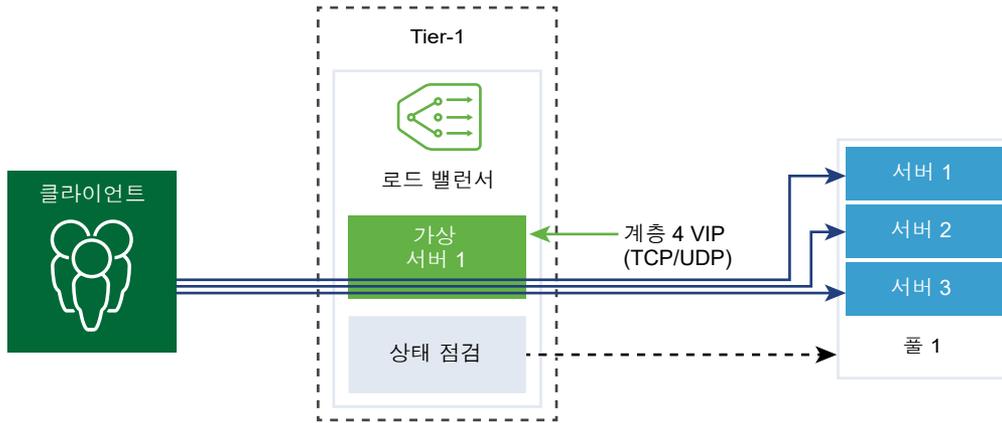
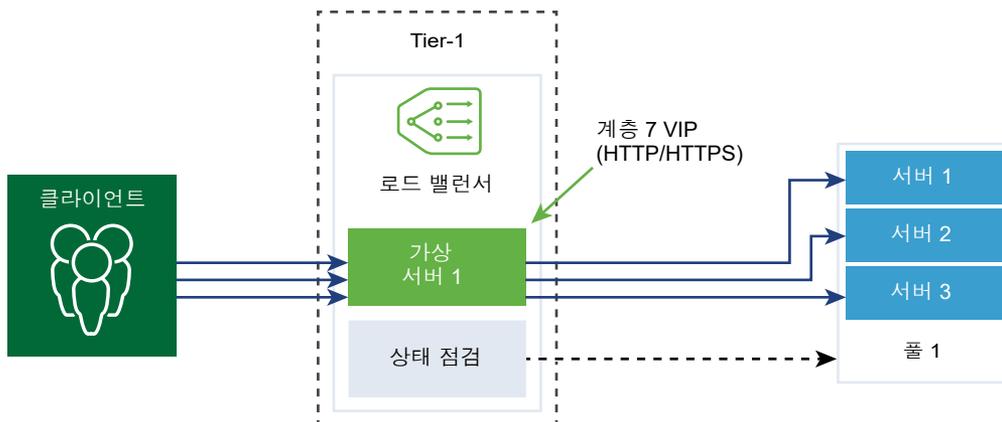


그림 7-4. 계층 7 HTTPS 애플리케이션 프로파일



절차

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

3 빠른 TCP 애플리케이션 프로파일을 선택하고 프로파일 세부 정보를 입력합니다.

빠른 TCP 프로파일 설정 기본값을 수락할 수도 있습니다.

옵션	설명
이름 및 설명	빠른 TCP 애플리케이션 프로파일에 대한 설명과 이름을 입력합니다.
유휴 시간 제한	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.
HA 흐름 미러링	버튼을 전환하여 연결된 가상 서버에 대한 모든 흐름을 HA 대기 노드로 미러링합니다.
연결 닫기 시간 제한	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.
태그	더 쉬운 검색을 위해 태그를 입력합니다. 태그를 지정하여 태그의 범위를 설정할 수 있습니다.

4 빠른 UDP 애플리케이션 프로파일을 선택하고 프로파일 세부 정보를 입력합니다.

UDP 프로파일 설정 기본값을 수락할 수도 있습니다.

옵션	설명
이름 및 설명	빠른 UDP 애플리케이션 프로파일에 대한 설명과 이름을 입력합니다.
유휴 시간 제한	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.
HA 흐름 미러링	버튼을 전환하여 연결된 가상 서버에 대한 모든 흐름을 HA 대기 노드로 미러링합니다.
태그	더 쉬운 검색을 위해 태그를 입력합니다. 태그를 지정하여 태그의 범위를 설정할 수 있습니다.

5 HTTP 애플리케이션 프로파일을 선택하고 프로파일 세부 정보를 입력합니다.

HTTP 프로파일 설정 기본값을 수락할 수도 있습니다.

HTTP 애플리케이션 프로파일은 HTTP 및 HTTPS 애플리케이션 모두에 사용됩니다.

옵션	설명
이름 및 설명	HTTP 애플리케이션 프로파일에 대한 설명과 이름을 입력합니다.
유류 시간 제한	TCP 애플리케이션 프로파일에 구성해야 하는 TCP 소켓 설정 대신 HTTP 애플리케이션이 유류 상태로 유지될 수 있는 시간을 초 단위로 입력합니다.
요청 헤더 크기	HTTP 요청 헤더를 저장하는 데 사용되는 최대 버퍼 크기를 바이트 단위로 지정합니다.
XFF(X-Forwarded-For)	<ul style="list-style-type: none"> ■ 삽입 - 들어오는 요청에 XFF HTTP 헤더가 없으면 로드 밸런서가 클라이언트 IP 주소로 새 XFF 헤더를 삽입합니다. 들어오는 요청에 XFF HTTP 헤더가 있으면 로드 밸런서가 클라이언트 IP 주소를 XFF 헤더 앞에 붙입니다. ■ 바꾸기 - 들어오는 요청에 XFF HTTP 헤더가 있으면 로드 밸런서가 헤더를 바꿉니다. <p>웹 서버는 요청하는 클라이언트 IP 주소로 처리하는 각 요청을 기록합니다. 이러한 로그는 디버깅 및 분석 용도로 사용됩니다. 배포 토폴로지 인헤 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>
요청 본문 크기	HTTP 요청 본문을 저장하는 데 사용되는 최대 버퍼 크기 값을 입력합니다. 크기를 지정하지 않는 경우 요청 본문 크기는 무제한입니다.
리디렉션	<ul style="list-style-type: none"> ■ 없음 - 웹 사이트가 일시적으로 다운된 경우 페이지를 찾을 수 없음 오류 메시지가 사용자에게 표시됩니다. ■ HTTP 리디렉션 - 웹 사이트가 일시적으로 다운되었거나 이동된 경우 해당 가상 서버에 들어오는 요청이 여기에 지정된 URL로 일시적으로 리디렉션될 수 있습니다. 정적 리디렉션만 지원됩니다. <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"> ■ 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. <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>

옵션	설명
NTLM 인증	<p>TCP 멀티플렉싱을 끄고 HTTP 연결을 유지하도록 로드 밸런서 버튼을 전환합니다. 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> <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>
태그	<p>더 쉬운 검색을 위해 태그를 입력합니다.</p> <p>태그를 지정하여 태그의 범위를 설정할 수 있습니다.</p>

지속성 프로파일 추가

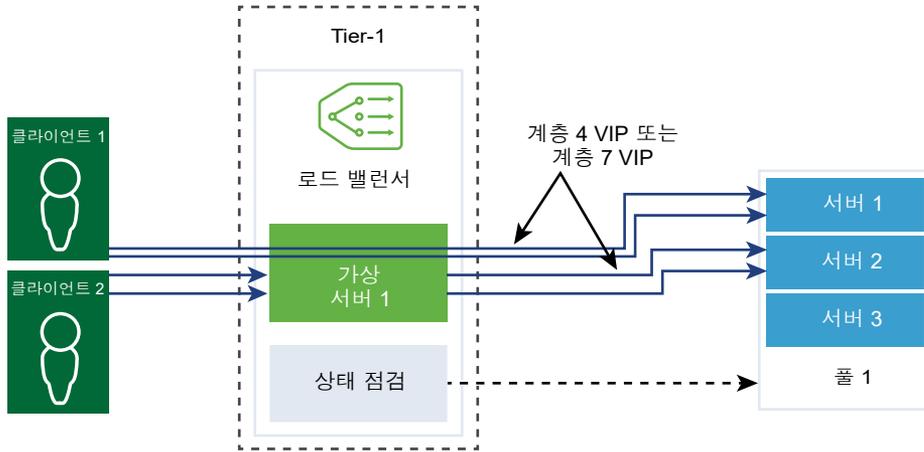
상태 저장 애플리케이션의 안정성을 보장하기 위해 로드 밸런서는 관련된 모든 연결을 동일한 서버로 보내는 지속성을 구현합니다. 다양한 유형의 애플리케이션 요구 사항을 해결하기 위해 다양한 유형의 지속성이 지원됩니다.

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. 클라이언트는 후속 요청에서 HTTP 쿠키를 전달하고 로드 밸런서는 해당 정보를 사용하여 쿠키 지속성을 제공합니다. 계층 7 가상 서버는 쿠키 지속성 프로파일만 사용할 수 있습니다. 쿠키 이름의 공개는 지원되지 **않습니다**.

일반 지속성 프로파일은 HTTP 요청의 HTTP 헤더, 쿠키 또는 URL을 기준으로 지속성을 지원합니다. 따라서 세션 ID가 URL의 일부인 경우 애플리케이션 세션 지속성을 지원합니다. 이 프로파일은 가상 서버에 직접 연결되어 있지 않습니다. 요청 전달 및 응답 재작성에 대한 로드 밸런서 규칙을 구성할 때 이 프로파일을 지정할 수 있습니다.



절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > 로드 밸런싱 > 프로파일 > 지속성 > 지속성 프로파일 추가**를 선택합니다.
- 3 **소스 IP**를 선택하여 소스 IP 지속성 프로파일을 추가하고 프로파일 세부 정보를 입력합니다.
기본적인 소스 IP 프로파일 설정을 수락할 수도 있습니다.

옵션	설명
이름 및 설명	소스 IP 지속성 프로파일에 대한 설명과 이름을 입력합니다.
지속성 공유	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.
지속성 항목 시간 초과	지속성 만료 시간(초)을 입력합니다. 로드 밸런서 지속성 테이블은 클라이언트 요청이 동일한 서버로 전송되는 것을 기록하는 항목을 유지합니다. 새 클라이언트 IP에서의 첫 번째 연결은 로드 밸런싱 알고리즘을 기준으로 풀 멤버에 대해 로드 밸런싱됩니다. NSX는 CLI 명령(<code>get load-balancer <LB-UUID> persistence-tables</code>)을 통해 활성 T1-LB를 호스팅하는 Edge 노드에서 볼 수 있는 LB 지속성 테이블에 해당 지속성 항목을 저장합니다. <ul style="list-style-type: none"> ■ 해당 클라이언트에서 VIP로의 연결이 있는 경우 지속성 항목은 유지됩니다. ■ 해당 클라이언트에서 VIP로의 연결이 더 이상 없는 경우 지속성 항목은 "지속성 항목 시간 초과" 값에 지정된 타이머 카운트다운을 시작합니다. 타이머가 만료되기 전에 해당 클라이언트에서 VIP로의 새 연결을 설정하지 않으면 해당 클라이언트 IP에 대한 지속성 항목이 삭제됩니다. 항목을 삭제한 후 해당 클라이언트가 다시 돌아오면 로드 밸런싱 알고리즘을 기준으로 풀 멤버에 대해 다시 로드 밸런싱됩니다.

옵션	설명
가득 차면 항목 제거	시간 초과 값이 크면 트래픽이 과도할 경우 지속성 테이블이 빠르게 채워질 수 있습니다. 이 옵션을 사용하도록 설정하면 최신 항목을 수용하기 위해 가장 오래된 항목부터 삭제됩니다. 이 옵션을 사용하지 않도록 설정하면 소스 IP 지속성 테이블이 가득 찰 경우 새 클라이언트 연결이 거부됩니다.
HA 지속성 미러링	버튼을 전환하여 지속성 항목을 HA 피어와 동기화합니다. HA 지속성 미러링을 사용하도록 설정하면 로드 밸런서 페일오버 시 클라이언트 IP 지속성이 유지됩니다.
태그	더 쉬운 검색을 위해 태그를 입력합니다. 태그를 지정하여 태그의 범위를 설정할 수 있습니다.

4 쿠키 지속성 프로파일을 선택하고 프로파일 세부 정보를 입력합니다.

옵션	설명
이름 및 설명	쿠키 지속성 프로파일에 대한 설명과 이름을 입력합니다.
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.
쿠키 모드	드롭다운 메뉴에서 모드를 선택합니다. <ul style="list-style-type: none"> ■ 삽입 - 세션을 식별하는 고유한 쿠키를 추가합니다. ■ 접두사 - 기존 HTTP 쿠키 정보에 추가합니다. ■ 재작성 - 기존 HTTP 쿠키 정보를 재작성합니다.
쿠키 이름	쿠키 이름을 입력합니다. 쿠키 이름의 공백은 지원되지 않습니다 .
쿠키 도메인	도메인 이름을 입력합니다. HTTP 쿠키 도메인은 삽입 모드에서만 구성 할 수 있습니다.
쿠키 대체	쿠키가 [사용 안 함] 또는 [종료] 상태인 서버를 가리키는 경우 클라이언트 요청이 거부되도록 버튼을 전환합니다. 쿠키가 [사용 안 함] 또는 [종료] 상태인 서버를 가리키는 경우 클라이언트 요청을 처리할 새 서버를 선택합니다.
쿠키 경로	쿠키 URL 경로를 입력합니다. HTTP 쿠키 경로는 삽입 모드에서만 설정할 수 있습니다.
쿠키 왜곡	버튼을 전환하여 암호화를 사용하지 않도록 설정합니다. 왜곡을 사용하지 않도록 설정하면 쿠키 서버 IP 주소 및 포트 정보가 일반 텍스트 형식입니다. 쿠키 서버 IP 주소 및 포트 정보를 암호화합니다.
쿠키 유형	드롭다운 메뉴에서 쿠키 유형을 선택합니다. 세션 쿠키 - 저장되지 않습니다. 브라우저가 닫히면 손실됩니다. 지속성 쿠키 - 브라우저에서 저장됩니다. 브라우저가 닫혀도 손실되지 않습니다.

옵션	설명
최대 유휴 시간	쿠키가 만료되기 전에 쿠키 유형이 유휴 상태일 수 있는 시간(초 단위)을 입력합니다.
최대 쿠키 사용 기간	세션 쿠키 유형에 대해 쿠키를 사용할 수 있는 시간(초 단위)을 입력합니다.
태그	더 쉬운 검색을 위해 태그를 입력합니다. 태그를 지정하여 태그의 범위를 설정할 수 있습니다.

5 일반을 선택하여 일반 지속성 프로파일을 추가하고 프로파일 세부 정보를 입력합니다.

옵션	설명
이름 및 설명	소스 IP 지속성 프로파일에 대한 설명과 이름을 입력합니다.
지속성 공유	버튼을 전환하여 가상 서버 간에 프로파일을 공유합니다.
지속성 항목 시간 초과	지속성 만료 시간(초)을 입력합니다. 로드 밸런서 지속성 테이블은 클라이언트 요청이 동일한 서버로 전송되는 것을 기록하는 항목을 유지합니다. 새 클라이언트 IP에서의 첫 번째 연결은 로드 밸런싱 알고리즘을 기준으로 풀 멤버에 대해 로드 밸런싱됩니다. NSX는 CLI 명령(<code>get load-balancer <LB-UUID> persistence-tables</code>)을 통해 활성 T1-LB를 호스팅하는 Edge 노드에서 볼 수 있는 LB 지속성 테이블에 해당 지속성 항목을 저장합니다. <ul style="list-style-type: none"> 해당 클라이언트에서 VIP로의 연결이 있는 경우 지속성 항목은 유지됩니다. 해당 클라이언트에서 VIP로의 연결이 더 이상 없는 경우 지속성 항목은 "지속성 항목 시간 초과" 값에 지정된 타이머 카운트다운을 시작합니다. 타이머가 만료되기 전에 해당 클라이언트에서 VIP로의 새 연결을 설정하지 않으면 해당 클라이언트 IP에 대한 지속성 항목이 삭제됩니다. 항목을 삭제한 후 해당 클라이언트가 다시 돌아오면 로드 밸런싱 알고리즘을 기준으로 풀 멤버에 대해 다시 로드 밸런싱됩니다.
HA 지속성 미러링	버튼을 전환하여 지속성 항목을 HA 피어와 동기화합니다.
태그	더 쉬운 검색을 위해 태그를 입력합니다. 태그를 지정하여 태그의 범위를 설정할 수 있습니다.

SSL 프로파일 추가

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 중지하는 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 7-5. SSL 오프로딩

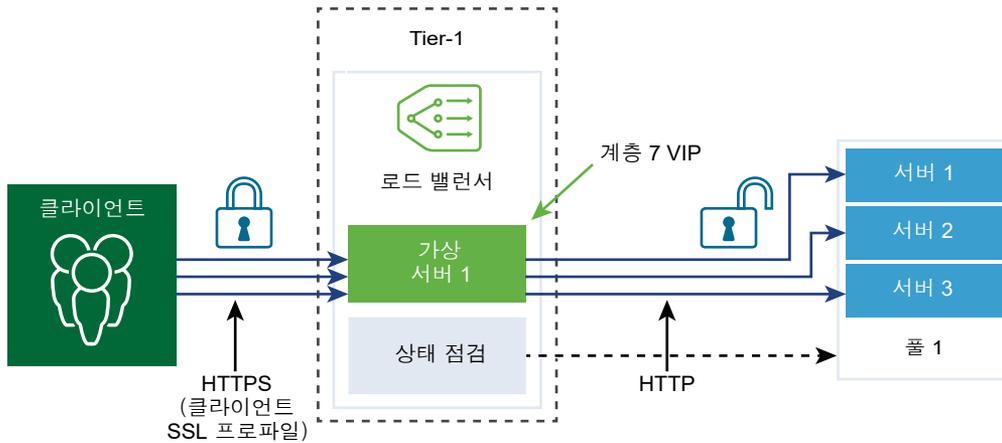
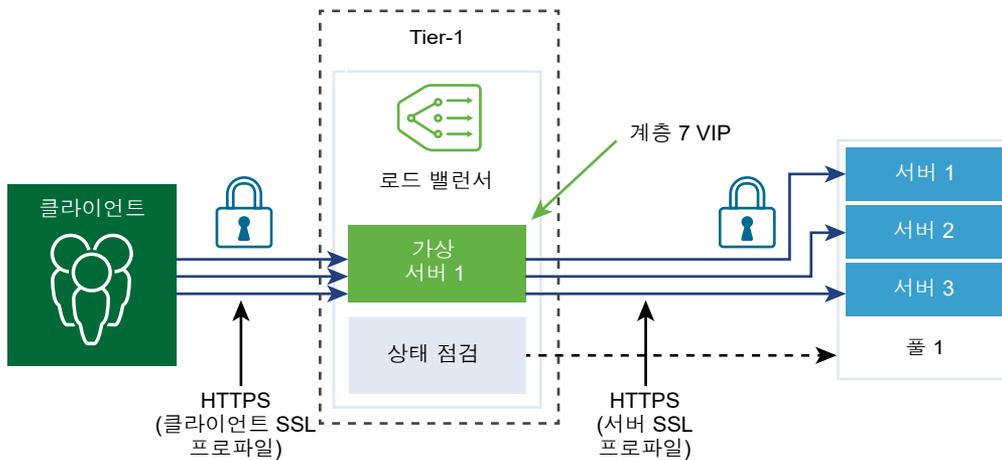


그림 7-6. 종단 간 SSL



절차

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

3 클라이언트 SSL 프로파일을 선택하고 프로파일 세부 정보를 입력합니다.

옵션	설명
이름 및 설명	클라이언트 SSL 프로파일에 대한 설명과 이름을 입력합니다.
SSL 집합	드롭다운 메뉴에서 SSL 암호 그룹을 선택하면 클라이언트 SSL 프로파일에 포함될 수 있는 SSL 암호와 SSL 프로토콜이 채워집니다. 균형 조정 SSL 암호 그룹이 기본값입니다.
세션 캐싱	버튼을 전환하여 SSL 클라이언트와 서버가 이전에 협상된 보안 매개 변수를 재사용할 수 있어 SSL 핸드셰이크 중에 비용이 높은 공용 키 작업을 방지할 수 있습니다.
태그	더 쉬운 검색을 위해 태그를 입력합니다. 태그를 지정하여 태그의 범위를 설정할 수 있습니다.
지원되는 SSL 암호	SSL 집합에 따라 사용자가 할당된 지원되는 SSL 암호가 여기에 채워집니다. 더 보기 를 클릭하여 전체 목록을 봅니다. 사용자 지정 을 선택한 경우 드롭다운 메뉴에서 SSL 암호를 선택해야 합니다.
지원되는 SSL 프로토콜	SSL 집합에 따라 사용자가 할당된 지원되는 SSL 프로토콜이 여기에 채워집니다. 더 보기 를 클릭하여 전체 목록을 봅니다. 사용자 지정 을 선택한 경우 드롭다운 메뉴에서 SSL 암호를 선택해야 합니다.
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.

4 서버 SSL 프로파일을 선택하고 프로파일 세부 정보를 입력합니다.

옵션	설명
이름 및 설명	서버 SSL 프로파일에 대한 설명과 이름을 입력합니다.
SSL 집합	드롭다운 메뉴에서 SSL 암호 그룹을 선택하면 서버 SSL 프로파일에 포함될 수 있는 SSL 암호와 SSL 프로토콜이 채워집니다. 균형 조정 SSL 암호 그룹이 기본값입니다.
세션 캐싱	버튼을 전환하여 SSL 클라이언트와 서버가 이전에 협상된 보안 매개 변수를 재사용할 수 있어 SSL 핸드셰이크 중에 비용이 높은 공용 키 작업을 방지할 수 있습니다.
태그	더 쉬운 검색을 위해 태그를 입력합니다. 태그를 지정하여 태그의 범위를 설정할 수 있습니다.
지원되는 SSL 암호	SSL 집합에 따라 사용자가 할당된 지원되는 SSL 암호가 여기에 채워집니다. 더 보기 를 클릭하여 전체 목록을 봅니다. 사용자 지정 을 선택한 경우 드롭다운 메뉴에서 SSL 암호를 선택해야 합니다.
지원되는 SSL 프로토콜	SSL 집합에 따라 사용자가 할당된 지원되는 SSL 프로토콜이 여기에 채워집니다. 더 보기 를 클릭하여 전체 목록을 봅니다. 사용자 지정 을 선택한 경우 드롭다운 메뉴에서 SSL 암호를 선택해야 합니다.

옵션	설명
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.

계층 4 가상 서버 추가

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 추가**의 내용을 참조하십시오.
- 영구 프로파일을 사용할 수 있는지 확인합니다. **지속성 프로파일 추가**의 내용을 참조하십시오.
- 클라이언트와 서버에 대한 **SSL 프로파일**을 사용할 수 있는지 확인합니다. **SSL 프로파일 추가**의 내용을 참조하십시오.
- 서버 풀을 사용할 수 있는지 확인합니다. **서버 풀 추가**의 내용을 참조하십시오.
- 로드 밸런서를 사용할 수 있는지 확인합니다. **로드 밸런서 추가**의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > 로드 밸런싱 > 가상 서버 > 가상 서버 추가**를 선택합니다.
- 3 **L4 TCP** 프로토콜을 선택하고 프로토콜 세부 정보를 입력합니다.

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.

옵션	설명
이름 및 설명	계층 4 가상 서버에 대한 설명과 이름을 입력합니다.
IP 주소	가상 서버 IP주소를 입력합니다.
포트	가상 서버 포트 번호를 입력합니다.
로드 밸런서	드롭다운 메뉴에서 이 계층 4 가상 서버에 연결할 기존 로드 밸런서를 선택합니다.
서버 풀	드롭다운 메뉴에서 기존 서버 풀을 선택합니다. 서버 풀은 유사하게 구성되고 동일한 애플리케이션을 실행하는 하나 이상의 서버로 구성되며, 이러한 서버를 풀 멤버라고도 합니다. 새로 만들임표를 클릭하여 서버 풀을 생성할 수 있습니다.
애플리케이션 프로파일	프로토콜 유형을 기반으로, 기존 애플리케이션 프로파일이 자동으로 채워집니다. 새로 만들임표를 클릭하여 애플리케이션 프로파일을 생성할 수 있습니다.
지속성	드롭다운 메뉴에서 기존 지속성 프로파일을 선택합니다. 지속성 프로파일은 가상 서버에서 사용하도록 설정되어 소스 IP 관련 클라이언트 연결을 동일한 서버로 전송하도록 허용합니다.
최대 동시 연결 수	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.
장애 대비 서버 풀	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. 새로 만들임표를 클릭하여 서버 풀을 생성할 수 있습니다.
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.
관리 상태	계층 4 가상 서버의 관리 상태를 사용하지 않도록 설정하려면 이 버튼을 전환합니다.
액세스 로그	계층 4 가상 서버에 대한 로깅을 사용하도록 설정하려면 버튼을 전환합니다.
태그	더 쉬운 검색을 위해 태그를 입력합니다. 태그를 지정하여 태그의 범위를 설정할 수 있습니다.

4 L4 UDP 프로토콜을 선택하고 프로토콜 세부 정보를 입력합니다.

옵션	설명
이름 및 설명	계층 4 가상 서버에 대한 설명과 이름을 입력합니다.
IP 주소	가상 서버 IP주소를 입력합니다.

옵션	설명
포트	가상 서버 포트 번호를 입력합니다.
로드 밸런서	드롭다운 메뉴에서 이 계층 4 가상 서버에 연결할 기존 로드 밸런서를 선택합니다.
서버 풀	드롭다운 메뉴에서 기존 서버 풀을 선택합니다. 서버 풀은 유사하게 구성되고 동일한 애플리케이션을 실행하는 하나 이상의 서버로 구성되며, 이러한 서버를 풀 멤버라고도 합니다. 새로 말줄임표를 클릭하여 서버 풀을 생성할 수 있습니다.
애플리케이션 프로파일	프로토콜 유형을 기반으로, 기존 애플리케이션 프로파일이 자동으로 채워집니다. 새로 말줄임표를 클릭하여 애플리케이션 프로파일을 생성할 수 있습니다.
지속성	드롭다운 메뉴에서 기존 지속성 프로파일을 선택합니다. 지속성 프로파일은 가상 서버에서 사용하도록 설정되어 소스 IP 관련 클라이언트 연결을 동일한 서버로 전송하도록 허용합니다.
최대 동시 연결 수	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.
장애 대비 서버 풀	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. 새로 말줄임표를 클릭하여 서버 풀을 생성할 수 있습니다.
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.
관리 상태	계층 4 가상 서버의 관리 상태를 사용하지 않도록 설정하려면 이 버튼을 전환합니다.
액세스 로그	계층 4 가상 서버에 대한 로깅을 사용하도록 설정하려면 버튼을 전환합니다.
태그	더 쉬운 검색을 위해 태그를 입력합니다. 태그를 지정하여 태그의 범위를 설정할 수 있습니다.

계층 7 HTTP 가상 서버 추가

가상 서버는 모든 클라이언트 연결을 수신하여 서버에 배포합니다. 가상 서버에는 IP 주소, 포트 및 TCP 프로토콜이 있습니다.

로드 밸런서 규칙은 HTTP 애플리케이션 프로파일이 있는 계층 7 가상 서버에만 지원됩니다. 서로 다른 로드 밸런서 서비스는 로드 밸런서 규칙을 사용할 수 있습니다.

참고 계층 7 SSL 패스스루는 NSX-T Data Center 3.0 이상에서 지원됩니다.

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.

참고 NSX-T Data Center 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

- 애플리케이션 프로파일을 사용할 수 있는지 확인합니다. 애플리케이션 프로파일 추가의 내용을 참조하십시오.
- 영구 프로파일을 사용할 수 있는지 확인합니다. 지속성 프로파일 추가의 내용을 참조하십시오.
- 클라이언트와 서버에 대한 SSL 프로파일을 사용할 수 있는지 확인합니다. SSL 프로파일 추가의 내용을 참조하십시오.
- 서버 풀을 사용할 수 있는지 확인합니다. 서버 풀 추가의 내용을 참조하십시오.
- CA 및 클라이언트 인증서를 사용할 수 있는지 확인합니다. 인증서 서명 요청 파일 생성의 내용을 참조하십시오.
- CRL(인증 해지 목록)을 사용할 수 있는지 확인합니다. 인증서 해지 목록 가져오기의 내용을 참조하십시오.
- 로드 밸런서를 사용할 수 있는지 확인합니다. 로드 밸런서 추가의 내용을 참조하십시오.

절차

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

- 2 **네트워킹 > 로드 밸런싱 > 가상 서버 > 가상 서버 추가**를 선택합니다.
- 3 **L7 HTTP** 프로토콜을 선택하고 프로토콜 세부 정보를 입력합니다.

계층 7 가상 서버는 HTTP 및 HTTPS 프로토콜을 지원합니다.

옵션	설명
이름 및 설명	계층 7 가상 서버에 대한 설명과 이름을 입력합니다.
IP 주소	가상 서버 IP주소를 입력합니다.
포트	가상 서버 포트 번호를 입력합니다.
로드 밸런서	드롭다운 메뉴에서 이 계층 4 가상 서버에 연결할 기존 로드 밸런서를 선택합니다.
서버 풀	드롭다운 메뉴에서 기존 서버 풀을 선택합니다. 서버 풀은 유사하게 구성되고 동일한 애플리케이션을 실행하는 하나 이상의 서버로 구성되며, 이러한 서버를 풀 멤버라고도 합니다. 새로 만들임포를 클릭하여 서버 풀을 생성할 수 있습니다.
애플리케이션 프로파일	프로토콜 유형을 기반으로, 기존 애플리케이션 프로파일이 자동으로 채워집니다. 새로 만들임포를 클릭하여 애플리케이션 프로파일을 생성할 수 있습니다.
지속성	드롭다운 메뉴에서 기존 지속성 프로파일을 선택합니다. 지속성 프로파일은 가상 서버에서 사용하도록 설정되어 소스 IP 및 쿠키 관련 클라이언트 연결을 동일한 서버로 전송하도록 허용합니다.

- 4 **구성**을 클릭하여 계층 7 가상 서버 SSL을 설정합니다.
클라이언트 SSL 및 서버 SSL을 구성할 수 있습니다.
- 5 클라이언트 SSL을 구성합니다.

옵션	설명
클라이언트 SSL	프로파일을 사용하도록 설정하려면 이 버튼을 전환합니다. 클라이언트 측 SSL 프로파일 바인딩을 사용하면 서로 다른 호스트 이름이 동일한 가상 서버에 연결될 수 있도록 여러 인증서가 허용됩니다.
기본 인증서	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.
클라이언트 SSL 프로파일	드롭다운 메뉴에서 클라이언트 측 SSL 프로파일을 선택합니다.
SNI 인증서	드롭다운 메뉴에서 사용 가능한 SNI 인증서를 선택합니다.
신뢰할 수 있는 CA 인증서	사용 가능한 CA 인증서를 선택합니다.
필수 클라이언트 인증	이 메뉴 항목을 사용하도록 설정하려면 이 버튼을 전환합니다.
인증서 체인 수준	인증서 체인 수준을 설정하여 서버 인증서 체인의 수준을 확인합니다.
인증서 해지 목록	손상된 서버 인증서를 허용하지 않으려면 사용 가능한 CRL을 선택합니다.

6 서버 SSL 구성

옵션	설명
서버 SSL	프로파일을 사용하도록 설정하려면 이 버튼을 전환합니다.
클라이언트 인증서	드롭다운 메뉴에서 클라이언트 인증서를 선택합니다. 이 인증서는 서버가 동일한 IP 주소에서 여러 호스트 이름을 호스팅하지 않거나 클라이언트가 SNI(서버 이름 표시) 확장을 지원하지 않는 경우 사용됩니다.
서버 SSL 프로파일	드롭다운 메뉴에서 서버 측 SSL 프로파일을 선택합니다.
신뢰할 수 있는 CA 인증서	사용 가능한 CA 인증서를 선택합니다.
필수 서버 인증	이 메뉴 항목을 사용하도록 설정하려면 이 버튼을 전환합니다. 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.
인증서 체인 수준	인증서 체인 수준을 설정하여 서버 인증서 체인의 수준을 확인합니다.
인증서 해지 목록	손상된 서버 인증서를 허용하지 않으려면 사용 가능한 CRL을 선택합니다. OCSP 및 OCSP 스테이플링은 서버 측에서 지원되지 않습니다.

7 추가 계층 7 가상 서버 속성을 구성합니다.

옵션	설명
최대 동시 연결 수	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.
장애 대비 서버 풀	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. 새로 말줄임표를 클릭하여 서버 풀을 생성할 수 있습니다.
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.
관리 상태	계층 7 가상 서버의 관리 상태를 사용하지 않도록 설정하려면 이 버튼을 전환합니다.
엑세스 로그	계층 7 가상 서버에 대한 로깅을 사용하도록 설정하려면 이 버튼을 전환합니다.
태그	더 쉬운 검색을 위해 태그를 입력합니다. 태그를 지정하여 태그의 범위를 설정할 수 있습니다.

8 저장을 클릭합니다.

로드 밸런서 규칙 추가

계층 7 HTTP 가상 서버를 사용하면 일치 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 \1부터 \9까지 사용할 수 있습니다.
- \ddd 형식이 아닌 \Odd 형식을 사용하여 8진수 문자와 일치시킵니다.
- 내장형 플래그는 최상위 레벨에서 지원되지 않으며 그룹 내에서만 지원됩니다. 예를 들어 "Case (?i:sensitive)" 대신 "Case ((?i:s)ensitive)"를 사용하십시오.
- 전처리 작업 \l, \u, \L, \U가 지원되지 않습니다. 여기서 \l - 다음 문자 소문자, \u - 다음 문자 대문자, \L - \E까지 소문자, \U - \E까지 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 \u2018를 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.html과 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=\$article과 같이 일치된 변수를 사용하여 URI를 다시 작성할 수 있습니다. 그러면 URI가 /news.py?year=2018&month=06&day=15&article=news1234.html로 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_addr로 작성될 수 있습니다. 그러면 예제 URI가 /news.py?year=2018&month=06&day=15&article=news1234.html&user_ip=1.1.1.1로 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

- `$_arg_<name>` - 요청 줄의 인수 `<name>`
- `$_cookie_<name>` - `<name>` 쿠키의 값
- `$_upstream_cookie_<name>` - "Set-Cookie" 응답 헤더 필드에서 업스트림 서버가 보낸 지정된 이름의 쿠키
- `$_upstream_http_<name>` - 임의 응답 헤더 필드이며 `<name>`은 소문자로 변환된 필드 이름이고 대시는 밑줄로 대체됨
- `$_host` - 우선 순위에 따라 - 요청 라인의 호스트 이름 또는 "Host" 요청 헤더 필드의 호스트 이름 또는 요청과 일치하는 서버 이름
- `$_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"
- (NSX-T Data Center 2.5.0만 해당) `$_ssl_client_cert` - 설정된 SSL 연결에 대한 PEM 형식의 클라이언트 인증서를 반환하며, 첫 줄을 제외한 각 줄 앞에 탭 문자가 추가되었습니다.
- (NSX-T Data Center 2.5.1 이상) `$_ssl_client_escaped_cert` - 설정된 SSL 연결에 대한 PEM 형식의 클라이언트 인증서를 반환합니다.
- `$_ssl_server_name` - SNI를 통해 요청된 서버 이름을 반환함
- `$_uri` - 요청의 URI 경로
- `$_ssl_ciphers`: 클라이언트 SSL 암호를 반환함
- `$_ssl_c_i_dn`: RFC 2253에 따라 설정된 SSL 연결에 대한 클라이언트 인증서의 "발급자 DN" 문자열을 반환함
- `$_ssl_client_s_dn`: RFC 2253에 따라 설정된 SSL 연결에 대한 클라이언트 인증서의 "주체 DN" 문자열을 반환함

- `$_ssl_protocol`: 설정된 SSL 연결의 프로토콜을 반환함
- `$_ssl_session_reused`: SSL 세션을 재사용하는 경우 "r"을 반환하고, 그렇지 않은 경우 "."를 반환함

사전 요구 사항

계층 7 HTTP 가상 서버를 사용할 수 있는지 확인합니다. 계층 7 HTTP 가상 서버 추가의 내용을 참조하십시오.

절차

- 1 계층 7 HTTP 가상 서버를 엽니다.
- 2 로드 밸런서 규칙 섹션에서 **설정 > 규칙 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. http_request.method - 일치시킬 값
HTTP 요청 URI	쿼리 인수 없이 HTTP 요청 URI를 일치시킵니다. http_request.uri - 일치시킬 값
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 쿠키	HTTP 요청 쿠키를 일치시킵니다. http_request.cookie_value - 일치시킬 값
HTTP 요청 본문	HTTP 요청 본문 콘텐츠를 일치시킵니다. http_request.body_value - 일치시킬 값
클라이언트 SSL	클라이언트 SSL 프로파일 ID를 일치시킵니다. ssl_profile_id - 일치시킬 값
TCP 헤더 포트	TCP 소스 또는 대상 포트를 일치시킵니다. tcp_header.source_port - 일치시킬 소스 포트 tcp_header.destination_port - 일치시킬 대상 포트
IP 헤더 소스	IP 소스 또는 대상 주소를 일치시킵니다. ip_header.source_address - 일치시킬 소스 주소 ip_header.destination_address - 일치시킬 대상 주소

지원되는 일치 조건	설명
변수	변수를 생성하고 변수에 값을 할당합니다.
대/소문자 구분	HTTP 헤더 값 비교에 대/소문자 구분 플래그를 설정합니다.
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
HTTP 요청 헤더 삭제	HTTP 헤더를 삭제합니다. http_request.header_delete - 헤더 이름 http_request.header_delete - 작성할 값

3 요청 전달 > 규칙 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 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 쿠키	HTTP 요청 쿠키를 일치시킵니다. http_request.cookie_value - 일치시킬 값
HTTP 요청 본문	HTTP 요청 본문 콘텐츠를 일치시킵니다. http_request.body_value - 일치시킬 값
클라이언트 SSL	클라이언트 SSL 프로파일 ID를 일치시킵니다. ssl_profile_id - 일치시킬 값
TCP 헤더 포트	TCP 소스 또는 대상 포트를 일치시킵니다. tcp_header.source_port - 일치시킬 소스 포트 tcp_header.destination_port - 일치시킬 대상 포트
IP 헤더 소스	IP 소스 또는 대상 주소를 일치시킵니다. ip_header.source_address - 일치시킬 소스 주소 ip_header.destination_address - 일치시킬 대상 주소

지원되는 일치 조건	설명
변수	변수를 생성하고 변수에 값을 할당합니다.
대/소문자 구분	HTTP 헤더 값 비교에 대/소문자 구분 플래그를 설정합니다.
작업	설명
HTTP 거절	예를 들면 상태를 5xx로 설정하여 요청을 거부합니다. http_forward.reply_status - 거부하는 데 사용되는 HTTP 상태 코드 http_forward.reply_message - HTTP 거부 메시지
HTTP 리디렉션	요청을 리디렉션합니다. 상태 코드를 3xx로 설정해야 합니다. http_forward.redirect_status - 리디렉션을 위한 HTTP 상태 코드 http_forward.redirect_url - HTTP 리디렉션 URL
풀 선택	요청을 특정 서버 풀에 강제 적용합니다. 지정된 풀 멤버의 구성된 알고리즘(예측자)은 서버 풀 내에서 서버를 선택하는 데 사용됩니다. hhttp_forward.select_pool - 서버 풀 UUID
가변 지속성 검사	일반 지속성 프로파일을 선택하고 변수 이름을 입력합니다. 해시 변수 를 사용하도록 설정할 수도 있습니다. 변수 값이 매우 긴 경우 변수를 해시 하면 해당 변수가 지속성 테이블에 올바르게 저장됩니다. 해시 변수 를 사용하도록 설정하지 않은 경우 변수 값이 매우 길면 변수 값의 고정 접두사 부분만 지속성 테이블에 저장됩니다. 따라서 긴 변수 값이 있는 두 개의 다른 요청을 다른 백엔드 서버로 디스패치해야 하는 경우에도 동일한 백엔드 서버로 디스패치될 수 있습니다(해당 변수 값이 동일한 접두사 부분을 포함하기 때문임).
응답 상태	응답의 상태를 표시합니다.
응답 메시지	서버는 확인된 주소와 구성이 포함된 응답 메시지로 응답합니다.

4 요청 재작성 > 규칙 추가를 클릭하여 HTTP 응답 재작성에 대한 로드 밸런서 규칙을 구성합니다.

모든 일치 값은 정규식을 허용합니다.

지원되는 일치 조건	설명
HTTP 응답 헤더	HTTP 응답 헤더를 일치시킵니다. http_response.header_name - 일치시킬 헤더 이름 http_response.header_value - 일치시킬 값
HTTP 응답 메서드	HTTP 응답 메서드를 일치시킵니다. http_response.method - 일치시킬 값
HTTP 응답 URI	HTTP 응답 URI를 일치시킵니다. http_response.uri - 일치시킬 값
HTTP 응답 URI 인수	HTTP 응답 URI 인수를 일치시킵니다. http_response.uri_args - 일치시킬 값
HTTP 응답 버전	HTTP 응답 버전을 일치시킵니다. http_response.version - 일치시킬 값
HTTP 응답 쿠키	HTTP 응답 쿠키를 일치시킵니다. http_response.cookie_value - 일치시킬 값

지원되는 일치 조건	설명
클라이언트 SSL	클라이언트 SSL 프로파일 ID를 일치시킵니다. ssl_profile_id - 일치시킬 값
TCP 헤더 포트	TCP 소스 또는 대상 포트를 일치시킵니다. tcp_header.source_port - 일치시킬 소스 포트 tcp_header.destination_port - 일치시킬 대상 포트
IP 헤더 소스	IP 소스 또는 대상 주소를 일치시킵니다. ip_header.source_address - 일치시킬 소스 주소 ip_header.destination_address - 일치시킬 대상 주소
변수	변수를 생성하고 변수에 값을 할당합니다.
대/소문자 구분	HTTP 헤더 값 비교에 대/소문자 구분 플래그를 설정합니다.
작업	설명
HTTP 응답 헤더 다시 쓰기	HTTP 응답 헤더의 값을 수정합니다. http_response.header_name - 헤더 이름 http_response.header_value - 작성할 값
HTTP 응답 헤더 삭제	HTTP 헤더를 삭제합니다. http_request.header_delete - 헤더 이름 http_request.header_delete - 작성할 값
가변 지속성 학습	일반 지속성 프로파일을 선택하고 변수 이름을 입력합니다. 해시 변수 를 사용하도록 설정할 수도 있습니다. 변수 값이 매우 긴 경우 변수를 해시 하면 해당 변수가 지속성 테이블에 올바르게 저장됩니다. 해시 변수 를 사용하도록 설정하지 않은 경우 변수 값이 매우 길면 변수 값의 고정 접두사 부분만 지속성 테이블에 저장됩니다. 따라서 긴 변수 값이 있는 두 개의 다른 요청을 다른 백엔드 서버로 디스패치해야 하는 경우에도 동일한 백엔드 서버로 디스패치될 수 있습니다(해당 변수 값이 동일한 접두사 부분을 포함하기 때문임).

서버 풀 및 가상 서버에 대해 생성되는 그룹

NSX Manager에서는 로드 밸런서 서버 풀 및 VIP 포트에 대한 그룹을 자동으로 생성합니다.

로드 밸런서 생성 그룹은 **인벤토리 > 그룹** 아래에 표시됩니다.

서버 풀 그룹은 다음과 같이 그룹 멤버 IP 주소가 할당되어 NLB.PoolLB.Pool_Name LB_Name 이름으로 생성됩니다.

- LB-SNAT(투명): 0.0.0.0/0 없이 구성된 풀
- LB-SNAT 자동 맵: T1-업링크 IP 100.64.x.y 및 T1-ServiceInterface IP 없이 구성된 풀
- LB-SNAT IP-Pool: LB-SNAT IP-Pool 없이 구성된 풀

VIP 그룹이 이름 NLB.VIP.가상 서버 이름(으)로 생성되고 VIP 그룹 멤버 IP 주소는 VIP IP@입니다.

서버 풀 그룹의 경우 로드 밸런서에서 트래픽 분산 방화벽 규칙을 생성할 수 있습니다(NLB.PoolLB.
Pool_Name LB_Name). Tier-1 게이트웨이 방화벽의 경우 클라이언트에서 LB VIP NLB.VIP. *가상 서버
이름(으)*로의 허용 트래픽을 생성할 수 있습니다.

이 기능은 NSX Cloud에 적용됩니다.

전달 정책 또는 PBR(정책 기반 라우팅) 규칙은 NSX-T가 NSX 관리 VM의 트래픽을 처리하는 방식을 정의합니다. 이 트래픽은 NSX-T 오버레이로 조종되거나 클라우드 제공자의 (언더레이) 네트워크를 통해 라우팅될 수 있습니다.

참고 NSX-T Data Center를 사용하여 공용 클라우드 워크로드 VM을 관리하는 방법에 대한 자세한 내용은 [장 22 NSX Cloud 사용](#)을 참조하십시오.

전송 VPC/VNet에서 PCG를 배포하거나 계산 VPC/VNet을 전송 VPC/VNet에 연결하면 세 가지 기본 전달 정책이 자동으로 설정됩니다.

- 1 전송/계산 VPC/vNet에서 주소가 지정된 모든 트래픽에 대해 한 가지 **경로에서 언더레이로**.
- 2 공용 클라우드의 메타데이터 서비스로 향하는 모든 트래픽에 대해 다른 **경로에서 언더레이로**.
- 3 기타 모든 트래픽(예: 전송/계산 VPC/vNet 외부로 이동되는 트래픽)에 대해 한 가지 **경로에서 오버레이로**. 이러한 트래픽은 NSX-T 오버레이 터널을 통해 PCG와 대상에 차례로 라우팅됩니다.

참고 동일한 PCG가 관리하는 다른 VPC/vNet으로 향하는 트래픽: 트래픽은 NSX-T 오버레이 터널을 통해 소스 NSX 관리 VPC/vNet에서 PCG로 라우팅된 다음, 대상 VPC/vNet으로 라우팅됩니다.

다른 PCG가 관리하는 다른 VPC/vNet으로 향하는 트래픽: 트래픽은 NSX 오버레이 터널을 통해 하나의 NSX 관리 VPC/vNet에서 소스 VPC/vNet의 PCG로 라우팅된 후 대상 NSX 관리 VPC/vNet의 PCG로 전달됩니다.

트래픽이 인터넷으로 이동되면 PCG는 트래픽을 인터넷의 대상으로 라우팅합니다.

언더레이로 라우팅하는 동안 마이크로 세분화

해당 트래픽이 언더레이 네트워크로 라우팅되는 워크로드 VM의 경우에도 마이크로 세분화가 적용됩니다.

NSX 관리 워크로드 VM에서 관리 VPC/VNet 외부의 대상으로 직접 연결되어 있고, PCG를 바이패스하려는 경우 언더레이를 통해 이 VM에서 트래픽을 라우팅하도록 전달 정책을 설정합니다.

트래픽이 언더레이 네트워크를 통해 라우팅되는 경우 PCG가 바이패스되므로 트래픽이 North-South 방향 화벽을 만나지 않습니다. 하지만 이러한 규칙은 PCG에 도달하기 전에 VM 수준에서 적용되기 때문에 여전히 East-West 또는 분산 방향화벽(DFW)에 대한 규칙을 관리해야 합니다.

지원되는 전달 정책 및 공통 사용 사례

드롭다운 메뉴에 전달 정책 목록이 표시될 수 있지만 이 릴리스에서는 다음 전달 정책만 지원됩니다.

- 경로에서 언더레이로
- 언더레이에서 경로로
- 경로에서 오버레이로

다음은 전달 정책이 유용하게 사용될 수 있는 일반적인 시나리오입니다.

- **언더레이로 라우팅:** NSX 관리 VM에서 언더레이의 서비스에 액세스합니다. 예를 들어 AWS 언더레이 네트워크에서 AWS S3 서비스에 액세스합니다.
- **언더레이에서 라우팅:** 언더레이 네트워크에서 NSX 관리 VM에 호스팅된 서비스에 액세스합니다. 예를 들어 AWS ELB에서 NSX 관리 VM으로 액세스합니다.

본 장은 다음 항목을 포함합니다.

- 전달 정책 추가 또는 편집

전달 정책 추가 또는 편집

자동으로 생성된 전달 정책을 편집하거나 새 정책을 추가할 수 있습니다.

예를 들어 공용 클라우드(예: AWS의 S3)에서 제공하는 서비스를 사용하려면 IP 주소 집합이 언더레이를 통해 라우팅되어 이 서비스에 액세스하도록 허용하는 정책을 수동으로 만들면 됩니다.

사전 요구 사항

PCG가 배포된 VPC 또는 VNet이 있어야 합니다.

절차

- 1 **섹션 추가**를 클릭합니다. 섹션의 이름을 적절하게 지정합니다(예: **AWS 서비스**).
- 2 섹션 옆의 확인란을 선택하고 **규칙 추가**를 클릭합니다. 규칙의 이름을 지정합니다(예: **s3 규칙**).
- 3 **소스** 탭에서 서비스 액세스를 제공할 워크로드 VM이 있는 VPC 또는 VNet을 선택합니다(예: AWS VPC). 여기에서 하나 이상의 조건과 일치하는 여러 VM을 포함하도록 **그룹**을 만들 수도 있습니다.
- 4 **대상** 탭에서 서비스가 호스팅되는 VPC 또는 VNet을 선택합니다(예: AWS에서 S3 서비스의 IP 주소가 포함된 **그룹**).
- 5 **서비스** 탭의 드롭다운 메뉴에서 서비스를 선택합니다. 서비스가 없으면 추가할 수 있습니다. **대상**에서 라우팅 세부 정보를 제공할 수 있기 때문에 선택 항목을 **임의**로 남겨 둘 수도 있습니다.

- 6 **작업** 탭에서 라우팅 작동 방식을 선택합니다. 예를 들어, **AWS S3** 서비스에 대해 이 정책을 설정하는 경우 **경로에서 언더레이로**를 선택합니다.
- 7 **게시**를 클릭하여 전달 정책 설정을 마칩니다.

IPAM(IP 주소 관리)

9

IP 주소를 관리하기 위해 DNS(Domain Name System), DHCP(Dynamic Host Configuration Protocol), IP 주소 풀 및 IP 주소 블록을 구성할 수 있습니다.

참고 IP 블록은 blocks are used by NCP(NSX Container Plug-in)에 사용됩니다. NCP에 대한 자세한 내용은 "Kubernetes 및 Cloud Foundry용 NSX Container Plug-in - 설치 및 관리 가이드"를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- DNS 영역 추가
- DNS 전달자 서비스 추가
- DHCP 서버 추가
- Tier-0 또는 Tier-1 게이트웨이에 대한 DHCP 릴레이 서버 구성
- IP 주소 풀 추가
- IP 주소 블록 추가

DNS 영역 추가

DNS 서비스에 대한 DNS 영역을 구성할 수 있습니다. DNS 영역은 DNS의 도메인 이름 공간의 고유한 부분입니다.

DNS 영역 구성에서 업스트림 DNS 서버로 DNS 쿼리를 전달할 때 DNS 전달자가 사용할 소스 IP를 지정할 수 있습니다. 소스 IP를 지정하지 않으면 DNS 쿼리 패킷의 소스 IP가 DNS 전달자의 수신기 IP가 됩니다. 수신기 IP가 외부 업스트림 DNS 서버에서 연결할 수 없는 내부 주소인 경우 소스 IP를 지정해야 합니다. DNS 응답 패킷이 전달자에게 다시 라우팅되도록 하려면 전용 소스 IP가 필요합니다. 또는 논리적 라우터에서 수신기 IP를 공용 IP로 변환하도록 SNAT를 구성할 수 있습니다. 이 경우 소스 IP를 지정할 필요가 없습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > IP 주소 관리 > DNS**를 선택합니다.

- 3 **DNS 영역** 탭을 클릭합니다.
- 4 기본 영역을 추가하려면 **DNS 영역 추가 > 기본 영역 추가**를 선택합니다.
 - a 이름과 설명(선택 사항)을 입력합니다.
 - b 최대 3개 DNS 서버의 IP 주소를 입력합니다.
 - c (선택 사항) **소스 IP** 필드에 IP 주소를 입력합니다.
- 5 FQDN 영역을 추가하려면 **DNS 영역 추가 > FQDN 영역 추가**를 선택합니다.
 - a 이름과 설명(선택 사항)을 입력합니다.
 - b 도메인의 FQDN을 입력합니다.
 - c 최대 3개 DNS 서버의 IP 주소를 입력합니다.
 - d (선택 사항) **소스 IP** 필드에 IP 주소를 입력합니다.
- 6 **저장**을 클릭합니다.

DNS 전달자 서비스 추가

DNS 쿼리를 외부 DNS 서버로 전달하도록 DNS 전달자를 구성할 수 있습니다.

DNS 전달자를 구성하기 전에 기본 DNS 영역을 구성해야 합니다. 필요한 경우 하나 이상의 FQDN DNS 영역을 구성할 수 있습니다. 각 DNS 영역은 최대 3개의 DNS 서버에 연결됩니다. FQDN DNS 영역을 구성할 때 하나 이상의 도메인 이름을 지정합니다. DNS 전달자는 기본 DNS 영역과 최대 5개의 FQDN DNS 영역에 연결됩니다. DNS 쿼리가 수신되면 DNS 전달자는 쿼리의 도메인 이름을 FQDN DNS 영역에 있는 도메인 이름과 비교합니다. 일치하는 항목이 있으면 FQDN DNS 영역에 지정된 DNS 서버로 쿼리가 전달됩니다. 일치하는 항목이 없으면 기본 DNS 영역에 지정된 DNS 서버로 쿼리가 전달됩니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > IP 주소 관리 > DNS**를 선택합니다.
- 3 **DNS 서비스 추가**를 클릭합니다.
- 4 이름과 설명(선택 사항)을 입력합니다.
- 5 Tier-0 또는 Tier-1 게이트웨이를 선택합니다.
- 6 DNS 서비스의 IP 주소를 입력합니다.
클라이언트는 DNS 전달자의 수신기 IP라고도 하는 이 IP 주소로 DNS 쿼리를 전송합니다.
- 7 기본 DNS 영역을 선택합니다.
- 8 로그 수준을 선택합니다.
- 9 최대 5개의 FQDN 영역을 선택합니다.

10 **관리 상태** 토글을 클릭하여 DNS 서비스를 사용하거나 사용하지 않도록 설정합니다.

11 **저장**을 클릭합니다.

DHCP 서버 추가

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 요청을 처리하기 위한 DHCP 서버를 생성할 수 있습니다.

참고 이 절차를 사용하여 생성되는 DHCP 서버는 VLAN 기반 세그먼트에서 사용할 수 없습니다. **고급 네트워킹 및 보안**에서 DHCP 기능을 사용하여 VLAN 기반 논리적 스위치에서 지원되는 DHCP 서버를 생성해야 합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > IP 주소 관리 > DHCP**를 선택합니다.
- 3 **서버 추가**를 클릭합니다.
- 4 서버 유형으로 **DHCP 서버**를 선택합니다.
- 5 서버의 이름을 입력합니다.
- 6 CIDR 형식으로 서버의 IP 주소를 입력합니다.

이 단계에서는 논리적 인터페이스용 1개, DHCP 서버 자체용 1개, 모두 2개의 논리적 포트를 생성하고 DHCP 서버를 특정 DHCP 논리적 스위치에 연결합니다. 이 인터페이스는 Tier-0 또는 Tier-1 게이트웨이에 연결된 인터페이스로 표시되므로 DHCP 서버를 할당하려는 Tier-1 또는 Tier-0 게이트웨이에 대해 겹치지 않는 서브넷을 선택해야 합니다. 이 목적을 위해 <IP 주소>/30을 지정할 수 있습니다. 여기에 사용된 서브넷 범위는 연결된 Tier-0 게이트웨이에 보급되지 않지만 Tier-1 게이트웨이의 전달 테이블에 표시됩니다.

- 7 리스 시간을 입력합니다.
- 8 NSX Edge 클러스터를 선택합니다.
- 9 **저장**을 클릭합니다.
- 10 DHCP 서버를 Tier-0 또는 Tier-1 게이트웨이에 할당하려면 다음을 수행합니다.
 - a **네트워킹 > Tier-0 게이트웨이** 또는 **네트워킹 > Tier-1 게이트웨이**로 이동합니다.
 - b 기존 게이트웨이를 편집합니다.
 - c **IP 주소 관리** 필드에서 **IP 할당 없음**을 클릭합니다.
 - d [유형] 드롭다운 목록에서 **DHCP 로컬 서버**를 선택합니다.
 - e DHCP 서버를 선택합니다.

- f **저장**을 클릭합니다.
 - g **저장**을 클릭합니다.
- 11 세그먼트에 DHCP 서버를 할당하려면 다음을 수행합니다.
- a **네트워킹 > 세그먼트**로 이동합니다.
 - b 세그먼트를 추가하거나 편집합니다.
세그먼트는 Tier-0 또는 Tier-1 게이트웨이와 연결되어야 합니다.
 - c 새 세그먼트를 추가하는 경우 **서브넷 설정**을 클릭하고, 서브넷을 추가하거나 수정하려면 **서브넷** 아래의 숫자를 클릭합니다.
 - d 적절한 DHCP 범위를 입력합니다.
 - e **적용**을 클릭합니다.
 - f **저장**을 클릭합니다.

Tier-0 또는 Tier-1 게이트웨이에 대한 DHCP 릴레이 서버 구성

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 트래픽을 외부 DHCP 서버로 릴레이하기 위한 DHCP 릴레이 서버를 생성할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > IP 주소 관리 > DHCP**를 선택합니다.
- 3 **서버 추가**를 클릭합니다.
- 4 서버 유형으로 **DHCP 릴레이**를 선택합니다.
- 5 릴레이 서버의 이름을 입력합니다.
- 6 서버에 대해 하나 이상의 IP 주소를 입력합니다.
- 7 **저장**을 클릭합니다.
- 8 **네트워킹 > Tier-0 게이트웨이** 또는 **네트워킹 > Tier-1 게이트웨이**로 이동하여 게이트웨이에 대한 DHCP 릴레이 서버를 구성합니다.
- 9 적절한 게이트웨이를 편집합니다.
- 10 **IP 주소 관리** 필드에서 Tier-0 게이트웨이에 대해 **IP 할당 없음** 또는 Tier-1 게이트웨이에 대해 **IP 할당 집합 없음**을 클릭합니다.
- 11 **유형** 필드에서 **DHCP 릴레이**를 선택합니다.
- 12 **DHCP 릴레이** 필드에서 이전에 생성한 DHCP 릴레이 서버를 선택합니다.

13 **저장**을 클릭합니다.

14 이 DHCP 릴레이 서비스를 사용하는 게이트웨이에 연결된 각 세그먼트에 대해 릴레이가 작동할 DHCP 범위를 지정해야 합니다.

- a **네트워킹 > 세그먼트**로 이동합니다.
- b 세그먼트를 추가하거나 편집합니다.
- c 새 세그먼트를 추가하는 경우 **서브넷 설정**을 클릭하고, 서브넷을 수정하려면 **서브넷** 아래의 숫자를 클릭합니다.
- d 하나 이상의 DHCP 범위를 지정합니다.
이는 릴레이가 작동하는 데 필요합니다.
- e **적용**을 클릭합니다.
- f **저장**을 클릭합니다.

IP 주소 풀 추가

DHCP 같은 구성 요소에 사용하기 위한 IP 주소 풀을 구성할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > IP 주소 관리 > IP 주소 풀**을 선택합니다.
- 3 **IP 주소 풀 추가**를 클릭합니다.
- 4 이름과 설명(선택 사항)을 입력합니다.
- 5 서브넷을 추가하려면 **서브넷** 열에서 **설정**을 클릭합니다.
- 6 주소 블록을 지정하려면 **서브넷 추가 > IP 블록**을 선택합니다.
 - a IP 블록을 선택합니다.
 - b 크기를 지정합니다.
 - c **게이트웨이 자동 할당** 토글을 클릭하여 자동 게이트웨이 IP 할당을 사용하거나 사용하지 않도록 설정합니다.
 - d **추가**를 클릭합니다.
- 7 IP 범위를 지정하려면 **서브넷 추가 > IP 범위**를 선택합니다.
 - a IPv4 또는 IPv6 IP 범위를 입력합니다.
 - b IP 범위를 CIDR 형식으로 입력합니다.

c **게이트웨이 IP**에 대한 주소를 입력합니다.

d **추가**를 클릭합니다.

8 **저장**을 클릭합니다.

IP 주소 블록 추가

다른 구성 요소에서 사용할 IP 주소 블록을 구성할 수 있습니다.

참고 [고급 네트워킹 및 보안 > 네트워킹 > IPAM](#)으로 이동하여 IP주소 블록을 추가할 수도 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **네트워킹 > IP 주소 관리 > IP 주소 풀**을 선택합니다.
- 3 **IP 주소 블록** 탭을 클릭합니다.
- 4 **IP 주소 블록 추가**를 클릭합니다.
- 5 이름과 설명(선택 사항)을 입력합니다.
- 6 IP 블록을 CIDR 형식으로 입력합니다.
- 7 **저장**을 클릭합니다.

이 섹션의 항목에서는 분산 방화벽 규칙, ID 방화벽, 네트워크 검사, 게이트웨이 방화벽 및 끝점 보호 정책에 대한 복습 및 동서 보안을 다룹니다.

본 장은 다음 항목을 포함합니다.

- 보안 구성 개요
- 보안 용어
- ID 기반 방화벽
- 계층 7 컨텍스트 프로파일
- 분산 방화벽
- East-West 네트워크 보안 - 타사 서비스 연결
- 게이트웨이 방화벽 구성
- 종방향 네트워크 보안 - 타사 서비스 삽입
- 끝점 보호
- 보안 프로파일

보안 구성 개요

환경에 대해 미리 정의된 범주 아래에 East-West 및 North-South 방화벽 정책을 구성합니다.

분산 방화벽(East-West) 및 게이트웨이 방화벽(North-South)은 범주로 구분된 여러 구성 가능한 규칙 집합을 제공합니다. 방화벽 적용에서 제외할 논리적 스위치, 논리적 포트 또는 그룹이 포함된 제외 목록을 구성할 수 있습니다.

보안 정책은 다음과 같이 적용됩니다.

- 규칙은 범주에서 왼쪽에서 오른쪽으로 처리됩니다.
- 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.

보안 용어

다음 용어는 분산 방화벽 전체에 사용됩니다.

표 10-1. 보안 관련 용어

구성체	정의
정책	보안 정책에는 방화벽 규칙 및 서비스 구성을 포함한 다양한 보안 요소가 포함되어 있습니다. 이전에는 정책을 방화벽 섹션이라고 했습니다.
규칙	흐름이 평가되는 기준이 되는 매개 변수 집합으로 일치 시 수행할 작업을 정의합니다. 규칙에는 소스 및 대상, 서비스, 컨텍스트 프로파일, 로깅 및 태그와 같은 매개 변수가 포함됩니다.
그룹	그룹은 정적으로 추가되고 동적으로 추가된 다른 개체를 포함하며 방화벽 규칙의 소스 및 대상 필드로 사용될 수 있습니다. 그룹은 가상 시스템, IP 집합, MAC 집합, 논리적 포트, 논리적 스위치, AD 사용자 그룹 및 기타 중첩된 그룹의 조합을 포함하도록 구성할 수 있습니다. 그룹의 동적 포함은 태그, 시스템 이름, OS 이름 또는 컴퓨터 이름을 기반으로 할 수 있습니다. 그룹을 생성할 때 그룹이 속할 도메인을 포함해야 하며 기본적으로 이 도메인이 기본 도메인입니다. 이전에는 그룹을 NSGroup 또는 보안 그룹이라고 했습니다.
서비스	포트 및 프로토콜의 조합을 정의합니다. 포트 및 프로토콜을 기반으로 트래픽을 분류하는 데 사용됩니다. 방화벽 규칙에서 사전 정의된 서비스 및 사용자 정의 서비스를 사용할 수 있습니다.
컨텍스트 프로파일	애플리케이션 ID 및 도메인 이름을 포함한 컨텍스트 인식 특성을 정의합니다. 애플리케이션 버전 또는 암호 집합과 같은 하위 특성도 포함됩니다. 방화벽 규칙에는 계층 7 방화벽 규칙을 사용하도록 설정하기 위한 컨텍스트 프로파일이 포함될 수 있습니다.

ID 기반 방화벽

IDFW(ID 기반 방화벽) 기능을 사용하여 NSX 관리자는 Active Directory 사용자 기반 DFW(분산 방화벽) 규칙을 생성할 수 있습니다.

IDFW는 가상 데스크톱(VDI) 또는 원격 데스크톱 세션(RDSH 지원)에 사용할 수 있기 때문에, 여러 사용자가 동시에 로그인 가능하고 요구 사항을 기반으로 사용자 애플리케이션에 액세스할 수 있고 독립형 사용자 환경을 유지 보수할 수 있습니다. VDI 관리 시스템은 어떤 사용자가 VDI 가상 시스템에 대한 액세스 권한을 부여 받을지를 제어합니다. NSX-T는 IDFW가 사용하도록 설정된 소스 VM(가상 시스템)에서 대상 서버에 대한 액세스를 제어합니다. RDSH를 통해, 관리자는 AD(Active Directory)에서 여러 사용자가 포함된 보안 그룹을 생성하고 사용자가 자신의 역할을 기반으로 애플리케이션 서버에 액세스하는 것을 허용하거나 거부합니다. 예를 들어 인적 자원 및 엔지니어링은 동일한 RDSH 서버에 연결하여 해당 서버의 다른 애플리케이션에 액세스 할 수 있습니다.

지원되는 운영 체제가 있는 VM에서 IDFW를 사용할 수도 있습니다. ID 방화벽 지원 구성 항목을 참조하십시오.

고급 수준의 IDFW 구성 워크플로 개요는 인프라의 준비에서 시작됩니다. 준비에는 관리자가 보호된 각 클러스터에서 호스트 준비 구성 요소를 설치하고 Active Directory 동기화를 설정하여 NSX에서 AD 사용자 및 그룹을 사용할 수 있도록 하는 과정이 포함됩니다. 다음으로 IDFW는 Active Directory 사용자가 IDFW 규칙을 적용하기 위해 로그인하는 데스크톱을 알고 있어야 합니다. 네트워크 이벤트가 사용자에 의해 생성되면, VM에 VMware Tools와 함께 설치된 Thin 에이전트는 정보를 수집하고 전달하여 컨텍스트 엔진으로 보냅니다. 이 정보는 분산 방화벽에 대한 적용을 제공하는 데 사용됩니다.

IDFW는 분산 방화벽 규칙에서만 소스의 사용자 ID를 처리합니다. ID 기반 그룹은 DFW 규칙에서 대상으로 사용할 수 없습니다.

참고 IDFW는 게스트 운영 체제의 보안 및 무결성에 의존합니다. 악의적인 로컬 관리자가 방화벽 규칙을 우회하기 위해 해당 ID를 스푸핑할 수 있는 여러 방법이 있습니다. 사용자 ID 정보는 게스트 VM 내부의 NSX Guest Introspection Thin Agent에서 제공됩니다. 보안 관리자는 각 게스트 VM에 Thin Agent가 설치 및 실행되고 있는지 확인해야 합니다. 로그인한 사용자에게 에이전트를 제거하거나 중지할 수 있는 권한이 없어야 합니다.

지원되는 IDFW 구성에 대해서는 [ID 방화벽 지원 구성](#) 내용을 참조하십시오.

IDFW 워크플로:

- 1 사용자가 VM에 로그인하고 Skype 또는 Outlook을 열어 네트워크 연결을 시작합니다.
- 2 사용자 로그인 이벤트가 Thin Agent에 의해 감지되고, 연결 정보 및 ID 정보를 수집하여 컨텍스트 엔진에 보냅니다.
- 3 컨텍스트 엔진은 해당 규칙 적용을 위해 연결 및 ID 정보를 분산 방화벽으로 전달합니다.

ID 방화벽 워크플로

IDFW는 사용자 ID 기반 방화벽 규칙을 허용하여 기존 방화벽을 향상합니다. 예를 들어 관리자는 단일 방화벽 정책을 사용하여 고객 지원 담당자가 HR 데이터베이스에 액세스하도록 허용하거나 허용하지 않을 수 있습니다.

ID 기반 분산 방화벽 규칙은 AD(Active Directory) 그룹 멤버 자격의 자격에 따라 결정됩니다. [ID 방화벽 지원 구성](#) 항목을 참조하십시오.

IDFW는 분산 방화벽 규칙에서만 소스의 사용자 ID를 처리합니다. ID 기반 그룹은 DFW 규칙에서 대상으로 사용할 수 없습니다.

참고 ID 방화벽 규칙 적용의 경우 Active Directory를 사용하는 모든 VM에 대해 Windows 시간을 설정해야 합니다. 이렇게 하면 Active Directory와 VM 간에 날짜와 시간이 동기화됩니다. 사용자를 사용하도록 설정하거나 삭제하는 경우를 비롯한 AD 그룹 멤버 자격 변경 시 로그인한 사용자에게 즉시 영향을 주지 않습니다. 변경 사항을 적용하려면 로그아웃했다가 다시 로그인해야 합니다. 그룹 멤버 자격이 수정된 경우 AD 관리자가 강제로 로그아웃해야 합니다. 이 동작은 Active Directory의 제한 사항입니다.

사전 요구 사항

VM에서 Windows 자동 로그인에 사용하도록 설정된 경우 **로컬 컴퓨터 정책 > 컴퓨터 구성 > 관리 템플릿 > 시스템 > 로그인**으로 이동한 후 **컴퓨터 시작 및 로그인 시 항상 네트워크 대기**를 사용하도록 설정합니다. 지원되는 IDFW 구성에 대해서는 **ID 방화벽 지원 구성** 내용을 참조하십시오.

절차

- 1 NSX File Introspection 드라이버 및 NSX Network Introspection 드라이버를 사용하도록 설정합니다. VMware Tools 전체 설치에서는 기본적으로 이러한 드라이버를 추가합니다.
- 2 클러스터 또는 독립형 호스트에서 IDFW를 사용하도록 설정합니다. **ID 기반 방화벽 사용**.
- 3 Active Directory 도메인을 구성합니다. **Active Directory 추가**.
- 4 Active Directory 동기화 작업을 구성합니다. **Active Directory 동기화**.
- 5 Active Directory 그룹 멤버가 포함된 SG(보안 그룹)를 생성합니다. **그룹 추가**.
- 6 분산 방화벽 규칙에 AD 그룹 멤버가 포함된 SG를 할당합니다. **분산 방화벽 추가**.

ID 기반 방화벽 사용

IDFW 방화벽 규칙을 적용하려면 ID 기반 방화벽을 사용하도록 설정해야 합니다.

절차

- 1 **보안 > 분산 방화벽**을 선택합니다.
- 2 왼쪽 모서리에서 **작업 > 일반 설정**을 클릭합니다.
- 3 상태 버튼을 전환하여 IDFW를 사용하도록 설정합니다.
또한 IDFW가 작동하려면 분산 방화벽도 사용하도록 설정해야 합니다.
- 4 독립형 호스트 또는 클러스터에서 IDFW를 사용하도록 설정하려면 **ID 방화벽 설정** 탭을 선택합니다.
- 5 **사용** 표시줄을 전환하고 독립형 호스트를 선택하거나 IDFW 호스트를 사용하도록 설정해야 하는 클러스터를 선택합니다.
- 6 **저장**을 클릭합니다.

ID 방화벽 모범 사례

다음 모범 사례는 ID 방화벽 규칙의 성공을 최대화하는 데 도움이 됩니다.

- IDFW는 다음 프로토콜을 지원합니다.:
 - 단일 사용자(VDI 또는 비 RDSH 서버) 사용 사례 지원 - TCP, UDP, ICMP
 - 다중 사용자(RDSH) 사용 사례 지원 - TCP, UDP
- 단일 ID 기반 그룹은 분산 방화벽 규칙 내에서만 소스로 사용할 수 있습니다. 소스에 IP 및 ID 기반 그룹이 필요한 경우 두 개의 별도 방화벽 규칙을 생성합니다.

- 도메인 이름 변경을 비롯한 모든 도메인 변경 시 **Active Directory**와의 전체 동기화를 트리거합니다. 전체 동기화는 시간이 오래 걸릴 수 있으므로 사용량이 많지 않을 때나 근무 외 시간에 동기화하는 것이 좋습니다.
- 로컬 도메인 컨트롤러의 경우 기본 LDAP 포트 389 및 LDAP 포트 636은 **Active Directory** 동기화에 사용되며 기본값과 다르게 편집해서는 안 됩니다.

ID 방화벽 지원 구성

다음 구성은 VM(가상 시스템)의 IDFW에 대해 지원됩니다. 물리적 디바이스에 대한 IDFW는 지원되지 않습니다.

게스트 운영 체제	적용 유형
Windows 8	데스크톱 - 데스크톱 사용자 사용 사례 지원
Windows 10	데스크톱 - 데스크톱 사용자 사용 사례 지원
Windows 2012	서버 - 서버 사용자 사용 사례 지원
Windows 2012R2	서버 - 서버 사용자 사용 사례 지원
Windows 2016	서버 - 서버 사용자 사용 사례 지원
Windows 2012R2	RDSH - 원격 데스크톱 세션 호스트 지원
Windows 2016	RDSH - 원격 데스크톱 세션 호스트 지원

Active Directory 도메인 컨트롤러:

- Windows Server 2012
- Windows Server 2012R2
- Windows Server 2016
- Windows Server 2019

호스트 운영 체제: ESXi

VMware Tools - 버전 11

- VMCI 드라이버
- NSX 파일 자체 검사 드라이버
- NSX 네트워크 검사 드라이버

계층 7 컨텍스트 프로파일

계층 7 애플리케이션 ID는 컨텍스트 프로파일의 일부로 구성됩니다.

컨텍스트 프로파일은 하나 이상의 특성을 지정할 수 있으며, DFW(분산 방화벽) 규칙 및 게이트웨이 방화벽 규칙에 사용하기 위한 하위 특성을 포함할 수도 있습니다. TLS 버전 1.2와 같은 하위 특성이 정의되면 여러 애플리케이션 ID 특성이 지원되지 않습니다. DFW는 특성 외에도 FQDN 화이트리스트 또는 블랙리스트 추가를 위한 컨텍스트 프로파일에 지정할 수 있는 FQDN(정규화된 도메인 이름) 또는 URL을 지원합니다. 현재 미리 정의된 도메인 목록이 지원됩니다. FQDN을 컨텍스트 프로파일의 특성으로 구성하거나, 각각 서로 다른 컨텍스트 프로파일에 설정할 수 있습니다. 컨텍스트 프로파일이 정의되면 하나 이상의 분산 방화벽 규칙에 적용할 수 있습니다.

현재 미리 정의된 도메인 목록이 지원됩니다. 특성 유형 "도메인(FQDN) 이름"의 새 컨텍스트 프로파일을 추가할 때 FQDN 목록을 볼 수 있습니다. API 호출 `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME`을 실행하여 FQDN 목록을 볼 수도 있습니다.

참고

- 게이트웨이 방화벽 규칙은 컨텍스트 프로파일에서 FQDN 특성 또는 기타 하위 특성의 사용을 지원하지 않습니다.
- 컨텍스트 프로파일은 Tier-0 게이트웨이 방화벽 정책에서 지원되지 않습니다. 게이트웨이 방화벽 규칙은 FQDN 특성 또는 기타 하위 특성의 사용을 지원하지 않습니다.

컨텍스트 프로파일이 규칙에 사용되면 가상 시스템에서 들어오는 트래픽이 5-튜플 기준 규칙 테이블과 일치하는지 확인됩니다. 규칙이 일치하면 흐름에 계층 7 컨텍스트 프로파일도 포함되며, 해당 패킷은 vDPI 엔진이라는 사용자 공간 구성 요소로 리디렉션됩니다. 적은 수의 후속 패킷이 각 흐름의 해당 vDPI 엔진으로 펀트되고 일단 애플리케이션 ID가 결정되면 이 정보는 커널 내 컨텍스트 테이블에 저장됩니다. 흐름에 대한 다음 패킷이 들어오면 컨텍스트 테이블의 정보가 규칙 테이블과 다시 비교되고 5-튜플 및 계층 7 애플리케이션 ID에 대해 일치하는지 확인됩니다. 완전 일치 규칙에 정의된 대로 적절한 작업이 수행되고, 허용 규칙의 경우, 흐름에 대한 모든 후속 패킷이 커널에서 처리되고 연결 테이블과 일치하는지 확인됩니다. 완전 일치 DROP 규칙의 경우 거부 패킷이 생성됩니다. 방화벽에 의해 생성된 로그에는 해당 흐름이 DPI에 펀트된 경우 계층 7 애플리케이션 ID 및 해당 URL이 포함됩니다.

수신 패킷에 대한 규칙 처리:

- 1 DFW 또는 게이트웨이 필터를 입력하면 5-튜플 기준의 흐름 테이블에서 패킷이 조회됩니다.
- 2 흐름/상태가 없는 경우 5-튜플 기준의 규칙 테이블에서 일치하는 흐름이 있는지 검색되고, 흐름 테이블에 항목이 생성됩니다.
- 3 흐름이 계층 7 서비스 개체가 있는 규칙과 일치하는 경우 흐름 테이블 상태는 "DPI 진행 중"으로 표시됩니다.
- 4 그런 후 트래픽이 DPI 엔진에 펀트됩니다. DPI 엔진은 애플리케이션 ID를 확인합니다.
- 5 애플리케이션 ID가 확인되면 DPI 엔진은 이 흐름에 대한 컨텍스트 테이블에 삽입되는 특성을 전송합니다. "DPI 진행 중" 플래그가 제거되고 트래픽은 더 이상 DPI 엔진에 펀트되지 않습니다.
- 6 흐름(이제 애플리케이션 ID 포함)은 5-튜플에 따라 일치하는 원래 규칙부터 시작해서 애플리케이션 ID와 일치하는 규칙이 있는지 모두 다시 평가되고 최초 완전 일치 L4/L7 규칙이 선택됩니다. 적절한 작업(허용/거부/거절)이 수행되고, 그에 따라 흐름 테이블 항목이 업데이트됩니다.

계층 7 방화벽 규칙 워크플로

계층 7 애플리케이션 ID는 분산 방화벽 규칙 또는 게이트웨이 방화벽 규칙에 사용되는 컨텍스트 프로파일을 생성하는 데 사용됩니다. 특성을 기준으로 규칙을 적용하면 사용자는 애플리케이션을 임의의 포트에서 실행하는 것을 허용 또는 거부할 수 있습니다.

NSX-T는 공통 인프라 및 엔터프라이즈 애플리케이션을 위한 기본 제공 특성을 제공합니다. 애플리케이션 ID에는 버전(SSL/TLS 및 CIFS/SMB)과 암호 그룹(SSL/TLS)이 포함됩니다. 분산 방화벽의 경우 애플리케이션 ID는 컨텍스트 프로파일을 통해 규칙에서 사용되며 FQDN 화이트리스트 및 블랙리스트와 함께 사용할 수 있습니다. 애플리케이션 ID는 ESXi 및 KVM 호스트에서 지원됩니다.

참고

- 게이트웨이 방화벽 규칙은 컨텍스트 프로파일에서 FQDN 특성 또는 기타 하위 특성의 사용을 지원하지 않습니다.
- 컨텍스트 프로파일은 Tier-0 게이트웨이 방화벽 정책에서 지원되지 않습니다. 게이트웨이 방화벽 규칙은 FQDN 특성 또는 기타 하위 특성의 사용을 지원하지 않습니다.

지원되는 애플리케이션 ID 및 FQDN:

- FQDN의 경우 사용자는 포트 53에서 지정된 DNS 서버의 DNS 애플리케이션 ID로 높은 우선 순위 규칙을 구성해야 합니다.
- ALG 애플리케이션 ID(FTP, ORACLE, DCERPC, TFTP)에는 방화벽 규칙에 해당하는 ALG 서비스가 필요합니다.
- SYSLOG 애플리케이션 ID는 표준 포트에서만 감지됩니다.

KVM 지원되는 애플리케이션 ID 및 FQDN:

- 하위 특성은 KVM에서 지원되지 않습니다.
- FTP 및 TFTP ALG 애플리케이션 ID는 KVM에서 지원됩니다.

계층 7과 ICMP 또는 다른 프로토콜의 조합을 사용하는 경우 계층 7 방화벽 규칙을 마지막에 배치해야 합니다. 계층 7 위의 모든 규칙은 실행되지 않습니다.

절차

- 1 사용자 지정 컨텍스트 프로파일을 생성합니다. **컨텍스트 프로파일 추가**.
- 2 분산 방화벽 규칙 또는 게이트웨이 방화벽 규칙에서 컨텍스트 프로파일을 사용합니다. **분산 방화벽 추가 또는 게이트웨이 방화벽 정책 및 규칙 추가**.

서비스가 **임의**로 설정된 방화벽 규칙에서는 여러 애플리케이션 ID 컨텍스트 프로파일을 사용할 수 있습니다. ALG 프로파일(FTP, ORACLE, DCERPC, TFTP)의 경우, 규칙당 하나의 컨텍스트 프로파일이 지원됩니다.

특성

계층 7 특성(애플리케이션 ID)은 특정 패킷 또는 흐름이 사용되는 포트와 관계없이, 이러한 패킷 또는 흐름이 생성된 애플리케이션을 식별합니다.

애플리케이션 ID에 따른 적용 기능을 사용하여 모든 포트에서 애플리케이션이 실행되도록 허용하거나 거부할 수도 있고, 강제로 애플리케이션이 해당 표준 포트에서 실행되도록 할 수도 있습니다. vDPI는 일반적으로 서명이라고 하는 정의된 패턴에 따라 일치하는 패킷 페이로드를 사용하도록 설정합니다. 서명 기반 식별 및 적용을 통해 고객은 흐름이 속하는 특정 애플리케이션/프로토콜뿐만 아니라 해당 프로토콜의 버전(예: TLS 버전 1.0 버전 TLS 버전 1.2) 또는 다른 버전의 CIFS 트래픽과도 일치시킬 수 있습니다. 이를 통해 고객은 데이터 센터 내 E-W 흐름 및 배포된 모든 애플리케이션에 대해 알려진 취약점이 있는 프로토콜의 가시성을 확보하거나 프로토콜의 사용을 제한할 수 있습니다.

계층 7 애플리케이션 ID는 분산 방화벽 및 게이트웨이 방화벽 규칙의 컨텍스트 프로파일에서 사용되며 ESXi 및 KVM 호스트에서 지원됩니다.

참고 NFS 버전 4는 지원되지 않는 특성입니다.

참고

- 게이트웨이 방화벽 규칙은 컨텍스트 프로파일에서 FQDN 특성 또는 기타 하위 특성의 사용을 지원하지 않습니다.
 - 컨텍스트 프로파일은 Tier-0 게이트웨이 방화벽 정책에서 지원되지 않습니다. 게이트웨이 방화벽 규칙은 FQDN 특성 또는 기타 하위 특성의 사용을 지원하지 않습니다.
-

지원되는 애플리케이션 ID 및 FQDN:

- FQDN의 경우 사용자는 포트 53에서 지정된 DNS 서버의 DNS 애플리케이션 ID로 높은 우선 순위 규칙을 구성해야 합니다.
- ALG 애플리케이션 ID(FTP, ORACLE, DCERPC, TFTP)에는 방화벽 규칙에 해당하는 ALG 서비스가 필요합니다.
- SYSLOG 애플리케이션 ID는 표준 포트에서만 감지됩니다.

KVM 지원되는 애플리케이션 ID 및 FQDN:

- 하위 특성은 KVM에서 지원되지 않습니다.
- FTP 및 TFTP ALG 애플리케이션 ID는 KVM에서 지원됩니다.

특성(애플리케이션 ID)	설명	유형
360ANTIV	360 Safeguard는 중국의 IT 기업인 Qihoo 360이 개발한 프로그램입니다.	웹 서비스
ACTIVDIR	Microsoft Active Directory	네트워킹
AMQP	Advanced Message Queuing Protocol은 애플리케이션 또는 조직 간의 비즈니스 메시지 통신을 지원하는 애플리케이션 계층 프로토콜입니다.	네트워킹

특성(애플리케이션 ID)	설명	유형
AVAST	Avast!의 Avast.com 공식 웹 사이트를 검색할 때 생성되는 트래픽 Antivirus 다운로드	웹 서비스
AVG	AVG Antivirus/Security 소프트웨어 다운로드 및 업데이트	파일 전송
AVIRA	Avira Antivirus/Security 소프트웨어 다운로드 및 업데이트	파일 전송
BLAST	데이터 센터에서 컴퓨팅 환경을 압축, 암호화 및 인코딩한 후 VMware Horizon 데스크톱용 표준 IP 네트워크를 통해 전송하는 원격 액세스 프로토콜입니다.	원격 액세스
BDEFENDER	BitDefender Antivirus/Security 소프트웨어 다운로드 및 업데이트	파일 전송
CA_CERT	CA(인증 기관)는 메시지 암호화에 대한 공용 키 소유권을 인증하는 디 지털 인증서를 발급합니다.	네트워킹
CIFS	CIFS(Common Internet File System)는 디렉토리, 파일, 프린터, 직렬 포트 및 네트워크의 노드 간 기타 통신에 대한 공유 액세스를 제공하 는 데 사용됩니다.	파일 전송
CLDAP	Connectionless Lightweight Directory Access Protocol은 UDP를 사용하는 IP(인터넷 프로토콜) 네트워크를 통해 분산 디렉토리 정보 서 비스를 액세스하고 유지하는 애플리케이션 프로토콜입니다.	네트워킹
CTRXCGP	Citrix Common Gateway Protocol은 UDP를 사용하는 IP(인터넷 프 로토콜) 네트워크를 통해 분산 디렉토리 정보 서비스를 액세스하고 유 지하는 애플리케이션 프로토콜입니다.	데이터베이스
CTRXCOTO	Hosting Citrix GoToMeeting 또는 GoToMeeting 플랫폼을 기준으로 하는 유사한 세션입니다. 음성, 비디오 및 제한된 군중 관리 기능을 포 함합니다.	공동 작업
CTRXCICA	ICA(Independent Computing Architecture)는 Citrix Systems에서 디자인한 애플리케이션 서버 시스템용 독점 프로토콜입니다.	원격 액세스
DCERPC	분산 컴퓨팅 환경/원격 프로시저 호출은 DCE(분산 컴퓨팅 환경)용으로 개발된 원격 프로시저 호출 시스템입니다.	네트워킹
DIAMETER	컴퓨터 네트워크에 대한 인증, 권한 부여 및 계정 프로토콜	네트워킹
DHCP	DHCP는 네트워크 내의 IP 주소 분산의 관리에 사용되는 프로토콜입니 다.	네트워킹
DNS	TCP 또는 UDP를 통해 DNS 서버 쿼리	네트워킹
EPIC	Epic EMR은 환자 치료 및 의료 정보를 제공하는 전자 의료 기록 애플 리케이션입니다.	클라이언트 서버
ESET	Eset Antivirus/Security 소프트웨어 다운로드 및 업데이트	파일 전송
FPROT	F-Prot Antivirus/Security 소프트웨어 다운로드 및 업데이트	파일 전송
FTP	FTP(파일 전송 프로토콜)는 파일 서버에서 로컬 시스템으로 파일을 전 송하는 데 사용됩니다.	파일 전송
GITHUB	웹 기반 Git 또는 버전 제어 저장소 및 인터넷 호스팅 서비스	공동 작업

특성(애플리케이션 ID)	설명	유형
HTTP	(HyperText Transfer Protocol) World Wide Web용 주요 전송 프로토콜	웹 서비스
HTTP2	HTTP 2.0 프로토콜을 지원하는 웹 사이트를 검색할 때 생성되는 트래픽	웹 서비스
IMAP	IMAP(Internet Message Access Protocol)는 원격 서버에서 이메일에 액세스하기 위한 인터넷 표준 프로토콜입니다.	메일
KASPRSKY	Kaspersky Antivirus/Security 소프트웨어 다운로드 및 업데이트	파일 전송
KERBEROS	Kerberos는 비밀 키 암호화를 사용하여 클라이언트/서버 애플리케이션에 대한 강력한 인증을 제공하도록 고안된 네트워크 인증 프로토콜입니다.	네트워킹
LDAP	LDAP(Lightweight Directory Access Protocol)는 IP 네트워크를 통해 디렉토리를 읽고 편집하기 위한 프로토콜입니다.	데이터베이스
MAXDB	MaxDB SQL Server에 대해 수행된 SQL 연결 및 쿼리	데이터베이스
MCAFFEE	McAfee Antivirus/Security 소프트웨어 다운로드 및 업데이트	파일 전송
MSSQL	Microsoft SQL Server는 관계형 데이터베이스입니다.	데이터베이스
NFS	클라이언트 컴퓨터의 사용자가 로컬 스토리지에 액세스하는 것과 비슷한 방법으로 네트워크를 통해 파일에 액세스할 수 있도록 합니다. 참고 NFS 버전 4는 지원되지 않는 특성입니다.	파일 전송
NNTP	뉴스 서버 간에 유즈넷 뉴스 기사(netnews)를 전송하고 최종 사용자 클라이언트 애플리케이션에서 기사를 읽고 게시하는 데 사용되는 인터넷 애플리케이션 프로토콜입니다.	파일 전송
NTBIOSNS	NetBIOS 이름 서비스입니다. 세션을 시작하거나 데이터그램을 배포하기 위해 애플리케이션은 이름 서비스를 사용하여 해당 NetBIOS 이름을 등록해야 합니다.	네트워킹
NTP	NTP(Network Time Protocol)은 네트워크를 통해 컴퓨터 시스템의 시계를 동기화하는 데 사용됩니다.	네트워킹
OCSP	사용자의 개인 키가 손상 또는 해지되지 않았음을 확인하는 OCSP 응답자	네트워킹
ORACLE	Oracle Corporation에서 생산하고 판매하는 ORDBMS(개체 관계형 데이터베이스 관리 시스템)입니다.	데이터베이스
PANDA	Panda Security Antivirus/Security 소프트웨어 다운로드 및 업데이트입니다.	파일 전송
PCOIP	데이터 센터에서 컴퓨팅 환경을 압축, 암호화 및 인코딩한 후 표준 IP 네트워크를 통해 전송하는 원격 액세스 프로토콜입니다.	원격 액세스
POP2	POP(Post Office Protocol)는 로컬 이메일 클라이언트가 원격 서버에서 이메일을 검색하는 데 사용하는 프로토콜입니다.	메일
POP3	Microsoft에서 구현한 NetBIOS 컴퓨터 이름에 대한 이름 서버 및 서비스인 NBNS(NetBIOS 이름 서비스)입니다.	메일

특성(애플리케이션 ID)	설명	유형
RADIUS	컴퓨터에서 네트워크 서비스를 연결 및 사용하기 위한 중앙 집중식 인증, 권한 부여 및 계정(AAA) 관리 기능을 제공합니다.	네트워킹
RDP	RDP(원격 데스크톱 프로토콜)은 사용자에게 다른 컴퓨터에 대한 그래픽 인터페이스를 제공합니다.	원격 액세스
RTCP	RTCP(실시간 전송 제어 프로토콜)은 RTP(실시간 전송 프로토콜)의 동급 프로토콜입니다. RTCP는 RTP 흐름에 대한 대역외 제어 정보를 제공합니다.	스트리밍 미디어
RTP	RTP(실시간 전송 프로토콜)은 기본적으로 실시간 오디오 및 비디오를 제공하는 데 사용됩니다.	스트리밍 미디어
RTSP	RTSP(실시간 스트리밍 프로토콜)은 끝점 간에 미디어 세션을 설정 및 제어하는 데 사용됩니다.	스트리밍 미디어
SIP	SIP(Session Initiation Protocol)은 음성 및 영상 통화를 설정하고 제어하기 위한 일반 제어 프로토콜입니다.	스트리밍 미디어
SMTP	SMTP(Simple Mail Transfer Protocol)은 IP(인터넷 프로토콜) 네트워크 간의 이메일 전송을 위한 인터넷 표준입니다.	메일
SNMP	SNMP(Simple Network Management Protocol)는 IP 네트워크에서 디바이스를 관리하기 위한 인터넷 표준 프로토콜입니다.	네트워크 모니터링
SSH	SSH(보안 셸)은 네트워크로 연결된 두 디바이스 간에 보안 채널을 사용하여 데이터를 교환할 수 있도록 하는 네트워크 프로토콜입니다.	원격 액세스
SSL	SSL(Secure Sockets Layer)은 인터넷을 통해 보안을 제공하는 암호화 프로토콜입니다.	웹 서비스
SYMUPDAT	Symantec LiveUpdate 트래픽으로, 스카이웨어 정의, 방화벽 규칙, 바이러스 백신 서명 파일 및 소프트웨어 업데이트를 포함합니다.	파일 전송
SYSLOG	SYSLOG는 네트워크 디바이스가 로깅 서버에 이벤트 메시지를 보낼 수 있도록 하는 프로토콜입니다.	네트워크 모니터링
TELNET	가상 터미널 연결을 사용하여 양방향 대화형 텍스트 지향 통신 기능을 제공하기 위해 인터넷 또는 LAN(Local Area Network)에서 사용되는 네트워크 프로토콜입니다.	원격 액세스
TFTP	WinAgents TFTP 클라이언트와 같은 클라이언트를 사용하여 SolarWinds TFTP Server와 같은 TFTP 서버에 파일을 나열하고 다운로드하고 업로드하는 데 사용되는 TFTP(Trivial File Transfer Protocol)입니다.	파일 전송
VNC	가상 네트워크 컴퓨팅에 대한 트래픽입니다.	원격 액세스
WINS	Microsoft에서 구현한 NetBIOS 컴퓨터 이름에 대한 이름 서버 및 서비스인 NBNS(NetBIOS 이름 서비스)입니다.	네트워킹

분산 방화벽

분산 방화벽에는 방화벽 규칙에 대해 미리 정의된 범주가 포함됩니다. 규칙은 위에서 아래로 평가되고 왼쪽에서 오른쪽으로 평가됩니다.

표 10-2. 분산 방화벽 규칙 범주

범주	설명
이더넷	계층 2 기반 규칙에 사용됨
진급	격리 및 허용 규칙에 사용됨
인프라	공유 서비스에 대한 액세스를 정의합니다. 글로벌 규칙 - AD, DNS, NTP, DHCP, 백업, 관리 서버
환경	영역 간 규칙 - 운영 및 개발, 사업부 간 규칙
애플리케이션	애플리케이션, 애플리케이션 계층 간 규칙 또는 마이크로 서비스 간 규칙

방화벽 초안

초안은 정책 섹션 및 규칙을 포함하는 완전한 분산 방화벽 구성입니다. 초안은 자동으로 저장하거나 수동으로 저장할 수 있고, 즉시 게시하거나 나중에 게시하기 위해 저장할 수 있습니다.

수동 초안 방화벽 구성을 저장하려면 분산 방화벽 화면의 오른쪽 상단으로 이동한 후 **작업 > 저장**을 클릭하십시오. 구성을 저장한 후 **작업 > 보기**를 선택하여 구성을 볼 수 있습니다. 자동 초안은 기본적으로 사용하도록 설정됩니다. **작업 > 일반 설정**으로 이동하여 자동 초안을 사용하지 않도록 설정할 수 있습니다. 자동 초안을 사용하도록 설정한 경우 방화벽 구성을 변경하면 시스템에서 자동 초안을 생성합니다. 최대 100개의 자동 초안 및 10개의 수동 초안을 저장할 수 있습니다. 자동 초안은 편집한 후 수동 초안으로 저장하여 지금 또는 나중에 게시할 수 있습니다. 여러 사용자가 초안을 열고 편집하지 못하도록 하기 위해 수동 초안을 잠글 수 있습니다. 초안이 게시되면 현재 구성이 초안의 구성으로 바뀝니다.

방화벽 초안 저장 또는 보기

초안은 게시되었거나 나중에 게시하기 위해 저장한 분산 방화벽 구성입니다. 초안은 자동으로 또는 수동으로 생성됩니다.

수동 초안을 편집 및 저장할 수 있습니다. 자동 초안을 복제하고 수동 초안으로 저장한 다음, 편집할 수 있습니다. 저장할 수 있는 최대 초안 수는 자동 초안 100개, 수동 초안 10개입니다.

절차

- 1 **보안 > 분산 방화벽**을 클릭합니다.
- 2 방화벽 구성을 수동으로 저장하려면 **작업 > 저장**으로 이동합니다.
수동 초안을 저장하거나 편집한 후 저장할 수 있습니다. 저장한 후 원래 구성으로 되돌릴 수 있습니다.
- 3 구성에 **이름을 지정**합니다.
- 4 여러 사용자가 수동 초안을 열고 편집하지 못하게 하려면 구성을 **잠그고** 설명을 추가합니다.
- 5 **저장**을 클릭합니다.

6 저장된 구성을 보려면 **작업 > 보기**를 클릭합니다.

저장된 모든 구성을 표시하는 타임라인이 열립니다. 초안 이름, 날짜, 시간 및 저장한 사용자 등의 세부 정보를 보려면 초안의 점 또는 별모양 아이콘을 가리킵니다. 저장된 구성은 시간별로 필터링되어 1일, 1주, 30일 또는 최근 3개월 동안의 모든 초안을 표시합니다. 자동 초안별로 필터링하고 저장할 수 있습니다. 또한 오른쪽 상단의 검색 도구를 사용하여 이름을 기준으로 필터링할 수도 있습니다.

7 초안 위로 마우스를 가져가면 저장된 구성의 이름, 날짜 및 시간 세부 정보가 표시됩니다. 초안 세부 정보를 보려면 이름을 클릭합니다.

세부 초안 보기에는 현재 방화벽 구성에서 필요한 변경 사항이 표시되므로 이 초안과 동기화 상태를 유지할 수 있습니다. 이 초안이 게시되면 이 보기에 표시되는 모든 변경 내용이 현재 구성에 적용됩니다.

아래쪽 화살표를 클릭하면 각 섹션이 확장되고 각 섹션에 추가, 수정 및 삭제된 변경 내용이 표시됩니다. 비교해보면 추가된 규칙은 상자 왼쪽에 녹색 막대가 표시되고, 수정된 요소(예: 이름 변경)는 노란색 막대가 표시되고, 삭제된 요소는 빨간색 막대가 표시됩니다.

8 선택한 초안의 이름 또는 설명을 편집하려면 **초안 세부 정보 보기** 창에서 메뉴 아이콘(3개의 점)을 클릭하고 **편집**을 선택합니다.

수동 초안은 잠글 수 있습니다. 잠글 경우 초안에 대한 설명을 제공해야 합니다.

엔터프라이즈 관리자와 같은 일부 역할은 전체 액세스 자격 증명을 가지며 잠글 수 없습니다. [역할 기반 액세스 제어](#) 항목을 참조하십시오.

9 **클론**을 클릭하여 자동 초안 및 수동 초안을 복제하고 저장할 수도 있습니다.

[저장된 구성] 창에서 기본 이름을 그대로 수락하거나 편집할 수 있습니다. 구성을 잠글 수도 있습니다. 잠글 경우 초안에 대한 설명을 제공해야 합니다.

10 초안 구성의 복제된 버전을 저장하려면 **저장**을 클릭합니다. 이제 초안이 [저장된 구성] 섹션에 표시됩니다.

다음에 수행할 작업

초안을 본 후에 로드하여 게시할 수 있습니다. 그러면 활성 방화벽 구성이 됩니다.

방화벽 초안 게시 또는 되돌리기

자동 초안 및 저장된 수동 초안을 둘 다 활성 구성이 되도록 로드 및 게시할 수 있습니다.

게시하는 동안 새 자동 초안이 생성됩니다. 이 자동 초안을 게시하여 이전 구성으로 되돌릴 수 있습니다.

절차

1 저장된 구성을 보려면 **작업 > 보기**를 클릭합니다.

저장된 모든 구성을 표시하는 타임라인이 열립니다. 초안 이름, 날짜, 시간 및 저장한 사용자 등의 세부 정보를 보려면 초안의 점 아이콘을 가리킵니다. 저장된 구성은 시간별로 필터링되어 1일, 1주, 30일 또는 최근 3개월 동안 생성된 모든 초안을 표시합니다.

2 초안 이름을 클릭하면 초안 세부 정보 보기 창이 나타납니다.

3 **로드**를 클릭합니다. 새 방화벽 구성이 주 창에 나타납니다.

참고 방화벽 필터가 사용되고 있거나 현재 구성에 저장되지 않은 변경 내용이 있는 경우 초안을 로드할 수 없습니다.

4 초안 구성을 커밋하고 활성화 상태로 만들려면 **게시**를 클릭합니다. 이전에 게시된 구성으로 돌아가려면 **되돌리기**를 클릭합니다.

게시 후 초안의 변경 내용이 활성화 구성에 표시됩니다.

5 게시하기 전에 선택한 초안의 콘텐츠를 편집하려면 **로드**를 클릭한 후 구성을 편집합니다.

6 초안 구성의 편집된 버전을 저장하려면 **작업 > 저장**을 클릭합니다.

수동 초안은 새 구성으로 저장하거나 기존 구성에 대한 업데이트로 저장할 수 있습니다. 자동 초안은 새 구성으로만 저장할 수 있습니다.

7 **이름** 및 **설명**(선택사항)을 입력합니다. 초안을 **잠글 수도** 있습니다. 잠글 경우 초안에 대한 설명을 제공해야 합니다.

8 **저장**을 클릭합니다.

9 초안 구성을 커밋하고 활성화 상태로 만들려면 **게시**를 클릭하고, 이전의 게시된 구성으로 돌아가려면 **되돌리기**를 클릭합니다.

분산 방화벽 추가

분산 방화벽(DFW)은 가상 시스템의 모든 횡방향 트래픽을 모니터링합니다.

사전 요구 사항

DFW로 보호되는 게스트 VM의 vNIC는 전송 영역에 연결된 N-VDS 논리적 스위치에 연결되어야 합니다.

ID 방화벽에 대한 규칙을 생성하는 경우 먼저 Active Directory 멤버로 그룹을 생성합니다. IDFW는 TCP 기반 방화벽 규칙만 지원합니다.

참고 ID 방화벽 규칙 적용의 경우 Active Directory를 사용하는 모든 VM에 대해 Windows 시간을 설정해야 합니다. 이렇게 하면 Active Directory와 VM 간에 날짜와 시간이 동기화됩니다. 사용자를 사용하도록 설정하거나 삭제하는 경우를 비롯한 AD 그룹 멤버 자격 변경 시 로그인한 사용자에게 즉시 영향을 주지 않습니다. 변경 사항을 적용하려면 로그아웃했다가 다시 로그인해야 합니다. 그룹 멤버 자격이 수정된 경우 AD 관리자가 강제로 로그아웃해야 합니다. 이 동작은 Active Directory의 제한 사항입니다.

계층 7과 ICMP 또는 다른 프로토콜의 조합을 사용하는 경우 계층 7 방화벽 규칙을 마지막에 배치해야 합니다. 계층 7 위의 모든 규칙은 실행되지 않습니다.

절차

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

2 탐색 패널에서 **보안 > 분산 방화벽**을 선택합니다.

- 3 **작업 > 일반 설정**을 선택하고 분산 방화벽 상태를 전환하여 분산 방화벽을 사용하도록 설정합니다. **저장**을 클릭합니다.
- 4 올바른 미리 정의된 범주에 있는지 확인하고 **정책 추가**를 클릭합니다. 범주에 대한 자세한 내용은 **분산 방화벽**을 참조하십시오.
- 5 새 정책 섹션에 대한 **이름**을 입력합니다.
- 6 (선택 사항) 다음 정책 설정을 구성하려면 톱니 바퀴 아이콘을 클릭합니다.

옵션	설명
TCP Strict	TCP 연결은 3방향 핸드셰이크(SYN, SYN-ACK, ACK)로 시작되고, 일반적으로 2방향 교환(FIN, ACK)으로 끝납니다. 특정 상황에서 DFW(분산 방화벽)가 특정 흐름의 3방향 핸드셰이크를 확인하지 못할 수 있습니다(예: 흐름이 존재하는 동안 비대칭 트래픽 또는 사용하도록 설정된 분산 방화벽으로 인해). 기본적으로 분산 방화벽은 3방향 핸드셰이크를 확인해야 한다는 요구를 적용하지 않으며 이미 설정된 세션을 선택합니다. 섹션별로 TCP Strict를 사용하도록 설정하여 중간 세션 선택을 해제하고 3방향 핸드셰이크에 대한 요구 사항을 적용할 수 있습니다. 특정 DFW 정책에 대해 TCP Strict 모드를 사용하도록 설정하고 기본 임의-임의 차단 규칙을 사용할 경우, 3방향 핸드셰이크 연결 요구 사항을 완료하지 못하고 이 섹션의 TCP 기반 규칙과 일치하는 패킷은 삭제됩니다. Strict는 상태 저장 TCP 규칙에만 적용되며 분산 방화벽 정책 수준에서 사용하도록 설정됩니다. TCP Strict는 TCP 서비스가 지정되지 않은 기본 임의-임의 허용과 일치하는 패킷에는 적용되지 않습니다.
상태 저장	상태 저장 방화벽은 활성 연결 상태를 모니터링하고 이 정보를 사용하여 방화벽을 통해 보낼 패킷을 결정합니다.
잠금	여러 사용자가 동일한 섹션을 편집하지 못하도록 정책을 잠글 수 있습니다. 섹션을 잠글 때는 주석을 포함해야 합니다. 엔터프라이즈 관리자와 같은 일부 역할은 전체 액세스 자격 증명을 가지며 잠글 수 없습니다. 역할 기반 액세스 제어 항목을 참조하십시오.

- 7 **게시**를 클릭합니다. 한 번에 여러 정책을 추가하고 함께 게시할 수 있습니다.
새 정책이 화면에 표시됩니다.
- 8 정책 섹션을 선택하고 **규칙 추가**를 클릭합니다.
- 9 규칙의 이름을 입력합니다.
- 10 **소스** 열에서 편집 아이콘을 클릭하고 규칙의 소스를 선택합니다. Active Directory 멤버가 포함된 그룹을 IDFW 규칙의 소스 필드로 사용할 수 있습니다. 자세한 내용은 **그룹 추가** 항목을 참조하십시오.

IPv4, IPv6 및 멀티캐스트 주소가 지원됩니다.

참고: IPv6 방화벽에는 연결된 세그먼트에서 IPv6용 IP 검색을 사용하도록 설정해야 합니다. 세부 정보는 **IP 검색 세그먼트 프로파일 이해**를 참조하십시오.

11 대상 열에서 편집 아이콘을 클릭하고 규칙의 대상을 선택합니다. 정의되지 않은 경우 대상은 **임의**와 일치합니다. 자세한 내용은 **그룹 추가** 항목을 참조하십시오. IPv4, IPv6 및 멀티캐스트 주소가 지원됩니다.

12 서비스 열에서 편집 아이콘을 클릭하고 서비스를 선택합니다. 정의되지 않은 경우 서비스는 **임의**와 일치합니다.

13 프로파일 열은 이더넷 범주에 규칙을 추가할 때 사용할 수 없습니다. 다른 모든 규칙 범주의 경우 **프로파일** 열에서 편집 아이콘을 클릭하고 컨텍스트 프로파일을 선택하거나 **새 컨텍스트 프로파일 추가**를 클릭합니다. **컨텍스트 프로파일 추가**의 내용을 참조하십시오.

컨텍스트 프로파일은 분산 방화벽 규칙 및 게이트웨이 방화벽 규칙에서 사용하기 위해 계층 7 APP ID 특성을 사용합니다. 서비스가 **임의**로 설정된 방화벽 규칙에서는 여러 애플리케이션 ID 컨텍스트 프로파일을 사용할 수 있습니다. ALG 프로파일(FTP 및 TFTP)의 경우, 규칙당 하나의 컨텍스트 프로파일이 지원됩니다.

14 적용을 클릭하여 규칙에 컨텍스트 프로파일을 적용합니다.

15 기본적으로 **적용 대상** 열은 DFW로 설정되고 규칙은 모든 워크로드에 적용됩니다. 선택한 그룹에 규칙 또는 정책을 적용할 수도 있습니다. **적용 대상**은 규칙별 적용 범위를 정의하며 주로 ESXi 및 KVM 호스트의 최적화 또는 리소스에 사용됩니다. 다른 테넌트 및 영역에 대해 정의된 다른 정책을 방해하지 않으면서 특정 영역 및 테넌트로 대상이 지정된 정책을 정의하는 데 도움이 됩니다.

IP 주소, MAC 주소 또는 Active Directory 그룹만 구성된 그룹은 **적용 대상** 텍스트 상자에서 사용할 수 없습니다.

16 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.

17 상태 전환 버튼을 클릭하여 규칙을 사용하거나 사용하지 않도록 설정합니다.

18 (선택 사항) 톱니 바퀴 아이콘을 클릭하여 다음 규칙 옵션을 구성합니다.

옵션	설명
로깅	로깅이 기본으로 꺼져 있습니다. 로그는 ESXi와 KVM 호스트의 /var/log/dfwpklogs.log 파일에 저장됩니다.
방향	대상 개체의 관점에서 트래픽 방향을 나타냅니다. [인]은 개체로 들어오는 트래픽만 확인하고, [아웃]은 개체에서 나가는 트래픽만 확인하며, [인/아웃]은 양쪽 방향 트래픽 모두를 확인합니다.
IP 프로토콜	IPv4, IPv6 또는 IPv4-IPv6 둘 모두를 기반으로 규칙을 적용합니다.
로그 레이블	로그 레이블은 로깅이 사용하도록 설정된 경우 방화벽 로그에서 수행됩니다.

19 게시를 클릭합니다. 한 번에 여러 규칙을 추가하고 함께 게시할 수 있습니다.

20 각 규칙에서 **정보** 아이콘을 클릭하여 규칙 ID 번호 및 적용되는 위치를 봅니다.

이 아이콘은 규칙을 게시할 때까지 회색으로 표시됩니다. 필터 아이콘을 클릭할 경우 규칙 ID를 지정하여 필터 조건을 충족하는 정책 및 규칙만 표시할 수도 있습니다.

21 추가 인식 상태 정보를 제공하기 위해 보안 정책 수준의 인식 상태 API가 개선되었습니다.

*intent_path*와 함께 쿼리 매개 변수 *include_enforced_status=true*를 지정하여 이러한 개선을 구현할 수 있습니다. 다음 API 호출을 작성합니다.

```
GET https://<nsx>/policy/api/v1/infra/realized-state/status?intent_path=/infra/domains/default/security-policies/<security-policy-id>&include_enforced_status=true
```

분산 방화벽 패킷 로그

로깅이 방화벽 규칙에 대해 사용되도록 설정된 경우 문제를 해결하기 위해 방화벽 패킷 로그를 살펴볼 수 있습니다.

로그 파일은 ESXi 호스트와 KVM 호스트에 대해 /var/log/dfwpklogs.log입니다.

다음은 분산 방화벽 규칙에 대한 일반 로그 샘플입니다.

```
2018-07-03T19:44:09.749Z b6507827 INET match PASS mainrs/1024 IN 52 TCP 192.168.4.3/49627->192.168.4.4/49153 SEW
2018-07-03T19:46:02.338Z 7396c504 INET match DROP mainrs/1024 OUT 52 TCP 192.168.4.3/49676->192.168.4.4/135 SEW
2018-07-06T18:15:49.647Z 028cd586 INET match DROP mainrs/1027 IN 36 PROTO 2 0.0.0.0->224.0.0.1
2018-07-06T18:19:54.764Z 028cd586 INET6 match DROP mainrs/1027 OUT 143 UDP fe80:0:0:0:68c2:8472:2364:9be/546->ff02:0:0:0:0:1:2/547
```

DFW 로그 파일 형식의 요소에는 공백으로 구분된 다음 항목이 포함됩니다.

- 타임 스탬프:
- 인터페이스의 VIF ID의 마지막 8자리 숫자

- INET 유형(v4 또는 v6)
- 이유(일치)
- 작업(PASS, DROP, REJECT)
- 규칙 집합 이름/규칙 ID
- 패킷 방향(IN/OUT)
- 패킷 크기
- 프로토콜(TCP, UDP 또는 PROTO #)
- netx 규칙 적용에 대한 SVM 방향
- 소스 IP 주소/소스 포트>대상 IP 주소/대상 포트
- TCP 플래그(SEW)

통과한 TCP 패킷의 경우 세션이 종료되면 종료 로그가 생성합니다.

```
2018-07-03T19:44:30.585Z 7396c504 INET TERM mainrs/1024 OUT TCP RST 192.168.4.3/49627-
>192.168.4.4/49153 20/16 1718/76308
```

TCP 종료 로그의 요소에는 공백으로 구분된 다음 항목이 포함됩니다.

- 타임 스탬프:
- 인터페이스 VIF ID의 마지막 8자리 숫자
- INET 유형(v4 또는 v6)
- 작업(TERM)
- 규칙 집합 이름/규칙 ID
- 패킷 방향(IN/OUT)
- 프로토콜(TCP, UDP 또는 PROTO #)
- TCP RST 플래그
- netx 규칙 적용에 대한 SVM 방향
- 소스 IP 주소/소스 포트>대상 IP 주소/대상 포트
- IN 패킷 수/OUT 패킷 수(모두 누적됨)
- IN 패킷 크기/OUT 패킷 크기

다음은 분산 방화벽 규칙에 대한 FQDN 로그 파일 예입니다.

```
2019-01-15T00:34:45.903Z 7c607b29 INET match PASS 1031 OUT 48 TCP 10.172.178.226/32808-
>23.72.199.234/80 S www.sway.com(034fe78d-5857-0680-81e4-d8da6b28d1b4)
```

FQDN 로그의 요소에는 공백으로 구분된 다음 항목이 포함됩니다.

- 타임 스탬프:
- 인터페이스의 VIF ID의 마지막 8자리 숫자
- INET 유형(v4 또는 v6)
- 이유(일치)
- 작업(PASS, DROP, REJECT)
- 규칙 집합 이름/규칙 ID
- 패킷 방향(IN/OUT)
- 패킷 크기
- 프로토콜(TCP, UDP 또는 PROTO #)
- 소스 IP 주소/소스 포트>대상 IP 주소/대상 포트
- 도메인 이름/UUID. 여기서 UUID는 도메인 이름의 바이너리 내부 표현입니다.

다음은 분산 방화벽 규칙에 대한 계층 7 로그 파일 샘플입니다.

```
2019-01-15T00:35:07.221Z 82f365ae INET match REJECT 1034 OUT 48 TCP 10.172.179.6/49818-
>23.214.173.202/80 S APP_HTTP

2019-01-15T00:34:46.486Z 7c607b29 INET match PASS 1030 OUT 48 UDP 10.172.178.226/42035-
>10.172.40.1/53 APP_DNS
```

계층 7 로그의 요소에는 공백으로 구분된 다음 항목이 포함됩니다.

- 타임 스탬프:
- 인터페이스의 VIF ID의 마지막 8자리 숫자
- INET 유형(v4 또는 v6)
- 이유(일치)
- 작업(PASS, DROP, REJECT)
- 규칙 집합 이름/규칙 ID
- 패킷 방향(IN/OUT)
- 패킷 크기
- 프로토콜(TCP, UDP 또는 PROTO #)
- 소스 IP 주소/소스 포트>대상 IP 주소/대상 포트
- APP_XXX는 검색된 애플리케이션입니다.

기본 연결 전략 선택

기본 연결 전략을 선택하여 보안 모델을 적용할 수 있습니다.

기본 연결 전략은 개별 규칙을 수정하는 대신 직접 생성한 다른 방화벽 규칙 위에 모두 허용(차단 목록) 또는 모두 거부(허용 목록) 방화벽 정책을 생성합니다. 기본 연결 전략을 설정하려면 **분산 방화벽**으로 이동하십시오. 페이지 맨 위에서 연결 상태를 클릭하여 다른 옵션을 선택합니다.

선택한 기본 연결 전략을 변경하려면 방화벽 정책 및 규칙이 이미 생성되어 있어야 하며 즉시 적용해야 합니다. 정책이나 규칙이 생성되지 않은 경우에는 정책 및 규칙이 생성될 때까지 기본 연결 전략이 유지됩니다.

다음 옵션을 사용할 수 있습니다.

- **차단 목록(로깅 포함 또는 불포함):** 기본 옵션이며 DFW에 대해 모두 허용 규칙을 생성합니다.
- **화이트리스트(로깅 포함 또는 불포함):** 모든 트래픽 거부 방화벽 규칙을 생성합니다. 방화벽 규칙에 정의된 사이트 또는 애플리케이션의 통신만 허용되며 DHCP 트래픽을 포함하는 다른 모든 통신은 액세스가 거부됩니다.
- **없음:** 방화벽 규칙의 차단 목록 또는 허용 목록 작성을 둘 다 사용하지 않도록 설정하려면 이 옵션을 선택합니다. 이전 버전의 NSX-T Data Center를 사용하여 이미 구성된 규칙 집합이 있는 경우 유용합니다.

방화벽 제외 목록 관리

방화벽 제외 목록은 그룹 멤버 자격을 기준으로 방화벽 규칙에서 제외할 수 있는 그룹으로 구성되어 있습니다.

그룹을 방화벽 규칙에서 제외할 수 있으며, 목록에는 최대 100개의 그룹이 있습니다. IP 집합, MAC 집합 및 AD 그룹은 방화벽 제외 목록에 사용되는 그룹에 멤버로 포함될 수 없습니다.

참고 NSX-T Data Center는 NSX Manager 및 NSX Edge 노드 가상 시스템을 방화벽 제외 목록에 자동으로 추가합니다.

절차

- 1 **보안 > 분산 방화벽 > 작업 > 제외 목록**으로 이동합니다.
사용 가능한 그룹을 나열하는 창이 표시됩니다.
- 2 그룹을 제외 목록에 추가하려면 그룹 옆에 있는 확인란을 클릭합니다. 그런 후 **적용**을 클릭합니다.
- 3 그룹을 생성하려면 **그룹 추가**를 클릭합니다. **그룹 추가** 항목을 참조하십시오.
- 4 그룹을 편집하려면 그룹 옆에 있는 3개 점 메뉴를 클릭하고 **편집**을 선택합니다.
- 5 그룹을 삭제하려면 3개 메뉴를 클릭하고 **삭제**를 선택합니다.
- 6 그룹 세부 정보를 표시하려면 **모두 확장**을 클릭합니다.

특정 도메인 필터링(FQDN/URL)

FQDN/URL(예: "*.office365.com")로 식별된 특정 도메인을 필터링하도록 분산 방화벽 규칙을 설정합니다.

현재 미리 정의된 도메인 목록이 지원됩니다. 특성 유형 "도메인(FQDN) 이름"의 새 컨텍스트 프로파일을 추가할 때 FQDN 목록을 볼 수 있습니다. API 호출 `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME`을 실행하여 FQDN 목록을 볼 수도 있습니다.

DNS 규칙을 먼저 설정한 다음, 아래에 FQDN 허용 목록 또는 거부 목록 규칙을 설정해야 합니다. NSX-T Data Center는 DNS 응답(DNS 서버에서 가상 시스템으로 전송)의 TTL(Time to Live)을 사용하여 VM(가상 시스템)에 대한 DNS-IP 매핑 캐시 항목을 유지합니다. DNS 보안 프로파일을 사용하여 DNS TTL을 재정의하려면 [DNS 보안 구성](#)을 참조하십시오. FQDN 필터링을 적용하려면 가상 시스템이 도메인 확인을 위해 DNS 서버를 사용해야 하고(고정 DNS 항목 없음) DNS 응답에서 수신된 TTL도 준수해야 합니다. NSX-T Data Center가 DNS 스누핑을 사용하여 IP 주소와 FQDN 간의 매핑을 확보합니다. 모든 논리적 포트의 스위치에서 SpoofGuard를 사용하도록 설정하여 DNS 스누핑 공격의 위협으로부터 보호해야 합니다. DNS 스누핑 공격은 악의적인 VM이 스누핑된 DNS 응답을 삽입하여 악의적인 끝점으로 트래픽을 리디렉션하거나 방화벽을 우회하도록 하는 경우입니다. SpoofGuard에 대한 자세한 내용은 [SpoofGuard 세그먼트 프로파일 이해](#)를 참조하십시오.

이 기능은 계층 7에서 작동하며 ICMP를 포함하지 않습니다. 사용자가 example.com의 모든 서비스에 대해 거부 목록 규칙을 생성할 경우 ping example.com이 응답하지만 curl example.com은 응답하지 않으면 해당 기능이 예상대로 작동하는 것입니다.

하위 도메인을 포함하기 때문에 와일드카드 FQDN을 선택하는 것이 가장 좋습니다. 예를 들어 *example.com을 선택하면 americas.example.com 및 emea.example.com과 같은 하위 도메인이 포함됩니다. example.com을 사용하는 경우 하위 도메인이 포함되지 않습니다.

FQDN 기반 규칙은 ESXi 호스트에 대한 vMotion 동안 유지됩니다.

참고 ESXi 및 KVM 호스트가 지원됩니다. KVM 호스트는 FQDN 허용 목록만 지원됩니다. FQDN 필터링은 TCP 및 UDP 트래픽에만 사용할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **보안 > 분산 방화벽**으로 이동합니다.
- 3 **분산 방화벽 추가**의 단계를 수행하여 방화벽 정책 섹션을 추가합니다. 기존 방화벽 정책 섹션을 사용할 수도 있습니다.
- 4 신규 또는 기존 방화벽 정책 섹션을 선택하고 **규칙 추가**를 클릭하여 DNS 방화벽 규칙을 먼저 생성합니다.

5 방화벽 규칙의 이름(예: **DNS 규칙**)을 입력한 다음, 세부 정보를 제공합니다.

옵션	설명
서비스	편집 아이콘을 클릭하고 환경에 맞게 DNS 또는 DNS-UDP 서비스를 선택합니다.
프로파일	편집 아이콘을 클릭하고 DNS 컨텍스트 프로파일을 선택합니다. 이것은 미리 생성되어 있으며 기본적으로 배포에 사용할 수 있습니다.
적용 대상	필요에 따라 그룹을 선택합니다.
작업	허용을 선택합니다.

6 **규칙 추가**를 다시 클릭하고 FQDN 허용 목록 또는 거부 목록 규칙을 설정합니다.

7 규칙의 이름을 적절하게 지정합니다(예: **FQDN/URL 허용 목록**). 규칙을 이 정책 섹션의 DNS 규칙 아래에 끌어다 놓습니다.

8 다음 세부 정보를 제공합니다.

옵션	설명
서비스	편집 아이콘을 클릭하고 이 규칙과 연결할 서비스(예: HTTP)를 선택합니다.
프로파일	편집 아이콘을 클릭하고 새 컨텍스트 프로파일 추가 를 클릭합니다. 특성 열을 클릭하고 도메인(FQDN) 이름 을 선택합니다. 미리 정의된 목록에서 특성 이름/값 목록을 선택합니다. 추가 를 클릭합니다. 자세한 내용은 컨텍스트 프로파일 추가 항목을 참조하십시오.
적용 대상	필요에 따라 DFW 또는 그룹을 선택합니다.
작업	허용, 삭제 또는 거부 를 선택합니다.

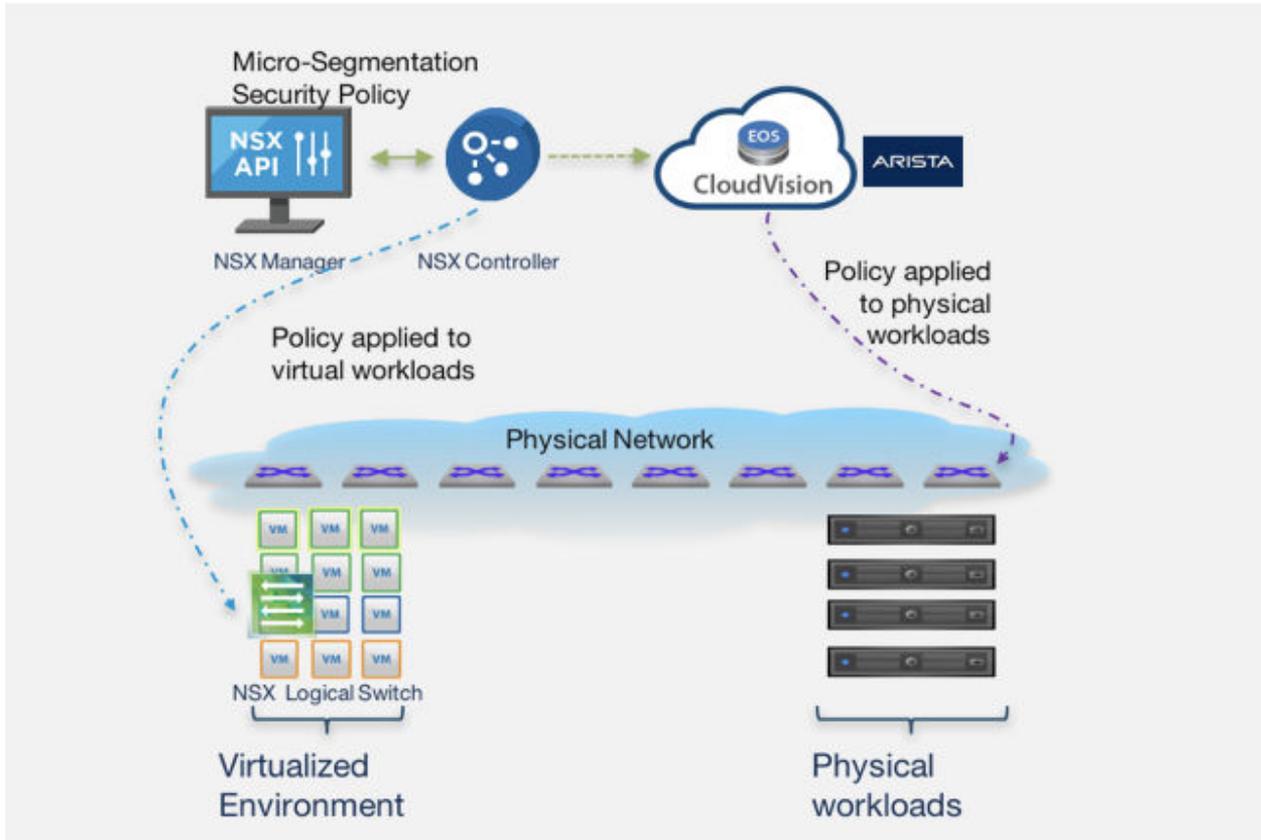
9 **계시**를 클릭합니다.

물리적 워크로드에 대한 보안 정책 확장

NSX-T Data Center는 가상 및 물리적 워크로드 모두에 대해 단일 관리 지점으로 작동할 수 있습니다.

NSX-T Data Center 2.5.1부터는 Arista CVX(CloudVision eXchange)와의 통합이 지원됩니다. 이 통합은 애플리케이션 프레임워크 또는 물리적 네트워크 인프라와 관계없이 가상 및 물리적 워크로드 간에 일관된 네트워킹 및 보안 서비스를 용이하게 합니다. NSX-T Data Center는 물리적 네트워크 스위치 또는 라우터를 직접 프로그래밍하지 않고 물리적 SDN 컨트롤러 수준에서 통합되므로 보안 관리자 및 물리적 네트워크 관리자의 자율성을 유지합니다.

NSX-T Data Center 2.5.1부터는 Arista EOS 4.22.1FX-PCS 이상과 통합될 수 있습니다.



제한 사항

- Arista 스위치에 연결된 최종 호스트에 방화벽 규칙을 적용하기 전에 ARP 트래픽이 있어야 이 스위치를 사용할 수 있습니다. 따라서 패킷은 방화벽 규칙이 트래픽을 차단하도록 구성되기 전에 스위치를 통과할 수 있습니다.
- 스위치가 충돌하거나 다시 로드될 경우 허용된 트래픽이 재개되지 않습니다. 스위치가 표시된 후 스위치에 방화벽 규칙이 적용되도록 ARP 표를 다시 채워야 합니다.
- Arista 물리적 스위치에 연결된 FTP 서버에 연결되어 있는 FTP 수동 클라이언트의 경우에는 Arista 물리적 스위치에 방화벽 규칙을 적용할 수 없습니다.
- CVX 클러스터에 대해 가상 IP를 사용하는 CVX HA 설정에서 CVX VM의 dvpg 무차별 모드 및 위조 전송을 [수락]으로 설정해야 합니다. 기본값(거부)으로 설정된 경우에는 NSX Manager에서 CVX HA 가상 IP에 연결할 수 없습니다.

NSX-T Manager와 상호 작용하도록 Arista CVX 구성

NSX-T Data Center를 구성한 후 Arista CVX(CloudVision eXchange)에 대한 구성 절차를 완료하여 CVX가 NSX-T Data Center와 상호 작용하도록 설정합니다.

사전 요구 사항

NSX-T Data Center에서는 CVX를 적용 지점으로 등록했습니다.

절차

- 1 NSX Manager에 루트 사용자로 로그인하고 다음 명령을 실행하여 CVX에서 NSX Manager와 통신하는 데 필요한 지문을 생성합니다.

```
openssl s_client -connect <IP address of nsx-manager>:443 | openssl x509 -pubkey -noout |
openssl rsa -pubin -outform der | openssl dgst -sha256 -binary | openssl base64
```

샘플 출력:

```
depth=0 C = US, ST = CA, L = Palo Alto, O = VMware Inc., OU = NSX, CN = nsx-mgr
verify error:num=18:self signed certificate
verify return:1
depth=0 C = US, ST = CA, L = Palo Alto, O = VMware Inc., OU = NSX, CN = nsx-mgr
verify return:1
writing RSA key
S+zwADluzeNf+dnffDpYvgs4YrS6QBgyeDry40bPgms=
```

- 2 CVX CLI에서 다음 명령을 실행합니다.

```
cvx
no shutdown
service pcs
no shutdown
controller <IP address of nsx-manager>
username <NSX administrator user name>
password <NSX administrator password>
enforcement-point cvx-default-ep
pinned-public-key <thumbprint for CVX to communicate with NSX
                    Manager>
notification-id <notification ID created while registering CVX with NSX>
end
```

- 3 CVX CLI에서 다음 명령을 실행하여 구성을 확인합니다.

```
show running-config
```

샘플 출력:

```
cvx
    no shutdown
    source-interface Management1
    !
    service hsc
        no shutdown
    !
    service pcs
        no shutdown
        controller 192.168.2.80
        username admin
```

```
password 7 046D26110E33491F482F2800131909556B
enforcement-point cvx-default-ep
pinned-public-key sha256//S+zwADluzeNf+dnffDpYvgs4YrS6QBgyeDry40bPgms=
notification-id a0286cb6-de4d-41de-99a0-294465345b80
```

- 4 물리적 서버에 연결하는 물리적 스위치의 이더넷 인터페이스에서 태그를 구성합니다. CVX에서 관리하는 물리적 스위치에서 다음 명령을 실행합니다.

```
configure terminal
interface ethernet 4
tag phy_app_server
end
copy running-config startup-config
Copy completed successfully.
```

- 5 다음 명령을 실행하여 스위치에 대한 태그 구성을 확인합니다.

```
show running-config section tag
```

샘플 출력:

```
interface Ethernet4
description connected-to-7150s-3
switchport trunk allowed vlan 1-4093
switchport mode trunk
tag sx4_app_server
```

ARP를 사용하여 태그가 지정된 인터페이스에서 확인된 IP 주소는 NSX-T Data Center와 공유됩니다.

- 6 NSX Manager에 로그인하여 CVX에서 관리하는 물리적 워크로드의 방화벽 규칙을 생성하고 게시합니다. 규칙 생성에 대한 자세한 내용은 [장 10 보안 항목](#)을 참조하십시오. 예:

이름	소스	대상	서비스	프로파일	적용 대상	작업
Firewall_Services (2)	적용 대상	DFW				실행 중
vm_to_phy_server	vm	phy_server	임의	없음	DFW	허용
phy_server_to_vm	phy_server	vm	임의	없음	DFW	허용

NSX-T Data Center에 게시된 NSX-T Data Center 정책 및 규칙은 CVX에서 관리하는 물리적 스위치에 동적 ACL로 나타납니다.

```
prmh-nsx-tor-7050sx-4#show ip access-lists dynamic
IP Access List et4.v4.in [dynamic]
 10 permit ip host 71.1.1.3 host 27.1.1.11
IP Access List et4.v4.out [dynamic]
 10 permit ip host 27.1.1.11 host 71.1.1.3
```

자세한 내용은 [CVX HA 설정](#), [CVX HA 가상 IP 설정](#) 및 [물리적 스위치 Mlag 설정](#)을 참조하십시오.

Arista CVX와 상호 작용하도록 NSX-T Data Center 구성

NSX-T Data Center에 대한 구성 절차를 완료하여 NSX-T Data Center에 적용 지점으로 CVX를 추가하고 NSX-T Data Center가 CVX와 상호 작용할 수 있도록 합니다.

사전 요구 사항

Arista CVX 클러스터의 가상 IP 주소를 가져옵니다.

절차

- 1 NSX Manager에 루트 사용자로 로그인하고 다음 명령을 실행하여 CVX용 지문을 검색합니다.

```
openssl s_client -connect <virtual IP address of CVX cluster> | openssl x509 -noout
-fingerprint -sha256
```

샘플 출력:

```
depth=0 CN = self.signed
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = self.signed
verify return:1
SHA256
Fingerprint=35:C1:42:BC:7A:2A:57:46:E8:72:F4:C8:B8:31:E3:13:5F:41:95:EF:D8:1E:E9:3D:F0:CC:3
B:09:A2:FE:22:DE
```

- 2 검색된 지문을 편집하여 소문자만 사용하고 지문에서 모든 콜론을 제외합니다.

CVX용으로 편집된 지문 샘플:

```
35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de
```

- 3 `PATCH /policy/api/v1/infra/sites/default/enforcement-points` API를 호출하고 CVX 지문을 사용하여 CVX의 적용 끝점을 생성합니다. 예:

```
PATCH https://<nsx-manager>/policy/api/v1/infra/sites/default/enforcement-points/cvx-
default-ep
{
  "auto_enforce": "false",
  "connection_info": {
    "enforcement_point_address": "<IP address of CVX>",
    "resource_type": "CvxConnectionInfo",
    "username": "cvpadmin",
    "password": "1q2w3e4rT",
    "thumbprint": "65a9785e88b784f54269e908175ada662be55f156a2dc5f3a1b0c339cea5e343"
  }
}
```

- 4 GET /policy/api/v1/infra/sites/default/enforcement-points API를 호출하여 끝점 정보를 검색합니다. 예:

```
https://<nsx-manager>/policy/api/v1/infra/sites/default/enforcement-points/cvx-default-ep
{
  "auto_enforce": "false",
  "connection_info": {
    "enforcement_point_address": "<IP address of CVX>",
    "resource_type": "CvxConnectionInfo",
    "username": "admin",
    "password": "1q2w3e4rT",
    "thumbprint": "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de"
  }
}
```

샘플 출력:

```
{
  "connection_info": {
    "thumbprint": "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
    "enforcement_point_address": "192.168.2.198",
    "resource_type": "CvxConnectionInfo"
  },
  "auto_enforce": false,
  "resource_type": "EnforcementPoint",
  "id": "cvx-default-ep",
  "display_name": "cvx-default-ep",
  "path": "/infra/sites/default/enforcement-points/cvx-default-ep",
  "relative_path": "cvx-default-ep",
  "parent_path": "/infra/sites/default",
  "marked_for_delete": false,
  "_system_owned": false,
  "_create_user": "admin",
  "_create_time": 1564036461953,
  "_last_modified_user": "admin",
  "_last_modified_time": 1564036461953,
  "_protection": "NOT_PROTECTED",
  "_revision": 0
}
```

- 5 POST /api/v1/notification-watchers/ API를 호출하고 CVX 지문을 사용하여 알림 ID를 생성합니다. 예:

```
POST https://<nsx-manager>/api/v1/notification-watchers/
{
  "server": "<virtual IP address of CVX cluster>",
  "method": "POST",
  "uri": "/pcs/v1/nsgroup/notification",
  "use_https": true,
  "certificate_sha256_thumbprint":
  "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
  "authentication_scheme": {
    "scheme_name": "BASIC_AUTH",
```

```
"username": "cvpadmin",
"password": "1q2w3e4rT"
}
}
```

- 6 GET /api/v1/notification-watchers/를 호출하여 알림 ID를 검색합니다.

샘플 출력:

```
{
  "id": "a0286cb6-de4d-41de-99a0-294465345b80",
  "server": "192.168.2.198",
  "port": 443,
  "use_https": true,
  "certificate_sha256_thumbprint":
  "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
  "method": "POST",
  "uri": "/pcs/v1/nsgroup/notification",
  "authentication_scheme": {
    "scheme_name": "BASIC_AUTH",
    "username": "cvpadmin"
  },
  "send_timeout": 30,
  "max_send_uri_count": 5000,
  "resource_type": "NotificationWatcher",
  "display_name": "a0286cb6-de4d-41de-99a0-294465345b80",
  "_create_user": "admin",
  "_create_time": 1564038044780,
  "_last_modified_user": "admin",
  "_last_modified_time": 1564038044780,
  "_system_owned": false,
  "_protection": "NOT_PROTECTED",
  "_revision": 0
}
```

- 7 PATCH /policy/api/v1/infra/domains/default/domain-deployment-maps/cvx-default-dmap API를 호출하여 CVX 도메인 배포 맵을 생성합니다. 예:

```
PATCH https://<nsx-manager>/policy/api/v1/infra/domains/default/domain-deployment-maps/cvx-
default-dmap
{
  "display_name": "cvx-deployment-map",
  "id": "cvx-default-dmap",
  "enforcement_point_path": "/infra/sites/default/enforcement-points/cvx-default-ep"
}
```

- 8 GET /policy/api/v1/infra/domains/default/domain-deployment-maps API를 호출하여 배포 맵 정보를 검색합니다.

공유 주소 집합

동적 또는 논리적 개체를 기준으로 하는 보안 그룹을 생성하고 분산 방화벽 규칙의 **적용 대상** 텍스트 상자에서 사용할 수 있습니다.

주소 집합은 가상 시스템 이름 또는 태그를 기준으로 동적으로 채워지며, 각 필터에서 업데이트되어야 하므로 DFW 규칙 및 IP 주소 집합을 저장하느라 호스트에서 사용 가능한 힙 메모리 양이 고갈될 수 있습니다.

NSX-T Data Center 버전 2.5 이상에서는 글로벌 또는 공유 주소 집합이라는 기능을 통해 모든 필터에서 주소 집합을 공유합니다. 각 필터에는 **적용 대상**에 따라 서로 다른 규칙이 있을 수 있지만 주소 집합 멤버는 모든 필터에서 일정합니다. 이 기능은 기본적으로 사용하도록 설정되어 있으므로 힙 메모리 사용을 줄일 수 있습니다. 사용하지 않도록 설정할 수 없습니다.

NSX-T Data Center 버전 2.4 및 이전 버전에서는 글로벌 또는 공유 주소 집합이 사용되지 않도록 설정되고 분산 방화벽 규칙이 과도한 환경에서 VSIP 힙이 고갈될 수 있습니다.

East-West 네트워크 보안 - 타사 서비스 연결

파트너가 NSX-T Data Center에 IDS(침입 감지 시스템) 또는 IPS(침입 방지 시스템)와 같은 네트워크 서비스를 등록한 후 관리자는 온-프레미스 데이터 센터의 VM 사이에 이동하는 East-West 트래픽을 검사하기 위한 네트워크 서비스를 구성할 수 있습니다.

사전 요구 사항

- 파트너는 NSX-T Data Center에 서비스를 등록해야 합니다.
- ESXi 호스트는 전송 노드 프로파일을 사용하여 NSX-T Data Center 전송 노드로 준비해야 합니다.

참고

- 서비스 VM은 ESXi 호스트에서만 지원되고 KVM 호스트에서는 지원되지 않습니다.
- NSX-T Data Center는 ESXi 호스트에서 실행되는 게스트 VM만 보호합니다.
- NSX-T Data Center는 KVM 호스트에서 실행되는 게스트 VM을 보호하지 않습니다.

네트워크 보호 East-West의 핵심 개념

온-프레미스 데이터 센터의 게스트 VM 간에 흐르는 트래픽은 파트너가 제공하는 타사 서비스에 의해 보호됩니다. 다음은 해당 워크플로를 이해하는 데 도움이 되는 몇 가지 개념입니다.

- 서비스: 파트너가 NSX-T Data Center에 서비스를 등록합니다. 서비스는 파트너가 제공하는 보안 기능, 서비스 VM의 OVF URL과 같은 서비스 배포 세부 정보, 서비스를 연결할 점, 서비스의 상태를 나타냅니다.
- 벤더 템플릿: 서비스가 네트워크 트래픽에서 수행할 수 있는 기능으로 구성됩니다. 파트너가 벤더 템플릿을 정의합니다. 예를 들어 벤더 템플릿은 IPSec 서비스를 사용한 터널링과 같은 네트워크 작업 서비스를 제공할 수 있습니다.

- 서비스 프로파일: 벤더 템플릿의 인스턴스입니다. NSX-T Data Center 관리자는 서비스 VM에서 사용할 서비스 프로파일을 생성할 수 있습니다.
- 게스트 VM: 네트워크의 트래픽의 소스 또는 대상입니다. 수신 또는 송신 트래픽은 East-West 네트워크 서비스를 실행하는 규칙에 대해 정의된 서비스 체인에서 검사됩니다.
- 서비스 VM: 서비스에서 지정된 OVA 또는 OVF 장치를 실행하는 VM입니다. 리디렉션된 트래픽을 수신하기 위해 서비스부를 통해 연결됩니다.
- 서비스 인스턴스: 서비스가 호스트에 배포될 때 생성됩니다. 각 서비스 인스턴스에는 해당하는 서비스 VM이 있습니다.
- 서비스 세그먼트: 전송 영역과 연결된 서비스부의 세그먼트입니다. 각 서비스 연결은 기타 서비스 연결과 분리되고 NSX-T가 제공한 일반 L2 또는 L3 네트워크 세그먼트와 분리됩니다. 서비스부는 서비스 연결을 관리합니다.
- Service Manager: 서비스 집합을 가리키는 파트너 Service Manager입니다.
- 서비스 체인: 관리자가 정의한 서비스 프로파일의 논리적 순서입니다. 서비스 프로파일은 서비스 체인에 정의된 순서대로 네트워크 트래픽을 검사합니다. 예를 들어 첫 번째 서비스 프로파일은 방화벽이고, 두 번째 서비스 프로파일은 모니터 등입니다. 서비스 체인은 다른 방향의 트래픽(송신/수신)에 대해 다른 순서의 서비스 프로파일을 지정할 수 있습니다.
- 리디렉션 정책: 특정 서비스 체인에 대해 분류된 트래픽이 해당 서비스 체인으로 리디렉션되도록 합니다. NSX-T Data Center 보안 그룹 및 서비스 체인과 일치하는 트래픽 패턴을 기반으로 합니다. 패턴과 일치하는 모든 트래픽이 서비스 체인을 따라 리디렉션됩니다.
- 서비스 경로: 서비스 체인의 서비스 프로파일을 구현하는 서비스 VM의 순서입니다. 관리자는 사전 정의된 순서의 서비스 프로파일로 구성된 서비스 체인을 정의합니다. NSX-T Data Center는 게스트 VM 및 서비스 VM의 수 및 위치를 기반으로 서비스 체인에서 여러 서비스 경로를 생성합니다. 검사할 트래픽 흐름에 대한 최적의 서비스 경로를 선택합니다. 각 서비스 경로는 SPI(서비스 경로 인덱스)에서 식별되고 경로에 따른 각 홉에는 고유한 SI(서비스 인덱스)가 있습니다.

East-West 트래픽에 대한 NSX-T Data Center 요구 사항

NSX-T Data Center 배포에서는 오버레이 전송 영역 및 오버레이 지원 논리적 스위치가 있는지 확인해야 합니다.

동-서 서비스 삽입은 전체 NSX-T 배포에 적용됩니다. 클러스터 수준 또는 호스트 수준에서 서비스를 배포할 수 없습니다.

서비스가 GENEVE 또는 오버레이 지원 논리적 스위치에서 트래픽을 전송하기 때문에 모든 전송 노드가 오버레이 유형이어야 합니다. 오버레이 지원(GENEVE 지원) 논리적 스위치는 내부적으로 프로비저닝되며 사용자 인터페이스에 표시되지 않습니다.

VLAN 지원 논리적 스위치만 사용하여 배포를 계획하는 경우에도 East-West 트래픽은 오버레이 전송 영역 및 오버레이 지원 논리적 스위치를 통과합니다. 따라서 오버레이 전송 영역 및 GENEVE 지원 논리적 스위치를 생성해야 합니다. 이러한 요구 사항이 없으면 vMotion 동안 호스트의 게스트VM을 다른 전송 노드로 마이그레이션할 수 없습니다. 게스트VM은 연결 끊김 상태로 전환되고 동-서 서비스에서 구성 오류를 발생시킵니다.

East-West 네트워크 보안에 대한 상위 수준 작업

East-West 트래픽에 대한 네트워크 보안을 설정하려면 다음 단계를 따르십시오.

표 10-3. East-West 네트워크 검사를 구성하기 위한 작업 목록

워크플로 작업	개인 설정	구현
서비스 등록	파트너	API만
벤더 템플릿 등록	파트너	API만
Service Manager 등록	파트너	API만
East-West 트래픽 검사를 위한 서비스 배포	관리자	API 및 NSX Manager UI
서비스 프로파일 추가	관리자	API 및 NSX Manager UI
서비스 체인 추가	관리자	API 및 NSX Manager UI
East-West 트래픽에 대한 리디렉션 규칙 추가	관리자	API 및 NSX Manager UI

East-West 트래픽 검사를 위한 서비스 배포

파트너가 서비스를 등록한 후 관리자는 클러스터의 멤버 호스트에 서비스의 인스턴스를 배포해야 합니다. 클러스터의 모든 NSX-T Data Center 호스트에서 파트너 보안 엔진을 실행하는 파트너 서비스 VM을 배포합니다. SVM을 배포한 후 게스트 VM을 보호하기 위해 SVM에 사용되는 정책 규칙을 생성할 수 있습니다.

사전 요구 사항

- 모든 호스트가 vCenter Server에서 관리됩니다.
- 파트너 서비스가 NSX-T Data Center에 등록되고 배포할 수 있는 상태가 됩니다.
- NSX-T Data Center 관리자가 파트너 서비스 및 벤더 템플릿에 액세스할 수 있습니다.
- 서비스 VM과 파트너 Service Manager(콘솔)가 관리 네트워크 수준에서 서로 통신할 수 있어야 합니다.
- 호스트 기반 서비스 배포: 각 호스트에 서비스 VM을 배포하기 전에 전송 노드 프로파일을 적용하여 NSX-T Data Center로 클러스터의 각 호스트를 구성합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 서비스 배포 > 배포 > 서비스 배포**를 선택합니다.
- 3 [파트너 서비스] 필드에서 파트너 서비스를 선택합니다.
- 4 서비스 배포 이름을 입력합니다.
- 5 [계산 관리자] 필드에서 서비스를 배포하기 위한 vCenter Server를 선택합니다.
- 6 [클러스터] 필드에서 서비스를 배포해야 하는 클러스터를 선택합니다.
- 7 [데이터스토어] 드롭다운 메뉴에서 서비스 가상 시스템에 대한 저장소로 사용할 데이터스토어를 선택합니다.
- 8 [네트워크] 열에서 **설정**을 클릭하고 DHCP 또는 정적 IP 주소 유형 및 데이터 네트워크를 선택하여 관리 네트워크 인터페이스를 입력합니다.
- 9 [서비스 세그먼트] 필드에서 목록에서 서비스 세그먼트를 선택하거나 작업 아이콘을 클릭하여 서비스 세그먼트를 추가하거나 편집합니다. 서비스 세그먼트에 연결된 게스트 VM은 East-West 네트워크 트래픽 보호를 제공합니다.
- 10 [배포 유형] 필드에서 다음 배포 옵션 중 하나를 선택합니다. 파트너가 등록한 서비스에 따라, 여러 서비스를 단일 서비스 VM의 일부로 배포할 수 있습니다.
 - 클러스터링됨: 호스트 서비스 VM에 전용으로 설정된 클러스터에 속하는 호스트에 서비스를 배포합니다.
 - 호스트 기반: 클러스터 내의 모든 호스트에 서비스를 배포합니다.
- 11 [배포 템플릿] 필드에서 게스트 VM 그룹에서 실행할 워크로드를 보호하기 위한 특성을 제공하는 템플릿을 선택합니다.
- 12 (클러스터 기반 배포만 해당) [클러스터링된 배포 수]에서 클러스터에 배포할 서비스 VM의 수를 입력합니다. vCenter Server는 서비스 VM을 배포할 호스트를 결정합니다.
- 13 **저장**을 클릭합니다.

결과

서비스를 배포한 후 파트너 Service Manager에게 업데이트에 대한 알림이 전송됩니다.

다음에 수행할 작업

호스트에 배포된 서비스 인스턴스에 대한 상태 및 배포 세부 정보를 확인합니다. 서비스 프로파일 추가 항목을 참조하십시오.

서비스 프로파일 추가

서비스 프로파일은 파트너 벤더 템플릿의 인스턴스입니다. 관리자는 벤더 템플릿의 특성을 사용자 지정하여 템플릿의 인스턴스를 생성할 수 있습니다.

참고 단일 벤더에 대해 여러 개의 서비스 프로파일을 생성할 수 있습니다. 예를 들어, 전달 경로에 대해 설정한 서비스 프로파일은 IDS 보호를 제공하지만 역방향 경로에 대해 설정한 서비스 프로파일은 IPS 보호를 지원합니다. 그러나 정방향 및 역방향 경로 모두에 대해 단일 서비스 프로파일을 설정할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **보안 > East West 보안 > 네트워크 검사 > 서비스 프로파일**로 이동합니다.
- 3 [파트너 서비스] 드롭다운 필드에서 서비스를 선택합니다. 선택한 서비스에 대한 서비스 프로파일을 생성할 수 있습니다.
- 4 서비스 프로파일 이름을 입력하고 벤더 템플릿을 선택합니다.
- 5 [리디렉션 작업] 필드는 벤더 템플릿의 기능을 상속합니다. 예를 들어, 복사가 벤더 템플릿에서 제공하는 기능이면 기본적으로 서비스 프로파일을 생성할 때의 리디렉션 작업은 복사입니다.
- 6 (옵션) 태그를 정의하여 서비스 프로파일을 필터링하고 관리합니다.
- 7 **저장**을 클릭합니다.

결과

파트너 서비스에 대한 새 서비스 프로파일이 생성됩니다.

다음에 수행할 작업

서비스 체인을 추가합니다. [서비스 체인 추가](#)의 내용을 참조하십시오.

서비스 체인 추가

서비스 체인은 네트워크 관리자가 정의한 서비스 프로파일의 논리적 순서입니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **보안 > East West 보안 > 네트워크 검사 > 서비스 체인 > 체인 추가**를 선택합니다.
- 3 서비스 체인 이름을 입력합니다.

- 4 [서비스 세그먼트] 필드에서 서비스 체인을 적용할 서비스 세그먼트를 선택합니다. 서비스 세그먼트는 오버레이 전송 영역의 여러 서비스 VM을 연결하는 서비스부의 세그먼트입니다. 서비스 체인의 각 서비스 VM은 NSX-T Data Center에서 실행하는 다른 서비스 VM 및 L2/L3 네트워크 세그먼트와 별도입니다. 서비스부는 서비스 VM에 대한 액세스를 제어합니다.
- 5 전달 경로를 설정하려면 **전달 경로 설정** 필드를 클릭하고 **프로파일을 순서대로 추가**를 클릭합니다.
- 6 서비스 체인의 첫 번째 프로파일을 추가하고 **추가**를 클릭합니다.
- 7 다음 서비스 프로파일을 지정하려면 **프로파일을 순서대로 추가**를 클릭하고 세부 정보를 입력합니다. 위로 및 아래로 화살표 아이콘을 사용하여 프로파일 순서를 재정렬할 수도 있습니다.
- 8 **저장**을 클릭하여 서비스 체인에 대한 전달 경로 추가를 완료합니다.
- 9 서비스부에서 정방향 경로에 대해 설정한 서비스 프로파일을 사용하도록 하려면 [역방향 경로] 열에서 **역방향 전달 경로**를 선택합니다.
- 10 역방향 경로에 대해 새 서비스 프로파일을 설정하려면 **역방향 경로 설정**을 클릭하고 서비스 프로파일을 추가합니다.
- 11 **저장**을 클릭하여 서비스 체인에 대한 역방향 경로 추가를 완료합니다.
- 12 [실패 정책] 필드에서
 - **허용**을 선택하면 서비스 VM이 실패할 때 트래픽을 대상 VM으로 전송합니다. 서비스 VM 실패는 파트너에 의해서만 사용되도록 설정될 수 있는 작동 여부 감지 메커니즘을 통해 감지됩니다.
 - **차단**을 선택하면 서비스 VM이 실패할 때 트래픽을 대상 VM으로 전송하지 않습니다.
- 13 **저장**을 클릭합니다.

결과

서비스 체인을 추가한 후 파트너 Service Manager에게 업데이트에 대한 알림이 전송됩니다.

다음에 수행할 작업

East-West 네트워크 트래픽을 검사하기 위한 리디렉션 규칙을 생성합니다. [East-West 트래픽에 대한 리디렉션 규칙 추가](#)의 내용을 참조하십시오.

East-West 트래픽에 대한 리디렉션 규칙 추가

네트워크 검사를 위한 East-West 트래픽을 리디렉션하는 규칙을 추가합니다.

규칙은 정책에 정의됩니다. 개념으로서의 정책은 방화벽의 섹션 개념과 유사합니다. 정책을 추가할 때 서비스 체인의 서비스 프로파일을 기준으로 검사하기 위해 트래픽을 리디렉션할 서비스 체인을 선택합니다.

규칙 정의는 트래픽의 소스 및 대상, 검사 서비스, 규칙을 적용할 NSX-T Data Center 개체 및 트래픽 리디렉션 정책으로 구성됩니다. 규칙을 게시한 후 NSX Manager는 일치하는 트래픽 패턴을 찾으면 규칙을 트리거합니다. 규칙은 트래픽을 검사하기 시작합니다. 예를 들어 NSX Manager는 검사해야 하는 트래픽 흐름을 분류할 때 일반 분산 방화벽으로 전달하는 대신 정책의 지정된 서비스 체인에 따라 해당 트래픽을 리

디렉션합니다. 서비스 체인에 정의된 서비스 프로파일은 파트너가 제공하는 네트워크 서비스에 대한 트래픽을 검사합니다. 서비스 프로파일이 트래픽의 보안 문제를 감지하지 않고 검사를 완료하는 경우 트래픽은 서비스 체인의 다음 서비스 프로파일로 전달됩니다. 서비스 체인의 마지막에 트래픽이 대상으로 전달됩니다.

모든 알림은 파트너 Service Manager 및 NSX-T Data Center로 전송됩니다.

사전 요구 사항

네트워크 검사를 위한 트래픽을 리디렉션하는 데 서비스 체인을 사용할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nvx-manager-ip-address>>)에 로그인합니다.
- 2 **보안 > East West 보안 > 네트워크 검사 > 규칙 > 정책 추가.**
정책 섹션은 트래픽이 흐르는 방식을 결정하는 규칙을 정의하는 방화벽 섹션과 유사합니다.
- 3 서비스 체인을 선택합니다.
- 4 정책을 추가하려면 **게시**를 클릭합니다.
- 5 섹션의  세로 말줄임표를 클릭하고 **규칙 추가**를 클릭합니다.
- 6 멤버 자격 조건, 정적 멤버, IP/MAC 주소 또는 Active Directory 그룹을 정의하여 그룹을 추가할 **소스** 필드를 편집합니다.
 - a 다음 엔티티 중 하나를 사용하여 멤버 자격 조건을 정의합니다.
 - 가상 시스템
 - 논리적 스위치
 - 논리적 포트
 - IP 집합
 - b 다음 엔티티 중 하나를 사용하여 정적 멤버 목록을 정의합니다.
 - 그룹
 - 세그먼트
 - 세그먼트 포트
 - 가상 네트워크 인터페이스
 - 가상 시스템
- 7 **저장**을 클릭합니다.
- 8 대상 그룹을 추가하려면 **대상** 필드를 편집합니다.

- 9 [적용 대상] 필드에서 다음 중 하나를 수행할 수 있습니다.
 - **DFW**를 선택하여 논리적 스위치에 연결된 모든 가상 NIC에 규칙을 적용합니다.
 - **VM 그룹**을 선택하여 그룹의 멤버 VM의 가상 NIC에 규칙을 적용합니다. 멤버는 정적 목록에서 또는 동적 조건을 기반으로 선택될 수 있습니다. 지원되는 NSX-T Data Center 개체는 가상 시스템, 논리적 스위치, 논리적 포트, IP 집합 등입니다.
- 10 [작업] 필드에서 **리디렉션**을 선택하여 서비스 체인에 따라 트래픽을 리디렉션하거나 **리디렉션 안 함**을 선택하여 트래픽에 네트워크 검사를 적용하지 않습니다.
- 11 **게시**를 클릭합니다.
- 12 게시된 규칙을 되돌리려면 규칙을 선택하고 **되돌리기**를 클릭합니다.
- 13 정책을 추가하려면 **+ 정책 추가**를 클릭합니다.
- 14 정책 또는 규칙을 복제하려면 정책 또는 규칙을 선택하고 **복제**를 클릭합니다.
- 15 규칙을 사용하도록 설정하려면 **사용/사용 안 함** 아이콘을 사용하도록 설정하거나 규칙을 선택하고 메뉴에서 **사용 > 규칙 사용**을 클릭합니다.
- 16 규칙을 사용하거나 사용하지 않도록 설정한 후 **게시**를 클릭하여 규칙을 적용합니다.

결과

소스로 이동하는 트래픽은 네트워크 검사를 위해 서비스 체인으로 리디렉션됩니다. 체인의 서비스 프로파일 이 해당 트래픽을 검사한 후 대상으로 전송됩니다.

배포 중에는 특정 정책에 대한 VM 그룹 멤버 자격이 변경될 수 있습니다. NSX-T Data Center는 파트너 Service Manager에게 이러한 업데이트에 대해 알립니다.

게이트웨이 방화벽 구성

게이트웨이 방화벽은 경계 방화벽에서 적용된 규칙을 나타냅니다.

모든 게이트웨이 전체의 규칙이 표시되는 **모든 공유 규칙** 보기 아래에 미리 정의된 범주가 있습니다. 규칙은 위에서 아래로 평가되고 왼쪽에서 오른쪽으로 평가됩니다. 범주 이름은 API를 사용하여 변경할 수 있습니다.

표 10-4. 게이트웨이 방화벽 규칙에 대한 범주

규칙 범주	용도
진급	격리에 사용됩니다. 허용 규칙에도 사용될 수 있습니다.
시스템	이러한 규칙은 NSX-T Data Center에서 자동으로 생성되고 BFD 규칙, VPN 규칙 등과 같은 내부 제어부 트래픽과 관련이 있습니다. 참고 시스템 규칙을 편집하지 마십시오.
공유 사전 규칙	이러한 규칙은 게이트웨이에 전체적으로 적용됩니다.

표 10-4. 게이트웨이 방화벽 규칙에 대한 범주 (계속)

규칙 범주	용도
로컬 게이트웨이	이러한 규칙은 특정 게이트웨이와 관련이 있습니다.
자동 서비스 규칙	데이터부에 적용되는 자동 연결 규칙입니다. 필요에 따라 이러한 규칙을 편집할 수 있습니다.
기본값	이러한 규칙은 기본 게이트웨이 방화벽 동작을 정의합니다.

게이트웨이 방화벽 정책 및 규칙 추가

미리 정의된 범주에 속하는 방화벽 정책 섹션 아래에 추가하여 게이트웨이 방화벽 규칙을 구현합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **보안 > North South 보안 > 게이트웨이 방화벽**을 선택합니다.
- 3 게이트웨이 방화벽을 사용하도록 설정하려면 **작업 > 일반 설정**을 선택하고 상태 버튼을 전환합니다. **저장**을 클릭합니다.
- 4 **정책 추가**를 클릭합니다. 범주에 대한 자세한 내용은 **게이트웨이 방화벽 구성**을 참조하십시오.
- 5 새 정책 섹션에 대한 **이름**을 입력합니다.
- 6 정책 **대상**을 선택합니다.

7 톱니 바퀴 아이콘을 클릭하여 다음과 같은 정책 설정을 구성합니다.

설정	설명
TCP Strict	TCP 연결은 3방향 핸드셰이크(SYN, SYN-ACK, ACK)로 시작되고, 일반적으로 2방향 교환(FIN, ACK)으로 끝납니다. 특정 상황에서 방화벽에 특정 흐름에 대한 3방향 핸드셰이크가 표시되지 않을 수 있습니다(예: 비대칭 트래픽으로 인해). 기본적으로 방화벽은 3방향 핸드셰이크를 확인해야 한다는 요구를 적용하지 않으며 이미 설정된 세션을 선택합니다. 섹션별로 TCP Strict를 사용하도록 설정하여 중간 세션 선택을 해제하고 3방향 핸드셰이크에 대한 요구 사항을 적용할 수 있습니다. 특정 방화벽 정책에 대해 TCP Strict 모드를 사용하도록 설정하고 기본 임의-임의 차단 규칙을 사용할 경우, 3방향 핸드셰이크 연결 요구 사항을 완료하지 못하고 이 정책 섹션의 TCP 기반 규칙과 일치하는 패킷은 삭제됩니다. Strict는 상태 저장 TCP 규칙에만 적용되며 게이트웨이 방화벽 정책 수준에서 사용하도록 설정됩니다. TCP Strict는 TCP 서비스가 지정되지 않은 기본 임의-임의 허용과 일치하는 패킷에는 적용되지 않습니다.
상태 저장	상태 저장 방화벽은 활성 연결 상태를 모니터링하고 이 정보를 사용하여 방화벽을 통해 보낼 패킷을 결정합니다.
잠금	여러 사용자가 동일한 섹션을 변경하지 못하도록 정책을 잠글 수 있습니다. 섹션을 잠글 때는 주석을 포함해야 합니다.

- 8 **게시**를 클릭합니다. 한 번에 여러 정책을 추가하고 함께 게시할 수 있습니다.
새 정책이 화면에 표시됩니다.
- 9 정책 섹션을 선택하고 **규칙 추가**를 클릭합니다.
- 10 규칙의 이름을 입력합니다. IPv4, IPv6 및 멀티캐스트 주소가 지원됩니다.
- 11 **소스** 열에서 편집 아이콘을 클릭하고 규칙의 소스를 선택합니다. 자세한 내용은 **그룹 추가** 항목을 참조하십시오.
- 12 **대상** 열에서 편집 아이콘을 클릭하고 규칙의 대상을 선택합니다. 정의되지 않은 경우 대상은 임의와 일치합니다. 자세한 내용은 **그룹 추가** 항목을 참조하십시오.
- 13 **서비스** 열에서 연필 아이콘을 클릭하고 서비스를 선택합니다. 정의되지 않은 경우 서비스는 임의와 일치합니다.
- 14 **프로파일** 열에서 편집 아이콘을 클릭하고 컨텍스트 프로파일을 선택하거나 **새 컨텍스트 프로파일 추가**를 클릭합니다. **컨텍스트 프로파일 추가**의 내용을 참조하십시오.
 - 컨텍스트 프로파일은 Tier-0 게이트웨이 방화벽 정책에서 지원되지 않습니다.
 - 게이트웨이 방화벽 규칙은 FQDN 특성 또는 기타 하위 특성이 있는 컨텍스트 프로파일을 지원하지 않습니다.

컨텍스트 프로파일은 분산 방화벽 규칙 및 게이트웨이 방화벽 규칙에서 사용하기 위해 계층 7 APP ID 특성을 사용합니다. 서비스가 **임의**로 설정된 방화벽 규칙에서는 여러 애플리케이션 ID 컨텍스트 프로파일을 사용할 수 있습니다. ALG 프로파일(FTP 및 TFTP)의 경우 규칙당 하나의 컨텍스트 프로파일이 지원됩니다.

15 **적용**을 클릭합니다.

16 **적용 대상** 열은 규칙 당 적용 범위를 정의하고 사용자가 하나 이상의 업링크 인터페이스 또는 서비스 인터페이스에 규칙을 선택적으로 적용할 수 있도록 허용합니다. 기본적으로 게이트웨이 방화벽 규칙은 선택한 게이트웨이의 사용 가능한 모든 업링크 및 서비스 인터페이스에 적용됩니다.

17 **작업** 열에서 작업을 선택합니다.

옵션	설명
허용	지정된 소스, 대상 및 프로토콜을 가진 모든 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. 패킷을 거부하면 연결할 수 없는 대상 메시지가 보낸 사람에게 전송됩니다. 프로토콜이 TCP인 경우 TCP RST 메시지가 전송됩니다. UDP, ICMP 및 기타 IP 연결에 대해 관리 목적으로 금지된 코드가 포함된 ICMP 메시지가 전송됩니다. 1번 시도된 후에 전송하는 애플리케이션에 연결을 설정할 수 없다는 알림이 제공됩니다.

18 **상태 전환** 버튼을 클릭하여 규칙을 사용하거나 사용하지 않도록 설정합니다.

19 **톱니 바퀴** 아이콘을 클릭하여 로깅, 방향, IP 프로토콜, 태그 및 메모를 설정합니다.

옵션	설명
로깅	로깅은 끄거나 켤 수 있습니다. 로그는 Edge의 /var/log/syslog에 저장됩니다.
방향	옵션은 수신 , 송신 및 수신/송신 입니다. 기본값은 수신/송신 입니다. 이 필드는 대상 개체의 관점에서 트래픽 방향을 나타냅니다. 수신 은 개체로 들어오는 트래픽만 확인하고, 송신 은 개체에서 나가는 트래픽만 확인하며, 수신/송신 은 양쪽 방향 트래픽 모두 확인함을 의미합니다.
IP 프로토콜	옵션은 IPv4 , IPv6 및 IPv4_IPv6 입니다. 기본값은 IPv4_IPv6 입니다.
태그	규칙에 추가된 태그입니다.

참고 방화벽 규칙의 흐름 통계를 보려면 그래프 아이콘을 클릭합니다. 바이트, 패킷 수 및 세션과 같은 정보를 볼 수 있습니다.

20 **게시**를 클릭합니다. 한 번에 여러 규칙을 추가하고 함께 게시할 수 있습니다.

21 각 정책 섹션에서 **정보** 아이콘을 클릭하여 Edge 노드로 푸시된 Edge 방화벽 규칙의 현재 상태를 확인합니다. 규칙이 Edge 노드로 푸시되었을 때 생성된 경보도 표시됩니다.

22 Edge 노드에 적용되는 정책 규칙의 통합 상태를 보려면 API 호출을 수행합니다.

```
GET https://<policy-mgr>/policy/api/v1/infra/realized-state/status?
intent_path=/infra/domains/default/gateway-policies/
<GatewayPolicy_ID>&include_enforced_status=true
```

종방향 네트워크 보안 - 타사 서비스 삽입

NSX-T Data Center는 데이터 센터의 Tier-0 또는 Tier-1 라우터에 타사 서비스를 삽입하여 자체 검사를 위해 타사 서비스로 트래픽을 리디렉션하는 기능을 제공합니다. 북-남 서비스 VM을 배포하려는 경우 ESXi 호스트만 지원됩니다. KVM 호스트는 지원되지 않습니다.

종방향 네트워크 보안에 대한 상위 수준 작업

North-South 트래픽에 대한 네트워크 보안을 설정하려면 다음 단계를 따르십시오.

표 10-5. North-South 네트워크 검사를 구성하기 위한 작업 목록

워크플로 작업	개인 설정	구현
NSX-T Data Center에 서비스 등록	파트너	API만
North-South 트래픽 검사를 위한 서비스 배포	관리자	API 및 NSX Manager UI
트래픽 리디렉션 구성	관리자	API 및 NSX Manager UI

North-South 트래픽 검사를 위한 서비스 배포

서비스를 등록한 후 서비스가 네트워크 트래픽 처리를 시작하려면 서비스의 인스턴스를 배포해야 합니다.

vCenter Server에서 물리적 환경과 논리적 네트워크 간에 게이트웨이로 작동하는 Tier-0 또는 Tier-1 논리적 라우터에서 파트너 서비스 VM을 배포합니다 SVM을 독립형 서비스 인스턴스 또는 활성-대기 서비스 인스턴스로 배포한 후 트래픽을 네트워크 검사를 위한 SVM으로 리디렉션하기 위한 리디렉션 규칙을 생성할 수 있습니다.

사전 요구 사항

- 모든 호스트가 vCenter Server에서 관리됩니다.
- 파트너 서비스가 NSX-T Data Center에 등록되었고 배포할 수 있습니다.
- NSX-T Data Center 관리자는 파트너 서비스에 액세스할 수 있습니다.
- 논리적 라우터의 고가용성 모드는 액티브-대기 모드에 있어야 합니다.
- Distributed Resource Scheduler 유틸리티를 켭니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(https://<nsx-manager-ip-address>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 파트너 서비스 > 서비스 인스턴스 > 카탈로그**를 선택합니다.
- 3 [카탈로그] 탭에는 등록된 서비스가 표시됩니다.
- 4 OVF 폼 팩터에 표시된 서비스를 선택하고 **배포**를 클릭하여 서비스 인스턴스의 배포를 시작합니다.
- 5 [파트너 서비스 삽입] 창에서 **계속**을 클릭합니다.
- 6 [파트너 서비스] 창에서 세부 정보를 입력합니다.

표 10-6. 파트너 서비스 세부 정보

필드	설명
인스턴스 이름	서비스 인스턴스를 식별할 이름을 입력합니다.
설명	서비스 인스턴스에 대한 설명입니다.
파트너 서비스	NSX-T Data Center에 등록된 파트너 서비스를 선택합니다.
배포 구역	배포할 폼 팩터를 선택합니다.
논리적 라우터	서비스 인스턴스를 배포해야 하는 Tier-0 논리적 라우터를 선택합니다.

- 7 **다음**을 클릭합니다.
- 8 [인스턴스 구성] 창에서 세부 정보를 입력합니다.

표 10-7. 서비스 인스턴스 세부 정보

필드	설명
배포 모드	Tier-0 논리적 라우터에서 단일 서비스 인스턴스를 배포하려면 독립형 을 선택합니다. Tier-0 논리적 라우터에서 활성-대기 모드로 몇 개의 서비스 인스턴스를 배포하려면 고가용성 을 선택합니다.
실패 정책	허용 또는 차단 을 선택합니다.
서비스 인스턴스 IP 주소	서비스 인스턴스에 사용할 IP 주소를 입력합니다.
게이트웨이	게이트웨이 주소를 입력합니다.
서브넷 마스크	서브넷 마스크를 입력합니다.
네트워크 ID	관리 네트워크를 연결할 논리적 스위치의 네트워크 ID를 입력합니다.
계산 관리자	등록된 vCenter Server를 선택합니다.
리소스 풀	서비스 인스턴스를 배포하기 위한 리소스를 제공하는 리소스 풀을 선택합니다.

표 10-7. 서비스 인스턴스 세부 정보 (계속)

필드	설명
데이터스토어	서비스 인스턴스 데이터를 저장할 저장소를 선택합니다.

9 다음을 클릭합니다.

10 [고급 구성] 창에서 세부 정보를 입력합니다.

표 10-8.

필드	설명
배포 템플릿	서비스 인스턴스의 배포 중에 사용할 템플릿을 선택합니다.
라이선스	템플릿의 라이선스를 입력합니다.

11 완료를 클릭합니다.

결과

[서비스 인스턴스] 탭에는 배포 진행률이 표시됩니다. 배포를 완료하려면 몇 분 정도 걸릴 수 있습니다. 배포 상태를 확인하여 Tier-0 논리적 라우터에서 서비스 인스턴스가 배포되었는지 확인합니다.

또는 vCenter Server로 이동하여 배포 상태를 확인합니다.

다음에 수행할 작업

Tier-0 라우터에서 배포된 서비스 인스턴스로 트래픽을 리디렉션하도록 규칙을 구성합니다. 트래픽 리디렉션 구성 항목을 참조하십시오.

트래픽 리디렉션 구성

서비스 인스턴스를 배포한 후 라우터가 서비스로 리디렉션하는 트래픽의 유형을 구성합니다. 트래픽 리디렉션 구성은 방화벽 구성과 유사합니다.

방화벽 구성에 대한 자세한 내용은 방화벽 섹션 및 방화벽 규칙을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 고급 네트워킹 및 보안 > 파트너 서비스 > 서비스 인스턴스를 선택합니다.
- 3 서비스 인스턴스를 클릭합니다.
- 4 트래픽 리디렉션 탭을 클릭합니다.
- 5 섹션을 추가하려면 기존 섹션을 선택하고 섹션 추가를 클릭합니다.
 - ◆ 메뉴에서 위에 섹션 추가 또는 아래에 섹션 추가를 선택합니다.

새 섹션이 생성됩니다. 리디렉션할 트래픽 유형이 **L3 리디렉션**으로 설정되고, 서비스 유형은 **상태 정보를 저장하지 않는**이며, **적용 대상** 필드가 호스트에 구성된 Tier-0 논리적 라우터에 연결됩니다. 규칙을 정의하면 **규칙** 필드가 자동으로 채워집니다.

- 6 **계시**를 클릭하여 섹션의 구성 세부 정보를 유지합니다.
- 7 해당 섹션에 규칙을 추가하려면 섹션을 선택하고 **규칙 추가**를 클릭합니다.
- 8 규칙 행에 다음 세부 정보를 입력합니다.
 - a 규칙 이름을 입력합니다.
 - b L3 트래픽의 소스 및 대상을 입력합니다. 파트너 서비스 VM은 대상 VM으로 리디렉션하기 전에 소스에서의 트래픽 흐름을 검사합니다.
 - c **적용 대상** 필드에서 Tier-0 라우터의 업링크를 선택합니다.
 - d **작업** 필드에서 서비스 VM이 트래픽을 검사해야 하는 경우에는 **리디렉션**을 선택하고, 트래픽이 North-South를 검사할 필요가 없는 경우에는 **리디렉션 안 함**을 선택합니다.
- 9 각 규칙은 개별적으로 사용하도록 설정할 수 있습니다. 규칙을 사용하도록 설정하면 규칙과 일치하는 트래픽에 해당 규칙이 적용됩니다.
- 10 [고급 설정]을 클릭하여 트래픽 방향을 구성하고 로깅을 사용하도록 설정합니다.
- 11 규칙을 포함하는 섹션의 끝에서 **계시**를 클릭하여 섹션에 규칙을 유지하거나 **복구**를 클릭하여 작업을 취소합니다.

결과

트래픽은 정책 규칙이 트래픽에 적용되는 네트워크 검사 규칙으로 전송됩니다.

다음에 수행할 작업

[North-South 트래픽에 대한 리디렉션 규칙 추가](#)의 내용을 참조하십시오.

North-South 트래픽에 대한 리디렉션 규칙 추가

고급 네트워킹 및 보안 UI를 사용하여 North-South 리디렉션 규칙을 설정합니다. 트래픽 리디렉션은 Tier-0 라우터에 삽입된 서비스에 대해서만 발생합니다.

트래픽 리디렉션 구성의 지침을 참조하십시오.

사전 요구 사항

- NSX-T에 타사 서비스를 등록하고 배포합니다.
- Tier-0 라우터를 구성합니다.

절차

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

2 보안 > North South 방화벽 > 네트워크 검사(N-S) > 정책 추가.

정책 섹션은 트래픽이 흐르는 방식을 결정하는 규칙을 정의하는 방화벽 섹션과 유사합니다.

- 3 **리디렉션 대상**을 NSX-T에 등록된 서비스 인스턴스로 설정하여 소스 및 대상 엔티티 간의 트래픽 흐름에 대해 네트워크 검사를 수행합니다.
- 4 정책을 추가하려면 **계시**를 클릭합니다.
- 5 섹션의  세로 말줄임표를 클릭하고 **규칙 추가**를 클릭합니다.
- 6 멤버 자격 조건, 정적 멤버, IP/MAC 주소 또는 Active Directory 그룹을 정의하여 그룹을 추가할 **소스** 필드를 편집합니다. 멤버 자격 조건은 가상 시스템, 논리적 스위치, 논리적 포트, IP 집합의 유형 중 하나에서 정의될 수 있습니다. 그룹, 세그먼트, 세그먼트 포트, 가상 네트워크 인터페이스, 가상 시스템의 범주 중 하나에서 정적 멤버를 선택할 수 있습니다.
- 7 **저장**을 클릭합니다.
- 8 대상 그룹을 추가하려면 **대상** 필드를 편집합니다.
- 9 [적용 대상] 필드에서 다음 중 하나를 수행할 수 있습니다.
 - **DFW**를 선택하여 논리적 스위치에 연결된 모든 가상 NIC에 규칙을 적용합니다.
 - **VM 그룹**을 선택하여 그룹의 멤버 VM의 가상 NIC에 규칙을 적용합니다. 멤버는 정적 목록에서 또는 동적 조건을 기반으로 선택될 수 있습니다. 지원되는 NSX-T Data Center 개체는 가상 시스템, 논리적 스위치, 논리적 포트, IP 집합 등입니다.
- 10 [작업] 필드에서 **리디렉션**을 선택하여 서비스 인스턴스에 따라 트래픽을 리디렉션하거나 **리디렉션 안 함**을 선택하여 트래픽에 네트워크 검사를 적용하지 않습니다.
- 11 **계시**를 클릭합니다.
- 12 게시된 규칙을 되돌리려면 규칙을 선택하고 **되돌리기**를 클릭합니다.
- 13 정책을 추가하려면 **+ 정책 추가**를 클릭합니다.
- 14 정책 또는 규칙을 복제하려면 정책 또는 규칙을 선택하고 **복제**를 클릭합니다.
- 15 규칙을 사용하도록 설정하려면 사용/사용 안 함 아이콘을 사용하도록 설정하거나 규칙을 선택하고 메뉴에서 **사용 > 규칙 사용**을 클릭합니다.
- 16 규칙을 사용하거나 사용하지 않도록 설정한 후 **계시**를 클릭하여 규칙을 적용합니다.

결과

작업 설정에 따라, North-South 트래픽이 네트워크 검사를 위해 서비스 인스턴스로 리디렉션됩니다.

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 **고급 네트워킹 및 보안 > 파트너 서비스 > 서비스 인스턴스**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.

끝점 보호

NSX-T Data Center를 사용하면 타사 파트너 서비스를 끝점 보호 서비스를 제공하는 별도의 서비스 VM으로 삽입할 수 있습니다. 파트너 서비스 VM은 NSX-T Data Center 관리자가 적용한 끝점 보호 정책 규칙을 기준으로 게스트 VM에서 파일, 프로세스 및 레지스트리 이벤트를 처리합니다.

끝점 보호 이해

끝점 보호의 사용 사례, 워크플로 및 주요 개념을 파악합니다.

끝점 보호 사용 사례

가상 환경에서 게스트 검사 플랫폼을 사용하여 게스트 VM에 바이러스 백신 및 맬웨어 방지 보호 기능을 제공합니다.

NSX 관리자는 게스트 VM에서 파일 또는 프로세스 활동을 모니터링하기 위해 서비스 가상 시스템(서비스 VM 또는 SVM)으로 배포되는 바이러스 백신 및 맬웨어 방지 솔루션을 구현합니다. 파일에 액세스 할 때마다(예: 파일 열기 시도) 맬웨어 방지 서비스 VM에 이벤트가 통보됩니다. 그런 다음, 서비스 VM은 이벤트에 응답하는 방법을 결정합니다. 예를 들어, 파일의 바이러스 서명을 검사합니다.

- 서비스 VM이 파일에 바이러스가 없다고 판단하면 파일 열기 작업이 허용됩니다.
- 서비스 VM이 파일에서 바이러스를 감지하면 게스트 VM의 Thin Agent에 다음 방법 중 하나로 작동하도록 요청합니다.
 - 감염된 파일을 삭제하거나 파일에 대한 액세스를 거부합니다.
 - 감염된 VM에는 NSX를 통해 태그를 할당할 수 있습니다. 또한 태그가 지정된 게스트 VM을 보안 그룹으로 자동으로 이동하여 추가 검색 및 격리를 위해 감염이 완전히 제거될 때까지 감염된 VM을 네트워크에서 격리하는 규칙을 정의할 수 있습니다.

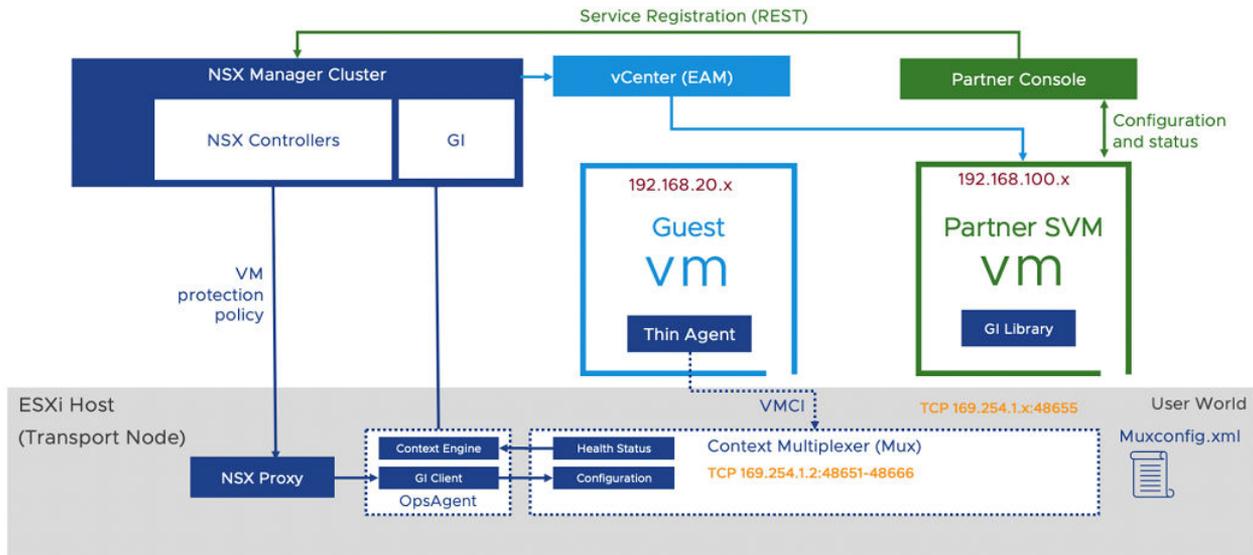
Guest Introspection 플랫폼을 사용하여 게스트 VM 끝점을 보호하면 다음과 같은 이점이 있습니다.

- 계산 리소스 사용량 감소: Guest Introspection은 호스트의 각 끝점에서 호스트의 타사 파트너 서비스 VM으로 바이러스 서명 및 보안 검색 논리를 오프로드합니다. 바이러스 검색은 서비스 VM에서만 발생하므로 바이러스 검색을 실행하기 위해 게스트 VM의 계산 리소스를 소비할 필요가 없습니다.
- 보다 효율적인 관리: 바이러스 검색을 서비스 VM으로 오프로드하면 호스트당 하나의 개체로만 바이러스 서명을 업데이트해야 합니다. 이와 같은 메커니즘은 동일한 바이러스 서명을 모든 게스트 VM에서 업데이트해야 하는 에이전트 기반 솔루션보다 더 잘 작동합니다.
- 지속적인 바이러스 백신 및 맬웨어 방지 보호: 서비스 VM이 계속해서 실행되므로 게스트 VM이 최신 바이러스 서명을 실행하도록 위임되지 않습니다. 예를 들어, 스냅샷 VM은 이전 버전의 바이러스 서명을 실행하여 끝점을 보호하는 기존 방식으로 보호할 수 있습니다. Guest Introspection 플랫폼을 사용하면 서비스 VM이 최신 바이러스 및 맬웨어 서명을 계속 실행하여 새로 추가된 VM도 최신 바이러스 서명으로 보호되도록 합니다.
- 서비스 VM으로 바이러스 서명 오프로드: 바이러스 데이터베이스 수명 주기가 게스트 VM 수명 주기를 벗어나며 서비스 VM이 게스트 VM 중단에 영향을 받지 않습니다.

Guest Introspection 아키텍처

NSX-T Data Center의 서비스 삽입 및 Guest Introspection 구성 요소에 대한 아키텍처를 이해합니다.

그림 10-1. Guest Introspection 아키텍처



핵심 개념:

- 파트너 콘솔: Guest Introspection 플랫폼에서 작업하기 위해 보안 벤더에서 제공하는 웹 애플리케이션입니다.
- NSX Manager: 네트워크 및 보안 정책 구성을 위해 고객 및 파트너에게 API 및 그래픽 사용자 인터페이스를 제공하는 NSX용 관리부 장치입니다. Guest Introspection의 경우 NSX Manager는 파트너 장치를 배포 및 관리하기 위한 API 및 GUI를 제공합니다.

- Guest Introspection SDK: 보안 벤더에서 사용하는 VMware 제공 라이브러리입니다.
- 서비스 VM: VMware에서 제공한 Guest Introspection SDK를 사용하는 보안 벤더 제공 VM입니다. 게스트에서 바이러스 또는 맬웨어를 감지하기 위해 파일을 검색하거나 이벤트를 처리하는 논리가 포함되어 있습니다. 요청을 검색한 후에는 요청에서 게스트 VM이 수행한 작업에 대한 결과 또는 알림을 다시 전송합니다.
- Guest Introspection 호스트 에이전트(컨텍스트 멀티플렉서): 끝점 보호 정책의 구성을 처리합니다. 또한 메시지를 멀티플렉싱한 후 보호된 VM에서 서비스 VM으로 전달합니다. Guest Introspection 플랫폼의 상태를 보고하고 서비스 VM 구성의 기록을 muxconfig.xml 파일에 유지합니다.
- Ops 에이전트(컨텍스트 엔진 및 Guest Introspection 클라이언트): Guest Introspection 구성을 Guest Introspection 호스트 에이전트(컨텍스트 멀티플렉서)로 전달합니다. 또한 솔루션의 상태를 NSX Manager로 릴레이합니다.
- EAM: NSX Manager는 ESXi Agent Manager를 사용하여 보호를 위해 구성된 클러스터의 모든 호스트에 파트너 서비스 VM을 배포합니다.
- Thin Agent: 게스트 VM에서 실행되는 파일 또는 네트워크 자체 검사 에이전트입니다. 또한 호스트 에이전트를 통해 서비스 VM으로 전달되는 파일 및 네트워크 작업을 가로챍니다. 이 에이전트는 VMware Tools의 일부입니다. 바이러스 백신 또는 맬웨어 방지 보안 벤더에서 제공하는 기존 에이전트를 교체합니다. 이는 벤더가 제공한 서비스 VM을 검색하기 위해 파일 및 프로세스를 용이하게 오픈로드하도록 하는 일반적인 경량 에이전트입니다.

끝점 보호의 핵심 개념

끝점 보호 워크플로에서는 파트너가 NSX-T Data Center에 서비스를 등록해야 하며 관리자가 이러한 서비스를 사용해야 합니다. 다음은 해당 워크플로를 이해하는 데 도움이 되는 몇 가지 개념입니다.

- 서비스 정의: 파트너는 이름, 설명, 지원되는 폼 팩터, 네트워크 인터페이스 및 SVM에서 사용될 장치 OVF 패키지 위치를 포함하는 배포 특성으로 서비스를 정의합니다.
- 서비스 삽입: NSX는 파트너가 네트워킹 및 보안 솔루션을 NSX 플랫폼과 통합할 수 있도록 하는 서비스 삽입 프레임워크를 제공합니다. Guest Introspection 솔루션은 이와 같은 서비스 삽입 형식입니다.
- 서비스 프로파일 및 벤더 템플릿: 파트너는 정책에 대한 보호 수준을 표시하는 벤더 템플릿을 등록합니다. 예를 들어 보호 수준은 Gold, Silver 또는 Platinum일 수 있습니다. NSX 관리자가 기본 설정에 따라 벤더 템플릿에 이름을 지정할 수 있는 벤더 템플릿에서 서비스 프로파일을 생성할 수 있습니다. Guest Introspection 이외의 서비스에서 서비스 프로파일은 특성을 사용한 추가 사용자 지정을 허용합니다. 그런 다음, 서비스 프로파일을 끝점 보호 정책 규칙에서 사용하여 NSX에 정의된 가상 시스템 그룹에 대한 보호를 구성할 수 있습니다. 관리자는 VM 이름, 태그 또는 식별자를 기준으로 그룹을 생성할 수 있습니다. 단일 벤더 템플릿에서 여러 서비스 프로파일을 선택적으로 생성할 수 있습니다.
- 끝점 보호 정책: 정책은 규칙의 모음입니다. 여러 정책이 있는 경우에는 순서대로 정렬하여 실행합니다. 정책 내에 정의된 규칙의 경우도 마찬가지입니다. 예를 들어, 정책 A에는 세 개의 규칙이 있고, 정책 B에는 4개의 규칙이 있고, 정책 A가 정책 B보다 우선하는 순서로 정렬되어 있습니다. Guest Introspection이 정책 실행을 시작할 때 정책 A의 규칙이 정책 B의 규칙보다 먼저 실행됩니다.

- **끝점 보호 규칙:** NSX 관리자는 보호될 가상 시스템 그룹을 지정하는 규칙을 생성하고 각 규칙에 대한 서비스 프로파일을 지정하여 해당 그룹에 대한 보호 수준을 선택할 수 있습니다.
- **서비스 인스턴스:** 호스트의 서비스 VM을 참조합니다. 서비스 VM은 vCenter에서 특수 VM으로 취급되며 게스트 VM의 전원이 켜지기 전에 시작되고, 모든 게스트 VM의 전원이 꺼진 후에 중지됩니다. 서비스당 호스트별로 하나의 서비스 인스턴스가 있습니다.

중요 서비스 인스턴스의 수는 서비스가 호스트를 실행 중인 호스트 수와 같습니다. 예를 들어, 클러스터에 호스트가 8개 있고 파트너 서비스가 두 개의 클러스터에 배포된 경우 실행 중인 총 서비스 인스턴스 수는 16개의 SVM입니다.

- **서비스 배포:** admin는 클러스터별로 NSX-T를 통해 파트너 서비스 VM을 배포합니다. 배포는 클러스터 수준에서 관리되므로 클러스터에 호스트를 추가할 때 EAM은 서비스 VM을 자동으로 배포합니다. SVM을 자동으로 배포하는 것은 DRS(Distributed Resource Scheduler) 서비스가 vCenter Cluster에 구성된 경우 SVM이 새 호스트에서 배포되고 시작된 후 vCenter가 클러스터에 추가된 새 호스트로 기존 VM을 재조정하거나 배포할 수 있으므로 중요한 작업입니다. 게스트 VM에 보안을 제공하기 위해서는 파트너 서비스 VM에 NSX-T 플랫폼이 필요하므로 호스트를 전송 노드로 준비해야 합니다.

중요 하나의 서비스 배포는 하나의 파트너 서비스를 배포 및 구성하기 위해 관리되는 vCenter Server의 단일 클러스터를 참조합니다.

- **파일 자체 검사 드라이버:** 게스트 VM에 설치되며, 게스트 VM의 파일 작업을 가로칩니다.
- **네트워크 자체 검사 드라이버:** 게스트 VM에 설치되고 게스트 VM의 네트워크 트래픽, 프로세스 및 사용자 활동을 가로칩니다.

끝점 보호를 위한 상위 수준 작업

보안 검색 논리가 포함된 타사 파트너 서비스는 게스트 VM 보호를 위해 NSX-T Data Center에 등록됩니다. NSX 관리자가 등록된 서비스를 배포하고 끝점 보호 정책을 게스트 VM 그룹에 적용할 때 파트너 서비스가 적용됩니다.

끝점 보호 사용 사례에 대한 Guest Introspection 워크플로는 다음과 같습니다.

그림 10-2. 끝점 보호 워크플로

워크플로 작업	역할/개인 설정	구현
NSX-T Data Center에 서비스 등록	파트너 관리자	파트너 콘솔
NSX-T Data Center에 서비스 등록	파트너 관리자	파트너 콘솔
NSX-T Data Center에 서비스 등록	파트너 관리자	파트너 콘솔
서비스 배포	NSX 관리자	API 및 NSX Manager UI
서비스 인스턴스 세부 정보 보기	NSX 관리자	API 및 NSX Manager UI
서비스 인스턴스 가져오기	NSX 관리자	API 및 NSX Manager UI
서비스 프로파일 추가	NSX 관리자	API 및 NSX Manager UI

워크플로 작업	역할/개인 설정	구현
Guest Introspection 정책 사용	NSX 관리자	API 및 NSX Manager UI
끝점 보호 규칙 추가 및 게시	NSX 관리자	API 및 NSX Manager UI
끝점 보호 상태 모니터링	NSX 관리자	API 및 NSX Manager UI

끝점 보호 구성

타사 파트너 보안 서비스를 사용하여 NSX-T Data Center 환경에서 실행되는 게스트 VM을 보호합니다. 끝점 보호 정책을 구성하기 위한 상위 수준 단계는 다음과 같습니다.

- 1 게스트 VM의 끝점 보호를 구성하기 전에 끝점 보호를 구성하기 위한 전제 조건이 충족되는지 확인하십시오.
- 2 지원되는 소프트웨어. 지원되는 소프트웨어 항목을 참조하십시오.
- 3 Linux VM용 파일 자체 검사 드라이버를 설치합니다. Linux 가상 시스템에서 Guest Introspection Thin Agent 설치 항목을 참조하십시오.
- 4 Windows VM용 파일 자체 검사 드라이버를 설치합니다. Linux 가상 시스템에서 Guest Introspection Thin Agent 설치 항목을 참조하십시오.
- 5 Linux VM용 Network Introspection 드라이버를 설치합니다. 네트워크 자체 검사용 Linux Thin Agent 설치 항목을 참조하십시오.
- 6 Guest Introspection 파트너 관리자 역할을 사용하여 사용자를 생성합니다. Guest Introspection 파트너 관리자 역할을 사용하여 사용자 생성 항목을 참조하십시오.
- 7 파트너 서비스를 NSX-T Data Center에 등록합니다. 파트너 설명서를 참조하십시오.
- 8 서비스를 배포합니다. 서비스 배포 항목을 참조하십시오.
- 9 Guest Introspection 정책을 사용합니다. Guest Introspection 정책 사용 항목을 참조하십시오.
- 10 끝점 보호 규칙을 추가 및 게시합니다. 끝점 보호 규칙 추가 및 게시 항목을 참조하십시오.
- 11 끝점 보호 규칙을 모니터링합니다. 끝점 보호 상태 모니터링 항목을 참조하십시오.

끝점 보호를 구성하기 위한 전제 조건

게스트 VM에 대한 끝점 보호를 구성하기 전에 사전 요구 사항이 충족되었는지 확인합니다.

사전 요구 사항

- NSX Manager가 모든 호스트에 설치되어 있습니다.
- 전송 노드 프로파일을 적용하여 NSX-T Data Center 클러스터를 전송 노드로 준비하고 구성합니다. 호스트가 전송 노드로 구성된 후 Guest Introspection 구성 요소가 설치됩니다. "NSX-T Data Center 설치 가이드"를 참조하십시오.
- 파트너 콘솔을 설치하고 NSX-T Data Center에 서비스를 등록하도록 구성합니다.
- 게스트 VM이 VM 하드웨어 구성 파일 버전 9 이상을 실행하는지 확인합니다.

- VMware Tools를 구성하고 Thin Agent를 설치합니다.
 - Linux 가상 시스템에서 Guest Introspection Thin Agent 설치 항목을 참조하십시오.
 - Windows 가상 시스템에서 Guest Introspection Thin Agent 설치 항목을 참조하십시오.
 - 네트워크 자체 검사용 Linux Thin Agent 설치 항목을 참조하십시오.

Linux 가상 시스템에서 Guest Introspection Thin Agent 설치

Guest Introspection은 바이러스 백신 용도로만 Linux에서 파일 검사를 지원합니다. Guest Introspection 보안 솔루션을 사용하여 Linux VM을 보호하려면 Guest Introspection Thin Agent를 설치해야 합니다.

Linux Thin Agent는 OSP(운영 체제별 패키지)의 일부로 사용할 수 있습니다. 패키지는 VMware 패키지 포털에서 호스팅됩니다. 엔터프라이즈 또는 보안 관리자(비 NSX 관리자)는 NSX 외부의 게스트 VM에 에이전트를 설치할 수 있습니다.

VMware Tools는 설치하지 않아도 됩니다.

Linux 운영 체제에 따라 루트 권한을 사용하여 다음 단계를 수행하십시오.

사전 요구 사항

- 게스트 가상 시스템에 지원되는 Linux 버전이 설치되어 있는지 확인하십시오.
 - RHEL(Red Hat Enterprise Linux) 7.4(64비트) GA
 - SLES(SUSE Linux Enterprise Server) 12(64비트) GA
 - Ubuntu 16.04.5 LTS(64비트) GA
 - CentOS 7.4 GA
- Linux VM에 GLib 2.0이 설치되어 있는지 확인합니다.

절차

1 Ubuntu 시스템

- a 다음 명령을 사용하여 VMware 패키징 공개 키를 가져옵니다.

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
apt-key add VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b /etc/apt/sources.list.d에 새 파일 vmware.list를 생성합니다.
- c 다음 내용으로 파일을 편집합니다.

```
deb [arch=amd64] https://packages.vmware.com/packages/nsx-gi/latest/ubuntu/ xenial main
```

- d 패키지를 설치합니다.

```
apt-get update
apt-get install vmware-nsx-gi-file
```

2 RHEL7 시스템

- a 다음 명령을 사용하여 VMware 패키징 공개 키를 가져옵니다.

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b /etc/yum.repos.d에 새 파일 vmware.repo를 생성합니다.

- c 다음 내용으로 파일을 편집합니다.

```
[vmware]
name = VMware
baseurl = https://packages.vmware.com/packages/nsx-gi/latest/rhel7/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```

3 패키지를 설치합니다.

```
yum install vmware-nsx-gi-file
```

4 SLES 시스템

- a 다음 명령을 사용하여 VMware 패키징 공개 키를 가져옵니다.

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b 다음 저장소를 추가합니다.

```
zypper ar -f "https://packages.vmware.com/packages/nsx-gi/latest/sle12/x86_64/" VMware
```

- c 패키지를 설치합니다.

```
zypper install vmware-nsx-gi-file
```

5 CentOS 시스템

- a 다음 명령을 사용하여 VMware 패키징 공개 키를 가져옵니다.

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-
RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b /etc/yum.repos.d에 새 파일 vmware.repo를 생성합니다.

- c 다음 내용으로 파일을 편집합니다.

```
[vmware]
name = VMware
baseurl = https://packages.vmware.com/packages/nsx-gi/latest/centos7/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```

다음에 수행할 작업

Thin Agent가 관리 권한의 서비스 vsepd status 명령을 사용하여 실행되고 있는지 확인합니다. 상태는 실행 중이어야 합니다.

네트워크 자체 검사용 Linux Thin Agent 설치

Linux Thin Agent를 설치하여 네트워크 트래픽을 검사합니다.

중요 게스트 VM을 바이러스 백신으로 보호하기 위해 네트워크 자체 검사용 Linux Thin Agent를 설치할 필요가 없습니다.

네트워크 트래픽을 검사하는 데 사용되는 Linux Thin Agent 드라이버는 오픈 소스 드라이버에 따라 다릅니다.

사전 요구 사항

다음 패키지를 설치합니다.

- glib2
- libnetfilter-contrack3/ libnetfilter-contrack
- libnetfilter-queue1/ libnetfilter-queue
- iptables

절차

1 Guest Introspection에서 제공하는 오픈 소스 드라이버를 설치하려면

- a 다음 URL을 운영 체제의 기본 URL로 추가합니다.

```
deb [arch=amd64] https://packages.vmware.com/guest-introspection-for-vmware-nsx/latest/
```

- b VMware 패키징 키를 가져옵니다.

```
https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- c 저장소를 업데이트하고 오픈 소스 드라이버를 설치합니다.

```
apt-get install Guest-Introspection-for-VMware-NSX
```

2 파일 및 네트워크 트래픽을 검사하는 데 사용되는 Linux Thin Agent를 설치합니다.

- 파일 및 네트워크 자체 검사 패키지를 설치하려면 c단계에서 vmware-nsx-gi 패키지를 선택합니다.
 - 네트워크 자체 검사 패키지를 설치하려면 c단계에서 vmware-nsx-gi-net 패키지를 선택합니다.
- a 다음 URL을 운영 체제의 기본 URL로 추가합니다.

```
deb [arch=amd64] https://packages.vmware.com/packages/nsx-gi/latest
```

- b VMware 패키징 키를 가져옵니다.

```
https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- c 드라이버 중 하나를 설치합니다.

```
vmware-nsx-gi
vmware-nsx-gi-net
```

Windows 가상 시스템에서 Guest Introspection Thin Agent 설치

Guest Introspection 보안 솔루션을 사용하여 VM을 보호하려면 VM에 Guest Introspection 드라이버라고도 하는 Guest Introspection Thin Agent를 설치해야 합니다. Guest Introspection 드라이버는 Windows용 VMware Tools에 포함되어 있으나 기본 설치의 일부는 아닙니다. Windows VM에 Guest Introspection을 설치하려면 사용자 지정 설치를 수행하고 해당 드라이버를 선택해야 합니다.

Guest Introspection 드라이버가 설치된 Windows 가상 시스템은 보안 솔루션이 설치된 ESXi 호스트에서 시작될 때마다 자동으로 보호됩니다. 보호된 가상 시스템은 보안 솔루션이 설치된 다른 ESXi 호스트로 vMotion이 이동한 후에도 종료할 때부터 다시 시작할 때까지 보안 상태를 유지합니다.

- vSphere 6.0을 사용하는 경우 VMware Tools 설치의 경우 **Windows 가상 시스템에서 VMware Tools**를 수동으로 설치 또는 업그레이드를 참조하십시오.

- vSphere 6.5를 사용하는 경우 <https://www.vmware.com/support/pubs/vmware-tools-pubs.html>에서 VMware Tools 설치 지침을 참조하십시오.

사전 요구 사항

게스트 가상 시스템에 지원되는 Windows 버전이 설치되어 있는지 확인하십시오. NSX Guest Introspection에서는 다음 Windows 운영 체제가 지원됩니다.

- Windows XP SP3 이상(32비트)
- Windows Vista(32비트)
- Windows 7(32/64비트)
- Windows 8(32/64비트)
- Windows 8.1(32/64)(vSphere 6.0 이상)
- Windows 10
- Windows 2003 SP2 이상(32/64비트)
- Windows 2003 R2(32/64비트)
- Windows 2008(32/64비트)
- Windows 2008 R2(64비트)
- Win2012(64)
- Win2012 R2(64)(vSphere 6.0 이상)
- Windows Server 2016
- Windows Server 2019

절차

- 1 VMware Tools 설치를 시작하고 사용 중인 vSphere 버전의 지침을 따릅니다. **사용자 지정 설치**를 선택합니다.
- 2 VMCI 드라이버 섹션을 확장합니다.
사용 가능한 옵션은 VMware Tools 버전에 따라 다릅니다.

3 VM에 설치할 드라이버를 선택합니다.

드라이버	설명
vShield Endpoint 드라이버	파일 자체 검사(vsepflt) 및 네트워크 자체 검사(vnetflt) 드라이버를 설치합니다.
Guest Introspection 드라이버	파일 자체 검사(vsepflt) 및 네트워크 자체 검사(vnetflt) 드라이버를 설치합니다.
NSX 파일 자체 검사 드라이버 및 NSX 네트워크 자체 검사 드라이버	[NSX 파일 자체 검사 드라이버]를 선택하여 vsepflt을 설치합니다. 필요에 따라 [NSX 네트워크 자체 검사 드라이버]를 선택하여 vnetflt(Windows 10 이상에서는 vnetWFP)를 설치합니다. 참고 ID 방화벽 또는 끝점 모니터링 기능을 사용하는 경우에만 [NSX 네트워크 자체 검사 드라이버]를 선택합니다.

4 추가하려는 드라이버 옆의 드롭다운 메뉴에서 [이 기능은 로컬 하드 드라이브에 설치됩니다.]를 선택합니다.

5 절차의 나머지 단계를 수행합니다.

다음에 수행할 작업

Thin Agent가 관리 권한의 fltmc 명령을 사용하여 실행되고 있는지 확인합니다. 출력의 [파일 이름] 옆에는 vsepflt 항목이 있는 Thin Agent가 나열됩니다.

지원되는 소프트웨어

Guest Introspection은 특정 버전의 소프트웨어와 상호 운용 가능합니다.

VMware Tools

VMware Tool 10.3.10 버전이 지원됩니다.

VMware Tools와 NSX-T 간의 상호 운용성을 확인하십시오. [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.

지원되는 OS

- Windows 7
- Windows 8/8.1
- Windows 10
- Windows 2008 Server R2
- Windows 2012 Server R2
- Windows 2016 Server
- CentOS 7.4 GA
- RHEL 7.4 GA
- Ubuntu 16.04.5 LTS(64비트)
- SLES 12 GA

지원되는 호스트

지원되는 ESXi 호스트에 대해서는 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.

Guest Introspection 파트너 관리자 역할을 사용하여 사용자 생성

NSX-T Data Center에서 사용할 수 있는 Guest Introspection 파트너 관리자 역할이 있는 사용자를 할당하십시오.

참고: 보안 문제를 피하려면 Guest Introspection 파트너 관리자 역할에 연결된 사용자가 파트너 서비스를 등록하는 것이 좋습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템** → **사용자** → **역할 할당**을 선택하십시오.
- 3 **추가**를 클릭합니다.
- 4 사용자를 선택하고 이 사용자에게 **GI 파트너 관리자** 역할을 할당합니다.

다음에 수행할 작업

NSX-T Data Center에 서비스를 등록합니다. [NSX-T Data Center에 서비스 등록 항목](#)을 참조하십시오.

NSX-T Data Center에 서비스 등록

타사 보안 서비스를 NSX-T Data Center에 등록합니다.

사전 요구 사항

- 필수 구성 요소가 충족되었는지 확인합니다. [끝점 보호를 구성하기 위한 전제 조건 항목](#)을 참조하십시오.
- vIDM 사용자에게 GI 파트너 관리자 역할이 할당되었는지 확인합니다. 이 역할은 서비스를 NSX-T Data Center에 등록하는 데 사용됩니다.

절차

- 1 GI 파트너 관리자 권한으로 파트너 콘솔에 로그인합니다.
- 2 NSX-T Data Center에 서비스, 벤더 템플릿을 등록하고 파트너 솔루션을 구성합니다. 파트너 설명서를 참조하십시오.

다음에 수행할 작업

파트너 서비스의 카탈로그를 확인합니다. [파트너 서비스의 카탈로그 보기 항목](#)을 참조하십시오.

파트너 서비스의 카탈로그 보기

[카탈로그] 페이지에는 NSX-T Data Center에 등록된 모든 파트너 및 서비스가 표시됩니다.

사전 요구 사항

- 파트너는 NSX-T Data Center에 서비스를 등록합니다.
- 서비스가 클러스터에 배포됩니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 서비스 배포 > 카탈로그**를 선택합니다.
- 3 서비스에서 **보기**를 클릭합니다. [배포] 페이지에는 배포의 상태, 네트워크 세부 정보, 클러스터 세부 정보 등과 같은 서비스에 대한 세부 정보가 표시됩니다.

다음에 수행할 작업

파트너 서비스 VM을 업그레이드합니다.

서비스 배포

서비스를 등록한 후 서비스가 네트워크 트래픽 처리를 시작하려면 서비스의 인스턴스를 배포해야 합니다. 클러스터의 모든 NSX-T Data Center 호스트에서 파트너 보안 엔진을 실행하는 파트너 서비스 VM을 배포합니다. vSphere EAM(ESX Agency Manager) 서비스는 각 호스트에 파트너 서비스 VM을 배포하는 데 사용됩니다. SVM을 배포한 후 게스트 VM을 보호하기 위해 SVM에 사용되는 정책 규칙을 생성할 수 있습니다.

사전 요구 사항

- 모든 호스트가 vCenter Server에서 관리됩니다.
- 파트너 서비스가 NSX-T Data Center에 등록되었고 배포할 수 있습니다.
- NSX-T Data Center 관리자가 파트너 서비스 및 벤더 템플릿에 액세스할 수 있습니다.
- 서비스 VM과 파트너 Service Manager(콘솔)가 관리 네트워크 수준에서 서로 통신할 수 있어야 합니다.
- 호스트를 NSX-T Data Center 전송 노드로 준비합니다.
 - 전송 영역을 생성합니다.
 - 터널 끝점 IP 주소에 대한 IP 풀을 생성합니다.
 - 업링크 프로파일을 생성합니다.
 - 전송 노드 프로파일을 추가하여 NSX-T Data Center 전송 노드의 자동 배포를 위한 클러스터를 준비합니다.
 - 독립형 또는 관리 호스트를 구성합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템** 탭으로 이동하고 **서비스 배포**를 클릭합니다.
- 3 [파트너 서비스] 드롭다운에서 배포할 서비스를 선택합니다.
- 4 **배포**를 클릭하고 **서비스 배포**를 클릭합니다.
- 5 서비스 배포 이름을 입력합니다.
- 6 [계산 관리자] 필드에서 서비스를 배포하기 위한 vCenter Server의 계산 리소스를 선택합니다.
- 7 [클러스터] 필드에서 서비스를 배포해야 하는 클러스터를 선택합니다.
- 8 [데이터스토어] 드롭다운 메뉴에서 다음을 수행할 수 있습니다.
 - a 서비스 가상 시스템을 위한 저장소로 사용할 데이터스토어를 선택합니다.
 - b **호스트에 지정됨**을 선택합니다. 이 설정은 이 마법사에서 데이터스토어 및 포트 그룹을 선택하지 않아도 됨을 의미합니다. 서비스 배포에 사용할 특정 데이터스토어 및 포트 그룹을 가리키도록 직접 vCenter Server의 EAM에서 에이전트 설정을 구성할 수 있습니다.

EAM 구성 방법을 확인하려면 vSphere 설명서를 참조하십시오.
- 9 [네트워크] 열에서 **설정**을 클릭합니다.
- 10 관리 네트워크 인터페이스를 **호스트에 지정됨** 또는 **DVPG**로 설정합니다.
- 11 네트워크 유형을 DHCP 또는 정적 IP 풀로 설정합니다. 네트워크 유형을 정적 IP 풀로 설정하는 경우 사용 가능한 IP 풀 목록에서 선택합니다.
- 12 [배포 규격] 필드에서 호스트 기반 배포를 선택하여 모든 호스트에 서비스를 배포합니다. 파트너가 등록한 서비스에 따라, 여러 서비스를 단일 서비스 VM의 일부로 배포할 수 있습니다.
- 13 [배포 템플릿] 필드에서 등록된 배포 템플릿을 선택합니다.
- 14 **저장**을 클릭합니다.

결과

새 호스트가 클러스터에 추가되면 EAM이 새 호스트에 자동으로 서비스 VM을 배포합니다. 벤더의 구현에 따라 배포 프로세스에 시간이 다소 걸릴 수 있습니다. NSX Manager 사용자 인터페이스에서 상태를 볼 수 있습니다. 상태가 배포 성공으로 바뀌지면 서비스가 호스트에 성공적으로 배포됩니다.

클러스터에서 호스트를 제거하려면 먼저 유지 보수 모드로 전환합니다. 그런 다음 게스트 VM을 다른 호스트로 마이그레이션하는 옵션을 선택하여 마이그레이션을 완료합니다.

다음에 수행할 작업

호스트에 배포된 서비스 인스턴스에 대한 상태 및 배포 세부 정보를 확인합니다. 서비스 인스턴스 세부 정보 보기의 내용을 참조하십시오.

서비스 인스턴스 세부 정보 보기

클러스터의 멤버 호스트에 배포된 서비스 인스턴스의 상태 및 배포 세부 정보를 확인합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 서비스 배포 > 서비스 인스턴스**를 선택합니다.
- 3 파트너 서비스 드롭다운 메뉴에서 서비스 인스턴스와 관련된 세부 정보를 볼 파트너 서비스를 선택합니다.

표 10-9.

필드	설명
서비스 인스턴스 이름	특정 호스트에서 서비스 인스턴스를 식별하는 고유한 ID입니다.
서비스 배포 이름	서비스를 배포할 때 입력한 이름입니다.
배포 위치	호스트 IP 주소 또는 FQDN
배포 모드	클러스터 또는 독립형
배포 상태	성공적인 배포를 확인하기 위한 실행 중 상태
상태	<p>서비스 인스턴스가 배포되면 상태는 준비가 됩니다. 상태를 준비에서 실행 중으로 전환하려면 필요한 구성 변경을 수행해야 합니다. 서비스 인스턴스 가져오기 항목을 참조하십시오.</p> <p>다음 매개 변수가 NSX-T Data Center에서 성공적으로 인식되면 상태는 준비에서 실행 중으로 변경됩니다.</p> <ul style="list-style-type: none"> ■ 솔루션 상태: 실행 중 ■ NSX-T Data Center Guest Introspection 에이전트와 NSX-T Data Center Ops 에이전트 간 연결: 실행 중 ■ 상태 수신 시간: <Day, Date, Time>

다음에 수행할 작업

서비스 인스턴스를 가져옵니다. [서비스 인스턴스 가져오기](#) 항목을 참조하십시오.

서비스 인스턴스 가져오기

서비스 인스턴스를 배포한 후에는 상태를 실행 중으로 전환하기 위해 NSX-T Data Center에서 특정 매개 변수를 구현해야 합니다.

절차

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

- 2 **시스템 > 서비스 배포 > 서비스 인스턴스**를 선택합니다.
- 3 파트너 서비스 드롭다운 메뉴에서 서비스 인스턴스와 관련된 세부 정보를 볼 파트너 서비스를 선택합니다.
- 4 [상태] 열에 서비스 인스턴스의 상태가 준비로 표시됩니다. 이것은 VM을 보호하기 위해 서비스 인스턴스를 끝점 보호 정책 규칙으로 구성할 준비가 되었음을 나타냅니다.
- 5 상태를 실행 중으로 변경하려면 NSX-T Data Center에서 다음 매개 변수를 구현해야 합니다.
 - 호스트에서 게스트 가상 시스템을 사용할 수 있어야 합니다.
 - 게스트 가상 시스템의 전원을 켜야 합니다.
 - 끝점 보호 규칙을 게스트 가상 시스템에 적용해야 합니다.
 - 게스트 가상 시스템은 지원되는 VMtools 및 파일 검사 드라이버 버전으로 구성되어야 합니다.

다음에 수행할 작업

서비스 프로파일을 추가합니다. **서비스 프로파일 추가** 항목을 참조하십시오.

서비스 프로파일 추가

Guest Introspection 정책은 NSX-T Data Center에서 서비스 프로파일을 사용할 수 있는 경우에만 구현될 수 있습니다. 서비스 프로파일은 파트너가 제공한 템플릿에서 생성됩니다. 서비스 프로파일은 관리자가 벤더가 제공한 벤더 템플릿을 선택하여 VM에 대한 보호 수준(Gold, Silver, Platinum 정책)을 선택하는 방식입니다.

예를 들어 벤더는 Gold, Platinum 및 Silver 정책 수준을 제공할 수 있습니다. 생성된 각 프로파일은 다른 유형의 워크로드를 서비스할 수 있습니다. Gold 서비스 프로파일은 PCI 유형 워크로드에 완전한 멀웨어 차단 제공하고 Silver 서비스 프로파일은 일반 워크로드에 기본 멀웨어 차단 보호만 제공합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **보안 > 끝점 보호 > 끝점 보호 규칙 > 서비스 프로파일**를 선택합니다.
- 3 [파트너 서비스] 필드에서 서비스 프로파일을 생성할 서비스를 선택합니다.
- 4 **서비스 프로파일 추가**를 클릭합니다.
- 5 서비스 프로파일 이름을 입력하고 벤더 템플릿을 선택합니다. 필요한 경우 설명 및 태그를 추가합니다.
- 6 **저장**을 클릭합니다.

서비스 프로파일을 생성하는 데 사용되는 벤더 템플릿 ID가 파트너 콘솔에 전달됩니다. 파트너는 벤더 템플릿 ID를 저장하여 이러한 벤더 템플릿에서 보호되는 게스트 VM의 사용량을 추적합니다.

결과

서비스 프로파일을 생성한 후 NSX 관리자는 정책 규칙을 게시하기 전에 서비스 프로파일을 VM 그룹에 연결하기 위한 규칙을 생성합니다.

다음에 수행할 작업

멀웨어로부터 보호해야 할 게스트 VM 그룹에 끝점 보호 정책을 적용합니다. [Guest Introspection](#) 정책 사용 항목을 참조하십시오.

Guest Introspection 정책 사용

서비스 프로파일을 VM 그룹과 연결하는 규칙을 생성하여 정책을 VM 그룹에 적용할 수 있습니다. 보호는 규칙이 VM 그룹에 적용된 직후 시작됩니다.

끝점 보호 정책은 게스트 VM에 서비스 프로파일을 구현하여 멀웨어로부터 게스트 VM을 보호하기 위해 파트너가 제공하는 보호 서비스입니다. VM 그룹에 적용되는 규칙을 사용하여 해당 그룹 내의 모든 게스트 VM은 해당 서비스 프로파일을 통해 보호됩니다. 게스트 VM에서 파일 액세스 이벤트가 발생하면 GI Thin Agent(각 게스트 VM에서 실행)는 파일의 컨텍스트(파일 특성, 파일 핸들 및 기타 컨텍스트 세부 정보)를 수집하고 이벤트를 SVM에 알립니다. SVM이 파일 콘텐츠를 검색하려는 경우 EPsec API 라이브러리를 사용하여 세부 정보를 요청합니다. SVM에서 정리를 결정하면 사용자가 GI Thin Agent를 사용하여 파일에 액세스할 수 있습니다. SVM이 파일을 감염됨으로 보고하는 경우 GI Thin Agent가 파일에 대한 사용자 액세스를 거부합니다.

VM 그룹에서 보안 서비스를 실행하려면 다음을 수행해야 합니다.

절차

- 1 정책 및 규칙을 정의합니다.
- 2 VM 그룹을 구성하기 위한 멤버 자격 조건을 정의합니다.
- 3 VM 그룹에 대한 규칙을 정의합니다.
- 4 규칙을 게시합니다.

끝점 보호 규칙 추가 및 게시

VM 그룹에 정책 규칙을 게시하면 보호해야 하는 VM 그룹이 특정 서비스 프로파일과 연결됩니다.

절차

- 1 정책 섹션에서 정책을 선택합니다.
- 2 **추가 -> 규칙 추가**를 클릭합니다.
- 3 새 규칙에 규칙 이름을 입력합니다.
- 4 [그룹 선택] 필드에서 [편집] 아이콘을 클릭합니다.

- 5 [그룹 설정] 창에서 기존 그룹 목록에서 선택하거나 새 그룹을 추가합니다.
 - a 새 그룹을 추가하려면 **그룹 추가**를 클릭하고 세부 정보를 입력한 후 **저장**을 클릭합니다.
 그룹 추가 항목을 참조하십시오.
- 6 [그룹] 열에서 VM 그룹을 선택합니다.
- 7 [서비스 프로파일] 열에서 그룹의 게스트 VM에 원하는 보호 수준을 제공하는 서비스 프로파일을 선택합니다.
 - a 새 서비스 프로파일을 추가하려면 **서비스 프로파일 추가**를 클릭하고 세부 정보를 입력한 후 **저장**을 클릭합니다.
 서비스 프로파일 추가 항목을 참조하십시오.
- 8 **게시**를 클릭합니다.

결과

끝점 보호 정책은 VM 그룹을 보호합니다.

다음에 수행할 작업

다른 VM 그룹에 필요한 보호 유형에 따라 규칙 순서를 변경할 수도 있습니다. **Guest Introspection**이 끝점 보호 정책을 실행하는 방식 항목을 참조하십시오.

끝점 보호 상태 모니터링

보호 및 비보호 VM의 구성 상태, 호스트 에이전트 및 서비스 VM의 문제, VMtools 설치의 일부로 설치된 파일 자체 검사 드라이버로 구성된 VM을 모니터링합니다.

다음을 확인할 수 있습니다.

- 서비스 배포 상태를 봅니다.
- 끝점 보호의 구성 상태를 봅니다.
- 끝점 보호용으로 설정된 용량 상태를 봅니다.

서비스 배포 상태 보기

모니터링 대시보드에서 서비스 배포 세부 정보를 봅니다.

EPP 정책의 시스템 전체 상태를 봅니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **홈 > 모니터링 - 대시보드**로 이동합니다.
- 3 드롭다운 메뉴에서 **모니터링 - 시스템**을 클릭합니다.

- 4 시스템의 클러스터 간 배포 상태를 보려면 [끝점 보호] 위젯으로 이동한 후 도넛형 차트를 클릭하여 성공 또는 실패한 배포를 확인합니다.

[서비스 배포] 페이지에는 배포 세부 정보가 표시됩니다.

끝점 보호의 구성 상태 보기

끝점 보호 서비스의 구성 상태를 봅니다.

EPP 정책의 시스템 전체 상태를 봅니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **홈 > 보안 > 보안 개요**로 이동합니다.
- 3 클러스터에서 EPP 상태를 보려면 [보안] 위젯을 클릭합니다.
- 4 [보안 개요] 페이지에서 **구성**를 클릭합니다.



- 5 [끝점 보호] 섹션에서 다음을 확인합니다.

a [서비스 프로파일에 따라 VM 배포] 위젯에 다음이 표시됩니다.

- 1 상위 프로파일로 보호되는 VM의 수. 상위 프로파일은 클러스터의 최대 VM 수를 보호하는 프로파일을 나타냅니다.
- 2 [기타 프로파일]로 분류된 나머지 서비스 프로파일로 보호되는 VM.
- 3 [프로파일 없음]으로 분류된 보호되지 않는 VM.

[끝점 보호 규칙] 페이지에는 끝점 보호 정책으로 보호되는 VM이 표시됩니다.

b [문제가 있는 구성 요소] 위젯에 다음이 표시됩니다.

- 1 호스트: 컨텍스트 멀티플렉서와 관련된 문제입니다.
- 2 SVM: 서비스 VM과 관련된 문제입니다. 예를 들어, SVM 상태가 종료인 경우 게스트 VM과의 SVM 연결이 종료됩니다.

[배포] 페이지의 [상태] 열에는 상태 문제가 표시됩니다.

c [파일 자체 검사를 실행하여 VM 구성] 위젯에 다음이 표시됩니다.

- 1 파일 자체 검사 드라이버로 보호되는 VM.
- 2 파일 자체 검사 드라이버를 알 수 없는 경우의 VM.

ESXi Agency Manager(EAM)는 호스트, SVM 및 구성 오류와 관련된 몇 가지 문제를 해결하려고 시도합니다. [파트너 서비스 문제 해결](#) 항목을 참조하십시오.

끝점 보호용으로 설정된 용량 상태 보기

끝점 보호 서비스의 용량 상태를 봅니다.

EPP 정책의 용량 상태를 봅니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **홈 > 모니터링 - 대시보드**로 이동합니다.
- 3 드롭다운 메뉴에서 **모니터링 - 네트워킹 및 보안**을 클릭합니다.
- 4 클러스터에서 EPP 상태를 보려면 [보안] 위젯을 클릭합니다.
- 5 [보안 개요] 페이지에서 **용량**을 클릭하고 이러한 매개 변수의 용량 상태를 확인합니다.

제한	최대 용량	현재 인벤토리(인식됨)	주의 경고	위험 경고
분산 방화벽 규칙	100,000	2	0%	70% 100%
시스템 전체 방화벽 액션	10,000	5	0.05%	70% 100%

- a **시스템 전체 끝점 보호 사용 호스트:** 보호된 호스트 수가 임계값 제한에 도달하면 NSX Manager는 해당 임계값 제한에 도달할 때 주의 경고 또는 위험 경고를 알립니다.
- b **시스템 전체 끝점 보호 사용 가상 시스템:** 보호된 가상 시스템의 수가 임계값 제한에 도달하면 NSX Manager는 해당 임계값 제한에 도달할 때 주의 경고 또는 위험 경고를 알립니다.

참고 이러한 매개 변수에 대해 임계값 제한을 설정하고 이러한 매개 변수가 설정된 임계값 제한에 도달하면 상태를 보고 경고를 수신할 수 있습니다.

끝점 보호 관리

정책 충돌, 서비스 VM의 상태 문제를 해결하고 끝점 보호 정책의 작동 방식을 확인합니다.

파트너 서비스 문제 해결

파트너 서비스 가상 시스템이 작동하지 않으면 게스트 VM이 멀웨어로부터 보호되지 않습니다.

각 호스트에서 다음 서비스 또는 프로세스가 작동 및 실행 중인지 확인합니다.

- EAM(ESXi Agency Manager) 서비스가 작동 및 실행 중이어야 합니다. 다음 URL에 액세스할 수 있어야 합니다.

```
https://<vCenter_Server_IP_Address>/eam/mob
```

ESXi Agency Manager가 온라인 상태인지 확인합니다.

```
root> service-control --status vmware-eam
```

- SVM이 게스트 VM을 계속 보호하는 데 필요하므로 SVM의 포트 그룹을 삭제하면 안 됩니다.

```
https://<vCenter_Server_IP_Address>/ui
```

- vCenter Server에서 가상 시스템으로 이동하고 **네트워크** 탭을 클릭하고 **vmervice-vshield-pg**가 나열되었는지 확인합니다.
- Context Multiplexer(MUX) 서비스가 작동 및 실행 중입니다. nsx-context-mux VIB가 호스트에서 작동 및 실행 중인지 확인합니다.
- NSX-T Data Center가 파트너 서비스 콘솔과 통신하는 관리 인터페이스가 실행되고 있어야 합니다.
- MUX와 SVM 간 통신을 사용하도록 설정하는 제어 인터페이스가 실행되고 있어야 합니다. MUX를 SVM에 연결하는 포트 그룹을 생성해야 합니다. 파트너 서비스가 작동하려면 이 인터페이스 및 포트 그룹 둘 다 필요합니다.

ESXi Agency Manager 문제

이 테이블에는 NSX Manager 사용자 인터페이스에서 [해결] 버튼을 사용하여 해결할 수 있는 ESXi Agency Manager 문제가 나열됩니다. NSX Manager에 오류 세부 정보를 알립니다.

표 10-10. ESXi Agency Manager 문제

문제	범주	설명	해결 방법
에이전트 OVF에 액세스할 수 없음	VM이 배포되지 않음	에이전트 가상 시스템이 호스트에서 배포되어야 하지만 ESXi Agent Manager가 해당 에이전트에 대한 OVF 패키지에 액세스할 수 없어 에이전트 가상 시스템을 배포할 수 없습니다. 일반적으로 이는 OVF 패키지를 제공하는 웹 서버가 종료되었을 때 발생합니다. 웹 서버는 에이전트를 생성한 솔루션에 대한 내부용으로 사용되는 경우가 많습니다.	ESXi Agency Manager (EAM) 서비스가 OVF 다운로드 작업을 다시 시도합니다. 파트너 관리 콘솔 상태를 확인합니다. 해결 을 클릭합니다.

표 10-10. ESXi Agency Manager 문제 (계속)

호환되지 않는 호스트 버전	VM이 배포되지 않음	에이전트 가상 시스템을 호스트에 배포해야 합니다. 하지만 호환성 문제로 인해 에이전트가 호스트에 배포되지 않았습니다.	호스트 또는 솔루션을 업그레이드하여 에이전트가 호스트와 호환되도록 합니다. SVM의 호환성을 확인합니다. 해결 을 클릭합니다.
불충분한 리소스	VM이 배포되지 않음	에이전트 가상 시스템을 호스트에 배포해야 합니다. 그러나 호스트의 CPU 또는 메모리 리소스가 적기 때문에 ESXi Agency Manager(EAM) 서비스에서 에이전트 가상 시스템을 배포하지 않았습니다.	ESXi Agency Manager(EAM) 서비스가 가상 시스템을 다시 배포하려고 시도합니다. CPU 및 메모리 리소스를 사용할 수 있는지 확인합니다. 호스트를 확인하고 일부 리소스를 확보합니다. 해결 을 클릭합니다.
불충분한 공간	VM이 배포되지 않음	에이전트 가상 시스템을 호스트에 배포해야 합니다. 하지만 호스트의 에이전트 데이터 스토어에 사용 가능한 공간이 부족하기 때문에 에이전트 가상 시스템이 배포되지 않았습니다.	ESXi Agency Manager(EAM) 서비스가 가상 시스템을 다시 배포하려고 시도합니다. 데이터 스토어의 공간을 확보합니다. 해결 을 클릭합니다.
에이전트 VM 네트워크가 없음	VM이 배포되지 않음	에이전트 가상 시스템이 호스트에서 배포되어야 하지만 에이전트 네트워크가 호스트에 구성되어 있지 않아 에이전트를 배포할 수 없습니다.	customAgentVmNetwork에 나열된 네트워크 중 하나를 호스트에 추가합니다. 데이터 스토어를 사용할 수 있게 되면 문제가 자동으로 해결됩니다.
Ovf 잘못된 형식	VM이 배포되지 않음	에이전트 가상 시스템이 호스트에서 프로비저닝되어야 하지만 OVF 패키지가 프로비저닝되지 않아 가상 시스템이 프로비저닝되지 않았습니다. OVF 패키지를 제공하는 솔루션이 업그레이드되거나 패치되어 에이전트 가상 시스템에 대한 유효한 패키지를 제공할 때까지는 프로비저닝이 성공하지 않을 수 있습니다.	ESXi Agency Manager(EAM) 서비스가 SVM을 다시 배포하려고 시도합니다. 파트너 솔루션 설명서를 확인하거나 파트너 솔루션을 업그레이드하여 유효한 OVF 패키지를 가져옵니다. 해결 을 클릭합니다.
에이전트 IP 풀이 누락됨	VM의 전원이 꺼짐	에이전트 가상 시스템의 전원이 켜져야 하지만 에이전트의 가상 시스템 네트워크에 정의된 IP 주소가 없어 에이전트 가상 시스템의 전원이 꺼져 있습니다.	가상 시스템 네트워크에서 IP 주소를 정의합니다. 해결 을 클릭합니다.

표 10-10. ESXi Agency Manager 문제 (계속)

에이전트 VM 데이터스토어가 없음	VM의 전원이 꺼짐	에이전트 가상 시스템이 호스트에서 배포되어야 하지만 에이전트 데이터스토어가 호스트에 구성되어 있지 않아 에이전트를 배포할 수 없습니다.	customAgentVmDatastore 데이터 스토어에 나열된 데이터 스토어 중 하나를 호스트에 추가합니다. 데이터 스토어를 사용할 수 있게 되면 문제가 자동으로 해결됩니다.
사용자 지정 에이전트 VM 네트워크가 없음	에이전트 VM 네트워크가 없음	에이전트 가상 시스템이 호스트에서 배포되어야 하지만 에이전트 네트워크가 호스트에 구성되어 있지 않아 에이전트를 배포할 수 없습니다.	사용자 지정 에이전트 VM 네트워크에 나열된 네트워크 중 하나에 호스트를 추가합니다. 사용자 지정 VM 네트워크를 사용할 수 있게 되면 문제가 자동으로 해결됩니다.
사용자 지정 에이전트 VM 데이터스토어가 없음	에이전트 VM 데이터스토어가 없음	에이전트 가상 시스템이 호스트에서 배포되어야 하지만 에이전트 데이터스토어가 호스트에 구성되어 있지 않아 에이전트를 배포할 수 없습니다.	사용자 지정 에이전트 VM 데이터 스토어에 나열된 데이터 스토어 중 하나에 호스트를 추가합니다. 이 문제는 자동으로 해결됩니다.
분리된 에이전시	에이전시 문제	에이전시를 생성한 솔루션이 더 이상 vCenter Server에 등록되어 있지 않습니다.	vCenter Server에 솔루션을 등록합니다.
분리된 DvFilter 스위치	호스트 문제	dvFilter 스위치가 호스트에 있지만 호스트에서 dvFilter에 종속된 에이전트가 없습니다. 이 문제는 에이전시 구성이 변경되었을 때 호스트의 연결이 끊기는 경우에 발생합니다.	해결을 클릭합니다. ESXi Agency Manager(EAM) 서비스에서 에이전시 구성이 업데이트되기 전에 호스트에 연결하려고 합니다.
알 수 없는 에이전트 VM	호스트 문제	에이전트 가상 시스템이 이 vSphere ESX Agent Manager 서버 인스턴스의 에이전시에 속하지 않은 vCenter Server 인벤토리에서 발견되었습니다.	해결을 클릭합니다. ESXi Agency Manager(EAM) 서비스에서 가상 시스템을 자신이 속한 인벤토리에 배치하려고 시도합니다.
Ovf 잘못된 속성	VM 문제	에이전트 가상 시스템의 전원이 켜져야 하지만 OVF 속성이 누락되어 있거나 유효한 값이 아닙니다.	해결을 클릭합니다. ESXi Agency Manager(EAM) 서비스가 올바른 OVF 속성을 다시 구성하려고 시도합니다.
VM이 손상됨	VM 문제	에이전트 가상 시스템이 손상되었습니다.	해결을 클릭합니다. ESXi Agency Manager(EAM) 서비스가 가상 시스템을 복구하려고 시도합니다.

표 10-10. ESXi Agency Manager 문제 (계속)

VM이 분리됨	VM 문제	에이전트 가상 시스템이 호스트에 있지만 호스트가 더 이상 에이전시에 대한 범위의 일부가 아닙니다. 이 문제는 에이전시 구성이 변경되었을 때 호스트의 연결이 끊기는 경우에 발생합니다.	해결 을 클릭합니다. ESXi Agency Manager(EAM) 서비스가 호스트를 에이전트 구성으로 다시 연결하려고 시도합니다.
VM이 배포됨	VM 문제	에이전트 가상 시스템이 호스트에서 제거되어야 하지만 에이전트 가상 시스템이 제거되지 않았습니다. vSphere ESX Agent Manager가 에이전트 가상 시스템을 제거할 수 없는 구체적인 이유는 호스트가 유지 보수 모드이거나 전원이 꺼져 있거나 대기 모드이기 때문입니다.	해결 을 클릭합니다. ESXi Agency Manager(EAM) 서비스가 호스트에서 에이전트 가상 시스템을 제거하려고 시도합니다.
VM의 전원이 꺼짐	VM 문제	에이전트 가상 시스템의 전원이 켜져야 하지만 에이전트 가상 시스템의 전원이 꺼져 있습니다.	해결 을 클릭합니다. ESXi Agency Manager(EAM) 서비스가 가상 시스템의 전원을 켜려고 시도합니다.
VM의 전원이 켜짐	VM 문제	에이전트 가상 시스템의 전원이 꺼져야 하지만 에이전트 가상 시스템의 전원이 켜져 있습니다.	해결 을 클릭합니다. ESXi Agency Manager(EAM) 서비스가 가상 시스템의 전원을 끄려고 시도합니다.
VM이 일시 중단됨	VM 문제	에이전트 가상 시스템의 전원이 켜져야 하지만 에이전트 가상 시스템이 일시 중단되었습니다.	해결 을 클릭합니다. ESXi Agency Manager(EAM) 서비스가 가상 시스템의 전원을 켜려고 시도합니다.
VM 잘못된 폴더	VM 문제	에이전트 가상 시스템이 지정된 에이전트 가상 시스템 폴더에 있어야 하지만 다른 폴더에서 발견되었습니다.	해결 을 클릭합니다. ESXi Agency Manager(EAM) 서비스가 지정된 폴더에 에이전트 가상 시스템을 배치하려고 시도합니다.

표 10-10. ESXi Agency Manager 문제 (계속)

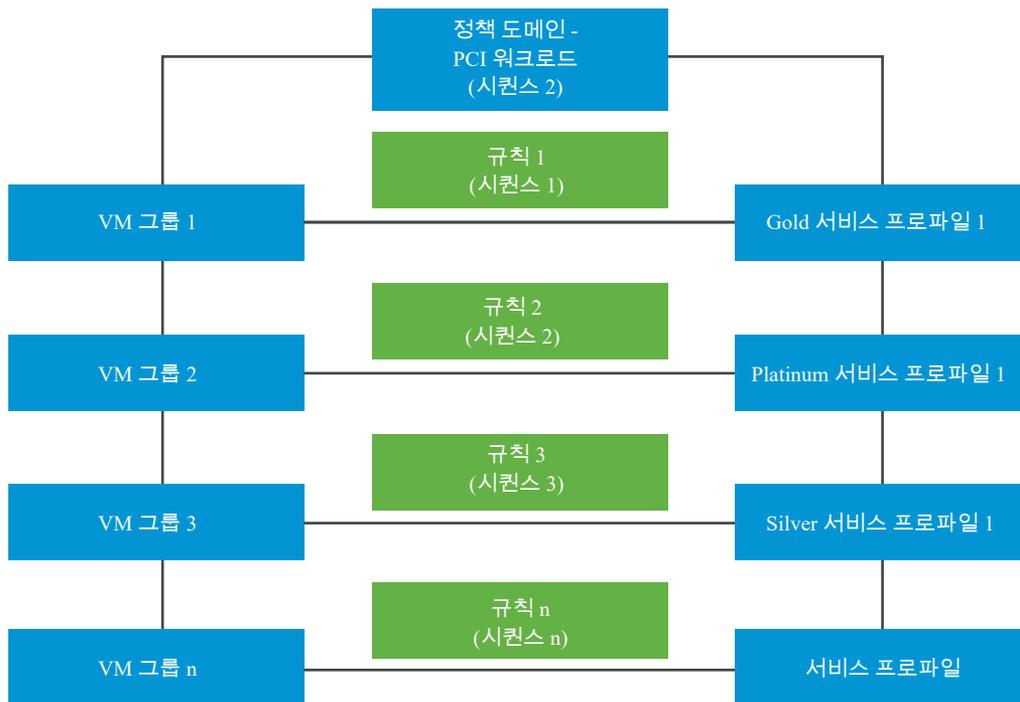
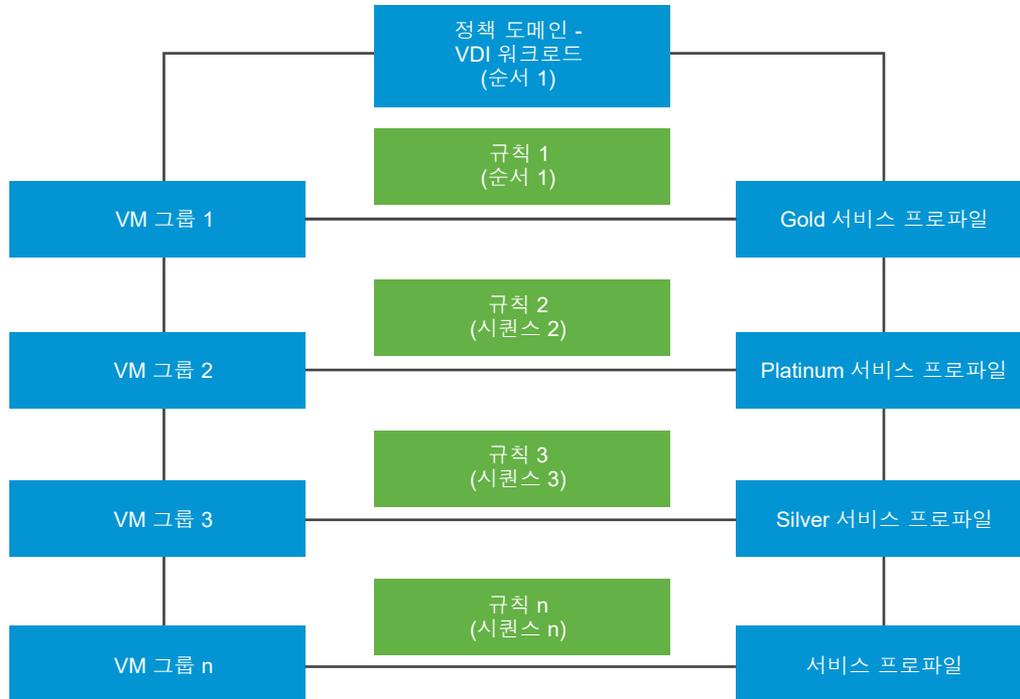
VM 잘못된 리소스 풀	VM 문제	에이전트 가상 시스템이 지정된 에이전트 가상 시스템 리소스 풀에 있어야 하지만 다른 리소스 풀에서 발견되었습니다.	해결 을 클릭합니다. ESXi Agency Manager(EAM) 서비스가 지정된 리소스 풀에 에이전트 가상 시스템을 배치하려고 시도합니다.
VM이 배포되지 않음	에이전트 문제	에이전트 가상 시스템이 호스트에서 배포되어야 하지만 에이전트 가상 시스템이 배포되지 않았습니다. ESXi Agent Manager가 에이전트를 배포할 수 없는 구체적인 이유는 에이전트에 대한 OVF 패키지에 액세스할 수 없거나 호스트 구성이 누락되었기 때문입니다. 이 문제는 에이전트 가상 시스템이 호스트에서 명시적으로 삭제된 경우에도 발생할 수 있습니다.	에이전트 가상 시스템을 배포하려면 해결 을 클릭합니다.

다음으로, VM 그룹에 대한 끝점 보호를 구성합니다. 끝점 보호의 내용을 참조하십시오.

Guest Introspection이 끝점 보호 정책을 실행하는 방식

끝점 보호 정책은 특정 순서대로 적용됩니다. 정책을 설계할 때 규칙을 호스팅하는 도메인 및 규칙에 연결된 순서 번호를 고려합니다.

시나리오: 조직에서 실행하는 수많은 워크로드 중에서 설명 목적으로 두 가지 종류의 워크로드, VDI(Virtual Desktop Infrastructure) 워크로드를 실행 중인 VM, PCI-DSS(Payments Cards Industry Data Security Standards) 워크로드를 실행 중인 VM을 고려합니다. 조직의 직원 섹션에는 VDI(Virtual Desktop Infrastructure) 워크로드를 구성하는 원격 데스크톱 액세스가 필요합니다. 이러한 VDI 워크로드에는 조직이 설정한 규정 준수 규칙을 기반으로 하는 Gold 보호 정책 수준이 필요할 수 있습니다. 이에 비해 PCI-DSS 워크로드에는 최고 수준의 보호인 Platinum 수준 보호가 필요합니다.



2개의 워크로드 유형이 있기 때문에 각각 VDI 워크로드와 서버 워크로드에 대한 2개의 정책을 생성합니다. 각 정책 또는 섹션 내에서 워크로드 유형을 반영하기 위한 도메인을 정의하고 해당 섹션 내에서 해당 워크로드에 대한 규칙을 정의합니다. 게스트 VM에서 GI 서비스를 시작하기 위한 규칙을 게시합니다. GI는 내부적으로 2개의 순서 번호, 정책 순서 번호와 규칙 순서 번호를 사용합니다. 이러한 번호는 실행할 규칙의 전체 순서를 결정하는 데 사용됩니다. 각 규칙은 2개의 용도로 사용됩니다. 즉, 보호할 VM과 VM을 보호하기 위해 적용해야 하는 보호 정책을 결정하는 데 사용됩니다.

순서를 변경하려면 NSX-T Policy Manager UI에서 규칙을 끌어 해당 순서를 변경합니다. 또는 API를 사용하여 규칙에 대한 순서 번호를 명시적으로 할당할 수 있습니다.

또는 NSX-T Data Center API 호출을 수행하여 서비스 프로파일을 VM 그룹과 연결하여 수동으로 규칙을 정의하고 해당 규칙의 순서 번호를 선언합니다. API 및 매개 변수 세부 정보는 NSX-T Data Center "API 가이드"에 자세히 나와 있습니다. 서비스 구성 API 호출을 수행하여 프로파일을 VM 그룹 등과 같은 엔티티에 적용합니다.

표 10-11. 서비스 프로파일을 VM 그룹에 적용하는 규칙을 정의하는 데 사용되는 NSX-T Data Center API

API	세부 정보
모든 서비스 구성 세부 정보를 가져옵니다.	<pre>GET /api/v1/service-configs</pre> <p>서비스 구성 API가 VM 그룹에 적용된 서비스 프로파일, 보호되는 VM 그룹, 규칙의 우선 순위를 결정하는 순서 또는 우선 순위 번호의 세부 정보를 반환합니다.</p>
서비스 구성을 생성합니다.	<pre>POST /api/v1/service-configs</pre> <p>서비스 구성 API가 서비스 프로파일, 보호할 VM 그룹, 규칙에 적용해야 하는 순서 또는 우선 순위 번호의 입력 매개 변수를 가져옵니다.</p>
서비스 구성을 삭제합니다.	<pre>DELETE /api/v1/service-configs/ <config-set-id></pre> <p>서비스 구성 API가 VM 그룹에 적용된 구성을 삭제합니다.</p>
특정 구성의 세부 정보를 가져옵니다.	<pre>GET /api/v1/service-configs/ <config-set-id></pre> <p>특정 구성의 세부 정보를 가져옵니다.</p>
서비스 구성을 업데이트합니다.	<pre>PUT /api/v1/service-configs/ <config-set-id></pre> <p>서비스 구성을 업데이트합니다.</p>
유효한 프로파일을 가져옵니다.	<pre>GET /api/v1/service-configs/ effective-profiles?resource_id=<resource-id> &resource_type=<resource-type></pre> <p>서비스 구성 API가 특정 VM 그룹에 적용된 해당 프로파일만 반환합니다.</p>

이러한 권장 사항에 따라 규칙을 효율적으로 관리합니다.

- 규칙을 먼저 실행해야 하는 정책에 대해 더 높은 순서 번호를 설정합니다. UI에서 정책을 끌어 우선 순위를 변경할 수 있습니다.
- 마찬가지로 각 정책 내의 규칙에 대해 더 높은 순서 번호를 설정합니다.
- 필요한 규칙 수에 따라 2, 3, 4 또는 심지어 10의 배수로 떨어져 규칙을 배치할 수 있습니다. 따라서 10 자리 떨어진 2개의 연속 규칙을 사용하여 모든 규칙의 순서를 변경하지 않고도 보다 유연하게 순서를 재지정할 수 있습니다. 예를 들어 많은 규칙을 정의하지 않으려는 경우 10자리 떨어져 규칙을 배치하도록 선택할 수 있습니다. 따라서 규칙 1은 1의 순서 번호를 가져오고, 규칙 2는 10의 순서 번호를 가져오고, 규칙 3은 20의 순서 번호를 가져오는 등입니다. 이 권장 사항은 유연하고 효율적으로 규칙을 관리하여 모든 규칙의 순서를 재지정하지 않아도 되도록 해 줍니다.

내부적으로 Guest Introspection은 다음과 같은 방식으로 이러한 정책 규칙의 순서를 지정합니다.

```
Policy 1 ↔ Sequence Number 1 (1000)

- Rule 1 : Group 1↔ Service Profile ↔ Sequence Number 1 (1001)
- Rule 2 : Group 1↔ Service Profile ↔ Sequence Number 10 (1010)
- Rule 3 : Group 1↔ Service Profile ↔ Sequence Number 20 (1020)
- Rule 4 : Group 1↔ Service Profile ↔ Sequence Number 30 (1030)

Policy 2 ↔ Sequence Number 2 (2000)

- Rule 1 : Group 1↔ Service Profile ↔ Sequence Number 1 (2001)
- Rule 2 : Group 1↔ Service Profile ↔ Sequence Number 10 (2010)
- Rule 3 : Group 1↔ Service Profile ↔ Sequence Number 20 (2020)
- Rule 4 : Group 1↔ Service Profile ↔ Sequence Number 30 (2030)
```

위의 순서 번호를 기반으로 GI는 정책 2의 규칙을 실행하기 전에 정책 1의 규칙을 실행합니다.

하지만 대상 규칙이 VM 그룹 또는 VM에 적용되지 않는 경우의 상황도 있습니다. 원하는 정책 보호 수준을 적용하려면 이러한 충돌을 해결해야 합니다.

끝점 정책 충돌 해결

각각 여러 규칙으로 구성된 2개의 정책 도메인이 있는 시나리오를 고려합니다. VM은 OS 이름, 컴퓨터 이름, 사용자, 태그 지정과 같은 동적 멤버 자격 조건을 기반으로 그룹에 연결되기 때문에, 결과적으로 어느 VM이 그룹의 멤버 자격을 가지게 되는지를 admin가 항상 확신할 수는 없습니다.

충돌은 다음과 같은 시나리오에서 발생합니다.

- VM이 두 그룹에 속하며 각 그룹이 서로 다른 프로파일에 의해 보호됩니다.

- 파트너 서비스 VM이 2개 이상의 서비스 프로파일과 연결되어 있습니다.
- 예기치 않은 규칙이 게스트 VM에서 실행되었거나 규칙이 VM 그룹에서 실행되지 않습니다.
- 순서 번호가 정책 규칙 또는 도메인에 할당되지 않았습니다.

표 10-12. 정책 충돌 해결

시나리오	예상된 끝점 보호 흐름	해결 방법
<p>VM이 여러 그룹의 멤버 자격을 가지며 각 그룹이 서로 다른 유형의 서비스 프로파일을 통해 보호되는 경우. 예상 보호가 VM에 적용되지 않습니다.</p>	<p>멤버 자격 조건으로 생성된 VM 그룹은 VM이 동적으로 그룹에 추가됨을 의미합니다. 이 경우 동일한 VM이 여러 그룹에 속하게 될 수 있습니다. 멤버 자격 조건이 동적으로 VM을 그룹으로 채우기 때문에 VM이 속하게 되는 그룹을 미리 확인할 수 있는 방법이 없습니다.</p> <p>VM 1이 그룹 1과 그룹 2에 속하는 경우를 고려합니다.</p> <ul style="list-style-type: none"> ■ 규칙 1: 그룹 1(OS 이름별)에 순서 번호 1로 Gold(서비스 프로파일)가 적용됨 ■ 규칙 2: 그룹 2(태그별)에 순서 번호 10으로 Platinum이 적용됨 <p>끝점 보호 정책이 VM 1에서 Gold 서비스 프로파일을 실행하지만 VM1에서 Platinum 서비스 프로파일을 실행하지 않습니다.</p>	<p>규칙 1 앞에 실행되도록 규칙 2의 순서 번호를 변경합니다.</p> <ul style="list-style-type: none"> ■ NSX-T Policy Manager UI에서 규칙 목록에서 규칙 1 앞에 규칙 2를 끌어옵니다. ■ NSX-T Policy Manager API를 사용하여 수동으로 규칙 2에 더 높은 순서 번호를 추가합니다.
<p>규칙이 동일한 서비스 프로파일을 연결하여 두 VM 그룹을 보호하는 경우. 끝점 보호가 두 번째 VM 그룹에서 규칙을 실행하지 않습니다.</p>	<p>동일한 서비스 프로파일을 정책 또는 도메인 전체의 기타 규칙에 다시 적용할 수 없기 때문에 끝점 보호가 VM에서 첫 번째 서비스 프로파일만 실행합니다.</p> <p>VM 1이 그룹 1과 그룹 2에 속하는 경우를 고려합니다.</p> <p>규칙 1: 그룹 1(OS 이름별)에 Gold(서비스 프로파일)가 적용됨</p> <p>규칙 2: 그룹 2(태그별)에 Gold(서비스 프로파일)가 적용됨</p>	<ul style="list-style-type: none"> ■ 그룹 2를 규칙 1에 추가합니다. (규칙 1: 그룹 1, 그룹 2에 프로파일 1이 적용됨)

VM 격리

규칙이 파트너가 설정한 보호 수준 및 태그를 기반으로 VM 그룹에 적용된 후, 감염된 것으로 식별되어 격리가 필요한 VM이 있을 수 있습니다.

파트너는 virus_found=true 태그와 API를 사용하여 감염된 VM에 태그를 지정합니다. 영향을 받은 VM에는 virus_found=true 태그가 추가됩니다.

관리자는 값이 virus_found=true인 태그를 기반으로 미리 정의된 격리 그룹을 생성하여 감염된 VM에 태그가 지정되는 즉시 이 그룹에 채워지도록 설정할 수 있습니다. admin는 격리 그룹에 대해 특정 방화벽 규칙을 설정하도록 선택할 수 있습니다. 격리 그룹에 대한 방화벽 규칙을 설정할 수 있습니다. 예를 들어 격리 그룹의 모든 송신 및 수신 트래픽을 차단하도록 선택할 수 있습니다.

서비스 인스턴스의 상태 확인

서비스 인스턴스의 상태는 여러 요인에 따라 달라집니다. 파트너 솔루션의 상태, Guest Introspection Agent(컨텍스트 멀티플렉서)와 컨텍스트 엔진(Ops Agent) 간의 연결, Guest Introspection Agent 정보의 가용성, NSX Manager의 SVM 프로토콜 정보

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 서비스 배포 > 서비스 인스턴스**를 선택합니다.
- 3 상태 열에서 ⓘ를 클릭하여 서비스 인스턴스의 상태를 확인합니다.

표 10-13. 타사 서비스 인스턴스의 상태

매개 변수	설명
상태 수신 시간	NSX Manager가 서비스 인스턴스의 상태 세부 정보를 수신한 최신 타임 스탬프입니다.
솔루션 상태	SVM에서 실행되는 파트너 솔루션의 상태입니다. 실행 중 상태는 파트너 솔루션이 올바르게 실행 중임을 나타냅니다.
NSX-T Data Center Guest Introspection Agent와 NSX-T Data Center Ops Agent 간 연결	NSX-T Data Center Guest Introspection Agent(컨텍스트 멀티플렉서)가 Ops에이전트(컨텍스트 엔진 포함)와 연결되면 상태가 실행 중입니다. 컨텍스트 멀티플렉서는 SVM의 상태 정보를 컨텍스트 엔진에 전달합니다. 또한 서로 간에 SVM-VM 구성을 공유하여 어떤 게스트 VM이 SVM에 의해 보호되는지 알 수 있습니다.
서비스 VM 프로토콜 버전	문제 해결을 위해 내부적으로 사용되는 전송 프로토콜 버전입니다.
NSX-T Data Center Guest Introspection Agent 정보	NSX-T Data Center Guest Introspection Agent와 SVM 간의 프로토콜 버전 호환성을 나타냅니다.

- 4 상태가 실행 중(녹색으로 표시된 상태)이고 파트너 콘솔에 모든 게스트 VM이 보호된 것으로 표시되면 서비스 인스턴스의 상태는 실행 중입니다.
- 5 상태가 실행 중(녹색으로 표시된 상태)이지만 파트너 콘솔에 게스트 VM이 보호되지 않은 상태로 표시되면 다음 단계를 수행합니다.
 - a VMware 지원에 문의하여 문제를 해결하십시오. 서비스 인스턴스가 종료 상태가 되고 NSX Manager 사용자 인터페이스에 제대로 반영되지 않을 수 있습니다.

- 6 상태가 종료됨(빨간색으로 표시된 상태)인 경우에는 서비스 인스턴스 상태를 확인하는 하나 이상의 요인이 작동하지 않습니다.

표 10-14. 상태 문제 해결

상태 특성	해결 방법
솔루션 상태는 종료됨 또는 사용할 수 없음입니다.	<ol style="list-style-type: none"> 1 서비스 배포 상태가 실행 중(녹색)인지 확인합니다. 오류가 발생하면 파트너 서비스 문제 해결의 내용을 참조하십시오. 2 영향을 받는 호스트에 있는 하나 이상의 게스트 VM이 끝점 보호 정책으로 보호되는지 확인합니다. 3 파트너 콘솔에서 솔루션 서비스가 호스트의 SVM에서 실행 중인지 확인합니다. 자세한 내용은 파트너 설명서를 참조하십시오. 4 위의 단계를 수행해도 문제가 해결되지 않으면 VMware 지원팀에 문의하십시오.
NSX-T Data Center Guest Introspection Agent와 NSX-T Data Center Ops Agent 간 연결 상태가 종료됨입니다.	<ol style="list-style-type: none"> 1 서비스 배포 상태가 실행 중(녹색)인지 확인합니다. 오류가 발생하면 파트너 서비스 문제 해결의 내용을 참조하십시오. 2 영향을 받는 호스트에 있는 하나 이상의 게스트 VM이 끝점 보호 정책으로 보호되는지 확인합니다. 3 파트너 콘솔에서 솔루션 서비스가 호스트의 SVM에서 실행 중인지 확인합니다. 자세한 내용은 파트너 설명서를 참조하십시오. 4 위의 단계를 수행해도 문제가 해결되지 않으면 VMware 지원팀에 문의하십시오.
서비스 VM 프로토콜 버전이 사용할 수 없음입니다.	<ol style="list-style-type: none"> 1 서비스 배포 상태가 실행 중(녹색)인지 확인합니다. 오류가 발생하면 파트너 서비스 문제 해결의 내용을 참조하십시오. 2 영향을 받는 호스트에 있는 하나 이상의 게스트 VM이 끝점 보호 정책으로 보호되는지 확인합니다. 3 파트너 콘솔에서 솔루션 서비스가 호스트의 SVM에서 실행 중인지 확인합니다. 자세한 내용은 파트너 설명서를 참조하십시오. 4 위의 단계를 수행해도 문제가 해결되지 않으면 VMware 지원팀에 문의하십시오.
NSX-T Data Center Guest Introspection Agent 정보가 사용할 수 없음입니다.	VMware 지원팀에 문의하십시오.

파트너 서비스 삭제

파트너 서비스를 삭제하려면 API 호출을 수행합니다. API 호출을 수행하여 파트너 서비스 또는 호스트에 배포된 SVM을 삭제하기 전에 NSX Manager 사용자 인터페이스에서 다음을 수행해야 합니다.

파트너 서비스를 삭제하려면 다음과 같이 하십시오.

절차

- 1 호스트에서 실행 중인 VM 그룹에 적용된 EPP 규칙을 제거합니다.
- 2 VM 그룹에 적용된 서비스 프로파일 보호를 제거합니다.
- 3 파트너 Service Manager와의 솔루션 바인딩 SVM을 제거하려면 다음 API 호출을 수행합니다.

```
/DEL https://<NSX_Manager_IPAddress>/api/v1/serviceinsertion/services/{{service_id}}/solution-configs/<solution-config-id>
```

- 4 서비스 배포를 삭제하려면 다음 API 호출을 수행합니다.

```
/DEL https://<NSX_Manager_IPAddress>/api/v1/serviceinsertion/services/<service-id>/service-deployments/<service-deployment-id>
```

API 매개 변수에 대한 자세한 내용은 "NSX-T Data Center API 가이드" 를 참조하십시오.

보안 프로파일

이 섹션에는 방화벽 작업을 미세 조정하는 프로파일(세션 타이머, 플러드 보호 및 DNS 보안)이 포함되어 있습니다.

세션 타이머 생성

세션 타이머는 세션에서 비활성 상태가 된 후에 방화벽에서 세션이 유지되는 기간을 정의합니다.

프로토콜에 대한 세션 제한 시간이 만료되면 세션이 닫힙니다. 방화벽에서 사용자 정의 그룹이나 Tier-0 또는 Tier-1 게이트웨이에 TCP, UDP 및 ICMP 세션에 대한 여러 시간 초과를 적용하도록 지정할 수 있습니다. 기본 세션 값은 네트워크 요구에 따라 수정될 수 있습니다. 값을 너무 낮게 설정하면 시간 초과가 너무 자주 발생하고, 값을 너무 높게 설정하면 실패 감지가 지연될 수 있습니다.

절차

- 1 **보안 > 설정 > 보안 프로파일 > 세션 타이머**로 이동합니다.
- 2 **프로파일 추가**를 클릭합니다.
기본값으로 채워진 **프로파일** 화면이 나타납니다.
- 3 타이머 프로파일에 대해 **이름** 및 **설명**(옵션)을 입력합니다.
- 4 **설정**을 클릭하여 타이머 프로파일을 적용할 Tier-0 또는 Tier-1 게이트웨이 또는 그룹을 선택합니다.
- 5 프로토콜을 선택합니다. 기본값을 그대로 적용하거나 자체 값을 입력합니다.

TCP 변수	설명
First Packet	첫 번째 패킷이 전송된 이후 연결에 대한 시간 초과 값입니다. 기본값은 120초입니다.
여는 중	두 번째 패킷이 전송된 이후 연결에 대한 시간 초과 값입니다. 기본값은 30초입니다.
ESTABLISHED	연결이 완전히 설정된 다음 연결에 대한 시간 초과 값입니다.

TCP 변수	설명
CLOSING	첫 번째 핀이 전송된 이후 연결에 대한 시간 초과 값입니다. 기본값은 120초입니다.
FIN WAIT	두 핀이 교환되고 연결이 닫힌 이후 연결에 대한 시간 초과 값입니다. 기본값은 45초입니다.
CLOSED	한 끝점이 RST를 전송한 이후 연결에 대한 시간 초과 값입니다. 기본값은 20초입니다.

UDP 변수	설명
First Packet	첫 번째 패킷이 전송된 이후 연결에 대한 시간 초과 값입니다. 새 UDP 흐름에 대한 초기 시간 초과입니다. 기본값은 60초입니다.
SINGLE	소스 호스트가 둘 이상의 패킷을 전송하고 대상 호스트가 하나를 전송받지 못한 경우 연결에 대한 시간 초과 값입니다. 기본값은 30초입니다.
MULTIPLE	두 호스트가 패킷을 전송한 경우 연결에 대한 시간 초과 값입니다. 기본값은 60초입니다.

ICMP 변수	설명
First Packet	첫 번째 패킷이 전송된 이후 연결에 대한 시간 초과 값입니다. 새 ICMP 흐름에 대한 초기 시간 초과입니다. 기본값은 20초입니다.
오류 응답	ICMP 패킷에 대한 응답으로 ICMP 오류가 반환된 후 연결에 대한 시간 초과 값입니다. 기본값은 10초입니다.

6 저장을 클릭합니다.

다음에 수행할 작업

저장한 후 **그룹-프로파일 우선 순위 관리**를 클릭하여 프로파일 바인딩 우선 순위에 따라 그룹을 관리합니다.

기본 세션 타이머 값

세션 타이머 프로파일은 시간 초과 값을 Tier-0 또는 Tier-1 라우터 인터페이스 또는 세그먼트를 포함하는 그룹에 적용합니다. 시간 초과 값은 세션이 종료된 후에 프로토콜 세션이 활성 상태를 유지하는 기간을 결정합니다.

세션 타이머 값

- API 및 UI와 함께 표시되는 기본 타이머 프로파일은 DFW(분산 방화벽)에만 적용됩니다.
- GFW(게이트웨이 방화벽) 기본 세션 타이머는 API 및 UI를 사용할 때 표시되는 기본 프로파일 타이머와는 다릅니다. GFW 기본 세션 타이머는 북-남 트래픽에 맞게 최적화되어 있으며 기본적으로 더 낮습니다.
- API 및 UI를 사용하여 DFW와 GFW 모두에 대해 FW 세션 타이머를 변경할 수 있습니다.
- 필요한 경우 동일한 비기본 타이머 프로파일을 DFW 및 GFW 둘 다에 적용할 수 있습니다.

타이머 값을 사용자 지정하지 않으면 게이트웨이가 기본값을 사용합니다. 게이트웨이 방화벽 기본 타이머 값:

타이머 속성	Edge 기본값(초)	최소(초)	최대(초)
ICMP 오류 응답	6	10	4320000
ICMP 첫 번째 패킷	6	10	4320000
TCP 닫힘	2	10	4320000
TCP 닫는 중	900	10	4320000
TCP 설정됨	7200	120	4320000
TCP Fin-wait	4	10	4320000
TCP 첫 번째 패킷	120	10	4320000
TCP 여는 중	30	10	4320000
UDP 첫 번째 패킷	30	10	4320000
UDP 다중	30	10	4320000
UDP 단일	30	10	4320000

분산 방화벽 기본 세션 타이머 값:

타이머 속성	DFW 기본값(초)	최소(초)	최대(초)
ICMP 오류 응답	10	10	4320000
ICMP 첫 번째 패킷	20	10	4320000
TCP 닫힘	20	10	4320000
TCP 닫는 중	120	10	4320000
TCP 설정됨	43200	120	4320000
TCP Fin-wait	45	10	4320000
TCP 첫 번째 패킷	120	10	4320000
TCP 여는 중	30	10	4320000
UDP 첫 번째 패킷	60	10	4320000
UDP 다중	60	10	4320000
UDP 단일	30	10	4320000

플러드 보호

플러드 보호는 DDoS(서비스 거부) 공격으로부터 보호하는 데 도움을 줍니다.

DDoS 공격은 사용 가능한 모든 서버 리소스를 소비하여 서버가 요청으로 플러드되도록 하여 합법적인 트래픽에 서버를 사용할 수 없도록 하기 위한 것입니다. 플러드 보호 프로파일을 생성하면 ICMP, UDP 및 절반 개방 TCP 흐름에 대해 활성 세션 제한이 적용됩니다. 분산 방화벽은 SYN_SENT 및 SYN_RECEIVED 상태에 있는 흐름 항목을 캐시하고, 이니시에이터에서 ACK가 수신된 후 각 항목을 TCP 상태로 승격하여 3방향 핸드셰이크를 완료할 수 있습니다.

절차

- 1 **보안 > 보안 프로파일 > 플러드 보호**로 이동합니다.
- 2 **프로파일 추가**를 클릭하고 **Edge 게이트웨이 프로파일 추가** 또는 **방화벽 프로파일 추가**를 선택합니다.
- 3 다음과 같은 플러드 보호 프로파일 매개 변수를 입력합니다.

표 10-15. 방화벽 및 Edge 게이트웨이 프로파일에 대한 매개 변수

매개 변수	최소값 및 최대값	기본값	
TCP 절반 개방 연결 제한 - 방화벽에서 허용하는 완전히 설정되지 않은 활성 TCP 흐름 수를 제한하여 TCP SYN 플러드 공격을 방지합니다.	1-1,000,000	방화벽 - 없음 Edge 게이트웨이 - 1,000,000	이 텍스트 상자를 설정하여 활성 TCP 절반 개방 연결 수를 제한합니다. 이 텍스트 상자가 비어 있는 경우 이 제한은 ESX 노드에서 사용하지 않도록 설정되고 Edge 게이트웨이의 기본값으로 설정됩니다.
UDP 활성 흐름 제한 - 방화벽에서 허용하는 활성 UDP 흐름 수를 제한하여 UDP 플러드 공격을 방지합니다. 설정된 UDP 흐름 제한에 도달하면 새 흐름을 설정할 수 있는 후속 UDP 패킷이 삭제됩니다.	1-1,000,000	방화벽 - 없음 Edge 게이트웨이 - 1,000,000	이 텍스트 상자를 설정하여 활성 UDP 연결 수를 제한합니다. 이 텍스트 상자가 비어 있는 경우 이 제한은 ESX 노드에서 사용하지 않도록 설정되고 Edge 게이트웨이의 기본값으로 설정됩니다.
ICMP 활성 흐름 제한 - 방화벽에서 허용하는 활성 ICMP 흐름 수를 제한하여 ICMP 플러드 공격을 방지합니다. 설정된 흐름 제한에 도달하면 새 흐름을 설정할 수 있는 후속 ICMP 패킷이 삭제됩니다.	1-1,000,000	방화벽 - 없음 Edge 게이트웨이 - 10,000	이 텍스트 상자를 설정하여 활성 ICMP 개방 연결 수를 제한합니다. 이 텍스트 상자가 비어 있는 경우 이 제한은 ESX 노드에서 사용하지 않도록 설정되고 Edge 게이트웨이의 기본값으로 설정됩니다.
기타 활성 연결 제한	1-1,000,000	방화벽 - 없음 Edge 게이트웨이 - 10,000	이 텍스트 상자를 설정하여 ICMP, TCP 및 UDP 절반 개방 연결 이외의 활성 연결 수를 제한합니다. 이 텍스트 상자가 비어 있는 경우 이 제한은 ESX 노드에서 사용하지 않도록 설정되고 Edge 게이트웨이의 기본값으로 설정됩니다.

표 10-15. 방화벽 및 Edge 게이트웨이 프로파일에 대한 매개 변수 (계속)

매개 변수	최소값 및 최대값	기본값	
<p>SYN 캐시 - SYN 캐시는 TCP 절반 개방 연결 제한이 구성된 경우에도 사용됩니 다. 활성 절반 개방 연결 수는 완전히 설정되지 않은 TCP 세션의 syncache를 유지하 여 적용됩니다. 이 캐시는 SYN_SENT 및 SYN_RECEIVED 상태에 있 는 흐름 항목을 유지합니다. 이니시에이터에서 ACK가 수 신된 후에는 각 syncache 항 목이 전체 TCP 상태 항목으 로 승격되고 3방향 핸드셰이 크를 완료합니다.</p>		방화벽 프로파일에만 사용할 수 있습니다.	설정/해제합니다. SYN 캐시 를 사용하도록 설정하는 것 은 TCP 절반 개방 연결 제한 이 구성된 경우에만 유효합 니다.
<p>RST 스푸핑 - SYN 캐시에서 반개방 상태를 제거할 때 서 버에 대해 스푸핑된 RST를 생성합니다. 서버에서 SYN 플러드(반개방)와 연결된 상 태를 정리할 수 있습니다.</p>		방화벽 프로파일에만 사용할 수 있습니다.	설정/해제합니다. 이 옵션을 사용하려면 SYN 캐시를 선 택해야 합니다.

4 프로파일을 Edge 게이트웨이 및 방화벽 그룹에 적용하려면 **설정**을 클릭하십시오.

5 **저장**을 클릭합니다.

다음에 수행할 작업

저장한 후 **그룹-프로파일 우선 순위 관리**를 클릭하여 프로파일 바인딩 우선 순위에 따라 그룹을 관리합니 다.

DNS 보안 구성

DNS 보안 프로파일을 생성하면 DNS 관련 공격으로부터 보호할 수 있습니다.

DNS 보안 프로파일을 설정한 후에는 다음을 수행할 수 있습니다.

- VM에 대한 DNS 응답 또는 FQDN을 IP 주소에 연결하기 위한 전송 노드의 VM 그룹에 대해 스누핑을 수행합니다.
- 글로벌 및 기본 DNS 서버 정보를 추가하고 DFW 규칙을 사용하는 모든 VM에 적용합니다.
- 선택한 VM에 대해 선택된 DNS 서버 정보를 지정합니다.
- 그룹에 DNS 프로파일을 적용합니다.

참고 현재 릴리스에서는 ESXi만 지원됩니다.

절차

- 1 보안 > 설정 > 보안 프로파일 > DNS 보안로 이동합니다.
- 2 프로파일 추가를 클릭합니다.
- 3 다음 값을 입력합니다.

옵션	설명
프로파일 이름	프로파일 이름을 입력하십시오.
TTL	이 필드는 DNS 캐시 항목에 대한 TTL(Time to live)(초)을 캡처합니다. 다음과 같은 옵션이 있습니다. TTL 0 - 캐시된 항목이 만료되지 않습니다. TTL 1 ~ 3599 - 유효하지 않음 TTL 3600 ~ 864000 - 유효함 TTL이 빈 상태임 - DNS 응답 패킷에서 자동 TTL이 설정됩니다. 참고 DNS 보안 프로파일의 기본 DNS 캐시 시간 초과는 24시간입니다.
적용 대상	조건에 따라 DNS 보안 프로파일을 적용할 그룹을 선택할 수 있습니다. 참고 VM에 하나의 DNS 서버 프로파일만 적용됩니다.
태그	선택 사항입니다. 태그 및 범위를 DNS 프로파일에 할당하여 보다 쉽게 검색할 수 있도록 합니다. 자세한 내용은 개체에 태그 추가 항목을 참조하십시오.

- 4 저장을 클릭합니다.

다음에 수행할 작업

저장한 후 그룹-프로파일 우선 순위 관리를 클릭하여 프로파일 바인딩 우선 순위에 따라 그룹을 관리합니다.

그룹-프로파일 우선 순위 관리

여러 그룹을 보안 프로파일에 바인딩할 수 있습니다. NSX-T Data Center는 우선 순위가 가장 높은 그룹에 보안 프로파일을 적용합니다.

보안 프로파일을 여러 그룹에 바인딩하는 경우 NSX-T Data Center가 해당 목록의 최신 그룹에 가장 높은 우선 순위를 할당합니다. 그러나 그룹의 우선 순위 수준은 변경할 수 있습니다.

그룹에 우선 순위를 할당하려면:

사전 요구 사항

- 세션 타이머 그룹에는 세그먼트, 세그먼트 포트 및 VM만 멤버로 포함되어야 합니다. 다른 범주 유형은 지원되지 않습니다.
- DNS 보안 그룹에는 VM만 멤버로 포함되어야 합니다. 다른 범주 유형은 지원되지 않습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **보안 > 보안 프로파일**로 이동합니다.
- 3 **그룹-프로파일 우선 순위 관리**를 클릭합니다.
- 4 그룹에 가장 높은 우선 순위 수준을 할당하려면 해당 그룹을 목록 맨 위로 이동합니다.
- 5 **닫기**를 클릭합니다.

결과

보안 프로파일이 우선 순위가 가장 높은 그룹에 적용됩니다.

NSX-T Data Center 인벤토리에 대한 서비스, 그룹, 컨텍스트 프로파일 및 가상 시스템을 구성할 수 있습니다.

인벤토리 탭을 클릭하면 인벤토리에 있는 그룹, 서비스, 가상 시스템 및 컨텍스트 프로파일의 수를 표시하는 인벤토리 개체 개요가 표시됩니다. 또한 그룹에 대한 다음 정보가 표시됩니다.

- 정책에 사용되는 그룹 수
- 정책에 사용되지 않는 그룹 수
- 멤버가 있는 그룹 수
- 멤버가 없는 그룹 수
- ID 그룹 수
- 정책에 사용되는 ID 그룹 수
- 정책에서 사용되지 않는 ID 그룹 수

본 장은 다음 항목을 포함합니다.

- 서비스 추가
- 그룹 추가
- 컨텍스트 프로파일 추가

서비스 추가

서비스를 구성하고 일치하는 네트워크 트래픽에 대해 포트 및 프로토콜 연결과 같은 매개 변수를 지정할 수 있습니다.

서비스를 사용하여 방화벽 규칙에서 특정 유형의 트래픽을 허용하거나 차단할 수도 있습니다. 서비스를 생성한 후에는 유형을 변경할 수 없습니다. 일부 서비스는 미리 정의되며 수정되거나 삭제될 수 없습니다.

절차

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

- 3 새 서비스 추가를 클릭합니다.
- 4 이름을 입력합니다.
- 5 서비스 항목 설정을 클릭합니다. 새 서비스 항목 추가를 클릭합니다.
- 6 새 서비스에 대해 서비스 유형을 선택하고 추가 속성을 지정합니다.
사용 가능한 유형은 IP, IGMP, ICMPv4, ICMPv6, ALG, TCP, UDP 및 이더넷입니다.
- 7 저장을 클릭합니다.
- 8 (선택 사항) 하나 이상의 태그를 추가합니다.
- 9 (선택 사항) 설명을 입력합니다.
- 10 저장을 클릭합니다.

그룹 추가

그룹은 정적으로 추가되고 동적으로 추가된 다른 개체를 포함하며 방화벽 규칙의 소스 및 대상으로 사용될 수 있습니다.

그룹은 가상 시스템, IP 집합, MAC 집합, 세그먼트 포트, 세그먼트, AD 사용자 그룹 및 기타 그룹의 조합을 포함하도록 구성할 수 있습니다. 그룹의 동적 포함은 태그, 시스템 이름, OS 이름 또는 컴퓨터 이름을 기반으로 할 수 있습니다. 동적 또는 논리적 개체를 기준으로 하는 그룹은 분산 방화벽 규칙의 적용 대상 필드에서 사용할 수 없습니다.

NSX의 태그는 대/소문자를 구분하지만 태그를 기준으로 하는 그룹은 "대/소문자를 구분하지 않습니다". 예를 들어 동적 그룹 멤버 자격 조건이 VM Tag Equals 'quarantine'이면 그룹에는 'quarantine' 또는 'QUARANTINE' 태그 중 하나가 포함된 모든 VM이 포함됩니다.

그룹을 방화벽 규칙에서 제외할 수도 있으며, 목록에는 최대 100개의 그룹이 있습니다. IP 집합, MAC 집합 및 AD 그룹은 방화벽 제외 목록에 사용되는 그룹에 멤버로 포함될 수 없습니다. 자세한 내용은 방화벽 제외 목록 관리 항목을 참조하십시오.

NSX Cloud 참고 NSX Cloud를 사용하는 경우, 공용 클라우드 태그를 사용하여 NSX Manager에서 워크로드 VM을 그룹화하는 방법에 대한 내용을 [NSX-T Data Center 및 공용 클라우드 태그를 사용하여 VM 그룹화](#)에서 참조하십시오.

단일 ID 기반 그룹은 분산 방화벽 규칙 내에서만 소스로 사용할 수 있습니다. 소스에 IP 및 ID 기반 그룹이 필요한 경우 두 개의 별도 방화벽 규칙을 생성합니다.

IP 주소, MAC 주소 또는 Active Directory 그룹만 구성된 그룹은 **적용 대상** 텍스트 상자에서 사용할 수 없습니다.

참고 vCenter Server에서 호스트를 추가하거나 제거하면 호스트에 있는 VM의 외부 ID가 변경됩니다. VM이 그룹의 정적 멤버이고 VM의 외부 ID가 변경되면 NSX Manager UI가 VM을 더 이상 그룹의 멤버로 표시하지 않습니다. 그러나 그룹을 나열하는 API는 그룹에 원래 외부 ID를 갖는 VM이 포함되어 있다고 계속 표시합니다. VM을 그룹의 정적 멤버로 추가하고 VM의 외부 ID를 변경하는 경우 새 외부 ID를 사용하여 VM을 다시 추가해야 합니다. 동적 멤버 자격 조건을 사용하여 이 문제를 방지할 수도 있습니다.

절차

1 탐색 패널에서 **인벤토리 > 그룹**을 선택합니다.

2 **그룹 추가**를 클릭합니다.

3 그룹 이름을 입력합니다.

4 (선택 사항) **멤버 설정**을 클릭합니다.

각 멤버 자격 조건의 경우 논리적 AND 연산자로 조합된 최대 5개의 규칙을 지정할 수 있습니다. 사용 가능한 멤버 조건은 다음에 대해 적용할 수 있습니다.

- **세그먼트 포트** - 태그 및 선택적 범위를 지정할 수 있습니다.
- **세그먼트** - 태그 및 선택적 범위를 지정할 수 있습니다.
- **가상 시스템** - 특정 문자열을 포함하거나, 특정 문자열과 같거나 같지 않거나, 특정 문자열로 시작하거나 끝나는 이름, 태그, 컴퓨터 OS 이름 또는 컴퓨터 이름을 지정할 수 있습니다.
- **IP 집합** - 태그 및 선택적 범위를 지정할 수 있습니다.

5 (선택 사항) **멤버**를 클릭하여 멤버를 선택합니다.

다음과 같은 멤버 유형을 사용할 수 있습니다.

- **그룹**
- **세그먼트**
- **세그먼트 포트**
- **가상 네트워크 인터페이스**
- **가상 시스템**

6 (선택 사항) **IP/MAC 주소**를 클릭하여 IP 및 MAC 주소를 그룹 멤버로 추가합니다.

IPv4, IPv6 및 멀티캐스트 주소가 지원됩니다.

7 (선택 사항) **AD 그룹**을 클릭하여 Active Directory 그룹을 추가합니다. Active Directory 멤버가 포함된 그룹을 ID 방화벽에 대한 분산 방화벽 규칙의 소스 필드에서 사용할 수 있습니다. 그룹에는 AD 및 계산 멤버가 둘 다 포함될 수 있습니다.

8 (선택 사항) 설명 및 태그를 입력합니다.

9 **적용**을 클릭합니다.

그룹이 멤버와 그룹이 사용되는 위치를 볼 수 있는 옵션과 함께 나열됩니다.

컨텍스트 프로파일 추가

컨텍스트 프로파일을 사용하여 계층 7 애플리케이션 ID 및 도메인 이름과 같은 특성 키 값 쌍을 생성할 수 있습니다. 컨텍스트 프로파일은 정의된 후 하나 이상의 분산 방화벽 규칙 및 게이트웨이 방화벽 규칙에 사용될 수 있습니다.

컨텍스트 프로파일에 사용할 수 있는 애플리케이션 ID와 도메인(FQDN) 이름의 2개 특성이 있습니다. 애플리케이션 ID를 선택하면 TLS_Version 및 CIPHER_SUITE와 같은 하나 이상의 하위 특성이 있을 수 있습니다. 애플리케이션 ID와 도메인 이름은 단일 컨텍스트 프로파일에서 사용될 수 있습니다. 동일한 프로파일에서 여러 애플리케이션 ID가 사용될 수 있습니다. 하위 특성이 있는 하나의 애플리케이션 ID를 사용할 수 있습니다. 하위 특성은 여러 애플리케이션 ID 특성이 단일 프로파일에서 사용될 때 지워집니다.

현재 미리 정의된 도메인 목록이 지원됩니다. 특성 유형 "도메인(FQDN) 이름"의 새 컨텍스트 프로파일을 추가할 때 FQDN 목록을 볼 수 있습니다. API 호출 /policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME을 실행하여 FQDN 목록을 볼 수도 있습니다.

참고

- 게이트웨이 방화벽 규칙은 컨텍스트 프로파일에서 FQDN 특성 또는 기타 하위 특성의 사용을 지원하지 않습니다.
- 컨텍스트 프로파일은 Tier-0 게이트웨이 방화벽 정책에서 지원되지 않습니다. 게이트웨이 방화벽 규칙은 FQDN 특성 또는 기타 하위 특성의 사용을 지원하지 않습니다.

절차

- 1 인벤토리 > 컨텍스트 프로파일을 선택합니다.
- 2 새 컨텍스트 프로파일 추가를 클릭합니다.
- 3 프로파일 이름을 입력합니다.
- 4 [특성] 옆에서 설정을 클릭합니다.
- 5 특성을 선택하거나 특성 추가를 클릭하고 애플리케이션 ID 또는 도메인(FQDN) 이름을 선택합니다.
- 6 하나 이상의 특성을 선택합니다.
- 7 (선택 사항) SSL 또는 CIFS와 같은 하위 특성이 있는 특성을 선택한 경우 [하위 특성/값] 옆에서 설정을 클릭합니다.
 - a 하위 특성 추가를 클릭하고 드롭다운 메뉴에서 하위 특성 범주를 선택합니다.
 - b 하나 이상의 하위 특성을 선택합니다.
 - c 추가를 클릭합니다. 다른 하위 특성은 하위 특성 추가를 클릭하여 추가할 수 있습니다.
 - d 적용을 클릭합니다.
- 8 추가를 클릭합니다.
- 9 (선택 사항) 다른 유형의 특성을 추가하려면 다시 특성 추가를 클릭합니다.
- 10 적용을 클릭합니다.

11 (선택 사항) 설명을 입력합니다.

12 (선택 사항) 태그를 입력합니다.

13 저장을 클릭합니다.

다음에 수행할 작업

이 컨텍스트 프로파일을 계층 7 분산 방화벽 규칙(계층 7 또는 도메인 이름의 경우) 또는 게이트웨이 방화벽 규칙(계층 7의 경우)에 적용합니다.

네트워크 트래픽뿐만 아니라 NSX-T 환경을 모니터링하는 방법에는 여러 가지가 있습니다.

본 장은 다음 항목을 포함합니다.

- 방화벽 IPFIX 프로파일 추가
- 스위치 IPFIX 프로파일 추가
- IPFIX 수집기 추가
- 포트 미러링 프로파일 추가
- SNMP(단순 네트워크 관리 프로토콜)
- 시스템 모니터링에 vRealize Log Insight 사용
- 시스템 모니터링에 vRealize Operations Manager 사용
- 시스템 모니터링에 vRealize Network Insight Cloud 사용
- 고급 모니터링 도구

방화벽 IPFIX 프로파일 추가

방화벽의 IPFIX 프로파일을 구성할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **계획 및 문제 해결 > IPFIX**를 선택합니다.
- 3 **방화벽 IPFIX 프로파일** 탭을 클릭합니다.
- 4 **방화벽 IPFIX 프로파일 추가**를 클릭합니다.

5 다음 세부 정보를 작성합니다.

설정	설명
이름 및 설명	이름과 설명(선택 사항)을 입력합니다. 참고 전역 프로파일을 생성하려면 프로파일 이름을 Global 로 지정합니다. 전역 프로파일은 UI에서 편집하거나 삭제할 수 없으며 NSX-T Data Center API를 통해 이러한 작업을 수행할 수 있습니다.
활성화된 흐름 내보내기 시간 초과(분)	흐름과 연결된 추가 패킷이 수신되는 경우라도 흐름이 시간 초과되기까지의 시간입니다. 기본값은 1입니다.
관찰 도메인 ID	이 매개 변수는 네트워크 흐름이 시작되는 관찰 도메인을 식별합니다. 기본값은 0이며 특정 관찰 도메인이 없음을 나타냅니다.
수집기 구성	드롭다운 메뉴에서 수집기를 선택합니다.
적용 대상	설정 을 클릭하고 필터를 적용할 그룹을 선택하거나 새 그룹을 생성합니다.
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.

6 **저장**을 클릭한 후 **예**를 클릭하고 프로파일을 계속 구성합니다.

7 **저장**을 클릭합니다.

스위치 IPFIX 프로파일 추가

세그먼트라고도 하는 스위치의 IPFIX 프로파일을 구성할 수 있습니다.

흐름 기반 네트워크 모니터링을 사용하면 네트워크 관리자가 네트워크를 통과하는 트래픽에 대한 정보를 얻을 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **계획 및 문제 해결 > IPFIX**를 선택합니다.
- 3 **스위치 IPFIX 프로파일** 탭을 클릭합니다.
- 4 **스위치 IPFIX 프로파일 추가**를 클릭합니다.

5 다음 세부 정보를 입력합니다.

설정	설명
이름 및 설명	이름과 설명(선택 사항)을 입력합니다. 참고 전역 프로파일을 생성하려면 프로파일 이름을 Global 로 지정합니다. 전역 프로파일은 UI에서 편집하거나 삭제할 수 없으며 NSX-T Data Center API를 통해 이러한 작업을 수행할 수 있습니다.
활성 시간 초과(초)	흐름과 연결된 추가 패킷이 수신되는 경우라도 흐름이 시간 초과되기까지의 시간입니다. 기본값은 300입니다.
유휴 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.
패킷 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.
수집기 구성	드롭다운 메뉴에서 수집기를 선택합니다.
적용 대상	범주(세그먼트, 세그먼트 포트 또는 그룹)를 선택합니다. 선택한 개체에 IPFIX 프로파일이 적용됩니다.
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.
최대 흐름 수	브리지에 캐시되는 최대 흐름입니다(KVM만 해당, ESXi에서 구성 가능하지 않음). 기본값은 16384입니다.
관찰 도메인 ID	관찰 도메인 ID는 네트워크 흐름이 시작되는 관찰 도메인을 식별합니다. 특정 관찰 도메인을 지정하지 않으려면 0을 입력합니다.
오버레이 흐름 내보내기	이 매개 변수는 업링크 및 터널 포트에서 오버레이 흐름을 샘플링하고 내보낼지 여부를 정의합니다. vNIC 흐름과 오버레이 흐름이 모두 샘플에 포함됩니다. 기본값은 사용 입니다. 사용하지 않도록 설정하면 vNIC 흐름이 샘플링된 후 내보내집니다.
태그	더 쉬운 검색을 위해 태그를 입력합니다.

6 **저장**을 클릭한 후 **예**를 클릭하고 프로파일을 계속 구성합니다.

7 **적용 대상**을 클릭하여 개체에 프로파일을 적용합니다.

개체를 하나 이상 선택합니다.

8 **저장**을 클릭합니다.

IPFIX 수집기 추가

방화벽 및 스위치의 IPFIX 수집기를 구성할 수 있습니다.

절차

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

- 2 **계획 및 문제 해결 > IPFIX**를 선택합니다.
- 3 **수집기** 탭을 클릭합니다.
- 4 **새 수집기 추가 > IPFIX 스위치** 또는 **새 수집기 추가 > IPFIX 방화벽**을 선택합니다.
- 5 이름을 입력합니다.
- 6 최대 4개 수집기의 IP 주소 및 포트를 입력합니다. IPv4 및 IPv6 주소가 둘 다 지원됩니다.
- 7 **저장**을 클릭합니다.

포트 미러링 프로파일 추가

포트 미러링 세션에 대한 포트 미러링 프로파일을 구성할 수 있습니다.

논리적 SPAN은 VLAN 세그먼트가 아닌 오버레이 세그먼트에 대해서만 지원됩니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **계획 및 문제 해결 > 포트 미러링**을 선택합니다.
- 3 **프로파일 추가 > 원격 L3 Span** 또는 **프로파일 추가 > 논리적 Span**을 선택합니다.
- 4 이름과 설명(선택 사항)을 입력합니다.
- 5 다음 프로파일 세부 정보를 모두 입력합니다.

세션 유형	매개 변수
원격 L3 SPAN	<ul style="list-style-type: none"> ■ 방향 - 양방향, 수신 또는 송신을 선택합니다. ■ 스냅 길이 - 패킷에서 캡처할 바이트 수를 지정합니다. ■ 캡슐화 유형 - GRE, ERSPAN 2 또는 ERSPAN 3을 선택합니다. ■ GRE 키 - 캡슐화 유형이 GRE인 경우 GRE 키를 지정합니다. ■ ERSPAN ID - 캡슐화 유형이 ERSPAN 2 또는 ERSPAN 3인 경우 ERSPAN ID를 지정합니다.
논리적 SPAN	<ul style="list-style-type: none"> ■ 방향 - 양방향, 수신 또는 송신을 선택합니다. ■ 스냅 길이 - 패킷에서 캡처할 바이트 수를 지정합니다.

- 6 **소스** 열에서 **설정**을 클릭하여 소스를 설정합니다.

논리적 SPAN의 경우 사용 가능한 소스는 **세그먼트 포트**, **가상 시스템 그룹** 및 **가상 네트워크 인터페이스 그룹**입니다.

원격 L3 SPAN의 경우 사용 가능한 소스는 **세그먼트**, **세그먼트 포트**, **가상 시스템 그룹** 및 **가상 네트워크 인터페이스 그룹**입니다.

- 7 **대상** 열에서 **설정**을 클릭하여 대상을 설정합니다.
- 8 **저장**을 클릭합니다.

SNMP(단순 네트워크 관리 프로토콜)

SNMP(단순 네트워크 관리 프로토콜)를 사용하여 NSX-T Data Center 구성 요소를 모니터링할 수 있습니다. SNMP 서비스는 기본적으로 설치 후에 시작되지 않습니다.

절차

1 NSX Manager CLI 또는 NSX Edge CLI에 로그인합니다.

2 다음 명령을 실행합니다.

- SNMPv1/SNMPv2의 경우:

```
set snmp community <community-string>
start service snmp
```

community-string의 최대 문자 제한은 64입니다.

- SNMPv3의 경우

```
set snmp v3-users <user_name> auth-password <auth_password> priv-password
<priv_password>

start service snmp
```

user_name의 최대 문자 제한은 32입니다. 암호가 PAM 제약 조건을 충족하는지 확인하십시오. 기본 엔진 ID를 변경하려는 경우 다음 명령을 사용합니다.

```
set snmp v3-engine-id <v3-engine-id>

start service snmp
```

v3-engine-id는 10~64자 길이의 16진수 문자열입니다.

NSX-T Data Center는 SHA1 및 AES128을 증 및 개인 정보 프로토콜로서 지원합니다. API 호출을 사용하여 SNMPv3을 설정할 수도 있습니다. 자세한 정보는 "NSX-T Data Center API 가이드"를 참조하십시오.

예제:

시스템 모니터링에 vRealize Log Insight 사용

Log Insight NSX-T 컨텐츠 팩을 사용하여 NSX-T Data Center 환경을 모니터링할 수 있습니다.

이 컨텐츠 팩은 다음과 같은 경고를 발생합니다.

경고 이름	설명
SysCpuUsage	CPU 사용량이 10분 넘게 95%를 초과합니다.
SysMemUsage	메모리 사용량이 10분 넘게 95%를 초과합니다.

경고 이름	설명
SysDiskUsage	하나 이상의 파티션에 대한 디스크 사용량이 10분 넘게 89%를 초과합니다.
PasswordExpiry	장치 사용자 계정에 대한 암호가 곧 만료될 예정이거나 만료되었습니다.
CertificateExpiry	하나 이상의 CA 서명 인증서가 만료되었습니다.
ClusterNodeStatus	로컬 Edge 클러스터 노드가 종료되었습니다.
BackupFailure	스케줄링된 NSX 백업 작업이 실패했습니다.
VipLeadership	NSX 관리 클러스터 VIP가 종료되었습니다.
ApiRateLimit	클라이언트 API가 구성된 임계값에 도달했습니다.
CorfuQuorumLost	클러스터에서 두 개의 노드가 종료되고 corfu 쿼럼이 손실됩니다.
DfwHeapMem	DFW 힙 메모리가 구성된 임계값을 초과했습니다.
ProcessStatus	위험 프로세스 상태가 변경되었습니다.
ClusterFailoverStatus	SR 고가용성 상태가 변경되었거나 활성/대기 서비스가 페일오버됩니다.
DhcpPoolUsageOverloadedEvent	DHCP 풀이 구성된 사용량 임계값에 도달했습니다.
FabricCryptoStatus	실패한 KAT(Known_Answer_Tests)에 대해 Edge 암호화 mux 드라이버가 종료되었습니다.
VpnTunnelState	VPN 터널이 종료되었습니다.
BfdTunnelStatus	BFD 터널 상태가 변경되었습니다.
RoutingBgpNeighborStatus	BGP 인접 네트워크 상태가 종료되었습니다.
VpnL2SessionStatus	L2 VPN 세션이 종료되었습니다.
VpnIkeSessionStatus	IKE 세션이 종료되었습니다.
RoutingStatus	라우팅(BGP/BFD)이 종료되었습니다.
DnsForwarderStatus	DNS 전달자 실행 중 상태가 종료입니다.
TnConnDown_15min	컨트롤러/관리자에 대한 전송 노드 연결이 최소 15분 동안 종료되었습니다.
TnConnDown_5min	컨트롤러/관리자에 대한 전송 노드 연결이 최소 5분 동안 종료되었습니다.
ServiceDown	하나 이상의 서비스가 종료되었습니다.
IpNotAvailableInPool	풀에서 사용할 수 있는 IP가 없거나 구성된 임계값에 도달했습니다.
LoadBalancerError	NSX 로드 밸런서 서비스가 오류 상태입니다.
LoadBalancerDown	NSX 로드 밸런서 서비스가 종료 상태입니다.
LoadBalancerVsDown	VS 상태: 모든 풀 멤버가 종료되었습니다.
LoadBalancerPoolDown	풀 상태: 모든 풀 멤버가 종료되었습니다.
ProcessCrash	데이터 경로 또는 다른 LB 프로세스(예: 디스패처)에서 프로세스 또는 데몬이 충돌합니다.

시스템 모니터링에 vRealize Operations Manager 사용

vRealize Operations Manager를 사용하여 NSX-T Data Center 환경을 모니터링할 수 있습니다.

표 12-1. NSX-T용 관리 팩의 경고

경고	설명	권장 사항
NSX-T 관리 서비스가 실패했습니다.	NSX-T Data Center 호스트의 관리 서비스가 실행되고 있지 않을 때 트리거됩니다.	NSX-T Manager에 로그인하고 실패한 관리 서비스를 다시 시작하십시오.
논리적 스위치의 관리 상태가 실행 중이 아닙니다.	관리 상태가 논리적 스위치에서 사용되지 않도록 설정된 경우 트리거됩니다.	원할 경우 NSX-T에 로그인하고 원하는 경우 관리 상태를 사용하도록 설정하십시오.
Edge 노드 컨트롤러/관리자 연결이 실행 중이 아닙니다.	Edge 노드 연결 상태가 NSX-T Data Center에서 종료된 경우 트리거됩니다.	컨트롤러 클러스터 및 관리자 클러스터와의 Edge 노드 연결 상태를 확인하고 끊어진 연결을 수정하십시오.
Edge 호스트 노드가 실패/오류 상태에 있습니다.	다음 이유 중 하나로 인해 NSX-T Data Center의 호스트 노드가 오류 또는 실패 상태인 경우 트리거됩니다. <ul style="list-style-type: none"> ■ Edge 구성 오류 ■ 설치 실패 ■ 제거 실패 ■ 업그레이드 실패 ■ 가상 시스템 배포 실패 ■ 가상 시스템 전원 끄기 실패 ■ 가상 시스템 전원 켜기 실패 ■ 가상 시스템 배포 해제 실패 	Edge 호스트 노드가 실패/오류 상태에 있습니다. 호스트 노드 상태를 확인하고 문제를 해결하십시오.
BFD 서비스가 사용되지 않도록 설정되어 있습니다.	BFD 서비스가 논리적 라우터에서 사용하도록 설정되지 않은 경우 트리거됩니다.	인접 항목이 구성된 경우에도 TIER0 라우터에 대한 BFD 서비스가 사용하도록 설정되어 있지 않습니다. 필요한 경우 BFD 서비스를 사용하도록 설정하십시오.
NAT 규칙이 구성되지 않음	논리적 라우터의 NAT 규칙이 구성되지 않은 경우 트리거됩니다.	NSX-T Manager에 로그인하고 논리적 라우터에 대한 NAT 규칙을 추가하십시오.
정적 경로가 구성되지 않음	논리적 라우터의 정적 경로가 구성되지 않은 경우 트리거됩니다.	필요한 경우 NSX-T Manager에 로그인하고 논리적 라우터에 대한 정적 경로를 추가하십시오.
경로 보급 서비스가 사용되지 않도록 설정됨	경로 보급 서비스가 논리적 라우터에서 사용하도록 설정되지 않은 경우 트리거됩니다.	경로 보급이 구성된 경우에도 TIER1 라우터에 대한 경로 보급 서비스가 사용하도록 설정되지 않았습니다. NSX-T Manager에 로그인하고 서비스를 사용하도록 설정하십시오.

표 12-1. NSX-T용 관리 팩의 경고 (계속)

경고	설명	권장 사항
경로 재배포 서비스가 사용되지 않도록 설정됨	경로 재배포 서비스가 논리적 라우터에서 사용하도록 설정되지 않은 경우 트리거됩니다.	경로 재배포 규칙이 구성된 경우에도 TIER0 라우터에 대한 경로 재배포 서비스가 사용하도록 설정되지 않았습니다. NSX-T Manager에 로그인하고 서비스를 사용하도록 설정하십시오.
ECMP 서비스가 논리적 라우터에 대해 사용하지 않도록 설정됨	ECMP 서비스가 논리적 라우터에서 사용하도록 설정되지 않은 경우 트리거됩니다.	인접 항목이 구성된 경우에도 TIER0 라우터에 대한 BGP ECMP 서비스가 사용하도록 설정되지 않았습니다. NSX-T Manager에 로그인하고 서비스를 사용하도록 설정하십시오.
컨트롤러 노드 연결이 끊어짐	컨트롤러 노드 연결 상태가 NSX-T Data Center에서 종료된 경우 트리거됩니다.	NSX-T Manager에 로그인하고 관리 노드 및 컨트롤러 클러스터와의 컨트롤러 노드 연결을 확인하고 연결 끊기 상태를 해결하십시오.
3개 미만의 컨트롤러 노드가 배포됨	NSX-T Data Center 서버에 컨트롤러 노드가 3개 미만인 경우 트리거됩니다.	클러스터에 컨트롤러 노드를 3개 이상 배포합니다.
컨트롤러 클러스터 상태가 안정적이지 않음	모든 컨트롤러 노드가 NSX-T Data Center에서 종료된 경우 트리거됩니다.	컨트롤러 클러스터의 상태를 확인하십시오.
관리 상태가 안정적이지 않음	관리 클러스터의 노드 상태가 종료된 경우 트리거됩니다.	관리 클러스터의 상태를 확인하십시오.
파일 시스템 사용량이 85%를 초과함	컨트롤러 가상 시스템의 게스트 파일 시스템 사용량이 85%를 초과하는 경우 트리거됩니다.	파일 시스템 사용량이 85%보다 큼니다. 파일 시스템을 확인하고 정리하여 더 많은 공간을 확보하십시오.
파일 시스템 사용량이 75%를 초과함	컨트롤러 가상 시스템의 게스트 파일 시스템 사용량이 75%를 초과하는 경우 트리거됩니다.	파일 시스템 사용량이 75%보다 큼니다. 파일 시스템을 확인하고 정리하여 더 많은 공간을 확보하십시오.
파일 시스템 사용량이 70%를 초과함	컨트롤러 가상 시스템의 게스트 파일 시스템 사용량이 70%를 초과하는 경우 트리거됩니다.	파일 시스템 사용량이 70%보다 큼니다. 파일 시스템을 확인하고 정리하여 더 많은 공간을 확보하십시오.
Edge 클러스터 상태가 종료됨	Edge 클러스터 상태가 종료된 경우 트리거됩니다.	Edge 클러스터 상태를 확인하고 필요한 경우 NSX-T 설명서 및 VMware 설명서에서 권장하는 표준 문제 해결 단계를 수행하십시오.

표 12-1. NSX-T용 관리 팩의 경고 (계속)

경고	설명	권장 사항
논리적 스위치 상태가 실패	논리적 스위치의 상태가 실패인 경우 트리거됩니다.	논리적 스위치 상태를 확인하고 필요한 경우 NSX-T 설명서 및 VMware 설명서에서 권장하는 표준 문제 해결 단계를 수행하십시오.
로드 밸런서 서비스가 작동 상태가 종료	로드 밸런서 서비스의 작동 상태가 종료인 경우 트리거됩니다.	로드 밸런서 서비스의 작동 상태를 확인하고 필요한 경우 NSX-T 설명서 및 VMware 설명서에서 권장하는 표준 문제 해결 단계를 수행하십시오.
로드 밸런서 서비스 작동 상태 오류	로드 밸런서 서비스의 작동 상태에 오류가 포함된 경우 트리거됩니다.	로드 밸런서 서비스의 작동 상태를 확인하고 필요한 경우 NSX-T 설명서 및 VMware 설명서에서 권장하는 표준 문제 해결 단계를 수행하십시오.
로드 밸런서 가상 서버 작동 상태가 종료	로드 밸런서 가상 서버의 작동 상태가 종료인 경우 트리거됩니다.	로드 밸런서 가상 서버의 작동 상태를 확인하고 필요한 경우 NSX-T 설명서 및 VMware 설명서에서 권장하는 표준 문제 해결 단계를 수행하십시오.
로드 밸런서 가상 서버 작동 상태가 분리됨	로드 밸런서 가상 서버의 작동 상태가 분리됨인 경우 트리거됩니다.	로드 밸런서 가상 서버의 작동 상태를 확인하고 필요한 경우 NSX-T 설명서 및 VMware 설명서에서 권장하는 표준 문제 해결 단계를 수행하십시오.
Edge 노드 구성 상태가 실패	Edge 노드의 구성 상태가 실패한 경우 트리거됩니다.	Edge 노드의 구성 상태를 확인하고 필요한 경우 NSX-T 설명서 및 VMware 설명서에서 권장하는 표준 문제 해결 단계를 수행하십시오.
관리 서비스 모니터 런타임 상태가 실패	관리 서비스의 모니터 런타임 상태가 실행을 중지할 경우 트리거됩니다.	NSX-T Manager VA에 로그인하고 실패한 관리 서비스를 다시 시작하십시오.
관리 클러스터의 관리 상태가 안정적이지 않음	관리 클러스터의 관리 상태가 안정적이지 않은 경우 트리거됩니다.	관리 클러스터의 상태를 확인하십시오.
3개 미만의 관리자 노드가 배포됨	NSX-T 서버에 관리자 노드가 3개 미만인 경우 트리거됩니다.	클러스터에 관리자 노드를 3개 이상 배포합니다.
관리자 노드 연결이 끊어짐	관리자 노드의 관리자 연결 상태가 종료인 경우 트리거됩니다.	NSX-T Manager에 로그인하고 관리자 노드의 관리자 연결을 확인한 후 NSX-T 설명서 및 VMware 설명서에서 권장하는 표준 문제 해결 단계를 수행하십시오.

표 12-1. NSX-T용 관리 팩의 경고 (계속)

경고	설명	권장 사항
관리자 노드의 파일 시스템 사용량이 85%를 초과함	관리자 노드의 게스트 파일 시스템 사용량이 85%를 초과하는 경우 트리거됩니다.	파일 시스템 사용량이 85보다 큽니다. 파일 시스템을 확인하고 정리하여 더 많은 공간을 확보하십시오.
관리자 노드의 파일 시스템 사용량이 75%를 초과함	관리자 노드의 게스트 파일 시스템 사용량이 75%를 초과하는 경우 트리거됩니다.	파일 시스템 사용량이 75보다 큽니다. 파일 시스템을 확인하고 정리하여 더 많은 공간을 확보하십시오.
관리자 노드의 파일 시스템 사용량이 70%를 초과함	관리자 노드의 게스트 파일 시스템 사용량이 70%를 초과하는 경우 트리거됩니다.	파일 시스템 사용량이 70보다 큽니다. 파일 시스템을 확인하고 정리하여 더 많은 공간을 확보하십시오.

시스템 모니터링에 vRealize Network Insight Cloud 사용

vRealize Network Insight Cloud를 사용하여 NSX-T Data Center 환경을 모니터링할 수 있습니다.

표 12-2. vRealize Network Insight 계산 NSX-T 이벤트

OID	이벤트 이름	기본 심각도	UI 이름	설명
1.3.6.1.4.1.6876.100.1.0.80205	NSXTNoUplinkConnectivityEvent	주의	NSX-T Tier-1 논리적 라우터 연결 끊기 이벤트	Tier-0 라우터에서 NSX-T Tier-1 논리적 라우터 연결이 끊겼습니다. 이 라우터 아래의 네트워크는 외부에서 연결할 수 없으며 그 반대 경우도 마찬가지입니다.
1.3.6.1.4.1.6876.100.1.0.80206	NSXTRoutingAdvertisementEvent	주의	라우팅 알림 사용 안 함	라우팅 알림이 NSX-T Tier-1 논리적 라우터에 대해 사용하지 않도록 설정되었습니다. 이 라우터 아래의 네트워크는 외부에서 연결할 수 없습니다.
1.3.6.1.4.1.6876.100.1.0.80207	NSXTManagerConnectivityDownEvent	위험	NSX-T Edge 노드에 관리자 연결이 없음	NSX-T Edge 노드와 관리자 사이의 연결이 끊어졌습니다.
1.3.6.1.4.1.6876.100.1.0.80208	NSXTControllerConnectivityDegradedEvent	주의	NSX-T Edge 노드의 컨트롤러 연결 성능이 저하됨	NSX-T Edge 노드가 하나 이상의 컨트롤러와 통신할 수 없습니다.
1.3.6.1.4.1.6876.100.1.0.80209	NSXTControllerConnectivityDownEvent	위험	NSX-T Edge 노드에 컨트롤러 연결이 없음	NSX-T Edge 노드가 모든 컨트롤러와 통신할 수 없습니다.

표 12-2. vRealize Network Insight 계산 NSX-T 이벤트 (계속)

OID	이벤트 이름	기본 심각도	UI 이름	설명
1.3.6.1.4.1.6876.100.1.0.80210	NSXTMtumismatchEvent	주의	NSX-T Tier-0 및 업링크 스위치/라우터 간 MTU 불일치	Tier-0 논리적 라우터의 인터페이스에 구성된 MTU가 동일한 L2 네트워크에 있는 업링크 스위치/라우터 인터페이스와 일치하지 않습니다. 이는 네트워크 성능에 영향을 줄 수 있습니다.
1.3.6.1.4.1.6876.100.1.0.80211	NSXTExcludedVmFlowEvent	정보	하나 이상의 VM이 NSX-T DFW 방화벽에서 제외되었습니다.	하나 이상의 VM이 NSX-T DFW 방화벽으로 보호되지 않습니다. vRealize Network Insight는 이러한 VM에 대해 IPFIX 흐름을 수신하지 않습니다.
1.3.6.1.4.1.6876.100.1.0.80212	NSXTDoubleVlanTaggingEvent	주의	잘못된 VLAN 구성	Tier-0 라우터의 업링크 포트에 있는 VLAN이 외부 게이트웨이에 있는 VLAN과 다르기 때문에 통신이 중단됩니다.
1.3.6.1.4.1.6876.100.1.0.80213	NSXTNoTzAttachedOntnEvent	주의	전송 노드에 연결된 전송 영역이 없습니다.	전송 노드에 연결된 전송 영역이 없습니다. 이로 인해 VM 연결이 끊어질 수 있습니다.
1.3.6.1.4.1.6876.100.1.0.80214	NSXTVtepedeleteevent	주의	전송 노드에서 VTEP를 사용할 수 없습니다.	전송 노드에서 모든 VTEP가 삭제됩니다. 이로 인해 VM 연결이 끊어질 수 있습니다.
1.3.6.1.4.1.6876.100.1.0.80225	NSXTControllerNodeToControlClusterConnectivityEvent	위험	NSX-T Controller 노드에 제어 클러스터 연결이 없음	NSX-T 컨트롤러 노드가 제어 클러스터 연결을 손실했습니다.
1.3.6.1.4.1.6876.100.1.0.80226	NSXTControllerNodeToMgmtPlaneConnectivityEvent	위험	NSX-T Controller 노드에 관리부 연결이 없음	NSX-T 컨트롤러 노드가 관리부 연결을 손실했습니다.
1.3.6.1.4.1.6876.100.1.0.80227	NSXTMPNodeToMgmtClusterConnectivityEvent	위험	NSX-T 관리 노드에 관리 클러스터 연결이 없음	NSX-T 관리 노드가 관리 클러스터 연결을 손실했습니다.
1.3.6.1.4.1.6876.100.1.0.80246	NSXTHostNodeMgmtConnectivityStatusDownEvent	주의	NSX-T 호스트 노드에 관리자 연결이 없음	NSX Manager와 호스트 전송 노드 간 연결 상태 비동기화

표 12-2. vRealize Network Insight 계산 NSX-T 이벤트 (계속)

OID	이벤트 이름	기본 심각도	UI 이름	설명
1.3.6.1.4.1.6876.100.1.0.80247	NSXTEdgeNodeCtrlConnectivityStatusUnknownEvent	위험	NSX-T Edge 노드에 대한 컨트롤러 연결을 알 수 없습니다.	NSX-T Edge 노드 컨트롤러 연결을 알 수 없습니다.
1.3.6.1.4.1.6876.100.1.0.80248	NSXTHostNodeCtrlConnectivityStatusDownEvent	주의	NSX-T 호스트 노드에 컨트롤러 연결이 없음	NSX-T 호스트 노드가 모든 컨트롤러와 통신할 수 없습니다.
1.3.6.1.4.1.6876.100.1.0.80249	NSXTHostNodeCtrlConnectivityStatusDegradedEvent	주의	NSX-T 호스트 노드에 대한 컨트롤러 연결 성능이 저하됨	NSX-T 호스트 노드가 하나 이상의 컨트롤러와 통신할 수 없습니다.
1.3.6.1.4.1.6876.100.1.0.80250	NSXTHostNodeCtrlConnectivityStatusUnknownEvent	주의	NSX-T 호스트 노드에 대한 컨트롤러 연결을 알 수 없습니다.	NSX-T 호스트 노드 컨트롤러 연결을 알 수 없습니다.
1.3.6.1.4.1.6876.100.1.0.80228	NSXTHostNodePnicStatusDownEvent	주의	NSX-T 호스트 전송 노드 pNIC가 '가동 중지' 상태입니다.	NSX-T 호스트 전송 노드 pNIC가 '가동 중지' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80229	NSXTHostNodePnicStatusDegradedEvent	주의	NSX-T 호스트 전송 노드 pNIC가 '성능 저하됨' 상태입니다.	NSX-T 호스트 전송 노드 pNIC가 '성능 저하됨' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80230	NSXTHostNodePnicStatusUnknownEvent	주의	NSX-T 호스트 전송 노드 pNIC가 '알 수 없음' 상태입니다.	NSX-T 호스트 전송 노드 pNIC가 '알 수 없음' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80237	NSXTEdgeNodePnicStatusDownEvent	위험	NSX-T Edge 전송 노드 pNIC가 '가동 중지' 상태입니다.	NSX-T Edge 전송 노드 pNIC가 '가동 중지' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80238	NSXTEdgeNodePnicStatusDegradedEvent	위험	NSX-T Edge 전송 노드 pNIC가 '성능 저하됨' 상태입니다.	NSX-T Edge 전송 노드 pNIC가 '성능 저하됨' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80239	NSXTEdgeNodePnicStatusUnknownEvent	위험	NSX-T Edge 전송 노드 pNIC가 '알 수 없음' 상태입니다.	NSX-T Edge 전송 노드 pNIC가 '알 수 없음' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80231	NSXTHostNodeTunnelStatusDownEvent	주의	NSX-T 호스트 전송 노드 터널이 '가동 중지' 상태입니다.	NSX-T 호스트 전송 노드 터널이 '가동 중지' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80232	NSXTHostNodeTunnelStatusDegradedEvent	주의	NSX-T 호스트 전송 노드 터널이 '성능 저하됨' 상태입니다.	NSX-T 호스트 전송 노드 터널이 '성능 저하됨' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80233	NSXTHostNodeTunnelStatusUnknownEvent	주의	NSX-T 호스트 전송 노드 터널이 '알 수 없음' 상태입니다.	NSX-T 호스트 전송 노드 터널이 '알 수 없음' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80240	NSXTEdgeNodeTunnelStatusDownEvent	위험	NSX-T Edge 전송 노드 터널이 '가동 중지' 상태입니다.	NSX-T Edge 전송 노드 터널이 '가동 중지' 상태입니다.

표 12-2. vRealize Network Insight 계산 NSX-T 이벤트 (계속)

OID	이벤트 이름	기본 심각도	UI 이름	설명
1.3.6.1.4.1.6876.100.1.0.80241	NSXTEdgeNodeTunnelStatusDegradedEvent	위험	NSX-T Edge 전송 노드 터널이 '성능 저하됨' 상태입니다.	NSX-T Edge 전송 노드 터널이 '성능 저하됨' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80242	NSXTEdgeNodeTunnelStatusUnknownEvent	위험	NSX-T Edge 전송 노드 터널이 '알 수 없음' 상태입니다.	NSX-T Edge 전송 노드 터널이 '알 수 없음' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80234	NSXTHostNodeStatusDownEvent	주의	NSX-T 호스트 전송 노드가 '가동 중지' 상태입니다.	NSX-T 호스트 전송 노드가 '가동 중지' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80235	NSXTHostNodeStatusDegradedEvent	주의	NSX-T 호스트 전송 노드가 '성능 저하됨' 상태입니다.	NSX-T 호스트 전송 노드가 '성능 저하됨' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80236	NSXTHostNodeStatusUnknownEvent	주의	NSX-T 호스트 전송 노드가 '알 수 없음' 상태입니다.	NSX-T 호스트 전송 노드가 '알 수 없음' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80243	NSXTEdgeNodeStatusDownEvent	위험	NSX-T Edge 전송 노드가 '가동 중지' 상태입니다.	NSX-T Edge 전송 노드가 '가동 중지' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80244	NSXTEdgeNodeStatusDegradedEvent	위험	NSX-T Edge 전송 노드가 '성능 저하됨' 상태입니다.	NSX-T Edge 전송 노드가 '성능 저하됨' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80245	NSXTEdgeNodeStatusUnknownEvent	위험	NSX-T Edge 전송 노드가 '알 수 없음' 상태입니다.	NSX-T Edge 전송 노드가 '알 수 없음' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80252	NSXTLogicalSwitchAdminStatusDownEvent	주의	NSX-T 논리적 스위치 관리가 '가동 중지' 상태입니다.	NSX-T 논리적 스위치 관리가 '가동 중지' 상태입니다.
1.3.6.1.4.1.6876.100.1.0.80253	NSXTLogicalPortOperationalStatusDownEvent	위험	NSX-T 논리적 포트 작동이 '가동 중지' 상태입니다.	NSX-T 논리적 포트 작동이 '가동 중지' 상태입니다. 이로 인해 동일한 논리적 스위치에 연결된 두 VIF(가상 인터페이스) 간에 통신 오류(예: 한 VM에서 다른 VM을 ping할 수 없음)가 발생할 수 있습니다.

표 12-2. vRealize Network Insight 계산 NSX-T 이벤트 (계속)

OID	이벤트 이름	기본 심각도	UI 이름	설명
1.3.6.1.4.1.6876.100.1.0.80254	NSXTLogicalPortOperationalStatusUnknownEvent	주의	NSX-T 논리적 포트 작동이 '알 수 없음' 상태입니다.	NSX-T 논리적 포트 작동이 '알 수 없음' 상태입니다. 이로 인해 동일한 논리적 스위치에 연결된 두 VIF(가상 인터페이스) 간에 통신 오류(예: 한 VM에서 다른 VM을 ping할 수 없음)가 발생할 수 있습니다.
1.3.6.1.4.1.6876.100.1.0.80255	NSXTComputeManagerConnectionStatusNotUpEvent	주의	NSX-T 계산 관리자 연결 상태가 작동 중이 아닙니다.	NSX-T 계산 관리자 연결 상태가 작동 중이 아닙니다.
1.3.6.1.4.1.6876.100.1.0.80256	NSXTClusterBackupDisabledEvent	주의	NSX-T Manager 백업이 예약되지 않았습니다.	NSX-T Manager 백업이 예약되지 않았습니다.
1.3.6.1.4.1.6876.100.1.0.80257	NSXTDFWFirewallDisabledEvent	위험	NSX-T DFW 방화벽이 사용되지 않도록 설정되었습니다.	분산 방화벽이 NSX-T Manager에서 사용되지 않도록 설정되었습니다.
1.3.6.1.4.1.6876.100.1.0.80258	NSXTLogicalPortReceivedPacketDropEvent	주의	NSX-T 논리적 포트 수신 패킷이 삭제됩니다.	수신된 패킷이 NSX-T 논리적 포트에서 삭제되고 관련 엔티티가 영향을 받을 수 있습니다.
1.3.6.1.4.1.6876.100.1.0.80259	NSXTLogicalPortTransmittedPacketDropEvent	주의	NSX-T 논리적 포트 전송 패킷이 삭제됩니다.	전송된 패킷이 NSX-T 논리적 포트에서 삭제되고 관련 엔티티가 영향을 받을 수 있습니다.
1.3.6.1.4.1.6876.100.1.0.80260	NSXTLogicalSwitchReceivedPacketDropEvent	주의	NSX-T 논리적 스위치 수신 패킷이 삭제됩니다.	수신된 패킷이 NSX-T 논리적 스위치에서 삭제되고 관련 엔티티가 영향을 받을 수 있습니다.
1.3.6.1.4.1.6876.100.1.0.80261	NSXTLogicalSwitchTransmittedPacketDropEvent	주의	NSX-T 논리적 스위치 전송 패킷이 삭제됩니다.	전송된 패킷이 NSX-T 논리적 스위치에서 삭제되고 관련 엔티티가 영향을 받을 수 있습니다.
1.3.6.1.4.1.6876.100.1.0.80262	NSXTRxPacketDropOnMPNicEvent	주의	수신된 패킷이 NSX-T 관리 노드의 네트워크 인터페이스에서 삭제되고 있습니다.	수신된 패킷이 NSX-T 관리 노드의 네트워크 인터페이스에서 삭제되고 있습니다. 이것은 NSX-T 관리 클러스터와 관련된 네트워크 트래픽에 영향을 줄 수 있습니다.

표 12-2. vRealize Network Insight 계산 NSX-T 이벤트 (계속)

OID	이벤트 이름	기본 심각도	UI 이름	설명
1.3.6.1.4.1.6876.100.1.0.80263	NSXTRxPacketDropOnEdgeTnNicEvent	위험	수신된 패킷이 NSX-T Edge 노드의 네트워크 인터페이스에서 삭제되고 있습니다.	수신된 패킷이 NSX-T Edge 노드의 네트워크 인터페이스에서 삭제되고 있습니다. 이것은 Edge 클러스터의 네트워크 트래픽에 영향을 줄 수 있습니다.
1.3.6.1.4.1.6876.100.1.0.80264	NSXTRxPacketDropOnHostTnNicEvent	주의	수신된 패킷이 NSX-T 호스트 노드의 네트워크 인터페이스에서 삭제되고 있습니다.	수신된 패킷이 NSX-T 호스트 노드의 네트워크 인터페이스에서 삭제되고 있습니다. 이것은 ESXi 호스트의 네트워크 트래픽에 영향을 줄 수 있습니다.
1.3.6.1.4.1.6876.100.1.0.80265	NSXTTxPacketDropOnMPNicEvent	주의	전송된 패킷이 NSX-T 관리 노드의 네트워크 인터페이스에서 삭제되고 있습니다.	전송된 패킷이 NSX-T 관리 노드의 네트워크 인터페이스에서 삭제되고 있습니다. 이것은 NSX-T 관리 클러스터와 관련된 네트워크 트래픽에 영향을 줄 수 있습니다.
1.3.6.1.4.1.6876.100.1.0.80266	NSXTTxPacketDropOnEdgeTnNicEvent	위험	전송된 패킷이 NSX-T Edge 노드의 네트워크 인터페이스에서 삭제되고 있습니다.	전송된 패킷이 NSX-T Edge 노드의 네트워크 인터페이스에서 삭제되고 있습니다. 이것은 Edge 클러스터의 네트워크 트래픽에 영향을 줄 수 있습니다.
1.3.6.1.4.1.6876.100.1.0.80267	NSXTTxPacketDropOnHostTnNicEvent	주의	전송된 패킷이 NSX-T 호스트 노드의 네트워크 인터페이스에서 삭제되고 있습니다.	전송된 패킷이 NSX-T 호스트 노드의 네트워크 인터페이스에서 삭제되고 있습니다. 이것은 ESXi 호스트의 네트워크 트래픽에 영향을 줄 수 있습니다.
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeServiceCmlInventoryStatusEvent	주의	CM 인벤토리 서비스가 실행 중지되었습니다.	CM 인벤토리 서비스 상태가 중지됨으로 바뀌었습니다.
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeServiceControllerStatusEvent	주의	컨트롤러 서비스가 실행 중지되었습니다.	컨트롤러 서비스 상태가 중지됨으로 바뀌었습니다.
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeServiceDataStoreStatusEvent	주의	데이터스토어 서비스가 실행 중지되었습니다.	데이터스토어 서비스 상태가 중지됨으로 바뀌었습니다.

표 12-2. vRealize Network Insight 계산 NSX-T 이벤트 (계속)

OID	이벤트 이름	기본 심각도	UI 이름	설명
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeService HttpStatusEvent	주의	HTTP 서비스가 실행 중 지되었습니다.	HTTP 서비스 상태가 중 지됨으로 바뀌었습니다.
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeService InstallUpgradeEvent	주의	설치 업그레이드 서비스 가 실행 중 지되었습니다.	설치 업그레이드 서비스 상태가 중 지됨으로 바뀌었습니다.
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeService LiagentStatusEvent	주의	Liagent 서비스가 실행 중 지되었습니다.	Liagent 서비스 상태가 중 지됨으로 바뀌었습니다.
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeService ManagerStatusEvent	주의	관리자 서비스가 실행 중 지되었습니다.	관리자 서비스 상태가 중 지됨으로 바뀌었습니다.
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeService MgmtPlaneBusStatus Event	주의	관리부 서비스가 실행 중 지되었습니다.	관리 서비스 상태가 중 지됨으로 바뀌었습니다.
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeService MigrationCoordinator StatusEvent	주의	마이그레이션 조정기 서비스가 실행 중 지되 었습니다.	마이그레이션 조정기 서비스 상태가 중 지됨 으로 바뀌었습니다.
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeService NodeMgmtStatusEve nt	주의	노드 관리 서비스가 실행 중 지되었습니다.	노드 관리 서비스 상태 가 중 지됨으로 바뀌었 습니다.
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeService NodeStatsStatusEve nt	주의	노드 통계 서비스가 실행 중 지되었습니다.	노드 통계 서비스 상태 가 중 지됨으로 바뀌었 습니다.
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeService NSXMessageBusStat usEvent	주의	메시지 버스 서비스가 실행 중 지되었습니다.	메시지 버스 클라이언 트 서비스 상태가 중 지 됨으로 바뀌었습니다.
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeService NSXPlatformClientSta tusEvent	주의	플랫폼 클라이언트 서 비스가 실행 중 지되었 습니다.	플랫폼 클라이언트 서 비스 상태가 중 지됨으 로 바뀌었습니다.
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeService NSXUpgradeAgentSt atusEvent	주의	업그레이드 에이전트 서비스가 실행 중 지되 었습니다.	업그레이드 서비스 상 태가 중 지됨으로 바뀌 었습니다.
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeService NTPStatusEvent	주의	NTP 서비스가 실행 중 지되었습니다.	NTP 서비스 상태가 중 지됨으로 바뀌었습니 다.
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeService PolicyStatusEvent	주의	정책 서비스가 실행 중 지되었습니다.	정책 서비스 상태가 중 지됨으로 바뀌었습니 다.

표 12-2. vRealize Network Insight 계산 NSX-T 이벤트 (계속)

OID	이벤트 이름	기본 심각도	UI 이름	설명
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeService SearchStatusEvent	주의	검색 서비스가 실행 중 중지되었습니다.	검색 서비스 상태가 중 지됨으로 바뀌었습니 다.
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeService SNMPStatusEvent	주의	SNMP 서비스가 실행 중지되었습니다.	SNMP 서비스 상태가 중지됨으로 바뀌었습니 다.
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeService SSHStatusEvent	주의	SSH 서비스가 실행 중 중지되었습니다.	SSH 서비스 상태가 중 지됨으로 바뀌었습니 다.
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeService SyslogStatusEvent	주의	Syslog 서비스가 실행 중지되었습니다.	Syslog 서비스 상태가 중지됨으로 바뀌었습니 다.
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeService TelemetryStatusEvent	주의	원격 분석 서비스가 실 행 중지되었습니다.	원격 분석 서비스 상태 가 중지됨으로 바뀌었 습니다.
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeService UIServiceStatusEvent	주의	UI 서비스가 실행 중지 되었습니다.	UI 서비스 상태가 중지 됨으로 바뀌었습니다.
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeService CmlInventoryStatusEvent	위험	CM 인벤토리 서비스가 중지되었습니다.	NSX-T 관리 노드의 서 비스 중 하나, 즉 CM 인 벤토리 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeService ControllerStatusEvent	위험	컨트롤러 서비스가 중 지되었습니다.	NSX-T 관리 노드의 서 비스 중 하나, 즉 컨트롤 러 서비스가 실행 중지 되었습니다.
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeService DataStoreStatusEvent	위험	데이터스토어 서비스가 중지되었습니다.	NSX-T 관리 노드의 서 비스 중 하나, 즉 데이터 스토어 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeService HttpStatusEvent	위험	HTTP 서비스가 중지되 었습니다.	NSX-T 관리 노드의 서 비스 중 하나, 즉 HTTP 서비스가 실행 중지되 었습니다.
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeService InstallUpgradeEvent	주의	설치 업그레이드 서비 스가 중지되었습니다.	NSX-T 관리 노드의 서 비스 중 하나, 즉 설치 업그레이드 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeService LiagentStatusEvent	주의	Liagent 서비스가 중지 되었습니다.	NSX-T 관리 노드의 서 비스 중 하나, 즉 LI Agent 서비스가 실행 중지되었습니다.

표 12-2. vRealize Network Insight 계산 NSX-T 이벤트 (계속)

OID	이벤트 이름	기본 심각도	UI 이름	설명
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeService ManagerStatusEvent	위험	관리자 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 관리자 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeService MgmtPlaneBusStatus Event	주의	관리부 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 관리부 버스 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeService MigrationCoordinator StatusEvent	주의	마이그레이션 조정기 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 마이그레이션 조정기 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeService NodeMgmtStatusEvent	위험	노드 관리 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 노드 관리 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeService NodeStatsStatusEvent	위험	노드 통계 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 노드 통계가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeService NSXMessageBusStatusEvent	주의	메시지 버스 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 메시지 버스 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeService NSXPlatformClientStatusEvent	위험	플랫폼 클라이언트 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 플랫폼 클라이언트 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeService NSXUpgradeAgentStatusEvent	주의	업그레이드 에이전트 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 업그레이드 에이전트 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeService NTPStatusEvent	위험	NTP 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 NTP 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeService PolicyStatusEvent	위험	정책 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 정책 서비스가 실행 중지되었습니다.

표 12-2. vRealize Network Insight 계산 NSX-T 이벤트 (계속)

OID	이벤트 이름	기본 심각도	UI 이름	설명
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeService SearchStatusEvent	위험	검색 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 검색 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeService SNMPStatusEvent	주의	SNMP 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 SNMP 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeService SSHStatusEvent	위험	SSH 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 SSH 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeService SyslogStatusEvent	위험	Syslog 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 Syslog 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeService TelemetryStatusEvent	주의	원격 분석 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 원격 분석 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeService UIServiceStatusEvent	위험	UI 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 UI 서비스가 실행 중지되었습니다.
1.3.6.1.4.1.6876.100.1.0.80424	NSXTMPNodeService ClusterManagerStatusEvent	위험	클러스터 관리자 서비스가 중지되었습니다.	NSX-T 관리 노드의 서비스 중 하나, 즉 클러스터 관리자 서비스가 실행 중지되었습니다.

NSX-T 시스템 이벤트

다음은 vRealize Network Insight에서 지원되는 NSX-T 2.2 ~ 2.5 이벤트의 목록입니다. 이러한 모든 NSX-T 시스템 이벤트에 대한 OID(개체 ID)는 1.3.6.1.4.1.6876.100.1.0.80203입니다.

표 12-3. NSX-T 시스템 이벤트

이벤트 이름	설명
vmwNSXPlatformSysCpuUsage	관리자와 Edge 장치 둘 모두의 CPU 사용량입니다(NSX-T 2.2).
vmwNSXPlatformSysDiskUsage	/var/log 파티션에 대한 관리자 및 Edge 장치의 디스크 공간 사용량입니다(NSX-T 2.2).
vmwNSXPlatformSysMemUsage	관리자와 Edge 장치 둘 모두의 메모리 사용량입니다(NSX-T 2.2).

표 12-3. NSX-T 시스템 이벤트 (계속)

이벤트 이름	설명
vmwNSXPlatformSysConfigDiskUsage	/config 파티션에 대한 관리자 및 Edge 장치의 디스크 사용량입니다(NSX-T 2.4).
vmwNSXPlatformSysVarDumpDiskUsage	/var/dump 파티션에 대한 관리자 및 Edge 장치의 디스크 사용량입니다(NSX-T 2.5).
vmwNSXPlatformSysRepositoryDiskUsage	/repository 파티션에 대한 관리자 및 Edge 장치의 디스크 사용량입니다(NSX-T 2.5).
vmwNSXPlatformSysRootDiskUsage	루트 파티션에 대한 관리자 및 Edge 장치의 디스크 사용량입니다(NSX-T 2.5).
vmwNSXPlatformSysTmpDiskUsage	tmp 파티션에 대한 관리자 및 Edge 장치의 디스크 사용량입니다(NSX-T 2.5).
vmwNSXPlatformSysImageDiskUsage	/image 파티션에 대한 관리자 및 Edge 장치의 디스크 사용량입니다(NSX-T 2.5).
vmwNSXDhcpPoolUsageOverloadedEvent	DHCP 풀이 오버로드되지 않음/정상입니다(NSX-T 2.5).
vmwNSXDhcpPoolLeaseAllocationFailedEvent	DHCP 풀 리스 할당이 실패/성공했습니다(NSX-T 2.5).
vmwNSXPlatformPasswordExpiryStatus	관리자의 암호 만료(NSX-T 2.4)입니다.
vmwNSXPlatformCertificateExpiryStatus	관리자의 인증서 만료(NSX-T 2.4)입니다.
vmwNSXRoutingBgpNeighborStatus	BGP 인접 항목 상태(NSX-T 2.2)입니다.
vmwNSXVpnTunnelState	VPN 터널 가동/다운 상태입니다(NSX-T 2.2).
vmwNSXVpnL2TunnelStatus	L2 VPN 세션 가동/다운 상태입니다(NSX-T 2.2).
vmwNSXVpnIkeSessionStatus	IKE 세션 가동/다운 상태입니다(NSX-T 2.2).
vmwNSXDnsForwarderStatus	DNS 전달자 상태입니다(NSX-T 2.4).
vmwNSXClusterNodeStatus	클러스터 노드 상태입니다(NSX-T 2.4).
vmwNSXFabricCryptoStatus	Edge 암호화 mux 드라이버의 KAT(Known_Answer_Tests) 실패/통과 상태입니다(NSX-T 2.4).
관리자 디스크 활용도가 정상이 아닙니다.	
BGP 인접 네트워크가 종료되었습니다.	BGP 인접 네트워크가 종료된 경우 경고가 필요합니다.
BGP 인접 네트워크가 실행 중입니다.	인접 네트워크 실행 중 상태가 되면 경보를 지웁니다.
X 초과 스토리지 사용량	X 초과 스토리지에 대한 경고 - 모든 장치 VM(MP, CCP) 또는 전송 노드(Edge, 호스트)에 대해 이벤트가 발생합니다.
X 초과 메모리 사용량	X 초과 메모리에 대한 경고 - 모든 장치 VM(MP, CCP) 또는 전송 노드(Edge, 호스트)에 대해 이벤트가 발생합니다.
X 초과 CPU 사용량	X 초과 CPU에 대한 경고 - 모든 장치 VM(MP, CCP) 또는 전송 노드(Edge, 호스트)에 대해 이벤트가 발생합니다.

고급 모니터링 도구

NSX-T는 포트 연결 보기, Traceflow, 포트 미러링, Activity Monitoring 등을 포함하는 고급 모니터링 방법을 지원합니다.

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 **고급 네트워킹 및 보안 > 도구 > 포트 연결**을 선택합니다.
- 3 **소스 가상 시스템** 드롭다운 메뉴에서 VM을 선택합니다.
- 4 **대상 가상 시스템** 드롭다운 메뉴에서 VM을 선택합니다.
- 5 **이동**을 클릭합니다.

포트 연결 토폴로지의 시각적 맵이 표시됩니다. 시각적 출력에서 구성 요소를 클릭하여 해당 구성 요소에 대한 세부 정보를 확인할 수 있습니다.

Traceflow

Traceflow를 사용하면 네트워크에 패킷을 주입하고 네트워크에서 해당 흐름을 모니터링할 수 있습니다. 이 흐름을 통해 네트워크를 모니터링하고 병목 현상 또는 중단 등의 문제를 식별할 수 있습니다.

Traceflow를 통해 패킷이 대상에 도달하기까지의 경로 또는 반대로 도중에 패킷이 삭제되는 지점을 식별할 수 있습니다. 각 엔티티는 입력 및 출력에서의 패킷 처리를 보고하므로 패킷을 받을 때 또는 패킷을 전달할 때 문제가 발생하는지 확인할 수 있습니다.

Traceflow는 게스트 VM 스택 간을 이동하는 ping 요청/응답과는 다릅니다. Traceflow는 오버레이 네트워크를 통과할 때 표시된 패킷을 관찰하고, 각 패킷은 대상 게스트 VM 또는 Edge 업링크에 도달할 때까지 오버레이 네트워크와 교차될 때 모니터링됩니다. 삽입 표시된 패킷은 실제로는 대상 게스트 VM에 절대 도달되지 않습니다.

Traceflow는 전송 노드에서 사용할 수 있으며 ICMP, TCP, UDP, DHCP, DNS 및 ARP/NDP를 포함하는 IPv4 및 IPv6 프로토콜을 둘 다 지원합니다.

사용자 지정 헤더 필드 및 패킷 크기를 사용하여 패킷을 구성할 수 있습니다. Traceflow의 소스 또는 대상은 논리적 스위치 포트, 논리적 라우터 업링크 포트, CSP 또는 DHCP 포트가 될 수 있습니다. 대상 끝점은 NSX 오버레이 또는 언더레이의 임의 디바이스일 수 있습니다. 그렇지만 NSX Edge 노드의 상위(North)에 있는 대상은 선택할 수 없습니다. 대상은 동일한 서브넷에 있거나 NSX 논리적 분산 라우터를 통해 연결할 수 있어야 합니다.

NSX 브리징이 구성되면 알 수 없는 대상 MAC 주소가 있는 패킷이 항상 브리지로 전송됩니다. 일반적으로 브리지에서 이러한 패킷을 VLAN에 전달하고 해당 Traceflow 패킷을 전달됨으로 보고합니다. 패킷이 전달된 것으로 보고되었다고 해서 추적 패킷이 지정된 대상으로 전달되었음을 의미하는 것은 아닙니다.

Traceflow 관찰에는 브로드캐스트된 Traceflow 패킷의 관찰이 포함될 수 있습니다. ESXi 호스트는 대상 호스트의 MAC 주소를 모를 경우 Traceflow 패킷을 브로드캐스트합니다. 브로드캐스트 트래픽의 경우 소스는 VM vNIC입니다. 브로드캐스트 트래픽의 계층 2 대상 MAC 주소는 FF:FF:FF:FF:FF:FF입니다. 방화벽 검사를 위한 올바른 패킷을 생성하기 위해 브로드캐스트 Traceflow 작업에 서브넷 접두사 길이가 필요합니다. 서브넷 마스크를 통해 NSX에서 패킷에 대한 IP 네트워크 주소를 계산할 수 있습니다.

Traceflow를 사용하여 패킷의 경로 추적

Traceflow를 사용하여 패킷의 경로를 검사합니다. Traceflow는 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 **고급 네트워킹 및 보안 > 도구 > Traceflow**를 선택합니다.
- 3 IPv4 또는 IPv6 주소 유형을 선택합니다.
- 4 트래픽 유형을 선택합니다.

IPv4 주소의 경우 트래픽 유형 선택 옵션은 유니캐스트, 멀티캐스트 및 브로드캐스트입니다. IPv6 주소의 경우 트래픽 유형 선택 옵션은 유니캐스트 또는 멀티캐스트입니다.

참고: 멀티캐스트 및 브로드캐스트는 VMC(VMware Cloud) 환경에서 지원되지 않습니다.

5 트래픽 유형에 따라 소스 및 대상 정보를 지정합니다.

트래픽 유형	소스	대상
유니캐스트	<p>VM 또는 논리적 포트를 선택합니다. VM의 경우:</p> <ul style="list-style-type: none"> ■ 드롭다운 목록에서 VM을 선택합니다. ■ 가상 인터페이스를 선택합니다. ■ 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 목록에서 하나를 선택합니다. ■ IP 주소 및 MAC 주소가 표시되지 않으면 텍스트 상자에 IP 주소 및 MAC 주소를 입력합니다. <p>논리적 포트의 경우:</p> <ul style="list-style-type: none"> ■ 연결 유형 VIF, DHCP, Edge 업링크 또는 Edge 중앙 집중식 서비스를 선택합니다. ■ 포트를 선택합니다. 	<p>VM, 논리적 포트 또는 IP-MAC을 선택합니다. VM의 경우:</p> <ul style="list-style-type: none"> ■ 드롭다운 목록에서 VM을 선택합니다. ■ 가상 인터페이스를 선택합니다. ■ 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 목록에서 하나를 선택합니다. ■ IP 주소 및 MAC 주소가 표시되지 않으면 텍스트 상자에 IP 주소 및 MAC 주소를 입력합니다. <p>논리적 포트의 경우:</p> <ul style="list-style-type: none"> ■ 연결 유형 VIF, DHCP, Edge 업링크 또는 Edge 중앙 집중식 서비스를 선택합니다. ■ 포트를 선택합니다. <p>IP-MAC의 경우:</p> <ul style="list-style-type: none"> ■ 추적 유형(계층 2 또는 계층 3)을 선택합니다. 계층 2의 경우 IP 주소 및 MAC 주소를 입력합니다. 계층 3의 경우 IP 주소를 입력합니다.
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.

6 (선택 사항) 고급을 클릭하여 고급 옵션을 표시합니다.

7 (선택 사항) 왼쪽 열에서 다음 필드에 대해 원하는 값 또는 입력을 넣습니다.

옵션	설명
프레임 크기	기본값은 128입니다.
TTL	기본값은 64입니다.
시간 초과(밀리초)	기본값은 10000입니다.
Ethertype	기본값은 2048입니다.
페이로드 유형	Base64, 16진수, 일반 텍스트, 바이너리 또는 십진수를 선택합니다.
페이로드 데이터	페이로드가 선택된 유형을 기반으로 형식이 지정됩니다.

8 (선택 사항) 프로토콜을 선택하고 관련 정보를 제공합니다.

프로토콜	매개 변수
TCP	소스 포트, 대상 포트 및 TCP 플래그를 지정합니다.
UDP	소스 포트 및 대상 포트를 지정합니다.
ICMPv6	ICMP ID 및 순서를 지정합니다.
ICMP	ICMP ID 및 순서를 지정합니다.
DHCPv6	DHCP 메시지 유형 요청 , 보급 , 요청 또는 응답 을 선택합니다.
DHCP	DHCP OP 코드 부팅 요청 또는 부팅 응답 을 선택합니다.
DNS	주소를 지정하고 메시지 유형 쿼리 또는 응답 을 선택합니다.

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. 그러지 않으면 **모두** 필터가 적용됩니다. 그래픽 맵에 백플레이인 및 라우터 링크가 표시됩니다. 브리징 정보는 표시되지 않습니다.

포트 미러링 세션 모니터링

문제 해결 및 기타 목적으로 포트 미러링 세션을 모니터링할 수 있습니다.

논리적 SPAN은 VLAN 논리적 스위치가 아닌 오버레이 논리적 스위치에 대해서만 지원됩니다.

NSX Cloud 참고 NSX Cloud를 사용하는 경우 [NSX Cloud](#)에서 지원되는 [NSX-T Data Center](#) 기능에서 자동 생성된 논리적 엔티티, 지원되는 기능 및 [NSX Cloud](#)에 필요한 구성 목록을 확인하십시오.

이 기능에는 다음과 같은 제한 사항이 있습니다.

- 소스 미러 포트는 둘 이상의 미러 세션일 수 없습니다.
- KVM을 사용하면 여러 NIC가 동일한 OVS 포트에 연결될 수 있습니다. 미러링은 OVS 업링크 포트에서 발생합니다. 즉, OVA 포트에 연결된 모든 물리적 NIC의 트래픽이 미러링됩니다.
- 로컬 SPAN 세션의 경우 미러 세션 소스 및 대상 포트가 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 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 3 **고급 네트워킹 및 보안 > 도구 > 포트 미러링 세션**을 선택합니다.
- 4 **추가**를 클릭하고 세션 유형을 선택합니다.

사용 가능한 유형은 **로컬 SPAN**, **원격 SPAN**, **원격 L3 SPAN** 및 **논리적 SPAN**입니다.

- 5 세션 이름과 설명(선택 사항)을 입력합니다.
- 6 추가 매개 변수를 제공합니다.

세션 유형	매개 변수
로컬 SPAN	<ul style="list-style-type: none"> ■ 전송 노드 - 전송 노드를 선택합니다. ■ 방향 - 양방향, 수신 또는 송신을 선택합니다. ■ 패킷 잘림 - 패킷 잘림 값을 선택합니다.
원격 SPAN	<ul style="list-style-type: none"> ■ 세션 유형 - RSPAN 소스 세션 또는 RSPAN 대상 세션을 선택합니다. ■ 전송 노드 - 전송 노드를 선택합니다. ■ 방향 - 양방향, 수신 또는 송신을 선택합니다. ■ 패킷 잘림 - 패킷 잘림 값을 선택합니다. ■ VLAN ID 캡슐화 - 캡슐화 VLAN ID를 지정합니다. ■ 원본 VLAN 유지 - 원본 VLAN ID 유지 여부를 선택합니다.
원격 L3 SPAN	<ul style="list-style-type: none"> ■ 캡슐화 - GRE, ERSPAN 2, 또는 ERSPAN 3를 선택합니다. ■ GRE 키 - 캡슐화가 GRE인 경우 GRE 키를 지정합니다. ERSPAN ID - 캡슐화가 ERSPAN 2 또는 ERSPAN 3인 경우 ERSPAN ID를 지정합니다. ■ 방향 - 양방향, 수신 또는 송신을 선택합니다. ■ 패킷 잘림 - 패킷 잘림 값을 선택합니다.
논리적 SPAN	<ul style="list-style-type: none"> ■ 논리적 스위치 - 논리적 스위치를 선택합니다. ■ 방향 - 양방향, 수신 또는 송신을 선택합니다. ■ 패킷 잘림 - 패킷 잘림 값을 선택합니다.

- 7 다음을 클릭합니다.
- 8 소스 정보를 제공합니다.

세션 유형	매개 변수
로컬 SPAN	<ul style="list-style-type: none"> ■ N-VDS를 선택합니다. ■ 물리적 인터페이스를 선택합니다. ■ 캡슐화된 패킷을 사용하거나 사용하지 않도록 설정합니다. ■ 가상 시스템을 선택합니다. ■ 가상 인터페이스를 선택합니다.
원격 SPAN	<ul style="list-style-type: none"> ■ 가상 시스템을 선택합니다. ■ 가상 인터페이스를 선택합니다.
원격 L3 SPAN	<ul style="list-style-type: none"> ■ 가상 시스템을 선택합니다. ■ 가상 인터페이스를 선택합니다. ■ 논리적 스위치를 선택합니다.
논리적 SPAN	<ul style="list-style-type: none"> ■ 논리적 포트를 선택합니다.

- 9 다음을 클릭합니다.

10 대상 정보를 제공합니다.

세션 유형	매개 변수
로컬 SPAN	<ul style="list-style-type: none"> ■ 가상 시스템을 선택합니다. ■ 가상 인터페이스를 선택합니다.
원격 SPAN	<ul style="list-style-type: none"> ■ N-VDS를 선택합니다. ■ 물리적 인터페이스를 선택합니다.
원격 L3 SPAN	<ul style="list-style-type: none"> ■ IPv4 주소를 지정합니다.
논리적 SPAN	<ul style="list-style-type: none"> ■ 논리적 포트를 선택합니다.

11 저장을 클릭합니다.

포트 미러링 세션을 저장한 후에는 소스나 대상을 변경할 수 없습니다.

포트 미러링 세션에 대한 필터 구성

포트 미러링 세션에 대한 필터를 구성하여 미러링되는 데이터의 양을 제한할 수 있습니다.

이 기능에는 다음과 같은 기능 및 제한 사항이 있습니다.

- ESXi 및 KVM 호스트 전송 노드만 지원됩니다.
- 소스 및 대상에 대해 IP 주소, IP 접두사 및 IP 범위가 지원됩니다.
- 소스 또는 대상에 대한 IPSet가 지원되지 않습니다.
- ESXi 또는 KVM에서 미러 통계는 지원되지 않습니다.

API를 사용하여 필터를 구성해야 합니다. NSX Manager UI 사용은 지원되지 않습니다. 포트 미러링 API 및 PortMirroringFilter 스키마에 대한 자세한 내용은 "NSX-T Data Center API 참조" 를 참조하십시오.

절차

- 1 NSX Manager UI 또는 API를 사용하여 포트 미러링 세션을 구성합니다.
- 2 포트 미러링 세션에 대한 정보를 얻으려면 GET /api/v1/mirror-sessions API를 호출합니다.
- 3 하나 이상의 필터를 추가하려면 GET /api/v1/mirror-sessions/<mirror-session-id> API를 호출합니다. 예를 들면 다음과 같습니다.

```
PUT https://<nsx-mgr>/api/v1/mirror-sessions/e57e8b2d-3047-4550-b230-dd1ee0e10b49
{
  "resource_type": "PortMirroringSession",
  "id": "e57e8b2d-3047-4550-b230-dd1ee0e10b49",
  "display_name": "port-mirror-session-1",
  "description": "Pnic port mirror session 1",
  "mirror_sources": [
    {
      "resource_type": "LogicalPortMirrorSource",
      "port_ids": [
```

```

        "6a361832-43e4-430d-a48a-b84a6cba73c3"
    ]
}
],
"mirror_destination": {
    "resource_type": "LogicalPortMirrorDestination",
    "port_ids": [
        "3e42e8b2d-3047-4550-b230-ddlee0e10b34"
    ]
},
"port_mirroring_filters": [
    {
        "filter_action": "MIRROR",
        "src_ips": {
            "ip-addresses": [
                "192.168.175.250",
                "2001:bd6::c:2957:160:126"
            ]
        }
        "dst_ips": {
            "ip-addresses": [
                "192.168.160.126",
                "2001:bd6::c:2957:175:250"
            ]
        }
    }
}
"session_type": "LogicalPortMirrorSession",
"preserve_original_vlan": false,
"direction": "BIDIRECTIONAL",
"_revision": 0
}

```

- 4 (선택 사항) `get mirroring-session <session-number>` CLI 명령을 호출하여 필터를 포함한 포트 미러링 세션의 속성을 표시할 수 있습니다.

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 사용하는 경우 [NSX Cloud](#)에서 지원되는 NSX-T Data Center 기능에서 자동 생성된 논리적 엔티티, 지원되는 기능 및 NSX Cloud에 필요한 구성 목록을 확인하십시오.

이 기능은 RFC 7011 및 RFC 7012에 지정된 표준과 호환됩니다.

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.

스위치 IPFIX 수집기 구성

스위치의 IPFIX 수집기를 구성할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 도구 > IPFIX**를 선택합니다.
- 3 **스위치 IPFIX 수집기** 탭을 클릭합니다.
- 4 **추가**를 클릭하여 수집기를 추가합니다.
- 5 이름과 설명(선택 사항)을 입력합니다.
- 6 **추가**를 클릭하고 수집기의 IP 주소와 포트를 입력합니다.
최대 4개의 수집기를 추가할 수 있습니다.
- 7 **추가**를 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 **고급 네트워킹 및 보안 > 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. 참고 전역 프로파일을 생성하려면 프로파일 이름을 Global 로 지정합니다. 전역 프로파일은 UI에서 편집하거나 삭제할 수 없으며 NSX-T Data Center API를 통해 이러한 작업을 수행할 수 있습니다.
활성 시간 초과(초)	흐름과 연결된 추가 패킷이 수신되는 경우라도 흐름이 시간 초과되기까지의 시간입니다. 기본값은 300입니다.
유휴 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.
오버레이 흐름 내보내기	샘플 결과에 오버레이 흐름 정보가 포함되는지 여부를 제어하는 설정입니다.
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 **추가**를 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 **고급 네트워킹 및 보안 > 도구 > IPFIX**를 선택합니다.
- 3 **방화벽 IPFIX 수집기** 탭을 클릭합니다.

- 4 **추가**를 클릭하여 수집기를 추가합니다.
- 5 이름과 설명(선택 사항)을 입력합니다.
- 6 **추가**를 클릭하고 수집기의 IP 주소와 포트를 입력합니다.
최대 4개의 수집기를 추가할 수 있습니다.
- 7 **추가**를 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 **고급 네트워킹 및 보안 > 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. 참고 전역 프로파일을 생성하려면 프로파일 이름을 Global 로 지정합니다. 전역 프로파일은 UI에서 편집하거나 삭제할 수 없으며 NSX-T Data Center API를 통해 이러한 작업을 수행할 수 있습니다.
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 **추가**를 클릭합니다.

ESXi IPFIX 템플릿

ESXi 호스트 전송 노드는 8개의 논리적 스위치 IPFIX 흐름 템플릿과 두 개의 분산 방화벽 IPFIX 흐름 템플릿을 지원합니다.

다음 표에는 논리적 스위치 IPFIX 패킷의 VMware 관련 요소가 나와 있습니다.

요소 ID	매개 변수 이름	데이터 유형	단위
880	tenantProtocol	unsigned8	1바이트
881	tenantSourceIPv4	ipv4Address	4바이트
882	tenantDestIPv4	ipv4Address	4바이트
883	tenantSourceIPv6	ipv6Address	16바이트
884	tenantDestIPv6	ipv6Address	16바이트
886	tenantSourcePort	unsigned16	2바이트
887	tenantDestPort	unsigned16	2바이트
888	egressInterfaceAttr	unsigned16	2바이트
889	vxlانExportRole	unsigned8	1바이트
890	ingressInterfaceAttr	unsigned16	2바이트
898	virtualObsID	string	가변 길이

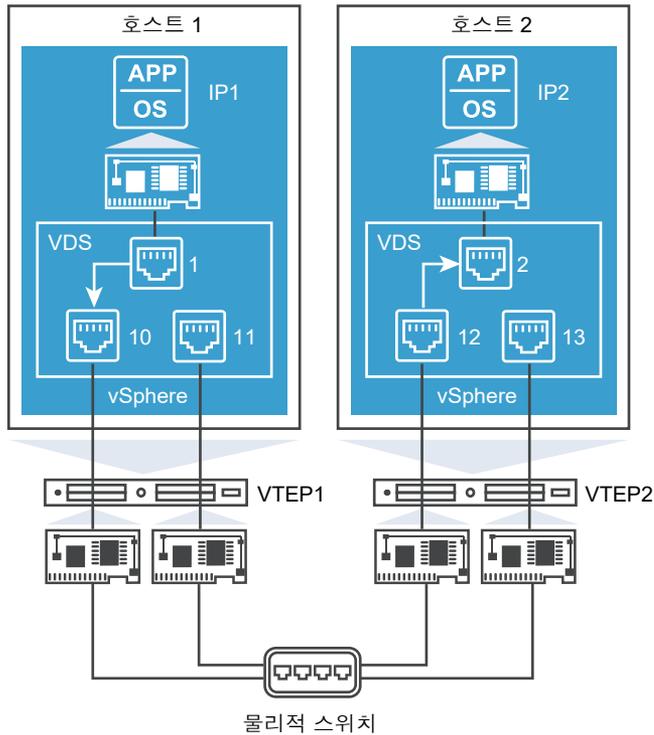
다음 표에는 분산 방화벽 IPFIX 패킷의 VMware 관련 요소가 나와 있습니다.

요소 ID	매개 변수 이름	데이터 유형	단위
950	ruleId	Unsigned32	4바이트
951	vmUuid	string	16바이트
952	vnicIndex	Unsigned32	4바이트
953	sessionFlags	unsigned8	1바이트
954	flowDirection	unsigned8	1바이트
955	algControlFlowId	unsigned64	8바이트
956	algType	unsigned8	1바이트
957	algFlowType	unsigned8	1바이트
958	averageLatency	Unsigned32	4바이트
959	retransmissionCount	Unsigned32	4바이트
960	vifUuid	octetArray	16바이트
961	vifId	string	가변 길이

ESXi 논리적 스위치 IPFIX 템플릿

ESXi 호스트 전송 노드는 8개의 논리적 스위치 IPFIX 흐름 템플릿을 지원합니다.

다음 다이어그램은 IPFIX 기능으로 모니터링되는 ESXi 호스트에 연결된 VM 간의 트래픽 흐름을 보여 줍니다.



IPv4 캡슐화 템플릿에는 다음 요소가 포함됩니다.

- 표준 요소
- SrcAddr: VTEP1
- DstAddr: VTEP2
- tenantSourceIPv4: IP1
- tenantDestIPv4: IP2
- tenantSourcePort: 10000
- tenantDestPort: 80
- tenantProtocol: TCP
- ingressInterfaceAttr: 0x03(터널 포트)
- egressInterfaceAttr: 0x01
- encapExportRole: 01
- virtualObsID: 89fd5032-2dc9-4fc3-993a-9bb4b616de54(논리적 포트 ID)

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()
```

ESXi 분산 방화벽 IPFIX 템플릿

ESXi 호스트 전송 노드는 2개의 분산 방화벽 IPFIX 흐름 템플릿을 지원합니다.

IPv4 템플릿

템플릿 ID: 288

```
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(icmpTypeIPv4, 1)
IPFIX_TEMPLATE_FIELD(icmpCodeIPv4, 1)
IPFIX_TEMPLATE_FIELD(flowStartSeconds, 4)
IPFIX_TEMPLATE_FIELD(flowEndSeconds, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(firewallEvent, 1)
IPFIX_TEMPLATE_FIELD(direction, 1)
IPFIX_TEMPLATE_FIELD(ruleId, 4)
```

```

IPFIX_TEMPLATE_FIELD(vifUuid,16)
IPFIX_TEMPLATE_FIELD(sessionFlags,1)
IPFIX_TEMPLATE_FIELD(flowDirection,1)
IPFIX_TEMPLATE_FIELD(flowId,8)
IPFIX_TEMPLATE_FIELD(algControlFlowId,8)
IPFIX_TEMPLATE_FIELD(algType,1)
IPFIX_TEMPLATE_FIELD(algFlowType,1)
IPFIX_TEMPLATE_FIELD(averageLatency,4)
IPFIX_TEMPLATE_FIELD(retransmissionCount,4)

```

IPv6 템플릿

템플릿 ID: 289

```

IPFIX_TEMPLATE_FIELD(sourceIPv6Address,16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address,16)
IPFIX_TEMPLATE_FIELD(sourceTransportPort,2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort,2)
IPFIX_TEMPLATE_FIELD(protocolIdentifier,1)
IPFIX_TEMPLATE_FIELD(icmpTypeIPv6,1)
IPFIX_TEMPLATE_FIELD(icmpCodeIPv6,1)
IPFIX_TEMPLATE_FIELD(flowStartSeconds,4)
IPFIX_TEMPLATE_FIELD(flowEndSeconds,4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(firewallEvent,1)
IPFIX_TEMPLATE_FIELD(direction,1)
IPFIX_TEMPLATE_FIELD(ruleId,4)
IPFIX_TEMPLATE_FIELD(vifUuid,16)
IPFIX_TEMPLATE_FIELD(sessionFlags,1)
IPFIX_TEMPLATE_FIELD(flowDirection,1)
IPFIX_TEMPLATE_FIELD(flowId,8)
IPFIX_TEMPLATE_FIELD(algControlFlowId,8)
IPFIX_TEMPLATE_FIELD(algType,1)
IPFIX_TEMPLATE_FIELD(algFlowType,1)
IPFIX_TEMPLATE_FIELD(averageLatency,4)
IPFIX_TEMPLATE_FIELD(retransmissionCount,4)

```

KVM IPFIX 템플릿

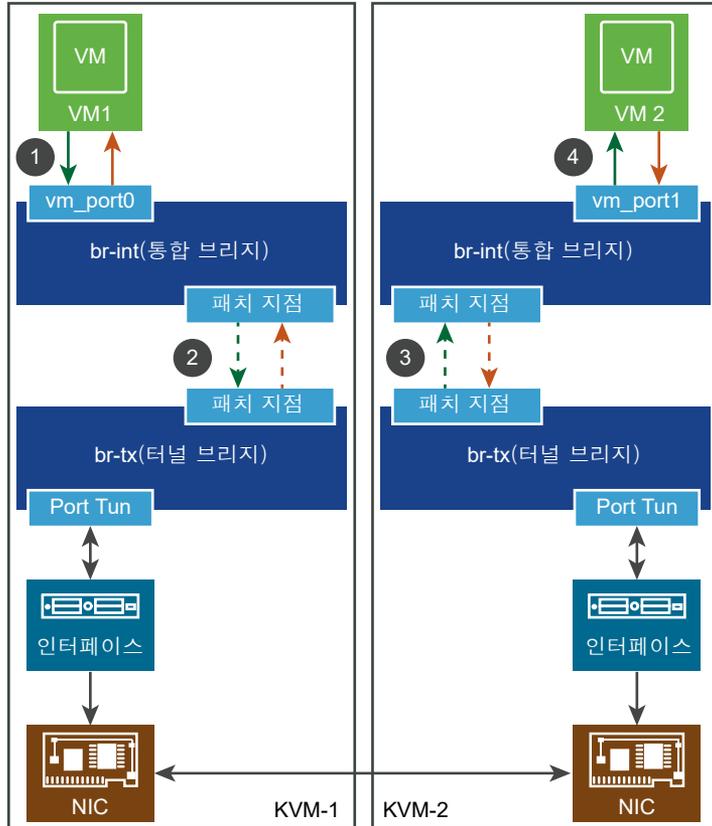
KVM 호스트 전송 노드는 88개의 IPFIX 흐름 템플릿 및 하나의 옵션 템플릿을 지원합니다.

다음 표에는 KVM IPFIX 패킷의 VMware 관련 요소가 나와 있습니다.

요소 ID	매개 변수 이름	데이터 유형	단위
891	tunnelType	unsigned8	1바이트
892	tunnelKey	바이트	가변 길이
893	tunnelSourceIPv4Address	Unsigned32	4바이트
894	tunnelDestinationIPv4Address	Unsigned32	4바이트
895	tunnelProtocolIdentifier	unsigned8	1바이트

요소 ID	매개 변수 이름	데이터 유형	단위
896	tunnelSourceTransportPort	unsigned16	2바이트
897	tunnelDestinationTransportPort	unsigned16	2바이트
898	virtualObsID	string	가변 길이

다음 다이어그램은 IPFIX 기능으로 모니터링되는 KVM 호스트에 연결된 VM 간의 트래픽 흐름을 보여 줍니다.



KVM IPv4 IPFIX 수신 템플릿에는 다음 요소가 포함됩니다.

- 표준 요소
- virtualObsID: 6d876a1c-e0ac-4bcf-85ee-bdd42fa7ba34(논리적 포트 ID)

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.

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 연결의 내용을 참조하십시오.

절차

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

2 **고급 네트워킹 및 보안 > 네트워킹 > 스위칭 > 포트** 선택

3 포트의 이름을 클릭합니다.

4 **모니터** 탭을 클릭합니다.

포트 상태 및 통계가 표시됩니다.

5 호스트에서 학습한 MAC 주소의 CSV 파일을 다운로드하려면 **MAC 테이블 다운로드**를 클릭합니다.

6 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 이해의 내용을 참조하십시오.

고급 네트워킹 및 보안 탭에서 논리적 스위치 및 관련 개체를 구성할 수 있습니다. 논리적 스위치는 기본 하드웨어에서 분리된 가상 환경에서 스위칭 기능, 브로드캐스트, 알 수 없는 유니캐스트, 멀티캐스트(BUM) 트래픽을 재현합니다.

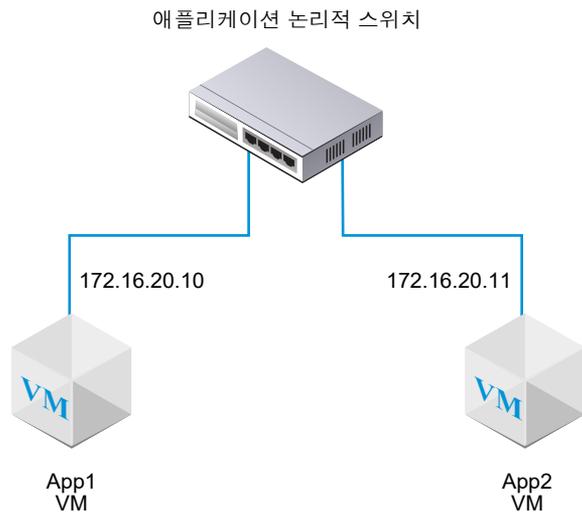
참고 고급 네트워킹 및 보안 사용자 인터페이스를 사용하여 정책 인터페이스에서 생성된 개체를 수정하는 경우 일부 설정을 구성하지 못할 수 있습니다. 이러한 읽기 전용 설정에는 옆에 ⊖ 아이콘이 있습니다. 자세한 내용은 [장 1 NSX Manager 개요](#) 항목을 참조하십시오.

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 13-1. 논리적 스위치 토폴로지



예를 들어 위의 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.

NSX Cloud 참고 NSX Cloud를 사용하는 경우 NSX Cloud에서 지원되는 NSX-T Data Center 기능에서 자동 생성된 논리적 엔티티, 지원되는 기능 및 NSX Cloud에 필요한 구성 목록을 확인하십시오.

본 장은 다음 항목을 포함합니다.

- BUM 프레임 복제 모드 이해
- 논리적 스위치 생성
- VM을 논리적 스위치에 연결
- 논리적 스위치 포트 생성
- 계층 2 연결 테스트
- NSX Edge 업링크에 대한 VLAN 논리적 스위치 생성
- 논리적 스위치 및 논리적 포트에 대한 스위칭 프로파일
- 향상된 네트워킹 스택
- 계층 2 브리징

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 플러딩에 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 생각해봅니다. 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 13 논리적 스위치 및 BUM 프레임 복제 모드](#) 이해를 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 스위칭 > 스위치 > 추가**를 선택합니다.
- 3 논리적 스위치 이름 및 필요한 경우 설명을 입력합니다.
- 4 논리적 스위치에 대한 전송 영역을 선택합니다.
동일한 전송 영역에 있는 논리적 스위치에 연결된 VM은 서로 통신할 수 있습니다.
- 5 업링크 팀 구성 정책의 이름을 입력합니다.
- 6 **관리 상태를 실행** 또는 **종료**로 설정합니다.
- 7 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.

- 8 (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.
- 9 (선택 사항) **스위칭 프로파일** 탭을 클릭하고 스위칭 프로파일을 선택합니다.
- 10 **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.

VM을 논리적 스위치에 연결

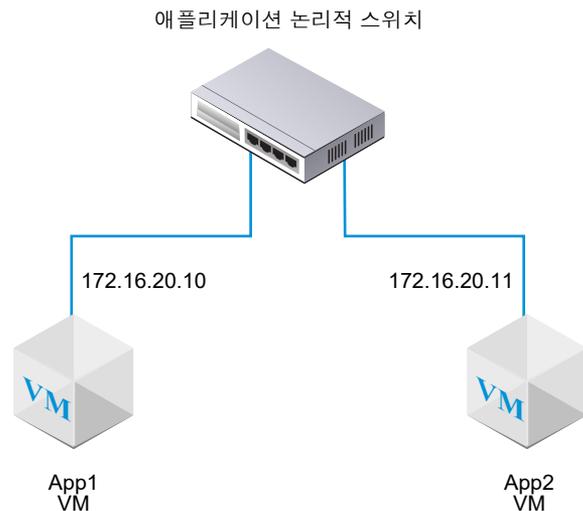
호스트에 따라 VM을 논리적 스위치에 연결하기 위한 구성이 다를 수 있습니다.

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 연결를 참조하십시오.

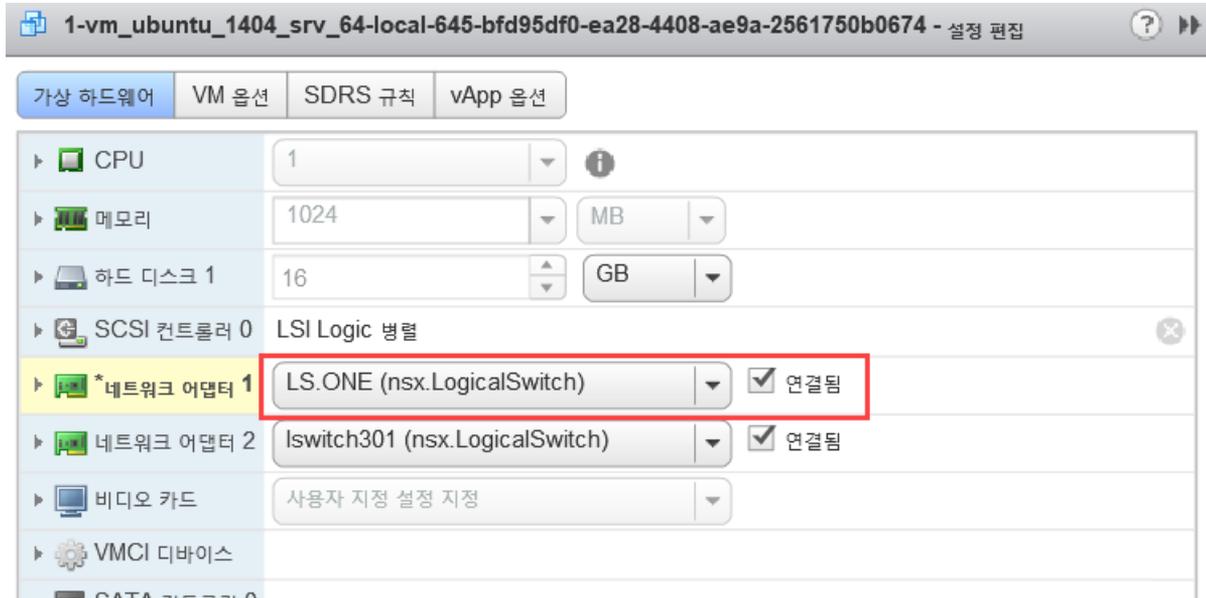
사전 요구 사항

- 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. **고급 네트워킹 및 보안 > 네트워킹 > 스위칭 > 포트**의 NSX Manager에서 논리적 스위치 포트 및 VIF 첨부 파일 ID를 볼 수 있습니다.

GET <https://<mgr-ip>/api/v1/logical-ports/> API 호출을 사용하여 해당 VIF 첨부 파일 ID에 대한 포트 세부 정보 및 관리자 상태를 봅니다. 작동 상태를 보려면 적절한 논리적 포트 ID를 사용해서 <https://<mgr-ip>/api/v1/logical-ports/<logical-port-id>/status> API 호출을 수행합니다.

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

다음에 수행할 작업

논리적 라우터를 추가합니다.

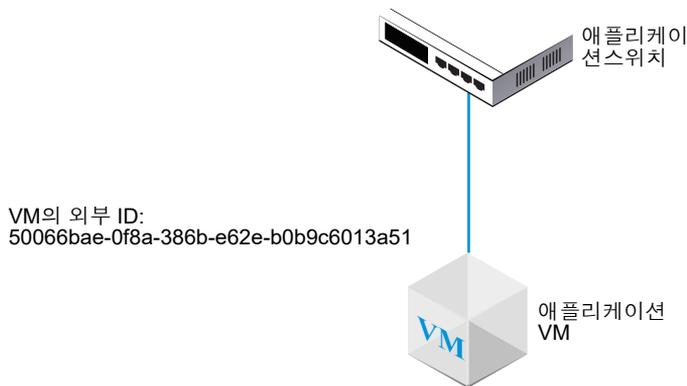
논리적 스위치 포트에서의 활동을 모니터링하여 문제를 해결할 수 있습니다. 자세한 내용은 "NSX-T Data Center 관리 가이드"의 "논리적 스위치 포트 활동 모니터링"을 참조하십시오.

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



사전 요구 사항

- VM은 NSX-T Data Center 팩브릭에 추가된 하이퍼바이저에 호스팅되어야 합니다.
- 팩브릭 노드는 NSX-T Data Center 관리부(MPA) 및 NSX-T Data Center 제어부(LCP)에 연결할 수 있어야 합니다.
- 팩브릭 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.

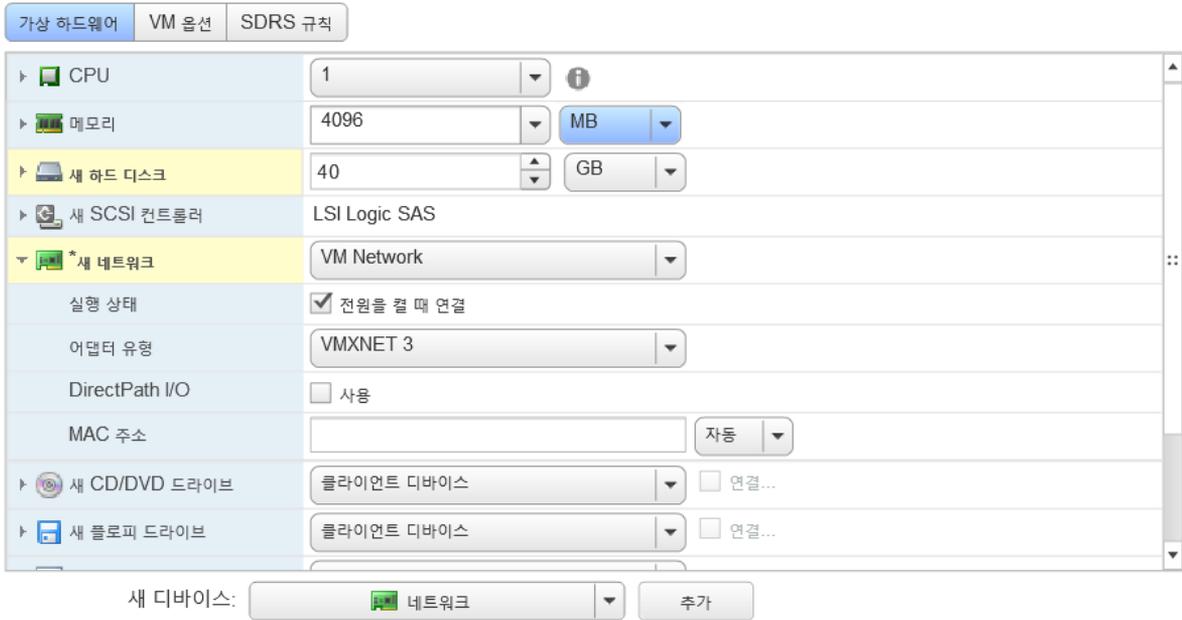
절차

- 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.



- 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": [
    "instanceUuid:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "moIdOnHost:5",
    "externalId:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "hostLocalId:5",
    "locationId:564dc020-1565-e3f4-f591-ee3953eef3ff",
    "biosUuid:4206f47d-fef7-08c5-5bf7-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 **고급 네트워킹 및 보안 > 네트워킹 > 스위칭 > 포트**에서 VM의 externalId와 일치하는 VIF 연결 ID를 찾은 후 관리 및 작업 상태가 [실행 중]/[실행 중]인지 확인합니다.

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

다음에 수행할 작업

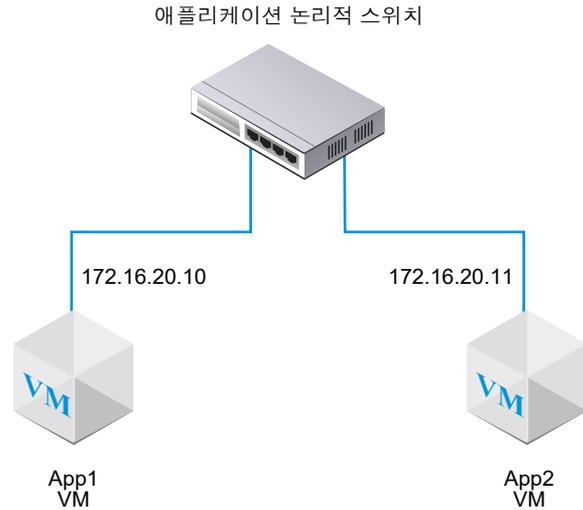
논리적 라우터를 추가합니다.

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 **고급 네트워킹 및 보안 > 네트워킹 > 스위칭 > 포트**에서 VIF 연결 ID를 찾고 관리 및 작동 상태가 둘 다 [실행 중]인지 확인합니다.

두 VM이 동일한 논리적 스위치에 연결되어 있고 동일한 서브넷에 IP 주소가 구성된 경우 서로 간에 ping 할 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.

논리적 스위치 포트 생성

논리적 스위치에는 여러 스위치 포트가 있습니다. 논리적 스위치 포트에서는 다른 네트워크 구성 요소, VM 또는 컨테이너를 논리적 스위치에 연결합니다.

vCenter Server에서 관리하는 ESXi 호스트에서 VM을 논리적 스위치에 연결하는 경우 논리적 스위치 포트가 자동으로 생성됩니다. VM을 논리적 스위치에 연결하는 방법에 대한 자세한 내용은 [VM을 논리적 스위치에 연결](#) 항목을 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.

논리적 스위치 포트의 작업을 모니터링하려면 [논리적 스위치 포트 활동 모니터링](#) 항목을 참조하십시오.

사전 요구 사항

논리적 스위치가 생성되었는지 확인합니다. [장 13 논리적 스위치](#) 항목을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 스위칭 > 포트 > 추가**를 선택합니다.
- 3 **일반** 탭에서 포트 세부 정보를 완료합니다.

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

API를 사용하여 연결 유형을 추가 값(LOGICALROUTER, BRIDGEENDPOINT, DHCP_SERVICE, METADATA_PROXY, L2VPN_SESSION)으로 설정할 수 있습니다. 연결 유형이 DHCP 서비스, 메타데이터 프록시 또는 L2 VPN 세션인 경우 포트에 대한 스위칭 프로파일이 기본 프로파일이 되어야 합니다. 사용자 정의 프로파일은 사용할 수 없습니다.

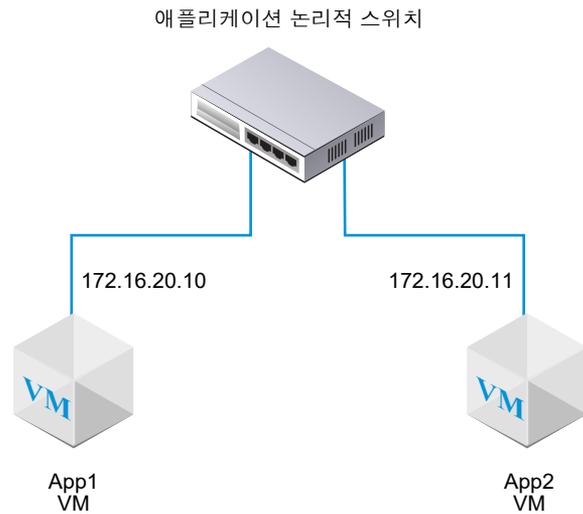
- 4 (선택 사항) **스위칭 프로파일** 탭에서 스위칭 프로파일을 선택합니다.
- 5 **저장**을 클릭합니다.

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 13-2. 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 **고급 네트워킹 및 보안 > 네트워킹 > 스위칭 > 스위치**를 선택합니다.

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

명령	설명
<pre>get logical-switch <VNI 또는 UUID> arp-table</pre>	<p>지정된 논리적 스위치에 대한 ARP 테이블을 표시합니다. 샘플 출력</p> <pre>nsx-manager1> get logical-switch 41866 arp-table VNI IP MAC Connection-ID 41866 172.16.20.11 00:50:56:b1:70:5e 295422</pre>
<pre>get logical-switch <VNI 또는 UUID> connection-table</pre>	<p>지정된 논리적 스위치에 대한 연결을 표시합니다. 샘플 출력</p> <pre>nsx-manager1> 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>
<pre>get logical-switch <VNI 또는 UUID> mac-table</pre>	<p>지정된 논리적 스위치에 대한 MAC 테이블을 표시합니다. 샘플 출력</p> <pre>nsx-manager1> 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>
<pre>get logical-switch <VNI 또는 UUID> stats</pre>	<p>지정된 논리적 스위치에 대한 통계 정보를 표시합니다. 샘플 출력</p> <pre>nsx-manager1> 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>
<pre>get logical-switch <VNI 또는 UUID> stats-sample</pre>	<p>시간에 따른 모든 논리적 스위치 통계의 요약을 표시합니다. 샘플 출력</p> <pre>nsx-manager1> 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>

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>
<pre>get logical-switch <VNI 또는 UUID> vtep</pre>	<p>지정된 논리적 스위치와 관련된 모든 가상 터널 끝점을 표시합니다. 샘플 출력</p> <pre>nsx-manager1> 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>

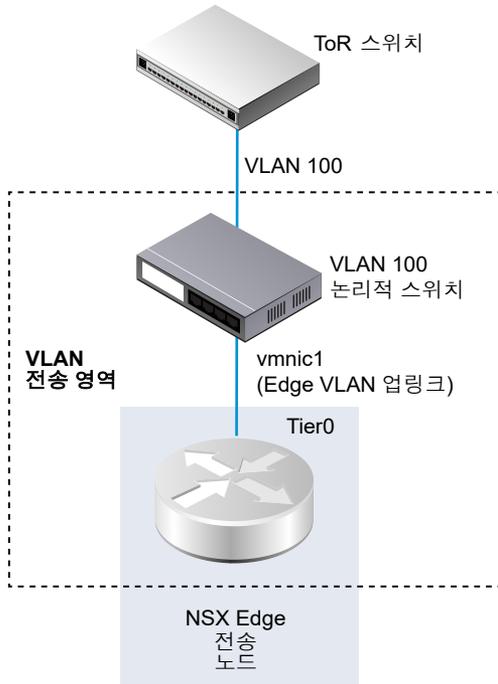
결과

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

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 하이퍼바이저 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
    
```

- 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 고급 네트워킹 및 보안 > 네트워킹 > 스위칭 > 스위치 > 추가를 선택합니다.
- 3 논리적 스위치의 이름을 입력합니다.
- 4 논리적 스위치에 대한 전송 영역을 선택합니다.
- 5 업링크 팀 구성 정책을 선택합니다.
- 6 관리 상태의 경우 **실행** 또는 **종료**를 선택합니다.
- 7 VLAN ID를 입력합니다.

물리적 TOR로의 업링크에 대한 VLAN ID가 없으면 VLAN 필드에 0을 입력합니다.

- 8 (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.

논리적 스위치 및 논리적 포트에 대한 스위칭 프로파일

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)
- 포트 미러링
- 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.

기본 프로파일을 사용하기 전에 프로파일에 필요한 설정을 확인합니다. 사용자 지정 프로파일을 생성할 때 일부 설정에는 기본값이 있습니다. 기본 프로파일에서 이러한 설정에 기본값이 사용되지 않습니다.

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 정의의 스위칭 프로파일을 연결합니다. 하위 논리적 포트는 상위 논리적 스위치에서 기본 시스템 정의의 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.

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 **고급 네트워킹 및 보안 > 네트워킹 > 스위칭 > 스위칭 프로파일 > 추가** 선택

3 QoS를 선택하고 QoS 스위칭 프로파일 세부 정보 입력을 완료합니다.

옵션	설명
이름 및 설명	<p>사용자 지정 QoS 스위칭 프로파일에 이름을 할당합니다.</p> <p>필요한 경우 프로파일에서 수정한 설정에 대한 설명을 입력할 수 있습니다.</p>
모드	<p>[모드] 드롭다운 메뉴에서 신뢰함 또는 신뢰하지 않음 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>참고 DSCP 설정은 터널링된 트래픽에서만 작동합니다. 이러한 설정은 동일한 하이퍼바이저 내의 트래픽에는 적용되지 않습니다.</p>
우선 순위	<p>DSCP 값을 설정합니다.</p> <p>우선 순위 값의 범위는 0~63입니다.</p>
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 네트워크로의 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 크기는 대역폭이 최대인 기간을 기준으로 결정됩니다. 버스트 크기 설정에서 버스트 기간을 설정합니다. 대역폭은 보장할 수 없습니다. 그러나 평균, 최대 크기 및 버스트 크기 설정을 사용하여 네트워크 대역폭을 제한할 수 있습니다.</p> <p>예를 들어, 평균 대역폭이 30Mbps이고 최대 대역폭이 60Mbps이고 허용된 기간이 0.1초이면 버스트 크기는 $60 * 1000000 * 0.10/8 = 750000$바이트입니다.</p> <p>기본값은 0이며, 수신 트래픽에 대한 속도 제한이 사용되지 않도록 설정됩니다.</p>

옵션	설명
수신 브로드캐스트	<p>브로드캐스트를 기준으로 VM에서 논리적 네트워크로의 아웃바운드 네트워크 트래픽에 대한 사용자 지정 값을 설정합니다.</p> <p>브로드캐스트를 기준으로 VM에서 논리적 네트워크로의 아웃바운드 네트워크 트래픽에 대한 사용자 지정 값을 설정합니다. 예를 들어, 논리적 스위치에 대한 평균 대역폭을 3,000Kbps로 설정하고, 최대 대역폭이 6,000Kbps이고, 허용되는 기간은 0.1초이면 버스트 크기는 $6000 * 1000 * 0.10/8 = 75,000$바이트입니다.</p> <p>기본값은 0이며, 수신 브로드캐스트 트래픽에 대한 속도 제한이 사용되지 않도록 설정됩니다.</p>
송신	<p>논리적 네트워크에서 VM으로의 인바운드 네트워크 트래픽에 대한 사용자 지정 값을 설정합니다.</p> <p>기본값은 0이며, 송신 트래픽에 대한 속도 제한이 사용되지 않도록 설정됩니다.</p>

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

4 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 연결의 내용을 참조하십시오.

포트 미러링 스위칭 프로파일 이해

논리적 포트 미러링을 사용하면 VM VIF 포트에 연결된 논리적 스위치 포트에 들어오거나 이러한 포트에서 나가는 모든 트래픽을 복제하고 리디렉션할 수 있습니다. 미러링된 트래픽은 수집기에 대한 GRE(Generic Routing Encapsulation) 터널 내에서 캡슐화되어 전송되므로 네트워크에서 원격 대상으로 이동하는 동안 모든 원본 패킷 정보가 유지됩니다.

포트 미러링은 문제 해결에만 사용하는 것이 좋습니다.

참고 포트 미러링은 더 장기적으로 사용할 때 성능에 영향을 미치므로 모니터링에 권장되지 않습니다.

물리적 포트 미러링과 비교할 때 논리적 포트 미러링은 모든 VM 네트워크 트래픽이 캡처되도록 합니다. 물리적 네트워크에서만 포트 미러링을 구현하는 경우 일부 VM 네트워크 트래픽이 미러링되지 못합니다. 이는 동일한 호스트에 상주하는 VM 간 통신이 물리적 네트워크로 들어가지 못하므로 미러링되지 않기 때문입니다. 논리적 포트 미러링을 사용할 경우 해당 VM이 다른 호스트로 마이그레이션되더라도 VM 트래픽을 계속 미러링할 수 있습니다.

포트 미러링 프로세스는 NSX-T Data Center 도메인의 VM 포트와 물리적 애플리케이션의 포트 둘 다에서 비슷합니다. 논리적 네트워크에 연결된 워크로드에 의해 캡처된 트래픽을 전달하고 해당 트래픽을 수집기에 미러링할 수 있습니다. IP 주소는 VM이 호스팅된 게스트 IP 주소에서 연결 가능해야 합니다. 이 프로세스는 게이트웨이 노드에 연결된 물리적 애플리케이션에 대해서도 동일하게 적용됩니다.

사용자 지정 포트 미러링 스위칭 프로파일 구성

다른 대상 및 키 값을 사용하여 사용자 지정 포트 미러링 스위칭 프로파일을 생성할 수 있습니다.

사전 요구 사항

- 포트 미러링 스위칭 프로파일 개념을 숙지합니다. **포트 미러링 스위칭 프로파일 이해**의 내용을 참조하십시오.
- 네트워크 트래픽을 리디렉션하려는 대상 논리적 포트 ID의 IP 주소를 식별합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 스위칭 > 스위칭 프로파일 > 추가** 선택
- 3 **포트 미러링**을 선택하고 포트 미러링 스위칭 프로파일 세부 정보 입력을 완료합니다.

옵션	설명
이름 및 설명	사용자 지정 포트 미러링 스위칭 프로파일에 이름을 할당합니다. 필요한 경우 이 프로파일을 사용자 지정하기 위해 수정한 설정에 대한 설명을 입력할 수 있습니다.
방향	드롭다운 메뉴에서 옵션을 선택하여 수신 , 송신 또는 양방향 트래픽에 대해 이 소스를 사용합니다. 수신은 VM에서 논리적 네트워크로의 아웃바운드 네트워크 트래픽입니다. 송신은 논리적 네트워크에서 VM으로의 인바운드 네트워크 트래픽입니다. 양방향은 VM에서 논리적 네트워크로, 논리적 네트워크에서 VM으로의 양방향 트래픽입니다. 이는 기본 옵션입니다.
패킷 잘라내기 길이	선택 사항입니다. 범위는 60 - 65535입니다.
키	논리적 포트에서 미러링된 패킷을 식별하기 위한 임의의 32비트 값을 입력합니다. 이 [키] 값은 각 미러 패킷의 GRE 헤더에 있는 [키] 필드로 복사됩니다. [키] 값이 0으로 설정되면 기본 정의가 GRE 헤더에 있는 [키] 필드로 복사됩니다. 기본 32비트 값은 다음 값으로 구성됩니다. <ul style="list-style-type: none"> ■ 처음 24비트는 VNI 값입니다. VNI는 캡슐화된 프레임의 IP 헤더 부분입니다. ■ 25번째 비트는 처음 24비트가 유효한 VNI 값인지를 나타냅니다. 1이면 이 값이 유효하고, 0이면 유효하지 않습니다. ■ 26번째 비트는 미러링된 트래픽의 방향을 나타냅니다. 1은 수신 방향이고, 0은 송신 방향입니다. ■ 나머지 6개 비트는 사용되지 않습니다.
대상	미러링 세션에 대한 수집기의 대상 ID를 입력합니다. 대상 IP 주소 ID는 네트워크 내의 IPv4 주소 또는 NSX-T Data Center에서 관리되지 않는 원격 IPv4 주소만 될 수 있습니다. 최대 3개의 대상 IP 주소를 쉼표로 구분해서 추가할 수 있습니다.

- 4 **저장**을 클릭합니다.

결과

사용자 지정 포트 미러링 스위칭 프로파일은 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 연결의 내용을 참조하십시오.

사용자 지정된 포트 미러링 스위칭 프로파일이 작동하는지 확인합니다. 사용자 지정 포트 미러링 스위칭 프로파일 확인의 내용을 참조하십시오.

사용자 지정 포트 미러링 스위칭 프로파일 확인

사용자 지정 포트 미러링 스위칭 프로파일을 사용하기 전에 사용자 지정이 제대로 작동하는지 확인합니다.

사전 요구 사항

- 사용자 지정 포트 미러링 스위칭 프로파일이 구성되어 있는지 확인합니다. 사용자 지정 포트 미러링 스위칭 프로파일 구성의 내용을 참조하십시오.
- 사용자 지정된 포트 미러링 스위칭 프로파일이 논리적 스위치에 연결되어 있는지 확인합니다. 사용자 지정 프로파일을 논리적 스위치에 연결의 내용을 참조하십시오.

절차

- 1 포트 미러링에 대해 구성된 논리적 포트에 대해 VIF 연결이 설정된 2개의 VM을 찾습니다.

예를 들어 VM1 10.70.1.1 및 VM2 10.70.1.2에는 VIF 연결이 있으며 동일한 논리적 네트워크에 있습니다.

- 2 대상 IP 주소에 대해 tcpdump 명령을 실행합니다.

```
sudo tcpdump -n -i eth0 dst host 대상 IP 주소 and proto gre
```

예를 들어 대상 IP 주소는 10.24.123.196입니다.

- 3 첫 번째 VM에 로그인하고 두 번째 VM을 ping하여 해당 ECHO 요청 및 응답이 대상 주소에서 수신되는지 확인합니다.

다음에 수행할 작업

이 포트 미러링 사용자 지정 스위칭 프로파일을 논리적 스위치에 연결하여 스위칭 프로파일의 수정된 매개 변수를 네트워크 트래픽에 적용합니다. 사용자 지정 프로파일을 논리적 스위치에 연결의 내용을 참조하십시오.

IP 검색 스위칭 프로파일 이해

IP 검색은 DHCP 및 DHCPv6 스누핑, ARP(주소 확인 프로토콜) 스누핑, ND(Neighbor Discovery) 스누핑 및 VM Tools를 사용하여 MAC 및 IP 주소를 학습합니다.

검색된 MAC 및 IP 주소는 동일한 논리적 스위치에 연결된 VM 간의 트래픽을 최소화하는 ARP/ND 억제를 구현하는 데 사용됩니다. 이 주소는 SpoofGuard 및 DFw(분산 방화벽) 구성 요소에도 사용됩니다. DFw는 주소 바인딩을 사용하여 방화벽 규칙에 있는 개체의 IP 주소를 확인합니다.

DHCP/DHCPv6 스누핑은 DHCP/DHCPv6 클라이언트와 서버 간에 교환되는 DHCP/DHCPv6 패킷을 조사하여 IP 및 MAC 주소를 학습합니다.

ARP 스누핑은 VM의 송신 ARP 및 GARP(Gratuitous ARP) 패킷을 조사하여 IP 및 MAC 주소를 학습합니다.

VM Tools는 ESXi 호스팅 VM에서 실행되며 VM의 구성 정보(MAC 및 IP 또는 IPv6 주소 포함)를 제공할 수 있는 소프트웨어입니다. 이 IP 검색 방법은 ESXi 호스트에서 실행되는 VM에서만 사용할 수 있습니다.

ND 스누핑은 IPv6 형태의 ARP 스누핑입니다. NS(인접 라우터 요청) 및 NA(Neighbor Advertisement) 메시지를 조사하여 IP 및 MAC 주소를 학습합니다.

중복 주소 감지는 새로 검색된 IP 주소가 다른 포트에 대한 인식되는 바인딩 목록에 이미 있는지 여부를 확인합니다. 이 확인은 동일한 세그먼트의 포트에 대해 수행됩니다. 중복 주소가 감지되면 새로 검색된 주소는 검색된 목록에 추가되지만 인식되는 바인딩 목록에는 추가되지 않습니다. 모든 중복 IP에는 연결된 검색 타임 스탬프가 있습니다. 인식되는 바인딩 목록에 있는 IP가 바인딩 무시 목록에 추가되거나 스누핑을 사용하지 않도록 설정하여 제거되면 가장 오래된 타임스탬프가 있는 중복 IP가 인식되는 바인딩 목록으로 이동됩니다. 중복 주소 정보는 API 호출을 통해 사용할 수 있습니다.

기본적으로 검색 방법 ARP 스누핑과 ND 스누핑은 TOFU(최초 사용 시 신뢰)라는 모드에서 작동합니다. TOFU 모드에서 주소가 검색되고 인식되는 바인딩 목록에 추가되면 해당 바인딩은 인식되는 목록에 계속 남아 있게 됩니다. TOFU는 ARP/ND 스누핑을 사용하여 검색된 처음 'n'개의 고유한 <IP, MAC, VLAN> 바인딩에 적용됩니다. 여기서 'n'은 구성할 수 있는 바인딩 제한입니다. ARP/ND 스누핑에 대해 TOFU를 사용하지 않도록 설정할 수 있습니다. 그러면 이 메시드는 모든 사용(TOEU) 모드에서 신뢰 상태로 작동합니다. TOEU 모드에서 주소가 검색되면 인식되는 바인딩 목록에 추가되고, 삭제 또는 만료될 경우 인식되는 바인딩 목록에서 제거됩니다. DHCP 스누핑 및 VM Tools는 항상 TOEU 모드에서 작동합니다.

각 포트에 대해 NSX Manager는 포트에 바인딩할 수 없는 IP 주소를 포함하는 바인딩 무시 목록을 유지합니다. **고급 네트워킹 및 보안 > 스위칭 > 포트**로 이동한 후 포트를 선택하여 검색된 바인딩을 [바인딩 무시] 목록에 추가할 수 있습니다. 또한 기존의 검색되었거나 인식되는 바인딩을 **바인딩 무시**로 복사하여 삭제할 수도 있습니다.

참고 TOFU는 SpoofGuard와 동일하지 않으며 SpoofGuard와 같은 방식으로 트래픽을 차단하지 않습니다. 자세한 내용은 [SpoofGuard 세그먼트 프로파일 이해](#)를 참조하십시오.

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

NSX-T Data Center에는 여러 기본 IP 검색 스위칭 프로파일이 있습니다. 추가 항목을 생성할 수도 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 **고급 네트워킹 및 보안 > 네트워킹 > 스위칭 > 스위칭 프로파일 > 추가**를 선택합니다.
- 3 **IP 검색**을 선택하고 IP 검색 스위칭 프로파일 세부 정보를 지정합니다.

옵션	설명
이름 및 설명	이름과 설명(선택 사항)을 입력합니다.
ARP 스누핑	IPv4 환경의 경우, VM에 정적 IP 주소가 있는 경우에 해당합니다.
ARP 바인딩 제한	포트에 바인딩할 수 있는 최대 IPv4 IP 주소 수입니다. 허용되는 최소값은 1(기본값)이고 최대값은 256입니다.
ARP ND 바인딩 제한 시간 초과	TOFU가 사용되지 않도록 설정된 경우 ARP/ND 바인딩 테이블의 IP 주소에 대한 시간 초과 값(분)입니다. 주소 시간이 초과되면 새로 검색된 주소로 대체됩니다.
DHCP 스누핑	IPv4 환경의 경우, VM에 IPv4 주소가 있는 경우에 해당합니다.
DHCP V6 스누핑	IPv6 환경의 경우, VM에 IPv6 주소가 있는 경우에 해당합니다.
VM Tools	ESXi 호스팅 VM에만 사용할 수 있습니다.
IPv6용 VM Tools	ESXi 호스팅 VM에만 사용할 수 있습니다.
인접 항목 검색 스누핑	IPv6 환경의 경우, VM에 정적 IP 주소가 있는 경우에 해당합니다.
인접 항목 검색 바인딩 제한	포트에 바인딩할 수 있는 최대 IPv6 주소 수입니다.
최초 사용 시 신뢰	ARP 및 ND 스누핑에 적용됩니다.
중복 IP 감지	모든 스누핑 방법 및 IPv4 환경과 IPv6 환경의 경우.

- 4 **추가**를 클릭합니다.

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 기존 IP 주소를 변경하지 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 허용 목록은 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 허용 목록은 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 활성화하거나 비활성화하는 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 **고급 네트워킹 및 보안 > 네트워킹 > 스위칭 > 포트**를 선택합니다.
- 2 주소 바인딩을 적용하려는 논리적 포트를 클릭합니다.
논리적 포트 요약이 표시됩니다.
- 3 개요 탭에서 **주소 바인딩 > 수동 바인딩**을 확장합니다.
- 4 **추가**를 클릭합니다.
[주소 바인딩 추가] 대화상자가 표시됩니다.
- 5 주소 바인딩(IPv4 주소, IPv6 주소 또는 IPv6 서브넷)을 적용하려는 논리적 포트의 IP 및 MAC 주소를 지정합니다. 예를 들어, IPv6의 경우 2001::/64는 IPv6 서브넷이고 2001::1은 호스트 IP이고, 2001::1/64는 잘못된 입력입니다. VLAN ID를 지정할 수도 있습니다.
- 6 **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 **고급 네트워킹 및 보안 > 네트워킹 > 스위칭 > 스위칭 프로파일 > 추가**를 선택합니다.
- 3 **Spoof Guard**를 선택합니다.
- 4 이름과 설명(선택 사항)을 입력합니다.
- 5 포트 수준 SpoofGuard를 사용하도록 설정하려면 **포트 바인딩**을 **사용**으로 설정합니다.
- 6 **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 **고급 네트워킹 및 보안 > 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	BPDU 필터 버튼을 전환하여 BPDU 필터링을 사용하도록 설정합니다. 기본적으로 사용하지 않도록 설정됩니다. 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. BPDU 필터 목록에서 선택할 수 있도록 설정해야 합니다.
DHCP 필터	서버 차단 버튼 및 클라이언트 차단 버튼을 전환하여 DHCP 필터링을 사용하도록 설정합니다. 둘 다 기본적으로 사용하지 않도록 설정되어 있습니다. 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.

옵션	설명
DHCPv6 필터	<p>V6 서버 차단 버튼 및 V6 클라이언트 차단 버튼을 전환하여 DHCP 필터링을 사용하도록 설정합니다. 둘 다 기본적으로 사용하지 않도록 설정되어 있습니다.</p> <p>DHCPv6 서버 차단은 DHCPv6 서버에서 DHCPv6 클라이언트로의 트래픽을 차단합니다. DHCP 서버에서 DHCP 릴레이 에이전트로의 트래픽은 차단하지 않습니다. UDP 소스 포트 번호가 547인 패킷이 필터링됩니다.</p> <p>DHCPv6 클라이언트 차단은 DHCP 요청을 차단하여 VM이 DHCP IP 주소를 획득하지 못하게 합니다. UDP 소스 포트 번호가 546인 패킷이 필터링됩니다.</p>
비 IP 트래픽 차단	<p>비 IP 트래픽 차단 버튼을 전환하여 IPv4, IPv6, ARP 및 BPDU 트래픽만 허용합니다.</p> <p>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.</p>
RA 가드	<p>RA 가드 버튼을 전환하여 수신 IPv6 라우터 알림을 필터링합니다. ICMPv6 유형 134 패킷이 필터링됩니다. 이 옵션은 기본적으로 사용하도록 설정되어 있습니다.</p>
속도 제한	<p>브로드캐스트 및 멀티캐스트 트래픽에 대한 속도 제한을 설정합니다. 이 옵션은 기본적으로 사용하도록 설정되어 있습니다.</p> <p>속도 제한은 브로드캐스트 스톱과 같은 이벤트에서 논리적 스위치 또는 VM을 보호하는 데 사용될 수 있습니다.</p> <p>연결 문제를 방지하려면 최소 속도 제한 값을 10pps 이상으로 설정해야 합니다.</p>

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. VMware Integrated OpenStack을 사용하여 게스트 VM을 배포하는 경우를 제외하고 이 속성은 기본적으로 사용하지 않도록 설정됩니다.

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.

또한 MAC 학습은 알 수 없는 유니캐스트 플러딩을 지원합니다. 일반적으로 포트에서 수신된 패킷에 알 수 없는 대상 MAC 주소가 있으면 패킷이 삭제됩니다. 알 수 없는 유니캐스트 플러딩이 사용되도록 설정되면 포트는 MAC 학습 및 알 수 없는 유니캐스트 플러딩이 사용되도록 설정된 스위치의 모든 포트에 알 수 없는 유니캐스트 트래픽을 플러딩합니다. 이 속성은 기본적으로 사용되도록 설정되어 있지만 MAC 학습이 사용되도록 설정된 경우에만 사용할 수 있습니다.

학습할 수 있는 MAC 주소 수는 구성 가능합니다. 최대값은 4096(기본값)입니다. 제한에 도달하는 경우에 대해 이 정책을 설정할 수도 있습니다. 옵션은 다음과 같습니다.

- **삭제** - 알 수 없는 소스 MAC 주소의 패킷이 삭제됩니다. 이 MAC 주소로의 인바운드 패킷은 알 수 없는 유니캐스트로 처리됩니다. 포트는 알 수 없는 유니캐스트 플러딩을 사용하도록 설정한 경우에만 패킷을 수신합니다.
- **허용** - 주소가 학습되지 않더라도 알 수 없는 소스 MAC 주소의 패킷이 전달됩니다. 이 MAC 주소로의 인바운드 패킷은 알 수 없는 유니캐스트로 처리됩니다. 포트는 알 수 없는 유니캐스트 플러딩을 사용하도록 설정한 경우에만 패킷을 수신합니다.

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 **고급 네트워킹 및 보안 > 네트워킹 > 스위칭 > 스위칭 프로파일 > 추가**를 선택합니다.

3 MAC 관리를 선택하고 MAC 관리 프로파일 세부 정보 입력을 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. 기본값은 사용 안 함입니다.
상태	MAC 학습 기능을 사용하거나 사용하지 않도록 설정합니다. 기본값은 사용 안 함입니다.
알 수 없는 유니캐스트 플러딩	알 수 없는 유니캐스트 플러딩 기능을 사용하거나 사용하지 않도록 설정합니다. 기본값은 사용 안 함입니다. 이 옵션은 MAC 학습을 사용하도록 설정한 경우 사용할 수 있습니다.
MAC 제한	최대 MAC 주소 개수를 설정합니다. 기본값은 4096입니다. 이 옵션은 MAC 학습을 사용하도록 설정한 경우 사용할 수 있습니다.
MAC 제한 정책	허용 또는 삭제를 선택합니다. 기본값은 허용입니다. 이 옵션은 MAC 학습을 사용하도록 설정한 경우 사용할 수 있습니다.

4 추가를 클릭합니다.

다음에 수행할 작업

스위칭 프로파일을 논리적 스위치 또는 논리적 포트에 연결합니다. 사용자 지정 프로파일을 논리적 스위치에 연결 또는 사용자 지정 프로파일을 논리적 포트에 연결의 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 생성의 내용을 참조하십시오.
- 사용자 지정 스위칭 프로파일이 구성되어 있는지 확인합니다. 논리적 스위치 및 논리적 포트에 대한 스위칭 프로파일의 내용을 참조하십시오.

절차

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

- 2 고급 네트워킹 및 보안 > 네트워킹 > 스위칭 > 스위치를 선택합니다.
- 3 사용자 지정 스위칭 프로파일을 적용할 논리적 스위치를 클릭합니다.
- 4 관리 탭을 클릭합니다.
- 5 드롭다운 메뉴에서 사용자 지정 스위칭 프로파일 유형을 선택합니다.
 - QoS
 - 포트 미러링
 - IP 검색
 - SpoofGuard
 - 스위치 보안
 - MAC 관리
- 6 변경을 클릭합니다.
- 7 드롭다운 메뉴에서 이전에 생성한 사용자 지정 스위칭 프로파일을 선택합니다.
- 8 저장을 클릭합니다.

이제 논리적 스위치가 사용자 지정 스위칭 프로파일에 연결됩니다.
- 9 관리 탭 아래에 구성이 수정된 새로운 사용자 지정 스위칭 프로파일이 나타나는지 확인합니다.
- 10 (선택 사항) **관련** 탭을 클릭하고 드롭다운 메뉴에서 **포트**를 선택하여 사용자 지정 스위칭 프로파일이 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 연결의 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. **VM**을 논리적 스위치에 연결의 내용을 참조하십시오.
- 사용자 지정 스위칭 프로파일이 구성되어 있는지 확인합니다. 논리적 스위치 및 논리적 포트에 대한 스위칭 프로파일의 내용을 참조하십시오.

절차

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

이제 논리적 포트가 사용자 지정 스위칭 프로파일에 연결됩니다.
- 9 **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.

향상된 네트워킹 스택

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

ESXi 호스트에만 N-VDS 스위치를 고급 데이터 경로 모드로 구성할 수 있습니다. ENS는 Edge VM을 통과하는 트래픽도 지원합니다. 향상된 데이터 경로 모드에서는 오버레이 트래픽 및 VLAN 트래픽을 구성할 수 있습니다.

ENS 논리적 코어 자동 할당

논리적 코어를 vNIC에 자동으로 할당하여 전용 논리적 코어에서 vNIC에 대해 수신 트래픽 및 송신 트래픽을 관리하도록 합니다.

강화된 데이터 경로 모드로 구성된 N-VDS 스위치를 사용하면 단일 논리적 코어가 vNIC에 연결된 경우 논리적 코어는 vNIC로 들어오거나 vNIC에서 나가는 양방향 트래픽을 처리합니다. 여러 개의 논리적 코어가 구성된 경우 호스트는 vNIC 트래픽을 처리해야 하는 논리적 코어를 자동으로 결정합니다.

이러한 매개 변수 중 하나를 기준으로 vNIC에 논리적 코어를 할당합니다.

- **vNIC-count**: 호스트는 vNIC 방향에 대한 수신 또는 송신 트래픽의 전송에서 동일한 양의 CPU 리소스가 필요하다고 가정합니다. 각 논리적 코어에는 사용 가능한 논리 코어 풀을 기준으로 동일한 수의 vNIC가 할당됩니다. 이것이 기본 모드입니다. vNIC-count 모드는 신뢰할 수 있지만 비대칭 트래픽에는 최적이지 않습니다.
- **CPU-usage**: 호스트는 내부 통계를 사용하여 각 vNIC 방향에서 수신 또는 송신 트래픽을 전송하기 위한 CPU 사용량을 예측합니다. 호스트는 트래픽을 전송하기 위한 CPU 사용량에 따라, 논리적 코어 할당을 변경하여 논리적 코어 간의 로드 밸런스를 조정합니다. CPU 사용량 모드는 vNIC-count보다 더 최적이지만 트래픽이 안정적이지 않은 경우 신뢰할 수 없습니다.

CPU 사용량 모드에서 전송된 트래픽이 자주 변경되는 경우에는 예상 CPU 리소스 및 vNIC 할당도 자주 변경될 수 있습니다. 할당 변경이 너무 자주 발생하면 패킷이 손실될 수 있습니다.

트래픽 패턴이 vNIC 간에 대칭적인 경우 vNIC-count 옵션은 잦은 변경에도 덜 취약한 신뢰할 수 있는 동작을 제공합니다. 그러나 트래픽 패턴이 비대칭인 경우 vNIC-count는 vNIC 간의 트래픽 차이를 구분하지 않으므로 패킷 손실을 일으킬 수 있습니다.

vNIC-count 모드에서는 각 논리적 코어가 동일한 수의 vNIC에 할당되도록 적절한 수의 논리적 코어를 구성하는 것이 좋습니다. 각 논리적 코어에 연결된 vNIC 수가 서로 다른 경우 CPU 할당은 균일하지 않고 성능은 확정적이지 않습니다.

vNIC가 연결되거나 연결이 끊어질 경우 또는 논리적 코어가 추가 또는 제거될 경우 호스트는 자동으로 변경 사항을 감지하고 재조정합니다.

절차

- ◆ 한 모드에서 다른 모드로 전환하려면 다음 명령을 실행합니다.

```
set ens lcore-assignment-mode <host-switch-name> <ens-lc-mode>
```

여기서 *<ens-lc-mode>*를 **vNIC-count** 또는 **cpu-usage** 모드로 설정할 수 있습니다.

vNIC-count는 vNIC/방향 수 기반 논리적 코어 할당입니다.

cpu-usage는 CPU 사용량 기반 논리 코어 할당입니다.

게스트 VLAN 간 라우팅 구성

오버레이 네트워크에서 NSX-T는 L3 도메인의 VLAN 간 트래픽 라우팅을 지원합니다. 라우팅 중에 VDR(가상 분산 라우터)은 VLAN ID를 사용하여 VLAN 서브넷 간에 패킷을 라우팅합니다.

VLAN 간 라우팅을 사용하면 VM당 사용할 수 있는 10개의 vNIC 제한이 해소됩니다. NSX-T에서 VLAN 간 라우팅을 지원하므로 네트워크 서비스마다 다른 여러 VLAN 하위 인터페이스를 vNIC에서 생성하고 사용할 수 있습니다. 예를 들어, VM의 한 vNIC를 여러 하위 인터페이스로 나눌 수 있습니다. 각 하위 인터페이스는 SNMP 또는 DHCP와 같은 네트워크 서비스를 호스팅할 수 있는 서브넷에 속합니다. 예를 들어 VLAN 간 라우팅을 사용하는 경우 VLAN-10의 하위 인터페이스는 VLAN-10 또는 다른 VLAN의 하위 인터페이스에 연결될 수 있습니다.

VM의 각 vNIC는 태그 없는 패킷을 관리하는 상위 논리적 포트를 통해 N-VDS에 연결됩니다.

하위 인터페이스를 생성하려면 향상된 N-VDS 스위치에서 절차에 설명된 API 호출을 사용하여 연결된 VIF에서 API를 사용하여 하위 포트를 생성합니다. VLAN ID로 태그가 지정된 하위 인터페이스는 새 논리적 스위치에 연결됩니다. 예를 들어, VLAN10은 논리적 스위치 LS-VLAN-10에 연결됩니다. VLAN10의 모든 하위 인터페이스를 LS-VLAN-10에 연결해야 합니다. 하위 인터페이스의 VLAN ID와 연결된 논리적 스위치 사이의 이 일대일 매핑은 중요한 사전 요구 사항입니다. 예를 들어 VLAN20이 있는 하위 포트를 VLAN-10에 매핑된 논리적 스위치 LS-VLAN-10에 추가하면 VLAN 사이의 패킷 라우팅이 작동하지 않게 됩니다. 이러한 구성 오류는 VLAN 간 라우팅이 작동하지 않게 합니다.

사전 요구 사항

- VLAN 하위 인터페이스를 논리적 스위치에 연결하기 전에 논리적 스위치에 다른 VLAN 하위 인터페이스와의 다른 연결이 없는지 확인합니다. 불일치 상황이 발생하면 오버레이 네트워크의 VLAN 간 라우팅이 작동하지 않을 수 있습니다.
- 호스트가 ESXi v 6.7 U2 이상 버전을 실행하는지 확인합니다.

절차

- 1 vNIC에 대한 하위 인터페이스를 생성하려면 vNIC가 상위 포트에 업데이트되었는지 확인합니다. 다음 REST API 호출을 수행합니다.

```
PUT https://<nsx-mgr-ip>/api/v1/logical-ports/<Logical-Port UUID-of-the-vNIC>
{
  "resource_type" : "LogicalPort",
  "display_name" : "parentport",
  "attachment" : {
    "attachment_type" : "VIF",
    "context" : {
      "resource_type" : "VifAttachmentContext",
      "vif_type": "PARENT"
    },
    "id" : "<Attachment UUID of the vNIC>"
  },
  "admin_state" : "UP",
  "logical_switch_id" : "UUID of Logical Switch to which the vNIC is connected",
  "_revision" : 0
}
```

- 2 VM의 하위 인터페이스에 연결된 N-VDS의 상위 vNIC 포트에 대한 하위 포트를 생성하려면 API 호출을 수행합니다. API 호출을 수행하기 전에 하위 포트를 VM의 하위 인터페이스에 연결하기 위한 논리적 스위치가 있는지 확인합니다.

```
POST https://<nsx-mgr-ip>/api/v1/logical-ports/
{
  "resource_type" : "LogicalPort",
  "display_name" : "<Name of the Child PORT>",
  "attachment" : {
    "attachment_type" : "VIF",
    "context" : {
      "resource_type" : "VifAttachmentContext",
      "parent_vif_id" : "<UUID of the PARENT port from Step 1>",
      "traffic_tag" : <VLAN ID>,
      "app_id" : "<ID of the attachment>", ==> display id(can give any string). Must be
      unique.
      "vif_type" : "CHILD"
    },
    "id" : "<ID of the CHILD port>"
  },

  "logical_switch_id" : "<UUID of the Logical switch(not the PARENT PORT's logical switch)
  to which Child port would be connected to>",
  "address_bindings" : [ { "mac_address" : "<vNIC MAC address>", "ip_address" : "<IP
  address to the corresponding VLAN>", "vlan" : <VLAN ID> } ],
  "admin_state" : "UP"
}
```

결과

NSX-T Data Center는 VM에 하위 인터페이스를 생성합니다.

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. 이 계층 2 브리징은 물리적 및 가상 워크로드에서 서브넷을 분할해야 하는 마이그레이션 시나리오에서 특히 유용합니다.

계층 2 브리징에 포함된 NSX-T Data Center 개념은 Edge 클러스터 및 Edge 브리지 프로파일입니다. NSX Edge 전송 노드를 사용하여 계층 2 브리징을 구성할 수 있습니다. 브리징에 NSX Edge 전송 노드를 사용하려면 Edge 브리지 프로파일을 생성합니다. Edge 브리지 프로파일은 브리징에 사용할 Edge 클러스터와 기본 및 백업 브리지로 작동하는 Edge 전송 노드를 지정합니다.

Edge 브리지 프로파일은 논리적 스위치에 연결되고, 매핑은 브리징에 사용되는 Edge의 물리적 업링크와 논리적 스위치에 연결될 VLAN ID를 지정합니다. 논리적 스위치를 여러 브리지 프로파일에 연결할 수 있습니다.

Edge 브리지 프로파일 생성

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

Edge 브리지 프로파일을 생성할 때 페일오버 모드가 선점형으로 설정되고 페일오버가 발생하면 대기 노드가 활성 노드가 됩니다. 장애가 발생한 노드가 복구되면 해당 노드가 다시 활성 노드가 됩니다. 페일오버 모드가 선점형으로 설정되고 페일오버가 발생하면 대기 노드가 활성 노드가 됩니다. 장애가 발생한 노드가 복구되면 해당 노드가 대기 노드가 됩니다. 대기 Edge 노드에서 CLI 명령 `set l2bridge-port <uuid> state active`를 실행하여 수동으로 대기 Edge 노드를 활성 노드로 설정할 수 있습니다. 이 명령은 비선점형 모드에서만 적용할 수 있습니다. 그렇지 않은 경우에는 오류가 발생합니다. 비선점형 모드에서 이 명령은 대기 노드에 적용될 때는 HA 페일오버를 트리거하고 활성 노드에 적용될 때는 무시됩니다. 자세한 내용은 "NSX-T Data Center Command-Line Interface 참조" 를 참조하십시오.

사전 요구 사항

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

절차

- 1 시스템 > 패브릭 > 프로파일 > Edge 브리지 프로파일 > 추가를 선택합니다.
- 2 Edge 브리지 프로파일 이름 및 설명(선택 사항)을 입력합니다.
- 3 NSX Edge 클러스터를 선택합니다.
- 4 기본 노드를 선택합니다.
- 5 백업 노드를 선택합니다.
- 6 페일오버 모드를 선택합니다.
옵션은 **선점** 및 **비선점**입니다.
- 7 **추가** 버튼을 클릭합니다.

다음에 수행할 작업

이제 논리적 스위치를 브리지 프로파일에 연결할 수 있습니다.

Edge 기반 브리징 구성

Edge 기반 브리징을 구성할 때 Edge 클러스터에 대한 Edge 브리지 프로파일을 생성한 후 일부 추가 구성이 필요합니다.

동일한 Edge 노드에서 하나의 논리적 스위치를 두 번 브리징하는 것은 지원되지 않습니다. 그러나 두 개의 서로 다른 Edge 노드에 있는 동일한 논리적 스위치에 두 개의 VLAN을 브리징할 수 있습니다.

세 가지 구성 옵션이 있습니다.

옵션 1: 무차별 모드 구성

- 포트 그룹에서 무차별 모드를 설정합니다.

- 포트 그룹에서 위조 전송을 허용합니다.
- Edge VM이 실행 중인 ESXi 호스트에서 다음 명령을 실행하여 역방향 필터를 사용하도록 설정합니다.

```
esxcli system settings advanced set -o /Net/ReversePathFwdCheckPromisc -i 1
```

그런 후 다음 단계에 따라 포트 그룹에서 무차별 모드를 사용하거나 사용하지 않도록 설정합니다.

- 포트 그룹의 설정을 편집합니다.
- 무차별 모드를 사용하지 않도록 설정하고 설정을 저장합니다.
- 포트 그룹 설정을 다시 편집합니다.
- 무차별 모드를 사용하도록 설정하고 설정을 저장합니다.
- 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 줄어들 수 있습니다.

옵션 2: MAC 학습 구성

NSX-T가 설치된 호스트에 Edge를 배포한 경우 VLAN 논리적 스위치 또는 세그먼트에 연결할 수 있습니다. 논리적 스위치의 MAC 관리 프로파일에 MAC 학습을 사용하도록 설정해야 합니다. 마찬가지로 세그먼트의 MAC 검색 프로파일에 MAC 학습을 사용하도록 설정해야 합니다.

옵션 3: 싱크 포트 구성

- 1 싱크 포트 구성하려는 트렁크 vNIC에 대한 포트 번호를 검색합니다.
 - a vSphere Web Client에 로그인하고 **홈 > 네트워킹**으로 이동합니다.
 - b NSX Edge 트렁크 인터페이스가 연결된 분산 포트 그룹을 클릭하고 **포트**를 클릭하여 포트 및 연결된 VM을 확인합니다. 트렁크 인터페이스와 연결된 포트 번호를 기억해 둡니다. 불투명한 데이터를 가져오고 업데이트할 때 이 포트 번호를 사용합니다.
- 2 vSphere Distributed Switch에 대한 dvsUuid 값을 검색합니다.
 - a `https://<vc-ip>/mob`에서 vCenter Mob UI에 로그인합니다.
 - b **컨텐츠**를 클릭합니다.
 - c **rootFolder**에 연결된 링크(예: *group-d1 (Datacenters)*)를 클릭합니다.
 - d **childEntity**에 연결된 링크(예: *datacenter-1*)를 클릭합니다.
 - e **networkFolder**에 연결된 링크(예: *group-n6*)를 클릭합니다.
 - f NSX Edge에 연결된 vSphere Distributed Switch에 대한 DVS 이름 링크(예: *dvs-1 (Mgmt_VDS)*)를 클릭합니다.
 - g UUID 문자열 값을 복사합니다. 불투명한 데이터를 가져오고 업데이트할 때 dvsUuid에 대해 이 값을 사용합니다.

3 지정된 포트에 대해 불투명 데이터가 있는지를 확인합니다.

- a `https://<vc-ip>/mob/?moid=DVSManager&vmodl=1`로 이동합니다.
- b **fetchOpaqueDataEx**를 클릭합니다.
- c **selectionSet** 값 상자에 다음 XML 입력을 붙여 넣습니다.

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example
dvsUuid -->
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

NSX Edge 트렁크 인터페이스에 대해 검색한 포트 번호 및 `dvsUuid` 값을 사용합니다.

- d `isRuntime`을 `false`으로 설정합니다.
- e **메서드 호출**을 클릭합니다. 결과에 `vim.dvs.OpaqueData.ConfigInfo`에 대한 값이 표시되며 이미 불투명한 데이터 집합이 있는 경우 싱크 포트를 설정할 때 `edit` 작업을 사용합니다. `vim.dvs.OpaqueData.ConfigInfo`에 대한 값이 비어 있으면 싱크 포트를 설정할 때 `add` 작업을 사용합니다.

4 vCenter MOB(관리 개체 브라우저)에서 싱크 포트를 구성합니다.

- a `https://<vc-ip>/mob/?moid=DVSManager&vmodl=1`로 이동합니다.
- b **updateOpaqueDataEx**를 클릭합니다.
- c **selectionSet** 값 상자에 다음 XML 입력을 붙여 넣습니다. 예를 들면 다음과 같습니다.

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example
dvsUuid -->
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

vCenter MOB에서 검색한 `dvsUuid` 값을 사용합니다.

d `opaqueDataSpec` 값 상자에 다음 XML 입력 중 하나를 붙여 넣습니다.

불투명 데이터가 설정되어 있지 않으면(`operation`이 `add`로 설정) 이 입력을 사용하여 싱크 포트를 사용하도록 설정합니다.

```
<opaqueDataSpec>
  <operation>add</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
xsi:type="vmodl.Binary">AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
```

불투명 데이터가 이미 설정되어 있으면(operation이 edit로 설정) 이 입력을 사용하여 싱크 포트를 사용하도록 설정합니다.

```

<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
      xsi:type="vmodl.Binary">AAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
```

싱크 포트를 사용하지 않도록 설정하려면 다음 입력을 사용합니다.

```

<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
      xsi:type="vmodl.Binary">AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
```

- e isRuntime을 false으로 설정합니다.
- f 메서드 호출을 클릭합니다.

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.

사전 요구 사항

- Edge 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 **고급 네트워킹 및 보안 > 네트워킹 > 스위칭**을 선택합니다.
- 3 오버레이 스위치(트래픽 유형: 오버레이)의 이름을 클릭합니다.
- 4 **관련 > Edge 브리지 프로파일**을 클릭합니다.
- 5 **연결**을 클릭합니다.
- 6 Edge 브리지 프로파일에 연결하려면
 - a Edge 브리지 프로파일을 선택합니다.
 - b 전송 영역을 선택합니다.
 - c VLAN ID를 입력합니다.
 - d **저장**을 클릭합니다.
- 7 아직 연결하지 않은 경우 VM을 논리적 스위치에 연결합니다.
VM은 Edge 브리지 프로파일과 동일한 전송 영역의 전송 노드에 있어야 합니다.

결과

NSX-T Data Center 내부 VM에서 NSX-T Data Center외부 노드로 ping을 전송하여 브리지의 기능을 테스트할 수 있습니다.

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-T Data Center는 2계층 라우팅 모델을 지원합니다.

상위 계층은 Tier-0 논리적 라우터입니다. 노스바운드에서 Tier-0 논리적 라우터는 하나 이상의 물리적 라우터 또는 계층 3 스위치에 연결되며 물리적 인프라에 대한 게이트웨이 역할을 합니다. 사우스바운드에서 Tier-0 논리적 라우터는 하나 이상의 Tier-1 논리적 라우터 또는 하나 이상의 논리적 스위치에 직접 연결됩니다.

하위 계층은 Tier-1 논리적 라우터입니다. 노스바운드에서 Tier-1 논리적 라우터는 Tier-0 논리적 라우터에 연결됩니다. 사우스바운드에서는 하나 이상의 논리적 스위치에 연결됩니다.

참고 고급 네트워킹 및 보안 사용자 인터페이스를 사용하여 정책 인터페이스에서 생성된 개체를 수정하는 경우 일부 설정을 구성하지 못할 수 있습니다. 이러한 읽기 전용 설정에는 옆에 ⊖ 아이콘이 있습니다. 자세한 내용은 [장 1 NSX Manager 개요](#) 항목을 참조하십시오.

본 장은 다음 항목을 포함합니다.

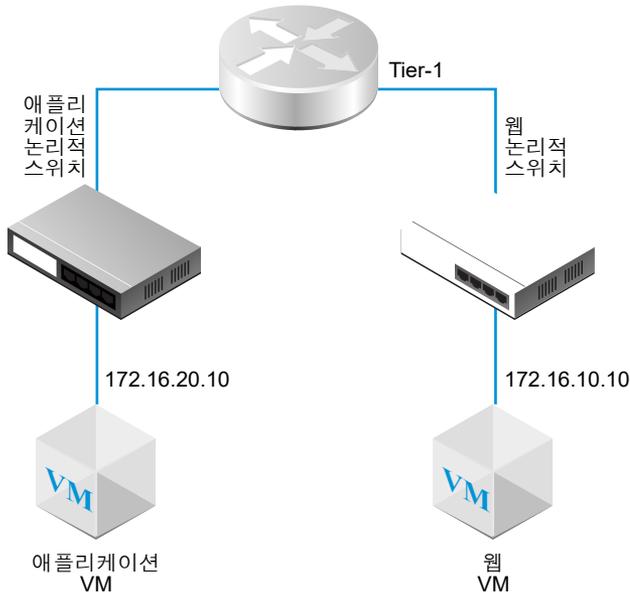
- Tier-1 논리적 라우터
- Tier-0 논리적 라우터

Tier-1 논리적 라우터

Tier-1 논리적 라우터에는 논리적 스위치에 연결하기 위한 다운링크 포트와 Tier-0 논리적 라우터에 연결하기 위한 업링크 포트가 있습니다.

논리적 라우터를 추가하는 경우 구축하려는 네트워킹 토폴로지를 계획하는 것이 중요합니다.

그림 14-1. 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.

일부 시나리오에서는 외부 클라이언트가 LB VIP 포트에 바인딩된 MAC 주소에 대한 ARP 쿼리를 전송합니다. 하지만 LB VIP 포트는 MAC 주소가 없으며 이러한 쿼리를 처리할 수 없습니다. LB VIP 포트 대신 ARP 쿼리를 처리하기 위해 프록시 ARP가 Tier-1 논리적 라우터의 중앙 집중식 서비스 포트에서 구현됩니다.

Tier-1 논리적 라우터를 DNAT, Edge 방화벽 및 로드 밸런서를 사용하여 구성하면 Tier-1 논리적 라우터로 또는 부터의 트래픽은 DNAT, Edge 방화벽, 로드 밸런서 순서로 처리됩니다. Tier-1 논리적 라우터의 트래픽은 먼저 DNAT를 통해 처리된 후 로드 밸런서를 통해 처리됩니다. Edge 방화벽 처리는 건너뛸니다.

Tier-0 또는 Tier-1 논리적 라우터에서는 서로 다른 유형의 포트를 구성할 수 있습니다. 한 가지 유형을 CSP(중앙 집중식 서비스 포트)라고 합니다. VLAN 지원 논리적 스위치에 연결하거나 독립형 Tier-1 논리적 라우터를 생성하도록 활성-대기 모드의 Tier-0 논리적 라우터 또는 Tier-1 논리적 라우터의 CSP를 구성해야 합니다. CSP는 활성-대기 모드의 Tier-0 논리적 라우터 또는 Tier-1 논리적 라우터에서 다음 서비스를 지원합니다.

- NAT
- 로드 밸런싱
- 상태 저장 방화벽
- VPN(IPsec 및 L2VPN)

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. **Tier-1 논리적 라우터**의 내용을 참조하십시오.

절차

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

2 **고급 네트워킹 및 보안 > 라우터 > 라우터 > 추가**를 선택합니다.

3 **Tier-1 라우터**를 선택하고 논리적 라우터에 대한 이름을 입력하고 필요한 경우 설명을 입력합니다.

4 (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.

5 (선택 사항) NSX Edge 클러스터를 선택합니다.

선택한 클러스터를 선택 취소하려면 **x** 아이콘을 클릭합니다. 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.

6 (선택 사항) **대기 재배치** 토글 버튼을 클릭하여 대기 재배치를 사용하거나 사용하지 않도록 설정합니다.

대기 재배치는 활성 또는 대기 논리적 라우터가 실행되고 있는 Edge 노드가 실패하는 경우고가용성을 유지하기 위해 다른 Edge 노드에서 새 대기 논리적 라우터가 생성됨을 의미합니다. 실패한 Edge 노드가 활성 논리적 라우터를 실행 중인 경우 원래의 대기 논리적 라우터가 활성 논리적 라우터가 되고 새 대기 논리적 라우터가 생성됩니다. 실패하는 Edge 노드에서 대기 논리적 라우터가 실행 중인 경우 새 대기 논리적 라우터가 대신 사용됩니다.

7 (선택 사항) NSX Edge 클러스터를 선택한 경우 **페일오버 모드**를 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 **추가**를 클릭합니다.

결과

논리적 라우터가 생성된 후, 라우터 구성에서 Edge 클러스터를 제거하려면 다음 단계를 수행합니다.

- 구성 세부 정보를 보려면 라우터의 이름을 클릭합니다.
- **서비스 > Edge 방화벽**을 선택합니다.
- **방화벽 사용 안 함**을 클릭합니다.
- **개요** 탭을 클릭하고 **편집**을 클릭합니다.
- **Edge 클러스터** 필드에서 **x** 아이콘을 클릭합니다.
- **저장**을 클릭합니다.

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 추가의 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 생성의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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 구성의 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

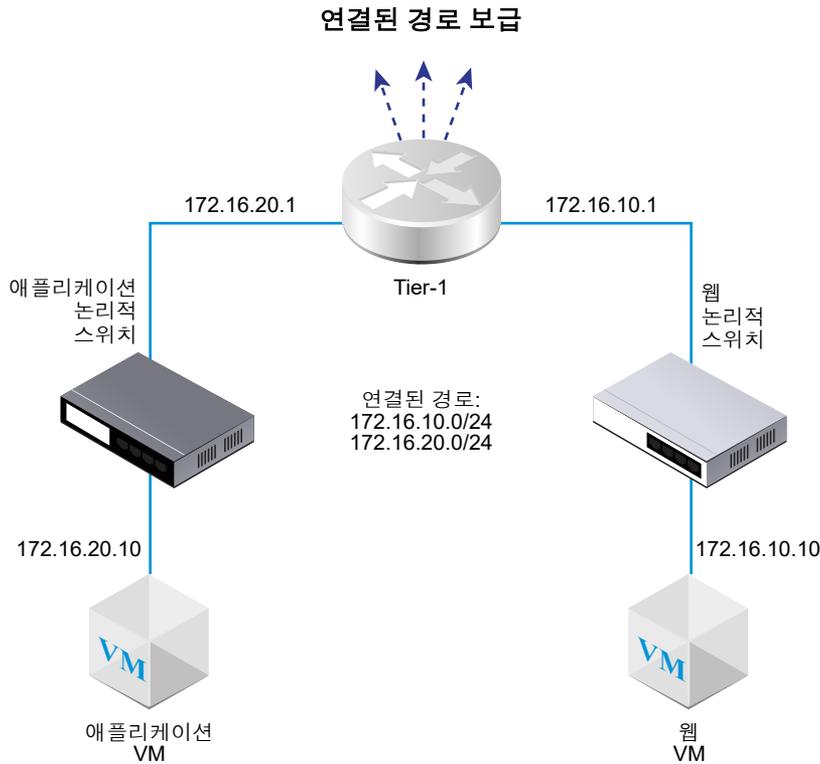
- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 선택합니다.
- 3 라우터의 이름을 클릭합니다.
- 4 **구성** 탭을 클릭하고 **라우터 포트**를 선택합니다.
- 5 **추가**를 클릭합니다.
- 6 라우터 포트 이름 및 필요한 경우 설명을 입력합니다.
- 7 **유형** 필드에서 **중앙 집중식**을 선택합니다.
- 8 **URPF 모드**의 경우 **엄격** 또는 **없음**을 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 13 논리적 스위치의 내용](#)을 참조하십시오.
- Tier-1 논리적 라우터에 대한 다운로드 포트가 구성되어 있는지 확인합니다. [Tier-1 논리적 라우터에서 다운로드 포트 추가의 내용](#)을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(https://<nsx-manager-ip-address>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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
- 모든 DNS 전달자 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.

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

d **추가**를 클릭합니다.

다음에 수행할 작업

Tier-0 논리적 라우터 토폴로지를 숙지하고 Tier-0 논리적 라우터를 생성합니다. Tier-0 논리적 라우터의 내용을 참조하십시오.

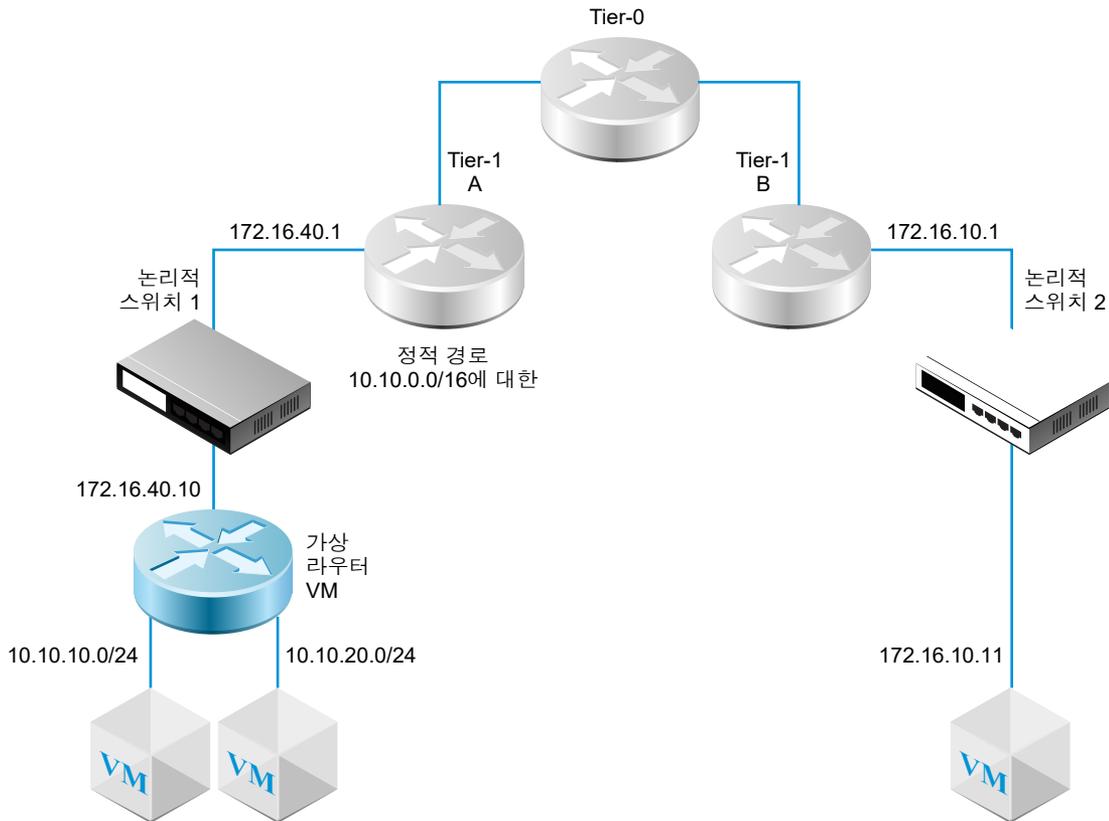
Tier-0 논리적 라우터가 Tier-1 논리적 라우터에 이미 연결된 경우 Tier-0 라우터가 Tier-1 라우터 연결 경로를 학습하고 있는지 확인할 수 있습니다. Tier-0 라우터에 Tier-1 라우터에서 학습된 경로가 있는지 확인의 내용을 참조하십시오.

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 14-2. Tier-1 논리적 라우터 정적 경로 토폴로지



재귀 정적 경로가 지원됩니다.

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 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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.
IPv6 기반의 정적 경로가 지원됩니다. IPv6 접두사에는 IPv6 다음 홉만 포함될 수 있습니다.
예를 들어 10.10.10.0/16 또는 IPv6 주소입니다.
- 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.
- 서비스 IPsec, DNAT, 방화벽, 로드 밸런서 및 서비스 삽입의 모든 조합을 지원합니다. 수신 경우 처리 순서는 IPsec - DNAT 방화벽 - 로드 밸런서 - 서비스 삽입입니다. 송신 경우 처리 순서는 서비스 삽입 - 로드 밸런서 - 방화벽 - DNAT - IPsec입니다.

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.

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 프로세스가 지원됩니다. CSP의 서브넷에 LB 가상 서버 IP 또는 LB SNAT IP를 구성할 수 있습니다. 예를 들어 CSP IP가 1.1.1.1/24인 경우 가상 IP가 1.1.1.2일 수 있습니다. 또한, 라우팅이 적절하게 구성된 경우 2.2.2.2와 같은 다른 서브넷의 IP가 될 수도 있습니다. 이로 인해 2.2.2.2의 트래픽이 독립형 라우터에 도달할 수 있습니다.
- 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.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 라우터 > 라우터 > 추가**를 선택합니다.
- 3 **Tier-1 라우터**를 선택하고 논리적 라우터에 대한 이름을 입력하고 필요한 경우 설명을 입력합니다.
- 4 (필수 사항) 이 Tier-1 논리적 라우터에 연결할 NSX Edge 클러스터를 선택합니다.
- 5 (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.

- 6 **추가**를 클릭합니다.
- 7 방금 생성한 라우터의 이름을 클릭합니다.
- 8 **구성** 탭을 클릭하고 **라우터 포트**를 선택합니다
- 9 **추가**를 클릭합니다.
- 10 라우터 포트 이름 및 필요한 경우 설명을 입력합니다.
- 11 **유형** 필드에서 **중앙 집중식**을 선택합니다.
- 12 **URPF 모드**의 경우 **엄격** 또는 **없음**을 선택합니다.
URPF(유니캐스트 역방향 경로 전달)는 보안 기능입니다.

- 13 (필수 사항) 논리적 스위치를 선택합니다.
- 14 이 연결이 스위치 포트를 생성할지 또는 기존 스위치 포트를 업데이트할지 선택합니다.
- 15 CIDR 표기법으로 라우터 포트 IP 주소를 입력합니다.
- 16 추가를 클릭합니다.

Tier-0 논리적 라우터

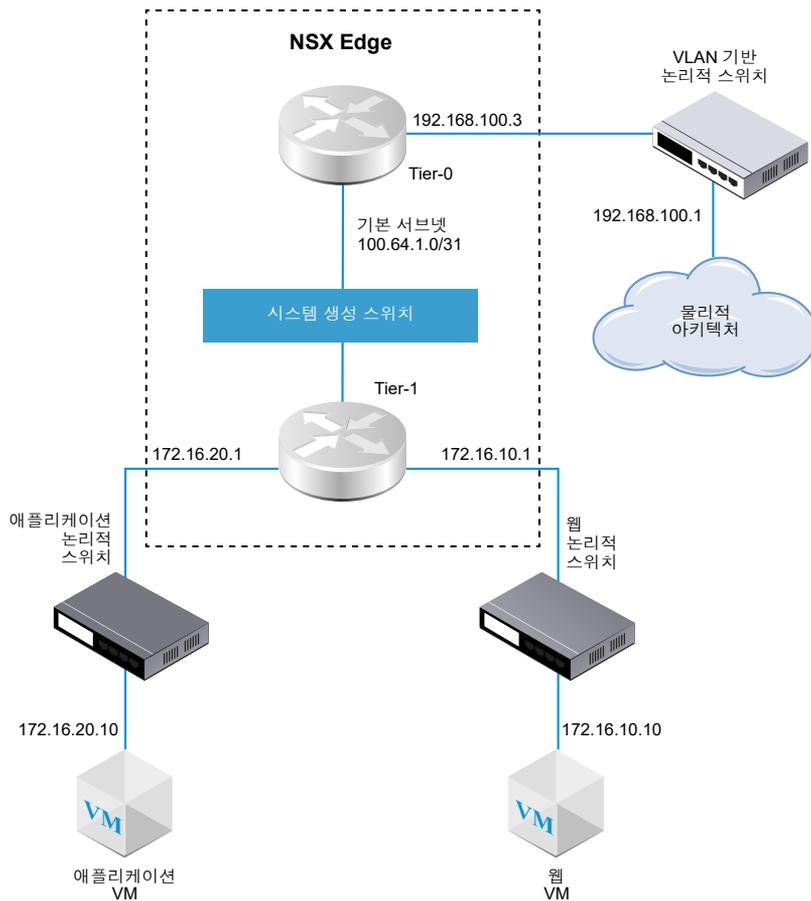
Tier-0 논리적 라우터는 논리적 및 물리적 네트워크 간에 게이트웨이 서비스를 제공합니다.

NSX Cloud 참고 NSX Cloud를 사용하는 경우 NSX Cloud에서 지원되는 NSX-T Data Center 기능에서 자동 생성된 논리적 엔티티, 지원되는 기능 및 NSX Cloud에 필요한 구성 목록을 확인하십시오.

Edge 노드는 하나의 Tier-0 게이트웨이 또는 논리적 라우터만 지원할 수 있습니다. Tier-0 게이트웨이 또는 논리적 라우터를 생성할 때 NSX Edge 클러스터에 Edge 노드 수보다 더 많은 Tier-0 게이트웨이 또는 논리적 라우터를 생성하지 않아야 합니다.

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

그림 14-3. 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.

일부 시나리오에서는 외부 클라이언트가 루프백 또는 IKE IP 포트에 바인딩된 MAC 주소에 대한 ARP 쿼리를 보냅니다. 단, 루프백 및 IKE IP 포트에는 MAC 주소가 없어서 이러한 쿼리를 처리할 수 없습니다. 루프백 및 IKE IP 포트를 대신하여 ARP 쿼리를 처리하기 위해 프록시 ARP는 Tier-0 논리적 라우터의 업링크 및 중앙 집중식 서비스 포트에 구현됩니다.

Tier-0 논리적 라우터가 DNAT, IPsec 및 Edge 방화벽으로 구성된 경우 트래픽은 IPsec, DNAT, Edge 방화벽 순서로 처리됩니다.

Tier-0 또는 Tier-1 논리적 라우터에서는 서로 다른 유형의 포트를 구성할 수 있습니다. 한 가지 유형을 CSP(중앙 집중식 서비스 포트)라고 합니다. VLAN 지원 논리적 스위치에 연결하거나 독립형 Tier-1 논리적 라우터를 생성하도록 활성-대기 모드의 Tier-0 논리적 라우터 또는 Tier-1 논리적 라우터의 CSP를 구성해야 합니다. CSP는 활성-대기 모드의 Tier-0 논리적 라우터 또는 Tier-1 논리적 라우터에서 다음 서비스를 지원합니다.

- NAT
- 로드 밸런싱
- 상태 저장 방화벽
- VPN(IPsec 및 L2VPN)

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 Edge 클러스터가 구성되었는지 확인합니다. "NSX-T Data Center 설치 가이드"의 내용을 참조하십시오.
- Tier-0 논리적 라우터의 네트워킹 토폴로지를 숙지합니다. Tier-0 논리적 라우터의 내용을 참조하십시오.

절차

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

2 고급 네트워킹 및 보안 > 라우터 > 라우터 > 추가를 선택합니다.

3 드롭다운 메뉴에서 **Tier-0 라우터**를 선택합니다.

4 Tier-0 논리적 라우터에 이름을 할당합니다.

5 드롭다운 메뉴에서 이 Tier-0 논리적 라우터를 지원할 기존 NSX Edge 클러스터를 선택합니다.

6 (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.

7 (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.

8 (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 100.64.0.0/16입니다. 각 Tier-0과 Tier-1 간의 피어 연결에는 100.64.0.0/16 주소 공간 내에 /31 서브넷이 제공됩니다.

9 **저장**을 클릭합니다.

새 Tier-0 논리적 라우터가 링크로 표시됩니다.

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

다음에 수행할 작업

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

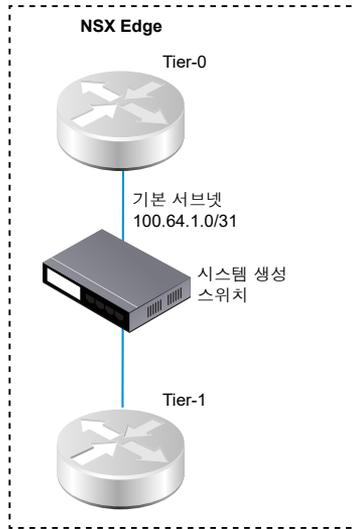
Tier-0 논리적 라우터를 구성하여 이를 VLAN 논리적 스위치에 연결하고 외부 네트워크에 대한 업링크를 생성합니다. NSX Edge 업링크를 위해 VLAN 논리적 스위치에 Tier-0 논리적 라우터 연결의 내용을 참조하십시오.

Tier-0과 Tier-1 연결

Tier-0 논리적 라우터를 Tier-1 논리적 라우터에 연결하면 Tier-1 논리적 라우터가 노스바운드 및 동-서 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 100.64.0.0/16입니다. 각 Tier-0과 Tier-1 간의 피어 연결에는 100.64.0.0/16 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 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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-edgel(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-edgel1(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

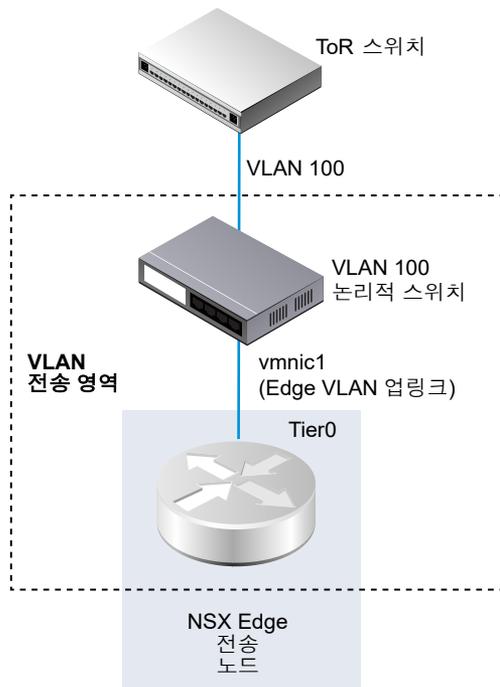
Total number of routes: 7

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 생성의 내용을 참조하십시오.

Tier-0 라우터를 생성합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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 연결의 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-O 서비스 라우터 컨텍스트를 시작합니다.

```

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

```

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

TOR에 대한 경로는 연결됨(c)으로 나타납니다.

```

nsx-edgel(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 구성의 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 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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

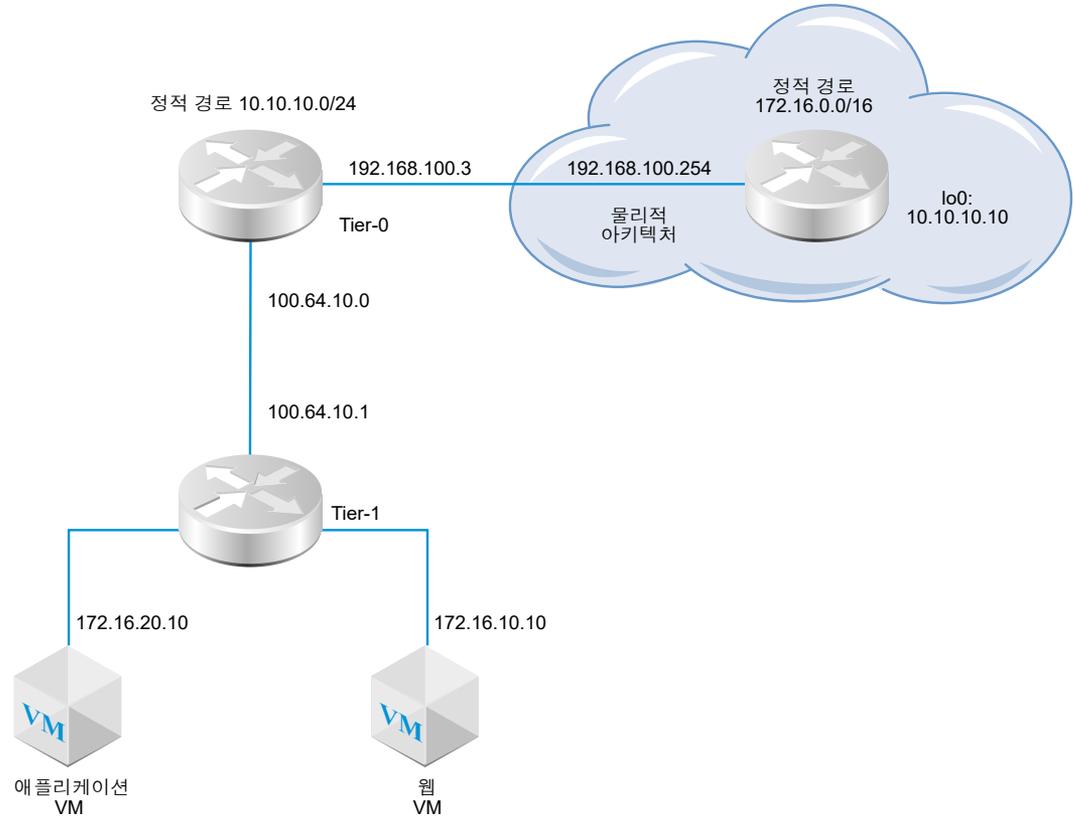
- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 선택합니다.
- 3 라우터의 이름을 클릭합니다.
- 4 **구성** 탭을 클릭하고 **라우터 포트**를 선택합니다.
- 5 **추가**를 클릭합니다.
- 6 라우터 포트 이름 및 필요한 경우 설명을 입력합니다.
- 7 **유형** 필드에서 **중앙 집중식**을 선택합니다.
- 8 **URPF 모드**의 경우 **엄격** 또는 **없음**을 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 14-4. 정적 경로 토폴로지



재귀 정적 경로가 지원됩니다.

사전 요구 사항

- 물리적 라우터 및 Tier-0 논리적 라우터가 연결되어 있는지 확인합니다. Tier-0 논리적 라우터 및 TOR 연결 확인의 내용을 참조하십시오.
- 연결된 경로를 보급하기 위해 Tier-1 라우터가 구성되어 있는지 확인합니다. Tier-1 논리적 라우터 생성의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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 route 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.

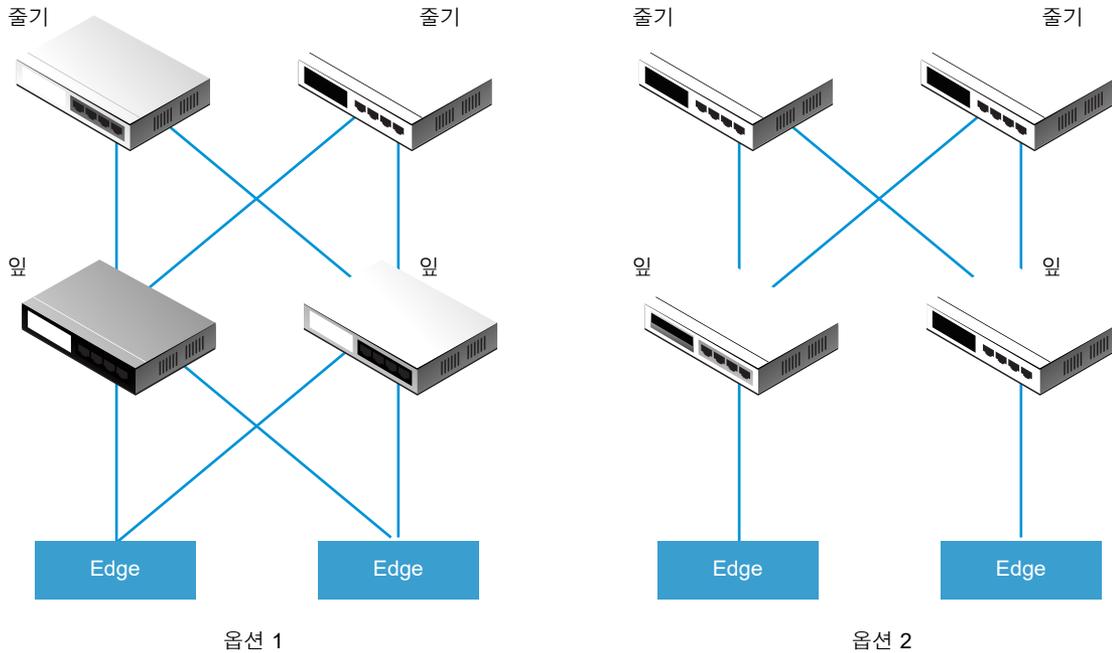
```
ping 10.10.10.10
```

```
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/iBGP(외부 또는 내부 BGP) 연결을 구성하면 됩니다.

iBGP 기능에는 다음과 같은 기능 및 제한 사항이 있습니다.

- 재배포, 접두사 목록 및 경로 맵이 지원됩니다.
- 경로 리플렉터가 지원되지 않습니다.
- BGP 연합이 지원되지 않습니다.

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 원격 AS 번호도 구성해야 합니다. EBGP 인접 네트워크는 직접 연결되어야 하고 Tier-0 업링크와 동일한 서브넷에 있어야 합니다. 동일한 서브넷에 있지 않으면 BGP 다중 홉을 사용해야 합니다.

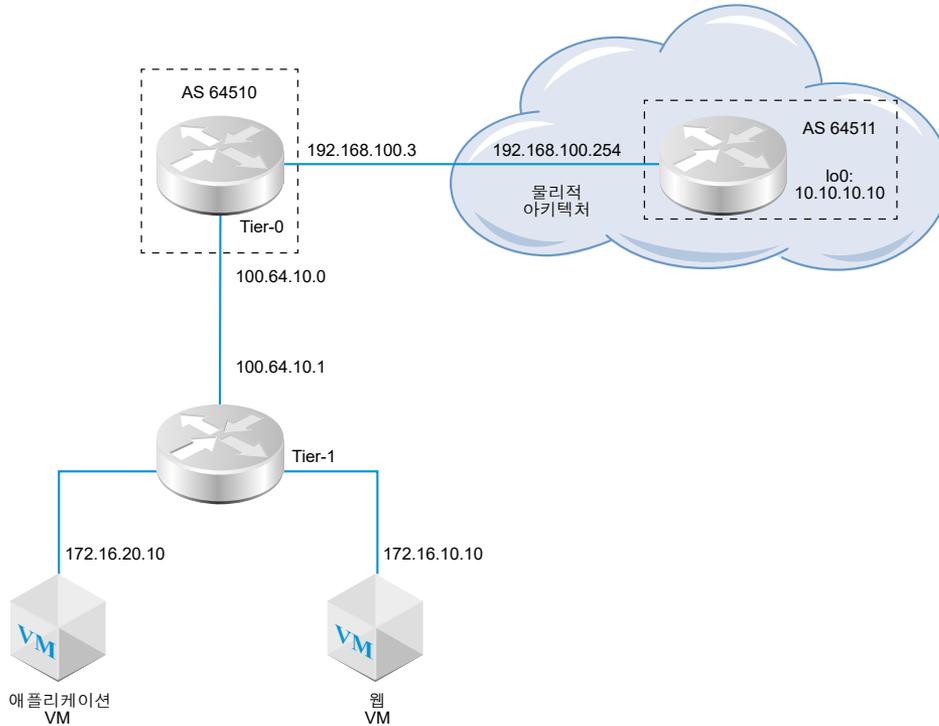
액티브-액티브 모드의 Tier-0 논리적 라우터는 SR(서비스 라우터) 간 라우팅을 지원합니다. 라우터 1번이 노스바운드 물리적 라우터와 통신할 수 없으면 트래픽이 액티브-액티브 클러스터의 라우터 2번으로 라우팅됩니다. 라우터 2번이 물리적 라우터와 통신할 수 있으면, 라우터 1번과 물리적 라우터 간의 트래픽은 영향을 받지 않습니다.

활성-활성 모드의 Tier-0 논리적 라우터가 활성-대기 모드의 Tier-1 논리적 라우터에 연결된 토폴로지에서는 비대칭 라우팅을 처리하기 위해 SR 간 라우팅을 사용하도록 설정해야 합니다. SR 중 하나에 정적 경로를 구성하거나 한 SR에서 다른 SR의 업링크에 도달해야 하는 경우 비대칭 라우팅이 유지됩니다. 또한 다음을 참조하십시오.

- 하나의 SR(예: Edge 노드 #1의 SR #1)에 구성된 정적 경로의 경우 다른 SR(예: Edge 노드 #2의 SR #2)은 eBGP 피어의 동일한 경로를 학습하며 이 경로가 더 효율적이므로 SR #1의 정적 경로보다 학습된 경로를 선호합니다. SR #2가 SR #1에 구성된 정적 경로를 사용하도록 하려면 선점형 모드에서 Tier-1 논리적 라우터를 구성하고 Edge 노드 #1을 기본 노드로 구성합니다.
- Tier-0 논리적 라우터에 Edge 노드 #1의 업링크 포트가 있고 Edge 노드 #2에 다른 업링크 포트가 있는 경우 두 업링크가 서로 다른 서브넷에 있으면 테넌트 VM에서 업링크로의 트래픽 ping이 작동합니다. 두 업링크가 동일한 서브넷에 있으면 트래픽 Ping이 실패합니다.

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 14-5. BGP 연결 토폴로지



BGP 또는 BFD와 관련된 연결 장애가 있는 경우 다음과 같은 시나리오를 참조하십시오.

- BGP만 구성된 경우, 모든 BGP 인접 라우터가 다운되면 서비스 라우터의 상태가 종료입니다.
- BFD만 구성된 경우, 모든 BFD 인접 라우터가 다운되면 서비스 라우터의 상태가 종료입니다.
- BGP 및 BFD가 구성된 경우, 모든 BGP 및 BFD 인접 라우터가 다운되면 서비스 라우터의 상태가 종료입니다.
- BGP 및 정적 경로가 구성된 경우, 모든 BGP 인접 라우터가 다운되면 서비스 라우터의 상태가 종료입니다.
- 정적 경로만 구성된 경우 노드에 장애가 발생하거나 유지 보수 모드에 있지 않으면 서비스 라우터의 상태가 항상 실행 중입니다.

사전 요구 사항

- 연결된 경로를 보급하기 위해 Tier-1 라우터가 구성되어 있는지 확인합니다. Tier-1 논리적 라우터에서 경로 보급 구성의 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 생성의 내용을 참조하십시오.
- Tier-0 논리적 라우터가 Tier-1 논리적 라우터의 경로를 학습했는지 확인합니다. Tier-0 라우터에 Tier-1 라우터에서 학습된 경로가 있는지 확인의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 선택합니다.
- 3 Tier-0 논리적 라우터를 선택합니다.
- 4 **라우팅** 탭을 클릭하고 드롭다운 메뉴에서 **BGP**를 선택합니다.
- 5 **편집**을 클릭합니다.
 - a 로컬 AS 번호를 입력합니다.
예: 64510
 - b **상태**를 전환하여 BGP를 사용하거나 사용하지 않도록 설정합니다.
 - c **ECMP**를 전환하여 ECMP를 사용하거나 사용하지 않도록 설정합니다.
 - d **정상적인 다시 시작** 토글 버튼을 클릭하여 정상적인 다시 시작을 사용하거나 사용하지 않도록 설정합니다.
정상적인 다시 시작은 Tier-0 라우터와 연결된 NSX Edge 클러스터에 하나의 Edge 노드가 있을 때만 지원됩니다.
 - e 이 논리적 라우터가 액티브-액티브 모드이면 **서비스 라우터 간 라우팅** 토글을 클릭하여 SR 간 라우팅을 사용하거나 사용하지 않도록 설정합니다.
 - f 경로 집계를 구성합니다.
 - g **저장**을 클릭합니다.
- 6 **추가**를 클릭하여 BGP 인접 네트워크를 추가합니다.
- 7 인접 네트워크 IP 주소를 입력합니다.
예: 192.168.100.254
- 8 최대 홉 한계를 지정합니다.
기본값은 1입니다.
- 9 원격 AS 번호를 입력합니다.
예: 64511(eBGP 인접 네트워크) 또는 64510(iBGP 인접 네트워크)
- 10 타이머(연결 유지 시간 및 보류 시간) 및 암호를 구성합니다.
- 11 **로컬 주소** 탭을 클릭하여 로컬 주소를 선택합니다.
 - a (선택 사항) **모든 업링크**를 선택 취소하여 루프백 포트와 업링크 포트를 둘 다 확인합니다.
- 12 **주소 패밀리** 탭을 클릭하여 주소 패밀리를 추가합니다.
- 13 **BFD 구성** 탭을 클릭하여 BFD를 사용하도록 설정합니다.

14 저장을 클릭합니다.

다음에 수행할 작업

BGP가 제대로 작동하는지 테스트합니다. Tier-O 서비스 라우터에서 BGP 연결 확인의 내용을 참조하십시오.

Tier-O 서비스 라우터에서 BGP 연결 확인

CLI를 사용하여 Tier-O 서비스 라우터에서 인접 항목에 대한 BGP 연결이 설정되어 있는지 확인합니다.

사전 요구 사항

BGP가 구성되어 있는지 확인합니다. Tier-O 논리적 라우터에서 BGP 구성의 내용을 참조하십시오.

절차

- 1 NSX Manager CLI에 로그인합니다.
- 2 NSX Edge에서 `get logical-routers` 명령을 실행하여 Tier-O 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-edgel(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 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 선택합니다.
- 3 Tier-0 논리적 라우터를 선택합니다.
- 4 **라우팅** 탭을 클릭하고 드롭다운 메뉴에서 **경로 재배포**를 선택합니다.
- 5 **편집**을 클릭하여 경로 재배포를 사용하거나 사용하지 않도록 설정합니다.

6 추가를 클릭하여 경로 재배포 조건 집합을 추가합니다.

옵션	설명
이름 및 설명	경로 재배포에 이름을 할당합니다. 필요한 경우 설명을 제공할 수 있습니다. 이름의 예로 advertise-to-bgp-neighbor를 들 수 있습니다.
소스	다음 소스 중 하나 이상을 선택합니다. <ul style="list-style-type: none"> ■ TO 연결됨 ■ TO 업링크 ■ TO 다운링크 ■ TO CSP ■ TO 루프백 ■ TO 정적 ■ TO NAT ■ TO DNS 전달자 IP ■ TO IPSec 로컬 IP ■ T1 연결됨 ■ T1 CSP ■ T1 다운링크 ■ T1 정적 ■ T1 LB SNAT ■ T1 NAT ■ T1 LB VIP ■ T1 DNS 전달자 IP
경로 맵	(선택 사항) 경로 맵을 할당하여 경로 재배포에서 IP 주소 시퀀스를 필터링합니다.

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 구성의 내용을 참조하십시오.
- NSX-T Data Center 정적 경로가 재배포되도록 설정되어 있는지 확인합니다. Tier-0 논리적 라우터에서 경로 재배포 사용의 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

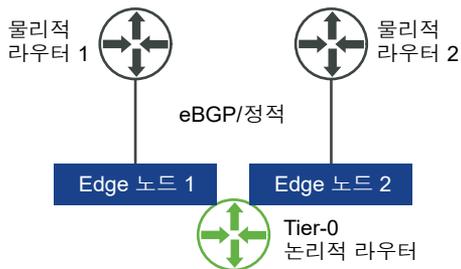
ECMP와 같은 추가 라우팅 기능을 구성합니다.

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.

ECMP를 사용하려면 Tier-0 논리적 라우터가 액티브-액티브 모드여야 합니다. 최대 8개의 ECMP 경로가 지원됩니다. NSX Edge의 ECMP 구현은 프로토콜 번호의 5-튜플, 소스 주소, 대상 주소, 소스 포트 및 대상 포트를 기준으로 합니다. ECMP 경로 간에 데이터를 분산하는 데 사용되는 알고리즘은 라운드 로빈이 아닙니다. 따라서 일부 경로가 다른 경로보다 더 많은 트래픽을 전송할 수 있습니다. 프로토콜이 IPv6이고 IPv6 헤더에 확장 헤더가 둘 이상 있는 경우 ECMP는 소스 및 대상 주소만을 기준으로 합니다.

그림 14-6. ECMP 라우팅 토폴로지



예를 들어 위의 토폴로지에서는 2노드 NSX Edge 클러스터에서 실행 중인 액티브-액티브 모드의 단일 Tier-0 논리적 라우터를 표시합니다. 두 개의 업링크 포트가 각 Edge 노드에 하나씩 구성됩니다.

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 생성의 내용을 참조하십시오.
- Tier-0 논리적 라우터가 구성되어 있는지 확인합니다. Tier-0 논리적 라우터 생성의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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 업링크 를 수락합니다.
MTU	이 필드를 비워 두면 기본값은 1500입니다.
전송 노드	드롭다운 메뉴에서 Edge 전송 노드를 할당합니다.
URPF 모드	유니캐스트 역방향 경로 전달은 보안 기능입니다. ECMP 모드에 다중 액티브-액티브 Edge 노드가 있는 경우 없음 으로 설정하는 것이 좋습니다. 기본값은 엄격 입니다.
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 추가의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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 사용을 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.
- 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 분산 라우터가 연결되어 있는지 확인합니다.

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

UUID의 경로 유형은 **NSX_CONNECTED**로 표시됩니다.

8 두 Edge 노드에서 SSH 세션을 시작합니다.

9 패킷을 캡처하기 위한 세션을 시작합니다.

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

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

10 Tier-0 라우터에 연결된 소스 VM에서 대상 VM으로 트래픽을 생성할 수 있는 도구를 사용합니다.

11 두 Edge 노드에서 트래픽을 관찰합니다.

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 생성의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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 생성의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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.
가중치	가중치를 설정하여 경로 선택에 영향을 줍니다. 범위는 0 - 65535입니다.
커뮤니티	aa:nn 형식을 사용하여 커뮤니티를 지정합니다(예: 300:500). 또는 드롭다운 메뉴를 사용하여 다음 중 하나를 선택합니다. <ul style="list-style-type: none"> ■ NO_EXPORT_SUBCONFED - EBGП 피어로 보급하지 마십시오. ■ NO_ADVERTISE - 어떤 피어로도 보급하지 마십시오. ■ NO_EXPORT - BGP 연합 외부로 보급하지 마십시오.

- 10 [작업] 열에서 **허용** 또는 **거부**를 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 보급하는 데 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 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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.

고급 네트워킹 및 보안 탭에서 NAT를 구성할 수 있습니다.

참고 고급 네트워킹 및 보안 사용자 인터페이스를 사용하여 정책 인터페이스에서 생성된 개체를 수정하는 경우 일부 설정을 구성하지 못할 수 있습니다. 이러한 읽기 전용 설정에는 옆에 ⊖ 아이콘이 있습니다. 자세한 내용은 [장 1 NSX Manager 개요](#) 항목을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- 네트워크 주소 변환

네트워크 주소 변환

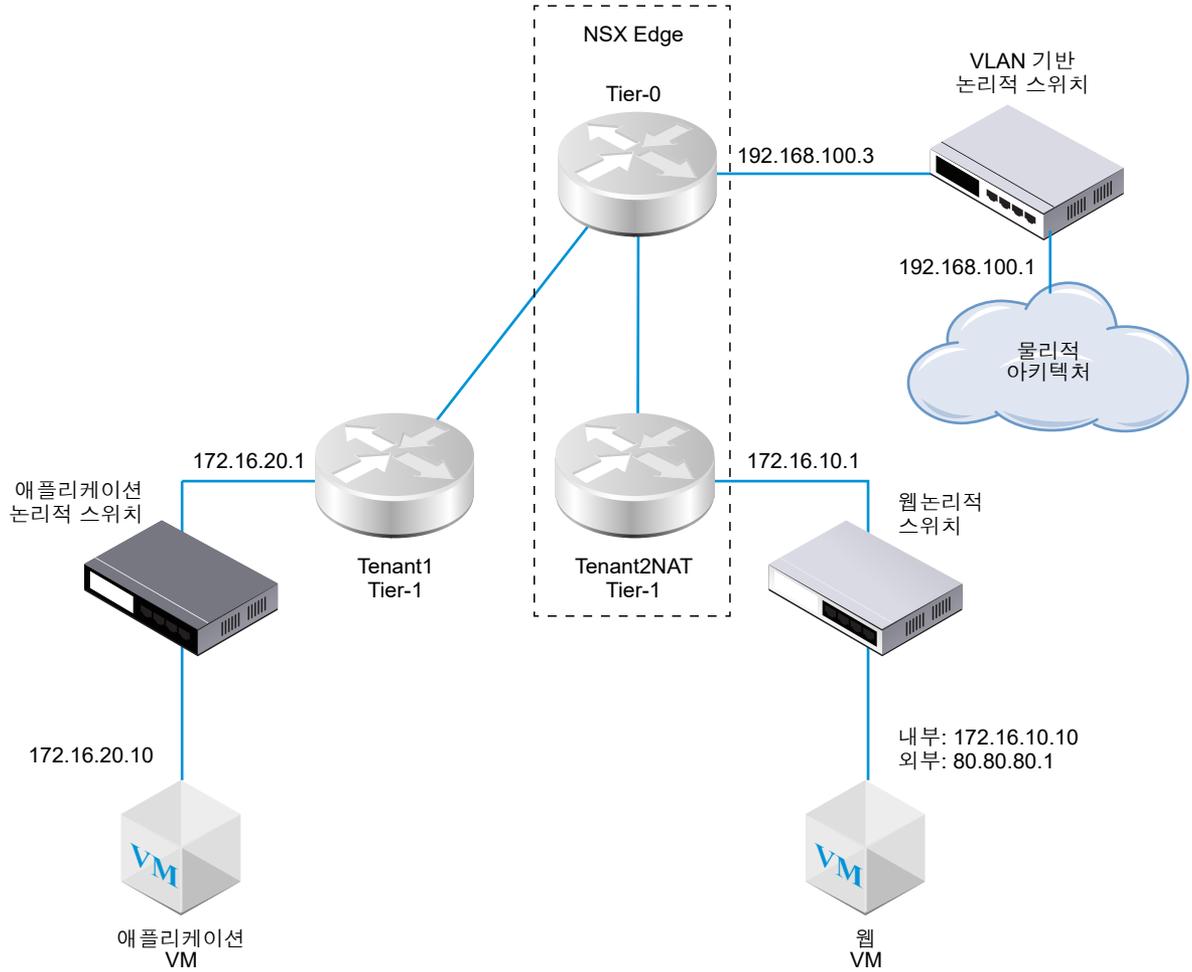
NSX-T Data Center의 NAT(네트워크 주소 변환)를 Tier-0 및 Tier-1 논리적 라우터에서 구성할 수 있습니다.

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.

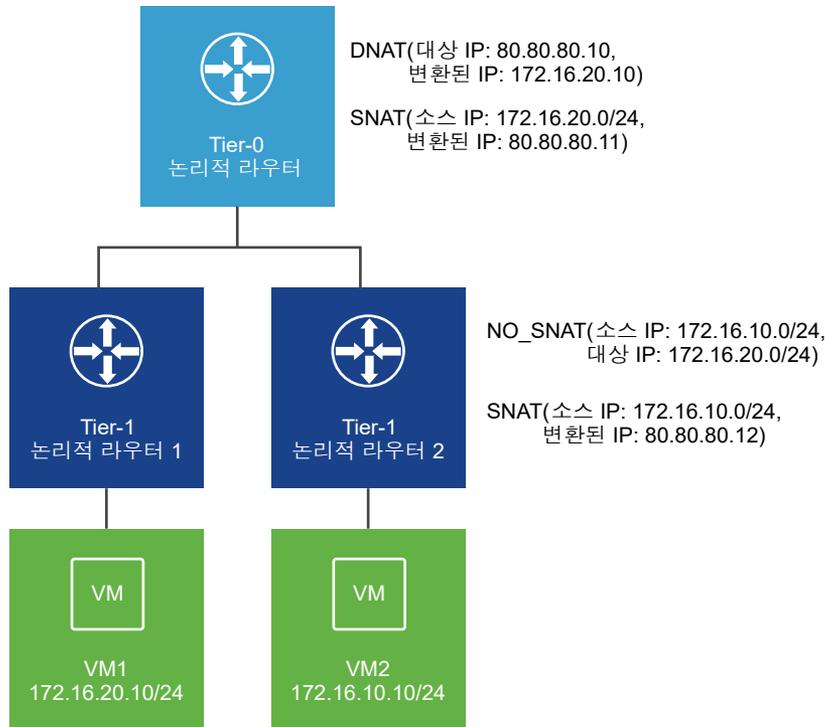
NAT는 Tier-0 논리적 라우터에 대한 연결에서 Tenant2NAT 논리적 라우터의 업링크에 적용됩니다.

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

그림 15-1. NAT 토폴로지



참고: 다음 시나리오에서는 NAT 헤어핀이 지원되지 않습니다. Tier-0 논리적 라우터에는 DNAT 및 SNAT가 구성되어 있습니다. Tier-1 논리적 라우터 2에는 NO_SNAT 및 SNAT가 구성되어 있습니다. VM2는 VM1의 외부 주소 80.80.80.10을 사용하여 VM1에 액세스할 수 없습니다.



다음 섹션에서는 관리자 UI를 사용하여 NAT 규칙을 생성하는 방법을 설명합니다. API 호출 (POST /api/v1/logical-routers/<logical-router-id>/nat/rules?action=create_multiple)로 여러 NAT 규칙을 동시에 생성할 수도 있습니다. 자세한 정보는 "NSX-T Data Center API 가이드" 를 참조하십시오.

Tier-1 NAT

Tier-1 논리적 라우터는 SNAT(소스 NAT), DNAT(대상 NAT) 및 재귀 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 연결의 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 사용을 참조하십시오.
- Tier-1 라우터 각각에는 Tier-0 라우터에 대한 업링크가 구성되어 있어야 합니다. Tenant2NAT는 NSX Edge 클러스터에서 지원해야 합니다. Tier-0과 Tier-1 연결의 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 구성을 참조하십시오.
- VM은 올바른 논리적 스위치에 연결되어야 합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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 작업에 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:

ID	작업	일치				변환됨		적용 대상	통계
		프로토콜	소스 IP	소스 포트	대상 IP	대상 포트	IP		
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 연결의 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 사용을 참조하십시오.
- Tier-1 라우터 각각에는 Tier-0 라우터에 대한 업링크가 구성되어 있어야 합니다. Tenant2NAT는 NSX Edge 클러스터에서 지원해야 합니다. Tier-0과 Tier-1 연결의 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 구성을 참조하십시오.
- VM은 올바른 논리적 스위치에 연결되어야 합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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 DNAT인 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 DNAT인 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		
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 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 선택합니다.
- 3 NAT가 구성된 Tier-1 논리적 라우터를 클릭합니다.
- 4 Tier-1 라우터에서 **라우팅 > 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
- 모든 DNS 전달자 경로 보급

- 6 **저장**을 클릭합니다.

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 **편집**을 클릭하여 경로 재배포를 사용하거나 사용하지 않도록 설정합니다.
- 6 **추가**를 클릭하여 경로 재배포 조건 집합을 추가합니다.

옵션	설명
이름 및 설명	경로 재배포에 이름을 할당합니다. 필요한 경우 설명을 제공할 수 있습니다. 이름의 예로 advertise-to-bgp-neighbor를 들 수 있습니다.
소스	<p>다음 소스 중 하나 이상을 선택합니다.</p> <ul style="list-style-type: none"> ■ TO 연결됨 ■ TO 업링크 ■ TO 다운링크 ■ TO CSP ■ TO 루프백 ■ TO 정적 ■ TO NAT ■ TO DNS 전달자 IP ■ TO IPSec 로컬 IP ■ T1 연결됨 ■ T1 CSP ■ T1 다운링크 ■ T1 정적 ■ T1 LB SNAT ■ T1 NAT ■ T1 LB VIP ■ T1 DNS 전달자 IP
경로 맵	(선택 사항) 경로 맵을 할당하여 경로 재배포에서 IP 주소 시퀀스를 필터링합니다.

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 `80.80.80.1`을 ping할 수 있는지 확인합니다.
- 7 Ping이 여전히 실행 중인 경우 DNAT 규칙의 통계 열을 확인합니다.
활성 세션이 하나만 있어야 합니다.

Tier-0 NAT

액티브-대기 모드의 Tier-0 논리적 라우터는 SNAT(소스 NAT), DNAT(대상 NAT) 및 재귀 NAT를 지원합니다. 활성-활성 모드의 Tier-0 논리적 라우터는 재귀 NAT만 지원합니다.

Tier-0 논리적 라우터에서 소스 및 대상 NAT 구성

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

IP 주소 또는 주소 범위에 대해 SNAT 또는 DNAT를 사용하지 않도록 설정할 수도 있습니다. 여러 NAT 규칙이 주소에 적용되는 경우 우선 순위가 가장 높은 규칙이 적용됩니다.

Tier-0 논리적 라우터의 업링크에 구성된 SNAT는 Tier-1 논리적 라우터의 트래픽뿐만 아니라 Tier-0 논리적 라우터의 또 다른 업링크 트래픽도 처리합니다.

절차

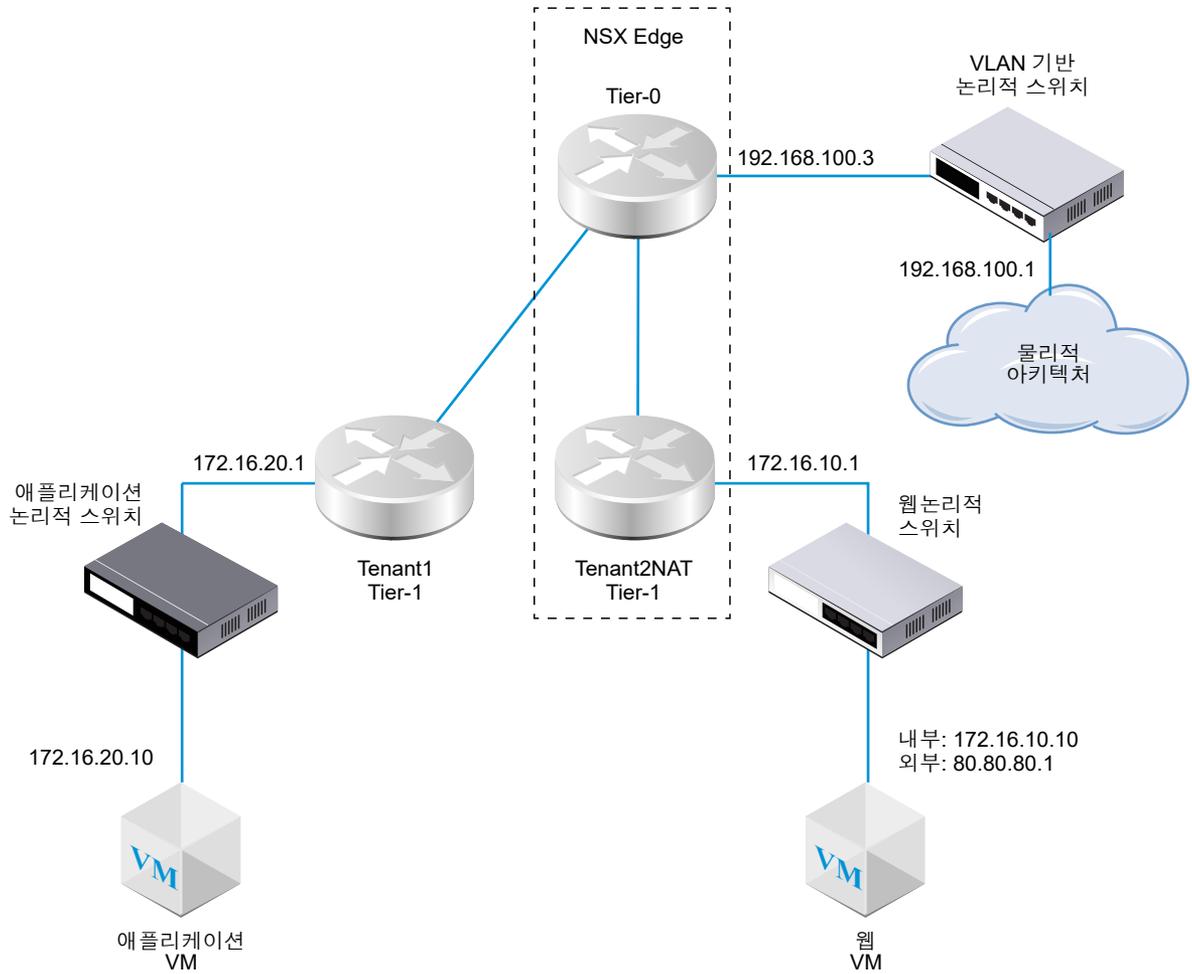
- 1 브라우저에서 관리자 권한으로 NSX Manager(`https://<nsx-manager-ip-address>`)에 로그인합니다.

- 2 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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 **작업**의 경우 **SNAT, DNAT, 재귀, 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) **작업**이 **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.

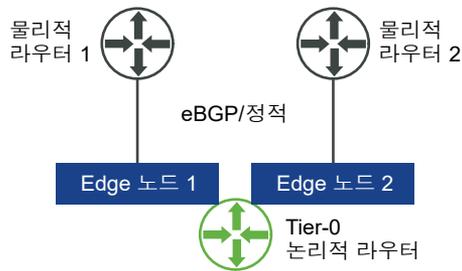
재귀 NAT

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



아래에 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 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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 **작업**에 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	일지				변환됨		적용 대상	통계
		프로토콜	소스 IP	소스 포트	대상 IP	대상 포트	IP		
▼ 우선 순위: 1024									
2048	재귀	임의	80.80.80.1	임의	임의	임의	172.16.10.10	임의	

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

참고 고급 네트워킹 및 보안 사용자 인터페이스를 사용하여 정책 인터페이스에서 생성된 개체를 수정하는 경우 일부 설정을 구성하지 못할 수 있습니다. 이러한 읽기 전용 설정에는 옆에 ⊖ 아이콘이 있습니다. 자세한 내용은 [장 1 NSX Manager 개요](#) 항목을 참조하십시오.

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. 이 방법으로 생성된 IP 집합은 정책 모드에 표시되지 않습니다. 정책 모드에서는 그룹을 생성하고 **인벤토리 > 그룹 > 멤버 설정**으로 이동하고 IP 또는 MAC 주소를 지정하여 멤버를 IP 주소, 범위, 네트워크 주소 또는 MAC 주소로 추가할 수 있습니다.

참고 방화벽 규칙의 소스 또는 대상 범위로 IPv4 주소와 IPv6 주소가 지원됩니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 인벤토리 > 그룹 > IP 집합 > 추가**를 선택합니다.

- 3 이름을 입력합니다.
- 4 (선택 사항) 설명을 입력합니다.
- 5 **멤버**에 개별 IP 주소, IP 범위 및 서브넷을 쉼표로 구분된 목록으로 입력합니다.
- 6 **저장**을 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 **고급 네트워킹 및 보안 > 인벤토리 > 그룹 > IP 풀 > 추가**를 선택합니다.
- 3 새 IP 풀의 이름을 입력합니다.
- 4 (선택 사항) 설명을 입력합니다.
- 5 **추가**를 클릭합니다.
- 6 IP 범위 셀을 클릭하고 IP 범위를 입력합니다.
셀의 오른쪽 상단 모서리로 마우스를 가져간 후 연필 아이콘을 클릭하여 편집합니다.
- 7 (선택 사항) 게이트웨이를 입력합니다.
- 8 CIDR IP 주소와 접미사를 입력합니다.
- 9 (선택 사항) DNS 서버를 입력합니다.
- 10 (선택 사항) DNS 접미사를 입력합니다.
- 11 **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 **고급 네트워킹 및 보안 > 인벤토리 > 그룹 > MAC 집합 > 추가**를 선택합니다.
- 3 이름을 입력합니다.
- 4 (선택 사항) 설명을 입력합니다.

5 MAC 주소를 쉼표로 구분된 목록으로 입력합니다.

6 **추가**를 클릭합니다.

NSGroup 생성

NSGroup을 구성하여 IP 집합, MAC 집합, 논리적 포트, 논리적 스위치 및 기타 NSGroup의 조합을 포함할 수 있습니다. 논리적 스위치, 논리적 포트 및 VM이 포함된 NSGroup을 소스 및 대상으로 지정할 수 있으며 방화벽 규칙의 Applied To 필드에도 지정할 수 있습니다. IPset 및 MACSet이 포함된 NSGroup은 분산 방화벽 Applied To 필드에서 무시됩니다.

NSX Cloud 참고 NSX Cloud를 사용하는 경우 NSX Cloud에서 지원되는 NSX-T Data Center 기능에서 자동 생성된 논리적 엔티티, 지원되는 기능 및 NSX Cloud에 필요한 구성 목록을 확인하십시오.

NSGroup은 다음과 같은 특성을 갖습니다.

- 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. 기본 그룹 테이블에서 그룹을 클릭한 후 **관련 > NSGroup**을 선택하면 직접적으로든 간접적으로든 LogicalSwitch-1이 멤버로 있는 3개의 NSGroup, 즉 NSGroup-1, NSGroup-2 및 NSGroup-3이 표시됩니다.
- NSGroup에는 최대 500개의 직접 멤버가 있을 수 있습니다.
- NSGroup에서 권장되는 유효한 멤버 수 제한은 5000개입니다. NSX Manager는 하루에 2번, 즉 오전 7시와 오후 7시에 NSGroup에서 해당 제한을 확인합니다. 이 제한을 초과해도 기능에는 영향이 없으나 성능이 저하될 수 있습니다.
 - 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 표시됩니다. 이 수가 5000을 초과하면 경고 메시지 NSGroup xyz has reached the maximum numbers limit. Total number in NSGroup = ...이 표시됩니다.
 - 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.
- 지원되는 최대 VM 수는 10,000개입니다.
- 최대 1만 개의 NSGroup을 생성할 수 있습니다.

NSGroup에 멤버로 추가할 수 있는 모든 개체의 경우 해당 개체 화면으로 이동한 후 **관련 > NSGroup**을 선택할 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 인벤토리 > 그룹 > 추가**를 선택합니다.
- 3 NSGroup의 이름을 입력합니다.
- 4 (선택 사항) 설명을 입력합니다.
- 5 (선택 사항) **멤버 자격 조건**을 클릭합니다

각 기준의 경우 논리적 AND 연산자로 조합된 최대 5개의 규칙을 지정할 수 있습니다. 사용 가능한 멤버 조건은 다음에 대해 적용할 수 있습니다.

- **논리적 포트** - 태그 및 선택적 범위를 지정할 수 있습니다.
- **논리적 스위치** - 태그 및 선택적 범위를 지정할 수 있습니다.
- **가상 시스템** - 특정 문자열을 포함하거나, 특정 문자열과 같거나 같지 않거나, 특정 문자열로 시작하거나 끝나는 이름, 태그, 컴퓨터 OS 이름 또는 컴퓨터 이름을 지정할 수 있습니다.
- **전송 노드** - Edge 노드 또는 호스트 노드와 동일한 노드 유형을 지정할 수 있습니다.
- **IP 집합** - 태그 및 선택적 범위를 지정할 수 있습니다.

- 6 (선택 사항) **멤버**를 클릭하여 멤버를 선택합니다.

다음과 같은 멤버 유형을 사용할 수 있습니다.

- **AD 그룹** - ADGroup이 있는 NSGroup은 분산 방화벽 규칙의 extended_source 필드에만 사용할 수 있으며 그룹 내의 유일한 멤버여야 합니다. 예를 들어 ADGroup과 IPSet 둘 모두 멤버로 있는 NSGroup은 존재할 수 없습니다.
- **IP 집합** - IPv4 주소와 IPv6 주소 둘 다 포함할 수 있습니다.
- **논리적 포트** - IPv4 주소와 IPv6 주소 둘 다 포함할 수 있습니다.
- **논리적 스위치** - IPv4 주소와 IPv6 주소 둘 다 포함할 수 있습니다.
- **MAC 집합**
- **NSGroup**
- **전송 노드**
- **VIF**
- **가상 시스템**

- 7 **추가**를 클릭합니다.

그룹 테이블에 그룹이 추가됩니다. 그룹 이름을 클릭하여 개요를 표시하고 멤버 자격 조건, 멤버, 애플리케이션 및 관련 그룹을 포함한 그룹 정보를 편집할 수 있습니다. **개요** 탭 맨 아래로 스크롤하면 태그를 추가 및 삭제할 수 있습니다. 자세한 내용은 **개체에 태그 추가** 항목을 참조하십시오. **관련>** NSGroup을 선택하면 선택된 NSGroup이 멤버로 있는 모든 NSGroup이 표시됩니다.

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 **고급 네트워킹 및 보안 > 인벤토리 > 서비스 > 추가**를 선택합니다.
- 3 이름을 입력합니다.
- 4 (선택 사항) 설명을 입력합니다.
- 5 **프로토콜 지정**을 선택하여 개별 서비스를 구성하거나 **기존 서비스 그룹화**를 선택하여 NSService 그룹을 구성합니다.
- 6 개별 서비스에 대해 서비스 유형 및 프로토콜을 선택합니다.

사용 가능한 유형은 **이더넷**, **IP**, **IGMP**, **ICMP**, **ALG** 및 **L4 포트 집합**입니다.

- 7 서비스 그룹에 대해 그룹의 유형 및 멤버를 선택합니다.
사용 가능한 유형은 **계층 2** 및 **계층 3 이상**입니다.
- 8 **추가**를 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 **고급 네트워킹 및 보안 > 인벤토리 > 가상 시스템**을 선택합니다.
가상 시스템, 외부 ID, 소스 및 태그라는 4개의 열로 구성된 VM 목록이 표시됩니다. 처음 3개 열의 머릿글에 있는 필터 아이콘을 클릭하여 목록을 필터링합니다. 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 탐색 패널에서 **인벤토리 > 가상 시스템**을 선택합니다.
- 4 VM을 선택합니다.
- 5 **태그 관리**를 클릭합니다.
- 6 태그를 추가하거나 삭제합니다.

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

NSX Manager에서 가상 시스템에 할당할 수 있는 최대 태그 수는 25개입니다. 논리적 스위치, 포트 등 관리되는 다른 모드 개체의 최대 태그 수는 30개입니다.

- 7 **저장**을 클릭합니다.

고급 네트워크 및 보안 탭에서 DHCP를 구성할 수 있습니다.

참고 고급 네트워크 및 보안 사용자 인터페이스를 사용하여 정책 인터페이스에서 생성된 개체를 수정하는 경우 일부 설정을 구성하지 못할 수 있습니다. 이러한 읽기 전용 설정에는 옆에 ⊖ 아이콘이 있습니다. 자세한 내용은 [장 1 NSX Manager 개요](#) 항목을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- DHCP
- 메타데이터 프록시

DHCP

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.

이 릴리스에서 DHCP 서버는 게스트 VLAN 태깅을 지원하지 않습니다.

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 **고급 네트워킹 및 보안 > 네트워킹 > DHCP > 서버 프로파일 > 추가**를 선택합니다.
- 3 이름과 설명(선택 사항)을 입력합니다.
- 4 드롭다운 목록에서 NSX Edge 클러스터를 선택합니다.
- 5 (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 **고급 네트워킹 및 보안 > 네트워킹 > DHCP > 서버 > 추가**를 선택합니다.
- 3 이름과 설명(선택 사항)을 입력합니다.
- 4 DHCP 서버의 IP 주소와 해당 서브넷 마스크를 CIDR 형식으로 입력합니다.
예: 192.168.1.2/24
- 5 (필수 사항) 드롭다운 메뉴에서 DHCP 프로파일을 선택합니다.
- 6 (선택 사항) 도메인 이름, 기본 게이트웨이, DNS 서버 및 서브넷 마스크와 같은 일반 옵션을 입력합니다.
- 7 (선택 사항) 클래스 없는 정적 경로 옵션을 입력합니다.
- 8 (선택 사항) 기타 옵션을 입력합니다.
- 9 **저장**을 클릭합니다.
- 10 새로 생성된 DHCP 서버를 선택합니다.
- 11 [IP 풀] 섹션을 확장합니다.
- 12 **추가**를 클릭하여 IP 범위, 기본 게이트웨이, 리스 기간, 주의 임계값, 오류 임계값, 클래스 없는 정적 경로 옵션 및 기타 옵션을 추가합니다.
- 13 [정적 바인딩] 섹션을 확장합니다.

14 추가를 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.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 스위칭**을 선택합니다.
 - a 논리적 스위치의 확인란을 클릭합니다.
 - b **작업 > DHCP 서버 연결**을 클릭합니다.
- 3 또는 **고급 네트워킹 및 보안 > DHCP**를 선택합니다.
 - a **서버** 탭을 클릭합니다.
 - b DHCP 서버의 확인란을 클릭합니다.
 - c **작업 > 논리적 스위치에 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 **고급 네트워킹 및 보안 > 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 또는 DHCPv6 서버를 지정합니다. DHCP/DHCPv6 릴레이 서비스를 생성할 때 DHCP 릴레이 프로파일을 지정해야 합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > DHCP > 릴레이 프로파일 > 추가**를 선택합니다.
- 3 이름과 설명(선택 사항)을 입력합니다.
- 4 하나 이상의 외부 DHCP/DHCPv6 서버 주소를 입력합니다.

다음에 수행할 작업

DHCP/DHCPv6 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 **고급 네트워킹 및 보안 > 네트워킹 > DHCP > 릴레이 서비스 > 추가**를 선택합니다.
- 3 이름과 설명(선택 사항)을 입력합니다.
- 4 드롭다운 메뉴에서 DHCP 릴레이 프로파일을 선택합니다.

다음에 수행할 작업

논리적 라우터 포트에 DHCP 서비스를 추가합니다. [논리적 라우터 포트에 DHCP 릴레이 서비스 추가](#)의 내용을 참조하십시오.

논리적 라우터 포트에 DHCP 릴레이 서비스 추가

논리적 라우터 포트에 DHCP 릴레이 서비스를 추가할 수 있습니다. 해당 포트에 연결된 논리적 스위치의 VM은 릴레이 서비스에 구성된 DHCP 서버와 통신할 수 있습니다.

사전 요구 사항

- DHCP 릴레이 서비스가 구성되어 있는지 확인합니다. [DHCP 릴레이 서비스 생성](#)의 내용을 참조하십시오.
- 라우터 포트가 **다운링크** 유형인지 확인합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 선택합니다.

- 3 적절한 라우터를 선택하여 추가 정보와 구성 옵션을 표시합니다.
- 4 구성 > 라우터 포트를 선택합니다.
- 5 원하는 논리적 스위치에 연결된 라우터 포트를 선택하고 편집을 클릭합니다.
- 6 릴레이 서비스 드롭다운 목록에서 DHCP 릴레이 서비스를 선택하고 저장을 클릭합니다.

또한 새 논리적 라우터 포트를 추가할 때 DHCP 릴레이 서비스를 선택할 수 있습니다.

DHCP 리스 삭제

경우에 따라 DHCP 리스를 삭제해야 할 수 있습니다. 예를 들어 DHCP 클라이언트가 다른 IP 주소를 가져 오도록 하거나, 클라이언트가 해당 IP 주소를 해제하지 않고 종료했으나 다른 클라이언트에서 해당 주소를 사용할 수 있게 하려는 경우가 있습니다.

다음 API를 사용하여 DHCP 리스를 삭제할 수 있습니다.

```
DELETE /api/v1/dhcp/servers/<server-id>/leases?ip=<ip>&mac=<mac>
```

올바른 리스가 삭제되도록 하려면 DELETE API 전후에 다음 API를 호출합니다.

```
GET /api/v1/dhcp/servers/<server-id>/leases
```

DELETE API를 호출한 후에는 GET API의 출력에 삭제된 리스가 표시되지 않는지 확인합니다.

자세한 내용은 "NSX-T Data Center API 참조" 를 참조하십시오.

메타데이터 프록시

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://169.254.169.254:80으로 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.

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 **고급 네트워킹 및 보안 > 네트워킹 > DHCP > 메타데이터 프록시 > 추가**를 선택합니다.
- 3 메타데이터 프록시 서버의 이름을 입력합니다.
- 4 (선택 사항) 설명을 입력합니다.
- 5 Nova 서버의 URL 및 포트를 입력합니다.
유효한 포트 범위는 3000 - 9000입니다.
- 6 **암호**에 대한 값을 입력합니다.
- 7 드롭다운 목록에서 NSX Edge 클러스터를 선택합니다.
- 8 (선택 사항) NSX Edge 클러스터의 멤버를 선택합니다.

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 **고급 네트워킹 및 보안 > 네트워킹 > DHCP > 메타데이터 프록시**를 선택합니다.
- 3 메타데이터 프록시 서버를 선택합니다.
- 4 메뉴 옵션 **작업 > 논리적 스위치에 연결**을 선택합니다.
- 5 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 **고급 네트워킹 및 보안 > 네트워킹 > DHCP > 메타데이터 프록시**를 선택합니다.
- 3 메타데이터 프록시 서버를 선택합니다.
- 4 메뉴 옵션 **작업 > 논리적 스위치에서 분리**를 선택합니다.
- 5 드롭다운 목록에서 논리적 스위치를 선택합니다.

결과

스위칭 > 스위치로 이동하고 스위치를 선택한 후 메뉴 옵션 **작업 > 메타데이터 프록시 분리**를 선택하여 논리적 스위치에서 메타데이터 프록시 서버를 분리할 수도 있습니다.

IPAM(IP 주소 관리)을 사용하면 NCP(NSX 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.

참고 고급 네트워킹 및 보안 사용자 인터페이스를 사용하여 정책 인터페이스에서 생성된 개체를 수정하는 경우 일부 설정을 구성하지 못할 수 있습니다. 이러한 읽기 전용 설정에는 옆에 ⊖ 아이콘이 있습니다. 자세한 내용은 [장 1 NSX Manager 개요](#) 항목을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- IP 블록 관리
- IP 블록에 대한 서브넷 관리

IP 블록 관리

NSX Container Plug-in을 설치하려면 컨테이너용 IP 블록을 생성해야 합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > IPAM**를 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

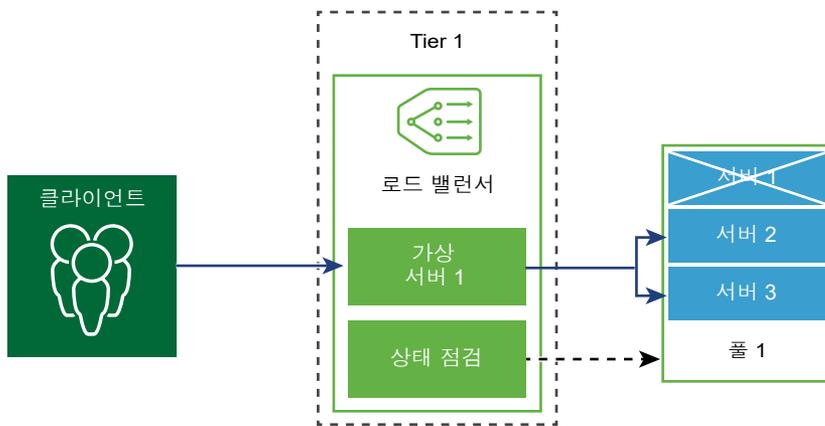
- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 네트워킹 > IPAM**를 선택합니다.
- 3 IP 블록의 이름을 클릭합니다.
- 4 **서브넷** 탭을 클릭합니다.
- 5 서브넷을 추가하려면 **추가**를 클릭합니다.
 - a 이름과 설명(선택 사항)을 입력합니다.
 - b 서브넷의 크기를 입력합니다.
- 6 하나 이상의 서브넷을 삭제하려면 서브넷을 선택합니다.
 - a **삭제**를 클릭합니다.

이 정보는 **고급 네트워킹 및 보안** 탭에 있는 NSX-T Data Center 로드 밸런싱 구성에 관해 다룹니다.

NSX 고급 로드 밸런서(Avi 네트워크)에 대한 자세한 내용은 <https://www.vmware.com/products/nsx-advanced-load-balancer.html>을 참조하십시오.

참고 고급 네트워킹 및 보안 사용자 인터페이스를 사용하여 정책 인터페이스에서 생성된 개체를 수정하는 경우 일부 설정을 구성하지 못할 수 있습니다. 이러한 읽기 전용 설정에는 옆에 ⊖ 아이콘이 있습니다. 자세한 내용은 **장 1 NSX Manager 개요** 항목을 참조하십시오.

NSX-T Data Center 논리적 로드 밸런서는 애플리케이션에고가용성 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.

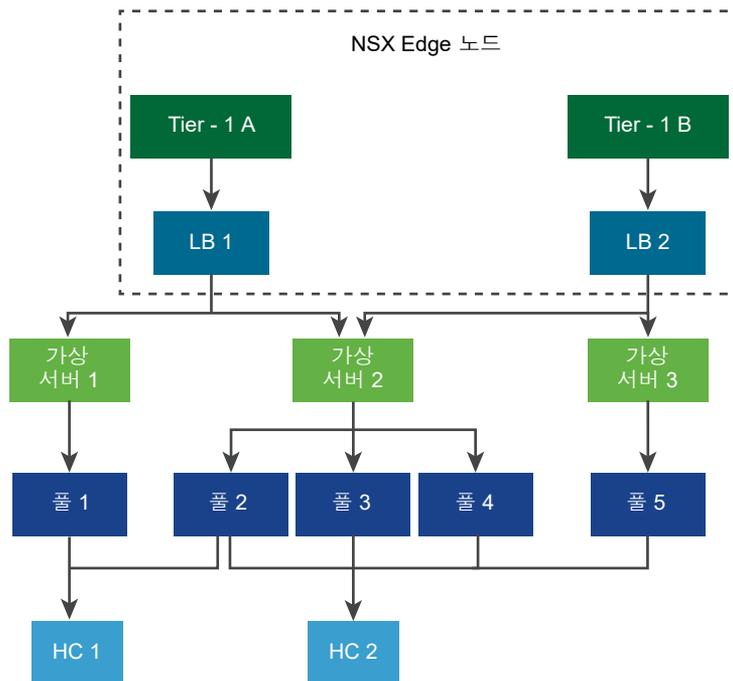
- 키 로드 밸런서 개념
- 로드 밸런서 구성 요소 구성

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.

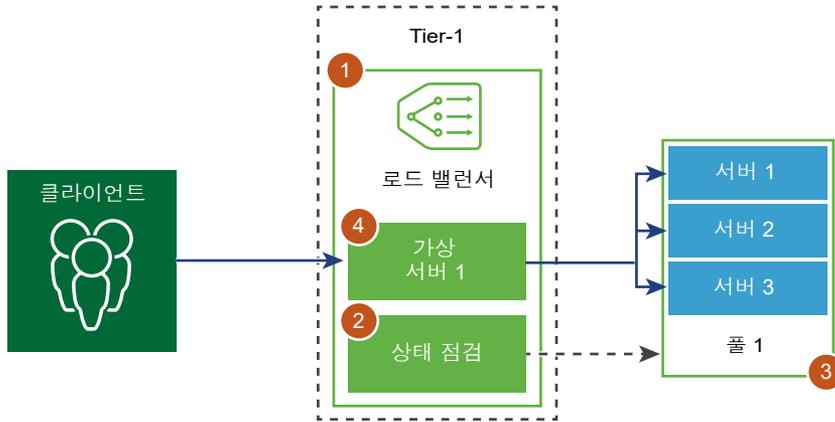
각 서버가 애플리케이션을 올바르게 실행하는지 테스트하려면 서버의 상태를 점검하는 상태 점검 모니터를 추가하십시오.



로드 밸런서 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.

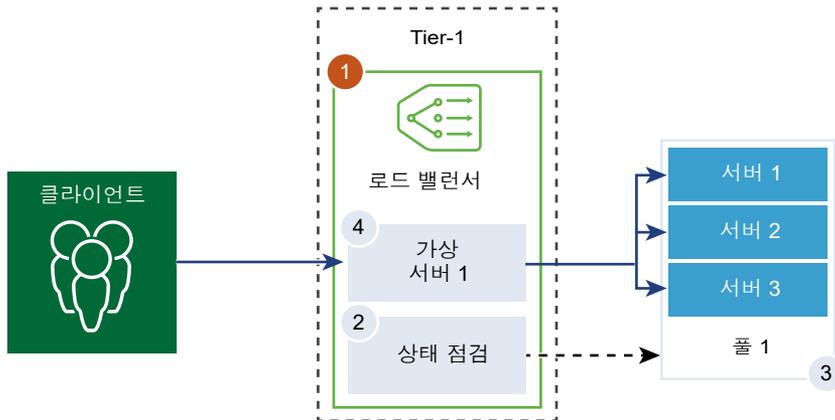


로드 밸런서 생성

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 생성의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 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

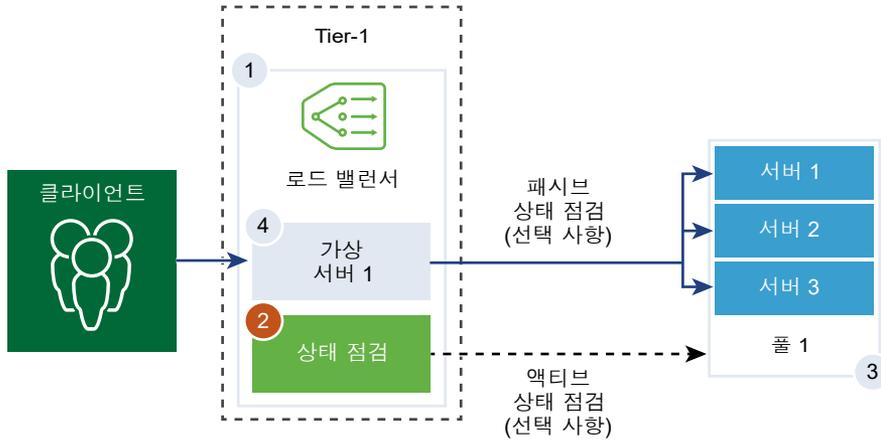
액티브 상태 모니터는 서버가 사용 가능한지 여부를 테스트하는 데 사용됩니다. 액티브 상태 모니터는 서버에 기본 ping을 보내거나 애플리케이션 상태를 모니터링하기 위해 고급 HTTP 요청을 보내는 등 여러 유형의 테스트를 사용합니다.

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 게이트웨이(이전에는 Tier-1 논리적 라우터로 지칭함)에 연결된 후 서버 풀 멤버에 액티브 상태 점검이 수행됩니다.

Tier-1 게이트웨이가 Tier-0 게이트웨이에 연결되어 있으면 라우터 링크 포트가 생성되고 해당 IP 주소(일반적으로 100.64.x.x 형식)가 로드 밸런서 서비스의 상태 점검을 수행하는 데 사용됩니다. Tier-1 게이트웨이가 독립 실행형인 경우(중앙 집중식 서비스 포트가 하나만 있고 Tier-0 게이트웨이에 연결되지 않은 경우) 중앙 집중식 서비스 포트 IP 주소는 로드 밸런서 서비스의 상태 점검을 수행하는 데 사용됩니다. 독립 실행형 Tier-1 게이트웨이에 대한 자세한 내용은 독립형 Tier-1 논리적 라우터 생성을 참조하십시오.

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 **고급 네트워킹 및 보안 > 네트워킹 > 로드 밸런서 > 모니터 > 액티브 상태 모니터 > 추가**를 선택합니다.
- 3 액티브 상태 모니터에 대한 설명과 이름을 입력합니다.
- 4 드롭다운 메뉴에서 서버의 상태 점검 프로토콜을 선택합니다.

또한 NSX Manager; http-monitor, https-monitor, Icmp-monitor, Tcp-monitor 및 Udp-monitor 에서 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
HTTP 메서드	드롭다운 메뉴에서 서버 상태를 감지할 메서드를 GET, OPTIONS, POST, HEAD 및 PUT 중에서 선택합니다.
HTTP 요청 URL	메서드에 대한 요청 URI를 입력합니다.
HTTP 요청 버전	드롭다운 메뉴에서 지원되는 요청 버전을 선택합니다. 기본 버전인 HTTP_VERSION_1_1을 수락할 수도 있습니다.
HTTP 요청 본문	요청 본문을 입력합니다. POST 및 PUT 메서드에 유효합니다.
HTTP 응답 코드	모니터가 HTTP 응답 본문의 상태 줄에서 일치할 것으로 예상하는 문자열을 입력합니다. 응답 코드는 쉼표로 구분된 목록입니다. 예: 200,301,302,401.
HTTP 응답 본문	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
HTTP 메서드	드롭다운 메뉴에서 서버 상태를 감지할 메서드를 GET, OPTIONS, POST, HEAD 및 PUT 중에서 선택합니다.
HTTP 요청 URL	메서드에 대한 요청 URI를 입력합니다.
HTTP 요청 버전	드롭다운 메뉴에서 지원되는 요청 버전을 선택합니다. 기본 버전인 HTTP_VERSION_1_1을 수락할 수도 있습니다.
HTTP 요청 본문	요청 본문을 입력합니다. POST 및 PUT 메서드에 유효합니다.
HTTP 응답 코드	모니터가 HTTP 응답 본문의 상태 줄에서 일치할 것으로 예상하는 문자열을 입력합니다. 응답 코드는 쉼표로 구분된 목록입니다. 예: 200,301,302,401.
HTTP 응답 본문	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 문자열 이어야 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 완료를 클릭합니다.

다음에 수행할 작업

액티브 상태 모니터를 서버 풀과 연결합니다. 로드 밸런싱을 위한 서버 풀 추가의 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 **고급 네트워킹 및 보안 > 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 **확인**을 클릭합니다.

다음에 수행할 작업

패시브 상태 모니터를 서버 풀과 연결합니다. 로드 밸런싱을 위한 서버 풀 추가의 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.

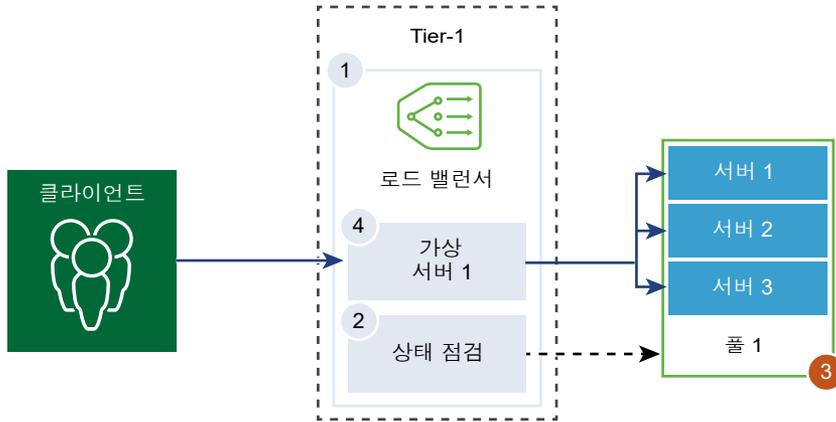
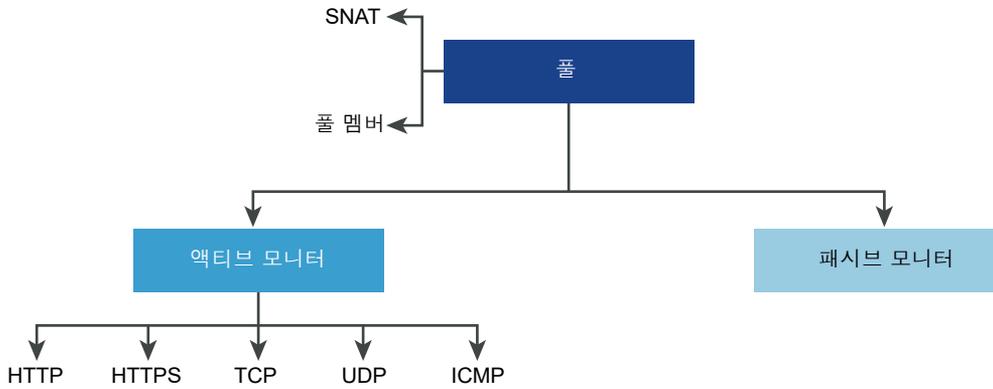


그림 19-1. 서버 풀 매개 변수 구성



사전 요구 사항

- 동적 풀 멤버를 사용하는 경우 NSGroup을 구성해야 합니다. NSGroup 생성의 내용을 참조하십시오.
- 사용하는 모니터링에 따라 액티브 또는 패시브 상태 모니터가 구성되어 있는지 확인합니다. 액티브 상태 모니터 구성 또는 패시브 상태 모니터 구성의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 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 있습니다.
- 관리 상태가 [정상적으로 사용 안 함]으로 설정되어 있고 일치하는 지속성 항목이 없습니다.
- 액티브 또는 패시브 상태 점검 상태가 [종료]입니다.
- 서버 풀 최대 동시 연결에 대한 연결 제한에 도달했습니다.

옵션	설명
ROUND_ROBIN	들어오는 클라이언트 요청이 요청을 처리할 수 있는 사용 가능한 서버 목록을 통해 순환됩니다. 서버 풀 멤버 가중치가 구성되어 있어도 무시합니다.
WEIGHTED_ROUND_ROBIN	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 리소스간에 로드를 균등하게 분산하는데 중점을 둡니다.
LEAST_CONNECTION	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.
WEIGHTED_LEAST_CONNECTION	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 간에 로드를 적절히 분산하는데 중점을 둡니다. 기본적으로 가중치 값은 해당 값이 구성되지 않았으며 느린 시작이 사용되도록 설정된 경우 1입니다.
IP-HASH	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 스퓨핑을 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 처리할 수 있는 로드의 양을 나타냅니다.

백업 멤버로 풀 멤버 지정은 상태 모니터와 작동하여 액티브/대기 상태를 제공합니다. 활성 멤버가 상태 점검에 실패하면 백업 멤버에 대해 트래픽 페일오버가 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.

서버 풀에 대해 액티브 및 패시브 상태 모니터를 설정하는 것은 선택 사항입니다. 액티브 상태 모니터를 선택하고 Tier-1 게이트웨이가 Tier-0 게이트웨이에 연결된 경우 라우터 링크 포트가 생성됩니다. 라우터 링크 포트의 IP 주소(일반적으로 100.64.x.x 형식)는 로드 밸런서 서비스의 상태 점검을 수행하는 데 사용됩니다. Tier-1 게이트웨이가 독립 실행형인 경우(중앙 집중식 서비스 포트가 하나만 있고 Tier-0 게이트웨이에 연결되지 않은 경우) 중앙 집중식 서비스 포트 IP 주소는 로드 밸런서 서비스의 상태 점검을 수행하는 데 사용됩니다. 독립 실행형 Tier-1 게이트웨이에 대한 자세한 내용은 독립형 Tier-1 논리적 라우터 생성을 참조하십시오.

IP 주소가 로드 밸런서 서비스의 상태 점검을 수행하도록 허용하는 방화벽 규칙을 추가합니다.

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.

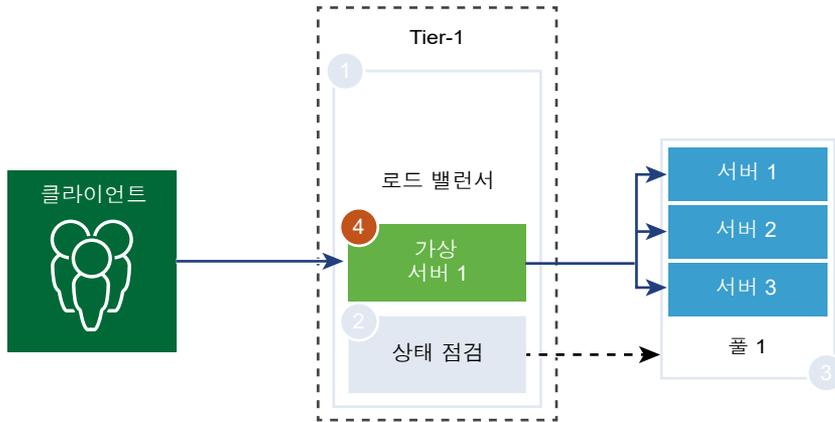
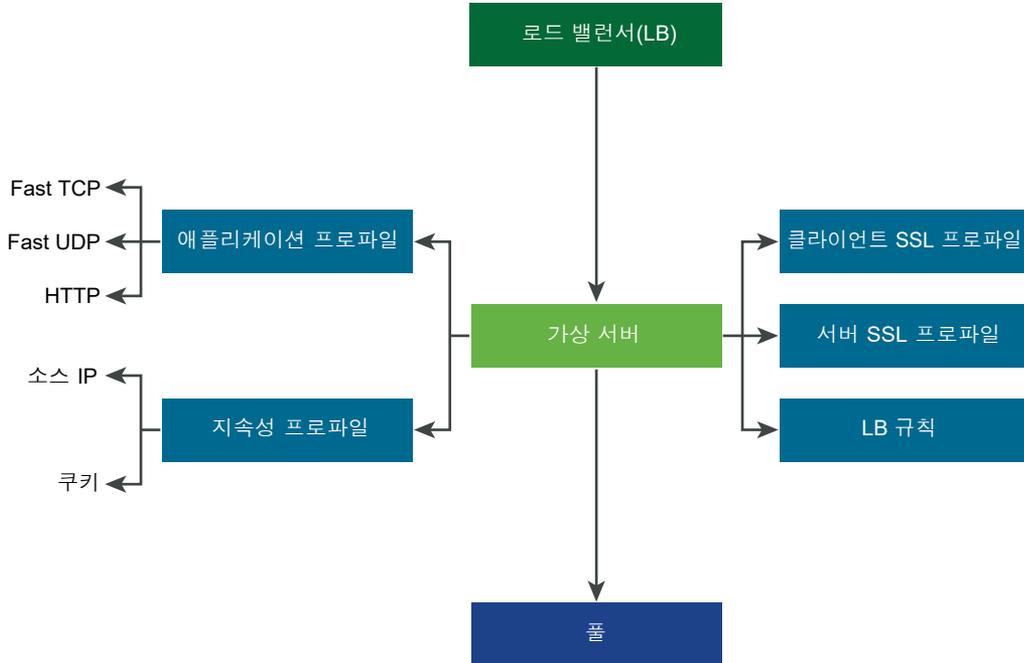


그림 19-2. 가상 서버 구성 요소



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 19-3. 계층 4 TCP 및 UDP 애플리케이션 프로파일

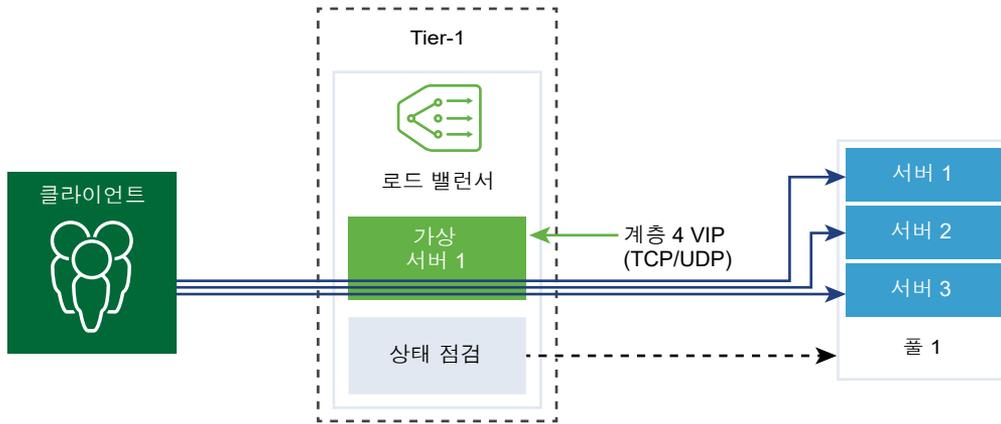
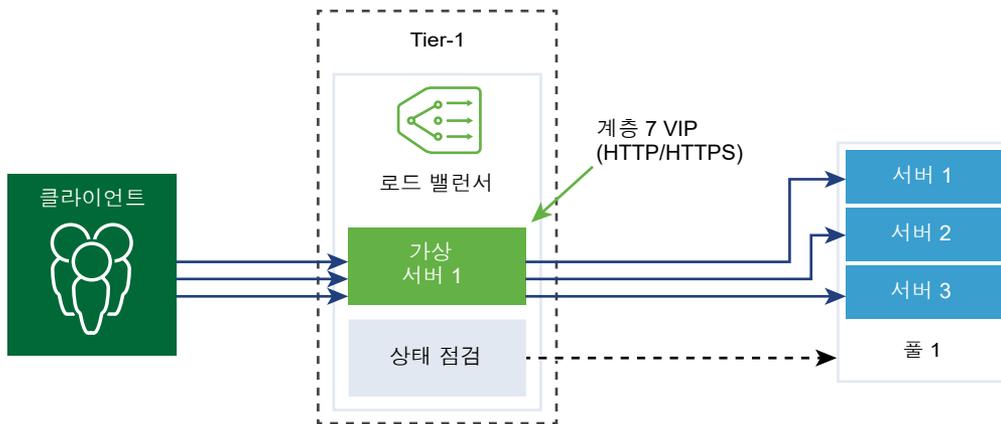


그림 19-4. 계층 7 HTTPS 애플리케이션 프로파일



절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 고급 네트워킹 및 보안 > 네트워킹 > 로드 밸런서 > 프로파일 > 애플리케이션 프로파일을 선택합니다.
- 3 빠른 TCP 애플리케이션 프로파일을 생성합니다.
 - a 드롭다운 메뉴에서 추가 > 빠른 TCP 프로파일을 선택합니다.
 - b 빠른 TCP 애플리케이션 프로파일에 대한 설명과 이름을 입력합니다.

- c 애플리케이션 프로파일 세부 정보를 모두 입력합니다.

빠른 TCP 프로파일 설정 기본값을 수락할 수도 있습니다.

옵션	설명
연결 유휴 시간 제한	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.
연결 닫기 시간 제한	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.
HA 흐름 미러링	버튼을 전환하여 연결된 가상 서버에 대한 모든 흐름을 HA 대기 노드로 미러링합니다.

- d **확인**을 클릭합니다.

4 빠른 UDP 애플리케이션 프로파일을 생성합니다.

UDP 프로파일 설정 기본값을 수락할 수도 있습니다.

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

옵션	설명
유휴 시간 제한	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.
HA 흐름 미러링	버튼을 전환하여 연결된 가상 서버에 대한 모든 흐름을 HA 대기 노드로 미러링합니다.

- d **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
리디렉션	<ul style="list-style-type: none"> ■ 없음 - 웹 사이트가 일시적으로 다운된 경우 페이지를 찾을 수 없음 오류 메시지가 사용자에게 표시됩니다. ■ HTTP 리디렉션 - 웹 사이트가 일시적으로 다운되었거나 이동된 경우 해당 가상 서버에 들어오는 요청이 여기에 지정된 URL로 일시적으로 리디렉션될 수 있습니다. 정적 리디렉션만 지원됩니다. 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. ■ 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. HTTP에서 HTTPS로 리디렉션의 경우, HTTPS 가상 서버에 포트 443이어야 하며 동일한 로드 밸런서에 동일한 가상 서버 IP 주소를 구성해야 합니다. 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.
XFF(X-Forwarded-For)	<ul style="list-style-type: none"> ■ 삽입 - 들어오는 요청에 XFF HTTP 헤더가 없으면 로드 밸런서가 클라이언트 IP 주소로 새 XFF 헤더를 삽입합니다. 들어오는 요청에 XFF HTTP 헤더가 있으면 로드 밸런서가 클라이언트 IP 주소를 XFF 헤더 앞에 붙입니다. ■ 바꾸기 - 들어오는 요청에 XFF HTTP 헤더가 있으면 로드 밸런서가 헤더를 바꿉니다. <p>웹 서버는 요청하는 클라이언트 IP 주소로 처리하는 각 요청을 기록합니다. 이러한 로그는 디버깅 및 분석 용도로 사용됩니다. 배포 토폴로지 인헤 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>
연결 유휴 시간 제한	<p>TCP 애플리케이션 프로파일에 구성해야 하는 TCP 소켓 설정 대신 HTTP 애플리케이션이 유휴 상태로 유지될 수 있는 시간을 초 단위로 입력합니다.</p>
요청 헤더 크기	<p>HTTP 요청 헤더를 저장하는 데 사용되는 최대 버퍼 크기를 바이트 단위로 지정합니다.</p>
NTLM 인증	<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.

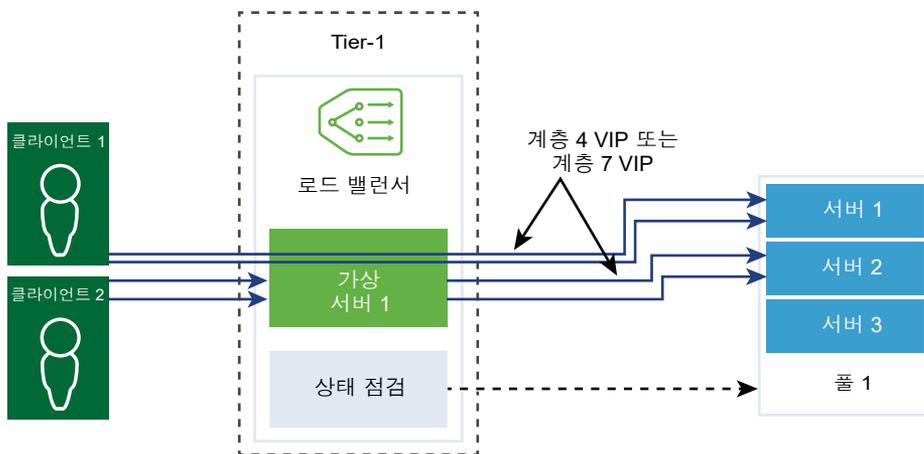
영구 프로파일 구성

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. 쿠키 이름의 공백은 지원되지 **않습니다**.



절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 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
지속성 공유	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.
지속성 항목 시간 초과	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"> ■ 새 연결 요청이 시간 초과 기간 내에 동일한 클라이언트에서 수신되면 지속성 항목이 만료되어 삭제됩니다. ■ 시간 초과 기간 내에 동일한 클라이언트의 새 연결 요청이 수신되면 타이머가 재설정되고 클라이언트 요청이 고정 풀 멤버로 전송됩니다. 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.
HA 지속성 미러링	버튼을 전환하여 지속성 항목을 HA 피어와 동기화합니다.
가득 차면 항목 제거	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
쿠키 모드	드롭다운 메뉴에서 모드를 선택합니다. <ul style="list-style-type: none"> ■ 삽입 - 세션을 식별하는 고유한 쿠키를 추가합니다. ■ 접두사 - 기존 HTTP 쿠키 정보에 추가합니다. ■ 재작성 - 기존 HTTP 쿠키 정보를 재작성합니다.
쿠키 이름	쿠키 이름을 입력합니다. 쿠키 이름의 공백은 지원되지 않습니다 .
쿠키 도메인	도메인 이름을 입력합니다. HTTP 쿠키 도메인은 삽입 모드에서만 구성 할 수 있습니다.
쿠키 경로	쿠키 URL 경로를 입력합니다. HTTP 쿠키 경로는 삽입 모드에서만 설정할 수 있습니다.
쿠키 왜곡	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.
쿠키 대체	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
쿠키 시간 유형	드롭다운 메뉴에서 쿠키 시간 유형을 선택합니다. 세션 쿠키 는 저장되지 않으며 브라우저가 닫히면 손실됩니다. 지속성 쿠키 는 브라우저에서 저장되며 브라우저가 닫히면 손실되지 않습니다.
최대 유효 시간	쿠키가 만료되기 전에 쿠키가 유효 상태일 수 있는 시간(초 단위)을 입력합니다.
최대 쿠키 사용 기간	세션 쿠키 만 해당. 쿠키가 활성 상태가 될 수 있는 최대 기간(초)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 19-5. SSL 오프로딩

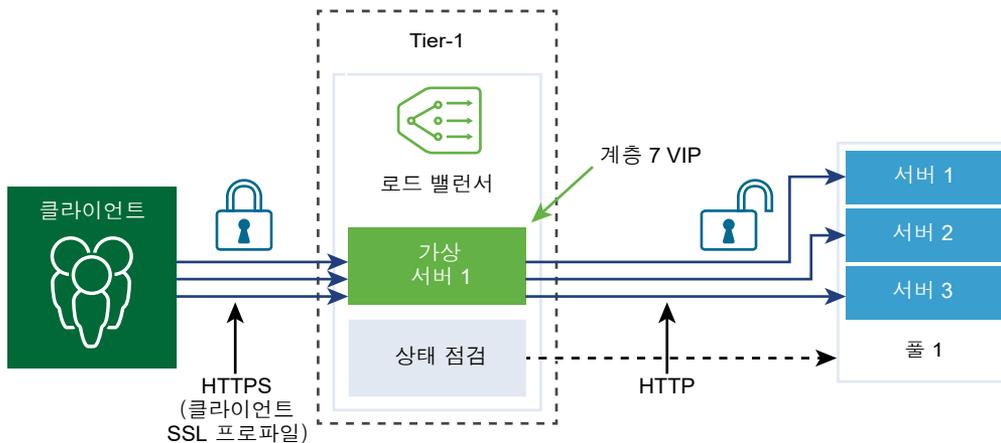
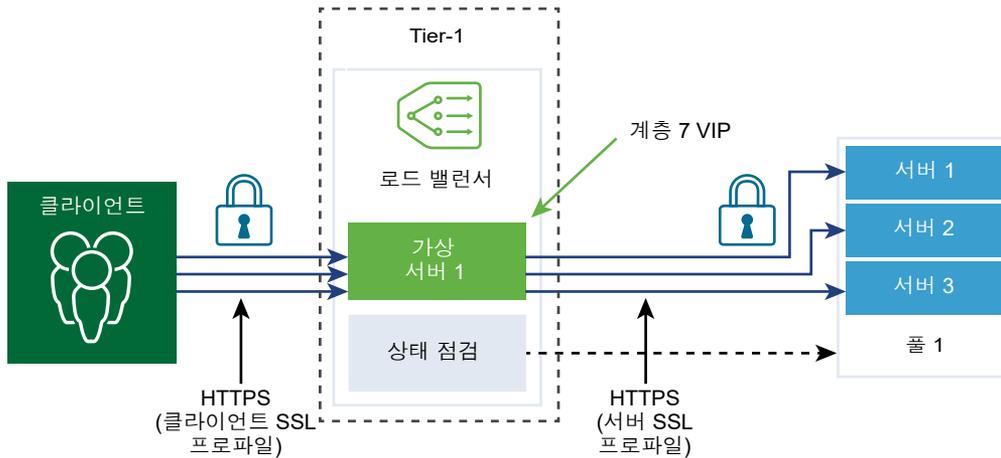


그림 19-6. 종단 간 SSL



절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 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 구성의 내용을 참조하십시오.
- 영구 프로파일을 사용할 수 있는지 확인합니다. 영구 프로파일 구성의 내용을 참조하십시오.
- 클라이언트와 서버에 대한 SSL 프로파일을 사용할 수 있는지 확인합니다. SSL 프로파일 구성의 내용을 참조하십시오.
- 서버 풀을 사용할 수 있는지 확인합니다. 로드 밸런싱을 위한 서버 풀 추가의 내용을 참조하십시오.

절차

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

2 **고급 네트워킹 및 보안 > 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
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.

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 프로파일이 있는 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 구성의 내용을 참조하십시오.
- 영구 프로파일을 사용할 수 있는지 확인합니다. 영구 프로파일 구성의 내용을 참조하십시오.
- 클라이언트와 서버에 대한 SSL 프로파일을 사용할 수 있는지 확인합니다. SSL 프로파일 구성의 내용을 참조하십시오.
- 서버 풀을 사용할 수 있는지 확인합니다. 로드 밸런싱을 위한 서버 풀 추가의 내용을 참조하십시오.
- CA 및 클라이언트 인증서를 사용할 수 있는지 확인합니다. 인증서 서명 요청 파일 생성의 내용을 참조하십시오.
- CRL(인증 해지 목록)을 사용할 수 있는지 확인합니다. 인증서 해지 목록 가져오기의 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 **고급 네트워킹 및 보안 > 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 \1부터 \9까지 사용할 수 있습니다.
- \ddd 형식이 아닌 \Odd 형식을 사용하여 8진수 문자와 일치시킵니다.
- 내장형 플래그는 최상위 레벨에서 지원되지 않으며 그룹 내에서만 지원됩니다. 예를 들어 "Case (?i:sensitive)" 대신 "Case ((?i:sensitive))"를 사용하십시오.
- 전처리 작업 \l, \u, \L, \U가 지원되지 않습니다. 여기서 \l - 다음 문자 소문자, \u - 다음 문자 대문자, \L - \E까지 소문자, \U - \E까지 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 \u2018를 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.html과 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=\$article과 같이 일치된 변수를 사용하여 URI를 다시 작성할 수 있습니다. 그러면 URI가 /news.py?year=2018&month=06&day=15&article=news1234.html로 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_addr로 작성될 수 있습니다. 그러면 예제 URI가 /news.py?year=2018&month=06&day=15&article=news1234.html&user_ip=1.1.1.1로 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

- `$_arg_<name>` - 요청 줄의 인수 `<name>`
- `$_cookie_<name>` - `<name>` 쿠키의 값
- `$_upstream_cookie_<name>` - "Set-Cookie" 응답 헤더 필드에서 업스트림 서버가 보낸 지정된 이름의 쿠키
- `$_upstream_http_<name>` - 임의 응답 헤더 필드이며 `<name>`은 소문자로 변환된 필드 이름이고 대시는 밑줄로 대체됨
- `$_host` - 우선 순위에 따라 - 요청 라인의 호스트 이름 또는 "Host" 요청 헤더 필드의 호스트 이름 또는 요청과 일치하는 서버 이름
- `$_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
- `$_uri` - 요청의 URI 경로
- `$_ssl_ciphers`: 클라이언트 SSL 암호를 반환함
- `$_ssl_c_i_dn`: RFC 2253에 따라 설정된 SSL 연결에 대한 클라이언트 인증서의 "발급자 DN" 문자열을 반환함
- `$_ssl_client_s_dn`: RFC 2253에 따라 설정된 SSL 연결에 대한 클라이언트 인증서의 "주체 DN" 문자열을 반환함
- `$_ssl_protocol`: 설정된 SSL 연결의 프로토콜을 반환함
- `$_ssl_session_reused`: SSL 세션을 재사용하는 경우 "r"을 반환하고, 그렇지 않은 경우 "."를 반환함

사전 요구 사항

계층 7 가상 서버를 사용할 수 있는지 확인합니다. 계층 7 가상 서버 구성의 내용을 참조하십시오.

절차

- 1 계층 7 가상 서버를 엽니다.
- 2 [가상 서버 식별자] 페이지로 건너뛩니다.
- 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. http_request.method - 일치시킬 값
HTTP 요청 URI	쿼리 인수 없이 HTTP 요청 URI를 일치시킵니다. http_request.uri - 일치시킬 값
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

지원되는 일치 조건	설명
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
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 주소를 일치시킵니다. ip_header.source_address - 일치시킬 소스 주소
작업	설명
거절	예를 들면 상태를 5xx로 설정하여 요청을 거부합니다. http_forward.reply_status - 거부하는 데 사용되는 HTTP 상태 코드 http_forward.reply_message - HTTP 거부 메시지
리디렉션	요청을 리디렉션합니다. 상태 코드를 3xx로 설정해야 합니다. http_forward.redirect_status - 리디렉션을 위한 HTTP 상태 코드 http_forward.redirect_url - HTTP 리디렉션 URL
풀 선택	요청을 특정 서버 풀에 강제 적용합니다. 지정된 풀 멤버의 구성된 알고리즘(예측자)은 서버 풀 내에서 서버를 선택하는 데 사용됩니다. hhttp_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
HTTP 응답 헤더	HTTP 응답 헤더를 일치시킵니다. http_response.header_name - 일치시킬 헤더 이름 http_response.header_value - 일치시킬 값
작업	설명
HTTP 응답 헤더 다시 쓰기	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 완료를 클릭합니다.

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 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 Fast 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 건너뛩니다.
- 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 **다음**을 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 **다음**을 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** 완료를 클릭합니다.

참고 고급 네트워킹 및 보안 사용자 인터페이스를 사용하여 정책 인터페이스에서 생성된 개체를 수정하는 경우 일부 설정을 구성하지 못할 수 있습니다. 이러한 읽기 전용 설정에는 옆에 ⊖ 아이콘이 있습니다. 자세한 내용은 [장 1 NSX Manager 개요](#) 항목을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- 논리적 라우터에 방화벽 규칙 추가 또는 삭제
- 논리 스위치 브리지 포트에 대한 방화벽 구성
- 방화벽 섹션 및 방화벽 규칙
- 방화벽 규칙 정보

논리적 라우터에 방화벽 규칙 추가 또는 삭제

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

Edge 방화벽은 업링크 라우터 포트에서 구현됩니다. 즉, 방화벽 규칙은 트래픽이 Edge의 업링크 라우터 포트에 도달하는 경우에만 적용됩니다. 특정 IP 대상에 방화벽 규칙을 적용하려면 /32 네트워크를 사용하여 그룹을 구성해야 합니다. /32 이외의 서브넷을 제공하는 경우 방화벽 규칙이 전체 서브넷에 적용됩니다.

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 **고급 네트워킹 및 보안 > 네트워킹 > 라우터**를 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 활성화-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 활성화-대기 모드에서 실행되도록 구성합니다.

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 생성의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **고급 네트워킹 및 보안 > 보안 > 브리지 방화벽**를 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 섹션 및 방화벽 규칙

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 지침이 포함되어 있습니다. 판매 및 엔지니어링 부서에 대한 특정 규칙이 별도의 섹션에 있는 경우처럼, 섹션은 다중 테넌시에 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.

분산 방화벽 사용 및 사용 안 함

분산 방화벽 기능을 사용하거나 사용하지 않도록 설정할 수 있습니다.

사용하지 않도록 설정하는 경우 데이터부 수준에서 방화벽 규칙이 적용되지 않습니다. 다시 사용하도록 설정하면 규칙이 다시 적용됩니다.

절차

- 1 고급 네트워킹 및 보안 > 보안 > 분산 방화벽로 이동합니다.
- 2 설정 탭을 클릭합니다.
- 3 분산 방화벽 편집을 클릭합니다.
- 4 대화 상자에서 방화벽 상태를 녹색(사용) 또는 회색(사용 안 함)으로 전환합니다.
- 5 저장을 클릭합니다.

방화벽 규칙 섹션 추가

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

절차

- 1 고급 네트워킹 및 보안 > 보안 > 분산 방화벽를 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. TCP 및 UDP 흐름의 경우 첫 번째 패킷 이후에 방화벽 결과가 [허용]인 경우 트래픽 튜플에 대해 캐시가 생성 및 유지 관리됩니다. 즉, 방화벽 규칙에 따라 트래픽을 더 이상 확인할 필요가 없으므로 지연 시간이 줄어듭니다. 따라서 상태 비저장 방화벽은 트래픽 부하가 심한 경우에 일반적으로 더 빠르고 성능이 더 좋습니다.

상태 저장 방화벽은 트래픽 스트림을 처음부터 끝까지 관찰할 수 있습니다. 상태 및 시퀀스 번호를 검증하기 위해 방화벽은 모든 패킷에 대해 항상 확인됩니다. 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 **고급 네트워킹 및 보안 > 보안 > 분산 방화벽**를 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 **고급 네트워킹 및 보안 > 보안 > 분산 방화벽**를 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 **계시**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 ESXi 및 KVM 호스트의 /var/log/dfwpktlogs.log 파일에 저장됩니다.

절차

- 1 **고급 네트워킹 및 보안 > 보안 > 분산 방화벽**를 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 **계시**를 클릭합니다.

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.

참고 NSX-T Data Center는 NSX Manager 및 NSX Edge 노드 가상 시스템을 방화벽 제외 목록에 자동으로 추가합니다.

절차

- 1 **고급 네트워킹 및 보안 > 보안 > 분산 방화벽 > 제외 목록 > 추가**를 선택합니다.
- 2 유형 및 개체를 선택합니다.
사용 가능한 유형에는 **논리적 포트**, **논리적 스위치** 및 **NSGroup**이 있습니다.

3 **확인**을 클릭합니다.

4 제외 목록에서 개체를 제거하려면 개체를 선택하고 메뉴 모음에서 **삭제**를 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 섹션별로 TCP Strict를 사용하도록 설정하여 중간 세션 선택을 해제하고 3방향 핸드셰이크에 대한 요구 사항을 적용할 수 있습니다. 특정 분산 방화벽 섹션에 대해 TCP Strict 모드를 사용하도록 설정하고 기본 임의-임의 차단 규칙을 사용할 경우, 3방향 핸드셰이크 연결 요구 사항을 완료하지 못하고 이 섹션의 TCP 기반 규칙과 일치하는 패킷은 삭제됩니다. Strict는 상태 저장 TCP 규칙에만 적용되며 분산 방화벽 섹션 수준에서 사용하도록 설정됩니다. TCP Strict는 TCP 서비스가 지정되지 않은 기본 임의-임의 허용과 일치하는 패킷에는 적용되지 않습니다.

표 20-1. 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. 소스 또는 대상 범위에 IPv4 및 IPv6 둘 다 지원됩니다.
대상	규칙에 영향을 받는 연결의 대상 IP 또는 MAC 주소/넷마스크입니다. 대상이 정의되지 않은 경우 임의로 일치하는 항목을 찾습니다. 소스 또는 대상 범위에 IPv4 및 IPv6 둘 다 지원됩니다.

표 20-1. 방화벽 규칙의 속성 (계속)

속성	설명
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.
작업	규칙이 적용하는 작업은 허용 , 삭제 또는 거절 입니다. 기본값은 허용 입니다.
IP 프로토콜	옵션은 IPv4 , IPv6 및 IPv4_IPv6 입니다. 기본값은 IPv4_IPv6 입니다. 이 속성에 액세스하려면 고급 설정 아이콘을 클릭합니다.
방향	옵션은 수신 , 송신 및 수신/송신 입니다. 기본값은 수신/송신 입니다. 이 필드는 대상 개체의 관점에서 트래픽 방향을 나타냅니다. 수신 은 개체로 들어오는 트래픽만 확인하고, 송신 은 개체에서 나가는 트래픽만 확인하며, 수신/송신 은 양쪽 방향 트래픽 모두 확인함을 의미합니다. 이 속성에 액세스하려면 고급 설정 아이콘을 클릭합니다.
규칙 태그	규칙에 추가된 태그입니다. 이 속성에 액세스하려면 고급 설정 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 **고급 네트워킹 및 보안 > 보안 > 분산 방화벽**를 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 확인 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 확인 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"> ■ ALG ■ ICMP ■ IGMP ■ IP ■ L4 포트 집합
프로토콜	사용 가능한 프로토콜 중 하나를 선택합니다.

옵션	설명
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 **계시**를 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 **고급 네트워킹 및 보안 > 보안 > 분산 방화벽**를 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 **계시**를 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 **고급 네트워킹 및 보안 > 보안 > 분산 방화벽**를 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 고급 네트워크 및 보안 > 보안 > 분산 방화벽을 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 게시를 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 고급 네트워크 및 보안 > 보안 > 분산 방화벽을 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.

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 로깅, 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.

- 모니터링 대시보드 보기
- 개체 범주의 사용량 및 용량 보기
- 구성 변경의 인식된 상태 확인
- 개체 검색
- 개체 특성별 필터링
- 계산 관리자 추가
- Active Directory 추가
- LDAP 서버 추가
- Active Directory 동기화
- 사용자 계정 및 역할 기반 액세스 제어 관리
- NSX Manager 백업 및 복원
- vCenter Server에서 NSX-T Data Center 확장 제거
- NSX Manager 클러스터 관리
- NSX Edge 클러스터에서 NSX Edge 전송 노드 교체
- vCenter Server가 손실되어 복구할 수 없는 경우 NSX-T 복구
- NSX-T Data Center 다중 사이트 배포
- 장치 구성
- 라이선스 키 추가 및 라이선스 사용량 보고서 생성
- 인증서 설정

- 규정 준수 기반 구성
- 지원 번들 수집
- 로그 메시지 및 오류 코드
- 고객 환경 향상 프로그램
- 개체에 태그 추가
- 원격 서버의 SSH 지문 찾기
- VM에서 실행되는 애플리케이션에 대한 데이터 보기
- 외부 로드 밸런서 구성

모니터링 대시보드 보기

NSX Manager 인터페이스는 시스템 상태, 네트워킹 및 보안, 규정 준수 보고와 관련된 세부 정보를 보여 주는 다양한 모니터링 대시보드를 제공합니다. 이 정보는 NSX Manager 인터페이스 전체에서 표시되거나 액세스 가능하지만 **홈 > 모니터링 대시보드** 페이지에서도 액세스할 수 있습니다.

NSX Manager 인터페이스의 홈페이지에서 모니터링 대시보드에 액세스할 수 있습니다. 대시보드에서 클릭하면서 대시보드 데이터를 끌어온 소스 페이지에 액세스할 수 있습니다.

절차

- 1 NSX Manager 인터페이스에 관리자로 로그인합니다.
- 2 아직 홈페이지에 있지 않은 경우 **홈**을 클릭합니다.
- 3 [모니터링 대시보드]를 클릭하고 드롭다운 메뉴에서 원하는 대시보드 범주를 선택합니다.
 선택한 범주의 대시보드가 페이지에 표시됩니다. 대시보드 그래픽은 색으로 구분되며, 대시보드 바로 위에 색 코드 키가 표시됩니다.
- 4 보다 세부적인 수준에 액세스하려면 대시보드의 제목 또는 대시보드의 요소 중 하나를 클릭합니다(활성화된 경우).

다음 표에서는 기본 대시보드와 해당 소스에 대해 설명합니다.

표 21-1. 시스템 대시보드

대시보드	소스	설명
시스템	시스템 > 장치 > 개요	NSX Manager 클러스터의 상태와 리소스(CPU, 메모리, 디스크) 사용량을 표시합니다.
패브릭	시스템 > 패브릭 > 노드 시스템 > 패브릭 > 전송 영역 시스템 > 패브릭 > 계산 관리자	호스트 및 Edge 전송 노드, 전송 영역 및 계산 관리자를 포함하는 NSX-T 패브릭을 표시합니다.

표 21-1. 시스템 대시보드 (계속)

대시보드	소스	설명
백업	시스템 > 백업 및 복원	구성된 경우 NSX-T 백업의 상태를 표시합니다. SFTP 사이트에 원격으로 저장된 스케줄링된 백업을 구성하는 것이 좋습니다.
끝점 보호	시스템 > 서비스 배포	끝점 보호 배포의 상태를 표시합니다.

표 21-2. 네트워킹 및 보안 대시보드

대시보드	소스	설명
보안	인벤토리 > 그룹 보안 > 분산 방화벽	그룹의 상태 및 보안 정책을 표시합니다. 그룹은 East-West 방화벽 규칙을 포함하는 보안 정책이 적용될 수 있는 워크로드, 세그먼트, 세그먼트 포트 및 IP 주소의 모음입니다.
게이트웨이	네트워킹 > Tier-0 게이트웨이 네트워킹 > Tier-1 게이트웨이	Tier-0 및 Tier-1 게이트웨이의 상태를 표시합니다.
세그먼트	네트워킹 > 세그먼트	네트워크 세그먼트의 상태를 표시합니다.
로드 밸런서	네트워킹 > 로드 밸런싱	로드 밸런서 VM의 상태를 표시합니다.
VPN	네트워킹 > VPN	가상 개인 네트워크의 상태를 표시합니다.

표 21-3. 고급 네트워킹 및 보안 대시보드

대시보드	소스	설명
로드 밸런서	고급 네트워킹 및 보안 > 로드 밸런서	로드 밸런서 서비스, 로드 밸런서 가상 서버 및 로드 밸런서 서버 풀의 상태를 표시합니다. 로드 밸런서는 하나 이상의 가상 서버를 호스팅할 수 있습니다. 가상 서버는 애플리케이션을 호스팅하는 멤버를 포함하는 서버 풀에 바인딩됩니다.
방화벽	고급 네트워킹 및 보안 > 보안 > 분산 방화벽 고급 네트워킹 및 보안 > 보안 > 브리지 방화벽 고급 네트워킹 및 보안 > 네트워킹 > 라우터	방화벽을 사용하도록 설정했는지 여부를 나타내고 정책, 규칙 및 제외 목록 멤버의 수를 표시합니다. 참고 이 대시보드에 표시되는 각 세부 항목은 인용된 소스 페이지의 특정 하위 탭에서 시작됩니다.
VPN	해당 없음.	가상 개인 네트워크의 상태와 열려 있는 IPSec 및 L2 VPN 세션의 수를 표시합니다.
스위칭	고급 네트워킹 및 보안 > 스위칭	VM 및 컨테이너 포트를 포함하여 논리적 스위치 및 논리적 포트의 상태를 표시합니다.

표 21-4. 규정 준수 보고서 대시보드

열	설명
규정 비준수 코드	특정 규정 비준수 코드를 표시합니다.
설명	규정 비준수 상태의 구체적인 원인.

표 21-4. 규정 준수 보고서 대시보드 (계속)

열	설명
리소스 이름	규정 비준수의 NSX-T 리소스(노드, 스위치 및 프로파일).
리소스 유형	원인의 리소스 유형.
영향을 받는 리소스	영향을 받는 리소스 수. 숫자 값을 클릭하여 목록을 봅니다.

각 장치 보고서 코드에 대한 자세한 내용은 [규정 준수 상태 보고서 코드](#)를 참조하십시오.

개체 범주의 사용량 및 용량 보기

NSX-T Data Center 환경에서 다양한 범주의 개체에 대한 사용량 및 용량을 볼 수 있습니다. 특정 사용량 임계값에 도달했을 때 쉽게 알 수 있도록 경고를 설정할 수도 있습니다.

다른 개체 범주의 사용량 및 용량을 보려면 다음 탭 중 하나를 클릭하십시오.

- [네트워킹 > 네트워크 개요 > 용량](#)
- [보안 > 보안 개요 > 용량](#)
- [인벤토리 > 인벤토리 개요 > 용량](#)
- [시스템 > 시스템 개요 > 용량](#)

[계획 및 문제 해결 > 통합 용량](#)으로 이동하여 모든 개체 범주를 한 페이지에서 볼 수도 있습니다.

각 용량 페이지에는 각 개체 범주에 관한 다음 정보가 표시됩니다.

- **최대 용량** - 이 값은 대형 장치의 용량을 기준으로 합니다.
- **현재 인벤토리(인식됨)** - 성공적으로 생성 또는 구성된 개체 수입니다. 이 개수에는 **고급 네트워킹 및 보안** 탭에 표시된 NSX Manager 개체가 반영됩니다. 이러한 개체에는 **네트워킹, 보안, 인벤토리** 또는 **시스템** 탭에서 생성한 일부 항목이 포함될 수 있습니다. 사용 비율을 나타내는 색으로 구분된 막대가 표시됩니다. 사용량이 주의 경고 수준 미만이면 녹색으로 표시됩니다. 사용량이 주의 경고 수준 이상, 위험 경고 수준 미만이면 주황색으로 표시됩니다. 사용량이 위험 경고 수준 이상이면 빨간색으로 표시됩니다.
- **주의 경고** - 위에서 언급한 사용량 표시줄에 주황색이 표시되는 사용량 수준입니다. 이 값을 변경할 수 있습니다.
- **위험 경고** - 위에서 언급한 사용량 표시줄에 빨간색이 표시되는 사용량 수준입니다. 이 값을 변경할 수 있습니다.

주의 경고 또는 위험 경고 값을 변경할 때 **되돌리기**를 클릭하여 마지막으로 저장한 값으로 돌아갈 수 있습니다. **값 재설정**을 클릭하여 모든 개체 범주의 기본값을 복원할 수 있습니다.

[네트워킹 용량] 페이지에는 다음과 같은 개체 범주가 표시됩니다.

- Tier-0 논리적 라우터
- Tier-1 논리적 라우터

- 접두사 목록
- 시스템 전체 NAT 규칙
- DHCP 서버 인스턴스
- 시스템 전체 DHCP 범위 및 풀
- NAT를 사용하도록 설정한 Tier 1 논리적 라우터
- 논리적 스위치
- 시스템 전체 논리적 스위치 포트

[보안 용량] 페이지에는 다음과 같은 개체 범주가 표시됩니다.

- 시스템 전체 끝점 보호 사용 호스트
- 시스템 전체 끝점 보호 사용 가상 시스템
- Active Directory 그룹
- Active Directory 도메인
- 분산 방화벽 규칙
- 시스템 전체 방화벽 규칙
- 시스템 전체 방화벽 섹션
- 분산 방화벽 섹션

[인벤토리 용량] 페이지에는 다음과 같은 개체 범주가 표시됩니다.

- 네트워킹 및 보안 그룹
- IP 집합
- IP 집합 기반 그룹
- vCenter 클러스터
- 하이퍼바이저 호스트

[시스템 용량] 페이지에는 다음과 같은 개체 범주가 표시됩니다.

- 시스템 전체 가상 인터페이스
- Edge 클러스터
- 시스템 전체 Edge 노드

구성 변경의 인식된 상태 확인

구성을 변경하면 NSX Manager는 일반적으로 변경을 구현하기 위해 다른 구성 요소에 요청을 전송합니다. 일부 계층 3 엔티티의 경우 API를 사용하여 구성을 변경하는 경우 요청의 상태를 추적하여 변경이 성공적으로 구현되었는지 확인할 수 있습니다.

시작하는 구성 변경을 원하는 상태라고 합니다. 변경 구현의 결과를 인식된 상태라고 합니다. NSX Manager가 성공적으로 변경을 구현하면 인식된 상태가 원하는 상태와 동일하게 됩니다. 오류가 있는 경우 인식된 상태가 원하는 상태와 동일하지 않게 됩니다.

일부 계층 3 엔티티의 경우 구성을 변경하기 위해 API를 호출하는 경우 응답에 매개 변수 request_id가 포함됩니다. 매개 변수 request_id 및 entity_id를 사용하여 API를 호출하여 요청의 상태를 확인할 수 있습니다.

이 기능은 다음 엔티티 및 API를 지원합니다.

```

EdgeCluster
  POST /edge-clusters
  PUT /edge-clusters/<edge-cluster-id>
  DELETE /edge-clusters/<edge-cluster-id>
  POST /edge-clusters/<edge-cluster-id>?action=replace_transport_node

LogicalRouter
  POST /logical-routers
  PUT /logical-routers/<logical-router-id>
  DELETE /logical-routers/<logical-router-id>
  POST /logical-routers/<logical-router-id>?action=reprocess
  POST /logical-routers/<logical-router-id>?action=reallocate

LogicalRouterPort
  POST /logical-router-ports
  PUT /logical-router-ports/<logical-router-port-id>
  DELETE /logical-router-ports/<logical-router-port-id>

StaticRoute
  POST /logical-routers/<logical-router-id>/routing/static-routes
  PUT /logical-routers/<logical-router-id>/routing/static-routes/<static-route-id>
  DELETE /logical-routers/<logical-router-id>/routing/static-routes/<static-route-id>

BGPConfig
  PUT /logical-routers/<logical-router-id>/routing/bgp

BgpNeighbor
  POST /logical-routers/<logical-router-id>/routing/bgp/neighbors
  PUT /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
  DELETE /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
  POST /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>

BGPCommunityList
  POST /logical-routers/<logical-router-id>/routing/bgp/community-lists
  PUT /logical-routers/<logical-router-id>/routing/bgp/community-lists/<community-list-id>
  DELETE /logical-routers/<logical-router-id>/routing/bgp/community-lists/<community-list-id>

AdvertisementConfig
  PUT /logical-routers/<logical-router-id>/routing/advertisement

AdvertiseRouteList
  PUT /logical-routers/<logical-router-id>/routing/advertisement/rules

```

```

NatRule
  POST /logical-routers/<logical-router-id>/nat/rules
  PUT /logical-routers/<logical-router-id>/nat/rules/<rule-id>
  DELETE /logical-routers/<logical-router-id>/nat/rules/<rule-id>

DhcpRelayService
  POST /dhcp/relays
  PUT /dhcp/relays/<relay-id>
  DELETE /dhcp/relays/<relay-id>

DhcpRelayProfile
  POST /dhcp/relay-profiles
  PUT /dhcp/relay-profiles/<relay-profile-id>
  DELETE /dhcp/relay-profiles/<relay-profile-id>

StaticHopBfdPeer
  POST /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers
  PUT /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers/<bfd-peers-id>
  DELETE /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers/<bfd-peers-id>

IPPrefixList
  POST /logical-routers/<logical-router-id>/routing/ip-prefix-lists
  PUT /logical-routers/<logical-router-id>/routing/ip-prefix-lists/<ip-prefix-list-id>
  DELETE /logical-routers/<logical-router-id>/routing/ip-prefix-lists/<ip-prefix-list-id>

RouteMap
  POST /logical-routers/<logical-router-id>/routing/route-maps
  PUT /logical-routers/<logical-router-id>/routing/route-maps/<route-map-id>
  DELETE /logical-routers/<logical-router-id>/routing/route-maps/<route-map-id>

RedistributionConfig
  PUT /logical-routers/<logical-router-id>/routing/redistribution

RedistributionRuleList
  PUT /logical-routers/<logical-router-id>/routing/redistribution/rules

BfdConfig
  PUT /logical-routers/<logical-router-id>/routing/bfd-config

MplsConfig
  PUT /logical-routers/<logical-router-id>/routing/mps

RoutingGlobalConfig
  PUT /logical-routers/<logical-router-id>/routing

IPSecVPNIKEProfile
  POST /vpn/ipsec/ike-profiles
  PUT /vpn/ipsec/ike-profiles/<ike-profile-id>
  DELETE /vpn/ipsec/ike-profiles/<ike-profile-id>

IPSecVPNDPDProfile
  POST /vpn/ipsec/dpd-profiles
  PUT /vpn/ipsec/dpd-profiles/<dpd-profile-id>
  DELETE /vpn/ipsec/dpd-profiles/<dpd-profile-id>

IPSecVPNTunnelProfile

```

```

POST /vpn/ipsec/tunnel-profiles
PUT /vpn/ipsec/tunnel-profiles/<tunnel-profile-id>
DELETE /vpn/ipsec/tunnel-profiles/<tunnel-profile-id>

```

IPSecVPNLocalEndpoint

```

POST /vpn/ipsec/local-endpoints
PUT /vpn/ipsec/local-endpoints/<local-endpoint-id>
DELETE /vpn/ipsec/local-endpoints/<local-endpoint-id>

```

IPSecVPNPeerEndpoint

```

POST /vpn/ipsec/peer-endpoints
PUT /vpn/ipsec/peer-endpoints/<peer-endpoint-id>
DELETE /vpn/ipsec/peer-endpoints/<peer-endpoint-id>

```

IPSecVPNService

```

POST /vpn/ipsec/services
PUT /vpn/ipsec/services/<service-id>
DELETE /vpn/ipsec/services/<service-id>

```

IPSecVPNSession

```

POST /vpn/ipsec/sessions
PUT /vpn/ipsec/sessions/<session-id>
DELETE /vpn/ipsec/sessions/<session-id>

```

DhcpServer

```

POST /dhcp/servers
PUT /dhcp/servers/<server-id>
DELETE /dhcp/servers/<server-id>

```

DhcpStaticBinding

```

POST /dhcp/servers/static-bindings
PUT /dhcp/servers/<server-id>/static-bindings/<binding-id>
DELETE /dhcp/servers/<server-id>/static-bindings/<binding-id>

```

DhcpIpPool

```

POST /dhcp/servers/ip-pools
PUT /dhcp/servers/<server-id>/ip-pools/<pool-id>
DELETE /dhcp/servers/<server-id>/ip-pools/<pool-id>

```

DnsForwarder

```

POST /dns/forwarders
PUT /dns/forwarders/<forwarder-id>
DELETE /dns/forwarders/<forwarder-id>

```

다음 API를 호출하여 인식된 상태를 가져올 수 있습니다.

EdgeCluster

Request - GET /edge-clusters/<edge-cluster-id>/state?request_id=<request-id>

Response - An instance of EdgeClusterStateDto which will inherit ConfigurationState. If the edge cluster is deleted then the state will be unknown and it will return the common entity not found error.

LogicalRouter / All L3 Entities - All L3 entities can use this API to get realization state

Request - GET /logical-routers/<logical-router-id>/state?request_id=<request-id>

Response - An instance of LogicalRouterStateDto which will inherit ConfigurationState. Delete

operation of any entity other than logical router can be covered by getting the state of logical router but if the logical router itself is deleted then the state will be unknown and it will return the common entity not found error.

LogicalServiceRouterCluster - All L3 entities which are the part of services can use this API to get the realization state

Request - GET /logical-routers/<logical-router-id>/service-cluster/state?request_id=<request-id>

Response - An instance of LogicalServiceRouterClusterState which will inherit ConfigurationState.

LogicalRouterPort / DhcpRelayService / DhcpRelayProfile

Request - GET /logical-router-ports/<logical-router-port-id>/state?request_id=<request-id>

Response - An instance of LogicalRouterPortStateDto which will inherit ConfigurationState.

IPSecVPNIKEProfile / IPSecVPNDPDProfile / IPSecVPNTunnelProfile / IPSecVPNLocalEndpoint / IPSecVPNPeerEndpoint / IPSecVPNService / IPSecVPNSession

Request - GET /vpn/ipsec/sessions/<session-id>/state?request_id=<request-id>

Response - An instance of IPSecVPNSessionStateDto which will inherit ConfigurationState. If the session is deleted then the state will be unknown and it will return the common entity not found error. When IPSecVPNService is disabled, IKE itself is down and it does not respond. It will return unknown state in such a case.

DhcpServer

Request - GET /dhcp/servers/<server-id>/state?request_id=<request-id>

Response - An instance of ConfigurationState.

DhcpStaticBinding

Request - GET /dhcp/servers/<server-id>/static-bindings/<binding-id>/state?request_id=<request-id>

Response - An instance of ConfigurationState.

DhcpIpPool

Request - GET /dhcp/servers/<server-id>/ip-pools/<pool-id>/state?request_id=<request-id>

Response - An instance of ConfigurationState.

DnsForwarder

Request - GET /dns/forwarders/<forwarder-id>/state?request_id=<request-id>

Response - An instance of ConfigurationState.

API에 대한 자세한 내용은 "NSX-T Data Center API 참조" 를 참조하십시오.

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 Logical이 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.

개체 특성별 필터링

NSX Manager에서 개체를 볼 때 하나 이상의 특성을 기준으로 개체를 필터링할 수 있습니다. 예를 들어, Tier-0 게이트웨이의 세부 정보를 보는 경우 **상태**를 기준으로 필터링하여 **종료** 상태의 게이트웨이만 볼 수 있습니다.

다음 유형의 필터를 사용할 수 있습니다.

- 미리 정의된 필터 - 개체에 적용할 수 있는 일반적으로 사용되는 필터 목록입니다.
- 텍스트 기반 필터 - 입력한 특성 값을 기준으로 하는 필터입니다. 이 필터는 개체의 **이름, 태그, 경로** 및 **설명** 특성에만 적용됩니다.
- 특성-값 쌍 - 필터링할 특성-값 쌍을 지정하는 데 사용할 수 있는 특성 드롭다운 메뉴입니다.

한 개체의 여러 특성을 사용하거나 단일 특성의 여러 값을 사용해 개체를 필터링할 수 있습니다. 여러 특성을 선택하는 경우 **AND** 연산자가 적용되지만 단일 특성의 여러 값을 지정할 때는 **OR** 연산자를 사용합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 보려는 개체를 표시하는 탭으로 이동합니다.
- 3 개체를 필터링하는 데 사용할 특성을 지정합니다.
 -  아이콘을 클릭하고 미리 정의된 필터 목록에서 선택합니다.
 - **이름, 태그, 경로** 또는 **설명** 특성에 값을 입력합니다.
 - 드롭다운 메뉴에서 특성을 선택하고 해당 값을 지정합니다. 예를 들어 **상태: 종료**를 지정합니다. 필터 조건을 충족하는 개체가 표시됩니다.
- 4 (선택 사항) 필터를 재설정하려면 **지우기**를 클릭합니다.

계산 관리자 추가

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

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

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

Extension.Register extension
Extension.Unregister extension
Extension.Update extension
Sessions.Message
Sessions.Validate session
Sessions.View and stop sessions
Host.Configuration.Maintenance

Host.Local Operations.Create virtual machine
Host.Local Operations.Delete virtual machine
Host.Local Operations.Reconfigure virtual machine
Tasks
Scheduled task
Global.Cancel task
Permissions.Reassign role permissions
Resource.Assign vApp to resource pool
Resource.Assign virtual machine to resource pool
Virtual Machine.Configuration
Virtual Machine.Guest Operations
Virtual Machine.Provisioning
Virtual Machine.Inventory
Network.Assign network
vApp

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

사전 요구 사항

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

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

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 패브릭 > 계산 관리자 > 추가**를 선택합니다.
- 3 계산 관리자 세부 정보를 완료합니다.

옵션	설명
이름 및 설명	vCenter Server를 식별하는 이름을 입력합니다. 선택적으로 vCenter Server의 클러스터 수와 같은 특별한 세부 사항을 설명할 수 있습니다.
도메인 이름/IP 주소	vCenter Server의 IP 주소를 입력합니다.

옵션	설명
유형	기본 옵션을 그대로 둡니다.
사용자 이름 및 암호	vCenter Server 로그인 자격 증명을 입력합니다.
지문	vCenter Server SHA-256 지문 알고리즘 값을 입력합니다.

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

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

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

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

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

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

기존 등록이 있으면 교체됩니다.

결과

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

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

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

Active Directory 추가

Active Directory는 사용자 기반 ID 방화벽 규칙을 생성하는 데 사용됩니다.

Windows 2008은 Active Directory 서버 또는 RDSH 서버 OS로 지원되지 않습니다.

하나 이상의 Windows 도메인을 NSX Manager에 등록할 수 있습니다. NSX Manager는 등록된 각 도메인에서 그룹 및 사용자 정보와 서로 간의 관계를 가져옵니다. 또한 NSX Manager는 AD(Active Directory) 자격 증명을 검색합니다.

Active Directory가 NSX Manager와 동기화되면 사용자 ID를 기준으로 보안 그룹을 생성하고 ID 기반 방화벽 규칙을 생성할 수 있습니다.

참고 ID 방화벽 규칙 적용의 경우 Active Directory를 사용하는 모든 VM에 대해 Windows 시간 서비스를 **설정**해야 합니다. 이렇게 하면 Active Directory와 VM 간에 날짜와 시간이 동기화됩니다. 사용자를 사용하도록 설정하거나 삭제하는 경우를 비롯한 AD 그룹 멤버 자격 변경 시 로그인한 사용자에게 즉시 영향을 주지 않습니다. 변경 사항을 적용하려면 로그아웃했다가 다시 로그인해야 합니다. 그룹 멤버 자격이 수정된 경우 AD 관리자가 강제로 로그아웃해야 합니다. 이 동작은 Active Directory의 제한 사항입니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > Active Directory**로 이동합니다.
- 3 **Active Directory 추가**를 클릭합니다.
- 4 Active Directory의 이름을 입력합니다.
- 5 **NetBios 이름 및 기본 고유 이름**을 입력합니다.

도메인에 대한 netBIOS 이름을 검색하려면 도메인에 포함되거나 도메인 컨트롤러에 있는 Windows 워크스테이션의 명령 창에서 `nbtstat -n`을 입력합니다. NetBIOS 로컬 이름 테이블에서 <00> 접두사가 있고 유형이 그룹인 항목이 NetBIOS 이름입니다.

Active Directory 도메인을 추가하려면 기본 DN(기본 고유 이름)이 필요합니다. 기본 DN은 LDAP 서버가 Active Directory 도메인 내에서 사용자 인증을 검색할 때 사용하는 시작점입니다. 예를 들어, 도메인 이름이 corp.local인 경우, Active Directory의 기본 DN은 "DC=corp,DC=local"입니다.

- 6 필요한 경우 **델타 동기화 간격**을 설정합니다. 델타 동기화는 마지막 동기화 이벤트 이후에 변경된 로컬 AD 개체만 업데이트합니다.

Active Directory에서 변경한 사항은 델타 또는 전체 동기화가 수행될 때까지 NSX Manager에 표시되지 않습니다.

- 7 **저장**을 클릭합니다.

LDAP 서버 추가

LDAP(Lightweight Directory Access Protocol) 서버 구성 및 기능은 ID 방화벽에만 사용할 수 있습니다. LDAP는 인증을 위한 중앙 위치를 제공합니다. 즉, LDAP 서버에 대한 연결을 구성할 때 사용자 레코드가 외부 LDAP 서버에 저장됩니다.

사전 요구 사항

도메인 계정에는 도메인 트리의 모든 개체에 대한 AD 읽기 권한이 있어야 합니다. 이벤트 로그 판독기 계정에는 보안 이벤트 로그에 대한 읽기 권한이 있어야 합니다.

NSX Manager의 클러스터가 있는 경우 모든 노드가 LDAP 서버에 연결할 수 있어야 합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > Active Directory**로 이동합니다.
- 3 **LDAP 서버** 탭을 선택합니다.
- 4 **LDAP 서버 추가**를 클릭합니다.
- 5 LDAP 서버의 **호스트** 이름을 입력합니다.
- 6 **연결 대상(디렉토리)** 드롭다운 메뉴에서 LDAP 서버가 연결된 Active Directory를 선택합니다.
- 7 (선택 사항) **프로토콜**: LDAP(보안 안 됨) 또는 LDAPS(보안)를 선택합니다.
- 8 LDAPS를 선택한 경우 NSX Manager에서 제안한 SHA-256 지문을 선택하거나 SHA-256 지문을 입력합니다.
- 9 LDAP 서버의 **포트** 번호를 입력합니다.
로컬 도메인 컨트롤러의 경우 기본 LDAP 포트 389 및 LDAP 포트 636은 Active Directory 동기화에 사용되며 기본값과 다르게 편집해서는 안 됩니다.
- 10 Active Directory 도메인에 대해 최소한 읽기 전용 액세스 권한이 있는 Active Directory 계정의 **사용자 이름** 및 **암호**를 입력합니다.
- 11 **저장**을 클릭합니다.
- 12 LDAP 서버에 연결할 수 있는지 확인하려면 **연결 테스트**를 클릭합니다.

Active Directory 동기화

Active Directory 개체는 사용자 ID 및 ID 기반 방화벽 규칙을 기반으로 보안 그룹을 생성하는 데 사용될 수 있습니다.

API를 사용하여 시작된 후 전체 동기화를 수동으로 종료하면 동기화 통계가 올바르게 업데이트되지 않습니다.

참고 IDFW는 게스트 운영 체제의 보안 및 무결성에 의존합니다. 악의적인 로컬 관리자가 방화벽 규칙을 우회하기 위해 해당 ID를 스푸핑할 수 있는 여러 방법이 있습니다. 사용자 ID 정보는 게스트 VM 내부의 Guest Introspection Agent에서 제공됩니다. 보안 관리자는 각 게스트 VM에 NSX Guest Introspection 에이전트가 설치 및 실행되고 있는지 확인해야 합니다. 로그인한 사용자에게 에이전트를 제거하거나 중지할 수 있는 권한이 없어야 합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > Active Directory**로 이동합니다.

- 3 동기화할 Active Directory 옆의 3개 버튼 메뉴를 클릭하고 다음 중 하나를 선택합니다.

메뉴 항목	설명
델타 동기화	마지막 동기화 이후에 변경된 로컬 AD 개체만 업데이트하는 델타 동기화를 수행합니다.
모두 동기화	모든 AD 개체의 로컬 상태를 업데이트하는 전체 동기화를 수행합니다.

- 4 동기화 상태 보기를 클릭하여 Active Directory의 현재 상태, 이전 동기화 상태, 동기화 상태 및 마지막 동기화 시간을 봅니다.

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 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.

사용자의 암호 관리

각 NSX Manager 및 NSX Edge 장치에는 admin, audit 및 root의 세 가지 로컬 계정이 있습니다. 이러한 사용자의 암호는 관리할 수 있지만, 사용자를 추가하거나 삭제할 수는 없습니다.

감사 사용자는 기본적으로 활성화 상태가 아닙니다. 이를 활성화하려면 관리자로 로그인하고 `set user audit` 명령을 실행한 후 새 암호를 입력합니다. 현재 암호를 묻는 메시지가 표시되면 Enter 키를 누릅니다.

기본적으로 사용자 암호는 90일 후에 만료됩니다. 각 사용자에게 대한 암호 만료를 변경하거나 사용하지 않도록 설정할 수 있습니다.

NSX Manager에 있는 로컬 사용자의 암호가 30일 이내에 만료되면 NSX Manager 웹 인터페이스에 암호 만료 알림이 표시됩니다. 로컬 사용자의 암호 만료를 30일 이하로 설정하면 알림이 항상 표시됩니다.

NSX-T Data Center 2.5.1부터는 알림에 "암호 변경" 링크가 포함됩니다. 이 링크를 클릭하여 웹 인터페이스에서 로컬 사용자의 암호를 변경합니다.

사전 요구 사항

NSX Manager 및 NSX Edge에 대한 암호 복잡성 요구 사항을 숙지하십시오. "NSX-T Data Center 설치 가이드"에서 "NSX Manager 설치" 및 "NSX Edge 설치"를 참조하십시오.

절차

- 1 장치의 CLI에 로그인합니다.

- 2 암호를 변경하려면 `set user` 명령을 실행합니다. 예:

```
nsx> set user admin
Current password:
New password:
Confirm new password:
nsx>
```

- 3 암호 만료 정보를 가져오려면 `get user <username> password-expiration` 명령을 실행합니다. 예:

```
nsx> get user admin password-expiration
Password expires 90 days after last change
nsx>
```

- 4 암호 만료 시간(일)을 설정하려면 `set user <username> password-expiration <number of days>` 명령을 실행합니다. 예:

```
nsx> set user admin password-expiration 120
nsx>
```

- 5 암호 만료를 사용하지 않도록 설정하려면 `clear user <username> password-expiration` 명령을 실행합니다. 예:

```
nsx> clear user admin password-expiration
nsx>
```

장치의 암호 재설정

다음 절차는 NSX Manager, NSX Edge 및 Cloud Service Manager 장치에 적용됩니다.

참고 NSX Manager 클러스터가 있는 경우 하나의 NSX Manager에서 root, admin 또는 audit 사용자의 암호를 재설정하면 클러스터에 있는 다른 NSX Manager에 대한 암호가 자동으로 재설정됩니다. 암호 동기화에 몇 분 정도가 소요될 수 있습니다.

사용자 admin 또는 audit의 이름을 변경한 경우 다음 절차에서 새 이름을 사용합니다.

장치를 재부팅하면 기본적으로 GRUB 부팅 메뉴가 표시되지 않습니다. 다음 절차를 수행하려면 GRUB 부팅 메뉴를 표시하도록 GRUB를 구성해야 합니다. GRUB 구성 및 GRUB root 암호 변경에 대한 자세한 내용은 "NSX-T Data Center 설치 가이드"에서 "부팅 시 GRUB 메뉴를 표시하도록 NSX-T Data Center 구성"을 참조하십시오.

NSX-T Data Center 2.5.2 이상을 실행하고 있으며 root에 대한 암호는 알고 있지만 admin 또는 audit에 대한 암호를 잊어버린 경우 다음 절차에 따라 재설정할 수 있습니다.

- 1 root 권한으로 장치에 로그인합니다.
- 2 NSX Edge의 경우 `/etc/init.d/nsx-edge-api-server stop` 명령을 실행합니다. NSX Edge가 아닌 경우 `/etc/init.d/nsx-mp-api-server stop` 명령을 실행합니다.

- 3 admin에 대한 암호를 재설정하려면 `passwd admin` 명령을 실행합니다.
- 4 audit에 대한 암호를 재설정하려면 `passwd audit` 명령을 실행합니다.
- 5 `touch /var/vmware/nsx/reset_cluster_credentials` 명령을 실행합니다.
- 6 NSX Edge의 경우 `/etc/init.d/nsx-edge-api-server start` 명령을 실행합니다. NSX Edge가 아닌 경우 `/etc/init.d/nsx-mp-api-server start` 명령을 실행합니다.

root 사용자 암호를 잊어버린 경우 다음 절차를 사용하여 재설정할 수 있습니다. NSX-T Data Center 2.5.0 또는 2.5.1을 실행하고 있으며 admin 및 audit의 암호를 재설정하려는 경우 다음 절차도 사용됩니다. NSX-T Data Center 2.5.2 이상을 실행하고 있는 경우 root에 대한 암호를 재설정 한 후에 위의 절차를 사용하여 admin 또는 audit에 대한 암호를 재설정할 수 있습니다.

절차

- 1 장치 콘솔에 연결합니다.
- 2 시스템을 재부팅합니다.
- 3 GRUB 부팅 메뉴가 나타나면 왼쪽 **Shift** 키 또는 **Esc** 키를 빠르게 누릅니다. 너무 늦게 눌러서 부팅 시퀀스가 일시 중지되지 않으면 시스템을 다시 재부팅해야 합니다.
- 4 **e**를 눌러 메뉴를 편집합니다.
사용자 이름(root)과 root에 대한 GRUB 암호(장치의 사용자 root와 같지 않음)를 입력합니다.
- 5 Ubuntu 선택 항목 위에 커서를 둡니다.
- 6 **e**를 눌러 선택한 옵션을 편집합니다.
- 7 linux로 시작하는 줄을 검색합니다.
- 8 NSX-T Data Center 2.5.0 또는 2.5.1을 실행하는 경우 다음 단계를 수행하십시오.
 - a `root=UUID=<ID number>` 다음에 나오는 모든 옵션을 제거하고 UUID 다음에 `rw single init=/bin/bash`를 추가합니다.
 - b **Ctrl-x**를 눌러 부팅합니다.
 - c 로그 메시지가 중지되면 **Enter** 키를 누릅니다.
`root@(none) :/#` 프롬프트가 표시됩니다.
 - d root에 대한 암호를 재설정하려면 `passwd` 명령을 실행합니다.
admin 또는 audit에 대한 암호를 재설정하려면 `passwd <admin or audit user ID>` 명령을 실행합니다.
`passwd` 명령을 여러 번 실행할 수 있습니다.
 - e 새 암호를 입력하고 확인을 위해 한 번 더 입력합니다.

- f NSX Manager에 대한 암호를 재설정하려면 `touch /var/vmware/nsx/reset_cluster_credentials` 명령을 실행합니다.
 - g `sync` 명령을 실행합니다.
 - h `reboot -f` 명령을 실행합니다.
- 9 NSX-T Data Center 2.5.2 이상을 실행하는 경우 다음 단계를 수행하십시오.
- a 줄 끝에 `systemd.wants=PasswordRecovery.service`를 추가합니다.
 - b **Ctrl-x**를 눌러 부팅합니다.
 - c `root`에 대한 새 암호를 입력하고 확인을 위해 다시 입력합니다.
- 부팅 프로세스가 완료되면 새 암호를 사용하여 `root`에 로그인하여 암호 변경을 확인할 수 있습니다.

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 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.

지문에는 OpenSSL 버전 1.x 이상을 사용해야 합니다. vIDM 호스트에서 `openssl` 명령은 이전 버전의 OpenSSL를 실행하므로 반드시 vIDM 호스트에서 `openssl1` 명령을 사용해야 합니다. 이 명령은 vIDM 호스트에서만 사용할 수 있습니다.

vIDM 호스트가 아닌 서버에서는 1.x 이후 버전의 OpenSSL을 실행하는 `openssl` 명령을 사용할 수 있습니다.

절차

- 1 vIDM 호스트의 콘솔에 로그인하거나 SSH로 vIDM 호스트에 `sshuser` 사용자로 로그인하고, 아니면 vIDM 호스트를 ping할 수 있는 서버에 로그인합니다.
- 2 다음 명령 중 하나를 실행하여 vIDM 호스트 지문을 가져옵니다.
 - vIDM 호스트에 로그인되어 있으면 `openssl1` 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
```

해당 명령을 실행하는 동안 오류가 발생하면 `sudo` 명령을 사용하여 `openssl1`를 실행해야 할 수 있습니다(즉, `sudo openssl ...`).

- vIDM 호스트를 ping할 수 있는 서버에 로그인되어 있다면 `openssl` 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
```

VMware Identity Manager 통합 구성

NSX-T Data Center를 ID 관리 서비스를 제공하는 vIDM(VMware Identity Manager)과 통합할 수 있습니다. vIDM 배포는 독립형 vIDM 호스트 또는 vIDM 클러스터일 수 있습니다.

vIDM 호스트 또는 모든 vIDM 클러스터 구성 요소에는 CA(인증 기관)에서 서명한 인증서가 있어야 합니다. 그렇지 않으면 NSX Manager에서 vIDM에 로그인하는 것이 Microsoft Edge나 Internet Explorer 11과 같은 특정 브라우저에서 작동하지 않을 수 있습니다. vIDM에 CA 서명 인증서를 설치하는 방법에 대한 정보는 <https://docs.vmware.com/kr/VMware-Identity-Manager/index.html>에서 VMware Identity Manager 설명서를 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.

NSX-T API 액세스가 필요한 경우 다음 구성 중 하나가 true여야 합니다.

- VIDM에 알려진 CA 서명 인증서가 있습니다.
- VIDM에 VIDM 서비스 측에 신뢰할 수 있는 커넥터 CA 인증서가 있습니다.
- VIDM에서 아웃바운드 커넥터 모드를 사용합니다.

참고 NSX Manager 및 VIDM은 동일한 표준 시간대에 있어야 합니다. 권장되는 방법은 UTC를 사용하는 것입니다.

가상 IP 또는 외부 로드 밸런서를 사용하지 않는 경우 PTR 레코드를 포함하도록 DNS 서버를 구성해야 합니다(즉, Manager가 노드의 물리적 IP 또는 FQDN을 사용하여 구성됨).

외부 로드 밸런서와 통합되도록 VIDM을 구성하는 경우 로드 밸런서에서 세션 지속성을 사용하도록 설정하여 페이지가 로드되지 않거나 사용자가 예기치 않게 로그아웃되는 것과 같은 문제를 방지해야 합니다.

VIDM 배포가 VIDM 클러스터인 경우에는 VIDM 로드 밸런서를 SSL 종료 및 다시 암호화로 구성해야 합니다.

VIDM을 사용하도록 설정한 상태에서 해당 URL(<https://<nsx-manager-ip-address>/login.jsp?local=true>)을 사용할 경우 로컬 사용자 계정을 사용하여 NSX Manager에 계속 로그인할 수 있습니다.

UPN(UserPrincipalName)을 사용하여 VIDM에 로그인하는 경우 NSX-T에 대한 인증이 실패할 수 있습니다. 이 문제를 방지하려면 다른 유형의 자격 증명(예: SAMAccountName)을 사용합니다.

NSX Cloud를 사용하는 경우 해당 URL(<https://<csm-ip-address>/login.jsp?local=true>)을 사용하여 CSM에 별도로 로그인할 수 있습니다.

사전 요구 사항

- VIDM 배포 유형(독립형 VIDM 호스트 또는 VIDM 클러스터)에 따라 VIDM 호스트 또는 VIDM 로드 밸런서의 인증서 지문이 있는지 확인합니다. 지문을 가져오는 명령은 두 경우 모두에서 동일합니다. [VIDM 호스트에서 인증서 지문 가져오기](#)의 내용을 참조하십시오.
- NSX Manager가 VIDM에 대한 OAuth 클라이언트로 등록되어 있는지 확인합니다. 등록 프로세스 중에 클라이언트 ID와 클라이언트 암호를 적어두십시오. 자세한 정보는 <https://docs.vmware.com/kr/VMware-Workspace-ONE-Access/3.3/idm-administrator/GUID-AD4B6F91-2D68-48F2-9212-5B69D40A1FAE.html>에서 VMware Identity Manager 설명서를 참조하십시오. 클라이언트를 생성할 때는 다음 작업만 수행하면 됩니다.
 - 액세스 유형을 서비스 클라이언트 토큰으로 설정합니다.
 - 클라이언트 ID를 지정합니다.
 - 고급 필드를 확장하고 공유 암호 생성을 클릭합니다.
 - 추가를 클릭합니다.

NSX Cloud 참고 NSX Cloud를 사용하는 경우 CSM이 VIDM에 OAuth 클라이언트로 등록되어 있는지 확인합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(https://<nsx-manager-ip-address>)에 로그인합니다.
- 2 **시스템 > 사용자**를 선택합니다.
- 3 **구성** 탭을 클릭합니다.
- 4 **편집**을 클릭합니다.
- 5 외부 로드 밸런서 통합을 사용하도록 설정하려면 **외부 로드 밸런서 통합** 토글을 클릭합니다.

참고 VIP(가상 IP)가 설정된 경우(**시스템 > 장치 > 가상 IP**) 외부 로드 밸런서 통합을 사용할 수 없습니다. 이는 vIDM을 구성하는 동안 VIP 또는 외부 로드 밸런서 중 하나만 사용할 수 있기 때문입니다. 외부 로드 밸런서를 사용하려면 VIP를 사용하지 않도록 설정합니다. 자세한 내용은 "NSX-T Data Center 설치 가이드"에서 클러스터에 대한 VIP(가상 IP) 주소 구성을 참조하십시오.

- 6 VMware Identity Manager 통합을 사용하도록 설정하려면 **VMware Identity Manager 통합** 전환을 클릭합니다.
- 7 다음 정보를 제공합니다.

매개 변수	설명
VMware Identity Manager 장치	vIDM 배포 유형(독립형 vIDM 호스트 또는 vIDM 클러스터)에 따라 vIDM 호스트 또는 vIDM 로드 밸런서의 FQDN(정규화된 도메인 이름)
OAuth 클라이언트 ID	NSX Manager를 vIDM에 등록할 때 생성되는 ID입니다.
OAuth 클라이언트 암호	NSX Manager를 vIDM에 등록할 때 생성되는 암호입니다.
SSL 지문	vIDM 호스트의 인증서 지문입니다.
NSX 장치	NSX Manager의 IP 주소 또는 FQDN(정규화된 도메인 이름)입니다. NSX Manager 클러스터를 사용하는 경우 로드 밸런서 FQDN이나 클러스터 VIP FQDN 또는 IP 주소를 사용합니다. 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.

- 8 **저장**을 클릭합니다.
- 9 NSX Cloud를 사용하는 경우 NSX Manager 대신 CSM에 로그인하여 CSM 장치에서 1 ~ 8단계를 반복합니다.

VMware Identity Manager 기능 검증

VMware Identity Manager를 구성한 후 기능을 검증하십시오. VMware Identity Manager가 올바르게 구성되고 검증되지 않으면 일부 사용자에게 로그인하려고 할 때 인증되지 않음(오류 코드 98) 메시지가 표시될 수 있습니다.

VMware Identity Manager가 올바르게 구성되고 검증되지 않으면 일부 사용자에게 로그인하려고 할 때 인증되지 않음(오류 코드 98) 메시지가 표시될 수 있습니다.

절차

- 1 사용자 이름 및 암호의 base64 인코딩을 생성합니다.

다음 명령을 실행하여 인코딩을 가져오고 후행 '\n' 문자를 제거합니다. 예:

```
echo -n 'sfadmin@ad.node.com:password1234!' | base64 | tr -d '\n'
c2ZhZG1pbkZhZC5ub2RlLmNvbTpwYXNzd29yZDEyMzQhCg==
```

- 2 각 사용자가 각 노드에 대해 API 호출을 수행할 수 있는지 확인합니다.

원격 인증 curl 명령을 사용하십시오. curl -k -H 'Authorization: Remote <base64 encoding string>' https://<node FQDN>/api/v1/node/aaa/auth-policy. 예:

```
curl -k -H 'Authorization: Remote c2ZhZG1pbkZhZC5ub2RlLmNvbTpwYXNzd29yZDEyMzQhCg==' /
https://tmgr1.cptroot.com/api/v1/node/aaa/auth-policy
```

그러면 다음과 같은 권한 부여 정책 설정이 반환됩니다.

```
{
  "_schema": "AuthenticationPolicyProperties",
  "_self": {
    "href": "/node/aaa/auth-policy",
    "rel": "self"
  },
  "api_failed_auth_lockout_period": 900,
  "api_failed_auth_reset_period": 900,
  "api_max_auth_failures": 5,
  "cli_failed_auth_lockout_period": 900,
  "cli_max_auth_failures": 5,
  "minimum_password_length": 12
}
```

이 명령이 오류를 반환하지 않으면 VMware Identity Manager가 올바르게 작동하는 것입니다. 추가 단계는 필요하지 않습니다. curl 명령이 오류를 반환하면 사용자가 잠길 수 있습니다.

참고 계정 잠금 정책은 노드별로 설정되고 적용됩니다. 클러스터의 한 노드가 사용자를 잠근 경우 다른 노드는 그렇지 않을 수 있습니다.

- 3 노드의 사용자 잠금을 재설정하려면:

- a 로컬 NSX Manager admin를 사용하여 권한 부여 정책을 검색합니다.

```
curl -k -u 'admin:<password>' https://nsxmgr/api/v1/node/aaa/auth-policy
```

- b 출력을 현재 작업 디렉토리에 있는 JSON 파일에 저장합니다.

- c 파일을 수정하여 잠금 기간 설정을 변경합니다.

예를 들어, 대부분의 기본 설정은 잠금 및 재설정 기간(900초)을 적용합니다. 다음과 같이 이러한 값을 변경하여 즉시 재설정을 사용하도록 설정합니다.

```
{
  "_schema": "AuthenticationPolicyProperties",
  "_self": {
    "href": "/node/aaa/auth-policy",
    "rel": "self"
  },
  "api_failed_auth_lockout_period": 1,
  "api_failed_auth_reset_period": 1,
  "api_max_auth_failures": 5,
  "cli_failed_auth_lockout_period": 1,
  "cli_max_auth_failures": 5,
  "minimum_password_length": 12
}
```

- d 영향을 받는 노드에 변경 사항을 적용합니다.

```
curl -k -u 'admin:<password>' -H 'Content-Type: application/json' -d \
@<modified_policy_setting.json> https://nsxmgr/api/v1/node/aaa/auth-policy
```

- e (선택 사항) 권한 부여 정책 설정 파일을 이전 설정으로 되돌립니다.

이로 인해 잠금 문제가 해결될 수 있습니다. 여전히 원격 인증 API 호출을 수행할 수 있지만 브라우저를 통해 로그인할 수 없는 경우, 브라우저에 잘못된 캐시 또는 쿠키가 저장되어 있을 수 있습니다. 캐시 및 쿠키를 지우고 다시 시도하십시오.

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>

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 time.nist.gov
server pool.ntp.org
server time.is dynamic
restrict 192.168.100.0 netmask 255.255.255.0 nomodify notrap
```

- 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
- 로드 밸런서 관리자
- 로드 밸런서 감사자
- VPN 관리자
- Guest Introspection 관리자
- 네트워크 검사 관리자

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 21-5. 역할 및 사용 권한 및 표 21-6. 고급 네트워킹 및 보안을 위한 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
- LB Adm - 로드 밸런서 관리자
- LB Aud - 로드 밸런서 감사자
- VPN Adm - VPN 관리자
- GI Adm - Guest Introspection 관리자

- NI Adm - 네트워크 검사 관리자
- FA - 전체 액세스 권한
- E - 실행
- R - 읽기

표 21-5. 역할 및 사용 권한

작업	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Au d	VPN Adm	GI Adm	NI Adm
네트워킹 > Tier-0 게이트웨이	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
네트워킹 > 네트워크 인터페이스	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
네트워킹 > 네트워크 정적 경로	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
네트워킹 > 로케일 서비스	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
네트워킹 > 정적 ARP 구성	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
네트워킹 > 세그먼트	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
네트워킹 > 세그먼트 > 세그먼트 프로파일	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
네트워킹 > IP 주소 풀	FA	R	FA	FA	R	R	FA	R	R	R	없음	없음	없음
네트워킹 전달 정책	FA	R	FA	R	FA	R	FA	R	없음	없음	없음	없음	없음
네트워킹 > DNS	FA	R	FA	FA	R	R	FA	R	R	R	없음	없음	없음

표 21-5. 역할 및 사용 권한 (계속)

작업	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
네트워킹 > 로드 밸런싱	FA	R	없음	없음	R	없음	FA	R	FA	R	없음	없음	없음
네트워킹 > NAT	FA	R	FA	R	FA	R	FA	R	R	R	없음	없음	없음
네트워킹 > VPN	FA	R	FA	R	FA	R	FA	R	없음	없음	FA	없음	없음
네트워킹 > IPv6 프로파일													
보안 > 분산 방화벽	FA	R	R	R	FA	R	FA	R	R	R	R	R	R
보안 > 게이트웨이 방화벽	FA	R	R	R	FA	R	FA	R	없음	없음	없음	없음	FA
보안 > 네트워크 자체 검사	FA	R	R	R	R	R	FA	R	없음	없음	없음	없음	FA
보안 > 끝점 보호 규칙	FA	R	R	R	R	R	FA	R	없음	없음	없음	FA	없음
인벤토리 > 컨텍스트 프로파일	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
인벤토리 > 가상 시스템	R	R	R	R	R	R	R	R	R	R	R	R	R
계획 및 문제 해결 > 포트 미러링	FA	R	FA	R	R	R	FA	R	없음	없음	없음	없음	없음
계획 및 문제 해결 > 포트 미러링 바인딩	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R

표 21-5. 역할 및 사용 권한 (계속)

작업	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
계획 및 문제 해결 > 프로파일 바인딩 모니터링	FA	R	FA	FA	R	R	FA	R	R	R	R	R	R
계획 및 문제 해결 > 방화벽 IPFIX 프로파일	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
계획 및 문제 해결 > 스위치 IPFIX 프로파일	FA	R	FA	R	R	R	FA	R	R	R	R	R	R
시스템 > 패브릭 > 노드 > 호스트	FA	R	R	R	R	R	R	R	없음	없음	없음	없음	없음
시스템 > 패브릭 > 노드 > 노드	FA	R	FA	R	FA	R	R	R	R	R	없음	없음	없음
시스템 > 패브릭 > 노드 > Edge	FA	R	FA	R	R	R	R	R	없음	없음	없음	없음	없음
시스템 > 패브릭 > 노드 > Edge 클러스터	FA	R	FA	R	R	R	R	R	없음	없음	없음	없음	없음
시스템 > 패브릭 > 노드 > 브리지	FA	R	FA	R	R	R	없음	없음	R	R	없음	없음	없음
시스템 > 패브릭 > 노드 > 전송 노드	FA	R	R	R	R	R	R	R	R	R	없음	없음	없음

표 21-5. 역할 및 사용 권한 (계속)

작업	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
시스템 > 패브릭 > 노드 > 터널	R	R	R	R	R	R	R	R	R	R	없음	없음	없음
시스템 > 패브릭 > 프로파일 > 업링크 프로파일	FA	R	R	R	R	R	R	R	R	R	없음	없음	없음
시스템 > 패브릭 > 프로파일 > Edge 클러스터 프로파일	FA	R	FA	R	R	R	R	R	R	R	없음	없음	없음
시스템 > 패브릭 > 프로파일 > 구성	FA	R	없음	없음	없음	없음	R	R	없음	없음	없음	없음	없음
시스템 > 패브릭 > 전송 영역 > 전송 영역	FA	R	R	R	R	R	R	R	R	R	없음	없음	없음
시스템 > 패브릭 > 전송 영역 > 전송 영역 프로파일	FA	R	R	R	R	R	R	R	없음	없음	없음	없음	없음
시스템 > 패브릭 > 계산 관리자	FA	R	R	R	R	R	R	R	없음	없음	없음	R	R
시스템 > 인증서	FA	R	없음	없음	FA	R	없음	없음	FA	R	FA	없음	없음
시스템 > 서비스 배포 > 서비스 인스턴스	FA	R	R	R	FA	R	FA	R	없음	없음	없음	FA	FA

표 21-5. 역할 및 사용 권한 (계속)

작업	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
시스템 > 유틸리티 > 지원 번들	FA	R	없음	없음	없음	없음	없음	없음	없음	없음	없음	없음	없음
시스템 > 유틸리티 > 백업	FA	R	없음	없음	없음	없음	없음	없음	없음	없음	없음	없음	없음
시스템 > 유틸리티 > 복원	FA	R	없음	없음	없음	없음	없음	없음	없음	없음	없음	없음	없음
시스템 > 유틸리티 > 업그레이드	FA	R	R	R	R	R	없음	없음	없음	없음	없음	없음	없음
시스템 > 사용자 > 역할 할당	FA	R	없음	없음	없음	없음	없음	없음	없음	없음	없음	없음	없음
시스템 > Active Directory	FA	R	FA	R	FA	FA	R	R	R	R	R	R	R
시스템 > 사용자 > 구성	FA	R	없음	없음	없음	없음	없음	없음	없음	없음	없음	없음	없음
시스템 > 라이선스	FA	R	R	R	R	R	없음	없음	없음	없음	없음	없음	없음
시스템 > 시스템 관리	FA	R	R	R	R	R	R	R	없음	없음	없음	없음	없음
사용자 지정 대시보드 구성	FA	R	R	R	R	R	FA	R	R	R	R	R	R
시스템 > 수명 주기 관리 > 마이그레이션	FA	없음	없음	없음	없음	없음	없음	없음	없음	없음	없음	없음	없음

표 21-6. 고급 네트워킹 및 보안을 위한 역할 및 사용 권한

작업	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
도구 > 포트 연결	E	R	E	E	E	E	E	R	E	E	없음	없음	없음
도구 > 흐름 추적	E	R	E	E	E	E	E	R	E	E	없음	없음	없음
도구 > 포트 미러링	FA	R	FA	R	R	R	FA	R	없음	없음	없음	없음	없음
도구 > IPFIX	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
방화벽 > 분산 방화벽 > 일반	FA	R	R	R	FA	R	FA	R	없음	없음	없음	없음	R
방화벽 > 분산 방화벽 > 구성	FA	R	R	R	FA	R	FA	R	없음	없음	없음	없음	없음
방화벽 > Edge 방화벽	FA	R	R	R	FA	R	FA	R	없음	없음	없음	없음	FA
라우팅 > 라우터	FA	R	FA	FA	R	R	FA	R	R	R	R	없음	R
라우팅 > NAT	FA	R	FA	R	FA	R	FA	R	R	R	없음	없음	없음
DHCP > 서버 프로파일	FA	R	FA	R	없음	없음	FA	R	없음	없음	없음	없음	없음
DHCP > 서버	FA	R	FA	R	없음	없음	FA	R	없음	없음	없음	없음	없음
DHCP > 릴레이 프로파일	FA	R	FA	R	없음	없음	FA	R	없음	없음	없음	없음	없음
DHCP > 릴레이 서비스	FA	R	FA	R	없음	없음	FA	R	없음	없음	없음	없음	없음
DHCP > 메타데이터 프로세스	FA	R	FA	R	없음	없음	없음	없음	없음	없음	없음	없음	없음
IPAM	FA	R	FA	FA	R	R	없음	없음	R	R	없음	없음	없음

표 21-6. 고급 네트워킹 및 보안을 위한 역할 및 사용 권한 (계속)

작업	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud	VPN Adm	GI Adm	NI Adm
스위칭 > 스위치	FA	R	FA	FA	R	R	FA	R	R	R	R	없음	R
스위칭 > 포트	FA	R	FA	FA	R	R	FA	R	R	R	R	없음	R
스위칭 > 스위칭 프로파일	FA	R	FA	FA	R	R	FA	R	R	R	없음	없음	없음
네트워킹 > 로드 밸런서	FA	R	없음	없음	R	없음	FA	R	FA	R	없음	없음	없음
로드 밸런싱 > 프로파일 > SSL 프로파일	FA	R	없음	없음	FA	R	FA	R	FA	R	없음	없음	없음
인벤토리 > 그룹	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
인벤토리 > IP 집합	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
인벤토리 > IP 풀	FA	R	FA	R	없음	없음	없음	없음	R	R	R	R	R
인벤토리 > MAC 집합	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
인벤토리 > 서비스	FA	R	FA	R	FA	R	FA	R	R	R	R	R	R
인벤토리 > 가상 시스템	R	R	R	R	R	R	R	R	R	R	R	R	R
인벤토리 > 가상 시스템 > 태그 구성	FA	없음	없음	없음	없음	없음	없음	없음	없음	없음	없음	없음	없음

역할 할당 또는 주체 ID 추가

VMware Identity Manager가 NSX-T Data Center와 통합된 경우 역할을 사용자 또는 사용자 그룹에 할당할 수 있습니다. 역할을 주체 ID에 할당할 수도 있습니다.

주체는 NSX-T Data Center 구성 요소 또는 OpenStack 제품과 같은 타사 애플리케이션입니다. 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 - 주체 ID에 할당된 모든 영숫자 값일 수 있습니다.
- 인증서
- 주체의 액세스 권한을 나타내는 RBAC 역할

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.

주체 ID 사용자의 인증서가 만료되면 새 인증서를 가져온 후 API를 호출하여 주체 ID 사용자의 인증서를 업데이트해야 합니다(아래 절차 참조). NSX-T Data Center API에 대한 자세한 내용은 <https://docs.vmware.com/kr/VMware-NSX-T-Data-Center>에서 사용할 수 있는 API 리소스에 대한 링크를 참조하십시오.

주체 ID 사용자의 인증서는 다음 요구 사항을 충족해야 합니다.

- SHA256을 기준으로 합니다.
- 2048비트 또는 키 크기보다 큰 RSA/DSA 메시지 알고리즘입니다.
- 루트 인증서일 수 없습니다.

API를 사용하여 주체 ID를 삭제할 수 있습니다. 그러나 주체 ID를 삭제해도 해당 인증서가 자동으로 삭제되지는 않습니다. 인증서를 수동으로 삭제해야 합니다.

주체 ID 및 해당 인증서를 삭제하는 단계:

- 1 삭제할 주체 ID의 세부 정보를 가져오고 응답에 `certificate_id` 값을 기록합니다.

```
GET /api/v1/trust-management/principal-identities/<principal-identity-id>
```

- 2 주체 ID를 삭제합니다.

```
DELETE /api/v1/trust-management/principal-identities/<principal-identity-id>
```

- 3 1단계에서 가져온 `certificate_id` 값을 사용하여 인증서를 삭제합니다.

```
DELETE /api/v1/trust-management/certificates/<certificate_id>
```

사전 요구 사항

- 역할을 사용자에게 할당하려는 경우 vIDM 호스트가 NSX-T와 연결되어 있는지 확인합니다. 자세한 내용은 [VMware Identity Manager 통합 구성의 내용을 참조하십시오.](#)

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 사용자**를 선택합니다.
- 3 역할을 사용자에게 할당하려면 **추가 > 역할 할당**을 선택합니다.
 - a 사용자 또는 사용자 그룹을 선택합니다.
 - b 역할을 선택합니다.
 - c **저장**을 클릭합니다.
- 4 주체 ID를 추가하려면 **추가 > 역할을 가진 주체 ID**를 선택합니다.
 - a 주체 ID의 이름을 입력합니다.
 - b 역할을 선택합니다.
 - c 노드 ID를 입력합니다.
 - d 인증서를 PEM 형식으로 입력합니다.
 - e **저장**을 클릭합니다.
- 5 (선택 사항) NSX Cloud를 사용하는 경우 NSX Manager 대신 CSM 장치에 로그인하고 1~4단계를 반복합니다.
- 6 주체 ID에 대한 인증서가 완료되면 다음 단계를 수행합니다.
 - a 새 인증서를 가져오고 인증서 ID를 기록해 둡니다. **인증서 가져오기**의 내용을 참조하십시오.
 - b 다음 API를 호출하여 주체 ID의 ID를 가져옵니다.


```
GET https://<nsx-mgr>/api/v1/trust-management/principal-identities
```
 - c 다음 API를 호출하여 주체 ID의 인증서를 업데이트합니다. 가져온 인증서의 ID와 주체 ID의 사용자 ID를 제공해야 합니다.

예를 들면 다음과 같습니다.

```
POST https://<nsx-mgr>/api/v1/trust-management/principal-identities?
action=update_certificate
{
  "principal_identity_id": "ebd3032d-728e-44d4-9914-d4f81c9972cb",
  "certificate_id" : "abd3032d-728e-44d4-9914-d4f81c9972cc"
}
```

NSX Manager 백업 및 복원

NSX Manager 클러스터가 작동 불가능 상태가 되거나 환경을 이전 상태로 복원하려는 경우 백업에서 복원할 수 있습니다. NSX Manager를 작동할 수 없는 동안 데이터부는 영향을 받지 않지만 구성을 변경할 수는 없습니다.

백업에는 다음과 같은 두 가지 유형이 있습니다.

클러스터 백업

이 백업에는 가상 네트워크의 원하는 상태가 포함됩니다.

노드 백업

NSX Manager 노드의 백업입니다.

백업 방법으로는 다음 두 가지가 있습니다.

수동

언제든지 수동으로 백업을 실행할 수 있습니다.

자동

자동 백업은 설정된 스케줄에 따라 실행됩니다. 백업을 최신 상태로 유지하려면 자동 백업이 매우 권장됩니다.

NSX-T Data Center 구성을 백업에 캡처된 상태로 다시 복원할 수 있습니다. 백업을 복원할 때는 백업된 장치와 동일한 NSX Manager 버전이 실행되는 새 NSX Manager 장치로 복원해야 합니다.

백업 구성

백업을 수행하려면 백업 파일 서버를 구성해야 합니다. 백업 파일 서버가 구성된 후 언제든지 백업을 시작하거나 자동 백업에 대한 스케줄을 구성할 수 있습니다.

사전 요구 사항

백업 파일 서버의 SSH 지문이 있는지 확인합니다. SHA256 해시 ECDSA(256비트) 키만 지문으로 허용됩니다. 원격 서버의 SSH 지문 찾기의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 백업 및 복원**을 선택합니다.
- 3 백업을 구성하려면 페이지 상단 오른쪽에서 **편집**을 클릭합니다.
- 4 백업 파일 서버의 IP 주소 또는 호스트 이름을 입력합니다.
- 5 필요한 경우 기본 포트를 변경합니다.
- 6 프로토콜 필드는 이미 채워져 있습니다. 이 값을 변경하지 마십시오.
SFTP가 지원되는 유일한 프로토콜입니다.
- 7 백업 파일 서버에 로그인하는 데 필요한 사용자 이름 및 암호를 입력합니다.

처음 파일 서버를 구성할 때 암호를 제공해야 합니다. 이후에는 파일 서버를 재구성하고 서버 IP(또는 호스트 이름), 포트 및 사용자 이름이 동일한 경우 암호를 다시 입력하지 않아도 됩니다.

8 대상 디렉토리 필드에서 백업이 저장될 절대 디렉토리 경로를 입력합니다.

디렉토리는 이미 존재해야 하며 /일 수 없습니다. 여러 NSX-T Data Center 배포가 있는 경우 각 배포에 대해 서로 다른 디렉토리를 사용해야 합니다. 백업 파일 서버가 Windows 시스템인 경우 대상 디렉토리를 지정할 때 슬래시를 계속 사용합니다. 예를 들어, Windows 시스템의 백업 디렉토리가 `c:\SFTP_Root\backup`인 경우 대상 디렉토리로 `/SFTP_Root/backup`을 지정합니다.

참고 백업 프로세스는 매우 길어질 수 있는 백업 파일의 이름을 생성합니다. Windows Server에서 백업 파일의 전체 경로 이름의 길이가 Windows에서 설정된 제한을 초과하여 백업이 실패할 수 있습니다. 이 문제를 방지하려면 KB 문서 <https://kb.vmware.com/s/article/76528> 내용을 참조하십시오.

9 백업을 암호화하려면 **암호화 암호 변경** 토글을 클릭하고 암호화 암호를 입력합니다.

백업을 복원하려면 이 암호가 필요합니다. 암호를 잊어버리면 백업을 복원할 수 없습니다.

10 백업을 저장하는 서버의 SSH 지문을 입력합니다.

이 항목을 비워 두고 서버가 제공한 지문을 수락하거나 거절할 수 있습니다.

11 스케줄 탭을 클릭합니다.**12** 자동 백업을 사용하도록 설정하려면 **자동 백업** 토글을 클릭합니다.**13** **매주**를 클릭하고 백업의 요일 및 시간을 설정하거나 **간격**을 클릭하고 백업 사이의 간격을 설정합니다.**14 NSX 구성 변경 내용 감지**를 사용하도록 설정하면 런타임 또는 구성되지 않은 관련 변경 내용이나 사용자 구성의 변경 내용을 감지할 때 예약되지 않은 전체 구성 백업이 트리거 될 것입니다.

구성 변경으로 트리거되는 백업 간의 간격을 설정할 수 있습니다. 기본값은 5분입니다.

참고 이 옵션을 선택하면 많은 수의 백업이 생성될 수 있습니다. 사용할 때는 주의하십시오.

15 저장을 클릭합니다.**결과**

백업 파일 서버를 구성한 후 **지금 백업**을 클릭하여 언제든지 백업을 시작할 수 있습니다.

이전 백업 제거

백업은 백업 파일 서버에서 누적되어 많은 양의 스토리지를 사용할 수 있습니다. NSX-T Data Center와 함께 제공되는 스크립트를 실행하여 이전 백업을 자동으로 삭제할 수 있습니다.

NSX Manager의 디렉토리 `/var/vmware/nsx/file-store`에서 Python script

`nsx_backup_cleaner.py`를 찾을 수 있습니다. 이 파일에 액세스하려면 루트로 로그인해야 합니다. 일반적으로 백업 파일 서버에서 작업을 스케줄링하여 이전 백업을 지우도록 이 스크립트를 정기적으로 실행합니다. 다음 사용량 정보에서는 스크립트를 실행하는 방법에 대해 설명합니다.

```
nsx_backup_cleaner.py -d backup_dir [-k 1] [-l 5] [-h]
Or
nsx_backup_cleaner.py --dir backup_dir [--retention-period 1] [--min-count 5] [--help]
```

Required parameters:

```
-d/--dir: Backup root directory
-k/--retention-period: Number of days need to retain a backup file
```

Optional parameters:

```
-l/--min-count: Minimum number of backup files to be kept, default value is 100
-h/--help: Display help message
```

백업의 사용 기간은 백업의 타임 스탬프와 스크립트가 실행되는 시간 사이의 차이점으로 계산됩니다. 이 값이 보존 기간보다 큰 경우 디스크에 최소 백업 수보다 더 많은 백업이 있으면 해당 백업이 삭제됩니다.

Linux 또는 Windows Server에서 정기적으로 실행할 스크립트 설정에 대한 자세한 내용은 스크립트 시작 부분의 주석을 참조하십시오.

사용 가능한 백업 나열

백업 파일 서버는 모든 NSX Manager의 백업을 저장합니다. 복원하려는 백업을 찾을 수 있도록 백업 목록을 가져오려면, `get_backup_timestamps.sh` 스크립트를 실행해야 합니다.

이 스크립트는 NSX Manager에 있습니다. 전체 경로 이름은 `/var/vmware/nsx/file-store/get_backup_timestamps.sh`입니다. 이 스크립트는 모든 Linux 시스템이나 NSX-T Data Center 장치에서 실행할 수 있습니다. 모든 NSX Manager에 액세스할 수 없어도 이 스크립트를 실행할 수 있도록 NSX Manager가 아닌 시스템에 NSX-T Data Center를 설치한 후에 이 스크립트를 복사하는 것이 가장 좋습니다. 백업을 복원해야 하지만 이 스크립트에 액세스할 수 없으면 새 NSX Manager를 설치하고 스크립트를 실행하면 됩니다.

관리자 권한으로 NSX Manager에 로그인하고 CLI 명령을 실행하여 스크립트를 다른 시스템 또는 백업 파일 서버에 복사할 수 있습니다. 예:

```
nsxmgr-1> copy file get_backup_timestamps.sh url scp://admin@10.127.1.20/tmp/
admin@10.127.1.20's password:
nsxmgr-1>
```

이 스크립트는 대화형이며 백업 파일 서버를 구성할 때 지정한 정보를 묻는 메시지가 표시됩니다. 표시할 백업 수를 지정할 수 있습니다. 각 백업은 타임 스탬프, NSX Manager 노드의 IP 주소 또는 FQDN(NSX Manager 노드가 FQDN을 게시하도록 설정된 경우) 및 노드 ID와 함께 나열됩니다. 예를 들면 다음과 같습니다.

```
admin@host1:/home/admin# ./get_backup_timestamps.sh
Enter file server ip:
10.108.115.108
Enter port:
22
Enter directory path:
/home/nsx/backups
Enter number of latest backup or press Enter to list all backups:

root@10.108.115.108's password:
Latest backups:
[Backup timestamp; IP address/FQDN; Node id]
2019-01-22;09:00:33 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
```

```
2019-01-22;09:01:52 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
2019-01-22;09:13:30 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:14:42 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:16:43 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
```

백업 복원

백업을 복원하면 백업 시 네트워크 상태가 복원됩니다. 또한, NSX Manager에서 유지 보수되는 구성도 복원되고, 백업이 실행된 이후에 패브릭에 대해 시행된 노드 추가 또는 삭제와 같은 모든 변경 사항이 조정됩니다.

백업을 새 NSX Manager 장치로 복원해야 합니다.

백업이 실행되었을 때 NSX Manager 클러스터가 있었다면 NSX Manager 클러스터로도 복원해야 합니다. 복원 프로세스는 먼저 하나의 NSX Manager 노드를 복원한 다음, 나머지 NSX Manager 노드를 추가 하라는 메시지를 표시합니다.

중요 NSX Manager 클러스터의 노드를 계속 사용할 수 있는 경우 복원을 시작하기 전에 전원을 꺼야 합니다.

사전 요구 사항

- 백업 파일 서버의 로그인 자격 증명이 있는지 확인합니다.
- 백업 파일 서버의 SSH 지문이 있는지 확인합니다. SHA256 해시 ECDSA(256비트) 키만 지문으로 허용됩니다. 원격 서버의 SSH 지문 찾기 항목을 참조하십시오.
- 백업 파일의 암호가 있는지 확인합니다.
- 사용 가능한 백업 나열의 절차에 따라 복원하려는 백업을 식별합니다. 백업을 수행한 NSX Manager 노드의 IP 또는 FQDN을 기록해 둡니다.
- FQDN을 게시하도록 NSX Manager 노드를 구성하는 경우 DNS 서버의 NSX Manager 노드에 대한 정방향 및 역방향 조회 항목을 구성해야 합니다.

절차

- 1 복원할 NSX Manager 클러스터의 모든 노드 전원을 끕니다.
- 2 백업을 복원할 새 NSX Manager 노드를 하나 설치합니다.
 - 복원하려는 백업의 백업 목록에 IP 주소가 포함되어 있으면 동일한 IP 주소를 사용하여 새 NSX Manager 노드를 배포해야 합니다. 해당 FQDN을 게시하도록 NSX Manager 노드를 구성하지 마십시오.

```
2019-01-22;09:01:52 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
```

- 복원하려는 백업의 백업 목록에 FQDN이 포함된 경우 이 FQDN을 사용하여 새 NSX Manager 노드를 구성해야 합니다(자세한 내용은 "NSX-T Data Center 설치 가이드"의 "NSX Manager 설치" 항목에서 "NSX Manager의 FQDN 게시" 섹션을 참조). 또한 새 NSX Manager 노드의 IP 주소가 원래 주소와 다른 경우에는 새 IP 주소를 사용하여 NSX Manager 노드에 대한 DNS 서버의 정방향 및 역방향 조회 항목을 업데이트해야 합니다.

```
2019-01-22;09:16:43 nsxmgr.example.com 41893642-597b-915f-5117-7da576df4ff2
```

새 NSX Manager 노드가 실행 중이고 온라인 상태가 되면 복원을 계속할 수 있습니다.

- 3 브라우저에서 관리자 권한으로 새 NSX Manager에 로그인합니다.
- 4 **시스템 > 백업 및 복원**을 선택합니다.
- 5 **복원** 탭을 클릭합니다.
- 6 백업 파일 서버를 구성하려면 **편집**을 클릭합니다.
- 7 IP 주소 또는 호스트 이름을 입력합니다.
- 8 필요한 경우 포트 번호를 변경합니다.
기본값은 22입니다.
- 9 서버에 로그인하려면 사용자 이름과 암호를 입력합니다.
- 10 **대상 디렉토리** 텍스트 상자에서 백업이 저장될 절대 디렉토리 경로를 입력합니다.
- 11 백업 데이터를 암호화하는 데 사용된 암호를 입력합니다.
- 12 백업을 저장하는 서버의 SSH 지문을 입력합니다.
- 13 **저장**을 클릭합니다.
- 14 백업을 선택합니다.
- 15 **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.

백업에 NSX Manager 클러스터에 대한 정보가 있는 경우 NSX Manager 노드를 추가하라는 메시지가 표시됩니다. NSX Manager 노드를 추가하지 않기로 결정한 경우에도 복원을 계속할 수 있습니다.

복원 작업이 완료되면 **복원 완료** 화면에 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.

로그 파일을 확인하여 클러스터 복원 또는 노드 복원 실패가 발생했는지 여부를 파악할 수도 있습니다. `get log-file syslog`를 실행하여 시스템 로그 파일을 확인하고 클러스터 복원 실패 및 노드 복원 실패를 검색합니다.

관리자를 다시 시작하려면 `restart service manager` 명령을 실행합니다.

관리자를 재부팅하려면 `reboot` 명령을 실행합니다.

- 16** 노드가 하나만 배포된 경우 복원된 NSX Manager 노드가 실행되게 되면 추가 노드를 배포하여 NSX Manager 클러스터를 구성할 수 있습니다.

지침은 "NSX-T Data Center 설치 가이드"를 참조하십시오.

- 17** 새 NSX Manager 클러스터가 배포된 후 1단계에서 전원을 껐던 원래 NSX Manager 클러스터 VM을 삭제합니다.

또한 클러스터의 두 번째 및 세 번째 노드에서 인증서를 교체해야 합니다.

결과

백업 후 계산 관리자를 추가한 경우 복원 후 계산 관리자를 다시 추가하려고 하면 등록이 실패했다는 오류 메시지가 표시됩니다. **해결** 버튼을 클릭하여 오류를 해결하고 계산 관리자를 성공적으로 추가할 수 있습니다. 자세한 내용은 [계산 관리자 추가의 4단계를 참조](#)하십시오. vCenter Server에 저장된 NSX-T Data Center에 대한 정보를 제거하려면 [vCenter Server에서 NSX-T Data Center 확장 제거의 단계](#)를 수행합니다.

업그레이드 중 백업 및 복원

업그레이드 프로세스 동안 관리부의 응답이 중지되고 업그레이드가 진행되는 동안 생성된 백업을 복원해야 합니다.

문제

업그레이드 조정기가 업그레이드되었으며 관리부는 응답을 중지합니다. 업그레이드가 진행되는 동안 생성된 백업이 있습니다.

해결책

- 1 백업이 생성된 동일한 IP 주소를 사용하여 관리부 노드를 배포합니다.
- 2 업그레이드 프로세스를 시작할 때 사용한 업그레이드 번들을 업로드합니다.
- 3 업그레이드 조정기를 업그레이드합니다.
- 4 업그레이드 프로세스 동안 생성된 백업을 복원합니다.
- 5 필요한 경우 새 업그레이드 번들을 업로드합니다.
- 6 업그레이드 프로세스를 계속합니다.

vCenter Server에서 NSX-T Data Center 확장 제거

계산 관리자를 추가하면 NSX Manager는 자체 ID를 확장으로 vCenter Server에 추가합니다. 계산 관리자를 제거하면 vCenter Server의 확장이 자동으로 제거됩니다. 어떤 이유로든 확장이 제거되지 않은 경우 다음 절차를 사용하여 확장을 수동으로 제거할 수 있습니다.

사전 요구 사항

<https://kb.vmware.com/s/article/2042554>의 절차에 따라 vCenter Server MOB(관리 개체 브라우저)에 대한 액세스를 사용하도록 설정합니다.

절차

- 1 `https://<vCenter Server 호스트 이름 또는 IP 주소>/mob`에서 MOB에 로그인합니다.
- 2 속성 테이블에서 **content** 속성에 대한 값인 **content** 링크를 클릭합니다.
- 3 속성 테이블에서 **extensionManager** 속성에 대한 값인 **ExtensionManager** 링크를 클릭합니다.
- 4 메서드 테이블에서 **UnregisterExtension** 링크를 클릭합니다.
- 5 값 텍스트 필드에 `com.vmware.nsx.management.nsx`를 입력합니다.
- 6 페이지 오른쪽에서 매개 변수 테이블 아래에 있는 **메서드 호출** 링크를 클릭합니다.
메서드 결과에 void가 표시되지만 확장은 제거됩니다.
- 7 확장이 제거되었는지 확인하려면 이전 페이지에서 **FindExtension** 메서드를 클릭하고 확장에 대해 동일한 값을 입력하여 호출합니다.
결과는 void여야 합니다.

NSX Manager 클러스터 관리

NSX Manager가 작동 불가능 상태가 될 경우 재부팅할 수 있습니다. NSX Manager의 IP 주소를 변경할 수도 있습니다.

운영 환경에서는 고가용성을 제공하기 위해 NSX Manager 클러스터에 3개의 멤버가 포함되는 것이 좋습니다. NSX Manager를 삭제하고 새로 배포하는 경우 새 NSX Manager에 동일하거나 다른 IP 주소가 포함될 수 있습니다.

참고 기본 NSX Manager 노드는 Manager 클러스터를 생성하기 전에 먼저 생성한 노드입니다. 이 노드는 삭제할 수 없습니다. 기본 관리자 노드의 UI에서 2개 이상의 관리자 노드를 배포하여 클러스터를 구성하면 두 번째 및 세 번째 관리자 노드에만 삭제 옵션(톱니바퀴 아이콘)이 제공됩니다. 관리자 노드 제거 및 추가에 대한 자세한 내용은 [NSX Manager의 IP 주소 변경 항목](#)을 참조하십시오.

NSX Manager 클러스터의 상태 및 구성 보기

NSX Manager UI에서 NSX Manager 클러스터의 구성 및 상태를 볼 수 있습니다. CLI를 사용하여 추가 정보를 얻을 수 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 <https://nsx-manager-ip-address>에서 NSX Manager에 로그인합니다.
- 2 **시스템 > 개요** 선택
NSX Manager 클러스터의 상태가 표시됩니다.
- 3 구성에 대한 추가 정보를 보려면 다음 CLI 명령을 실행합니다.

```

manager1> get cluster config
Cluster Id: 18807edd-56d1-4107-b7b7-508d766a08e3
Cluster Configuration Version: 3
Number of nodes in the cluster: 3

Node UUID: 43cd0642-275c-af1d-fe46-1f5200f9e5f9
Node Status: JOINED
  ENTITY                                UUID                                IP
ADDRESS    PORT    FQDN
  HTTPS                                5c8d01f1-f3ee-4f94-b517-a093d8fbfad3
10.160.71.225  443    ychin-nsxmanager-ob-12065118-1-F5
  CONTROLLER                            06fd0574-69c0-432e-a8af-53d140dbef8f
10.160.71.225  -      ychin-nsxmanager-ob-12065118-1-F5
  CLUSTER_BOOT_MANAGER                  da8d535e-7a0c-4dd8-8919-d88bdde006b8
10.160.71.225  -      ychin-nsxmanager-ob-12065118-1-F5
  DATASTORE                            3c9c4ec1-afef-47bd-aadb-1ed6a5536bc4
10.160.71.225  9000   ychin-nsxmanager-ob-12065118-1-F5
  MANAGER                               eb5e8922-23bd-4c3a-ae22-d13d9195a6bc
10.160.71.225  -      ychin-nsxmanager-ob-12065118-1-F5
  POLICY                                f9da1039-08ad-4a20-bacc-5b91c5d67730
10.160.71.225  -      ychin-nsxmanager-ob-12065118-1-F5

Node UUID: 8ebb0642-201e-6a5f-dd47-a1e38542e672
Node Status: JOINED
  ENTITY                                UUID                                IP
ADDRESS    PORT    FQDN
  HTTPS                                3757f155-8a5d-4b53-828f-d67041d5a210
10.160.93.240  443    ychin-nsxmanager-ob-12065118-2-F5
  CONTROLLER                            7b1c9952-8738-4900-b68b-ca862aa4f6a9
10.160.93.240  -      ychin-nsxmanager-ob-12065118-2-F5
  CLUSTER_BOOT_MANAGER                  b5e12db1-5e0d-4e33-a571-6ba258dceb2e
10.160.93.240  -      ychin-nsxmanager-ob-12065118-2-F5
  DATASTORE                            bee1f629-4e23-4ab8-8083-9e0f0bb83178
10.160.93.240  9000   ychin-nsxmanager-ob-12065118-2-F5
  MANAGER                               45ccd6e3-1497-4334-944c-e6bbcd5c723e
10.160.93.240  -      ychin-nsxmanager-ob-12065118-2-F5
  POLICY                                d5ba5803-b059-4fbc-897c-3aace8cf1219
10.160.93.240  -      ychin-nsxmanager-ob-12065118-2-F5

Node UUID: 2e7e0642-df4a-b2ec-b9e8-633d1469f1ea
Node Status: JOINED
  ENTITY                                UUID                                IP
ADDRESS    PORT    FQDN
  HTTPS                                bce3cc4c-7d60-45e2-aa7b-cdc75e445a14

```

10.160.76.33	443	ychin-nsxmanager-ob-12065118-3-F5
	CONTROLLER	ced46f5c-9e52-4b31-a1cb-b3dead991c71
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5
	CLUSTER_BOOT_MANAGER	88b70d31-3428-4ccc-ab57-55859f45030c
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5
	DATASTORE	fb4aec3c-cae3-4386-b5b9-c0b99b7d9048
10.160.76.33	9000	ychin-nsxmanager-ob-12065118-3-F5
	MANAGER	82b07440-3ff6-4f67-a1c9-e9327d1686ad
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5
	POLICY	61f21a78-a56c-4af1-867b-3f24132d53c7
10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5

4 상태에 대한 추가 정보를 보려면 다음 CLI 명령을 실행합니다.

```

manager1> get cluster status
Cluster Id: 18807edd-56d1-4107-b7b7-508d766a08e3
Group Type: DATASTORE
Group Status: STABLE

Members:
  UUID                                FQDN
IP          STATUS
 43cd0642-275c-af1d-fe46-1f5200f9e5f9  ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225  UP
 8ebb0642-201e-6a5f-dd47-a1e38542e672  ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240  UP
 2e7e0642-df4a-b2ec-b9e8-633d1469f1ea  ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33  UP

Group Type: CLUSTER_BOOT_MANAGER
Group Status: STABLE

Members:
  UUID                                FQDN
IP          STATUS
 43cd0642-275c-af1d-fe46-1f5200f9e5f9  ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225  UP
 8ebb0642-201e-6a5f-dd47-a1e38542e672  ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240  UP
 2e7e0642-df4a-b2ec-b9e8-633d1469f1ea  ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33  UP

Group Type: CONTROLLER
Group Status: STABLE

Members:
  UUID                                FQDN
IP          STATUS
 7b1c9952-8738-4900-b68b-ca862aa4f6a9  ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240  UP
 ced46f5c-9e52-4b31-a1cb-b3dead991c71  ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33  UP
 06fd0574-69c0-432e-a8af-53d140dbef8f  ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225  UP

```

```

Group Type: MANAGER
Group Status: STABLE

Members:
  UUID                                FQDN
IP          STATUS
  43cd0642-275c-af1d-fe46-1f5200f9e5f9  ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225  UP
  8ebb0642-201e-6a5f-dd47-a1e38542e672  ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240  UP
  2e7e0642-df4a-b2ec-b9e8-633d1469f1ea  ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33  UP

Group Type: POLICY
Group Status: STABLE

Members:
  UUID                                FQDN
IP          STATUS
  43cd0642-275c-af1d-fe46-1f5200f9e5f9  ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225  UP
  8ebb0642-201e-6a5f-dd47-a1e38542e672  ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240  UP
  2e7e0642-df4a-b2ec-b9e8-633d1469f1ea  ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33  UP

Group Type: HTTPS
Group Status: STABLE

Members:
  UUID                                FQDN
IP          STATUS
  43cd0642-275c-af1d-fe46-1f5200f9e5f9  ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225  UP
  8ebb0642-201e-6a5f-dd47-a1e38542e672  ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240  UP
  2e7e0642-df4a-b2ec-b9e8-633d1469f1ea  ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33  UP

```

NSX Manager 클러스터 종료 및 전원 켜기

NSX Manager 클러스터를 종료해야 하는 경우 다음 절차를 사용하십시오.

절차

- 1 NSX Manager 클러스터를 종료하려면 한 번에 하나의 관리자 노드를 종료하십시오. admin 관리자 노드의 CLI(명령줄 인터페이스)에 로그인하여 shutdown 명령을 실행하고 vCenter Server에서 관리자 노드 VM을 종료할 수 있습니다.

다음 단계를 진행하기 전에 vCenter Server에서 VM 전원이 꺼져 있는지 확인합니다.

- 2 NSX Manager 클러스터의 전원을 켜려면 vCenter Server에서 한 번에 하나의 관리자 노드 VM의 전원을 켜십시오.

다음 단계를 진행하기 전에 노드가 실행 중인지 확인합니다.

NSX Manager 재부팅

CLI 명령을 통해 NSX Manager를 재부팅하여 위험 오류에서 복구할 수 있습니다.

여러 NSX Manager를 재부팅해야 하는 경우 한 번에 하나씩 재부팅해야 합니다. 재부팅된 NSX Manager가 온라인 상태가 될 때까지 기다린 후 다음을 재부팅합니다.

절차

- 1 NSX Manager의 CLI에 로그인합니다.
- 2 다음 명령을 실행합니다.

```
nsx-manager> reboot
Are you sure you want to reboot (yes/no): y
```

NSX Manager의 IP 주소 변경

NSX Manager 클러스터에서 NSX Manager의 IP 주소를 변경할 수 있습니다. 이 섹션에서는 몇 가지 접근 방법에 대해 설명합니다.

예를 들어, Manager A, Manager B 및 Manager C로 구성된 클러스터가 있는 경우 다음과 같은 방법으로 하나 이상의 관리자에 대한 IP 주소를 변경할 수 있습니다.

- 시나리오 A:
 - Manager A의 IP 주소는 172.16.1.11입니다.
 - Manager B의 IP 주소는 172.16.1.12입니다.
 - Manager C의 IP 주소는 172.16.1.13입니다.
 - 새 IP 주소(예: 192.168.55.11)를 사용하는 Manager D를 추가합니다.
 - Manager A를 제거합니다.
 - 새 IP 주소(예: 192.168.55.12)를 사용하는 Manager E를 추가합니다.
 - Manager B를 제거합니다.
 - 새 IP 주소(예: 192.168.55.13)를 사용하는 Manager F를 추가합니다.
 - Manager C를 제거합니다.
- 시나리오 B:
 - Manager A의 IP 주소는 172.16.1.11입니다.
 - Manager B의 IP 주소는 172.16.1.12입니다.
 - Manager C의 IP 주소는 172.16.1.13입니다.

- 새 IP 주소(예: 192.168.55.11)를 사용하는 Manager D를 추가합니다.
 - 새 IP 주소(예: 192.168.55.12)를 사용하는 Manager E를 추가합니다.
 - 새 IP 주소(예: 192.168.55.13)를 사용하는 Manager F를 추가합니다.
 - Manager A, Manager B 및 Manager C를 제거합니다.
- 시나리오 C:
- Manager A의 IP 주소는 172.16.1.11입니다.
 - Manager B의 IP 주소는 172.16.1.12입니다.
 - Manager C의 IP 주소는 172.16.1.13입니다.
 - Manager A를 제거합니다.
 - 새 IP 주소(예: 192.168.55.11)를 사용하는 Manager D를 추가합니다.
 - Manager B를 제거합니다.
 - 새 IP 주소(예: 192.168.55.12)를 사용하는 Manager E를 추가합니다.
 - Manager C를 제거합니다.
 - 새 IP 주소(예: 192.168.55.13)를 사용하는 Manager F를 추가합니다.

처음 두 시나리오에서는 이 IP 주소를 변경하는 동안 추가 NSX Manager에 대한 추가 가상 RAM, CPU 및 디스크가 필요합니다.

시나리오 C는 NSX Manager의 수를 일시적으로 줄이고, IP 주소를 변경하는 동안 두 활성 관리자 중 하나가 손실되면서 NSX-T의 작업에 영향을 주게 되므로 권장되지 않습니다. 이 시나리오는 추가 가상 RAM, CPU 및 디스크를 사용할 수 없고 IP 주소 변경이 필요한 상황을 위한 것입니다.

참고 클러스터 VIP 기능을 사용하는 경우 클러스터 VIP에서 모든 NSX Manager가 동일한 서브넷에 있어야 하므로 IP 주소 변경 중에 새 IP 주소에 대해 동일한 서브넷을 사용하거나 클러스터 VIP를 사용하지 않도록 설정해야 합니다.

사전 요구 사항

NSX Manager를 클러스터에 배포하는 방법을 숙지합니다. 자세한 내용은 "NSX-T 데이터 센터 설치 가이드" 를 참조하십시오.

절차

- 1 제거할 NSX Manager가 수동으로 배포된 경우 다음 단계를 수행합니다.
 - a 다음 CLI 명령을 실행하여 NSX Manager를 클러스터에서 분리합니다.


```
detach node <node-id>
```
 - b NSX Manager VM을 삭제합니다.

- 2 삭제할 NSX Manager가 NSX Manager UI를 통해 자동으로 배포된 경우 다음 단계를 수행합니다.
 - a 브라우저에서 관리자 권한으로 NSX Manager(<https://nsx-manager-ip-address>)에 로그인합니다.
이 NSX Manager는 삭제할 대상이 아니어야 합니다.
 - b 시스템 탭에서 **NSX 관리 노드**를 클릭합니다.
NSX Manager 클러스터의 상태가 표시됩니다.
 - c 삭제할 NSX Manager에 대해 톱니 바퀴 아이콘을 클릭하고 **삭제**를 선택합니다.
- 3 새 NSX Manager를 배포합니다.

NSX Manager 노드 크기 조정

언제든지 NSX Manager 노드의 CPU 코어 수 또는 메모리를 변경할 수 있습니다.

정상 작동 조건에서는 3개의 Manager 노드 모두 CPU 코어 및 메모리 수가 동일해야 합니다. NSX 관리 클러스터의 NSX Manager 간 CPU 또는 메모리 불일치는 한 크기의 NSX Manager를 다른 크기의 NSX Manager로 전환하는 경우에만 허용됩니다.

vCenter Server에서 NSX Manager VM에 대한 리소스 할당 예약을 구성한 경우 예약을 조정해야 할 수 있습니다. 자세한 내용은 vSphere 설명서를 참조하십시오.

사전 요구 사항

- 새 크기가 Manager 노드의 시스템 요구 사항을 충족하는지 확인합니다. 자세한 내용은 "NSX-T Data Center 설치 가이드"의 "NSX Manager VM 시스템 요구 사항"을 참조하십시오.
- NSX Manager를 클러스터에 배포하는 방법을 숙지합니다. 자세한 내용은 "NSX-T 데이터 센터 설치 가이드"를 참조하십시오.
- 클러스터에서 Manager 노드를 제거하는 방법에 대한 내용은 NSX Manager의 IP 주소 변경을 참조하십시오.

절차

- 1 새 크기의 새 Manager 노드를 배포합니다.
- 2 새 Manager 노드를 클러스터에 추가합니다.
- 3 이전 Manager 노드를 제거합니다.
- 4 1 ~ 3 단계를 반복하여 다른 두 개의 이전 Manager 노드를 교체합니다.

vCenter Server에서 ESXi 호스트 전송 노드 추가 및 제거

한 VC(vCenter Server)에서 다른 VC로, 한 NSX Manager 클러스터에서 다른 클러스터로 ESXi 호스트 전송 노드를 이동할 수도 있습니다.

시나리오 1: VC1은 NSX Manager 클러스터 1에 연결되어 있고 VC2는 NSX Manager 클러스터 2에 연결되어 있음

ESXi 호스트 전송 노드인 ESX1이 VC1에 있는 경우 다음 단계를 수행하여 VC2로 이동할 수 있습니다.

- 1 ESX1에서 NSX를 제거합니다.
- 2 ESX1을 VC2로 이동합니다.
- 3 전송 노드 프로파일을 ESX1에 적용합니다.

시나리오 2: VC1 및 VC2 모두 NSX Manager 클러스터에 연결됨

ESXi 호스트 전송 노드인 ESX1이 VC1에 있는 경우 다음 단계를 수행하여 VC2로 이동할 수 있습니다.

- 1 ESX1에서 NSX를 제거합니다.
- 2 ESX1을 VC2로 이동합니다.
- 3 전송 노드 프로파일을 ESX1에 적용합니다.

시나리오 3: VC1이 NSX Manager 클러스터 1에 연결됨

ESXi 호스트 전송 노드인 ESX1이 VC1에 있는 경우 다음 단계를 수행하여 독립형 호스트로 NSX Manager 클러스터 2로 이동할 수 있습니다.

- 1 ESX1에서 NSX를 제거합니다.
- 2 NSX Manager 클러스터 2에 ESX1을 추가합니다.

NSX Edge 클러스터에서 NSX Edge 전송 노드 교체

NSX Manager UI 또는 API를 사용하여 NSX Edge 클러스터에서 NSX Edge 전송 노드를 교체할 수 있습니다.

NSX Manager UI를 사용하여 NSX Edge 전송 노드 교체

다음 절차에서는 NSX Manager UI를 사용하여 NSX Edge 클러스터에서 NSX Edge 전송 노드를 교체하는 방법을 설명합니다. Edge 전송 노드는 실행 중인지 여부에 관계없이 교체할 수 있습니다.

교체할 Edge 노드가 실행되고 있지 않은 경우 새 Edge 노드는 동일한 관리 IP 주소와 TEP IP 주소를 가질 수 있습니다. 교체할 Edge 노드가 실행되고 있는 경우 새 Edge 노드는 다른 관리 IP 주소와 TEP IP 주소를 가져야 합니다.

사전 요구 사항

NSX Edge 노드를 설치하고, Edge 노드를 관리부에 가입시키고, NSX Edge 전송 노드를 생성하는 절차를 숙지하십시오. 자세한 내용은 "NSX-T 데이터 센터 설치 가이드" 를 참조하십시오.

절차

- 1 새 Edge 전송 노드에 교체할 Edge 전송 노드와 동일한 구성이 포함되도록 하려면 다음 API 호출을 수행하여 구성을 찾습니다.

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes/<tn-id>
```

- 2 Edge 전송 노드를 설치하고 구성하려면 "NSX-T Data Center 설치" 가이드의 절차를 따르십시오.
이 Edge 전송 노드에 교체할 Edge 전송 노드와 동일한 구성이 포함되도록 하려면 1단계에서 가져온 구성을 사용합니다.
- 3 NSX Manager에서 **시스템 > 패브릭 > 노드 > Edge 클러스터**를 선택합니다.
- 4 첫 번째 열의 확인란을 클릭하여 Edge 클러스터를 선택합니다.
- 5 **작업 > Edge 클러스터 멤버 교체**를 클릭합니다.
교체할 전송 노드를 유지 보수 모드로 전환하는 것이 좋습니다. 전송 노드가 실행되고 있지 않은 경우 이 권장 사항을 무시해도 됩니다.
- 6 드롭다운 목록에서 교체할 노드를 선택합니다.
- 7 드롭다운 목록에서 교체용 노드를 선택합니다.
- 8 **저장**을 클릭합니다.

API를 사용하여 NSX Edge 전송 노드 교체

다음 절차에서는 NSX-T API를 사용하여 NSX Edge 클러스터에서 NSX Edge 전송 노드를 교체하는 방법을 설명합니다. Edge 전송 노드는 실행 중인지 여부에 관계없이 교체할 수 있습니다.

교체할 Edge 노드가 실행되고 있지 않은 경우 새 Edge 노드는 동일한 관리 IP 주소와 TEP IP 주소를 가질 수 있습니다. 교체할 Edge 노드가 실행되고 있는 경우 새 Edge 노드는 다른 관리 IP 주소와 TEP IP 주소를 가져야 합니다.

사전 요구 사항

NSX Edge 노드를 설치하고, Edge 노드를 관리부에 가입시키고, NSX Edge 전송 노드를 생성하는 절차를 숙지하십시오. 자세한 내용은 "NSX-T 데이터 센터 설치 가이드" 를 참조하십시오.

절차

- 1 새 Edge 전송 노드에 교체할 Edge 전송 노드와 동일한 구성이 포함되도록 하려면 다음 API 호출을 수행하여 구성을 찾습니다.

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes/<tn-id>
```

- 2 Edge 전송 노드를 설치하고 구성하려면 NSX-T Data Center 설치 가이드의 절차를 따르십시오.
이 Edge 전송 노드에 교체할 Edge 전송 노드와 동일한 구성이 포함되도록 하려면 1단계에서 가져온 구성을 사용합니다.

- 3 API 호출을 수행하여 새 전송 노드 및 교체할 전송 노드의 ID를 가져옵니다. id 필드에는 전송 노드 ID가 포함됩니다. 예를 들면 다음과 같습니다.

```
GET https://<nsx-manager-IP>/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",
  }
}
```

- 4 API 호출을 수행하여 NSX Edge 클러스터의 ID를 가져옵니다. id 필드에는 NSX Edge 클러스터 ID가 포함됩니다. members 어레이에서 NSX Edge 클러스터의 멤버를 가져옵니다. 예를 들면 다음과 같습니다.

```
GET https://<nsx-manager-IP>/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"
    }
  ],
}
```

- 5 NSX Edge 클러스터에서 전송 노드를 교체할 API를 만듭니다. member_index는 교체할 전송 노드의 인덱스와 일치해야 합니다.

예를 들어 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://<nsx-manager-IP>/api/v1/edge-clusters/9a302df7-0833-4237-af1f-4d826c25ad78?
action=replace_transport_node
```

```
{
  "member_index": 0,
  "transport_node_id" : "890f0e3c-aa81-46aa-843b-8ac25fe30bd3"
}
```

vCenter Server가 손실되어 복구할 수 없는 경우 NSX-T 복구

VC(vCenter Server)가 손실되어 복구할 수 없는 경우(백업이 없거나 백업이 손상되었기 때문일 수 있음) VC를 다시 배포한 후 다음 절차를 사용하여 NSX-T 환경을 복구합니다.

새 VC는 원래 VC와 동일한 FQDN 및 IP 주소를 가져야 합니다. 또한 동일한 호스트를 포함하는 동일한 클러스터가 있어야 합니다. 전원이 켜진 VM이 있는 호스트는 VC에 추가할 때 주의해야 합니다. VC 데이터 센터가 아닌 올바른 클러스터에 추가되었는지 확인합니다.

계산 관리자

NSX Manager에서 이전 계산 관리자를 삭제합니다. 그런 다음, 새 VC를 계산 관리자로 추가합니다.

호스트 전송 노드

NSX Manager에서 호스트가 올바른 VC 클러스터에 나타납니다. 어떠한 작업도 필요하지 않습니다.

Edge 노드

NSX Manager UI에서 배포된 Edge 노드를 교체해야 합니다.

- 1 NSX Manager UI를 사용하여 NSX Edge 전송 노드 교체의 절차에 따라 Edge 노드를 교체합니다.
- 2 게이트웨이(또는 논리적 라우터) 및 터널이 새 Edge VM에 구성되어 있는지 확인합니다.
- 3 **시스템 > 패브릭 > Edge 전송 노드**로 이동하여 이전 Edge 노드를 삭제합니다. Edge 노드를 선택하고 **작업 > 삭제**를 클릭합니다. "전원 끄기 실패"와 같은 오류는 무시해도 됩니다.
- 4 VC에서 이전 Edge VM의 전원을 끄고 삭제합니다.
- 5 각 Edge 노드에 대해 위 단계를 반복합니다.

NSX Manager

NSX Manager UI에서 배포된 NSX Manager를 바꿔야 합니다. 일반적으로 두 번째 및 세 번째 NSX Manager는 이러한 방식으로 배포됩니다.

- 1 첫 번째 NSX Manager의 UI에 로그인합니다.
- 2 **시스템 > 장치**로 이동하고 세 번째 NSX Manager를 선택합니다. **작업 > 삭제**를 클릭합니다. 이 작업은 관리자 VM의 전원을 끌 수 없기 때문에 실패합니다. 이제 강제 삭제 옵션을 사용할 수 있습니다. **작업 > 강제 삭제**를 선택합니다.
- 3 강제 삭제가 작동하지 않으면 다음을 수행합니다.
 - a 첫 번째 NSX Manager의 CLI에 로그인합니다.

- b `get cluster status` 명령을 실행하여 세 번째 NSX Manager의 UID를 가져옵니다.
- c `detach node <node-uid>` 명령을 실행하여 클러스터에서 세 번째 NSX Manager를 분리합니다.
- d 다음 API 호출을 수행하여 세 번째 NSX Manager를 강제로 삭제합니다.

```
POST : https://<nsx-manager-1>/api/v1/cluster/nodes/deployments/<node-uid>?
      action=delete&force_delete=true
```

- 4 VC에서 세 번째 NSX Manager의 전원을 끄고 삭제합니다.
- 5 세 번째 NSX Manager와 동일한 구성을 사용하여 새 NSX Manager를 배포합니다.
- 6 위 단계를 반복하여 두 번째 NSX Manager를 삭제합니다.
- 7 두 개의 새 NSX Manager를 배포합니다.

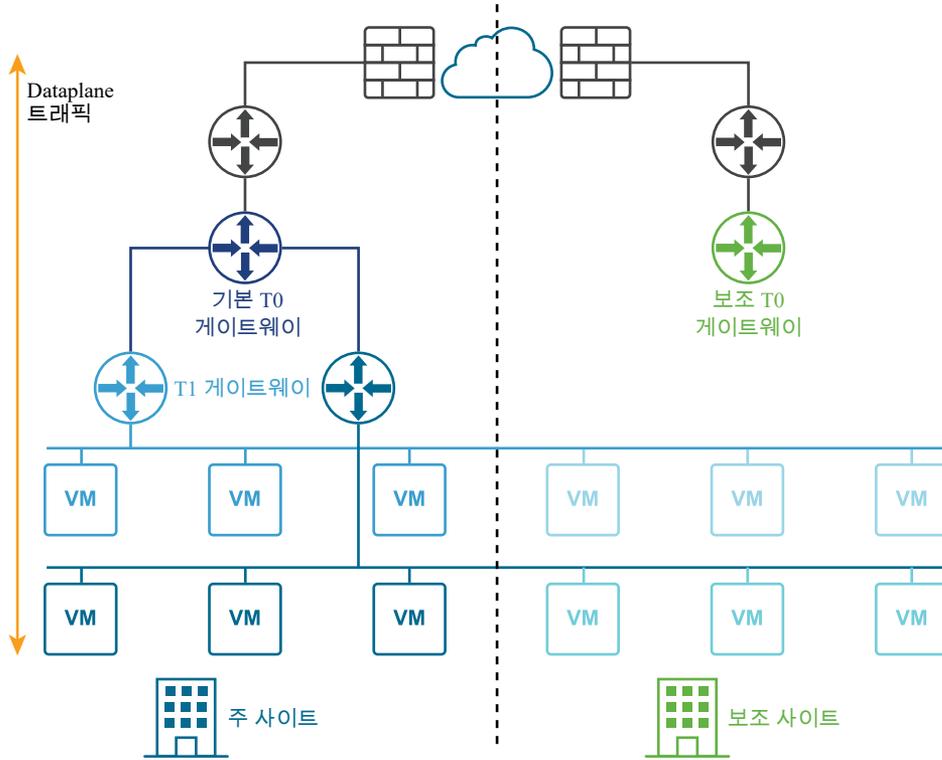
NSX-T Data Center 다중 사이트 배포

NSX-T Data Center는 하나의 NSX Manager 클러스터에서 모든 사이트를 관리할 수 있는 다중 사이트 배포를 지원합니다.

다음과 같은 두 가지 유형의 다중 사이트 배포가 지원됩니다.

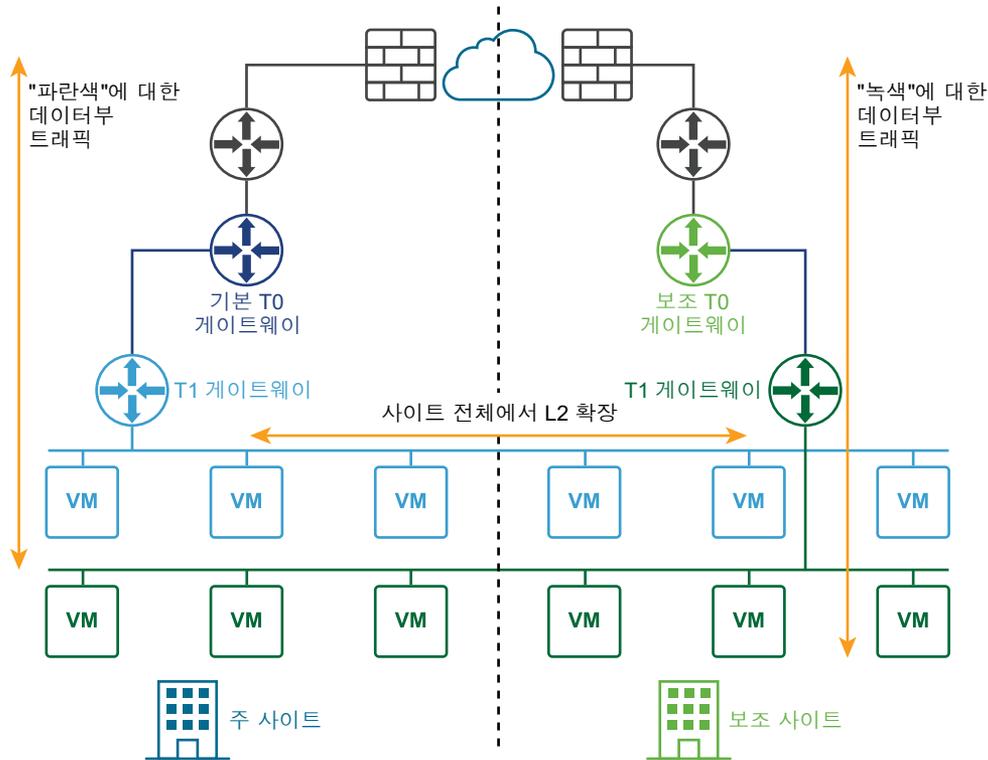
- 재해 복구
- 액티브-액티브

다음 다이어그램은 재해 복구 배포를 보여줍니다.



액티브-액티브 배포의 경우, 모든 사이트가 액티브 상태이고 계층 2 트래픽이 사이트 경계를 넘습니다. 재해 복구 배포의 경우, 주 사이트의 NSX-T Data Center가 엔터프라이즈에 대한 네트워킹을 처리합니다. 보조 사이트는 주 사이트에 심각한 오류가 발생하는 경우 인계하기 위해 대기 중입니다.

다음 다이어그램은 액티브-액티브 배포를 보여줍니다.



관리부 및 데이터부의 자동 또는 수동/스크립팅된 복구를 위해 두 개의 사이트를 배포할 수 있습니다.

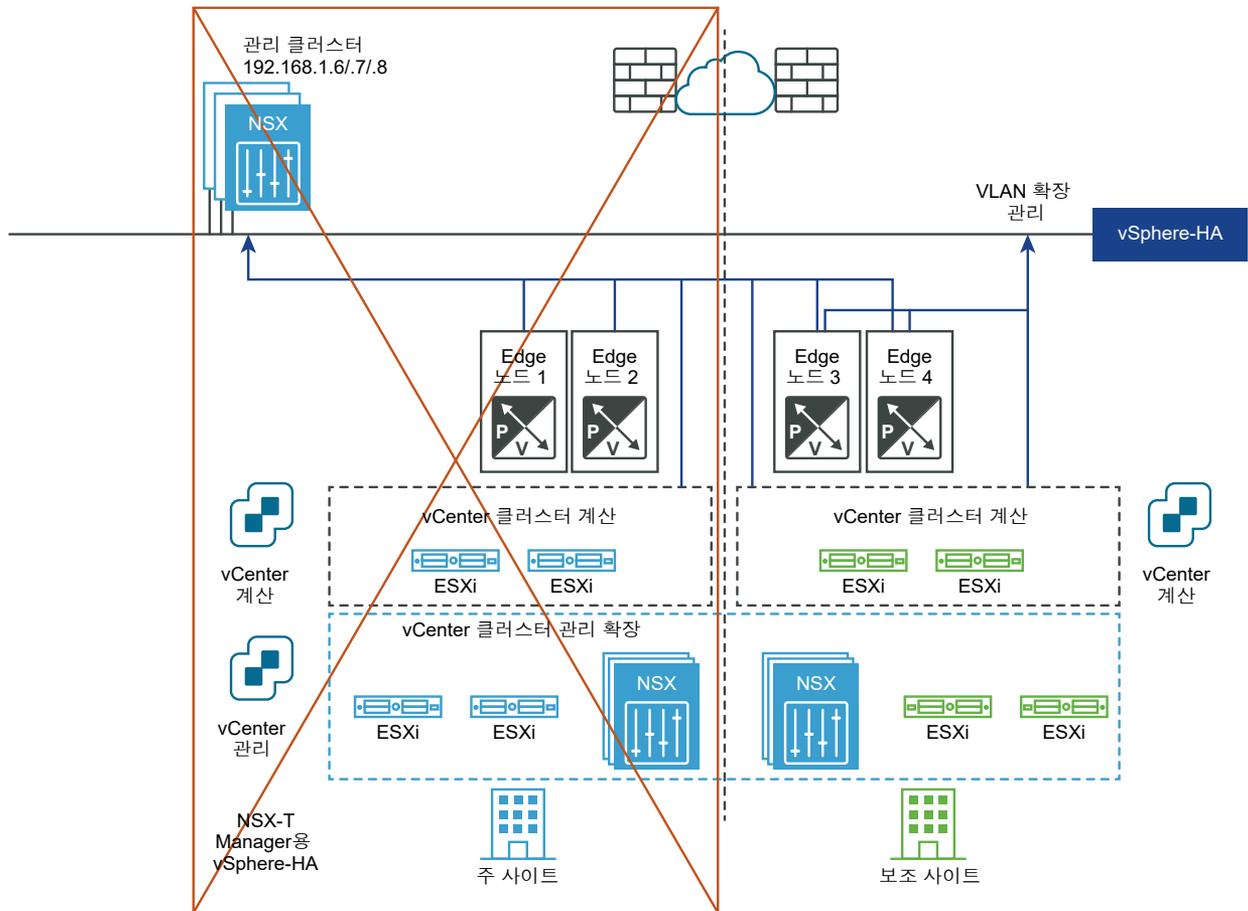
관리부의 자동 복구

요구 사항:

- 구성된 사이트 간에 HA가 있는 확장된 vCenter 클러스터.
- 확장된 관리 VLAN.

NSX Manager 클러스터가 관리 VLAN에 배포되고 물리적으로 기본 사이트에 있습니다. 기본 사이트 장애가 있는 경우 vSphere HA는 보조 사이트에서 NSX Manager를 다시 시작합니다. 모든 전송 노드가 다시 시작된 NSX Manager에 자동으로 다시 연결됩니다. 이 프로세스는 10분 정도 소요됩니다. 이 시간 동안에는 관리부를 사용할 수 없지만 데이터부는 영향을 받지 않습니다.

다음 다이어그램에서는 관리부의 자동 복구를 보여 줍니다.



데이터부의 자동 복구

요구 사항:

- Edge 노드 간의 최대 지연 시간은 10밀리초입니다.
- Tier-0 게이트웨이에 대한 HA 모드는 액티브-대기 상태여야 하며 페일오버 모드는 선점형이어야 합니다.

참고: Tier-1 게이트웨이의 페일오버 모드는 선점형 또는 비선점형일 수 있습니다.

구성 단계:

- API를 사용하여 두 사이트에 대한 장애 도메인을 생성합니다(예: FD1A-Preferred_Site1 및 FD2A-Preferred_Site1). 기본 사이트의 경우 매개 변수 preferred_active_edge_services 를 true로 설정하고 보조 사이트의 경우 false로 설정합니다.

```
POST /api/v1/failure-domains
{
  "display_name": "FD1A-Preferred_Site1",
  "preferred_active_edge_services": "true"
}
```

```
POST /api/v1/failure-domains
```

```
{
  "display_name": "FD2A-Preferred_Site1",
  "preferred_active_edge_services": "false"
}
```

- API를 사용하여 두 사이트 간에 확장되는 Edge 클러스터를 구성합니다. 예를 들어, 클러스터의 기본 사이트에는 Edge 노드 EdgeNode1A 및 EdgeNode1B가 있고 보조 사이트에는 Edge 노드 EdgeNode2A 및 EdgeNode2B가 있습니다. 활성 Tier-0 및 Tier-1 게이트웨이는 EdgeNode1A 및 EdgeNode1B에서 실행됩니다. 대기 Tier-0 및 Tier-1 게이트웨이는 EdgeNode2A 및 EdgeNode2B에서 실행됩니다.
- API를 사용하여 각 Edge 노드를 사이트의 장애 도메인에 연결합니다. 먼저 GET /api/v1/transport-nodes/<transport-node-id> API를 호출하여 Edge 노드에 대한 데이터를 가져옵니다. 추가 속성인 failure_domain_id를 적절하게 설정하여 GET API의 결과를 PUT /api/v1/transport-nodes/<transport-node-id> API 입력으로 사용합니다. 예를 들면 다음과 같습니다.

```
GET /api/v1/transport-nodes/<transport-node-id>
Response:
{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  ...
}

PUT /api/v1/transport-nodes/<transport-node-id>
{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  ...
  "failure_domain_id": "<UUID>",
}
```

- API를 사용하여 장애 도메인에 따라 노드를 할당하도록 Edge 클러스터를 구성합니다. 먼저 GET /api/v1/edge-clusters/<edge-cluster-id> API를 호출하여 Edge 클러스터에 대한 데이터를 가져옵니다. 추가 속성인 allocation_rules를 적절하게 설정하여 GET API의 결과를 PUT /api/v1/edge-clusters/<edge-cluster-id> API 입력으로 사용합니다. 예를 들면 다음과 같습니다.

```
GET /api/v1/edge-clusters/<edge-cluster-id>
Response:
{
  "_revision": 0,
  "id": "bf8d4daf-93f6-4c23-af38-63f6d372e14e",
  "resource_type": "EdgeCluster",
  ...
}

PUT /api/v1/edge-clusters/<edge-cluster-id>
```

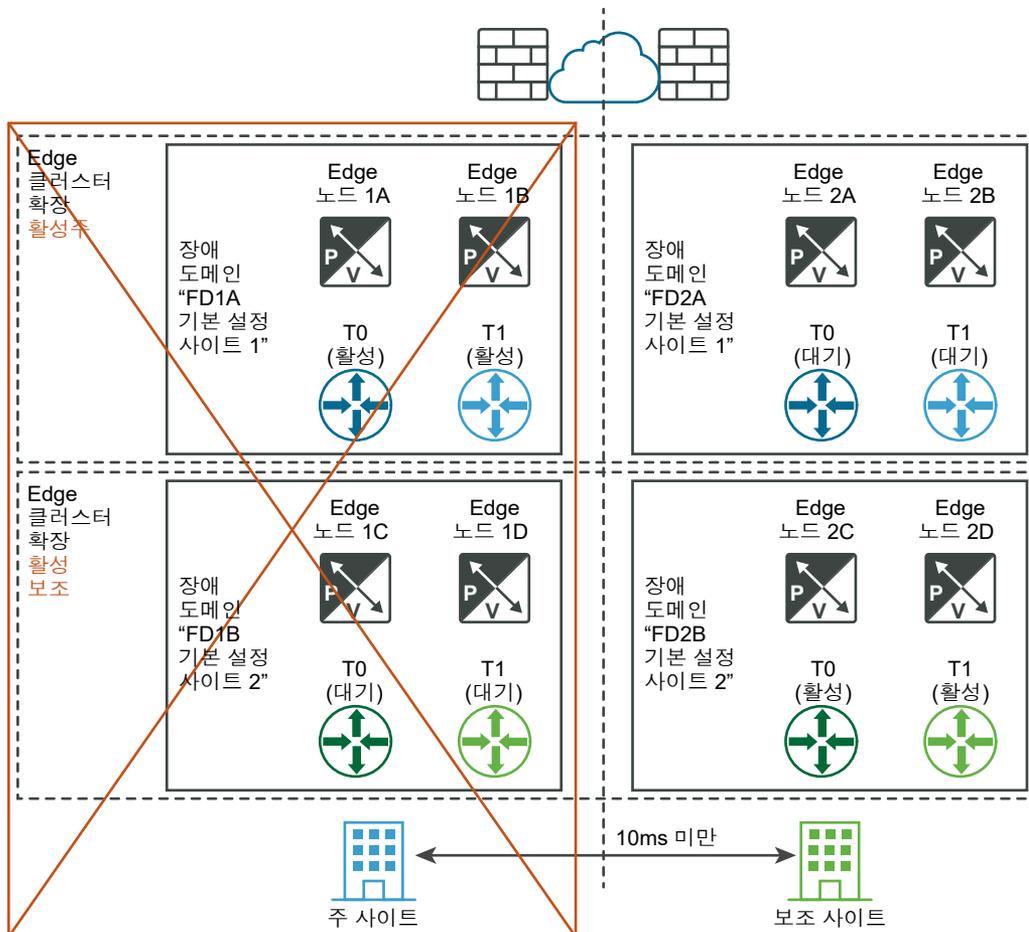
```

{
  "_revision": 0,
  "id": "bf8d4daf-93f6-4c23-af38-63f6d372e14e",
  "resource_type": "EdgeCluster",
  ...
  "allocation_rules": [
    {
      "action": {
        "enabled": true,
        "action_type": "AllocationBasedOnFailureDomain"
      }
    }
  ],
}
    
```

- API 또는 NSX Manager UI를 사용하여 Tier-0 및 Tier-1 게이트웨이를 생성합니다.

기본 사이트의 Edge 노드가 실패하면 해당 노드에 호스팅되는 Tier-0 및 Tier-1 게이트웨이가 보조 사이트의 Edge 노드로 마이그레이션됩니다.

다음 다이어그램에서는 데이터부의 자동 복구를 보여줍니다.



관리부의 수동/스크립팅된 복구

요구 사항:

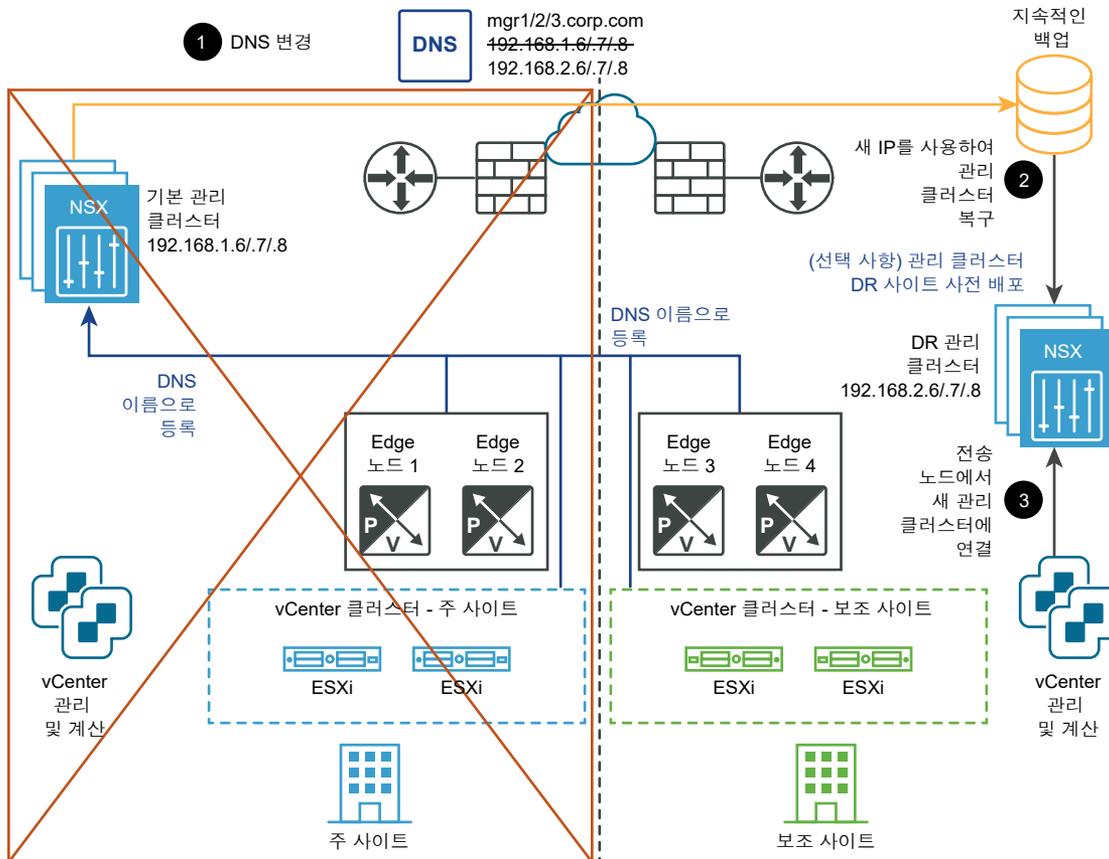
- 짧은 TTL(예: 5분)이 지정된 NSX Manager의 DNS.
- 연속 백업

vSphere HA 및 확장된 관리 VLAN은 필요하지 않습니다. NSX-T Manager는 짧은 TTL을 가진 DNS 이름과 연결되어야 합니다. 모든 전송 노드(Edge 노드 및 하이퍼바이저)는 해당 DNS 이름을 사용하여 NSX Manager에 연결해야 합니다. 시간을 절약하기 위해 선택적으로 보조 사이트에 NSX Manager 클러스터를 미리 설치할 수 있습니다.

복구 단계는 다음과 같습니다.

- 1 NSX Manager 클러스터에 다른 IP 주소가 사용되도록 DNS 레코드를 변경합니다.
- 2 백업에서 NSX Manager 클러스터를 복원합니다.
- 3 전송 노드를 새 NSX Manager 클러스터에 연결합니다.

다음 다이어그램은 관리부의 수동/스크립팅된 복구를 보여 줍니다.



데이터부의 수동/스크립팅된 복구

요구 사항:

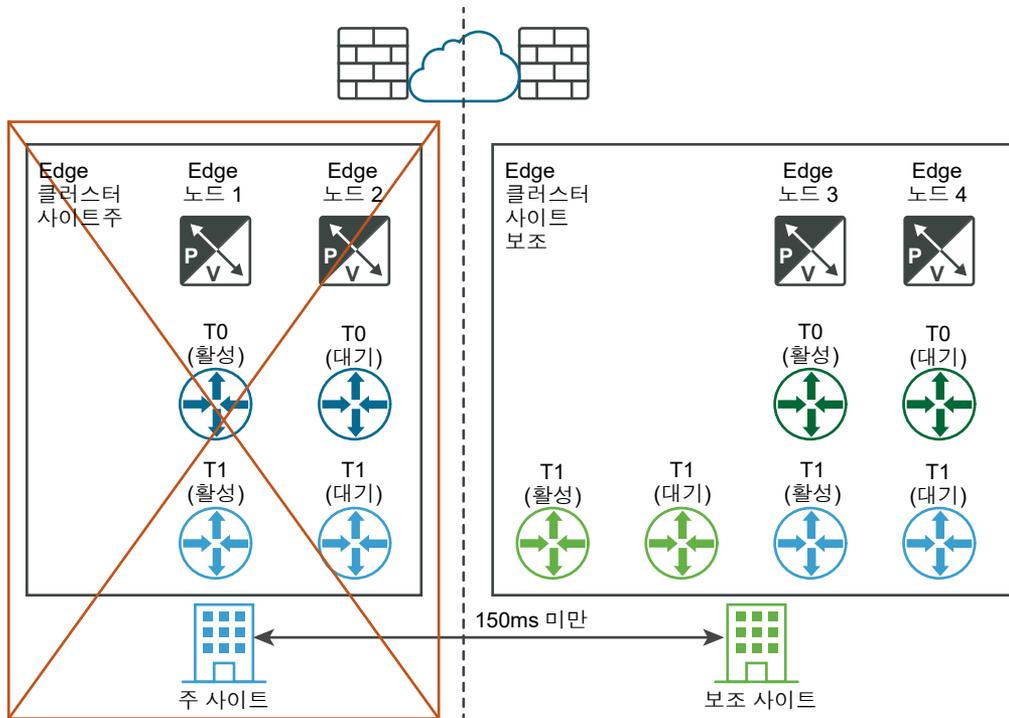
- Edge 노드 간의 최대 지연 시간은 150밀리초입니다.

Edge 노드는 VM 또는 베어메탈일 수 있습니다. Tier-0 게이트웨이는 액티브-대기 또는 액티브-액티브일 수 있습니다. Edge 노드 VM을 서로 다른 vCenter Server에 설치할 수 있습니다. vSphere HA는 필요하지 않습니다.

복구 단계는 다음과 같습니다.

- 1 DR(재해 복구) 사이트의 기존 Edge 클러스터에 대기 Tier-0 게이트웨이를 생성합니다.
- 2 API를 사용하여 Tier-0 게이트웨이에 연결된 Tier-1 게이트웨이를 DR 사이트의 Tier-0 게이트웨이로 이동합니다.
- 3 API를 사용하여 독립형 Tier-1 게이트웨이를 DR 사이트로 이동합니다.
- 4 API를 사용하여 계층-2 브리지를 DR 사이트로 이동합니다.

다음 다이어그램은 데이터부의 수동/스크립팅된 복구를 보여 줍니다.



Edge 클러스터 주에서 T1(파란색)에 대한 스크립트 또는 수동 작업:

- Edge 클러스터 보조로 전송
- T0 - 보조(녹색)로 연결

다중 사이트 배포에 대한 요구 사항

사이트 간 통신

- 대역폭은 1Gbps 이상이어야 하고 지연 시간(RTT)은 150ms 미만이어야 합니다.
- MTU는 1,600 이상이어야 합니다. 9,000이 권장됩니다.

NSX Manager 구성

- NSX-T Data Center 구성 변경 시 자동 백업을 사용하도록 설정해야 합니다.
- NSX Manager는 FQDN을 사용하도록 설정되어야 합니다.

데이터부 복구

- 공용 IP 주소가 NAT 또는 로드 밸런서와 같은 서비스를 통해 노출되는 경우 동일한 인터넷 제공자를 사용해야 합니다.
- Tier-0 게이트웨이에 대한 HA 모드는 액티브-대기 상태여야 하며 페일오버 모드는 선점형이어야 합니다.

클라우드 관리 시스템

- CMS(클라우드 관리 시스템)에서 NSX-T Data Center 플러그인을 지원해야 합니다. 이 릴리스에서는 VIO(VMware Integrated Openstack) 및 vRA(vRealize Automation)가 이 요구 사항을 충족합니다.

제한 사항

- 로컬 송신 기능이 없습니다. 모든 North-South 트래픽이 한 사이트 내에서 발생해야 합니다.
- 계산 재해 복구 소프트웨어는 NSX-T Data Center(예: VMware SRM 8.1.2 이상)를 지원해야 합니다.

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 21-7. 시스템 구성 명령 및 API 요청

작업	명령줄 (NSX Manager 및 NSX Edge)	API 요청 (NSX Manager만 해당)
시스템 시간대 설정	set timezone <timezone>	PUT https://<nsx-mgr>/api/v1/node
NTP 서버 설정	set ntp-server <ntp-server>	PUT https://<nsx-mgr>/api/v1/node/ services/ntp
DNS 서버 설정	set name-servers <dns-server>	PUT https://<nsx-mgr>/api/v1/node/ network/name-servers
DNS 검색 도메인 설정	set search-domains <domain>	PUT https://<nsx-mgr>/api/v1/node/ network/search-domains

라이선스 키 추가 및 라이선스 사용량 보고서 생성

라이선스 키를 추가하고 라이선스 사용량 보고서를 생성할 수 있습니다. 사용량 보고서는 CSV 형식의 파일입니다.

다음의 비평가판 NSX-T Data Center 라이선스 유형을 사용할 수 있습니다.

- NSX Data Center Standard
- NSX Data Center Professional
- NSX Data Center Advanced
- NSX Data Center Enterprise Plus
- NSX Data Center Remote Office Branch Office(ROBO)
- NSX Advanced(NSX-T Data Center 2.5.1에서 사용 가능)
- NSX Enterprise(NSX-T Data Center 2.5.1에서 사용 가능)

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. 기본 평가 라이선스가 있으면 새 평가 라이선스를 할당할 수 있습니다. 새 평가 라이선스가 기본 평가 라이선스를 재정의합니다. 기본이 아닌 평가판 라이선스를 할당 취소할 수도 있습니다. 이 경우 기본 평가판 라이선스가 복원됩니다.

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.

라이선스가 60일 내에 만료되거나 만료된 경우 NSX Manager에 로그인하면 상황을 알려 주는 알림 창이 표시됩니다. 창의 오른쪽 상단 모서리에 있는 알림 아이콘을 클릭하여 알림을 볼 수도 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 라이선스 > 추가**를 선택합니다.
- 3 라이선스 키를 입력합니다.
- 4 라이선스 사용량 보고서를 생성하려면 **내보내기 > 라이선스 사용량 보고서**를 선택합니다.

CSV 보고서에는 다음 기능의 VM, CPU, 고유한 동시 사용자, vCPU 및 코어 사용량이 나열됩니다.

- 스위칭 및 라우팅
- NSX Edge 로드 밸런서

- VPN
- DFW
- 컨텍스트를 인식하는 마이크로 세분화 - 애플리케이션 식별
- 컨텍스트를 인식하는 마이크로 세분화 - 원격 데스크톱 세션 호스트에 대한 ID 방화벽
- 서비스 삽입
- ID 기반 방화벽
- 고급 Guest Introspection

참고 다음 기능은 Limited Export 릴리스 버전에 대해 사용하지 않도록 설정되었습니다.

- IPsec VPN
- HTTPS 기반 로드 밸런서

인증서 설정

인증서를 가져오고, CSR(인증서 서명 요청)을 생성하고, 자체 서명된 인증서를 생성하고, CRL(인증서 해지 목록)을 가져올 수 있습니다.

NSX-T Data Center를 설치하면 관리자 노드 및 클러스터에 자체 서명된 인증서가 생깁니다. 보안을 강화하려면 자체 서명된 인증서를 CA 서명 인증서로 바꾸는 것이 좋습니다.

인증서 가져오기

활성화 후에 개인 키를 사용하여 인증서를 가져와 자체 서명된 기본 인증서를 대체할 수 있습니다.

RSA 기반 인증서만 지원됩니다.

사전 요구 사항

인증서를 사용할 수 있는지 확인합니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 인증서**를 선택합니다.
- 3 **가져오기 > 인증서 가져오기**를 선택하고 인증서 세부 정보를 입력합니다.

옵션	설명
이름	인증서에 이름을 할당합니다.
인증서 콘텐츠	컴퓨터의 인증서 파일을 찾은 후 해당 파일을 추가합니다. 인증서는 암호화되지 않아야 합니다. CA 서명 인증서인 경우에는 인증서 - 중간 - 루트 순서로 전체 체인을 포함해야 합니다.

옵션	설명
개인 키	컴퓨터의 개인 키 파일을 찾은 후 해당 파일을 추가합니다.
암호	암호화된 경우 이 인증서에 대한 암호를 추가합니다. 이 릴리스에서는 암호화된 인증서가 지원되지 않기 때문에 이 필드가 사용되지 않습니다.
설명	이 인증서에 포함된 내용의 설명을 입력합니다.
서비스 인증서	서비스(예: 로드 밸런서 및 VPN)에 이 인증서를 사용하려면 예로 설정합니다. 이 인증서가 NSX Manager 노드용인 경우 아니오 로 설정합니다.

4 가져오기를 클릭합니다.

인증서 서명 요청 파일 생성

CSR(인증서 서명 요청)은 조직 이름, 일반 이름, 구/군/시 및 국가/지역과 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 국가/지역을 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 **시스템 > 인증서**를 선택합니다.
- 3 **CSR** 탭을 클릭합니다.
- 4 **CSR 생성**을 클릭합니다.
- 5 CSR 파일 세부 정보 입력을 완료합니다.

옵션	설명
이름	인증서에 이름을 할당합니다.
일반 이름	서버의 FQDN(정규화된 도메인 이름)을 입력합니다. 예: test.vmware.com
조직 이름	해당 접미사를 포함하여 조직 이름을 입력합니다. 예: VMware Inc.
조직 구성 단위	이 인증서를 처리하는 조직의 부서를 입력합니다. 예: IT 부서
인접성	조직이 위치한 구/군/시를 추가합니다. 예: Palo Alto
상태	조직이 위치한 시/도를 추가합니다. 예: California

옵션	설명
국가/지역	조직이 위치한 국가/지역을 추가합니다. 예: US(United States)
메시지 알고리즘	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.
키 크기	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.
설명	나중에 이 인증서를 식별하는 데 도움이 되는 특정 세부 정보를 입력합니다.

6 생성을 클릭합니다.

사용자 지정 CSR이 링크로 표시됩니다.

7 CSR을 선택하고 작업을 클릭합니다.

8 드롭다운 메뉴에서 CSR PEM 다운로드를 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 사용자에 게 전송합니다. 또한 CA는 사용자에게 루트 CA 인증서도 전송합니다.

CA 인증서 가져오기

서명된 CA 인증서를 가져올 수 있습니다. 가져오기 및 활성화 후에는 해당 CA에서 서명한 다른 인증서를 NSX-T Data Center에서 신뢰합니다.

RSA 기반 인증서만 지원됩니다.

사전 요구 사항

CA 인증서를 사용할 수 있는지 확인합니다.

절차

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

3 가져오기 > CA 인증서 가져오기를 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.
서비스 인증서	서비스(예: 로드 밸런서 및 VPN)에 이 인증서를 사용하려면 예로 설정합니다. 이 인증서가 NSX Manager 노드용인 경우 아니오 로 설정합니다.

4 가져오기를 클릭합니다.

자체 서명된 인증서 생성

자체 서명된 인증서를 생성할 수 있습니다. 하지만 자체 서명된 인증서 사용은 신뢰할 수 있는 인증서 사용보다 보안 수준이 낮습니다.

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 생성의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 시스템 > 인증서를 선택합니다.
- 3 CSR 탭을 클릭합니다.
- 4 CSR을 선택합니다.
- 5 작업 > CSR에 대한 자체 서명된 인증서를 선택합니다.
- 6 자체 서명된 인증서가 유효한 일 수를 입력합니다.
기본값은 10년입니다.
- 7 추가를 클릭합니다.

결과

자체 서명된 인증서는 인증서 탭에 표시됩니다.

NSX Manager 노드 또는 NSX Manager 클러스터 가상 IP에 대한 인증서 바꾸기

API를 호출하여 관리자 노드 또는 관리자 클러스터 VIP(가상 IP)에 대한 인증서를 바꿀 수 있습니다.

NSX-T Data Center를 설치하면 관리자 노드 및 클러스터에 자체 서명된 인증서가 생깁니다. 보안을 강화하려면 자체 서명된 인증서를 CA 서명 인증서로 바꾸고 각 노드에 대해 다른 인증서를 사용하는 것이 좋습니다.

사전 요구 사항

NSX Manager에서 인증서를 사용할 수 있는지 확인합니다. [인증서 가져오기](#)의 내용을 참조하십시오.

절차

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

2 **시스템 > 인증서**를 선택합니다.

3 ID 열에서 사용하려는 인증서의 ID를 클릭하고 팝업 창에서 인증서 ID를 복사합니다.
이 인증서를 가져올 때 옵션 **서비스 인증서**가 **아니오**로 설정되었는지 확인합니다.

4 관리자 노드의 인증서를 바꾸려면 `POST /api/v1/node/services/http?action=apply_certificate` API 호출을 사용하십시오. 예를 들면 다음과 같습니다.

```
POST https://<nsx-mgr>/api/v1/node/services/http?
action=apply_certificate&certificate_id=e61c7537-3090-4149-b2b6-19915c20504f
```

참고: 인증서 체인은 '인증서 - 중간 - 루트'의 업계 표준 순서여야 합니다.

API에 대한 자세한 내용은 "[NSX-T Data Center API 참조](#)"를 참조하십시오.

5 관리자 클러스터 VIP의 인증서를 바꾸려면 `POST /api/v1/cluster/api-certificate?action=set_cluster_certificate` API 호출을 사용하십시오. 예를 들면 다음과 같습니다.

```
POST https://<nsx-mgr>/api/v1/cluster/api-certificate?
action=set_cluster_certificate&certificate_id=d60c6a07-6e59-4873-8edb-339bf75711ac
```

참고: 인증서 체인은 '인증서 - 중간 - 루트'의 업계 표준 순서여야 합니다.

API에 대한 자세한 내용은 "[NSX-T Data Center API 참조](#)"를 참조하십시오. 이 단계는 VIP를 구성하지 않은 경우에는 필요하지 않습니다.

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 **시스템 > 인증서**를 선택합니다.
- 3 **CRL** 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 <pre>-----BEGIN X509 CRL----- MIIBODCB4zANBgkqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTEMMaOGA1 UECBMD UUxEMRkwFwYDVQQKExBNaW5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUz EbMBkG A1UEAxMSU1NMZWF5IGRlbW8gc2VydmVyFw0wMTAxMTUxNjI2NTdaFw0wMT AyMTQx NjI2NTdaMFwiEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEwMT AwMDBa MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA 0GCSqG S1b3DQEBAUAA0EAHPjQ3M93QOj8Ufi+jZM7Y78TfAzG4jJn/ E6MYBPFVQFYc/Gp UZexfjSVo5CIyyS0tYscz8o07avwBxTiMpDEQg== -----END X509 CRL--</pre>
설명	이 CRL에 포함된 항목의 요약을 입력합니다.

- 5 **가져오기**를 클릭합니다.

결과

가져온 CRL이 링크로 나타납니다.

인증서 해지 목록을 검색하도록 NSX Manager 구성

API를 사용하여 CRL(인증서 해지 목록)을 검색하도록 NSX Manager를 구성할 수 있습니다. 그런 다음, CA(인증 기관) 대신 NSX Manager에 대한 API를 호출하여 CRL을 확인할 수 있습니다.

이 기능에는 다음과 같은 장점이 있습니다.

- 서버, 즉 NSX Manager에서 CRL을 좀 더 효율적으로 캐시할 수 있습니다.
- 클라이언트는 CA(인증 기관)로 임의의 아웃바운드 연결을 생성할 필요가 없습니다.

인증서 해지 목록과 관련된 다음 API를 사용할 수 있습니다.

```
GET /api/v1/trust-management
GET /api/v1/trust-management/crl-distribution-points
POST /api/v1/trust-management/crl-distribution-points
DELETE /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
GET /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
PUT /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
GET /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>/status
POST /api/v1/trust-management/crl-distribution-points/pem-file
```

CRL 분포 지점을 관리하고 NSX Manager에 저장된 CRL을 검색할 수 있습니다. 자세한 내용은 "NSX-T Data Center API 참조" 를 참조하십시오.

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 생성의 내용을 참조하십시오.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 **시스템 > 인증서**를 선택합니다.
- 3 **CSR** 탭을 클릭합니다.
- 4 CSR을 선택합니다.
- 5 **작업 > CSR에 대한 인증서 가져오기**를 선택합니다.
- 6 컴퓨터의 서명된 인증서 파일을 찾은 후 해당 파일을 추가합니다.
- 7 **추가**를 클릭합니다.

결과

자체 서명된 인증서는 **인증서** 탭에 표시됩니다.

공용 인증서 및 개인 키 스토리지

공용 인증서 및 개인 키는 NSX Manager에 저장됩니다. 개인 키가 필요한 로드 밸런서 또는 VPN 서비스가 생성되면 NSX Manager가 로드 밸런서 또는 VPN 서비스가 실행 중인 Edge 노드로 개인 키의 복사본을 전송합니다.

규정 준수 기반 구성

FIPS 호환 모드에서 실행하려면 FIPS 140-2 검증 암호화 모듈을 사용하도록 NSX-T Data Center를 구성할 수 있습니다. 모듈은 NIST CMVP(암호화 모듈 검증 프로그램)를 통해 FIPS 140-2 표준으로 검증됩니다.

FIPS 규정 준수에 대한 모든 예외는 규정 준수 보고서를 사용하여 검색할 수 있습니다. 자세한 내용은 [준수 상태 보고서 보기](#) 항목을 참조하십시오.

다음의 검증된 모듈은 NSX-T Data Center 2.5에서 사용됩니다.

- VMware OpenSSL FIPS 개체 모듈 버전 2.0.9: [인증서 #2839](#)
- VMware OpenSSL FIPS 개체 모듈 버전 2.0.20-vmw: [인증서 #3550](#)
- BC-FJA(Bouncy Castle FIPS Java API) 버전 1.0.1: [인증서 #3152](#)
- VMware의 IKE 암호화 모듈 버전 1.1.0: [인증서 #3435](#)
- VMware의 VPN 암호화 모듈 버전 1.0: [인증서 #3542](#)

<https://www.vmware.com/security/certifications/fips.html>에서 VMware가 FIPS 140-2 표준에 부합하는지 검증한 암호화 모듈에 대한 자세한 정보를 확인할 수 있습니다.

기본적으로 로드 밸런서는 FIPS 모드가 꺼져 있는 모듈을 사용합니다. 로드 밸런서에 사용되는 모듈에 대해 FIPS 모드를 켤 수 있습니다. 자세한 내용은 로드 밸런서에 대한 [글로벌 FIPS 규정 준수 모드 구성](#) 항목을 참조하십시오.

준수 상태 보고서 보기

NSX-T Data Center 기능에 대한 규정 준수 보고서를 볼 수 있습니다. 이 보고서를 사용하여 IT 정책 및 업계 표준을 준수하도록 NSX-T Data Center 환경을 구성할 수 있습니다.

규정 준수 보고서에는 각 규정 미준수 구성에 대한 정보가 포함되어 있습니다.

표 21-8. 규정 준수 보고서 정보

규정 준수 보고서 열	설명	Example
규정 미준수 코드	규정 미준수 유형을 식별하는 코드입니다.	72301
설명	규정 미준수 유형에 대한 설명입니다.	CA가 서명한 인증서가 아닙니다.
리소스 이름	영향을 받는 리소스의 이름 또는 ID입니다.	nsx-manager-1
리소스 유형	영향을 받는 리소스의 유형입니다.	CertificateComplianceReporter
영향을 받는 리소스	영향을 받는 리소스 수입니다. 규정 미준수 구성이 있는 경우 이 개수는 0일 수 있지만 해당 기능은 사용되지 않습니다.	1

API: GET /policy/api/v1/compliance/status를 사용하여 보고서를 검색할 수도 있습니다.

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 홈 페이지에서 **모니터링 대시보드 > 규정 준수 보고서** 를 클릭합니다.

규정 준수 상태 보고서 코드

규정 준수 상태 보고서의 의미에 대한 자세한 정보를 확인할 수 있습니다.

표 21-9. 규정 준수 보고서 코드

코드	설명	규정 준수 상태 소스	수정
72001	암호화가 사용되지 않도록 설정되어 있습니다.	이 상태는 VPN IPSec 프로파일 구성에 NO_ENCRYPTION, NO_ENCRYPTION_AUTH_AES_GMAC_128, NO_ENCRYPTION_AUTH_AES_GMAC_192 또는 NO_ENCRYPTION_AUTH_AES_GMAC_256 encryption_algorithms가 포함된 경우에 보고됩니다. 이 상태는 보고된 규정 미준수 구성을 사용하는 IPSec VPN 세션 구성에 영향을 미칩니다.	이 상태를 업데이트하려면 준수 암호화 알고리즘을 사용하는 VPN IPSec 프로파일을 추가하고 모든 VPN 구성에서 해당 프로파일을 사용하십시오. IPSec 프로파일 추가 항목을 참조하십시오.
72011	인접 네트워크가 있는 BGP 메시지가 무결성 검사를 우회합니다. 메시지 인증이 정의되지 않았습니다.	이 상태는 BGP 인접 네트워크에 대해 암호가 구성되지 않은 경우에 보고됩니다. 이 상태는 BGP 인접 네트워크 구성에 영향을 줍니다.	이 상태를 업데이트하려면 BGP 인접 네트워크에서 암호를 구성하고 해당 암호를 사용하도록 Tier-0 게이트웨이 구성을 업데이트하십시오. BGP 구성 항목을 참조하십시오.
72012	BGP 인접 네트워크와의 통신에 약한 무결성 검사가 사용됩니다. MD5가 메시지 인증에 사용됩니다.	이 상태는 BGP 인접 네트워크 암호에 MD5 인증이 사용되는 경우에 보고됩니다. 이 상태는 BGP 인접 네트워크 구성에 영향을 줍니다.	NSX-T Data Center에서는 BGP에 대해 MD5 인증만 지원하므로 사용할 수 있는 업데이트 방법이 없습니다.

표 21-9. 규정 준수 보고서 코드 (계속)

코드	설명	규정 준수 상태 소스	수정
72021	보안 소켓 연결을 설정하는 데 SSLv3가 사용됩니다. TLSv 1.1 이상을 실행하고 프로토콜 약점이 있는 SSLv3를 완전히 사용하지 않도록 설정하는 것이 좋습니다.	이 상태는 SSLv3가 로드 밸런서 클라이언트 SSL 프로파일, 로드 밸런서 서버 SSL 프로파일 또는 로드 밸런서 HTTPS 모니터에 구성된 경우에 보고됩니다. 이 상태는 다음 구성에 영향을 줍니다. <ul style="list-style-type: none"> ■ HTTPS 모니터에 연결된 로드 밸런서 풀. ■ 로드 밸런서 클라이언트 SSL 프로파일 또는 서버 SSL 프로파일에 연결된 로드 밸런서 가상 서버. 	이 상태를 업데이트하려면 TLS 1.1 이상을 사용하도록 SSL 프로파일을 구성하고 모든 로드 밸런서 구성에서 이 프로파일을 사용하십시오. SSL 프로파일 추가 항목을 참조하십시오.
72022	보안 소켓 연결을 설정하는 데 TLSv1.0가 사용됩니다. TLSv 1.1 이상을 실행하고 프로토콜 약점이 있는 TLSv1.0를 완전히 사용하지 않도록 설정하는 것이 좋습니다.	이 상태는 TLSv1.0가 로드 밸런서 클라이언트 SSL 프로파일, 로드 밸런서 서버 SSL 프로파일 또는 로드 밸런서 HTTPS 모니터에 구성된 경우에 보고됩니다. 이 상태는 다음 구성에 영향을 줍니다. <ul style="list-style-type: none"> ■ HTTPS 모니터에 연결된 로드 밸런서 풀. ■ 로드 밸런서 클라이언트 SSL 프로파일 또는 서버 SSL 프로파일에 연결된 로드 밸런서 가상 서버. 	이 상태를 업데이트하려면 TLS 1.1 이상을 사용하도록 SSL 프로파일을 구성하고 모든 로드 밸런서 구성에서 이 프로파일을 사용하십시오. SSL 프로파일 추가 항목을 참조하십시오.
72023	취약한 Diffie-Hellman 그룹이 사용됩니다.	이 오류는 VPN IPsec 프로파일 또는 VPN IKE 프로파일 구성에 다음과 같은 Diffie-Hellman 그룹(2, 5, 14, 15 또는 16)이 포함된 경우에 보고됩니다. 그룹 2와 5는 약한 Diffie-Hellman 그룹입니다. 그룹 14, 15 및 16은 약한 그룹이 아니지만 FIPS 규격이 아닙니다. 이 상태는 보고된 규정 미준수 구성을 사용하는 IPsec VPN 세션 구성에 영향을 미칩니다.	이 상태를 업데이트하려면 Diffie-Hellman 그룹 19, 20 또는 21을 사용하도록 VPN 프로파일을 구성하십시오. 프로파일 추가 항목을 참조하십시오.

표 21-9. 규정 준수 보고서 코드 (계속)

코드	설명	규정 준수 상태 소스	수정
72024	로드 밸런서 FIPS 글로벌 설정이 사용하지 않도록 설정되었습니다.	이 오류는 로드 밸런서 FIPS 글로벌 설정이 사용하지 않도록 설정된 경우에 보고됩니다. 이 상태는 모든 로드 밸런서 서비스에 영향을 미칩니다.	이 상태를 업데이트하려면 로드 밸런서에 FIPS를 사용하도록 설정하십시오. 로드 밸런서에 대한 글로벌 FIPS 규정 준수 모드 구성 항목을 참조하십시오.
72200	실제 엔트로피가 충분하지 않습니다.	이 상태는 의사 난수 생성기가 하드웨어 생성 엔트로피에 의존하는 것이 아니라 엔트로피를 생성하는 데 사용될 때 보고됩니다. NSX Manager 노드에 충분한 실제 엔트로피를 생성하는 데 필요한 하드웨어 가속화 지원이 없기 때문에 하드웨어 생성 엔트로피가 사용되지 않습니다.	이 상태를 업데이트하려면 최신 하드웨어를 사용하여 NSX Manager 노드를 실행해야 할 수 있습니다. 대부분의 최신 하드웨어는 이 기능을 지원합니다. 참고 기본 인프라가 가상인 경우 실제 엔트로피를 얻을 수 없습니다.
72201	엔트로피 소스를 알 수 없습니다.	이 상태는 표시된 노드에 사용할 수 있는 엔트로피 상태가 없을 때 보고됩니다.	이 상태를 업데이트하려면 표시된 노드가 제대로 작동하고 있는지 확인하십시오.
72301	CA가 서명한 인증서가 아닙니다.	이 상태는 NSX Manager 인증서 중 하나가 CA 서명 인증서가 아닐 때 보고됩니다. NSX Manager는 다음과 같은 인증서를 사용합니다. <ul style="list-style-type: none"> ■ Syslog 인증서. ■ 개별 NSX Manager 노드에 대한 API 인증서. ■ NSX Manager VIP에 사용되는 클러스터 인증서. 	이 상태를 업데이트하려면 CA 서명 인증서를 설치하십시오. 인증서 설정 항목을 참조하십시오.

로드 밸런서에 대한 글로벌 FIPS 규정 준수 모드 구성

로드 밸런서의 FIPS 규정 준수에 대한 글로벌 설정이 있습니다. 기본적으로 이 설정은 성능을 향상시키기 위해 꺼집니다.

로드 밸런서의 FIPS 규정 준수에 대한 글로벌 구성을 변경하면 새 로드 밸런서 인스턴스에 영향을 주지만 기존 로드 밸런서 인스턴스에는 영향을 주지 않습니다.

로드 밸런서의 FIPS에 대한 글로벌 설정(lb_fips_enabled)을 *true*로 설정하면 새 로드 밸런서 인스턴스가 FIPS 140-2를 준수하는 모듈을 사용합니다. 기존 로드 밸런서 인스턴스는 비준수 모듈을 사용 중일 수 있습니다.

기존 로드 밸런서에 변경 내용을 적용하려면 Tier-1 게이트웨이에서 로드 밸런서를 분리했다가 다시 연결해야 합니다.

GET /policy/api/v1/compliance/status 사용으로 로드 밸런서의 글로벌 FIPS 규정 준수 상태를 확인할 수 있습니다.

```

...
{
  "non_compliance_code": 72024,
  "description": "Load balancer FIPS global setting is disabled.",
  "reported_by": {
    "target_id": "971ca477-df1a-4108-8187-7918c2f8c3ba",
    "target_display_name": "971ca477-df1a-4108-8187-7918c2f8c3ba",
    "target_type": "FipsGlobalConfig",
    "is_valid": true
  },
  "affected_resources": [
    {
      "path": "/infra/lb-services/LB_Service",
      "target_id": "/infra/lb-services/LB_Service",
      "target_display_name": "LB_1",
      "target_type": "LBService",
      "is_valid": true
    }
  ]
},
...

```

참고 규정 준수 보고서에는 로드 밸런서의 FIPS 규정 준수에 대한 글로벌 설정이 표시됩니다. 지정된 모든 로드 밸런서 인스턴스에 글로벌 설정과 다른 FIPS 규정 준수 상태가 지정되어 있을 수 있습니다.

절차

- 1 로드 밸런서의 글로벌 FIPS 설정을 검색합니다.

GET https://nsx-mgr1/policy/api/v1/infra/global-config

응답 본문의 예:

```

{
  "fips": {
    "lb_fips_enabled": false
  },
  "resource_type": "GlobalConfig",
  "id": "global-config",
  "display_name": "global-config",
  "path": "/infra/global-config",
  "relative_path": "global-config",
  "marked_for_delete": false,
  "_create_user": "system",
  "_create_time": 1561225479619,
  "_last_modified_user": "admin",
  "_last_modified_time": 1561937915337,

```

```

    "_system_owned": true,
    "_protection": "NOT_PROTECTED",
    "_revision": 2
  }

```

2 로드 밸런서의 글로벌 FIPS 설정을 변경합니다.

글로벌 설정은 새 로드 밸런서 인스턴스를 생성할 때 사용됩니다. 이 설정을 변경해도 기존 로드 밸런서 인스턴스에는 영향을 주지 않습니다.

PUT <https://nsx-mgr1/policy/api/v1/infra/global-config>

요청 본문 예:

```

{
  "fips": {
    "lb_fips_enabled": true
  },
  "resource_type": "GlobalConfig",
  "_revision": 2
}

```

응답 본문의 예:

```

{
  "fips": {
    "lb_fips_enabled": true
  },
  "resource_type": "GlobalConfig",
  "id": "global-config",
  "display_name": "global-config",
  "path": "/infra/global-config",
  "relative_path": "global-config",
  "marked_for_delete": false,
  "_create_user": "system",
  "_create_time": 1561225479619,
  "_last_modified_user": "admin",
  "_last_modified_time": 1561937960950,
  "_system_owned": true,
  "_protection": "NOT_PROTECTED",
  "_revision": 3
}

```

3 기존 로드 밸런서 인스턴스에 이 글로벌 설정을 사용하려면 로드 밸런서를 Tier-1 게이트웨이에서 분리했다가 다시 연결해야 합니다.

경고 Tier-1 게이트웨이에서 로드 밸런서를 분리하면 로드 밸런서 인스턴스에 대한 트래픽이 중단됩니다.

a **네트워킹 > 로드 밸런싱**로 이동합니다.

b 분리하려는 로드 밸런서에서 3개 점 메뉴(**⋮**)를 클릭한 다음, **편집**을 클릭합니다.

- c  을 클릭한 다음, **저장**을 클릭하여 로드 밸런서를 Tier-1 게이트웨이에서 분리합니다.



- d 3개 점 메뉴 (...)를 클릭한 다음, **편집**을 클릭합니다.
- e **Tier-1 게이트웨이** 드롭다운 메뉴에서 올바른 게이트웨이를 선택한 다음, **저장**을 클릭하여 로드 밸런서를 Tier-1 게이트웨이에 다시 연결합니다.

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 **시스템 > 지원 번들**을 선택합니다.
- 3 대상 노드를 선택합니다.
사용 가능한 노드 유형은 **관리 노드**, **Edge**, **호스트** 및 **공용 클라우드 게이트웨이**입니다.
- 4 (선택 사항) 로그 수명(일)을 지정하여 지정된 일 수보다 오래된 로그를 제외합니다.
- 5 (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.

- 6 (선택 사항) 확인란을 선택하여 번들을 원격 파일 서버에 업로드합니다.
- 7 **번들 수집 시작**을 클릭하여 지원 번들 수집을 시작합니다.
존재하는 로그 파일의 개수에 따라 노드마다 몇 분 정도 걸릴 수 있습니다.
- 8 수집 프로세스 상태를 모니터링합니다.
상태 탭에 지원 번들 수집에 대한 진행률이 표시됩니다.

- 9 번들을 파일 원격 서버로 전송하는 옵션이 설정되지 않은 경우 **다운로드**를 클릭하여 번들을 다운로드합니다.

디스크 공간이 충분하지 않으면 관리자 노드에 대한 번들 수집이 실패할 수 있습니다. 오류가 발생하는 경우 실패한 노드에 이전 지원 번들이 있는지 확인합니다. 해당 IP 주소를 사용하여 실패한 관리자 노드의 NSX Manager UI에 로그인하고 해당 노드에서 번들 수집을 시작합니다. NSX Manager에서 메시지가 표시되면 이전 번들을 다운로드하거나 삭제합니다.

로그 메시지 및 오류 코드

NSX-T Data Center 구성 요소는 디렉터리 /var/log의 로그 파일에 씁니다. NSX-T 장치 및 KVM 호스트에서 NSX syslog 메시지는 RFC 5424를 준수합니다. ESXi 호스트에서 syslog 메시지는 RFC 3164를 준수합니다.

로그 보기

NSX-T 장치 syslog 메시지는 /var/log/syslog에 있습니다. KVM 호스트에서 syslog 메시지는 /var/log/vmware/nsx-syslog에 있습니다.

NSX-T 장치에서 다음 NSX-T CLI 명령을 실행하여 로그를 확인할 수 있습니다.

```
get log-file <auth.log | controller | controller-error | http.log | kern.log | manager.log |
node-mgmt.log | policy.log | syslog> [follow]
```

로그 파일은 다음과 같습니다.

이름	설명
auth.log	권한 부여 로그
컨트롤러	컨트롤러 로그
controller-error	컨트롤러 오류 로그
http.log	HTTP 서비스 로그
kern.log	커널 로그
manager.log	Manager Service 로그
node-mgmt.log	노드 관리 로그
policy.log	정책 서비스 로그
syslog	시스템 로그

하이퍼바이저에서 tac, tail, grep 및 more와 같은 Linux 명령을 사용하여 로그를 확인할 수 있습니다.

모든 syslog 메시지에는 메시지의 소스를 식별하는 데 도움이 되는 구성 요소(comp) 및 하위 구성 요소(subcomp) 정보가 있습니다.

NSX-T Data Center는 숫자 값이 22인 시설 local6을 포함하는 로그를 생성합니다.

감사 로그는 `syslog`의 일부입니다. 감사 로그 메시지는 `structured-data` 필드의 `audit="true"` 문자열로 식별할 수 있습니다. 예:

```
<182>1 2020-05-05T00:29:02.900Z nsx-manager1 NSX 14389 - [nsx@6876 audit="true" comp="nsx-manager" level="INFO" reqId="fe75651d-c3e7-4680-8753-9ae9d92d7f0c" subcomp="policy" username="admin"] UserName="admin", ModuleName="AAA", Operation="GetCurrentUserInfo", Operation status="success"
```

각 API 호출은 하나의 감사 로그 메시지를 생성합니다. 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 5424 및 RFC 3164는 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.

로그 메시지 형식

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.
```

오류 코드

오류 코드 목록을 보려면 기술 자료 문서 [71077 NSX-T Data Center 2.x 오류 코드](#)를 참조하십시오.

원격 로깅 구성

원격 로그 서버로 로그 메시지를 전송하도록 NSX-T Data Center 장치 및 하이퍼바이저를 구성할 수 있습니다.

원격 로깅은 NSX Manager, 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

- CLI 명령 `set logging-server` 사용을 숙지하십시오. 자세한 내용은 "NSX-T CLI 참조" 를 참조하십시오.
- NSX CLI에서 프로토콜 TLS 또는 LI-TLS를 사용하여 로그 서버에 대한 보안 연결을 구성하는 경우 서버 및 클라이언트 인증서를 각 NSX-T Data Center 장치의 /image/vmware/nsx/file-store에 저장해야 합니다. 파일 저장소의 인증서는 NSX CLI에서 내보내기 기능을 구성한 경우에만 필요합니다. API를 사용하는 경우 파일 저장소를 사용할 필요가 없습니다. syslog 내보내기 구성을 완료한 후 잠재적인 보안 취약점을 방지하기 위해 이 위치에서 모든 인증서와 키를 삭제해야 합니다.
- 로그 서버에 대한 보안 연결을 구성하려면 서버가 CA 서명 인증서로 구성되어 있는지 확인합니다. 예를 들어, Log Insight 서버 `vrli.prome.local`을 로그 서버로 사용하는 경우 클라이언트에서 다음 명령을 실행하여 서버의 인증서 체인을 볼 수 있습니다.

```
root@caserver:~# echo -n | openssl s_client -connect vrli.prome.local:443 | sed -ne '/
^Certificate chain/,/^---/p'
depth=2 C = US, L = California, O = GS, CN = Orange Root Certification Authority
verify error:num=19:self signed certificate in certificate chain
Certificate chain
 0 s:/C=US/ST=California/L=HTG/O=GSS/CN=vrli.prome.local
  i:/C=US/L=California/O=GS/CN=Green Intermediate Certification Authority
 1 s:/C=US/L=California/O=GS/CN=Green Intermediate Certification Authority
  i:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
 2 s:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
  i:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
---
DONE
```

절차

- 1 NSX-T Data Center 장치에서 원격 로깅을 구성하려면 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>] [serverca <filename>] [clientca <filename>] [certificate <filename>] [key <filename>] [structured-data <structured-data>]
```

명령을 여러 번 실행하여 여러 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
```

원격 서버에 감사 로그만 전달하려면 structured-data 매개 변수에 audit="true"를 지정합니다. 예:

```
set logging-server <server-ip> proto udp level info structured-data audit="true"
```

- 2 프로토콜 LI-TLS를 사용하여 보안 원격 로깅을 구성하려면 proto li-tls 매개 변수를 지정합니다. 예:

```
set logging-server vrl1.prome.local proto li-tls level info messageid SWITCHING,ROUTING,FABRIC,SYSTEM,POLICY,HEALTHCHECK,SHA,MONITORING serverca intermed-ca-full-chain.crt
```

구성이 성공하면 텍스트 없이 메시지가 표시됩니다. 서버 인증서 체인(다음에 루트 인증서가 있는 중간 인증서임)의 콘텐츠를 보려면 root로 로그인하고 다음 명령을 실행합니다.

```
root@nsx1:~# keytool -printcert -file /image/vmware/nsx/file-store/intermed-ca-full-chain.crt
Certificate[1]:
Owner: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd2
Valid from: Sun Mar 15 00:00:00 UTC 2020 until: Mon Mar 17 00:00:00 UTC 2025
Certificate fingerprints:
  MD5: 94:C8:9F:92:56:60:EB:DB:ED:4B:11:17:33:27:C0:C9
  SHA1: 42:9C:3C:51:E8:8E:AC:2E:5E:62:95:82:D7:22:E0:FB:08:B8:64:29
  SHA256:
58:B8:63:3D:0C:34:35:39:FC:3D:1E:BA:AA:E3:CE:A9:C0:F3:58:53:1F:AD:89:A5:01:0D:D3:89:9E:7B:C5:69
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[2]:
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
```

```
Certificate fingerprints:
  MD5:  ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
  SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
  SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
```

성공 및 실패 조건 모두에 대한 로그는 /var/log/loginsight-agent/liagent_2020-MM-DD-
<file-num>.log에 있습니다. 구성이 성공하면 다음 명령을 사용하여 Log Insight 구성을 볼 수 있
습니다.

```
root@nsx1:/image/vmware/nsx/file-store# cat /var/lib/loginsight-agent/liagent-effective.ini
; Dynamic file representing the effective configuration of VMware Log Insight Agent
(merged server-side and client-side configuration)
; DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
; Creation time: 2020-03-22T19:41:21.648800

[server]
hostname=vrl1.prome.local
proto=cfapi
ssl=yes
ssl_ca_path=/config/vmware/nsx-node-api/syslog/bb466082-996f-4d77-b6e3-1fa93f4a20d4_ca.pem
ssl_accept_any_trusted=yes
port=9543
filter={filelog; nsx-syslog; pri_severity <= 6 and ( msgid == "SWITCHING" or msgid ==
"ROUTING" or msgid == "FABRIC" or msgid == "SYSTEM" or msgid == "POLICY" or msgid ==
"HEALTHCHECK" or msgid == "SHA" or msgid == "MONITORING" )}

[filelog|nsx-syslog]
directory=/var/log
include=syslog;syslog.*
parser=nsx-syslog_parser

[parser|nsx-syslog_parser]
base_parser=syslog
extract_sd=yes

[update]
auto_update=no
```

- 3 프로토콜 TLS를 사용하여 보안 원격 로깅을 구성하려면 proto tls 매개 변수를 지정합니다. 예:

```
set logging-server vrl1.prome.local proto tls level info serverca Orange-CA.crt.pem
clientca Orange-CA.crt.pem certificate gc-nsxt-mgr-full.crt.pem key gc-nsxt-mgr.key.pem
```

다음에 유의하십시오.

- serverCA 매개 변수의 경우, 전체 체인이 아닌 루트 인증서만 필요합니다.
- clientCA가 serverCA와 다른 경우 루트 인증서만 필요합니다.

- 인증서는 NSX Manager의 전체 체인을 포함해야 합니다(NDcPP 준수 - EKU, BASIC 및 CDP여야 함(CDP - 이 검사를 무시할 수 있음))

각 인증서의 콘텐츠를 검사할 수 있습니다. 예:

```

root@gc3:~# keytool -printcert -file /image/vmware/nsx/file-store/Orange-CA.crt.pem
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e7226e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
    MD5: ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
    SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
    SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
root@gc3:~#

root@gc3:/image/vmware/nsx/file-store# keytool -printcert -file gc-nsxt-mgr-full.crt.pem
Certificate[1]:
Owner: CN=gc.prome.local, O=GS, L=HTG, ST=California, C=US
Issuer: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Serial number: bdf43ab31340b87f323b438a2895a075
Valid from: Mon Mar 16 07:26:51 UTC 2020 until: Wed Mar 16 07:26:51 UTC 2022
Certificate fingerprints:
    MD5: 36:3C:1F:57:96:07:84:C0:6D:B7:33:9A:8D:25:4D:27
    SHA1: D1:4E:F9:45:2D:0D:34:79:D2:B4:FA:65:28:E0:5C:DC:74:50:CA:3B
    SHA256:
3C:FF:A9:5D:AA:68:44:44:DD:07:2F:DD:E2:BE:9C:32:19:7A:03:D5:26:8D:5F:AD:56:CA:D2:6C:91:96:2
7:6F
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[2]:
Owner: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e7226e7fbb3b0a7a6b4edd767f867fd2
Valid from: Sun Mar 15 00:00:00 UTC 2020 until: Mon Mar 17 00:00:00 UTC 2025
Certificate fingerprints:
    MD5: 94:C8:9F:92:56:60:EB:DB:ED:4B:11:17:33:27:C0:C9
    SHA1: 42:9C:3C:51:E8:8E:AC:2E:5E:62:95:82:D7:22:E0:FB:08:B8:64:29
    SHA256:
58:B8:63:3D:0C:34:35:39:FC:3D:1E:BA:AA:E3:CE:A9:C0:F3:58:53:1F:AD:89:A5:01:0D:D3:89:9E:7B:C
5:69
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[3]:
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e7226e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045

```

Certificate fingerprints:

```

MD5: ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

```

/var/log/syslog의 성공적인 로그인 예::

```

<182>1 2020-03-22T21:54:34.501Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created CA PEM file /
config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_ca.pem for logging
server vrli.prome.local:6514
<182>1 2020-03-22T21:54:36.269Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created client CA PEM
file /config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_client_ca.pem
for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:54:36.495Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert issuer = /C=US/L=California/O=GS/
CN=Green IntermediateCertification Authority
<182>1 2020-03-22T21:54:36.514Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert subject = /C=US/ST=California/L=HTG/
O=GS/CN=gc.promelocal
<182>1 2020-03-22T21:54:36.539Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] certificate trust check succeeded.
status: 200, result: {'status': 'OK'}
<182>1 2020-03-22T21:54:36.612Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] Certificate already exists, skip import
<182>1 2020-03-22T21:54:37.322Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created certificate PEM
file /config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_cert.pem for
logging server vrli.prome.local:6514
<182>1 2020-03-22T21:54:38.020Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created key PEM file /
config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_key.pem for logging
server vrli.prome.local:6514

```

/var/log/syslog의 로깅 실패의 예::

```

<182>1 2020-03-22T21:33:30.424Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created client CA PEM
file /config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_client_ca.pem
for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:33:30.779Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert issuer = /C=US/L=California/O=GS/
CN=Green IntermediateCertification Authority
<182>1 2020-03-22T21:33:30.803Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert subject = /C=US/ST=California/L=HTG/
O=GS/CN=gc.promelocal
<179>1 2020-03-22T21:33:30.823Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="ERROR" errorCode="NODE10"] Certificate trust

```

```

check failed. status:200, result: {'error_message': 'Certificate
CN=gc.prome.local,O=GS,L=HTG,ST=California,C=US was not verifiably signed by
CN=gc.prome.local,O=GS,L=HTG,ST=California,C=US: certificate does not verifywith supplied
key', 'status': 'ERROR'}
<179>1 2020-03-22T21:33:30.824Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="ERROR" errorCode="NODE10"] Failed to create
certificate PEM file config/vmware/nsx-node-api/syslog/
76332782-1ec6-483a-95d4-2adeaf2ef112_cert.pem for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:33:31.578Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully deleted CA PEM file /
config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_ca.pem
<182>1 2020-03-22T21:33:32.342Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully deleted client CA PEM
file /config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_ca.pem
<182>1 2020-03-22T21:33:32.346Z gc3.prome.local NSX 16698 - [nsx@6876 comp="nsx-cli"
subcomp="node-mgmt" username="admin" level="INFO" audit="true"] CMD: set logging-server
vrli.prome.local prototls level info serverca Orange-CA.crt.pem clientca Orange-CA.crt.pem
certifi
cate gc-nsxt-mgr.crt.pem key gc-nsxt-mgr.key.pem (duration: 6.365s), Operation status:
CMD_EXECUTED

```

인증서 및 개인 키가 다음 명령과 일치하는지 확인할 수 있습니다. 일치하는 경우 출력은 RSA 키를 작성합니다. 다른 출력은 일치하지 않음을 의미합니다. 예:

```

root@caserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/gc-nsxt-mgr.key.pem -pubout)
writing RSA key

```

손상된 개인 키의 예:

```

root@caserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/gc-nsxt-mgr-corrupt.key.pem -pubout)
unable to load Private Key
140404188370584:error:0D07209B:asn1 encoding routines:ASN1_get_object:too
long:asn1_lib.c:147:
140404188370584:error:0D068066:asn1 encoding routines:ASN1_CHECK_TLEN:bad object
header:tasn_dec.c:1205:
140404188370584:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1
error:tasn_dec.c:386:Type=RSA
140404188370584:error:04093004:rsa routines:OLD_RSA_PRIV_DECODE:RSA lib:rsa_ameth.c:119:
140404188370584:error:0D07209B:asn1 encoding routines:ASN1_get_object:too
long:asn1_lib.c:147:
140404188370584:error:0D068066:asn1 encoding routines:ASN1_CHECK_TLEN:bad object
header:tasn_dec.c:1205:
140404188370584:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1
error:tasn_dec.c:386:Type=PKCS8_PRIV_KEY_INFO
140404188370584:error:0907B00D:PEM routines:PEM_READ_BIO_PRIVATEKEY:ASN1
lib:pem_pkey.c:141:
1,14d0
< -----BEGIN PUBLIC KEY-----
< MIIICjANBgkqhkiG9w0BAQEFAAOCAg8AMIICGkKCAgEAv3yH7pZidfkLrEP3zVa9
< EcOKXlFFjkThZRZMfguenlm8s6QHYYVvuUX8IRB48Li3/DUfOj0bzaPWktpv+Q2P0
< N/j4LoX2RzjV/DPxYfLP6GMNMc21L3s9ruBeWUtthUP8khCwd2d2rZ09cUZV10P9
< kIYBb5RMFC7Z10Uth3bKdepEf+sXz3DaKZ/WySzYq9x86QDaA3ABO3Q0i7txBscI

```

```
< FvXuMDOMQaC3pPp9FWO6IPRAWB57wahLJv6K5qGIfwubSBFg53grT4snf11DZAhZ
< 9hz5JgGr80GVyWyb7rgigpl9iUWAZx8U9De9XoxmvBN5iEGTIuKGaEgICL176crb
< RMkhjnCqNHI+z6sQvpYJ7U0zZc72eBIWoHUKcWWk3eU6Oy4OiyW6jYuXG7hZY1ly
< nSkme3mZUWJKvcoX05+3zeCP623/HzE7X2sNyWFjzeF3XEvauZrIbsJh/xp2ShDa
< uKKEY0gUGhLtCa3TpV918d6tFWVy8XjVjdjoVt4s7MfUo/airVmRykfsWrKyNUOQ
< qRZvSbqjt8pm+3bSvKdXX4ul7ptPG2GF20ETWHPwj2JwQpGhR9zK8fsKzvm6hXi
< kq76zI4FefuVps3e1r39+0F+p6d6i2oUoo24sC1iSePTDhU74efVp6iv8HmnDgYX
< Ylm6Kusr0JT5TJFDfASmrj8CAwEAAQ==
< -----END PUBLIC KEY-----
```

유효하지만 서로를 위해 작성되지 않은 개인 키 및 인증서의 예:

```
root@caserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/vrli.key.pem -pubout)
writing RSA key
2,13c2,13
< MIIcIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAv3yH7pZidfkLrEP3zVa9
< EcOKX1FFjkThZRZMfguenlm8s6QHYYVvuUX8IRB48Li3/DUfOj0bzaPWktpv+Q2P0
< N/j4LoX2RzjV/DPxYfLP6GMNMc21L3s9ruBeWUtthtUP8khCwd2d2rZ09cUZV10P9
< kiYBb5RMFC7Z10UtH3bKdepEf+sXz3DaKZ/WySzYq9x86QDaA3ABO3Q0i7txBscI
< FvXuMDOMQaC3pPp9FWO6IPRAWB57wahLJv6K5qGIfwubSBFg53grT4snf11DZAhZ
< 9hz5JgGr80GVyWyb7rgigpl9iUWAZx8U9De9XoxmvBN5iEGTIuKGaEgICL176crb
< RMkhjnCqNHI+z6sQvpYJ7U0zZc72eBIWoHUKcWWk3eU6Oy4OiyW6jYuXG7hZY1ly
< nSkme3mZUWJKvcoX05+3zeCP623/HzE7X2sNyWFjzeF3XEvauZrIbsJh/xp2ShDa
< uKKEY0gUGhLtCa3TpV918d6tFWVy8XjVjdjoVt4s7MfUo/airVmRykfsWrKyNUOQ
< qRZvSbqjt8pm+3bSvKdXX4ul7ptPG2GF20ETWHPwj2JwQpGhR9zK8fsKzvm6hXi
< kq76zI4FefuVps3e1r39+0F+p6d6i2oUoo24sC1iSePTDhU74efVp6iv8HmnDgYX
< Ylm6Kusr0JT5TJFDfASmrj8CAwEAAQ==
---
> MIIcIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAqvsjay7+o7gCW7szT3ho
> bc34XX216u5J14/X/pUDI/YHmIf06bsZ1r/14bTL4Q7BM6+9MI6UYEE7DxUoINGO
> o4FEEQE32KWVFe3gw3homHU39q4pQjsJsxTcTE3oDMLIY0nWJ0PRUst3DdfyUH1L
> W0NUN9YdN+fa12Uf021iuDqVy9V8AH3ON6fu+QCA8nt71zkzeTxSA01dp12NA17F
> rD8rm05wxnV7WtuV7V8PstISiClzhHgZRM1+B0r300itnyAzEGLaRT3//PKfe00e
> HCdxGmlrUtMqxIItJahEsqvMufyqNYecVscyXLHPelizKCsQfy8c08LnznG8VAdc
> YILSn3uYGZap6aF1SgVxsvZicwv1YnssmgE13Af0nScmfM96k9h5joHVEkWK608v
> oT5DGG1kVL2Qly97x0b6EnzUorzivv5zJMKvFcOektR8HdMHQit5uvmMRY3S5zow
> FtvfSDFwxxKyTy6GBRrp+8F+Jq91yGy/qa9lhKBzT2lg+rJp7T8k7/Nm9Tjyx7jL
> EqgEKZEL4chxpo8ucF98hbvXWRuaFHC2iDzGuUmuS1FfjVvHTuIbEMQfjapLZrHx
> 8jHfOP/PL+6kPbvNZZ2rTpczuEoGTQFFW9vX48GzIEyMeR6QWpPR0F7r4xak68P5
> 2PJmVveinDhU35IqWEXHawcCAwEAAQ==
```

4 로깅 구성을 보려면 `get logging-server` 명령을 실행합니다. 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
```

5 원격 로깅 구성을 지우려면 다음 명령을 실행합니다.

```
nsx> clear logging-servers
```

6 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
```

7 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 21-10. 로그 메시지 ID

메시지 ID	예
FABRIC	호스트 노드 호스트 준비 Edge 노드 전송 영역 전송 노드 업링크 프로파일 클러스터 프로파일 Edge 클러스터
SWITCHING	논리적 스위치 논리적 스위치 포트 스위칭 프로파일 스위치 보안 기능

표 21-10. 로그 메시지 ID (계속)

메시지 ID	예
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 라이센싱 사용자 및 역할 작업 관리 설치 업그레이드(NSX Manager, NSX Edge 및 호스트 패키지 업그레이드) 인식 태그
MONITORING	SNMP 포트 연결 Traceflow
-	다른 모든 로그 메시지

Syslog 문제 해결

원격 로그 서버에 로그가 수신되지 않을 경우 다음 단계를 수행하십시오.

- 원격 로그 서버의 IP 주소를 확인합니다.
- level 매개 변수가 올바르게 구성되어 있는지 확인합니다.
- facility 매개 변수가 올바르게 구성되어 있는지 확인합니다.

- TLS 프로토콜을 사용하는 경우 프로토콜을 UDP로 설정하여, 인증서 불일치 문제가 있는지 확인합니다.
- TLS 프로토콜을 사용하는 경우 포트 6514가 양쪽 끝에 열려 있는지 확인합니다.
- 메시지 ID 필터를 제거하고, 서버에 로그가 수신되는지 확인합니다.
- `restart service rsyslogd` 명령을 사용하여 `rsyslog` 서비스를 다시 시작합니다.

장치 VM에서 직렬 로깅 구성

VM이 충돌할 때 로그 메시지를 캡처하도록 장치 VM에서 직렬 로깅을 구성할 수 있습니다.

절차

- 1 root 권한으로 VM에 로그인합니다.
- 2 `/etc/default/grub`을 편집합니다.
- 3 매개 변수 `GRUB_CMDLINE_LINUX_DEFAULT`를 찾고 `console=ttyS0 console=tty0`을 추가합니다.
- 4 `update-grub2` 명령을 실행합니다.
- 5 `/boot/grub/grub.cfg` 파일에 3단계에서 변경한 사항이 있는지 확인합니다.
- 6 VM의 전원을 끕니다.
- 7 VM의 구성 파일(.vmx)을 편집하고 다음 줄을 추가합니다.

```
serial0.present = "TRUE"
serial0.fileType = "file"
serial0.fileName = "serial.out"
serial0.yieldOnMsrRead = "TRUE"
answer.msg.serial.file.open = "Append"
```

- 8 VM의 전원을 켭니다.

결과

VM에서 커널 패닉이 발생한 경우 .vmx 파일과 동일한 위치에 로그 메시지를 포함하는 `serial.out` 파일을 찾을 수 있습니다.

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 CEIP 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 > 고객 프로그램**를 선택합니다.
- 3 [고객 환경 향상 프로그램] 섹션에서 **편집**을 클릭합니다.
- 4 [고객 환경 향상 프로그램 편집] 대화상자에서 **VMware 고객 환경 향상 프로그램 참여** 확인란을 선택합니다.
- 5 **스케줄** 스위치를 전환하여 데이터 수집을 사용하지 않거나 사용하도록 설정합니다.
스케줄은 기본적으로 사용되도록 설정됩니다.
- 6 (선택 사항) 데이터 수집을 구성하고 되풀이 설정을 업로드합니다.
- 7 **저장**을 클릭합니다.

개체에 태그 추가

개체에 태그를 추가하여 보다 쉽게 검색할 수 있습니다. 태그를 지정할 때 범위도 지정할 수 있습니다.

NSX Cloud 참고 NSX Cloud를 사용하는 경우 NSX Cloud에서 지원되는 NSX-T Data Center 기능에서 자동 생성된 논리적 엔티티, 지원되는 기능 및 NSX Cloud에 필요한 구성 목록을 확인하십시오.

대부분의 개체는 최대 30개의 태그를 가질 수 있습니다. 다음 개체의 경우 내부적으로 생성되고 사용되는 태그 때문에 최대값이 낮습니다.

표 21-11. [고급 네트워킹 및 보안] 탭을 사용하여 생성된 개체의 최대 태그 수

개체	최대 태그 수
가상 시스템	25
논리적 포트	29

표 21-12. [네트워킹], [보안] 또는 [인벤토리] 탭을 사용하여 생성된 개체의 최대 태그 수

개체	최대 태그 수
그룹	29
세그먼트	27
세그먼트 포트	29
논리적 라우터 포트	30 - 레이블 수
NAT 규칙	27
IPSec VPN 세션	29

표 21-13. Cloud Service Manager 개체의 최대 태그 수

개체	최대 태그 수
BFD 상태 모니터링 프로파일, 전송 영역, 업링크 호스트 스위치 프로파일, 전송 노드, Edge 클러스터	23

표 21-14. Public Cloud Manager 개체의 최대 태그 수

개체	최대 태그 수
BFD 상태 모니터링 프로파일, 전송 영역, 논리적 스위치, 노드, 전송 노드, Edge 클러스터, 논리적 라우터, 논리적 라우터 업링크 포트, 정적 경로, DHCP 프로파일, NSGroup, 방화벽 섹션 규칙 목록	23
NAT 규칙	20
IP 집합, NSGroup	22

절차

- 1 브라우저에서 관리자 권한으로 NSX Manager(<https://<nsx-manager-ip-address>>)에 로그인합니다.
- 2 개체를 편집합니다.
예를 들어, **세그먼트** 탭으로 이동하여 세그먼트를 편집합니다.
- 3 **태그** 필드를 이동한 후 태그를 추가합니다.
각 태그에는 태그 값(필수)과 범위 값(옵션)이 있습니다. 태그의 최대 길이는 256자입니다. 범위의 최대 길이는 128자입니다.
- 4 **저장**을 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 21-15. 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/hn7EEflhJ4m1698rRhMmNN2IW8y9iq2A
```

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 **고급 네트워킹 및 보안 > 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.

외부 로드 밸런서 구성

외부 로드 밸런서를 구성하여 관리자 클러스터의 NSX Manager로 트래픽을 분산할 수 있습니다.

NSX Manager 클러스터에는 외부 로드 밸런서가 필요하지 않습니다. NSX Manager VIP(가상 IP)는 관리자 노드 장애 시 복원력을 제공하지만 다음과 같은 제한 사항이 있습니다.

- VIP는 NSX Manager 전체에서 로드 밸런싱을 수행하지 않습니다.
- VIP를 사용하려면 모든 NSX Manager가 동일한 서브넷에 있어야 합니다.
- 관리자 노드 장애가 발생하는 경우 VIP 복구가 약 1-3분 정도 소요됩니다.

외부 로드 밸런서는 다음과 같은 이점을 제공할 수 있습니다.

- NSX Manager 전체에서 로드 밸런싱
- NSX Manager는 서로 다른 서브넷에 있을 수 있습니다.
- 관리자 노드 실패 시 빠른 복구 시간

외부 로드 밸런서는 NSX Manager VIP에서 작동하지 않습니다. 외부 로드 밸런서를 사용하는 경우 NSX Manager VIP를 구성하지 마십시오.

외부 로드 밸런서를 통해 브라우저에서 NSX Manager에 액세스하는 경우 로드 밸런서에서 세션 지속성을 사용하도록 설정해야 합니다.

외부 로드 밸런서를 통해 API 클라이언트에서 NSX Manager에 액세스할 때 4가지 인증 방법을 사용할 수 있습니다(자세한 내용은 "NSX-T Data Center API 가이드" 참조).

- HTTP 기본 인증 - 로드 밸런서 세션 지속성은 필요하지 않습니다.
- 클라이언트 인증서 인증 - 로드 밸런서 세션 지속성이 필요하지 않습니다.

- vIDM - 로드 밸런서 세션 지속성에 대한 인증이 필요하지 않습니다.
- 세션 기반 인증 - 로드 밸런서 세션 지속성이 필요합니다.

권장 사항:

- 브라우저 및 API 액세스 둘 다를 위해 로드 밸런서에 단일 IP를 구성합니다. 로드 밸런서는 세션 지속성을 사용하도록 설정해야 합니다.

NSX Cloud에서는 NSX-T Data Center를 사용하여 공용 클라우드 인벤토리를 관리하고 보호할 수 있습니다.

NSX Cloud 배포 워크플로에 대한 "NSX-T Data Center 설치 가이드"에서 NSX Cloud 구성 요소 설치를 참조하십시오.

참고 항목: 공용 클라우드

본 장은 다음 항목을 포함합니다.

- Cloud Service Manager의 빠른 둘러보기
- NSX Cloud 격리 정책을 사용한 위협 감지
- NSX 적용 모드
- 기본 클라우드 적용 모드
- NSX Cloud에서 지원되는 NSX-T Data Center 기능
- FAQ(질문과 대답)

Cloud Service Manager의 빠른 둘러보기

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

클라우드를 클릭하여 공용 클라우드 계정에 액세스합니다.

개요: 이 화면의 각 타일은 공용 클라우드 계정과 여기에 포함된 계정, 지역, VPC 또는 VNet 및 인스턴스(위크로드 VM)의 수를 나타냅니다.

다음 작업을 수행할 수 있습니다.

공용 클라우드 계정 또는 구독 추가	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. 자세한 지침은 "NSX-T Data Center 설치 가이드"의 공용 클라우드 계정 추가 를 참조하십시오.
NSX Public Cloud Gateway 배포/배포 해제	하나 또는 두 개(HA의 경우)의 PCG를 배포하거나 배포 해제할 수 있습니다. 또한 CSM에서 PCG를 배포 해제할 수도 있습니다. 자세한 지침은 "NSX-T Data Center 설치 가이드"의 PCG 배포 또는 PCG 배포 해제 를 참조하십시오.
격리 정책을 사용하거나 사용하지 않도록 설정	격리 정책을 사용하거나 사용하지 않도록 설정할 수 있습니다. 자세한 내용은 NSX Cloud 격리 정책을 사용한 위험 감지 항목을 참조하십시오.
그리드 및 카드 보기 사이 전환	카드에는 인벤토리 개요가 표시됩니다. 그리드에 더 자세한 내용이 표시됩니다. 보기 유형을 전환하려면 아이콘을 클릭하십시오.

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 VPC/vNet 수를 볼 수 있습니다.
- VPC/vNet당 위크로드 VM의 수를 볼 수 있습니다.

클라우드 아래에는 4개의 탭이 있습니다.

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/vNet 및 인스턴스가 있습니다. PCG를 배포한 경우 해당 PCG가 여기에서 PCG 상태 표시기가 있는 **게이트웨이**로 표시됩니다.

클라우드 > {공용 클라우드} > VPC 또는 VNet

[VPC] 또는 [vNet] 섹션에는 공용 클라우드 인벤토리가 표시됩니다.

인벤토리는 계정 및 지역별로 필터링할 수 있습니다.

- 각 카드는 하나의 VPC/vNet을 나타냅니다.
- 전송 VPC/vNet에 하나 또는 두 개(HA의 경우)의 PCG를 배포할 수 있습니다.
- 계산 VPC/vNet을 전송 VPC/vNet에 연결할 수 있습니다.
- 그리드 보기로 전환하면 각 VPC 또는 VNet에 대한 자세한 정보를 볼 수 있습니다.

참고 그리드 보기에서는 **개요**, **인스턴스** 및 **세그먼트**의 세 가지 탭을 볼 수 있습니다.

- **개요**에는 다음 단계에 설명된 것처럼 [작업] 아래의 옵션이 표시됩니다.
 - **인스턴스**에서는 VPC/VNet의 인스턴스 목록을 표시합니다.
 - **세그먼트**에서는 NSX-T의 오버레이 세그먼트를 표시합니다. 이 기능은 현재 NSX Cloud용 릴리스에서 지원되지 않습니다. 이 화면에 표시된 태그는 AWS 또는 Microsoft Azure의 워크로드 VM에 지정하지 마십시오.
-
- 다음에 액세스하려면 **작업**을 클릭하십시오.
 - **구성 편집**(전송 VPC/vNet에만 사용 가능):
 - NSX 적용 모드인 경우 격리 정책을 사용하거나 사용하지 않도록 설정합니다.
 - NSX 적용 모드를 사용할 때 VPC/vNet이 NSX Cloud에서 오프보드될 경우 필요한 폴백 보안 그룹을 제공합니다. 격리 정책을 사용하지 않을 때의 영향 항목을 참조하십시오.
 - 프록시 서버 선택을 변경합니다.
 - **전송 VPC/vNet에 연결**: 이 옵션은 PCG를 배포하지 않은 VPC/vNet에만 사용할 수 있습니다. 연결할 [전송 VPC/vNet]을 클릭합니다.
 - **NSX Cloud 게이트웨이 배포**: 이 옵션은 PCG를 배포하지 않은 VPC/vNet에만 사용할 수 있습니다. 이 VPC/vNet에 PCG 배포를 시작하고 전송 또는 자체 관리 VPC/vNet으로 만들려면 이 옵션을 클릭합니다. 자세한 지침은 "NSX-T Data Center 설치 가이드"의 **NSX 공용 클라우드 게이트웨이 배포 또는 연결**을 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.

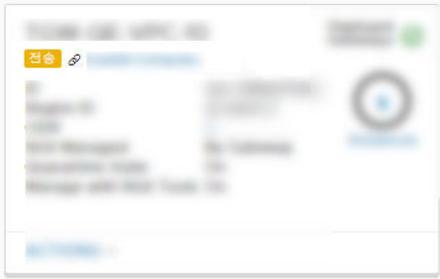
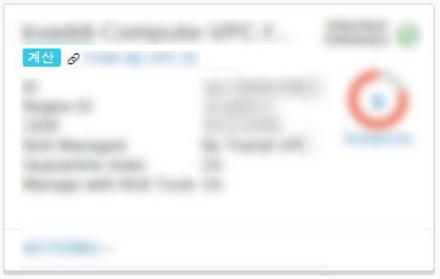
CSM 화이트리스트에서 인스턴스를 추가하거나 인스턴스를 제거할 수 있습니다. 자세한 내용은 [VM을 화이트리스트에 추가 항목을 참조하십시오.](#)

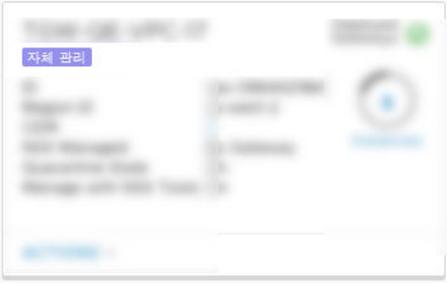
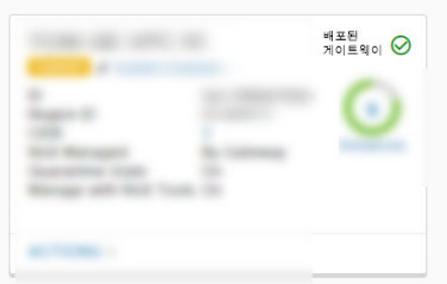
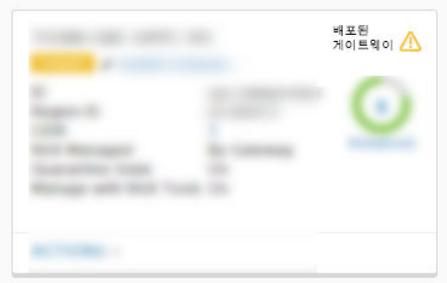
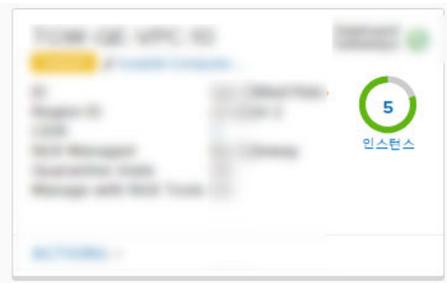
CSM 아이콘

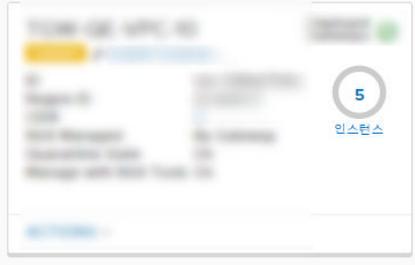
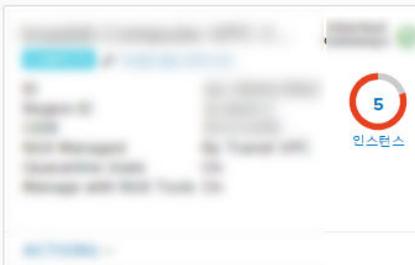
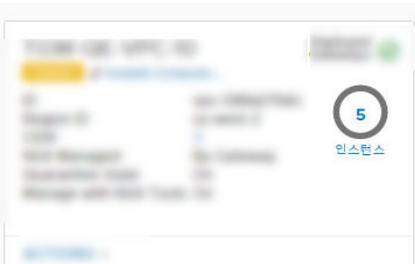
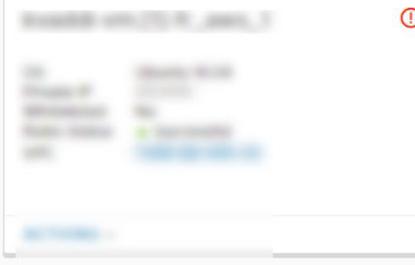
CSM은 알아보기 쉬운 아이콘을 사용하여 공용 클라우드 구성의 상태를 표시합니다.

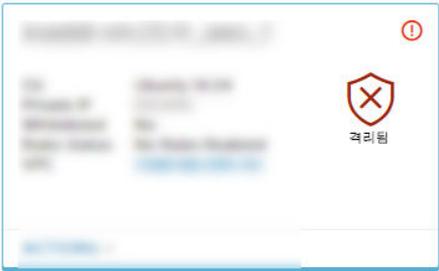
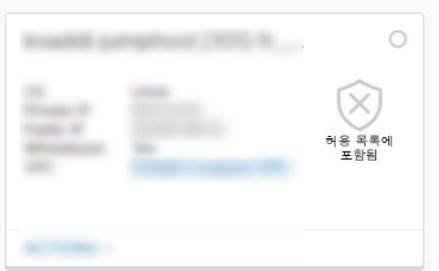
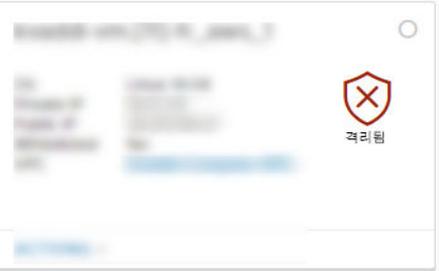
참고 기본 클라우드 적용 모드: 격리 정책은 항상 사용하도록 설정되며 모든 VM은 항상 NSX로 관리됩니다. NSX 관리 VM에 대해 격리 정책이 사용하도록 설정된 상태만 이 모드에서 적용됩니다.

NSX 적용 모드: 격리 정책을 사용하지 않도록 설정하고 VPC/vNet에 관리되지 않는 VM이 있을 수 있습니다. 모든 관련 상태가 이 모드에 적용됩니다.

CSM 섹션 및 아이콘	설명
VPC/vNet	
	전송 VPC/VNet
	계산 VPC/VNet

CSM 섹션 및 아이콘	설명
	<p>자체 관리 VPC/vNet</p>
	<p>정상 PCG를 표시하는 VPC/vNet</p>
	<p>PCG를 오류 상태로 표시하는 VPC/vNet</p>
	<p>하나의 PCG를 오류 상태로 표시하고 하나를 정상 상태로 표시하는 VPC/vNet.</p>
	<p>NSX 관리 VM을 표시하는 VPC/vNet.</p>

CSM 섹션 및 아이콘	설명
	<p>관리되지 않는 VM을 표시하는 VPC/vNet.</p>
	<p>오류 상태의 VM을 표시하는 VPC/vNet.</p>
	<p>전원이 꺼진 VM을 표시하는 VPC/vNet.</p>
<p>인스턴스</p>	
	<p>오류 없는 NSX 관리 VM.</p>
	<p>오류 및 격리 정책이 사용하지 않도록 설정된 NSX 관리 VM.</p>

CSM 섹션 및 아이콘	설명
	오류 및 격리 정책이 사용하도록 설정된 NSX 관리 VM.
	화이트리스트에 포함된 관리되지 않는 VM.
	격리된 관리되지 않는 VM.

시스템

다음은 **시스템** 아래의 섹션입니다.

시스템 > 설정

이러한 설정은 CSM를 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 있어야 하며 관리자 계정으로 NSX Manager에 로그인할 수 있도록 사용자 이름과 암호가 있어야 합니다.
- CSM이 설치되어 있고 CSM에 엔터프라이즈 관리자 역할이 할당되어 있어야 합니다.

절차

- 1 브라우저에서 CSM에 로그인합니다.
- 2 설정 마법사에서 해당하는 메시지가 표시되면 **설정 시작**을 클릭합니다.
- 3 [NSX Manager 자격 증명] 화면에 다음 세부 정보를 입력합니다.

옵션	설명
NSX Manager 호스트 이름	가능한 경우 NSX Manager의 FQDN(정규화된 도메인 이름)을 입력합니다. NSX Manager의 IP 주소를 입력할 수도 있습니다.
관리 자격 증명	NSX Manager에 대한 엔터프라이즈 관리자 사용자 이름 및 암호를 입력합니다.
관리자 지문	필요한 경우 NSX Manager의 지문 값을 입력합니다. 이 필드를 비워 두면 시스템에서 지문을 식별하고 이를 다음 화면에 표시합니다.

- 4 (선택 사항) NSX Manager에 대한 지문 값을 제공하지 않거나 잘못된 값을 제공하면 **지문 확인** 화면이 나타납니다. 시스템에서 검색된 지문을 수락하려면 확인란을 선택합니다.

- 5 **연결**을 클릭합니다.

참고 설정 마법사에서 이 설정을 누락했거나 연결된 NSX Manager를 변경하려는 경우 CSM에 로그인하고 **시스템 > 설정**을 클릭한 다음 **연결된 NSX 노드** 패널에서 **구성**을 클릭합니다.

CSM에서 NSX Manager 지문을 확인하고 연결을 설정합니다.

- 6 (선택 사항) 프록시 서버를 설정합니다. (선택 사항) 프록시 서버 구성의 지침을 참조하십시오.

(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.

NSX Cloud 격리 정책을 사용한 위협 감지

NSX Cloud의 격리 정책 기능은 NSX 관리 워크로드 VM에 대한 위협 감지 메커니즘을 제공합니다.

격리 정책은 두 개의 VM 관리 모드에서 다르게 구현됩니다.

표 22-1. NSX 적용 모드 및 기본 클라우드 적용 모드의 격리 정책 구현

격리 정책과 관련된 구성	NSX 적용 모드에서	기본 클라우드 적용 모드에서
기본 상태	NSX Tools를 사용하여 PCG 배포 시 사용 안 함. PCG 배포 화면 이상에서 이 기능을 사용하도록 설정할 수 있습니다. 격리 정책을 사용하거나 사용하지 않도록 설정하는 방법 항목을 참조하십시오.	항상 사용. 사용하지 않도록 설정할 수 없습니다.
각 모드에 고유한 자동 생성 보안 그룹	모든 정상 NSX 관리 VM에는 vm-underlay-sg 보안 그룹이 할당됩니다.	NSX Manager의 분산 방화벽 정책과 일치하는 NSX 관리 워크로드 VM에 nsx-<NSX GUID> 보안 그룹이 생성되고 적용됩니다.
두 모드 모두에 공통된 자동 생성 공용 클라우드 보안 그룹:	<p>gw 보안 그룹이 AWS 및 Microsoft Azure의 해당 PCG 인터페이스에 적용됩니다.</p> <ul style="list-style-type: none"> ■ gw-mgmt-sg ■ gw-uplink-sg ■ gw-vtep-sg <p>현재 상태와 격리 정책을 사용하도록 설정했는지 여부에 따라, vm의 보안 그룹이 NSX 관리 VM에 적용됩니다.</p> <ul style="list-style-type: none"> ■ Microsoft Azure의 vm-quarantine-sg 및 AWS의 default <p>참고 AWS에는 default 보안 그룹이 이미 있습니다. NSX Cloud에서 생성되지 않습니다.</p>	

NSX 적용 모드에 대한 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.

NSX 적용 모드의 격리 정책

격리 정책을 사용하도록 설정하는 것은 NSX 적용 모드에서 선택 사항입니다.

격리 정책을 사용하거나 사용하지 않도록 설정하는 방법

NSX 적용 모드에서는 두 가지 방법으로 격리 정책을 사용하도록 선택할 수 있습니다.

격리 정책을 사용하도록 설정할 수 있는 첫 번째 가능성은 전송 VPC/vNet에 PCG를 배포하거나 계산 VPC/vNet을 전송 대상에 연결하는 경우입니다. **연결된 VPC/vNet의 격리 정책**에 대한 슬라이더를 기본 **사용 안 함**에서 **사용**으로 전환합니다. "NSX-T Data Center 설치 가이드" 에서 **PCG 배포**를 참조하십시오.

나중에 이 단계에 따라 격리 정책을 사용하도록 설정할 수도 있습니다.

사전 요구 사항

PCG를 배포하거나 여기에 연결한 후 격리 정책을 사용하도록 설정하는 경우, NSX 적용 모드에 온보딩된 전송 또는 계산 VPC/vNet이 하나 이상 있어야 합니다. 이 경우 워크로드 VM을 관리하는 데 NSX Tools를 사용하기로 선택하게 됩니다.

절차

- 1 CSM에 로그인하고 공용 클라우드로 이동합니다.
 - a AWS를 사용 중인 경우 **클라우드 > AWS > VPC**로 이동합니다. [전송] 또는 [계산 VPC]를 클릭합니다.
 - b Microsoft Azure를 사용 중인 경우 **클라우드 > Azure > VNet**으로 이동합니다. [전송] 또는 [계산 vNet]을 클릭합니다.
- 2 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 클릭합니다.

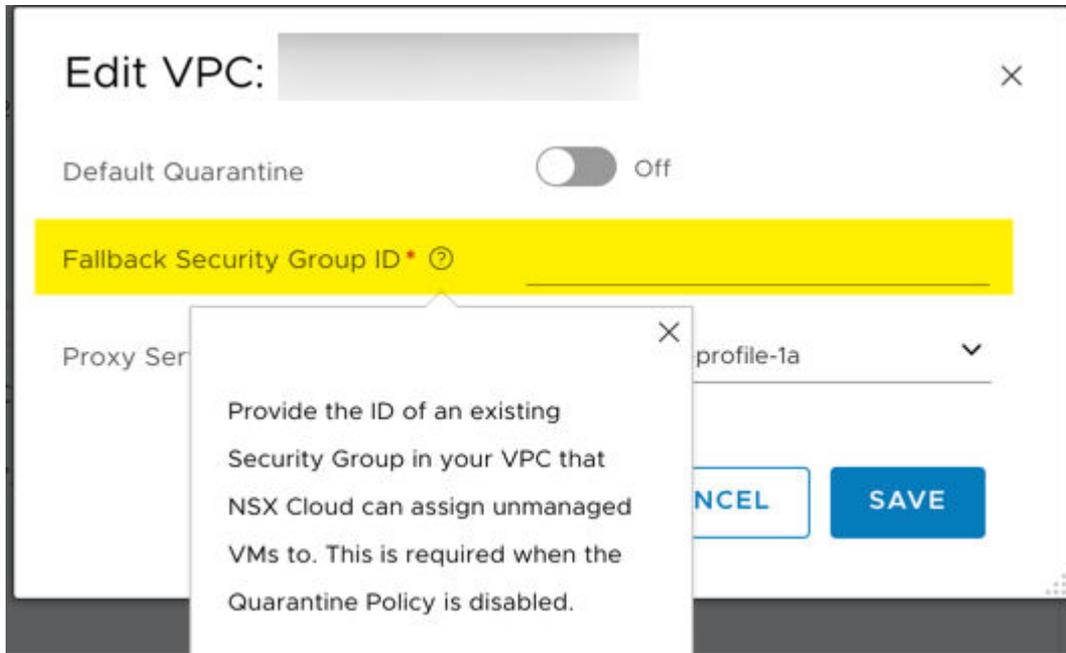


- ◆ VPC 또는 VNet의 페이지에 있는 경우 작업 아이콘을 클릭하여 **구성 편집**으로 이동합니다.



- 3 **기본 격리**를 설정 또는 해제하여 격리를 사용하거나 사용하지 않도록 설정합니다.
- 4 격리 정책을 사용하지 않도록 설정하는 경우에는 풀백 보안 그룹을 제공해야 합니다.

참고 풀백 보안 그룹은 공용 클라우드에 있는 기존의 사용자 정의 보안 그룹이어야 합니다. NSX Cloud 보안 그룹은 풀백 보안 그룹으로 사용할 수 없습니다.



- 이 VPC 또는 vNet에 있는 관리되지 않는 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 저장을 클릭합니다.

격리 정책을 사용하지 않을 때의 영향

격리 정책을 사용하지 않도록 설정한 경우 NSX Cloud가 태그 없는 VM의 공용 클라우드 보안 그룹을 관리하지 않습니다.

그러나 공용 클라우드에서 `nsx.network=default` 태그가 지정된 VM의 경우, NSX Cloud는 VM의 상태에 따라 적절한 보안 그룹을 할당합니다. 이 동작은 격리 정책을 사용하도록 설정한 경우와 비슷하지만 Microsoft Azure에서는 `vm-quarantine-sg`, AWS에서는 `default`에 해당하는 격리 보안 그룹의 규칙은 덜 제한적입니다. 태그가 지정된 VM의 보안 그룹이 수동으로 변경되면 2분 내에 NSX Cloud 할당 보안 그룹으로 복귀됩니다.

참고 NSX Cloud에서 NSX 관리(태그 지정) VM에 보안 그룹을 할당하지 않으려면 CSM에서 화이트리스트에 추가합니다. VM을 화이트리스트에 추가 항목을 참조하십시오.

다음 표에서는 격리 정책을 사용하지 않도록 설정한 경우 NSX Cloud가 워크로드 VM의 공용 클라우드 보안 그룹을 관리하는 방법을 보여 줍니다.

표 22-2. 격리 정책을 사용하지 않도록 설정한 경우 공용 클라우드 보안 그룹의 NSX Cloud 할당

VM이 공용 클라우드에서 <i>nsx.network=default</i> 태그가 지정되어 있습니까?	VM이 화이트리스트에 포함되어 있습니까?	격리 정책을 사용하지 않도록 설정할 때의 VM의 공용 클라우드 보안 그룹 및 설명
태그 지정	화이트리스트에 포함되지 않음	<ul style="list-style-type: none"> ■ VM에 위협이 없는 경우: <i>vm-underlay-sg</i> ■ VM에 잠재적인 위협이 있는 경우(참고 사항 참조): Microsoft Azure의 <i>vm-quarantine-sg</i>, AWS의 <i>default</i> <p>참고 공용 클라우드 보안 그룹의 할당은 워크로드 VM에 <i>nsx.network=default</i> 태그를 적용하고 90초 이내에 트리거됩니다. NSX를 통해 VM을 관리하려면 여전히 NSX Tools를 설치해야 합니다. NSX Tools를 설치할 때까지 태그가 지정된 워크로드 VM이 격리됩니다.</p>
태그가 지정되지 않음	화이트리스트에 포함되지 않음	NSX Cloud가 태그를 지정하지 않은 VM에 대해 작업을 수행하지 않으므로 기존 공용 클라우드 보안 그룹을 유지합니다.
태그 지정 태그가 지정되지 않음	허용 목록에 포함됨	NSX Cloud가 화이트리스트에 추가된 VM에 대해 어떤 작업도 수행하지 않으므로 기존 공용 클라우드 보안 그룹을 유지합니다.

다음 표에서는 이전에 격리 정책을 사용하도록 설정했다가 지금은 사용하지 않도록 설정한 경우, NSX Cloud가 이 VPC/vNet에 대한 보안 그룹 할당 처리를 위해 폴백 보안 그룹을 구성하여 VM의 공용 클라우드 보안 그룹을 관리하는 방법을 보여 줍니다.

표 22-3. 처음에 사용하도록 설정했던 격리 정책을 사용하지 않도록 설정한 경우 공용 클라우드 보안 그룹의 NSX Cloud 할당

VM이 공용 클라우드에서 <i>nsx.network=default</i> 태그가 지정되어 있습니까?	VM이 화이트리스트에 포함되어 있습니까?	격리 정책을 사용하도록 설정한 경우 VM의 기존 공용 클라우드 보안 그룹	격리 정책을 사용하지 않도록 설정하고 폴백 보안 그룹을 제공한 이후의 VM의 공용 클라우드 보안 그룹
태그가 지정되지 않음	화이트리스트에 포함되지 않음	vm-quarantine-sg(Microsoft Azure) 또는 default(AWS)	이 VM에는 격리 정책이 태그를 지정하지 않고 NSX를 통해 관리되는 것으로 간주되지 않기 때문에 사용하지 않도록 설정할 때 제공되는 폴백 보안 그룹이 할당됩니다. 따라서 격리 정책을 사용하지 않도록 설정하면 NSX Cloud는 이 VM이 할당된 보안 그룹을 되돌립니다.
태그 지정	화이트리스트에 포함되지 않음	vm-underlay-sg, vm-quarantine-sg(Microsoft Azure) 또는 default(AWS)	격리 사용 또는 사용 안 함 모드에서 태그가 지정된 VM에 대해 일관되므로 NSX Cloud 할당된 보안 그룹을 유지합니다.
태그 지정	허용 목록에 포함됨	기존 공용 클라우드 보안 그룹	NSX Cloud가 화이트리스트에 추가된 VM에 대해 어떤 작업도 수행하지 않으므로 기존 공용 클라우드 보안 그룹을 유지합니다. 참고 화이트리스트에 추가된 VM이 NSX Cloud 할당 보안 그룹에 있는 경우 지정된 폴백 보안 그룹에 수동으로 이동해야 합니다.
태그가 지정되지 않음			

격리 정책을 사용할 때의 영향

격리 정책을 사용하도록 설정하면 NSX Cloud가 이 VPC/vNet에 있는 모든 워크로드 VM의 공용 클라우드 보안 그룹을 관리합니다.

보안 그룹이 수동으로 변경되면 2분 내에 NSX Cloud 할당 보안 그룹으로 되돌려집니다. NSX Cloud에서 VM에 보안 그룹을 할당하지 않도록 하려면 CSM에서 화이트리스트에 추가합니다. VM을 화이트리스트에 추가 항목을 참조하십시오.

참고 화이트리스트에서 VM을 제거하면 해당 VM이 NSX Cloud 할당 보안 그룹으로 복귀됩니다.

표 22-4. 격리 정책을 사용하도록 설정한 경우 공용 클라우드 보안 그룹의 NSX Cloud 할당

VM이 공용 클라우드에서 <i>nsx.network=default</i> 태그가 지정되어 있습니까?	VM이 화이트리스트에 포함되어 있습니까?	격리 정책을 사용하도록 설정할 때의 VM의 공용 클라우드 보안 그룹 및 설명
태그 지정	화이트리스트에 포함되지 않음	<ul style="list-style-type: none"> VM에 위협이 없는 경우: <i>vm-underlay-sg</i> VM에 잠재적인 위협이 있는 경우(참고 사항 참조): Microsoft Azure의 <i>vm-quarantine-sg</i>, AWS의 <i>default</i> <p>참고 공용 클라우드 보안 그룹의 할당은 워크로드 VM에 <i>nsx.network=default</i> 태그를 적용하고 90초 이내에 트리거됩니다. NSX를 통해 VM을 관리하려면 여전히 NSX Tools를 설치해야 합니다. NSX Tools를 설치할 때까지 태그가 지정된 워크로드 VM이 격리됩니다.</p>
태그가 지정되지 않음	화이트리스트에 포함되지 않음	Microsoft Azure의 <i>vm-quarantine-sg</i> 및 AWS의 <i>default</i> 태그 없는 VM은 관리되지 않는 것으로 간주되므로 NSX Cloud에서 격리됩니다.
태그 지정	허용 목록에 포함됨	NSX Cloud가 화이트리스트에 추가된 VM에 대해 작업을 수행하지 않으므로 기존 공용 클라우드 보안 그룹을 유지합니다.
태그가 지정되지 않음		

다음 표에는 격리 정책이 처음에는 사용되지 않도록 설정되었다가 사용되도록 설정된 경우 보안 그룹 할당에 대한 영향이 캡처되어 있습니다.

표 22-5. 처음에 사용하지 않도록 설정했던 격리 정책을 사용하도록 설정한 경우 공용 클라우드 보안 그룹의 NSX Cloud 할당

VM이 공용 클라우드에서 <i>nsx.network=default</i> 태그가 지정되어 있습니까?	VM이 화이트리스트에 포함되어 있습니까?	격리 정책을 사용하지 않도록 설정한 경우 VM의 기존 공용 클라우드 보안 그룹	격리 정책을 사용하도록 설정한 후의 VM의 공용 클라우드 보안 그룹
태그가 지정되지 않음	화이트리스트에 포함되지 않음	기존 공용 클라우드 보안 그룹	<i>vm-quarantine-sg</i> (Microsoft Azure) 또는 <i>default</i> (AWS)
태그 지정	화이트리스트에 포함되지 않음	<i>vm-underlay-sg</i> , <i>vm-quarantine-sg</i> (Microsoft Azure) 또는 <i>default</i> (AWS)	격리 사용 또는 사용 안 함 모드에서 태그가 지정된 VM에 대해 일관되므로 NSX Cloud 할당된 보안 그룹을 유지합니다.

표 22-5. 처음에 사용하지 않도록 설정했던 격리 정책을 사용하도록 설정한 경우 공용 클라우드 보안 그룹의 NSX Cloud 할당 (계속)

VM이 공용 클라우드에서 <code>nsx.network=default</code> 태그가 지정되어 있습니까?	VM이 화이트리스트에 포함되어 있습니까?	격리 정책을 사용하지 않도록 설정한 경우 VM의 기존 공용 클라우드 보안 그룹	격리 정책을 사용하도록 설정한 후의 VM의 공용 클라우드 보안 그룹
태그 지정	허용 목록에 포함됨	모든 기존 공용 클라우드 보안 그룹.	NSX Cloud가 화이트리스트에 추가된 VM에 대해 어떤 작업도 수행하지 않으므로 기존 공용 클라우드 보안 그룹을 유지합니다.
태그가 지정되지 않음			

기본 클라우드 적용 모드의 격리 정책

격리 정책은 항상 기본 클라우드 적용 모드에서 사용하도록 설정합니다.

표 22-6. 기본 클라우드 적용 모드에서 공용 클라우드 보안 그룹 할당

VM이 유효한 NSX-T 보안 정책에 속합니까?	VM이 화이트리스트에 포함되어 있습니까?	VM의 공용 클라우드 보안 그룹 및 설명
예, VM이 유효한 NSX-T 보안 정책과 일치합니다.	화이트리스트에 포함되지 않음	NSX-T 보안 정책에 대한 해당 공용 클라우드 보안 그룹인 NSX Cloud에서 생성된 공용 클라우드 보안 그룹(<code>nsx-{NSX-GUID}</code>)입니다.
아니요, VM에 유효한 NSX-T 방화벽 정책이 없습니다.	화이트리스트에 포함되지 않음	NSX Cloud의 위협 감지 동작이므로 Microsoft Azure의 default 또는 AWS의 <code>vm-quarantine-sg</code> 입니다. 기본 클라우드 적용 모드에서 Microsoft Azure의 NSX Cloud 생성 보안 그룹 default 또는 AWS의 <code>vm-quarantine-sg</code> 는 기본 공용 클라우드 보안 정책을 모방합니다. 참고 CSM에서 VM은 오류 상태를 표시합니다.
예, VM에 유효한 NSX-T 보안 정책이 있습니다.	허용 목록에 포함됨	NSX Cloud가 화이트리스트에 추가된 VM에 대해 어떤 작업도 수행하지 않으므로 기존 공용 클라우드 보안 그룹을 유지합니다.
아니요, VM에 유효한 NSX-T 보안 정책이 없습니다.		

VM을 화이트리스트에 추가

화이트리스트는 공용 클라우드 인벤토리의 모든 워크로드 VM에 대해 CSM에서 사용할 수 있는 옵션입니다.

화이트리스트는 VM 관리 모드 NSX 적용 모드 및 기본 클라우드 적용 모드 둘 다에서 작동합니다.

VM을 화이트리스트에 추가하는 이유는 무엇입니까?

- NSX 적용 모드: 격리 정책을 사용하도록 설정했고 VM에서 기존 애플리케이션을 사용하여 특정 DFW 정책을 확인해야 하는 경우 NSX Cloud에 온보딩하기 전에 이러한 VM을 화이트리스트에 추가합니다.

- NSX 적용 모드 또는 기본 클라우드 적용 모드에서:
 - 오류가 있는 VM이 있고 이러한 오류를 해결하기 위해 액세스하려는 경우 해당 VM을 화이트리스트에 추가하여 격리 상태를 벗어나도록 하고 필요에 따라 디버깅 도구를 사용할 수 있습니다.
 - DNS 전달자, 프록시 서버 등과 같이 NSX-T에서 관리하지 않으려는 공용 클라우드 인벤토리의 VM을 화이트리스트에 추가합니다.

VM을 화이트리스트에 추가하거나 화이트리스트에서 제거하는 방법

다음 지침에 따라 VM을 화이트리스트에 추가하거나 제거합니다.

사전 요구 사항

하나 이상의 공용 클라우드 계정이 CSM에 추가되어 있어야 합니다.

절차

- 1 엔터프라이즈 관리자 계정을 사용하여 CSM에 로그인하고 공용 클라우드 계정으로 이동합니다.
 - a AWS를 사용 중인 경우 **클라우드 > AWS > VPC > 인스턴스**로 이동합니다.
 - b Microsoft Azure를 사용 중인 경우 **클라우드 > Azure > vNet > 인스턴스**로 이동합니다.
- 2 타일 모드에서 인스턴스 뷰의 오른쪽 모서리에 있는 모드 선택기를 클릭하여 그리드 모드로 전환합니다.
- 3 화이트리스트에 추가하거나 화이트 리스트에서 제거할 VM(인스턴스)을 선택합니다.
- 4 **작업**을 클릭하고 **화이트리스트에 추가** 또는 **화이트 리스트에서 제거**를 선택합니다.
- 5 [계정] 탭으로 돌아가서 계정 타일을 선택하고 **작업 > 계정 다시 동기화**를 클릭합니다.

결과

화이트리스트에 추가된 각 VM은 화이트리스트에 추가하기 전에 할당되었던 보안 그룹에 남아 있습니다. 이제 필요할 때 다른 보안 그룹을 VM에 적용할 수 있습니다. NSX Cloud는 격리 정책의 상태와 관계없이 화이트리스트에 들어 있는 VM을 무시합니다.

기본 클라우드 적용 모드의 화이트리스트에서 VM을 제거하거나 NSX 적용 모드의 화이트리스트에서 NSX 관리 VM을 제거하면 NSX Cloud는 해당 상태에 따라 해당 VM에 보안 그룹을 할당하기 시작합니다.

NSX 적용 모드

NSX 적용 모드에서 NSX-T Data Center를 사용하여 이러한 VM의 관리를 시작하기 전에 NSX Tools를 사용하여 공용 클라우드에서 태그를 지정하고 NSX Tools에 설치하여 VM을 온보딩해야 합니다.

현재 워크로드 VM에 대해 지원되는 운영 체제

NSX 적용 모드의 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. 지원되는 운영 체제의 경우 표준 Linux 커널 버전을 사용하는 것으로 간주됩니다. 사용자 지정 커널을 사용하는 공용 클라우드 마켓플레이스 이미지(예: 소스가 변경된 업스트림 Linux 커널)는 지원되지 않습니다.

- Red Hat Enterprise Linux(RHEL) 7.2, 7.3, 7.4, 7.5, 7.6
- CentOS 7.2, 7.3, 7.4, 7.5, 7.6

참고 RHEL 및 CentOS의 RHEL EUS(확장 업데이트 지원) 커널은 지원되지 않습니다.

참고 NSX Cloud에서는 해당 배포 버전이 예상되는 부 커널 버전과 일치하는 CentOS 마켓플레이스 이미지만 지원됩니다. 예를 들어 배포 버전과 해당하는 커널 버전은 다음과 같아야 합니다.

RHEL 버전	커널 버전
RHEL 7.6	3.10.0-957
RHEL 7.5	3.10.0-862
RHEL 7.4	3.10.0-693
RHEL 7.3	3.10.0-514
RHEL 7.2	3.10.0-327

- Ubuntu 14.04, 16.04, 18.04
- Microsoft Windows Server 2016 - 서비스 기반 릴리스, 데스크톱 환경(1709, 1803, 1809)
- Microsoft Windows Server 2019 데이터센터
- Microsoft Windows Server 2012 R2
- Microsoft Windows 10 버전 1809, 1803, 1709(현재 NSX Cloud 릴리스의 Microsoft Azure에서만 지원됨)

NSX 적용 모드에서 VM 온보딩

NSX 적용 모드의 공용 클라우드에서 워크로드 VM을 온보딩하고 관리하는 단계에 대한 개요는 이 워크플로를 참조하십시오.

표 22-7. 워크로드 VM을 NSX Cloud에 온보딩하는 Day-N 워크플로

작업	지침
<p><input type="checkbox"/> 키-값 <code>nsx.network=default</code>로 워크로드 VM에 태그를 지정합니다.</p>	<p>워크로드 VM에 태그를 지정하는 방법은 공용 클라우드 설명서의 지침을 참조하십시오.</p>
<p><input type="checkbox"/> Windows 및 Linux 워크로드 VM에 NSX Tools를 설치합니다.</p> <p>참고 자동 설치 NSX Tools가 Microsoft Azure vNet용 CSM에서 사용하도록 설정된 경우, NSX Tools가 자동으로 설치됩니다.</p>	<p>NSX Tools 설치 항목을 참조하십시오.</p>
<p><input type="checkbox"/> (옵션) CSM에서 NSX를 통해 관리하려는 모든 VM을 화이트리스트에서 제거합니다.</p> <p>참고 화이트리스트는 CSM에 공용 클라우드 인벤토리를 추가하는 즉시 day-0 워크플로에서 권장되는 수동 단계입니다. 화이트리스트에 추가하지 않은 경우에는 화이트리스트에서 VM을 제거할 필요가 없습니다.</p>	<p>VM을 화이트리스트에 추가하거나 화이트리스트에서 제거하는 방법 항목을 참조하십시오.</p>

공용 클라우드에서 VM 태그 지정

NSX-T Data Center를 사용하여 관리하려는 VM에 `nsx.network=default` 태그를 적용합니다.

절차

- 1 공용 클라우드 계정에 로그인하고 NSX-T Data Center에서 워크로드 VM을 관리하려는 VPC 또는 vNet으로 이동합니다.
- 2 NSX-T Data Center를 사용하여 관리하려는 VM을 선택합니다.
- 3 VM에 대한 태그 세부 정보를 추가하고 변경 내용을 저장합니다.

```
Key: nsx.network
Value: default
```

참고 이 태그를 VM 수준에서 적용합니다.

결과

`nsx.network=default` 태그를 워크로드 VM에 적용한 VPC/vNet을 이미 온보딩했을 수 있습니다. 태그를 적용한 후에 이러한 VPC/vNet을 온보딩할 수도 있습니다. VPC/vNet을 성공적으로 온보딩하면 워크로드 VM이 NSX를 통해 관리되는 것으로 간주됩니다.

다음에 수행할 작업

이러한 VM에 NSX Tools를 설치하십시오. [NSX Tools 설치](#)의 내용을 참조하십시오.

Microsoft Azure를 사용하는 경우 태그 지정된 VM에 NSX Tools를 자동으로 설치할 수 있습니다. 자세한 내용은 [자동으로 NSX Tools 설치](#) 항목을 참조하십시오.

NSX Tools 설치

워크로드 VM에 NSX Tools 설치

NSX Tools를 설치하는 데 사용할 수 있는 몇 가지 옵션이 있습니다.

- 개별 워크로드 VM에 NSX Tools를 다운로드하고 설치합니다. Linux 및 Windows VM에는 몇 가지 버전이 있습니다.
- 공용 클라우드의 지원되는 방법을 사용하여 설치한 NSX Tools에서 복제 가능 이미지를 사용합니다. 예를 들어 AWS에서는 AMI를, Microsoft Azure에서는 관리되는 이미지를 생성합니다.
- AWS 전용: VM을 시작할 때 **사용자 데이터**에서 NSX Tools 다운로드 위치 및 설치 명령을 제공합니다.
- Microsoft Azure 전용: Microsoft Azure vNet에서 PCG를 배포하거나 전송 vNet에 연결하는 동안 또는 전송/계산 vNet 구성을 편집하여 NSX Tools의 자동 설치를 사용하도록 설정합니다.

참고 NSX Tools를 설치하려는 화이트리스트의 워크로드 VM이 있는 경우 다음 포트가 이러한 VM에 할당된 보안 그룹에서 열려 있는지 확인합니다.

- 인바운드 UDP 6081: 오버레이 데이터 패킷의 경우. (활성/대기) PCG의 VTEP IP 주소(eth1 인터페이스)에 대해 허용되어야 합니다.
- 아웃바운드 TCP 5555: 제어 패킷의 경우. (활성/대기) PCG의 관리 IP 주소(eth0 인터페이스)에 대해 허용되어야 합니다.
- TCP 8080: PCG의 관리 IP 주소에 대한 설치/업그레이드의 경우
- TCP 80: NSX Tools를 설치하는 동안 임의의 타사 종속성을 다운로드하는 경우
- UDP 67, 68: DHCP 패킷의 경우
- UDP 53: DNS 해결의 경우

Linux VM에 NSX Tools 설치

Linux 워크로드 VM에 NSX Tools를 설치하려면 다음 지침을 따릅니다.

현재 지원되는 Linux 배포 목록은 [현재 워크로드 VM에 대해 지원되는 운영 체제 항목](#)을 참조하십시오.

참고 이 스크립트의 체크섬을 확인하려면 **VMware 다운로드 > 드라이버 및 도구 > NSX Cloud 스크립트**로 이동하십시오.

사전 요구 사항

NSX Tools 설치 스크립트를 실행하려면 다음 명령이 필요합니다.

- **wget**
- **nslookup**
- **dmidecode**

절차

- 1 CSM에 로그인하고 공용 클라우드로 이동합니다.
 - a AWS를 사용 중인 경우 **클라우드 > AWS > VPC**로 이동합니다. 전송 또는 계산 VPC를 클릭합니다.
 - b Microsoft Azure를 사용 중인 경우 **클라우드 > Azure > VNet**으로 이동합니다. 하나 또는 한 쌍의 PCG가 배포되어 실행 중인 VNet을 클릭합니다.

참고: 전송 VPC/VNet에서는 하나 또는 한 쌍의 PCG가 배포되고 실행됩니다. 계산 VPC/VNet은 전송에 연결되며 여기에서 배포된 PCG 인스턴스를 사용할 수 있습니다.

- 2 화면의 **NSX Tools 다운로드 및 설치** 섹션에서 **Linux** 아래에 있는 **다운로드 위치** 및 **설치 명령**을 적어 둡니다.

참고 VNet의 경우, 설치 명령의 DNS 접미사는 PCG를 배포할 때 선택한 DNS 설정과 일치하도록 동적으로 생성됩니다. 전송 VNet의 경우 `-dnsServer <dns-server-ip>` 매개 변수는 선택 사항입니다. 계산 VNet의 경우 이 명령을 완료하려면 DNS 전달자 IP 주소를 제공해야 합니다.

- 3 슈퍼유저 권한으로 Linux 워크로드 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.

참고 이 스크립트의 체크섬을 확인하려면 **VMware 다운로드 > 드라이버 및 도구 > NSX Cloud 스크립트**로 이동하십시오.

- 5 필요한 경우 설치 스크립트에 대한 권한을 실행이 가능하도록 변경하고 실행합니다.

```
$ chmod +x install_nsx_vm_agent.sh && sudo ./install_nsx_vm_agent.sh
```

참고: Red Hat Enterprise Linux 및 해당 파생 제품에서 SELinux가 지원되지 않습니다. NSX Tools를 설치하려면 SELinux를 사용하지 않도록 설정합니다.

- 6 NSX Tools 설치가 시작된 후 Linux VM과의 연결이 끊어집니다. 화면에 다음과 같은 메시지가 표시됩니다. `Installation completed!!! Starting NSX Agent service. SSH connection will now be lost.` 온보딩 프로세스를 완료하려면 VM에 다시 로그인합니다.

결과

NSX Tools가 워크로드 VM에 설치됩니다.

참고

- NSX Tools가 설치된 후 포트 8888은 워크로드 VM에서 열린 상태로 표시되지만 언더레이 모드에서 VM에 대해 차단되어 있으며 고급 문제 해결에 필요한 경우에만 사용해야 합니다. 점프 호스트가 액세스하려는 워크로드 VM과 동일한 VPC에도 있는 경우 점프 호스트를 사용하여 포트 8888을 통해 워크로드 VM에 액세스할 수 있습니다.
- 스크립트는 eth0을 기본 인터페이스로 사용합니다.

다음에 수행할 작업

NSX 적용 모드에서 VM 관리

Windows VM에 NSX Tools 설치

다음 지침에 따라 Windows 워크로드 VM에 NSX Tools를 설치합니다.

현재 지원되는 Microsoft Windows 버전 목록은 현재 워크로드 VM에 대해 지원되는 운영 체제를 참조하십시오.

참고 이 스크립트의 체크섬을 확인하려면 **VMware 다운로드 > 드라이버 및 도구 > NSX Cloud 스크립트**로 이동하십시오.

절차

- 1 CSM에 로그인하고 공용 클라우드로 이동합니다.
 - a AWS를 사용 중인 경우 **클라우드 > AWS > VPC**로 이동합니다. 전송 또는 계산 VPC를 클릭합니다.
 - b Microsoft Azure를 사용 중인 경우 **클라우드 > Azure > VNet**으로 이동합니다. 하나 또는 한 쌍의 PCG가 배포되어 실행 중인 VNet을 클릭합니다.

참고: 전송 VPC/VNet에서는 하나 또는 한 쌍의 PCG가 배포되고 실행됩니다. 계산 VPC/VNet은 전송에 연결되며 여기에서 배포된 PCG를 사용할 수 있습니다.
- 2 화면의 **NSX Tools 다운로드 및 설치** 섹션에서 **Windows** 아래에 있는 **다운로드 위치 및 설치 명령**을 적어둡니다.

참고 VNet의 경우, 설치 명령의 DNS 접미사는 PCG를 배포할 때 선택한 DNS 설정과 일치하도록 동적으로 생성됩니다. 전송 VNet의 경우 `-dnsServer <dns-server-ip>` 매개 변수는 선택 사항입니다. 계산 VNet의 경우 이 명령을 완료하려면 DNS 전달자 IP 주소를 제공해야 합니다.

- 3 Windows 워크로드 VM에 관리자 권한으로 연결합니다.

- 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.

참고 이 스크립트의 체크섬을 확인하려면 **VMware 다운로드 > 드라이버 및 도구 > NSX Cloud 스크립트**로 이동하십시오.

참고:

- PowerShell 프롬프트를 열어 다운로드한 스크립트가 포함된 디렉토리로 이동합니다.
- CSM에서 확인한 **설치 명령**을 사용하여 다운로드한 스크립트를 실행합니다.

예:

```
c:\> 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.

- 스크립트가 실행되고 완료되면 NSX Tools가 성공적으로 설치되었는지 여부를 나타내는 메시지가 표시됩니다.

참고 스크립트는 기본 네트워크 인터페이스를 기본값으로 간주합니다.

다음에 수행할 작업

NSX 적용 모드에서 VM 관리

복제 가능 이미지 생성

NSX 에이전트가 설치된 VM의 Microsoft Azure에서 관리 이미지 또는 AWS에서 AMI를 생성할 수 있습니다.

이 기능을 사용하여 에이전트가 구성되어 실행 중인 여러 VM을 시작할 수 있습니다.

NSX 에이전트가 설치된 VM의 AMI/관리 이미지(이 항목의 나머지 부분에서 이미지로 칭함)를 생성할 수 있는 두 가지 방법이 있습니다.

- **구성되지 않은 NSX 에이전트를 사용하여 이미지 생성:** `-noStart` 옵션을 사용하여 NSX 에이전트가 설치되었지만 구성되지 않은 VM에서 이미지를 생성할 수 있습니다. 이 옵션을 사용하면 NSX 에이전트 패키지를 가져오고 설치할 수 있지만 NSX 서비스가 시작되지 않습니다. 또한 인증서 생성과 같은 NSX 구성이 수행되지 않습니다.
- **기존 NSX 에이전트 구성을 제거한 후 이미지 생성:** 기존 NSX 관리 VM에서 구성을 제거하고 이미지 생성에 사용할 수 있습니다.

구성되지 않은 NSX 에이전트를 사용하여 AMI 생성

설치되고 구성되지 않은 NSX 에이전트를 사용하여 VM의 AMI를 생성할 수 있습니다.

-noStart 옵션을 사용하여 설치된 NSX 에이전트가 있는 VM에서 이미지를 생성하려면 다음을 수행합니다.

절차

- 1 CSM에서 NSX 에이전트 설치 명령을 복사하여 붙여넣습니다. **NSX Tools 설치**의 지침을 참조하십시오.

- a Windows에 대한 명령을 다음과 같이 편집합니다.

```
c:\> powershell -file 'nsx_install.ps1' -operation install -dnsSuffix <> -noStart true
```

- b Linux에 대한 명령을 다음과 같이 편집합니다.

```
$ chmod +x install_nsx_vm_agent.sh && sudo ./install_nsx_vm_agent.sh --no-start
```

- 2 공용 클라우드의 이 VM으로 이동하고 이미지를 생성합니다.

기존 NSX 에이전트 구성을 제거한 후 이미지 생성

구성된 NSX 에이전트가 있는 VM의 이미지를 생성할 수 있습니다.

기존 NSX 관리 VM에서 구성을 제거하고 이미지를 생성하는 데 사용하려면 다음을 수행합니다.

절차

- 1 Windows 또는 Linux VM에서 NSX 에이전트 구성을 제거합니다.

- a 가능하면 점프 호스트를 사용하여 워크로드 VM에 로그인합니다.
- b NSX-T CLI를 엽니다.

```
sudo nsxcli
```

- c 다음 명령을 입력합니다.

```
hostname> set debug
hostname> clear nsx-vm-agent state
```

- 2 공용 클라우드의 이 VM을 찾고 이미지를 생성합니다.

자동으로 NSX Tools 설치

현재 Microsoft Azure에 대해서만 지원됩니다.

Microsoft Azure에서 다음 기준이 충족되는 경우 NSX Tools가 자동으로 설치됩니다.

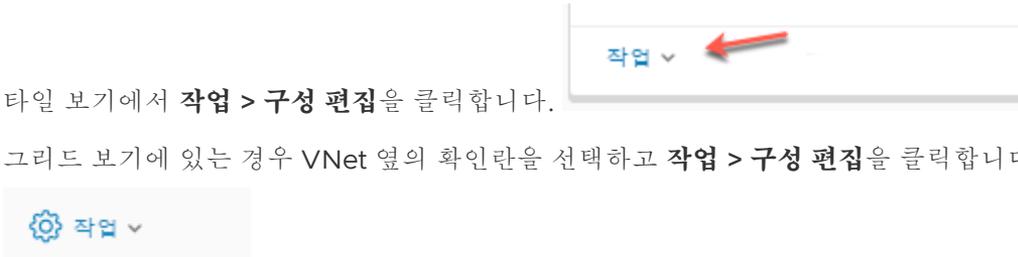
- NSX Cloud에 추가된 vNet의 VM에 Azure VM 확장이 설치되어 있습니다. 자세한 내용은 **VM 확장에 대한 Microsoft Azure 설명서**를 참조하십시오.

- Microsoft Azure의 VM에 적용된 보안 그룹은 NSX Tools 설치를 위해 액세스를 허용해야 합니다. 격리 정책을 사용하도록 설정한 경우 설치 전에 CSM에서 VM을 화이트리스트하고 설치한 후에는 화이트리스트에서 제거할 수 있습니다.
- VM에 nsx.network 및 값 default를 사용하여 태그가 지정되었습니다.

이 기능을 사용하도록 설정하려면 다음과 같이 하십시오.

- 1 클라우드 > Azure > VNet으로 이동합니다.
- 2 CSM을 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.



- [vNet] 탭에 있는 경우 작업 아이콘을 클릭하여 **구성 편집**으로 이동합니다.

- 4 NSX Tools 자동 설치 옆에 있는 슬라이더를 켜짐 위치로 이동합니다.

참고 NSX Tools 설치가 실패하면 다음을 수행합니다.

- 1 Microsoft Azure Portal에 로그인하여 NSX Tools 설치가 실패한 VM으로 이동합니다.
- 2 VM의 확장으로 이동하여 이름이 VMwareNsxAgentInstallCustomScriptExtension인 확장을 제거합니다.
- 3 이 VM에서 nsx.network=default 태그를 제거합니다.
- 4 이 VM에 nsx.network=default 태그를 다시 추가합니다.

약 3분 내에 NSX Tools가 이 VM에 설치됩니다.

AWS에서 사용자 데이터를 사용하여 NSX Tools 설치

AWS VPC에서 새 워크로드 VM을 실행할 때 [사용자 데이터] 필드에 NSX Tools 다운로드 및 설치 지침을 제공하여 NSX Tools를 설치할 수 있습니다.

CSM에서 NSX Tools에 대한 다운로드 및 설치 지침을 복사한 후 새 워크로드 VM을 시작할 때 사용자 데이터에 붙여넣습니다.

절차

- 1 AWS 콘솔에 로그인하고 새 워크로드 VM을 실행하는 프로세스를 시작합니다.

- 2 다른 브라우저 창에서 CSM에 로그인합니다.
 - a **클라우드 > AWS > VPC**로 이동합니다.

참고 전송 VPC/vNet에서는 하나 또는 한 쌍의 PCG가 배포되고 실행됩니다. 계산 VPC/VNet은 전송에 연결되며 여기에서 배포된 PCG를 사용할 수 있습니다.

- b 전송 또는 계산 VPC를 클릭합니다.
 - c 화면의 **NSX Tools 다운로드 및 설치** 섹션에서 워크로드 VM에 사용하는 OS에 따라 **Linux** 또는 **Windows**에서 **다운로드 위치** 및 **설치 명령**을 복사합니다.
- 3 AWS에서 새 워크로드 VM 인스턴스를 실행하는 단계에서 [고급 세부 정보] 섹션의 [사용자 데이터]에 다운로드 위치와 설치 명령을 **텍스트**로 붙여넣습니다.

결과

워크로드 VM이 실행되고 NSX Tools가 자동으로 설치됩니다.

NSX Tools 제거

다음 OS 관련 명령을 사용하여 NSX Tools를 제거하십시오.

Windows VM에서 NSX Tools 제거

참고 설치 스크립트에 사용 가능한 다른 옵션을 보려면 `-help`를 사용합니다.

- 1 RDP를 사용하여 VM에 원격 로그인합니다.
- 2 설치 스크립트를 제거 옵션과 함께 실행합니다.

```
\nsx_install.ps1 -operation uninstall
```

Linux VM에서 NSX Tools 제거

참고 설치 스크립트에 사용 가능한 다른 옵션을 보려면 `--help`를 사용합니다.

- 1 SSH를 사용하여 VM에 원격 로그인합니다.
- 2 설치 스크립트를 제거 옵션과 함께 실행합니다.

```
sudo ./install_nsx_vm_agent.sh --uninstall
```

NSX 적용 모드에 온보딩한 후의 보안 그룹

다음 보안 그룹 구성은 자동으로 수행됩니다.

격리 정책을 사용하도록 설정하면:

- 정상 NSX 관리 VM이 공용 클라우드의 `vm-underlay-sg`로 이동됩니다.
- 오류가 있는 관리되지 않는 VM 또는 NSX 관리 VM이 AWS에서는 `default` 보안 그룹으로 이동되고, Microsoft Azure에서는 `vm-quarantine-sg` 네트워크 보안 그룹으로 이동됩니다.

- 화이트리스트 VM은 영향을 받지 않습니다.

격리 정책을 사용하지 않도록 설정하면:

- 정상 NSX 관리 VM이 공용 클라우드의 vm-underlay-sg로 이동됩니다.
- 오류가 있는 NSX 관리 VM이 AWS에서는 default 보안 그룹으로 이동되고, Microsoft Azure에서는 vm-quarantine-sg 네트워크 보안 그룹으로 이동됩니다.
- 관리되지 않는 VM 및 화이트리스트 VM은 영향을 받지 않습니다.

NSX 적용 모드에서 VM 관리

NSX 적용 모드에서 성공적으로 온보딩된 VM 관리를 시작하려면 다음 단계를 따르십시오.

표 22-8. NSX 적용 모드의 NSX 관리 워크로드 V에 대한 마이크로 세분화 워크플로

작업	지침
<input type="checkbox"/> 워크로드 VM에 인바운드 액세스를 허용하려면 필요에 따라 DFW(분산 방화벽) 규칙을 생성합니다.	NSX 적용 모드의 NSX 관리 워크로드 VM에 대한 기본 연결 전략의 내용을 참조하십시오.
<input type="checkbox"/> 공용 클라우드 태그 또는 NSX-T Data Center 태그를 사용하여 워크로드 VM을 그룹화하고 마이크로 세분화를 설정합니다.	NSX 적용 모드에서 워크로드 VM에 대한 마이크로 세분화 설정의 내용을 참조하십시오. NSX-T Data Center 및 공용 클라우드 태그를 사용하여 VM 그룹화도 참조하십시오.

NSX 적용 모드의 NSX 관리 워크로드 VM에 대한 기본 연결 전략

전송 VPC/vNet에서 PCG를 배포하거나 계산 VPC/vNet을 전송 대상으로 연결하는 경우 NSX Cloud는 NSX 관리 워크로드 VM에 대한 기본 보안 정책 및 DFW 규칙을 생성합니다.

2개의 상태 비저장 규칙은 DHCP 액세스용이며 워크로드 VM에 대한 액세스에 영향을 미치지 않습니다.

2개의 상태 저장 규칙은 다음과 같습니다.

다음 정책 아래에서 NSX Cloud에 의해 생성된 DFW 규칙:	속성
cloud-stateful-cloud-<VPC/vNet ID>	
cloud-<VPC/vNet ID>-managed	동일한 VPC/vNet 내에서 VM에 대한 액세스를 허용합니다.
cloud-<VPC/vNet ID>-inbound	VPC/vNet 외부의 어느 위치에서나 NSX 관리 VM에 대한 액세스를 차단합니다.

참고 기본 규칙을 편집하지 마십시오.

기존 인바운드 규칙의 복사본을 생성하고, 소스 및 대상을 조정하고, **허용**으로 설정할 수 있습니다. 기본 **거절** 규칙 위에 **허용** 규칙을 배치합니다. 새 정책 및 규칙을 추가할 수도 있습니다. 지침에 대해서는 분산 방화벽 추가 를 참조하십시오.

NSX 적용 모드에서 워크로드 VM에 대한 마이크로 세분화 설정

관리 워크로드 VM에 대한 마이크로 세분화를 설정할 수 있습니다.

NSX 관리 워크로드 VM에 분산 방화벽 규칙을 적용하려면 다음을 수행합니다.

- 1 VM 이름이나 태그 또는 기타 멤버 자격 조건(예: 웹, 애플리케이션, DB 계층)을 사용하여 그룹을 생성합니다. 자세한 내용은 [그룹 추가](#) 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
-

참고 DFW 규칙은 VM에 할당된 태그에 따라 다릅니다. 이러한 태그는 적절한 공용 클라우드 사용 권한이 있는 모든 사용자가 수정할 수 있기 때문에 NSX-T Data Center는 이러한 사용자를 신뢰할 만하며, 해당 VM에 항상 올바른 태그가 지정되어 있음을 보장하고 감사하는 책임이 공용 클라우드 네트워크 관리자에게 있다고 가정합니다.

- 2 East-West 분산 방화벽 정책 및 규칙을 생성하여 앞서 만든 그룹에 적용합니다. [분산 방화벽 추가](#)의 내용을 참조하십시오.

이 마이크로 세분화는 인벤토리가 CSM에서 수동으로 다시 동기화되거나 공용 클라우드에서 CSM으로 변경 사항을 가져올 때 약 3분 이내에 적용됩니다.

기본 클라우드 적용 모드

기본 클라우드 적용 모드에서는 모든 워크로드 VM이 자동으로 NSX를 통해 관리됩니다. 여기에 설명된 워크플로를 따라 NSX-T Data Center에서 이러한 VM 관리를 시작하십시오.

참고 기본 클라우드 적용 모드의 워크로드 VM에서 모든 운영 체제가 지원됩니다.

기본 클라우드 적용 모드에서 VM 관리

기본 클라우드 적용 모드에서 NSX Cloud는 NSX-T Data Center 그룹 및 분산 방화벽 규칙을 활용하여 Microsoft Azure에서는 해당 애플리케이션 보안 그룹 및 네트워크 보안 그룹을, AWS에서는 보안 그룹을 생성합니다.

기본 클라우드 적용 모드에 온보딩된 VPC/vNet의 모든 워크로드 VM은 NSX를 통해 관리됩니다.

다음 워크플로를 따르십시오.

표 22-9. 기본 클라우드 적용 모드의 워크로드 VM에 대한 마이크로 세분화 워크플로

작업	지침
<input type="checkbox"/> NSX Manager에서 하나 이상의 그룹을 생성하여 공용 클라우드의 워크로드 VM을 포함합니다.	자세한 내용은 기본 클라우드 적용 모드에서 워크로드 VM에 대한 마이크로 세분화 설정 NSX-T Data Center 및 공용 클라우드 태그를 사용하여 VM 그룹화 도 참조하십시오.
<input type="checkbox"/> 공용 클라우드 워크로드 VM용으로 생성한 그룹에 적용되는 하나 이상의 보안 정책을 NSX Manager에서 생성합니다.	
<input type="checkbox"/> NSX-T 보안 정책을 통해 관리하려는 경우 CSM의 화이트리스트에서 워크로드 VM을 제거합니다.	
<input type="checkbox"/> CSM에서 공용 클라우드 계정을 다시 동기화합니다.	
<input type="checkbox"/> VPC/vNet에서 오류가 있는 경우 보안 정책 문제를 해결하기 위해 CSM의 세부 정보 보기로 전환합니다.	자세한 내용은 현재 제한 사항 및 일반적인 오류

기본 클라우드 적용 모드에서 워크로드 VM에 대한 마이크로 세분화 설정

기본 클라우드 적용 모드의 워크로드 VM에 대해 NSX Manager에서 보안 정책을 구성하려면 이 워크플로를 참조하십시오. 이 방식에서는 워크로드 VM에 NSX Tools를 설치하지 않습니다.

사전 요구 사항

전송 또는 계산 VPC/vNet이 기본 클라우드 적용 모드여야 합니다.

절차

- 1 NSX Manager에서 워크로드 VM에 대한 그룹을 편집하거나 생성합니다. 예를 들어 web, app, db로 시작하는 VM 이름은 별도의 세 개 그룹이 될 수 있습니다. 지침에 대해서는 [그룹 추가](#)를 참조하십시오. 공용 클라우드 태그를 사용하여 워크로드 VM용 그룹을 생성하는 방법에 대한 자세한 내용은 [NSX-T Data Center 및 공용 클라우드 태그를 사용하여 VM 그룹화](#)를 참조하십시오.

기준과 일치하는 워크로드 VM이 해당 그룹에 추가됩니다. 그룹화 기준과 일치하지 않는 VM은 AWS의 default 보안 그룹 및 Microsoft Azure의 vm-quarantine-sg 네트워크 보안 그룹에 배치됩니다.

참고 NSX Cloud에서 자동 생성된 그룹은 사용할 수 없습니다.

참고 DFW 규칙은 VM에 할당된 태그에 따라 다릅니다. 이러한 태그는 적절한 공용 클라우드 사용 권한이 있는 모든 사용자가 수정할 수 있기 때문에 NSX-T Data Center는 이러한 사용자를 신뢰할 만하며, 해당 VM에 항상 올바른 태그가 지정되어 있음을 보장하고 감사하는 책임이 공용 클라우드 네트워크 관리자에게 있다고 가정합니다.

- 2 NSX Manager의 **소스, 대상** 또는 **적용 대상** 필드에 그룹이 있는 DFW(분산 방화벽) 규칙을 생성합니다. 지침에 대해서는 **분산 방화벽 추가** 를 참조하십시오.

참고 공용 클라우드 워크로드 VM에서는 상태 저장 정책만 지원됩니다. 상태 비저장 정책은 NSX Manager에서 생성할 수 있지만 공용 클라우드 워크로드 VM이 포함된 그룹과 일치하지 않습니다.

- 3 CSM에서 NSX를 통해 관리하려는 해당 VM을 화이트리스트에서 제거합니다. 지침에 대해서는 **VM을 화이트리스트에 추가하거나 화이트리스트에서 제거하는 방법** 를 참조하십시오.

참고 화이트리스트는 CSM에 공용 클라우드 인벤토리를 추가하는 즉시 **day-0** 워크플로에서 권장되는 수동 단계입니다. VM을 화이트리스트에 추가하지 않은 경우 화이트리스트에서 제거할 필요가 없습니다.

- 4 공용 클라우드에 일치 항목이 있는 그룹 및 DFW 규칙의 경우 다음 작업이 자동으로 수행됩니다.

- a AWS에서 NSX Cloud가 nsx-`<NSX GUID>`와 이름이 같은 새 보안 그룹을 만듭니다.
- b Microsoft Azure에서 NSX Cloud는 NSX Manager에서 생성된 그룹에 해당하는 ASG(애플리케이션 보안 그룹)와 그룹화된 워크플로 VM과 일치하는 DFW 규칙에 해당하는 NSG(네트워크 보안 그룹)를 생성합니다.

참고 NSX Cloud는 NSX Manager 및 공용 클라우드 그룹과 DFW 규칙을 30초 간격으로 동기화합니다.

- 5 CSM에서 공용 클라우드 계정을 다시 동기화합니다.

- a CSM에 로그인하고 공용 클라우드 계정으로 이동합니다.
- b 공용 클라우드 계정에서 **작업 > 계정 다시 동기화**를 클릭합니다. 다시 동기화가 완료될 때까지 기다립니다.
- c VPC/vNet으로 이동하고 빨간색 오류 표시기를 클릭합니다. 그러면 인스턴스 보기로 이동합니다.
- d 그리드로 표시되는 경우 보기를 [세부 정보]로 전환하고, [규칙 인식] 열에서 **실패**를 클릭하여 오류를 확인합니다(있는 경우).

다음에 수행할 작업

현재 제한 사항 및 일반적인 오류 항목을 참조하십시오.

현재 제한 사항 및 일반적인 오류

이러한 알려진 제한 사항 및 일반적인 오류를 참조하여 기본 클라우드 적용 모드에서 공용 클라우드 워크로드 VM을 관리하는 문제를 해결하십시오.

참고 공용 클라우드에서 설정되는 제한은 다음과 같습니다.

- 워크로드 VM에 적용할 수 있는 보안 그룹의 수
- 워크로드 VM에 대해 실현할 수 있는 규칙의 수
- 보안 그룹당 실현할 수 있는 규칙의 수
- 보안 그룹 할당 범위. 예를 들어, Microsoft Azure의 NSG(네트워크 보안 그룹) 범위는 해당 지역으로 제한되지만 AWS의 SG(보안 그룹) 범위는 해당 VPC로 제한됩니다.

이러한 제한에 대한 자세한 내용은 공용 클라우드 설명서를 참조하십시오.

현재 제한 사항

현재 릴리스에는 워크로드 VM의 DFW 규칙에 대한 다음과 같은 제한 사항이 있습니다.

- 중첩된 그룹은 지원되지 않습니다.
- VM 및/또는 IP 주소가 멤버로 포함되지 않은 그룹은 지원되지 않습니다. 예를 들어 세그먼트 또는 논리적 포트 기반 기준은 지원되지 않습니다.
- 소스 및 대상이 둘 다 IP 주소 또는 CIDR 기반 그룹인 경우는 지원되지 않습니다.
- 소스와 대상이 둘 다 "임의"인 경우는 지원되지 않습니다.
- **Applied_To** 그룹은 소스 또는 대상 또는 소스 + 대상 그룹이 될 수 있습니다. 다른 옵션은 지원되지 않습니다.
- 로컬 VPC/vNet 규칙 적용만 지원됩니다. 여러 VPC/vNet에 걸쳐 있는 그룹을 NSX Manager에서 생성할 수 있습니다. 그러나 이러한 규칙의 인식 기능은 VPC/vNet에서만 작동합니다. 크로스 VPC/vNet DFW 규칙은 인식되지 않습니다.

- TCP와 UDP가 모두 지원됩니다.

참고 AWS에만 해당:

AWS VPC에서 워크로드 VM에 대해 생성된 거부 규칙이 AWS에서는 인식되지 않습니다. AWS에서는 모든 항목이 기본적으로 블랙리스트에 추가되기 때문입니다. 이로 인해 NSX-T Data Center에서 다음 결과가 발생합니다.

- VM1과 VM2 사이에 거부 규칙이 있는 경우 거부 규칙 때문이 아니라 기본 AWS 동작으로 인해 VM1 및 VM2 간에 트래픽이 허용되지 않습니다. 해당 거부 규칙은 AWS에서 인식되지 않습니다.
- 규칙 1이 규칙 2보다 높은 우선 순위를 가진 동일한 VM에 대해 NSX Manager에서 다음 두 가지 규칙이 생성되었다고 가정합니다.
 - a VM1 - VM2 SSH 거부
 - b VM1 - VM2 SSH 허용

거부 규칙은 AWS에서 인식되지 않으며, SSH 허용 규칙이 인식되기 때문에 무시됩니다. 이러한 동작은 예상과 다르지만, 기본 AWS 동작 때문에 제한이 발생합니다.

일반 오류 및 해결 방법

오류: VM에 적용된 NSX 정책이 없습니다.

이 오류가 표시되는 경우 특정 VM에 DFW 규칙이 적용되지 않습니다. 이 VM을 포함하려면 NSX Manager에서 규칙 또는 그룹을 편집하십시오.

오류: 상태 비저장 NSX 규칙이 지원되지 않습니다.

이 오류가 표시되면 상태 비저장 보안 정책에서 공용 클라우드 워크로드 VM에 대해 DFW 규칙을 추가한 것입니다. 이것은 지원되지 않습니다. 상태 저장 모드에서 새 보안 정책을 생성하거나 기존 보안 정책을 사용합니다.

NSX Cloud에서 지원되는 NSX-T Data Center 기능

NSX Cloud는 NSX-T Data Center에서 논리적 네트워킹 엔티티를 생성하여 공용 클라우드 VPC 또는 VNet에 대한 네트워크 토폴로지를 생성합니다.

이 목록을 자동 생성되는 항목과 공용 클라우드에 적용할 때 NSX-T Data Center 기능을 사용하는 방법에 대한 참조로 사용하십시오.

NSX Manager 구성

PCG가 성공적으로 배포된 후 생성된 논리적 엔티티에 대한 자세한 내용은 " NSX-T Data Center 설치 가이드" 에서 "자동 생성된 NSX-T 논리적 엔티티"를 참조하십시오.

중요 이러한 자동 생성된 엔티티를 편집하거나 삭제하지 마십시오.

참고 Windows 워크로드 VM의 일부 기능에 액세스할 수 없으면, Windows 방화벽 설정이 올바르게 구성되어 있는지 확인하십시오.

표 22-10.

NSX-T Data Center 기능	세부 정보	NSX Cloud 참고
세그먼트 또는 논리적 스위치	장 4 세그먼트 항목을 참조하십시오.	관리형 VM이 연결된 모든 공용 클라우드 서브넷에 대해 세그먼트가 생성됩니다. 이 세그먼트는 하이브리드 세그먼트입니다.
게이트웨이 또는 논리적 라우터	장 2 Tier-0 게이트웨이 및 장 3 Tier-1 게이트웨이를 참조하십시오.	PCG가 전송 VPC 또는 VNet에 배포되면 NSX Cloud에 의해 Tier-0 논리적 라우터가 자동으로 생성됩니다. 전송 VPC/VNet에 연결되면 Tier-1 라우터가 각 계산 VPC/VNet에 대해 생성됩니다.
IPFIX	IPFIX 구성의 내용을 참조하십시오.	<ul style="list-style-type: none"> ■ IPFIX는 NSX Cloud의 UDP 포트 4739에서만 지원됩니다. ■ 스위치 및 DFW IPFIX: 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.
포트 미러링	포트 미러링 세션 모니터링의 내용을 참조하십시오.	<p>포트 미러링은 현재 릴리스의 AWS에서만 지원됩니다.</p> <ul style="list-style-type: none"> ■ NSX Cloud의 경우, 도구 > 포트 미러링 세션에서 포트 미러링을 구성합니다. ■ L3SPAN 포트 미러링만 지원됩니다. ■ 수집기가 소스 워크로드 VM과 동일한 VPC에 있어야 합니다.
게이트웨이 방화벽	게이트웨이 방화벽 구성 항목을 참조하십시오.	Tier-0 게이트웨이에서만 지원됩니다.

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.

참고 DFW 규칙은 VM에 할당된 태그에 따라 다릅니다. 이러한 태그는 적절한 공용 클라우드 사용 권한이 있는 모든 사용자가 수정할 수 있기 때문에 NSX-T Data Center는 이러한 사용자를 신뢰할 만하며, 해당 VM에 항상 올바른 태그가 지정되어 있음을 보장하고 감사하는 책임이 공용 클라우드 네트워크 관리자에게 있다고 가정합니다.

태그 용어

NSX Manager에서 **태그**란 공용 클라우드 컨텍스트에서 **값**으로 알려진 것을 말합니다. 공용 클라우드 태그의 **키**는 NSX Manager에서 **범위**라고 합니다.

태그 구성 요소	
범위	키
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
 - azure:transit_vnet_name
 - azure:transit_vnet_rg
 - aws:account
 - aws:availabilityzone
 - aws:region
 - aws:vpc
 - aws:subnet
 - aws:transit_vpc

- **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:`, AWS에서 검색되었음을 나타내기 위해 접두사 `dis:aws`가 붙습니다.

공용 클라우드의 태그를 변경하면 변경 내용이 3분 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 22-11. 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: ■ azure:subscription_id ■ azure:region ■ azure:vm_rg ■ azure:vnet_name ■ azure:vnet_rg ■ aws:vpc ■ aws:availability zone	범위(키): 20자 태그(값): 65자 최대 허용: 5	읽기 전용	읽기 전용
검색됨	VNet에서 가져온 Microsoft Azure 태그에 대한 접두사: dis:azure: VPC에서 가져온 AWS 태그에 대한 접두사: dis:aws:	범위(키): 20자 태그(값): 65자 최대 허용: 무제한 참고 문자에 대한 제한에서 접두사 dis:<공용 클라우드 이름> 은 제외됩니다. 이러한 제한을 초과하는 태그는 NSX Manager에 반영되지 않습니다. 접두사 nsx 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. ■ 범위(키) 접두사 dis:azure: 또는 dis:aws: ■ 시스템 태그와 동일한 범위(키)	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 22-12.

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=value2	아니요(키가 20자를 초과함)	없음
tag3=AbcdefghijklmnopqrstuvwxyzAb23690hgjgytrespwqacvbcdefghijklmnopqrstuvwxyz	아니요(값이 65자를 초과함)	없음
nsx.name=Tester	아니요(키에 접두사 nsx가 있음)	없음

NSX Manager에서 태그를 사용하는 방법

- VM용 태그 관리의 내용을 참조하십시오.
- 개체 검색의 내용을 참조하십시오.
- 그룹 추가의 내용을 참조하십시오.
- NSX 적용 모드에서 워크로드 VM에 대한 마이크로 세분화 설정의 내용을 참조하십시오.

기본 클라우드 서비스 사용

다음 기본 클라우드 서비스는 NSX Manager에서 공용 클라우드 워크로드 VM과 함께 사용하도록 지원됩니다.

PCG를 배포하면 지원되는 각 기본 클라우드 서비스에 대해 NSX Manager에서 그룹이 생성됩니다.

현재 지원되는 공용 클라우드 서비스에 대해 다음 그룹이 생성됩니다.

- aws-dynamo-db-service-endpoint
- aws-elb-service-endpoint
- aws-rds-service-endpoint
- aws-s3-service-endpoint
- azure-cosmos-db-service-endpoint
- azure-load-balancer-service-endpoint
- azure-sql-service-endpoint
- azure-storage-service-endpoint

이러한 기본 클라우드 서비스를 사용하려면 필요에 따라 규칙의 소스 또는 대상 필드에 기본 클라우드 서비스 그룹이 포함된 DFW 정책을 생성합니다.

DFW 규칙은 기본 클라우드 서비스에 없는 VM에 적용됩니다.

참고 NSX Tools에서 워크로드를 관리하는 NSX 적용 모드에서는 현재 Microsoft Azure의 기본 클라우드 서비스를 지원하지 않습니다.

현재 제한 사항

ENDPOINT			서비스를 대상으로 사용하는 DFW 규칙		서비스를 소스로 사용하는 DFW 규칙	
공용 클라우드	서비스	범위	VM에 적용됩니다 니까?	서비스에 적용됩니 까?	서비스에 적용됩니 까?	VM에 적용됩 니까?
Microsoft Azure	BLOB 스토리지	글로벌	예	아니오	아니오	예
	Cosmos DB					
	SQL					
	로드 밸런서					
AWS	S3	VPC 로컬	예	아니오	아니오	예
	Dynamo DB					
	RDS					
	ELB					

공용 클라우드에 대한 서비스 삽입

NSX Cloud는 NSX 관리 워크로드 VM에 대해 공용 클라우드의 타사 서비스 사용을 지원합니다.

공용 클라우드 워크로드 VM에 대해 서비스 삽입을 사용하려면 NSX-T Data Center가 아닌 공용 클라우드에서 서비스 장치를 호스팅해야 합니다. 전용 VPC/VNet에서 서비스 장치를 호스팅하는 것이 좋습니다.

서비스 삽입을 사용하도록 설정하려면 전용 VPC 또는 VNet에서 PCG가 배포되어 있어야 합니다.

NSX 관리 워크로드 VM에 대해 서비스 삽입을 허용하기 위한 일회성 구성 개요는 다음과 같습니다.

표 22-13. 공용 클라우드의 NSX 관리 워크로드 VM에 대한 서비스 삽입에 필요한 구성 개요

작업 수행 시 기	작업	지침
초기 설정에 대해 한 번	가능한 PCG를 배포한 전용 VPC 또는 VNet의 공용 클라우드에서 서비스 장 치를 설정합니다.	타사 서비스 장치 및 공용 클라 우드와 관련된 지침을 참조하 십시오.
	NSX-T Data Center에 타사 서비스를 등록합니다.	서비스 정의 및 해당 가상 끝점 생성 항목을 참조하십시오.
	서비스 장치에 의한 서비스 삽입에만 사용할 /32 VSIP(가상 서비스 IP 주소)를 사용하여 서비스의 가상 인스턴스 끝점을 생성합니다. VSIP는 VPC 또는 VNet 의 CIDR 범위와 충돌하지 않아야 합니다. 이 VSIP는 BGP를 통해 PCG로 보급 됩니다.	서비스 정의 및 해당 가상 끝점 생성 항목을 참조하십시오.

표 22-13. 공용 클라우드의 NSX 관리 워크로드 VM에 대한 서비스 삽입에 필요한 구성 개요 (계속)

작업 수행 시기	작업	지침
	서비스 장치와 PCG 간에 IPSec VPN 터널을 생성합니다.	IPSec VPN 세션 설정 항목을 참조하십시오.
	PCG와 서비스 장치 사이에 BGP를 구성하고 서비스 장치에서 VSIP를, PCG에서 기본 경로(0.0.0.0/0)를 보급합니다.	BGP 및 경로 재배포 구성 항목을 참조하십시오.
	참고 현재 릴리스에서는 서비스 삽입이 북-남 트래픽에만 지원됩니다.	
필요할 때마다	일회성 구성이 완료된 후 NSX 관리 워크로드 VM에서 VSIP로 선택적 트래픽을 재라우팅하도록 리디렉션 규칙을 설정합니다. 이러한 규칙은 PCG의 업링크 포트에 적용됩니다.	리디렉션 규칙 설정의 내용을 참조하십시오.

절차

1 서비스 정의 및 해당 가상 끝점 생성

NSX Manager API를 사용하여 공용 클라우드의 서비스 장치에 대한 서비스 정의 및 가상 끝점을 생성해야 합니다.

2 IPSec VPN 세션 설정

PCG와 서비스 장치 사이에 IPSec VPN 세션을 설정합니다.

3 BGP 및 경로 재배포 구성

IPSec VPN 터널을 통해 PCG와 서비스 장치 사이에 BGP를 구성합니다.

4 리디렉션 규칙 설정

리디렉션 규칙은 요구 사항에 따라 조정될 수 있습니다.

서비스 정의 및 해당 가상 끝점 생성

NSX Manager API를 사용하여 공용 클라우드의 서비스 장치에 대한 서비스 정의 및 가상 끝점을 생성해야 합니다.

사전 요구 사항

공용 클라우드의 서비스 장치에 대한 가상 끝점 역할을 수행할 /32 예약된 IP 주소를 선택합니다(예: 100.100.100.100/32). 이는 VSIP(가상 서비스 IP)라고 합니다.

참고고가용성 쌍으로 서비스 장치를 배포한 경우 다른 서비스 정의를 생성하지 않고 BGP 구성 중에 PCG로 보급할 때 동일한 VSIP를 사용합니다.

절차

- 1 서비스 장치에 대한 서비스 정의를 생성하려면 인증을 위한 NSX Manager 자격 증명을 사용하여 다음 API 호출을 실행합니다.

```
POST https://{NSX Manager-IP}/policy/api/v1/enforcement-points/default/service-definitions
```

요청 예:

```
{
  "resource_type": "ServiceDefinition",
  "description": "NS-Service",
  "display_name": "Service_Appliance1",
  "attachment_point": [
    "TIER0_LR"
  ],
  "transports": [
    "L3_ROUTED"
  ],
  "functionalities": [
    "NG_FW", "BYOD"
  ],
  "on_failure_policy": "ALLOW",
  "implementations": [
    "NORTH_SOUTH"
  ],
  "vendor_id" : "Vendor1"
}
```

응답 예:

```
{
  "resource_type": "ServiceDefinition",
  "description": "NS-Service",
  "id": "33890153-6eea-4c9d-8e34-7b6532b9d65c",
  "display_name": "Service_Appliance1",
  "attachment_point": [
    "TIER0_LR"
  ],
  "transports": [
    "L3_ROUTED"
  ],
  "functionalities": [
    "NG_FW", "BYOD"
  ],
  "vendor_id": "Vendor1",
  "on_failure_policy": "ALLOW",
  "implementations": [
    "NORTH_SOUTH"
  ],
  "_create_time": 1540424262137,
  "_last_modified_user": "nsx_policy",
  "_system_owned": false,
}
```

```

    "_protection": "REQUIRE_OVERRIDE",
    "_last_modified_time": 1540424262137,
    "_create_user": "nsx_policy",
    "_revision": 0
  }

```

- 2 서비스 장치에 대한 가상 끝점을 생성하려면 인증을 위한 NSX Manager 자격 증명을 사용하여 다음 API 호출을 실행합니다.

```

PATCH https://{NSX Manager-IP}policy/api/v1/infra/tier-0s/<tier-0 router ID>/locale-
services/cloud/endpoints/virtual-endpoints/Service_Appliance1_Endpoint

```

요청 예:

```

{
  "resource_type": "VirtualEndpoint",
  "display_name": "Service_Appliance1_Endpoint",
  "target_ips": [
    {
      "ip_addresses": [
        "100.100.100.100"
      ],
      "prefix_length": 32
    }
  ],
  "service_names": [
    "Service_Appliance1"
  ]
}

```

응답 예:

```
200 OK
```

참고 1단계의 display_name이 2단계의 service_names 와 일치해야 합니다.

다음에 수행할 작업

IPSec VPN 세션 설정

IPSec VPN 세션 설정

PCG와 서비스 장치 사이에 IPSec VPN 세션을 설정합니다.

사전 요구 사항

- 하나 또는 한 HA 쌍의 PCG를 전송 VPC/VNet에서 배포해야 합니다.
- 서비스 장치를 공용 클라우드, 가능하면 전송 VPC/VNet에서 설정해야 합니다.

절차

- 1 **네트워킹 > VPN**으로 이동합니다.

- 2 IPsec 유형의 **VPN 서비스**를 추가하고 NSX Cloud와 관련된 다음 구성 옵션을 확인합니다. 자세한 내용은 [IPsec VPN 서비스 추가](#)의 내용을 참조하십시오.

옵션	설명
이름	이 VPN 서비스의 이름은 로컬 끝점 및 IPsec VPN 세션을 설정하는 데 사용됩니다. 이를 적어 둡니다.
서비스 유형	이 값이 IPsec로 설정되었는지 확인합니다.
Tier-0 게이트웨이	전송 VPC/VNet에 대해 자동 생성된 Tier-0 게이트웨이를 선택합니다. 해당 이름에 VPC/VNet ID(예: cloud-t0-vpc-6bcd2c13)가 포함되어 있습니다.

- 3 PCG에 대한 **로컬 끝점**을 추가합니다. 로컬 끝점의 IP 주소는 전송 VPC/VNet에 배포된 PCG에 대한 태그 nsx:local_endpoint_ip의 값입니다. 이 값에 대한 전송 VPC/VNet에 로그인합니다. NSX Cloud와 관련된 다음 구성을 확인하고 자세한 내용은 [로컬 끝점 추가](#)의 내용을 참조하십시오.

옵션	설명
이름	로컬 끝점 이름은 IPsec VPN 세션을 설정하는 데 사용됩니다. 이를 적어 둡니다.
VPN 서비스	2단계에서 추가한 VPN 서비스를 선택합니다.
IP 주소	AWS 콘솔 또는 Microsoft Azure 포털에 로그인하여 이 값을 찾습니다. PCG의 업링크 인터페이스에 적용된 태그 nsx:local_endpoint_ip의 값입니다.

- 4 가능하면 전송 VPC/VNet에서 호스팅되는 공용 클라우드의 서비스 장치와 PCG 사이에 **경로 기반 IPsec 세션**을 생성합니다.

옵션	설명
유형	이 값이 경로 기반 으로 설정되었는지 확인합니다.
VPN 서비스	2단계에서 추가한 VPN 서비스를 선택합니다.
로컬 끝점	3단계에서 생성한 로컬 끝점을 선택합니다.
원격 IP	서비스 장치의 개인 IP 주소를 입력합니다. 참고 공용 IP 주소를 사용하여 서비스 장치에 액세스할 수 있는 경우 로컬 끝점 IP(보조 IP라고도 함)에 대한 공용 IP 주소를 PCG의 업링크 인터페이스에 할당합니다.
터널 인터페이스	이 서브넷은 VPN 터널에 대한 서비스 장치 서브넷과 일치해야 합니다. VPN 터널에 대한 서비스 장치에서 설정한 서브넷 값을 입력하거나 여기에 입력한 값을 확인하고 서비스 장치에서 VPN 터널을 설정할 때 동일한 서브넷이 사용되었는지 확인합니다. 참고 이 터널 인터페이스에서 BGP를 구성합니다. BGP 및 경로 재배포 구성 의 내용을 참조하십시오.
원격 ID	공용 클라우드에서 서비스 장치의 개인 IP 주소를 입력합니다.
IKE 프로파일	IPsec VPN 세션은 IKE 프로파일과 연결되어야 합니다. 프로파일을 생성한 경우 드롭다운 메뉴에서 선택합니다. 기본 프로파일을 사용할 수도 있습니다.

다음에 수행할 작업

BGP 및 경로 재배포 구성

BGP 및 경로 재배포 구성

IPSec VPN 터널을 통해 PCG와 서비스 장치 사이에 BGP를 구성합니다.

PCG와 서비스 장치 사이에 설정한 IPSec VPN 터널 인터페이스에서 BGP 인접 항목을 설정합니다. 자세한 내용은 [BGP 구성](#)의 내용을 참조하십시오.

서비스 장치에서 이와 유사하게 BGP를 구성해야 합니다. 자세한 내용은 공용 클라우드의 특정 서비스에 대한 설명서를 참조하십시오.

다음으로 경로 재배포를 다음과 같이 설정합니다.

- PCG는 기본 경로(0.0.0.0/0)를 서비스 장치에 보급합니다.
- 서비스 장치는 VSIP를 PCG에 보급합니다. 이는 서비스를 등록할 때 사용된 동일한 IP 주소입니다. 서비스 정의 및 해당 가상 끝점 생성의 내용을 참조하십시오.

참고 서비스 장치가 고가용성 쌍으로 배포되는 경우 두 서비스 장치에서 동일한 VSIP를 보급합니다.

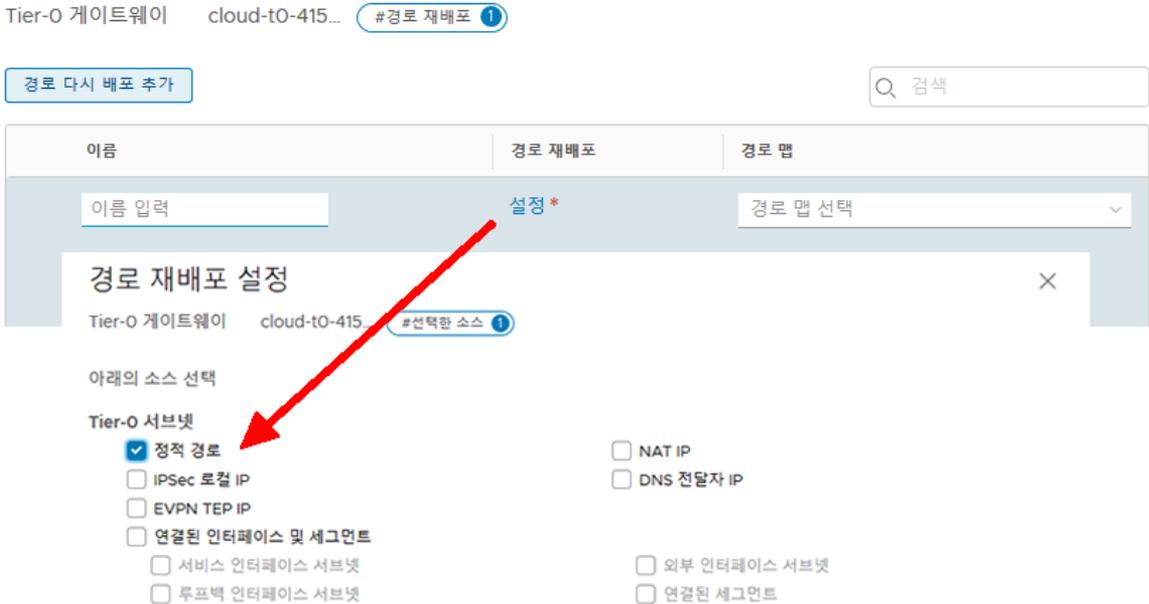
절차

- 1 **네트워킹 > Tier-0 게이트웨이**로 이동합니다.
- 2 cloud-t0-vpc-6bcd2c13과 같은 이름의 전송 VPC/VNet에 대해 자동 생성된 Tier-0 게이트웨이를 선택하고 **편집**을 클릭합니다.
- 3 **BGP** 섹션 아래에서 **BGP 인접 항목** 옆의 번호 또는 아이콘을 클릭합니다.
- 4 다음과 같은 구성을 확인합니다.

옵션	설명
IP 주소	PCG와 서비스 장치 사이에 VPN에 대한 서비스 장치 터널 인터페이스에 구성된 IP 주소를 사용합니다.
원격 AS 번호	이 번호는 공용 클라우드의 서비스 장치의 AS 번호와 일치해야 합니다.
경로 필터	PCG에서 서비스 장치로 기본 경로(0.0.0.0/0)를 보급하도록 출력 필터를 설정합니다.

5 경로 재배포 섹션의 Tier-0 게이트웨이에서 정적 경로를 사용하도록 설정합니다.

경로 재배포 설정



다음에 수행할 작업

리디렉션 규칙 설정

리디렉션 규칙 설정

리디렉션 규칙은 요구 사항에 따라 조정될 수 있습니다.

초기 설정이 완료된 후 서비스 장치 전체에서 NSX 관리 워크로드 VM에 대한 다양한 유형의 트래픽을 재라우팅하는 데 필요한 리디렉션 규칙을 생성 및 편집할 수 있습니다.

사전 요구 사항

리디렉션 규칙을 생성하려면 모든 서비스 삽입 설정을 완료해야 합니다.

절차

- 1 보안 > North South 방화벽 > 네트워크 검사(N-S)로 이동합니다.
- 2 정책 추가를 클릭합니다.

옵션	설명
이름:	정책을 설명하는 이름을 제공합니다(예: Azure VM에 대한 북-남 서비스 삽입).
리디렉션 대상:	서비스를 등록할 때 이 서비스 장치에 대해 생성한 가상 끝점의 이름을 선택합니다. 서비스 정의 및 해당 가상 끝점 생성의 내용을 참조하십시오.
적용 대상:	PCG의 Tier-0 게이트웨이를 선택합니다.

3 새 정책을 선택하고 **규칙 추가**를 클릭합니다. 서비스 삽입과 관련된 다음 값을 확인합니다.

옵션	설명
소스	트래픽을 리디렉션해야 하는 서브넷 그룹(예: NSX 관리 워크로드 VM의 그룹)을 선택합니다.
대상	대상 IP 주소 또는 서비스 목록을 선택합니다. 서비스 장치 전체에서 라우팅할 Google 을 예로 들 수 있습니다.
적용 대상	활성 및 대기 PCG의 업링크 포트를 선택합니다.
작업	리디렉션을 선택합니다.

NSX 관리 VM에서 NAT를 사용하도록 설정

NSX Cloud는 NSX 관리 VM에서 NAT 사용을 지원합니다.

공용 클라우드 태그를 사용하여 NSX 관리 VM의 VM에서 North-South 트래픽을 사용하도록 설정할 수 있습니다.

NAT를 사용하도록 설정할 NSX 관리 VM에서 다음 태그를 적용합니다.

표 22-14.

키	값
<code>nsx.publicip</code>	공용 클라우드의 공용 IP 주소(예: 50.1.2.3)

참고 여기에 제공하는 공용 IP 주소는 무료로 사용할 수 있어야 하며 NAT를 사용하도록 설정할 워크로드 VM을 비롯한 모든 VM에 할당되지 않아야 합니다. 이전에 기타 인스턴스 또는 개인 IP 주소와 연결되었던 공용 IP 주소를 할당하는 경우 NAT가 작동하지 않습니다. 이 경우 공용 IP 주소를 할당 취소합니다.

이 태그가 적용된 후 워크로드 VM은 인터넷 트래픽에 액세스할 수 있습니다.

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.

다음을 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 <server-IP-address> proto udp level info
messageid FIREWALL-PKTLOG
```

이 설정이 완료되면 PCG의 /var/log/syslog에서 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>
```

NSX 적용 모드에서 VPN 설정

온-프레미스 NSX-T Data Center 배포에서 자동으로 생성된 Tier-0 게이트웨이로 나타나는 PCG를 사용하여 VPN을 설정할 수 있습니다. 이러한 지침은 NSX 적용 모드에서 관리되는 워크로드 VM에만 해당됩니다.

여기에서 설명하는 추가 단계를 수행하여 VPN을 설정하려면 NSX Manager에서 Tier-0 게이트웨이를 사용하는 것과 동일한 방식으로 PCG를 사용합니다. 동일한 공용 클라우드나 다른 공용 클라우드에 또는 온-프레미스 게이트웨이나 라우터를 사용하여 배포된 PCG 간에 VPN 터널을 만들 수 있습니다. NSX-T Data Center의 VPN 지원에 대한 자세한 내용은 [장 5 VPN\(Virtual Private Network\)](#)를 참조하십시오.

사전 요구 사항

- VPC/VNet에 배포된 하나의 PCG 또는 PCG의 HA 쌍이 있는지 확인합니다.
- 원격 피어가 경로 기반 VPN 및 BGP를 지원하는지 확인합니다.

절차

- 1 공용 클라우드에서 PCG에 대한 NSX 할당 로컬 끝점을 찾고 필요한 경우 공용 IP 주소를 할당합니다.
 - a 공용 클라우드의 PCG 인스턴스로 이동한 후 [태그]로 이동합니다.
 - b `nsx.local_endpoint_ip` 태그의 값 필드에 있는 IP 주소를 기록해 둡니다.
 - c (선택 사항) VPN 터널에 공용 IP가 필요한 경우, 예를 들어 VPN을 다른 공용 클라우드 또는 온-프레미스 NSX-T Data Center 배포로 설정하려는 경우 다음을 수행합니다.
 - 1 PCG 인스턴스의 업링크 인터페이스로 이동합니다.
 - 2 b단계에서 적어둔 `nsx.local_endpoint_ip` IP 주소에 공용 IP 주소를 연결합니다.
 - d (선택 사항) PCG 인스턴스의 HA 쌍이 있는 경우 a 및 b단계를 반복하고 필요한 경우 c단계에 설명된 대로 공용 IP 주소를 연결합니다.

2 NSX Manager에서 cloud-t0-vpc/vnet-<vpc/vnet-id>와 같이 이름이 지정된 Tier-O 게이트웨이로 표시되는 PCG에 대해 IPsec VPN을 사용하도록 설정하고, 이 Tier-O 게이트웨이의 끝점과 원하는 VPN 피어의 원격 IP 주소 사이에 경로 기반 IPsec 세션을 생성합니다. 자세한 내용은 **IPsec VPN 서비스 추가**의 내용을 참조하십시오.

- a **네트워킹 > VPN > VPN 서비스 > 서비스 추가 > IPsec**으로 이동합니다. 다음 세부 정보를 제공합니다.

옵션	설명
이름	VPN 서비스를 설명하는 이름(예: <VPC-ID>-AWS_VPN 또는 <VNet-ID>-AZURE_VPN)을 입력합니다.
Tier0/Tier1 게이트웨이	공용 클라우드의 PCG에 대한 Tier-O 게이트웨이를 선택합니다.

- b **네트워킹 > VPN > 로컬 끝점 > 로컬 끝점 추가**로 이동합니다. 다음 정보를 제공하고 **로컬 끝점 추가**에서 자세한 내용을 참조하십시오.

참고 PCG 인스턴스의 HA 쌍이 있는 경우 공용 클라우드에서 연결된 해당 로컬 끝점 IP 주소를 사용하여 각 인스턴스에 대한 로컬 끝점을 생성합니다.

옵션	설명
이름	로컬 끝점을 설명하는 이름을 입력합니다(예: <VPC-ID>-PCG-preferred-LE 또는 <VNET-ID>-PCG-preferred-LE).
VPN 서비스	2a단계에서 생성한 PCG의 Tier-O 게이트웨이에 대한 VPN 서비스를 선택합니다.
IP 주소	1b단계에서 적어 둔 PCG의 로컬 끝점 IP 주소 값을 입력합니다.

- c **네트워킹 > VPN > IPsec 세션 > IPsec 세션 추가 > 경로 기반**으로 이동합니다. 다음 정보를 제공하고 **경로 기반 IPsec 세션 추가**에서 자세한 내용을 참조하십시오.

참고 VPC에 배포된 PCG와 VNet에 배포된 PCG 간에 VPN 터널을 생성하는 경우 VPC에 있는 각 PCG의 로컬 끝점과 VNet에 있는 PCG의 원격 IP 주소에 대해 터널을 생성하고, 반대로 VNet의 PCG에서 VPC에 있는 PCG의 원격 IP 주소로의 터널을 생성해야 합니다. 활성 및 대기 PCG에 대해 별도의 터널을 생성해야 합니다. 이로 인해 두 공용 클라우드 간에 IPsec 세션의 풀 메시지가 생성됩니다.

옵션	설명
이름	IPsec 세션을 설명하는 이름을 입력합니다(예: <VPC--ID>-PCG1-to-remote_edge).
VPN 서비스	2a단계에서 생성한 VPN 서비스를 선택합니다.
로컬 끝점	2b단계에서 생성한 로컬 끝점을 선택합니다.
원격 IP	VPN 터널을 생성하는 원격 피어의 공용 IP 주소를 입력합니다.

옵션	설명
	참고 DirectConnect 또는 ExpressRoute를 사용하는 경우처럼 개인 IP 주소에 연결할 수 있는 경우 원격 IP가 개인 IP 주소일 수 있습니다.
터널 인터페이스	터널 인터페이스를 CIDR 형식으로 입력합니다. 원격 피어에서 IPSec 세션을 설정하려면 동일한 서브넷을 사용해야 합니다.

2a단계.

VPN 서비스

이름	서비스 유형	Tier0/Tier1 게이트웨이	세션	상태
<VPC-ID>-AWS_VPN	IPSec	cloud-to-vpc-073617880a9622d93	1	성공

설명: VPN service on AWS Transit VPC ID vpc-073617880a9622d93

IKE 로그 수준: 정보

세션 동기화: 사용

태그: 0

2b단계.

로컬 끝점

이름	VPN 서비스	IP 주소	사이드 인증서	세션	상태
<VPC-ID>-PCG-preferred-LE	<VPC-ID>-AWS_VPN	10.99.3.35	설정되지 않음	1	성공

설명: 설정되지 않음

신뢰할 수 있는 CA 인증서: 설정되지 않음

태그: 0

2c단계.

IPSec 세션

이름	유형	VPN 서비스	로컬 끝점	원격 IP	상태	경보
<VPC-ID>-PCG1-to-remote_edge	경로 기반	<VPC-ID>-AWS_VPN	<VPC-ID>-PCG-preferred-LE	3.213.92.220	종료	0

VPN 피어의 IP 주소입니다.

규정 준수 제품군: 없음

인증 모드: PSK

사건 공유 키:

고급 속성

IKE 프로파일: nsx-default-l3vpn-ike-profile

IPSec 프로파일: nsx-default-l3vpn-tunnel-profile

3 2단계에서 설정한 IPsec VPN 터널 인터페이스에 BGP 인접 네트워크를 설정합니다. 자세한 내용은 BGP 구성의 내용을 참조하십시오.

- a 네트워킹 > Tier-0 게이트웨이로 이동합니다.
- b IPsec 세션을 생성한 자동 생성 Tier-0 게이트웨이를 선택하고 **편집**을 클릭합니다.
- c BGP 섹션 아래에서 **BGP 인접 항목** 옆의 번호 또는 아이콘을 클릭하고 다음 세부 정보를 제공합니다.

옵션	설명
IP 주소	VPN 피어에 대한 IPsec 세션의 터널 인터페이스에 구성된 원격 VTI의 IP 주소를 사용합니다.
원격 AS 번호	이 숫자는 원격 피어의 AS 번호와 일치해야 합니다.

Tier-0 게이트웨이

게이트웨이 추가 > 모두 확장 이름, 경

	Tier-0 게이트웨이 이름	HA 모드	연결된 Tier-1 게이트웨이	연결된 세그먼트
▼	BGP			
	로컬 AS	1000	SR iBGP 간	● 켜짐
	BGP	● 켜짐	ECMP	● 켜짐
	정상적인 다시 시작	도우미만	다중 경로 완화	● 켜짐
	정상 다시 시작 타이머	180 초	정상 다시 시작 부실 타이머	600 초
	경로 집계	0	BGP 인접 항목	1

3단계.

BGP 인접 항목

Tier-0 게이트웨이 cloud-t0-415... #인접 항목

	IP 주소	BFD	원격 AS 번호
⋮ ▼	192.168.50.11	사용 안 함	1000
	소스 주소	설정되지 않음	
	최대 홉 제한	1	

- 4 재배포 프로파일을 사용하여 VPN에 사용하려는 접두사를 보급합니다. NSX 적용 모드의 재배포 프로파일, 1단계에서 Tier-1 지원 경로를 연결합니다.

Tier-0 게이트웨이

게이트웨이 추가 ▾ 모두 확장 이름, 경로 등을 기준!

Tier-0 게이트웨이 이름	HA 모드	연결된 Tier-1 게이트웨이	연결된 세그먼트	상태 ①
<ul style="list-style-type: none"> > BGP ▼ 경로 재배포 <ul style="list-style-type: none"> 경로 재배포 2 4단계. 경로 재배포 상태 ● 켜짐 ⋮ > [VRF] TORvf 활성 활성 0 0 ● 성공 				

새로 고침

경로 재배포

Tier-0 게이트웨이 cloud-t0-vpc... #선택한 소스 ①

Tier-0 서브넷

보급된 Tier-1 서브넷

- 연결된 인터페이스 및 세그먼트
- 서비스 인터페이스 서브넷
- 연결된 세그먼트

FAQ(질문과 대답)

이 항목에서는 몇 가지 질문과 대답을 제공합니다.

NSX Cloud 구성 요소가 설치되어 실행 중인지 확인하려면 어떻게 합니까?

- 1 워크로드 VM의 NSX Tools가 PCG에 연결되어 있는지 확인하려면 다음을 수행합니다.
 - a nsxcli 명령을 입력하여 NSX CLI를 엽니다.
 - b 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
```

- 2 워크로드 VM에 올바른 태그가 있어야 PCG에 연결할 수 있습니다.
 - a AWS 콘솔 또는 Microsoft Azure 포털에 로그인합니다.
 - b VM의 eth0 또는 인터페이스 태그를 확인합니다.

nsx.network 키의 값은 default여야 합니다.

cloud-init를 사용하여 시작된 내 VM이 격리되고 타사 도구의 설치를 허용하지 않습니다. 어떻게 해야 합니까?

격리 정책을 사용하도록 설정하면 다음 규격의 cloud-init 스크립트를 사용하여 VM을 시작할 때 VM이 격리되고 사용자 지정 애플리케이션 또는 도구를 설치할 수 없습니다.

- `nsx.network=default` 태그 지정
- VM의 전원을 켤 때 자동으로 설치되거나 부트스트랩된 사용자 지정 서비스

해결 방법:

`default(AWS)` 또는 `default-vnet-<vnet-ID>-sg(Microsoft Azure)` 보안 그룹을 업데이트하여 사용자 지정 또는 타사 애플리케이션을 설치하는 데 필요한 인바운드/아웃바운드 포트를 추가합니다.

VM에 태그를 올바르게 지정하고 NSX Tools를 설치했지만 VM이 격리되었습니다. 어떻게 해야 합니까?

이 문제가 발생하면 다음을 시도해 보십시오.

- NSX Cloud 태그 `nsx.network` 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 합니까?

공용 클라우드에서(AWS 또는 Microsoft Azure)

- 1 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 [NSX Cloud 격리 정책을 사용한 위협 감지 항목](#)을 참조하십시오.
 - NSX-T Data Center DFW 규칙. 자세한 내용은 [NSX 적용 모드의 NSX 관리 워크로드 VM에 대한 기본 연결 전략 항목](#)을 참조하십시오.
 - Windows Firewall 또는 Linux의 IPTables
- 2 SSH 또는 다른 방법(예: Microsoft Azure의 직렬 콘솔)을 사용하여 VM에 로그인하고 문제에 대한 해결을 시도합니다.
 - 3 잠겨 있는 VM을 재부팅할 수 있습니다.

- 4 그래도 VM에 액세스할 수 없으면 보조 NIC를 워크로드 VM에 연결하여 이 NIC에서 해당 워크로드 VM에 액세스합니다.

기본 클라우드 적용 모드에서도 PCG가 필요합니까?

예.

CSM에서 내 공용 클라우드 계정을 온보딩한 후에 PCG에 대한 IAM 역할을 변경할 수 있습니까?

예. 공용 클라우드에 적용 가능한 NSX Cloud 스크립트를 다시 실행하여 PCG 역할을 재생성할 수 있습니다. PCG 역할을 재생성한 후 새 역할 이름을 사용하여 CSM에서 공용 클라우드 계정을 편집합니다. 공용 클라우드 계정에 배포된 모든 새 PCG 인스턴스에 새 역할이 사용됩니다.

기존 PCG 인스턴스는 이전 PCG 역할을 계속 사용합니다. 기존 PCG 인스턴스에 대한 IAM 역할을 업데이트하려면 공용 클라우드로 이동하여 해당 PCG 인스턴스에 대한 역할을 수동으로 변경합니다.

NSX Cloud에 대해 NSX-T Data Center 온-프레미스 라이선스를 사용할 수 있습니까?

예. ELA에 대한 조항이 있는 경우 가능합니다.

VMware NSX® Intelligence™에서는 온 프레미스 NSX-T Data Center 환경의 보안 상태를 시각화합니다. 시각화는 특정 기간 내에 집계된 네트워크 트래픽 흐름을 기준으로 합니다. NSX Intelligence는 보안 정책이 적용된 분석을 기준으로 권장 사항을 제공하여 마이크로 세분화 계획을 지원합니다.

중요 NSX Intelligence를 설치, 구성 및 사용하기 위한 권한을 얻으려면 엔터프라이즈 관리자 역할이 있어야 합니다.

NSX Intelligence 기능 사용을 시작하려면 먼저 NSX Intelligence 장치를 설치하고 구성해야 합니다. "NSX-T Data Center 설치 가이드"에서 "NSX Intelligence 장치 설치 및 구성"을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- NSX Intelligence 시작
- NSX Intelligence 보기 및 흐름 이해
- NSX Intelligence 권장 사항 사용
- NSX Intelligence 백업 및 복원
- NSX Intelligence 문제 해결

NSX Intelligence 시작

NSX Intelligence 기능을 사용하려면 NSX Intelligence 그래픽 사용자 인터페이스를 숙지하십시오.

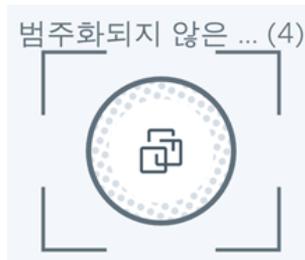
NSX Intelligence 장치가 설치 및 구성된 후에 NSX Manager UI의 **계획 및 문제 해결** 탭에서 NSX Intelligence 기능이 사용하도록 설정됩니다. 마이크로 세분화 계획에 대한 권장 사항을 보려면 **검색 및 계획** 섹션에서 **검색 및 작업 수행**을 사용하여 NSX-T Data Center 엔티티 및 **권장 사항**을 시각화하십시오.

NSX Intelligence 홈 페이지 둘러보기

NSX Manager 사용자 인터페이스에서 **계획 및 문제 해결 > 검색 및 작업 수행**을 클릭하여 NSX Intelligence 홈 페이지에 액세스합니다.

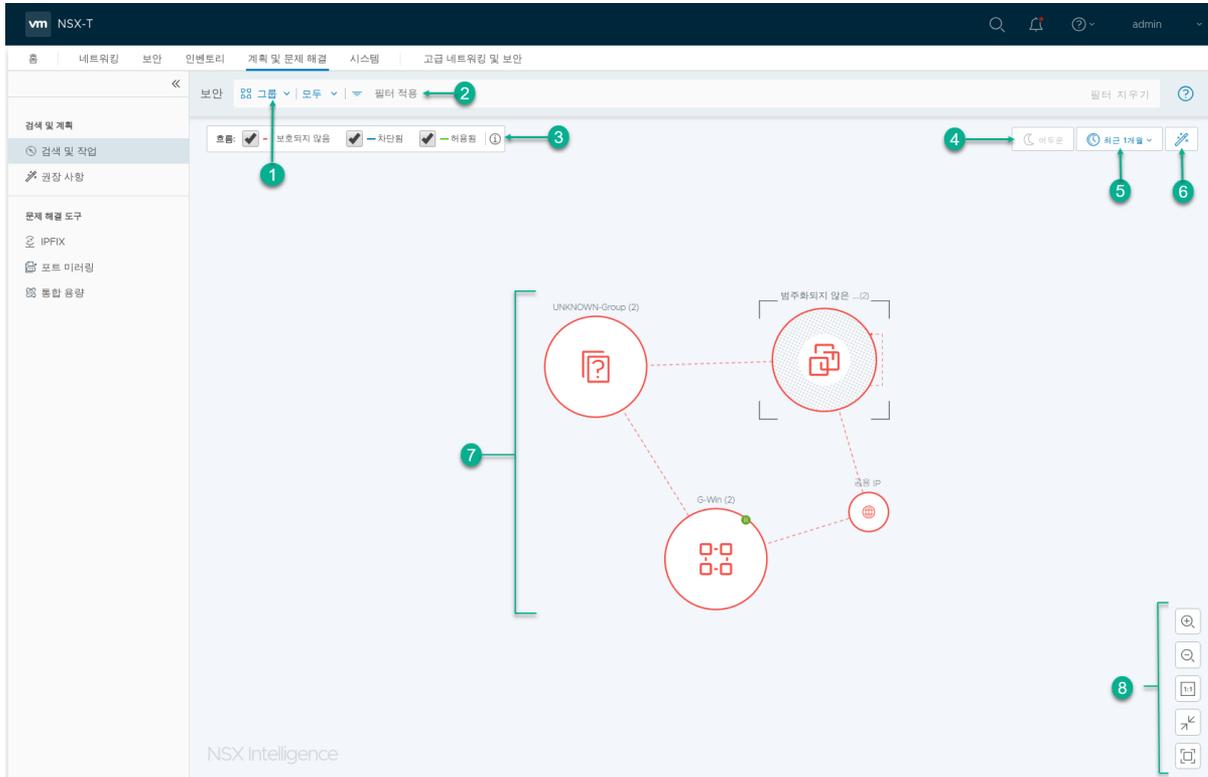
처음으로 NSX Intelligence를 설치 및 구성한 후 **검색 및 작업 수행**을 클릭하면 데이터를 찾을 수 없습니다. 위의 필터를 수정해야 할 수 있습니다. 메시지가 표시될 수 있습니다. 이 메시지는 NSX Intelligence가 네트워크 트래픽 데이터를 수신하여 시각화를 생성해야 하기 때문에 표시됩니다. NSX Intelligence는 NSX Manager에서 일부 네트워크 트래픽 데이터가 수신된 후에 일부 시각화를 렌더링하기 시작할 수 있습니다.

기본적으로 **검색 및 작업 수행**을 클릭하면 지난 24시간 동안 VM 멤버 간에 보호되지 않은 트래픽이 발생한 온 프레미스 NSX-T Data Center의 모든 그룹에 대한 보안 상태가 시각화됩니다. 보호되지 않은 네트워크 트래픽 흐름은 마이크로 조각화가 구현되지 않은 VM 간의 흐름입니다. 아직 정의된 그룹이 없는 경우 그룹이 표시되지 않습니다. VM이 있지만 어떤 그룹에도 속하지 않는 경우 범주화되지 않은 VM 그룹에 대한 아이콘이 표시됩니다.



이미 정의된 그룹이 있고 트래픽 데이터를 캡처한 경우 다음 스크린샷과 유사한 시각화가 표시될 수 있습니다. 다음 표에서는 스크린샷의 번호가 매겨진 섹션에 관해 설명합니다.

참고 NSX Intelligence는 CIDR 표기법(192.168.0.0/16, 172.16.0.0/12 및 10.0.0.0/8) 중 하나에 속하는 IP 주소를 전용 IP 주소로 분류합니다. 이러한 CIDR 표기법에 속하지 않는 모든 IP 주소는 공용 IP 주소로 분류됩니다. VM의 IP 주소가 이러한 CIDR 표기법 중 하나에 속하지 않는 경우 "NSX-T Data Center API 가이드"에서 PATCH /api/v1/intelligence/host-config API를 사용하여 CIDR 표기법 추가 방법을 참조하십시오.



섹션	설명
1	<p>보안 보기 선택 영역에서는 표시할 보안 시각화 유형을 선택할 수 있습니다. 두 가지 유형의 보안 보기, 즉 그룹 및 VM을 사용할 수 있습니다. 검색 및 작업 수행을 클릭하면 기본 보안 보기는 최근 24시간 이내에 보호되지 않는 흐름 트래픽이 있던 NSX-T Data Center의 그룹 개체에 대한 그룹 보기입니다.</p> <ul style="list-style-type: none"> ■ VM 보기를 선택하려면 그룹 옆의 아래쪽 화살표를 클릭하고 VM을 선택합니다. ■ 보기에 포함할 특정 그룹 또는 VM을 선택하려면 모두 옆의 아래쪽 화살표를 클릭하고 목록에서 선택합니다. ■ 선택 필터를 지우려면 화면의 오른쪽 상단에 있는 필터 지우기를 클릭합니다. VM 보기에서 필터 지우기를 클릭하면 선택 필터가 지워지고 그룹 보기가 표시됩니다. <p>두 가지 보기 유형을 사용하는 방법에 대한 자세한 내용은 그룹 보기 사용 및 VM 보기 사용 항목을 참조하십시오.</p>
2	<p>필터 적용을 사용하여 시각화에 사용되는 기준을 구체화할 수 있습니다. 드롭다운 목록에서 시각화에 사용할 기준을 선택할 수 있습니다. VM 멤버, 태그, 흐름 유형, 소스 IP, 대상 IP, 규칙 ID 또는 이름을 선택할 수 있습니다. 필터 적용을 클릭하여 적용할 여러 필터를 정의할 수 있습니다.</p>
3	<p>이 흐름 섹션에서 선택한 기간에 시각화에 포함할 트래픽 흐름 유형을 선택할 수 있습니다. 이 섹션에는 흐름 유형에 대한 시각화에 사용된 색상도 표시됩니다.</p> <ul style="list-style-type: none"> ■ 보호되지 않은 흐름에 해당하는 빨간색 파선 ■ 차단된 흐름에 해당하는 파란색 실선 ■ 허용된 흐름에 해당하는 녹색 실선 <p>기본적으로 현재 NSX Intelligence 시각화에 대해 보호되지 않은 트래픽 흐름 유형이 선택됩니다. 자세한 내용은 트래픽 흐름 사용 항목을 참조하십시오.</p>
4	<p>디스플레이 모드 섹션에서는 시각화에 사용할 테마를 정의합니다. 밝은 테마는 기본 사용 모드입니다.</p> <ul style="list-style-type: none"> ■ 어두운 테마 모드를 사용하려면 어두운 아이콘을 클릭합니다. 전체 화면 모드에서 시각화를 보는 경우에만 어두운 테마를 사용할 수 있습니다. ■ 전체 화면 모드로 전환하려면 보기 제어 섹션에서  을 클릭하십시오.

섹션	설명
5	이 섹션에서는 원하는 시각화 및 권장 사항을 생성하는 데 사용되는 네트워크 흐름 데이터를 결정할 때 사용할 기간을 선택합니다. 선택 사항에 따라 그룹 또는 VM 보기에서 사용되는 기간별 데이터가 결정됩니다. 기간은 현재 시간과 과거의 일부 시간을 기준으로 합니다. 최근 24시간은 사용되는 기본 시간 범위입니다. 선택한 기간을 변경하려면 현재 선택된 기간을 클릭하고 최근 1시간 , 최근 12시간 , 최근 24시간 , 최근 1주 또는 최근 1개월 을 선택합니다.
6	이 권장 사항 막대  아이콘을 클릭하면 [권장 사항] 대화상자에 현재 보기에 대한 인벤토리 요약이 표시됩니다. VM 보기에 있는 경우 새 권장 사항 시작 을 클릭하여 NSX Intelligence 권장 사항을 생성할 수 있습니다. NSX Intelligence 권장 사항 사용 항목을 참조하십시오.
7	이 섹션은 온 프레미스 NSX-T Data Center에 있는 그룹 또는 VM의 보안 상태를 시각화한 것입니다. 또한 선택한 기간 동안 발생한 네트워크 트래픽 흐름의 시각화도 포함됩니다. 이 섹션에서는 특정 노드 또는 흐름 화살표를 가리켜 해당 특정 엔티티에 대한 세부 정보를 가져올 수 있습니다. 자세한 내용은 NSX Intelligence 그래픽 요소 사용해 보기 및 NSX Intelligence 보기 및 흐름 이해 항목을 참조하십시오.
8	이 섹션에는 확대, 축소, 1:1 가로세로 비율 적용, 크기 조정-보기에 맞추기, 전체 화면 보기 모드 시작 또는 종료를 수행하기 위한 보기 컨트롤이 포함됩니다. 또한 키보드 바로 가기를 사용하여 보기 컨트롤을 관리할 수 있습니다. 바로 가기 키 도움말 창을 표시하려면 Shift+/ 를 누릅니다. 이전에 표시했던 시각화로 이동하려면 웹 브라우저의 [뒤로] 버튼을 사용합니다. 전체 화면 모드에서는 뒤로 (화면의 왼쪽 상단)를 클릭하여 동일한 뒤로 단추 탐색을 수행합니다.

NSX Intelligence 그래픽 요소 사용해 보기

NSX Intelligence 사용자 인터페이스는 NSX-T Data Center 환경의 데이터 센터 엔티티, 트래픽 흐름 및 특정 작업을 시각화하는 데 도움이 되는 몇 가지 그래픽 요소를 제공합니다.

다음 표에는 NSX Intelligence 시각화에서 볼 수 있는 NSX-T Data Center 그래픽 요소에 대한 용어 설명 목록이 나와 있습니다.

그래픽 요소	설명
	이 아이콘은 동-서 방화벽 규칙을 비롯한 보안 정책이 적용될 수 있는 VM 모음에 해당하는 그룹을 나타냅니다. 그룹 보기 사용 항목을 참조하십시오.
	이 아이콘은 NSX-T Data Center의 일부인 VM(가상 시스템)을 나타냅니다. VM은 둘 이상의 그룹에 속할 수 있습니다. VM 보기 사용 항목을 참조하십시오.
	이 아이콘은 인터넷의 공용 IP를 나타냅니다. 선택한 기간 동안 NSX-T Data Center 환경에서 하나 이상의 VM이 공용 IP와 통신하는 경우 해당 트래픽 흐름이 현재 시각화에 포함됩니다.
	선택한 기간 동안 네트워크 트래픽 활동에 참여하는 유니캐스트, 브로드캐스트 또는 멀티캐스트 IP와 같은 IP 주소입니다.

그래픽 요소	설명
	<p>이 아이콘은 그룹에 속하지 않는 VM 그룹에 사용됩니다.</p>
	<p>화살표는 선택한 기간에 두 VM 간에 발생한 네트워크 트래픽 흐름을 나타냅니다. 화살표에는 보호되지 않는 흐름을 나타내는 빨간색 파선 화살표, 차단된 흐름을 나타내는 파란색 실선 화살표, 허용된 흐름을 나타내는 녹색 실선 화살표의 세 가지 유형이 있습니다. 트래픽 흐름 사용 항목을 참조하십시오.</p>
	<p>포커스가 있는 현재 노드로 선택된 노드의 둘레에는 파선 원이 표시됩니다. 이는 선택 모드를 진행하는 동안 고정된 노드로 사용되며, 현재 보기를 표시합니다.</p>
	<p>이 아이콘은 선택한 기간 동안 그룹이 NSX-T Data Center 인벤토리에 추가된 경우 그룹 노드의 테두리에 표시됩니다. 선택한 기간 동안 NSX-T Data Center가 VM을 검색하면 해당 VM 노드 테두리에 해당 아이콘이 표시됩니다.</p>
	<p>이 아이콘은 선택한 기간에 그룹이 삭제되고 VM 멤버가 삭제되지 않은 경우 그룹 노드의 테두리에 표시됩니다. VM 노드의 테두리에서 이 아이콘은 선택한 기간에 VM이 삭제되었음을 나타냅니다. VM 또는 그룹이 삭제되었지만 현재 시각화에 계속 표시되면서 선택한 기간에 VM 또는 그룹이 제거된 경우를 보여 주는 기록 보기를 제공합니다.</p>
	<p>이 아이콘은 그룹 및 VM이 함께 표시될 때마다 나타납니다. 예를 들어, 심층 작업 그룹 보기 또는 그룹의 관련 VM에 표시됩니다.</p> <p>이 아이콘은 다음과 같은 경우 VM 노드의 테두리에 표시됩니다.</p> <ul style="list-style-type: none"> ■ 선택한 기간 동안 현재 표시된 그룹에서 VM이 이동된 경우 ■ 선택한 기간 중 특정 시점에 VM이 현재 표시되는 그룹의 일부이지만 더 이상 동일한 그룹의 멤버가 아닌 경우

NSX Intelligence 보기 및 흐름 이해

NSX Intelligence 시각화는 그룹 또는 VM, 그리고 선택한 기간에 해당 그룹 또는 VM에서 발생한 네트워크 흐름 크 흐름으로 구성됩니다.

중요 특정 기간에 표시되는 시각화는 해당 기간에 NSX-T Data Center에서 발생한 모든 네트워크 흐름 및 작업(예: VM 및 그룹의 추가, 삭제 또는 이동)을 나타냅니다. 가상화에서 VM이 두 번 이상 나타날 수 있습니다. 예를 들어, VM이 원래 관리되지 않는 ESXi 호스트에 연결되어 있고 선택한 기간에 호스트가 VMware vCenter Server™에서 관리되는 경우 해당 VM이 VM 보기에 두 번 나타납니다. 마찬가지로 vCenter Server에서 ESXi 호스트의 연결을 끊었다가 선택한 동일한 기간에 다시 추가하면 호스트에 연결된 VM이 선택한 기간에 삭제된 호스트와 신규 호스트 둘 다로 표시됩니다. 그룹 보기에서 VM이 범주화되지 않은 그룹에 있고 동일한 선택 기간에 그룹에 추가된 경우 범주화되지 않은 그룹과 새 그룹 둘 다에 표시됩니다.

NSX Intelligence는 VM 멤버 유형만 포함된 그룹을 지원합니다. 다른 유형의 멤버를 포함하는 그룹이 있는 경우 그룹 보기에는 보안 규칙의 실제 그룹 대신, VM 멤버 유형을 포함하는 그룹 간의 상호 연관된 흐름이 표시될 수 있습니다.

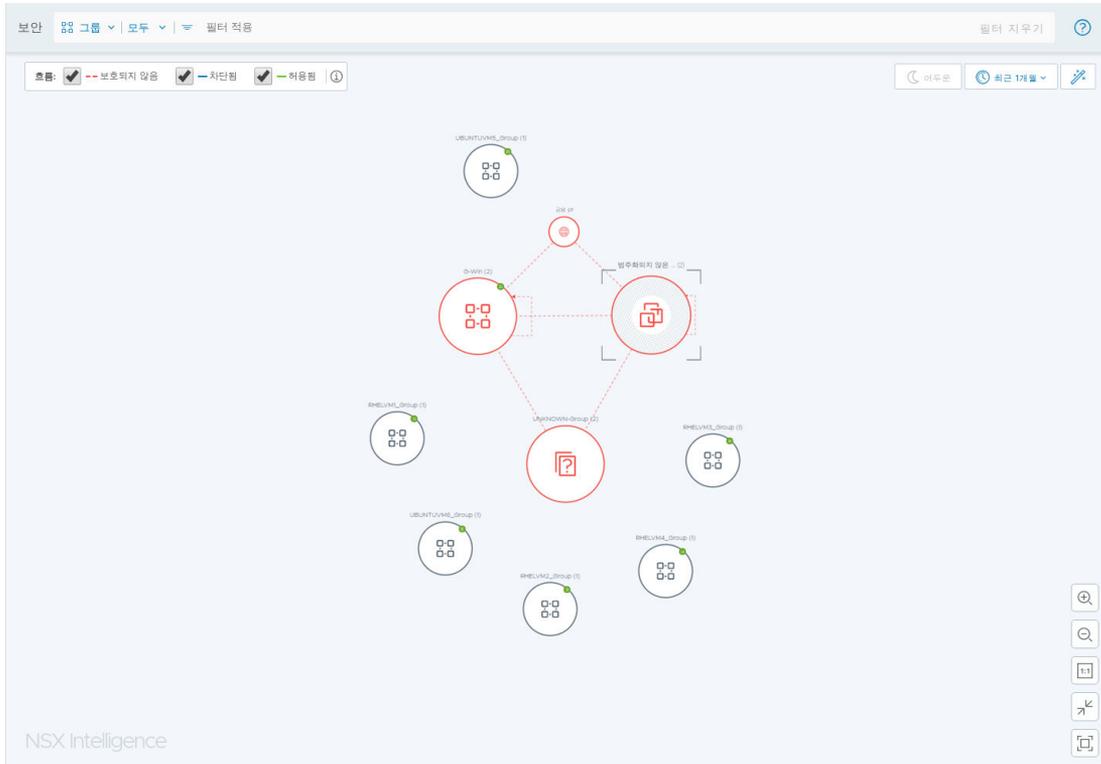
이 섹션의 정보를 사용하여 그룹 보기, VM 보기 및 다른 트래픽 흐름 작업에 대해 자세히 알아보십시오.

그룹 보기 사용

NSX Intelligence 홈페이지에 표시되는 기본 보기는 그룹 보기입니다. 이 그룹 보기는 지난 24시간 동안 보호되지 않은 트래픽 흐름이 있는 모든 그룹을 표시하도록 필터링됩니다.

그룹 보기의 노드 및 화살표

그룹 보기의 노드는 NSX-T Data Center 환경의 NSX 개체(예: VM, IP 집합 등)를 나타냅니다. 다음 스크린샷은 그룹 보기 샘플입니다.



다음 표에는 그룹 보기에 표시될 수 있는 그룹 노드 유형이 나열되어 있습니다.

그룹 노드 유형	아이콘	설명
일반 그룹		NSX Intelligence의 일반 그룹 노드는 NSX-T Data Center 환경에 있는 모든 NSX 개체의 컬렉션을 나타냅니다. 이번 릴리스에서 이러한 NSX 개체는 VM 전용이며 NSX Intelligence는 VM 멤버 유형의 일반 그룹만 지원합니다. 하나의 NSX 개체가 둘 이상의 그룹에 속할 수 있으므로 하나의 VM은 둘 이상의 그룹 노드에 나타날 수 있습니다.
범주화되지 않은 그룹		범주화되지 않은 그룹 노드는 어떤 그룹에도 속하지 않는 VM 컬렉션을 나타냅니다.
알 수 없는 그룹		알 수 없는 그룹 노드는 NSX-T Data Center 인벤토리에 없는 기타 개체 집합을 나타냅니다. 하지만 이러한 개체는 NSX-T Data Center 환경에서 하나 이상의 NSX 개체와 통신합니다.
공용 IP 그룹		공용 IP 그룹 노드는 NSX-T Data Center의 NSX 개체와 통신하는 공용 IP 주소(IPv4 또는 IPv6) 컬렉션을 나타냅니다.

그룹 보기에서 노드의 크기는 VM과 같이 해당 그룹에 속하는 NSX 개체의 수를 기준으로 합니다. 그룹 노드가 클수록 해당 그룹에 더 많은 VM이 속합니다. 그룹의 이름과 해당 그룹에 있는 멤버 VM의 전체 수가 노드 위에 표시됩니다.

그룹 노드 사이의 화살표는 선택한 기간에 연결된 해당 그룹 노드에 있는 VM 간에 발생한 트래픽 흐름을 나타냅니다. 그룹 노드의 자체 참조 화살표는 하나 이상의 VM이 동일한 그룹 내의 다른 VM과 통신하고 있음을 나타냅니다. 자세한 내용은 [트래픽 흐름 사용](#) 항목을 참조하십시오.

빨간색 테두리가 그려진 노드는 선택한 기간 동안 감지된 차단 또는 허용된 흐름의 수에 관계없이, 해당 그룹의 VM에서 하나 이상의 보호되지 않는 흐름이 발생했음을 나타냅니다. 노드의 파란색 테두리는 보호되지 않는 트래픽 흐름은 감지되지 않았으나, 선택한 기간 동안 감지된 허용된 흐름의 수에 관계없이 하나 이상의 차단된 흐름이 감지되었음을 나타냅니다. 녹색 테두리가 있는 노드는 선택한 기간 동안 보호되지 않거나 차단된 흐름이 감지되지 않았으며 하나 이상의 허용된 흐름이 감지되었음을 나타냅니다. 회색 테두리가 있는 노드는 선택한 기간 동안 해당 그룹에 속하는 VM에 대해 트래픽 흐름이 감지되지 않았음을 나타냅니다.

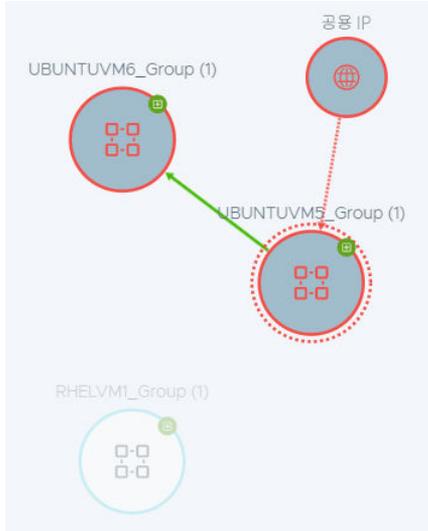
그룹 보기가 표시되지 않는 경우 [보안] 보기 선택 영역에서 VM 옆에 있는 아래쪽 화살표를 클릭하고 **그룹**을 선택합니다. 표시되는 선택 드롭다운 목록에서 **모든 그룹** 또는 목록의 특정 그룹을 선택한 후 **적용**을 클릭할 수 있습니다. **검색** 텍스트 상자를 사용하여 선택 목록을 필터링합니다. 어떤 항목도 선택하지 않고 선택 드롭다운 목록 외부 클릭하거나 드롭다운 목록에서 **모든 그룹**을 선택하면 **모든 그룹** 옵션이 그룹 보기에 적용됩니다.

그룹 보기에서 노드 선택

그룹의 노드를 가리키면 그룹 G-Win에 대한 다음 예제와 같이, 해당 그룹에 대한 정보가 표시됩니다. 선택한 기간에 검색된 흐름 수와 유형도 나열됩니다. 선택한 기간에 그룹이 추가된 경우 새 배지 아이콘과 그룹이 생성된 시기에 대한 세부 정보도 표시됩니다.



그룹의 노드를 클릭하면 파선 원을 사용하여 선택 영역이 고정된 그룹 노드로 표시됩니다. 선택한 그룹 노드에 연결된 다른 그룹도 보기에서 좀 더 두드러지게 표시됩니다. 다른 모든 노드는 흐리게 표시됩니다. 예를 들어, 다음 스크린샷에서 노드 UBUNTUVM5_Group이 선택되어 있고, 선택한 기간에 UBUNTUVM5_Group과 트래픽 흐름을 공유하는 다른 그룹도 강조 표시됩니다. UBUNTUVM5_Group과 통신하지 않는 다른 모든 그룹은 보기에서 페이드 아웃됩니다.

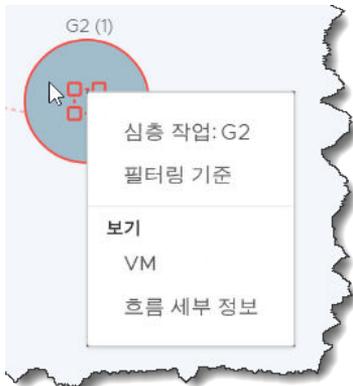


고정된 선택 영역을 지우려면 그룹 보기의 빈 영역을 클릭합니다.

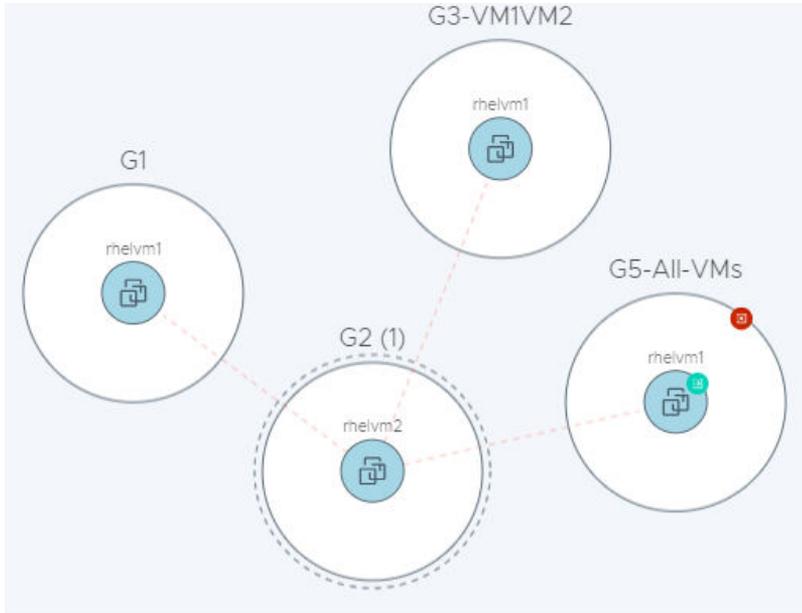
그룹 보기를 축소하고 노드의 세부 정보가 더 이상 표시되지 않을 경우 노드의 보이는 부분을 가리키면 해당 세부 정보가 표시됩니다.

그룹 보기에서 사용 가능한 작업

다음 이미지와 같이 그룹의 노드를 마우스 오른쪽 버튼으로 클릭하면 사용 가능한 작업의 컨텍스트 메뉴가 표시됩니다.



- 심층 작업: Group_Name**을 선택하면 선택한 그룹의 노드 둘레에 파선 원이 표시되어 고정된 그룹 노드 또는 포커스가 있는 현재 그룹으로 표시됩니다. 그룹에 속한 VM이 그룹의 노드 내에 표시됩니다. 선택한 기간에 고정된 그룹의 VM과의 트래픽 흐름이 있었던 모든 그룹도 그룹 보기에 배치됩니다. 다음 예에서, 그룹 G2는 고정된 그룹이고 다른 그룹은 해당 VM 멤버가 선택한 기간 동안 그룹 G2의 rhelvm2와의 트래픽 흐름이 있었으므로 보기에 표시됩니다.



- **필터링 기준**을 선택하면 현재 그룹 보기에 사용되는 시각화 필터에 현재 그룹이 추가됩니다.
- **VM**을 선택하면 선택한 기간에 현재 그룹에 속한 모든 **VM**의 포가 표시됩니다. 해당 보기 **VM** 포에서, 선택한 그룹에 속하는 **VM**과 각 **VM**이 속하는 다른 그룹에 대한 세부 정보를 볼 수 있습니다. 현재 시각화 필터에 **VM**을 추가하려면 필터 아이콘을 클릭합니다.
- **흐름 세부 정보**를 선택하면 다음 스크린샷과 같이 현재 선택한 그룹의 흐름 세부 정보 포가 표시됩니다. 여기에는 선택한 기간 동안 발생한 흐름 및 현재 그룹에 속하는 **VM**에서 현재 활성 상태인 흐름에 대한 세부 정보가 표시됩니다. 세부 정보에는 흐름 유형, 흐름의 소스 및 대상 그룹, 흐름의 시작 및 종료 시간, 사용된 서비스가 포함됩니다. 일부 세부 정보를 클릭하여 자세한 내용을 확인할 수 있습니다. 자세한 내용은 [트래픽 흐름 사용을 참조하십시오](#).

흐름 세부 정보 ×

🕒 최근 24시간

범주화되지 않은 VM에 대한 흐름 세부 정보 표시

완료된 흐름
활성화된 흐름

소스	소스 그룹	대상	대상 그룹	서비스	종료 시간	최신 흐름
ubuntu12.04.1-2G-L...	G5	ubuntu12.04-...	UNCATEGORIZED	SSH... + 2개 더	19. 11. 6. AM 8:05	● 보호되지 않
ubuntu12.04.1-2G-L...	G1	ubuntu12.04-...	UNCATEGORIZED	SSH... + 2개 더	19. 11. 6. AM 8:05	● 보호되지 않

🔄 새로 고침
1 - 2 of 2 흐름(초)

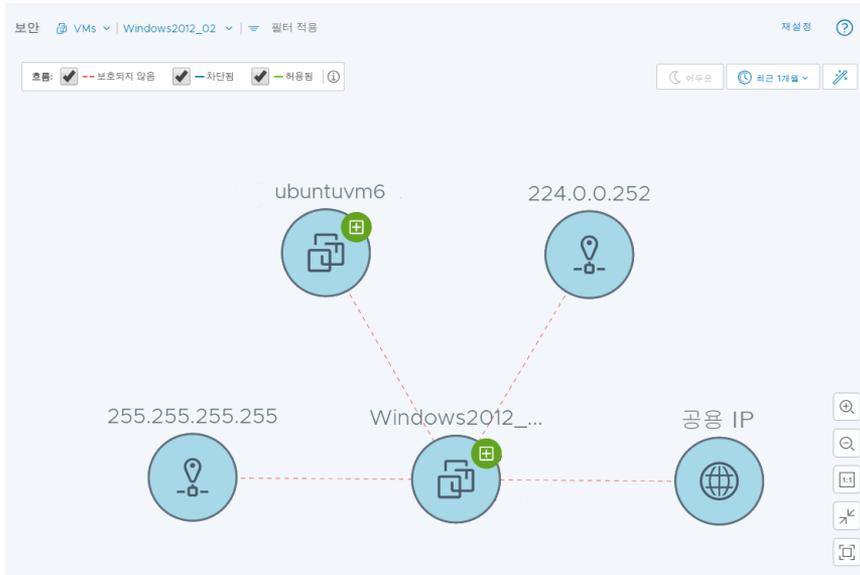
닫기

VM 보기 사용

VM 보기의 노드는 온 프레미스 NSX-T Data Center 환경의 VM(가상 시스템)을 나타냅니다.

VM 보기의 노드 및 화살표

VM 보기 상태에서는 그룹 경계가 표시되지 않습니다. NSX-T Data Center 환경에서 VM 중 하나와 통신하지만 NSX-T Data Center 인벤토리에 속하는 것으로 식별되지 않은 모든 노드는 VM 보기에 표시됩니다. 다음은 간단한 VM 보기입니다.



다음 표에는 VM 보기에 표시될 수 있는 VM 노드 유형이 나열되어 있습니다.

VM 노드 유형	아이콘	설명
일반 VM		일반 VM 노드는 NSX-T Data Center 환경의 일부인 VM(가상 시스템)을 나타냅니다. VM은 둘 이상의 그룹에 속할 수 있습니다.
공용 IP		공용 IP 노드는 NSX-T Data Center 환경과 통신하는 공용 IP 주소(IPv4 또는 IPv6)를 나타냅니다.
IP		IP 노드는 선택한 기간 동안 네트워크 트래픽 작업에 참여하는 IP 주소를 나타냅니다. IP 주소는 유니캐스트, 브로드캐스트 또는 멀티캐스트 IP일 수 있습니다.

VM 보기가 표시되지 않는 경우 [보안] 보기 선택 영역에서 **그룹** 옆에 있는 아래쪽 화살표를 클릭하고 **VM** 을 선택합니다. 표시되는 선택 드롭다운 목록에서 **모든 VM** 또는 목록의 특정 VM을 선택한 후 **적용**을 클릭 할 수 있습니다. **검색** 텍스트 상자를 사용하여 선택 목록을 필터링합니다. 어떤 항목도 선택하지 않고 드롭 다운 목록 외부를 클릭하거나 드롭다운 목록에서 **모든 VM**을 선택하면 **모든 VM** 옵션이 VM 보기에 적용됩니다.

VM 노드 사이의 화살표는 선택한 기간에 VM 간에 발생한 트래픽 흐름을 나타냅니다. 자세한 내용은 [트래픽 흐름 사용 항목](#)을 참조하십시오.

VM 보기에서 노드 선택

VM 노드를 가리키면 다음 예제와 같이 노드에 대한 정보가 표시됩니다. 선택한 기간에 검색된 VM에 대한 흐름 수와 유형도 나열됩니다. 선택한 기간에 그룹이 추가된 경우 새 배지 아이콘과 VM이 추가된 시기에 대한 세부 정보도 표시됩니다.



VM의 노드를 클릭하면 파선 원을 사용하여 선택 영역이 고정된 VM 노드로 표시됩니다. 고정된 해당 VM 노드와의 트래픽 흐름이 있었던 다른 VM 노드도 VM 보기에서 더 두드러지게 나타납니다. 다른 모든 노드는 흐리게 표시되어 잘 보이지 않게 됩니다. 고정된 선택 영역을 지우려면 VM 보기의 빈 영역을 클릭합니다.

VM 보기를 축소하고 VM 노드의 세부 정보가 더 이상 표시되지 않을 경우 VM 노드의 보이는 부분을 가리키면 해당 세부 정보가 표시됩니다.

VM 보기에서 사용 가능한 작업

다음 이미지와 같이 VM의 노드를 마우스 오른쪽 버튼으로 클릭하면 사용 가능한 작업의 컨텍스트 메뉴가 표시됩니다.



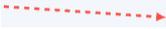
선택	설명
필터링 기준	현재 VM 보기에 사용되는 시각화 필터에 해당 VM이 추가됩니다.
VM 정보	선택한 기간 동안의 VM 세부 정보가 표시됩니다.
관련 그룹	선택한 기간 동안 VM이 속한 그룹에 대한 정보를 포함하는 그룹 포입니다.
흐름 세부 정보	<p>선택한 기간 동안 발생한 흐름 및 VM에서 현재 활성 상태인 흐름에 대한 세부 정보가 표시됩니다. 세부 정보에는 다음이 포함됩니다.</p> <ul style="list-style-type: none"> ■ 흐름 유형 ■ 흐름의 소스 및 대상 그룹 ■ 흐름의 시작 및 종료 시간 ■ 사용된 서비스 <p>일부 세부 정보를 클릭하여 자세한 내용을 확인할 수 있습니다. 자세한 내용은 트래픽 흐름 사용 항목을 참조하십시오.</p>
권장 사항 시작	새 권장 사항 시작 마법사를 표시합니다. 자세한 내용은 NSX Intelligence 권장 사항 사용 를 참조하십시오.

트래픽 흐름 사용

그룹 또는 VM 노드 사이의 화살표는 선택한 기간에 VM 간에 발생한 네트워크 트래픽 흐름을 나타냅니다.

네트워크 트래픽 흐름은 설정된 L3 분산 방화벽(DFW) 규칙 및 선택한 기간 동안 발생한 트래픽 흐름을 기준으로 합니다. TCP, UDP, GRE, ESP 및 SCTP 프로토콜에서 IPv4 또는 IPv6을 사용하며 상태 저장 L3 DFW 규칙과 일치하는 모든 네트워크 트래픽 흐름은 시각화되고 흐름 세부 정보에 포함됩니다. TCP 및 UDP 흐름은 IP 및 포트 수준 세부 정보가 지정되며, IP 수준 세부 정보만 지정된 흐름도 있습니다.

트래픽 흐름은 다음과 같은 유형으로 분류됩니다.

흐름 유형	그래픽	설명
보호되지 않음		빨간색 파선 화살표는 시스템에서 트래픽 흐름이 규칙(소스: 모두 대상: 모두 작업: 허용 또는 거부 또는 삭제)을 충족했으며 좀 더 세분화된 보안 정책이 필요하다는 사실을 감지했음을 나타냅니다. 이 규칙은 기본 규칙일 수도 있고, 동-서 분산 방화벽의 임의 위치에 상주할 수도 있습니다.
차단됨		파란색 단색 화살표는 시스템에서 트래픽 흐름이 '보호되지 않음' 흐름 정의에 언급된 것보다 좀 더 세분화된 '거부' 또는 '삭제' 규칙을 충족했다는 사실을 감지했음을 나타냅니다.
허용됨		녹색 단색 화살표는 시스템에서 트래픽 흐름이 '보호되지 않음' 흐름 정의에 언급된 것보다 좀 더 세분화된 '허용' 규칙을 충족했다는 사실을 감지했음을 나타냅니다.

특정 유형의 트래픽 흐름을 가진 개체에만 집중하려면 보안 보기 선택 영역을 사용하여 보기 유형을 선택하고 '흐름 유형' 필터 특성을 사용하여 선택 범위를 좁힙니다.

흐름 유형을 선택 취소하면 해당 흐름 유형에 대한 흐름 라인이 표시된 그래프에서 숨겨집니다. 특정 개체를 제외하는 필터가 적용되지 않으면 선택한 기간 동안 해당 개체에서 발생한 트래픽 흐름 유형에 관계없이 모든 그룹 또는 VM 개체가 표시됩니다. 예를 들어 '허용됨' 흐름 유형을 선택 취소하면 그래프에서 "허용됨" 흐름 라인이 모두 숨겨집니다. 그러나 선택한 기간 동안 '허용됨' 트래픽 흐름이 있는 개체에 대해서도 모든 개체가 계속 표시됩니다.

흐름 화살표의 방향은 검색된 트래픽 흐름의 소스 및 대상을 나타냅니다. 그룹 보기에서 그룹 노드의 자체 참조 화살표는 하나 이상의 VM이 동일한 그룹 내의 다른 VM과 통신하고 있음을 나타냅니다. VM 보기에서 자체 참조 화살표는 VM의 NSX 개체가 동일한 VM의 다른 NSX 개체와 통신했음을 나타냅니다.

흐름 화살표를 가리키면 그룹 G2에 대한 다음 예제와 같이 그룹 또는 VM을 포함하는 흐름에 대한 정보가 표시됩니다.



흐름 화살표를 클릭하면 [흐름 세부 정보] 대화상자가 표시됩니다. 선택한 기간에 발생한 완료된 흐름과 활성화된 흐름에 대한 세부 정보가 표시됩니다. 흐름의 소스, 대상, 서비스 유형 및 흐름 유형에 대한 자세한 내용을 보려면 표에서 링크를 클릭합니다.

NSX Intelligence 권장 사항 사용

NSX Intelligence는 선택한 기간 동안 NSX-T Data Center 환경의 VM 간에 발생한 트래픽 흐름 패턴을 기준으로 하는 마이크로 세분화 권장 사항을 제공할 수 있습니다.

NSX Intelligence 권장 사항 이해

NSX Intelligence에서 생성하는 권장 사항에는 애플리케이션에 대한 보안 정책, 정책 보안 그룹 및 서비스가 포함됩니다.

권장 사항은 vCenter Server에서 관리되는 ESXi 호스트의 VM 워크로드 간 네트워크 트래픽 흐름 패턴을 기준으로 합니다. 이 기능은 NSX-T Data Center 환경에서 발생한 통신의 트래픽 패턴에서 상관관계를 분석하여 보다 동적인 보안 정책을 적용할 수 있도록 합니다.

보안 정책 권장 사항은 애플리케이션 범주의 East-West 분산 방화벽 보안 정책입니다. 보안 그룹 권장 사항은 사용자가 지정한 기간 및 VM 경계에 대해 분석된 네트워크 트래픽 흐름에 나타나는 VM의 목록으로 구성됩니다. 서비스 권장 사항은 사용자가 지정한 VM의 애플리케이션이 특정 포트에서 사용한 서비스 개체이지만 NSX-T Data Center 인벤토리에 아직 정의되지 않은 서비스 개체입니다.

권장 사항을 요청하는 방법에는 여러 가지가 있지만 가장 간단한 방법은 **계획 및 문제 해결 > 권장 사항** 탭에서 **새 권장 사항 시작**을 클릭하는 것입니다. 해당 특정 VM에 대해 네트워크 트래픽 흐름을 분석하는 애플리케이션 경계 및 시간 범위로 구성되는 VM(가상 시스템)을 제공합니다. 권장 사항 분석이 완료되면 권장 사항에 대한 세부 정보를 보고, 필요한 경우 게시하기 전에 권장 사항을 수정할 수 있습니다. 자세한 내용은 새 **NSX Intelligence 권장 사항 생성** 항목을 참조하십시오.

새 NSX Intelligence 권장 사항 생성

NSX Intelligence 권장 사항 기능은 애플리케이션을 마이크로 크기만큼 세그먼트화하는 데 도움이 되는 권장 사항을 제공합니다.

NSX Intelligence 권장 사항을 생성하면 애플리케이션에 대한 보안 정책, 정책 보안 그룹 및 서비스 권장 사항이 포함됩니다. 권장 사항은 NSX-T Data Center의 VM 간에 발생하는 통신 트래픽 패턴을 기준으로 생성됩니다. NSX Intelligence UI를 사용하여 여러 가지 방법으로 권장 사항을 생성할 수 있습니다. 다음 절차에서는 사용할 수 있는 세 가지 방법에 대해 설명합니다.

사전 요구 사항

NSX Intelligence를 설치합니다. "NSX-T Data Center 설치 가이드"에서 "NSX Intelligence 설치 및 구성"을 참조하십시오.

절차

- 1 브라우저에서 엔터프라이즈 관리자 권한으로 <https://<nsx-manager-ip-address>>에서 NSX Manager에 로그인합니다.
- 2 새 권장 사항의 생성을 시작합니다.

다음 표를 사용하여 세 가지 방법 중에서 사용할 방법을 결정합니다.

방법	단계
계획 및 문제 해결 > 권장 사항을 선택합니다.	새 권장 사항 시작을 클릭합니다.
VM 보기에서 VM을 선택하고 마우스 오른쪽 버튼을 클릭합니다.	상황별 메뉴에서 새 권장 사항 시작을 선택합니다.
계획 및 문제 해결 > 검색 및 작업 수행을 선택합니다.	<ol style="list-style-type: none"> 1 보안 상황 필터에서 아래쪽 화살표를 클릭하고 VM을 선택합니다. 2 애플리케이션 경계를 구성하는 VM을 선택하고 적용을 클릭합니다. 3 권장 사항 막대 아이콘  을 클릭합니다. 4 [권장 사항] 대화상자에서 새 권장 사항 시작을 클릭합니다.

- 3 새 권장 사항 시작 마법사에서 선택적으로 권장 사항 이름의 기본값을 변경합니다.

4 보안 정책 권장 사항에 대한 경계로 사용할 VM을 정의하거나 수정합니다.

a **VM 선택** 또는 **선택한 VM**의 수를 클릭합니다.

b [VM 선택] 대화상자에서 분석에 대한 경계로 사용할 VM을 선택하고 포함하지 않을 VM을 선택 취소합니다.

권장 사항 경계에 사용할 VM은 100개까지 선택할 수 있습니다. 선택 표시줄에 이름을 입력하여 선택할 VM을 필터링할 수도 있습니다.

c **저장**을 클릭합니다.

선택한 VM의 수가 [새 권장 사항 검색] 대화상자에 표시됩니다.

5 권장 사항 분석에 사용되는 **설명 및 시간 범위**의 기본값을 변경하려면 **추가 옵션**을 확장합니다. 기본 **시간 범위** 값은 최근 1개월이며, 이는 최근 1개월 내에 선택한 VM 간의 네트워크 트래픽 흐름이 권장 사항을 분석하는 동안 사용됨을 의미합니다.

6 **검색 시작**을 클릭합니다.

권장 사항은 순차적으로 처리됩니다. 평균적으로, 처리가 보류된 다른 권장 사항이 있는지 여부에 따라 각 권장 사항을 완료하는 데 3 ~ 4분 정도 걸릴 수 있습니다. VM 간에 분석해야 하는 트래픽 흐름이 많이 있는 경우 권장 사항은 10 ~ 15분 사이에 생성될 수 있습니다. 상태는 **권장 사항** 탭에서 추적할 수 있습니다. 상태는 대기 중에서 분석 중으로 바뀌었다가 마지막으로 게시 준비 완료가 됩니다. 다음 스크린샷은 생성된 권장 사항의 세 가지 다른 상태를 보여 줍니다.

이름	상태	VM	생성 시간	마지막으로 수정한 날짜
REC 20191107 10:09:19	사용 가능한 권장 사항 없음	6	19. 11. 7. AM 2:09	19. 11. 7. AM 2:09
REC 20191106 16:39:30	사용 가능한 권장 사항 없음	1	19. 11. 6. AM 8:39	19. 11. 6. AM 8:39
REC 20191106 16:15:53	사용 가능한 권장 사항 없음	1	19. 11. 6. AM 8:16	19. 11. 6. AM 8:16

권장 사항이 성공적으로 게시된 후 상태가 [게시됨]으로 변경됩니다.

다음에 수행할 작업

생성된 권장 사항을 검토하고 게시할지 결정합니다. 생성된 권장 사항 검토 및 게시 항목을 참조하십시오.

생성된 권장 사항 검토 및 게시

생성된 NSX Intelligence 권장 사항이 [게시 준비 완료] 상태가 되면 권장 사항을 검토하고, 필요한 경우 수정한 후 게시 여부를 결정할 수 있습니다.

사전 요구 사항

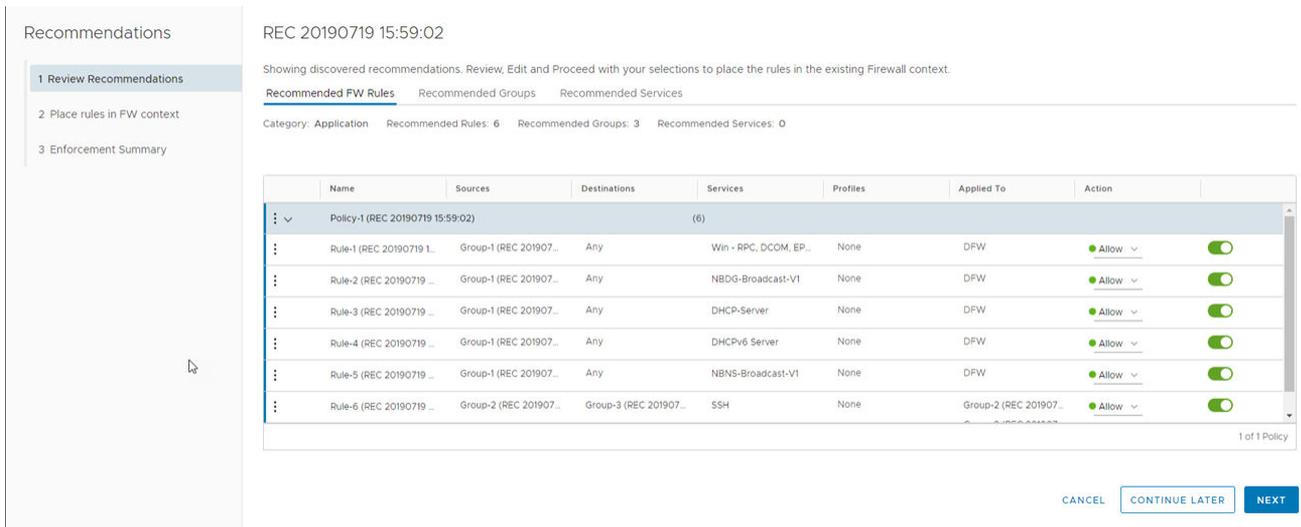
새 권장 사항을 생성합니다. 새 **NSX Intelligence** 권장 사항 생성 항목을 참조하십시오.

절차

1 브라우저에서 엔터프라이즈 관리자 권한으로 <https://<nsx-manager-ip-address>>에서 NSX Manager에 로그인합니다.

- 2 계획 및 문제 해결 > 권장 사항을 클릭합니다.
- 3 표시되는 권장 사항의 목록을 좀 더 좁히려면 화면 오른쪽 상단에 있는 이름, 경로 등을 기준으로 필터링을 클릭하고 사용할 필터 조건을 지정합니다.
- 4 권장 사항을 사용하지 않기로 한 경우 점 3개 메뉴 아이콘을 클릭하고 삭제를 선택합니다.
- 5 권장 사항에 대한 요약을 보려면 권장 사항 이름 옆의 화살표를 클릭하여 행을 확장합니다. 생성된 규칙 수와 영향을 받은 그룹 수를 볼 수 있습니다.
- 6 권장 사항에 대한 세부 정보를 검토 및 관리합니다.
 - a 권장 사항 이름을 클릭합니다.

다음 이미지와 유사하게 권장 사항 마법사가 표시됩니다.



- b 권장 FW 규칙 탭에서 방화벽 규칙 세부 정보를 검토합니다. 세부 정보를 수정하려면 해당 열의 값을 클릭하고 편집(연필) 아이콘을 선택합니다.
- c 패킷이 처리되는 방법을 정의하려면 작업 열에서 허용, 삭제 또는 거절을 선택합니다.
- d 오른쪽의 버튼을 전환하여 규칙을 사용하거나 사용하지 않도록 설정합니다. 기본적으로 생성된 규칙은 이전 단계의 이미지에 표시된 것처럼 게시할 때 사용하도록 설정됩니다.
- e 권장 그룹을 클릭합니다.
- f 멤버 열의 링크를 클릭하여 그룹 권장 사항에 대해 설정된 VM 및 IP에 대한 세부 정보를 검토합니다.
- g 그룹 이름 옆의 메뉴 아이콘(점 3개)을 클릭하고 편집을 선택하여 그룹 권장 사항을 수정합니다.
- h 권장 서비스를 클릭하고 세부 정보를 검토하십시오.
- i 서비스 이름 옆의 메뉴 아이콘(점 3개)을 클릭하고 편집을 선택하여 이름 또는 설명을 수정합니다. 서비스를 삭제하기 전에 서비스를 사용하는 규칙이 없는지 확인합니다.
- j 다음을 클릭합니다.

- 7 **FW 컨텍스트에 규칙 배치** 창에서 규칙 권장 사항이 기존 방화벽 규칙에 적용되는 순서를 변경할 수 있습니다. 강조 표시된 섹션을 끌거나 점 3개 메뉴 아이콘을 클릭한 후 **선택한 섹션 위로 이동** 또는 **선택한 섹션 아래로 이동**을 선택합니다.
- 8 **게시**를 클릭합니다.
- 9 **권장 사항 게시** 대화상자에서 **예**를 클릭합니다.
- 10 [적용 요약] 페이지에서 보안 정책이 성공적으로 게시되었는지 확인하고 **닫기**를 클릭합니다.
권장 사항 테이블에서 권장 사항에 대한 상태 열이 [게시됨]으로 변경됩니다.

결과

보안 정책 권장 사항이 성공적으로 게시되면 **계획 및 문제 해결 > 권장 사항** 탭에서 읽기 전용 모드로 전환됩니다. 게시된 규칙 권장 사항을 보고 관리하려면 **보안 > 분산 방화벽**으로 이동합니다.

중요 규칙 권장 사항을 게시한 후에는 영향을 받는 VM 간에 새 흐름이 생성될 때까지 VM 간에 영향을 받는 흐름을 주황색 화살표(보호되지 않는 흐름)로 계속 표시합니다. 시각화 기능은 호스트에서 발생한 시간을 기준으로 하는 트래픽 흐름만 보고하며, 해당 트래픽 흐름이 발생한 후에 게시된 규칙 집합은 반영하지 않습니다. 규칙 집합이 게시되고 새 트래픽 흐름이 생성되면 새 흐름이 녹색 화살표(허용된 흐름)로 표시됩니다.

NSX Intelligence 백업 및 복원

현재 NSX Intelligence 구성이 작동 불가능 상태가 되거나 이를 이전 상태로 복원하려는 경우 백업에서 구성을 복원할 수 있습니다. 백업 및 복원 워크플로는 NSX Intelligence CLI를 사용해야만 지원됩니다.

백업 시 NSX Intelligence는 NSX Intelligence 장치를 구성하는 모든 서비스에서 사용하는 구성 파일만 백업합니다. 백업에 포함된 시각화 데이터가 없습니다.

NSX Intelligence에서 데이터 손실 또는 손상이 발생할 경우 관련 흐름 및 권장 사항에 대한 모든 기존 데이터도 손실됩니다. NSX Intelligence를 재설치하면 해당 시점부터 네트워크 트래픽 데이터 수집 및 해당 수집된 데이터의 시각화가 다시 시작됩니다.

백업 구성을 완료한 후에는 언제든지 NSX Intelligence 장치에서 백업 명령을 수동으로 실행할 수 있습니다. 백업은 백업 구성 중에 정의된 원격 서버에서 암호화, 압축 및 저장됩니다. 백업을 생성할 때 백업이 생성된 날짜와 시간이 백업 파일 이름에 추가되어 각 백업 파일이 고유해집니다. 예: config-backup-2019-06-21T21_06_07UTC.tar.gz.

NSX Intelligence 백업을 복원하면 백업이 캡처되었을 때의 구성 상태가 복원됩니다. 백업 파일이 생성된 NSX Intelligence 장치와 동일한 버전을 실행 중인 NSX Intelligence 장치로 백업을 복원해야 합니다. 기존 NSX Intelligence 장치로 복원하거나 새로 설치된 NSX Intelligence 장치로 복원할 수 있지만 백업한 NSX Intelligence 장치와 동일한 버전이어야 합니다.

NSX Intelligence 백업 구성

NSX Intelligence 구성을 백업하려면 먼저 백업 파일 서버를 구성해야 합니다. 백업 파일 서버가 구성된 후에는 언제든지 NSX Intelligence를 백업할 수 있습니다.

사전 요구 사항

- NSX Intelligence CLI에 대한 CLI 관리 자격 증명이 있는지 확인합니다.
- 원격 서버에 대한 사용자 이름과 암호가 있는지 확인합니다.
- 원격 서버에 백업 파일이 저장될 파일 경로를 가져옵니다.

절차

- 1 명령줄 프롬프트에서 NSX Intelligence CLI 호스트에 관리자 권한으로 로그인합니다.

```
$ ssh admin@ "cli-ip-address"
admin@ "cli-ip-address" 's password:
```

- 2 백업 파일 서버를 구성합니다.

명령 구문은 다음과 같습니다.

```
set backup remote-host "remote_host_address" remote-path "remote_folder_path" remote-
host-username "remote_host_username" remote-host-password "remote_host_password"
passphrase "pass_phrase"
```

여기서 "remote_host_address" 는 백업 파일 서버의 원격 호스트 IP 또는 FQDN 주소이고, "remote_host_username" 계정에는 "remote_folder_path" 에서 백업 파일을 생성하는 데 필요한 권한이 있어야 합니다. passphrase 매개 변수에 강력한 값을 제공해야 합니다. 길이는 8자 이상이어야 하며 하나 이상의 대문자, 소문자 및 특수 문자를 포함해야 합니다. 예를 들면 다음과 같습니다.

```
set backup remote-host 10.11.22.33 remote-path /root remote-host-username root remote-host-
password MyRemotePassword passphrase MyPassPhra$e
```

- 3 구성을 확인합니다.

```
get configuration
```

출력에서 set backup이 있는 줄이 올바르게 나타나는지 확인합니다. 이전 단계의 예제를 사용할 경우 출력에 다음 줄이 포함되어야 합니다.

```
set backup remote-host 10.11.22.33 remote-path /root remote-host-username root
```

NSX Intelligence 백업

CLI 명령을 사용하여 NSX Intelligence 장치 구성 파일을 백업할 수 있습니다.

사전 요구 사항

- NSX Intelligence CLI에 대한 관리자 액세스 권한이 있는지 확인합니다.

- 백업 파일 서버를 구성합니다. **NSX Intelligence** 백업 구성 항목을 참조하십시오.

절차

- 1 NSX Intelligence CLI에 관리자 권한으로 로그인합니다.
- 2 백업을 생성합니다.

```
backup intelligence configuration
```

성공적으로 백업되면 다음과 유사한 메시지가 표시됩니다.

```
Backup Complete. Archived at: "backup_file_server-IP_address" :/root/backup_archives/
intelligence-config-backup-2019-07-18T07_00_26UTC.tar.gz
```

- 3 다른 CLI 세션을 사용하여 백업 진행 과정을 볼 수 있습니다.
 - a 다른 NSX Intelligence CLI 세션에 로그인합니다.
 - b 다음 명령을 입력합니다.

```
get log-file node-mgmt.log follow
```

NSX Intelligence 백업 복원

백업을 복원하면 백업이 생성되었을 때 NSX Intelligence 구성의 상태가 복원됩니다. CLI 명령을 사용하여 NSX Intelligence 백업을 복원할 수 있습니다.

복원 중인 백업과 동일한 버전인 NSX Intelligence 장치의 설치에서 백업을 복원해야 합니다. 기본적으로 복원된 백업 파일은 가장 최근에 생성된 백업입니다. 새로 설치된 NSX Intelligence 장치에 백업을 복원하는 경우 백업을 복원하기 전에 아카이브 이름을 설정합니다.

사전 요구 사항

- 백업 파일 서버의 관리자 로그인 자격 증명 및 호스트 정보가 있는지 확인합니다.
- NSX Intelligence CLI에 대한 관리자 액세스 권한이 있는지 확인합니다.

절차

- 1 새 NSX Intelligence CLI 서버에 관리자 권한으로 로그인합니다.
- 2 백업이 있는 원격 서버를 구성합니다.

명령 구문은 다음과 같습니다.

```
set restore remote-host "backup_server_IP_address" remote-path "remote_folder_path"
remote-host-username "remote_host_username" remote-host-password
"remote_host_password" passphrase "pass_phrase"
```

여기서 "backup_server_IP_address" 는 백업 파일 서버의 원격 호스트 IP 또는 FQDN 주소이고, "remote_host_username" 계정에는 "remote_folder_path" 에서 백업 파일에 액세스하는 데 필요한 권한이 있어야 합니다. 예를 들면 다음과 같습니다.

```
set restore remote-host 10.11.22.33 remote-path /root remote-host-username root remote-host-password MyRemotePassword passphrase MyPassPhra$e
```

3 복원 구성을 확인합니다.

```
get configuration
```

출력에서 set restore이 있는 줄이 올바르게 나타나는지 확인합니다. 이전 단계의 예제를 사용할 경우 출력에 다음 줄이 포함되어야 합니다.

```
set restore remote-host 10.11.22.33 remote-path /root remote-host-username root
```

4 다음 명령을 사용하여 백업을 복원합니다.

```
restore intelligence configuration
```

성공적으로 복원되면 다음과 유사한 메시지가 표시됩니다.

```
NSX Intelligence Restore Complete.
```

5 다른 CLI 세션을 사용하여 백업 복원의 진행 과정을 볼 수 있습니다.

- a 다른 NSX Intelligence CLI 세션에 로그인합니다.
- b 다음 명령을 입력합니다.

```
get log-file node-mgmt.log follow
```

NSX Intelligence 문제 해결

NSX Intelligence 장치가 응답하지 않거나 장치를 사용하는 동안 수신한 오류 메시지에 대한 자세한 정보가 필요한 경우에는 특정 명령을 실행하여 NSX Intelligence 서비스의 상태를 가져올 수 있습니다.

또한 지원 번들을 수집하여 발생했을 수 있는 문제를 디버깅할 때 유용하게 사용하거나 VMware 지원 담당자를 지원할 수 있습니다.

NSX Intelligence 장치의 상태 확인

만약 NSX Intelligence 장치가 응답하지 않을 경우 NSX Intelligence 서비스의 상태를 확인합니다.

문제

NSX Intelligence 장치가 응답하지 않거나 장치가 예상대로 작동하지 않음을 나타내는 오류 메시지가 수신되었습니다.

원인

하나 이상의 기본 NSX Intelligence 서비스가 중지되었거나 정상 상태가 아닐 수 있습니다.

해결책

- 1 엔터프라이즈 관리자 역할이 있는 계정을 사용하여 NSX Intelligence 장치 CLI 호스트에 로그인합니다.
- 2 `get services` 명령을 사용하여 NSX Intelligence 서비스의 상태를 확인합니다.

모든 NSX Intelligence 서비스가 제대로 작동하는 경우 다음 예와 비슷한 출력이 표시됩니다.

```
my_nsx-intel> get services
Service name:          druid
Service state:         running
Coordinator health:    good
Broker health:         good
Historical health:     good
Overlord health:       good
MiddleManager health:  good

Service name:          http
Service state:         running
Session timeout:       1800
Connection timeout:    30
Redirect host:         (not configured)
Client API rate limit: 100 requests/sec
Client API concurrency limit: 40
Global API concurrency limit: 199

Service name:          kafka
Service state:         running
Service health:        good

Service name:          liagent
Service state:         stopped

Service name:          mgmt-plane-bus
Service state:         stopped

Service name:          node-mgmt
Service state:         running

Service name:          nsx-config
Service state:         running

Service name:          nsx-message-bus
Service state:         stopped

Service name:          nsx-upgrade-agent
Service state:         running

Service name:          ntp
Service state:         running
```

```

Start on boot:           True

Service name:           pace-server
Service state:         running

Service name:           postgres
Service state:         running
Service health:        good

Service name:           processing
Service state:         running

Service name:           snmp
Service state:         stopped
Start on boot:         False

Service name:           spark
Service state:         running
Service health:        good

Service name:           spark-job-scheduler
Service state:         running

Service name:           ssh
Service state:         running
Start on boot:         True

Service name:           syslog
Service state:         running

Service name:           ui-service
Service state:         running

Service name:           zookeeper
Service state:         running
Service health:        good

my_nsx-intel>

```

서비스 상태가 실행 중 또는 중지됨일 수 있습니다. 서비스 상태가 정상 또는 성능 저하됨일 수 있습니다.

- 3 syslog 파일을 보고, NSX Intelligence 서비스의 상태를 syslog 파일에 기록하는 `pace-monitor.sh` 상태 점검 스크립트의 출력을 검색합니다.

모든 서비스가 예상대로 작동하는 경우 `get log-file syslog | find pace-monitor` 명령을 실행한 후에 다음 샘플 출력과 비슷한 결과가 나타납니다.

```

my_nsx-intel> get log-file syslog | find pace-monitor
<13>1 2019-08-30T03:19:20.409899+00:00 my_nsx-intel pace-monitor.sh - - -   "_self": {
<13>1 2019-08-30T03:19:20.410253+00:00 my_nsx-intel pace-monitor.sh - - -   "href": "/
node/pace/appliance-health",
<13>1 2019-08-30T03:19:20.410623+00:00 my_nsx-intel pace-monitor.sh - - -   "rel":
"self"

```

```

<13>1 2019-08-30T03:19:20.410908+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.411162+00:00 my_nsx-intel pace-monitor.sh - - - "appliance-
health": {
<13>1 2019-08-30T03:19:20.411416+00:00 my_nsx-intel pace-monitor.sh - - - "status":
"Following NSX Intelligence first boot services are either PENDING or FAILED - Token-
Registration",
<13>1 2019-08-30T03:19:20.411668+00:00 my_nsx-intel pace-monitor.sh - - - "sub-system-
status": {
<13>1 2019-08-30T03:19:20.411923+00:00 my_nsx-intel pace-monitor.sh - - - "app-
services": {
<13>1 2019-08-30T03:19:20.412280+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [],
<13>1 2019-08-30T03:19:20.412528+00:00 my_nsx-intel pace-monitor.sh - - -
"status": ""
<13>1 2019-08-30T03:19:20.412807+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.413075+00:00 my_nsx-intel pace-monitor.sh - - - "base-
infra-services": {
<13>1 2019-08-30T03:19:20.413303+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [
<13>1 2019-08-30T03:19:20.413613+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.413848+00:00 my_nsx-intel pace-monitor.sh - - -
"druid-health": {
<13>1 2019-08-30T03:19:20.414146+00:00 my_nsx-intel pace-monitor.sh - - -
"broker": "good",
<13>1 2019-08-30T03:19:20.414473+00:00 my_nsx-intel pace-monitor.sh - - -
"coordinator": "good",
<13>1 2019-08-30T03:19:20.414717+00:00 my_nsx-intel pace-monitor.sh - - -
"historical": "good",
<13>1 2019-08-30T03:19:20.414979+00:00 my_nsx-intel pace-monitor.sh - - -
"middlemanager": "good",
<13>1 2019-08-30T03:19:20.415295+00:00 my_nsx-intel pace-monitor.sh - - -
"overlord": "good"
<13>1 2019-08-30T03:19:20.415533+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.415762+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "druid"
<13>1 2019-08-30T03:19:20.415982+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.416269+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.416539+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.416772+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "kafka"
<13>1 2019-08-30T03:19:20.416991+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.417204+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.417510+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.417745+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "postgres"
<13>1 2019-08-30T03:19:20.418133+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.418389+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.418626+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.418855+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "spark"
<13>1 2019-08-30T03:19:20.419157+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.419435+00:00 my_nsx-intel pace-monitor.sh - - - {

```

```

<13>1 2019-08-30T03:19:20.419684+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.419928+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "zookeeper"
<13>1 2019-08-30T03:19:20.420165+00:00 my_nsx-intel pace-monitor.sh - - -      }
<13>1 2019-08-30T03:19:20.420496+00:00 my_nsx-intel pace-monitor.sh - - -      ],
<13>1 2019-08-30T03:19:20.420786+00:00 my_nsx-intel pace-monitor.sh - - -
"status": ""
<13>1 2019-08-30T03:19:20.421022+00:00 my_nsx-intel pace-monitor.sh - - -      },
<13>1 2019-08-30T03:19:20.421255+00:00 my_nsx-intel pace-monitor.sh - - -      "first-
boot-services": {
<13>1 2019-08-30T03:19:20.421539+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [
<13>1 2019-08-30T03:19:20.421777+00:00 my_nsx-intel pace-monitor.sh - - -      {
<13>1 2019-08-30T03:19:20.422010+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "degraded",
<13>1 2019-08-30T03:19:20.422277+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "token-registration"
<13>1 2019-08-30T03:19:20.422512+00:00 my_nsx-intel pace-monitor.sh - - -      }
<13>1 2019-08-30T03:19:20.422770+00:00 my_nsx-intel pace-monitor.sh - - -      ],
<13>1 2019-08-30T03:19:20.423012+00:00 my_nsx-intel pace-monitor.sh - - -
"status": "Following NSX Intelligence first boot, services are either PENDING or FAILED -
Token-Registration"
<13>1 2019-08-30T03:19:20.423354+00:00 my_nsx-intel pace-monitor.sh - - -      }
<13>1 2019-08-30T03:19:20.423601+00:00 my_nsx-intel pace-monitor.sh - - -      }
<13>1 2019-08-30T03:19:20.423882+00:00 my_nsx-intel pace-monitor.sh - - -      }
<13>1 2019-08-30T03:19:20.424339+00:00 my_nsx-intel pace-monitor.sh - - -      }
<13>1 2019-08-30T03:19:20.972629+00:00 my_nsx-intel pace-monitor.sh - - - NSX
Intelligence health OK.
<30>1 2019-08-30T03:19:20.973076+00:00 my_nsx-intel pace-monitor 20804 - - <13>Aug 30
03:19:19 pace-monitor.sh: NSX Intelligence health OK.
<182>1 2019-08-30T03:23:23.857Z my_nsx-intel NSX 21752 - [nsx@6876 comp="nsx-cli"
subcomp="node-mgmt" username="admin" level="INFO"] CMD: get log-file syslog | find pace-
monitor

```

서비스 중 하나에 문제가 있으면 `get log-file syslog | grep pace-monitor`를 실행할 때 다음 줄이 표시될 수 있습니다.

```
NSX Intelligence health DEGRADED. Return code not HTTP OK.
```

4 다음 출력 중 하나가 표시되면 `restart service service-name` 명령을 사용하여 서비스를 다시 시작합니다.

- `get services` 명령을 실행한 후에 서비스 중 하나에 서비스 상태: 중지됨 또는 서비스 상태: 성능 저하됨이 표시됩니다.
- `get log-file syslog | grep pace-monitor` 명령을 실행한 후에 PACE health DEGRADED. Return code not HTTP OK. 메시지와 비슷한 출력이 표시됩니다.

예를 들어, postgres 서비스 상태가 중지됨으로 표시되거나 서비스 상태가 실행 중으로 표시되지만 실제로는 서비스 상태가 성능 저하됨이면 다음 명령을 실행합니다.

```
restart service postgres
```

중요 NSX Intelligence 서비스를 다시 시작하려면 `restart service service-name` 명령을 사용해야 합니다. 대신 `stop service service-name` 및 `start service service-name` 명령을 사용하기로 한 경우 `service-name`에 의존하는 각 서비스를 수동으로 다시 시작해야 합니다. 다음 목록에는 NSX Intelligence 서비스를 다시 시작해야 하는 종속성 순서가 나와 있습니다.

```
zookeeper > druid > kafka > spark > spark-job-scheduler > nsx-config > processing > pace-server
```

예를 들어 nsx-config 서비스를 중지했다가 `stop|start service service-name` 명령을 사용하여 시작하는 경우 `restart service service-name` 명령을 사용하여 processing 및 pace-server 서비스를 다시 시작해야 합니다.

또한, `restart service service-name` 명령을 사용하여 spark-job-scheduler 서비스 이전에 종속성 순서 목록에 표시된 서비스를 다시 시작하는 경우에는 `restart service spark-job-scheduler` 명령을 사용하여 spark-job-scheduler 서비스를 수동으로 다시 시작해야 합니다. 그렇게 하지 않으면 spark-job-scheduler 서비스가 잘못된 상태가 됩니다.

NSX Intelligence 지원 번들 수집

NSX Intelligence CLI를 사용하여 지원 번들을 수집할 수 있습니다.

지원 번들 파일 콘텐츠는 데이터를 포함하지 않습니다. 여기에는 다음 디렉토리의 파일이 포함됩니다.

- /opt/vmware/*
- /var/log/*
- /etc/*
- journalctl 및 systemctl을 사용하는 시스템 상태

사전 요구 사항

NSX Intelligence CLI에 대한 엔터프라이즈 관리자 액세스 권한이 있는지 확인합니다.

절차

- 1 엔터프라이즈 관리자 역할 권한이 있는 계정을 사용하여 NSX Intelligence CLI에 로그인합니다.
- 2 지원 번들을 생성합니다.

명령 구문은 다음과 같습니다. 여기서 "support_filename" .tgz의 값을 제공합니다.

```
get support-bundle file "support_filename" .tgz
```

예를 들면 다음과 같습니다.

```
get support-bundle file support_bundle123.tgz
```

번들 파일이 성공적으로 생성되면 다음 예와 유사한 메시지가 표시됩니다.

```
support_bundle123.tgz가 생성되었습니다. 다음 명령을 사용하여 파일을 전송하십시오. copy file  
support_bundle123.tgz url <url> support_bundle123.tgz를 전송한 후에는 tar xvf  
support_bundle123.tgz를 압축을 푸십시오.
```

3 다음 명령을 사용하여 지원 번들이 있는지 확인합니다.

```
get files
```

다음과 유사한 출력이 표시됩니다.

```
Directory of filestore:/  
-rw- 21377586 June 29 05:29:12 UTC support_bundle123.tgz
```