

# vSphere 네트워킹

업데이트 3

VMware vSphere 8.0

VMware ESXi 8.0

vCenter Server 8.0

VMware by Broadcom 웹 사이트

<https://docs.vmware.com/kr>에서 최신 기술 문서를 찾을 수 있습니다.

**VMware by Broadcom**

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

Copyright © 2009-2024 Broadcom. All Rights Reserved. “Broadcom”은 Broadcom Inc. 및/또는 해당 자회사를 뜻합니다. 자세한 내용은 <https://www.broadcom.com> 페이지를 참조하십시오. 여기에서 언급된 모든 상표, 상호, 서비스 마크 및 로고는 해당 회사의 소유입니다.

# 목차

vSphere 네트워킹 정보	12
<b>1 vSphere 네트워킹 소개</b>	<b>13</b>
<b>2 vSphere 표준 스위치를 사용하여 네트워킹을 설정하는 방법</b>	<b>17</b>
vSphere 표준 스위치 생성	19
가상 시스템의 포트 그룹 구성	20
가상 시스템 포트 그룹 추가	21
표준 스위치 포트 그룹 편집	22
vSphere 표준 스위치에서 포트 그룹 제거	23
vSphere 표준 스위치 속성	23
vSphere 표준 스위치의 MTU 크기 변경	23
물리적 어댑터의 속도 변경	24
vSphere Standard 스위치에 물리적 어댑터 할당	24
vSphere Standard 스위치의 토폴로지	25
<b>3 vSphere Distributed Switch를 사용하여 네트워킹을 설정하는 방법</b>	<b>26</b>
네트워크 오프로드 호환성이란?	30
vSphere Distributed Switch 생성	31
최신 버전으로 vSphere Distributed Switch 업그레이드	34
일반 및 고급 vSphere Distributed Switch 설정 편집	36
vSphere Distributed Switch의 여러 호스트에서 네트워킹 관리	37
vSphere Distributed Switch의 호스트 네트워킹 관리 작업	39
vSphere Distributed Switch에 호스트 추가	41
vSphere Distributed Switch에서 물리적 네트워크 어댑터 구성	43
VMkernel 어댑터를 vSphere Distributed Switch로 마이그레이션	45
vSphere Distributed Switch에서 VMkernel 어댑터 생성	46
가상 시스템 네트워킹을 vSphere Distributed Switch로 마이그레이션	48
vSphere Distributed Switch에서 호스트 제거	49
호스트 프록시 스위치의 네트워킹 관리	50
호스트의 네트워크 어댑터를 vSphere Distributed Switch로 마이그레이션	50
호스트의 VMkernel 어댑터를 vSphere 표준 스위치로 마이그레이션	51
vSphere Distributed Switch에 호스트의 물리적 NIC 할당	52
vSphere Distributed Switch에서 물리적 NIC 제거	52
활성 가상 시스템에서 NIC 제거	52
분산 포트 그룹	53

- 분산 포트 그룹 추가 53
- 일반적인 분산 포트 그룹 설정 편집 60
- 분산 포트 그룹 제거 60
- 분산 포트 사용 61
  - vSphere Client에서 분산 포트의 상태 모니터링 61
  - vSphere Client 분산 포트 설정 구성 62
- vSphere Distributed Switch에 가상 시스템 네트워킹 구성 63
  - 가상 시스템과 vSphere Distributed Switch 간 마이그레이션 63
  - 분산 포트 그룹에 개별 가상 시스템 연결 63
- vSphere Distributed Switch 토폴로지 64
  - vSphere Distributed Switch의 토폴로지 보기 65
  - 호스트 프록시 스위치의 토폴로지 보기 66
  - 네트워크 오프로드 스위치의 토폴로지 보기 66

#### 4 VMkernel 네트워킹을 설정하는 방법 67

- VMkernel 네트워킹 계층 68
  - 호스트에서 VMkernel 어댑터에 대한 정보 보기 71
- vSphere 표준 스위치에서 VMkernel 어댑터 생성 71
- vSphere Distributed Switch와 연결된 호스트에서 VMkernel 어댑터 생성 74
- VMkernel 어댑터 구성 편집 77
- VMkernel 기본 게이트웨이 재정의 79
- Esxcli 명령을 사용하여 VMkernel 어댑터 게이트웨이 구성 80
- esxcli 명령을 사용하여 resolv.conf 파일 구성 81
- ESXCLI 명령을 사용하여 DNS 호스트 파일 구성 83
- 호스트의 TCP/IP 스택 구성 보기 84
- 호스트의 TCP/IP 스택 구성 변경 84
  - 명시적 정체 알림 85
- 사용자 지정 TCP/IP 스택 생성 86
- VMkernel 어댑터 제거 86

#### 5 vSphere Distributed Switch의 LACP 지원 87

- 분산 포트 그룹에 대한 LACP 팀 구성 및 페일오버 구성 89
- 분산 포트 그룹에 대한 트래픽을 처리하기 위한 링크 집계 그룹 구성 90
- 링크 집계 그룹 편집 94
- vSphere Distributed Switch에 대한 LACP 지원의 제한 사항 95

#### 6 네트워크 구성 백업 및 복원 97

- vSphere Distributed Switch 구성 백업 및 복원 97
  - vSphere Distributed Switch 구성 내보내기 97
  - vSphere Distributed Switch 구성 가져오기 98

vSphere Distributed Switch 구성 복원	99
vSphere 분산 포트 그룹 구성 내보내기, 가져오기 및 복원	99
vSphere 분산 포트 그룹 구성 내보내기	99
vSphere 분산 포트 그룹 구성 가져오기	100
vSphere 분산 포트 그룹 구성 복원	100
ESXi Configuration Manager 통합	101
호스트 구성 내보내기	101
호스트 구성 가져오기	102

## 7 관리 네트워크의 롤백 및 복구 104

vSphere 네트워킹 롤백	104
네트워크 롤백 사용 안 함	105
vCenter Server 구성 파일을 사용하여 네트워크 롤백을 사용하지 않도록 설정	106
vSphere Distributed Switch의 관리 네트워크 구성에서 오류 해결	106

## 8 vSphere 네트워킹 정책 108

vSphere Standard 또는 Distributed Switch에 네트워킹 정책 적용	109
포트 수준에서 네트워킹 정책 재정의 구성	110
팀 구성 및 페일오버 정책이란?	111
가상 스위치에 사용 가능한 로드 밸런싱 알고리즘	112
원래 가상 포트 기준 라우팅	113
소스 MAC 해시 기준 라우팅	114
IP 해시 기준 라우팅	114
물리적 NIC 로드 기준 라우팅	116
명시적 페일오버 명령 사용	116
vSphere 표준 스위치 또는 표준 포트 그룹에서 NIC 팀 구성, 페일오버 및 로드 밸런싱 구성	116
분산 포트 그룹 또는 분산 포트에서 NIC 팀 구성, 페일오버 및 로드 밸런싱 구성	118
VLAN 정책이란?	121
분산 포트 그룹 또는 분산 포트에서 VLAN 태그 지정 구성	121
업링크 포트 그룹 또는 업링크 포트에 VLAN 태그 지정 구성	122
보안 정책이란?	123
vSphere 표준 스위치 또는 표준 포트 그룹에 대한 보안 정책 구성	123
분산 포트 그룹 또는 분산 포트에 대한 보안 정책 구성	125
트래픽 조절 정책이란?	126
vSphere 표준 스위치 또는 표준 포트 그룹의 트래픽 조절 구성	127
분산 포트 그룹 또는 분산 포트의 트래픽 조절 정책 편집	128
리소스 할당 정책이란?	129
분산 포트 그룹의 리소스 할당 정책 편집	129
모니터링 정책이란?	130
분산 포트 그룹 또는 분산 포트에서 NetFlow 모니터링 관리	130

트래픽 필터링 및 표시 정책이란?	131
분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 필터링 및 표시	131
분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 필터링 및 표시 사용	132
분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 표시	133
분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 필터링	135
분산 포트 그룹 또는 업링크 포트 그룹의 네트워크 트래픽 규칙	136
분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 필터링 및 표시 사용 안 함	139
분산 포트 또는 업링크 포트의 트래픽 필터링 및 표시	139
분산 포트 또는 업링크 포트의 트래픽 필터링 및 표시 사용	140
분산 포트 또는 업링크 포트의 트래픽 표시	141
분산 포트 또는 업링크 포트에 대한 트래픽 필터링	142
분산 포트 또는 업링크 포트의 네트워크 트래픽 규칙	144
분산 포트 또는 업링크 포트의 트래픽 필터링 및 표시 사용 안 함	147
필터링 및 표시할 트래픽 한정	148
시스템 트래픽 한정자	148
MAC 트래픽 한정자	148
IP 트래픽 한정자	150
vSphere Distributed Switch에서 여러 포트 그룹에 대한 정책 관리	150
포트 차단 정책	154
분산 포트 그룹의 포트 차단 정책 편집	154
분산 포트 또는 업링크 포트의 차단 정책 편집	155
MAC 학습 정책이란?	155
<b>9 VLAN을 사용하여 네트워크 트래픽을 분리하는 방법</b>	<b>157</b>
VLAN 구성	157
전용 VLAN	158
전용 VLAN 생성	158
기본 전용 VLAN 제거	159
보조 전용 VLAN 제거	159
<b>10 네트워크 리소스 관리</b>	<b>161</b>
DirectPath I/O	161
호스트의 네트워크 디바이스에 대한 패스스루 사용	162
가상 시스템에 PCI 디바이스 구성	162
VMDirectPath I/O 디바이스에 대한 무중단 추가 및 무중단 제거 지원	163
VMDirectPath I/O 디바이스의 무중단 추가 및 무중단 제거 사용	165
VM 준비 및 구성	166
vSphere Client를 사용하여 핫 플러그 작업이 성공했는지 확인	167
VM을 사용하여 핫 플러그 작업이 성공했는지 확인	167
SR-IOV(단일 루트 I/O 가상화)란?	168

SR-IOV 지원	169
SR-IOV 구성 요소 아키텍처 및 상호 작용	170
vSphere와 가상 기능의 상호 작용	172
DirectPath I/O 및 SR-IOV	173
SR-IOV를 사용하도록 가상 시스템 구성	173
호스트 물리적 어댑터에서 SR-IOV 사용	174
가상 시스템에 SR-IOV 패스스루 어댑터로 가상 기능 할당	175
SR-IOV 지원 가상 시스템과 관련된 트래픽에 대한 네트워킹 옵션	176
SR-IOV 물리적 어댑터를 사용하여 가상 시스템 트래픽 처리	176
호스트 프로파일 또는 ESXCLI 명령을 사용하여 SR-IOV 사용	177
호스트 프로파일에서 SR-IOV 사용	177
ESXCLI 명령을 통해 호스트의 물리적 어댑터에서 SR-IOV를 사용하도록 설정	178
가상 시스템에 대한 RDMA란?	179
PVRDMA 지원	179
PVRDMA를 사용하도록 ESXi 호스트 구성	181
PVRDMA용 VMkernel 어댑터 태그 지정	181
PVRDMA에 대한 방화벽 규칙 사용	181
가상 시스템에 PVRDMA 어댑터 할당	182
PVRDMA 네이티브 끝점을 사용하도록 가상 시스템 구성	183
PVRDMA 비동기 모드를 사용하도록 가상 시스템 구성	183
RDMA over Converged Ethernet의 네트워크 요구 사항	184
Remote Direct Memory Access 네트워크 어댑터 구성	185
RDMA 가능 네트워크 어댑터 보기	185
Remote Direct Memory Access 네트워크 어댑터 구성	186
점보 프레임이란?	188
vSphere Distributed Switch에서 점보 프레임 사용	189
vSphere 표준 스위치에서 점보 프레임 사용	189
VMkernel 어댑터에 대한 점보 프레임 사용	189
가상 시스템에서 점보 프레임 지원 기능 사용	190
TCP 세분화 오프로드란?	191
VMkernel에서 소프트웨어 TSO 관리	191
TSO가 ESXi 호스트의 물리적 네트워크 어댑터에서 지원되는지 확인하는 방법	192
ESXi 호스트에서 TSO 관리	192
ESXi 호스트에서 TSO가 사용되도록 설정되어 있는지 확인하는 방법	193
Linux 가상 시스템에서 TSO 관리	193
Windows 가상 시스템에서 TSO 관리	194
대규모 수신 오프로드란?	194
ESXi 호스트의 모든 VMXNET3 어댑터에 대해 하드웨어 LRO 관리	194
ESXi 호스트의 모든 VMXNET3 어댑터에 대해 소프트웨어 LRO 관리	195
LRO가 ESXi 호스트의 VMXNET3 어댑터에 대해 사용하도록 설정되어 있는지 확인	195

VMXNET 3 어댑터의 LRO 버퍼 크기 변경	196
ESXi 호스트에서 모든 VMkernel 어댑터에 대해 LRO 활성화 또는 비활성화	196
VMkernel 어댑터에 대한 LRO 버퍼의 크기 변경	197
Linux 가상 시스템의 VMXNET3 어댑터에서 LRO 관리	197
Windows 가상 시스템의 VMXNET3 어댑터에서 LRO 관리	197
Windows 가상 시스템에서 전체적으로 LRO 관리	198
NetQueue 및 네트워킹 성능	199
호스트에서 NetQueue 활성화	199
호스트에서 NetQueue 비활성	199

## 11 vSphere Network I/O Control 201

vSphere Network I/O Control이란?	201
vSphere Distributed Switch에서 Network I/O Control 사용	202
시스템 트래픽에 대한 대역폭 할당	203
시스템 트래픽에 대한 대역폭 할당 매개 변수	203
시스템 트래픽에 대한 대역폭 예약 예제	204
시스템 트래픽에 대한 대역폭을 할당하는 방법	204
가상 시스템 트래픽에 대한 대역폭 할당	205
가상 시스템에 대역폭을 할당하는 방법	205
가상 시스템 트래픽에 대한 대역폭 할당 매개 변수	207
가상 시스템 대역폭에 대한 승인 제어	208
네트워크 리소스 풀 생성	209
네트워크 리소스 풀에 분산 포트 그룹 추가	210
가상 시스템에 대한 대역폭 할당 구성	211
여러 가상 시스템에서 대역폭 할당 구성	212
네트워크 리소스 풀의 할당량 수정	213
네트워크 리소스 풀에서 분산 포트 그룹 제거	213
네트워크 리소스 풀 삭제	214
Network I/O Control 외부로 물리적 어댑터 이동	214

## 12 MAC 주소 관리 216

vCenter Server에서 MAC 주소 지정	216
VMware OUI 할당이란?	217
접두사 기반 MAC 주소 할당이란?	217
범위 기반 MAC 주소 할당이란?	218
MAC 주소 할당	218
범위 또는 접두사 기반 할당으로 변경 또는 조정	218
할당 유형 설정 또는 변경	219
ESXi 호스트에서 MAC 주소 생성	220
가상 시스템에 대해 정적 MAC 주소를 설정하는 방법	221



- 정적 MAC 주소의 VMware OUI 221
- 정적 MAC 주소 할당 222
- 가상 시스템 구성 파일에서 정적 MAC 주소 할당 222

### 13 IPv6에 대한 vSphere 구성 224

- vSphere IPv6 연결 224
- IPv6에 vSphere 배포 226
  - vSphere 설치에서 IPv6 사용 226
  - 업그레이드된 vSphere 환경에서 IPv6 사용 227
- 호스트에서 IPv6 지원 활성화 또는 비활성화 229
- ESXi 호스트에서 IPv6 설정 230
- vCenter Server에서 IPv6 설정 230

### 14 네트워크 연결 및 트래픽 모니터링 232

- 네트워크 패킷을 캡처하는 방법 232
- pktcap-uw 유틸리티를 사용하여 네트워크 패킷 캡처 및 추적 234
  - 패킷 캡처를 위한 pktcap-uw 명령 구문 234
  - 패킷 추적을 위한 pktcap-uw 명령 구문 237
  - 출력 제어를 위한 pktcap-uw 옵션 238
  - 패킷 필터링을 위한 pktcap-uw 옵션 238
  - pktcap-uw 유틸리티를 사용하여 패킷 캡처 240
    - 물리적 어댑터에 도달하는 패킷 캡처 240
    - VMXNET3 가상 시스템 어댑터에 대한 패킷을 캡처하는 방법 242
    - VMkernel 어댑터에 대한 패킷을 캡처하는 방법 244
    - 손실된 패킷을 캡처하는 방법 245
    - DVFilter 수준에서 패킷을 캡처하는 방법 246
    - pktcap-uw 유틸리티의 캡처 시점을 사용하는 방법 247
  - pktcap-uw 유틸리티를 사용하여 패킷을 추적하는 방법 250
- vSphere Distributed Switch의 NetFlow 설정 구성 251
- 포트 미러링이란? 252
  - 포트 미러링 상호 운용성이란? 252
  - 포트 미러링 세션 생성 254
    - 포트 미러링 세션 유형 254
    - 포트 미러링 이름 및 세션 세부 정보 255
    - 포트 미러링 소스 256
    - 포트 미러링 대상 257
  - 포트 미러링 세션 세부 정보 보기 258
  - 포트 미러링 세션 세부 정보, 소스 및 대상 편집 258
- vSphere Distributed Switch 상태 점검 259
  - vSphere Distributed Switch 상태 점검 관리 260

- vSphere Distributed Switch 상태 보기 260
  - 스위치 탐색 프로토콜 261
    - vSphere Distributed Switch에서 Cisco 탐색 프로토콜 사용 261
    - vSphere Distributed Switch에서 링크 계층 탐색 프로토콜 사용 262
    - 스위치 정보 보기 262
  - NSX 가상 Distributed Switch의 토폴로지 보기 263
- 15 가상 시스템 네트워킹에 대한 프로토콜 프로파일 구성 264**
  - 네트워크 프로토콜 프로파일 추가 264
    - 네트워크 프로토콜 프로파일 이름 및 네트워크 선택 266
    - 네트워크 프로토콜 프로파일 IPv4 구성 지정 267
    - 네트워크 프로토콜 프로파일 IPv6 구성 지정 267
    - 네트워크 프로토콜 프로파일 DNS 및 기타 구성 지정 268
    - 네트워크 프로토콜 프로파일 생성 완료 268
  - 네트워크 프로토콜 프로파일과 포트 그룹 연결 268
  - 네트워크 프로토콜 프로파일을 사용하여 가상 시스템 또는 vApp에 IP 주소 할당 269
- 16 멀티캐스트 필터링이란? 271**
  - 멀티캐스트 필터링 모드 271
  - vSphere Distributed Switch에서 멀티캐스트 스누핑 사용 272
  - 멀티캐스트 스누핑에 대한 쿼리 시간 간격 편집 273
  - IGMP 및 MLD의 소스 IP 주소 개수 편집 273
- 17 상태 비저장 네트워크 배포란? 275**
- 18 vSphere 네트워킹 모범 사례 277**
- 19 vSphere 네트워킹 문제 해결 279**
  - vSphere 구현 문제 해결을 위한 지침 279
    - 증상 식별 280
    - 문제 공간 정의 280
    - 가능한 솔루션 테스트 281
  - vCenter Server 로그를 사용하여 문제 해결 281
  - MAC 주소 할당 문제 해결 282
    - 동일한 네트워크에 있는 가상 시스템의 중복된 MAC 주소 283
    - MAC 주소 충돌로 인해 가상 시스템 전원 켜기 시도가 실패함 285
  - vSphere Distributed Switch에서 호스트를 제거할 수 없음 286
  - vSphere Distributed Switch의 호스트와 vCenter Server의 연결 끊김 287
  - 호스트의 네트워크 이중화 손실에 대한 경보 288
  - 분산 포트 그룹의 업링크 페일오버 순서를 변경한 후에 가상 시스템의 연결 끊김 289

- 물리적 어댑터를 vSphere Distributed Switch에 추가할 수 없음 290
- SR-IOV 지원 워크로드 문제 해결 291
  - 해당 MAC 주소를 변경한 후 SR-IOV 지원 워크로드가 통신할 수 없음 291
- 호스트의 인터럽트 벡터 부족으로 SR-IOV 가상 기능을 사용하는 가상 시스템의 전원이 켜지지 않음 292
- VPN 클라이언트를 실행하는 가상 시스템으로 인해 호스트 또는 vSphere HA 클러스터에서 가상 시스템에 대한 서비스 거부가 발생함 293
- Windows 가상 시스템에서 UDP 워크로드에 대한 처리량이 낮음 295
- 동일한 분산 포트 그룹에 속하지만 서로 다른 호스트에 위치한 가상 시스템은 서로 통신할 수 없음 297
- 연결된 프로토콜 프로파일이 없어서 마이그레이션된 vApp 전원 켜기가 실패함 297
- 네트워킹 구성 작업이 롤백되고 vCenter Server에서 호스트 연결이 끊김 299

# vSphere 네트워킹 정보

"vSphere 네트워킹"에서는 vSphere Distributed Switch 및 vSphere 표준 스위치를 생성하는 방법을 비롯하여 VMware vSphere®의 네트워킹 구성에 대한 정보를 제공합니다.

"vSphere 네트워킹"에서는 네트워크 모니터링, 네트워크 리소스 관리 및 네트워킹 모범 사례에 대한 정보도 제공합니다.

VMware는 포용성을 중요하게 생각합니다. 고객, 파트너 및 내부 커뮤니티 안에서 이러한 원칙을 강화하기 위해 포용성 있는 언어를 사용하여 콘텐츠를 만듭니다.

## 대상 사용자

여기에 제공된 정보는 네트워크 구성과 가상 시스템 기술에 익숙한 숙련된 Windows 또는 Linux 시스템 관리자를 대상으로 작성되었습니다.

# vSphere 네트워킹 소개

# 1

vSphere 네트워킹의 기본 개념을 알아보고 vSphere 환경에서 네트워크를 설정하고 구성하는 방법을 알아보십시오.

## 네트워킹 개념

가상 네트워킹을 완전하게 이해하기 위해서는 몇 가지 기본적인 개념을 알고 있어야 합니다. vSphere가 생소한 경우에는 다음과 같은 개념을 숙지하면 도움이 됩니다.

네트워킹 개념	설명
물리적 네트워크	서로 데이터를 주고받을 수 있도록 연결되어 있는 물리적 시스템의 네트워크입니다. VMware ESXi는 물리적 시스템에서 실행됩니다.
가상 네트워크	하나의 물리적 시스템에서 실행되며 서로 데이터를 주고받을 수 있도록 논리적으로 상호 연결된 가상 시스템의 네트워크입니다. 가상 시스템은 사용자가 네트워크를 추가할 때 생성하는 가상 네트워크에 연결될 수 있습니다.
불투명 네트워크	불투명 네트워크는 vSphere 외부에 있는 별도의 엔티티를 통해 생성되고 관리되는 네트워크입니다. 예를 들어 VMware NSX <sup>®</sup> 를 통해 생성되고 관리되는 논리적 네트워크는 vCenter Server에서 nsx.LogicalSwitch 유형의 불투명 네트워크로 표시됩니다. VM 네트워크 어댑터에 대한 백업으로 불투명 네트워크를 선택합니다. 불투명 네트워크를 관리하려면 VMware NSX <sup>®</sup> Manager <sup>™</sup> 또는 VMware NSX <sup>®</sup> API 관리 도구와 같은 불투명 네트워크와 연결된 관리 도구를 사용합니다.  <b>참고</b> VMware NSX <sup>®</sup> 3.0을 사용하면 vDS(vSphere Distributed Switch) 버전 7.0 이상에서 NSX를 직접 실행할 수 있습니다. 이러한 네트워크는 불투명하지 않으며, vDS 7.0에서 실행되는 NSX 논리적 세그먼트로 식별됩니다. 자세한 내용은 기술 자료 문서 <a href="#">KB #79872</a> 를 참조하십시오.
물리적 이더넷 스위치	물리적 이더넷 스위치는 물리적 네트워크의 시스템 간 네트워크 트래픽을 관리합니다. 스위치에는 포트가 여러 개 있으며 각 포트는 하나의 시스템 또는 네트워크의 다른 스위치에 연결될 수 있습니다. 각 포트는 해당 포트에 연결된 시스템의 필요에 따라 특정 방식으로 작동하도록 구성할 수 있습니다. 스위치는 어느 포트에 어느 호스트가 연결되었는지 확인한 후 이 정보를 사용하여 올바른 물리적 시스템에 트래픽을 전달합니다. 스위치는 물리적 네트워크의 핵심입니다. 스위치를 여러 개 연결하여 큰 규모의 네트워크를 구성할 수 있습니다.

네트워킹 개념	설명
vSphere 표준 스위치	물리적 이더넷 스위치와 작동 방식이 유사합니다. vSphere 표준 스위치는 각 가상 포트에 어떤 가상 시스템이 논리적으로 연결되었는지 확인한 후 이 정보를 사용하여 올바른 가상 시스템에 트래픽을 전송합니다. vSphere 표준 스위치는 업링크 어댑터라고도 하는 물리적 이더넷 어댑터를 사용하여 물리적 스위치에 연결될 수 있으며, 이를 통해 가상 네트워크를 물리적 네트워크와 조인하는 것이 가능합니다. 이 연결 유형은 물리적 스위치를 서로 연결하여 큰 규모의 네트워크를 생성하는 것과 유사합니다. vSphere 표준 스위치는 물리적 스위치와 작동 방식이 유사하지만 물리적 스위치의 고급 기능 중 일부가 없습니다.
vSphere Distributed Switch	vSphere Distributed Switch는 데이터 센터에서 연결된 모든 호스트에 대해 단일 스위치처럼 작동하여 가상 네트워크의 중앙 집중식 프로비저닝, 관리 및 모니터링 기능을 제공합니다. vCenter Server 시스템에 vSphere Distributed Switch를 구성하면 해당 구성이 스위치와 연결된 모든 호스트에 전파됩니다. 이를 통해 가상 시스템은 여러 호스트 간에 마이그레이션될 때 일관된 네트워크 구성을 유지할 수 있습니다.
호스트 프록시 스위치	vSphere Distributed Switch와 연결된 모든 호스트에 있는 숨겨진 표준 스위치입니다. 호스트 프록시 스위치는 vSphere Distributed Switch에 설정된 네트워킹 구성을 특정 호스트에 복제합니다.
표준 포트 그룹	네트워크 서비스는 이러한 포트 그룹을 통해 표준 스위치에 연결합니다. 또한 포트 그룹은 스위치를 통해 네트워크에 연결하는 방법을 정의합니다. 일반적으로 하나의 표준 스위치가 포트 그룹 하나 이상과 연결됩니다. 포트 그룹은 각 멤버 포트에 대해 대역폭 제한 및 VLAN 태깅 정책과 같은 포트 구성 옵션을 지정합니다.
분산 포트	호스트의 VMkernel 또는 가상 시스템의 네트워크 어댑터에 연결되는 vSphere Distributed Switch의 포트입니다.
분산 포트 그룹	vSphere Distributed Switch에 연결된 포트 그룹으로, 각 멤버 포트에 대한 포트 구성 옵션을 지정합니다. 분산 포트 그룹은 vSphere Distributed Switch를 통해 네트워크에 연결하는 방법을 정의합니다.
NSX 분산 포트 그룹	vSphere Distributed Switch에 연결된 포트 그룹으로, 각 멤버 포트에 대한 포트 구성 옵션을 지정합니다. vSphere 분산 포트 그룹과 NSX 포트 그룹을 구분하기 위해 vSphere Client에서 NSX 가상 Distributed Switch와 연결된 포트 그룹은  아이콘으로 식별됩니다. NSX는 vCenter Server에서 불투명 네트워크로 나타나고 vCenter Server에서 NSX 설정을 구성할 수 없습니다. 표시된 NSX 설정은 읽기 전용입니다. NSX 분산 포트 그룹은 VMware NSX <sup>®</sup> Manager 또는 VMware NSX API 관리 도구를 사용하여 구성합니다. NSX 구성에 대해 알아보려면 "NSX Data Center for vSphere" 설명서를 참조하십시오.

네트워킹 개념	설명
NSX Manager 장치 플러그인	NSX Manager 장치는 vSphere Web Client에서 설치할 수 있습니다. NSX Manager UI에서 설치 작업을 수행할 필요가 없습니다. NSX Manager가 설치된 후 NSX는 가상 네트워킹 또는 보안 사용 사례를 위해 VMware NSX를 설치할 준비가 완료된 플러그인으로 vCenter Server에 나타납니다. 자세한 내용은 "VMware NSX" 설명서를 참조하십시오. 이 기능은 VMware vSphere 7.0 업데이트 3 이상 및 VMware NSX® 3.2 이상에서 사용할 수 있습니다.
NIC 팀 구성	NIC 팀 구성은 여러 개의 업링크 어댑터가 스위치 하나에 연결되어 팀을 구성할 때 발생합니다. 팀은 물리적 네트워크와 가상 네트워크 간의 트래픽 로드를 전체 또는 일부 멤버가 공유하거나, 하드웨어 장애 또는 네트워크 운영 중단이 발생하면 수동 페일오버를 제공할 수 있습니다.
VLAN	VLAN은 하나의 물리적 LAN 세그먼트를 더 세분화하여 포트 그룹이 물리적으로 다른 세그먼트에 있는 것처럼 서로 분리시킵니다. 표준 값은 802.1Q입니다.
VMkernel TCP/IP 네트워킹 계층	VMkernel 네트워킹 계층은 호스트에 대한 연결을 제공하고 vSphere vMotion, IP 스토리지, Fault Tolerance 및 vSAN의 표준 인프라 트래픽을 처리합니다.
IP 스토리지	TCP/IP 네트워크 통신을 기반으로 사용하는 모든 스토리지. iSCSI 및 NFS는 가상 시스템 데이터스토어로 사용하거나 CD-ROM으로 가상 시스템에 제공되는 .ISO 파일의 직접 마운트 대상으로 사용할 수 있습니다.
TCP 세분화 오프로드	TCP 세분화 오프로드(TSO)를 통해 TCP/IP 스택은 인터페이스의 MTU(Maximum Transmission Unit)보다 더 큰 프레임(최대 64 KB)을 보낼 수 있습니다. 그러면 네트워크 어댑터가 큰 프레임을 MTU 크기의 프레임으로 분할하고 원래 TCP/IP 헤더의 조정된 복사본을 앞부분에 추가합니다.

## 네트워크 서비스

가상 네트워크는 호스트와 가상 시스템에 여러 가지 서비스를 제공합니다. ESXi에서는 다음과 같이 두 가지 유형의 네트워크 서비스를 사용할 수 있습니다.

- 가상 시스템을 물리적 네트워크 및 가상 시스템 간에 연결합니다.
- VMkernel 서비스(예: NFS, iSCSI 또는 vMotion)를 물리적 네트워크에 연결합니다.

## VMware ESXi Dump Collector 지원

ESXi Dump Collector는 시스템에서 심각한 오류가 발생할 때 VMkernel 메모리의 상태, 즉 코어 덤프를 네트워크 서버로 보냅니다. ESXi의 ESXi Dump Collector는 vSphere Standard Switch와 Distributed Switch를 모두 지원합니다. 또한 ESXi Dump Collector는 Collector의 VMkernel 어댑터를 처리하는 포트 그룹의 팀에서 활성 업링크 어댑터를 사용할 수 있습니다.

구성된 VMkernel 어댑터의 IP 주소가 변경되는 경우 ESXi Dump Collector 인터페이스의 IP 주소 변경 사항이 자동으로 업데이트됩니다. 또한 ESXi Dump Collector는 VMkernel 어댑터의 게이트웨이 구성이 변경되는 경우 Collector의 기본 게이트웨이를 조정합니다.

ESXi Dump Collector에서 사용하는 VMkernel 네트워크 어댑터를 삭제하려고 하면 작업이 실패하고 주의 메시지가 나타납니다. VMkernel 네트워크 어댑터를 삭제하려면 덤프 수집을 비활성화하고 어댑터를 삭제합니다.

충돌이 발생한 호스트에서 ESXi Dump Collector로 이동하는 파일 전송 세션에는 인증이나 암호화가 없습니다. 가능하면 ESXi Dump Collector를 별도의 VLAN에 구성하여 일반 네트워크 트래픽에서 ESXi 코어 덤프를 분리합니다.

ESXi Dump Collector를 설치 및 구성하는 방법에 대한 자세한 내용은 "vCenter Server 설치 및 설정" 설명서를 참조하십시오.



# vSphere 표준 스위치를 사용하여 네트워크를 설정하는 방법

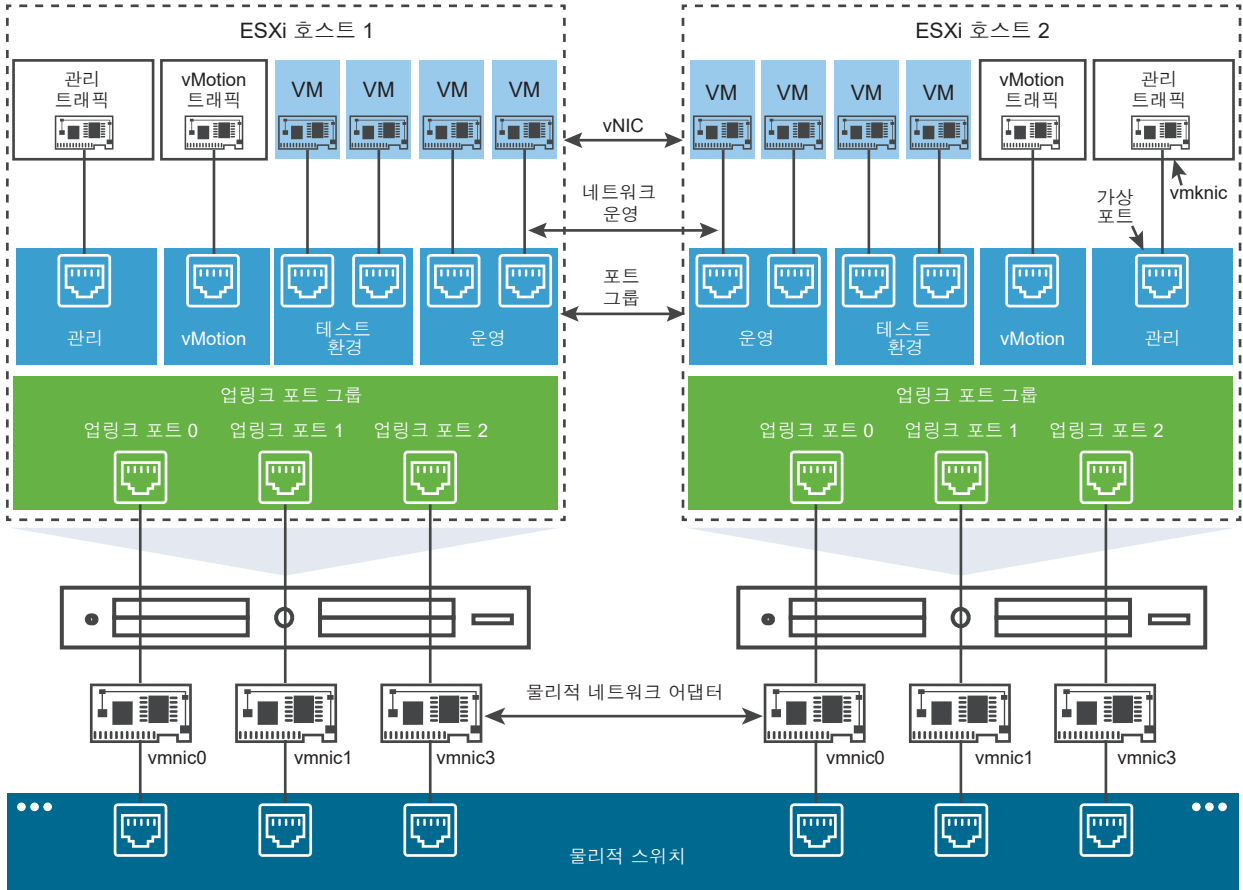
# 2

vSphere 표준 스위치는 vSphere 배포의 호스트 수준에서 네트워크 트래픽을 처리합니다. vSphere 표준 스위치라는 추상화된 네트워크 디바이스를 생성할 수 있습니다. 표준 스위치를 사용하여 호스트 및 가상 시스템에 네트워크 연결 기능을 제공하는 방법을 알아봅니다. 표준 스위치는 동일한 VLAN에 있는 가상 시스템 간의 트래픽을 내부적으로 브리지하고 외부 네트워크에 연결할 수 있습니다.

## 표준 스위치 개요

호스트 및 가상 시스템에 네트워크 연결 기능을 제공하려면 호스트의 물리적 NIC를 표준 스위치의 업링크 포트에 연결합니다. 가상 시스템에는 표준 스위치의 포트 그룹에 연결하는 네트워크 어댑터(vNIC)가 있습니다. 모든 포트 그룹은 하나 이상의 물리적 NIC를 사용하여 해당 네트워크 트래픽을 처리할 수 있습니다. 포트 그룹에 물리적 NIC가 연결되어 있지 않은 경우 동일한 포트 그룹의 가상 시스템은 서로 간에만 통신할 수 있고 외부 네트워크와는 통신할 수 없습니다.

그림 2-1. vSphere 표준 스위치 아키텍처



vSphere 표준 스위치는 물리적 이더넷 스위치와 매우 유사합니다. 호스트의 가상 시스템 네트워크 어댑터 및 NIC는 스위치의 논리적 포트를 각각 하나씩 사용합니다. 표준 스위치의 각 논리적 포트는 단일 포트 그룹의 멤버입니다. 최대 허용되는 포트 및 포트 그룹에 대한 자세한 내용은 "구성 최대값" 설명서를 참조하십시오.

## 표준 포트 그룹

표준 스위치의 각 포트 그룹은 현재 호스트에서 고유해야 하는 네트워크 레이블로 식별됩니다. 네트워크 레이블을 사용하면 가상 시스템의 네트워킹 구성을 호스트 간에 쉽게 이동할 수 있습니다. 데이터 센터에서 물리적 네트워크의 한 브로드캐스트 도메인에 연결된 물리적 NIC를 사용하는 포트 그룹에는 동일한 레이블을 지정해야 합니다. 이와 반대로 두 개의 포트 그룹이 서로 다른 브로드캐스트 도메인의 물리적 NIC에 연결되어 있는 경우에는 각 포트 그룹에 별개의 레이블이 있어야 합니다.

예를 들어 물리적 네트워크의 동일한 브로드캐스트 도메인을 공유하는 호스트에 가상 시스템 네트워크로 *프로덕션* 및 *테스트 환경* 포트 그룹을 생성할 수 있습니다.

VLAN ID는 선택적이며 물리적 네트워크 내의 논리적 이더넷 세그먼트로 포트 그룹 트래픽을 제한합니다. 포트 그룹이 동일한 호스트에 표시되지만 둘 이상의 VLAN에서 들어오는 트래픽을 수신하려면 VLAN ID가 VGT(VLAN 4095)로 설정되어야 합니다.

## 표준 포트 수

ESXi 호스트에서는 호스트 리소스를 효율적으로 사용할 수 있도록 표준 스위치의 포트 수가 동적으로 증가하거나 감소합니다. 이러한 호스트의 표준 스위치는 호스트에서 지원되는 최대 포트 수까지 확장할 수 있습니다.

다음으로 아래 항목을 읽으십시오.

- vSphere 표준 스위치 생성
- 가상 시스템의 포트 그룹 구성
- vSphere 표준 스위치 속성

## vSphere 표준 스위치 생성

vSphere 표준 스위치를 생성하여 호스트, 가상 시스템에 대한 네트워크 연결을 제공하고 VMkernel 트래픽을 처리할 수 있습니다. 생성하려는 연결 유형에 따라 VMkernel 어댑터를 포함하는 새 vSphere 표준 스위치를 생성하거나 물리적 네트워크 어댑터를 새 스위치에 연결만 하거나 가상 시스템 포트 그룹을 포함하는 스위치를 생성할 수 있습니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **네트워킹**을 확장하고 **가상 스위치**를 선택합니다.
- 3 **네트워킹 추가**를 클릭합니다.
- 4 새 표준 스위치를 사용하려는 연결 유형을 선택하고 **다음**을 클릭합니다.

옵션	설명
VMkernel 네트워크 어댑터	새 VMkernel 어댑터를 생성하여 호스트 관리 트래픽, vMotion, 네트워크 스토리지, Fault Tolerance 또는 vSAN 트래픽을 처리합니다.
물리적 네트워크 어댑터	물리적 네트워크 어댑터를 기존 또는 새 표준 스위치에 추가합니다.
표준 스위치용 가상 시스템 포트 그룹	가상 시스템 네트워킹에 사용할 새 포트 그룹을 생성합니다.

- 5 새 **표준 스위치**를 선택하고 **다음**을 클릭합니다.
- 6 물리적 네트워크 어댑터를 새 표준 스위치에 추가합니다.
  - a 할당된 어댑터에서 **어댑터 추가**를 클릭합니다.
  - b 목록에서 하나 이상의 물리적 네트워크 어댑터를 선택하고 **확인**을 클릭합니다.  
더 높은 처리량 및 이중화를 제공하려면 활성 목록에서 최소 두 개의 물리적 네트워크 어댑터를 구성합니다.
  - c (선택 사항) **할당된 어댑터** 목록에서 **위로 이동** 및 **아래로 이동** 화살표를 사용하여 어댑터의 위치를 변경합니다.
  - d **다음**을 클릭합니다.

- 7 VMkernel 어댑터 또는 가상 시스템 포트 그룹을 포함하는 새 표준 스위치를 생성하는 경우 어댑터 또는 포트 그룹에 대한 연결 설정을 입력합니다.

옵션	설명
VMkernel 어댑터	<ul style="list-style-type: none"> <li>a VMkernel 어댑터의 트래픽 유형을 나타내는 레이블을 입력합니다(예: <b>vMotion</b>).</li> <li>b VMkernel 어댑터의 네트워크 트래픽이 사용할 VLAN을 식별하도록 VLAN ID를 설정합니다.</li> <li>c IPv4, IPv6 또는 둘 다 선택합니다.</li> <li>d 드롭다운 메뉴에서 옵션을 선택하여 MTU 크기를 설정합니다. [사용자 지정]을 선택한 경우, MTU 크기 값을 입력합니다. MTU를 1500보다 큰 값으로 설정하여 점보 프레임을 사용하도록 설정할 수 있습니다. MTU 크기를 9,000바이트보다 큰 값으로 설정할 수 없습니다.</li> <li>e TCP/IP 스택을 선택합니다. VMkernel 어댑터에 대한 TCP/IP 스택을 설정하고 나면 나중에 변경할 수 없습니다. vMotion이나 프로비저닝 TCP/IP 스택을 선택하는 경우 이 스택만 사용하여 호스트의 vMotion 또는 프로비저닝 스택을 처리할 수 있습니다.</li> <li>f 기본 TCP/IP 스택을 사용하는 경우 사용 가능한 서비스에서 선택합니다.</li> <li>g IPv4 및 IPv6 설정을 구성합니다.</li> </ul>
가상 시스템 포트 그룹	<ul style="list-style-type: none"> <li>a 네트워크 레이블 또는 포트 그룹을 입력하거나 생성된 레이블을 수락합니다.</li> <li>b VLAN ID를 설정하여 포트 그룹에서의 VLAN 처리를 구성합니다.</li> </ul>

- 8 [완료 준비] 페이지에서 **마침**을 클릭합니다.

#### 다음에 수행할 작업

- 새 표준 스위치의 팀 구성 및 페일오버 정책을 변경해야 할 수도 있습니다. 예를 들어 호스트가 물리적 스위치의 Etherchannel에 연결된 경우 IP 해시 기준 라우팅을 사용하는 vSphere 표준 스위치를 로드 밸런싱 알고리즘으로 구성해야 합니다. 자세한 내용은 [팀 구성 및 페일오버 정책이란?](#)의 내용을 참조하십시오.
- 가상 시스템 네트워킹에 사용할 포트 그룹을 포함하는 새 표준 스위치를 생성하는 경우 가상 시스템을 포트 그룹에 연결합니다.

## 가상 시스템의 포트 그룹 구성

가상 시스템 포트 그룹을 추가하거나 수정하여 가상 시스템 집합에 대한 트래픽 관리를 설정하는 방법을 알아봅니다.

vSphere Client의 **네트워킹 추가** 마법사는 가상 시스템을 연결할 수 있는 가상 네트워크의 생성 프로세스를 안내하며, 여기에는 vSphere 표준 스위치를 생성하고 네트워크 레이블의 설정을 구성하는 작업이 포함됩니다.

가상 시스템 네트워크를 설정할 때는 네트워크의 가상 시스템을 호스트 간에 마이그레이션할지 고려해야 합니다. 그렇다면 두 호스트에서 동일한 브로드캐스트 도메인 즉, 동일한 계층 2 서브넷에 액세스할 수 있는지 확인합니다.

ESXi에서는 서로 다른 브로드캐스트 도메인에 있는 호스트 간의 가상 시스템 마이그레이션을 지원하지 않는데, 그 이유는 마이그레이션한 가상 시스템에서 새 네트워크에서는 더 이상 액세스할 수 없는 시스템 및 리소스를 필요로 할 수 있기 때문입니다. 네트워크 구성이고가용성 환경으로 설정되거나, 서로 다른 네트워크 간에 가상 시스템의 필요 사항을 해결하는 지능형 스위치를 포함하고 있더라도 ARP(주소 분석 프로토콜) 테이블을 업데이트하고 가상 시스템에서 사용하는 네트워크 트래픽을 재개하는 동안 시간이 지연될 수 있습니다.

가상 시스템은 업링크 어댑터를 통해 물리적 네트워크에 연결됩니다. vSphere 표준 스위치는 하나 이상의 네트워크 어댑터가 연결되어 있는 경우에만 외부 네트워크로 데이터를 전송할 수 있습니다. 둘 이상의 어댑터가 단일 표준 스위치에 연결되어 있는 경우 어댑터들은 투명하게 팀을 구성하게 됩니다.

## 가상 시스템 포트 그룹 추가

vSphere 표준 스위치에서 VM 포트 그룹을 추가하여 가상 시스템에 적합한 연결 및 공통 네트워크 구성을 제공하는 방법을 알아봅니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 호스트를 마우스 오른쪽 버튼으로 클릭하고 **네트워킹 추가**를 선택합니다.
- 3 **연결 유형 선택**에서 **표준 스위치용 가상 시스템 포트 그룹**을 선택하고 **다음**을 클릭합니다.
- 4 **대상 디바이스 선택**에서 기존 표준 스위치를 선택하거나 새 표준 스위치를 생성합니다.
- 5 새 포트 그룹이 기존 표준 스위치의 포트 그룹이면 해당 스위치로 이동합니다.
  - a **찾아보기**를 클릭합니다.
  - b 목록에서 표준 스위치를 선택하고 **확인**을 클릭합니다.
  - c **다음**을 클릭하고 **단계 7단계**로 이동합니다.
- 6 (선택 사항) 새 표준 스위치를 생성하도록 선택하는 경우 MTU 크기에 대한 값을 입력하고 **다음**을 클릭합니다. 어댑터 사용 여부와 관계없이 표준 스위치를 생성할 수 있습니다.

물리적 네트워크 어댑터 없이 표준 스위치를 생성하면 스위치의 모든 트래픽이 해당 스위치에 국한됩니다. 이 경우 물리적 네트워크의 다른 호스트 또는 다른 표준 스위치의 가상 시스템이 이 표준 스위치를 통해 트래픽을 보내거나 받을 수 없습니다. 특정 그룹에 속한 가상 시스템이 서로 통신할 수 있지만 그룹 외부의 다른 가상 시스템이나 호스트와는 통신하지 못하도록 할 경우에 물리적 네트워크 어댑터 없이 표준 스위치를 생성할 수 있습니다.

- a **어댑터 추가**를 클릭합니다.
- b **네트워크 어댑터** 목록에서 어댑터를 선택하고 **확인**을 클릭합니다.
- c (선택 사항) 필요한 경우 **할당된 어댑터** 목록에서 위쪽 및 아래쪽 화살표를 사용하여 어댑터의 위치를 변경합니다.
- d **다음**을 클릭합니다.

- 7 [연결 설정] 페이지에서 그룹의 포트를 통해 트래픽을 식별합니다.
  - a 포트 그룹의 **네트워크 레이블**을 입력하거나 생성된 레이블을 수락합니다.

**참고** 포트 그룹 이름에는 콜론 문자(:)를 포함할 수 없습니다.

- b **VLAN ID**를 설정하여 포트 그룹에서의 VLAN 처리를 구성합니다.

VLAN ID는 또한 포트 그룹의 VLAN 태깅 모드를 반영합니다.

VLAN 태그 지정 모드	VLAN ID	설명
EST(External Switch Tagging)	0	가상 스위치는 VLAN과 연결된 트래픽을 전달하지 않습니다.
VGT(Virtual Guest Tagging)	4095	가상 시스템은 VLAN을 처리합니다. 가상 스위치는 모든 VLAN의 트래픽을 전달합니다.

- c 다음을 클릭합니다.
- 8 완료 준비 페이지에서 포트 그룹 설정을 검토하고 **마침**을 클릭합니다.  
설정을 변경하려면 **뒤로**를 클릭합니다.

## 표준 스위치 포트 그룹 편집

표준 스위치 포트 그룹의 이름과 VLAN ID를 편집하고 포트 그룹 수준에서 네트워킹 정책을 재정의하는 방법을 알아봅니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **네트워킹**을 확장하고 **가상 스위치**를 선택합니다.
- 3 목록에서 표준 스위치를 선택합니다.  
스위치의 토폴로지 다이어그램이 표시됩니다.
- 4 스위치의 토폴로지 다이어그램에서 포트 그룹 이름을 클릭합니다.
- 5 토폴로지 다이어그램 제목 옆에 있는 가로 줄임표 아이콘을 클릭하고 **설정 편집**을 선택합니다.
- 6 [속성] 페이지에서 **네트워크 레이블** 텍스트 필드에 있는 포트 그룹 이름을 변경합니다.
- 7 **VLAN ID** 드롭다운 메뉴에서 VLAN 태깅을 구성합니다.

VLAN 태그 지정 모드	VLAN ID	설명
EST(External Switch Tagging)	0	가상 스위치는 VLAN과 연결된 트래픽을 전달하지 않습니다.
VGT(Virtual Guest Tagging)	4095	가상 시스템은 VLAN을 처리합니다. 가상 스위치는 모든 VLAN의 트래픽을 전달합니다.

- 8 [보안] 페이지에서 MAC 주소 변경 및 위조 전송으로부터 보호하고 가상 시스템을 비규칙(Promiscuous) 모드로 실행하도록 스위치 설정을 재정의합니다.

9 [트래픽 조절] 페이지에서는 평균 대역폭, 최대 대역폭 및 버스트 크기를 포트 그룹 수준에서 재정의합니다.

10 [팀 구성 및 페일오버] 페이지에서는 표준 스위치에서 상속된 팀 구성 및 페일오버 설정을 재정의합니다.

포트 그룹과 연결된 물리적 어댑터 간의 트래픽 분산 및 재라우팅을 구성할 수 있습니다. 또한 장애 시 호스트의 물리적 어댑터 사용 순서를 변경할 수 있습니다.

11 **확인**을 클릭합니다.

## vSphere 표준 스위치에서 포트 그룹 제거

연결된 레이블 지정 네트워크가 더 이상 필요하지 않은 경우 vSphere 표준 스위치에서 포트 그룹을 제거하는 방법을 알아봅니다.

### 사전 요구 사항

제거할 포트 그룹에 전원이 켜진 가상 시스템이 연결되어 있지 않은지 확인합니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 **구성** 탭에서 **네트워킹**을 확장하고 **가상 스위치**를 선택합니다.
- 3 표준 스위치를 선택합니다.
- 4 스위치의 토폴로지 다이어그램에서 해당 레이블을 클릭하여 제거할 포트 그룹을 선택합니다.
- 5 스위치 토폴로지의 도구 모음에서 **제거** 작업 아이콘을 클릭합니다.

## vSphere 표준 스위치 속성

vSphere 표준 스위치 설정은 포트에 대한 스위치 수준의 기본값을 제어하며, 각 표준 스위치의 포트 그룹 설정에 의해 재정의될 수 있습니다. 업링크 구성 및 사용 가능한 포트 수 등의 표준 스위치 속성을 편집하는 방법을 알아봅니다.

### ESXi 호스트에 있는 포트의 수

ESXi 호스트에서는 호스트 리소스를 효율적으로 사용할 수 있도록 가상 스위치의 포트가 동적으로 증가하거나 감소합니다. 이러한 호스트의 스위치는 호스트에서 지원되는 최대 포트 수까지 확장할 수 있습니다. 포트 수 제한은 호스트에서 처리할 수 있는 최대 가상 시스템 수에 따라 달라집니다.

### vSphere 표준 스위치의 MTU 크기 변경

단일 패킷으로 전송되는 페이로드 데이터의 양을 늘려 네트워킹 효율성을 향상함으로써 점보 프레임 사용할 수 있도록 설정하기 위해 vSphere Standard Switch의 MTU(최대 전송 단위) 크기를 변경하는 방법을 알아봅니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 **구성** 탭에서 **네트워킹**을 확장하고 **가상 스위치**를 선택합니다.

3 표에서 표준 스위치를 선택하고 **설정 편집**을 클릭합니다.

4 표준 스위치의 **MTU(바이트)** 값을 변경합니다.

MTU를 1500보다 큰 값으로 설정하여 점보 프레임을 사용하도록 설정할 수 있습니다. MTU 크기를 9,000 바이트보다 큰 값으로 설정할 수 없습니다.

5 **확인**을 클릭합니다.

## 물리적 어댑터의 속도 변경

트래픽 속도 규정을 준수하도록 데이터를 전송하기 위해 물리적 어댑터의 연결 속도 및 이중 설정을 변경하는 방법을 알아봅니다.

물리적 어댑터가 SR-IOV를 지원하는 경우 이 어댑터를 사용하도록 설정하고 가상 시스템 네트워킹에 사용할 가상 기능의 수를 구성할 수 있습니다.

### 절차

1 vSphere Client에서 호스트로 이동합니다.

2 **구성** 탭에서 **네트워킹**을 확장하고 **물리적 어댑터**를 선택합니다.

각 물리적 네트워크 어댑터에 대한 세부 정보가 포함된 표에 호스트의 물리적 네트워크 어댑터가 나타납니다.

3 목록에서 물리적 네트워크 어댑터를 선택하고 **어댑터 설정 편집** 아이콘을 클릭합니다.

4 드롭다운 메뉴에서 물리적 네트워크 어댑터의 속도와 이중 모드를 선택합니다.

선택하는 속도 및 이중 설정은 물리적 스위치에 구성된 속도 및 설정과 일치해야 합니다. 속도는 보통 초당 메가비트(Mbps)로 나열된 인터페이스 속도입니다. 이중(duplex)은 인터페이스에서 데이터가 흐르는 방식을 나타냅니다.

5 **확인**을 클릭합니다.

## vSphere Standard 스위치에 물리적 어댑터 할당

표준 스위치에 물리적 어댑터를 할당하여 호스트의 가상 시스템과 VMkernel 어댑터에 대한 연결을 제공하는 방법을 알아봅니다. NIC 팀을 구성하여 트래픽 로드를 분산하고 페일오버를 구성할 수 있습니다.

NIC 팀 구성을 사용하면 여러 네트워크 연결이 결합되어 처리량이 증가하고, 연결에 실패할 경우 이중화 기능이 제공됩니다. 팀을 생성하려면 여러 물리적 어댑터를 단일 vSphere 표준 스위치에 연결합니다.

### 절차

1 vSphere Client에서 호스트로 이동합니다.

2 **구성** 탭에서 **네트워킹**을 확장하고 **가상 스위치**를 선택합니다.

3 물리적 어댑터에 추가할 표준 스위치를 선택합니다.

4 **물리적 어댑터 관리**를 클릭합니다.



- 5 스위치에 하나 이상의 사용 가능한 물리적 네트워크 어댑터를 추가합니다.
  - a **어댑터 추가**의 목록에서 네트워크 어댑터를 하나 이상 선택하고 **확인**을 클릭합니다.  
선택한 어댑터가 할당된 어댑터 목록 아래의 페일오버 그룹 목록에 나타납니다.
  - b (선택 사항) 페일오버 그룹에서 어댑터의 위치를 변경하려면 위쪽 및 아래쪽 화살표를 사용합니다.  
페일오버 그룹은 외부 네트워크를 통한 데이터 교환을 위한 어댑터 역할(활성, 대기 또는 사용되지 않음)을 결정합니다. 기본적으로 어댑터는 표준 스위치에 활성 상태로 추가됩니다.
- 6 **확인**을 클릭하여 물리적 어댑터 구성을 적용합니다.

## vSphere Standard 스위치의 토폴로지

토폴로지 다이어그램을 사용하여 vSphere Standard 스위치의 구조 및 구성 요소를 봅니다.

표준 스위치의 토폴로지 다이어그램에는 스위치에 연결된 어댑터 및 포트 그룹이 시각적으로 표현됩니다.

이 다이어그램에서 선택한 포트 그룹 및 선택한 어댑터의 설정을 편집할 수 있습니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 **구성** 탭에서 **네트워킹**을 확장하고 **가상 스위치**를 선택합니다.
- 3 목록에서 표준 스위치를 선택합니다.

### 결과

호스트의 가상 스위치 목록 아래에 다이어그램이 나타납니다.

### 예제: VMkernel 및 가상 시스템을 네트워크에 연결하는 표준 스위치의 다이어그램

가상 환경에서 vSphere 표준 스위치는 vSphere vMotion 및 관리 네트워크에 대한 VMkernel 어댑터와 가상 시스템 그룹을 처리합니다. 중앙 토폴로지 다이어그램을 사용하여 가상 시스템 또는 VMkernel 어댑터가 외부 네트워크에 연결되어 있는지 검사하고 데이터를 전송하는 물리적 어댑터를 식별할 수 있습니다.

그림 2-2. vSphere Standard Switch의 토폴로지 다이어그램

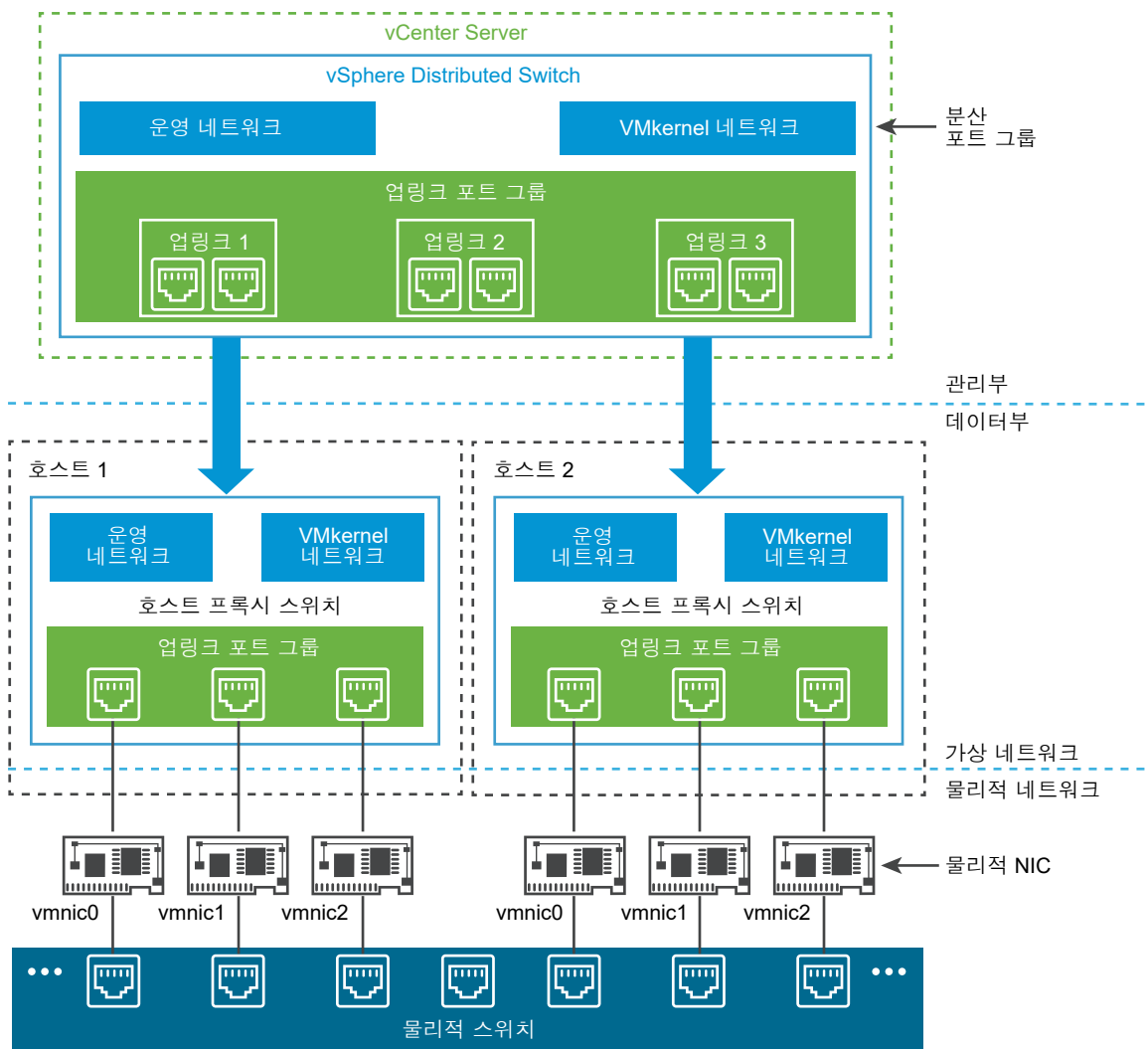


# vSphere Distributed Switch를 사용하여 네트워킹을 설정하는 방법

# 3

vSphere Distributed Switch를 사용하면 vSphere 환경에서 네트워킹을 설정하고 구성할 수 있습니다.

그림 3-1. vSphere Distributed Switch 아키텍처



vSphere의 네트워크 스위치는 데이터부 및 관리부가 있는 두 개의 논리 섹션으로 구성되어 있습니다. 데이터부는 패킷 스위칭, 필터링, 태그 지정 등을 구현합니다. 관리부는 데이터부 기능을 구성하기 위해 사용하는 제어 구조입니다. vSphere 표준 스위치에는 데이터부 및 관리부가 모두 포함되어 있으며 각 표준 스위치를 개별적으로 구성하고 유지 보수합니다.

vSphere Distributed Switch는 데이터부와 관리부를 구분합니다. Distributed Switch의 관리 기능은 데이터 센터 수준에서 환경의 네트워킹 구성을 관리할 수 있는 vCenter Server 시스템에 있습니다. 데이터부는 Distributed Switch와 연결된 모든 호스트에서 로컬로 유지됩니다. Distributed Switch의 데이터부 섹션은 호스트 프록시 스위치라고 합니다. vCenter Server(관리부)에서 생성하는 네트워킹 구성은 모든 호스트 프록시 스위치(데이터부)에 자동으로 푸시 다운됩니다.

vSphere Distributed Switch에는 물리적 NIC, 가상 시스템 및 VMkernel 서비스에 대해 일관된 네트워킹 구성을 생성하기 위해 사용하는 두 개의 추상화가 도입되었습니다.

### 업링크 포트 그룹

업링크 포트 그룹 또는 dvuplink 포트 그룹이 Distributed Switch를 생성하는 동안 정의되며 하나 이상의 업링크를 가질 수 있습니다. 업링크는 호스트의 물리적 연결뿐만 아니라 페일오버 및 로드 밸런싱 정책을 구성하기 위해 사용하는 템플릿입니다. 호스트의 물리적 NIC를 Distributed Switch의 업링크에 매핑합니다. 호스트 수준에서 각 물리적 NIC는 특정 ID를 사용하여 업링크 포트에 연결됩니다. 업링크에 대한 페일오버 및 로드 밸런싱 정책을 설정하면 정책이 호스트 프록시 스위치 또는 데이터부에 자동으로 전파됩니다. 이 방식으로 Distributed Switch와 연결된 모든 호스트의 물리적 NIC에 대해 일관된 페일오버 및 로드 밸런싱 구성을 적용할 수 있습니다.

### 분산 포트 그룹

분산 포트 그룹은 가상 시스템에 대한 네트워크 연결을 제공하고 VMkernel 트래픽을 수용합니다. 각 분산 포트 그룹은 네트워크 레이블을 사용하여 식별하며, 이 레이블은 현재 데이터 센터에서 고유해야 합니다. 분산 포트 그룹에서 NIC 팀 구성, 페일오버, 로드 밸런싱, VLAN, 보안, 트래픽 조절 및 기타 정책을 구성합니다. 분산 포트 그룹에 연결된 가상 포트는 분산 포트 그룹에 구성된 동일한 속성을 공유합니다. 업링크 포트 그룹과 마찬가지로 vCenter Server(관리부)의 분산 포트 그룹에 대해 설정하는 구성은 해당 호스트 프록시 스위치(데이터부)를 통해 Distributed Switch의 모든 호스트에 자동으로 전파됩니다. 이 방식으로 가상 시스템을 동일한 분산 포트 그룹에 연결하여 동일한 네트워킹 구성을 공유하도록 가상 시스템 그룹을 구성할 수 있습니다.

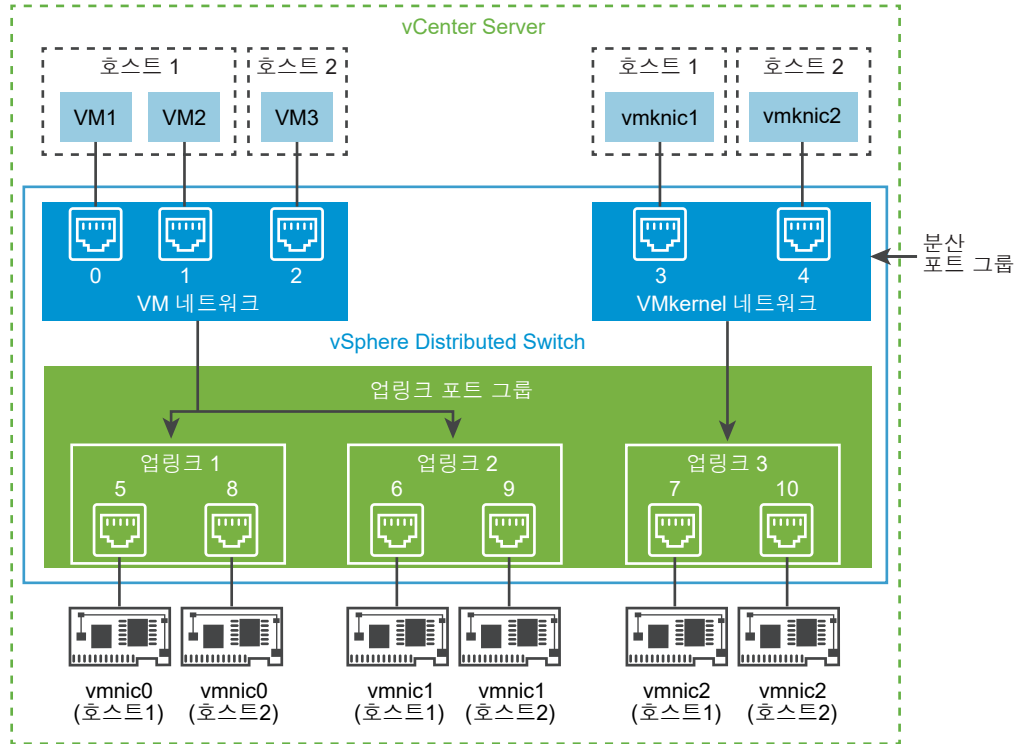
예를 들어 데이터 센터에서 vSphere Distributed Switch를 생성하고 여기에 두 개의 호스트를 연결한다고 가정합니다. 세 개의 업링크를 업링크 포트 그룹에 구성하고 각 호스트의 물리적 NIC를 업링크에 연결합니다. 각 업링크에는 매핑된 각 호스트에서 하나씩 2개의 물리적 NIC가 있습니다. 예를 들어 업링크 1은 호스트 1과 호스트 2의 vmnic0으로 구성됩니다. 다음으로 가상 시스템 네트워킹 및 VMkernel 서비스에 대한 운영 및 VMkernel 네트워크 분산 포트 그룹을 생성합니다. 또한 운영 및 VMkernel 네트워크 포트 그룹의 표현도 호스트 1 및 호스트 2에서 생성됩니다. 운영 및 VMkernel 네트워크 포트 그룹에 설정한 모든 정책이 호스트 1 및 호스트 2의 해당 표현으로 전파됩니다.

호스트 리소스를 효율적으로 사용할 수 있도록 프록시 스위치의 분산 포트 수가 동적으로 증가하거나 감소합니다. 이러한 호스트의 프록시 스위치는 호스트에서 지원되는 최대 포트 수까지 확장할 수 있습니다. 포트 수 제한은 호스트에서 처리할 수 있는 최대 가상 시스템 수에 따라 달라집니다.

## vSphere Distributed Switch 데이터 흐름

가상 시스템 및 VMkernel 어댑터에서 물리적 네트워크까지의 데이터 흐름은 분산 포트 그룹에 설정된 NIC 팀 구성과 로드 밸런싱에 따라 다릅니다. 또한 데이터 흐름은 Distributed Switch의 포트 할당에 따라 다릅니다.

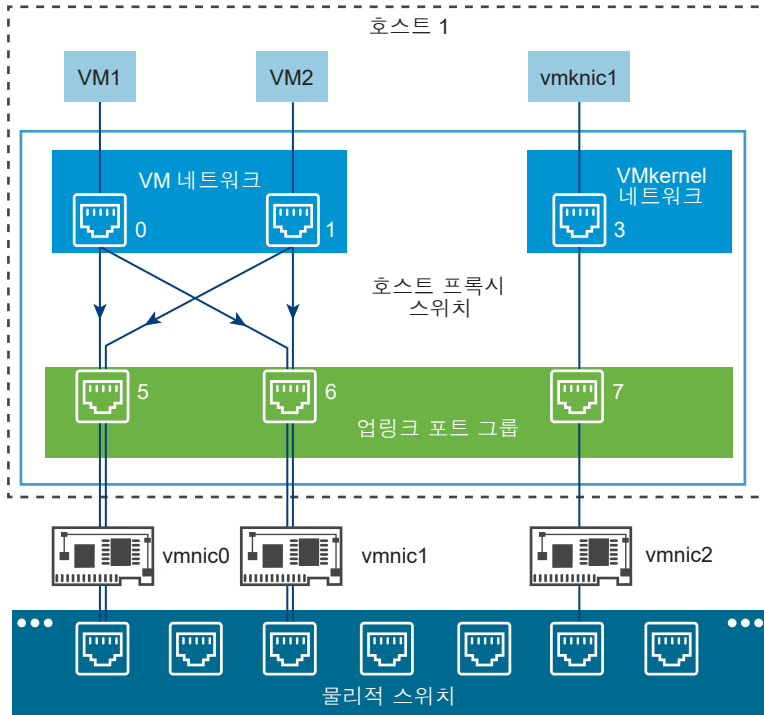
그림 3-2. vSphere Distributed Switch의 NIC 팀 구성 및 포트 할당



예를 들어 각각 3개 및 2개의 분산 포트를 가진 VM 네트워크 및 VMkernel 네트워크 분산 포트 그룹을 생성한다고 가정합니다. Distributed Switch는 분산 포트 그룹을 생성하는 순서대로 0에서 4까지의 ID를 포트에 할당합니다. 그 다음 호스트 1 및 호스트 2를 Distributed Switch와 연결합니다. Distributed Switch는 호스트의 모든 물리적 NIC에 포트를 할당하고, 이때 호스트를 추가하는 순서대로 5부터 포트 번호를 계속 지정합니다. 각 호스트에서 네트워크 연결을 제공하기 위해 vmnic0을 업링크 1에, vmnic1을 업링크 2에, vmnic2를 업링크 3에 매핑합니다.

가상 시스템에 대한 연결을 제공하고 VMkernel 트래픽을 수용하려면 VM 네트워크 및 VMkernel 네트워크 포트 그룹에 팀 구성 및 페일오버를 구성합니다. 업링크 1 및 업링크 2는 VM 네트워크 포트 그룹의 트래픽을 처리하고 업링크 3은 VMkernel 네트워크 포트 그룹의 트래픽을 처리합니다.

그림 3-3. 호스트 프록시 스위치에서의 패킷 흐름



호스트 측에서 가상 시스템 및 VMkernel 서비스의 패킷 흐름이 특정 포트를 통과해 물리적 네트워크에 도달합니다. 예를 들어 호스트 1의 VM1에서 보낸 패킷이 먼저 VM 네트워크 분산 포트 그룹의 포트 0에 도달합니다. 업링크 1 및 업링크 2가 VM 네트워크 포트 그룹의 트래픽을 처리하기 때문에 패킷은 업링크 포트 5 또는 업링크 포트 6에서 계속될 수 있습니다. 패킷이 업링크 포트 5를 통과하면 vmnic0으로 계속되고 패킷이 업링크 포트 6으로 이동하면 vmnic1로 계속됩니다.

다음으로 아래 항목을 읽으십시오.

- 네트워크 오프로드 호환성이란?
- vSphere Distributed Switch 생성
- 최신 버전으로 vSphere Distributed Switch 업그레이드
- 일반 및 고급 vSphere Distributed Switch 설정 편집
- vSphere Distributed Switch의 여러 호스트에서 네트워킹 관리
- 호스트 프록시 스위치의 네트워킹 관리
- 분산 포트 그룹
- 분산 포트 사용
- vSphere Distributed Switch에 가상 시스템 네트워킹 구성
- vSphere Distributed Switch 토폴로지

## 네트워크 오프로드 호환성이란?

vSphere 8.0부터 vDSE(vSphere Distributed Services Engine)는 호스트 또는 서버 CPU에서 DPU(데이터 처리 장치)로 인프라 기능을 오프로드할 수 있는 SmartNIC라고도 하는 DPU(데이터 처리 장치)를 추가하여 가상 인프라를 분산 아키텍처로 도입했습니다.

네트워크 오프로드 호환성을 통해 네트워킹 작업을 DPU 디바이스로 오프로드할 수 있습니다. 성능 향상을 위해 ESXi 호스트에서 DPU로 네트워킹 기능을 오프로드할 수 있습니다. DPU에서 ESXi가 지원하는 vSphere Distributed Switch는 다음 모드를 지원합니다.

- NSX가 사용되도록 설정되기 전 비오프로딩 모드: DPU가 기존 NIC로 사용됩니다.
- NSX가 사용되도록 설정된 후 오프로딩 모드: 트래픽 전달 논리가 ESXi 호스트에서 DPU가 지원하는 vSphere Distributed Switch로 오프로드됩니다.

DPU가 지원하는 호스트는 vSphere Distributed Switch와 연결되며 Distributed Switch를 생성하는 동안 구성됩니다. 호스트를 Distributed Switch에 연결한 후에는 네트워크 오프로드 호환성을 수정할 수 없습니다. 이러한 Distributed Switch에는 DPU가 지원하는 호스트만 추가할 수 있습니다. DPU의 ESXi는 VMware NSX® 전송 노드가 구성될 때까지 기존 NIC로 사용되었습니다. vCenter Server의 vSphere Distributed Switch는 VMware NSX®가 사용되도록 설정되면 네트워크 오프로딩이 허용되는지 여부를 표시합니다.

DPU가 지원하는 vSphere Distributed Switch는 다음과 같은 기능을 지원합니다.

- vSphere Distributed Switch의 생성 및 삭제.
- 구성 관리.
- vSphere Distributed Switch 상태 점검.
- LACP(Link Aggregation Control Protocol).
- 포트 미러링.
- 사설 LAN.
- 링크 계층 탐색 프로토콜.

---

**참고** 다음 기능은 DPU가 지원하는 vSphere Distributed Switch에서 지원되지 않습니다.

- Network I/O Control.
  - 트래픽 조절 정책.
  - DV 필터.
- 

## 이중 DPU

vSphere 8.0 업데이트 3부터는 고가용성 모드에서 2개의 DPU(데이터 처리 장치)와 함께 vDSE를 사용할 수 있습니다. 이중 DPU에 대한 자세한 내용은 [VMware vSphere® 분산 서비스 엔진™ 소개 및 DPU를 사용한 네트워킹 가속](#)을 참조하십시오.

이중 DPU는 HA(고가용성) 및 비HA(비고가용성) 모드에서 사용할 수 있습니다.

- HA 모드: 이 모드에서는 각 DPU가 오프로드된 단일 vDS(분산 가상 스위치)에 의해 사용됩니다. 예를 들어, DPU 1이 활성으로 지정되면 DPU 2는 대기 상태로 작동합니다. 대기 DPU는 백업 DPU로 지정됩니다. 활성 DPU에 장애가 발생하면 활성 네트워킹 오프로드가 대기 DPU로 전환됩니다. 이를 통해 DPU에 고가용성이 제공됩니다. 이 전환은 활성 워크로드의 장애 위험을 최소화합니다.

이중 DPU를 동일한 네트워크 스위치에 동시에 연결하면 그 중 하나만 데이터 패킷을 처리합니다. 다른 DPU는 대기 모드에 있습니다. 그러나 새도 스위치와 포트는 대기 DPU에 생성됩니다. 네트워킹 정책은 DPU에도 적용되지만 새도 스위치는 패킷을 처리하지 않습니다. ESXi는 활성 DPU 장애가 감지되면 대기 DPU로 페일 오버를 시작하고 패킷 처리를 사용하도록 설정하기 위해 새도 스위치에 신호를 보냅니다.

- 비HA 모드: 이 모드에서는 HA(고가용성)가 없지만 각 DPU는 별도의 오프로드된 vDS에서 사용할 수 있습니다. 이 모드에서는 활성 네트워킹 데이터 경로 오프로드에 두 DPU를 모두 사용할 수 있습니다.

## 네트워크 오프로드 사용

네트워크 오프로드를 사용하도록 설정하려면 vCenter Server 및 VMware NSX®에서 여러 단계를 수행해야 합니다.

단계	솔루션
vSphere Distributed Switch 생성	<a href="#">vSphere Distributed Switch 생성</a>
호스트를 vSphere Distributed Switch에 연결	<a href="#">vSphere Distributed Switch에 호스트 추가</a>
NSX 호스트 전송 노드 구성	<a href="#">DPU 지원 vSphere Lifecycle Manager 클러스터에서 NSX 호스트 전송 노드 구성</a>
네트워크 오프로드가 있는 vSphere Distributed Switch의 토폴로지 보기	<a href="#">네트워크 오프로드 스위치의 토폴로지 보기</a>

## vSphere Distributed Switch 생성

여러 호스트의 네트워킹 구성을 중앙 위치에서 한 번에 처리할 수 있도록 데이터 센터에 vSphere Distributed Switch를 생성하는 방법을 알아봅니다.

### 절차

- 1 vSphere Client에서 인벤토리 트리의 데이터 센터를 마우스 오른쪽 버튼으로 클릭합니다.
- 2 **Distributed Switch > 새 Distributed Switch**를 선택합니다.
- 3 **이름 및 위치** 페이지에서 새 분산 스위치의 이름을 입력하거나 생성된 이름을 그대로 사용하고 **다음**을 클릭합니다.

#### 4 버전 선택 페이지에서 분산 스위치 버전을 선택하고 다음을 클릭합니다.

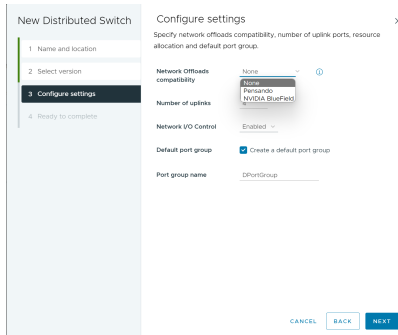
옵션	설명
Distributed Switch: 8.0.3	ESXi 8.0.3 이상과 호환됩니다. 이후 버전의 vSphere Distributed Switch에서 출시된 기능은 지원되지 않습니다.
Distributed Switch: 8.0.0	ESXi 8.0 이상과 호환됩니다. 이후 버전의 vSphere Distributed Switch에서 출시된 기능은 지원되지 않습니다.
Distributed Switch: 7.0.3	ESXi 7.0.3 이상과 호환됩니다. 이후 버전의 vSphere Distributed Switch에서 출시된 기능은 지원되지 않습니다.
Distributed Switch: 7.0.2	ESXi 7.0.2 이상과 호환됩니다. 이후 버전의 vSphere Distributed Switch에서 출시된 기능은 지원되지 않습니다.
Distributed Switch: 7.0.0	ESXi 7.0 이상과 호환됩니다. 이후 버전의 vSphere Distributed Switch에서 출시된 기능은 지원되지 않습니다.
Distributed Switch: 6.6.0	ESXi 6.7, ESXi 7.0 이상과 호환됩니다. 이후 버전의 vSphere Distributed Switch에서 출시된 기능은 지원되지 않습니다.



## 5 설정 구성 페이지에서 분산 스위치 설정을 구성합니다.

- a 드롭다운 메뉴를 사용하여 **네트워크 오프로드 호환성** 유형을 선택합니다.

그림 3-4. 네트워크 오프로드 호환성



네트워크 오프로드 호환성을 사용하여 네트워크 및 보안 기능을 DPU 디바이스로 오프로드할 수 있습니다. DPU는 계산 기능이 내장된 네트워크 카드입니다. 성능 향상을 위해 ESXi 호스트에서 DPU로 네트워킹 기능을 오프로드할 수 있습니다.

- **없음: 없음**을 선택하면 네트워크 오프로드 호환성이 지원되지 않습니다.
- **Pensando: Pensando**를 선택하면 네트워크 오프로드 호환성이 지원됩니다. **Network I/O Control**은 사용되지 않도록 설정됩니다.
- **NVIDIA BlueField: NVIDIA BlueField**를 선택하면 네트워크 오프로드 호환성이 지원됩니다. **Network I/O Control**은 사용되지 않도록 설정됩니다.

**참고** vSphere Distributed Switch 8.0.0 이상을 사용하는 경우 네트워크 오프로드 호환성을 구성할 수 있습니다.

- b 화살표 버튼을 사용하여 **업링크 수**를 선택합니다.

업링크 포트는 관련된 각 호스트의 물리적 NIC에 Distributed Switch를 연결합니다. 업링크 포트 수는 호스트당 Distributed Switch에 허용되는 물리적 최대 연결 수입니다.

- c 드롭다운 메뉴를 사용하여 **Network I/O Control**을 사용하거나 사용하지 않도록 설정합니다.

Network I/O Control을 사용하여 배포 요구 사항에 따라 특정 유형의 인프라 및 워크로드 트래픽의 네트워크 리소스에 대한 액세스에 우선 순위를 지정할 수 있습니다. Network I/O Control은 네트워크의 I/O 로드를 지속적으로 모니터링하고 사용 가능한 리소스를 동적으로 할당합니다.

- d (선택 사항) **기본 포트 그룹 생성** 확인란을 선택하여 이 스위치에 대한 기본 설정으로 새 분산 포트 그룹을 생성합니다. **포트 그룹 이름**을 입력하거나, 생성된 이름을 사용합니다.

시스템에 사용자 지정 포트 그룹 요구 사항이 있는 경우에는 Distributed Switch를 추가한 후에 해당 요구 사항을 충족하는 분산 포트 그룹을 생성하십시오.

- 6 **DPU 페일오버 구성** 페이지에서 페일오버 순서 목록을 구성하여 페일오버 발생 시 팀의 업링크가 사용되는 방식을 지정합니다. 일부 업링크만 사용하고 나머지 업링크는 사용 중인 업링크가 고장 나는 경우에 사용할 수 있도록 긴급용으로 예약하려면 **위로 이동** 및 **아래로 이동**을 사용하여 업링크를 다른 그룹으로 이동합니다.

**DPU 페일오버 구성** 페이지에서 DPU 매핑 업링크를 사용하는 방법을 지정할 수 있습니다. 호스트에 여러 DPU가 있는 경우 고가용성 모드에서 동일한 분산 스위치에 연결할 수 있습니다. 즉, 하나의 DPU는 활성 트래픽을 실행하고 다른 DPU는 대기 모드로 사용할 수 있습니다.

- a **미리 설정** 드롭다운 메뉴에서 DPU 유형을 선택합니다.
- **단일 DPU:** 단일 DPU를 선택하면 한 번에 하나의 DPU만 활성 DPU로 스위치에 연결됩니다.
  - **이중 DPU:** 이중 DPU를 선택하면 두 DPU가 동시에 스위치에 연결됩니다. 그 중 하나만 활성화됩니다.
  - **사용자 지정:** 사용자 지정을 선택하면 업링크를 지정할 수 있습니다.

옵션	설명
활성 업링크	DPU 어댑터 연결을 사용할 수 있고 활성 상태인 경우에 이 업링크를 계속 사용합니다.
대기 업링크	활성 DPU 어댑터가 다운된 경우 이 업링크를 사용합니다.

- 7 **완료 준비** 페이지에서 선택한 설정을 검토하고 **마침**을 클릭합니다.

설정을 편집하려면 **뒤로** 버튼을 사용합니다.

## 결과

데이터 센터에 Distributed Switch가 생성됩니다. 새 Distributed Switch로 이동하여 **요약** 탭을 클릭하면 Distributed Switch에서 지원되는 기능과 그 밖의 세부 정보를 볼 수 있습니다.

## 다음에 수행할 작업

Distributed Switch에 호스트를 추가하고 스위치에서 네트워크 어댑터를 구성합니다.

# 최신 버전으로 vSphere Distributed Switch 업그레이드

vSphere Distributed Switch 버전 6.x를 최신 버전으로 업그레이드하는 방법을 알아봅니다. 업그레이드하면 Distributed Switch에서 최신 버전에만 제공되는 기능을 이용할 수 있습니다.

Distributed Switch를 업그레이드하면 이 스위치에 연결된 호스트와 가상 시스템에서 잠시 동안 다운타임이 발생합니다.

**참고** 현재 VDS 버전이 6.5인 경우 스위치를 최신 버전으로 업그레이드하는 동안 짧은 다운타임이 발생할 수 있습니다. 현재 VDS 버전이 6.6이상이라면 스위치를 최신 버전으로 업그레이드하는 동안 다운타임이 발생하지 않을 수 있습니다.

자세한 내용은 [KB 52621](#)을 참조하십시오.

**참고** 업그레이드에 실패할 경우 가상 시스템 및 VMkernel 어댑터의 연결을 복원할 수 있도록 Distributed Switch의 구성을 백업하십시오.

성공적으로 업그레이드되지 않은 경우 해당 포트 그룹과 연결된 호스트로 스위치를 다시 생성하려면 스위치 구성 파일을 가져오면 됩니다. [vSphere Distributed Switch 구성 내보내기](#) 및 [vSphere Distributed Switch 구성 가져오기](#) 항목을 참조하십시오.

#### 사전 요구 사항

- vCenter Server를 버전 8.0로 업그레이드합니다.
- Distributed Switch에 연결된 모든 호스트를 ESXi 8.0로 업그레이드합니다.

#### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 Distributed Switch를 마우스 오른쪽 버튼으로 클릭하고 **업그레이드 > Distributed Switch 업그레이드**를 선택합니다.
- 3 스위치를 업그레이드할 vSphere Distributed Switch 버전을 선택하고 **다음**을 클릭합니다.

옵션	설명
Distributed Switch: 8.0.3	ESXi 8.0.3 이상과 호환됩니다. 새로운 기능 및 향상된 기능 <ul style="list-style-type: none"> <li>■ 이중 DPU 지원. <a href="#">네트워크 오프로드 호환성이란?</a>을 참조하십시오.</li> </ul>
Distributed Switch: 8.0.0	ESXi 8.0.0 이상과 호환됩니다. 새로운 기능 및 향상된 기능. <a href="#">네트워크 오프로드 호환성이란?</a> 을 참조하십시오.
Distributed Switch: 7.0.3	ESXi 7.0.3 이상과 호환됩니다. 새로운 기능 및 향상된 기능 <ul style="list-style-type: none"> <li>■ NVMe over TCP. <a href="#">vSphere Distributed Switch와 연결된 호스트에서 VMkernel 어댑터 생성</a>을 참조하십시오.</li> </ul>
Distributed Switch: 7.0.2	ESXi 7.0.2 이상과 호환됩니다. 새로운 기능 및 향상된 기능. <ul style="list-style-type: none"> <li>■ LACP 고속 모드. <a href="#">장 5 vSphere Distributed Switch의 LACP 지원</a>을 참조하십시오.</li> </ul>
Distributed Switch: 7.0.0	ESXi 7.0 이상과 호환됩니다. 새로운 기능 및 향상된 기능. <ul style="list-style-type: none"> <li>■ NSX 분산 포트 그룹. <a href="#">네트워킹 개념 개요</a>를 참조하십시오.</li> </ul>
Distributed Switch: 6.6.0	ESXi 6.7 이상과 호환됩니다. 이후 버전의 vSphere Distributed Switch에서 출시된 기능은 지원되지 않습니다. 새로운 기능 및 향상된 기능. <ul style="list-style-type: none"> <li>■ MAC 학습. <a href="#">MAC 학습 정책이란?</a> 항목을 참조하십시오.</li> </ul>

#### 4 호스트 호환성을 검토하고 다음을 클릭합니다.

Distributed Switch에 연결된 일부 ESXi 인스턴스가 선택한 대상 버전과 호환되지 않을 수도 있습니다. 호환되지 않는 호스트를 업그레이드 또는 제거하거나, Distributed Switch의 다른 업그레이드 버전을 선택하십시오.

#### 5 업그레이드 구성을 완료하고 마침을 클릭합니다.

**경고** vSphere Distributed Switch를 업그레이드한 후에는 이전 버전으로 되돌릴 수 없습니다. 스위치의 새 버전보다 이전 버전을 실행하고 있는 ESXi 호스트도 추가할 수 없습니다.

## 일반 및 고급 vSphere Distributed Switch 설정 편집

스위치 이름 및 업링크 수를 설정하여 vSphere Distributed Switch의 기본 설정을 사용하는 방법을 알아보십시오. Cisco Discovery Protocol 및 스위치의 최대 MTU를 비롯한 Distributed Switch에 대한 고급 설정을 사용하는 방법도 알아볼 수 있습니다.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치를 선택합니다.
- 2 **구성** 탭에서 **설정**을 확장하고 **속성**을 선택합니다.
- 3 **편집**을 클릭합니다.
- 4 **일반**을 클릭하여 vSphere Distributed Switch 설정을 편집합니다.

옵션	설명
이름	분산 스위치의 이름을 입력합니다.
Network I/O Control	Network I/O Control을 활성화하거나 비활성화하려면 드롭다운 메뉴를 사용합니다. <b>참고</b> 이 메뉴 옵션은 <b>네트워크 오프로드 호환성</b> 이 활성화되면 비활성화됩니다.
네트워크 오프로드 호환성	네트워크 오프로드 호환성 유형을 선택하려면 드롭다운 메뉴를 사용합니다. <ul style="list-style-type: none"> <li>■ <b>없음</b>: 없음을 선택하면 네트워크 오프로드 호환성이 활성화되지 않습니다.</li> <li>■ <b>Pensando</b>: Pensando를 선택하면 Network I/O Control이 비활성화됩니다.</li> <li>■ <b>NVIDIA BlueField</b>: NVIDIA BlueField를 선택하면 Network I/O Control이 비활성화됩니다.</li> </ul>
설명	Distributed Switch 설정의 설명을 추가하거나 수정합니다.

## 5 고급을 클릭하여 vSphere Distributed Switch 설정을 편집합니다.

옵션	설명
MTU(바이트)	vSphere Distributed Switch의 최대 MTU 크기입니다. 점보 프레임을 사용하도록 설정하려면 1,500바이트보다 큰 값을 설정합니다.
멀티캐스트 필터링 모드	<ul style="list-style-type: none"> <li>■ <b>기본.</b> Distributed Switch는 멀티캐스트 그룹 IPv4 주소의 마지막 23비트에서 생성된 MAC 주소를 기반으로 하는 멀티캐스트 그룹과 관련된 트래픽을 전달합니다.</li> <li>■ <b>IGMP/MLD 스누핑.</b> Distributed Switch는 IGMP(Internet Group Management Protocol) 및 MLD(Multicast Listener Discovery) 프로토콜에서 정의한 멤버 자격 메시지를 사용하여 구독된 멀티캐스트 그룹의 IPv4 및 IPv6 주소에 따라 멀티캐스트 트래픽을 가상 시스템으로 전달합니다.</li> </ul>
검색 프로토콜	<p>a <b>유형</b> 드롭다운 메뉴에서 Cisco Discovery Protocol, Link Layer Discovery Protocol 또는 (사용 안 함)을 선택합니다.</p> <p>b <b>작업</b>을 [수신], [알림] 또는 [둘 다]로 설정합니다.</p> <p>탐색 프로토콜에 대한 자세한 내용은 <a href="#">스위치 탐색 프로토콜</a>의 내용을 참조하십시오.</p>
관리자 연락처	분산 스위치 관리자의 이름 및 기타 세부 정보를 입력합니다.

## 6 업링크를 클릭하여 vSphere Distributed Switch 설정을 편집합니다.

옵션	설명
업링크 수	Distributed Switch에 대한 업링크 포트를 추가하려면 <b>추가</b> 를 선택합니다. 업링크의 이름을 수정하려면 업링크 이름 편집을 수행합니다.

## 7 확인을 클릭합니다.

# vSphere Distributed Switch의 여러 호스트에서 네트워킹 관리

호스트를 스위치에 추가하고 해당 네트워크 어댑터를 이 스위치에 연결하여 vSphere Distributed Switch에서 가상 네트워크를 생성하고 관리하는 방법을 알아봅니다. Distributed Switch의 여러 호스트 전체에서 동일한 네트워킹 구성을 생성하려면 호스트 하나를 템플릿으로 사용하여 해당 구성을 다른 호스트에 적용하면 됩니다.

## vSphere Distributed Switch의 호스트 네트워킹 관리 작업

vSphere Distributed Switch에 새 호스트를 추가하고, 네트워크 어댑터를 스위치에 연결하며, 스위치에서 호스트를 제거할 수 있습니다. 운영 환경에서는 Distributed Switch의 호스트 네트워킹을 관리하는 동안 가상 시스템 및 VMkernel 서비스에 대해 네트워크 연결을 유지해야 할 수 있습니다.

## vSphere Distributed Switch에 호스트 추가

환경을 준비하고 나서 Distributed Switch에 새 호스트를 추가하는 것이 좋습니다.

- 가상 시스템 네트워킹에 사용할 분산 포트 그룹을 생성합니다.
- VMkernel 서비스에 사용할 분산 포트 그룹을 생성합니다. 예를 들어 관리 네트워크, vMotion 및 Fault Tolerance에 대한 분산 포트 그룹을 생성합니다.

- Distributed Switch에서 스위치에 연결할 모든 물리적 NIC에 대해 업링크를 충분히 구성합니다. 예를 들어 Distributed Switch에 연결할 호스트에 각각 8개의 물리적 NIC가 있는 경우 Distributed Switch에서 8개의 업링크를 구성합니다.
- 특정 네트워킹 요구 사항이 있는 서비스에 대해 Distributed Switch의 구성을 준비해야 합니다. 예를 들어 iSCSI의 경우 iSCSI VMkernel 어댑터를 연결하는 분산 포트 그룹의 팀 구성 및 페일오버 구성에 대한 특정 요구 사항이 있습니다.

**호스트 추가 및 관리** 마법사를 사용하여 여러 호스트를 동시에 추가할 수 있습니다.

## vSphere Distributed Switch의 네트워크 어댑터 관리

Distributed Switch에 호스트를 추가한 후 스위치의 물리적 NIC를 연결하고, 가상 시스템 네트워크 어댑터를 구성하며, VMkernel 네트워킹을 관리할 수 있습니다.

Distributed Switch의 일부 호스트가 데이터 센터의 다른 스위치에 연결된 경우 Distributed Switch 간에 네트워크 어댑터를 마이그레이션할 수 있습니다.

가상 시스템 네트워크 어댑터 또는 VMkernel 어댑터를 마이그레이션하는 경우 대상 분산 포트 그룹에 하나 이상의 활성 업링크가 있고 이 업링크가 호스트의 물리적 NIC에 연결되어 있어야 합니다. 또 다른 방법으로 물리적 NIC, 가상 네트워크 어댑터 및 VMkernel 어댑터를 동시에 마이그레이션할 수도 있습니다.

물리적 NIC를 마이그레이션하는 경우 포트 그룹의 트래픽을 처리하는 활성 NIC를 하나 이상 유지하십시오. 예를 들어 *vmnic0*과 *vmnic1*이 *VM Network* 포트 그룹의 트래픽을 처리하는 경우 *vmnic0*은 마이그레이션하고 *vmnic1*은 그룹에 연결된 상태를 유지합니다.

VMkernel 인터페이스 및 물리적 NIC를 vSphere Distributed Switch에 마이그레이션하는 데 관한 동영상을 시청하십시오.

## vSphere Distributed Switch에서 호스트 제거

Distributed Switch에서 호스트를 제거하기 전에 사용 중인 네트워크 어댑터를 다른 스위치로 마이그레이션해야 합니다.

- 다른 Distributed Switch에 호스트를 추가하기 위해 **호스트 추가 및 관리** 마법사를 사용하여 호스트의 네트워크 어댑터를 모두 함께 새 스위치로 마이그레이션할 수 있습니다. 그런 다음 현재 Distributed Switch에서 안전하게 호스트를 제거할 수 있습니다.
- 호스트 네트워킹을 표준 스위치로 마이그레이션하려면 네트워크 어댑터를 단계적으로 마이그레이션해야 합니다. 예를 들어 네트워크 연결을 유지할 수 있도록 Distributed Switch에 연결된 각 호스트에 하나의 물리적

NIC를 남기는 방식으로 Distributed Switch에서 호스트의 물리적 NIC를 제거합니다. 그런 다음 물리적 NIC를 표준 스위치에 연결하고 VMkernel 어댑터 및 가상 시스템 네트워크 어댑터를 스위치로 마이그레이션합니다. 마지막으로 Distributed Switch에 연결된 상태로 유지한 물리적 NIC를 표준 스위치로 마이그레이션합니다.

## 다음으로 읽을 항목

- [vSphere Distributed Switch의 호스트 네트워킹 관리 작업](#)  
vSphere Distributed Switch에 새 호스트를 추가하고, 네트워크 어댑터를 스위치에 연결하며, 스위치에서 호스트를 제거할 수 있습니다. 운영 환경에서는 Distributed Switch의 호스트 네트워킹을 관리하는 동안 가상 시스템 및 VMkernel 서비스에 대해 네트워크 연결을 유지해야 할 수 있습니다.
- [vSphere Distributed Switch에 호스트 추가](#)  
vSphere Distributed Switch를 사용하여 vSphere 환경의 네트워킹을 관리하는 방법을 알아봅니다. 호스트를 스위치와 연결해야 합니다. 호스트의 물리적 NIC, VMkernel 어댑터 및 가상 시스템 네트워크 어댑터를 Distributed Switch에 연결합니다.
- [vSphere Distributed Switch에서 물리적 네트워크 어댑터 구성](#)  
Distributed Switch와 연결된 호스트에 대한 스위치의 업링크에 물리적 NIC를 할당하는 방법을 알아봅니다. Distributed Switch에서 여러 호스트에 대한 물리적 NIC를 한 번에 구성할 수 있습니다.
- [VMkernel 어댑터를 vSphere Distributed Switch로 마이그레이션](#)  
Distributed Switch만 사용하여 VMkernel 서비스에 대한 트래픽을 처리하고 다른 표준 스위치 또는 Distributed Switch에서 더 이상 VMkernel 어댑터가 필요하지 않은 경우 VMkernel 어댑터를 Distributed Switch로 마이그레이션하는 방법을 알아봅니다.
- [vSphere Distributed Switch에서 VMkernel 어댑터 생성](#)  
Distributed Switch와 연결된 호스트에 VMkernel 어댑터를 생성하여 호스트에 네트워크 연결을 제공하고 vSphere vMotion, IP 스토리지, Fault Tolerance 로깅 및 vSAN의 트래픽을 처리하는 방법을 알아봅니다.
- [가상 시스템 네트워킹을 vSphere Distributed Switch로 마이그레이션](#)  
Distributed Switch를 사용하여 가상 시스템 네트워킹을 관리하고 스위치에서 레이블이 지정된 네트워크로 가상 시스템 네트워크 어댑터를 마이그레이션하는 방법을 알아봅니다.
- [vSphere Distributed Switch에서 호스트 제거](#)  
호스트에 대해 다른 스위치를 구성한 경우 vSphere Distributed Switch에서 호스트를 제거하는 방법을 알아봅니다.

## vSphere Distributed Switch의 호스트 네트워킹 관리 작업

vSphere Distributed Switch에 새 호스트를 추가하고, 네트워크 어댑터를 스위치에 연결하며, 스위치에서 호스트를 제거할 수 있습니다. 운영 환경에서는 Distributed Switch의 호스트 네트워킹을 관리하는 동안 가상 시스템 및 VMkernel 서비스에 대해 네트워크 연결을 유지해야 할 수 있습니다.

## vSphere Distributed Switch에 호스트 추가

환경을 준비하고 나서 Distributed Switch에 새 호스트를 추가하는 것이 좋습니다.

- 가상 시스템 네트워킹에 사용할 분산 포트 그룹을 생성합니다.
- VMkernel 서비스에 사용할 분산 포트 그룹을 생성합니다. 예를 들어 관리 네트워크, vMotion 및 Fault Tolerance에 대한 분산 포트 그룹을 생성합니다.
- Distributed Switch에서 스위치에 연결할 모든 물리적 NIC에 대해 업링크를 충분히 구성합니다. 예를 들어 Distributed Switch에 연결할 호스트에 각각 8개의 물리적 NIC가 있는 경우 Distributed Switch에서 8개의 업링크를 구성합니다.
- 특정 네트워킹 요구 사항이 있는 서비스에 대해 Distributed Switch의 구성을 준비해야 합니다. 예를 들어 iSCSI의 경우 iSCSI VMkernel 어댑터를 연결하는 분산 포트 그룹의 팀 구성 및 페일오버 구성에 대한 특정 요구 사항이 있습니다.

**호스트 추가 및 관리** 마법사를 사용하여 여러 호스트를 동시에 추가할 수 있습니다.

## vSphere Distributed Switch의 네트워크 어댑터 관리

Distributed Switch에 호스트를 추가한 후 스위치의 물리적 NIC를 연결하고, 가상 시스템 네트워크 어댑터를 구성하며, VMkernel 네트워킹을 관리할 수 있습니다.

Distributed Switch의 일부 호스트가 데이터 센터의 다른 스위치에 연결된 경우 Distributed Switch 간에 네트워크 어댑터를 마이그레이션할 수 있습니다.

가상 시스템 네트워크 어댑터 또는 VMkernel 어댑터를 마이그레이션하는 경우 대상 분산 포트 그룹에 하나 이상의 활성 업링크가 있고 이 업링크가 호스트의 물리적 NIC에 연결되어 있어야 합니다. 또 다른 방법으로 물리적 NIC, 가상 네트워크 어댑터 및 VMkernel 어댑터를 동시에 마이그레이션할 수도 있습니다.

물리적 NIC를 마이그레이션하는 경우 포트 그룹의 트래픽을 처리하는 활성 NIC를 하나 이상 유지하십시오. 예를 들어 *vmnic0*과 *vmnic1*이 *VM Network* 포트 그룹의 트래픽을 처리하는 경우 *vmnic0*은 마이그레이션하고 *vmnic1*은 그룹에 연결된 상태를 유지합니다.

VMkernel 인터페이스 및 물리적 NIC를 vSphere Distributed Switch에 마이그레이션하는 데 관한 동영상을 시청하십시오.

## vSphere Distributed Switch에서 호스트 제거

Distributed Switch에서 호스트를 제거하기 전에 사용 중인 네트워크 어댑터를 다른 스위치로 마이그레이션해야 합니다.

- 다른 Distributed Switch에 호스트를 추가하기 위해 **호스트 추가 및 관리** 마법사를 사용하여 호스트의 네트워크 어댑터를 모두 함께 새 스위치로 마이그레이션할 수 있습니다. 그런 다음 현재 Distributed Switch에서 안전하게 호스트를 제거할 수 있습니다.
- 호스트 네트워킹을 표준 스위치로 마이그레이션하려면 네트워크 어댑터를 단계적으로 마이그레이션해야 합니다. 예를 들어 네트워크 연결을 유지할 수 있도록 Distributed Switch에 연결된 각 호스트에 하나의 물리적



NIC를 남기는 방식으로 Distributed Switch에서 호스트의 물리적 NIC를 제거합니다. 그런 다음 물리적 NIC를 표준 스위치에 연결하고 VMkernel 어댑터 및 가상 시스템 네트워크 어댑터를 스위치로 마이그레이션합니다. 마지막으로 Distributed Switch에 연결된 상태로 유지한 물리적 NIC를 표준 스위치로 마이그레이션합니다.

## vSphere Distributed Switch에 호스트 추가

vSphere Distributed Switch를 사용하여 vSphere 환경의 네트워킹을 관리하는 방법을 알아봅니다. 호스트를 스위치와 연결해야 합니다. 호스트의 물리적 NIC, VMkernel 어댑터 및 가상 시스템 네트워크 어댑터를 Distributed Switch에 연결합니다.

### 사전 요구 사항

- 스위치에 연결하려는 물리적 NIC에 할당할 수 있는 업링크가 Distributed Switch에 충분히 있는지 확인합니다.
- Distributed Switch에 하나 이상의 분산 포트 그룹이 있는지 확인합니다.
- 분산 포트 그룹의 팀 구성 및 페일오버 정책에 활성 업링크가 구성되어 있는지 확인합니다.

iSCSI용 VMkernel 어댑터를 마이그레이션하거나 생성하는 경우 대상 분산 포트 그룹의 팀 구성 및 페일오버 정책이 iSCSI에 대한 요구 사항을 충족하는지 확인합니다.

- 업링크 하나만 활성 상태이고 대기 목록은 비어 있으며 나머지 업링크는 사용되지 않는지 확인합니다.
- 호스트당 물리적 NIC 하나만 활성 업링크에 할당되어 있는지 확인합니다.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 Distributed Switch를 마우스 오른쪽 버튼으로 클릭하고 **호스트 추가 및 관리**를 선택합니다.
- 3 작업 선택 페이지에서 **호스트 추가**를 선택하고 **다음**을 클릭합니다.
- 4 [호스트 선택] 페이지에서
  - a **모든 호스트** 아래에 있는 사용 가능한 호스트 목록에서 호스트를 선택합니다.
  - b 선택한 호스트를 보려면 **선택됨**을 클릭합니다.  
선택한 호스트가 표시됩니다.
  - c 호환성을 기준으로 호스트를 필터링하려면 **호환성**을 클릭합니다.

---

**참고** 네트워크 오프로드 호환성이 있는 vSphere Distributed Switch에 호스트를 추가하는 동안은 호환되는 DPU가 지원하는 호환되는 어댑터만 추가할 수 있습니다.

  - d 사용 가능한 모든 호스트를 선택하려면 **모두 선택**을 클릭합니다.
- 5 **다음**을 클릭합니다.
- 6 **물리적 어댑터 관리** 페이지에서 업링크를 할당하거나 할당 취소하여 Distributed Switch에 네트워크 어댑터를 추가하거나 제거할 수 있습니다.

7 동일한 물리적 네트워크 어댑터가 있는 모든 호스트의 어댑터를 관리하려면 **모든 호스트의 어댑터**를 선택합니다.

- a **모두 선택**을 클릭하여 모든 호스트를 선택합니다.
- b 호스트에 업링크를 할당하려면 드롭다운 메뉴에서 업링크를 선택합니다.
- c 호스트에서 업링크를 할당 취소하려면 드롭다운 메뉴에서 **없음**을 선택합니다.
- d 호스트에 대한 자세한 내용을 보려면 **물리적 네트워크 어댑터** 아래에 나열된 네트워크 어댑터를 확장합니다.
- e 이 VMkernel 어댑터를 사용하는 스위치는 **스위치에서 사용 중**에서 볼 수 있습니다.

예를 들어 *uplink1*을 *vmnic1*에 할당하면 *vmnic1*을 물리적 네트워크 어댑터로 사용하는 모든 호스트에 할당됩니다.

8 호스트별로 어댑터를 관리하려면 **호스트당 어댑터**를 선택합니다.

- a 목록에서 개별 호스트를 선택합니다.
- b 호스트에 업링크를 할당하려면 드롭다운 메뉴에서 업링크를 선택합니다.
- c 호스트에서 업링크를 할당 취소하려면 드롭다운 메뉴에서 **없음**을 선택합니다.

다른 표준 스위치 또는 Distributed Switch에 할당된 물리적 NIC를 선택하면 해당 NIC가 현재 분산 스위치로 마이그레이션됩니다.

일관된 네트워크 구성을 위해 각 호스트에 있는 하나의 동일한 물리적 NIC를 Distributed Switch의 동일한 업링크에 연결할 수 있습니다.

예를 들어 두 개의 호스트를 추가하는 경우 각 호스트의 *vmnic1*을 Distributed Switch의 *Uplink1*에 연결합니다.

9 다음을 클릭합니다.

---

**참고** 호스트에 물리적 네트워크 어댑터가 할당되어 있지 않으면 주의 메시지가 나타납니다.

---

10 **VMkernel 어댑터 관리 페이지**에서 Distributed Switch에 대한 VMkernel 어댑터를 관리할 수 있습니다.

11 동일한 VMkernel 어댑터가 있는 모든 호스트에서 VMkernel 어댑터를 관리하려면 **모든 호스트의 어댑터**를 선택합니다.

- a 모든 호스트를 선택하려면 **모두 선택**을 클릭합니다.
- b **포트 그룹 할당**을 클릭합니다.  
사용 가능한 모든 포트 그룹을 볼 수 있습니다.
- c 포트 그룹을 할당하려면 **할당**을 클릭합니다.
- d 포트 그룹을 할당 취소하려면 **할당 취소**를 클릭합니다.
- e 이 VMkernel 어댑터를 사용하는 스위치는 **스위치에서 사용 중**에서 볼 수 있습니다.
- f 호스트에 대한 자세한 내용을 보려면 **이름** 아래에 나열된 VMkernel 어댑터를 확장합니다.

예를 들어 *DPortGroup1*을 *vmk00*에 할당하면 *vmk00*을 VMkernel 네트워크 어댑터로 사용하는 모든 호스트에 포트 그룹이 할당됩니다.

12 호스트별로 VMkernel 어댑터를 관리하려면 **호스트당 어댑터**를 선택합니다.

- a 목록에서 개별 호스트를 선택합니다.
- b **포트 그룹 할당**을 클릭합니다.  
사용 가능한 모든 포트 그룹을 볼 수 있습니다.
- c 포트 그룹을 할당하려면 **할당**을 클릭합니다.
- d 포트 그룹을 할당 취소하려면 **할당 취소**를 클릭합니다.

13 다음을 클릭합니다.

14 **VM 네트워킹 마이그레이션** 페이지에서 **가상 시스템 네트워킹 마이그레이션** 확인란을 선택하여 가상 시스템을 Distributed Switch로 마이그레이션합니다.

15 네트워크 어댑터별로 구성하려면 **포트 그룹 할당**을 클릭합니다.

- a 포트 그룹을 할당하려면 **할당**을 클릭합니다.  
예를 들어 포트 그룹은 네트워크 어댑터가 동일한 모든 가상 시스템에 할당됩니다.
- b 포트 그룹을 할당 취소하려면 **할당 취소**를 클릭합니다.

16 가상 시스템별로 구성하려면 **포트 그룹 할당**을 클릭합니다.

- a 포트 그룹을 할당하려면 **할당**을 클릭합니다.
- b 포트 그룹을 할당 취소하려면 **할당 취소**를 클릭합니다.

17 다음을 클릭합니다.

18 **호스트 추가 및 관리** 마법사의 **완료 준비** 페이지에서 가상 시스템의 설정을 검토합니다.

19 **마침**을 클릭합니다.

이제 vSphere Distributed Switch에 호스트가 추가되었습니다.

#### 다음에 수행할 작업

호스트를 Distributed Switch에 연결한 후에는 물리적 네트워크 어댑터, VMkernel 어댑터 및 가상 시스템 네트워크 어댑터를 관리할 수 있습니다.

## vSphere Distributed Switch에서 물리적 네트워크 어댑터 구성

Distributed Switch와 연결된 호스트에 대한 스위치의 업링크에 물리적 NIC를 할당하는 방법을 알아봅니다. Distributed Switch에서 여러 호스트에 대한 물리적 NIC를 한 번에 구성할 수 있습니다.

모든 호스트에서 일관된 네트워킹 구성을 적용하려면 각 호스트에서 동일한 물리적 NIC를 Distributed Switch의 동일한 업링크에 할당하면 됩니다. 예를 들어 *ESXi A* 및 *ESXi B* 호스트의 *vmnic1*을 *Uplink 10*에 할당할 수 있습니다.

## 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 Distributed Switch를 마우스 오른쪽 버튼으로 클릭하고 **호스트 추가 및 관리**를 선택합니다.
- 3 [작업 선택] 페이지에서 **호스트 네트워킹 관리**를 선택하고 **다음**을 클릭합니다.
- 4 [호스트 선택] 페이지의 **멤버 호스트**에서 Distributed Switch와 연결된 호스트 중에 선택합니다.
- 5 **다음**을 클릭합니다.

- 6 **물리적 어댑터 관리 페이지**에서 업링크를 할당하거나 할당 취소하여 Distributed Switch에 네트워크 어댑터를 추가하거나 제거할 수 있습니다.
- 7 동일한 물리적 네트워크 어댑터가 있는 모든 호스트의 어댑터를 관리하려면 **모든 호스트의 어댑터**를 선택합니다.

업링크 드롭다운 메뉴에서 옵션을 선택하는 동안 사용자가 --를 볼 수 있습니다. 이 옵션은 동일한 네트워크 어댑터를 사용하는 호스트 중 일부는 동일한 업링크에 할당될 수 없음을 나타냅니다.

예를 들어 *vmnic 00*이 *ESXI A*의 *Uplink 1*에 할당되고 *ESXI B*의 *Uplink 2*에 할당된 경우 드롭다운 메뉴에서 -- 옵션이 선택됩니다. 이 옵션을 선택하고 다음 작업으로 이동해도 구성이 변경되지 않습니다.

- a 호스트에 업링크를 할당하려면 드롭다운 메뉴에서 업링크를 선택합니다.
  - b 호스트에서 업링크를 할당 취소하려면 드롭다운 메뉴에서 **없음**을 선택합니다.
  - c 이 VMkernel 어댑터를 사용하는 스위치는 **스위치에서 사용 중**에서 볼 수 있습니다.
  - d 호스트에 대한 자세한 내용을 보려면 **물리적 네트워크 어댑터** 아래에 나열된 네트워크 어댑터를 확장합니다.
- 8 호스트별로 어댑터를 관리하려면 **호스트당 어댑터**를 선택합니다.
    - a 목록에서 개별 호스트를 선택합니다.
    - b 호스트에 업링크를 할당하려면 드롭다운 메뉴에서 업링크를 선택합니다.
    - c 호스트에서 업링크를 할당 취소하려면 드롭다운 메뉴에서 **없음**을 선택합니다.

---

**참고** 네트워크 오프로드 호환성이 있는 vSphere Distributed Switch에 호스트를 추가하는 동안은 호환되는 DPU에서 지원되는 호환 어댑터만 추가할 수 있습니다.

---

다른 표준 스위치 또는 Distributed Switch에 이미 할당된 물리적 NIC를 선택하면 해당 NIC가 현재 Distributed Switch로 마이그레이션됩니다.

일관된 네트워크 구성을 위해 각 호스트에 있는 하나의 동일한 물리적 NIC를 Distributed Switch의 동일한 업링크에 연결할 수 있습니다.

예를 들어 두 개의 호스트를 추가하는 경우 각 호스트의 *vmnic 1*을 분산 스위치의 *Uplink 1*에 연결합니다.

- 9 **다음**을 클릭합니다.

---

**참고** 호스트에 물리적 네트워크 어댑터가 할당되어 있지 않으면 주의 메시지가 나타납니다.

---

- 10 **VMkernel 어댑터 관리** 페이지에서 VMkernel 어댑터를 Distributed Switch에 추가할 수 있습니다.
- 11 **VM 네트워킹 마이그레이션** 페이지에서 **가상 시스템 네트워킹 마이그레이션** 확인란을 선택하여 가상 시스템을 Distributed Switch로 마이그레이션합니다.
- 12 다음을 클릭합니다.
- 13 **호스트 추가 및 관리** 마법사의 **완료 준비** 페이지에서 가상 시스템의 설정을 검토합니다.
- 14 **마침**을 클릭합니다.

## VMkernel 어댑터를 vSphere Distributed Switch로 마이그레이션

Distributed Switch만 사용하여 VMkernel 서비스에 대한 트래픽을 처리하고 다른 표준 스위치 또는 Distributed Switch에서 더 이상 VMkernel 어댑터가 필요하지 않은 경우 VMkernel 어댑터를 Distributed Switch로 마이그레이션하는 방법을 알아봅니다.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 Distributed Switch를 마우스 오른쪽 버튼으로 클릭하고 **호스트 추가 및 관리**를 선택합니다.
- 3 [작업 선택] 페이지에서 **호스트 네트워킹 관리**를 선택하고 **다음**을 클릭합니다.
- 4 [호스트 선택] 페이지의 **멤버 호스트**에서 Distributed Switch와 연결된 호스트 중에 선택합니다.
- 5 **다음**을 클릭합니다.
- 6 **물리적 어댑터 관리** 페이지에서 업링크를 할당하거나 할당 취소하여 Distributed Switch에 네트워크 어댑터를 추가하거나 제거할 수 있습니다.
- 7 **다음**을 클릭합니다.

---

**참고** 호스트에 물리적 네트워크 어댑터가 할당되어 있지 않으면 주의 메시지가 나타납니다.

---

- 8 **VMkernel 어댑터 관리** 페이지에서 Distributed Switch에 대한 VMkernel 어댑터를 관리할 수 있습니다.
- 9 동일한 VMkernel 어댑터가 있는 모든 호스트에서 VMkernel 어댑터를 관리하려면 **모든 호스트의 어댑터**를 선택합니다.
  - a **포트 그룹 할당**을 클릭합니다.  
사용 가능한 모든 포트 그룹을 볼 수 있습니다.
  - b 포트 그룹을 할당하려면 **할당**을 클릭합니다.
  - c 포트 그룹을 할당 취소하려면 **할당 취소**를 클릭합니다.  
예를 들어 *DPortGroup1*을 *vmk00*에 할당하면 *vmk00*을 VMkernel 네트워크 어댑터로 사용하는 모든 호스트에 포트 그룹이 할당됩니다.
- 10 호스트에 대한 자세한 내용을 보려면 **이름** 아래에 나열된 VMkernel 어댑터를 확장합니다.
- 11 이 VMkernel 어댑터를 사용하는 스위치는 **스위치에서 사용** 중에서 볼 수 있습니다.

- 12 호스트별로 VMkernel 어댑터를 관리하려면 **호스트당 어댑터**를 선택합니다.
  - a 목록에서 개별 호스트를 선택합니다.
  - b **포트 그룹 할당**을 클릭합니다.  
사용 가능한 모든 포트 그룹을 볼 수 있습니다.
  - c 포트 그룹을 할당하려면 **할당**을 클릭합니다.
  - d 포트 그룹을 할당 취소하려면 **할당 취소**를 클릭합니다.
- 13 다음을 클릭합니다.
- 14 **VM 네트워킹 마이그레이션** 페이지에서 **가상 시스템 네트워킹 마이그레이션** 확인란을 선택하여 가상 시스템을 Distributed Switch로 마이그레이션합니다.
- 15 다음을 클릭합니다.
- 16 **호스트 추가 및 관리** 마법사의 **완료 준비** 페이지에서 가상 시스템의 설정을 검토합니다.
- 17 **마침**을 클릭합니다.

## vSphere Distributed Switch에서 VMkernel 어댑터 생성

Distributed Switch와 연결된 호스트에 VMkernel 어댑터를 생성하여 호스트에 네트워크 연결을 제공하고 vSphere vMotion, IP 스토리지, Fault Tolerance 로깅 및 vSAN의 트래픽을 처리하는 방법을 알아봅니다.

각 VMkernel 어댑터에 대해 전용 분산 포트 그룹을 하나씩 사용해야 하며, 한 VMkernel 어댑터는 트래픽 유형을 하나씩만 처리해야 합니다.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 포트 그룹으로 이동합니다.
- 2 **작업** 메뉴에서 **VMkernel 어댑터 추가**를 선택합니다.
- 3 [호스트 선택] 페이지에서 **연결된 호스트**를 클릭하고 Distributed Switch와 연결된 호스트에서 선택한 후 **확인**을 클릭합니다.
- 4 다음을 클릭합니다.
- 5 VMkernel 인터페이스 구성 페이지에서 VMkernel 어댑터에 대한 설정을 구성합니다.

옵션	설명
네트워크 레이블	네트워크 레이블은 분산 포트 그룹의 레이블에서 상속됩니다.
IP 설정	IPv4, IPv6 또는 둘 모두를 선택합니다. <b>참고</b> IPv6을 사용하도록 설정하지 않은 호스트에는 IPv6 옵션이 표시되지 않습니다.
MTU	스위치에서 네트워크 어댑터에 대한 MTU를 가져올지 또는 사용자 지정 크기를 설정할지 선택합니다. MTU 크기를 9,000바이트보다 큰 값으로 설정할 수 없습니다.

옵션	설명
TCP/IP 스택	<p>목록에서 TCP/IP 스택을 선택합니다. VMkernel 어댑터에 대한 TCP/IP 스택을 설정하고 나면 나중에 변경할 수 없습니다. vMotion 또는 프로비저닝 TCP/IP 스택을 선택하는 경우 이러한 스택만 사용하여 호스트의 vMotion 또는 프로비저닝 스택을 처리할 수 있습니다. 기본 TCP/IP 스택의 vMotion에 대한 모든 VMkernel 어댑터는 이후 vMotion 세션에 대해 비활성화되어 있습니다. 프로비저닝 TCP/IP 스택을 설정하는 경우 기본 TCP/IP 스택의 VMkernel 어댑터가 프로비저닝 트래픽이 포함된 작업(예: 가상 시스템 콜드 마이그레이션, 복제, 스냅샷 마이그레이션)에 대해 비활성화됩니다.</p>
사용 가능한 서비스	<p>호스트의 기본 TCP/IP 스택에 대해 서비스를 사용하도록 설정할 수 있습니다. 사용 가능한 다음 서비스 중에서 선택합니다.</p> <ul style="list-style-type: none"> <li>■ <b>vMotion.</b> VMkernel 어댑터가 자신이 vMotion 트래픽이 전송되는 네트워크 연결 임을 다른 호스트에 알리도록 설정합니다. vMotion을 사용한 선택된 호스트로의 마이그레이션은 vMotion 서비스가 기본 TCP/IP 스택의 VMkernel 어댑터에 대해 사용되도록 설정되어 있지 않거나 vMotion TCP/IP 스택을 사용하는 어댑터가 없는 경우 불가능합니다.</li> <li>■ <b>프로비저닝.</b> 가상 시스템 콜드 마이그레이션, 복제 및 스냅샷 마이그레이션을 위해 전송된 데이터를 처리합니다.</li> <li>■ <b>Fault Tolerance 로깅.</b> 호스트에서 Fault Tolerance 로깅을 사용하도록 설정합니다. 호스트당 FT 트래픽에 대해 하나의 VMkernel 어댑터만 사용할 수 있습니다.</li> <li>■ <b>관리.</b> 호스트 및 vCenter Server에 관리 트래픽을 사용하도록 설정합니다. 일반적으로 호스트에서는 ESXi 소프트웨어가 설치될 때 이러한 VMkernel 어댑터가 생성됩니다. 호스트에서 관리 트래픽용 VMkernel 어댑터를 추가로 생성하여 이중화 기능을 제공할 수 있습니다.</li> <li>■ <b>vSphere Replication.</b> 소스 ESXi 호스트에서 vSphere Replication 서버로 전송된 나가는 복제 데이터를 처리합니다.</li> <li>■ <b>vSphere Replication NFC.</b> 대상 복제 사이트의 들어오는 복제 데이터를 처리합니다.</li> <li>■ <b>vSAN.</b> 호스트에서 vSAN 트래픽이 사용되도록 설정합니다. vSAN 클러스터에 속하는 모든 호스트에는 이러한 VMkernel 어댑터가 있어야 합니다.</li> <li>■ <b>vSphere Backup NFC.</b> 전용 백업 NFC 트래픽에 대한 VMkernel 포트 설정입니다. vSphere 백업 NFC 서비스를 사용하도록 설정하면 NFC 트래픽이 VMkernel 어댑터를 통과합니다.</li> <li>■ <b>NVMe over TCP.</b> 전용 NVMe over TCP 스토리지 트래픽에 대한 VMkernel 포트 설정입니다. NVMe over TCP 어댑터를 사용하도록 설정하면 NVMe over TCP 스토리지 트래픽이 VMkernel 어댑터를 통과합니다. 자세한 내용은 "vSphere 스토리지 가이드" 를 참조하십시오.</li> <li>■ <b>NVMe over RDMA.</b> 전용 NVMe over RDMA 스토리지 트래픽에 대한 VMkernel 포트 설정입니다. NVMe over RDMA 어댑터를 사용하도록 설정하면 NVMe over RDMA 스토리지 트래픽이 VMkernel 어댑터를 통과합니다. 자세한 내용은 "vSphere 스토리지 가이드" 를 참조하십시오.</li> </ul>

## 6 IPv4 설정 페이지에서 IP 주소를 가져오는 옵션을 선택합니다.

옵션	설명
자동으로 IPv4 설정 가져오기	DHCP를 사용하여 IP 설정을 가져옵니다. DHCP 서버가 네트워크에 표시되어야 합니다.
정적 IPv4 설정 사용	VMkernel 어댑터의 IPv4 IP 주소와 서브넷 마스크를 입력합니다. IPv4에 대한 VMkernel 기본 게이트웨이와 DNS 서버 주소는 선택한 TCP/IP 스택에서 가져옵니다. VMkernel 기본 게이트웨이를 변경하려면 <b>VMkernel 어댑터에 구성</b> 또는 <b>TCP/IP 스택에 구성</b> 을 선택하고 게이트웨이 주소를 입력합니다.

## 7 IPv6 설정 페이지에서 IPv6 주소를 가져오는 옵션을 선택합니다.

옵션	설명
DHCP를 통해 자동으로 IPv6 주소 가져오기	DHCP를 사용하여 IPv6 주소를 가져옵니다. DHCPv6 서버가 네트워크에 표시되어야 합니다.
라우터 알림을 통해 자동으로 IPv6 주소 가져오기	라우터 알림을 사용하여 IPv6 주소를 가져옵니다. ESXi 6.5 이상에서는 라우터 알림이 기본적으로 사용되며 RFC 4861에 따라 M 및 O 플래그를 지원합니다.
정적 IPv6 주소	a IPv6 주소 및 서브넷 접두사 길이를 입력합니다. b VMkernel 기본 게이트웨이를 변경하려면 <b>VMkernel 어댑터에 구성</b> 또는 <b>TCP/IP 스택에 구성</b> 을 선택하고 게이트웨이 주소를 입력합니다. IPv6에 대한 VMkernel 기본 게이트웨이 주소는 선택한 TCP/IP 스택에서 가져옵니다.

8 [완료 준비] 페이지에서 선택한 설정을 검토하고 **마침**을 클릭합니다.

## 가상 시스템 네트워킹을 vSphere Distributed Switch로 마이그레이션

Distributed Switch를 사용하여 가상 시스템 네트워킹을 관리하고 스위치에서 레이블이 지정된 네트워크로 가상 시스템 네트워크 어댑터를 마이그레이션하는 방법을 알아봅니다.

### 사전 요구 사항

Distributed Switch에서 가상 시스템 네트워킹에 사용할 분산 포트 그룹이 하나 이상 있는지 확인합니다.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 [작업 선택] 페이지에서 **호스트 네트워킹 관리**를 선택하고 **다음**을 클릭합니다.
- 3 [호스트 선택] 페이지의 **멤버 호스트**에서 Distributed Switch와 연결된 호스트 중에 선택합니다.
- 4 **다음**을 클릭합니다.
- 5 **물리적 어댑터 관리** 페이지에서 업링크를 할당하거나 할당 취소하여 Distributed Switch에 네트워크 어댑터를 추가하거나 제거할 수 있습니다.



6 다음을 클릭합니다.

---

**참고** 호스트에 물리적 네트워크 어댑터가 할당되어 있지 않으면 주의 메시지가 나타납니다.

---

- 7 **VMkernel 어댑터 관리 페이지**에서 Distributed Switch에 VMkernel 어댑터를 추가할 수 있습니다.
- 8 **VM 네트워킹 마이그레이션** 페이지에서 **가상 시스템 네트워킹 마이그레이션** 확인란을 선택하여 가상 시스템을 Distributed Switch로 마이그레이션합니다.
- 9 네트워크 어댑터별로 구성하려면 **포트 그룹 할당**을 클릭합니다.
  - a 포트 그룹을 할당하려면 **할당**을 클릭합니다.  
예를 들어 포트 그룹은 네트워크 어댑터가 동일한 모든 가상 시스템에 할당됩니다.
  - b 포트 그룹을 할당 취소하려면 **할당 취소**를 클릭합니다.
- 10 가상 시스템별로 구성하려면 **포트 그룹 할당**을 클릭합니다.
  - a 포트 그룹을 할당하려면 **할당**을 클릭합니다.
  - b 포트 그룹을 할당 취소하려면 **할당 취소**를 클릭합니다.
- 11 다음을 클릭합니다.
- 12 **호스트 추가 및 관리** 마법사의 **완료 준비** 페이지에서 가상 시스템의 설정을 검토합니다.
- 13 **마침**을 클릭합니다.

## vSphere Distributed Switch에서 호스트 제거

호스트에 대해 다른 스위치를 구성한 경우 vSphere Distributed Switch에서 호스트를 제거하는 방법을 알아봅니다.

### 사전 요구 사항

- 대상 호스트의 물리적 NIC가 다른 스위치로 마이그레이션되었는지 확인합니다.
- 호스트의 VMkernel 어댑터가 다른 스위치로 마이그레이션되었는지 확인합니다.
- 가상 시스템 네트워크 어댑터가 다른 스위치로 마이그레이션되었는지 확인합니다.

네트워크 어댑터를 다른 스위치로 마이그레이션하는 방법에 대한 자세한 내용은 [vSphere Distributed Switch의 호스트 네트워킹 관리 작업](#) 항목을 참조하십시오.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **작업** 메뉴에서 **호스트 추가 및 관리**를 선택합니다.
- 3 작업 선택 페이지에서 **호스트 제거**를 선택하고 **다음**을 클릭합니다.
- 4 Distributed Switch에서 개별 호스트를 제거하려면 해당 호스트를 선택합니다.
- 5 Distributed Switch에서 모든 호스트를 제거하려면 **모두 선택**을 클릭합니다.

6 다음을 클릭합니다.

7 마침을 클릭합니다.

## 호스트 프록시 스위치의 네트워킹 관리

vSphere Distributed Switch와 연결된 모든 호스트에서 프록시 스위치의 구성을 변경하는 방법을 알아봅니다. 물리적 NIC, VMkernel 어댑터 및 가상 시스템 네트워크 어댑터를 관리할 수 있습니다.

호스트 프록시 스위치에서 VMkernel 네트워킹을 설정하는 방법에 대한 자세한 내용은 [vSphere Distributed Switch에서 VMkernel 어댑터 생성](#) 항목을 참조하십시오.

## 호스트의 네트워크 어댑터를 vSphere Distributed Switch로 마이그레이션

Distributed Switch와 연결된 호스트에 대해 표준 스위치에서 Distributed Switch로 네트워크 어댑터를 마이그레이션하는 방법을 알아봅니다. 물리적 NIC, VMkernel 어댑터 및 가상 시스템 네트워크 어댑터를 동시에 마이그레이션할 수 있습니다.

가상 시스템 네트워크 어댑터 또는 VMkernel 어댑터를 마이그레이션하려면 대상 분산 포트 그룹에 하나 이상의 활성 업링크가 있고 이 업링크가 이 호스트의 물리적 NIC에 연결되어 있어야 합니다. 또는 물리적 NIC, 가상 네트워크 어댑터 및 VMkernel 어댑터를 동시에 마이그레이션합니다.

물리적 NIC를 마이그레이션하려면 표준 스위치의 소스 포트 그룹에 해당 트래픽을 처리할 하나 이상의 물리적 NIC가 있어야 합니다. 예를 들어 가상 시스템 네트워킹의 포트 그룹에 할당된 물리적 NIC를 마이그레이션할 경우 이 포트 그룹이 하나 이상의 물리적 NIC에 연결되어 있어야 합니다. 그렇지 않으면 표준 스위치의 동일 VLAN에 있는 가상 시스템이 서로 연결되지만 외부 네트워크에는 연결되지 않습니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **네트워킹**을 확장하고 **가상 스위치**를 선택합니다.
- 3 대상 분산 스위치를 선택하고 **물리적 어댑터 관리** 옆의 가로 줄임표 아이콘을 클릭합니다.
- 4 **네트워킹 마이그레이션**을 선택합니다.
- 5 물리적 NIC를 구성합니다.
  - a **다른 스위치/할당되지 않음** 목록에서 물리적 NIC를 선택하고 **업링크 할당**을 클릭합니다.
  - b 업링크를 선택하고 **확인**을 클릭합니다.
  - c **다음**을 클릭합니다.

- 6 VMkernel 어댑터를 구성합니다.
  - a 어댑터를 선택하고 **포트 그룹 할당**을 클릭합니다.
  - b 분산 포트 그룹을 선택하고 **확인**을 클릭합니다.

한 번에 하나의 VMkernel 어댑터를 하나의 분산 포트 그룹에 연결해야 합니다.
  - c **다음**을 클릭합니다.
- 7 가상 시스템 네트워크 어댑터를 구성합니다.
  - a **가상 시스템 네트워킹 마이그레이션** 확인란을 선택합니다.
  - b 가상 시스템 또는 가상 시스템 네트워크 어댑터를 선택하고 **포트 그룹 할당**을 클릭합니다.

가상 시스템을 선택하는 경우 해당 가상 시스템의 모든 네트워크 어댑터가 마이그레이션되고, 네트워크 어댑터를 선택하는 경우 해당 네트워크 어댑터만 마이그레이션됩니다.
  - c 목록에서 분산 포트 그룹을 선택하고 **확인**을 클릭합니다.
  - d **다음**을 클릭합니다.
- 8 [완료 준비] 페이지에서 새 네트워킹 구성을 검토한 후 **마침**을 클릭합니다.

## 호스트의 VMkernel 어댑터를 vSphere 표준 스위치로 마이그레이션

호스트가 Distributed Switch와 연결된 경우 VMkernel 어댑터를 분산 스위치에서 표준 스위치로 마이그레이션하는 방법을 알아봅니다.

vSphere Distributed Switch에서 VMkernel 어댑터를 생성하는 방법에 대한 자세한 내용은 [vSphere Distributed Switch에서 VMkernel 어댑터 생성](#) 항목을 참조하십시오.

### 사전 요구 사항

대상 표준 스위치에 하나 이상의 물리적 NIC가 있는지 확인합니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 **구성** 탭에서 **네트워킹**을 확장하고 **가상 스위치**를 선택합니다.
- 3 목록에서 대상 표준 스위치를 선택합니다.
- 4 **VMkernel 어댑터 마이그레이션**을 클릭합니다.
- 5 VMkernel 어댑터 선택 페이지의 목록에서 표준 스위치로 마이그레이션할 가상 네트워크 어댑터를 선택합니다.
- 6 [설정 구성] 페이지에서 네트워크 어댑터의 **네트워크 레이블** 및 **VLAN ID**를 편집합니다.
- 7 [완료 준비] 페이지에서 마이그레이션 세부 정보를 검토하고 **마침**을 클릭합니다.

설정을 편집하려면 **뒤로**를 클릭합니다.

## vSphere Distributed Switch에 호스트의 물리적 NIC 할당

Distributed Switch와 연결된 호스트의 물리적 NIC를 호스트 프록시 스위치의 업링크 포트에 할당하는 방법을 알아봅니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **네트워킹**을 확장하고 **가상 스위치**를 선택합니다.
- 3 목록에서 Distributed Switch를 선택합니다.
- 4 **물리적 어댑터 관리**를 클릭합니다.
- 5 목록에서 사용 가능한 빈 업링크를 선택하고 **어댑터 추가**를 클릭합니다.
- 6 물리적 NIC를 선택하고 **확인**을 클릭합니다.

## vSphere Distributed Switch에서 물리적 NIC 제거

vSphere Distributed Switch의 업링크에서 호스트의 물리적 NIC를 제거하는 방법을 알아봅니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **네트워킹**을 확장하고 **가상 스위치**를 선택합니다.
- 3 Distributed Switch를 선택합니다.
- 4 **물리적 어댑터 관리**를 클릭합니다.
- 5 업링크를 선택하고 **선택한 항목 제거**를 클릭합니다.
- 6 **확인**을 클릭합니다.

### 다음에 수행할 작업

활성 가상 시스템에서 물리적 NIC를 제거하면 제거된 NIC가 그대로 보고될 수 있습니다. [활성 가상 시스템에서 NIC 제거](#)의 내용을 참조하십시오.

## 활성 가상 시스템에서 NIC 제거

활성 가상 시스템에서 NIC를 제거하고 제거된 NIC를 vSphere Client에서 확인하는 방법을 알아봅니다.

### 게스트 운영 체제가 설치되지 않은 활성 가상 시스템에서 NIC 제거

운영 체제가 설치되지 않은 활성 가상 시스템에서는 NIC를 제거할 수 없습니다.

vSphere Client에서 NIC가 제거되었다고 보고될 수 있지만 NIC가 가상 시스템에 계속 연결되어 있는 것으로 표시됩니다.

## 게스트 운영 체제가 설치된 활성화 가상 시스템에서 NIC 제거

활성 가상 시스템에서 NIC를 제거할 수 있지만 한동안 vSphere Client에 보고되지 않을 수 있습니다. 가상 시스템의 **설정 편집**을 클릭하면 작업을 완료한 후에도 제거된 NIC가 표시될 수 있습니다. 가상 시스템의 설정 편집 대화상자에 제거된 NIC가 바로 표시되지는 않습니다.

가상 시스템의 게스트 운영 체제에서 NIC에 대해 무중단 제거를 지원하지 않는 경우 가상 시스템에 연결된 NIC를 볼 수도 있습니다.

## 분산 포트 그룹

분산 포트 그룹이 vSphere Distributed Switch의 각 멤버 포트에 대한 포트 구성 옵션을 지정하는 방법을 알아봅니다. 분산 포트 그룹은 네트워크에 대한 연결 방법을 정의합니다.

## 분산 포트 그룹 추가

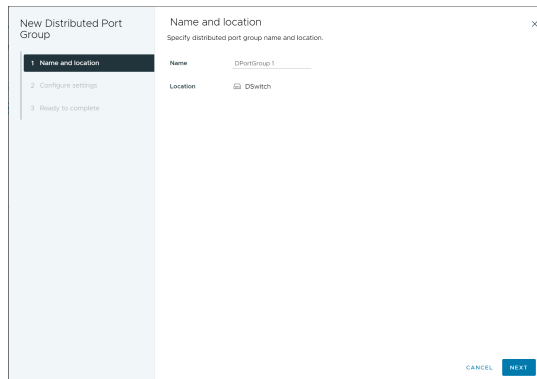
가상 시스템에 대한 Distributed Switch 네트워크를 생성하고, VMkernel 어댑터를 연결하고, 분산 포트 그룹을 vSphere Distributed Switch에 추가하는 방법을 알아봅니다.

포트 그룹 추가와 관련하여 모든 분산 포트에 VLAN 태그 지정을 전역적으로 적용합니다. VLAN 옵션을 사용하여 VLAN 태그를 선택할 수 있습니다. 자세한 내용은 [분산 포트 그룹](#) 또는 [분산 포트에서 VLAN 태그 지정 구성](#)에서 참조하십시오.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 분산 스위치를 마우스 오른쪽 버튼으로 클릭하고 **분산 포트 그룹 > 새 분산 포트 그룹**을 선택합니다.
- 3 이름 및 위치 페이지에서 새 분산 포트 그룹의 이름을 입력하거나 생성된 이름을 그대로 사용하고 **다음**을 클릭합니다.

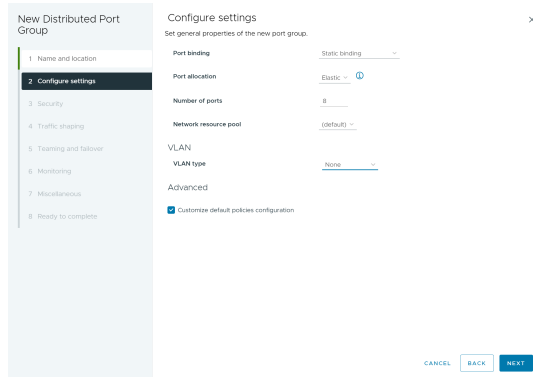
그림 3-5. 새 분산 포트 그룹 - 이름 및 위치



#### 4 설정 구성 페이지에서 새 분산 포트 그룹의 일반 속성을 설정합니다.

설정	설명
포트 바인딩	이 분산 포트 그룹에 연결된 가상 시스템에 할당된 포트를 선택합니다. <ul style="list-style-type: none"> <li>■ <b>정적 바인딩:</b> 가상 시스템이 분산 포트 그룹에 연결할 때 가상 시스템에 포트를 할당합니다.</li> <li>■ <b>사용 후 삭제 - 바인딩 없음:</b> 포트 바인딩이 없습니다. 호스트에 연결할 때에도 사용 후 삭제 포트 바인딩을 사용하여 가상 시스템을 분산 포트 그룹에 할당할 수 있습니다.</li> </ul>
포트 할당	<ul style="list-style-type: none"> <li>■ <b>탄력적:</b> 기본 포트 수는 8개이지만 포트가 모두 할당되면 새로 여덟 개의 포트가 생성됩니다.</li> <li>■ <b>고정:</b> 기본 포트 수가 8개로 설정됩니다. 모든 포트가 할당되면 추가 포트가 생성되지 않습니다.</li> </ul>
포트 수	분산 포트 그룹의 포트 수를 입력합니다.
네트워크 리소스 풀	<p>사용자 정의 네트워크 리소스 풀에 새 분산 포트 그룹을 할당하려면 드롭다운 메뉴를 사용합니다. 네트워크 리소스 풀을 생성하지 않은 경우 이 메뉴는 비어 있습니다.</p> <p><b>참고</b> 네트워크 오프로드를 사용하도록 설정한 경우에는 네트워크 리소스 풀을 할당할 수 없습니다.</p>
VLAN	<p><b>VLAN 유형</b> 드롭다운 메뉴를 사용하여 VLAN 트래픽 필터링 및 표시 유형을 지정합니다.</p> <ul style="list-style-type: none"> <li>■ <b>없음:</b> VLAN을 사용하지 않습니다. External Switch Tagging을 사용하는 경우 <b>없음</b>을 선택합니다.</li> <li>■ <b>VLAN:</b> VLAN ID 텍스트 상자에 Virtual Switch Tagging에 대해 1-4094 사이의 숫자를 입력합니다.</li> <li>■ <b>VLAN 트렁킹:</b> VLAN 트렁킹 범위를 입력합니다.</li> </ul> <p>ID가 있는 VLAN 트래픽을 게스트 운영 체제에 전달합니다. 심표로 구분된 목록을 사용하여 여러 개의 범위와 개별 VLAN을 설정할 수 있습니다. 예: <b>1702-1705, 1848-1849</b></p> <p>VG(TVirtual Guest Tagging)의 경우 이 옵션을 사용합니다.</p> <ul style="list-style-type: none"> <li>■ <b>전용 VLAN:</b> 트래픽을 Distributed Switch에서 생성된 전용 VLAN과 연결합니다. 전용 VLAN을 생성하지 않은 경우에 이 메뉴는 비어 있습니다.</li> </ul>
고급	새 분산 포트 그룹에 대해 정책 구성을 사용자 지정하려면 이 확인란을 선택합니다.

그림 3-6. 새 분산 포트 그룹 - 설정 구성

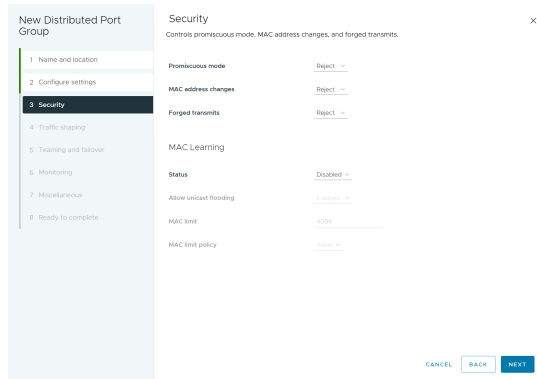


#### 5 다음을 클릭합니다.

6 (선택 사항) [보안] 페이지에서 보안 예외를 편집하고 다음을 클릭합니다.

설정	설명
비규칙(Promiscuous) 모드	<ul style="list-style-type: none"> <li>■ <b>거부:</b> 게스트 운영 체제에서 어댑터를 무차별 모드로 설정하면 다른 가상 시스템의 프레임이 수신되지 않습니다.</li> <li>■ <b>수락:</b> 게스트 운영 체제에서 어댑터를 무차별 모드로 설정하는 경우 어댑터가 연결된 포트에 대한 활성 VLAN 정책에 따라 스위치는 게스트 어댑터가 스위치에 전달된 모든 프레임을 수신하도록 허용합니다.  방화벽, 포트 스캐너, 침입 탐지 시스템 등이 무차별 모드로 실행되어야 합니다.</li> </ul>
MAC 주소 변경	<p>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.</p> <ul style="list-style-type: none"> <li>■ <b>거부:</b> 옵션이 거부로 설정되고 게스트 OS가 어댑터의 MAC 주소를 .vmx 구성 파일에 있는 주소와 다른 값으로 변경하면 스위치가 가상 시스템 어댑터에 대한 모든 inbound 프레임을 삭제합니다.  게스트 OS가 MAC 주소를 원래대로 되돌리면 가상 시스템이 프레임을 다시 수신합니다.</li> <li>■ <b>수락:</b> 게스트 OS가 네트워크 어댑터의 MAC 주소를 변경하는 경우 어댑터는 새 주소에 대한 프레임을 수신합니다.</li> </ul>
위조 전송	<ul style="list-style-type: none"> <li>■ <b>거부:</b> 스위치는 .vmx 구성 파일에 있는 주소와 다른 소스 MAC 주소가 있는 아웃바운드 프레임을 모두 삭제합니다.</li> <li>■ <b>수락:</b> 스위치가 필터링을 수행하지 않고 모든 아웃바운드 프레임을 허용합니다.</li> </ul>

그림 3-7. 새 분산 포트 그룹 - 보안



7 (선택 사항) [보안] 페이지에서 MAC 학습 정책을 편집하고 다음을 클릭합니다.

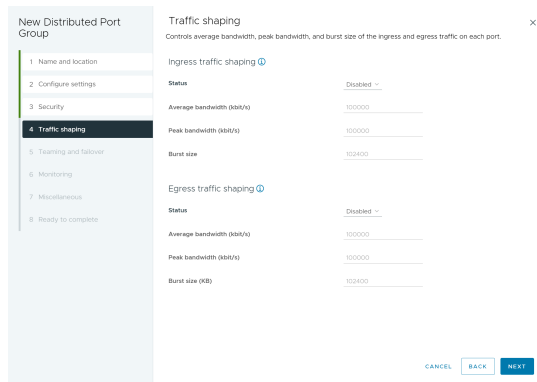
설정	설명
상태	MAC 학습 기능을 사용하거나 사용하지 않도록 설정합니다. 기본값은 사용 안 함입니다.
유니캐스트 플러딩 허용	포트에서 수신한 패킷에 알 수 없는 대상 MAC 주소가 있으면 패킷이 삭제됩니다. 알 수 없는 유니캐스트 플러딩이 사용되도록 설정되면 포트는 MAC 학습 및 알 수 없는 유니캐스트 플러딩이 사용되도록 설정된 스위치의 모든 포트에 알 수 없는 유니캐스트 트래픽을 플러딩합니다. 이 속성은 MAC 학습이 사용되도록 설정된 경우 기본적으로 사용되도록 설정됩니다.

설정	설명
MAC 제한	학습할 수 있는 MAC 주소 수는 구성 가능합니다. 최대값은 포트당 4096(기본값)입니다.
MAC 제한 정책	MAC 제한에 도달한 경우에 대한 정책입니다. 옵션은 다음과 같습니다. <ul style="list-style-type: none"> <li>■ 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.</li> <li>■ 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.</li> </ul>

8 (선택 사항) [트래픽 조절] 페이지에서 수신 또는 송신 트래픽 조절을 사용하거나 사용하지 않도록 설정하고 다음을 클릭합니다.

설정	설명
상태	수신 트래픽 조절 또는 송신 트래픽 조절을 사용하도록 설정하면 이 특정 포트 그룹과 관련된 각 가상 어댑터에 할당되는 네트워크 대역폭 양에 제한이 설정됩니다. 정책을 사용하지 않도록 설정하면 기본적으로 서비스는 물리적 네트워크에 아무런 제한 없이 연결됩니다.  <b>참고</b> [네트워크 오프로드 호환성]을 사용하도록 설정한 경우 트래픽 조절 정책을 할당할 수 없습니다.
평균 대역폭	이 기능은 평균적으로 포트를 통과할 수 있는 초당 비트 수를 설정합니다. 허용되는 평균 로드입니다.
최대 대역폭	트래픽 버스트를 송신/수신할 때 포트를 통과할 수 있는 초당 최대 비트 수입입니다. 포트가 추가 버스트를 사용할 때마다 이 값은 포트에서 사용하는 대역폭보다 커집니다.
버스트 크기	버스트에 허용할 최대 바이트 수입입니다. 이 매개 변수를 설정하면 할당된 대역폭의 일부만 사용될 때 포트가 추가 버스트를 얻을 수 있습니다. 추가 버스트를 사용할 수 있는 경우, <b>평균 대역폭</b> 에 지정한 것보다 더 높은 대역폭이 포트에 필요할 때마다 일시적으로 더 빠른 속도로 데이터를 전송할 수 있습니다. 이 매개 변수는 추가 버스트에 누적될 수 있는 바이트 수의 상한값을 지정하기 때문에 더 빠른 속도로 전송됩니다.

그림 3-8. 새 분산 포트 그룹 - 트래픽 조절



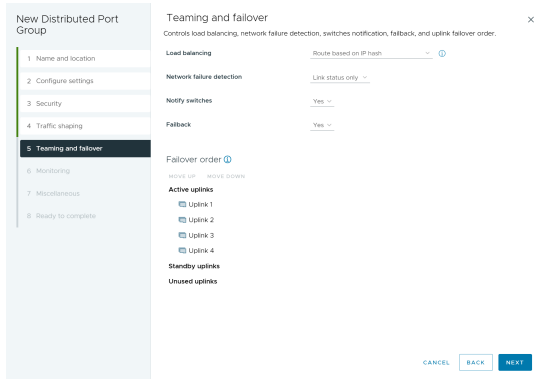


## 9 (선택 사항) [팀 구성 및 페일오버] 페이지에서 설정을 편집하고 다음을 클릭합니다.

설정	설명
로드 밸런싱	<p>업링크가 선택되는 방식을 지정합니다.</p> <ul style="list-style-type: none"> <li>■ <b>원래 가상 포트 기준 라우팅:</b> Distributed Switch의 트래픽 진입 가상 포트를 기반으로 하여 업링크를 선택합니다.</li> <li>■ <b>IP 해시 기준 라우팅:</b> 각 패킷의 소스 및 대상 IP 주소의 해시에 기반하여 업링크를 선택합니다. 비 IP 패킷에 대해서는 오프셋에 있는 어떤 것도 해시를 계산하기 위해 사용 됩니다.</li> <li>■ <b>소스 MAC 해시 기준 라우팅:</b> 소스 이더넷의 해시에 기반하여 업링크를 선택합니다.</li> <li>■ <b>물리적 NIC 로드 기준 라우팅:</b> 물리적 NIC의 현재 로드 에 기반하여 업링크를 선택합니다.</li> <li>■ <b>명시적 페일오버 명령 사용:</b> 페일오버 검색 기준을 통과한 활성 어댑터 목록에서 가장 높은 순서의 업링크를 항상 사용합니다.</li> </ul> <p><b>참고</b> IP 기반 팀 구성을 수행하려면 물리적 스위치가 EtherChannel로 구성되어야 합니다. 다른 모든 옵션의 경우 이더 채널(etherchannel)을 사용하지 않도록 설정합니다.</p>
네트워크 장애 감지	<p>페일오버 감지에 사용하는 방법을 지정합니다.</p> <ul style="list-style-type: none"> <li>■ <b>링크 상태만:</b> 네트워크 어댑터가 제공하는 링크 상태에만 의거합니다. 이 옵션은 케이블 당김, 물리적 스위치 전원 고장과 같은 고장을 감지하지만 스페닝 트리(spanning tree)로 차단되는 물리적 스위치 포트 또는 물리적 스위치의 다른 측면에서 케이블 당김이나 잘못된 VLAN으로의 잘못된 구성과 같은 구성 오류는 감지하지 않습니다.</li> <li>■ <b>비콘 검색 -</b> 팀의 모든 NIC에서 beacon probe을 보내고 수신하여 해당 정보를 연결 상태와 함께 연결 장애를 판단하는 데 사용합니다. 링크 상태만으로 검색할 수 없는 이전에 언급한 많은 장애를 검색합니다.</li> </ul> <p><b>참고</b> 신호 검색을 IP-해시 로드 밸런싱과 함께 사용하지 마십시오.</p>
스위치 알림	<p>페일오버가 발생할 경우의 스위치 알림에 대해 예 또는 아니요를 선택합니다. 예를 선택한 경우, 가상 NIC가 Distributed Switch에 연결될 때마다 또는 가상 NIC의 트래픽이 페일 오버 이벤트로 인해 팀의 다른 물리적 NIC로 라우팅될 때마다 물리적 스위치의 조회 표를 업데이트하기 위해 네트워크 전체에 알림이 전송됩니다. 거의 모든 경우에서 이 프로세스는 페일오버 발생의 가장 낮은 지연 시간 그리고 vMotion으로 마이그레이션하는 데 바람직합니다.</p> <p><b>알림 스위치가 예로</b> 설정된 경우에는 vCenter Server가 ESXi 호스트와 다시 연결될 때 연결된 모든 포트, 포트 그룹 및 Distributed Switch가 호스트에 다시 연결됩니다.</p> <p><b>참고</b> 포트 그룹을 사용하는 가상 시스템이 유니캐스트 모드의 Microsoft 네트워크 로드 밸런싱을 이용할 때에는 이 옵션을 사용하지 않습니다. NLB가 멀티캐스트 모드에서 실행되는 경우에는 이러한 문제가 존재하지 않습니다.</p>

설정	설명
페일백	<p>페일백을 사용하거나 사용하지 않도록 설정하려면 <b>예</b> 또는 <b>아니요</b>를 선택합니다.</p> <p>이 옵션은 물리적 어댑터가 고장을 복구한 후에 어떻게 실행 상태로 돌아가는가를 결정합니다. 페일백을 <b>예</b>(기본값)로 설정한 경우 인계받았던 대기 어댑터(있는 경우)를 대체함으로써 복구 시 어댑터가 즉시 실행 상태로 돌아갑니다. 페일오버가 <b>아니요</b>로 설정된 경우 고장난 어댑터는 복구되어도 현재의 다른 활성 어댑터가 고장나 교체가 필요할 때까지 비활성 상태로 둡니다.</p>
페일오버 순서	<p>업링크로 워크로드를 어떻게 분산하는가를 지정합니다. 일부 업링크만 사용하고 나머지 업링크는 사용 중인 업링크가 고장나는 긴급 상황에 사용할 수 있도록 예약하려면 해당 업링크를 여러 다른 그룹으로 이동하여 이 조건을 설정합니다.</p> <ul style="list-style-type: none"> <li>■ <b>활성 업링크:</b> 네트워크 어댑터 연결이 정상이고 활성일 경우 계속 해당 업링크를 사용합니다.</li> <li>■ <b>대기 업링크:</b> 활성 어댑터 중 하나의 연결을 사용할 수 없는 경우 이 업링크를 사용합니다.</li> <li>■ <b>사용되지 않은 업링크:</b> 이 업링크를 사용하지 않습니다.</li> </ul> <p><b>참고</b> IP-해시 로드 밸런싱을 이용할 때에는 대기 업링크를 구성하지 마십시오.</p>

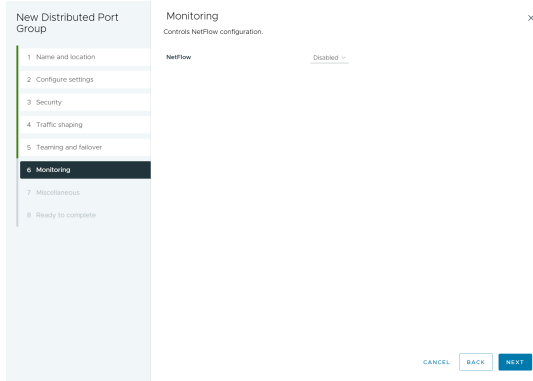
그림 3-9. 새 분산 포트 그룹 - 팀 구성 및 페일오버



10 (선택 사항) [모니터링] 페이지에서 NetFlow를 사용하거나 사용하지 않도록 설정하고 다음을 클릭합니다.

설정	설명
사용 안 함	분산 포트 그룹에서 NetFlow를 사용하지 않습니다.
사용	분산 포트 그룹에서 NetFlow를 사용합니다. NetFlow 설정은 vSphere Distributed Switch 수준에서 구성할 수 있습니다.

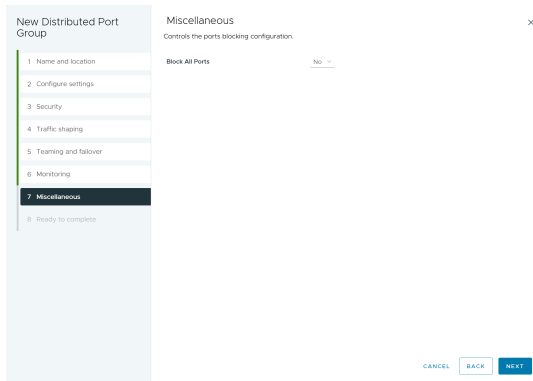
그림 3-10. 새 분산 포트 그룹 - 모니터링



11 (선택 사항) [기타] 페이지에서 **예** 또는 **아니요**를 선택하고 **다음**을 클릭합니다.

**예**를 선택하면 포트 그룹의 모든 포트가 종료됩니다. 이로 인해 해당 포트를 사용하는 호스트 또는 가상 시스템의 정상적인 네트워크 작업이 중단될 수 있습니다.

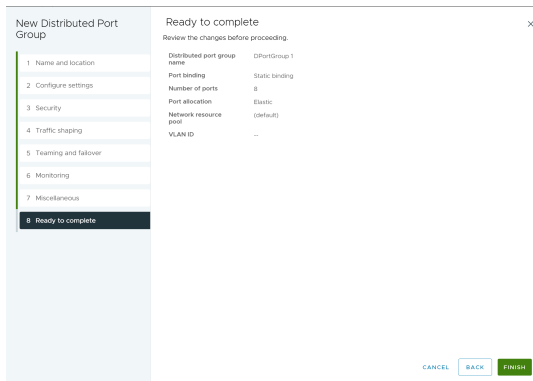
그림 3-11. 새 분산 포트 그룹 - 기타



12 [완료 준비] 페이지에서 설정을 검토하고 **마침**을 클릭합니다.

설정을 변경하려면 **뒤로** 버튼을 클릭합니다.

그림 3-12. 새 분산 포트 그룹 - 완료 준비



## 일반적인 분산 포트 그룹 설정 편집

분산 포트 그룹 이름, 포트 설정 및 네트워크 리소스 풀과 같은 일반 분산 포트 그룹 설정을 편집하는 방법을 알아 봅니다.

### 절차

- 1 vSphere Client에서 분산 포트 그룹을 찾습니다.
  - a Distributed Switch를 선택하고 **네트워크** 탭을 클릭합니다.
  - b **분산 포트 그룹**을 클릭합니다.
- 2 분산 포트 그룹을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 3 **일반**을 선택하여 다음의 분산 포트 그룹 설정을 편집합니다.

옵션	설명
이름	분산 포트 그룹의 이름입니다. 텍스트 필드에서 이름을 편집할 수 있습니다.
포트 바인딩	이 분산 포트 그룹에 연결된 가상 시스템에 포트가 할당되는 시점을 선택합니다. <ul style="list-style-type: none"> <li>■ <b>정적 바인딩</b>: 가상 시스템이 분산 포트 그룹에 연결할 때 가상 시스템에 포트를 할당합니다.</li> <li>■ <b>사용 후 삭제</b>: 포트 바인딩 없음. 호스트에 연결되었을 때 사용 후 삭제 포트 바인딩을 사용하여 가상 시스템을 분산 포트 그룹에 할당할 수도 있습니다.</li> </ul>
포트 할당	<ul style="list-style-type: none"> <li>■ <b>유연하게</b>: 포트의 기본 개수는 8개로 설정됩니다. 포트가 모두 할당되면 새로 여덟 개의 포트가 생성됩니다. 이 옵션이 기본값입니다.</li> <li>■ <b>고정</b>: 기본 포트 수가 8개로 설정됩니다. 포트가 모두 할당되어도 추가 포트가 생성되지 않습니다.</li> </ul>
포트 수	분산 포트 그룹의 포트 수를 입력합니다.
네트워크 리소스 풀	드롭다운 메뉴를 사용하여 사용자 정의 네트워크 리소스 풀에 새 분산 포트 그룹을 할당합니다. 네트워크 리소스 풀을 생성하지 않은 경우 이 메뉴는 비어 있습니다.
설명	분산 포트 그룹에 대한 원하는 정보를 설명 필드에 입력합니다.

- 4 **확인**을 클릭합니다.

## 분산 포트 그룹 제거

가상 시스템 또는 VMkernel 네트워킹에 대해 연결을 제공하고 연결 설정을 구성하기 위한 분산 포트 그룹의 레이블 지정 네트워크가 더 이상 필요하지 않은 경우 해당 분산 포트 그룹을 제거하는 방법을 알아봅니다.

### 사전 요구 사항

- 해당 분산 포트 그룹 레이블의 네트워크에 연결된 모든 가상 시스템이 다른 레이블의 네트워크로 마이그레이션되었는지 확인합니다.
- 해당 분산 포트 그룹에 연결된 모든 VMkernel 어댑터가 다른 포트 그룹으로 마이그레이션되었거나 삭제되었는지 확인합니다.

## 절차

- 1 vSphere Client에서 분산 포트 그룹을 찾습니다.
  - a Distributed Switch를 선택하고 **네트워크** 탭을 클릭합니다.
  - b **분산 포트 그룹**을 클릭합니다.
- 2 분산 포트 그룹을 선택합니다.
- 3 **작업** 메뉴에서 **삭제**를 선택합니다.

## 분산 포트 사용

분산 포트는 VMkernel 또는 가상 시스템의 네트워크 어댑터에 연결되는 vSphere Distributed Switch의 포트입니다.

기본 분산 포트 그룹 구성은 분산 포트 그룹 설정에 따라 결정되며 개별 분산 포트의 일부 설정은 무시될 수 있습니다.

## vSphere Client에서 분산 포트의 상태 모니터링

vSphere 분산 포트를 모니터링하고 각 포트의 현재 상태 및 런타임 통계에 대한 정보를 제공하는 방법을 알아봅니다. vSphere 8.0 업데이트 3부터 모든 포트가 표시되고 포트 목록의 모든 열을 필터링할 수 있습니다.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치를 선택합니다.
- 2 **포트** 탭을 클릭하고 목록에서 포트를 선택합니다.  
모든 포트가 그리드에 표시됩니다.  
분산 스위치에 대한 포트 테이블에는 각 분산 포트에 대한 런타임 통계가 표시됩니다.
- 3 포트 ID별로 포트를 필터링하려면 **포트 ID** 옆에 있는 갈때기 아이콘을 클릭합니다.
- 4 **이름** 옆에 있는 갈때기 아이콘을 클릭하여 포트 이름을 사용하여 포트를 필터링합니다.
- 5 **연결 대상** 열 옆에 있는 갈때기 아이콘을 클릭하여 각 분산 포트의 연결 대상을 기준으로 필터링합니다.

옵션	설명
물리적 어댑터	검색은 연결된 물리적 어댑터를 기반으로 합니다.
VMkernel 어댑터	검색은 연결된 호스트 VmkVnic를 기반으로 합니다.
가상 시스템	검색은 연결된 VM을 기반으로 합니다.
호스트	검색은 연결된 호스트를 기반으로 합니다.
--	이 분산 포트의 연결 대상을 기준으로 한 검색을 현재 사용할 수 없습니다.

- 6 **런타임 MAC 주소** 옆에 있는 갈때기 아이콘을 클릭하여 분산 포트의 MAC 주소로 포트를 필터링합니다.
- 7 **포트 그룹** 옆에 있는 갈때기 아이콘을 클릭하여 포트그룹의 이름을 사용하여 포트를 필터링합니다.

- 8 **상태** 열 옆에 있는 깡때기 아이콘을 클릭하여 각 분산 포트의 업링크 연결을 기준으로 필터링합니다.  
**상태** 열에는 각 분산 포트의 현재 상태가 표시됩니다.

옵션	설명
연결 사용	이 분산 포트의 링크가 사용 중입니다.
연결 해제	이 분산 포트의 링크가 사용 중이 아닙니다.
차단됨	이 분산 포트가 차단되었습니다.
--	이 분산 포트의 상태를 현재 알 수 없습니다.

- 9 **VLAN ID** 열 옆에 있는 깡때기 아이콘을 클릭하여 각 분산 포트의 연결 대상을 기준으로 필터링합니다.

옵션	설명
VLAN	검색 결과는 VLAN ID를 기준으로 합니다.
전용 VLAN	검색 결과는 기본 VLAN ID로 식별되는 전용 VLAN을 기준으로 합니다.
VLAN 트렁크	검색 결과는 VLAN 트렁크 범위 내에서 ID를 가진 VLAN 트래픽을 기준으로 합니다.
--	검색은 이 분산 포트의 VLAN ID를 기준으로 하며, 이는 현재 사용할 수 없습니다.

- 10 가상 인터페이스 식별자별로 포트를 필터링하려면 **VIF ID** 옆의 깡때기 아이콘을 클릭합니다.

## vSphere Client 분산 포트 설정 구성

포트 이름 및 설명과 같은 일반 분산 포트 설정을 구성하는 방법을 알아봅니다.

### 절차

- vSphere Client에서 분산 포트 그룹을 찾습니다.
  - Distributed Switch를 선택하고 **네트워크** 탭을 클릭합니다.
  - 분산 포트 그룹**을 클릭합니다.
- 목록에서 분산 포트 그룹을 클릭합니다.
- 포트** 탭을 클릭하고 테이블에서 분산 포트를 선택합니다.  
 분산 포트에 대한 정보가 화면 아래쪽에 나타납니다.
- 설정 편집** 아이콘을 클릭합니다.
- 속성 페이지와 정책 페이지에서 분산 포트에 대한 정보를 편집하고 **확인**을 클릭합니다.  
 재정의가 허용되지 않는 경우에는 정책 옵션이 사용되지 않도록 설정됩니다.  
 분산 포트 그룹의 **고급** 설정을 변경하여 포트 수준에서 재정의의 허용할 수 있습니다. **포트 수준에서 네트워킹 정책 재정의 구성**의 내용을 참조하십시오.

## vSphere Distributed Switch에 가상 시스템 네트워킹 구성

개별 가상 시스템 NIC를 구성하거나 vSphere Distributed Switch 자체에서 가상 시스템 그룹을 마이그레이션 하여 가상 시스템을 vSphere Distributed Switch에 연결합니다.

연결된 가상 네트워크 어댑터를 분산 포트 그룹에 연결하여 가상 시스템을 vSphere Distributed Switch에 연결합니다. 이 작업은 가상 시스템의 네트워크 구성을 수정하여 개별 가상 시스템에 대해 수행하거나 기존 가상 네트워크에서 vSphere Distributed Switch로 가상 시스템을 마이그레이션하여 가상 시스템 그룹에 대해 수행할 수 있습니다.

### 가상 시스템과 vSphere Distributed Switch 간 마이그레이션

가상 시스템을 개별 가상 시스템 수준에서 Distributed Switch로 연결하는 것 이외에도 가상 시스템 그룹을 vSphere Distributed Switch 네트워크와 vSphere Standard Switch 네트워크 간에 마이그레이션하는 방법을 알아봅니다.

#### 절차

- 1 vSphere Client에서 데이터 센터로 이동합니다.
- 2 탐색기에서 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 **VM을 다른 네트워크로 마이그레이션**을 선택합니다.
- 3 소스 네트워크를 선택합니다.
  - **특정 네트워크**를 선택하고 **찾아보기** 버튼을 사용하여 특정 소스 네트워크를 선택합니다.
  - 어느 네트워크에도 연결되지 않은 모든 가상 시스템 네트워크 어댑터를 마이그레이션하려면 **네트워크 없음**을 선택합니다.
- 4 **찾아보기**를 사용하여 대상 네트워크를 선택하고 **다음**을 클릭합니다.
- 5 소스 네트워크에서 대상 네트워크로 마이그레이션할 가상 시스템을 목록에서 선택하고 **다음**을 클릭합니다.
- 6 선택 사항을 검토하고 **마침**을 클릭합니다.
 

선택 내용을 편집하려면 **뒤로**를 클릭합니다.

### 분산 포트 그룹에 개별 가상 시스템 연결

개별 가상 시스템의 NIC 구성을 수정하여 가상 시스템을 vSphere Distributed Switch에 연결하는 방법을 알아봅니다.

#### 절차

- 1 vSphere Client에서 가상 시스템을 찾습니다.
  - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택하고 **VM** 탭을 클릭합니다.
  - b **가상 시스템**을 클릭하고 목록에서 가상 시스템을 클릭합니다.
- 2 [작업] 메뉴에서 [설정 편집]을 선택합니다.

- 3 **네트워크 어댑터** 섹션을 확장하고 **네트워크 어댑터** 드롭다운 메뉴에서 **찾아보기**를 선택합니다.
- 4 [네트워크 선택] 대화상자에서 분산 포트 그룹을 선택하고 **확인**을 클릭합니다.
- 5 **확인**을 클릭합니다.

## vSphere Distributed Switch 토폴로지

vSphere Client의 vSphere Distributed Switch에 대한 토폴로지 다이어그램에는 스위치에 있는 가상 시스템 어댑터, VMkernel 어댑터 및 물리적 어댑터의 구조가 표시됩니다.

트래픽이 스위치에서 처리되는 구성 요소를 포트 그룹으로 정렬된 상태로 살펴보고 해당 구성 요소 간 연결을 검토할 수 있습니다. 다이어그램에는 가상 어댑터를 외부 네트워크에 연결하는 물리적 어댑터에 대한 정보가 표시됩니다.

전체 Distributed Switch 및 이 스위치에 연결된 각 호스트에서 실행 중인 구성 요소를 볼 수 있습니다.

vSphere Distributed Switch의 토폴로지 다이어그램에서 수행할 수 있는 작업에 대한 비디오를 시청하십시오.



(VDS 토폴로지 다이어그램을 사용하여 가상 네트워킹 처리)

### 중앙 토폴로지 다이어그램

스위치의 중앙 토폴로지 다이어그램을 사용하여 여러 호스트와 연결된 분산 포트 그룹 및 업링크 그룹에 대한 설정을 찾아 편집할 수 있습니다. 포트 그룹의 가상 시스템 어댑터를 동일한 스위치나 다른 스위치로 마이그레이션하는 작업을 시작할 수 있습니다. 또한 **호스트 추가 및 관리** 마법사를 사용하여 스위치에 있는 호스트와 해당 네트워킹을 재구성할 수도 있습니다.

### 호스트 프록시 스위치의 토폴로지 다이어그램

호스트 프록시 스위치의 토폴로지 다이어그램에는 호스트의 스위치 포트에 연결된 어댑터가 표시됩니다. VMkernel 및 물리적 어댑터의 설정을 편집할 수 있습니다.

### 네트워크 오프로드 스위치의 토폴로지 다이어그램

네트워크 오프로드 스위치의 토폴로지 다이어그램에는 호스트의 스위치 포트에 연결된 어댑터가 표시됩니다. VMkernel 및 물리적 어댑터의 설정을 편집할 수 있습니다.

### 다이어그램 필터

다이어그램 필터를 사용하여 토폴로지 다이어그램에 표시되는 정보를 제한할 수 있습니다. 기본 필터는 토폴로지 다이어그램에 포트 그룹과 호스트가 각각 32개, 가상 시스템이 1024개 표시되도록 제한합니다.

필터를 사용하지 않거나 사용자 지정 필터를 적용하여 다이어그램의 범위를 변경할 수 있습니다. 사용자 지정 필터를 사용하여 가상 시스템 집합에 대한 정보만 표시하거나, 특정 호스트의 포트 그룹 집합에 대한 정보만 표시하거나, 포트에 대한 정보만 표시할 수 있습니다. 필터는 Distributed Switch의 중앙 토폴로지 다이어그램에서 생성할 수 있습니다.



## vSphere Distributed Switch의 토폴로지 보기

vCenter Server에서 여러 호스트의 Distributed Switch에 연결된 구성 요소의 구성을 검사합니다.

### 절차

- 1 vSphere Client에서 vSphere Distributed Switch로 이동합니다.
- 2 구성 탭에서 설정을 확장하고 토폴로지를 선택합니다.

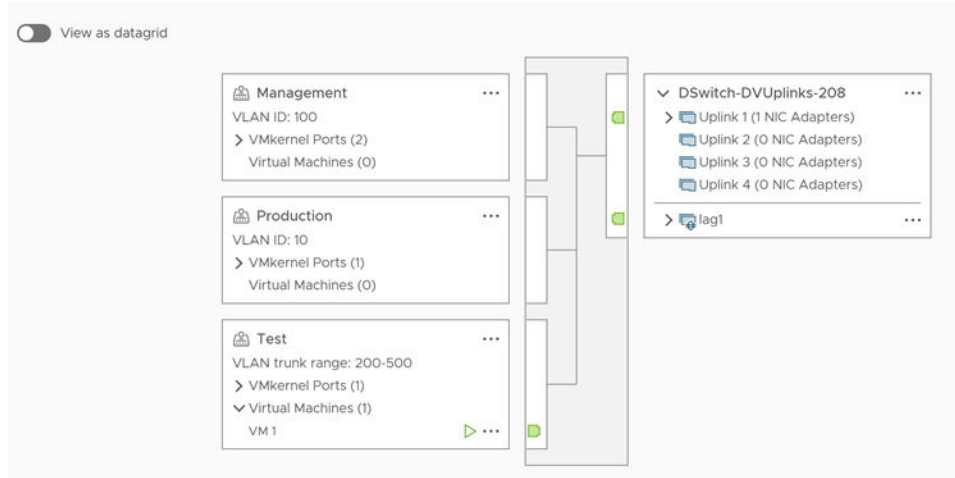
### 결과

기본적으로 다이어그램에는 최대 32개의 분산 포트 그룹, 32개의 호스트 및 1,024개의 가상 시스템이 표시됩니다.

### 예제: VMkernel 및 가상 시스템을 네트워크에 연결하는 Distributed Switch의 다이어그램

가상 환경에서 vSphere Distributed Switch는 vSphere vMotion 및 관리 네트워크에 대한 VMkernel 어댑터와 가상 시스템 그룹을 처리합니다. 중앙 토폴로지 다이어그램을 사용하여 가상 시스템 또는 VMkernel 어댑터가 외부 네트워크에 연결되어 있는지 검사하고 데이터를 전송하는 물리적 어댑터를 식별할 수 있습니다.

그림 3-13. VMkernel 및 가상 시스템 네트워킹을 처리하는 Distributed Switch의 토폴로지 다이어그램



### 다음에 수행할 작업

Distributed Switch의 토폴로지에서 수행할 수 있는 일반적인 작업은 다음과 같습니다.

- 필터를 사용하여 특정 호스트에서 선택한 포트 그룹, 선택한 가상 시스템 또는 포트에 대한 네트워킹 구성 요소만 볼 수 있습니다.
- 가상 시스템 네트워킹 마이그레이션 마법사를 사용하여 호스트 및 포트 그룹 전체에서 가상 시스템 네트워킹 구성 요소를 찾고 구성하고 마이그레이션할 수 있습니다.
- 가상 시스템 네트워킹 마이그레이션 마법사를 통해 네트워크가 할당되지 않은 가상 시스템 어댑터를 검색하여 선택한 포트 그룹으로 이동할 수 있습니다.
- 호스트 추가 및 관리 마법사를 사용하여 여러 호스트의 네트워킹 구성 요소를 처리할 수 있습니다.

- 선택한 가상 시스템 어댑터 또는 VMkernel 어댑터와 관련된 트래픽을 전송하는 물리적 NIC 또는 NIC 팀을 볼 수 있습니다.

이 방법으로 선택한 VMkernel 어댑터가 있는 호스트를 볼 수도 있습니다. 어댑터를 선택하고 연결된 물리적 NIC의 경로를 추적한 후 해당 NIC 옆에 있는 IP 주소나 도메인 이름을 확인합니다.

- 포트 그룹의 VLAN 모드 및 ID를 확인합니다. VLAN 모드에 대한 자세한 내용은 [VLAN 구성](#) 항목을 참조하십시오.

## 호스트 프록시 스위치의 토폴로지 보기

vSphere Distributed Switch가 호스트에서 처리하는 VMkernel 및 가상 시스템의 네트워킹을 검토하고 재구성할 수 있습니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **네트워킹**을 확장하고 **가상 스위치**를 선택합니다.
- 3 목록에서 Distributed Switch를 선택합니다.


### 결과

호스트 프록시 스위치의 토폴로지가 목록에 나타납니다.

## 네트워크 오프로드 스위치의 토폴로지 보기

네트워크 오프로드를 사용하여 Distributed Switch의 조직을 검토합니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **네트워킹**을 확장하고 **가상 스위치**를 선택합니다.
- 3  아이콘은 이 Distributed Switch에 대해 네트워크 오프로드가 지원됨을 나타냅니다.

# VMkernel 네트워킹을 설정하는 방법

# 4

VMkernel 어댑터를 설정하여 호스트에 대한 네트워크 연결을 제공하고 vMotion, IP 스토리지, Fault Tolerance 로깅, vSAN 등의 시스템 트래픽을 수용하는 방법을 알아봅니다.

## ■ VMkernel 네트워킹 계층

VMkernel 네트워킹 계층은 호스트에 대한 연결을 제공하고 vSphere vMotion, IP 스토리지, Fault Tolerance, vSAN 등의 표준 시스템 트래픽을 처리합니다. 소스 및 대상 vSphere Replication 호스트에서 VMkernel 어댑터를 생성하여 복제 데이터 트래픽을 분리할 수도 있습니다.

## ■ vSphere 표준 스위치에서 VMkernel 어댑터 생성

호스트에 대한 네트워크 연결을 제공하고 vSphere vMotion, IP 스토리지, Fault Tolerance 로깅, vSAN 등의 시스템 트래픽을 처리하기 위해 vSphere 표준 스위치에서 VMkernel 네트워크 어댑터를 생성하는 방법을 알아봅니다. 소스 및 대상 vSphere Replication 호스트에서 VMkernel 어댑터를 생성하여 복제 데이터 트래픽을 분리할 수도 있습니다. 한 VMkernel 어댑터를 한 트래픽 유형에만 전용으로 사용해야 합니다.

## ■ vSphere Distributed Switch와 연결된 호스트에서 VMkernel 어댑터 생성

Distributed Switch와 연결된 호스트에서 VMkernel 어댑터를 생성하여 호스트에 네트워크 연결을 제공하고 vSphere vMotion, IP 스토리지, Fault Tolerance 로깅, vSAN 등의 트래픽을 처리하는 방법을 알아봅니다. vSphere 표준 스위치 및 vSphere Distributed Switch에서 표준 시스템 트래픽에 대한 VMkernel 어댑터를 설정할 수 있습니다.

## ■ VMkernel 어댑터 구성 편집

VMkernel 어댑터에 대해 지원되는 트래픽 유형 또는 IPv4 또는 IPv6 주소를 가져오는 방법을 수정하는 방법을 알아봅니다.

## ■ VMkernel 기본 게이트웨이 재정의

vSphere vMotion에 다른 게이트웨이를 제공하기 위해 VMkernel 어댑터의 기본 게이트웨이를 재정의하는 방법을 알아봅니다.

## ■ Esxcli 명령을 사용하여 VMkernel 어댑터 게이트웨이 구성

esxcli 명령을 사용하여 vSphere vMotion에 다른 게이트웨이를 제공할 수 있도록 VMkernel 어댑터의 기본 게이트웨이를 재정의하는 방법을 알아봅니다.

- **esxcli 명령을 사용하여 resolv.conf 파일 구성**

resolv.conf 파일은 중앙에서 관리되는 DNS 서버를 구성하는 데 사용됩니다. esxcli 명령을 사용하여 /etc/resolv.conf 파일의 항목을 구성할 수 있습니다. 그러면 ESXi 호스트를 재부팅할 때 수정 사항이 유지됩니다. DHCP를 사용하도록 설정하지 않은 경우 속성을 명시적으로 설정할 수 있습니다.

- **ESXCLI 명령을 사용하여 DNS 호스트 파일 구성**

DNS 호스트 파일은 호스트 이름 또는 도메인 이름을 IP 주소에 매핑하는 데 사용됩니다. esxcli 명령을 사용하여 /etc/hosts 파일의 항목을 구성할 수 있습니다. 그러면 ESXi 호스트를 재부팅하는 동안 수정 사항이 변경되지 않은 상태로 유지됩니다.

- **호스트의 TCP/IP 스택 구성 보기**

호스트의 TCP/IP 스택에 대한 DNS 및 라우팅 구성을 볼 수 있습니다. 또한 IPv4 및 IPv6 라우팅 테이블, 정체 제어 알고리즘, 허용되는 최대 연결 수를 볼 수도 있습니다.

- **호스트의 TCP/IP 스택 구성 변경**

호스트의 TCP/IP 스택에 대한 DNS 및 기본 게이트웨이 구성을 수정하는 방법을 알아봅니다. 또한 정체 제어 알고리즘, 최대 연결 수 및 사용자 지정 TCP/IP 스택의 이름을 변경할 수도 있습니다.

- **사용자 지정 TCP/IP 스택 생성**

사용자 지정 애플리케이션을 통해 네트워킹 트래픽을 전달할 수 있도록 호스트에서 사용자 지정 TCP/IP 스택을 생성하는 방법을 알아봅니다.

- **VMkernel 어댑터 제거**

VMkernel 어댑터가 더 이상 필요하지 않으면 vSphere Distributed Switch나 vSphere 표준 스위치에서 이 어댑터를 제거하는 방법을 알아봅니다. 네트워크 연결을 유지하기 위해 관리 트래픽용 VMkernel 어댑터 하나 이상을 호스트에 남겨 두어야 합니다.

## VMkernel 네트워킹 계층

VMkernel 네트워킹 계층은 호스트에 대한 연결을 제공하고 vSphere vMotion, IP 스토리지, Fault Tolerance, vSAN 등의 표준 시스템 트래픽을 처리합니다. 소스 및 대상 vSphere Replication 호스트에서 VMkernel 어댑터를 생성하여 복제 데이터 트래픽을 분리할 수도 있습니다.

VMkernel 네트워킹에서 멀티호밍은 TCP/IP 스택에서 여러 VMkernel 어댑터로 정의됩니다.

---

**참고** 여러 TCP/IP 스택이 있는 단일 vmnic가 있는 경우에는 멀티호밍으로 정의할 수 없습니다.

---

멀티호밍은 vmknics가 다른 IP 서브넷에 있는 경우 지원됩니다. 관리자는 경로 항목이 의도를 반영하는지 확인해야 합니다. ESXi는 라우팅 프로토콜을 실행하지 않으며 동적 경로를 지원하거나 추가하지 않습니다. 특정 경로 항목의 경우 vCenter 또는 ESXi 호스트에서 정적으로 추가해야 합니다. 단일 네트워크 스택 인스턴스의 동일한 IP 서브넷에 둘 이상의 vmnic 인터페이스가 있는 구성은 지원되지 않습니다. 이러한 구성을 배포하면 연결 문제, 낮은 처리량 및 비대칭 라우팅과 같은 예기치 않은 결과가 발생할 수 있습니다. 단, 이 규칙에는 몇 가지 예외가 있습니다. 예를 들어 iSCSI, 다중 NIC vMotion 및 NSX VTEPS가 있습니다. 자세한 내용은 <http://kb.vmware.com/kb/2010877>의 내용을 참조하십시오.

## VMkernel 수준의 TCP/IP 스택

### 기본 TCP/IP 스택

vCenter Server 및 ESXi 호스트 간의 관리 트래픽 그리고 vMotion, IP 스토리지, Fault Tolerance 등과 같은 시스템 트래픽에 대한 네트워킹 지원을 제공합니다.

### vMotion TCP/IP 스택

가상 시스템의 실시간 마이그레이션을 위한 트래픽을 지원합니다. vMotion 트래픽에 대한 분리를 향상시키려면 vMotion TCP/IP를 사용하십시오. vMotion TCP/IP 스택에서 VMkernel 어댑터를 생성한 후에는 이 호스트의 vMotion에 대해 이 스택만 사용할 수 있습니다. 기본 TCP/IP 스택의 VMkernel 어댑터는 vMotion 서비스에 대해 사용되지 않도록 설정됩니다. vMotion TCP/IP 스택으로 VMkernel 어댑터를 구성하는 동안 실시간 마이그레이션에서 기본 TCP/IP 스택을 사용하면 마이그레이션이 성공적으로 완료됩니다. 하지만 기본 TCP/IP 스택의 관련된 VMkernel 어댑터는 이후 vMotion 세션에 대해 사용되지 않도록 설정됩니다.

### 프로비저닝 TCP/IP 스택

가상 시스템 콜드 마이그레이션, 복제 및 스냅샷 마이그레이션을 위한 트래픽을 지원합니다. 프로비저닝 TCP/IP를 사용하여 원거리 vMotion 중에 NFC(Network File Copy) 트래픽을 처리할 수 있습니다. NFC는 vSphere를 위한 파일별 FTP 서비스를 제공합니다. ESXi는 데이터스토어 간 데이터 복제 및 이동에 NFC를 사용합니다. 프로비저닝 TCP/IP 스택으로 구성된 VMkernel 어댑터는 원거리 vMotion에서 마이그레이션된 가상 시스템의 가상 디스크 복제에 따른 트래픽을 처리합니다. 프로비저닝 TCP/IP 스택을 사용함으로써 별도의 게이트웨이에서 복제 작업의 트래픽을 분리할 수 있습니다. 프로비저닝 TCP/IP 스택으로 VMkernel 어댑터를 구성한 후에는 기본 TCP/IP 스택의 모든 어댑터가 프로비저닝 트래픽에 대해 사용되지 않도록 설정됩니다.

### 사용자 지정 TCP/IP 스택

VMkernel 수준에서 사용자 지정 TCP/IP 스택을 추가하여 사용자 지정 애플리케이션의 네트워킹 트래픽을 처리할 수 있습니다.

### 미러 TCP/IP 스택

ERSPAN에 대해 미러 스택을 선택할 때 미러 TCP/IP 스택에서 vmknic를 생성할 수 있습니다.

## 시스템 트래픽 보호

vSphere 환경의 관리 및 시스템 트래픽에 대한 무단 액세스를 방지할 수 있도록 적절한 보안 조치를 취하십시오. 예를 들어 vMotion 트래픽을 마이그레이션에 참여하는 ESXi 호스트만 포함하는 별도의 네트워크에 분리합니다. 관리 트래픽을 네트워크 및 보안 관리자만 액세스할 수 있는 네트워크에 분리합니다. 자세한 내용은 "vSphere 보안" 과 "vSphere 설치 및 설정" 을 참조하십시오.

## 시스템 트래픽 유형

모든 트래픽 유형에 대해 별도의 전용 VMkernel 어댑터를 사용해야 합니다. Distributed Switch의 경우 각 VMkernel 어댑터에 대해 별도의 전용 분산 포트 그룹을 사용해야 합니다.

### 관리 트래픽

ESXi 호스트, vCenter Server 및 호스트 간 High Availability 트래픽에 대한 구성 및 관리 통신을 전송합니다. 기본적으로 ESXi 소프트웨어를 설치할 때 vSphere 표준 스위치가 관리 트래픽용 VMkernel 어댑터와 함께 호스트에 생성됩니다. 이중화를 제공하려면 관리 트래픽용 VMkernel 어댑터에 두 개 이상의 물리적 NIC를 연결하면 됩니다.

### vMotion 트래픽

vMotion을 수용합니다. 소스 및 대상 호스트 모두에 vMotion용 VMkernel 어댑터가 필요합니다. vMotion용 VMkernel 어댑터는 vMotion 트래픽만 처리하도록 구성되어야 합니다. 성능 향상을 위해 여러 NIC vMotion을 구성할 수 있습니다. 여러 NIC vMotion을 가지려면 vMotion 트래픽에 두 개 이상의 전용 포트 그룹을 지정할 수 있습니다. 각 포트 그룹에는 그룹에 연결된 vMotion VMkernel 어댑터 하나가 있어야 합니다. 그러면 하나 이상의 물리적 NIC를 각 포트 그룹에 연결할 수 있습니다. 이러한 방법으로 vMotion에 여러 물리적 NIC를 사용하여 대역폭을 넓힐 수 있습니다.

---

**참고** vMotion 네트워크 트래픽이 암호화되어 있지 않습니다. vMotion으로만 사용할 수 있도록 보안 전용 네트워크를 프로비저닝해야 합니다.

---

### 프로비저닝 트래픽

가상 시스템 콜드 마이그레이션, 복제 및 스냅샷 마이그레이션을 위해 전송된 데이터를 처리합니다.

### IP 스토리지 트래픽 및 검색

표준 TCP/IP 네트워크를 사용하고 VMkernel 네트워킹에 종속된 스토리지 유형에 대한 연결을 처리합니다. 이러한 스토리지 유형은 소프트웨어 iSCSI, 종속 하드웨어 iSCSI 및 NFS입니다. iSCSI용 물리적 NIC가 둘 이상 있는 경우 iSCSI 다중 경로 지정을 구성할 수 있습니다. ESXi 호스트는 NFS 3 및 4.1을 지원합니다.

### Fault Tolerance 트래픽

기본 무장애 가상 시스템이 VMkernel 네트워킹 계층을 통해 보조 무장애 가상 시스템에 전송하는 데이터를 처리합니다. vSphere HA 클러스터에 속한 모든 호스트에는 Fault Tolerance 로깅을 위한 별도의 VMkernel 어댑터가 필요합니다.

### vSphere Replication 트래픽

소스 ESXi 호스트에서 vSphere Replication 서버로 전송되는 나가는 복제 데이터를 처리합니다. 나가는 복제 트래픽을 분리하려면 소스 사이트에서 전용 VMkernel 어댑터를 사용하십시오.

### vSphere Replication NFC 트래픽

대상 복제 사이트의 들어오는 복제 데이터를 처리합니다.

### vSAN 트래픽

vSAN 클러스터에 참여하는 모든 호스트에는 vSAN 트래픽을 처리하기 위한 VMkernel 어댑터가 있어야 합니다.

### vSphere 백업 NFC

전용 백업 NFC 트래픽에 대한 VMkernel 포트 설정입니다. vSphere 백업 NFC 서비스를 사용하도록 설정하면 NFC 트래픽이 VMkernel 어댑터를 통과합니다.

### NVMe over TCP

전용 NVMe over TCP 스토리지 트래픽에 대한 VMkernel 포트 설정입니다. NVMe over TCP 어댑터를 사용하도록 설정하면 NVMe over TCP 스토리지 트래픽이 VMkernel 어댑터를 통과합니다. 자세한 내용은 "vSphere 스토리지 가이드" 를 참조하십시오.

### NVMe over RDMA

전용 NVMe over RDMA 스토리지 트래픽에 대한 VMkernel 포트 설정입니다. NVMe over RDMA 어댑터를 사용하도록 설정하면 NVMe over RDMA 스토리지 트래픽이 VMkernel 어댑터를 통과합니다. 자세한 내용은 "vSphere 스토리지 가이드" 를 참조하십시오.

## 호스트에서 VMkernel 어댑터에 대한 정보 보기

각 VMkernel 어댑터에 대해 할당된 서비스, 연결된 스위치, 포트 설정, IP 설정, TCP/IP 스택, VLAN ID 및 정책을 볼 수 있습니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭을 클릭하고 **네트워킹** 메뉴를 확장합니다.
- 3 호스트의 모든 VMkernel 어댑터에 대한 정보를 보려면 **VMkernel 어댑터**를 선택합니다.
- 4 VMkernel 어댑터 목록에서 어댑터의 설정을 보려면 해당 어댑터를 선택합니다.

탭	설명
모두	VMkernel 어댑터에 대한 모든 구성 정보를 표시합니다. 이 정보에는 포트/NIC 설정, IPv4 및 IPv6 설정, 트래픽 조절, 팀 구성 및 페일오버, 보안 정책이 포함됩니다.
속성	VMkernel 어댑터의 포트 속성 및 NIC 설정을 표시합니다. 포트 속성에는 어댑터가 연결된 포트 그룹(네트워크 레이블), VLAN ID 및 사용하도록 설정된 서비스가 포함됩니다. NIC 설정에는 MAC 주소와 구성된 MTU 크기가 포함됩니다.
IP 설정	VMkernel 어댑터에 대한 모든 IPv4 및 IPv6 설정을 표시합니다. 호스트에서 IPv6을 사용하도록 설정하지 않은 경우 IPv6 정보가 표시되지 않습니다.
정책	VMkernel 어댑터가 연결된 포트 그룹에 적용하도록 구성된 트래픽 조절 정책, 팀 구성 및 페일오버 정책과 보안 정책을 표시합니다.

## vSphere 표준 스위치에서 VMkernel 어댑터 생성

호스트에 대한 네트워크 연결을 제공하고 vSphere vMotion, IP 스토리지, Fault Tolerance 로깅, vSAN 등의 시스템 트래픽을 처리하기 위해 vSphere 표준 스위치에서 VMkernel 네트워크 어댑터를 생성하는 방법을 알아

됩니다. 소스 및 대상 vSphere Replication 호스트에서 VMkernel 어댑터를 생성하여 복제 데이터 트래픽을 분리할 수도 있습니다. 한 VMkernel 어댑터를 한 트래픽 유형에만 전용으로 사용해야 합니다.

#### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **네트워킹**을 확장하고 **VMkernel 어댑터**를 선택합니다.
- 3 **네트워킹 추가**를 클릭합니다.
- 4 연결 유형 선택 페이지에서 **VMkernel 네트워크 어댑터**를 선택하고 **다음**을 클릭합니다.
- 5 [대상 디바이스 선택] 페이지에서 기존 표준 스위치를 선택하거나 **새 표준 스위치**를 선택합니다.
- 6 (선택 사항) 표준 스위치 생성 페이지에서 물리적 NIC를 스위치에 할당합니다.

물리적 NIC 없이 표준 스위치를 생성하고 나중에 물리적 NIC를 구성할 수 있습니다. 어떤 물리적 NIC도 호스트에 연결되지 않는 시간 동안 호스트는 물리적 네트워크의 다른 호스트에 대해 네트워크 연결을 가지지 않습니다. 호스트의 가상 시스템은 서로 통신할 수 있습니다.

- a **어댑터 추가**를 클릭하고 물리적 NIC를 필요한 만큼 선택합니다.
  - b 위쪽 및 아래쪽 화살표를 사용하여 활성 및 대기 NIC를 구성합니다.
- 7 포트 속성 페이지에서 VMkernel 어댑터에 대한 설정을 구성합니다.

옵션	설명
네트워크 레이블	네트워크 레이블은 분산 포트 그룹의 레이블에서 상속됩니다.
IP 설정	IPv4, IPv6 또는 둘 모두를 선택합니다. <b>참고</b> IPv6을 사용하도록 설정하지 않은 호스트에는 IPv6 옵션이 표시되지 않습니다.
MTU	스위치에서 네트워크 어댑터에 대한 MTU를 가져올지 또는 사용자 지정 크기를 설정할지 선택합니다. MTU 크기를 9,000바이트보다 큰 값으로 설정할 수 없습니다.



옵션	설명
TCP/IP 스택	<p>목록에서 TCP/IP 스택을 선택합니다. VMkernel 어댑터에 대한 TCP/IP 스택을 설정하고 나면 나중에 변경할 수 없습니다. vMotion 또는 프로비저닝 TCP/IP 스택을 선택하는 경우 이러한 스택만 사용하여 호스트의 vMotion 또는 프로비저닝 스택을 처리할 수 있습니다. 기본 TCP/IP 스택의 vMotion에 대한 모든 VMkernel 어댑터는 이후 vMotion 세션에 대해 비활성화되어 있습니다. 프로비저닝 TCP/IP 스택을 설정하는 경우 기본 TCP/IP 스택의 VMkernel 어댑터가 프로비저닝 트래픽이 포함된 작업(예: 가상 시스템 콜드 마이그레이션, 복제, 스냅샷 마이그레이션)에 대해 비활성화됩니다.</p>
사용 가능한 서비스	<p>호스트의 기본 TCP/IP 스택에 대해 서비스를 사용하도록 설정할 수 있습니다. 사용 가능한 다음 서비스 중에서 선택합니다.</p> <ul style="list-style-type: none"> <li>■ <b>vMotion.</b> VMkernel 어댑터가 자신이 vMotion 트래픽이 전송되는 네트워크 연결 임을 다른 호스트에 알리도록 설정합니다. vMotion을 사용한 선택된 호스트로의 마이그레이션은 vMotion 서비스가 기본 TCP/IP 스택의 VMkernel 어댑터에 대해 사용되도록 설정되어 있지 않거나 vMotion TCP/IP 스택을 사용하는 어댑터가 없는 경우 불가능합니다.</li> <li>■ <b>프로비저닝.</b> 가상 시스템 콜드 마이그레이션, 복제 및 스냅샷 마이그레이션을 위해 전송된 데이터를 처리합니다.</li> <li>■ <b>Fault Tolerance 로깅.</b> 호스트에서 Fault Tolerance 로깅을 사용하도록 설정합니다. 호스트당 FT 트래픽에 대해 하나의 VMkernel 어댑터만 사용할 수 있습니다.</li> <li>■ <b>관리.</b> 호스트 및 vCenter Server에 관리 트래픽을 사용하도록 설정합니다. 일반적으로 호스트에서는 ESXi 소프트웨어가 설치될 때 이러한 VMkernel 어댑터가 생성됩니다. 호스트에서 관리 트래픽용 VMkernel 어댑터를 추가로 생성하여 이중화 기능을 제공할 수 있습니다.</li> <li>■ <b>vSphere Replication.</b> 소스 ESXi 호스트에서 vSphere Replication 서버로 전송된 나가는 복제 데이터를 처리합니다.</li> <li>■ <b>vSphere Replication NFC.</b> 대상 복제 사이트의 들어오는 복제 데이터를 처리합니다.</li> <li>■ <b>vSAN.</b> 호스트에서 vSAN 트래픽이 사용되도록 설정합니다. vSAN 클러스터에 속하는 모든 호스트에는 이러한 VMkernel 어댑터가 있어야 합니다.</li> <li>■ <b>vSphere Backup NFC.</b> 전용 백업 NFC 트래픽에 대한 VMkernel 포트 설정입니다. vSphere 백업 NFC 서비스를 사용하도록 설정하면 NFC 트래픽이 VMkernel 어댑터를 통과합니다.</li> <li>■ <b>NVMe over TCP.</b> 전용 NVMe over TCP 스토리지 트래픽에 대한 VMkernel 포트 설정입니다. NVMe over TCP 어댑터를 사용하도록 설정하면 NVMe over TCP 스토리지 트래픽이 VMkernel 어댑터를 통과합니다. 자세한 내용은 "vSphere 스토리지 가이드" 를 참조하십시오.</li> <li>■ <b>NVMe over RDMA.</b> 전용 NVMe over RDMA 스토리지 트래픽에 대한 VMkernel 포트 설정입니다. NVMe over RDMA 어댑터를 사용하도록 설정하면 NVMe over RDMA 스토리지 트래픽이 VMkernel 어댑터를 통과합니다. 자세한 내용은 "vSphere 스토리지 가이드" 를 참조하십시오.</li> </ul>

8 (선택 사항) IPv4 설정 페이지에서 IP 주소를 가져오는 옵션을 선택합니다.

옵션	설명
자동으로 IPv4 설정 가져오기	DHCP를 사용하여 IP 설정을 가져옵니다. DHCP 서버가 네트워크에 표시되어야 합니다.
정적 IPv4 설정 사용	VMkernel 어댑터의 IPv4 IP 주소와 서브넷 마스크를 입력합니다. IPv4에 대한 VMkernel 기본 게이트웨이와 DNS 서버 주소는 선택한 TCP/IP 스택에서 가져옵니다. VMkernel 어댑터에 대한 다른 게이트웨이를 지정하려는 경우 <b>이 어댑터의 기본 게이트웨이 재정의</b> 의 확인란을 선택하고 게이트웨이 주소를 입력합니다. <a href="#">참고</a> 선택한 Netstack에는 각 호스트에 명시적으로 기본 게이트웨이가 있어야 합니다.

9 (선택 사항) IPv6 설정 페이지에서 IPv6 주소를 가져오는 옵션을 선택합니다.

옵션	설명
DHCP를 통해 자동으로 IPv6 주소 가져오기	DHCP를 사용하여 IPv6 주소를 가져옵니다. DHCPv6 서버가 네트워크에 표시되어야 합니다.
라우터 알림을 통해 자동으로 IPv6 주소 가져오기	라우터 알림을 사용하여 IPv6 주소를 가져옵니다. ESXi 6.5 이상에서는 라우터 알림이 기본적으로 사용되며 RFC 4861에 따라 M 및 O 플래그를 지원합니다.
정적 IPv6 주소	<ul style="list-style-type: none"> <li>a <b>IPv6 주소 추가</b>를 클릭하여 새 IPv6 주소를 추가합니다.</li> <li>b IPv6 주소와 서브넷 접두사 길이를 입력하고 <b>확인</b>을 클릭합니다.</li> <li>c VMkernel 기본 게이트웨이를 변경하려면 <b>이 어댑터의 기본 게이트웨이 재정의</b>를 클릭합니다.</li> </ul> IPv6에 대한 VMkernel 기본 게이트웨이 주소는 선택한 TCP/IP 스택에서 가져옵니다.

10 [완료 준비] 페이지에서 선택한 설정을 검토하고 **마침**을 클릭합니다.

## vSphere Distributed Switch와 연결된 호스트에서 VMkernel 어댑터 생성

Distributed Switch와 연결된 호스트에서 VMkernel 어댑터를 생성하여 호스트에 네트워크 연결을 제공하고 vSphere vMotion, IP 스토리지, Fault Tolerance 로깅, vSAN 등의 트래픽을 처리하는 방법을 알아봅니다. vSphere 표준 스위치 및 vSphere Distributed Switch에서 표준 시스템 트래픽에 대한 VMkernel 어댑터를 설정할 수 있습니다.

VMkernel 어댑터별로 전용 분산 포트 그룹을 하나씩 사용해야 합니다. 분리를 향상시키려면 하나의 트래픽 유형으로 하나의 VMkernel 어댑터를 구성해야 합니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **네트워킹**을 확장하고 **VMkernel 어댑터**를 선택합니다.
- 3 **네트워킹 추가**를 클릭합니다.

- 4 연결 유형 선택 페이지에서 **VMkernel 네트워크 어댑터**를 선택하고 **다음**을 클릭합니다.
- 5 **기존 네트워크 선택** 옵션에서 분산 포트 그룹을 선택하고 **다음**을 클릭합니다.
- 6 포트 속성 페이지에서 VMkernel 어댑터에 대한 설정을 구성합니다.

옵션	설명
네트워크 레이블	네트워크 레이블은 분산 포트 그룹의 레이블에서 상속됩니다.
IP 설정	IPv4, IPv6 또는 둘 모두를 선택합니다. <b>참고</b> IPv6을 사용하도록 설정하지 않은 호스트에는 IPv6 옵션이 표시되지 않습니다.
MTU	스위치에서 네트워크 어댑터에 대한 MTU를 가져올지 또는 사용자 지정 크기를 설정할지 선택합니다. MTU 크기를 9,000바이트보다 큰 값으로 설정할 수 없습니다.

옵션	설명
TCP/IP 스택	<p>목록에서 TCP/IP 스택을 선택합니다. VMkernel 어댑터에 대한 TCP/IP 스택을 설정하고 나면 나중에 변경할 수 없습니다. vMotion 또는 프로비저닝 TCP/IP 스택을 선택하는 경우 이러한 스택만 사용하여 호스트의 vMotion 또는 프로비저닝 스택을 처리할 수 있습니다. 기본 TCP/IP 스택의 vMotion에 대한 모든 VMkernel 어댑터는 이후 vMotion 세션에 대해 비활성화되어 있습니다. 프로비저닝 TCP/IP 스택을 설정하는 경우 기본 TCP/IP 스택의 VMkernel 어댑터가 프로비저닝 트래픽이 포함된 작업(예: 가상 시스템 콜드 마이그레이션, 복제, 스냅샷 마이그레이션)에 대해 비활성화됩니다.</p>
사용 가능한 서비스	<p>호스트의 기본 TCP/IP 스택에 대해 서비스를 사용하도록 설정할 수 있습니다. 사용 가능한 다음 서비스 중에서 선택합니다.</p> <ul style="list-style-type: none"> <li>■ <b>vMotion.</b> VMkernel 어댑터가 자신이 vMotion 트래픽이 전송되는 네트워크 연결 임을 다른 호스트에 알리도록 설정합니다. vMotion을 사용한 선택된 호스트로의 마이그레이션은 vMotion 서비스가 기본 TCP/IP 스택의 VMkernel 어댑터에 대해 사용되도록 설정되어 있지 않거나 vMotion TCP/IP 스택을 사용하는 어댑터가 없는 경우 불가능합니다.</li> <li>■ <b>프로비저닝.</b> 가상 시스템 콜드 마이그레이션, 복제 및 스냅샷 마이그레이션을 위해 전송된 데이터를 처리합니다.</li> <li>■ <b>Fault Tolerance 로깅.</b> 호스트에서 Fault Tolerance 로깅을 사용하도록 설정합니다. 호스트당 FT 트래픽에 대해 하나의 VMkernel 어댑터만 사용할 수 있습니다.</li> <li>■ <b>관리.</b> 호스트 및 vCenter Server에 관리 트래픽을 사용하도록 설정합니다. 일반적으로 호스트에서는 ESXi 소프트웨어가 설치될 때 이러한 VMkernel 어댑터가 생성됩니다. 호스트에서 관리 트래픽용 VMkernel 어댑터를 추가로 생성하여 이중화 기능을 제공할 수 있습니다.</li> <li>■ <b>vSphere Replication.</b> 소스 ESXi 호스트에서 vSphere Replication 서버로 전송된 나가는 복제 데이터를 처리합니다.</li> <li>■ <b>vSphere Replication NFC.</b> 대상 복제 사이트의 들어오는 복제 데이터를 처리합니다.</li> <li>■ <b>vSAN.</b> 호스트에서 vSAN 트래픽이 사용되도록 설정합니다. vSAN 클러스터에 속하는 모든 호스트에는 이러한 VMkernel 어댑터가 있어야 합니다.</li> <li>■ <b>vSphere Backup NFC.</b> 전용 백업 NFC 트래픽에 대한 VMkernel 포트 설정입니다. vSphere 백업 NFC 서비스를 사용하도록 설정하면 NFC 트래픽이 VMkernel 어댑터를 통과합니다.</li> <li>■ <b>NVMe over TCP.</b> 전용 NVMe over TCP 스토리지 트래픽에 대한 VMkernel 포트 설정입니다. NVMe over TCP 어댑터를 사용하도록 설정하면 NVMe over TCP 스토리지 트래픽이 VMkernel 어댑터를 통과합니다. 자세한 내용은 "vSphere 스토리지 가이드" 를 참조하십시오.</li> <li>■ <b>NVMe over RDMA.</b> 전용 NVMe over RDMA 스토리지 트래픽에 대한 VMkernel 포트 설정입니다. NVMe over RDMA 어댑터를 사용하도록 설정하면 NVMe over RDMA 스토리지 트래픽이 VMkernel 어댑터를 통과합니다. 자세한 내용은 "vSphere 스토리지 가이드" 를 참조하십시오.</li> </ul>

- 7 (선택 사항) IPv4 설정 페이지에서 IP 주소를 가져오는 옵션을 선택합니다.

옵션	설명
자동으로 IPv4 설정 가져오기	DHCP를 사용하여 IP 설정을 가져옵니다. DHCP 서버가 네트워크에 표시되어야 합니다.
정적 IPv4 설정 사용	VMkernel 어댑터의 IPv4 IP 주소와 서브넷 마스크를 입력합니다. IPv4에 대한 VMkernel 기본 게이트웨이와 DNS 서버 주소는 선택한 TCP/IP 스택에서 가져옵니다. VMkernel 어댑터에 대한 다른 게이트웨이를 지정하려는 경우 <b>이 어댑터의 기본 게이트웨이 재정의</b> 확인란을 선택하고 게이트웨이 주소를 입력합니다. <a href="#">참고</a> 선택한 Netstack에는 각 호스트에 명시적으로 기본 게이트웨이가 있어야 합니다.

- 8 (선택 사항) IPv6 설정 페이지에서 IPv6 주소를 가져오는 옵션을 선택합니다.

옵션	설명
DHCP를 통해 자동으로 IPv6 주소 가져오기	DHCP를 사용하여 IPv6 주소를 가져옵니다. DHCPv6 서버가 네트워크에 표시되어야 합니다.
라우터 알림을 통해 자동으로 IPv6 주소 가져오기	라우터 알림을 사용하여 IPv6 주소를 가져옵니다. ESXi 6.5 이상에서는 라우터 알림이 기본적으로 사용되며 RFC 4861에 따라 M 및 O 플래그를 지원합니다.
정적 IPv6 주소	<ul style="list-style-type: none"> <li>a <b>IPv6 주소 추가</b>를 클릭하여 새 IPv6 주소를 추가합니다.</li> <li>b IPv6 주소와 서브넷 접두사 길이를 입력하고 <b>확인</b>을 클릭합니다.</li> <li>c VMkernel 기본 게이트웨이를 변경하려면 <b>이 어댑터의 기본 게이트웨이 재정의</b>를 클릭합니다.</li> </ul> IPv6에 대한 VMkernel 기본 게이트웨이 주소는 선택한 TCP/IP 스택에서 가져옵니다.

- 9 [완료 준비] 페이지에서 선택한 설정을 검토하고 **마침**을 클릭합니다.

## VMkernel 어댑터 구성 편집

VMkernel 어댑터에 대해 지원되는 트래픽 유형 또는 IPv4 또는 IPv6 주소를 가져오는 방법을 수정하는 방법을 알아봅니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **네트워킹**을 확장하고 **VMkernel 어댑터**를 선택합니다.
- 3 대상 Distributed Switch 또는 표준 스위치에 있는 VMkernel 어댑터를 선택하고 **편집**을 클릭합니다.

## 4 포트 속성 페이지에서 VMkernel 어댑터에 대한 설정을 편집합니다.

옵션	설명
MTU	스위치에서 네트워크 어댑터에 대한 MTU를 가져올지 또는 사용자 지정 크기를 설정할지 선택합니다. MTU 크기를 9,000바이트보다 큰 값으로 설정할 수 없습니다.
TCP/IP 스택	목록에서 TCP/IP 스택을 선택합니다. VMkernel 어댑터에 대한 TCP/IP 스택을 설정하고 나면 나중에 변경할 수 없습니다. vMotion 또는 프로비저닝 TCP/IP 스택을 선택하는 경우 이러한 스택만 사용하여 호스트의 vMotion 또는 프로비저닝 스택을 처리할 수 있습니다. 기본 TCP/IP 스택의 vMotion에 대한 모든 VMkernel 어댑터는 이후 vMotion 세션에 대해 사용되지 않도록 설정되어 있습니다. 프로비저닝 TCP/IP 스택을 설정하는 경우 기본 TCP/IP 스택의 VMkernel 어댑터가 프로비저닝 트래픽이 포함된 작업(예: 가상 시스템 콜드 마이그레이션, 복제, 스냅샷 마이그레이션)에 대해 사용되지 않도록 설정됩니다.
사용 가능한 서비스	<p>호스트의 기본 TCP/IP 스택에 대해 서비스를 사용하도록 설정할 수 있습니다. 사용 가능한 다음 서비스 중에서 선택합니다.</p> <ul style="list-style-type: none"> <li>■ <b>vMotion.</b> VMkernel 어댑터가 자신이 vMotion 트래픽이 전송되는 네트워크 연결 임을 다른 호스트에 알리도록 설정합니다. vMotion을 사용한 선택된 호스트로의 마이그레이션은 vMotion 서비스가 기본 TCP/IP 스택의 VMkernel 어댑터에 대해 사용되도록 설정되어 있지 않거나 vMotion TCP/IP 스택을 사용하는 어댑터가 없는 경우 불가능합니다.</li> <li>■ <b>프로비저닝.</b> 가상 시스템 콜드 마이그레이션, 복제 및 스냅샷 마이그레이션을 위해 전송된 데이터를 처리합니다.</li> <li>■ <b>Fault Tolerance 로깅.</b> 호스트에서 Fault Tolerance 로깅을 사용하도록 설정합니다. 호스트당 FT 트래픽에 대해 하나의 VMkernel 어댑터만 사용할 수 있습니다.</li> <li>■ <b>관리.</b> 호스트 및 vCenter Server에 관리 트래픽을 사용하도록 설정합니다. 일반적으로 호스트에서는 ESXi 소프트웨어가 설치될 때 이러한 VMkernel 어댑터가 생성됩니다. 호스트에서 관리 트래픽용 VMkernel 어댑터를 추가로 생성하여 이중화 기능을 제공할 수 있습니다.</li> <li>■ <b>vSphere Replication.</b> 소스 ESXi 호스트에서 vSphere Replication 서버로 전송된 나가는 복제 데이터를 처리합니다.</li> <li>■ <b>vSphere Replication NFC.</b> 대상 복제 사이트의 들어오는 복제 데이터를 처리합니다.</li> <li>■ <b>vSAN.</b> 호스트에서 vSAN 트래픽이 사용되도록 설정합니다. vSAN 클러스터에 속하는 모든 호스트에는 이러한 VMkernel 어댑터가 있어야 합니다.</li> <li>■ <b>vSphere Backup NFC.</b> 전용 백업 NFC 트래픽에 대한 VMkernel 포트 설정입니다. vSphere 백업 NFC 서비스를 사용하도록 설정하면 NFC 트래픽이 VMkernel 어댑터를 통과합니다.</li> <li>■ <b>NVMe over TCP.</b> 전용 NVMe over TCP 스토리지 트래픽에 대한 VMkernel 포트 설정입니다. NVMe over TCP 어댑터를 사용하도록 설정하면 NVMe over TCP 스토리지 트래픽이 VMkernel 어댑터를 통과합니다. 자세한 내용은 "vSphere 스토리지 가이드"를 참조하십시오.</li> <li>■ <b>NVMe over RDMA.</b> 전용 NVMe over RDMA 스토리지 트래픽에 대한 VMkernel 포트 설정입니다. NVMe over RDMA 어댑터를 사용하도록 설정하면 NVMe over RDMA 스토리지 트래픽이 VMkernel 어댑터를 통과합니다. 자세한 내용은 "vSphere 스토리지 가이드"를 참조하십시오.</li> </ul>

5 (선택 사항) IPv4 설정 페이지에서 IP 주소를 가져오는 방법을 선택합니다.

옵션	설명
자동으로 IPv4 설정 가져오기	DHCP를 사용하여 IP 설정을 가져옵니다. DHCP 서버가 네트워크에 표시되어야 합니다.
정적 IPv4 설정 사용	VMkernel 어댑터의 IPv4 IP 주소와 서브넷 마스크를 입력합니다. IPv4에 대한 VMkernel 기본 게이트웨이와 DNS 서버 주소는 선택한 TCP/IP 스택에서 가져옵니다. VMkernel 어댑터에 대한 다른 게이트웨이를 지정하려는 경우 <b>이 어댑터의 기본 게이트웨이 재정의</b> 확인란을 선택하고 게이트웨이 주소를 입력합니다.
<b>참고</b> 선택한 Netstack에는 각 호스트에 명시적으로 기본 게이트웨이가 있어야 합니다.	

6 (선택 사항) IPv6 설정 페이지에서 IPv6 주소를 가져오는 옵션을 선택합니다.

**참고** IPv6을 사용하도록 설정하지 않은 호스트에는 IPv6 옵션이 표시되지 않습니다.

옵션	설명
DHCP를 통해 자동으로 IPv6 주소 가져오기	DHCP를 사용하여 IPv6 주소를 가져옵니다. DHCPv6 서버가 네트워크에 표시되어야 합니다.
라우터 알림을 통해 자동으로 IPv6 주소 가져오기	라우터 알림을 사용하여 IPv6 주소를 가져옵니다. ESXi 6.5 이상에서는 라우터 알림이 기본적으로 사용되며 RFC 4861에 따라 M 및 O 플래그를 지원합니다.
정적 IPv6 주소	<ul style="list-style-type: none"> <li>a <b>IPv6 주소 추가</b>를 클릭하여 새 IPv6 주소를 추가합니다.</li> <li>b IPv6 주소와 서브넷 접두사 길이를 입력하고 <b>확인</b>을 클릭합니다.</li> <li>c VMkernel 기본 게이트웨이를 변경하려면 <b>이 어댑터의 기본 게이트웨이 재정의</b>를 클릭합니다.</li> </ul> IPv6에 대한 VMkernel 기본 게이트웨이 주소는 선택한 TCP/IP 스택에서 가져옵니다.

7 **확인**을 클릭합니다.

## VMkernel 기본 게이트웨이 재정의

vSphere vMotion에 다른 게이트웨이를 제공하기 위해 VMkernel 어댑터의 기본 게이트웨이를 재정의하는 방법을 알아봅니다.

호스트의 각 TCP/IP 스택에는 기본 게이트웨이가 하나만 있을 수 있습니다. 이 기본 게이트웨이는 라우팅 테이블의 일부로서 TCP/IP 스택에서 작동하는 모든 서비스는 이 게이트웨이를 사용합니다.

예를 들어 VMkernel 어댑터 vmk0 및 vmk1을 호스트에 구성할 수 있습니다.

- vmk0은 기본 게이트웨이가 10.162.10.1인 10.162.10.0/24 서브넷의 관리 트래픽에 사용됩니다.
- vmk1은 172.16.1.0/24 서브넷의 vMotion 트래픽에 사용됩니다.

172.16.1.1을 vmk1의 기본 게이트웨이로 설정하는 경우 vMotion이 게이트웨이가 172.16.1.1인 송신 인터페이스로 vmk1을 사용합니다. 172.16.1.1 게이트웨이는 vmk1 구성의 일부이며 라우팅 테이블에 포함되지 않습니다. vmk1을 송신 인터페이스로 지정하는 서비스만 이 게이트웨이를 사용합니다. 이를 통해 여러 게이트웨이가 필요한 서비스에 추가 Layer 3 연결 옵션이 제공됩니다.

vSphere Client 또는 ESXCLI 명령을 사용하여 VMkernel 어댑터의 기본 게이트웨이를 구성할 수 있습니다.

vSphere 표준 스위치에서 VMkernel 어댑터 생성, vSphere Distributed Switch와 연결된 호스트에서 VMkernel 어댑터 생성 및 Esxcli 명령을 사용하여 VMkernel 어댑터 게이트웨이 구성 항목을 참조하십시오.

## Esxcli 명령을 사용하여 VMkernel 어댑터 게이트웨이 구성

esxcli 명령을 사용하여 vSphere vMotion에 다른 게이트웨이를 제공할 수 있도록 VMkernel 어댑터의 기본 게이트웨이를 재정의하는 방법을 알아봅니다.

### 절차

- 1 호스트에 대한 SSH 연결을 엽니다.
- 2 루트 사용자로 로그인합니다.
- 3 다음 명령을 실행합니다.

옵션	설명
IPv4	<pre>esxcli network ip interface ipv4 set -i vmknic -t static -g IPv4 gateway -I IPv4 address -N mask</pre>
IPv6	<p><b>중요</b> IPv6 vmknic 게이트웨이를 설정하기 전에 DHCPv6 또는 라우터 알림을 해제해야 합니다.</p> <pre>esxcli network ip interface ipv6 set -i vmknic -d off -r off</pre> <p>정적 IPv6 주소를 추가하려면 다음을 수행합니다.</p> <pre>esxcli network ip interface ipv6 address add -i vmknic -I IPv6 address</pre> <p>IPv6 vmknic 게이트웨이를 설정하려면 다음을 수행합니다.</p> <pre>esxcli network ip interface ipv6 set -i vmknic -g IPv6 gateway</pre>

여기서 *vmknic*는 VMkernel 어댑터의 이름이고, *gateway*는 게이트웨이의 IP 주소이고, *IP address*는 VMkernel 어댑터의 주소이고, *mask*는 네트워크 마스크입니다.



## esxcli 명령을 사용하여 resolv.conf 파일 구성

resolv.conf 파일은 중앙에서 관리되는 DNS 서버를 구성하는 데 사용됩니다. esxcli 명령을 사용하여 /etc/resolv.conf 파일의 항목을 구성할 수 있습니다. 그러면 ESXi 호스트를 재부팅할 때 수정 사항이 유지됩니다. DHCP를 사용하도록 설정하지 않은 경우 속성을 명시적으로 설정할 수 있습니다.

### 절차

- 1 호스트에 대한 SSH 연결을 엽니다.
- 2 루트 사용자로 로그인합니다.
- 3 다음 명령을 실행합니다.

옵션	설명
DNS 서버 추가	<p>이 ESXi 호스트에 사용할 DNS 서버 목록의 끝에 새 DNS 서버를 추가하려면 다음을 실행합니다.</p> <pre>esxcli network ip dns server add</pre> <p>명령 옵션</p> <pre>-N --netstack=&lt;str&gt;</pre> <p>네트워크 스택 인스턴스. 지정되어 있지 않으면 기본 Netstack 인스턴스가 사용됩니다.</p> <pre>-s --server=&lt;str&gt;</pre> <p>DNS 서버 목록에 추가하려는 DNS 서버의 IPV4 또는 IPV6 주소입니다.</p> <p><b>참고</b> 이 명령은 필수입니다.</p> <pre>For example: esxcli network ip dns server add -N vmotion -s xx.xx.xx.xx</pre>
DNS 검색 추가	<p>ESXi 호스트에서 호스트 이름을 확인하려고 할 때 검색할 도메인 목록에 검색 도메인을 추가하려면 다음을 실행합니다.</p> <pre>esxcli network ip dns search add</pre> <p>명령 옵션</p> <pre>-d --domain=&lt;str&gt;</pre> <p>검색 도메인 목록에 추가하려는 도메인의 문자열 이름입니다.</p> <p><b>참고</b> 이 명령은 필수입니다.</p> <pre>-N --netstack=&lt;str&gt;</pre> <p>네트워크 스택 인스턴스. 지정되어 있지 않으면 기본 Netstack 인스턴스가 사용됩니다.</p>

옵션	설명
DNS 서버 제거	<p>이 ESXi 호스트에 사용할 DNS 서버 목록에서 DNS 서버를 제거하려면 다음을 실행합니다.</p> <pre>esxcli network ip dns server remove IP address</pre> <p>명령 옵션</p> <pre>-a --all</pre> <pre>-N --netstack=&lt;str&gt;</pre> <p>네트워크 스택 인스턴스. 지정되어 있지 않으면 기본 Netstack 인스턴스가 사용됩니다.</p> <pre>-s --server=&lt;str&gt;</pre>
DNS 검색 제거	<p>ESXi 호스트에서 호스트 이름을 확인하려고 할 때 검색할 도메인 목록에서 검색 도메인을 제거하려면 다음을 실행합니다.</p> <pre>esxcli network ip dns search remove</pre> <p>명령 옵션</p> <pre>-d --domain=&lt;str&gt;</pre> <p>검색 도메인 목록에서 제거하려는 도메인의 문자열 이름입니다.</p> <p><b>참고</b> 이 명령은 필수입니다.</p> <pre>-N --netstack=&lt;str&gt;</pre> <p>네트워크 스택 인스턴스. 지정되어 있지 않으면 기본 Netstack 인스턴스가 사용됩니다.</p>
DNS 검색 나열	<p>시스템에 현재 구성되어 있는 DNS 서버 목록을 사용할 순서대로 출력하려면 다음을 실행합니다.</p> <pre>esxcli network ip dns server list</pre> <p>명령 옵션</p> <pre>-N --netstack=&lt;str&gt;</pre> <p>네트워크 스택 인스턴스. 지정되어 있지 않으면 기본 Netstack 인스턴스가 사용됩니다.</p> <pre>For example: esxcli network ip dns server list -N vmotion</pre>
DNS 검색 도메인 나열	<p>ESXi 호스트에 현재 구성되어 있는 검색 도메인을 검색하는 동안 사용될 순서대로 나열하려면 다음을 실행합니다.</p> <pre>esxcli network ip dns search list -N</pre> <p>명령 옵션</p> <pre>---N --netstack=&lt;str&gt;</pre> <p>네트워크 스택 인스턴스. 지정되어 있지 않으면 기본 Netstack 인스턴스가 사용됩니다.</p> <pre>For example: esxcli network ip dns search list -N vmotion</pre>

## ESXCLI 명령을 사용하여 DNS 호스트 파일 구성

DNS 호스트 파일은 호스트 이름 또는 도메인 이름을 IP 주소에 매핑하는 데 사용됩니다. `esxcli` 명령을 사용하여 `/etc/hosts` 파일의 항목을 구성할 수 있습니다. 그러면 ESXi 호스트를 재부팅하는 동안 수정 사항이 변경되지 않은 상태로 유지됩니다.

### 절차

- 1 호스트에 대한 SSH 연결을 엽니다.
- 2 루트 사용자로 로그인합니다.
- 3 다음 명령을 실행합니다.

옵션	설명
추가	<p>호스트 이름 및 IP 주소 매핑을 추가하려면 다음 명령을 실행합니다.</p> <pre>esxcli network ip hosts add --ip --hostname</pre> <p>For example: <code>esxcli network ip hosts add --hostname www.samplehostname.com --ip xx.xx.xx.xx</code></p>
제거	<p>구성에서 호스트 이름 매핑을 제거하려면 다음 명령을 실행합니다.</p> <pre>esxcli network ip hosts remove --hostname</pre> <p>For example: <code>esxcli network ip hosts remove --hostname www.samplehostname.com --ip xx.xx.xx.xx</code></p>
목록	<p>IP 주소 및 연결된 DNS 항목을 나열하려면 다음 명령을 실행합니다.</p> <pre>esxcli network ip hosts list</pre>

여기서 *IP address*는 VMkernel 어댑터의 주소이고, *hostname*은 IP 주소와 연결하려는 DNS 항목이고, *aliases*는 연결하려는 모든 별칭이고, *comment*는 이 항목에 대한 줄입니다.

**참고** ESXCLI 네트워크 IP 호스트는 다른 호스트에만 값을 추가합니다. ESXCLI 네트워크 IP 호스트는 현재 호스트에 값을 추가하지 않습니다. 현재 호스트에 대한 정보는 **네트워크 설정** 아래의 호스트 이름을 통해 관리됩니다. 현재 호스트 이름을 변경하려고 하면 다음과 유사한 오류가 표시될 수 있습니다.

```
Error adding etc host item: User can not set item for management IP: X.X.X.X
```

현재 호스트의 호스트 이름을 변경하는 방법에 대한 자세한 내용은 **호스트의 TCP/IP 스택 구성 변경 항목**을 참조하십시오.

## 호스트의 TCP/IP 스택 구성 보기

호스트의 TCP/IP 스택에 대한 DNS 및 라우팅 구성을 볼 수 있습니다. 또한 IPv4 및 IPv6 라우팅 테이블, 정체 제어 알고리즘, 허용되는 최대 연결 수를 볼 수도 있습니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **네트워킹**을 확장하고 **TCP/IP 구성**을 선택합니다.
- 3 TCP/IP 스택 테이블에서 스택을 선택합니다.

호스트에 구성된 사용자 지정 TCP/IP 스택이 없을 경우 호스트의 기본 TCP/IP 스택, vMotion TCP/IP 스택 및 프로비저닝 TCP/IP 스택이 표시됩니다.

### 결과

선택한 TCP/IP 스택에 대한 DNS 및 라우팅 세부 정보는 TCP/IP 스택 테이블 아래에 나타납니다. IPv4 및 IPv6 라우팅 테이블과 스택의 DNS 및 라우팅 구성을 볼 수 있습니다.

---

**참고** IPv6 라우팅 테이블은 호스트에 IPv6를 사용하도록 설정된 경우에만 표시됩니다.

---

**고급** 탭에는 구성된 정체 제어 알고리즘 및 스택에 허용되는 최대 연결 수에 대한 정보가 표시됩니다.

## 호스트의 TCP/IP 스택 구성 변경

호스트의 TCP/IP 스택에 대한 DNS 및 기본 게이트웨이 구성을 수정하는 방법을 알아봅니다. 또한 정체 제어 알고리즘, 최대 연결 수 및 사용자 지정 TCP/IP 스택의 이름을 변경할 수도 있습니다.

---

**참고** 기본 TCP/IP 스택의 DNS 및 기본 게이트웨이 구성만 변경할 수 있습니다. 별도의 TCP/IP 스택을 사용하는 경우 여러 DNS 및 게이트웨이 구성이 지원됩니다.

---

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **네트워킹**을 확장하고 **TCP/IP 구성**을 선택합니다.

### 3 테이블에서 스택을 선택하고 편집을 클릭한 다음 필요한 내용을 변경합니다.

페이지	옵션
DNS 구성	DNS 서버를 가져오는 방법을 선택합니다. <ul style="list-style-type: none"> <li>■ 하나의 VMkernel 네트워크 어댑터에서 자동으로 설정 가져오기를 선택하고 VMKernel 네트워크 어댑터 드롭다운 메뉴에서 네트워크 어댑터를 선택합니다.</li> <li>■ 수동으로 설정 입력을 선택하고 DNS 구성 설정을 편집합니다.               <ol style="list-style-type: none"> <li>a 호스트 이름을 편집합니다.</li> <li>b 도메인 이름을 편집합니다.</li> <li>c 기본 설정 DNS 서버 IP 주소를 입력합니다.</li> <li>d 대체 DNS 서버 IP 주소를 입력합니다.</li> <li>e (선택 사항) 도메인 검색 텍스트 상자를 사용하여 정규화되지 않은 도메인 이름을 해결할 때 DNS 검색에서 사용할 DNS 접미사를 지정합니다.</li> </ol> </li> </ul>
라우팅	VMkernel 게이트웨이 정보를 편집합니다. <p><b>참고</b> 기본 게이트웨이를 제거하면 클라이언트에서 호스트와의 연결이 끊어질 수 있습니다.</p>
이름	사용자 지정 TCP/IP 스택의 이름을 변경합니다.
고급	스택의 정체 제어 알고리즘과 최대 연결 수를 편집합니다.

### 4 확인을 클릭하여 변경 내용을 적용합니다.

#### 다음에 수행할 작업

CLI 명령을 사용하여 추가 게이트웨이에 정적 경로를 추가할 수 있습니다. 자세한 내용은 <http://kb.vmware.com/kb/2001426>을 참조하십시오.

## 명시적 정체 알림

ECN(명시적 정체 알림)을 사용하면 TCP 발신자가 패킷 손실을 방지하기 위해 전송 속도를 줄일 수 있습니다. ECN은 RFC 3168에 상술되어 있습니다. vSphere 7.0 이상은 ECN을 지원하며 기본적으로 사용하도록 설정됩니다.

esxcli 명령을 사용하여 모든 Netstack의 ECN 상태를 가져올 수 있습니다.

#### 절차

- 1 호스트의 ESXi Shell에서 다음 명령을 사용합니다.

```
esxcli network ip netstack set -N <NetStack-Name> --ecn=<str>
```

- 2 ECN의 상태를 설정할 수 있습니다. 이 설정은 ESXi에서 다음과 같은 값을 가질 수 있습니다.

```
... --ecn=<str> ECN(명시적 정체 알림)의 상태. disabled: ECN 기능을 완전히 사용 안 함으로 설정, echo-only: ECN만 예고하고 시작하지 않음, enabled: ECN 기능을 완전히 사용하도록 설정
```

이 매개 변수의 기본값은 enabled입니다. ESXi는 이 매개 변수의 값이 enabled인 경우 ECN을 사용할 가능성이 높습니다. 환경의 라우터 또는 네트워크 장치가 ECN 비트가 포함된 IP 패킷을 정확하게 처리할 수 없는 경우에는 ECN 기능을 disabled로 설정할 수 있습니다.

## 사용자 지정 TCP/IP 스택 생성

사용자 지정 애플리케이션을 통해 네트워킹 트래픽을 전달할 수 있도록 호스트에서 사용자 지정 TCP/IP 스택을 생성하는 방법을 알아봅니다.

VMkernel 어댑터에 대한 TCP/IP 스택을 설정하고 나면 나중에 변경할 수 없습니다. vMotion 또는 프로비저닝 TCP/IP 스택을 선택하는 경우 이러한 스택만 사용하여 호스트의 vMotion 또는 프로비저닝 트래픽을 처리할 수 있습니다. 기본 TCP/IP 스택의 vMotion에 대한 모든 VMkernel 어댑터는 이후 vMotion 세션에 대해 사용되지 않도록 설정되어 있습니다. 프로비저닝 TCP/IP 스택을 설정하는 경우 기본 TCP/IP 스택의 VMkernel 어댑터가 프로비저닝 트래픽이 포함된 작업(예: 가상 시스템 콜드 마이그레이션, 복제, 스냅샷 마이그레이션)에 대해 사용되지 않도록 설정됩니다.

TCP/IP 스택 구성을 변경해야 하는 경우 기존 VMkernel 어댑터를 삭제하고 새 어댑터를 만듭니다. 그런 다음, 해당 어댑터에 대한 TCP/IP 스택을 생성할 수 있습니다.

### 절차

- 1 호스트에 대한 SSH 연결을 엽니다.
- 2 루트 사용자로 로그인합니다.
- 3 ESXCLI 명령을 실행합니다.

```
esxcli network ip netstack add -N="stack_name"
```

### 결과

호스트에서 사용자 지정 TCP/IP 스택이 생성되었습니다. 이 스택에 VMkernel 어댑터를 할당할 수 있습니다.

## VMkernel 어댑터 제거

VMkernel 어댑터가 더 이상 필요하지 않으면 vSphere Distributed Switch나 vSphere 표준 스위치에서 이 어댑터를 제거하는 방법을 알아봅니다. 네트워크 연결을 유지하기 위해 관리 트래픽용 VMkernel 어댑터 하나 이상을 호스트에 남겨 두어야 합니다.

### 절차

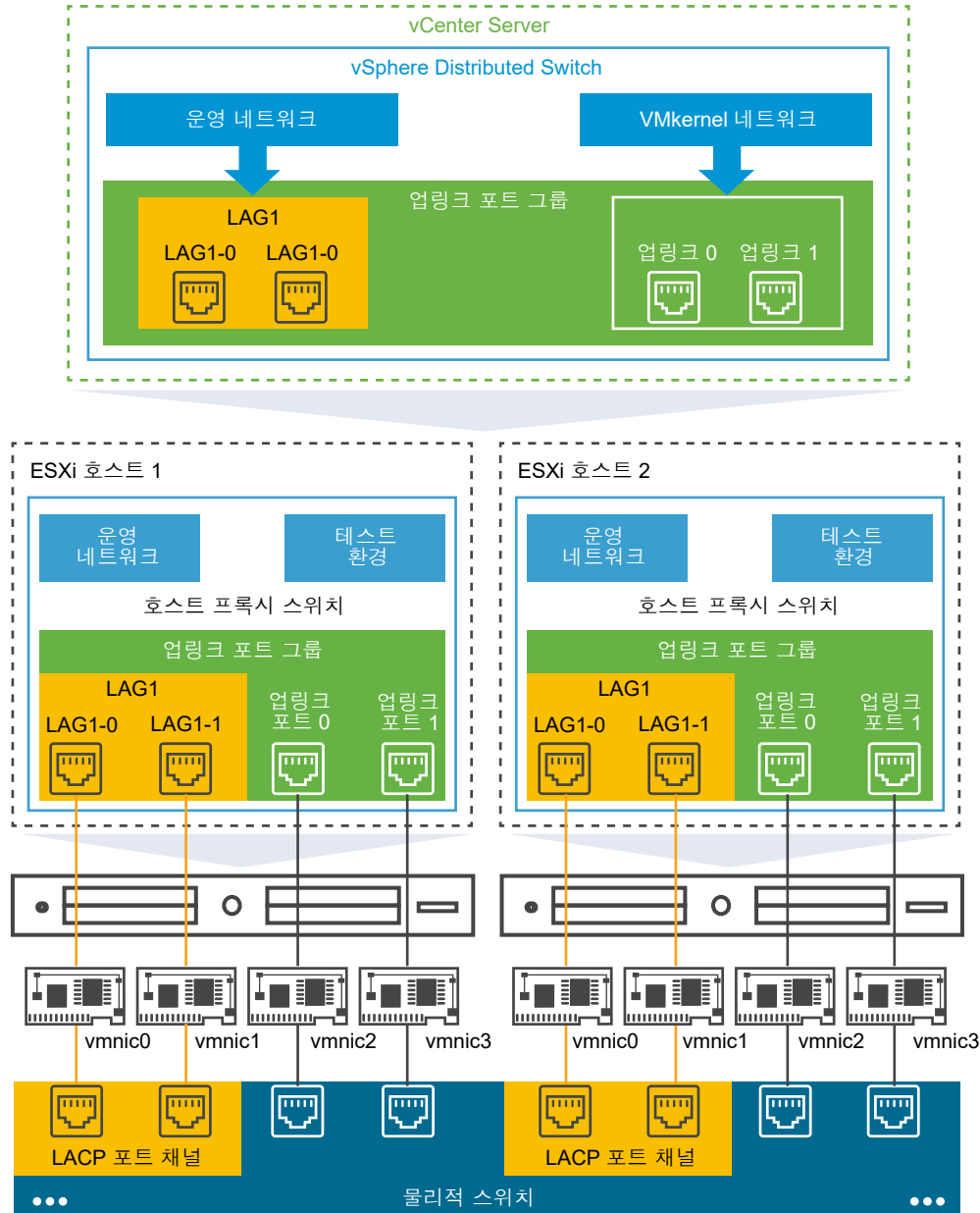
- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 네트워킹을 확장하고 VMkernel 어댑터를 선택합니다.
- 3 목록에서 VMkernel 어댑터를 선택하고 선택된 네트워크 어댑터 제거 아이콘을 클릭합니다.
- 4 제거를 클릭합니다.

# vSphere Distributed Switch의 LACP 지원

# 5

vSphere Distributed Switch에서 LACP(Link Aggregation Control Protocol) 지원 기능을 사용하면 동적 링크 집계를 통해 ESXi 호스트를 물리적 스위치에 연결할 수 있습니다. Distributed Switch에 여러 LAG(링크 집계 그룹)를 생성하여 LACP 포트 채널에 연결된 ESXi 호스트에서 물리적 NIC의 대역폭을 집계할 수 있습니다.

그림 5-1. vSphere Distributed Switch의 향상된 LACP 지원



## Distributed Switch의 LACP 구성

두 개 이상의 포트가 있는 LAG를 구성하고 물리적 NIC를 포트에 연결합니다. LAG 포트는 LAG 내에서 팀으로 구성되며, 네트워크 트래픽은 LACP 해싱 알고리즘을 통해 포트 간에 로드 밸런싱됩니다. 하나의 LAG로 분산 포트 그룹의 트래픽을 처리하여 네트워크 대역폭, 이중화 및 포트 그룹으로의 로드 밸런싱을 향상시킬 수 있습니다.

Distributed Switch에서 LAG를 생성하면 Distributed Switch에 연결된 모든 호스트의 프록시 스위치에서 LAG 개체도 생성됩니다. 예를 들어 포트가 두 개 있는 LAG1을 생성하면 Distributed Switch에 연결된 모든 호스트에 같은 포트 수의 LAG1이 생성됩니다.



호스트 프록시 스위치에서는 한 물리적 NIC를 한 LAG 포트에만 연결할 수 있습니다. Distributed Switch에서는 한 LAG 포트에 여러 호스트의 여러 물리적 NIC가 연결될 수 있습니다. LAG 포트에 연결하는 호스트의 물리적 NIC는 물리적 스위치에서 LACP 포트 채널에 속한 링크에 연결되어야 합니다.

Distributed Switch에서 최대 64개의 LAG를 생성할 수 있습니다. 호스트는 최대 32개의 LAG를 지원할 수 있습니다. 하지만 실제로 사용할 수 있는 LAG 수는 기본 물리적 환경의 기능과 가상 네트워크의 토폴로지에 따라 다릅니다. 예를 들어 물리적 스위치가 LACP 포트 채널에서 최대 네 개의 포트를 지원하는 경우 호스트당 최대 네 개의 물리적 NIC를 LAG에 연결할 수 있습니다.

LACP 시간 초과 값을 구성할 수 있습니다. LACP는 프로토콜이 사용되도록 설정된 모든 링크로 프레임을 전송하여 작동합니다. 링크의 다른 쪽 끝에서 역시 LACP를 사용하도록 설정된 디바이스를 찾으면 동일한 링크를 따라 독립적으로 프레임을 전송하여 두 장치가 서로 간에 여러 링크를 감지한 다음 단일 논리적 링크로 결합할 수 있습니다. 시간 초과 값은 LACP 세션이 종료되기까지 LAG 인터페이스가 원격 시스템의 PDU(Protocol Data Unit)를 대기하는 시간입니다. LACP PDU의 주기적 전송은 느리거나 빠른 전송 속도로 발생합니다.

## 물리적 스위치에서 포트 채널 구성

LACP를 사용할 각 호스트에 대해 물리적 스위치에서 별도의 LACP 포트 채널을 생성해야 합니다. 물리적 스위치에서 LACP를 구성할 때에는 다음 요구 사항을 고려해야 합니다.

- LACP 포트 채널의 포트 수는 호스트에서 그룹화하려는 물리적 NIC의 수와 같아야 합니다. 예를 들어 호스트에서 물리적 NIC 두 개의 대역폭을 집계하려는 경우 물리적 스위치에서 두 개의 포트가 있는 LACP 포트 채널을 생성해야 합니다. Distributed Switch의 LAG는 최소한 두 개의 포트에 구성해야 합니다.
- 물리적 스위치에 있는 LACP 포트 채널의 해싱 알고리즘은 Distributed Switch의 LAG에 구성된 해싱 알고리즘과 동일해야 합니다.
- LACP 포트 채널에 연결하려는 모든 물리적 NIC는 동일한 속도와 이중 방식으로 구성해야 합니다.

다음으로 아래 항목을 읽으십시오.

- [분산 포트 그룹에 대한 LACP 팀 구성 및 페일오버 구성](#)
- [분산 포트 그룹에 대한 트래픽을 처리하기 위한 링크 집계 그룹 구성](#)
- [링크 집계 그룹 편집](#)
- [vSphere Distributed Switch에 대한 LACP 지원의 제한 사항](#)

## 분산 포트 그룹에 대한 LACP 팀 구성 및 페일오버 구성

LAG를 사용하여 분산 포트 그룹의 네트워크 트래픽을 처리하려면 물리적 NIC를 LAG 포트에 할당하고 분산 포트 그룹의 팀 구성 및 페일오버 순서에서 LAG를 활성 상태로 설정합니다.

표 5-1. 분산 포트 그룹의 LACP 팀 구성 및 페일오버 구성

페일오버 순서	업링크	설명
활성	단일 LAG	분산 포트 그룹의 트래픽을 처리하는 데는 하나의 활성 LAG나 여러 독립형 업링크만 사용할 수 있습니다. 여러 활성 LAG를 구성하거나 활성 LAG와 독립형 업링크를 혼합 구성할 수는 없습니다.
대기	비어 있음	활성 LAG 및 대기 업링크를 조합하거나, 반대로 대기 LAG 및 활성 업링크를 조합하는 것은 지원되지 않습니다. LAG와 다른 대기 LAG를 조합하는 것도 지원되지 않습니다.
사용되지 않음	모든 독립형 업링크 및 다른 LAG(있는 경우)	하나의 LAG만 활성 상태이고 대기 목록은 비어 있어야 하므로 모든 독립형 업링크와 다른 LAG는 사용되지 않은 상태로 설정해야 합니다.

## 분산 포트 그룹에 대한 트래픽을 처리하기 위한 링크 집계 그룹 구성

호스트에 있는 여러 물리적 NIC의 대역폭을 집계하기 위해 LAG(링크 집계 그룹)를 Distributed Switch에 생성하고 이 LAG를 사용하여 분산 포트 그룹의 트래픽을 처리할 수 있습니다.

새로 생성된 LAG의 포트에는 물리적 NIC가 할당되어 있지 않으며 이 LAG는 분산 포트 그룹의 팀 구성 및 페일오버 순서에 사용되지 않습니다. LAG를 사용하여 분산 포트 그룹의 네트워크 트래픽을 처리하려면 트래픽을 독립형 업링크에서 LAG로 마이그레이션해야 합니다.

### 사전 요구 사항

- LACP를 사용할 모든 호스트에 대해 별도의 LACP 포트 채널이 물리적 스위치에 존재하는지 확인합니다. [장 5 vSphere Distributed Switch의 LACP 지원](#)의 내용을 참조하십시오.
- LAG를 구성하는 vSphere Distributed Switch의 버전이 6.5 이상인지 확인합니다.
- Distributed Switch에서 향상된 LACP가 지원되는지 확인합니다.

### 절차

#### 1 링크 집계 그룹 생성

분산 포트 그룹의 네트워크 트래픽을 LAG(링크 집계 그룹)로 마이그레이션하려면 Distributed Switch에서 LAG를 생성해야 합니다.

#### 2 분산 포트 그룹의 팀 구성 및 페일오버 순서에서 링크 집계 그룹을 대기 상태로 설정

기본적으로 새 LAG(링크 집계 그룹)는 분산 포트 그룹의 팀 구성 및 페일오버 순서에 사용되지 않습니다. 분산 포트 그룹에 대해 오직 한 LAG 또는 독립형 업링크만 활성 상태가 될 수 있으므로 LAG가 대기 상태인 경우 중간 팀 구성 및 페일오버 구성을 생성해야 합니다. 이 구성을 사용하면 네트워크 연결을 유지하면서 물리적 NIC를 LAG 포트에 마이그레이션할 수 있습니다.

#### 3 링크 집계 그룹의 포트에 물리적 NIC 할당

분산 포트 그룹의 팀 구성 및 페일오버 순서에서 새 LAG(링크 집계 그룹)를 대기 상태로 설정하는 방법을 알아봅니다. LAG를 대기 상태로 설정하면 네트워크 연결을 유지한 상태로 물리적 NIC를 독립형 업링크에서 LAG 포트에 안전하게 마이그레이션할 수 있습니다.

#### 4 분산 포트 그룹의 팀 구성 및 페일오버 순서에서 링크 집계 그룹을 활성 상태로 설정

물리적 NIC를 LAG(링크 집계 그룹)의 포트로 마이그레이션한 후 분산 포트 그룹의 팀 구성 및 페일오버 순서에서 LAG를 활성으로 설정하고 모든 독립형 업링크를 사용되지 않음으로 이동하는 방법을 알아봅니다.

## 링크 집계 그룹 생성

분산 포트 그룹의 네트워크 트래픽을 LAG(링크 집계 그룹)로 마이그레이션하려면 Distributed Switch에서 LAG를 생성해야 합니다.

### 절차

- 1 vSphere Client에서 Distributed Switch로 이동합니다.
- 2 구성 탭에서 **설정**을 확장하고 **LACP**를 선택합니다.
- 3 새 링크 집계 그룹 아이콘을 클릭합니다.
- 4 새 LAG의 이름을 지정합니다.
- 5 LAG의 포트 수를 설정합니다.

LAG의 포트 수를 물리적 스위치에 있는 LACP 포트 채널의 포트 수와 동일하게 설정합니다. LAG 포트는 Distributed Switch의 업링크와 동일한 역할을 합니다. 모든 LAG 포트는 LAG 컨텍스트에서 NIC 팀을 구성합니다.

- 6 LAG의 LACP 협상 모드를 선택합니다.

옵션	설명
활성	모든 LAG 포트가 활성 협상 모드에 있습니다. 즉, LAG 포트가 LACP 패킷을 전송하여 물리적 스위치에서 LACP 포트 채널과의 협상을 시작합니다.
수동	LAG 포트가 수동 협상 모드에 있습니다. LAG 포트는 수신되는 LACP 패킷에 응답하지만 LACP 협상을 시작하지는 않습니다.

물리적 스위치의 LACP 지원 포트가 활성 협상 모드인 경우 LAG 포트를 수동 모드로 설정할 수 있으며, 그 반대의 경우도 가능합니다.

- 7 LACP가 정의하는 해싱 알고리즘에서 로드 밸런싱 모드를 선택합니다.

**참고** 해싱 알고리즘은 물리적 스위치의 LACP 포트 채널에 설정된 해싱 알고리즘과 동일해야 합니다.

- 8 링크 집계 시간 초과 모드를 선택합니다.

LACP PDU의 주기적 전송은 선택한 LACP 시간 초과 기본 설정에 따라 느리거나 빠른 전송 속도로 발생합니다. 빠른 시간 초과와 느린 시간 초과와 같은 경우 PDU가 1초마다 전송되고, 느린 시간 초과와 같은 경우 PDU가 30초마다 전송됩니다. 느린 시간 초과가 기본 설정입니다.

**참고** 빠른 시간 초과는 Distributed Switch 버전 7.0.2 이상에서만 지원됩니다.

## 9 LAG에 대한 VLAN 및 NetFlow 정책을 설정합니다.

개별 업링크 포트별로 VLAN 및 NetFlow 정책을 재정의하는 기능이 업링크 포트 그룹에서 사용하도록 설정된 경우 이 옵션이 활성화됩니다. LAG에 설정한 VLAN 및 NetFlow 정책은 업링크 포트 그룹 수준에서 설정된 정책을 재정의합니다.

## 10 확인을 클릭합니다.

### 결과

새 LAG는 분산 포트 그룹의 팀 구성 및 페일오버 순서에 사용되지 않으며, LAG 포트에는 물리적 NIC가 할당되지 않습니다.

독립형 업링크와 마찬가지로 LAG도 Distributed Switch와 연결된 모든 호스트에 반영됩니다. 예를 들어 Distributed Switch에 포트 2개가 포함된 LAG1을 생성할 경우 포트 2개를 포함하는 LAG1이 Distributed Switch에 연결된 모든 호스트에 생성됩니다.

### 다음에 수행할 작업

분산 포트 그룹의 팀 구성 및 페일오버 구성에서 LAG를 대기 상태로 설정합니다. 이렇게 하면 네트워크 연결을 끊지 않고도 네트워크 트래픽을 LAG로 마이그레이션할 수 있는 중간 구성을 생성할 수 있습니다.

## 분산 포트 그룹의 팀 구성 및 페일오버 순서에서 링크 집계 그룹을 대기 상태로 설정

기본적으로 새 LAG(링크 집계 그룹)는 분산 포트 그룹의 팀 구성 및 페일오버 순서에 사용되지 않습니다. 분산 포트 그룹에 대해 오직 한 LAG 또는 독립형 업링크만 활성화 상태가 될 수 있으므로 LAG가 대기 상태인 경우 중간 팀 구성 및 페일오버 구성을 생성해야 합니다. 이 구성을 사용하면 네트워크 연결을 유지하면서 물리적 NIC를 LAG 포트에 마이그레이션할 수 있습니다.

### 절차

- 1 Distributed Switch로 이동합니다.
- 2 **작업** 메뉴에서 **분산 포트 그룹 > 분산 포트 그룹 관리**를 선택합니다.
- 3 **팀 구성 및 페일오버**를 선택하고 **다음**을 클릭합니다.
- 4 LAG를 사용할 포트 그룹을 선택합니다.
- 5 페일오버 순서에서 LAG를 선택하고 위쪽 화살표를 사용하여 대기 업링크 목록으로 이동합니다.
- 6 **다음**을 클릭하고 중간 팀 구성 및 페일오버 구성의 사용 현황을 알리는 메시지를 검토한 후 **확인**을 클릭합니다.
- 7 완료 준비 페이지에서 **마침**을 클릭합니다.

### 다음에 수행할 작업

물리적 NIC를 독립형 업링크에서 LAG 포트에 마이그레이션합니다.

## 링크 집계 그룹의 포트에 물리적 NIC 할당

분산 포트 그룹의 팀 구성 및 페일오버 순서에서 새 LAG(링크 집계 그룹)를 대기 상태로 설정하는 방법을 알아봅니다. LAG를 대기 상태로 설정하면 네트워크 연결을 유지한 상태로 물리적 NIC를 독립형 업링크에서 LAG 포트 로 안전하게 마이그레이션할 수 있습니다.

### 사전 요구 사항

- 모든 LAG 포트 또는 물리적 스위치에 있는 해당 LACP 지원 포트가 활성 LACP 협상 모드인지 확인합니다.
- LAG 포트에 할당하려는 물리적 NIC의 속도가 동일하고 전이중으로 구성되었는지 확인합니다.

### 절차

- 1 vSphere Client에서 LAG가 있는 Distributed Switch로 이동합니다.
- 2 **작업** 메뉴에서 **호스트 추가 및 관리**를 선택합니다.
- 3 **호스트 네트워킹 관리**를 선택합니다.
- 4 물리적 NIC를 LAG 포트에 할당할 호스트를 선택하고 **다음**을 클릭합니다.
- 5 네트워크 어댑터 작업 선택 페이지에서 **물리적 어댑터 관리**를 선택하고 **다음**을 클릭합니다.
- 6 물리적 어댑터 관리 페이지에서 NIC를 선택하고 **업링크 할당**을 클릭합니다.
- 7 LAG 포트를 선택하고 **확인**을 클릭합니다.
- 8 LAG 포트에 할당할 모든 물리적 NIC에 대해 **6단계** 및 **7단계**를 반복합니다.
- 9 마법사를 완료합니다.

### 예제: 호스트 추가 및 관리 마법사에서 LAG에 두 개의 물리적 NIC 구성

예를 들어 포트가 두 개 있는 LAG의 경우 **호스트 추가 및 관리** 마법사에서 각 LAG 포트에 물리적 NIC를 구성합니다.

### 다음에 수행할 작업

분산 포트 그룹의 팀 구성 및 페일오버 순서에서 LAG를 활성 상태로 설정하고, 모든 독립형 업링크를 사용되지 않은 상태로 설정합니다.

## 분산 포트 그룹의 팀 구성 및 페일오버 순서에서 링크 집계 그룹을 활성 상태로 설정

물리적 NIC를 LAG(링크 집계 그룹)의 포트에 마이그레이션한 후 분산 포트 그룹의 팀 구성 및 페일오버 순서에서 LAG를 활성으로 설정하고 모든 독립형 업링크를 사용되지 않음으로 이동하는 방법을 알아봅니다.

### 절차

- 1 Distributed Switch로 이동합니다.
- 2 **작업** 메뉴에서 **분산 포트 그룹 > 분산 포트 그룹 관리**를 선택합니다.
- 3 **팀 구성 및 페일오버**를 선택하고 **다음**을 클릭합니다.

- LAG를 대기 상태로 설정한 포트 그룹을 선택하고 **다음**을 클릭합니다.
- 페일오버 순서에서 위쪽 및 아래쪽 화살표를 사용하여 LAG를 활성 목록으로 이동하고, 모든 독립형 업링크는 사용되지 않음 목록으로 각각 이동하여 대기 목록은 비워 둡니다.
- 다음**을 클릭한 후 **마침**을 클릭합니다.

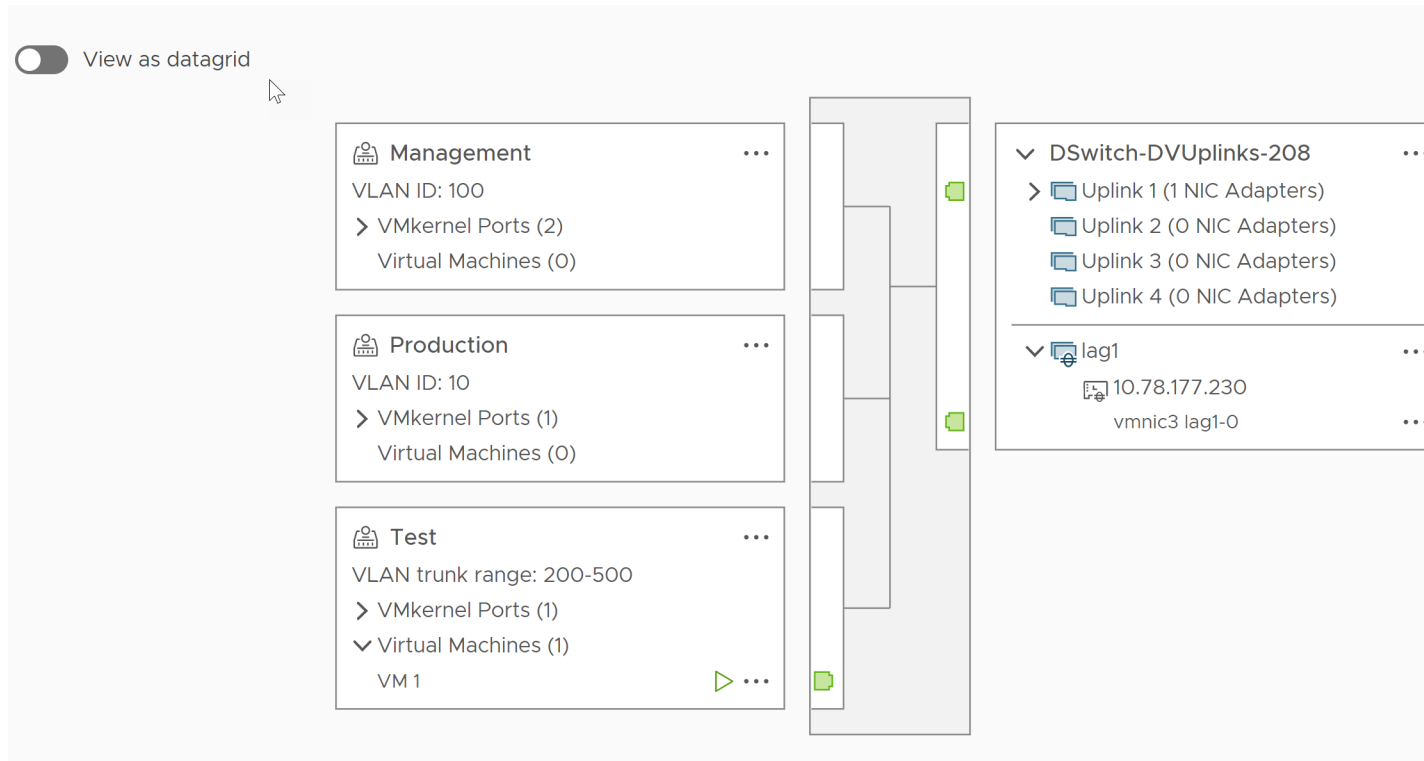
## 결과

네트워크 트래픽을 독립형 업링크에서 분산 포트 그룹의 LAG로 안전하게 마이그레이션하고 이러한 그룹에 대해 올바른 LACP 팀 구성 및 페일오버 구성을 생성했습니다.

## 예제: LAG를 사용하는 Distributed Switch의 토폴로지

분산 포트 그룹의 트래픽을 처리하기 위해 두 개의 포트가 포함된 LAG를 구성하는 경우 Distributed Switch의 토폴로지에서 새 구성에 따라 변경된 결과를 확인할 수 있습니다.

그림 5-2. LAG가 포함된 Distributed Switch 토폴로지



## 링크 집계 그룹 편집

그룹에 더 많은 포트를 추가하거나 LACP 협상 모드, 로드 밸런싱 알고리즘 또는 VLAN 및 NetFlow 정책을 변경해야 할 경우 LAG(링크 집계 그룹)의 설정을 수정하는 방법을 알아봅니다.

### 절차

- vSphere Client에서 vSphere Distributed Switch로 이동합니다.

2 구성 탭에서 **설정**을 확장하고 **LACP**를 선택합니다.

3 새 링크 집계 그룹 아이콘을 클릭합니다.

4 이름 텍스트 상자에 LAG의 새 이름을 입력합니다.

5 물리적 NIC를 더 추가하려면 LAG의 포트 수를 변경합니다.

새 NIC는 물리적 스위치의 LACP 포트 채널에 속한 포트에 연결되어야 합니다.

6 LAG의 LACP 협상 모드를 변경합니다.

물리적 LACP 포트 채널에 있는 모든 포트가 활성 LACP 모드일 경우에는 LAG의 LACP 모드를 수동 모드로 변경할 수 있고, 수동 모드일 경우에는 활성 모드로 변경할 수 있습니다.

7 LAG의 로드 밸런싱 모드를 변경합니다.

LACP가 정의하는 로드 밸런싱 알고리즘 중에서 선택할 수 있습니다.

8 링크 집계 시간 초과 모드를 선택합니다.

LACP PDU의 주기적 전송은 선택한 LACP 시간 초과 기본 설정에 따라 느리거나 빠른 전송 속도로 발생합니다. 빠른 시간 초과와 경우 PDU가 1초마다 전송되고, 느린 시간 초과와 경우 PDU가 30초마다 전송됩니다. 느린 시간 초과가 기본 설정입니다.

**참고** 다음 ESXCLI 명령을 실행하여 빠른 LACP 시간 초과를 설정할 수 있습니다. 하지만 NSX 지원 DVS 또는 N-VDS(볼투명 NSX Distributed vSwitch)에 대해서는 이 설정을 사용할 수 없습니다.

```
esxcli network vswitch dvs vmware lacp timeout set --vds DVS-name --lag-id <integer> --
timeout 1
```

9 VLAN 및 NetFlow 정책을 변경합니다.

개별 포트의 VLAN 및 NetFlow 정책을 재정의하는 옵션이 업링크 포트 그룹에서 사용하도록 설정된 경우 이 옵션이 활성화됩니다. LAG에 대해 변경한 VLAN 및 NetFlow 정책은 업링크 포트 그룹 수준에 설정된 정책을 재정의합니다.

10 **확인**을 클릭합니다.

## vSphere Distributed Switch에 대한 LACP 지원의 제한 사항

vSphere Distributed Switch의 LACP 지원 기능을 사용하면 네트워크 디바이스가 피어에 LACP 패킷을 전송하여 링크의 자동 번들을 협상할 수 있습니다. 그러나 vSphere Distributed Switch의 LACP 지원 기능에는 다음과 같은 제한이 있습니다.

- 소프트웨어 iSCSI 포트 바인딩을 사용하는 경우 LACP가 지원되지 않습니다. 포트 바인딩이 사용되지 않는 경우 LAG를 통한 iSCSI 다중 경로 지정이 지원됩니다.
- 호스트 프로파일에서는 LACP 지원 설정을 사용할 수 없습니다.
- 중첩된 ESXi 호스트 간에는 LACP 지원이 불가능합니다.

- LACP 지원은 ESXi Dump Collector와는 함께 작동하지 않습니다.
- 포트 미러링을 사용하도록 설정하면 LACP PDU(LACP 제어 패킷)가 미러링되지 않습니다.
- LAG 포트에 대해 팀 구성 및 페일오버 상태 점검을 수행할 수 없습니다. LACP는 LAG 포트의 연결을 확인합니다.
- 향상된 LACP 지원 기능은 분산 포트 또는 포트 그룹별로 하나의 LAG에서만 트래픽을 처리하는 경우에 제대로 작동합니다.



# 네트워크 구성 백업 및 복원

# 6

vSphere를 사용하면 잘못된 변경 또는 다른 배포로의 전송의 경우 vSphere Distributed Switch, 분산 및 업링크 포트 그룹의 구성을 백업 및 복원할 수 있습니다.

다음으로 아래 항목을 읽으십시오.

- vSphere Distributed Switch 구성 백업 및 복원
- vSphere 분산 포트 그룹 구성 내보내기, 가져오기 및 복원
- ESXi Configuration Manager 통합

## vSphere Distributed Switch 구성 백업 및 복원

vCenter Server는 vSphere Distributed Switch의 구성에 대한 백업 및 복원 기능을 제공합니다. 데이터베이스 또는 업그레이드 실패가 발생하는 경우 가상 네트워크 구성을 복원하는 방법에 대해 알아보십시오. 또한 저장된 스위치 구성을 템플릿으로 사용하여 동일한 또는 새로운 vSphere 환경에서 스위치의 사본을 생성할 수도 있습니다.

해당 포트 그룹을 포함하여 Distributed Switch의 구성을 가져오거나 내보낼 수 있습니다. 포트 그룹 구성을 내보내고, 가져오고, 복원하는 방법에 대한 자세한 내용은 [vSphere 분산 포트 그룹 구성 내보내기, 가져오기 및 복원](#) 항목을 참조하십시오.

---

**참고** 저장된 구성 파일을 사용하여 배포된 스위치에서 정책 및 호스트 연결을 복원할 수 있습니다. 물리적 NIC와 업링크 포트 또는 링크 집계 그룹의 포트 간 연결은 복원할 수 없습니다.

---

## vSphere Distributed Switch 구성 내보내기

vSphere Distributed Switch 및 분산 포트 그룹 구성을 파일로 내보내는 방법을 알아봅니다. 파일에는 유효한 네트워크 구성이 유지되므로 이러한 구성을 다른 환경으로 전송할 수 있습니다.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 Distributed Switch를 마우스 오른쪽 버튼으로 클릭하고 **설정 > 구성 내보내기**를 선택합니다.
- 3 Distributed Switch 구성 내보내기를 선택하거나 Distributed Switch 구성과 모든 포트 그룹 내보내기를 선택합니다.

- 4 (선택 사항) **설명** 필드에 이 구성에 대한 메모를 입력합니다.
- 5 **확인**을 클릭합니다.
- 6 **예**를 클릭하여 구성 파일을 로컬 시스템에 저장합니다.

#### 다음에 수행할 작업

내보낸 구성 파일을 사용하여 다음 작업을 수행합니다.

- vSphere 환경에서 내보낸 Distributed Switch의 사본을 생성합니다. [vSphere Distributed Switch 구성 가져오기](#)의 내용을 참조하십시오.
- 기존 Distributed Switch의 설정을 덮어씁니다. [vSphere Distributed Switch 구성 복원](#)의 내용을 참조하십시오.

포트 그룹 구성만 내보내고, 가져오고, 복원할 수 있습니다. [vSphere 분산 포트 그룹 구성 내보내기, 가져오기 및 복원](#)의 내용을 참조하십시오.

## vSphere Distributed Switch 구성 가져오기

새 vSphere Distributed Switch를 생성하거나 이전에 삭제된 스위치를 복원하기 위해 저장된 구성 파일을 가져오는 방법을 알아봅니다.

구성 파일에는 스위치의 네트워킹 설정이 포함되어 있습니다. 이 설정을 사용하여 다른 가상 환경의 스위치를 복제할 수도 있습니다.

---

**참고** 저장된 구성 파일을 사용하여 스위치 인스턴스, 호스트 연결 및 정책을 복제할 수 있습니다. 물리적 NIC와 업링크 포트 또는 링크 집계 그룹의 포트 간 연결은 복제할 수 없습니다.

---

#### 절차

- 1 vSphere Client에서 데이터 센터로 이동합니다.
- 2 데이터 센터를 마우스 오른쪽 버튼으로 클릭하고 **Distributed Switch > Distributed Switch 가져오기**를 선택합니다.
- 3 구성 파일의 위치로 이동합니다.
- 4 구성 파일의 키를 스위치와 해당 포트 그룹에 할당하려면 **원래 Distributed Switch 및 포트 그룹 식별자 유지** 확인란을 선택하고 **다음**을 클릭합니다.

다음과 같은 경우 **원래 Distributed Switch 및 포트 그룹 식별자 유지** 옵션을 사용할 수 있습니다.

- 삭제된 스위치를 다시 생성합니다.
- 업그레이드가 실패한 스위치를 복원합니다.

모든 포트 그룹이 다시 생성되고 스위치에 연결된 호스트가 다시 추가됩니다.

- 5 스위치의 설정을 검토하고 **마침**을 클릭합니다.

## 결과

구성 파일의 설정을 사용하여 새 Distributed Switch가 생성됩니다. 분산 포트 그룹 정보를 구성 파일에 포함한 경우에는 분산 포트 그룹도 만들어집니다.

## vSphere Distributed Switch 구성 복원

복원 옵션을 사용하여 기존 Distributed Switch의 구성을 구성 파일의 설정으로 재설정하는 방법을 알아봅니다. Distributed Switch를 복원하면 선택된 스위치의 설정이 구성 파일에 저장된 설정으로 변경됩니다.

**참고** 저장된 구성 파일을 사용하여 배포된 스위치에서 정책 및 호스트 연결을 복원할 수 있습니다. 물리적 NIC와 업링크 포트 또는 링크 집계 그룹의 포트 간 연결은 복원할 수 없습니다.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 탐색기에서 Distributed Switch를 마우스 오른쪽 버튼으로 클릭하고 **설정 > 복원 구성**을 선택합니다.
- 3 사용할 구성 백업 파일을 찾습니다.
- 4 **Distributed Switch 및 모든 포트 그룹 복원** 또는 **Distributed Switch만 복원**을 선택하고 **다음**을 클릭합니다.
- 5 복원에 대한 요약 정보를 검토합니다.

Distributed Switch를 복원하면 Distributed Switch 및 해당 포트 그룹의 현재 설정을 덮어씁니다. 구성 파일의 일부가 아닌 기존 포트 그룹은 삭제하지 않습니다.

- 6 **마침**을 클릭합니다.

Distributed Switch 구성이 구성 파일의 설정으로 복원되었습니다.

## vSphere 분산 포트 그룹 구성 내보내기, 가져오기 및 복원

vSphere 분산 포트 그룹 구성을 파일로 내보내는 방법을 알아봅니다. 구성 파일을 사용하면 유효한 포트 그룹 구성을 유지하고 이러한 구성을 다른 배포로 분배할 수 있습니다.

분산 스위치 구성을 내보내는 동시에 포트 그룹 정보를 내보낼 수 있습니다. [vSphere Distributed Switch 구성 백업 및 복원](#)의 내용을 참조하십시오.

### vSphere 분산 포트 그룹 구성 내보내기

분산 포트 그룹 구성을 파일로 내보내는 방법을 알아봅니다. 구성은 유효한 네트워크 구성을 유지하므로 이러한 구성을 다른 배포로 분배할 수 있습니다.

## 절차

- 1 vSphere Client에서 분산 포트 그룹을 찾습니다.
  - a Distributed Switch를 선택하고 **네트워크** 탭을 클릭합니다.
  - b **분산 포트 그룹**을 클릭합니다.
- 2 분산 포트 그룹을 마우스 오른쪽 버튼으로 클릭하고 **구성 내보내기**를 선택합니다.
- 3 (선택 사항) **설명** 필드에서 이 구성에 대한 메모를 입력합니다.
- 4 **확인**을 클릭합니다.

**예**를 클릭하여 구성 파일을 로컬 시스템에 저장합니다.

## 결과

이제 선택된 분산 포트 그룹의 모든 설정이 포함된 구성 파일이 생성되었습니다. 이 파일을 사용하여 기존 배포에 이 구성의 사본을 여러 개 만들거나 기존 분산 포트 그룹의 설정을 이 설정으로 덮어쓸 수 있습니다.

## 다음에 수행할 작업

내보낸 구성 파일을 사용하여 다음 작업을 수행할 수 있습니다.

- 내보낸 분산 포트 그룹의 사본을 만들려면 [vSphere 분산 포트 그룹 구성 가져오기](#)의 내용을 참조하십시오.
- 기존 분산 포트 그룹의 설정을 덮어쓰려면 [vSphere 분산 포트 그룹 구성 복원](#)의 내용을 참조하십시오.

## vSphere 분산 포트 그룹 구성 가져오기

를 가져와서 구성 파일에서 분산 포트 그룹을 생성하는 방법을 알아봅니다.

기존 포트 그룹이 가져온 포트 그룹과 이름이 같은 경우 새 포트 그룹 이름에 괄호 안에 포함된 숫자가 추가됩니다. 가져온 구성의 설정이 새 포트 그룹에 적용되고 원래 포트 그룹의 설정은 변경 없이 유지됩니다.

## 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 Distributed Switch를 마우스 오른쪽 버튼으로 클릭하고 **분산 포트 그룹 > 분산 포트 그룹 가져오기**를 선택합니다.
- 3 구성 파일이 저장된 위치로 이동하고 **다음**을 클릭합니다.
- 4 가져오기를 완료하기 전에 가져오기 설정을 검토합니다.
- 5 **마침**을 클릭합니다.

## vSphere 분산 포트 그룹 구성 복원

복원 옵션을 사용하여 기존 분산 포트 그룹의 구성을 구성 파일의 설정으로 재설정하는 방법을 알아봅니다.

## 절차

- 1 vSphere Client에서 분산 포트 그룹을 찾습니다.
  - a Distributed Switch를 선택하고 **네트워크** 탭을 클릭합니다.
  - b **분산 포트 그룹**을 클릭합니다.
- 2 분산 포트 그룹을 마우스 오른쪽 버튼으로 클릭하고 **구성 복원**을 선택합니다.
- 3 다음 중 하나를 선택하고 **다음**을 클릭합니다.
  - ◆ **이전 구성으로 복원** - 포트 그룹 구성을 한 단계 뒤로 롤백합니다. 두 단계 이상을 수행했을 경우 포트 그룹 구성을 완전히 복원하지 못할 수 있습니다.
  - ◆ **파일에서 구성 복원** - 내보낸 백업 파일을 사용하여 포트 그룹 구성을 복원할 수 있습니다. Distributed Switch 백업 파일에 포트 그룹 구성 정보가 있을 경우 이 파일을 사용할 수도 있습니다.
- 4 복원에 대한 요약 정보를 검토합니다.
 

복원 작업을 수행하면 분산 포트 그룹의 현재 설정을 백업의 설정으로 덮어씁니다. 스위치 백업 파일에서 포트 그룹 구성을 복원하는 경우 복원 작업을 통해 파일의 일부가 아닌 기존 포트 그룹이 삭제되지 않습니다.
- 5 **마침**을 클릭합니다.

## ESXi Configuration Manager 통합

vSphere Lifecycle Manager 클러스터 수준 구성 관리자에서 핵심 vSphere 네트워킹 구성을 관리할 수 있습니다. vSphere 네트워킹 구성에는 다음이 포함됩니다. *vmknics, netstacks, vdsvsitches, pnic, netdump, firewall, ipsec, /etc/hosts, /etc/resolv.conf*가 포함됩니다.

vSphere 8.0 업데이트 3부터 vSphere Distributed Switch가 VCP(vSphere Configuration Profiles)와 통합됩니다. VCP(vSphere Configuration Profiles) 클러스터에서 호스트 분산 스위치 구성을 관리할 수 있습니다.

---

**참고** MTU와 같은 글로벌 분산 스위치 구성은 VCP 범위를 벗어납니다.

---

JSON 형식의 단일 구성 파일을 사용하여 클러스터 수준에서 모든 호스트 구성 외에도 vSphere Distributed Switch를 관리할 수 있습니다. 클러스터의 모든 호스트가 분산 및 호스트 구성을 준수하는지 확인할 수 있습니다. 클러스터 수준의 업데이트 적용 작업 흐름을 사용하여 ESXi 호스트 네트워킹을 표준 스위치에서 분산 스위치로 마이그레이션할 수 있습니다. 이제 분산 스위치의 VMkernel 네트워크 어댑터가 구성 관리자에서 완전히 지원됩니다.

구성 관리자를 사용하면 호스트 설정(예: 호스트가 가입할 수 있는 분산 스위치 목록 및 PNIC-VDS 업링크 매핑)을 포함하는 VCP 클러스터에 연결된 VCP를 구성할 수 있습니다.

## 호스트 구성 내보내기

원하는 상태 구성을 사용하면 여러 지역 및 서로 다른 도메인에서 vSphere 네트워킹 구성을 원활하게 관리하는데 어떻게 도움이 되는지 알아봅니다.

이 작업에서는 vmknic에 대한 원하는 상태 규격을 포함하는 JSON 파일을 내보냅니다.

#### 사전 요구 사항

- vSphere Life Cycle Manager 지원 클러스터가 있어야 합니다.
- 클러스터에 호스트가 있는지 확인합니다.

#### 절차

- 1 vSphere Client에서 클러스터로 이동합니다.
- 2 **원하는 상태 > 호스트 설정 > 참조 호스트에서 추출**을 클릭합니다. **설정 추출** 대화상자가 나타납니다.
- 3 기존 클러스터에서 호스트를 선택합니다.
- 4 **다음**을 클릭합니다.
- 5 **설정 다운로드**를 클릭하여 파일을 다운로드합니다.

#### 결과

JSON 파일이 다운로드되었습니다.

#### 다음에 수행할 작업

이제 JSON 파일을 재사용하여 포함된 원하는 상태를 동일한 또는 서로 다른 vCenter Server 인스턴스의 다른 클러스터에 적용할 수 있습니다.

---

**참고** 솔루션 구성은 포함되지 않습니다. 캐시된 정보는 포함되지 않습니다. 호스트별 속성만 포함됩니다.

---

**참고** vSphere Life Cycle Manager 지원 클러스터가 있는 경우 클러스터의 호스트를 vSphere Distributed Switch에 가입시킬 수 없습니다.

---

## 호스트 구성 가져오기

원하는 상태를 JSON 파일로 가져오는 방법을 알아봅니다.

호스트 구성을 사용하여 JSON 파일을 가져오는 방법을 알아봅니다. 클러스터에 원하는 상태를 적용하기 전에 원하는 상태를 기준으로 클러스터의 모든 호스트를 검색하고 클러스터 규정 준수를 확인할 수 있습니다. 규정 준수 검사를 실행하여 드리프트를 즉시 감지할 수 있습니다.

#### 사전 요구 사항

- vSphere Lifecycle Manager 지원 클러스터가 있어야 합니다.
- 클러스터에 호스트가 있는지 확인합니다.
- 올바른 호스트 구성 JSON 파일이 있는지 확인합니다.

#### 절차

- 1 vSphere Client에서 클러스터로 이동합니다.

- 2 원하는 상태 > 호스트 설정 > 설정 가져오기를 클릭합니다. 호스트 설정 가져오기 대화상자가 나타납니다.
- 3 찾아보기를 클릭하여 파일을 선택합니다. 규정 준수가 검증됩니다.  
규정을 준수하지 않는 호스트가 있는 경우 오류 메시지가 표시됩니다.
- 4 호스트 규정 준수 문제를 해결하려면 업데이트 적용을 클릭합니다. 업데이트 적용 설정 대화상자가 나타납니다. 사전 확인을 진행합니다.
- 5 사전 확인이 완료되었습니다. 호스트 수준 업데이트 적용 세부 정보가 영향 검토 아래에 표시됩니다.
- 6 업데이트 적용을 클릭하여 구성 설정에 업데이트를 적용합니다.

#### 결과

호스트에서 가져온 설정을 볼 수 있습니다.

#### 예제:

# 관리 네트워크의 롤백 및 복구

# 7

vSphere Distributed Switch 및 vSphere Standard Switch의 롤백 및 복구 지원을 사용하여 관리 네트워크의 잘못된 구성을 방지하고 복구하는 방법을 알아봅니다.

롤백은 표준 스위치 및 Distributed Switch 모두에 사용할 수 있습니다. 관리 네트워크의 잘못된 구성을 수정하려면 DCUI를 통해 문제를 해결할 호스트에 직접 연결합니다.

다음으로 아래 항목을 읽으십시오.

- vSphere 네트워킹 롤백
- vSphere Distributed Switch의 관리 네트워크 구성에서 오류 해결

## vSphere 네트워킹 롤백

구성이 잘못된 관리 네트워크 때문에 호스트와 vCenter Server의 연결이 끊기지 않도록 vSphere가 구성 변경 사항을 롤백하여 호스트를 보호하는 방법을 알아봅니다.

vSphere 네트워킹에서는 기본적으로 롤백이 사용되도록 설정되어 있습니다. 하지만 vCenter Server 수준에서 롤백을 활성화하거나 비활성화할 수 있습니다.

## 호스트 네트워킹 롤백

호스트 네트워킹 롤백은 vCenter Server와의 연결에 대한 네트워킹 구성이 잘못된 상태로 변경될 때 발생합니다. 호스트의 연결을 끊는 모든 네트워크 변경 사항도 롤백을 트리거합니다. 다음은 롤백을 트리거할 수 있는 호스트 네트워킹 구성 변경 사항의 예입니다.

- 물리적 NIC의 속도 또는 이중 모드 업데이트
- DNS 및 라우팅 설정 업데이트
- 관리 VMkernel 네트워크 어댑터를 포함하는 표준 포트 그룹의 팀 구성 및 페일오버 정책이나 트래픽 조절 정책 업데이트
- 관리 VMkernel 네트워크 어댑터를 포함하는 표준 포트 그룹의 VLAN 업데이트
- 물리적 인프라에서 지원되지 않는 값으로 관리 VMkernel 네트워크 어댑터 및 해당 스위치의 MTU 증가
- 관리 VMkernel 네트워크 어댑터의 IP 설정 변경
- 표준 스위치 또는 Distributed Switch에서 관리 VMkernel 네트워크 어댑터 제거



- 관리 VMkernel 네트워크 어댑터를 포함하는 표준 스위치 또는 Distributed Switch의 물리적 NIC 제거
  - 관리 VMkernel 어댑터를 vSphere 표준 스위치에서 vSphere Distributed Switch로 마이그레이션
- 이러한 이유로 인해 네트워크의 연결이 끊기면 작업이 실패하고 호스트가 유효한 마지막 구성으로 복구됩니다.

## vSphere Distributed Switch 롤백

Distributed Switch 롤백은 Distributed Switch, 분산 포트 그룹, 분산 포트가 잘못된 상태로 업데이트될 때 발생합니다. 다음은 롤백을 트리거하는 Distributed Switch 구성 변경 사항의 예입니다.

- Distributed Switch의 MTU 변경
- 관리 VMkernel 네트워크 어댑터의 분산 포트 그룹에서 다음 설정 변경
  - 팀 구성 및 페일오버
  - VLAN
  - 트래픽 조절
- 관리 VMkernel 네트워크 어댑터를 포함하는 분산 포트 그룹의 모든 포트 차단
- 분산 포트 수준에서 관리 VMkernel 네트워크 어댑터에 대한 정책 재정의

변경 사항으로 인해 구성이 잘못되면 하나 이상의 호스트가 Distributed Switch와 동기화되지 않을 수 있습니다.

충돌하는 구성 설정의 위치를 알고 있는 경우 해당 설정을 수동으로 수정할 수 있습니다. 예를 들어 관리 VMkernel 네트워크 어댑터를 새 VLAN으로 마이그레이션한 경우 VLAN이 물리적 스위치에서 실제로 트렁킹되지 않을 수 있습니다. 이 경우 물리적 스위치 구성을 수정하면 다음에 Distributed Switch와 호스트를 동기화할 때 구성 문제가 해결됩니다.

문제가 발생한 위치가 확실하지 않은 경우에는 Distributed Switch 또는 분산 포트 그룹의 상태를 이전 구성으로 복원할 수 있습니다. [vSphere 분산 포트 그룹 구성 복원](#)의 내용을 참조하십시오.

## 네트워크 롤백 사용 안 함

vSphere에서는 기본적으로 롤백이 사용되도록 설정되어 있습니다. vSphere Client를 사용하여 vCenter Server에서 롤백을 사용하지 않도록 설정할 수 있습니다.

### 절차

- 1 vSphere Client에서 vCenter Server 인스턴스로 이동합니다.
- 2 구성 탭에서 **설정**을 확장하고 **고급 설정**을 선택합니다.
- 3 **설정 편집**을 클릭합니다.
- 4 `config.vpxd.network.rollback` 키를 선택하고 값을 `false`로 변경합니다.  
키가 없으면 키를 추가한 후 값을 `false`로 설정할 수 있습니다.
- 5 **확인**을 클릭합니다.
- 6 vCenter Server를 다시 시작하여 변경 내용을 적용합니다.

## vCenter Server 구성 파일을 사용하여 네트워크 롤백을 사용하지 않도록 설정

vSphere에서는 기본적으로 롤백이 사용되도록 설정되어 있습니다. vCenter Server의 `vpzd.cfg` 구성 파일을 직접 편집하여 롤백을 사용하지 않도록 설정할 수 있습니다.

### 절차

- 1 vCenter Server의 호스트 시스템에서 `/etc/vmware-vpx` 디렉토리로 이동합니다.
- 2 편집할 `vpzd.cfg` 파일을 엽니다.
- 3 `<network>` 요소에서 `<rollback>` 요소를 **false**로 설정합니다.

```
<config>
  <vpzd>
    <network>
      <rollback>false</rollback>
    </network>
  </vpzd>
</config>
```

- 4 파일을 저장한 후 닫습니다.
- 5 vCenter Server 시스템을 다시 시작합니다.

## vSphere Distributed Switch의 관리 네트워크 구성에서 오류 해결

DCUI(Direct Console User Interface)를 사용하여 Distributed Switch를 통해 관리 네트워크에 액세스하는 호스트와 vCenter Server 간의 연결을 복원하는 방법을 알아봅니다.

네트워킹 롤백이 사용하지 않도록 설정된 경우 Distributed Switch에서 관리 네트워크의 포트 그룹을 잘못 구성하면 vCenter Server와 이 Distributed Switch에 추가된 호스트 간의 연결이 끊어집니다. 그러면 DCUI를 사용하여 각 호스트를 개별적으로 연결해야 합니다.

다른 유형의 트래픽(vMotion, Fault Tolerance 등)을 처리하는 VMkernel 어댑터에서 관리 네트워크를 복원하는 데 사용하는 업링크도 사용되는 경우 복원 후 해당 어댑터의 네트워크 연결이 끊어집니다.

DCUI 액세스 및 사용에 대한 자세한 내용은 "vSphere 보안" 설명서를 참조하십시오.

---

**참고** 상태 비저장 ESXi 인스턴스에서는 Distributed Switch의 관리 연결을 복구할 수 없습니다.

---

### 사전 요구 사항

Distributed Switch의 포트 그룹에서 관리 네트워크가 구성되어 있는지 확인합니다.

### 절차

- 1 호스트의 DCUI에 연결합니다.
- 2 **네트워크 복원 옵션** 메뉴에서 **vDS 복원**을 선택합니다.
- 3 업링크를 구성하고 필요한 경우 관리 네트워크에 대한 VLAN을 구성합니다.

#### 4 구성을 적용합니다.

##### 결과

DCUI에서 사용 후 삭제 로컬 포트가 생성되고 사용자가 제공한 VLAN 및 업링크 값이 적용됩니다. 또한 관리 네트워크의 VMkernel 어댑터가 새 로컬 포트로 이동하여 vCenter Server와의 연결이 복원됩니다.

##### 다음에 수행할 작업

호스트와 vCenter Server의 연결이 복원되면 분산 포트 그룹의 구성을 수정하고 VMkernel 어댑터를 그룹에 다시 추가합니다.

# vSphere 네트워킹 정책

# 8

표준 스위치나 분산 포트 그룹 수준에 설정된 정책은 표준 스위치의 모든 포트 그룹 또는 분산 포트 그룹의 모든 포트에 적용됩니다. 단, 표준 포트 그룹이나 분산 포트 수준에서 재정의된 구성 옵션은 예외입니다.

vSphere 표준 스위치 및 Distributed Switch에 대한 네트워킹 정책 적용에 대한 비디오를 시청하십시오.



(네트워킹 정책 사용)

- **vSphere Standard 또는 Distributed Switch에 네트워킹 정책 적용**  
vSphere 표준 스위치와 vSphere Distributed Switch에 네트워킹 정책을 다르게 적용합니다. vSphere Distributed Switch에 사용 가능한 일부 정책은 vSphere 표준 스위치에서 사용할 수 없습니다.
- **포트 수준에서 네트워킹 정책 재정의 구성**  
분산 포트에 대해 서로 다른 정책을 적용하는 방법을 알아보고 포트 그룹 수준에서 설정된 정책의 포트별 재정의 구성을 구성합니다. 또한 분산 포트가 가상 시스템에서 연결이 끊어지는 경우 포트별 수준에서 설정된 구성을 재설정하도록 설정할 수도 있습니다.
- **팀 구성 및 페일오버 정책이란?**  
NIC 팀 구성을 사용하면 팀에 2개 이상의 물리적 NIC를 포함하여 가상 스위치의 네트워크 용량을 늘릴 수 있습니다. 어댑터 장애 시 트래픽이 재라우팅되는 방식을 결정하려면 페일오버 순서에 물리적 NIC를 포함합니다. 가상 스위치가 팀의 물리적 NIC 간에 네트워크 트래픽을 분산하는 방식을 결정하려면 환경의 요구와 기능에 따라 로드 밸런싱 알고리즘을 선택합니다.
- **VLAN 정책이란?**  
VLAN 정책은 네트워크 환경에서 VLAN이 작동하는 방식을 결정합니다.
- **보안 정책이란?**  
네트워킹 보안 정책은 MAC 주소 가장 행위 및 원치 않는 포트 검색으로부터 트래픽을 보호합니다.
- **트래픽 조절 정책이란?**  
트래픽 조절 정책은 평균 대역폭, 최대 대역폭 및 버스트 크기에 의해 정의됩니다. 각 포트 그룹과 각 분산 포트 또는 분산 포트 그룹에 대한 트래픽 조절 정책을 설정할 수 있습니다.
- **리소스 할당 정책이란?**  
리소스 할당 정책을 사용하면 분산 포트 또는 포트 그룹을 사용자가 생성한 네트워크 리소스 풀과 연결할 수 있습니다. 이 정책을 사용하면 포트 또는 포트 그룹에 지정된 대역폭을 보다 강력하게 제어할 수 있습니다.

- **모니터링 정책이란?**

모니터링 정책은 분산 포트 또는 포트 그룹에 대한 NetFlow 모니터링을 사용하거나 사용하지 않도록 설정합니다.

- **트래픽 필터링 및 표시 정책이란?**

vSphere Distributed Switch에서 트래픽 필터링 및 표시 정책을 사용하여 원하지 않는 트래픽과 보안 공격으로부터 가상 네트워크를 보호하거나 특정 유형의 트래픽에 QoS 태그를 적용할 수 있습니다.

- **vSphere Distributed Switch에서 여러 포트 그룹에 대한 정책 관리**

vSphere Distributed Switch 여러 포트 그룹에 대한 네트워킹 정책을 수정하는 방법을 알아봅니다.

- **포트 차단 정책**

포트 차단 정책을 사용하면 포트에서 데이터를 보내거나 받는 것을 선택적으로 차단할 수 있습니다.

- **MAC 학습 정책이란?**

MAC 학습은 하나의 vNIC에서 여러 MAC 주소가 사용되는 배포에 대한 네트워크 연결을 제공합니다.

## vSphere Standard 또는 Distributed Switch에 네트워킹 정책 적용

vSphere 표준 스위치와 vSphere Distributed Switch에 네트워킹 정책을 다르게 적용합니다. vSphere Distributed Switch에 사용 가능한 일부 정책은 vSphere 표준 스위치에서 사용할 수 없습니다.

표 8-1. 정책이 적용되는 가상 스위치 개체

가상 스위치	가상 스위치 개체	설명
vSphere 표준 스위치	전체 스위치	전체 표준 스위치에 정책을 적용하는 경우 정책이 스위치의 모든 표준 포트 그룹에 전파됩니다.
	표준 포트 그룹	스위치에서 상속된 정책을 무시하여 개별 포트 그룹에 각기 다른 정책을 적용할 수 있습니다.
vSphere Distributed Switch	분산 포트 그룹	분산 포트 그룹에 정책을 적용하는 경우 정책이 그룹의 모든 포트에 전파됩니다.
	분산 포트	분산 포트 그룹에서 상속된 정책을 무시하여 개별 분산 포트에 각기 다른 정책을 적용할 수 있습니다.
	업링크 포트 그룹	업링크 포트 그룹 수준에서 정책을 적용할 수 있으며 정책이 그룹의 모든 포트에 전파됩니다.
	업링크 포트	업링크 포트 그룹에서 상속된 정책을 무시하여 개별 업링크 포트에 각기 다른 정책을 적용할 수 있습니다.

표 8-2. vSphere 표준 스위치 및 vSphere Distributed Switch에 사용 가능한 정책

정책	표준 스위치	분산 스위치	설명
팀 구성 및 페일오버	예	예	표준 스위치, 표준 포트 그룹, 분산 포트 그룹 또는 분산 포트에 대한 네트워크 트래픽을 처리하는 물리적 NIC를 구성할 수 있습니다. 페일오버 순서로 물리적 NIC를 배열한 후 각기 다른 로드 밸런싱 정책을 적용합니다.
보안	예	예	MAC 주소 가장 행위 및 원치 않는 포트 검색으로부터 트래픽을 보호합니다. 네트워킹 보안 정책은 네트워킹 프로토콜 스택의 계층 2에서 구현됩니다.
트래픽 조절	예	예	포트에서 사용 가능한 네트워크 대역폭을 제한하지만 보다 빠른 속도의 트래픽 버스트도 통과하도록 허용할 수 있습니다. ESXi는 표준 스위치에서 아웃바운드 네트워크 트래픽을 조절하고 Distributed Switch에서 인바운드 및 아웃바운드 트래픽을 조절합니다.
VLAN	예	예	표준 스위치 또는 Distributed Switch에 대한 VLAN 태그 지정을 구성할 수 있습니다. EST(External Switch Tagging), VST(Virtual Switch Tagging) 및 VGT(Virtual Guest Tagging)를 구성할 수 있습니다.
모니터링	아니요	예	분산 포트 또는 포트 그룹에 대한 NetFlow 모니터링을 사용하거나 사용하지 않도록 설정합니다.
트래픽 필터링 및 표시	아니요	예	원치 않는 트래픽 및 보안 공격으로부터 가상 네트워크를 보호하고 특정 트래픽 유형에 QoS 태그를 적용할 수 있습니다.
리소스 할당	아니요	예	분산 포트 또는 포트 그룹을 사용자 정의 네트워크 리소스 풀에 연결할 수 있습니다. 이러한 방식으로 포트 또는 포트 그룹에 사용 가능한 대역폭을 보다 효과적으로 제어할 수 있습니다. vSphere Network I/O Control 버전 2 및 3과 함께 리소스 할당 정책을 사용할 수 있습니다.
포트 차단	아니요	예	포트가 데이터를 전송 및 수신하는 것을 선택적으로 차단할 수 있습니다.

## 포트 수준에서 네트워킹 정책 재정의 구성

분산 포트에 대해 서로 다른 정책을 적용하는 방법을 알아보고 포트 그룹 수준에서 설정된 정책의 포트별 재정의 구성합니다. 또한 분산 포트가 가상 시스템에서 연결이 끊어지는 경우 포트별 수준에서 설정된 구성을 재설정하도록 설정할 수도 있습니다.

### 절차

- 1 vSphere Client에서 분산 포트 그룹을 찾습니다.
  - a Distributed Switch를 선택하고 **네트워크** 탭을 클릭합니다.
  - b **분산 포트 그룹**을 클릭합니다.
- 2 분산 포트 그룹을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.

### 3 고급 페이지를 선택합니다.

옵션	설명
연결이 끊길 때 리셋 구성	드롭다운 메뉴에서 연결이 끊길 때 재설정을 사용하거나 사용하지 않도록 설정합니다. 분산 포트와 가상 시스템의 연결이 끊어지면 분산 포트의 구성이 분산 포트 그룹 설정으로 재설정됩니다. 이때 모든 포트별 재정의가 삭제됩니다.
포트 정책 재정의	포트별 수준에서 재정의할 분산 포트 그룹 정책을 선택합니다.

### 4 (선택 사항) 정책 페이지를 사용하여 각 포트 정책의 재정의를 설정합니다.

### 5 확인을 클릭합니다.

## 팀 구성 및 페일오버 정책이란?

NIC 팀 구성을 사용하면 팀에 2개 이상의 물리적 NIC를 포함하여 가상 스위치의 네트워크 용량을 늘릴 수 있습니다. 어댑터 장애 시 트래픽이 재라우팅되는 방식을 결정하려면 페일오버 순서에 물리적 NIC를 포함합니다. 가상 스위치가 팀의 물리적 NIC 간에 네트워크 트래픽을 분산하는 방식을 결정하려면 환경의 요구와 기능에 따라 로드 밸런싱 알고리즘을 선택합니다.

### NIC 팀 정책

NIC 팀 구성을 사용하여 가상 스위치를 호스트의 여러 물리적 NIC에 연결하여 스위치의 네트워크 대역폭을 늘리고 이중화 기능을 제공할 수 있습니다. NIC 팀은 멤버 간에 트래픽을 분산하고 어댑터 장애나 네트워크 중단 시 수동 페일오버를 제공할 수 있습니다. vSphere 표준 스위치에 대한 가상 스위치 또는 포트 그룹 수준에서 그리고 vSphere Distributed Switch에 대한 포트 그룹 또는 포트 수준에서 NIC 팀 구성 정책을 설정합니다.

**참고** 동일한 팀에서 물리적 스위치의 모든 포트가 동일한 계층 2 브로드캐스트 도메인에 있어야 합니다.

### 로드 밸런싱 정책

로드 밸런싱 정책은 NIC 팀의 네트워크 어댑터 간에 네트워크 트래픽이 분산되는 방식을 결정합니다. vSphere 가상 스위치는 송신 트래픽만 로드 밸런싱합니다. 들어오는 트래픽은 물리적 스위치의 로드 밸런싱 정책으로 제어됩니다.

각 로드 밸런싱 알고리즘에 대한 자세한 내용은 [가상 스위치에 사용 가능한 로드 밸런싱 알고리즘 항목](#)을 참조하십시오.

### 네트워크 장애 감지 정책

가상 스위치가 페일오버 감지를 위해 사용하는 다음 방법 중 하나를 지정할 수 있습니다.

#### 링크 상태만

네트워크 어댑터가 제공하는 링크 상태만 기준으로 합니다. 제거된 케이블 및 물리적 스위치 전원 장애와 같은 장애를 감지합니다. 그러나 링크 상태는 다음과 같은 구성 오류는 감지하지 못합니다.

- 스패닝 트리에 따라 차단되거나 올바르게 않은 VLAN으로 잘못 구성된 물리적 스위치 포트

- 물리적 스위치를 업스트림 스위치 등의 다른 네트워킹 디바이스에 연결하는 분리된 케이블

## 비콘 검색

물리적 NIC가 팀의 모든 물리적 NIC에서 연결 장애를 감지하기 위해 전송하는 이더넷 브로드캐스트 프레임 또는 신호 검색을 전송 및 수신합니다. ESXi 호스트는 1초마다 신호 패킷을 전송합니다. 신호 검색은 장애가 호스트에 대한 연결 중단 이벤트를 초래하지 않는 ESXi 호스트와 가장 가까운 물리적 스위치의 장애를 감지하는 데 가장 유용합니다.

ESXi는 단일 어댑터의 장애를 감지할 수 있으므로 NIC가 3개 이상인 팀에 신호 검색을 사용합니다. NIC가 두 개만 할당된 상태에서 둘 중 하나의 연결이 끊기면 두 NIC가 모두 신호를 받지 못해 스위치에서 서비스를 중지해야 하는 NIC를 결정할 수 없기 때문에 모든 패킷이 두 업링크에 전송됩니다. 이러한 팀에서 3개 이상의 NIC를 사용하면 모호한 상황이 발생하기 전에  $n-2$ 번의 장애가 허용됩니다. 여기서  $n$ 은 팀의 NIC 수입니다.

## 페일백 정책

기본적으로 페일백 정책은 NIC 팀에서 사용하도록 설정됩니다. 장애가 발생한 물리적 NIC가 다시 온라인으로 전환되면, 가상 스위치가 슬롯을 인계받았던 대기 NIC를 교체하여 NIC를 다시 활성 상태로 설정합니다.

페일오버 순서에서 첫 번째인 물리적 NIC에 간헐적으로 장애가 발생하는 경우 페일백 정책으로 인해 사용되는 NIC가 빈번하게 변경될 수 있습니다. 물리적 스위치는 MAC 주소의 빈번한 변경을 확인하며 어댑터가 온라인으로 전환할 때 물리적 스위치 포트가 트래픽을 즉시 수락하지 않을 수 있습니다. 이러한 지연을 최소화하려면 물리적 스위치에서 다음과 같은 설정을 변경하는 것을 고려할 수 있습니다.

- ESXi 호스트에 연결된 물리적 NIC에서 STP(스패닝 트리 프로토콜)를 사용하지 않도록 설정합니다.
- Cisco 기반 네트워크의 경우 액세스 인터페이스를 위한 PortFast 모드를 사용하도록 설정하거나 트렁크 인터페이스를 위한 PortFast 트렁크 모드를 사용하도록 설정합니다. 이에 따라 물리적 스위치 포트의 초기화 동안 약 30초가 절약될 수 있습니다.
- 트렁킹 협상을 비활성화합니다.

## 스위치 알림 정책

스위치 알림 정책을 사용하여 ESXi 호스트가 페일오버 이벤트를 전달하는 방식을 결정할 수 있습니다. 물리적 NIC가 가상 스위치에 연결되거나 트래픽이 팀의 다른 물리적 NIC로 재라우팅되는 경우 가상 스위치가 네트워크를 통해 알림을 전송하여 물리적 스위치의 조회 테이블을 업데이트합니다. 물리적 스위치에 알림 기능을 사용하면 페일오버나 vSphere vMotion을 사용한 마이그레이션이 발생할 때 지연 시간이 최소화됩니다.

## 가상 스위치에 사용 가능한 로드 밸런싱 알고리즘

가상 스위치에서 다양한 로드 밸런싱 알고리즘을 구성하여 팀의 물리적 NIC 간에 네트워크 트래픽이 분산되는 방식을 결정하는 방법을 알아봅니다.

- **원래 가상 포트 기준 라우팅**

가상 스위치는 vSphere 표준 스위치 또는 vSphere Distributed Switch의 가상 시스템 포트 ID에 따라 업링크를 선택합니다.



- **소스 MAC 해시 기준 라우팅**

가상 스위치는 가상 시스템 MAC 주소에 따라 가상 시스템에 대한 업링크를 선택합니다. 가상 시스템에 대한 업링크를 계산하기 위해 가상 스위치는 가상 시스템 MAC 주소 및 NIC 팀의 업링크 수를 사용합니다.

- **IP 해시 기준 라우팅**

가상 스위치는 각 패킷의 소스 및 대상 IP 주소를 기준으로 가상 시스템에 대한 업링크를 선택합니다.

- **물리적 NIC 로드 기준 라우팅**

물리적 NIC 로드 기준 라우팅은 원래 가상 포트를 기반으로 라우팅을 기반으로 하여, 가상 스위치가 업링크의 실제 로드를 검사하고 오버로드된 업링크에서 로드를 줄이는 단계를 수행합니다. vSphere Distributed Switch에만 사용할 수 있습니다.

- **명시적 페일오버 명령 사용**

이 정책으로 사용 가능한 실제 로드 밸런싱이 없습니다. 가상 스위치는 항상 페일오버 명령에서 활성 어댑터 목록 처음에 있으며 페일오버 감지 기준을 통과하는 업링크를 사용합니다. 활성 목록에 사용 가능한 업링크가 없는 경우 가상 스위치는 대기 목록에 있는 업링크를 사용합니다.

## 원래 가상 포트 기준 라우팅

가상 스위치는 vSphere 표준 스위치 또는 vSphere Distributed Switch의 가상 시스템 포트 ID에 따라 업링크를 선택합니다.

[원래 가상 포트 기준 라우팅]은 vSphere Standard Switch 및 vSphere Distributed Switch의 기본 로드 밸런싱 방법입니다.

ESXi 호스트에서 실행되는 각 가상 시스템에는 가상 스위치에 대한 관련 가상 포트 ID가 있습니다. 가상 시스템에 대한 업링크를 계산하기 위해 가상 스위치는 가상 시스템 포트 ID 및 NIC 팀의 업링크 수를 사용합니다. 가상 스위치가 가상 시스템에 대한 업링크를 선택한 다음에는 시스템이 동일한 포트에서 실행되는 한 항상 이 가상 시스템에 대해 동일한 업링크를 통해 트래픽을 전달합니다. 업링크가 NIC 팀에 추가되거나 NIC 팀에서 제거되지 않는 한 가상 스위치는 가상 시스템에 대한 업링크를 한 번만 계산합니다.

가상 시스템이 동일한 호스트에서 실행되는 동안 가상 시스템의 포트 ID가 고정됩니다. 가상 시스템 마이그레이션, 전원 끄기 또는 삭제를 수행하면 가상 스위치의 포트 ID가 해제됩니다. 가상 스위치가 이 포트에 트래픽을 전달하는 작업을 중지하기 때문에 관련된 업링크에 대한 전체 트래픽이 줄어듭니다. 가상 시스템의 전원을 켜거나 마이그레이션하는 경우 다른 포트에 표시되고 새 포트에 연결되는 업링크를 사용할 수 있습니다.

표 8-3. 원래 가상 포트를 기반으로 라우팅 사용 고려 사항

고려 사항	설명
장점	<ul style="list-style-type: none"> <li>가상 NIC 수가 팀의 물리적 NIC 수보다 큰 경우 트래픽이 균일하게 배포됩니다.</li> <li>대부분의 경우 가상 스위치는 가상 시스템에 대한 업링크를 한 번만 계산하기 때문에 리소스 소모가 적습니다.</li> <li>물리적 스위치는 변경하지 않아도 됩니다.</li> </ul>
단점	<ul style="list-style-type: none"> <li>가상 스위치는 업링크에 대한 트래픽 로드를 인식하지 못하기 때문에 트래픽을 덜 사용되는 업링크로 로드 밸런싱하지 않습니다.</li> <li>가상 시스템에 둘 이상의 가상 NIC가 없는 한 가상 시스템에 사용 가능한 대역폭은 관련 포트 ID에 연결된 업링크 속도로 제한됩니다.</li> </ul>

## 소스 MAC 해시 기준 라우팅

가상 스위치는 가상 시스템 MAC 주소에 따라 가상 시스템에 대한 업링크를 선택합니다. 가상 시스템에 대한 업링크를 계산하기 위해 가상 스위치는 가상 시스템 MAC 주소 및 NIC 팀의 업링크 수를 사용합니다.

표 8-4. 소스 MAC 해시 기준 라우팅 사용에 대한 고려 사항

고려 사항	설명
장점	<ul style="list-style-type: none"> <li>가상 스위치가 모든 패킷에 대해 업링크를 계산하기 때문에 원래 가상 포트를 기반으로 라우팅보다 트래픽 배포가 더 균일합니다.</li> <li>MAC 주소가 정적이기 때문에 가상 시스템이 동일한 업링크를 사용합니다. 가상 시스템의 전원을 켜거나 꺼도 가상 시스템이 사용하는 업링크가 변경되지 않습니다.</li> <li>물리적 스위치는 변경하지 않아도 됩니다.</li> </ul>
단점	<ul style="list-style-type: none"> <li>가상 시스템이 다중 소스 MAC 주소를 사용하지 않는 한 가상 시스템에 사용 가능한 대역폭이 관련 포트 ID에 연결된 업링크 속도로 제한됩니다.</li> <li>가상 스위치가 모든 패킷에 대해 업링크를 계산하기 때문에 원래 가상 포트를 기반으로 라우팅보다 리소스 소모가 많습니다.</li> <li>가상 스위치가 업링크의 로드를 인식하지 못하므로 업링크가 오버로드될 수 있습니다.</li> </ul>

## IP 해시 기준 라우팅

가상 스위치는 각 패킷의 소스 및 대상 IP 주소를 기준으로 가상 시스템에 대한 업링크를 선택합니다.

가상 스위치는 가상 시스템에 대한 업링크를 계산하기 위해 패킷의 소스 IP 주소와 대상 IP 주소의 마지막 8진수를 가져와 XOR 연산을 거친 다음 해당 결과에 대해 NIC 팀의 업링크 수를 기준으로 한 다른 계산을 실행합니다. 그 결과는 0과 팀의 업링크 수에서 1을 뺀 것 사이의 숫자입니다. 예를 들어 NIC 팀에 4개의 업링크가 있는 경우 결과는 0과 3 사이의 숫자이며 각 숫자는 팀의 NIC와 연결되어 있습니다. 비IP 패킷의 경우 가상 스위치는 IP 주소가 위치한 프레임이나 패킷에서 2개의 32비트 이진 값을 가져옵니다.

모든 가상 시스템은 소스 및 대상 IP 주소에 따라 NIC 팀의 모든 업링크를 사용할 수 있습니다. 이러한 방식으로 각 가상 시스템은 팀에 있는 모든 업링크의 대역폭을 사용할 수 있습니다. 가상 시스템이 다수의 독립형 가상 시스템이 있는 환경에서 실행되는 경우 IP 해시 알고리즘은 트래픽을 팀의 NIC 간에 일정하게 확산합니다. 가상 시스템이 여러 대상 IP 주소와 통신할 때 가상 스위치는 각 대상 IP에 대해 각기 다른 해시를 생성할 수 있습니다. 이러한 방식으로 패킷은 가상 스위치에서 각기 다른 업링크를 사용하여 더 높은 잠재적 처리량을 얻을 수 있습니다.

그러나 환경에 소수의 IP 주소가 있는 경우에는 가상 스위치가 팀의 하나의 업링크를 통해 트래픽을 일관되게 전달할 수 있습니다. 예를 들어 하나의 애플리케이션 서버가 액세스하는 데이터베이스 서버가 있는 경우 하나의 소스-대상 쌍만 존재하므로 가상 스위치는 항상 동일한 업링크를 계산합니다.

### 물리적 스위치 구성

IP 해시 로드 밸런싱이 올바르게 작동하도록 하려면 물리적 스위치에 Etherchannel이 구성되어 있어야 합니다. Etherchannel은 여러 네트워크 어댑터를 단일 논리적 링크에 결합합니다. 포트가 Etherchannel에 바인딩된 경우 물리적 스위치가 서로 다른 포트를 통해 동일한 가상 시스템 MAC 주소로부터 패킷을 수신할 때마다 스위치는 해당 CAM(내용 주소 지정 가능 메모리) 테이블을 올바르게 업데이트합니다.

예를 들어 물리적 스위치가 MAC 주소 A로부터 포트 01 및 02를 통해 패킷을 수신하는 경우 스위치는 해당 CAM 테이블에 01-A 및 02-A 항목을 만듭니다. 그 결과 물리적 스위치는 들어오는 트래픽을 올바른 포트에 분산합니다. Etherchannel을 구성하지 않은 경우, 물리적 스위치는 먼저 포트 01에서 MAC 주소 A의 패킷을 수신한다는 기록을 생성한 다음 포트 02에서 MAC 주소 A의 패킷을 수신한다고 동일한 기록을 업데이트합니다. 따라서 물리적 스위치가 들어오는 트래픽을 포트 02에만 전달하므로 패킷이 대상에 도달하지 않고 해당 업링크가 오버로드될 수 있습니다.

### 제한 사항 및 구성 요구 사항

- ESXi 호스트는 단일 물리적 스위치 또는 누적 스위치에서 IP 해시 팀 구성을 지원합니다.
- ESXi 호스트는 정적 모드에서 802.3ad 링크 집계만 지원합니다. vSphere 표준 스위치에는 정적 Etherchannel만 사용할 수 있습니다. LACP는 지원되지 않습니다. 802.3ad 링크 집계 없이 IP 해시 로드 밸런싱을 사용하도록 설정하거나 그 반대의 경우 네트워킹 중단이 발생할 수 있습니다.
- IP 해시 로드 밸런싱에서 네트워크 장애 감지로 [링크 상태만]을 사용해야 합니다.
- 활성 페일오버 목록의 팀에서 모든 업링크를 설정해야 합니다. 대기 및 사용되지 않음 목록은 비어 있어야 합니다.
- Etherchannel의 포트 수는 팀의 업링크 수와 동일해야 합니다.

## IP 해시 기준 라우팅 사용에 대한 고려 사항

고려 사항	설명
장점	<ul style="list-style-type: none"> <li>가상 스위치가 모든 패킷에 대한 업링크를 계산하므로 원래 가상 포트 기준 라우팅과 소스 MAC 해시 기준 라우팅에 비해 로드 분산이 훨씬 일정합니다.</li> <li>여러 IP 주소와 통신하는 가상 시스템에 대한 잠재적 처리량이 더 높습니다.</li> </ul>
단점	<ul style="list-style-type: none"> <li>다른 로드 밸런싱 알고리즘과 비교하여 리소스 사용량이 가장 많습니다.</li> <li>가상 스위치가 업링크의 실제 로드를 인식하지 못합니다.</li> <li>물리적 네트워크 변경이 필요합니다.</li> <li>문제 해결이 복잡합니다.</li> </ul>

## 물리적 NIC 로드 기준 라우팅

물리적 NIC 로드 기준 라우팅은 원래 가상 포트를 기반으로 라우팅을 기반으로 하여, 가상 스위치가 업링크의 실제 로드를 검사하고 오버로드된 업링크에서 로드를 줄이는 단계를 수행합니다. vSphere Distributed Switch에만 사용할 수 있습니다.

Distributed Switch는 NIC 팀의 포트 ID 및 업링크 수를 사용하여 가상 시스템에 대한 업링크를 계산합니다. Distributed Switch는 30초마다 업링크를 테스트하고 해당 로드가 사용량의 75퍼센트를 초과하는 경우 가장 높은 I/O를 가진 가상 시스템의 포트 ID를 다른 업링크로 이동합니다.

표 8-5. 물리적 NIC 로드 기준 라우팅 사용에 대한 고려 사항

고려 사항	설명
장점	<ul style="list-style-type: none"> <li>Distributed Switch가 가상 시스템에 대한 업링크를 한 번만 계산하여 업링크 검사에 최소한의 영향만 미치기 때문에 리소스 소모가 낮습니다.</li> <li>Distributed Switch가 업링크 로드를 인식하고 필요한 경우 로드를 줄입니다.</li> <li>물리적 스위치는 변경하지 않아도 됩니다.</li> </ul>
단점	<ul style="list-style-type: none"> <li>가상 시스템에 사용 가능한 대역폭이 Distributed Switch에 연결된 업링크로 제한됩니다.</li> </ul>

## 명시적 페일오버 명령 사용

이 정책으로 사용 가능한 실제 로드 밸런싱이 없습니다. 가상 스위치는 항상 페일오버 명령에서 활성 어댑터 목록 처음에 있으며 페일오버 감지 기준을 통과하는 업링크를 사용합니다. 활성 목록에 사용 가능한 업링크가 없는 경우 가상 스위치는 대기 목록에 있는 업링크를 사용합니다.

## vSphere 표준 스위치 또는 표준 포트 그룹에서 NIC 팀 구성, 페일오버 및 로드 밸런싱 구성

어댑터 장애 발생 시 네트워크 트래픽이 재라우팅되는 방식을 결정하기 위한 페일오버 순서를 구성하는 방법을 알아봅니다. vSphere 표준 스위치 또는 표준 포트 그룹의 네트워크 용량을 늘리려면 팀에 둘 이상의 물리적 NIC를

포함합니다. 로드 밸런싱 알고리즘을 선택하여 표준 스위치가 팀의 물리적 NIC 간에 트래픽을 배포하는 방법을 결정합니다.

표준 스위치의 토폴로지 및 물리적 스위치의 네트워크 구성에 따라 NIC 팀 구성, 페일오버 및 로드 밸런싱을 구성합니다. 자세한 내용은 [팀 구성 및 페일오버 정책이란?](#) 및 [가상 스위치에 사용 가능한 로드 밸런싱 알고리즘 항목](#)을 참조하십시오.

표준 스위치에서 팀 구성 및 페일오버 정책을 구성하는 경우 정책이 스위치의 모든 포트 그룹에 전파됩니다. 표준 포트 그룹에서 정책을 구성하는 경우 스위치에서 상속된 정책이 재정의됩니다.

#### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **네트워킹**을 확장하고 **가상 스위치**를 선택합니다.
- 3 표준 스위치 또는 표준 포트 그룹의 팀 구성 및 페일오버 정책으로 이동합니다.

옵션	작업
표준 스위치	<ol style="list-style-type: none"> <li>a 목록에서 스위치를 선택합니다.</li> <li>b <b>설정 편집</b>을 클릭하고 <b>팀 구성 및 페일오버</b>를 선택합니다.</li> </ol>
표준 포트 그룹	<ol style="list-style-type: none"> <li>a 포트 그룹이 있는 스위치를 선택합니다.</li> <li>b 스위치 토폴로지 다이어그램에서 표준 포트 그룹을 선택하고 <b>설정 편집</b>을 클릭합니다.</li> <li>c <b>팀 구성 및 페일오버</b>를 선택합니다.</li> <li>d 재정의하려는 정책 옆의 <b>재정의</b>를 선택합니다.</li> </ol>

- 4 **로드 밸런싱** 드롭다운 메뉴에서 가상 스위치가 팀의 물리적 NIC 간에 송신 트래픽을 로드 밸런싱하는 방법을 지정합니다.

옵션	설명
원래 가상 포트 기준 라우팅	스위치의 가상 포트 ID를 기반으로 업링크를 선택합니다. 가상 스위치가 가상 시스템 또는 VMkernel 어댑터에 대한 업링크를 선택한 후 항상 이 가상 시스템 또는 VMkernel 어댑터에 대해 동일한 업링크를 통해 트래픽을 전달합니다.
IP 해시 기준 라우팅	각 패킷의 소스 및 대상 IP 주소의 해시에 기반하여 업링크를 선택합니다. 비IP 패킷의 경우 스위치는 해당 필드의 데이터를 사용하여 해시를 계산합니다. IP 기반 팀 구성을 수행하려면 물리적 스위치가 EtherChannel로 구성되어야 합니다.
소스 MAC 해시 기준 라우팅	소스 이더넷의 해시에 기반한 업링크를 선택합니다.
명시적 페일오버 명령 사용	활성 어댑터 목록에서 항상 페일오버 검색 기준을 통과한 업링크 중 가장 높은 순서의 업링크를 사용합니다. 이 옵션을 사용하여 수행되는 실제 로드 밸런싱이 없습니다.

- 5 **네트워크 장애 감지** 드롭다운 메뉴에서 가상 스위치가 페일오버 감지에 사용하는 방법을 선택합니다.

옵션	설명
링크 상태만	네트워크 어댑터가 제공하는 링크 상태만 기준으로 합니다. 이 옵션은 제거된 케이블 및 물리적 스위치 전원 장애와 같은 장애를 감지합니다.
비콘 검색	팀의 모든 NIC에서 beacon probe를 보내고 수신하며 이 정보를 연결 상태와 함께 사용하여 연결 장애를 판단합니다.ESXi가 1초마다 비콘 패킷을 보냅니다. 사용되지 않은 상태에서는 NIC가 비콘 검색에 참여하지 않으므로 NIC는 활성/활성 또는 활성/대기 상태로 구성되어야 합니다.

- 6 **스위치 알림** 드롭다운 메뉴에서 페일오버가 발생할 경우 표준 스위치 또는 Distributed Switch를 통해 물리적 스위치에 알릴지 여부를 선택합니다.

**참고** 알림 스위치가 예로 설정된 경우에는 vCenter Server가 ESXi 호스트와 다시 연결될 때 연결된 모든 포트, 포트 그룹 및 Distributed Switch가 호스트에 다시 연결됩니다.

**참고** 연결된 가상 시스템이 Microsoft 네트워크 로드 밸런싱을 유니캐스트 모드에서 사용하고 있는 경우에는 이 옵션을 **아니요**로 설정합니다. 네트워크 로드 밸런싱이 멀티캐스트 모드에서 실행되는 경우에는 문제가 없습니다.

7

- 8 **페일백** 드롭다운 메뉴에서 장애 복구 후 물리적 어댑터가 활성 상태로 돌아오는지 여부를 선택합니다.

페일백이 예(기본 선택)로 설정된 경우 어댑터는 복구 즉시 활성 상태로 돌아가며 해당 슬롯을 인계받았던 대기 어댑터(있는 경우)를 대체합니다.

표준 포트에 대해 페일백이 **아니요**로 설정된 경우 장애가 있었던 어댑터는 복구 후에도 현재 활성 상태인 다른 어댑터에 장애가 발생하여 교체해야 할 때까지 비활성 상태로 유지됩니다.

- 9 페일오버 순서 목록을 구성하여 페일오버 발생 시 팀의 업링크가 사용되는 방식을 지정합니다.

일부 업링크만 사용하고 나머지 업링크는 사용 중인 업링크가 고장 나는 경우에 사용할 수 있도록 긴급용으로 예약하려면 위쪽 및 아래쪽 화살표 키를 사용하여 업링크를 다른 그룹으로 이동합니다.

옵션	설명
활성 어댑터	네트워크 어댑터 연결을 사용할 수 있고 활성 상태인 경우에 이 업링크를 계속 사용합니다.
대기 어댑터	활성 물리적 어댑터 중 하나가 다운 상태인 경우 이 업링크를 사용합니다.
사용되지 않은 어댑터	이 업링크를 사용하지 않습니다.

- 10 **확인**을 클릭합니다.

## 분산 포트 그룹 또는 분산 포트에서 NIC 팀 구성, 페일오버 및 로드 밸런싱 구성

어댑터 장애 발생 시 네트워크 트래픽이 재라우팅되는 방식을 결정하기 위한 페일오버 순서를 구성하는 방법을 알아봅니다. 팀에 2개 이상의 물리적 NIC를 포함하여 분산 포트 그룹 또는 포트의 네트워크 용량을 늘립니다.

Distributed Switch가 팀의 물리적 NIC 간의 트래픽을 로드 밸런싱하는 방식을 결정하기 위한 로드 밸런싱 알고리즘을 선택합니다.

물리적 스위치에 대한 네트워크 구성과 Distributed Switch의 토폴로지에 따라 NIC 팀 구성, 페일오버 및 로드 밸런싱을 구성합니다. 자세한 내용은 [팀 구성 및 페일오버 정책이란?](#) 및 [가상 스위치에 사용 가능한 로드 밸런싱 알고리즘](#) 항목을 참조하십시오.

분산 포트 그룹에 대한 팀 구성 및 페일오버 정책을 구성하는 경우 정책이 그룹의 모든 포트에 전파됩니다. 분산 포트에 대한 정책을 구성하는 경우 그룹에서 상속된 정책을 재정의합니다.

**참고** 페일백 옵션 설정은 **물리적 NIC 로드 기준 라우팅** 팀 구성 정책에서 지원되지 않습니다.

#### 사전 요구 사항

분산 포트 수준에서 정책을 재정의하려면 이 정책에 대해 포트 수준 재정의 옵션을 사용하도록 설정합니다. [포트 수준에서 네트워킹 정책 재정의 구성](#)의 내용을 참조하십시오.

#### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 분산 포트 그룹 또는 포트의 팀 구성 및 페일오버 정책을 탐색합니다.

옵션	작업
분산 포트 그룹	<ol style="list-style-type: none"> <li>a 작업 메뉴에서 <b>분산 포트 그룹 &gt; 분산 포트 그룹 관리</b>를 선택합니다.</li> <li>b 포트 그룹을 선택하고 <b>다음</b>을 클릭합니다.</li> <li>c <b>팀 구성 및 페일오버</b>를 선택합니다.</li> </ol>
분산 포트	<ol style="list-style-type: none"> <li>a <b>네트워크</b> 탭에서 <b>분산 포트 그룹</b>을 클릭하고 원하는 분산 포트 그룹을 두 번 클릭합니다.</li> <li>b <b>포트</b> 탭에서 포트를 선택하고 <b>분산 포트 설정을 편집합니다</b>를 클릭합니다.</li> <li>c <b>팀 구성 및 페일오버</b>를 선택합니다.</li> <li>d 재정의할 속성 옆의 <b>재정의</b>를 선택합니다.</li> </ol>

- 3 **로드 밸런싱** 드롭다운 메뉴에서 가상 스위치가 팀의 물리적 NIC 간에 송신 트래픽을 로드 밸런싱하는 방법을 지정합니다.

옵션	설명
원래 가상 포트 기준 라우팅	스위치의 가상 포트 ID를 기반으로 업링크를 선택합니다. 가상 스위치가 가상 시스템 또는 VMkernel 어댑터에 대한 업링크를 선택한 후 항상 이 가상 시스템 또는 VMkernel 어댑터에 대해 동일한 업링크를 통해 트래픽을 전달합니다.
IP 해시 기준 라우팅	각 패킷의 소스 및 대상 IP 주소의 해시에 기반하여 업링크를 선택합니다. 비IP 패킷의 경우 스위치는 해당 필드의 데이터를 사용하여 해시를 계산합니다. IP 기반 팀 구성을 수행하려면 물리적 스위치가 EtherChannel로 구성되어야 합니다.
소스 MAC 해시 기준 라우팅	소스 이더넷의 해시에 기반한 업링크를 선택합니다.

옵션	설명
물리적 NIC 로드 기준 라우팅	분산 포트 그룹 또는 분산 포트에 사용 가능합니다. 포트 그룹 또는 포트에 연결된 물리적 네트워크 어댑터의 현재 로드에서 기반하여 업링크를 선택합니다. 업링크가 30초 동안 75% 이상 사용 중인 경우 호스트 프록시 스위치가 가상 시스템 트래픽의 일부를 사용할 수 있는 물리적 어댑터로 이동합니다.  <b>참고</b> 물리적 NIC 로드 기준 라우팅을 선택하면 분산 포트 그룹에 대한 페일백 옵션을 설정할 수 없습니다.
명시적 페일오버 명령 사용	활성 어댑터 목록에서 항상 페일오버 검색 기준을 통과한 업링크 중 가장 높은 순서의 업링크를 사용합니다. 이 옵션을 사용하여 수행되는 실제 로드 밸런싱이 없습니다.

#### 4 네트워크 장애 감지 드롭다운 메뉴에서 가상 스위치가 페일오버 감지에 사용하는 방법을 선택합니다.

옵션	설명
링크 상태만	네트워크 어댑터가 제공하는 링크 상태만 기준으로 합니다. 이 옵션은 제거된 케이블 및 물리적 스위치 전원 장애와 같은 장애를 감지합니다.
비콘 검색	팀의 모든 NIC에서 beacon probe를 보내고 수신하며 이 정보를 연결 상태와 함께 사용하여 연결 장애를 판단합니다. ESXi가 1초마다 비콘 패킷을 보냅니다.  사용되지 않은 상태에서는 NIC가 비콘 검색에 참여하지 않으므로 NIC는 활성/활성 또는 활성/대기 상태로 구성되어야 합니다.

#### 5 스위치 알림 드롭다운 메뉴에서 페일오버가 발생할 경우 표준 스위치 또는 Distributed Switch를 통해 물리적 스위치에 알릴지 여부를 선택합니다.

**참고** 알림 스위치가 예로 설정된 경우에는 vCenter Server가 ESXi 호스트와 다시 연결될 때 연결된 모든 포트, 포트 그룹 및 Distributed Switch가 호스트에 다시 연결됩니다.

**참고** 연결된 가상 시스템이 Microsoft 네트워크 로드 밸런싱을 유니캐스트 모드에서 사용하고 있는 경우에는 이 옵션을 **아니오**로 설정합니다. 네트워크 로드 밸런싱이 멀티캐스트 모드에서 실행되는 경우에는 문제가 없습니다.

#### 6 페일백 드롭다운 메뉴에서 장애 복구 후 물리적 어댑터가 활성 상태로 돌아오는지 여부를 선택합니다.

페일백이 예(기본 선택)로 설정된 경우 어댑터는 복구 즉시 활성 상태로 돌아가며 해당 슬롯을 인계받았던 대기 어댑터(있는 경우)를 대체합니다.

분산 포트에 대해 페일백이 **아니오**로 설정된 경우 장애가 있었던 어댑터는 복구 후 연결된 가상 시스템이 실행 중인 경우에만 비활성 상태로 유지됩니다. **페일백** 옵션이 **아니오**이고 가상 시스템의 전원이 꺼져 있으면 모든 활성 물리적 어댑터에 장애가 발생한 다음 그 중 하나가 복구되는 경우 가상 시스템의 전원이 켜진 후 가상 NIC가 대기 어댑터 대신 복구된 어댑터에 연결됩니다. 가상 시스템의 전원을 껐다가 켜면 가상 NIC가 분산 포트에 다시 연결됩니다. Distributed Switch는 이 포트를 새로 추가된 것으로 간주하고 포트에 기본 업링크 포트, 즉 활성 업링크 어댑터를 할당합니다.



7 페일오버 순서 목록을 구성하여 페일오버 발생 시 팀의 업링크가 사용되는 방식을 지정합니다.

일부 업링크만 사용하고 나머지 업링크는 사용 중인 업링크가 고장 나는 경우에 사용할 수 있도록 긴급용으로 예약하려면 위쪽 및 아래쪽 화살표 키를 사용하여 업링크를 다른 그룹으로 이동합니다.

옵션	설명
활성 어댑터	네트워크 어댑터 연결을 사용할 수 있고 활성 상태인 경우에 이 업링크를 계속 사용합니다.
대기 어댑터	활성 물리적 어댑터 중 하나가 다운 상태인 경우 이 업링크를 사용합니다.
사용되지 않은 어댑터	이 업링크를 사용하지 않습니다.

8 설정을 검토하고 구성을 적용합니다.

## VLAN 정책이란?

VLAN 정책은 네트워크 환경에서 VLAN이 작동하는 방식을 결정합니다.

VLAN(Virtual Local Area Network)은 공통적인 요구 사항 집합을 가진 호스트의 그룹으로 해당하는 물리적 위치에 상관없이 동일한 브로드캐스트 도메인에 연결된 것처럼 통신합니다. VLAN은 물리적 LAN(Local Area Network)과 특성이 동일하지만 최종 스테이션을 동일한 네트워크 스위치에 있는지 여부와 관계없이 그룹화할 수 있습니다.

VLAN 정책의 범위는 분산 포트 그룹 및 분산 포트와 업링크 포트 그룹 및 업링크 포트일 수 있습니다.

## 분산 포트 그룹 또는 분산 포트에서 VLAN 태그 지정 구성

모든 분산 포트에 전체적으로 VLAN 태그 지정을 적용하려면 분산 포트 그룹에서 VLAN 정책을 설정해야 합니다. 상위 분산 포트 그룹과 다른 방식으로 포트의 가상 트래픽을 물리적 VLAN과 통합하려면 분산 포트에서 VLAN 정책을 사용해야 합니다.

### 사전 요구 사항

분산 포트 수준에서 정책을 재정의하려면 이 정책에 대해 포트 수준 재정의 옵션을 사용하도록 설정합니다. **포트 수준에서 네트워킹 정책 재정의 구성**의 내용을 참조하십시오.

### 절차

1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.

## 2 분산 포트 그룹 또는 분산 포트에 대한 VLAN 정책으로 이동합니다.

옵션	작업
분산 포트 그룹	a 작업 메뉴에서 <b>분산 포트 그룹 &gt; 분산 포트 그룹 관리</b> 를 선택합니다. b <b>VLAN</b> 을 선택하고 <b>다음</b> 을 클릭합니다. c 포트 그룹을 선택하고 <b>다음</b> 을 클릭합니다.
분산 포트	a <b>네트워크</b> 탭에서 <b>분산 포트 그룹</b> 을 클릭하고 원하는 분산 포트 그룹을 두 번 클릭합니다. b <b>포트</b> 탭에서 포트를 선택하고 <b>분산 포트 설정을 편집합니다</b> 아이콘을 클릭합니다. c <b>VLAN</b> 을 선택합니다. d 재정의할 속성 옆의 <b>재정의</b> 를 선택합니다.

## 3 VLAN 유형 드롭다운 메뉴에서 VLAN 트래픽 필터링 및 표시 유형을 선택하고 다음을 클릭합니다.

옵션	설명
없음	VLAN을 사용하지 않습니다. EST(External Switch Tagging)의 경우 이 옵션을 사용합니다.
VLAN	<b>VLAN ID</b> 필드의 ID를 사용하여 트래픽에 태그를 지정합니다. VST(Virtual Switch Tagging)의 경우 1에서 4094 사이의 숫자를 입력합니다.
VLAN 트렁킹	<b>VLAN 트렁크 범위</b> 내의 ID를 사용하여 VLAN 트래픽을 게스트 운영 체제로 전달합니다. 침표로 구분된 목록을 사용하여 여러 개의 범위와 개별 VLAN을 설정할 수 있습니다. 예를 들어 1702-1705, 1848-1849와 같이 입력합니다. VGT(Virtual Guest Tagging)의 경우 이 옵션을 사용합니다.
전용 VLAN	트래픽을 Distributed Switch에서 생성된 전용 VLAN과 연결합니다.

## 4 설정을 검토하고 구성을 적용합니다.

### 업링크 포트 그룹 또는 업링크 포트에 VLAN 태그 지정 구성

모든 멤버 업링크에 대해 VLAN 트래픽 처리를 일반적으로 구성하려면 업링크 포트에서 VLAN 정책을 설정해야 합니다. 상위 업링크 포트 그룹과 다른 방식으로 포트를 통해 VLAN 트래픽을 처리하려면 업링크에서 VLAN 정책을 설정해야 합니다.

트래픽 필터링을 위해 업링크 포트 수준의 VLAN 정책을 사용하여 VLAN ID의 트렁크 범위를 물리적 네트워크 어댑터로 전파합니다. VLAN을 기준으로 필터링을 지원할 경우 물리적 네트워크 어댑터가 다른 VLAN의 패킷을 삭제합니다. 트렁크 범위를 설정하면 물리적 네트워크 어댑터가 그룹의 업링크 포트 대신 트래픽을 필터링하므로 네트워킹 성능이 향상됩니다.

물리적 네트워크 어댑터가 VLAN 필터링을 지원하지 않을 경우 VLAN이 차단되지 않을 수 있습니다. 이 경우 분산 포트 그룹 또는 분산 포트에서 VLAN 필터링을 구성합니다.

VLAN 필터링 지원에 대한 자세한 내용은 어댑터 벤더의 기술 설명서를 참조하십시오.

## 사전 요구 사항

포트 수준에서 VLAN 정책을 재정의하려면 포트 수준 재정의의 사용하도록 설정하십시오. [포트 수준에서 네트워킹 정책 재정의 구성](#)의 내용을 참조하십시오.

## 절차

- 1 vSphere Client에서 Distributed Switch로 이동합니다.
- 2 **네트워크** 탭에서 **업링크 포트 그룹**을 클릭합니다.
- 3 업링크 포트 그룹 또는 포트에 대한 VLAN 정책으로 이동합니다.

옵션	작업
업링크 포트 그룹	<ol style="list-style-type: none"> <li>a 목록에서 업링크 포트 그룹을 마우스 오른쪽 버튼으로 클릭하고 <b>설정 편집</b>을 선택합니다.</li> <li>b <b>VLAN</b>을 클릭합니다.</li> </ol>
업링크 포트	<ol style="list-style-type: none"> <li>a 업링크 포트 그룹을 두 번 클릭합니다.</li> <li>b <b>포트</b> 탭에서 포트를 선택하고 <b>분산 포트 설정을 편집합니다</b> 탭을 클릭합니다.</li> <li>c <b>VLAN</b>을 클릭하고 <b>재정의</b>를 선택합니다.</li> </ol>

- 4 물리적 네트워크 어댑터에 전파할 **VLAN 트렁크 범위** 값을 입력합니다.  
여러 개의 범위와 개별 VLAN에 대한 트렁크 범위를 지정하는 경우 쉼표로 각 항목을 구분합니다.
- 5 **확인**을 클릭합니다.

## 보안 정책이란?

네트워킹 보안 정책은 MAC 주소 가장 행위 및 원치 않는 포트 검색으로부터 트래픽을 보호합니다.

표준 스위치 또는 Distributed Switch의 보안 정책은 네트워크 프로토콜 스택의 계층 2(데이터 링크 계층)에서 구현됩니다. 보안 정책의 세 가지 요소는 비규칙(promiscuous) 모드, MAC 주소 변경 및 위조 전송입니다. 잠재적인 네트워킹 위협에 대한 자세한 내용은 "vSphere 보안" 설명서를 참조하십시오.

## vSphere 표준 스위치 또는 표준 포트 그룹에 대한 보안 정책 구성

가상 시스템의 게스트 운영 체제에서 vSphere 표준 스위치에 대해 MAC 주소 및 비규칙(Promiscuous) 모드 변경을 거부하는 보안 정책을 구성할 수 있습니다. 개별 포트 그룹의 표준 스위치에서 상속되는 보안 정책을 재정의할 수 있습니다.

## 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 **구성** 탭에서 **네트워킹**을 확장하고 **가상 스위치**를 선택합니다.

## 3 표준 스위치 또는 포트 그룹에 대한 보안 정책으로 이동합니다.

옵션	작업
vSphere 표준 스위치	<ul style="list-style-type: none"> <li>a 목록에서 표준 스위치를 선택합니다.</li> <li>b <b>설정 편집</b>을 클릭합니다.</li> <li>c <b>보안</b>을 선택합니다.</li> </ul>
표준 포트 그룹	<ul style="list-style-type: none"> <li>a 포트 그룹이 있는 표준 스위치를 선택합니다.</li> <li>b 토폴로지 다이어그램에서 표준 포트 그룹을 선택합니다.</li> <li>c <b>설정 편집</b>을 클릭합니다.</li> <li>d <b>보안</b>을 선택하고 재정의할 옵션 옆의 <b>재정의</b>를 선택합니다.</li> </ul>

## 4 표준 스위치 또는 포트 그룹에 연결된 가상 시스템의 게스트 운영 체제에서 비규칙(Promiscuous) 모드 활성화 또는 MAC 주소 변경을 거부하거나 수락합니다.

옵션	설명
무차별 모드	<ul style="list-style-type: none"> <li>■ <b>거부.</b> VM 네트워크 어댑터가 가상 시스템에 전송된 프레임만 수신합니다.</li> <li>■ <b>동의.</b> 가상 스위치가 VM 네트워크 어댑터가 연결된 포트에 대한 활성 VLAN 정책에 따라 모든 프레임을 가상 시스템에 전달합니다.</li> </ul> <p><b>참고</b> 무차별 모드는 안전하지 않은 작업 모드입니다. 방화벽, 포트 스캐너, 침입 감지 시스템이 무차별 모드로 실행되어야 합니다.</p>
MAC 주소 변경	<ul style="list-style-type: none"> <li>■ <b>거부.</b> 게스트 운영 체제가 가상 시스템의 유효 MAC 주소를 VM 네트워크 어댑터의 MAC 주소와 다른 값으로 변경하는 경우 스위치가 어댑터에 대한 모든 인바운드 프레임을 삭제합니다.</li> </ul> <p>게스트 운영 체제가 가상 시스템의 유효 MAC 주소를 VM 네트워크 어댑터의 MAC 주소로 다시 변경하는 경우 가상 시스템이 프레임을 다시 수신합니다.</p> <ul style="list-style-type: none"> <li>■ <b>동의.</b> 게스트 운영 체제가 가상 시스템의 유효 MAC 주소를 VM 네트워크 어댑터의 MAC 주소와 다른 값으로 변경하는 경우 스위치가 프레임을 새 주소에 전달할 수 있도록 허용합니다.</li> </ul>
위조 전송	<ul style="list-style-type: none"> <li>■ <b>거부.</b> 소스 MAC 주소가 .vmx 구성 파일에 있는 주소와 다를 경우 스위치가 가상 시스템 어댑터에서 모든 아웃바운드 프레임을 삭제합니다.</li> <li>■ <b>동의.</b> 스위치가 필터링을 수행하지 않고 모든 아웃바운드 프레임을 허용합니다.</li> </ul>
상태	MAC 학습 기능을 사용하거나 사용하지 않도록 설정합니다. 기본값은 사용 안 함입니다.
유니캐스트 플러딩 허용	포트에서 수신한 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 MAC 학습이 사용되도록 설정된 경우 기본적으로 사용되도록 설정됩니다.

옵션	설명
MAC 제한	학습할 수 있는 MAC 주소 수는 구성 가능합니다. 최대값은 포트당 4096(기본값)입니다.
MAC 제한 정책	MAC 제한에 도달한 경우에 대한 정책입니다. 옵션은 다음과 같습니다. <ul style="list-style-type: none"> <li>■ 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.</li> <li>■ 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.</li> </ul>

5 **확인**을 클릭합니다.

## 분산 포트 그룹 또는 분산 포트에 대한 보안 정책 구성

포트 그룹과 연결된 가상 시스템의 게스트 운영 체제에서 비규칙 모드 및 MAC 주소 변경을 허용하거나 거부하도록 분산 포트 그룹에 보안 정책을 설정하는 방법을 알아봅니다. 개별 포트의 분산 포트 그룹에서 상속된 보안 정책을 재정의할 수 있습니다.

### 사전 요구 사항

분산 포트 수준에서 정책을 재정의하려면 이 정책에 대해 포트 수준 재정의 옵션을 사용하도록 설정합니다. [포트 수준에서 네트워킹 정책 재정의 구성](#)의 내용을 참조하십시오.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 분산 포트 그룹 또는 포트에 대한 보안 정책으로 이동합니다.

옵션	작업
분산 포트 그룹	<ol style="list-style-type: none"> <li>a 작업 메뉴에서 <b>분산 포트 그룹 &gt; 분산 포트 그룹 관리</b>를 선택합니다.</li> <li>b <b>보안</b>을 선택하고 <b>다음</b>을 클릭합니다.</li> <li>c 포트 그룹을 선택하고 <b>다음</b>을 클릭합니다.</li> </ol>
분산 포트	<ol style="list-style-type: none"> <li>a <b>네트워크</b> 탭에서 <b>분산 포트 그룹</b>을 클릭하고 원하는 분산 포트 그룹을 두 번 클릭합니다.</li> <li>b <b>포트</b> 탭에서 포트를 선택하고 <b>설정 편집</b> 아이콘을 클릭합니다.</li> <li>c <b>보안</b>을 선택합니다.</li> <li>d 재정의할 속성 옆의 <b>재정의</b>를 선택합니다.</li> </ol>

- 3 분산 포트 그룹 또는 포트에 연결된 가상 시스템의 게스트 운영 체제에서 비규칙(Promiscuous) 모드 활성화 또는 MAC 주소 변경을 거부하거나 수락합니다.

옵션	설명
무차별 모드	<ul style="list-style-type: none"> <li>■ <b>거부.</b> VM 네트워크 어댑터가 가상 시스템에 전송된 프레임만 수신합니다.</li> <li>■ <b>동의.</b> 가상 스위치가 VM 네트워크 어댑터가 연결된 포트에 대한 활성 VLAN 정책에 따라 모든 프레임을 가상 시스템에 전달합니다.</li> </ul> <p><b>참고</b> 무차별 모드는 안전하지 않은 작업 모드입니다. 방화벽, 포트 스캐너, 침입 감지 시스템이 무차별 모드로 실행되어야 합니다.</p>
MAC 주소 변경	<ul style="list-style-type: none"> <li>■ <b>거부.</b> 게스트 운영 체제가 가상 시스템의 유효 MAC 주소를 VM 네트워크 어댑터의 MAC 주소와 다른 값으로 변경하는 경우 스위치가 어댑터에 대한 모든 인바운드 프레임을 삭제합니다.</li> </ul> <p>게스트 운영 체제가 가상 시스템의 유효 MAC 주소를 VM 네트워크 어댑터의 MAC 주소로 다시 변경하는 경우 가상 시스템이 프레임을 다시 수신합니다.</p> <ul style="list-style-type: none"> <li>■ <b>동의.</b> 게스트 운영 체제가 가상 시스템의 유효 MAC 주소를 VM 네트워크 어댑터의 MAC 주소와 다른 값으로 변경하는 경우 스위치가 프레임을 새 주소에 전달할 수 있도록 허용합니다.</li> </ul>
위조 전송	<ul style="list-style-type: none"> <li>■ <b>거부.</b> 소스 MAC 주소가 .vmx 구성 파일에 있는 주소와 다를 경우 스위치가 가상 시스템 어댑터에서 모든 아웃바운드 프레임을 삭제합니다.</li> <li>■ <b>동의.</b> 스위치가 필터링을 수행하지 않고 모든 아웃바운드 프레임을 허용합니다.</li> </ul>
상태	MAC 학습 기능을 사용하거나 사용하지 않도록 설정합니다. 기본값은 사용 안 함입니다.
유니캐스트 플러딩 허용	포트에서 수신한 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 MAC 학습이 사용되도록 설정된 경우 기본적으로 사용되도록 설정됩니다.
MAC 제한	학습할 수 있는 MAC 주소 수는 구성 가능합니다. 최대값은 포트당 4096(기본값)입니다.
MAC 제한 정책	MAC 제한에 도달한 경우에 대한 정책입니다. 옵션은 다음과 같습니다. <ul style="list-style-type: none"> <li>■ <b>삭제</b> - 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.</li> <li>■ <b>허용</b> - 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.</li> </ul>

- 4 설정을 검토하고 구성을 적용합니다.

## 트래픽 조절 정책이란?

트래픽 조절 정책은 평균 대역폭, 최대 대역폭 및 버스트 크기에 의해 정의됩니다. 각 포트 그룹과 각 분산 포트 또는 분산 포트 그룹에 대한 트래픽 조절 정책을 설정할 수 있습니다.

ESXi는 표준 스위치에서 아웃바운드 네트워크 트래픽을 조절하고 Distributed Switch에서 인바운드 및 아웃바운드 트래픽을 조절합니다. 트래픽 조절은 포트에 사용 가능한 네트워크 대역폭을 제한하지만, 버스트 트래픽이 더 높은 속도로 통과하는 것을 허용하도록 구성할 수도 있습니다.

### 평균 대역폭

평균적으로 포트를 통과할 수 있는 초당 비트 수를 설정합니다. 이 숫자는 허용되는 평균 로드입니다.

### 최대 대역폭

트래픽 버스트를 송신 또는 수신할 때 포트를 통과할 수 있는 초당 최대 비트 수입니다. 이 숫자는 추가 버스트를 사용할 때 포트에서 사용하는 대역폭을 제한합니다.

### 버스트 크기

버스트에 허용할 최대 바이트 수입니다. 이 매개 변수를 설정하면 할당된 대역폭의 일부만 사용되는 경우 포트에 추가 버스트가 제공될 수 있습니다. 추가 버스트를 사용할 수 있는 경우, 평균 대역폭에서 지정한 것보다 더 많은 대역폭이 포트에 필요할 때 일시적으로 더 높은 속도로 데이터를 전송할 수 있습니다. 이 매개 변수는 추가 버스트에서 누적된 바이트 수를 제한하기 때문에 더 높은 속도로 전송됩니다.

## vSphere 표준 스위치 또는 표준 포트 그룹의 트래픽 조절 구성

ESXi에서는 표준 스위치 또는 포트 그룹의 아웃바운드 트래픽을 조절할 수 있습니다. 트래픽 조절기는 모든 포트의 사용 가능한 네트워크 대역폭을 제한하지만, 일시적으로 버스트 트래픽이 더 높은 속도로 포트를 통과하는 것을 허용하도록 구성할 수도 있습니다.

스위치 또는 포트 그룹 수준에서 설정하는 트래픽 조절 정책은 스위치 또는 포트 그룹에 참여하는 각 개별 포트에서 적용됩니다. 예를 들어 표준 포트 그룹에 대해 100000Kbps의 평균 대역폭을 설정하는 경우 평균 초당 12500KB의 데이터가 표준 포트 그룹과 연결된 각 포트를 통과할 수 있습니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 네트워킹을 확장하고 가상 스위치를 선택합니다.
- 3 표준 스위치 또는 포트 그룹에 대한 트래픽 조절 정책으로 이동합니다.

옵션	작업
vSphere 표준 스위치	<ol style="list-style-type: none"> <li>a 목록에서 표준 스위치를 선택합니다.</li> <li>b 설정 편집을 클릭합니다.</li> <li>c 트래픽 조절을 선택합니다.</li> </ol>
표준 포트 그룹	<ol style="list-style-type: none"> <li>a 포트 그룹이 있는 표준 스위치를 선택합니다.</li> <li>b 토폴로지 다이어그램에서 표준 포트 그룹을 선택합니다.</li> <li>c 설정 편집을 클릭합니다.</li> <li>d 트래픽 조절을 선택하고 재정의할 옵션 옆의 재정의를 선택합니다.</li> </ol>

#### 4 트래픽 조절 정책을 구성합니다.

옵션	설명
상태	표준 스위치 또는 포트 그룹과 연결된 각 포트에 대해 할당된 네트워킹 대역폭 양에 대한 제한 설정을 사용하도록 설정합니다.
평균 대역폭	포트를 통과할 수 있는 평균 초당 비트 수, 즉 허용되는 평균 로드를 설정합니다.
최대 대역폭	트래픽 버스트를 송신할 때 포트를 통과할 수 있는 초당 최대 비트 수입니다. 포트가 추가 버스트를 사용할 때마다 이 설정은 포트에서 사용하는 대역폭보다 커집니다. 이 매개 변수는 평균 대역폭보다 작을 수 없습니다.
버스트 크기	버스트에 허용할 최대 바이트 수입니다. 이 매개 변수를 설정하면 할당된 대역폭의 일부만 사용될 때 포트에 추가 버스트가 제공될 수 있습니다. 추가 버스트를 사용할 수 있는 경우 포트는 포트에 평균 대역폭에서 지정한 것보다 더 많은 대역폭이 필요할 때마다 일시적으로 더 높은 속도로 데이터를 전송할 수 있습니다. 이 매개 변수는 추가 버스트에서 누적될 수 있는 바이트 수의 상한값을 지정하기 때문에 더 높은 속도로 전송될 수 있습니다.

5 각 트래픽 조절 정책(**평균 대역폭**, **최대 대역폭** 및 **버스트 크기**)에 대해 대역폭 값을 입력합니다.

6 **확인**을 클릭합니다.

### 분산 포트 그룹 또는 분산 포트의 트래픽 조절 정책 편집

vSphere 분산 포트 그룹 또는 분산 포트에서 인바운드 트래픽과 아웃바운드 트래픽을 모두 조절할 수 있습니다. 트래픽 조절기는 그룹의 모든 포트에 대한 네트워크 대역폭을 제한하지만, 일시적으로 "버스트" 트래픽이 더 높은 속도로 포트를 통과하는 것을 허용하도록 구성할 수도 있습니다.

분산 포트 그룹 수준에서 설정하는 트래픽 조절 정책은 포트 그룹에 참여하는 각 개별 포트에 적용됩니다. 예를 들어 분산 포트 그룹에 대해 100000Kbps의 평균 대역폭을 설정하는 경우 평균 초당 100000KB의 데이터가 분산 포트 그룹과 연결된 각 포트를 통과할 수 있습니다.

#### 사전 요구 사항

분산 포트 수준에서 정책을 재정의하려면 이 정책에 대해 포트 수준 재정의 옵션을 사용하도록 설정합니다. [포트 수준에서 네트워킹 정책 재정의 구성](#)의 내용을 참조하십시오.

#### 절차

1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.



## 2 분산 포트 그룹 또는 포트에 대한 트래픽 조절 정책으로 이동합니다.

옵션	작업
분산 포트 그룹	a 작업 메뉴에서 <b>분산 포트 그룹 &gt; 분산 포트 그룹 관리</b> 를 선택합니다. b <b>트래픽 조절</b> 을 선택하고 <b>다음</b> 을 클릭합니다. c 포트 그룹을 선택하고 <b>다음</b> 을 클릭합니다.
분산 포트	a <b>네트워크</b> 탭에서 <b>분산 포트 그룹</b> 을 클릭하고 원하는 분산 포트 그룹을 두 번 클릭합니다. b <b>포트</b> 탭에서 포트를 선택하고 <b>분산 포트 설정을 편집합니다</b> 아이콘을 클릭합니다. c <b>트래픽 조절</b> 을 선택합니다. d 재정의할 속성 옆의 <b>재정의</b> 를 선택합니다.

## 3 트래픽 조절 정책을 구성합니다.

**참고** 트래픽은 호스트가 아닌 Distributed Switch에서 트래픽 방향에 따라 수신 및 송신으로 분류됩니다.

옵션	설명
상태	상태 드롭다운 메뉴를 사용하여 <b>수신 트래픽 조절</b> 또는 <b>송신 트래픽 조절</b> 을 사용하도록 설정합니다.
평균 대역폭	포트를 통과할 수 있는 평균 초당 비트 수, 즉 허용되는 평균 로드를 설정합니다.
최대 대역폭	트래픽 버스트를 송신/수신 또는 수신할 때 포트를 통과할 수 있는 초당 최대 비트 수입니다. 포트가 추가 버스트를 사용할 때마다 이 매개 변수는 포트에서 사용하는 대역폭보다 커 집니다.
버스트 크기	버스트에 허용할 최대 바이트 수입니다. 이 매개 변수를 설정하면 할당된 대역폭의 일부만 사용될 때 포트에 추가 버스트가 제공될 수 있습니다. 추가 버스트를 사용할 수 있는 경우 평균 대역폭에서 지정한 것보다 더 많은 대역폭이 포트에 필요할 때마다 포트는 일시적으로 더 높은 속도로 데이터를 전송할 수 있습니다. 이 매개 변수는 추가 버스트에서 누적될 수 있는 바이트 수의 상한값을 지정하기 때문에 더 높은 속도로 전송됩니다.

## 4 설정을 검토하고 구성을 적용합니다.

## 리소스 할당 정책이란?

리소스 할당 정책을 사용하면 분산 포트 또는 포트 그룹을 사용자가 생성한 네트워크 리소스 풀과 연결할 수 있습니다. 이 정책을 사용하면 포트 또는 포트 그룹에 지정된 대역폭을 보다 강력하게 제어할 수 있습니다.

네트워크 리소스 풀 생성 및 구성에 대한 자세한 내용은 [장 11 vSphere Network I/O Control](#) 항목을 참조하십시오.

## 분산 포트 그룹의 리소스 할당 정책 편집

분산 포트 그룹을 네트워크 리소스 풀에 연결하면 분산 포트 그룹에 지정된 대역폭을 보다 효과적으로 제어하는 방법을 알아봅니다.

### 사전 요구 사항

- Distributed Switch에서 Network I/O Control을 사용하도록 설정합니다. [vSphere Distributed Switch에서 Network I/O Control 사용](#)의 내용을 참조하십시오.
- 네트워크 리소스 풀을 생성 및 구성합니다. [네트워크 리소스 풀 생성](#)의 내용을 참조하십시오.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 탐색기에서 Distributed Switch를 마우스 오른쪽 버튼으로 클릭하고 **분산 포트 그룹 > 분산 포트 그룹 관리**를 선택합니다.
- 3 **리소스 할당** 확인란을 선택하고 **다음**을 클릭합니다.
- 4 구성할 분산 포트 그룹을 선택하고 **다음**을 클릭합니다.
- 5 네트워크 리소스 풀에서 분산 포트 그룹을 추가하거나 제거하고 **다음**을 클릭합니다.
  - 분산 포트 그룹을 추가하려면 **네트워크 리소스 풀** 드롭다운 메뉴에서 사용자 정의 리소스 풀을 선택합니다.
  - 분산 포트 그룹을 제거하려면 **네트워크 리소스 풀** 드롭다운 메뉴에서 **기본값**을 선택합니다.
- 6 **완료 준비** 섹션에서 설정을 검토하고 **마침**을 클릭합니다.  
 설정을 변경하려면 **뒤로** 버튼을 사용합니다.

## 모니터링 정책이란?

모니터링 정책은 분산 포트 또는 포트 그룹에 대한 NetFlow 모니터링을 사용하거나 사용하지 않도록 설정합니다.

NetFlow 설정은 vSphere Distributed Switch 수준에서 구성됩니다. [vSphere Distributed Switch의 NetFlow 설정 구성](#)의 내용을 참조하십시오.

## 분산 포트 그룹 또는 분산 포트에서 NetFlow 모니터링 관리

분산 포트 그룹의 포트 또는 개별 분산 포트를 통과하는 IP 패킷을 모니터링하도록 NetFlow를 구성하는 방법을 알아봅니다.

vSphere Distributed Switch에서 NetFlow 설정을 구성할 수 있습니다. [vSphere Distributed Switch의 NetFlow 설정 구성](#)의 내용을 참조하십시오.

### 사전 요구 사항

분산 포트 수준에서 정책을 재정의하려면 이 정책에 대해 포트 수준 재정의 옵션을 사용하도록 설정합니다. [포트 수준에서 네트워킹 정책 재정의 구성](#)의 내용을 참조하십시오.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.

2 분산 포트 그룹 또는 분산 포트에 대한 모니터링 정책으로 이동합니다.

옵션	작업
분산 포트 그룹	a 작업 메뉴에서 <b>분산 포트 그룹 &gt; 분산 포트 그룹 관리</b> 를 선택합니다. b <b>모니터링</b> 을 선택하고 <b>다음</b> 을 클릭합니다. c 포트 그룹을 선택하고 <b>다음</b> 을 클릭합니다.
분산 포트	a <b>네트워크</b> 탭에서 <b>분산 포트 그룹</b> 을 클릭하고 원하는 분산 포트 그룹을 두 번 클릭합니다. b <b>포트</b> 탭에서 포트를 선택하고 <b>분산 포트 설정을 편집합니다</b> 아이콘을 클릭합니다. c <b>모니터링</b> 을 선택합니다. d 재정의할 속성 옆의 <b>재정의</b> 를 선택합니다.

3 NetFlow 드롭다운 메뉴에서 **사용** 또는 **사용 안 함**을 선택하고 **다음**을 클릭합니다.

4 설정을 확인하고 구성을 적용합니다.

## 트래픽 필터링 및 표시 정책이란?

vSphere Distributed Switch에서 트래픽 필터링 및 표시 정책을 사용하여 원하지 않는 트래픽과 보안 공격으로부터 가상 네트워크를 보호하거나 특정 유형의 트래픽에 QoS 태그를 적용할 수 있습니다.

트래픽 필터링 및 표시 정책은 Distributed Switch 포트를 통하는 데이터 흐름의 보안 및 QoS 태그 지정을 위한 순서가 지정된 일련의 네트워크 트래픽 규칙입니다. 일반적으로 이 규칙은 트래픽 한정자와, 일치하는 트래픽을 제한하거나 우선 순위를 부여하기 위한 작업으로 구성됩니다.

vSphere Distributed Switch는 데이터 스트림의 다양한 위치에서 트래픽에 규칙을 적용합니다. Distributed Switch는 가상 시스템 네트워크 어댑터 및 분산 포트 사이의 데이터 경로에 트래픽 필터 규칙을 적용하거나, 업링크 포트 및 물리적 네트워크 어댑터 사이의 데이터 경로에 업링크 규칙을 적용합니다. 트래픽 필터링 및 표시 정책은 네트워크 오프로드 호환성으로 구성된 vSphere Distributed Switch를 지원하지 않습니다.

## 분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 필터링 및 표시

분산 포트 그룹 또는 업링크 포트 그룹 수준의 트래픽 규칙을 설정하여 가상 시스템, VMkernel 어댑터 또는 물리적 어댑터를 통하는 트래픽 액세스에 대해 필터링 및 우선 순위 태깅을 적용할 수 있습니다.

### ■ 분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 필터링 및 표시 사용

포트 그룹에서 트래픽 필터링 및 표시 정책을 사용하여 그룹에 참여하는 모든 가상 시스템 네트워크 어댑터 또는 업링크 어댑터에 트래픽 보안 및 표시를 구성할 수 있습니다.

### ■ 분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 표시

VoIP 및 스트리밍 비디오와 같이 대역폭, 낮은 지연 시간 등 네트워킹 요구 사항이 더 높은 트래픽에 우선 순위 태그를 할당하는 방법을 알아봅니다. 네트워크 프로토콜 스택의 계층 2에 CoS 태그를 사용하거나 계층 3에 DSCP 태그를 사용하여 트래픽을 표시할 수 있습니다.

- **분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 필터링**  
분산 포트 그룹 또는 업링크 포트 그룹의 포트를 통해 흐르는 데이터를 보호하기 위해 트래픽을 허용하거나 중지하는 방법을 알아봅니다.
- **분산 포트 그룹 또는 업링크 포트 그룹의 네트워크 트래픽 규칙**  
분산 포트 그룹 또는 업링크 포트 그룹에서 트래픽 규칙을 정의하여 가상 시스템 또는 물리적 어댑터와 관련된 트래픽을 처리하는 정책을 적용하는 방법을 알아봅니다. 특정 트래픽을 필터링하거나 해당 QoS 요구 사항을 명시할 수 있습니다.
- **분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 필터링 및 표시 사용 안 함**  
트래픽 필터링 및 표시 정책을 사용하지 않도록 설정하여 보안 또는 QoS와 관련된 추가적인 제어 없이 트래픽을 가상 시스템 또는 물리적 어댑터로 흐르도록 하는 방법을 알아봅니다.

## 분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 필터링 및 표시 사용

포트 그룹에서 트래픽 필터링 및 표시 정책을 사용하여 그룹에 참여하는 모든 가상 시스템 네트워크 어댑터 또는 업링크 어댑터에 트래픽 보안 및 표시를 구성할 수 있습니다.

---

**참고** 특정 포트에서 트래픽 필터링 및 표시 정책을 사용하지 않도록 설정하여 포트를 통하는 트래픽 흐름이 처리되는 것을 방지할 수 있습니다. [분산 포트 또는 업링크 포트의 트래픽 필터링 및 표시 사용 안 함](#)의 내용을 참조하십시오

---

**참고** 트래픽 필터링 및 표시 정책은 네트워크 오프로드 기능으로 구성된 vSphere Distributed Switch를 지원하지 않습니다.

---

### 절차

- 1 vSphere Client에서 분산 포트 그룹 또는 업링크 포트 그룹을 찾습니다.
  - a Distributed Switch를 선택하고 **네트워크** 탭을 클릭합니다.
  - b **분산 포트 그룹**을 클릭하여 분산 포트 그룹 목록을 확인하거나 **업링크 포트 그룹**을 클릭하여 업링크 포트 그룹 목록을 확인합니다.
- 2 분산 포트 그룹 또는 업링크 포트 그룹을 클릭하고 **구성** 탭을 선택합니다.
- 3 [설정]에서 **트래픽 필터링 및 표시**를 선택합니다.
- 4 **사용 및 순서 변경** 버튼을 클릭합니다.
- 5 **모든 트래픽 규칙 사용**을 클릭합니다.
- 6 **확인**을 클릭합니다.

### 다음에 수행할 작업

분산 포트 그룹의 포트를 통해 또는 업링크 포트 그룹을 통해 흐르는 데이터에 대해 트래픽 표시 및 필터링을 설정합니다. [분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 표시 및 분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 필터링 항목](#)을 참조하십시오.

## 분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 표시

VoIP 및 스트리밍 비디오와 같이 대역폭, 낮은 지연 시간 등 네트워킹 요구 사항이 더 높은 트래픽에 우선 순위 태그를 할당하는 방법을 알아봅니다. 네트워크 프로토콜 스택의 계층 2에 CoS 태그를 사용하거나 계층 3에 DSCP 태그를 사용하여 트래픽을 표시할 수 있습니다.

우선 순위 태깅은 QoS 요구가 더 높은 트래픽을 표시하기 위한 메커니즘입니다. 이 방식으로 네트워크는 서로 다른 클래스의 트래픽을 인식할 수 있습니다. 네트워크 디바이스는 해당 우선 순위 및 요구 사항에 따라 각 클래스의 트래픽을 처리할 수 있습니다.

또한 트래픽을 다시 태그 처리하여 흐름의 중요도를 높이거나 낮출 수 있습니다. 낮은 QoS 태그를 사용하면 게스트 운영 체제에서 태그 처리된 데이터를 제한할 수 있습니다.

### 절차

- 1 vSphere Client에서 분산 포트 그룹 또는 업링크 포트 그룹을 찾습니다.
  - a Distributed Switch를 선택하고 **네트워크** 탭을 클릭합니다.
  - b **분산 포트 그룹**을 클릭하여 분산 포트 그룹 목록을 확인하거나 **업링크 포트 그룹**을 클릭하여 업링크 포트 그룹 목록을 확인합니다.
- 2 분산 포트 그룹 또는 업링크 포트 그룹을 클릭하고 **구성** 탭을 선택합니다.
- 3 [설정]에서 **트래픽 필터링 및 표시**를 선택합니다.
- 4 트래픽 필터링 및 표시가 사용되지 않도록 설정된 경우 **사용 및 순서 변경 > 모든 트래픽 규칙 사용 > 확인**을 클릭합니다.
- 5 **추가**를 클릭하여 새 규칙을 생성하거나, 규칙을 선택하고 **편집**을 클릭하여 규칙을 편집합니다.
- 6 네트워크 트래픽 규칙 대화상자의 **작업** 드롭다운 메뉴에서 **태그** 옵션을 선택합니다.
- 7 규칙의 범위 내에서 트래픽의 우선 순위 태그를 설정합니다.

옵션	설명
CoS 값	네트워크 계층 2의 CoS 우선 순위 태그와 규칙이 일치하는 트래픽을 표시합니다. 확인란을 선택하고 0~7 사이에서 값을 입력합니다.
DSCP 값	네트워크 계층 3의 DSCP 태그와 규칙이 연결된 트래픽을 표시합니다. 확인란을 선택하고 0~63 사이에서 값을 입력합니다.

## 8 규칙을 적용할 수 있는 트래픽 종류를 지정합니다.

데이터 흐름이 표시 또는 필터링할 규칙의 범위 내에 있는지 확인하기 위해 vSphere Distributed Switch는 트래픽의 방향, 소스/대상과 같은 속성, VLAN, 다음 수준 프로토콜, 인프라 트래픽 유형 등을 검토합니다.

- a **트래픽 방향** 드롭다운 메뉴에서 규칙과 일치하는 것으로 인식하도록 트래픽을 수신, 송신 또는 수신/송신 해야 하는지를 선택합니다.

또한 방향은 트래픽 소스 및 대상을 식별하는 방법에 영향을 줍니다.

- b 시스템 데이터 유형, 계층 2 패킷 특성 및 계층 3 패킷 특성의 한정자를 사용하여 규칙을 일치시켜야 하는 패킷의 속성을 설정합니다.

한정자는 네트워킹 계층과 관련된 일치 기준의 집합을 나타냅니다. 시스템 데이터 유형, 계층 2 트래픽 속성 및 계층 3 트래픽 속성에 트래픽을 일치시킬 수 있습니다. 특정 네트워킹 계층에 맞는 한정자를 사용하거나 한정자를 결합하여 패킷을 더 정확히 일치시킬 수 있습니다.

- 시스템 트래픽 한정자를 사용하여 그룹의 포트를 통과하고 있는 가상 인프라 데이터의 유형에 패킷을 일치시킵니다. 예를 들면 NFS를 선택하여 네트워크 스토리지로 데이터를 전송할 수 있습니다.
- MAC 트래픽 한정자를 사용하여 MAC 주소, VLAN ID 및 다음 수준 프로토콜을 기준으로 패킷을 일치시킵니다.

분산 포트 그룹에서 VLAN ID로 트래픽을 찾을 때 VGT(Virtual Guest Tagging)를 사용할 수 있습니다. VST(Virtual Switch Tagging)가 활성 상태인 경우 트래픽을 VLAN ID에 일치시키려면 업링크 포트 그룹이나 업링크 포트의 규칙을 사용합니다.

- IP 트래픽 한정자를 사용하여 IP 버전, IP 주소, 다음 수준 프로토콜 및 포트를 기준으로 패킷을 일치시킵니다.

## 9 규칙 대화상자에서 **확인**을 클릭하여 규칙을 저장합니다.

### 예제: VoIP 트래픽 표시

VoIP(Voice over IP) 흐름에는 낮은 손실 및 지연과 관련하여 QoS에 대한 특별 요구 사항이 있습니다. VoIP의 SIP(Session Initiation Protocol) 관련 트래픽에는 주로 26의 값을 가지는 DSCP 태그가 있으며, 이는 낮은 삭제 확률의 Assured Forwarding Class 3(AF31)을 나타냅니다.

예를 들어 서브넷 192.168.2.0/24로 나가는 SIP UDP 패킷을 표시하려면 다음 규칙을 사용합니다.

규칙 매개 변수	매개 변수 값
작업	태그
DSCP 값	26
트래픽 방향	송신
트래픽 한정자	IP 한정자
프로토콜	UDP
대상 포트	5060
소스 주소	IP 주소는 접두사 길이 24인 192.168.2.0과 일치합니다.

## 분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 필터링

분산 포트 그룹 또는 업링크 포트 그룹의 포트를 통해 흐르는 데이터를 보호하기 위해 트래픽을 허용하거나 중지하는 방법을 알아봅니다.

### 절차

- 1 vSphere Client에서 분산 포트 그룹 또는 업링크 포트 그룹을 찾습니다.
  - a Distributed Switch를 선택하고 **네트워크** 탭을 클릭합니다.
  - b **분산 포트 그룹**을 클릭하여 분산 포트 그룹 목록을 확인하거나 **업링크 포트 그룹**을 클릭하여 업링크 포트 그룹 목록을 확인합니다.
- 2 분산 포트 그룹 또는 업링크 포트 그룹을 클릭하고 **구성** 탭을 선택합니다.
- 3 [설정]에서 **트래픽 필터링 및 표시**를 선택합니다.
- 4 트래픽 필터링 및 표시가 사용되지 않도록 설정된 경우 **사용 및 순서 변경 > 모든 트래픽 규칙 사용 > 확인**을 클릭합니다.
- 5 **추가**를 클릭하여 새 규칙을 생성하거나, 규칙을 선택하고 **편집**을 클릭하여 규칙을 편집합니다.
- 6 네트워크 트래픽 규칙 대화상자에서 작업 옵션을 사용하여 트래픽이 분산 포트 그룹 또는 업링크 포트 그룹의 포트를 통과하도록 허용하거나 이를 제한합니다.

## 7 규칙을 적용할 수 있는 트래픽 종류를 지정합니다.

데이터 흐름이 표시 또는 필터링할 규칙의 범위 내에 있는지 확인하기 위해 vSphere Distributed Switch는 트래픽의 방향, 소스/대상과 같은 속성, VLAN, 다음 수준 프로토콜, 인프라 트래픽 유형 등을 검토합니다.

- a **트래픽 방향** 드롭다운 메뉴에서 규칙과 일치하는 것으로 인식하도록 트래픽을 수신, 송신 또는 수신/송신 해야 하는지를 선택합니다.

또한 방향은 트래픽 소스 및 대상을 식별하는 방법에 영향을 줍니다.

- b 시스템 데이터 유형, 계층 2 패킷 특성 및 계층 3 패킷 특성의 한정자를 사용하여 규칙을 일치시켜야 하는 패킷의 속성을 설정합니다.

한정자는 네트워킹 계층과 관련된 일치 기준의 집합을 나타냅니다. 시스템 데이터 유형, 계층 2 트래픽 속성 및 계층 3 트래픽 속성에 트래픽을 일치시킬 수 있습니다. 특정 네트워킹 계층에 맞는 한정자를 사용하거나 한정자를 결합하여 패킷을 더 정확히 일치시킬 수 있습니다.

- 시스템 트래픽 한정자를 사용하여 그룹의 포트를 통과하고 있는 가상 인프라 데이터의 유형에 패킷을 일치시킵니다. 예를 들면 NFS를 선택하여 네트워크 스토리지로 데이터를 전송할 수 있습니다.
- MAC 트래픽 한정자를 사용하여 MAC 주소, VLAN ID 및 다음 수준 프로토콜을 기준으로 패킷을 일치시킵니다.

분산 포트 그룹에서 VLAN ID로 트래픽을 찾을 때 VGT(Virtual Guest Tagging)를 사용할 수 있습니다. VST(Virtual Switch Tagging)가 활성 상태인 경우 트래픽을 VLAN ID에 일치시키려면 업링크 포트 그룹이나 업링크 포트의 규칙을 사용합니다.

- IP 트래픽 한정자를 사용하여 IP 버전, IP 주소, 다음 수준 프로토콜 및 포트를 기준으로 패킷을 일치시킵니다.

## 8 규칙 대화상자에서 **확인**을 클릭하여 규칙을 저장합니다.

### 분산 포트 그룹 또는 업링크 포트 그룹의 네트워크 트래픽 규칙

분산 포트 그룹 또는 업링크 포트 그룹에서 트래픽 규칙을 정의하여 가상 시스템 또는 물리적 어댑터와 관련된 트래픽을 처리하는 정책을 적용하는 방법을 알아봅니다. 특정 트래픽을 필터링하거나 해당 QoS 요구 사항을 명시할 수 있습니다.

**참고** 포트 수준에서 트래픽 필터링 및 표시에 대한 정책의 규칙을 재정의할 수 있습니다. [분산 포트 또는 업링크 포트의 네트워크 트래픽 규칙](#)의 내용을 참조하십시오.

#### ■ [분산 포트 그룹 또는 업링크 그룹의 트래픽 규칙 보기](#)

분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 필터링 및 표시 정책을 구성하는 트래픽 규칙을 볼 수 있습니다.

#### ■ [분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 규칙 편집](#)

트래픽 규칙을 생성 또는 편집하고 해당 매개 변수를 사용하여 분산 포트 그룹 또는 업링크 포트 그룹에서 트래픽을 필터링하거나 표시하기 위한 정책을 구성하는 방법을 알아봅니다.



- **분산 포트 그룹 또는 업링크 포트 그룹의 규칙 우선 순위 수정**

분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 필터링 및 표시 정책을 구성하는 규칙의 순서를 변경하여 트래픽 처리를 위한 작업 순서를 변경하는 방법을 알아봅니다.

- **분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 규칙 삭제**

분산 포트 그룹이나 업링크 포트 그룹에서 트래픽 규칙을 삭제하여 가상 시스템 또는 물리적 어댑터에 특정 방식으로 전송되는 패킷의 처리를 중지하는 방법을 알아봅니다.

### 분산 포트 그룹 또는 업링크 그룹의 트래픽 규칙 보기

분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 필터링 및 표시 정책을 구성하는 트래픽 규칙을 볼 수 있습니다.

#### 절차

- 1 vSphere Client에서 분산 포트 그룹 또는 업링크 포트 그룹을 찾습니다.
  - a Distributed Switch를 선택하고 **네트워크** 탭을 클릭합니다.
  - b **분산 포트 그룹**을 클릭하여 분산 포트 그룹 목록을 확인하거나 **업링크 포트 그룹**을 클릭하여 업링크 포트 그룹 목록을 확인합니다.
- 2 분산 포트 그룹 또는 업링크 포트 그룹을 클릭하고 **구성** 탭을 선택합니다.
- 3 [설정]에서 **트래픽 필터링 및 표시**를 선택합니다.
- 4 트래픽 필터링 및 표시가 사용되지 않도록 설정된 경우 **사용 및 순서 변경 > 모든 트래픽 규칙 사용 > 확인**을 클릭합니다.
- 5 **작업**을 검토하여 규칙이 특별한 QoS 요구 사항이 있는 트래픽을 필터링(허용 또는 삭제)하거나 표시(태그)하는지 확인합니다.
- 6 상위 목록에서 트래픽을 찾을 수 있는 기준을 보려는 규칙을 선택합니다.  
트래픽 한정자 목록에 규칙의 트래픽 한정 매개 변수가 나타납니다.

### 분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 규칙 편집

트래픽 규칙을 생성 또는 편집하고 해당 매개 변수를 사용하여 분산 포트 그룹 또는 업링크 포트 그룹에서 트래픽을 필터링하거나 표시하기 위한 정책을 구성하는 방법을 알아봅니다.

#### 절차

- 1 vSphere Client에서 분산 포트 그룹 또는 업링크 포트 그룹을 찾습니다.
  - a Distributed Switch를 선택하고 **네트워크** 탭을 클릭합니다.
  - b **분산 포트 그룹**을 클릭하여 분산 포트 그룹 목록을 확인하거나 **업링크 포트 그룹**을 클릭하여 업링크 포트 그룹 목록을 확인합니다.
- 2 분산 포트 그룹 또는 업링크 포트 그룹을 클릭하고 **구성** 탭을 선택합니다.
- 3 [설정]에서 **트래픽 필터링 및 표시**를 선택합니다.

- 4 트래픽 필터링 및 표시가 사용되지 않도록 설정된 경우 **사용 및 순서 변경 > 모든 트래픽 규칙 사용 > 확인**을 클릭합니다.
- 5 **추가**를 클릭하여 새 규칙을 생성하거나, 규칙을 선택하고 **편집**을 클릭하여 규칙을 편집합니다.

#### 다음에 수행할 작업

네트워크 트래픽 규칙 이름을 지정하고 대상 트래픽을 거부, 허용 또는 태그 처리합니다.

#### 분산 포트 그룹 또는 업링크 포트 그룹의 규칙 우선 순위 수정

분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 필터링 및 표시 정책을 구성하는 규칙의 순서를 변경하여 트래픽 처리를 위한 작업 순서를 변경하는 방법을 알아봅니다.

vSphere Distributed Switch는 엄격하게 순서대로 네트워크 트래픽 규칙을 적용합니다. 패킷이 이미 규칙을 충족하는 경우 정책의 다음 규칙으로 패킷이 전달되지 않을 수 있습니다.

#### 절차

- 1 vSphere Client에서 분산 포트 그룹 또는 업링크 포트 그룹을 찾습니다.
  - a Distributed Switch를 선택하고 **네트워크** 탭을 클릭합니다.
  - b **분산 포트 그룹**을 클릭하여 분산 포트 그룹 목록을 확인하거나 **업링크 포트 그룹**을 클릭하여 업링크 포트 그룹 목록을 확인합니다.
- 2 분산 포트 그룹 또는 업링크 포트 그룹을 클릭하고 **구성** 탭을 선택합니다.
- 3 [설정]에서 **트래픽 필터링 및 표시**를 선택합니다.
- 4 **사용 및 순서 변경** 버튼을 클릭합니다.
- 5 트래픽 필터링 및 표시가 사용되지 않도록 설정된 경우 **모든 트래픽 규칙 사용**을 클릭하여 사용되도록 설정합니다.
- 6 규칙을 선택하고 **위로 이동** 또는 **아래로 이동** 버튼을 사용하여 규칙의 우선 순위를 변경합니다.
- 7 **확인**을 클릭하여 변경 사항을 적용합니다.

#### 분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 규칙 삭제

분산 포트 그룹이나 업링크 포트 그룹에서 트래픽 규칙을 삭제하여 가상 시스템 또는 물리적 어댑터에 특정 방식으로 전송되는 패킷의 처리를 중지하는 방법을 알아봅니다.

#### 절차

- 1 vSphere Client에서 분산 포트 그룹 또는 업링크 포트 그룹을 찾습니다.
  - a Distributed Switch를 선택하고 **네트워크** 탭을 클릭합니다.
  - b **분산 포트 그룹**을 클릭하여 분산 포트 그룹 목록을 확인하거나 **업링크 포트 그룹**을 클릭하여 업링크 포트 그룹 목록을 확인합니다.
- 2 분산 포트 그룹 또는 업링크 포트 그룹을 클릭하고 **구성** 탭을 선택합니다.

- 3 [설정]에서 **트래픽 필터링 및 표시**를 선택합니다.
- 4 트래픽 필터링 및 표시가 사용되지 않도록 설정된 경우 **사용 및 순서 변경 > 모든 트래픽 규칙 사용 > 확인**을 클릭합니다.
- 5 규칙을 선택하고 **삭제** 버튼을 클릭합니다.
- 6 **확인**을 클릭합니다.

## 분산 포트 그룹 또는 업링크 포트 그룹의 트래픽 필터링 및 표시 사용 안 함

트래픽 필터링 및 표시 정책을 사용하지 않도록 설정하여 보안 또는 QoS와 관련된 추가적인 제어 없이 트래픽을 가상 시스템 또는 물리적 어댑터로 흐르도록 하는 방법을 알아봅니다.

**참고** 특정 포트에 트래픽 필터링 및 표시 정책을 사용하고 설정할 수 있습니다. **분산 포트 또는 업링크 포트의 트래픽 필터링 및 표시 사용** 항목을 참조하십시오.

### 절차

- 1 vSphere Client에서 분산 포트 그룹 또는 업링크 포트 그룹을 찾습니다.
  - a Distributed Switch를 선택하고 **네트워크** 탭을 클릭합니다.
  - b **분산 포트 그룹**을 클릭하여 분산 포트 그룹 목록을 확인하거나 **업링크 포트 그룹**을 클릭하여 업링크 포트 그룹 목록을 확인합니다.
- 2 분산 포트 그룹 또는 업링크 포트 그룹을 클릭하고 **구성** 탭을 선택합니다.
- 3 [설정]에서 **트래픽 필터링 및 표시**를 선택합니다.
- 4 **사용 및 순서 변경** 버튼을 클릭합니다.
- 5 전환 버튼을 사용하여 모든 트래픽 규칙을 사용하지 않도록 설정합니다.
- 6 **확인**을 클릭합니다.

## 분산 포트 또는 업링크 포트의 트래픽 필터링 및 표시

분산 포트 또는 업링크 포트에 트래픽 필터링 및 표시 정책을 구성하여 트래픽을 필터링하거나 개별 가상 시스템, VMkernel 어댑터 또는 물리적 어댑터에 대한 QoS 요구 사항을 명시하는 방법을 알아봅니다.

### ■ 분산 포트 또는 업링크 포트의 트래픽 필터링 및 표시 사용

포트에서 트래픽 필터링 및 표시 정책을 사용하여 가상 시스템 네트워크 어댑터, VMkernel 어댑터 또는 업링크 어댑터에서 트래픽 보안 및 표시를 구성할 수 있습니다. 트래픽 필터링 및 표시 정책은 네트워크 오프로드 호환성으로 구성된 vSphere Distributed Switch를 지원하지 않습니다.

### ■ 분산 포트 또는 업링크 포트의 트래픽 표시

VoIP 및 스트리밍 비디오와 같이 특별한 처리가 필요한 트래픽의 규칙에 우선 순위 태그를 할당할 수 있습니다. 네트워크 프로토콜 스택의 계층 2에 CoS 태그를 사용하거나 계층 3에 DSCP 태그를 사용하여 가상 시스템, VMkernel 어댑터 또는 물리적 어댑터의 트래픽을 표시할 수 있습니다.

- **분산 포트 또는 업링크 포트에 대한 트래픽 필터링**  
규칙을 통해 트래픽을 허용하거나 중지하여 가상 시스템, VMkernel 어댑터 또는 물리적 어댑터를 통하는 데이터 흐름을 보호할 수 있습니다.
- **분산 포트 또는 업링크 포트의 네트워크 트래픽 규칙**  
분산 포트 또는 업링크 포트 그룹에서 트래픽 규칙을 정의하여 가상 시스템 또는 물리적 어댑터와 관련된 트래픽을 처리하는 정책을 적용하는 방법을 알아봅니다. 특정 트래픽을 필터링하거나 해당 QoS 요구 사항을 명시할 수 있습니다.
- **분산 포트 또는 업링크 포트의 트래픽 필터링 및 표시 사용 안 함**  
포트에서 트래픽 필터링 및 표시 정책을 사용하지 않도록 설정하여 보안 필터링 또는 QoS 표시 없이 트래픽이 가상 시스템 또는 물리적 어댑터로 흐르도록 합니다.

## 분산 포트 또는 업링크 포트의 트래픽 필터링 및 표시 사용

포트에서 트래픽 필터링 및 표시 정책을 사용하여 가상 시스템 네트워크 어댑터, VMkernel 어댑터 또는 업링크 어댑터에서 트래픽 보안 및 표시를 구성할 수 있습니다. 트래픽 필터링 및 표시 정책은 네트워크 오프로드 호환성으로 구성된 vSphere Distributed Switch를 지원하지 않습니다.

### 사전 요구 사항

분산 포트 수준에서 정책을 재정의하려면 이 정책에 대해 포트 수준 재정의 옵션을 사용하도록 설정합니다. **포트 수준에서 네트워킹 정책 재정의 구성**의 내용을 참조하십시오.

### 절차

- 1 Distributed Switch로 이동한 다음 분산 포트 또는 업링크 포트에 이동합니다.
  - 스위치의 분산 포트에 이동하려면 **네트워크 > 분산 포트 그룹**을 클릭하고 목록에서 분산 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
  - 업링크 포트 그룹의 업링크 포트에 이동하려면 **네트워크 > 업링크 포트 그룹**을 클릭하고 목록에서 업링크 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
- 2 목록에서 포트를 선택합니다.
- 3 **트래픽 필터링 및 표시** 탭을 선택합니다.
- 4 **사용 및 순서 변경** 버튼을 클릭합니다.
- 5 전환 버튼을 사용하여 기본 설정을 재정의합니다.
- 6 (선택 사항) **모든 트래픽 규칙 사용**을 클릭합니다.  
그룹 수준에서 트래픽 규칙을 사용하도록 설정한 경우 포트에 대한 기본 설정을 재정의하면 트래픽 규칙이 자동으로 사용되도록 설정됩니다.
- 7 **확인**을 클릭합니다.

## 다음에 수행할 작업

분산 포트 또는 업링크 포트를 통하는 데이터 흐름에 대해 트래픽 필터링 또는 표시를 설정합니다. [분산 포트 또는 업링크 포트의 트래픽 표시](#) 및 [분산 포트 또는 업링크 포트에 대한 트래픽 필터링](#) 항목을 참조하십시오.

## 분산 포트 또는 업링크 포트의 트래픽 표시

VoIP 및 스트리밍 비디오와 같이 특별한 처리가 필요한 트래픽의 규칙에 우선 순위 태그를 할당할 수 있습니다. 네트워크 프로토콜 스택의 계층 2에 CoS 태그를 사용하거나 계층 3에 DSCP 태그를 사용하여 가상 시스템, VMkernel 어댑터 또는 물리적 어댑터의 트래픽을 표시할 수 있습니다.

우선 순위 태깅은 QoS 요구가 더 높은 트래픽을 표시하기 위한 메커니즘입니다. 이 방식으로 네트워크는 서로 다른 클래스의 트래픽을 인식할 수 있습니다. 네트워크 디바이스는 해당 우선 순위 및 요구 사항에 따라 각 클래스의 트래픽을 처리할 수 있습니다.

또한 트래픽을 다시 태그 처리하여 흐름의 중요도를 높이거나 낮출 수 있습니다. 낮은 QoS 태그를 사용하면 게스트 운영 체제에서 태그 처리된 데이터를 제한할 수 있습니다.

### 사전 요구 사항

분산 포트 수준에서 정책을 재정의하려면 이 정책에 대해 포트 수준 재정의 옵션을 사용하도록 설정합니다. [포트 수준에서 네트워킹 정책 재정의 구성](#)의 내용을 참조하십시오.

### 절차

- Distributed Switch로 이동한 다음 분산 포트 또는 업링크 포트에 이동합니다.
  - 스위치의 분산 포트에 이동하려면 **네트워크 > 분산 포트 그룹**을 클릭하고 목록에서 분산 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
  - 업링크 포트 그룹의 업링크 포트에 이동하려면 **네트워크 > 업링크 포트 그룹**을 클릭하고 목록에서 업링크 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
- 목록에서 포트를 선택합니다.
- 트래픽 필터링 및 표시** 탭을 선택합니다.
- 포트 수준에서 [트래픽 필터링 및 표시]가 사용되지 않도록 설정된 경우 [사용 및 순서 변경] 버튼을 클릭하고 기본 설정을 재정의한 다음 **모든 트래픽 규칙 사용**을 클릭합니다.
 

그룹 수준에서 트래픽 규칙을 사용하도록 설정한 경우 포트에 대한 기본 설정을 재정의하면 트래픽 규칙이 자동으로 사용되도록 설정됩니다.
- 추가**를 클릭하여 새 규칙을 생성하거나, 규칙을 선택하고 **편집**을 클릭하여 규칙을 편집합니다.
 

분산 포트 그룹이나 업링크 포트 그룹에서 상속된 규칙을 변경할 수 있습니다. 그러면 규칙이 포트 범위 내에서 고유해집니다.
- 네트워크 트래픽 규칙 대화상자의 **작업** 드롭다운 메뉴에서 **태그** 옵션을 선택합니다.

## 7 규칙의 범위 내에서 트래픽의 우선 순위 태그를 설정합니다.

옵션	설명
CoS 값	네트워크 계층 2의 CoS 우선 순위 태그와 규칙이 일치하는 트래픽을 표시합니다. 확인란을 선택하고 0-7 사이에서 값을 입력합니다.
DSCP 값	네트워크 계층 3의 DSCP 태그와 규칙이 연결된 트래픽을 표시합니다. 확인란을 선택하고 0-63 사이에서 값을 입력합니다.

## 8 규칙을 적용할 수 있는 트래픽 종류를 지정합니다.

데이터 흐름이 표시 또는 필터링할 규칙의 범위 내에 있는지 확인하기 위해 vSphere Distributed Switch는 트래픽의 방향, 소스/대상과 같은 속성, VLAN, 다음 수준 프로토콜, 인프라 트래픽 유형 등을 검토합니다.

- a **트래픽 방향** 드롭다운 메뉴에서 규칙과 일치하는 것으로 인식하도록 트래픽을 수신, 송신 또는 수신/송신해야 하는지를 선택합니다.

또한 방향은 트래픽 소스 및 대상을 식별하는 방법에 영향을 줍니다.

- b 시스템 데이터 유형, 계층 2 패킷 특성 및 계층 3 패킷 특성의 한정자를 사용하여 규칙을 일치시켜야 하는 패킷의 속성을 설정합니다.

한정자는 네트워킹 계층과 관련된 일치 기준의 집합을 나타냅니다. 시스템 데이터 유형, 계층 2 트래픽 속성 및 계층 3 트래픽 속성에 트래픽을 일치시킬 수 있습니다. 특정 네트워킹 계층에 맞는 한정자를 사용하거나 한정자를 결합하여 패킷을 더 정확히 일치시킬 수 있습니다.

- 시스템 트래픽 한정자를 사용하여 그룹의 포트를 통과하고 있는 가상 인프라 데이터의 유형에 패킷을 일치시킵니다. 예를 들면 NFS를 선택하여 네트워크 스토리지로 데이터를 전송할 수 있습니다.
- MAC 트래픽 한정자를 사용하여 MAC 주소, VLAN ID 및 다음 수준 프로토콜을 기준으로 패킷을 일치시킵니다.

분산 포트 그룹에서 VLAN ID로 트래픽을 찾을 때 VGT(Virtual Guest Tagging)를 사용할 수 있습니다. VST(Virtual Switch Tagging)가 활성 상태인 경우 트래픽을 VLAD ID에 일치시키려면 업링크 포트 그룹이나 업링크 포트의 규칙을 사용합니다.

- IP 트래픽 한정자를 사용하여 IP 버전, IP 주소, 다음 수준 프로토콜 및 포트를 기준으로 패킷을 일치시킵니다.

## 9 규칙 대화상자에서 **확인**을 클릭하여 규칙을 저장합니다.

### 분산 포트 또는 업링크 포트에 대한 트래픽 필터링

규칙을 통해 트래픽을 허용하거나 중지하여 가상 시스템, VMkernel 어댑터 또는 물리적 어댑터를 통하는 데이터 흐름을 보호할 수 있습니다.

#### 사전 요구 사항

분산 포트 수준에서 정책을 재정의하려면 이 정책에 대해 포트 수준 재정의 옵션을 사용하도록 설정합니다. [포트 수준에서 네트워킹 정책 재정의 구성](#)의 내용을 참조하십시오.

## 절차

- 1 Distributed Switch로 이동한 다음 분산 포트 또는 업링크 포트에 이동합니다.
  - 스위치의 분산 포트에 이동하려면 **네트워크 > 분산 포트 그룹**을 클릭하고 목록에서 분산 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
  - 업링크 포트 그룹의 업링크 포트에 이동하려면 **네트워크 > 업링크 포트 그룹**을 클릭하고 목록에서 업링크 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
- 2 목록에서 포트를 선택합니다.
- 3 **트래픽 필터링 및 표시** 탭을 선택합니다.
- 4 포트 수준에서 [트래픽 필터링 및 표시]가 사용되지 않도록 설정된 경우 [사용 및 순서 변경] 버튼을 클릭하고 기본 설정을 재정의한 다음 **모든 트래픽 규칙 사용**을 클릭합니다.  
 그룹 수준에서 트래픽 규칙을 사용하도록 설정한 경우 포트에 대한 기본 설정을 재정의하면 트래픽 규칙이 자동으로 사용되도록 설정됩니다.
- 5 **추가**를 클릭하여 새 규칙을 생성하거나, 규칙을 선택하고 **편집**을 클릭하여 규칙을 편집합니다.  
 분산 포트 그룹이나 업링크 포트 그룹에서 상속된 규칙을 변경할 수 있습니다. 그러면 규칙이 포트 범위 내에서 고유해집니다.
- 6 네트워크 트래픽 규칙 대화상자에서 트래픽이 분산 포트 또는 업링크 포트를 통과하도록 하려면 **허용** 작업을 선택하고, 통과하지 못하도록 제한하려면 **삭제** 작업을 선택합니다.

## 7 규칙을 적용할 수 있는 트래픽 종류를 지정합니다.

데이터 흐름이 표시 또는 필터링할 규칙의 범위 내에 있는지 확인하기 위해 vSphere Distributed Switch는 트래픽의 방향, 소스/대상과 같은 속성, VLAN, 다음 수준 프로토콜, 인프라 트래픽 유형 등을 검토합니다.

- a **트래픽 방향** 드롭다운 메뉴에서 규칙과 일치하는 것으로 인식하도록 트래픽을 수신, 송신 또는 수신/송신 해야 하는지를 선택합니다.

또한 방향은 트래픽 소스 및 대상을 식별하는 방법에 영향을 줍니다.

- b 시스템 데이터 유형, 계층 2 패킷 특성 및 계층 3 패킷 특성의 한정자를 사용하여 규칙을 일치시켜야 하는 패킷의 속성을 설정합니다.

한정자는 네트워킹 계층과 관련된 일치 기준의 집합을 나타냅니다. 시스템 데이터 유형, 계층 2 트래픽 속성 및 계층 3 트래픽 속성에 트래픽을 일치시킬 수 있습니다. 특정 네트워킹 계층에 맞는 한정자를 사용하거나 한정자를 결합하여 패킷을 더 정확히 일치시킬 수 있습니다.

- 시스템 트래픽 한정자를 사용하여 그룹의 포트를 통과하고 있는 가상 인프라 데이터의 유형에 패킷을 일치시킵니다. 예를 들면 NFS를 선택하여 네트워크 스토리지로 데이터를 전송할 수 있습니다.
- MAC 트래픽 한정자를 사용하여 MAC 주소, VLAN ID 및 다음 수준 프로토콜을 기준으로 패킷을 일치시킵니다.

분산 포트 그룹에서 VLAN ID로 트래픽을 찾을 때 VGT(Virtual Guest Tagging)를 사용할 수 있습니다. VST(Virtual Switch Tagging)가 활성 상태인 경우 트래픽을 VLAN ID에 일치시키려면 업링크 포트 그룹이나 업링크 포트의 규칙을 사용합니다.

- IP 트래픽 한정자를 사용하여 IP 버전, IP 주소, 다음 수준 프로토콜 및 포트를 기준으로 패킷을 일치시킵니다.

## 8 규칙 대화상자에서 **확인**을 클릭하여 규칙을 저장합니다.

### 분산 포트 또는 업링크 포트의 네트워크 트래픽 규칙

분산 포트 또는 업링크 포트 그룹에서 트래픽 규칙을 정의하여 가상 시스템 또는 물리적 어댑터와 관련된 트래픽을 처리하는 정책을 적용하는 방법을 알아봅니다. 특정 트래픽을 필터링하거나 해당 QoS 요구 사항을 명시할 수 있습니다.

- **분산 포트 또는 업링크 포트의 트래픽 규칙 보기**

분산 포트 또는 업링크 포트의 트래픽 필터링 및 표시 정책을 구성하는 트래픽 규칙을 검토할 수 있습니다.

- **분산 포트 또는 업링크 포트의 트래픽 규칙 편집**

트래픽 규칙을 생성 또는 편집하고 해당 매개 변수를 사용하여 분산 포트 또는 업링크 포트에서 트래픽을 필터링하거나 표시하기 위한 정책을 구성하는 방법을 알아봅니다.

- **분산 포트 또는 업링크 포트의 규칙 우선 순위 수정**

분산 포트 또는 업링크 포트의 트래픽 필터링 및 표시 정책을 구성하는 규칙의 순서를 변경하여 보안 및 QoS를 위해 트래픽을 분석하는 작업 순서를 변경하는 방법을 알아봅니다.



## ■ 분산 포트 또는 업링크 포트의 트래픽 규칙 삭제

분산 포트나 업링크 포트에서 트래픽 규칙을 삭제하여 가상 시스템 또는 물리적 어댑터로 전송되는 특정 유형의 패킷에 대한 필터링이나 표시를 중지할 수 있습니다.

### 분산 포트 또는 업링크 포트의 트래픽 규칙 보기

분산 포트 또는 업링크 포트의 트래픽 필터링 및 표시 정책을 구성하는 트래픽 규칙을 검토할 수 있습니다.

#### 사전 요구 사항

분산 포트 수준에서 정책을 재정의하려면 이 정책에 대해 포트 수준 재정의 옵션을 사용하도록 설정합니다. [포트 수준에서 네트워킹 정책 재정의 구성](#)의 내용을 참조하십시오.

#### 절차

- Distributed Switch로 이동한 다음 분산 포트 또는 업링크 포트에 이동합니다.
  - 스위치의 분산 포트에 이동하려면 **네트워크 > 분산 포트 그룹**을 클릭하고 목록에서 분산 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
  - 업링크 포트 그룹의 업링크 포트에 이동하려면 **네트워크 > 업링크 포트 그룹**을 클릭하고 목록에서 업링크 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
- 목록에서 포트를 선택합니다.
- 트래픽 필터링 및 표시** 탭을 선택합니다.
- 포트 수준에서 [트래픽 필터링 및 표시]가 사용되지 않도록 설정된 경우 [사용 및 순서 변경] 버튼을 클릭하고 기본 설정을 재정의한 다음 **모든 트래픽 규칙 사용**을 클릭합니다.
 

그룹 수준에서 트래픽 규칙을 사용하도록 설정한 경우 포트에 대한 기본 설정을 재정의하면 트래픽 규칙이 자동으로 사용되도록 설정됩니다.
- 작업**을 검토하여 규칙이 특별한 QoS 요구 사항이 있는 트래픽을 필터링(허용 또는 삭제)하거나 표시(태그)하는지 확인합니다.
- 상위 목록에서 트래픽을 찾을 수 있는 기준을 보려는 규칙을 선택합니다.
 

트래픽 한정자 목록에 규칙의 트래픽 한정 매개 변수가 나타납니다.

### 분산 포트 또는 업링크 포트의 트래픽 규칙 편집

트래픽 규칙을 생성 또는 편집하고 해당 매개 변수를 사용하여 분산 포트 또는 업링크 포트에서 트래픽을 필터링하거나 표시하기 위한 정책을 구성하는 방법을 알아봅니다.

#### 사전 요구 사항

분산 포트 수준에서 정책을 재정의하려면 이 정책에 대해 포트 수준 재정의 옵션을 사용하도록 설정합니다. [포트 수준에서 네트워킹 정책 재정의 구성](#)의 내용을 참조하십시오.

## 절차

- 1 Distributed Switch로 이동한 다음 분산 포트 또는 업링크 포트에 이동합니다.
  - 스위치의 분산 포트에 이동하려면 **네트워크 > 분산 포트 그룹**을 클릭하고 목록에서 분산 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
  - 업링크 포트 그룹의 업링크 포트에 이동하려면 **네트워크 > 업링크 포트 그룹**을 클릭하고 목록에서 업링크 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
- 2 목록에서 포트를 선택합니다.
- 3 **트래픽 필터링 및 표시** 탭을 선택합니다.
- 4 포트 수준에서 [트래픽 필터링 및 표시]가 사용되지 않도록 설정된 경우 [사용 및 순서 변경] 버튼을 클릭하고 기본 설정을 재정의한 다음 **모든 트래픽 규칙 사용**을 클릭합니다.
 

그룹 수준에서 트래픽 규칙을 사용하도록 설정한 경우 포트에 대한 기본 설정을 재정의하면 트래픽 규칙이 자동으로 사용되도록 설정됩니다.
- 5 **추가**를 클릭하여 새 규칙을 생성하거나, 규칙을 선택하고 **편집**을 클릭하여 규칙을 편집합니다.
 

분산 포트 그룹이나 업링크 포트 그룹에서 상속된 규칙을 변경할 수 있습니다. 그러면 규칙이 포트 범위 내에서 고유해집니다.

## 다음에 수행할 작업

네트워크 트래픽 규칙 이름을 지정하고 대상 트래픽을 거부, 허용 또는 태그 처리합니다.

## 분산 포트 또는 업링크 포트의 규칙 우선 순위 수정

분산 포트 또는 업링크 포트의 트래픽 필터링 및 표시 정책을 구성하는 규칙의 순서를 변경하여 보안 및 QoS를 위해 트래픽을 분석하는 작업 순서를 변경하는 방법을 알아봅니다.

vSphere Distributed Switch는 엄격하게 순서대로 네트워크 트래픽 규칙을 적용합니다. 패킷이 이미 규칙을 충족하는 경우 정책의 다음 규칙으로 패킷이 전달되지 않을 수 있습니다.

## 사전 요구 사항

분산 포트 수준에서 정책을 재정의하려면 이 정책에 대해 포트 수준 재정의 옵션을 사용하도록 설정합니다. [포트 수준에서 네트워킹 정책 재정의 구성](#)의 내용을 참조하십시오.

## 절차

- 1 Distributed Switch로 이동한 다음 분산 포트 또는 업링크 포트에 이동합니다.
  - 스위치의 분산 포트에 이동하려면 **네트워크 > 분산 포트 그룹**을 클릭하고 목록에서 분산 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
  - 업링크 포트 그룹의 업링크 포트에 이동하려면 **네트워크 > 업링크 포트 그룹**을 클릭하고 목록에서 업링크 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
- 2 목록에서 포트를 선택합니다.

- 3 **트래픽 필터링 및 표시** 탭을 선택합니다.
- 4 **사용 및 순서 변경** 버튼을 클릭합니다.
- 5 포트 수준에서 [트래픽 필터링 및 표시]가 사용되지 않도록 설정된 경우 기본 설정을 재정의하고 [모든 트래픽 규칙 사용]을 클릭합니다.  
그룹 수준에서 트래픽 규칙을 사용하도록 설정한 경우 포트에 대한 기본 설정을 재정의하면 트래픽 규칙이 자동으로 사용되도록 설정됩니다.
- 6 규칙을 선택하고 **위로 이동** 또는 **아래로 이동** 버튼을 사용하여 규칙의 우선 순위를 변경합니다.
- 7 **확인**을 클릭하여 변경 사항을 적용합니다.

### 분산 포트 또는 업링크 포트의 트래픽 규칙 삭제

분산 포트나 업링크 포트에서 트래픽 규칙을 삭제하여 가상 시스템 또는 물리적 어댑터로 전송되는 특정 유형의 패킷에 대한 필터링이나 표시를 중지할 수 있습니다.

#### 사전 요구 사항

분산 포트 수준에서 정책을 재정의하려면 이 정책에 대해 포트 수준 재정의 옵션을 사용하도록 설정합니다. [포트 수준에서 네트워킹 정책 재정의 구성](#)의 내용을 참조하십시오.

#### 절차

- 1 Distributed Switch로 이동한 다음 분산 포트 또는 업링크 포트에 이동합니다.
  - 스위치의 분산 포트에 이동하려면 **네트워크 > 분산 포트 그룹**을 클릭하고 목록에서 분산 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
  - 업링크 포트 그룹의 업링크 포트에 이동하려면 **네트워크 > 업링크 포트 그룹**을 클릭하고 목록에서 업링크 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
- 2 목록에서 포트를 선택합니다.
- 3 **트래픽 필터링 및 표시** 탭을 선택합니다.
- 4 포트 수준에서 [트래픽 필터링 및 표시]가 사용되지 않도록 설정된 경우 [사용 및 순서 변경] 버튼을 클릭하고 기본 설정을 재정의한 다음 **모든 트래픽 규칙 사용**을 클릭합니다.  
그룹 수준에서 트래픽 규칙을 사용하도록 설정한 경우 포트에 대한 기본 설정을 재정의하면 트래픽 규칙이 자동으로 사용되도록 설정됩니다.
- 5 규칙을 선택하고 **삭제** 버튼을 클릭합니다.
- 6 **확인**을 클릭합니다.

### 분산 포트 또는 업링크 포트의 트래픽 필터링 및 표시 사용 안 함

포트에서 트래픽 필터링 및 표시 정책을 사용하지 않도록 설정하여 보안 필터링 또는 QoS 표시 없이 트래픽이 가상 시스템 또는 물리적 어댑터로 흐르도록 합니다.

## 사전 요구 사항

분산 포트 수준에서 정책을 재정의하려면 이 정책에 대해 포트 수준 재정의 옵션을 사용하도록 설정합니다. **포트 수준에서 네트워킹 정책 재정의 구성**의 내용을 참조하십시오.

## 절차

- 1 Distributed Switch로 이동한 다음 분산 포트 또는 업링크 포트에 이동합니다.
  - 스위치의 분산 포트에 이동하려면 **네트워크 > 분산 포트 그룹**을 클릭하고 목록에서 분산 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
  - 업링크 포트 그룹의 업링크 포트에 이동하려면 **네트워크 > 업링크 포트 그룹**을 클릭하고 목록에서 업링크 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
- 2 목록에서 포트를 선택합니다.
- 3 **트래픽 필터링 및 표시** 탭을 선택합니다.
- 4 **사용 및 순서 변경** 버튼을 클릭합니다.
- 5 전환 버튼을 사용하여 포트 수준에서 기본 설정을 재정의하고 모든 트래픽 규칙을 사용하지 않도록 설정합니다.
- 6 **확인**을 클릭합니다.

## 필터링 및 표시할 트래픽 한정

스토리지, vCenter Server 관리 등을 위한 데이터와 같이 전송되는 인프라 데이터의 유형과 일치하거나 계층 2 및 계층 3 속성과 일치하는 트래픽을 필터링하거나 QoS 태그로 표시할 수 있습니다.

규칙의 범위 내에서 트래픽을 보다 정확히 일치시키려면 시스템 데이터 유형, 계층 2 헤더, 계층 3 헤더 등의 기준을 결합할 수 있습니다.

## 시스템 트래픽 한정자

포트 그룹 또는 포트에 대한 규칙에서 시스템 트래픽 한정자를 사용하여, 특정 시스템 데이터 트래픽을 QoS 태그로 표시해야 하는지 여부와 해당 트래픽을 허용 또는 삭제해야 할지를 결정할 수 있습니다.

### 시스템 트래픽 유형

시스템 데이터를 전송하는 포트 그룹의 트래픽 유형을 선택할 수 있습니다. 즉, vCenter Server, 스토리지, VMware vSphere vMotion<sup>®</sup> 및 vSphere Fault Tolerance의 트래픽 중 관리할 트래픽을 선택할 수 있습니다. 특정 트래픽 유형만 표시 또는 필터링하거나, 인프라 기능을 제외한 모든 시스템 데이터 트래픽을 표시 또는 필터링할 수 있습니다. 예를 들어 vCenter Server, 스토리지 및 vMotion의 트래픽은 관리하도록 필터링하거나 QoS 값으로 표시하고, Fault Tolerance 데이터를 전송하는 트래픽은 제외할 수 있습니다.

## MAC 트래픽 한정자

규칙에 MAC 트래픽 한정자를 사용함으로써 MAC 주소, VLAN ID, 프레임 페이로드를 소비하는 다음 수준 프로토콜 등 패킷의 계층 2(데이터 링크 계층) 속성에 대한 일치 조건을 정의할 수 있습니다.

## 프로토콜 유형

MAC 트래픽 한정자의 **프로토콜 유형** 특성은 이더넷 프레임의 EtherType 필드와 일치합니다. EtherType은 프레임 페이로드를 소비할 다음 수준 프로토콜의 유형을 나타냅니다.

드롭다운 메뉴에서 프로토콜을 선택하거나 해당 16진수 숫자를 입력할 수 있습니다. 예를 들어 LLDP(링크 계층 탐색 프로토콜) 프로토콜의 트래픽을 캡처하려면 **88CC**를 입력합니다.

## VLAN ID

MAC 트래픽 한정자의 VLAN ID 특성을 사용하여 특정 VLAN에서 트래픽을 표시하거나 필터링할 수 있습니다.

**참고** 분산 포트 그룹에 있는 VLAN ID 한정자에 VGT(Virtual Guest Tagging)를 사용할 수 있습니다.

VST(Virtual Switch Tagging)를 통해 VLAN ID로 태그가 지정된 흐름의 경우 분산 포트 그룹 또는 분산 포트의 규칙에서 이 ID를 사용하여 찾을 수 없습니다. Distributed Switch가 트래픽에서 태그를 해제한 후에야 스위치가 VLAN ID를 비롯한 규칙 조건을 확인하기 때문입니다. 이 경우 VLAN ID가 일치하는 트래픽을 찾으려면 업링크 포트 그룹 또는 업링크 포트의 규칙을 사용해야 합니다.

## 소스 주소

소스 주소 특성 그룹을 사용하여 소스 MAC 주소 또는 네트워크를 기준으로 패킷을 일치시킬 수 있습니다.

비교 연산자를 사용하여 지정된 소스 주소나 네트워크가 있는 패킷 또는 없는 패킷을 표시하거나 필터링할 수 있습니다.

다양한 방법으로 트래픽 소스를 일치시킬 수 있습니다.

**표 8-6. MAC 소스 주소를 기준으로 트래픽을 필터링하고 표시하기 위한 패턴**

트래픽 소스 주소 일치에 사용되는 매개 변수	비교 연산자	네트워킹 인수 형식
MAC 주소	같음 또는 같지 않음	일치시킬 MAC 주소를 입력합니다. 포함된 8진수를 콜론으로 구분합니다.
MAC 네트워크	일치 또는 일치하지 않음	네트워크에서 가장 낮은 주소와 마스크를 입력합니다. 네트워크 비트의 위치에 1을 설정하고, 호스트 부분에는 0을 설정합니다.

예를 들어 접두사가 05:50:56인 MAC 네트워크의 길이가 23비트인 경우에는 주소를 **00:50:56:00:00:00**로 설정하고, 마스크를 **ff:ff:fe:00:00:00**로 설정합니다.

## 대상 주소

대상 주소 특성 그룹을 사용하여 패킷을 해당 대상 주소에 일치시킬 수 있습니다. MAC 대상 주소 옵션은 소스 주소 옵션과 형식이 동일합니다.

## 비교 연산자

MAC 한정자에서 트래픽을 원하는 바에 보다 가깝게 일치시키기 위해 긍정 비교나 부정을 사용할 수 있습니다. 특정 특성을 가지고 있는 패킷 외에 모든 패킷이 규칙 범위에 포함되도록 연산자를 사용할 수 있습니다.

## IP 트래픽 한정자

규칙에 IP 트래픽 한정자를 사용하여 IP 버전, IP 주소, 다음 수준 프로토콜, 포트 등 계층 3(네트워크 계층) 속성에 대한 트래픽 일치 조건을 정의할 수 있습니다.

### 프로토콜

IP 트래픽 한정자의 **프로토콜** 특성은 패킷의 페이로드를 소비하는 다음 수준 프로토콜을 나타냅니다. 드롭다운 메뉴에서 프로토콜을 선택하거나 RFC 1700에 따라 해당 십진수 숫자를 입력할 수 있습니다.

TCP 및 UDP 프로토콜의 경우 소스 및 대상 포트를 기준으로 트래픽을 일치시킬 수도 있습니다.

### 소스 포트

소스 포트 특성을 사용하여 소스 포트를 기준으로 TCP 또는 UDP 패킷을 일치시킬 수 있습니다. 트래픽을 소스 포트에 일치시키는 경우 트래픽 방향을 고려해야 합니다.

### 대상 포트

대상 포트 특성을 사용하여 대상 포트를 기준으로 TCP 또는 UDP 패킷을 일치시킬 수 있습니다. 트래픽을 대상 포트에 일치시키는 경우 트래픽 방향을 고려해야 합니다.

### 소스 주소

소스 주소 특성을 사용하여 소스 주소 또는 서브넷을 기준으로 패킷을 일치시킬 수 있습니다. 트래픽을 소스 주소 또는 네트워크에 일치시키는 경우 트래픽 방향을 고려해야 합니다.

다양한 방법으로 트래픽 소스를 일치시킬 수 있습니다.

**표 8-7. IP 소스 주소를 기준으로 트래픽을 필터링하고 표시하기 위한 패턴**

트래픽 소스 주소 일치에 사용되는 매개 변수	비교 연산자	네트워킹 인수 형식
IP 버전	임의	드롭다운 메뉴에서 IP 버전을 선택합니다.
IP 주소	같음 또는 같지 않음	일치시킬 IP 주소를 입력합니다.
IP 서브넷	일치 또는 일치하지 않음	서브넷에서 가장 낮은 주소와 서브넷 접두사의 비트 길이를 입력합니다.

### 대상 주소

대상 주소를 사용하여 IP 주소, 서브넷 또는 IP 버전을 기준으로 패킷을 일치시킵니다. 대상 주소 형식은 소스 주소 형식과 같습니다.

### 비교 연산자

IP 한정자에서 트래픽을 원하는 바에 보다 가깝게 일치시키기 위해 긍정 비교나 부정을 사용할 수 있습니다. 특정 특성의 패킷을 제외하고 모든 패킷이 규칙의 범위 안에 포함되도록 정의할 수 있습니다.

## vSphere Distributed Switch에서 여러 포트 그룹에 대한 정책 관리

vSphere Distributed Switch 여러 포트 그룹에 대한 네트워킹 정책을 수정하는 방법을 알아봅니다.

## 사전 요구 사항

하나 이상의 포트 그룹이 있는 vSphere Distributed Switch를 생성합니다.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 개체 탐색기에서 Distributed Switch를 마우스 오른쪽 버튼으로 클릭하고 **분산 포트 그룹 > 분산 포트 그룹 관리**를 선택합니다.
- 3 포트 그룹 정책 선택 페이지에서 수정할 정책 범주 옆의 확인란을 선택하고 **다음**을 클릭합니다.

옵션	설명
보안	선택한 포트 그룹에 대해 MAC 주소 변경, 위조 전송 및 비규칙(Promiscuous) 모드를 설정합니다.
트래픽 조절	선택한 포트 그룹의 인바운드 및 아웃바운드 트래픽에 대해 평균 대역폭, 최대 대역폭 및 버스트 크기를 설정합니다.
VLAN	선택한 포트 그룹이 물리적 VLAN에 연결되는 방법을 구성합니다.
팀 구성 및 페일오버	선택한 포트 그룹에 대한 로드 밸런싱, 페일오버 감지, 스위치 알림 및 페일오버 순서를 설정합니다.
리소스 할당	선택한 포트 그룹에 대한 네트워크 리소스 풀 연결을 설정합니다.
모니터링	선택한 포트 그룹에 대해 NetFlow를 사용하거나 사용하지 않도록 설정합니다.
기타	선택한 포트 그룹에 대한 포트 차단을 사용하거나 사용하지 않도록 설정합니다.

- 4 포트 그룹 선택 페이지에서 편집할 분산 포트 그룹을 선택하고 **다음**을 클릭합니다.
- 5 (선택 사항) 보안 페이지에서 드롭다운 메뉴를 사용하여 보안 예외를 편집하고 **다음**을 클릭합니다.

옵션	설명
비규칙(Promiscuous) 모드	<ul style="list-style-type: none"> <li>■ <b>거부.</b> 게스트 어댑터를 비규칙(Promiscuous) 모드로 설정해도 어댑터로 수신되는 프레임에 영향을 미치지 않습니다.</li> <li>■ <b>동의.</b> 게스트 어댑터를 비규칙(Promiscuous) 모드로 설정하면 어댑터는 vSphere Distributed Switch를 통과하는 프레임 중 해당 어댑터가 연결되어 있는 포트 그룹의 VLAN 정책에서 허용하는 모든 프레임을 감지합니다.</li> </ul>
MAC 주소 변경	<ul style="list-style-type: none"> <li>■ <b>거부.</b> 거부로 설정하고 게스트 운영 체제에서 어댑터의 MAC 주소를 .vmx 구성 파일에 지정된 것 이외의 MAC 주소로 변경하면, 모든 인바운드 프레임이 삭제됩니다. 게스트 OS가 .vmx 구성 파일에서 MAC 주소와 다시 일치하도록 MAC 주소를 변경하면 인바운드 프레임이 다시 통과합니다.</li> <li>■ <b>동의.</b> 게스트 OS에서 변경한 MAC 주소가 그대로 적용됩니다. 새로운 MAC 주소로 프레임이 수신됩니다.</li> </ul>
위조 전송	<ul style="list-style-type: none"> <li>■ <b>거부.</b> 어댑터에 현재 설정된 주소와 다른 소스 MAC 주소를 사용하는 모든 아웃바운드 프레임이 삭제됩니다.</li> <li>■ <b>동의.</b> 필터링 없이 모든 아웃바운드 프레임이 통과합니다.</li> </ul>

- 6 (선택 사항) VLAN 페이지에서 드롭다운 메뉴를 사용하여 VLAN 정책을 편집하고 다음을 클릭합니다.

옵션	설명
없음	VLAN을 사용하지 않습니다.
VLAN	VLAN ID 필드에서 1과 4094 사이의 숫자를 입력합니다.
VLAN 트렁크	VLAN 트렁크 범위를 입력합니다.
전용 VLAN	사용하려는 가능한 전용 VLAN을 선택합니다.

- 7 (선택 사항) 트래픽 조절 페이지에서 드롭다운 메뉴를 사용하여 수신 또는 송신 트래픽 조절을 사용하거나 사용하지 않도록 설정하고 다음을 클릭합니다.

옵션	설명
상태	수신 트래픽 조절 또는 송신 트래픽 조절을 사용하도록 설정하면 이 포트 그룹과 관련된 각 VMkernel 어댑터 또는 가상 네트워크 어댑터에 할당되는 네트워크 대역폭 양에 제한이 설정됩니다. 정책을 사용하지 않도록 설정하면 기본적으로 서비스는 물리적 네트워크에 아무런 제한 없이 연결됩니다.
평균 대역폭	포트를 통과할 수 있는 평균 초당 비트 수, 즉 허용되는 평균 로드를 설정합니다.
최대 대역폭	트래픽 버스트를 송신 또는 수신할 때 포트를 통과할 수 있는 초당 최대 비트 수입니다. 포트가 추가 버스트를 사용할 때마다 이 최대값은 포트에서 사용하는 대역폭보다 커집니다.
버스트 크기	버스트에 허용할 최대 바이트 수입니다. 이 매개 변수를 설정하면 할당된 대역폭의 일부만 사용될 때 포트에 추가 버스트가 제공될 수 있습니다. 추가 버스트를 사용할 수 있는 경우 평균 대역폭에서 지정한 것보다 더 많은 대역폭이 포트에 필요할 때마다 더 높은 속도로 데이터를 전송할 수 있습니다. 이 매개 변수는 추가 버스트에서 누적될 수 있는 바이트 수의 상한값을 지정하기 때문에 더 높은 속도로 전송됩니다.



## 8 (선택 사항) 팀 구성 및 페일오버 페이지에서 드롭다운 메뉴를 사용하여 설정을 편집하고 다음을 클릭합니다.

옵션	설명
로드 밸런싱	<p>IP 기반 팀 구성의 경우 물리적 스위치를 이더 채널(Etherchannel)로 구성해야 합니다. 다른 모든 옵션의 경우에는 이더 채널(Etherchannel)을 사용하지 않도록 설정해야 합니다. 업링크 선택 방법을 지정합니다.</p> <ul style="list-style-type: none"> <li>■ <b>원래 가상 포트 기준 라우팅.</b> Distributed Switch의 트래픽 진입 가상 포트에 기반하여 업링크를 선택합니다.</li> <li>■ <b>IP 해시 기준 라우팅.</b> 각 패킷의 소스 및 대상 IP 주소의 해시에 기반하여 업링크를 선택합니다. 비 IP 패킷에 대해서는 오프셋에 있는 어떤 것도 해시를 계산하기 위해 사용됩니다.</li> <li>■ <b>소스 MAC 해시 기준 라우팅.</b> 소스 이더넷의 해시에 기반하여 업링크를 선택합니다.</li> <li>■ <b>물리적 NIC 로드 기준 라우팅.</b> 물리적 NIC의 현재 로드에서 기반하여 업링크를 선택합니다.</li> <li>■ <b>명시적 페일오버 순서 사용.</b> 페일오버 감지 기준을 통과한 활성 어댑터 목록에서 순서가 가장 높은 업링크를 항상 사용합니다.</li> </ul>
네트워크 장애 감지	<p>페일오버 감지에 사용할 방법을 선택합니다.</p> <ul style="list-style-type: none"> <li>■ <b>링크 상태만.</b> 네트워크 어댑터가 제공하는 링크 상태에만 의거합니다. 이 옵션은 케이블 당김, 물리적 스위치 전원 고장과 같은 고장을 감지하지만 스페닝 트리(spanning tree)로 차단되는 물리적 스위치 포트 또는 물리적 스위치의 다른 측면에서 케이블 당김이나 잘못된 VLAN으로의 잘못된 구성과 같은 구성 오류는 감지하지 않습니다.</li> <li>■ <b>신호 검색.</b> 팀의 모든 NIC에서 beacon probe을 보내고 수신하여 해당 정보를 연결 상태와 함께 연결 장애를 판단하는 데 사용합니다. IP-해시 로드 밸런싱과 함께 신호 검색을 사용하지 않습니다.</li> </ul>
스위치 알림	<p>페일오버의 경우에 스위치 알림을 위해 <b>예</b> 또는 <b>아니요</b>를 선택합니다. 포트 그룹을 사용하는 가상 시스템이 유니캐스트 모드의 Microsoft 네트워크 로드 밸런싱을 이용할 때에는 이 옵션을 사용하지 않습니다.</p> <p><b>예</b>를 선택한 경우, 가상 NIC가 Distributed Switch에 연결될 때마다 또는 가상 NIC의 트래픽이 페일오버 이벤트로 인해 팀의 다른 물리적 NIC로 라우팅될 때마다 물리적 스위치의 조회 표를 업데이트하기 위해 네트워크 전체에 알림이 전송됩니다. 페일오버 발생의 가장 낮은 대기 시간이 필요할 때 그리고 vMotion으로 마이그레이션할 때 이 프로세스를 사용합니다.</p> <p><b>알림 스위치가 예</b>로 설정된 경우에는 vCenter Server가 ESXi 호스트와 다시 연결될 때 연결된 모든 포트, 포트 그룹 및 Distributed Switch가 호스트에 다시 연결됩니다.</p>

옵션	설명
페일백	<p>페일백을 사용하거나 사용하지 않도록 설정하려면 <b>예</b> 또는 <b>아니요</b>를 선택합니다. 이 옵션은 물리적 어댑터가 고장을 복구한 후에 어떻게 실행 상태로 돌아가는가를 결정합니다.</p> <ul style="list-style-type: none"> <li>■ <b>예</b>(기본값): 슬롯을 인계 받았던 대기 어댑터(있는 경우)를 대체함으로써 복구 시 어댑터가 즉시 실행 상태로 돌아갑니다.</li> <li>■ <b>아니요</b>: 장애가 발생했던 어댑터를 복구 후에도 현재 활성 상태인 다른 어댑터에서 장애가 발생하여 어댑터를 교체해야 할 때까지 비활성 상태로 둡니다.</li> </ul>
페일오버 순서	<p>업링크로 작업 로드를 어떻게 분산하는지를 선택합니다. 일부 업링크만 사용하고 나머지 업링크는 사용 중인 업링크가 고장나는 상황에 사용할 수 있도록 예약하려면 해당 업링크를 여러 다른 그룹으로 이동하여 이 조건을 설정합니다.</p> <ul style="list-style-type: none"> <li>■ <b>활성 업링크</b>. 네트워크 어댑터 연결을 사용할 수 있고 활성 상태인 경우에 이 업링크를 계속 사용합니다.</li> <li>■ <b>대기 업링크</b>. 활성 어댑터 중 하나의 연결을 사용할 수 없는 경우 이 업링크를 사용합니다. IP-해시 로드 밸런싱을 이용할 때에는 대기 업링크를 구성하지 않습니다.</li> <li>■ <b>사용되지 않은 업링크</b>. 이 업링크를 사용하지 않습니다.</li> </ul>

- (선택 사항) [리소스 할당] 페이지에서 **네트워크 리소스 풀** 드롭다운 메뉴를 사용하여 리소스 할당을 추가하거나 제거하고 **다음**을 클릭합니다.
- (선택 사항) [모니터링] 페이지에서 드롭다운 메뉴를 사용하여 NetFlow를 사용하거나 사용하지 않도록 설정하고 **다음**을 클릭합니다.

옵션	설명
사용 안 함	분산 포트 그룹에서 NetFlow를 사용하지 않습니다.
사용	분산 포트 그룹에서 NetFlow를 사용합니다. NetFlow 설정을 vSphere Distributed Switch 수준에서 구성할 수 있습니다.

- (선택 사항) 기타 페이지의 드롭다운 메뉴에서 **예** 또는 **아니요**를 선택하고 **다음**을 클릭합니다.
 

포트 그룹의 모든 포트를 종료하려면 **예**를 선택합니다. 이렇게 종료하는 경우 포트를 사용하는 호스트나 가상 시스템의 정상적인 네트워크 작동이 중단될 수 있습니다.
- 완료 준비 페이지에서 설정을 검토하고 **마침**을 클릭합니다.
 

설정을 변경하려면 **뒤로** 버튼을 사용합니다.

## 포트 차단 정책

포트 차단 정책을 사용하면 포트에서 데이터를 보내거나 받는 것을 선택적으로 차단할 수 있습니다.

### 분산 포트 그룹의 포트 차단 정책 편집

분산 포트 그룹의 모든 포트를 차단할 수 있습니다.

분산 포트 그룹의 포트를 차단하면 해당 호트를 사용하는 호스트 또는 가상 시스템의 정상적인 네트워크 작업이 중단될 수 있습니다.

## 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 개체 탐색기에서 Distributed Switch를 마우스 오른쪽 버튼으로 클릭하고 **분산 포트 그룹 > 분산 포트 그룹 관리**를 선택합니다.
- 3 **기타** 확인란을 선택하고 **다음**을 클릭합니다.
- 4 구성할 하나 이상의 분산 포트 그룹을 선택하고 **다음**을 클릭합니다.
- 5 **모든 포트 차단** 드롭다운 메뉴에서 포트 차단을 사용하거나 사용하지 않도록 설정하고 **다음**을 클릭합니다.
- 6 설정을 검토하고 **마침**을 클릭합니다.

## 분산 포트 또는 업링크 포트의 차단 정책 편집

개별 분산 포트 또는 업링크 포트를 차단할 수 있습니다.

포트를 통한 흐름을 차단하면 해당 포트를 사용하는 호스트 또는 가상 시스템에 대한 정상적인 네트워크 작업이 중단될 수 있습니다.

### 사전 요구 사항

포트 수준 재정의의 사용하도록 설정합니다. [포트 수준에서 네트워킹 정책 재정의 구성 항목을 참조하십시오.](#)

## 절차

- 1 Distributed Switch로 이동한 다음 분산 포트 또는 업링크 포트에 이동합니다.
  - 스위치의 분산 포트에 이동하려면 **네트워크 > 분산 포트 그룹**을 클릭하고 목록에서 분산 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
  - 업링크 포트 그룹의 업링크 포트에 이동하려면 **네트워크 > 업링크 포트 그룹**을 클릭하고 목록에서 업링크 포트 그룹을 클릭한 다음 **포트** 탭을 클릭합니다.
- 2 목록에서 포트를 선택합니다.
- 3 **분산 포트 설정 편집**을 클릭합니다.
- 4 **기타** 섹션에서 **재정의** 확인란을 선택하고 드롭다운 메뉴에서 포트 차단을 사용하거나 사용하지 않도록 설정합니다.
- 5 **확인**을 클릭합니다.

## MAC 학습 정책이란?

MAC 학습은 하나의 vNIC에서 여러 MAC 주소가 사용되는 배포에 대한 네트워크 연결을 제공합니다.

예를 들어 중첩된 하이퍼바이저 배포에서 ESXi VM이 ESXi 호스트에서 실행되고 여러 VM이 ESXi VM 내에서 실행될 수 있습니다. MAC 학습을 사용하지 않을 경우 ESXi VM의 vNIC가 스위치 포트에 연결되면 여기에는 정적 MAC 주소만 포함됩니다. 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, 해당 MAC 테이블의 MAC 주소를 학습하고, 패킷이 통과되도록 합니다. 학습된 MAC 주소는 특정 기간 동안 사용되지 않으면 제거됩니다.

MAC 학습은 알 수 없는 유니캐스트 플러딩도 지원합니다. 일반적으로 포트에서 수신한 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 MAC 학습이 사용되도록 설정된 경우에만 기본적으로 사용되도록 설정됩니다.

학습할 수 있는 MAC 주소 수는 구성 가능합니다. 최대값은 포트당 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.

vSphere 6.7 이상에서는 vSphere API를 사용하여 분산 가상 포트 그룹에서 MAC 학습을 사용하도록 설정할 수 있습니다. vSphere Distributed Switch, 분산 가상 포트 그룹 및 분산 가상 포트에서 MAC 학습 정책을 구성할 수 있습니다. MAC 학습 정책이 분산 가상 포트 그룹에 설정되지 않은 경우 vSphere Distributed Switch에서 상속되고 DVport에서 사용하도록 설정되지 않으면 분산 가상 포트 그룹에서 상속됩니다. 자세한 내용은 "vSphere Web Services API 참조" 를 참조하십시오.

# VLAN을 사용하여 네트워크 트래픽을 분리하는 방법

## 9

VLAN을 통해 네트워크 프로토콜 스택의 계층 2에서 네트워크를 여러 논리적 브로드캐스트 도메인으로 세분화할 수 있습니다.

다음으로 아래 항목을 읽으십시오.

- VLAN 구성
- 전용 VLAN

## VLAN 구성

VLAN(가상 LAN)은 하나의 물리적 LAN 세그먼트를 더 분리하여 포트 그룹이 물리적으로 다른 세그먼트에 있는 것처럼 서로 분리시킵니다.

## vSphere에서 VLAN 사용의 이점

vSphere 환경의 VLAN 구성은 특정 이점을 제공합니다.

- ESXi 호스트를 기존 VLAN 토폴로지에 통합합니다.
- 네트워크 트래픽을 분리하고 보호합니다.
- 네트워크 트래픽의 정체를 줄여 줍니다.

vSphere 환경에 VLAN 도입의 이점과 기본 원칙에 대한 비디오를 시청하십시오.



(vSphere 환경에서 VLAN 사용)

## VLAN 태그 지정 모드

vSphere는 ESXi에서 EST(External Switch Tagging), VST(Virtual Switch Tagging), VGT(Virtual Guest Tagging)라는 세 가지 VLAN 태그 지정 모드를 지원합니다.

태그 지정 모드	스위치 포트 그룹에 대한 VLAN ID	설명
EST	0	물리적 스위치는 VLAN 태그 지정을 수행합니다. 호스트 네트워크 어댑터는 물리적 스위치의 액세스 포트에 연결됩니다.
VST	1과 4094 사이	가상 스위치는 패킷이 호스트를 떠나기 전에 VLAN 태그 지정을 수행합니다. 호스트 네트워크 어댑터는 물리적 스위치의 트렁크 포트에 연결되어야 합니다.
VGT	<ul style="list-style-type: none"> <li>■ 표준 스위치를 위한 4095</li> <li>■ Distributed Switch를 위한 개별 VLAN의 범위</li> </ul>	<p>가상 시스템이 VLAN 태그 지정을 수행합니다. 가상 스위치는 가상 시스템 네트워킹 스택과 외부 스위치 간에 패킷을 전달할 때 VLAN 태그를 유지합니다. 호스트 네트워크 어댑터는 물리적 스위치의 트렁크 포트에 연결되어야 합니다.</p> <p>vSphere Distributed Switch는 VGT의 수정을 지원합니다. 보안상의 이유로 특정 VLAN에 속하는 패킷만 통과하도록 Distributed Switch를 구성할 수 있습니다.</p> <p><b>참고</b> VGT의 경우 가상 시스템의 게스트 운영 체제에 802.1Q VLAN 트렁킹 드라이버가 설치되어 있어야 합니다.</p>

가상 스위치의 VLAN 태그 지정 모드에 대해 설명하는 비디오를 시청하십시오.



(vSphere의 VLAN 태그 지정 모드)

## 전용 VLAN

전용 VLAN은 논리적 브로드캐스트 도메인의 추가 세분화를 보다 작은 여러 브로드캐스트 하위 도메인에 추가하여 VLAN ID 제한을 해결하는 데 사용됩니다.

전용 VLAN은 기본 VLAN ID로 식별되며, 기본 VLAN ID는 여러 개의 보조 VLAN ID와 연결될 수 있습니다. 기본 VLAN은 전용 VLAN의 포트가 기본 VLAN으로 구성된 포트와 통신할 수 있도록 **비규칙(Promiscuous)** 형식입니다. 보조 VLAN의 포트는 비규칙(Promiscuous) 포트와만 통신하는 **분리된** 형식이거나 비규칙(Promiscuous) 포트 및 동일한 보조 VLAN의 다른 포트와 모두 통신하는 **커뮤니티** 형식일 수 있습니다.

호스트와 물리적 네트워크의 나머지 요소 간에 전용 VLAN을 사용하려면 호스트에 연결된 물리적 스위치가 전용 VLAN을 지원해야 하며 ESXi에서 전용 VLAN 기능에 사용하는 VLAN ID로 구성되어야 합니다. 동적 MAC+VLAN ID 기반 학습을 사용하는 물리적 스위치의 경우 해당하는 모든 전용 VLAN ID를 스위치의 VLAN 데이터베이스에 먼저 입력해야 합니다.

## 전용 VLAN 생성

전용 VLAN에 참여할 분산 포트를 할당할 수 있도록 vSphere Distributed Switch에서 필요한 전용 VLAN을 생성합니다.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 구성 탭에서 **설정**을 확장하고 **전용 VLAN**을 선택합니다.
- 3 **편집**을 클릭합니다.

- 4 기본 VLAN을 추가하려면 기본 VLAN ID 위에서 **더하기 기호(+)** 버튼을 클릭합니다.  
기본 전용 VLAN이 보조 전용 VLAN ID에도 나타납니다.
- 5 보조 VLAN을 추가하려면 오른쪽 창에서 **더하기 기호(+)** 버튼을 클릭합니다.
- 6 **보조 VLAN 유형** 열의 드롭다운 메뉴에서 **분리됨** 또는 **커뮤니티**를 선택합니다.
- 7 **확인**을 클릭합니다.

#### 다음에 수행할 작업

트래픽을 전용 VLAN과 연결하도록 분산 포트 그룹 또는 포트를 구성합니다. [분산 포트 그룹 또는 분산 포트에서 VLAN 태그 지정 구성](#)의 내용을 참조하십시오.

## 기본 전용 VLAN 제거

vSphere Distributed Switch의 구성에서 사용되지 않은 기본 VLAN을 제거합니다.

기본 전용 VLAN을 제거하면 연결된 보조 전용 VLAN도 제거됩니다.

#### 사전 요구 사항

기본 VLAN 및 이와 연결된 보조 VLAN을 사용하도록 구성된 포트 그룹이 없는지 확인합니다.

#### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **구성** 탭에서 **설정**을 확장하고 **전용 VLAN**을 선택합니다.
- 3 **편집**을 클릭합니다.
- 4 제거할 기본 전용 VLAN을 선택합니다.
- 5 기본 VLAN ID 목록 위의 **곱하기 기호(x)** 버튼을 클릭합니다.
- 6 **확인**을 클릭합니다.

## 보조 전용 VLAN 제거

vSphere Distributed Switch의 구성에서 사용되지 않은 보조 전용 VLAN을 제거합니다.

#### 사전 요구 사항

보조 VLAN을 사용하도록 구성된 포트 그룹이 없는지 확인합니다.

#### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **구성** 탭에서 **설정**을 확장하고 **전용 VLAN**을 선택합니다.
- 3 **편집**을 클릭합니다.

4 기본 전용 VLAN을 선택합니다.

이와 연결된 보조 전용 VLAN이 오른쪽에 나타납니다.

5 제거할 보조 전용 VLAN을 선택합니다.

6 위 보조 VLAN ID 목록에서 **x 확인**을 클릭합니다.



# 네트워크 리소스 관리

# 10

vSphere는 네트워크 리소스를 관리하는 데 도움이 되는 여러 가지 방법을 제공합니다.

다음으로 아래 항목을 읽으십시오.

- DirectPath I/O
- VMDirectPath I/O 디바이스에 대한 무중단 추가 및 무중단 제거 지원
- SR-IOV(단일 루트 I/O 가상화)란?
- 가상 시스템에 대한 RDMA란?
- Remote Direct Memory Access 네트워크 어댑터 구성
- 점보 프레임이란?
- TCP 세분화 오프로드란?
- 대규모 수신 오프로드란?
- NetQueue 및 네트워킹 성능

## DirectPath I/O

DirectPath I/O를 사용하면 가상 시스템에서 I/O MMU(메모리 관리 장치)가 있는 플랫폼의 물리적 PCI 기능에 액세스할 수 있습니다.

다음 기능은 DirectPath로 구성된 가상 시스템에 사용할 수 없습니다.

- 가상 디바이스 핫 추가 및 제거
- 일시 중단 및 재개
- 기록 및 재생
- Fault Tolerance
- 고가용성
- DRS(제한된 가용성. 가상 시스템이 클러스터에 포함될 수 있지만 호스트 사이에 마이그레이션될 수는 없음)

- 스냅샷

### 다음으로 읽을 항목

- [호스트의 네트워크 디바이스에 대한 패스스루 사용](#)

패스스루 디바이스를 구성하면 리소스를 효율적으로 사용하고 환경의 성능을 향상시킬 수 있습니다. 호스트의 네트워크 디바이스에 대해 DirectPath I/O 패스스루를 사용하도록 설정할 수 있습니다.

- [가상 시스템에 PCI 디바이스 구성](#)

패스스루 디바이스를 구성하면 리소스를 보다 효율적으로 사용하고 환경의 성능을 향상시킬 수 있습니다. vSphere Client에서 가상 시스템에 패스스루 PCI 디바이스를 구성할 수 있습니다.

## 호스트의 네트워크 디바이스에 대한 패스스루 사용

패스스루 디바이스를 구성하면 리소스를 효율적으로 사용하고 환경의 성능을 향상시킬 수 있습니다. 호스트의 네트워크 디바이스에 대해 DirectPath I/O 패스스루를 사용하도록 설정할 수 있습니다.

**경고** ESXi 호스트가 USB 채널에 연결된 USB 디바이스 또는 SD 카드에서 부팅되도록 구성된 경우 USB 컨트롤러에 대해 DirectPath I/O 패스스루를 사용하지 않도록 설정합니다. USB 디바이스 또는 SD 카드에서 부팅되는 ESXi 호스트의 USB 컨트롤러를 통과하면 해당 호스트가 호스트 구성이 유지될 수 없는 상태가 될 수 있습니다.

### 절차

- 1 vSphere Client 탐색기에서 호스트를 찾습니다.
- 2 구성 탭에서 **하드웨어**를 확장하고 **PCI 디바이스**를 클릭합니다.
- 3 호스트의 PCI 네트워크 디바이스에 대해 DirectPath I/O 패스스루를 사용하도록 설정하려면 **편집**을 클릭합니다.

사용 가능한 패스스루 디바이스 목록이 나타납니다.

아이콘	설명
녹색 아이콘	디바이스가 활성 상태이며 사용하도록 설정할 수 있습니다.
주황색 아이콘	디바이스 상태가 변경되었으며, 디바이스를 사용하려면 먼저 호스트를 재부팅해야 합니다.

- 4 패스스루에 사용할 네트워크 디바이스를 선택하고 **확인**을 클릭합니다.

선택한 PCI 디바이스가 표에 나타납니다. 디바이스 정보는 화면 아래쪽에 표시됩니다.

## 가상 시스템에 PCI 디바이스 구성

패스스루 디바이스를 구성하면 리소스를 보다 효율적으로 사용하고 환경의 성능을 향상시킬 수 있습니다.

vSphere Client에서 가상 시스템에 패스스루 PCI 디바이스를 구성할 수 있습니다.

Linux 커널 버전 2.6.20 이전이 있는 패스스루 디바이스를 사용할 경우 MSI 및 MSI-X 모드는 성능 저하에 큰 영향을 주므로 이러한 모드는 사용하지 않는 것이 좋습니다.

## 사전 요구 사항

가상 시스템의 호스트에 패스스루 네트워킹 디바이스가 구성되어 있는지 확인합니다. [호스트의 네트워크 디바이스에 대한 패스스루 사용](#)의 내용을 참조하십시오.

## 절차

- 1 vSphere Client에서 가상 시스템을 찾습니다.
  - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택하고 **VM** 탭을 클릭합니다.
  - b **가상 시스템**을 클릭하고 목록에서 가상 시스템을 클릭합니다.
- 2 가상 시스템의 전원을 끕니다.
- 3 [작업] 메뉴에서 [설정 편집]을 선택합니다.
- 4 설정을 표시하는 대화상자에서 **가상 하드웨어** 탭을 선택합니다.
- 5 **메모리** 섹션을 확장하고 **제한을 제한 없음**으로 설정합니다.
- 6 [기타 디바이스]에서 **새 디바이스 추가** 버튼을 클릭하고 **PCI 디바이스**를 선택합니다.
 

**새 PCI 디바이스** 드롭다운 메뉴가 **가상 하드웨어** 탭의 목록에 추가됩니다.
- 7 **새 PCI 디바이스** 드롭다운 메뉴에서 사용할 패스스루 디바이스를 선택하고 **확인**을 클릭합니다.
- 8 가상 시스템 전원 켜기.

## 결과

가상 시스템에 DirectPath I/O 디바이스를 추가하면 가상 시스템의 메모리 크기로 메모리 예약이 설정됩니다.

## VMDirectPath I/O 디바이스에 대한 무중단 추가 및 무중단 제거 지원

패스스루 디바이스를 구성하면 리소스를 효율적으로 사용하고 환경의 성능을 향상시킬 수 있습니다.

vSphere 8.0 및 이전 버전에서는 VM의 전원이 꺼진 경우에만 패스스루 디바이스가 추가되거나 제거되었습니다. vSphere의 현재 버전은 VMDirectPath I/O 디바이스에 대한 무중단 추가 및 무중단 제거 지원을 제공합니다. 무중단 추가는 VM의 전원이 켜져 있을 때 패스스루 디바이스를 추가하는 절차를 말합니다.

다음 기능은 VMDirectPath I/O 디바이스에 대한 무중단 추가 및 무중단 제거 지원에 사용할 수 있습니다.

- vSphere API를 통해 패스스루 지원 디바이스를 VM에 무중단 추가합니다. 이 작업은 다음 방법 중 하나로 수행할 수 있습니다.
  - a ESXi 부팅 시 검색된 기존 디바이스에 대해 패스스루를 사용하도록 설정하고 해당 디바이스를 VM에 무중단 추가합니다.
  - b 또는 호스트의 빈 PCIe 핫 플러그 슬롯에 새 디바이스를 물리적으로 무중단 추가하고 새로 추가된 디바이스에 대한 패스스루를 사용하도록 설정한 다음 디바이스를 VM에 무중단 추가할 수 있습니다.

---

**참고** 이 기능을 사용하려면 서버에 대한 PCIe 네이티브 핫 플러그 인증이 필요합니다.

- vSphere API를 통해 패스스루 디바이스를 VM에서 무중단 제거합니다.
- VM에서 사용 중인 패스스루 디바이스를 서프라이즈 무중단 제거하는 것은 호스트에서 디바이스를 물리적으로 끌어내는 것일 수 있습니다.

---

**참고** 이 기능을 사용하려면 서버에 대한 PCIe 네이티브 서프라이즈 핫 플러그 인증이 필요합니다.

---

**참고** VMDirectPath I/O의 무중단 추가 및 무중단 제거는 NVMe 디바이스에 대해서만 지원됩니다. vSphere Client에서는 VMdirectPath I/O의 무중단 추가 및 무중단 제거에 대한 지원을 사용할 수 없습니다.

---

패스스루의 핫 플러그가 사용되도록 설정된 VM에는 다음 기능이 지원되지 않습니다.

- 게스트 운영 체제에 노출되는 IOMMU(입/출력 메모리 관리 장치).
- CPU 핫 플러그.
- 메모리 핫 플러그.
- 동적 DirectPath I/O.
- vCPU 수가 128개를 초과하는 VM 지원.
- 인터럽트 게시라고도 하는 가상 인터럽트는 패스스루의 핫 플러그가 사용되도록 설정된 VM에 대해 사용하지 않도록 설정될 수 있습니다.
- 호스트에서 패스스루 디바이스의 정상적인 물리적 무중단 제거는 지원되지 않습니다.
- 무중단 추가 및 무중단 제거에 대한 UI 지원.
- VM DirectPath I/O에서 사용할 수 없는 모든 기능.

## 플랫폼, 디바이스 및 게스트 운영 체제에 대한 요구 사항

### 서버 및 장치 요구 사항

- VMDirectPath I/O 디바이스의 무중단 추가 및 무중단 제거 기능을 서버 OEM(원래 장비 제조업체)이 지원하는지 확인합니다.
- 서버 플랫폼 펌웨어는 UEFI(Unified Extensible Firmware Interface)여야 합니다.
- 서버 플랫폼 및 디바이스가 KB 2142307에 언급된 요구 사항을 준수하는지 확인합니다.
- 서버가 VM DirectPath I/O에 대해 인증되어야 합니다.
- VM에서 패스스루 디바이스를 서프라이즈 무중단 제거하려면 서버 모델이 PCIe 네이티브 서프라이즈 핫 플러그 인증을 받아야 합니다.

---

**참고** 서버 인증에 대한 자세한 내용은 [VMware 호환성 가이드](#)를 참조하십시오.

---

## 게스트 운영 체제 요구 사항

- 게스트 운영 체제에서 NVMe 핫 플러그 및 NVMe 서프라이즈 무중단 제거가 지원되는지 확인합니다.
- NVMe 드라이버 I/O 스택의 모든 수정 사항이 포함된 안정적인 최신 GOS 배포판을 사용합니다.

## vCenter 및 ESXi 요구 사항

ESXi 및 vCenter 버전은 8.0 업데이트 1 이상이어야 합니다.

## 제한

- 단일 ReconfigureVM API 호출에서 무중단 추가할 수 있는 최대 패스스루 디바이스 수는 1개입니다.
- 단일 ReconfigureVM API 호출에서 무중단 제거할 수 있는 최대 패스스루 디바이스 수는 1개입니다.
- 패스스루 디바이스 무중단 추가 또는 무중단 제거가 요청된 경우 동일한 ReconfigureVM API 호출에서 다른 VM 재구성 변경을 요청할 수 없습니다.
- VM이 지원할 수 있는 최대 NVMe 패스스루 디바이스 수는 32개입니다.

## VMDirectPath I/O 디바이스의 무중단 추가 및 무중단 제거 사용

vCenter 및 ESXi 호스트를 준비하여 VMDirectPath I/O 디바이스의 무중단 추가 및 무중단 제거를 사용하도록 설정할 수 있습니다.

### 사전 요구 사항

vCenter 및 ESXi 호스트를 준비합니다.

- 빌드 조합으로 vCenter 및 상태 저장 설치 ESXi를 배포합니다.
- VMKernel 부팅 매개 변수를 설정합니다.

```
set -s maxIntrCookies -v 4096
```

- ESXi 호스트를 다시 시작합니다.
- 데이터 센터를 배포하고 호스트를 추가합니다.

### 절차

- 1 vSphere Client에서 호스트를 찾습니다.
- 2 구성 탭에서 **하드웨어**를 확장하고 **PCI 디바이스**를 클릭합니다.
- 3 **NVMe PCI** 디바이스를 선택하고 **패스스루 전환**을 누릅니다.

### 다음에 수행할 작업

VM을 준비하고 구성합니다.

## VM 준비 및 구성

패스스루 디바이스를 구성하면 리소스를 효율적으로 사용하고 환경의 성능을 향상시킬 수 있습니다. 가상 시스템을 준비하고 구성할 수 있습니다.

VM 배포 및 구성(UEFI 부팅)

### 절차

- 1 vSphere Client에서 가상 시스템을 찾습니다.
  - a 가상 시스템을 찾으려면 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택합니다.
  - b **VM** 탭을 클릭합니다.
- 2 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 3 **메모리** 섹션을 확장하고 **모든 게스트 메모리 예약(모두 잠김)**을 설정합니다.
- 4 **저장**을 클릭합니다.
- 5 vSphere API `ReconfigVM_Task()`를 사용하여 VM에 대해 `fixedPassthruHotPlugEnabled`를 **TRUE**로 설정합니다. 자세한 내용은 <https://developer.broadcom.com>에서 참조하십시오.

---

**참고** <https://developer.broadcom.com>의 검색 창을 사용하여 "핫 플러그"라는 용어를 검색합니다.

- a vCenter에서 `vmx-20`에 대해 **VM** → **호환성** → **VM 호환성 업그레이드**를 마우스 오른쪽 버튼으로 클릭하고 [저장]을 클릭합니다.
- b vSphere API를 사용하여 `motherboardLayout`을 `ACPI`로 설정합니다. 자세한 내용은 <https://developer.broadcom.com>의 내용을 참조하십시오.

---

**참고** <https://developer.broadcom.com>의 검색 창을 사용하여 "핫 플러그"라는 용어를 검색합니다.

- 6 (선택 사항) 패스스루 지원 PCI 디바이스를 VM에 추가합니다.
- 7 VM의 전원을 켭니다.

---

**참고** 다음 핫 플러그 작업을 진행하기 전에 진행 중인 핫 플러그 작업이 성공했는지 확인합니다.

- 8 vSphere API를 사용하여 패스스루 디바이스의 무중단 추가 및 무중단 제거를 수행합니다. 자세한 내용은 <https://developer.broadcom.com>의 내용을 참조하십시오.

---

**참고** <https://developer.vmware.com/samples>의 검색 창을 사용하여 "핫 플러그"라는 용어를 검색합니다.

### 다음에 수행할 작업

핫 플러그 작업이 성공했는지 확인합니다.

## vSphere Client를 사용하여 핫 플러그 작업이 성공했는지 확인

무중단 추가, 무중단 제거 및 서프라이즈 무중단 제거 작업이 성공했는지 확인하려면 vSphere Client를 사용하여 확인할 수 있습니다.

### 절차

- 1 vSphere Client에서 가상 시스템을 찾습니다.
- 2 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택하고 VM 탭을 클릭합니다.
- 3 가상 시스템을 클릭하고 목록에서 가상 시스템을 클릭합니다.
- 4 PCI 디바이스 테이블에서 다음을 확인합니다.

옵션	설명
vSphere API를 사용하여 패스스루 지원 디바이스를 VM에 무중단 추가하는 데 성공했는지 확인합니다.	무중단 추가된 패스스루 디바이스가 표시됩니다.
vSphere API를 사용하여 패스스루 디바이스를 VM에서 무중단 제거하는 데 성공했는지 확인합니다.	무중단 제거된 패스스루 디바이스가 표시되지 않습니다.
VM의 패스스루 디바이스를 ESXi 호스트에서 서프라이즈 무중단 제거(물리적 무중단 제거)하는 데 성공했는지 확인합니다.	<ul style="list-style-type: none"> <li>■ 서프라이즈 무중단 제거된 디바이스가 표시되지 않습니다.</li> <li>■ 호스트 보기의:               <ol style="list-style-type: none"> <li>1 vSphere Client에서 호스트를 찾습니다.</li> <li>2 구성 탭에서 하드웨어를 확장하고 PCI 디바이스를 클릭합니다.</li> <li>3 서프라이즈 무중단 제거된 디바이스가 표시되지 않는지 확인합니다.</li> </ol> </li> </ul>

## VM을 사용하여 핫 플러그 작업이 성공했는지 확인

무중단 추가, 무중단 제거 및 서프라이즈 무중단 제거 작업이 성공했는지 확인하려면 가상 시스템을 사용하여 확인할 수 있습니다.

### 절차

- 1 가상 시스템에서 게스트 운영 체제에 대한 SSH 연결을 엽니다.
- 2 루트 사용자로 로그인합니다.
- 3 lspci 명령을 실행합니다.

#### 4 결과를 확인합니다.

옵션	설명
vSphere API를 사용하여 패스루 지원 디바이스를 VM에 무중단 추가하는 데 성공했는지 확인합니다.	무중단 추가된 패스루 디바이스가 표시됩니다.  <b>참고</b> 패스루 디바이스의 SBDF(Spotfire Binary Data File) 주소가 호스트의 해당 주소와 다를 수 있습니다.
vSphere API를 사용하여 패스루 디바이스를 VM에서 무중단 제거하는 데 성공했는지 확인합니다.	무중단 제거된 패스루 디바이스가 표시되지 않습니다.
VM의 패스루 디바이스를 ESXi 호스트에서 서프라이즈 무중단 제거(물리적 무중단 제거)하는 데 성공했는지 확인합니다.	서프라이즈 무중단 제거된 디바이스가 표시되지 않습니다.

## SR-IOV(단일 루트 I/O 가상화)란?

vSphere는 단일 루트 I/O 가상화(SR-IOV)를 지원합니다. 지연 시간에 민감하거나 더 많은 CPU 리소스가 필요한 가상 시스템의 네트워킹에 SR-IOV를 사용할 수 있습니다.

### SR-IOV 개요

SR-IOV는 단일 루트 포트 아래의 단일 PCIe(Peripheral Component Interconnect Express) 물리적 디바이스가 하이퍼바이저 또는 게스트 운영 체제에 여러 개별 물리적 디바이스로 표시되도록 하는 규격입니다.

SR-IOV에서는 PF(물리적 기능) 및 VF(가상 기능)를 사용하여 SR-IOV 디바이스의 글로벌 기능을 관리합니다. PF는 SR-IOV 기능을 구성하고 관리할 수 있는 전체 PCIe 기능입니다. PF를 사용하여 PCIe 디바이스를 구성하거나 제어할 수 있으며, PF에는 디바이스 안팎으로 데이터를 이동하는 모든 기능이 있습니다. VF는 데이터 흐름을 지원하지만 구성 리소스 집합이 제한된 경량 PCIe 기능입니다.

하이퍼바이저 또는 게스트 운영 체제에 제공되는 가상 기능의 수는 디바이스에 따라 다릅니다. SR-IOV 지원 PCIe 디바이스를 사용하려면 적절한 BIOS 및 하드웨어 지원뿐 아니라 게스트 운영 체제 드라이버 또는 하이퍼바이저 인스턴스의 SR-IOV 지원도 필요합니다. [SR-IOV 지원](#)의 내용을 참조하십시오.

### vSphere에서 SR-IOV 사용

vSphere에서 가상 시스템은 네트워킹에 SR-IOV 가상 기능을 사용할 수 있습니다. 가상 시스템과 물리적 어댑터는 VMkernel을 중재자로 사용하지 않고 직접 데이터를 주고받습니다. 네트워킹에서 VMkernel을 우회하면 지연 시간이 줄고 CPU 효율성이 향상됩니다.

vSphere에서는 가상 스위치(표준 스위치 또는 Distributed Switch)가 해당 스위치에 연결된 SR-IOV 지원 가상 시스템의 네트워크 트래픽을 처리하지 않더라도 포트 그룹 또는 포트 수준에서 스위치 구성 정책을 사용하여 할당된 가상 기능을 제어할 수 있습니다.



## SR-IOV 지원

vSphere는 특정 구성의 환경에서만 SR-IOV를 지원합니다. vSphere의 일부 기능은 SR-IOV를 사용하도록 설정할 경우 작동하지 않습니다.

### 지원되는 구성

vSphere에서 SR-IOV를 사용하려면 사용 환경이 몇 가지 구성 요구 사항을 충족해야 합니다.

표 10-1. SR-IOV 사용 시 지원되는 구성

구성 요소	요구 사항
물리적 호스트	<ul style="list-style-type: none"> <li>■ ESXi 릴리스와 호환되어야 합니다.</li> <li>■ Intel 또는 AMD 프로세서가 있어야 합니다.</li> <li>■ IOMMU(입/출력 메모리 관리 장치)를 지원해야 하고 BIOS에서 IOMMU를 사용하도록 설정해야 합니다.</li> <li>■ SR-IOV를 지원해야 하고 BIOS에서 SR-IOV를 사용하도록 설정해야 합니다. 서버 벤더에 문의하여 호스트에서 SR-IOV를 지원하는지 여부를 확인합니다.</li> </ul>
물리적 NIC	<ul style="list-style-type: none"> <li>■ ESXi 릴리스와 호환되어야 합니다.</li> <li>■ 서버 벤더의 기술 설명서에 따라 호스트 및 SR-IOV에서 사용할 수 있도록 지원되어야 합니다.</li> <li>■ 펌웨어에서 SR-IOV를 사용하도록 설정해야 합니다.</li> <li>■ MSI-X 인터럽트를 사용해야 합니다.</li> </ul>
물리적 NIC에 사용할 ESXi의 PF 드라이버	<ul style="list-style-type: none"> <li>■ VMware의 인증을 받아야 합니다.</li> <li>■ ESXi 호스트에 설치해야 합니다. ESXi 릴리스는 일부 NIC의 기본 드라이버를 제공하지만 나머지 NIC의 경우 드라이버를 다운로드하여 수동으로 설치해야 합니다.</li> </ul>
게스트 운영 체제	NIC 벤더의 기술 설명서에 따라 설치된 ESXi 릴리스의 NIC에서 지원되어야 합니다.
게스트 OS의 VF 드라이버	<ul style="list-style-type: none"> <li>■ NIC와 호환되어야 합니다.</li> <li>■ NIC 벤더의 기술 설명서에 따라 게스트 OS 릴리스에서 지원되어야 합니다.</li> <li>■ Windows 가상 시스템에 대해 Microsoft WLK 또는 WHCK 인증을 받아야 합니다.</li> <li>■ 운영 체제에 설치해야 합니다. 운영 체제 릴리스에는 일부 NIC의 기본 드라이버가 포함되어 있지만 나머지 NIC의 경우 해당 NIC 또는 호스트 벤더가 제공하는 위치에서 드라이버를 다운로드하여 설치해야 합니다.</li> </ul>

물리적 호스트와 NIC가 ESXi 릴리스와 호환되는지 확인하려면 "VMware 호환성 가이드" 를 참조하십시오.

### 기능 사용 가능 여부

다음 기능은 SR-IOV로 구성된 가상 시스템에 사용할 수 없습니다.

- vSphere vMotion
- Storage vMotion

- vShield
- NetFlow
- VXLAN 가상 와이어
- vSphere High Availability
- vSphere Fault Tolerance
- vSphere DRS
- vSphere DPM
- 가상 시스템 일시 중단 및 재개
- 가상 시스템 스냅샷
- 패스스루 가상 기능에 대한 MAC 기반 VLAN
- 가상 디바이스, 메모리 및 vCPU의 핫 추가 및 제거
- 클러스터 환경 참가
- SR-IOV 패스스루를 사용하는 가상 시스템 NIC에 대한 네트워크 통계

---

**참고** SR-IOV를 사용하여 지원되지 않는 기능을 사용하도록 설정하거나 구성하려고 하면 해당 환경에서 예기치 않은 동작이 발생합니다.

---

## 지원되는 NIC

모든 NIC에 SR-IOV를 지원하는 드라이버 및 펌웨어가 있어야 합니다. 일부 NIC의 경우 SR-IOV 기능을 펌웨어에서 사용하도록 설정해야 할 수 있습니다. SR-IOV로 구성된 가상 시스템에 대해 지원되는 NIC를 알아보려면 [VMware 호환성 가이드](#)를 참조하십시오.

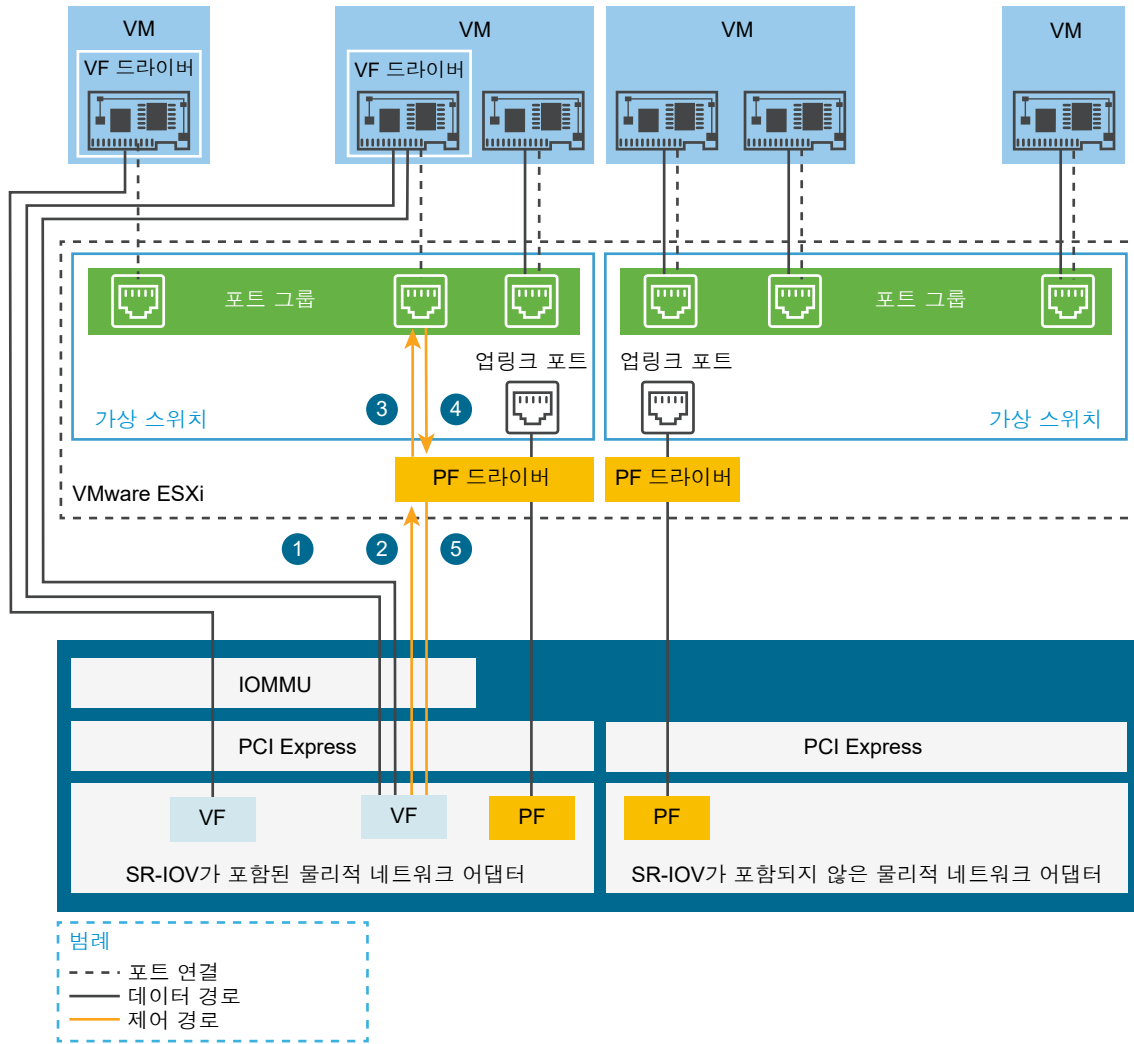
## SR-IOV 구성 요소 아키텍처 및 상호 작용

vSphere SR-IOV 지원을 사용하려면 성능 향상을 위해 VF(가상 기능)와 PF(물리적 기능) 간의 상호 작용이 필요하고 트래픽 제어를 위해 PF 드라이버와 호스트 스위치 간의 상호 작용이 필요합니다.

SR-IOV 물리적 어댑터의 상위 수준에서 가상 시스템 트래픽을 실행하는 호스트의 경우, 가상 시스템 어댑터는 가상 기능에 직접 연결하여 데이터를 주고받습니다. 그러나 네트워크를 구성하는 기능은 가상 시스템을 유지하는 포트의 활성화 정책을 기반으로 합니다.

SR-IOV를 사용하지 않는 ESXi 호스트의 경우 가상 스위치는 관련 포트 그룹의 물리적 어댑터로 들어오고 나가는 외부 네트워크 트래픽을 호스트의 포트를 통해 보냅니다. 또한 가상 스위치는 관리되는 패킷에 네트워킹 정책을 적용합니다.

그림 10-1. vSphere SR-IOV 지원의 데이터 및 구성 경로



데이터 경로는 가상 시스템을 NIC의 가상 기능에 직접 연결합니다. 제어 경로는 가상 시스템의 가상 스위치 및 활성 정책을 포함합니다.

### SR-IOV의 데이터 경로

가상 시스템 네트워크 어댑터가 가상 기능에 할당되면 게스트 운영 체제의 VF 드라이버에서 네트워크를 통해 데이터를 받거나 보내야 하는 가상 기능에 액세스할 때 IOMMU(입/출력 메모리 관리 장치) 기술을 사용합니다. VMkernel, 특히 가상 스위치는 데이터 흐름을 처리하지 않으므로 SR-IOV 지원 워크로드의 총 지연 시간이 줄어 듭니다.

### SR-IOV의 구성 경로

게스트 운영 체제가 VF에 매핑된 가상 시스템 어댑터의 구성을 변경하려고 할 경우 가상 시스템 어댑터에 연결된 포트의 정책에 따라 변경이 허용되면 변경 작업이 수행됩니다.

구성 워크플로우는 다음과 같은 작업으로 구성됩니다.

- 1 게스트 운영 체제가 VF의 구성 변경을 요청합니다.
- 2 VF는 편지함 메커니즘을 통해 이 요청을 PF에 전달합니다.
- 3 PF 드라이버는 가상 스위치(표준 스위치 또는 Distributed Switch의 호스트 프록시 스위치)를 사용하여 구성 요청을 검사합니다.
- 4 가상 스위치는 VF 지원 가상 시스템 어댑터가 연결된 포트의 정책을 기준으로 구성 요청을 확인합니다.
- 5 새 설정이 가상 시스템 어댑터의 포트 정책 규정을 준수하면 PF 드라이버가 VF를 구성합니다.

예를 들어 VF 드라이버가 MAC 주소를 수정하려고 할 경우 해당 포트 그룹 또는 포트의 보안 정책에 따라 MAC 주소 변경이 허용되지 않으면 해당 주소가 동일하게 유지됩니다. 게스트 운영 체제는 변경에 성공한 것으로 표시할 수 있지만 로그 메시지는 작업에 실패한 것으로 표시됩니다. 결과적으로 게스트 운영 체제와 가상 디바이스는 서로 다른 MAC 주소를 저장하게 됩니다. 이 경우 게스트 운영 체제의 네트워크 인터페이스는 IP 주소를 얻을 수 없어 통신하지 못할 수도 있습니다. 이 경우 게스트 운영 체제의 인터페이스를 재설정하여 가상 디바이스가 최신 MAC 주소를 가져오고 IP 주소를 얻도록 해야 합니다.

## vSphere와 가상 기능의 상호 작용

VF(가상 기능)는 데이터 교환에 필요한 모든 리소스가 포함되어 있지만 구성 리소스 집합이 최소화된 경량 PCIe 기능입니다. 따라서 vSphere와 VF 간의 상호 작용은 제한적입니다.

- 물리적 NIC는 MSI-X 인터럽트를 사용해야 합니다.
- VF는 vSphere에서 비율 제어를 구현하지 않습니다. 모든 VF는 잠재적으로 물리적 링크의 전체 대역폭을 사용할 수 있습니다.
- VF 디바이스가 가상 시스템에서 패스스루 디바이스로 구성된 경우 가상 시스템의 대기 및 최대 절전 모드 기능이 지원되지 않습니다.
- 생성할 수 있는 최대 VF 수와 패스스루에 사용할 수 있는 최대 VF 수는 다릅니다. 인스턴스화할 수 있는 최대 VF 수는 NIC 기능과 호스트의 하드웨어 구성에 따라 다릅니다. 그러나 패스스루 디바이스에 사용 가능한 인터럽트 벡터 수가 제한되어 있으므로 ESXi 호스트에서는 인스턴스화된 모든 VF 중 제한된 수만 사용할 수 있습니다.

각 ESXi 호스트의 총 인터럽트 벡터 수는 32개 CPU의 경우 4096개까지 증가할 수 있습니다. 호스트가 부팅될 때 스토리지 컨트롤러, 물리적 네트워크 어댑터 및 USB 컨트롤러와 같은 호스트 디바이스는 벡터 4096개 중 일부를 사용합니다. 이러한 디바이스에 벡터가 1024개보다 많이 필요한 경우 지원될 수 있는 최대 VF 수가 줄어듭니다.

- Intel NIC에서 지원되는 VF 수는 Emulex NIC에서 지원되는 수와 다를 수 있습니다. NIC 벤더의 기술 설명서를 참조하십시오.

- SR-IOV 사용하도록 설정한 Intel NIC 및 Emulex NIC가 있는 경우 Intel NIC에 사용할 수 있는 VF 수는 Emulex NIC에 구성된 VF 수에 따라 달라지고 그 반대의 경우도 마찬가지입니다. 다음 공식을 통해 인터럽트 벡터 3072개를 모두 패스스루에 사용할 수 있는 경우 이용 가능한 최대 VF 수를 예측할 수 있습니다.

$$3x + 2y < 3072$$

여기서  $x$ 는 Intel VF의 수이고  $y$ 는 Emulex VF의 수입니다.

호스트에 있는 다른 유형의 디바이스가 호스트에 있는 벡터 총 4096개 중 인터럽트 벡터를 1024개 넘게 사용하는 경우 이 수는 더 작을 수 있습니다.

- vSphere SR-IOV는 지원되는 Intel 및 Emulex NIC에서 최대 1024개의 VF를 지원합니다.
- vSphere SR-IOV는 지원되는 Intel 또는 Emulex NIC에서 최대 64개의 VF를 지원합니다.
- 지원되는 Intel NIC의 연결이 끊어질 경우 VF 간 통신을 포함하여 물리적 NIC의 모든 VF가 통신을 중지합니다.
- 지원되는 Emulex NIC의 연결이 끊어질 경우 모든 VF는 외부 환경과의 통신을 중지하지만 VF 간 통신은 계속 작동합니다.
- VF 드라이버는 IPv6 지원, TSO, LRO 체크섬과 같은 다양한 기능을 제공합니다. 자세한 내용은 NIC 벤더의 기술 설명서를 참조하십시오.

## DirectPath I/O 및 SR-IOV

SR-IOV에는 DirectPath I/O와 유사한 성능상의 이점과 단점이 있습니다. DirectPath I/O와 SR-IOV는 기능이 유사하지만 다른 목적으로 사용됩니다.

SR-IOV는 매우 높은 패킷 속도나 매우 낮은 지연 시간을 요구하는 워크로드에서 유용합니다. DirectPath I/O와 마찬가지로 SR-IOV는 vMotion과 같은 특정 핵심 가상화 기능과 호환되지 않습니다. 그러나 SR-IOV를 사용할 경우 단일 물리적 디바이스를 여러 게스트 간에 공유할 수 있습니다.

DirectPath I/O를 사용할 경우 하나의 가상 시스템에 하나의 물리적 기능만 매핑할 수 있습니다. SR-IOV를 사용하면 단일 물리적 디바이스를 공유하여 여러 가상 시스템을 물리적 기능에 직접 연결할 수 있습니다.

## SR-IOV를 사용하도록 가상 시스템 구성

SR-IOV 기능을 사용하려면 호스트에서 SR-IOV 가상 기능을 사용하도록 설정하고 가상 시스템을 기능에 연결해야 합니다.

### 사전 요구 사항

사용자 환경의 구성이 SR-IOV를 지원하는지 확인합니다. [SR-IOV 지원](#)을 참조하십시오.

### 절차

#### 1 호스트 물리적 어댑터에서 SR-IOV 사용

가상 시스템을 가상 기능에 연결하기 전에 vSphere Client를 사용하여 SR-IOV를 사용하도록 설정하고 호스트의 가상 기능 수를 설정합니다.


## 2 가상 시스템에 SR-IOV 패스스루 어댑터로 가상 기능 할당

가상 시스템과 물리적 NIC가 데이터를 교환할 수 있게 하려면 가상 시스템을 SR-IOV 패스스루 네트워크 어댑터로 하나 이상의 가상 기능과 연결해야 합니다.

### 결과

트래픽이 표준 스위치 또는 Distributed Switch에 연결된 포트의 활성화 정책을 준수하여 SR-IOV 패스스루 어댑터에서 물리적 어댑터로 전달됩니다.

가상 기능이 SR-IOV 패스스루 네트워크 어댑터에 할당되었는지 검사하려면 가상 시스템의 **요약** 탭에서 **VM 하드웨어** 패널을 확장하고 어댑터의 속성을 확인합니다.

스위치의 토폴로지 다이어그램에는 가상 기능을 사용하는 가상 시스템 어댑터가  아이콘으로 표시됩니다.

### 다음에 수행할 작업

스위치, 포트 그룹 및 포트에 대한 네트워킹 정책을 사용하여 가상 시스템에 연결된 가상 기능을 통과하는 트래픽을 설정합니다. [SR-IOV 지원 가상 시스템과 관련된 트래픽에 대한 네트워킹 옵션](#) 항목을 참조하십시오.

## 호스트 물리적 어댑터에서 SR-IOV 사용

가상 시스템을 가상 기능에 연결하기 전에 vSphere Client를 사용하여 SR-IOV를 사용하도록 설정하고 호스트의 가상 기능 수를 설정합니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 **구성** 탭에서 **네트워킹**을 확장하고 **물리적 어댑터**를 선택합니다.  
SR-IOV 속성을 통해 물리적 어댑터가 SR-IOV를 지원하는지 여부를 확인할 수 있습니다.
- 3 물리적 어댑터를 선택하고 **어댑터 설정 편집**을 클릭합니다.
- 4 SR-IOV의 **상태** 드롭다운 메뉴에서 **사용**을 선택합니다.
- 5 **가상 기능 수** 텍스트 상자에 어댑터에 대해 구성할 가상 기능의 수를 입력합니다.  
값이 0이면 해당 물리적 기능에 대해 SR-IOV가 사용되지 않도록 설정됩니다.
- 6 **확인**을 클릭합니다.
- 7 호스트를 다시 시작합니다.

### 결과

물리적 어댑터 항목이 나타내는 NIC 포트에서 가상 기능이 활성화됩니다. 또한 호스트의 **설정** 탭에 있는 PCI 디바이스 목록에 가상 기능이 표시됩니다.

`esxcli network sriovnic vCLI` 명령을 사용하여 호스트의 가상 기능 구성을 검사할 수 있습니다.

### 다음에 수행할 작업

SR-IOV 패스스루 네트워크 어댑터를 통해 가상 시스템을 가상 기능에 연결합니다.

## 가상 시스템에 SR-IOV 패스스루 어댑터로 가상 기능 할당

가상 시스템과 물리적 NIC가 데이터를 교환할 수 있게 하려면 가상 시스템을 SR-IOV 패스스루 네트워크 어댑터로 하나 이상의 가상 기능과 연결해야 합니다.

### 사전 요구 사항

- 호스트에 가상 기능이 존재하는지 확인합니다.
- 가상 기능의 패스스루 네트워킹 디바이스가 호스트의 **설정** 탭에 있는 PCI 디바이스 목록에서 활성 상태인지 확인합니다.
- 가상 시스템이 ESXi 5.5 이상과 호환되는지 확인합니다.
- 가상 시스템이 생성될 때 게스트 운영 체제로 Red Hat Enterprise Linux 6 이상 또는 Windows가 선택되었는지 확인합니다.

### 절차

- 1 vSphere Client에서 가상 시스템을 찾습니다.
  - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택하고 **VM** 탭을 클릭합니다.
  - b **가상 시스템**을 클릭하고 목록에서 가상 시스템을 클릭합니다.
- 2 가상 시스템의 전원을 끕니다.
- 3 [작업] 메뉴에서 [설정 편집]을 선택합니다.
- 4 설정을 표시하는 대화상자에서 **가상 하드웨어** 탭을 선택합니다.
- 5 **새 디바이스 추가** 드롭다운 메뉴에서 **네트워크 어댑터**를 선택합니다.  
[새 네트워크] 섹션이 **가상 하드웨어** 탭의 목록에 추가됩니다.
- 6 새 네트워크 섹션을 확장하고 가상 시스템을 포트 그룹에 연결합니다.  
가상 NIC는 데이터 트래픽에 이 포트 그룹을 사용하지 않습니다. 이 포트 그룹은 데이터 트래픽에서 적용할 네트워크 속성(예: VLAN 태그 지정)을 추출하는 데 사용됩니다.
- 7 **어댑터 유형** 드롭다운 메뉴에서 **PCI 장치 패스스루**를 선택합니다.
- 8 **물리적 기능** 드롭다운 메뉴에서 패스스루 가상 시스템 어댑터를 지원할 물리적 어댑터를 선택합니다.
- 9 게스트 운영 체제의 패킷 MTU를 변경하도록 허용하려면 **게스트 OS MTU 변경** 드롭다운 메뉴를 사용합니다.
- 10 메모리 섹션을 확장하고 **모든 게스트 메모리 예약(모두 잠김)**을 선택한 다음 **확인**을 클릭합니다.  
패스스루 디바이스가 DMA(Direct Memory Access)를 사용하여 메모리에 액세스할 수 있도록 하려면 I/O MMU(I/O 메모리 관리 장치)가 모든 가상 시스템 메모리에 연결해야 합니다.
- 11 가상 시스템의 전원을 켭니다.

## 결과

가상 시스템의 전원을 켜면 ESXi 호스트는 물리적 어댑터에서 사용 가능한 가상 기능을 선택한 후 이를 SR-IOV 패스스루 어댑터에 매핑합니다. 호스트는 가상 시스템이 속한 포트 그룹의 설정을 기준으로 가상 시스템 어댑터 및 기본 가상 기능의 모든 속성에 대해 유효성을 검사합니다.

## SR-IOV 지원 가상 시스템과 관련된 트래픽에 대한 네트워킹 옵션

vSphere에서는 VF(가상 기능)가 연결된 가상 시스템 어댑터의 특정 네트워킹 기능을 구성할 수 있습니다. 트래픽을 처리하는 가상 스위치의 유형(표준 스위치 또는 Distributed Switch)에 따라 스위치, 포트 그룹 또는 포트에 대한 설정을 사용합니다.

표 10-2. VF를 사용하는 가상 시스템 어댑터에 대한 네트워킹 옵션

네트워킹 옵션	설명
MTU 크기	예를 들어 정보 프레임 등을 사용할 수 있도록 MTU의 크기를 변경합니다.
VF 트래픽에 대한 보안 정책	<ul style="list-style-type: none"> <li>게스트 운영 체제에서 VF를 사용하는 가상 시스템 네트워크 어댑터의 초기 설정 MAC 주소를 변경할 경우 <b>MAC 주소 변경</b> 옵션을 설정하여 새 주소에 들어오는 프레임을 허용하거나 거부합니다.</li> <li>VF를 사용하는 어댑터를 포함하여 가상 시스템 네트워크 어댑터에 대해 글로벌 비규칙 모드를 사용하도록 설정합니다.</li> </ul>
VLAN 태그 지정 모드	표준 스위치 또는 분산 스위치에서 VLAN 태그 지정을 구성하고 태그가 지정된 트래픽이 VF와 연결된 가상 시스템에 도달할 수 있도록 합니다(즉, VGT(Virtual Guest Tagging) 사용).

## SR-IOV 물리적 어댑터를 사용하여 가상 시스템 트래픽 처리


vSphere에서는 SR-IOV 지원 물리적 어댑터의 PF(물리적 기능)와 VF(가상 기능)가 모두 가상 시스템 트래픽을 처리하도록 구성할 수 있습니다.

SR-IOV 물리적 어댑터의 PF는 가상 시스템에서 사용하는 VF를 제어하고, 이러한 SR-IOV 지원 가상 시스템의 네트워킹을 처리하는 표준 스위치 또는 Distributed Switch를 통과하는 트래픽을 전송할 수 있습니다.

SR-IOV 물리적 어댑터는 스위치의 트래픽 지원 여부에 따라 여러 가지 모드에서 작동합니다.

### 혼합 모드


물리적 어댑터가 스위치에 연결된 가상 시스템에 가상 기능을 제공하고 스위치에서 비SR-IOV 가상 시스템의 트래픽을 직접 처리합니다.

스위치의 토폴로지 다이어그램에서 SR-IOV 물리적 어댑터가 혼합 모드인지 확인할 수 있습니다. 혼합 모드의 SR-IOV 물리적 어댑터는 표준 스위치용 물리적 어댑터 목록 또는 분산 스위치용 업링크 그룹 어댑터 목록에서  아이콘이 표시됩니다.



## SR-IOV 단독 모드

물리적 어댑터가 가상 스위치에 연결된 가상 시스템에 가상 기능을 제공하지만 스위치에서 비SR-IOV 가상 시스템의 트래픽은 지원하지 않습니다.

물리적 어댑터가 SR-IOV 단독 모드인지 확인하려면 스위치의 토폴로지 다이어그램을 살펴봅니다. 이 모드에서는 물리적 어댑터가 외부 SR-IOV 어댑터라는 별도의 목록에 있고  아이콘이 표시됩니다.

## 비SR-IOV 모드

물리적 어댑터가 VF 인식 가상 시스템과 관련된 트래픽에 사용되지 않고, 비SR-IOV 가상 시스템의 트래픽만 처리합니다.

## 호스트 프로파일 또는 ESXCLI 명령을 사용하여 SR-IOV 사용

ESXCLI 명령 또는 호스트 프로파일을 통해 여러 호스트를 동시에 설정하거나 상태 비저장 호스트를 설정하여 ESXi 호스트에서 가상 기능을 구성할 수 있습니다.

### 호스트 프로파일에서 SR-IOV 사용

여러 호스트나 상태 비저장 호스트의 경우 호스트 프로파일을 사용하여 물리적 NIC의 가상 기능을 구성하고 Auto Deploy를 사용하여 호스트에 프로파일을 적용할 수 있습니다.

호스트 프로파일과 함께 Auto Deploy를 사용하여 ESXi를 실행하는 방법에 대한 자세한 내용은 "vCenter Server 설치 및 설정" 설명서를 참조하십시오.

드라이버 설명서에 나와 있는 대로, 가상 기능의 NIC 드라이버 매개 변수에 대한 `esxcli system module parameters set vCLI` 명령을 사용하여 호스트에서 SR-IOV 가상 기능을 사용하도록 설정할 수도 있습니다. ESXCLI 명령 사용에 대한 자세한 내용은 "ESXCLI 개념 및 예제" 설명서를 참조하십시오.

### 사전 요구 사항

- 사용자 환경의 구성이 SR-IOV를 지원하는지 확인합니다. [SR-IOV 지원](#)을 참조하십시오.
- SR-IOV 지원 호스트를 기반으로 호스트 프로파일을 생성합니다. "vSphere 호스트 프로파일" 설명서를 참조하십시오.

### 절차

- 1 홈 페이지에서 **호스트 프로파일**을 클릭합니다.
- 2 목록에서 호스트 프로파일을 선택하고 **구성** 탭을 클릭합니다.
- 3 **호스트 프로파일 편집**을 클릭하고 **일반 시스템 설정** 노드를 확장합니다.
- 4 **커널 모듈 매개 변수**를 확장하고 가상 기능을 만들기 위한 물리적 기능 드라이버의 매개 변수를 선택합니다.  
예를 들어 Intel 물리적 NIC의 물리적 기능 드라이버에 대한 매개 변수는 `max_vfs`입니다.
- 5 **값** 텍스트 상자에 유효한 가상 기능 수를 심볼로 구분된 목록으로 입력합니다.  
각 목록 항목은 각 물리적 기능에 대해 구성할 가상 기능의 수를 나타냅니다. 값이 0이면 해당 물리적 기능에 대해 SR-IOV가 사용되지 않습니다.

예를 들어 이중 포트가 있는 경우 값을  $x, y$ 로 설정합니다. 여기서  $x$  또는  $y$ 는 단일 포트에 사용하도록 설정할 가상 기능의 수입니다.

단일 호스트에서 목표로 하는 가상 기능의 수가 30인 경우 이중 포트 카드 두 개를  $0, 10, 10, 10$ 으로 설정할 수 있습니다.

---

**참고** 구성에 사용할 수 있도록 지원되는 가상 기능의 수는 시스템 구성에 따라 다릅니다.

---

6 마침을 클릭합니다.

7 필요한 대로 호스트 프로파일 업데이트를 호스트에 적용합니다.

## 결과

호스트의 **설정** 탭에 있는 PCI 디바이스 목록에 가상 기능이 표시됩니다.

## 다음에 수행할 작업

SR-IOV 패스스루 네트워크 어댑터 유형을 사용하여 가상 기능을 가상 시스템 어댑터에 연결합니다. [가상 시스템에 SR-IOV 패스스루 어댑터로 가상 기능 할당](#)의 내용을 참조하십시오.

## ESXCLI 명령을 통해 호스트의 물리적 어댑터에서 SR-IOV를 사용하도록 설정

ESXi에서 콘솔 명령을 실행하여 물리적 어댑터에서 SR-IOV 가상 기능을 생성하여 문제를 해결하거나 호스트를 직접 구성하는 방법을 알아봅니다.

드라이버 설명서에 따라 가상 기능의 NIC 드라이버 매개 변수를 조작하여 호스트에 SR-IOV 가상 기능을 생성할 수 있습니다.

## 사전 요구 사항

vCLI 패키지를 설치하거나, vMA(vSphere Management Assistant) 가상 시스템을 배포하거나, ESXi Shell을 사용합니다. "ESXCLI 시작"의 내용을 참조하십시오.

## 절차

- 1 NIC 드라이버의 가상 기능에 대한 매개 변수를 설정하여 가상 기능을 생성하려면 명령 프롬프트에서 `esxcli system module parameters set` 명령을 실행합니다.

```
esxcli system module parameters set -m driver -p vf_param=w,x,y,z
```

여기서 *driver*는 NIC 드라이버의 이름이고 *vf\_param*은 가상 기능을 생성하기 위한 드라이버별 매개 변수입니다.

쉼표로 구분된 목록을 사용하여 *vf\_param* 매개 변수의 값을 설정할 수 있습니다. 목록의 각 항목은 포트의 가상 기능 수를 나타냅니다. 값이 0이면 해당 물리적 기능에 대해 SR-IOV가 사용되지 않습니다.

이중 포트 NIC가 두 개 있는 경우 값을  $w, x, y, z$ 로 설정할 수 있습니다. 여기서  $w, x, y$  및  $z$ 는 단일 포트에 사용하도록 설정할 가상 기능의 수입니다. 예를 들어 ixgbe 드라이버를 사용하여 두 이중 포트 Intel 카드에 분산되는 가상 기능을 30개 생성하려면 ixgbe 드라이버 및 `max_vfs` 매개 변수에 대한 다음 명령을 실행합니다.

```
esxcli system module parameters set -m ixgbe -p max_vfs=0,10,10,10
```

2 호스트를 다시 시작하여 가상 기능을 생성합니다.

다음에 수행할 작업

SR-IOV 패스스루 네트워크 어댑터 유형을 사용하여 가상 기능을 가상 시스템 어댑터에 연결합니다. [가상 시스템에 SR-IOV 패스스루 어댑터로 가상 기능 할당](#)의 내용을 참조하십시오.

## 가상 시스템에 대한 RDMA란?

vSphere 6.5 이상 릴리스는 반가상화 RDMA(PVRDMA) 네트워크 어댑터가 있는 가상 시스템 간의 RDMA(Remote Direct Memory Access) 통신을 지원합니다.

### RDMA 개요

RDMA를 사용하면 운영 체제 또는 CPU의 관여 없이 한 컴퓨터 메모리에서 다른 컴퓨터 메모리로 직접 메모리 액세스가 가능합니다. 메모리 전송은 RDMA 지원 HCA(호스트 채널 어댑터)에 오프로드됩니다. PVRDMA 네트워크 어댑터가 가상 환경에서 RDMA를 제공합니다.

### vSphere에서 RDMA 사용

vSphere에서 가상 시스템은 PVRDMA 네트워크 어댑터를 사용하여 PVRDMA 디바이스가 있는 다른 가상 시스템과 통신할 수 있습니다. 가상 시스템을 동일한 vSphere Distributed Switch에 연결해야 합니다.

PVRDMA 디바이스는 가상 시스템 간의 통신 방법을 자동으로 선택합니다. 물리적 RDMA 디바이스 여부에 관계 없이 동일한 ESXi 호스트에서 실행되는 가상 시스템의 경우 두 가상 시스템 간에 memcpy 방식으로 데이터가 전송됩니다. 이 경우 물리적 RDMA 하드웨어는 사용되지 않습니다.

다른 ESXi 호스트에 상주하고 물리적 RDMA 연결이 있는 가상 시스템의 경우 물리적 RDMA 디바이스가 Distributed Switch의 업링크여야 합니다. 이 경우 PVRDMA를 통한 가상 시스템 간 통신에 기본 물리적 RDMA 디바이스가 사용됩니다.

서로 다른 ESXi 호스트에서 실행되는 두 가상 시스템의 경우 호스트 중 적어도 하나에 물리적 RDMA 디바이스가 없으면 통신이 TCP 기반 채널로 폴백되고 성능이 저하됩니다.

### PVRDMA 지원

vSphere 6.5 이상은 특정 구성이 있는 환경에서만 PVRDMA를 지원합니다.

### 지원되는 구성

vSphere 6.5 이상에서 PVRDMA를 사용하려면 사용 환경이 몇 가지 구성 요구 사항을 충족해야 합니다.

표 10-3. PVRDMA 사용 시 지원되는 구성

구성 요소	요구 사항
vSphere	<ul style="list-style-type: none"> <li>■ ESXi 호스트 6.5 이상.</li> <li>■ vCenter Server 6.5 이상.</li> <li>■ vSphere Distributed Switch.</li> </ul>
물리적 호스트	<ul style="list-style-type: none"> <li>■ ESXi 릴리스와 호환되어야 합니다.</li> </ul>
HCA(호스트 채널 어댑터)	<ul style="list-style-type: none"> <li>■ ESXi 릴리스와 호환되어야 합니다.</li> </ul> <p><b>참고</b> 다른 ESXi 호스트에 상주하는 가상 시스템은 RDMA 를 사용하기 위해 HCA가 필요합니다. vSphere Distributed Switch에 대한 업링크로서 HCA를 할당해야 합니다. PVRDMA는 NIC 팀 구성을 지원하지 않습니다. HCA는 vSphere Distributed Switch에서 유일한 업링크여야 합니다.</p> <p>동일한 ESXi 호스트에 있는 가상 시스템 또는 TCP 기반 풀백을 사용하는 가상 시스템의 경우 HCA가 필수가 아닙니다.</p>
가상 시스템	<ul style="list-style-type: none"> <li>■ 가상 하드웨어 버전 13 이상</li> </ul>
게스트 운영 체제	<ul style="list-style-type: none"> <li>■ Linux(64비트)</li> </ul>

물리적 호스트와 HCA가 ESXi 릴리스와 호환되는지 확인하려면 "VMware 호환성 가이드" 를 참조하십시오.

**참고** PVRDMA를 사용하여 지원되지 않는 기능을 사용하도록 설정하거나 구성하려고 하면 환경에서 예기치 않은 동작이 발생할 수 있습니다.

## PVRDMA 네임스페이스 지원

vSphere 7.0 이전의 릴리스에서, PVRDMA는 vMotion을 사용하여 가상 시스템을 한 물리적 호스트 서버에서 다른 물리적 호스트 서버로 이동한 후 작업을 다시 시작할 때 물리적 리소스가 동일한 공용 식별자로 할당될 수 있도록 기본 하드웨어의 공용 리소스 식별자를 가상화합니다. 이를 위해, PVRDMA는 리소스를 생성할 때 가상에서 물리적 리소스 식별자로의 변환을 피어로 분산합니다. 이로 인해 많은 수의 리소스를 생성할 때 상당한 추가 오버헤드가 발생합니다.

PVRDMA 네임스페이스를 사용하면 식별자 할당을 조정하지 않고도 여러 가상 시스템을 함께 사용할 수 있으므로 추가적인 오버헤드를 방지할 수 있습니다. 각 가상 시스템에는 RDMA 하드웨어에 분리된 식별자 네임스페이스가 할당되기 때문에 가상 시스템은 다른 가상 시스템과 충돌하지 않고 동일한 범위 내에서 식별자를 선택할 수 있습니다. 물리적 리소스 식별자가 vMotion 후에도 더 이상 변경되지 않으므로 가상에서 물리적 리소스 식별자로 변환이 더 이상 필요하지 않습니다.

PVRDMA 네임스페이스는 가상 시스템 하드웨어 버전 17 이상이 설치된 vSphere 7.0 이상에서 자동으로 사용하도록 설정됩니다. 기본 하드웨어도 PVRDMA 네임스페이스를 지원해야 합니다. 환경의 하드웨어에서 PVRDMA 네임스페이스를 사용하도록 설정하는 방법을 알아보려면 RDMA 벤더 설명서를 참조하십시오.

## PVRDMA 네이티브 끝점 지원

PVRDMA 네이티브 끝점은 vSphere 7.0 업데이트 1 이상 릴리스부터 가상 시스템 하드웨어 버전 18 이상에서 지원됩니다. PVRDMA 네이티브 끝점을 사용하면 PVRDMA가 비 PVRDMA 끝점과 통신할 수 있습니다. PVRDMA 네이티브 끝점을 사용하려면 PVRDMA 네임스페이스를 사용하도록 설정해야 합니다. 환경의 특정 하드웨어에서 PVRDMA 네임스페이스를 사용하도록 설정하는 방법을 알아보려면 RDMA 벤더 설명서를 참조하십시오.

PVRDMA 네이티브 끝점을 사용하도록 가상 시스템을 구성해야 합니다. [PVRDMA 네이티브 끝점을 사용하도록 가상 시스템 구성](#)의 내용을 참조하십시오.

## PVRDMA를 사용하도록 ESXi 호스트 구성

PVRDMA 통신이 가능하도록 ESXi 호스트의 VMkernel 어댑터와 방화벽 규칙을 구성합니다.

### 사전 요구 사항

ESXi 호스트가 PVRDMA의 요구 사항을 충족하는지 확인합니다. [PVRDMA 지원](#)을 참조하십시오.

- [PVRDMA용 VMkernel 어댑터 태그 지정](#)

VMkernel 어댑터를 선택하고 PVRDMA 통신에 사용하도록 설정하는 방법을 알아봅니다.

- [PVRDMA에 대한 방화벽 규칙 사용](#)

ESXi 호스트의 보안 프로파일에서 PVRDMA에 대한 방화벽 규칙을 사용하도록 설정하는 방법을 알아봅니다.

## PVRDMA용 VMkernel 어댑터 태그 지정

VMkernel 어댑터를 선택하고 PVRDMA 통신에 사용하도록 설정하는 방법을 알아봅니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 **구성** 탭에서 **시스템**을 확장합니다.
- 3 **고급 시스템 설정**을 클릭합니다.
- 4 **편집** 버튼을 클릭합니다.
- 5 필터 텍스트 필드를 사용하여 `Net.PVRDMAVmknics`를 찾습니다.
- 6 값 필드를 클릭하고 사용하려는 VMkernel 어댑터의 값(예: vmk0)을 입력합니다.
- 7 **확인**을 클릭합니다.

## PVRDMA에 대한 방화벽 규칙 사용

ESXi 호스트의 보안 프로파일에서 PVRDMA에 대한 방화벽 규칙을 사용하도록 설정하는 방법을 알아봅니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.

- 2 구성 탭에서 **시스템**을 확장합니다.
- 3 **방화벽**을 클릭합니다.
- 4 **편집** 버튼을 클릭합니다.
- 5 필터 텍스트 필드를 사용하여 PVRDMA 규칙을 찾습니다.
- 6 PVRDMA 규칙 옆의 확인란을 선택하고 **확인**을 클릭합니다.

## 가상 시스템에 PVRDMA 어댑터 할당

가상 시스템이 RDMA를 사용하여 데이터를 교환할 수 있으려면 가상 시스템을 PVRDMA 네트워크 어댑터에 연결해야 합니다.

vSphere 7.0.2 이상을 사용하는 경우 가상 시스템에 최대 10개의 PVRDMA 네트워크 어댑터를 추가할 수 있습니다.

### 사전 요구 사항

- 가상 시스템이 실행되는 호스트가 RDMA를 사용하도록 구성되었는지 확인합니다. [PVRDMA를 사용하도록 ESXi 호스트 구성](#)의 내용을 참조하십시오.
- 호스트가 vSphere Distributed Switch에 연결되어 있는지 확인합니다.
- 가상 시스템이 가상 하드웨어 버전 13 이상을 사용하고 있는지 확인합니다.
- 게스트 운영 체제가 Linux 64비트 배포인지 확인합니다.

### 절차

- 1 vSphere Client에서 가상 시스템을 찾습니다.
  - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택하고 **VM** 탭을 클릭합니다.
  - b **가상 시스템**을 클릭하고 목록에서 가상 시스템을 클릭합니다.
- 2 가상 시스템의 전원을 끕니다.
- 3 [작업] 메뉴에서 [설정 편집]을 선택합니다.
- 4 설정을 표시하는 대화상자에서 **가상 하드웨어** 탭을 선택합니다.
- 5 **새 디바이스 추가** 드롭다운 메뉴에서 **네트워크 어댑터**를 선택합니다.  
[새 네트워크] 섹션이 **가상 하드웨어** 탭의 목록에 추가됩니다.
- 6 [새 네트워크] 섹션을 확장하고 가상 시스템을 분산 포트 그룹에 연결합니다.
- 7 **어댑터 유형** 드롭다운 메뉴에서 PVRDMA를 선택합니다.
- 8 **메모리** 섹션을 확장하고 **모든 게스트 메모리 예약(모두 잠김)**을 선택한 다음 **확인**을 클릭합니다.
- 9 가상 시스템의 전원을 켭니다.

## PVRDMA 네이티브 끝점을 사용하도록 가상 시스템 구성

PVRDMA 네이티브 끝점은 고급 가상 시스템 구성으로 사용할 수 있습니다.

PVRDMA 네이티브 끝점은 vSphere 7.0 업데이트 1 이상 릴리스부터 가상 시스템 하드웨어 버전 18 이상에서 지원됩니다. PVRDMA 네이티브 끝점을 사용하려면 PVRDMA 네임스페이스를 사용하도록 설정해야 합니다. 환경의 특정 하드웨어에서 PVRDMA 네임스페이스를 사용하도록 설정하는 방법을 알아보려면 벤더 설명서를 참조하십시오.

vSphere Client를 사용하여 네이티브 끝점을 구성하거나 가상 시스템의 VMX 파일을 편집할 수 있습니다. VMX 파일을 직접 편집하는 경우 `vrddmax.nativeEndpointSupport = "TRUE"` 매개 변수를 추가합니다. 여기서 *x*는 PVRDMA 어댑터의 인덱스입니다. 다음 절차에서는 vSphere Client를 사용하여 네이티브 끝점을 구성합니다.

### 사전 요구 사항

환경이 PVRDMA를 지원하는지 확인합니다. [PVRDMA 지원](#)의 내용을 참조하십시오.

### 절차

- 1 vSphere Client에서 가상 시스템을 찾습니다.
  - a 가상 시스템을 찾으려면 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택합니다.
  - b **VM** 탭을 클릭합니다.
- 2 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 3 **VM 옵션**을 클릭합니다.
- 4 **고급**을 확장합니다.
- 5 구성 매개 변수에서 **구성 편집** 버튼을 클릭합니다.
- 6 대화상자가 나타나면 **행 추가**를 클릭하여 새 매개 변수와 그 값을 입력합니다.
- 7 `vrddmax.nativeEndpointSupport` 매개 변수를 입력합니다. 여기서 *x*는 PVRDMA 어댑터의 인덱스이며 값은 **TRUE**로 설정합니다.

인덱스 *x*는 PVRDMA 어댑터의 번호에서 1을 뺀 값입니다. 예를 들어 네이티브 끝점을 사용하도록 설정하려는 PVRDMA 어댑터에 "네트워크 어댑터 2"라는 레이블이 지정된 경우 인덱스는 1입니다.

## PVRDMA 비동기 모드를 사용하도록 가상 시스템 구성

PVRDMA 비동기 모드를 사용하도록 가상 시스템을 구성하는 방법을 알아봅니다. 고급 가상 시스템 구성으로 사용할 수 있습니다.

PVRDMA 비동기 모드는 vSphere 8.0 이상에서 실행되는 가상 시스템에서 사용할 수 있습니다. 비동기 모드는 가상 시스템에서 실행되는 RDMA 워크로드의 처리량 및 지연 시간을 향상시킬 수 있습니다. 비동기 모드를 사용하도록 설정하면 호스트에서 CPU 사용 증가가 관찰될 수 있습니다. 비동기 모드를 사용 중인 경우 가상 시스템을 높은 지연 시간 감도로 구성하는 것이 좋습니다.

## 사전 요구 사항

환경이 PVRDMA를 지원하는지 확인합니다. [PVRDMA 지원](#)의 내용을 참조하십시오.

### 절차

- 1 vSphere Client에서 가상 시스템을 찾습니다.
  - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택하고 **VM** 탭을 클릭합니다.
  - b **가상 시스템**을 클릭하고 목록에서 가상 시스템을 클릭합니다.
- 2 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 3 **VM 옵션**을 클릭합니다.
- 4 **고급**을 확장합니다.
- 5 구성 매개 변수에서 **구성 편집** 버튼을 클릭합니다.
- 6 대화상자가 나타나면 **행 추가**를 클릭하여 새 매개 변수와 그 값을 입력합니다.
- 7 매개 변수 `vrDMA.asyncMode`를 입력하고 값을 `TRUE`로 설정합니다.

## RDMA over Converged Ethernet의 네트워크 요구 사항

RDMA over Converged Ethernet은 이더넷 네트워크를 통해 지연 시간이 짧고 처리량이 높은 경량의 RDMA 통신을 보장합니다. RoCE를 사용하려면 정보 무손실 트래픽을 지원하도록 구성된 네트워크가 계층 2에만 있거나 계층 2와 계층 3 둘 모두에 있어야 합니다.

RoCE(RDMA over Converged Ethernet)는 네트워크를 많이 사용하는 애플리케이션에 데이터를 보다 빠르게 전송하기 위해 RDMA를 사용하는 네트워크 프로토콜입니다. RoCE는 호스트의 CPU를 관련시키지 않고 호스트 사이의 직접적인 메모리 전송을 허용합니다.

RoCE 프로토콜에는 두 가지 버전이 있습니다. RoCE v1은 링크 네트워크 계층(계층 2)에서 작동합니다. RoCE v2는 인터넷 네트워크 계층(계층 3)에서 작동합니다. RoCE v1과 RoCE v2 모두에는 무손실 네트워크 구성이 필요합니다. RoCE v1의 경우에는 무손실 계층 2 네트워크가 필요하고 RoCE v2의 경우에는 계층 2와 계층 3 모두 무손실 작업을 지원하도록 구성되어야 합니다.

### 무손실 계층 2 네트워크

무손실 계층 2 환경을 보장하려면 트래픽 흐름을 제어할 수 있어야 합니다. 흐름 제어는 네트워크에서 글로벌 일시 중지를 사용하도록 설정하거나 DCB(Data Center Bridging) 그룹을 통해 정의된 PFC(Priority Flow Control) 프로토콜을 사용하여 구현할 수 있습니다. PFC는 802.1Q VLAN 태그의 서비스 클래스 필드를 사용하여 개별 트래픽 우선 순위를 설정하는 계층 2 프로토콜입니다. 이 프로토콜은 개별 서비스 클래스 우선 순위에 따라 수신기를 대상으로 하는 패킷의 전송을 일시 중지합니다. 이 방법으로 단일 링크를 통해 무손실 RoCE 트래픽 및 손실이 허용되는 최상의 기타 트래픽 모두 전달할 수 있습니다. 트래픽 흐름 정체로 인해 중요한 손실 허용 트래픽이 영향을 받을 수 있습니다. 서로 다른 흐름을 분리하려면 PFC 우선 순위가 설정된 VLAN에서 RoCE를 사용할 수 있습니다.



## 무손실 계층 3 네트워크

RoCE v2의 경우 무손실 데이터 전송을 계층 3 라우팅 디바이스에 보존해야 합니다. 계층 3 라우터를 통해 계층 2 PFC 무손실 우선 순위를 전송할 수 있으려면 수신된 패킷의 우선 순위 설정을 계층 3에서 작동하는 해당 DSCP(Differentiated Serviced Code Point) QoS 설정에 매핑하도록 라우터를 구성해야 합니다. 전송된 RDMA 패킷에는 계층 3 DSCP, 계층 2 PCP(Priority Code Point) 또는 둘 모두가 표시됩니다. 패킷 라우터에서 우선 순위 정보를 추출하려면 DSCP 또는 PCP를 사용합니다. PCP를 사용하는 경우, 패킷에는 VLAN 태그가 지정되어야 하며 라우터는 태그의 PCP 비트를 복사하여 다음 네트워크에 전달해야 합니다. 패킷에 DSCP가 표시된 경우, 라우터는 DSCP 비트를 변경되지 않은 상태로 유지해야 합니다.

RoCE v1과 마찬가지로 RoCE v2도 PFC 우선 순위가 설정된 VLAN에서 실행해야 합니다.

---

**참고** RoCE NIC에서 RDMA를 사용할 계획인 경우에는 해당 RoCE NIC를 팀으로 구성하지 않아야 합니다.

---

벤더별 구성 정보는 해당 디바이스 또는 스위치 벤더의 공식 설명서를 참조하십시오.

## Remote Direct Memory Access 네트워크 어댑터 구성

ESXi 호스트에 RDMA(Remote Direct Memory Access) 네트워크 어댑터를 설치하는 방법을 알아봅니다. 설치된 후에는 vSphere Client를 사용하여 RDMA 어댑터와 해당하는 네트워크 어댑터를 보고 VMkernel 바인딩을 구성할 수 있습니다.

RDMA는 원격 운영 체제 및 CPU의 관여 없이 한 호스트의 메모리에서 다른 호스트의 메모리로 직접 메모리 액세스를 제공합니다. 이렇게 하면 더 낮은 지연 시간 및 CPU 로드 그리고 더 빠른 대역폭을 통해 네트워크 및 호스트 성능이 향상됩니다.

### 사전 요구 사항

ESXi 호스트에 RDMA 지원 어댑터를 설치합니다. 예: Mellanox Technologies MT27700 Family ConnectX-4.

## RDMA 가능 네트워크 어댑터 보기

ESXi는 RDMA 지원 네트워크 어댑터를 지원합니다. ESXi 호스트에 이러한 어댑터를 설치하면 vSphere Client에 RDMA 어댑터와 물리적 네트워크 어댑터라는 두 가지 구성 요소가 표시됩니다.

vSphere Client를 사용하여 RDMA 어댑터 및 해당 네트워크 어댑터를 볼 수 있습니다.

### 사전 요구 사항

ESXi 호스트에서 RDMA(RoCE v2)를 지원하는 RDMA 지원 어댑터를 설치합니다. 예: Mellanox Technologies MT27700 Family ConnectX-4.

### 절차

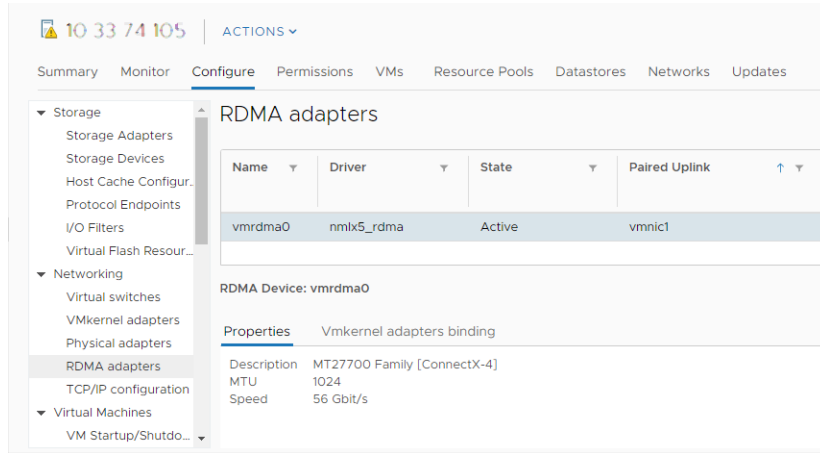
- 1 ESXi 호스트에서 RDMA(RoCE v2)를 지원하는 RDMA 지원 어댑터를 설치합니다.

호스트가 어댑터를 검색하고 vSphere Client에 RDMA 어댑터와 물리적 네트워크 어댑터라는 두 가지 구성 요소가 표시됩니다.

- 2 호스트로 이동합니다.
- 3 네트워킹에서 RDMA 어댑터를 클릭합니다.

이 예에서 RDMA 어댑터는 목록에 `vmrdma0`으로 표시됩니다. **연결된 업링크** 열에는 네트워크 구성 요소가 `vmnic1` 물리적 네트워크 어댑터로 표시됩니다.

그림 10-2. vSphere 환경의 ESXi 호스트에 RDMA 어댑터가 설치됩니다.



- 4 어댑터에 대한 설명을 확인하려면 목록에서 RDMA 어댑터를 선택하고 **속성** 탭을 클릭합니다.

## Remote Direct Memory Access 네트워크 어댑터 구성

RDMA(Remote Direct Memory Access) 네트워크 어댑터를 설치하고 해당 VMkernel 바인딩을 구성할 수 있습니다.

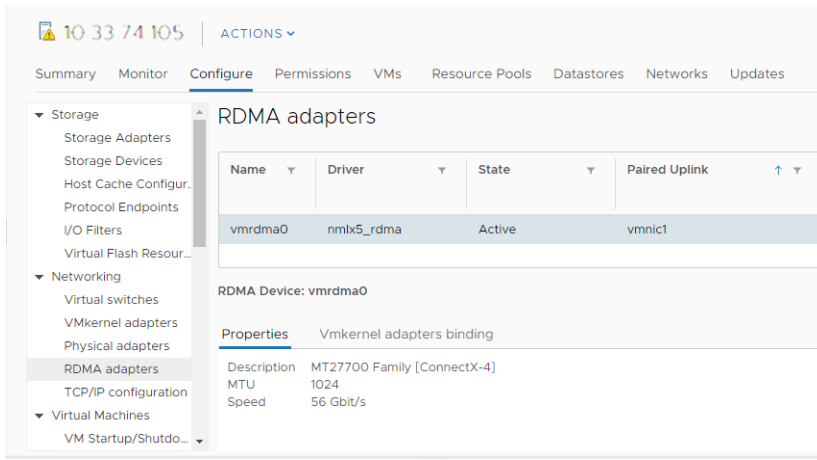
### 절차

- 1 ESXi 호스트에 RDMA(RoCE v2)를 지원하는 RDMA 지원 어댑터를 설치합니다.
 

호스트가 어댑터를 검색하고 vSphere Client에 RDMA 어댑터와 물리적 네트워크 어댑터라는 두 가지 구성 요소가 표시됩니다.
- 2 vSphere Client에서 호스트가 RDMA 어댑터를 검색했는지 확인합니다.
  - a 호스트로 이동합니다.
  - b 구성 탭을 클릭합니다.

c **네트워킹에서 RDMA 어댑터를 클릭합니다.**

이 예에서 RDMA 어댑터는 목록에 `vmrdma0`으로 표시됩니다. **연결된 업링크** 열에는 네트워크 구성 요소가 `vmnic1` 물리적 네트워크 어댑터로 표시됩니다.



d 어댑터에 대한 설명을 확인하려면 목록에서 RDMA 어댑터를 선택하고 **속성** 탭을 클릭합니다.

3 RDMA 어댑터에 대한 VMkernel 바인딩을 구성합니다.

구성에서는 vSphere 표준 스위치 또는 vSphere Distributed Switch를 사용할 수 있습니다. 다음 단계에서는 표준 스위치를 예로 사용합니다.

a vSphere 표준 스위치를 생성하고 네트워크 구성 요소를 스위치에 추가합니다.

**참고** RDMA 어댑터에 해당하는 물리적 네트워크 어댑터를 선택해야 합니다. 이 예에서는 `vmnic1` 어댑터입니다.

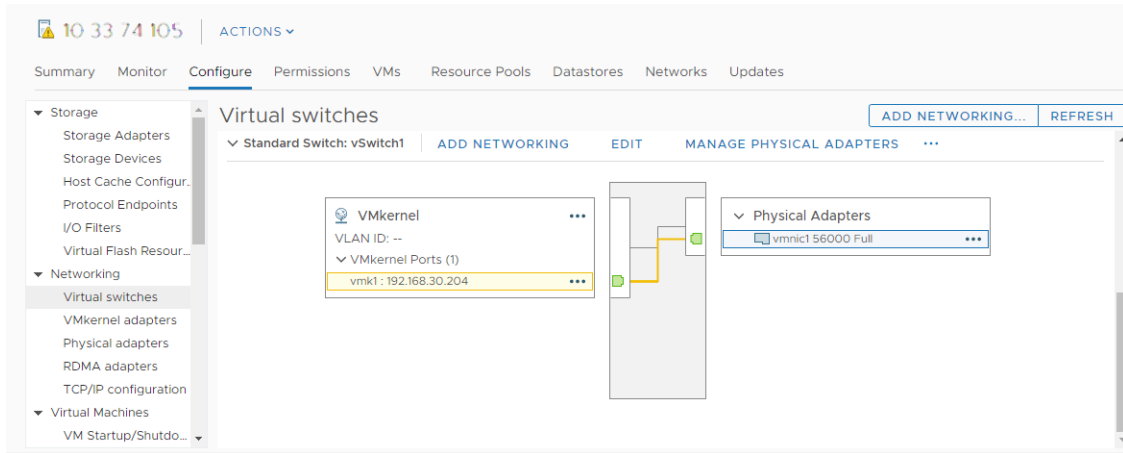
스위치 생성에 대한 자세한 내용은 [vSphere 표준 스위치 생성](#) 또는 [vSphere Distributed Switch 생성](#)의 내용을 참조하십시오.

b 생성한 vSphere 표준 스위치에 VMkernel 어댑터를 추가합니다.

VMkernel 어댑터에 적절한 정적 IPv4 또는 IPv6 주소를 할당합니다. 그래야 RDMA 어댑터가 NVMe over RDMA 대상을 검색할 수 있습니다.

VMkernel 어댑터 추가에 대한 자세한 내용은 [장 4 VMkernel 네트워킹을 설정하는 방법](#)의 내용을 참조하십시오.

이 그림에서는 물리적 네트워크 어댑터와 VMkernel 어댑터가 vSphere 표준 스위치에 연결되어 있음을 보여줍니다. 이 연결을 통해 RDMA 어댑터가 VMkernel 어댑터에 바인딩됩니다.

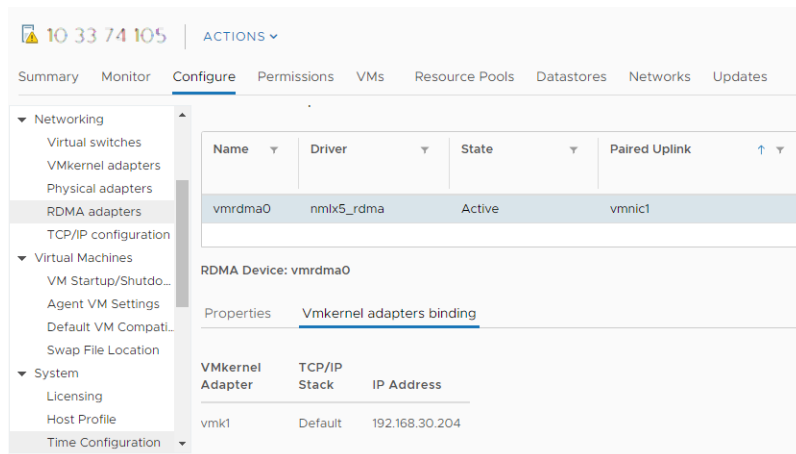


#### 4 RDMA 어댑터에 대한 VMkernel 바인딩 구성을 확인합니다.

a RDMA 어댑터로 이동합니다.

b **VMkernel 어댑터 바인딩** 탭을 클릭하고 연결된 VMkernel 어댑터가 페이지에 나타나는지 확인합니다.

이 예에서 `vmrdma0` RDMA 어댑터는 `vmnic1` 네트워크 어댑터와 쌍을 이루고 `vmk1` VMkernel 어댑터에 연결됩니다.



#### 다음에 수행할 작업

어댑터의 RDMA 네트워크 구성 요소를 iSER 또는 NVMe over RDMA와 같은 스토리지 구성에 사용할 수 있습니다. 자세한 내용은 "vSphere 스토리지" 설명서를 참조하십시오.

## 점보 프레임이란?

점보 프레임을 사용하면 ESXi 호스트에서 더 큰 프레임을 물리적 네트워크에 전송할 수 있습니다. 네트워크는 물리적 네트워크 어댑터, 물리적 스위치 및 스토리지 디바이스를 포함하는 점보 프레임을 완벽하게 지원해야 합니다.

점보 프레임을 사용하도록 설정하기 전에 물리적 네트워크 어댑터가 점보 프레임을 지원하는지 해당 하드웨어 벤더에게 문의하십시오.

MTU(최대 전송 단위)를 1280바이트보다 큰 값으로 변경하여 vSphere Distributed Switch 또는 vSphere standard switch에서 점보 프레임을 사용하도록 설정할 수 있습니다. vCenter Server 7.0 업데이트 3을 사용하면 vSphere Distributed Switch의 MTU(최대 전송 단위) 크기를 최대 9190 바이트로 설정하여 패킷 크기가 더 큰 스위치를 지원할 수 있습니다.

## vSphere Distributed Switch에서 점보 프레임 사용

vSphere Distributed Switch를 통과하는 전체 트래픽에 대해 점보 프레임을 사용하도록 설정합니다.

**중요** vSphere Distributed Switch의 MTU 크기를 변경하면 업링크로 할당된 물리적 NIC가 작동이 중단되었다가 다시 실행됩니다. 이로 인해 업링크를 사용하는 서비스 또는 가상 시스템에 대해 5~10밀리초 동안 잠시 네트워크가 중단됩니다.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **구성** 탭에서 **설정**을 확장하고 **속성**을 선택합니다.
- 3 **편집**을 클릭합니다.
- 4 **고급**을 클릭하고 **MTU** 속성을 1,500바이트보다 큰 값으로 설정합니다.  
MTU 크기를 9190바이트보다 큰 값으로 설정할 수 없습니다.
- 5 **확인**을 클릭합니다.

## vSphere 표준 스위치에서 점보 프레임 사용

호스트의 vSphere 표준 스위치를 통과하는 모든 트래픽에 대해 점보 프레임을 사용하도록 설정합니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 **구성** 탭에서 **네트워킹**을 확장하고 **가상 스위치**를 선택합니다.
- 3 가상 스위치 테이블에서 표준 스위치를 선택하고 **설정 편집**을 클릭합니다.
- 4 **속성** 섹션에서 **MTU** 속성을 1,500바이트보다 큰 값으로 설정합니다.  
MTU 크기를 최대 9,000바이트까지 높일 수 있습니다.
- 5 **확인**을 클릭합니다.

## VMkernel 어댑터에 대한 점보 프레임 사용

점보 프레임은 데이터 전송으로 인해 발생하는 CPU 로드를 줄입니다. VMkernel 어댑터의 MTU(최대 전송 단위)를 변경하여 VMkernel 어댑터에 점보 프레임을 사용하도록 설정할 수 있습니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.

- 2 구성 탭에서 **네트워킹**을 확장하고 **VMkernel 어댑터**를 선택합니다.
- 3 어댑터 표에서 VMkernel 어댑터를 선택합니다.  
어댑터의 속성이 표시됩니다.
- 4 **편집**을 클릭합니다.
- 5 [포트 속성] 페이지에서 **MTU** 속성을 1500보다 큰 값으로 설정합니다.  
MTU 크기를 최대 9,000바이트까지 높일 수 있습니다.
- 6 **확인**을 클릭합니다.

## 가상 시스템에서 점보 프레임 지원 기능 사용

가상 시스템에서 점보 프레임 지원 기능을 사용하려면 해당 가상 시스템에 사용할 고급 VMXNET 어댑터가 필요합니다.

### 절차

- 1 vSphere Client에서 가상 시스템을 찾습니다.
  - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택하고 **VM** 탭을 클릭합니다.
  - b **가상 시스템**을 클릭하고 목록에서 가상 시스템을 클릭합니다.
- 2 [작업] 메뉴에서 [설정 편집]을 선택합니다.
- 3 설정을 표시하는 대화상자에서 **가상 하드웨어** 탭을 선택합니다.
- 4 **네트워크 어댑터** 섹션을 확장합니다. 네트워크 어댑터가 사용하는 네트워크 설정과 MAC 주소를 기록합니다.
- 5 times-circle 버튼을 클릭하여 가상 시스템에서 네트워크 어댑터를 제거합니다.
- 6 **새 디바이스 추가** 드롭다운 메뉴에서 **네트워크 어댑터**를 선택합니다.  
[새 네트워크] 섹션이 [가상 하드웨어] 탭의 목록에 추가됩니다.
- 7 [새 네트워크] 섹션을 확장합니다.
- 8 **어댑터 유형** 드롭다운 메뉴에서 **VMXNET 2(고급)** 또는 **VMXNET 3**을 선택합니다.
- 9 네트워크 설정을 이전의 네트워크 어댑터에 대해 기록해 둔 설정으로 지정합니다.
- 10 **MAC 주소**를 수동으로 설정하고 이전 네트워크 어댑터가 사용하던 MAC 주소를 입력합니다.
- 11 **확인**을 클릭합니다.

### 다음에 수행할 작업

- 고급 VMXNET 어댑터가 점보 프레임을 사용하도록 설정된 표준 스위치 또는 Distributed Switch에 연결되었는지 확인합니다.
- 게스트 운영 체제에서 점보 프레임을 허용하도록 네트워크 어댑터를 구성합니다. 자세한 내용은 게스트 운영 체제의 설명서를 참조하십시오.

- 점보 프레임을 지원하도록 모든 물리적 스위치 및 이 가상 시스템이 연결하는 모든 물리적 시스템 및 가상 시스템을 구성합니다.

## TCP 세분화 오프로드란?

VMkernel 네트워크 어댑터 및 가상 시스템에서 TSO(TCP 세분화 오프로드)를 사용하여 심각한 지연 요구 사항이 있는 워크로드의 네트워크 성능을 향상시키는 방법을 알아봅니다.

물리적 네트워크 어댑터, VMkernel 및 가상 시스템 네트워크 어댑터의 전송 경로에서 TSO를 사용하면 TCP/IP 네트워크 작업에 대한 CPU의 오버헤드가 줄어 ESXi 호스트의 성능이 향상됩니다. TSO를 사용하도록 설정할 경우 네트워크 어댑터가 CPU를 나누는 대신 크기가 큰 데이터 청크를 TCP 세그먼트로 나누기 때문에 VMkernel 및 게스트 운영 체제가 더 많은 CPU 주기를 사용하여 장치를 실행할 수 있습니다.

TSO가 제공하는 성능 향상 혜택을 누리려면 물리적 네트워크 어댑터, VMkernel 및 게스트 운영 체제를 포함하여 ESXi 호스트에서 데이터 경로를 따라 TSO를 사용하도록 설정합니다. 기본적으로 ESXi 호스트의 VMkernel, VMXNET 2 및 VMXNET 3 가상 시스템 어댑터에서 TSO가 사용되도록 설정되어 있습니다.

데이터 경로에서 TCP 패킷 세분화 위치에 대한 자세한 내용은 VMware 기술 자료 문서 [Understanding TCP Segmentation Offload \(TSO\) and Large Receive Offload \(LRO\) in a VMware environment](#)를 참조하십시오.

## VMkernel에서 소프트웨어 TSO 관리

물리적 네트워크 어댑터에 TSO와 관련한 문제가 발생하는 경우 문제가 해결될 때까지 VMkernel에서 TSO의 소프트웨어 시뮬레이션을 일시적으로 사용하도록 설정할 수 있습니다.

### 절차

- ◆ VMkernel에서 TSO의 소프트웨어 시뮬레이션을 활성화 또는 비활성화하려면 이러한 `esxcli network nic software set` 콘솔 명령을 실행합니다.

- VMkernel에서 TSO의 소프트웨어 시뮬레이션을 활성화합니다.

```
esxcli network nic software set --ipv4tso=1 -n vmnicX
esxcli network nic software set --ipv6tso=1 -n vmnicX
```

- VMkernel에서 TSO의 소프트웨어 시뮬레이션을 비활성화합니다.

```
esxcli network nic software set --ipv4tso=0 -n vmnicX
esxcli network nic software set --ipv6tso=0 -n vmnicX
```

여기서 `vmnicX`의 `X`는 호스트의 NIC 포트 수를 나타냅니다.

이 구성 변경 사항은 호스트 재부팅 후에도 유지됩니다.

## TSO가 ESXi 호스트의 물리적 네트워크 어댑터에서 지원되는지 확인하는 방법

지연 시간에 민감한 워크로드를 실행하는 호스트에서 네트워킹 성능을 예상할 때 물리적 네트워크 어댑터가 TCP/IP 패킷 세분화를 오프로드하는지 검사합니다. 물리적 네트워크 어댑터가 TSO를 지원하는 경우 TSO가 기본적으로 사용하도록 설정됩니다.

### 절차

- ◆ TSO가 호스트의 물리적 네트워크 어댑터에서 사용되도록 설정되어 있는지 확인하려면 다음 콘솔 명령을 실행합니다.

```
esxcli network nic tso get
```

## ESXi 호스트에서 TSO 관리

NIC가 큰 데이터 청크를 TCP 세그먼트로 나누도록 하려면 전송 경로에서 TSO(TCP 세분화 오프로드)를 활성화합니다. CPU가 TCP 세분화를 수행하도록 하려면 TSO를 비활성화합니다.

기본적으로 호스트는 물리적 어댑터가 지원하는 경우 하드웨어 TSO를 사용합니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 시스템을 확장합니다.
- 3 고급 시스템 설정을 클릭합니다.
- 4 IPv4에 대한 `Net.UseHwTSO` 매개 변수 및 IPv6에 대한 `Net.UseHwTSO6`의 값을 편집합니다.
  - TSO를 활성화하려면 `Net.UseHwTSO` 및 `Net.UseHwTSO6`을 1로 설정합니다.
  - TSO를 비활성화하려면 `Net.UseHwTSO` 및 `Net.UseHwTSO6`을 0으로 설정합니다.
- 5 확인을 클릭하여 변경 사항을 적용합니다.
- 6 물리적 어댑터의 드라이버 모듈을 다시 로드하려면 호스트의 ESXi Shell에서 `esxcli system module set` 콘솔 명령을 실행합니다.
  - a 드라이버를 비활성화하려면 `esxcli system module set` 명령을 `--enabled false` 옵션과 함께 실행합니다.

```
esxcli system module set --enabled false --module nic_driver_module
```

- b 드라이버를 활성화하려면 `esxcli system module set` 명령을 `--enabled true` 옵션과 함께 실행합니다.

```
esxcli system module set --enabled true --module nic_driver_module
```



## 결과

물리적 어댑터가 하드웨어 TSO를 지원하지 않는 경우 VMkernel은 게스트 운영 체제에서 오는 큰 TCP 패킷을 세분화하여 어댑터로 전송합니다.

## ESXi 호스트에서 TSO가 사용되도록 설정되어 있는지 확인하는 방법

지연 시간에 민감한 워크로드를 실행하는 호스트에 대한 네트워킹 성능을 예측할 때 하드웨어 TSO가 VMkernel에서 사용하도록 설정되어 있는지 검토합니다. 기본적으로 하드웨어 TSO는 ESXi 호스트에서 사용하도록 설정되어 있습니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **시스템**을 확장합니다.
- 3 **고급 시스템 설정**을 클릭합니다.
- 4 `Net.UseHwTSO` 및 `Net.UseHwTSO6` 매개 변수의 값을 검토합니다.

`Net.UseHwTSO`는 IPv4에 대한 TSO 상태를 표시하고 `Net.UseHwTSO6`은 IPv6에 대한 TSO 상태를 표시합니다. 속성이 1로 설정되어 있으면 TSO가 사용하도록 설정됩니다.

## Linux 가상 시스템에서 TSO 관리

게스트 운영 체제에서 세분화가 필요한 TCP 패킷을 VMkernel에 리디렉션하도록 Linux 가상 시스템의 네트워크 어댑터에서 TSO 지원을 활성화합니다.

### 사전 요구 사항

- ESXi가 Linux 게스트 운영 체제를 지원하는지 확인합니다.  
"VMware 호환성 가이드" 설명서를 참조하십시오.
- Linux 가상 시스템의 네트워크 어댑터가 VMXNET2 또는 VMXNET3인지 확인합니다.

### 절차

- ◆ Linux 게스트 운영 체제의 터미널 창에서 TSO를 활성화 또는 비활성화하려면 `ethtool` 명령을 `-K` 및 `tso` 옵션과 함께 실행합니다.
  - TSO를 활성화하려면 다음 명령을 실행합니다.

```
ethtool -K ethY tso on
```

- TSO를 비활성화하려면 다음 명령을 실행합니다.

```
ethtool -K ethY tso off
```

여기서 `eth Y`의 `Y`는 가상 시스템의 NIC 시퀀스 번호입니다.

## Windows 가상 시스템에서 TSO 관리

기본적으로 TSO는 VMXNET2 및 VMXNET3 네트워크 어댑터의 Windows 가상 시스템에서 활성화됩니다. 성능상의 이유로 TSO를 비활성화하려고 할 수 있습니다.

### 사전 요구 사항

- ESXi가 Windows 게스트 운영 체제를 지원하는지 확인합니다. "VMware 호환성 가이드" 설명서를 참조하십시오.
- Windows 가상 시스템의 네트워크 어댑터가 VMXNET2 또는 VMXNET3인지 확인합니다.

### 절차

- 1 Windows 제어판의 네트워크 및 공유 센터에서 네트워크 어댑터의 이름을 클릭합니다.
- 2 이름을 클릭합니다.  
대화상자에 어댑터의 상태가 표시됩니다.
- 3 속성을 클릭하고 네트워크 어댑터 유형에서 구성을 클릭합니다.
- 4 고급 탭에서 Large Send Offload V2(IPv4) 및 Large Send Offload V2(IPv6) 속성을 사용 또는 사용 안 함으로 설정합니다.
- 5 확인을 클릭합니다.
- 6 가상 시스템을 다시 시작합니다.

## 대규모 수신 오프로드란?

LRO(대규모 수신 오프로드)를 사용하여 네트워크에서 도착하는 고속 패킷을 처리하기 위한 CPU 오버헤드를 줄이는 방법을 알아봅니다.

LRO는 들어오는 네트워크 패킷을 큰 버퍼로 재구성하고 크지만 소수인 결과 패킷을 호스트 또는 가상 시스템의 네트워크 스택으로 전송합니다. CPU는 LRO가 비활성화되었을 때보다 적은 수의 패킷을 처리해야 합니다. 이에 따라 특히 대역폭이 높은 연결의 경우에 네트워킹 활용도가 줄어듭니다.

LRO의 성능 향상의 이점을 누리려면 VMkernel 및 게스트 운영 체제를 포함하여 ESXi 호스트의 데이터 경로와 함께 LRO를 사용하도록 설정합니다. 기본적으로 LRO는 VMkernel 및 VMXNET3 가상 시스템 어댑터에서 활성화되어 있습니다.

데이터 경로의 TCP 패킷 집계 위치에 대한 자세한 내용은 VMware 기술 자료 문서 [Understanding TCP Segmentation Offload \(TSO\) and Large Receive Offload \(LRO\) in a VMware environment](#)를 참조하십시오.

## ESXi 호스트의 모든 VMXNET3 어댑터에 대해 하드웨어 LRO 관리

호스트 물리적 어댑터의 하드웨어 기능을 활성화하여 게스트 운영 체제에서 구성하기 위한 리소스를 사용하는 대신 LRO 기술을 사용하여 VMXNET3 VM 어댑터에 대해 들어오는 TCP 패킷을 집계합니다.

**절차**

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **시스템**을 확장합니다.
- 3 **고급 시스템 설정**을 클릭합니다.
- 4 `Net.Vmxnet3HwLRO` 매개 변수의 값을 편집합니다.
  - 하드웨어 LRO를 활성화하려면 `Net.Vmxnet3HwLRO`를 1로 설정합니다.
  - 하드웨어 LRO를 비활성화하려면 `Net.Vmxnet3HwLRO`를 0으로 설정합니다.
- 5 **확인**을 클릭하여 변경 사항을 적용합니다.

**ESXi 호스트의 모든 VMXNET3 어댑터에 대해 소프트웨어 LRO 관리**

호스트 물리적 어댑터가 하드웨어 LRO를 지원하지 않는 경우 VMXNET3 어댑터의 VMkernel 백엔드에서 소프트웨어 LRO를 사용하여 가상 시스템의 네트워킹 성능을 향상합니다.

vSphere에서는 IPv4 패킷과 IPv6 패킷에 대해 소프트웨어 LRO를 지원합니다.

**사전 요구 사항****절차**

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **시스템**을 확장합니다.
- 3 **고급 시스템 설정**을 클릭합니다.
- 4 VMXNET3 어댑터에 대해 `Net.Vmxnet3SwLRO` 매개 변수의 값을 편집합니다.
  - 소프트웨어 LRO를 활성화하려면 `Net.Vmxnet3SwLRO`를 1로 설정합니다.
  - 소프트웨어 LRO를 비활성화하려면 `Net.Vmxnet3SwLRO`를 0으로 설정합니다.
- 5 **확인**을 클릭하여 변경 사항을 적용합니다.

**LRO가 ESXi 호스트의 VMXNET3 어댑터에 대해 사용하도록 설정되어 있는지 확인**

지연 시간에 민감한 워크로드를 실행하는 호스트에서 네트워킹 성능을 예상할 때 ESXi에서 LRO 상태를 검사합니다.

**사전 요구 사항****절차**

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **시스템**을 확장합니다.

3 고급 시스템 설정을 클릭합니다.

4 VMXNET2 및 VMXNET3의 LRO 매개 변수의 값을 검토합니다.

- 하드웨어 LRO의 경우 `Net.Vmxnet3HwLRO` 매개 변수를 검토합니다. 1과 같은 경우 하드웨어 LRO가 사용하도록 설정됩니다.
- 소프트웨어 LRO의 경우 `Net.Vmxnet3SwLRO` 매개 변수를 검토합니다. 1과 같은 경우 하드웨어 LRO가 사용하도록 설정됩니다.

## VMXNET 3 어댑터의 LRO 버퍼 크기 변경

VMXNET 3 네트워크 어댑터를 통해 가상 시스템 연결에 대한 패킷 집계용 버퍼 크기를 변경할 수 있습니다. 워크로드에서 TCP 확인 수를 줄이고 VMkernel의 효율성을 향상시키려면 버퍼 크기를 늘립니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 시스템을 확장합니다.
- 3 고급 시스템 설정을 클릭합니다.
- 4 `Net.VmxnetLROMaxLength` 매개 변수에 1에서 65535 사이의 값을 입력하여 LRO 버퍼 크기를 바이트로 설정합니다.

기본적으로 LRO 버퍼 크기는 32000바이트입니다.

## ESXi 호스트에서 모든 VMkernel 어댑터에 대해 LRO 활성화 또는 비활성화

ESXi 호스트에서 VMkernel 네트워크 어댑터에 대해 LRO를 사용하여 수신 인프라 트래픽의 네트워크 성능을 향상합니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 시스템을 확장합니다.
- 3 고급 시스템 설정을 클릭합니다.
- 4 `Net.TcpipDefLROEnabled` 매개 변수의 값을 편집합니다.
  - 호스트에서 VMkernel 네트워크 어댑터에 대해 LRO를 활성화하려면 `Net.TcpipDefLROEnabled`를 1로 설정합니다.
  - 호스트에서 VMkernel 네트워크 어댑터에 대해 소프트웨어 LRO를 비활성화하려면 `Net.TcpipDefLROEnabled`를 0으로 설정합니다.
- 5 확인을 클릭하여 변경 사항을 적용합니다.

## VMkernel 어댑터에 대한 LRO 버퍼의 크기 변경

VMkernel 연결의 패킷 집계를 위한 버퍼 크기를 변경할 수 있습니다. TCP 확인 수를 줄이고 VMkernel의 효율성을 향상시키려면 버퍼 크기를 늘립니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 시스템을 확장합니다.
- 3 고급 시스템 설정을 클릭합니다.
- 4 `Net.TcpipDefLROMaxLength` 매개 변수에 1에서 65535 사이의 값을 입력하여 LRO 버퍼 크기를 바이트로 설정합니다.

기본적으로 LRO 버퍼 크기는 32768바이트와 동일합니다.

## Linux 가상 시스템의 VMXNET3 어댑터에서 LRO 관리

LRO가 호스트의 VMXNET3 어댑터에 대해 사용하도록 설정된 경우 게스트 운영 체제가 수신 패킷을 큰 버퍼로 집계하기 위해 리소스를 소모하지 않도록 Linux 가상 시스템에서 네트워크 어댑터에 대해 LRO 지원을 활성화합니다.

### 사전 요구 사항

Linux 커널이 2.6.24 이상인지 확인합니다.

### 절차

- ◆ Linux 게스트 운영 체제의 터미널 창에서 `-k` 및 `lro` 옵션과 함께 `ethtool` 명령을 실행합니다.
  - LRO를 활성화하려면 다음 명령을 실행합니다.

```
ethtool -K ethY lro on
```

여기서 `eth Y`의 `Y`는 가상 시스템의 NIC 시퀀스 번호입니다.

- LRO를 비활성화하려면 다음 명령을 실행합니다.

```
ethtool -K ethY lro off
```

여기서 `eth Y`의 `Y`는 가상 시스템의 NIC 시퀀스 번호입니다.

## Windows 가상 시스템의 VMXNET3 어댑터에서 LRO 관리

LRO가 호스트의 VMXNET3 어댑터에 대해 사용하도록 설정된 경우 게스트 운영 체제가 수신 패킷을 큰 버퍼로 집계하기 위해 리소스를 소모하지 않도록 Windows 가상 시스템에서 네트워크 어댑터에 대해 LRO 지원을 활성화합니다.

Windows에서 LRO 기술은 RSC(Receive Side Coalescing)로도 참조됩니다.

## 사전 요구 사항

- 가상 시스템이 Windows Server 2012 이상 또는 Windows 8 이상을 실행하는지 확인합니다.
- 가상 시스템이 ESXi 6.0 이상과 호환되는지 확인합니다.
- 게스트 운영 체제에 설치된 VMXNET3 드라이버의 버전이 1.6.6.0 이상인지 확인합니다.
- LRO가 Windows Server 2012 이상 또는 Windows 8 이상을 실행하는 가상 시스템에서 전체적으로 사용하도록 설정되어 있는지 확인합니다. [Windows 가상 시스템에서 전체적으로 LRO 관리](#)의 내용을 참조하십시오.

## 절차

- 1 게스트 운영 체제의 제어판의 **네트워크 및 공유 센터**에서 네트워크 어댑터의 이름을 클릭합니다.  
대화상자에 어댑터의 상태가 표시됩니다.
- 2 **속성**을 클릭하고 VMXNET3 네트워크 어댑터 유형에서 **구성**을 클릭합니다.
- 3 **고급** 탭에서 **Recv Segment Coalescing(IPv4)**과 **Recv Segment Coalescing(IPv6)**을 **사용** 또는 **사용 안 함**으로 설정합니다.
- 4 **확인**을 클릭합니다.

## Windows 가상 시스템에서 전체적으로 LRO 관리

Windows 8 이상 또는 Windows Server 2012 이상을 실행하는 가상 시스템의 VMXNET3 어댑터에서 LRO(대규모 수신 오프로드)를 사용하려면 게스트 운영 체제에서 전체적으로 LRO를 사용하도록 설정해야 합니다. Windows에서 LRO 기술은 RSC(Receive Side Coalescing)로도 참조됩니다.

## 절차

- 1 LRO가 Windows 8 이상 또는 Windows Server 2012 게스트 OS에서 전체적으로 비활성화되었는지 확인하려면 명령 프롬프트에서 `netsh int tcp show global` 명령을 실행합니다.

```
netsh int tcp show global
```

이 명령은 Windows 8.x OS에서 설정된 글로벌 TCP(Transmission Control Protocol) 매개 변수의 상태를 표시합니다.

```
TCP 글로벌 매개 변수 ----- 수신 측 크기 조정 상태 : 사용
Chimney 오프로드 상태 : 사용 안 함 NetDMA 상태 : 사용 안 함 DCA(Direct Cache Access) : 사용 안 함 수
신 창 자동 조절 수준 : 보통 추가 기능 정체 제어 제공자 : 없음 ECN 기능 : 사용 안 함 RFC 1323 타임스탬프 :
사용 안 함 초기 RTO : 3000 세그먼트 병합 상태 수신 : 사용 안 함
```

LRO가 Windows 8 이상 또는 Windows Server 2012 시스템에서 전체적으로 비활성화된 경우, 세그먼트 병합 상태 수신 속성이 사용 안 함으로 표시됩니다.

- 2 LRO를 Windows OS에서 전체적으로 사용하려면 명령 프롬프트에서 `netsh int tcp set global` 명령을 실행합니다.

```
netsh int tcp set global rsc=enabled
```

#### 다음에 수행할 작업

Windows 8 이상 또는 Windows Server 2012 가상 시스템의 VMXNET3 어댑터에서 LRO를 사용하도록 설정합니다. [Windows 가상 시스템의 VMXNET3 어댑터에서 LRO 관리](#)의 내용을 참조하십시오.

## NetQueue 및 네트워킹 성능

NetQueue는 시스템에 네트워크 트래픽을 전달할 때 개별적으로 처리될 수 있는 여러 수신 대기열을 사용하는 일부 네트워크 어댑터의 기능을 활용하여 처리 작업을 여러 CPU에 분산함으로써 수신 측의 네트워킹 성능을 개선합니다.

vNIC 및 VMkernel 어댑터 필터를 관리하여 물리적 NIC에서 Rx 대기열을 효과적으로 사용하기 위해 ESXi의 NetQueue 밸런서는 로드 밸런싱 알고리즘을 사용합니다.

다양한 유형의 Rx 대기열을 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 "ESXCLI 참조" 설명서에서 `esxcli network nic queue loadbalancer set` 명령을 참조하십시오.

### 호스트에서 NetQueue 활성화

NetQueue는 기본적으로 사용하도록 설정되어 있습니다. NetQueue가 비활성화된 사용하려면 다시 활성화해야 합니다.

#### 사전 요구 사항

#### 절차

- 1 호스트의 ESXi Shell에서 다음 명령을 사용합니다.

```
esxcli system settings kernel set --setting="netNetqueueEnabled" --value="TRUE"
```

- 2 NetQueue를 사용하도록 NIC 드라이버를 구성하려면 `esxcli module parameters set` 명령을 사용합니다.

이중 포트 Emulex NIC에서 8개의 수신 대기열로 드라이버를 구성하려면 이 ESXCLI 명령을 실행합니다.

```
esxcli system module parameters set -m tg3 -p force_netq=8,8
```

- 3 호스트를 재부팅합니다.

### 호스트에서 NetQueue 비활성

NetQueue는 기본적으로 활성화되어 있습니다.

## 사전 요구 사항

"ESXCLI 시작" 에서 NIC 드라이버 구성에 대한 정보를 숙지하십시오.

## 절차

- 1 ESXCLI에서 호스트 버전에 따라 다음 명령을 사용합니다.

```
esxcli system settings kernel set --setting="netNetqueueEnabled" --value="FALSE"
```

- 2 NIC 드라이버에서 NetQueue를 비활성화하려면 `esxcli module parameters set` 명령을 사용합니다.

하나의 수신 대기열로 드라이버를 구성하려면 이중 포트 Emulex NIC에서 ESXCLI 명령을 실행합니다.

```
esxcli system module parameters set -m tg3 -p force_netq=1,1
```

- 3 호스트를 재부팅합니다.



vSphere Network I/O Control을 사용하여 비즈니스에 중요한 애플리케이션에 네트워크 대역폭을 할당하고 몇 가지 트래픽 유형이 공통 리소스를 얻기 위해 경쟁하는 상황을 해결합니다.

## ■ vSphere Network I/O Control이란?

vSphere Network I/O Control 버전 3에서는 호스트에 있는 물리적 어댑터의 용량을 기반으로 시스템 트래픽에 대한 대역폭을 예약하는 메커니즘을 사용합니다. 이를 통해 CPU 및 메모리 리소스를 할당할 때 사용하는 모델과 유사한 방식으로 VM 네트워크 어댑터 수준에서 리소스를 세부적으로 제어할 수 있습니다.

## ■ vSphere Distributed Switch에서 Network I/O Control 사용

vSphere 기능의 시스템 트래픽 및 가상 시스템 트래픽에 대한 최소 대역폭을 보장하려면 vSphere Distributed Switch에서 네트워크 리소스 관리를 사용하도록 설정합니다.

## ■ 시스템 트래픽에 대한 대역폭 할당

Network I/O Control을 구성하여 vSphere Fault Tolerance, vSphere vMotion 등이 생성하는 트래픽에 특정 양의 대역폭을 할당할 수 있습니다.

## ■ 가상 시스템 트래픽에 대한 대역폭 할당

Network I/O Control 버전 3에서는 개별 가상 시스템에 대한 대역폭 요구 사항을 구성할 수 있습니다. 또한 네트워크 리소스 풀을 사용할 수 있는데, 여기에서 집계된 예약으로부터 가상 시스템 트래픽에 대한 대역폭 할당량을 할당하고 풀의 대역폭을 개별 가상 시스템에 할당할 수 있습니다.

## ■ Network I/O Control 외부로 물리적 어댑터 이동

특정 조건에서 용량이 낮은 물리적 어댑터를 Network I/O Control 버전 3의 대역폭 할당 모델에서 제외해야 할 수 있습니다.

## vSphere Network I/O Control이란?

vSphere Network I/O Control 버전 3에서는 호스트에 있는 물리적 어댑터의 용량을 기반으로 시스템 트래픽에 대한 대역폭을 예약하는 메커니즘을 사용합니다. 이를 통해 CPU 및 메모리 리소스를 할당할 때 사용하는 모델과 유사한 방식으로 VM 네트워크 어댑터 수준에서 리소스를 세부적으로 제어할 수 있습니다.

Network I/O Control 버전 3은 향상된 네트워크 리소스 예약과 전체 스위치에 걸친 할당을 제공합니다.

## 대역폭 리소스 예약을 위한 모델

Network I/O Control 버전 3은 인프라 서비스(예: vSphere Fault Tolerance)와 관련된 시스템 트래픽과 가상 시스템의 리소스 관리를 위한 별도의 모델을 지원합니다.

두 가지 트래픽 범주가 서로 다른 성격을 가지고 있습니다. 시스템 트래픽은 ESXi 호스트와 전적으로 연관되어 있습니다. 네트워크 트래픽 라우트는 환경에서 가상 시스템을 마이그레이션하면 변경됩니다. 해당 호스트와 관계없이 가상 시스템에 네트워크 리소스를 제공하려면 Network I/O Control에서 전체 Distributed Switch의 범위에서 유효한 가상 시스템에 대해 리소스 할당을 구성하면 됩니다.

## 가상 시스템에 대역폭 보장

Network I/O Control 버전 3은 공유, 예약 및 제한의 구성체를 사용하여 가상 시스템의 네트워크 어댑터에 대역폭을 프로비저닝합니다. 이러한 구성체를 기반으로 충분한 대역폭을 수신하기 위해 가상 워크로드는 vSphere Distributed Switch, vSphere DRS 및 vSphere HA의 승인 제어를 사용할 수 있습니다. [가상 시스템 대역폭에 대한 승인 제어](#)의 내용을 참조하십시오.

## 기능 사용 가능 여부

SR-IOV는 Network I/O Control 버전 3을 사용하도록 구성된 가상 시스템에서는 사용할 수 없습니다.

## vSphere Distributed Switch에서 Network I/O Control 사용

vSphere 기능의 시스템 트래픽 및 가상 시스템 트래픽에 대한 최소 대역폭을 보장하려면 vSphere Distributed Switch에서 네트워크 리소스 관리를 사용하도록 설정합니다.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **작업** 메뉴에서 **설정 > 설정 편집**을 선택합니다.
- 3 **Network I/O Control** 드롭다운 메뉴에서 **사용**을 선택합니다.

---

**참고** 네트워크 오프로드 호환성을 사용하도록 설정하면 **Network I/O Control**이 사용되지 않도록 설정됩니다. **네트워크 오프로드**가 **없음**으로 설정되면 **Network I/O Control**이 지원됩니다.

---

- 4 **확인**을 클릭합니다.

### 결과

사용하도록 설정하는 경우 시스템 트래픽과 가상 시스템 트래픽에 대한 대역폭 할당을 처리하기 위해 Network I/O Control에서 사용하는 모델은 Distributed Switch에서 활성인 Network I/O Control 버전을 기반으로 합니다. [vSphere Network I/O Control이란?](#)의 내용을 참조하십시오.

## 시스템 트래픽에 대한 대역폭 할당

Network I/O Control을 구성하여 vSphere Fault Tolerance, vSphere vMotion 등이 생성하는 트래픽에 특정 양의 대역폭을 할당할 수 있습니다.

분산 스위치에서 Network I/O Control을 사용하여 기본 vSphere 기능과 관련된 트래픽에 대한 대역폭 할당을 구성할 수 있습니다.

- 관리
- Fault Tolerance
- NFS
- vSAN
- vMotion
- vSphere Replication
- vSphere Data Protection 백업
- 가상 시스템
- NVMe over TCP

vCenter Server는 스위치에 연결된 호스트의 각 물리적 어댑터로 Distributed Switch의 할당을 전파합니다.

### 다음으로 읽을 항목

- [시스템 트래픽에 대한 대역폭 할당 매개 변수](#)  
Network I/O Control은 몇 가지 구성 매개 변수를 사용하여 기본 vSphere 시스템 기능의 트래픽에 대역폭을 할당합니다.
- [시스템 트래픽에 대한 대역폭 예약 예제](#)  
물리적 어댑터의 용량은 보장하는 대역폭을 결정합니다. 이 용량에 따라 시스템 기능의 최적의 작동을 위한 최소한의 대역폭을 보장할 수 있습니다.
- [시스템 트래픽에 대한 대역폭을 할당하는 방법](#)  
vSphere Distributed Switch에 연결된 물리적 어댑터에서 호스트 관리, 가상 시스템, NFS 스토리지, vSphere vMotion, vSphere Fault Tolerance, vSAN 및 vSphere Replication에 대한 대역폭을 할당합니다.

## 시스템 트래픽에 대한 대역폭 할당 매개 변수

Network I/O Control은 몇 가지 구성 매개 변수를 사용하여 기본 vSphere 시스템 기능의 트래픽에 대역폭을 할당합니다.

표 11-1. 시스템 트래픽에 대한 할당 매개 변수

대역폭 할당 매개 변수	설명
공유	공유(1~100)는 동일한 물리적 어댑터에서 활성인 다른 시스템 트래픽 유형에 대한 특정 시스템 트래픽 유형의 상대적 우선 순위를 반영합니다. 시스템 트래픽 유형에 사용할 수 있는 대역폭의 양은 해당 상대적 공유 및 다른 시스템 기능이 전송하는 데이터의 양으로 결정됩니다.
예약	단일 물리적 어댑터에서 보장되어야 하는 최소 대역폭(Mbps). 모든 시스템 트래픽 유형 간에 예약된 총 대역폭은 최저 용량을 가진 물리적 네트워크 어댑터가 제공할 수 있는 대역폭의 75%를 초과할 수 없습니다. 사용되지 않은 예약된 대역폭은 다른 유형의 시스템 트래픽에서 사용할 수 있게 됩니다. 하지만 Network I/O Control은 시스템 트래픽이 사용하지 않는 용량을 가상 시스템 배치로 재배포하지 않습니다.
제한	단일 물리적 어댑터에서 시스템 트래픽 유형이 소모할 수 있는 최대 대역폭(Mbps 또는 Gbps).

## 시스템 트래픽에 대한 대역폭 예약 예제

물리적 어댑터의 용량은 보장하는 대역폭을 결정합니다. 이 용량에 따라 시스템 기능의 최적의 작동을 위한 최소한의 대역폭을 보장할 수 있습니다.

예를 들어 10GbE 네트워크 어댑터가 포함된 ESXi 호스트에 연결된 Distributed Switch에서 vCenter Server를 통한 관리를 위한 1Gbps, vSphere Fault Tolerance를 위한 1Gbps, vSphere vMotion 트래픽을 위한 1Gbps 및 가상 시스템 트래픽을 위한 0.5Gbps를 보장하기 위한 예약을 구성할 수 있습니다. Network I/O Control은 각 물리적 네트워크 어댑터에 요청된 대역폭을 할당합니다. 물리적 네트워크 어댑터 대역폭의 75% 이하(7.5Gbps 이하)를 예약할 수 있습니다.

호스트에서 공유, 제한 및 사용에 따라 대역폭을 동적으로 할당하도록 하거나 시스템 기능의 작동을 위한 충분한 대역폭만 예약하도록 더 많은 용량을 예약되지 않은 상태로 둘 수 있습니다.

## 시스템 트래픽에 대한 대역폭을 할당하는 방법

vSphere Distributed Switch에 연결된 물리적 어댑터에서 호스트 관리, 가상 시스템, NFS 스토리지, vSphere vMotion, vSphere Fault Tolerance, vSAN 및 vSphere Replication에 대한 대역폭을 할당합니다.

Network I/O Control을 사용하여 가상 시스템에 대한 대역폭 할당을 사용하려면 가상 시스템 시스템 트래픽을 구성합니다. 승인 제어에서는 가상 시스템 트래픽에 대한 대역폭 예약도 사용됩니다. 가상 시스템의 전원을 켜면 승인 제어에서 충분한 대역폭을 사용할 수 있는지 확인합니다.

### 사전 요구 사항

- vSphere Distributed Switch의 버전이 6.5.0 이상인지 확인합니다.
- 스위치의 Network I/O Control의 버전이 3인지 확인합니다.

- Network I/O Control이 사용되도록 설정되어 있는지 확인합니다. vSphere Distributed Switch에서 Network I/O Control [사용](#)의 내용을 참조하십시오.

#### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **구성** 탭에서 **리소스 할당**을 확장합니다.
- 3 **시스템 트래픽**을 클릭합니다.  
시스템 트래픽 유형에 대한 대역폭 할당이 표시됩니다.
- 4 프로비저닝하려는 vSphere 기능에 따라 트래픽 유형을 선택하고 **편집**을 클릭합니다.  
트래픽 유형에 대한 네트워크 리소스 설정이 나타납니다.
- 5 **공유** 드롭다운 메뉴에서 물리적 어댑터를 통과하는 전체적인 흐름에서 트래픽의 공유를 편집합니다.  
Network I/O Control은 물리적 어댑터가 포화 상태가 되면 구성된 공유를 적용합니다.  
미리 정의된 값을 설정하기 위한 옵션을 선택하거나, **사용자 지정**을 선택하고 1에서 100 사이의 숫자를 입력하여 다른 공유를 설정합니다.
- 6 **예약** 텍스트 상자에서 트래픽 유형에 대해 반드시 사용할 수 있어야 하는 최소 대역폭 값을 입력합니다.  
시스템 트래픽의 총 예약은 Distributed Switch에 연결된 모든 어댑터 중 최저 용량을 가진 물리적 어댑터가 지원하는 대역폭의 75%를 초과해서는 안 됩니다.
- 7 **제한** 텍스트 상자에서 선택된 유형의 시스템 트래픽이 사용할 수 있는 최대 대역폭을 설정합니다.
- 8 **확인**을 클릭하여 할당 설정을 적용합니다.

#### 결과

vCenter Server는 스위치에 연결된 호스트 물리적 어댑터로 Distributed Switch의 할당을 전파합니다.

## 가상 시스템 트래픽에 대한 대역폭 할당

Network I/O Control 버전 3에서는 개별 가상 시스템에 대한 대역폭 요구 사항을 구성할 수 있습니다. 또한 네트워크 리소스 풀을 사용할 수 있는데, 여기에서 집계된 예약으로부터 가상 시스템 트래픽에 대한 대역폭 할당량을 할당하고 풀의 대역폭을 개별 가상 시스템에 할당할 수 있습니다.

### 가상 시스템에 대역폭을 할당하는 방법

Network I/O Control은 네트워크 리소스 풀에 기반한 전체 vSphere Distributed Switch에 대한 할당 및 가상 시스템의 트래픽을 전달하는 물리적 어댑터에 대한 할당이라는 두 가지 모델을 사용하여 가상 시스템에 대한 대역폭을 할당합니다.

#### 네트워크 리소스 풀

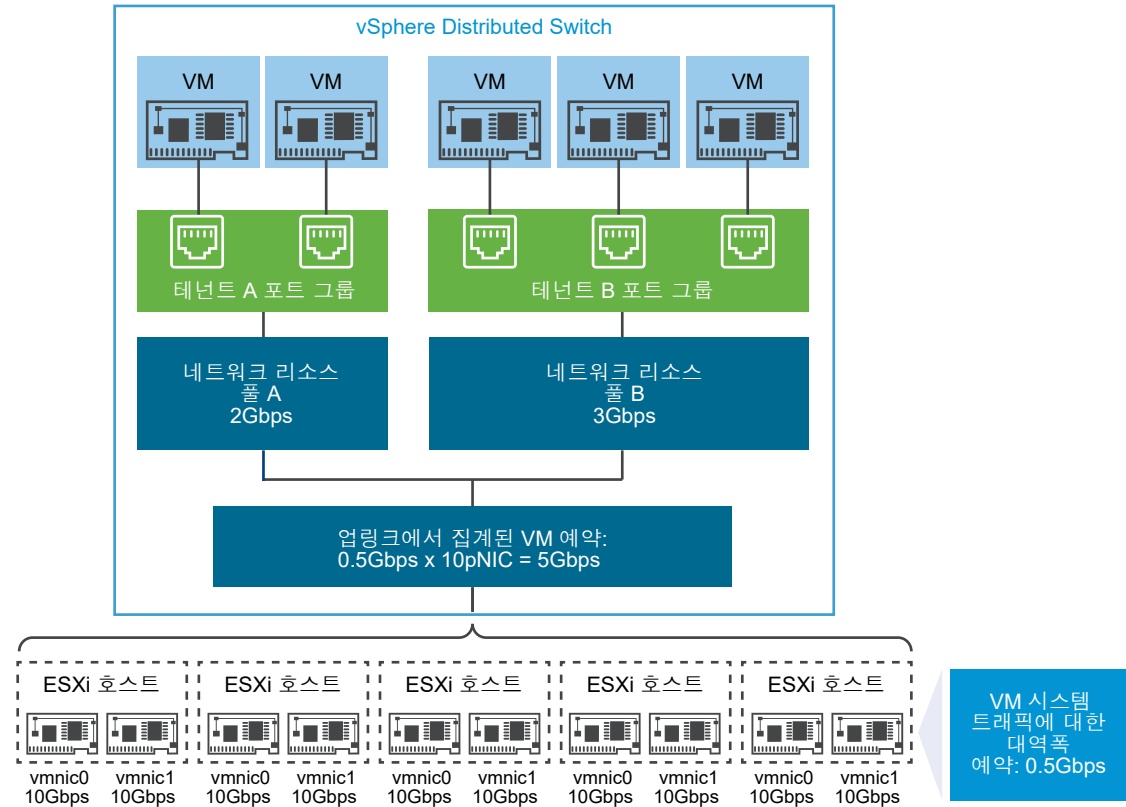
네트워크 리소스 풀은 Distributed Switch에 연결된 모든 물리적 어댑터의 가상 시스템 시스템 트래픽에 예약되어 있는 집계된 대역폭의 일부를 나타냅니다.

예를 들어, 가상 시스템 시스템 트래픽이 10개의 업링크를 가진 Distributed Switch에서 10GbE 업링크 각각에 대해 0.5Gbps를 예약한 경우 이 스위치의 VM 예약에 사용할 수 있는 집계된 총 대역폭은 5Gbps가 됩니다. 각 네트워크 리소스 풀은 이 5Gbps 용량의 할당량을 예약할 수 있습니다.

네트워크 리소스 풀에만 사용되는 대역폭 할당량은 풀에 연결된 분산 포트 그룹 간에 공유됩니다. 가상 시스템은 VM이 연결되어 있는 분산 포트 그룹을 통해 풀의 대역폭을 수신합니다.

기본적으로, 스위치의 분산 포트 그룹은 할당량이 구성되지 않은 네트워크 리소스 풀(기본값)에 할당됩니다.

그림 11-1. vSphere Distributed Switch의 업링크 전반에 걸쳐 네트워크 리소스 풀의 대역폭 집계



### 가상 시스템의 대역폭 요구 사항 정의

개별 가상 시스템에 대한 대역폭 할당은 CPU 및 메모리 리소스 할당과 유사한 방식으로 수행합니다. Network I/O Control 버전 3에서는 VM 하드웨어 설정에서 네트워크 어댑터에 대해 정의된 공유, 예약 및 제한에 따라 가상 시스템에 대역폭을 프로비저닝합니다. 예약이란 가상 시스템의 트래픽이 최소한 지정 대역폭을 소모할 수 있음을 보장하는 것입니다. 물리적 어댑터에 더 많은 용량이 있다면 가상 시스템이 지정된 공유 및 제한에 따라 추가적인 대역폭을 사용할 수 있습니다.

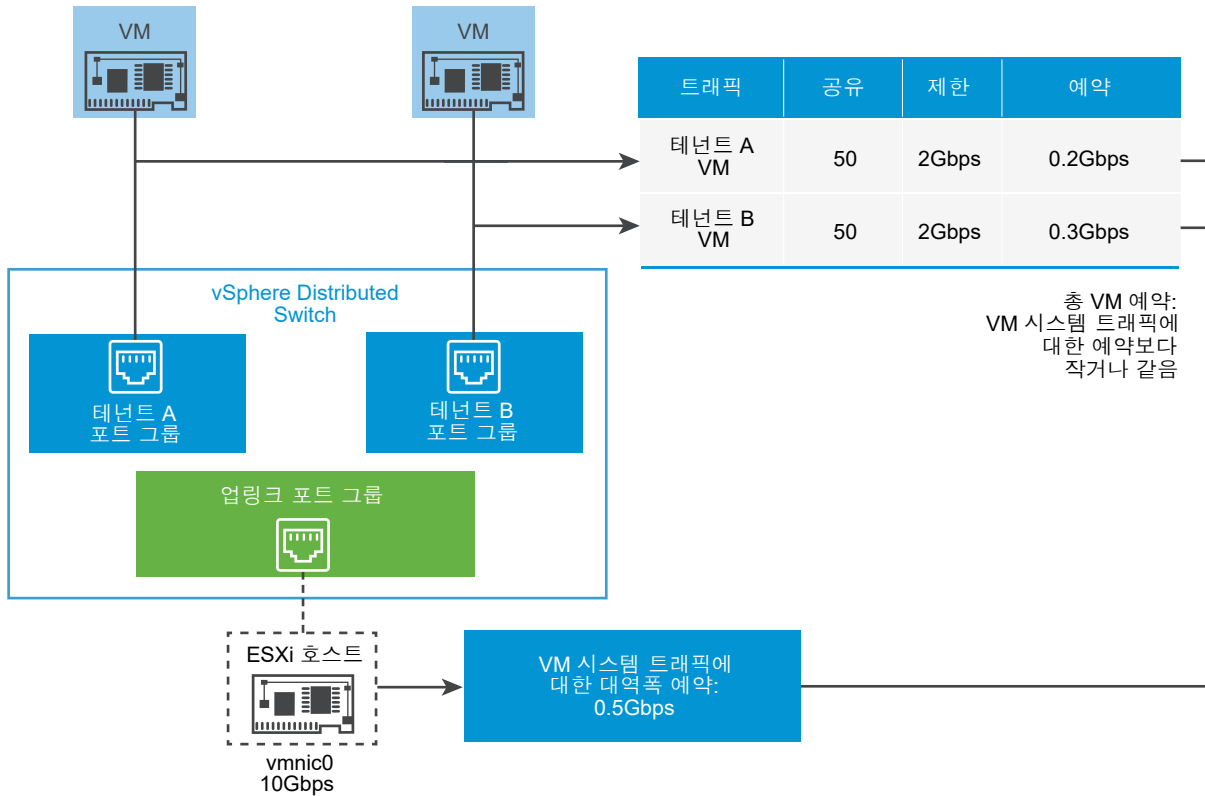
### 호스트의 가상 시스템에 대역폭 프로비저닝

Network I/O Control은 대역폭을 보장할 수 있도록 가상 시스템에 대역폭 예약을 구성했을 때 활성화되는 트래픽 배치 엔진을 구현합니다. Distributed Switch는 필요한 대역폭을 제공할 수 있고 활성 팀 구성 정책 범위 내에 있는 물리적 어댑터에 VM 네트워크 어댑터의 트래픽을 배치하려고 시도합니다.

호스트에 있는 가상 시스템의 총 대역폭 예약은 가상 시스템 시스템 트래픽에 대해 구성되어 있는 예약된 대역폭을 초과할 수 없습니다.

실제 제한 및 예약도 어댑터가 연결되어 있는 분산 포트 그룹의 트래픽 조절 정책에 따라 달라집니다. 예를 들어 VM 네트워크 어댑터에 200Mbps의 제한이 필요하고 트래픽 조절 정책에 구성된 평균 대역폭이 100Mbps라면 효과적인 제한은 100Mbps가 됩니다.

그림 11-2. 개별 가상 시스템에 대한 대역폭 할당 구성



Network I/O Control의 VM에 대한 대역폭 예약은 VM에서 트래픽을 보내는 물리적 어댑터의 VM 시스템 트래픽의 예약에 대해 보장됩니다.

### 가상 시스템 트래픽에 대한 대역폭 할당 매개 변수

Network I/O Control 버전 3은 VM 하드웨어 설정의 네트워크 어댑터에 대해 구성된 공유, 예약 및 제한을 기반으로 개별 가상 시스템에 대역폭을 할당합니다.

표 11-2. VM 네트워크 어댑터에 대한 대역폭 할당 매개 변수

대역폭 할당 매개 변수	설명
공유	네트워크에 VM 트래픽을 전송하는 물리적 어댑터의 용량에 대해 이 VM 네트워크 어댑터를 통과하는 트래픽의 상대적 우선 순위 (1-100).
예약	VM 네트워크 어댑터가 물리적 어댑터에서 반드시 수신해야 하는 최소 대역폭(Mbps).
제한	동일한 또는 다른 호스트에 있는 다른 가상 시스템의 트래픽에 대한 VM 네트워크 어댑터의 최대 대역폭.

## 가상 시스템 대역폭에 대한 승인 제어

vSphere는 가상 시스템에서 충분한 대역폭을 사용할 수 있도록 대역폭 예약과 팀 구성 정책을 기반으로 호스트 및 클러스터 수준에서 승인 제어를 구현합니다.

### vSphere Distributed Switch의 대역폭 승인 제어

가상 시스템의 전원을 켜올 때 Distributed Switch의 Network I/O Control 기능은 이러한 조건이 호스트에서 충족되는지 확인합니다.

- 호스트의 물리적 어댑터는 팀 구성 정책과 예약에 따라 최소의 대역폭을 VM 네트워크 어댑터에 제공할 수 있습니다.
- VM 네트워크 어댑터에 대한 예약은 네트워크 리소스 풀에서 사용 가능한 할당량보다 작습니다.

실행 중인 가상 시스템의 네트워크 어댑터에 대한 예약을 변경하면 연결된 네트워크 리소스 풀이 새로운 예약을 수용할 수 있는지 여부를 Network I/O Control이 다시 확인합니다. 풀에 미할당량이 충분치 않은 경우 변경 내용은 적용되지 않습니다.

vSphere Distributed Switch에서 승인 제어를 사용하려면 다음 작업을 수행하십시오.

- Distributed Switch의 가상 시스템 시스템 트래픽에 대한 대역폭 할당을 구성합니다.
- 가상 시스템 시스템 트래픽에 대해 구성된 대역폭의 예약 할당량으로 네트워크 리소스 풀을 구성합니다.
- 가상 시스템을 스위치에 연결하는 분산 포트 그룹에 네트워크 리소스 풀을 연결합니다.
- 포트 그룹에 연결된 가상 시스템의 대역폭 요구 사항을 구성합니다.

### vSphere DRS의 대역폭 승인 제어

클러스터에 있는 가상 시스템의 전원을 켜면 vSphere DRS가 용량이 있는 호스트에 가상 시스템을 배치하고 활성 팀 구성 정책에 따라 가상 시스템에 예약된 대역폭을 보장합니다.

다음과 같은 상황에서 vSphere DRS는 가상 시스템의 대역폭 예약을 충족시키기 위해 가상 시스템을 다른 호스트로 마이그레이션합니다.

- 초기 호스트가 더 이상 충족할 수 없는 값으로 예약이 변경된 경우.
- 가상 시스템의 트래픽을 전송하는 물리적 어댑터가 오프라인인 경우.



vSphere DRS에서 승인 제어를 사용하려면 다음 작업을 수행하십시오.

- Distributed Switch의 가상 시스템 시스템 트래픽에 대한 대역폭 할당을 구성합니다.
- Distributed Switch에 연결된 가상 시스템의 대역폭 요구 사항을 구성합니다.

가상 시스템의 대역폭 요구에 따른 리소스 관리에 대한 자세한 내용은 "vSphere 리소스 관리" 문서를 참조하십시오.

## vSphere HA의 대역폭 승인 제어

호스트가 실패하거나 분리되는 경우 vSphere HA는 대역폭 예약과 팀 구성 정책에 따라 클러스터에 있는 다른 호스트의 가상 시스템 전원을 켭니다.

vSphere HA에서 승인 제어를 사용하려면 다음 작업을 수행하십시오.

- 가상 시스템 시스템 트래픽에 대한 대역폭을 할당합니다.
- Distributed Switch에 연결된 가상 시스템의 대역폭 요구 사항을 구성합니다.

vSphere HA에서 가상 시스템의 대역폭 요구를 기반으로 페일오버를 제공하는 방법에 대한 자세한 내용은 "vSphere 가용성" 문서를 참조하십시오.

## 네트워크 리소스 풀 생성

vSphere Distributed Switch에서 네트워크 리소스 풀을 생성하여 가상 시스템 집합에 대한 대역폭을 예약합니다.

네트워크 리소스 풀은 가상 시스템에 예약 할당량을 제공합니다. 할당량은 Distributed Switch에 연결된 물리적 어댑터의 가상 시스템 시스템 트래픽에 대해 예약된 대역폭의 일부를 나타냅니다. 풀과 연결된 가상 시스템에 대한 할당량과 별도로 대역폭을 설정할 수 있습니다. 풀과 연결된 전원이 켜진 VM의 네트워크 어댑터의 예약은 풀의 할당량을 초과하면 안 됩니다. [가상 시스템에 대역폭을 할당하는 방법](#)을 참조하십시오.

### 사전 요구 사항

- vSphere Distributed Switch의 버전이 6.5.0 이상인지 확인합니다.
- 스위치의 Network I/O Control의 버전이 3인지 확인합니다.
- Network I/O Control이 사용되도록 설정되어 있는지 확인합니다. [vSphere Distributed Switch에서 Network I/O Control 사용](#)의 내용을 참조하십시오.
- 가상 시스템의 시스템 트래픽에 구성된 대역폭 예약이 있는지 확인합니다. [시스템 트래픽에 대한 대역폭을 할당하는 방법](#)의 내용을 참조하십시오.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **구성** 탭에서 **리소스 할당**을 확장합니다.
- 3 **네트워크 리소스 풀**을 클릭합니다.
- 4 **추가** 아이콘을 클릭합니다.

- 5 (선택 사항) 네트워크 리소스 풀의 이름과 설명을 입력합니다.
- 6 가상 시스템 시스템 트래픽에 대해 예약된 사용 가능 대역폭에서 **예약 할당량**의 값(Mbps)을 입력합니다.  
풀에 할당할 수 있는 최대 할당량은 다음 공식에 따라 결정됩니다.

```
max reservation quota = aggregated reservation for vm system traffic - quotas of the other resource pools
```

#### 위치

- aggregated reservation for vm system traffic = 각 pNIC의 가상 시스템 시스템 트래픽에 대해 구성된 대역폭 예약 \* Distributed Switch에 연결된 pNIC 수
- quotas of the other pools = 다른 네트워크 리소스 풀의 예약 할당량 합계

- 7 **확인**을 클릭합니다.

#### 다음에 수행할 작업

풀의 할당량에서 개별 가상 시스템에 대역폭을 할당할 수 있도록 하나 이상의 분산 포트 그룹을 네트워크 리소스 풀에 추가합니다. [네트워크 리소스 풀에 분산 포트 그룹 추가](#)를 참조하십시오.

## 네트워크 리소스 풀에 분산 포트 그룹 추가

포트 그룹에 연결된 가상 시스템에 대역폭을 할당할 수 있도록 분산 포트 그룹을 네트워크 리소스 풀에 추가합니다.

네트워크 리소스 풀을 동시에 여러 개의 분산 포트 그룹에 할당하려면 **분산 포트 그룹 관리** 마법사에서 리소스 할당 정책을 사용하면 됩니다. [vSphere Distributed Switch에서 여러 포트 그룹에 대한 정책 관리](#)의 내용을 참조하십시오.

Network I/O Control은 Distributed Switch에서 활성화된 Network I/O Control 버전에 구현된 모델에 따라 분산 포트 그룹에 연결된 가상 시스템에 대역폭을 할당합니다. [vSphere Network I/O Control이란?](#)의 내용을 참조하십시오.

#### 사전 요구 사항

- Network I/O Control이 사용되도록 설정되어 있는지 확인합니다. [vSphere Distributed Switch에서 Network I/O Control 사용](#)의 내용을 참조하십시오.

#### 절차

- 1 vSphere Client에서 분산 포트 그룹을 찾습니다.
  - a Distributed Switch를 선택하고 **네트워크** 탭을 클릭합니다.
  - b **분산 포트 그룹**을 클릭합니다.
- 2 분산 포트 그룹을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 3 설정 편집 대화상자에서 **일반**을 클릭합니다.

#### 4 네트워크 리소스 풀 드롭다운 메뉴에서 네트워크 리소스 풀을 선택하고 **확인**을 클릭합니다.

Distributed Switch에 네트워크 리소스 풀이 포함되어 있지 않으면 드롭다운 메뉴에는 **(기본값)** 옵션만 표시됩니다.

## 가상 시스템에 대한 대역폭 할당 구성

분산 포트 그룹에 연결된 개별 가상 시스템에 대역폭 할당을 구성할 수 있습니다. 대역폭에 대한 공유, 예약 및 제한 설정을 사용할 수 있습니다.

### 사전 요구 사항

- vSphere Distributed Switch의 버전이 6.5.0 이상인지 확인합니다.
- 스위치의 Network I/O Control의 버전이 3인지 확인합니다.
- Network I/O Control이 사용되도록 설정되어 있는지 확인합니다. [vSphere Distributed Switch에서 Network I/O Control 사용](#)의 내용을 참조하십시오.
- 가상 시스템의 시스템 트래픽에 구성된 대역폭 예약이 있는지 확인합니다. [시스템 트래픽에 대한 대역폭을 할당하는 방법](#)의 내용을 참조하십시오.

### 절차

- 1 vSphere Client에서 가상 시스템을 찾습니다.
  - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택하고 **VM** 탭을 클릭합니다.
  - b **가상 시스템**을 클릭하고 목록에서 가상 시스템을 클릭합니다.
- 2 [작업] 메뉴에서 [설정 편집]을 선택합니다.
- 3 VM 네트워크 어댑터의 네트워크 어댑터 섹션을 확장합니다.
- 4 새 VM 네트워크 어댑터에 대한 대역폭 할당을 구성하려면 **새디바이스 추가** 드롭다운 메뉴에서 **네트워크 어댑터**버튼을 클릭합니다.

새 네트워크 섹션에서 대역폭 할당 옵션 및 기타 네트워크 어댑터 설정이 표시됩니다.

- 5 VM 네트워크 어댑터가 분산 포트 그룹에 연결되어 있지 않은 경우 네트워크 어댑터 또는 새 네트워크 레이블 옆의 드롭다운 메뉴에서 포트 그룹을 선택합니다.
- 6 **공유** 드롭다운 메뉴에서 이 가상 시스템의 트래픽의 상대적인 우선 순위를 연결된 물리적 어댑터의 용량의 공유로 설정합니다.

Network I/O Control은 물리적 어댑터가 포화 상태가 되면 구성된 공유를 적용합니다.

미리 정의된 값을 설정하기 위한 옵션을 선택하거나, **사용자 지정**을 선택하고 1에서 100 사이의 숫자를 입력하여 다른 공유를 설정합니다.

- 7 **예약** 텍스트 상자에서 가상 시스템의 전원이 켜졌을 때 VM 네트워크 어댑터에 대해 사용할 수 있어야 하는 최소 대역폭을 예약합니다.

네트워크 리소스 풀을 사용하여 대역폭을 프로비저닝하는 경우 풀과 연결된 전원이 켜진 VM의 네트워크 어댑터의 예약이 풀의 할당량을 초과해서는 안 됩니다.

vSphere DRS가 사용되도록 설정된 경우 가상 시스템의 전원을 켜려면 호스트의 모든 VM 네트워크 어댑터의 예약이 호스트 물리적 어댑터의 가상 시스템 시스템 트래픽에 대해 예약된 대역폭을 초과하지 않아야 합니다.

- 8 **제한** 텍스트 상자에서 VM 네트워크 어댑터가 사용할 수 있는 대역폭에 대한 제한을 설정합니다.
- 9 **확인**을 클릭합니다.

## 결과

### 네트워크

I/O Control은 네트워크 리소스 풀의 예약 할당량 중에서 가상 시스템의 네트워크 어댑터에 대해 예약한 대역폭을 할당합니다.

## 여러 가상 시스템에서 대역폭 할당 구성

예를 들어 Network I/O Control을 버전 3으로 업그레이드한 후에 한 번의 작업으로 특정 네트워크 리소스 풀에 연결된 여러 가상 시스템에서 대역폭 할당을 구성합니다.

### 사전 요구 사항

- vSphere Distributed Switch의 버전이 6.5.0 이상인지 확인합니다.
- 스위치의 Network I/O Control의 버전이 3인지 확인합니다.
- Network I/O Control이 사용되도록 설정되어 있는지 확인합니다. [vSphere Distributed Switch에서 Network I/O Control 사용](#)의 내용을 참조하십시오.
- 가상 시스템의 시스템 트래픽에 구성된 대역폭 예약이 있는지 확인합니다. [시스템 트래픽에 대한 대역폭을 할당하는 방법](#)의 내용을 참조하십시오.
- 가상 시스템이 연결된 분산 포트 그룹을 통해 특정 네트워크 리소스 풀과 연결되어 있는지 확인합니다. [네트워크 리소스 풀에 분산 포트 그룹 추가](#)를 참조하십시오.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **구성** 탭에서 **리소스 할당**을 확장합니다.
- 3 **네트워크 리소스 풀**을 클릭합니다.
- 4 네트워크 리소스 풀을 선택합니다.
- 5 **가상 시스템**을 클릭합니다.

선택한 네트워크 리소스 풀에 연결된 VM 네트워크 어댑터의 목록이 나타납니다.

- 6 설정을 구성하려는 VM 네트워크 어댑터를 선택하고 **편집**을 클릭합니다.
- 7 **공유** 드롭다운 메뉴에서, 트래픽을 전송하는 물리적 어댑터의 범위에서 이러한 가상 시스템의 트래픽에 대한 상대적인 우선 순위를 설정합니다.  
Network I/O Control은 물리적 어댑터가 포화 상태가 되면 구성된 공유를 적용합니다.
- 8 **예약** 텍스트 상자에서 가상 시스템의 전원이 켜졌을 때 각 VM 네트워크 어댑터에서 사용할 수 있어야 하는 최소 대역폭을 예약합니다.  
네트워크 리소스 풀을 사용하여 대역폭을 프로비저닝하는 경우 풀과 연결된 전원이 켜진 VM의 네트워크 어댑터의 예약이 풀의 할당량을 초과해서는 안 됩니다.
- 9 **제한** 텍스트 상자에서 각 VM 네트워크 어댑터가 사용할 수 있는 대역폭에 대한 제한을 설정합니다.
- 10 **확인**을 클릭합니다.

## 네트워크 리소스 풀의 할당량 수정

분산 포트 그룹 집합에 연결된 가상 시스템에 대해 예약할 수 있는 대역폭 할당량을 수정하는 방법을 알아봅니다.

### 사전 요구 사항

- vSphere Distributed Switch의 버전이 6.5.0 이상인지 확인합니다.
- 스위치의 Network I/O Control의 버전이 3인지 확인합니다.
- Network I/O Control이 사용되도록 설정되어 있는지 확인합니다. [vSphere Distributed Switch에서 Network I/O Control 사용](#)의 내용을 참조하십시오.
- 가상 시스템의 시스템 트래픽에 구성된 대역폭 예약이 있는지 확인합니다. [시스템 트래픽에 대한 대역폭을 할당하는 방법](#)의 내용을 참조하십시오.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **구성** 탭에서 **리소스 할당**을 확장합니다.
- 3 **네트워크 리소스 풀**을 클릭합니다.
- 4 목록에서 네트워크 리소스 풀을 선택하고 **편집**을 클릭합니다.
- 5 **예약 할당량** 텍스트 상자에서, 스위치에 있는 모든 물리적 어댑터의 가상 시스템 시스템 트래픽에 대해 예약된 여유 대역폭의 집계에서 가상 시스템에 대한 대역폭 할당량을 입력합니다.
- 6 **확인**을 클릭합니다.

## 네트워크 리소스 풀에서 분산 포트 그룹 제거

네트워크 리소스 풀의 예약 할당량에서 가상 시스템에 대한 대역폭 할당을 중지하려면 가상 시스템이 연결되어 있는 포트 그룹과 풀 간의 연결을 제거합니다.

**절차**

- 1 vSphere Client에서 분산 포트 그룹을 찾습니다.
  - a Distributed Switch를 선택하고 **네트워크** 탭을 클릭합니다.
  - b **분산 포트 그룹**을 클릭합니다.
- 2 분산 포트 그룹을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 3 포트 그룹에 대한 설정 편집 대화상자에서 **일반**을 클릭합니다.
- 4 **네트워크 리소스 풀** 드롭다운 메뉴에서 (**기본값**)을 선택하고 **확인**을 클릭합니다.

**결과**

분산 포트 그룹이 기본 VM 네트워크 리소스 풀과 연결됩니다.

**네트워크 리소스 풀 삭제**

더 이상 사용하지 않는 네트워크 리소스 풀을 삭제합니다.

**사전 요구 사항**

연결된 모든 분산 포트 그룹에서 네트워크 리소스 풀을 분리합니다. **네트워크 리소스 풀에서 분산 포트 그룹 제거**의 내용을 참조하십시오.

**절차**

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **구성** 탭에서 **리소스 할당**을 확장합니다.
- 3 **네트워크 리소스 풀**을 클릭합니다.
- 4 네트워크 리소스 풀을 선택하고 **제거**를 클릭합니다.
- 5 **확인**을 클릭하여 리소스 풀을 삭제합니다.

**Network I/O Control 외부로 물리적 어댑터 이동**

특정 조건에서 용량이 낮은 물리적 어댑터를 Network I/O Control 버전 3의 대역폭 할당 모델에서 제외해야 할 수 있습니다.

예를 들어, vSphere Distributed Switch의 대역폭 할당이 10 GbE NIC에서 조정된 경우 10 GbE NIC에서 구성된 더 높은 할당 요구 사항을 충족하지 못하므로 스위치에 1GbE NIC를 추가하지 못할 수 있습니다.

**사전 요구 사항**

- 호스트가 ESXi 6.5 이상을 실행 중인지 확인합니다.
- vSphere Distributed Switch의 버전이 6.5.0 이상인지 확인합니다.
- 스위치의 Network I/O Control의 버전이 3인지 확인합니다.

## 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 시스템을 확장하고 고급 시스템 설정을 선택합니다.
- 3 Network I/O Control 범위 밖에서 작동하려는 물리적 어댑터를 Net.IOControlPnicOptOut 매개 변수에 대해 심표로 구분된 목록으로 설정합니다.

예: `vmnic0,vmnic3`

- 4 확인을 클릭하여 변경 사항을 적용합니다.

MAC 주소는 네트워크 프로토콜 스택의 계층 2(데이터 링크 계층)에서 수신자에게 프레임 전송하는 데 사용됩니다. vSphere에서 vCenter Server가 가상 시스템 어댑터 및 VMkernel 어댑터에 대한 MAC 주소를 생성하거나, 사용자가 수동으로 주소를 할당할 수 있습니다.

각 네트워크 어댑터 제조업체에는 고유한 MAC 주소를 생성하는 데 사용할 수 있도록 OUI(Organizationally Unique Identifier)라고 하는 고유한 3바이트 접두사가 할당됩니다.

VMware에서는 여러 주소 할당 메커니즘이 지원되며, 메커니즘마다 별도의 OUI가 있습니다.

- 생성된 MAC 주소
  - vCenter Server에서 할당됨
  - ESXi 호스트에 의해 할당됨
- 수동 설정된 MAC 주소
- 레거시 가상 시스템용으로 생성되었지만 ESXi에는 더 이상 사용되지 않는 MAC 주소

자동 MAC 주소 할당 유형을 변경하거나 정적 MAC 주소를 설정하는 등 전원이 꺼진 가상 시스템의 네트워크 어댑터를 재구성하는 경우 vCenter Server는 MAC 주소 충돌 문제를 해결한 다음 어댑터를 재구성합니다.

다음으로 아래 항목을 읽으십시오.

- [vCenter Server에서 MAC 주소 지정](#)
- [ESXi 호스트에서 MAC 주소 생성](#)
- [가상 시스템에 대해 정적 MAC 주소를 설정하는 방법](#)

## vCenter Server에서 MAC 주소 지정

vSphere에서는 vCenter Server의 MAC 주소를 자동 할당하기 위한 여러 가지 체계를 제공합니다. MAC 주소 중복에 대한 요구 사항, 로컬 또는 전역에서 관리되는 주소에 대한 OUI 요구 사항 등에 가장 적합한 체계를 선택할 수 있습니다.

vCenter Server에서 사용할 수 있는 MAC 주소 생성 체계는 다음과 같습니다.

- VMware OUI 할당 - 기본 할당
- 접두사 기반 할당



## ■ 범위 기반 할당

생성된 MAC 주소는 가상 시스템의 MAC 주소가 등록된 다른 가상 시스템의 MAC 주소와 충돌하는 경우 이외에는 변경되지 않습니다. MAC 주소는 가상 시스템의 구성 파일에 저장됩니다.

---

**참고** 잘못된 접두사 또는 범위 기반 할당 값을 사용하면 `vpxd.log` 파일에 오류가 기록됩니다. vCenter Server는 가상 시스템을 프로비저닝할 때 MAC 주소를 할당하지 않습니다.

---

## MAC 주소 충돌 방지

전원이 꺼진 가상 시스템의 MAC 주소는 실행 중이거나 일시 중단된 가상 시스템의 MAC 주소를 기준으로 확인되지 않습니다.

가상 시스템의 전원을 다시 켤 때 다른 MAC 주소가 할당될 수 있습니다. 다른 가상 시스템과 주소가 충돌하면 이와 같이 변경될 수 있습니다. 즉, 이 가상 시스템의 전원이 꺼져 있던 동안 해당 MAC 주소가 전원이 켜져 있는 다른 가상 시스템에 할당되었기 때문일 수 있습니다.

자동 MAC 주소 할당 유형을 변경하거나 정적 MAC 주소를 설정하는 등 전원이 꺼진 가상 시스템의 네트워크 어댑터를 재구성하는 경우 vCenter Server는 MAC 주소 충돌 문제를 해결한 다음 어댑터를 재구성합니다.

MAC 주소 충돌 문제를 해결하는 방법에 대한 자세한 내용은 "vSphere 문제 해결" 설명서를 참조하십시오.

## VMware OUI 할당이란?

VMware OUI(Organizationally Unique Identifier) 할당은 기본 VMware OUI 00:50:56 및 vCenter Server ID를 기반으로 MAC 주소를 할당합니다.

VMware OUI 할당은 가상 시스템의 기본 MAC 주소 할당 모델입니다. 이 할당은 최대 64개의 vCenter Server 인스턴스에 적용되며, 각 vCenter Server는 최대 64,000개의 고유한 MAC 주소를 할당할 수 있습니다. VMware OUI 할당 체계는 소규모 배포 환경에 적합합니다.

## MAC 주소 형식

VMware OUI 할당 체계에 따르면 MAC 주소의 형식은 00:50:56:XX:YY:ZZ이며, 여기서 00:50:56은 VMware OUI를 나타내고, XX는 (128+ vCenter Server ID)로 계산되고 YY 및 ZZ는 임의의 두 자리 16진수 숫자입니다.

VMware OUI 할당을 통해 생성된 주소는 00:50:56:80:YY:ZZ - 00:50:56:BF:YY:ZZ 범위에 있습니다.

## 접두사 기반 MAC 주소 할당이란?

접두사 기반 할당을 사용하여 VMware의 기본 OUI인 00:50:56 이외의 OUI를 지정하거나, 더 큰 주소 공간에 대해 LAA(Locally Administered MAC Address)를 사용할 수 있습니다.

접두사 기반 MAC 주소 할당은 기본 VMware 할당의 한계를 해결하여 대규모 배포 환경에서 고유한 주소를 제공합니다. LAA 접두사를 사용하면 1,600만 개의 MAC 주소만 제공할 수 있는 범용 고유 주소 OUI 대신 매우 큰 MAC 주소 공간(2의 46제곱)을 이용할 수 있습니다.

동일한 네트워크의 서로 다른 vCenter Server 인스턴스에 제공하는 접두사가 고유한지 확인합니다. vCenter Server는 접두사를 사용하여 MAC 주소 중복 문제를 방지합니다. [MAC 주소 할당 문제 해결](#)을 참조하십시오.

## 범위 기반 MAC 주소 할당이란?

범위 기반 할당을 사용하여 LAA(Locally Administered Address)의 범위를 포함하거나 제외할 수 있습니다.

시작 및 끝 MAC 주소를 사용하여 범위를 하나 이상 지정합니다. 예를 들어 (02:50:68:00:00:02, 02:50:68:00:00:FF)와 같이 지정합니다. 그러면 MAC 주소가 지정된 범위 내에서만 생성됩니다.

여러 LAA 범위를 지정할 수 있으며 vCenter Server는 각 범위의 사용된 주소 수를 추적합니다. vCenter Server는 아직 사용 가능한 주소가 있는 첫 번째 범위의 MAC 주소를 할당합니다. vCenter Server는 해당 범위 내에서 MAC 주소 충돌이 있는지 확인합니다.

범위 기반 할당을 사용하는 경우 범위가 겹치지 않는 서로 다른 vCenter Server 인스턴스를 제공해야 합니다. vCenter Server는 다른 vCenter Server 인스턴스와 충돌할 수 있는 범위를 감지하지 않습니다. 중복된 MAC 주소와 관련하여 발생하는 문제를 해결하는 방법에 대한 자세한 내용은 [MAC 주소 할당 문제 해결](#)을 참조하십시오.

---

**참고** 새 버전의 vCenter Server로 업그레이드하면 범위 기반 MAC 주소 할당 설정이 손실됩니다. 업그레이드 후 범위 기반 MAC 주소 할당 설정을 수동으로 다시 생성해야 합니다.

---

## MAC 주소 할당

vSphere Client를 사용하여 접두사 기반 또는 범위 기반 MAC 주소 할당을 사용하도록 설정하고 할당 매개 변수를 조정할 수 있습니다.

VMware OUI 할당에서 범위 기반 할당으로 변경하는 등 할당 유형을 변경할 경우에는 vSphere Client를 사용합니다. 그러나 할당 체계가 접두사 기반 또는 범위 기반인 경우 다른 할당 체계로 변경하려면 `vpxd.cfg` 파일을 수동으로 편집하고 vCenter Server를 다시 시작해야 합니다.

### 범위 또는 접두사 기반 할당으로 변경 또는 조정

vSphere Client를 통해 기본 VMware OUI에서 범위 기반 또는 접두사 기반 MAC 주소 할당으로 전환하여 vSphere 배포에서 MAC 주소 중복 충돌을 방지하고 해결할 수 있습니다.

vSphere Client에서 vCenter Server 인스턴스에 사용할 수 있는 **고급 설정**을 사용하여 기본 VMware OUI에서 범위 기반 또는 접두사 기반 할당으로 할당 체계를 변경합니다.

범위 기반 또는 접두사 기반 할당에서 VMware OUI 할당으로 다시 전환하거나 범위 기반 할당과 접두사 기반 할당 사이에 전환하려면 `vpxd.cfg` 파일을 수동으로 편집합니다. [할당 유형 설정 또는 변경](#)의 내용을 참조하십시오.

#### 절차

- 1 vSphere Client에서 vCenter Server 인스턴스로 이동합니다.
- 2 구성 탭에서 **설정**을 확장하고 **고급 설정**을 선택합니다.
- 3 **설정 편집**을 클릭합니다.

#### 4 대상 할당 유형에 대한 매개 변수를 추가 또는 편집합니다.

할당 유형은 하나만 사용하십시오.

- 접두사 기반 할당으로 변경합니다.

키	예제 값
<code>config.vpxd.macAllocScheme.prefixScheme.prefix</code>	005026
<code>config.vpxd.macAllocScheme.prefixScheme.prefixLength</code>	23

`prefix` 및 `prefixLength`는 새로 추가된 vNIC의 MAC 주소 접두사 범위를 결정합니다. `prefix`는 vCenter Server 인스턴스와 관련된 MAC 주소의 시작 OUI이고 `prefixLength`는 해당 접두사의 길이 (비트)를 결정합니다.

예를 들어 표의 설정을 사용하면 VM NIC MAC 주소가 00:50:26 또는 00:50:27로 시작합니다.

- 범위 기반 할당으로 변경합니다.

키	예제 값
<code>config.vpxd.macAllocScheme.rangeScheme.range[X].begin</code>	005067000000
<code>config.vpxd.macAllocScheme.rangeScheme.range[X].end</code>	005067ffffff

`range[X]`의 `range[X]`는 범위 시퀀스 번호를 나타냅니다. 예를 들어 `range[0]`의 0은 MAC 주소 할당에서 첫 번째 범위의 할당 설정을 나타냅니다.

#### 5 저장을 클릭합니다.

### 할당 유형 설정 또는 변경

범위 또는 접두사 기반 할당을 VMware OUI 할당으로 변경하려는 경우 `vpxd.cfg` 파일에서 할당 유형을 설정하고 vCenter Server를 다시 시작해야 합니다.

#### 사전 요구 사항

`vpxd.cfg` 파일을 변경하기 전에 할당 유형을 선택합니다. 할당 유형에 대한 자세한 내용은 [vCenter Server에서 MAC 주소 지정](#)의 내용을 참조하십시오.

#### 절차

- 1 vCenter Server의 호스트 시스템에서 `/etc/vmware-vpx` 디렉토리로 이동합니다.
- 2 `vpxd.cfg` 파일을 엽니다.

- 3 사용할 할당 유형을 선택하고 파일에 해당하는 XML 코드를 입력하여 할당 유형을 구성합니다.  
다음은 사용할 XML 코드의 예입니다.

**참고** 할당 유형은 하나만 사용하십시오.

◆ VMware OUI 할당

```
<vpxd>
  <macAllocScheme>
    <VMwareOUI>true</VMwareOUI>
  </macAllocScheme>
</vpxd>
```

◆ 접두사 기반 할당

```
<vpxd>
  <macAllocScheme>
    <prefixScheme>
      <prefix>005026</prefix>
      <prefixLength>23</prefixLength>
    </prefixScheme>
  </macAllocScheme>
</vpxd>
```

◆ 범위 기반 할당

```
<vpxd>
  <macAllocScheme>
    <rangeScheme>
      <range id="0">
        <begin>005067000001</begin>
        <end>005067000001</end>
      </range>
    </rangeScheme>
  </macAllocScheme>
</vpxd>
```

- 4 vpxd.cfg를 저장합니다.  
5 vCenter Server 호스트를 다시 시작합니다.

## ESXi 호스트에서 MAC 주소 생성

ESXi 호스트는 vCenter Server에 연결되어 있지 않을 때 가상 시스템 어댑터의 MAC 주소를 생성합니다. 이러한 주소에는 충돌을 방지하기 위한 별도의 VMware OUI가 포함됩니다.

ESXi 호스트는 다음 중 하나에 해당하는 경우에 가상 시스템 어댑터의 MAC 주소를 생성합니다.

- 호스트가 vCenter Server에 연결되어 있지 않은 경우
- 가상 시스템 구성 파일에 MAC 주소와 MAC 주소 할당 유형에 대한 정보가 포함되어 있지 않은 경우

## MAC 주소 형식

호스트는 VMware OUI 00:0c:29와 16진수 형식의 가상 시스템 UUID 중 마지막 세 개의 옥텟으로 구성된 MAC 주소를 생성합니다. 가상 시스템 UUID는 ESXi 물리적 시스템의 UUID와 가상 시스템의 구성 파일(.vmx) 경로를 사용하여 계산된 해시를 기반으로 합니다.

## MAC 주소 충돌 방지

지정된 물리적 시스템에서 일시 중단된 가상 시스템과 실행 중인 가상 시스템의 네트워크 어댑터에 할당된 모든 MAC 주소는 충돌 여부가 추적됩니다.

호스트에서 생성된 MAC 주소를 사용하는 가상 시스템을 한 vCenter Server에서 다른 vCenter Server로 가져올 경우, 가상 시스템의 전원을 켜 때 **복사함** 옵션을 선택하면 주소가 다시 생성되므로 대상 vCenter Server 내에서 또는 vCenter Server 시스템 간에 발생할 수 있는 충돌을 방지할 수 있습니다.

## 가상 시스템에 대해 정적 MAC 주소를 설정하는 방법

대부분의 네트워크 배포에서는 생성된 MAC 주소를 사용하는 것이 좋습니다. 하지만 고유한 값을 사용하여 가상 시스템 어댑터의 정적 MAC 주소를 설정해야 할 수도 있습니다.

다음은 정적 MAC 주소를 설정할 수 있는 경우를 보여 줍니다.

- 서로 다른 물리적 호스트에 있는 가상 시스템 어댑터가 동일한 서브넷을 공유하고 동일한 MAC 주소가 할당되어 충돌이 발생하는 경우
- 가상 시스템 어댑터에 항상 동일한 MAC 주소를 사용하려는 경우

기본적으로 VMware에서는 수동으로 생성된 주소에 OUI(Organizationally Unique Identifier) 00:50:56을 사용하지만 수동으로 생성된 모든 고유 주소도 지원됩니다.

**참고** VMware가 아닌 다른 디바이스에서 VMware 구성 요소에 할당된 주소를 사용하지 않도록 해야 합니다. 예를 들어 동일한 서브넷에 11:11:11:11:11:11, 22:22:22:22:22:22를 정적 MAC 주소로 사용하는 물리적 서버가 여러 개 있을 수 있습니다. 물리적 서버는 vCenter Server 인벤토리에 속하지 않으므로 vCenter Server가 주소 충돌 여부를 확인할 수 없습니다.

## 정적 MAC 주소의 VMware OUI

기본적으로 정적 MAC 주소에는 접두사로 VMware OUI(Organizationally Unique Identifier)가 포함됩니다. 그러나 VMware OUI가 제공하는 사용 가능한 주소의 범위는 제한되어 있습니다.

VMware OUI를 사용하도록 결정할 경우 범위 중 일부는 vCenter Server, 호스트 물리적 NIC 및 가상 NIC에서 사용하거나 나중에 사용할 수 있도록 예약됩니다.

다음 형식을 준수하여 VMware OUI 접두사가 포함된 정적 MAC 주소를 설정할 수 있습니다.

```
00:50:56:XX:YY:ZZ
```

여기서 *XX*는 00과 3F 사이의 유효한 16진수 숫자이고, *YY*와 *ZZ*는 00과 FF 사이의 유효한 16진수 숫자입니다. vCenter Server에 의해 생성되거나 인프라 트래픽을 위해 VMkernel 어댑터에 할당된 MAC 주소와 충돌하지 않도록 하려면 *XX*의 값이 3F보다 크지 않아야 합니다.

수동으로 생성하는 MAC 주소의 최대값은 다음과 같습니다.

```
00:50:56:3F:FF:FF
```

생성된 MAC 주소와 수동으로 할당된 MAC 주소 간의 충돌을 방지하려면 하드 코딩된 주소에서 *XX:YY:ZZ*의 고유한 값을 선택합니다.

## 정적 MAC 주소 할당

vSphere Client를 사용하여 전원이 꺼진 가상 시스템의 가상 NIC에 정적 MAC 주소를 할당할 수 있습니다.

### 절차

- 1 vSphere Client에서 가상 시스템을 찾습니다.
  - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택하고 **VM** 탭을 클릭합니다.
  - b **가상 시스템**을 클릭하고 목록에서 가상 시스템을 클릭합니다.
- 2 가상 시스템의 전원을 끕니다.
- 3 [작업] 메뉴에서 [설정 편집]을 선택합니다.
- 4 설정을 표시하는 대화상자에서 **가상 하드웨어** 탭을 선택합니다.
- 5 네트워크 어댑터 섹션을 확장합니다.
- 6 MAC 주소 아래의 드롭다운 메뉴에서 **수동**을 선택합니다.
- 7 정적 MAC 주소를 입력하고 **확인**을 클릭합니다.
- 8 가상 시스템의 전원을 켭니다.

## 가상 시스템 구성 파일에서 정적 MAC 주소 할당

가상 시스템에 정적 MAC 주소를 설정하려면 vSphere Client를 사용하여 가상 시스템의 구성 파일을 편집하면 됩니다.

### 절차

- 1 vSphere Client에서 가상 시스템을 찾습니다.
  - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택하고 **VM** 탭을 클릭합니다.
  - b **가상 시스템**을 클릭하고 목록에서 가상 시스템을 클릭합니다.
- 2 가상 시스템의 전원을 끕니다.
- 3 **작업** 드롭다운 메뉴에서 **설정 편집**을 선택합니다.
- 4 **VM 옵션** 탭을 선택하고 **고급**을 확장합니다.

- 5 구성 편집 메뉴를 클릭합니다.
- 6 정적 MAC 주소를 할당하려면 필요한 대로 매개 변수를 추가하거나 편집합니다.

매개 변수	값
<code>ethernetX.addressType</code>	정적
<code>ethernetX.address</code>	<code>MAC_address_of_the_virtual_NIC</code>

`ethernet` 옆의 `X`는 가상 시스템에서 가상 NIC의 시퀀스 번호를 나타냅니다.

예를 들어 `ethernet0`의 `0`은 가상 시스템에 추가된 첫 번째 가상 NIC 디바이스의 설정을 나타냅니다.

- 7 확인을 클릭합니다.
- 8 가상 시스템의 전원을 켭니다.

# IPv6에 대한 vSphere 구성

# 13

더 큰 주소 공간과 향상된 주소 할당을 위해 순수 IPv6 환경에서 작업을 위한 ESXi 호스트 및 vCenter Server를 구성합니다.

IPv6은 IETF(Internet Engineering Task Force)에 의해 IPv4의 후속 버전으로 지정되어 다음과 같은 이점을 제공합니다.

- 늘어난 주소 길이. 늘어난 주소 공간은 주소 소진 문제를 해결하고 네트워크 주소 변환의 필요성을 없앱니다. IPv4는 32비트 주소를 사용하는 데 비해 IPv6은 128비트 주소를 사용합니다.
- 노드의 향상된 주소 자동 구성 기능.

다음으로 아래 항목을 읽으십시오.

- [vSphere IPv6 연결](#)
- [IPv6에 vSphere 배포](#)
- [호스트에서 IPv6 지원 활성화 또는 비활성화](#)
- [ESXi 호스트에서 IPv6 설정](#)
- [vCenter Server에서 IPv6 설정](#)

## vSphere IPv6 연결

vSphere 6.0 이상을 기반으로 하는 환경에서 노드와 기능은 정적 및 자동 주소 구성을 지원하는 IPv6을 통해 투명하게 통신할 수 있습니다.

## vSphere 노드 간 통신의 IPv6

vSphere 배포의 노드는 IPv6을 사용하여 통신하고 네트워크 구성에 따라 할당된 주소를 수락할 수 있습니다.

표 13-1. vSphere 환경에서 노드의 IPv6 지원

연결 유형	IPv6 지원	vSphere 노드의 주소 구성
ESXi에서 ESXi로	예	<ul style="list-style-type: none"><li>■ 정적</li><li>■ 자동: AUTOCONF/DHCPv6</li></ul>
vCenter Server 시스템에서 ESXi로	예	<ul style="list-style-type: none"><li>■ 정적</li><li>■ 자동: AUTOCONF/DHCPv6</li></ul>



표 13-1. vSphere 환경에서 노드의 IPv6 지원 (계속)

연결 유형	IPv6 지원	vSphere 노드의 주소 구성
vCenter Server 시스템에서 시스템으로	예	<ul style="list-style-type: none"> <li>■ 정적</li> <li>■ 자동: AUTOCONF/DHCPv6</li> </ul>
ESXi에서 vSphere Client 시스템으로	예	<ul style="list-style-type: none"> <li>■ 정적</li> <li>■ 자동: AUTOCONF/DHCPv6</li> </ul>
가상 시스템에서 가상 시스템으로	예	<ul style="list-style-type: none"> <li>■ 정적</li> <li>■ 자동: AUTOCONF/DHCPv6</li> </ul>
ESXi에서 iSCSI 스토리지로	예	<ul style="list-style-type: none"> <li>■ 정적</li> <li>■ 자동: AUTOCONF/DHCPv6</li> </ul>
ESXi에서 NFS 스토리지로	예	<ul style="list-style-type: none"> <li>■ 정적</li> <li>■ 자동: AUTOCONF/DHCPv6</li> </ul>
ESXi에서 Active Directory로	아니요 vCenter Server를 통해 LDAP를 사용하여 ESXi를 Active Directory 데이터베이스에 연결	-
vCenter Server에서 Active Directory로	아니요 LDAP를 사용하여 vCenter Server를 Active Directory 데이터베이스에 연결	-

## vSphere 기능의 IPv6 연결

특정 vSphere 기능은 IPv6을 지원하지 않습니다.

- IPMI(Intelligent Platform Management Interface) 및 Hewlett-Packard iLO(Integrated Lights-Out).를 통한 vSphere DPM. vSphere 6.5 이상은 호스트의 대기 모드를 종료하기 위한 WOL(Wake-On-LAN)만 지원합니다.
- Authentication Proxy
- Active Directory에 연결된 vSphere Management Assistant 및 ESXCLI.

LDAP를 사용하여 vSphere Management Assistant 또는 ESXCLI를 Active Directory 데이터베이스에 연결합니다.

## 가상 시스템의 IPv6 연결

가상 시스템은 IPv6을 통해 네트워크에서 데이터를 교환할 수 있습니다. vSphere는 가상 시스템에 대한 IPv6 주소의 정적 및 자동 할당을 지원합니다.

가상 시스템의 게스트 운영 체제를 사용자 지정할 때 하나 이상의 IPv6 주소를 구성할 수도 있습니다.

## vSAN 연결

vSAN은 IPv6을 지원합니다. NFS 4.1에 AUTH\_SYS를 사용합니다.

## FQDN 및 IPv6 주소

vSphere에서는 DNS 서버의 IPv6 주소에 매핑된 FQDN(정규화된 도메인 이름)을 사용해야 합니다. DNS 서버에 역방향 조회를 위한 올바른 FQDN이 있는 경우 IPv6 주소를 사용할 수 있습니다.

순수 IPv6 환경에서 vCenter Server를 배포하려면 FQDN만 사용해야 합니다.

## IPv6에 vSphere 배포

순수 IPv6 환경에서 vSphere를 실행하여 확장된 주소 공간과 유연한 주소 할당을 사용합니다.

IPv6 네트워크에서 vCenter Server 및 ESXi 호스트를 배포하려는 경우 추가 단계를 수행해야 합니다.

### 다음으로 읽을 항목

- [vSphere 설치에서 IPv6 사용](#)

IPv6 네트워크에 vSphere 6.5의 그린필드 배포가 있는 경우 배포 노드에서 IPv6을 구성하고 연결하여 순수 IPv6 관리 연결을 위한 ESXi 및 vCenter Server를 구성합니다.

- [업그레이드된 vSphere 환경에서 IPv6 사용](#)

설치 또는 업그레이드된 vCenter Server와 업그레이드된 ESXi로 구성된 vSphere 6.5의 IPv4 배포에서 배포된 노드에서 IPv6을 사용하도록 설정하고 다시 연결하여 순수 IPv6 관리 연결을 위한 ESXi 및 vCenter Server를 구성합니다.

## vSphere 설치에서 IPv6 사용

IPv6 네트워크에 vSphere 6.5의 그린필드 배포가 있는 경우 배포 노드에서 IPv6을 구성하고 연결하여 순수 IPv6 관리 연결을 위한 ESXi 및 vCenter Server를 구성합니다.

### 사전 요구 사항

- vCenter Server, ESXi 호스트 및 외부 데이터베이스(사용된 경우)에 대한 IPv6 주소가 DNS 서버의 FQDN(정규화된 도메인 이름)에 매핑되었는지 확인합니다.
- 네트워크 인프라가 ESXi 호스트, vCenter Server 및 외부 데이터베이스(사용된 경우)에 대한 IPv6 연결을 제공하는지 확인합니다.
- IPv6 주소에 매핑된 FQDN을 통해 설치된 6.5 버전의 vCenter Server가 있는지 확인합니다. "vCenter Server 설치 및 설정" 설명서를 참조하십시오.
- 호스트에 ESXi 6.5이 설치되어 있는지 확인합니다. "vCenter Server 설치 및 설정" 설명서를 참조하십시오.

### 절차

- 1 DCUI(Direct Console User Interface)에서 각 ESXi 호스트를 순수 IPv6 노드로 구성합니다.
  - a DCUI에서 F2 키를 눌러 호스트에 로그인합니다.
  - b **관리 네트워크 구성** 메뉴에서 **IPv6 구성**을 선택하고 Enter 키를 누릅니다.

- c IPv6 주소를 호스트에 할당합니다.

주소 할당 옵션	설명
DHCPv6을 사용하여 자동 주소 할당	<ol style="list-style-type: none"> <li>동적 IPv6 주소 및 네트워크 구성 사용 옵션을 선택하고 DHCPv6 사용을 선택합니다.</li> <li>Enter 키를 눌러 변경 사항을 저장합니다.</li> </ol>
정적 주소 할당	<ol style="list-style-type: none"> <li>정적 IPv6 주소 및 네트워크 구성 설정 옵션을 선택하고 호스트 및 기본 게이트웨이의 IPv6 주소를 입력합니다.</li> <li>Enter 키를 눌러 변경 사항을 저장합니다.</li> </ol>

- d 관리 네트워크 구성 메뉴에서 IPv4 구성을 선택하고 Enter 키를 누릅니다.

- e 관리 네트워크에 대한 IPv4 구성 사용 안 함을 선택하고 Enter 키를 누릅니다.

- 2 vSphere Client에서 호스트를 인벤토리에 추가합니다.

## 업그레이드된 vSphere 환경에서 IPv6 사용

설치 또는 업그레이드된 vCenter Server와 업그레이드된 ESXi로 구성된 vSphere 6.5의 IPv4 배포에서 배포된 노드에서 IPv6을 사용하도록 설정하고 다시 연결하여 순수 IPv6 관리 연결을 위한 ESXi 및 vCenter Server를 구성합니다.

### 사전 요구 사항

- 네트워크 인프라가 ESXi 호스트, vCenter Server 및 외부 데이터베이스(사용된 경우)에 대한 IPv6 연결을 제공하는지 확인합니다.
- vCenter Server, ESXi 호스트 및 외부 데이터베이스(사용된 경우)에 대한 IPv6 주소가 DNS 서버의 FQDN(정규화된 도메인 이름)에 매핑되었는지 확인합니다.
- vCenter Server 버전 6.x가 설치되거나 업그레이드되었는지 확인합니다. "vCenter Server 설치 및 설정" 및 "vCenter Server 업그레이드" 설명서를 참조하십시오.
- 모든 ESXi 호스트가 버전 6.x로 업그레이드되었는지 확인합니다. "VMware ESXi 업그레이드" 설명서를 참조하십시오.

### 절차

- 1 vSphere Client에서 호스트와 vCenter Server의 연결을 끊습니다.

## 2 각 ESXi 호스트를 순수 IPv6 노드로 구성합니다.

- a SSH 연결을 열고 ESXi 호스트에 로그인합니다.
- b 다음 명령을 실행합니다.

```
esxcli network ip interface ipv6 set -i vmk0 -e true
```

- c IPv6 주소를 관리 네트워크에 할당합니다.

주소 할당 옵션	설명
정적 주소 할당	<ol style="list-style-type: none"> <li>1 SSH 연결을 열고 ESXi 호스트에 로그인합니다.</li> <li>2 다음 명령을 실행하여 관리 네트워크 vmk0에 대한 정적 IPv6 주소를 설정합니다.           <pre>esxcli network ip interface ipv6 address add -I IPv6_address -i vmk0</pre> </li> <li>3 다음 명령을 실행하여 관리 네트워크 vmk0의 기본 게이트웨이를 설정합니다.           <pre>esxcli network ip interface ipv6 set -i vmk0 -g default_gateway_IPv6_address</pre> </li> <li>4 다음 명령을 실행하여 DNS 서버를 추가합니다.           <pre>esxcli network ip dns server add -s DNS_server_IPv6_address</pre> </li> </ol>
DHCPv6을 사용하여 자동 주소 할당	<ol style="list-style-type: none"> <li>1 SSH 연결을 열고 ESXi 호스트에 로그인합니다.</li> <li>2 다음 명령을 실행하여 관리 네트워크 vmk0에 대해 DHCPv6을 사용하도록 설정합니다.           <pre>esxcli network ip interface ipv6 -i vmk0 -enable-dhcpv6 = true</pre> </li> <li>3 다음 명령을 실행하여 관리 네트워크 vmk0에 IPv6 라우터가 보급되도록 설정합니다.           <pre>esxcli network ip interface ipv6 set -i vmk0 -enable-router-adv =true</pre> </li> <li>4 다음 명령 중 하나를 실행하여 DHCPv6에서 게시한 DNS 설정을 사용하거나 DNS 서버를 추가합니다.           <pre>esxcli network ip dns server add -s DNS_server_IPv6_address</pre> <pre>esxcli network ip interface ipv6 set -i vmk0 --peer-dns=true</pre> </li> </ol>

- 3 관리 네트워크에 대한 IPv4 구성을 비활성화합니다.
  - a SSH 연결을 열고 ESXi 호스트에 로그인합니다.
  - b 다음 명령을 실행합니다.

```
esxcli network ip interface ipv4 set -i vmk0 --type=none
```

- 4 vCenter Server가 외부 데이터베이스를 사용하는 경우 해당 데이터베이스를 IPv6 노드로 구성합니다.
- 5 vCenter Server를 순수 IPv6 노드로 구성하고 다시 시작합니다.
- 6 데이터베이스 서버에서 IPv4를 비활성화합니다.
- 7 vSphere Client에서 호스트를 인벤토리에 추가합니다.
- 8 네트워크 인프라에서 IPv4를 비활성화합니다.

## 호스트에서 IPv6 지원 활성화 또는 비활성화

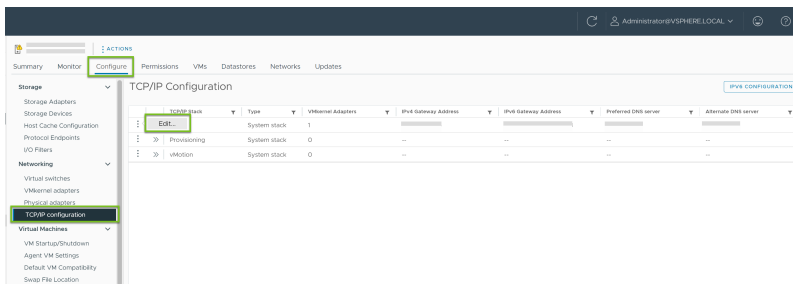
vSphere의 IPv6 지원을 통해 호스트는 큰 주소 공간, 향상된 멀티 캐스팅, 단순화된 라우팅 등의 기능을 갖춘 IPv6 네트워크에서 작동할 수 있습니다.

ESXi 6.0 이상 릴리스에서는 기본적으로 IPv6이 사용되도록 설정되어 있습니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 네트워킹을 확장하고 TCP/IP 구성을 선택합니다.
- 3 편집을 클릭합니다.

그림 13-1. TCP/IP 구성



- 4 전환 버튼을 사용하여 IPv6 지원을 활성화하거나 비활성화합니다.
- 5 확인을 클릭합니다.
- 6 호스트를 재부팅하여 IPv6 지원의 변경 내용을 적용합니다.

### 다음에 수행할 작업

호스트에서 VMkernel 어댑터(예: 관리 네트워크의 VMkernel 어댑터)의 IPv6 설정을 구성합니다. [ESXi 호스트에서 IPv6 설정의 내용을 참조하십시오.](#)

## ESXi 호스트에서 IPv6 설정

IPv6을 통해 ESXi 호스트를 관리 네트워크, vSphere vMotion, 공유 스토리지, vSphere Fault Tolerance 등에 연결하려면 호스트에서 VMkernel 어댑터의 IPv6 설정을 편집합니다.

### 사전 요구 사항

IPv6이 ESXi 호스트에서 사용하도록 설정되어 있는지 확인합니다. [호스트에서 IPv6 지원 활성화 또는 비활성화](#)의 내용을 참조하십시오.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **네트워킹**을 확장하고 **VMkernel 어댑터**를 선택합니다.
- 3 대상 Distributed Switch 또는 표준 스위치의 VMkernel 어댑터를 선택하고 **편집**을 클릭합니다.
- 4 설정 편집 대화상자에서 **IPv6 설정**을 클릭합니다.
- 5 VMkernel 어댑터의 주소 할당을 구성합니다.

IPv6 주소 옵션	설명
DHCP를 통해 자동으로 IPv6 주소 가져오기	DHCPv6 서버에서 VMkernel 어댑터에 대한 IPv6 주소를 수신합니다.
라우터 알림을 통해 자동으로 IPv6 주소 가져오기	라우터 알림을 통해 라우터에서 VMkernel 어댑터에 대한 IPv6 주소를 수신합니다.
정적 IPv6 주소	하나 이상의 주소를 설정합니다. 각 주소 항목에 대해 어댑터의 IPv6 주소, 기본 게이트웨이의 서브넷 접두사 길이 및 IPv6 주소를 입력합니다.

네트워크의 구성에 따라 여러 할당 옵션을 선택할 수 있습니다.

- 6 **확인**을 클릭하여 VMkernel 어댑터에 대한 변경 사항을 적용합니다.

## vCenter Server에서 IPv6 설정

vSphere Client를 사용하여 IPv6 네트워크에서 ESXi 호스트와의 통신을 위한 vCenter Server를 구성합니다.

### 절차

- 1 vSphere Client 기본 페이지에서 **관리 > 배포 > 시스템 구성**을 클릭합니다.
- 2 **시스템 구성** 아래의 목록에서 노드를 선택합니다.
- 3 **로그인**을 클릭합니다.
- 4 vSphere Client를 사용하여 vCenter Server 인스턴스에 administrator@your\_domain\_name으로 로그인합니다.  
주소의 유형은 http://appliance-IP-address-or-FQDN/ui입니다.
- 5 일반에서 **네트워킹**을 선택하고 **편집**을 클릭합니다.

- 6 네트워크 인터페이스 이름을 확장하여 IP 주소 설정을 편집합니다.
- 7 IPv6 주소 설정을 편집합니다.

옵션	설명
IPv6 설정 사용 또는 사용 안 함	전환 스위치 옵션을 기반으로 IPv6 주소를 사용하거나 사용하지 않도록 설정합니다.
DHCP를 통해 자동으로 IPv6 설정 가져오기	DHCP를 사용하여 네트워크에서 장치에 IPv6 주소를 자동으로 할당합니다.
라우터 알림을 통해 자동으로 IPv6 설정 가져오기	라우터 알림을 사용하여 네트워크에서 장치에 IPv6 주소를 자동으로 할당합니다.
정적 IPv6 주소 사용	수동으로 설정한 정적 IPv6 주소를 사용합니다. <ol style="list-style-type: none"> <li>확인란을 클릭합니다.</li> <li>IPv6 주소 및 서브넷 접두사 길이를 입력합니다.</li> <li><b>추가</b>를 클릭하여 추가 IPv6 주소를 입력합니다.</li> <li><b>저장</b>을 클릭합니다.</li> </ol>
<b>참고</b> 고정 IPv4 또는 IPv6 주소의 경우 DNS 서버를 수동으로 설정해야 합니다.	

DHCP 및 라우터 알림을 통해 IPv6 설정을 자동으로 가져오도록 장치를 구성할 수 있습니다. 동시에 정적 IPv6 주소를 할당할 수 있습니다.

**참고** IPv4 및 IPv6 IP 주소가 변경되면 세컨드 파티 및 타사 솔루션을 다시 등록해야 합니다.

- 8 (선택 사항) 라우터 알림을 통해 자동으로 할당된 IPv6 주소를 제거하려면 **주소 제거**를 클릭하고 주소를 삭제합니다.

vCenter Server가 라우터 알림을 통해 가져온 특정 IPv6 주소를 삭제하여 이러한 주소에 대한 통신을 중지하고 구성된 정적 주소를 적용하고자 할 수 있습니다.

#### 다음에 수행할 작업

FQDN을 사용하여 IPv6을 통해 ESXi 호스트를 vCenter Server에 연결합니다.

가상 시스템과 호스트 간의 트래픽을 분석하려면 vSphere 표준 스위치 또는 vSphere Distributed Switch의 포트를 통과하는 네트워크 연결 및 패킷을 모니터링합니다.

다음으로 아래 항목을 읽으십시오.

- 네트워크 패킷을 캡처하는 방법
- pktcap-uw 유틸리티를 사용하여 네트워크 패킷 캡처 및 추적
- vSphere Distributed Switch의 NetFlow 설정 구성
- 포트 미러링이란?
- vSphere Distributed Switch 상태 점검
- 스위치 탐색 프로토콜
- NSX 가상 Distributed Switch의 토폴로지 보기

## 네트워크 패킷을 캡처하는 방법

PacketCapture 유틸리티를 사용하여 연결 속도 저하, 패킷 손실 및 연결 문제와 같은 네트워킹 문제를 진단하는 방법을 알아봅니다.

PacketCapture는 네트워크 문제를 진단하는 데 필요한 최소한의 데이터만 캡처하여 저장하는 경량 tcpdump 유틸리티입니다. PacketCapture는 ESXi 및 vCenter Server의 rhttpproxy 서비스에 통합되어 있습니다. rhttpproxy 서비스 XML 구성 파일을 편집하여 PacketCapture를 시작하고 중지합니다.

---

**참고** ESXi 8.0 이하의 경우, 네트워크 패킷 캡처를 사용하도록 설정하는 프로세스는 rhttpproxy 서비스 XML 구성 파일을 편집하는 것이었습니다. ESXi 8.0 업데이트 1 이상부터 역방향 프록시 구성이 XML 파일에서 configstore 데이터베이스로 이동되었습니다. configstorecli를 사용하여 네트워크 패킷 캡처를 사용하도록 설정하려면 <https://kb.vmware.com/s/article/89489> 항목을 참조하십시오.

---



## 절차

## 1 패킷 캡처를 시작합니다.

- a SSH 연결을 열고 ESXi 호스트 또는 vCenter Server에 로그인합니다.
- b 편집을 위해 config.xml 파일을 엽니다.

vSphere 구성 요소	파일 위치
ESXi	/etc/vmware/rhttpproxy/config.xml
vCenter Server	/etc/vmware-rhttpproxy/config.xml

- c 다음과 같이 변경합니다.

```
<config>
  <packetCapture>
    <enabled>>true</enabled>
```

- d (선택 사항) PacketCapture 옵션을 구성합니다.

옵션 및 기본값	설명
<code>&lt;validity&gt;72&lt;/validity&gt;</code>	시작 시 지정된 시간 이전에 마지막으로 수정되어 현재 프로세스에 속하지 않는 모든 pcap 및 pcap.gz 파일을 삭제합니다.
<code>&lt;directory&gt;/directory_path&lt;/directory&gt;</code>	pcap 및 pcap.gz 파일이 저장된 디렉토리입니다. 디렉토리가 존재하고 액세스가 가능해야 합니다.
<code>&lt;maxDataInPcapFile&gt;52428800&lt;/maxDataInPcapFile&gt;</code>	다음 파일 크기 초과하기 전에 pcap 및 pcap.gz 파일이 각각 저장할 수 있는 캡처된 데이터의 양(바이트)입니다. 최소 크기는 vCenter Server에서 5MB이고 ESXi에서는 2.5MB입니다. <b>참고</b> 캡처된 데이터 50MB를 pcap 파일에 저장하려면 pcap 파일이 약 67.5MB 필요합니다.
<code>&lt;maxPcapFilesCount&gt;5&lt;/maxPcapFilesCount&gt;</code>	순환할 pcap 또는 pcap.gz 파일의 수입니다. 최소 수는 2입니다.

- e config.xml 파일을 저장하고 닫습니다.
- f 다음 명령을 실행하여 config.xml 파일을 다시 로드합니다.

```
kill -SIGHUP `pidof rhttpproxy`
```

## 2 패킷 캡처를 중지합니다.

- a SSH 연결을 열고 ESXi 호스트 또는 vCenter Server에 로그인합니다.
- b 편집을 위해 config.xml 파일을 엽니다.
- c 다음과 같이 변경합니다.

```
<config>
  <packetCapture>
    <enabled>>false</enabled>
```

- d config.xml 파일을 저장하고 닫습니다.
- e 다음 명령을 실행하여 config.xml 파일을 다시 로드합니다.
 

```
kill -SIGHUP `pidof rhttpproxy`
```

### 3 캡처된 데이터를 수집합니다.

pcap 또는 pcap.gz 파일은 다음 기본 디렉토리에 저장됩니다.

vSphere 구성 요소	파일 위치
ESXi	/var/run/log
vCenter Server	/var/log/vmware/rhttpproxy

#### 다음에 수행할 작업

pcap 및 pcap.gz 파일을 Wireshark와 같은 네트워크 분석기 도구를 실행하는 시스템에 복사하고 패킷 세부 정보를 검토합니다.

ESXi 호스트에서 캡처된 pcap 및 pcap.gz를 분석하기 전에 TraceWrangler 유틸리티를 사용하여 프레임 크기 메타데이터를 수정합니다. 자세한 내용은 <https://kb.vmware.com/kb/52843>을 참조하십시오.

## pktcap-uw 유틸리티를 사용하여 네트워크 패킷 캡처 및 추적

Wireshark와 같은 네트워크 분석 도구의 그래픽 사용자 인터페이스를 사용하여 패킷 정보를 분석하고 물리적 네트워크 어댑터, VMkernel 어댑터 및 가상 시스템 어댑터를 통과하는 트래픽을 모니터링하는 방법을 알아봅니다.

vSphere에서는 pktcap-uw 콘솔 유틸리티를 사용하여 호스트의 패킷을 모니터링할 수 있습니다. ESXi 호스트에 추가 설치 없이 유틸리티를 사용할 수 있습니다. pktcap-uw는 트래픽을 모니터링할 수 있는 호스트 네트워크 스택의 여러 지점을 제공합니다.

캡처한 패킷을 자세히 분석하려면 pktcap-uw 유틸리티에서 패킷 내용을 PCAP 또는 PCAPNG 형식의 파일에 저장하고 해당 파일을 Wireshark에서 열 수 있습니다. 손실된 패킷의 문제를 해결하고 패킷 경로를 네트워크 스택에서 추적할 수도 있습니다.

**참고** pktcap-uw 유틸리티는 vSphere 릴리스 간에 이전 버전과의 호환성이 완벽하게 지원되지는 않습니다. 유틸리티의 옵션은 향후에 변경될 수 있습니다.

### 패킷 캡처를 위한 pktcap-uw 명령 구문

패킷이 ESXi 호스트의 네트워크 스택을 이동하는 동안 패킷 내용을 검사하려면 pktcap-uw 유틸리티를 사용합니다.

## 패킷 캡처를 위한 pktcap-uw 구문

pktcap-uw 명령에는 네트워크 스택의 특정 위치에서 패킷을 캡처하기 위한 다음과 같은 구문이 포함됩니다.

```
pktcap-uw
  switch_port_arguments
  capture_point_options
  filter_options
  output_control_options
```

**참고** pktcap-uw 유틸리티의 특정 옵션은 VMware 내부용으로 설계되었으며 VMware 기술 지원팀의 감독 하에서만 사용해야 합니다. 이러한 옵션은 "vSphere 네트워킹" 가이드에서 설명하지 않습니다.

표 14-1. 패킷 캡처를 위한 pktcap-uw 인수

인수 그룹	인수	설명
<i>switch_port_arguments</i>	--uplink vmnicX	물리적 어댑터와 관련된 패킷을 캡처합니다.  물리적 어댑터와 가상 스위치 사이의 경로에 있는 특정 위치에서 패킷을 모니터링하기 위해 --uplink 옵션 및 --capture 옵션을 결합할 수 있습니다.  물리적 어댑터에 도달하는 패킷 캡처의 내용을 참조하십시오.
	--vmk vmkX	VMkernel 어댑터와 관련된 패킷을 캡처합니다.  VMkernel 어댑터와 가상 스위치 사이의 경로에 있는 특정 위치에서 패킷을 모니터링하기 위해 vmk 옵션 및 --capture 옵션을 결합할 수 있습니다.  VMkernel 어댑터에 대한 패킷을 캡처하는 방법의 내용을 참조하십시오.

표 14-1. 패킷 캡처를 위한 pktcap-uw 인수 (계속)

인수 그룹	인수	설명
	<code>--switchport {vmxnet3_port_ID   vmkernel_adapter_port_ID}</code>	<p>VMXNET3 가상 시스템 어댑터 또는 특정 가상 스위치 포트에 연결된 VMkernel 어댑터와 관련된 패킷을 캡처합니다. <code>esxstop</code> 유틸리티의 네트워크 패널에서 포트 ID를 확인할 수 있습니다.</p> <p>VMXNET3 어댑터 또는 VMkernel 어댑터와 가상 스위치 사이의 경로에 있는 특정 위치에서 패킷을 모니터링하기 위해 <code>switchport</code> 옵션 및 <code>capture</code> 옵션을 결합할 수 있습니다. <a href="#">VMXNET3 가상 시스템 어댑터에 대한 패킷을 캡처하는 방법의 내용을 참조하십시오.</a></p>
	<code>--lifID lif_ID</code>	분산 라우터의 논리 인터페이스와 관련된 패킷을 캡처합니다. 자세한 내용은 "VMware NSX" 설명서를 참조하십시오.
<i>capture_point_options</i>	<code>--capture capture_point</code>	네트워크 스택의 특정 위치에서 패킷을 캡처합니다. 예를 들어 패킷이 물리적 어댑터에서 도착한 직후에 패킷을 모니터링할 수 있습니다.
	<code>--dir {0 1 2}</code>	<p>가상 스위치와 관련하여 흐름의 방향에 따라 패킷을 캡처합니다.</p> <p>0은 수신 트래픽을 나타내고, 1은 송신 트래픽을 나타내며, 2는 양방향 트래픽을 나타냅니다.</p> <p>기본적으로 <code>pktcap-uw</code> 유틸리티는 수신 트래픽을 캡처합니다.</p> <p><code>--dir</code> 옵션을 <code>--uplink</code>, <code>--vmk</code> 또는 <code>--switchport</code> 옵션과 함께 사용합니다.</p>
	<code>--stage {0 1}</code>	<p>소스 또는 대상에 더 가까운 패킷을 캡처합니다. 스택 내의 위치를 이동하는 동안 패킷이 어떻게 변하는지 확인하려면 이 옵션을 사용합니다.</p> <p>0은 소스에 가까운 트래픽, 1은 대상에 가까운 트래픽을 나타냅니다.</p> <p><code>--stage</code> 옵션을 <code>--uplink</code>, <code>--vmk</code>, <code>--switchport</code> 또는 <code>--dvfilter</code> 옵션과 함께 사용합니다.</p>

표 14-1. 패킷 캡처를 위한 pktcap-uw 인수 (계속)

인수 그룹	인수	설명
	<code>--dvfilter filter_name --capture PreDVFilter PostDVFilter</code>	vSphere Network Appliance(DVFilter)가 패킷을 가로채기 이전 또는 이후의 패킷을 캡처합니다. DVFilter 수준에서 패킷을 캡처하는 방법의 내용을 참조하십시오.
	<code>-A   --availpoints</code>	pktcap-uw 유틸리티에서 지원하는 캡처 시점을 모두 봅니다.
		pktcap-uw 유틸리티의 캡처 시점에 대한 자세한 내용은 pktcap-uw 유틸리티의 캡처 시점 항목을 참조하십시오.
<i>filter_options</i>		캡처된 패킷을 소스 또는 대상 주소, VLAN ID, VXLAN ID, 계층 3 프로토콜 및 TCP 포트에 따라 필터링합니다. 패킷 필터링을 위한 pktcap-uw 옵션의 내용을 참조하십시오.
<i>output_control_options</i>		패킷 내용을 파일에 저장하고, 일부 패킷만 캡처하고, 패킷 시작 부분에서 일부 바이트를 캡처하는 등의 작업을 수행합니다. 출력 제어를 위한 pktcap-uw 옵션의 내용을 참조하십시오.

세로 막대(|)는 대체 값을 나타내고, 세로 막대와 함께 사용되는 중괄호({})는 인수 또는 옵션의 선택 목록을 지정합니다.

## 패킷 추적을 위한 pktcap-uw 명령 구문

지연 시간 분석을 위해 ESXi 호스트의 네트워크 스택에서 패킷 경로를 확인하려면 pktcap-uw 유틸리티를 사용합니다.

### 패킷 추적을 위한 pktcap-uw 구문

pktcap-uw 유틸리티 명령에는 네트워크 스택에서 패킷을 추적하기 위한 다음과 같은 구문이 포함됩니다.

```
pktcap-uw --trace filter_options output_control_options
```

### 패킷 추적을 위한 pktcap-uw 유틸리티에 대한 옵션

pktcap-uw 유틸리티에서는 패킷 추적을 위해 유틸리티를 사용할 때 다음과 같은 옵션을 지원합니다.

표 14-2. 패킷 추적을 위한 pktcap-uw 옵션

인수	설명
<i>filter_options</i>	추적된 패킷을 소스 또는 대상 주소, VLAN ID, VXLAN ID, 계층 3 프로토콜 및 TCP 포트에 따라 필터링합니다. 패킷 필터링을 위한 pktcap-uw 옵션을 참조하십시오.
<i>output_control_options</i>	패킷의 내용을 파일에 저장하고 여러 패킷만 추적합니다. 출력 제어를 위한 pktcap-uw 옵션을 참조하십시오.

## 출력 제어를 위한 pktcap-uw 옵션

pktcap-uw 유틸리티의 출력 제어를 위한 옵션을 사용하여 패킷 내용을 파일에 저장하고 각 패킷에서 특정 바이트 수까지 캡처하고 캡처되는 패킷의 수를 제한합니다.

### 출력 제어를 위한 pktcap-uw 옵션

출력 제어를 위한 pktcap-uw 유틸리티의 옵션은 패킷을 캡처하고 추적할 때 사용할 수 있습니다. pktcap-uw 유틸리티의 명령 구문에 대한 자세한 내용은 [패킷 캡처를 위한 pktcap-uw 명령 구문](#) 및 [패킷 추적을 위한 pktcap-uw 명령 구문](#) 항목을 참조하십시오.

표 14-3. pktcap-uw 유틸리티가 지원하는 출력 제어를 위한 옵션

옵션	설명
{-o   --outfile} <i>pcap_file</i>	캡처하거나 추적한 패킷을 패킷 캡처(PCAP) 형식으로 파일에 저장합니다. 이 옵션을 사용하여 Wireshark와 같은 시각적 분석기 도구에서 패킷을 검토합니다.
-P   --ng	패킷 내용을 PCAPNG 파일 형식으로 저장합니다. 이 옵션을 -o 또는 --outfile 옵션과 함께 사용합니다.
--console	패킷 세부 정보와 내용을 콘솔 출력으로 인쇄합니다. 기본적으로 pktcap-uw 유틸리티는 콘솔 출력에 패킷 정보를 표시합니다.
{-c   --count} <i>number_of_packets</i>	처음 <i>number_of_packets</i> 개 패킷을 캡처합니다.
{-s   --snaplen} <i>snapshot_length</i>	각 패킷에서 첫 번째 <i>snapshot_length</i> 바이트만 캡처합니다. 호스트에 대한 트래픽이 많은 경우 이 옵션을 사용하여 CPU와 스토리지에 대한 로드를 줄입니다. 캡처되는 내용의 크기를 제한하려면 24 이상의 값을 설정합니다. 완전한 패킷을 캡처하려면 이 옵션을 0으로 설정합니다.
-h	pktcap-uw 유틸리티에 대한 도움말을 봅니다.

세로 막대(|)는 대체 값을 나타내고, 세로 막대와 함께 사용되는 중괄호({})는 인수 또는 옵션의 선택 목록을 지정합니다.

## 패킷 필터링을 위한 pktcap-uw 옵션

소스/대상 주소, VLAN, VXLAN 및 패킷 페이로드를 소비하는 다음 수준 프로토콜을 위한 필터링 옵션을 적용하는 pktcap-uw 유틸리티를 사용하여 모니터링하는 패킷의 범위를 좁힙니다.

### 필터 옵션

pktcap-uw의 필터 옵션은 패킷을 캡처하고 추적할 때 사용할 수 있습니다. pktcap-uw 유틸리티의 명령 구문에 대한 자세한 내용은 [패킷 캡처를 위한 pktcap-uw 명령 구문](#) 및 [패킷 추적을 위한 pktcap-uw 명령 구문](#) 항목을 참조하십시오.

표 14-4. pktcap-uw 유틸리티의 필터 옵션

옵션	설명
<code>--srcmac mac_address</code>	특정 소스 MAC 주소가 있는 패킷을 캡처하거나 추적합니다. 포함된 8진수를 콜론으로 구분합니다.
<code>--dstmac mac_address</code>	특정 대상 MAC 주소가 있는 패킷을 캡처하거나 추적합니다. 포함된 8진수를 콜론으로 구분합니다.
<code>--mac mac_address</code>	특정 소스 또는 대상 MAC 주소가 있는 패킷을 캡처하거나 추적합니다. 포함된 8진수를 콜론으로 구분합니다.
<code>--ethertype 0xEthertype</code>	패킷 페이로드를 소비하는 다음 수준 프로토콜에 따라 계층 2에서 패킷을 캡처하거나 추적합니다. <i>EtherType</i> 은 이더넷 프레임의 이더넷 유형 필드에 해당합니다. <i>EtherType</i> 은 프레임 페이로드를 소비하는 다음 수준 프로토콜의 유형을 나타냅니다. 예를 들어 LLDP(링크 계층 탐색 프로토콜) 프로토콜의 트래픽을 모니터링하려면 <code>--ethertype 0x88CC</code> 를 입력합니다.
<code>--vlan VLAN_ID</code>	VLAN에 속하는 패킷을 캡처하거나 추적합니다.
<code>--srcip IP_address IP_address/subnet_range</code>	특정 소스 IPv4 주소 또는 서브넷이 있는 패킷을 캡처하거나 추적합니다.
<code>--dstip IP_address IP_address/subnet_range</code>	특정 대상 IPv4 주소 또는 서브넷이 있는 패킷을 캡처하거나 추적합니다.
<code>--ip IP_address</code>	특정 소스 또는 대상 IPv4 주소가 있는 패킷을 캡처하거나 추적합니다.
<code>--proto 0xIP_protocol_number</code>	페이로드를 소비하는 다음 수준 프로토콜에 따라 계층 3에서 패킷을 캡처하거나 추적합니다. 예를 들어 UDP 프로토콜의 트래픽을 모니터링하려면 <code>--proto 0x11</code> 을 입력합니다.
<code>--srcport source_port</code>	해당 소스 TCP 포트에 따라 패킷을 캡처하거나 추적합니다.
<code>--dstport destination_port</code>	해당 대상 TCP 포트에 따라 패킷을 캡처하거나 추적합니다.
<code>--tcpport TCP_port</code>	해당 소스 또는 대상 TCP 포트에 따라 패킷을 캡처하거나 추적합니다.
<code>--vxlan VXLAN_ID</code>	VXLAN에 속하는 패킷을 캡처하거나 추적합니다.

표 14-4. pktcap-uw 유틸리티의 필터 옵션 (계속)

옵션	설명
<code>--rcf pcap_filter_expression</code>	<p>풍부한 공통 필터 표현식을 사용하여 패킷을 캡처하거나 추적합니다.</p> <p>예를 들어 IP 콘텐츠 길이가 1000바이트 보다 큰 모든 수신 및 송신 패킷을 캡처하려면 <code>--rcf "ip[2:2]&gt;1000"</code> 필터 식을 사용합니다.</p> <p>특정 소스 호스트 주소와 포트 번호를 선택하려면 <code>--rcf "src host 12.0.0.1 and port 5000"</code> 필터 식을 사용합니다. 이 예에서는 포트 5000을 사용하는 호스트 주소 12.0.0.1에 대한 트래픽을 필터링합니다.</p> <p><code>--rcf</code> 옵션을 사용하여 네트워크 트래픽을 필터링하는 방법에 대한 자세한 내용은 <code>tcpdump</code>와 같은 명령줄 패킷 분석기를 사용하는 pcap 필터 표현식에 대한 설명서를 참조하십시오. <a href="#">pcap-filter - 패킷 필터 구문</a>을 참조하십시오.</p> <p><b>참고</b> <code>--rcf</code> 옵션을 사용하는 경우 다음 제한 사항을 준수하십시오.</p> <ul style="list-style-type: none"> <li>■ <code>--rcf</code> 옵션을 사용하여 VLAN 패킷을 필터링하지 마십시오. VLAN 또는 VXLAN을 추적하려면 <code>pktcap-uw --vlan</code> 또는 <code>--vxlan</code> 옵션을 사용합니다.</li> <li>■ IP 브로드캐스트 주소를 필터링하지 마십시오.</li> <li>■ ENS 포트에 <code>--rcf</code>를 사용하지 마십시오.</li> </ul>
<code>--rcf-tcp-data tcp_packet_data_filter</code>	<p>풍부한 공통 필터 표현식을 사용하여 TCP 데이터 패킷을 캡처하거나 추적합니다.</p> <p>예를 들어 200 OK로 모든 HTTP/1.0 응답 패킷을 캡처하려면 <code>--rcf-tcp-data "HTTP/1.0 200 OK"</code> 필터 식을 사용합니다.</p> <p><code>index.html</code> 파일을 반환하는 HTTP GET 요청을 필터링하려면 <code>--rcf-tcp-data "GET /index.html"</code> 필터 식을 사용합니다.</p>

세로 막대(|)는 대체 값을 나타냅니다.

## pktcap-uw 유틸리티를 사용하여 패킷 캡처

가상 스위치와 물리적 어댑터, VMkernel 어댑터 및 가상 시스템 어댑터 사이의 경로에서 `pktcap-uw` 유틸리티를 통해 패킷을 캡처하여 ESXi 호스트에서의 네트워크 스택의 데이터 전송 문제를 해결할 수 있습니다.

### 물리적 어댑터에 도달하는 패킷 캡처

vSphere 표준 스위치 또는 vSphere Distributed Switch와 물리적 어댑터 간 경로의 특정 시점에서 패킷을 캡처하여 외부 네트워크와 관련된 호스트 트래픽을 모니터링합니다.

가상 스위치와 물리적 어댑터 간 데이터 경로에서 특정 캡처 시점을 지정하거나 패킷 소스 또는 대상에 대한 근접성 및 스위치와 관련한 트래픽 방향으로 캡처 시점을 결정할 수 있습니다. 지원되는 캡처 시점에 대한 자세한 내용은 `pktcap-uw` 유틸리티의 [캡처 시점](#)의 내용을 참조하십시오.



## 절차

1 (선택 사항) 호스트 어댑터 목록에서 모니터링하려는 물리적 어댑터의 이름을 찾습니다.

- vSphere Client에서, 호스트의 구성 탭으로 이동한 후 네트워킹을 확장하고 물리적 어댑터를 선택합니다.
- 호스트에 대한 ESXi Shell에서 다음 ESXCLI 명령을 실행하여 물리적 어댑터의 목록을 확인하고 해당 상태를 검토합니다.

```
esxcli network nic list
```

각 물리적 어댑터는 `vmnicX`로 표시됩니다. 여기서 `X`는 ESXi가 물리적 어댑터 포트에 할당한 번호입니다.

2 호스트에 대한 ESXi Shell에서 `pktcap-uw` 명령을 `--uplink vmnicX` 인수 및 특정 시점의 패킷을 모니터링하는 옵션과 함께 실행하고, 캡처한 패킷을 필터링하고, 결과를 파일에 저장합니다.

```
pktcap-uw --uplink vmnicX [--capture capture_point|--dir 0|1] [filter_options] [--outfile pcap_file_path [--ng]] [--count number_of_packets]
```

여기서 대괄호([])는 `pktcap-uw --uplink vmnicX` 명령의 옵션을 묶고 세로 막대(|)는 대체 값을 나타냅니다.

옵션 없이 `pktcap-uw --uplink vmnicX` 명령을 실행하는 경우에는 콘솔 출력의 표준 스위치 또는 Distributed Switch로 들어오는 패킷 내용을 전환 시점에 가져옵니다.

a `--capture` 옵션을 사용하여 다른 캡처 시점에서 패킷을 검사하거나 `--dir` 옵션을 사용하여 다른 트래픽 방향에서 패킷을 검사합니다.

pktcap-uw 명령 옵션	목표
<code>--capture UplinkSnd</code>	물리적 어댑터 디바이스로 들어가기 직전에 패킷을 모니터링합니다.
<code>--capture UplinkRcv</code>	물리적 어댑터에서 네트워크 스택에 수신된 직후에 패킷을 모니터링합니다.
<code>--dir 1</code>	가상 스위치를 떠나는 패킷을 모니터링합니다.
<code>--dir 0</code>	가상 스위치로 들어가는 패킷을 모니터링합니다.

b `filter_options`를 사용하여 소스 및 대상 주소, VLAN ID, VXLAN ID, 계층 3 프로토콜 및 TCP 포트에 따라 패킷을 필터링합니다.

예를 들어 IP 주소가 192.168.25.113인 소스 시스템에서 패킷을 모니터링하려면 `--srcip 192.168.25.113` 필터 옵션을 사용합니다.

- c 각 패킷의 콘텐츠 또는 제한된 패킷 수의 콘텐츠를 .pcap 또는 .pcapng 파일에 저장하는 옵션을 사용합니다.

- 패킷을 .pcap 파일에 저장하려면 --outfile 옵션을 사용합니다.
- 패킷을 .pcapng 파일에 저장하려면 --ng 및 --outfile 옵션을 사용합니다.

파일을 Wireshark와 같은 네트워크 분석기 도구에서 열 수 있습니다.

기본적으로 pktcap-uw 유틸리티는 패킷 파일을 ESXi 파일 시스템의 루트 폴더에 저장합니다.

- d 패킷 수만 모니터링하려면 --count 옵션을 사용합니다.

3 --count 옵션을 사용하여 패킷 수를 제한하지 않은 경우 Ctrl+C를 눌러 패킷 캡처 또는 추적을 중지합니다.

### 예제: vmnic0이 IP 주소 192.168.25.113에서 수신한 패킷 캡처

vmnic0에서 IP 주소 192.168.25.113이 할당된 소스 시스템으로부터 처음 60개 패킷을 캡처하고 vmnic0\_rcv\_srcip.pcap라는 파일에 저장하려면 다음 pktcap-uw 명령을 실행합니다.

```
pktcap-uw --uplink vmnic0 --capture UplinkRcv --srcip 192.168.25.113 --outfile
vmnic0_rcv_srcip.pcap --count 60
```

#### 다음에 수행할 작업

패킷의 콘텐츠가 파일에 저장된 경우 해당 파일을 ESXi 호스트에서 Wireshark와 같은 그래픽 분석기 도구를 실행하는 시스템으로 복사하고 해당 도구에서 열어 패킷 세부 정보를 검토합니다.

### VMXNET3 가상 시스템 어댑터에 대한 패킷을 캡처하는 방법

pktcap-uw 유틸리티를 사용하여 가상 스위치와 VMXNET3 가상 시스템 어댑터 간에 흐르는 트래픽을 모니터링합니다.

가상 스위치와 가상 시스템 어댑터 간의 데이터 경로에서 특정 캡처 시점을 지정할 수 있습니다. 또한 패킷 소스 또는 대상에 대한 근접성 및 스위치와 관련한 트래픽 방향으로 캡처 시점을 결정할 수도 있습니다. 지원되는 캡처 시점에 대한 자세한 내용은 [pktcap-uw 유틸리티의 캡처 시점의 내용](#)을 참조하십시오.

#### 사전 요구 사항

가상 시스템 어댑터의 유형이 VMXNET3인지 확인합니다.

#### 절차

- 1 호스트에서 esxtop 유틸리티를 사용하여 가상 시스템 어댑터의 포트 ID를 확인합니다.
  - a 호스트에 대한 ESXi Shell에서 esxtop을 실행하여 유틸리티를 시작합니다.
  - b 유틸리티의 네트워크 패널로 전환하려면 n을 누릅니다.
  - c 사용 대상 열에서 가상 시스템 어댑터를 찾아 포트 ID 값을 기록해 둡니다.  
사용 대상 필드에는 가상 시스템의 이름과 가상 시스템 어댑터가 연결된 포트가 포함되어 있습니다.
  - d Q를 눌러 esxtop을 종료합니다.

- 2 ESXi Shell에서 `pktcap-uw --switchport port_ID`를 실행합니다.

`port_ID`는 `esxtop` 유틸리티가 포트 ID 열에서 가상 시스템 어댑터에 대해 표시하는 ID입니다.

- 3 ESXi Shell에서 `pktcap-uw` 명령을 `--switchport port_ID` 인수 및 특정 시점의 패킷을 모니터링하고, 캡처한 패킷을 필터링하고, 결과를 파일에 저장하는 옵션과 함께 실행합니다.

```
pktcap-uw --switchport port_ID [--capture capture_point|--dir 0|1 --stage 0|1]
[filter_options] [--outfile pcap_file_path [--ng]] [--count number_of_packets]
```

여기서 대괄호([])는 `pktcap-uw --switchport port_ID` 명령의 옵션을 묶고 세로 막대(|)는 대체 값을 나타냅니다.

옵션 없이 `pktcap-uw --switchport port_ID` 명령을 실행하는 경우에는 콘솔 출력의 표준 스위치 또는 분산 스위치로 들어오는 패킷 내용을 전환 시점에 가져옵니다.

- a 게스트 운영 체제와 가상 스위치 사이의 경로에 있는 다른 캡처 시점이나 방향에서 패킷을 확인하려면 `--capture` 옵션을 사용하거나 `--dir` 옵션과 `--stage` 옵션의 값을 결합합니다.

pktcap-uw 명령 옵션	목표
<code>--capture VnicTx</code>	가상 시스템에서 스위치로 전달되는 패킷을 모니터링합니다.
<code>--capture VnicRx</code>	가상 시스템에 도착하는 패킷을 모니터링합니다.
<code>--dir 1 --stage 0</code>	가상 스위치를 떠난 직후에 패킷을 모니터링합니다.
<code>--dir 1</code>	가상 시스템으로 들어가기 직전에 패킷을 모니터링합니다.
<code>--dir 0 --stage 1</code>	가상 스위치로 들어간 직후에 패킷을 모니터링합니다.

- b `filter_options`를 사용하여 소스 및 대상 주소, VLAN ID, VXLAN ID, 계층 3 프로토콜 및 TCP 포트에 따라 패킷을 필터링합니다.

예를 들어 IP 주소가 192.168.25.113인 소스 시스템에서 패킷을 모니터링하려면 `--srcip 192.168.25.113` 필터 옵션을 사용합니다.

- c 각 패킷의 콘텐츠 또는 제한된 패킷 수의 콘텐츠를 `.pcap` 또는 `.pcapng` 파일에 저장하는 옵션을 사용합니다.

- 패킷을 `.pcap` 파일에 저장하려면 `--outfile` 옵션을 사용합니다.
- 패킷을 `.pcapng` 파일에 저장하려면 `--ng` 및 `--outfile` 옵션을 사용합니다.

파일을 Wireshark와 같은 네트워크 분석기 도구에서 열 수 있습니다.

기본적으로 `pktcap-uw` 유틸리티는 패킷 파일을 ESXi 파일 시스템의 루트 폴더에 저장합니다.

- d 패킷 수만 모니터링하려면 `--count` 옵션을 사용합니다.

- 4 `--count` 옵션을 사용하여 패킷 수를 제한하지 않은 경우 Ctrl+C를 눌러 패킷 캡처 또는 추적을 중지합니다.

## 예제: 가상 시스템이 IP 주소 192.168.25.113에서 수신한 패킷 캡처

포트 ID가 33554481인 가상 시스템 어댑터에 도착할 때 IP 주소 192.168.25.113이 할당된 소스에서 처음 60개 패킷을 캡처한 후 `vmxnet3_rcv_srcip.pcap`라고 하는 파일에 저장하려면 다음 `pktcap-uw` 명령을 실행합니다.

```
pktcap-uw --switchport 33554481 --capture VnicRx --srcip 192.168.25.113 --outfile
vmxnet3_rcv_srcip.pcap --count 60
```

### 다음에 수행할 작업

패킷의 콘텐츠가 파일에 저장된 경우 해당 파일을 ESXi 호스트에서 Wireshark와 같은 그래픽 분석기 도구를 실행하는 시스템으로 복사하고 해당 도구에서 열어 패킷 세부 정보를 검토합니다.

## VMkernel 어댑터에 대한 패킷을 캡처하는 방법

`pktcap-uw` 유틸리티를 사용하여 VMkernel 어댑터와 가상 스위치 간에 교환되는 패킷을 모니터링합니다.

가상 스위치와 VMkernel 어댑터 간 흐름의 특정 캡처 시점에서 패킷을 캡처할 수 있습니다. 또한 패킷 소스 또는 대상에 대한 근접성 및 스위치와 관련한 트래픽 방향으로 캡처 시점을 결정할 수도 있습니다. 지원되는 캡처 시점에 대한 자세한 내용은 [pktcap-uw 유틸리티의 캡처 시점](#)의 내용을 참조하십시오.

### 절차

- (선택 사항) VMkernel 어댑터 목록에서 모니터링하려는 VMkernel 어댑터의 이름을 찾습니다.
  - vSphere Web Client에서 호스트에 대한 구성 탭의 네트워킹을 확장하여 **VMkernel 어댑터**를 선택합니다.
  - 호스트에 대한 ESXi Shell에서 다음 콘솔 명령을 실행하여 물리적 어댑터의 목록을 확인합니다.

```
esxcli network ip interface list
```

각 VMkernel 어댑터는 `vmkX`로 표시됩니다. 여기서 `X`는 ESXi가 어댑터에 할당한 시퀀스 번호입니다.

- 호스트에 대한 ESXi Shell에서 `pktcap-uw` 명령을 `--vmk vmkX` 인수 및 특정 시점의 패킷을 모니터링하는 옵션과 함께 실행하고, 캡처한 패킷을 필터링하고, 결과를 파일에 저장합니다.

```
pktcap-uw --vmk vmkX [--capture capture_point|--dir 0|1 --stage 0|1] [filter_options]
[--outfile pcap_file_path [--ng]] [--count number_of_packets]
```

여기서 대괄호([])는 `pktcap-uw --vmk vmkX` 명령의 옵션을 묶고 세로 막대(|)는 대체 값을 나타냅니다.

`--vmk vmkX` 옵션을 `--switchport vmkernel_adapter_port_ID`로 바꿀 수 있습니다. 여기서 `vmkernel_adapter_port_ID`는 `esxtop` 유틸리티의 네트워크 패널이 어댑터에 대해 표시하는 포트 ID 값입니다.

옵션 없이 `pktcap-uw --vmk vmkX` 명령을 실행하는 경우에는 VMkernel 어댑터를 떠나는 패킷의 내용을 가져옵니다.

- a 특정 위치 및 방향에서 전송되거나 수신된 패킷을 확인하려면 `--capture` 옵션을 사용하거나 `--dir`과 `--stage` 옵션의 값을 결합합니다.

<b>pktcap-uw 명령 옵션</b>	<b>목표</b>
<code>--dir 1 --stage 0</code>	가상 스위치를 떠난 직후에 패킷을 모니터링합니다.
<code>--dir 1</code>	VMkernel 어댑터로 들어가기 직전에 패킷을 모니터링합니다.
<code>--dir 0 --stage 1</code>	가상 스위치로 들어가기 직전에 패킷을 모니터링합니다.

- b `filter_options`를 사용하여 소스 및 대상 주소, VLAN ID, VXLAN ID, 계층 3 프로토콜 및 TCP 포트에 따라 패킷을 필터링합니다.

예를 들어 IP 주소가 192.168.25.113인 소스 시스템에서 패킷을 모니터링하려면 `--srcip 192.168.25.113` 필터 옵션을 사용합니다.

- c 각 패킷의 콘텐츠 또는 제한된 패킷 수의 콘텐츠를 `.pcap` 또는 `.pcapng` 파일에 저장하는 옵션을 사용합니다.

- 패킷을 `.pcap` 파일에 저장하려면 `--outfile` 옵션을 사용합니다.
- 패킷을 `.pcapng` 파일에 저장하려면 `--ng` 및 `--outfile` 옵션을 사용합니다.

파일을 Wireshark와 같은 네트워크 분석기 도구에서 열 수 있습니다.

기본적으로 `pktcap-uw` 유틸리티는 패킷 파일을 ESXi 파일 시스템의 루트 폴더에 저장합니다.

- d 패킷 수만 모니터링하려면 `--count` 옵션을 사용합니다.

3 `--count` 옵션을 사용하여 패킷 수를 제한하지 않은 경우 Ctrl+C를 눌러 패킷 캡처 또는 추적을 중지합니다.

#### 다음에 수행할 작업

패킷의 콘텐츠가 파일에 저장된 경우 해당 파일을 ESXi 호스트에서 Wireshark와 같은 그래픽 분석기 도구를 실행하는 시스템으로 복사하고 해당 도구에서 열어 패킷 세부 정보를 검토합니다.

### 손실된 패킷을 캡처하는 방법

`pktcap-uw` 유틸리티를 통해 손실된 패킷을 캡처하여 연결 손실 문제를 해결합니다.

방화벽 규칙, IOChain 및 DVfilter에서의 필터링, VLAN 불일치, 물리적 어댑터 오작동, 체크섬 오류 등의 많은 이유로 인해 패킷이 네트워크 스트림의 어느 시점에서 손실될 수 있습니다. `pktcap-uw` 유틸리티를 사용하면 패킷이 손실된 위치와 손실 이유를 확인할 수 있습니다.

## 절차

- 1 호스트에 대한 ESXi Shell에서 `pktcap-uw --capture Drop` 명령을 특정 시점의 패킷을 모니터링하는 옵션과 함께 실행하고, 캡처한 패킷을 필터링하고, 결과를 파일에 저장합니다.

```
pktcap-uw --capture Drop [filter_options] [--outfile pcap_file_path [--ng]] [--count
number_of_packets]
```

여기서 대괄호([])는 `pktcap-uw --capture Drop` 명령의 옵션을 묶고 세로 막대(|)는 대체 값을 나타냅니다.

- a `filter_options`를 사용하여 소스 및 대상 주소, VLAN ID, VXLAN ID, 계층 3 프로토콜 및 TCP 포트에 따라 패킷을 필터링합니다.

예를 들어 IP 주소가 192.168.25.113인 소스 시스템에서 패킷을 모니터링하려면 `--srcip 192.168.25.113` 필터 옵션을 사용합니다.

- b 각 패킷의 콘텐츠 또는 제한된 패킷 수의 콘텐츠를 `.pcap` 또는 `.pcapng` 파일에 저장하는 옵션을 사용합니다.

- 패킷을 `.pcap` 파일에 저장하려면 `--outfile` 옵션을 사용합니다.

- 패킷을 `.pcapng` 파일에 저장하려면 `--ng` 및 `--outfile` 옵션을 사용합니다.

파일을 Wireshark와 같은 네트워크 분석기 도구에서 열 수 있습니다.

기본적으로 `pktcap-uw` 유틸리티는 패킷 파일을 ESXi 파일 시스템의 루트 폴더에 저장합니다.

---

**참고** 패킷을 콘솔 출력으로 캡처한 경우에만 패킷이 손실된 이유와 위치를 확인할 수 있습니다.

`pktcap-uw` 유틸리티는 패킷 내용만 `.pcap` 또는 `.pcapng` 파일에 저장합니다.

---

- c 패킷 수만 모니터링하려면 `--count` 옵션을 사용합니다.

- 2 `--count` 옵션을 사용하여 패킷 수를 제한하지 않은 경우 Ctrl+C를 눌러 패킷 캡처 또는 추적을 중지합니다.

## 결과

손실된 패킷 내용 이외에도 `pktcap-uw` 유틸리티 출력에는 손실 이유와 패킷을 마지막으로 처리한 네트워크 스택의 함수가 표시됩니다.

### 다음에 수행할 작업

패킷의 콘텐츠가 파일에 저장된 경우 해당 파일을 ESXi 호스트에서 Wireshark와 같은 그래픽 분석기 도구를 실행하는 시스템으로 복사하고 해당 도구에서 열어 패킷 세부 정보를 검토합니다.

## DVFilter 수준에서 패킷을 캡처하는 방법

패킷이 vSphere Network Appliance(DVFilter)를 통과할 때 패킷이 어떻게 변하는지 검토합니다.

DVFilter는 가상 시스템 어댑터와 가상 스위치 간의 스트림에 상주하는 에이전트입니다. 패킷을 가로채어 보안 공격 및 원하지 않는 트래픽으로부터 가상 시스템을 보호합니다.

## 절차

- 1 (선택 사항) 모니터링할 DVFilter 이름을 찾으려면 ESXi Shell에서 `summarize-dvfilter` 명령을 실행합니다.

명령 출력에는 호스트에 배포된 DVFilter의 빠른 경로 에이전트와 느린 경로 에이전트가 포함되어 있습니다.

- 2 `pktcap-uw` 유틸리티를 `--dvfilter dvfilter_name` 인수 및 특정 시점의 패킷을 모니터링하는 옵션과 함께 실행하고, 캡처한 패킷을 필터링하고, 결과를 파일에 저장합니다.

```
pktcap-uw --dvFilter dvfilter_name --capture PreDVFilter|PostDVFilter [filter_options]
[--outfile pcap_file_path [--ng]] [--count number_of_packets]
```

여기서 대괄호([])는 `pktcap-uw --dvFilter vmnicX` 명령의 옵션 항목을 묶고 세로 막대(|)는 대체 값을 나타냅니다.

- a DVFilter가 패킷을 가로채기 이전 및 이후의 패킷을 모니터링하려면 `--capture` 옵션을 사용합니다.

pktcap-uw 명령 옵션	목표
<code>--capture PreDVFilter</code>	패킷이 DVFilter에 들어가기 이전에 패킷을 캡처합니다.
<code>--capture PostDVFilter</code>	패킷이 DVFilter를 나간 이후에 패킷을 캡처합니다.

- b `filter_options`를 사용하여 소스 및 대상 주소, VLAN ID, VXLAN ID, 계층 3 프로토콜 및 TCP 포트에 따라 패킷을 필터링합니다.

예를 들어 IP 주소가 192.168.25.113인 소스 시스템에서 패킷을 모니터링하려면 `--srcip 192.168.25.113` 필터 옵션을 사용합니다.

- c 각 패킷의 콘텐츠 또는 제한된 패킷 수의 콘텐츠를 `.pcap` 또는 `.pcapng` 파일에 저장하는 옵션을 사용합니다.

- 패킷을 `.pcap` 파일에 저장하려면 `--outfile` 옵션을 사용합니다.
- 패킷을 `.pcapng` 파일에 저장하려면 `--ng` 및 `--outfile` 옵션을 사용합니다.

파일을 Wireshark와 같은 네트워크 분석기 도구에서 열 수 있습니다.

기본적으로 `pktcap-uw` 유틸리티는 패킷 파일을 ESXi 파일 시스템의 루트 폴더에 저장합니다.

- d 패킷 수만 모니터링하려면 `--count` 옵션을 사용합니다.

- 3 `--count` 옵션을 사용하여 패킷 수를 제한하지 않은 경우 Ctrl+C를 눌러 패킷 캡처 또는 추적을 중지합니다.

## 다음에 수행할 작업

패킷의 콘텐츠가 파일에 저장된 경우 해당 파일을 ESXi 호스트에서 Wireshark와 같은 그래픽 분석기 도구를 실행하는 시스템으로 복사하고 해당 도구에서 열어 패킷 세부 정보를 검토합니다.

## pktcap-uw 유틸리티의 캡처 시점을 사용하는 방법

함수가 호스트의 네트워크 스택의 특정 위치에서 패킷을 처리할 때 `pktcap-uw` 유틸리티의 캡처 시점을 사용하여 해당 패킷을 모니터링하는 방법을 알아봅니다.

## 캡처 시점 개요

`pktcap-uw` 유틸리티의 캡처 시점은 한쪽의 가상 스위치와 다른 쪽의 물리적 어댑터, VMkernel 어댑터 또는 가상 시스템 어댑터 간의 경로에 있는 위치를 나타냅니다.

특정 캡처 시점을 어댑터 옵션과 결합해 사용할 수 있습니다. 예를 들어 업링크 트래픽을 캡처할 때 `UplinkRcv` 지점을 사용합니다. 다른 포인트를 독립형으로 해결할 수 있습니다. 예를 들어 모든 손실된 패킷을 검사하려면 `Drop` 시점을 사용할 수 있습니다.

**참고** `pktcap-uw` 유틸리티의 특정 캡처 시점은 VMware 내부용으로 설계되었으며 VMware 기술 지원의 감독 하에서만 사용해야 합니다. 이러한 캡처 시점은 "vSphere 네트워킹" 가이드에서 설명하지 않습니다.

## pktcap-uw 유틸리티에서 캡처 시점을 사용하기 위한 옵션

캡처 시점에서 패킷 상태 또는 내용을 검토하려면 `--capture capture_point` 옵션을 `pktcap-uw` 유틸리티에 추가합니다.

## 캡처 시점 자동 선택

물리적, VMkernel 또는 VMXNET3 어댑터와 관련된 트래픽의 경우 `--dir` 옵션과 `--stage` 옵션을 결합하여 캡처 시점을 자동으로 선택하고 전환하여 패킷이 시점 전후에 어떻게 변화하는지 검토할 수 있습니다.

## pktcap-uw 유틸리티의 캡처 시점

`pktcap-uw` 유틸리티는 업링크, VMkernel 또는 가상 시스템 트래픽을 모니터링할 때만 사용할 수 있는 캡처 시점을 지원하고, 어댑터 유형과 관련되지 않은 스택 내의 특수 위치를 표시하는 캡처 시점을 지원합니다.

### 물리적 어댑터 트래픽과 관련된 캡처 시점

`pktcap-uw --uplink vmnicX` 명령은 물리적 어댑터와 가상 스위치 사이의 경로에 있는 특정 위치 및 방향의 트래픽을 처리하는 함수에 대해 캡처 시점을 지원합니다.

캡처 시점	설명
UplinkRcv	물리적 어댑터로부터 패킷을 수신하는 함수입니다.
UplinkSnd	물리적 어댑터로 패킷을 전송하는 함수입니다.
PortInput	UplinkRcv에서 가상 스위치의 포트에 패킷 목록을 전달하는 함수입니다.
PortOutput	가상 스위치의 포트에서 UplinkSnd 시점으로 패킷 목록을 전달하는 함수입니다.

### 가상 시스템 트래픽과 관련된 캡처 시점

`pktcap-uw --switchport vmxnet3_port_ID` 명령은 VMXNET3 어댑터와 가상 스위치 사이의 경로에 있는 특정 위치 및 방향의 트래픽 패킷을 처리하는 함수에 대해 캡처 시점을 지원합니다.

캡처 시점	설명
VnicRx	가상 스위치로부터 패킷을 수신하는 가상 시스템 NIC 백엔드의 함수입니다.
VnicTx	가상 시스템에서 가상 스위치로 패킷을 전송하는 가상 시스템 NIC 백엔드의 함수입니다.



캡처 시점	설명
PortOutput	가상 스위치의 포트에서 Vmxnet3Rx로 패킷 목록을 전달하는 함수입니다.
PortInput	Vmxnet3Tx에서 가상 스위치의 포트로 패킷 목록을 전달하는 함수입니다. VMXNET3 어댑터와 관련된 트래픽의 기본 캡처 시점입니다.

### VMkernel 어댑터 트래픽과 관련된 캡처 시점

`pktcap-uw --vmk vmkX` 명령 및 `pktcap-uw --switchport vmkernel_adapter_port_ID` 명령은 VMkernel 어댑터와 가상 스위치 사이의 경로에 있는 특정 위치 및 방향의 함수를 나타내는 캡처 시점을 지원합니다.

캡처 시점	설명
PortOutput	가상 스위치의 포트에서 VMkernel 어댑터로 패킷 목록을 전달하는 함수입니다.
PortInput	VMkernel 어댑터에서 가상 스위치의 포트로 패킷 목록을 전달하는 함수입니다. VMkernel 어댑터와 관련된 트래픽의 기본 캡처 시점입니다.

### 분산 가상 필터와 관련된 캡처 시점

`pktcap-uw --dvfilter divfilter_name` 명령에는 패킷이 DVFilter로 들어올 때 또는 DVFilter를 나갈 때 패킷을 캡처할지 여부를 나타내는 캡처 시점이 필요합니다.

캡처 시점	설명
PreDVFilter	DVFilter가 패킷을 가로채기 이전의 시점입니다.
PostDVFilter	DVFilter가 패킷을 가로채기 이후의 시점입니다.

### 독립형 캡처 시점

특정 캡처 시점은 물리적, VMkernel 또는 VMXNET3 어댑터가 아니라 네트워크 스택에 직접 매핑됩니다.

캡처 시점	설명
삭제	손실된 패킷을 캡처하고 손실이 일어난 위치를 보여줍니다.
TcpipDispatch	가상 스위치에서 VMkernel의 TCP/IP 스택으로, 또한 그 반대로 트래픽을 디스패치하는 함수에서 패킷을 캡처합니다.
PktFree	패킷이 해제되기 직전에 패킷을 캡처합니다.
VdrRxLeaf	VMware NSX에 있는 동적 라우터의 수신 리프 I/O 체인에서 패킷을 캡처합니다. 이 캡처 시점은 <code>--lifID</code> 옵션과 함께 사용합니다.
VdrRxTerminal	VMware NSX에 있는 동적 라우터의 수신 터미널 I/O 체인에서 패킷을 캡처합니다. 이 캡처 시점은 <code>--lifID</code> 옵션과 함께 사용합니다.
VdrTxLeaf	VMware NSX에 있는 동적 라우터의 전송 리프 I/O 체인에서 패킷을 캡처합니다. 이 캡처 시점은 <code>--lifID</code> 옵션과 함께 사용합니다.
VdrTxTerminal	VMware NSX에 있는 동적 라우터의 전송 터미널 I/O 체인에서 패킷을 캡처합니다. 이 캡처 시점은 <code>--lifID</code> 옵션과 함께 사용합니다.

동적 라우터에 대한 자세한 내용은 "VMware NSX" 설명서를 참조하십시오.

## pktcap-uw 유틸리티의 캡처 시점을 나열하는 방법

pktcap-uw 유틸리티의 모든 캡처 시점을 확인하여 ESXi 호스트의 네트워크 스택에 있는 특정 위치에서 트래픽을 모니터링하기 위한 캡처 시점의 이름을 찾습니다.

pktcap-uw 유틸리티의 캡처 시점에 대한 자세한 내용은 [pktcap-uw 유틸리티의 캡처 시점 항목](#)을 참조하십시오.

### 절차

- ◆ 호스트에 대한 ESXi Shell에서 `pktcap-uw -A` 명령을 실행하여 pktcap-uw 유틸리티에서 지원하는 모든 캡처 시점을 봅니다.

## pktcap-uw 유틸리티를 사용하여 패킷을 추적하는 방법

지연 시간을 분석하고 패킷이 손상 또는 손실된 시점의 위치를 찾기 위해 네트워크 스택 내에서 패킷이 이동한 경로를 추적하려면 pktcap-uw 유틸리티를 사용합니다.

pktcap-uw 유틸리티는 패킷의 경로와 더불어 패킷이 ESXi의 네트워킹 함수에 의해 처리된 시간을 표시하는 타임스탬프를 보여줍니다. 또한 패킷이 스택에서 해제되기 직전에 패킷 경로를 보고합니다.

패킷의 전체 경로 정보를 보려면 pktcap-uw 유틸리티의 결과를 콘솔 출력에 인쇄하거나 PCAPNG 파일에 저장해야 합니다.

### 절차

- 1 호스트에 대한 ESXi Shell에서 `pktcap-uw --trace` 명령을 추적된 패킷을 필터링하는 옵션과 함께 실행하고, 결과를 파일에 저장하고, 추적된 패킷 수를 제한합니다.

```
pktcap-uw --trace [filter_options] [--outfile pcap_file_path [--ng]] [--count
number_of_packets]
```

여기서 대괄호([])는 `pktcap-uw --trace` 명령의 옵션 항목을 묶고 세로 막대(|)는 대체 값을 나타냅니다.

- a `filter_options`를 사용하여 소스 및 대상 주소, VLAN ID, VXLAN ID, 계층 3 프로토콜 및 TCP 포트에 따라 패킷을 필터링합니다.

예를 들어 IP 주소가 192.168.25.113인 소스 시스템에서 패킷을 모니터링하려면 `--srcip 192.168.25.113` 필터 옵션을 사용합니다.

- b 각 패킷의 콘텐츠 또는 제한된 패킷 수의 콘텐츠를 `.pcap` 또는 `.pcapng` 파일에 저장하는 옵션을 사용합니다.

- 패킷을 `.pcap` 파일에 저장하려면 `--outfile` 옵션을 사용합니다.
- 패킷을 `.pcapng` 파일에 저장하려면 `--ng` 및 `--outfile` 옵션을 사용합니다.

파일을 Wireshark와 같은 네트워크 분석기 도구에서 열 수 있습니다.

기본적으로 `pktcap-uw` 유틸리티는 패킷 파일을 ESXi 파일 시스템의 루트 폴더에 저장합니다.

---

**참고** `.pcap` 파일에는 추적된 패킷의 내용만 들어 있습니다. 패킷 내용 외에 패킷 경로를 수집하려면 출력을 `.pcapng` 파일에 저장합니다.

---

- c 패킷 수만 모니터링하려면 `--count` 옵션을 사용합니다.

- 2 `--count` 옵션을 사용하여 패킷 수를 제한하지 않은 경우 Ctrl+C를 눌러 패킷 캡처 또는 추적을 중지합니다.

#### 다음에 수행할 작업

패킷의 콘텐츠가 파일에 저장된 경우 해당 파일을 ESXi 호스트에서 Wireshark와 같은 그래픽 분석기 도구를 실행하는 시스템으로 복사하고 해당 도구에서 열어 패킷 세부 정보를 검토합니다.

## vSphere Distributed Switch의 NetFlow 설정 구성

보고서를 NetFlow 수집기로 보내 vSphere Distributed Switch를 통과하는 가상 시스템 IP 트래픽을 분석합니다.

vSphere Distributed Switch는 IPFIX(NetFlow 버전 10)를 지원합니다.

---

**참고** DPU의 ESXi가 지원하는 vSphere Distributed Switch에서 IPFIX를 구성하려면 ops TCP/IP 스택에 `vmknic`를 생성해야 합니다. 그렇지 않으면 흐름 정보가 수집기로 내보내지지 않습니다.

---

#### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **작업** 메뉴에서 **설정 > NetFlow 편집**을 선택합니다.
- 3 NetFlow 수집기의 **수집기 IP 주소**와 **수집기 포트**를 입력합니다.  
IPv4 또는 IPv6 주소로 NetFlow 수집기에 연결할 수 있습니다.
- 4 스위치 관련 정보를 식별하는 **관찰 도메인 ID**를 설정합니다.

- 5 스위치에 있는 각 호스트의 개별 디바이스 대신 단일 네트워크 디바이스 아래에서 NetFlow 수집기의 Distributed Switch 정보를 보려면 **스위치 IP 주소** 텍스트 상자에 IPv4 주소를 입력합니다.
- 6 (선택 사항) **활성화된 흐름 내보내기 시간 초과** 및 **유휴 흐름 내보내기 시간 초과** 텍스트 상자에서 흐름 시작 후 정보를 보낼 때까지 대기할 시간(초)을 설정합니다.
- 7 (선택 사항) 스위치에서 수집하는 데이터 부분을 변경하려면 **샘플링 속도**를 구성합니다.  
 샘플링 속도는 NetFlow에서 수집된 패킷 이후마다 삭제하는 패킷 수를 나타냅니다. 샘플링 속도가  $x$ 이면 NetFlow가 패킷을 수집된 패킷:손실된 패킷 비율을 1: $x$ 로 삭제하도록 지정됩니다. 이 비율이 0이면 NetFlow가 모든 패킷을 샘플링합니다. 즉, 한 패킷을 수집한 후 패킷을 삭제하지 않습니다. 이 비율이 1인 경우에는 NetFlow가 한 패킷을 샘플링하면 다음 패킷을 삭제하는 방식으로 지정됩니다.
- 8 (선택 사항) 같은 호스트에 있는 가상 시스템 간 네트워크 작업에 대한 데이터만 수집하려면 **내부 흐름만 처리**를 사용하도록 설정합니다.  
 Distributed Switch 및 물리적 네트워크 디바이스에서 중복된 정보가 전송되지 않도록 물리적 네트워크에서 NetFlow를 사용하도록 설정하면 내부 흐름만 수집합니다.
- 9 **확인**을 클릭합니다.

#### 다음에 수행할 작업

분산 포트 그룹 또는 포트에 연결된 가상 시스템의 트래픽에 대해 NetFlow 보고를 사용하도록 설정합니다. [분산 포트 그룹 또는 분산 포트에서 NetFlow 모니터링 관리](#)의 내용을 참조하십시오.

## 포트 미러링이란?

포트 미러링을 사용하면 분산 포트의 트래픽을 다른 분산 포트나 특정 물리적 스위치 포트에 미러링할 수 있습니다.

포트 미러링은 스위치에서 한 스위치 포트(또는 전체 VLAN)에 표시된 패킷의 복사본을 다른 스위치 포트의 모니터링 연결로 보내는 데 사용됩니다. 포트 미러링은 데이터를 분석 및 디버그하거나 네트워크의 오류를 진단하는 데 사용됩니다.

## 포트 미러링 상호 운용성이란?

다른 vSphere 기능과 함께 vSphere 포트 미러링을 사용하는 경우 몇 가지 상호 운용성 문제를 고려해야 합니다.

### vMotion

선택한 vSphere 포트 미러링 세션 유형에 따라 vMotion 기능이 달라집니다. vMotion을 실행하는 동안 미러링 경로가 일시적으로 무효화될 수 있지만 vMotion이 완료되면 복원됩니다.

표 14-5. 포트 미러링 시 vMotion 상호 운용성

포트 미러링 세션 유형	소스 및 대상	vMotion과 상호 운용 가능	기능
분산 포트 미러링	비업링크 분산 포트 소스 및 대상	예	분산 포트 간의 포트 미러링은 로컬에서만 가능합니다. vMotion으로 인해 소스와 대상이 서로 다른 호스트에 있는 경우 소스와 대상 간의 미러링이 작동하지 않습니다. 하지만 소스와 대상이 동일한 호스트로 이동하면 포트 미러링이 작동합니다.
원격 미러링 소스	비업링크 분산 포트 소스	예	소스 분산 포트가 호스트 A에서 호스트 B로 이동하면 소스 포트에서 A의 업링크로 향하는 원래 미러링 경로가 A에서 제거되고 소스 포트에서 B의 업링크로 향하는 새 미러링 경로가 B에 생성됩니다. 사용되는 업링크는 세션에서 지정한 업링크 이름에 따라 결정됩니다.
	업링크 포트 대상	아니요	vMotion을 통해 업링크를 이동할 수는 없습니다.
원격 미러링 대상	VLAN 소스	아니요	
	비업링크 분산 포트 대상	예	대상 분산 포트가 호스트 A에서 호스트 B로 이동하면 소스 VLAN에서 대상 포트에 향하는 원래 미러링 경로가 모두 A에서 B로 이동합니다.
캡슐화된 원격 미러링(L3) 소스	비업링크 분산 포트 소스	예	소스 분산 포트가 호스트 A에서 호스트 B로 이동하면 소스 포트에서 대상 IP로 향하는 원래 미러링 경로가 모두 A에서 B로 이동합니다.
	IP 대상	아니요	
분산 포트 미러링(레거시)	IP 소스	아니요	
	비업링크 분산 포트 대상	아니요	대상 분산 포트가 호스트 A에서 호스트 B로 이동하면 포트 미러링 세션 소스가 여전히 A에서 대상을 확인하기 때문에 소스 IP에서 대상 포트에 향하는 원래 미러링 경로가 모두 무효화됩니다.

## TSO 및 LRO

TSO(TCP 세분화 오프로드) 및 LRO(대규모 수신 오프로드)로 인해 미러링 패킷 수가 미러링된 패킷 수와 달라질 수 있습니다.

vNIC에서 TSO를 사용하도록 설정한 경우 vNIC가 큰 패킷을 Distributed Switch에 전송할 수 있습니다. vNIC에서 LRO를 사용하도록 설정한 경우에는 vNIC에 전송된 작은 패킷이 큰 패킷으로 병합될 수 있습니다.

소스	대상	설명
TSO	LRO	소스 vNIC의 패킷은 큰 패킷일 수 있으며 분할 여부는 해당 패킷의 크기가 대상 vNIC LRO 제한 사항보다 큰지 여부에 따라 결정됩니다.
TSO	임의의 대상	소스 vNIC의 패킷은 큰 패킷일 수 있으며 대상 vNIC에서 표준 패킷으로 분할됩니다.
임의의 소스	LRO	소스 vNIC의 패킷은 표준 패킷이며 대상 vNIC에서 더 큰 패킷으로 병합될 수 있습니다.

## 포트 미러링 세션 생성

vSphere Client를 사용하여 포트 미러링 세션을 생성하여 vSphere Distributed Switch 트래픽을 포트, 업링크 및 원격 IP 주소에 미러링합니다.

### 사전 요구 사항

vSphere Distributed Switch의 버전이 5.0.0 이상인지 확인합니다.

### 절차

#### 1 포트 미러링 세션 유형

포트 미러링 세션을 시작하려면 포트 미러링 세션의 유형을 지정해야 합니다.

#### 2 포트 미러링 이름 및 세션 세부 정보

포트 미러링 세션 생성을 계속하려면 새 포트 미러링 세션의 이름, 설명 및 세션 세부 정보를 지정합니다.

#### 3 포트 미러링 소스

포트 미러링 세션 생성을 계속하려면 새 포트 미러링 세션의 소스 및 트래픽 방향을 선택합니다.

#### 4 포트 미러링 대상

포트 미러링 세션 생성 절차를 완료하려면 포트 또는 업링크를 포트 미러링 세션의 대상으로 선택합니다.

## 포트 미러링 세션 유형

포트 미러링 세션을 시작하려면 포트 미러링 세션의 유형을 지정해야 합니다.

### 절차

1 vSphere Client 탐색기에서 Distributed Switch를 찾습니다.

2 구성 탭을 클릭하고 설정을 확장합니다.

3 포트 미러링 옵션을 선택하고 새로 만들기를 클릭합니다.

#### 4 포트 미러링 세션의 세션 유형을 선택합니다.

옵션	설명
분산 포트 미러링	여러 분산 포트의 패킷을 동일한 호스트의 다른 분산 포트에 미러링합니다. 소스와 대상이 서로 다른 호스트에 있는 경우 이 세션 유형은 작동하지 않습니다.
원격 미러링 소스	여러 분산 포트의 패킷을 해당 호스트의 특정 업링크 포트에 미러링합니다.
원격 미러링 대상	여러 VLAN의 패킷을 분산 포트에 미러링합니다.
캡슐화된 원격 미러링(L3) 소스	여러 분산 포트의 패킷을 원격 에이전트의 IP 주소로 미러링합니다. 가상 시스템의 트래픽이 IP 터널을 통해 물리적 또는 가상 대상으로 미러링됩니다.

#### 5 다음을 클릭합니다.

### 포트 미러링 이름 및 세션 세부 정보

포트 미러링 세션 생성을 계속하려면 새 포트 미러링 세션의 이름, 설명 및 세션 세부 정보를 지정합니다.

#### 절차

- 1 세션 속성을 설정합니다. 선택한 세션 유형에 따라 구성에 서로 다른 옵션을 사용할 수 있습니다.

옵션	설명
이름	포트 미러링 세션에 대한 고유한 이름을 입력하거나 자동으로 생성된 세션 이름을 수락할 수 있습니다.
상태	드롭다운 메뉴를 사용하여 세션을 사용하거나 사용하지 않도록 설정합니다.
세션 유형	선택한 세션 유형을 표시합니다.
캡슐화 유형	GRE, ERSPAN 2 또는 ERSPAN 3을 선택합니다. <b>참고</b> 이 옵션은 세션 유형이 <b>캡슐화된 원격 미러링(L3) 소스</b> 로 설정된 경우에 사용하도록 설정됩니다.
세션 ID	캡슐화 유형이 ERSPAN 2 또는 ERSPAN 3으로 설정되면 ERSPAN ID를 지정합니다. <b>참고</b> 이 옵션은 세션 유형이 <b>캡슐화된 원격 미러링(L3) 소스</b> 로 설정된 경우에 사용하도록 설정됩니다.
캡슐화 VLAN ID	대상 포트에서 모든 프레임에 캡슐화하는 VLAN ID입니다. <b>참고</b> 원래 프레임에 VLAN이 있고 원래 VLAN 유지가 선택되어 있지 않은 경우 캡슐화 VLAN이 원래 VLAN을 대체합니다. 이 옵션은 세션 유형이 <b>원격 미러링 소스</b> 로 설정된 경우에 사용하도록 설정됩니다.
원래 VLAN 유지	미러링된 프레임이 이중 캡슐화되도록 내부 태그에 원래 VLAN을 보관하려면 [원래 VLAN 유지]를 선택합니다. 이 옵션은 세션 유형이 <b>원격 미러링 소스</b> 로 설정된 경우에 사용하도록 설정됩니다.
대상 포트의 일반 I/O	드롭다운 메뉴를 사용하여 대상 포트의 일반 I/O를 허용하거나 허용하지 않습니다. 이 속성은 업링크 및 분산 포트 대상에만 사용할 수 있습니다. 이 옵션을 허용하지 않으면 송신 대상 포트에서 미러링된 트래픽은 허용되지만 수신 트래픽은 허용되지 않습니다.

옵션	설명
TCP/IP 스택	<p>드롭다운 메뉴를 사용하여 TCP/IP 스택 유형을 선택합니다.</p> <ul style="list-style-type: none"> <li>■ 기본값: 기본 TCP/IP 스택입니다.</li> <li>■ 미러: 기본 TCP/IP Netstack 대신 미러 스택을 사용하면 미러 트래픽을 관리 트래픽과 분리할 수 있습니다. 미러 스택이 없으면 미러 트래픽은 기본 TCP/IP 스택에 바인딩됩니다. 관리 트래픽은 기본 TCP/IP 스택도 사용합니다. 미러 트래픽이 크면 관리 트래픽에 영향을 미칩니다. 미러 트래픽을 기본 TCP/IP 스택에서 분리하려는 경우 ESXi에 전용 미러 Netstack을 사용할 수 있습니다. 캡슐화된 원격 미러링 세션을 구성하는 동안 전용 Netstack을 사용하도록 설정할 수 있습니다.</li> </ul> <p><b>참고</b> DPU에서 ESXi가 지원하는 vSphere Distributed Switch에서 ERSPAN을 구성하려면 미러 TCP/IP 스택에 vmknic를 생성합니다.</p> <p><b>참고</b> 이 옵션은 세션 유형이 <b>캡슐화된 원격 미러링(L3) 소스</b>로 설정된 경우에 사용하도록 설정됩니다.</p>
미러링된 패킷 길이(바이트)	<p>이 확인란을 사용하여 미러링된 패킷 길이(바이트)를 사용하도록 설정합니다. 이 경우 미러링된 프레임의 크기가 제한됩니다. 이 옵션을 선택하면 미러링된 모든 프레임이 지정된 길이로 잘립니다.</p>
샘플링 속도	<p>패킷이 샘플링되는 속도를 선택합니다. 레거시 세션을 제외한 모든 포트 미러링 세션에 대해 기본적으로 사용하도록 설정됩니다.</p> <p><b>참고</b> NSX 전송 노드 및 ENS(고급 네트워크 스택)를 사용하도록 설정한 경우 샘플링 속도가 사용되도록 설정되지 않습니다.</p>
설명	<p>포트 미러링 세션 구성의 설명을 입력할 수 있습니다.</p>

## 2 다음을 클릭합니다.

### 포트 미러링 소스

포트 미러링 세션 생성을 계속하려면 새 포트 미러링 세션의 소스 및 트래픽 방향을 선택합니다.

소스 및 대상을 설정하지 않고 포트 미러링 세션을 생성할 수 있습니다. 소스와 대상을 설정하지 않으면 포트 미러링 세션이 미러링 경로 없이 생성됩니다. 따라서 올바른 속성이 설정된 포트 미러링 세션을 생성할 수 있습니다. 속성을 설정했으면 포트 미러링 세션을 편집하여 소스 및 대상 정보를 추가할 수 있습니다.

**참고** 포트 미러링 소스를 선택할 때는 다음과 같은 제한 사항을 고려하십시오.

- 소스 미러 포트는 둘 이상의 미러 세션에서 사용할 수 없습니다.
- 포트는 동시에 동일하거나 다른 미러 세션에서 미러 소스 및 미러 대상으로 사용될 수 없습니다.



## 절차

### 1 미러링할 트래픽의 소스와 트래픽 방향을 선택합니다.

선택한 포트 미러링 세션 유형에 따라 다른 옵션을 구성에 사용할 수 있습니다.

옵션	설명
목록에서 기존 포트 추가	분산 <b>포트 선택</b> 을 클릭합니다. 대화상자에 기존 포트 목록이 표시됩니다. 분산 포트 옆의 확인란을 선택하고 <b>확인</b> 을 클릭합니다. 둘 이상의 분산 포트를 선택할 수 있습니다.
포트 번호로 기존 포트 추가	분산 <b>포트 추가</b> 를 클릭하고 포트 번호를 입력한 다음 <b>확인</b> 을 클릭합니다.
트래픽 방향 설정	포트를 추가한 후에는 목록의 포트를 선택하고 수신, 송신 또는 수신/송신 버튼을 클릭합니다. 선택한 항목이 트래픽 방향 열에 표시됩니다.
소스 VLAN 지정	원격 미러링 대상 세션 유형을 선택한 경우에는 소스 VLAN을 지정해야 합니다. <b>추가</b> 를 클릭하여 VLAN ID를 추가합니다. 위쪽 및 아래쪽 화살표를 사용하거나 필드를 클릭하고 VLAN ID를 수동으로 입력하여 ID를 편집합니다.

### 2 다음을 클릭합니다.

## 포트 미러링 대상

포트 미러링 세션 생성 절차를 완료하려면 포트 또는 업링크를 포트 미러링 세션의 대상으로 선택합니다.

소스 및 대상을 설정하지 않고 포트 미러링 세션을 생성할 수 있습니다. 소스와 대상을 설정하지 않으면 포트 미러링 세션이 미러링 경로 없이 생성됩니다. 따라서 올바른 속성이 설정된 포트 미러링 세션을 생성할 수 있습니다. 속성을 설정했으면 포트 미러링 세션을 편집하여 소스 및 대상 정보를 추가할 수 있습니다.

포트 미러링은 VLAN 전달 정책을 기준으로 검사됩니다. 원래 프레임의 VLAN이 대상 포트와 같지 않거나 대상 포트에 의해 트렁킹되지 않았으면 프레임이 미러링되지 않습니다.

## 절차

### 1 포트 미러링 세션의 대상을 선택합니다.

선택하는 세션 유형에 따라 다른 옵션을 사용할 수 있습니다.

옵션	설명
대상 분산 포트 선택	분산 <b>포트 선택</b> 을 클릭하여 목록에서 포트를 선택하거나 <b>분산 포트 추가</b> 를 클릭하여 포트 번호로 포트를 추가합니다. 둘 이상의 분산 포트를 추가할 수 있습니다.
업링크를 선택합니다	목록에서 사용 가능한 업링크를 선택하고 <b>추가</b> 를 클릭하여 업링크를 포트 미러링 세션에 추가합니다. 둘 이상의 업링크를 선택할 수 있습니다.
포트 또는 업링크 선택	분산 <b>포트 선택</b> 을 클릭하여 목록에서 포트를 선택하거나 <b>분산 포트 추가</b> 를 클릭하여 포트 번호로 포트를 추가합니다. 둘 이상의 분산 포트를 추가할 수 있습니다. <b>업링크 추가</b> 를 클릭하여 업링크를 대상으로 추가합니다. 목록에서 업링크를 선택하고 <b>확인</b> 을 클릭합니다.
IP 주소 지정	<b>추가</b> 를 클릭합니다. 새 목록 항목이 생성됩니다. 항목을 선택하고 <b>편집</b> 을 클릭하여 IP 주소를 입력하거나 IP 주소 필드를 직접 클릭하여 IP 주소를 입력합니다. IP 주소가 잘못된 경우 주의 메시지가 표시됩니다.

- 2 다음을 클릭합니다.
- 3 **완료 준비** 페이지에서 포트 미러링 세션에 대해 입력한 정보를 검토합니다.
- 4 (선택 사항) 정보를 편집하려면 **뒤로** 버튼을 사용합니다.
- 5 **마침**을 클릭합니다.

#### 결과

설정 탭의 포트 미러링 섹션에 새 포트 미러링 세션이 표시됩니다.

## 포트 미러링 세션 세부 정보 보기

상태, 소스 및 대상을 포함한 포트 미러링 세션 세부 정보를 봅니다.

#### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **구성** 탭에서 **설정**을 확장하고 **포트 미러링**을 클릭합니다.
- 3 목록에서 포트 미러링 세션을 선택하여 화면 아래쪽에 자세한 정보를 표시합니다. 탭을 사용하여 구성 세부 정보를 검토합니다.
- 4 (선택 사항) 새 포트 미러링 세션을 추가하려면 **새로 만들기**를 클릭합니다.
- 5 (선택 사항) 선택한 포트 미러링 세션의 세부 정보를 편집하려면 **편집**을 클릭합니다.
- 6 (선택 사항) 선택한 포트 미러링 세션을 삭제하려면 **제거**를 클릭합니다.

## 포트 미러링 세션 세부 정보, 소스 및 대상 편집

이름, 설명, 상태, 소스 및 대상을 포함하여 포트 미러링 세션의 세부 정보를 편집합니다.

#### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **구성** 탭에서 **설정**을 확장하고 **포트 미러링**을 클릭합니다.
- 3 목록에서 포트 미러링 세션을 선택하고 **편집**을 클릭합니다.
- 4 **속성** 페이지에서 세션 속성을 편집합니다.

편집할 포트 미러링 세션의 유형에 따라 서로 다른 옵션을 구성에 사용할 수 있습니다.

옵션	설명
이름	포트 미러링 세션에 대한 고유한 이름을 입력하거나 자동으로 생성된 세션 이름을 수락할 수 있습니다.
상태	드롭다운 메뉴를 사용하여 세션을 사용하거나 사용하지 않도록 설정합니다.

옵션	설명
대상 포트의 일반 I/O	드롭다운 메뉴를 사용하여 대상 포트의 일반 I/O를 허용하거나 허용하지 않습니다. 이 속성은 업링크 및 분산 포트 대상에만 사용할 수 있습니다. 이 옵션을 선택하지 않을 경우 대상 포트에서 미러링된 트래픽은 외부로 허용되지만 내부로의 트래픽은 허용되지 않습니다.
샘플링 속도	패킷이 샘플링되는 속도를 선택합니다. 레거시 세션을 제외한 모든 포트 미러링 세션에 대해 기본적으로 사용하도록 설정됩니다.  <b>참고</b> NSX 전송 노드 및 고급 네트워크 스택이 사용되도록 설정되면 샘플링 속도가 사용되도록 설정되지 않습니다.
미러링된 패킷 길이(바이트)	이 확인란을 사용하여 미러링된 패킷 길이(바이트)를 사용하도록 설정합니다. 이 경우 미러링된 프레임의 크기가 제한됩니다. 이 옵션을 선택하면 미러링된 모든 프레임이 지정된 길이로 잘립니다.
설명	포트 미러링 세션 구성의 설명을 입력할 수 있습니다.

## 5 소스 페이지에서 포트 미러링 세션의 소스를 편집합니다.

편집할 포트 미러링 세션의 유형에 따라 서로 다른 옵션을 구성에 사용할 수 있습니다.

옵션	설명
목록에서 기존 포트 추가	<b>이 포트 미러링 세션에 추가할 분산 포트를 선택합니다.</b> 버튼을 클릭합니다. 기존 포트 목록이 있는 대화상자가 열립니다. 분산 포트 옆의 확인란을 선택하고 <b>확인</b> 을 클릭합니다. 둘 이상의 분산 포트를 선택할 수 있습니다.
트래픽 방향 설정	포트를 추가한 후에는 목록의 포트를 선택하고 수신, 송신 또는 수신/송신 버튼을 클릭합니다. 선택 내용이 트래픽 방향 옆에 표시됩니다.

## 6 대상 섹션에서 포트 미러링 세션의 대상을 편집합니다.

편집할 포트 미러링 세션의 유형에 따라 서로 다른 옵션을 구성에 사용할 수 있습니다.

옵션	설명
대상 분산 포트 선택	<b>이 포트 미러링 세션에 추가할 분산 포트를 선택합니다.</b> 버튼을 클릭하여 목록에서 포트를 선택합니다. 둘 이상의 분산 포트를 추가할 수 있습니다.

## 7 확인을 클릭합니다.

# vSphere Distributed Switch 상태 점검

상태 점검 지원을 통해 vSphere Distributed Switch에서 구성 오류를 파악하고 해결할 수 있습니다.

vSphere Distributed Switch 상태 점검을 사용하여 분산 및 물리적 스위치의 특정 설정을 검사하고 환경의 네트워킹 구성에서 일반 오류를 식별합니다. 두 상태 점검 간의 기본 간격은 1분입니다.

**중요** 상태 점검을 사용하여 네트워크 문제를 해결한 다음, 문제를 식별하고 해결한 후 비활성화합니다. vSphere Distributed Switch 상태 점검을 비활성화한 후에는 생성된 MAC 주소가 사용자의 네트워크 정책에 따라 물리적 네트워크 환경에서 만료됩니다. 자세한 내용은 기술 자료 문서 [KB 2034795](#)를 참조하십시오.

구성 오류	상태 점검	Distributed Switch의 필요한 구성
Distributed Switch에 구성된 VLAN 트렁크 범위는 물리적 스위치의 트렁크 범위와 일치하지 않습니다.	Distributed Switch의 VLAN 설정이 연결된 물리적 스위치 포트의 트렁크 포트 구성과 일치하는지 확인합니다.	2개 이상의 활성 물리적 NIC
물리적 네트워크 어댑터, Distributed Switch 및 물리적 스위치 포트의 MTU 설정은 일치하지 않습니다.	VLAN별 물리적 액세스 스위치 포트 MTU 정보 프레임 설정이 vSphere Distributed Switch MTU 설정과 일치하는지 확인합니다.	2개 이상의 활성 물리적 NIC
포트 그룹에 구성된 팀 구성 정책은 물리적 스위치 포트 채널의 정책과 일치하지 않습니다.	EtherChannel에 참여하는 물리적 스위치의 연결된 액세스 포트가 팀 구성 정책이 IP 해시로 설정된 분산 포트와 쌍을 이루는지 확인합니다.	2개 이상의 활성 물리적 NIC 및 2개의 호스트

상태 점검은 Distributed Switch 업링크가 연결되는 액세스 스위치 포트만으로 제한됩니다.

## vSphere Distributed Switch 상태 점검 관리

상태 점검은 vSphere Distributed Switch 구성의 변경 내용을 모니터링합니다. Distributed Switch 구성에 대한 점검을 수행하려면 vSphere Distributed Switch 상태 점검을 사용하도록 설정해야 합니다.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **구성** 탭을 선택하고 [설정]을 확장합니다.
- 3 **상태 점검**을 선택하고 **편집** 버튼을 클릭합니다.
- 4 드롭다운 메뉴를 사용하여 상태 점검 옵션을 사용하거나 사용하지 않도록 설정합니다.

옵션	설명
VLAN 및 MTU	분산 업링크 포트 및 VLAN 범위의 상태를 보고합니다.
팀 구성 및 페일오버	ESXi 호스트와 팀 구성 정책에 사용된 물리적 스위치 간에 일치하지 않는 구성이 있는지 확인합니다.

- 5 **확인**을 클릭합니다.

### 다음에 수행할 작업

vSphere Distributed Switch의 구성을 변경할 경우 vSphere Client의 **모니터링** 탭에서 변경 내용에 대한 정보를 볼 수 있습니다. [vSphere Distributed Switch 상태 보기](#)의 내용을 참조하십시오.

## vSphere Distributed Switch 상태 보기

vSphere Distributed Switch에서 상태 점검을 사용하도록 설정했다면 vSphere Client에 연결된 호스트의 네트워크 상태를 볼 수 있습니다.

## 사전 요구 사항

vSphere Distributed Switch에서 VLAN, MTU 및 팀 구성 정책에 대한 상태 점검을 사용하도록 설정했는지 확인합니다. [vSphere Distributed Switch 상태 점검 관리](#)의 내용을 참조하십시오.

## 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **모니터링** 탭에서 **상태**를 클릭합니다.
- 3 호스트 멤버 상태 섹션에서 스위치에 연결된 호스트의 전체 상태와 VLAN, MTU 및 팀 구성 상태를 검사합니다.

## 스위치 탐색 프로토콜

vSphere 관리자는 스위치 탐색 프로토콜을 사용하여 vSphere 표준 스위치 또는 vSphere Distributed Switch에 연결되어 있는 물리적 스위치의 포트를 확인할 수 있습니다.

vSphere 5.0 이상은 CDP(Cisco 탐색 프로토콜) 및 LLDP(링크 계층 탐색 프로토콜)를 지원합니다. CDP는 Cisco 물리적 스위치에 연결되어 있는 vSphere 표준 스위치와 vSphere Distributed Switch에 사용할 수 있고 LLDP는 vSphere Distributed Switch 버전 5.0.0 이상에서 사용할 수 있습니다.

특정 vSphere Distributed Switch 또는 vSphere 표준 스위치에 대해 CDP 또는 LLDP를 사용하도록 설정한 경우 vSphere Client에서 디바이스 ID, 소프트웨어 버전, 시간 초과 등 피어 물리적 스위치의 속성을 볼 수 있습니다.

## vSphere Distributed Switch에서 Cisco 탐색 프로토콜 사용

vSphere 관리자는 CDP(Cisco 탐색 프로토콜)를 사용하여 vSphere 표준 스위치 또는 vSphere Distributed Switch에 연결되는 물리적인 Cisco 스위치의 포트를 확인할 수 있습니다. vSphere Distributed Switch에 대해 CDP가 사용하도록 설정된 경우 디바이스 ID, 소프트웨어 버전 및 시간 초과 같은 Cisco 스위치의 속성을 볼 수 있습니다.

## 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **작업** 메뉴에서 **설정 > 설정 편집**을 선택합니다.
- 3 설정 편집 대화상자에서 **고급**을 클릭합니다.
- 4 탐색 프로토콜 섹션의 **유형** 드롭다운 메뉴에서 **Cisco 탐색 프로토콜**을 선택합니다.

- 5 **작업** 드롭다운 메뉴에서 스위치에 연결된 ESXi 호스트의 작업 모드를 선택합니다.

옵션	설명
수신	ESXi에서 관련된 Cisco 스위치 포트에 대한 정보를 검색 및 표시하지만 vSphere Distributed Switch에 대한 정보는 Cisco 스위치 관리자가 사용할 수 없습니다.
알림	ESXi에서 vSphere Distributed Switch에 대한 정보를 Cisco 스위치 관리자가 사용할 수 있도록 하지만 Cisco 스위치에 대한 정보는 감지 및 표시하지 않습니다.
둘 다	ESXi에서 관련된 Cisco 스위치에 대한 정보를 검색 및 표시하고 Cisco 스위치 관리자가 vSphere Distributed Switch에 대한 정보를 사용할 수 있도록 합니다.

- 6 **확인**을 클릭합니다.

## vSphere Distributed Switch에서 링크 계층 탐색 프로토콜 사용

vSphere 관리자는 LLDP(링크 계층 탐색 프로토콜)를 사용하여 지정된 vSphere Distributed Switch에 연결되는 물리적 스위치 포트를 확인할 수 있습니다. 특정 Distributed Switch에 대해 LLDP를 사용할 수 있는 경우 새 시 ID, 시스템 이름 및 설명, 디바이스 기능 같은 물리적 스위치의 속성을 볼 수 있습니다.

### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **작업** 메뉴에서 **설정 > 설정 편집**을 선택합니다.
- 3 설정 편집 대화상자에서 **고급**을 클릭합니다.
- 4 탐색 프로토콜 섹션의 **유형** 드롭다운 메뉴에서 **링크 계층 탐색 프로토콜**을 선택합니다.
- 5 **작업** 드롭다운 메뉴에서 스위치에 연결된 ESXi 호스트의 작업 모드를 선택합니다.

작업	설명
수신	ESXi에서 관련된 물리적 스위치 포트에 대한 정보를 검색 및 표시하지만 vSphere Distributed Switch에 대한 정보는 스위치 관리자가 사용할 수 없습니다.
알림	ESXi에서 vSphere Distributed Switch에 대한 정보를 스위치 관리자가 사용할 수 있도록 하지만 물리적 스위치에 대한 정보는 감지 및 표시하지 않습니다.
둘 다	ESXi에서 관련된 물리적 스위치에 대한 정보를 검색 및 표시하고 스위치 관리자가 vSphere Distributed Switch에 대한 정보를 사용할 수 있도록 합니다.

- 6 **확인**을 클릭합니다.

## 스위치 정보 보기

Distributed Switch에서 Cisco 탐색 프로토콜(CDP) 또는 링크 계층 탐색 프로토콜(LLDP)을 사용하도록 설정하고 스위치에 연결된 호스트가 '수신' 또는 '둘 다' 작업 모드에 있는 경우 vSphere Client에서 물리적 스위치 정보를 볼 수 있습니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **네트워킹**을 확장하고 **물리적 어댑터**를 클릭합니다.
- 3 목록에서 물리적 어댑터를 선택하여 자세한 정보를 봅니다.

### 결과

사용 설정된 스위치 탐색 프로토콜에 따라, 스위치의 속성이 **CDP** 또는 **LLDP** 탭 아래에 나타납니다. 네트워크에서 해당 정보를 사용할 수 있는 경우 피어 디바이스 기능 아래에서 스위치의 시스템 기능을 검토할 수 있습니다.

## NSX 가상 Distributed Switch의 토폴로지 보기

N-VDS(NSX 가상 Distributed Switch)의 토폴로지 다이어그램을 확인하여 해당 구조 및 구성 요소를 검사할 수 있습니다.

이 다이어그램에서 선택한 포트 그룹 및 선택한 어댑터의 설정을 볼 수 있습니다.

### 사전 요구 사항

N-VDS의 토폴로지 다이어그램에는 스위치에 연결된 어댑터 및 포트 그룹이 시각적으로 표현됩니다.

### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 **네트워킹**을 확장하고 **가상 스위치**를 선택합니다.
- 3 목록에서 N-VDS를 선택합니다.

### 결과

호스트의 가상 스위치 목록 아래에 다이어그램이 나타납니다.

### 다음에 수행할 작업

토폴로지 다이어그램을 사용하여 가상 시스템 또는 VMkernel 어댑터가 외부 네트워크에 연결되어 있는지 검사하고 데이터를 전송하는 물리적 어댑터를 식별할 수 있습니다.

# 가상 시스템 네트워킹에 대한 프로토콜 프로파일 구성

# 15

네트워크 프로토콜 프로파일에는 해당 프로파일과 연관된 포트 그룹에 연결되어 있는 vApp이나 vApp 기능을 갖춘 가상 시스템에 vCenter Server가 할당하는 IPv4 및 IPv6 주소 풀이 포함됩니다.

네트워크 프로토콜 프로파일에는 IP 서브넷, DNS 및 HTTP 프록시 서버에 대한 설정도 포함됩니다.

네트워크 프로토콜 프로파일을 사용하여 가상 시스템의 네트워킹 설정을 구성하려면 다음 작업을 수행하십시오.

- 데이터 센터 또는 vSphere Distributed Switch 수준에서 네트워크 프로파일을 생성합니다.
- 프로토콜 프로파일을 vApp 가상 시스템의 포트 그룹과 연결합니다.
- vApp의 설정이나 가상 시스템의 vApp 옵션에서 임시 또는 정적 IP 할당 정책을 사용하도록 설정합니다.

**참고** 프로토콜 프로파일에서 해당 네트워크 설정을 검색하는 가상 시스템 또는 vApp를 다른 데이터 센터로 이동하는 경우 전원을 켜기 위해서는 프로토콜 프로파일을 대상 데이터 센터의 연결된 포트 그룹에 할당해야 합니다.

## ■ 네트워크 프로토콜 프로파일 추가

네트워크 프로토콜 프로파일에는 해당 프로파일과 연관된 포트 그룹에 연결되어 있는 vApp이나 vApp 기능을 갖춘 가상 시스템에 vCenter Server가 할당하는 IPv4 및 IPv6 주소 풀이 포함됩니다.

## ■ 네트워크 프로토콜 프로파일과 포트 그룹 연결

네트워크 프로토콜 프로파일의 IP 주소 범위를 vApp의 일부이거나 vApp 기능이 사용되도록 설정된 가상 시스템에 적용하려면 가상 시스템의 네트워킹을 제어하는 프로파일을 포트 그룹에 연결합니다.

## ■ 네트워크 프로토콜 프로파일을 사용하여 가상 시스템 또는 vApp에 IP 주소 할당

네트워크 프로토콜 프로파일을 표준 스위치 또는 Distributed Switch의 포트 그룹에 연결한 후 프로필을 사용하여 vApp 내의 가상 시스템에 IP 주소를 동적으로 할당할 수 있습니다.

## 네트워크 프로토콜 프로파일 추가

네트워크 프로토콜 프로파일에는 해당 프로파일과 연관된 포트 그룹에 연결되어 있는 vApp이나 vApp 기능을 갖춘 가상 시스템에 vCenter Server가 할당하는 IPv4 및 IPv6 주소 풀이 포함됩니다.

IPv4, IPv6 또는 둘 다에 대한 네트워크 프로토콜 프로파일 범위를 구성할 수 있습니다. vApp에 임시 IP 할당 정책이 사용되는 경우 vCenter Server는 이러한 범위를 사용하여 vApp 내의 가상 시스템에 IP 주소를 동적으로 할당합니다.



네트워크 프로토콜 프로파일에는 IP 서브넷, DNS 및 HTTP 프록시 서버에 대한 설정도 포함됩니다.

**참고** vApp 또는 가상 시스템의 전원을 켜기 위해 프로토콜 프로파일과 다른 데이터 센터 중에서 해당 네트워크 설정을 검색하는 vApp 또는 가상 시스템을 이동하는 경우 프로토콜 프로파일을 대상 데이터 센터의 연결된 포트 그룹에 할당해야 합니다.

## 절차

1 vApp과 연결된 데이터 센터로 이동합니다.

2 구성 탭에서 **자세히 > 네트워크 프로토콜 프로파일**을 선택합니다.

기존 네트워크 프로토콜 프로파일이 나열됩니다.

3 **추가** 버튼을 클릭합니다.

**네트워크 프로토콜 프로파일 추가** 마법사가 열립니다.

4 **이름 및 네트워크** 페이지에서 네트워크 프로토콜 프로파일의 이름을 입력하고 이 프로파일을 사용하는 네트워크를 선택합니다. **다음**을 클릭합니다.

네트워크는 한 번에 네트워크 프로토콜 프로파일 하나와 연결될 수 있습니다.

5 **IPv4** 페이지에서 관련 IPv4 설정을 구성합니다.

a **서브넷 및 게이트웨이** 텍스트 상자에 IP 서브넷 및 게이트웨이를 입력합니다.

b 네트워크에서 DHCP 서버를 사용할 수 있음을 나타내려면 **DHCP 있음** 라디오 버튼을 선택합니다.

c **DNS 서버 주소** 텍스트 상자에 DNS 서버 정보를 입력합니다.

d IP 풀 범위를 지정하려면 **IP 풀** 옵션을 사용하도록 설정합니다.

e IP 풀을 사용하도록 설정할 경우 **IP 풀 범위** 텍스트 상자에 호스트 주소 범위를 쉼표로 구분하여 입력합니다.

범위는 IP 주소, 파운드 기호(#) 및 범위의 길이를 나타내는 숫자로 구성됩니다.

예를 들어 **10.20.60.4#10**, **10.20.61.0#2**의 경우 IPv4 주소는 10.20.60.4에서 10.20.60.13 사이이, 그리고 10.20.61.0에서 10.20.61.1 사이일 수 있습니다.

게이트웨이와 범위는 서브넷 내에 있어야 합니다. **IP 풀 범위** 텍스트 상자에 입력하는 범위에는 게이트웨이 주소를 포함할 수 없습니다.

f **다음**을 클릭합니다.

6 **IPv6** 페이지에서 관련 IPv6 설정을 구성합니다.

a **서브넷 및 게이트웨이** 텍스트 상자에 IP 서브넷 및 게이트웨이를 입력합니다.

b **DHCP 있음** 라디오 버튼을 선택하여 이 네트워크에서 DHCP 서버를 사용할 수 있음을 나타냅니다.

c **DNS 서버 주소**에 DNS 서버 정보를 입력합니다.

d **IP 풀** 옵션을 사용하도록 설정하여 IP 풀 범위를 지정합니다.

- e IP 풀을 사용하도록 설정할 경우 **IP 풀 범위** 텍스트 상자에 호스트 주소 범위를 쉼표로 구분하여 입력합니다.

범위는 IP 주소, 파운드 기호(#) 및 범위의 길이를 나타내는 숫자로 구성됩니다.

예를 들어, 다음과 같은 IP 풀 범위를 지정할 수 있습니다.

**fe80:0:0:0:2bff:fe59:5a:2b#10**, **fe80:0:0:0:2bff:fe59:5f:b1#2**. 이 경우 주소 범위는 다음과 같습니다.

fe80:0:0:0:2bff:fe59:5a:2b - fe80:0:0:0:2bff:fe59:5a:34

및

fe80:0:0:0:2bff:fe59:5f:b1 - fe80:0:0:0:2bff:fe59:5f:b2 .

게이트웨이와 범위는 서브넷 내에 있어야 합니다. **IP 풀 범위** 텍스트 상자에 입력하는 범위에는 게이트웨이 주소를 포함할 수 없습니다.

- f 다음을 클릭합니다.

## 7 다른 네트워크 구성 페이지에서 추가적인 네트워크 구성을 지정합니다.

- a DNS 도메인을 입력합니다.

- b 호스트 접두사를 입력합니다.

- c DNS 검색 경로를 입력합니다.

검색 경로는 쉼표, 세미콜론 또는 공백으로 구분된 DNS 도메인 목록으로 지정됩니다.

- d 프록시 서버의 서버 이름과 포트 번호를 입력합니다.

서버 이름에는 콜론과 포트 번호를 포함해야 합니다. 예를 들어 `web-proxy:3912`는 유효한 프록시 서버입니다.

- e 다음을 클릭합니다.

## 8 이름 및 네트워크 할당 페이지에서 설정을 검토하고 마침을 클릭합니다.

## 네트워크 프로토콜 프로파일 이름 및 네트워크 선택

네트워크 프로토콜 프로파일 이름을 지정하고 이 프로파일을 사용할 네트워크를 선택합니다.

### 절차

- 1 네트워크 프로토콜 프로파일의 이름을 입력합니다.

- 2 이 네트워크 프로토콜 프로파일을 사용하는 네트워크를 선택합니다.

네트워크는 한 번에 네트워크 프로토콜 프로파일 하나와 연결될 수 있습니다.

- 3 다음을 클릭합니다.

## 네트워크 프로토콜 프로파일 IPv4 구성 지정

네트워크 프로토콜 프로파일에는 vApp에서 사용할 수 있는 IPv4 및 IPv6 주소의 풀이 포함되어 있습니다. 네트워크 프로토콜 프로파일을 생성할 때 해당 IPv4 구성을 설정합니다.

IPv4, IPv6 또는 둘 다를 위한 네트워크 프로토콜 프로파일 범위를 구성할 수 있습니다. vApp이 임시 IP 할당을 사용하도록 설정된 경우 vCenter Server는 이러한 범위를 사용하여 가상 시스템에 IP 주소를 동적으로 할당합니다.

### 절차

- 1 **IP 서브넷 및 게이트웨이**를 해당 필드에 입력합니다.
- 2 **DHCP 있음**을 선택하여 이 네트워크에서 DHCP 서버를 사용할 수 있음을 나타냅니다.
- 3 DNS 서버 정보를 입력합니다.  
IP 주소를 심표, 세미콜론 또는 공백으로 구분하여 서버를 지정합니다.
- 4 **IP 풀 사용** 확인란을 선택하여 IP 풀 범위를 지정합니다.
- 5 IP 풀을 사용하도록 설정할 경우 **IP 풀 범위** 필드에 호스트 주소 범위를 심표로 구분하여 입력합니다.  
범위는 IP 주소, 파운드 기호(#) 및 범위의 길이를 나타내는 숫자로 구성됩니다.  
게이트웨이와 범위는 서브넷 내에 있어야 합니다. **IP 풀 범위** 필드에 입력하는 범위에는 게이트웨이 주소를 포함할 수 없습니다.  
예를 들어 **10.20.60.4#10**, **10.20.61.0#2**의 경우 IPv4 주소는 10.20.60.4에서 10.20.60.13 사이, 그리고 10.20.61.0에서 10.20.61.1 사이일 수 있습니다.
- 6 다음을 클릭합니다.

## 네트워크 프로토콜 프로파일 IPv6 구성 지정

네트워크 프로토콜 프로파일에는 vApp에서 사용할 수 있는 IPv4/IPv6 주소 풀이 포함되어 있습니다. 네트워크 프로토콜 프로파일을 생성할 때 해당 IPv6 구성을 설정합니다.

IPv4나 IPv6 또는 둘 모두에 필요한 네트워크 프로토콜 프로파일 범위를 구성할 수 있습니다. vApp이 임시 IP 할당을 사용하도록 설정된 경우 vCenter Server는 이러한 범위를 사용하여 가상 시스템에 IP 주소를 동적으로 할당합니다.

### 절차

- 1 **IP 서브넷 및 게이트웨이**를 해당 필드에 입력합니다.
- 2 **DHCP 있음**을 선택하여 이 네트워크에서 DHCP 서버를 사용할 수 있음을 나타냅니다.
- 3 DNS 서버 정보를 입력합니다.  
IP 주소를 심표, 세미콜론 또는 공백으로 구분하여 서버를 지정합니다.
- 4 **IP 풀 사용** 확인란을 선택하여 IP 풀 범위를 지정합니다.

- 5 IP 풀을 사용하도록 설정할 경우 **IP 풀 범위** 필드에 호스트 주소 범위를 쉼표로 구분하여 입력합니다.

범위는 IP 주소, 파운드 기호(#) 및 범위의 길이를 나타내는 숫자로 구성됩니다. 예를 들어 다음과 같은 IP 풀 범위를 지정한다고 가정해 보겠습니다.

```
fe80:0:0:0:2bff:fe59:5a:2b#10,fe80:0:0:0:2bff:fe59:5f:b1#2
```

이 경우 주소 범위는 다음과 같습니다.

```
fe80:0:0:0:2bff:fe59:5a:2b - fe80:0:0:0:2bff:fe59:5a:34
```

및

```
fe80:0:0:0:2bff:fe59:5f:b1 - fe80:0:0:0:2bff:fe59:5f:b2
```

게이트웨이와 범위는 서브넷 내에 있어야 합니다. **IP 풀 범위** 필드에 입력하는 범위에는 게이트웨이 주소를 포함할 수 없습니다.

- 6 다음을 클릭합니다.

## 네트워크 프로토콜 프로파일 DNS 및 기타 구성 지정

네트워크 프로토콜 프로파일을 생성할 때 DNS 도메인, DNS 검색 경로, 호스트 접두사 및 HTTP 프록시를 지정할 수 있습니다.

### 절차

- 1 DNS 도메인을 입력합니다.
- 2 호스트 접두사를 입력합니다.
- 3 DNS 검색 경로를 입력합니다.  
검색 경로는 쉼표, 세미콜론 또는 공백으로 구분된 DNS 도메인 목록으로 지정됩니다.
- 4 프록시 서버의 서버 이름과 포트 번호를 입력합니다.  
서버 이름에는 콜론과 포트 번호를 선택적으로 포함할 수 있습니다.  
예를 들어 `web-proxy:3912`는 유효한 프록시 서버입니다.
- 5 다음을 클릭합니다.

## 네트워크 프로토콜 프로파일 생성 완료

### 절차

- ◆ 설정을 검토하고 **마침**을 클릭하여 네트워크 프로토콜 프로파일 추가를 완료합니다.

## 네트워크 프로토콜 프로파일과 포트 그룹 연결

네트워크 프로토콜 프로파일의 IP 주소 범위를 vApp의 일부이거나 vApp 기능이 사용되도록 설정된 가상 시스템에 적용하려면 가상 시스템의 네트워킹을 제어하는 프로파일을 포트 그룹에 연결합니다.

## 절차

- 1 vApp과 연결된 데이터 센터로 이동합니다.
- 2 구성 탭에서 **자세히> 네트워크 프로토콜 프로파일**을 선택합니다.  
기존 네트워크 프로토콜 프로파일이 나열됩니다.
- 3 목록에서 네트워크 프로파일을 선택하고 **할당**을 클릭합니다.  
**네트워크 할당** 대화상자가 열립니다.
- 4 네트워크 프로파일에 할당할 포트 그룹 또는 네트워크를 선택합니다.
  - **분산 포트 그룹** 탭에서 분산 포트 그룹의 목록을 확인합니다.
  - **네트워크** 탭에서 표준 스위치의 포트 그룹 목록을 확인합니다.대화상자를 닫기 전에 여러 포트 그룹을 선택할 수 있습니다.
- 5 **저장**을 클릭합니다.

## 네트워크 프로토콜 프로파일을 사용하여 가상 시스템 또는 vApp에 IP 주소 할당

네트워크 프로토콜 프로파일을 표준 스위치 또는 Distributed Switch의 포트 그룹에 연결한 후 프로필을 사용하여 vApp 내의 가상 시스템에 IP 주소를 동적으로 할당할 수 있습니다.

### 사전 요구 사항

가상 시스템이 네트워크 프로토콜 프로파일과 연관된 포트 그룹에 연결되어 있는지 확인합니다.

## 절차

- ◆ 작업을 선택합니다.

옵션	설명
네트워크 프로토콜 프로파일을 사용하여 가상 시스템에 IP 주소 할당	<ul style="list-style-type: none"> <li>a vCenter Server 인벤토리의 가상 시스템으로 이동합니다.</li> <li>b 구성 탭에서 설정을 확장하고 <b>vApp 옵션</b>을 선택합니다.</li> <li>c 편집 버튼을 클릭합니다.</li> </ul> <p style="text-align: center;"><b>vApp 옵션 편집</b> 대화상자가 열립니다.</p> <ul style="list-style-type: none"> <li>d vApp 옵션을 사용하도록 설정하지 않은 경우 <b>vApp 옵션 사용</b> 확인란을 선택합니다.</li> <li>e <b>IP 할당</b> 탭을 클릭합니다.</li> <li>f [제작] 섹션에서 <b>OVF 환경</b>을 IP 할당 체계로 선택합니다.</li> <li>g [배포] 섹션에서 <b>IP 할당을 임시 - IP 풀</b> 또는 <b>정적 - IP 풀</b>로 설정합니다.</li> <li>h <b>확인</b>을 클릭합니다.</li> </ul>
네트워크 프로토콜 프로파일을 사용하여 vApp에 IP 주소 할당	<ul style="list-style-type: none"> <li>a vCenter Server 인벤토리의 vApp으로 이동합니다.</li> <li>b vApp을 마우스 오른쪽 버튼으로 클릭하고 <b>설정 편집</b>을 선택합니다.</li> </ul> <p style="text-align: center;"><b>vApp 편집</b> 대화상자가 열립니다.</p> <ul style="list-style-type: none"> <li>c <b>IP 할당</b> 탭을 클릭합니다.</li> <li>d [제작] 섹션에서 <b>OVF 환경</b>을 IP 할당 체계로 선택합니다.</li> <li>e [배포] 섹션에서 <b>IP 할당을 임시 - IP 풀</b> 또는 <b>정적 - IP 풀</b>로 설정합니다.</li> <li>f <b>확인</b>을 클릭합니다.</li> </ul>

**정적 - IP 풀**과 **임시 - IP 풀** 옵션 모두 포트 그룹과 연관된 네트워크 프로토콜 프로파일에 정의된 범위에서 IP 주소를 할당합니다. **정적 - IP 풀**을 선택하는 경우 가상 시스템이나 vApp의 전원을 처음 켤 때 IP 주소가 할당됩니다. 할당된 IP 주소는 다시 시작하더라도 유지됩니다. **임시 - IP 풀**을 선택하는 경우 가상 시스템이나 vApp의 전원을 켤 때마다 IP 주소가 할당됩니다.

## 결과

가상 시스템의 전원을 켜면 포트 그룹에 연결된 어댑터가 프로토콜 프로파일의 범위에서 IP 주소를 받습니다. 가상 시스템의 전원을 끄면 IP 주소가 해제됩니다.

# 멀티캐스트 필터링이란?

# 16

vSphere 6.0 이상에서 vSphere Distributed Switch는 개별 멀티캐스트 그룹과 관련된 멀티캐스트 패킷의 필터링을 위한 기본 및 스누핑 모델을 지원합니다. 스위치의 가상 시스템이 구독하는 멀티캐스트 그룹 수에 따라 모델을 선택합니다.

- **멀티캐스트 필터링 모드**

vSphere Distributed Switch 6.0.0 이상 릴리스는 멀티캐스트 트래픽 필터링을 위한 기본 모드 외에도 가상 시스템의 IGMP(Internet Group Management Protocol) 및 MLD(Multicast Listener Discovery) 메시지를 기반으로 보다 정확한 방식으로 멀티캐스트 트래픽을 전달하는 멀티캐스트 스누핑을 지원합니다.

- **vSphere Distributed Switch에서 멀티캐스트 스누핑 사용**

vSphere Distributed Switch에서 멀티캐스트 스누핑을 사용하여 가상 시스템이 멀티캐스트 트래픽 구독을 위해 전송하는 IGMP(Internet Group Management Protocol) 또는 MLD(Multicast Listener Discovery) 멤버 자격 정보에 따라 정확한 방식으로 트래픽을 전달합니다.

- **멀티캐스트 스누핑에 대한 쿼리 시간 간격 편집**

vSphere Distributed Switch에서 IGMP 또는 MLD 멀티캐스트 스누핑이 사용하도록 설정된 경우 스누핑 쿼리 발송기가 물리적 스위치에 구성되어 있지 않으면 해당 스위치가 가상 시스템의 멤버 자격에 대한 일반 쿼리를 전송합니다. Distributed Switch에 연결된 ESXi 호스트에서 스위치가 일반 쿼리를 전송하는 시간 간격을 편집할 수 있습니다.

- **IGMP 및 MLD의 소스 IP 주소 개수 편집**

vSphere Distributed Switch에서 IGMP 또는 MLD 멀티캐스트 스누핑을 사용하도록 설정하면 멀티캐스트 그룹의 멤버가 패킷을 수신할 수 있는 IP 소스의 최대 개수를 편집할 수 있습니다.

## 멀티캐스트 필터링 모드

vSphere Distributed Switch 6.0.0 이상 릴리스는 멀티캐스트 트래픽 필터링을 위한 기본 모드 외에도 가상 시스템의 IGMP(Internet Group Management Protocol) 및 MLD(Multicast Listener Discovery) 메시지를 기반으로 보다 정확한 방식으로 멀티캐스트 트래픽을 전달하는 멀티캐스트 스누핑을 지원합니다.

## 기본 멀티캐스트 필터링

vSphere Standard Switch 또는 vSphere Distributed Switch는 기본 멀티캐스트 필터링 모드에서 멀티캐스트 그룹의 대상 MAC 주소에 따라 가상 시스템에 대한 멀티캐스트 트래픽을 전달합니다. 멀티캐스트 그룹에 가입할 때 게스트 운영 체제는 스위치를 통해 그룹의 멀티캐스트 MAC 주소를 네트워크로 푸시 다운합니다. 스위치는 로컬 전달 테이블에서 포트와 대상 멀티캐스트 MAC 주소 간의 매핑을 저장합니다.

스위치는 가상 시스템이 그룹에 가입하거나 그룹을 탈퇴하기 위해 전송하는 IGMP 메시지를 해석하지 않습니다. 스위치는 이 메시지를 직접 로컬 멀티캐스트 라우터로 전송합니다. 그러면 해당 라우터가 메시지를 해석하여 가상 시스템이 그룹에 가입하거나 그룹에서 탈퇴하도록 합니다.

기본 모드는 다음과 같은 제한 사항이 있습니다.

- 가상 시스템은 스위치가 멀티캐스트 그룹의 대상 MAC 주소에 따라 패킷을 전달하기 때문에 구독되지 않은 그룹으로부터 패킷을 수신할 수 있습니다. 이러한 패킷은 최대 32개의 IP 멀티캐스트 그룹으로 매핑될 수 있습니다.
- 32개가 넘는 멀티캐스트 MAC 주소의 트래픽을 위해 구독되는 가상 시스템이 전달 모델의 제한으로 인해 구독하지 않은 패킷을 수신합니다.
- 스위치는 IGMP 버전 3에 정의된 소스 주소에 따라 패킷을 필터링하지 않습니다.

## 멀티캐스트 스누핑

멀티캐스트 스누핑 모드에서 vSphere Distributed Switch는 RFC 4541에 따라 IGMP 및 MLD 스누핑을 제공합니다. 스위치는 IP 주소를 사용하여 멀티캐스트 트래픽을 보다 정확하게 디스패치합니다. 이 모드는 IPv4 멀티캐스트 그룹 주소에 대한 IGMPv1, IGMPv2 및 IGMPv3 그리고 IPv6 멀티캐스트 그룹 주소에 대한 MLDv1 및 MLDv2를 지원합니다.

스위치는 가상 시스템의 멤버 자격을 동적으로 감지합니다. 가상 시스템이 스위치 포트를 통해 IGMP 또는 MLD 멤버 자격 정보가 포함된 패킷을 전송할 때 스위치는 그룹의 대상 IP 주소에 대한 기록 그리고 IGMPv3의 경우 가상 시스템의 트래픽 수신 선호 대상인 소스 IP 주소에 대한 기록을 생성합니다. 가상 시스템이 특정 기간 이내에 그룹에 대한 멤버 자격을 갱신하지 않는 경우 스위치는 조회 기록에서 그룹에 대한 항목을 제거합니다.

Distributed Switch의 멀티캐스트 스누핑 모드에서 가상 시스템은 최대 512개의 그룹과 10개의 소스로부터 단일 스위치 포트에 대한 멀티캐스트 트래픽을 수신할 수 있습니다.

**참고** vSphere 6.7에서는 기본 멀티캐스트 필터링 모드가 기본입니다. vSphere 7.0에서 기본 멀티캐스트 필터링 모드는 IGMP/MLD 스누핑입니다. DVS가 7.0으로 업그레이드되면 기본 멀티캐스트 필터링 모드가 기본에서 IGMP/MLD 스누핑으로 변경됩니다.

## vSphere Distributed Switch에서 멀티캐스트 스누핑 사용

vSphere Distributed Switch에서 멀티캐스트 스누핑을 사용하여 가상 시스템이 멀티캐스트 트래픽 구독을 위해 전송하는 IGMP(Internet Group Management Protocol) 또는 MLD(Multicast Listener Discovery) 멤버 자격 정보에 따라 정확한 방식으로 트래픽을 전달합니다.



스위치의 가상화된 워크로드가 32개가 넘는 멀티캐스트 그룹을 구독하거나 특정 소스 노드에서 트래픽을 수신해야 하는 경우 멀티캐스트 스누핑을 사용합니다. vSphere Distributed Switch의 멀티캐스트 필터링 모드에 대한 자세한 내용은 [멀티캐스트 필터링 모드](#) 항목을 참조하십시오.

#### 사전 요구 사항

vSphere Distributed Switch의 버전이 6.0.0 이상인지 확인합니다.

#### 절차

- 1 vSphere Client 홈 페이지에서 **네트워킹**을 클릭하고 분산 스위치로 이동합니다.
- 2 **작업** 메뉴에서 **설정 > 설정 편집**을 선택합니다.
- 3 스위치의 설정을 표시하는 대화상자에서 **고급**을 클릭합니다.
- 4 **멀티캐스트 필터링 모드** 드롭다운 메뉴에서 **IGMP/MLD 스누핑**을 선택하고 **확인**을 클릭합니다.

#### 결과

멀티캐스트 스누핑이 ESXi 6.0 이상을 실행하는 호스트에서 활성화됩니다.

## 멀티캐스트 스누핑에 대한 쿼리 시간 간격 편집

vSphere Distributed Switch에서 IGMP 또는 MLD 멀티캐스트 스누핑이 사용하도록 설정된 경우 스누핑 쿼리 발송기가 물리적 스위치에 구성되어 있지 않으면 해당 스위치가 가상 시스템의 멤버 자격에 대한 일반 쿼리를 전송합니다. Distributed Switch에 연결된 ESXi 호스트에서 스위치가 일반 쿼리를 전송하는 시간 간격을 편집할 수 있습니다.

스누핑 쿼리 전송을 위한 기본 시간 간격은 125초입니다.

#### 절차

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 **구성** 탭에서 **시스템**을 확장하고 **고급 시스템 설정**을 선택합니다.
- 3 **편집**을 클릭합니다.
- 4 `Net.IGMPQueryInterval` 시스템 설정을 찾아 설정에 대한 새 값(초)을 입력합니다.
- 5 **확인**을 클릭합니다.

## IGMP 및 MLD의 소스 IP 주소 개수 편집

vSphere Distributed Switch에서 IGMP 또는 MLD 멀티캐스트 스누핑을 사용하도록 설정하면 멀티캐스트 그룹의 멤버가 패킷을 수신할 수 있는 IP 소스의 최대 개수를 편집할 수 있습니다.

#### 절차

- 1 vSphere Client에서 호스트로 이동합니다.

- 2 구성 탭에서 **시스템**을 확장하고 **고급 시스템 설정**을 선택합니다.
- 3 **편집**을 클릭합니다.
- 4 `Net.IGMPV3MaxSrcIPNum` 또는 `Net.MLDV2MaxSrcIPNum` 시스템 설정 을 찾아 설정에 대한 1~32 사이의 새 값을 입력합니다.
- 5 **확인**을 클릭합니다.

# 상태 비저장 네트워크 배포란?

# 17

상태 비저장은 이전에 구성 또는 상태를 저장했던 로컬 스토리지가 없는 ESXi 호스트의 실행 모드입니다. 구성은 호스트 프로파일로 추상화됩니다. 호스트 프로파일은 시스템 클래스에 적용되는 템플릿입니다. 상태 비저장을 사용하면 오류가 있는 하드웨어를 쉽게 교체, 제거 및 추가할 수 있고 하드웨어 배포를 더 쉽게 확장할 수 있습니다.

모든 상태 비저장 ESXi 부팅은 처음 부팅과 같습니다. ESXi 호스트는 기본 제공 표준 스위치를 통한 vCenter Server와의 네트워킹 연결을 사용하여 부팅됩니다. 호스트 프로파일에 분산 스위치 구성원이 지정된 경우 vCenter Server가 ESXi 호스트를 VMware 분산 스위치에 가입시킵니다.

상태 비저장 ESXi 호스트에 대한 네트워크 설정을 계획할 때는 구성을 최대한 일반적으로 유지하고 호스트 관련 항목을 사용하지 않아야 합니다. 현재 설계 환경에는 새 호스트를 배포할 때 물리적 스위치를 재구성하는 후크가 포함되지 않습니다. 이러한 요구 사항은 특별한 처리가 필요합니다.

상태 비저장 배포를 설정하려면 하나의 ESXi 호스트를 표준 방식으로 설치해야 합니다. 그런 다음 호스트 프로파일에 저장할 다음과 같은 네트워크 관련 정보를 찾아서 기록합니다.

- vSphere 표준 스위치 인스턴스 및 설정(포트 그룹, 업링크, MTU 등)
- 분산 스위치 인스턴스
- 업링크 선택 규칙 및 업링크 포트 또는 포트 그룹
- vNIC 정보:
  - 주소 정보(IPv4 또는 IPv6, 정적 또는 DHCP, 게이트웨이)
  - 물리적 네트워크 어댑터에 할당된 포트 그룹 및 분산 포트 그룹(vmknics)
  - Distributed Switch가 있는 경우 VLAN, vmknics에 바인딩된 물리적 NIC 및 Etherchannel이 구성되어 있는지 여부를 기록합니다.

기록된 정보는 호스트 프로파일의 템플릿으로 사용됩니다. 호스트 프로파일 가상 스위치 정보를 추출하여 호스트 프로파일에 저장했다면 원하는 정보를 변경할 수 있습니다. vmnic 이름 또는 디바이스 번호를 기반으로 하는 업링크 선택 정책 및 VLAN ID를 기반으로 하는 자동 검색 섹션에서 표준 스위치와 분산 스위치 모두에 대한 수정 사항이 제공됩니다. (수정 가능) 정보는 상태 비저장 부팅 인프라에 의해 저장되고 다음 부팅 시 상태 비저장 ESXi 호스트에 적용됩니다. 네트워크 초기화 중 일반 네트워크 플러그인은 기록된 호스트 프로파일 설정을 해석하고 다음을 수행합니다.

- 적절한 물리적 NIC 드라이버를 로드합니다.

- 모든 표준 스위치 인스턴스를 포트 그룹과 함께 만듭니다. 정책을 기반으로 업링크를 선택합니다. 정책이 VLAN ID를 기반으로 하는 경우 관련 정보를 수집하는 검색 프로세스가 있습니다.
- 표준 스위치에 연결된 VMkernel 네트워크 어댑터의 경우 VMkernel 네트워크 어댑터를 만들어 포트 그룹에 연결합니다.
- Distributed Switch에 연결된 각 VMkernel 네트워크 어댑터의 경우 필요에 따라 VMkernel 네트워크 어댑터에 바인딩된 업링크를 사용하여 임시 표준 스위치를 만듭니다. VLAN을 사용하여 임시 포트 그룹을 만들고 기록된 정보를 기반으로 팀 구성 정책을 만듭니다. 특히, Distributed Switch에서 이더 채널(Etherchannel)이 사용된 경우 IP 해시가 사용됩니다.
- 모든 VMkernel 네트워크 어댑터 설정을 구성(주소, 게이트웨이, MTU 등을 할당)합니다.

기본 연결이 작동하고 Distributed Switch가 없는 경우 네트워크 설정이 완료됩니다.

Distributed Switch가 있는 경우에는 Distributed Switch 업데이트 적용이 완료될 때까지 시스템이 유지 보수 모드로 유지됩니다. 이때는 가상 시스템이 시작되지 않습니다. Distributed Switch에는 vCenter Server가 필요하므로 vCenter Server 연결이 설정되고 vCenter Server에서 호스트가 Distributed Switch의 일부임을 인식할 때까지 부팅 프로세스가 계속됩니다. Distributed Switch 호스트 가입을 실행하여 호스트에 Distributed Switch 프록시 표준 스위치를 만들고, 적절한 업링크를 선택하고, vmknics를 표준 스위치에서 Distributed Switch로 마이그레이션합니다. 이 작업이 완료되면 임시 표준 스위치와 포트 그룹을 삭제합니다.

업데이트 적용 프로세스가 끝나면 ESXi 호스트가 유지 보수 모드를 종료하고 HA 또는 DRS가 호스트에서 가상 시스템을 시작할 수 있습니다.

호스트 프로파일이 없으면 "기본 네트워킹" 논리를 사용하여 임시 표준 스위치를 만듭니다. 즉, 업링크가 PXE 부팅 vNIC에 해당하는 관리 네트워크 스위치(VLAN 태그 없음)를 만듭니다. 관리 네트워크 포트 그룹에 PXE 부팅 vNIC와 동일한 MAC 주소를 사용하여 vmknics를 만듭니다. 이 논리는 기존에 PXE 부팅에 사용되었습니다. 호스트 프로파일이 있지만 네트워킹 호스트 프로파일이 비활성화되었거나 매우 불안정한 경우 vCenter Server는 기본 네트워킹으로 돌아가므로 ESXi 호스트를 원격으로 관리할 수 있습니다. 이 경우 규정 준수 실패가 트리거되므로 vCenter Server가 복구 작업을 시작합니다.

네트워크를 구성할 때 다음 모범 사례를 고려하십시오.

- vCenter Server, ESXi 및 기타 제품과 서비스 사이의 연결을 안정적으로 유지하려면 제품 간에 연결 제한 및 시간 초과를 설정하지 않아야 합니다. 제한 및 시간 초과를 설정하면 패킷 흐름에 영향을 주어 서비스가 중단될 수 있습니다.
- 호스트 관리, vSphere vMotion, vSphere FT 등에 사용되는 네트워크를 서로 분리하여 보안 및 성능을 향상시킬 수 있습니다.
- 별도의 물리적 NIC를 가상 시스템 그룹 전용으로 사용하거나 Network I/O Control 및 트래픽 조절을 사용하여 가상 시스템에 대한 대역폭을 보장합니다. 이러한 분리를 통해 전체 네트워킹 워크로드의 일부를 여러 CPU에 분산할 수도 있습니다. 분리된 가상 시스템은 vSphere Client 등에서 발생하는 애플리케이션 트래픽을 효과적으로 처리할 수 있습니다.
- 네트워크 서비스를 물리적으로 분리하고 특정 NIC 집합을 특정 네트워크 서비스에 전적으로 사용하려면 각 서비스에 대한 vSphere 표준 스위치나 vSphere Distributed Switch를 생성합니다. 이렇게 할 수 없는 경우 단일 스위치의 네트워크 서비스를 VLAN ID가 다른 포트 그룹에 연결하여 분리합니다. 어떤 경우든 네트워크 관리자와 함께 사용자가 선택한 네트워크 또는 VLAN이 다른 사용 환경에서 분리되어 있고 연결된 라우터가 없는지 확인해야 합니다.
- 개별 네트워크의 vSphere vMotion 연결을 유지합니다. vMotion을 사용한 마이그레이션이 발생할 때 게스트 운영 체제의 메모리 내용이 네트워크를 통해 전송됩니다. VLAN을 사용하여 단일 물리적 네트워크를 세그먼트로 나누거나 개별 물리적 네트워크를 사용(권장)하여 이 작업을 수행할 수 있습니다.  
  
IP 서브넷 간에 마이그레이션하고 별도의 버퍼 및 소켓 풀을 사용하기 위해 vMotion TCP/IP 스택에 vMotion을 위한 트래픽을 배치하고 전원이 꺼진 가상 시스템의 마이그레이션 및 복제를 위한 트래픽을 프로비저닝 TCP/IP 스택에 배치합니다. [VMkernel 네트워킹 계층](#)의 내용을 참조하십시오.
- VMkernel 네트워킹에서 멀티호밍은 지원되지 않습니다. 자세한 내용은 <http://kb.vmware.com/kb/2010877>을 참조하십시오.
- 표준 또는 Distributed Switch에서 실행 중인 가상 시스템 또는 네트워크 서비스에 영향을 주지 않고 해당 스위치에서 네트워크 어댑터를 추가하거나 제거할 수 있습니다. 실행 중인 하드웨어를 모두 제거해도 가상 시스템은 계속 통신할 수 있습니다. 하나의 네트워크 어댑터가 그대로 유지되면 모든 가상 시스템은 여전히 물리적 네트워크와 연결할 수 있습니다.
- 가장 중요한 가상 시스템을 보호하려면 물리적 네트워크에 대한 업링크가 있는 가상 네트워크와 업링크가 없는 순수 가상 네트워크 간에 라우팅하는 방화벽을 가상 시스템에 배포합니다.

- 최상의 성능을 위해 VMXNET 3 가상 시스템 NIC를 사용합니다.
- 동일한 vSphere 표준 스위치나 vSphere Distributed Switch에 연결된 물리적 네트워크 어댑터는 동일한 물리적 네트워크에도 연결되어야 합니다.
- vSphere Distributed Switch의 모든 VMkernel 네트워크 어댑터에 대해 동일한 MTU를 구성합니다. 서로 다른 MTU로 구성된 일부 VMkernel 네트워크 어댑터가 vSphere Distributed Switch에 연결된 경우 네트워크 연결 문제가 발생할 수 있습니다.

# vSphere 네트워킹 문제 해결

# 19

vSphere의 네트워킹에 대한 문제 해결 항목에서는 ESXi 호스트, vCenter Server 및 가상 시스템을 연결할 때 발생할 수 있는 잠재적인 문제에 대한 해결 방법을 제공합니다.

다음으로 아래 항목을 읽으십시오.

- vSphere 구현 문제 해결을 위한 지침
- MAC 주소 할당 문제 해결
- vSphere Distributed Switch에서 호스트를 제거할 수 없음
- vSphere Distributed Switch의 호스트와 vCenter Server의 연결 끊김
- 호스트의 네트워크 이중화 손실에 대한 경보
- 분산 포트 그룹의 업링크 페일오버 순서를 변경한 후에 가상 시스템의 연결 끊김
- 물리적 어댑터를 Network I/O Control이 사용하도록 설정된 vSphere Distributed Switch에 추가할 수 없음
- SR-IOV 지원 워크로드 문제 해결
- 호스트의 인터럽트 벡터 부족으로 SR-IOV 가상 기능을 사용하는 가상 시스템의 전원이 켜지지 않음
- VPN 클라이언트를 실행하는 가상 시스템으로 인해 호스트 또는 vSphere HA 클러스터에서 가상 시스템에 대한 서비스 거부가 발생함
- Windows 가상 시스템에서 UDP 워크로드에 대한 처리량이 낮음
- 동일한 분산 포트 그룹에 속하지만 서로 다른 호스트에 위치한 가상 시스템은 서로 통신할 수 없음
- 연결된 프로토콜 프로파일이 없어서 마이그레이션된 vApp 전원 켜기가 실패함
- 네트워킹 구성 작업이 롤백되고 vCenter Server에서 호스트 연결이 끊김

## vSphere 구현 문제 해결을 위한 지침

vSphere 구현의 문제를 해결하려면 증상을 식별하고, 영향을 받는 구성 요소를 확인하고, 가능한 솔루션을 테스트하십시오.

### 증상 식별

다양한 잠재적 원인이 구현의 성능 저하 또는 구현 실패로 이어질 수 있습니다. 효율적인 문제 해결을 위한 첫 단계는 문제점을 정확하게 식별하는 것입니다.

## 문제 공간 정의

문제의 증상을 파악한 후에는 문제 공간을 정의해야 합니다. 영향을 받는 그리고 문제의 원인일 수 있는 소프트웨어 또는 하드웨어 구성 요소와 문제와 관련 없는 구성 요소를 식별합니다.

## 가능한 솔루션 테스트

문제의 증상 및 문제와 연관된 구성 요소를 파악했다면 문제가 해결될 때까지 체계적으로 솔루션을 테스트합니다.



(문제 해결 기본 사항)

## 증상 식별

구현에서 문제 해결을 시도하기 전에 실패의 원인을 정확하게 식별해야 합니다.

문제 해결 프로세스의 첫 번째 단계는 발생한 특정 증상을 정의하는 정보를 수집하는 것입니다. 이 정보를 수집할 때 다음과 같은 질문을 할 수 있습니다.

- 발생하지 않은 작업 또는 예상 동작은 무엇입니까?
- 영향을 받는 작업을 개별 평가가 가능한 하위 작업으로 나눌 수 있습니까?
- 작업에서 오류가 발생합니까? 오류 메시지가 해당 오류와 관련되어 있습니까?
- 작업이 완료되기는 하지만 너무 오래 걸립니까?
- 오류 발생이 일관됩니까? 아니면 산발적입니까?
- 최근에 오류와 관련이 있을 수 있는 소프트웨어 또는 하드웨어 변경이 있었습니까?

## 문제 공간 정의

문제의 증상을 식별한 후에는 설정에서 영향을 받는 구성 요소, 문제를 야기하는 구성 요소 그리고 문제에 연관되지 않은 구성 요소를 판별해야 합니다.

vSphere 구현에서 문제 공간을 정의하려면 현재 어떤 구성 요소가 존재하는지 확실히 알아야 합니다. VMware 소프트웨어 외에, 사용 중인 타사 소프트웨어 및 VMware 가상 하드웨어와 함께 사용 중인 하드웨어도 고려하십시오.

소프트웨어/하드웨어 요소의 특성 및 이러한 특성이 문제에 영향을 미치는 방식을 인식함으로써 증상을 야기할 수 있는 일반적인 문제점을 살펴볼 수 있습니다.

- 잘못된 소프트웨어 설정 구성
- 물리적 하드웨어 장애
- 구성 요소의 비호환성



프로세스를 세분화하고 세분화된 각 프로세스의 연관 가능성을 개별적으로 고려합니다. 예를 들어, 로컬 스토리지의 가상 디스크와 관련된 경우는 타사 라우터 구성과 관련이 없을 수 있습니다. 하지만 로컬 디스크 컨트롤러 설정은 문제의 원인일 수 있습니다. 어떤 구성 요소가 특정 증상과 관련이 없는 경우 해당 구성 요소를 솔루션 테스트를 위한 후보에서 제외할 수 있습니다.

문제가 시작되기 전 최근에 어떤 구성을 변경했는지 생각해 보십시오. 문제의 공통 부분을 찾아 보십시오. 몇 가지 문제가 동시에 시작되었다면 모든 문제를 동일 원인으로 추적할 수 있습니다.

## 가능한 솔루션 테스트

문제의 증상 그리고 해당 문제와 관련되어 있을 가능성이 가장 높은 소프트웨어 또는 하드웨어 구성 요소를 파악했다면 문제가 해결될 때까지 체계적으로 솔루션을 테스트할 수 있습니다.

영향을 받는 구성 요소 및 증상과 관련하여 얻은 정보를 토대로 문제를 확인하고 해결하기 위한 테스트를 설계할 수 있습니다. 다음 팁을 사용하면 이 프로세스의 효율성을 더 높일 수 있습니다.

- 잠재적 솔루션에 대한 아이디어를 가능한 많이 구상합니다.
- 각 솔루션이 문제의 해결 여부를 분명하게 판별하는지 확인합니다. 각각의 잠재적 솔루션을 테스트하되 문제가 해결되지 않으면 다음 솔루션으로 즉시 전환합니다.
- 가능성을 기반으로 잠재적 솔루션의 계층을 개발하고 실행합니다. 증상이 사라질 때까지 가능성이 가장 높은 것에서 가장 낮은 것 순으로 각각의 잠재적 문제를 체계적으로 제거합니다.
- 잠재적 솔루션을 테스트할 때에는 한 번에 하나의 설정만 변경합니다. 한 번에 여러 설정을 변경하면 문제가 해결된다고 해도 어떠한 설정 변경으로 문제가 해결되었는지 파악하지 못할 수 있습니다.
- 설정을 변경했는데도 문제를 해결하는 데 도움이 되지 않았다면 구현을 이전 상태로 되돌립니다. 구현을 이전 상태로 되돌리지 않으면 새로운 문제가 발생할 수 있습니다.
- 정상적으로 작동하는 유사한 구현을 찾아 제대로 작동하지 않는 구현과 병렬로 테스트합니다. 두 시스템 간 차이점이 몇 가지 또는 단 한 가지가 될 때까지 두 시스템의 설정을 동시에 변경합니다.

## vCenter Server 로그를 사용하여 문제 해결

사용자 구현에서 사용 중인 다양한 서비스 및 에이전트가 제공하는 로그를 검토하면 종종 유용한 문제 해결 정보를 얻을 수 있습니다.

대부분의 로그는 vCenter Server 배포의 `/var/log/vmware/<service_name>`에 있습니다.

### 일반 로그

다음 로그는 모든 vCenter Server 배포에 공통입니다.

표 19-1. 일반 로그 디렉토리

로그 디렉토리	설명
<code>../firstboot</code>	첫 번째 부팅 로그 저장
<code>applmgmt</code> 및 <code>applmgmt-audit</code>	VMware Appliance Management Service와 관련된 로그 저장

표 19-1. 일반 로그 디렉토리 (계속)

로그 디렉토리	설명
cloudvm	서비스 간 리소스 할당 및 배포에 대한 로그 저장
rhttpproxy	VMware HTTP Reverse Proxy 서비스에 대한 로그 저장
sca	VMware Service Control Agent 서비스에 대한 로그 저장
vapi	VMware vAPI Endpoint 서비스에 대한 로그 저장
vmafdd	VMware Authentication Framework - LDAP 서비스에 대한 로그 저장
vmdird	VMware Directory Service - LDAP 서비스에 대한 로그 저장
vmon	VMware Service Lifecycle Manager 서비스에 대한 로그 저장

## 관리 노드 로그

관리 노드 배포가 선택된 경우 다음 로그를 사용할 수 있습니다.

표 19-2. 관리 노드 로그 디렉토리

로그 디렉토리	서비스
rbd	VMware vSphere Auto Deploy
content-library	VMware Content Library Service
eam	VMware ESX Agent Manager
netdumper	VMware vSphere ESXi Dump Collector
perfcharts	VMware 성능 차트 서비스
vmcam	VMware vSphere Authentication Proxy
vmdird	VMware Directory Service - LDAP
vmware-sps	VMware vSphere Profile-Driven Storage Service
vpzd	VMware vCenter Server
vpostgres	VMware Postgres 서비스
vcha	VMware vCenter High Availability 서비스

## MAC 주소 할당 문제 해결

vSphere에서, 가상 시스템에 할당할 수 있는 MAC 주소 범위에 대한 특정 제한이 연결 손실 문제 또는 워크로드의 전원을 켜지 못하는 문제를 유발할 수 있습니다.

## 동일한 네트워크에 있는 가상 시스템의 중복된 MAC 주소

vCenter Server에서 생성된 가상 시스템의 MAC 주소가 중복되어 패킷이 손실되고 연결이 끊깁니다.

### 문제

동일한 브로드캐스트 도메인 또는 IP 서브넷에서 가상 시스템의 MAC 주소가 충돌하거나 새로 생성된 가상 시스템에 대해 vCenter Server가 중복된 MAC 주소를 생성합니다.

가상 시스템이 전원이 켜지고 제대로 작동하지만 다른 가상 시스템과 MAC 주소를 공유합니다. 이로 인해 패킷 손실 및 기타 문제가 발생할 수 있습니다.

### 원인

여러 가지 이유로 가상 시스템의 MAC 주소가 중복될 수 있습니다.

- 두 vCenter Server 인스턴스의 ID가 동일하여 가상 시스템 네트워크 어댑터에 대해 겹치는 MAC 주소가 생성됩니다.

각 vCenter Server 인스턴스의 ID는 0에서 63 사이로 설치 시 임의로 생성되지만, 설치 후 재구성할 수 있습니다. vCenter Server는 이 인스턴스 ID를 사용하여 가상 시스템의 네트워크 어댑터에 대한 MAC 주소를 생성합니다.

- 가상 시스템이 전원이 꺼진 상태에서 공유 스토리지 등을 사용하여 한 vCenter Server 인스턴스에서 동일 네트워크에 있는 다른 인스턴스로 전송되었고 첫 번째 vCenter Server에 있는 새 가상 시스템 네트워크 어댑터가 해제된 MAC 주소를 받습니다.

### 해결책

- ◆ 가상 시스템 네트워크 어댑터의 MAC 주소를 수동으로 변경합니다.

MAC 주소가 충돌하는 기존 가상 시스템이 있을 경우 **가상 하드웨어** 설정에서 고유한 MAC 주소를 제공해야 합니다.

- 가상 시스템의 전원을 끄고 수동 MAC 주소를 사용하도록 어댑터를 구성한 다음 새 주소를 입력합니다.
- 구성 시 가상 시스템의 전원을 끌 수 없을 경우 수동 MAC 주소 할당을 구성하도록 설정한 상태에서 충돌하는 네트워크 어댑터를 다시 생성하고 새 주소를 입력합니다. 게스트 운영 체제에서 다시 추가한 어댑터에 전과 동일한 정적 IP 주소를 설정합니다.

가상 시스템의 네트워크 어댑터 구성에 대한 자세한 내용은 "vSphere 네트워킹" 및 "vSphere 가상 시스템 관리" 설명서를 참조하십시오.

- ◆ vCenter Server 인스턴스가 기본 할당인 VMware OUI에 따라 가상 시스템의 MAC 주소를 생성하는 경우 vCenter Server 인스턴스 ID를 변경하거나 다른 할당 방법을 사용하여 충돌을 해결합니다.

**참고** vCenter Server 인스턴스 ID를 변경하거나 다른 할당 체계로 전환해도 기존 가상 시스템의 MAC 주소 충돌은 해결되지 않습니다. 변경 후 생성된 가상 시스템 또는 추가된 네트워크 어댑터만 새 체계에 따라 주소를 받기 때문입니다.

MAC 주소 할당 체계 및 설정에 대한 자세한 내용은 "vSphere 네트워킹" 설명서를 참조하십시오.

솔루션	설명
vCenter Server ID 변경	<p>배포 환경에 vCenter Server 인스턴스 수가 적을 경우 VMware OUI 할당 체계를 계속 사용할 수 있습니다. 이 체계에 따라 MAC 주소는 다음과 같은 형식으로 구성됩니다.</p> <pre>00:50:56:XX:YY:ZZ</pre> <p>여기서 00:50:56은 VMware OUI를 나타내고 XX는 (80 + vCenter Server ID)로 계산되며 YY:ZZ는 난수입니다.</p> <p>vCenter Server ID를 변경하려면 vCenter Server 인스턴스의 <b>일반</b> 설정을 열고 <b>런타임 설정</b> 섹션에서 <b>vCenter Server 고유 ID</b> 옵션을 구성한 다음 vCenter Server 인스턴스를 다시 시작합니다.</p> <p>VMware OUI 할당은 최대 64개의 vCenter Server 인스턴스에 적용되며, 소규모 배포 환경에 적합합니다.</p>
접두사 기반 할당으로 전환	<p>사용자 지정 OUI를 사용할 수 있습니다. 예를 들어 LAA(Locally Administered Address) 범위가 02:12:34인 경우 MAC 주소의 형식은 02:12:34:XX:YY:ZZ입니다. 네 번째 8진수 XX를 사용하여 OUI 주소 공간을 vCenter Server 인스턴스 간에 분산할 수 있습니다. 이 구조는 255개의 주소 클러스터를 지원하고 각 클러스터는 vCenter Server 인스턴스에서 관리하며 vCenter Server별로 MAC 주소 약 65,000개를 지원합니다. 예를 들어 vCenter Server A에는 02:12:34:01:YY:ZZ를, vCenter Server B에는 02:12:34:02:YY:ZZ를 지정하는 방식으로 사용됩니다.</p> <p>접두사 기반 할당은 대규모 배포 환경에 적합합니다.</p> <p>전 세계적으로 고유한 MAC 주소의 경우 OUI를 IEEE에 등록해야 합니다.</p>

- a MAC 주소 할당을 구성합니다.
- b 기존 가상 시스템의 **가상 하드웨어** 설정에서 새 MAC 주소 할당 체계를 적용합니다.
  - 가상 시스템의 전원을 끄고 수동 MAC 주소를 사용하도록 어댑터를 구성한 다음 자동 MAC 주소 할당으로 되돌리고 가상 시스템의 전원을 켭니다.
  - 가상 시스템이 운영 환경에 있어 구성 시 전원을 끌 수 없는 경우 vCenter Server ID 또는 주소 할당 체계를 변경한 후 자동 MAC 주소 할당을 구성하도록 설정한 상태에서 충돌하는 네트워크 어댑터를 다시 생성합니다. 게스트 운영 체제에서 다시 추가한 어댑터에 전과 동일한 정적 IP 주소를 설정합니다.

- ◆ 데이터스토어의 가상 시스템 파일을 사용하여 가상 시스템을 vCenter Server 인스턴스 간에 전송할 때 MAC 주소 재생성을 적용합니다.
  - a 가상 시스템의 전원을 끄고 인벤토리에서 제거한 다음 해당 구성 파일(.vmtx)에서 ethernetX.addressType 매개 변수를 **generated**로 설정합니다.  
ethernet 옆의 x는 가상 시스템에서 가상 NIC의 시퀀스 번호를 나타냅니다.
  - b 데이터스토어의 가상 시스템을 대상 vCenter Server에 등록하여 한 vCenter Server 시스템에서 다른 시스템으로 가상 시스템을 가져옵니다.  
가상 시스템 파일은 두 vCenter Server 인스턴스 간에 공유되는 데이터스토어에 배치하거나 대상 vCenter Server 시스템에서만 액세스할 수 있는 데이터스토어에 업로드할 수 있습니다.  
데이터스토어의 가상 시스템을 등록하는 방법에 대한 자세한 내용은 "vSphere 가상 시스템 관리" 항목을 참조하십시오.
  - c 처음으로 가상 시스템의 전원을 켵니다.  
가상 시스템이 시작되는 동안 vSphere Client에 가상 시스템에 대한 정보 아이콘이 표시됩니다.
  - d 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **게스트 운영 체제 > 질문에 응답**을 선택합니다.
  - e **복사함** 옵션을 선택합니다.  
대상 vCenter Server가 가상 시스템의 MAC 주소를 다시 생성합니다. 새로운 MAC 주소는 VMware OUI 00:0c:29로 시작하고 가상 시스템의 BIOS UUID를 기반으로 합니다. 가상 시스템의 BIOS UUID는 호스트의 BIOS UUID를 기준으로 계산됩니다.
- ◆ vCenter Server와 호스트가 버전 6.0 이상이고 vCenter Server 인스턴스가 고급 연결 모드에서 연결되어 있는 경우 vCenter Server 시스템에서 vMotion을 사용하여 가상 시스템을 마이그레이션하십시오.  
vCenter Server 시스템에서 가상 시스템이 마이그레이션되면 소스 vCenter Server가 가상 시스템의 MAC 주소를 거부 목록에 추가하고 다른 가상 시스템에 할당하지 않습니다.

## MAC 주소 충돌로 인해 가상 시스템 전원 켜기 시도가 실패함

가상 시스템 어댑터에 특정 정적 MAC 주소를 설정하면 가상 시스템의 전원을 켤 수 없습니다.

### 문제

vSphere Client에서 가상 시스템에 00:50:56:40:YY:ZZ - 00:50:56:7F:YY:ZZ 범위 내의 MAC 주소를 할당하면 가상 시스템의 전원을 켜려는 시도가 실패하고 MAC 주소에서 충돌이 발생했다는 상태 메시지가 표시됩니다.

00:50:56:XX:YY:ZZ는 올바른 정적 이더넷 주소가 아닙니다. 기타 사용을 위한 VMware의 예약된 MAC과 충돌합니다.

### 원인

VMware OUI 00:50:56으로 시작되며 vCenter Server 시스템의 호스트 VMkernel 어댑터에 할당된 주소 범위 내에 있는 MAC 주소를 할당하려고 합니다.

## 해결책

VMware OUI 접두사를 유지하려는 경우 00:50:56:00:00:00 - 00:50:56:3F:FF:FF 범위 내에서 정적 MAC 주소를 설정합니다. 그렇지 않으면 접두사가 VMware OUI와 다른 임의의 MAC 주소를 설정합니다. VMware OUI 접두사가 있는 정적 MAC 주소에 사용 가능한 범위에 대한 자세한 내용은 "vSphere 네트워킹" 설명서를 참조하십시오.

## vSphere Distributed Switch에서 호스트를 제거할 수 없음

경우에 따라 vSphere Distributed Switch에서 호스트를 제거하지 못할 수 있습니다.

### 문제

- vSphere Distributed Switch에서 호스트를 제거하려는 시도가 실패하고 리소스가 아직 사용 중이라는 알림을 받습니다. 사용자가 받는 알림은 다음과 같을 수 있습니다.

```
'16' 리소스가 사용 중입니다. vDS DSwitch 포트 16이 MyVM nic=4000 type=vmVnic에 연결된 호스트 10.23.112.2에 아직 있습니다.
```

- 호스트에서 이전 네트워킹 구성에서 설정한 호스트 프록시 스위치를 제거하려는 시도가 실패합니다. 예를 들어 호스트를 다른 데이터 센터 또는 vCenter Server 시스템으로 이동하거나 ESXi 및 vCenter Server 소프트웨어를 업그레이드한 후 새 네트워킹 구성을 생성합니다. 호스트 프록시 스위치를 제거하려고 하면 프록시 스위치의 리소스가 아직 사용 중이기 때문에 작업이 실패합니다.

### 원인

다음과 같은 이유로 Distributed Switch에서 호스트를 제거할 수 없거나 호스트 프록시 스위치를 삭제할 수 없습니다.

- 스위치에 사용 중인 VMkernel 어댑터가 있습니다.
- 스위치에 연결된 가상 시스템 네트워크 어댑터가 있습니다.

## 해결책

문제	솔루션
Distributed Switch에서 호스트를 제거할 수 없음	<ol style="list-style-type: none"> <li>1 vSphere Client에서 Distributed Switch로 이동합니다.</li> <li>2 구성 탭에서 <b>더 보기 &gt; 포트</b>를 선택합니다.</li> <li>3 아직 사용 중인 포트를 모두 찾고, 호스트에서 포트에 아직 연결되어 있는 VMkernel 또는 가상 시스템 네트워크 어댑터를 확인합니다.</li> <li>4 스위치에 아직 연결되어 있는 VMkernel 및 가상 시스템 네트워크 어댑터를 마이그레이션하거나 삭제합니다.</li> <li>5 vSphere Client에서 <b>호스트 추가 및 관리</b> 마법사를 사용하여 스위치에서 호스트를 제거합니다. 호스트가 제거되면 호스트 프록시 스위치가 자동으로 삭제됩니다.</li> </ol>
호스트 프록시 스위치를 제거할 수 없음	<ol style="list-style-type: none"> <li>1 vSphere Client에서 호스트로 이동합니다.</li> <li>2 호스트 프록시 스위치에 아직 연결되어 있는 VMkernel 또는 가상 시스템 네트워크 어댑터를 삭제하거나 마이그레이션합니다.</li> <li>3 호스트의 네트워킹 보기에서 호스트 프록시 스위치를 삭제합니다.</li> </ol>

## vSphere Distributed Switch의 호스트와 vCenter Server의 연결 끊김

포트 그룹 구성 후 vSphere Distributed Switch의 호스트가 vCenter Server에 연결하지 못합니다.

### 문제

관리 네트워크의 VMkernel 어댑터가 포함된 vSphere Distributed Switch에서 포트 그룹의 네트워킹 구성을 변경하면 이 스위치의 호스트와 vCenter Server의 연결이 끊어집니다. vSphere Client에서 호스트의 상태가 응답하지 않음으로 나타납니다.

### 원인

네트워킹 롤백이 비활성화된 vCenter Server의 vSphere Distributed Switch에서는 관리 네트워크의 VMkernel 어댑터가 포함된 포트 그룹이 vCenter Server에서 잘못 구성되고 이 잘못된 구성이 스위치의 호스트에 전파됩니다.

**참고** vSphere 네트워킹에서는 기본적으로 롤백이 사용되도록 설정되어 있습니다. 하지만 vCenter Server 수준에서 롤백을 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 "vSphere 네트워킹" 설명서를 참조하십시오.

## 해결책

- 1 영향받는 호스트에 대한 DCUI(Direct Console User Interface)에서 **네트워크 복원 옵션** 메뉴의 **vDS 복원 옵션**을 사용하여 관리 네트워크의 VLAN에 대한 ID와 업링크를 구성합니다.

DCUI에서 사용 후 삭제 로컬 포트가 생성되고 VLAN 및 업링크 구성이 포트에 적용됩니다. 또한 DCUI에서 새 호스트 로컬 포트를 사용하도록 관리 네트워크의 VMkernel 어댑터를 변경하여 vCenter Server와의 연결을 복원합니다.

호스트가 vCenter Server에 다시 연결된 후 vSphere Client에서 스위치에 있는 일부 호스트의 네트워킹 구성이 vSphere Distributed Switch에 저장된 구성과 다르다는 주의가 표시됩니다.

- 2 vSphere Client에서 관리 네트워크의 분산 포트 그룹을 올바른 설정으로 구성합니다.

상황	솔루션
포트 그룹 구성을 한 번만 변경했을 경우	포트 그룹의 구성을 한 단계 뒤로 롤백할 수 있습니다. 포트 그룹을 마우스 오른쪽 버튼으로 클릭하고 <b>구성 복원</b> 을 클릭한 후 <b>이전 구성으로 복원</b> 을 선택합니다.
유효한 포트 그룹 구성을 백업했을 경우	백업 파일을 사용하여 포트 그룹의 구성을 복원할 수 있습니다. 포트 그룹을 마우스 오른쪽 버튼으로 클릭하고 <b>구성 복원</b> 을 클릭한 후 <b>파일에서 구성 복원</b> 을 선택합니다. 또한 스위치의 백업 파일을 사용하여 포트 그룹을 포함한 전체 스위치의 구성을 복원할 수도 있습니다.
두 단계 이상의 구성을 수행했고 백업 파일이 없을 경우	포트 그룹에 유효한 설정을 수동으로 제공해야 합니다.

네트워킹 롤백, 복구 및 복원에 대한 자세한 내용은 "vSphere 네트워킹" 설명서를 참조하십시오.

- 3 **호스트 추가 및 관리** 마법사를 사용하여 관리 네트워크의 VMkernel 어댑터를 호스트 사용 후 삭제 로컬 포트에서 스위치의 분산 포트에 마이그레이션합니다.

분산 포트와 달리 VMkernel의 사용 후 삭제 로컬 포트 ID는 숫자가 아닙니다.

**호스트 추가 및 관리** 마법사를 통해 VMkernel 어댑터를 처리하는 방법에 대한 자세한 내용은 "vSphere 네트워킹" 설명서를 참조하십시오.

- 4 vCenter Server의 분산 포트 그룹 및 VMkernel 어댑터 구성을 호스트에 적용합니다.
  - vCenter Server의 올바른 분산 포트 그룹 및 VMkernel 어댑터 구성을 호스트에 푸시합니다.
    - a vSphere Client에서 호스트로 이동합니다.
    - b **구성** 탭에서 **네트워킹**을 클릭합니다.
    - c **가상 스위치** 목록에서 Distributed Switch를 선택하고 **호스트에서 선택한 Distributed Switch 상태 수정**을 클릭합니다.
  - vCenter Server가 다음 24시간 내에 설정을 적용할 때까지 기다립니다.

## 호스트의 네트워크 이중화 손실에 대한 경보

호스트의 vSphere 표준 스위치 또는 vSphere Distributed Switch에서 업링크 이중화가 손실되었음을 보고하는 경보가 발생합니다.

### 문제

특정 표준 스위치 또는 Distributed Switch에 연결되어 있는 호스트에 중복된 물리적 NIC가 없으면 다음 경보가 나타납니다.

*Host name or IP* 네트워크 업링크 이중화가 손실됨



## 원인

호스트에 있는 물리적 NIC 하나만 특정 표준 스위치 또는 Distributed Switch에 연결됩니다. 중복된 물리적 NIC는 다운되거나 스위치에 할당되지 않습니다.

예를 들어 호스트의 물리적 NIC *vmnic0* 및 *vmnic1*이 *vSwitch0*에 연결된 환경에서 물리적 NIC *vmnic1*이 오프라인 상태가 되고 *vmnic0*만 *vSwitch0*에 연결된 상태가 되면 결과적으로, 호스트에서 *vSwitch0*에 대한 업링크 이중화가 손실됩니다.

## 해결책

호스트에서 업링크 이중화가 손실된 스위치를 확인합니다. 호스트의 물리적 NIC를 이 스위치에 하나 이상 더 연결하고 경보를 녹색으로 재설정합니다. vSphere Client 또는 ESXi Shell을 사용할 수 있습니다.

물리적 NIC가 다운되면 호스트에서 ESXi Shell을 사용하여 이 NIC를 다시 가동합니다.

ESXi Shell에서 네트워킹 명령을 사용하는 방법에 대한 자세한 내용은 "ESXCLI 참조"의 내용을 참조하십시오. vSphere Client의 호스트에서 네트워킹을 구성하는 방법에 대한 자세한 내용은 "vSphere 네트워킹"의 내용을 참조하십시오.

## 분산 포트 그룹의 업링크 페일오버 순서를 변경한 후에 가상 시스템의 연결 끊김

분산 포트 그룹의 페일오버 NIC 순서가 변경되면 해당 그룹과 연결된 가상 시스템의 외부 네트워크 연결이 끊깁니다.

## 문제

vCenter Server에서 vSphere Client 등을 사용하여 분산 포트 그룹에 대한 페일오버 그룹의 업링크를 다시 정렬하고 나면 포트 그룹의 일부 가상 시스템이 외부 네트워크에 더 이상 액세스하지 못할 수 있습니다.

## 원인

페일오버 순서를 변경한 후 여러 가지 이유로 인해 가상 시스템과 외부 네트워크의 연결이 끊길 수 있습니다.

- 가상 시스템을 실행하는 호스트의 물리적 NIC가 활성화 또는 대기로 설정된 업링크에 연결되어 있지 않습니다. 호스트의 물리적 NIC에 연결된 모든 포트 그룹 관련 업링크가 '사용되지 않음' 상태로 변경되었습니다.
- 호스트의 물리적 NIC가 없는 LAG(링크 집계 그룹)가 vSphere에서 LACP를 사용해야 하는 요구 사항에 따라 유일한 활성화 업링크로 설정됩니다.
- 가상 시스템 트래픽이 여러 VLAN에 분리되어 있으면 활성화 업링크에 대한 호스트의 물리적 어댑터가 이러한 VLAN의 트래픽을 처리하지 않는 물리적 스위치의 트렁크 포트에 연결될 수 있습니다.
- 포트 그룹이 IP 해시 로드 밸런싱 정책으로 구성되어 있으면 활성화 업링크 어댑터가 EtherChannel에 포함되지 않은 물리적 스위치 포트에 연결될 수 있습니다.

Distributed Switch의 중앙 토폴로지 다이어그램 또는 호스트의 프록시 스위치 다이어그램을 통해 포트 그룹의 가상 시스템과 관련 호스트 업링크 및 업링크 어댑터 간의 연결을 검토할 수 있습니다.

## 해결책

- ◆ 호스트의 단일 물리적 NIC에 연결된 업링크의 페일오버 순서를 활성으로 다시 복원합니다.
- ◆ 포트 그룹을 동일한 설정으로 생성하고, 유효한 수의 호스트 업링크를 사용하도록 설정하며, 가상 시스템 네트워킹을 해당 포트 그룹으로 마이그레이션합니다.
- ◆ NIC를 활성 페일오버 그룹에 속한 업링크로 이동합니다.

vSphere Client를 사용하여 호스트 물리적 NIC를 다른 업링크로 이동할 수 있습니다.

- Distributed Switch의 **호스트 추가 및 관리** 마법사를 사용합니다.
  - a vSphere Client에서 Distributed Switch로 이동합니다.
  - b **작업** 메뉴에서 **호스트 추가 및 관리**를 선택합니다.
  - c **작업 선택** 페이지에서 **호스트 네트워킹 관리** 옵션을 선택하고 호스트를 선택합니다.
  - d 호스트의 NIC를 활성 업링크에 할당하려면 **물리적 네트워크 어댑터 관리** 페이지로 이동하고 NIC를 스위치 업링크에 연결합니다.
- 호스트 수준에서 NIC를 이동합니다.
  - a vSphere Client의 호스트로 이동하고 **구성** 탭에서 **네트워킹** 메뉴를 확장합니다.
  - b **가상 스위치**를 선택하고 분산 프록시 스위치를 선택합니다.
  - c **선택한 스위치에 연결된 물리적 네트워크 어댑터 관리**를 클릭하고 NIC를 활성 업링크로 이동합니다.

## 물리적 어댑터를 Network I/O Control이 사용하도록 설정된 vSphere Distributed Switch에 추가할 수 없음

1Gbps와 같이 속도가 느린 물리적 어댑터를 vSphere Network I/O Control 버전 3이 구성된 vSphere Distributed Switch에 추가하지 못할 수 있습니다.

### 문제

1Gbps와 같이 속도가 느린 물리적 어댑터를 10Gbps와 같이 속도가 빠른 물리적 어댑터와 연결된 vSphere Distributed Switch에 추가하려고 합니다. Network I/O Control 버전 3이 스위치에서 사용하도록 설정되어 있으며 vSphere 관리 트래픽, vSphere vMotion 트래픽, vSphere NFS 트래픽 등과 같은 여러 시스템 트래픽 유형을 위한 대역폭 예약이 존재합니다. 물리적 어댑터 추가 작업이 매개 변수가 잘못되었다는 상태 메시지가 표시되며 실패합니다.

```
A specified parameter was not correct: spec.host[].backing.pnicSpec[]
```

### 원인

Network I/O Control에서는 이미 Distributed Switch에 연결된 개별 물리적 어댑터의 10Gbps 속도를 예약하는 데 사용할 수 있는 대역폭을 정렬합니다. 이 대역폭의 일부를 예약한 후 10Gbps보다 속도가 낮은 물리적 어댑터를 추가하면 시스템 트래픽 유형을 처리하기 위한 잠재적 요구 사항을 충족하지 못할 수 있습니다.

Network I/O Control 버전 3에 대한 자세한 내용은 "vSphere 네트워킹" 설명서를 참조하십시오

### 해결책

- 1 vSphere Client에서 호스트로 이동합니다.
- 2 구성 탭에서 설정의 **시스템** 그룹을 확장합니다.
- 3 **고급 시스템 설정**을 선택하고 **편집**을 클릭합니다.
- 4 Network I/O Control 범위 밖에서 사용하려는 물리적 어댑터를 `Net.IOControlPnicOptOut` 매개 변수에 대해 심표로 구분된 목록으로 입력합니다.

예: `vmnic2,vmnic3`

- 5 **확인**을 클릭하여 변경 사항을 적용합니다.
- 6 vSphere Client에서 물리적 어댑터를 Distributed Switch에 추가합니다.

## SR-IOV 지원 워크로드 문제 해결

특정 상황에서, SR-IOV를 사용하여 물리적 네트워크 어댑터에 데이터를 전송하는 가상 시스템에서 연결 또는 전원 켜기 문제가 발생할 수 있습니다.

### 해당 MAC 주소를 변경한 후 SR-IOV 지원 워크로드가 통신할 수 없음

SR-IOV 지원 가상 시스템의 게스트 운영 체제에서 MAC 주소를 변경한 후 가상 시스템의 연결이 끊어집니다.

#### 문제

가상 시스템의 네트워크 어댑터를 SR-IOV VF(가상 기능)에 연결할 때 가상 시스템에 대한 패스스루 네트워크 어댑터를 생성하게 됩니다. 게스트 운영 체제의 (VF) 드라이버가 패스스루 네트워크 어댑터에 대한 MAC 주소를 수정하면 게스트 운영 체제는 변경에 성공한 것으로 표시할 수 있지만 VM 네트워크 어댑터는 연결이 끊어집니다. 게스트 운영 체제는 새 MAC 주소를 사용하도록 설정되었다고 표시할 수 있지만 `/var/log/vmkernel.log` 파일의 로그 메시지는 작업이 실패한 것으로 표시됩니다.

요청된 MAC 주소가 `vswitch` 정책에서 허용되지 않는 포트 VM NIC 포트 번호의 새 MAC 주소로 변경됩니다.

#### 위치

- 새 MAC 주소는 게스트 운영 체제의 MAC 주소입니다.
- VM NIC 포트 번호는 16진수 형식의 VM 네트워크 어댑터의 포트 번호입니다.

#### 원인

패스스루 네트워크 어댑터가 연결된 포트 그룹의 기본 보안 정책은 게스트 운영 체제에서 MAC 주소의 변경을 허용하지 않습니다. 따라서 게스트 운영 체제의 네트워킹 인터페이스는 IP 주소를 획득할 수 없어서 연결이 끊어집니다.

## 해결책

- ◆ 게스트 운영 체제에서 패스스루 네트워크 어댑터가 유효한 해당 MAC 주소를 다시 얻으려면 인터페이스를 재 설정합니다. 인터페이스가 DHCP를 사용하여 주소를 할당하도록 구성된 경우 인터페이스가 자동으로 IP 주소를 획득합니다.

예를 들어 Linux 가상 시스템에서 `ifconfig` 콘솔 명령을 실행합니다.

```
ifconfig ethX down
ifconfig ethX up
```

여기서 `ethX`의 `X`는 게스트 운영 체제에서 가상 시스템 네트워크 어댑터의 시퀀스 번호를 나타냅니다.

## 호스트의 인터럽트 벡터 부족으로 SR-IOV 가상 기능을 사용하는 가상 시스템의 전원이 켜지지 않음

ESXi 호스트에서 네트워킹에 대해 SR-IOV VF(가상 기능)를 사용하는 가상 시스템 하나 이상의 전원이 꺼집니다.

### 문제

ESXi 호스트에서, 할당된 가상 기능의 총 수가 "vSphere 구성 최대값" 가이드에 지정된 가상 기능의 최대 수에 근접하면 네트워킹에 대한 SR-IOV 가상 기능(VF)을 사용하는 하나 이상의 가상 시스템 전원이 켜지지 않습니다.

가상 시스템 로그 파일 `vmware.log`에는 VF와 관련된 다음 메시지가 포함되어 있습니다.

```
PCIPassthruChangeIntrSettings: vf_name failed to register interrupt (error code 195887110)
```

VMkernel 로그 파일 `vmkernel.log`에는 가상 시스템에 할당된 VF와 관련된 다음 메시지가 포함되어 있습니다.

```
VMKPCIPassthru: 2565: BDF = vf_name intrType = 4 numVectors: 3
WARNING: IntrVector: 233: Out of interrupt vectors
```

### 원인

할당 가능한 인터럽트 벡터의 수는 ESXi 호스트에 있는 물리적 CPU의 수에 따라 증가합니다. 32개의 CPU가 있는 ESXi 호스트는 총 4096개의 인터럽트 벡터를 제공할 수 있습니다. 호스트가 부팅될 때 스토리지 컨트롤러, 물리적 네트워크 어댑터 및 USB 컨트롤러와 같은 호스트 디바이스는 벡터 4096개 중 일부를 사용합니다. 이러한 디바이스에 벡터가 1024개보다 많이 필요한 경우 지원될 수 있는 최대 VF 수가 줄어듭니다.

가상 시스템의 전원이 켜지고 게스트 운영 체제 VF 드라이버가 시작될 때 인터럽트 벡터가 사용됩니다. 인터럽트 벡터를 필요한 수만큼 사용할 수 없는 경우 게스트 운영 체제가 오류 메시지 없이 예기치 않게 종료됩니다.

호스트에서 사용되거나 사용 가능한 인터럽트 벡터의 수를 확인할 수 있는 규칙은 현재 없습니다. 이 수는 호스트의 하드웨어 구성에 따라 달라집니다.

## 해결책

- ◆ 가상 시스템의 전원을 켜려면 호스트의 가상 시스템에 할당된 총 VF 수를 줄입니다.

예를 들어 vSphere 표준 스위치 또는 vSphere Distributed Switch에 연결된 어댑터에 대한 가상 시스템의 SR-IOV 네트워크 어댑터를 변경합니다.

## VPN 클라이언트를 실행하는 가상 시스템으로 인해 호스트 또는 vSphere HA 클러스터에서 가상 시스템에 대한 서비스 거부가 발생함

VPN 클라이언트와 같이 BPDU(Bridge Protocol Data Unit) 프레임을 보내는 가상 시스템으로 인해 동일한 포트 그룹에 연결된 일부 가상 시스템의 연결이 끊어질 수 있습니다. 또한 BPDU 프레임 전송으로 인해 호스트 또는 상위 vSphere HA 클러스터의 연결이 끊어질 수도 있습니다.

### 문제

BPDU 프레임을 보낼 것으로 예상되는 가상 시스템으로 인해 동일한 포트 그룹에 있는 가상 시스템의 외부 네트워크로 보내는 트래픽이 차단될 수 있습니다.

가상 시스템이 vSphere HA 클러스터에 속한 호스트에서 실행되고 호스트가 특정 조건에 따라 네트워크에서 분리되면 클러스터의 모든 호스트에서 DoS(서비스 거부)가 나타납니다.

### 원인

가장 좋은 방법은 ESXi 호스트에 연결된 물리적 스위치 포트에서 PortFast 및 BPDU 가드를 사용하도록 설정하여 STP(스패닝 트리 프로토콜)의 경계를 적용하는 것입니다. 표준 스위치 또는 Distributed Switch는 STP를 지원하지 않으며 스위치 포트에 BPDU 프레임을 보내지 않습니다. 하지만 손상된 가상 시스템에서 보내는 BPDU 프레임이 ESXi 호스트와 연결된 물리적 스위치 포트에 도착하면 BPDU 가드 기능이 해당 포트를 비활성화하여 프레임이 네트워크의 STP(Spanning Tree Topology)에 영향을 미치지 못합니다.

Windows 브리지 디바이스 또는 브리지 기능을 통해 연결된 VPN을 배포하는 등의 특정한 경우에는 가상 시스템에서 BPDU 프레임을 보낼 수 있습니다. 이 가상 시스템의 트래픽을 처리하는 물리적 어댑터와 쌍으로 구성된 물리적 스위치 포트에서 BPDU 가드가 설정되면 포트가 오류로 인해 비활성화되고 호스트의 물리적 어댑터를 사용하는 VMkernel 어댑터 및 가상 시스템이 더 이상 외부 네트워크와 통신할 수 없습니다.

포트 그룹의 팀 구성 및 페일오버 정책에 여러 활성 업링크가 포함되어 있을 경우 BPDU 트래픽이 그 다음 활성 업링크의 어댑터로 이동됩니다. 새로운 물리적 스위치 포트는 비활성화되고 더 많은 워크로드에서 네트워크를 통해 패킷을 교환할 수 없게 됩니다. 결국 ESXi 호스트의 거의 모든 엔티티에 액세스하지 못하게 될 수도 있습니다.

가상 시스템이 vSphere HA 클러스터에 속한 호스트에서 실행되고 호스트에 연결된 대부분의 물리적 스위치 포트가 비활성화되어 호스트가 네트워크에서 분리되면 클러스터의 활성 기본 호스트가 BPDU를 보내는 가상 시스템을 다른 호스트로 이동합니다. 가상 시스템은 새 호스트에 연결된 물리적 스위치 포트를 비활성화하기 시작합니다. vSphere HA 클러스터 전체의 마이그레이션은 결국 전체 클러스터에서 누적된 DoS(서비스 거부)를 유발합니다.

## 해결책

- ◆ VPN 소프트웨어를 가상 시스템에서 계속 작동해야 할 경우 가상 시스템에서 내보내는 트래픽을 허용하고 BPDU 프레임을 통과시키도록 물리적 스위치 포트를 개별적으로 구성해야 합니다.

네트워크 디바이스	구성
Distributed Switch 또는 표준 스위치	<p>포트 그룹의 위조 전송 보안 속성을 <b>동의로</b> 설정하여 BPDU 프레임이 호스트에서 출발해서 물리적 스위치 포트에 도달하도록 허용합니다.</p> <p>가상 시스템을 별도의 포트 그룹에 배치하고 물리적 어댑터를 해당 그룹에 할당하는 방식으로 VPN 트래픽에 대한 설정 및 물리적 어댑터를 분리할 수 있습니다.</p> <p><b>경고</b> 위조 전송 보안 속성을 <b>동의로</b> 설정하여 호스트가 BPDU 프레임을 전송하도록 하면 손상된 가상 시스템이 스푸핑 공격을 수행할 수 있기 때문에 보안 위험이 야기됩니다.</p>
물리적 스위치	<ul style="list-style-type: none"> <li>■ PortFast를 사용하도록 설정된 상태로 유지합니다.</li> <li>■ 개별 포트에서 BPDU 필터를 사용하도록 설정합니다. BPDU 프레임이 해당 포트에 도착하면 필터링됩니다.</li> </ul> <p><b>참고</b> BPDU 필터를 전체적으로 사용하도록 설정하지 마십시오. BPDU 필터를 전체적으로 사용하도록 설정하면 PortFast 모드가 비활성화되고 모든 물리적 스위치 포트가 전체 STP 기능 집합을 수행합니다.</p>

- ◆ 동일한 계층 2 네트워크에 연결된 두 가상 시스템 NIC 간에 브리지 디바이스를 배포하려면 가상 시스템에서 BPDU 트래픽을 허용하고 PortFast 및 BPDU 루프 방지 기능을 비활성화해야 합니다.

네트워크 디바이스	구성
Distributed Switch 또는 표준 스위치	<p>포트 그룹에 대한 보안 정책의 위조 전송 속성을 <b>동의로</b> 설정하여 BPDU 프레임이 호스트에서 출발해서 물리적 스위치 포트에 도달하도록 허용합니다.</p> <p>가상 시스템을 별도의 포트 그룹에 배치하고 물리적 어댑터를 해당 그룹에 할당하는 방식으로 브리지 트래픽에 대한 설정 및 하나 이상의 물리적 어댑터를 분리할 수 있습니다.</p> <p><b>경고</b> 위조 전송 보안 속성을 <b>동의로</b> 설정하여 브리지 배포를 활성화하면 손상된 가상 시스템이 스푸핑 공격을 수행할 수 있기 때문에 보안 위험이 야기됩니다.</p>
물리적 스위치	<ul style="list-style-type: none"> <li>■ 가상 브리지 디바이스로 연결되는 포트에서 PortFast를 비활성화하여 해당 포트에서 STP를 실행합니다.</li> <li>■ 브리지 디바이스와 연결되는 포트에서 BPDU 가드 및 필터를 비활성화합니다.</li> </ul>

- ◆ ESXi 호스트 또는 물리적 스위치에서 BPDU 필터를 활성화하여 항상 DoS 공격으로부터 환경을 보호합니다.
  - ◆ 게스트 BPDU 필터가 구현되지 않은 호스트에서 가상 브리지 디바이스와 연결되는 물리적 스위치 포트에 대해 BPDU 필터를 사용하도록 설정합니다.

네트워크 디바이스	구성
Distributed Switch 또는 표준 스위치	포트 그룹에 대한 보안 정책의 위조 전송 속성을 <b>거부</b> 로 설정합니다.
물리적 스위치	<ul style="list-style-type: none"> <li>■ PortFast 구성을 그대로 유지합니다.</li> <li>■ 개별 물리적 스위치 포트에서 BPDU 필터를 사용하도록 설정합니다. BPDU 프레임이 해당 물리적 포트에 도착하면 필터링됩니다.</li> </ul> <p><b>참고</b> BPDU 필터를 전체적으로 사용하도록 설정하지 마십시오. BPDU 필터를 전체적으로 사용하도록 설정하면 PortFast 모드가 비활성화되고 모든 물리적 스위치 포트가 전체 STP 기능 집합을 수행합니다.</p>

## Windows 가상 시스템에서 UDP 워크로드에 대한 처리량이 낮음

vSphere의 Windows 가상 시스템에서 대형 UDP 패킷을 전송할 때 다른 트래픽이 무시해도 될 정도인 경우에도 처리량이 예상보다 낮거나 안정적이지 않습니다.

### 문제

Windows 가상 시스템에서 1024바이트보다 큰 UDP 패킷을 전송할 때 다른 트래픽이 무시해도 될 정도인 경우에도 처리량이 예상보다 낮거나 안정적이지 않습니다. 비디오 스트리밍 서버의 경우 비디오 재생이 일시 중지됩니다.

### 원인

1024바이트보다 큰 모든 UDP 패킷에 대해 Windows 네트워크 스택은 다음 패킷을 보내기 전에 전송 완료 인터럽트를 기다립니다. vSphere는 이러한 상황을 투명하게 해결하지 못합니다.

### 해결책

- ◆ Windows 게스트 OS의 레지스트리를 수정하여 UDP 패킷에 대해 Windows 동작이 변경되는 임계값(바이트)을 늘립니다.
  - HKLM\System\CurrentControlSet\Services\Afd\Parameters 레지스트리 키를 찾습니다.
  - 이름이 FastSendDatagramThreshold이고 종류가 DWORD인 값 1,500을 추가합니다.

Windows 레지스트리에서 이 문제를 해결하는 방법에 대한 자세한 내용은 <http://support.microsoft.com/kb/235257>을 참조하십시오.
- ◆ 가상 시스템 NIC의 병합 설정을 수정합니다.

Windows 가상 시스템에 VMXNET3 vNIC 어댑터가 있는 경우 가상 시스템의 .vmx 파일에서 다음 매개 변수 중 하나를 구성합니다. vSphere Client를 사용하거나 .vmx 파일을 직접 수정합니다.

작업	매개 변수	값
가상 시스템의 인터럽트 속도를 예상 패킷 속도보다 높은 값으로 설정합니다. 예를 들어 예상되는 패킷 속도가 초당 15,000번의 인터럽트인 경우 인터럽트 속도를 초당 16,000번의 인터럽트로 설정합니다. ethernetX.coalescingScheme 매개 변수를 <b>rbc</b> 로 설정하고, ethernetX.coalescingParams 매개 변수를 <b>16000</b> 으로 설정합니다. 기본 인터럽트 속도는 초당 4000번의 인터럽트입니다.	ethernetX.coalescingScheme ethernetX.coalescingParams	rbc 16000
낮은 처리량 또는 지연 시간에 민감한 워크로드에 대해 병합을 비활성화합니다. 지연 시간이 낮은 워크로드 구성에 대한 자세한 내용은 <a href="#">Best Practices for Performance Tuning of Latency-Sensitive Workloads in vSphere VMs</a> (vSphere VM에서 지연 시간에 민감한 워크로드의 성능 조정을 위한 모범 사례)을 참조하십시오.	ethernetX.coalescingScheme	사용 안 함
이전 ESXi 릴리스의 병합 알고리즘으로 복구합니다.	ethernetX.coalescingScheme	calibrate
<b>참고</b> 최신 vSphere 릴리스에서는 이전 알고리즘으로 복구하는 기능을 사용할 수 없습니다.		

ethernet 옆의 X는 가상 시스템에서 vNIC의 시퀀스 번호를 나타냅니다.

.vmx 파일에서 매개 변수를 구성하는 방법에 대한 자세한 내용은 "vSphere 가상 시스템 관리" 설명서를 참조하십시오.

◆ ESXi 호스트 병합 설정을 수정합니다.

이 방법은 호스트에 있는 모든 가상 시스템과 모든 가상 시스템 NIC에 영향을 미칩니다.

vSphere Client를 사용하거나 ESXi Shell에서 호스트에 대해 vCLI 콘솔 명령을 사용하여 호스트에 대한 고급 시스템 설정 목록을 편집할 수 있습니다.

작업	vSphere Client의 매개 변수	esxcli system settings advanced set 명령에 대한 매개 변수	값
기본 인터럽트 속도를 예상 패킷 속도보다 높게 설정합니다. 예를 들어 초당 15,000번의 인터럽트가 예상되는 경우 인터럽트 속도를 16,000으로 설정합니다.	Net.CoalesceScheme Net.CoalesceParams	/Net/CoalesceScheme /Net/CoalesceParams	rbc 16000
낮은 처리량 또는 지연 시간에 민감한 워크로드에 대해 병합을 비활성화합니다. 지연 시간이 낮은 워크로드 구성에 대한 자세한 내용은 <a href="#">Best Practices for Performance Tuning of Latency-Sensitive Workloads in vSphere VMs</a> (vSphere VM에서 지연 시간에 민감한 워크로드의 성능 조정을 위한 모범 사례)을 참조하십시오.	Net.CoalesceDefaultOn	/Net/ CoalesceDefaultOn	0
이전 ESXi 릴리스의 병합 체계로 복구합니다.	Net.CoalesceScheme	/Net/CoalesceScheme	calibrate
<b>참고</b> 최신 vSphere 릴리스에서는 이전 알고리즘으로 복구하는 기능을 사용할 수 없습니다.			

vSphere Client에서 호스트를 구성하는 방법에 대한 자세한 내용은 "vCenter Server 및 호스트 관리" 설명서를 참조하십시오. vCLI 명령을 사용하여 호스트 속성을 설정하는 방법에 대한 자세한 내용은 "ESXCLI 참조" 설명서를 참조하십시오.



## 동일한 분산 포트 그룹에 속하지만 서로 다른 호스트에 위치한 가상 시스템은 서로 통신할 수 없음

특정 상황에서 동일한 분산 포트 그룹에 속하지만 서로 다른 호스트에 위치한 가상 시스템은 서로 통신할 수 없습니다.

### 문제

동일한 포트 그룹에 속하지만 서로 다른 호스트에 상주하는 가상 시스템은 서로 통신할 수 없습니다. 가상 시스템 간에 ping하더라도 아무런 반응이 나타나지 않으며 vMotion을 사용하여 호스트 간에 가상 시스템을 마이그레이션할 수 없습니다.

### 원인

- 일부 호스트의 물리적 NIC가 분산 포트 그룹의 팀 구성 및 페일오버 순서대로 활성화 또는 대기 업링크에 할당되지 않았습니다.
- 활성화 또는 대기 업링크에 할당된 호스트의 물리적 NIC가 물리적 스위치의 서로 다른 VLAN에 상주합니다. 다른 VLAN의 물리적 NIC는 서로 인식할 수 없으므로 서로 통신할 수 없습니다.

### 해결책

- Distributed Switch의 토폴로지에서 분산 포트 그룹의 활성화 또는 대기 업링크에 할당된 물리적 NIC가 없는 호스트를 확인합니다. 해당 호스트의 물리적 NIC를 포트 그룹의 활성화 업링크에 하나 이상 할당합니다.
- Distributed Switch의 토폴로지에서 분산 포트 그룹의 활성화 업링크에 할당된 물리적 NIC의 VLAN ID를 확인합니다. 모든 호스트에서 동일한 VLAN의 물리적 NIC를 분산 포트 그룹의 활성화 업링크에 할당합니다.
- 물리적 계층에서 문제가 없음을 확인하려면 가상 시스템을 동일한 호스트로 마이그레이션하고 상호 간의 통신을 확인합니다. 게스트 OS에서 인바운드 및 아웃바운드 ICMP 트래픽이 사용되도록 설정되었는지 확인합니다. 기본적으로 ICMP 트래픽은 Windows Server 2008 및 Windows Server 2012에서 비활성화됩니다.

## 연결된 프로토콜 프로파일이 없어서 마이그레이션된 vApp 전원이 켜기가 실패함

네트워크 프로토콜 프로파일이 없기 때문에 데이터 센터 또는 vCenter Server 시스템으로 전송한 vApp 또는 가상 시스템의 전원을 켤 수 없습니다.

## 문제

다른 데이터 센터 또는 vCenter Server 시스템으로 vApp 또는 가상 시스템을 콜드 마이그레이션한 후 전원 켜기가 실패합니다. 연결된 네트워크 프로토콜 프로파일이 vApp 또는 가상 시스템의 네트워크에 없기 때문에 속성을 초기화하거나 할당할 수 없다는 오류 메시지가 표시됩니다.

'*property*' 속성을 초기화할 수 없습니다. 네트워크 '*port group*'에 연결된 네트워크 프로토콜 프로파일이 없습니다.

'*property*' 속성에 대해 IP 주소를 할당할 수 없습니다. 네트워크 '*port group*'에 연결된 네트워크 프로토콜 프로파일이 없습니다.

## 원인

vApp 또는 가상 시스템은 OVF 환경을 사용하여 해당 vApp 또는 가상 시스템의 포트 그룹과 관련된 네트워크 프로토콜 프로파일에서 네트워크 설정을 검색합니다.

vCenter Server는 vApp의 OVF를 설치할 때 이러한 네트워크 프로토콜 프로파일을 생성하고, 설치하는 동안 프로파일을 사용자가 지정하는 포트 그룹과 연결합니다.

프로토콜 프로파일과 포트 그룹 간의 매핑은 데이터 센터 범위에서만 유효합니다. 다음과 같은 이유 때문에 vApp을 이동할 때 해당 프로토콜 프로파일이 대상 데이터 센터로 전송되지 않습니다.

- 프로토콜 프로파일의 네트워크 설정이 대상 데이터 센터의 네트워크 환경에서 유효하지 않을 수 있습니다.
- 다른 프로토콜 프로파일과 연결되어 있으며 이름이 동일한 포트 그룹이 대상 데이터 센터에 이미 있을 수 있으며 vApp과 가상 시스템이 이 그룹에 연결되어 있을 수 있습니다. 포트 그룹에 대한 프로토콜 프로파일을 교체하면 이러한 vApp과 가상 시스템의 연결에 영향을 미칠 수 있습니다.

## 해결책

- 필요한 네트워크 설정을 사용하여 대상 데이터 센터 또는 vCenter Server 시스템에 네트워크 프로토콜 프로파일을 생성한 후 프로토콜 프로파일을 vApp 또는 가상 시스템이 연결되는 포트 그룹과 연결합니다. 이 방식은 vApp 또는 가상 시스템이 vCenter Extension vService를 사용하는 vCenter Server 확장인 경우 등에 적합합니다.

네트워크 프로토콜 프로파일에서 vApp 또는 가상 시스템으로 네트워크 설정을 제공하는 방법에 대한 자세한 내용은 "vSphere 네트워킹" 설명서를 참조하십시오.

- vSphere Client를 사용하여 vApp 또는 가상 시스템의 OVF 파일을 소스 데이터 센터 또는 vCenter Server 시스템에서 내보낸 후 대상 데이터 센터 또는 vCenter Server 시스템에 배포합니다.

vSphere Client를 사용하여 OVF 파일을 배포하면 대상 vCenter Server 시스템이 vApp에 대한 네트워크 프로토콜 프로파일을 생성합니다.

vSphere Client에서 OVF 파일을 관리하는 방법에 대한 자세한 내용은 "vSphere 가상 시스템 관리" 설명서를 참조하십시오.

## 네트워킹 구성 작업이 롤백되고 vCenter Server에서 호스트 연결이 끊김

호스트의 vSphere Distributed Switch에 네트워킹을 추가 또는 구성하려고 하면 작업이 롤백되고 vCenter Server에서 호스트 연결이 끊깁니다.

### 문제

호스트의 vSphere Distributed Switch에서 가상 시스템 어댑터 또는 포트 그룹 생성과 같은 네트워킹 구성 작업을 수행하려고 하면 vCenter Server에서 호스트 연결이 끊기고 호스트에서 트랜잭션이 롤백되었습니다. 오류 메시지가 표시됩니다.

### 원인

많은 동시 네트워킹 작업이 한정된 리소스를 놓고 경합하는 경우와 같이 호스트의 워크로드가 폭증하는 상황에서는 일부 작업을 수행하는 데 걸리는 시간이 Distributed Switch의 네트워크 구성 작업에 대한 기본 롤백 시간 제한을 초과할 수 있습니다. 이로 인해 해당 작업이 롤백됩니다.

예를 들어 스위치 포트 또는 가상 어댑터 수가 매우 많은 호스트에서 VMkernel 어댑터를 생성할 때 이러한 포트 또는 어댑터 전체가 호스트의 시스템 리소스를 소비한다면 이러한 상황이 일어날 수 있습니다.

작업 롤백에 대한 기본 시간 제한은 30초입니다.

### 해결책

- ◆ vCenter Server의 롤백 시간 제한을 늘리려면 vSphere Client를 사용합니다.
  - 같은 문제가 다시 발생하면 작업 성공에 필요한 충분한 시간이 설정될 때까지 롤백 시간 제한을 60초씩 늘립니다.
    - a vCenter Server 인스턴스의 구성 탭에서 설정을 확장합니다.
    - b 고급 설정을 선택하고 편집을 클릭합니다.
    - c 속성이 없으면 `config.vpxd.network.rollbackTimeout` 매개 변수를 설정에 추가합니다.
    - d `config.vpxd.network.rollbackTimeout` 매개 변수에 새로운 값(초)을 입력합니다.
    - e 확인을 클릭합니다.
    - f vCenter Server 시스템을 다시 시작하여 변경 내용을 적용합니다.
- ◆ `vpxd.cfg` 구성 파일을 편집하여 롤백 시간 제한을 늘립니다.
  - 같은 문제가 다시 발생하면 작업 성공에 필요한 충분한 시간이 설정될 때까지 롤백 시간 제한을 60초씩 늘립니다.
    - a vCenter Server의 호스트 시스템에서 `/etc/vmware-vpx` 디렉토리로 이동합니다.
    - b 편집할 `vpxd.cfg` 파일을 엽니다.

- c <network> 섹션에서 <rollbackTimeout> 요소의 시간 제한을 늘립니다.

```
<config>
  <vpxd>
    <network>
      <rollbackTimeout>60</rollbackTimeout>
    </network>
  </vpxd>
</config>
```

- d 파일을 저장한 후 닫습니다.
- e vCenter Server 시스템을 다시 시작하여 변경 내용을 적용합니다.